HPM-SRSUA

Intel® single 4th Gen. Xeon® Scalable Processor ATX Server Board with Intel® C741 Chipset and IPMI2.0 Processor supports up to 250W TDP

User's Manual

2nd Ed –11 July 2023

Part No: E2047A4S001R

FCC Statement

THIS DEVICE COMPLIES WITH PART 15 FCC RULES. OPERATION IS SUBJECT TO THE FOLLOWING TWO CONDITIONS:

(1) THIS DEVICE MAY NOT CAUSE HARMFUL INTERFERENCE.

(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 "A" DIGITAL DEVICE, PURSUANT TO PART 15 OF THE FCC RULES.

THESE LIMITS ARE DESIGNED TO PROVIDE REASONABLE PROTECTION AGAINST HARMFUL INTERFERENCE WHEN THE EQUIPMENT IS OPERATED IN A COMMERCIAL ENVIRONMENT. THIS EQUIPMENT GENERATES, USES, AND CAN RADIATE RADIO FREQUENCY ENERGY AND, IF NOT INSTALLED AND USED IN ACCORDANCE WITH THE INSTRUCTION MANUAL, MAY CAUSE HARMFUL INTERFERENCE TO RADIO COMMUNICATIONS.

OPERATION OF THIS EQUIPMENT IN A RESIDENTIAL AREA IS LIKELY TO CAUSE HARMFUL INTERFERENCE IN WHICH CASE THE USER WILL BE REQUIRED TO CORRECT THE INTERFERENCE AT HIS OWN EXPENSE.

Notice

This guide is designed for experienced users to setup the system within the shortest time. For detailed information, please always refer to the electronic user's manual.

Copyright Notice

Trademark Acknowledgement

Brand and product names are trademarks or registered trademarks of their respective owners.

Disclaimer

Avalue Technology Inc. reserves the right to make changes, without notice, to any product, including circuits and/or software described or contained in this manual in order to improve design and/or performance. Avalue Technology assumes no responsibility or liability for the use of the described product(s), conveys no license or title under any patent, copyright, or masks work rights to these products, and makes no representations or warranties that

these products are free from patent, copyright, or mask work right infringement, unless otherwise specified. Applications that are described in this manual are for illustration purposes only. Avalue Technology Inc. makes no representation or warranty that such application will be suitable for the specified use without further testing or modification.

Life Support Policy

Avalue Technology's PRODUCTS ARE NOT FOR USE AS CRITICAL COMPONENTS IN LIFE SUPPORT DEVICES OR SYSTEMS WITHOUT THE PRIOR WRITTEN APPROVAL OF Avalue Technology Inc.

As used herein:

1. Life support devices or systems are devices or systems which, (a) are intended for surgical implant into body, or (b) support or sustain life and whose failure to perform, when properly used in accordance with instructions for use provided in the labeling, can be reasonably expected to result in significant injury to the user.
2. A critical component is any component of a life support device or system whose failure to perform can be reasonably expected to cause the failure of the life support device or system, or to affect its safety or effectiveness.

A Message to the Customer

Avalue Customer Services

Each and every Avalue's product is built to the most exacting specifications to ensure reliable performance in the harsh and demanding conditions typical of industrial environments. Whether your new Avalue device is destined for the laboratory or the factory floor, you can be assured that your product will provide the reliability and ease of operation for which the name Avalue has come to be known.

Your satisfaction is our primary concern. Here is a guide to Avalue's customer services. To ensure you get the full benefit of our services, please follow the instructions below carefully.

Technical Support

We want you to get the maximum performance from your products. So if you run into technical difficulties, we are here to help. For the most frequently asked questions, you can easily find answers in your product documentation. These answers are normally a lot more detailed than the ones we can give over the phone. So please consult the user's manual first.

To receive the latest version of the user's manual; please visit our Web site at:
http://www.avalue.com.tw/

Product Warranty

Avalue warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for two years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Avalue, or which have been subject to misuse, abuse, accident or improper installation. Avalue assumes no liability under the terms of this warranty as a consequence of such events. Because of Avalue's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If any of Avalue's products is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time, and freight. Please consult your dealer for more details. If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU type and speed, Avalue's products model name, hardware & BIOS revision number, other hardware and software used, etc.) Note anything abnormal and list any on-screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information available.
3. If your product is diagnosed as defective, obtain an RMA (return material authorization) number from your dealer. This allows us to process your good return more quickly.
4. Carefully pack the defective product, a complete Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Content

1. Getting Started

1.1 Safety Precautions

Warning!

Always completely disconnect the power cord from your chassis whenever you work with the hardware. Do not make connections while the power is on. Sensitive electronic components can be damaged by sudden power surges. Only experienced electronics personnel should open the PC chassis.

Caution!

Always ground yourself to remove any static charge before touching the CPU card. Modern electronic devices are very sensitive to static electric charges. As a safety precaution, use a grounding wrist strap at all times. Place all electronic components in a static-dissipative surface or static-shielded bag when they are not in the chassis.

1.2 Packing List

Before you begin installing your single board, please make sure that the following materials have been shipped:

- 1 x HPM-SRSUA motherboard
- 1 x I/O Shield
- 1 x LGA4677 CPU carrier-E1B

If any of the above items is damaged or missing, contact your retailer.

1.3 Document Amendment History

Revision	Date	By	Comment
1st	March 2023	Avalue	Initial Release
2nd	July 2023	Avalue	Update Packing List

1.4 Manual Objectives

This manual describes in details Avalue Technology HPM-SRSUA Single Board.

We have tried to include as much information as possible but we have not duplicated information that is provided in the standard IBM Technical References, unless it proved to be necessary to aid in the understanding of this board.

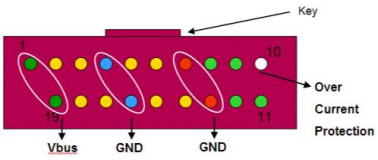
We strongly recommend that you study this manual carefully before attempting to set up HPM-SRSUA or change the standard configurations. Whilst all the necessary information is available in this manual we would recommend that unless you are confident, you contact your supplier for guidance.

Please be aware that it is possible to create configurations within the CMOS RAM that make booting impossible. If this should happen, clear the CMOS settings, (see the description of the Jumper Settings for details).

If you have any suggestions or find any errors regarding this manual and want to inform us of these, please contact our Customer Service department with the relevant details.

1.5 System Specifications

System	
CPU	Supports single 4th Gen. Intel® Xeon® Scalable Processors up to 250W TDP in Socket E
BIOS	AMI UEFI BIOS
System Chipset	Intel C741 Chipset
System Memory	6 x DDR5 4800MT/s RDIMM up to 1.5TB
Watchdog Timer	System reset event 0~6553 second.
H/W Status Monitor	Temperature. Fan. Voltage. Case open. (1 x 2.5mm pitch Box Wafer, Pinrex 753-71-02TW07 or equivalent)
RAID	Intel VMD and Virtual RAID on CPU(VROC) 1 x Intel VROC header
TPM	TPM 2.0 NuvoTon NPCT750AADYX or equivalent TCM Nationz Z32H330TC or equivalent (Optional)
Other	IPMI 2.0 with AST 2600 BMC controller onboard.
Expansion Slot	
PCIe	4 x PCIe Gen5 x16 slots and 3 x PCIe Gen5 x4 slots Slot 1, PCIe Gen5 x16 Slot 2, PCIe Gen5 x4 Slot 3, PCIe Gen5 x16 Slot 4, PCIe Gen5 x4 Slot 5, PCIe Gen5 x16 Slot 6, PCIe Gen5 x4 Slot 7, PCIe Gen5 x16 (The slot closest to CPU)
Storage	
M.2	1 x M.2 M-Key Slot to support 1 x SATA or 1 x PCIe 3.0 x4 NVMe SSD 2242/2260/2280/22110 form factor
SATA	5 x SATA III Supports up to 6.0 Gb/s (Note: SATA 1~4 support RAID 0,1,5,10)
Edge I/O	
COM	1 x DB-9 male connector (Connector : DB-9(male) and DB-15(female) dual port right angle)
LAN	5 x RJ45 (Including MGMT, LAN1, 2, 3, and 4) MGMT port : Dedicated IPMI function access LAN 1 : 1GbE Ethernet port, LAN1 shared with IPMI function access

<table>
<tr><td></td><td>(Connector : 1 x 1G Base-T RJ45 module jack over 2 x USB 3.1 Gen1 stacked receptacle)
LAN 2 : 2.5GbE Ethernet port
(Connector : 1 x 2.5G Base-T RJ45 module jack over 2 x USB 3.1 Gen1 stacked receptacle)
LAN 3 and 4 : 2 x 10GbE Ethernet ports (Optional)
(Connector : 1 x 2X1 10G Base-T RJ45 module jack)</td></tr>
<tr><td>USB 2.0</td><td>2 x USB 2.0 type A ports
(Connector : USB 2.0 type A double stacked USB receptacle)</td></tr>
<tr><td>USB 3.1</td><td>4 x USB 3.1 type A ports
(Connector : 1 x 1G Base-T RJ45 module jack over 2 x USB 3.1 Gen1 stacked receptacle)
(Connector : 1 x 2.5G Base-T RJ45 module jack over 2 x USB 3.1 Gen1 stacked receptacle)</td></tr>
<tr><td>VGA</td><td>1 x DB-15 female connector (Connector : DB-9(male) and DB-15(female) dual port right angle)</td></tr>
<tr><td>Onboard I/O</td><td></td></tr>
<tr><td>COM</td><td>1 x RS232 ports (1 x 2.0mm pitch Box Header)
Pin definition: Follow Avalue standard.</td></tr>
<tr><td>USB 3.1</td><td>4 x USB 3.1 Gen1 ports (2 x USB 3.1 Gen1 2.0mm pitch Box Header (Pinrex 52X-8020GB52 or equivalent)
Pin definition :
 

<table>
<tr><th>Pin No.</th><th>Signal</th><th>Description</th></tr>
<tr><td>1</td><td>Vbus</td><td>Power</td></tr>
<tr><td>2</td><td>IntA_P1_SSRX-</td><td>USB3 ICC Port1 SuperSpeed Rx-</td></tr>
<tr><td>3</td><td>IntA_P1_SSRX+</td><td>USB3 ICC Port1 SuperSpeed Rx+</td></tr>
<tr><td>4</td><td>GND</td><td>GND</td></tr>
<tr><td>5</td><td>IntA_P1_SSTX-</td><td>USB3 ICC Port1 SuperSpeed Tx-</td></tr>
<tr><td>6</td><td>IntA_P1_SSTX+</td><td>USB3 ICC Port1 SuperSpeed Tx+</td></tr>
<tr><td>7</td><td>GND</td><td>GND</td></tr>
<tr><td>8</td><td>IntA_P1_D-</td><td>USB3 ICC Port1 D- (USB2 Signal D-)</td></tr>
<tr><td>9</td><td>IntA_P1_D+</td><td>USB3 ICC Port1 D+ (USB2 Signal D+)</td></tr>
<tr><td>10</td><td>ID</td><td>Over Current Protection</td></tr>
<tr><td>11</td><td>IntA_P2_D+</td><td>USB3 ICC Port2 D+ (USB2 Signal D+)</td></tr>
<tr><td>12</td><td>IntA_P2_D-</td><td>USB3 ICC Port2 D- (USB2 Signal D-)</td></tr>
<tr><td>13</td><td>GND</td><td>GND</td></tr>
<tr><td>14</td><td>IntA_P2_SSTX+</td><td>USB3 ICC Port2 SuperSpeed Tx+</td></tr>
<tr><td>15</td><td>IntA_P2_SSTX-</td><td>USB3 ICC Port2 Super Speed Tx-</td></tr>
<tr><td>16</td><td>GND</td><td>GND</td></tr>
<tr><td>17</td><td>IntA_P2_SSRX+</td><td>USB3 ICC Port2 SuperSpeed Rx+</td></tr>
<tr><td>18</td><td>IntA_P2_SSRX-</td><td>USB3 ICC Port2 SuperSpeed Rx-</td></tr>
<tr><td>19</td><td>Vbus</td><td>Power</td></tr>
</table></td></tr>
<tr><td>CPU/System FAN</td><td>1 x 4 Pin CPU Fan Header (4 Pin PWM)</td></tr>
</table>

<table>
<tr><td></td><td>6 x 4 Pin Chassis Fan Header (4 Pin PWM, 2 for front fans and 4 for rear fans)</td></tr>
<tr><td>Buzzer</td><td>1 x onboard buzzer</td></tr>
<tr><td>Front Panel</td><td>1 x front panel connector (2.54 mm Pitch)
<table>
<tr><td>Pin</td><td>Function</td><td>Pin</td><td>Function</td></tr>
<tr><td>1-3</td><td>HDD LED</td><td>2-4</td><td>POWER LED</td></tr>
<tr><td>5-7</td><td>RESET BUTTON</td><td>6-8</td><td>POWER BUTTON</td></tr>
<tr><td>9-11</td><td>STATUS LED</td><td>10-12</td><td>LAN1 ACT LED</td></tr>
<tr><td>13-15</td><td>UID LED</td><td>14-16</td><td>STBY POWER LED</td></tr>
<tr><td>17-19</td><td>UID BUTTON</td><td>18-20</td><td>LAN2-X ACT LED</td></tr>
</table>
Notes: LAN2-X ACT LED, "X" means the max number of Ethernet ports.</td></tr>
<tr><td>RTC Battery</td><td>1 x Horizontal Socket Type CMOS Battery Holder with CR2450</td></tr>
<tr><td>Clear CMOS</td><td>1 x Clear CMOS header (1 x 2.0 mm pitch Header)</td></tr>
<tr><td>Audio</td><td>1 x Avalue HD audio interface (1 x 6x2 2.0mm pitch wafer connector)
<table>
<tr><td>Signal</td><td>Pin</td><td>Pin</td><td>Signal</td></tr>
<tr><td>ACZ_VCC3</td><td>1</td><td>2</td><td>GND</td></tr>
<tr><td>ACZ_SYNC</td><td>3</td><td>4</td><td>ACZ_BITCLK</td></tr>
<tr><td>ACZ_SDOUT</td><td>5</td><td>6</td><td>ACZ_SDIN0</td></tr>
<tr><td>ACZ_SDIN1</td><td>7</td><td>8</td><td>ACZ_RST#</td></tr>
<tr><td>ACZ_5VSB</td><td>9</td><td>10</td><td>GND-Chassis</td></tr>
<tr><td>GND</td><td>11</td><td>12</td><td>NC</td></tr>
</table></td></tr>
<tr><td>Display</td><td></td></tr>
<tr><td>Graphic Chipset</td><td>1 x VGA port (DB15 on edge I/O)
AST2600 BMC controller</td></tr>
<tr><td>Spec. & Resolution</td><td>1920 x 1200@60Hz 32bpp</td></tr>
<tr><td>Audio</td><td></td></tr>
<tr><td>Audio Codec</td><td>ALC888S through Avalue HD Audio daughter board.</td></tr>
<tr><td>Ethernet</td><td></td></tr>
<tr><td>LAN Chipset</td><td>1 x Intel I210AT
1 x Intel I226-LM
1 x Intel X550-AT2 (Optional)</td></tr>
<tr><td>LAN Spec.</td><td>1 x 1G Base-T Ethernet Controller
1 x 2.5G Base-T Ethernet controller
1 x Dual 10G Base-T Ethernet controller (Optional)</td></tr>
<tr><td>Mechanical & Environmental</td><td></td></tr>
<tr><td>Power Requirement</td><td>1 x Std. 24 pin ATX Connector
3 x 8 Pin SSI 12V Connectors</td></tr>
<tr><td>ACPI</td><td>Yes</td></tr>
<tr><td>Power Mode</td><td>H/W: ATX power well design only</td></tr>
</table>

	BMC: AT (Default)
Operating Temp.	0 °C to 60 °C (without Intel X550) 0 °C to 55 °C (with Intel X550)
Storage Temp.	-40 °C to 85 °C
Operating Humidity	40°C 95% non-condensing
Size (L x W) (Please consult product engineers for the production feasibility if the size is larger than 410x360mm or smaller than 80x70mm)	ATX form factor 12" x 9.6" (304.8mm x 243.84mm) PCB thickness is 2.54mm
Weight	1.19KG
Vibration Test	Follow Avalue standard test. Random Vibration Operation 1 Test PSD : 0.00454G²/Hz , 1.5 Grms 2 System condition : operation mode 3 Test frequency : 5~500 Hz 4 Test axis : X,Y and Z axis 5 Test time : 30 minutes per each axis 6 IEC60068-2-64 Test Fh 6 Storage : mSATA Random vibration test (Non-operation) 1 PSD: 0.00808G²/Hz , 2.0 Grms 2 Non-Operation mode 3 Test Frequency : 5-500Hz 4 Test Axis : X,Y and Z axis 5 30 min. per each axis 6 IEC 60068-2-64 Test:Fh Package Vibration Test: 1 Test PSD : 0.026G²/Hz , 2.16 Grms 2 Test frequency : 5~500 Hz 3 Test axis : X,Y and Z axis 4 Test time : 30 minutes per each axis 5 IEC 60068-2-64 Test Fh
Drop Test	Follow Avalue standard test. Reference ISTA 2A, Method : IEC-60068-2-32 Test:Ed Test Ea : Drop Test 1 Test phase : One corner, three edges, six faces

	2 Test high : 96.5cm 3 Package weight : 5Kg 4 Test drawing
OS Information	Windows : Windows 10 IoT Enterprise LTSC 2021. Windows 11 IoT Enterprise. Windows Server IoT 2019 with VT-d disabled. Windows Server IoT 2022. Linux : Ubuntu 20.04 LTS or later Red Hat Enterprise Linux (RHEL) 8.2 and later

Note: Specifications are subject to change without notice.

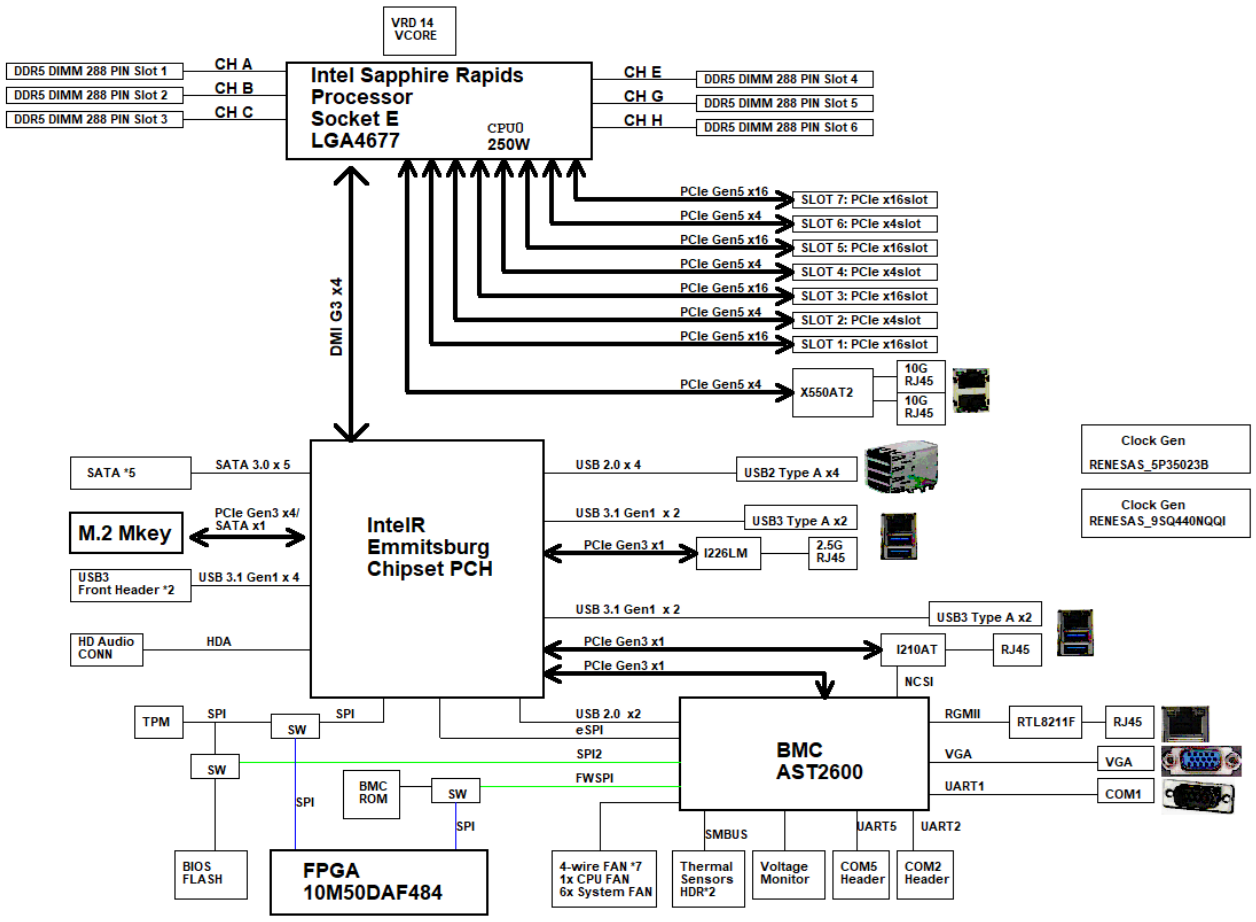
*Install 1/2/4/6 RAM

DIMM Quantity	HPM-SRSUA DIMM Sockets					
	DIMM1	DIMM2	DIMM3	DIMM4	DIMM5	DIMM6
1 DIMM	V					
1 DIMM		V				
1 DIMM				V		
2 DIMMs	V				V	
2 DIMMs			V	V		
4 DIMMs	V		V	V	V	
6 DIMMs	V	V	V	V	V	V

Sapphire Rapids DDR5 only DIMM configurations Diagram

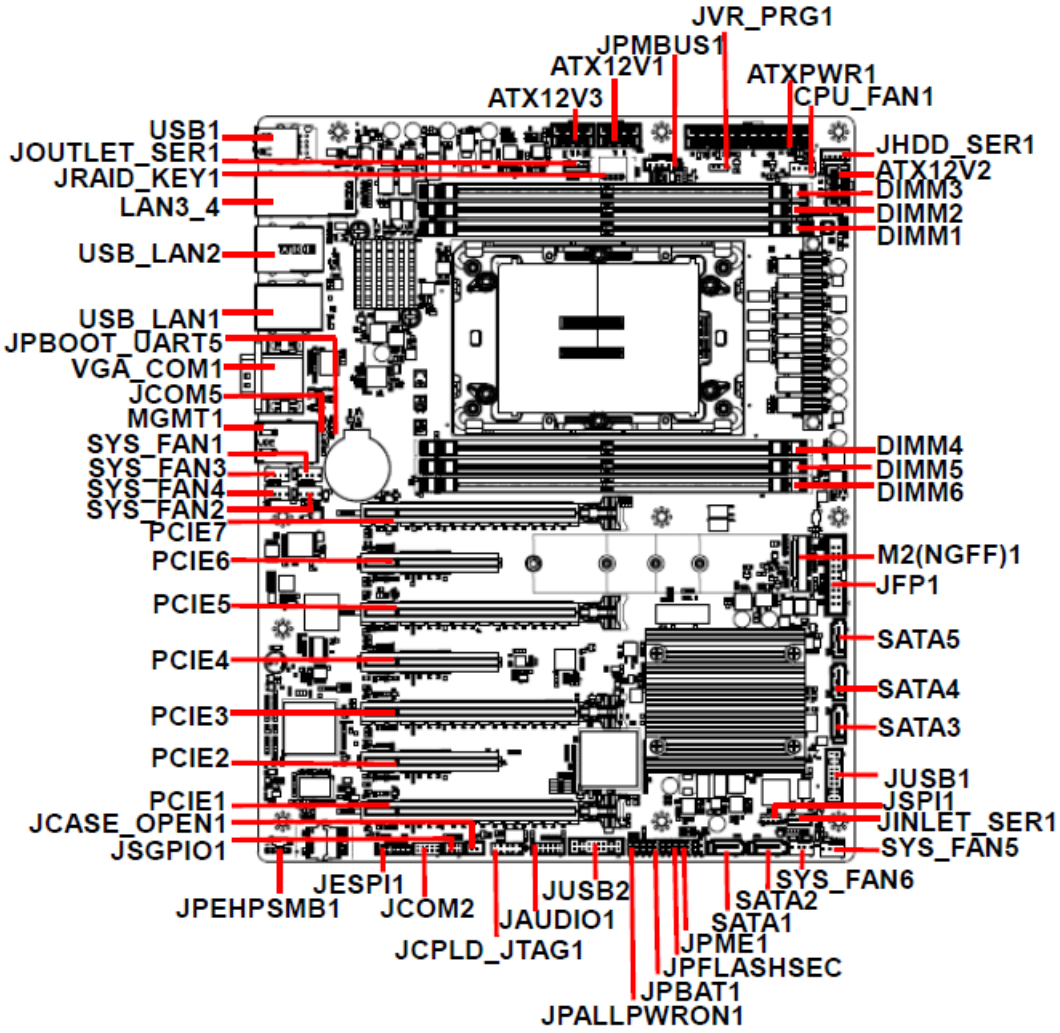
1.6 Architecture Overview—Block Diagram

The following block diagram shows the architecture and main components of HPM-SRSUA.



