



Dubhe

Server Motherboard User's Manual

Table of Contents

Preface	i
Safety Instructions	ii
About This Manual	iii
Chapter 1. Product Features	1
1.1 Component	1
1.2 Specifications	2
1.3 Feature	3
Chapter 2. Hardware Setup	4
2.1 Central Processing Unit	4
2.2 System Memory	8
2.2.1 Placement	8
2.2.2 DIMM Population	9
2.2.3 Mapping Table	10
2.2.4 Installation	11
Chapter 3. Motherboard Settings	12
3.1 Block Diagram	12
3.2 Placement	13
3.3 Content List	14
3.4 External Port	16
3.5 Connector Definition	17
3.6 Jumper Setting	27
3.7 LED	30
3.7.1 Rear Chassis LEDs	30
3.7.2 Internal LEDs	30
3.7.3 LEDs Placement	31
Chapter 4. BIOS Configuration Settings	32
4.1 Navigation Keys	32
4.2 BIOS Setup	33
4.2.1 Menu	33
4.2.2 Startup	33
4.3 Main	34
4.3.1 Main	34
4.4 Advanced	35
4.4.1 RC ACPI Settings	35
4.4.2 CPU Configuration	38
4.4.3 Power & Performance	39
4.4.4 System Agent (SA) Configuration	57
4.4.5 PCIE Configuration	67
4.4.6 PCIE Hot-Plug Settings	73
4.4.7 PCH-IO Configuration	73
4.4.8 PCH-FW Configuration	77
4.4.9 Thermal Configuration	79
4.4.10 Platform Settings	83
4.4.11 ACPI D3Cold settings	86
4.4.12 OverClock Performance Menu	87

4.4.13 AMT Configuration.....	87
4.4.14 BCLK Configuration	87
4.4.15 Trusted Computing	88
4.4.16 ACPI Settings	88
4.4.17 UEFI Variables Protection.....	88
4.4.18 Serial Port Console Redirection	89
4.4.19 Switchable Graphics	89
4.4.20 AMI Graphic Output Protocol Policy	89
4.4.21 Option ROM Dispatch Policy	89
4.4.22 PCI Subsystem Settings	90
4.4.23 USB Configuration.....	90
4.4.24 Network Stack Configuration	90
4.4.25 NVMe Stack Configuration.....	90
4.4.26 SATA Configuration.....	91
4.4.27 RAM Disk Configuration	91
4.4.28 T1s Auth Configuration.....	91
4.4.29 Broadcom BCM57416 NetXtreme-E 10GBASE-T RDMA Ethernet Controller - 00:00:00:00:00:00	92
4.4.30 Intel(R) Rapid Storage Technology	93
4.5 Security	94
4.5.1 Administrator Password	94
4.5.2 User Password	94
4.5.3 Secure Boot	94
4.6 Boot.....	95
4.7 Save & Exit.....	96
4.8 Server Mgmt.....	97
4.8.1 BMC Support	97
4.8.2 Wait for BMC	97
4.8.3 FRB-2 Timer	97
4.8.4 OS Watchdog Timer	98
4.8.5 Power Control Policy.....	98
4.8.6 BMC network configurtion.....	98
4.9 BIOS Update Process.....	99
4.10 BIOS Post Code	100
Chapter 5. Technical Support	105

Document Release History

Release Date	Version	Update Content
June, 2025	1	User's Manual release to public.
January, 2026	1.1	Remove connector info. (PFR)



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

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

Preface

Copyright

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

Trademarks

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

Changes

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

Warning

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

Disclaimer

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

Instruction Symbols

Special attention should be given to the instruction symbols below.



NOTE

This symbol indicates that there is an explanatory or supplementary instruction.



CAUTION

This symbol denotes possible hardware impairment. Upmost precaution must be taken to prevent serious hardware damage.



WARNING

This symbol serves as a warning alert for potential body injury. The user may suffer possible injury from disregard or lack of attention.

Safety Instructions

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

Carefully read the safety instructions below before using this product.

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

About This Manual

Thank you for selecting and purchasing the Dubhe server board.

This user's manual is provided for professional technicians to perform easy hardware setup, basic system configurations, and quick software startup. This document pellucidly presents a brief overview of the product design, device installation, and firmware settings for the Scutum motherboard.

Chapter 1 Product Features

This chapter delivers the overall layout of the product, including the fundamental components on the motherboard, design specifications, and noteworthy features. Scutum is an ideal server grade motherboard that is specifically designed to accommodate diverse enterprises for managing heavy workloads, databases, nearline applications, and cloud deployments. This product supports single processor with LGA1851 socket type and 2 channel per slot DDR5 ECC/Non-ECC UDIMM up to 5600MT/s.

Chapter 2 Hardware Setup

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

Chapter 3 Motherboard Settings

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

Chapter 4 BIOS Configuration Settings

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

Chapter 5 Technical Support

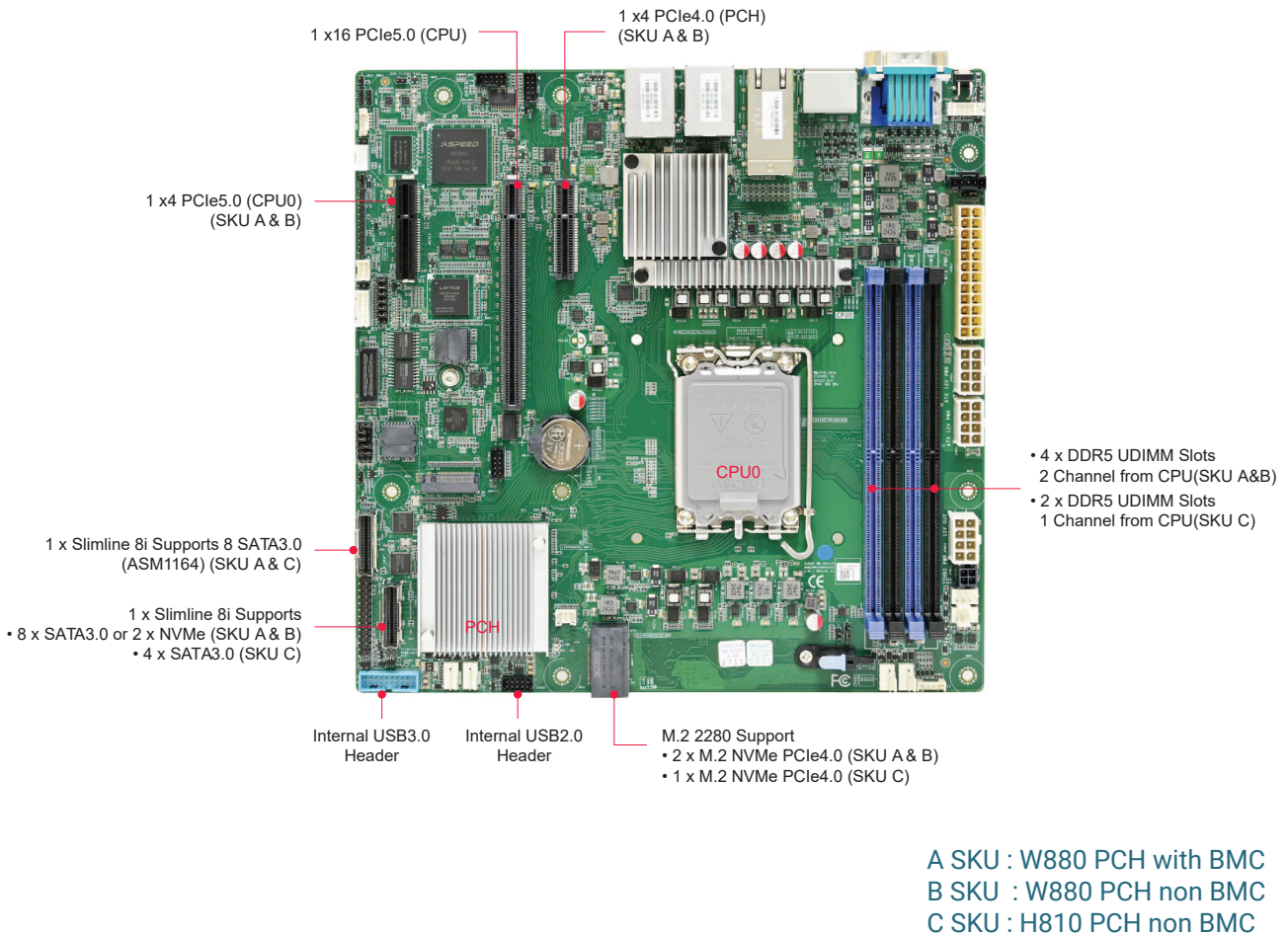
For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: <https://www.aicipc.com/en/index>. It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

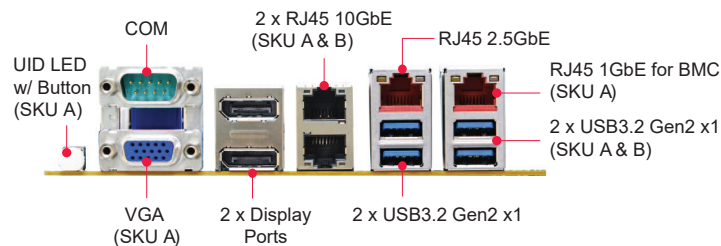
This section describes the hardware specifications and features of the Dubhe motherboard. The fundamental components of the Dubhe severboard are provided below.

1.1 Component

Dubhe Serverboard



I/O View



Dimensions

mm : 243.84 x 243.84

inches : 9.6 x 9.6

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

1.2 Specifications

System	Processor Support	Single Intel® Arrow Lake S CPU	On-board Devices	SATA	• 1 x Slimline 8i support (by PCH, in SFF8654-8i, RSTe RAID 0/1) - 8 x SATA3.0 or 2 x NVMe (SKU A & B) - 4 x SATA3.0 (SKU C) • 8 x SATA3.0 (by 2 x ASM1164, Slimline 8i connector) (SKU A & C)
	CPU TDP	125W		BMC	ASPEED AST2600
	Socket Type	Socket LGA 1851		Network Controller	• Realtek RTL8211FS 1GbE for BMC dedicated management port (NCSI shared NIC - reserved for Broadcom NIC) • Broadcom BCM57416 for dual port 10GbE (NCSI for share NIC) • I226-LM Ethernet Controller for single port 2.5GbE
	System Memory	• DDR5 ECC (SKU A & B) /non-ECC UDIMM - 5600MHz (1SPC 1R/2R) - 4800MHz (2SPC 2R) - 4400MHz (2SPC 2R) • Total 4 memory slots; 2 slots per channel (2SPC) (SKU A & B) - Total 2 memory slots; 1 slot per channel (1SPC) (SKU C) * Supports up to 192G (SKU A & B) - Supports up to 96G (SKU C)		Graphics	• Integrated VGA support by ASPEED AST2600 • Resolution up to 1920x1200 @60Hz 32bpp
	Expansion Slots	Total support 32 lanes of PCIe (PCH W880) : 20 lanes of PCIe (PCH H810) • PCIe slots - 1 x16 PCIe5.0 (CPU0) - 1 x4 PCIe5.0 from CPU0 (SKU A & B) - 1 x4 PCIe4.0 from PCH (SKU A & B) • M.2 2280 support - 2 x M.2 NVMe PCIe4.0 (SKU A & B) - 1 x M.2 NVMe PCIe4.0 (SKU C) • Slimline 8i for SATA/NVme support - SKU A : Slimline support 16 x SATA3.0 or 8 x SATA 3.0 + 2 x NVMe - SKU B : 1 Slimline support 8 x SATA3.0 or 2 x NVMe - SKU C : Slimline support 12 x SATA3.0 • 2 x USB double-stack Type-A connector supports two USB3.2 Gen2 x1 devices (SKU A & B) • 1 x USB double-stack Type-A connector supports two USB3.2 Gen2 x1 devices (SKU C) • 1 x USB pin header supports two USB3.0 Gen1 devices • 1 x USB pin header support two USB2.0 devices		Additional Information	TPM 2.0 - NUVOTON NPCT760AABYX
System BIOS	BIOS Type	AMI UEFI BIOS (64M ROM size)	Input/Output	SATA	• 1 x Slimline 8i support (by PCH, in SFF8654-8i, RSTe RAID 0/1) - 8 x SATA3.0 or 2 x NVMe (SKU A & B) - 4 x SATA3.0 (SKU C) • 8 x SATA3.0 (by 2 x ASM1164, Slimline 8i connector) (SKU A & C)
	BIOS Features	• ACPI • PXE • WOL • AC loss recovery • IPMI 2.0 KCS mode interface • SRIOV • SMBIOS • TPM • Serial console redirection • PCIe hotplug		LAN	• 2 x RJ45 10GbE (SKU A & B) • 1 x RJ45 2.5GbE • 1 x RJ45 GbE connector for BMC management port (SKU A)
				USB	• 2 x USB3.2 Gen2 x1 double-stack Type-A connectors (SKU A & B) • 1 x USB3.2 Gen2 x1 double-stack Type-A connector (SKU C) • 1 x USB pin header supports two USB3.0 Gen1 • 1 x USB pin header supports two USB2.0
				Display	• 1 x DB-15 VGA connector (SKU A) • 2 x Display ports
				Serial Port	1 x COM connector
			Others	• PCIe slots - 1 x16 PCIe5.0 (CPU0) - 1 x4 PCIe5.0 from CPU0 (SKU A & B) - 1 x4 PCIe4.0 from PCH (SKU A & B) • M.2 2280 support - 2 x M.2 NVMe PCIe4.0 (SKU A & B) - 1 x M.2 NVMe PCIe4.0 (SKU C)	
			Additional Information	Security: • TPM 2.0 onboard	

1.3 Feature

Dubhe supports single Intel® Arrow Lake-S family processors with up to 24 CPU cores and TDP up to 125W. It supports up to 192G DDR5 ECC/Non-ECC UDIMMs with 4 memory slots and memory speeds up to 5600MT/s.

The high-speed expansion I/O includes 1 x PCIe Gen 5x16 and 1 x PCIe Gen5 x4 (SKU A & B) linked to the CPU, 1 x PCIe Gen4 x4, 2 x M.2 2280 PCIe Gen4 (SKU A & B), and up to 2 Slimline 8i connectors, support up to 16 SATA 3.0 or 2 NVMe + 8 SATA 3.0 (SKU A). Security features include TPM2.0 onboard.

- Supports single Intel® Core Family Processors for highest every performance and improved power efficiency
- Supports 4 x DDR5 DIMM slots for maximum memory performance
- Supports DDR5 (SKU A&B)/Non-ECC UDIMMs (5600MHz)
- Supports up to 20 lanes of PCIe 5.0 from CPU, including 1 x16 + 1 x4 slots (SKU A & B)
- SKU A (W880): 2 x Slimline 8i support 8 SATA 3.0 (by ASM1164) + 8 SATA 3.0 or 2 NVMe G4 x 4 (from PCH)
 SKU B (W880): 1 x Slimline 8i supports 8 SATA 3.0 or 2 NVMe G4 x 4(from PCH)
 SKU C (H810): 1 x Slimline 8i support 8 SATA 3.0 (by ASM1164) + 4 SATA 3.0(PCH)
- 1 x Slimline 8i supports 8 x SATA3.0 or 2 x NVMe (W880 SKU) or 4 x SATA3.0 (SKU C)
- Supports 2 x RJ45 10GbE (SKU A & B only)

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 Single Intel® Arrow Lake S CPU and Socket LGA1851.

2.1.1 Installation

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

- ☒ a PH2 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.

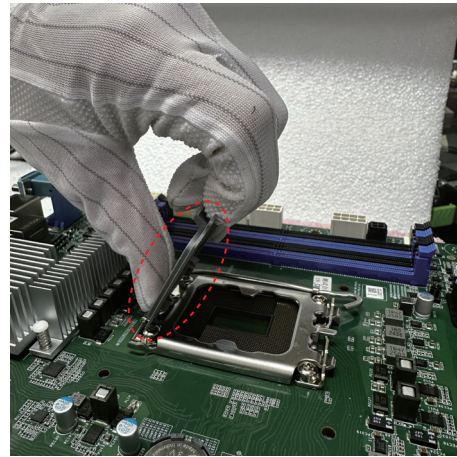
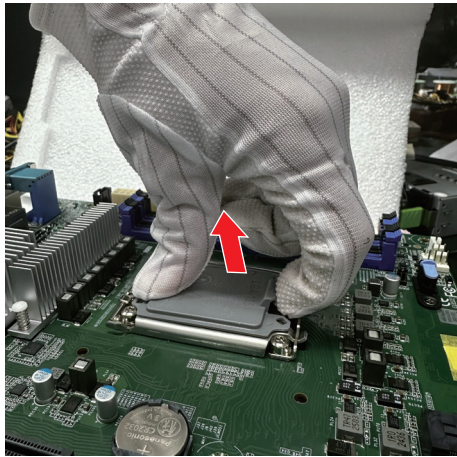
**CAUTION**

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

CPU installation and Heatsink Procedures:

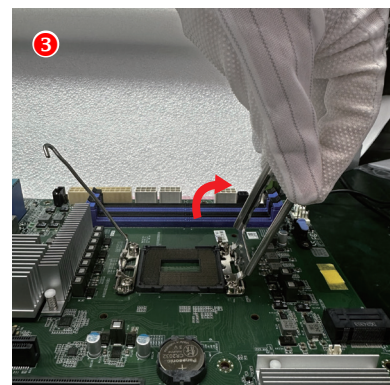
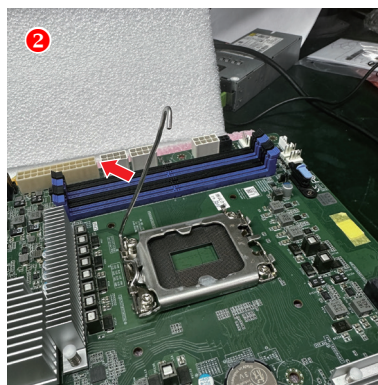
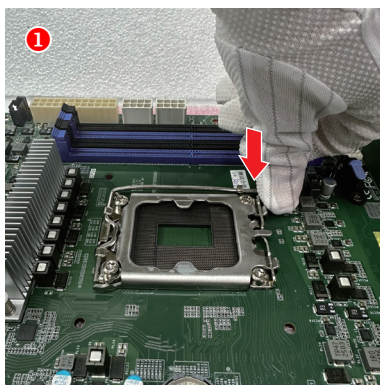
Step 1: Remove the dust cover

- ① Gently remove and save the dust cover as shown below.



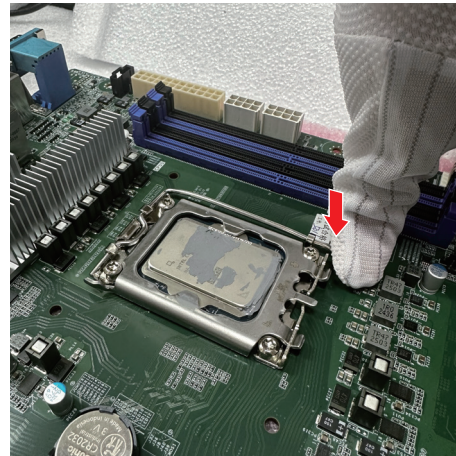
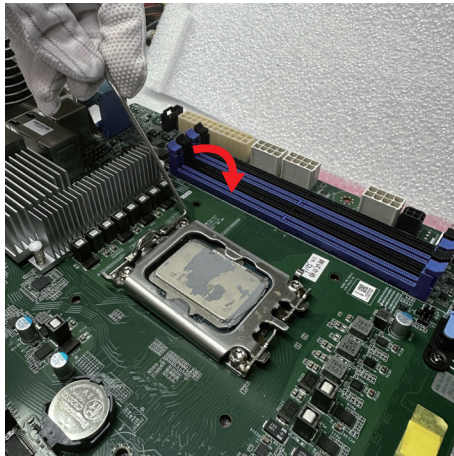
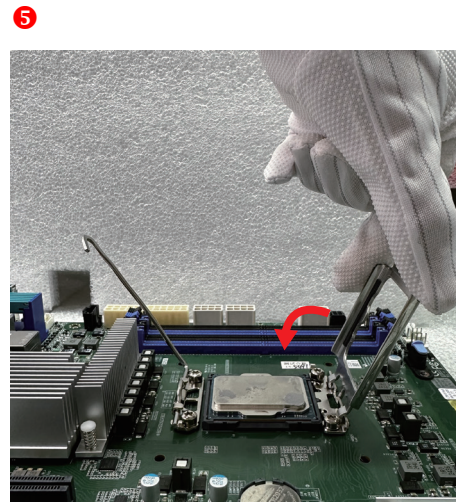
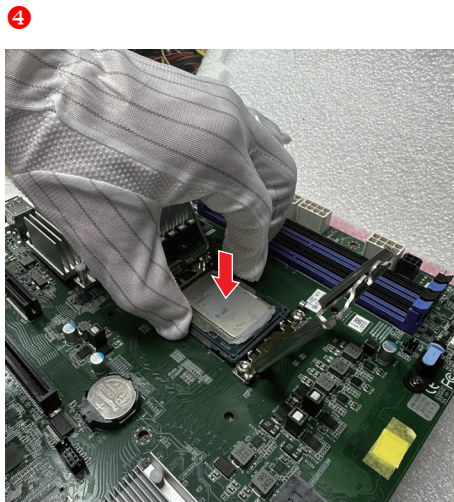
Step 2: Assemble the CPU onto the ILM

- ① Use your thumb to press the lever and hold it slowly to open
- ② Rotate the lever to fully open position.
- ③ Then open the load plate as shown below.



This information is provided for professional technicians only.

- ④ Hold both sides of the CPU and carefully place it onto the socket.
- ⑤ Close the load plate and rotate the lever through the lever head.



Step 3: Assembly Heatsink Operation Guide

- ① Align the CPU heatsink bracket's (image A) locating pins with the holes on the underside of the motherboard.
- ② Please refer to image for the correct position of the top side.

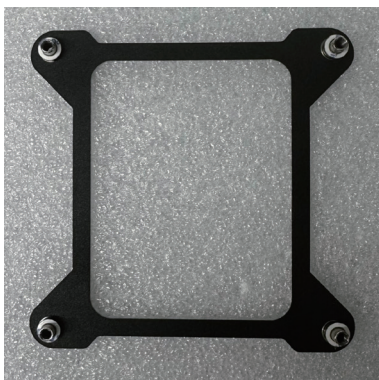
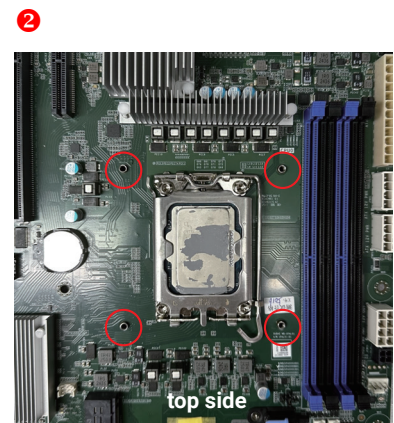
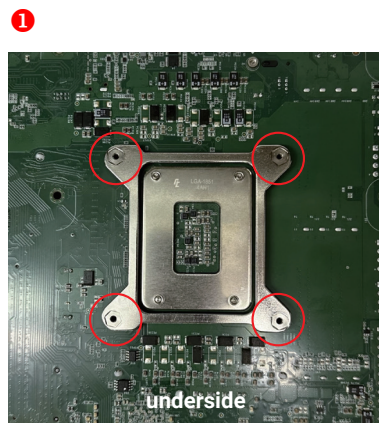
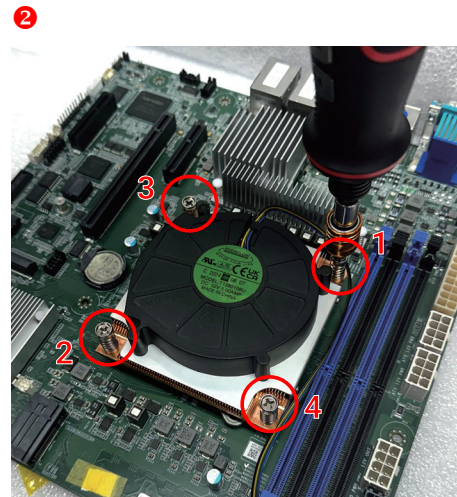
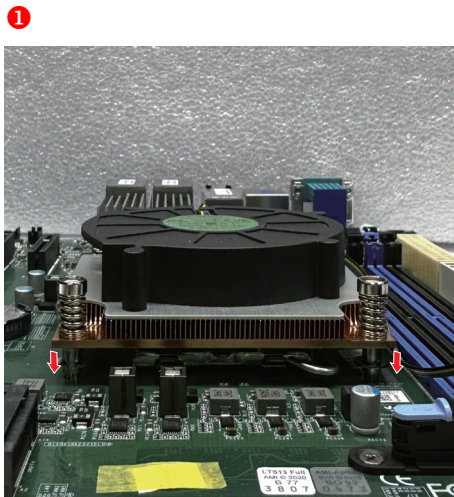


image (A)



Step 4: Loading the Heatsink

- ① Align the Heatsink with 4 screws on CPU heatsink bracket's locating pins.
- ② Tighten four Heatsink nuts in sequence as 1 to 4.
- ③ Connect the fan cable to the appropriate connector, as demonstrated below.



This information is provided for professional technicians only.

