

OPEN Industry Standard, Flexible Architecture

GREEN Less Heat, Less Power Consumption

STABLE Robust Design, Quality Parts

Stable and
Reliable Solution

Server/Workstation
Motherboard

SP2C741D16HM3

User Manual

English



Version 1.20

Published Jun. 2025

Copyright©2025 ASRock Rack INC. All rights reserved.

Copyright Notice:

No part of this documentation may be reproduced, transcribed, transmitted, or translated in any language, in any form or by any means, except duplication of documentation by the purchaser for backup purpose, without written consent of ASRock Rack Inc.

Products and corporate names appearing in this documentation may or may not be registered trademarks or copyrights of their respective companies, and are used only for identification or explanation and to the owners' benefit, without intent to infringe.

Disclaimer:

Specifications and information contained in this documentation are furnished for informational use only and subject to change without notice, and should not be constructed as a commitment by ASRock Rack. ASRock Rack assumes no responsibility for any errors or omissions that may appear in this documentation.

With respect to the contents of this documentation, ASRock Rack does not provide warranty of any kind, either expressed or implied, including but not limited to the implied warranties or conditions of merchantability or fitness for a particular purpose.

In no event shall ASRock Rack, its directors, officers, employees, or agents be liable for any indirect, special, incidental, or consequential damages (including damages for loss of profits, loss of business, loss of data, interruption of business and the like), even if ASRock Rack has been advised of the possibility of such damages arising from any defect or error in the documentation or product.



The terms HDMI® and HDMI High-Definition Multimedia Interface, and the HDMI logo are trademarks or registered trademarks of HDMI Licensing LLC in the United States and other countries.

WARNING



THIS PRODUCT CONTAINS A BUTTON BATTERY

If swallowed, a button battery can cause serious injury or death.

Please keep batteries out of sight or reach of children.

ASRock Rack's Website: www.ASRockRack.com

INTEL END USER SOFTWARE LICENSE AGREEMENT
IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING.

LICENSE. Licensee has a license under Intel's copyrights to reproduce Intel's Software only in its unmodified and binary form, (with the accompanying documentation, the "Software") for Licensee's personal use only, and not commercial use, in connection with Intel-based products for which the Software has been provided, subject to the following conditions:

- (a) Licensee may not disclose, distribute or transfer any part of the Software, and You agree to prevent unauthorized copying of the Software.
- (b) Licensee may not reverse engineer, decompile, or disassemble the Software.
- (c) Licensee may not sublicense the Software.
- (d) The Software may contain the software and other intellectual property of third party suppliers, some of which may be identified in, and licensed in accordance with, an enclosed license.txt file or other text or file.
- (e) Intel has no obligation to provide any support, technical assistance or updates for the Software.

OWNERSHIP OF SOFTWARE AND COPYRIGHTS. Title to all copies of the Software remains with Intel or its licensors or suppliers. The Software is copyrighted and protected by the laws of the United States and other countries, and international treaty provisions. Licensee may not remove any copyright notices from the Software. Except as otherwise expressly provided above, Intel grants no express or implied right under Intel patents, copyrights, trademarks, or other intellectual property rights. Transfer of the license terminates Licensee's right to use the Software.

DISCLAIMER OF WARRANTY. The Software is provided "AS IS" without warranty of any kind, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

LIMITATION OF LIABILITY. NEITHER INTEL NOR ITS LICENSORS OR SUPPLIERS WILL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS, OR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER UNDER THIS AGREEMENT OR OTHERWISE, EVEN IF INTEL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

LICENSE TO USE COMMENTS AND SUGGESTIONS. This Agreement does NOT obligate Licensee to provide Intel with comments or suggestions regarding the Software. However, if Licensee provides Intel with comments or suggestions for the modification,

correction, improvement or enhancement of (a) the Software or (b) Intel products or processes that work with the Software, Licensee grants to Intel a non-exclusive, worldwide, perpetual, irrevocable, transferable, royalty-free license, with the right to sublicense, under Licensee's intellectual property rights, to incorporate or otherwise utilize those comments and suggestions.

TERMINATION OF THIS LICENSE. Intel or the sublicensor may terminate this license at any time if Licensee is in breach of any of its terms or conditions. Upon termination, Licensee will immediately destroy or return to Intel all copies of the Software.

THIRD PARTY BENEFICIARY. Intel is an intended beneficiary of the End User License Agreement and has the right to enforce all of its terms.

U.S. GOVERNMENT RESTRICTED RIGHTS. The Software is a commercial item (as defined in 48 C.F.R. 2.101) consisting of commercial computer software and commercial computer software documentation (as those terms are used in 48 C.F.R. 12.212), consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4. You will not provide the Software to the U.S. Government. Contractor or Manufacturer is Intel Corporation, 2200 Mission College Blvd., Santa Clara, CA 95054.

EXPORT LAWS. Licensee agrees that neither Licensee nor Licensee's subsidiaries will export/re-export the Software, directly or indirectly, to any country for which the U.S. Department of Commerce or any other agency or department of the U.S. Government or the foreign government from where it is shipping requires an export license, or other governmental approval, without first obtaining any such required license or approval. In the event the Software is exported from the U.S.A. or re-exported from a foreign destination by Licensee, Licensee will ensure that the distribution and export/re-export or import of the Software complies with all laws, regulations, orders, or other restrictions of the U.S. Export Administration Regulations and the appropriate foreign government.

APPLICABLE LAWS. This Agreement and any dispute arising out of or relating to it will be governed by the laws of the U.S.A. and Delaware, without regard to conflict of laws principles. The Parties to this Agreement exclude the application of the United Nations Convention on Contracts for the International Sale of Goods (1980). The state and federal courts sitting in Delaware, U.S.A. will have exclusive jurisdiction over any dispute arising out of or relating to this Agreement. The Parties consent to personal jurisdiction and venue in those courts. A Party that obtains a judgment against the other Party in the courts identified in this section may enforce that judgment in any court that has jurisdiction over the Parties.

CALIFORNIA, USA ONLY

The Lithium battery adopted on this motherboard contains Perchlorate, a toxic substance controlled in Perchlorate Best Management Practices (BMP) regulations passed by the California Legislature. When you discard the Lithium battery in California, USA, please follow the related regulations in advance.

"Perchlorate Material-special handling may apply, see www.dtsc.ca.gov/hazardouswaste/perchlorate"

AUSTRALIA ONLY

Our goods come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and compensation for any other reasonably foreseeable loss or damage caused by our goods. You are also entitled to have the goods repaired or replaced if the goods fail to be of acceptable quality and the failure does not amount to a major failure. If you require assistance please call ASRock Rack Tel : +886-2-55599600 ext.123 (Standard International call charges apply)

Licensee's specific rights may vary from country to country.



This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) this device may not cause harmful interference, and
- (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following

measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.



ASRock Rack INC. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related UKCA Directives. Full text of UKCA declaration of conformity is available at: <http://www.asrockrack.com>



ASRock Rack INC. hereby declares that this device is in compliance with the essential requirements and other relevant provisions of related Directives. Full text of EU declaration of conformity is available at: <http://www.asrockrack.com>

ASRock Rack follows the green design concept to design and manufacture our products, and makes sure that each stage of the product life cycle of ASRock Rack product is in line with global environmental regulations. In addition, ASRock Rack disclose the relevant information based on regulation requirements.

Please refer to <https://www.asrockrack.com/general/about.asp?cat=Responsibility> for information disclosure based on regulation requirements ASRock Rack is complied with:



DO NOT throw the motherboard in municipal waste. This product has been designed to enable proper reuse of parts and recycling. This symbol of the crossed out wheeled bin indicates that the product (electrical and electronic equipment) should not be placed in municipal waste. Check local regulations for disposal of electronic products.

Contents

Chapter 1 Introduction	1
1.1 Package Contents	1
1.2 Specifications	2
1.3 Unique Features	5
1.4 Motherboard Layout	6
1.5 Onboard LED Indicators	9
1.6 I/O Panel	11
1.7 Block Diagram	12
Chapter 2 Installation	13
2.1 Screw Holes	13
2.2 Pre-installation Precautions	13
2.3 Installing the CPU and Heatsink	14
2.4 Installing Memory Modules (DIMM)	21
2.4.1 Memory Support	21
2.4.2 Memory Configurations	22
2.5 Expansion Slots (PCI Express Slots)	25
2.6 Jumper Setup	26
2.7 Onboard Headers and Connectors	28
2.8 Unit Identification purpose LED/Switch	37
2.9 M.2 SSD Module Installation Guide	38
Chapter 3 UEFI Setup Utility	39
3.1 Introduction	39
3.1.1 UEFI Menu Bar	39

3.1.2	Navigation Keys	40
3.2	Main Screen	41
3.2.1	Motherboard Information	42
3.2.2	Processor Information	42
3.2.3	Memory Information	43
3.3	Advanced Screen	44
3.3.1	CPU Configuration	45
3.3.2	Platform Power Configuration	47
3.3.3	DRAM Configuration	50
3.3.4	Chipset Configuration	52
3.3.5	Storage Configuration	55
3.3.6	NVMe Configuration	56
3.3.7	ACPI Configuration	57
3.3.8	USB Configuration	58
3.3.9	Super IO Configuration	59
3.3.10	Serial Port Console Redirection	60
3.3.11	H/W Monitor	63
3.3.12	Runtime Error Logging	64
3.3.13	Intel SPS Configuration	66
3.3.14	Network Stack Configuration	67
3.3.15	Intel VMD technology	68
3.3.16	Driver Health	69
3.3.17	Tls Auth Configuration	70
3.3.18	Instant Flash	71

3.4	Server Mgmt	72
3.4.1	BMC Network Configuration	74
3.4.2	System Event Log	76
3.4.3	BMC Tools	77
3.5	Security	78
3.5.1	Key Management	79
3.6	Event Logs	83
3.7	Boot Screen	84
3.8	Exit Screen	85
Chapter 4 Software Support		86
4.1	Download and Install Operating System	86
4.2	Download and Install Software Drivers	86
4.3	Contact Information	86
Chapter 5 Troubleshooting		87
5.1	Troubleshooting Procedures	87
5.2	Technical Support Procedures	89
5.3	Returning Merchandise for Service	89

Chapter 1 Introduction

Thank you for purchasing ASRock Rack **SP2C741D16HM3** motherboard, a reliable motherboard produced under ASRock Rack's consistently stringent quality control. It delivers excellent performance with robust design conforming to ASRock Rack's commitment to quality and endurance.

In this manual, chapter 1 and 2 contains introduction of the motherboard and step-by-step guide to the hardware installation. Chapter 3 and 4 contains the configuration guide to BIOS setup and information of the Support CD.



Because the motherboard specifications and the BIOS software might be updated, the content of this manual will be subject to change without notice. In case any modifications of this manual occur, the updated version will be available on ASRock Rack website without further notice. Find the latest memory and CPU support lists on ASRock Rack website as well. ASRock Rack's Website: www.ASRockRack.com

*Please visit the website for specific information and technical support:
<http://www.asrockrack.com/support/>*

1.1 Package Contents

- ASRock Rack SP2C741D16HM3 motherboard
(Half-Width form factor: 6.7" x 21", 170.18mm x 533.4mm)
- 2 Screws for M.2 sockets
- 4 CPU Non-Fabric carriers (2xE1A, 2xE1B)



If any items are missing or appear damaged, contact the authorized dealer.

1.2 Specifications

SP2C741D16HM3	
Physical Status	
Form Factor	Half-Width
Dimension	6.7" x 21" (170.18mm x 533.4mm)
Processor System	
CPU	Supports 5 th and 4 th Gen Intel® Xeon® Scalable processors
Socket	1+1 Socket E (LGA4677)
Thermal Design Power (TDP)	350W
Chipset	Intel® C741
System Memory	
Supported DIMM Quantity	8+8 DIMM slots (1DPC)
Supported Type	288-pin DDR5 RDIMM/RDIMM-3DS
Max. Capacity per DIMM	RDIMM: 96GB RDIMM-3DS: 2H- 128GB/4H- 256GB
Max. DIMM Frequency	5600 MT/s on 5 th Gen Intel® Xeon® Scalable Processors 4800 MT/s on 4 th Gen Intel® Xeon® Scalable Processors
Voltage	1.1V
Note: Memory support is to be validated.	
PCIe Expansion Slots	
PCIe x16	SLOT2: Gen Z 4C (PCIe5.0/CXL1.1 x16) [CPU0]
	SLOT1: Gen Z 4C (PCIe5.0/CXL1.1 x16) [CPU0]
Other PCIe Expansion Connectors	
M.2	2 M-key (PCIe4.0 x4 or SATA 6Gb/s); supports 2280 form factor [CPU0]
MCIO	2 MCIO (PCIe5.0 x8) [CPU0]
Others	2 ExaMAX (PCIe5.0 x16) [CPU1] 1 SlimSAS*
*SAS is supported by additional RAID card only; The SlimSAS is reserved only to extend SAS from RAID card to ExaMAX3.	
SATA/SAS Storage	
PCH Built-in Storage	Intel® C741 (Up to 10 SATA 6Gb/s, support RAID 0/1/5/10); 2 SATA 7-pin, 2 M.2, 1 ExaMAX3 for 6 SATA
Ethernet	
Additional GbE Controller	1 RJ45* (1GbE) by Intel® i210
OCP Slot	1 OCP NIC 3.0 (PCIe5.0) [CPU0]
*SP2C741D16HM3 has only 1 RJ45 for dedicated IPMI or shared NIC, and is configurable by jumper setting.	

Server Management	
BMC Controller	ASPEED AST2600: IPMI2.0 with iKVM and vMedia support
IPMI Dedicated GLAN	2 Realtek RTL8211F for dedicated management GLAN*
*SP2C741D16HM3 has only 1 RJ45 for dedicated IPMI or shared NIC, and is configurable by jumper setting.	
Graphics	
Controller	ASPEED AST2600: 1 DB15 (VGA)
Rear I/O	
UID Button/LED	1 UID button w/ LED
VGA	1 DB15 (VGA)
USB	2 Type-A (USB3.2 Gen1)
RJ45	1 RJ45 (dedicated IPMI or Intel® i210 share NIC)
Internal Connectors/Headers	
Power Connector	3 Micro-Hi (8-pin, 12V), 1 (19-pin, CM Board Standby Power 12V)
Auxiliary Panel Header	1 (17-pin): chassis intrusion, system fault LED, locate, SMBus
System Panel Header	1 (9-pin): power switch, reset switch, system power LED, HDD activity LED
NMI Header	1
COM Header	1
Speaker Header	1 (4-pin)
Fan Header	6 (6-pin)
TPM Header	1 (13-pin, SPI)
VROC Header	1
SGPIO Header	1
HSBP	2
SMBus Header	1
PMbus Header	1
IPMB Header	1
Clear CMOS	1
USB 2.0 Header	2 USB2.0 in ExaMAX3
LED Indicators	
Standby Power LED	1
Fan Fail LED	6
BMC Heartbeat LED	1
Other LED	1 CPU CATERR LED
System BIOS	
Type	AMI UEFI BIOS; 512Mb SPI Flash ROM
Features	Plug and Play (PnP), ACPI 4.0 and above compliance wake up events, SMBIOS 3.4 and above , ASRock Rack Instant Flash

Hardware Monitor	
Temperature	CPU, PCH, MB, Card side, TR1 Temperature sensing
Fan	Fan Tachometer CPU Quiet Fan (Allow Chassis Fan Speed Auto-Adjust by CPU Temperature) Fan Multi-Speed Control
Voltage	PVCCIN_CPU0, PVCCIN_CPU1, PCH_PVNN, 1.05V_PCH, 1.8V_PCH, 12VSB, 5VSB, 3VSB, 12V, 5V, 3V, BAT
Supported OS	
OS	Microsoft® Windows® - Server 2022 (64bit) Linux® - Red Hat Enterprise Linux Server 8.4 (64bit) / 8.5 (64bit) / 9.1 (64bit) - SUSE Enterprise Linux Server 15 SP3 (64bit) - Ubuntu 21.10 (64bit) / 22.04 (64bit) Hypervisor - VMWare® ESXi 7.0 U3g / 8.0 <i>*Please refer to the website for the latest OS support list.</i>
Enviroment	
Operating Temperature	10°C - 35°C
Non-operating Temperature	-40°C - 70°C

NOTE: Please refer to the website for the latest specifications.



