



Elpis

Server Motherboard User's Manual

Table of Contents

Preface	i
Safety Instructions	ii
About This Manual	iii
Chapter 1. Product Features	1
1.1 Components	1
1.2 Specifications	2
1.3 Feature	3
Chapter 2. Hardware Setup	4
2.1 Central Processing Unit Setup	4
2.1.1 Processor Installation	4
2.2 System Memory Setup	7
2.2.1 DIMM Installation	7
2.2.2 DIMM Population	8
Chapter 3. Motherboard Settings	9
3.1 Motherboard Block Diagram	9
3.2 Content List	10
3.3 Connector and Jumper	11
3.3.1 Placement	11
3.4 Connector and Jumper Pin Definition	12
3.4.1 Connector	12
3.4.2 Jumper	15
3.4 LED Indicator	16
Chapter 4. BIOS Configuration Settings	17
4.1 Navigation Keys	17
4.2 BIOS Setup	18
4.2.1 BIOS Menu	18
4.2.2 BIOS Basic Utility	18
4.2.3 BIOS Update	20
4.3 Main	22
4.4 AMD CBS	23
4.4.1 CPU Common Options	23
4.4.2 DF Common Options	25
4.4.3 UMC Common Options	27

4.4.4 NBIO Common Options	34
4.4.5 FCH Common Options	39
4.4.5 NTB Common Options	40
4.4.6 Soc Miscellaneous Control.....	40
4.4.7 BIXBY Common Options.....	41
4.5 Advanced	42
4.5.1 Demo Board.....	42
4.5.2 USB Configuration.....	42
4.5.3 CPU Related setting	43
4.5.4 PCI SubSystem Setting.....	43
4.5.5 OEMBoard Function	43
4.5.6 H2O IPMI Configuration.....	43
4.5.7 SIO AST2500/2520	44
4.6 Security	45
4.6.1 H2O IPMI Configuration.....	45
4.7 Power	46
4.7.1 Auto Wake on S5.....	46
4.8 Boot	47
4.9 Exit.....	49
Chapter 5. Technical Support.....	50

Document Release History

Release Date	Version	Update Content
April, 2022	1	User's Manual release to public.
June, 2025	1.1	Update connector image.



Copyright © 2022 AIC®, Inc. All Rights Reserved.

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

Preface

Copyright

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

Trademarks

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

Changes

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

Warning

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

Disclaimer

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

Instruction Symbols

Special attention should be given to the instruction symbols below.



NOTE

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



CAUTION

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



WARNING

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

Safety Instructions

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 Elpis Serverboard.

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 Elpis motherboard. For the latest version of this user's manual, please refer to the AIC® website: <https://www.aicipc.com/en/productdetail/51284>.

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. Elpis is an ideal server grade motherboard that is specifically designed to accommodate diverse enterprises for managing heavy workloads, databases, nearline applications, and cloud deployments. This product supports Single AMD EPYC™ 7003/7002/7001 processor (Milan/Rome/Naples) with SP3 socket type and a memory support of 8 DDR4 3200/2933MHz RDIMM/LRDIMM 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 placement of each connector and jumper.

Chapter 4 BIOS Configuration Settings

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

Chapter 5 BMC Configuration Settings

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

Chapter 6 Technical Support

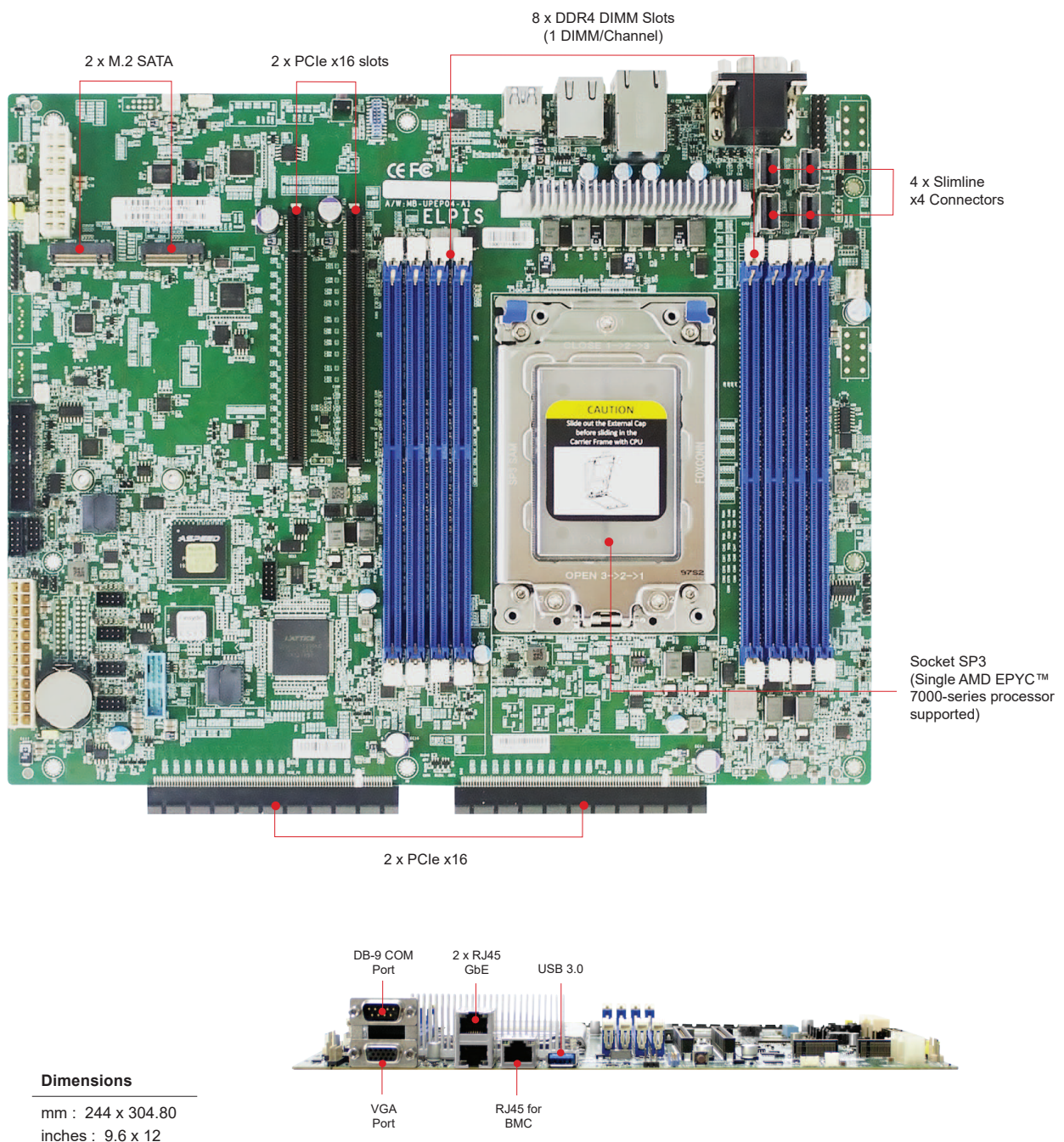
For more information or suggestion, please contact the nearest AIC® corporation representative in your district or visit the AIC® website: <https://www.aicipc.com/en/index>. It is our greatest honor to provide the best service for our customers.

Chapter 1. Product Features

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

1.1 Components

Elpis Serverboard



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

1.2 Specifications

System	Processor Support	Single AMD EPYC™ 7003/7002/7001 processor	On-board Devices	Network Controller	• 2 x Intel I210 Ethernet Controller support dual ports 1GbE with RJ45 connectors on rear I/O • Realtek RTL8211E for BMC dedicated management port
	CPU TDP	280W (support by EPYC™ 7003 CPU)		Graphics	Aspeed AST2500 Advanced PCIe Graphics & Remote Management Processor • PCIe VGA/2D Controller • 1920x1200@60Hz 32bpp
	Socket Type	Socket SP3	Input/Output	SATA	AMD CPU Integrated I/O • 2 x M.2 SATA 6.0 Gb/s support RAID 0/1 (by ASMedia ASM1061R)
	System Memory	• DDR4 3200/2933MHz RDIMM/LRDIMM • Total 8 memory slots ; 8 channel • Supports up to 2TB (support by EPYC™ 7003/7002 CPU)		LAN	• 2 x GbE RJ45, and one within BMC shared management • 1 x GbE RJ45 dedicated to BMC management
System BIOS	Expansion Slots	• 4 x Slimline x4 with PCI Express Gen4/Gen3 (Gen4 supported by EPYC™ 7003/7002 CPU) • 2 x PCI Express Gen4/Gen3 x16 slots (Gen4 supported by EPYC™ 7003/7002 CPU) • 2 x PCI Express Gen4/Gen3 x16 front side edge conn. (Gen4 supported by EPYC™ 7003/7002 CPU) • 2 x NGFF(M.2) M Key(2280) support SATA		USB	• 1 x USB 3.0 Type A connectors on rear I/O • 2 x USB 3.0 by onboard by pin header
	BIOS Type	• For EPYC™ 7002/7001 – Insyde UEFI BIOS • For EPYC™ 7003 – AMI UEFI BIOS		VGA	• 1 x external VGA port • 1 x internal VGA pin-header (share with external VGA port)
On-board Devices	BIOS Features	• ACPI • PXE • IPMI KCS interface • SMBIOS • Serial console redirection • PCIe Hotplug • SRIOV • iSCSI • TPM		Serial Port	• 1 x DB-9 for COM port • 1 x internal COM pin-header • 1 x internal LCM (UART type) pin-header
	SATA	AMD CPU Integrated I/O • 2 x M.2 SATA 6.0 Gb/s support RAID 0/1 (by ASMedia ASM1061R)		Others	1 x TPM 2.0 onboard
On-board Devices	BMC	Aspeed AST2500 Advanced PCIe Graphics & Remote Management Processor • Baseboard Management Controller • Intelligent Platform Interface 2.0 (IPMI 2.0) • iKVM, Media Redirection, IPMI over LAN, Serial over LAN • HTML5 • Redfish • SMASH Support			



NOTE

Please refer to the processor type (AMD EPYC™ 7003/7002/7001) on your serverboard for the corresponding firmware information.

- If the AMD processor generation is EPYC™ 7003, the serverboard executes with AMI UEFI BIOS.
- If the AMD processor generation is EPYC™ 7002/7001, the serverboard executes with Insyde UEFI BIOS.

1.3 Feature

The Elpis server board uniquely features the latest single AMD EPYC™ 7003/7002/7001 processor with up to 64 AMD Zen x86 cores and higher memory capacity of 8 slots up to 2TB. Based on AMD Zen microarchitecture, distinguished for 64 cores and 128 threads, AMD Security Root-of-Trust Technology for advanced data protection, and integrating a single processor socket for greater I/O extensions, the server board is genuinely dedicated to offer an ideal choice for pursuing greater bandwidth, reduced power consumption, and scalability in your server.

With the goal of optimization, this product seeks to achieve versatility, system expansion, and easy management. The server board implements PCIe Gen4 slots, PCIe Slimline connectors, SATA (support RAID 0/1) with support for various edge connectors, including COM, VGA, and USB 3.0 ports. Innovatively integrating BIOS Insyde/AMI and Aspeed AST2500 Advanced PCIe Graphics to the server board, Elpis profoundly delivers immediate and efficient control with Onboard Baseboard Management Controller for managing heavy workflow and executing complex operations.

- Supports AMD EPYC™ 7003/7002/7001 processor
- Supports eight DDR4 DIMM slots up to 2TB memory capacity
- Supports two PCI Express Gen4/Gen3 x16 slots(Gen4 supported by EPYC™ 7003/7002 CPU)
- Supports four Slimline x4 with PCI Express Gen4/Gen3(Gen4 supported by EPYC™ 7003/7002 CPU)
- Onboard dual GbE ports come from 2 x Intel® Ethernet Controller I210
- Onboard Baseboard Management Controller for system management and IPMI control
- Embedded components for 5+ year long life

Chapter 2. Hardware Setup

This section describes a simple instruction guide for installing the hardware components on the serverboard system. Turn off and unplug all system and peripheral devices before proceeding.

2.1 Central Processing Unit Setup

The serverboard supports a single AMD EPYC™ 7003/7002/7001 and socket type SP3.

2.1.1 Processor 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

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.

Procedure:

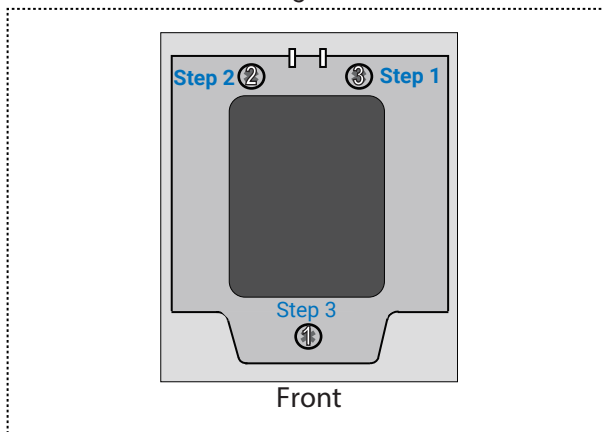
- ① Remove the screw in the order designated in blue (the screw labeled 3⇒2⇒1) as demonstrated in figure 1. After the screws are dislodged, the load plate will automatically be ejected as demonstrated in figure 2.



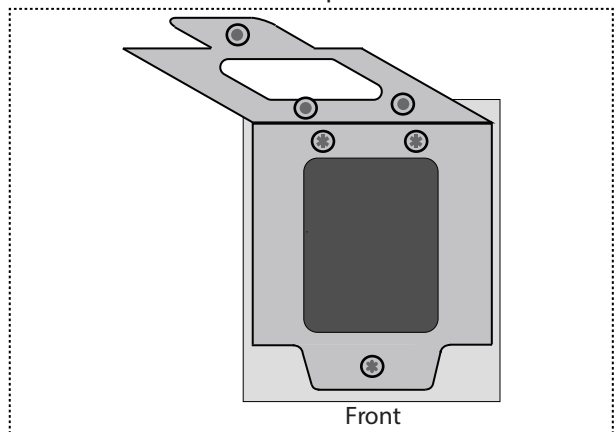
NOTE

The screws cannot be completely removed from the CPU cover.

Dislodge screw

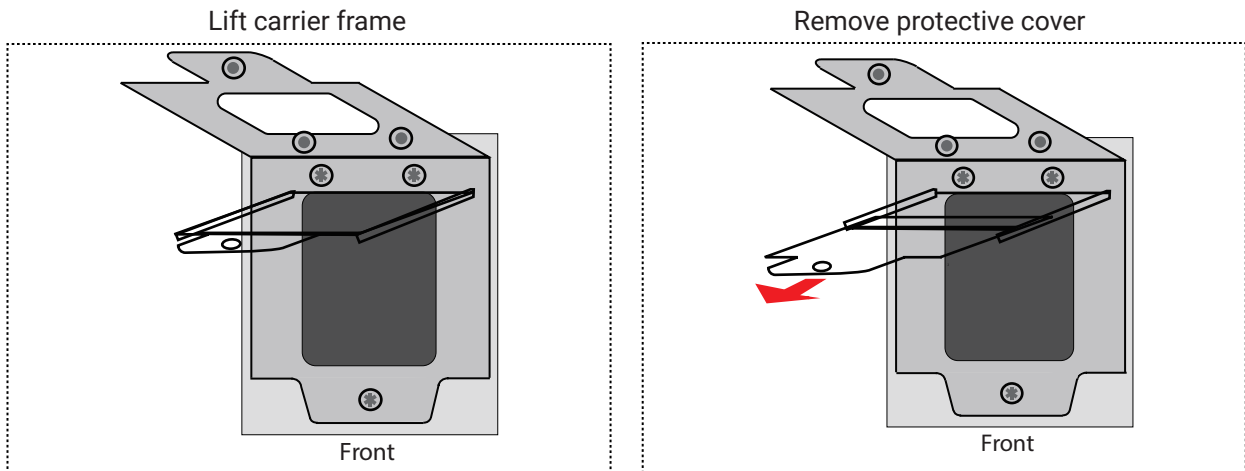


Remove top cover

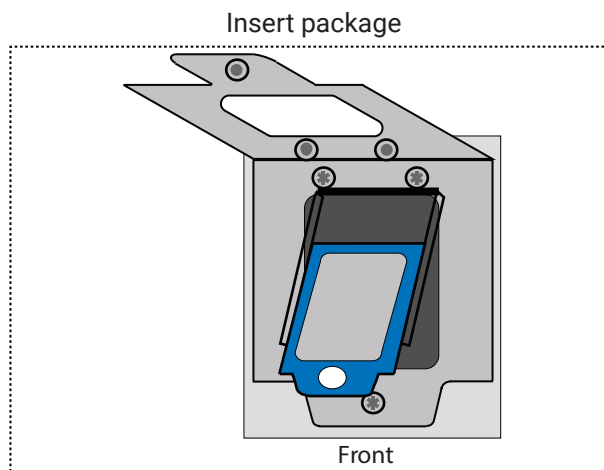


This information is provided for professional technicians only.

