Capella

Server Motherboard
User's Manual

UM_Capella_v1.4_081225

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 31
3.7 Internal LED 36
Chapter 4. BIOS Configuration Settings 37
4.1 Navigation Keys 37
4.2 BIOS Setup 38
4.2.1 Menu 38
4.2.2 Startup 38
4.3 Main 39
4.3.1 Main 39
4.4 Advanced 40
4.4.1 Trusted Computing 40
4.4.2 PSP Firmware Versions 41
4.4.3 ACPI Settings 41
4.4.4 Redfish Host Interface Settings 41
4.4.5 AMD CBS 42
4.4.6 AST2600 Super IO Configuration 59
4.4.7 Serial Port Console Redirection 59
4.4.8 CPU Configuration 60
4.4.9 Debug Port Table Configuration 60
4.4.10 SIO Common Configuration 60
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 AMD Mem Configuration Status 62
4.4.17 Tls Auth Configuration 63
4.4.18 RAM Disk Configuration 63
4.4.19 AMD PBS 63
4.4.20 Driver Health 64
4.5 Chipset 65
4.5.1 PCIe Link Training Type 65
4.5.2 PCIe Compliance Mode 65
4.5.3 South Bridge 66
4.5.4 North Bridge 67
4.6 Security 68
4.7 Boot 69
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 FRB-2 Timer 72
4.9.4 FRB-2 Timer timeout 72
4.9.5 FRB-2 Timer Policy 73
4.9.6 OS Watchdog Timer 73
4.9.7 Power Control Policy 73
4.9.8 System Event Log 73
4.9.9 BMC network configurtion 73
4.9.10 View System Event Log 73
4.10 BIOS Post Code 74
Chapter 5. Technical Support 106

Document Release History

Release Date	Version	Update Content
August 2023	1	User's Manual release to public.
November 2023	1.1	Add new section: 4.10 BIOS Post Code
December 2024	1.2	Correct jumper label typo.
January 2025	1.3	Correct typo of I/O view.
August 2025	1.4	Update specifictaion (M.2).

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

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

Preface

Copyright

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

Trademarks

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

Changes

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

Warning

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

Disclaimer

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

Instruction Symbols

Special attention should be given to the instruction symbols below.

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

Safety Instructions

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

Carefully read the safety instructions below before using this product.

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

About This Manual

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

Chapter 1 Product Features
This chapter delivers the overall layout of the product, including the fundamental components on the motherboard, design specifications, and noteworthy features. Scutum is an ideal server grade motherboard that is specifically designed to accommodate diverse enterprises for managing heavy workloads, databases, nearline applications, and cloud deployments. This product supports the dual processor with Socket P+(LGA-4189) socket type with a memory support of 8 channel DDR4 RDIMM/LRDIMM/Barlow Pass with EEC up to 3200/2933 MHz.

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

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

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

Chapter 5 BMC Configuration Settings
This chapter illustrates the diverse functions of IPMI BMC, including the details on logging into the web page and assorted definitions. These descriptions are helpful in configuring various functions through Web GUI without entering the BIOS setup. For more information of BMC configurations, please refer to IPMI BMC (Aspeed AST2500) User's Manual for a more detailed description.

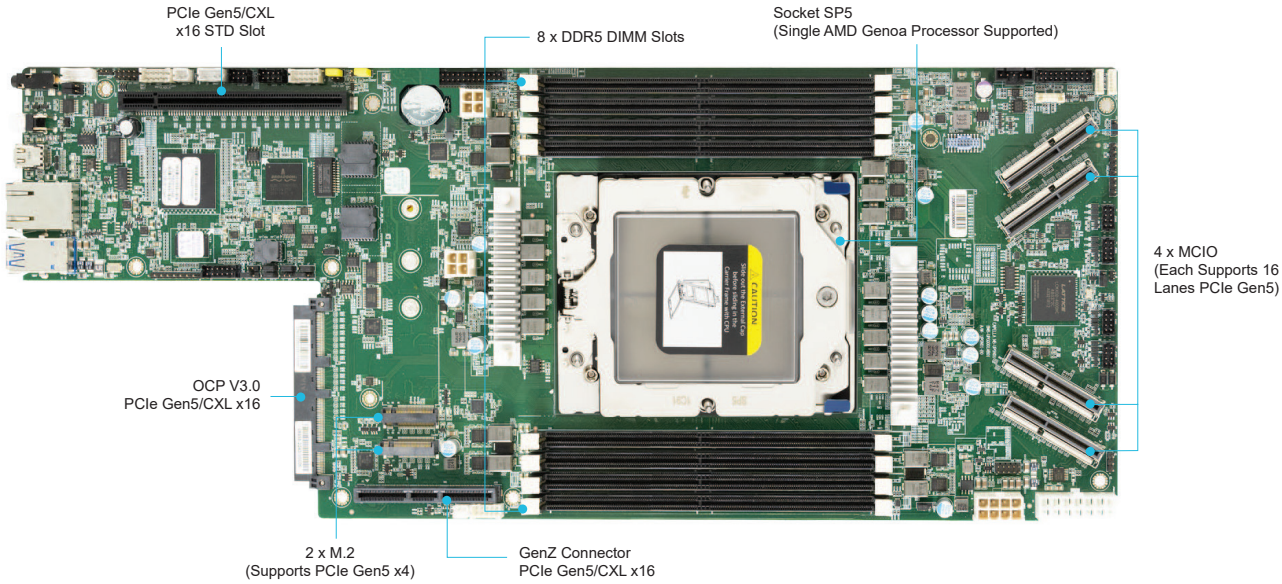
Chapter 6 Technical Support
For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: https://www.aicipc.com/en/index.
It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

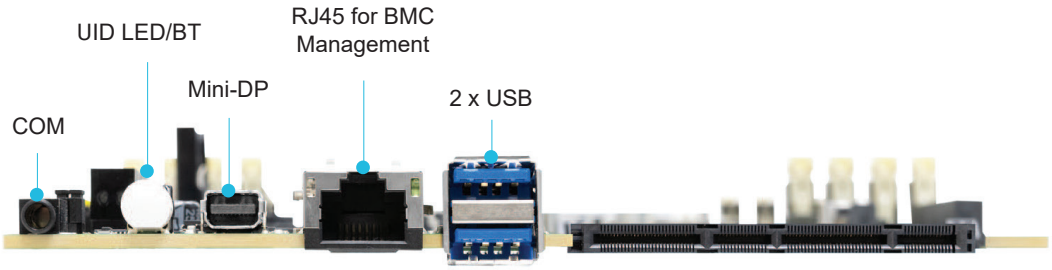
This section describes the hardware specifications and features of the Scutum motherboard. The fundamental components of the Scutum severboard are provided below.

1.1 Component

Capella Serverboard



I/O View



Dimensions
mm : 431.8 x 172.7
inches : 17 x 6.8

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

1.2 Specifications

System	Processor Support	Single AMD EPYC™ 9000-series processor
	CPU TDP	400W
	Socket Type	Socket SP5
	System Memory	• DDR5 6000(Turin only)/4800/3600MHz RDIMM • Total 8 memory slots • Supports up to 3TB
	Expansion Slots	• Total support 120 lanes of PCIe Gen5 - 4 x MCIO x16 (PCIe Gen5) - 1 x PCIe Gen5/CXL X16 slot - 1 x OCP Mezzanine V3.0 supports PCIe Gen5/CXL X16 - 1 x GenZ PCIe Gen5/CXL X16 slot - 2 x NGFF (M.2) M-Key (2280) support PCIe Gen5/CXL X4
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	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 Ethernet for BMC dedicated management port • Broadcom BCM5720 GbE for BMC shared NIC and data transfer by onboard header (NCSI shared NIC - reserved for OCP & BCM5720 by jumper setting)
	Graphics	Aspeed AST2600 Advanced PCIe Graphics & Remote Management Processor • PCIe VGA/2D Controller • 1920x1200@60Hz 32bpp
Input/Output	LAN	1 x GbE RJ45 dedicated to BMC management
	USB	2 x USB3.2 Gen1 (5Gbps) double-stack Type-A connectors
	Video Output	1 x Mini-DP
	Serial Port	• 1 x external COM (by Audio Jack) • 1 x internal COM1 header + rear IO COM by phone jack + LCM header
	Others	• 1 x external UID/switch button • 1 x TPM 2.0 onboard

1.3 Feature

The Capella server board offers the latest AMD EPYC™ SoC technology which can support the highest core count in an x86-architecture with EPYC™ 9000-series processor, more main memory capacity and bandwidth with greater efficiency and greatest I/O density.

Capella has 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. By offering the parallelism to speed high performance computing environments, machine learning and predictive analysis benefit from the capability to process more data in memory and to accelerate computation with more direct GPU connectivity.

- Supports AMD EPYC™ 9000-series processor Genoa based on the AMD "Zen4" microarchitecture for highest server performance
- Supports 8 DDR5 DIMM slots for maximum memory performance
- Supports one OCP Mezzanine V3.0 up to PCI Express Gen5 x16 extension
- Supports four MCIO x16 total 64 PCI Express Gen5 lanes
- Onboard Baseboard Management Controller for system management and IPMI control
- Embedded components for 5+ year long life
- Rackmount Technology Extension (RTX) form factor utilizes full internal chassis volume for optimum I/O configurations
- 2 Gen5 capable x4 M.2 slots

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

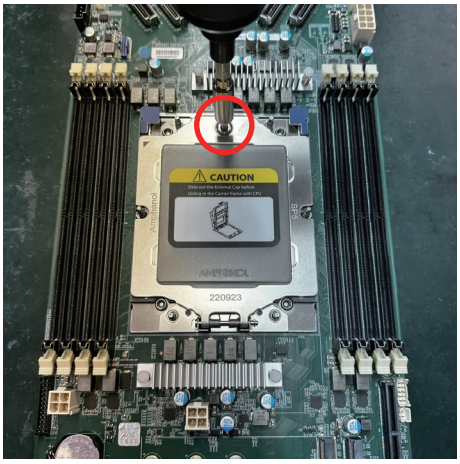
CAUTION
The pins of the processor socket are vulnerable and easily susceptible to damage if fingers or any foreign objects are pressed against them. Please keep the socket protective cover on when the processor is not installed.

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

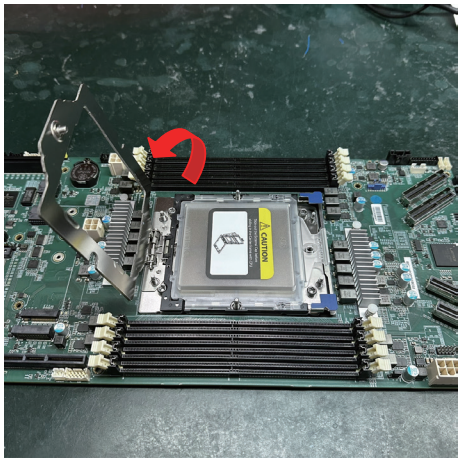
Assembly of Package and Heatsink
Procesures:

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

❶

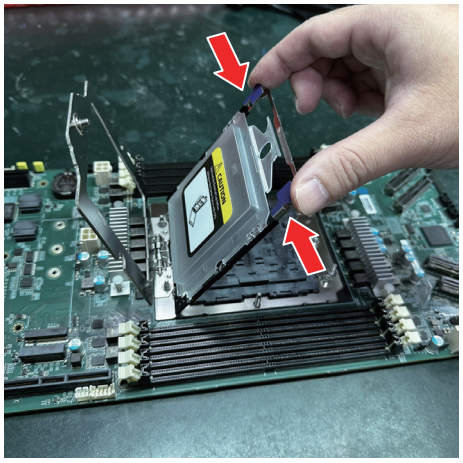


❷

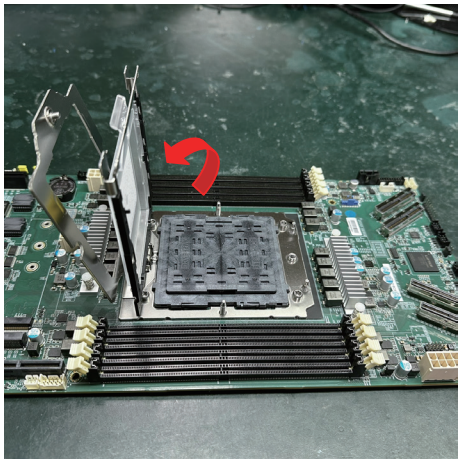


Step 2: Bounce the Rail Frame
① Use your the index finger the both hands placed on Rail Frame both sides of the metal handle.
② Then rotate Rail frame to fully open position.

❶



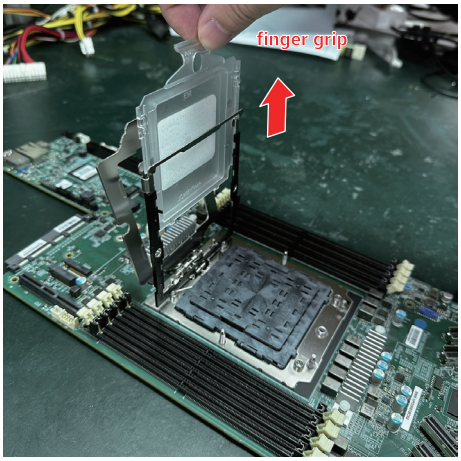
❷



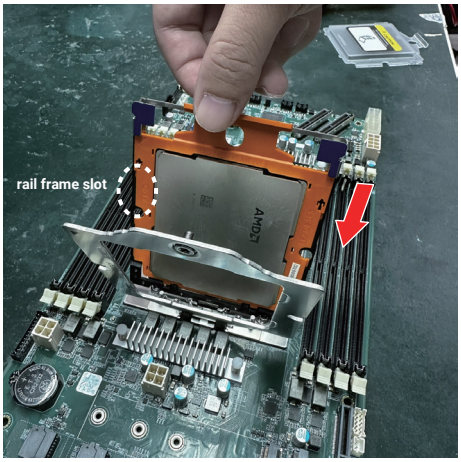
This information is provided for professional technicians only.

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

❶



❷

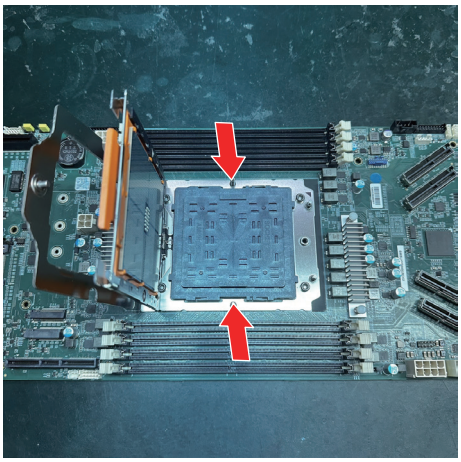


- Do not touch the package pad.
- Carrier Frame should slide into Rail Frame slot when insert the Package.

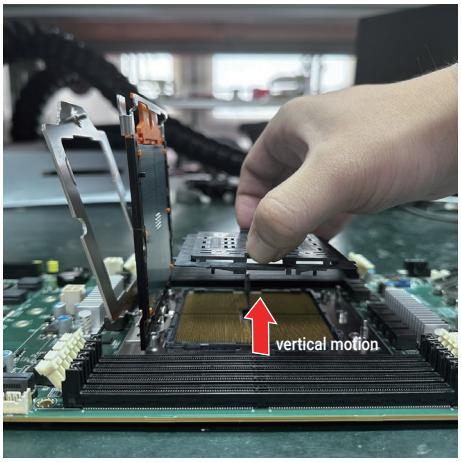
CAUTION
Be sure Carrier Frame with Package may be drop off if Frame did not fix by Rail Frame slot. Make sure carrier frame will slightly “click” with rail frame. Carrier Frame drop off will damage socket cap & contact.

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



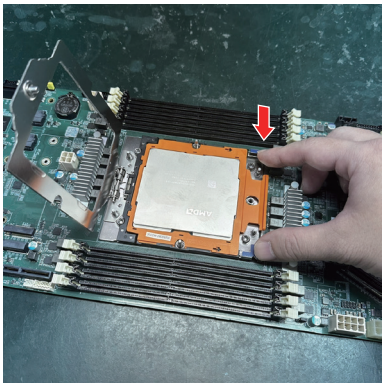
Step 5: Assembly Package and Heatsink Operation Guide

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

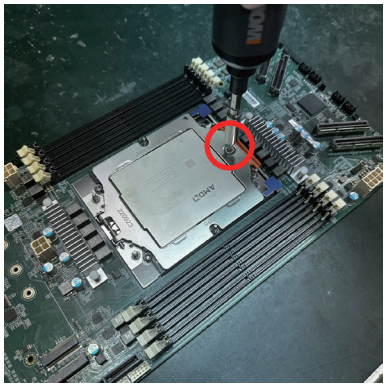
② Press Retention Frame and then tighten the captive screw.

③ Final status of whole assembly process.

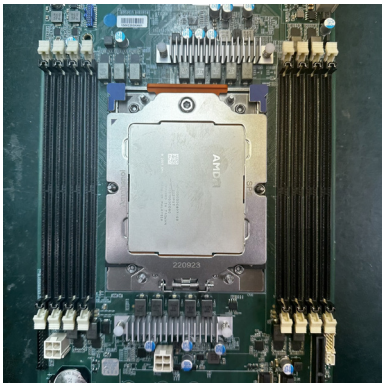
❶



❷



❸



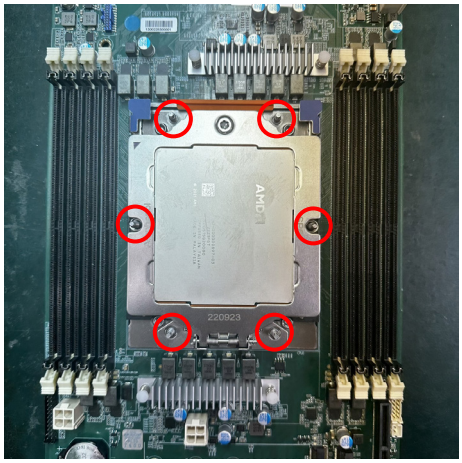
- Be care that Carrier Frame drop off with abnormal operation, Socket contact will been damaged.
- Torque : 12.5-15kgf cm

Step 6: Loading the Heatsink

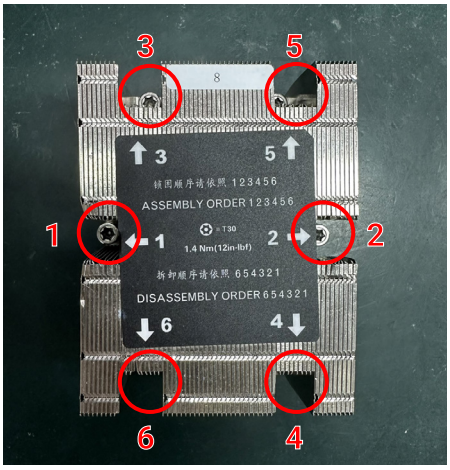
① Align the Heatsink with 4 screws on Stiffener Frame and 2 screws on Back Plate.

② Use T20 6 Lobe driver tighten 6 Heatsink nuts in sequence as 1 to 6.

❶



❷



- Torque : 12.5-15kgf cm
- When tightening 6 Heatsink nuts, we need to pre-tighten the nuts instead of completely tightening them, and we need to balance the Heatsink as much as possible.

2.2 System Memory

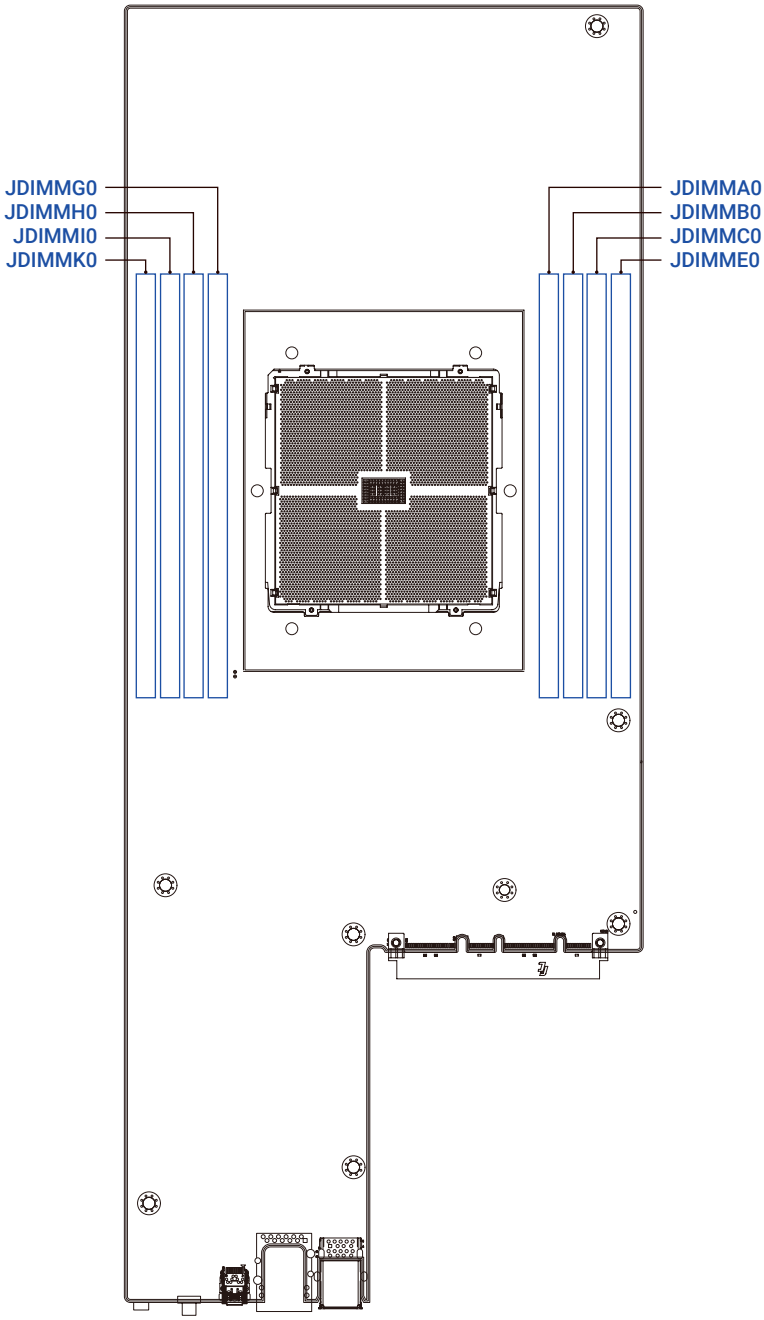
2.2.1 Placement

The DIMMs are displayed on the Capella board as JDIMME0/JDIMMC0/JDIMMB0/JDIMMA0/JDIMMG0/JDIMMH0/JDIMMI0/JDIMMK0

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.