2. Hardware Configuration

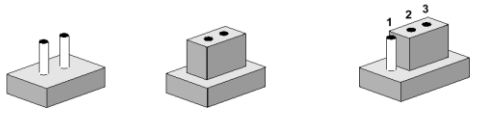
2.1 Product Overview



2.2 Jumper and Connector List

You can configure your board to match the needs of your application by setting jumpers. A jumper is the simplest kind of electric switch.

It consists of two metal pins and a small metal clip (often protected by a plastic cover) that slides over the pins to connect them. To "close" a jumper you connect the pins with the clip. To "open" a jumper you remove the clip. Sometimes a jumper will have three pins, labeled 1, 2, and 3. In this case, you would connect either two pins.



Open Closed Closed 2-3

The jumper settings are schematically depicted in this manual as follows:

Open Closed Closed 2-3

A pair of needle-nose pliers may be helpful when working with jumpers.

Connectors on the board are linked to external devices such as hard disk drives, a keyboard, or floppy drives. In addition, the board has a number of jumpers that allow you to configure your system to suit your application.

If you have any doubts about the best hardware configuration for your application, contact your local distributor or sales representative before you make any changes.

The following tables list the function of each of the board's jumpers and connectors.

Jumpers

Label	Function	Note
JPFLASHSEC	Flash Security Override	3 x 1 header, pitch 2.00mm
JPME1	ME FW update	3 x 1 header, pitch 2.00mm
JPALLPWRON1	Force PWRON setting	3 x 1 header, pitch 2.00mm
JPBAT1	Clear CMOS	3 x 1 header, pitch 2.00mm
JPBOOT_UART5	Boot UART5 setting	3 x 1 header, pitch 2.00mm

Connectors

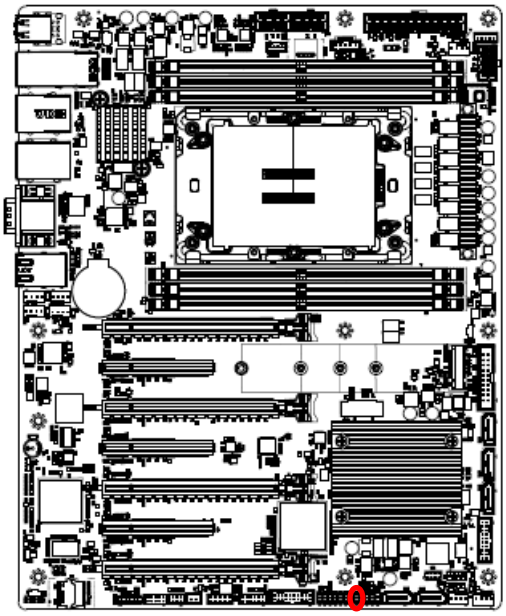
Label	Function	Note
SYS_FAN1	System fan connector 1	4 x 1 wafer, pitch 2.54mm
SYS_FAN2	System fan connector 2	4 x 1 wafer, pitch 2.54mm
SYS_FAN3	System fan connector 3	4 x 1 wafer, pitch 2.54mm
SYS_FAN4	System fan connector 4	4 x 1 wafer, pitch 2.54mm

SYS_FAN5	System fan connector 5	4 x 1 wafer, pitch 2.54mm
SYS_FAN6	System fan connector 6	4 x 1 wafer, pitch 2.54mm
CPU_FAN1	CPU fan connector	4 x 1 wafer, pitch 2.54mm
VGA_COM1	Serial port 1 connector VGA connector	
JCOM2	Serial port 2 connector	5 x 2 wafer, pitch 2.00mm
JCOM5	BMC_UART5 debug connector	4 x 1 header, pitch 2.54mm
MGMT1	MGMT port	
JSGPIO1	Serial General Purpose I/O connector	3 x 2 wafer, pitch 2.00mm
PCIE1	PCIe Gen5 x16	
PCIE2	PCIe Gen5 x4	
PCIE3	PCIe Gen5 x16	
PCIE4	PCIe Gen5 x4	
PCIE5	PCIe Gen5 x16	
PCIE6	PCIe Gen5 x4	
PCIE7	PCIe Gen5 x16 (The slot closest to CPU)	
JFP1	Front Panel connector	10 x 2 wafer, pitch 2.54mm
USB_LAN1	2 x USB3.1 Gen1 connector 1 x RJ-45 Ethernet (LAN1 Share IPMI Port)	
USB_LAN2	2 x USB3.1 Gen1 connector 1 x RJ-45 Ethernet	
LAN3_4	2 x RJ-45 Ethernet	
USB1	2 x USB2.0 connector	
JUSB1	USB3.1 Gen1 connector 1	10 x 2 wafer, pitch 2.00mm
JUSB2	USB3.1 Gen1 connector 2	10 x 2 wafer, pitch 2.00mm
JSPI1	SPI connector	4 x 2 header, pitch 2.00mm
JESPI1	ESPI connector	6 x 2 header, pitch 2.00mm
SATA1-5	5 x Serial ATA connector	
JRAID_KEY1	SATA RAID KEY connector	4 x 1 header, pitch 2.00mm
DIMM1-6	6 x DDR5 RDIMM socket	
JVR_PRG1	SMBUS VR connector	3 x 1 header, pitch 2.54mm
JCASE_OPEN1	CASE OPEN connector	2 x 1 wafer, pitch 2.50mm
ATX12V1	ATX 12V power connector 1	4 x 2 wafer, pitch 4.20mm
ATX12V2	ATX 12V power connector 2	4 x 2 wafer, pitch 4.20mm

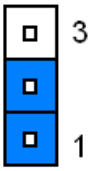
ATX12V3	ATX 12V power connector 3	4 x 2 wafer, pitch 4.20mm
ATXPWR1	ATX power connector	12 x 2 wafer, pitch 4.20mm
JPMBUS1	Power supply PMBus connector	5 x 1 wafer, pitch 2.54mm
JINLET_SER1	Inlet Thermal Sensor	4 x 1 wafer, pitch 2.00mm
JOUTLET_SER1	Outlet Thermal Sensor	4 x 1 wafer, pitch 2.00mm
JHDD_SER1	HDD Backplane thermal Sensor	5 x 1 wafer, pitch 2.00mm
JPEHPSMB1	CPU PCIE HP SMB connector	5 x 1 header, pitch 2.00mm
JAUDIO1	AZALIA connector	6 x 2 header, pitch 2.00mm
M2(NGFF)1	M.2 M-Key PCIe 3.0 x4 NVMe SSD	
JCPLD_JTAG1	CPLD JTAG header	5 x 2 header, pitch 2.54mm

2.3 Setting Jumpers & Connectors

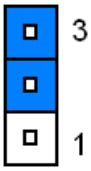
2.3.1 Flash Security Override (JPFLASHSEC)



Disable*

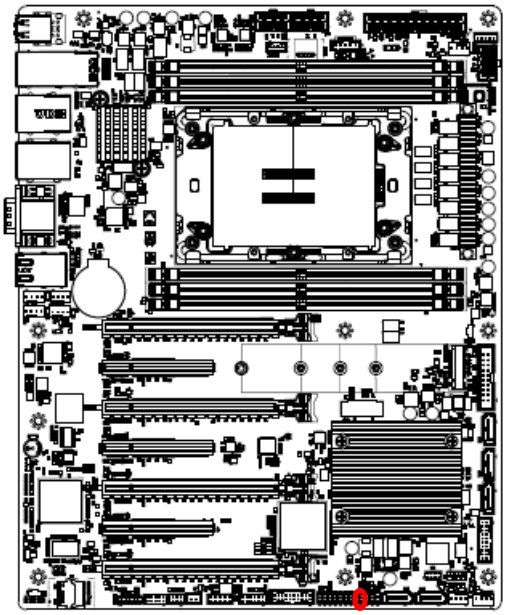


Enable

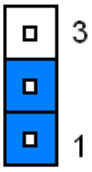


*** Default**

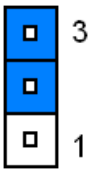
2.3.2 ME FW update (JPME1)



Normal*

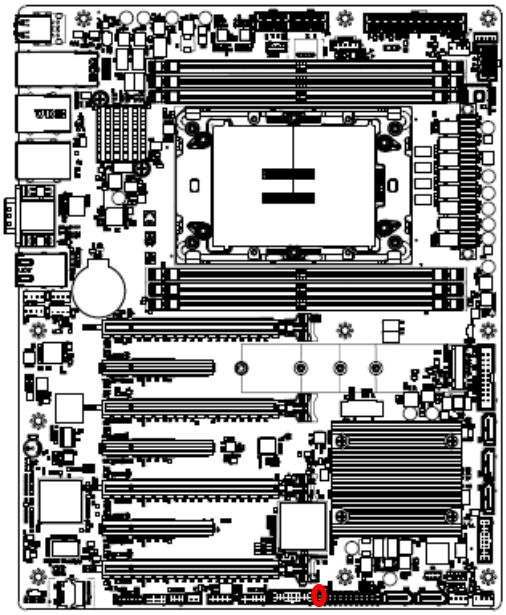


ME Force Update

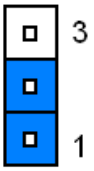


*** Default**

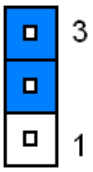
2.3.3 Force PWRON setting (JPALLPWRON1)



Normal Operation*

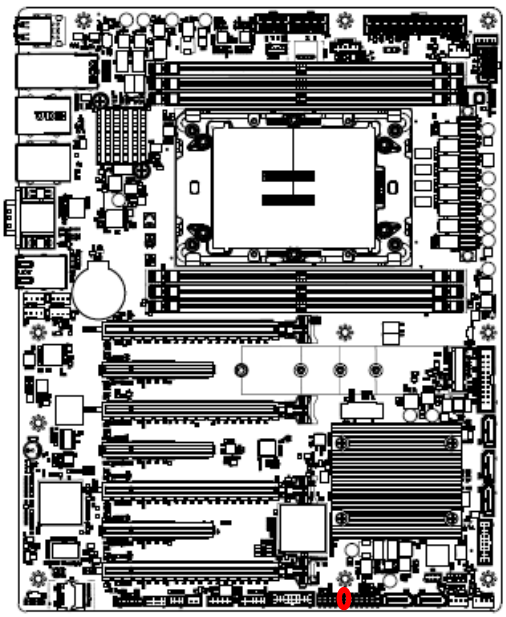


Enable Force PWR-ON

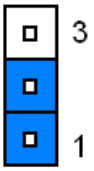


*** Default**

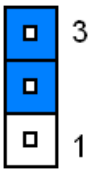
2.3.4 Clear CMOS (JPBAT1)



Normal Operation*

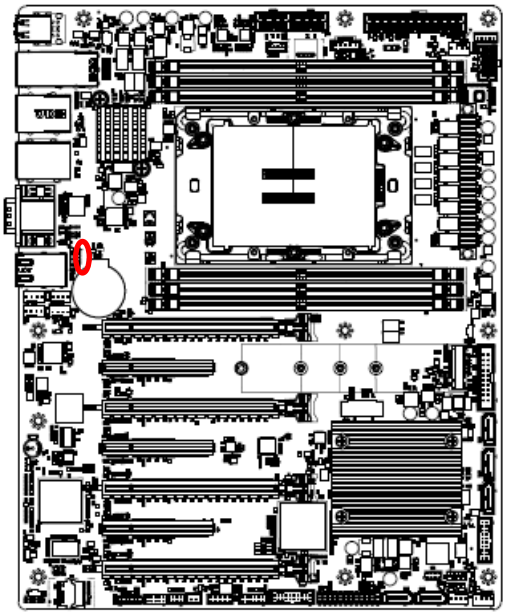


Clear RTC REGISTERS

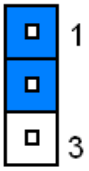


*** Default**

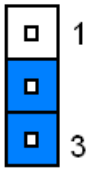
2.3.5 Boot UART5 setting (JPBOOT_UART5)



Disable*

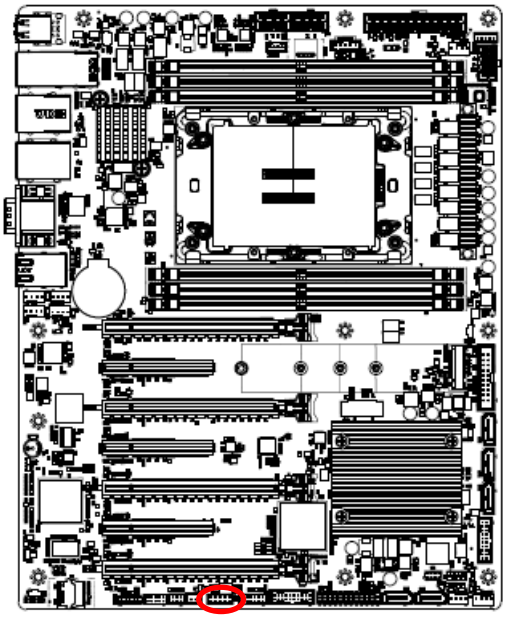


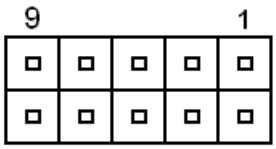
Enable BOOT FROM UART5



*** Default**

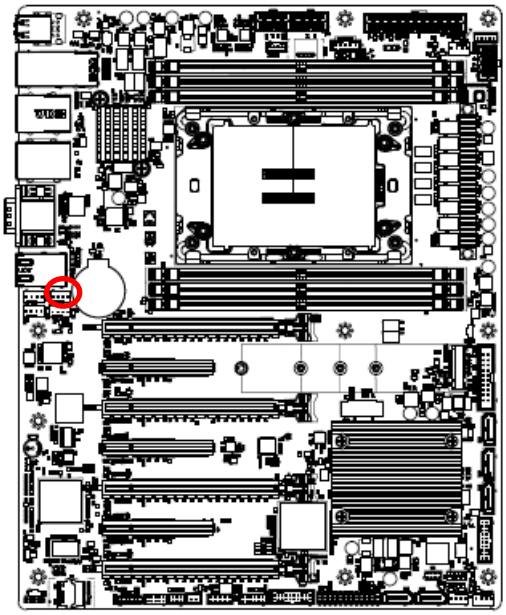
2.3.6 CPLD JTAG header (JCPLD_JTAG1)

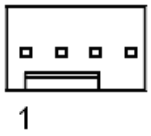




Signal	PIN	PIN	Signal
JTAG_TCK	1	2	GND
JTAG_TDO	3	4	+3.3VSB
JTAG_TMS	5	6	NC
NC	7	8	NC
JTAG_TDI	9	10	GND

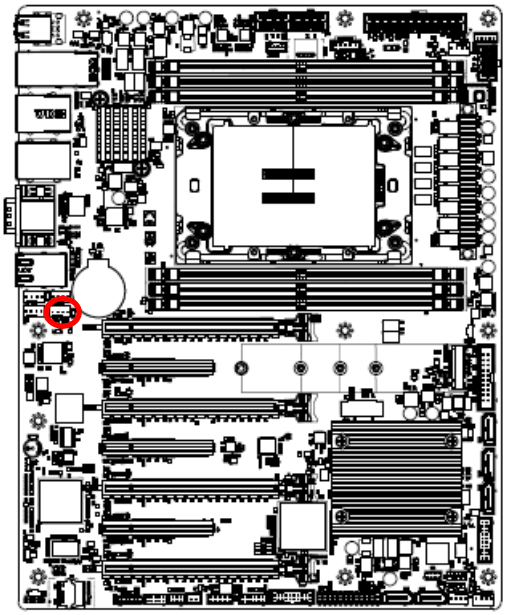
2.3.7 System fan connector 1 (SYS_FAN1)

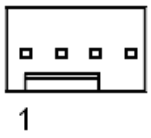




Signal	PIN
GND	1
+12V	2
FAN_TACH1	3
SYS_PWM1	4

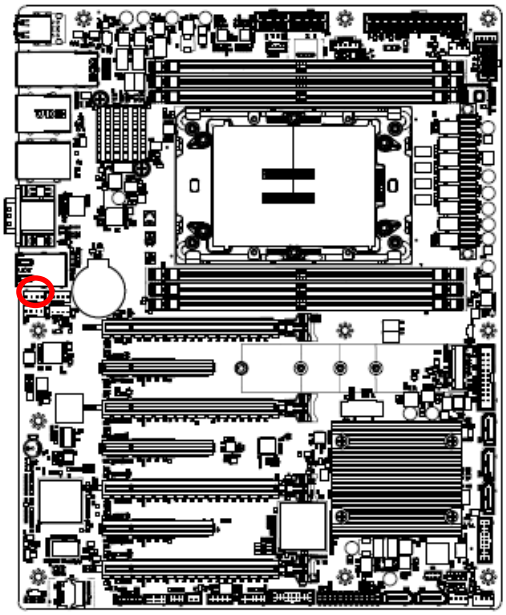
2.3.8 System fan connector 2 (SYS_FAN2)

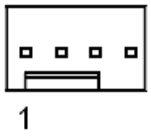




Signal	PIN
GND	1
+12V	2
FAN_TACH2	3
SYS_PWM2	4

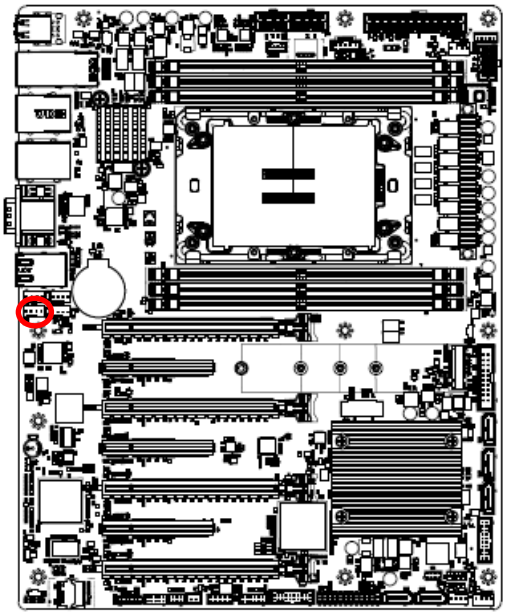
2.3.9 System fan connector 3 (SYS_FAN3)

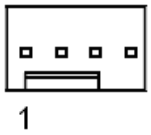




Signal	PIN
GND	1
+12V	2
FAN_TACH3	3
SYS_PWM3	4

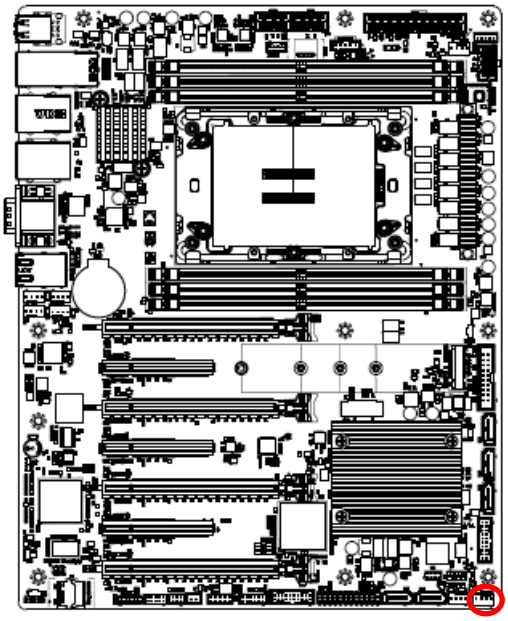
2.3.10 System fan connector 4 (SYS_FAN4)

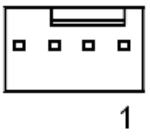




Signal	PIN
GND	1
+12V	2
FAN_TACH4	3
SYS_PWM4	4

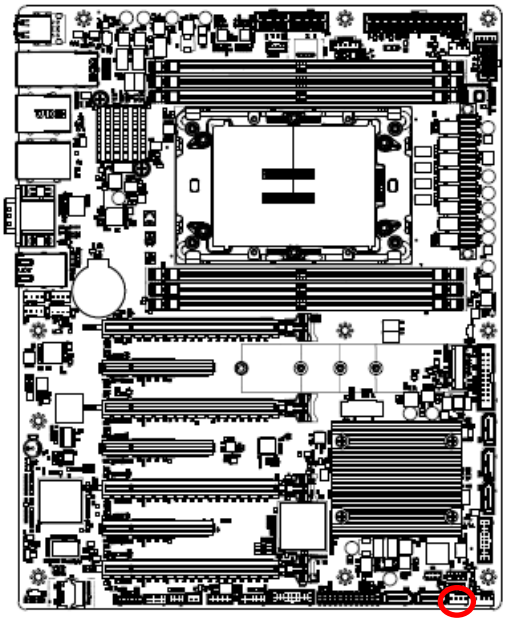
2.3.11 System fan connector 5 (SYS_FAN5)