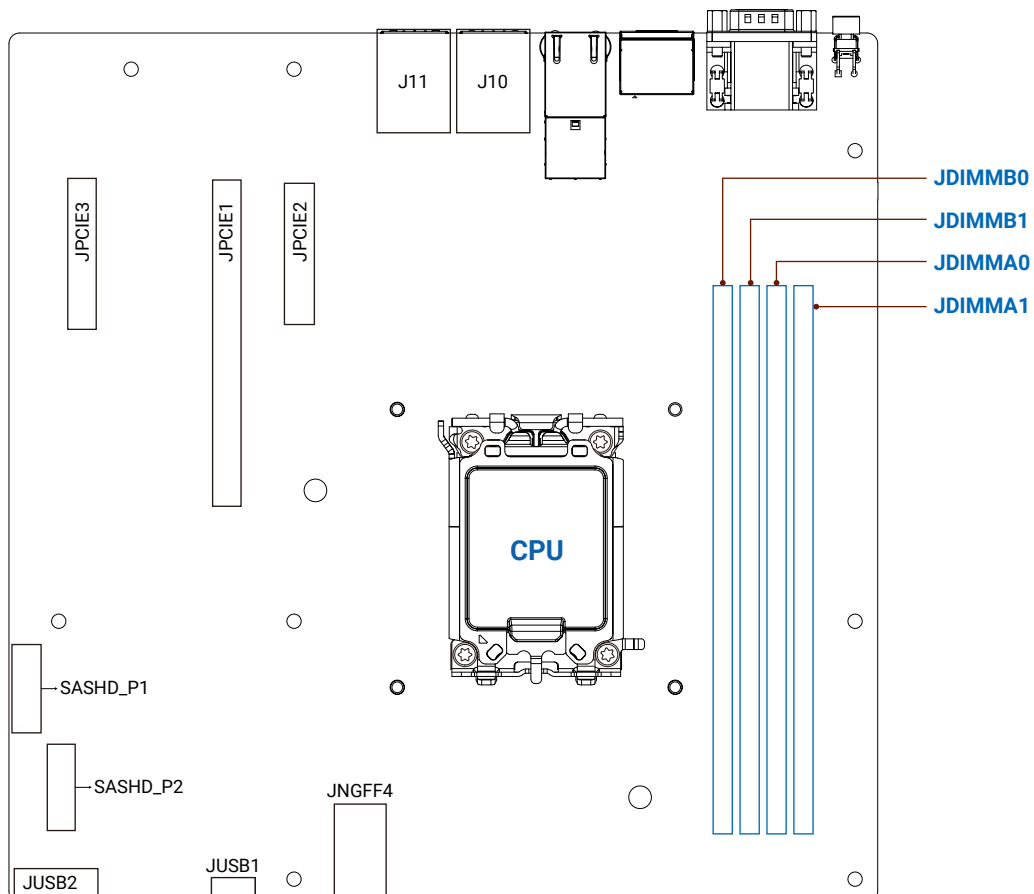
2.2 System Memory

2.2.1 Placement

The DIMMs are displayed on the Dubhe board as JDIMMA0/JDIMMA1/JDIMMB0/JDIMMB1

To ensure satisfactory performance, you need to:

- ☑ Verify the DIMM type:
This product supports DDR5 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 DDR5 DIMM per socket.



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

CPU Configuration

Placement		DIMM Number		
		1	2	4
CPU	JDIMMA0			#
	JDIMMA1	#	#	#
	JDIMMB0			#
	JDIMMB1		#	#

2.2.3 Mapping Table

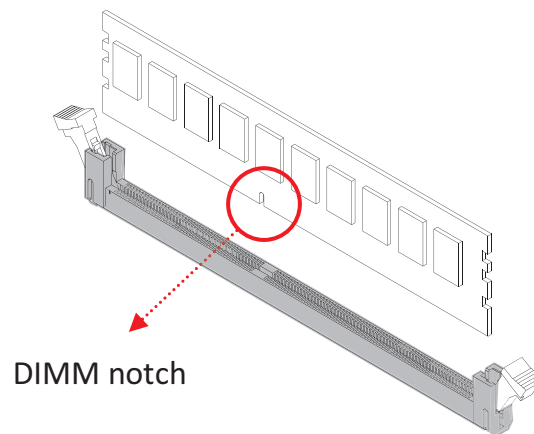
MB Location	Description	PCB silkscreen
JCPU0	Legacy CPU	CPU0
JDIMMA0	CPU0 Channel A DIMM0	A0
JDIMMA1	CPU0 Channel A DIMM1	A1
JDIMMB0	CPU0 Channel B DIMM0	B0
JDIMMB1	CPU0 Channel B DIMM1	B1
JPCIE1	CPU0 PCIE Lane 0-15	JPCIE1
JPCIE2	PCH PCIE Lane 20-23	JPCIE2
JPCIE3	CPU0 PCIE Lane 20-23	JPCIE3
JNGFF4	PCH PCIE Lane 4-7 / Lane 8-11	JNGFF4
SASHD_P1	PCH PCIE lane 0-1 to ASM1164 SATA Controller	SASHD_P1
SASHD_P2	PCH SATA/PCIE Lane 12-19	SASHD_P2

2.2.4 Installation

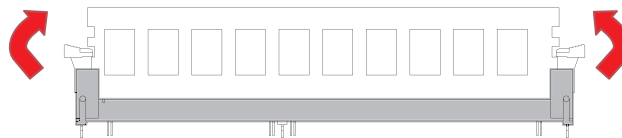
Step 1 Unlock the DIMM socket by pressing the retaining clip outward.



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



Step 3 Close the retaining clip to complete installation.

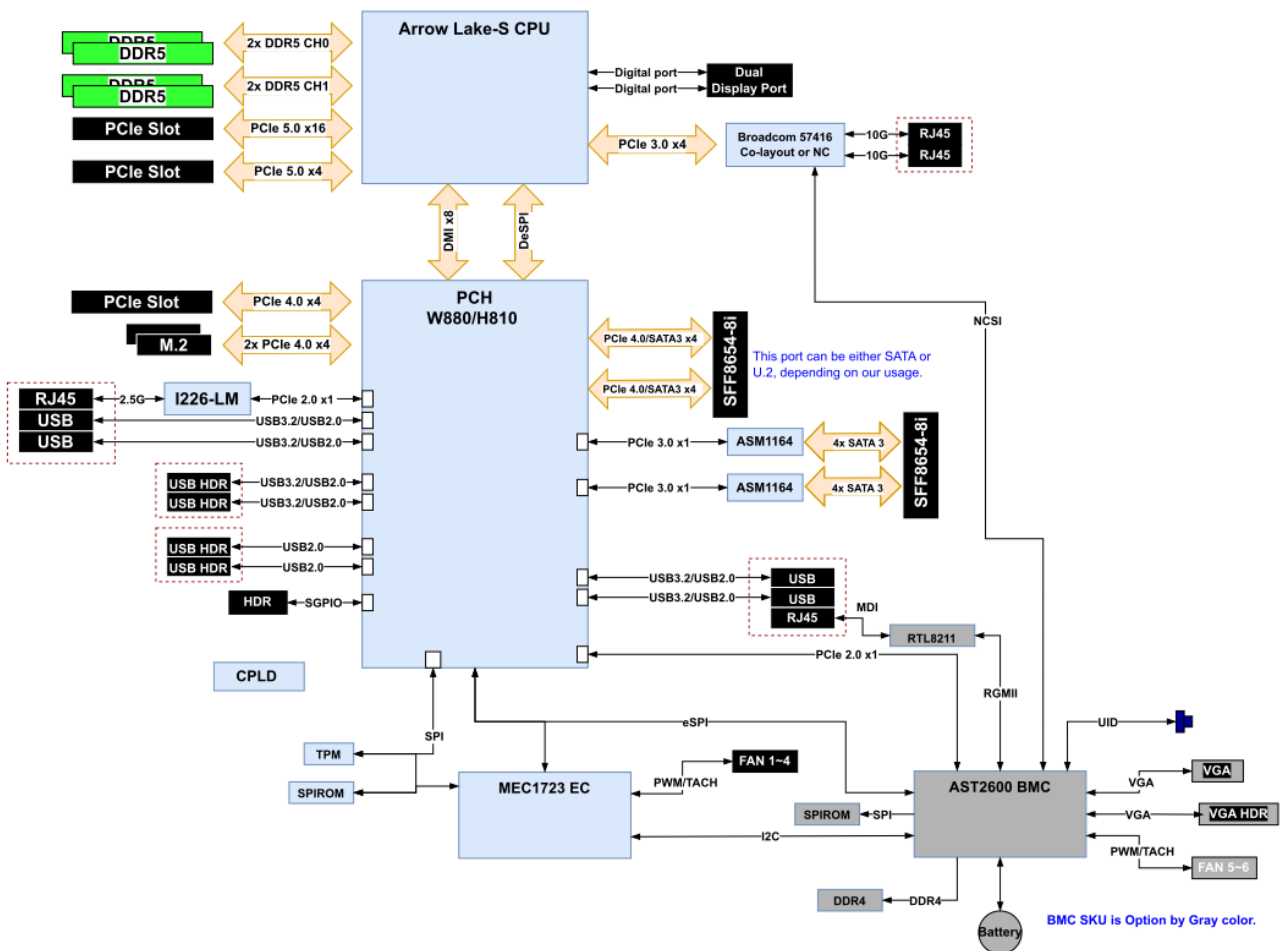


Chapter 3. Motherboard Settings

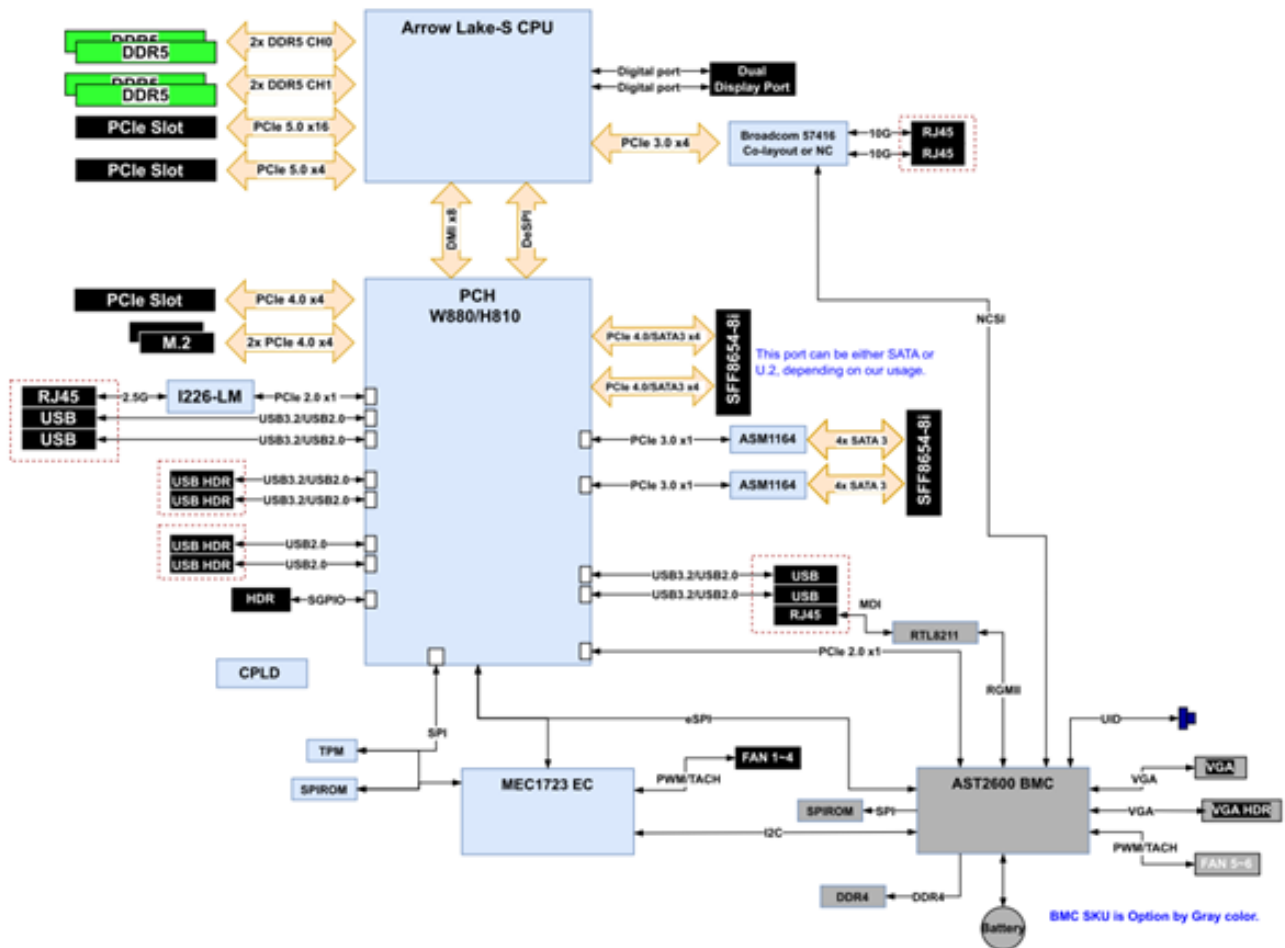
This section provides illustrations that display the internal jumpers, connectors, and system LED indicators on the Dubhe motherboard. The motherboard layout and essential connectors are listed below for your reference.

3.1 Block Diagram

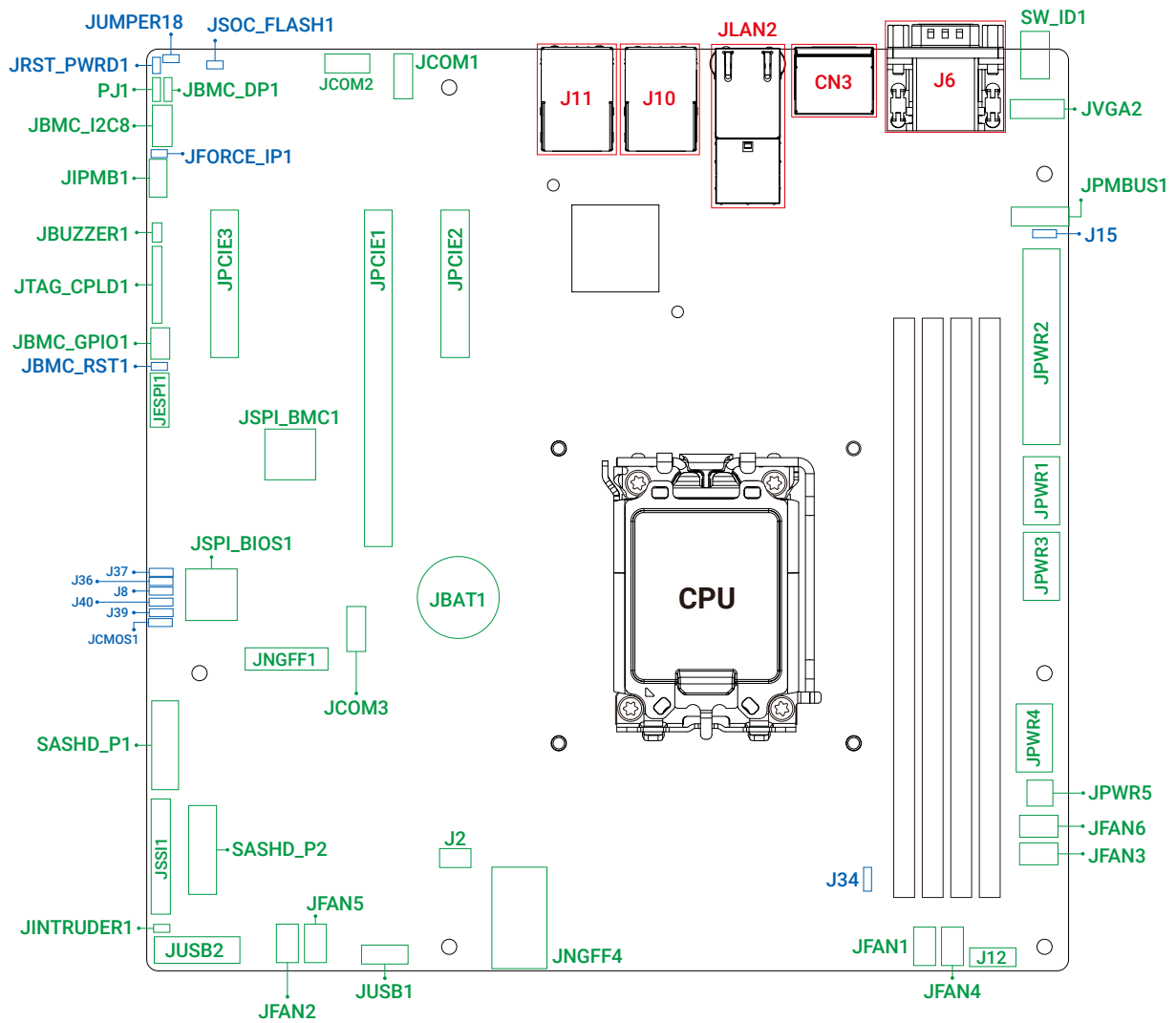
SKU A/B



SKU C



3.2 Placement



- External connectors
- Internal connectors
- Jumpers

3.3 Content List

External Connectors - Rear I/O

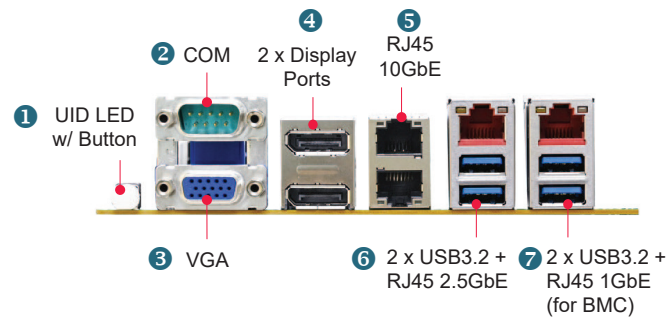
Function	Description	Comments
Ethernet x2(Stacked)	RJ45	JLAN2 : 10G/1G NIC Controller (Broadcom BCM57416)
VGA+COM	DSUB 15 Female+DB9 Female	J6
Ethernet x1+USB3.2 Gen2x1 x2	RJ45 + USB3.2 Gen2x1 Type A	J10 : 2.5G/1G NIC Controller(Intel I226-LM) +USB3.2 Gen2x1 x2
Ethernet x1+USB3.2 Gen2x1 x2	RJ45 + USB3.2 Gen2x1 Type A	J11 : 10/100/1000M PHYCEIVER (RTL8211FS)+USB3.2 Gen2x1 x2
Display++ x2(Stacked)	Displayport	CN3

Internal Connectors Summary

Function	Description	Comments
Power Supply	12 x 2 Pin ATX CONN	JPWR2: P12V_PSU, P5V_STBY_PSU
Power Supply	4 x 2 Pin ATX CONN	JPWR1: JPWR3, P12V_PSU
Power CONN for GPU	4 x 2 Pin ATX CONN	JPWR4: P12V
Power CONN for HDD	2 x 2 Pin ATX CONN	JPWR5: P12V, P5V
CPU	ARL-S LGA1851	JCPU0
XDP CONN	Samtec QSH 60-Pin CONN	JXDP1
Front Panel	12 x 2 Pin 2.54mm Box Header	JSSI1
Front USB2.0	5 x 2 Pin 2.0mm Box Header	JUSB1
Front USB3.2 Gen1x1	10 x 2 Pin 2.0mm Box Header	JUSB2
DIMM Sockets	287 Pin DDR5 DIMM	JEDEC Specified DDR5 Connector: JDIMM A0/A1/B0/B1
FAN CONN	4 x 1 Pin 2.54mm Box Header	JFAN1~JFAN6
Serial ATA	Slimline 8i CONN	SASHD_P1, SASHD_P2
eSPI Debug Port	2 x 6 Pin 2.0mm Box Header	JESPI1
VGA	2 x 8 Pin 2.0mm Box Header	JVGA2
M.2 2280	GEN4_M2_KEY_M_H=10.85MM (Stack type)	JNGFF4
Clear CMOS	3 Pin 2.0mm Header	JCMOS1
Battery Socket	2 Pin Socket	JBAT1
PMBUS Power Select	3 x 1 Pin 2.00mm Header	J15
PMBUS	5 x 1 Pin 2.54mm Box Header	JPMBUS1
Program CPLD FW	8 x 1 Pin 2.54mm Header	JTAG_CPLD1
BIOS SPI ROM Socket	SOIC-16 Socket	JSPI_BIOS1
EC COM	2 x 5 Pin 2.0mm Box Header	JCOM3
Intruder	2 x 1 Pin 2.0mm Box Header	JINTRUDER1
BMC COM	2 x 5 Pin 2.0mm Box Header	JCOM1, JCOM2
BMC GPIO	3 x 2 Pin 2.0mm Box Header	JBMC_GPIO1
BMC IPMB	4 x 1 Pin 2.0mm Box Header	JIPMB1
BMC Debug Port	3 x 1 Pin 2.0mm Header	JBMC_DP1
BMC Buzzer	2 x 1 Pin 2.54mm Header	JBUZZER1
BMC Reset	2 x 1 Pin 2.0mm Header	JBMC_RST1
BMC Force IP	2 x 1 Pin 2.0mm Header	JFORCE_IP1
BMC RST PSD	2 x 1 Pin 2.0mm Header	JRST_PWD1
BMC SPI ROM Socket	SOIC-16 Socket	JSPI_BMC1
BMC Socflash Enable	2 x 1 Pin 2.0mm Header	JSOC_FLASH1

Function	Description	Comments
BMC Bypass	3 x 1 Pin 2.0mm Header	J8
PCH Bypass	3 x 1 Pin 2.0mm Header	J36, J37, J39, J40
VRM SMB	3 x 1 Pin 2.0mm Header	PJ1
PCH GPIO	3 x 2 Pin 2.0mm Box Header	J2

3.4 External Port



Item	Description
1	UID LED with Button
2	COM port
3	VGA
4	2 x Display Ports
5	RJ45 10GbE
6	2 x USB3.2 + RJ45 2.5GbE
7	2 x USB3.2 + RJ45 1GbE (for BMC)

LAN LED Indicator

1G Speed LED Activity/Link LED	10G Speed LED Activity/Link LED
2.5G Speed LED Activity/Link LED	10G Speed LED Activity/Link LED

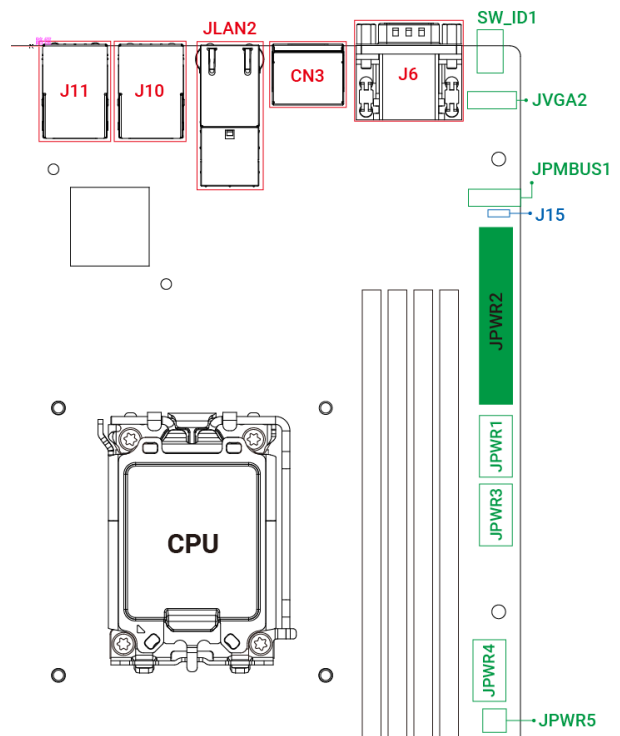
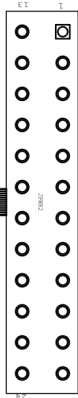
Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED 1GbE	Off	10M bps connection or no link.
	Green	100M bps connection.
	Orange	1G bps connection.
Speed LED 2.5GbE/10GbE	Off	100M/10M bps connection or no link.
	Orange	1G bps connection.
	Green	10G/2.5G bps connection.

3.5 Connector Definition

Power Supply Connector (JPWR2)

This is a 2x12-pin connector that provides the motherboard with power.

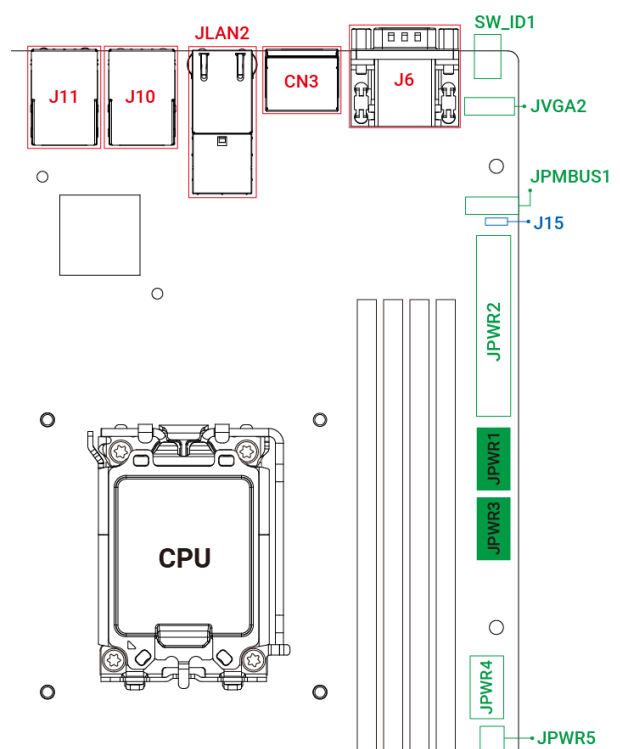
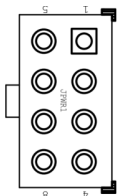
N.C.	13	1	N.C.
N.C.	14	2	N.C.
GND	15	3	GND
PSU_PSON_BUF_N	16	4	N.C.
GND	17	5	GND
GND	18	6	N.C.
GND	19	7	GND
N.C.	20	8	PSU_PWROK
N.C.	21	9	P5V_STBY_PSU
N.C.	22	10	P12V_PSU
N.C.	23	11	P12V_PSU
GND	24	12	N.C.



Power Supply Connector (JPWR1, JPWR3)

This is a 2x4-pin connector that provides the motherboard with power.

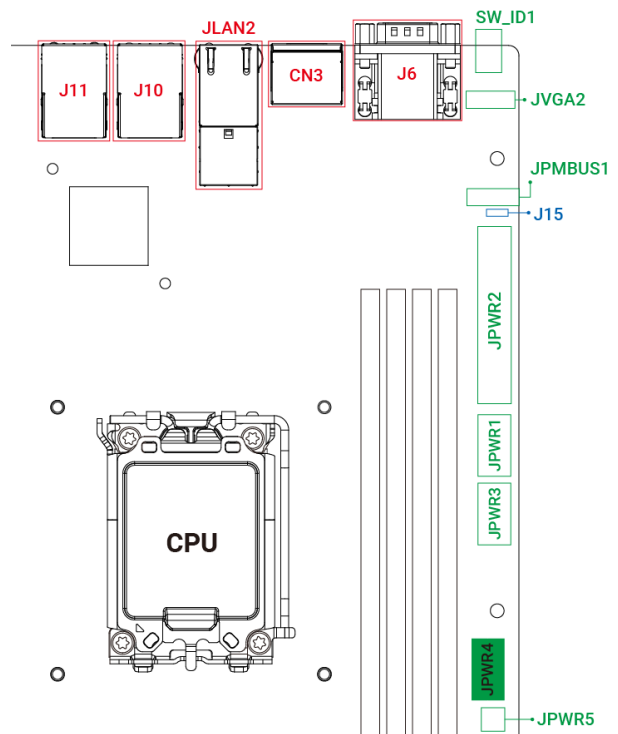
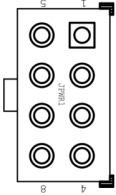
P12V_PSU	5	1	GND
P12V_PSU	6	2	GND
P12V_PSU	7	3	GND
P12V_PSU	8	4	GND



Power Supply Connector (JPWR4)

This is a 2x4-pin connector that provides the GPU card with power.