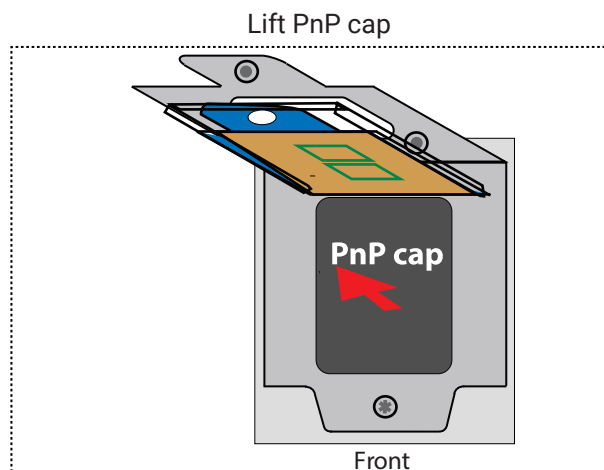
- ② Lift the carrier frame by the blue metal tab and remove the protective cover as demonstrated in figure 3 and figure 4.



- ③ Insert the CPU package into the carrier frame as demonstrated in figure 5.

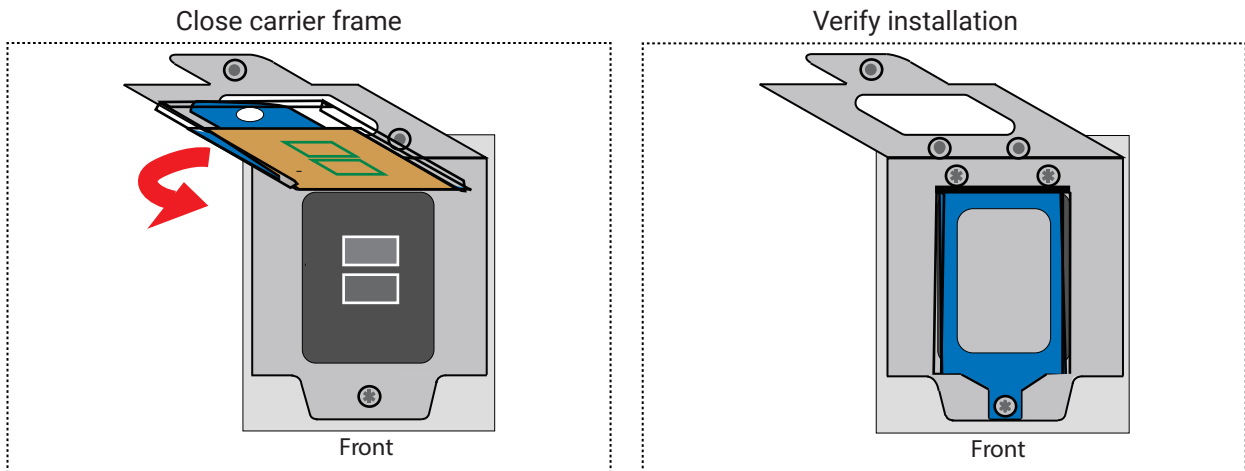


- ④ Remove the Pick and Place (PnP) cap by lifting it upward as demonstrated in figure 6.

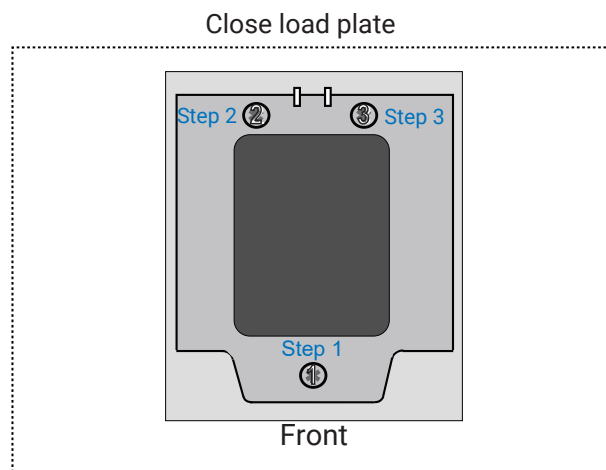


This information is provided for professional technicians only.

- ⑤ Close the carrier frame with the CPU package as demonstrated in figure 7. Check if the frame is properly installed as demonstrated in figure 8.



- ⑥ Close the load plate and fasten the screws in the order 1⇒2⇒3 to complete installation as demonstrated in figure 9.



- ⑦ Apply thermal grease/paste on top of the CPU assembly.
- ⑧ Secure the heatsink on top of the processor assembly to complete installation.



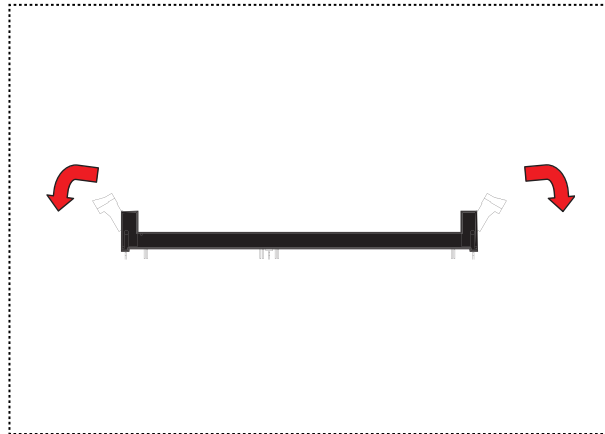
This information is provided for professional technicians only.

2.2 System Memory Setup

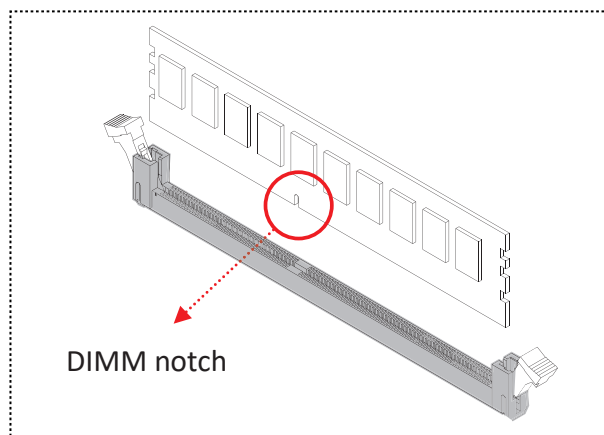
This server board supports 8 DIMM memory slots with 1 DIMM per channel.

2.2.1 DIMM Installation

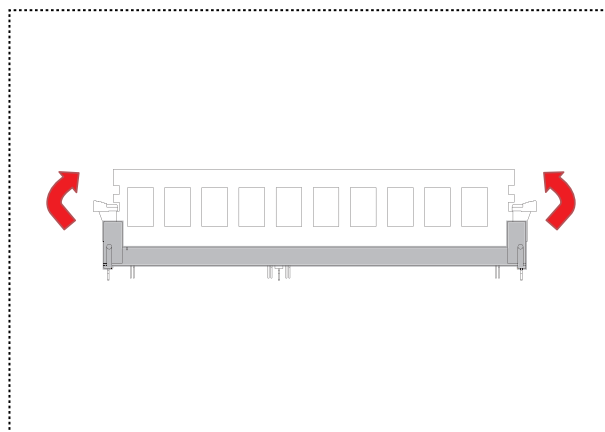
Step 1 Unlock the DIMM socket by pressing the retaining clips outward.



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



Step 3 Close the retaining clips to complete installation.



2.2.2 DIMM Population

The DIMMs are displayed on the Elpis board as DIMMD0, DIMMC0, DIMMB0, DIMMA0, DIMME0, DIMMF0, DIMMG0 and DIMMH0.

To ensure satisfactory performance, you need to:

- ☑ Verify the DIMM type: DDR4 RDIMM/LRDIMM up to 3200/2933MHz
- ☑ Verify if all of the DIMMs installed are of the same DIMM type to avoid memory failure and loss of performance speed.

NOTE



1. Mixing of DIMM base module types within a channel is not supported.
2. Mixing of ECC and non-ECC DIMMs within a channel is not supported.
3. DIMMs with asymmetrical DRAM package types are not supported.

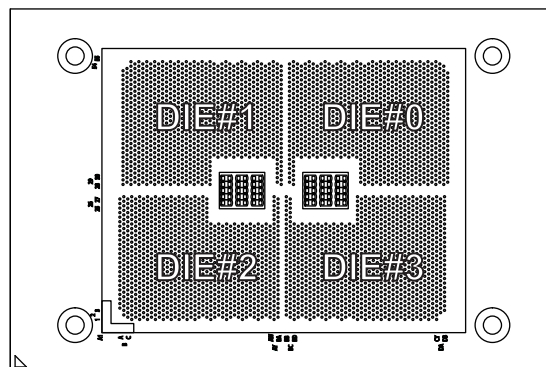
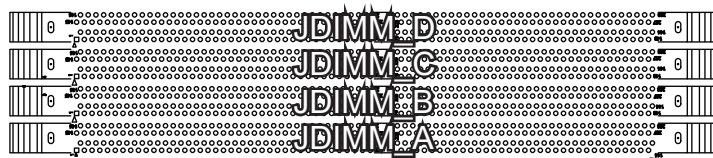
Populate the DIMM slots according to the corresponding Die as suggested to ensure a stable system performance.

Die #0: JDMC0 / JDMD0

Die #1: JDMA0 / JDMB0

Die #2: JDMG0 / JDMH0

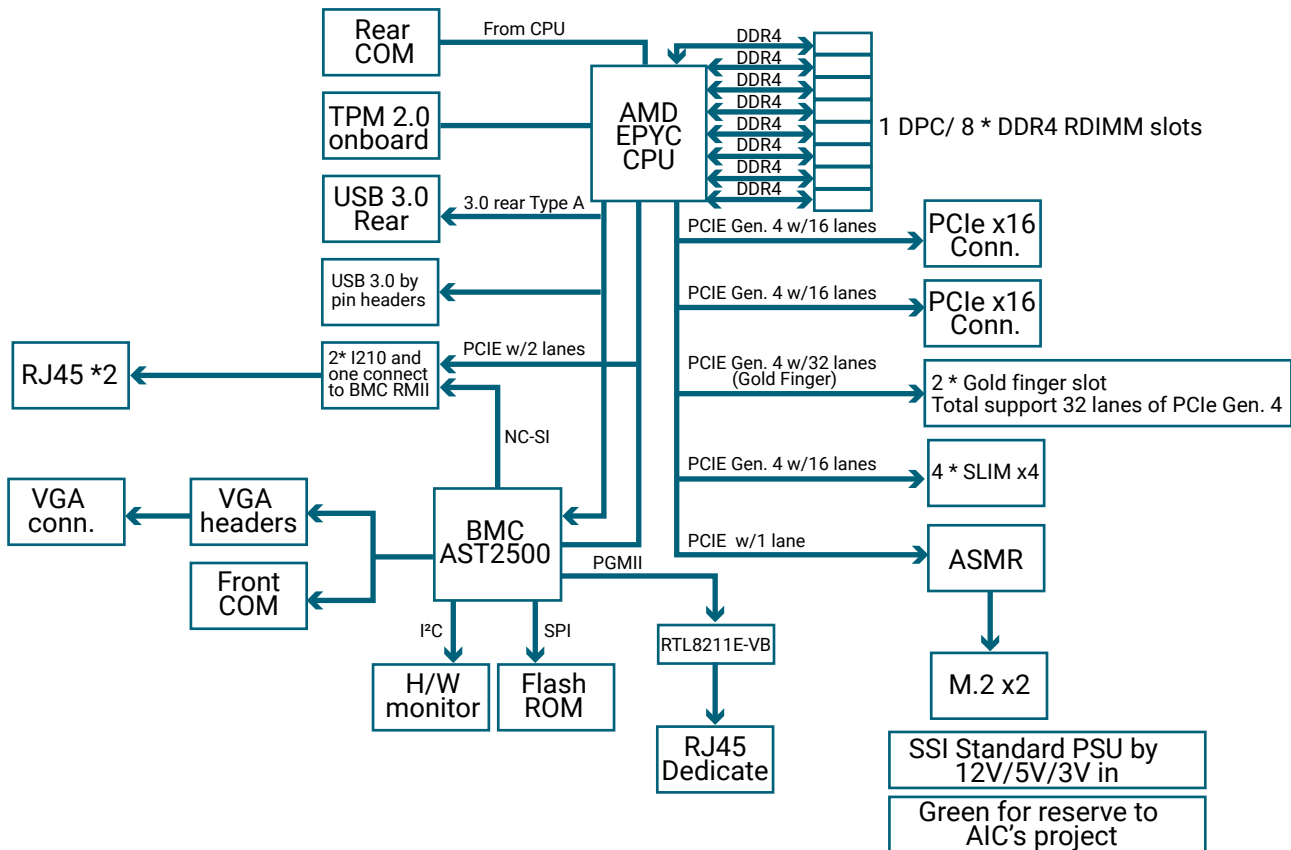
Die #3: JDME0 / JDMF0



Chapter 3. Motherboard Settings

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

3.1 Motherboard Block Diagram

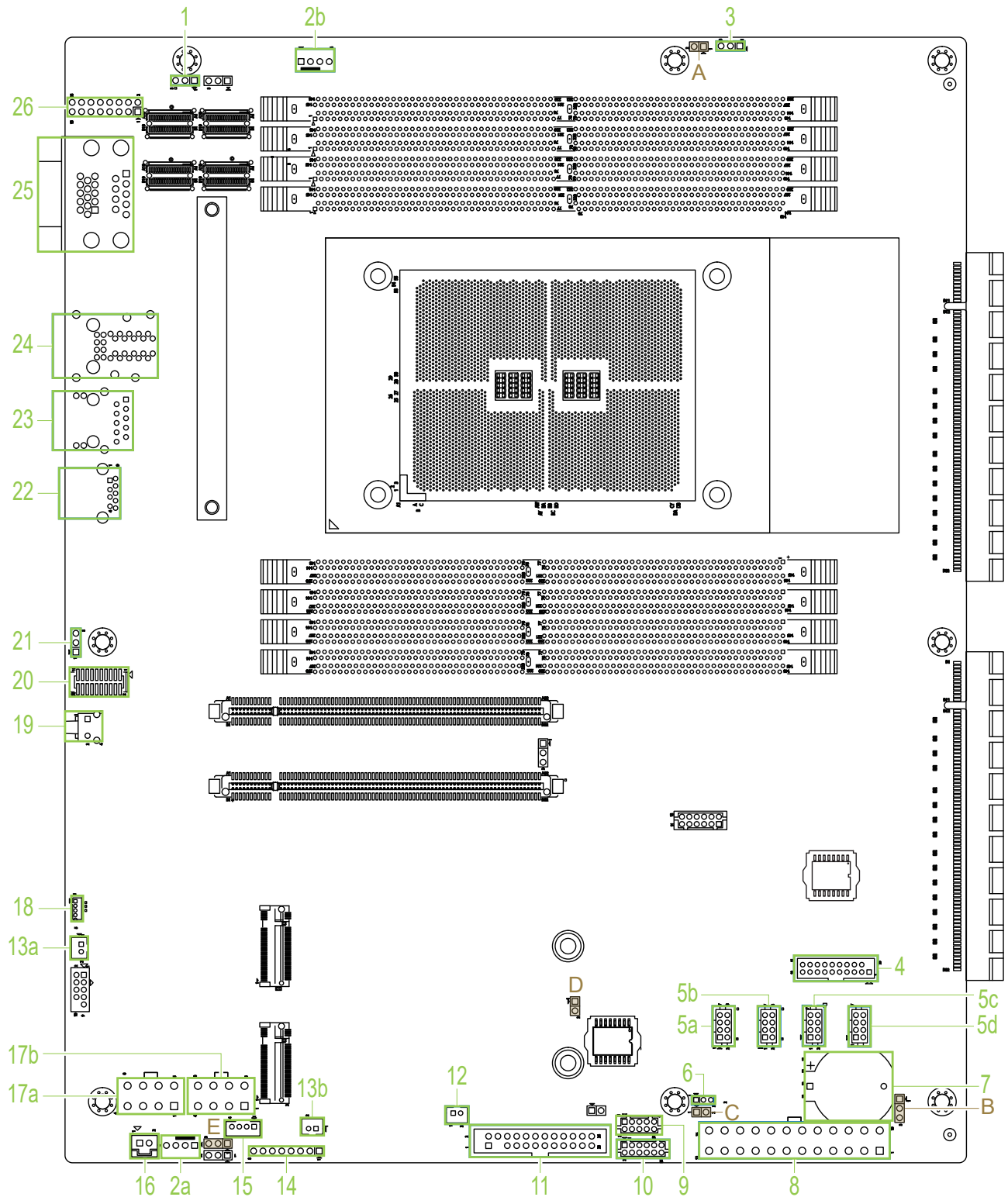


3.2 Content List

Connector and Header		Placement	Connector and Header		Placement
1	Slimline I ² C Header	J14	14	CPLD Program Header	J25
2a 2b	Single Rotor Fan Connector	JFAN5 JFAN6	15	BMC I ² C IPMBus Header	J21
3	CPU I ² C Bus Header	J53	16	Power Button Header	J10
4	USB 2.0/3.0 Header	JUSB1	17a 17b	Power Connector (2x4-pin)	JPWR2 JPWR3
5a 5b 5c 5d	Dual Rotor Fan Connector	JFAN1~4	18	BMC I ² C PMbus Header	J2
6	BMC Console Header	J51	19	Reset Button Header	SW1
7	Battery	BT1	20	JTAG Header	JTAG1
8	Power Connector (2 x12-pin)	JPWR5	21	BMC I2C VRM Program Header	J1
9	LCM Header	JLCM1	22	USB 3.0 Type A Connector	USB1
10	UART Header	J47	23	Single RJ45 tab up Connector supports one 1G LAN	JBMC_LAN2
11	Front Panel Header	FP1	24	Stacked RJ45 Connector supports two 1G LAN	JLAN12
12	Intrusion Header	J31	25	COM port (optional)	DSUB1
13a 13b	Thermal Sensor Header	J3 J26	26	VGA display	JVGA1
Jumper		Placement	Jumper		Placement
A	CPU UART Source Selection Jumper	J48	D	BMC Reset Jumper	J43
B	Clear CMOS Jumper	J60	E	Power Button Pass through mode Jumper	J20
C	CS0 (bit0): Enable CPU Running Jumper	J50			

3.3 Connector and Jumper

3.3.1 Placement

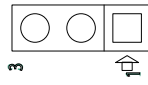


3.4 Connector and Jumper Pin Definition

3.4.1 Connector

1 Slimline I²C Header (J14)

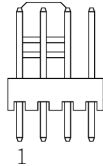
This is a 1x3-pin header that supports PCIe hot plug.