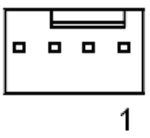




Signal	PIN
GND	1
+12V	2
FAN_TACH5	3
SYS_PWM5	4

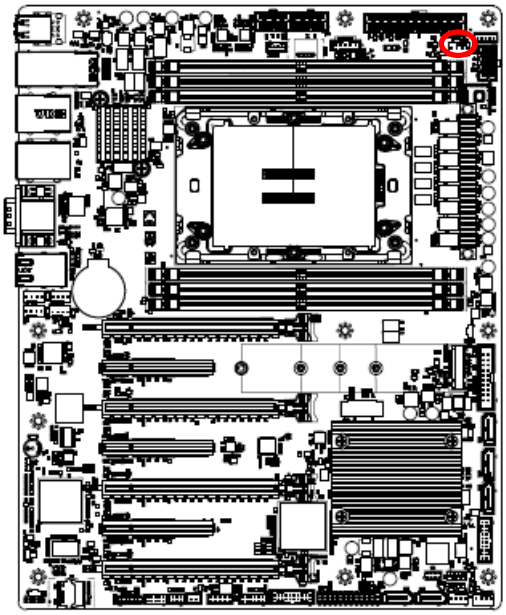
2.3.12 System fan connector 6 (SYS_FAN6)

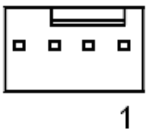




Signal	PIN
GND	1
+12V	2
FAN_TACH6	3
SYS_PWM6	4

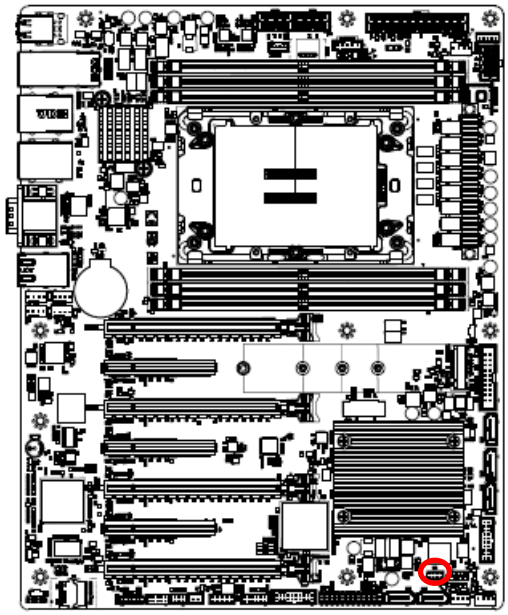
2.3.13 CPU fan connector (CPU_FAN1)

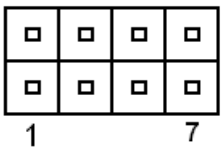




Signal	PIN
GND	1
+12V	2
FAN_TACH0	3
CPU0_PWM	4

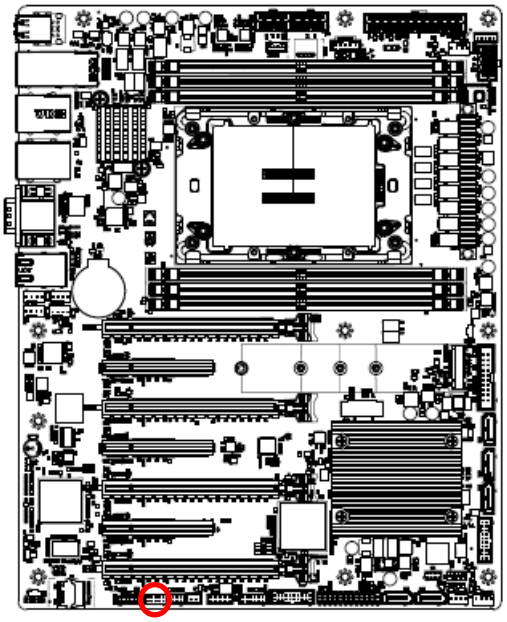
2.3.14 SPI connector (JSPI1)

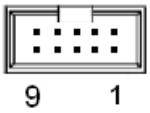




Signal	PIN	PIN	Signal
+3.3VSB	1	2	GND
SPI_CS#	3	4	SPI_CLK
SPI_MISO	5	6	SPI_MOSI
SPI_IO3	7	8	SPI_IO2

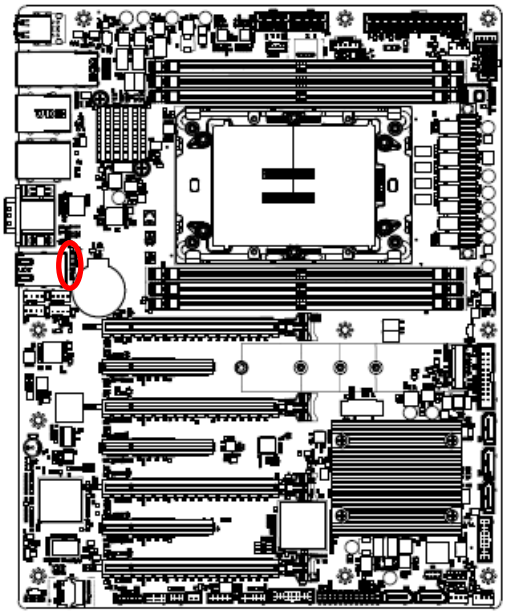
2.3.15 Serial port 2 connector (JCOM2)





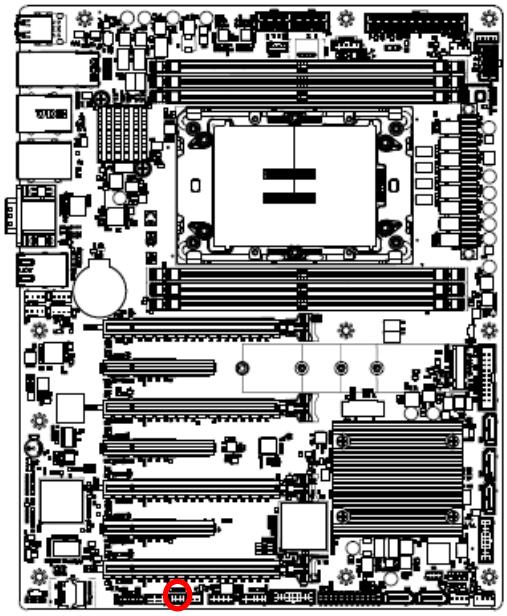
Signal	PIN	PIN	Signal
COM_DCD#2	1	2	COM_RXD2
COM_TXD2	3	4	COM_DTR#2
GND	5	6	COM_DSR#2
COM_RTS#2	7	8	COM_CTS#2
COM_RI#2	9	10	NC

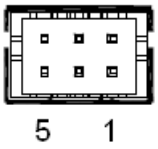
2.3.16 BMC_UART5 debug connector (JCOM5)



Signal	PIN
+3.3VSB	4
GND	3
UART5_RX	2
UART5_TX	1

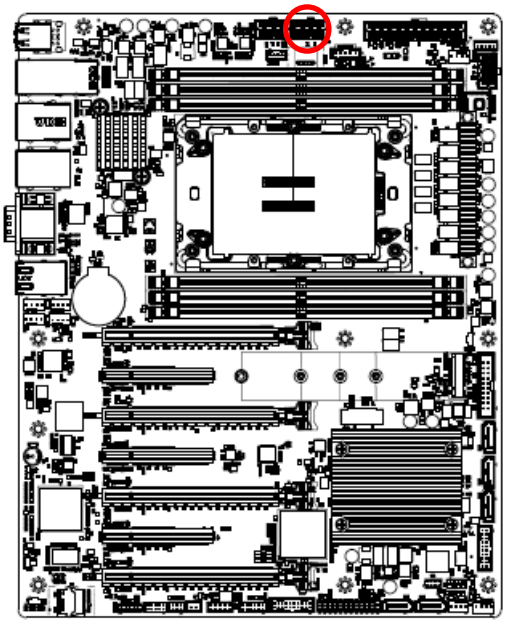
2.3.17 Serial General Purpose I/O connector (JSGPIO1)

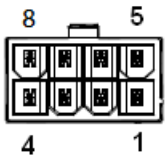




Signal	PIN	PIN	Signal
GND	2	1	GND
SGPIO_SATA0_DATA0	4	3	SGPIO_SATA0_LOAD
NC	6	5	SGPIO_SATA0_CLOCK

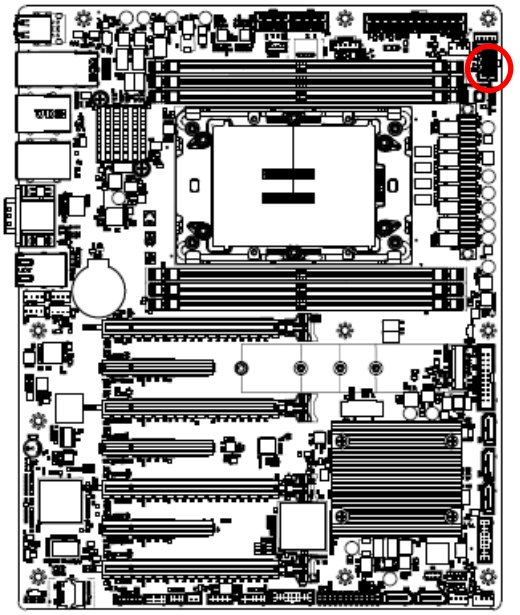
2.3.18 ATX 12V power connector 1 (ATX12V1)

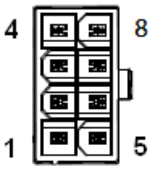




Signal	PIN	PIN	Signal
GND	1	5	+12V
GND	2	6	+12V
GND	3	7	+12V
GND	4	8	+12V

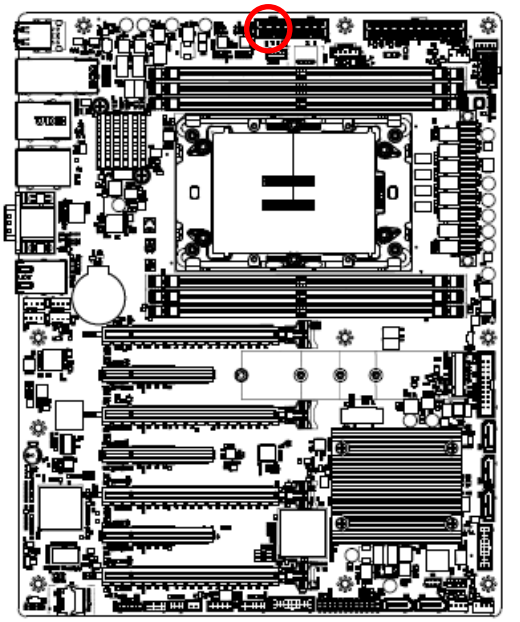
2.3.19 ATX 12V power connector 2 (ATX12V2)

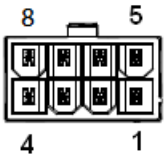




Signal	PIN	PIN	Signal
GND	1	5	+12V
GND	2	6	+12V
GND	3	7	+12V
GND	4	8	+12V

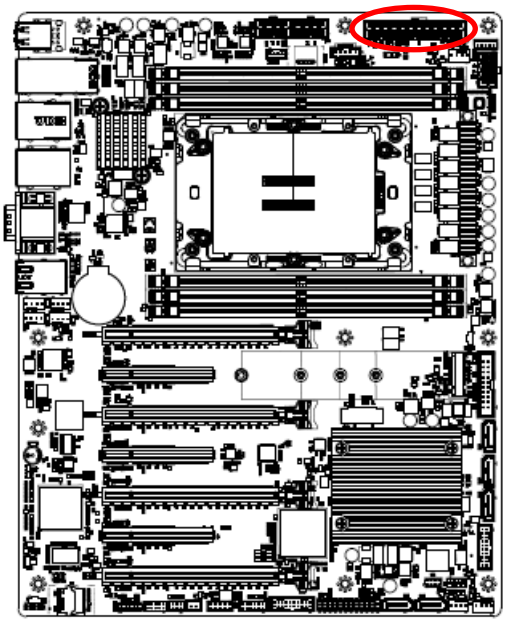
2.3.20 ATX 12V power connector 3 (ATX12V3)

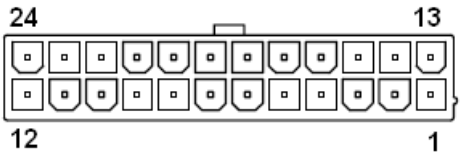




Signal	PIN	PIN	Signal
GND	1	5	+12V
GND	2	6	+12V
GND	3	7	+12V
GND	4	8	+12V

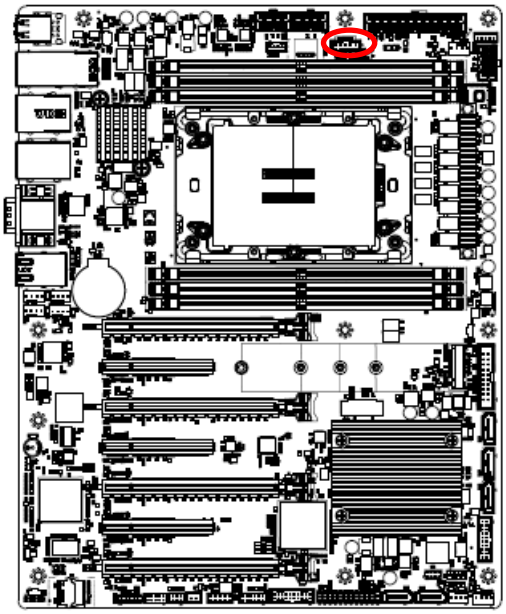
2.3.21 ATX power connector (ATXPWR1)

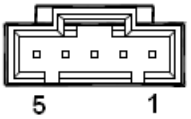




Signal	PIN	PIN	Signal
+3.3V	1	13	+3.3V
+3.3V	2	14	-12V
GND	3	15	GND
+5V	4	16	PSON#
GND	5	17	GND
+5V	6	18	GND
GND	7	19	GND
PSU_PWRGD	8	20	NC
+V5SB	9	21	+5V
+12V	10	22	+5V
+12V	11	23	+5V
+3.3V	12	24	GND

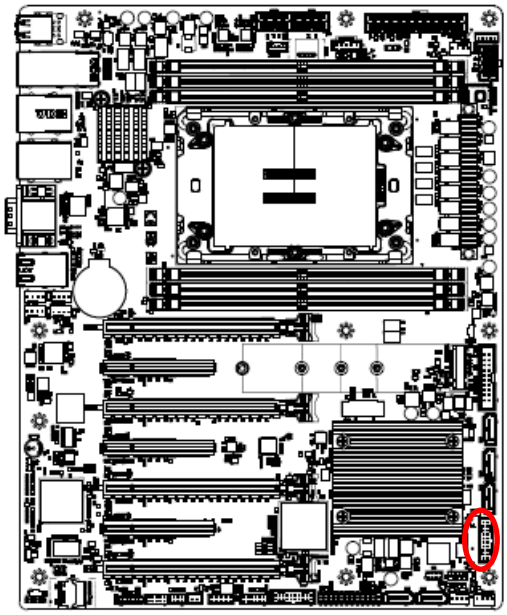
2.3.22 Power supply PMBus connector (JPMBUS1)

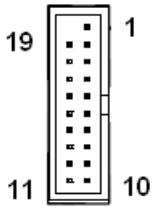




Signal	PIN
SMB_PSU_SCL	1
SMB_PSU_SDA	2
SMB_PSU_ALERT#	3
GND	4
NC	5

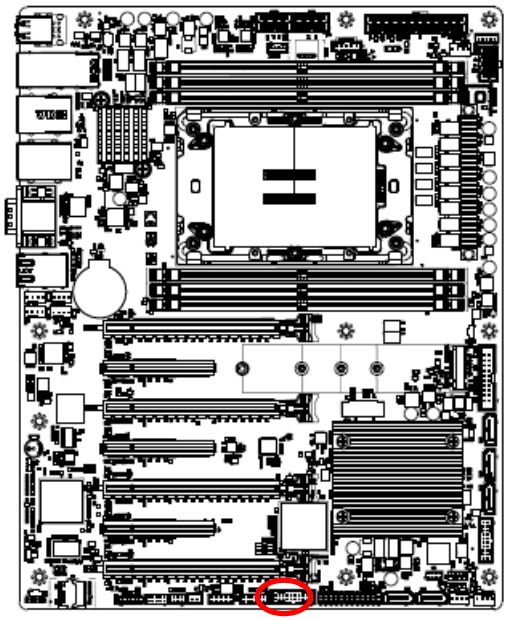
2.3.23 USB3.1 Gen1 connector 1 (JUSB1)

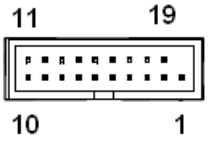




Signal	PIN	PIN	Signal
		1	+5V
+5V	19	2	USB3_RN4
USB3_RN5	18	3	USB3_RP4
USB3_RP5	17	4	GND
GND	16	5	USB3_TN4
USB3_TN5	15	6	USB3_TP4
USB3_TP5	14	7	GND
GND	13	8	USB3_PN8
USB3_PN9	12	9	USB3_PP8
USB3_PP9	11	10	USB_OC1#

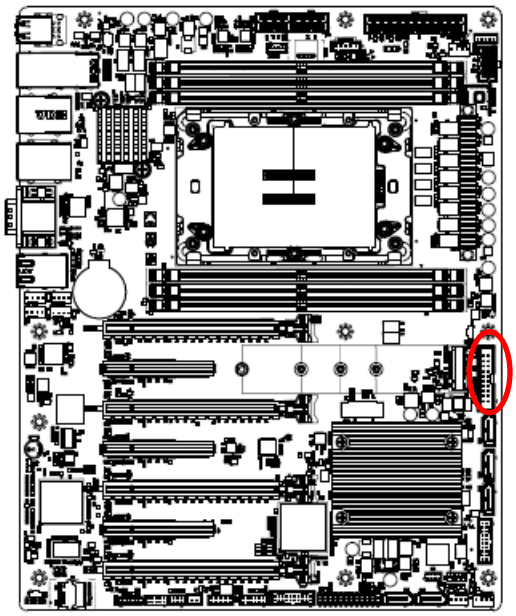
2.3.24 USB3.1 Gen1 connector 2 (JUSB2)

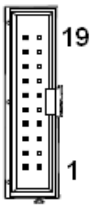




Signal	PIN	PIN	Signal
		1	+5V
+5V	19	2	USB3_RN6
USB3_RN7	18	3	USB3_RP6
USB3_RP7	17	4	GND
GND	16	5	USB3_TN6
USB3_TN7	15	6	USB3_TP6
USB3_TP7	14	7	GND
GND	13	8	USB3_PN11
USB3_PN13	12	9	USB3_PP11
USB3_PP13	11	10	USB_OC2#

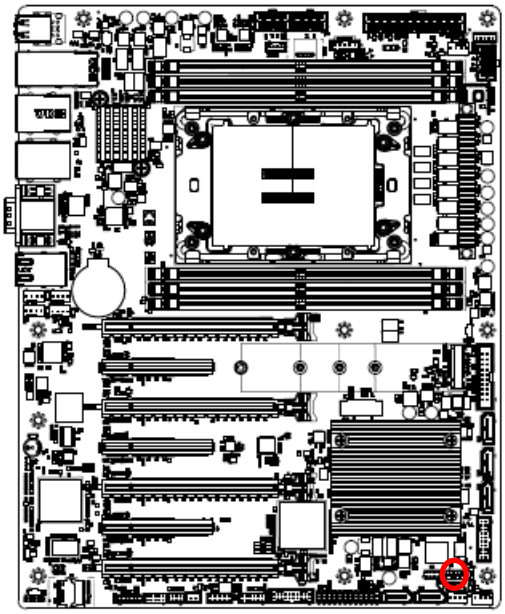
2.3.25 Front Panel connector (JFP1)

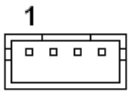




Signal	PIN	PIN	Signal
LAN2-X_LED#	20	19	GND
LAN2-X_LED_P	18	17	UID_BUTTON#
GND	16	15	UID_LED_P
SBPWRLED_P	14	13	UID_LED#
LAN1_LED#	12	11	STATUS_LED#
LAN1_LED_P	10	9	STATUS_LED_P
GND	8	7	GND
PWRON_BUTTON#	6	5	RESET_BUTTON#
PWR_LED#	4	3	HDD_LED#
+3.3VSB	2	1	HDD_LED_P

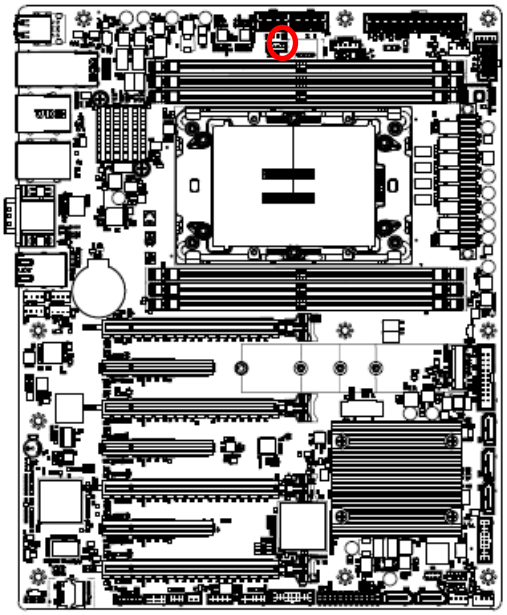
2.3.26 Inlet Thermal Sensor (JINLET_SER1)

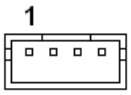




Signal	PIN
+3.3VSB	1
SMB_INLET_TEMPSENSOR_SDA	2
SMB_INLET_TEMPSENSOR_SCL	3
GND	4

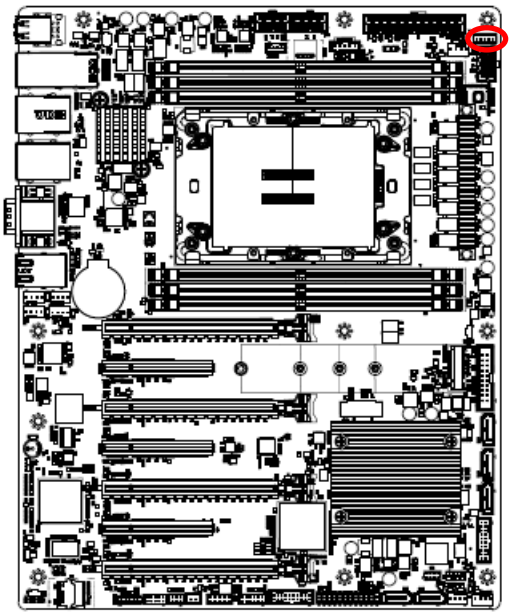
2.3.27 Outlet Thermal Sensor (JOUTLET_SER1)

