



TB116-DL

**Storage Barebone
User's Manual**

Table of Contents

Preface	i
Safety Instructions	ii
About This Manual	iv
Chapter 1. Product Features	1
1.1 Box Contents	1
1.2 Specifications	2
1.3 System Block Diagram.....	3
1.4 Feature.....	4
Chapter 2. Hardware Setup	6
2.1 Central Processing Unit	6
2.1.1 Installation	6
2.2 System Memory	10
2.2.1 Placement.....	10
2.2.2 DIMM Population	11
2.2.3 Installation	12
2.3 Top Cover	13
2.4 Power Supply Unit	14
2.4.1 Installation	14
2.4.2 LED Indicator	14
2.5 Fan	15
2.6 Disk Drive	16
2.6.1 HDD: 2.5-inch Installation	16
2.6.1 HDD: 3.5-inch Installation	17
2.8 PCIe Card	18
2.9 Slide Rail	19
Chapter 3. Hardware Settings	22
3.1 Motherboard Block Diagram	22
3.1.2 Placement	23
3.1.3 Content List.....	24
3.1.4 External Port	25
3.1.5 Connector Definition.....	26
3.1.6 Jumper Definition.....	41
3.1.7 Internal LED	46
Chapter 4. BIOS Configuration Settings	48
4.1 Navigation Keys.....	48
4.2 BIOS Setup	49
4.2.1 Menu	49
4.2.2 Startup	49
4.3 Main	50
4.4 Advanced	51

4.4.1 RC ACPI Settings	52
4.4.2 CPU Configuration.....	54
4.4.3 Power & Performance	57
4.4.4 Server ME Configuration.....	66
4.4.5 Server ME Debug Configuration	67
4.4.6 Thermal Configuration	71
4.4.6 Thermal Configuration	73
4.4.7 Platform Settings	75
4.4.8 System Event Log.....	77
4.4.9 Debug Settings	79
4.4.10 Debug Configuration	82
4.4.11 Trusted Computing	84
4.4.12 ACPI Settings	86
4.4.13 Serial Port Console Redirection	87
4.4.14 SIO Configuration.....	88
4.4.15 PCI Subsystem Settings	89
4.4.16 USB Configuration.....	90
4.4.17 Network Stack Configuration	92
4.5 Chipset.....	93
4.5.1 System Agent (SA) Configuration	94
4.5.2 PCH-IO Configuration.....	115
4.6 Security.....	129
4.6.1 Secure Boot	129
4.7 Boot	130
4.8 Save and Exit.....	131
4.9 Server Mgmt.....	132
4.9.1 System Event Log.....	134
4.9.2 BMC Network Configuration.....	135
4.9.3 View System Event Log	137
Chapter 5. BMC Configuration Settings	138
5.1 Login.....	138
5.2 Web GUI	139
5.2.1 Menu Bar.....	139
5.2.2 User Information and Quick Button	140
5.2.3 Dashboard	141
5.2.4 Sensor	141
5.2.5 FRU Information	142
5.2.6 Logs and Reports	142
5.2.7 Settings.....	143
5.2.8 Remote Control	144
5.2.9 Images redirection	145
5.2.10 Power Control.....	146
5.2.11 Maintenance.....	147
5.2.12 Sign out.....	148
Chapter 6. Technical Support.....	149

Document Release History

Release Date	Version	Update Content
March, 2022	1	User's Manual release to public.



Copyright © 2022 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 distintively 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 serverly 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 disintergration.
- Carefully and accurately mount the equipment into the rack. Uneven mechanical loading may lead to hazadous 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 Acess 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 TB116-DL.

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 TB116-DL. For the latest version of this user's manual, please refer to the AIC® website: <https://www.aicipc.com/en/productdetail/51334>.

Chapter 1 Product Features

TB116-DL 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 provides descriptions for the hardware, 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

TB116-DL 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.aicpc.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
✓	300W redundant power supply	1
✓	2.5-inch disk drive bracket	1
✓	2.5/3.5-inch disk drive bracket	1
✓	Heat sink	1
✓	Hot swap 40x56mm fan	3
✓	AIC® Delphinus motherboard	1
Accessory Item		Number
✓	EPE foam for front board: 575*420*105H	1
✓	EPE foam for rear board: 575*420*105H	1
✓	EPE foam for front tray: 575*300*145H	1
✓	EPE foam for rear tray: 575*300*145H	1
✓	EPE pad: 125*100*25T	2
✓	Power cord	vary per region
✓	20-inch fixed slide rail assembly	1

Product features are subject to change without notice.

1.2 Specifications

Dimensions (W x D x H)	mm : 432.8 x 524.7 x 43.8		
	inches : 17 x 20.6 x 1.72		
Motherboard	AIC Server Board Delphinu s		
Processor	Processor Support	• One Intel® Xeon® Processor E-2300 (Rocket Lake) Product Family • Supports CPU TDP up to 95W <i>*Please contact AIC Technical Support for more info/details about optimized CPUs and specialized system.</i>	
	Socket Type	Socket H5 (LGA 1200)	
Chipset Support	Intel® C256 PCH		
System Memory	2 channels DDR4 / 2 DPC UDIMM ECC Up to 3200 MT/s Total 4 memory slots; up to 128GB		
Front Panel	• System power on/off • System ID • System reset • NMI • USB 2.0 Type A • LCM module		
LEDs	• Power status • System management alert • Drive activity • Network activity • System ID		
Drive Bays	Internal	3.5"	1
		2.5"	2 (1x shared with 3.5")
		2x M.2(NGFF)/M-Key/22110	
Expansion Slots	PCIe 3.0	• 2 x PCIe Gen4 x8 slots • 1 x PCIe Gen3 x8 slot (with x4 link)	
Riser Card (included)	RC-PE1U35-TY	2 x PCIe x 8 slots	
System BIOS	BIOS Type	AMI UEFI BIOS	
	BIOS Features	• ACPI • PXE • WOL • AC loss recovery • IPMI KCS interface • SMBIOS • Serial console redirection • BIOS Boot Specification • BIOS Recovery Mode	

On-board Devices	SATA	• 6x SATA 6G ports (4x in miniSAS HD + 2x 7pin + 2x M.2)
	IPMI	Aspeed AST2500 Advanced PCIe Graphics & Remote Management Processor • Baseboard Management Controller • Intelligent Platform Interface 2.0 (IPMI 2.0) • iKVM, Media Redirection, IPMI over LAN, Serial over LAN
	Network Controller	• Intel® I350 AM4/AM2 co-design to support 2/4 x GbE (SKU option) • Realtek RTL8211EL for BMC dedicated management port
	Graphics	Aspeed AST2500 Advanced PCIe Graphics & Remote Management Processor • 2D Video Graphic Adapter with PCIe bus interface • 1920x1200@60Hz 32bpp
Rear I/O	LAN	3 x GbE RJ45
	USB	2 x USB 3.0 Type A
	Graphic	• 1 x DB-15 VGA port • 1 x Mini-Display port (enabled with specified CPU)
	Serial Port	1 x COM by 3.5mm audio jack
Power Supply	300W 1+1 redundant power supply 80+ Gold • AC INPUT : 100~240V,50-60Hz,5-3A • DC 36~72V input power module available (BTO)	
System Cooling	3 x 40x56mm hot swap fans	
System Management	• IPMI 2.0 • KVM over IP • Media redirection • KCS (Keyboard Controller Style), IOL (IPMI Over LAN) • SOL (Serial Over LAN) interface • Temp, voltage and fan speed monitoring • CPU temperature (PECI) • System temperature • Fan speed detection • Smart fan speed control • System ID / System fail indicator • SMASH support • Remote power on/off/reset	
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 : 22
		lbs : 48.5
Packaging Dimensions	(W x D x H)	mm : 590 x 850 x 343
		inches : 23.2 x 33.5 x 13.5
Mounting	Standard	20" fixed rail

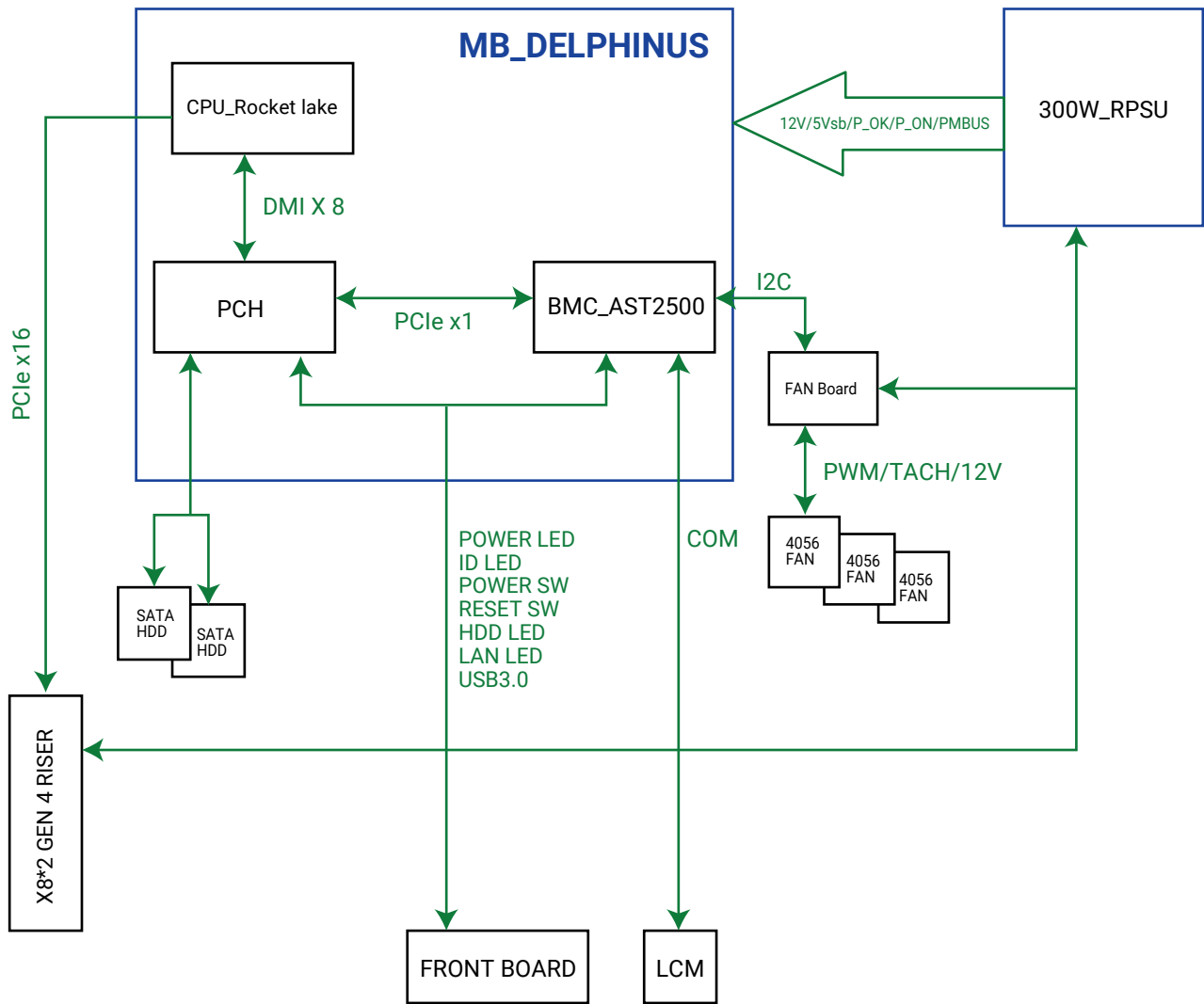
NOTE



HDD installation:

- Option① Insert 1 * 2.5-inch HDD and 1 * 3.5-inch HDD.
- Option② Insert 2 * 2.5-inch HDD.

1.3 System Block Diagram



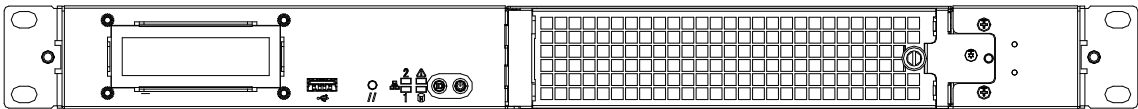
1.4 Feature

TB116-DL is a reliable 1U storage server barebone with 2 * 2.5-inch disk drives, and 3.5-inch disk drive. This product is designed to accommodate the AIC®-patented serverboard, Delphinus, which supports one Intel® Xeon® Scalable Processors (Rocket Lake) and 4 DDR4 DIMM to offer greater performance, efficiency and utility for our customers. Featuring Intel® C256 PCH, which is emphasized for its accelerated speed and expansion, this product enhances these advantages by integrating flexible I/O usage and system expansion into to provide greater bandwidth and utilization.

In addition to the noteworthy features of the barebone, TB116-DL provides immediate and efficient management with Onboard Baseboard Management Controller and greater I/O extension. Featuring IPMI 2.0 and Aspeed AST2500 Advanced PCIe Graphics, the server board offers support for iKVM, Media Redirection, Smash Support, IPMI over LAN and Serial over LAN.

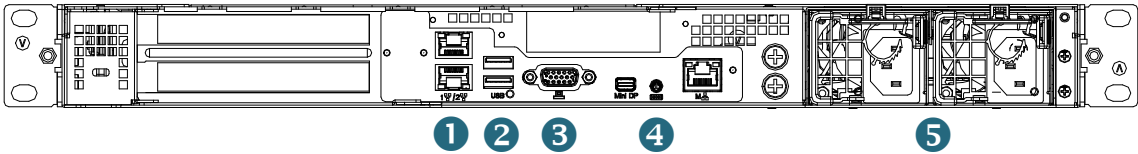
- 1U FIPS/NEBS compliant network appliance
- Supports one Intel® Xeon® Processor E-2300 (Rocket Lake) Product Family
- With Intel® C256 chipset to provide 5+ years product life cycle
- Flexible I/O design with MAX I/O® technology to support 2x PCIe 4.0 add-in cards in short depth 1U
- Onboard Baseboard Management Controller for system management and IPMI control
- Front-to-back airflow and hot swap redundant fans to provide optimal thermal conditions
- Supports intrusion switch

Front Panel



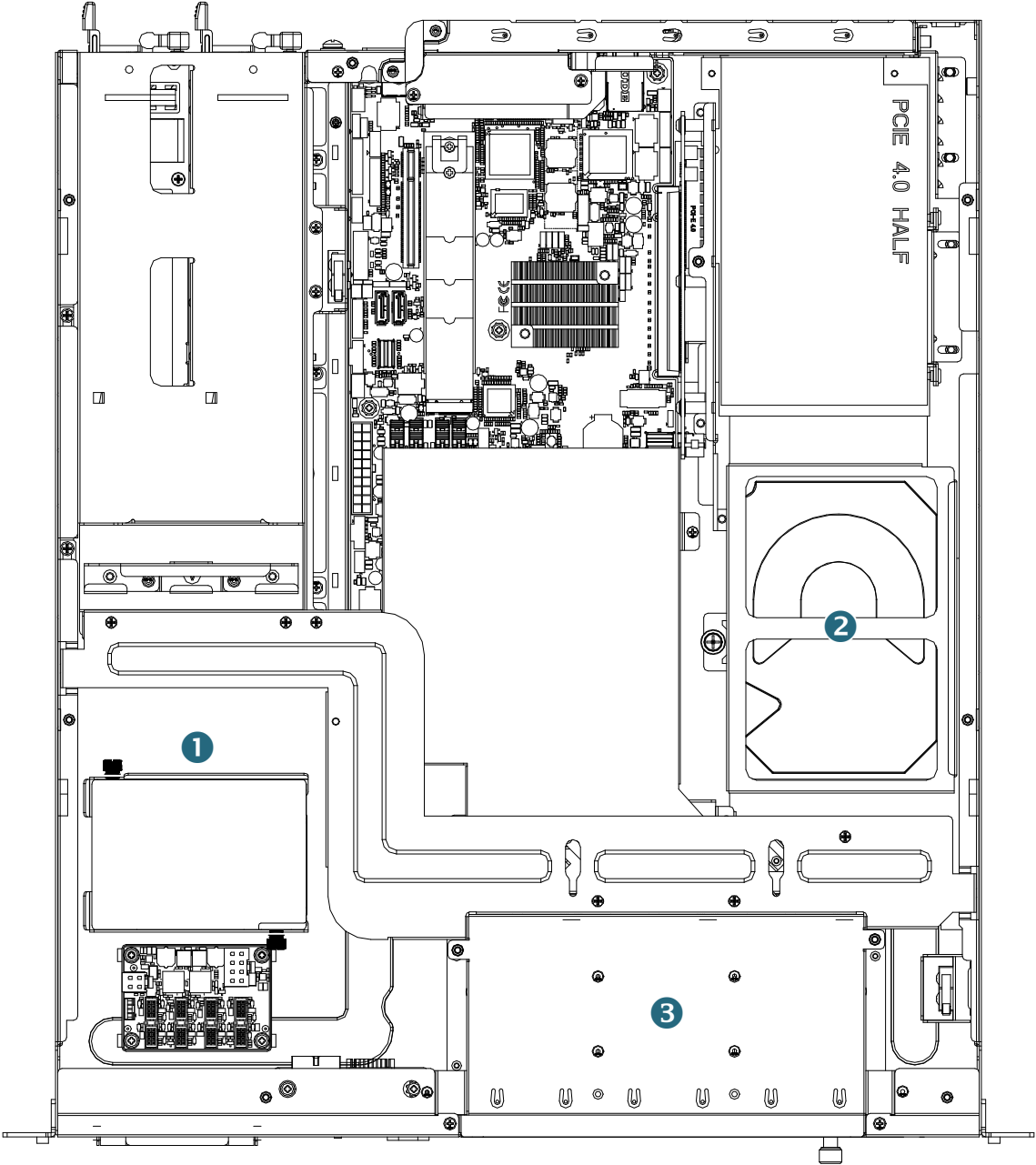
Item	Description		Item	Description	
	Power Button			Power Status LED	Green
	ID Button			ID LED	Blinking blue
	System Alert LED	Red		HDD LED	Green
	LAN1 LED	Green		LAN2 LED	Green
	System Reset			USB 3.0 type A	

Rear Panel



Item	Content	Description
1	LAN port	3 GbE RJ45 dedicated to BMC management
2	USB port	2 USB 3.0 Type A
3	VGA port	1 external DB-15 VGA port
4	Serial port	1 external 3.5mm phone jack for COM port
5	PSU socket	300W 1+1 redundant power supply 80+ Platinum • AC INPUT : 100~240V,50/60Hz,5-3A • DC 36~72V input power module available (BTO)

Top View



Item	Content	Description
1	Disk Drive	2.5-inch hot swap disk drive
2	Disk Drive	3.5-inch hot swap disk drive
3	Fan	3 x hot swap 40x56mm fan

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 H5 (LGA-1200).

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

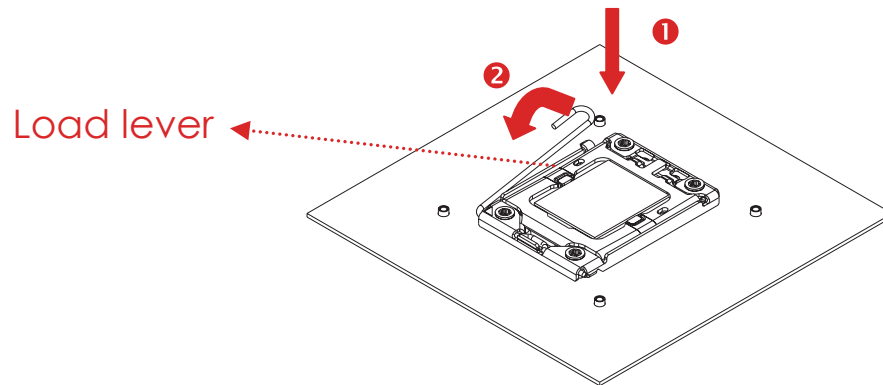
When unpacking a processor, hold the processor only by its edges to avoid touching the contacts.



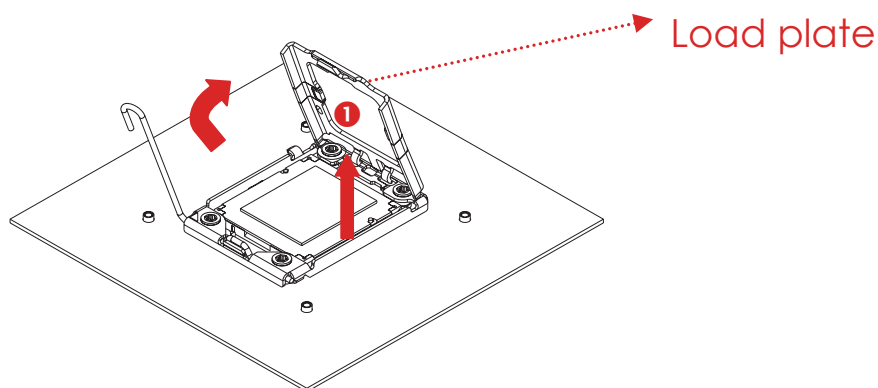
This information is provided for professional technicians only.

Procedure:

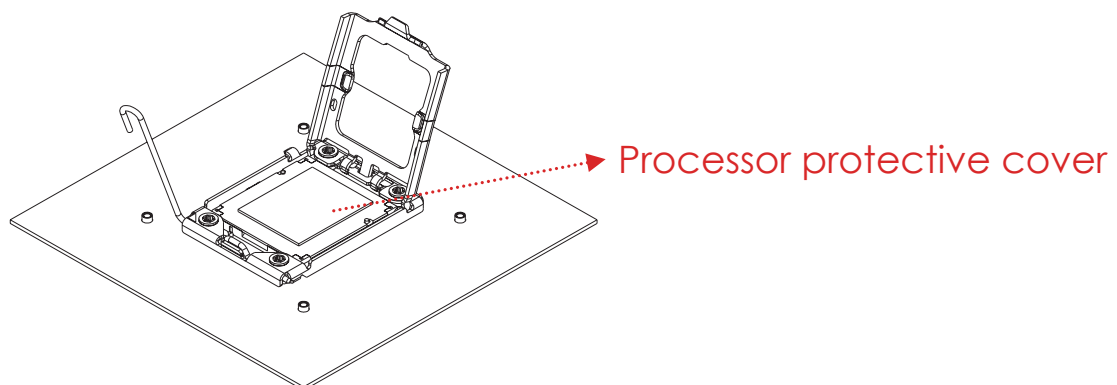
- ① Press the load lever to release the load plate.



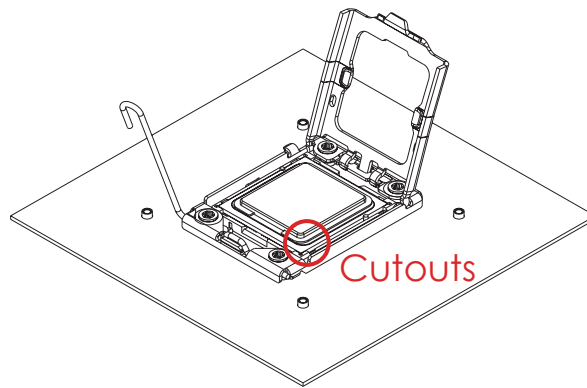
- ② Lift the load plate.



- ③ Remove the processor protective cover from CPU socket.

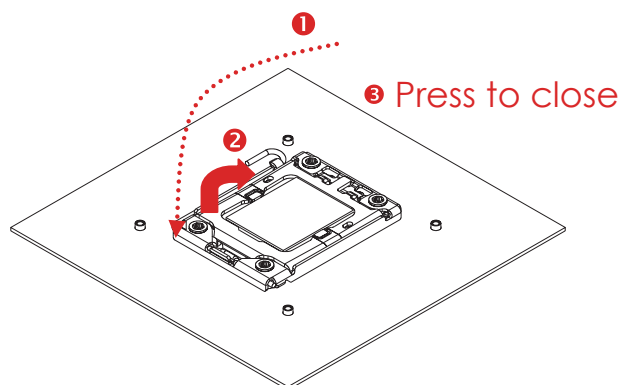


- ④ Align the processor cutouts against the socket notches.

**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.

- ⑤ Close the load plate & load lever.

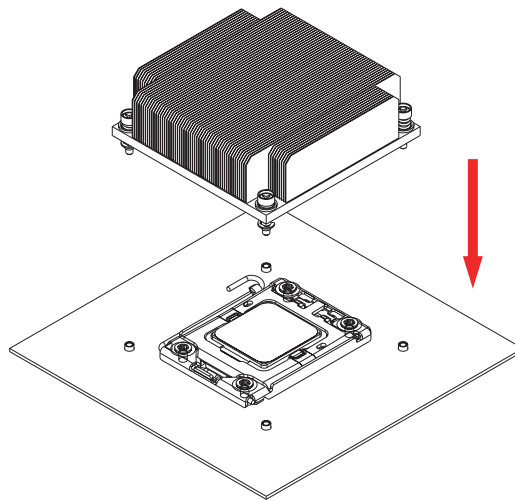


CAUTION

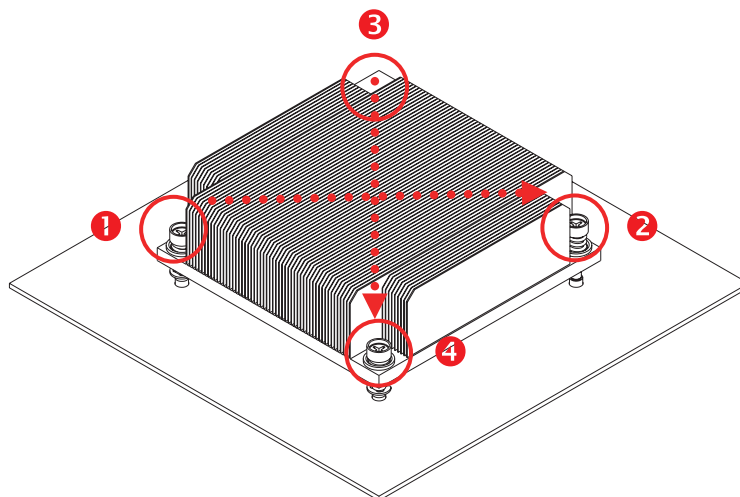
Apply thermal paste to the bottom of the heatsink and spread in an even thin layer before installing the heatsink.

To install the CPU heatsink

- ① Place the heatsink on top of the CPU, ensuring that the four fasteners match the holes on the motherboard.



- ② Tighten the four screws in a diagonal sequence, a couple of turns at a time, until all four screws are secure and the heatsink is securely fastened to the chassis.



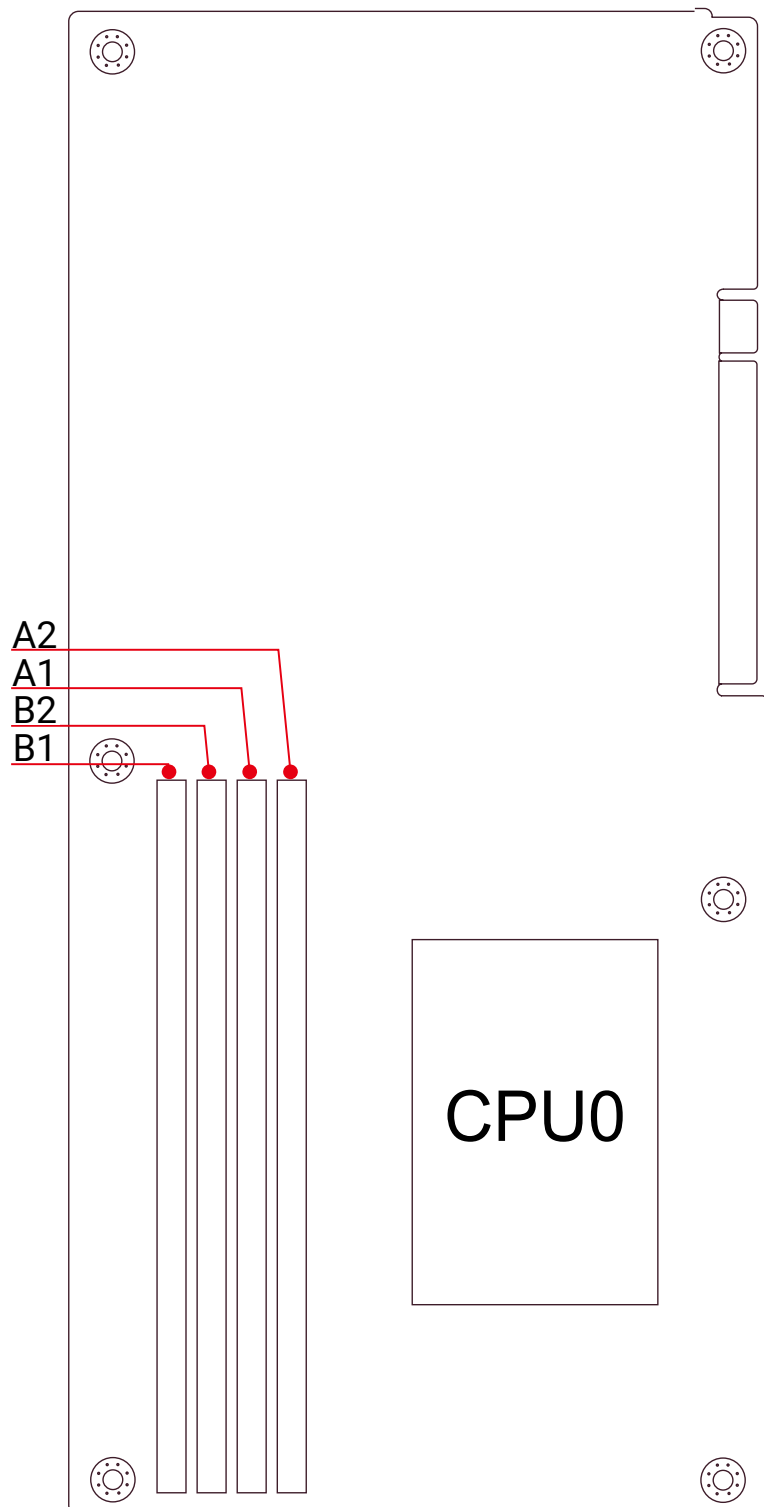
2.2 System Memory

2.2.1 Placement

The DIMMs are displayed on the Delphinus board as B1/B2/A1/A2.

To ensure satisfactory performance, you need to:

- ☑ Verify the DIMM type:
This product only supports DDR4 UDIMM.
- ☑ Verify if all of the DIMMs installed are of the same DIMM type to avoid memory failure and loss of performance speed.



2.2.2 DIMM Population



NOTE

Rules to abide by before installation:

- Must install at least one DDR4 DIMM per socket.
- If only one DIMM is populated in a channel, you must install it in the slot furthest away from the CPU.
- Must populate DIMM1 before DIMM2.



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

1 CPU Configuration

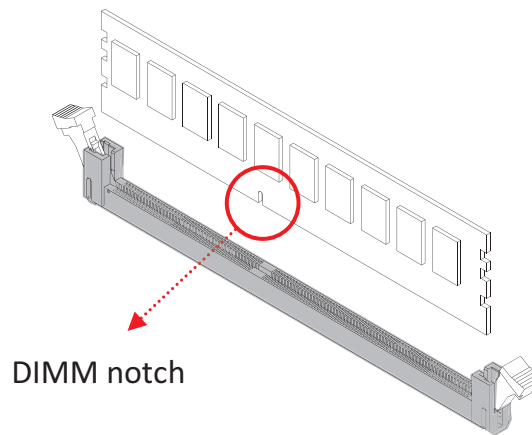
Placement		DIMM Number				
		1	1	2	3	4
CPU0	B1		#	#	#	#
	B2					#
	A1	#		#	#	#
	A2				#	#

2.2.3 Installation

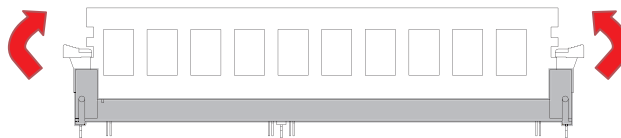
Step 1 Unlock the DIMM socket by pressing the retaining clips outward.



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

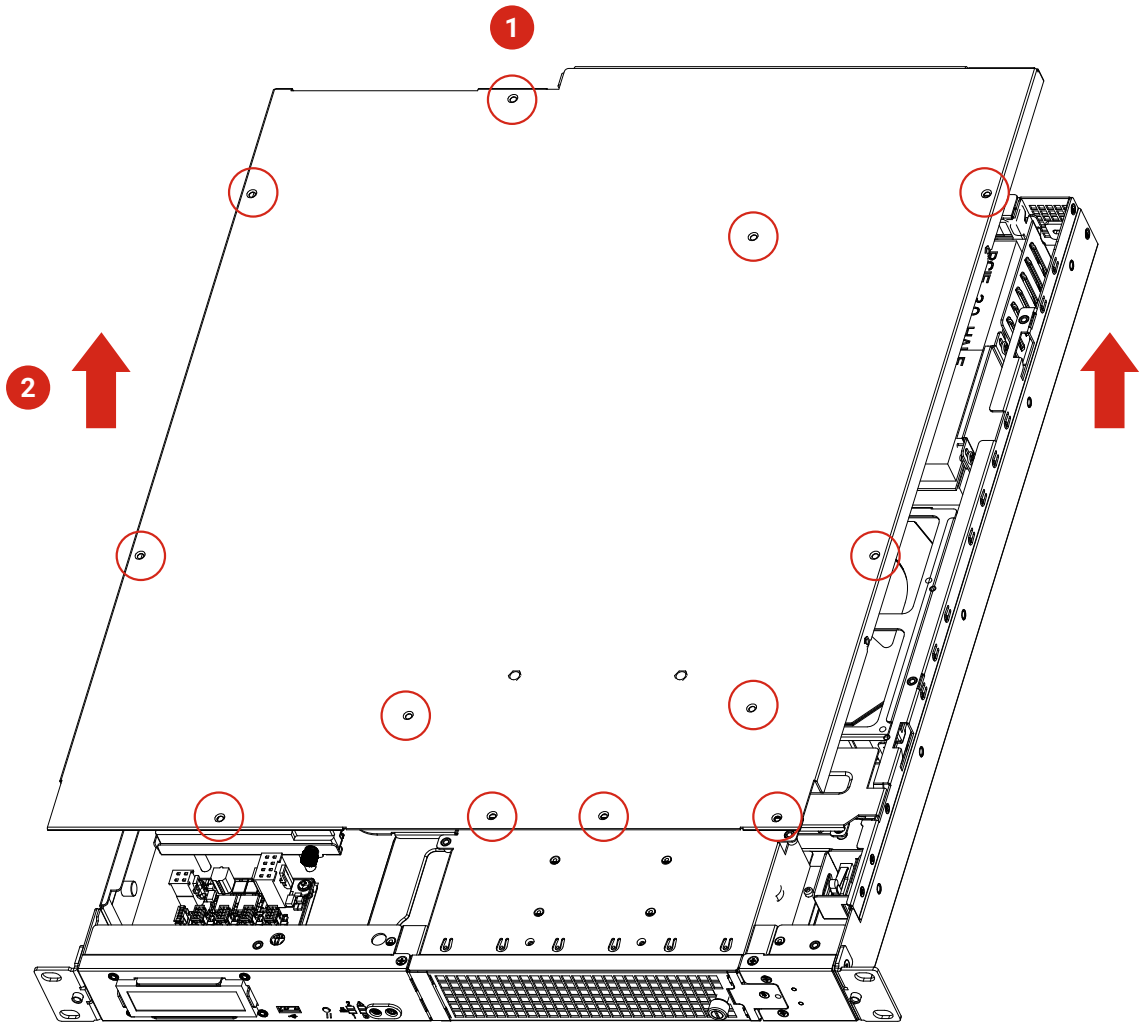


Step 3 Close the retaining clips to complete installation.



2.3 Top Cover

- ① Dislodge the screws on the top cover.
- ② Lift upward to remove.

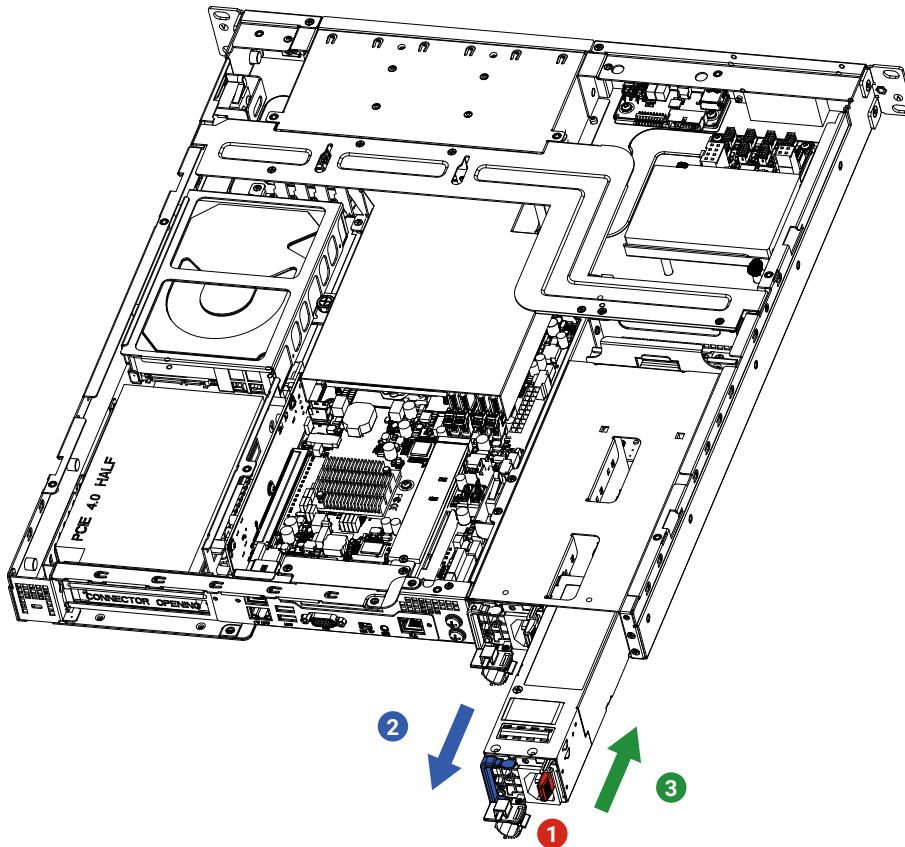


This information is provided for professional technicians only.

