Zelus

Server Motherboard
User's Manual

UM_Zelus_v1.1_012126

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 Installation 10
Chapter 3. Motherboard Settings 11
3.1 Block Diagram 11
3.2 Placement 12
3.3 Content List 13
3.4 External Port 15
3.5 Connector Definition 16
3.6 Jumper Setting 26
3.7 LED 28
3.7.1 Front Panel LEDs 28
3.7.2 Rear Chassis LEDs 28
3.7.3 Internal LEDs 29
3.7.4 LEDs Placement 29
Chapter 4. BIOS Configuration Settings 30
4.1 Navigation Keys 30
4.2 BIOS Setup 31
4.2.1 Menu 31
4.2.2 Startup 31
4.3 Main 32
4.3.1 Main 32
4.4 Advanced 33
4.4.1 Trusted Computing 33
4.4.2 PSP Firmware Versions 34
4.4.3 ACPI Settings 34
4.4.4 AMD CBS 35
4.4.5 AMD PBS 57
4.4.6 Serial Port Console Redirection 58
4.4.7 CPU Configuration 59
4.4.8 Debug Port Table Configuration 59
4.4.9 SIO Common Setting 59
4.4.10 SIO Configuration 59
4.4.11 PCI Subsystem Settings 60
4.4.12 USB Configuration 61

4.4.13 Network Stack Configuration 61
4.4.14 CSM Configuration 62
4.4.15 NVMe Configuration 62
4.4.16 SATA Configuration 62
4.4.17 AMD Mem Configuration Status 62
4.4.18 Tls Auth Configuration 63
4.4.19 RAM Disk Configuration 63
4.4.20 Driver Health 63
4.5 Chipset 64
4.5.1 PCIe Link Training Type 64
4.5.2 PCIe Compliance Mode 64
4.5.3 South Bridge 65
4.5.4 North Bridge 66
4.6 Security 67
4.7 Boot 68
4.8 Save & Exit 71
4.9 Server Mgmt 72
4.9.1 BMC Support 72
4.9.2 Wait for BMC 72
4.9.3 Power Control Policy 73
4.9.4 System Event Log 73
4.9.5 BMC network configurtion 73
4.9.6 View System Event Log 73
4.10 BIOS Post Code 74
Chapter 5. Technical Support 92

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

Chapter 1 Product Features
This chapter delivers the overall layout of the product, including the fundamental components on the motherboard, design specifications, and noteworthy features. Scutum is an ideal server grade motherboard that is specifically designed to accommodate diverse enterprises for managing heavy workloads, databases, nearline applications, and cloud deployments. This product supports the single AMD EPYC™ 8000-series processor with Socket SP6 socket type and 6 channel per slot DDR5 RDIMM with EEC up to 4800 MHz.

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

Chapter 3 Motherboard Settings
This chapter elaborates the overall layout of the server motherboard, including multifarious connectors, jumpers, and LED descriptions. These descriptions assist users to configure different settings and functions of the motherboard, as well as to confirm the location of each connector and jumper.

Chapter 4 BIOS Configuration Settings
This chapter introduces the key features of BIOS, including the descriptions and option keys for diverse functions. These details provide users to effortlessly navigate and configure the input/output devices.

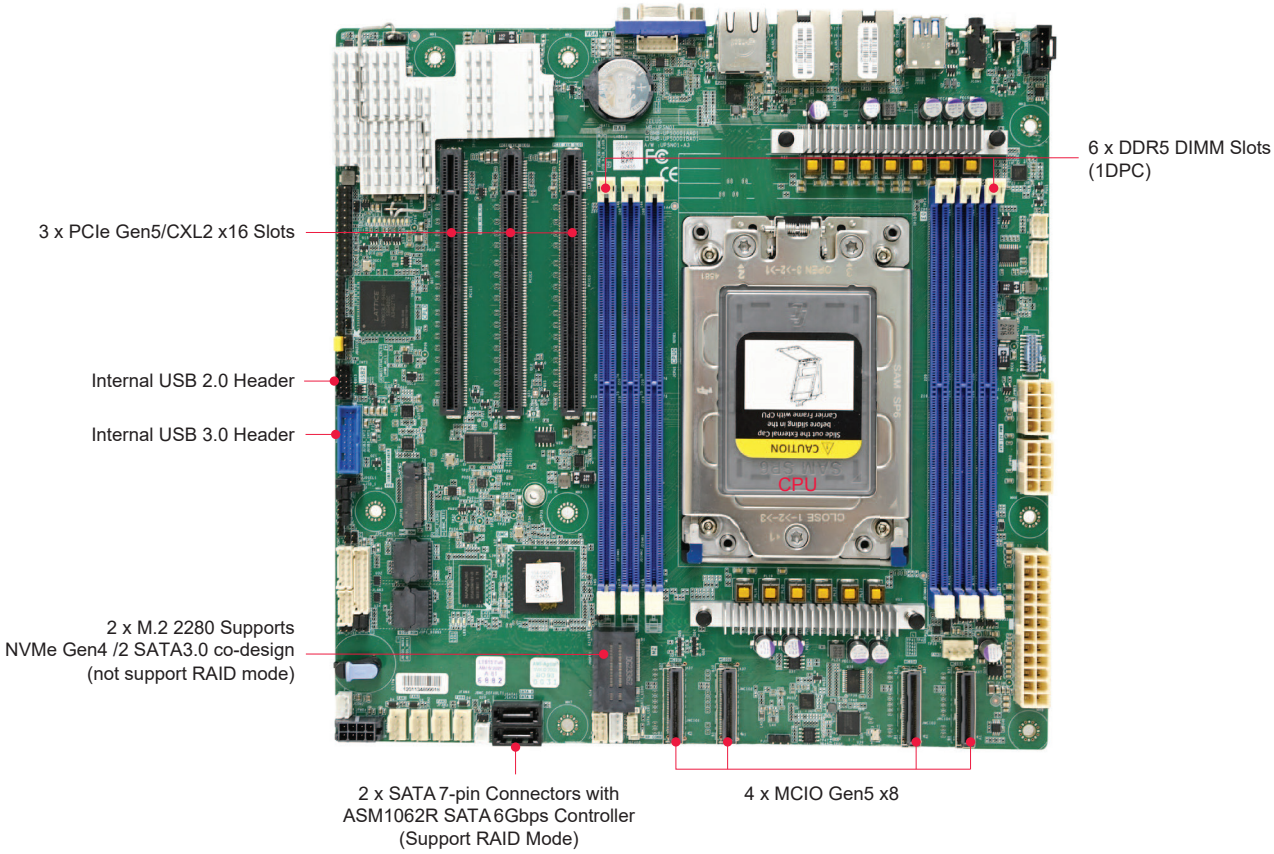
Chapter 5 Technical Support
For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: https://www.aicipc.com/en/index. It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

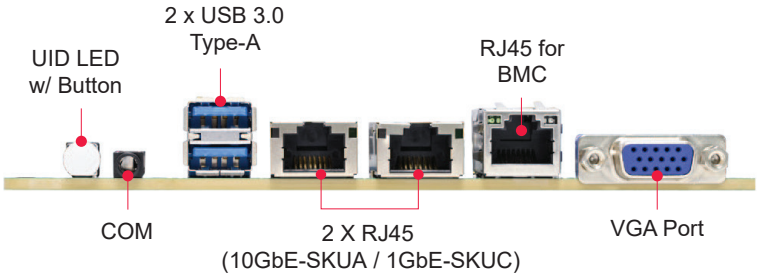
This section describes the hardware specifications and features of the Zelus motherboard. The fundamental components of the Zelus severboard are provided below.

1.1 Component

Zelus Serverboard



I/O View



Dimensions
mm : 243.84 x 245.2
inches : 9.6 x 9.65

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

1.2 Specifications

System	Processor Support	Single AMD EPYC™ 8000-series Processors
	CPU TDP	225W
	Socket Type	Socket SP6
	System Memory	• DDR5 4800MHz 1DPC RDIMM • Total 6 memory slots
	Expansion Slots	• 3 x PCI Express Gen5 x16 slots • 4 x MCIO x8 (PCIe Gen5) Total support 80 lanes of PCI Express Gen5 • 2 x NGFF(M.2) M-Key(2280) support NVMe x4/SATA co-design
System BIOS	BIOS Type	AMI UEFI BIOS
	BIOS Features	• ACPI • PXE • AC loss recovery • IPMI KCS interface • SMBIOS • Serial console redirection • SRIOV • TPM • PCIe hotplug
On-board Devices	SATA	2 x SATA 7-pin connectors with ASM1062R SATA 6Gbps Controller (Support RAID 0, RAID 1, SPAN)
	BMC	Aspeed AST2600 Advanced PCIe Graphics & Remote Management Processor • Baseboard Management Controller • Intelligent Platform Interface 2.0 (IPMI 2.0) • iKVM, Media Redirection, IPMI over LAN, Serial over LAN • SMASH support • HTML5 • Redfish

On-board Devices	Network Controller	• Realtek RTL8211FS GbE for BMC dedicate management port (NCSI shared NIC - reserved for Broadcom NIC) • Broadcom BCM57416/BCM5720L co-design supports 2 x 10G Base-T/1GbE
	Graphics	Integrated VGA support by ASPEED AST2600 Resolution up to 1920x1200 @60Hz 32bpp
Input/Output	SATA	2 x SATA 7-pin connectors with ASM1062R SATA 6Gbps Controller (Support RAID 0, RAID 1, SPAN)
	LAN	• 2 x RJ45 connectors for dual port 10GbE/GbE • 1 x RJ45 connector (for BMC management port)
	USB	• 2 x USB 3.0 double-stack Type-A connectors • 2 x USB pin headers support 4 x USB 3.0/2.0
	VGA	1 x external VGA port
	Serial Port	• 1 x external COM port • 1 x internal COM box header
	Additional Information	Security: • TPM 2.0 onboard

1.3 Feature

The Zelus server board offers the latest AMD EPYC™ SoC technology with efficiency core/power in an x86-architecture with EPYC™ 8000-series processor, 6x DDR5 memory channels and 96x PCIe Gen5 bandwidth with balanced I/O bandwidth that matches the capability of the CPU cores to move data to and from the network, spinning disks, NVMe storage, and graphics acceleration devices.

- Supports AMD EPYC™ 8000-series processor Siena based on the AMD "Zen4", future support Sorano (Zen5) microarchitecture for highest server performance
- Supports 6 DDR5 DIMM slots for maximum memory performance
- Supports 3 PCIe Gen5 x16 slots
- Supports four MCIO x8 total 32 PCI Express Gen5 lanes
- Onboard Baseboard Management Controller for system management and IPMI control
- Embedded components for 5+ year long life

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 AMD EPYC™ 9000-series processor and Socket SP5.

2.1.1 Installation

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

- ☑ a T20 Torx 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.

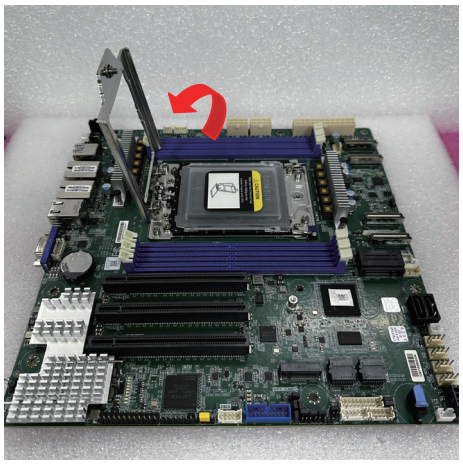
CAUTION
When unpacking a processor, hold the processor only by its edges to avoid touching the contacts.

Assembly of Package and Heatsink
Procesures:

Step 1: Open the captive screw and Retention Frame
① Use T-20 6-Lobe driver to loosen the captive screw and away from the Retention Frame.
② Loosen the captive screw the Retention Frame will automatically pump up.

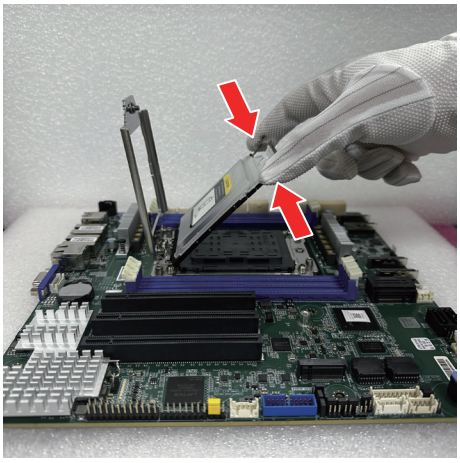
❶

❷

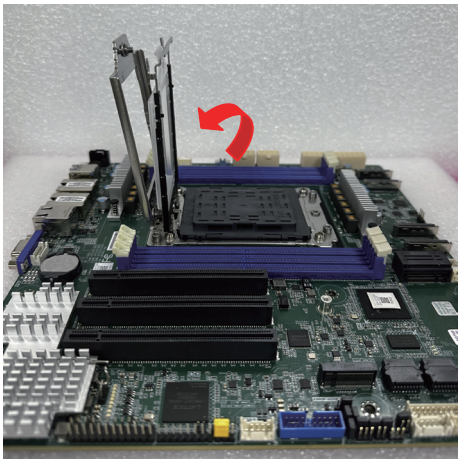


Step 2: Bounce the Rail Frame
① Use your the index finger the both hands placed on Rail Frame both sides of the metal handle.
② Then rotate Rail frame to fully open position.

❶



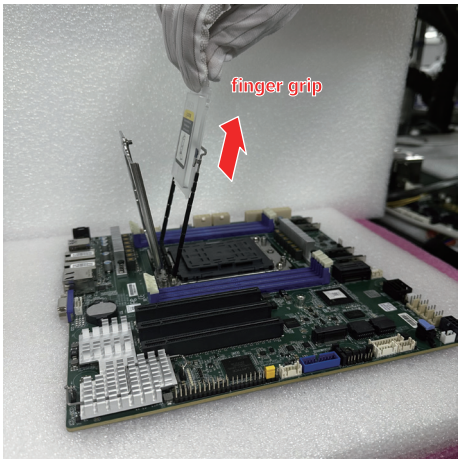
❷



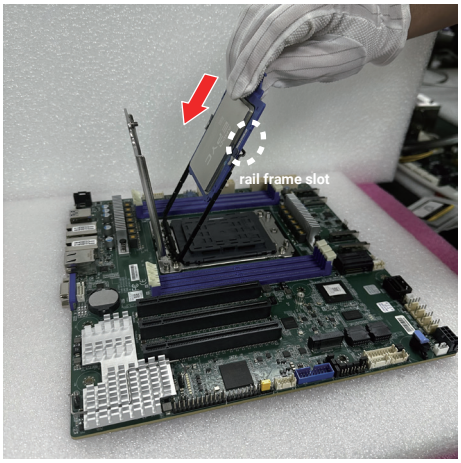
This information is provided for professional technicians only.

Step 3: Insert the package
① Hold the Rail Frame, then remove the External Cap.
② Insert the Carrier Frame with package into the Rail Frame slot by holding the finger grip.

❶



❷

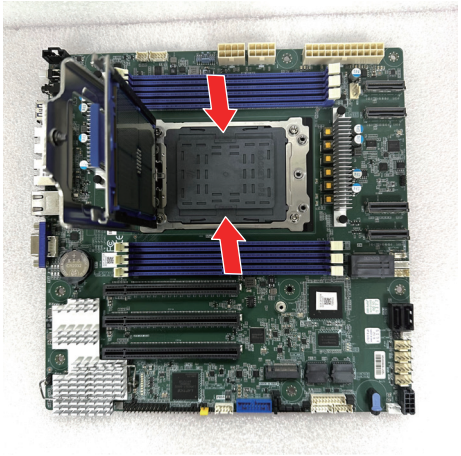


- Do not touch the package pad.
- Carrier Frame should slide into Rail Frame slot when insert the Package.

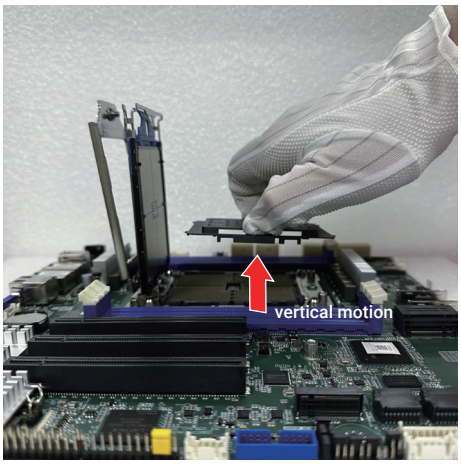
CAUTION
Be sure Carrier Frame with Package may be drop off if Frame did not fix by Rail Frame slot. Make sure carrier frame will slightly “click” with rail frame. Carrier Frame drop off will damage socket cap and contact.

Step 4: Remove PnP Cap
① Grip the two lift tabs marked "REMOVE" at the middle of the long sides of the PnP Cover Cap.
② Carefully remove the PnP Cap in a vertical motion only.

❶



❷



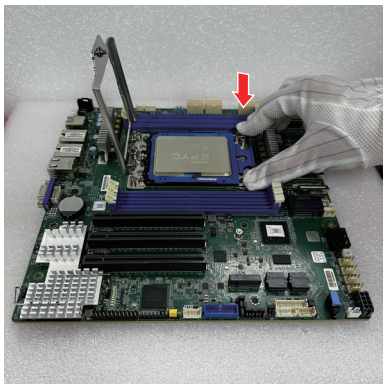
Step 5: Assembly Package and Heatsink Operation Guide

① Use the finger of two hands to press the Rail Frame with package on Stiffener Frame. Slightly press down with “click” feeling.

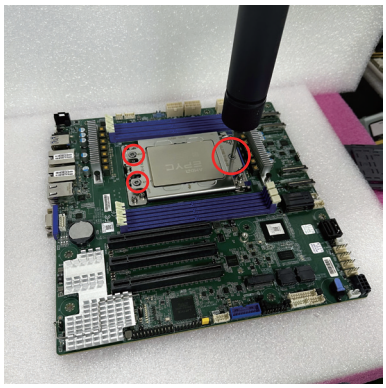
② Press Retention Frame and then tighten the captive screw.

③ Final status of whole assembly process.

❶



❷



❸

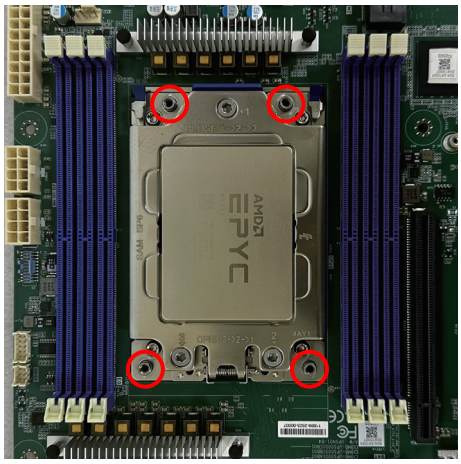
- Be care that Carrier Frame drop off with abnormal operation, Socket contact will been damaged.
- The applied torque must be within the range of 13.8±1.3 kg-f-cm (12.0±1.2 lb-f-in).

Step 6: Loading the Heatsink

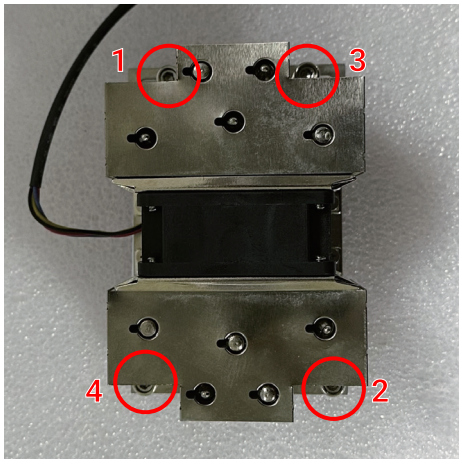
① Align the heatsink with the four nuts on the stiffener frame.

② Use T20 6 Lobe driver tighten 4 Heatsink nuts in sequence as 1 to 4. It is recommended to gradually tighten the screws by repeating this sequence several times to ensure the heatsink is balanced.

❶



❷



- The applied torque must be within the range of 13.8±1.3 kg-f-cm (12.0±1.2 lb-f-in).

2.2 System Memory

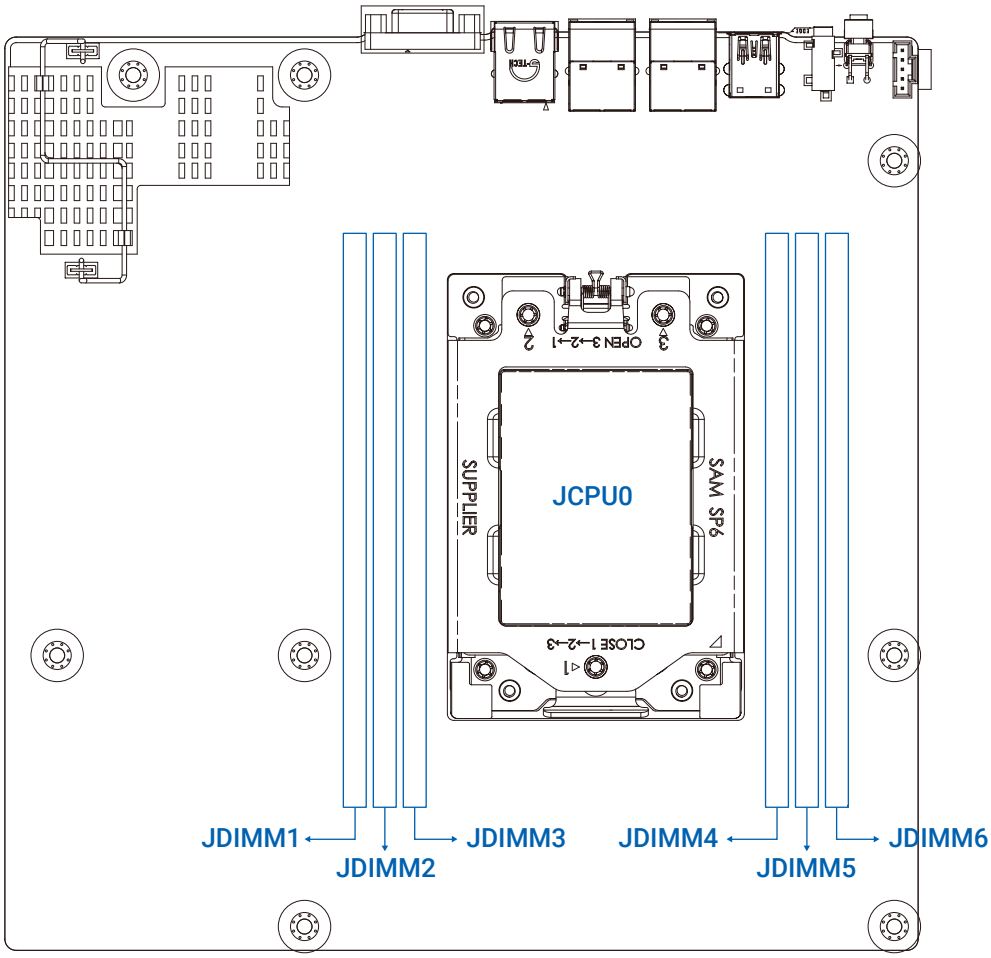
2.2.1 Placement

The DIMMs are displayed on the Zelus board as JDIMM1/JDIMM2/JDIMM3/JDIMM4/JDIMM5/JDIMM6

To ensure satisfactory performance, you need to:

☑ Verify the DIMM type:
This product supports DDR5 RDIMM

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



2.2.2 DIMM Population

NOTE
Rules to abide by before installation:
- Must install at least one DDR5 DIMM per socket.

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

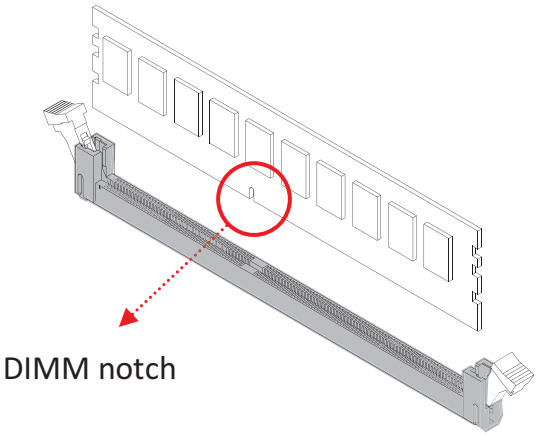
CPU Configuration

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

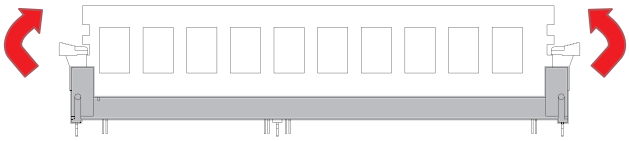
2.2.3 Installation

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

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



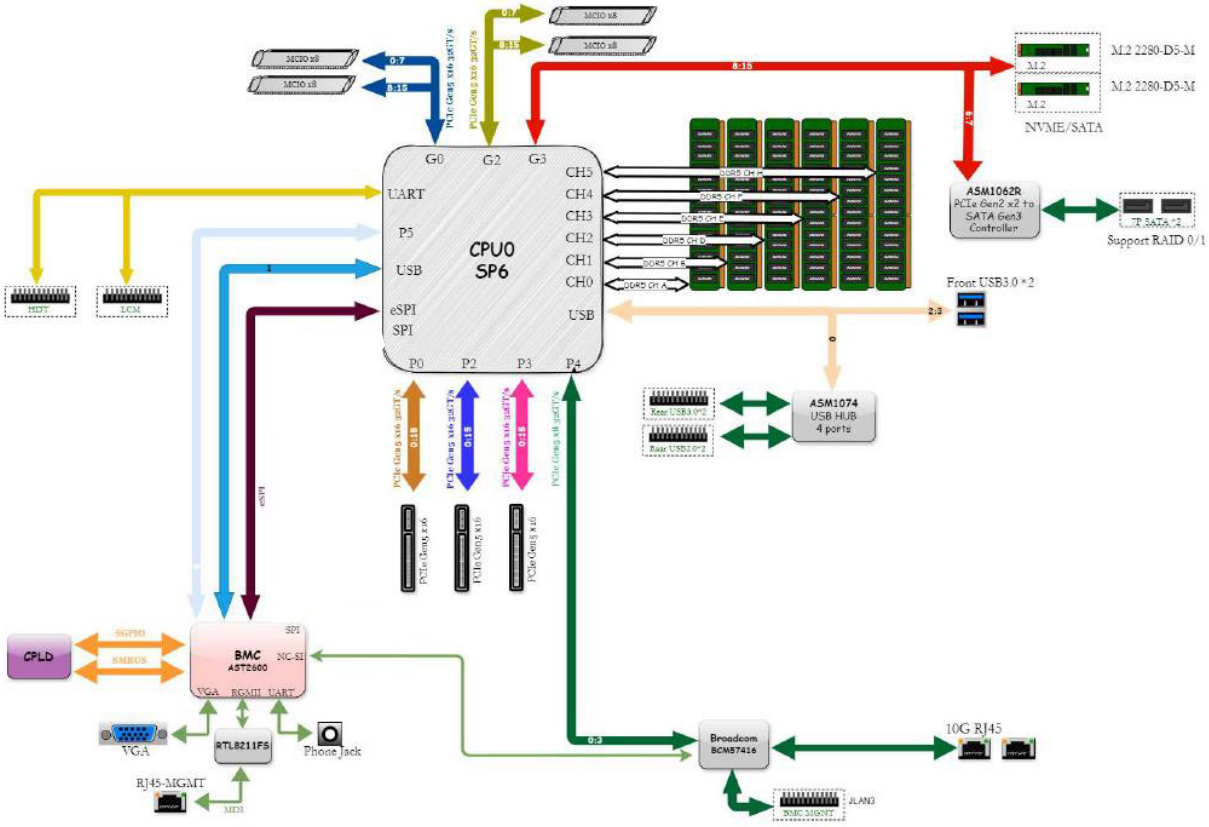
Step 3 Close the retaining clip to complete installation.