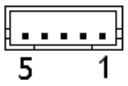




Signal	PIN
+3.3VSB	1
SMB_OUTLET_TEMPSENSOR_SDA	2
SMB_OUTLET_TEMPSENSOR_SCL	3
GND	4

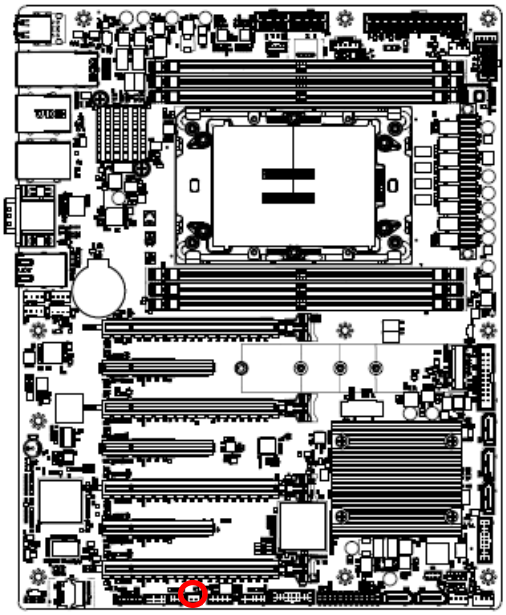
2.3.28 HDD Backplane thermal Sensor (JHDD_SER1)





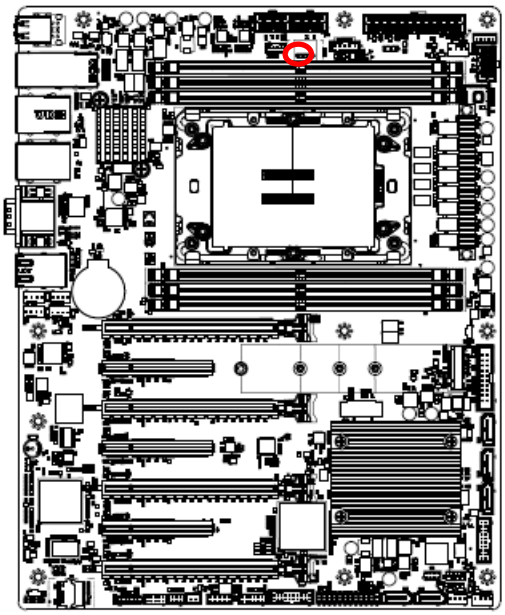
Signal	PIN
+3.3VSB	1
SMB_HDBP_TEMPSENSOR_SDA	2
SMB_HDBP_TEMPSENSOR_SCL	3
GND	4
SSD_LED_N	5

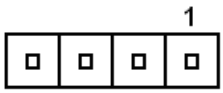
2.3.29 CASE OPEN connector (JCASE_OPEN1)



Signal	PIN
CHASSIS_INTRUSION	1
GND	2

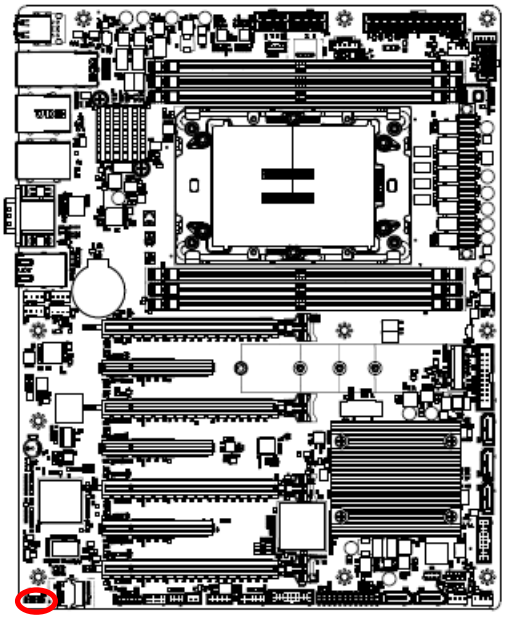
2.3.30 SATA RAID KEY connector (JRAID_KEY1)





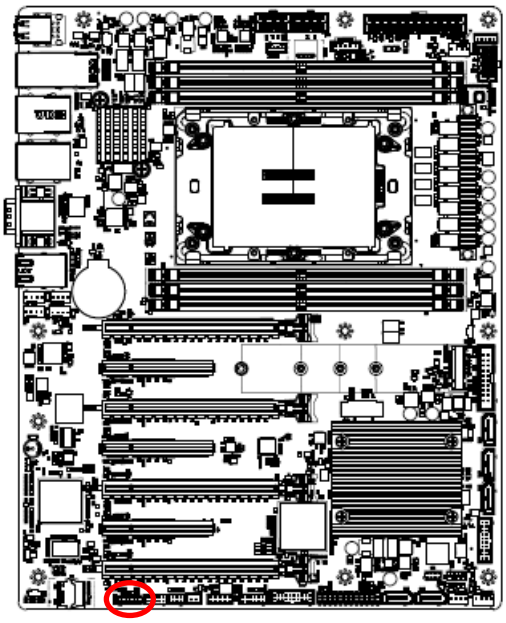
Signal	PIN
GND	1
PU_KEY_CONN	2
GND	3
PCH_SATA_RAIDKEY	4

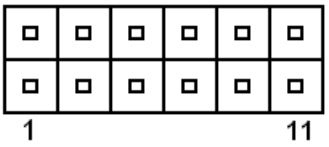
2.3.31 CPU PCIE HP SMB connector (JPEHPSMB1)



Signal	PIN
SMB_CPUHP_SCL	1
GND	2
SMB_CPUHP_SDA	3
GND	4
SMB_CPUHP_ALERT#	5

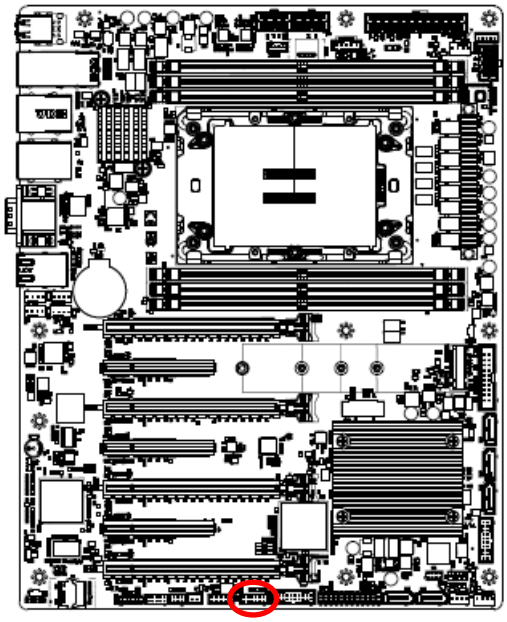
2.3.32 ESPI connector (JESPI1)

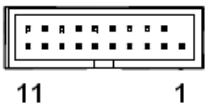




Signal	PIN	PIN	Signal
ESPI_D0	1	2	+3.3VSB
ESPI_D1	3	4	PLTRST#
ESPI_D2	5	6	ESPI_CS#
ESPI_D3	7	8	ESPI_CLK
NC	9	10	GND
ESPI_RESET#	11	12	ESPI_ALERT#

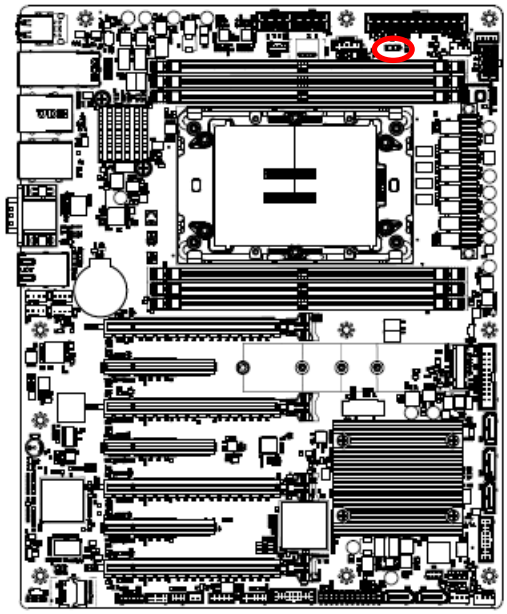
2.3.33 AZALIA connector (JAUDIO1)

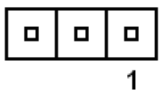




Signal	PIN	PIN	Signal
+3.3V	1	2	GND
AUD_AZA_SYNC	3	4	AUD_AZA_BCLK
AUD_AZA_SDO	5	6	AUD_AZA_SDI0
AUD_AZA_SDI1	7	8	AUD_AZA_RST_N
+5VSB	9	10	GND
GND	11	12	NC

2.3.34 SMBUS VR connector (JVR_PRG1)





Signal	PIN
SMB_VR_SDA	1
GND	2
SMB_VR_SCL	3

2.4 Processor Installation SOP

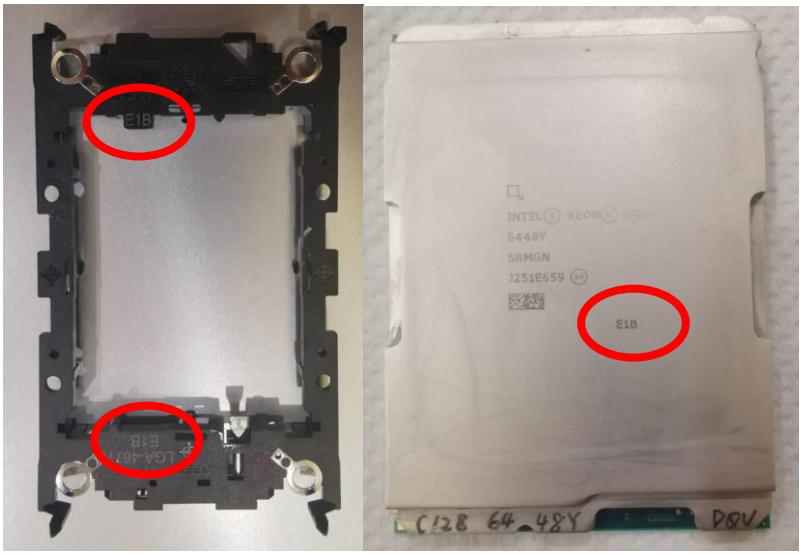
Overview of the Processor Assembly installation procedure

Note: Suggest installing the memory first, then installing the CPU cooler module to lower the memory installation difficulty.

The processor assembly contains the Intel Xeon SP with carrier and CPU cooler.

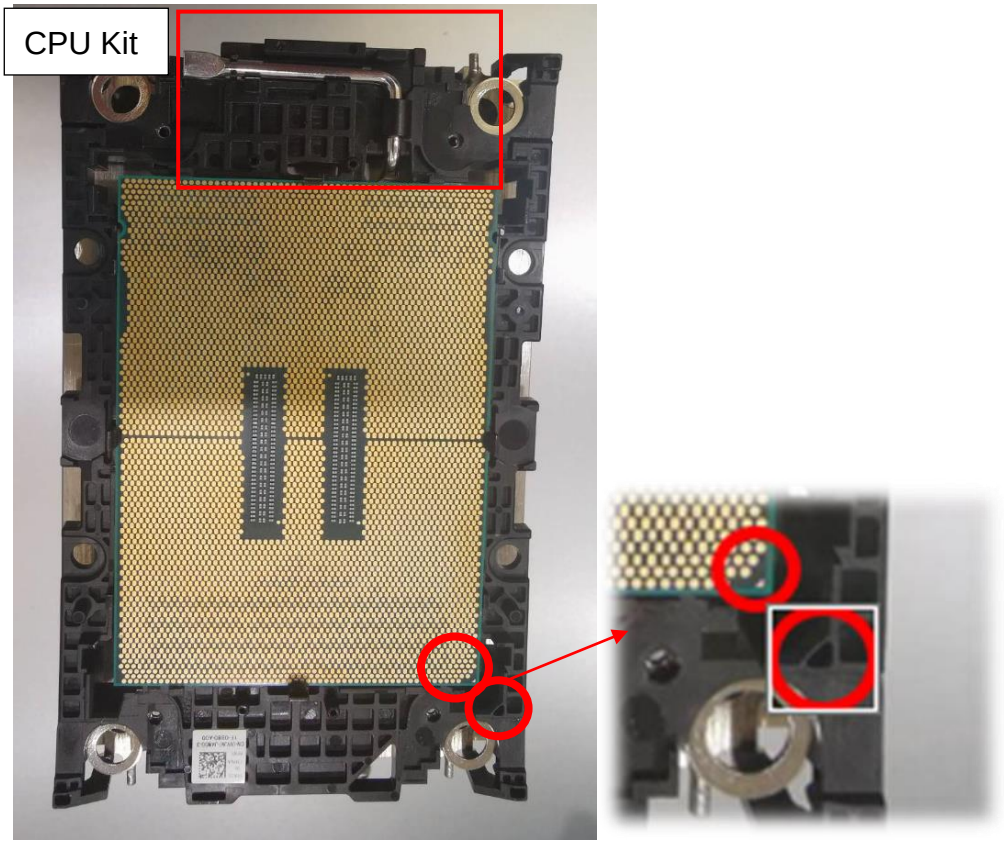
- 1x Intel 4th Xeon SP (MCC SKU)
- 1x E1B CPU Carrier (In the HPM-SRSUA package)
- 1x Cooler module (Avalue P/N:BCC-FAN-467-01R)

1. Please ensure the carrier model on the CPU is consistent with the carrier silkscreen.

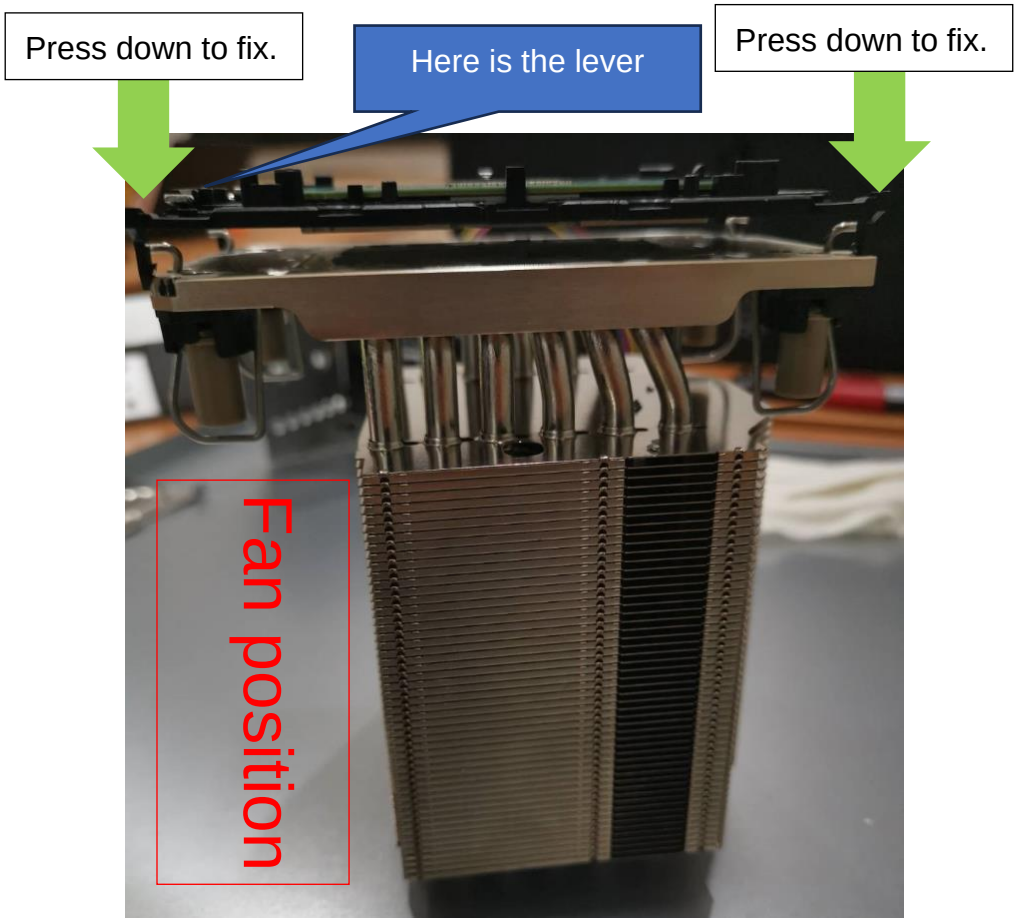


2. Install the CPU on the carrier and align the triangle marks (Pin 1).

Look at the below red frame, please make sure the lever is pressed down.



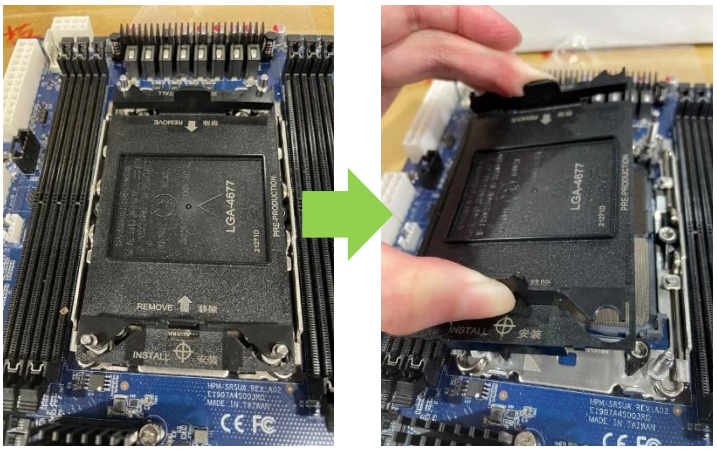
3. Install the CPU kit assembly on the cooler module, please press down the CPU kit to fixate it.
   Note: Make sure the lever on the carrier is on the same side as the fan. (Only applicable to HPM-SRSUA and Avalue Cooler BCC-FAN-467-01R.)
   Note: The Thermal grease must be pre-applied on the heatsink before installation.
   Note: Please ensure the direction of the fan before installing the CPU kit on the Cooler module.



4. The CPU socket is protected by a plastic protective cover.

a. Hold finger grips on socket cover and squeeze in on the grip tabs.

b. Then pull the cover up and off vertically to remove.



5. Cooler module with CPU kit installed on the motherboard.

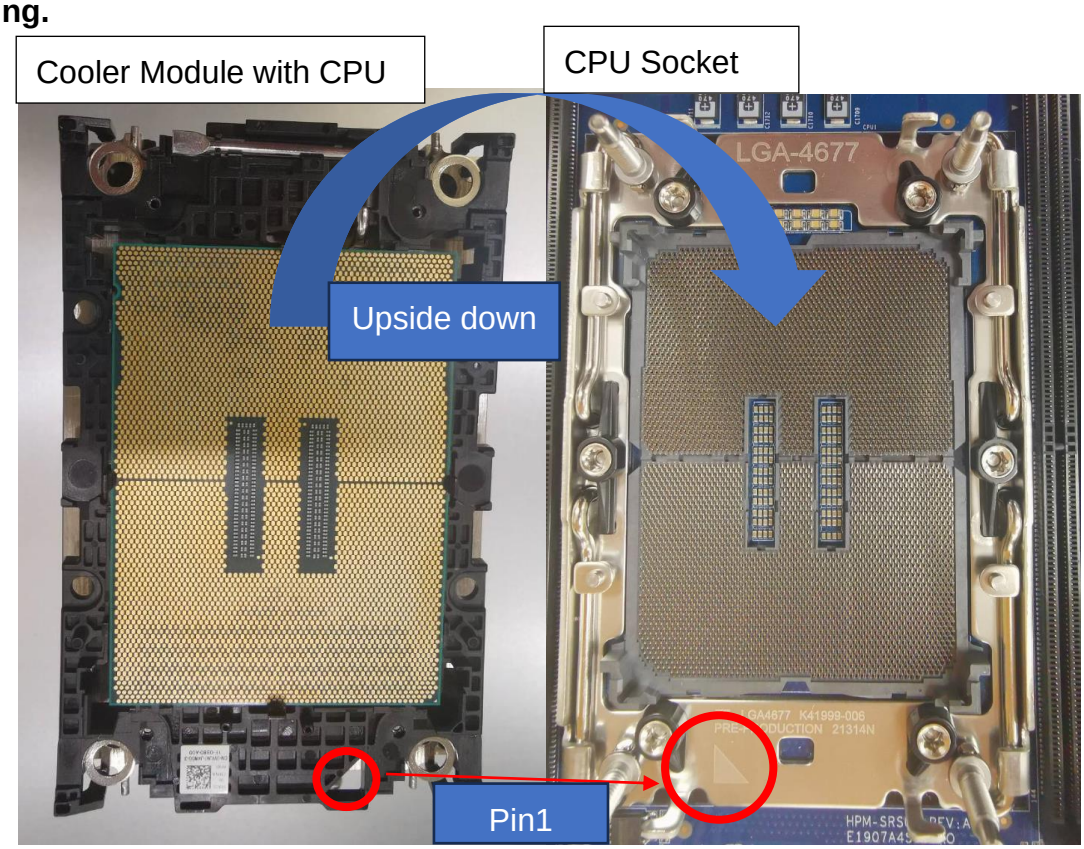
a. Please align the triangle mark between the Cooler module and CPU socket and install it. (Figure A)

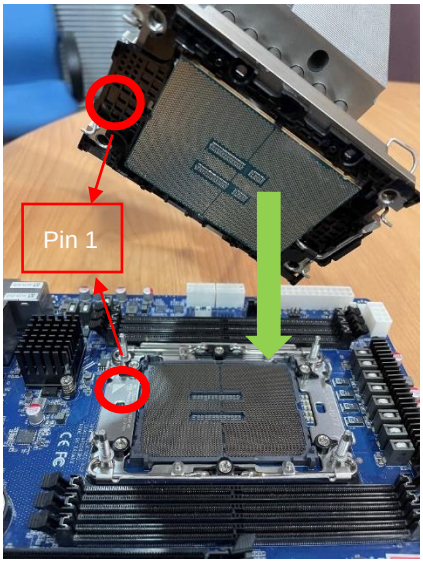
b. Hold the Cooler module with the CPU and align the holes with the CPU socket. Press the Cooler module down to the CPU socket until it snaps into place.

c. Press down the fixing tenons on the four sides to fixate. (Figure B)

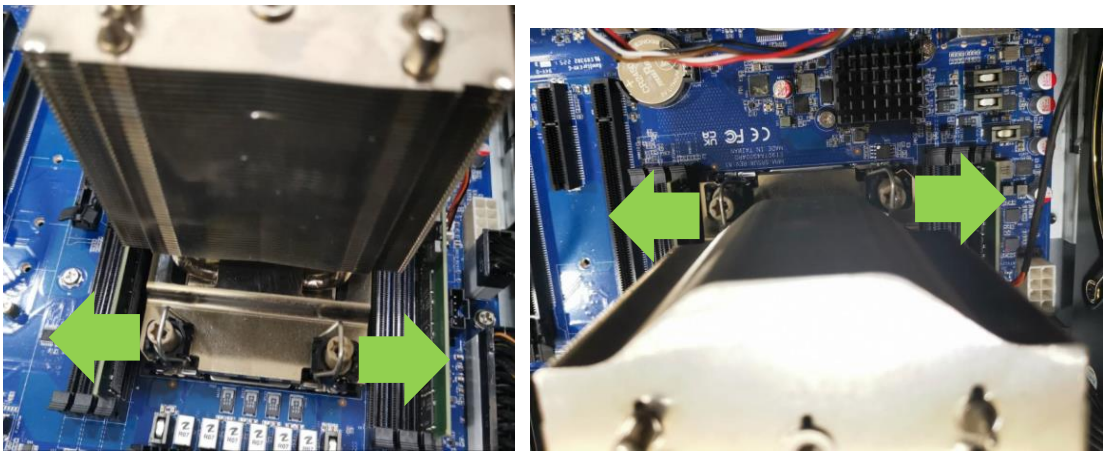
d. With a T30 screwdriver, gradually tighten the four screws to ensure even pressure. (Figure C)

★ The cooler module with CPU pin1 must be aligned with the CPU socket pin1 mark, and the direction cannot be changed at will, or it may cause the CPU to damage after pressing.