If installing Intel® LAN utility or Marvell SATA utility, this motherboard may fail Windows® Hardware Quality Lab (WHQL) certification tests. If installing the drivers only, it will pass the WHQL tests.

1.3 Unique Features

ASRock Rack Instant Flash is a BIOS flash utility embedded in Flash ROM. This convenient BIOS update tool allows user to update system BIOS without entering operating systems first like MS-DOS or Windows*. With this utility, press the <F6> key during the POST or the <F2> key to enter into the BIOS setup menu to access ASRock Rack Instant Flash. Just launch this tool and save the new BIOS file to the USB flash drive, floppy disk or hard drive, then update the BIOS only in a few clicks without preparing an additional floppy diskette or other complicated flash utility. Please be noted that the USB flash drive or hard drive must use FAT32/16/12 file system.

English

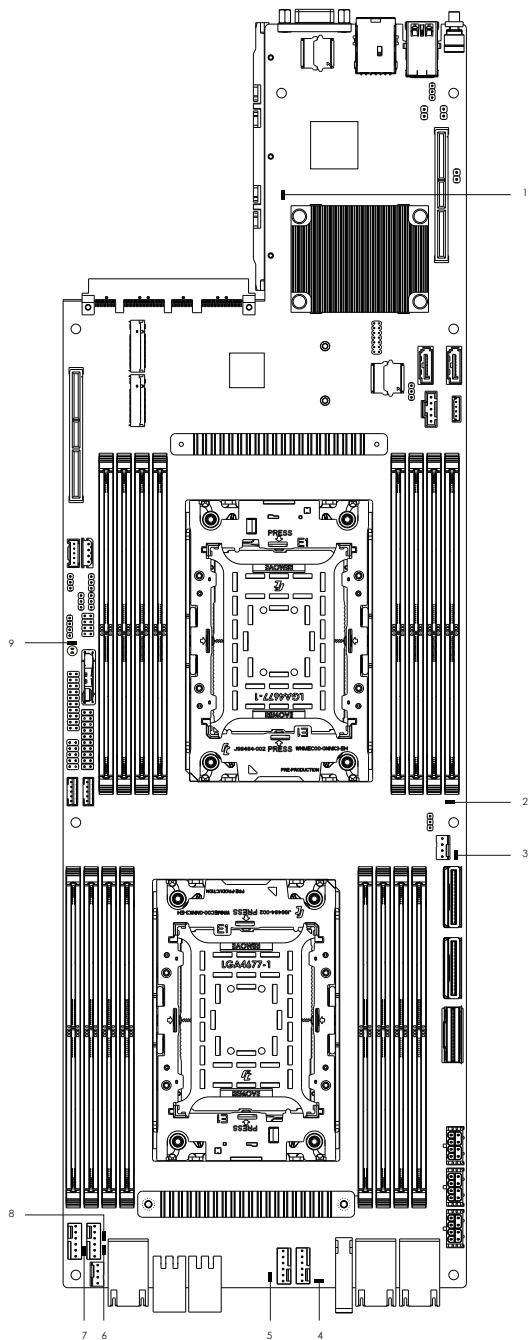


No.	Description
1	LAN Selection Jumper (LAN_SW1)
2	Password Reset Jumper (PASSWORD_CLEAR1)
3	Non Maskable Interrupt Button (NMI_BTN1)
4	PCI Express 5.0 x16 Slot (PCIE1)
5	BIOS Swap Override Jumper (BIOS_SWAP_OVERRIDE)
6	TPM-SPI Header (TPM_BIOS_PH1)
7	SATA3 Connector (SATA0)
8	SATA3 Connector (SATA1)
9	PWM Configuration Header (PWM_CFG1)
10	Virtual RAID On CPU Header (RAID_1)
11	PSU SMBus Header (PSU_SMB1)
12	2 x 288-pin DDR5 DIMM Slots (DDR5_E1, DDR5_G1)*
13	2 x 288-pin DDR5 DIMM Slots (DDR5_F1, DDR5_H1)*
14	LGA4677 CPU Socket (CPU0)
15	BPB Signal Source Selection Jumper (MUX_SW1)
16	System Fan Connector (FAN6)
17	Mini Cool Edge IO x8 Connector (MCIO2)
18	Mini Cool Edge IO x8 Connector (MCIO1)
19	Slimline x8 Connector (SLIMLIN1)
20	ATX 12V Power Connector (12VCON3)
21	ATX 12V Power Connector (12VCON2)
22	ATX 12V Power Connector (12VCON1)
23	2 x 288-pin DDR5 DIMM Slots (DDR5_J1, DDR5_L1)*
24	2 x 288-pin DDR5 DIMM Slots (DDR5_I1, DDR5_K1)*
25	System Fan Connector (FAN4)
26	System Fan Connector (FAN3)
27	2 x 288-pin DDR5 DIMM Slots (DDR5_M1, DDR5_O1)*
28	System Fan Connector (FAN5)
29	System Fan Connector (FAN2)
30	System Fan Connector (FAN1)
31	2 x 288-pin DDR5 DIMM Slots (DDR5_N1, DDR5_P1)*
32	LGA 4677 CPU Socket (CPU1)
33	Backplane PCI Express Hot-Plug Connector (CPU1_HSBP1)
34	Backplane PCI Express Hot-Plug Connector (CPU0_HSBP1)
35	System Panel Header (PANEL1)

No.	Description
36	Auxiliary Panel Header (AUX_PANEL1)
37	CM Board Standby Power Header (CM_SB_R)
38	SATA SGPIO Connector (SATA_SGPIO1)
39	Clear CMOS Pad (CLRMOS1)
40	Speaker Header (SPEAKER1)
41	CPU PECI Mode Jumper (PECI1)
42	ME Recovery Jumper (ME_RECOVERY1)
43	Thermal Sensor Header (TR1)
44	COM Header (COM1)
45	BMC SMBus Header (BMC_SMB1)
46	Intelligent Platform Management Bus Header (IPMB1)
47	2 x 288-pin DDR5 DIMM Slots (DDR5_B1, DDR5_D1)*
48	2 x 288-pin DDR5 DIMM Slots (DDR5_A1, DDR5_C1)*
49	PCI Express 5.0 x16 Slot (PCIE2)
50	M-key M.2 Socket (M2_1) (Type 2280)
51	M-key M.2 Socket (M2_2) (Type 2280)
52	OCP 3.0 Gen5 x16 NIC Slot (OCP1)

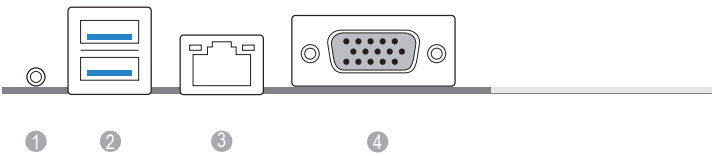
* For DIMM installation and configuration instructions, please see p.20 (Installation of Memory Modules (DIMM)) for more details.

1.5 Onboard LED Indicators



No.	Item	Status	Description
1	BMC_LED1	Green	BMC heartbeat LED
2	CATERR	Red	CPU CATERR error
3	LED_FAN6	Red	FAN6 failed
4	LED_FAN4	Red	FAN4 failed
5	LED_FAN3	Red	FAN3 failed
6	LED_FAN5	Red	FAN5 failed
7	LED_FAN1	Red	FAN1 failed
8	LED_FAN2	Red	FAN2 failed
9	SB_PWR1	Green	STB PWR ready

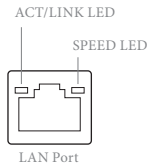
1.6 I/O Panel



No.	Description	No.	Description
1	UID Switch (UID1)	3	LAN RJ-45 Port (IPMI_LAN1)*
2	USB 3.2 Gen1 Ports (USB3_1_2)	4	VGA Port (VGA1)

LAN Port LED Indications

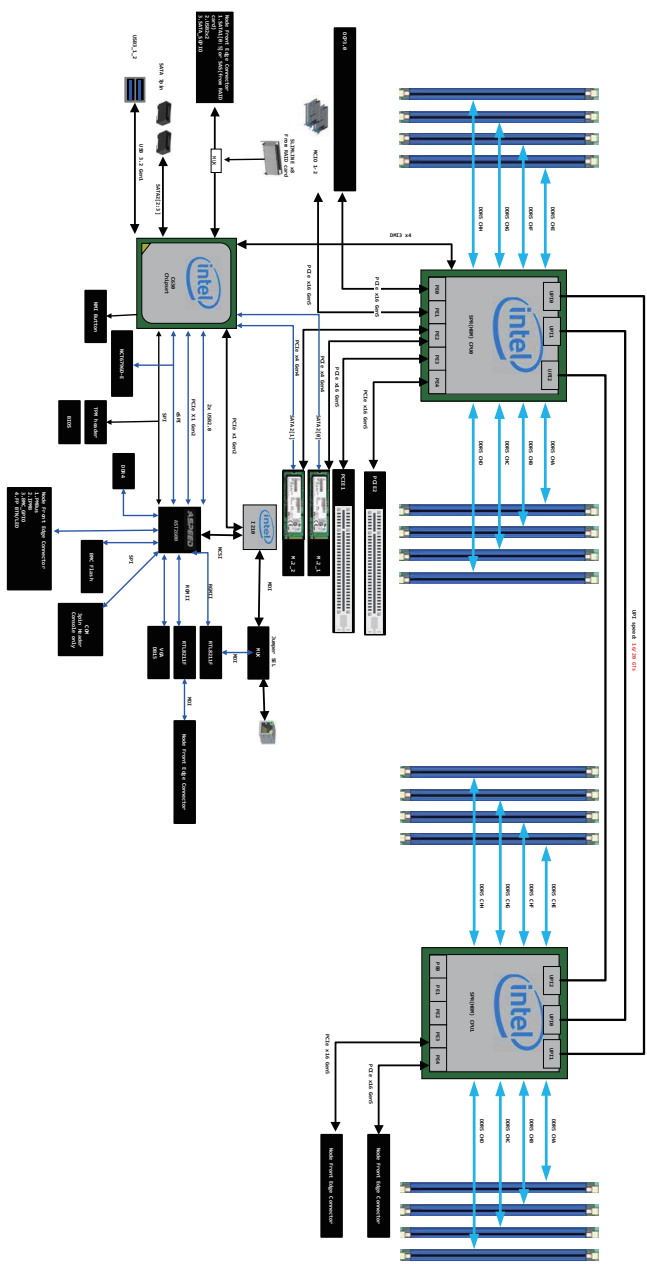
*There are two LED next to the LAN port. Please refer to the table below for the LAN port LED indications.



Dedicated IPMI LAN Port LED Indications

Activity / Link LED		Speed LED	
Status	Description	Status	Description
Off	No Link	Off	10M bps connection or no link
Blinking Yellow	Data Activity	Yellow	100M bps connection
On	Link	Green	1Gbps connection

1.7 Block Diagram



Chapter 2 Installation

This is a half-width form factor (6.7" x 21") motherboard. Before installing the motherboard, study the configuration of the chassis to ensure that the motherboard fits into it.



Make sure to unplug the power cord before installing or removing the motherboard. Failure to do so may cause physical injuries and motherboard damages.

2.1 Screw Holes

Place screws into the holes indicated by circles to secure the motherboard to the chassis.



Attention! Before installing this motherboard, be sure to unscrew and remove the standoff at the marked location, under the motherboard, from the chassis, in order to avoid electrical short circuit and damage to the motherboard.



Do not over-tighten the screws! Doing so may damage the motherboard.

2.2 Pre-installation Precautions

Take note of the following precautions before installing motherboard components or change any motherboard settings.

1. Unplug the power cord from the wall socket before touching any components.
2. To avoid damaging the motherboard's components due to static electricity, NEVER place the motherboard directly on the carpet or the like. Also remember to use a grounded wrist strap or touch a safety grounded object before handling the components.
3. Hold components by the edges and do not touch the ICs.
4. Whenever uninstall any component, place it on a grounded anti-static pad or in the bag that comes with the component.
5. When placing screws into the screw holes to secure the motherboard to the chassis, please do not over-tighten the screws! Doing so may damage the motherboard.



Before installing or removing any component, ensure that the power is switched off or the power cord is detached from the power supply. Failure to do so may cause severe damage to the motherboard, peripherals, and/or components.

2.3 Installing the CPU and Heatsink

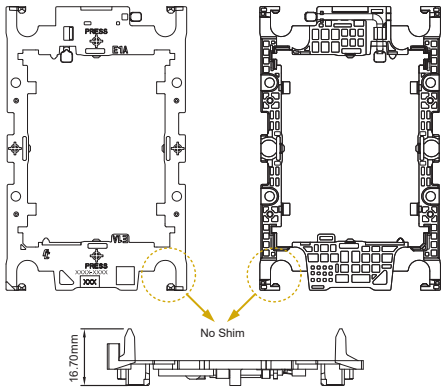


1. Unplug all power cables before installing the CPU.
2. Illustration in this documentation are examples only.

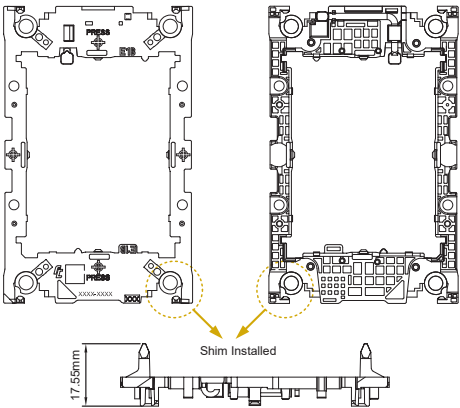
Carrier Used

Carrier Type	Xeon® SP XCC	Xeon® SP MCC/LCC
Carrier Code	E1A	E1B
Shim	No	Yes
Carrier Height	16.70mm	17.55mm

XCC Carrier

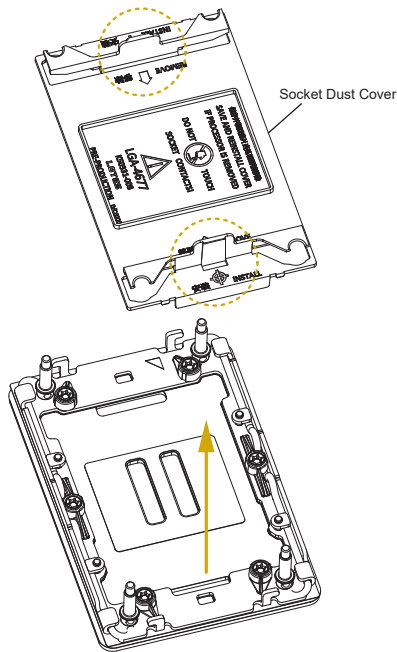


MCC Carrier

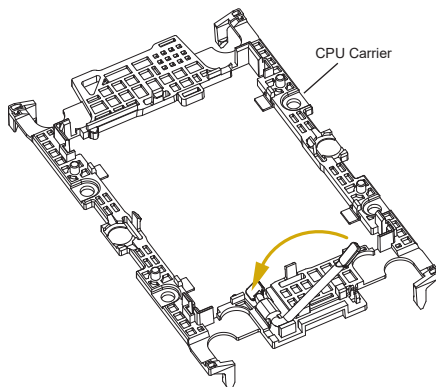


Follow the steps below to finish the CPU installation and please save the Socket Dust Cover when returning for service.