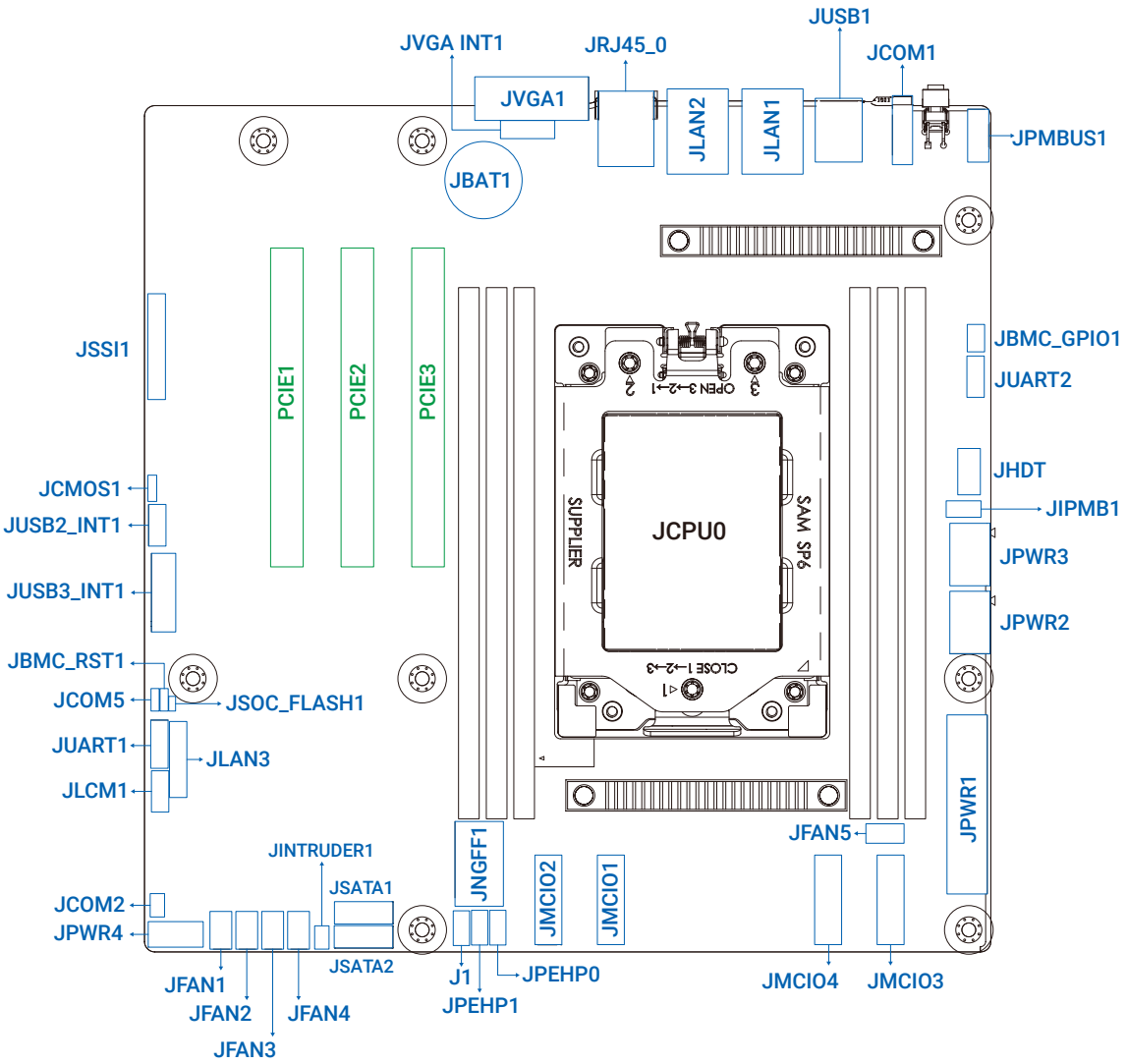
Chapter 3. Motherboard Settings

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

3.1 Block Diagram



3.2 Placement



3.3 Content List

External Connectors - Rear I/O

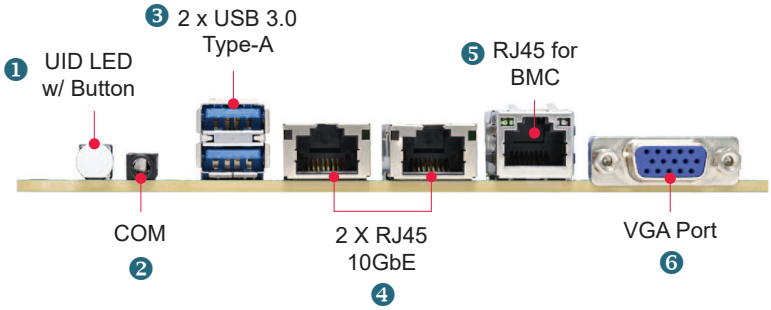
Function	Description	Comments
Ethernet x2	RJ45	JLAN1,JLAN2: 10G/1G NIC (Broadcom BCM57416) or 1G/100M NIC(Broadcom BCM5720L)
VGA	DSUB 15 Pin Blue Female	JVGA1
USB3.0 x2	USB3.0 Type A	JUSB1
Ethernet x1	RJ45	JRJ45_0: 10/100/1000M PHYCEIVER (RTL8211FS)
SERIAL PORT	Phone Jack	JCOM1

Internal Connectors Summary

Function	Description	Comments
Power Supply	12 x 2 Pin ATX CONN	JPWR1: 12V, 5V, 3.3V, 5VSB
Power Supply	4 x 2 Pin ATX CONN	JPWR2, JPWR3: 12V
Power CONN for FAN	4 x 2 Pin ATX CONN	JPWR4: 12V_FAN1-4
CPU	SP6 LGA4844	JCPU0
Front Panel	12 x 2 Pin 2.54mm Box Header	JSSI1
Front USB(3.0)	10 x 2 Pin 2.0mm Box Header	JUSB3_INT1
Front USB(2.0)	5 x 2 Pin 2.0mm Header	JUSB2_INT1
Front Ethernet(NCSI)	10 x 2 Pin 2.0mm Box Header	JLAN3
BMC GPIO	3 x 2 Pin 2.0mm Box Header	JBMC_GPIO1
FAN CONN	4 x 1 Pin 2.54mm Box Header	JFAN1~JFAN5
FAN Board CONN	4 x 2 Pin 2.0mm Box Header	J1
Serial ATA	7 Pin 1.27 mm Headers	JSATA1, JSATA2
PCIE Hot-Plug SMB	4 x 2 pin 2.0mm Box Header	JPEHP0
PCIE Hot-Plug CPU	4 x 1 pin 2.0mm Box Header	JPEHP01
HDT CONN	Samtec 10 x 2 Pin CONN	JHDT
BMC IPMB	4 x 1 Pin 2.0mm Box Header	JIPMB1
PMBUS	5 x 1 Pin 2.54mm Box Header	JPMBUS1
M.2 2280	GEN4_M2_KEY_M_ H=10.85MM (Stack type)	JNGFF1
BMC Debug Port	3 x 1 Pin 2.00mm Header	JCOM5
BMC Buzzer	2 x 1 Pin 2.54mm Header	JBUZZER1
Intruder	2 x 1 Pin 2.0mm Box Header	JINTRUDER1
BMC COM Port	5 x 2 Pin 2.0mm Box Header	JUART1
CPU COM Port	5 x 2 Pin 2.0mm Box Header	JUART2
COM Port to LCM	5 x 2 Pin 2.0mm Box Header	JLCM1
BMC COM Port	3 x 1 Pin 2.00mm Box Header	JCOM2
Battery Socket	2 Pin Socket	JBAT1
BMC Reset	2 x 1 Pin 2.0mm Header	JBMC_RST1
Program CPLD FW	8 x 1 Pin 2.54mm Header	JTAG_CPLD1
VRM SMB	3 x 1 Pin 2.54mm Header	PJ1
DIMM Sockets	288 Pin DDR5 DIMM	JEDEC Specified DDR5 Connector: JDIMM1~6
BIOS SPI ROM Socket	SOIC-16 Socket	JSPI_BIOS1
BMC SPI ROM Socket	SOIC-16 Socket	JSPI_BMC1

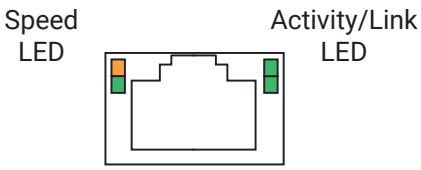
Function	Description	Comments
Clear CMOS	3 Pin 2.54mm Header	JCMOS1
BMC Disable	2 x 1 Pin 2.0mm Header	JBMC_DIS1
BMC RST PW	2 x 1 Pin 2.0mm Header	JBMC_DEFAULT1
CPU Bypass	3 x 1 Pin 2.0mm Header	JBIOS_MUX1, JBIOS_MUX2
BMC Socflash Enable	2 x 1 Pin 2.0mm Header	JSOC_FLASH1
BMC Bypass	2 x 1 Pin 2.0mm Header	JBMC_MUX1
PMBUS Power Select	3 x 1 Pin 2.54mm Header	JPMBUS_SEL1
Board SKU ID Select	2 x 1 Pin 2.0mm Header	JID_0~6

3.4 External Port



Item	Description
1	UID LED with Button
2	COM port
3	2 x USB 3.0 Type-A
4	2 x RJ45 10GbE
5	RJ45 for BMC
6	VGA Port

BMC Management RJ45 LED Indicator

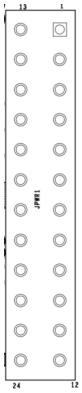


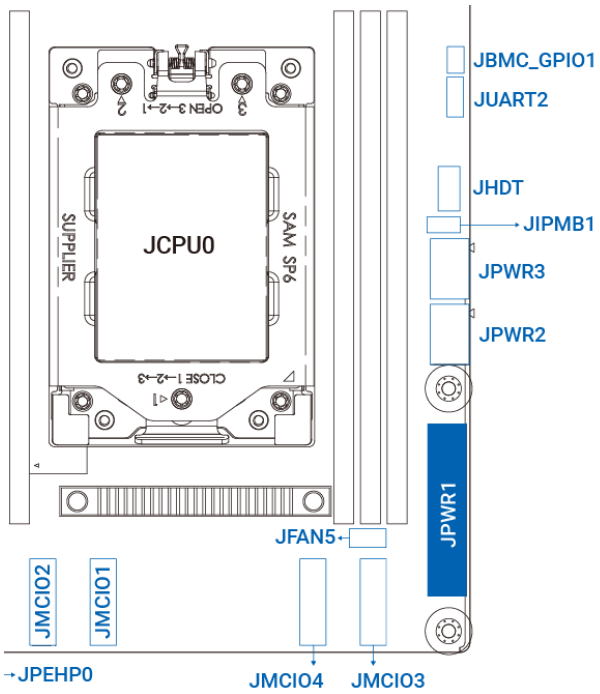
Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	10M bps connection or no link.
	Green	100M bps connection.
	Orange	1G bps connection.

3.5 Connector Definition

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

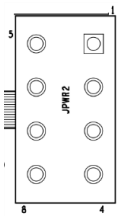
P3V3	13	1	P3V3
N.C.	14	2	P3V3
GND	15	3	GND
PSU_PSON_BUF_N	16	4	P5V_PSU
GND	17	5	GND
GND	18	6	P5V_PSU
GND	19	7	GND
N.C.	20	8	PSU_PWROK
P5V_PSU	21	9	P5V_STBY_PSU
P5V_PSU	22	10	P12V_PSU
P5V_PSU	23	11	P12V_PSU
GND	24	12	P3V3

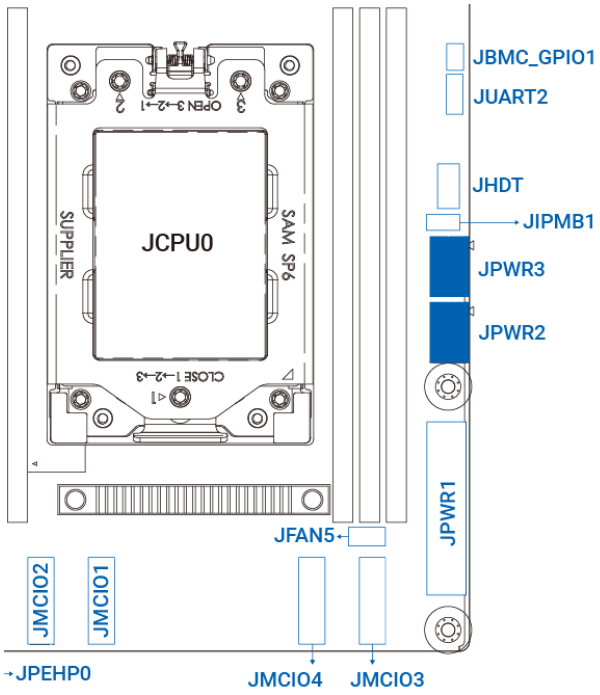




Power Supply Connector (JPWR2, JPWR3)
This is a 2x4-pin connector that provides the motherboard with power.

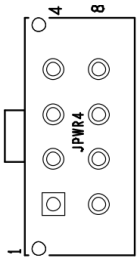
P12V_PSU	5	1	GND
P12V_PSU	6	2	GND
P12V_PSU	7	3	GND
P12V_PSU	8	4	GND

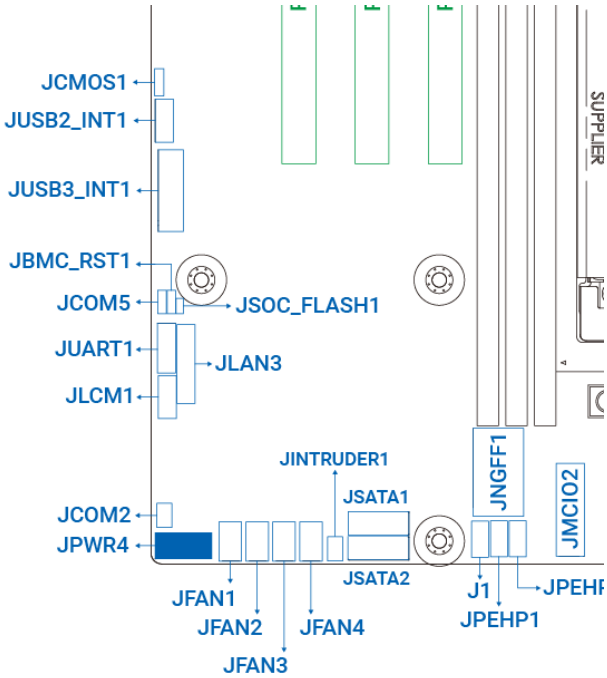




Power Supply Connector (JPWR4)
This is a 2x4-pin connector that provides the fan with power.

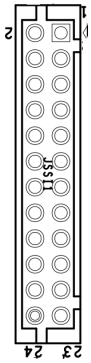
P12V_FAN4	4	8	GND
P12V_FAN3	3	7	GND
P12V_FAN2	2	6	GND
P12V_FAN1	1	5	GND

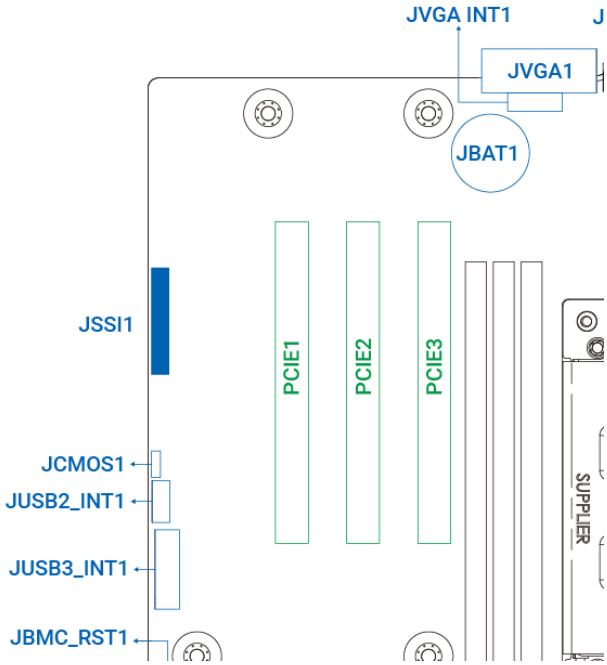




LED/Bezel Button Header (JSSI1)
This connector is a 2 x 12 Pin header.

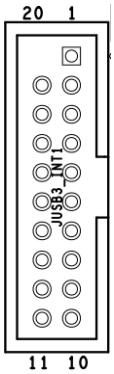
P3V3_AUX	2	1	FP_HDR_PWR_LED
P5V_STBY_PSU	4	3	NC
ID_LED_OUT_N	6	5	FP_PWR_LED_L
SYS_HEALTH2#	8	7	HDD_LED_P
SYS_HEALTH#	10	9	HDD_LED_N
LAN1_ACTLED_PWR	12	11	FP_PWR_BTN_N
LAN1_ACTLED_N	14	13	GND
SMBUS_SDA	16	15	FP_RST_BTN_N
SMBUS_SCL	18	17	GND
CHASSIS_OPEN	20	19	BMC_ID_IN_N
LAN 2_ACTLED_PWR	22	21	P3V3_AUX
LAN2 _ACTLED_N	24	23	FP_NMI_BTN_N

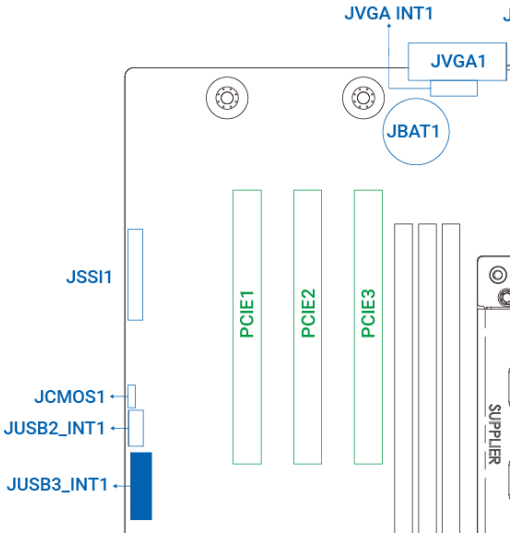




Front I/O USB3 Header (JUSB3_INT1)
This is a 19-pin header that supports USB in the front panel.

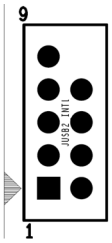
		1	P5V_USB23
P5V_USB23	19	2	USB3_HUB_RX_R_DN2
USB3_HUB_RX_R_DN1	18	3	USB3_HUB_RX_R_DP2
USB3_HUB_RX_R_DP1	17	4	GND
GND	16	5	USB3_HUB_TX_R_DN2
USB3_HUB_TX_R_DN1	15	6	USB3_HUB_TX_R_DP2
USB3_HUB_TX_R_DP1	14	7	GND
GND	13	8	USB2_HUB_R_DN2
USB2_HUB_R_DN1	12	9	USB2_HUB_R_DP2
USB2_HUB_R_DP1	11	10	USB_HUB_OCI2_N(NC)

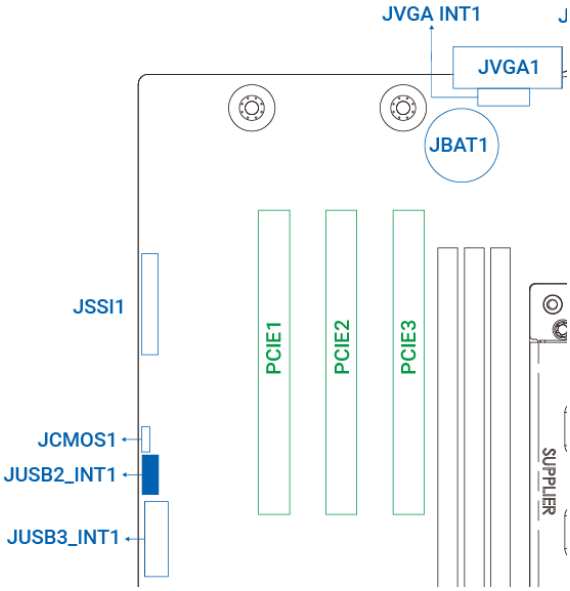




Front I/O USB Header (JUSB2_INT1)
This is a 9-pin header that supports USB in the front panel.

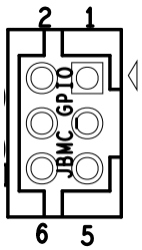
GND	9		
GND	7	8	GND
USB2_HUB_R_DP2	5	6	USB2_HUB_R_DP1
USB2_HUB_R_DN2	3	4	USB2_HUB_R_DN1
P5V_USB20	1	2	P5V_USB20

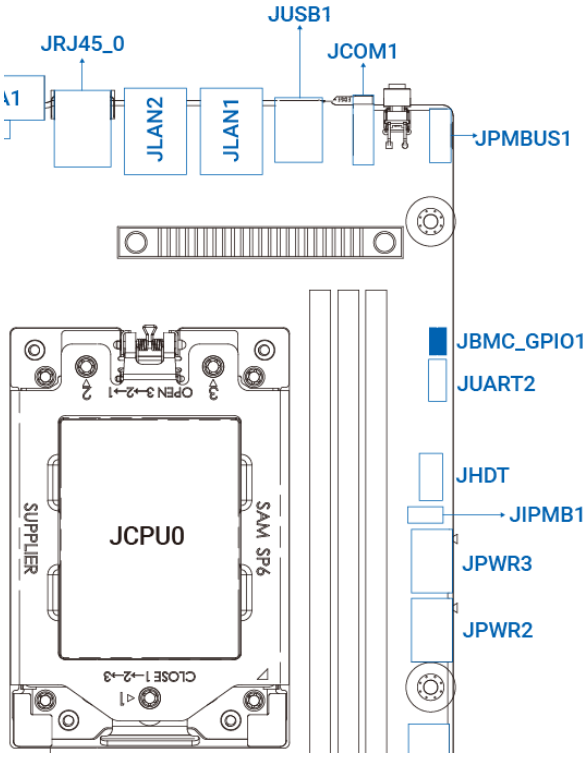




BMC GPIO header (JBMC_GPIO1)
This 2x3-pin header is used to provide BMC GPIO functionality.

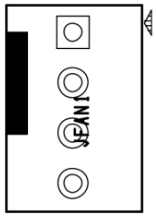
RACK_EXTRST_N	2	1	GND
BMC_GPY1	4	3	BMC_I2C_16_SDA
BMC_GPY0	6	5	BMC_I2C_16_SCL

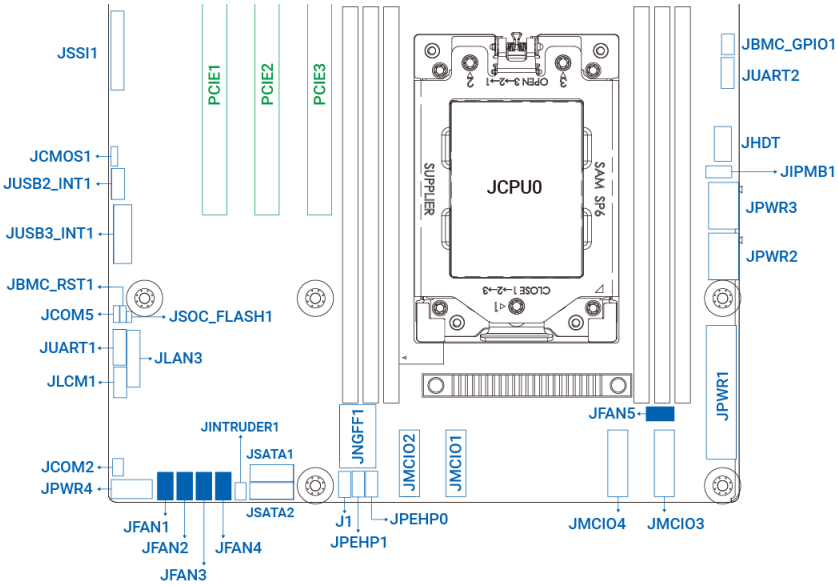




Fan Header (JFAN1~JFAN5)
This is a 4-pin Fan header.