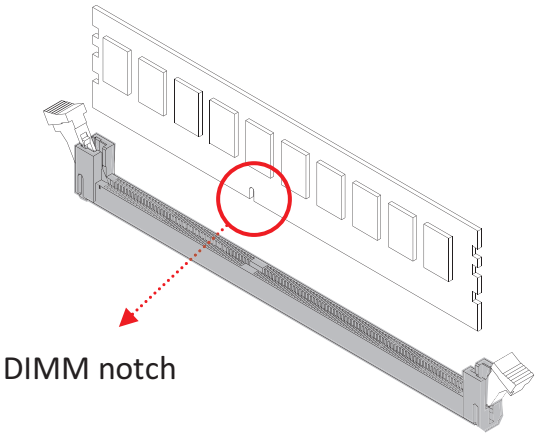
CPU Configuration

Placement		DIMM Number				
		1	2	4	6	8
CPU0	JDIMME0					#
	JDIMMC0			#	#	#
	JDIMMB0				#	#
	JDIMMA0	#	#	#	#	#
	JDIMMG0		#	#	#	#
	JDIMMH0				#	#
	JDIMMI0			#	#	#
	JDIMMK0					#

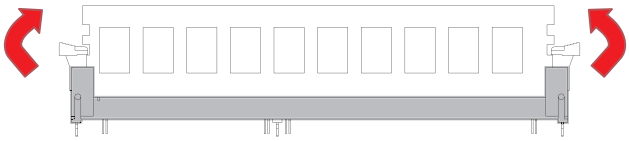
2.2.3 Installation

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.



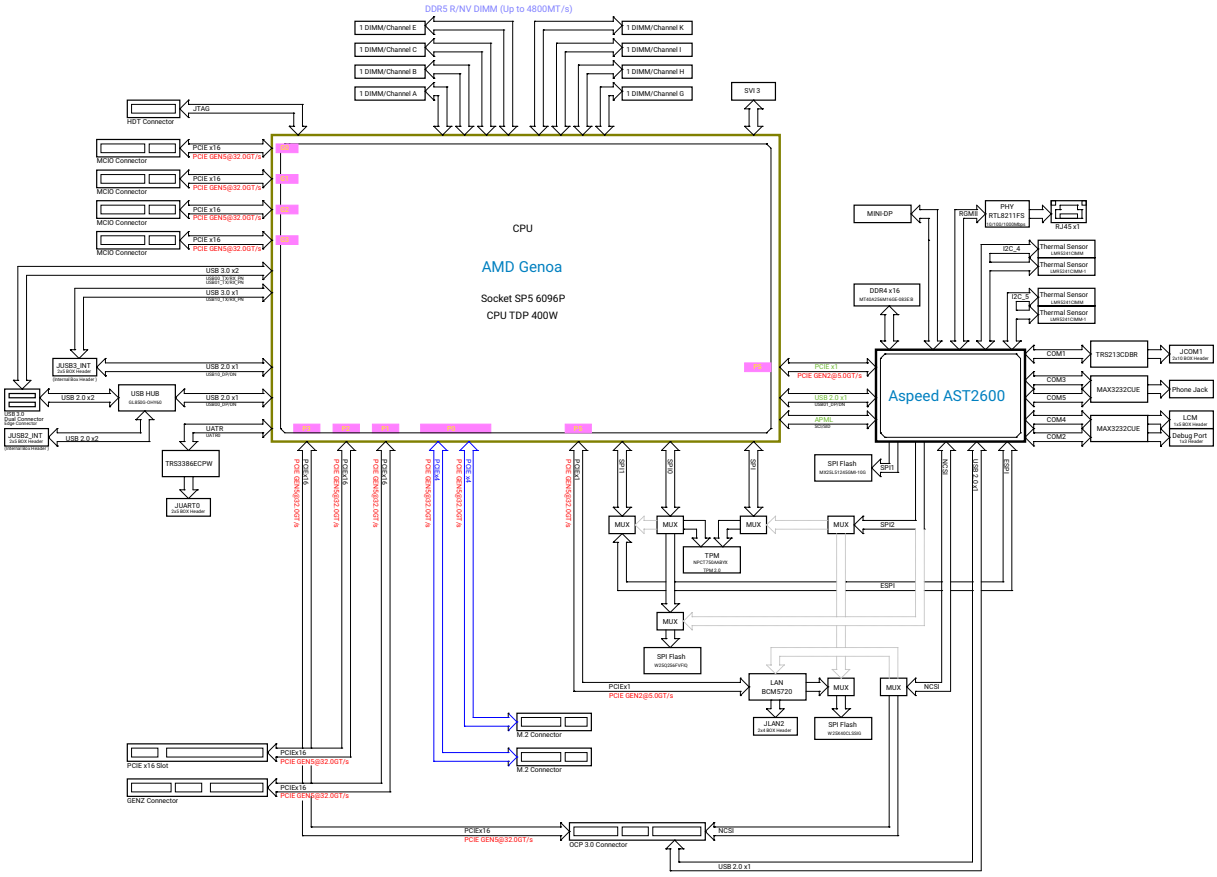
Step 3 Close the retaining clip to complete installation.



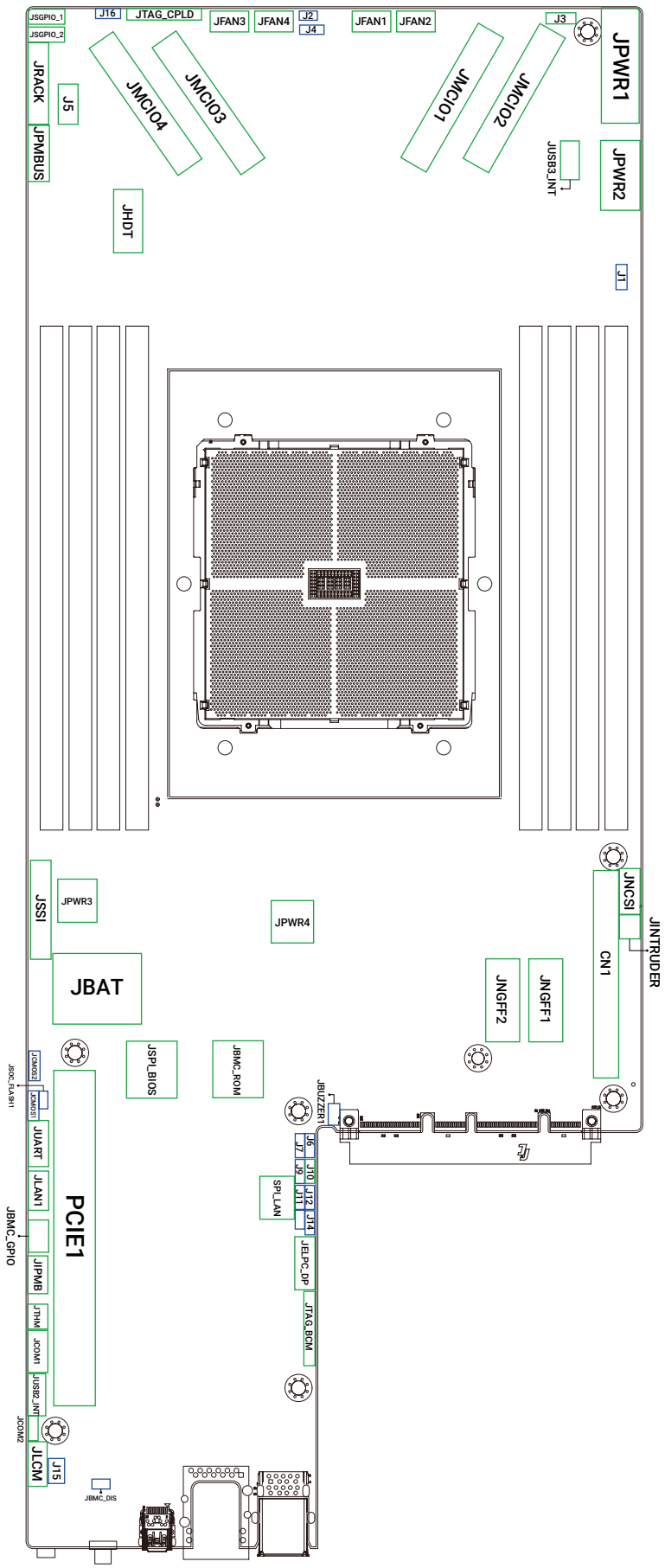
Chapter 3. Motherboard Settings

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

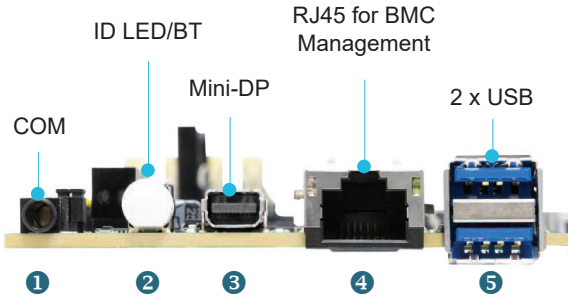
Function	Description	Comments
COM	Phone Jack	JCONSOLE
MINI DP	Mini Display Port	JMINI_DP1
USB3.0 x2	USB3.0 Type A	JUSB1
Ethernet x1	RJ45	JRJ45: 10/100/1000M PHYCEIVER (RTL8211FS)

Internal Connectors Summary

Function	Description	Comments
Power Supply	2 x 7 Pin ATX Header	JPWR1: 12V、5V、3.3V、5VSB (6A per pin)
Power Supply	2 x 4 Pin ATX Header	JPWR2: 12V
Power Supply	2 x 2 Pin ATX Header	JPWR3、JPWR4: 12V
Front Panel	2 x 12 Pin 2.54mm Box Header	JSSI
CPU UART0	2 x 5 Pin 2.0mm Box Header	JUART
Super IO1	2 x 5 Pin 2.0mm Box Header	JCOM1
LCM	1 x 5 Pin 2.0mm Header	JLCM
Front USB3.0	2 x 5 Pin 2.0mm Header	JUSB2_INT
Front USB2.0	2 x 5 Pin 2.0mm Header	JUSB3_INT
NGFF(Key-M)	67 Pin 0.5mm Header	JNGFF1、JNGFF2
HDT CONN	Samtec ASP-137098-05	JHDT
DIMM Sockets	288 Pin DDR5 DIMM	JEDEC Specified DDR5 Connector
eSPI Debug Port	2 x 6 Pin 2.0mm Box Header	JELPC_DP
Super IO2	1 x 3 Pin 2.0mm Header	JCOM2
BMC GPIO	2 x 3 Pin 2.0mm Box Header	JBMC_GPIO
SGPIO	1 x 6 Pin 1.25mm Box Header	JSGPIO_1、JSGPIO_2
FAN	2 x 4 Pin 2.0mm Box Header	JFAN1、JFAN2、JFAN3、JFAN4
CPU Clear CMOS	1 x 3 Pin 2.54mm Header	JCMOS1
BMC Clear CMOS	1 x 3 Pin 2.54mm Header	JCMOS2
BMC I2C1	1 x 4 Pin 2.0mm Box Header	JIPMB
Battery Socket	3 Pin Socket	JBAT
Intruder	1 x 2 Pin 2.0mm Box Header	JINTRUDER
PMBUS	1 x 5 Pin 2.54mm Box Header	JPMBUS
BIOS SPI ROM Socket	SOIC-16 Socket	JSPI_BIOS
BMC SPI ROM Socket	SOIC-16 Socket	JBMC_ROM
BCM5720 SPI ROM Socket	SOIC-8 Socket	SPI_LAN
BMC Reset	1 x 2 Pin 2.0mm Header	JBMC_RST
BMC Disable	1 x 2 Pin 2.0mm Header	JBMC_DIS
External NCSI	2 x 5 Pin 2.0mm Box Header	JNCSI
BMC update BCM5720 & BIOS	1 x 3 Pin 2.0mm Header	J1
BMC update CPLD	1 x 2 Pin 2.0mm Header	J2
BMC update BCM5720 ROM	1 x 3 Pin 2.0mm Header	J4
BMC NCSI Select	1 x 3 Pin 2.0mm Header	J6
CPU SPI0/eSPI0 Select	1 x 3 Pin 2.0mm Header	J7

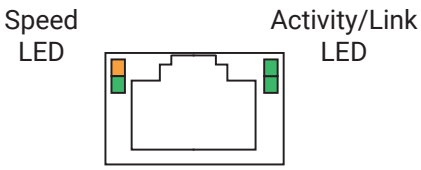
Function	Description	Comments
BIOS ROM SPI Select	1 x 3 Pin 2.0mm Header	J9
CPU SGPIO Select	1 x 3 Pin 2.0mm Header	J11
BMC NCSI Select	1 x 3 Pin 2.0mm Header	J12
DIMM I3C Select	1 x 3 Pin 2.0mm Header	J14
JCONSOLE UART Select	2 x 3 Pin 2.0mm Header	J15
CPLD JTAG	1 x 8 Pin 2.54mm Header	JTAG_CPLD
BMC JTAG	1 x 8 Pin 2.54mm Header	JTAG_BCM
External Thermal Sensor	1 x 2 Pin 2.0mm Box Header	JTHM
PCIE Hot-Plug SMB	1 x 4 pin 2.0mm Box Header	J5
VRM SMB	1 x 3 Pin 2.54mm Header	J3
RACK CONN	2 x 8 Pin 2.0mm Box Header	JRACK
BCM5720 MDI CONN	2 x 4 Pin 2.0mm Box Header	JLAN1
BCM5720 LED CONN	1 x 3 Pin 2.0mm Header	J10
CPU PCIE5.0 x16	PCIEx16 Standard Slot	PCIE1
CPU PCIE5.0 x16	OCP NIC 3.0 (SFF)	JOCP
CPU PCIE5.0 x16	GenZ	CN1
CPU PCIE5.0 x16	MCIO	JMCIO1、JMCIO2、JMCIO3、JMCIO4
BUZZER	1 x 2 Pin 2.54mm Header	JBUZZER1
SOC FLASH enable	1 x 2 Pin 2.0mm Box Header	JSOC_FLASH1
PMBUS Voltage select	1 x 3 Pin 2.0mm Header	J16

3.4 External Port



Item	Description
1	COM Phone Jack
2	ID LED/BT
3	MINI Display Port
4	BMC Management RJ45
5	USB3.0 Type A x2

BMC Management RJ45 LED Indicator

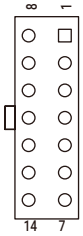


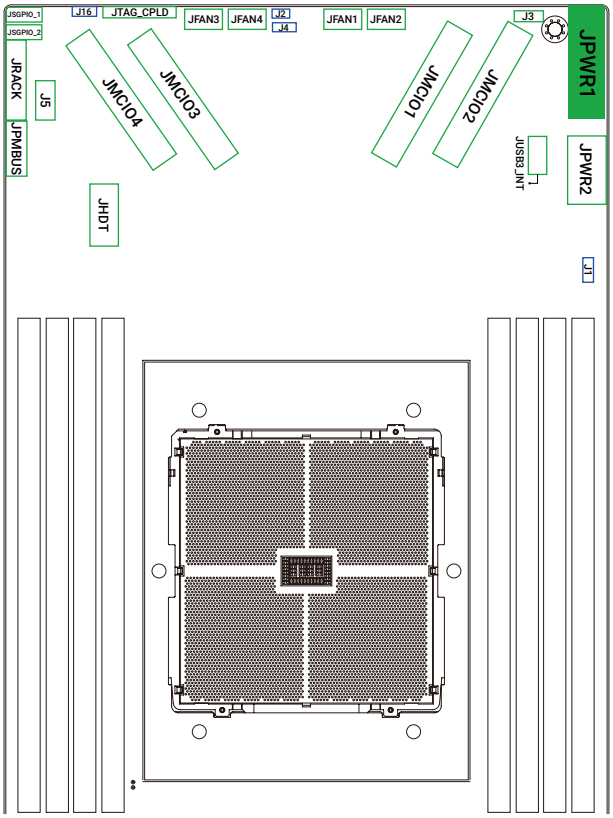
Item	Color	Behavior
Activity/Link LED	Green (blinking)	Activity detected.
	Off	Not active, LAN cable no connect.
	On	Link.
Speed LED	Off	10M bps connection or no link.
	Green	100M bps connection.
	Orange	1G bps connection.

3.5 Connector Definition

Power Supply Connector (JPWR1)
This is a 2x7-pin connector that provides the motherboard with power.

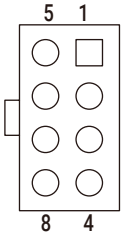
+12V_S0	8	1	GND
+12V_S0	9	2	GND
+12V_S0	10	3	GND
+12V_S0	11	4	GND
+12V_S0	12	5	GND
+5V_STBY_PSU	13	6	GND
PSU_PWROK	14	7	PSU_PSON_L

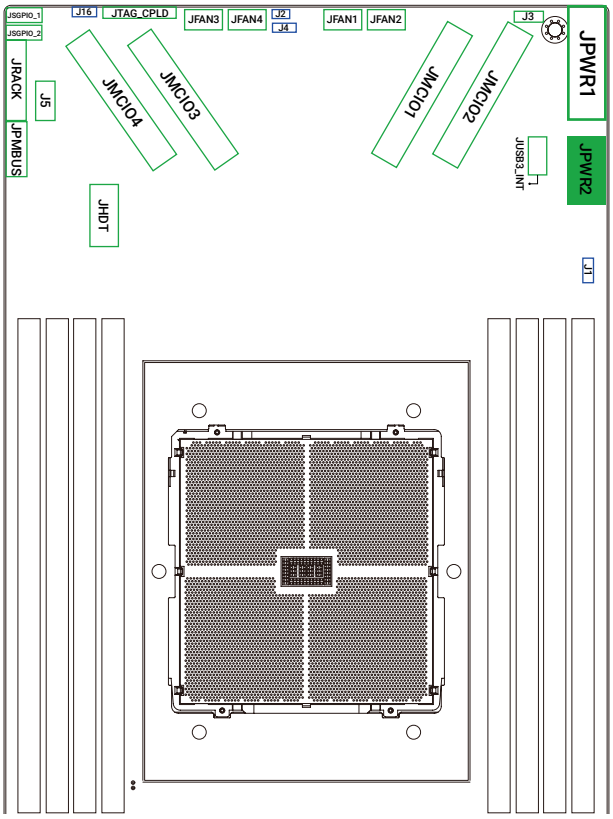




Power Supply Connector (JPWR2)
This is a 2x4-pin connector that provides the motherboard with power.

+12V_S0	5	1	GND
+12V_S0	6	2	GND
+12V_S0	7	3	GND
+12V_S0	8	4	GND

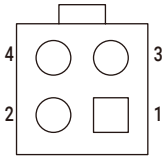


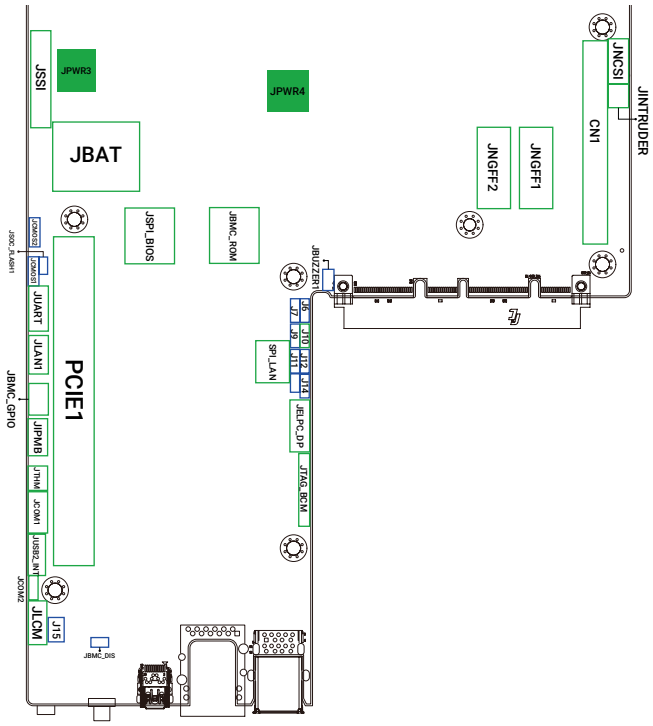


Power Supply Connector (JPWR3, JPWR4)

This is a 2x2-pin connector that provides the motherboard with power.

+12V_S0	3	1	GND
+12V_S0	4	2	GND

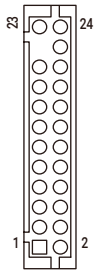


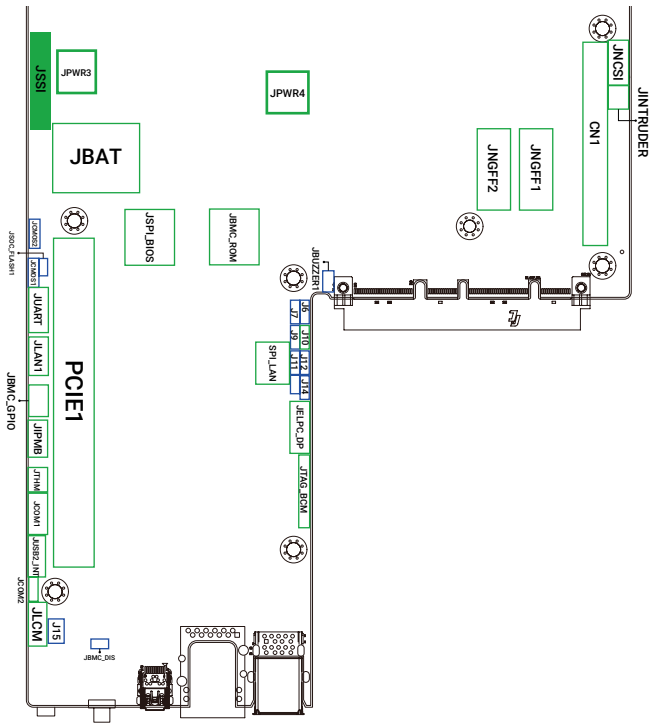


LED/Bezel Button Header (JSSI)

This connector is a 2 x 12 Pin header.