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

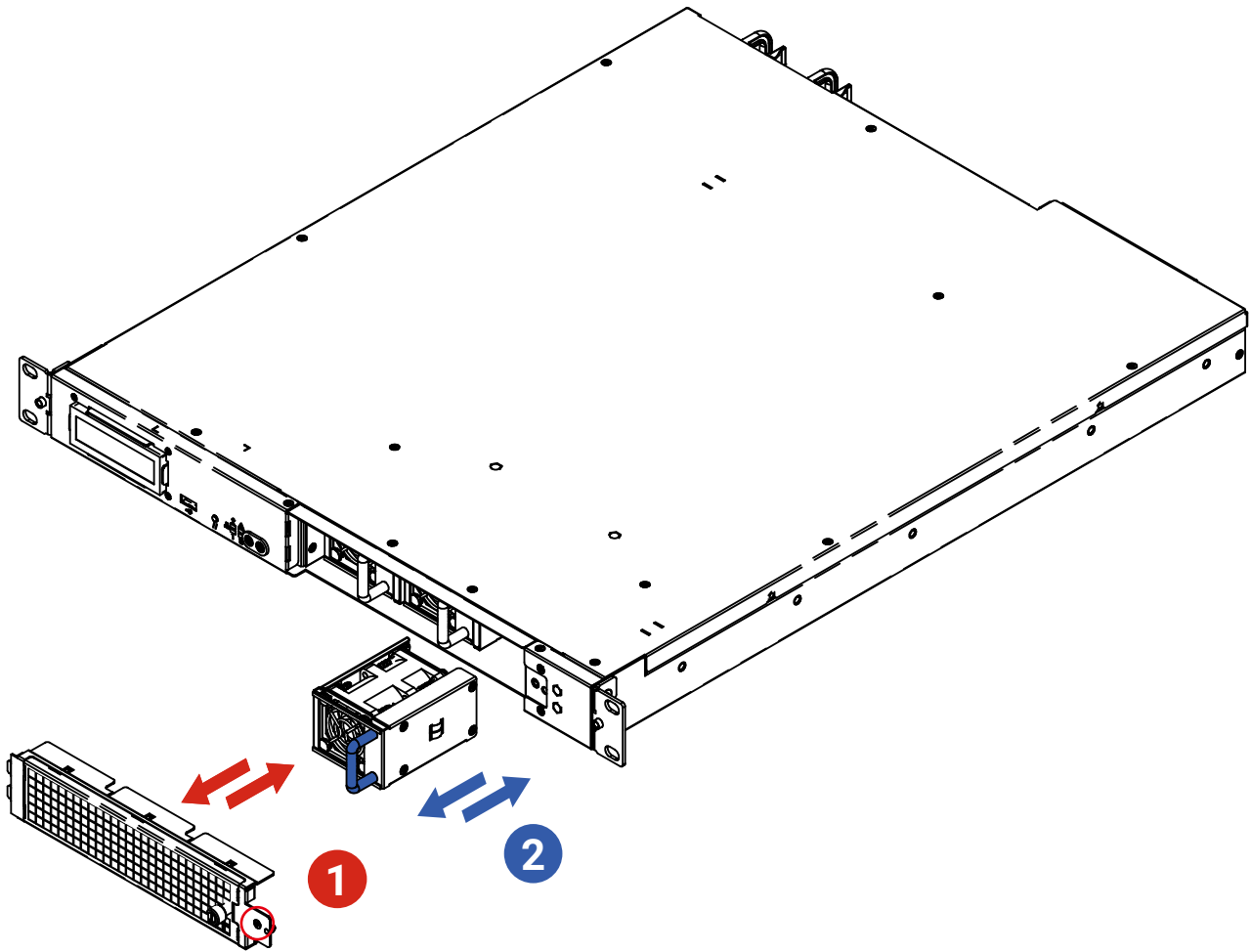
Color	Behavior	Description
Green	Off	No AC power to all power supplies.
	Solid	Output on and working normally.
	Blinking, 1Hz	AC present/ only AUX (PS off) or PSU is in cold redundant state.
Amber	Solid	AC cord unplugged or AC power lost with a second power supply in parallel still with AC input power.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



This information is provided for professional technicians only.

2.5 Fan

- ① Dislodge the screw and remove the bracket from the rear panel.
- ② Pull the handle to remove the fan module out of the chassis.

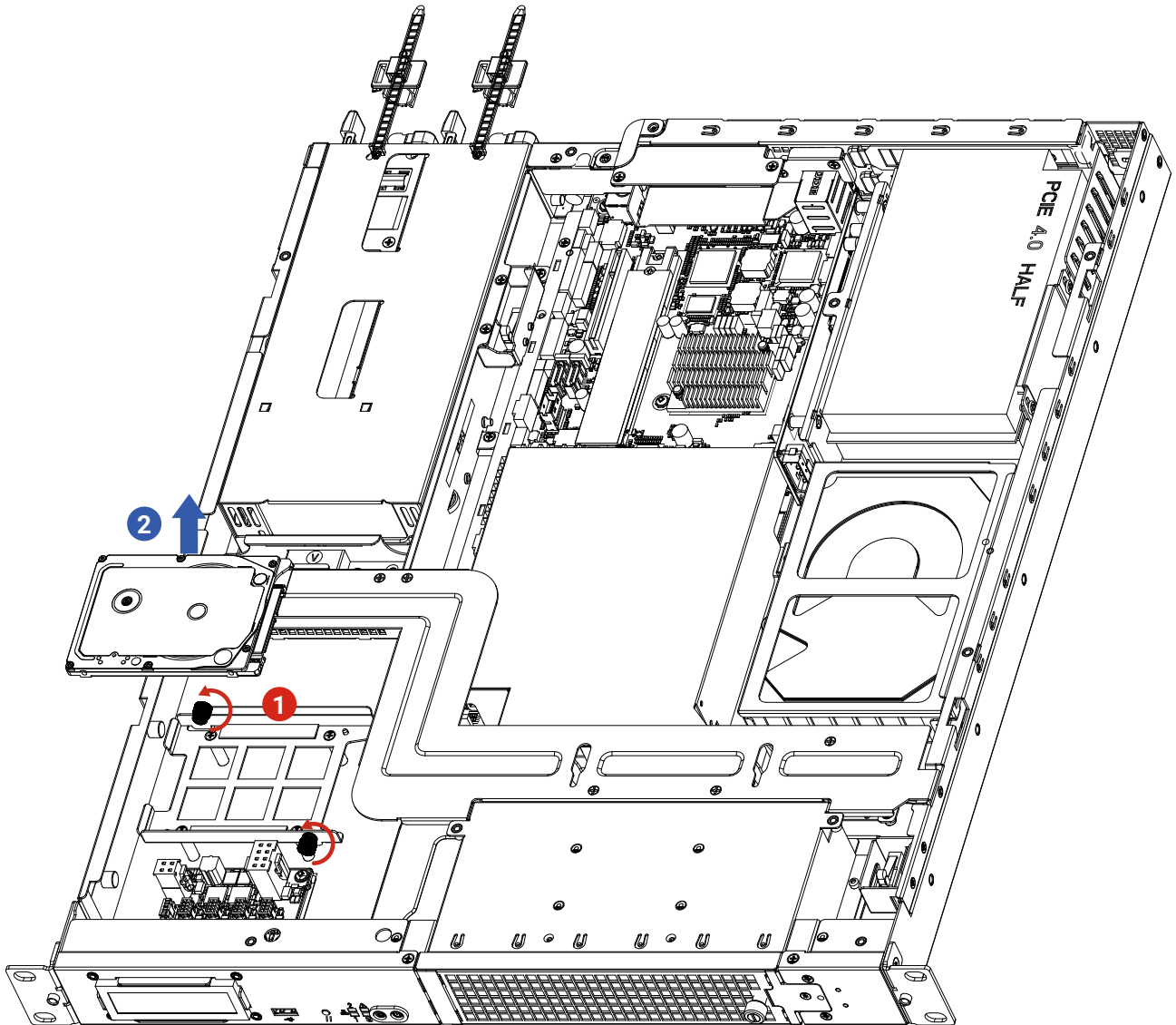


This information is provided for professional technicians only.

2.6 Disk Drive

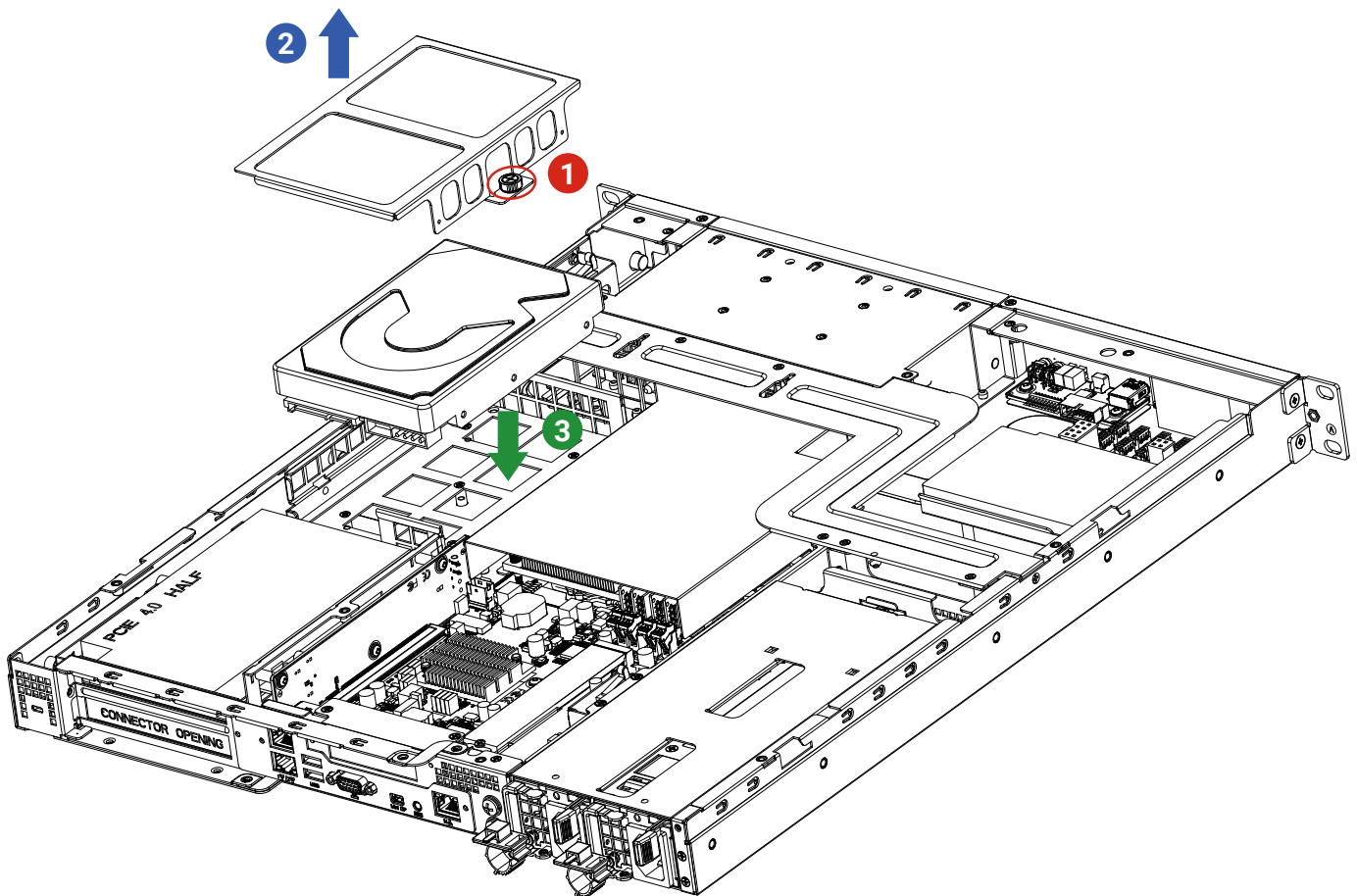
2.6.1 HDD: 2.5-inch Installation

- ① Loosen the captive screws on the cage to release the disk drive.
- ② Lift the disk drive upward.
- ③ Insert the new disk drive into the bracket holder and secure the captive screws.



2.6.1 HDD: 3.5-inch Installation

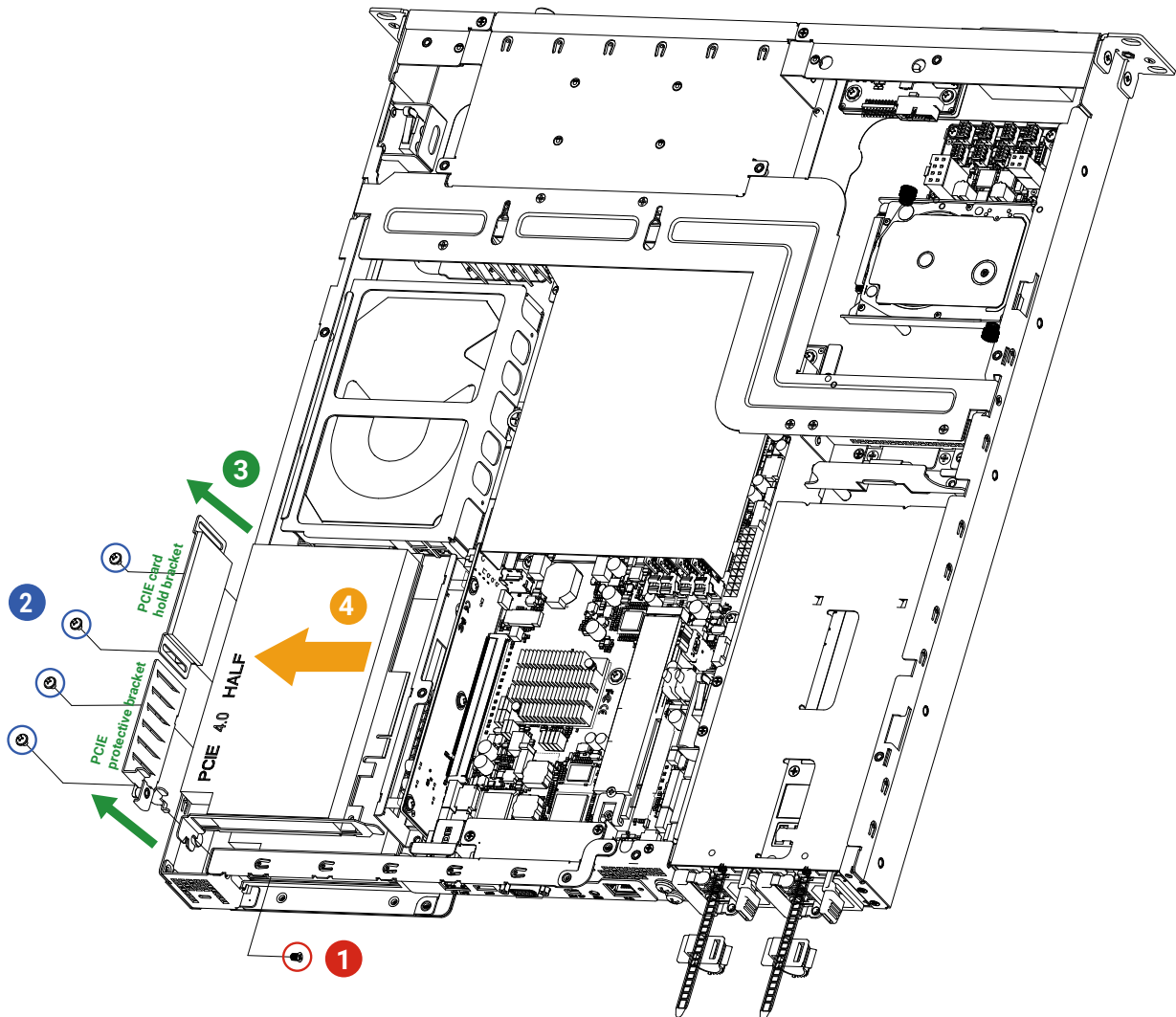
- ① Loosen the captive screw on the cage to remove the securing bracket.
- ② Lift the securing bracket upward.
- ③ Insert the 3.5-inch or 2.5-inch disk drive into the bracket holder.
- ④ Replace the securing bracket and secure the captive screw.



This information is provided for professional technicians only.

2.8 PCIe Card

- ① Dislodge the screw on the cage.
- ② Dislodge the screws*4 on the PCIe card bracket holder and protective bracket.
- ③ Remove the PCIe card bracket holder and protective bracket.
- ④ Push the PCIe card bracket outward to remove.
- ⑤ Replace the PCIe card.
- ⑥ Secure the brackets.



This information is provided for professional technicians only.

2.9 Slide Rail

NOTE



This sections 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.

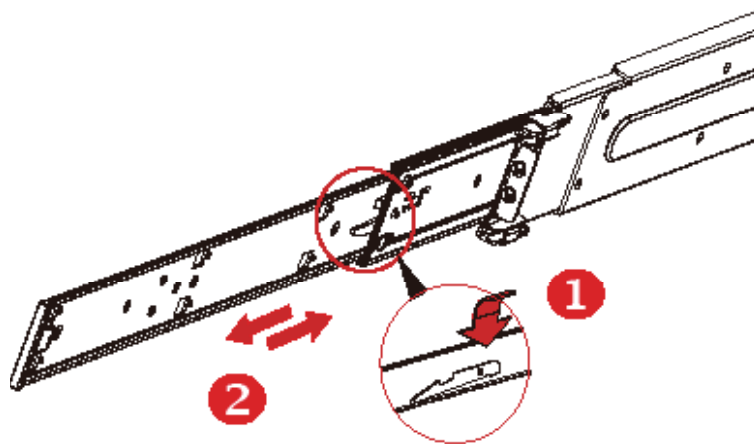
CAUTION



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.

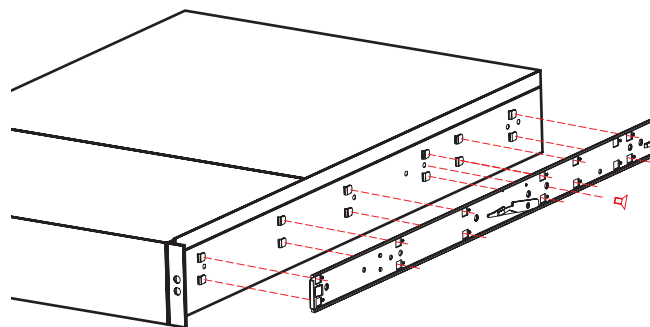
Pulling out the inner slide rail

- ① Press the trigger downward to release the inner side rail.
- ② Pull the inner rail out of the blade slide.



Installing the inner slide rail to the chassis

Align the rectangular holes on the inner side of the chassis with the bayonets on the side of chassis. Secure the inner chassis with the screws from the standard screw kit after the bayonets go through the holes and are accurately positioned.

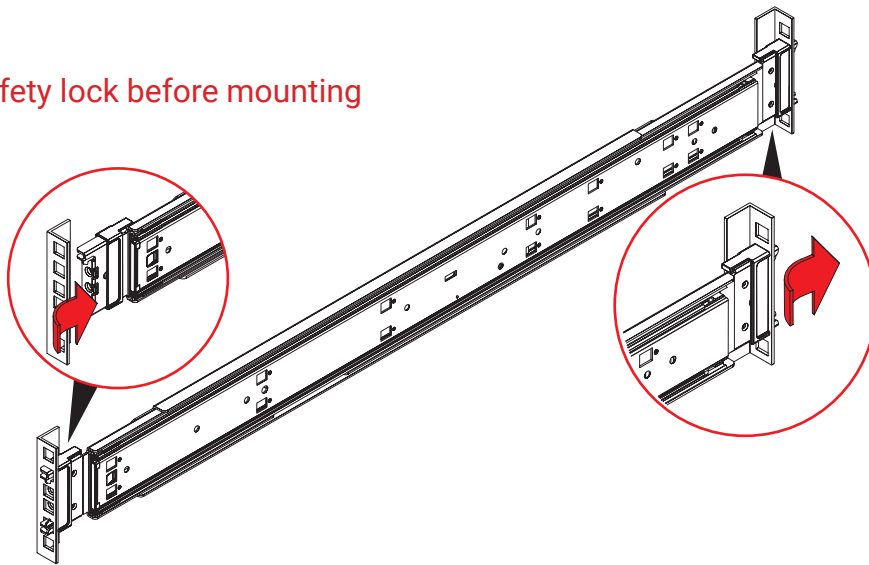


Bayonet on chassis shall be pre-formed as per the recommended dimension and location.

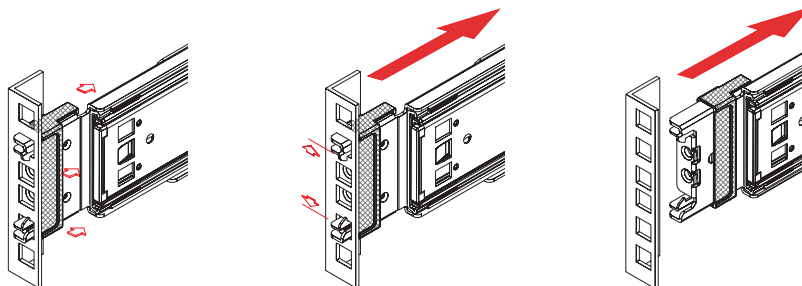
Installing the outer cabinet to the slide rail

Insert the stag into the upper and lower square holes on rail from the back of rail. Push the safety lock forward to secure the bracket. Be certain to check if the safety lock is in disengaged position before mounting the brackets.

Release safety lock before mounting



Push the safety lock forward to secure



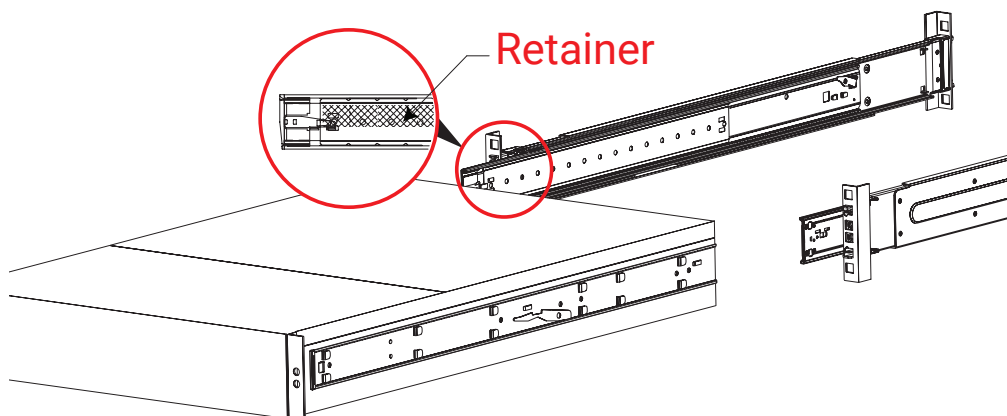
Installing the chassis into the cabinet

Insert the inner side of chassis into the cabinet. Check if the ball retainer is fully opened before installation. It may cause catastrophic damage to the chassis if ball retainer is not in fully open position while mounting the chassis. While pushing the chassis back into the cabinet, release the slide from locking position by pressing the trigger downward.



CAUTION

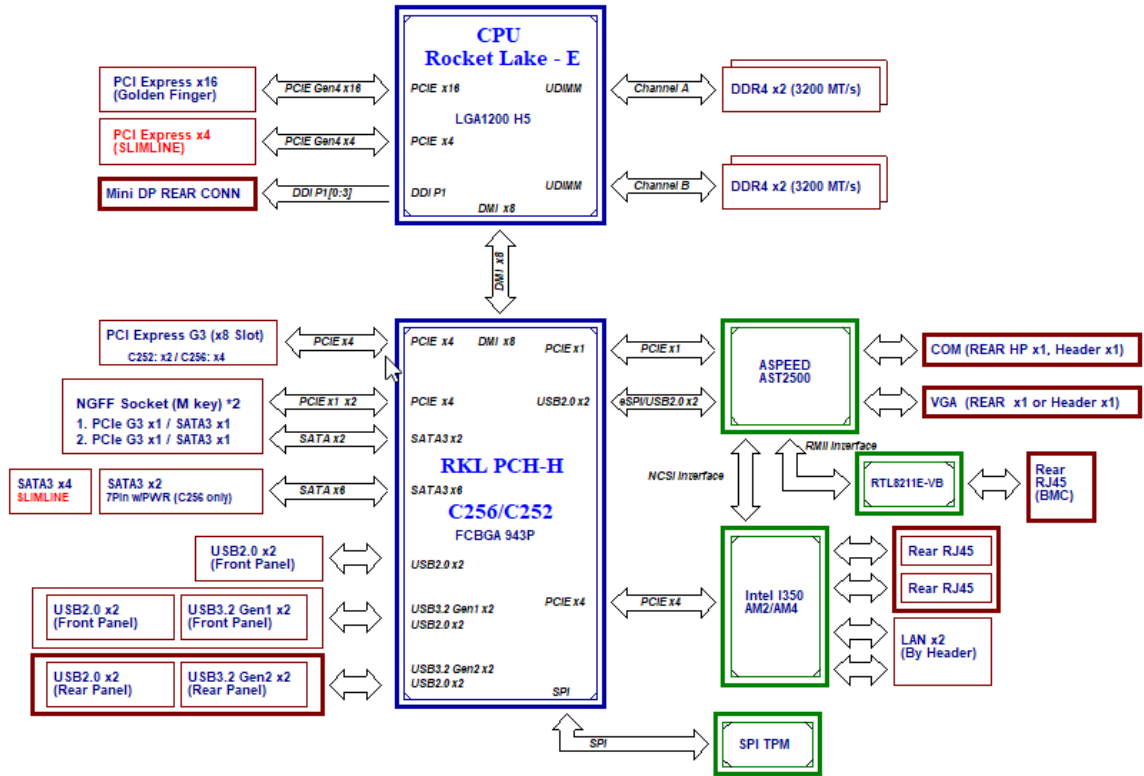
It requires at least two people to install the chassis for safety purpose.



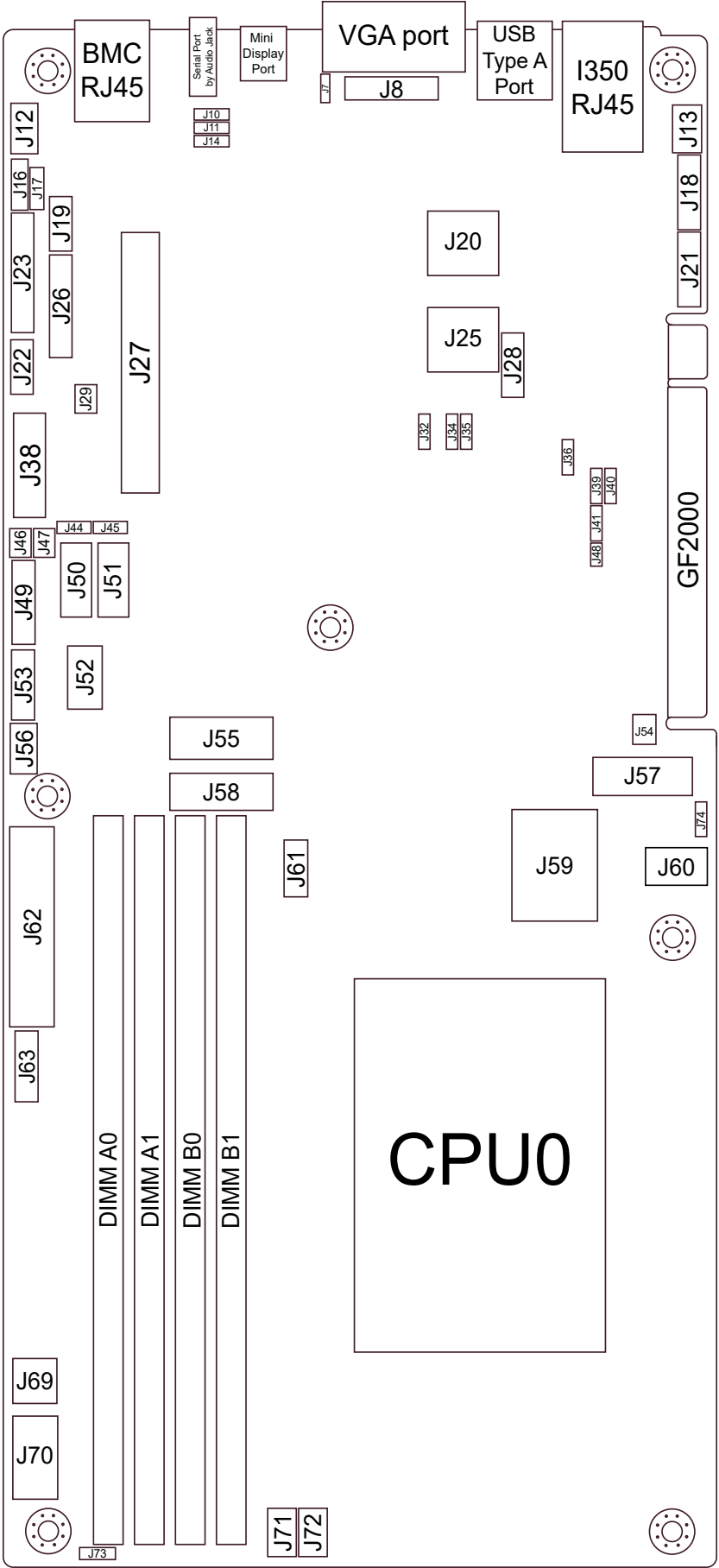
Chapter 3. Hardware Settings

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

3.1 Motherboard Block Diagram



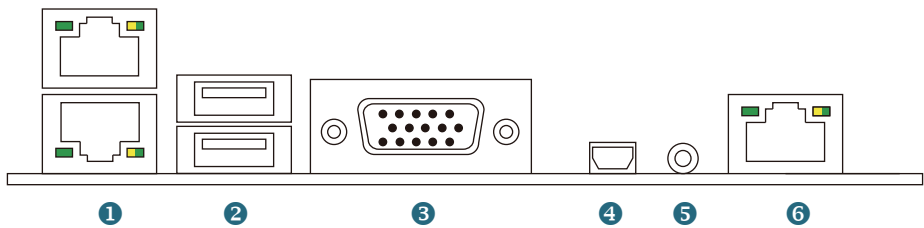
3.1.2 Placement



3.1.3 Content List

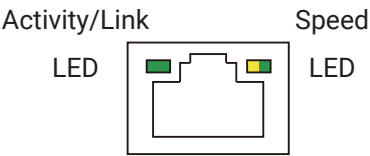
Port/Slot		Port/Slot	
RJ45 port dedicated to BMC		VGA port	
Serial Port by Audio Jack		USB 3.0 Type A port	
Mini Display Port		I350 RJ45 port	
Connector	Placement	Connector	Placement
BMC I ² C Header	J7	SATA DOM Power	J46 J47
Interanl VGA Header	J8	LPC/ESPI Debug Header	J49
Rack LAN Header	J12	SATA Connector	J50 J51
Fan Connector	J13 J71 J72	SATA Slimline connector	J52
BMC Debug Header	J14	LCD Header	J53
Intel I350 AM4 Connector	J18 J21	Battery Box Header	J54
COM Port Header	J19	NGFF Connector	J55 J58
BMC SPI Socket	J20	FPGA Download Connector	J56
Front I/O USB2.0 Header	J22	XDP header	J57
SSI Front Panel Header	J23	Battery Holder	J59
Host SPI Socket	J25	PCIe x4 NVME Slim Connector	J60
AIC Open Rack LAN Header	J26	AIC QST Debug Connector	J61
External TPM Header	J28	Power Supply Connector input	J62
Chassis Intrusion Header	J29	PSMI Header	J63
Front I/O USB3.0 Header	J38	Power Supply +12V input Connector	J69 J70
SATA DOM Set up	J44 J45	CPU VR SMBUS Debug Header	J73
Jumper	Placement	Jumper	Placement
Audio COM Port Source Select	J10, J11	Password Clear	J40
CONFIG / Recover Jumper	J32	PECI Master Select	J41
ME Firmware Update	J34	BMC SOCFlash function	J48
CMOS Clear	J35	CPU PEG60 Port	J74
BIOS Flash Security Override	J36		

3.1.4 External Port



Item		Item	
1	2 * I350 RJ45 port	4	Mini display port
2	2 * USB 3.0 Type A Port	5	Serial port by audio jack
3	VGA port	6	RJ-45 port dedicated to BMC

LAN LED Indicator



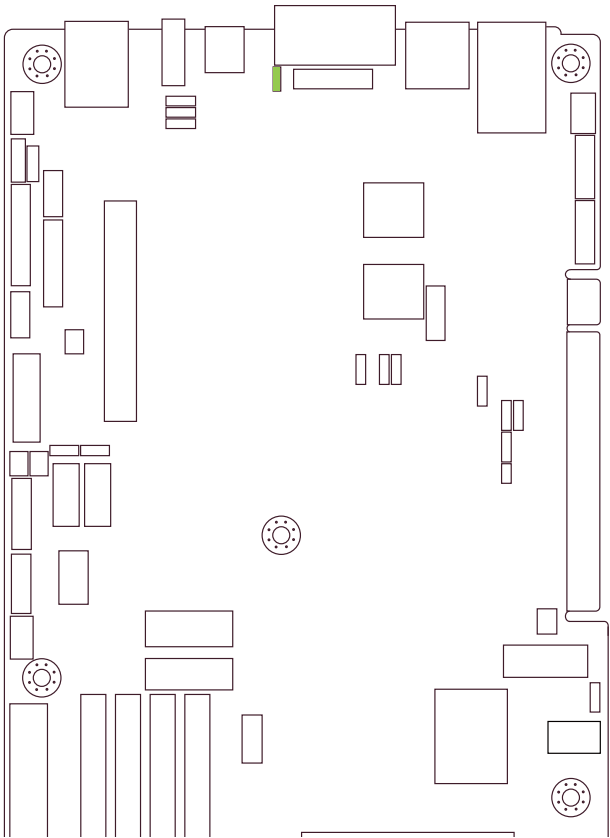
Item	Color	Behavior
Activity/Link LED	Off	No link.
	Green (blinking)	Data activity.
	On	Link.
Speed LED	Off	10M bps connection or no link.
	Green	100M bps connection.
	Yellow	1G bps connection.

3.1.5 Connector Definition

BMC I²C Header (J7)

3-pin Inter-Integrated Circuit that supports BMC.

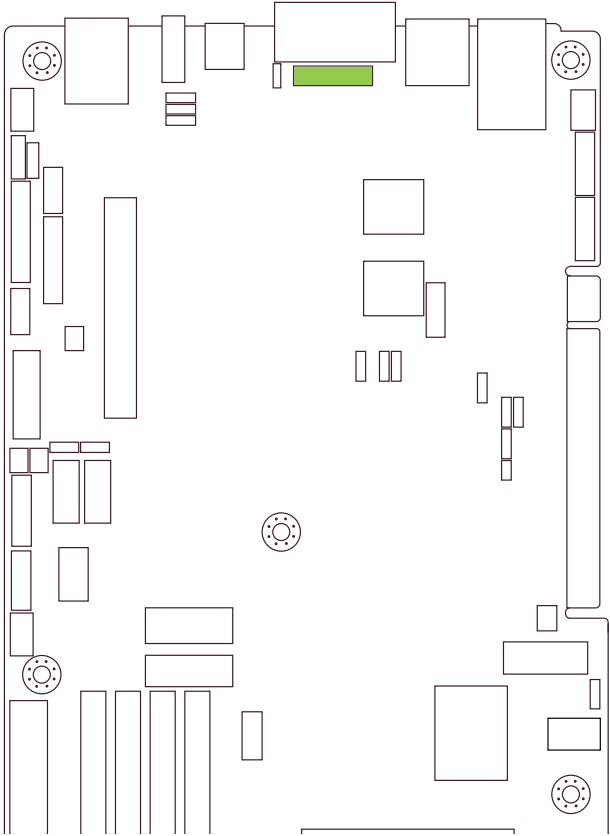
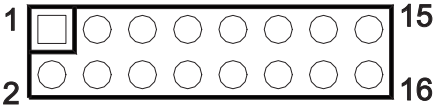
1	GND
2	I2C9SDA
3	I2C9SCL



Internal VGA Header (J8)

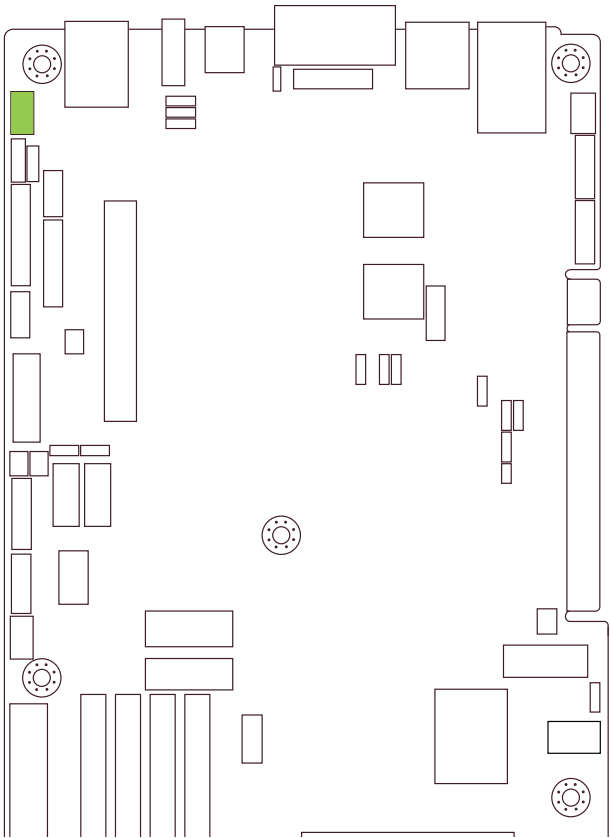
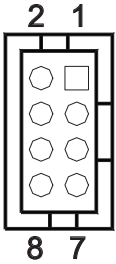
8x2-pin header that supports internal VGA.

DACROA	2	1	GND
N.C.	4	3	DACGOA
GND	6	5	DDC_DATA0
DACBOA	8	7	GND
AHSYNCO	10	9	N.C.
DVO_5V	12	11	AVSYNCO
GND	14	13	GND
DDC_CLKO	16	15	GND



Rack LAN Header (J12)
2x4-pin header that supports AIC Rack LAN.