1	SLIMLINE_SCL
2	GND
3	SLIMLINE_SDA

2a ~ 2b Single Fan Rotor Connector (JFAN5 & JFAN6)

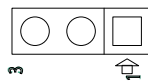
This is a 4-pin connector that supports single fan rotor.



1	GND
2	+12V_S0
3	TACH
4	PWM

3 CPU I²C Bus Header (J53)

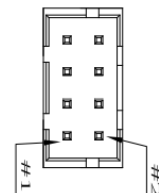
This is a 3-pin header that supports EEPROM and clock buffer.



1	P0_I2C5_CLK
2	GND
3	P0_I2C5_DAT

5a ~ 5b Dual Rotor Fan Connector (JFAN1~JFAN4)

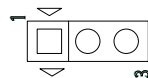
This is a 2x4-pin connector that supports dual fan rotor.



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

6 BMC Console Header (J51)

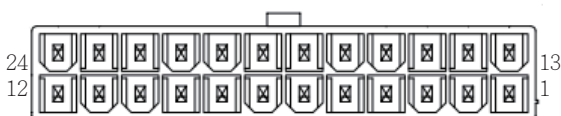
This is a 3-pin header that supports BMC UART console.



1	RS232_TXD5
2	RS232_RXD5
3	GND

8 Power Connector (JPWR5)

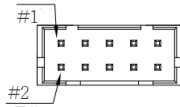
This is a 2x12-pin connector that supports power supply to the motherboard.



+3V3_S0	1	13	+3V3_S0
+3V3_S0	2	14	NC
GND	3	15	GND
+5V_S0	4	16	PS_ON_N
GND	5	17	GND
+5V_S0	6	18	GND
GND	7	19	GND
PS_OK	8	20	NC
+5V_STBY_PSU	9	21	+5V_S0
+12V_S0	10	22	+5V_S0
+12V_S0	11	23	+5V_S0
+3V3_S0	12	24	GND

9 LCM Header (JLCM1)

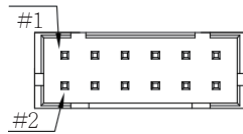
This is a 2x5-pin header that supports LCM (Liquid Display Module).



LED_PWR (5V)	1	2	GND
HDD_ACT_Q_N	3	4	POWER1_5V_RED_N
FP_COLD_RST_N	5	6	POWER1_5V_GREEN_N
LCM_TX_3V3_R	7	8	POWER2_5V_RED_N
LCM_RX_3V3_R	9	10	POWER2_5V_GREEN_N

10 UART Header (J47)

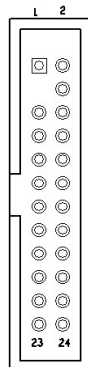
This is a 2x6-pin header that supports UART(Universal Asynchronous Receiver/Transmitter).



SYS_UART_RTS1	1	2	SYS_UART_TXD1
SYS_UART_DTR1	3	4	SYS_UART_RXD1
SYS_UART_DSR1	5	6	SYS_UART_CTS1
GND	7	8	GND
UART_PWR5V	9	10	PWR3V3_RI
SYS_UART_DCD1	11	12	FIO_UART_USBPRSNT_N

11 Front Panel Header (FP1)

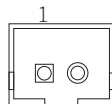
This is a 2x12-pin header that supports the management of switches and controls from the front panel.



PWR_LED_P	1	2	FP_PWR
		4	ID_LED_5V_P
PWR_LED_N	5	6	ID_LED_5V_N
HDD_ACT_P	7	8	SYS_HEALTH1_N
HDD_ACT_N	9	10	SYS_HEALTH2_N
FP_PWR_BTN_N	11	12	LAN1_ACTLED_P
GND	13	14	LAN1_ACTLED_N
FP_COLD_RST_N	15	16	BMC_I2C_08_SDA
GND	17	18	BMC_I2C_08_SCL
FP_BMC_ID_SW_N	19	20	FP_CHASSIS_INTRUSION
NC	21	22	LAN2_ACTLED_P
FP_NMI_BTN_N	23	24	LAN2_ACTLED_N

12 Intrusion Header (J31)

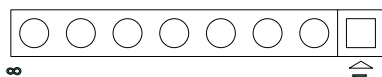
This is a 2-pin header that supports chassis security.



1	FP_CHASSIS_INTRUSION
2	GND

14 CPLD Program Header (J25)

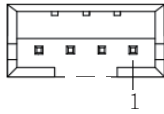
This is a 8-pin header that supports CPLD (Complex Programmable Logic Device) programming.



1	+3V3_STBY_CPLD
2	LCMX02_TDO
3	LCMX02_TDI
4	PU 4.7K to +3V3_STBY_CPLD
5	NC.
6	LCMX02_TMS
7	GND
8	LCMX02_TCK

15 BMC I²C IPMBus Header (J21)

This is a 4-pin IPMBus header that supports BMC I²C bus.



1	BMC_I2C_01_SDA
2	GND
3	BMC_I2C_01_SCL
4	GND by pass 1UF Cap

16 Power Button Header (J10)

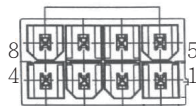
This is a 2-pin header that connects power button cable.



1	FP_PWR_BTN_N
2	GND

17a 17b Power Connector (JPWR2 & JPWR3)

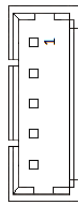
This is a 2x4-pin connector that supports power supply to the processor socket and related memory.



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

18 BMC I²C PMbus Header (J2)

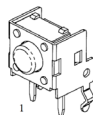
This is a 5-pin PMbus header that supports BMC I²C bus.



1	SMB_PMBUS_CLK
2	SMB_PMBUS_DATA
3	PMBUS_ALERT_N_Q
4	GND
5	NC

19 Reset Button (SW1)

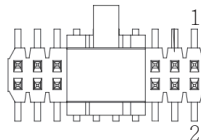
This is a reserved button used to reset the system.



1	FP_COLD_RST_N
2	GND

20 JTAG Header (JTAG1)

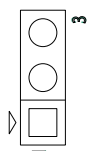
This is a reserved 2x10-pin header that supports CPU JTAG function.



+1V8_S5	1	2	P0_TCK
GND	3	4	P0_TMS
GND	5	6	P0_TDI
GND	7	8	P0_TDO
P0_TRST_N	9	10	HDT_HDR_PWROK
NC	11	12	HDT_HDR_RESET_N
NC	13	14	NC
NC	15	16	P0_DBREQ_N
GND	17	18	NC
+1V8_S5	19	20	NC

21 BMC I²C VRM Program Header (J1)

This is a reserved 3-pin header that supports VRM programming.



1	BMC_I2C_11_SCL(PWR_VR_SCL)
2	GND
3	BMC_I2C_11_SDA(PWR_VR_DAT)

3.4.2 Jumper

A CPU UART Source Selection Jumper (J48)

This is a 2-pin jumper that configures DSUB1B Dsub-9 signal source.

J48	Setting	
Short	UART1 (Low)	Default
Open	UART0 (High)	

B Clear CMOS Jumper (J60)

This is a 3-pin jumper that is used to provide SOC CMOS clear functionality.

J60	Setting	
Pin 1-2	Supply 1.5 RTC power	Default
Pin 2-3	Assert RTC reset	

C CS0(bit0): Enable CPU Running Jumper (J50)

This 2-pin jumper that enables/disables BMC to boot with SPI FM.

J50	Setting	
Short	Disable	
Open	Enable Boot	Default

D BMC Reset Jumper (J43)

This 2-pin jumper that configures BMC reset.

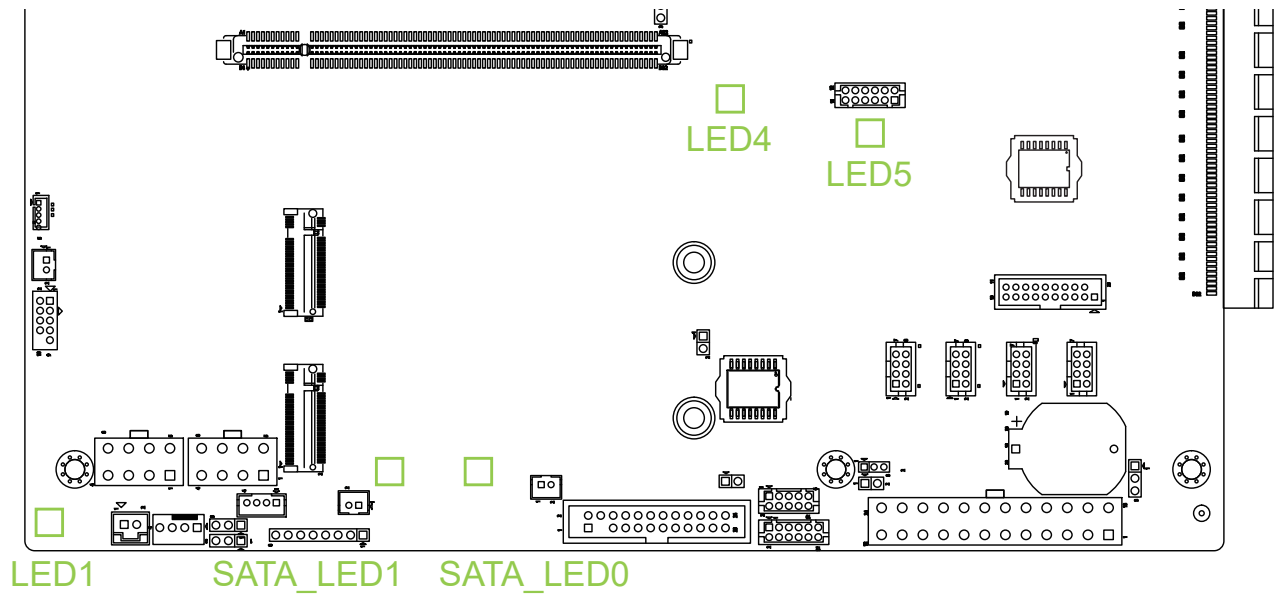
J43	Setting	
Short	Reset BMC	
Open	Normal Operation	Default

E Power Button Pass through mode Jumper (J20)

This is a 3-pin jumper that configures the power button in th front panel.

J20	Setting	
Pin 1-2	BMC pass through mode	Default
Pin 2-3	Directly Button switch mode	

3.4 LED Indicator



LED5	Heart beat	Green (Blinking)	BMC is alive in 1 Hz frequency.
		Solid or dark	BMC is abnormal or not in action.
LED1	Chassis ID	Solid	Identity system location.
		Twinkling	undefined
		Dark	Normal
LED4	PWR Status	Solid	Control by CPLD P0_PWR_GOOD when Sequence complete
		Blinking	On going
		Dark	System in S5
SATA_LED0	HDD Activity	Solid	undefined
		Blinking	HDD is active to access data
		Dark	No HDD attached or active
SATA_LED1	HDD Activity	Solid	undefined
		Blinking	HDD is active to access data
		Dark	No HDD attached or active

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 **F2** or **Del** 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.

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 BIOS Menu

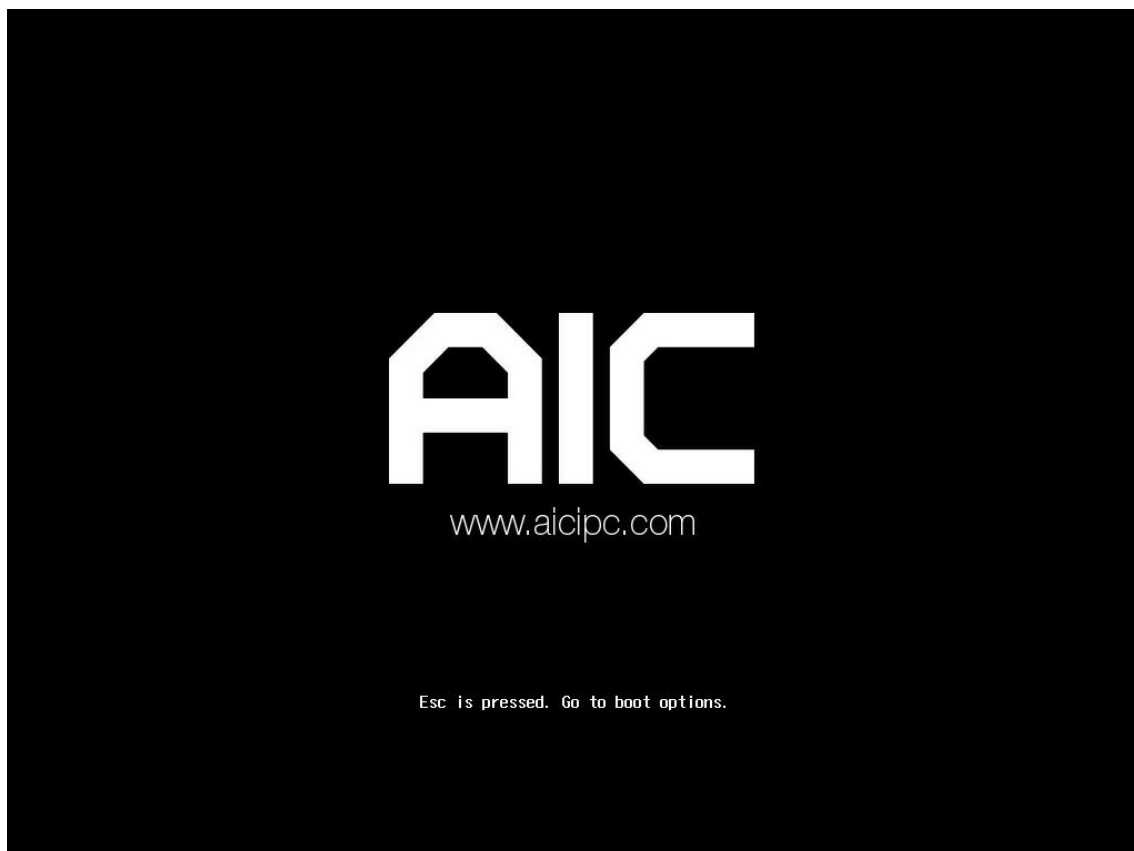
Press **←** and **→** to select the options of the menu bar.

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

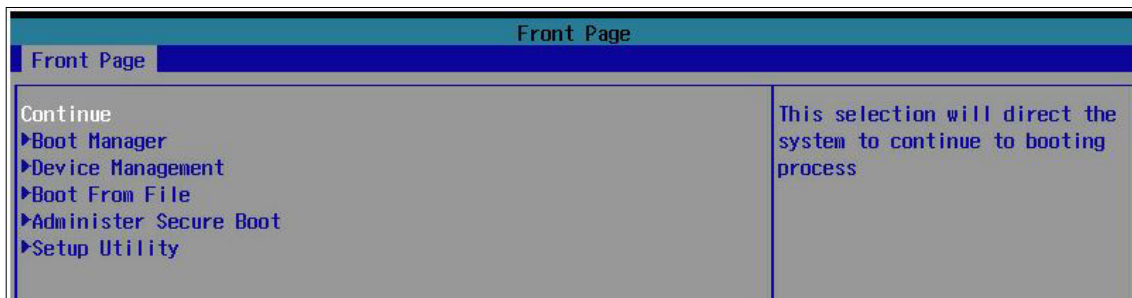
Menu	Description
Main	Displays system information such as CPU bus speed, system memory speed, total installed memory, current EFI language and system date & time.
AMD CBS	Displays AMD CBS Configurations.
Advanced	Allows configuration of advanced system settings such as ACPI features, boot and chipset configuration.
Security	Sets passwords and security functions.
Power	Configures Power Configurations.
Boot	Sets boot options such as Quick Boot or USB Boot.