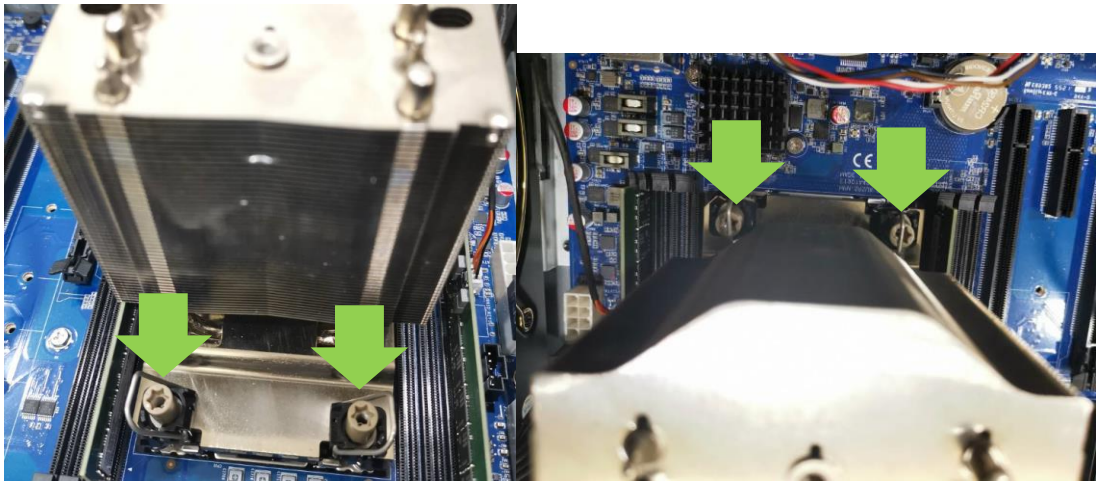




▲Figure A

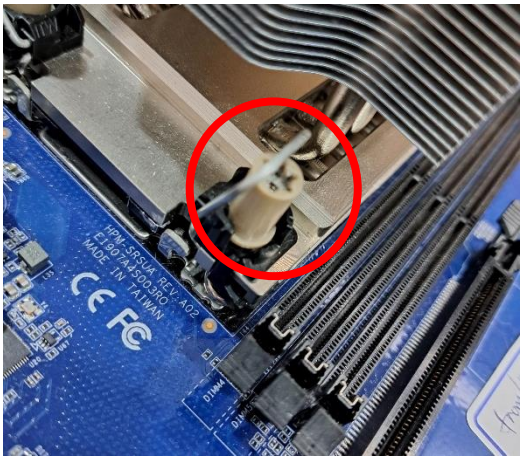


▲Figure B

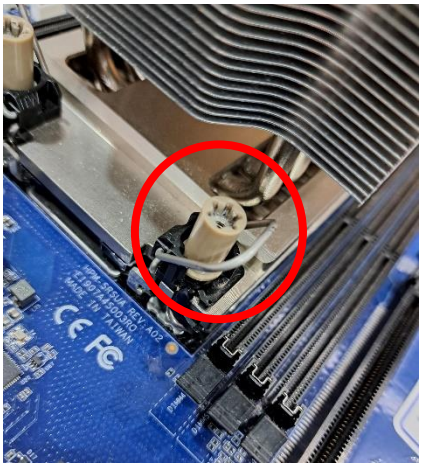


▲Figure C

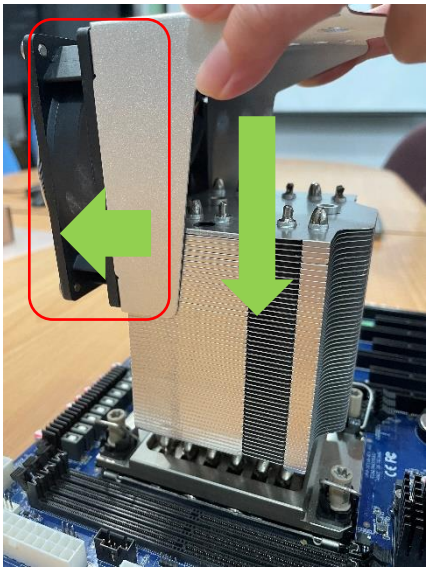
▼Before locking the tenons

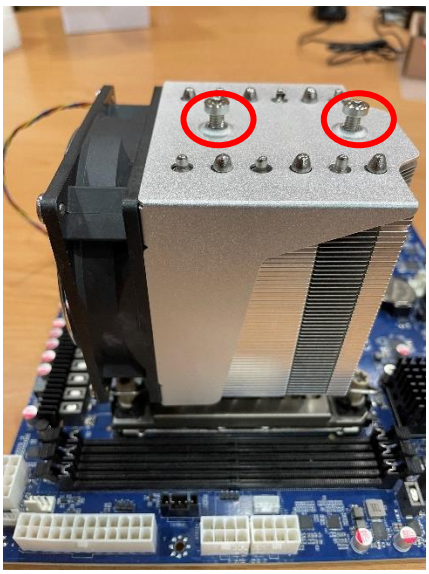


▼After locking the tenons



6. Install the cooling fan and holder on the cooler module and tighten two locking screws (T30) on the top of the fan holder.
   Note: The 4U cooler's fan for Xeon SP single socket is facing the opposite side of Edge I/O.





7. Connect the cooling fan connector to the fan header labeled for the CPU on the motherboard.

3.BIOS Setup

3.1 Introduction

The BIOS setup program allows users to modify the basic system configuration. In this following chapter will describe how to access the BIOS setup program and the configuration options that may be changed.

3.2 Starting Setup

AMI BIOS™ is immediately activated when you first power on the computer. The BIOS reads the system information contained in the NVRAM and begins the process of checking out the system and configuring it. When it finishes, the BIOS will seek an operating system on one of the disks and then launch and turn control over to the operating system.

While the BIOS is in control, the Setup program can be activated in one of two ways:
By pressing <ESC> or <Del> immediately after switching the system on, or
By pressing the < ESC> or <Del> key when the following message appears briefly at the left-top of the screen during the POST (Power On Self Test).

Press <ESC> or <Del> to enter SETUP

If the message disappears before you respond and you still wish to enter Setup, restart the system to try again by turning it OFF then ON or pressing the "RESET" button on the system case. You may also restart by simultaneously pressing <Ctrl>, <Alt>, and <Delete> keys.

3.3 Using Setup

In general, you use the arrow keys to highlight items, press <Enter> to select, use the PageUp and PageDown keys to change entries, press <F1> for help and press <Esc> to quit. The following table provides more detail about how to navigate in the Setup program using the keyboard.

Button	Description
↑	Move to previous item
↓	Move to next item
←	Move to the item in the left hand
→	Move to the item in the right hand
Esc key	Main Menu -- Quit and not save changes into NVRAM Status Page Setup Menu and Option Page Setup Menu -- Exit current page and return to Main Menu
+ key	Increase the numeric value or make changes
- key	Decrease the numeric value or make changes
F1 key	General help, only for Status Page Setup Menu and Option Page Setup Menu
F2 key	Previous Values
F3 key	Optimized defaults
F4 key	Save & Exit Setup

- **Navigating Through The Menu Bar**

  Use the left and right arrow keys to choose the menu you want to be in.

Note: Some of the navigation keys differ from one screen to another.

- **To Display a Sub Menu**

  Use the arrow keys to move the cursor to the sub menu you want. Then press <Enter>. A "➢" pointer marks all sub menus.

3.4 Getting Help

Press F1 to pop up a small help window that describes the appropriate keys to use and the possible selections for the highlighted item. To exit the Help Window press <Esc> or the <Enter> key again.

3.5 In Case of Problems

If, after making and saving system changes with Setup, you discover that your computer no longer is able to boot, the AMI BIOS supports an override to the NVRAM settings which resets your system to its defaults.

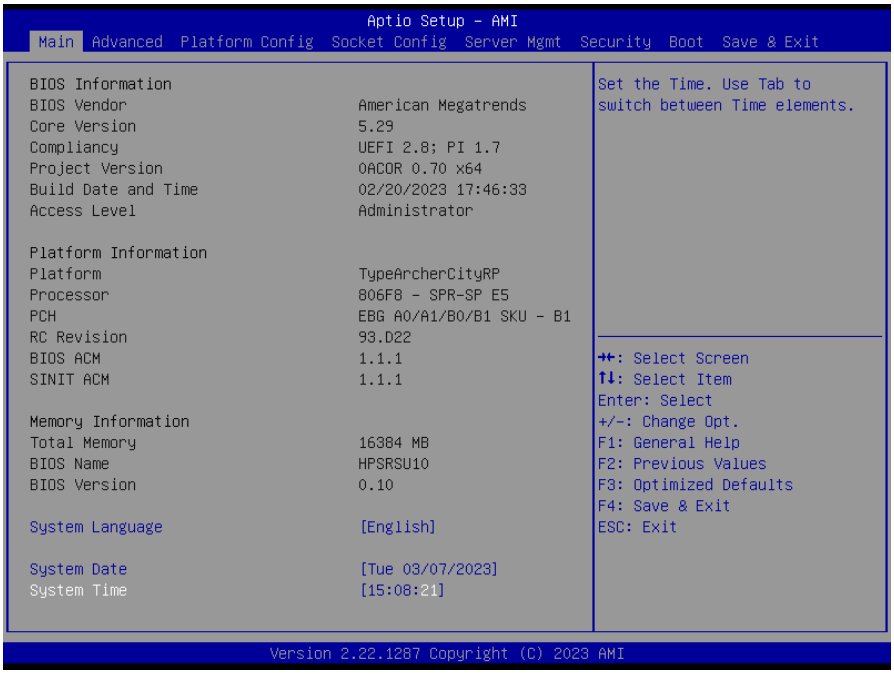
The best advice is to only alter settings which you thoroughly understand. To this end, we strongly recommend that you avoid making any changes to the chipset defaults. These defaults have been carefully chosen by both BIOS Vendor and your systems manufacturer to provide the absolute maximum performance and reliability. Even a seemingly small change to the chipset setup has the potential for causing you to use the override.

3.6 BIOS setup

Once you enter the Aptio Setup Utility, the Main Menu will appear on the screen. The Main Menu allows you to select from several setup functions and exit choices. Use the arrow keys to select among the items and press <Enter> to accept and enter the sub-menu.

3.6.1 Main Menu

This section allows you to record some basic hardware configurations in your computer and set the system clock.



3.6.1.1 System Language

This option allows choosing the system default language.

3.6.1.2 System Date

Use the system date option to set the system date. Manually enter the Month, day and year.

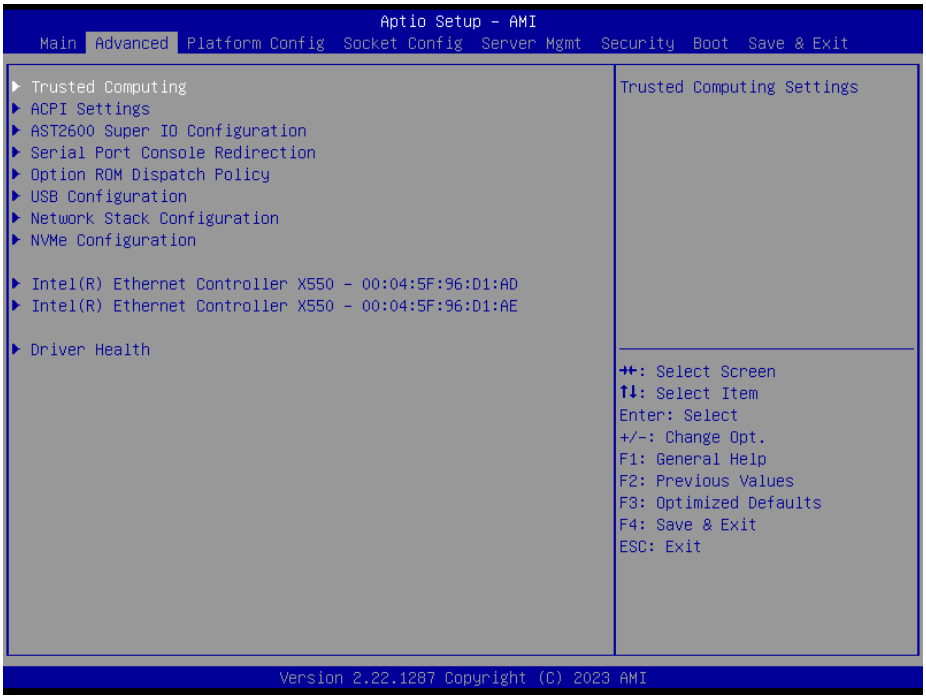
3.6.1.3 System Time

Use the system time option to set the system time. Manually enter the hours, minutes and seconds.

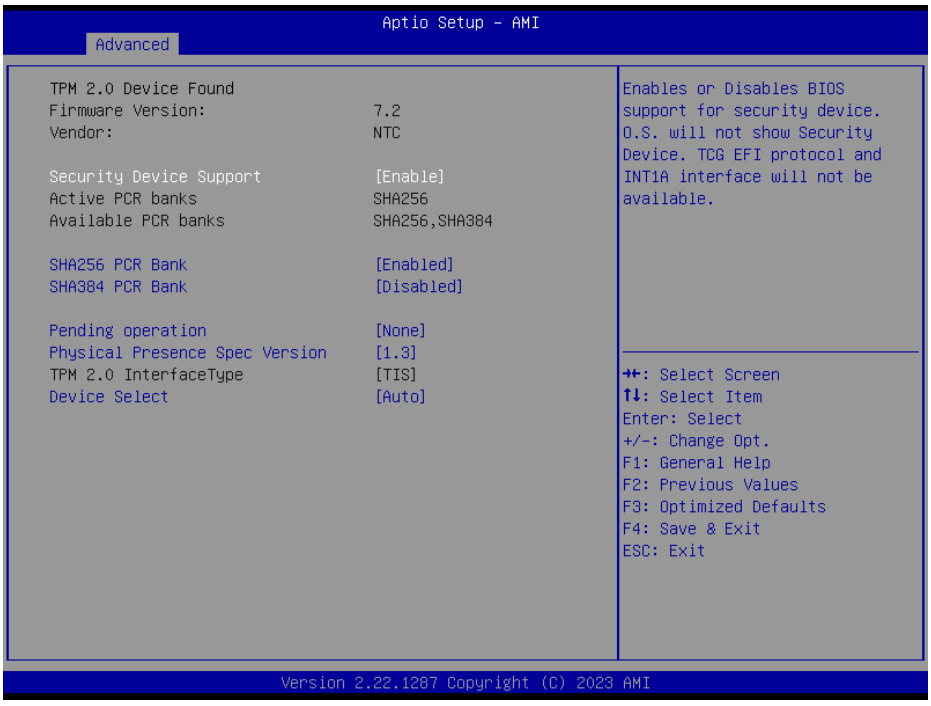
Note: The BIOS setup screens shown in this chapter are for reference purposes only, and may not exactly match what you see on your screen.
Visit the Avalue website (www.avalue.com.tw) to download the latest product and BIOS information.

3.6.2 Advanced Menu

This section allows you to configure your CPU and other system devices for basic operation through the following sub-menus.



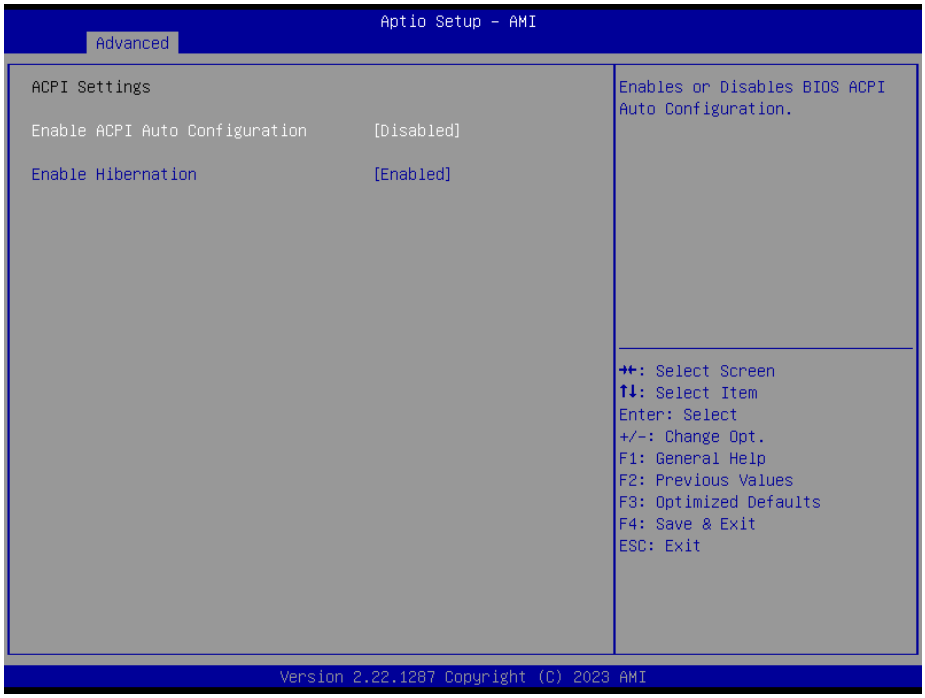
3.6.2.1 Trusted Computing



Item	Options	Description
Security Device Support	Disable, Enable**[Default]**	Enables or Disables BIOS support for security device. O.S. will not show Security Device. TCG EFI protocol and INT1A interface will not be available.

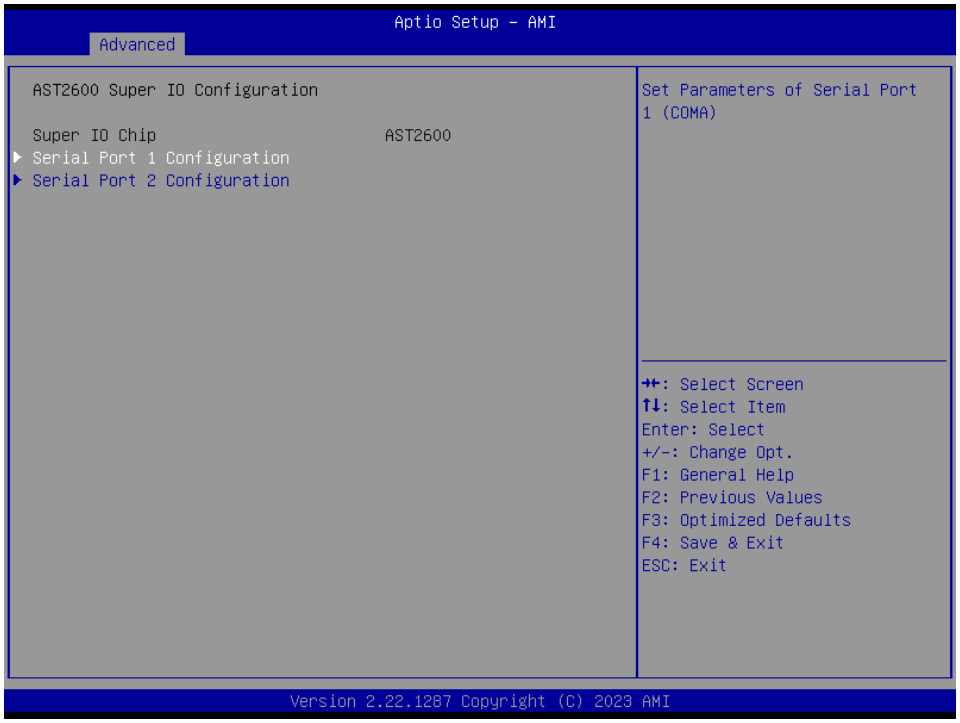
SHA256 PCR Bank	Disabled, Enabled**[Default]**	Enables or Disables SHA256 PCR Bank.
SHA384 PCR Bank	Disabled**[Default]**, Enabled	Enables or Disables SHA384 PCR Bank.
Pending operation	None**[Default]** TPM Clear	Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change State of Security Device.
Physical Presence Spec Version	1.2 1.3**[Default]**	Select to Tell O.S. to support PPI Spec Version 1.2 or1.3 Note some HCK tests might not support 1.3.
Device Select	TPM 2.0**[Default]** Auto	TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices, Auto will support both with default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.