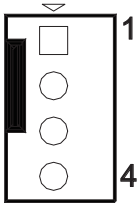
TF_MDI0_DP	2	1	TF_MDI3_DP
TF_MDI0_DN	4	3	TF_MDI3_DN
TF_MDI1_DP	6	5	TF_MDI2_DP
TF_MDI1_DN	8	7	TF_MDI2_DN



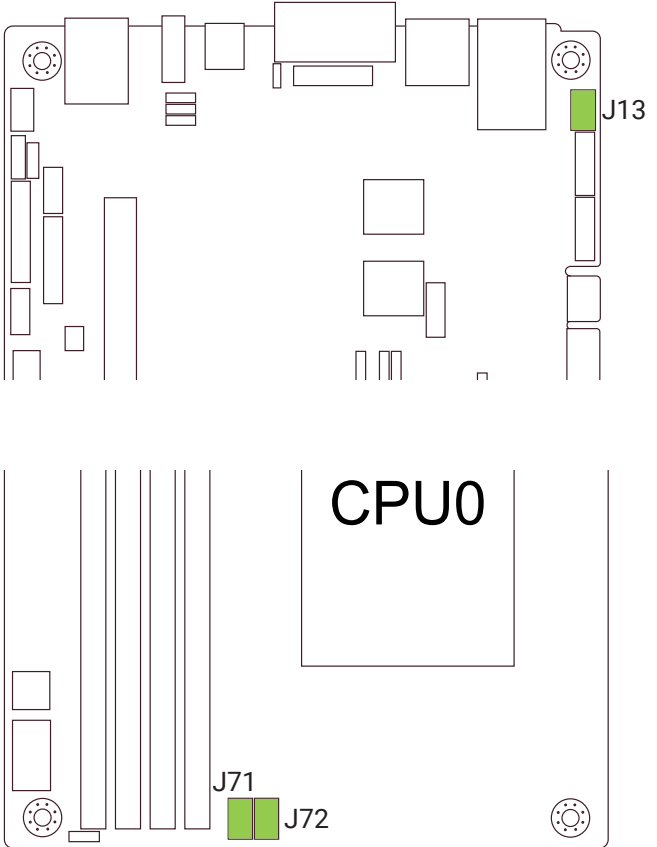
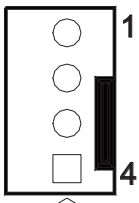
Fan Connector (J13, J71, J72)
4-pin connector that supplies power to fan.

1	GND
2	P12V
3	FAN_TACH_BMC_TACH0
4	FAN_BMC_PWM0

J13

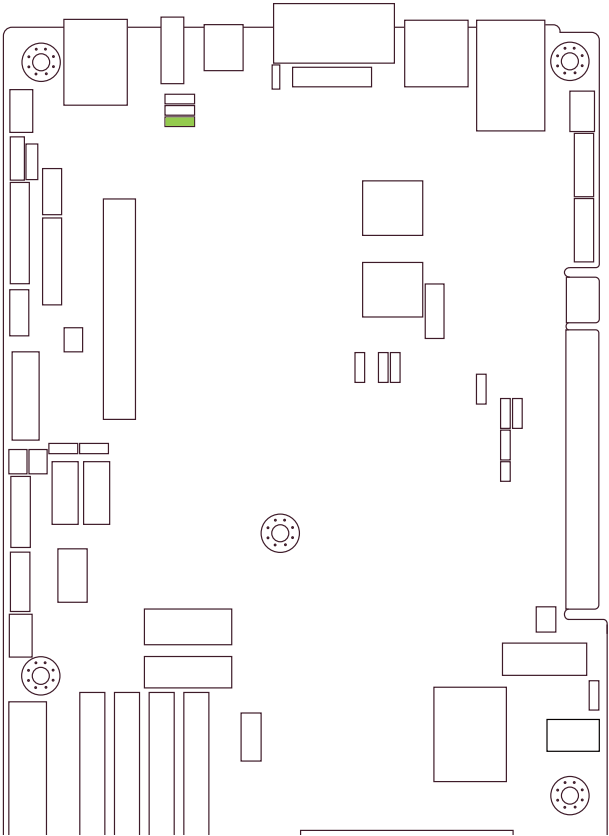
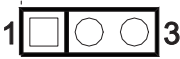


J71& J72



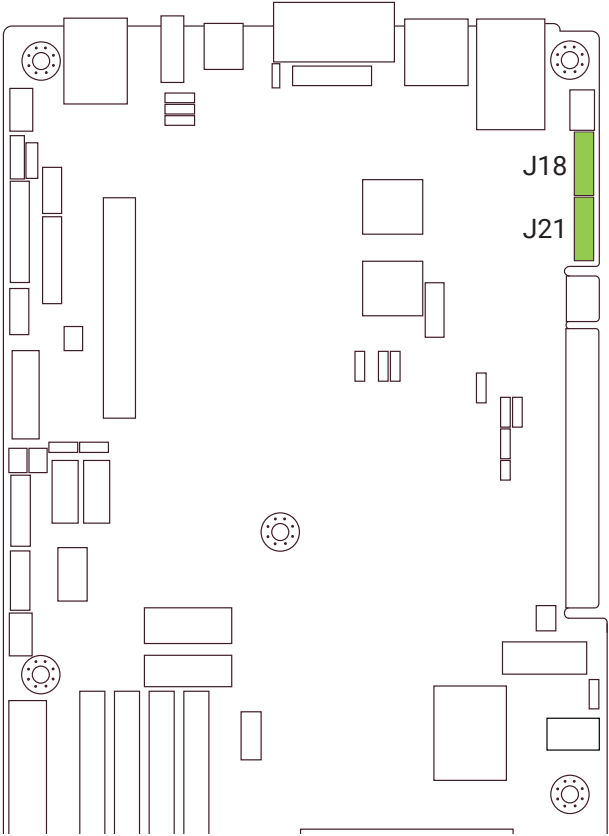
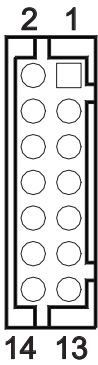
BMC Debug Header (J14)
3-pin header that supports BMC debug.

1	COM_OUT_TXD5
2	COM_OUT_RXD5
3	GND



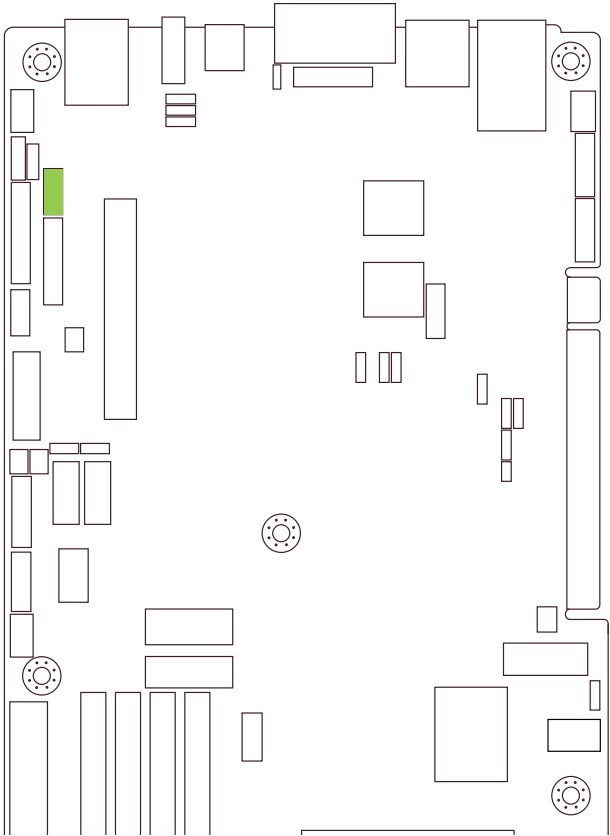
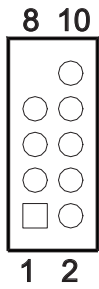
Intel I350 AM4 Connector (J18, J21)
2x7-pin connector that supports I350 LAN.

MX_LAN2_N0	2	1	MX_LAN2_P0
MX_LAN2_P1	4	3	GND
MX_LAN2_N1	6	5	LED_LAN2_1G_N
MX_LAN2_P2	8	7	LED_LAN2_100M_N
MX_LAN2_N2	10	9	GND
MX_LAN2_P3	12	11	LED_LAN2_ACT_N
MX_LAN2_N3	14	13	LED_LAN2_LINK_N



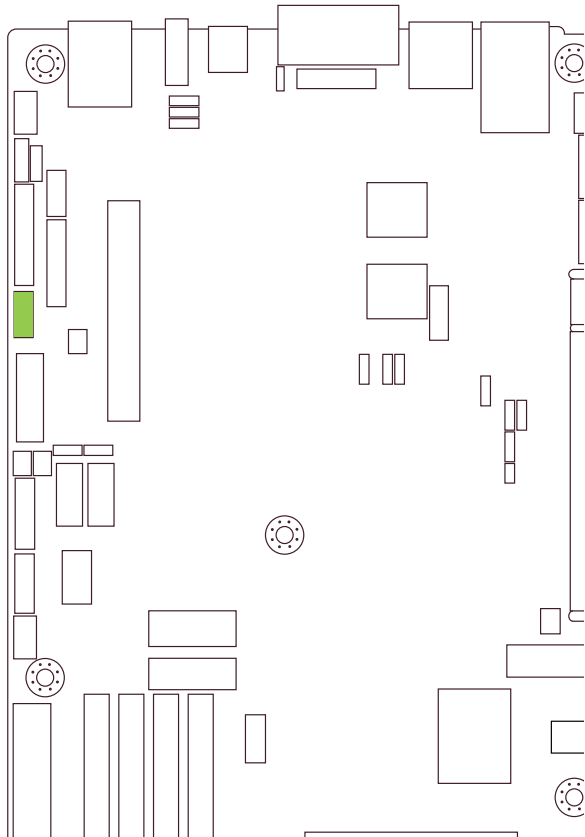
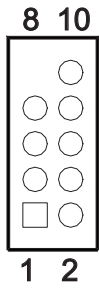
COM Port Header (J19)
2x5-pin header that supports COM port.

DCDx	2	1	DSRx
RxDx	4	3	RTSx
TxDx	6	5	CTSx
DTRx	8	7	RIx
GND	10	9	KEY (no pin)



Front I/O USB2.0 Header (J22)
2x5-pin header that supports USB2.0 in the front panel.

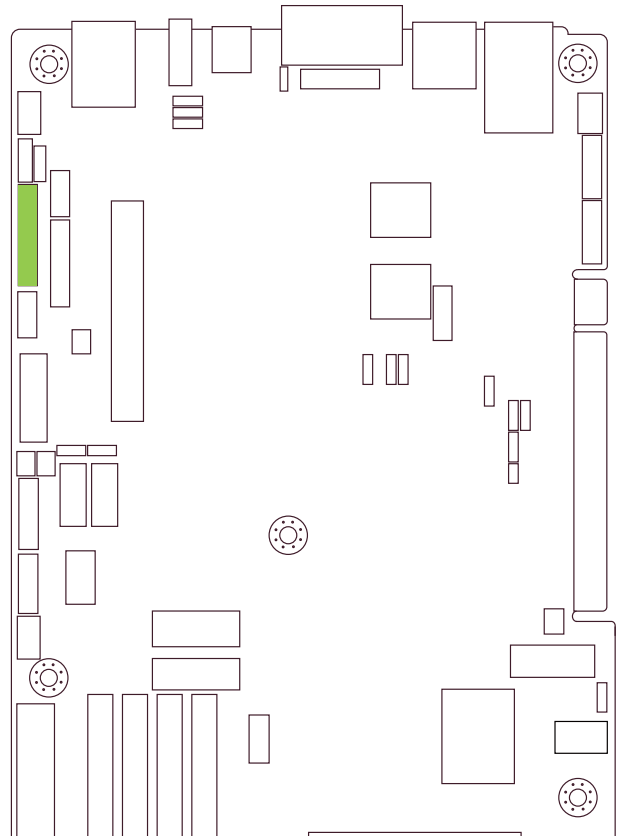
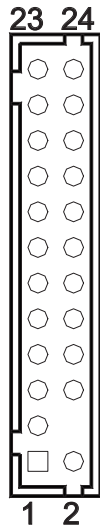
GND	9	10	KEY (no pin)
GND	7	8	GND
USB2_PCH_P9_ESD_DP	5	6	USB2_PCH_P8_ESD_DP
USB2_PCH_P9_ESD_DN	3	4	USB2_PCH_P8_ESD_DN
P5V_AUX_USB_HR	1	2	P5V_AUX_USB_HR



SSI Front Panel Header (J23)

2x12-pin header that supports SSI front panel.

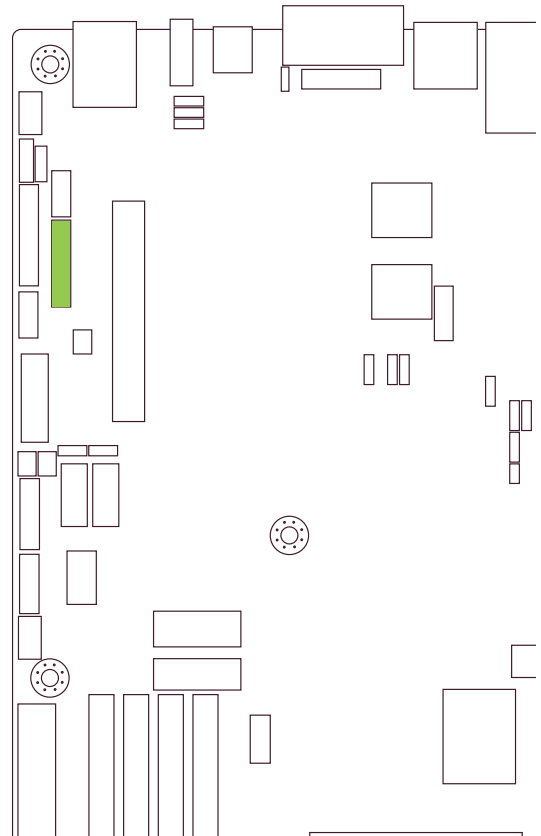
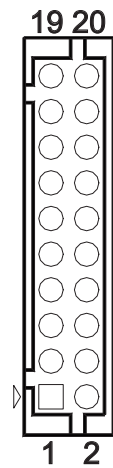
LED_PWRLED_ON	23	24	UIDBTN_FP_N
LED_LAN1_LINK_FP	21	22	NC
INTRUDER_FP	19	20	NMIBTN_FP_N
I2C8SCL_FP	17	18	GND
I2C8SDA_FP	15	16	RSTBTN_FP_N
LED_LAN0_ACT_FP_N	13	14	GND
LED_LAN0_LINK_FP	11	12	PWRBTN_FP_N
LED_FAULT2_N	9	10	LED_HDD_ACT_N
LED_FAULT_N	7	8	LED_HDD_ACT_ON
LED_UID_ON_N	5	6	LED_SYS_PWRLED_N
P5V_AUX	3	4	NC
P3V3_AUX	1	2	LED_PWRLED_ON



AIC Open Rack Header (J26)

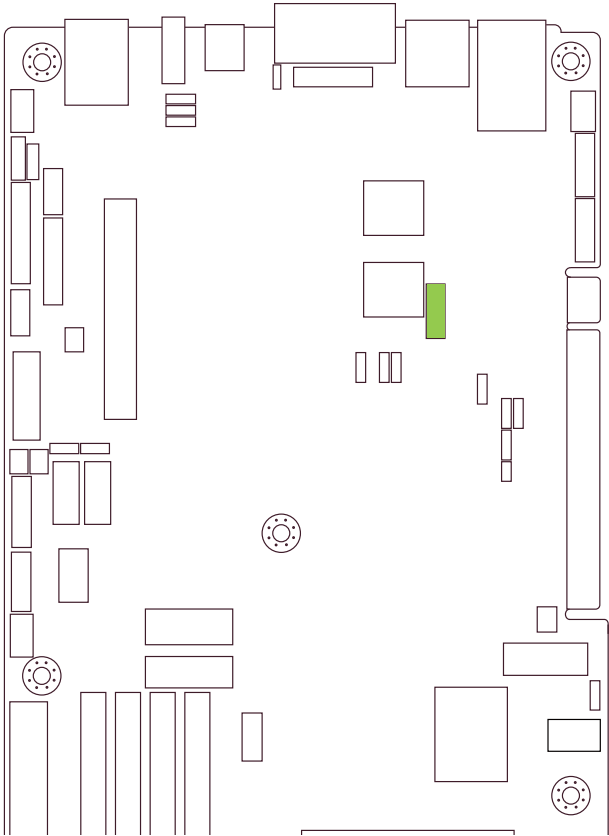
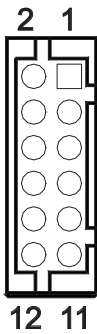
2x10-pin header that opens AIC Rack.

	GND	19	20	FM_CHASSIS_TYPE_N
	INTRUDER_FP	17	18	BMC_GPIO_EXIN
	IRQ_SML1_PMBUS_ALERT_N	15	16	FAN_TACH_BMC_TACH4
	I2C6SDA	13	14	FAN_BMC_PWM4
	I2C6SCL	11	12	GND
	GND	9	10	FAN_TACH_BMC_TACH3
	I2C1SDA	7	8	FAN_BMC_PWM3
	I2C1SCL	5	6	GND
	GND	3	4	I2C8SDA
	EXTRST_BMC_N	1	2	I2C8SCL



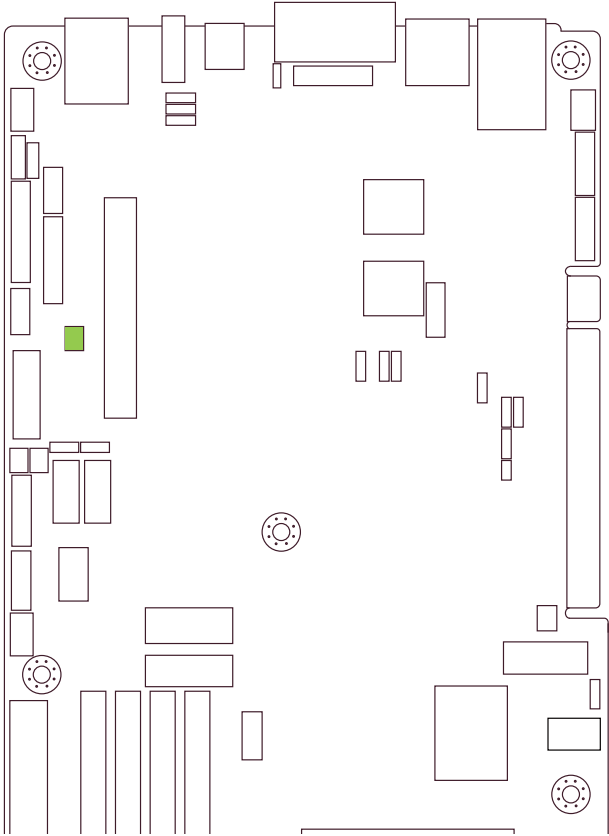
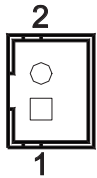
BMC Debug Port Header (J28)
2x6-pin header that supports BMC debug port.

FM_TPM_PRES_N	2	1	SPI_PCH_TPM_CONN_CS_N
GND	4	3	SPI_PCH_TPM_CLK
GND	6	5	SPI_PCH_TPM_MOSI
N.C	8	7	SPI_PCH_TPM_MISO
GND	10	9	IRQ_TPM_PIRQ_N
P3V3_AUX	12	11	RST_PLTRST_TPM_N



Chassis Intrusion Header (J29)
2-pin header that supports chassis security.

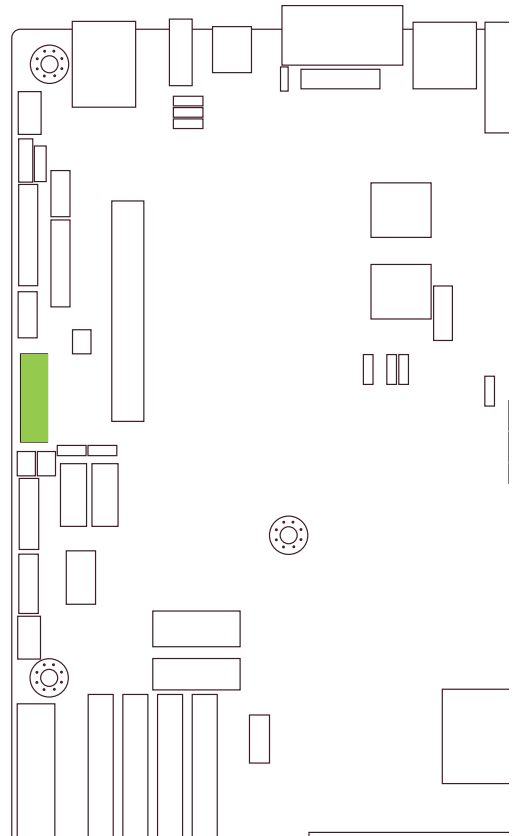
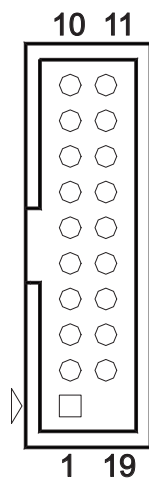
J29	Setting	
Short	Case open	
Open	Enable	Default



Front I/O USB3.0 Header (J38)

2x10-pin header that supports in the front panel.

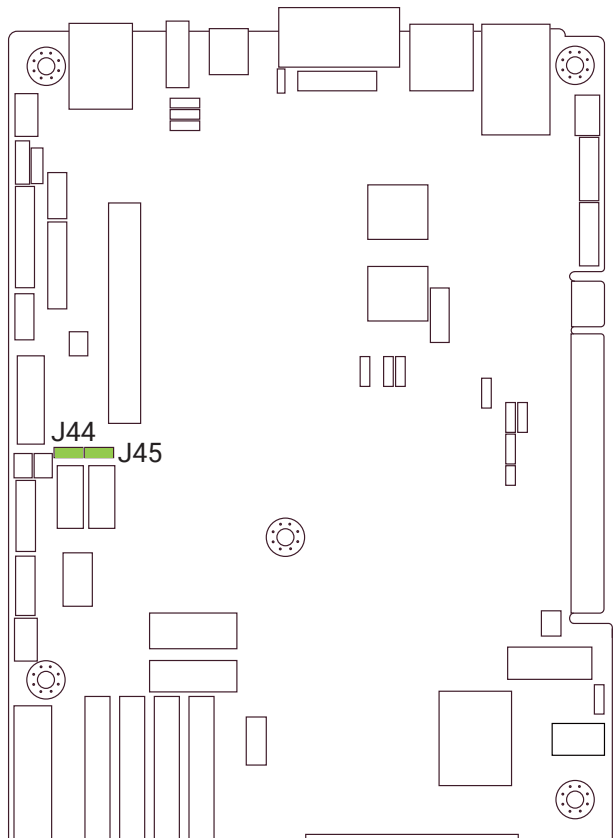
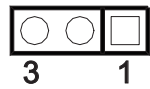
	10	11	USB2_PCH_P6_ESD_DP
USB2_PCH_P3_ESD_DP	9	12	USB2_PCH_P6_ESD_DN
USB2_PCH_P3_ESD_DN	8	13	GND
GND	7	14	USB3_PCH_P3_TX_ESD_DP
USB3_PCH_P4_TX_ESD_DP	6	15	USB3_PCH_P3_TX_ESD_DN
USB3_PCH_P4_TX_ESD_DN	5	16	GND
GND	4	17	USB3_PCH_P3_RX_ESD_DP
USB3_PCH_P4_RX_ESD_DP	3	18	USB3_PCH_P3_RX_ESD_DN
USB3_PCH_P4_RX_ESD_DN	2	19	P5V_AUX_USB_HR
P5V_AUX_USB_HR	1	20	KEY (no pin)



SATA DOM Set up (J44, J45)
3-pin header for SATA DOM.

3	P5V
2	SATAx_PIN7
1	GND

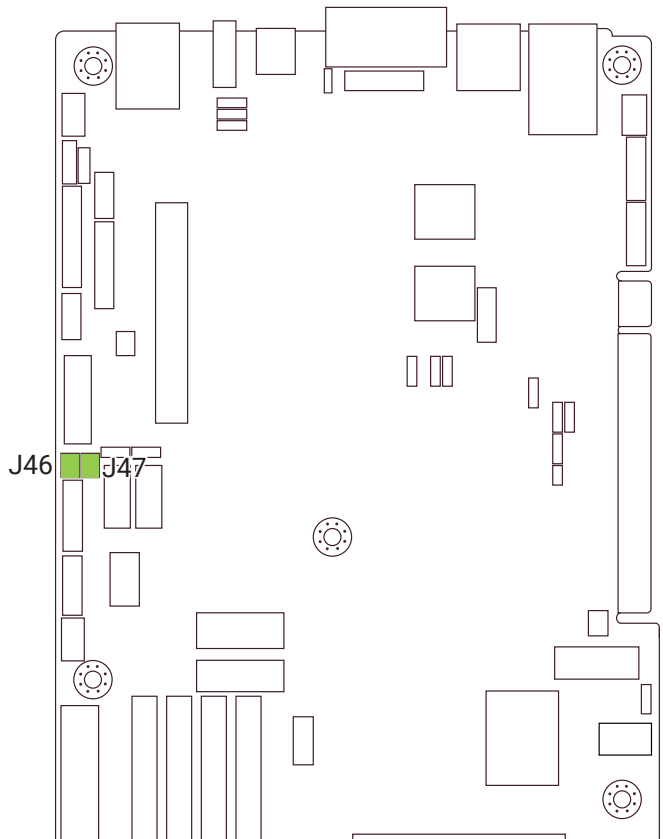
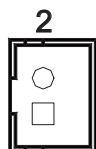
SATA DOM	Setting	
Pin1-2	SATAx_PIN7 is GND	Default
Pin2-3	SATAx_PIN7 is P5V	



SATA DOM Power Connector (J46, J47)
2-pin connector that supplies power to
SATA DOM.

2	SATAx_PWR
1	GND

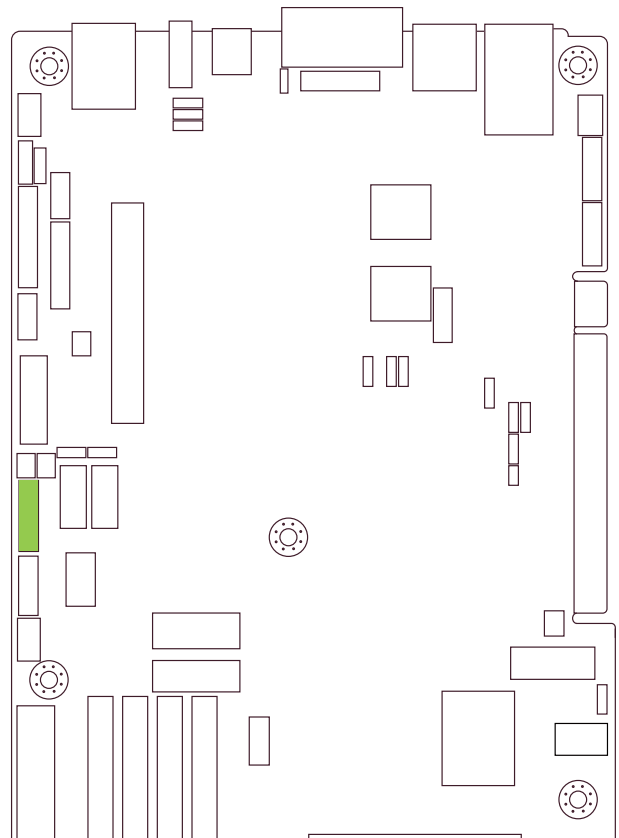
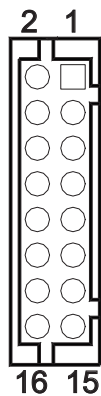
Note: SATAx_PWR support P5V power rail
to STAT-DOM.



LPC/ESPI Debug Header (J49)

2x8-pin header for LPC/ESPI debug.

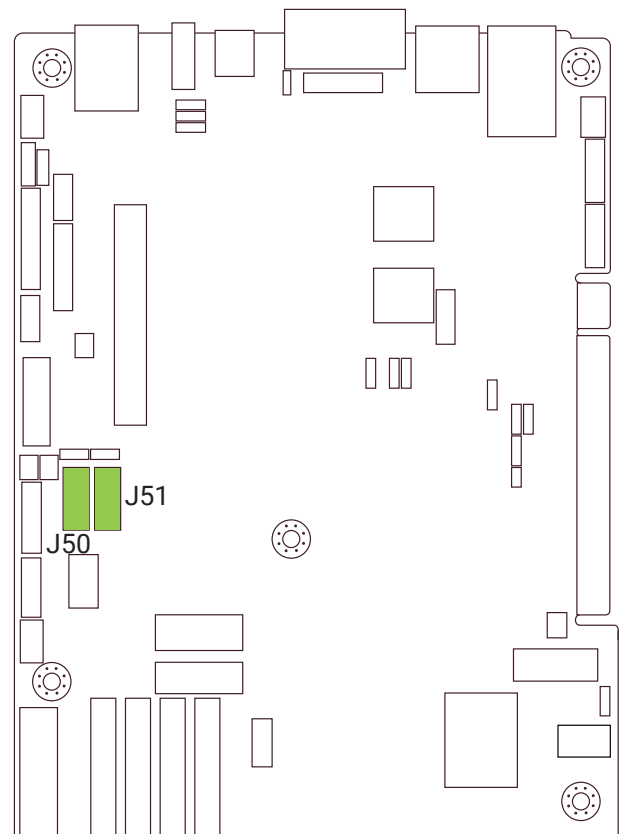
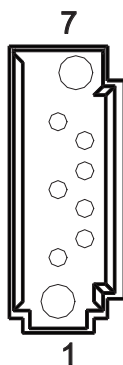
CLK_66M_24M_ESPI	2	1	GND
ESPI_CS0_N	4	3	IRQ_ESPI_ALERT0_N
RST_ESPI_RESET_N	6	5	P5V_AUX
ESPI_I03	8	7	ESPI_I02
P3V3_AUX	10	9	ESPI_I01
ESPI_I00	12	11	GND
SMB_HOST_LVC3_SCL	14	13	SMB_HOST_LVC3_SDA
P1V8_AUX	16	15	ESPI_CS1_N



SATA Connector (J50, J51)

7-pin connector for SATA.

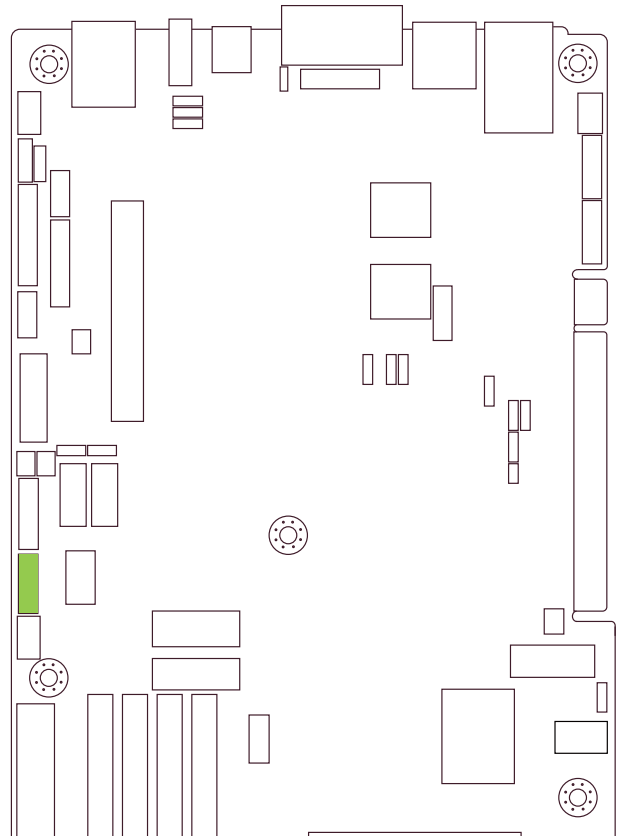
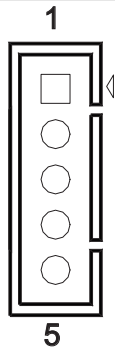
7	SATAx_PIN7
6	SATA6G_P6_RX_DP
5	SATA6G_P6_RX_DN
4	GND
3	SATA6G_P6_TX_DN
2	SATA6G_P6_TX_DP
1	GND



LCD Header (J53)

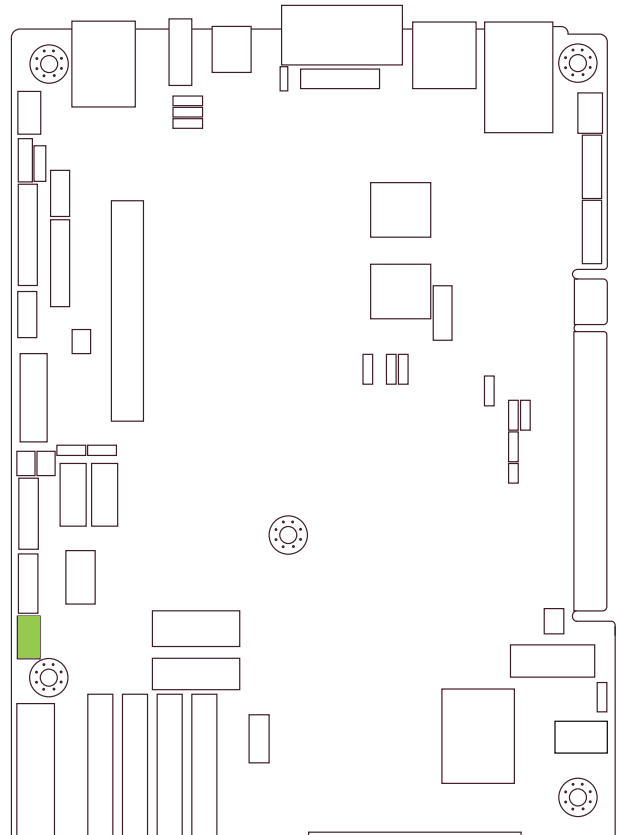
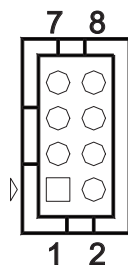
5-pin header for LCD.

1	PWRBTN_FP_BMC_N
2	RSTBTN_FP_BMC_N
3	COM_OUT_TXD4
4	COM_OUT_RXD4
5	GND

**FPGA Download Connector (J56)**

2x4-pin header for downloading FPGA.

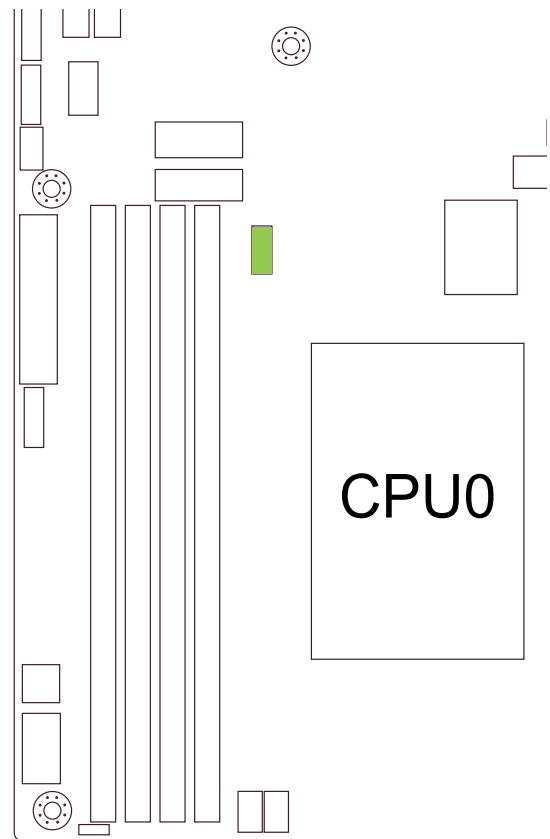
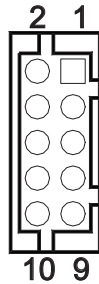
JTAG_PLD_TDI	7	8	PU_JTAG_PLD_FORCE_EN
JTAG_PLD_TMS	5	6	JTAG_PLD_JTAGEN
JTAG_PLD_TDO	3	4	P3V3_AUX
JTAG_PLD_TCK	1	2	GND



AIC QST Debug Connector (J61)

2x5-pin connector for AIC QST debug.