4.2.2 BIOS Basic Utility

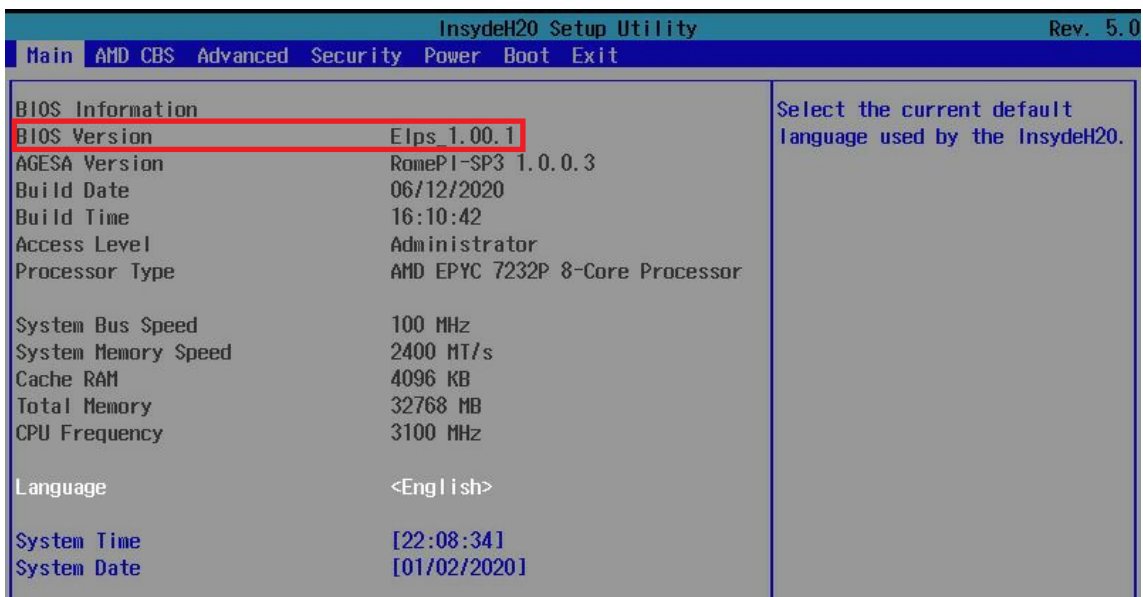
① Press **ESC** to run the BIOS setup procedure.



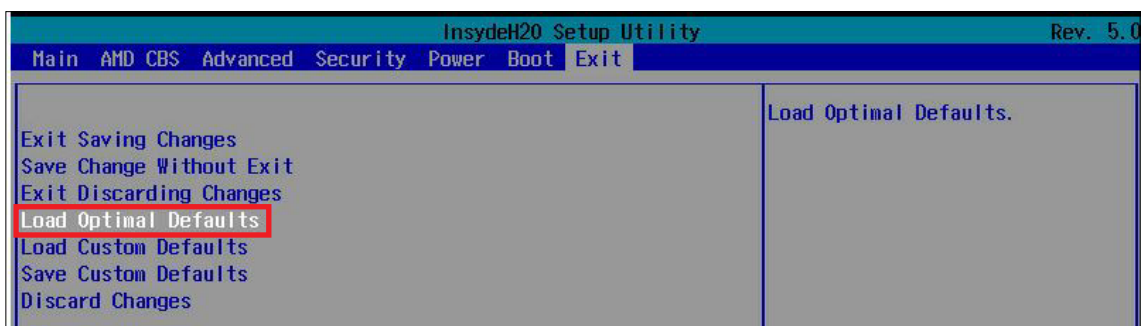
- ② There will be a message “Entering SETUP” displayed on the diagnostics screen.



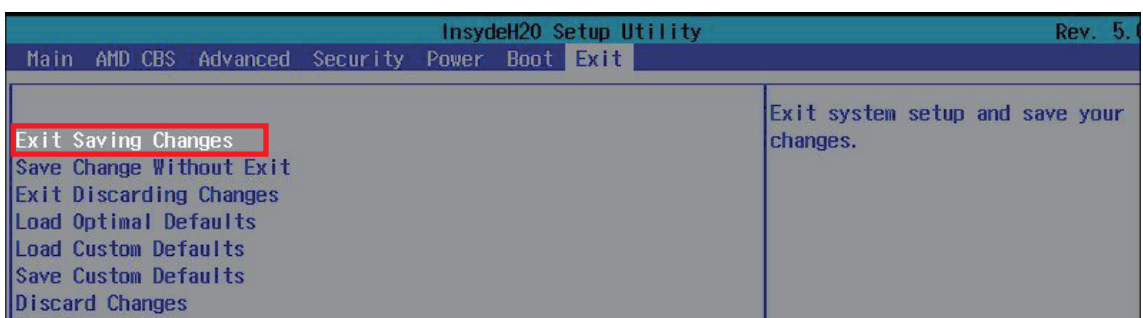
- ③ Identify the BIOS version.



- ④ Load Optimal Defaults setting.

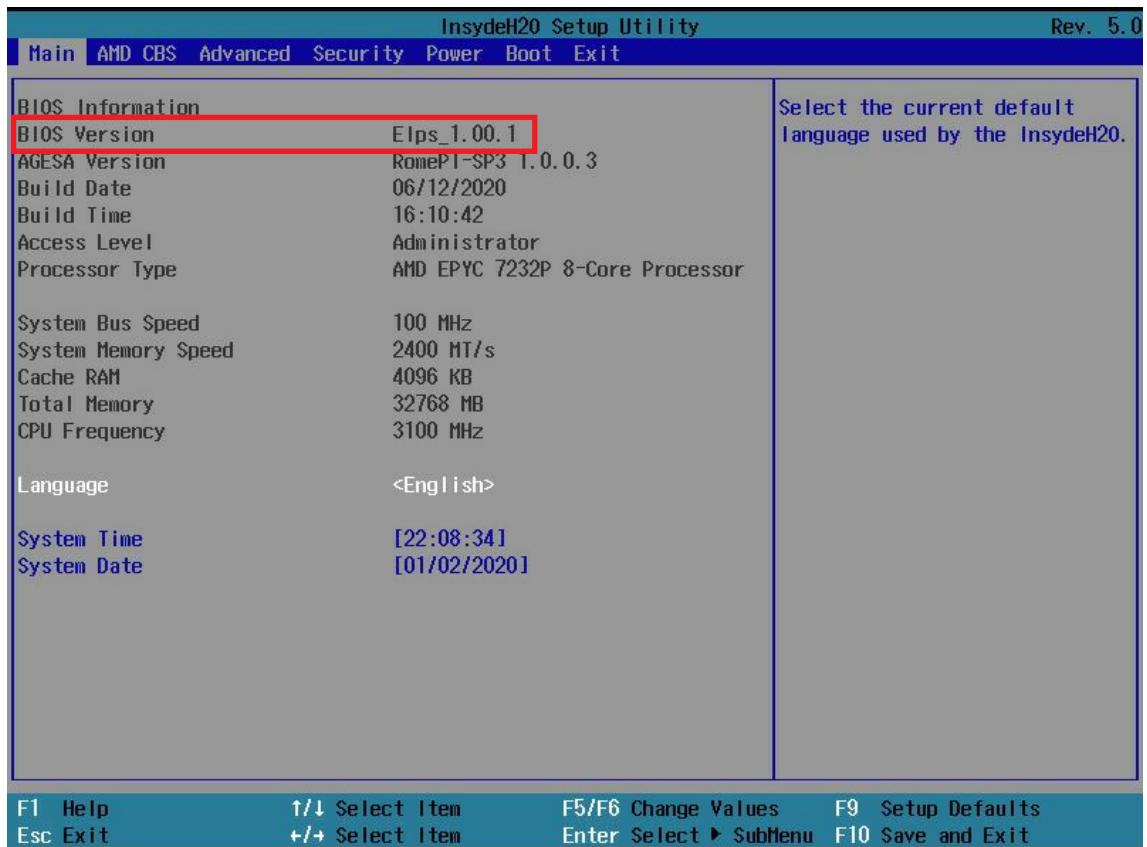


- ⑤ Save the setting and exit the BIOS setup utility.



4.2.3 BIOS Update

To identify the latest BIOS version, please check the BIOS setup.

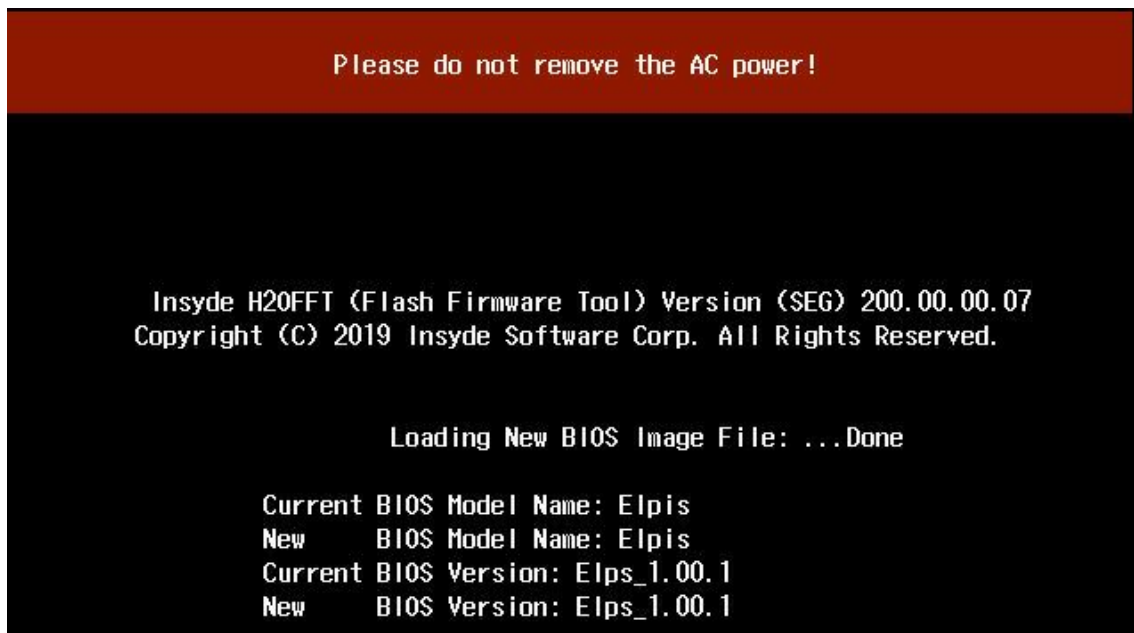


Update BIOS by INSYDE H2OFFT-Sx64 utility under shell environment

If you need to update Flash in the shell environment, please use H2OFFT-Sx64 utility. To use this utility, you must include the flash.nsh , H2OFFT-Sx64, and bin file in the same folder. Please follow the instructions below to update complete flash portion:

```
Shell> fs0:
FS0:\> cd Elips1001_BIOS
FS0:\Elips1001_BIOS> cd EFI
FS0:\Elips1001_BIOS\EFI> flash.nsh_
```

Step 1 Execute flash.nsh to update Flash in the shell environment.



```

Please do not remove the AC power!

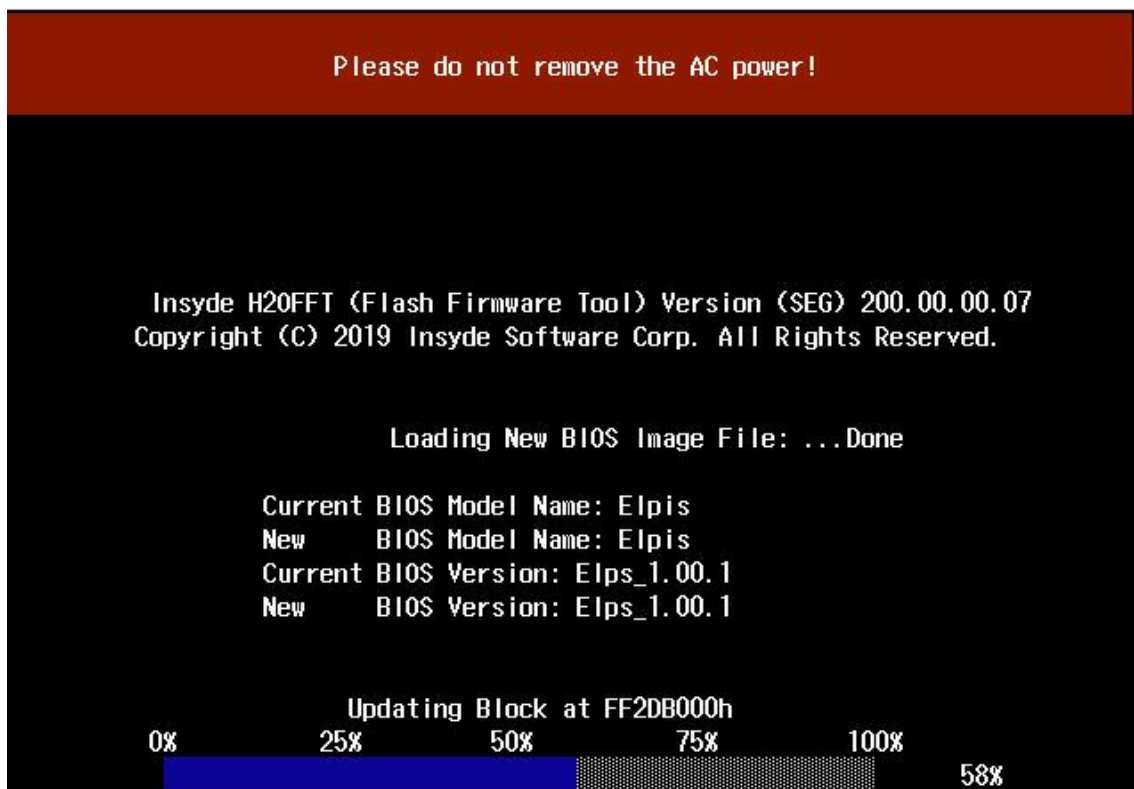
Insyde H2OFFT (Flash Firmware Tool) Version (SEG) 200.00.00.07
Copyright (C) 2019 Insyde Software Corp. All Rights Reserved.

Loading New BIOS Image File: ...Done

Current BIOS Model Name: Elpis
New BIOS Model Name: Elpis
Current BIOS Version: Elips_1.00.1
New BIOS Version: Elips_1.00.1

```

Step 2 When the BIOS flash update is completed, please reboot the system.



```

Please do not remove the AC power!

Insyde H2OFFT (Flash Firmware Tool) Version (SEG) 200.00.00.07
Copyright (C) 2019 Insyde Software Corp. All Rights Reserved.

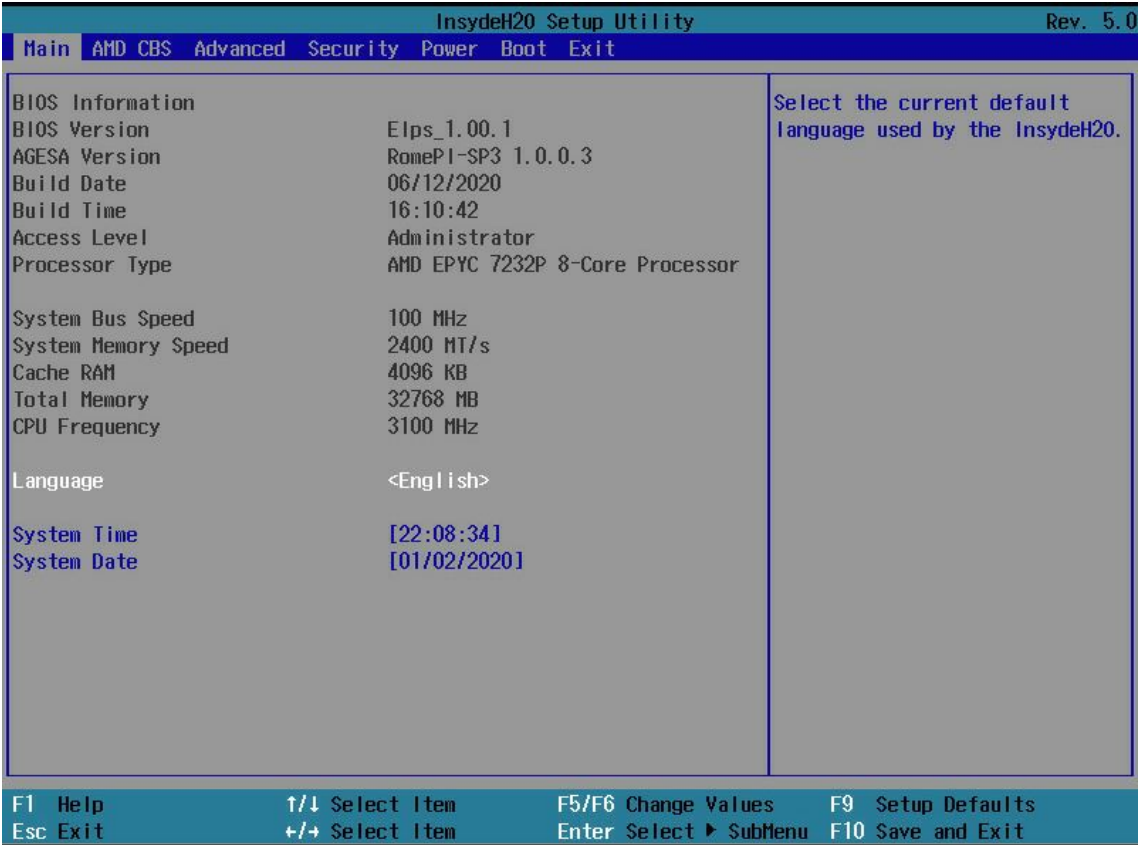
Loading New BIOS Image File: ...Done

Current BIOS Model Name: Elpis
New BIOS Model Name: Elpis
Current BIOS Version: Elips_1.00.1
New BIOS Version: Elips_1.00.1

Updating Block at FF2DB000h
0%      25%      50%      75%      100%
[Progress Bar] 58%

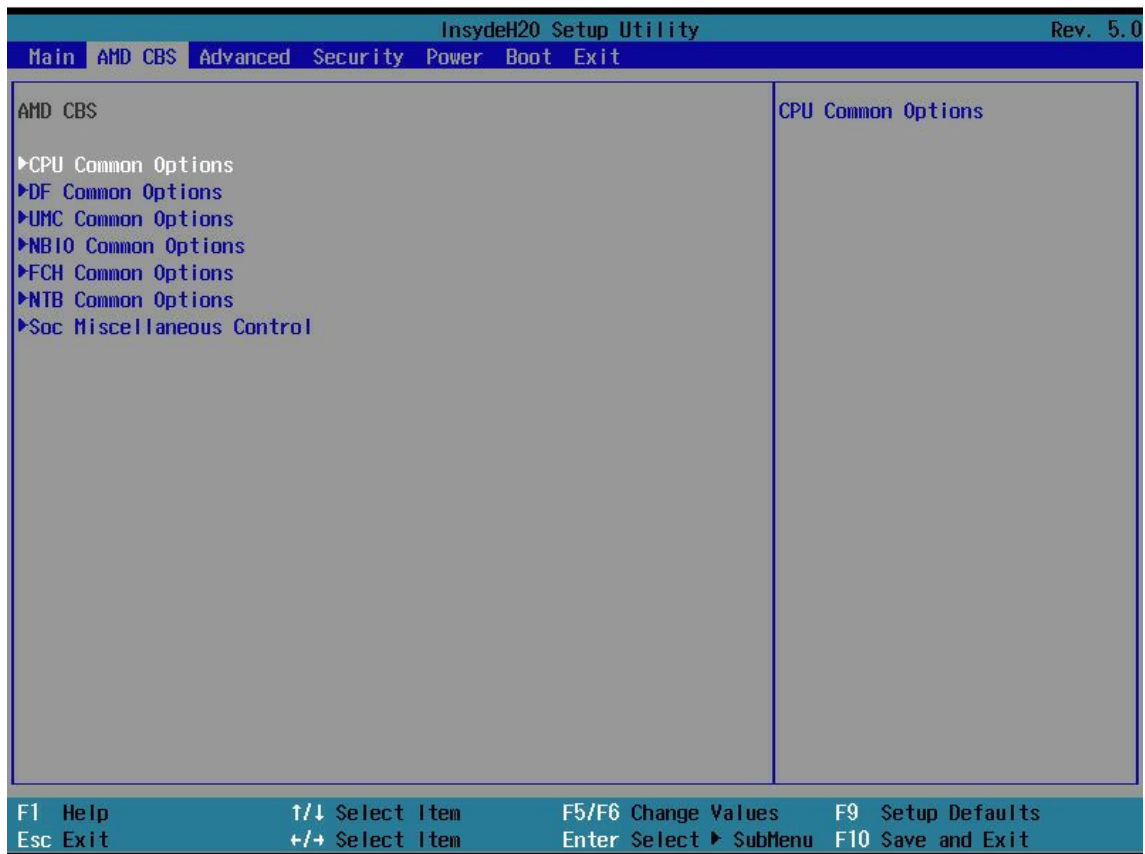
```