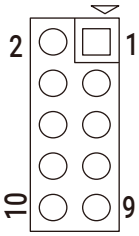
+3.3V_S0	2	1	+3.3V_DUAL
N.C.	4	3	+5V_STBY_PSU
FP_PWR_LED_L	6	5	ID_LED_OUT_N
+3.3V_S0	8	7	SYS_HEALTH#2
HDD_LED_N	10	9	SYS_HEALTH#
FP_PWR_BTN_N	12	11	LAN1_ACTLED_PWR
GND	14	13	LAN1_ACTLED_N
RST_SW	16	15	SMBUS_SDA
GND	18	17	SMBUS_SCL
BMC_ID_IN_N	20	19	CHASSIS_OPEN
+3.3V_DUAL	22	21	LAN2_ACTLED_PWR
FP_NMI_BTN_N	24	23	LAN2_ACTLED_N

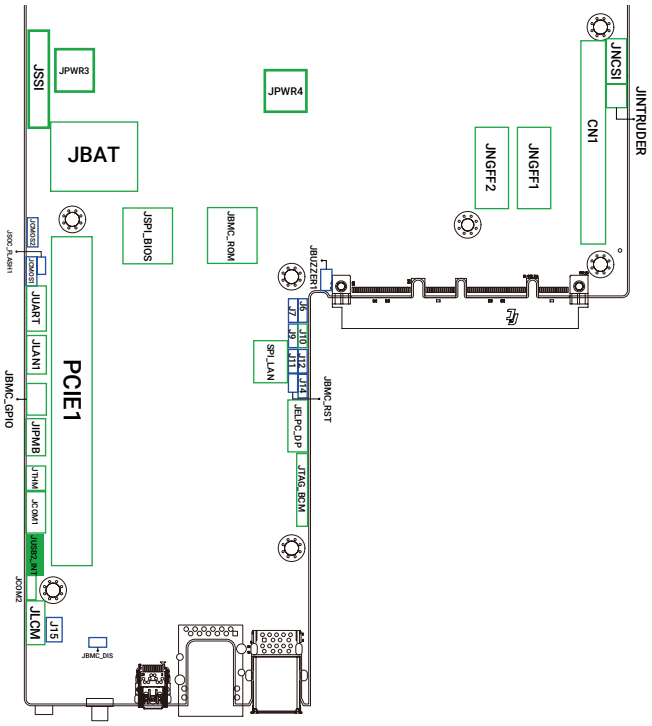




Front I/O USB2.0 Header (JUSB2_INT)
This is a 2x5-pin header that supports USB in the front panel.

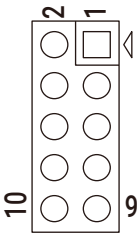
+5V_HUB2	2	1	+5V_HUB2
USB2_HUB2_DN	4	3	USB2_HUB1_DN
USB2_HUB2_DP	6	5	USB2_HUB1_DP
GND	8	7	GND
GND	10	9	KEY (no pin)

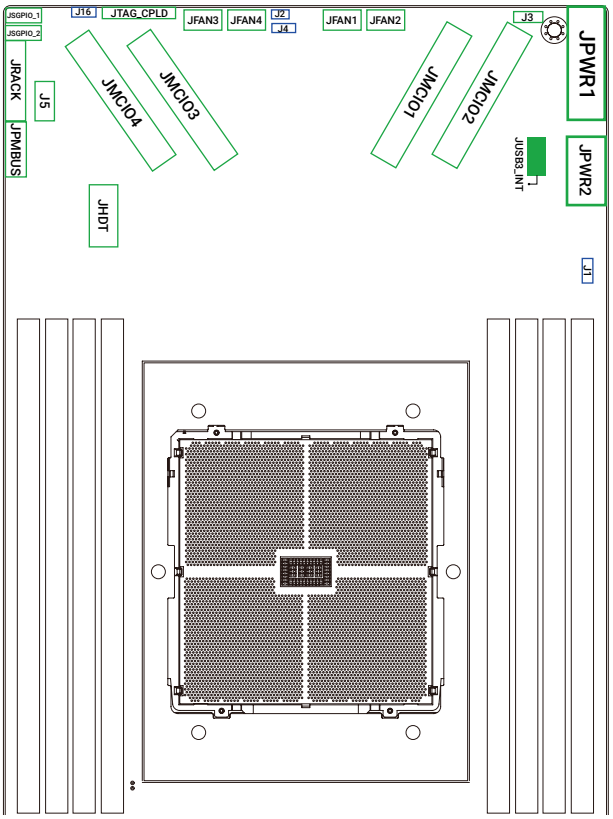




Front I/O USB3.0 Header (JUSB3_INT)
This is a 2x5-pin header that supports USB in the front panel.

P0_USB_SS_RX_L<2>	2	1	+5V_USB23
P0_USB_SS_RX_H<2>	4	3	+5V_USB23
P0_USB_SS_TX_L<2>	6	5	P0_USB_HS_L<2>
P0_USB_SS_TX_H<2>	8	7	P0_USB_HS_H<2>
GND	10	9	GND

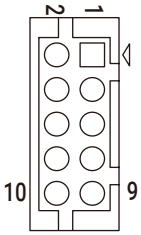


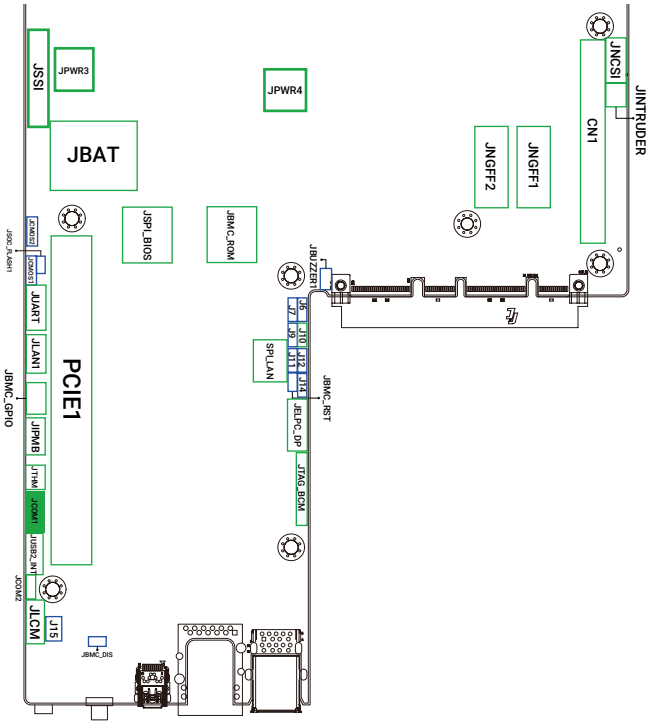


Front COM Header (JCOM1)

This 2x5-pin header is used to provide front COM functionality.

DCDB	2	1	DSRB
RXDB	4	3	RTSB
TXDB	6	5	CTSB
DTRB	8	7	RIB
GND	10	9	N.C.

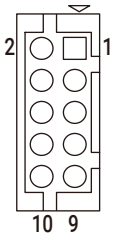


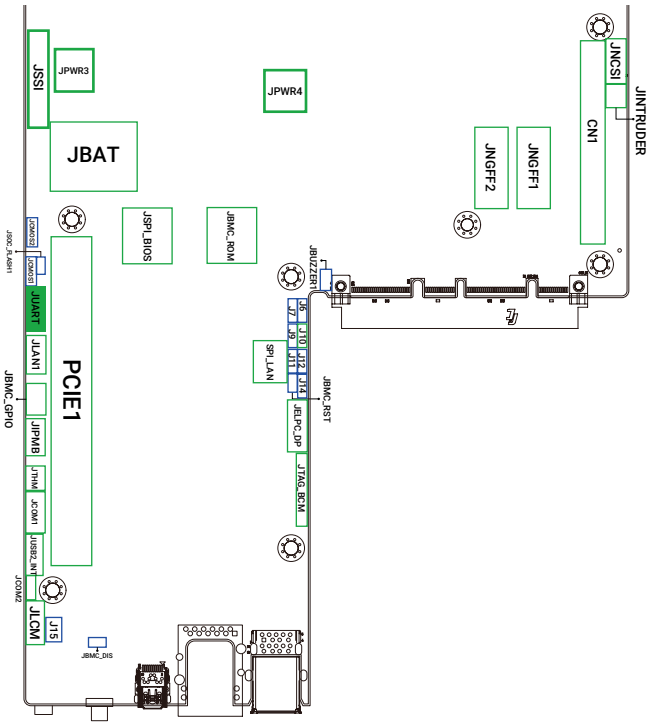


Front COM Header (JUART)

This 2x5-pin header is used to provide front COM functionality.

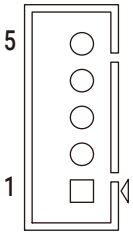
N.C.	2	1	N.C.
HDR_RXD	4	3	HDR_RTS_N
HDR_TXD	6	5	HDR_CTS_N
N.C.	8	7	N.C.
GND	10	9	N.C.

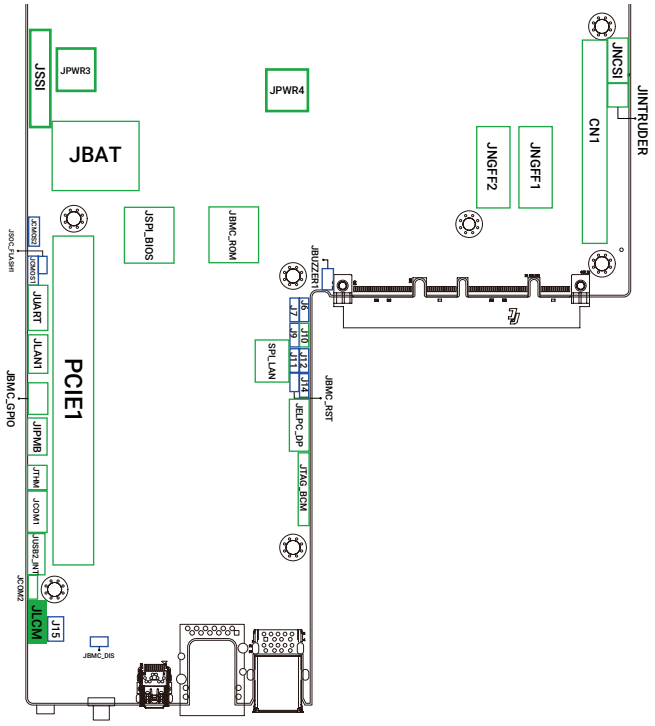




LCM header (JLCM)
This is a 5-pin connector that is used to provide LCM functionality.

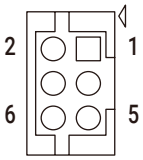
1	SW_PWR_BTN_N
2	SW_COLD_RST_N
3	RS232_TXD4
4	RS232_RXD4
5	GND

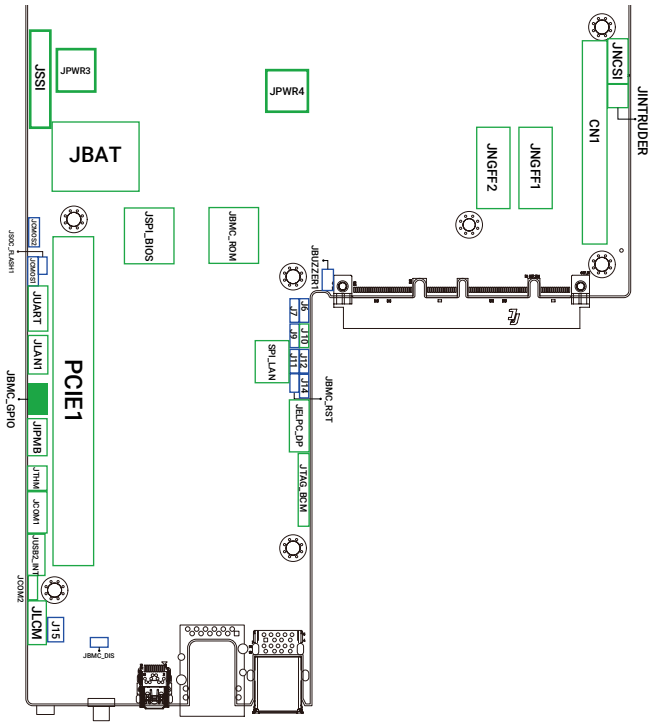




BMC GPIO header (JBMC_GPIO)
This is a 2x3-pin header that is used to provide BMC GPIO functionality.

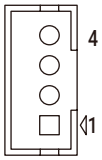
RACK_EXTRST_N	2	1	GND
BMC_GPY1	4	3	BMC_I2C_12_SDA
BMC_GPY0	6	5	BMC_I2C_12_SCL

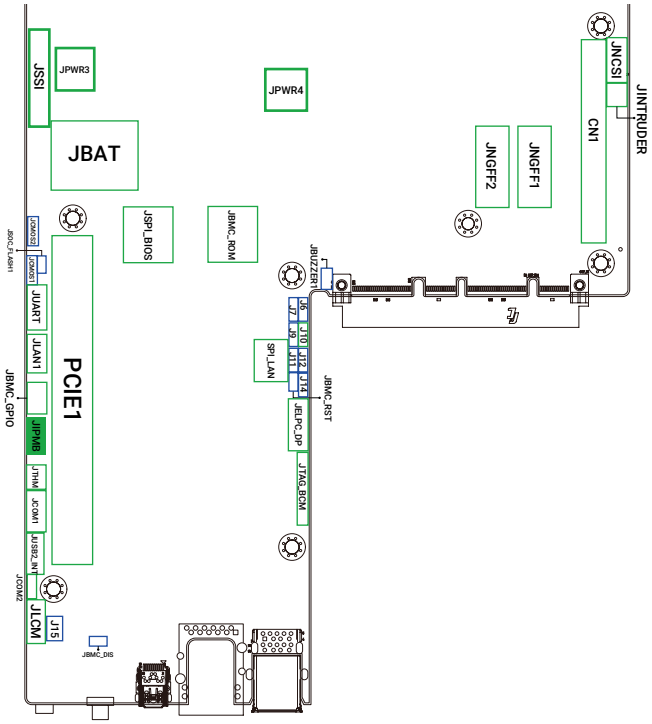




BMC I2C1 header (JIPMB)
This is a 4-pin header that is used to provide BMC I2C1 functionality.

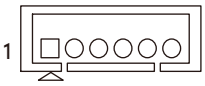
1	BMC_I2C_01_SDA
2	GND
3	BMC_I2C_01_SCL
4	N.C.

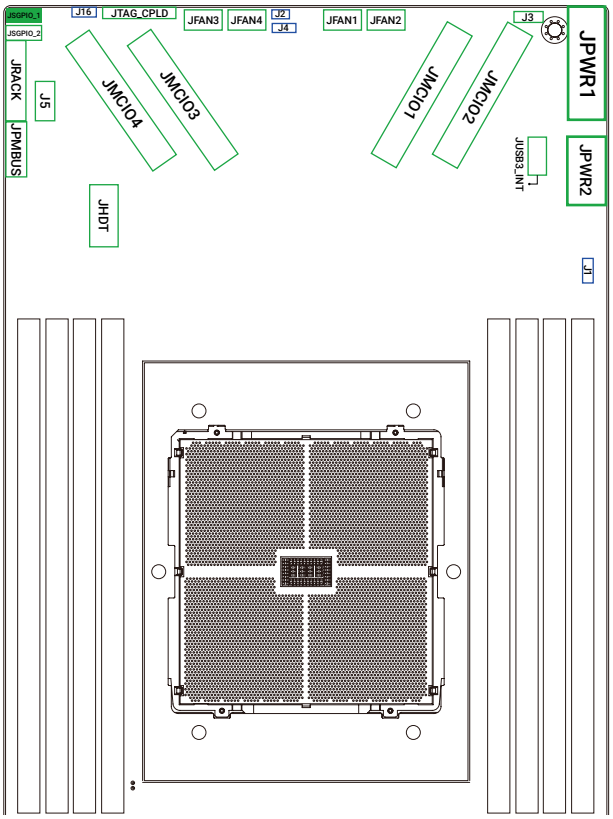




SGPIO header (JSGPIO_1)
This 6-pin header is used to provide CPU SGPIO functionality.

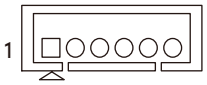
1	+3.3V_S0
2	CONN_SGPIO_CLK<2>
3	CONN_SGPIO_DATA_OUT
4	CONN_SGPIO_LOAD
5	N.C.
6	GND

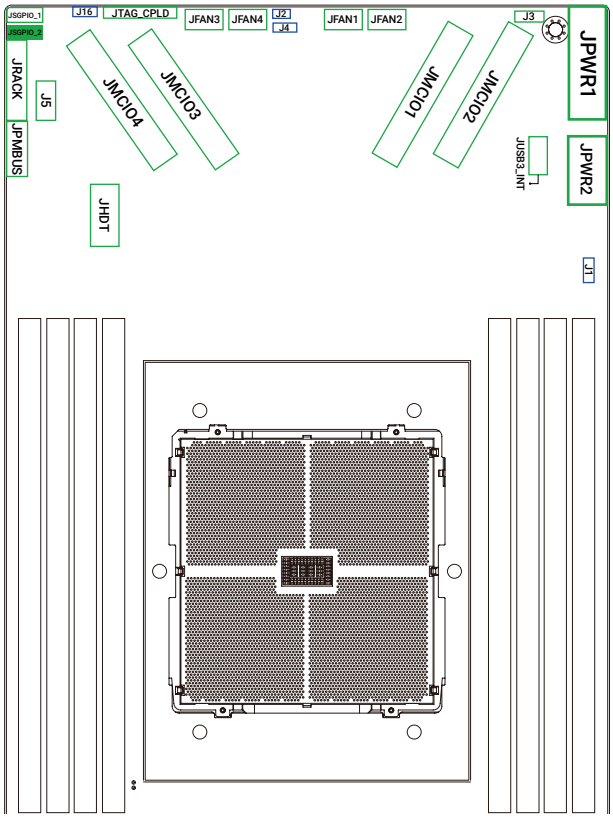




SGPIO header (JSGPIO_2)
This 6-pin header is used to provide CPU SGPIO functionality.

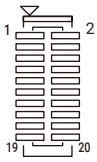
1	+3.3V_S0
2	CONN_SGPIO_CLK<3>
3	CONN_SGPIO_DATA_OUT
4	CONN_SGPIO_LOAD
5	N.C.
6	GND

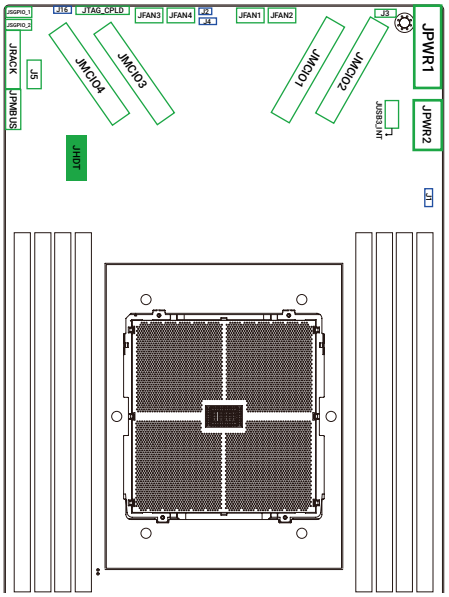




CPU HDT header (JHDT)
This is a 2x10-pin header that is used to provide CPU HDT functionality.

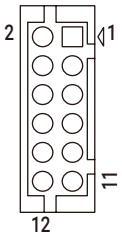
P0_VDD_18_DUAL	1	2	P0_HDT_TCK
GND	3	4	P0_HDT_TMS
GND	5	6	P0_HDT_TDI
GND	7	8	P0_HDT_TDO
P0_HDT_TRST_L	9	10	P0_HDT_CONN_PWROK
P0_G_HDT_CONN_XTRIG_L<6>	11	12	P0_HDT_CONN_RESET_L
P0_G_HDT_CONN_XTRIG_L<7>	13	14	N.C.
P0_G_HDT_CONN_XTRIG_L<5>	15	16	P0_HDT_DBREQ_L
GND	17	18	N.C.
P0_VDD_18_DUAL	19	20	N.C.

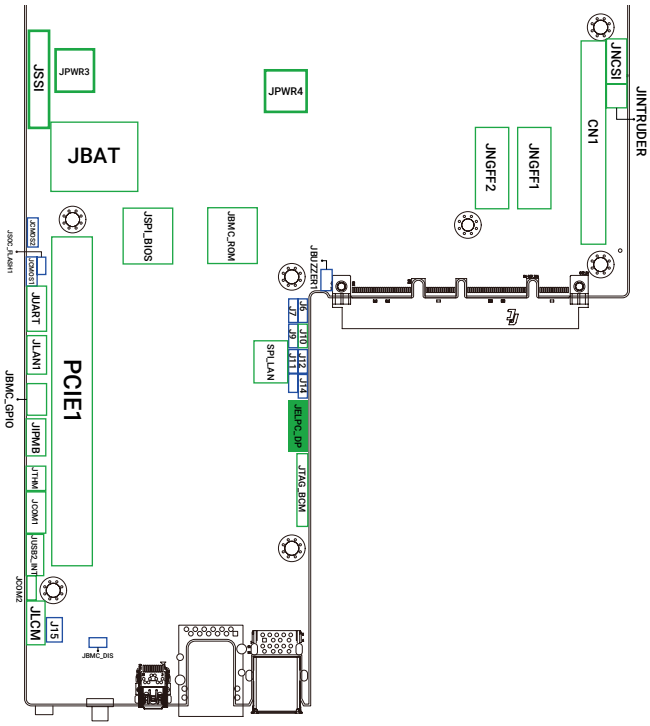




Debug port header (JELPC_DP)
This is a 2x6-pin header that is used to provide Debug port functionality.

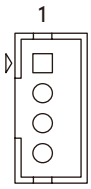
ESPI_CLK	2	1	GND
ESPI_CS	4	3	N.C.
ESPI_RST	6	5	ESPI_ALERT_L
ESPI_D3	8	7	ESPI_D2
+3.3V_DUAL	10	9	ESPI_D1
ESPI_D0	12	11	GND

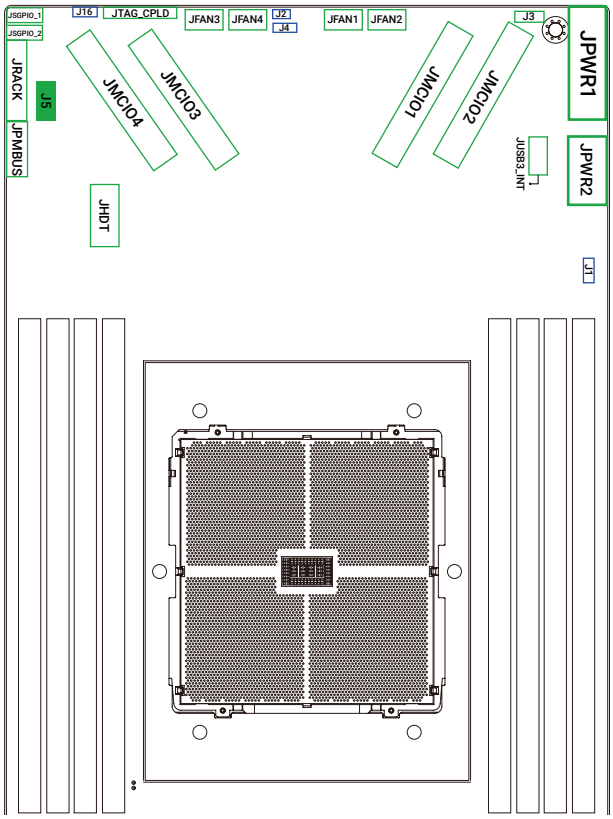




PCIE Hot-Plug SMB header (J5)
This is a 2x3-pin header that is used to provide PCIE Hot-Plug SMB functionality.