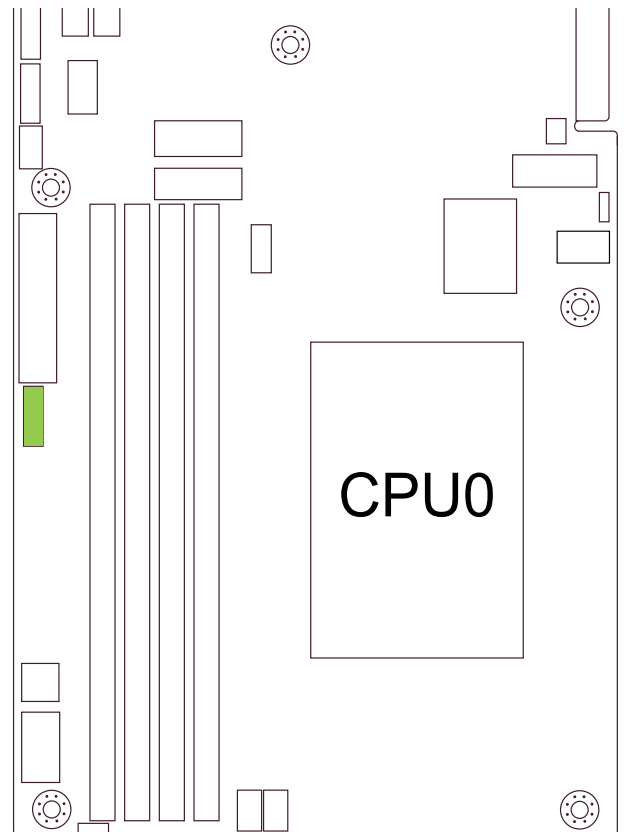
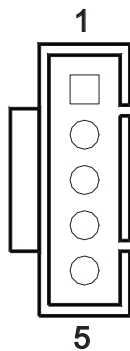
P3V3_AUX	2	1	SGPIO_PLD_QSD_CLK
GND	4	3	SGPIO_PLD_QSD_LD_N
SMB_DEBUG_STBY_SCL	6	5	SGPIO_PLD_QSD_DIN
SMB_DEBUG_STBY_SDA	8	7	SGPIO_PLD_QSD_DOUT
FM_DEBUG_MCU_PRSENT_N	10	9	GND



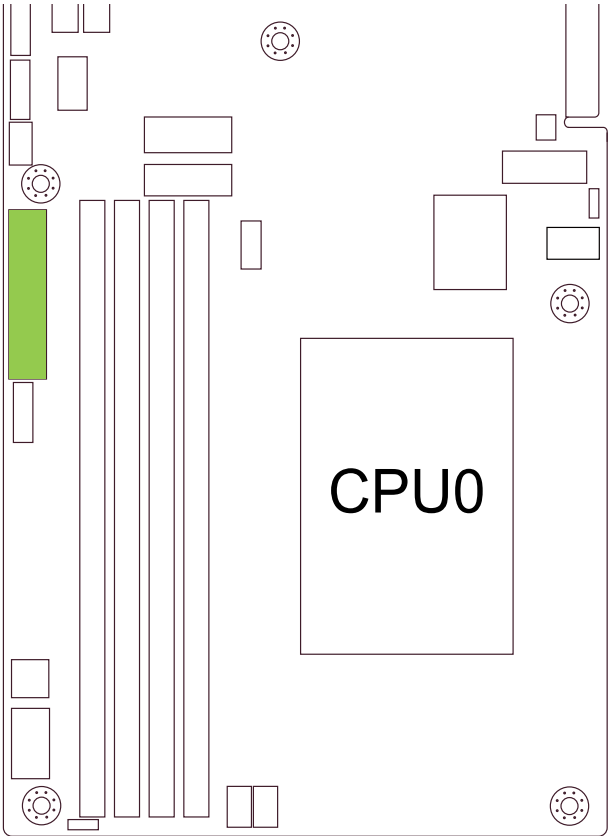
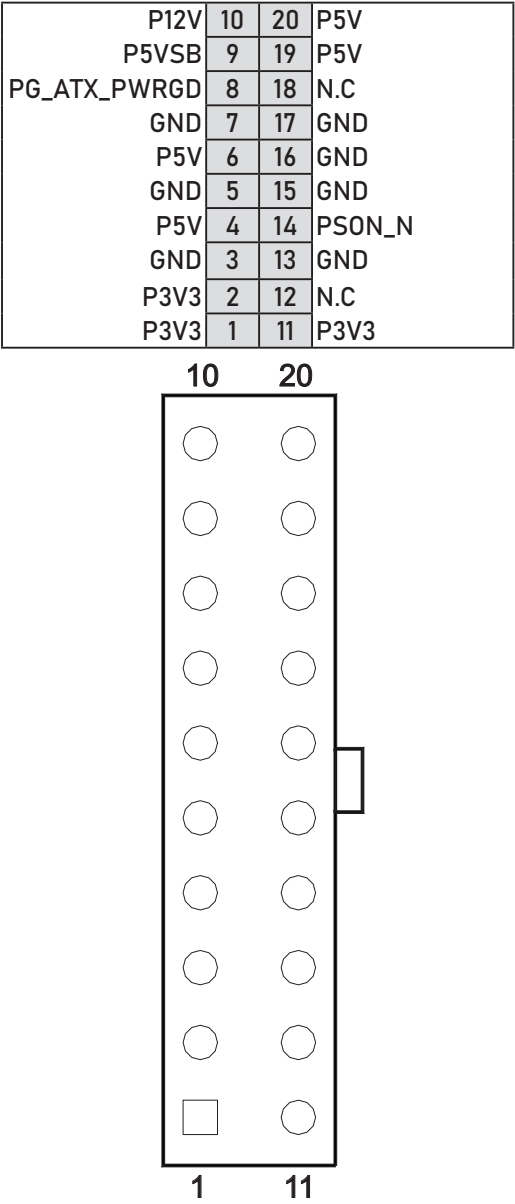
PSMI Header (J63)

5-pin header that supports PSML.

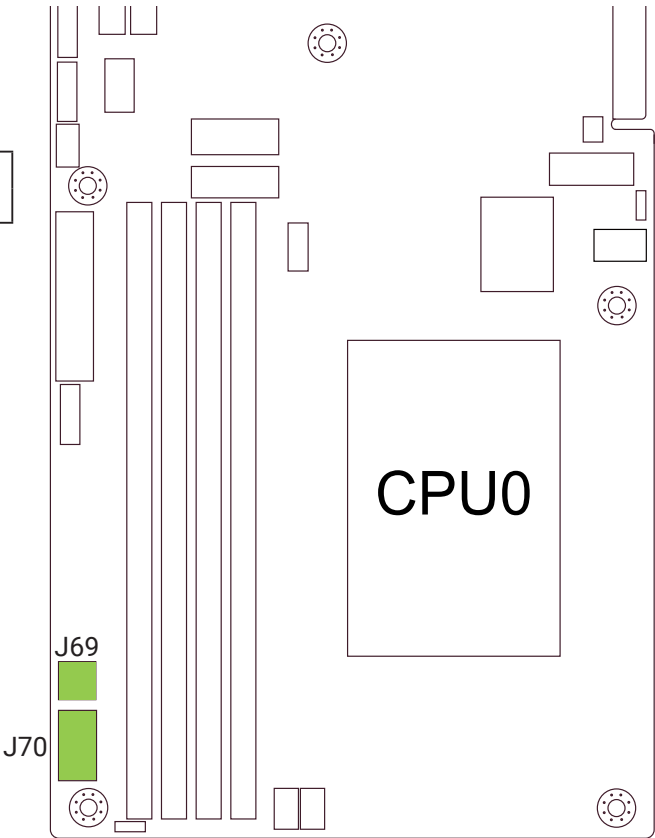
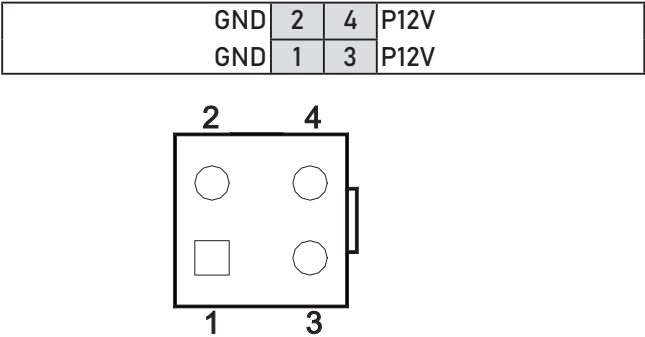
1	SMB_PMBUS_CLK
2	SMB_PMBUS_DATA
3	FM_PMBUS_ALERT_N
4	GND
5	+3.3V



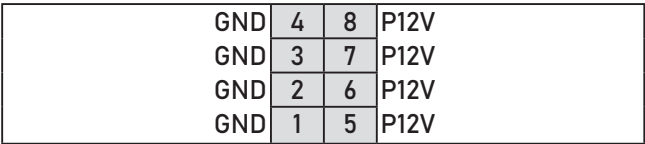
Power Connector (J62)
2x10-pin connector that supplies power.



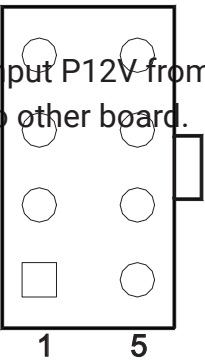
Power Supply Connector (J69, J70)
2x2-pin connector that supplies power.



2x4-pin connector that supplies power.

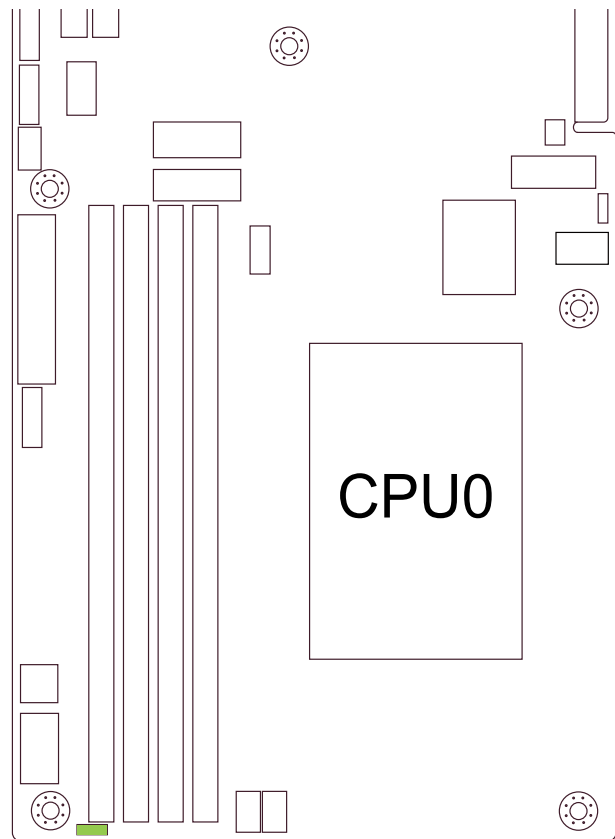
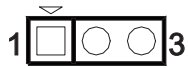


Note: J69 or J70 can be output or input for P12V.
Ex. J70 is input P12V from PSU, and J69 can be output to other board.



CPU VR SMBUS Debug Header (J73)
3-pin header that supports CPU Virtual
Reality SMBus debug.

1	I2C11SCL
2	GND
3	I2C11SDA

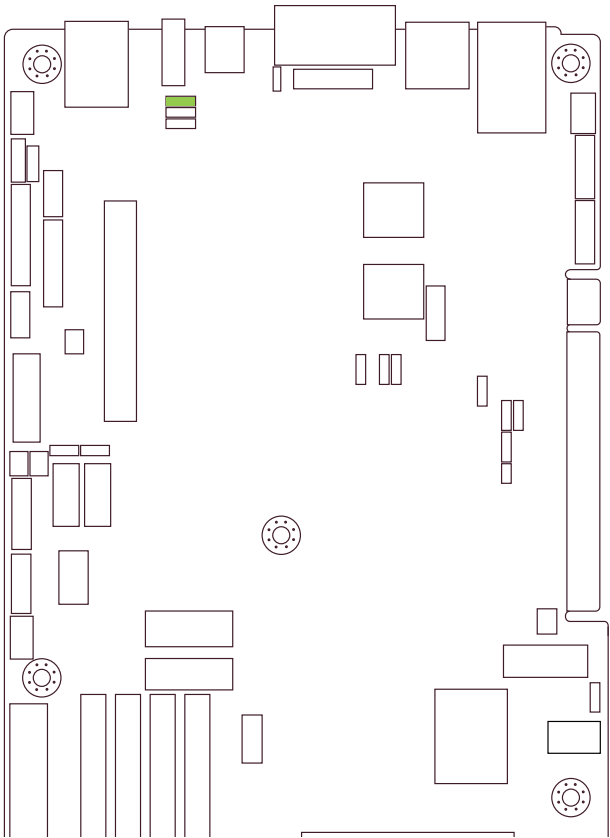
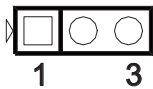


3.1.6 Jumper Definition

Audio COM Port Source Select (J10)
3-pin jumper that configures Audio COM
port source.

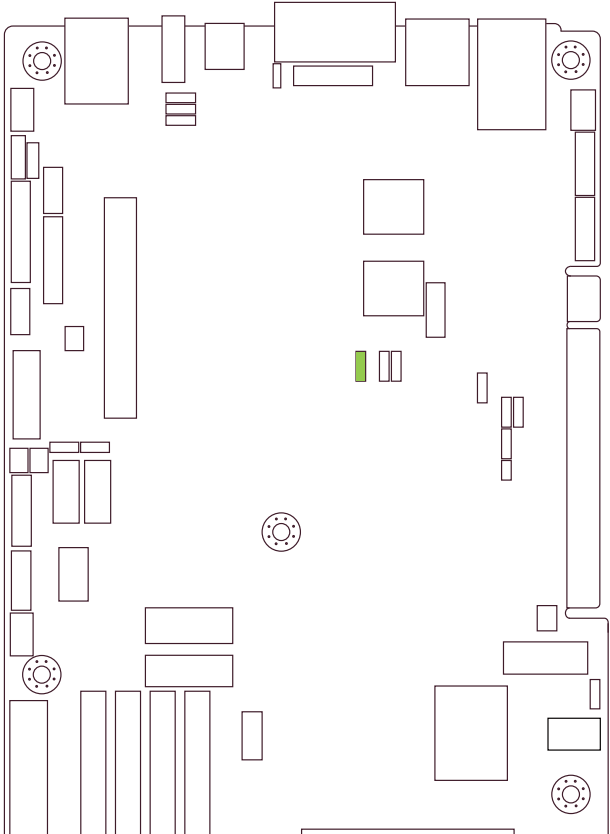
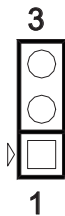
J10	Setting	
Pin1-2	PJ_TX= TXDA	Default
Pin2-3	PJ_TX= COM_ OUT_RXD5	

J11	Setting	
Pin1-2	PJ_RX= RXDA	Default
Pin2-3	PJ_TX= COM_ OUT_TXD5	



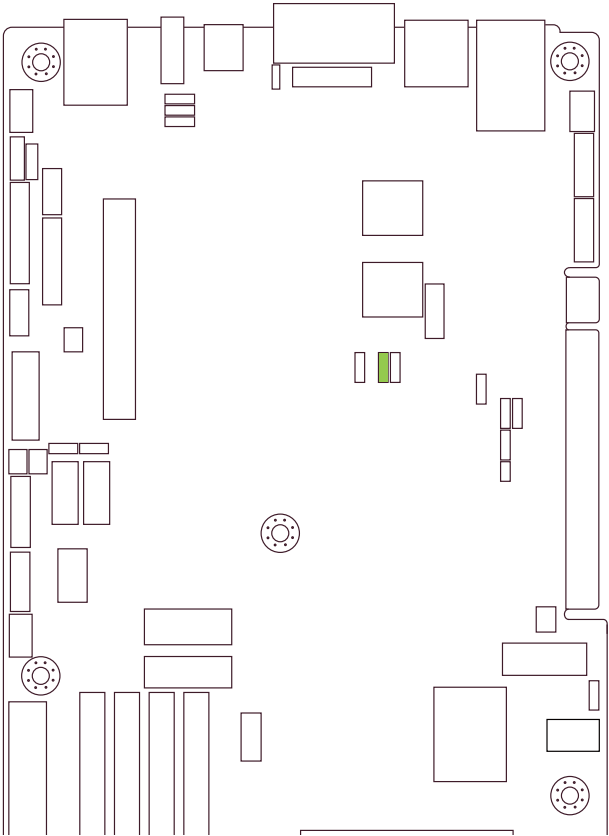
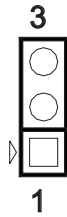
CONFIG/Recover Setting (J32)
3-pin jumper that supports Config/Recover
settings.

J32	Setting	
Pin1-2	Normal	Default
Pin2-3	Configure	



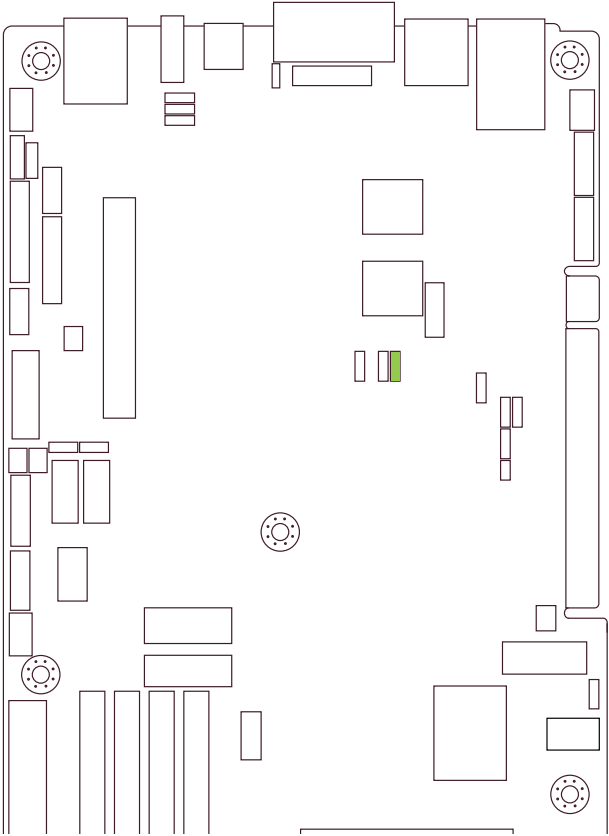
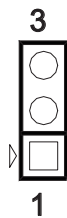
ME Firmware Update (J34)
3-pin jumper that supports ME firmware update.

J34	Setting	
Pin1-2	Normal	Default
Pin2-3	ME Force Update	



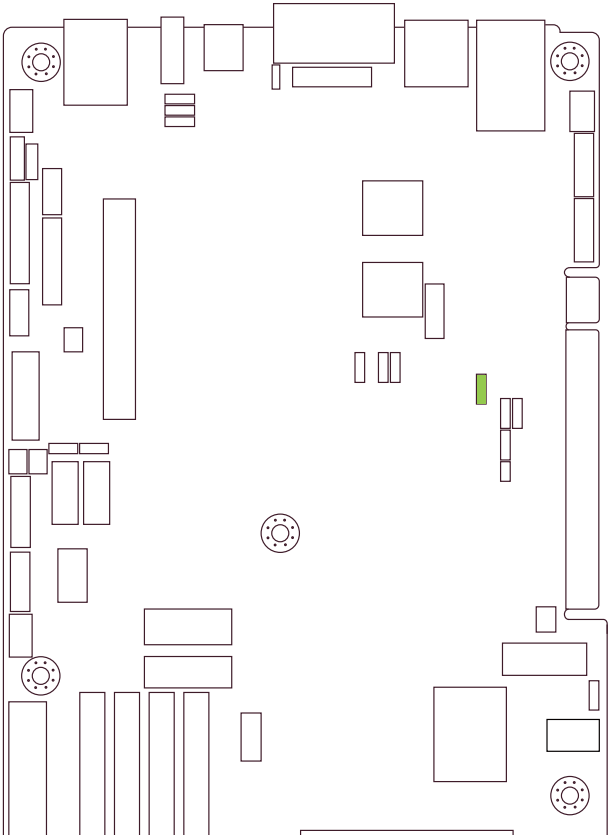
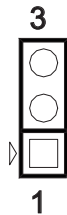
CMOS Clear (J35)
3-pin jumper that supports CMOS clear.

J35	Setting	
Pin1-2	Normal	Default
Pin2-3	Clear CMOS	



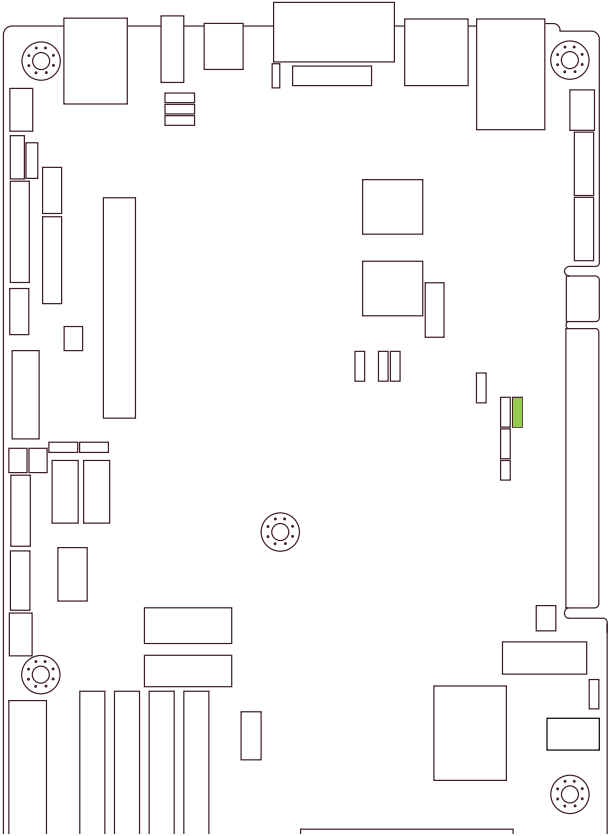
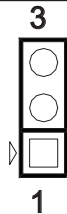
BIOS Flash Security Override (J36)
3-pin jumper that supports BIOS flash security
override.

J36	Setting	
Pin1-2	Disable	Default
Pin2-3	Enable override	



Password Clear (J40)
3-pin jumper that supports password clear
function.

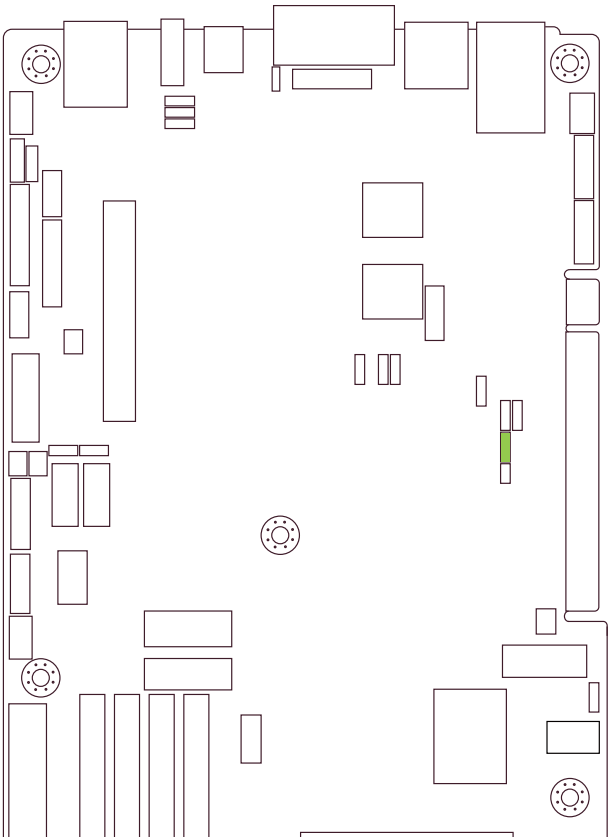
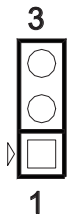
J40	Setting	
Pin1-2	Normal	Default
Pin2-3	Password Clear	



PECI Master Select (J41)

3-pin jumper that enables Peci access to BMC for DTS (Digital Thermal Sensor).

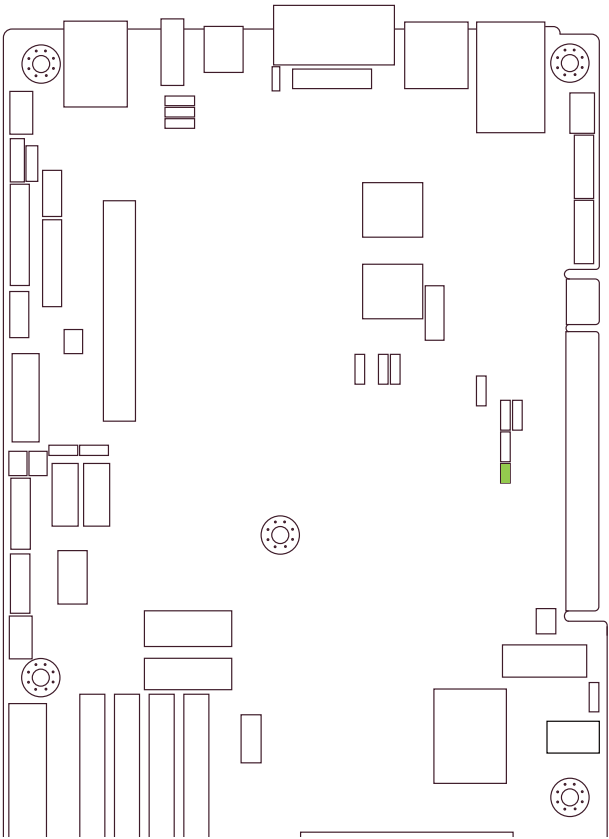
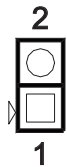
J41	Setting	
Pin 1-2	Master : PCH	Default
Pin 2-3	Master : BMC	



BMC SOCFlash Function (J48)

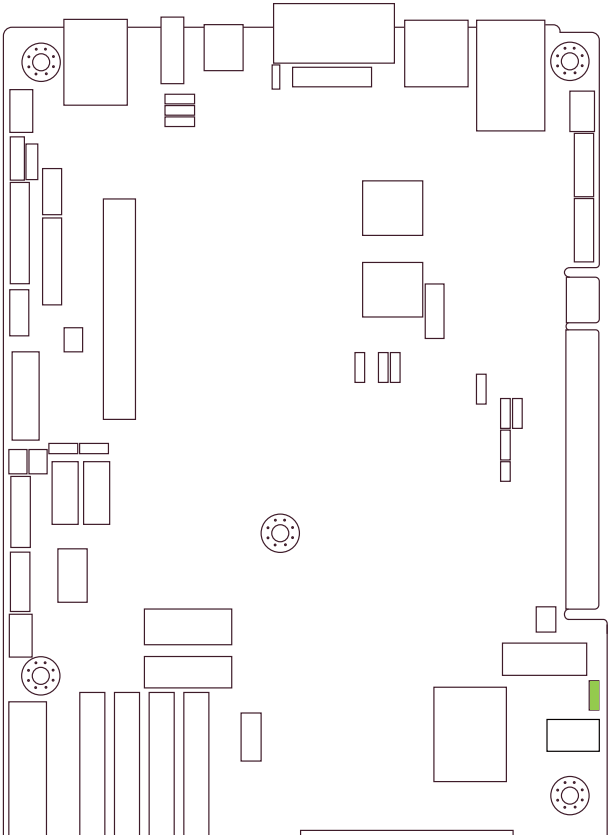
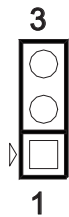
2-pin jumper that supports BMC SOC flash.

J48	Setting	
Open	Disable	Default
Short	Enable	

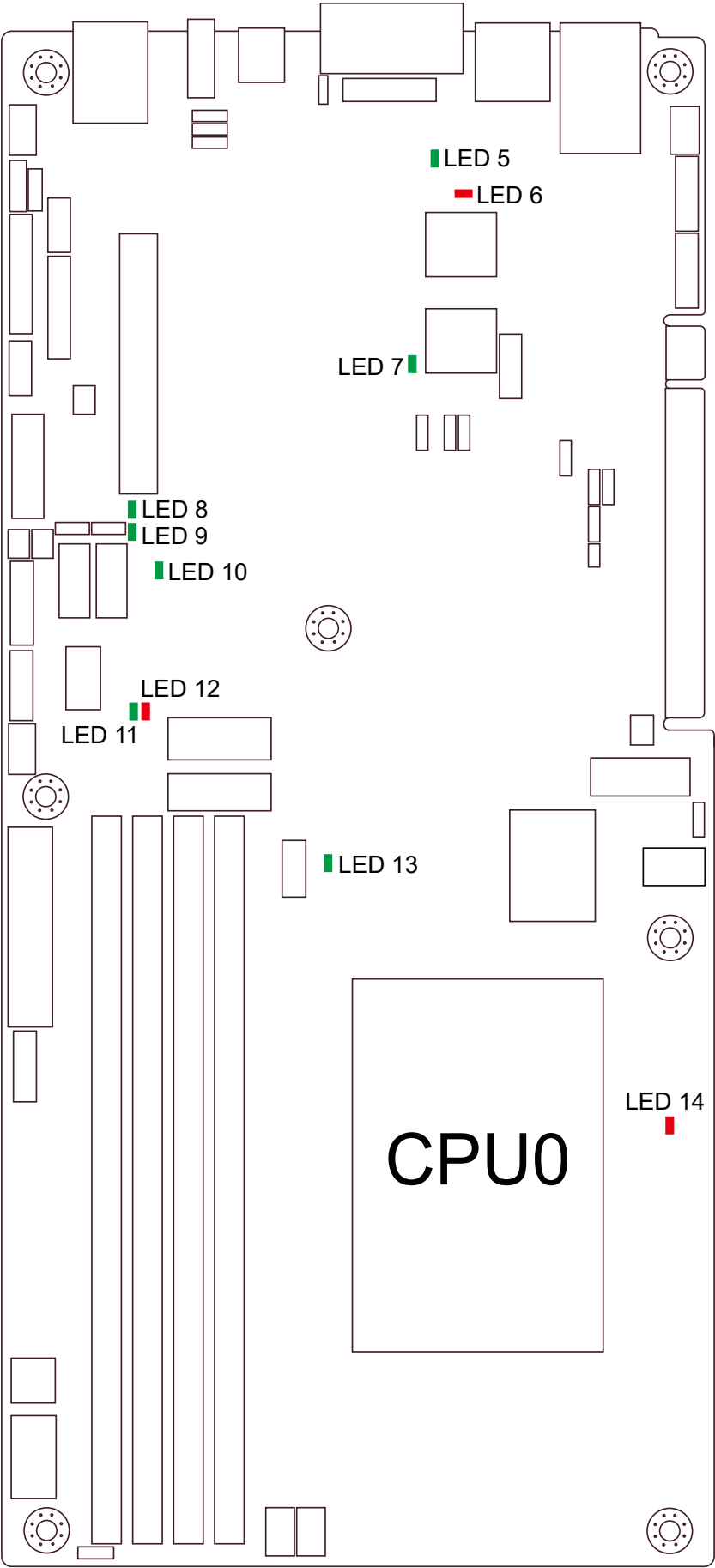


CPU PEG60 Port (J74)
3-pin jumper that supports CPU PEG60 port.

J74	Setting	
Pin1-2	Normal	Default
Pin2-3	PEG60_LANE_REVERSAL	



3.1.7 Internal LED



Item		Color	Behavior
LED5	PWRGD_SYS Signal active	Green	Power rails are fine when lighted.
LED6	System Event active	Red	System Event happen when lighted (PMBus Alert, PCH NM Throttle, PVCC_CPU_GT/ PVCC_VCCSA VRHOT protect) and will trigger CPU speed down.
LED7	BMC Heart Beat LED	Green	BMC alive when flash slow.
LED8	SLPS3_N Signal active	Green	In S0 (booting), it should off. In S5, it should on.
LED9	SLPA_N Signal active	Green	In S0 (booting), it should off. In S5, it should on.
LED10	RST_RSMRST_N Signal inactive	Green	In any mode, LED10 should on. If off, PCH would not go to ready.
LED11	PWRGD_CPU Signal active	Green	CPU Power rails are fine when lighted.
LED12	THERMTRIP_N Signal active	Red	PCH over heat when lighted.
LED13	FPGA Heart Beat / Configuration Done LED	Green	In S5, LED13 will flash. In S0, LED13 will off. In upgrade FPGA code, LED13 will on.
LED14	CATERR_N Signal active	Red	CPU/System had critical error happen when LED14 lighted.

Chapter 4. BIOS Configuration Settings

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

To enter BIOS configuration settings,

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

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

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

NOTE



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

4.1 Navigation Keys

The navigation keys are listed below.

Function Key	Description
< ↑ > < ← > < → > < ↓ >	Select item.
< Enter >	Select and enter sub-screen.
< + > < - >	Modify selected option.
< F1 >	General help.
< F2 >	Previous Value.
< F3 >	Optimized defaults.
< F4 >	Save & Exit.
< F5 > < F6 >	Change values.
< F7 >	Discard Change and Exit.
< F9 >	Load Optimal Default for all values.
< F10 >	Save changes and exit.
< F12 >	Print Screen.
< Esc >	Exit the current menu screen.

4.2 BIOS Setup

4.2.1 Menu

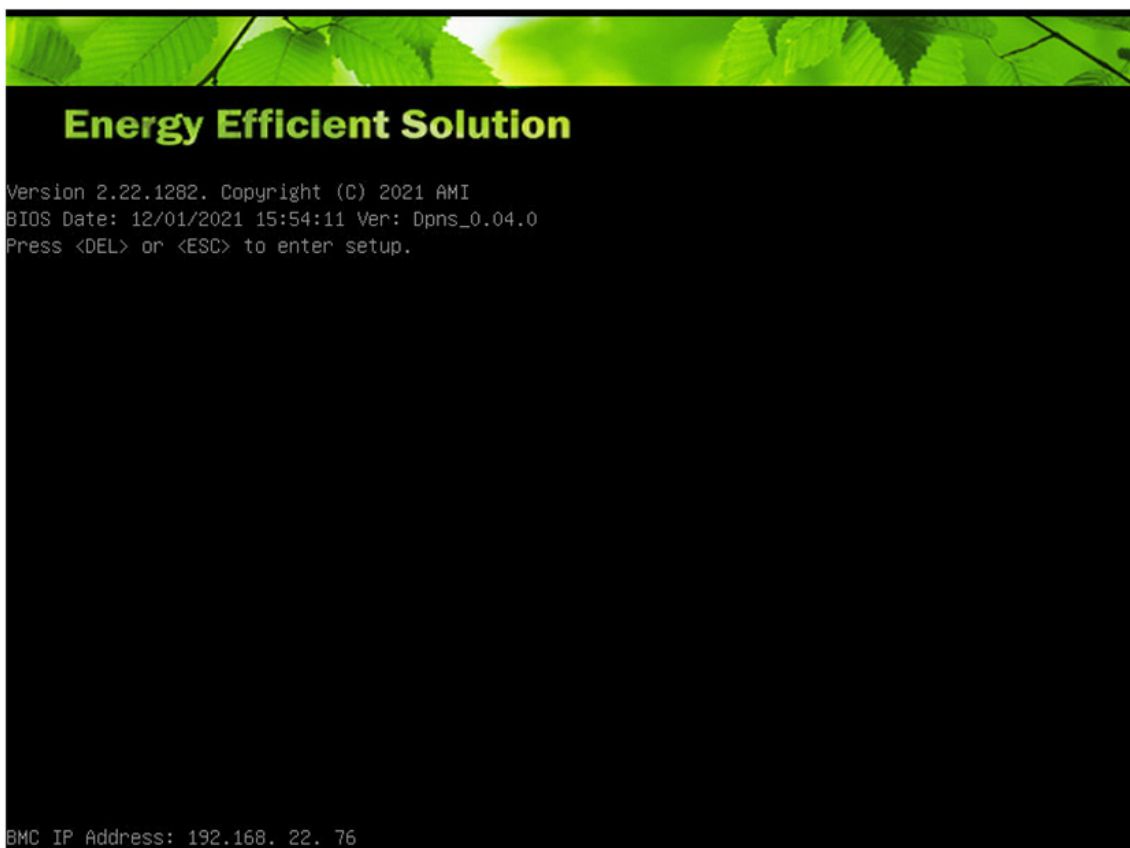
Press **←** and **→** to select the options of the menu bar.

Press **Enter** to access the option screen.

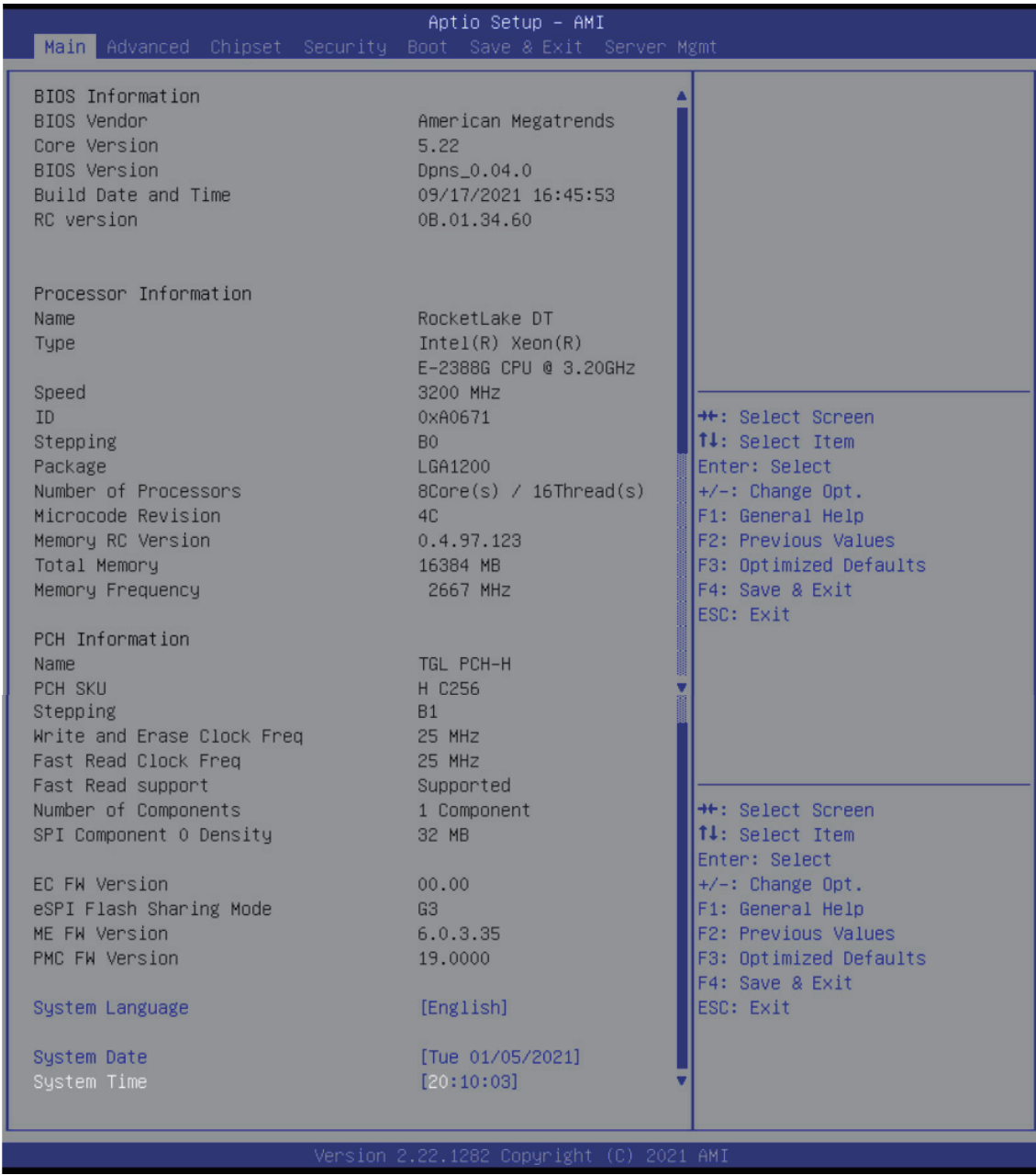
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Platform Configuration	Allows configuration of platform settings such as PCH, miscellaneous, and server ME configuration.
Socket Configuration	Allows configuration of socket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



System Language

Configures the language used in the system.