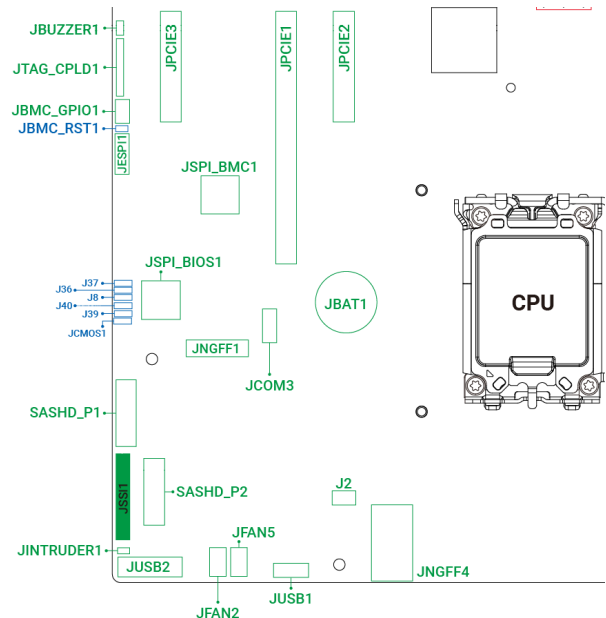
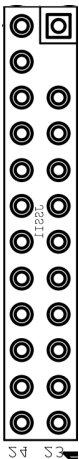
P12V	5	1	GND
P12V	6	2	GND
P12V	7	3	GND
P12V	8	4	GND



LED/Bezel Button Header (JSSI1)

This connector is a 2 x 12 Pin header.

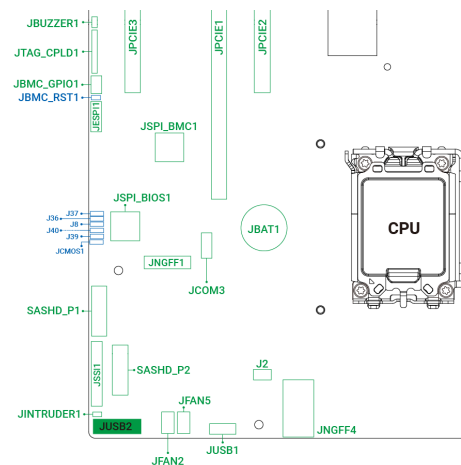
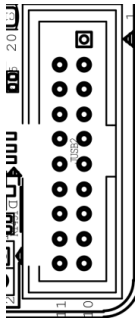
P3V3_STBY	2	1	FP_HDR_PWR_LED
P5V_DUAL	4	3	NC
ID_LED_OUT_N	6	5	FP_PWR_LED_L
SYS_HEALTH2#	8	7	HDD_LED_P
SYS_HEALTH#	10	9	HDD_LED_N
LAN1_ACTLED_PWR	12	11	FP_PWR_BTN_N
LAN1_ACTLED_N	14	13	GND
I2C_FRONT_SDA_R	16	15	FP_RST_BTN_N
I2C_FRONT_SCL_R	18	17	GND
CHASSIS_OPEN	20	19	BMC_ID_IN_N
LAN 2_ACTLED_PWR	22	21	FP_1WIRE_TEMP
LAN2_ACTLED_N	24	23	FP_NMI_BTN_N



Front I/O USB Header (JUSB2)

This is a 19-pin header that supports USB in the front panel.

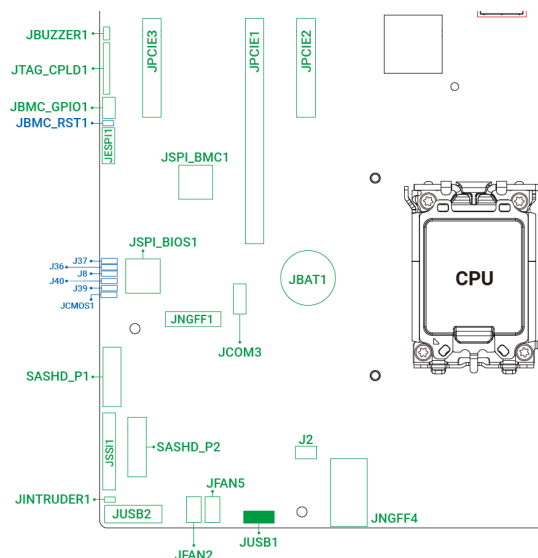
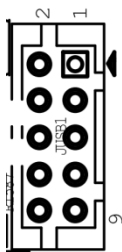
		1	P5V_USB23
P5V_USB23	19	2	USB3_PCH_JUSB2_RX_L_DN3
USB3_PCH_JUSB2_RX_L_DN2	18	3	USB3_PCH_JUSB2_RX_L_DP3
USB3_PCH_JUSB2_RX_L_DP2	17	4	GND
GND	16	5	USB3_PCH_JUSB2_TX_L_C_DN3
USB3_PCH_JUSB2_TX_L_C_DN2	15	6	USB3_PCH_JUSB2_TX_L_C_DP3
USB3_PCH_JUSB2_TX_L_C_DP2	14	7	GND
GND	13	8	USB2_PCH_JUSB2_L_DN3
USB2_PCH_JUSB2_L_DN2	12	9	USB2_PCH_JUSB2_L_DP3
USB2_PCH_JUSB2_L_DP2	11	10	USB_HUB_OC12_N(NC)



Front I/O USB2.0 Header (JUSB1)

This is a 2x5-pin header that supports USB in the front panel.

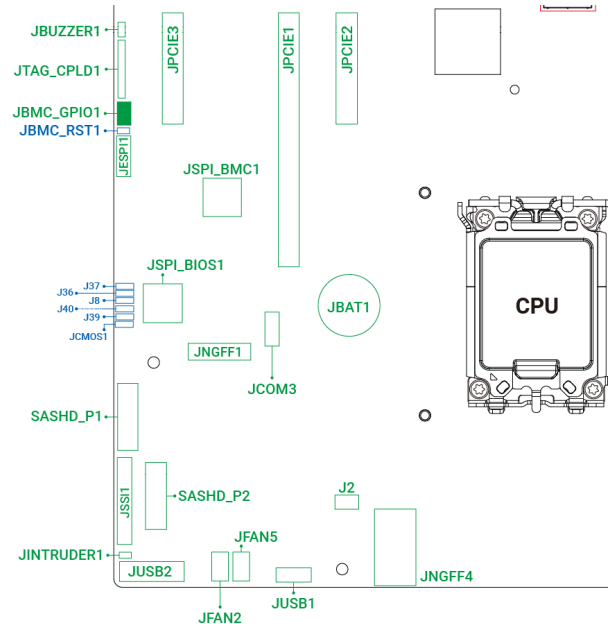
P5V_USB67	2	1	P5V_USB67
USB2_PCH_JUSB1_L_DN6	4	3	USB2_PCH_JUSB1_L_DN7
USB2_PCH_JUSB1_L_DP6	6	5	USB2_PCH_JUSB1_L_DP7
GND	8	7	GND
GND	10	9	USB_CONTROLLER_OC1x_N



BMC GPIO Header (JBMC_GPIO1)

This 2x3-pin header is used to provide BMC GPIO functionality.

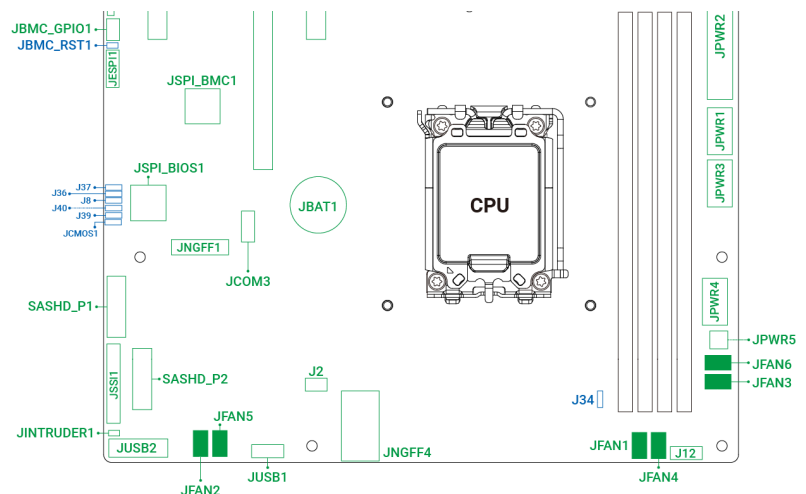
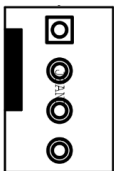
RACK_EXTRST_R_N	2	1	GND
BMC_GPY1	4	3	I2C_G16_SDA_R
BMC_GPY0	6	5	I2C_G16_SCL_R



Fan Header (JFAN1~JFAN6)

This 1x4-pin FAN header.

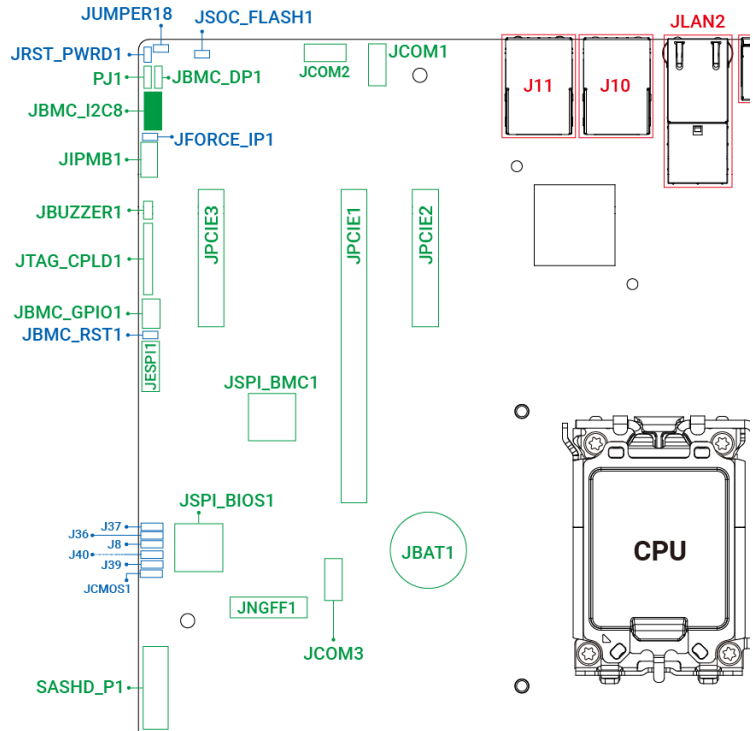
1	GND
2	P12V_FANx
3	FANx_TACH
4	FANx_PWM_R



BMC I2C header (JBMC_I2C8)

This is a 1x4-pin connector that is used to provide BMC I2C8 functionality.

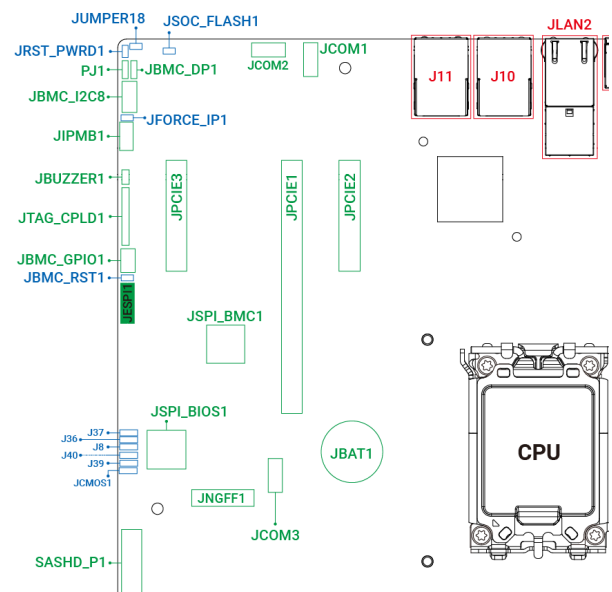
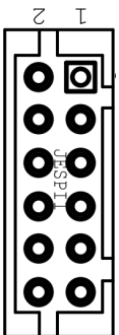
1	BMC_I2C_G8_SCL
2	BMC_I2C_G8_SDA
3	BP_BMC_I2C8_ALERT_N
4	GND



eSPI Debug header (JESPI1)

This is a 2x6-pin header that is used to provide eSPI Debug Port functionality.

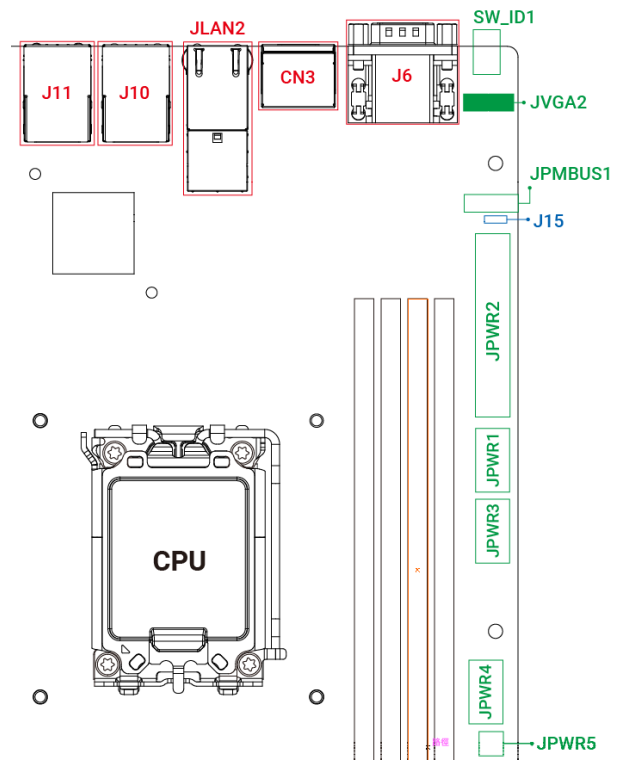
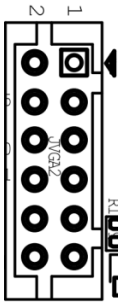
ESPI_DBP_CLK	2	1	GND
ESPI_DBP_CS_N	4	3	NC
ESPI_DBP_RST_N	6	5	ESPI_DBP_ALERT_N
ESPI_DBP_D3	8	7	ESPI_DBP_D2
P3V3_STBY	10	9	ESPI_DBP_D1
ESPI_DBP_D0	12	11	GND



VGA header (JVGA2)

This is a 2x6-pin header that is used to provide front VGA functionality.

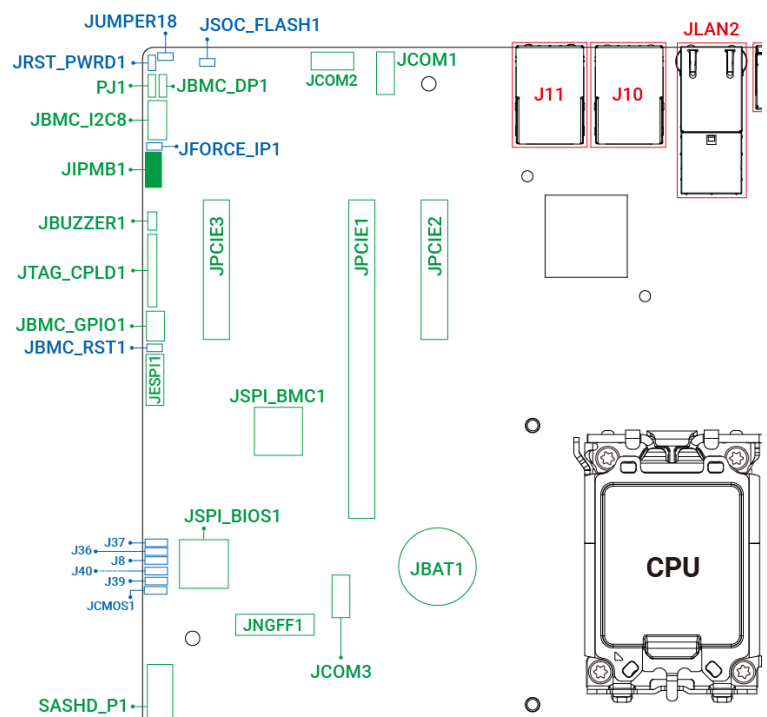
GND	2	1	DVO_5V
DACROA	4	3	GND
GND	6	5	DDC_DATA0
DACGOA	8	7	AVSYNCO
GND	10	9	AVSYNCO
DACBOA	12	11	DDC_CLKO



BMC IPMB header (JIPMB1)

This 1x4-pin header is used to provide BMC I2C14 IPMB functionality.

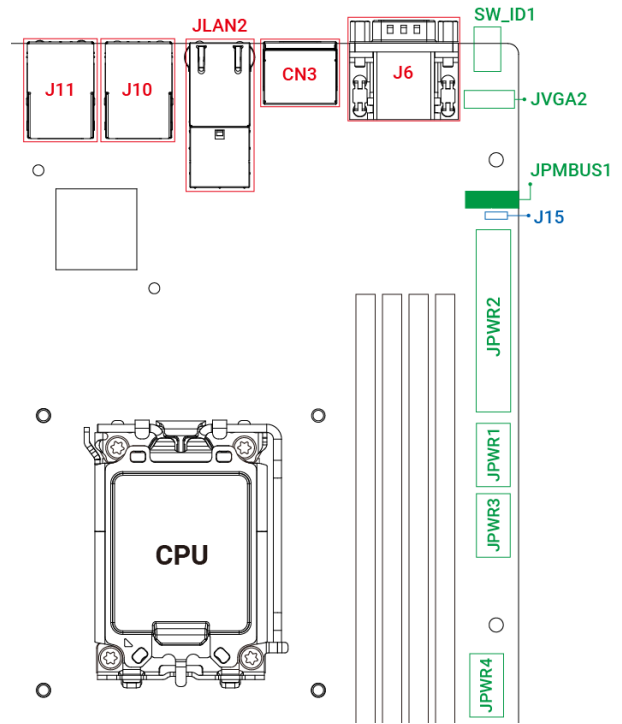
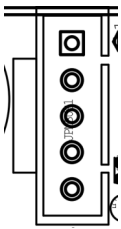
1	I2C_G14_SDA_R
2	GND
3	I2C_G14_SCL_R
4	NC



PMBUS header (JPMBUS1)

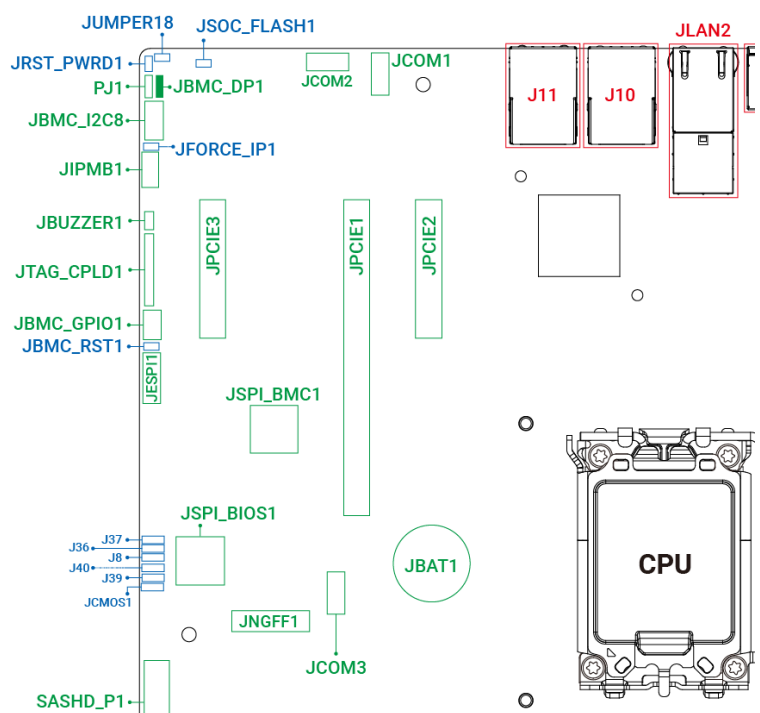
This 1x5-pin header is used to provide PMBus functionality.

1	SMB_PMBUS_SCL
2	SMB_PMBUS_SDA
3	PMBUS_ALERT_N_C
4	GND
5	P5V_P3V3_STBY

**BMC Debug port header (JBMC_DP1)**

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

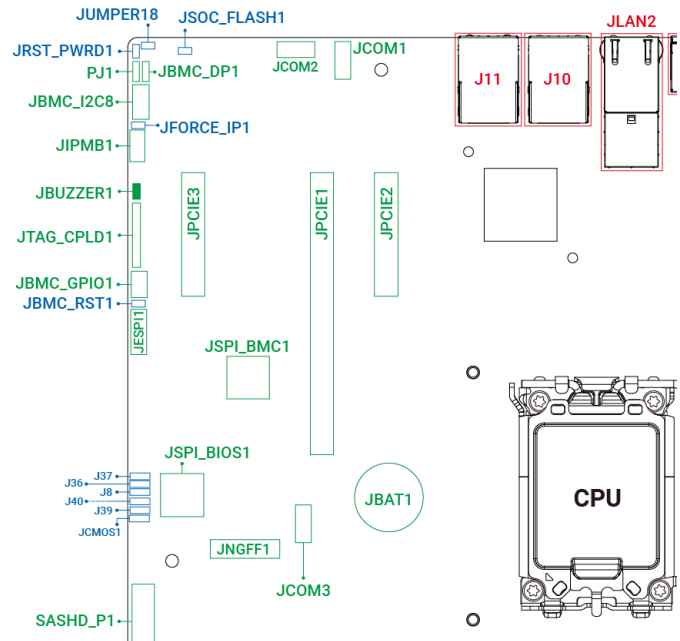
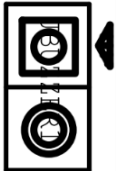
1	SPE_TXD
2	GND
3	SPE_RXD



BUZZER header (JBUZZER1)

This is a 1x2-pin header that is used to provide Buzzer functionality.

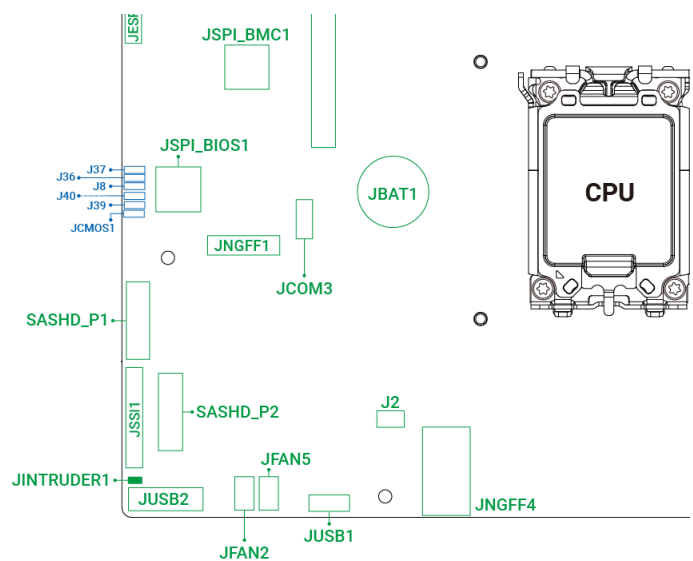
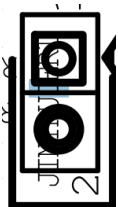
1	P5V_DUAL
2	BMC_BUZZER-



Chassis Intrusion header (JINTRUDER1)

This is a 1x2-pin header that is used to provide chassis intrusion functionality.

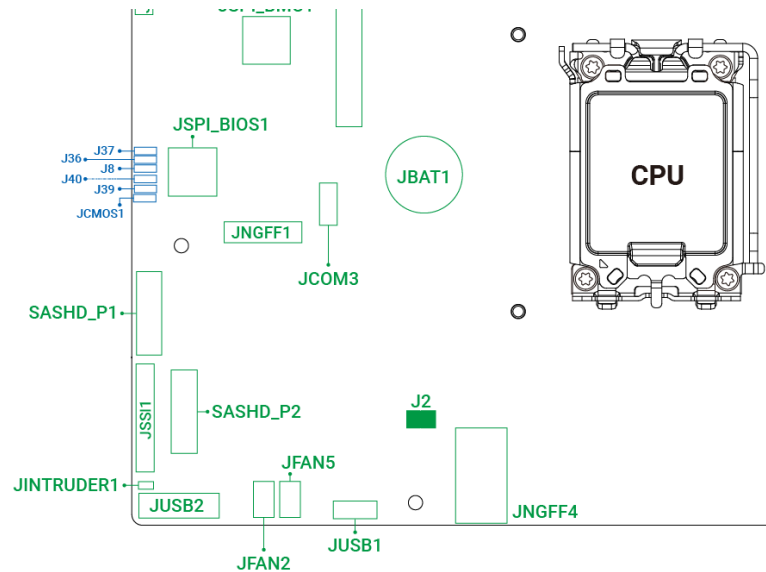
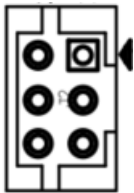
1	CHASSIS_OPEN
2	GND



PCH GPIO header (J2)

This is a 2x3-pin header that is used to provide PCH GPIO functionality.

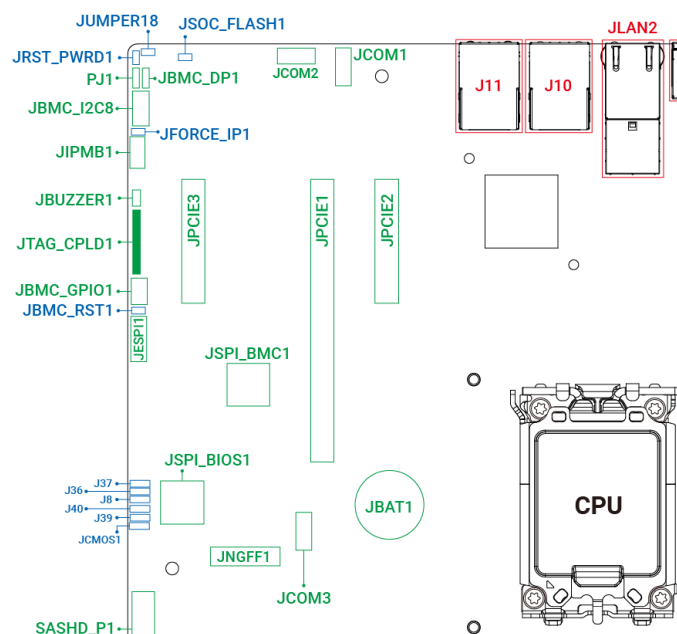
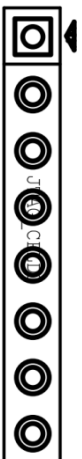
PCH_IO0_HDR_R	2	1	GND
PCH_IO1_HDR_R	4	3	P5V_AUX
PCH_IO2_HDR_R	6	5	P3V3_A



CPLD JTAG header (JTAG_CPLD1)

This 1x8-pin header is used to provide CPLD JTAG functionality.