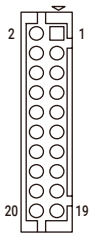
1	HP_SDA<0>
2	GND
3	HP_SCL<0>
4	HP_ALERT<0>

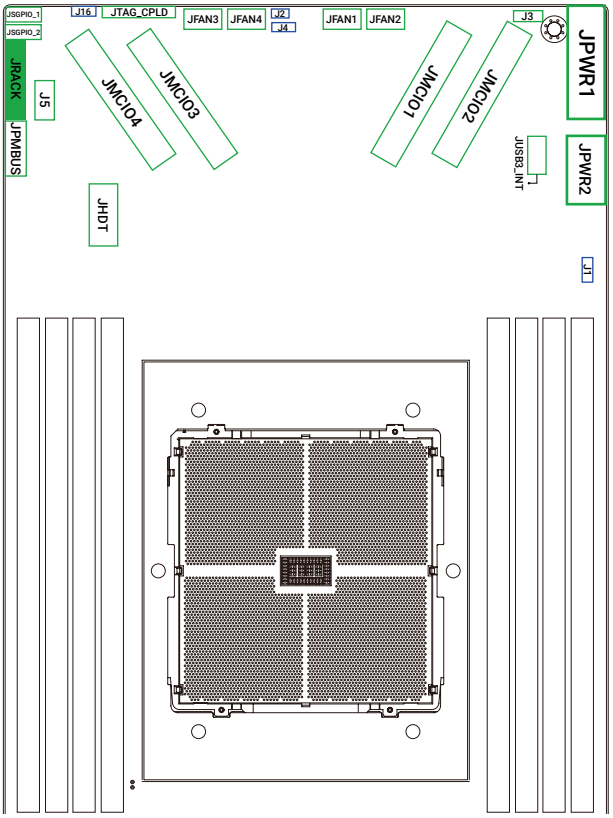




RACK header (JRACK)
This is a 2x10-pin header that is used to provide RACK functionality.

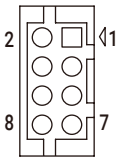
BMC_I2C_08_SCL	2	1	RACK_EXTRST_N
BMC_I2C_08_SDA	4	3	GND
GND	6	5	BMC_I2C_01_SCL
RACK_PWM5	8	7	BMC_I2C_01_SDA
RACK_TACH8	10	9	GND
GND	12	11	RACK_PMBUS _CLK
RACK_PWM6	14	13	RACK_PMBUS _DATA
RACK_TACH9	16	15	PMBUS_ALERT_N
RACK_GPIO_EXIN	18	17	CHASSIS_OPEN
CHASSIS_1U2N_N	20	19	GND

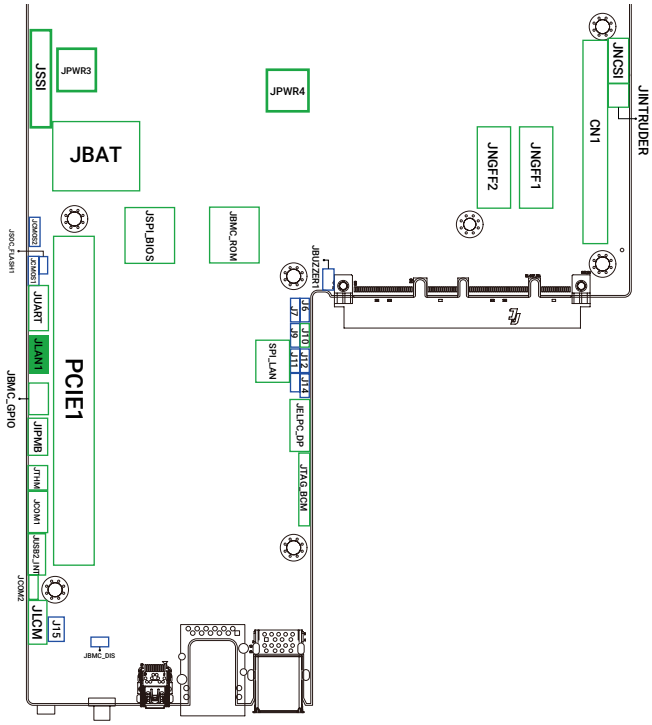




BCM5720 MDI header (JLAN1)
This 2x4-pin header is used to provide BCM5720 MDI functionality.

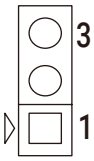
TF_MDI0_DP	2	1	TF_MDI3_DP
TF_MDI0_DN	4	3	TF_MDI3_DN
TF_MDI1_DP	6	5	TF_MDI2_DP
TF_MDI1_DN	8	7	TF_MDI2_DN

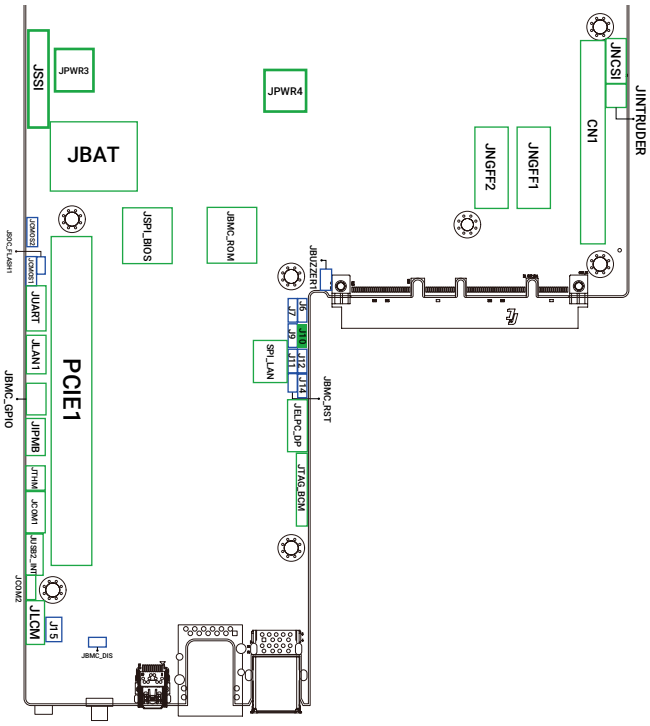




BCM5720 LED header (J10)
This is a 1x3-pin header that is used to provide BCM5720 LED functionality.

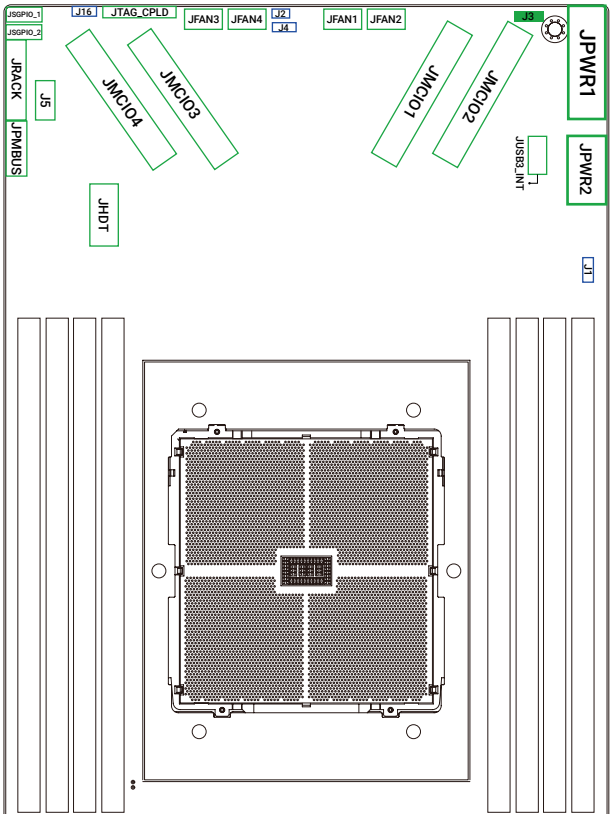
1	LOM_TRAFFIC_LED_L
2	GND
3	LOM_LINK_LED_L





VRM SMB header (J3)
This is a 3-pin connector that is used to provide VRM SMB functionality.

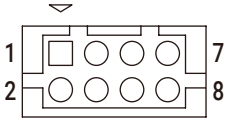
1	SMB_VR_DAT
2	GND
3	SMB_VR_CLK

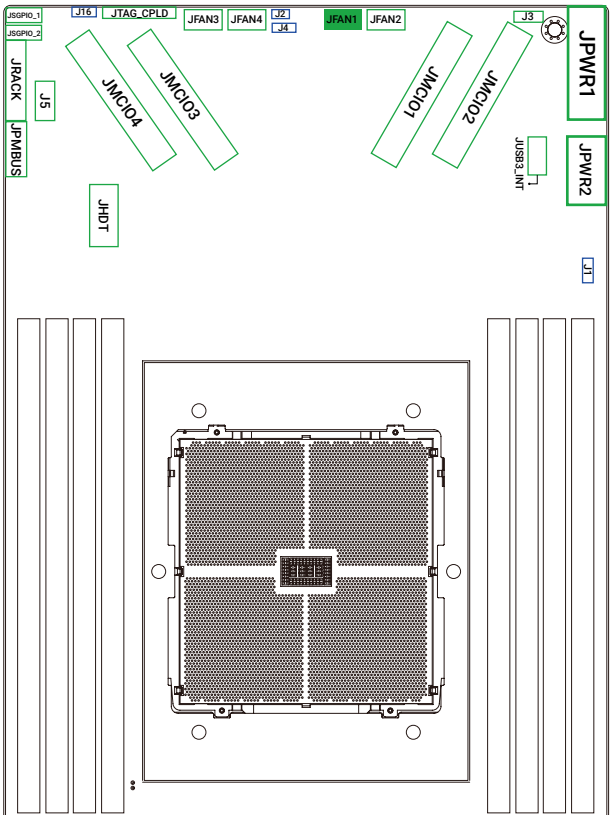


Fan Header (JFAN1)

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

HW3_TACH_FAN2	2	1	HW3_TACH_FAN1
+12V_FAN	4	3	+12V_FAN
PWM3_R	6	5	PWM3_R
GND	8	7	GND

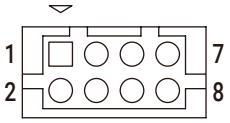


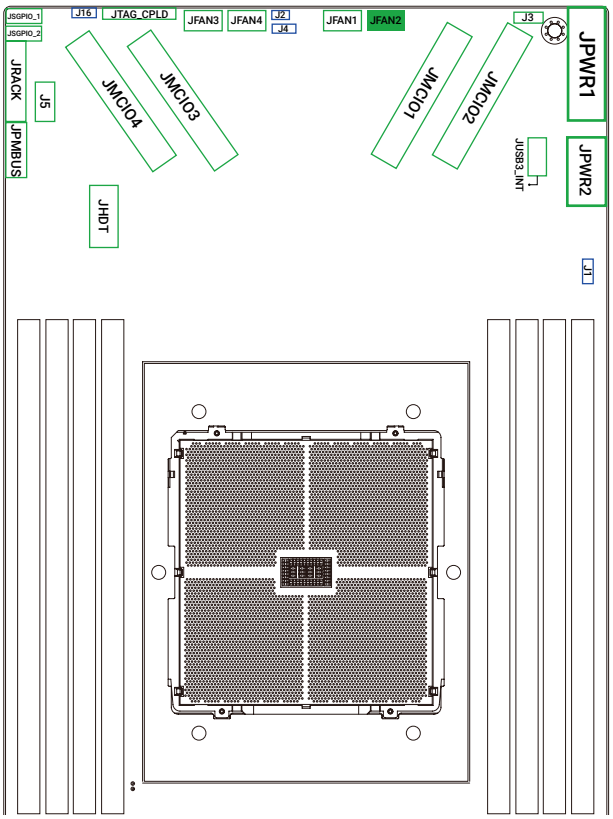


Fan Header (JFAN2)

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

HW4_TACH_FAN2	2	1	HW4_TACH_FAN1
+12V_FAN	4	3	+12V_FAN
PWM4_R	6	5	PWM4_R
GND	8	7	GND

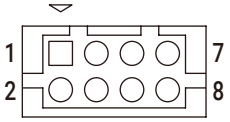


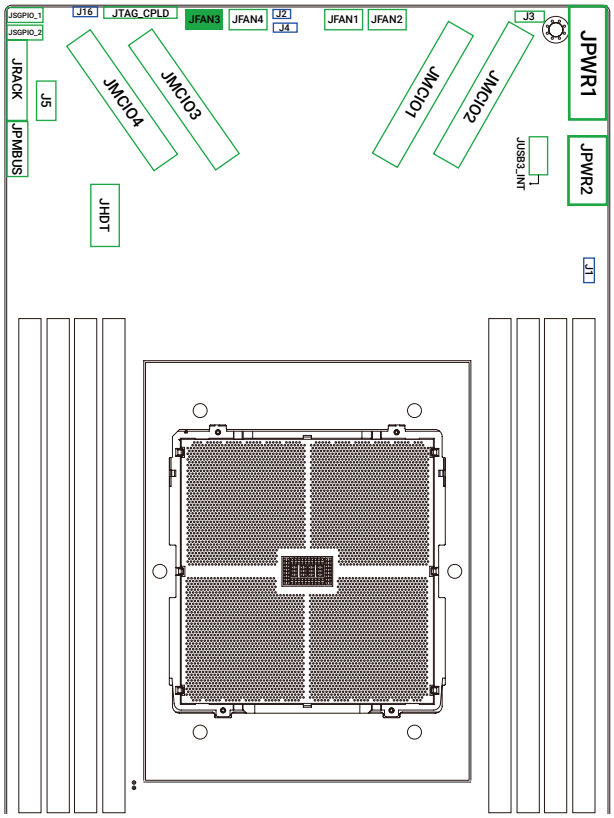


Fan Header (JFAN3)

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

HW1_TACH_FAN2	2	1	HW1_TACH_FAN1
+12V_FAN	4	3	+12V_FAN
PWM1_R	6	5	PWM1_R
GND	8	7	GND

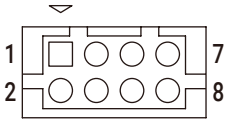


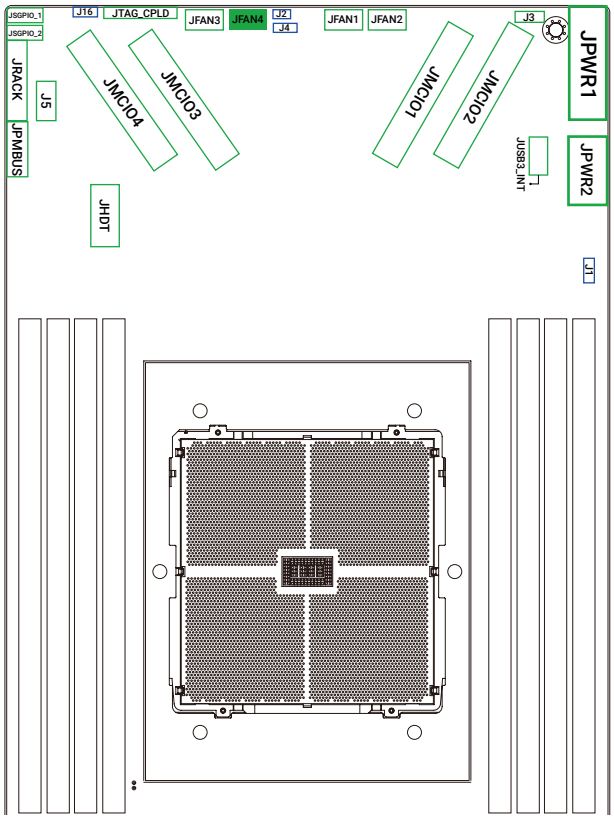


Fan Header (JFAN4)

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

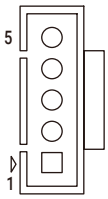
HW2_TACH_FAN2	2	1	HW2_TACH_FAN1
+12V_FAN	4	3	+12V_FAN
PWM2_R	6	5	PWM2_R
GND	8	7	GND

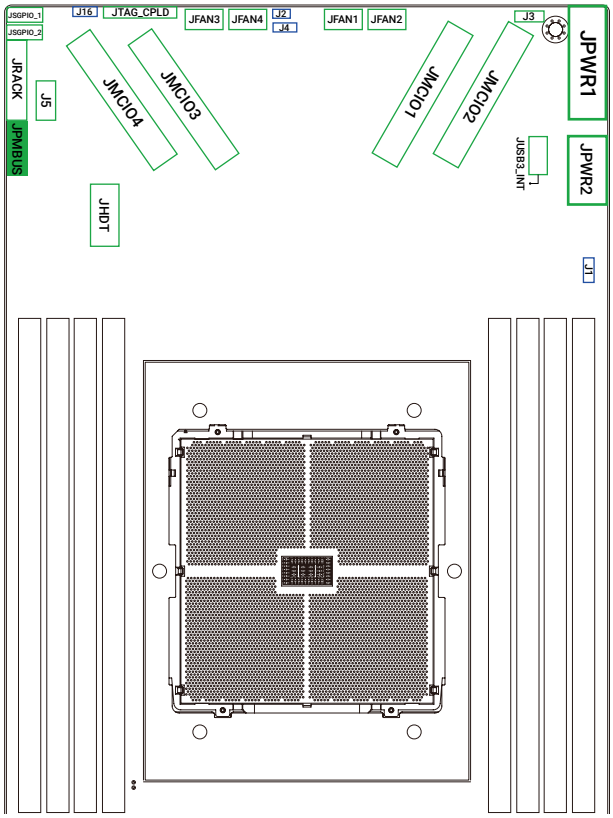




PMBus header (JPMBUS)
This is a 5-pin header that is used to provide PMBus functionality.

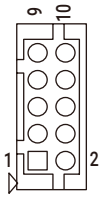
1	SMB_PMBUS_CLK
2	SMB_PMBUS_DATA
3	PMBUS_ALERT_N
4	GND
5	+3.3V_DUAL

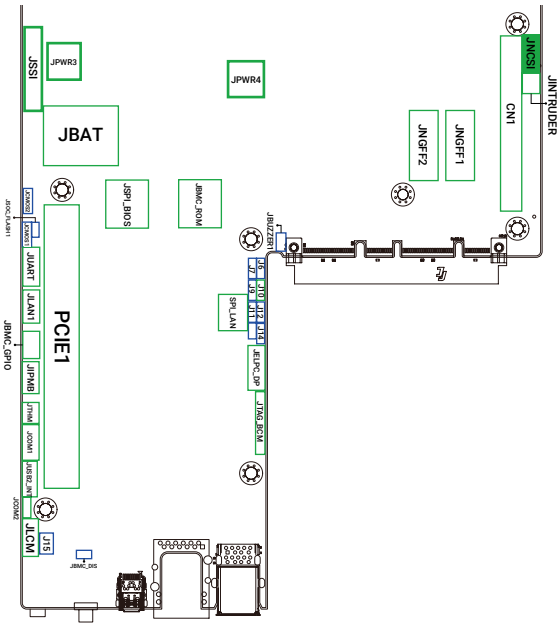




External NCSI (JNCSI)
This 2x5-pin header is used to provide external NCSI functionality.

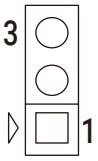
NCSI_HDR_SFF_CRSDV	2	1	NCSI_HDR_SFF_TXD0
NCSI_LOM_OCP_ARBOUT_R	4	3	NCSI_HDR_SFF_TXD1
GND	6	5	NCSI_HDR_SFF_RXD0
NCSI_LOM_ARBIN_R_SW	8	7	NCSI_HDR_SFF_RXD1
CLK_50M_HDR_SFF_CRSDV	10	9	NCSI_HDR_SFF_TXEN

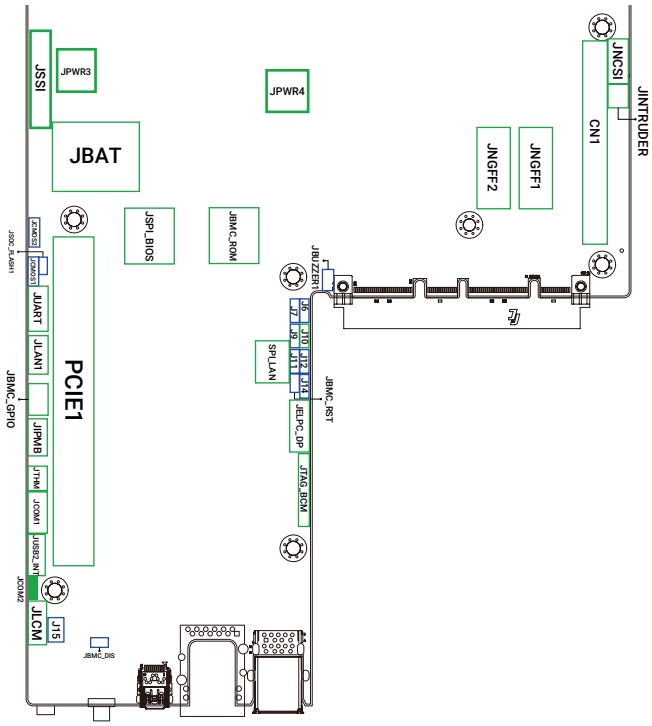




UART port Header (JCOM2)
This is a 3-pin header that is used to provide SuperIO UART4 functionality.