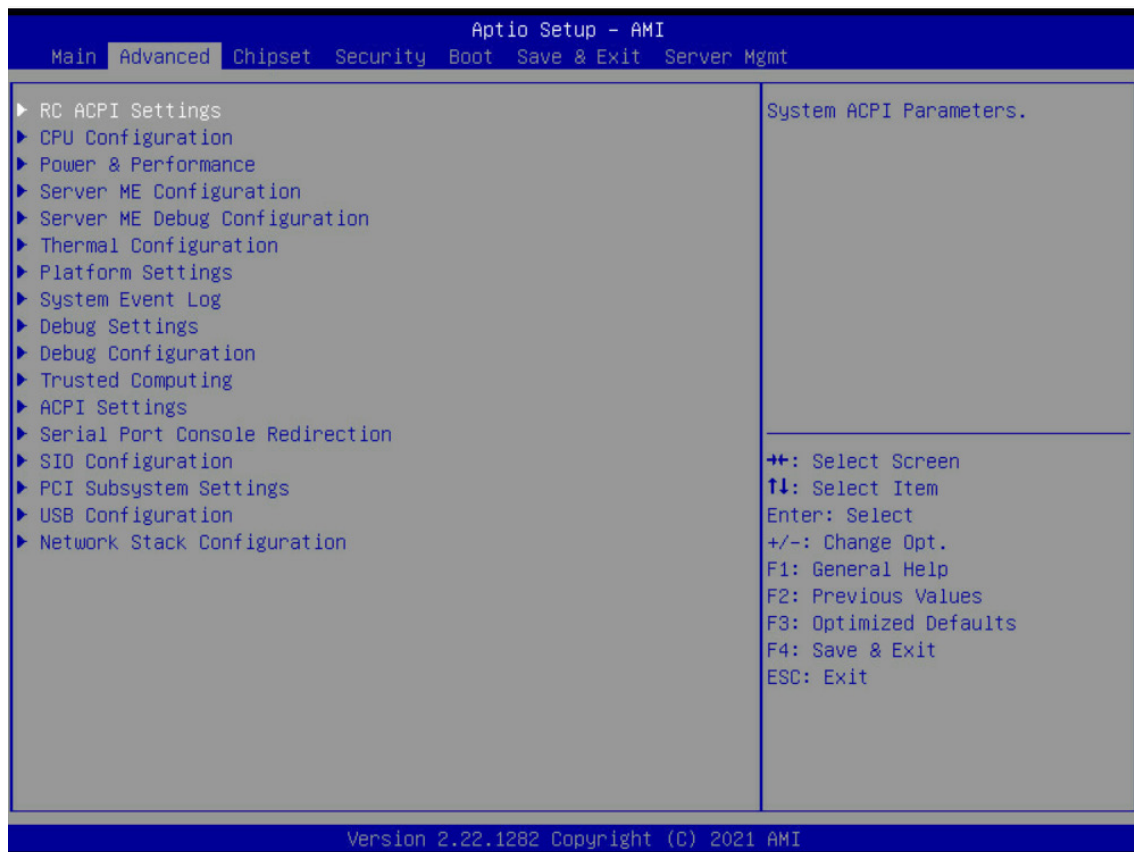
System time

Configures the current time.

System date

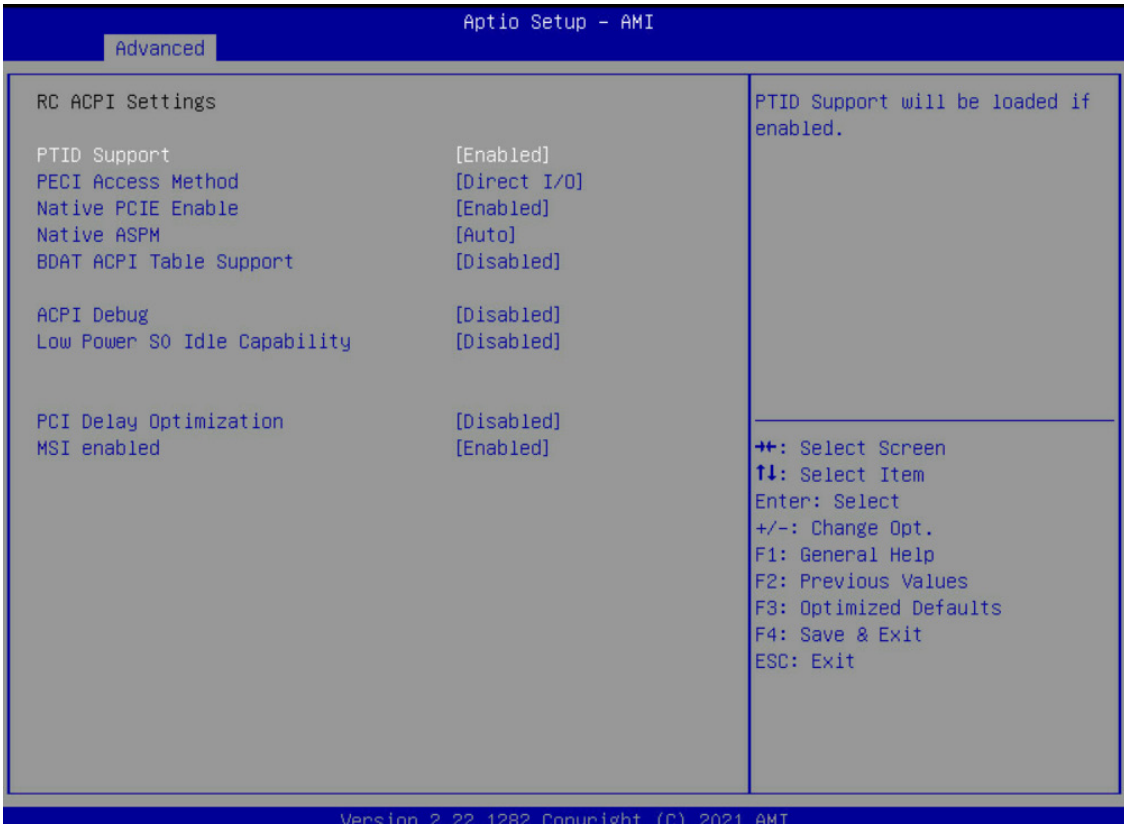
Configures the current date.

4.4 Advanced



- RC ACPI Settings
- CPU Configuration
- Power & Performance
- Server ME Configuration
- Server ME Debug Configuration
- Thermal Configuration
- Platform Settings
- System Event Log
- Debug Settings
- Debug Configuration
- Trusted Computing
- ACPI Settings
- Serial Port Console Redirection
- SIO Configuration
- PCI Subsystem Settings
- USB Configuration
- Network Stack Configuration

4.4.1 RC ACPI Settings



PTID Support

PTID Support will be loaded if enabled.

Enable
Disable

PECI Access Method

PECI Access Method is Direct I/O or ACPI.

Direct I/O
ACPI

Native PCIE Enable

Bit: PCIe Native * control

0: ~ Hot Plug

1: SHPC Native Hot Plug control

2: ~ Power Management Events

3: PCIe Advanced Error Reporting control

4: PCIe Capability Structure control

5: Latency Tolerance Reporting control

Enable
Disable

Native ASPM

Enabled: OS Controlled ASPM.

Disabled: BIOS Controlled ASPM.

Auto
Enable
Disable

BDAT ACPI Table Support

Enable support for the BDAT ACPI table.

Enable
Disable

ACPI Debug

Open a memory buffer for storing debug strings. Reenter SETUP after enabling to see the buffer address. Use method ADBG to write strings to buffer.

Enable
Disable

Low Power S0 Idle Capability

This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enabled, it also disable 8254 timer for SLP_S0 support.

Enable
Disable

PCI Delay Optimization

Experimental ACPI additions for FW latency optimizations.

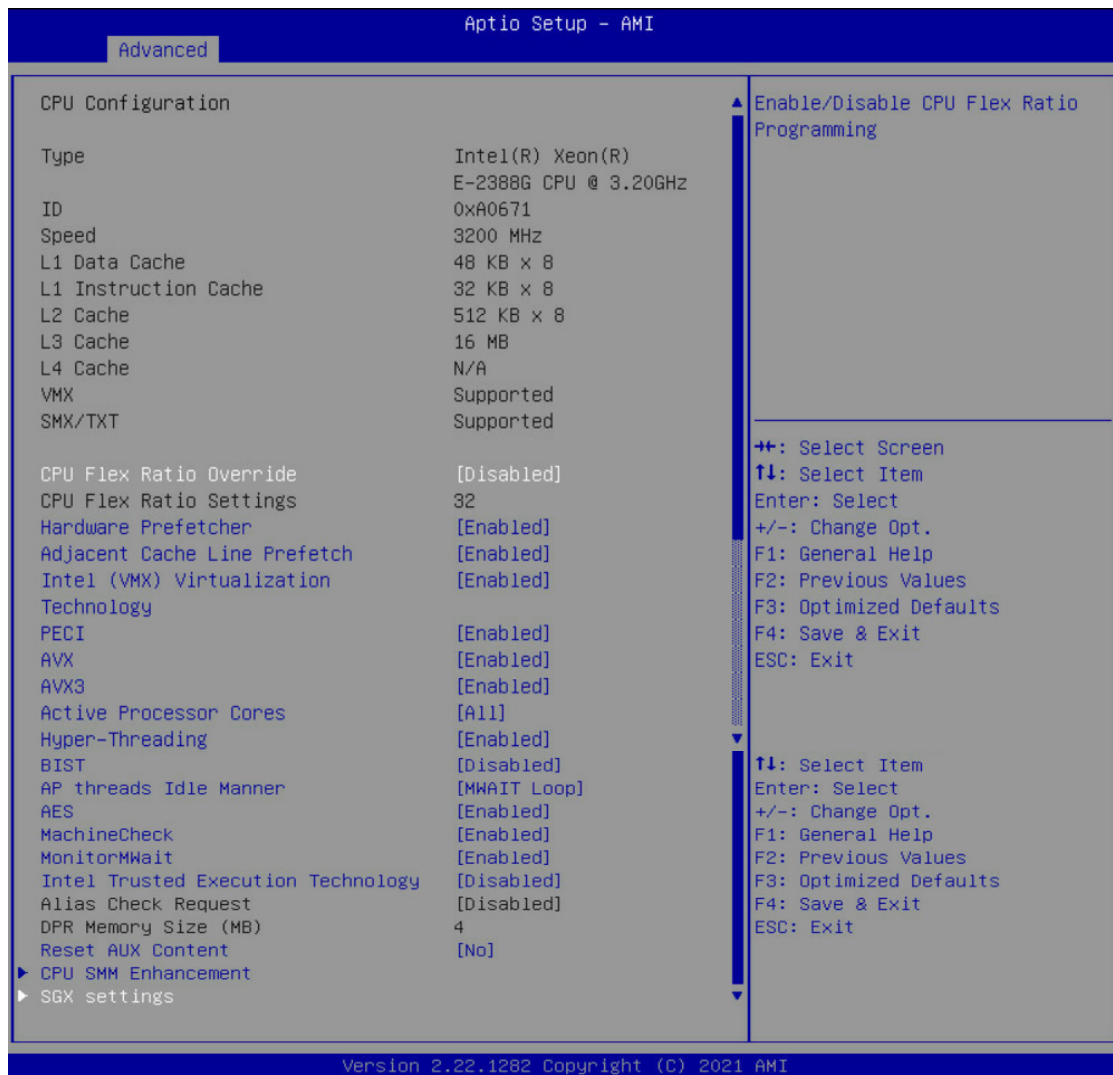
Enable
Disable

MSI enabled

When disabled, MSI support is disabled in FADT.

Enable
Disable

4.4.2 CPU Configuration



CPU Flex Ratio Override

Enable/disable CPU Flex Ratio Programming.

Enable
Disable

CPU Flex Ratio Settings

This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM).

32

Hardware Prefetcher

To turn on/off the MLC streamer prefetcher.

Enable
Disable

Adjacent Cache Line Prefetch

To turn on/off prefetching of adjacent cache lines.

Enable
Disable

Intel (VMX) Virtualization Technology

When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

Enable
Disable

PECI

Enable/disable PECI.

Enable
Disable

AVX

Enable/disable the AVX 2/3 Instructions. This is applicable for Big Core only.

Enable
Disable

AVX3

Enable/disable the AVX 3 Instructions. This is applicable for Big Core only.

Enable
Disable

Active Processor Cores

Number of cores to enable in each processor package.

All	3
1	4
2	5

Hyper-Threading

Enable or disable Hyper-Threading Technology.

Enable
Disable

BIST

Enable/disable BIST (Built-In Self Test) on reset.

Enable
Disable

AP threads Idle Manner

AP threads Idle Manner for waiting signal to run

HALT Loop
MWAIT Loop
RUN Loop

AES

Enable/disable AES (Advanced Encryption Standard).

Enable
Disable

Machine Check

Enable/disable Machine Check.

Enable
Disable

MonitorMWait

Enable/disable MonitorMWait.

Enable
Disable

Intel Trusted Execution Technology

Enables utilization of additional hardware capabilities provided by Intel (R) Trusted Execution Technology. Changes require a full power cycle to take effect.

Enable
Disable

Alias Check Request

Enables Txt Alias Checking capability. Changes require full Txt capability before it will take effect. It is a one time only change, next reboot will be reset.

Enable
Disable

DPR Memory Size (MB)

Reserve DPR memory size (0-255) MB.

4

Reset AUX Content

Reset TPM Aux content. Txt may not functional after AUX content gets reset.

Yes
No

➤ CPU SMM Enhancement**SMM Use Delay Indication**

Enable/disable usage of SMM_DELAYED MSR for MP sync in SMI.

Enable
Disable

SMM Use Block Indication

Enable/disable usage of SMM_BLOCKED MSR for MP sync in SMI.

Enable
Disable

SMM Use SMM en-US Indication

Enable/disable usage of SMM_ENABLE MSR for MP sync in SMI.

Enable
Disable

➤ SGX Settings**Software Guard Extensions (SGX)**

Enable/disable Software Guard Extensions (SGX).

Enable
Software Controlled
Disable

4.4.3 Power & Performance



➤ CPU- Power Management Control

Boot performance mode

Select the performance state that the BIOS will set starting from reset vector.

Max Battery
Max Non-Turbo Performance
Turbo Performance

Intel(R) SpeedStep(tm)

Allows more than two frequency ranges to be supported.

Enable
Disable

Race To Halt (RTH)

Enable/disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg tate faster to reduce overall power (RTH is controlled through MSR 1FC bit 20).

Enable
Disable

Intel(R) Speed Shift Technology

Enable/disable Native Mode support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.

Disable
Native Mode
Out of Band Mode

Per Core P State OS control mode

Enable/disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.

Enable
Disable

HwP Autonomous Per Core P State

Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11).

Enable
Disable

HwP Autonomous EPP Grouping

Enable EPP grouping (default Bit 29 = 0, command 0x11) Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 = 1, command 0x11) autonomous will not necessarily request same values for all cores with same EPP.

Enable
Disable

EPB override over Peci

Enable/disable EPB override over Peci. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow OOB EPB Peci override control.

Enable
Disable

HwP Fast MSR Support

Enable/disable HwP Fast MSR Support for IA32_HWP_REQUEST MSR.

Enable
Disable

HDC Control

This option allows HDC configuration. Disabled: Disable HDC Enabled: Can be enabled by OS if OS native support is available.

Enable
Disable

Turbo Mode

Enable/disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.

Enable
Disable

Platform PL1/PL2 Enable

Enable/disable Platform Power Limit 1 programming. If this option is enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window.

Enable
Disable

Power Limit 4 Override

Enable/disable Power Limit 4 override. If this option is disabled, BIOS will leave the default values for Power Limit 4.

Enable
Disable

C states

Enable/disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.

Enable
Disable

Enhanced C-states

Enable/disable C1E. When enabled, CPU will switch to minimum speed when all cores enter C-State.

Enable
Disable

C-State Auto Demotion

Configure C-State Auto Demotion.

C1
Disable

C-State Un-demotion

Configure C-State Un-demotion.

C1
Disable

Package C-State Demotion

Package C-State Demotion.

Enable
Disable

Package C-State Un-demotion

Package C-State Un-demotion.

Enable
Disable

CState Pre-Wake

Disable - Sets bit 30 of POWER_CTL MSR(0x1FC) to 1 to disable the Cstate Pre-Wake.

Enable
Disable

IO MWAIT Redirection

When set, will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+offset to MWAIT(offset).

Enable
Disable

Package C State Limit

Maximum Package C State Limit Setting. Cpu Default: Leaves to Factory default value.Auto: Initializes to deepest available Package C State Limit.

Auto	C7S
C0/C1	C8
C2	C9
C3	C10
C6	CPU Default
C7	

Time Unit

Unit of measurement for IRTL value - bits [12:10].

1 ns	32768 ns
32 ns	1048576 ns
1024 ns	33554432 ns

Latency

Interrupt Response Time Limit value- bits [9:0], Enter 0-1023.

78

Thermal Monitor

Enable/disable Thermal Monitor.

Enable
Disable

Interrupt Redirection Mode Selection

Interrupt Redirection Mode Select for Logical Interrupts.

Fixed Priority	Hash Vector
Round robin	No Change

Timed MWAIT

Enable/disable Timed MWAIT Support.

Enable
Disable

EC Turbo Control Mode

Enable/Disable EC Turbo Control mode.

Enable
Disable

Energy Performance Gain

Enable/disable Energy Performance Gain.

Enable
Disable

EPG DIMM Idd3N

Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.

26

EPG DIMM Idd3P

Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis.

11

➤➤ View/Configure Turbo Options

Package Power Limit MSR Lock

Enable/disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.

Enable
Disable

Power Limit 1/2 Override

Enable/disable Power Limit 1/2 override. If this option is disabled, BIOS will program the default values for Power Limit 1/2 and Power Limit 1/2 Time Window.

{ Power Limit 1 Override }

Enable
Disable

{ Power Limit 2 Override }

Enable
Disable

Power Limit 2

Power Limit 2 value in Milli Watts. BIOS will round to the nearest 1/8W when programming. If the value is 0, BIOS will program this value as 1.25*TDP. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.

Energy Efficient Turbo

Enable/disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. Recommended only to disable in overclocking situations where turbo frequency must remain constant. Otherwise, leave enabled.

Turbo Configuration

To change the PL2 and Tau to mitigate the thermal throttling event storm.

➤➤➤ Turbo Ratio Limit options**Turbo Ratio Limit Ratio0-7 (TRLR)**

Turbo Ratio Limit Ratio0-7 (TRLR) with range of Max Non-Turbo to 120. This Turbo Ratio Limit Ratio0-7 must be greater than or equal all other ratio values. If this value is invalid, then set all other active cores to minimum. Otherwise, align the Ratio Limit to 0.

➤➤ CPU VR Settings**VR Power Delivery Design**

Specifies the RKL-S board design used for the VR settings override values. By default, BIOS will override the default RKL-S VR settings based on the board design. A value of AUTO(0) will use the board ID to determine the board design. Any other value will override the board id logic to provide a custom VR Power Delivery Design value. This is intended primarily for validation.

AUTO	RKL S 6+1 35W
RKL S 8+1 35W0	RKL S 6+1 65W
RKL S 8+1 65W	RKL S 6+1 80W
RKL S 8+1 80W	RKL S 6+1 125W
RKL S 8+1 125W	

PSYS Slope

PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9."

PSYS Offset

PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4.

PSYS Prefix

Sets the offset value as positive or negative.

PSYS PMax Power

PSYS PMax power, defined in 1/8 Watt increments. Range 0-8192. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.

Min Voltage Override

Min Voltage Override. Enable to override minimum voltage for runtime and for C8.

Enable
Disable

➤➤➤ Acoustic Noise Settings**Acoustic Noise Mitigation**

Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state.

Enable
Disable

Pre Wake Time

Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.

0

Ramp Up Time

Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.

0

Ramp Down Time

Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.

0

Disable Fast PKG C State Ramp for IA Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

True
False

Slow Slew Rate for IA Domain

Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.

Fast/2	Fast/8
Fast/4	Fast/16

Disable Fast PKG C State Ramp for GT Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

True
False

Slow Slew Rate for GT Domain

Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.

Fast/2	Fast/8
Fast/4	Fast/16

Disable Fast PKG C State Ramp for SA Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

True
False

Slow Slew Rate for SA Domain

Set VR SA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled.

Fast/2	Fast/8
Fast/4	Fast/16

➤➤➤ System Agent VR Settings/Core I/A VR Settings/GT VR Settings

VR Config Enable

VR Config enable.

Enable
Disable

AC Loadline

AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.

0

DC Loadline

DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.

0

PS Current Threshold1/2/3

PS Current Threshold1, disable from BIOS.

0

PS3/4 Enable

PS3/4 enable/disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.

Enable
Disable

IMON Slope

IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.

0

IMON Offset

IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4.

0

IMON Prefix

Sets the offset value as positive or negative.

[00] +
[01] -

VR Current Limit

Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.

0

VR Voltage Limit

VR Voltage Limit, defined in mV. Range is 0-7999mV. For a Voltage Limit of 1.25V, enter 1250. 0 = AUTO. Uses BIOS VR mailbox command 0x6.

0

Min Voltage Override

Min Voltage Override. Enable to override minimum voltage for runtime and for C8.

Enable
Disable

➤➤➤ Acoustic Noise Settings**Acoustic Noise Mitigation**

Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state.

Enable
Disable

Pre Wake Time

Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.

0

Ramp Up Time

Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.

0

Ramp Down Time

Set the maximum Ramp Down randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Periodicity Alteration (DPA) tuning.

0

Disable Fast PKG C State Ramp for IA Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

True
False

Slow Slew Rate for IA Domain

Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.

Fast/2	Fast/8
Fast/4	Fast/16

Disable Fast PKG C State Ramp for GT Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

True
False

Slow Slew Rate for GT Domain

Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.

Fast/2	Fast/8
Fast/4	Fast/16

Disable Fast PKG C State Ramp for SA Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

True
False

Slow Slew Rate for SA Domain

Set VR SA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled.

Fast/2	Fast/8
Fast/4	Fast/16

➤➤➤ System Agent VR Settings/Core I/A VR Settings/GT VR Settings

VR Config Enable

VR Config enable.

Enable
Disable

AC Loadline

AC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.

0

DC Loadline

DC Loadline defined in 1/100 mOhms. A value of 100 = 1.00 mOhm, and 1255 = 12.55 mOhm. Range is 0-6249 (0-62.49 mOhms). 0 = AUTO/HW default. Uses BIOS mailbox command 0x2.

0

PS Current Threshold1/2/3

PS Current Threshold1, disable from BIOS.

0

PS3/4 Enable

PS3/4 enable/disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.

Enable
Disable

IMON Slope

IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x4.

0

IMON Offset

IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x4.

0

IMON Prefix

Sets the offset value as positive or negative.

[00] +
[01] -

VR Current Limit

Voltage Regulator Current Limit (Icc Max). This value represents the Maximum instantaneous current allowed at any given time. The value is represented in 1/4 A increments. A value of 400 = 100A. 0 means AUTO. Uses BIOS VR mailbox command 0x6.

0

VR Voltage Limit

VR Voltage Limit, defined in mV. Range is 0-7999mV. For a Voltage Limit of 1.25V, enter 1250. 0 = AUTO. Uses BIOS VR mailbox command 0x6.

0

4.4.4 Server ME Configuration



Altitude

The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 8000h value if the altitude is unknown.

8000

MCTP Bus Owner

MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.

0

PSU#1/#2/#3/#4

PMBus address (7-bit) that will be used to retrieve the status of PSU #1, use zero to disable query.

58/59/0

4.4.5 Server ME Debug Configuration



➤ Server ME General Configuration

ME Initialization Complete Timeout

This option defines how long BIOS waits for ME to initialize.

Enable HSIO Messaging

Enable/disable HSIO messaging.

Enable
Disable

DRAM Init Done Enable

Enable/disable notifying ME about DRAM initialization. (It Enables/Disables UMA functionality.)

Enable
Disable

DRAM Initialization Status

Override the DRAM initialization status value.

Auto - true status	Success
No Memory in Channels	Memory Init Error

Pre-DramInitDone ME Reset

When ME is in recovery because of internal error try to reset it.

Enable
Disable

HMRFP0 via HECI-3

Enables sending HMRFP0 and other SMM communication with ME via HECI-3 interface instead of HECI-1.

Enable
Disable

HMRFP0_LOCK Message

Enable/disable sending HMRFP0_LOCK message to ME.

Enable
Disable

HMRFP0_ENABLE Message

Enable/disable sending HMRFP0_ENABLE message to ME.

Enable
Disable

Region selector

Choose which region will be enabled.

Intel ME region
Region 13

END_OF_POST Message

Enable/disable sending END_OF_POST message to ME.

Enable
Disable

REGION_SELECT Message

Enable/disable sending REGION_SELECT message to ME.

Enable
Disable

WATCHDOG_CONTROL Message

Enable/disable sending WATCHDOG_CONTROL messages to ME.

Enable
Disable

Disable WATCHDOG in SPS

When set to Enable, disable WATCHDOG in SPS unconditionally.

Enable
Disable

ARB SVN Commit Message

Enable hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution.

Enable
Disable

CF9 global reset promotion

Enable/disable promoting CF9 reset to global.

Enable
Disable

Global Reset Lock

Enable/disable locking the joint ME and host reset capability.

Enable
Disable

HECI-1/2/3/4 Enable

Override HECI-1 status on PCI, or let firmware decide based on ME type (auto).

Options =[00]Disabled [01]Enabled *[02]

Auto
Enable
Disable

IDEr Enable

Override IDEr status on PCI, or let firmware decide based on ME type (auto).

Auto
Enable
Disable

KT Enable

Override KT status on PCI, or let firmware decide based on ME type (auto).

Auto
Enable
Disable

HECI-1/2/3/4 Hide in ME

Enables sending request to ME to hide or disable HECI-1 on host PCI.

Off
Hide
Disable

D0I3 Setting for HECI Disable

Setting this option disables setting D0I3 bit for all HECI devices.

Enable
Disable

Break RTC Configuration

This is a test option which breaks RTC configuration.

Enable
Disable

Core Bios Done Message

Enable/disable Core Bios Done message sent to ME.

Enable
Disable

Delayed Authentication Mode (DAM) Override

Enables overriding the state of the Delayed Authentication Mode (DAM).

Enable
Disable

Delayed Authentication Mode (DAM)

Enable/disable Delayed Authentication Mode (DAM).

Enable
Disable

MCTP Broadcast Cycle

Enable/disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner.

Enable
Disable

➤➤ Override ICC Clock Settings**ICC Clock Spread Spectrum**

Turn on / off Spread Spectrum Setting for IsCLK.

Enable
Disable

➤ **NM Configuration**

Power Measurement Override.

Override power measurement support status reported to ME.

Enable
Disable

Power Measurement

Override power measurement support status reported to ME.

Enable
Disable

Hardware Change Override

Override hardware change detection status reported to ME.

Enable
Disable

Hardware Changed

Override hardware change detection status reported to ME.

Yes
No

PTU Load Override

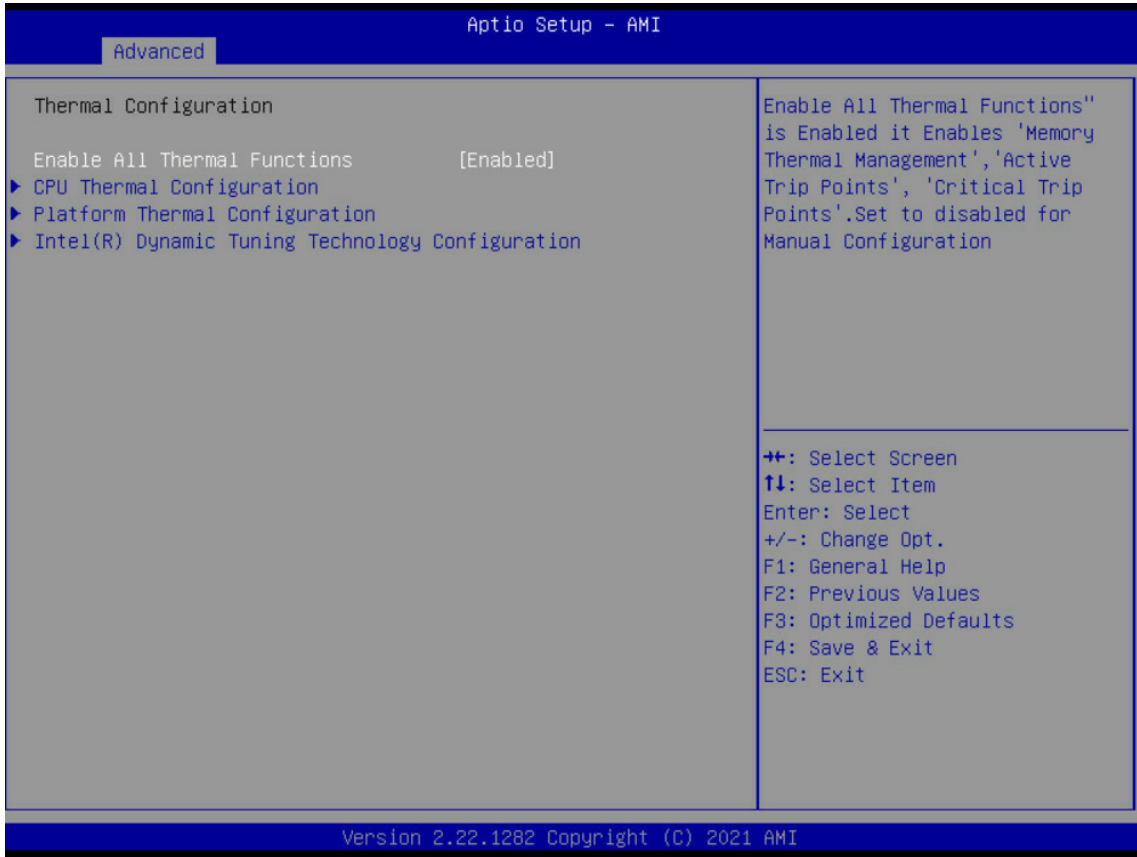
In MROM-less system force loading PTU regardless of ME request.

Enable
Disable

➤ **ME UEFI FW Health Status**

Information about ME UEFI FW Health Status.

4.4.6 Thermal Configuration



Enable All Thermal Functions

Enable All Thermal Functions" is Enabled it Enables 'Memory Thermal Management', 'Active Trip Points', 'Critical Trip Points'. Set to disabled for Manual Configuration.

Enable
Disable

➤ CPU Thermal Configuration

DTS SMM

Disabled: ACPI thermal management uses EC reported temperature values. Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values. Out of Spec: ACPI Thermal Management uses EC reported temperature values and DTS SMM is used to handle Out of Spec condition.

Critical Temp Reporting (Out Of spec)
Enable
Disable

Tcc Activation Offset

Offset from factory set Tcc activation temprature at which the Thermal Control Circuit must be activated. Tcc will be activated at: Tcc Activation Temp - Tcc Activation Offset. Tcc Activation Offset range is 0 to 63.

0

➤ **NM Configuration**

Power Measurement Override.

Override power measurement support status reported to ME.

Enable
Disable

Power Measurement

Override power measurement support status reported to ME.

Enable
Disable

Hardware Change Override

Override hardware change detection status reported to ME.

Enable
Disable

Hardware Changed

Override hardware change detection status reported to ME.

Yes
No

PTU Load Override

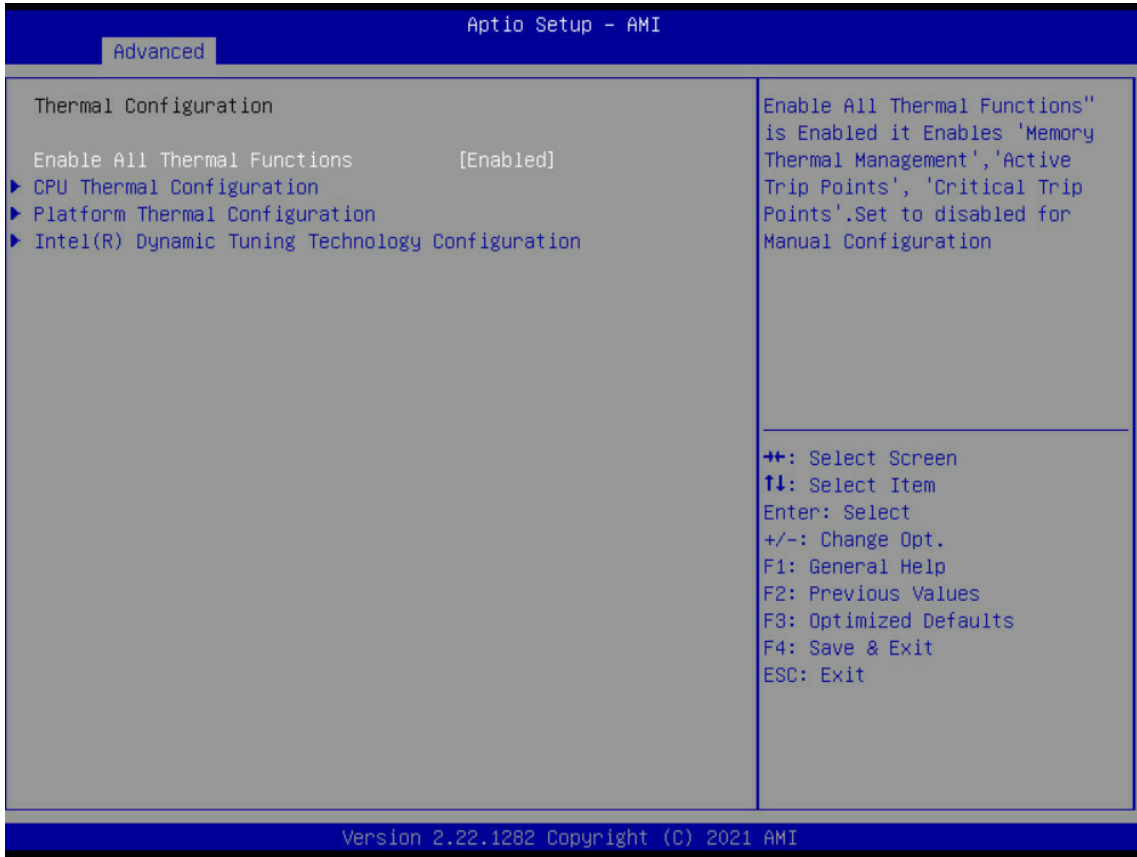
In MROM-less system force loading PTU regardless of ME request.

Enable
Disable

➤ **ME UEFI FW Health Status**

Information about ME UEFI FW Health Status.

4.4.6 Thermal Configuration



Enable All Thermal Functions

Enable All Thermal Functions" is Enabled it Enables 'Memory Thermal Management', 'Active Trip Points', 'Critical Trip Points'. Set to disabled for Manual Configuration.

Enable
Disable

➤ CPU Thermal Configuration

DTS SMM

Disabled: ACPI thermal management uses EC reported temperature values. Enabled: ACPI thermal management uses DTS SMM mechanism to obtain CPU temperature values. Out of Spec: ACPI Thermal Management uses EC reported temperature values and DTS SMM is used to handle Out of Spec condition.

Critical Temp Reporting (Out Of spec)
Enable
Disable

Tcc Activation Offset

Offset from factory set Tcc activation temprature at which the Thermal Control Circuit must be activated. Tcc will be activated at: Tcc Activation Temp - Tcc Activation Offset. Tcc Activation Offset range is 0 to 63.

0

Passive Trip Points

Disable Passive Trip Points.

Enable
Disable

Critical Trip Points

Disable Critical Trip Points.

Enable
Disable

PCH Temp Read

PCH Temperature Read enable.

Enable
Disable

CPU Energy Read

CPU Energy Read enable.

Enable
Disable

CPU Temp Read

CPU Temperature Read enable.

Enable
Disable

Alert Enable Lock

Lock all Alert enable settings.

Enable
Disable

CPU Temp

Fail Safe temp that EC will use if OS is hung.

72

CPU Fan Speed

Fan speed that EC will use if OS is hung.

65

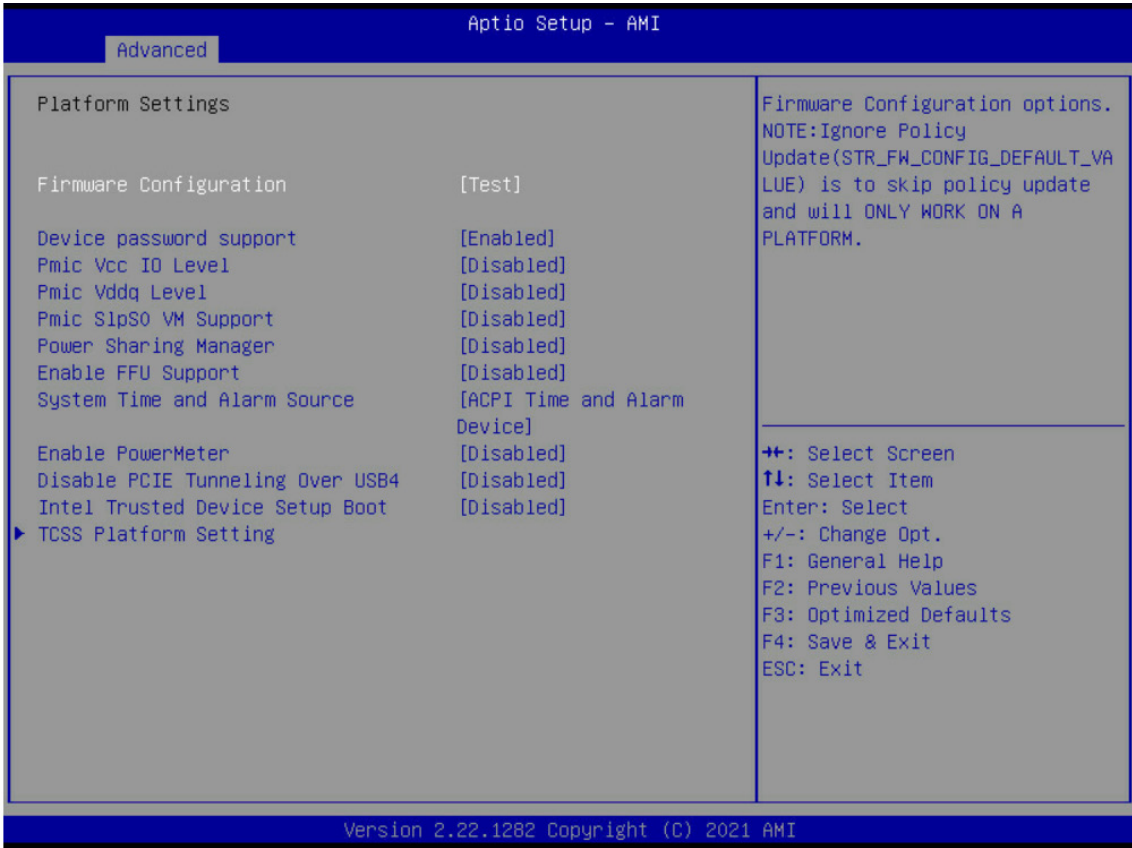
➤ **Intel Dynamic Tuning Technology Configuration**

Intel(R) Dynamic Tuning Technology

Enable/disable Intel Dynamic Platform Thermal Framework.