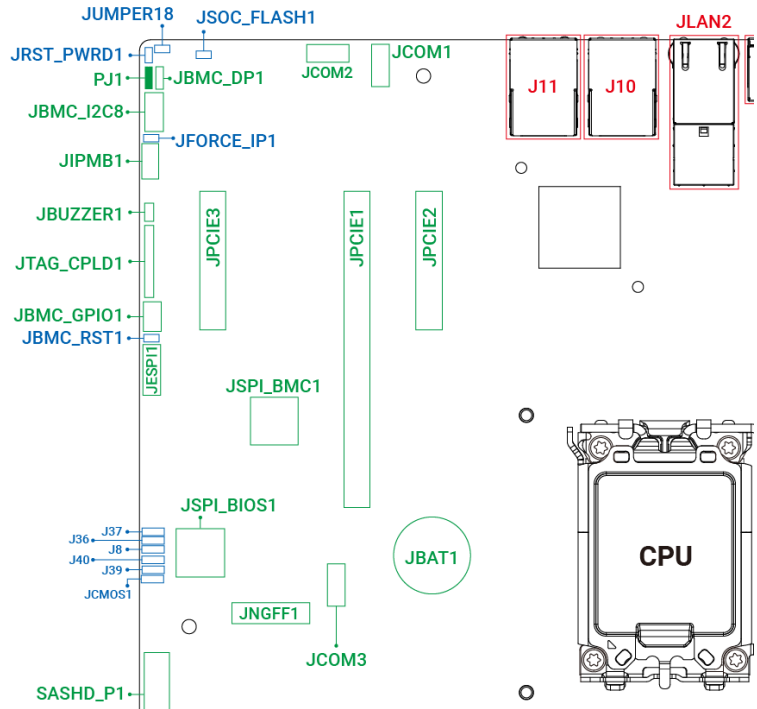
1	P3V3_STBY
2	JTAG_CPLD_TDO
3	JTAG_CPLD_TDI
4	JTAG_HDR_PRSENT_N
5	NC
6	JTAG_CPLD_TMS
7	GND
8	JTAG_CPLD_TCK



VRM SMB header (PJ1)

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

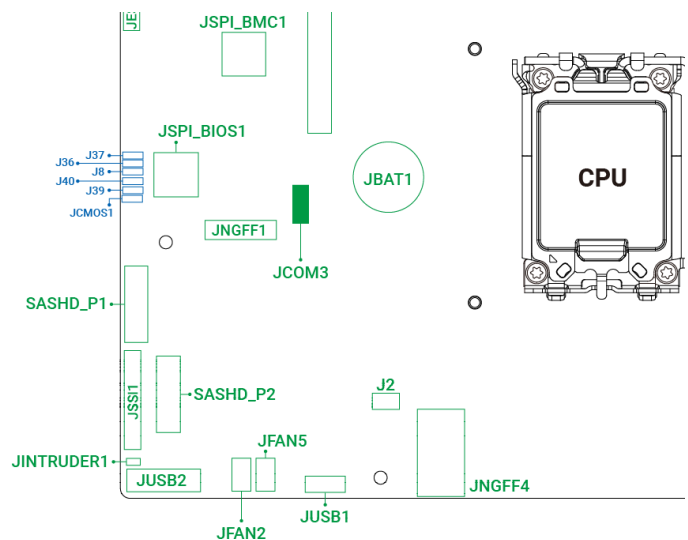
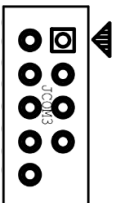
1	I2C_IMVP_SCL
2	GND
3	I2C_IMVP_SDA



EC Debug port header (JCOM3)

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

SPC_DCD	2	1	SPC_DSR
SPC_RXD	4	3	SPC_RTS
SPC_TXD	6	5	SPC_CTS
SPC_DTR	8	7	SPC_RI
GND	10		



3.6 Jumper Setting

BMC Reset Jumper (JBMC_RST1)

JBMC_RST1	Setting	
Short	Reset BMC	
Open	Normal	Default

BMC RESET header (JBMC_RST1)

This 1x2-pin header is used to provide BMC RESET functionality.

1	BMC_RESET
2	GND



Clear CMOS Jumper (JCMOS1)

JBMC_RST	Setting	
Pin1-2	Clear Secure RTC	
Pin2-3	Clear RTC	
Open	Normal	Default

BMC Reset Password Jumper (JRST_PWD1)

JRST_PWD1	Setting	
Short	Reset BMC Password	
Open	Normal	Default

PCH SPI Flash Jumper (J36, J37)

J36	J37	Setting	
Pin1-2	Pin1-2	PCH/EC to Flash Bypass	Default

BMC Force IP Jumper (JFORCE_IP1)

JFORCE_IP1	Setting	
Short	Force BMC IP	
Open	Normal	Default

BMC Socflash Configurations Jumper (JSOC_FLASH1)

JSOC_FLASH1	Setting	
Short	Enable	
Open	Disable	Default

BMC SPI MUX Jumper (J8)

J8	Setting	
Pin1-2	BMC to Flash Bypass	Default

PMBUS Power select Jumper (J15)

J15	Setting	
Pin1-2	P3V3_STBY	Default
Pin2-3	P5V_DUAL	

PSU Type select Jumper (Jumper18)

Jumper18	Setting
Short	ATX Power
Open	12V only

3.7 LED

3.7.1 Rear Chassis LEDs

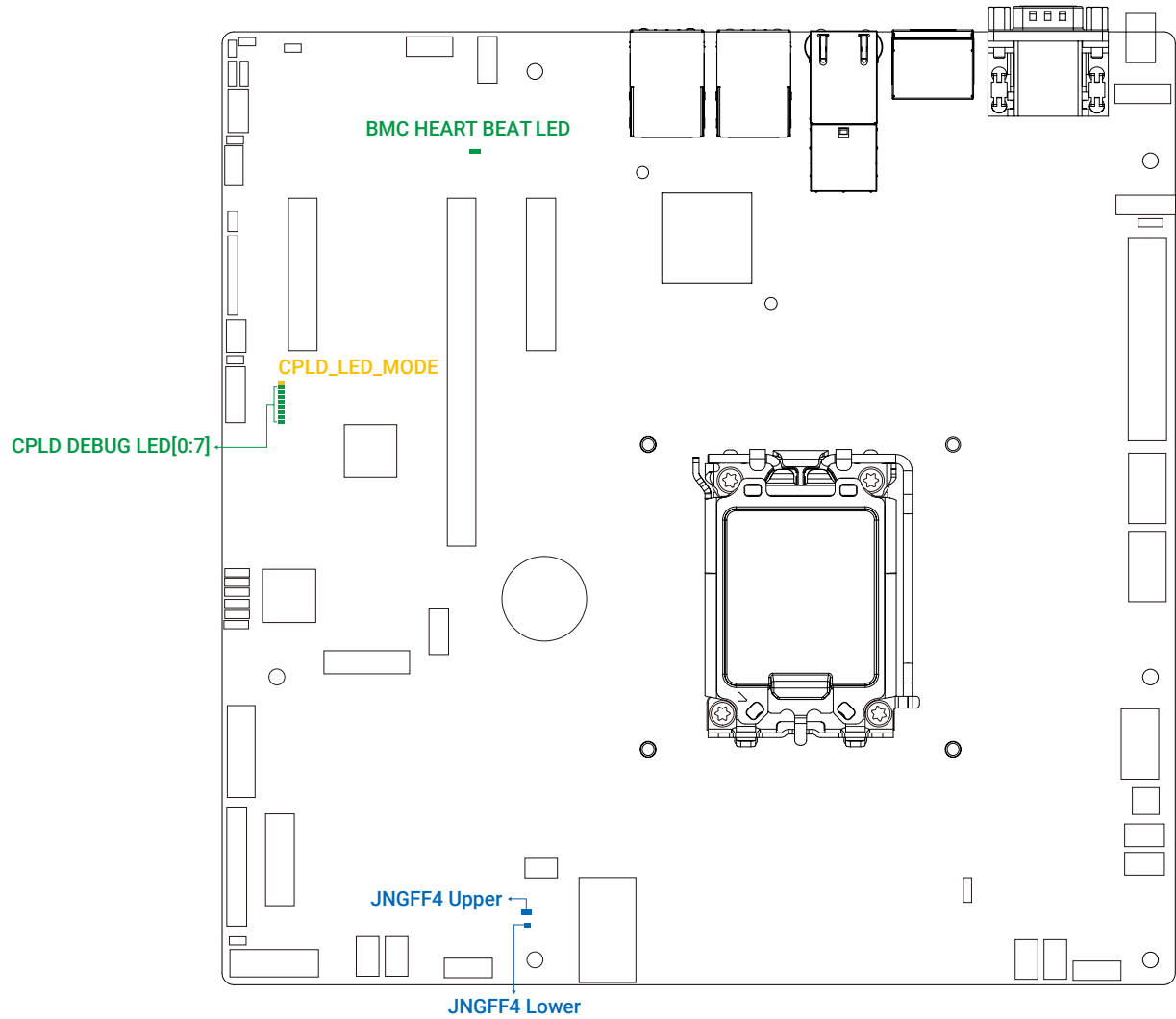
The RJ45 port/LED should be connected to Vaux (standby) voltage in order to provide the same functionality as stand-up NIC cards for WOL support.

Item		Color	Behavior
JLAN2(Upper)	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	10G : Green, 1G: Orange, No connect: Off
JLAN2(Lower)	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	10G : Green, 1G: Orange, No connect: Off
J11	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off
J10	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	2.5G : Green, 1G : Orange, 100M/10M/No connect: Off

3.7.2 Internal LEDs

Item	Color	Behavior
HEART BEAT LED	Green (Blinking)	BMC activity detected 1. 80Hz : Secure boot failed.(LED 50% on) 2. 20Hz : Boot passed with ABR(Show about 3s and then exit) 3. 4Hz : ARM CA7 is reading flash or SRAM 4. 1Hz : ARM CA7 is reading peripherals 5. 0.5Hz : ARM CA7 is reading DRAM 6. 0.2Hz : No ARM CA7 read access cycles 7. 0.1Hz : No ARM CA7 read access cycles over 6~8s. Stay in mode 8 if there is no ARM CA7 reading access. Exit to mode 4-6 if there is any ARM CA7 reading access
	Green	BMC is not active
CPLD DEBUG LED[0:7]	Green/Off	Refer to CPLD LED mapping table
CPLD_LED_MODE	Yellow/Off	Yellow: Port80 MODE, OFF: Sequence MODE
JNGFF4 ACTIVITY LED	Blue (Blinking)	JNGFF4 Upper activity detected
	Off	JNGFF4 Upper is not active
	Blue (Blinking)	JNGFF4 Lower activity detected
	Off	JNGFF4 Lower is not active

3.7.3 LEDs Placement



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

4.2 BIOS 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.
Security	Sets passwords and security functions.
Boot	Sets boot options such as Quick Boot or USB Boot.
Save & Exit	Save changes and exit, discard changes and exit, discard changes, or load optimal or fail-safe defaults.
Socket Configuration	Allows configuration of socket settings such as processor, Common RefCode, UPI, and memory configurataion.
MEBx	Configuration locked after EndOfPost.
Server Management	Allows configuration of timer, System Event Log, and BMC network.

4.2.2 Startup

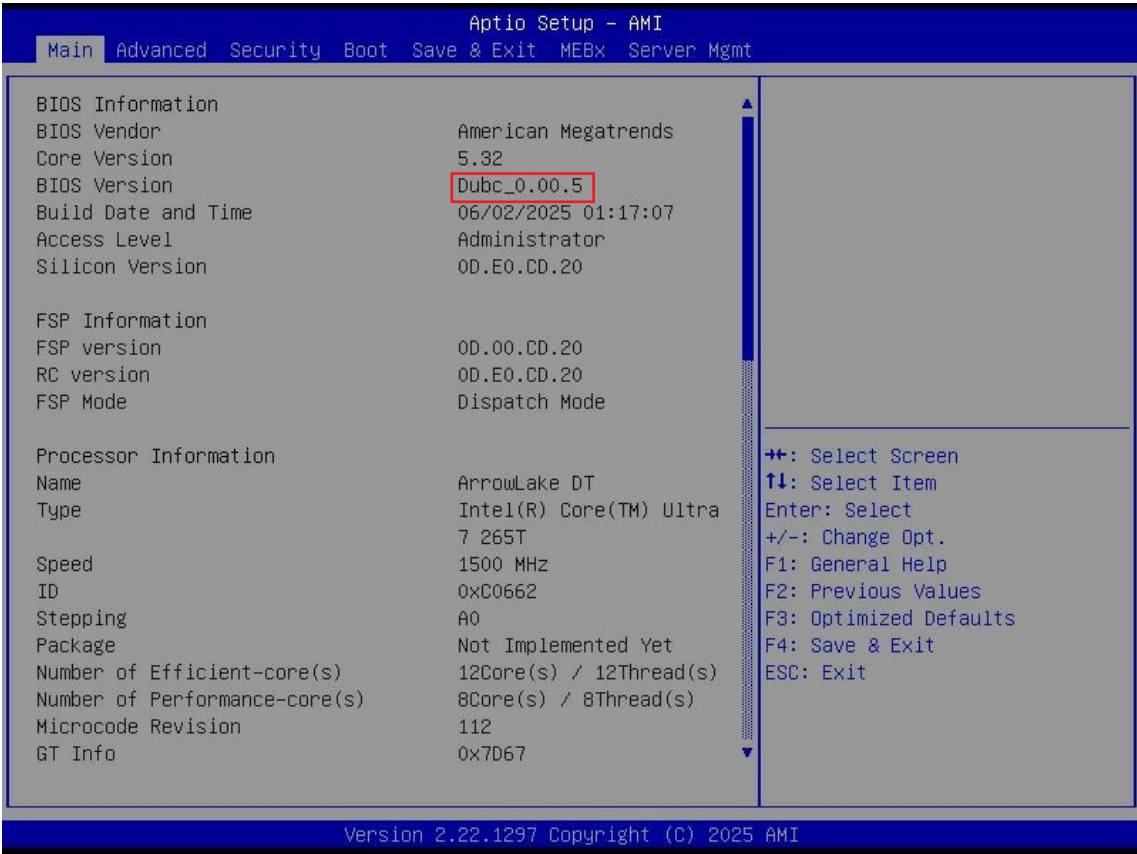
① Press **DEL** or **ESC** to run the BIOS setup procedure.

```
Version 2.22.1297. Copyright (C) 2025 AMI
BIOS Date: 06/03/2025 17:32:44 Ver: Dubc_0.00.5
Press <DEL> or <ESC> to enter setup.
Press <F7> to Boot Menu.
Press <F12> to Network Boot.
```

```
BMC IP Channel 1 : 192.168. 24.167
BMC IP Channel 8 : 0. 0. 0. 0
```

A2

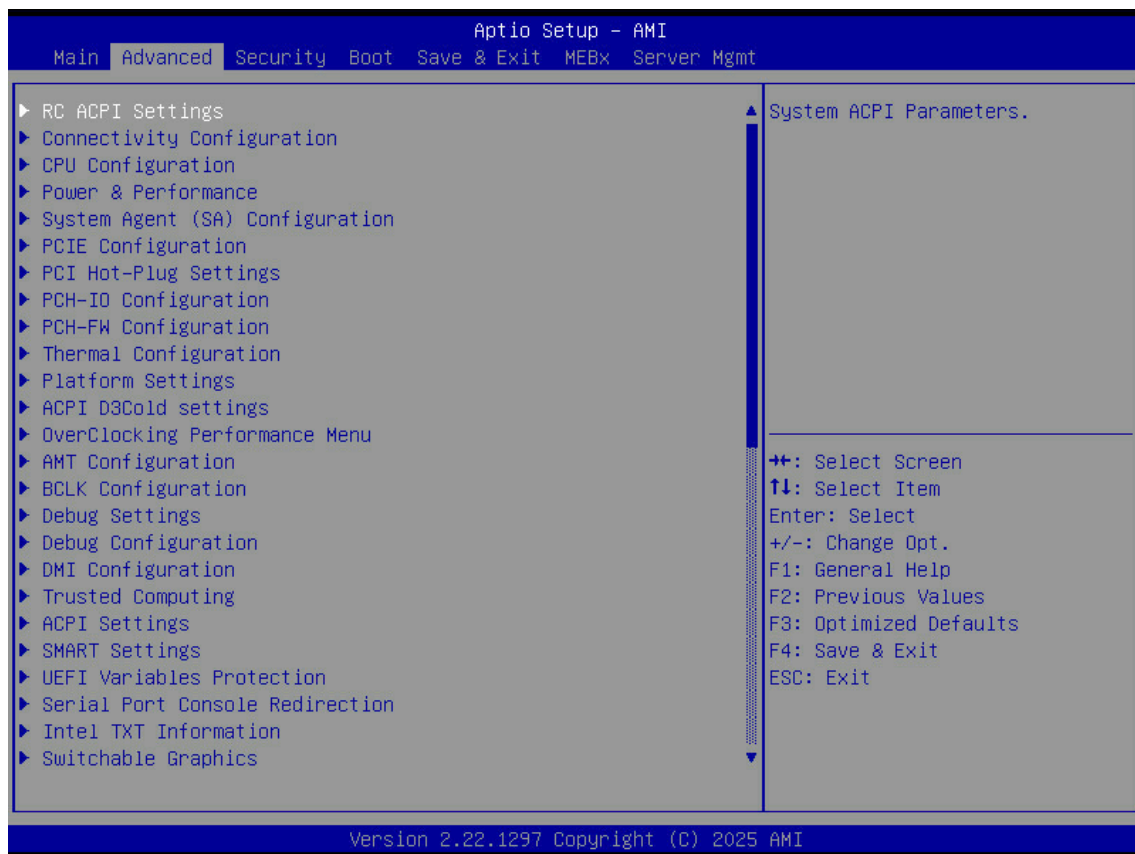
4.3 Main



4.3.1 Main

Main	
System Language	Choose the system default language
System Date	Configures the current date. Set the date. Use tab to switch between date elements.
System Time	Configures the current time. Set the time. Use tab to switch between time elements.

4.4 Advanced



4.4.1 RC ACPI Settings

System ACPI Parameters.

RC ACPI Settings	
PTID Support	PTID Support ▶ 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 Enabled Disabled
BDAT ACPI Table Support	Enables support for the BDAT ACPI table. Enable ▶ Disable
Wake System from S5 via RTC	Enable or disable System wake on alarm event. When enabled, System will wake on the hr::min::sec specified 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
D3 Setting for Storage	Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3 Note some HCK tests might not support 1.3. Disabled ▶ D3Hot D3Cold
DLRM Setting for Storage	Dynamic Link (PCIe) Rate management (DLRM) for Storage to reduce active power usage in D3 ▶ Disabled Enabled

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	
PUIS Enable	Enable/Disable Power-Up In Standby (PUIS) feature set allows devices to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the host to sequence the spin-up of devices.			
	Enable		► Disable	
EC Notification	Sends EC notification of Low Power S0 Idle State			
	► Enable		Disable	
EC CS Debug Light	When EC enters Low Power S0 Idle State, the CAPS LOCK light will be turned on			
	Enable		► Disable	
EC Low Power Mode	This option controls whether EC will go to Low power mode during Low Power S0 Idle State			
	► Enable		Disable	
Sensor Standby	Enable/Disable Sensor standby mode			
	Enable		► Disable	
CS PL1 Limit	Limit PL1 (Power Limit 1) while in Connected Standby			
	Enable		► Disable	
PEP Constraints Configuration	Control which controllers get included in PEP constraint list.			
	PEP CPU	Add CPU in PEP mitigation list		
		Disable		► Enable
	PEP Graphics	Add Gfx in PEP mitigation list		
		Disable		► Enable
	PEP IPU	Add IPU in PEP mitigation list		
		Disable		► Enable
	PEP GNA	Add GNA in PEP mitigation list		
		Disable		► Enable
	PEP SATA	Add Storage device in PEP mitigation list		
		No Constraint	Adapter D0/F1	Raid Volume0
	PEP enumerated SATA ports	Add enumerated SATA ports in PEP Constraint list		
		► Disable		Enable
	PEP PCIe Storage	Add PCIe root ports (storage) in PEP mitigation list		
		No Constraint	► D0/F1	
	PEP PCIe LAN	Add PCIe LAN device in PEP mitigation list		
No Constraint		D0/F1		► D3
PEP PCIe WLAN	Add PCIe WLAN device in PEP mitigation list			
	No Constraint	D0/F1		► D3
PEP PCIe GFX	Add PCIe GFX device in PEP mitigation list			
	No Constraint	D0/F1		► D3
PEP PCIe Other	Add PCIe Other device in PEP mitigation list			
	► No Constraint		D0/F1	D3
PEP UART	Add UART in PEP mitigation list			
	Disable		► Enable	

PEP Constraints Configuration	PEP I2C0	Adds I2C in PEP mitigation list Disabled	► Enabled
	PEP I2C1	Adds I2C in PEP mitigation list Disabled	► Enabled
	PEP I2C2	Adds I2C in PEP mitigation list Disabled	► Enabled
	PEP I2C3	Adds I2C in PEP mitigation list Disabled	► Enabled
	PEP I2C4	Adds I2C in PEP mitigation list Disabled	► Enabled
	PEP I2C5	Adds I2C in PEP mitigation list Disabled	► Enabled
	PEP SPI	Add SPI in PEP mitigation list Disabled	► Enabled
	PEP XHCI	Add XHCI in PEP mitigation list Disabled	► Enabled
	PEP CSME	Add CSME in PEP mitigation list Disabled	► Enabled
	PEP HECI3	Add HECI3 in PEP mitigation list Disabled	► Enabled
	PEP LAN(GBE)	Add HECI3 in PEP mitigation list Disabled	► Enabled
	PEP THC0	Add THC in PEP mitigation list. Applies only if THCx has assigned port Disabled	► Enabled
	PEP THC1	Add THC in PEP mitigation list. Applies only if THCx has assigned port Disabled	► Enabled
	PEP TCSS	Add TCSS IPs in PEP mitigation list Disabled	► Enabled
	PEP VMD	Add TCSS IPs in PEP mitigation list Disabled	► Enabled
	PEP NPU	Add NPU (Neural Processing Unit) in PEP mitigation list Disabled	► Enabled
LPIT Residency Counter	Select Residency Counter C10		
PCI Delay Optimization	Experimental ACPI additions for FW latency optimizations ► Disabled		
MSI enabled	When disabled, MSI support is disabled in FADT Disabled		
PCIe delay between _OFF _ON	Delay will be applied to all PCIe devices between OFF and ON methods to make sure minimum delay is passed before calling the ON sequence except WWAN, (Range 50ms to 500ms) 200		

4.4.2 CPU Configuration

CPU Configuration Parameters.

CPU Configuration								
Efficient-core Information	Display the E-core Information							
Performance-core	Display the P-core Information							
CPU Flex Ratio Override	Enable/Disable CPU Flex Ratio Programming							
	▶ Disabled				Enabled			
Intel (VMX) Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.							
	Disabled				▶ Enabled			
AVX	Enable/Disable the AVX and AVX2 Instructions							
	Disabled				▶ Enabled			
Active Performance-cores	Number of P-cores to enable in each processor package. Note: Number of Cores and E-Cores are looked at together. When both are {0,0}, Pcode will enable all cores.							
	▶ All	7	6	5	4	3	2	1
Active Efficient-cores	Number of E-cores to enable in each processor package. Note: Number of Cores and E-Cores are looked at together. When both are {0,0}, Pcode will enable all cores.							
	▶ All	15	14	13	12	11	10	9
	8	7	6	5	4	3	2	1
BIST	Enable/Disable BIST (Built-In Self Test) on reset							
	▶ Disabled				Enabled			
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)							
	Disabled				▶ Enabled			
MachineCheck	Enable/Disable Machine Check							
	Disabled				▶ Enabled			

MonitorMWait	Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop		
	Disabled		► Enabled
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.		
	► Disabled		Enabled
Total Memory Encryption	Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks. When this option is configured as 'Enabled', 'VT-d' option must be 'Enabled'. This option will be grayed out when 'VT-d' option is configured as 'Disabled'.		
	► Disabled		Enabled
X2APIC Enable	Enable/Disable X2APIC Operating Mode. When this option is configured as 'Enabled', 'VT-d' option must be 'Enabled' and 'X2APIC Opt Out' option must be 'Disabled' as well. This option will be grayed out when 'VT-d' option is configured as 'Disabled'.		
	Disabled		► Enabled
Legacy Game Compatibility Mode	When enabled, Pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when LED is off.		
	► Disabled		Enabled

4.4.3 Power & Performance

Power & Performance Options.