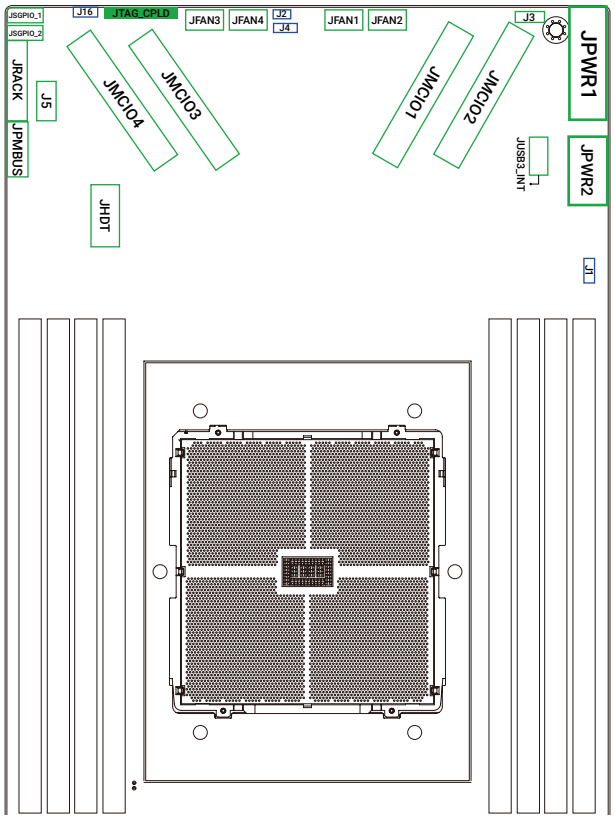
1	RS232_TXD2
2	RS232_RXD2
3	GND





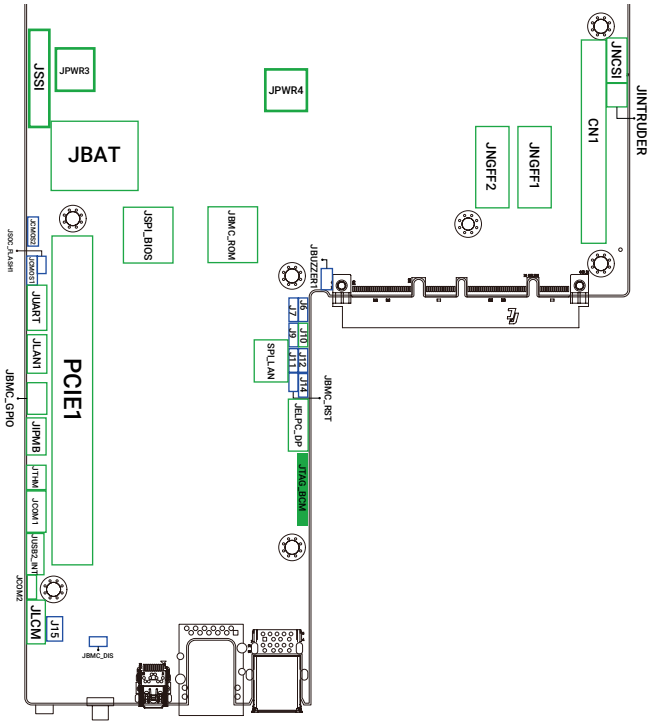
CPLD JTAG header (JTAG_CPLD)
This is a 8-pin header that is used to provide CPLD JTAG functionality.

1	HW2_TACH_FAN1
2	+12V_FAN
3	PWM2_R
4	GND
5	N.C.
6	JTAG_PLD_TMS
7	GND
8	JTAG_PLD_TCK



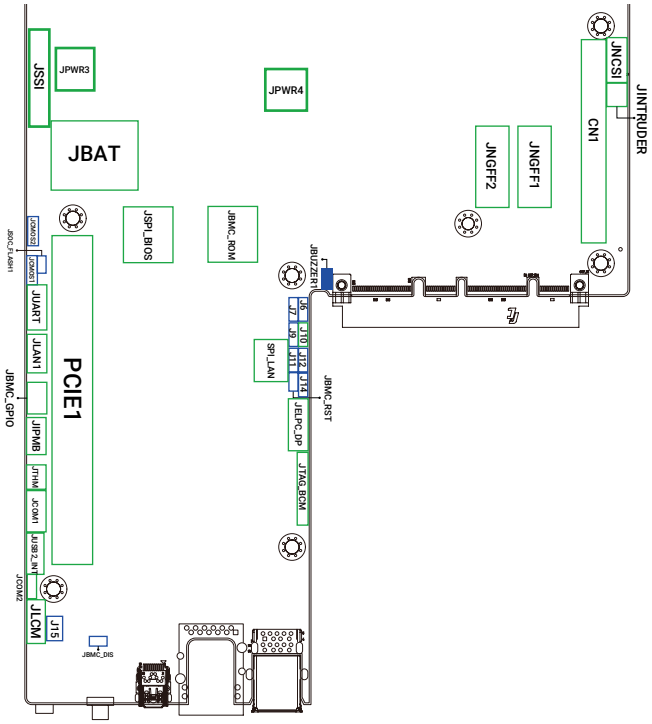
BMC JTAG header (JTAG_BCM)
This is a 8-pin header that is used to provide BMC JTAG functionality.

1	ARM_nTRST
2	ARM_TDI
3	ARM_TMS
4	ARM_TCK
5	GND
6	ARM_TDO
7	GND
8	GND



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

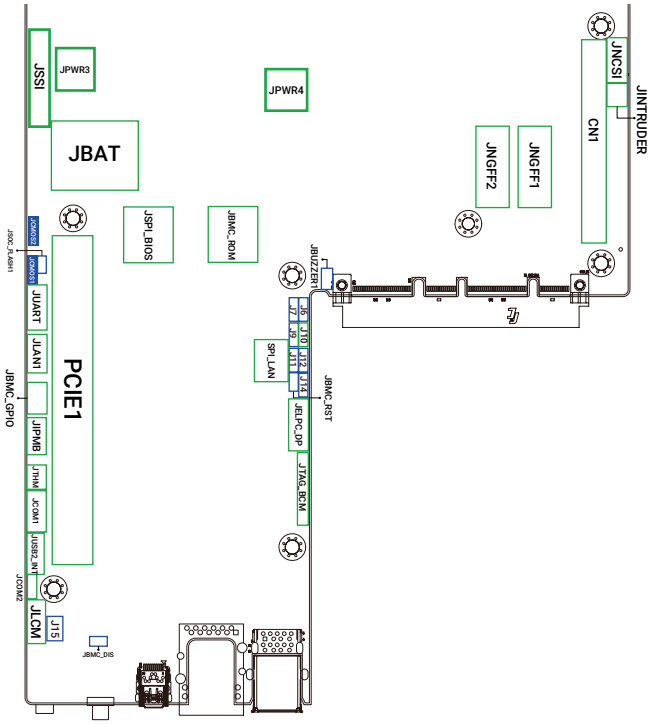
1	+5V_S0
2	BMC_BUZZER-



3.6 Jumper Setting

CPU CMOS Jumper (JCMOS1)

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



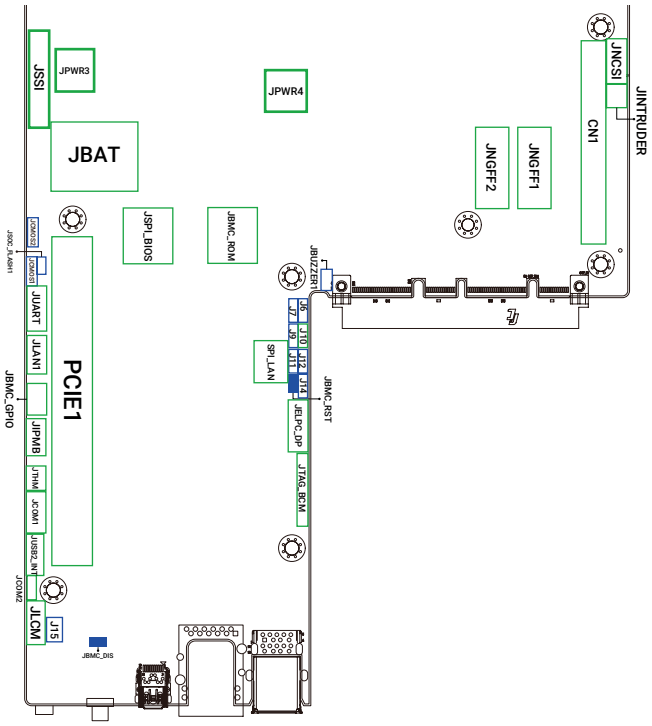
BMC CMOS Jumper (JCMOS2)

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

BMC Reset Jumper (JBMC_RST)

JBMC_RST	Setting	
Short	Reset BMC	
Open	Normal	Default

Note: Please shunt down before jumper short



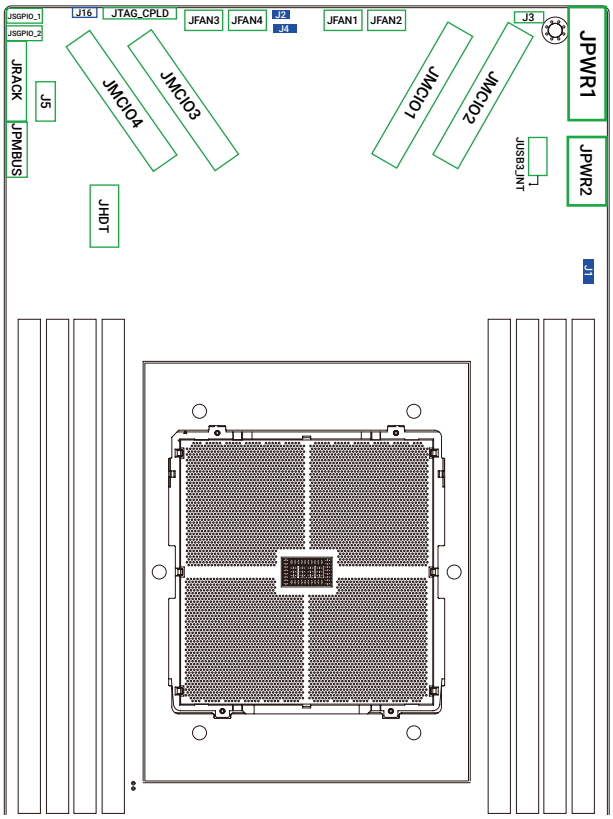
BMC ARM Disable Jumper (JBMC_DIS)

JBMC_DIS	Setting	
Short	Disable	
Open	Normal	Default

Note: Please shunt down before jumper short

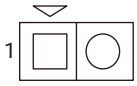
BMC update BCM5720 & BIOS (J1)

J1	Setting	
Pin1-2	BIOS (J9)	Default
Pin2-3	BCM5720 (J4)	



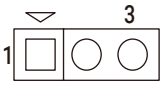
BMC update CPLD (J2)

J2	Setting	
Open	Control By BMC	Default
Short	Disable	



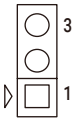
BMC update BCM5720 ROM (J4)

J4	Setting	
Pin1-2	Enable	
Pin2-3	Disable	Default



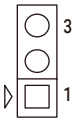
BMC NCSI Select (J6)

J6	Setting	
Pin1-2	JNCSI	
Pin2-3	JOCP	Default



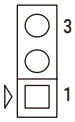
CPU SPI0/eSPI0 (J7)

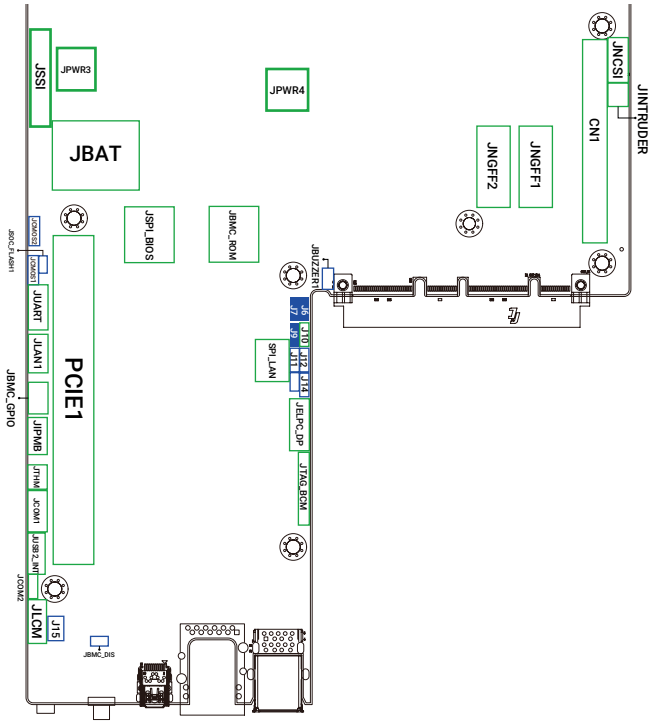
J7	Setting	
Pin1-2	BMC eSPI	
Pin2-3	BIOS ROM (J9)	Default



BIOS ROM SPI (J9)

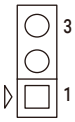
J9	Setting	
Pin1-2	BMC SPI2	Default
Pin2-3	CPU SPI0/eSPI0	

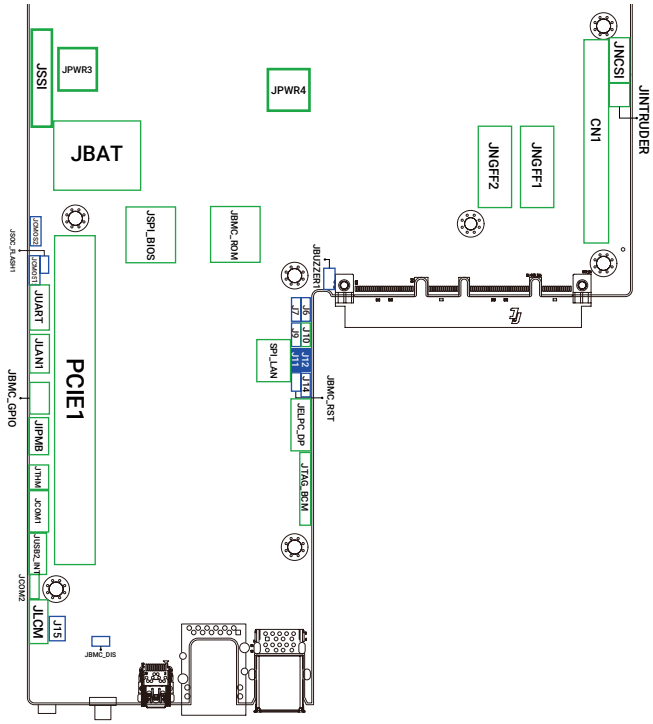




CPU SGPIO (J11)

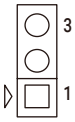
J11	Setting	
Pin1-2	JSPIO_1-2	
Pin2-3	CPLD	Default





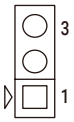
BMC NCSI (J12)

J12	Setting	
Pin1-2	BCM5720	
Pin2-3	JOCP & JNCSI (J6)	Default



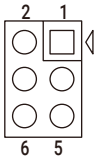
DIMM I3C (J14)

J14	Setting	
Pin1-2	Control by CPU GPIO	Default
Pin2-3	Force on CPU I3C	



JCONSOLE UART (J15)

J15	Setting	
Pin1-3 Pin2-4	UART1	Default
Pin3-5 Pin4-6	UART5	

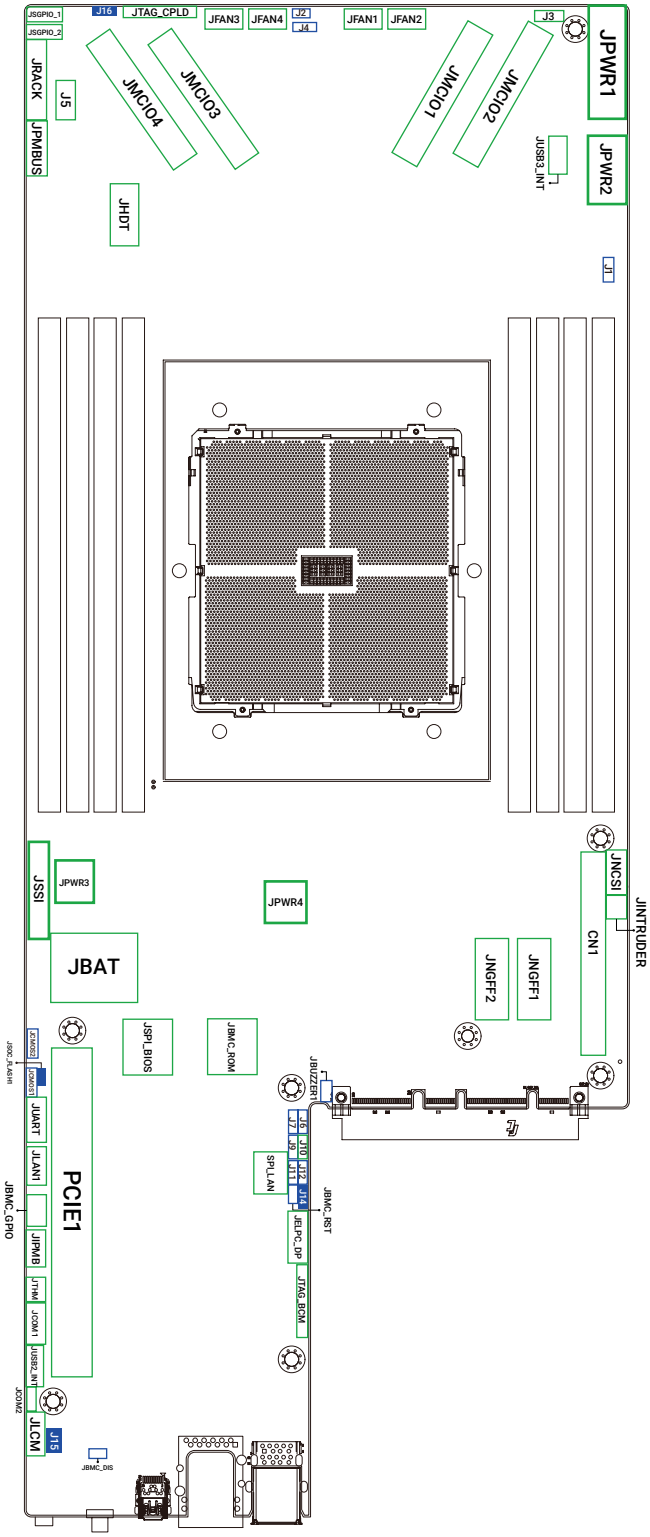


JSOC_FLASH1 Select (JSOC_FLASH1)

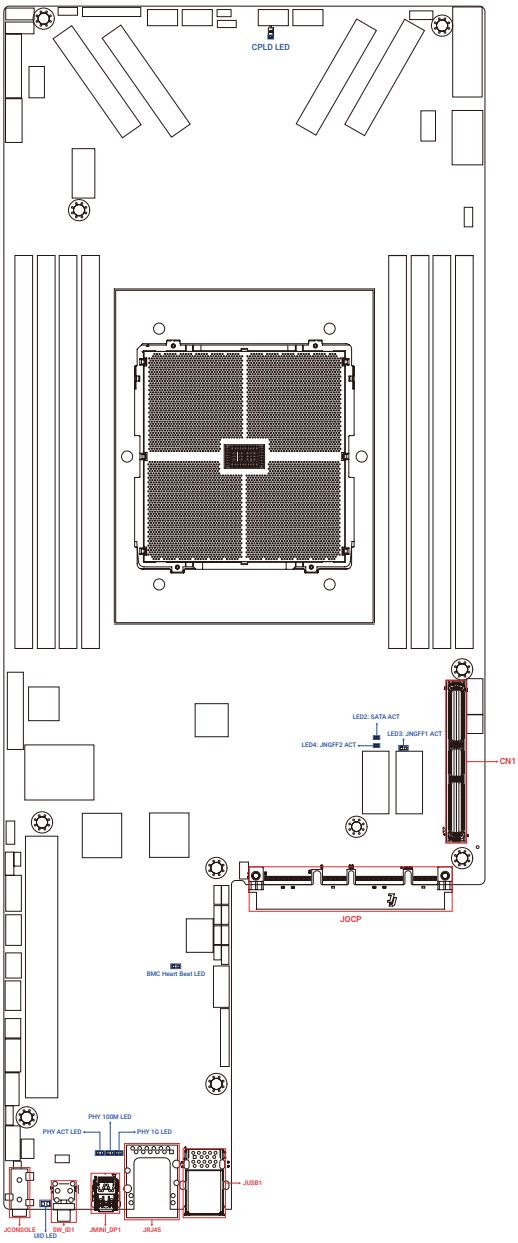
JSOC_ FLASH1	Setting	
Short	SOC_FLASH enable	
Open	SOC_FLASH disable	Default

J16 Select (J16)

J16	Setting	
Pin1-2	PMBUS +5V	
Pin2-3	PMBUS +3V3	Default



3.7 Internal LED



Item	Color	Behavior
BMC HEART BEAT LED	Green (Blinking)	BMC activity is detected.
	Off	BMC is not active.
CPLD LED	Solid Green	All power are ready.
	Breath Green	S5 power is ready.
	Off	CPLD is not active.
JNGFF1 ACTIVITY LED	Blue (Blinking)	JNGFF1 activity is detected.
	Off	JNGFF1 is not active.
JNGFF2 ACTIVITY LED	Blue (Blinking)	JNGFF2 activity is detected.
	Off	JNGFF2 is not active.
PHY 1G LED	Yellow	1G link detected
PHY 100M LED	Green	100M link detected
PHY ACT LED	Green (Blinking)	Activity detected