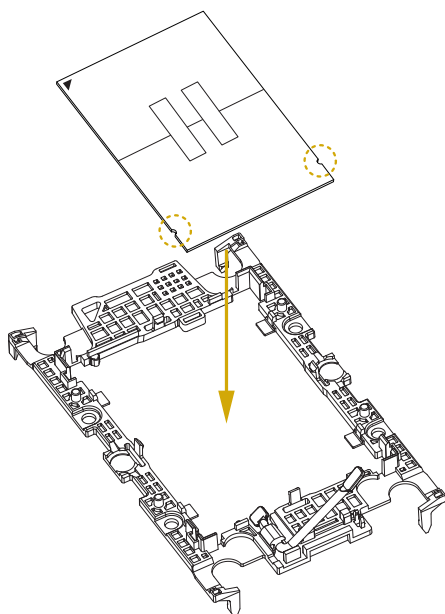
1



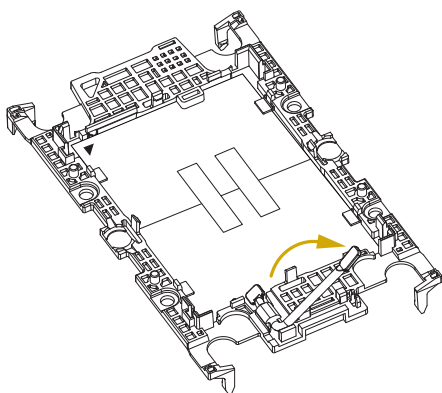
2



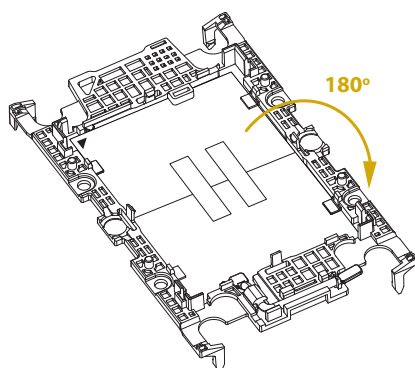
3



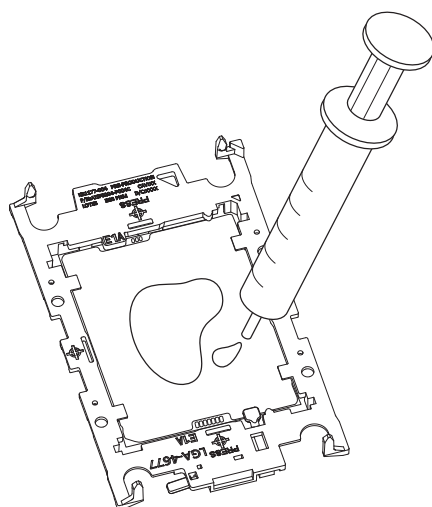
4



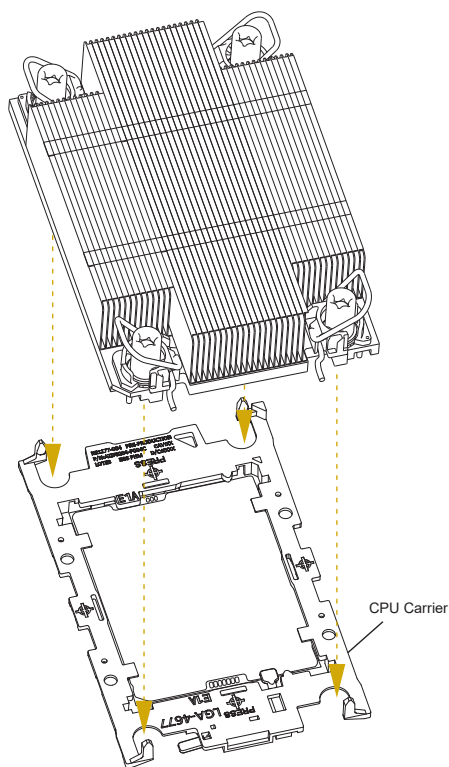
5



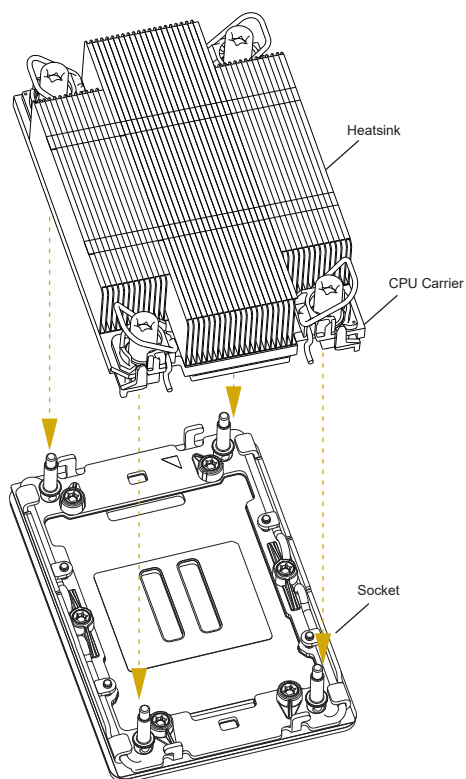
6



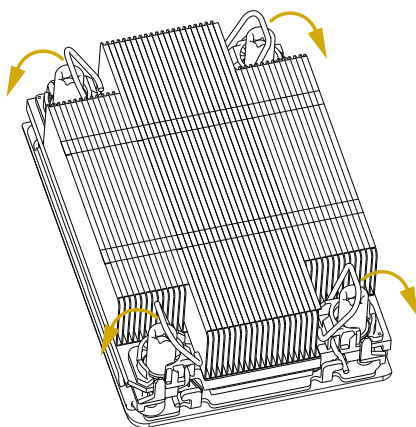
7



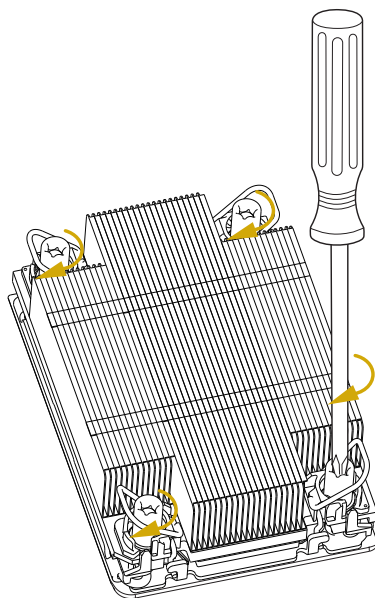
8



9



10



2.4 Installing Memory Modules (DIMM)

This motherboard provides sixteen 288-pin DDR5 (Double Data Rate 5) DIMM slots in two groups, and supports Single Channel Memory Technology.

CPU0	CPU1
DDR5_A1, B1, C1, D1, E1, F1, G1 H1	DDR5_I1, J1, K1, L1, M1, N1, O1, P1



- 1. Before installing a memory module, make sure to turn off the computer and unplug the powercord from the power outlet to prevent damage to the memory module.
- 2. For Eight channel configuration, it always needs to install identical (the same brand, speed, size and chip-type) DDR5 DIMM groups.
- 3. It is not allowed to install a DDR, DDR2, DDR3 or DDR4 memory module into a DDR5 slot; otherwise, this motherboard and DIMM may be damaged.

2.4.1 Memory Support

4th Gen Intel® Xeon® Scalable Processors - SP

Type	Ranks Per DIMM and Data Width	DRAM Density & DIMM Capacity			Speed (MT/s); Voltage (V); DIMM Per Channel (DPC)	
					1DPC ¹	2DPC
		16Gb	24Gb ²	32Gb	1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB	NA	4800	4400
	SRx4 (RC C)	32GB	48GB	NA		
	SRx4 (RC F) 9x4	32GB	NA	NA		
	DRx8 (RC E)	32GB	48GB	NA		
	DRx4 (RC A)	64GB	96GB	128GB		
	DRx4 (RC B) 9x4	64GB	NA	NA		
RDIMM-3DS	(4R/8R) x4	2H-128GB	NA	NA		
	(RC A)	4H-256GB				

Note1: 1DPC applies to 1 SPC or 2SPC implementations (SPC-Sockets Per Channel).

Note2: 24Gb XCC only w/ limited configs: 1DPC all DIMM types, 2DPC 96GB only. Only 8 and 16 DIMM configs, no fallbacks.

Note3: The memory speed will be 4800 MT/s 1DPC and 4400 MT/s 2DPC.

Note4: The table is for reference only.

5th Gen Intel® Xeon® Scalable Processors - SP

Type	Ranks Per DIMM and Data Width	DRAM Density & DIMM Capacity			Speed (MT/s); Voltage (V); DIMM Per Channel (DPC)	
					1DPC ¹	2DPC
		16Gb	24Gb	32Gb	1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB ²	NA	5600 ³	4400 ³
	SRx4 (RC C)	32GB	48GB ²	NA		
	SRx4 (RC F) 9x4	NA	NA	NA		
	DRx8 (RC E)	32GB	48GB ²	NA		
	DRx4 (RC A)	64GB	96GB	128GB		
	DRx4 (RC B) 9x4	NA	NA	NA		
RDIMM- 3DS	(4R/8R) x4 (RC A)	2H-128GB 4H-256GB	NA	NA	5600 ⁴	

Note1: 1DPC applies to 1 SPC or 2SPC implementations (SPC-Sockets Per Channel).

Note2: 24Gb 2DPC not POR w/ 24GB and 48GB DIMMs.

Note3: DDR5-5600 RDIMMs will be limited to 5600 MT/s 1DPC and 4400 MT/s 2DPC. DDR5-4800 DIMMs will be limited to 4800 MT/s 1DPC and 4400 MT/s 2DPC.

Note4: DDR5-5600 DIMM are required for 5600 and 5200 1DPC speeds.

Note5: EE LCC DDR5 memory support POR is 16GB/24GB/32GB at 4400 for 1DPC and 2DPC.

Note6: The table is for reference only.

2.4.2 Memory Configurations

1 CPU Configurations (Single P)

DIMM Slot		DIMM Number											
		1	1	1	1	2	2	4	6	6	6	6	8
CPU0	A1	V				V		V	V	V		V	V
	B1			V						V	V	V	V
	C1						V	V	V	V	V		V
	D1								V		V	V	V
	E1		V				V	V	V	V	V		V
	F1				V				V		V	V	V
	G1					V		V	V	V		V	V
	H1										V	V	V

The symbol V indicates the slot is populated.

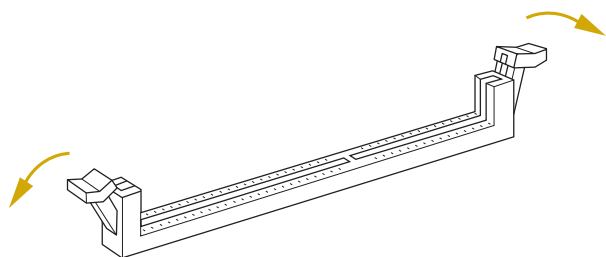
2 CPU Configurations (Dual P)

DIMM Slot		DIMM Number											
		1	1	1	1	2	2	4	6	6	6	6	8
CPU0	A1	V				V		V	V	V		V	V
	B1			V						V	V	V	V
	C1					V	V	V	V	V			V
	D1								V		V	V	V
	E1		V			V	V	V	V	V			V
	F1				V				V		V	V	V
	G1					V		V	V	V		V	V
	H1									V	V	V	V

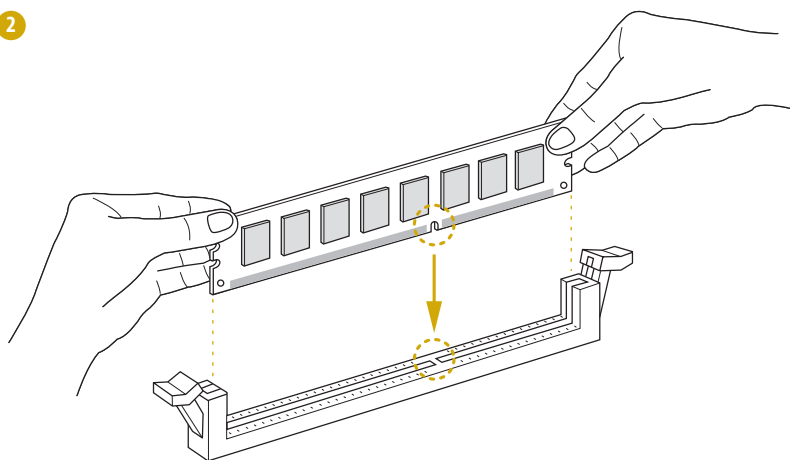
DIMM Slot		DIMM Number											
		1	1	1	1	2	2	4	6	6	6	6	8
CPU1	I1	V				V		V	V	V		V	V
	J1			V						V	V	V	V
	K1					V	V	V	V	V			V
	L1								V		V	V	V
	M1		V			V	V	V	V	V			V
	N1				V				V		V	V	V
	O1					V		V	V	V		V	V
	P1									V	V	V	V

The symbol V indicates the slot is populated.

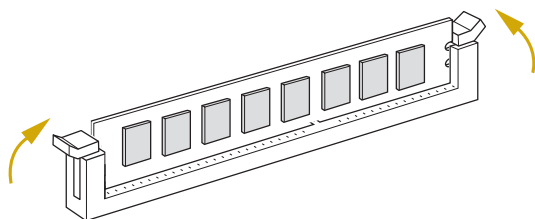
1



2



3



2.5 Expansion Slots (PCI Express Slots)

There are 2 PCI Express slots on this motherboard.

PCIe slots:

PCIe1 (PCIe 5.0 x16 slot, from CPU0) is used for PCI Express x16 lane width cards.

PCIe2 (PCIe 5.0 x16 slot, from CPU0) is used for PCI Express x16 lane width cards.

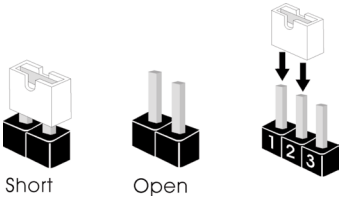
Slot	Generation	Mechanical	Electrical	Source
PCIe2	5.0	x16	x16	CPU0
PCIe1	5.0	x16	x16	CPU0

Installing an expansion card

- Step 1. Before installing an expansion card, please make sure that the power supply is switched off or the power cord is unplugged. Please read the documentation of the expansion card and make necessary hardware settings for the card before starting the installation.
- Step 2. Remove the system unit cover (if the motherboard is already installed in a chassis).
- Step 3. Remove the bracket facing the slot that intending to use. Keep the screws for later use.
- Step 4. Align the card connector with the slot and press firmly until the card is completely seated on the slot.
- Step 5. Fasten the card to the chassis with screws.
- Step 6. Replace the system cover.