4.3 Main



Main	
Language	Configures the language used for your BIOS.
System time	Configures the current time.
System date	Configures the current date.

4.4 AMD CBS



4.4.1 CPU Common Options

CPU Common Options			
Platform First Error Handling	Enables/disables PFEH, cloak individual banks and mask deferred error interrupts from each bank.		
	Auto	► Enable	Disable
Core Performance Boost	Enables/disables CPB.		
	► Auto	Disable	
Global C-state Control	Controls IO based C-state generation and DF C-states.		
	► Auto	Enable	Disable
Power Supply Idle Control	Power Supply Idle Control.		
	► Auto	Low Current Idle	Typical Current Idle
SEV ASID Count	This fields specifies the maximum valid ASID, which affects the maximum system physical address space. 16TB of physical address space is available for systems that support 253 ASIDs, while 8TB of physical address space is available for systems that support 509 ASIDs.		
	► Auto	253 ASIDs	509 ASIDs
SEV-ES ASID Space Limit Control	► Auto		Manual
SEV-ES ASID Space Limit	SEV VMs using ASIDs below the SEV-ES ASID Space Limit must enable the SEV-ES feature. ASIDs from SEV-ES ASID Space Limit to (SEV ASID Count + 1) can only be used with SEV VMs. If this field is set to (SEV ASID Count + 1), all ASIDs are forced to be SEV-ES ASIDs. Hence, the valid values for this field is 1 - (SEV ASID Count + 1)		
Streaming Stores Control	Enables or disables the streaming stores functionality.		
	► Auto	Enable	Disable
Local APIC Mode	► Auto	xAPIC	x2APIC

► : Default option key is for reference only. Option key may vary per system.

ACPI_CST C1 Declaration	Determines whether or not to declare the C1 state to the OS.						
	► Auto		Enable		Disable		
MCA error thresh enable	Effective error threshold count = 4095(0xFFFF) - <this value> (e.g. the default value of 0xFF5 results in a threshold of 10).						
	► Auto		Enable		Disable		
MCA error thresh count	MCA error thresh count.						
	► 0xff5		Min=0x1, Max=0xffff				
SMU and PSP Debug Mode	When this option is enabled, specific uncorrected errors detected by the PSP FW or SMU FW will hang and not reset the system.						
	► Auto		Enable		Disable		
Xtrig7 Workaround	- By default (Auto), the Bronze workaround is applied. - Bronze workaround: DbReq and PDM function as expected, breakpoint redirect capability compromised. - Silver workaround: DbReq, PDM, and breakpoint redirect function as expected, SCAN capability compromised.						
	► Auto		No Workaround	Bronze Workaround	Silver Workaround		
PPIN Opt-in	Turn on PPIN feature.						
	► Auto		Enable		Disable		
Performance	OC Mode	► Normal Operation	OC1	OC2	OC3	Customized	
	Custom Core Pstates	Accept	Decline				
			Custom Pstate0/1/2/3/4/5/6/7	- Disabled: Disables this Pstate. - Custom: Customize this Pstate, applicable only if Pcd Oc Disable=FALSE			
				► Auto		Custom	
				Frequency (MHz)	Current core frequency in MHz.		
				► 0		Min=0, Max=4294967295	
				Voltage (uV)	Voltage in uV (1V = 1000 * 1000 uV)		
				► 0		Min=0, Max=4294967295	
				Pstate0/1/2/3/4/5/6/7 FID	Specifies the core frequency multiplier. COF = 200MHz * FID / DID		
				► 0x10		Min=0x10, Max=0xff	
	Pstate01/2/3/4/5/6/7 DID	Specifies the core frequency divisor (DID[0] should zero if DID[5:0]>1Ah).					
	► 0x8		Min=0x8, Max=0x30				
	Pstate01/2/3/4/5/6/7 VID	Specifies the core voltage.					
	► 0xff		Min=0x0, Max=0xff				
	CCD/Core/Thread Enablement	Accept	Decline				
			CCD Control	Sets the number of CCDs to be used. Once this option has been used to remove any CCDs, a POWER CYCLE is required in order for future selections to take effect.			
				► Auto		1~4 CCD(s)	
				Core control	Sets the number of cores to be used. Once this option has been used to remove any cores, a POWER CYCLE is required in order for future selections to take effect.		
	► Auto	TWO	THREE		FOUR	SIX	

Performance	CCD/Core/ Thread Enablement	Accept	SMT Control	Used to disable symmetric multithreading. To re-enable SMT, a POWER CYCLE is needed after selecting the 'Auto' option. NOTE: S3 is NOT SUPPORTED on systems where SMT is disabled.	
				► Auto	Disable
			CCD 0/1/2/3 4/5/6/7 DownCore Bitmap	► 0x0	Min=0x0, Max=0xff
Prefetcher settings	L1/2 Stream HW Prefetcher	Option to enable/disable L1/2 Stream HW Prefetcher.			
			► Auto	Enable	Disable
Core Watchdog	Core Watchdog Timer Enable	Enables/disables CPU Watchdog Timer.			
			► Auto	Enable	Disable
	Core Watchdog Timer Interval	► Auto	21.461s/10.730s/5.364s/2.681s/1.340s/ 669.41ms/334.05ms/166.37ms/82.53ms /40.61ms/20.970ms/10.484ms/5.241ms /2.620ms/1.309ms/654.08us/ 326.4us/1 62.56us/80.64us/39.68us		
	Core Watchdog Timer Severity	► Auto	No Error	Corrected	Transparent
			Uncorrected		Deferred
					Fatal

4.4.2 DF Common Options

DF Common Options				
Disable DF to external IP Sync Flood Propagation	Disables/enables Sync Flood to UMC & downstream slaves.			
	▶ Auto	Sync flood enabled		Sync flood disabled
Disable DF sync flood propagation	Controls DF::PIE Config [Dis Sync Flood Prop]			
	▶ Auto	Sync flood enabled		Sync flood disabled
Freeze DF module queues on error	• Controls DF: PIE Config [Dis Imm Sync Flood On Fatal Error]. • Disabling this option sets DF: PIE Config [Dis Imm Sync Flood On Fatal Error].			
	▶ Auto	Enable		Disable
CC6 memory region encryption	Controls whether or not the CC6 save/restore memory is encrypted.			
	▶ Auto	Enable		Disable
System probe filter	Controls whether or not the probe filter is enabled. Has no effect on parts where the probe filter is fuse disabled.			
	▶ Auto	Enable		Disable
Memory Clear	When this feature is disabled, BIOS does not implement Mem Clear after memory training (only if non-ECC DIMMs are used).			
	▶ Auto	Enable		Disable
PSP error injection support	True: enables error injection.			
	True		▶ False	
Scrubber	DRAM scrub time	Provides a value that is the number of hours to scrub memory.		
		▶ Auto	1/4/8/16/24/48 hour(s)	Disable
	Poison scrubber control	Controls DF: Redirects Scrubber Ctrl[Redir Scrub Mode[1]].		
		▶ Auto	Enable	Disable
	Redirect scrubber control	Control DF: Redirects Scrubber Ctrl[RedirScrubMode[0]].		
▶ Auto	Enable	Disable		

Scrubber	Redirect scrubber limit	Control DF: Redirects Scrubber Ctrl[RedirScrubReqLmt].				
		► Auto	2	4	8	Infinite
	Periodic Directory Rinse	Controls Periodic Directory Rinse Mode.				
		► Auto	Enable		Disable	
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	NPS0	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			
	Memory interleaving size	Controls the memory interleaving size. The valid values are AUTO, 256 bytes, 512 bytes, 1 Kbytes or 2Kbytes. This determines the starting address of the interleave (bit 8, 9, 10 or 11).				
		► Auto	256 Bytes	512 Bytes	1 KB	2 KB
	1TB remap	Attempts to remap DRAM out of the space just below the 1TB boundary. The ability to remap depends on DRAM configuration, NPS, and interleaving selection. This may not always be possible.				
		► Auto	Attempt to remap		Do not 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	
ACPI	ACPI SRAT L3 Cache As NUMA Domain	- Enabled: Each CCX in the system will be declared as a separate NUMA domain. - Disabled: 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	Sets the remote socket distance for 2P systems as near (2.8) or far (3.2).				
		► Auto	Near		Far	
	ACPI SLIT virtual distance	Specifies the distance between two virtual domains (see L3 Cache as NUMA Domain) in the same physical domain.				
		► 0xb	Min=0xa, Max=0xff			
	ACPI SLIT same socket distance	Specifies the distance to other physical domains within the same socket.				
		► 0xc	Min=0xa, Max=0xff			
	ACPI SLIT remote socket distance	Specifies the distance to domains on the remote socket.				
		0x20	Min=0xa,Max=0xff			
ACPI SLIT local SLink distance	Specifies the distance to an SLink domain on the same socket.					
	► 0x32	Min=0xa, Max=0xff				
ACPI SLIT remote SLink distance	Specifies the distance to an SLink domain on the other socket.					
	► 0x3c	Min=0xa, Max=0xff				
ACPI SLIT local inter-SLink distance	Specifies the distance between two SLink domains on the same socket.					
	► 0xff	Min=0xa, Max=0xff				
ACPI SLIT remote inter-SLink distance	Specifies the distance between two SLink domains with each on a different socket.					
	► 0xff	Min=0xa, Max=0xff				

Link	GMI encryption control		Controls GMI link encryption.			
			► Auto	Enable	Disable	
	xGMI encryption control		Controls xGMI link encryption.			
			► Auto	Enable	Disable	
	CAKE CRC perf bounds Control		► Auto		Manual	
	CAKE CRC perf bounds		Specifies the amount of performance loss that is acceptable to enable CRC protection. Units are in 0.00001%, Range: disabled (0) - 10% (1000000).			
			► 0x64		Min=0x0, Max=0xf4240	
	4-link xGMI max speed	► Auto	10.667Gbps	13Gbps	16Gbps	18Gbps
	3-link xGMI max speed	► Auto	TXEQ_Lane	TXEQ_RX_Vet	TXEQ_Link	TXEQ_Disable
xGMI TXEQ Mode		Selects XGMI TXEQ/RX vetting Mode.				
		► Auto	TXEQ_Lane	TXEQ_RX_Vet	TXEQ_Link	TXEQ_Disable

4.4.3 UMC Common Options

UMC Common Options							
DDR4 Common Options	DRAM Timing Configuration	Decline					
		Accept	Overclock	Memory Overclock Settings.			
				► Auto	Enable		
			Memory Clock Speed	Specifies the memory clock frequency.			
				► Auto	667MHz/800MHz/933MHz /1067MHz/1200MHz/1333 MHz/1467MHz/1600MHz		
			Tcl	Specifies the CAS latency.			
					8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk/10h Clk/11h Clk/12h Clk/13h Clk/14h Clk/15h Clk/16h Clk/17h Clk/18h Clk/19h Clk/1Ah Clk/1Bh Clk/1Ch Clk/1Dh Clk/1Eh Clk/1Fh Clk/20h Clk/21h Clk		
				► Auto			
			Trcdrd	Specifies the RAS# Active to CAS# Read Delay Time.			
					8 Clk/9 Clk,0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk/10h Clk/11h Clk/12h Clk/13h Clk/14h Clk/15h Clk/16h Clk/17h Clk/18h Clk/19h Clk/1Ah Clk/1Bh Clk		
► Auto							
Trcdwr	Specifies the RAS# Active to CAS# Write Delay Time.						
		8 Clk/9 Clk,0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk/10h Clk/11h Clk/12h Clk/13h Clk/14h Clk/15h Clk/16h Clk/17h Clk/18h Clk/19h Clk/1Ah Clk/1Bh Clk					
	► Auto						

DDR4 Common Options	DRAM Timing Configuration	Accept	Tras	Specifies the Active to Precharge Delay Time.	
				► Auto	15h Clk/16h Clk/17h Clk/18h Clk/19h Clk/1Ah Clk/1Bh Clk/1Ch Clk/1Dh Clk/1Eh Clk/1Fh Clk/20h Clk/21h Clk/22h Clk/23h Clk/24h Clk/25h Clk/26h Clk/27h Clk/28h Clk/29h Clk/2Ah Clk/2Bh Clk/2Ch Clk/2Dh Clk/2Eh Clk/2Fh Clk/30h Clk/31h Clk/32h Clk/33h Clk/34h Clk/35h Clk/36h Clk/37h Clk/38h Clk/39h Clk/3Ah Clk
			Trc Ctrl	Specifies Trc.	
				► Auto	Manual
			Trc	Specifies Active to Active/Refresh Delay Time. Valid values 87h-1Dh.	
				► 0x39	Min=0x1d, Max=0x87
			Trrd S	Specifies the Activate to Activate Delay Time, different bank group (tRRD_S)	
				► Auto	4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk
			TrrdL	Specifies the Activate to Activate Delay Time, same bank group (tRRD_L).	
				► Auto	4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk
			Tfaw Ctrl	Specifies Tfaw.	
				► Auto	Manual
			Tfaw	Specifies the Four Activate Window Time. Valid values 36h-6h.	
				► 0x1a	Min=0x6, Max=0x36
			Twtr S	Specifies the Minimum Write to Read Time in different bank group.	
				► Auto	2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk
			Twtr L	Specifies the Minimum Write Recovery Time. Valid value 51h-Ah	
				► Auto	2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk
			Twr Ctrl	Specifies Twr.	
				► Auto	Manual
			Twr	Specifies the Minimum Write Recovery Time. Valid value 51h-Ah	
				► 0x12	Min=0xa, Max=0x51