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

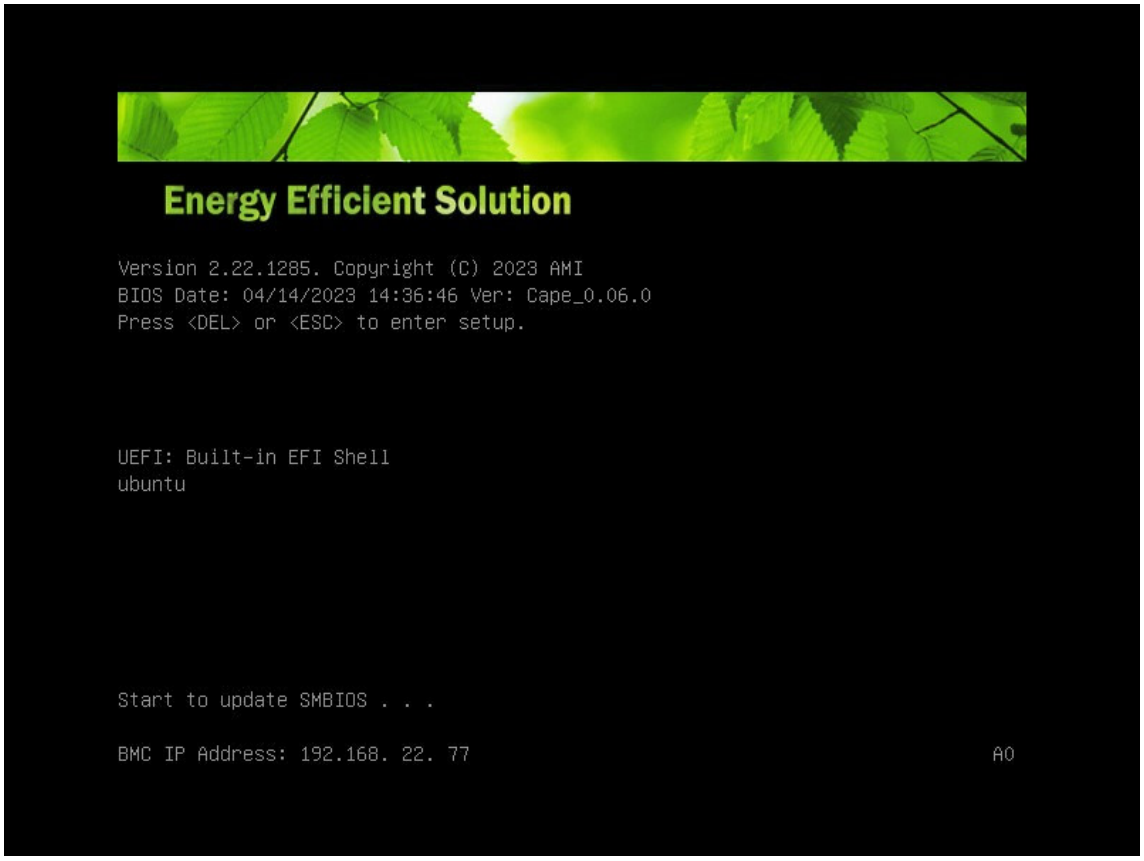
4.2.1 Menu

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

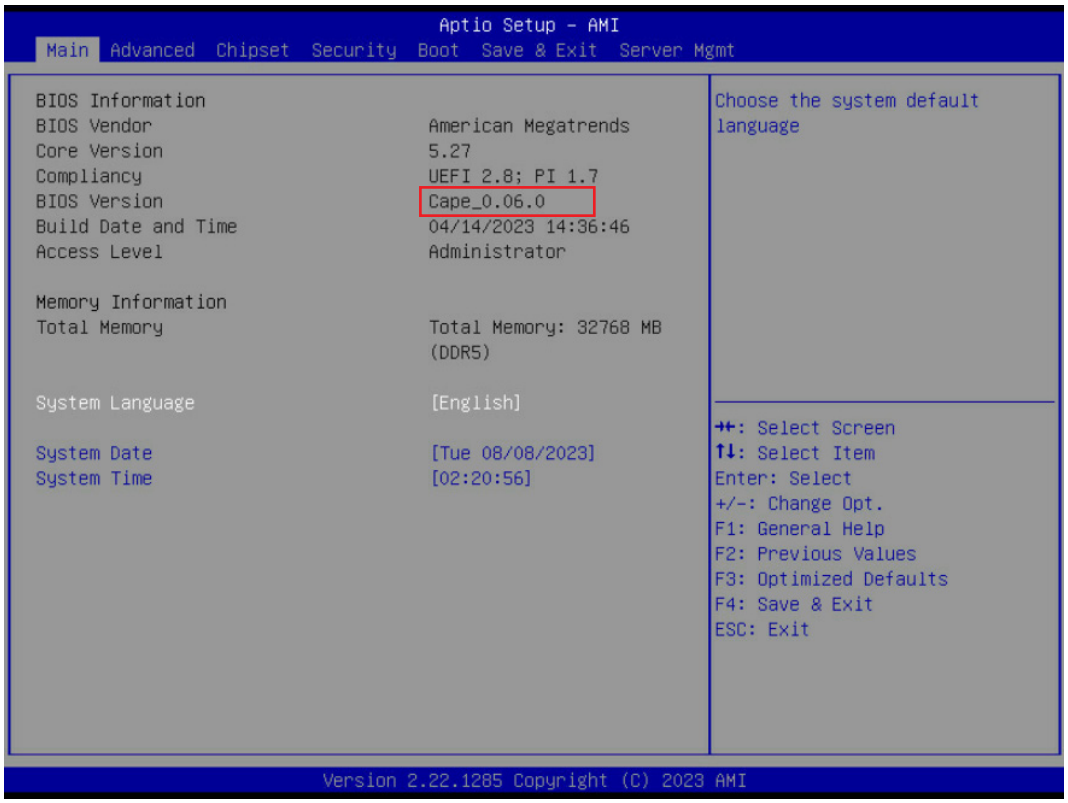
Menu	Description
Main	Displays basic system information and date & time.
Advanced	Allows configuration of advanced system settings.
Chipset	Communicate between the processor and external devices. Select North Bridge or South Bridge to access the parameters for different items.
Security	Sets passwords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



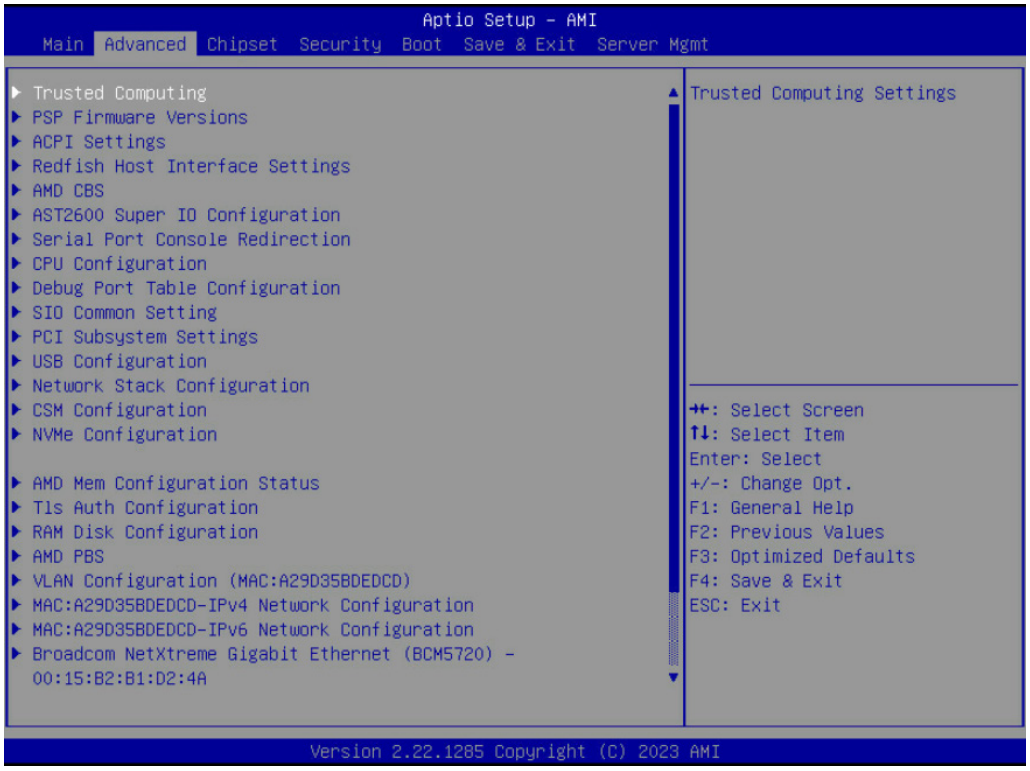
4.3 Main



4.3.1 Main

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

4.4 Advanced



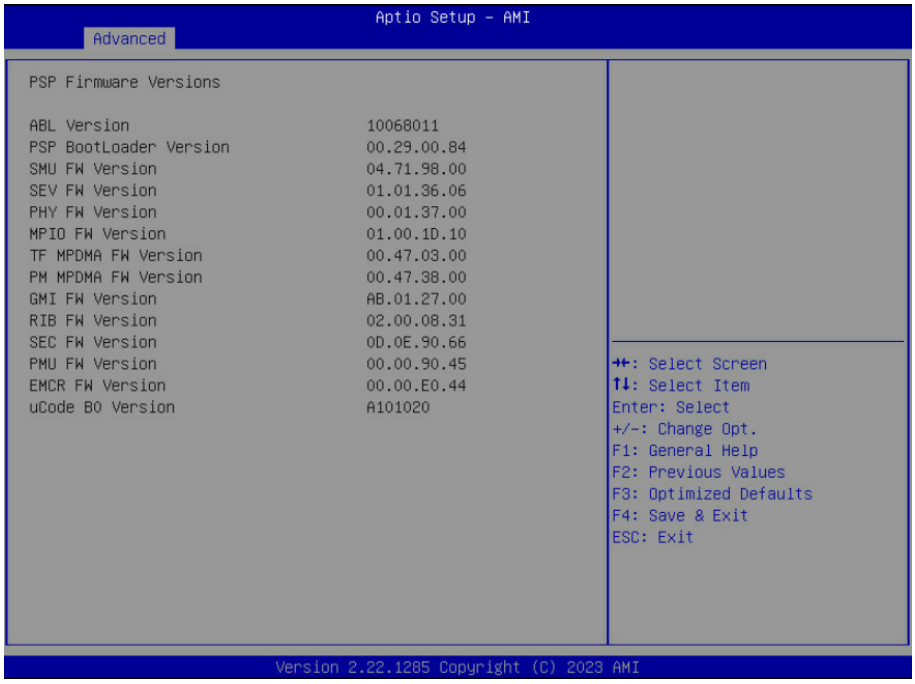
4.4.1 Trusted Computing

Trusted Computing Settings.

Trusted Computing			
Security Device Support	Enables/disables BIOS support for security device.		
	▶Enable	Disable	
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
Disable Block Sid	Override to allow SID authentication in TCG Storage device.		
	Enable	▶Disable	

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 Redfish Host Interface Settings

Redfish Host Interface Parameters.

Redfish Host Interface Settings		
Redfish	Enables/disables AMI Redfish.	
	▶Enable	Disable
Authentication mode	Select authentication mode.	
	▶Basic Authentication	Session Authentication
IP address	169.254.0.17	
IP Mask address	255.255.0.0	
IP Port	443	

4.4.5 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 Control	Sets the number of active CDDs. Once this option has been used to remove any CCDs, a Power Cycle is required in order for future selections to take effect.			
				▶Auto	2 CCDs	4 CCDs	
				6 CCDs	8 CCDs	10 CCDs	
			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	ONE (1+0)	TWO (2+0)	THREE (3+0)
				FOUR (4+0)	FIVE (5+0)	SIX (6+0)	SEVEN (7+0)
		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		
	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 alll 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 1006. 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/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		
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	NPS2	NPS4
		Memory interleaving	Allows for disabling memory interleaving. Note that NUMA nodes per socket will be honored regardless of this setting.			
			▶Auto	Enable	Disable	
		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	Enable	Disable	

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	Enable	Disable				
		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	Enable	Disable				
		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	Enable	Disable				
		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	12Gbps	16Gbps	17Gbps	18Gbps	20Gbps	22Gbps	23Gbps
			24Gbps	25Gbps	26Gbps	27Gbps	30Gbps	32Gbps		
		3-link xGMI max speed	Specifies the max frequency used for XGMI PState in a 3-link topology.						
			▶Auto	12Gbps	16Gbps	17Gbps	18Gbps	20Gbps	22Gbps	23Gbps
			24Gbps	25Gbps	26Gbps	27Gbps	30Gbps	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
		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

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)	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	
	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
UMC Common Options	DDR Addressing Options	Chipselect Interleaving	Interleaving memory blocks across the DRAM chip selects for node 0.				
			▶Auto	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 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	Socket 0 Channel 0-11	SPD reading will be skipped when channel is disabled. ►Enabled | Disabled
			Socket 1 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/(120)	RZQ/(80)
				RZQ/(60)	RZQ/(68)	RZQ/(40)	RZQ/(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 (68)	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 (68)	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 (68)	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	Active Memory Timing Settings.				
				Auto	▶Enabled			
			Memory Target Speed	Specifies the memory target speed in MT/s.				
				▶Auto	DDR3200	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 fo 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. ▶> 85'C | > 90'C | > 95'C
	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=Disabled		
			▶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
		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	Enable	Disable
		HSMP Support	Select HSMP support enable or disable.		
			▶Auto	Enable	Disable

NBIO Common Options	SMU Common Options	SVI3 SVC Speed Control	No help string			
			▶Auto	Manual		
		3D V-Cache	Override of X3D technology.			
			▶Auto	Disable	1 stack	
		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 milliseconds.			
			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 Onlly	
	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	Enabled	Disabled			
	Allow Compliance	When enabled, allows the PCIe RP to enter Polling. Compliance state.					
		▶Auto	Enabled	Disabled			
	SRIS	SRIS					
		▶Auto	Enabled	Disabled			
	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			
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.				
			▶Auto	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 Mode Speed	I3C Transfer Speed.				
			▶Auto	SDR2 (6 MHz)	SDR0 (12.5 MHz)		
		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	Enabled	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 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	
Workload Tuning	Workload Profile	Select the profile for different workloads.				
		▶Auto	Disable	CPU Intensive	Java Throughput	Java Latency
		Power Efficiency	Memory Throughput Intensive	Storage IO Intensive	NIC Throughput Intensive	NIC Latency Sensitive
		Accelerator Throughput	VMware vSphere Optimized	Linux KVM Optimized	Container Optimized	RDBMS Optimzed
		Big Data Analytics Optimized	IOT Gateway	HPC Optimized	OpenStack NFV	OpenStack for RealTime Kernel
	Performance Tracing	Enable to allow capturing performance traces.				
		▶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	ForceAerFwFirstIfCxlPresent
		CXL Component Error Reporting	Configuration CXL Component Error reporting mechanism.		
			OS First	▶FW-First	

4.4.6 AST2600 Super IO Configuration

System Super IO Chip Parameters.

AST2600 Super IO Configuration			
Serial Port 1 Configuration	Serial Port	Enable/Disable Serial Port1 (COM A)	
		▶Enable	Disable
	Change Settings	Select an optimal settings for Super IO Device.	
		▶Auto	IO=3F8h; IRQ=4;
		IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;	IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;
		IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;	IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;
Serial Port 2 Configuration	Serial Port	Enable/Disable Serial Port2 (COM B)	
		▶Enable	Disable
	Change Settings	Select an optimal settings for Super IO Device.	
		▶Auto	IO=3F8h; IRQ=4;
		IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;	IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;
		IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;	IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;
Serial Port 3 Configuration	Serial Port	Enable/Disable Serial Port3 (COM C)	
		▶Enable	Disable
Serial Port 4 Configuration	Serial Port	Enable/Disable Serial Port4 (COM D)	
		▶Enable	Disable

4.4.7 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	
Legacy Console Redirection Settings	Redirection COM Port	Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages.	
		▶COM0	COM1
	Resolution	On Legacy OS, the Number of Rows and Columns supported redirection.	
		▶80x24	80x25
	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	

4.4.8 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.	

4.4.9 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

4.4.10 SIO Common Configuration

SIO Common Configuration.

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

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	
CN1 Slot Control.	Select CN1 Slot x4x4x4x4 or x8x8 or x16.		
	x4x4x4x4	x8x8	▶x16
PCIe1 Slot Control.	Select PCIe1 Slot x4x4x4x4 or x8x8 or x16.		
	x4x4x4x4	x8x8	▶x16
JOCP Slot Control.	Select JOCP Slot x8x8 or x16.		
	x8x8	▶x16	
JMCIO1-4 Control.	Select JMCIO1-4 x4x4x4x4 or x8x8 or x16.		
	x4x4x4x4	x8x8	▶x16

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 CDROM1-3 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	
GateA20 Active	UPON REQUEST - GA20 can be disabled using BIOS services. ALWAYS - do not allow disabling GA20; this option is useful when any RT code is executed above 1MB.		
	▶Upon Request	Always	
INT19 Trap Response	BIOS reaction on INT19 trapping by Option ROM: IMMEDIATE - execute the trap right away; POSTPOMED - execute the trap during legacy boot.		
	▶Immediate	Postponed	
Boot option filter	This option controls Legacy/UEFI ROMs priority.		
	UEFI and Legacy	Legacy only	▶UEFI only
Network	Controls the execution of UEFI and Legacy Network OpROM.		
	Do not launch	▶UEFI	Legacy
Storage	Controls the execution of UEFI and Legacy Legacy OpROM.		
	Do not launch	▶UEFI	Legacy
Video	Controls the execution of UEFI and Legacy Video OpROM.		
	Do not launch	▶UEFI	Legacy
Other PCI devices	Determines OpROM execution policy for devices other than Network, Storage, or Video.		
	Do not launch	▶UEFI	Legacy

4.4.15 NVMe Configuration

NVMe Device Options Settings.

4.4.16 AMD Mem Configuration Status

To display memory configuration (initialized by ABL) status.

AMD Mem Configuration Status		
Socket 0	Socket-specific memory configuration status.	
	Channel 0-11	Channel-specific memory configurationii status.

4.4.17 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	FE9C6606-8B49-44A3-8B6B-DEA3A0E0324D	GUID for CERT	
			Enabled	▶Disabled

4.4.18 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.		
RAM Disk 0	Select to remove.		
	Enable	▶Disable	
Remove selected RAM disk(s)	Removes selected RAM disk(s).		

4.4.19 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	

RAS	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 Err 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 Err 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.	
		▶Enabled	Disabled
	DRAM Hard Post Package Repair	This feature allows spare DRAM rows to replace malfunctioning rows via an in-field repair mechanism.	
		Enabled	▶Disabled
	HEST DMC Structure Support	HEST DMC (Deferred Machine Check) Structure Support.	
		Enabled	▶Disabled
	CXL Error Report Support	Enable/Disable CXL Error Reporting.	
		Enabled	▶Disabled
SPI Locking	Enable/disable SPI Locking for protect ROM part.		
	Enabled	▶Disabled	
CXL Range Encryption	Range 1-7 Memory Base	Enter memory range base address and limit address.	
		0	
	Range 1, 2, 4, 5 Memory Limit	Enter memory range base address and limit address.	
		0	
	Range 3, 6, 7 Memory Size	Enter memory range base address and limit address.	
		0	
	Start CXL Range Encryption	Start to encrypt all memory ranges.	

4.4.20 Driver Health

Provides Health Status for the Drivers/Controllers.

MAC: 0015B2B1D24A-IPv6 Network Configuration		
Broadcom Gigabit Ethernet Driver	Provides Health Status for the Drivers/Controllers.	
	Healthy	
	Controller 9DD8EC18 Child 0	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

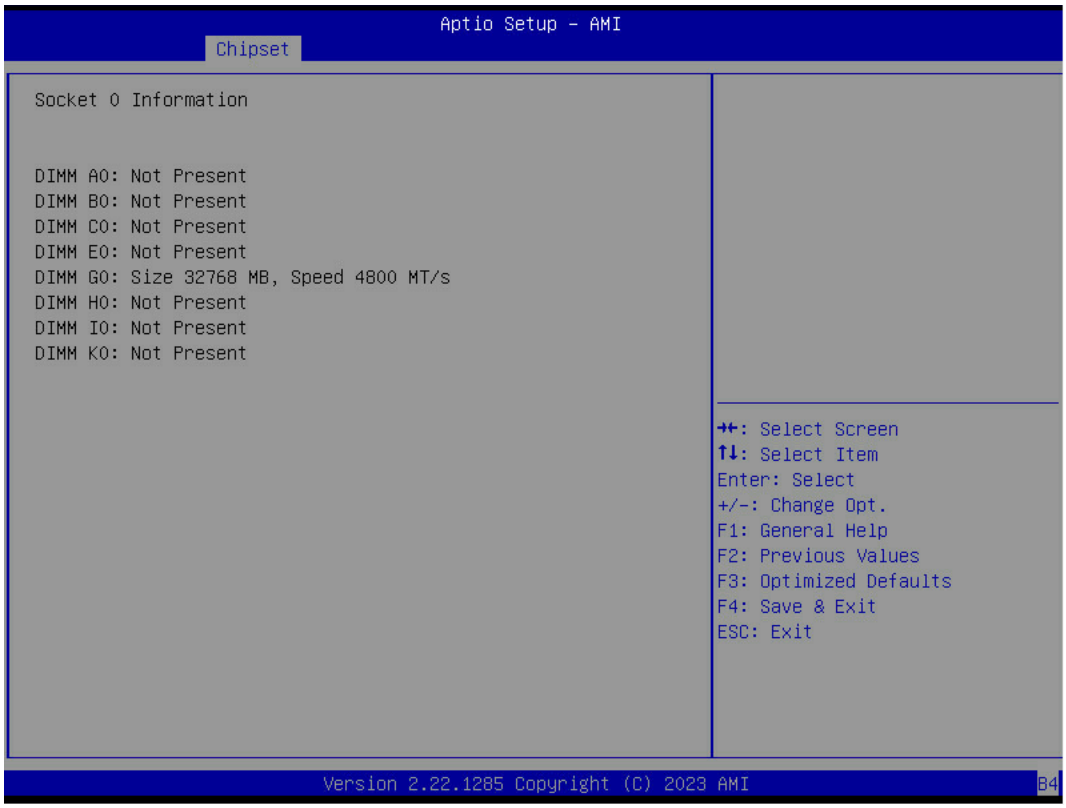
4.5.3 South Bridge

South Bridge Parameters

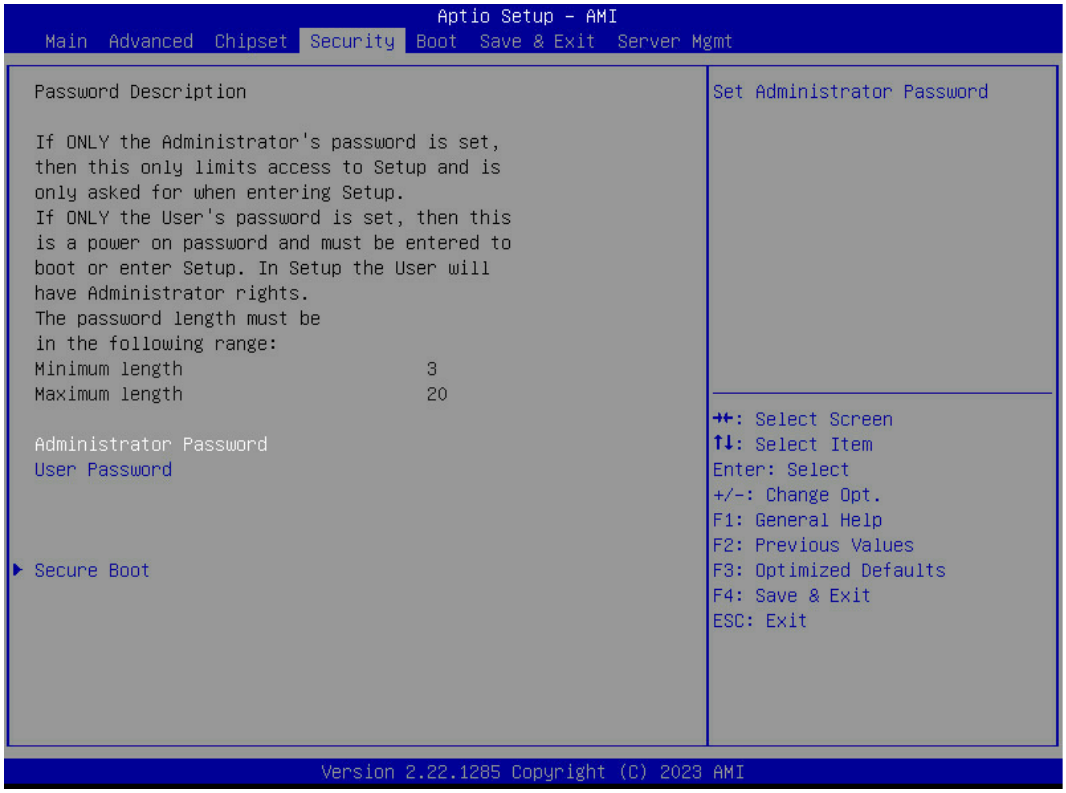
South Bridge				
SB Debug Configuration	Options For SB Debug Features.			
	SB SATA DEBUG Configuration	Aggressive Link PM Capability	Indicates Whether Host Bus Adapter (HBA) can support Auto-Generating Link Requests to the partial or slumber states when there are no commands to process.	
			▶Enable	Disable
		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	TimerTick Tracking	Enable	▶Disable
		Clock Interrupt Tag	Enable	▶Disable
	SB MISC 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
Example for installing one DIMM, please refer to the screenshot below.