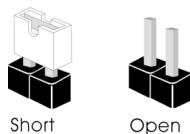
2.6 Jumper Setup

The illustration shows how jumpers are setup. When the jumper cap is placed on the pins, the jumper is “Short”. If no jumper cap is placed on the pins, the jumper is “Open”. The illustration shows a 3-pin jumper whose pin1 and pin2 are “Short” when a jumper cap is placed on these 2 pins.



Password Reset Jumper (3-pin PASSWORD_ CLEAR1) (see p.6, No. 2)	1_2  Normal Mode (Default)	2_3  Password Clear
CPU PECI Mode Jumper (3-pin PECI1) (see p.6, No. 41)	1_2  CPU PECI connected to PCH	2_3  CPU PECI connected to BMC (Default)
LAN Selection Jumper (3-pin LAN_SW1) (see p.6, No. 1)	1_2  LAN Intel i210 (Default)	2_3  IPMI LAN
BPB Signal Source Selection Jumper (3-pin MUX_SW1) (see p.6, No. 15)	1_2  SATA (Default)	2_3  RAID Card
ME Recovery Jumper (3-pin ME_RECOVERY1) (see p.6, No. 42)	1_2  Normal Mode (Default)	2_3  ME Recovery Mode

The illustration shows how jumpers are setup. When the jumper cap is placed on the pins, the jumper is “Short”. If no jumper cap is placed on the pins, the jumper is “Open”.



BIOS Swap Override

Jumper

(BIOS_SWAP_OVERRIDE)

(see p.6, No. 5)

1_2



2-pin Jumper

Open: Disable Override (Default)

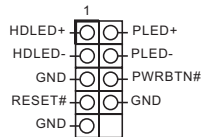
Short: Enable Override

2.7 Onboard Headers and Connectors



Onboard headers and connectors are NOT jumpers. Do NOT place jumper caps over these headers and connectors. Placing jumper caps over the headers and connectors will cause permanent damage to the motherboard.

System Panel Header
(9-pin PANEL1)
(see p.6, No. 35)



Connect the power switch, reset switch and system status indicator on the chassis to this header according to the pin assignments. Particularly note the positive and negative pins before connecting the cables.



PWRBTN (Power Switch):

Connect to the power switch on the chassis front panel. Configure the way to turn off the system using the power switch.

RESET (Reset Switch):

Connect to the reset switch on the chassis front panel. Press the reset switch to restart the computer if the computer freezes and fails to perform a normal restart.

PLED (System Power LED):

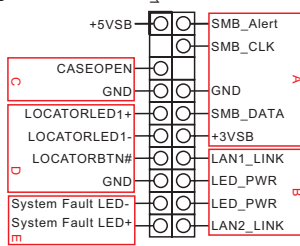
Connect to the power status indicator on the chassis front panel. The LED is on when the system is operating. The LED is off when the system is in S4 sleep state or powered off (S5).

HDLED (Hard Drive Activity LED):

Connect to the hard drive activity LED on the chassis front panel. The LED is on when the hard drive is reading or writing data.

The front panel design may differ by chassis. A front panel module mainly consists of power switch, reset switch, power LED, hard drive activity LED, speaker and etc. When connecting the chassis front panel module to this header, make sure the wire assignments and the pin assignments are matched correctly.

Auxiliary Panel Header (18-pin AUX PANEL1) (see p.6, No. 36)



This header supports multiple functions on the front panel, including the front panel SMB, internet status indicator and chassis intrusion pin.



A. Front panel SMBus connecting pin (6-1 pin FPSMB)

This header allows user to connect SMBus (System Management Bus) equipment. It can be used for communication between peripheral equipment in the system, which has slower transmission rates, and power management equipment.

B. Internet status indicator (2-pin LAN1_LED, LAN2_LED)

These two 2-pin headers allow user to use the Gigabit internet indicator cable to connect to the LAN status indicator. When this indicator flickers, it means that the internet is properly connected.

C. Chassis intrusion pin (2-pin CHASSIS)

This header is provided for host computer chassis with chassis intrusion detection designs. In addition, it must also work with external detection equipment, such as a chassis intrusion detection sensor or a microswitch. When this function is activated, if any chassis component movement occurs, the sensor will immediately detect it and send a signal to this header, and the system will then record this chassis intrusion event. The default setting is set to the CASEOPEN and GND pin; this function is off.

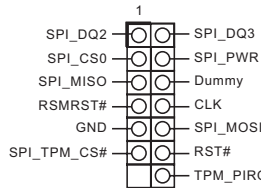
D. Locator LED (4-pin LOCATOR)

This header is for the locator switch and LED on the front panel.

E. System Fault LED (2-pin LOCATOR)

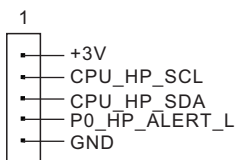
This header is for the Fault LED on the system.

TPM-SPI Header (13-pin TPM_BIOS_PH1) (see p.6, No. 6)



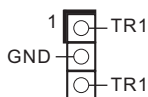
This connector supports SPI Trusted Platform Module (TPM) system, which can securely store keys, digital certificates, passwords, and data. A TPM system also helps enhance network security, protects digital identities, and ensures platform integrity.

Backplane PCI Express
Hot-Plug Connectors
(5-pin CPU0_HSBP1)
(see p.6, No. 34)
(5-pin CPU1_HSBP1)
(see p.6, No. 33)



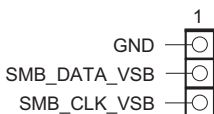
These headers are used for the hot plug feature of HDDs on the backplane.

Thermal Sensor Header
(3-pin TR1)
(see p.6, No. 43)



Please connect the thermal sensor cable to either pin 1-2 or pin 2-3 and the other end to the device to monitor its temperature.

PWM Configuration
Header
(3-pin PWM_CFG1)
(see p.6, No. 9)



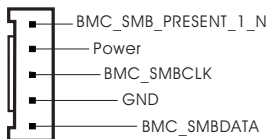
The header is used for PWM configurations.

Non Maskable Interrupt
Button Header
(NMI_BTN1)
(see p.6, No. 3)



Please connect a NMI device to this header.

BMC SMB Headers
(5-pin BMC_SMB1)
(see p.6, No. 45)



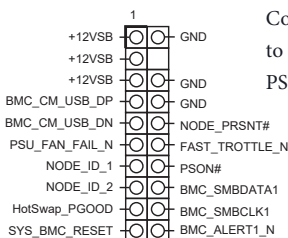
These headers are used for the SM BUS devices.

Clear CMOS Pad
(CLRMOS1)
(see p.6, No. 39)



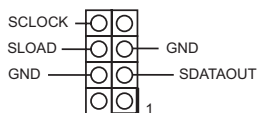
This allows user to clear the data in CMOS. To clear CMOS, take out the CMOS battery and short the Clear CMOS Pad.

CM Board Standby Power
Headers
(19-pin CM_SB_R)
(see p.6, No. 37)



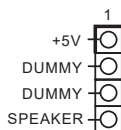
Connect this 19-pin header
to the PSU for +12VSB and
PS0N PWOK.

Serial General Purpose
Input/Output Header
(7-pin SATA_SGPIO1)
(see p.6, No. 38)



The header supports Serial
Link interface for onboard
SATA connections.

Chassis Speaker Header
(4-pin SPEAKER1)
(see p.6, No. 40)



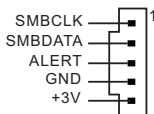
Please connect the chassis
speaker to this header.

Serial ATA3 Connectors
(SATA0)
(see p.6, No. 7)
(SATA1)
(see p.6, No. 8)



These two SATA3 connectors
support SATA data cables for
internal storage devices with
up to 6.0 Gb/s data transfer
rate.

PSU SMBus Header
(5-pin PSU_SMB1)
(see p.6, No. 11)



PSU SMBus monitors the
status of the power supply, fan
and system temperature.

Mini Cool Edge IO x8
Connectors
(MCIO1)
(see p.6, No. 18)
(MCIO2)
(see p.6, No. 17)



This motherboard supports
2 Mini Cool Edge IO 8x
Connectors. Please connect
these connectors to the HDD
backplane board.

MCIO1 Pin Definition

Pin	Defeinition	Pin	Defeinition
A1	GND	B1	GND
A2	RX_DP0	B2	TX_DP0
A3	RX_DN0	B3	TX_DN0
A4	GND	B4	GND
A5	RX_DP1	B5	TX_DP1
A6	RX_DN1	B6	TX_DN1
A7	GND	B7	GND
A8	SPARE_A1	B8	SMB_SCL1
A9	IRQ_LVC3_WAKE_N	B9	SMB_SDA1
A10	GND	B10	GND
A11	DIF8_DP	B11	PERST0
A12	DIF8_DN	B12	PRSNT0
A13	GND	B13	GND
A14	RX_DP2	B14	TX_DP2
A15	RX_DN2	B15	TX_DN2
A16	GND	B16	GND
A17	RX_DP3	B17	TX_DP3
A18	RX_DN3	B18	TX_DN3
A19	GND	B19	GND
A20	RX_DP4	B20	TX_DP4
A21	RX_DN4	B21	TX_DN4
A22	GND	B22	GND
A23	RX_DP5	B23	TX_DP5
A24	RX_DN5	B24	TX_DN5
A25	GND	B25	GND
A26	SPARE_A2	B26	SMB_SCL2
A27	IRQ_LVC3_WAKE_N	B27	SMB_SDA2
A28	GND	B28	GND
A29	DIF9_DP	B29	PERST1
A30	DIF9_DN	B30	PRSNT1
A31	GND	B31	GND
A32	RX_DP6	B32	TX_DP6
A33	RX_DN6	B33	TX_DN6
A34	GND	B34	GND
A35	RX_DP7	B35	TX_DP7
A36	RX_DN7	B36	TX_DN7
A37	GND	B37	GND
75	NP_NC_1	76	NP_NC_2
77	PGND_1	78	PGND_3
79	PGND_2	80	PGND_4

MCIO2 Pin Definition

Pin	Definition	Pin	Definition
A1	GND	B1	GND
A2	RX_DP8	B2	TX_DP8
A3	RX_DN8	B3	TX_DN8
A4	GND	B4	GND
A5	RX_DP9	B5	TX_DP9
A6	RX_DN9	B6	TX_DN9
A7	GND	B7	GND
A8	SPARE_A1	B8	SMB_SCL1
A9	IRQ_LVC3_WAKE_N	B9	SMB_SDA1
A10	GND	B10	GND
A11	DIF10_DP	B11	PERST0
A12	DIF10_DN	B12	PRSENT0
A13	GND	B13	GND
A14	RX_DP10	B14	TX_DP10
A15	RX_DN10	B15	TX_DN10
A16	GND	B16	GND
A17	RX_DP11	B17	TX_DP11
A18	RX_DN11	B18	TX_DN11
A19	GND	B19	GND
A20	RX_DP12	B20	TX_DP12
A21	RX_DN12	B21	TX_DN12
A22	GND	B22	GND
A23	RX_DP13	B23	TX_DP13
A24	RX_DN13	B24	TX_DN13
A25	GND	B25	GND
A26	SPARE_A2	B26	SMB_SCL2
A27	IRQ_LVC3_WAKE_N	B27	SMB_SDA2
A28	GND	B28	GND
A29	DIF11_DP	B29	PERST1
A30	DIF11_DN	B30	PRSENT1
A31	GND	B31	GND
A32	RX_DP14	B32	TX_DP14
A33	RX_DN14	B33	TX_DN14
A34	GND	B34	GND
A35	RX_DP15	B35	TX_DP15
A36	RX_DN15	B36	TX_DN15
A37	GND	B37	GND
75	NP_NC_1	76	NP_NC_2
77	PGND_1	78	PGND_3
79	PGND_2	80	PGND_4

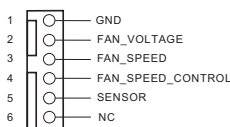
System Fan Connectors

(6-pin FAN1)

(see p.6, No. 30)

(6-pin FAN2)

(see p.6, No. 31)



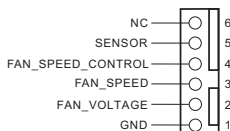
Please connect fan cables to the fan connectors and match the black wire to the ground pin. All fans support Fan Control.

(6-pin FAN3)

(see p.6, No. 26)

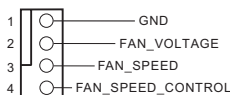
(6-pin FAN4)

(see p.6, No. 25)



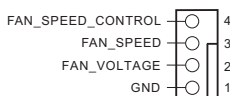
(4-pin FAN5)

(see p.6, No. 28)



(4-pin FAN6)

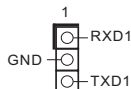
(see p.6, No. 16)



Serial Port Header

(3-pin COM1)

(see p.6, No. 44)



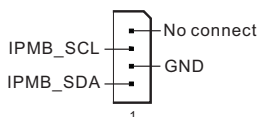
This COM1 header supports a serial port module.

Intelligent Platform

Management Bus Header

(4-pin IPMB1)

(see p.6, No. 46)

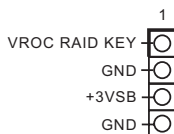


This 4-pin connector is used to provide a cabled base-board or front panel connection for value added features and 3rd-party add-in cards, such as Emergency Management cards, that provide management features using the IPMB.

Virtual RAID On CPU Header

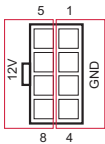
(4-pin RAID_1)

(see p.6, No. 10)



This connector supports Intel® Virtual RAID on CPU and NVME/AHCI RAID on CPU PCIE.

ATX 12V Power
Connectors
(8-pin 12VCON1)
(see p.6, No. 22)
(8-pin 12VCON2)
(see p.6, No. 21)
(8-pin 12VCON3)
(see p.6, No. 20)



This motherboard provides three 8-pin ATX 12V power connectors.

With the introduction of the Intel VROC product, there are three modes of operation:

SKU	HW key required	Key features
Pass-thru	Not needed	• Pass-thru only (no RAID) • LED Management • Hot Plug Support • RAID 0 support for Intel Fultondale NVMe SSDs
Standard	VROCSTANMOD	• Pass-thru SKU features • RAID 0, 1, 10
Premium	VROCPREMMOD	• Standard SKU features • RAID 5
ISS	VROCISSDMOD	• RAID 5 Write Hole Closure

*Only Intel SSDs are supported.
*For further details on VROC, please refer to the official information released by Intel.

Slimline SAS Connector
(SLIMLIN1)
(see p.6, No. 19)



The connector is used for the NVME PCIE devices.

SLIMLINE Pin Definition

Pin	Defeinition	Pin	Defeinition
A1	GND_1	B1	GND_12
A2	RX_0+	B2	TX_0+
A3	RX_0-	B3	TX_0-
A4	GND_2	B4	GND_13
A5	RX_1+	B5	TX_1+
A6	RX_1-	B6	TX_1-
A7	GND_3	B7	GND_14
A8	SIDEBAND_7A	B8	SIDEBAND_0A
A9	SIDEBAND_4A	B9	SIDEBAND_1A
A10	SIDEBAND_3A	B10	SIDEBAND_2A
A11	SIDEBAND_A+	B11	SIDEBAND_5A
A12	SIDEBAND_A-	B12	SIDEBAND_6A
A13	GND_4	B13	GND_15
A14	RX_2+	B14	TX_2+
A15	RX_2-	B15	TX_2-
A16	GND_5	B16	GND_16
A17	RX_3+	B17	TX_3+
A18	RX_3-	B18	TX_3-
A19	GND_6	B19	GND_17
A20	RX_4+	B20	TX_4+
A21	RX_4-	B21	TX_4-
A22	GND_7	B22	GND_18
A23	RX_5+	B23	TX_5+
A24	RX_5-	B24	TX_5-
A25	GND_8	B25	GND_19
A26	SIDEBAND_7B	B26	SIDEBAND_0B
A27	SIDEBAND_4B	B27	SIDEBAND_1B
A28	SIDEBAND_3B	B28	SIDEBAND_2B
A29	SIDEBAND_B+	B29	SIDEBAND_5B
A30	SIDEBAND_B-	B30	SIDEBAND_6B
A31	GND_9	B31	GND_20
A32	RX_6+	B32	TX_6+
A33	RX_6-	B33	TX_6-
A34	GND_10	B34	GND_21
A35	RX_7+	B35	TX_7+
A36	RX_7-	B36	TX_7-
A37	GND_11	B37	GND_32
75	P_GND_2	78	P_GND_3
76	P_GND_4	79	NP_NC_1
77	P_GND_1	80	NP_NC_2

2.8 Unit Identification purpose LED/Switch

Use the UID button to locate the server working on behind a rack of servers.