Power & Performance				
CPU - Power Management Control	PCU - Power Management Control Options			
	Boot Max Frequency	Enable/Disable Boot Maximum Frequency in CPU strap.		
		Disabled		► Enabled
	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.		
		Disabled		► Enabled
	Race To Halt (RTH)	Enable/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power.		
		Disabled		► Enabled
	Intel(R) Speed Shift Technology	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.		
		Disabled		► Enabled
	Resource Priority Feature	Enable/Disable Resource Priority Feature support.		
		► Disabled		Enabled
	Per Core P State OS control mode	Enable/Disable Per Core P state OS control mode. When set, the highest core request is used for all other core requests.		
		Disabled		► Enabled
	HwP Autonomous Per Core P State	Disable Autonomous PCPS Autonomous will request the same value for all cores all the time.		
		Disabled		► Enabled
	HwP Autonomous EPP Groupin	Enable EPP grouping Autonomous will request the same values for all cores with same EPP. Disable EPP grouping autonomous will not necessarily request same values for all cores with same EPP.		
		► Disabled		Enabled
	HwP Lock	Enable/Disable HWP Lock support in Misc Power Management MSR.		
		Disabled		► Enabled
	Turbo Mode	Enable/Disable processor Turbo Mode.		
		Disabled		► Enabled

CPU - Power Management Control	View Configure Turbo Options	View/Configure Turbo Options		
		Turbo Ratio Limit Options	View/Configure Turbo Ratio Limit Options	
			P-core Turbo Ratio Limit Core0	Performance-core Turbo Ratio Limit Core0 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio0. If value is zero, this entry is ignored. 1
			P-core Turbo Ratio Limit Core1	Performance-core Turbo Ratio Limit Core1 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio1. If value is zero, this entry is ignored. 2
			P-core Turbo Ratio Limit Core2	Performance-core Turbo Ratio Limit Core2 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio2. If value is zero, this entry is ignored. 3
			P-core Turbo Ratio Limit Core3	Performance-core Turbo Ratio Limit Core3 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio3. If value is zero, this entry is ignored. 4
			P-core Turbo Ratio Limit Core4	Performance-core Turbo Ratio Limit Core4 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio4. If value is zero, this entry is ignored. 5
			P-core Turbo Ratio Limit Core5	Performance-core Turbo Ratio Limit Core5 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio5. If value is zero, this entry is ignored. 6
			P-core Turbo Ratio Limit Core6	Performance-core Turbo Ratio Limit Core6 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio6. If value is zero, this entry is ignored. 7
			P-core Turbo Ratio Limit Core7	Performance-core Turbo Ratio Limit Core6 defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio6. If value is zero, this entry is ignored. 8

CPU - Power Management Control	View Configure Turbo Options	Turbo Ratio Limit Options	P-core Turbo Ratio Limit Ratio0 (TRLR)	Performance-core Turbo Ratio Limit Ratio0 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio0 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. Please check each active cores 54
			P-core Turbo Ratio Limit Ratio1 (TRLR)	Performance-core Turbo Ratio Limit Ratio1 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio1 must be <= to Turbo Ratio Limit Ratio0. 54
			P-core Turbo Ratio Limit Ratio2 (TRLR)	Performance-core Turbo Ratio Limit Ratio2 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio2 must be <= to Turbo Ratio Limit Ratio1. 51
			P-core Turbo Ratio Limit Ratio3 (TRLR)	Performance-core Turbo Ratio Limit Ratio3 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio3 must be <= to Turbo Ratio Limit Ratio2. 51
			P-core Turbo Ratio Limit Ratio4 (TRLR)	Performance-core Turbo Ratio Limit Ratio4 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio4 must be <= to Turbo Ratio Limit Ratio3. 51
			P-core Turbo Ratio Limit Ratio5 (TRLR)	Performance-core Turbo Ratio Limit Ratio5 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio5 must be <= to Turbo Ratio Limit Ratio4. 51

CPU - Power Management Control	View Configure Turbo Options	Turbo Ratio Limit Options	P-core Turbo Ratio Limit Ratio6 (TRLR)	Performance-core Turbo Ratio Limit Ratio6 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio6 must be <= to Turbo Ratio Limit Ratio5. 47
			P-core Turbo Ratio Limit Ratio7 (TRLR)	Performance-core Turbo Ratio Limit Ratio7 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode). This Turbo Ratio Limit Ratio7 must be <= to Turbo Ratio Limit Ratio6. 47
			E-core Turbo Ratio Limit CoreCount0	Efficient-core Turbo Ratio Limit CoreCount0 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio0. If value is zero, this entry is ignored. 1
			E-core Turbo Ratio Limit CoreCount1	Efficient-core Turbo Ratio Limit CoreCount1 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio1. If value is zero, this entry is ignored. 2
			E-core Turbo Ratio Limit CoreCount2	Efficient-core Turbo Ratio Limit CoreCount2 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio2. If value is zero, this entry is ignored. 3
			E-core Turbo Ratio Limit CoreCount3	Efficient-core Turbo Ratio Limit CoreCount3 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio3. If value is zero, this entry is ignored. 4
			E-core Turbo Ratio Limit CoreCount4	Efficient-core Turbo Ratio Limit CoreCount4 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio4. If value is zero, this entry is ignored. 6

CPU - Power Management Control	View Configure Turbo Options	Turbo Ratio Limit Options	E-core Turbo Ratio Limit CoreCount5	Efficient-core Turbo Ratio Limit CoreCount5 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio5. If value is zero, this entry is ignored. 8
			E-core Turbo Ratio Limit CoreCount6	Efficient-core Turbo Ratio Limit CoreCount6 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio6. If value is zero, this entry is ignored. 12
			E-core Turbo Ratio Limit CoreCount7	Efficient-core Turbo Ratio Limit CoreCount7 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio7. If value is zero, this entry is ignored. 16
			E-core Turbo Ratio Limit Ratio0	Efficient-core Turbo Ratio Limit Ratio0 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount0. 46
			E-core Turbo Ratio Limit Ratio1	Efficient-core Turbo Ratio Limit Ratio1 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount1. 46
			E-core Turbo Ratio Limit Ratio2	Efficient-core Turbo Ratio Limit Ratio2 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount2. 46

CPU - Power Management Control	View Configure Turbo Options	Turbo Ratio Limit Options	E-core Turbo Ratio Limit Ratio3	Efficient-core Turbo Ratio Limit Ratio3 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount3.	46
			E-core Turbo Ratio Limit Ratio4	Efficient-core Turbo Ratio Limit Ratio4 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount4.	46
			E-core Turbo Ratio Limit Ratio5	Efficient-core Turbo Ratio Limit Ratio5 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount5.	46
			E-core Turbo Ratio Limit Ratio6	Efficient-core Turbo Ratio Limit Ratio6 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount6.	46
			E-core Turbo Ratio Limit Ratio7	Efficient-core Turbo Ratio Limit Ratio7 defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount7.	45
		Energy Efficient P-state	Enable/Disable Energy Efficient P-state feature. When set to 0, will disable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function will read 0 indicating no support for Energy Efficient policy setting. When set to 1 will enable access to ENERGY_PERFORMANCE_BIAS MSR and CPUID Function will read 1 indicating Energy Efficient policy setting is supported.		
			Disabled		

CPU - Power Management Control	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.			
		► Disabled		Enabled		
		Power Limit 1 Override	Enable/Disable Power Limit 1 override. If this option is disabled, BIOS will program the default values for Power Limit 1 and Power Limit 1 Time Window.			
		► Disabled		Enabled		
		Power Limit 2 Override	Enable/Disable Power Limit 2 override. If this option is disabled, BIOS will program the default values for Power Limit 2.			
		Disabled		► Enabled		
		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*Processor Base Power (TDP). For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.			
		0				
		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.			
		► Disabled		Enabled		
	CPU VR Settings	CPU VR Settings				
		PSYS Slope	PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO.			
		0				
		PSYS Offset	PSYS Offset defined in 1/1000 increments. Range is 0-128000. For an offset of 25.348, enter 25348.			
		0				
		PSYS Prefix	Sets the offset value as positive or negative.			
		► +		-		
		PSYS PMax Power	PSYS PMax power, defined in 1/8 Watt or Percent increments. For Watts, Range is 0-8191 (ex. for 125W, enter 1000). For ATX12VO Percent, Range is 0-1600 (ex. for 200%, enter 1600).Uses BIOS VR mailbox command 0xB.			
		0				
		Vsys/Psys Critical	Vsys/Psys Critical Enable or disable			
		► Disabled		Psys Critical	Vsys Critical	
		Assertion Deglitch Mantissa	Assertion Deglitch Mantissa 0x4F[7-3]. Assertion Deglitch = 2s * Mantissa * 2^(Exponent)			
		1				

CPU - Power Management Control	CPU VR Settings	Assertion Deglitch Exponent	Assertion Deglitch Exponent 0x4F[3-0]. Assertion Deglitch = 2s * Mantissa * 2 ^(Exponent)	
			0	
		De assertion Deglitch Mantissa	De Assertion Deglitch Mantissa 0x49[7-3]. Assertion Deglitch = 2s * Mantissa * 2 ^(Exponent)	
			13	
		De assertion Deglitch Exponent	De Assertion Deglitch Exponent 0x49[3-0]. Assertion Deglitch = 2s * Mantissa * 2 ^(Exponent)	
			2	
		SVID Stabilization Delay	Configure SVID Stabilization Delay (in us) being used for the FVM feature when it is enabled. Note that this delay applies to all SVID domains equally (no unique values possible for IA/GT/SA).	
			3	
		Acoustic Noise Settings	Configure Acoustic Noise Settings for Core, GT and SA domains.	
			Acoustic Noise Mitigation	Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state
				► Disabled Enabled
		Efficiency/Performance VR Settings	Efficiency/Performance VR Settings	
			VR Config Enable	VR Config Enable
				► Disabled Enabled
			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.
				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.
				0
			PS Current Threshold1	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				80

CPU - Power Management Control	CPU VR Settings	Efficiency/ Performance VR Settings	PS Current Threshold2	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				20
			PS Current Threshold3	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				4
			PS3 Enable	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.
				Disabled ▶ Enabled
			PS4 Enable	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled.
				Disabled ▶ Enabled
			IMON Slope	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO.
				0
			IMON Offset	IMON Offset defined in 1/1000 increments. Range is 0-128000. For an offset of 25.348, enter 25348.
				0
			IMON Prefix	Sets the offset value as positive or negative.
				▶+ -
			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.
				0
			Core VR Fast Vmode	Core VR Fast Vmode. Use to control Core Fast Vmode Enable/Disable.
				Disabled ▶ Enabled
			VR Fast Vmode ICC Limit	Voltage Regulator Fast Vmode ICC Limit. A value of 400 = 100A. This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments.
				0

CPU - Power Management Control	CPU VR Settings	Efficiency/ Performance VR Settings	VR Fast Vmode Offset	Voltage Regulator Fast Vmode Offset. This value represents the ICC Max Offset(dV/dT) to be configured if Fast Vmode is enabled. IGNORED if Fast Vmode ICC LIMIT = 0. The value is represented in 1 mV increments. 0 = Use processor default setting. Highly recommend to keep at the default setting.			
			0				
			VR Voltage Limit	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV.			
			0				
			TDC Enable	TDC Enable. 0- Disable, 1 - Enable			
			Disabled		►Enabled		
			TDC Current Limit	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = AUTO.			
			0				
			TDC Time Window	VR TDC Time Window, value in seconds. Range from 1s to 448s. AUTO means using processor default setting.			
			►Auto		1sec	2sec	3sec
			4sec		5sec	6sec	7sec
			8sec		10sec	12sec	14sec
			16sec		20sec	24sec	28sec
			32sec		40sec	48sec	56sec
			64sec		80sec	96sec	112sec
			128sec		160sec	192sec	224sec
			256sec		320sec	384sec	448sec
			TDC Lock	TDC Lock			
			►Disabled		Enabled		
			IRMS	Enable/Disable IRMS - Current root mean square			
			►Disabled		Enabled		
			PS1 to PS0 Dynamic Cutoff Enable	PS1 to PS0 Dynamic Cutoff Enable/Disable			
			►Disabled		Enabled		
			PS2 to PS1 Dynamic Cutoff Enable	PS2 to PS1 Dynamic Cutoff Enable/Disable			
			►Disabled		Enabled		
			VCC Demotion Shutdown Threshold	User configured time threshold in msec. Range is 0~255 msec.			
			0				

CPU - Power Management Control	CPU VR Settings	Efficiency/Performance VR Settings	CEP Enable	Enable/Disable CEP (Current Excursion Protection) Support. ► Enabled Disabled
			SIRP Enable	Enable/Disable SIRP (SoC Iccmax Reactive Protection) Support. Enabled Disabled
			GT VR Settings	
		GT VR Settings	VR Config Enable	VR Config Enable ► Enabled Disabled
			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. 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. 0
			PS Current Threshold1	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO. 80

CPU - Power Management Control	CPU VR Settings	GT VR Settings	PS Current Threshold2	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				20
			PS Current Threshold3	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				4
			PS3 Enable	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.
				Disabled ☐ Enabled ☒
			PS4 Enable	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled.
				Disabled ☐ Enabled ☒
			IMON Slope	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO.
				0
			IMON Offset	IMON Offset defined in 1/1000 increments. Range is 0-128000. For an offset of 25.348, enter 25348.
				0
			IMON Prefix	Sets the offset value as positive or negative.
				☒ + ☐ -
			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.
				0
			GT VR Fast Vmode	GT VR Fast Vmode. Use to control GT Fast Vmode Enable/Disable.
				Disabled ☐ Enabled ☒
			VR Fast Vmode ICC Limit	Voltage Regulator Fast Vmode ICC Limit. A value of 400 = 100A. This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments.
				0

CPU - Power Management Control	CPU VR Settings	GT VR Settings	VR Fast Vmode Offset	Voltage Regulator Fast Vmode Offset. This value represents the ICC Max Offset(dV/dT) to be configured if Fast Vmode is enabled. IGNORED if Fast Vmode ICC LIMIT = 0. The value is represented in 1 mV increments. 0 = Use processor default setting. Highly recommend to keep at the default setting.			
			0				
			VR Voltage Limit	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV.			
			0				
			TDC Enable	TDC Enable. 0- Disable, 1 - Enable			
			Disabled		►Enabled		
			TDC Current Limit	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = AUTO.			
			0				
			TDC Time Window	VR TDC Time Window, value in seconds. Range from 1s to 448s. AUTO means using processor default setting.			
			►Auto		1sec	2sec	3sec
			4sec		5sec	6sec	7sec
			8sec		10sec	12sec	14sec
			16sec		20sec	24sec	28sec
			32sec		40sec	48sec	56sec
			64sec		80sec	96sec	112sec
			128sec		160sec	192sec	224sec
			256sec		320sec	384sec	448sec
			TDC Lock	TDC Lock			
			►Disabled		Enabled		
			IRMS	Enable/Disable IRMS - Current root mean square			
			►Disabled		Enabled		
			PS1 to PS0 Dynamic Cutoff Enable	PS1 to PS0 Dynamic Cutoff Enable/Disable			
			►Disabled		Enabled		
			PS2 to PS1 Dynamic Cutoff Enable	PS2 to PS1 Dynamic Cutoff Enable/Disable			
			►Disabled		Enabled		
			CEP Enable	Enable/Disable CEP (Current Excursion Protection) Support.			
			Disabled		►Enabled		

CPU - Power Management Control	CPU VR Settings	SA VR Settings	SA VR Settings		
			VR Config Enable	VR Config Enable	
				►Enabled	Disabled
			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.	
				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.	
				0	
			PS Current Threshold1	PS Current Threshold1, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.	
				80	

CPU - Power Management Control	CPU VR Settings	SA VR Settings	PS Current Threshold2	PS Current Threshold2, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				40
			PS Current Threshold3	PS Current Threshold3, defined in 1/4 A increments. A value of 400 = 100A. Range 0-512, which translates to 0-128A. 0 = AUTO.
				4
			PS3 Enable	PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.
				Disabled ☐ Enabled ☒
			PS4 Enable	PS4 Enable/Disable. 0 - Disabled, 1 - Enabled.
				Disabled ☐ Enabled ☒
			IMON Slope	IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO.
				0
			IMON Offset	IMON Offset defined in 1/1000 increments. Range is 0-128000. For an offset of 25.348, enter 25348.
				0
			IMON Prefix	Sets the offset value as positive or negative.
				☒ + ☐ -
			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.
				0
			SA VR Fast Vmode	SA VR Fast Vmode. Use to control SA Fast Vmode Enable/Disable.
				Disabled ☐ Enabled ☒
			VR Fast Vmode ICC Limit	Voltage Regulator Fast Vmode ICC Limit. A value of 400 = 100A. This value represents the current threshold where the VR would initiate reactive protection if Fast Vmode is enabled. The value is represented in 1/4 A increments.
				0

CPU - Power Management Control	CPU VR Settings	SA VR Settings	VR Fast Vmode Offset	Voltage Regulator Fast Vmode Offset. This value represents the ICC Max Offset(dV/dT) to be configured if Fast Vmode is enabled. IGNORED if Fast Vmode ICC LIMIT = 0. The value is represented in 1 mV increments. 0 = Use processor default setting. Highly recommend to keep at the default setting.			
				0			
			VR Voltage Limit	Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV.			
				0			
			TDC Enable	TDC Enable. 0- Disable, 1 - Enable			
				Disabled ▶ Enabled			
			TDC Current Limit	TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = AUTO.			
				0			
			TDC Time Window	VR TDC Time Window, value in seconds. Range from 1s to 448s. AUTO means using processor default setting.			
				▶ Auto	1sec	2sec	3sec
				4sec	5sec	6sec	7sec
				8sec	10sec	12sec	14sec
				16sec	20sec	24sec	28sec
				32sec	40sec	48sec	56sec
				64sec	80sec	96sec	112sec
				128sec	160sec	192sec	224sec
				256sec	320sec	384sec	448sec
			TDC Lock	TDC Lock			
				▶ Disabled Enabled			
			IRMS	Enable/Disable IRMS - Current root mean square			
				▶ Disabled Enabled			
			PS1 to PS0 Dynamic Cutoff Enable	PS1 to PS0 Dynamic Cutoff Enable/Disable			
				▶ Disabled Enabled			
			PS2 to PS1 Dynamic Cutoff Enable	PS2 to PS1 Dynamic Cutoff Enable/Disable			
				▶ Disabled Enabled			
			CEP Enable	Enable/Disable CEP (Current Excursion Protection) Support.			
				Disabled ▶ Enabled			

CPU - Power Management Control	CPU VR Settings	RFI Settings	RFI Settings				
			Global DLVR RFI Mitigation Control	Enable/Disable Global DLVR RFI Mitigation Control			
				Disabled	►Enabled		
			DLVR SSC Value	DLVR SSC in percentage with multiple of 0.25%. 0 = 0%, 31 = 7.75%.			
				6			
	DLVR RFI Frequency	DLVR RFI Frequency in MHz.					
		1370					
	Platform PL1 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.					
		►Disabled			Enabled		
	Platform PL2 Enable	Enable/Disable Platform Power Limit 2 programming. If this option is disabled, BIOS will program the default values for Platform Power Limit 2.					
		►Disabled			Enabled		
	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.					
		►Disabled			Enabled		
	Power Limit 4 Boost	Configure Power Limit 4 Boost in Watts. The value 0 means disable.					
		0					
	C states	Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.					
		Disabled			►Enabled		
	C-State Auto Demotion	Configure C-State Auto Demotion					
		Disabled			►C1		
	C-State Un-demotion	Configure C-State Un-demotion					
		Disabled			►C1		
	Package C-State Demotion	Package C-State Demotion					
		Disabled			►Enabled		
	Package C-State Un-demotion	Package C-State Un-demotion					
		Disabled			►Enabled		
	CState Pre-Wake	Disable - to 1 to disable the Cstate Pre-Wake					
		Disabled			►Enabled		
	IO MWAIT Redirection	When set, will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+offset to MWAIT(offset)					
	►Disabled			Enabled			
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.						
	C0/C1	C2	C3	C6			
	C7	C7S	C8	C9			
	C10	Cpu Default	►Auto				
DC6 Latency WA	DC6 Latency WA						
	►Disabled			Enabled			
Thermal Monitor	Enable/Disable Thermal Monitor						
	Disabled			►Enabled			
Interrupt Redirection Mode Selection	Interrupt Redirection Mode Select for Logical Interrupts						
	►Fixed Priority	Round robin	Hash Vector	No Change			
Timed MWAIT	Enable/Disable Timed MWAIT Support						
	►Disabled			Enabled			

CPU - Power Management Control	Custom P-state Table	Enable/Disable Timed MWAIT Support			
		Number of P states	Sets the number of custom P-states. At least 2 states must be present. 0		
	Energy Performance Gain	Enable/disable Energy Performance Gain. ▶ Disabled Enabled			
	CCF AutoGV	Enable/disable CCF AutoGV. Disabled ▶ Enabled			
	Power Floor Management	This option is to disable SoC's aggressive throttling to manage floor power (minimum power consumption). Disabling this might effectively raise power floor of the SoC and may lead to stability issues. Disabled ▶ Enabled			
	Display Disconnect	When this option is enabled, SoC can disconnect secondary/external display to lower SoC floor power. When disabled, display disconnect will not be used by SoC. Disabled ▶ Enabled			
	PCIe Gen Speed Downgrade	When this option is enabled, SoC can reduce PCIe Gen speed to lower SoC floor power. When disabled, Pcie Gen speed reduction option will not be used by SoC. Disabled ▶ Enabled			
	Power Limit 3 Settings	Power Limit 3 Settings			
		Power Limit 3 Override	Enable/Disable Power Limit 3 override. If this option is disabled, BIOS will leave the hardware default values for Power Limit 3 and Power Limit 3 Time Window. ▶ Disabled Enabled		
	CPU Lock Configuration	CPU Lock Configuration			
CFG Lock		Configure MSR to CFG Lock bit. Disabled ▶ Enabled			
GT/Media - Power Management Control	GT/Media - Power Management Control Options				
	RC6(Render Standby)	Check to enable render standby support. Disabled ▶ Enabled			
		MC6(Media Standby)	Check to enable Media standby support. Disabled ▶ Enabled		
	Maximum GT frequency		Maximum GT frequency limited by the user. Choose between 1650MHz (RPN) and 6000MHz (RP0). Value beyond the range will be clipped to min/max supported by SKU		
		▶ Default Max Frequency	100Mhz	150Mhz	200Mhz
		250Mhz	300Mhz	350Mhz	400Mhz
		450Mhz	500Mhz	550Mhz	600Mhz
		650Mhz	700Mhz	750Mhz	800Mhz
		850Mhz	900Mhz	950Mhz	1000Mhz
		1050Mhz	1100Mhz	1150Mhz	1200Mhz
		Disable Turbo GT frequency	Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited ▶ Disabled Enabled		
	Overclocking Lock		Enable/Disable Overclocking Lock. Disabled ▶ Enabled		

4.4.4 System Agent (SA) Configuration

System Agent (SA) Parameters.

System Agent (SA) Configuration				
Memory Configuration	Validation Menu	Validation Menu for internal validation.		
		Turn Around Timing Delta Programming	Knobs to override default timings. 0 is no override.	
			tRRSG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tRRDG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tRRDR Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tRRDD Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWRSG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWRDG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWRDR Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWRDD Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWWSG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWWDG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWWDR Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tWWDD Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tRWSG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0
			tRWDG Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127] 0

Memory Configuration	Validation Menu	Turn Around Timing Delta Programming	tRWDR Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127]			
				0			
			tRWDD Delta	0 - Auto. Signed TAT delta is (Value - 128). Input value range of [1..255] will give a TAT delta range of [-127..127]			
				0			
	Memory Thermal Configuration	Memory Power and Thermal Throttling	Memory Thermal Configuration Options				
				MC Refresh Rate	Select refresh rate on the MC		
					►NORMAL Refresh	2x Refresh	4x Refresh
				Throttler CKEMin Defeature	On, Off		
					►Enabled	Disabled	
				Throttler CKEMin Timer	Timer value for CKEMin, range[255;0]. Req'd min of SC_ROUND_T + BYTE_LENGTH (4)		
					0		
			Allow Opp Ref Below Write Threshold	Allow opportunistic refreshes while we don't exit power down.			
				►Enabled	Disabled		
				Write Threshold	Number of writes that can be accumulated while CKE is low before CKE is asserted.		
			0				
	Memory Training Algorithms	Enable/Disable Memory Training Algorithms.					
		Early Command Training	Early Command Training				
			Disabled	►Enabled			
		SenseAmp Offset Training	SenseAmp Offset Training				
			Disabled	►Enabled			
		Early ReadMPR Timing Centering 2D	Early ReadMPR Timing Centering 2D				
			Disabled	►Enabled			
		Read MPR Training	Read MPR Training				
			Disabled	►Enabled			
		Receive Enable Training	Receive Enable Training				
			Disabled	►Enabled			
		Jedec Write Leveling	Jedec Write Leveling				
			Disabled	►Enabled			
Early Write Time Centering 2D		Early Write Time Centering 2D					
		Disabled	►Enabled				
Early Read Time Centering 2D		Early Read Time Centering 2D					
		Disabled	►Enabled				
Unmatched Write Time Centering 1D		Unmatched Write Time Centering 1D					
	Disabled	►Enabled					
Write Timing Centering 1D	Write Timing Centering 1D						
	Disabled	►Enabled					
Write Voltage Centering 1D	Write Voltage Centering 1D						
	Disabled	►Enabled					
Read Timing Centering 1D	Read Timing Centering 1D						
	Disabled	►Enabled					
Read Voltage Centering 1D	Read Voltage Centering 1D						
	Disabled	►Enabled					
DDR5 ODT Timing Config	DDR5 ODT Timing Config						
	Disabled	►Enabled					

Memory Configuration	Memory Training Algorithms	View Pin Calibration	View Pin Calibration Disabled ▶ Enabled
		Read DQS ODT Training*	Read DQS On-Die Termination Training Disabled ▶ Enabled
		Read DQ ODT Training	Read DQ On-Die Termination Training Disabled ▶ Enabled
		Read Equalization Training	Read Equalization Training Disabled ▶ Enabled
		Read CTLE Training	Read CTLE Training Disabled ▶ Enabled
		Post Package Repair	Post Package Repair ▶ Disabled Enabled
		Write Timing Centering 2D	Write Timing Centering 2D Disabled ▶ Enabled
		Read Timing Centering 2D	Read Timing Centering 2D Disabled ▶ Enabled
		Write Voltage Centering 2D	Write Voltage Centering 2D Disabled ▶ Enabled
		Read Voltage Centering 2D	Read Voltage Centering 2D Disabled ▶ Enabled
		RxVref Per-Bit Training	RxVref Per-Bit Training Disabled ▶ Enabled
		Command Voltage Centering	Command Voltage Centering Disabled ▶ Enabled
		Late Command Training	Late Command Training Disabled ▶ Enabled
		Turn Around Timing Optimization	Turn Around Timing Optimization Disabled ▶ Enabled
		Rank Margin Tool	Rank Margin Tool ▶ Disabled Enabled
		Rank Margin Tool	Rank Margin Tool Disabled ▶ Enabled
		LVR Auto Trim	LVR Auto Trim Disabled ▶ Enabled
		DIMM SPD Alias Test	Test to determine if the SPD has been corrupted to cause memory aliasing. Disabled ▶ Enabled
		Retrain Margin Check	Retrain Margin Check Disabled ▶ Enabled
		Retrain Margin Check	Retrain Margin Check Disabled ▶ Enabled
		Dimm ODT Training*	Dimm On-Die Termination Training Disabled ▶ Enabled
		DIMM RON Training*	DIMM RON Training* Disabled ▶ Enabled
		TxDqTCO Comp Training*	TxDqTCO Comp Training* Disabled ▶ Enabled
		ClkTCO Comp Training*	ClkTCO Comp Training* Disabled ▶ Enabled
		CMD/CTL CLK Slew Rate	CMD/CTL CLK Slew Rate Disabled ▶ Enabled
		CMD/CTL Drive Strength	CMD/CTL Drive Strength Disabled ▶ Enabled