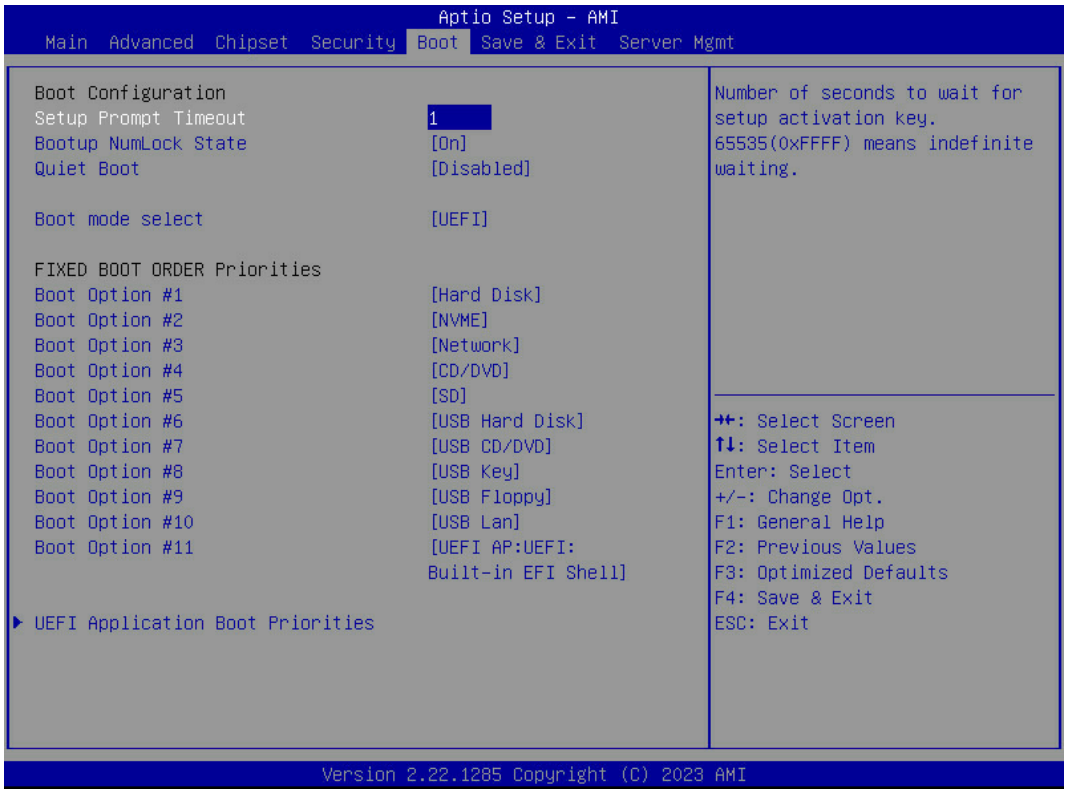


4.6 Security



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

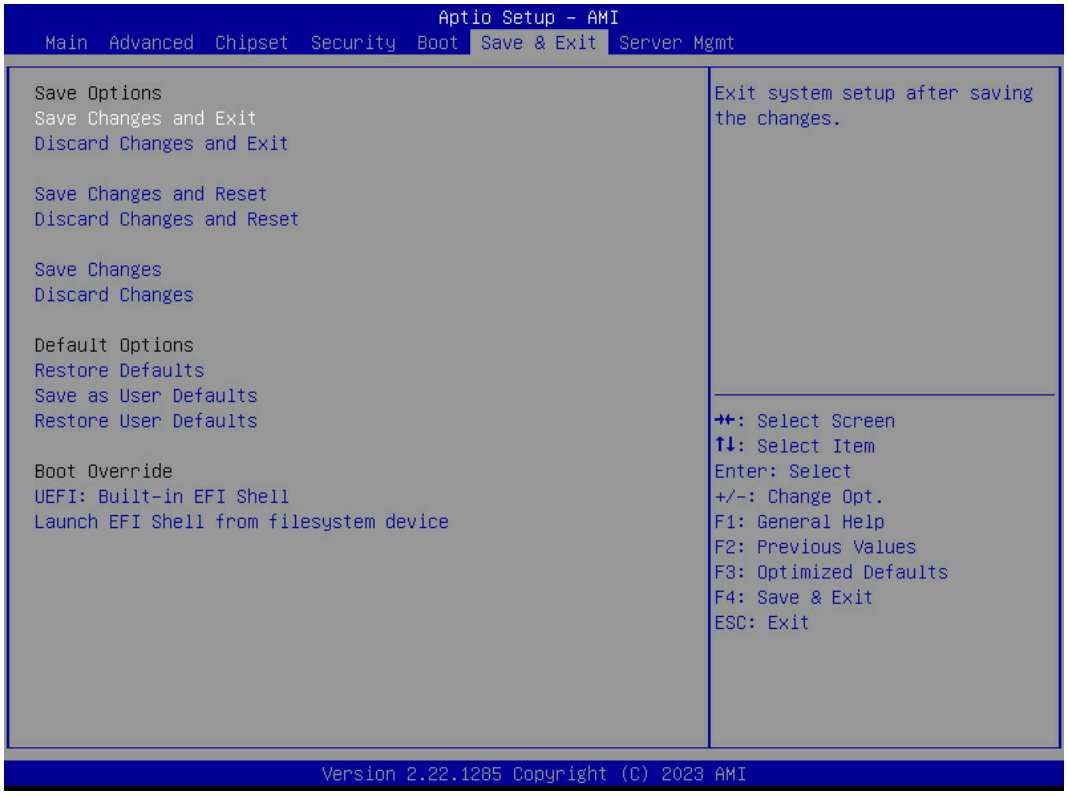
4.7 Boot



Boot				
Set Prompt Timeout	Number of seconds to wait for setup activation key. 65565 (0xFFFF) means indefinite waiting.			
	1			
Bootup Numlock State	Select the keyboard Numlock state.			
	▶On		Off	
Quiet Boot	Enables/disables Quiet Boot option.			
	Enable		▶Disable	
Boot mode select	Select boot mode LEGACY/UEFI.			
	▶UEFI		LEGACY	
Boot Option #1	Sets the system boot order.			
	▶Hard Disk	NVME	Network	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	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	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	▶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	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	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	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	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	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	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	CD/DVD
	SD	USB Hard Disk	USB CD/DVD	USB Key
	USB Floppy	USB Lan	▶UEFI AP:UEFI:Built-in EFI Shell	Disabled
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 interface.

Enabled
▶Disabled

4.9.3 FRB-2 Timer

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

▶Enabled
Disabled

4.9.4 FRB-2 Timer timeout

Enter value Between 1 to 30 min for FRB-2 Timer Expiration.

▶6

4.9.5 FRB-2 Timer Policy

Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.

▶Do Nothing	Reset
Power Down	Power Cycle

4.9.6 OS Watchdog Timer

If enabledl, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows the OS Boot Watchdog Timer policy.

Enabled
▶Disabled

4.9.7 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

4.9.8 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

4.9.9 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	

4.9.10 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)
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
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
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
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
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
0xE351	ABL DDR Runtime Post Package Repair End
0xE60B	ABL Functions execute Before
0xE60C	ABL Functions execute
0xEFFF	EndAgesas

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

Post Code	Description
Universal Post Code	
0xA001	Universal ACPI entry
0xA002	Universal ACPI exit
0xA003	Universal ACPI abort
0xA004	Universal SMBIOS entry
0xA005	Universal SMBIOS exit
0xA006	Universal SMBIOS abort

[0xA1XX] For CZ only memory Post codes	
0xA101	Memory structure initialization (Public interface)
0xA102	SPD Data processing (Public interface)
0xA103	Memory configuration (Public interface)
0xA104	DRAM initialization
0xA105	TpProcMemSPDChecking
0xA106	TpProcMemModeChecking
0xA107	Speed and TCL configuration
0xA108	TpProcMemSpdTiming
0xA109	TpProcMemDramMapping
0xA10A	TpProcMemPlatformSpecificConfig
0xA10B	TPProcMemPhyCompensation
0xA10C	TpProcMemStartDcts
0xA10D	(Public interface)
0xA10E	TpProcMemPhyFenceTraining
0xA10F	TpProcMemSynchronizeDcts
0xA110	TpProcMemSystemMemoryMapping
0xA111	TpProcMemMtrrConfiguration
0xA112	TpProcMemDramTraining
0xA113	(Public interface)
0xA114	TpProcMemWriteLevelizationTraining
0xA115	Below 800Mhz first pass start
0xA116	Above 800Mhz second pass start
0xA117	Target DIMM configured
0xA118	Prepare DIMMS for WL
0xA119	Configure DIMMS for WL
0xA11A	TpProcMemReceiverEnableTraining
0xA11B	Start sweep loop
0xA11C	Set receiver Delay
0xA11D	Write test pattern
0xA11E	Read test pattern
0xA11F	Compare test pattern
0xA120	Calculate MaxRdLatency per channel
0xA121	TpProcMemReceiveDqsTraining
0xA122	Set Write Data delay
0xA123	Write test pattern
0xA124	Start read sweep
0xA125	Set Receive DQS delay
0xA126	Read Test pattern
0xA127	Compare Test pattern
0xA128	Update results
0xA129	Start Find passing window
0xA12A	TpProcMemTransmitDqsTraining
0xA12B	Start write sweep
0xA12C	Set Transmit DQ delay
0xA12D	Write test pattern
0xA12E	Read Test pattern
0xA12F	Compare Test pattern

0xA130	Update results
0xA131	Start Find passing window
0xA132	TpProcMemMaxRdLatencyTraining
0xA133	Start sweep
0xA134	Set delay
0xA135	Write test pattern
0xA136	Read Test pattern
0xA137	Compare Test pattern
0xA138	Online Spare init
0xA139	Bank Interleave Init
0xA13A	Node Interleave Init
0xA13B	Channel Interleave Init
0xA13C	ECC initialization
0xA13D	Platform Specific Init
0xA13E	Before callout for "AgesaReadSpd"
0xA13F	After callout for "AgesaReadSpd"
0xA140	Before optional callout "AgesaHookBeforeDramInit"
0xA141	After optional callout "AgesaHookBeforeDramInit"
0xA142	Before optional callout "AgesaHookBeforeDQSTraining"
0xA143	After optional callout "AgesaHookBeforeDQSTraining"
0xA144	Before optional callout "AgesaHookBeforeDramInit"
0xA145	After optional callout "AgesaHookBeforeDramInit"
0xA146	After MemDataInit
0xA147	Before InitializeMCT
0xA148	Before LV DDR3
0xA149	Before InitMCT
0xA14A	Before OtherTiming
0xA14B	Before UMAMemTyping
0xA14C	Before SetDqsEccTmgs
0xA14D	Before MemClr
0xA14E	Before On DIMM Thermal
0xA14F	Before DMI
0xA150	End of memory code
0xA151	Entry point S3Init
0xA180	Sending MRS2
0xA181	Sedding MRS3
0xA182	Sending MRS1
0xA183	Sending MRS0
0xA184	Continuous Pattern Read
0xA185	Continuous Pattern Write
0xA186	Mem: 2d RdDqs Training begin
0xA187	Mem: Before optional callout to platform BIOS to change External Vref during 2d Training
0xA188	Mem: After optional callout to platform BIOS to change External Vref during 2d Training
0xA189	Configure DCT For General use begin
0xA18A	Configure DCT For training begin
0xA18B	Configure DCT For Non-Explicit

0xA18C	Configure to Sync channels
0xA18D	Allocate C6 Storage
0xA18E	Before LV DDR4
BR CPU	
0xA190	BR before AP launch
0xA191	Install AP launched PPI
0xA192	BR after AP launch
0xA193	Before CPU PM
0xA194	Enable IO Cstate
0xA195	Enable C6
0xA196	Install CCX PEI complete PPI
0xA197	BR CPU memory done call back entry
0xA198	Before APM weights
0xA199	0xA199
0xA19A	BR CPU memory done call back end
0xA19B	BR Init Mid entry
0xA19C	BR enable APM
0xA19D	BR Init Mid install protocol
0xA19E	BR Init Mid end
0xA19F	BR Init Late entry
0xA1A0	BR Init Late install protocol
0xA1A1	BR Init Late end
0xA1A2	BR DXE install complete protocol
0xA1A3	UNB install complete PPI
0xA1A4	UNB AfterApLaunch callback entry
0xA1A5	UNB AfterApLaunch callback end
S3 Interface Post Code	
0xA1EC	Before the S3 save code calls out to allocate a buffer
0xA1ED	After the S3 save code calls out to allocate a buffer
0xA1EE	Before the memory S3 save code calls out to allocate a buffer
0xA1EF	After the memory S3 save code calls out to allocate a buffer
0xA1F0	Before the memory code calls out to locate a buffer
0xA1F1	After the memory code calls out to locate a buffer
0xA1F2	Before the memory code calls out to locate a buffer
0xA1F3	After the memory code calls out to locate a buffer
0xA1F4	Before the memory code calls out to locate a buffer
0xA1F5	After the memory code calls out to locate a buffer
0xA1F6	Before the memory code calls out to locate a buffer
0xA1F7	After the memory code calls out to locate a buffer
PMU Post Code	
0xA1F9	Failed PMU training.
PSP V1 Modules	
0xA501	PspPeiV1 entry
0xA502	PspPeiV1 exit
0xA503	MemoryDiscoveredPpiCallback entry
0xA504	MemoryDiscoveredPpiCallback exit
0xA507	PspDxeV1 entry
0xA508	PspDxeV1 exit

0xA50A	PspDxeV1 PspPciEnumerationCompleteCallBack entry
0xA50B	PspDxeV1 PspPciEnumerationCompleteCallBack exit
0xA50C	PspDxeV1 ready to boot entry
0xA50D	PspDxeV1 ready to boot exit
0xA50E	PspSmmV1 entry
0xA50F	PspSmmV1 exit
0xA510	PspSmmV1 SwSmiCallBack entry, build the S3 save area for resume
0xA511	PspSmmV1 SwSmiCallBack exit, build the S3 save area for resume
0xA512	PspSmmV1 BspSmmResumeVector entry
0xA513	PspSmmV1 BspSmmResumeVector exit
0xA514	PspSmmV1 ApSmmResumeVector entry
0xA515	PspSmmV1 ApSmmResumeVector exit
0xA516	PspP2CmboxV1 entry
0xA517	PspP2CmboxV1 exit
PSP V2 Modules	
0xA521	PspPeiV2 entry
0xA522	PspPeiV2 exit
0xA523	PspDxeV2 entry
0xA524	PspDxeV2 exit
0xA525	PspDxeV2 PspMpServiceCallBack entry
0xA526	PspDxeV2 PspMpServiceCallBack exit
0xA527	PspDxeV2 FlashAccCallBack entry
0xA528	PspDxeV2 FlashAccCallBack exit
0xA529	PspDxeV2 ready to boot entry
0xA52A	PspDxeV2 ready to boot exit
0xA52B	PspDxeV2 exit boot serivce entry
0xA52C	PspDxeV2 exit boot serivce exit
0xA52D	PspSmmV2 entry
0xA52E	PspSmmV2 exit
0xA52F	PspSmmV2 SwSmiCallBack entry, build the S3 save area for resume
0xA530	PspSmmV2 SwSmiCallBack exit, build the S3 save area for resume
0xA531	PspSmmV2 BspSmmResumeVector entry
0xA532	PspSmmV2 BspSmmResumeVector exit
0xA533	PspSmmV2 ApSmmResumeVector entry
0xA534	PspSmmV2 ApSmmResumeVector exit
0xA535	PspP2CmboxV2 entry
0xA536	PspP2CmboxV2 exit
0xA537	TpPspRecoverApcbFail
0xA539	PspDxeV2 ApcbAccCallBack entry
0xA53A	PspDxeV2 ApcbAccCallBack exit
0xA53B	Enable Rd Instruction Fail
0xA53C	ScpcAutoEnablement failed due a variable with larger size detected
0xA53D	ScpcAutoEnablement failed due SetVariable
0xA53E	ScpcAutoEnablement failed due delete variable
0xA53F	C2P mailbox status field return with error, non-zero value

PSP fTpm modules	
0xA540	PspfTpmPei entry
0xA541	PspfTpmPei exit
0xA542	PspfTpmPei memory callback entry
0xA543	PspfTpmPei memory callback exit
0xA544	PspfTpmDxe entry
0xA545	PspfTpmDxe exit
PSP dTpm modules	
0xA546	PspdTpmPei entry
0xA547	PspdTpmPei exit
HSP fTpm modules	
0xA548	HspfTpmPei entry
0xA549	HspfTpmPei exit
0xA54A	HspfTpmPei Initialize Entry
0xA54B	HspfTpmPei Initialize Exit
0xA54C	HspfTpmDxe entry
0xA54D	HspfTpmDxe exit
Intrusion Detection [0xA56X]	
0xA560	PspIntrusionDetectionPei Entry
0xA561	PspIntrusionDetectionPei Exit
0xA562	PspIntrusionDetectionDxe Entry
0xA563	PspIntrusionDetectionDxe Exit
0xA564	Psp DoIntrusionDetectionAction in Dxe
0xA565	Psp IntrusionDetection Clear Tpm
0xA566	PspIntrusionDetectionSmm Entry
0xA567	PspIntrusionDetectionSmm Exit
0xA568	Psp IntrusionDetectionSmiCallback
0xA569	Psp DoIntrusionDetectionAction in Smm
0xA56E	Psp Intrusion Event Logging Error
0xA56F	Psp Intrusion Get Event Log Error
0xA570	Psp has got Async Cmd from the mailbox, but the routine is still running now
P2C mailbox Handling [0xA59X]	
0xA591	PspP2Cmbox Command SpiGetAttrib Handling entry
0xA592	PspP2Cmbox Command SpiSetAttrib Handling entry
0xA593	PspP2Cmbox Command SpiGetBlockSize Handling entry
0xA594	PspP2Cmbox Command SpiReadFV Handling entry
0xA595	PspP2Cmbox Command SpiWriteFV Handling entry
0xA596	PspP2Cmbox Command SpiEraseFV Handling entry
0xA598	PspP2Cmbox Command MboxPspCmdRpmcIncMc entry
0xA599	PspP2Cmbox Command TpMboxPspCmdRpmcReqMc entry
0xA59A	PspP2Cmbox Command TpMboxPspCmdArsStatus entry
0xA59B	PspP2Cmbox Command TpMboxPspCmdAsyncCmdDone entry
0xA59E	PspP2Cmbox Command Handling exit
0xA59F	PspP2Cmbox Command Handling Fail exit

fTPM command Handling [0xA5FX]	
0xA5F0	PspfTpm send TPM command entry
0xA5F1	PspfTpm send TPM command exit
0xA5F2	PspfTpm receive TPM command entry
0xA5F3	PspfTpm receive TPM command exit
0xA5F4	HspfTpm send TPM command entry
0xA5F5	HspfTpm send TPM command exit
0xA5F6	HspfTpm receive TPM command entry
0xA5F7	HspfTpm receive TPM command exit
C2P mailbox Handling [0xA601 ~ 0xA67F: before send C2P command, 0xA681 ~ 0xA6FF: wait C2P command]	
0xA600	PSP C2P mailbox entry base [0xA600 | Cmd]
0xA600	C2P command done, post code reused from TpPspC2PmboxBeforeSendCmdBase
0xA601	Before send C2P command MboxBiosCmdDramInfo
0xA602	Before send C2P command MboxBiosCmdSmmInfo
0xA603	Before send C2P command MboxBiosCmdSxInfo
0xA604	Before send C2P command MboxBiosCmdRsmInfo
0xA605	Before send C2P command MboxBiosCmdFtpmQuery
0xA606	Before send C2P command MboxBiosCmdBootDone
0xA607	Before send C2P command MboxBiosCmdClearS3Sts
0xA608	Before send C2P command MboxBiosS3DataInfo
0xA609	Before send C2P command MboxBiosCmdNop
0xA614	Before send C2P command MboxBiosCmdHSTIQuery
0xA619	Before send C2P command MboxBiosCmdGetVersion
0xA61B	Before send C2P command MboxBiosCmdLockDFReg
0xA61C	Before send C2P command MboxBiosCmdClrSmmLock
0xA61D	Before send C2P command MboxBiosCmdSetApCsBase
0xA61E	Before send C2P command MboxBiosCmdKvmInfo
0xA61F	Before send C2P command MboxBiosCmdLockSpi
0xA620	Before send C2P command MboxBiosCmdScreenOnGpio
0xA621	Before send C2P command MboxBiosCmdSpiOpWhiteList
0xA622	Before send C2P command MboxBiosCmdRasEinj
0xA624	Before send C2P command MboxBiosCmdStartArs
0xA625	Before send C2P command MboxBiosCmdStopArs
0xA626	Before send C2P command MboxBiosCmdSetBootPartitionId
0xA627	Before send C2P command MboxBiosCmdPspCapsQuery
0xA628	Before send C2P command MboxBiosCmdArmorEnterSmmOnlyMode
0xA629	Before send C2P command MboxBiosCmdArmorEnforceWhitelist
0xA62A	Before send C2P command MboxBiosCmdArmorExecuteSpiCommand
0xA62B	0xA62B
0xA62C	Before send C2P command MboxBiosCmdDrtmInfoId
0xA62D	Before send C2P command MboxBiosCmdLaterSplFuse
0xA62E	Before send C2P command MboxBiosCmdDtpmInfo
0xA62F	Before send C2P command MboxBiosCmdValidateManOsSignature
0xA630	Before send C2P command MboxBiosCmdLockFCHReg
0xA631	Before send C2P command MboxBiosCmdPostDrtmInfoQuery