Unit Identification
purpose LED/Switch
(UID1)



When the UID button on the front or rear panel is pressed, the front/rear UID blue LED indicator will be turned on. Press the UID button again to turn off the indicator.

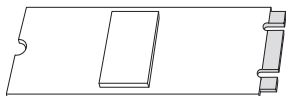


Press and hold the UID button for 4 seconds, the BMC will trigger an external reset.

2.9 M.2 SSD Module Installation Guide

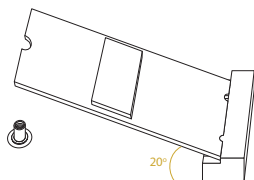
The Hyper M.2 Socket (M2_1/M2_2, Key M) supports type 2280 SATA3 6.0 Gb/s module or a M.2 PCI Express module up to Gen4 x4 (64Gb/s).

Installing the M.2 SSD Module



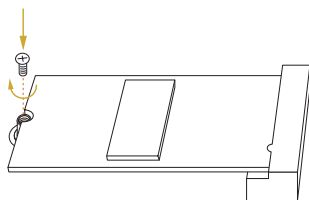
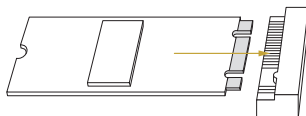
Step 1

Prepare a M.2 SSD module and the screw.



Step 2

Gently insert the M.2 SSD module into the M.2 slot. Please be aware that the M.2 SSD module only fits in one orientation.



Step 3

Tighten the screw with a screwdriver to secure the module into place. Please do not overtighten the screw as this might damage the module.

Chapter 3 UEFI Setup Utility

3.1 Introduction

This section explains how to use the UEFI SETUP UTILITY to configure the system. The UEFI chip on the motherboard stores the UEFI SETUP UTILITY. Run the UEFI SETUP UTILITY when starting up the computer. Please press <F2> or during the Power-On-Self-Test (POST) to enter the UEFI SETUP UTILITY; otherwise, POST will continue with its test routines.

Restart the system by pressing <Ctrl> + <Alt> + <Delete> or by pressing the reset button on the system chassis to enter the UEFI SETUP UTILITY after POST. It may also restart by turning the system off and then back on.



Because the UEFI software is constantly being updated, the following UEFI setup screens and descriptions are for reference purpose only, and they may not exactly match what seeing on the screen.

3.1.1 UEFI Menu Bar

The top of the screen has a menu bar with the following selections:

Item	Description
Main	To set up the system time/date information
Advanced	To set up the advanced UEFI features
Server Mgmt	To manage the server
Security	To set up the security features
Boot	To set up the default system device to locate and load the Operating System
Event Logs	For event log configuration
Exit	To exit the current screen or the UEFI SETUP UTILITY

Use < ← > key or < → > key to choose among the selections on the menu bar, and then press <Enter> to get into the sub screen.

3.1.2 Navigation Keys

Please check the following table for the function description of each navigation key.

Navigation Key(s)	Function Description
← / →	Moves cursor left or right to select Screens
↑ / ↓	Moves cursor up or down to select items
+ / -	To change option for the selected items
<Tab>	Switch to next function
<Enter>	To bring up the selected screen
<PGUP>	Go to the previous page
<PGDN>	Go to the next page
<HOME>	Go to the top of the screen
<END>	Go to the bottom of the screen
<F1>	To display the General Help Screen
<F7>	Discard changes and exit the UEFI SETUP UTILITY
<F9>	Load optimal default values for all the settings
<F10>	Save changes and exit the UEFI SETUP UTILITY
<F12>	Print screen
<ESC>	Jump to the Exit Screen or exit the current screen

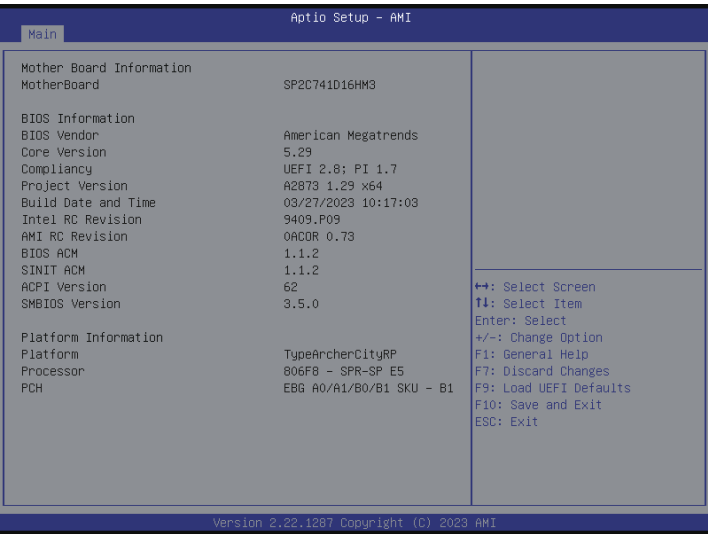
3.2 Main Screen

Once entering the UEFI SETUP UTILITY, the Main screen will appear and display the system overview. The Main screen provides system overview information and allows user to set the system time and date.



3.2.1 Motherboard Information

Press [Enter] to view the information of the motherboard.



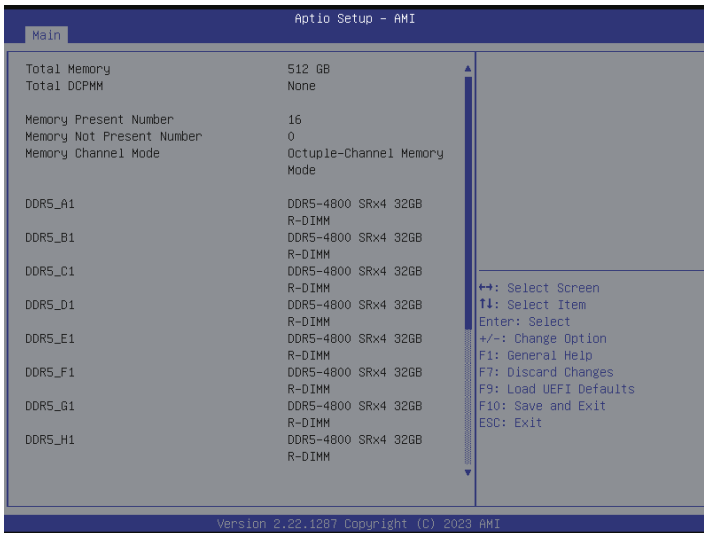
3.2.2 Processor Information

Press [Enter] to view the information of the processor.



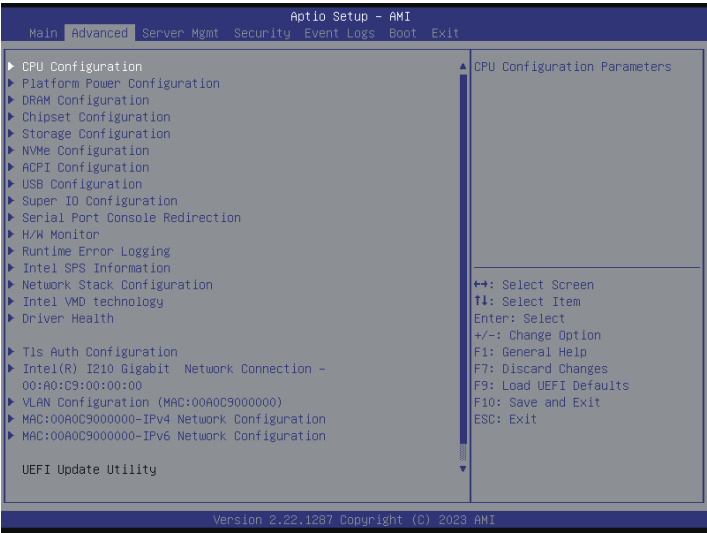
3.2.3 Memory Information

Press [Enter] to view the information of the memory.



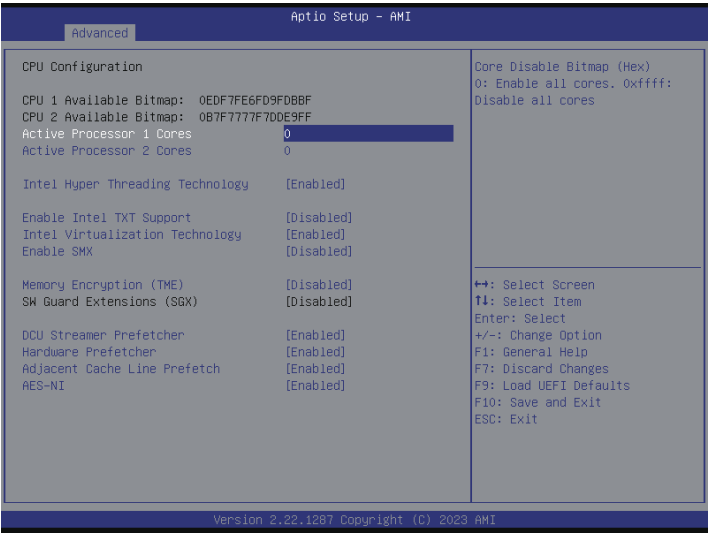
3.3 Advanced Screen

In this section, set the configurations for the following items: CPU Configuration, Platform Power Configuration, DRAM Configuration, Chipset Configuration, Storage Configuration, NVMe Configuration, ACPI Configuration, USB Configuration, Super IO Configuration, Serial Port Console Redirection, H/W Monitor, Runtime Error Logging, Intel SPS Configuration, Network Stack Configuration, Intel VMD Technology, Drive Health, Tls Auth Configuration and Instant Flash.



Setting wrong values in this section may cause the system to malfunction.

3.3.1 CPU Configuration



Active Processor 1/2 Cores

Select the number of cores to enable in each processor package.

Intel Hyper Threading Technology

Intel Hyper Threading Technology allows multiple threads to run on each core, so that the overall performance on threaded software is improved.

Enable Intel TXT Support

Enables Intel Trusted Execution Technology Configuration.

Intel Virtualization Technology

Intel Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions, so that one computer system can function as multiple virtual systems.

Enable SMX

Use this item to enable Safer Mode Extensions.

Memory Encryption (TME)

Use this item to enable or disable Memory Encryption (TME).

SW Guard Extensions (SGX)

Use this item to enable or disable Software Guard Extensions (SGX).

DCU Streamer Prefetcher

DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).

Hardware Prefetcher

Automatically prefetch data and code for the processor. Enable for better performance.

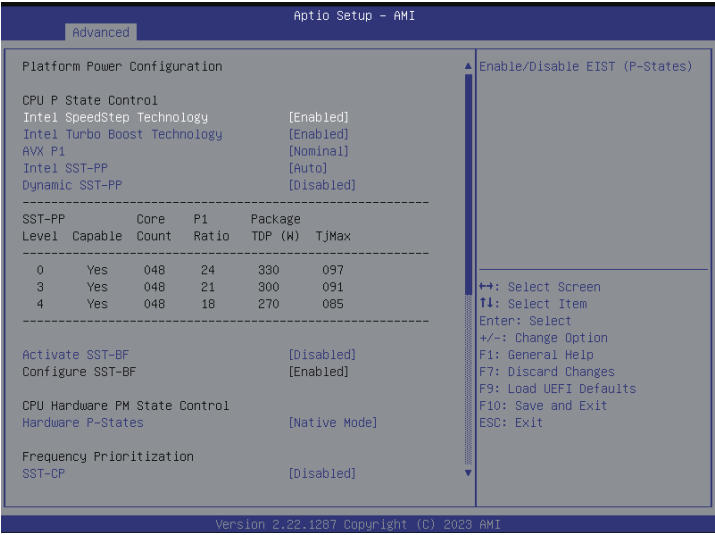
Adjacent Cache Line Prefetch

Automatically prefetch the subsequent cache line while retrieving the currently requested cache line. Enable for better performance.

AES-NI

Use this item to enable or disable AES-NI support.

3.3.2 Platform Power Configuration



Intel SpeedStep Technology

Intel SpeedStep technology allows processors to switch between multiple frequencies and voltage points for better power saving and heat dissipation. CPU turbo ratio can be fixed when Intel SpeedStep Technology set Disabled and Intel Turbo Boost Technology set Enabled.



Please note that enabling this function may reduce CPU voltage and lead to system stability or compatibility issues with some power supplies. Please set this item to [Disabled] if above issues occur.

Intel Turbo Boost Technology

Intel Turbo Boost Technology enables the processor to run above its base operating frequency when the operating system requests the highest performance state.

AVX P1

Select this item to configure AVX P1 level.

Intel SST-PP

Select this item to configure hardware supported level.

Dynamic SST-PP

Select this item to enable or disable the Dynamic SST-PP.



HWP Native Mode is a pre-requisite for enabling Dynamic SST-PP.

Activate SST-BF

Select this item to enable or disable the SST-BF.



HWP Native Mode is a pre-requisite for enabling SST-BF; HWP Native Mode with No Legacy is a pre-requisite for configuring SST-BF.

Configure SST-BF

Select this item to enable or disable the BIOS to configure SST-BF High Priority Cores so that SW does not have to configure.

Hardware P-States

This item supports below selections:

Disable: Hardware chooses a P-state based on OS Request (Legacy P-States).

Native Mode: Hardware chooses a P-state based on OS guidance.

Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance)

Native Mode with No Legacy Support: Hardware autonomously chooses a P-state based on OS guidance with no legacy support.

SST-CP

Select this item to enable or disable the SST-CP feature.



About SST configurations are base on the Intel® related supported specifications.

Enable Monitor MWAIT

Select this item to configure Monitor and MWAIT instructions whether Auto maps to enable.

CPU C6 State Support

Select this item to configure the CPU C6 (ACPI C3) report to OS.

Enhanced Halt State (C1E)

This item specific the Core C1E auto promotion Control whether takes effect after reboot.

Package C State Support

This item specific the Package C State limit, the state Auto maps is program specific.

CPU Thermal Throttling

Select this item to enable or disable Thermal Monitor.

Power Performance Tuning

This allows user to decide which controls EFB.

OS Controls EPB: Specifies IA32_ENERGY_PERF_BIAS is used.

BIOS Controls EPB: Specifies ENERGY_PERF_BIAS_CONFIG is used.

PECI Controls EPB: Specifies PCS53 is used.

ENERGY_PERF_BIAS_CFG mode

This allows user to use input from ENERGY_PERF_BIAS_CONFIG mode selection. PERF/Balanced, Perf/Balanced or Power/Power.

Long Duration Power Limit

Select this item to configure the Long Duration Power Limit. PL1 Power Limit is in Watts and the value may vary from 0 to Fused Value. If the value is 0, the fused value will be programmed. A value greater than fused TDP value will not be programmed.