Enable
Disable

4.4.7 Platform Settings



Firmware Configuration

Firmware Configuration options. NOTE:Ignore Policy Update(STR_FW_CONFIG_DEFAULT_VALUE) is to skip policy update and will ONLY WORK ON A PLATFORM.

Ignore Policy Update
Production
Test

Device password support

Support device password feature.

Enable
Disable

Pmic Vcc IO Level

Select the Pmic Vcc IO Voltage Level.

0.850V	0.997V	1.071V
0.900V	1.023V	Disable
0.950V	1.05V	

Pmic Vddq Level

Select the Pmic Vddq Voltage Level.

0	3	6
1	4	7
2	5	Disable

HEBC value

HEBC value 32bit.

144371

Pmic SlpS0 VM Support

Support to auto check Primium PMIC and disable SlpS0 voltage.

Enable
Disable

Power Sharing Manager

Configure the PSM ACPI objects.

Enable
Disable

Enable FFU Support

Enables/disables FFU Support.

Enable
Disable

HID Event Filter Driver

Enables/disables HID Event Filter Driver interface to OS.

Enable
Disable

System Time and Alarm Source

Select source of system time and alarm functions. ACPI Time and Alarm (default, legacy RTC disabled) or Legacy RTC support only.

ACPI Time and Alarm Device
Legacy RTC

Enable PowerMeter

Enables Power Meter.

Enable
Disable

Disable PCIE Tunneling Over USB4

Setting this option disables retry PCIE Tunneling Over USB4.

Enable
Disable

Intel Trusted Device Setup Boot

Enables/Disables a Intel Trusted Device Setup Boot on the next boot.

Enable
Disable

➤ TCSS Platform Setting**Control Iommu Pre-boot Behavior**

Enable IOMMU in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)

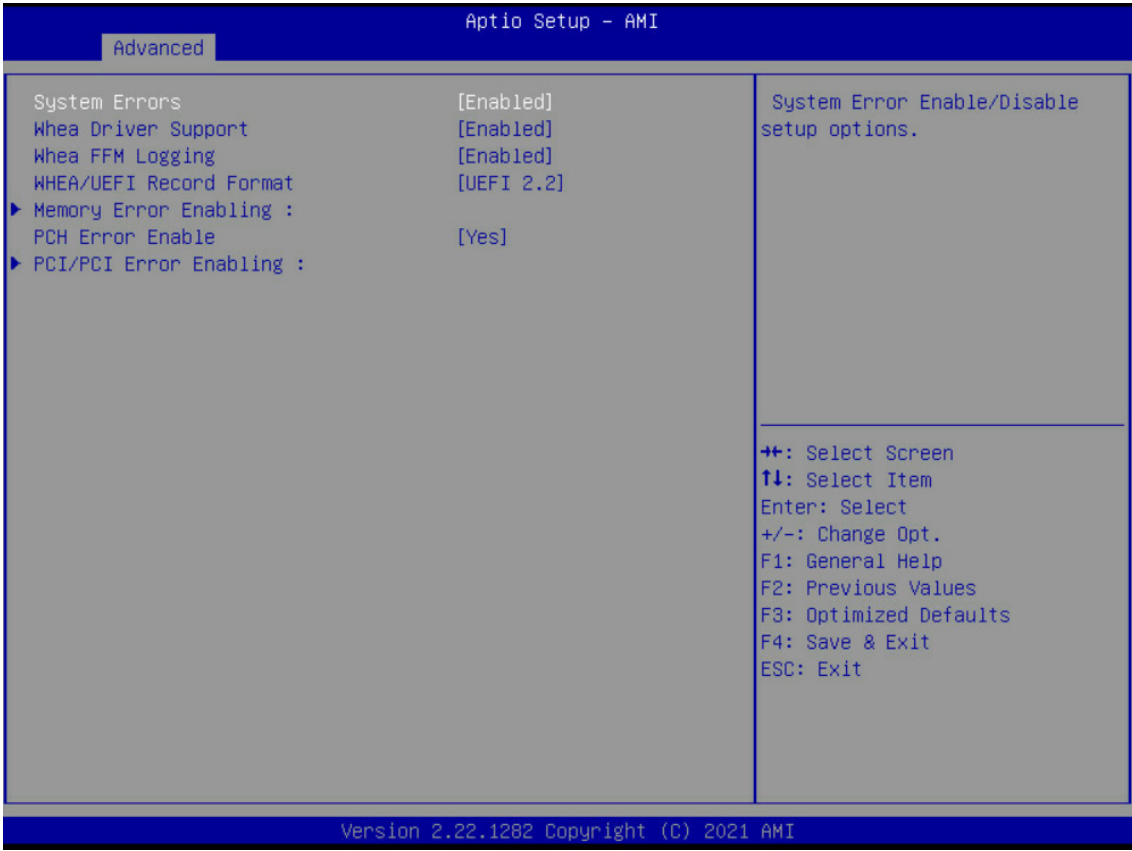
Enable IOMMU during boot
Disable IOMMU

USBC connector manager selection

Select UCSI or UCMC device in ACPI support based on configuration.

Enable UCSI Device
Enable UCMC Device
Disable

4.4.8 System Event Log



System Errors

System Error enable/disable setup options.

Enable
Disable

Whea Driver Support

Enables or Disables Whea Driver Support. This option may be not effective with some OS.

Enable
Disable

Whea FFM Logging

Enable/disable Whea FFM logging of errors.

Enable
Disable

WHEA/UEFI Record Format

Whea/UEFI FFM Error record format.

UEFI 2.2
UEFI 2.3.1

PCH Error Enable

Enables PCH Error.

Yes
No

➤ **Memory Error Enabling**

Memory corrected Error enabling

Memory corrected Error enabling.

Enable
Disable

Memory uncorrected Error enabling

Enable/ Disable Memory uncorrected Errors.

Enable
Disable

➤ **PCI/PCI Error Enabling**

PCI-Ex Error Enable

Enables PCI-Ex Error.

Yes
No

Fatal Error Enable

Enable & escalate fatal errors to error pins.

Enable
Disable

Uncorrected Error Enable

Enable & escalate Uncorrectable/Recoverable to error pins.

Enable
Disable

Corrected Error Enable

Enable & escalate Correctable Errors to error pins.

Enable
Disable

Enable SERR propagation

Enables SERR propagation.

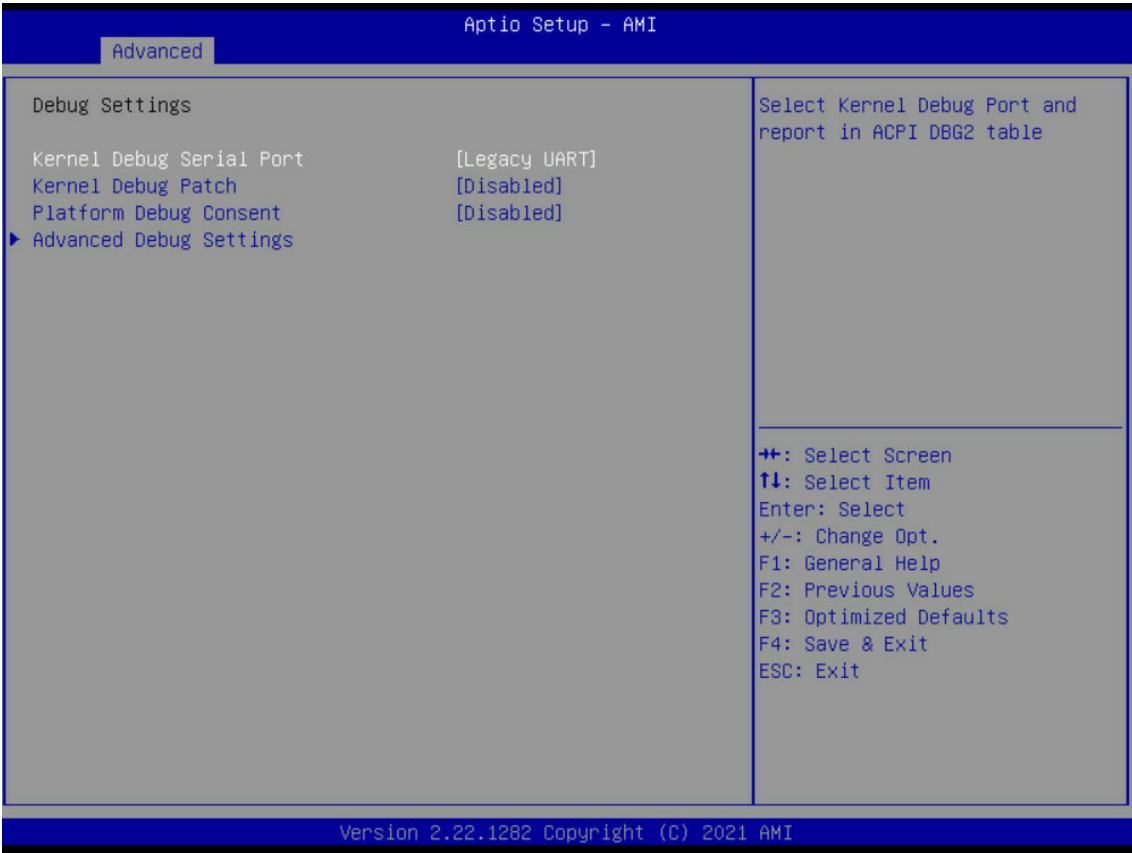
Yes
No

Enable PERR propagation

Enables SERR propagation.

Yes
No

4.4.9 Debug Settings



Kernel Debug Serial Port

Select Kernel Debug Port and report in ACPI DBG2 table.

Legacy UART
SERIALIO UART2

Kernel Debug Patch

Enable/disable Kernel Debug Patch.

Enable
Disable

Platform Debug Consent

To 'opt-in' for debug, please select 'Enabled' with the desired debug probe type. Enabling this BIOS option will override other debug-related BIOS options. Manual: Do not use Platform Debug Consent to override other debug-relevant policies, but the user must set each debug option manually, aimed at advanced users. Note: DCI OOB (aka BSSB) uses CCA probe.

Manual	Enable (USB3 DbC)
Enable (USB2 DbC)	Enable (XDP/MIPI60)
Enable (DCI OOB)	Disable
Enable (2 Wire DCI OOB)	

➤ Advanced Debug Settings

USB3 Type-C UFP2DFP Kernel/Platform Debug Support

This BIOS option enables kernel and platform debug for USB3 interface over a UFP Type-C receptacle, select 'No Change' will do nothing to UFP2DFP setting.

Enable
Disable
No Change

PCH Trace Hub Enable Mode

Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software. Note: If 'Host Debugger' is selected, Platform Debug Consent has to be ENABLED because DCI is one of the primary trace data output paths.

Target Debugger
Host Debugger
Disable

CPU Trace Hub Enable Mode

Select 'Host Debugger' if Trace Hub is used with host debugger tool or 'Target Debugger' if Trace Hub is used by target debugger software. Note: If 'Host Debugger' is selected, Platform Debug Consent has to be ENABLED because DCI is one of the primary trace data output paths.

Target Debugger
Host Debugger
Disable

CPU Run Control

Enable/disable CPU Run Control Support; No Change: Comply with HW value.

Enable
Disable
No Change

USB Overcurrent Override for DbC

This option overrides USB Over Current enablement state that USB OC will be disabled after enabling this option. Enable when DbC is used to avoid signaling conflicts.

Enable
Disable

Processor trace memory allocation

Disable or Select Processor trace memory region Size: from 4KB ~ 128MB.

4KB	256KB	16MB
8KB	512KB	32MB
16KB	1MB	64MB
32KB	2MB	128MB
64KB	4MB	Disable
128KB	8MB	

JTAG C10 Power Gate

When Enabled, JTAG is power gated in C10 state. When Disabled, keeps the JTAG power up during C10 and deeper power states for debug purpose.

Enable
Disable

Three Strike Counter

Enable/disable Three Strike Counter.

Enable
Disable

CrashLog Feature

The feature helps collecting crash data from PMC SSRAM.

Enable
Disable

CrashLog On All Reset

Option to invoke CrashLog collection on all reset.

Enable
Disable

CrashLog Clear Enable

Option to invoke CrashLog clear.

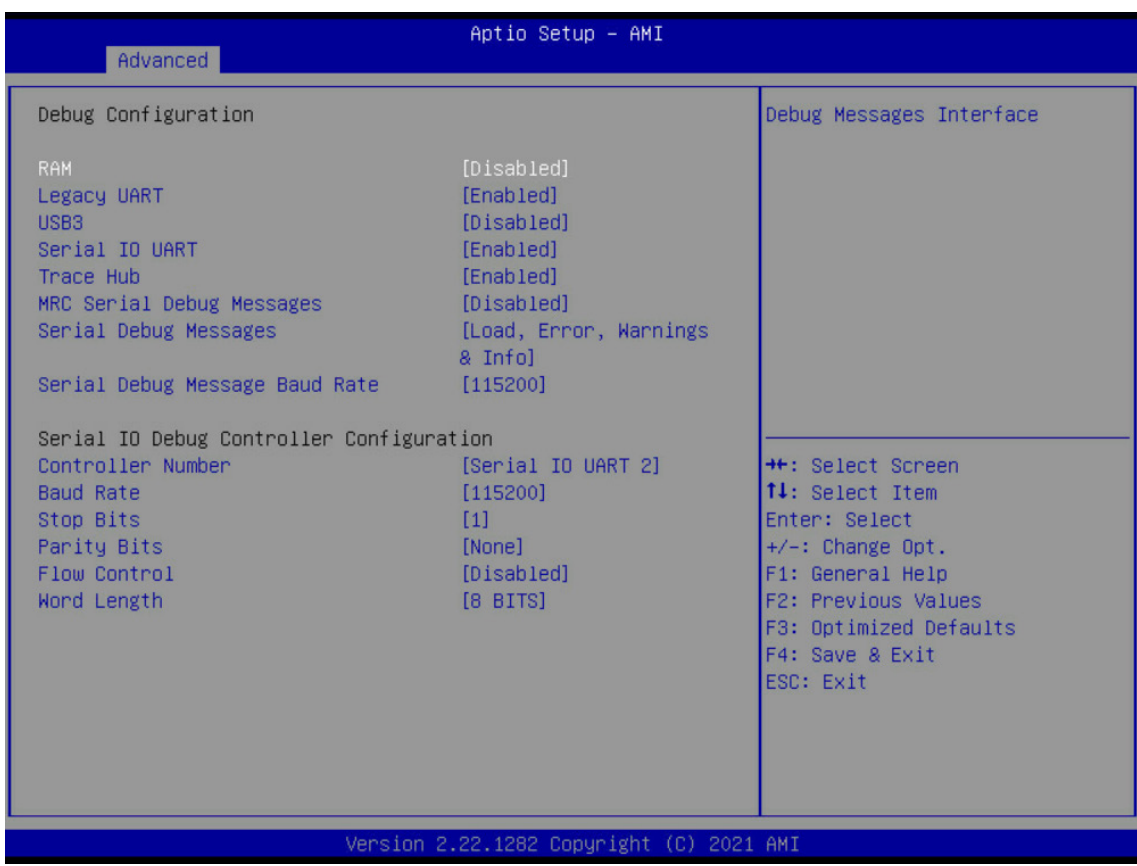
Enable
Disable

PMC Debug Message Enable

When Enabled, PMC HW will send debug messages to trace hub; When Disabled, PMC HW will never send debug meesages to trace hub. Noted: When Enabled, may not enter S0ix.

Enable
Disable

4.4.10 Debug Configuration



RAM
Debug Messages Interface.

Enable
Disable

Legacy UART
Debug Messages Interface.

Enable
Disable

USB3
Debug Messages Interface.

Enable
Disable

Serial IO UART
Debug Messages Interface.

Enable
Disable

Trace Hub
Debug Messages Interface

Enable
Disable

MRC Serial Debug Messages

Enable/disable MRC Serial Debug Messages.

Error Only	Load, Error, Warnings, Info & Event
Error & Warnings	Load, Error, Warnings, Info & Verbose
Load, Error, Warnings & Info	Disable

Serial Debug Messages

Enable/disable some Platform Serial Debug Messages.

Error Only	Load, Error, Warnings, Info & Event
Error & Warnings	Load, Error, Warnings, Info & Verbose
Load, Error, Warnings & Info	Disable

Serial Debug Message Baud Rate

Baud Rate for Serial Debug Messages.

9600	57600
19200	115200

Controller Number

Pch Integrated UART controller number.

Serial IO UART 0
Serial IO UART 1
Serial IO UART 2

Baud Rate

Serial IO transmission speed in baud [Bd] per second.

9600	460800	3000000
19200	921600	3686400
57600	1500000	6000000
115200	1843200	

Stop Bits

Number of stop bits. This is used to select the number of stop bits per character that the peripheral transmits and receives.

Default	1.5
1	2

Parity Bits

Enable and disable parity generation and detection in transmitted and received serial character.

Default	Even
None	Odd

Flow Control

Auto or None. Used to help for flow control using external IO pins with the pairing device.

Enable
Disable

Word Length

Select the number of data bits per character that the peripheral transmits and receives.

5 BITS	7 BITS
6 BITS	8 BITS

4.4.11 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.

TPM Clear
None

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

TPM 2.0 InterfaceType

Select the Communication Interface to TPM 2.0 Device.

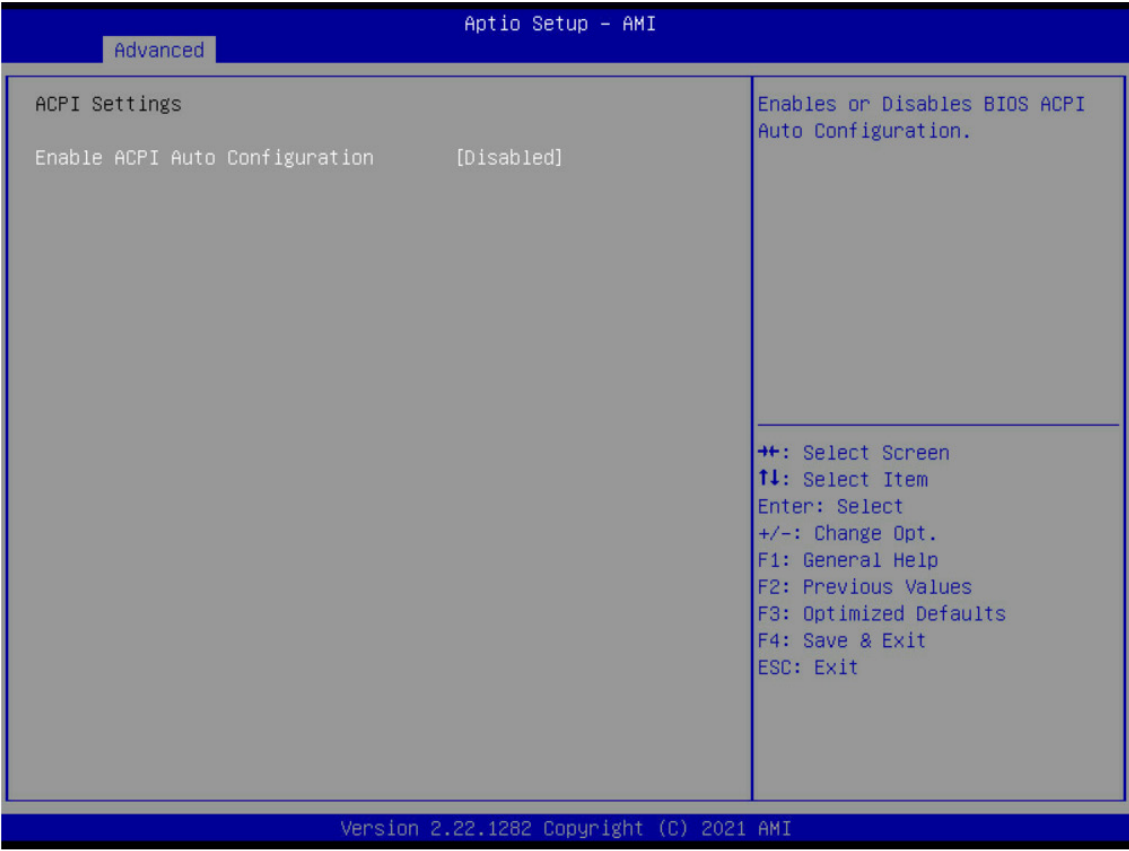
CRB
TIS

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.

Auto
TPM 1.2
TPM 2.0

4.4.12 ACPI Settings

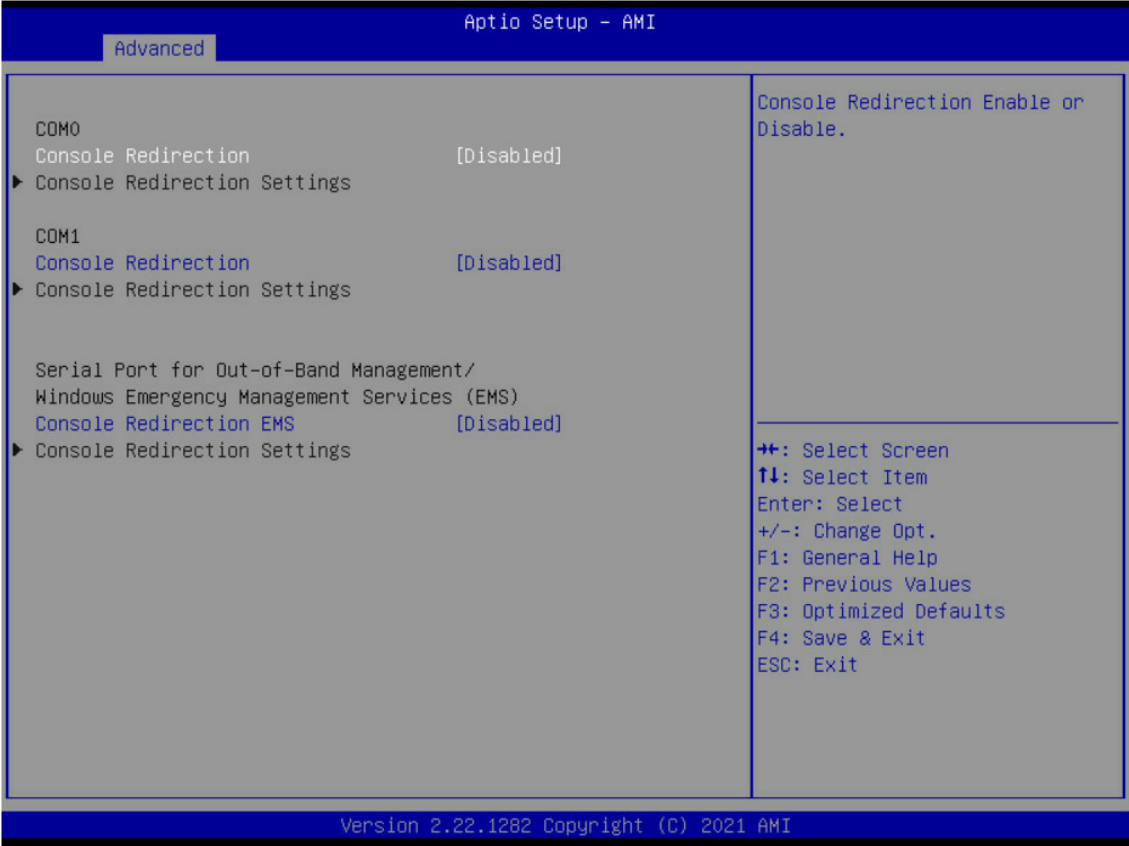


Enable ACPI Auto Configuration

Enables or Disables BIOS ACPI Auto Configuration.

Enable
Disable

4.4.13 Serial Port Console Redirection



Console Redirection

Console Redirection enable or disable.

Enable
Disable

Console Redirection EMS

Console Redirection enable or disable.

Enable
Disable

4.4.14 SIO Configuration



➤ **[*Active*] Serial Port 1/2**

Use This Device

Enable or disable this logical device.

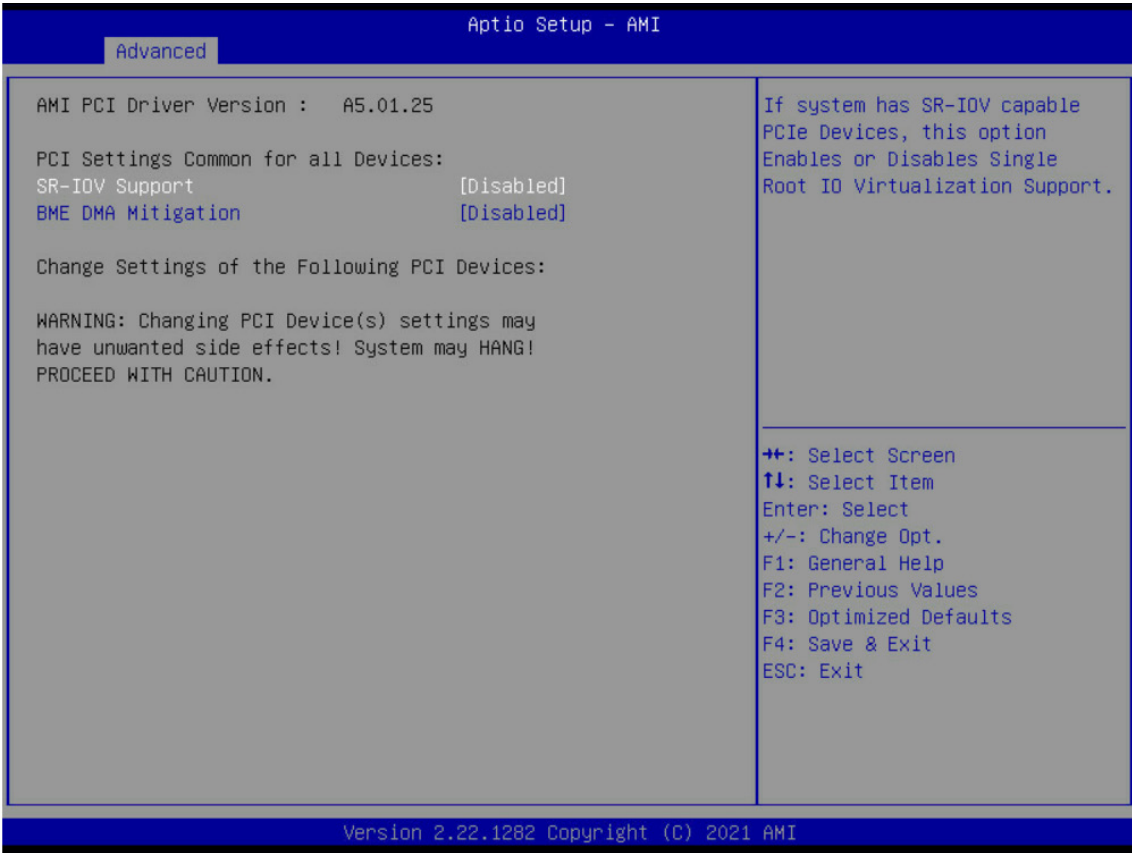
Enable
Disable

Possible

Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.

Use Automatic Setting;	I/O=3E8h; IRQ=4; DMA;
I/O=2F8h; IRQ=4; DMA;	I/O=3F8h; IRQ=4; DMA;
I/O=3F8h; IRQ=4; DMA;	I/O=3EF8h; IRQ=4; DMA;

4.4.15 PCI Subsystem Settings



SR-IOV Support

If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.

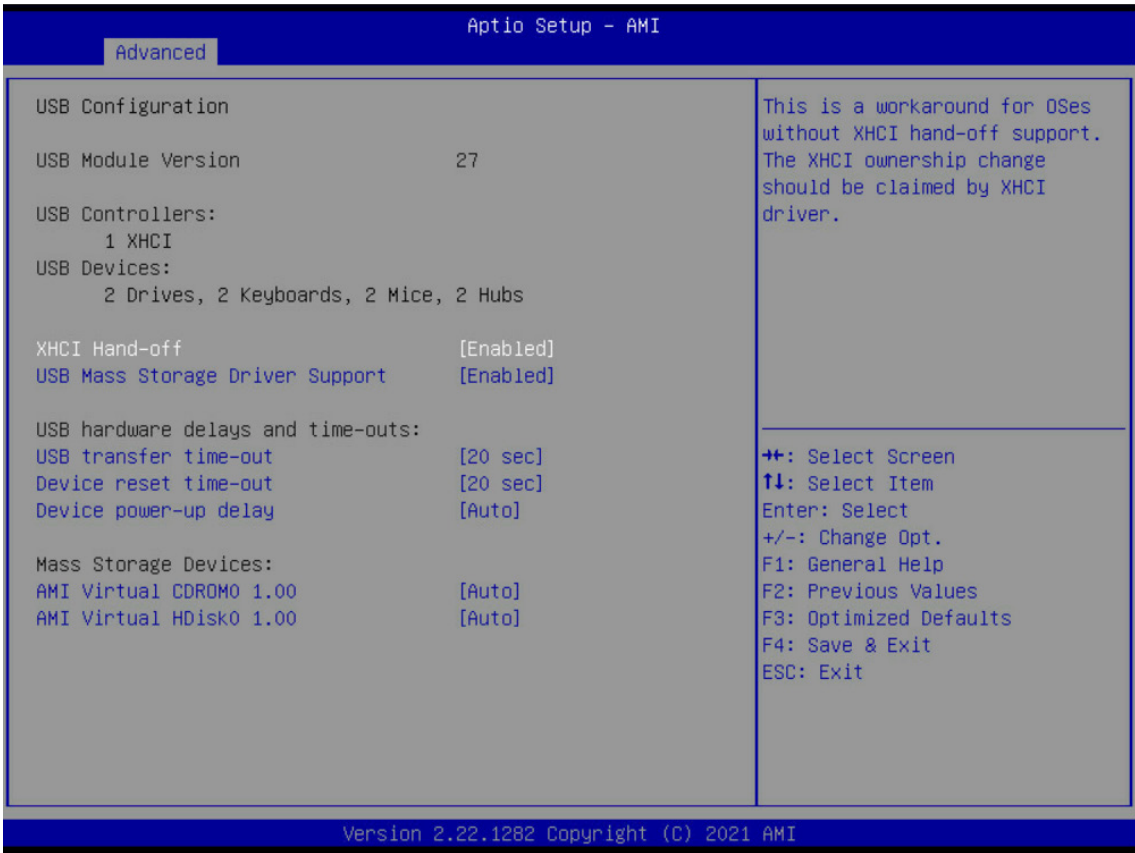
Enable
Disable

BME DMA Mitigation

Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked.

Enable
Disable

4.4.16 USB Configuration



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	10 sec
5 sec	20 sec

Device reset time-out

USB mass storage device Start Unit command time-out.

10 sec	30 sec
20 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 CDROM0 1.00

Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.

Auto	Hard Disk
Floppy	CD-ROM
Forced FDD	

AMI Virtual HDisk0 1.00

Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.

Auto	Hard Disk
Floppy	CD-ROM
Forced FDD	

4.4.17 Network Stack Configuration



Network Stack
Enable/disable UEFI Network Stack.

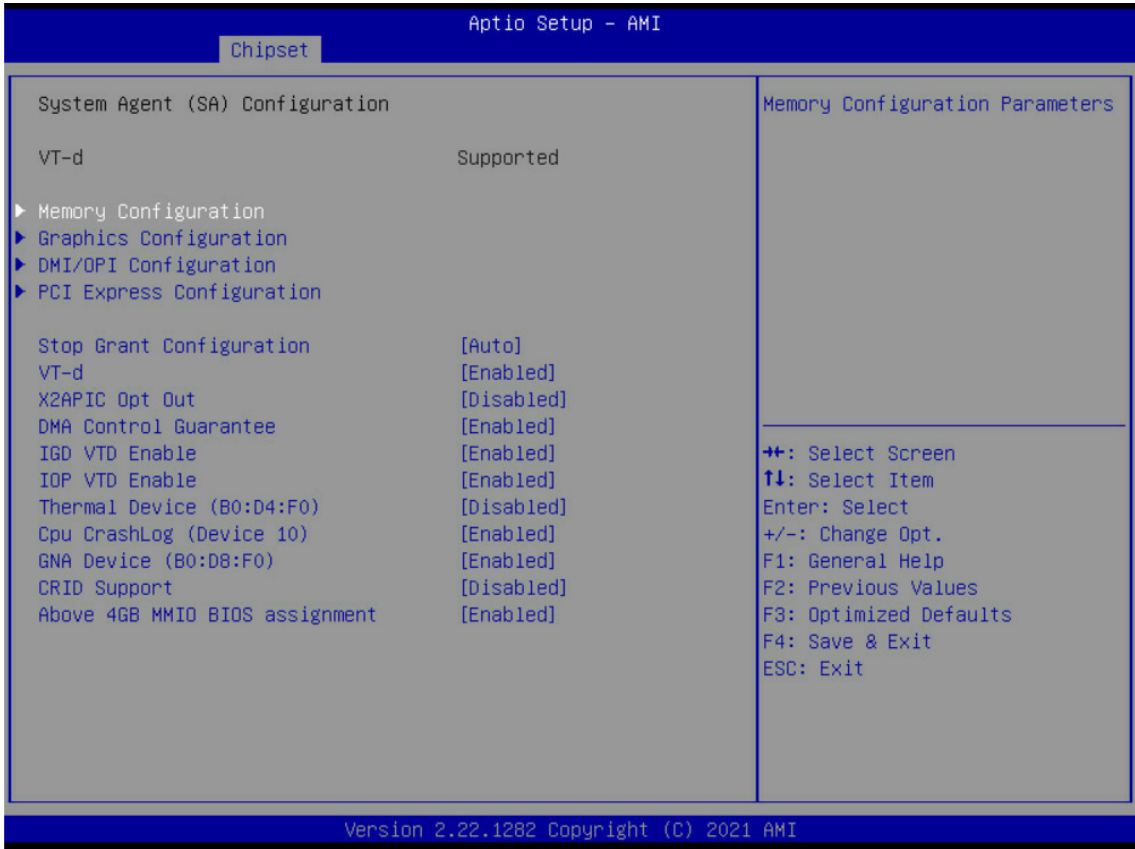
Enable
Disable

4.5 Chipset



- System Agent (SA) Configuration
- PCH-IO Configuration

4.5.1 System Agent (SA) Configuration



Stop Grant Configuration

Automatic/Manual stop grant configuration.

Auto
Manual

VT-d

VT-d capability.

Enable
Disable

X2APIC Opt Out

Enable/disable X2APIC_OPT_OUT bit.

Enable
Disable

DMA Control Guarantee

Enable/disable DMA_CONTROL_GUARANTEE bit.

Enable
Disable

IGD VTD Enable

Enable/disable IGD VTD.

Enable
Disable

IOP VTD Enable

Enable/disable IOP VTD.

Enable
Disable

Thermal Device (B0:D4:F0)

Enable/disable SA Thermal Device. Always enabled for ICL A0 stepping.

Enable
Disable

Cpu CrashLog (Device 10)

Enable/disable Cpu CrashLog Device.

Enable
Disable

GNA Device (B0:D8:F0)

Enable/disable SA GNA Device.

Enable
Disable

CRID Support

Enable/disable SA CRID and TCSS CRID control for Intel SIPP.

Enable
Disable

Above 4GB MMIO BIOS assignment

Enable/disable above 4GB MemoryMappedIO BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.

Enable
Disable

➤ Memory Configuration**MRC ULT Safe Config**

MRC ULT Safe Config for PO.

Enable
Disable

Safe Mode Support

Safe Mode enable support. Option will be used for changes/WAs that may affect an stable MRC.

Enable
Disable

Maximum Memory Frequency

Maximum Memory Frequency in Mhz. Must divide by 133 or 100 according to the refclk. In Gear2 must divide by 266 or 200. Lowest Gear2 speed is 2133.

Auto	1867	2667
1200	2000	2800
1333	2133	2933
1400	2200	3000
1600	2400	3200
1800	2600	

HOB Buffer Size

Size to set HOB Buffer.

Auto	1KB
1B	Max (assuming 63KB total HOB size)

ECC Support

Enable/disable DDR Ecc Support.

Enable
Disable

Max TOLUD

Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller.

Dynamic	1.75 GB	2.75 GB
1 GB	2 GB	3 GB
1.25 GB	2.25 GB	3.25 GB
1.5 GB	2.5 GB	3.5 GB

DDR Speed Control

DDR Frequency and Gear1 / Gear2 control for all SAGV points.

Auto
Manual

Retrain on Fast Fail

Restart MRC in Cold mode if SW MemTest fails during Fast flow. Default = Enabled.

Enable
Disable

DDR4_1DPC

DDR4 1DPC performance feature for 2R DIMMs. Can be enabled on DIMM0 or DIMM1 only, or on both.

Enabled on DIMM0 only
Enabled on DIMM1 only
Enable

Enable RH Prevention

Actively prevent Row Hammer.

Enable
Disable

Exit On Failure (MRC)

Exit On Failure for MRC training steps.

Enable
Disable

Ch Hash Support

Enable/disable Channel Hash Support. NOTE: ONLY if Memory interleaved Mode.

Enable
Disable

Ch Hash Mask

Set the BIT(s) to be included in the XOR function. NOTE BIT mask corresponds to BITS [19:6].

12492

Ch Hash Interleaved Bit

Select the BIT to be used for Channel Interleaved mode. NOTE: BIT7 will interlave the channels at a 2 cacheline granularity, BIT8 at 4 and BIT9 at 8.