0xA634	Before send C2P command MboxBiosCmdSignValidateHmacDataPre Smm
0xA635	Before send C2P command MboxBiosCmdSignValidateHmacDataS mm
0xA636	Before send C2P command MboxBiosCmdGetBootPartitionId
0xA639	Before send C2P command MboxBiosCmdSetRpmcAddress
0xA63A	Before send C2P command MboxBiosCmdSetGpioFencing
0xA63F	Before send C2P command MboxBiosCmdSendIvrsAcpiTable
0xA640	Before send C2P command MboxBiosCmdTa
0xA641	Before send C2P command MboxBiosCmdAcpiRasEinj
0xA642	Before send C2P command MboxBiosCmdQueryTCGLog
0xA647	Before send C2P command MboxBiosCmdQuerySplFuse
0xA649	Before send C2P command MboxBiosCmdManageabilityCfg
0xA64A	Before send C2P command MboxBiosCmdDisablePsb
0xA64B	Before send C2P command MboxBiosCmdUsbConfig
0xA64D	Before send C2P command MboxBiosCmdMpmPciAccess
0xA64F	Before send C2P command MboxBiosCmdStbVerbosity
0xA650	Before send C2P command MboxBiosCmdArmorEnterSmmOnlyMode2
0xA651	Before send C2P command MboxBiosCmdArmorSpiTransaction
0xA652	Before send C2P command MboxBiosCmdDeferredPsbFuse
0xA653	Before send C2P command MboxBiosCmdLoadWlanFw
0xA654	Before send C2P command MboxBiosCmdQuerySplValue
0xA680	PSP C2P mailbox exit base [0xA680 | Cmd]
0xA681	Wait C2P command MboxBiosCmdDramInfo finished
0xA682	Wait C2P command MboxBiosCmdSmmInfo finished
0xA683	Wait C2P command MboxBiosCmdSxInfo finished
0xA684	Wait C2P command MboxBiosCmdRsmInfo finished
0xA685	Wait C2P command MboxBiosCmdFtpmQuery finished
0xA686	Wait C2P command MboxBiosCmdBootDone finished
0xA687	Wait C2P command MboxBiosCmdClearS3Sts finished
0xA688	Wait C2P command MboxBiosS3DataInfo finished
0xA689	Wait C2P command MboxBiosCmdNop finished
0xA694	Wait C2P command MboxBiosCmdHSTIQuery finished
0xA699	Wait C2P command MboxBiosCmdGetVersion finished
0xA69B	Wait C2P command MboxBiosCmdLockDFReg finished
0xA69C	Wait C2P command MboxBiosCmdClrSmmLock finished
0xA69D	Wait C2P command MboxBiosCmdSetApCsBase finished
0xA69E	Wait C2P command MboxBiosCmdKvmInfo finished
0xA69F	Wait C2P command MboxBiosCmdLockSpi finished
0xA6A0	Wait C2P command MboxBiosCmdScreenOnGpio finished
0xA6A1	Wait C2P command MboxBiosCmdSpiOpWhiteList finished
0xA6A2	Wait C2P command MboxBiosCmdRasEinj finished
0xA6A4	Wait C2P command MboxBiosCmdStartArs finished
0xA6A5	Wait C2P command MboxBiosCmdStopArs finished
0xA6A6	Wait C2P command MboxBiosCmdSetBootPartitionId finished
0xA6A7	Wait C2P command MboxBiosCmdPspCapsQuery finished
0xA6A8	Wait C2P command MboxBiosCmdArmorEnterSmmOnlyMode finished

0xA6A9	Wait C2P command MboxBiosCmdArmorEnforceWhitelist finished
0xA6AA	Wait C2P command MboxBiosCmdArmorExecuteSpiCommand finished
0xA6AB	Wait C2P command MboxBiosCmdArmorSwitchCsMode finished
0xA6AC	Wait C2P command MboxBiosCmdDrtmInfoId finished
0xA6AD	Wait C2P command MboxBiosCmdLaterSplFuse finished
0xA6AE	Wait C2P command MboxBiosCmdDtpmInfo finished
0xA6AF	Wait C2P command MboxBiosCmdValidateManOsSignature finished
0xA6B0	Wait C2P command MboxBiosCmdLockFCHReg finished
0xA6B1	Wait C2P command MboxBiosCmdPostDrtmInfoQuery finished
0xA6B4	Wait C2P command MboxBiosCmdSignValidateHmacDataPreSmm finished
0xA6B5	Wait C2P command MboxBiosCmdSignValidateHmacDataSmm finished
0xA6B6	Wait C2P command MboxBiosCmdGetBootPartitionId finished
0xA6B9	Wait C2P command MboxBiosCmdSetRpmcAddress finished
0xA6BA	Wait C2P command MboxBiosCmdSetGpioFencing finished
0xA6BF	Wait C2P command MboxBiosCmdSendIvrsAcpiTable finished
0xA6C0	Wait C2P command MboxBiosCmdTa finished
0xA6C1	Wait C2P command MboxBiosCmdAcpiRasEinj finished
0xA6C2	Wait C2P command MboxBiosCmdQueryTCGLog finished
0xA6C7	Wait C2P command MboxBiosCmdQuerySplFuse finished
0xA6C9	Wait C2P command MboxBiosCmdManageabilityCfg finished
0xA6CA	Wait C2P command MboxBiosCmdDisablePsb finished
0xA6CB	Wait C2P command MboxBiosCmdUsbConfig finished
0xA6CD	Wait C2P command MboxBiosCmdMpmPciAccess finished
0xA6CF	Wait C2P command MboxBiosCmdStbVerbosity finished
0xA6D0	Wait C2P command MboxBiosCmdArmorEnterSmmOnlyMode2 finished
0xA6D1	Wait C2P command MboxBiosCmdArmorSpiTransaction finished
0xA6D2	Wait C2P command MboxBiosCmdDeferredPsbFuse finishe
0xA6D3	Wait C2P command MboxBiosCmdLoadWlanFw finished
0xA6D4	Wait C2P command MboxBiosCmdQuerySplValue finished
MPM related [0xA700 - 0xA77F]	
0xA700	MpmPei Driver entry
0xA701	MpmPei Driver exit
0xA702	MpmDxe Driver entry
0xA703	MpmDxe Driver exit
0xA704	MPM RTB event entry
0xA705	MPM RTB event exit
0xA706	Mpm SerialIo Entry
0xA707	Mpm SerialIo Exit
0xA708	TpMpmMoselleDxe Driver Entry
0xA709	TpMpmMoselleDxe Driver Exit
USB4 related [0xA780 - 0xA79F]	
0xA780	Usb4Pei Driver entry
0xA781	Usb4Pei Driver exit
0xA782	Usb4Pei MemoryDicoverPpiCallback entry

0xA783	Usb4Pei MemoryDicoverPpiCallback exit
0xA784	Usb4Dxe Driver entry
0xA785	Usb4Dxe Driver exit
[0xA900, 0xA94F] NBIO PEIM/DXE Driver	
0xA900	AmdNbioBase PEIM driver entry
0xA901	AmdNbioBase PEIM driver exit
0xA902	AmdNbioBase DXE driver entry
0xA903	AmdNbioBase DXE driver exit
PCIe	
0xA904	AmdNbioPcie PEIM driver entry
0xA905	AmdNbioPcie PEIM driver exit
0xA906	AmdNbioPcie DXE driver entry
0xA907	AmdNbioPcie DXE driver exit
GFX	
0xA908	AmdNbioGfx PEIM driver entry
0xA909	AmdNbioGfx PEIM driver exit
0xA90A	AmdNbioGfx DXE driver entr
0xA90B	AmdNbioGfx DXE driver exit
IOMMU	
0xA90C	AmdNbioIommu DXE driver entry
0xA90D	AmdNbioIommu DXE driver exit
ALIB	
0xA90E	AmdNbioALIB DXE driver entry
0xA90F	AmdNbioALIB DXE driver exit
SMU	
0xA910	AmdSmu PEI driver entry
0xA911	AmdSmu PEI driver exit
0xA912	AmdSmu DXE driver entry
0xA913	AmdSmu DXE driver exit
0xA914	SmuServiceRequest entry
0xA915	SmuServiceRequest exit
IOAPIC	
0xA916	AmdNbioIoApic PEI driver entry
0xA917	AmdNbioIoApic PEI driver exit
IOMMU PEIM	
0xA920	AmdNbioIommu PEIM driver entry
0xA921	AmdNbioIommu PEIM driver exit
APCB DXE	
0xA922	APCB DXE Entry
0xA923	APCB DXE Exit
APCB SMM	
0xA924	APCB SMM Entry
0xA925	APCB SMM Exit
0xA930	Early Exit
0xA931	Early Exit
0xA932	Early Training is completed

[0xA950, 0xA99F] NBIO PPI/PROTOCOL Callback	
0xA950	NbioTopologyConfigureCallback entry
0xA951	NbioTopologyConfigureCallback exit
0xA952	MemoryConfigDoneCallbackPpi entry
0xA953	MemoryConfigDoneCallbackPpi exit
0xA954	DxioInitializationCallbackPpi entry
0xA955	DxioInitializationCallbackPpi exit
0xA956	DispatchSmuV9Callback entry
0xA957	DispatchSmuV9Callback exit
0xA958	DispatchSmuV10Callback entry
0xA959	DispatchSmuV10Callback exit
0xA95A	AmdPcieMiscInit Event entry
0xA95B	AmdPcieMiscInit Event exit
0xA95C	NbioBaseHookReadyToBoot Event entry
0xA95D	NbioBaseHookReadyToBoot Event exit
0xA95E	NbioBaseHookPciIO Event entry
0xA95F	NbioBaseHookPciIO Event exit
0xA960	DispatchSmuV13Callback entry
0xA961	DispatchSmuV13Callback exit
[0xA980, 0xA99F] BR GNB task	
0xA970	GnbEarlyInterfaceCZ entry
0xA971	GnbEarlyInterfaceCZ exit
0xA972	PcieConfigurationInit entry
0xA973	PcieConfigurationInit exit
0xA974	GnbEarlierInterfaceCZ entry
0xA975	GnbEarlierInterfaceCZ exit
0xA976	PcieEarlyInterfaceCZ entry
0xA977	PcieEarlyInterfaceCZ exit
0xA978	PciePostEarlyInterfaceCZ entry
0xA979	PciePostEarlyInterfaceCZ exit
0xA97A	GfxConfigPostInterfaceCZ entry
0xA97B	GfxConfigPostInterfaceCZ exit
0xA97C	GfxPostInterfaceCZ entry
0xA97D	GfxPostInterfaceCZ exit
0xA97E	GnbPostInterfaceCZ entry
0xA97F	GnbPostInterfaceCZ exit
0xA980	PciePostInterfaceCZ entr
0xA981	PciePostInterfaceCZ exit
0xA982	GnbEnvInterfaceCZ entry
0xA983	GnbEnvInterfaceCZ exit
0xA984	GfxConfigEnvInterface entry
0xA985	GfxConfigEnvInterface exit
0xA986	GfxEnvInterfaceCZ entry
0xA987	GfxEnvInterfaceCZ exit
0xA988	GfxMidInterfaceCZ entry
0xA989	GfxMidInterfaceCZ exit
0xA98A	GfxIntInfoTableInterfaceCZ entry

0xA98B	GfxIntInfoTableInterfaceCZ exit
0xA98C	PcieMidInterfaceCZ entry
0xA98D	PcieMidInterfaceCZ exit
0xA98E	GnbMidInterfaceCZ entry
0xA98F	GnbMidInterfaceCZ exit
0xA990	GnbSmuMidInterfaceCZ entry
0xA991	GnbSmuMidInterfaceCZ exit
0xA992	InvokeAmdInitLate entry
0xA993	InvokeAmdInitLate exit
[0xAA80, 0xAAAF] Alib task	
0xAA80	ALib 0 entry
0xAA81	ALib 0 exit
0xAA82	ALib 1 entry
0xAA83	ALib 1 exit
0xAA84	ALib 2 entry
0xAA85	ALib 2 exit
0xAA86	ALib 3 entry
0xAA87	ALib 3 exit
0xAA88	ALib 6 entry
0xAA89	ALib 6 exit
0xAA8A	ALib A entry
0xAA8B	ALib A exit
0xAA8C	ALib B entry
0xAA8D	ALib B exit
0xAA8E	ALib C entry
0xAA8F	ALib C exit
0xAA90	ALib 10 entry
0xAA91	ALib 10 exit
0xAA92	ALib 11 entry
0xAA93	ALib 11 exit
0xAA94	ALib 12 entry
0xAA95	ALib 12 exit
0xAA96	ALib 13 entry
0xAA97	ALib 13 exit
0xAA98	ALib AA entry
0xAA99	ALib AA exit
[0xACXX] assigned for AGESA CCX Module	
0xAC10	CCX IDS IDS_HOOK_CCX_AFTER_AP_LAUNCH
0xAC50	CCX PEI entry
0xAC51	CCX downcore entry
0xAC55	CCX DXE entry
0xAC56	CCX MP service callback entry
0xAC57	CCX Ready To Boot callback entry
0xAC58	CCX oc service callback entry
0xAC5D	CCX SMM entry
0xAC70	CCX PEI start to launch APs for S3
0xAC71	CCX PEI end of launching APs for S3
0xAC90	CCX start to launch AP

0xAC91	CCX launch AP is ended
0xAC92	CCX launch AP abort
0xAC93	CCX MP service abort
0xAC94	CCX cac weights
0xAC95	CCX before install CcxDone
0xAC96	CCX after install CcxDone
0xAC97	CCX loaded microcode
0xACE0	CCX PEI exit
0xACE1	CCX downcore exit
0xACE5	CCX DXE exit
0xACE6	CCX MP service callback exit
0xACE7	CCX Ready To Boot callback exit
0xACE8	CCX OC service callback exit
0xACED	CCX SMM exit
[0xADXX] assigned for AGESA DF Module	
0xAD50	DF PEI entry
0xAD55	DF DXE entry
0xAD56	DF Ready to Boot entry
0xAD57	DF NbioSmuServicesPpiCallback entry
0xAD58	DF NbioSmuServicesProtocolCallback entry
0xAD59	DF SMM entry
0xAD60	DF FabricPciEnumerationCompleteCallBack entry
0xADE0	DF PEI exit
0xADE5	DF DXE exit
0xADE6	DF Ready to Boot exit
0xADE7	DF NbioSmuServicesPpiCallback exit
0xADE8	DF NbioSmuServicesProtocolCallback exit
0xADE9	DF SMM exit
0xADEA	DF FabricPciEnumerationCompleteCallBack exit
FCH	
0xAF01	FCH InitReset dispatch point
0xAF06	FCH InitEnv dispatch point
0xAF07	FCH InitMid dispatch point
0xAF08	FCH InitLate dispatch point
0xAF0B	FCH InitS3Early dispatch point
0xAF0C	FCH InitS3Late dispatch point
0xAF0D	FCH InitS3Early dispatch finished
0xAF0E	FCH InitS3Late dispatch finished
0xAF10	FCH Pei Entry
0xAF11	FCH Pei Exit
0xAF12	FCH MultiFch Pei Entry
0xAF13	FCH MultiFch Pei Exit
0xAF14	0xAF14
0xAF15	FCH Dxe Exit
0xAF16	FCH MultiFch Dxe Entry
0xAF17	FCH MultiFch Dxe Exit
0xAF18	FCH Smm Entry
0xAF19	FCH Smm Exit

0xAF20	FCH Smm Dispatcher Entry
0xAF21	FCH Smm Dispatcher Exit
0xAF40	FCH InitReset HwAcpi
0xAF41	FCH InitReset AB Link
0xAF42	FCH InitReset LPC
0xAF43	FCH InitReset SPI
0xAF44	FCH InitReset eSPI
0xAF45	FCH InitReset SD
0xAF46	FCH InitReset eMMC
0xAF47	FCH InitReset SATA
0xAF48	FCH InitReset USB
0xAF49	FCH InitReset xGbE
0xAF4A	FCH InitReset USB Ready
0xAF4B	FCH InitReset USB4 Ready
0xAF4E	FCH InitReset USB4
0xAF4F	FCH InitReset HwAcpiP
0xAF50	FCH InitEnv HwAcpi
0xAF51	FCH InitEnv AB Link
0xAF52	FCH InitEnv LPC
0xAF53	FCH InitEnv SPI
0xAF54	FCH InitEnv eSPI
0xAF55	FCH InitEnv SD
0xAF56	FCH InitEnv eMMC
0xAF57	FCH InitEnv SATA
0xAF58	FCH InitEnv USB
0xAF59	FCH InitEnv xGbE
0xAF5E	FCH InitEnv USB4
0xAF5F	FCH InitEnv HwAcpiP
0xAF60	FCH InitMid HwAcpi
0xAF61	FCH InitMid AB Link
0xAF62	FCH InitMid LPC
0xAF63	FCH InitMid SPI
0xAF64	FCH InitMid eSPI
0xAF65	FCH InitMid SD
0xAF66	FCH InitMid eMMC
0xAF67	FCH InitMid SATA
0xAF68	FCH InitMid USB
0xAF69	FCH InitMid xGbE
0xAF6E	FCH InitMid USB4
0xAF70	FCH InitLate HwAcpi
0xAF71	FCH InitLate AB Link
0xAF72	FCH InitLate LPC
0xAF73	FCH InitLate SPI
0xAF74	FCH InitLate eSPI
0xAF75	FCH InitLate SD
0xAF76	FCH InitLate eMMC
0xAF77	FCH InitLate SATA
0xAF78	FCH InitLate USB

0xAF79	FCH InitLate xGbE
0xAF7A	FCH PT load FW Entry
0xAF7B	FCH PT load FW Exit
0xAF7C	FCH PT_Plus load FW Entry
0xAF7D	FCH PT_Plus load FW Exit
0xAF7E	0xAF7E
0xAF7F	FCH PT Start to load FW
0xAF80	FCH Device Enter D x Status
0xAF81	FCH PT load FW Delay 1 sec
0xAF82	FCH PT load FW Delay 2 sec
0xAF83	FCH PT load FW Delay 3 sec
0xAF84	FCH PT load FW Delay 4 sec
0xAF85	FCH PT load FW Delay 5 sec
0xAF86	FCH PT load FW Delay 6 sec
0xAF87	FCH PT load FW Delay 7 sec
0xAF88	FCH PT load FW Delay 8 sec
0xAF89	FCH PT load FW Delay 9 sec
0xAF8A	FCH PT load FW Delay 10 sec
0xAF8B	FCH Secondary PT Start to load FW
0xAF90	FCH Turner Load FW Entry
0xAF91	FCH Turner Load FW Exit
0xAF92	FCH Turner Start to Load FW
0xAFB0	Bixby Pei Entry
0xAFB1	Bixby Pei Exit
0xAFB2	Bixby Dxe Entry
0xAFB3	Bixby Dxe Exit
0xAFB4	Bixby Smm Entry
0xAFB5	Bixby Smm Exit
0xAFB6	Bixby InitReset dispatch point
0xAFB7	Bixby InitMid dispatch point
0xAFB8	Bixby InitEnv dispatch point
0xAFB9	Bixby InitLate dispatch point
0xAFBA	Bixby InitS3Early dispatch point
0xAFBB	Bixby InitS3Late dispatch point
0xAFBC	Bixby InitS3Early dispatch finished
0xAFBD	Bixby InitS3Late dispatch finished
0xAFBE	Bixby InitReset SATA Entry
0xAFBF	Bixby InitReset SATA Exit
0xAFC0	Bixby InitMid SATA Entry
0xAFC1	Bixby InitMid SATA Exit
0xAFC2	Bixby InitEnv SATA Entry
0xAFC3	Bixby InitEnv SATA Exit
0xAFC4	Bixby InitLate SATA Entry
0xAFC5	Bixby InitLate SATA Exit
0xAFC6	Bixby InitReset USB Entry
0xAFC7	Bixby InitReset USB Exit
0xAFC8	Bixby InitMid USB Entry
0xAFC9	Bixby InitMid USB Exit

0xAFCA	Bixby InitEnv USB Entry
0xAFCB	Bixby InitEnv USB Exit
0xAFCC	Bixby InitLate USB Entry
0xAFCD	Bixby InitLate USB Exit
0xAFCE	Bixby InitEnv HwAcpiP
0xAFCF	Bixby InitReset HwAcpiP
0xAFFF	End of TP range for FCH
0xFFFF	Last defined AGESA PCs

AMI POST Code

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

0x38	Post-memory North Bridge initialization is started (North Bridge module specific)
0x39	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3A	Post-memory North Bridge initialization is started (North Bridge module specific)
0x3B	Post-memory South Bridge initialization is started
0x3C	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3D	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3E	Post-memory South Bridge initialization is started (South Bridge module specific)
0x3F~0x4E	OEM post memory initialization codes
0x4F	DXE IPL is started
S3 resume progress codes	
0xE0	S3 Resume is started (S3 Resume PPI is called by th DXE IPL)
0xE1	S3 Boot Script execution
0xE2	Video repost
0xE3	OS S3 wake vector call
0xE4~0xE7	Reserved for future AMI progress codes
Recovery Progress Codes	
0xF0	Recovery condition triggered by firmware (Auto recovery)
0xF1	Recovery condition triggered by user (Forced recovery)
0xF2	Recovery process started
0xF3	Recovery firmware image is found
0xF4	Recovery firmware image is loadded
0xF5~0xF7	Reserved for future AMI progress codes
DXE Phase	
0x60	DXE code is started
0x61	NVRAM initialization
0x62	Initialization of the South Bridge runtimes services
0x63	CPU DXE initialization is started
0x64	CPU DXE initialization (CPU module specific)
0x65	CPU DXE initialization (CPU module specific)
0x66	CPU DXE initialization (CPU module specific)
0x67	CPU DXE initialization (CPU module specific)
0x68	PCI host bridge initialization
0x69	North Bridge DXE initialization is started
0x6A	North Bridge DXE SMM initialization is started
0x6B	North Bridge DXE initialization (North Brodge module specific)
0x6C	North Bridge DXE initialization (North Brodge module specific)
0x6D	North Bridge DXE initialization (North Brodge module specific)
0x6E	North Bridge DXE initialization (North Brodge module specific)
0x6F	North Bridge DXE initialization (North Brodge module specific)
0x70	South Bridge DXE initialization is started
0x71	South Bridge DXE SMM initialization is started
0x72	South Bridge devices initialization

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

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

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.