Long Duration Maintained

Select this item to configure the Long Duration Maintained value. PL1 value is in seconds. The value may vary from 0 to 448. Indicates the time window over which TDP value should be maintained.

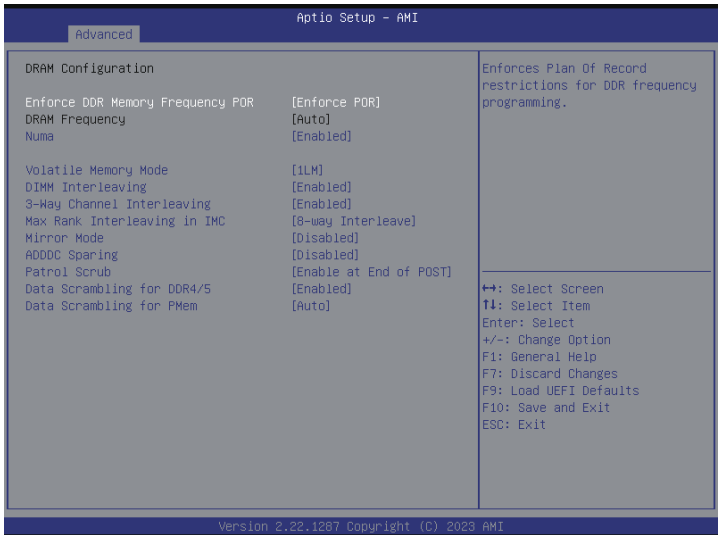
Short Duration Power Limit

Select this item to configure the Short Duration Power Limit. PL2 Power Limit in Watts. The value may vary from 0 to Fused Value. If the value is 0, BIOS programs $120\% * TDP$.

Short Duration Maintained

Select this item to configure the Short Duration Maintained value. PL2 value is in seconds. The value may vary from 0 to 0.438. Indicates the time window over which TDP value should be maintained.

3.3.3 DRAM Configuration



Enforce DDR Memory Frequency POR

Enable to enforce POR restrictions for DDR frequency and voltage programming.

DRAM Frequency

If [Auto] is selected, the motherboard will detect the memory module(s) inserted and assign the appropriate frequency automatically.

Numa

Use this item to enable or disable Non Uniform Memory Access (NUMA).

Volatile Memory Mode

Select 1LM or 2LM mode for Volatile memory. For 2LM memory mode, BIOS will try to configure 2LM but if BIOS is unable to configure 2LM, volatile memory mode will fail back to 1LM.

DIMM Interleaving

Enable this item to allow interleaving to be performed at the highest possible MC * Channel interleaving ways. Or disable this item to enforce interleaving to only 1-way.

3-Way Channel Interleaving

Enable this item to allow 3-way channel interleaving. Or disable this item to default to number of channels available per MC when DIMM interleaving is enabled.

Max Rank Interleaving in IMC

This item allows to select Rank Interleaving setting.

Mirror Mode

Mirror Mode will set entire 1LM/2LM memory in system to be mirrored, consequently reducing the memory capacity by half. Mirror Enable will disable XPT Prefetch.

ADDDC Sparing

Enable or disable Memory Rank Sparing.

Patrol Scrub

Patrol Scrub is a background activity initiated by the processor to seek out and fix memory errors.

Data Scrambling for DDR4/5

Enable - Enables data scrambling for DDR4 and DDR5.

Disable - Disables this feature.

Auto - Sets it to the MRC default setting; current default is Enable.

Data Scrambling for PMem

Enable - Enables data scrambling for PMem.

Disable - Disables this feature.

Auto - Sets it depending on stepping.

3.3.4 Chipset Configuration



MMCFG Base

Use this item to select MMCFG Base.

MMCFG Size

Use this item to select MMCFG Size.

NOTE: To ensure sufficient resource for usage, it is recommended for users to disable hot-plug option when setting this option to 128M

MMIO High Base

Use this item to select MMIO High Base.

MMIO High Granularity Size

Use this item to select MMIO Granularity Size.

SR-IOV Support

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

Re-Size BAR Support

Enable or disable this item to Re-Size BAR supported upon the sysem has resizable BAR capable PCIE Devices.

Onboard VGA

Use this to enable or disable the Onboard VGA function. The default value is [Auto].

Onboard LAN

Use this to enable or disable the Onboard LAN function.

VT-d

Intel Virtualization Technology for Directed I/O helps the virtual machine monitor better utilize hardware by improving application compatibility and reliability, and providing additional levels of manageability, security, isolation, and I/O performance.

PCIE Link Width

Select this item to configure PCIE Link Width.

PCIE1/2 Link Width

Select PCIE port Bifurcation for PCIE1/2.

PCIE Link Speed

Select PCIE Link Speed.

PCIE1/2 Link Speed

Select Link Speed for PCIE1/2.

OCPI Link Speed

Select Link Speed for OCP.

MCIO1-1/1-2/2-1/2-2 Link Speed

Select Link Speed for MCIO1-1/1-2/2-1/2-2.

M2_1/2_2 Link Speed

Select Link Speed for M2_1/2_2.

PCIE Hot Plug

Select this item to configure PCIE Hot Plug globally.

OCPI Hot Plug

Enable or disable OCP Hot Plug.

PCIE1/2, MCIO1-1/1-2/2-1/2-2 Hot Plug

Enable or disable PCIE and MCIO Hot Plug.

OCPI Surprise Hot Plug

Enable or disable OCP Surprise Hot Plug.

PCIE1/2, MCIO1-1/1-2/2-1/2-2 Surprise Hot Plug

Enable or disable PCIE and MCIO Surprise Hot Plug.

PCIE ASPM

Select this item to configure the PCIE ASPM.

PCI-E ASPM Support (Global)

Select this item to disable ASPM Support in all PCIe root ports.

OCPI ASPM Support

Select this item to configure PCIE Active State Power Management settings.

PCIE1/2 ASPM Support

Enables or disables the ASPM support for all CPU downstream devices. Select [Auto] for the default value.

MCIO1-1/1-2/2-1/2-2 ASPM Support

Enables or disables the ASPM support for all CPU downstream devices.

3.3.5 Storage Configuration



Hard Disk S.M.A.R.T.

S.M.A.R.T stands for Self-Monitoring, Analysis, and Reporting Technology. It is a monitoring system for computer hard disk drives to detect and report on various indicators of reliability.

SATA Controller 1/2

Use this item to enable or disable SATA Controllers.

SATA Controller 1/2/M.2 Mode Selection

Identify the SATA port is connected to Solid State Drive or Hard Disk Drive. Press <Ctrl+I> to enter RAID ROM during UEFI POST process.

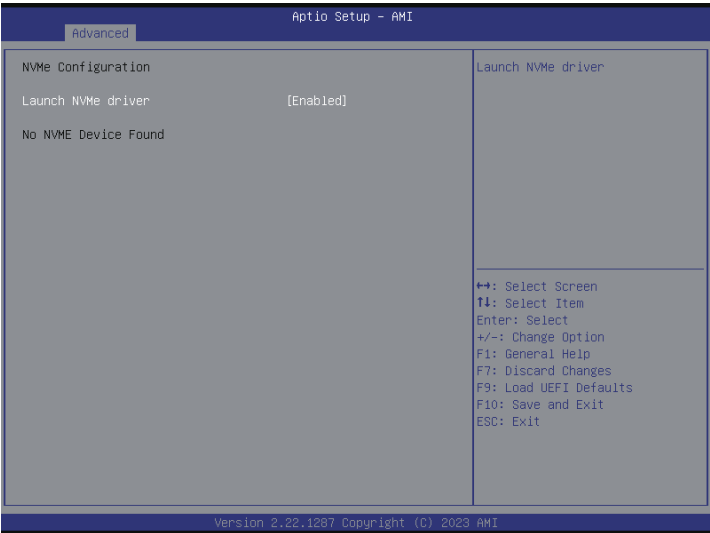
SATA Controller 1/2 ALPM

Use this item to enable or disable Aggressive Link Power Management.

SATA1_0/SATA1_1/SATA1_2/SATA1_2/SATA1_4/SATA1_5/SATA2_2/
SATA2_3/M2_1 (SATA2_0)/M2_2 (SATA2_1)

Select this item to configure the External SATA, Hot Plug, Spin Up Device and SATA Device Type.

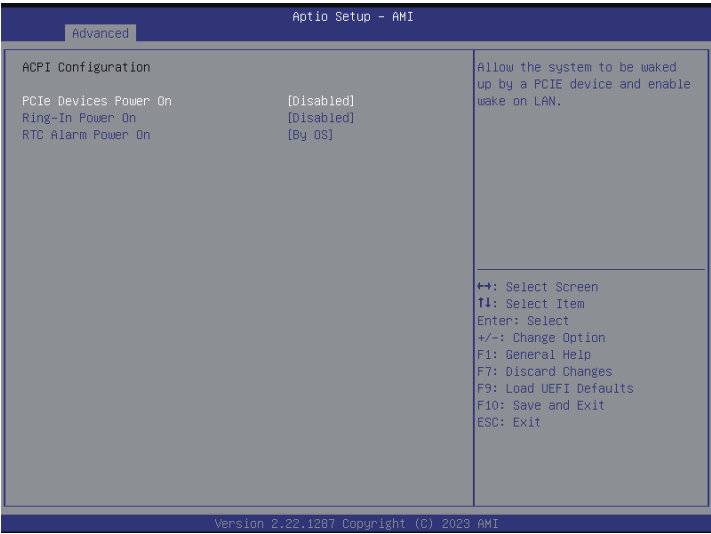
3.3.6 NVMe Configuration



Launch NVMe driver

Select this item to enable or disable launch NVMe driver.

3.3.7 ACPI Configuration



PCIe Devices Power On

Allow the system to be waked up by a PCIE device and enable wake on LAN.

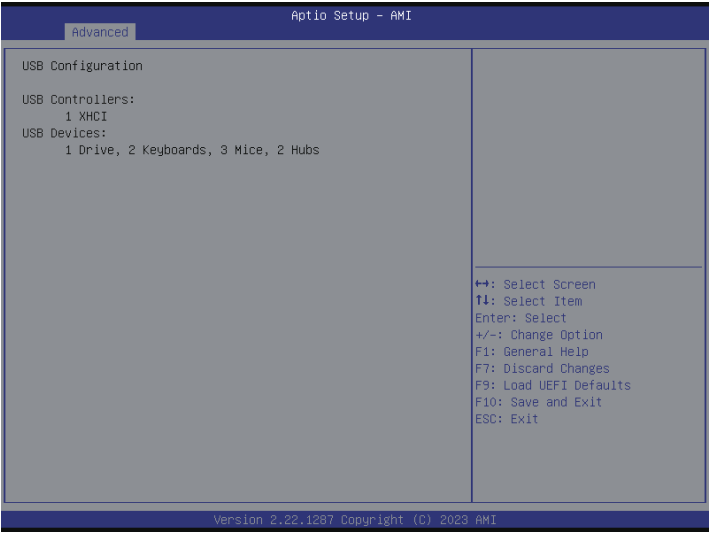
Ring-In Power On

Use this item to enable or disable Ring-In signals to turn on the system from the power-soft-off mode.

RTC Alarm Power On

Use this item to enable or disable RTC (Real Time Clock) to power on the system.

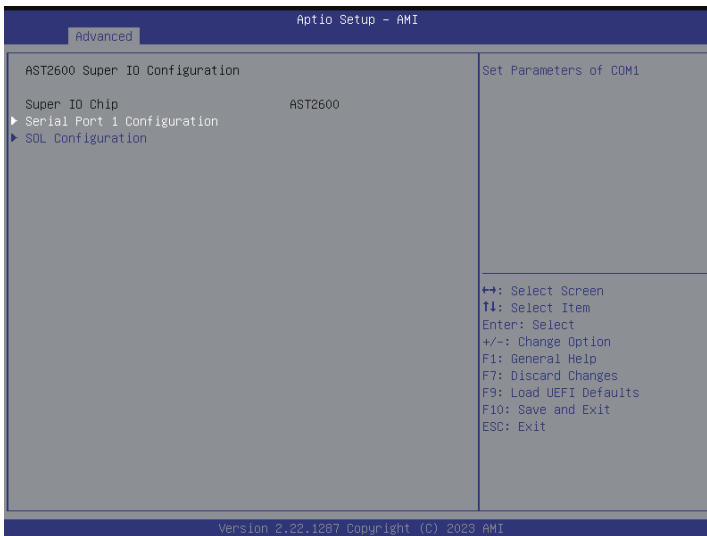
3.3.8 USB Configuration



USB Configuration

The USB Configuration displays the USB Controllers and USB Devices informations.

3.3.9 Super IO Configuration



Serial Port 1 Configuration

Use this item to set parameters of Serial Port 1 (COM1).

Serial Port

Use this item to enable or disable the serial port.

Change Settings

Use this item to select an optimal setting for Super IO device.

SOL Configuration

Use this item to set parameters of SOL.

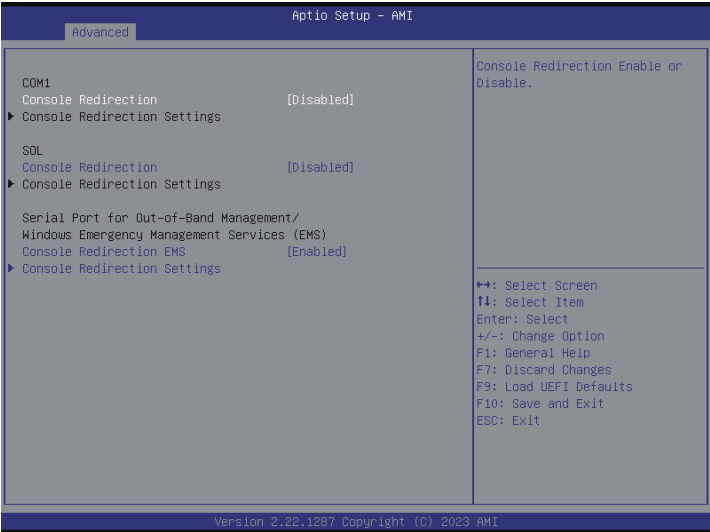
SOL Port

Use this item to set parameters of SOL.

Change Settings

Use this item to select an optimal setting for Super IO device.

3.3.10 Serial Port Console Redirection



COM1 / SOL

Console Redirection

Use this option to enable or disable Console Redirection. If this item is set to Enabled, select a COM Port to be used for Console Redirection.

Console Redirection Settings

Use this option to configure Console Redirection Settings, and specify how the computer and the host computer to exchange information. Both computers should have the same or compatible settings.

Terminal Type

Use this item to select the preferred terminal emulation type for out-of-band management. It is recommended to select [VT-UTF8].

Option	Description
VT100	ASCII character set
VT100+	Extended VT100 that supports color and function keys
VT-UTF8	UTF8 encoding is used to map Unicode chars onto 1 or more bytes
ANSI	Extended ASCII character set

Bits Per Second

Use this item to select the serial port transmission speed. The speed used in the host computer and the client computer must be the same. Long or noisy lines may require lower transmission speed. The options include [9600], [19200], [38400], [57600] and [115200].

Data Bits

Use this item to set the data transmission size. The options include [7] and [8] (Bits).

Parity

Use this item to select the parity bit. The options include [None], [Even], [Odd], [Mark] and [Space].

Stop Bits

The item indicates the end of a serial data packet. The standard setting is [1] Stop Bit. Select [2] Stop Bits for slower devices.