Memory Configuration	Memory Training Algorithms	CMD/CTL Tx Equalization	CMD/CTL Tx Equalization Disabled ▶ Enabled
		DIMM CA ODT Training	DIMM CA ODT Training Disabled ▶ Enabled
		DIMM CA ODT Split Training	DIMM CA ODT Split Training ▶ Disabled Enabled
		CMD/CTL Drive Strength Split	CMD/CTL Drive Strength Split ▶ Disabled Enabled
		CMD CTL CLK Slew Split Rate	CMD CTL CLK Slew Split Rate ▶ Disabled Enabled
		Write DQ/DQS Retrain	Write DQ/DQS Retrain Disabled ▶ Enabled
		Power Saving Meter Update	Power Saving Meter Update Disabled ▶ Enabled
		Pre Training Comp Calibration	Pre Training Comp Calibration Disabled ▶ Enabled
		Read Vref Decap Training*	Read Vref Decap Training* Disabled ▶ Enabled
		Vddq Training	Vddq Training Disabled ▶ Enabled
		Rank Margin Tool Per Bit	Rank Margin Tool Per Bit ▶ Disabled Enabled
		DQ/DQS Swizzle Training	DQ/DQS Swizzle Training Disabled ▶ Enabled
		Ref PI Calibration	Ref PI Calibration Disabled ▶ Enabled
		Rx SAL Calibration	Rx SAL Calibration Disabled ▶ Enabled
		VccClk FF Offset Correction	VccClk FF Offset Correction Disabled ▶ Enabled
		Duty Cycle Correction Training	Duty Cycle Correction Training Disabled ▶ Enabled
		Duty Cycle Correction Downstream Training	Duty Cycle Correction Downstream Training - PI Serializer/LUT Disabled ▶ Enabled
		Duty Cycle Correction QCLK Calibration	Duty Cycle Correction QCLK Calibration Disabled ▶ Enabled
		Duty Cycle Correction Rise/Fall Training	Duty Cycle Correction Rise/Fall Training Disabled ▶ Enabled
		Functional Duty Cycle Correction for DDR5 DQS	Functional Duty Cycle Correction for DDR5 DQS Disabled ▶ Enabled
		Functional Duty Cycle Correction for DDR5 CLK	Functional Duty Cycle Correction for DDR5 CLK Disabled ▶ Enabled
		Functional Duty Cycle Correction for LP5 WCK	Functional Duty Cycle Correction for LP5 WCK Disabled ▶ Enabled
		Functional Duty Cycle Correction for Data DQ	Functional Duty Cycle Correction for Data DQ Disabled ▶ Enabled

Memory Configuration	Memory Training Algorithms	Data PI Linearity Calibration	Data PI Linearity Calibration			
		Disabled			▶ Enabled	
		Ddr5 Rx Cross-Talk Cancellation	Ddr5 Rx Cross-Talk Cancellation			
		Disabled			▶ Enabled	
		Duty Cycle Correction for LP5 DCA	Duty Cycle Correction for LP5 DCA			
		Disabled			▶ Enabled	
		Unmatched Rx Calibration	Unmatched Rx Calibration			
		Disabled			▶ Enabled	
		Write Rank-to-Rank Training	Write Rank-to-Rank Training			
		Disabled			▶ Enabled	
		Read Rank-to-Rank Training	Read Rank-to-Rank Training			
		Disabled			▶ Enabled	
		Comp Optimization	Comp Optimization			
	Disabled			▶ Enabled		
	DIMM DFE Training	DIMM DFE Training				
	Disabled			▶ Enabled		
	Write Drive Strength	Write Drive Strength				
	Disabled			▶ Enabled		
	Write Equalizationq	Write Equalizationq				
	Disabled			▶ Enabled		
	Margin Check Limit	Checks Margin to Limit to see if next boot memory needs to be retrain				
	Disabled			▶ L1	L2	Both
	Overclocking	Memory Overclocking Menu				
		Realtime Memory Timing	Enable/Disable realtime memory timings. When enabled, the system will allow performing realtime memory timing changes after MRC_DONE.			
		▶ Disabled			Enabled	
		Memory profile	Select DIMM timing profile. The below values start with the currently running values and don't auto populate.			
		▶ Default SPD profile			Custom Profile	
		RecompTarget	RecompTarget Menu			
		Dimm Odt	Dimm Odt Menu			
		Memory Voltage VDD	Memory Voltage Override (Vdd) at DRAM Side. 0 = no override			
		0				
		Memory Voltage VDDQ	Memory Voltage VDDQ			
		0				
Memory Voltage VPP		Memory Voltage VPP				
0						
DIIBwEn[0]		DIIBwEn[0], for 1067 (0..7)				
0						
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						
RFI Setting	RFI Setting Menu					
	Global DDR RFI Mitigation	This is an option intended to Enable/Disable DDR-RFIM feature for Connectivity This RFI mitigation feature may result in temporary slowdown of the DDR speed.				
	Disabled			▶ Enabled		

Memory Configuration	MRC Safe Mode Override	Bit mask to enable the use of the input safe mode values. When a bit is set, the corresponding safe mode input field value will be used instead of the pre-defined MRC safe mode configuration. The definitions are: [0] Enable DdrSafeMode override, [1] Enable McSafeMode override, [2] Enable MrcSafeMode override, [3] Enable Training Algorithm (TrainingEnables) safe mode override, [4] Enable SaGv safe mode override							
		0							
	Memory Test on Warm Boot	Enable Or Disable Base Memory Test Run on Warm Boot							
		Disabled				► Enabled			
	Maximum Memory Frequency	Maximum Memory Frequency Selections in Mhz.							
		► Auto	1067	1333	1600	1867	2133	2400	2667
		2933	3200	3467	3600	3733	4000	4200	4267
		4400	4600	4800	5000	5200	5400	5600	5800
		6000	6200	6400	6600	6800	7000	7200	7400
		7600	7800	8000	8200	8400	8600	8800	9000
		9200	9400	9600	9800	10000	10200	10400	10600
		10800	11000	11200	11400	11600	11800	12000	12200
		12400	12600	12800					
	HOB Buffer Size	Size to set HOB Buffer							
		► Auto		1B		1KB		Max (assuming 63KB total HOB size)	
	ECC Support	Enable/disable DDR Ecc Support							
		Disabled				► Enabled			
	Max TOLUD	Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on largest MMIO length of installed graphic controller							
		► Dynamic		1GB		1.25GB		1.5GB	
		1.75GB		2GB		2.25GB		2.5GB	
		2.75GB		3GB		3.25GB		3.5GB	
	SAGV	System Agent Geyserville. Disabled or Enabled.							
		Disabled				► Enabled			
	SA GV Mask	System Agent Geyserville. Set the BIT(s) for which points to use in frequency switching.							
		Enable Points: 1st and 2nd		Enable Points: 1st and 2nd		► Enable All Points: 1st, 2nd, 3rd, and 4th			
	First Point Frequency	Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333							
		0							
	First Point Gear	Gear ratio for this SAGV point.							
		► Auto		Gear2		Gear4			
	Second Point Frequency	Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333							
	0								
Second Point Gear	Gear ratio for this SAGV point.								
	► Auto		Gear2		Gear4				
Third Point Frequency	Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333								
	0								
Third Point Gear	Gear ratio for this SAGV point.								
	► Auto		Gear2		Gear4				
Forth Point Frequency	Specify the frequency for the given point. 0 - MRC auto, Else a specific frequency as an integer: 1333								
	0								
Forth Point Gear	Gear ratio for this SAGV point.								
	► Auto		Gear2		Gear4				

Memory Configuration	Retrain on Fast Fail	Restart MRC in Cold mode if SW MemTest fails during Fast flow. Default = Enabled			
		Disabled		▶ Enabled	
	Retrain to Working Channel	Restart MRC in Cold mode after disabling failing channel. Default = Disabled			
		▶ Disabled		Enabled	
	DDR_1D PC	DDR 1DPC performance feature for 2R DIMMs. Can be enabled on DIMM0 or DIMM1 only, or on both			
		Disabled	Enabled on DIMM0 only	Enabled on DIMM1 only	▶ Enabled
	Row Hammer Mode	Row Hammer Prevention Mode. RFM will fall back to pTRR if not available			
		Disabled	▶ RFM		pTRR
	Refresh Watermarks	Sets Refresh Panic Watermark and Refresh High-Priority Watermark to HIGH or LOW values			
		Low		▶ High	
	LPDDR ODT RttWr	Initial RttWr ODT override for LP4/5 in Ohms. Range 0x01 - 0xFF, default 0 = AUTO			
		0			
	LPDDR ODT RttCa	Initial RttCa ODT override for LP4/5 in Ohms. Range 0x01 - 0xFF, default 0 = AUTO			
		0			
	Exit On Failure (MRC)	Exit On Failure for MRC training steps			
		Disabled		▶ Enabled	
	DCC Single Rank Track	Forces DCC to track only single rank			
		▶ Disabled		Enabled	
	Ch Hash Support	Enable/Disable Channel Hash Support. NOTE: ONLY if Memory interleaved Mode			
		Disabled		▶ Enabled	
	Ch Hash Mask	Set the BIT(s) to be included in the XOR function. NOTE BIT mask corresponds to BITS [19:6]			
		2096			
	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	BIT7	▶ BIT8	BIT9
		BIT10	BIT11	BIT12	BIT13
	Extended Bank Hashing	Enable/disable Extended Bank Hashing.			
		Disabled		▶ Enabled	
Per Bank Refresh	Enables and Disables the per bank refresh. This only impacts memory technologies that support PBR: LPDDR3, LPDDR4.				
	Disabled		▶ Enabled		
Strong Weak Leaker	Value for StrongWkLeaker				
	7				
Opportunistic Self Refresh	Enable/Disable Opportunistic Self Refresh.				
	Disabled		▶ Enabled		
Opportunistic Self Refresh IdleTimer	Default 0 = AUTO. Range 500 to 10000 (in ns)				
	0				
RxVref Temperature Coefficient	Default = 6. Range from 0-255				
	6				

Memory Configuration	RxDqsDelay Temperature Coefficient	Default = 4. Range from 0-255	
		4	
	Ca Parity Pattern Rotation	Default = 0 (Auto). 1 for high stress pattern rotation. 2 for no rotation.	
		0	
	WCK Offset	Enable/Disable WCK Offset WA. Default = 0 (Disabled)	
		► Disabled	Enabled
	Power Down Mode	CKE Power Down Mode Control	
		► Enabled	Disabled Auto
	Pwr Down Idle Timer	Default 0 = AUTO. Range 30 to 2000 (in ns)	
		0	
	Page Close Idle Timeout	Page Close Idle Timeout Control	
		Disabled	► Enabled
	Memory Scrambler	Enable/Disable Memory Scrambler support.	
		Disabled	► Enabled
	Board Stack Up	0: Typical, 1: Frequency Limited	
		► Freq Limited	Typical
	Board Topology	0: Daisy Chain, 1: Tee	
		Tee	► Daisy Chain
	2DPC Enhanced Frequency Limit	Enable or Disable Enhanced FreqLimit for 2DPC	
		Enabled	► Disabled
	Force Cold Reset	Force ColdReset OR Choose MrcColdBoot mode, when Coldboot is required during MRC execution. Note: If ME 5.0MB is present, ForceColdReset is required!	
		Enabled	► Disabled
	Controller 0, Channel 0-3 Control	Controller 0, Channel 0-3 Control - Enable or Disable Controller 0, Channel 0-3.	
		► Enabled	Disabled
	Controller 1, Channel 0-3 Control	Controller 1, Channel 0-3 Control - Enable or Disable Controller 1, Channel 0-3.	
		► Enabled	Disabled
	Force Single Rank	When enabled, only Rank 0 will be used in each DIMM	
		► Disabled	Enabled
	Memory Remap	Enable/Disable Memory Remap above 4GB	
		► Enabled	Disabled
	Time Measure	Enable/Disable printing of the time it takes to execute MRC.	
		► Disabled	Enabled
	Fast Boot	Enable/Disable fast path thru the MRC	
		Disabled	► Enabled
	Rank Margin Tool Per Task	Enables/Disables RMT running at every major training step	
		► Disabled	Enabled
	Training Training	Enables/Disables printing of the current trained state at every major training step.	
		► Disabled	Enabled
	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
	Rank Margin Tool Loop Count	Specifies the Loop Count to be used during Rank Margin Tool Testing. 0 - AUTO	
		0	

Memory Configuration	Write0	Write0 feature for LP5/DDR5					
		► Disabled			Enabled		
	Force CKD Bypass	Force CKD in Bypass Mode if CKD DIMM is detected					
		► Disabled			Enabled		
	DDR5 MR7 WICA support	Enable if DDR5 DRAM Device supports MR7 WICA 0.5 tCK offset alignment					
		► Disabled			Enabled		
	Driver Type Override	Force override the driver type. 0=Auto, 1=CMOS, 2=NMOS					
		0					
	Lp5 Bypass Vccddq Limits	Bypasses Fuse limits for Vccddq. Advised to keep disabled					
		0					
	Vddq Voltage Override	CPU FIVR TX Vddq:# is multiple of 1mV where 0 means Auto.					
		0					
Vcclog Voltage Override	CPU FIVR TX Vddq:# is multiple of 1mV where 0 means Auto.						
	0						
VccClk Voltage Override	CPU FIVR TX Vddq:# is multiple of 1mV where 0 means Auto.						
	0						
Initial DDR5 TxVref Override	Override for initial DDR5 TxVref value, 0 = Auto (default), valid range from 350 to 975, in increments of 5						
	0						
Graphics Configuration	Graphics Configuration						
	Skip Scanning of External Gfx Card	If Enable, it will not scan for External Gfx Card on PCIE Ports					
		► Disabled			Enabled		
	Primary Display	Select AUTO set IGD to be Primary Display if no external Graphics Device connected otherwise external Graphics Device detected on first PCIe port will be Primary Display or Select IGFX for IGD to be Primary Display Or Select HG for Hybrid Gfx.					
		► Auto		IGFX		HG	
	Internal Graphics	Keep IGFX enabled based on the setup options.					
		► Auto		Disabled		Enabled	
	DVMT Pre-Allocated	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.					
		0M	32M	64M	96M	► 128M	4M
		8M	12M	16M	20M	24M	28M
		32M/F7	36M	40M	44M	48M	52M
		56M	60M				
	Igfx Gsm2	Graphics Stolen Memory 2					
		► 0GB	2GB	4GB	6GB	8GB	10GB
		12GB	14GB	16GB	18GB	20GB	22GB
		24GB	26GB	28GB	30GB	32GB	
	Intel Graphics Pei Display Peim	Enable/Disable Pei (Early) Display					
		Disabled			► Enabled		
	VDD Enable	Enable/Disable forcing of VDD in the BIOS					
		Disabled			► Enabled		
	Configure GT for use	Enable/Disable GT configuration in BIOS					
		Disabled			► Enabled		
Configure Media for use	Enable/Disable Media configuration in BIOS						
	Disabled			► Enabled			
GT RC1p Support	Enable/Disable RC1p support. If GT RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met						
	► Disabled			Enabled			

Graphics Configuration	Media RC1p Support	Enable/Disable RC1p support. If Media RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met	
		► Disabled	Enabled
	PAVP Enable	Enable/Disable PAVP	
		Disabled	► Enabled
	V-by-One(iTE6807) Enable	Enable/Disable V-by-One(iTE6807)	
		► Disabled	Enabled
	Bypass VBT Update	Enable/Disable bypass VBT update	
		Disabled	► Enabled
	IUER Button Enable	Enable/Disable IUER Button Functionality	
		► Disabled	Enabled
VMD setup menu	VMD Configuration settings		
	Enable VMD controller	Enable/Disable to VMD controller	
		Disabled	► Enabled
	Enable VMD Global Mapping	Enable/Disable to VMD Global Mapping	
		► Disabled	Enabled
	Map PCH SATA Controller Under VMD	Map/UnMap this Root Port to VMD	
		► Disabled	Enabled
	RAID0-1/5/10	Enable/Disable RAID0-1/5/10 support	
	Disabled	► Enabled	
	ZPODD	Enable/Disable ZPODD. The option is only needed to be enabled when ZPODD is connected in VMD mode	
		► Disabled	Enabled
VT-d setup menu	VT-d Configuration settings		
	Pre-boot DMA Protection	Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)	
		DMA Control Guarantee	
	DMA Control Guarantee	DMA Control Guarantee	
		DMA Control Guarantee	
CRID Support	Enable/Disable SA CRID and TCSS CRID control for Intel SIPP		
	Enabled	► Disabled	
NPU Device (B0:D11:F0)	Enable/Disable NPU (Neural Processing Unit) Device.		
	► Enabled		Disabled

4.4.5 PCIE Configuration

PCIE Parameters.

PCIE Configuration					
Port8xh De-code	PCI Express Port8xh Decode Enable/Disable.				
	► Disable		Enable		
Compliance Test Mode	Enable when using Compliance Load Board.				
	► Disable		Enable		
PCIE clocks	PCIE clocks				
	Clock0-20 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	Enabled	Disabled	
	ClkReq for Clock0-20	Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.			
► Platform-POR		Disabled			
PCI Express Root Port PXPA1/PXPF	PCI Express Root Port Settings.				
	PCI Express Root Port PXPA1	Control the PCI Express Root Port.			
		Disable		► Enable	
	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			
		► Disabled	L0s	L1	L0sL1
	L1 Substates	PCI Express L1 Substates settings.			
		Disabled		L1.1	► L1.1 & L1.2
	ACS	Enable/Disable Access Control Services Extended Capability			
		Disable		► Enable	
	PTM	Enable/Disable Precision Time Measurement			
		Disable		► Enable	
	FOM Scoreboard Control Policy	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS			
		► Auto	Gen3	Gen4	Gen3/Gen4
	URR	PCI Express Unsupported Request Reporting Enable/Disable.			
		Disable		► Enable	
	FER	PCI Express Device Fatal Error Reporting Enable/Disable.			
		Disable		► Enable	
	NFER	PCI Express Device Non-Fatal Error Reporting Enable/Disable.			
		Disable		► Enable	
	CER	PCI Express Device Correctable Error Reporting Enable/Disable.			
		Disable		► Enable	
	SEFE	Root PCI Express System Error on Fatal Error Enable/Disable.			
		► Disable		Enable	
	SENF	Root PCI Express System Error on Non-Fatal Error Enable/Disable.			
		► Disable		Enable	
	SECE	Root PCI Express System Error on Correctable Error Enable/Disable.			
		► Disable		Enable	
	PME SCI	PCI Express PME SCI Enable/Disable.			
		► Disable		Enable	
	Hot Plug	PCI Express Hot Plug Enable/Disable.			
		► Disable		Enable	

PCI Express Root Port PXP1/PXPF	PCIe Speed	Configure PCIe Speed		
		► Auto	Gen2	Gen3
		Gen4	Gen5	Gen6
	Advanced Error Reporting	Advanced Error Reporting Enable/Disable.		
		Disabled		► Enable
	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		
	Assertion on Link Down GPIOs	GPIO Assertion on Link Down		
		Disabled		► Enable
	LTR	PCH PCIe Latency Reporting Enable/Disable		
		Disabled		► Enable
	Snoop Latency Override	Snoop Latency Override for PCH PCIe. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.		
		Disabled	Manual	► Auto
	Non Snoop Latency Override	Non Snoop Latency Override for PCH PCIe. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.		
		Disabled	Manual	► Auto
	LTR Override Spec Complaint	By default is Desired Value. When Desired Value is selected, LTR value will be programmed with recommended value. When Spec Complaint is selected, it will program 400ns LTR value and may block platform PG.		
		Spec Complaint - 400ns		► Desired Value - from BIOS option
	P2P Support	Program P2P Support Registers according to setup option		
		► Disabled		Enable
	PCIe EQ settings	PCIe EQ settings		
		PCIe EQ override	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process	
			► Disabled	Enable

PCI Express Root Port PXPd	PCI Express Root Port Settings.				
	PCI Express Root Port PXPd	Control the PCI Express Root Port.			
		Disable		► Enable	
	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			
		► Disabled	L0s	L1	L0sL1
	L1 Substates	PCI Express L1 Substates settings.			
		Disabled		L1.1	► L1.1 & L1.2
	ACS	Enable/Disable Access Control Services Extended Capability			
		Disable		► Enable	
	PTM	Enable/Disable Precision Time Measurement			
		Disable		► Enable	
	FOM Scoreboard Control Policy	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS			
		► Auto	Gen3	Gen4	Gen3/Gen4
	URR	PCI Express Unsupported Request Reporting Enable/Disable.			
		Disable		► Enable	
	FER	PCI Express Device Fatal Error Reporting Enable/Disable.			
		Disable		► Enable	
	NFER	PCI Express Device Non-Fatal Error Reporting Enable/Disable.			
		Disable		► Enable	
	CER	PCI Express Device Correctable Error Reporting Enable/Disable.			
		Disable		► Enable	
	SEFE	Root PCI Express System Error on Fatal Error Enable/Disable.			
		► Disable		Enable	
	SENGE	Root PCI Express System Error on Non-Fatal Error Enable/Disable.			
		► Disable		Enable	
	SECE	Root PCI Express System Error on Correctable Error Enable/Disable.			
		► Disable		Enable	
	PME SCI	PCI Express PME SCI Enable/Disable.			
		► Disable		Enable	
Hot Plug	PCI Express Hot Plug Enable/Disable.				
	► Disable		Enable		

PCI Express Root Port PXPd	PCIe Speed	Configure PCIe Speed			
		► Auto		Gen2	Gen3
		Gen4		Gen5	Gen6
	Advanced Error Reporting	Advanced Error Reporting Enable/Disable.			
		Disabled		► Enable	
	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			
	Assertion on Link Down GPIOs	GPIO Assertion on Link Down			
		Disabled		► Enable	
	Extra Bus Reserved	PCH PCIe Latency Reporting Enable/Disable			
		Disabled		► Enable	
	Snoop Latency Override	Extra Bus Reserved (0-7) for bridges behind this Root Bridge.			
0					

PCI Express Root Port PXPd	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	
		Disabled	► Enable
	Snoop Latency Override	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.	
		Disabled	Manual ► Auto
	Non Snoop Latency Override	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.	
		Disabled	Manual ► Auto
	LTR Override Spec Complaint	By default is Desired Value. When Desired Value is selected, LTR value will be programmed with recommended value. When Spec Complaint is selected, it will program 400ns LTR value and may block platform PG.	
		Spec Complaint - 400ns	► Desired Value - from BIOS option
	P2P Support	Program P2P Support Registers according to setup option	
		► Disabled	Enable
	PCIe EQ settings	PCIe EQ settings	
		PCIe EQ override	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
			► Disabled Enable

PCI Express Root Port SPA1-4/SPB1/SPC1/SPF1	PCI Express Root Port Settings.				
	PCI Express Root Port SPA1-4/SPB1/SPC1/SPF1	Control the PCI Express Root Port.			
		Disable		► Enable	
	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			
		► Disabled	L0s	L1	L0sL1
	L1 Substates	PCI Express L1 Substates settings.			
		Disabled		L1.1	► L1.1 & L1.2
	ACS	Enable/Disable Access Control Services Extended Capability			
		Disable		► Enable	
	PTM	Enable/Disable Precision Time Measurement			
		Disable		► Enable	
	FOM Scoreboard Control Policy	Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS			
		► Auto	Gen3	Gen4	Gen3/Gen4
	URR	PCI Express Unsupported Request Reporting Enable/Disable.			
		Disable		► Enable	
	FER	PCI Express Device Fatal Error Reporting Enable/Disable.			
		Disable		► Enable	
	NFER	PCI Express Device Non-Fatal Error Reporting Enable/Disable.			
		Disable		► Enable	
	CER	PCI Express Device Correctable Error Reporting Enable/Disable.			
		Disable		► Enable	
	SEFE	Root PCI Express System Error on Fatal Error Enable/Disable.			
		► Disable		Enable	
	SENEFE	Root PCI Express System Error on Non-Fatal Error Enable/Disable.			
		► Disable		Enable	
	SECE	Root PCI Express System Error on Correctable Error Enable/Disable.			
		► Disable		Enable	
	PME SCI	PCI Express PME SCI Enable/Disable.			
		► Disable		Enable	
	Hot Plug	PCI Express Hot Plug Enable/Disable.			
		► Disable		Enable	
	PCIe Speed	Configure PCIe Speed			
		► Auto	Gen2		Gen3
		Gen4		Gen5 Gen6	
	Advanced Error Reporting	Advanced Error Reporting Enable/Disable.			
		Disabled		► Enable	
	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			
	Assertion on Link Down GPIOs	GPIO Assertion on Link Down			
		Disabled		► Enable	

PCI Express Root Port SPA1-4/ SPB1/SPC1/ SPF1	LTR	PCH PCIE Latency Reporting Enable/Disable	
		Disabled	► Enable
	Snoop Latency Override	Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.	
		Disabled	Manual ► Auto
	Non Snoop Latency Override	Non Snoop Latency Override for PCH PCIE. Disabled: Disable override. Manual: Manually enter override values. Auto (default): Maintain default BIOS flow.	
		Disabled	Manual ► Auto
	LTR Override Spec Complaint	By default is Desired Value. When Desired Value is selected, LTR value will be programmed with recommended value. When Spec Complaint is selected, it will program 400ns LTR value and may block platform PG.	
		Spec Complaint - 400ns	► Desired Value - from BIOS option
	PCIe EQ settings	PCIe EQ settings	
		PCIe EQ override	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
			► Disabled Enable

4.4.6 PCIE Hot-Plug Settings

Allow Changing Build time Defined Hot-Plug Settings.

PCIE Hot-Plug Settings	
Bus	Number of reserved busses for hot plug 2
32-bit MMIO	Amount of 32-bit MMIO reserved for hot plug, in MB 10
32-bit MMIO alignment	Select the alignment of 32-bit MMIO, each increment shifts alignment by 1-bit 1
64-bit MMIO	Amount of 64-bit MMIO reserved for hot plug, in MB 10
64-bit MMIO alignment	Select the alignment of 64-bit MMIO, each increment shifts alignment by 1-bit 1
IO	Amount of IO reserved for hot plug, in KB 1

4.4.7 PCH-IO Configuration

PCH Parameters.