3.6.2.2 ACPI Settings



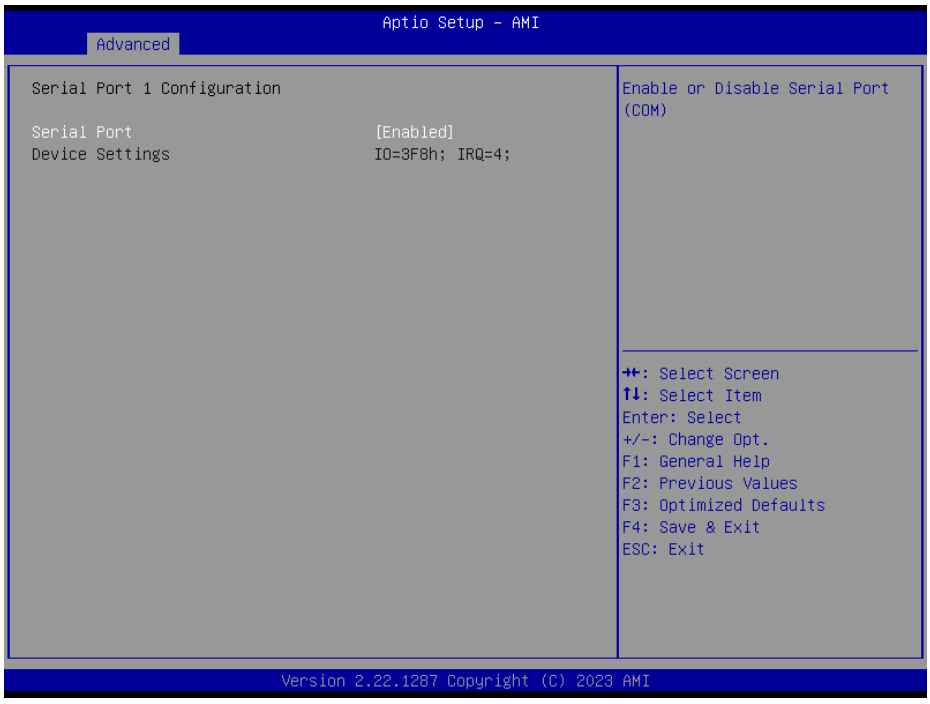
Item	Options	Description
Enable ACPI Auto Configuration	Disabled**[Default]** Enabled	Enables or Disables BIOS ACPI Auto Configuration.
Enable Hibernation	Disabled Enabled**[Default]**	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.

3.6.2.3 AST2600 Super IO Configuration



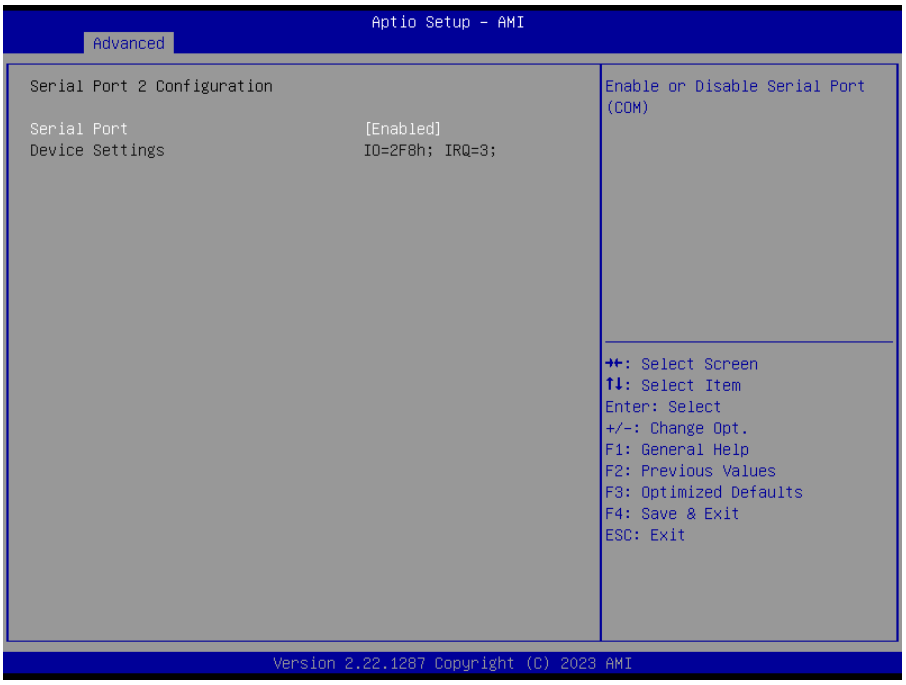
Item	Description
Serial Port 1 Configuration	Set Parameters of Serial Port 1 (COMA).
Serial Port 2 Configuration	Set Parameters of Serial Port 2 (COMB).

3.6.2.3.1 Serial Port 1 Configuration



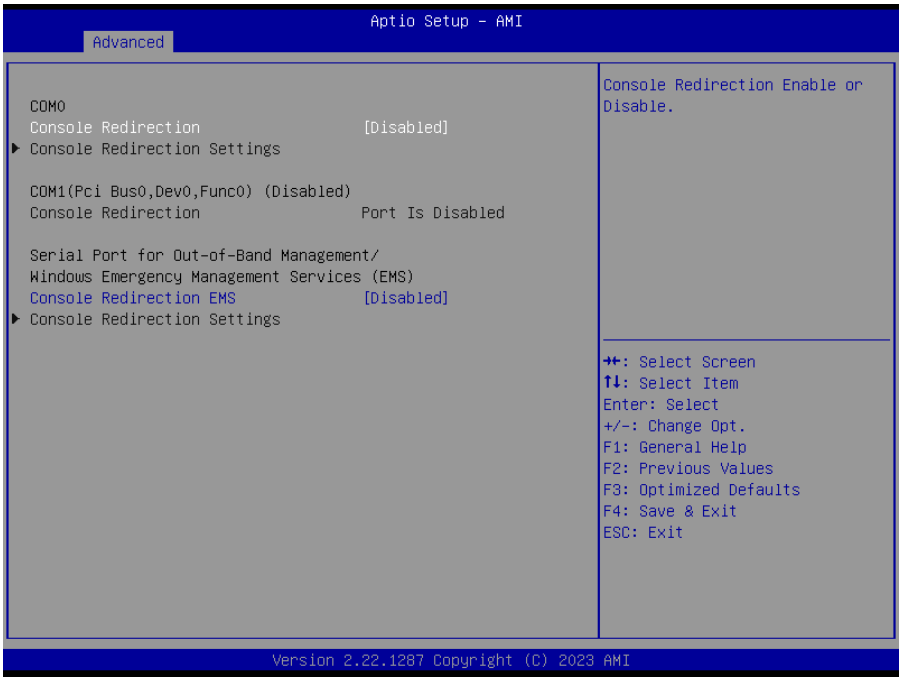
Item	Option	Description
Serial Port	Enabled**[Default]**, Disabled	Enable or Disable Serial Port (COM).

3.6.2.3.2 Serial Port 2 Configuration



Item	Option	Description
Serial Port	Enabled**[Default]**, Disabled	Enable or Disable Serial Port (COM).

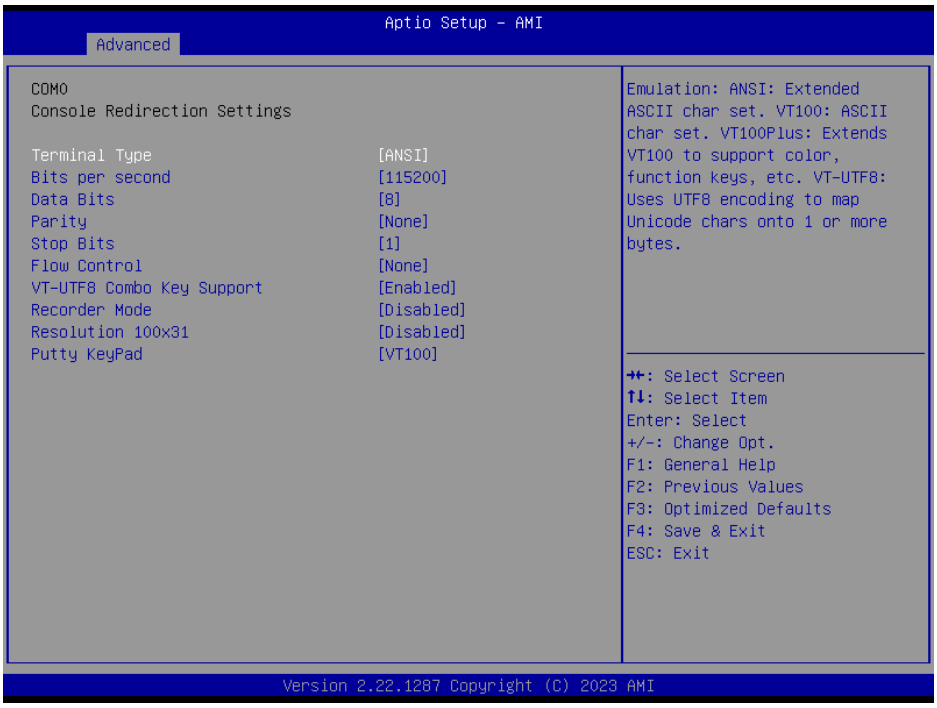
3.6.2.4 Serial Port Console Redirection



Item	Options	Description
Console Redirection	Disabled**[Default]**, Enabled	Console Redirection Enable or Disable.

Console Redirection EMS	Disabled**[Default]**, Enabled	Console Redirection Enable or Disable.

3.6.2.4.1 COM0



Item	Option	Description
Terminal Type	VT100 VT100Plus VT-UTF8 ANSI**[Default]**	Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Bits per second	9600 19200 38400 57600 115200**[Default]**	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Data Bits	7 8**[Default]**	Data Bits.
Parity	None**[Default]** Even Odd Mark Space	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the num of 1's in the data bits is even. Odd: parity bit is 0 if num of 1's in the data bits is odd. Mark: parity bit is always 1. Space: Parity bi is always 0. Mark and Space Parity do not allow for error detection.
Stop Bits	1**[Default]** 2	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stoop bit.
Flow Control	None**[Default]** Hardware RTS/CTS	Flow control can 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 re-start the flow. Hardware flow control uses two wires to send start/stop signals.
VT-UTF8 Combo Key Support	Disabled Enabled**[Default]**,	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
Recorder Mode	Disabled**[Default]**, Enabled	With this mode enabled only text will be sent. This is to capture Terminal data.
Resolution 100x31	Disabled**[Default]**, Enabled	Enables or disables extended terminal resolution.
Putty KeyPad	VT100**[Default]** LINUX XTERMR6 SCO ESCN VT400	Select FunctionKey and KeyPad on Putty.

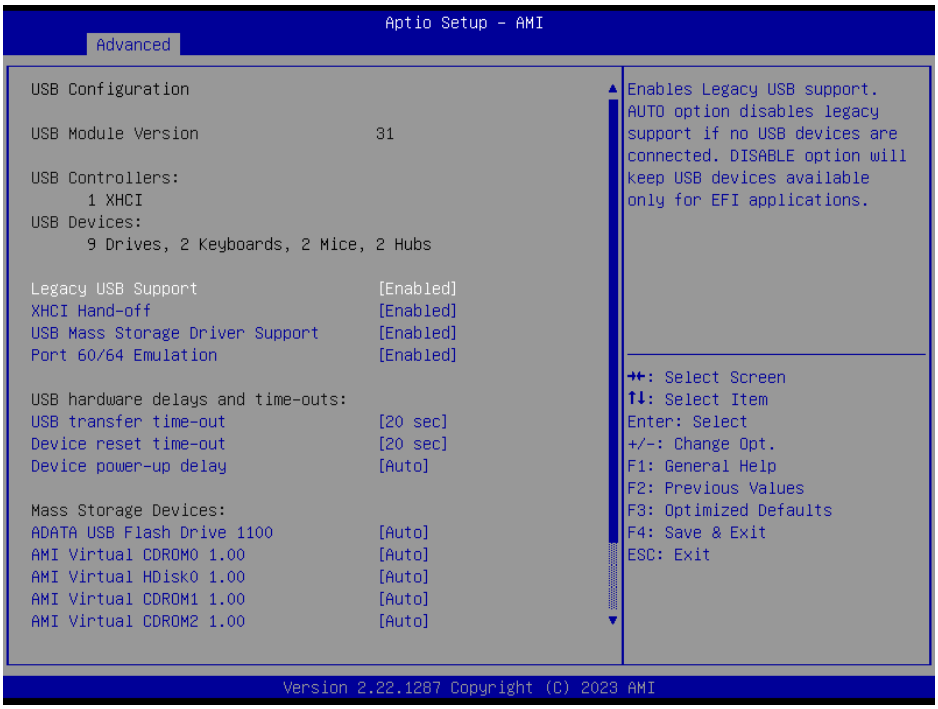
3.6.2.5 Option ROM Dispatch Policy

Item	Options	Description
Restore if Failure	Disabled Enabled**[Default]**,	If system fails to boot and this option is set to 'Enabled', software will reset settings of this page as well as CSM page to its default values automatically.
Primary Video Ignore	Disabled Enabled**[Default]**,	If software will detect that due to the Policy settings. Option ROM of Primary Video Device will not dispatch, it will ignore this device policy settings, and restore it to 'Enable' automatically.
Onboard Mass Storage Controller	Enabled**[Default],**	Onboard Device has:

	Disabled	UEFI [X] Legacy [X] Embedded ROM(s). VIDx8086; DIDxA1D2 @ s0|Bx0 |Dx11 |Fx5
Onboard Display Controller	Enabled**[Default],** Disabled	Onboard Device has: UEFI [X] Legacy [X] Embedded ROM(s). VIDx1A03; DIDx2000 @ s0|BxA |Dx0 |Fx0
Onboard Network Controller	Enabled**[Default],** Disabled	Onboard Device has: UEFI [X] Legacy [X] Embedded ROM(s). VIDx8086; DIDx1533 @ s0|Bx6 |Dx0 |Fx0
Slot#1 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.
Slot#2 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.
Slot#3 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.
Slot#4 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.
Slot#5 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.
Slot#6 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.
Slot#7 Empty	Enabled**[Default],** Disabled	Enable or Disable Option ROM execution for selected Slot.

3.6.2.6 USB Configuration

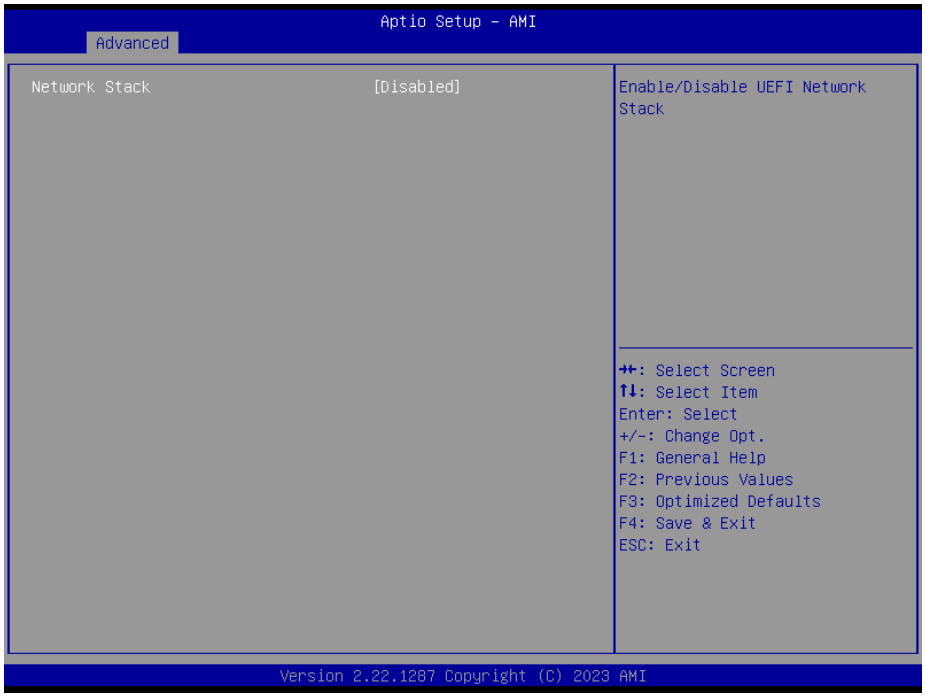
The USB Configuration menu helps read USB information and configures USB settings.



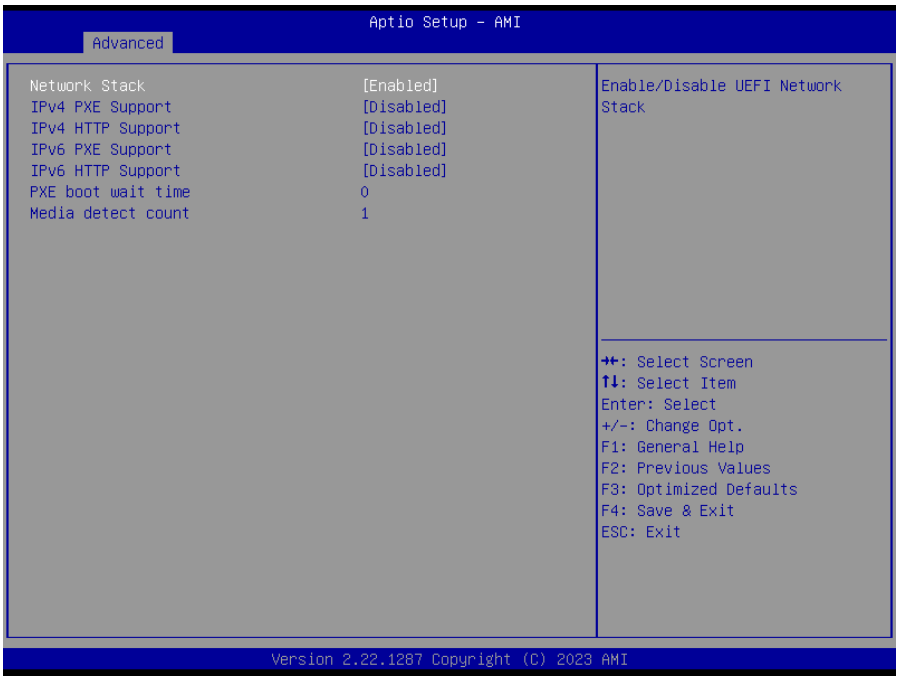
Item	Options	Description
Legacy USB Support	Enabled**[Default]**, Disabled Auto	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications.
XHCI Hand-off	Enabled**[Default]**, Disabled	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Disabled Enabled**[Default]**,	Enable/Disable USB Mass Storage Driver Support.
Port 60/64 Emulation	Disabled Enabled**[Default]**,	Enables I/O port 60h/64h emulation support. This should be enabled for the complete USB keyboard legacy support for non-USB aware OSes.
USB transfer time-out	1 sec 5 sec 10 sec 20 sec**[Default]**	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	10 sec 20 sec**[Default]** 30 sec 40 sec	USB mass storage device Start Unit command time-out.
Device power-up delay	Auto**[Default]** Manual	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.

Mass Storage Devices	Auto**[Default]** Floppy Forced FDD Hard Disk CD-ROM	Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media will be emulated according to a drive type.

3.6.2.7 Network Stack Configuration

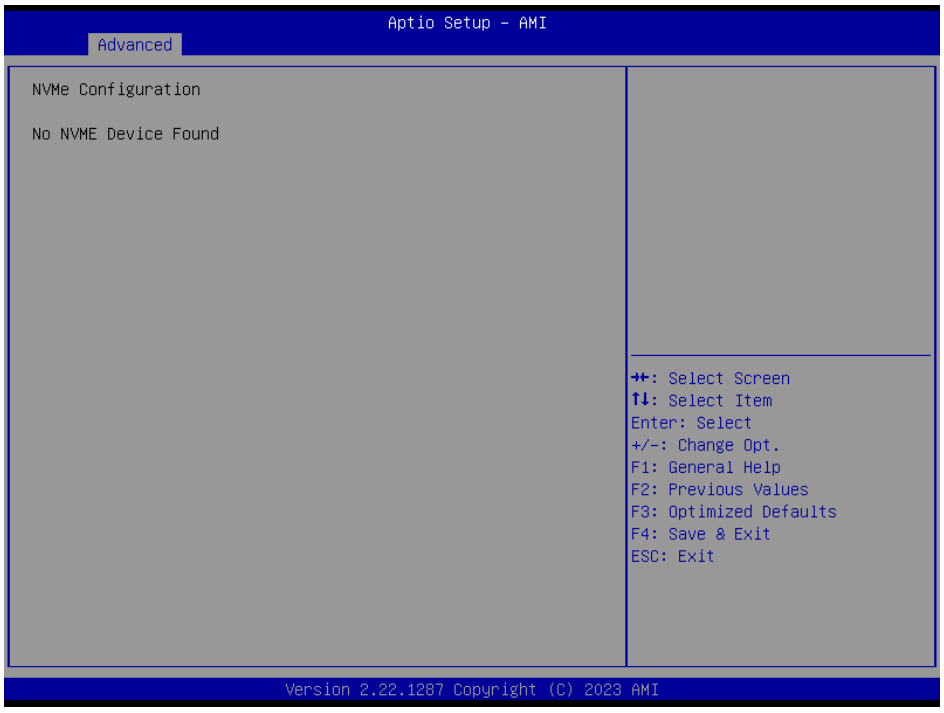


Item	Options	Description
Network Stack	Enabled Disabled**[Default]**	Enable/Disable UEFI Network Stack.