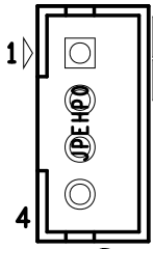
1	GND
2	P12V_FANx
3	FANx_R_TACH
4	FANx_R_PWM

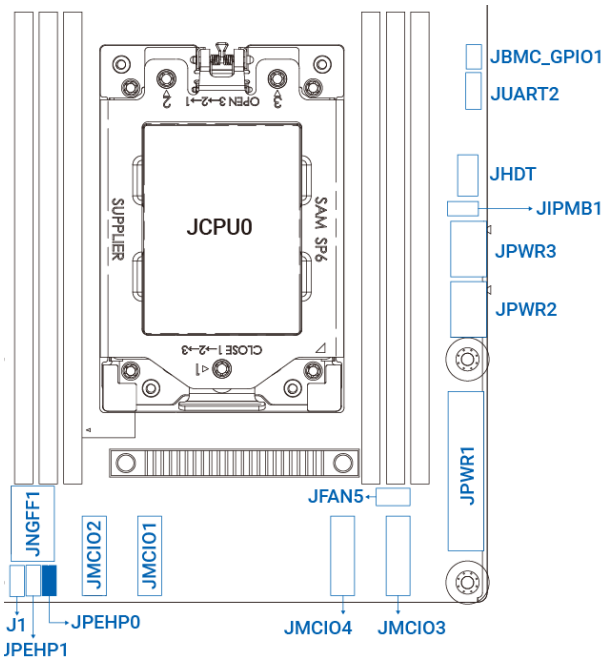




PCIe Hot-Plug header (JPEHP0)
This is a 4-pin connector that is used to provide PCIe Hot-Plug functionality.

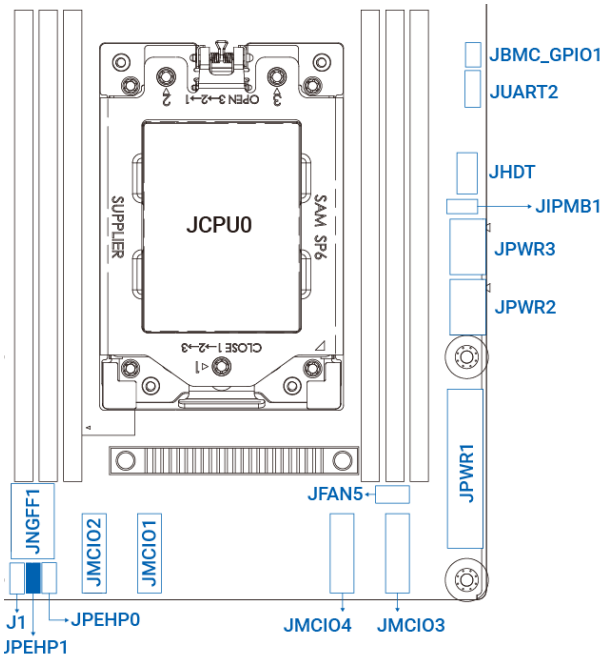
1	HP_HDR_CPU0_SDA
2	GND
3	HP_HDR_CPU0_SCL
4	HP_ALERT_CPU0_R_N





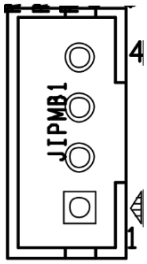
PCIe Hot-Plug header (JPEHP1)
This is a 4-pin connector that is used to provide PCIe Hot-Plug functionality.

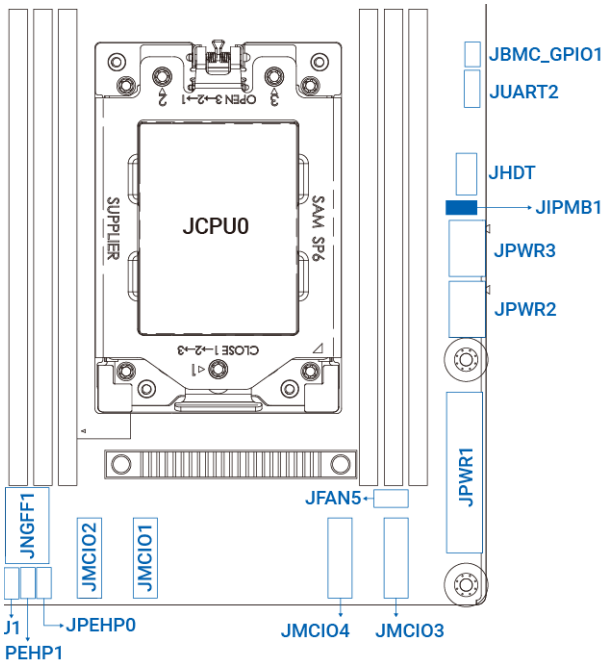
1	JPEHP_I2C_SDA
2	GND
3	JPEHP_I2C_SCL
4	JPEHP_I2C_ALERT



BMC IPMB header (JIPMB1)
This is a 4-pin header that is used to provide BMC I2C14 IPMB functionality.

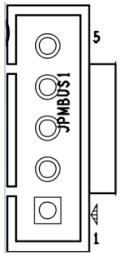
1	BMC_I2C_14_SDA
2	GND
3	BMC_I2C_14_SCL
4	NC

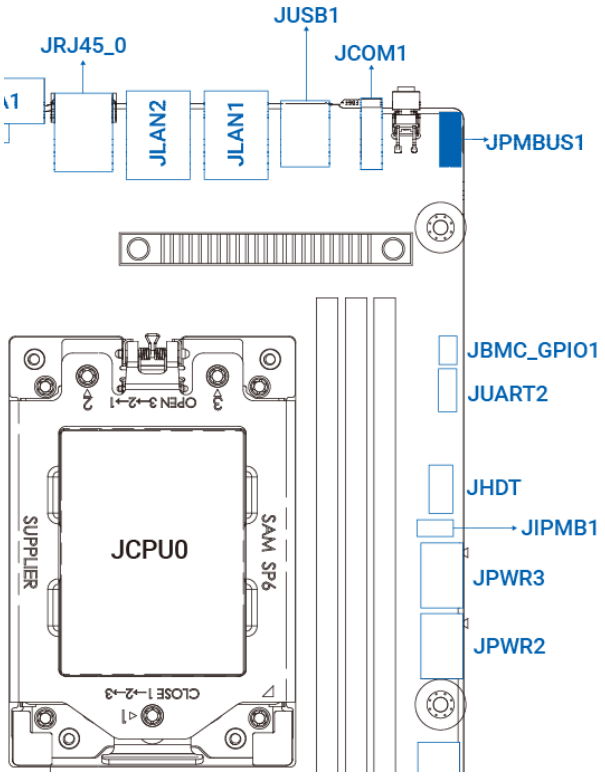




PMBUS header (JPMBUS1)
This is a 4-pin header that is used to provide PMBus functionality.

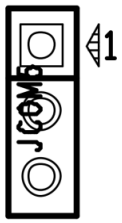
1	SMB_PMBUS_SCL
2	SMB_PMBUS_SDA
3	PMBUS_ALERT_N_C
4	GND
5	P5V_P3V3_AUX

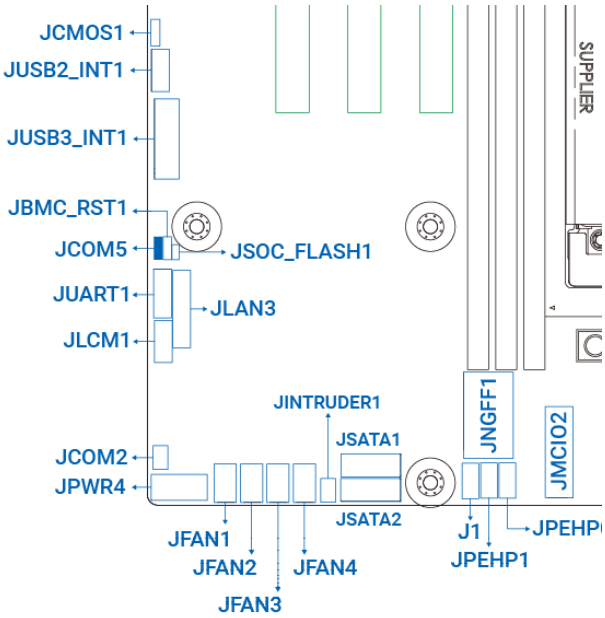




BMC Debug port header (JCOM5)
This 3-pin header is used to provide BMC Debug port functionality.

1	SPE_TXD
2	GND
3	SPE_RXD



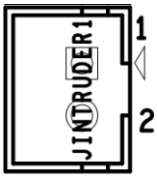


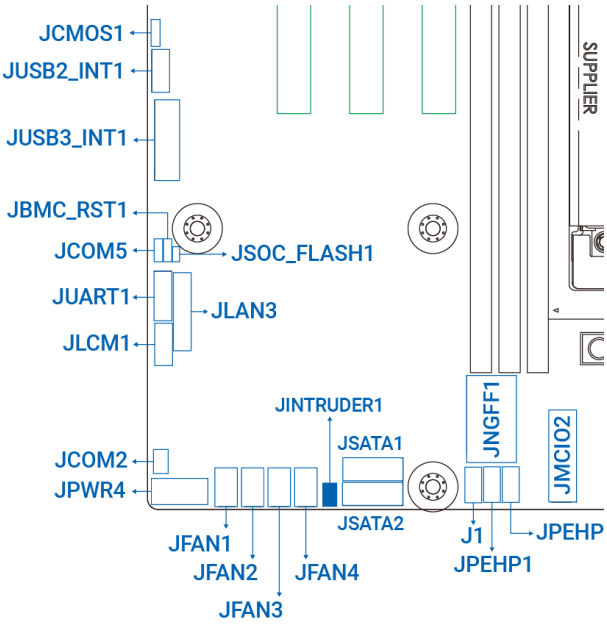
BUZZER header (JBUZZER1)
This 2-pin header is used to provide Buzzer functionality.

1	P5V_PSU
2	BMC_BUZZER-

Chassis Intrusion header (JINTRUDER1)
This 2-pin header is used to provide chassis intrusion functionality.

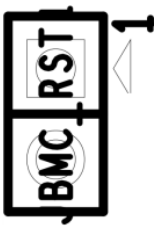
1	CHASSIS_OPEN
2	GND

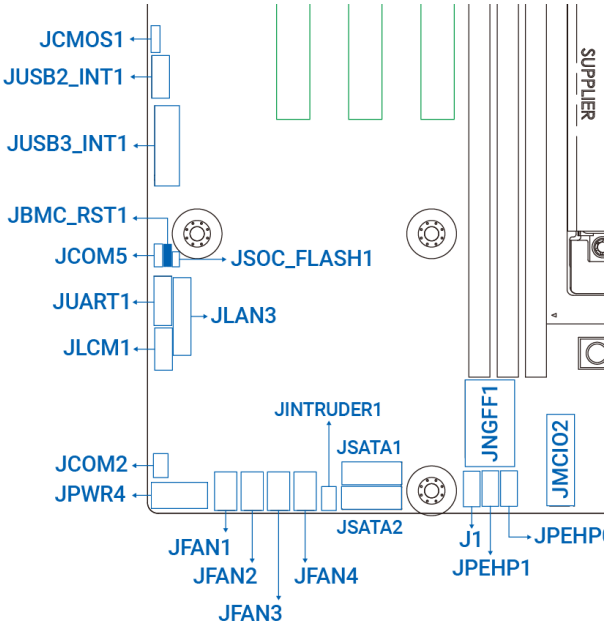




BMC RESET header (JBMC_RST1)
This 2-pin header is used to provide BMC RESET functionality.

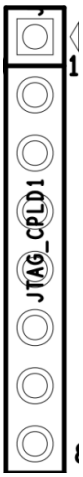
1	BMC_RESET
2	GND





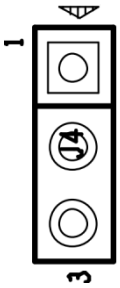
CPLD JTAG header (JTAG_CPLD1)
This 8-pin header is used to provide CPLD JTAG functionality.

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



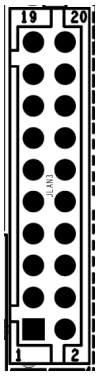
VRM SMB header (J4)
This 3-pin header is used to provide VRM SMB functionality.

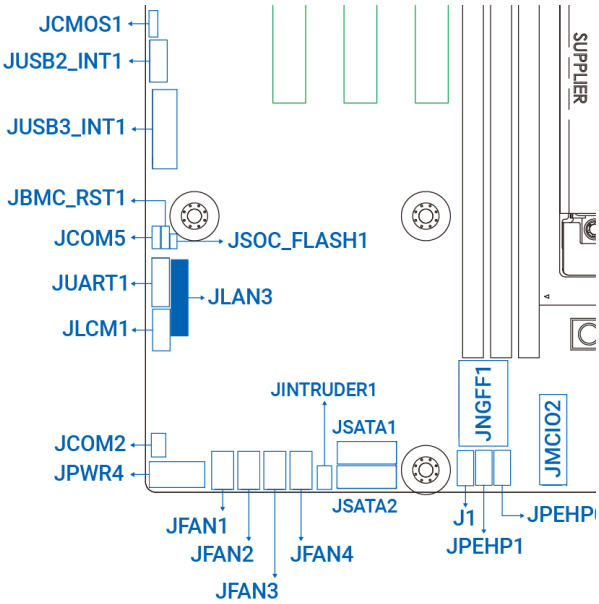
1	I2C_BMC_6_VR_CPU_SCL
2	GND
3	I2C_BMC_6_VR_CPU_SDA



Front ethernet (JLAN3)
This 2x4-pin header is used to provide BCM5720 MDI functionality.

NC	19	20	NC
LAN1_TRAFFIC	17	18	+3V3_S5
LAN1_LINK_100	15	16	LAN1_LINK_1000
GND	13	14	GND
EXT1_MDI_SP_P2	11	12	EXT1_MDI_SP_P3
EXT1_MDI_SP_N2	9	10	EXT1_MDI_SP_N3
GND	7	8	GND
EXT1_MDI_SP_P0	5	6	EXT1_MDI_SP_P1
EXT1_MDI_SP_N0	3	4	EXT1_MDI_SP_N1
GND	1	2	GND





3.6 Jumper Setting

BMC Reset Jumper (JBMC_RST1)

JBMC_RST1	Setting	
Short	Reset BMC	
Open	Normal	Default

CMOS Jumper (JCMOS1)

JCMOS2	Setting	
Pin1-2	Normal	Default
Pin2-3	Clear CMOS	

BMC Disable Jumper (JBMC_DIS1)

JBMC_DIS1	Setting	
Short	Disable BMC ARM boot	
Open	Normal	Default

BMC Reset Password Jumper (JBMC_DEFAULT1)

JBMC_DIS	Setting	
Short	Reset BMC Password	
Open	Normal	Default

CPU SPI Flash Jumper (JBIOS_MUX1, JBIOS_MUX2)

JBIOS_MUX1	JBIOS_MUX2	Setting	
Pin1-2	Pin1-2	CPU to Flash Bypass	Default

BMC Socflash Configurations (JSOC_FLASH1)

JSOC_FLASH1	Setting	
Short	Enable	
Open	Disable	Default

BMC SPI MUX Jumper (JBMC_MUX1)

JBMC_MUX1	Setting	
Pin2-3	BMC to Flash Bypass	Default

PMBUS Power select Jumper (JPMBUS_SEL1)

JPMBUS_SEL1	Setting	
Pin1-2	P3V3_AUX	Default
Pin2-3	P5V_AUX	

3.7 LED

3.7.1 Front Panel LEDs

The front panel Power, Health and UID LEDs shall be powered by Vaux (standby) voltage so system information can be conveyed even when the system is in standby mode. Front panel hard disk and NIC LEDs shall not to be connected to Vaux. It will not indicate activity or link if the system is not powered on. The LED will be cleared and restored to normal state after a power cycle.

Item	Color	Behavior
Power	Yellow	System is On
	Off	System has no AC power
UID	Blue	UID activity detected
	Off	No UID activity detected
System Fault-1	Red	Critical system failure detected (processors, memory, voltage regulators, thermal events,fan failures, NMI, etc)
	On	No critical failures detected
System Fault-2	Red	Critical system failure detected (processors, memory, voltage regulators, thermal events,fan failures, NMI, etc)
	Off	No critical failures detected
Hard Disk	Green (Blinking)	Disk activity detected
	Off	No disk activity detected
NIC-1	Green (Blinking)	NIC-1 activity detected
	Off	NIC is not active
NIC-2	Green (Blinking)	NIC-2 activity detected
	Off	NIC is not active

3.7.2 Rear Chassis LEDs

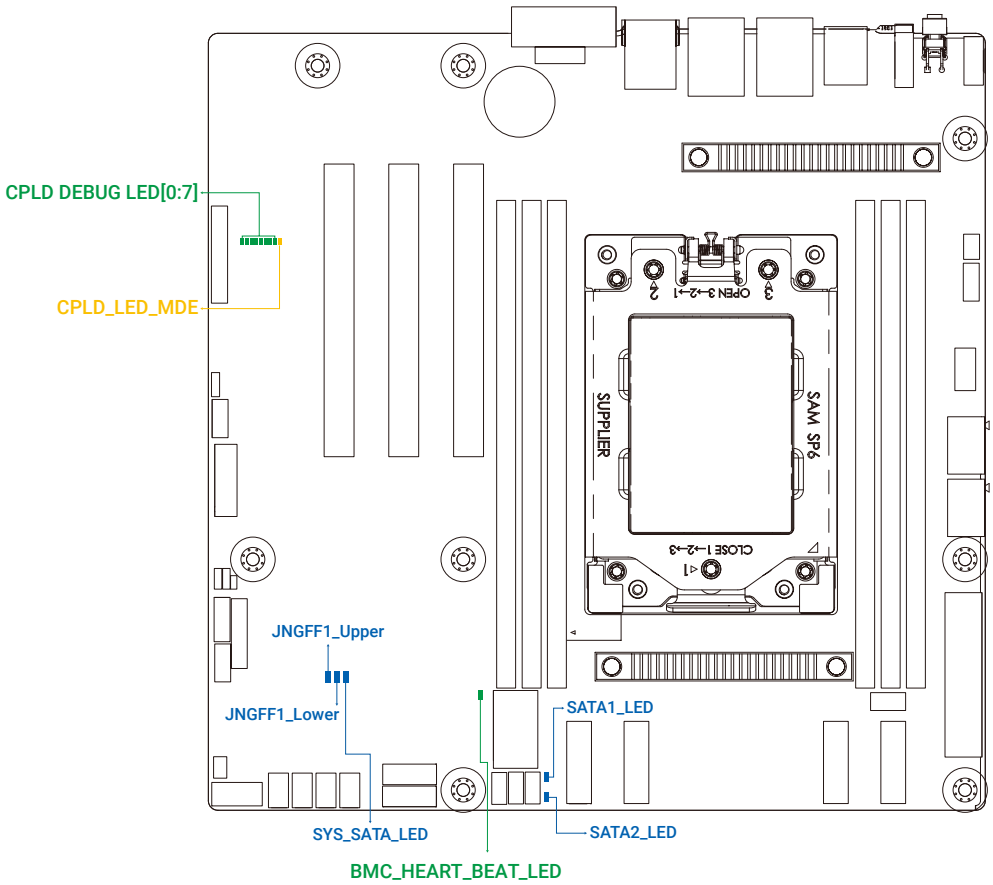
The NIC port/LED should be connected to Vaux (standby) voltage in order to provide the same functionality as stand-up NIC cards for WOL support.

Item		Color	Behavior
NIC 1 – JLAN1	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	10G : Green, 1G: Yellow, No connect: Off
NIC 2 – JLAN2	Right	Green (Blinking)	Activity detected
		Off	LAN cable no connect
	Left	Status LED	10G : Green, 1G: Yellow, No connect: Off
PHY 1 – JRJ45_0	Right	Green (Blinking)	PHY1 activity detected
		Off	PHY1 is not active, LAN cable no connect
	Left	Status LED	1G : Orange, 100M: Green, 10M/No connect: Off

3.7.3 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 aout 3s and then exit) 3. 4Hz : ARM CA7 is reading flash or SRAM 4. 1Hz : ARM CA7 is reading peripherals 5. 0.5Hz : ARM CA7 is reading DRAM 6. 0.2Hz : No ARM CA7 read access cycles 7. 0.1Hz : No ARM CA7 read access cycles over 6~8s. Stay in mode 8 if there is no ARM CA7 reading access. Exit to mode 4-6 if there is any ARM CA7 reading access
	Green	BMC is not active
CPLD DEBUG LED[0:7]	Green/Off	Refer to CPLD LED mapping table
CPLD_LED_MODE	Yellow/Off	Yellow: Port80 MODE, OFF: Sequence MODE
JNGFF1 ACTIVITY LED	Blue (Blinking)	JNGFF1 Upper activity detected
	Off	JNGFF1 Upper is not active
	Blue (Blinking)	JNGFF1 Lower activity detected
	Off	JNGFF1 Lower is not active
SATA LED	Blue (Blinking)	SATA1/2 activity detected
	Off	SATA1/2 is not active

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

4.2 BIOS Setup

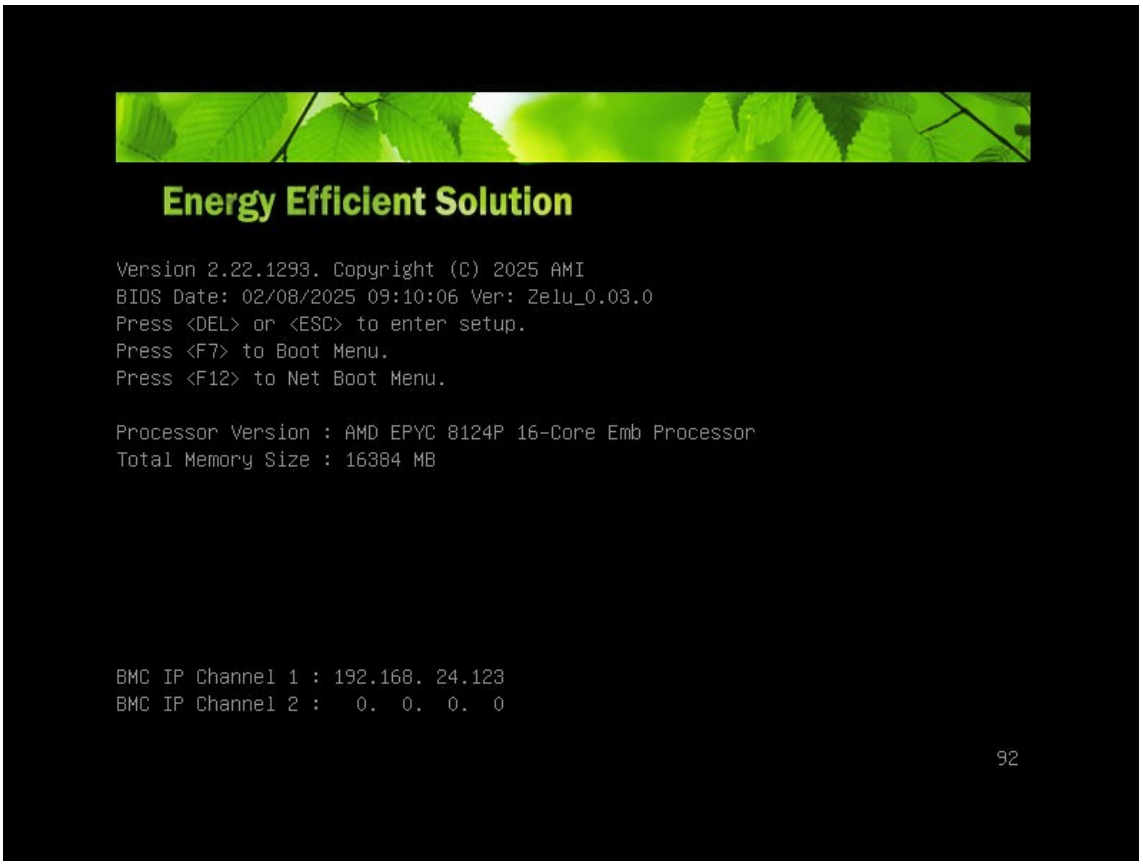
4.2.1 Menu

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

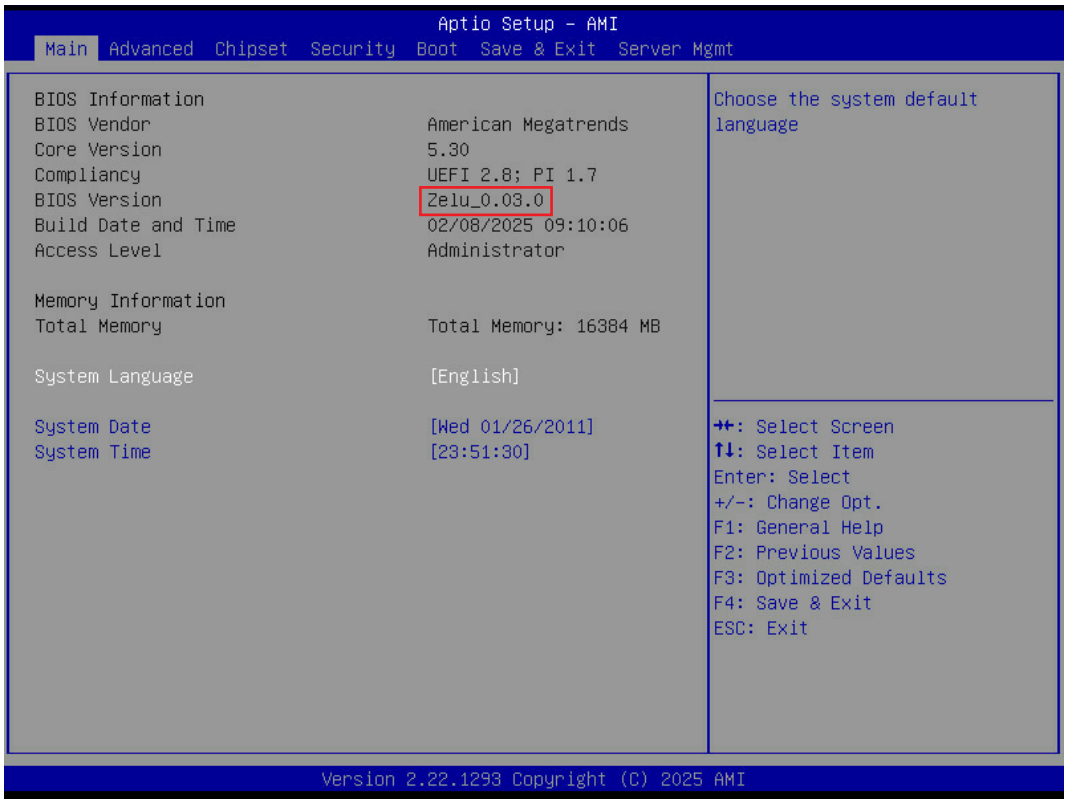
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Chipset	Communicate between the processor and external devices. Select North Bridge or South Bridge to access the parameters for different items.
Security	Sets passwords 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.
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.