DDR4 Common Options	DRAM Timing Configuration	Accept	Trcpage Ctrl	Specifies Trcpage. ► Auto Manual
			Trcpage	SDRAM Optional Features (tMAW, MAC). Valid value 3FFh - 0h ► 0x0 Min=0x0, Max=0x3ff
			TrdrdScL Ctrl	Specifies TrdrdScL ► Auto Manual
			TrdrdScL	Specifies the CAS to CAS Delay Time, same bank group. Valid values Fh-1h
			TwrwrScL Ctrl	Specifies TwrwrScL. ► Auto Manual
			TwrwrScL	Specifies the CAS to CAS Delay Time, same bank group. Valid values 3Fh-1h ► 0x3 Min=0x1, Max=0x3f
			Trfc Ctrl	Specifies Trfc. ► Auto Manual
			Trfc	► 0x138 Min=0x3c, Max=0x3de
			Trfc2 Ctrl	► Auto Manual
			Trfc2	► 0xc0 Min=0x3c, Max=0x3de
			Trfc4 Ctrl	► Auto Manual
			Tcwl	► Auto 9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Eh Clk/10h Clk/12h Clk/14h Clk
			Trtp	► Auto 5 Clk/Clk/Clk/Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk
			Tcke	► Auto 1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk/10h Clk/11h Clk/12h Clk/13h Clk/14h Clk/15h Clk/16h Clk/17h Clk/18h Clk/19h Clk/1Ah Clk/1Bh Clk/1Ch Clk/1Dh Clk/1Eh Clk/1Fh Clk
			Trdwr	Specifies the Read to Write turnaround timing. ► Auto 1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk/10h Clk/11h Clk/12h Clk/13h Clk/14h Clk/15h Clk/16h Clk/17h Clk/18h Clk/19h Clk/1Ah Clk/1Bh Clk/1Ch Clk/1Dh Clk/1Eh Clk/1Fh Clk
			Twrrd	Specifies the Write to Read turnaround timing. ► Auto 1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk

DDR4 Common Options	DRAM Timing Configuration	Accept	TwrrwrSc	Specifies the Write to Write turnaround timing in the same chipselect.		
			► Auto	1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk		
			TwrrwrSd	Specifies the Write to Write turnaround timing in the same DIMM.		
			► Auto	1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk		
			TwrrwrDd	Specifies the Write to Write turnaround timing in a different DIMM.		
			► Auto	1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk		
			TrdrdSc	Specifies the Read to Read turnaround timing in the same chipselect.		
	► Auto	1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk				
	TrdrdSd	Specifies the Read to Read turnaround timing in the same DIMM.				
	► Auto	1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk				
	TrdrdDd	Specifies the Read to Read turnaround timing in a different DIMM.				
	► Auto	1 Clk/2 Clk/3 Clk/4 Clk/5 Clk/6 Clk/7 Clk/8 Clk/9 Clk/0Ah Clk/0Bh Clk/0Ch Clk/0Dh Clk/0Eh Clk/0Fh Clk				
	ProcODT	Specifies the Processor ODT.				
► 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 ohm34.3 ohm/32 ohm/30 ohm/28.2 ohm					
DRAM Controller Configuration	Cmd2T		Select between 1T and 2T mode on ADDR/CMD.			
			► Auto	1T	2T	
	Gear Down Mode		► Auto	Enable	Disable	
	DRAM Power Options	Power Down Enable	Enables/disables DDR power down mode.			
		► Auto	Enable	Disable		

DDR4 Common Options	CAD Bus Configuration	CAD Bus Timing User Controls	Setup time on CAD bus signals to Auto or Manual.							
		► Auto				Manual				
		Addr Cmd Setup	Setup time on CAD bus signals. Valid values 3Fh-0h.							
		► 0x0				Min=0x0, Max=0x3f				
		Cs Odt Setup	► 0x0				Min=0x0, Max=0x3f			
		Cke Setup	► 0x0				Min=0x0, Max=0x3f			
		CAD Bus Drive Strength User Controls	Drive Strength on CAD bus signals to Auto or Manual.							
		► Auto				Manual				
		Clk Drv Stren	► Auto	120.0 Ohm	60.0 Ohm	40.0 Ohm	30.0 Ohm	24.0 Ohm	20.0 Ohm	
		Addr Cmd Drv Stren	► Auto	120.0 Ohm	60.0 Ohm	40.0 Ohm	30.0 Ohm	24.0 Ohm	20.0 Ohm	
	Cs Odt Drv Stren	► Auto	120.0 Ohm	60.0 Ohm	40.0 Ohm	30.0 Ohm	24.0 Ohm	20.0 Ohm		
	Cke Drv Stren	► Auto	120.0 Ohm	60.0 Ohm	40.0 Ohm	30.0 Ohm	24.0 Ohm	20.0 Ohm		
	Data Bus Configuration	Data Bus Configuration User Controls	Specifies the mode for drive strength to Auto or Manual.							
		► Auto				Manual				
		Rtt Nom	► Auto	RZQ/4	RZQ/2	RZQ/6	RZQ/1			
		Rtt_Nom Disable				RZQ/5	RZQ/3	RZQ/7		
		Rtt Wr	► Auto	Dynamic ODT Off	RZQ/2	RZQ/1	Hi-Z	RZQ/3		
		Rtt Park	► Auto	RZQ/4	RZQ/2	RZQ/6	RZQ/1			
		Rtt_PARK Disable				RZQ/5	RZQ/3	RZQ/7		
	Common RAS	Data Poisoning	Enables/disables data poisoning: UMC_CH::EccCtrl[UcFatalEn] UMC_CH::EccCtrl[WREccEn] Should be enabled/disabled together.							
		► Auto				Enable	Disable			
		DRAM Post Package Repair	Enables/disables DRAM Post Package Repair.							
		Enable				► Disable				
		RCD Parity	UMC_CH::RecCtrl[RecEn][0] and UMC_CH::RecCtrl[MaxParRply]							
		► Auto				Enable	Disable			
		Max Parity Error Replay	Value in hex, 1, 2 or 3 is invalid.							
		0x8				Min=0x0, Max=0x3f				
		Write CRC Enable	► Auto				Enable	Disable		
	DRAM Write CRC Enable and Retry Limit	UMC_CH::RecCtrl[RecEn][1] and UMC_CH::RecCtrl[MaxCrcRply]								
	► Auto				Enable	Disable				
	Max Write CRC Error Replay	Value in hex, 1, 2 or 3 is invalid.								
	0x8				Min=0x0, Max=0x3f					
	Disable Memory Error Injection	True: UMC::CH::MiscCfg[DisErrInj]=1								
	► True				False					

DDR4 Common Options	Common RAS	ECC Configuration	DRAM ECC Symbol Size	DRAM ECC Symbol Size (x4/x8/x16) - UMC_CH::EccCtrl[EccSymbolSize16, EccSymbolSize]			
			► Auto	x4	x8	x16	
			DRAM ECC Enable	Use this option to enable/disable DRAM ECC. Auto will set ECC to enable.			
			► Auto	Enable	Disable		
	DRAM UECC Retry	Use this option to enable/disable DRAM UECC Retry.					
		► Auto		Enable	Disable		
Security		TSME	Transparent SME: AddrTweakEn = 1; ForceEncrEn =1; DataEncrEn = 0				
	► Auto		Enable	Disable			
	Data Scramble	Data scrambling: DataScrambleEn					
► Auto		Enable	Disable				
DRAM Memory Mapping	Chipselect Interleaving	Interleave memory blocks across the DRAM chip selects for node 0.					
		► Auto			Disable		
	Bank Group Swap	- Bank Group Swap Alt default: Enabled in BIOS, which has priority than Bank Group Swap. - BIOS equation: If Bank Group Swap Alt = Enabled Then Bank Group Swap : Disabled Endif - Please set Bank Group Swap Alt to Disabled while set Bank Group Swap to Enabled.					
		► Auto			Enable	Disable	
	Bank Group Swap Alt	► Auto			Enable	Disable	
	Address Hash Bank	Enables/disables bank address hashing.					
		► Auto			Enable	Disable	
	Address Hash CS	Enables/disables CS address hashing.					
		► Auto			Enable	Disable	
Address Hash Rm	Enables/disables RM address hashing.						
	► Auto			Enable	Disable		
SPD Read Optimization	Enables/disables SPD Read Optimization.						
	- Enabled: SPD reads are skipped for Reserved fields and most of upper 256 Bytes. - Disabled: Read all 512 SPD Bytes.						
			► Auto			Enable	Disable
Memory MBIST	Address Hash CS	Enables/disables Memory MBIST.					
		Enable			► Disable		
	MBIST Test Mode	Select MBIST Test Mode -Interface Mode (Tests Single and Multiple CS transactions and Basic Connectivity) or Data Eye Mode (Measures Voltage vs. Timing)					
		► Auto		Interface Mode	Data Eye Mode	Both	
	MBIST Aggressors	Enables/disables MBIST Aggressor test.					
		► Auto			Enable	Disable	
	MBIST Per Bit Slave Die Reporting	Reports 2D Data Eye Results in ABL Log for each DQ, Chipselect and Channel.					
► Auto			Enable	Disable			
Data Eye	Pattern Select	► PRBS		SSO	Both		

Memory MBIST	Data Eye	Pattern Length	This token helps to determine the pattern length. The possible options are N=3...12 ► 0x3 Min=0x3, Max=0xc		
		Aggressor Channel	This helps read the aggressors channels. If it is enabled, you can read from one or more than one aggressor channel. The default is set to disabled. Disable ► 1 Aggressor Channel 3 Aggressor Channels 7 Aggressor Channels		
		Aggressor Static Lane Control	This option, if enabled, will control the Aggressor Static Lane Controls. Enable ► Disable		
		Aggressor Static Lane Select Upper 32 bits	Static Lane Select for Upper 32 bits. The bit mask represents the bits to be read. ► 0x0 Min=0x0, Max=0xffffffff		
		Aggressor Static Lane Select Lower 32 Bits	Static Lane Select for Lower 32 bits. The bit mask represents the bits to be read. ► 0x0 Min=0x0, Max=0xffffffff		
		Aggressor Static Lane Select ECC	Static Lane Select for ECC Lanes. The bit mask represents the bits to be read. ► 0x0 Min=0x0, Max=0xa		
		Aggressor Static Lane Value	► 0x0 Min=0x0, Max=0xa		
		Target Static Lane Control	Enable ► Disable		
		Target Static Lane Select Upper 32 bit	Static Lane Select for Upper 32 bit. The bit mask represents the bits to be read. ► 0x0 Min=0x0, Max=0xffffffff		
		Target Static Lane Select Lower 32 Bits	Static Lane Select for Lower 32 bit. The bit mask represents the bits to be read. ► 0x0 Min=0x0, Max=0xa		
		Target Static Lane Select ECC	► 0x0 Min=0x0, Max=0xa		
		Target Static Lane Value	► 0x0 Min=0x0, Max=0xa		
		Data Eye Type	This options determines which results are expected to be captured for Data Eye. Supported options are 1D Voltage Sweep, 1D Timing Sweep, 2D Full Data Eye and Worst Case Margin only. 1D Voltage Sweep 1D Timing Sweep 2D Full Data Eye ► Worst Case Margin Only		
		Worst Case Margin Granularity	► 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		

Memory MBIST	Data Eye	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

4.4.4 NBIO Common Options

NBIO Common Options				
IOMMU	Enables/disables IOMMU.			
	► Auto	Enable		Disable
System Configuration	NOTE: Select System Configuration may cause the system to hang, as some System Configuration may not be supported by your OPN.			
	► Auto	35W POR Configuration	45W POR Configuration	65W POR Configuration
ACS Enable	AER must be enabled for ACS enable to work.			
	► Auto	Enable		Disable
PCIe ARI Support	Enables/disables Alternative Routing-ID Interpretation.			
	Auto	► Enable		Disable
PCIe Ten Bit Tag Support	Enables/disables PCIe ten bit tags for supported devices; Auto = Disabled.			
	► Auto	Enable		Disable
HD Audio Enable	► Auto	Enable		Disable
FCLK Frequency	Specifies the FCLK frequency.			
	► Auto	667MHz/800MHz/933MHz/1067MHz/1200MHz/1333MHz/1367MHz/1400MHz/1433MHz/1467MHz/1500MHz/1533MHz/1567MHz/1600MHz/1633MHz/1667MHz/1700MHz/1733MHz/1767MHz/1800MHz/1833MHz/1867MHz/1900MHz/1933MHz/1967MHz/2000MHz/2033MHz/2067MHz/2100MHz/2133MHz/2167MHz/2200MHz/2233MHz/2267MHz/2300MHz/2333MHz/2367MHz/2400MHz		
MEMCLK Frequency	Specifies the MEMCLK frequency.			
	► Auto	667MHz/800MHz/933MHz/1067MHz/1200MHz/1333MHz/1367MHz/1400MHz/1433MHz/1467MHz/1500MHz/1533MHz/1567MHz/1600MHz/1633MHz/1667MHz/1700MHz/1733MHz/1767MHz/1800MHz/1833MHz/1867MHz/1900MHz/1933MHz/1967MHz/2000MHz/2033MHz/2067MHz/2100MHz/2133MHz/2167MHz/2200MHz/2233MHz/2267MHz/2300MHz/2333MHz/2367MHz/2400MHz/2433MHz/2467MHz/2500MHz		
SOC OVERCLOCK VID	Specifies the Voltage ID (VID) value for VDDR_SOC to support overclocking. NOTE: This is a VID value in hex and not a voltage level and applied if DDR speed is > 2933. Voltage(V)=1.55V-Hex2Dec(VID)*0.00625V.			
	► 0x0	Min=0x0, Max=0xff		
UCLK DIV1 MODE	If UclkDiv1Mode = 1, UCLK = MEMCLK; if UclkDiv1Mode = 0, UCLK = MEMCLK/2.			
	► Auto	QUCLK = MEMCLK		UCLK = MEMCLK/2

XFR Enhancement	Decline							
	Accept	Precision Boost Overdrive	- Disabled: stock board values for standard IRM. - Enabled: Loads board limits for EDC, TDC and PPT. - Manual: manual setting of PPT, TDC and EDC.					
			► Auto	Enable	Disable	Manual		
		PPT Limit	PPT Limit [W], Board Socket Power capability, adjustable up to motherboard programed PPT limit.					
			► 0	Min=0, Max=65535				
		TDC Limit	TDC Limit [A], Board thermally constrained current delivery capability, adjustable up to motherboard programed board TDC limit.					
			► 0	Min=0, Max=65535				
		EDC Limit	EDC Limit [A], Board electrically constrained current delivery capability, adjustable up to motherboard programed board EDC limit.					
			► 0	Min=0, Max=65535				
		Precision Boost Overdrive Scalar	- Disabled: Part runs with a scalar of 1X, i.e. normal operation. - Manual: Part runs with a scalar of customized Value.					
			► Auto	Manual	Disable			
		Customized Precision Boost Overdrive Scalar	Precision Boost Overdrive increases the maximum boost voltage used (runs above parts specified maximum) and the amount of time spent at that voltage. The larger the value entered the larger the boost voltage used and the longer that voltage will be maintained.					
			1X	► 2X	3X	4X	5X	6X
			7X	8X	9X	10X		
SMU Common Options	Determinism Control	- Auto: Uses the fused Determinism. - Manual: User can set customized Determinism.						
		► Auto		Manual				
	Determinism Slider	Auto: Uses default performance determinism settings.						
		► Auto		Power	Performance			
	cTDP Control	- Auto: Uses the fused TDP. - Manual: User can set customized TDP. - TDP is used to define the RC thermal model only.						
		► Auto		Manual				
	cTDP	cTDP [W] 0 = Invalid value.						
		► 0		Min=0, Max=4294967295				
	CLDO_VDDP Control	Manual: User can set customized CLDO_VDDP voltage.						
		► Auto		Manual				
	CLDO_VDDP voltage	CLDO_VDDP voltage [mV] = (supported range is 700mV to 'VDDIO-100mV'). NOTE: user must manually cold reset the system so that the CLDOs get re-latched otherwise the voltage change will not take into effect.						
		► 700		Min=700, Max=4294967295				

SMU Common Options	Efficiency Mode En	0: Uses performance optimized CCLK DPM settings. 1: Uses power efficiency optimized CCLK DPM settings.		
		► Auto	Enable	
	Package Power Limit Control	- Auto: Uses the fused PPT. - Manual: User can set customized PPT. ***PPT will be used as the ASIC power limit.***		
		► Auto	Manual	
	xGMI Link Width Control	- Auto: Uses default xGMI link width controller settings - Manual: User can set custom xGMI link width controller settings.		
		► Auto	Manual	
	xGMI Force Link Width	0: Force xGMI link width to x2. 1: Force xGMI link width to x8. 2: Force xGMI link width to x16.		
		0	1	► 2
	xGMI Max Link Width	0: Set max xGMI link width to x8. 1: Set max xGMI link width to x16.		
		0	► 1	
	xGMI Max Link Width Control	- Auto: Use default xGMI max supported link width. - Manual: User can set custom xGMI max link width.		
		► Auto	Manual	
	DF Cstates	- Enabled: Enable DF C-states - Disabled: Disable DF C-states		
		► Auto	Enable	Disable
	Fixed SOC Pstate	► P0	P1	P2 P3
	CPPC	FEATURE_CPPC_MASK.		
		► Auto	Enable	Disable
	Boost Fmax En	- Auto: Uses the default Fmax. - Manual: User can set the boost Fmax.		
		► Auto	Manual	
	Boost Fmax	Specifies the boost Fmax frequency limit to apply to all cores (MHz).		
		► 0	Min=0, Max=4294967295	
	Fan Control	Fan Table Control	- Auto: Uses the default fan table. - Manual: User can set customized fan table.	
			► Auto	Manual
		Low Temperature	Low Temperature [°C].	
			► 0	Min=0, Max=255
		Medium Temperature	Medium Temperature [°C].	
			► 0	Min=0, Max=255
		High Temperature	High Temperature [°C]	
		► 0	Min=0, Max=255	
	Critical Temperature	Critical Temperature [°C].		
		► 0	Min=0, Max=255	
	Low Pwm	Low Pwm [0-100].		
		► 0	Min=0, Max=100	
	Medium Pwm	Medium Pwm [0-100].		
		► 0	Min=0, Max=100	