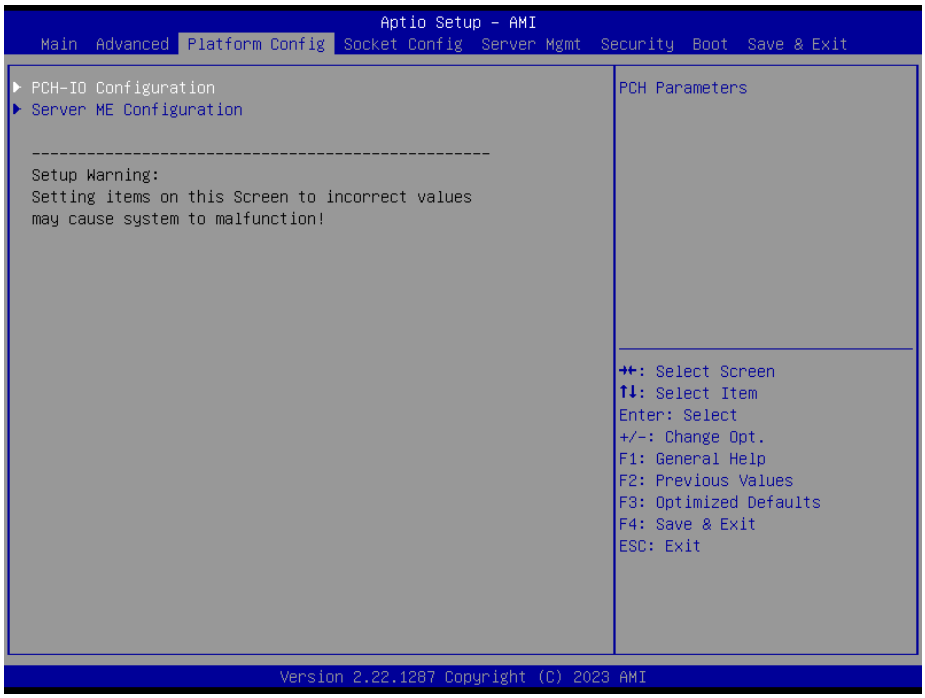


Item	Options	Description
Network Stack	Enabled**[Default]** Disabled	Enable/Disable UEFI Network Stack.
IPv4 PXE Support	Disabled**[Default]** Enabled	Enable/Disable IPv4 PXE boot Support. If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	Disabled**[Default]** Enabled	Enable/Disable IPv4 HTTP boot Support. If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	Disabled**[Default]** Enabled	Enable/Disable IPv6 PXE boot Support. If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	Disabled**[Default]** Enabled	Enable/Disable IPv6 HTTP boot Support. If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	0	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.
Media detect count	1	Number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

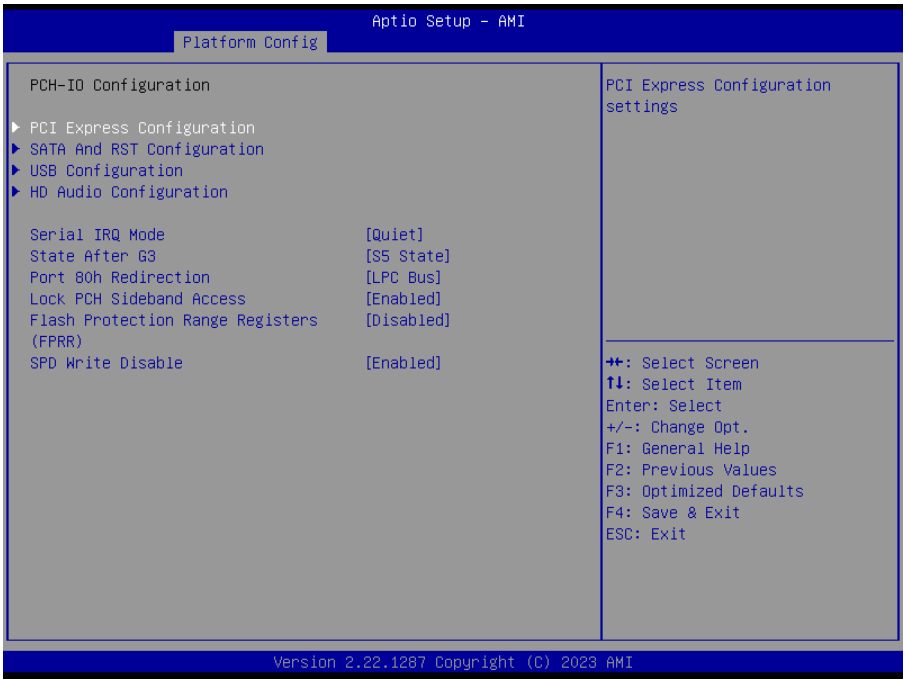
3.6.2.8 NVMe Configuration



3.6.3 Platform Config



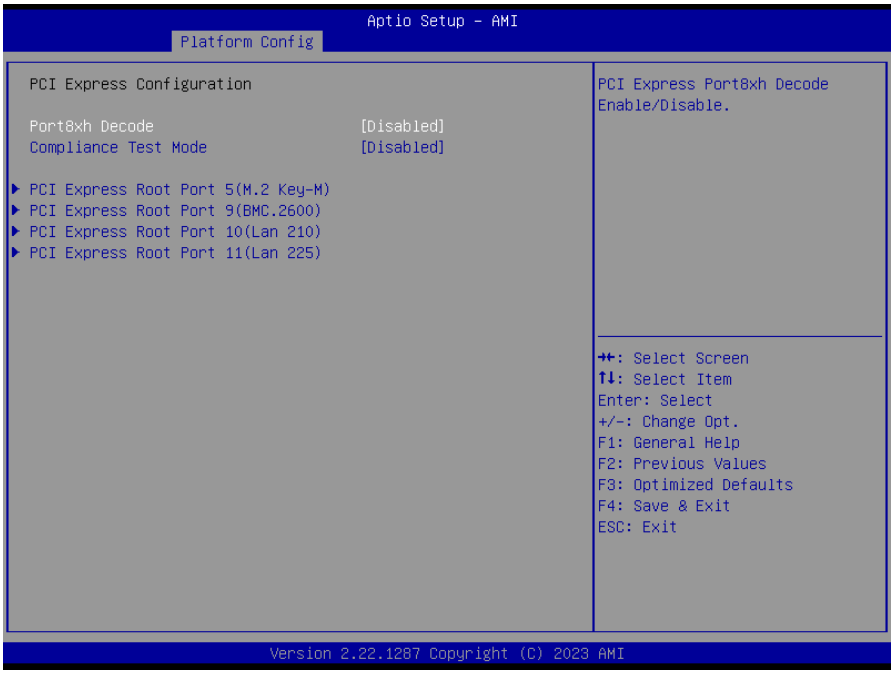
3.6.3.1 PCH-IO Configuration



Item	Option	Description
Serial IRQ Mode	Quiet**[Default]** Continuous	Configure Serieal IRQ Mode.
State After G3	S0 State	Specify what state to go to when power is

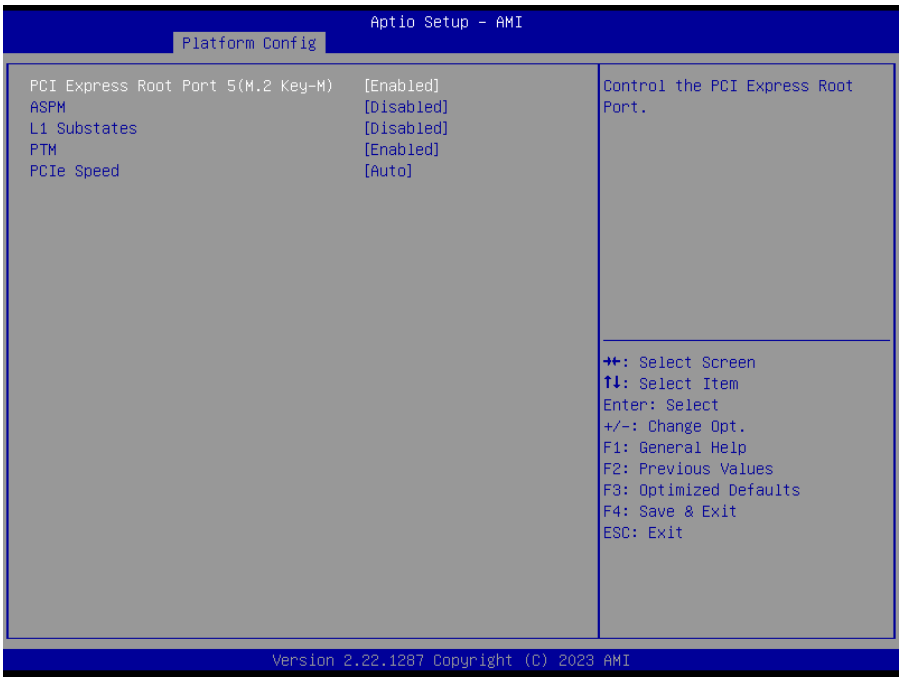
	S5 State**[Default]**	re-applied after a power failure (G3 state).
Port 80h Redirection	LPC Bus**[Default]** PCIE Bus	Control where the Port 80h cycles are sent.
Lock PCH Side band Access	Disabled Enabled**[Default]**	Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POSTBOOT SAI is set.
Flash Protection Range Registers(FRRR)	Disabled**[Default]** Enabled	Enable Flash Protection Range Registers.
SPD Write Disable	Disabled Enabled**[Default]**	Enable/Disable setting SPD Write Disable bit. For sucurity recommendations, SPD write disable bit must be set.

3.6.3.1.1 PCI Express Configuration



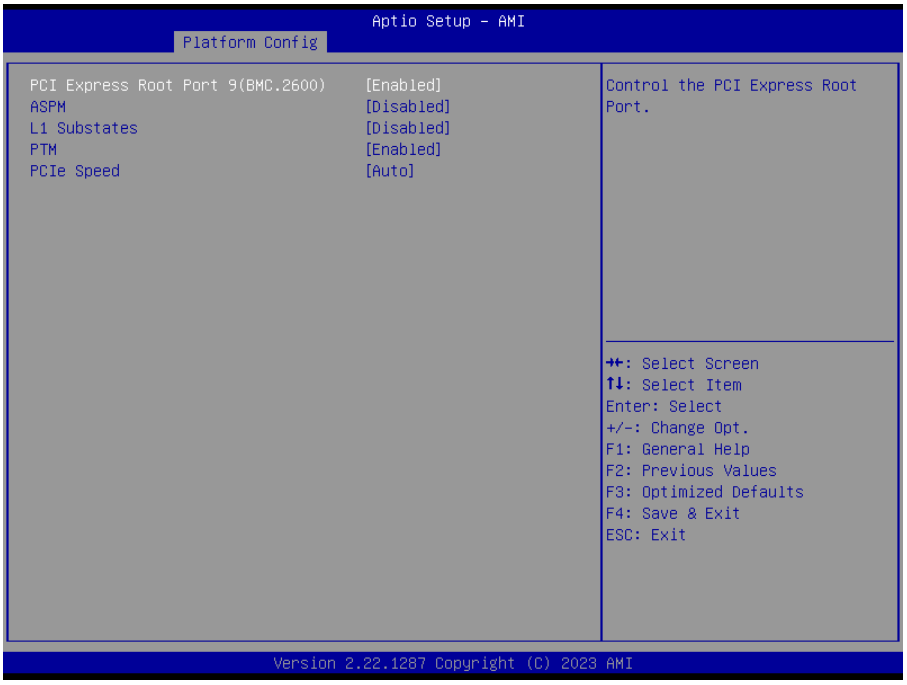
Item	Option	Description
Port8xh Decode	Disabled**[Default]** Enabled	PCI Express Port8xh Decode Enable/Disable.
Compliance Test Mode	Disabled**[Default]** Enabled	Enable when using Compliance Load Board.

3.6.3.1.1.1 PCI Express Root Port 5(M.2 Key-M)



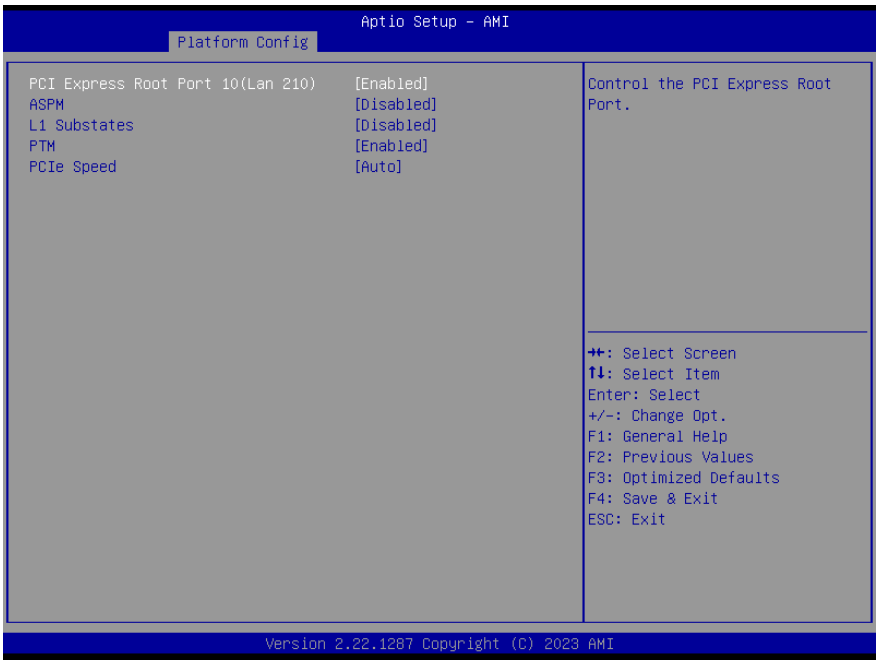
Item	Option	Description
PCI Express Root Port 5(M.2 Key-M)	Enabled**[Default]**, Disabled	Control the PCI Express Root Port.
ASPM	Disabled**[Default]**, L1	PCI Express Active State Power Management settings.
L1 Substates	Disabled**[Default]** L1.1 L1.2 L1.1 & L1.2	PCI Express L1 Substates settings.
PTM	Enabled**[Default]**, Disabled	Enable/Disable Precision Time Measurement.
PCIe Speed	Auto**[Default]** Gen1 Gen2 Gen3	Configure PCIe Speed.

3.6.3.1.1.2 PCI Express Root Port 9(BMC.2600)



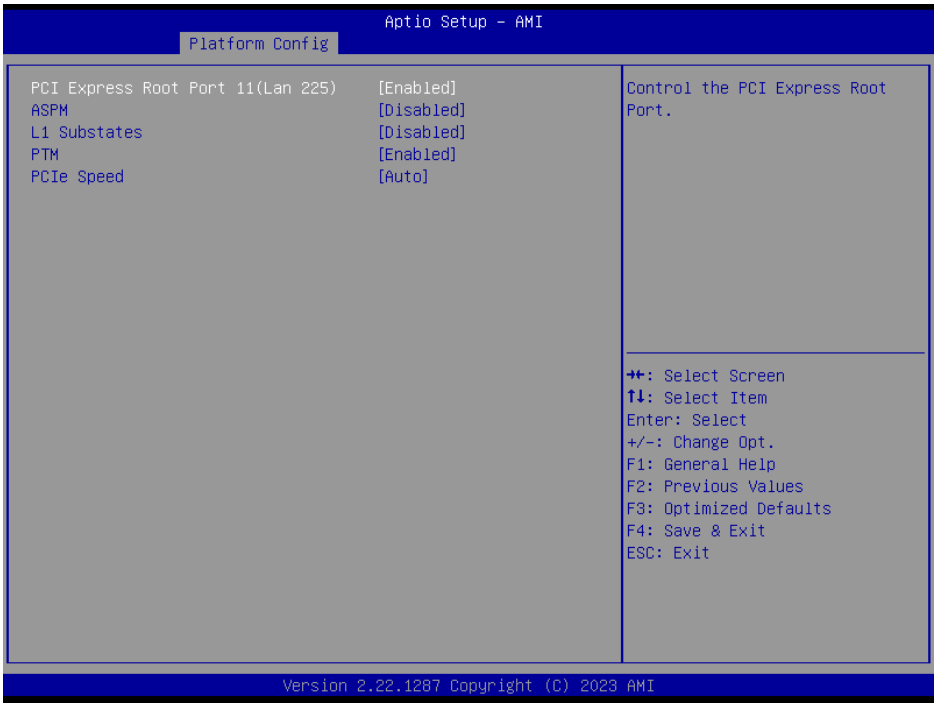
Item	Option	Description
PCI Express Root Port 9(BMC. 2600)	Enabled**[Default]**, Disabled	Control the PCI Express Root Port.
ASPM	Disabled**[Default]**, L1	PCI Express Active State Power Management settings.
L1 Substates	Disabled**[Default]** L1.1 L1.2 L1.1 & L1.2	PCI Express L1 Substates settings.
PTM	Enabled**[Default]**, Disabled	Enable/Disable Precision Time Measurement.
PCIe Speed	Auto**[Default]** Gen1 Gen2 Gen3	Configure PCIe Speed.

3.6.3.1.1.3 PCI Express Root Port 10(LAN 210)



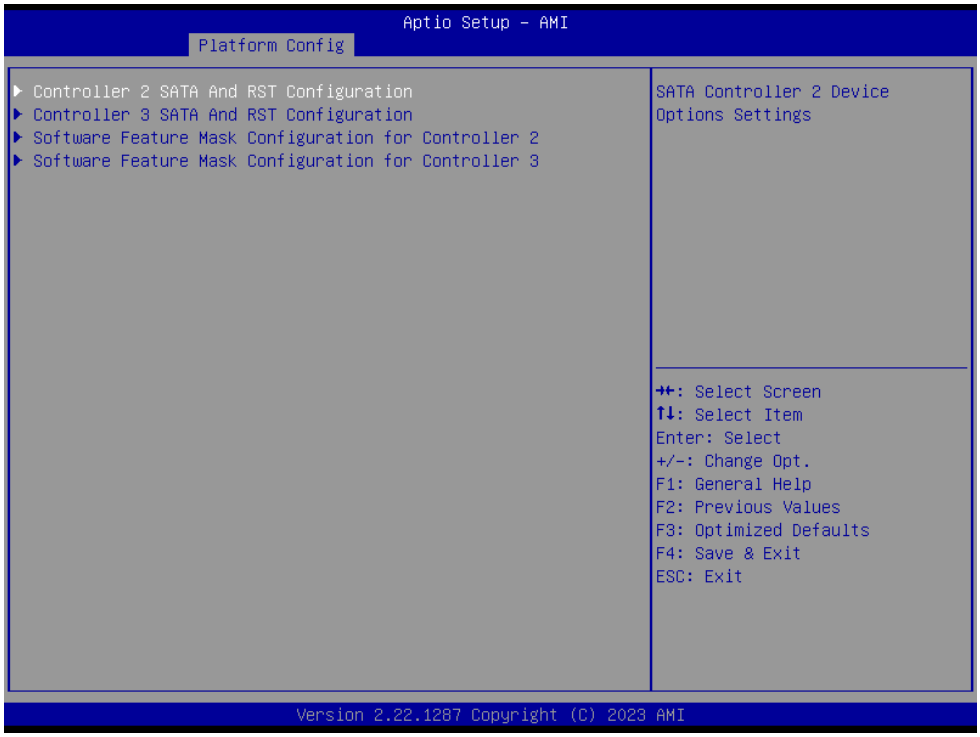
Item	Option	Description
PCI Express Root Port 10(LAN 210)	Enabled**[Default]**, Disabled	Control the PCI Express Root Port.
ASPM	Disabled**[Default]**, L1	PCI Express Active State Power Management settings.
L1 Substates	Disabled**[Default]** L1.1 L1.2 L1.1 & L1.2	PCI Express L1 Substates settings.
PTM	Enabled**[Default]**, Disabled	Enable/Disable Precision Time Measurement.
PCIe Speed	Auto**[Default]** Gen1 Gen2 Gen3	Configure PCIe Speed.

3.6.3.1.1.4 PCI Express Root Port 11(LAN 225)

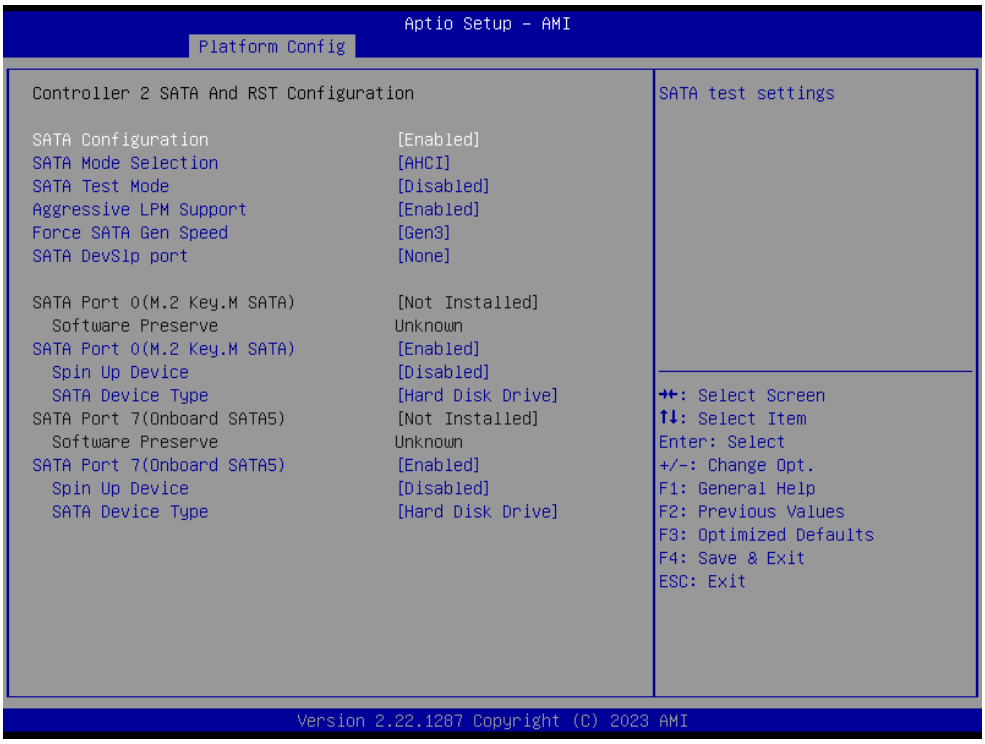


Item	Option	Description
PCI Express Root Port 11(LAN 225)	Enabled**[Default]**, Disabled	Control the PCI Express Root Port.
ASPM	Disabled**[Default]**, L1	PCI Express Active State Power Management settings.
L1 Substates	Disabled**[Default]** L1.1 L1.2 L1.1 & L1.2	PCI Express L1 Substates settings.
PTM	Enabled**[Default]**, Disabled	Enable/Disable Precision Time Measurement.
PCIe Speed	Auto**[Default]** Gen1 Gen2 Gen3	Configure PCIe Speed.

3.6.3.1.2 SATA And RST Configuration



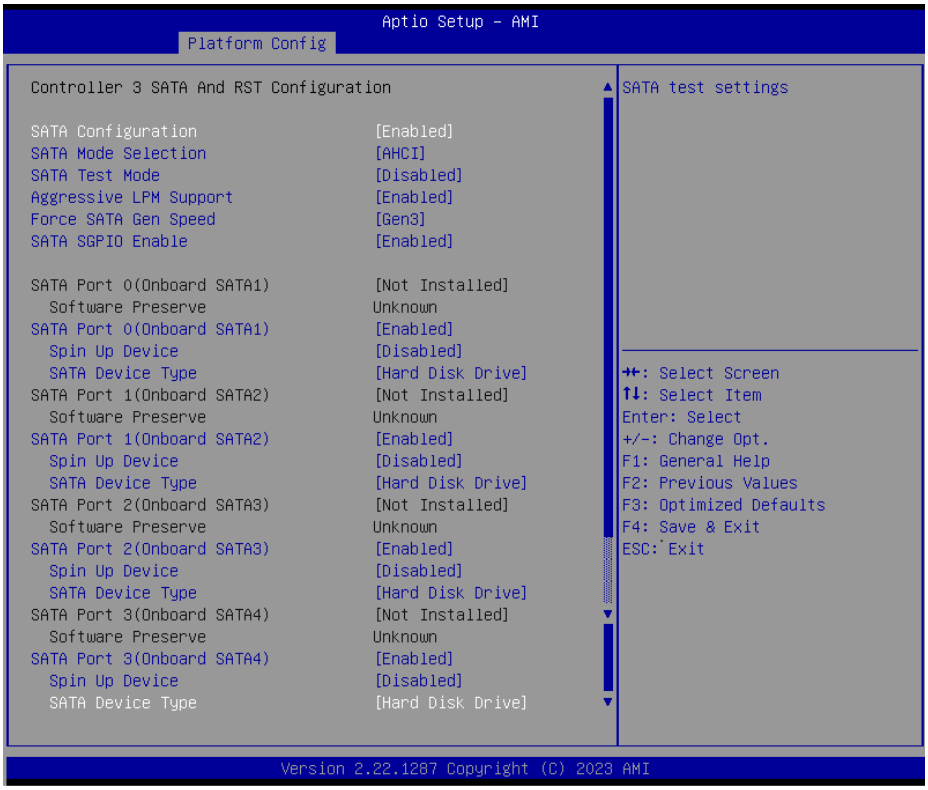
3.6.3.1.2.1 Controller 2 SATA And RST Configuration



Item	Options	Description
SATA Configuration	Enabled**[Default]** Disabled,	SATA test settings.