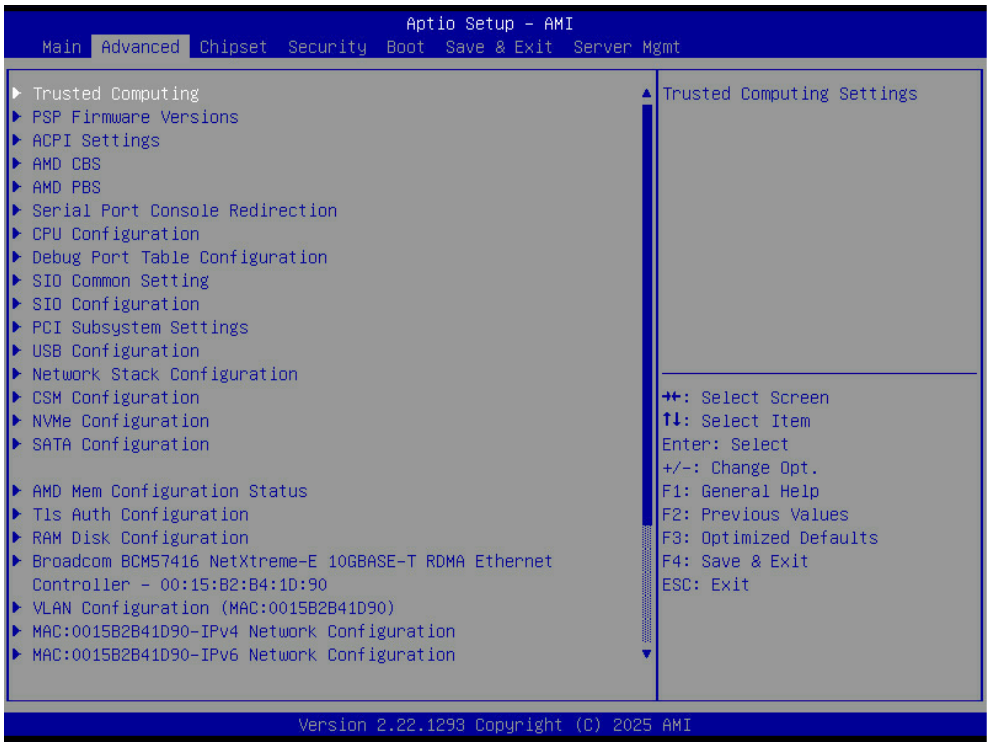
4.3 Main



4.3.1 Main

Main	
System Language	Configures the language used in the system.
System Date	Set the Date. Use Tab to switch between Date elements.
System Time	Set the Time. Use Tab to switch between Time elements.

4.4 Advanced



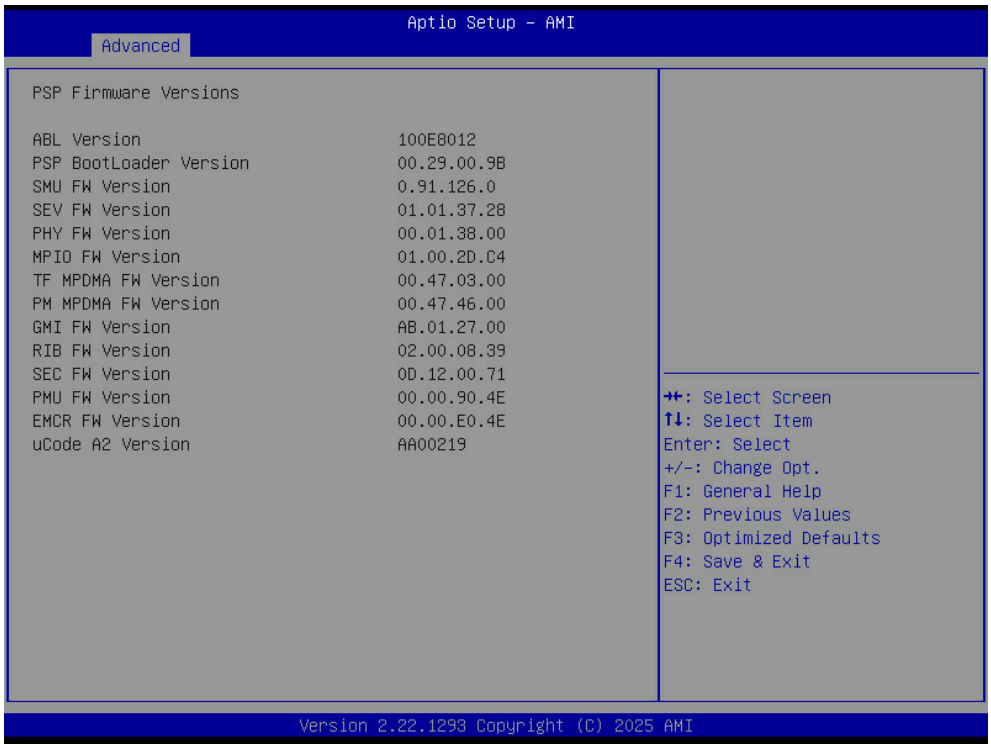
4.4.1 Trusted Computing

Trusted Computing Settings.

Trusted Computing			
Security Device Support	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.		
	▶Enable	Disable	
SHA256 PCR Bank	Enables/disables SHA-256 PCR Bank.		
	▶Enable	Disable	
SHA384 PCR Bank	Enables/disables SHA-384 PCR Bank.		
	Enable	▶Disable	
Pending opertation	Schedules an operation for the security deivce. NOTE: Your computer will reboot during restart in order to change the state of the security device.		
	▶None	TPM Clear	
Platform Hierarchy	Enables/disables platform hierarchy.		
	▶Enable	Disable	
Storage Hierarchy	Enables/disables storage hierarchy.		
	▶Enable	Disable	
Endorsement Hierarchy	Enables/disables endorsement hierarchy.		
	▶Enable	Disable	
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	
PH Randomization	Enables/disables Platform Hierarchy randomization. Do not enable this question in production platforms. This is for development testing. Override change Platform AUth ELINK for production platforms supporting TXT.		
	▶Enable	Disable	
Device Select	• TPM 1.2: TPM 1.2 will restrict support to TPM 1.2 devices. • TPM 2.0: TPM 2.0 will restrict support to TPM 2.0 devices. • Auto: Auto will support both with the defualt set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.		
	▶Auto	TPM 1.2	TPM 2.0

4.4.2 PSP Firmware Versions

PSP Firmware Versions



4.4.3 ACPI Settings

System ACPI Parameters.

ACPI Settings		
Enable ACPI Auto Configuration	Enables/disables BIOS ACPI Auto Configuration.	
	Enable	▶Disable

4.4.4 AMD CBS

AMD CBS Setup Page.

AMD CBS						
CPU Common Options	Perfor-mance	OC Mode	Select overclock operation modes.			
			▶Normal Operation	Customized		
		CCD/Core/ Thread Enable	CCD/Core/Thread Enablement			
			Core Control	Sets the number of cores to be used. Once this option has been used to remove any cores, a Power Cycle is required in order for future selections to take effect.		
				▶Auto	TWO (1+1)	FOUR (2+2) / SIX (3+3)
		SMT Control	Can be used to disable symmetric multithreading. To re-enable SMT, a Power Cycle is needed after selecting the 'Enable' option. Select 'Auto' base on BIOS PCD (PcdAmdSmtMode) default setting. Warning: S3 is NOT SUPPORTED on systems where SMT is disabled.			
			▶Auto	Enable	Disable	
		Enable Requested CPU min frequency	This allows for minimum requested CPU frequency to be used.			
			▶Disable	Enable		
	REP-MOV/ STOS Streaming	Allow REP-MOVS/STOS to use non-caching streaming stores for large sizes.				
			▶Enable	Disable		
	Prefetcher settings	L1 Stream HW Prefetcher	Option to Enable/Disable L1 Stream HW Prefetcher.			
			▶Auto	Enable	Disable	
		L1 Stride Prefetcher	Uses memory access history of individual instructions to fetch additional lines when each access is a constant distance from the previous.			
			▶Auto	Enable	Disable	
		L1 Region Prefetcher	Uses memory access history of individual instructions to fetch additional lines when the data access for a given instruction tends to be followed by other data accesses.			
			▶Auto	Enable	Disable	
		L2 Stream HW Prefetcher	Option to Enable/Disable L2 Stream HW Prefetcher			
			▶Auto	Enable	Disable	
		L2 Up/Down Prefetcher	Uses memory access history to determine whether to fetch the next or previous line for all memory accesses.			
			▶Auto	Enable	Disable	
		L1 Burst Prefetch Mode	Option to Enable/Disable L1 Burst Prefetch Mode.			
			▶Auto	Enable	Disable	
	Core Watchdog	Core Watchdog Timer Enable	Enable/Disable CPU Watchdog Timer.			
			▶Auto	Enable	Disable	
	Redirec-tion For Return Dis	From a workaround for GCC/C000005 issue for XV Core on CZ A0, setting MSRC001_1029 Decode Configuration (DE_CFG) bit 14 [DecfgNoRdrctForReturns] to 1				
		▶Auto	1	0		
	Platform First Error Handling	Enable/disable PFEH, clock individual banks, and mask deferred error interrupts from each bank.				
		▶Auto	Enable	Disable		
	Core Per-formance Boost	Disable CPB.				
		▶Auto	Disable			
	Global C-state Control	Controls I0 based C-state generation and DF C-state.				
		▶Auto	Enable	Disable		
	Power Supply Idle Control	Power Supply Idle Control.				
		▶Auto	Low Current Idle	Typical Current Idle		
	SEV-ES ASID Space Limit	SEV-ES and SNP guests must use ASIDs in the range 1 through(this value-1). SEV guests must use ASIDs in the range fo this value through 1007. To have all ASIDs support SEV-ES or SNP guests, set this value to 1007. The default is 1: all SEV guests and no SEV-ES or SNP guests.				
		1				

CPU Common Options	SEV Control	Can be used to disable SEV. To re-enable SEV, a Power Cycle is needed after selecting the 'Enable' option.			
		▶Enable	Disable		
	Streaming Stores Control	Enable or disable the streaming stores functionality.			
		▶Auto	Enable	Disable	
	Local APIC Mode	Select local APIC operation modes.			
		▶Auto	Compatibility	xAPIC	x2APIC
	ACPI _CST C1 Declaration	Determines whether or not to declare the C1 state to the OS.			
		▶Auto	Enable	Disable	
	ACPI CST C2 Latency	Enter in microseconds (decimal value). Larger C2 latency values will reduce the number of C2 transitions and reduce C2 residency. Fewer transitions can help when performance is sensitive to the latency of C2 entry and exit. Higher residency can improve performance by allowing higher frequency boost and reduce idle core power. With Linux kernel 6.0 or later, the C2 transition cost is significantly reduced. The best value will be dependent on kernel version, use case, and workload.			
		800			
	MCA error thresh enable	Enable MCA error thresholding.			
		▶Auto	True	False	
	MCA FruText	Enable MCA FruText.			
		▶True	False		
	SMU and PSP Debug Mode	When this option is enabled, uncorrected errors detected by the PSP FW or SMU FW that should cause a cold reset, will hang and not reset the system			
		▶Auto	Enable	Disable	
	PPIN Opt-in	Turn on PPIN feature			
		▶Auto	Enable	Disable	
	SNP Memory (RMP Table) Coverage	Enable=ENTIRE system memory is coverd.			
		▶Auto	Enable	Disable	Custom
	SMEE	Control secure memory encryption enable. Enabling both SMEE and SME-MK is not supported. Results in #GP.			
		▶Auto	Enable	Disable	
	Action on BIST Failure	Action to take when a CCD BIST failure is detected.			
		▶Auto	Do noting	Down-CCD	
	Fast Short REP MOVSB (FSRM)	Default is 1, can be set to zero for analysis purposes as long as OS supports it.			
		▶Auto	Enabled	Disabled	
	Enhanced REP MOVSB/ STOSB (ERSM)	Default is 1, can be set to zero for analysis purposes as long as OS supports it.			
		▶Auto	Enabled	Disabled	
	Log Transparent Errors	Log transparent errors in MCA in addition to debug registers.			
		▶Auto	Enabled	Disabled	
	AVX512	Enable/Disable AVX512.			
		▶Auto	Enabled	Disabled	

CPU Common Options	MONITOR and MWAIT disable	The MONITOR, MWAIT, MONITORX, and MWAITX opcodes become invalid, when Enabled.			
		▶Auto	Enabled	Disabled	
	Small Hammer Configuration	• Enabled: LS_CFG::DisSpecWcReq= 0 LS_CFG3::DisSpecWcNonStrmLd = 1 LS_CFG3::EnLockNeedProgressForSpecNC = 1 • Disabled: LS_CFG::DisSpecWcReq= 0 LS_CFG3::DisSpecWcNonStrmLd = 0 LS_CFG3::EnLockNeedProgressForSpecNC = 0			
		▶Auto	Enabled	Disabled	
	Corrector Branch Predictor	Enabling for branch heavy codes may reduce conditional branch mispredicts			
		▶Disable	Enable		
	PAUSE Delay	Number a cycles thread will be idle after a PAUSE instruction			
		▶Auto	Disable	16 cycles	
		32 cycles	64 cycles	128 cycles	
	CPU Speculative Store Modes	Balanced: Store instructions may delay sending out their invalidations to remote cacheline copies when the cacheline is present but not in a writable state in the local cache. More Speculative: Store instructions will send out invalidations to remote cacheline copies as soon as possible. Less Speculative: Store instructions may delay sending out their invalidations to remote cacheline copies when the cacheline is not present in the local cache or not in a writable state in the local cache.			
		Balanced	More Speculative	Less Speculative	▶Auto
	Prefetch/ Request Throttle	Enables XI logic which calculates average latency, updates throttle level, and sends throttle level messages to L2			
		▶Auto	Enabled	Disabled	

DF Common Options	Memory Addressing	NUMA nodes per socket	Specifies the number of desired NUMA nodes per socket Zero will attempt to interleave the two sockets together.		
			▶Auto	NPS1	
		Memory interleaving	Allows for disabling memory interleaving. Note that NUMA nodes per socket will be honored regardless of this setting.		
			▶Auto	Enabled	Disabled
		1TB remap	Attempt to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM configuration, NPS, and interleaving selection, and may not always be possible.		
			▶Auto	Do not remap	Attempt to remap
		DRAM map inversion	Inverting the map will cause the highest memory channels to get assigned the lowest addresses in the system.		
			▶Auto	Enabled	Disabled

DF Common Options	Memory Address-ing	Location of private memory regions		Controls whether or not the private memory regions (PSP, SMU and CC6) are at the top of DRAM, at the top of 1st DRAM pair or distributed. Note that distributed requires memory on all dies. Note that it will always be at the top of DRAM if some dies do not have memory regardless of this option's setting. Also, Consolidation to 1st DRAM pair is only valid in the non-interleaved case.			
				▶Auto	Distributed	Consolidated	
		CXL Memory interleaving		Allows for enabling/disabling CXL memory devices interleaving.			
				▶Auto	Enabled	Disabled	
		CXL Sublink interleaving		Enable/disable CXL sublink interleaving.			
				▶Auto	Enable	Disable	
	ACPI	ACPI SRAT L3 Cache As NUMA Domain		Enable: Each CCX in the system will be declared as a separate NUMA domain. Disable: Memory Addressing/ NUMA nodes per socket will be declared.			
				▶Auto	Enabled	Disabled	
		ACPI SLIT Distance Control		Determines how the SLIT distances are declared.			
				▶Auto	Manual		
		ACPI SLIT remote relative distance		Set the remote socket distance for 2P systems as near (2.8) or far (3.2)			
				▶Auto	Near	Far	
	Link	GMI encryption control		Control GMI link encryption.			
				▶Auto	Enabled	Disabled	
		xGMI encryption control		Control xGMI link encryption.			
				▶Auto	Enable	Disable	
		xGMI Link Configuration		Configures the number of xGMI2 links used on a multi-socket system.			
				▶Auto	3 xGMI Links	4 xGMI Links	2 xGMI Links+2 PCI Links
		4-link xGMI max speed		Specifies the max frequency used for XGMI PState in a 4-link topology.			
				▶Auto	20Gbps	25Gbps	32Gbps
		3-link xGMI max speed		Specifies the max frequency used for XGMI PState in a 3-link topology.			
				▶Auto	20Gbps	25Gbps	32Gbps
		xGMI 18GACOFC		xGMI 18GACOFC control.			
				▶Auto	Enable	Disable	
		xGMI CRC Scale		Configure leaky bucket scale for xGMI and WAFL CRC errors. Every scale milliseconds an error will leak from the CRC counter.			
				5			
		xGMI CRC Threshold		Configure leaky bucket threshold for xGMI and WAFL CRC errors. If link CRC counter exceeds this threshold, an error will be logged.			
				25			
		xGMI Press Control		Enable/Disable XGMI Present Control options.			
				Auto	▶Enable	Disable	
		xGMI Global Press List	Preset P11	Preset P11 Cmn1	Enable/Disable Preset P11 Cmn1 option on xGMI Global Preset List.		
					0		
				Preset P11 Cn	Enable/Disable Preset P11 Cn option on xGMI Global Preset List.		
					30		
				Preset P11 Cnp1	Enable/Disable Preset P11 Cnp1 option on xGMI Global Preset List.		
					0		

DF Common Options	Link	xGMI Global Press List	Preset P12	Preset P12 Cmn1	Enable/Disable Preset P12 Cmn1 option on xGMI Global Preset List. 0
				Preset P12 Cn	Enable/Disable Preset P12 Cn option on xGMI Global Preset List. 30
				Preset P12 Cnp1	Enable/Disable Preset P12 Cnp1 option on xGMI Global Preset List. 0
			Preset P13	Preset P13 Cmn1	Enable/Disable Preset P13 Cmn1 option on xGMI Global Preset List. 0
				Preset P13 Cn	Enable/Disable Preset P13 Cn option on xGMI Global Preset List. 30
				Preset P13 Cnp1	Enable/Disable Preset P13 Cnp1 option on xGMI Global Preset List. 0
			Preset P14	Preset P14 Cmn1	Enable/Disable Preset P14 Cmn1 option on xGMI Global Preset List. 0
				Preset P14 Cn	Enable/Disable Preset P14 Cn option on xGMI Global Preset List. 30
				Preset P14 Cnp1	Enable/Disable Preset P14 Cnp1 option on xGMI Global Preset List. 0
			Preset P15	Preset P15 Cmn1	Enable/Disable Preset P15 Cmn1 option on xGMI Global Preset List. 0
				Preset P15 Cn	Enable/Disable Preset P15 Cn option on xGMI Global Preset List. 30
				Preset P15 Cnp1	Enable/Disable Preset P15 Cnp1 option on xGMI Global Preset List. 0
		xGMI Initial Preset	Initial Preset Socket 0 Link0-3	Initial Preset Socket 0 Link 0 Pstate 0-3	Enable/Disable Initial Preset Socket 0 Link 0 Pstate 0-3 4
			Initial Preset Socket 1 Link0-3	Initial Preset Socket 1 Link 0 Pstate 0-3	Enable/Disable Initial Preset Socket 1 Link 0 Pstate 0-3 4
		xGMI TXEQ Search Mask	TXEQ Search Mask Socket 0 Link 0-3	TXEQ Search Mask Socket 0 Link 0 Pstate 0-3	Enable/Disable TXEQ Search Mask Socket 0 Link 0 Pstate 0-3 7A
			TXEQ Search Mask Socket 1 Link 0-3	TXEQ Search Mask Socket 1 Link 0 Pstate 0-3	Enable/Disable TXEQ Search Mask Socket 1 Link 0 Pstate 0-3 7A

DF Common Options	Link	xGMI AC/ DC Coupled Link	xGMI AC/DC Coupled Link Control	Control XGMI AC/DC Coupled Link. Valid value: 0 : AC coupled 1 : DC coupled	
				▶Auto	Manual
		xGMI Channel Type	xGMI Channel Type Control	Control xGMI Channel Type. Valid channel type : 0 : Disabled 1 : Long Reach	
				▶Auto	Manual
		xGMI Training Err Mask	Enable/Disable XGMI training err mask		
			▶Auto	Disable	Enable

DF Common Options	SDCI	SDCI	Enable/Disable Smart Data Cache Injection feature.				
			▶Auto	Enabled	Disabled		
	Probe Filter	Organization	Specifies whether multiple memory/CXL channels will share probe filter storage. For memory sizes of 16TB or larger, this feature is ignored as it is auto-selected to 'share'.				
			Auto	▶Dedicated	Shared		
		Periodic Directory Rinse (PDR) Tuning	Controls PDR settings that may impact performance by workload and/or processor. Memory-Sensitive: May accelerate high b/w scenarios. Cache-Bound: May accelerate cache-bound scenarios. Neutral: Fallback option for unknown or mixed scenarios.				
			▶Auto	Memory-Sensitive	Cache-Bound	Neutral	Adaptive
	DF Watchdog Timer Interval	Configure the Data Fabric watchdog timer interval.					
		▶Auto	41 ms	166 ms	334 ms		
		669 ms	1.34 seconds	2.68 seconds	5.36 seconds		
	Disable DF to external IP SyncFloodPropagation	Disable SyncFlood to UMC & downstream slaves.					
		▶Auto	Sync flood disabled	Sync flood enabled			
	Sync Flood Propagation to DF Components	Control DF: PIEConfig[DisSyncFloodProp]					
		▶Auto	Sync flood disabled	Sync flood enabled			
	Freeze DF module queues on error	Controls DF: PIEConfig[DisImmsyncFlood0nFatalError] Disabling this option sets DF: PIEConfig[DisImmsyncFlood0nFatalError]					
		▶Auto	Enabled	Disabled			
	CC6 memory region encryption	Control whether or not the CC6 save/restore memory is encrypted.					
		▶Auto	Enabled	Disabled			
	CCD B/W Balance Throttle Level	Enable throttling of memory traffic per CCD. Increased throttling can reduce imbalance across CCDs(expected to be rare).					
		▶Auto	Level 0	Level 1	Level 2	Level 3	Level 4
	Number of PCI Segments	No help string					
		▶Auto	1 Segment	2 Segment	4 Segment		
	P2P Ordered Writes	When set to Disabled, ordering of P2P writes targeting multiple end points is no longer guaranteed by the host.					
		▶Enabled	Disabled				

UMC Common Options	DDR Addressing Options	Chipselect Interleaving	Interleave DRAM accesses across ranks within a memory channel if the configuration supports it. 'Enable' will override certain optimization policies, but cannot force interleaving on configurations that do not support it.			
			▶Auto	Enabled	Disabled	
		Address Hash Bank	Enable/disable bank address hashing.			
			▶Auto	Enabled	Disabled	
		Address Hash CS	Enable/disable CS address hashing.			
			▶Auto	Enabled	Disabled	
		Address Hash RM	Enable or disable RM address hashing for 3DS DIMMs			
			▶Auto	Enabled	Disabled	
		Address Hash Subchannel	Enable/disable sub-channel address hashing.			
			▶Auto	Enabled	Disabled	
		BankSwapMode	BankSwapMode value: 0=Disabled, 1=SwapCPU			
			▶Auto	Disabled	Swap CPU	
	DDR Controller Configuration	DDR Power Options	Power Down Enable	Enable/disable DDR power down mode.		
				▶Auto	Enabled	Disabled
			Sub Urgent Refresh Lower Bound	Specifies the stored refresh limit required to enter sub-urgent refresh mode. Constraint: SubUrgRefLowerBound <= UrgRefLimit Valid value: 6~1		
				1		
			Urgent Refresh Limit	Specifies the stored refresh limit required to enter sub-urgent refresh mode. Constraint: SubUrgRefLowerBound <= UrgRefLimit Valid value: 6~1		
				4		

UMC Common Options	DDR Controller Configuration	DDR Power Options	DRAM Refresh Rate	DRAM refresh rate: 1.95us or 3.9us (default). ►3.9 usec | 1.95 usec
			Self-Refresh Exit Staggering	Tcksrx += (Trfc/n * (UMC_Number % 3)) Selectable by CBS Option: Disable Staggering n = 1 <= Stagger Channels by ~270 ns n = 2 n = 3 n = 4 . . . n = 9 <= Stagger Channels By ~30 ns (Default) Disabled | n= 1 | n= 2 | n= 3 | n= 4 n= 5 | n= 6 | n= 7 | n= 8 | ►n= 9
		Memory Channel Disable	Memory Channel Disable Float Power Good	Float Power Good when channel is disabled by BIOS setup options. Enabled | ►Disabled
			Socket 0 Channel 0-11	SPD reading will be skipped when channel is disabled. ►Enabled | Disabled
		Refresh Management (RFM)	Refresh Management	Auto: Disable Disable: Disable RFM for all Ranks. Enable: Enable RFM for Ranks which support RFM. Force Enable: Enable RFM for all Ranks regardless of support. Selecting 'Force Enable' will cause REFpb/REFsb to be disabled if all ranks do not support RFM ►Auto | Disable | Enable | Force Enable
			RAA Initial Management Threshold	Override Rolling Accumulated ACT Initial Management Threshold Auto: BIOS will choose the lowest supported value from SPD. Choices from list are for Normal Refresh Mode. In Fine Granularity Mode, the value will be divided by 2. ►Auto | 32 | 40 | 48 56 | 64 | 72 | 80
			RAA Maximum Management Threshold	Override Rolling Accumulated ACT Maximum Management Threshold Auto: BIOS will choose the lowest supported value from SPD. Choices from list are for Normal Refresh Mode. In Fine Granularity Mode, the value will be divided by 2. ►Auto | 3X | 4X | 5X | 6X
			RAA Refresh Decrement Multiplier	Override RAA Refresh Decrement Multiplier Auto: BIOS will choose the lowest supported value from SPD. ►Auto | 0.5 | 1