Flow Control

Use this item to set the flow control to prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to restart the flow. Hardware flow uses two wires to send start/stop signals. The options include [None] and [Hardware RTS/CTS].

VT-UTF8 Combo Key Support

Use this item to enable or disable the VT-UTF8 Combo Key Support for ANSI/VT100 terminals.

Recorder Mode

Use this item to enable or disable Recorder Mode to capture terminal data and send it as text messages.

Resolution 100x31

Use this item to enable or disable extended terminal resolution support.

Putty Keypad

Use this item to select Function Key and Keypad on Putty.

Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)**Console Redirection EMS**

Use this option to enable or disable Console Redirection. If this item is set to Enabled, it allows user to select a COM Port to be used for Console Redirection.

Console Redirection Settings

Use this option to configure Console Redirection Settings, and specify how the computer and the host computer to which are connected exchange information.

Out-of-Band Mgmt Port

Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port.

Terminal Type EMS

Use this item to select the preferred terminal emulation type for out-of-band management. It is recommended to select [VT-UTF8].

Option	Description
VT100	ASCII character set
VT100+	Extended VT100 that supports color and function keys
VT-UTF8	UTF8 encoding is used to map Unicode chars onto 1 or more bytes
ANSI	Extended ASCII character set

Bits Per Second EMS

Use this item to select the serial port transmission speed. The speed used in the host computer and the client computer must be the same. Long or noisy lines may require lower transmission speed. The options include [9600], [19200], [57600] and [115200].

Flow Control EMS

Use this item to set the flow control to prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to restart the flow. Hardware flow uses two wires to send start/stop signals. The options include [None], [Hardware RTS/CTS], and [Software Xon/Xoff].

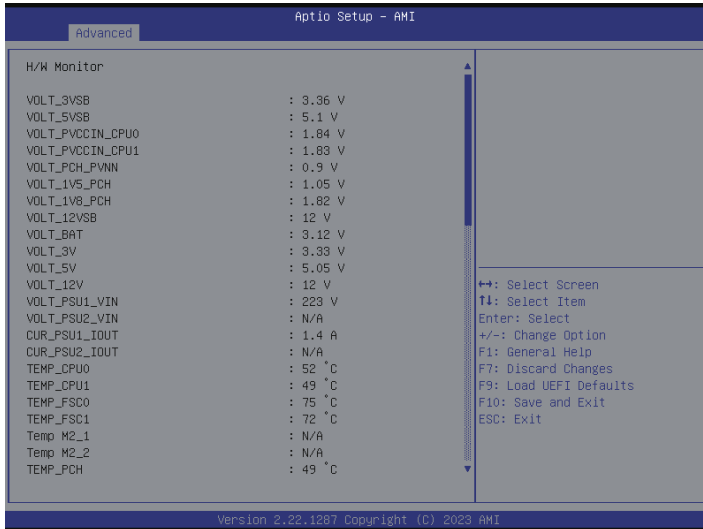
Data Bits EMS

Parity EMS

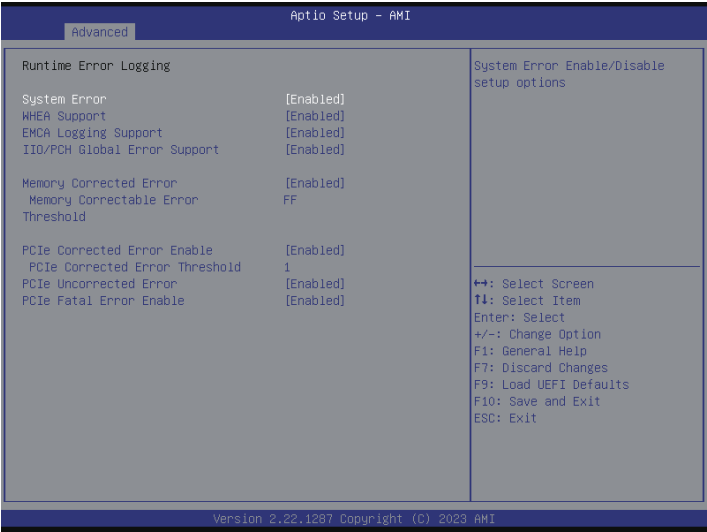
Stop Bits EMS

3.3.11 H/W Monitor

In this section, it allows user to monitor the status of the hardware on the system, including the parameters of the CPU temperature, motherboard temperature, CPU fan speed, chassis fan speed, and the critical voltage.



3.3.12 Runtime Error Logging



System Error

Use this item to enable or disable System Error feature. When it is set to [Enabled], it allows user to configure Memory Error and PCIe Error log features.

WHEA Support

Use this item to enable or disable Windows Hardware Error Architecture.

EMCA Logging Support

Use this item to enable or disable EMCA Logging.

IIO/PCH Global Error Support

Use this item to enable or disable IIO/PCH Error Support.

Memory Corrected Error

Use this item to enable or disable Memory Corrected Error.

Memory Correctable Error Threshold

Correctable Error Threshold (0 - 0x7FFF) used for sparing, tagging, and leaky bucket.

PCIe Corrected Error Enable

Use this item to enable or disable PCIe Correctable errors.

PCIe Corrected Error Threshold

PCIe Correctable Error Threshold (0x01-0xFF) used for sparing, tagging, and leaky bucket.

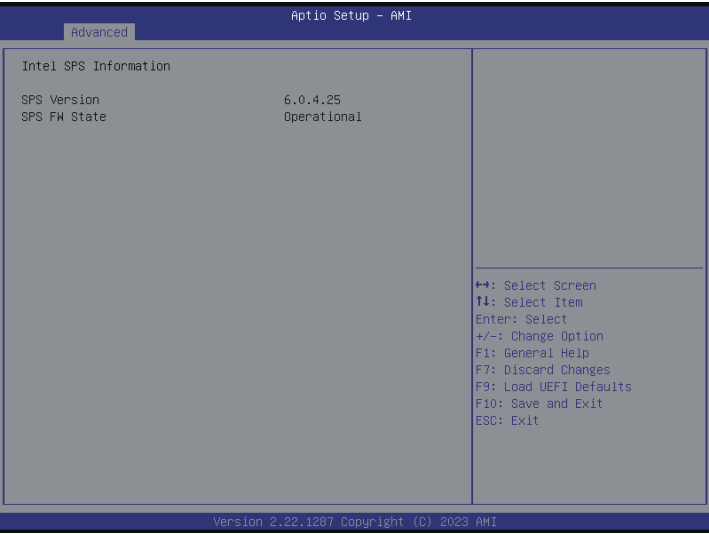
PCIe Uncorrected Error

Use this item to enable or disable PCIe Uncorrectable errors.

PCIeFatal Error Enable

Use this item to enable or disable PCIe Fatal errors.

3.3.13 Intel SPS Configuration



SPS screen displays the Intel SPS Configuration information, such as Operational Firmware Version and Firmware State.

3.3.14 Network Stack Configuration



Network Stack

Enable UEFI network stack can prevents to perform from the single-user network boots and network installation. If disabled, the host does not use the network interface.

IPv4 PXE Support

Enable IPv4 PXE Boot support. If disabled, IPv4 PXE Boot Option is not supported.

IPv4 HTTP Support

Enable IPv4 HTTP Boot support. If disabled, IPv4 HTTP Boot Option is not supported.

IPv6 PXE Support

Enable IPv6 PXE Boot support. If disabled, IPv6 PXE Boot Option is not supported.

IPv6 HTTP Support

Enable IPv6 HTTP Boot support. If disabled, IPv6 HTTP Boot Option is not supported.

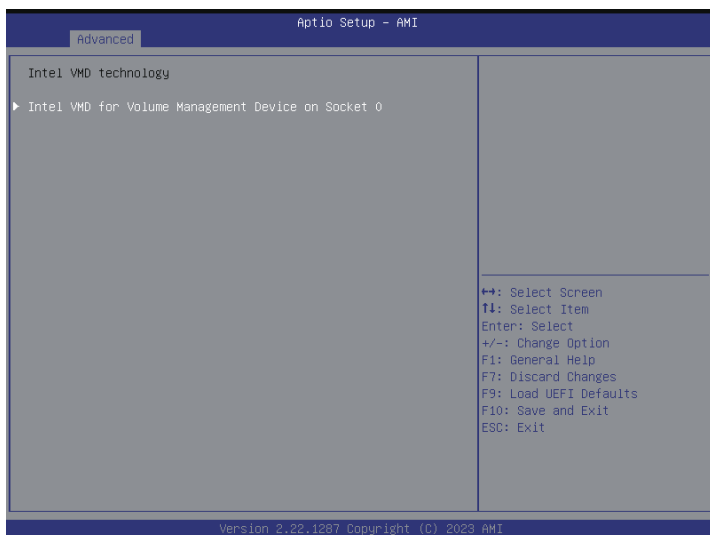
PXE Boot Wait Time

Specifies the wait time and press the ESC key to abort the PXE boot.

Media Detect Count

Specifies the number of times the presence of physical storage device are verified on a system reset or power cycle.

3.3.15 Intel VMD technology



Press <Enter> to bring up the Intel VMD for Volume Management Device Configuration menu.

Intel VMD for Volume Management Device on Socket 0

VMD Config for IOU1 (M.2)/IOU2 (MCIO2/MCIO1)/IOU3 (PCIE1)/IOU4 (PCIE2)

When [Enabled], users are allowed to configure the options below.

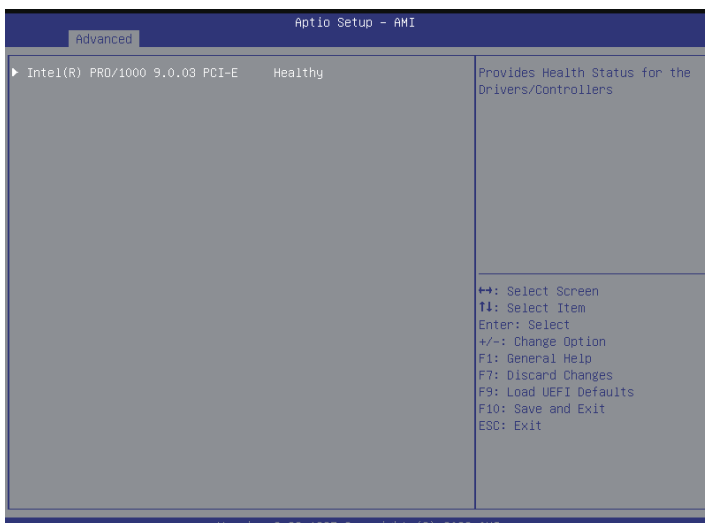
VMD port X

Use this item to enable or disable Intel Volume Management Device Technology on specific root port.

Hot Plug Capable

Use this item to enable or disable Hot Plug for specific Ports.

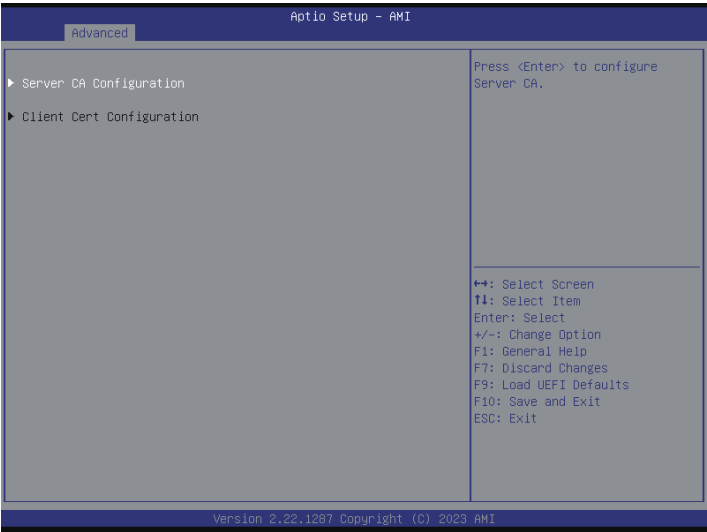
3.3.16 Driver Health



Inter(R) I210 Gigabit Network Connection Healthy

Provides Health Status for the Drivers/Controllers

3.3.17 Tls Auth Configuration



Server CA Configuration

Press <Enter> to configure Server CA.

Client Cert Configuration

Press <Enter> to configure Client Cert.

Enroll Cert

Press <Enter> to enroll cert.

Delete Cert

Press <Enter> to delete cert.

3.3.18 Instant Flash

Instant Flash is a UEFI flash utility embedded in Flash ROM. This convenient UEFI update tool allows user to update system UEFI without entering operating systems first like MS-DOS or Windows[®]. Just save the new UEFI file to the USB flash drive, floppy disk or hard drive and launch this tool, then update the UEFI only in a few clicks without preparing an additional floppy diskette or other complicated flash utility. Please be noted that the USB flash drive or hard drive must use FAT32/16/12 file system. Execute the Instant Flash utility, the utility will show the UEFI files and the respective information. Select the proper UEFI file to update UEFI, and reboot the system after the UEFI update process is completed.

3.4 Server Mgmt



Wait For BMC

Wait For BMC response for specified time out. BMC starts at the same time when BIOS starts during AC power ON. It takes around 90 seconds to initialize Host to BMC interfaces.

FRB-2 Timer

Select this item to enable or disable FRB-2 timer (POST timer)

FRB-2 Timer Timeout

Select this item to define the FRB-2 Time Expiration between 1 to 30 value.

FRB-2 Timer Policy

Configure how the system should respond. If the FRB-2 Timer expires is disabled, this item is not available.

OS Watchdog Timer

Select this item to enable or disable OS Watchdog Timer. If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads.

OS Wtd Timer Timeout

Configure the OS Boot Watchdog Timer Expiration between 1 to 30 min value. If the OS Boot Watchdog Timer is disabled, this item is not available.

OS Wtd Timer Policy

Configure how the system should respond if the OS Boot Watchdog Timer expires. If the OS Boot Watchdog Timer is disabled, this item is not available.

BMC Network Configuration

Select this item to configure BMC network parameters.

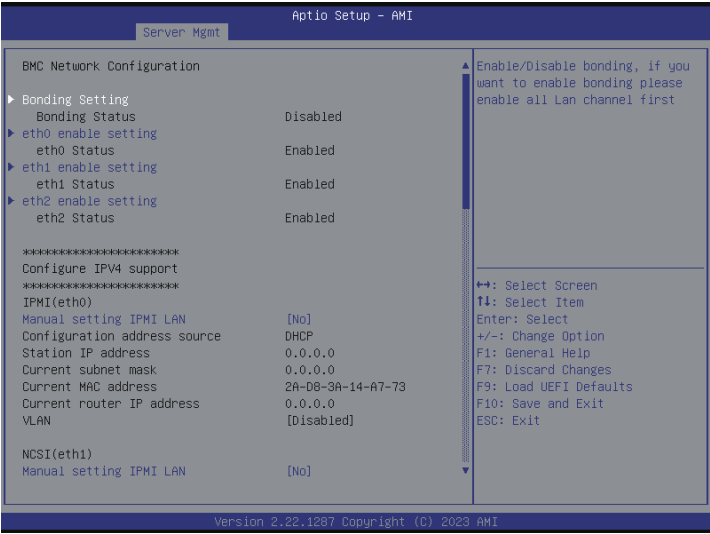
System Event Log

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

BMC Tools

Select this item to configure about KCS control, restore AC power loss and load BMC default settings.

3.4.1 BMC Network Configuration



Bonding Setting

Select this item to enabled or disabled bonding. Please enable all lan channel first when want to enable bonding.

Lan Channel (Failover)

Manual Setting IPMI LAN

If [No] is selected, the IP address is assigned by DHCP. Using a static IP address, toggle to [Yes], and the changes take effect after the system reboots. The default value is [No].