SMU Common Options	Fan Control	High Pwm	High Pwm [0-100]. ► 0Min=0, Max=100	
		Temperature Hysteresis	Temperature Hysteresis [°C] ► 0Min=0, Max=255	
		Pwm Frequency	0 = 25kHz 1 = 100Hz ► 25kHz100Hz	
		Fan Polarity	0 = negative 1 = positive Positive► Negative	
NBIO RAS Common Options	NBIO RAS Global Control	NBIO RAS Global Control. ► AutoManual		
	NBIO RAS Control	(0) Disabled, (1) MCA, (2) Legacy MCALegacyDisable		
	Egress Poison Severity High	Each bit sets to 1 enables HIGH severity on the associated IOHC egress port. A bit of 0 indicates LOW severity. 0x30011Min=0x0, Max=0xffffffff		
	Egress Poison Severity Low	Each bit sets to 1 enables HIGH severity on the associated IOHC egress port. A bit of 0 indicates LOW severity. 0x4Min=0x0, Max=0xffffffff		
	NBIO Sync Flood 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. ► AutoEnableDisable		
	NBIO Sync Flood 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 ► EnableDisable		
	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. ► 0xfffcffffMin=0x0, Max=0xffffffff		
	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. ► 0xffffffffbMin=0x0, Max=0xffffffff		
	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. ► 0x30000Min=0x0, Max=0xffffffff		
	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. ► 0x4Min=0x0, Max=0xffffffff		
	System Hub Watchdog Timer	This value specifies the timer interval of the SYSHUB Watchdog timer in milliseconds. 0xa28Min=0x0, Max=0xffff		

NBIO RAS Common Options	SLINK Read Response OK	This value specifies whether SLINK read response errors are converted to an Okay response. When this value is set to TRUE, read response errors are converted to Okay responses with data of all FFs. When set to FALSE read response errors are not converted.			
		Enable	► Disable		
	SLINK Read Response Error Handling	This value specifies whether SLINK write response errors are converted to an Okay response. When this value is set to 0, write response errors will be logged in the MCA. When set to 1, write response errors will trigger an MCOMMIT error. When this value is set to 2, write response errors are converted to Okay responses.			
		Enable	Trigger MCOMMIT Error	► Log Errors in MCA	
	Log Poison Data from SLINK	This value specifies whether poison data propagated from SLINK will generate a deferred error. When set to TRUE, deferred errors are enabled. When set to FALSE, errors are not generated.			
		Enable	► Disable		
	PCIe Aer Reporting Mechanism	This value selects the method of reporting AER errors from PCI Express. A value of 0 indicates that the hardware will report the error through MCA. 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	OS First	MCA
	Edpc Control	(0) Disabled; (1) Enabled; (3) Auto			
		► Auto	Enable	Disable	
NBIO Poison Consumption	NBIO Poison Consumption.				
	► Auto	Enable	Disable		
Sync Flood on PCIe Fatal Error	- When 'Sync Flood on PCIe Fatal Error' is True, Pcd Amd Pcie Sync Flood On Fatal should be set to True. - When Sync Flood on PCIe Fatal Error is False, Pcd Amd Pcie Sync Flood On Fatal should be set to False. - When 'Sync Flood on PCIe Fatal Error' is Auto, Pcd Amd Pcie Sync Flood On Fatal should retain its AGESA default.				
	► Auto	Enable	Disable		
Enable AER Cap	Enables/disables Advanced Error Reporting Capability.				
	► Auto	Enable	Disable		
Early Link Speed	Sets Early Link Speed.				
	► Auto	Gen1	Gen2		
Hot Plug Handling mode	Controls the Hot Plug Handling mode.				
	► Auto	A0 Mode	OS First (No Error Handling)		
	OS First (Error Handling - Not Implemented)		Firmware First (Not Implemented)		
Presence Detect Select mode	Controls the Presence Detect Select mode.				
	► Auto	And	Or		
Preferred IO	Preferred IO Select Type				
	- Manual: Bus Number manually - Auto: Default				
	► Auto	Manual			
Preferred IO Bus	Preferred IO Bus Number 0x0-0xFF: Bus Number				
	► 0x0	Min=0x0, Max=0xff			

4.4.5 FCH Common Options

FCH Common Options							
SATA Configuration Options	SATA Enable	Enables/disables On Chip SATA controller.					
		▶ Auto		Enable		Disable	
	SATA Mode	Select On Chip SATA Type.					
		▶ AHCI		AHCI as ID 0x7904		Auto RAID	
	Sata RAS Support	Enables/disables Sata RAS Support.					
		▶ Auto		Enable		Disable	
	Aggressive SATA Device Sleep Port 0/1	▶ Auto		Enable		Disable	
SATA Configuration Options	Dev Sleep0/1 Port Number	DEVSLP port 0.					
		0x0		Min=0x0, Max=0x7			
	SATA Controller options	SATA Controller Enable	Sata0-7 Enable	Enables/disables Sata0-7. Each IOD has 4 Sata Controllers.			
				▶ Auto		iSATA	eSATA
	SATA Controller eSATA	Sata0 eSATA	Sata0 eSATA Port0-7	External SATA Port support.			
			Sata1-7 eSATA Port0-7	▶ Auto		Enable	Disable
	SATA Controller DevSlp	Socket1 DevSlp	Socket1 Dev Slp0-1 Enable	Only Sata0 on each IOD/socket support DevSlp.			
			Dev Sleep 0-1 Port Number	▶ Auto		Enable	Disable
	SATA Controller SGPIO	Sata0 SGPIO		Enables/disables Sata0 SGPIO feature.			
		Sata1-7 SGPIO		Enables/disables Sata Sgpios on Sata1-7.			
USB Configuration Options	XHCI Controller0-1 enable	Enables/disables USB3 controller.					
		▶ Auto		Enable		Disable	
	USB ecc SMI Enable	▶ Auto		Enable		Disable	
	MCM USB enable	XHCI2/3 enable (Socket1)		Enables/disables USB3 controller.			
				▶ Auto		Enable	Disable
SD Dump Options	SD Configuration Mode	Select SD Mode.					
		SD Dump enable			▶ SD Dump disable		
Ac Power Loss Options	Ac Loss Control	Select Ac Loss Control Method.					
		Auto		Previous	Reserved	Always On	Always Off
I2C Configuration Options	I2C 0-5 Enable	▶ Auto		Enable		Disable	
Uart Configuration Options	Uart 0-3 Enable	Uart 0 has no HW FC if Uart 2 is enabled					
		▶ Auto		Enable		Disable	
	Uart 0-3 Legacy Options	▶ Auto	0x2E8	0x2F8	0x3E8	0x3F8	Disable

ESPI Configuration Options	ESPI Enable	► Auto	Enable	Disable
eMMC Options	eMMC/SD Configure	► Auto	SD Normal Speed	SD UHSI-DDR50
		Disable	SD High Speed	SD UHSI-SDR50
		eMMC HS200	eMMC High Speed DDR	SD UHSI-SDR104
		eMMC HS300	eMMC High Speed SDR	
		eMMC HS400	eMMC Emmc Backward Compatibility	
	Driver Type	BIOS will select MS driver for SD selections.		
		► Auto	AMD eMMC Driver	MS Driver
	D3 Cold Support	► Auto	Enable	Disable
eMMC Boot	► Auto	Enable	Disable	
FCH RAS Options	ALink RAS Support	► Auto	Enable	Disable
	Reset after sync flood	Enables/disables AB to forward downstream sync-flood message to system controller.		
		► Auto	Enable	Disable

4.4.5 NTB Common Options

NTB Common Options										
NTB Enable	Enables/disables NTB.									
	▶ Auto					Enable				
NTB Location	▶ Auto	Socket0 -Die0	Socket0 -Die1	Socket0 -Die2	Socket0 -Die3	Socket1 -Die0	Socket1 -Die1	Socket1 -Die2	Socket1 -Die3	
NTB active on PCIe Core	NTB enable on PCIe Core.									
	▶ Auto			Core0			Core1			
NTB Mode	Select NTB Mode (Core 0, Port 0).									
	▶ Auto		NTB Random		NTB Primary		NTB Secondary		NTB Disabled	
Link Speed	▶ Auto	Max Speed		Gen 1		Gen 2		Gen 3		Gen 4

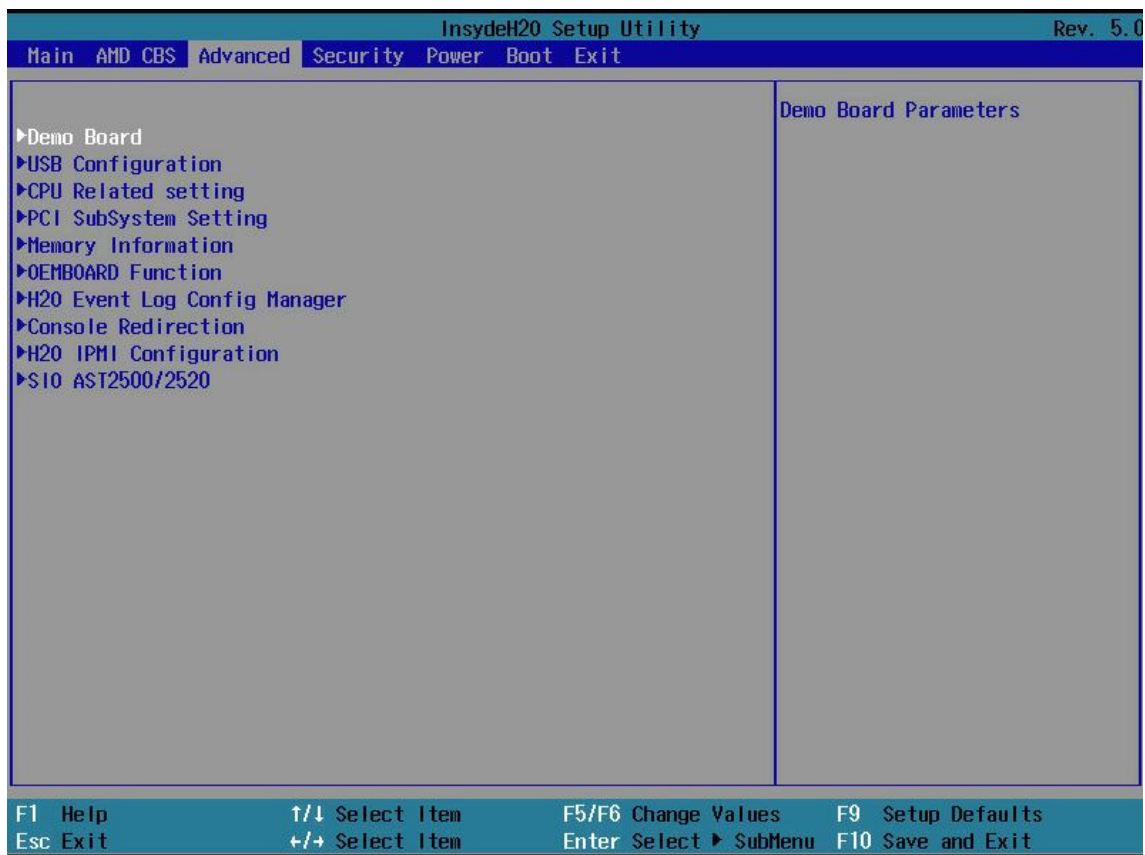
4.4.6 Soc Miscellaneous Control

Soc Miscellaneous Control					
ABL Console Out Control	• Enabled: Enables Console Out Function for ABL. • Disabled: Disable sConsole Out Function for ABL. • Auto: Keeps default behavior.				
	► Auto	Enable		Disable	
ABL PMU message Control	To control the total number of PMU debug messages. Several major controls are listed below: 1. Detailed debug messages (e.g. Eye delays) 2. Coarse debug messages (e.g. rank information) 3. Stage completion 4. Firmware completion messages only				
	► Auto	Detailed debug message	Coarse debug message	Stage completion	Firmware completion message only

4.4.7 BIXBY Common Options

BIXBY Common Options			
BIXBY SATA Configuration Options	BXB SATA0-1 Enable	Enables/disables Bixby SATA controller.	
		► Auto	Enable Disable
	BXB SATA Mode	Select Bixby SATA Type.	
		► AHCI	AHCI as ID 0x7904 Auto RAID
	BXB Sata Disabled AHCI Prefetch Function	Enables/disables Sata Disabled AHCI Prefetch Function.	
		► Auto	Enable Disable
BIXBY USB Configuration Options	BXB Aggressive SATA Device Sleep Port 0-1	► Auto Enable Disable	
	BXB DevSleep0 Port Number	DEVSLP port 0.	
		► 0x0	Min=0x0, Max=0x7
	BXB Aggressive SATA Device Sleep Port 1	► Auto Enable Disable	
BIXBY USB Configuration Options	BXB XHCI Controller0-1 enable	Enables/disables USB3 controller0.	
		► Auto	Enable Disable

4.5 Advanced



4.5.1 Demo Board

Demo Board			
OnBrd/Ext VGA Select	Select between onboard or external VGA support.		
	► Auto	Onboard	External

4.5.2 USB Configuration

USB Configuration		
USB Hardware SMI support	USB Hardware SMI support.	
	► Enable	Disable
USB Ports Per-Port Disable Control	Controls each of the USB ports disabling.	
	► Enable	Disable
USB 3.0 Port 0-1	Enables/disables USB port.	
	► Enable	Disable
USB 2.0 Port 0-1	Enables/disables USB port.	
	► Enable	Disable

4.5.3 CPU Related setting

CPU Related setting		
SVM support	Enables/disables SVM support.	
	► Enable	Disable
SMM Code Lock	Enables/disables the SMM code segment/registers.	
	► Enable	Disable
AMD CPU SMT Support	Select CPU Simultaneous multithreading support.	
	► Auto	Disable
AMD CPU P-state Control	Select CPU P-state Asl enable/disable.	
	► Enable	Disable

4.5.4 PCI SubSystem Setting

PCI SubSystem Setting		
Above 4G resource decoding	Enables/disables above 4G resource decoding	
	► Enable	Disable
Spread Spectrum	Enables/disables Spread Spectrum.	
	Enable	► Disable
PCIe SR-IOV	- Enabled: Enable SR-IOV function if PCIe Add-in Card Support. - Disabled: Disable SR-IOV function if PCIe Add-in Card Support.	
	► Enable	Disable
PCI NET Card UEFI OpROM	To load PCI Network add-on card embedded UEFI Option ROM during POST.	
	Enable	► Disable
PCI Storage Card UEFI OpROM	To load PCI Storage add-on card embedded UEFI Option ROM during POST.	
	► Enable	Disable

4.5.5 OEMBoard Function

OEMBOARD Function		
Messiah Function	SMBIOS Updated	Auto: Get data from BMC FRU and updated.
		► Auto By Utility

4.5.6 H2O IPMI Configuration

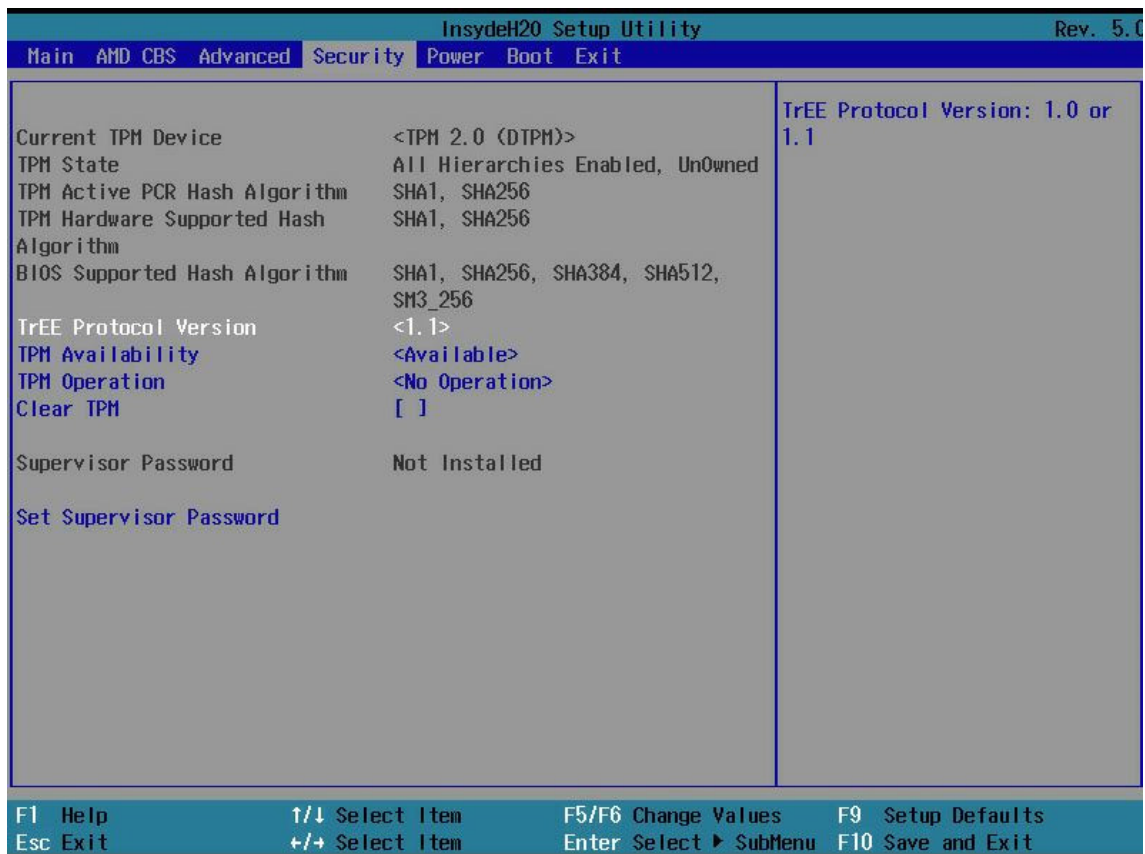
H2O IPMI Configuration		
IPMI Support	Enables/disables IPMI Support. Note: If changing to enable, BMC detailed information only valid after rebooting.	
	► Enable	Disable
BMC Warm Up Time	A maximum waiting time period from POST to BMC ready in seconds. Please increase the value if your BMC needs longer time to get ready.	
	► 60	Min=0, Max=240
ACPI SPMI Table	Enables/disables the ACPI SPMI Table for IPMI driver installation.	
	► Enable	Disable
Boot Option Support	Enables/disables IPMI boot option function.	
	► Enable	Disable
Set BIOS version to BMC	Enables/disables Set BIOS version to BMC. If the option is enabled, BIOS will send BIOS version string to BMC during POST.	
	Enable	► Disable
BMC Configuration	Watchdog Timer Support	Enables/disables BMC watchdog timer at start of POST.
		Enable ► Disable