UMC Common Options	DDR MBIST Options	MBIST Enable	Enable/disable Memory MBIST.	
			▶Auto	Enabled / Disabled
		Data Eye	Pattern Select	MBIST Data Eye Pattern Type. 0-PRBS (default) 1-SSO 2-Both
				▶PRBS / SSO / Both
			Pattern Length	This token determine the pattern length, available options: 3...C(input hex number, not decimal)
				3
			Aggressor Channel	One Sub-Channel enable the non-target subchannel on the target channel to be an aggressor. Half Channels enables all non-target channels on one half of the processor to be aggressors. All Channels enables all non-target channels to be aggressors.
				One Sub-Channel / Half Channels / ▶All Channels
			Aggressor Static Lane Control	This option, if enabled, will control the Aggressor Static Lane Controls.
				▶Disabled / Enabled
			Target Static Lane Control	Enable Mbist Target Static Lane Control.
				▶Disabled / Enabled
			Worst Case Margin Granularity	Mbist Worst Case Margin Granularity 0=Per Chip Select 1=Per Nibble
				▶Per Chip Select / Per Nibble
			Read Voltage Sweep Step Size	This option determines the step size for Read Data Eye voltage sweep, Supported options are 1, 2 and 4.
				▶1 / 2 / 4
			Read Timing Sweep Step Size	This options supports step size for Read Data Eye. Supported options are 1, 2 and 4.
				▶1 / 2 / 4
			Write Voltage Sweep Step Size	This option determines the step size for write Data Eye voltage sweep, Supported options are 1, 2 and 4.
				▶1 / 2 / 4
			Write Timing Sweep Step Size	This options supports step size for write Data Eye. Supported options are 1, 2 and 4.
				▶1 / 2 / 4
			Silent Execution	Execute MBIST Data Eye silently without ABL log output. Disabled- MBIST Enable will not be overridden Enable- Execute MBIST Data Eye silently without ABL log output.
				▶Disabled / Enabled
		DDR Healing BIST	This item enables a full memory test. Please note that this is a memory content test and is separate and distinct from the MBIST test of Interface and Data Eye. PMU Mem BIST: this uses PMU firmware to test memory on all channels simultaneously. Failing memory will be repaired using soft or hard PPR depending on the PPR configuration. Self-Healing Mem BIST: this runs the JEDEC DRAM self healing, if the device and DIMM support the feature. The DRAM will do a hard repair for failing memory. PMU and Self-Healing Mem BIST: this option runs the PMU Mem BIST then the Self-Healing Mem BIST tests sequentially.	
			▶Disabled	PMU Mem BIST / Self-Healing Mem BIST / PMU and Self-Healing Mem BIST

UMC Common Options	DDR RAS	DDR Poisoning		Enable poison data creation on uncorrectable DDR DRAM ECC errors and poison propagation to CPU cores and caches. Requires ECC memory. When FALSE, a fatal error event will occur on DDR ECC errors sets UMC_CH::EccCtrl[UcFatalEn] when MC_CH::EccCtrl[WrEccEn] is set.			
				▶Auto	Enabled	Disabled	
		DRAM Boot Time Post Package Repair		Enable/disable DRAM Boot Time Post Package Repair.			
				▶Disable	Enable		
		DRAM Runtime Post Package Repair		Enable/disable DRAM Run Time Post Package Repair.			
				▶Disable	Enable		
		RCD Parity		Enable RCD command and address parity.			
				Auto	▶Enabled	Disabled	
		Max RCD Parity Error Replay		Program to UMC::RecCtrl[MaxParRply] valid value:1-3F hex, default 8			
				8			
		Disable Memory Error Injection		0=Enable / 1=Disable Specifies UMC error injection configuration writes are disabled. True: UMC::CH::MiscCfg[DisErrInj]=1			
				▶Auto	True	False	
		ECC Configuration	DRAM ECC Symbol Size	DRAM ECC Symbol Size(x4/x16)-UMC_CH::EccCtrl[EccSymbolSize16, EccSymbolSize]			
				▶Auto	x4	x16	
			DRAM ECC Enable	Use this option to enable/disable DRAM ECC. Auto will set ECC to enable.			
				▶Auto	Enabled	Disabled	
			DRAM UECC Retry	DRAM UECC Retry. Program to UMC::RecCtrl.RecEn[2]			
				Auto	Enabled	▶Disabled	
			Memory Clear	Clear/Zero out Dram range [DramScrubBaseAddr: DramScrubLimitAddr].When this option is disabled, Memory is not cleared after training. ECC Dimms have memory clear enabled always. Non-ECC Dimms can choose to disable/enable using this option. Default = Memclear enabled			
				▶Auto	Enabled	Disabled	
			Address X0R after ECC	In order to provide data integrity when data is returned from the wrong address, UMC will hash the data after ECC with the normalized address.			
				▶Auto	Enabled	Disabled	
		DRAM Scrubbers	DRAM ECS Mode	0=AutoECS Mode 1=ManualECS mode			
				▶Auto	AutomaticECS	ManualECS	DisableECS
			DRAM Redirect Scrubber Enable	Enable/Disable Dram Redirect Scrubber.			
				▶Auto	Enabled	Disabled	

UMC Common Options	DDR RAS	DRAM Scrubbers	DRAM Scrub Redirection Limit	Dram ECC Scrub Redirection Limit:0=8 scrubs, 1=4 scrubs, 2=2 scrubs, 3=1 scrub ▶Auto / 8 scrubs / 4 scrubs / 2 scrubs / 1 scrub
			DRAM Scrub Time	Provide a value that is the number of hours to scrub memory. Disable / 1 hour / 4 hour / 6 hour / 8 hour 12 hour / 16 hour / ▶24 hour / 48 hour
			DRAM Error Threshold Count	List of Values: 0 = ETC_4, 1 = ETC_16, 2 = ETC_64, 3 = ETC_256 (default - Auto), 4 = ETC_1024, 5 = ETC_4096 ▶Auto / ETC_4 / ETC_16 / ETC_64 ETC_256 / ETC_1024 / ETC_4096
			DRAM ECS Count Mode	0: RowCount Mode 1: CodeWord Mode 0xFF: Auto - ABL decides default as CodeWord Mode Row Count Mode / Code Word Count Mode / ▶Auto
			DRAM AutoEcs during Self Refresh	0: AutoEcs Disabled 1: AutoEcs Enabled 0xFF: Auto - ABL choose AutoEcs Disabled AutoEcs Disabled / AutoEcs Enabled / ▶Auto
			DRAM ECS WriteBack Suppression	To enable/Disable ECS Error Correction Writeback suppression 0: ECS Writeback Suppression Disabled 1: ECS Writeback Suppression Enabled 0xFF: Auto - ABL chooses Writeback Suppression to be Enabled by default ▶Auto / Enable / Disable
			DRAM X4 WriteBack Suppression	To enable/Disable X4 device Error Correction Writeback suppression 0: X4 Writeback Suppression Disabled 1: X4 Writeback Suppression Enabled 0xFF: Auto ▶Auto / Enable / Disable
		DRAM Corrected Error Counter Enable		Configure DRAM Corrected Error Counter function. Only meaningful when PcdAmdCcxCfgPFEHEnable is TRUE. Disable / NoLeakMode / ▶LeakMode
		DRAM Corrected Error Counter Interrupt Enable		Enable SMI when DRAM Corrected Error Counter count exceeds the threshold value. ▶True / False
		DRAM Corrected Error Counter Leak Rate		Program Rate value for DRAM Corrected Error Counter function. Only meaningful when PcdAmdDdrEccErrorCounterEnable is set to LeakMode (Value :0x00-0x1F). 7
		DRAM Corrected Error Counter Start Count		Program starting count value for DRAM Corrected Error Counter function. Only meaningful when PcdAmdDdrEccErrorCounterEnable is not Disable (0x00 - 0xFFFF). FFF5

UMC Common Options	DDR Bus Configuration	Dram ODT impedance RTT_NOM_WR		Select the DRAMs On-die Termination impedance for RTT_NOM_WR.				
				▶Auto	RTT_OFF	RZQ(240)	RZQ/2(120)	RZQ/3(80)
				RZQ/4(60)	RZQ/5(48)	RZQ/6(40)	RZQ/7(34)	
		Dram ODT impedance RTT_NOM_RD		Select the DRAMs On-die Termination impedance for RTT_NOM_RD.				
				▶Auto	RTT_OFF	RZQ(240)	RZQ/2 (120)	RZQ/ 3 (80)
				RZQ/ 4 (60)	RZQ/ 5 (48)	RZQ/ 6 (40)	RZQ/ 7 (34)	
		Dram ODT impedance RTT_WR		Select the DRAMs On-die Termination impedance for RTT_WR.				
				▶Auto	RTT_OFF	RZQ(240)	RZQ/2 (120)	RZQ/ 3 (80)
				RZQ/ 4 (60)	RZQ/ 5 (68)	RZQ/ 6 (40)	RZQ/ 7 (34)	
		Dram ODT impedance RTT_PARK		Select the DRAMs On-die Termination impedance for RTT_PARK.				
				▶Auto	RTT_OFF	RZQ(240)	RZQ/2 (120)	RZQ/ 3 (80)
				RZQ/ 4 (60)	RZQ/ 5 (48)	RZQ/ 6 (40)	RZQ/ 7 (34)	
		Dram ODT impedance DQS_RTT_PARK		Select the DRAMs On-die Termination impedance for DQS_RTT_PARK.				
				▶Auto	RTT_OFF	RZQ(240)	RZQ/2 (120)	RZQ/ 3 (80)
				RZQ/ 4 (60)	RZQ/ 5 (48)	RZQ/ 6 (40)	RZQ/ 7 (34)	
		Processor ODT impedance		Select the ODT impedance for all DBYTE I0s.				
				▶Auto	High Impedance	480 ohm	240 ohm	160 ohm
				120 ohm	96 ohm	80 ohm	68.6 ohm	60 ohm
				53.3 ohm	48 ohm	43.6 ohm	40 ohm	36.9 ohm
				34.3 ohm	32 ohm	30 ohm	28.2 ohm	26.7 ohm
				25.3 ohm				
		Dram DQ drive strengths		Select the Dram Pull-up and Pull-Down Output Driver Impedance for all DQ and DMI I0s.				
				▶Auto	48 ohm	40 ohm	34 ohm	
	DDR Timing Configuration	Decline						
		Accept	Active Memory Timing Settings	Active Memory Timing Settings.				
				Auto	▶Enabled			
			Memory Target Speed	Specifies the memory target speed in MT/s.				
				▶Auto	DDR3600	DDR4000	DDR4400	
				DDR4800	DDR5200	DDR5600		
			SPD Timing	Tcl Ctrl/Trcd Ctrl/Trp Ctrl/Tras Ctrl/Trc Ctrl/Twr Ctrl/Trfc1 Ctrl/Trfc2 Ctrl/TrfcSb Ctrl			Auto: Follow default setting Manual: Manually specify	
							▶Auto	Manual
			Non-SPD Timing	Tcwl Ctrl/Trtp Ctrl/TrrdL Ctrl/ Trrds Ctrl/Tfaw Ctrl/ Twtrl Ctrl/TwtrS Ctrl/TrdrdScl Ctrl/TrdrdSc Ctrl/TrdrdSd Ctrl/ TrdrdDdCtrl/TwrwrScL Ctrl/ TwrwrSc Ctrl/TwrwrSd Ctrl/ TwrwrDd Ctrl/Twrrd Ctrl/ Trdwr Ctrl			Auto: Follow default setting Manual: Manually specify	
							▶Auto	Manual

UMC Common Options	DDR Training Options	DRAM PDA Enumerate ID Programming Mode	Specify PDA enumeration mode Auto: default 0: Continuous DQS toggling PDA enumeratioin mode(default) 1:Legacy PDa enumeratioinii mode ▶Auto | Toggling PDA enumeration mode | Legacy PDA enumeration mode
	DDR security	TSME	Transparent SME Auto | Enabled | ▶Disabled
		AES	AES mode: AES-128 or AES-256 (default) AES-128 | ▶AES-256
		Data Scramble	Data scrambling: DataScrambleEn ▶Enabled | Disabled
		SME-MK	SME-MK encryption mode. Enabling both SMEE and SME-MK is not supported. Results in #GP. Enabled | ▶Disabled
	DDR PMIC Configuration	PMIC Error Reporting	Enable support for PMIC Error Reporting. ▶Auto | True | False
		PMIC Operation Mode	1 - Programmable Mode Operation (default); 0 - Secure Mode Operation Programmable mode allows certain registers to be programmed after VR enable else they will be in secure mode Secure Mode | ▶Programmable Mode
		PMIC Fault Recovery	0 - Always; 1 - Never (default); 2 - Once Always - PMIC will ignore previous boot errors. No channel disabled Never - PMIC disables the channel with errors from previous boot. Once - PMIC will disable the channel if more than one error is detected on previous boot, else it is ignored. ▶Always | Never | Once
		PMIC SWC VDDIO	Range is from 1000mV to 1200mV; default of 1100mV. 1100
		PMIC SWA/SWB VDD Core	Range is from 1000mV to 1200mV; default of 1100mV. 1100
		PMIC Stagger Delay	Amount of time to wait between powering on DIMMs in milliseconds. 5
		Max PMIC Power On	Maximum number of DIMMs that can power on at the same time. FF
	DDR Miscellaneous	DRAM Survives Warm Reset	1 - Enabled (default); 0 - Disabled If enabled - Upon warm reset DRAM content is preserved, Training values are saved & retrieved. Enabled | ▶Disabled
		ODTS CMD Throttle Threshold	Dram MR4 Temperature status value to start ODTS Command Thermal Throttlling. ▶Auto | >85'C | > 90'C | > 95'C
		Vendor specific RCD workaround	Workaround a specific I2C/I3C switching issue with a specific DIMM SPD hub vendor Enabled | ▶Disabled
	DDR PHY (CMN)	Periodic Training	Specifies Periodic Training config ▶Auto | Enabled | Disabled
NBIO Common Options	IOMMU		Enable/Disable IOMMU. ▶Auto | Enabled | Disabled
	DMAr Support		Enable DMAr system protection during POST. ▶Auto | Enabled | Disabled
	DMA Protection		Enable DMA remap support in IVRS IVinfo Field. ▶Auto | Enabled | Disabled

	DRTM Virtual Device Support	EnableDDRTM ACPI virtual device.				
		▶Auto	Enabled	Disabled		
	DRTM Memory Reservation	Reserve 128MB memory below Bottom IO for DRTM. It is required to be enabled for Secured-Core Server function.				
		▶Auto	Enabled	Disabled		
	ACS Enable	AER must be enabled for ACS enable to work.				
		▶Auto	Enabled	Disabled		
	PCIe ARI Support	Enables Alternative Routing-ID Interrpretation.				
		▶Auto	Enabled	Disabled		
	PCIe ARI Enumeration	ARI Forwarding Enable for each downstream port.				
		▶Auto	Enabled	Disabled		
	PCIe Ten Bit Tag Support	Enables PCIe ten bit tags for supported devices.				
		▶Auto	Enabled	Disabled		
	Low Latency NIC Fast Mode Support	Enable/Disable Low Latency NIC Fast Mode Support				
		▶Auto	Enabled	Disabled		
	SMU Common Options	TDP Control	Auto= Use the fused TDP Manual= User can set customized TDP			
			▶Auto	Manual		
		PPT Control	Auto= Use the fused PPT Manual= User can set customized PPT			
			▶Auto	Manual		
		Determinism Control	Auto = Use default performance determinism settings Manual = User can set custom performance determinism settings			
			▶Auto	Manual		
		xGMI Link Width Control	Auto = Use default xGMI link width controller settings\nManual = User can set custom xGMI link width controller settings			
			▶Auto	Manual		
		APBDIS	0= not APBDIS (mission mode) 1= APBDIS			
			▶Auto	0	1	
		DfPstate Range Support	DF Pstate selection is overridden by the APB_DIS BIOS option if it is selected. If enable this feature, the range value setting should follow the rule that MaxDfPstate <= MinDfPstate. Otherwise it will not work.			
			▶Auto	Enable	Disable	
		Power Profile Selection	DF Pstate selection in the profile policy is overridden by the pstate range BIOS option or the APB_DIS BIOS option if either one is selected. [0 = High Performance Mode (DEFAULT); 1 = Efficiency Mode; 2 = Maximum IO Performance Mode]			
			▶High Performance Mode	Efficiency Mode	Maximum IO Performance Mode	Balanced Memory Performance Mode
		BoostFmaxEn	Auto= Use the default Fmax Manual= User can set the boost Fmax			
			▶Auto	Manual		
		DF PState Frequency Optimizer	Disabled - means disable the DFPstate CCLK effective frequency optimizer Enabled - means enable the DFPstate CCLK effective frequency optimizer			
			▶Auto	Enable	Disable	
		DF Cstates	Enable= Enable the feature : Disable= Disable the feature			
			▶Auto	Enable	Disable	
		CPPC	Enable= Enable the feature : Disable= Disable the feature			
			▶Auto	Enabled	Disabled	
		HSMP Support	Select HSMP support enable or disable.			
			Auto	Enabled	▶Disabled	

NBIO Common Options	SMU Common Options	SVI3 SVC Speed Control	No help string			
			▶Auto	Manual		
		Diagnostic Mode	Select Diag mode enable or disable.			
			▶Auto	Enabled	Disabled	
		PCIE Speed PMM Control	Reduce link speed when devices are idle.			
			▶Auto	Dynamic link speed determined by Power Management functionality	Static Target Link Speed (GEN4)	Static Target Link Speed (GEN5)
	NBIO RAS Common Options	NBIO RAS Control	(0) Disabled, (1) MCA			
			▶Auto	MCA	Disabled	
		Egress Poison Severity High	Each bit set to 1 enables HIGH severity on the associated IOHC egress port. A bit of 0 indicates LOW severity.			
			30011			
		Egress Poison Severity Low	Each bit set to 1 enables HIGH severity on the associated IOHC egress port. A bit of 0 indicates LOW severity.			
			4			
		NBIO SyncFlood Generation	This value may be used to mask SyncFlood caused by NBIO RAS options. When set to TRUE SyncFlood from NBIO is masked. When set to FALSE NBIO is capable of generating SyncFlood.			
			▶Auto	Enabled	Disabled	
		NBIO SyncFlood Reporting	This value may be used to enable SyncFlood reporting to APML. When set to TRUE SyncFlood will be reported to APML. When set to FALSE that reporting well be disabled.			
			▶Auto	Enabled	Disabled	
		Egress Poison Mask High	These set the enable mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.			
			FFFCFFFF			
		Egress Poison Mask Low	These set the enable mask for masking of errors logged in EGRESS_POISON_STATUS. For each bit set to 1, errors are masked. For each bit set to 0, errors trigger response actions.			
			FFFFFFFB			
		Uncorrected Converted to Poison Enable Mask High	These set the enable mask for masking of uncorrectable parity errors on internal arrays. For each bit set to 1, a system fatal error event is triggered for UCP errors on arrays associated with that egress port. For each bit set to 0, errors are masked.			
			30000			
		Uncorrected Converted to Poison Enable Mask Low	These set the enable mask for masking of uncorrectable parity errors on internal arrays. For each bit set to 1, a system fatal error event is triggered for UCP errors on arrays associated with that egress port. For each bit set to 0, errors are masked.			
			4			
		System Hub Watchdog Timer	This value specifies the timer interval of the SYSHUB Watchdog timer in miliseconds. Maximium value is 5200ms			
			2600			
		PCIe Aer Reporting Mechanism	This value selects the method of reporting AER errors from PCI Express. A value of 1 allows OS First handling of the errors through generation of a system control interrupt (SCI). A value of 2 provides for Firmware First handling of errors through generation of a system management interrupt (SMI).			
			▶Auto	Firmware First	Firmware First but allow OS First	Os First

NBIO Common Options	NBIO RAS Common Options	Edpc Control	(0) Disabled; (1) Enabled; (3) Auto				
			▶Auto	Enabled	Disabled		
		ACS RAS Request Value	No help string				
			▶Auto	Direct Request Access Enabled	Request Blocking Enabled	Request Redirect Enabled	
		NBIO Poison Consumption	NBIO Poison Consumption				
			▶Auto	Enabled	Disabled		
		Sync Flood on PCIe Fatal Error	When “Sync Flood on PCIe Fatal Error” is True, PcdAmdPcieSyncFloodOnFatal should be set to True. When “Sync Flood on PCIe Fatal Error” is False, PcdAmdPcieSyncFloodOnFatal should be set to False. When “Sync Flood on PCIe Fatal Error” is Auto, PcdAmdPcieSyncFloodOnFatal should retain its AGESA default.				
			▶Auto	True	False		
	Enable AER Cap	Enables Advanced Error Reporting Capability.					
		▶Auto	Enabled	Disabled			
	Early Link Speed	Set Early Link Speed.					
		▶Auto	Gen1	Gen2			
	Hot Plug Handling mode	Control the Hot Plug Handling mode Note: "Firmware First but allow OS First" is a development mode and not to be used until operating systems with this support are available. SFI mode REQUIRES an operating system that supports DPC. (Most recent Linux operating systems support/enable this)					
		▶Auto	OS First	Firmware First/EDR if OS supports	Firmware First but allow OS First	System Firmware Intermediary	
	Hot Plug Allow FF in Synchronous	Allows firmware first hot plug handling mode to operate in mode A and mode B synchronous mappings.					
		▶Disabled	Enabled				
	Presence Detect Select mode	Control the Presence Detect Select mode.					
		▶Auto	OR	AND	In-Band Only	Out-Of-Band Only	
	Data Link Feature Cap	Data Link Feature Capability.					
		▶Auto	Enabled	Disabled			
	CV test	Set this to Enabled to support running PCIECV tool. Auto - preserve h/w defaults					
		▶Auto	Enabled	Disabled			
	SEV-SNP Support	Enables support for Secure Encrypted Virtualization and Secure Nested Paging.					
		▶Auto	Enable	Disable			
	Allow Compliance	When enabled, allows the PCIe RP to enter Polling. Compliance state.					
		▶Auto	Enable	Disable			
	SRIS	SRIS					
		▶Auto	Enable	Disable			
	Multi upstream Auto Speed Change	Defines the setting of this feature for all PCIe devices. "Auto" uses the DXIO default setting of 0 for Gen1 and 1 for Gen2/3.					
		▶Auto	Enabled	Disabled			
	Multi Auto Speed Change On Last Rate	Force PCIe link training speed to last advertised for all ports. Disabled=Use highest data rate ever advertised. Enabled=Use last data rate advertised.					
		▶Auto	Enable	Disable			
	PCIE Link Speed Capability	Set all PCIe port speed capability					
		Maximum speed	Gen1	Gen2	Gen3		
		Gen4	Gen5	Auto			
	RTM Margining Support	RTM Margining Support					
		▶Auto	Enable	Disable			
	EQ Bypass To Highest Rate	Controls the ability to advertise Equalization Bypass to Highest Rate Support in TSxs sent prior to LinkUp=1					
		▶Auto	Enable	Disable			

NBIO Common Options	Non-PCIe Compliant Support	Enable this setting to send command to disable Extended EIEOS, DLF, and Gen 5 Support on training failure for non-pcie compliant devices.				
		▶Auto	Enabled	Disabled		
	PCIE Idle Power Setting	Modify PCIE Power Savings Features that Can Impact Lightly Loaded Latency				
		Optimize for Latency	▶Optimize for Perf/Power			
	nBif Common Options	nBif Common Options				
		MPDMA-TF	SRIOV	SRIOV capability Enablement for Pcie capability enablement. STRAP_SRIOV_EN_DEV0_F1[0]		
				▶Auto	Disable	Enable
			ARI	Enable ARI cap in EP function for Pcie capability enablement. STRAP_ARI_EN_DEV0_F1[15]		
				▶Auto/Default	Disable	Enable
			AER	EnableAER cap in EP function for Pcie capability enablement. STRAP_AER_EN_DEV0_F1[16]		
				▶Auto	Disable	Enable
			ACS	Enable ACS cap in EP function for Pcie capability enablement. STRAP_ACS_EN_DEV0_F1[17]		
				▶Auto	Disable	Enable
			ATS	Enable ATS cap in EP function for Pcie capability enablement. STRAP_ATS_EN_DEV0_F1[18]		
				▶Auto	Disable	Enable
			PASID	Enable PASID capability in EP function for Pcie capability enablement. STRAP_PASID_EN_DEV0_F1[28]		
				▶Auto	Disable	Enable
			RTR	Enable RTR capability in EP function for Pcie capability enablement. STRAP_RTR_EN_DEV0_F1[31]		
				▶Auto	Disable	Enable
			PAGE_REQ	Enable Page request capability in EP function for Pcie capability enablement.STRAP_PAGE_REQ_EN_DEV0_F1[27]		
				▶Auto	Disable	Enable
			PWR	Enable PWR budget capability for Pcie capability enablement. STRAP_PWR_EN_DEV0_F1[17]		
				▶Auto	Disable	Enable
			ATC_ENABLE	Enable ATC enable for Pcie ATS Control. PCIE_ATS_CNTL_dev0_func1 (in the instance nbio NBIF0, nbio0 NBIF1, nbio1 NBIF0, nbio1 NBIF1).ATC_ENABLE [15]		
				▶Auto	Disable	Enable
			SDXI Class Code	Program SDXI specific Class code		
				▶Auto	Disable	Enable
			PASID Control	ATS Control register, controls if the function is permitted to send requests that contain a PASID value		
				▶Auto	Disable	Enable
			ATOMIC OP_REQ UEST	Controls the ability of a function to initiate AtomicOp requests.		
				▶Auto	Disable	Enable