Configuration Address Source

Select to configure BMC network parameters statically or dynamically(by BIOS or BMC). Configuration options: [Static] and [DHCP].

Static: Manually enter the IP Address, Subnet Mask and Gateway Address in the BIOS for BMC LAN channel configuration.

DHCP: IP address, Subnet Mask and Gateway Address are automatically assigned by the network's DHCP server.



When [DHCP] or [Static] is selected, do NOT modify the BMC network settings on the IPMI web page.



The default login information for the IPMI web interface is:

Username: admin

Password: admin

For more instructions on how to set up remote control environment and use the IPMI management platform, please refer to the IPMI Configuration User Guide or go to the Support website at: <http://www.asrockrack.com/support/ipmi.asp>

VLAN

Enabled or disabled Virtual Local Area Network.

IPV6 Support

Enable or disable LAN1 IPV6 Support.

Manual Setting IPMI LAN(IPV6)

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.

3.4.2 System Event Log



SEL Components

Change this to enable or disable event logging for error/progress codes during boot.

Erase SEL

Use this to choose options for erasing SEL.

When SEL is Full

Use this to choose options for reactions to a full SEL.

Log EFI Status Codes

Use this item to disable the logging of EFI Status Codes or log only error code or only progress code or both.

PCIe Device Degrade ELog Support

Use this item to enable or disable PCIe Device Degrade Error Logging Support.

3.4.3 BMC Tools



KCS control

Select the KSC interface state after POST end. If [Enabled] is selected, the BMC will remain KCS interface after POST stage. If [Disabled] is selected, the BMC will disable KCS interface after POST stage.

Restore AC Power Loss

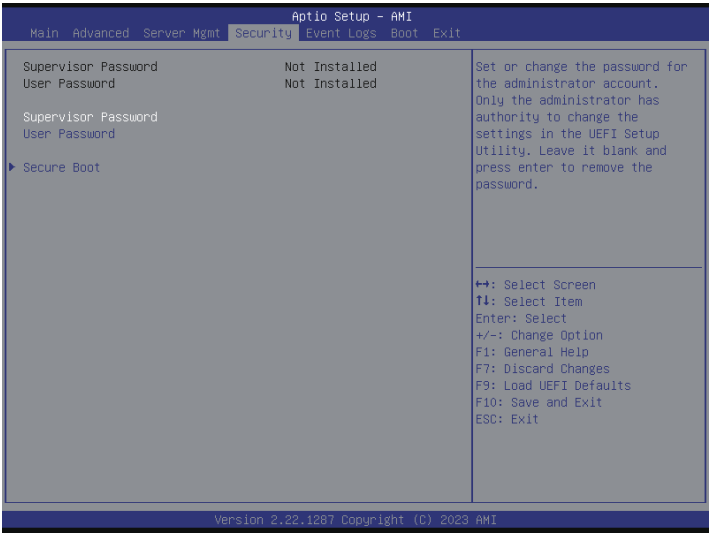
This allows user to set the power state after an unexpected AC/power loss. If [Power Off] is selected, the AC/power remains off when the power recovers. If [Power On] is selected, the AC/power resumes and the system starts to boot up when the power recovers. If [Last State] is selected, it will recover to the state before AC/power loss.

Load BMC Default Settings

Use this item to load BMC default settings.

3.5 Security

In this section, set or change the supervisor/user password for the system. For the user password, user may also clear it.



Supervisor Password

Set or change the password for the administrator account. Only the administrator has authority to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

User Password

Set or change the password for the user account. Users are unable to change the settings in the UEFI Setup Utility. Leave it blank and press enter to remove the password.

Secure Boot

Use this to enable or disable Secure Boot Control. The default value is [Disabled]. Enable to support Windows Server 2012 R2 or later versions Secure Boot.

Secure Boot Mode

Secure Boot mode selector: Standard/Custom. In Custom mode Secure Boot Variables can be configured without authentication.

3.5.1 Key Management

In this section, expert users can modify Secure Boot Policy variables without full authentication.



Factory Key Provision

Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.

Install Default Secure Boot Keys

Please install default secure boot keys if it's the first time using the secure boot.

Clear Secure Boot Keys

Force System to Setup Mode - clear all Secure Boot Variables. Change takes effect after reboot.

Enroll Efi Image

Allow the image to run in Secure Boot mode. Enroll SHA256 hash of the binary into Authorized Signature Database (db).

Export Secure Boot Variables

Copy NVRAM content of Secure Boot variables to files in a root folder on a file system device.

Platform Key(PK)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image(SHA256)

Key Source: Factory, Modified, Mixed

Key Exchange Keys(KEK)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image(SHA256)

Key Source: Factory, Modified, Mixed

Authorized Signatures(db)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image(SHA256)

Key Source: Factory, Modified, Mixed

Forbidden Signatures(dbx)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image(SHA256)

Key Source: Factory, Modified, Mixed

Authorized TimeStamps(dbt)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST
- b) EFI_CERT_X509 (DER)
- c) EFI_CERT_RSA2048 (bin)
- d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image(SHA256)

Key Source: Factory, Modified, Mixed

OsRecovery Signatures(dbr)

Enroll Factory Defaults or load certificates from a file:

1. Public Key Certificate in:

- a) EFI_SIGNATURE_LIST

b) EFI_CERT_X509 (DER)

c) EFI_CERT_RSA2048 (bin)

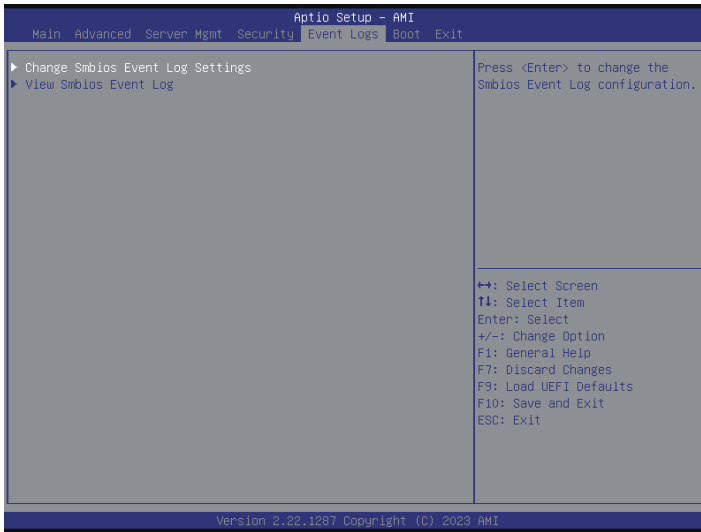
d) EFI_CERT_SHAXXX

2. Authenticated UEFI Variable

3. EFI PE/COFF Image(SHA256)

Key Source: Factory, Modified, Mixed

3.6 Event Logs



Change Smbios Event Log Settings

Select this item to configure the Smbios Event Log Settings.

When entering the item, the screen displays following sub-items:

Smbios Event Log

Use this item to enable or disable all features of the SMBIOS Event Logging during system boot.

Erase Event Log

The options include [No], [Yes, Next reset] and [Yes, Every reset]. If Yes is selected, all logged events will be erased.

When Log is Full

Use this item to choose options for reactions to a full Smbios Event Log. The options include [Do Nothing] and [Erase Immediately].

Log System Boot Event

Choose option to enable or disable logging of System boot event.

View Smbios Event Log

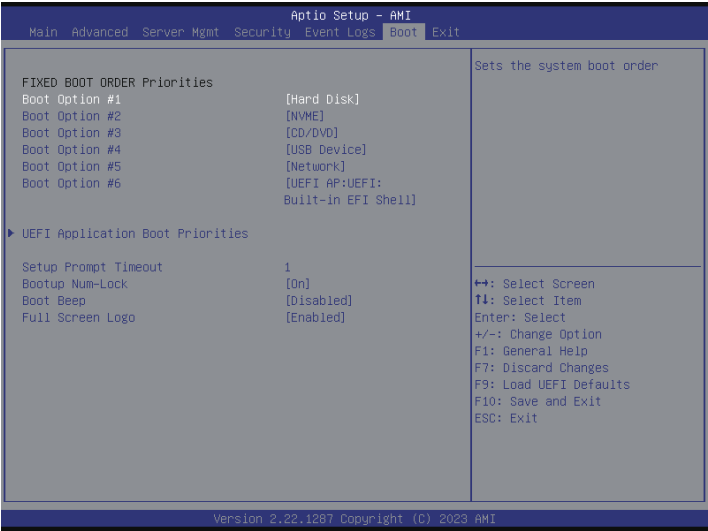
Press <Enter> to view the Smbios Event Log records.



All values changed here do not take effect until computer is restarted.

3.7 Boot Screen

In this section, it will display the available devices on the system for user to configure the boot settings and the boot priority.



Boot Option #1/#2/#3/#4/#5/#6

Use this item to set the system boot order.

UEFI Application Boot Priorities

Specifies the Boot Device Priority sequence from available UEFI Application.

Setup Prompt Timeout

Configure the number of seconds to wait for the UEFI setup utility.

Bootup Num-Lock

If this item is set to [On], it will automatically activate the Numeric Lock function after boot-up.

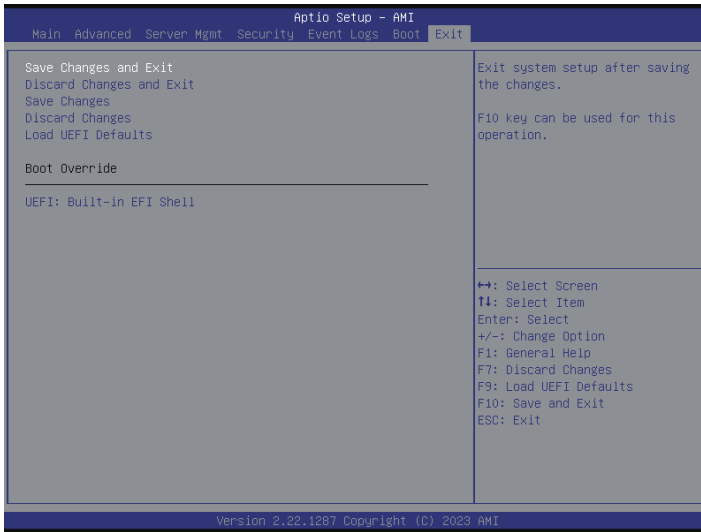
Boot Beep

Select whether the Boot Beep should be turned on or off when the system boots up. Please note that a buzzer is needed.

Full Screen Logo

Use this item to enable or disable OEM Logo. The default value is [Enabled].

3.8 Exit Screen



Save Changes and Exit

When selecting this option, the following message “Save configuration changes and exit setup?” will pop-out. Press <F10> key or select [Yes] to save the changes and exit the UEFI SETUP UTILITY.

Discard Changes and Exit

When selecting this option, the following message “Discard changes and exit setup?” will pop-out. Press <ESC> key or select [Yes] to exit the UEFI SETUP UTILITY without saving any changes.

Save Changes

When selecting this option, the following message “Save changes?” will pop-out. Press <F7> key or select [Yes] to save all changes.

Discard Changes

When selecting this option, the following message “Discard changes?” will pop-out. Press <F7> key or select [Yes] to discard all changes.

Load UEFI Defaults

Load UEFI default values for all the setup questions. F9 key can be used for this operation.

Chapter 4 Software Support

After all the hardware has been installed, it suggests to go to the official website at <http://www.ASRockRack.com> and make sure if there are any new updates of the BIOS / BMC firmware for the motherboard.

4.1 Download and Install Operating System

This motherboard supports various Microsoft® Windows® Server / Linux compliant operating systems. Please download the operating system from the OS manufacturer. Please refer to the OS documentation for more instructions.

**Please download the Intel® Rapid Storage Technology driver from the ASRock Rack's website (www.asrockrack.com) to the USB drive while installing OS in SATA RAID mode.*

4.2 Download and Install Software Drivers

This motherboard supports various Microsoft® Windows® compliant drivers. Please download the required drivers from the website at <http://www.ASRockRack.com>.

To download necessary drivers, go to the product page, click on the "Download" tab, choose the operating system that is used, and then download the using driver.

4.3 Contact Information

Contact ASRock Rack or want to know more about ASRock Rack, welcome to visit ASRock Rack's website at <http://www.ASRockRack.com>; or contact the dealer for further information.

Chapter 5 Troubleshooting

5.1 Troubleshooting Procedures

Follow the procedures below to troubleshoot the system.



Always unplug the power cord before adding, removing or changing any hardware components. Failure to do so may cause physical injuries and damages to motherboard components.

1. Disconnect the power cable and check whether the PWR LED is off.
2. Unplug all cables, connectors and remove all add-on cards from the motherboard.
Make sure that the jumpers are set to default settings.
3. Confirm that there are no short circuits between the motherboard and the chassis.
4. Install a CPU and fan on the motherboard, then connect the chassis speaker and power LED.

If there is no power...

1. Confirm that there are no short circuits between the motherboard and the chassis.
2. Make sure that the jumpers are set to default settings.
3. Check the settings of the 115V/230V switch on the power supply.
4. Verify if the battery on the motherboard provides ~3VDC. Install a new battery if it does not.

If there is no video...

1. Try replugging the monitor cables and power cord.
2. Check for memory errors.

If there are memory errors...

1. Verify that the DIMM modules are properly seated in the slots.
2. Use recommended DDR5 RDIMM/RDIMM-3DS
3. Install more than one DIMM modules that should be identical with the same brand, speed, size and chip-type.
4. Try inserting different DIMM modules into different slots to identify faulty ones.
5. Check the settings of the 115V/230V switch on the power supply.

Unable to save system setup configurations...

1. Verify if the battery on the motherboard provides ~3VDC. Install a new battery if it does not.
2. Confirm whether the power supply provides adequate and stable power.

Other problems...

1. Try searching keywords related to the related problem on ASRock Rack's FAQ page:
<http://www.asrockrack.com/support>

5.2 Technical Support Procedures

If the problems are still unsolved, please contact ASRock Rack's technical support with the following information:

1. Contact information
2. Model name, BIOS version and problem type.
3. System configuration.
4. Problem description.

Contact ASRock Rack's technical support at:
<http://www.asrockrack.com/support/tsd.asp>

5.3 Returning Merchandise for Service

For warranty service, the receipt or a copy of the invoice marked with the date of purchase is required. By calling the vendor or going to RMA website (<http://event.asrockrack.com/tsd.asp>) to obtain a Returned Merchandise Authorization (RMA) number.

The RMA number should be displayed on the outside of the shipping carton which is mailed prepaid or hand-carried when returning the motherboard to the manufacturer. Shipping and handling charges will be applied for all orders that must be mailed when service is complete.

This warranty does not cover damages incurred in shipping or from failure due to alteration, misuse, abuse or improper maintenance of products.

Contact the distributor first for any product related problems during the warranty period.

Contact Information

Contact ASRock Rack or want to know more about ASRock Rack, you're welcome to visit ASRock Rack's website at <http://www.asrockrack.com>; or contact the dealer for further information. For technical questions, please submit a support request form at <https://event.asrockrack.com/tsd.asp>

ASRock Rack Incorporation

e-mail: ASRockRack_sales@asrockrack.com

ASRock Rack Europe B.V.

Bijsterhuizen 11-11
6546 AR Nijmegen
The Netherlands
Phone: +31-24-345-44-33

ASRock Rack America Inc.

4331 Eucalyptus Ave., Chino, CA 91710 U.S.A.
Phone: +1-909-590-8308
Fax: +1-909-590-1026