PCH-IO Configuration		
SATA Configuration	SATA Device Option Settings	
	SATA Controller(s)	Enable/Disable SATA Device. ▶ Enable Disable
	SATA Mode Selection	Determines how SATA controller(s) operate. AHCI
	SATA Test Mode	Test Mode Enable/Disable (Loop Back). Enable ▶ Disable
	Aggressive LPM Support	Enable PCH to aggressively enter link power state. ▶ Disable Enable
	Serial ATA Port 0-1	
	Port 0-1	Enable or Disable SATA Port Disable ▶ Enable
	Hot Plug	Designates this port as Hot Pluggable. Disable ▶ Enable
	External	Marks this port as external. ▶ Disable Enable
	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. ▶ Disable Enable
	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 Direct-Connect or M2 ▶ Unknown ISATA Direct Connect Flex M2
	SATA Port 0-1 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. Disable ▶ Enable
	DITO Configuration	Enable/Disable DITO Configuration ▶ Disable Enable

SATA Configuration	Serial ATA Port 2-7		
	Port 2-7	Enable or Disable SATA Port	
		Disable	► Enable
	Hot Plug	Designates this port as Hot Pluggable.	
		Disable	► Enable
	External	Marks this port as external.	
		► Disable	Enable
	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.	
		► Disable	Enable
	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 Direct-Connect or M2	
		► Unknown	ISATA
		Direct Connect	Flex
		M2	
	SATA Port 2-7 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.	
		► Disable	Enable
	DITO Configuration	Enable/Disable DITO Configuration	
		► Disable	Enable

Security Configuration	Security Configuration settings					
	RTC Memory Lock	Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM				
		Disable		▶ Enable		
	BIOS Lock	Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.				
Disable		▶ Enable				
	Force unlock on all GPIO pads	If Enabled BIOS will force all GPIO pads to be in unlocked state.				
		▶ Disable		Enable		
Thermal Throttling Control	Thermal Throttling Control					
	SOC Thermal Throttling Level	Determine if use Intel suggested setting				
		▶ Suggested Setting		Manual		
	IOE Thermal Throttling Level	Determine if use Intel suggested setting				
		▶ Suggested Setting		Manual		
	PCH 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			
PMC Configuration	Power management controller configuration					
	PMC ADR Configuration	PMC ADR Configuration				
		ADR enable	Enable asynchronous DRAM refresh			
			▶ Platform-POR		Enabled	Disabled
		Host Partition Reset ADR Enable	Enables/Disables ADR on Host Partition Reset			
			Platform-POR		▶ Enabled	Disabled
		ADR timer 1 expire time	Type desired ADR timer expire time, valid values - <1, 256>. Entered time is scaled by ADR timer time unit.			
			32			
	ADR timer 1 time unit	Select ADR timer time unit.				
		1us	10us	100us	1ms	
	10ms	100ms	▶ 1s	10s		
PMC Watchdog Timer	Enable/Disable PMC Watchdog Timer					
	▶ Enabled		Disabled			
PCH LAN: Fast Starup wake support	Wake on lan enabled or disabled when Fast Startup is enabled.					
	Enabled		▶ Disabled			
Foxville I225 LAN Controller	Enable/Disable Foxville I225 LAN Controller.					
	▶ Enabled		Disabled			
Foxville I225 Wake on LAN Support	Enable/Disable Foxville I225 Wake on LAN Support.					
	▶ Enabled		Disabled			
DeepSx Power Policies	Configure the DeepSx Mode configuration.					
	▶ Disabled	Enabled in S4/S5-Battery	Enabled in S5-Battery	Enabled in S4/S5	Enabled in S5	
PS_ON Enable	Enable or disable PS_ON ()support a new C10 state from the CPU on desktop SKUs that enables a lower power target that will be required by the California Energy Commission (CEC).					
	▶ Enabled		Disabled			
Wake on WLAN and BT Enable	Enable/Disable PCI Express Wireless LAN and Bluetooth to wake the system.					
	Enabled		▶ Disabled			
Disable DSX ACPI PRESENT PullDown	Disable PCH internal ACPI PRESENT PullDown when DeepSx or G3 exit.					
	Enabled		▶ Disabled			
State After G3	Specify what state to go to when power is re-applied after a power failure (G3 state).					
	▶ S0 State		S5 State			

Port 80h Re-direction	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		
	Disabled		► Enabled
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.		
	► Disabled		Enabled
Energy Re-reporting	Enable Energy Report for all (PCH/SOC/IOE). MUST set it as ENABLED. This is only for test purpose.		
	► Disabled		Enabled
LPM S0i2.0/ LPM S0i2.1/ LPM S0i2.2	Enable/Disable S0ix sub-state. This setting is for test purpose. S0ix sub-states should be enabled for production.		
	Disabled		► Enabled
PCH LPM S0i2.0	Enable/Disable S0ix sub-state for PCH. This setting is for test purpose. S0ix sub-states should be enabled for production.		
	Disabled		► Enabled
C10 Dynamic threshold adjustment	Enable/Disable C10 dynamic threshold adjustment		
	► Disabled		Enabled
Energy Reporting Debug Mode	Energy Reporting Debug Mode		
	Disabled		► Enabled
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.		
	► Disabled		Enabled
ATX Telemetry Unit	ATX Telemetry Unit in Watts or Percentage.		
	► Watts		Percentage
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.		
	Disabled	► Enabled	Enabled In Runtime and S3 Resume
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.		
	Disabled		► Enabled
Flash Protection Range Registers (FPRR)	Enable Flash Protection Range Registers		
	► Disabled		Enabled
SPD Write Disable	Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.		
	► TRUE		FALSE
LGMR	64KB memory block for LGMR (LPC Memory Range Decode)		
	► Disabled		Enabled
HOST_C10 reporting to Target	This option enables HOST_C10 reporting to Target via eSPI Virtual Wire		
	► Disabled		Enabled
OS IDLE Mode	OS IDLE Mode		
	Disabled		► Enabled
S0ix Auto Demotion	Enable/Disable Host Low Power Mode S0ix Auto-Demotion		
	Disabled		► Enabled
Latch Events C10 Exit	Enable/Disable Latch Events on C10 Exit		
	► Disabled		Enabled

4.4.8 PCH-FW Configuration

Configure Management Engine Technology Parameter.

PCH-FW Configuration				
ME State	When Disabled, ME will be put into ME Temporarily Disabled Mode. NOTE: Once this option is changed and saved, it is grayed out to prevent command been sent again before reset.			
	► Enabled		Disabled	
Manageability Feature State	Enable/Disable Intel(R) Manageability features. NOTE: This option disables/enables Manageability Features support in FW. To disable support platform must be in an unprovisioned state first.			
	► Enabled		Disabled	
AMT BIOS Features	When disabled AMT BIOS Features are no longer supported and user is no longer able to access MEBx Setup. Note: This option does not disable Manageability Features in FW.			
	Enabled		► Disabled	
AMT Configuration	Configure Intel(R) Active Management Technology Parameters.			
	USB Provisioning of AMT	Enable/Disable of AMT USB Provisioning.		
		► Disabled		Enabled
	MAC Pass Through	Enable/Disable MAC Pass Through function.		
		► Disabled		Enabled
	Dynamic Lan Switch	Allow switching AMT support from Integrated LAN to Discrete LAN.		
		► As defined in FIT	Integrated LAN	Discrete LAN
	Activate Remote Assistance Process	Trigger CIRA boot Note: Network Access must be activated first from MEBx Setup.		
		► Disabled		Enabled
	Unconfigure ME	Unconfigure ME		
		► Disabled		Enabled
	ASF Configuration	Configure Alert Standard Format parameters.		
		PET Progress	Enable/Disable PET Events Progress to receive PET Events.	
			Disabled	► Enabled
		WatchDog	Enable/Disable WatchDog Timer.	
			► Disabled	Enabled
		ASF Sensors Table	Adds ASF Sensor Table into ASF! ACPI Table	
► Disabled			Enabled	
ME Unconfig on RTC Clear	When Disabled ME will not be unconfigured on RTC Clear			
	Disabled		► Enabled	
Core Bios Done Mes- sage	Enable/Disable Core Bios Done message sent to ME			
	Disabled		► Enabled	
CSE Data Resilience Support	Enable/Disable CSE Data Resilience Support			
	Disabled		► Enabled	
FDO Shipment State Override	Enable/Disable FDO Shipment State Override. BIOS will override soft strap setting when enabled			
	► Disabled		Enabled	
TPM Device Selection	Selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr dTPM 1.2 - Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost.			
	► dTPM		PTT	
Firmware Up date Configu ration	Configure Management Engine Technology Parameters.			
	ME FW Image Re-Flash	Enable/Disable Me FW Image Re-Flash function.		
		► Disabled		Enabled
	FW Update	Enable/Disable ME FW Update function.		
Disabled		► Enabled		
FIPS Configu ration	FIPS Mode help			
	FIPS Mode	FIPS Mode configuration		
		► Disabled		Enabled

Unique Platform Id Configuration	Configure Unique Platform Id Feature		
	Upid State	Enable/Disable Upid Feature	
		► Disabled	Enabled
	Upid OS Control State	Allows OS to enable/disable the Upid feature state	
		Disabled	► Enabled
ME Debug Configuration	Configure ME Debug options NOTE: This menu is provided for testing purposes. It is recommend to leave the options in their default states.		
	HECI Timeouts	Enable/Disable HECI Send/Receive Timeouts.	
		Disabled	► Enabled
	Force ME DID Init Status	Forces the DID Initialization Status value.	
		► Disabled	0 - Success
		1 - No Memory in Channels	2 - Memory Init Error
	CPU Replaced Polling Disable	CPU Replaced Polling Disable	
		► Disabled	Enabled
	HECI Message check Disable	Setting this option disables message check for Bios Boot Path when sending	
		► Disabled	Enabled
	MBP HOB Skip	Setting this option will skip sending Get MBP message and MBP HOB will not be created	
		► Disabled	Enabled
	HECI2 Interface Communication	Adds and Removes HECI2 Device from PCI space.	
		► Disabled	Enabled
	KT Device	Enable/Disable KT Device	
		► Platform-POR	Enabled Disabled
	End Of Post Message	Enable/Disable End of Post message sent to ME	
		Disabled	► Send in DXE
	D0I3 Setting for HECI Disable	Setting this option disables setting D0I3 bit for all HECI devices	
		► Disabled	Enabled
	MCTP Broadcast Cycle	Enable/Disable Management Component Transport Protocol Broadcast Cycle and Set PMT as Bus Owner	
		► Disabled	Enabled
	SMBIOS type 130 OEM capabilities	This menu allows changing SMBIOS type 130 OEM capabilities.	
		BIOS Reflash Capability State	Change BIOS Reflash Capability State
			Disabled ► Enabled
		BIOS Boot to Setup Capability State	Change BIOS Boot to Setup Capability State
			Disabled ► Enabled
		BIOS Pause Before Booting Capability State	Change BIOS Pause Before Booting Capability State
			► Disabled Enabled
		BIOS Secure Boot Capability Exposure to FW State	Change BIOS Secure Capability Exposure State to FW. This does not affect SecureBoot as such
			Disabled ► Enabled
		vPro TBT Dock Support	Enable/Disable vPro TBT Dock Support. Note: for the change to take effect, need to put system into G3 state then resume.
			Disabled ► Enabled

Anti-Rollback SVN Configuration	Configure Anti-Rollback SVN		
	Automatic HW-Enforced Anti-Rollback SVN	When enabled, hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution	
		► Disabled	Enabled
	Set HW-Enforced Anti-Rollback for Current SVN	Enable hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent.	
		► Disabled	Enabled
OEM Key Revocation Configuration	Configure OEM Key Revocation		
	Automatic OEM Key Revocation	When enabled, BIOS will automatically send HECI command to revoke OEM keys.	
		► Disabled	Enabled
	Invoke OEM Key Revocation	A Heci command will be send to revoke OEM key.	
		► Disabled	Enabled
Extend CSME Measurement to TPM-PCR	Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1]		
	► Disabled		Enabled

4.4.9 Thermal Configuration

Thermal Configuration Parameters.

Thermal Configuration			
Enable All Thermal Functions	Enable All Thermal Functions will enable 'Memory Thermal Management', 'Active Trip Points', and 'Critical Trip Points'. Set to disable for Manual Configuration		
	Disabled		► Enabled
CPU Thermal Configuration	CPU Thermal Configuration options		
	Tcc Activation Offset	Offset from factory set Tcc activation temperature 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	
	Tcc Offset Time Window	Tcc Offset Time Window for Running Average Temperature Limit(RATL) feature. The Tcc offset time window can range from 5ms to 448s.	
		► Disabled	5 ms 10 ms
		55 ms	156 ms 375 ms
		500 ms	750 ms 1 sec
		2 sec	3 sec 4 sec
		5 sec	6 sec 7 sec
		8 sec	10 sec 12 sec
		14 sec	16 sec 20 sec
		24 sec	28 sec 32 sec
		40 sec	48 sec 56 sec
		64 sec	80 sec 96 sec
		112 sec	128 sec 160 sec
		192 sec	224 sec 256 sec
		320 sec	384 sec 448 sec
	Tcc Offset Clamp Enable	Tcc Offset Clamp bit Enable for Running Average Temperature Limit(RATL) feature to allow CPU to throttle below P1.	
		► Disabled	Enabled
	Tcc Offset Lock Enable	Lock Enable for Running Average Temperature Limit(RATL) feature to lock Temperature Target MSR.	
		Disabled	► Enabled

CPU Thermal Configuration	Bi-directional PROCHOT#	When a processor thermal sensor trips (either core), the PROCHOT# will be driven. If bi-direction is enabled, external agents can drive PROCHOT# to throttle the processor.			
		Disabled		►Enabled	
	Disable PROCHOT# Output	Enable/Disable PROCHOT# Output			
		Disabled		►Enabled	
	Disable VR Thermal Alert	Enable/Disable VR Thermal Alert			
		►Disabled		Enabled	
	PROCHOT Response	Enable/Disable PROCHOT Response			
		Disabled		►Enabled	
	PROCHOT Demotion	PROCHOT Demotion Algorithm. PROCHOT Demotion Algorithm will limit the frequency to a lower point gradually instead of limiting to LFM immediately. Disable means BIOS provides the capability to disable it via pcode mailbox. Hardware Default means BIOS do nothing, thus keep Prochot Demotion Algorithm in hardware default status.			
		Disabled		►Hardware Default	
PROCHOT Lock	Enable/Disable PROCHOT Lock				
	Disabled		►Enabled		
ACPI T-States	Enable/Disable ACPI T-States.				
	►Disabled		Enabled		
Platform Thermal Configuration	Platform Thermal Configuration options				
	Active Trip Point 0	This value controls the temperature of the ACPI Active Trip Point 0 - the point in which the OS will turn the processor fan on Active Trip Point 0 Fan Speed.			
		Disabled	40 C	45 C	50 C
		55 C	60 C	65 C	►70 C
		75 C	80 C	85 C	90 C
		95 C	100 C	105 C	110 C
	Active Trip Point 0 Fan Speed	Active Trip Point 0 Fan Speed in percentage. Value must be between 0 (Fan off) - 100 (Max fan speed). This is the speed at which fan will run when Active Trip Point 0 is crossed.			
		100			
	Active Trip Point 1	This value controls the temperature of the ACPI Active Trip Point 1 - the point in which the OS will turn the processor fan on Active Trip Point 1 Fan Speed.			
		Disabled	►40 C	45 C	50 C
		55 C	60 C	65 C	70 C
		75 C	80 C	85 C	90 C
		95 C	100 C	105 C	110 C
	Passive Trip Point	This value controls the temperature of the ACPI Passive Trip Point - the point in which the OS will begin throttling the processor.			
		Disabled	40 C	45 C	50 C
		55 C	60 C	65 C	70 C
		75 C	80 C	85 C	90 C
		►95 C	100 C	105 C	110 C
	Passive TC1 Value	This value sets the TC1 value for the ACPI Passive Cooling Formula. Range 1 - 16			
		1			
	Passive TC2 Value	This value sets the TC2 value for the ACPI Passive Cooling Formula. Range 1 - 16			
		5			
	Passive TSP Value	This item sets the TSP value for the ACPI Passive Cooling Formula. It represents in tenths of a second how often the OS will read the temperature when passive cooling is enabled. Range 2 - 32			
		10			

Platform Thermal Configuration	Active Trip Points	Disable Active Trip Points			
		Disabled		► Enabled	
	Passive Trip Points	Disable Passive Trip Points			
		► Disabled		Enabled	
	Critical Trip Points	Disable Critical Trip Points			
		Disabled		► Enabled	
	PCH Temp Read	PCH Temperature Read Enable			
		Disabled		► Enabled	
	CPU Energy Read	CPU Energy Read Enable			
		Disabled		► Enabled	
	CPU Temp Read	CPU Temperature Read Enable			
		Disabled		► Enabled	
Alert Enable Lock	Lock all Alert Enable settings				
	► Disabled		Enabled		
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				
Boot DTS Read	Read PCH, CPU DTS Temperature and publish via SMBIOS table				
	► Disabled		Enabled		
Intel(R) Innovation Platform Framework Configuration	Intel(R) Innovation Platform Framework Configuration options				
	Intel(R) Innovation Platform Framework	Enable/Disable Intel Innovation Platform Thermal Framework			
		Disabled		► Enabled	
	IPF Manager Device	Enable/Disable the IPF Manager Device.			
		Disabled		► Enabled	
	Processor Thermal Device	Enable/Disable Processor Thermal Device.			
		Disabled		► SA Thermal Device	
	PPCC Step Size	Step size for Turbo power limit (RAPL) control			
		► 0.5 Watts	1.0 Watts	1.5 Watts	2.0 Watts
	Intel(R) Innovation Platform Framework Configuration	An Integer containing the Intel(R) Innovation Platform Framework Configuration bitmap: BIT0[Generic UI Access Control](0=enable,1=disable) BIT1[Restricted UI Access Control](0=enable,1=disable) BIT2[shell Access Control](0=enable,1=disable) BIT3[Environment Monitoring Report Control](0=report,1=silent) BIT4[Thermal Mitigation Report Control](0=silent,1=report) BIT5[Thermal Policy Report Control](0=silent,1=report)			
		0			
	FAN1 Device	Enable the Fan1 device.			
		Disabled		► Enabled	
	FAN2/3 Device	Enable the Fan2/3 device.			
		► Disabled		Enabled	
	Charger participant	Enable/Disable Charger device			
		Disabled		► Enabled	
	Power participant	Enable/Disable the Power participant.			
		► Disabled		Enabled	
	Battery Participant	Enable/Disable the Battery Participant.			
		► Disabled		Enabled	
	Sensor Device 1-5	Enable/Disable Sensor 1-5 device			
	► Disabled		Enabled		
OEM variable and Object	OEM variable and Object options				
	Design Variable 0	OEM Design Variable 0: PPS Support on Platform: 0 - Disabled, 1 - Enabled			
		► Disabled		Enabled	
	Design Variable 2-5	OEM Design Variable: an integer between 0-255. This allows OEMs to customize Intel(R) Dynamic Tuning Technology behavior based on platform changes.			
		0			

Intel(R) Innovation Platform Framework Configuration	OEM variable and Object	PPCC Object	Enable/Disable PPCC object for validation.	
			► Disabled	Enabled
		ARTG Object	Enable/Disable ARTG object for validation.	
			Disabled	► Enabled
		PMAX Object	Enable/Disable PMAX object for validation.	
			Disabled	► Enabled
OEM variable and Object	OEM variable and Object options			
	Design Variable 0	OEM Design Variable 0: PPS Support on Platform: 0 - Disabled, 1 - Enabled		
		Disabled	► Enabled	
	Design Variable 2-5	OEM Design Variable: an integer between 0-255. This allows OEMs to customize Intel(R) Dynamic Tuning Technology behavior based on platform changes.		
		0		
	PPCC Object	Enable/Disable PPCC object for validation.		
		► Disabled	Enabled	
	ARTG Object	PMAX Object		
		Disabled	► Enabled	
	PMAX Object	Enable/Disable PMAX object for validation.		
		Disabled	► Enabled	
Hardware Health Monitor	Monitor the Hardware Health			

4.4.10 Platform Settings

Platform related Settings.

Platform Settings				
Charging Method	Select charging method as Normal Charging or Fast Charging.			
	Normal Charging		► Fast Charging	
GPE1 support	Switch between GPE0 support only (disabled) and GPE0 + GPE1 support (enabled)			
	► Enable		Disable	
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	
Scan Matrix Keyboard Support	Enables/Disables Scan Matrix Keyboard Support			
	► Disable		Enable	
EC PECI Mode	Switch eSPI PECI Mode or Legacy PECI mode			
	Legacy PECI mode		► PECI over eSPI mode	
Power Loss Notification Feature	Enable/Disable Power Loss Notification Feature. Default is not change the PLN feature.			
	► Default		Disable Enable	
Device password support	Support device password feature			
	Disable		► Enable	
Pmic Vcc IO Level	Select the Pmic Vcc IO Voltage Level			
	► Disable	1.05V	1.071V	1.023V
	0.997V	0.850V	0.900V	0.950V
Pmic Vddq Level	Select the Pmic Vddq Voltage Level			
	► Disable	0	1	2
	3	4	5	6
CSC Pmic NVM Update Support	Enable/Disable CastroCove Pmic Nvm Update			
	► Disable		Enable	
Pmic NVM Write Lock Support	Enable/Disable WarrenCove/CastroCove Pmic Nvm Write Lock			
	► Disable		Enable	
HEBC value	HEBC value 32bit			
	144371			
Pmic SlpS0 VM Support	Support to auto check Primium PMIC and disable SlpS0 voltage.			
	► Disable		Enable	
Power Sharing Manager	Configure the PSM ACPI objects.			
	► Disable		Enable	
Enable FFU Support	Enable/Disable FFU Support.			
	► Disable		Enable	
HID Event Filter Driver	Enables/Disables HID Event Filter Driver interface to OS.			
	Disable		► Enable	
Enable OfflineCrashDump Support	Causes BIOS to enable OfflineCrashDump Support. BIOS will set BIT0 in the OfflineMemoryDumpCapable field in the Offline Crashdump Configuration Table and reserve memory for BIOS execution when the Crashdump occurs. The TCO Timer must be enabled for this feature to work.			
	► Disable		Enable	
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	
DG Platform Support	DG is supported as MotherBoard Down OR Add In Card			
	► Add In Card		MB Down	
Enable PowerMeter	Enables/Disables PowerMeter.			
	► Disable		Enable	
Aux Rail Budget (Watt)	Total aux rail budget available per RVP. Value must be between 0 (Min Watt) - 10 (Max Watt)			
	6			

MPDT Support	Enable(Sensor_BOM1,Sensor_BOM2 and Sensor_BOM1 with Companion Chip)/Disable MPDT Support in BIOS			
	▶ Disabled	Sensor_BOM1	Sensor_BOM2	Sensor_BOM1 with Companion Chip
Skip OBB HASH Verify	Auto(Default): Skip OBB HASH Verification for Profile 0 and Verify OBB HASH for profile 3/4/5 Enable : Skip OBB HASH Verification for Profile(0,3,4,5) Disable : Verify OBB HASH for Profile(0,3,4,5)			
	Disabled	Enabled	Auto	
Skip Patch Table	Enable Skip the patch table update Disable update patch table			
	Enabled	▶ Disabled		
Gbe Firmware Update Support	Enable Gbe Firmware Update Support			
	▶ Enabled	Disabled		
Safe Loading Bios Enable	Enable[Default] : Mrc Reallocate new 16 MB TSEG Region Disable : Mrc allocate default 16 MB TSEG Region			
	Enabled	▶ Disabled		
Tseg Reallocate Enable Count	0 [Default] : Mrc allocate default 16 MB TSEG Region			
	1 to 3 : Mrc Reallocate new 16 MB TSEG Region			
VTIO	4 : System will hang when Tseg retry count reach more than 3			
	0			
VTIO	Configure settings for VTIO			
	Enable VTIO Support	Enable/Disable VTIO Support.		
		▶ Disabled	Enabled	

TCSS Platform Setting	Thunderbolt (TM) Configuration	USB4 CM Mode	FW CM - The system boots with FW CM in both BIOS and OS phase. SW CM - The system boots with SW CM in both BIOS and OS phase. OS dependent - The system will boot with SW CM in BIOS phase after saving this setting, then boot to OS based on OS preference to reflect the CM setting to next BIOS boot. If OS version is not SWCM compatible and Barlow Ridge is set, Barlow Ridge will run in MFDP mode. CM debug - The system with boot without any CM in BIOS phase, then boot to OS with the CM based on OS' preference by every boot.		
			Firmware CM		Software CM
			► OS Dependent		CM Debug
		Integrated Thunderbolt(TM) Enable	Enable or Disable Integrated Thunderbolt(TM).		
			Disabled		► Enabled
		Integrated Thunderbolt(TM) Configuration	Integrated Thunderbolt(TM) Related Configuration		
			Os Native Resource Balance	Os Native Resource Balance	
				► Disabled Enabled	
			Connect Topology Timeout value for ITBT	Connect Topology Timeout value for Integrated Thunderbolt(TM) Controller	
				5000	
			Force Poweron Timeout value for ITBT	Force Poweron Timeout value for Integrated Thunderbolt(TM)	
				500	
			ITBT RTD3	ITBT RTD3 Enable/Disable. Note: ITBT RTD3 Disabled is not supported when SW CM is applied for OS	
				Disabled ► Enabled	
			ITBT RTD3 EXIT DELAY	ITBT RTD3 EXIT DELAY (milli seconds)	
				0	
			PCIE RTD3 POLLING LINK ACTIVE TIMEOUT	ADJUST LINK ACTIVE POLLING TIME DURING D3C EXIT AND DELAY IN PS0 BEFORE RETURN TO OS (milli seconds)	
	0				
	USBC DataRole Swap Platform Disable Option	Enable/Disable setting USBC DataRole Swap Platform Disable Option			
► TRUE		FALSE			

4.4.11 ACPI D3Cold settings

ACPI D3Cold related settings.

ACPI D3Cold settings			
ACPI D3Cold Support	Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit Note: Disable it would affect the Storage D3 setting		
	Disable		► Enable
VR Ramp up delay	Delay between subsequent VR ramp ups if they are all Turn ON at the same time		
	16		
PCIe Slot 5 Device Power-on delay in ms	Delay between applying core power and Deasserting PERST#		
	100		
SensorHub	Delay after applying power to SensorHub device.		
	68		
TouchPad	Delay after applying power to TouchPad device.		
	68		
TouchPanel	Delay in PR _ON after applying power to TouchPanel device.		
	68		
P-state Capping	Set _PPC and send ACPI notification		
	► Disable		Enable
USB Port 1	USB RTD3 support. Super Speed : USB3.0 devices will be exposed as RTD3 capable. High Speed: USB2.0 devices will be exposed as RTD3 capable. Disabled : USB RTD3 support disabled. For SawtoothPeak USB Port1(Below) is Superspeed and Port2(Top) is HighSpeed. Check respective board configuration to know about USB port position.		
	High Speed		Super Speed ► Disabled
USB Port 2	USB RTD3 support. Super Speed : USB3.0 devices will be exposed as RTD3 capable. High Speed: USB2.0 devices will be exposed as RTD3 capable. Disabled : USB RTD3 support disabled. For SawtoothPeak USB Port1(Below) is Superspeed and Port2(Top) is HighSpeed. Check respective board configuration to know about USB port position.		
	► Disabled	High Speed	Super Speed Super Speed WWAN
ZPODD	Zero Power ODD option is applicable only for the board with ZPODD support.		
	► Disable		Enable
Sata Port 0-7	Setup option to control the SATA port RTD3 functionality		
	► Disable		Enable
PCIe Remapped CR1-3	PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.		
	► Disable		Enable
RTD3 Support for PCIe Rootports	Enable/Disable PCIe RTD3 Support		
	Disable		► Enable

4.4.12 OverClock Performance Menu

Performance Menu for Processor and Memory.