NBIO Common Options	nBif Common Options	RCC_DEV0	ACS Rcc_Dev0	ACS Rcc_Dev0		
				▶Auto	Disable	Enable
			AER Rcc_Dev0	Enable AER enable for RCC_DEV0 ,STRAP_AER_EN_DN_DEV0		
				▶Auto	Disable	Enable
			DlfEnableStrap1	RCC_BIF_STRAP1,STRAP_DLF_EN=1		
				▶Auto	Disable	Enable
			Phy16GTStrap1	RCC_BIF_STRAP1 ,STRAP_PHY_16GT_EN=1		
				▶Auto	Disable	Enable
			MarginEnStrap1	RCC_BIF_STRAP1 ,STRAP_MARGIN_EN=1		
				▶Auto	Disable	Enable
			SourceValStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,Source Validation bit[23]		
				▶Auto	Disable	Enable
			TranslationalBlockingStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,Translational Blocking bit [24]		
				▶Auto	Disable	Enable
			P2pReq ACS Control	PCIE_ACS_CNTL_dev0 0x001D,P2P page request bit[2]		
				▶Auto	Disable	Enable
			P2pCompStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,P2P Completion bit[26]		
				▶Auto	Disable	Enable
			UpstreamFwdStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,Upstream Forwarding bit[27]		
				▶Auto	Disable	Enable
			P2PEgressStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,P2P Egress bit[28]		
				▶Auto	Disable	Enable
			DirectTranslatedStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,ACS Direct Translated bit [29]		
				▶Auto	Disable	Enable
			SsidEnStrap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,ACS SSID Enable bit [31]		
				▶Auto	Disable	Enable
			PriEnPageReq	PCIE_PAGE_REQ_CNTL (for all nbio instances) set to 0x0001,PriEn bit set		
				▶Auto	Disable	Enable
			PriResetPageReq	PCIE_PAGE_REQ_CNTL (for all nbio instances) set to 0x0001,Pri Reset bit clear		
				▶Auto	Disable	Enable
			Source Val ACS cntl	PCIE_ACS_CNTL_dev0 = 0x001D, Source Validation bit [0] is set		
				▶Auto	Disable	Enable
			TranslationalBlocking ACS Control	PCIE_ACS_CNTL_dev0 = 0x001D, Translational blocking bit[1]		
				▶Auto	Disable	Enable
			P2pComp ACS Control	PCIE_ACS_CNTL_dev0=0x001D,P2P Completion bit[3]		
				▶Auto	Disable	Enable
			UpstreamFwd ACS Control	PCIE_ACS_CNTL_dev0 = 0x001D,Upstream Forwarding bit[4]		
				▶Auto	Disable	Enable
			P2PEgress ACS Control	PCIE_ACS_CNTL_dev0 = 0x001D,P2P Egress bit[5]		
				▶Auto	Disable	Enable

NBIO Common Options	nBif Common Options	RCC_DEV0	P2pReq Strap5	RCC_DEV0_PORT_STRAP5 = 0xAF80_0000,P2P request strap bit ▶Auto / Disable / Enable
			E2E_PREFIX	RCC_DEV0_PORT_STRAP2 has bit STRAP_E2E_PREFIX_EN_DEV0 ▶Auto / Disable / Enable
			EXTENDED_FMT	RCC_DEV0_PORT_STRAP2 has bit STRAP_EXTENDED_FMT_SUPPORTED_DEV0 ▶Auto / Disable / Enable
			AtomicRoutingStrap5	NBIF DEV0 Enable AtomicOp Routing support in Downstream Port. ▶Auto / Disable / Enable
	Link EQ Preset Options	GEN3	Preset Search Mask Configuration (Gen3)	Configuration for Gen3 Preset Mask. Select Custom to modify Gen3 Preset Search Mask. Auto will default to platform configurations. Custom / ▶Auto
		GEN4	Preset Search Mask Configuration (Gen4)	Configuration for Gen4 Preset Mask. Select Custom to modify Gen4 Preset Search Mask. Auto will default to platform configurations. Custom / ▶Auto
		GEN5	Preset Search Mask Configuration (Gen5)	Configuration for Gen5 Preset Mask. Select Custom to modify Gen5Preset Search Mask. Auto will default to platform configurations. Custom / ▶Auto
	Enable 2 SPC (Gen4)	Enable 2 SPC (Gen4) ▶Auto / Enable		
	Safe recovery upon a BERExceeded Error	No help string ▶Auto / Enable / Disable		
	Periodic Calibration	No help string ▶Auto / Enabled / Disabled		
	Enable PCIe SFI Config via OOB	Enable PCIe SFI Config via OOB support True / ▶False		

FCH Common Options	I3C/I2C Configuration Options	I3C/I2C 0-3 Enable	Enable/disable Inter-Intergrated Circuit Control 0-3 ▶Auto / Both Disabled / I3C Enabled / I2C Enabled
		I2C 4-5 Enable	Enabled/disabled Inter-Intergrated Circuit Controller 4-5 ▶Auto / Enabled / Disabled
		Release SPD Host Control	Release SPD Host Control, so that BMC can take over the ownership of I2C/I3C bus. Enabled / ▶Disabled
		PMFW Poll DDR5 Telemetry	Send message to PMFW for polling DDR5 telemetry at the end of POST. ▶Enabled / Disabled
		Ixc Telemetry Ports Fence Control	Controls the Fencing off for I2C/I3C ports which are involved in DDR Telemetry. If this option is enabled, then the associated Ixc ports registers will be put in the secure region. Note: If this option is disabled, there is a risk of collision happening between x86 accessing IxC and PMFW running DDR Telemetry which can cause undefined behavior. ▶Enabled / Disabled
		I2C SDA Hold Override	Override I2C SDA_TX_HOLD and SDA_RX_HOLD. ▶Auto / Enabled / Disabled

FCH Common Options	I3C/I2C Configuration Options	APML SB-TSI Mode	Select APML SB-TSI over I3C or I2C. In I3C mode, the slave controller can support both I3C and I2C(-Adaptive mode).				
			I2C	▶I3C			
		I3C Push Pull HCNT Value	SCL push-pull High count for I3C transfers targeted to I3C devices.				
			8				
		I3C SDA Hold Override	Override I3C HOLD VALUE.				
			▶Auto	Enabled	Disabled		
	SATA Configuration Options	SATA Enable	Disable/enable OnChip SATA controller.				
			▶Auto	Enabled	Disabled		
		SATA RAS Support	Disable/enable OnChip SATA RAS Support.				
			▶Auto	Enabled	Disabled		
		SATA Staggered Spin-up	Enable/disable SATA staggered spin-up.				
			▶Auto	Enabled	Disabled		
		SATA Disabled AHCI Prefetch Function	Disable/enable Sata Disabled AHCI Prefetch Function.				
			▶Auto	Enabled	Disabled		
		Aggresive SAT Device Sleep P0-P1	Enable SATA DevSlp0-1. In SOC two DEVSLP pads are assigned. Aggressive Device Sleep enables the HBA to assert the DEVSLP signal as soon as there are no commands outstanding to the device and the port specific Device Sleep idle timer has expired.				
			▶Auto	Enabled	Disabled		
		SATA Controller options	SATA Controller Enable	Sata0-3 Enable	Enable/Disable Sata0-3. Each IOD has 4 Sata Controllers.		
					▶Auto	Enabled	Disabled
				Sata4-7 (Socket1) Enable	Enable/Disable Sata4-7 on Socket1(IOD1). Each IOD has 4 Sata Controllers.		
					▶Auto	Enabled	Disabled
			SATA Controller eSATA	SATA Controller eSATA			
			SATA Controller DevSlp	Socket1 DevSlp	Socket1 DevSlp0-1 Enable	Only Sata0 on each IOD/socket support DevSlp.	
						▶Auto	Enabled	Disabled
			SATA Controller SGPIO	Sata0-3 SGPIO	Enable/Disable SataSgpio on Sata0-3		
					▶Auto	Enabled	Disabled
				Sata4-7 SGPIO	Enable/Disable SataSgpio on Sata4-7 (Socket1)		
					▶Auto	Enabled	Disabled
	USB Configuration Options	XHCI Controller0-1 enable	Enable/disable USB3 controller.				
			▶Auto	Enabled	Disabled		
		USB ecc SMI Enable	Enable Double Error Detection output signal for USB S0 ram.				
			▶Auto	Enable	Off		
		MCM USB enable	XHCI2-3 enable (Socket1)	Enable/disable USB3 controller.			
				▶Auto	Enabled	Disabled	

FCH Common Options	Ac Power Loss Options	Ac Power Loss Options			
	Uart Configuration Options	Uart 0 Enable	Enable/disable Uart0. Uart 0 has no HW flow control if Uart 2 is enabled.		
			Auto	Enabled	▶Disabled
		Uart 2 Enable	Enable/disable Uart2. Uart 2 has no HW flow control if Uart 0 is enabled.		
			Auto	Enabled	▶Disabled
		Uart 1, 3 Enable	Enable/disable Uart 1, 3.		
			Auto	Enabled	▶Disabled
	ESPI Configuration Options	ESPI Enable	No help string.		
			▶Auto	Enabled	Disabled
	FCH RAS Options	ALink RAS Support	Enable FCH A-Link parity error.		
			▶Auto	Enabled	Disabled
		Reset After Sync-Flood	Enable AB to forward downstream sync-flood message to system controller.		
			▶Auto	Enabled	Disabled
	Miscellaneous Options	Boot Timer Enable	Boot Timer enable. Enable: force PMx44 bit 27 = 1 Disable: force PMx44 bit 27 = 0 Auto: PMx44 bit 27 = PcdBootTimerEnable		
			▶Auto	Enabled	Disabled
Soc Miscellaneou -s Control	ABL Console Out Control	Enable : Enable ConsoleOut Function for ABL Disable : Disable ConsoleOut Function for ABL Auto : Keep default behavior			
		▶Auto	Enable	Disable	
	ABL 2nd CPU PMU MsgBlock Log Control	ABL print 2nd CPU PMU MsgBlock contents after training.			
		▶Disabled	Enabled		
	ABL Memory Population message Control	Non-Recommended configurations may be functional but may not be validated by AMD. Select "warning message": To show warning messages if Memory channel configuration does NOT follow Memory Population Guidelines. "Fatal error": To show the messages and halt the system.			
		▶Warning message	Fatal error		
	PSP error injection support	Enable EINJ support.			
		True	▶False		
	Firmware Anti-rollback(FAR)	FAR Switch	[Enabled] : BIOS will update SPL fuse to SPL value in the SPL table. [Disabled] : BIOS will not set SPL fuse.		
			▶Auto	Enabled	Disabled
CXL Common Options	CXL Control	Enable/Disable CXL on all ports.			
		▶Auto	Enabled	Disabled	
	CXL SPM	Sets CXL memory as Special Purpose Memory.			
		▶Auto	Enabled	Disabled	
	CXL Encryption	CXL Encryption			
		Enabled	▶Disabled		
	CXL DVSEC Lock	Locks the CXL DVSEC			
		▶Auto	Enabled	Disabled	

CXL Common Options	Temp Gen5 Advertisement	Temp Gen5 Advertisement for Alternate Protocol.			
		▶Auto	Enabled	Disabled	
	Sync Header Bypass	Enable/Disable CXL Sync Header Bypass support.			
		▶Auto	Enabled	Disabled	
	CXL RAS	CXL Protocol Error Reporting	Configuration CXL Protocol Error reporting mechanism.		
			Disabled	▶SameAsPcieAer	ForceAerFwFirstIf CxlPresent
		CXL Component Error Reporting	Configuration CXL Component Error reporting mechanism.		
			Allow OS-First	Force FW-First	▶Debug FW-First
	AckFlushRetimer Configuration	Configure AckFlushRetimer register to revert it back to old value as backup. Configuration 1 will have the register as default value 0x380; Configuration 2 will revert it back to old value 0x100.			
		▶Configuration 1	Configuration 2		

4.4.5 AMD PBS

AMD PBS Setup Page.

AMD PBS				
RAS	RAS Periodic SMI Control	Enable/ disable Periodic SMI for polling [MCA Threshold] error.		
		▶Enable	Disable	
	SMI Threshold	The [SMI Threshold] limits the number of [MCA Threshold and Deferred Error SMI source] per a Unit time (Defined by [SMI Scale]). (Default: 5 dec interrupts)		
		5		
	SMI Scale	The [SMI Scale] defines the time scale. (Default: 1000 dec)		
		1000		
	SMI Scale Unit	The [SMI Scale Unit] defines the unit of time scale. (Default: ms)		
		▶millisecond	second	minute
	SMI Period	The [SMI Period] defines the polling interval (Default: 1000 dec, Maximum: 32767 dec, 0: Disable, Unit: ms)		
		1000		
	GHES Notify Type	Notification type for deferred/corrected errors		
		▶Polled	SCI	
	GHES UnCorr Notify Type	Notification type for uncorrected errors		
		▶Polled	NMI	
	PCIe GHES Notify Type	Notification type for PCIe corrected errors		
		▶Polled	SCI	
	PCIe UnCorr GHES Notify Type	Notification type for PCIe uncorrected errors		
		▶Polled	NMI	
	PCIe Root Port Corr Err Mask Reg	Initialize the PCIe AER Corrected Error Mask register of Root Port		
		0		
	PCIe Root Port UnCorr Err Mask Reg	Initialize the PCIe AER Uncorrected Error Mask register of Root Port		
		0		
	Pcie Root Port UnCorr Error Sev Reg	Initialize the PCIe AER Uncorrected Error Severity registers of Root Port		
		7EF6030		
	PCIe Device Corr Err Mask Reg	Initialize the PCIe AER Corrected Error Mask register of PCIe Device		
		0		
	PCIe Device UnCorr Err Mask Reg	Initialize the PCIe AER Uncorrected Error Mask register of PCIe Device		
		100000		
	Pcie Device UnCorr Error Sev Reg	Initialize the PCIe AER Uncorrected Error Severity registers of PCIe Device		
		7EF6030		
	CXL DP CIE Mask Enable	Enable/Disable masking of CXL DP Correctable Error - Internal Error		
		Disabled	▶Enabled	
	DRAM Hard Post Package Repair	This feature allows spare DRAM rows to replace malfunctioning rows via an in-field repair mechanism		
		▶Disabled	Enabled	

RAS	HEST DMC Structure Support	HEST DMC(Deferred Machine Check) Structure Support	
		Enable	▶Disable
	CXL Error Report Support	Enable/ disable CXL Error Reporting	
		Enable	▶Disable
SPI Locking	Enable/ disable SPI Locking for protect ROM part		
	▶Disable	Enable	

4.4.6 Serial Port Console Redirection

Serial Port Console Redirection

Serial Port Console Redirection					
COM0					
Console Redirection	Console Redirection Enable or Disable.				
	Enable	▶Disable			
COM1					
Console Redirection	Console Redirection Enable or Disable.				
	Enable	▶Disable			
COM2					
Console Redirection	Console Redirection Enable or Disable.				
	Enable	▶Disable			
COM3					
Console Redirection	Console Redirection Enable or Disable.				
	Enable	▶Disable			
Legacy Console Redirection Settings	Redirection COM Port	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.			
		▶COM0	COM1	COM2	COM3
	Resolution	On Legacy OS, the Number of Rows and Columns supported redirection.			
		▶80x24	80x25		
	Redirection After POST	When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always Enable.			
		▶Always Enable	BootLoader		
Console Redirection EMS	Console Redirection Enable or Disable.				
	Enable	▶Disable			

4.4.7 CPU Configuration

CPU Configuration Parameters.

CPU Configuration		
SVM Mode	Enable/disable CPU Virtualization.	
	▶Enabled	Disabled
Node 0 Information	View Memory Information related to Node 0.	

4.4.8 Debug Port Table Configuration

Enable or Disable DBGP and DBG2 Tables.

Debug Port Table Configuration		
Debug Port Table	Debug Port Table	
	Enabled	▶Disabled
Debug Port Table 2	Debug Port Table 2	
	Enabled	▶Disabled

4.4.9 SIO Common Setting

SIO Common Setting.

SIO Configuration		
Lock Legacy Resources	Enables/Disables Lock of Legacy Resources.	
	Enabled	▶Disabled

4.4.10 SIO Configuration

SIO Configuration.

SIO Configuration				
[*Active*] Serial Port 1	View and Set Basic properties of the SIO Logical device. Like IO Base, IRQ Range, DMA Channel and Device Mode.			
	Use This Device	Enable or Disable this Logical Device.		
		▶Enabled	Disabled	
	Possible:	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.		
		▶Use Automatic Settings	IO=3F8h; IRQ=4; DMA;	IO=3F8h; IRQ=3,4,5,7,9,10,11,12; DMA;
		IO=2F8h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=3E8h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA;
[*Active*] Serial Port 2	Use This Device	Enable or Disable this Logical Device.		
		▶Enabled	Disabled	
	Possible:	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.		
		▶Use Automatic Settings	IO=2F8h; IRQ=3; DMA;	IO=3F8h; IRQ=3,4,5,7,9,10,11,12; DMA;
		IO=2F8h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=3E8h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA;

[*Active*] Serial Port 3	View and Set Basic properties of the SIO Logical device. Like IO Base, IRQ Range, DMA Channel and Device Mode.			
	Use This Device	Enable or Disable this Logical Device.		
		▶Enabled	Disabled	
	Possible:	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.		
		▶Use Automatic Settings	IO=3E8h; IRQ=7; DMA;	IO=3E8h; IRQ=3,4,5,7,9,10,11,12; DMA;
		IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=220h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=228; IRQ=3,4,5,7,9,10,11,12; DMA;
[*Active*] Serial Port 4	Use This Device	Enable or Disable this Logical Device.		
		▶Enabled	Disabled	
	Possible:	Allows the user to change the device resource settings. New settings will be reflected on this setup page after system restarts.		
		▶Use Automatic Settings	IO=2E8h; IRQ=3; DMA;	IO=3E8h; IRQ=3,4,5,7,9,10,11,12; DMA;
		IO=2E8h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=220h; IRQ=3,4,5,7,9,10,11,12; DMA;	IO=228h; IRQ=3,4,5,7,9,10,11,12; DMA;

4.4.11 PCI Subsystem Settings

PCI Subsystem Settings.

PCI Subsystem Settings		
Above 4G decoding	Globally Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).	
	▶Enabled	Disabled
SR-IOV Support	If system has SR-IOV capable PCIe devices, this option enables or disables Single Root IO Virtualization Support.	
	▶Enable	Disable
BME DMA Mitigation	Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked.	
	Enabled	▶Disabled
Hot-Plug Support	Globally Enables or Disables Hot-Plug support for the entire System. If System has Hot-Plug capable Slots and this option set to Enabled, it provides a Setup screen for selecting PCI resource padding for Hot-Plug.	
	▶Enable	Disable

4.4.12 USB Configuration

USB Configuration Parameters.

USB Configuration					
Legacy USB Support	Enable Legacy USB support. AUTO option disalbes legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.				
	Auto	▶Enabled	Disabled		
XHCI Hand-off	This is a workaround for 0Ses without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.				
	▶Enable	Disable			
USB Mass Storage Driver Storage	Enables/disables USB Mass Storage Driver Support				
	▶Enable	Disable			
POST 60/64 Emulation	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.				
	▶Enable	Disable			
USB transfer time-out	The time-out value for control, bulk, and interrupt transfers.				
	1 sec	5 sec	10 sec	▶20 sec	
Device reset time-out	USB mass storage device Start Unit command time-out.				
	10 sec	▶20 sec	30 sec	40 sec	
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.				
	▶Auto	Manual			
AMI Virtual CDROM0 1.00	Mass storage device emulation type. Auto: Enumerates devices according to their media format. Optical drives are emulated as "CDROM," drives with no media will be emulated according to drive type.				
	▶Auto	Floppy	Forced FDD	Hard Disk	CD-ROM
AMI Virtual HDisk0 1.00	Mass storage device emulation type. Auto: Enumerates devices according to their media format. Optical drives are emulated as "CDROM," drives with no media will be emulated according to drive type.				
	▶Auto	Floppy	Forced FDD	Hard Disk	CD-ROM
AMI Virtual CDROM0 1.00	Mass storage device emulation type. Auto: Enumerates devices according to their media format. Optical drives are emulated as "CDROM," drives with no media will be emulated according to drive type.				
	▶Auto	Floppy	Forced FDD	Hard Disk	CD-ROM

4.4.13 Network Stack Configuration

Network Stack Settings.

Network Stack Configuration		
Network Stack	Enables/disables UEFI Network Stack.	
	▶Enable	Disable
IPv4 PXE Support	Enables/disables IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.	
	Enable	▶Disable
IPv4 HTTP Support	Enables/disables IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.	
	Enable	▶Disable
IPv6 PXE Support	Enables/disables IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.	
	Enable	▶Disable
IPv6 HTTP Support	Enables/disables 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	

4.4.14 CSM Configuration

CSM configuration: Enable/Disable, Option ROM execution settings, etc.

CSM Configuration		
CSM Support	Enables/disables CSM Support.	
	Enable	▶Disable

4.4.15 NVMe Configuration

NVMe Device Options Settings.

4.4.16 SATA Configuration

NVMe Device Options Settings.

4.4.17 AMD Mem Configuration Status

To display memory configuration (initialized by ABL) status.

AMD Mem Configuration Status		
Socket 0	Socket-specific memory configuration status.	
	Channel 0-1, 3-5, 7	Channel-specific memory configuration status.

4.4.18 Tls Auth Configuration

Press <Enter> to select Tls Auth Configuration.

T1s Auth Configuration			
Server CA Configuration	Press <Enter> to configure Server CA.		
	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.	

4.4.19 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).		

4.4.20 Driver Health

Provides Health Status for the Drivers/Controllers.

Driver Health		
Broadcom NXE Gigabit Ethernet Driver	Provides Health Status for the Drivers/Controllers.	
	Controller A15A9798 Child 0	Provides Health Status for the Drivers/Controllers.
		Healthy
	Controller A15A9798 Child 9F0A5918	Provides Health Status for the Drivers/Controllers.
		Healthy
Broadcom NXE Gigabit Ethernet Driver	Controller 9F881E18 Child 0	Provides Health Status for the Drivers/Controllers.
		Healthy
	Controller 9F881E18 Child 9EDBBD18	Provides Health Status for the Drivers/Controllers.
		Healthy

4.5 Chipset

4.5.1 PCIe Link Training Type

PCIe Link training in 1 or 2 steps.

▶1 Step
2 Step

4.5.2 PCIe Compliance Mode

PCIe Link Compliance Mode.