BIT6	BIT10
BIT7	BIT11
BIT8	BIT12
BIT9	BIT13

Extended Bank Hashing

Extended Bank Hashing.

Enable
Disable

Per Bank Refresh

Enables/disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR3, LPDDR4.

Enable
Disable

Power Down Mode

CKE Power Down Mode Control.

Auto	APD
No Power Down	PPD-DLLoff

Pwr Down Idle Timer

The minimum value should = to the worst case Roundtrip delay + Burst_Length. 0 means AUTO: 64 for ULX/ULT, 128 for DT/Halo.

0

Memory Scrambler

Enable/disable Memory Scrambler support.

Enable
Disable

Force ColdReset

Force ColdReset OR Choose MrcColdBoot mode, when Coldboot is required during MRC execution.

Note: If ME 5.0MB is present, ForceColdReset is required!

Enable
Disable

Channel 0/1 Control

Enable/disable Channel 0/1.

Enable
Disable

Force Single Rank

When enabled, only Rank 0 will be used in each DIMM.

Enable
Disable

Memory Remap

Enable/disable Memory Remap above 4GB.

Enable
Disable

Time Measure

Enable/disable printing of the time it takes to execute MRC.

Enable
Disable

Fast Boot

Enable/disable fast path thru the MRC.

Enable
Disable

Train On Warm boot

Enable/disable training on warm boot.

Enable
Disable

Rank Margin Tool Per Task

Enables/Disables RMT running at every major training step.

Enable
Disable

Training Tracing

Enables/Disables printing of the current trained state at every major training step.

Enable
Disable

Lpddr Mem WL Set

Only applicable to LPDDR, Memory Write Latency Set selection (A is default, B will be used if memory devices support it).

Set A
Set B

BDAT Memory Test Type

Indicates the type of Memory Training data to populate into the BDAT ACPI table.

Rank Margin Tool Rank
Rank Margin Tool Bit
Margin 2D

Rank Margin Tool Loop Count

Specifies the Loop Count to be used during Rank Margin Tool Testing. 0 - AUTO.

0

Low Supply for LPDDR4 Data

Low Supply for LPDDR4 Data.

Enable
Disable

Low Supply for LPDDR4 Clock/Command/Control

Low Supply for LPDDR4 Clock/Command/Control.

Enable
Disable

Memory Test on Warm Boot

Enable Or Disable Base Memory Test Run on Warm Boot.

Enable
Disable

➤➤ **Memory Thermal Configuration**

Memory Thermal Management

Enable/disable Memory Thermal Management.

Enable
Disable

➤➤➤ Memory Power and Thermal Throttling

DDR PowerDown and idle counter

BIOS: BIOS is in control of DDR CKE mode and idle timer value. PCODE: pcode will manage the modes.

PCODE
BIOS

For LPDDR Only: DDR PowerDown and idle counter

For LPDDR Only: BIOS: BIOS is in control of DDR CKE mode and idle timer value. PCODE: pcode will manage the modes.

PCODE
BIOS

REFRESH_2X_MODE

0- Disabled 1-iMC enables 2xRef when Warm and Hot 2- iMC enables 2xRef when Hot.

Enable for WARM or HOT
Enable HOT only
Disable

LPDDR Thermal Sensor

When enabled, MC uses MR4 to read LPDDR thermal sensors.

Enable
Disable

SelfRefresh Enable

Enable, Disable(Enable= Def).

Enable
Disable

SelfRefresh IdleTimer

Self Refresh idle timer in nCK units: 0 = Auto (default), or value in range [512 .. 65535].

0

Throttler CKEMin Defeature

On, Off.

Enable
Disable

Throttler CKEMin Timer

Timer value for CKEMin, range[255;0]. Req'd min of SC_ROUND_T + BYTE_LENGTH (4).

48

➤➤➤➤ DRAM Power Meter

Use user provided power weights, scale factor, and channel power floor values

Enabled: User provided power weights, scale factor, and channel power floor values are used.

Disabled: BIOS sets power weights, scale factor, and channel power floor values based on DIMMs present in system.

Enable
Disable

Energy Scale Factor

range[7;0]= [7.3;931.3]in pJ, (3= 116pJ Def).

4

Idle Energy Ch0Dimm0/Ch0Dimm1/Ch1Dimm0/Ch1Dimm1

Idle Energy Consumed for 1 clk w/dimm idle/cke on, range[63;0],(10= Def).

10

PowerDown Energy Ch0Dimm0/Ch0Dimm1/Ch1Dimm0/Ch1Dimm1

PowerDown Energy Consumed w/dimm idle/cke off, range[63;0],(6= Def).

6

Activate Energy Ch0Dimm0/Ch0Dimm1/Ch1Dimm0/Ch1Dimm1

Activate Energy Contribution, range[255;0],(172= Def).

172

Read Energy Ch0Dimm0/Ch0Dimm1/Ch1Dimm0/Ch1Dimm1

Read Energy Contribution, range[255;0],(212= Def).

212

Write Energy Ch0Dimm0/Ch0Dimm1/Ch1Dimm0/Ch1Dimm1

Write Energy Contribution, range[255;0],(221= Def).

221

➤➤➤➤ Memory Thermal Report

Lock Thermal Management Registers

Enabled: lock several PCU registers related to DDR power/thermal management.

Enable
Disable

Extern Therm Status

Enabled: The value from EXTTS is used Disabled: Pcode ignores the EXTTS.

Enable
Disable

Closed Loop Therm Manage

Enable/disable: Closed Loop Therm Manage (CLTM).

Enable
Disable

Warm Threshold Ch0 Dimm0/ Ch0 Dimm1/ Ch1 Dimm0/ Ch1 Dimm1

range[255;0]=[31.875;0] in W for OLTm, [127.5;0] in C for CLTM.

255

Hot Threshold Ch0 Dimm0/ Ch0 Dimm1/ Ch1 Dimm0/ Ch1 Dimm1

range[255;0]=[31.875;0] in W for OLTm, [127.5;0] in C for CLTM.

255

Warm Budget Ch0 Dimm0/ Ch0 Dimm1/ Ch1 Dimm0/ Ch1 Dimm1
range[255;0]=[31.875;0] in W for OLTm, [127.5;0] in C for CLTM.

Hot Budget Ch0 Dimm0/ Ch0 Dimm1/ Ch1 Dimm0/ Ch1 Dimm1
range[255;0]=[31.875;0] in W for OLTm, [127.5;0] in C for CLTM.

➤➤➤➤ Memory RAPL

Rapl Power Floor Ch0/1

Power budget, range[255;0], (0= 5.3W Def).

RAPL PL Lock

Enable= lock Rapl Limit register , Disable(Disable= Def).

RAPL PL 1/2 enable

Enable= enable, Disable(Disable= Def).

RAPL PL 1/2 Power

range[0;2¹⁴-1]= [2047.875;0]in W, (0= Def).

RAPL PL 1/2 WindowX

Power PL 1 time window X value, $(1/1024) * (1 + (x/4)) * (2^y)$ (0=Def).

RAPL PL 1/2 WindowY

Power PL 1 time window Y value, $(1/1024) * (1 + (x/4)) * (2^y)$ (0=Def).

➤➤ Memory Training Algorithms

Early Command Training

Early Command Training.

SenseAmp Offset Training

SenseAmp Offset Training.

Early ReadMPR Timing Centering 2D

Read MPR Training

Read MPR Training.

Receive Enable Training

Receive Enable Training.

Enable
Disable

Jedec Write Leveling

Jedec Write Leveling.

Enable
Disable

LPDDR4 Write DQ DQS Retraining

LPDDR4 Write DQ DQS Retraining.

Enable
Disable

Early Write Time Centering 2D

Early Write Time Centering 2D.

Enable
Disable

Early Read Time Centering 2D

Enable
Disable

Write Timing Centering 1D

Write Timing Centering 1D.

Enable
Disable

Write Voltage Centering 1D

Enable
Disable

Read Timing Centering 1D

Read Timing Centering 1D.

Enable
Disable

Dimm ODT Training*

Dimm On-Die Termination Training.

Enable
Disable

Max RTT_WR

Caps the maximum RTT_WR in power training.

ODT Off
120 Ohms

DIMM RON Training*

DIMM RON Training.

Enable
Disable

Write Drive Strength/Equalization 2D*

Enable
Disable

Write Slew Rate Training*

Write Slew Rate Training.

Enable
Disable

Read ODT Training*

Read On-Die Termination Training.

Enable
Disable

Read Equalization Training*

Read Equalization Training.

Enable
Disable

Read Amplifier Training*

Read Amplifier Training.

Enable
Disable

Write Timing Centering 2D

Write Dq-Dqs Timing Centering 2D.

Enable
Disable

Read Timing Centering 2D

Read Dq-Dqs Timing Centering 2D.

Enable
Disable

Command Voltage Centering

Command Voltage Centering.

Enable
Disable

Write Voltage Centering 2D

Write Voltage Centering 2D.

Enable
Disable

Late Command Training

Late Command Training.

Enable
Disable

Round Trip Latency

Round Trip Latency Training.

Enable
Disable

Turn Around Timing Training

Turn Around Timing Training.

Enable
Disable

Rank Margin Tool

Rank Margin Tool Training.

Enable
Disable

Rank Margin Tool Per Bit

Rank Margin Tool Per Bit Training.

Enable
Disable

Margin Check Limit

Checks Margin to Limit to see if next boot memory needs to be retrain.

L1	Both
L2	Disable

Margin Limit Check L2

L2 check threshold is scale of L1 check. Ex. 200 is 2 x L1 Check.

100

Memory Test

Memory Test Training.

Enable
Disable

DIMM SPD Alias Test

Test to determine if the SPD has been corrupted to cause memory aliasing.

Enable
Disable

Receive Enable Centering 1D

Receive Enable Centering 1D.

Enable
Disable

Retrain Margin Check

Retrain Margin Check.

Enable
Disable

Write Drive Strength Up/Dn independently

Write Drive Strength Up/Dn independently.

Enable
Disable

Command Slew Rate Training

Command Slew Rate Training.

Enable
Disable

Command Drive Strength and Equalization

Command Drive Strength and Equalization.

Enable
Disable

Command Normalization

Command Normalization.

Enable
Disable

Early DQ Write Drive Strength and Equalization Training

Early DQ Write Drive Strength and Equalization Training.

Enable
Disable

Read Voltage Centering 1D

Read Voltage Centering 1D.

Enable
Disable

Dimm ODT CA Training

Dimm ODT CA Training.

Enable
Disable

Duty Cycle Correction

Duty Cycle Correction.

Enable
Disable

DQ DFE Training

DQ DFE Training.

Enable
Disable

➤➤ **Memory**

Realtime Memory Timing

Enable/disable realtime memory timings. When enabled, the system will allow performing realtime memory timing changes after MRC_DONE.

Enable
Disable

Memory profile

Select DIMM timing profile. The below values start with the currently running values and don't auto populate.

Default profile
Custom profile

DIIBwEn[1]

DIIBwEn[1], for 1333 (0..7).

1

DIIBwEn[2]

DIIBwEn[2], for 1600 (0..7).

2

DIIBwEn[3]

DIIBwEn[3], for 1867 and up (0..7).

2

➤ Graphics Configuration

Skip Scanning of External Gfx Card

If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports.

Enable
Disable

Primary Display

Select which of IGFX/PEG/PCI Graphics device should be Primary Display Or select HG for Hybrid Gfx.

Auto	PCI
IGFX	HG

Select PCIE Card

Select the card used on the platform. Auto: Skip GPIO based Power Enable to dGPU Elk Creek 4: DGPU Power Enable = ActiveLow PEG Eval: DGPU Power Enable = ActiveHigh.

Auto
Elk Creek 4
PEG Eval

HG Delay After Power Enable

Delay in milli-seconds after power enable.

300

HG Delay After Hold Reset

Delay in milli-seconds after hold reset.

100

Internal Graphics

Keep IGFX enabled based on the setup options.

Auto
Enable
Disable

GTT Size

Select the GTT Size.

2 MB
4 MB
8 MB

Aperture Size

Select the Aperture Size. Note : Above 4GB MMIO BIOS assignment is automatically enabled when selecting 2048MB aperture. To use this feature, please disable CSM Support.

128 MB	512 MB
256 MB	1024 MB

PSMI SUPPORT

PSMI enable/disable.

Enable
Disable

DVMT Pre-Allocated

Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

0M	28M	52M
4M	32M/F7	56M
8M	32M	60M
12M	36M	64M
16M	40M	96M
20M	44M	128M
24M	48M	160M

DVMT Total Gfx Mem

Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics Device.

128M
256M
MAX

DFD Restore

Select Display memory map programming for DFD Restore.

Enable
Disable

Intel Graphics Pei Display Peim

Enable/disable Pei (Early) Display.

Enable
Disable

VDD Enable

Enable/Disable forcing of VDD in the BIOS.

Enable
Disable

Configure GT for use

Enable/disable GT configuration in BIOS.

Enable
Disable

RC1p Support

Enable/disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met.

Enable
Disable

PAVP Enable

Enable/disable PAVP.

Enable
Disable

Cdynmax Clamping Enable

Enable/disable Cdynmax Clamping.

Enable
Disable

Cd Clock Frequency

Select the highest Cd Clock frequency supported by the platform.

192 Mhz	648 Mhz
312 Mhz	Max CdClock freq based on Reference Clk
552 Mhz	

Skip Full CD Clock Init

Enabled: Skip Full CD clock initializaton. Disabled: Initialize the full CD clock if not initialized by Gfx PEIM.

Enable
Disable

IUER Button Enable

Enable/disable IUER Button Functionality.

Enable
Disable

➤➤ External Gfx Card Pimary Display Configuration

External Gfx Card Pimary Display Configuration.

➤➤ Intel(R) Ultrabook Event Support

➤ DMI/OPI Configuration

DMI Max Link Speed

Set DMI Speed Gen1/Gen2/Gen3.

Gen1
Gen2
Gen3

DMI Gen3 Eq Phase 2

Perform Gen3 Equalization Phase 2.

Auto
Enable
Disable

DMI Gen3 Eq Phase 3 Method

Select Method for Gen3 Equalization Phase 3.

Auto	Static Equalization
Adaptive Hardware Equalization	Disable
Adaptive Software Equalization	

Program Static Phase1 Eq

Program Phase1 Presets/CTLEp.

Enable
Disable

DMI De-emphasis Control

Configure the De-emphasis control on DMI.

-6 dB
-3.5 dB

DMI Gen3 ASPM

DMI Gen3 ASPM Support.

Auto	ASPM L0sL1
ASPM L0s	Disable
ASPM L1	

CDR Relock for CPU DMI

Enable/disable CDR Relock.

Enable
Disable

➤➤ Gen3 Root Port Preset value for each Lane

Lane 0-7

Value for Lane 0-7.

➤➤ Gen 3 Endpoint Preset value for each Lane

Lane 0-7

Value for Lane 0-7.

➤➤ Gen3 Endpoint Hint value for each Lane

Lane 0-7

Value for Lane 0-7.

➤➤ Gen3 RxCTLE Control

Bundle0-3

Gen3 RxCTLE setting for Bundle0 (Lane0, Lane1)/Bundle1 (Lane2, Lane3)/Bundle2 (Lane4, Lane5)/Bundle3 (Lane6, Lane7).

➤➤ DMI Gen3 ASPM

DMI Gen3 ASPM

DMI Gen3 ASPM Support.

Auto	ASPM L0sL1
ASPM L0s	Disable
ASPM L1	

DMI Gen3 L1 Exit Latency

DMI Gen3 L1 Exit Latency.

➤ PCI Express Configuration

PCI Express Clock Gating

PCI Express Clock Gating enable/disable for each root port.

Fia Programming

Load Fia Configuration if Enabled for each root port.

PCI Express Power Gating

PCI Express Power Gating enable/disable for each root port.

Compliance Test Mode

Enable when using Compliance Load Board.

PCIe function swap

When Disabled, prevents PCIe rootport function swap. If any function other than 0th is enabled, 0th will become visible.

Enable
Disable

CDR Relock for PEG60

Enable/disable CDR Relock.

Enable
Disable

CDR Relock for PEG10

Enable/disable CDR Relock.

Enable
Disable

Assertion on Link Down GPIOs

GPIO Assertion on Link Down.

Enable
Disable

Enable ClockReq Messaging

Enable or disable ClockReq Messaging.

Enable
Disable

PCI Express Slot Selection

Select the PCIe M2 or CEMx4 slot.

M2
CEMx4 slot

➤➤ PCI Express Gen3 Eq Lanes**PCIE1-4 Cm**

6

PCIE1-4 Cp

2

➤➤ PCI Express Root Port 1/2/3/4**PCI Express Root Port 1**

Control the PCI Express Root Port.

Enable
Disable

Connection Type

Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.

Built-in
Slot

ASPM

Set the ASPM Level: Force L0s - Force all links to L0s State AUTO - BIOS auto configure DISABLE - Disables ASPM.

L0s	L0sL1
L1	Disable

L1 Substates

PCI Express L1 Substates settings. L1SS cannot be enabled when CLKREQMSG is disabled.

L1.1
L1.1 & L1.2
Disable

Gen3 Eq Phase3 Method

PCIe Gen3 Equalization Phase 3 Method.

Hardware
Static Coeff

Gen4 Eq Phase3 Method

PCIe Gen3 Equalization Phase 3 Method.

Hardware
Static Coeff

ACS

Enable/disable Access Control Services Extended Capability.

Enable
Disable

PTM

Enable/disable Precision Time Measurement

Enable
Disable

DPC

Enable/disable Downstream Port Containment.

Enable
Disable

FOM Scoreboard Control Policy

Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS.

Auto	Gen4
Gen3	Gen3/Gen4

VC

Enable/disable Virtual Channel.

Enable
Disable

Multi-VC

Enable/disable Multi Virtual Channel.

Enable
Disable

EDPC

Enable/disable Rootport extensions for Downstream Port Containment.

Enable
Disable

URR

PCI Express Unsupported Request Reporting enable/disable.

Enable
Disable

FER

PCI Express Device Fatal Error Reporting enable/disable.

Enable
Disable

NFER

PCI Express Device Non-Fatal Error Reporting enable/disable.

Enable
Disable

CER

PCI Express Device Correctable Error Reporting enable/disable.

Enable
Disable

CTO

PCI Express Completion Timer TO enable/disable.

Enable
Disable

SEFE

Root PCI Express System Error on Fatal Error enable/disable.

Enable
Disable

SENFE

Root PCI Express System Error on Non-Fatal Error enable/disable.

Enable
Disable

SECE

Root PCI Express System Error on Correctable Error enable/disable.

Enable
Disable

PME SCI

PCI Express PME SCI enable/disable.

Enable
Disable

Advanced Error Reporting

Advanced Error Reporting enable/disable.

Enable
Disable

PCIe Speed

Configure PCIe Speed.

Auto	Gen3
Gen1	Gen4
Gen2	

Transmitter Half Swing

Transmitter Half Swing enable/disable.

Enable
Disable

Detect Timeout

The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.

0

P2P Support

Program P2P Support Registers according to setup option.

Enable
Disable

LTR

SA PCIE Latency Reporting enable/disable.

Enable
Disable

Snoop Latency Override

Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.

Auto
Manual
Disable

Non Snoop Latency Override

Non Snoop Latency Override for SA PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.

Auto
Manual
Disable

Force LTR Override

Force LTR Override for SA PCIE. Disabled: LTR override values will not be forced. Enable: LTR override values will be forced and LTR messages from the device will be ignored.

Enable
Disable

LTR Lock

PCIE LTR Configuration Lock.

Enable
Disable

UPTP

Upstream Port Transmitter Preset.

7

DPTP

Downstream Port Transmitter Preset.

7

UPTP

Upstream Port Transmitter Preset.

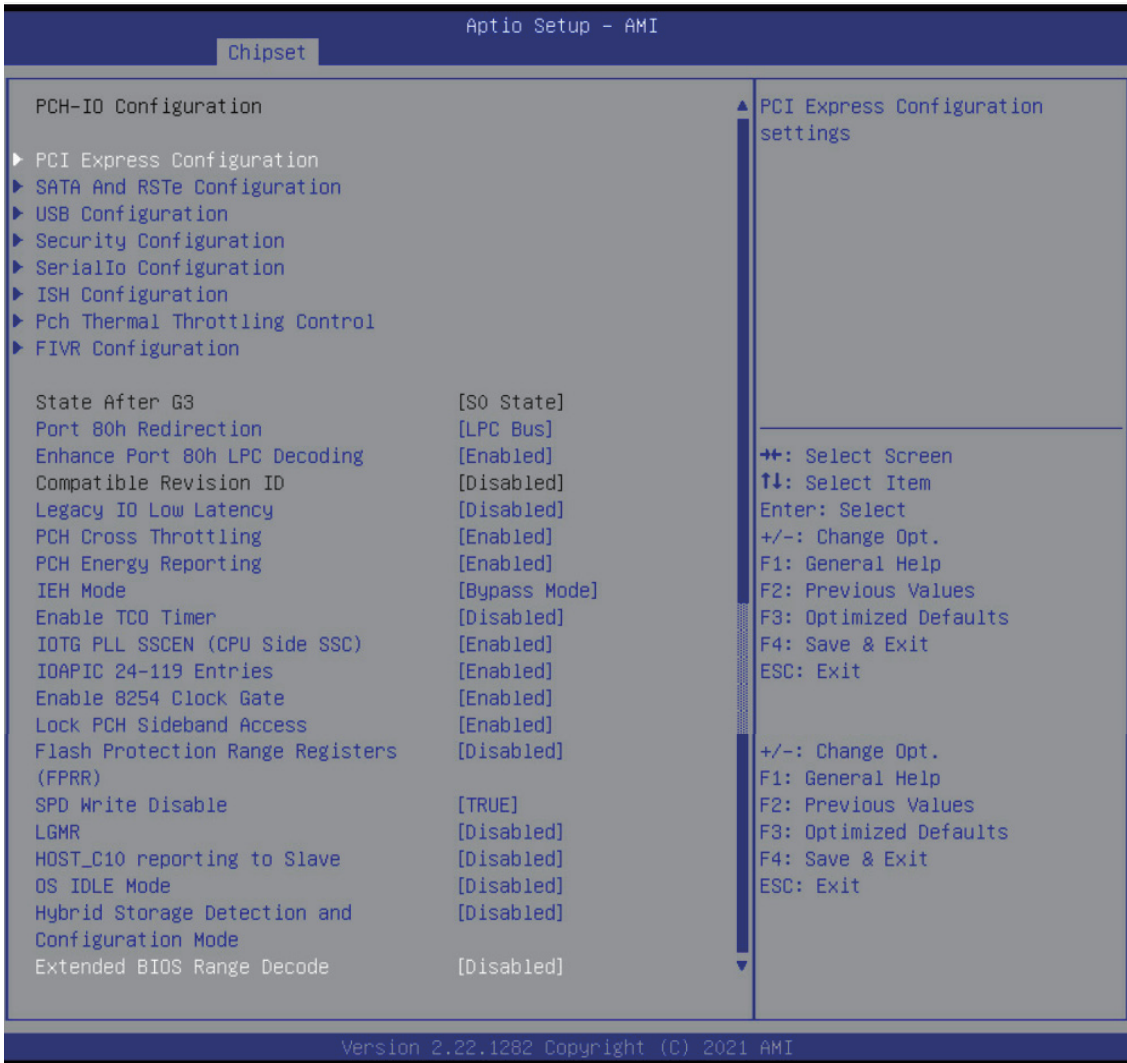
8

DPTP

Downstream Port Transmitter Preset.

9

4.5.2 PCH-IO Configuration



State After G3

Specify what state to go to when power is re-applied after a power failure (G3 state).

S0 State
S5 State

Leave power state unchanged

Port 80h Redirection

Control where the Port 80h cycles are sent.

LPC Bus
PCIE Bus

Enhance Port 80h LPC Decoding

Support the word/dword decoding of port 80h behind LPC.

Enable
Disable

Compatible Revision ID

Enable/disable the PCH Compatible Revision ID feature.

Enable
Disable

Legacy IO Low Latency

Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.

Enable
Disable

PCH Cross Throttling

Enable/disable the PCH Cross Throttling feature. Only ULT support this feature.

Enable
Disable

PCH Energy Reporting

Enable Energy Report. MUST set it as ENABLED. This is only for test purpose.

Enable
Disable

IEH Mode

Enable/Bypass IEH Mode.

Bypass Mode
Enable

Enable TCO Timer

Enable/disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.

Enable
Disable

IOTG PLL SSCEN (CPU Side SSC)

Enable/disable IOTG PLL SSCEN.

Enable
Disable

IOAPIC 24-119 Entries

Enables/Disables IOAPIC 24-119 Entries. IRQ24-119 may be used by PCH devices. Disabling those interrupts may cause certain devices failure.

Enable
Disable

Enable 8254 Clock Gate

Enables/Disables 8254 clock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is able to disable this policy and set 8254CGE in late phase.

Enable
Enabled In Runtime and S3 Resume
Disable

Lock PCH Sideband Access

Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAI is set.

Enable
Disable

Flash Protection Range Registers (FPRR)

Enable Flash Protection Range Registers.

Enable
Disable

SPD Write Disable

Enable/Disable setting SPD Write Disable.

True
False

LGMR

64KB memory block for LGMR (LPC Memory Range Decode).

Enable
Disable

HOST_C10 reporting to Slave

This option enables HOST_C10 reporting to Slave via eSPI Virtual Wire.

Enable
Disable

OS IDLE Mode

Enable/Disable OS Idle Mode Feature.

Enable
Disable

Hybrid Storage Detection and Configuration Mode

Select Hybrid Storage Detection and Configuration Mode

Dynamic Configuration for Hybrid Storage Enable
Disabled

Extended BIOS Range Decode

Enabling this will make memory cycles falling in a specific area to be redirected to SPI flash controller.

Enable
Disable

➤ PCI Express Configuration

DMI Link ASPM Control

The control of Active State Power Management of the DMI Link.

Auto	L0sL1
L0s	Disable
L1	

Port8xh Decode

PCI Express Port8xh Decode enable/disable.

Enable
Disable

Peer Memory Write Enable

Peer Memory Write enable/disable.

Enable
Disable

Compliance Test Mode

Enable when using Compliance Load Board.

Enable
Disable

PCIe function swap

When Disabled, prevents PCIe rootport function swap. If any function other than 0th is enabled, 0th will become visible.

Enable
Disable

➤➤ PCIe EQ Settings

PCIe EQ override

Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process.

Enable
Disable

➤➤ PCI Express Root Port 1-24

PCI Express Root Port 1-24

Control the PCI Express Root Port.

Enable
Disable

Connection Type

Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.

Built-in
Slot

ASPM

Set the ASPM Level: Force L0s - Force all links to L0s State AUTO - BIOS auto configure DISABLE - Disables ASPM.

Auto	L0sL1
L0s	Disable
L1	

L1 Substates

PCI Express L1 Substates settings.

L1.1
L1.1 & L1.2
Disable

ACS

Enable/disable Access Control Services Extended Capability.

Enable
Disable

PTM

Enable/disable Precision Time Measurement.

Enable
Disable

DPC

Enable/disable Downstream Port Containment.

Enable
Disable

EDPC

Enable/disable Rootport extensions for Downstream Port Containment.

Enable
Disable

URR

PCI Express Unsupported Request Reporting enable/disable.

Enable
Disable

FER

PCI Express Device Fatal Error Reporting enable/disable.

Enable
Disable

NFER

PCI Express Device Non-Fatal Error Reporting enable/disable.

Enable
Disable

CER

PCI Express Device Correctable Error Reporting enable/disable.

Enable
Disable

SEFE

Root PCI Express System Error on Fatal Error enable/disable.

Enable
Disable

SENF

Root PCI Express System Error on Non-Fatal Error enable/disable.

Enable
Disable

SECE

Root PCI Express System Error on Correctable Error enable/disable.

Enable
Disable

PME SCI

PCI Express PME SCI enable/disable.

Enable
Disable

Hot Plug

PCI Express Hot Plug enable/disable.

Enable
Disable

Advanced Error Reporting

Advanced Error Reporting enable/disable.

Enable
Disable

PCIe Speed

Configure PCIe Speed.

Auto	Gen2
Gen1	Gen3

Transmitter Half Swing

Transmitter Half Swing enable/disable.

Enable
Disable

Detect Timeout

The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.

0

Extra Bus Reserved

Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

0

Reserved Memory

Reserved Memory for this Root Bridge (1-20) MB.

10

Reserved I/O

Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.

4

LTR

PCH PCIE Latency Reporting enable/disable.

Enable
Disable

LTR Lock

PCIE LTR Configuration Lock.

Enable
Disable

➤➤➤ **Extra Options**

Detect Non-Compliance Device

Detect Non-Compliance PCI Express Device. If enable, it will take more time at POST time.

Enable
Disable

Prefetchable Memory

Prefetchable Memory Range for this Root Bridge.

10

Reserved Memory Alignment

Reserved Memory Alignment (0 - 31 bits).

1

Prefetchable Memory Alignment

Prefetchable Memory Alignment (0 - 31 bits).

1

➤➤ **PCIE Clock**

Clock0-15 assignment

Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.

Platform-POR
Enable
Disable

ClkReq for Clock0-15

Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.

Platform-POR
Disable

➤ SATA and RSTe Configuration

SATA Controller(s)

Enable/disable SATA Device.

Enable
Disable

SATA Mode Selection

Determines how SATA controller(s) operate.

AHCI
Intel RSTe Premium With Intel Optane System Acceleration

SATA Test Mode

Test Mode enable/disable (Loop Back).

Enable
Disable

Aggressive LPM Support

Enable PCH to aggressively enter link power state.

Enable
Disable

Port 0/1/2/3/4/5/6/7

Enable or disable SATA Port

Enable
Disable

Hot Plug

Designates this port as Hot Pluggable.

Enable
Disable

External

Marks this port as external.

Enable
Disable

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

Enable
Disable

SATA Device Type

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

Hard Disk Drive
Solid State Drive

Topology

Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2.

Unknown	Flex
ISATA	M2
Direct Connect	

SATA Port 0 DevSlp

Enable/disable SATA Port 0 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it.

Enable
Disable

DITO Configuration

Enable/disable DITO Configuration.

Enable
Disable

DITO Value

DITO Value.

625

DM Value

DM Value.

15

➤➤ Software Feature Mask Configuration

HDD Unlock

If enabled, indicates that the HDD password unlock in the OS is enabled.

Enable
Disable

LED Locate

If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

Enable
Disable

➤ USB Configuration

xDCI Support

Enable/disable xDCI (USB OTG Device).

Enable
Disable

USB2 PHY Sus Well Power Gating

Select 'Enabled' to enable SUS Well PG for USB2 PHY. This option has no effect on PCH-H.

Enable
Disable

USB3 Link Compliance

Enable/disable USB3 Link Compliance.

Enable
Disable

XHCI LTR Mode

Enable/disable XHCI LTR Mode.

Enable
Disable

USB PDO Programming

Select 'Enabled' if Port Disable Override functionality is used.

Enable
Disable

USB Overcurrent

Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.

Enable
Disable

USB Overcurrent Lock

Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.

Enable
Disable

USB Port Disable Override

Selectively enable/disable the corresponding USB port from reporting a Device Connection to the controller.

Select Per-Pin
Disable

➤ Security Configuration

RTC Memory Lock

Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.

Enable
Disable

BIOS Lock

Enable/disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.

Enable
Disable

Force unlock on all GPIO pads

If Enabled BIOS will force all GPIO pads to be in unlocked state.

Enable
Disable

➤ Seriallo Configuration**I2C0-7 Controller**

Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC).

Enable
Disable

SPI0-3 Controller

Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC).

Enable
Disable

UART0-6 Controller

Enables/Disables Serial IO Controller If given device is Function 0 PSF disabling is skipped. PSF default will remain and device PCI CFG Space will still be visible. This is needed to allow PCI enumerator access functions above 0 in a multifunction device. The following devices depend on each other: I2C0 and I2C1,2,3 UART0 and UART1,SPI0,1 UART2 and I2C4,5 UART 0 (00:30:00) cannot be enabled when: 1. I2S Audio codec is enabled (_SB.PC00.I2C0.HDAC).

Enable
Communication port (COM)
Disable

GPIO IRQ Route

Route all GPIOs to one of the IRQ.

IRQ14
IRQ15

WITT/MITT Test Device

Choose if WITT Device is used and with which controller.

Enabled - I2C0	Enabled - I2C5
Enabled - I2C1	Enabled - SPI0
Enabled - I2C2	Enabled - SPI1
Enabled - I2C3	Enabled - SPI2
Enabled - I2C4	Disable

UART Test Device

Choose if UART Test Device is used and with which controller.

Enabled - UART0	Enabled - UART2
Enabled - UART1	Disable

Additional Serial IO devices

When enabled, ACPI will report additional devices connected to Serial IO.

Enable
Disable

SerialIO timing parameters

Enables additional timing parameters for all Serial IO controllers. Defaults can be changed in each controller setting. Platform restart required to apply changes.

Enable
Disable

➤➤ Serial IO I2C0/1/3/5 Settings

Configure Serial IO Controller.

➤ ISH Configuration**ISH Controller**

Enables/disables Integrated Sensor Hub (ISH) Device.

Enable
Disable

PDT Unlock Message

Checked = Sends PDT Unlock Message to ISH. After the message is sent the field is set back to unchecked automatically.

Enable
Disable

SPI_0

Checked = Pin set to ISH Native function. Checkbox grayed out = disable conflicting SerialIO controller to set. Shared pins: 1. ISH UART0 - LPSS I2C2(PCH-H) 2. ISH UART1 - LPSS UART1 3. ISH I2C2 - LPSS I2C5(PCH-LP) / I2C3(PCH-H).

Enable
Disable

UART0-1

Checked = Pin set to ISH Native function. Checkbox grayed out = disable conflicting SerialIO controller to set. Shared pins: 1. ISH UART0 - LPSS I2C2(PCH-H) 2. ISH UART1 - LPSS UART1 3. ISH I2C2 - LPSS I2C5(PCH-LP) / I2C3(PCH-H).

Enable
Disable

I2C0-2

Checked = Pin set to ISH Native function. Checkbox grayed out = disable conflicting SerialIO controller to set. Shared pins: 1. ISH UART0 - LPSS I2C2(PCH-H) 2. ISH UART1 - LPSS UART1 3. ISH I2C2 - LPSS I2C5(PCH-LP) / I2C3(PCH-H).

Enable
Disable

GP_0-7

Checked = Pin set to ISH Native function. Checkbox grayed out = disable conflicting SerialIO controller to set. Shared pins: 1. ISH UART0 - LPSS I2C2(PCH-H) 2. ISH UART1 - LPSS UART1 3. ISH I2C2 - LPSS I2C5(PCH-LP) / I2C3(PCH-H)

1

➤ Pch Thermal Throttling Control**Thermal Throttling Level**

Determine if use Intel suggested setting.

Suggested Setting
Manual

DMI Thermal Setting

Determine if use Intel suggested setting.

Suggested Setting
Manual

SATA Thermal Setting

Determine if use Intel suggested setting.

Suggested Setting
Manual

➤ FIVR Configuration

Enable Rail in S0i1/S0i2

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Enable Rail in S0i3

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Enable Rail in S5

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Active Switch Supported

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Normal Active Voltage Supported

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Minimum Active Voltage

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Minimum Retention Voltage

Enables External V1P05 Rail in corresponding Sx/S0ix.

Enable
Disable

Enable Rail in S5

Enables External Vnn Rail in corresponding Sx/S0ix.

Enable
Disable

External V1P05 Icc Max Value

Icc Max Value for external V1p05 rail. Expressed in mA. Accepted value are between 0 and 500 mA.

500

External V1P05 Voltage Value

Voltage Value for external V1p05 rail. Specified in 2.5mV increments (0=0mV, 1=2.5mV, 2=5mV...).

External Vnn Icc Max Value

Icc Max Value for external Vnn rail. Expressed in mA. Accepted value are between 0 and 500 mA.

External Vnn Voltage Value

Voltage Value for external Vnn rail. Specified in 2.5mV increments (0=0mV, 1=2.5mV, 2=5mV...)

External Vnn Sx Icc Max Value

Icc Max Value for external Vnn rail in Sx states. Expressed in mA. Accepted value are between 0 and 500 mA.

External Vnn Sx Voltage Value

Voltage Value for external Vnn rail in Sx states. Specified in 2.5mV increments (0=0mV, 1=2.5mV, 2=5mV...).

Retention to Low Current Mode

Transition time in microseconds from Off (0V) to High Current Mode Voltage. This field has 1us resolution.

Retention to High Current Mode

Transition time in microseconds from Retention Mode Voltage to High Current Mode Voltage. This field has 1us resolution.

Low to High Current Mode

Transition time in microseconds from Low Current Mode Voltage to High Current Mode Voltage. This field has 1us resolution.

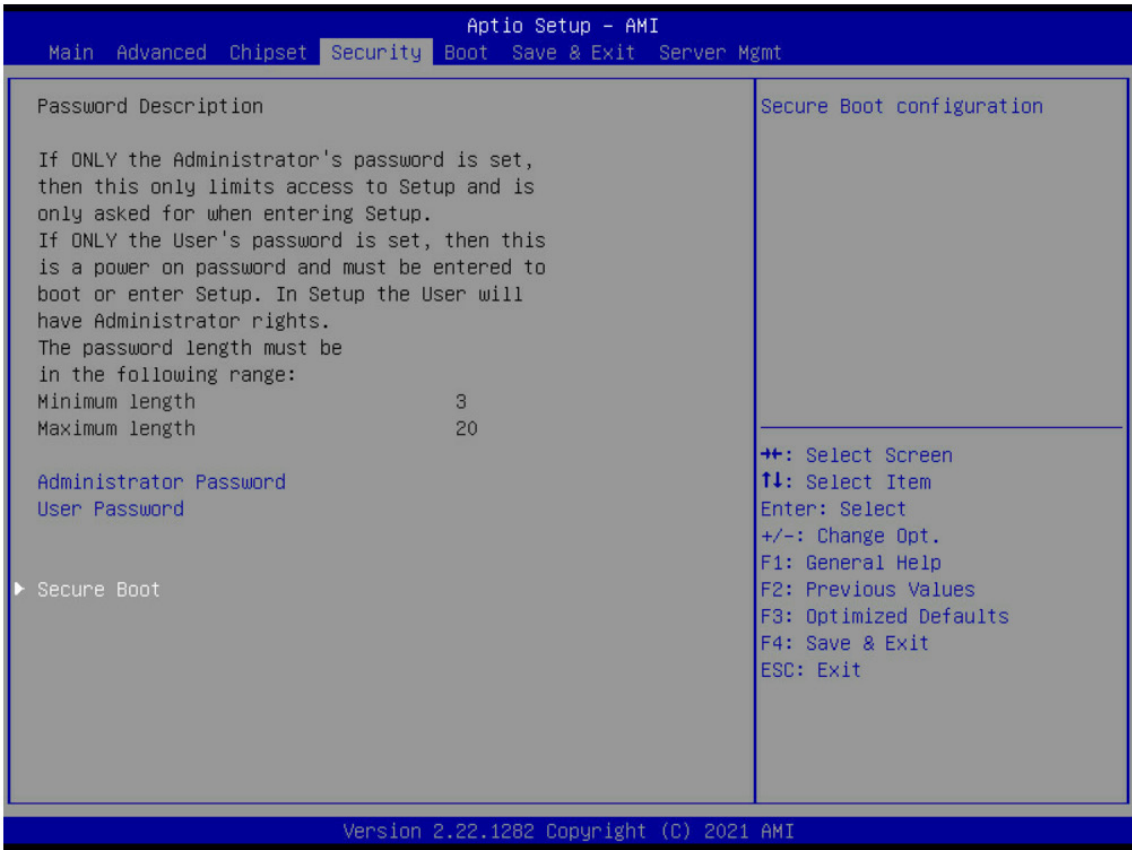
Off to High Current Mode

Transition time in microseconds from Off (0V) to High Current Mode Voltage. This field has 1us resolution. 0 = Transition to 0V is disabled.