BMC Configuration	Not disable in OS	Not disable bmc watchdog when boot to OS.			
		Enable		▶ Disable	
	Watchdog Timer Timeout	Enter the number of minutes the system firmware has to boot the OS before it takes the Timeout Action. Valid values are from 2 to 8 minutes.			
		▶ 5		Min=2, Max=8	
	Watchdog Timer Action	Timeout Action Choices: No Action, Hard Reset, Power Down or Power Cycle.			
		▶ Hard Reset		Power Down	Power Cycle
	Power Cycle Time Support	Enables/disables send power cycle time command to BMC.			
		Enable		▶ Disable	
	Power Cycle Time	The time that system power will be powered down during a power cycle operation initiated by the Chassis Control command or the watchdog time. Valid values are from 0 to 255 seconds.			
		▶ 10		Min=0, Max=255	
	Power Button	Enables/disables power button function.			
		Enable		▶ Disable	
	Reset Button	Enables/disables reset button function.			
		Enable		▶ Disable	
	NMI Button	Enables/disables NMI button function.			
		Enable		▶ Disable	
User Configuration	Lan Port Configuration	Config the LAN port access mode.			
		▶ Dedicate		Share	
	LAN Channel Number	Select the LAN channel number.			
		▶ 1		Min=0, Max=15	
	IPv4 Source	- DHCP: BMC IPv4 settings will be configured automatically by DHCP. - Static: BMC IPv4 settings will be configured manually			
		Static		▶ DHCP	
	IPv6 Mode	Enables/disables IPv6 internet protocol support.			
Enable		▶ Disable			
IPv6 Prefix Length	Sets IPv6 prefix length.				
	▶ 0		Min=0, Max=255		
SDR List	SDR List Support	Enable		▶ Disable	

4.5.7 SIO AST2500/2520

SIO AST2500/2520							
UART Port 1-4 Configuration	Configures UART Port using options: - Disabled: Disable device. - Enabled: Enable device and use below settings.						
	► Enable				Disable		
Base I/O Address	System I/O base resources.						
	► 3F8h	2F8h	3E8h	2E8h	338h	228h	220h 238h
Interrupt	System interrupt resources.						
	IRQ3	► IRQ4	IRQ5	IRQ6	IRQ7	IRQ10	IRQ11
Peripheral Type	Choose Port Mode: ► RS232						
Clock Source	Clock Source.						
	► 1.8462 MHz				24 MHz		

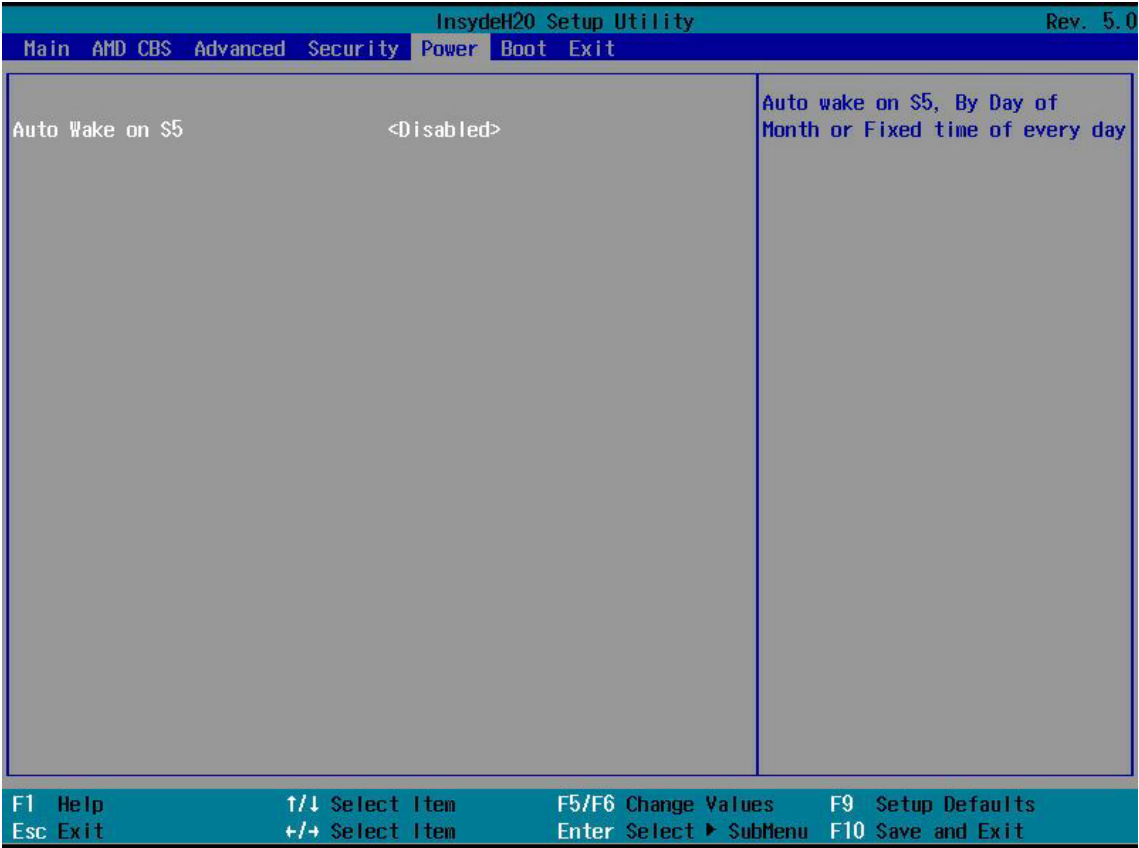
4.6 Security



4.6.1 H20 IPMI Configuration

H2O IPMI Configuration			
Current TPM Device	Current TPM Device: TPM1.2, or TPM2.0.		
	▶ Not Detected	TPM 1.2	TPM 2.0
TPM Availability	When Hidden, this option shields TPM from OS,		
	▶ Available	Hidden	
TPM Operation	Disables/enables TPM Function. This option will automatically return to No-Operation.		
	▶ No Operation	Disable and Deactivate	Enable and Activate
Clear TPM	Clears TPM. Removes all TPM context associated with a specific Owner.		
	▶ 0	1	None
TrEE Protocol Version	TrEE Protocol Version: 1.0 or 1.1		
	1.0	▶ 1.1	
TPM Availability	When Hidden, this option shields TPM from OS.		
	▶ Available	Hidden	
PCR Bank: SHA1	TCG2 Request PCR Bank: SHA1.		
	▶ 0	1	None
PCR Bank: SHA256/384/512/256	TCG2 Request PCR Bank: SHA1/SHA256/SHA384/SHA512/SM3_256.		
	▶ 0	1	None
Clear TPM	Clears TPM. Removes all TPM context associated with a specific Owner.		
	▶ 0	1	None
Power on Password	• Enabled: System will ask input password on post time. • Disabled: System will ask input password when go to Setup Utility.		
	Enable		▶ Disable

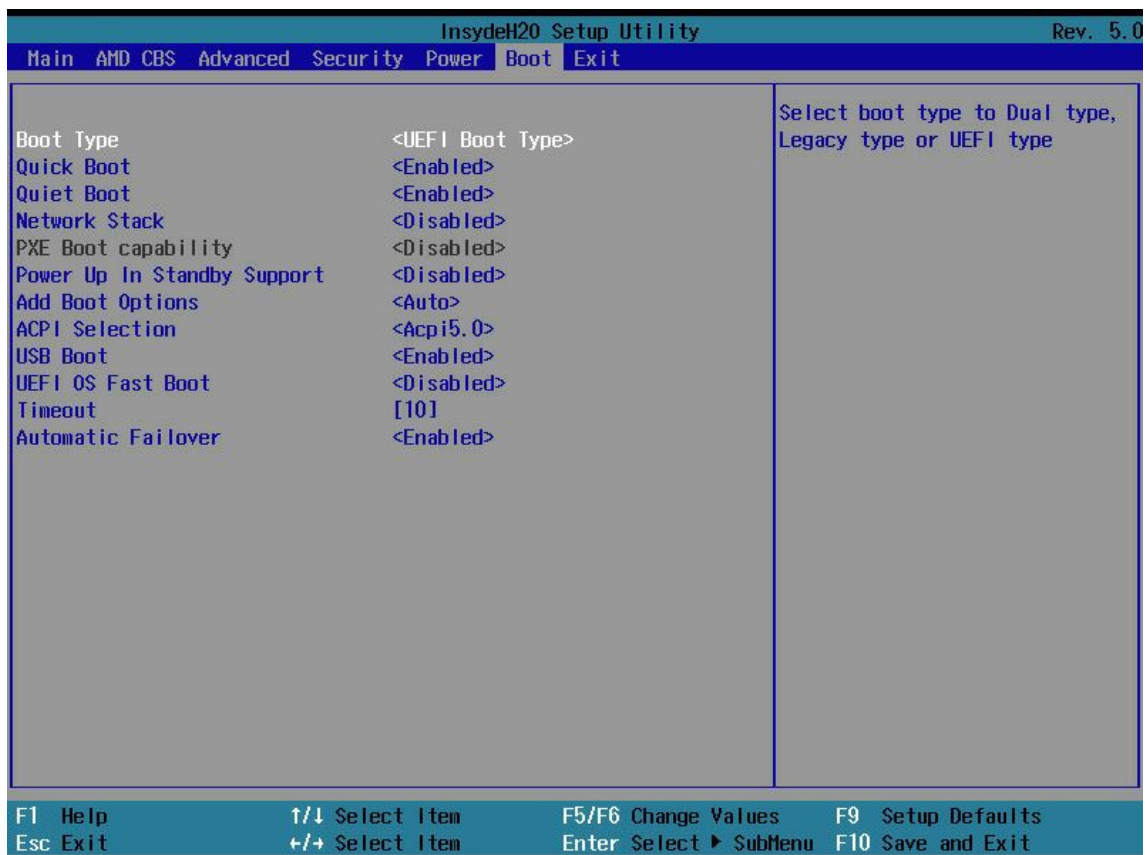
4.7 Power



4.7.1 Auto Wake on S5

Auto Wake on S5			
Auto Wake on S5	By Every Day	By Day of Month	► Disable

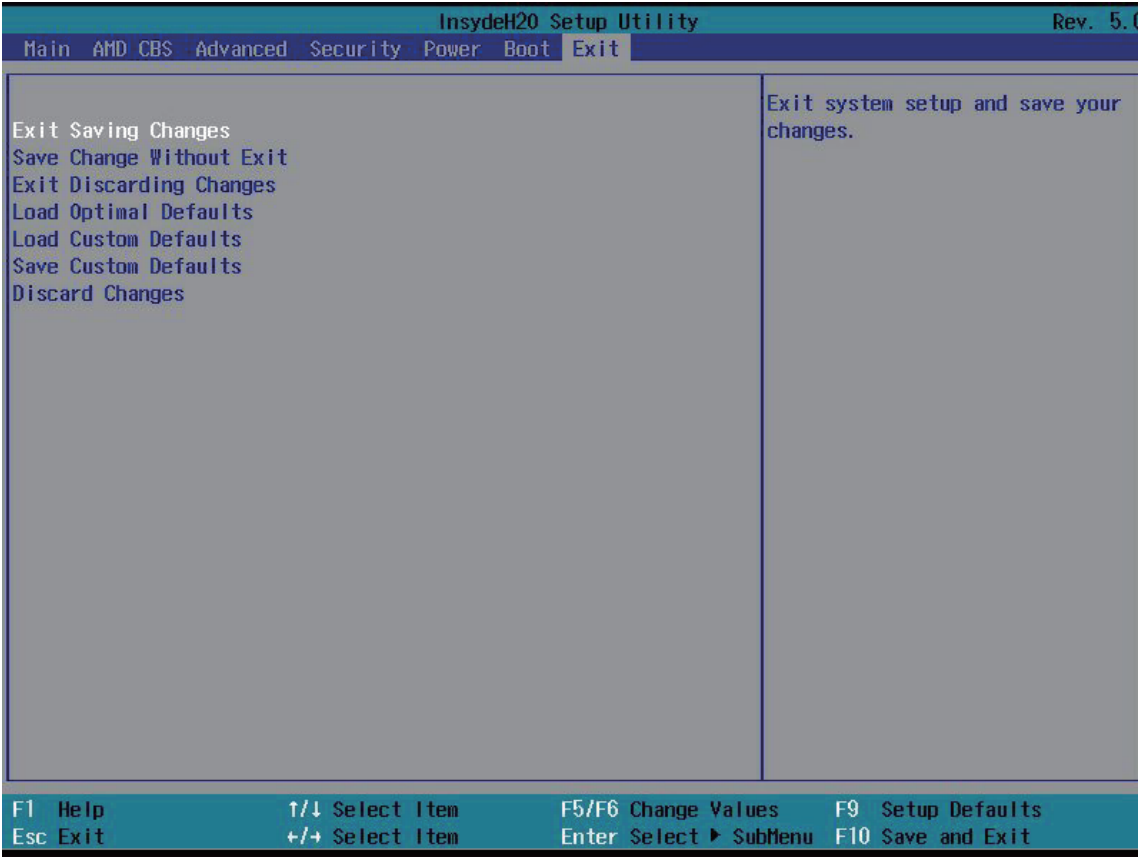
4.8 Boot



H2O IPMI Configuration							
Boot Type	UEFI Boot Type.						
Quick Boot	Allows InsydeH2O to skip certain tests while booting. This will decrease the time needed to boot the system.						
	► Enable			Disable			
Quiet Boot	Enables/disables or enables booting in Text Mode.						
	► Enable			Disable			
Network Stack	Network Stack Support: - Windows 8 BitLocker Unlock - UEFI IPv4/IPv6 PXE - Legacy PXE OPROM						
	Enable			► Disable			
PXE Boot to LAN	Enables/disables PXE boot to LAN.						
	Enable			► Disable			
PXE Boot capability	- Disabled: Support Network Stack - UEFI PXE: IPv4/IPv6 - Legacy: Legacy PXE OPROM only						
	Legacy	UEFI:IPv4	UEFI:IPv6	UEFI:IPv4/IPv6	Disable		
Power Up In Standby Support	Enables/disables Power Up In Standby Support. The PUIS feature set allows devices to be powered-up into the Standby power management state to minimize inrush current at power-up and to allow the host to sequence the spin-up of devices.						
	Enable			► Disable			
Add Boot Options	Positions in Boot Order for Shell, Network and Removable.						
	► Auto		First		Last		
ACPI Selection	Select booting to Acpi3.0/Acpi1.0B						
	Acpi1.0B	Acpi3.0	Acpi4.0	► Acpi5.0	Acpi6.0	Acpi6.1	Acpi6.2

USB Boot	Enables/disables booting to USB boot devices.	
	► Enable	Disable
UEFI OS Fast Boot	If enabled the system firmware does not initialize keyboard and check for firmware menu key.	
	Enable	► Disable
USB Hot Key Support	Enables/disables to support USB hot key while booting. This will decrease the time needed to boot the system.	
	► Enable	Disable
Timeout	The number of seconds that the firmware will wait before booting the original default boot selection.	
	► 10	Min=0, Max=10
Automatic Failover	• Enable: if boot to default device fail, it will directly try to boot next device. • Disable: if boot to default device fail, it will pop warning message then go into firmware UI.	
	► Enable	Disable

4.9 Exit



Save and Exit	
Exit Saving Changes	Exits system setup and save your changes.
Save Change Without Exit	Saves your changes without exiting the system.
Exit Discarding Changes	Discards your changes when existing the system.
Load Optimal Defaults	Loads your optimal defaults.
Load Custom Defaults	Resets the BIOS settings to the default values and overwrites any previously customized settings.
Save Custom Defaults	Saves the customized defaults in BIOS settings.
Discard Changes	Discards your changes.

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: Khoroshevskoye Shosse, 32A,
Office 403 (2nd Entrance, 4th Floor),
Moscow 123007, Russia
Tel: +7-4997019998
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States

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

South California, United States

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

New Jersey, United States

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

Houten, The Netherlands

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