On
▶Off

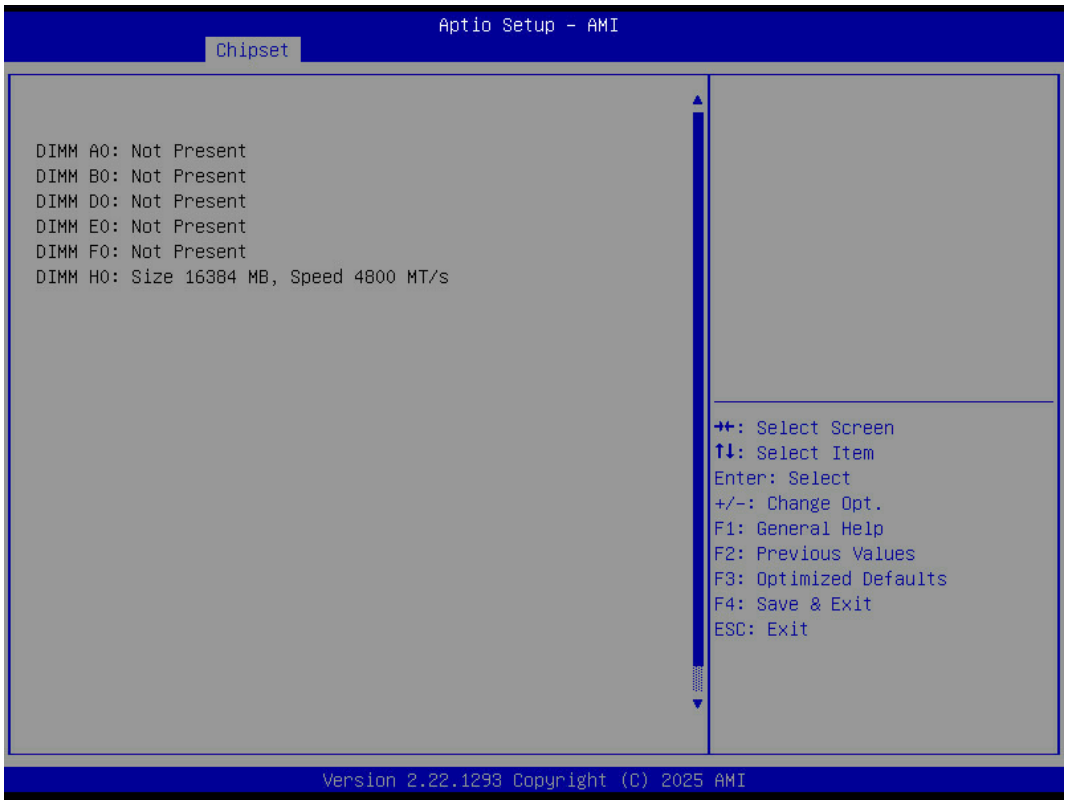
4.5.3 South Bridge

South Bridge Parameters

South Bridge				
SB Debug Configuration	Options For SB Debug Features.			
	SB SATA DEBUG Configuration	Aggressive Link PM Capability	Indicates Whether Host Bus Adapter (HBA) can support Auto-Generating Link Requests to the partial or slumber states when there are no commands to process.	
			▶Enable	Disable
		Port Multiplier Capability	Indicates whether Host Bus Adapter (HBA) can support a port multiplier.	
			▶Enable	Disable
		SATA Ports Auto Clock Control	Enable/disable SATA Ports Auto Clock Control.	
			▶Enable	Disable
		SATA Partial State Capability	Indicates whether SATA Host Bus Adapter (HBA) can support transitions to the Partial State.	
			▶Enable	Disable
		SATA FIS Based Switching	Indicates whether SATA Host Bus Adapter (HBA) can support Port Multiplier FIS-Based Switching.	
			▶Enable	Disable
		SATA Command Completion Coalescing Support	Indicates whether SATA Host Bus Adapter (HBA) can support Command Completion Coalescing.	
			Enable	▶Disable
		SATA Slumber State Capability	Indicates whether SATA Host Bus Adapter (HBA) can support Transition to the Slumber State.	
			▶Enable	Disable
		SATA Target Support 8 Devices	Indicates whether SATA Target support 8 devices function.	
			Enable	▶Disable
		Generic Mode	Sata Disable Generic Mode.	
			Enable	▶Disable
		SATA AHCI Enclosure	SATA AHCI Enclosure Management.	
			Enable	▶Disable
		SATA SGPIO 0	Enable/Disable SATA Serial General Purpose Input/Output (SGPIO) 0.	
			Enable	▶Disable
	SB FUSION DEBUG Configuration	Options For SB FUSION DEBUG Configuration.		
		TimerTick Tracking	Enable	▶Disable
		Clock Interrupt Tag	Enable	▶Disable
	SB MISC DEBUG Configuration	Options For SB DEBUG Configuration.		
		SB Clock Spread Spectrum	Enable/Disable CG1_PLL Spread Spectrum.	
			Enable	▶Disable
		HPET In SB	HPET Function Switch	
			▶Enable	Disable
		MsiDis in HPET	Expose MSI capability in HPET Capability register.	
			▶Enable	Disable

4.5.4 North Bridge
North Bridge Parameters

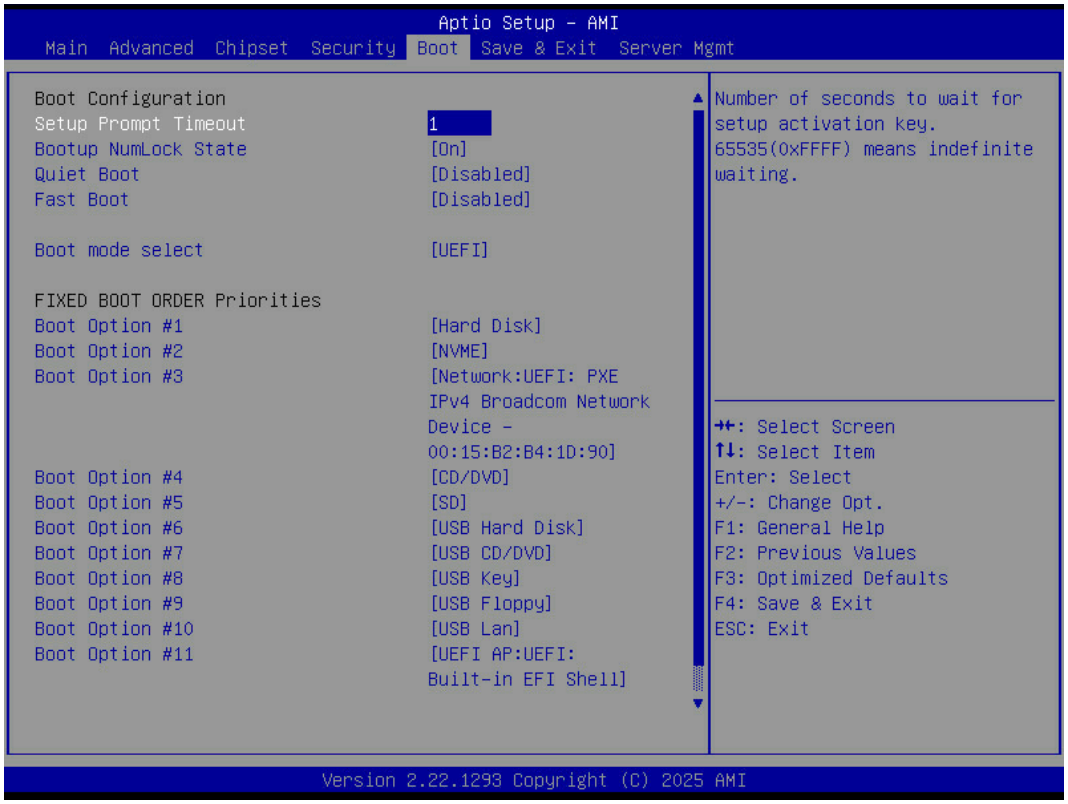
Socket 0 Information
View Information related to Socket 0.



4.6 Security

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

4.7 Boot



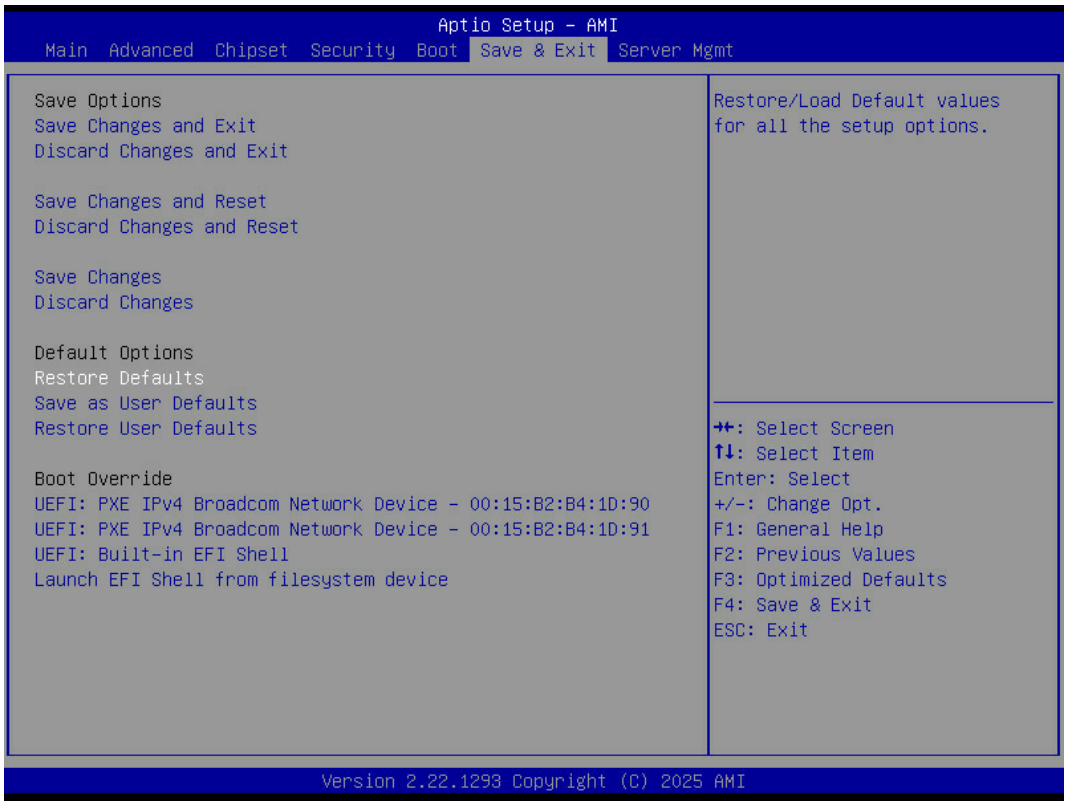
Boot				
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.			
	1			
Bootup Numlock State	Select the keyboard Numlock state.			
	▶On		Off	
Quiet Boot	Enables/disables Quiet Boot option.			
	Enable		▶Disable	
Fast Boot	Enables or disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.			
	Enable		▶Disable	
Boot mode select	Select boot mode LEGACY/UEFI.			
	▶UEFI		LEGACY	
Boot Option #1	Sets the system boot order.			
	▶Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #2	Sets the system boot order.			
	Hard Disk	▶NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #3	Sets the system boot order.			
	Hard Disk	NVME	▶Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled

Boot Option #4	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	▶CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled

Boot Option #5	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	▶SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #6	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	▶USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #7	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	▶USB CD/DVD	USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #8	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	▶USB Key
	USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #9	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	▶USB Floppy	USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #10	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	▶USB Lan	UEFI AP:UEFI:Built-in EFI Shell	Disabled
Boot Option #11	Sets the system boot order.			
	Hard Disk	NVME	Network:UEFI: PXE IPv4 Broadcom Network Device	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	▶UEFI AP:UEFI:Built-in EFI Shell	Disabled

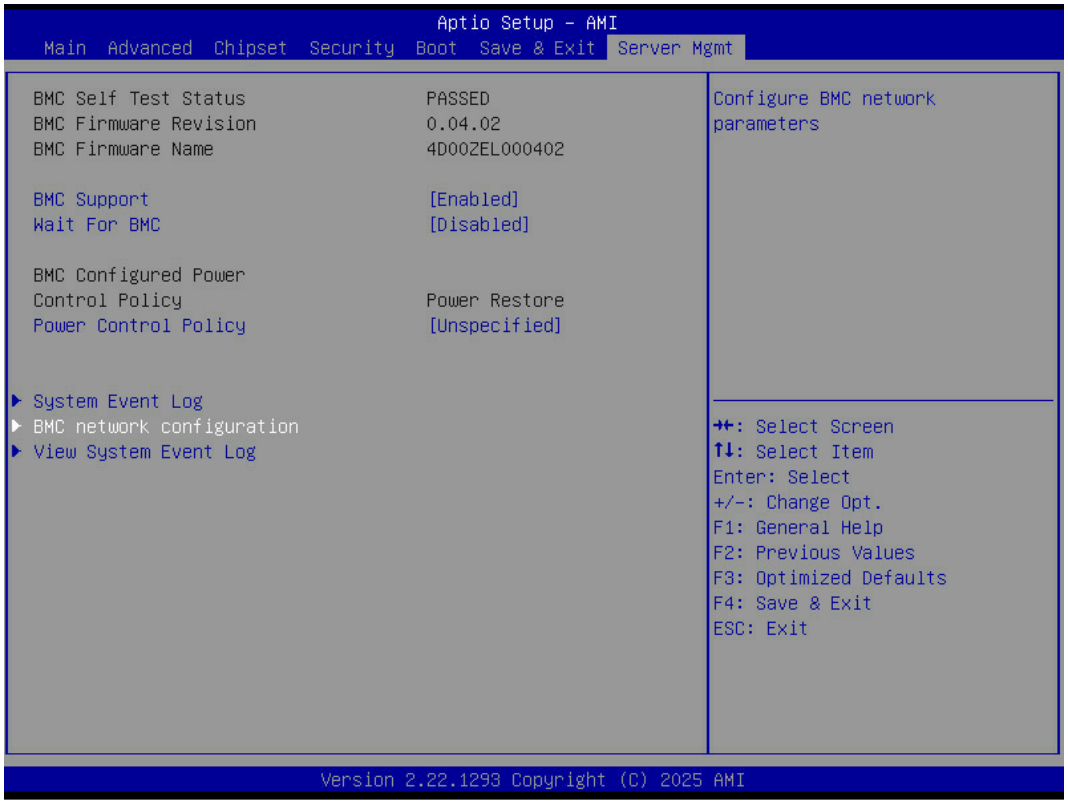
UEFI NETWORK Drive BBS Priorities	Specifies the Boot Device Priority sequence from available UEFI NETWORK Drives.			
	Boot Option #1	Sets the system boot order.		
		▶Network:UEFI: PXE IPv4 Broadcom Network Device - 00:15:B2:B4:1D:90	Network:UEFI: PXE IPv4 Broadcom Network Device - 00:15:B2:B4:1D:91	Disable
	Boot Option #2	Sets the system boot order.		
		Network:UEFI: PXE IPv4 Broadcom Network Device - 00:15:B2:B4:1D:90	▶Network:UEFI: PXE IPv4 Broadcom Network Device - 00:15:B2:B4:1D:91	Disable
UEFI Application Boot Priorities	Specifies the Boot Device Priority sequence from available UEFI Application.			
	Boot Option #1	Sets the system boot order.		
		▶UEFI: Built-in EFI Shell	Disabled	

4.8 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	
Launch EFI Shell from filesystem device	Attempts to Launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

4.9 Server Mgmt



4.9.1 BMC Support

Enable/Disable interfaces to communicate with BMC.

▶Enabled
Disabled

4.9.2 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 interfaces.

Enabled
▶Disabled

4.9.3 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

4.9.4 System Event Log

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

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

4.9.5 BMC network configurtion

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/Disable LAN1 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	

4.9.6 View System Event Log

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

4.10 BIOS Post Code

There are two ways to get post code,

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

(1) Read the first 256 bytes:$ipmitool -I lanplus -H "$BMC_IP" -U "$BMC_USER" -P "$BMC_PASSWD" raw 0x32 0x73 0x00
(2) Read the next 256 bytes: $ipmitool -I lanplus -H "$BMC_IP" -U "$BMC_USER" -P "$BMC_PASSWD" raw 0x32 0x73 0x02

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

AMD PSP FW POST code
(FW output 2 bytes post code,but user only can see low byte on IPMI command output)

Post Code	Description
Start Processor Test Points	
0xE000	Entry used for range testing for @b Processor related TPs
Memory test points	
0xE001	Memory structure initialization (Public interface)
0xE002	SPD Data processing (Public interface)
0xE003	Memory configuration (Public interface) Phase 1
0xE004	DRAM initialization
0xE005	ProcMemSPDChecking
0xE006	ProcMemModeChecking
0xE007	Speed and TCL configuration
0xE008	ProcMemSpdTiming
0xE009	ProcMemDramMapping
0xE00A	ProcMemPlatformSpecificConfig
0xE00B	ProcMemPhyCompensation
0xE00C	ProcMemStartDcts
0xE00D	ProcMemBeforeDramInit (Public interface)
0xE00E	ProcMemPhyFenceTraining
0xE00F	ProcMemSynchronizeDcts
0xE010	ProcMemSystemMemoryMapping
0xE011	ProcMemMtrrConfiguration
0xE012	ProcMemDramTraining
0xE013	ProcMemBeforeAnyTraining(Public interface)
PMU Test Points	
0xE014	ABL Mem - PMU - Before PMU Firmware load
0xE015	ABL Mem - PMU - After PMU Firmware load
0xE016	ABL Mem - PMU Populate SRAM Timing
0xE017	ABL Mem - PMU Populate SRAM Config
0xE018	ABL Mem - PMU Write SRAM Msg Block
0xE019	ABL Mem - Wait for Phy Cal Complete
0xE01A	ABL Mem - Phy Cal Complete
0xE01B	ABL Mem - PMU Start

0xE01C	ABL Mem - PMU Started
0xE01D	ABL Mem - PMU Waiting for Complete
0xE01E	ABL Mem - PMU Stage Dec Init
0xE01F	ABL Mem - PMU Stage Training Wr Lvl
0xE020	ABL Mem - PMU Stage Training Rx En
0xE021	ABL Mem - PMU Stage Training Rd Dqs
0xE022	ABL Mem - PMU Stage Traning Rd 2D
0xE023	ABL Mem - PMU Stage Training Wr 2D
0xE024	ABL Mem - PMU Queue Empty
0xE025	ABL Mem - PMU US message Start
0xE026	ABL Mem - PMU US message End
0xE027	ABL Mem - PMU Complete
0xE028	ABL Mem - PMU - After PMU Training
0xE029	ABL Mem - PMU - Before Disable PMU
Original Post code	
0xE02A	ABL Mem - ProcMemTransmitDqsTraining
0xE02B	ABL Mem - Start write sweep
0xE02C	ABL Mem - Set Transmit DQ delay
0xE02D	ABL Mem - Write test pattern
0xE02E	ABL Mem - Read Test pattern
0xE02F	ABL Mem - Compare Test pattern
0xE030	ABL Mem - Update results
0xE031	ABL Mem - Start Find passing window
0xE032	ABL Mem - ProcMemMaxRdLatencyTraining
0xE033	ABL Mem - Start sweep
0xE034	ABL Mem - Set delay
0xE035	ABL Mem - Write test pattern
0xE036	ABL Mem - Read Test pattern
0xE037	ABL Mem - Compare Test pattern
0xE038	ABL Mem - Online Spare init
0xE039	ABL Mem - Chip select Interleave Init
0xE03A	ABL Mem - Node Interleave Init
0xE03B	ABL Mem - Channel Interleave Init
0xE03C	ABL Mem - ECC initialization
0xE03D	ABL Mem - Platform Specific Init
0xE03E	ABL Mem - Before callout for "AgesaReadSpd"
0xE03F	ABL Mem - After callout for "AgesaReadSpd"
0xE040	ABL Mem - Before optional callout "AgesaHookBeforeDramInit"
0xE041	ABL Mem - After optional callout "AgesaHookBeforeDramInit"
0xE042	ABL Mem - Before optional callout "AgesaHookBeforeDQSTraining"
0xE043	ABL Mem - After optional callout "AgesaHookBeforeDQSTraining"
0xE044	ABL Mem - Before optional callout "AgesaHookBeforeDramInit"
0xE045	ABL Mem - After optional callout "AgesaHookBeforeDramInit"
0xE046	ABL Mem - After MemDataInit
0xE047	ABL Mem - Before InitializeMCT
0xE048	ABL Mem - Before LV DDR3
0xE049	ABL Mem - Before InitMCT
0xE04A	ABL Mem - Before OtherTiming

0xE04B	ABL Mem - Before UMAMemTyping
0xE04C	ABL Mem - Before SetDqsEccTmgs
0xE04D	ABL Mem - Before MemClr
0xE04E	ABL Mem - Before On DIMM Thermal
0xE04F	ABL Mem - Before DMI
0xE050	ABL MEM - End of phase 3 memory code
CPU test points	
0xE051	Entry point CPU init after training
0xE052	Exit point CPU init after training
0xE053	Entry point CPU APOB data init
0xE054	Exit point CPU APOB data init
0xE055	Entry point CPU Optimized boot init
0xE056	Exit point CPU Optimized boot init
0xE057	Entry point CPU APOB EDC info init
0xE058	Exit point CPU APOB EDC info init
0xE059	Entry point CPU APOB CCD map data init
0xE05A	Exit point CPU APOB CCD map data init
Extended memory test point	
0xE080	ProcMemSendMRS2
0xE081	Sedding MRS3
0xE082	Sending MRS1
0xE083	Sending MRS0
0xE084	Continuous Pattern Read
0xE085	Continuous Pattern Write
0xE086	Mem: 2d RdDqs Training begin
0xE087	Mem: Before optional callout to platform BIOS to change External Vref during 2d Training
0xE088	Mem: After optional callout to platform BIOS to change External Vref during 2d Training
0xE089	Configure DCT For General use begin
0xE08A	Configure DCT For training begin
0xE08B	Configure DCT For Non-Explicit
0xE08C	Configure to Sync channels
0xE08D	Allocate C6 Storage
0xE08E	Before LV DDR4
0xE08F	Before LV DDR3
Gnb Earlier init	
0xE090	TP0x90
0xE091	GNB earlier interface
0xE092	GNB Early VGA entry
0xE093	GNB Early VGA exit
0xE094	GNB Initialization entry
0xE095	GNB Initialization exit
0xE096	GNB internal debug code
0xE097	GNB internal debug code
0xE098	GNB internal debug code
0xE099	GNB internal debug code
0xE09A	GNB internal debug code

0xE09B	GNB internal debug code
0xE09C	GNB internal debug code
0xE09D	GNB internal debug code
0xE09E	GNB internal debug code
0xE09F	GNB internal debug code

0xE0A0	TP0xA0
0xE0A1	GNB internal debug code
0xE0A2	GNB internal debug code
0xE0A3	GNB internal debug code
0xE0A4	GNB internal debug code
0xE0A5	GNB internal debug code
0xE0A6	GNB internal debug code
0xE0A7	GNB internal debug code
0xE0A8	GNB internal debug code
0xE0A9	GNB internal debug code
0xE0AA	GNB internal debug code
0xE0AB	GNB internal debug code
0xE0AC	GNB internal debug code
0xE0AD	GNB internal debug code
0xE0AE	GNB internal debug code
0xE0AF	GNB internal debug code
New ABL Post Code Definitions	
These are temporary values until a new assignment is made	
0xEA00	ABL Begin
0xEA01	ABL End
0xEA10	ABL Debug Synchronization
0xE0B0	Abl1Begin
0xE0B1	ABL 1 Initialization
0xE0B2	ABL 1 DF Early
0xE0B3	ABL 1 DF Pre Training
0xE0B4	ABL 1 Debug Synchronization
0xE0B5	ABL 1 Error Detected
0xE0B6	ABL 1 Global memory error detected
0xE0B7	ABL 1 End
0xE0B8	ABL 2 Begin
0xE0B9	ABL 2 Initialization
0xE0BA	ABL 2 After Training
0xE0BB	ABL 2 Debug Synchronization
0xE0BC	ABL 2 Error detected
0xE0BD	ABL 2 Global memory error detected
0xE0BE	ABL 2 End
0xE0BF	ABL 3 Begin
0xE0C0	ABL 3 Initialziation
0xE1C0	ABL 3 GMI/xGMI Initialization Stage 1
0xB1C0	ABL 3 GMI/xGMI Initialization Stage 1 Warning
0xF1C0	ABL 3 GMI/xGMI Initialization Stage 2 Error
0xE2C0	ABL 3 GMI/xGMI Initialization Stage 2
0xB2C0	ABL 3 GMI/xGMI Initialization Stage 2 Warning

0xF2C0	ABL 3 GMI/xGMI Initialization Stage 2 Error
0xE3C0	ABL 3 GMI/xGMI Initialization Stage 3
0xB3C0	ABL 3 GMI/xGMI Initialization Stage 3 Warning
0xF3C0	ABL 3 GMI/xGMI Initialization Stage 3 Error
0xE4C0	ABL 3 GMI/xGMI Initialization Stage 4
0xB4C0	ABL 3 GMI/xGMI Initialization Stage 4 Warning
0xF4C0	ABL 3 GMI/xGMI Initialization Stage 4 Error
0xE5C0	ABL 3 GMI/xGMI Initialization Stage 5
0xB5C0	ABL 3 GMI/xGMI Initialization Stage 5 Warning
0xF5C0	ABL 3 GMI/xGMI Initialization Stage 5 Error
0xE6C0	ABL 3 GMI/xGMI Initialization Stage 6
0xB6C0	ABL 3 GMI/xGMI Initialization Stage 6 Warning
0xF6C0	ABL 3 GMI/xGMI Initialization Stage 6 Error
0xE7C0	ABL 3 GMI/xGMI Initialization Stage 7
0xE8C0	ABL 3 GMI/xGMI Initialization Stage 8
0xE9C0	ABL 3 GMI/xGMI Initialization Stage 9
0xF9C0	ABL 3 GMI/xGMI Initialization Stage 9 Error
0xEAC0	ABL 3 GMI/xGMI Initialization Stage 10
0xFAC0	ABL 3 GMI/xGMI Initialization Stage 10 Error
0xE0C1	Abl3ProgramUmcKeys
0xE0C2	ABL 3 DF Final Initalization
0xE0C3	ABL 3 Execute Synchronization Function
0xE0C4	ABL 3 Debug Synchronization Function
0xE0C5	ABL 3 Error Detected
0xE0C6	ABL 3 Global memroy error detected
0xE0C7	ABL 4 Initialiation - cold boot
0xE0C8	ABL 4 Memory test - cold boot
0xE0C9	ABL 4 APOB Initialization - cold boot
0xE0CA	ABL 4 Finalize memory settings - cold boot
0xE0CB	ABL 4 CPU Initialize Optimized Boot - cold boot
0xE0CC	ABL 4 Gmi Pcie Training - cold boot
0xE0CD	ABL 4 Cold boot End
0xE0CE	ABL 4 Initialization - Resume boot
0xE0CF	ABL 4 Resume End
0xE0D0	ABL 4 End Cold/Resume boot
0xE0D1	ABL 2 memory initialization
0xE0D2	ABL 3 memory initialization
0xE0D3	ABL 3 End
0xE0D4	ABL 1 Enter Memory Flow
0xE0D5	Memorry flow memory clock synchronization
0xE0E0	Before IDS calls out to get IDS data
0xE0E1	After IDS calls out to get IDS data
PMU test points	
0xE0F9	Failed PMU training.
0xE0FA	End of phase 1 memory code
0xE0FB	End of phase 2 memory code
ABL0 test points	
0xE0FC	Abl0Begin

0xE0FD	ABL 0 End
0xE0FE	Abl0 Begin with Fatal Mode
0xE0FF	ABL 0 End with Fatal Mode
ABL5 test points	
0xE100	ABL 7 End
0xE101	ABL 7 Resume boot
0xE102	ABL 6 End
0xE103	ABL 6 Initialization
0xE104	End of phase 1b memory code
0xE105	ABL 1b memory initialization
0xE106	ABL 6 Global memroy error detected
0xE107	ABL 1b Debug Synchronization Function
0xE108	ABL 4b Debug Synchronization Function
0xE109	AblbBegin
0xE10A	Ab4bBegin
0xE10B	BSP encountered HMAC fail on APOB Header
0xE10C	ABL 18 End
0xE10D	ABL 18 Resume boot
0xE10E	ABL 15 End
0xE10F	ABL 15 Initialization
0xE110	Before UMC based device initialization
0xE111	After UMC based device initialization
0xE2A0	ABL Error General ASSERT
0xE2A1	Unknown Error
0xE2A3	ABL Error Log Inig Error
0xE2A4	ABL Error for On DIMM thermal Heap allocation error
0xE2A5	ABL Error for memory test error
0xE2A6	ABL Error while executing memory test error
0xE2A7	ABL Error DDR Post Packge Repair Mem Auto Heap Alloc error
0xE2A8	ABL Error for DDR Post Package repair Apob Heap Alloc error
0xE2A9	ABL Error for DDR Post Package Repair No PPR Table Heap Aloc error
0xE2AA	ABL Error for Ecc Mem Auto Aloc Error error
0xE2AB	ABL Error for Soc Scan Heap Aloc error
0xE2AC	ABL Error for Soc Scan No Die error
0xE2AD	ABL Error for Nb Tech Heap Aloc error
0xE2AE	ABL Error for No Nb Constructor error
0xE2B0	ABL Error for No Tech Constructor error
0xE2B1	ABL Error for ABL1b Auto Alocation error
0xE2B2	ABL Error for ABL1b No NB Constructor error
0xE2B3	ABL Error for ABL2 No Nb Constructor error
0xE2B4	ABL Error for ABL3 Auto Allocation error
0xE2B5	ABL Error for ABL3 No Nb Constructor error
0xE2B6	ABL Error for ABL1b General error
0xE2B7	ABL Error for ABL2 General error
0xE2B8	ABL Error for ABL3 General error
0xE2B9	ABL Error for Get Target Speed error
0xE2BA	ABL Error for Flow P1 Family Support error
0xE2BB	ABL Error for No Valid Ddr4 Dimms error