FIVR Dynamic PM

Enable/disable FIVR Dynamic Power Management.

4.6 Security



Administrator Password

Set administer password.

User Password

Create new password.

4.6.1 Secure Boot

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.

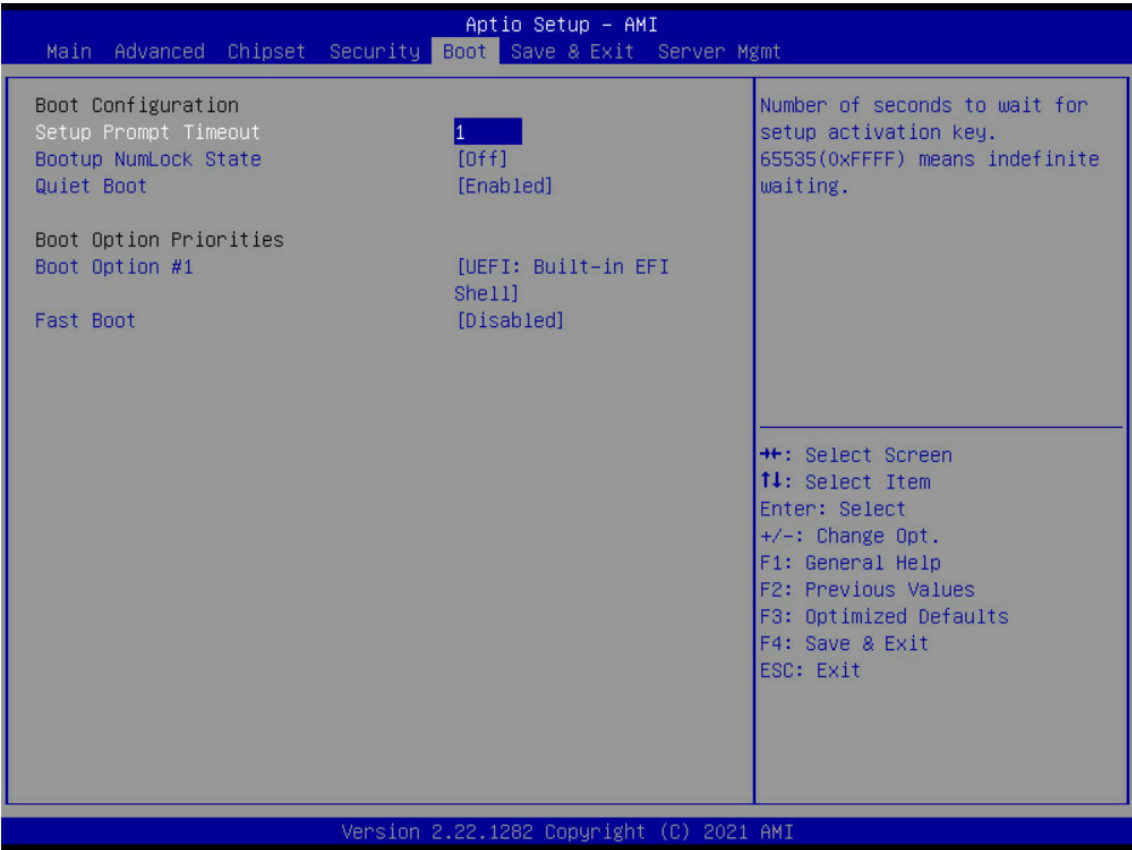
Enable
Disable

Secure Boot Mode

Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication.

Standard
Custom

4.7 Boot



Setup Prompt Timeout

Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.

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.

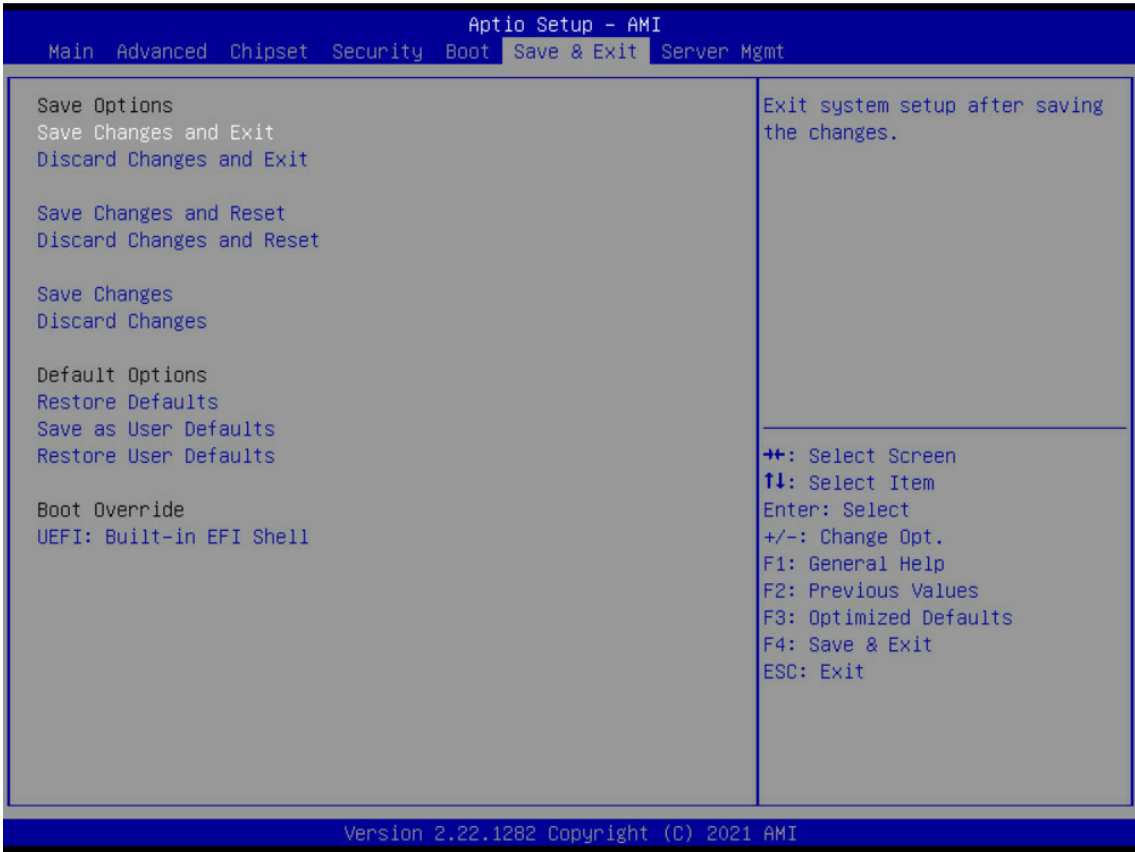
UEFI: Built-in EFI Shell
Disable

Fast Boot

Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.

Enable
Disable

4.8 Save and Exit



Save Options

Exit system setup after saving the changes.

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: Built-in EFI Shell

Save configuration and reset.

4.9 Server Mgmt



BMC Support

Enable/disable interfaces to communicate with BMC.

Enable
Disable

IPMI Interface Type

Type of Interface to communicate BMC from HOST.

Kcs Interface
Bt Interface

Wait For BMC

Wait For BMC response for specified time out. In PILOTII, BMC starts at the same time when BIOS starts during 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	Power Down
Reset	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

OS Wtd Timer Timeout

Enter the value Between 1 to 30 min for OS Boot Watchdog Timer Expiration. Not available if OS Boot Watchdog Timer is disabled.

10

OS Wtd Timer Policy

Configure how the system should respond if the OS Boot Watchdog Timer expires. Not available if OS Boot Watchdog Timer is disabled.

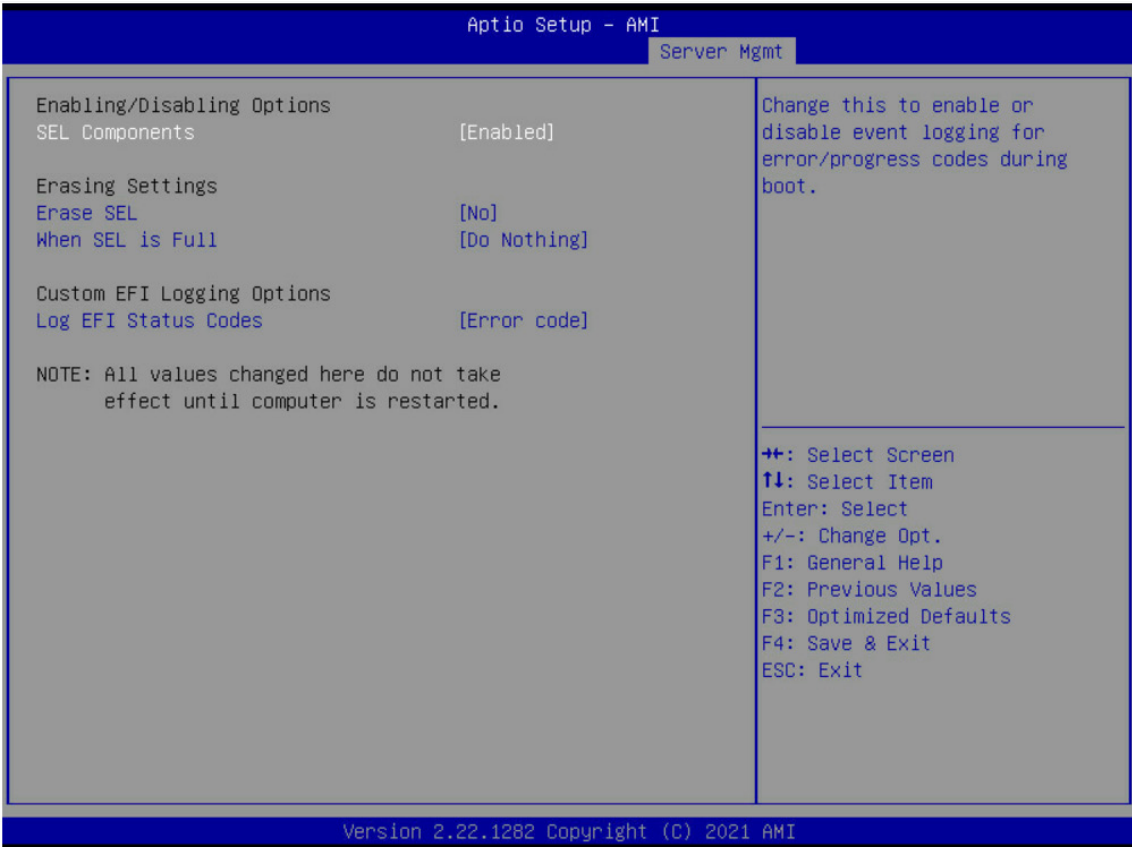
Do Nothing	Power Down
Reset	Power Cycle

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 Power Up	Power Restore
Last Power State	Unspecified

4.9.1 System Event Log



SEL Components

Change this to enable or disable event logging for 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 a full SEL.

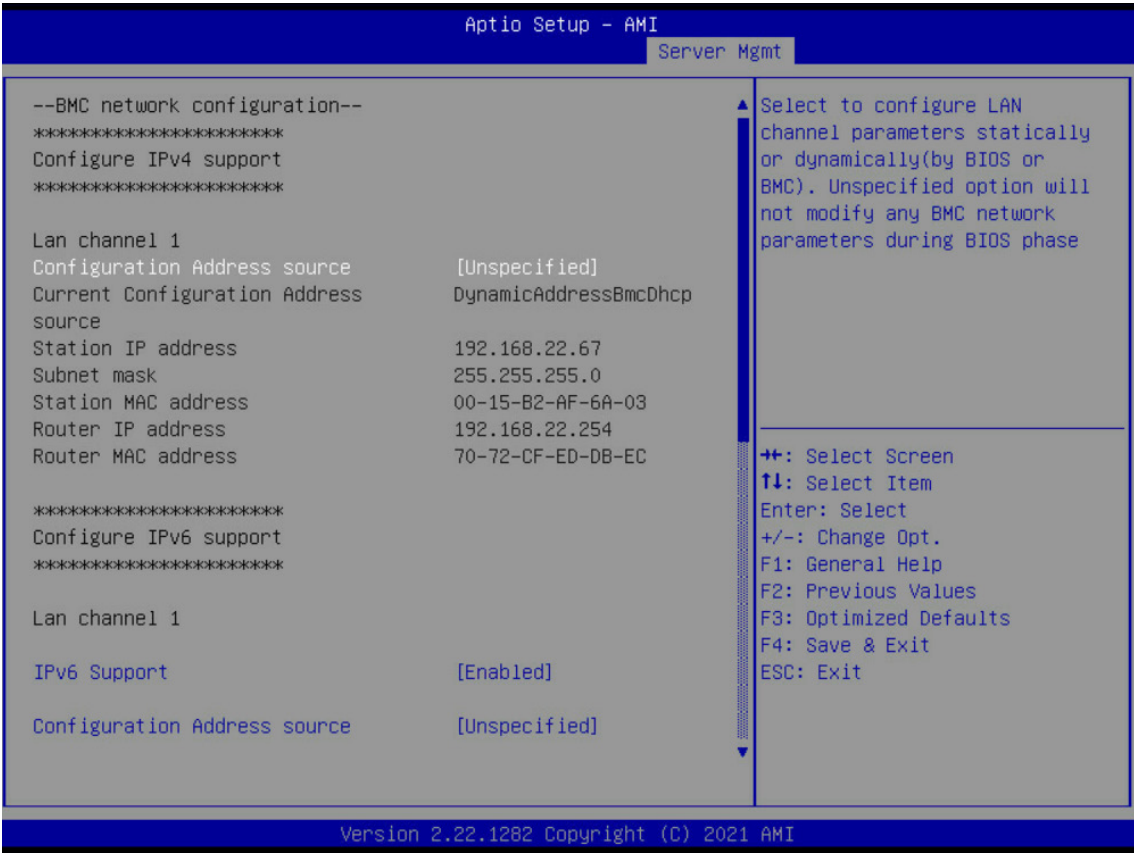
Do Nothing
Erase Immediately
Delete Oldest Record

Log EFI Status Codes

Disable the logging of EFI Status Codes or log only error code or only progress code or both.

Error code	Both
Progress code	Disable

4.9.2 BMC Network Configuration



Configuration Address source

Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.

Static	DynamicBmcNonDhcp
DynamicBmcDhcp	Unspecified

Station IP address

Enter station IP address.

Subnet mask

Enter subnet mask.

Router IP address

Enter router IP address.

Router MAC address

Enter router MAC address.

IPv6 Support

Enable or disable LAN1 IPv6 Support.

Enable
Disable

Configuration Address source

Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.

Static
DynamicBmcDhcp
Unspecified

Station IPv6 address

Enter station IPv6 address.

Prefix Length

Change the prefix length.

Configuration Router Lan1 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.

Static
DynamicBmcDhcp
Unspecified

IPv6 Router IP Address

Change the IPv6 Router IP Address.

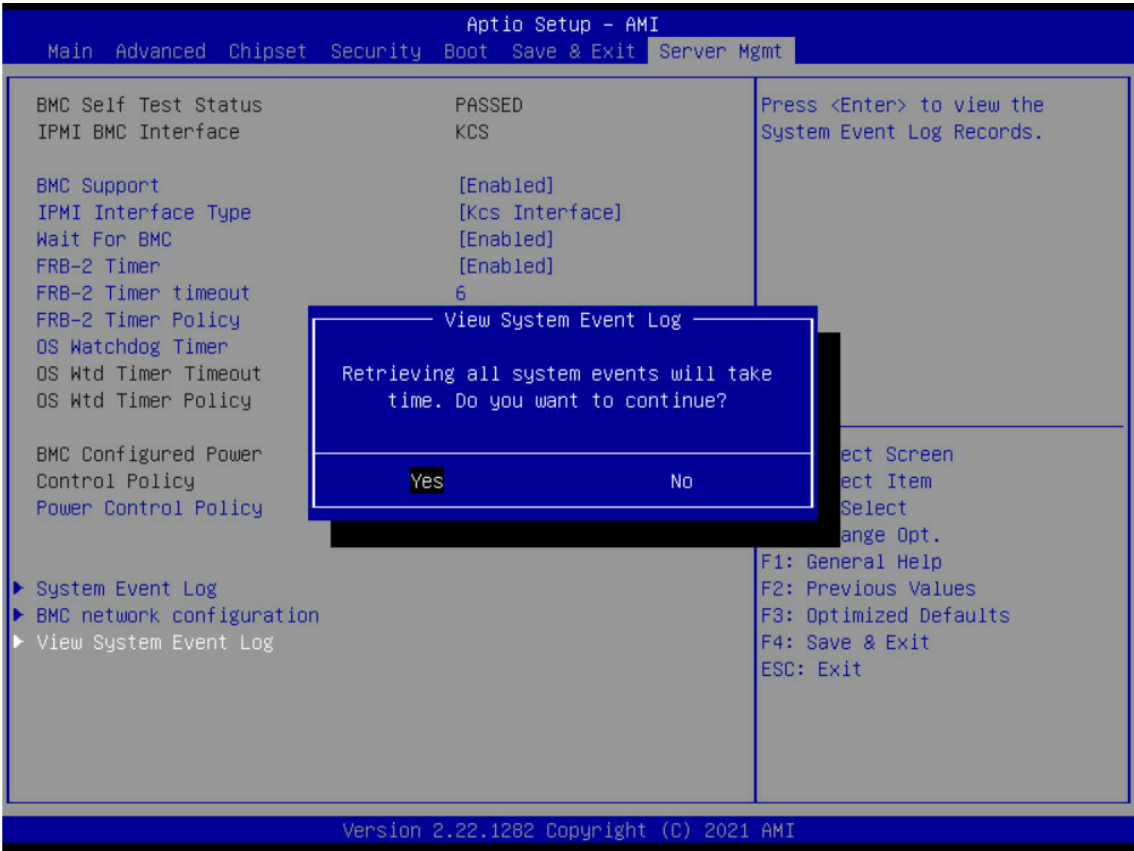
IPv6 Router Prefix Length

Change the IPv6 Router Prefix Length.

IPv6 Router1 Prefix Value

Change the IPv6 Router Prefix Value.

4.9.3 View System Event Log



Chapter 5. BMC Configuration Settings

5.1 Login



NOTE

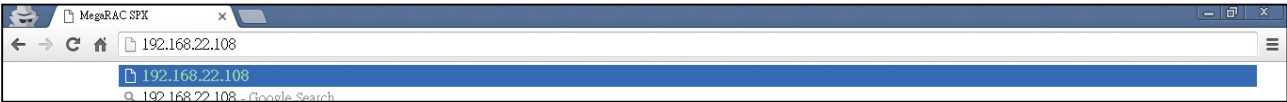
For further details about the BMC, please refer to Delphinus BMC Manual for reference.

AIC® website link: <https://www.aicpc.com/en/productdetail/51202>.

The BMC default IP source is DHCP. The IP address can be configured in H2O IPMI configuration as demonstrated by the example below.

Step 1 Open the browser and then type in the BMC IP address.

IP address example: 192.168.22.108



Step 2 Use the default user name and password for first-time BMC WEB GUI login.

Field:	Default
UserName:	admin
Password:	admin



NOTE

The default user name and password are in lower-case characters.

Users who login with the root user name and password will have full administrative power. The root password can be changed after login.

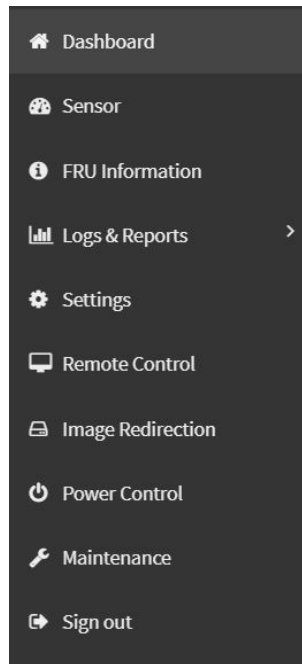
5.2 Web GUI

5.2.1 Menu Bar

The menu bar displays the following.

Firmware Information will be displayed with the latest version, date and time details. Power Control Status will be displayed as Host Online. To change the Power Control Status, click [Host Online](#) link.

- Dashboard
- Sensor
- FRU Information
- Logs & Report
- Settings
- Remote Control
- Image Redirection
- Power Control
- Maintenance
- Sign out



5.2.2 User Information and Quick Button

The user information and quick buttons are located at the top right. A screenshot of the logged-in user information is shown below.

User Information

The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions.



Logged-in user and its privilege level

This option shows the logged-in user name and privilege. There are five kinds of privileges.

User: Only valid commands are allowed.

Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.

Administrator: All BMC commands are allowed.

No Access: Login access denied.

OEM: All OEM commands are allowed.

Message: Click the icon to view the event log alert messages. On clicking the messages, it will navigate to the Logs and Reports page.

Language Selection: Change the language to view the language strings in different languages.

Refresh: Click the Refresh icon or pressing key F5 to reload the current page.

Sync: Click the Sync icon to synchronize with Latest Sensor and Event Log updates.

Signout: Click the Sign out icon to log out.

Notification: Click to view the notification received.

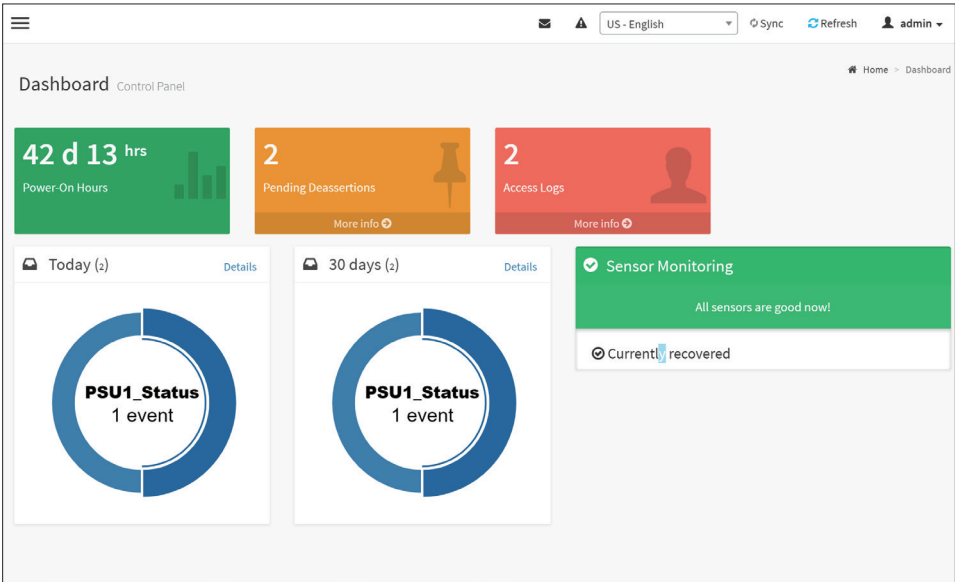
Quick Search: Quick Search is a short-cut for the available menu and sub-menu pages. It displays available search queries. Click (Quick Search) field, and type search terms of the lists in the menu bar. As you type, the suggestions will be displayed in a drop-down list below the Quick Search field as a navigational links of the menu and sub-menu. On selecting your search term from the drop-down list, it will directly go to the specific page which you have searched.

Help

Help - The Help icon () is Located at the top right of each page. Click this help icon to view more detailed field descriptions.

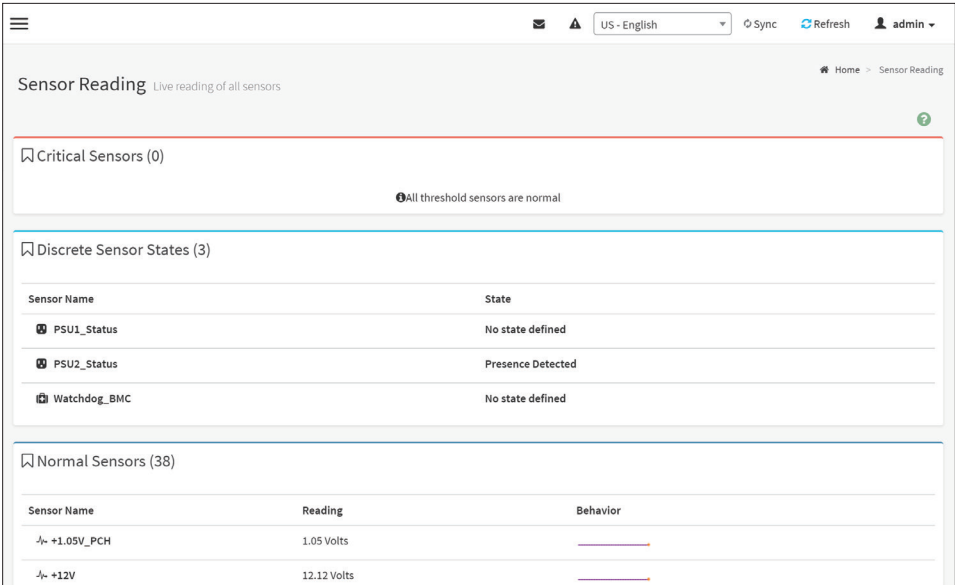
5.2.3 Dashboard

The Dashboard page displays device, system and network information. Click [Dashboard](#) on the menu bar to view the overall information of the server.



5.2.4 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.



5.2.5 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.

The screenshot displays the 'FRU Field Replaceable Units' page. At the top, there's a header with navigation links and a user profile. Below the header, the 'Available FRU Devices' section shows a dropdown menu with '0' selected and the device name 'BMC_FRU'. The main content area is divided into three columns: 'Chassis Information', 'Board Information', and 'Product Information'. Each column contains a table of details.

Chassis Information	
Chassis Information Area Format Version	1
Chassis Type	Main Server Chassis
Chassis Part Number	
Chassis Serial Number	
Chassis Extra	

Board Information	
Board Information Area Format Version	1
Language	0
Manufacture Date Time	Tue Sep 18 14:32:00 2018
Board Manufacturer	AIC
Board Product Name	VIRGO
Board Serial Number	35992-1837-00043
Board Part Number	BMB-DP50002B
FRU File ID	
Board Extra	

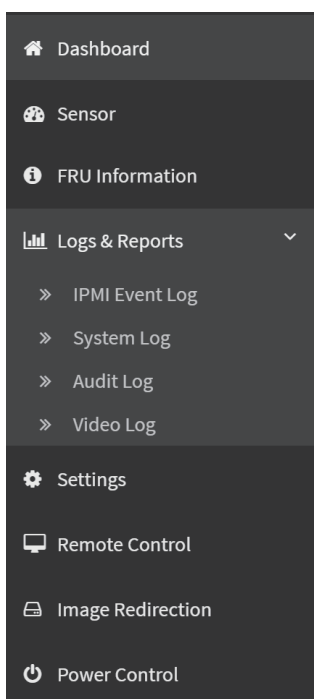
Product Information	
Product Information Area Format Version	1
Language	0
Product Manufacturer	
Product Name	
Product Part Number	
Product Version	
Product Serial Number	
Asset Tag	
FRU File ID	
Product Extra	

5.2.6 Logs and Reports

The Logs & Reports page displays the following information.

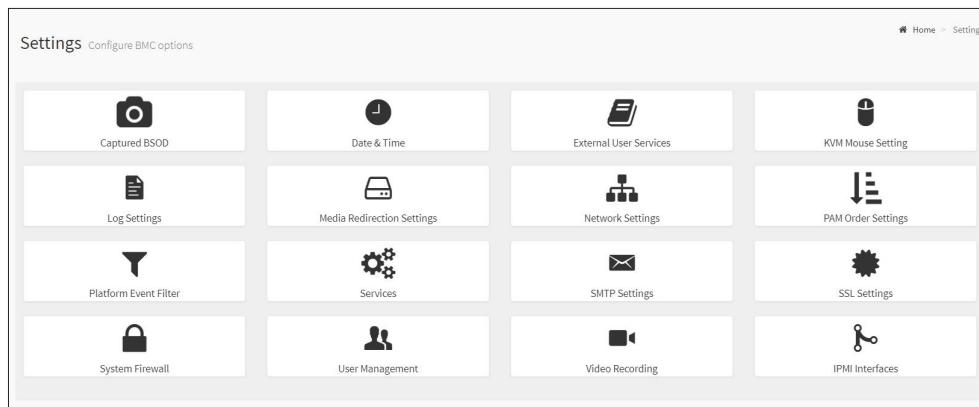
- IPMI Event Log
- System Log
- Audit Log
- Video Log

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



5.2.7 Settings

This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



- Captured BSOD
- Date&Time
- External User Services
- KVM Mouse Setting
- Log Settiings
- Media Redirection Settings
- Network Settings
- PAM Order Settings
- Platform Event Fliter
- Services
- SMTP Settings
- SSL Settings
- System Firewell
- User Management
- Video Recording
- IPM Interfaces

5.2.8 Remote Control

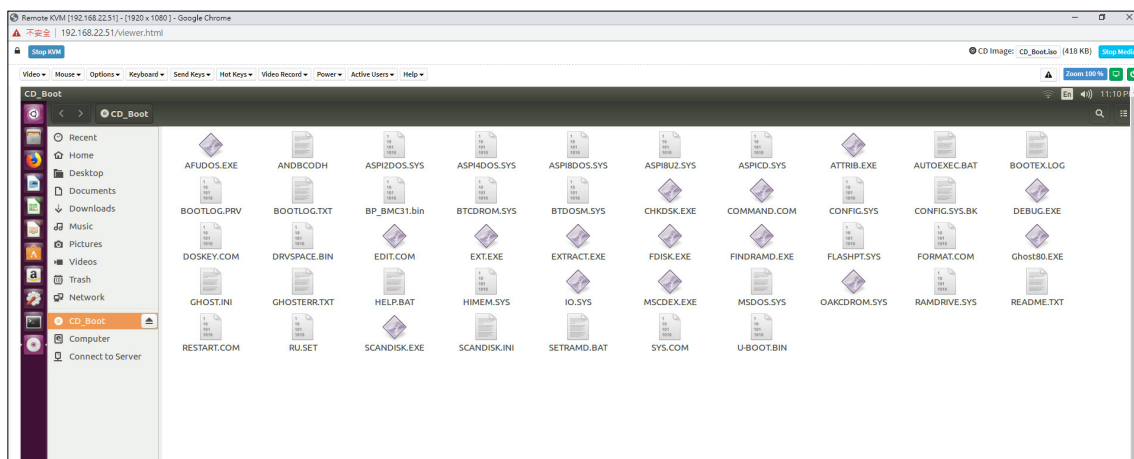
The Remote Control page consists of the following options. A sample screenshot is displayed below.

- Launch H5Viewer
- Launch JViewer
- Launch Serial Over LAN



Procedure To Start KVM

Step 1 Click Launch H5Viewer to open the Remote Control KVM page. A sample screenshot of the Remote KVM page is shown below.

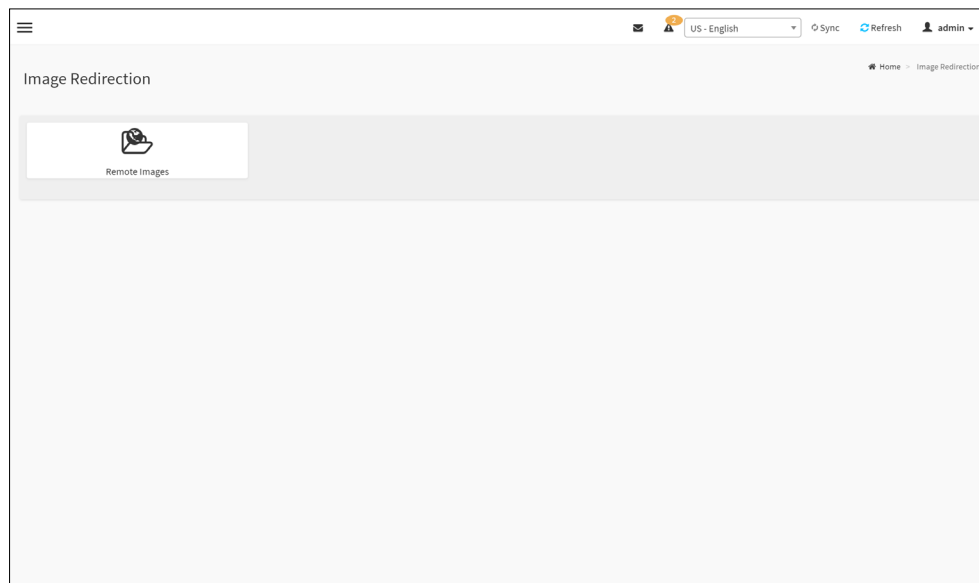


Step 2 To stop the H5Viewer video redirection, click [Stop KVM](#).

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.



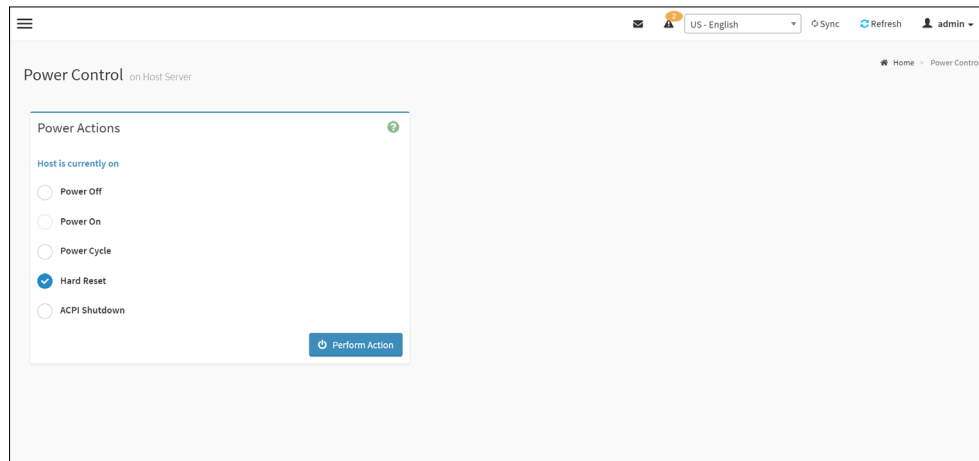
The fields of Images Redirection page are explained below.

- Remote Images

5.2.10 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

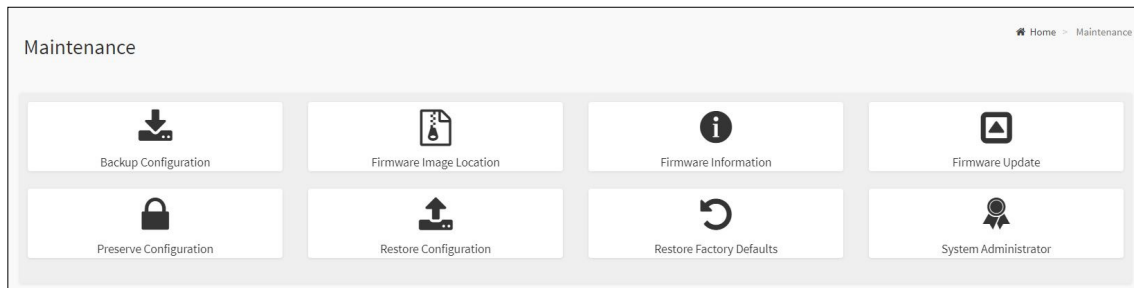
During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

5.2.11 Maintenance

This group of pages allows you to do maintenance tasks on the device. The menu contains the following items:

- Backup Configuration
- Firmware Image Location
- Firmware Information
- Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- System Administrator

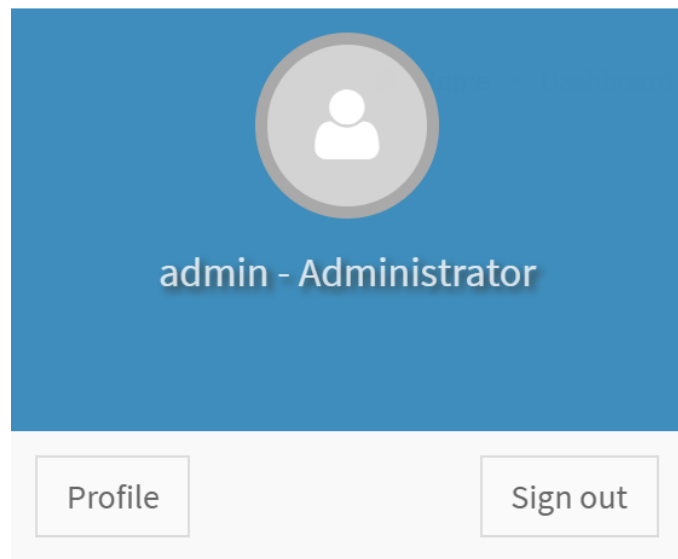
A sample screenshot of Maintenance page is displayed below.



A detailed description is given below.

5.2.12 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

Taiwain, Global Headquarters

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

Shanghai, China

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

Moscow, Russia

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

North California, United States

Address: 48531 Warm Springs
Boulevard 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>.