OverClock Performance Menu		
OverClocking Feature	Performance Menu for Processor and Memory.	
	► Disabled	Enabled
WDT Enable	Enable/Disable WatchDog Timer. Note: This option is ignored on debug BIOS.	
	► Disabled	Enabled

4.4.13 AMT Configuration

Configure Intel(R) Active Management Technology Parameters.

AMT Configuration			
USB Provisioning of AMT	Enable/Disable of AMT USB Provisioning.		
	▶ Disabled		Enabled
MAC Pass Through	Enable/Disable MAC Pass Through function.		
	▶ Disabled		Enabled
Dynamic Lan Switch	Allow switching AMT support from Integrated LAN to Discrete LAN.		
	▶ As defined in FIT	Integrated LAN	Discrete LAN
Activate Remote Assistance Process	Trigger CIRA boot Note: Network Access must be activated first from MEBx Setup.		
	▶ Disabled		Enabled
Unconfigure ME	Unconfigure ME with resetting MEBx password to default on next boot.		
	▶ Disabled		Enabled
ASF Configuration	Configure Alert Standard Format parameters.		
	PET Progress	Enable/Disable PET Events Progress to receive PET Events.	
		Disabled	▶ Enabled
	WatchDog	Enable/Disable WatchDog Timer.	
		▶ Disabled	Enabled
	ASF Sensors Table	Adds ASF Sensor Table into ASF! ACPI Table	
		▶ Disabled	Enabled

4.4.14 BCLK Configuration

BCLK Configuration

BCLK Configuration			
OC Watchdog Timer	When enabled, the OC watchdog timer is exposed to OS as an ACPI device. WDT HW is always used by BIOS when clock settings are changed.		
	► Disabled		Enabled
SoC BCLK PLL configuration	Configure SOC BCLK PLL state. When this PLL is ON, BCLK source for SOC-N and for CPU (unless CPU PLL is ON) will be from the SOC PLL.		
	► PLL in HW default state		PLL ON PLL OFF
CPU BCLK PLL configuration	Configure CPU BCLK PLL state. When this PLL is ON, BCLK source for CPU will be from the CPU PLL.		
	► PLL in HW default state		PLL ON PLL OFF

4.4.15 Trusted Computing

Trusted Computing Settings.

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

4.4.16 ACPI Settings

System ACPI Parameters.

ACPI Settings		
Enable ACPI Auto Configuration	Enables/disables BIOS ACPI Auto Configuration.	
	Enable	► Disable
Enable Hibernation	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.	
	► Enable	Disable
ACPI Sleep State	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.	
	Token =1DAB // Do NOT change this line	
	Suspend Disabled	► S3 (Suspend to RAM)

4.4.17 UEFI Variables Protection

NVRAM Runtime Variable Protection Settings.

SMART Settings		
Password protection of Runtime Variables	Control the NVRAM Runtime Variable protection through System Admin Password	
	► Enable	Disable

4.4.18 Serial Port Console Redirection

Serial Port Console Redirection

Serial Port Console Redirection		
Console Redirection EMS	Console Redirection Enable or Disable.	
	Enable	► Disable

4.4.19 Switchable Graphics

Switchable Graphics selections

Switchable Graphics	
GPU Package Power Limit Value	ATIF function 22 to get GPU Package Power Limit Default:0x0 Minimum:0x0 Maximum:0xFF00
	0

4.4.20 AMI Graphic Output Protocol Policy

User Select Monitor Output by Graphic Output Protocol.

Switchable Graphics	
Output Select	Output Interface
	DP1 [ACTIVE]

4.4.21 Option ROM Dispatch Policy

Option ROM Dispatch Policy.

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

4.4.22 PCI Subsystem Settings

PCI Subsystem Settings

PCI Subsystem Settings	
Re-Size BAR Support	If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support.
	Disable ► Enabled
SR-IOV Support	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.
	Disable ► Enabled
BME DMA Mitigation	Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked
	► Disable Enabled

4.4.23 USB Configuration

USB Configuration Parameters

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 5 sec 10 sec ► 20 sec
Device reset time-out	USB mass storage device Start Unit command time-out.
	10 sec ► 20 sec 30 sec 40 sec
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.
	► Auto Manual

4.4.24 Network Stack Configuration

Network Stack Settings.

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

4.4.25 NVMe Stack Configuration

NVMe Device Options Settings.

4.4.26 SATA Configuration

SATA Devices Information.

4.4.27 RAM Disk Configuration

Press <Enter> to add/remove RAM disks.

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

4.4.28 T1s Auth Configuration

Press <Enter> to select T1s Auth Configuration.

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

4.4.29 Broadcom BCM57416 NetXtreme-E 10GBASE-T RDMA Ethernet Controller

- 00:00:00:00:00:00

Configure Device Parameters.

Broadcom BCM57416 NetXtreme-E 10GBASE-T RDMA Ethernet Controller - 00:00:00:00:00:00				
Firmware Image Menu	Firmware image information			
	Family Firmware Version	Installed device firmware family version information. 227.1.114.0		
	Boot Code	Boot Code 227.0.135.0		
	MBA	Multiple Boot Agent 227.0.135.0		
	EFI	UEFI Option ROM 227.0.133.0		
	NCSI	Management FW 227.0.135.0		
	RDMA FW	RDMA FW 227.0.135.0		
Device Configuration Menu	Device Configuration Menu.			
	Multi-Function Mode	Configure NIC Hardware Mode. Switching from multi-function to single function will result in the clearing of Virtual Function values in the extended partitions. Advanced NPar option is a feature preview only. ▶SF NPAR 1.0		
	SR-IOV	Enable/Disable Single Root I/O Virtualization. ▶Disabled Enabled		
	Number of MSI-X Vectors per VF	Configure number of MSI-X Vectors per VF (1-64). 16		
	Maximum Number of PF MSI-X Vectors	Configure maximum number of PF MSI-X Vectors (0-152 per controller). 74		
	Energy Efficient Ethernet	Configure Energy Efficient Ethernet operation. ▶Disabled Enabled		
	Operational Link Speed	Configure the default link speed for the selected port. On dual port adapters, if one port is configured for 10G and user selects 25G on the othre port, both ports will be set to 25G, or vice versa. If either port is set to Auto Negotiated, ensure that one port does not attempt to operate at 10 Gbps while the... AutoNeg		
	Support RDMA	Configure RDMA Support for this port. ▶Disabled Enabled		
	DCB Protocol	▶Disabled	Enabled (IEEE only)	CEE (only) Both (IEEE preferred with fallback to CEE)
	LLDP nearest bridge	Configure LLDP nearest bridge state. Disabled ▶Enabled		
	Default EVB Mode	Configure Default Edge Virtual Bridging mode. ▶VEB VEPA None		
	Enable PME Capability	Configure PME Capability support. Disabled ▶Enabled		
	Flow Offload	Configure Flow Offload Mode. This Feature is supported on Linux DPDK only. Not supported on Windows or ESX OS. ▶Disabled Enabled		
	Adapter Error Recovery	Enable recovery of firmware from fatal errors without manual intervention, host reboot and power cycle. ▶Disabled Enabled		

MBA Configuration Menu	Configure Multiple Boot Agent (MBA) parameters.			
	Option ROM	Controls the enablement of legacy Boot Protocols in the Option ROM.		
		Disabled ▶ Enabled		
	Legacy Boot Protocol	Select a boot protocol to be used in legacy BIOS (non-UEFI) boot mode.		
		▶ PXE NONE		
	Boot Strap Type	Specify the boot strap method used to boot to the operating system.		
		▶ Auto Detect BBS Int 18h Int 19h		
	Pre-boot Wake On LAN	Configure Pre-boot Wake on LAN (WOL).		
		Disabled ▶ Enabled		
	VLAN Mode	Virtual LAN mode enables use of a VLAN tag.		
		▶ Disabled Enabled		
	Boot Retry Count	Specify the number of retries to attempt in case of a boot failure.		
		No Retry	1 Retry	2 Retries
		4 Retries	▶ 5 Retries	6 Retries
				Indefinite Retries
Blink LEDs	Blink LEDs for a duration up to 15 seconds. 0			
Link Status	Link Status. Disconnected			
Permanent MAC Address	Permanent MAC Address. 00:00:00:00:00:00			
Virtual MAC Address	Virtual MAC Address 00:00:00:00:00:00			
Restore Defaults	Reset adapter to factory defaults.			

4.4.30 Intel(R) Rapid Storage Technology

This formset allows the user to manage RAID volumes on the Intel(R) RAID Controller.

Intel(R) Rapid Storage Technology	
No disks connected to system	

4.5 Security



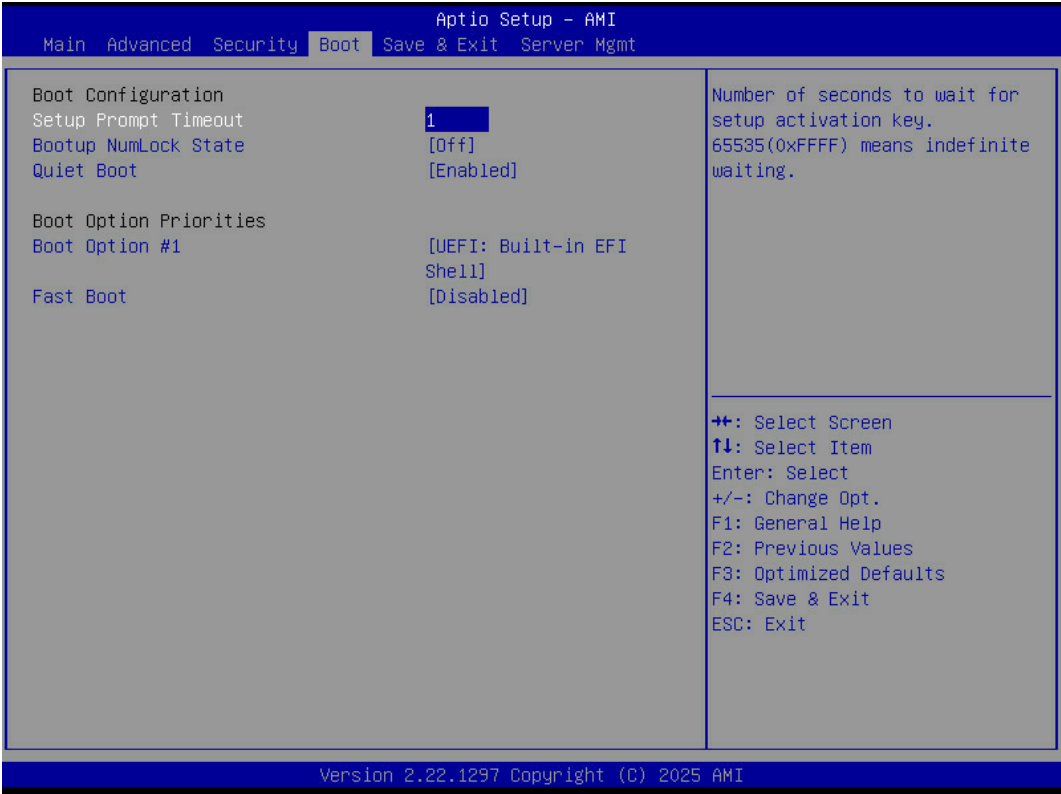
4.5.1 Administrator Password
Set Administrator Password.

4.5.2 User Password
Set User Password.

4.5.3 Secure Boot
Secure Boot configuration

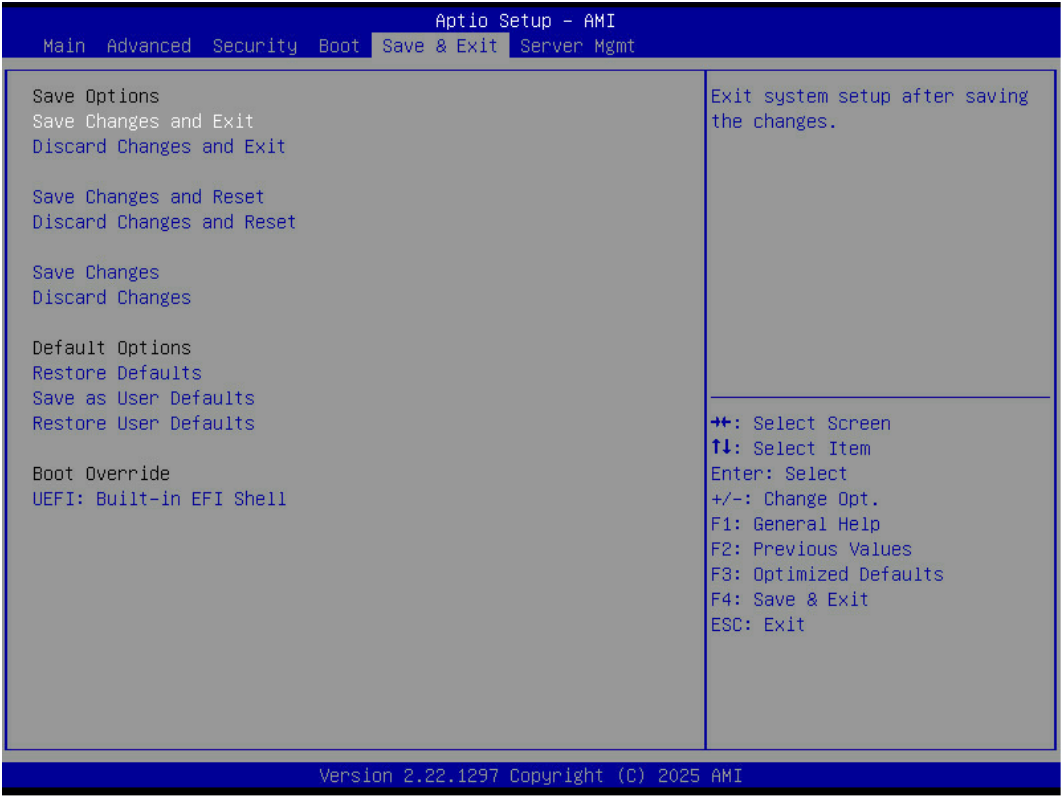
Secure Boot		
Secure Boot	Secure Boot feature is Active if Secure Boot is Enabled, Platform Key(PK) is enrolled and the System is in User mode. The mode change requires platform reset	
	► Disable	Enable
Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication	
	► Standard	Custom

4.6 Boot



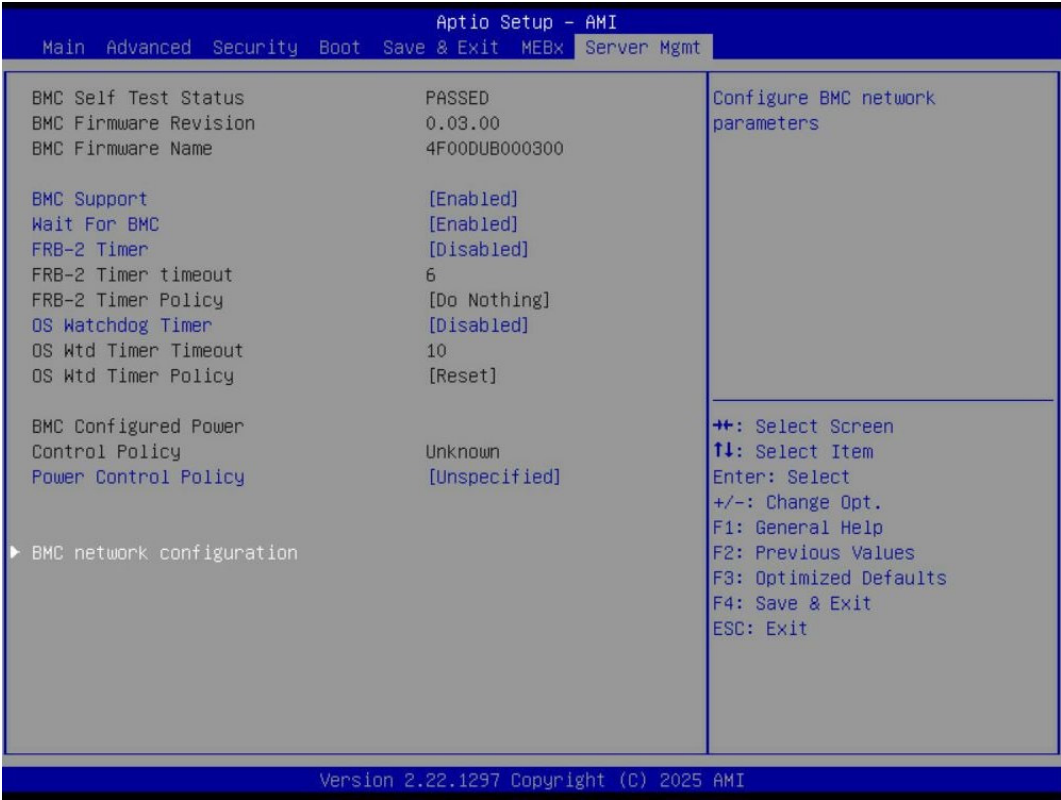
Boot		
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.	
	1	
Bootup Numlock State	Select the keyboard Numlock state.	
	On	► Off
Quiet Boot	Enables or disables Quiet Boot option.	
	Enabled	► Disabled
Boot Option #1	Sets the system boot order.	
	►UEFI: Build-in EFI Shell	Disabled
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.	
	Enabled	► Disabled

4.7 Save & Exit



Save & Exit	
Save Change and Exit	Exit system setup after saving the changes.
Discard Changes and Exit	Exit system setup without saving any changes.
Save Changes and Reset	Reset the system after saving the changes.
Discard Changes and Reset	Reset system setup without saving any changes.
Save Changes	Save changes done so far to any of the setup options.
Discard Changes	Discard changes done so far to any of the setup options
Restore Defaults	Restore/Load default values for all the setup options.
Save as User Defaults	Save the changes done so far as User Defaults.
Restore User Defaults	Restore the user defaults to all the setup options.
UEFI: Built-in EFI Shell	

4.8 Server Mgmt



4.8.1 BMC Support

Enable/Disable interfaces to communicate with BMC.

► Enabled
Disabled

4.8.2 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 interface.

► Enabled
Disabled

4.8.3 FRB-2 Timer

Enable or Disable FRB-2 timer (POST timer).

Enabled
► Disabled

4.8.4 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.

Enabled
► Disabled

4.8.5 Power Control Policy

Configure how the system should respond if AC Power is lost, Reset not required as selected Power policy will be set in BMC when policy is saved.

Do Not PowerUp	Last Power State
Power Restore	► Unspecified

4.8.6 BMC network configuration

Configure BMC network parameters.

BMC network configuration				
Lan channel 1/ Lan channel 2				
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.			
	►Unspecified	Static	DynamicBmcDhcp	DynamicBmcNonDhcp
IPv6 Support	Enable or Disable LAN1/2 IPv6 Support.			
	►Enabled		Disabled	
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.			
	►Unspecified	Static	DynamicBmcDhcp	
Configuration Router Lan1/2 Address source	Select to configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.			
	►Unspecified	Static	DynamicBmcDhcp	
VLAN Support	Enable VLAN Support to specify the 802.1q VLAN ID.			
	►Unspecified	Enabled	Disabled	

4.9 BIOS Update Process

This is the manual for updating BIOS on **Duba** system. Please check current system BIOS version is **Dubc0003** or later. Here are the update procedures.

Windows:

1. Copy **Dubc0004**.bin to EFI folder
2. Copy AfuWin64 folder to USB stick or HDD
3. **Boot into internal shell** enters the usb AfuWin64 folder and executes the **flash.nsh**
4. If the firmware update is complete, perform an AC power cycle.

Linux:

1. Copy **Dubc0004**.bin to AfuLnx64 folder
2. Copy AfuLnx64 folder to USB stick or HDD
3. Enter to AfuLnx64 folder and execute the below command./flash.sh
4. Reboot if complete the updated



NOTE

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

4.10 BIOS Post Code

There are two portions of Post code in BIOS, Intel RC Post code and AMI BIOS Post code. In the early power up stage, CPU executed Intel RC, and output Intel RC POST codes, AMI BIOS post code will be output after Intel RC done.

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

(1) Read the first 256 bytes: "\$ ipmitool -I lanplus -H 192.168.13.30 -U xxxx -P xxxx raw 0x32 0x73 0x00"

Please note that the second IPMI command only applies to Dubhe A Sku.

NOTE

BMC IP: -H \$BMC_IP

User Account: -U \$BMC_USER

Password: -P \$BMC_PASSWD

Intel RC

Post Code	Description
0x00DF	Failure Indication
0xDD00	Initialization Start
0xDD7F	Initialization End
0xDD01	Interpreter
0xDD03	CMD DS
0xDD04	VDDQ
0xDD05	CMD EQ
0xDD06	VCC LVR AUTO TRIM
0xDD07	CMD SR
0xDD08	VIEW PIN CAL
0xDD09	CMD DS Split
0xDD0A	CMD SR Split
0xDD0C	Unmatched RX CAL PRE
0xDD0D	DCC LPDDR5 WCK
0xDD0E	Data PI Linearity
0xDD0F	RX SAL TAIL CAL
0xDD11	FREQ Lock
0xDD12	DDRIO Init
0xDD14	DDRCOMP CAL PRE
0xDD15	DCC DATA DQ
0xDD16	Read VREF DECAP
0xDD18	TXDQTCO COMP Training
0xDD19	Margin Limit Check
0xDD1A	DCC Init
0xDD1B	Fast Boot Permitted
0xDD1C	Restore Non Training
0xDD1D	Print Input Params
0xDD1E	DCC Downstream
0xDD20	SPD Processing Static
0xDD21	Set Overrides

0xDD22	MC Capability
0xDD23	MC Config
0xDD24	PPR Enable
0xDD25	Print DDR MRS
0xDD26	Reset Sequence
0xDD27	PRE Training
0xDD28	Early Command
0xDD29	Sense AMP Offset
0xDD2B	Receive Enabl
0xDD2C	JEDEC Write Leveling
0xDD2D	LP5 WCK Mode
0xDD2E	Write Timing 1D
0xDD2F	Read Timing 1D
0xDD30	DIMM ODT
0xDD31	Early Write Timing 2D
0xDD32	Write DS
0xDD33	Write EQ
0xDD34	Early Read Timing 2D
0xDD35	Read DQS ODT
0xDD36	Read EQ
0xDD37	Read CTL
0xDD38	Write Timing 2D
0xDD39	Read Timing 2D
0xDD3A	CMD Vref
0xDD3B	Write Vref 2D
0xDD3C	Read Vref 2D
0xDD3D	Read DQ ODT
0xDD3E	Late Command
0xDD40	Turn Around
0xDD41	CMP OPT
0xDD42	Save Mc Values
0xDD43	Restore Training
0xDD44	RMT Tool
0xDD45	RX Rank to Rank
0xDD46	DIMM RON
0xDD48	MR FILL
0xDD49	PWR MTR
0xDD4A	SPD Processing Calc
0xDD4B	Write Voltage 1D
0xDD4C	Early Rdmpr Timing 2D
0xDD4D	DIMM DFE
0xDD4E	Roundtrip Match
0xDD4F	Roundtrip Match Finalize
0xDD50	Data Summary
0xDD51	RH Prevention
0xDD52	DDR5 ODT Config
0xDD53	Write DQ DQS Retraining

0x0055	Mem Init Done
0xDF55	Mem Init Done With Errors
0xDD57	Read Voltage 1D
0xDD58	Retrain Check
0xDD59	RMT Tool Bit
0xDD5A	SA GV Switch
0xDD5B	Alias Check
0xDD5C	ECC Clean Start
0xDD5D	REFPI Optimize
0xDD5E	DDR5 RX XTALK
0xDD62	CLKTCO COMP Training
0xDD65	WCKTCO COMP Training
0xDD67	DIMM ODT CA
0xDD68	DIMM ODT CA Split
0xDD69	Fill BDAT Structure
0xDD6A	WCK Leveling
0xDD6B	MBIST
0xDD6C	Unmatched Write Timing 1D
0xDD6E	REFPI CAL Post DCC
0xDD6F	DCC Rise Fall Alignment
0xDD70	DDR5 CKD Config
0xDD71	Normal Mode
0xDD72	MC Finalize
0xDD74	TX Rank to Rank
0xDD75	DCC LP5 WCK DCA
0xDD76	DCC DDR5 CLK
0xDD77	IBECC
0xDD78	Update Save Mc Values
0xDD79	Map DQDQS Swizzle
0xDD7A	RMT Tool Evenodd
0xDD7B	PMA Config
0xDD7C	DDRIO Finalize
0xDD7D	REFPI CAL
0xDF7E	No Memory Detected
0xDD7F	DCC DDR5 DQS

AMI BIOS standard POST Code

Post Code	Description
0x10	PEI core is started
0x11	Pre-memory CPU initialization is started
0x15	Pre-memory North Bridge initialization is started
0x19	Pre-memory South Bridge initialization is started
0x2B	Memory initialization. Serial Presence Detect (SPD) data reading
0x2C	Memory initialization. Memory Presence detection
0x2D	Memory initialization. Programming memory timing information
0x2E	Memory initialization. Configuring memory
0x2F	Memory initialization. (Other)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. Boot Strap Processor (BSP) initialization
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-memory North Bridge initialization is started
0x3B	Post-memory South Bridge initialization is started
0x4F	DXE IPL is started
S3 resume progress codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by the DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4~0xE7	Reserved for future AMI progress codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery process started
0xF4	Recovery firmware image is loaded
DXE Phase	
0x60	DXE code is started
0x61	NVRAM initialization
0x62	Initialization of the South Bridge runtimes services
0x63	CPU DXE initialization is started
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization
0x78	ACPI module initialization

0x79	CSM initialization
0x90	Boot Device Selection(BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Start of Setup
0xAB	Setup Input Wait
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM initialization
0xB3	Legacy Option ROM initialization
0xB4	USB Hot Plug
0xB5	PCI bus Hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reset (reset of NVRAM settings)