0xE2BC	ABL Error for No Dimm Present error
0xE2BD	ABL Error for Flow P2 Family Supprot error
0xE2BE	ABL Error for Heap Deallocation for PMU Sram Msg Block error
0xE2BF	ABL Error for DDR Recovery error
0xEBC0	ABL Error for RRW Test error
0xE2C1	ABL Error for On Die Thermal error
0xE2C2	ABL Error for Heap Allocation For Dct Struct Amd Ch Def structure error
0xE2C3	ABL Error for Heap Allocation for PMU SRAM Msg block error
0xE2C4	ABL Error for Heap Phy PLL lock Flure error
0xE2C5	ABL Error for Pmu Training error
0xE2C6	ABL Error for Failure to Load or Verify PMU FW error
0xE2C7	ABL Error for Allocate for PMU SRAM Msg Block No Init error
0xE2C8	ABL Error for Failure BIOS PMU FW Mismatch AGESA PMU FW version error
0xE2C9	ABL Error for Agesa memory test error
0xE2CA	ABL Error for Deallocate for PMU SRAM Msg Block error
0xE2CB	ABL Error for Module Type Mismatch RDIMM error
0xE2CC	ABL Error for Module type Mismatch LRDIMM error
0xE2CD	ABL Error for MEm Auto NVDIM error
0xE2CE	ABL Error for Unknowm Responce error
0xE2CF	ABL Error for Over Clock Error RRW Test Results Error
0xE2D0	ABL Error for Over Clock Error PMU Training Error
0xE2D1	ABL Error for ABL1 General Error
0xE2D2	ABL Error for ABL2 General Error
0xE2D3	ABL Error for ABL3 General Error
0xE2D4	ABL Error for ABL4 General Error
0xE2D5	ABL Error over clock Mem Init Error
0xE2D6	ABL Error over clock Mem Other Error
0xE2D7	ABL Error for ABL6 General Error
0xE2D8	ABL Error Event Log Error
0xE2D9	ABL Error FATAL ABL1 Log Error
0xE2DA	ABL Error FATAL ABL2 Log Error
0xE2DB	ABL Error FATAL ABL3 Log Error
0xE2DC	ABL Error FATAL ABL4 Log Error
0xE2DD	ABL Error Slave Sync function execution Error
0xE2DE	ABL Error Slave Sync communicaton with data set to master Error
0xE2DF	ABL Error Slave broadcast communication from master to slave Error
0xE2E0	ABL Error FATAL ABL6 Log Error
0xE2E1	ABL Error Slave Offline Error
0xE2E2	ABL Error Slave Informs Master Error Info Error
0xE2E3	ABL Error Error Heap Locate for PMU SRAM Msg Block Error
0xE2E4	ABL Error ABL2 Auto Error
0xE2E5	ABL Error Flow P3 Family support Error
0xE2E5	ABL Error Abl 4 Gen Error
0xE2E7	ABL Error Mix RDIMM & LRDIMM in a channel
0xE2E8	ABL Error Memory Present on Disconnected Channel
0xE2EB	ABL Error MBIST Heap Allocation Error

0xE2EC	ABL Error MBIST Results Error
0xE2ED	ABL Error NO Dimm Smcus Info Error
0xE2EE	ABL Error Por Max Freq Table Error
0xE2EF	ABL Error Unsupproted DIMM Config Error
0xE2F0	ABL Error No Ps Table Error
0xE2F1	ABL Error Cad Bus Timing Not Found Error
0xE2F2	ABL Error Data Bus Timing Not Found Error
0xE2F3	ABL Error LrDIMM IBT Not Found Error
0xE2F4	ABL Error Unsupprote Dimm Config Max Freq Error Error
0xE2F5	ABL Error Mr0 Not Found Error
0xE2F6	ABL Error Obt Pattern Not found Error
0xE2F7	ABL Error Rc10 Op Speed Not FOund Error
0xE2F8	ABL Error Rc2 Ibt Not Found Error
0xE2F9	ABL Error Rtt Not Found Error
0xE2FA	ABL Error Checksum ReStrt Results Error
0xE2FB	ABL Error No Chipselect Results Error
0xE2FC	ABL Error No Common Cas Latency Results Error
0xE2FD	ABL Error Cas Latecncy exceeds Taa Max Error
0xE2FE	ABL Error Nvdimm Arm Missmatch Power Policy Error
0xE2FF	ABL Error Nvdimm Arm Missmatch Power Source Error
0xE300	ABL Error ABL 1 Mem Init Error
0xE301	ABL Error ABL 2 Mem Init Error
0xE302	ABL Error ABL 4 Mem Init Error
0xE303	ABL Error ABL 6 Mem Init Error
0xE304	ABL Error ABL 1 error repor Error
0xE305	ABL Error ABL 2 error repor Error
0xE306	ABL Error ABL 3 error repor Error
0xE307	ABL Error ABL 4 error repor Error
0xE308	ABL Error ABL 6 error repor Error
0xE30A	ABL Error message slave sync function execution Error
0xE30B	ABL Error slave offline Error
0xE30C	ABL Error Sync Master Error
0xE30D	ABL Error Slave Informs Master Info Message Error
0xE30E	ABL Error Mix Hynix LRDIMM with other vendor LRDIMM in a channel
0xE30F	ABL Error General Assert Error
0xE310	ABL ErrorNo Dimms On Any Channel in sysem
0xE311	ABL Error for Shared Heap Aloc error
0xE312	ABL Error for Main Heap Aloc error
0xE313	ABL Error for Shared Heap loc error
0xE314	ABL Error for Main Heap loc error
0xE316	ABL Error No memory available in system
0xE320	0xE320
0xE321	ABL Error Mixed 3DS and Non-3DS DIMM in a channel
0xE322	ABL Error Mixed x4 and x8 DIMM in a channel
0xE323	ABL Memory MBIST Rrw default test
0xE324	ABL Memory MBIST Interface test
0xE325	ABL Memory MBIST DataEye
0xE326	ABL Memory Post Package Repair

0xE327	ABL Error S0i3 DF restore buffer Error
0xE328	ABL Error CPU OPN Mismatch in case of Multi Socket population
0xE329	Recoverable APCB Checksum Error
0xE32A	Fatal APCB Checksum Error
0xE32B	ABL Error BIST Failure
0xE32C	ABL Error DDR Type Mismatch DDR5 Error
0xE32D	ABL Error Mix DIMM with different ECC bit size in a channel
0xE32E	ABL Error No ability to recover I2C bus without power cycling the platform
0xE32F	ABL Error I2C reset failure
0xE330	ABL Error DDR Module Type Mismatch
0xE331	ABL Error PMIC Error
0xE332	ABL Error Incompatible OPN
0xE333	ABL Error No ability to recover I3C bus without power cycling the platform
0xE334	ABL Error I3C reset failure
0xE335	ABL Error Absence of either or both AC-Power GPIO or WLAN GPIO Apcb Data
0xE336	ABL Memory Heal BIST Start
0xE337	ABL Memory Heal BIST End
0xE338	ABL Memory Heal BIST Write
0xE339	ABL Memory Heal BIST Read
0xE33A	ABL Memory Heal BIST Repair
0xE33B	Timeout at PMFW SwitchToMemoryTrainingState
0xE33C	DIMM with RCD Montage version B1 detected
0xE33D	ABL DDR PMU training complete
0xE33E	Timeout at PMFW SwitchToMemoryTrainingState
0xE33F	DIMM with TI PMIC revision 1.1 (XTPS) detected
0xE343	ABL DDR DIMM SPD verify CRC failure
0xE344	ABL DDR DIMM SPD Invalid Field Value
0xE345	ABL Timeout to detect CPU OPN Mismatch in case of Multi Socket population
0xE346	ABL Error 3DS DIMM in a SP6 system
0xE350	ABL DDR Runtime Post Package Repair Begin
0xE351	ABL DDR Runtime Post Package Repair End
0xE60B	ABL Functions execute Before
0xE60C	ABL Functions execute
0xEFFF	EndAgesas

AMI POST Code

Post Code	Description
0x10	PEI core is started
0x11	Pre-memory CPU initialization is started
0x12	Pre-memory CPU initialization is started (CPU module specific)
0x13	Pre-memory CPU initialization is started (CPU module specific)
0x14	Pre-memory CPU initialization is started (CPU module specific)
0x15	Pre-memory North Bridge initialization is started
0x16	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x17	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x18	Pre-memory North Bridge initialization is started (North Bridge module specific)
0x19	Pre-memory South Bridge initialization is started
0x1A	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1B	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1C	Pre-memory South Bridge initialization is started (South Bridge module specific)
0x1D~ 0x2A	Oem pre-memory initialization codes
0x2B	Memory initialization. Serial Presence Detect(SPD) data reading
0x2C	Memory initialization. Meory Presence detection
0xB2	Memory initialization. Programming memory timing information
0xB7	Memory initialization. Configuring memory
0xB9	Memory_Optimizing
0x2F	Memory initialization. (Other)
0x30	Reserved for ASL (See ASL status codes section below)
0x31	Memory Installed
0x32	CPU post-memory initialization is started
0x33	CPU post-memory initialization. Cache initialization
0x34	CPU post-memory initialization. Application Processor(s) (AP) initialization
0x35	CPU post-memory initialization. BootStrap Processor(BSP) initialization
0x36	CPU post-memory initialization. System Management Mode (SMM) initialization
0x37	Post-memory North Bridge initialization is started

0x38	Post-memory North Bridge initialization is started (North Bridge module specific)
0x39	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3A	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3B	Post-memory South Bridge initialization is started
0x3C	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3D	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3E	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3F~0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
S3 resume progress codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by th DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loadded
DXE	
0x60	DXE code is started
0x61	NVRAM initialization
0x62	Initialization of the South Bridge runtimes services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Brodge module specific)
0x6C	North Bridge DXE initialization (North Brodge module specific)
0x6D	North Bridge DXE initialization (North Brodge module specific)
0x6E	North Bridge DXE initialization (North Brodge module specific)
0x6F	North Bridge DXE initialization (North Brodge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization

0x73	North Bridge DXE initialization (South Brodge module specific)
0x74	North Bridge DXE initialization (South Brodge module specific)
0x75	North Bridge DXE initialization (South Brodge module specific)
0x76	North Bridge DXE initialization (South Brodge module specific)
0x77	North Bridge DXE initialization (South Brodge module specific)
0x78	ACPI module initialization
0x79	CSM initialization
0x7A~0x7F	Reserved for future AMI DXE codes
0x80~0x8F	OEM DXE initialization codes
0x90	Boot Device Selection(BDS) phase is started
0x91	Driver connecting is started
0x92	PCI Bus initialization is started
0x93	PCI Bus Hot Plug Controller initialization
0x94	PCI Bus Enumeration
0x95	PCI Bus Request Resources
0x96	PCI Bus Assign Resources
0x97	Console Output devices connect
0x98	Console input devices connect
0x99	Super IO initialization
0x9A	USB initialization is started
0x9B	USB Reset
0x9C	USB Detect
0x9D	USB Enable
0x9E~0x9F	Reserved for future AMI codes
0xA0	IDE initialization is started
0xA1	IDE Reset
0xA2	IDE detect
0xA3	IDE Enable
0xA4	SCSI initialization is started
0xA5	SCSI Reset
0xA6	SCSI Detect
0xA7	SCSI Enable
0xA8	Setup Verifying Password
0xA9	Satrt of Setup
0xAA	Reserved for ASL(See ASL Status Codes selection below)
0xAB	Setup Input Wait
0xAC	Reserved for ASL(See ASL Status Codes selection below)
0xAD	Ready To Boot event
0xAE	Legacy Boot event
0xAF	Exit Boot Services event
0xB0	Runtime Set Virtual Address MAP Begin
0xB1	Runtime Set Virtual Address MAP End
0xB2	Legacy Option ROM initialization
0xB3	System Reset
0xB4	USB Hot Plug
0xB5	PCI bus Hot plug
0xB6	Clean-up of NVRAM
0xB7	Configuration Reste (reset of NVRAM settings)

0xB8~0xBF	Reserved for future AMI codes
0xC0~0xCF	OEM BDS initialization codes
ACPI ASL Checkpoints	
0x01	System is entering S1 sleeping state
0x02	System is entering S2 sleeping state
0x03	System is entering S3 sleeping state
0x04	System is entering S4 sleeping state
0x05	System is entering S5 sleeping state
0x10	System is waking up from the S1 sleep state
0x20	System is waking up from the S2 sleep state
0x30	System is waking up from the S3 sleep state
0x40	System is waking up from the S4 sleep state
0xAC	System has transitioned into ACPI mode. Interrupt controller is in PIC mode.
0xAA	System has transitioned into ACPI mode. Interrupt controller is in APIC mode.

Boot loader Error codes

Post Code	Description
0x00	General - Success
0x01	Generic Error Code
0x02	Generic Memory Error
0x03	Buffer Overflow
0x04	Invalid Parameter(s)
0x05	Invalid Data Length
0x06	Data Alignment Error
0x07	Null Pointer Error
0x08	Unsupported Function
0x09	Invalid Service ID
0x0A	Invalid Address
0x0B	Out of Resource Error
0x0C	Timeout
0x0D	data abort exception
0x0E	prefetch abort exception
0x0F	Out of Boundary Condition Reached
0x10	Data corruption
0x11	Invalid command
0x12	The package type provided by BR is incorrect
0x13	Failed to retrieve FW header during FW validation
0x14	Key size not supported
0x15	Agesa0 verification error
0x16	SMU FW verification error
0x17	OEM SINGING KEY verification error
0x18	Generic FW Validation error
0x19	RSA operation fail - bootloader
0x1A	CCP Passthrough operation failed - internal status
0x1B	AES operation fail

0x1C	CCP state save failed
0x1D	CCP state restore failed
0x1E	SHA256/384 operation fail - internal status
0x1F	ZLib Decompression operation fail
0x20	HMAC-SHA256/384 operation fail - internal status
0x21	Booted from boot source not recognized by PSP
0x22	PSP directory entry not found
0x23	PSP failed to set the write enable latch
0x24	PSP timed out because spirom took too long
0x25	Cannot find BIOS directory
0x26	SpiRom is not valid
0x27	slave die has different security state from master
0x28	SMI interface init failure
0x29	SMI interface generic error
0x2A	invalid die ID executes MCM related function
0x2B	invalid MCM configuration table read from bootrom
0x2C	Valid boot mode wasn't detected
0x2D	NVStorage init failure
0x2E	NVStorage generic error
0x2F	MCM 'error' to indicate slave has more data to send
0x30	MCM error if data size exceeds 32B
0x31	Invalid client id for SVC MCM call
0x32	MCM slave status register contains bad bits
0x33	MCM call was made in a single die environment
0x34	PSP secure mapped to invalid segment (should be 0x400_0000)
0x35	No physical x86 cores were found on die
0x36	Insufficient space for secure OS (range of free SRAM to SVC stack base)
0x37	SYSHUB mapping memory target type is not supported
0x38	Attempt to unmap permanently mapped TLB to PSP secure region
0x39	Unable to map an SMN address to AXI space
0x3A	Unable to map a SYSHUB address to AXI space
0x3B	The count of CCXs or cores provided by bootrom is not consistent
0x3C	Uncompressed image size doesn't match value in compressed header
0x3D	Compressed option used in case where not supported
0x3E	Fuse info on all dies don't match
0x3F	PSP sent message to SMU; SMU reported an error
0x40	Function RunPostX86ReleaseUnitTests failed in memcmp()
0x41	Interface between PSP to SMU not available.
0x42	Timer wait parameter too large
0x43	Test harness module reported an error
0x44	x86 wrote C2PMSG_0 interrupting PSP, but the command has an invalid format
0x45	Failed to read from SPI the Bios Directory or Bios Combo Directory
0x46	Failed to find FW entry in SPL Table
0x47	Failed to read the combo bios header
0x48	SPL version missmatch
0x49	Error in Validate and Loading AGESA APOB SVC call

0x4A	Correct fuse bits for DIAG_BL loading not set
0x4B	The UmcProgramKeys() function was not called by AGESA
0x4C	Unconditional Unlock based on serial numbers failure
0x4D	Syshub register programming mismatch during readback
0x4E	Family ID in MP0_SFUSE_SEC[7:3] not correct
0x4F	An operation was invoked that can only be performed by the GM
0x50	Failed to acquire host controller semaphore to claim ownership of SMB
0x51	Timed out waiting for host to complete pending transactions
0x52	Timed out waiting for slave to complete pending transactions
0x53	Unable to kill current transaction on host, to force idle
0x54	One of: Illegal command, Unclaimed cycle, or Host time out
0x55	An smbus transaction collision detected, operation restarted
0x56	Transaction failed to be started or processed by host, or not completed
0x57	An unsolicited smbus interrupt was received
0x58	An attempt to send an unsupported PSP-SMU message was made
0x59	An error/data corruption detected on response from SMU for sent msg
0x5A	MCM Steady-state unit test failed
0x5B	S3 Enter failed
0x5C	AGESA BL did not set PSP SMU reserved addresses via SVC call
0x5D	Reserved PSP/SMU memory region is invalid
0x5E	CcxSecBisiEn not set in fuse RAM
0x5F	Received an unexpected result
0x60	VMG Storage Init failed
0x61	failure in mbedTLS user app
0x62	An error occured whilst attempting to SMN map a fuse register
0x63	Fuse burn sequence/operation failed due to internal SOC error
0x64	Fuse sense operation timed out
0x65	Fuse burn sequence/operation timed out waiting for burn done
0x66	The PMU FW Public key certificate loading or authentication fails
0x67	This PSP FW was revoked
0x68	The platform model/vendor id fuse is not matching the BIOS public key token
0x69	The BIOS OEM public key of the BIOS was revoked for this platform
0x6A	PSP level 2 directory not match expected value.
0x6B	BIOS level 2 directory not match expected value.
0x6C	Reset image not found
0x6D	Generic error indicating the CCP HAL initialization failed
0x6E	failure to copy NVRAM to DRAM.
0x6F	Invalid key usage flag
0x70	Unexpected fuse set
0x71	RSMU signaled a security violation
0x72	Error programming the WAFL PCS registers
0x73	Error setting wafl PCS threshold value
0x74	Error loading OEM trustlets
0x75	Recovery mode accross all dies is not sync'd

0x76	Uncorrectable WAFL error detected
0x77	Fatal MP1 error detected
0x78	Bootloader failed to find OEM signature
0x79	Error copying BIOS to DRAM
0x7A	Error validating BIOS image signature
0x7B	OEM Key validation failed
0x7C	Platform Vendor ID and/or Model ID binding violation
0x7D	Bootloader detects BIOS request boot from SPI-ROM, which is unsupported for PSB.
0x7E	Requested fuse is already blown, reblow will cause ASIC malfunction
0x7F	Error with actual fusing operation
0x80	(Local Master PSP on P1 socket) Error reading fuse info
0x81	(Local Master PSP on P1 socket) Platform Vendor ID and/or Model ID binding violation
0x82	(Local Master PSP on P1 socket) Requested fuse is already blown, reblow will cause ASIC malfunction
0x83	(Local Master PSP on P1 socket) Error with actual fusing operation
0x84	SEV FW Rollback attempt is detected
0x85	SEV download FW command fail to broadcase and clear the IsInSRAM field on slave dies
0x86	Agesa error injection failure
0x87	Uncorrectable TWIX error detected
0x88	Error programming the TWIX PCS registers
0x89	Error setting TWIX PCS threshold value
0x8A	SW CCP queue is full, cannot add more entries
0x8B	CCP command description syntax error detected from input
0x8C	Return value stating that the command has not yet be scheduled
0x8D	The command is scheduled and being worked on
0x8E	The DXIO PHY SRAM Public key certificate loading or authentication fails
0x8F	fTPM binary size exceeds limit allocated in Private DRAM, need to increase the limit
0x90	The TWIX link for a particular CCD is not trained Fatal error
0x91	Security check failed (not all dies are in same security state)
0x92	FW type mismatch between the requested FW type and the FW type embedded in the FW binary header
0x93	SVC call input parameter address violation
0x94	Firmware Compatibility Level mismatch
0x95	Bad status returned by I2CKnollCheck
0x96	NACK to general call (no device on Knoll I2C bus)
0x97	Null pointer passed to I2CKnollCheck
0x98	Invalid device-ID found during Knoll authentication
0x99	Error during Knoll/Prom key derivation
0x9A	Null pointer passed to Crypto function
0x9B	Error in checksum from wrapped Knoll/Prom keys
0x9C	Knoll returned an invalid response to a command
0x9D	Bootloader failed in Knoll Send Command function
0x9E	No Knoll device found by verifying MAC
0x9F	The maximum allowable error post code

BL_TRACECODE	
0xA0	Bootloader successfully entered C Main
0xA1	Master initialized C2P / slave waited for master to init C2P
0xA2	HMAC key successfully derived
0xA3	Master got Boot Mode and sent boot mode to all slaves
0xA4	SpiRom successfully initialized
0xA5	BIOS Directory successfully read from SPI to SRAM
0xA6	Early unlock check
0xA7	Inline Aes key successfully derived
0xA8	Inline-AES key programming is done
0xA9	Inline-AES key wrapper derivation is done
0xAA	Bootloader successfully loaded HW IP configuration values
0xAB	Bootloader successfully programmed MBAT table
0xAC	Bootloader successfully loaded SMU FW
0xAE	User mode test Uapp completed successfully
0xAF	Bootloader loaded Agesa0 from SpiRom
0xB0	AGESA phase has completed
0xB1	RunPostDramTrainingTests() completed successfully
0xB2	SMU FW Successfully loaded to SMU Secure DRAM
0xB3	Sent all required boot time messages to SMU
0xB4	Validated and ran Security Gasket binary
0xB5	UMC Keys generated and programmed
0xB6	Inline AES key wrapper stored in DRAM
0xB7	Completed FW Validation step
0xB8	Completed FW Validation step
0xB9	BIOS copy from SPI to DRAM complete
0xBA	Completed FW Validation step
0xBB	BIOS load process fully complete
0xBC	Bootloader successfully release x86
0xBD	Early Secure Debug completed
0xBE	GetFWVersion command received from BIOS is completed
0xBF	SMIInfo command received from BIOS is completed
0xC0	Successfully entered WarmBootResume()
0xC1	Successfully copied SecureOS image to SRAM
0xC2	Successfully copied trustlets to PSP Secure Memory
0xC3	About to jump to Secure OS (SBL about to copy and jump)
0xC4	Successfully restored CCP and UMC state on S3 resume
0xC5	PSP SRAM HMAC validated by Mini BL
0xC6	About to jump to <t-base in Mini BL
0xC7	VMG ECDH unit test started
0xC8	VMG ECDH unit test passed
0xC9	VMG ECC CDH primitive unit test started
0xCA	VMG ECC CDH primitive unit test passed
0xCB	VMG SP800-108 KDF-CTR HMAC unit test starte
0xCC	VMG SP800-108 KDF-CTR HMAC unit test passed
0xCD	VMG LAUNCH_* test started
0xCE	VMG LAUNCH_* test passed
0xCF	MP1 has been taken out of reset, and executing SMUFW

0xD0	PSP and SMU Reserved Addresses correct
0xD1	Reached Naples steady-state WFI loop
0xD2	Knoll device successfully initialized
0xD3	32-byte RandOut successfully returned from Knoll
0xD4	32-byte MAC successfully received from Knoll.
0xD5	Knoll device verified successfully
0xD6	CNLI Keys generated and programmed
0xD7	Enter recovery mode due to trustlet validation fail.
0xD8	Enter recovery mode due to OS validation fail.
0xD9	Enter recovery mode due to OEM public key not found.
0xDA	Enter recovery mode with header corruption
0xDB	We should not treat this error as blocking
0xDC	When same fw image type is already loaded in SRAM
0xE0	Unlock return
0xE2	Token exipration reset triggered
0xE3	Completed DXIO PHY SRAM FW key Validation step
0xE4	MP1 firmware load to SRAM success
0xE5	Bootloader read the MP1 SRAM successfully
0xE6	Bootloader successfully reset MP1
0xE7	DF init successfully done (in absence of AGESA)
0xE8	UMC init successfully done (in absence of AGESA)
0xE9	LX6 Boot ROM code ready
0xEA	Bootloader successfully asserted LX6 reset
0xEB	LX6 load to SRAM success
0xEC	Bootloader successfully set LX6 reset vector to SRAM
0xED	Bootloader successfully de-asserted LX6 reset
0xEE	LX6 firmware is running and ready
0xEF	Loading of S3 image done successfully
0xF0	Bootloader successfully verify signed image using 4K/2K key
0xF1	Bootloader identified as running on SP32P or multi-socket boot
0xF2	Security Policy check successful (only in secure boot)
0xF3	Bootloader successfully loaded SS3
0xF4	Bootloader successfully load fTPM Driver
0xF5	Bootloader successfully loaded sys_drv
0xF6	Bootloader successfully loaded secure OS
0xF7	Bootloader about to transfer control to secureOS
0xFC	Fatal error reported by another socket
0xFD	MP0 Data abort exception happened - PSP in debug unlockable state
0xFE	Uncorrectable error happened - PSP in debug unlockable state
0xFF	Bootloader sequence finished
BL_SUCCESS_ BOOT_DONE	This is the Max Value for PostCode
0x7FFFFFFF	[UNUSED] Added to force this enum to 32-bits

Chapter 5. Technical Support

www.aicipc.com

Taiwan, Global Headquarters

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

Shanghai, China

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

Moscow, Russia

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

North California, United States

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

South California, United States

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

New Jersey, United States

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

Houten, The Netherlands

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

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