SATA Mode Selection	AHCI**[Default]**, RAID	Determines how SATA controller(s) operate.
SATA Test Mode	Enabled Disabled**[Default]**	Test Mode Enable/Disable (Loop Back).
Aggressive LPM Support	Enabled Disabled**[Default]**	Enable PCH to aggressively enter link power state.
Force SATA Gen Speed	Gen1 Gen2 Gen3**[Default]**	Changes SATA Gen Speed for port.
SATA DevSlp port	None**[Default]** Port0 Port1 Port2 Port3 Port4 Port5 Port6 Port7	Enable SATA DevSlp feature for port. It is possible to enable DevSlp for only one port or none.
SATA Port 0(M.2 Key.M SATA)	Disabled Enabled**[Default]**	Enable or Disable SATA Port.
Spin Up Device	Disabled**[Default]** Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive**[Default]** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
SATA Port 7(Onboard SATA5)	Disabled Enabled**[Default]**	Enable or Disable SATA Port.
Spin Up Device	Disabled**[Default]** Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive**[Default]** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

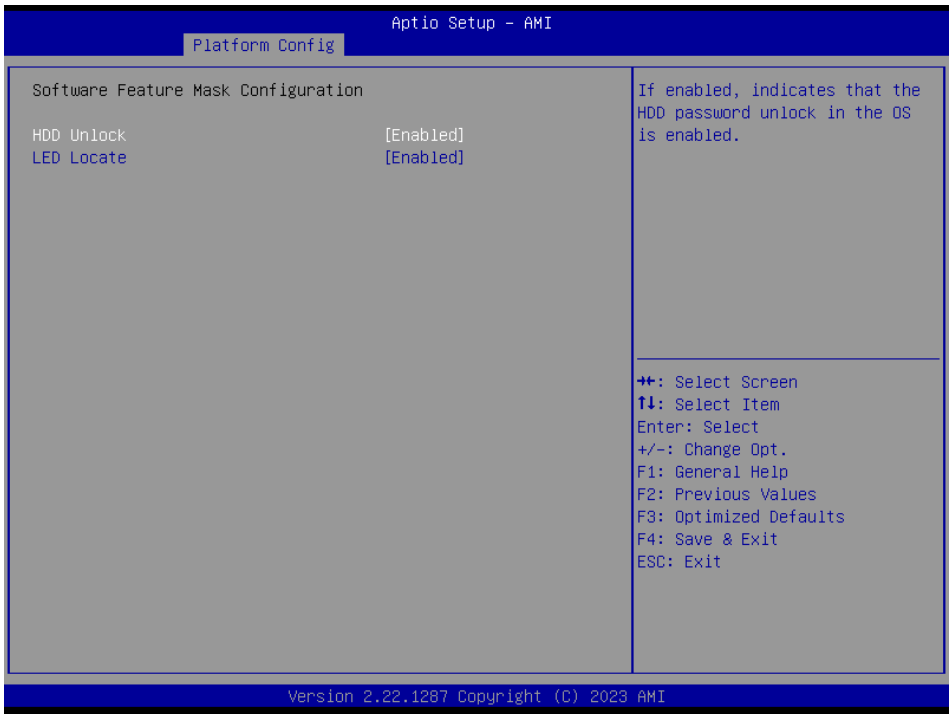
3.6.3.1.2.2 Controller 3 SATA And RST Configuration



Item	Options	Description
SATA Configuration	Enabled**[Default]** Disabled,	SATA test settings.
SATA Mode Selection	AHCI**[Default]**, RAID	Determines how SATA controller(s) operate.
SATA Test Mode	Enabled Disabled**[Default]**	Test Mode Enable/Disable (Loop Back).
Aggressive LPM Support	Enabled Disabled**[Default]**	Enable PCH to aggressively enter link power state.
Force SATA Gen Speed	Gen1 Gen2 Gen3**[Default]**	Changes SATA Gen Speed for port.
SATA DevSlp port	None**[Default]** Port0 Port1 Port2 Port3 Port4 Port5 Port6 Port7	Enable SATA DevSlp feature for port. It is possible to enable DevSlp for only one port or none.
SATA Port 0(Onboard SATA1)	Disabled Enabled**[Default]**	Enable or Disable SATA Port.

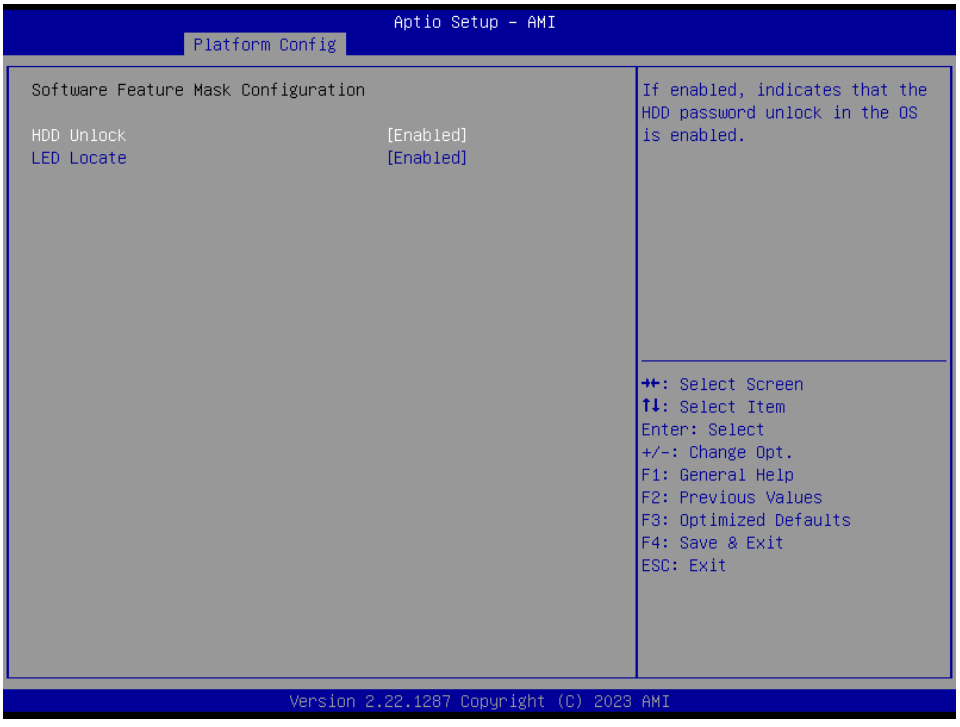
Spin Up Device	Disabled**[Default]** Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive**[Default]** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
SATA Port 1(Onboard SATA2)	Disabled Enabled**[Default]**	Enable or Disable SATA Port.
Spin Up Device	Disabled**[Default]** Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive**[Default]** Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
SATA Port 2(Onboard SATA3)	Disabled Enabled[Default]	Enable or Disable SATA Port.
Spin Up Device	Disabled[Default] Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive[Default] Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.
SATA Port 3(Onboard SATA4)	Disabled Enabled[Default]	Enable or Disable SATA Port.
Spin Up Device	Disabled[Default] Enabled	If enabled for any of ports Staggerred Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.
SATA Device Type	Hard Disk Drive[Default] Solid State Drive	Identify the SATA port is connected to Solid State Drive or Hard Disk Drive.

3.6.3.1.2.3 Software Feature Mask Configuration for Controller 2



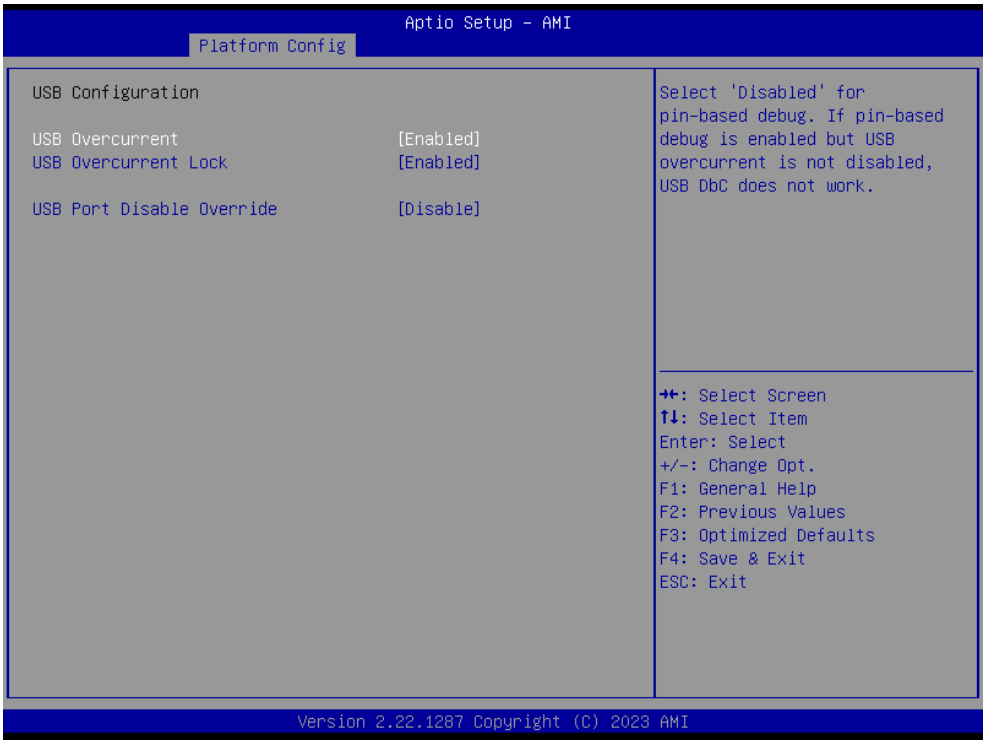
Item	Options	Description
HDD Unlock	Disabled, Enabled**[Default]**	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	Disabled, Enabled**[Default]**	If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

3.6.3.1.2.4 Software Feature Mask Configuration for Controller 3



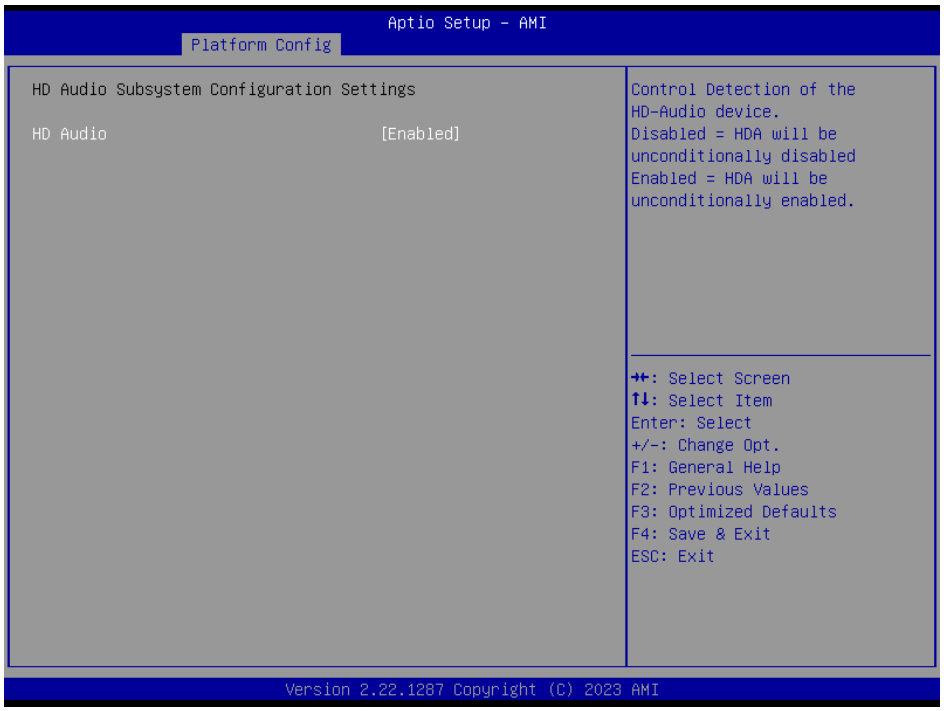
Item	Options	Description
HDD Unlock	Disabled, Enabled**[Default]**	If enabled, indicates that the HDD password unlock in the OS is enabled.
LED Locate	Disabled, Enabled**[Default]**	If enabled, indicates that the LED/SGPIO hardware is attached and ping to locate feature is enabled on the OS.

3.6.3.1.3 USB Configuration



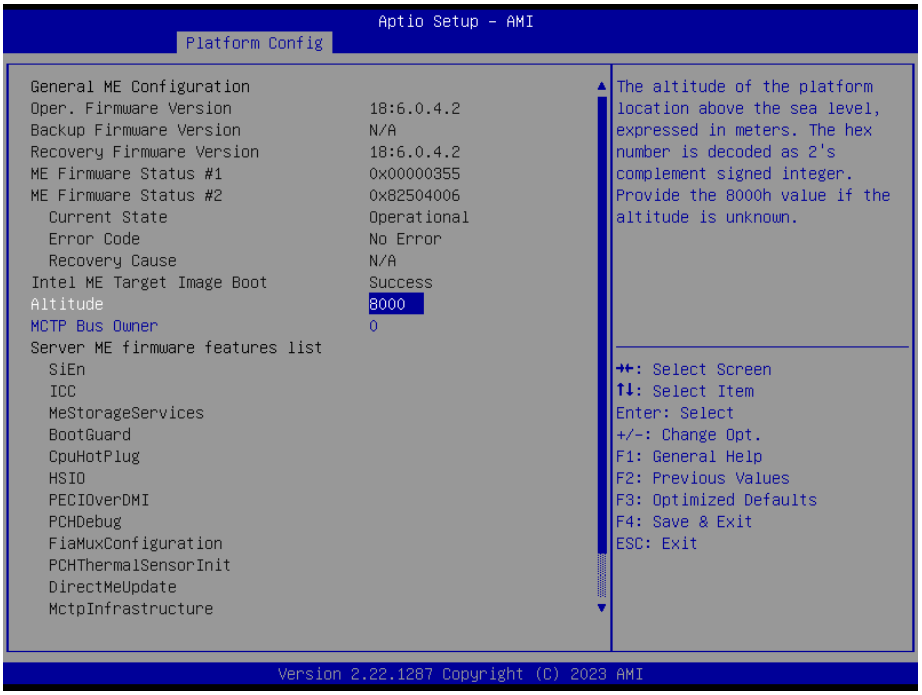
Item	Options	Description
USB Overcurrent	Disabled, Enabled**[Default]**	Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
USB Overcurrent Lock	Disabled, Enabled**[Default]**	Select 'Enabled'. If Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.
USB Port Disable Override	Disabled**[Default]** Select Per-Pin	Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

3.6.3.1.4 HD Audio Configuration



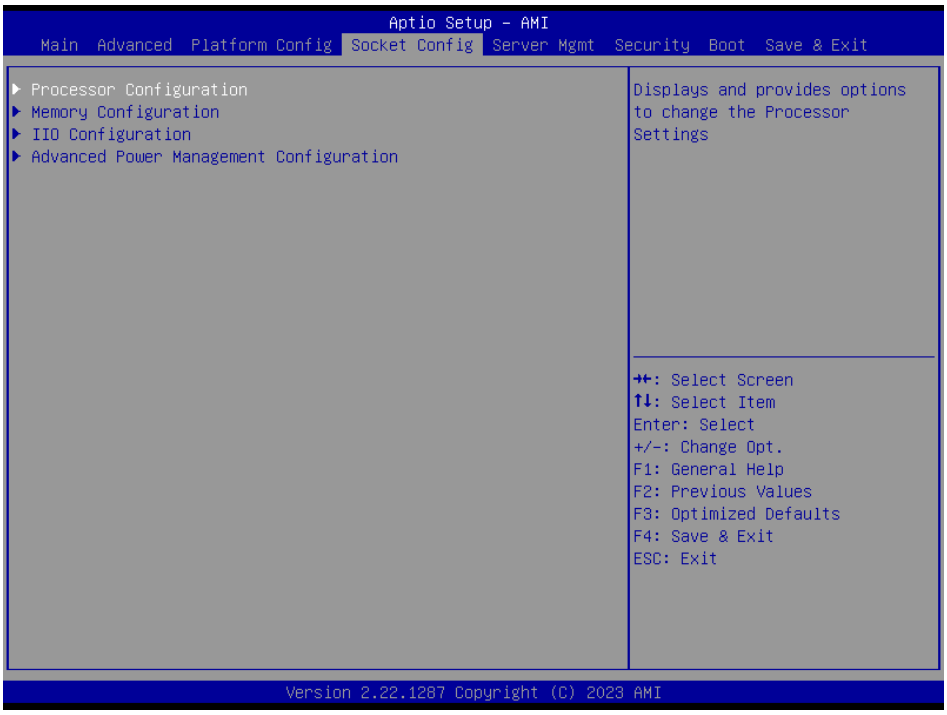
Item	Options	Description
HD Audio	Disabled, Enabled**[Default]**	Control Detection of the HD-Audio device. Disabled=HDA will be unconditionally disabled Enabled=HDA will be unconditionally enabled.

3.6.3.2 Server ME Configuration

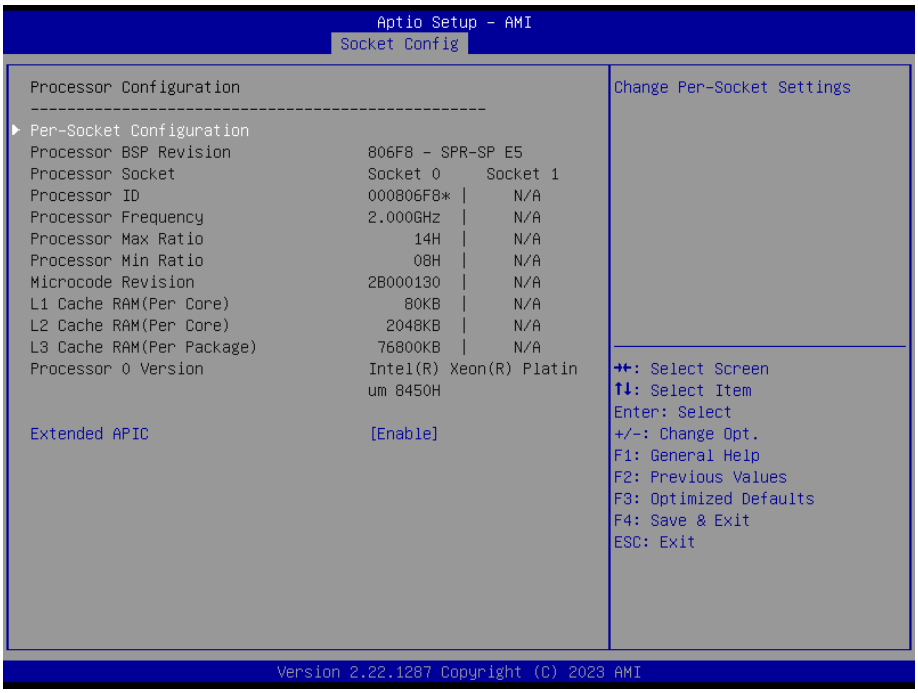


Item	Option	Description
Altitude	8000	The altitude of the platform location above the sea level, expressed in meters. The hex number is decoded as 2's complement signed integer. Provide the 8000h value if the altitude is unknown.
MCTP Bus Owner	0	MCTP bus owner location on PCIe: [15:8] bus, [7:3] device, [2:0] function. If all zeros sending bus owner is disabled.

3.6.4 Socket Config

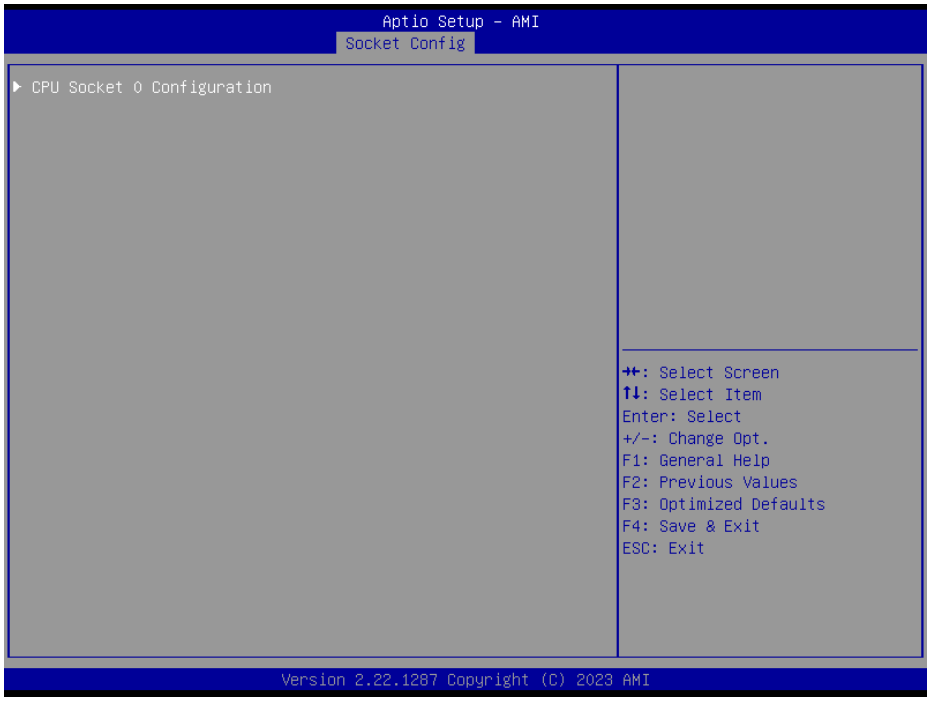


3.6.4.1 Processor Configuration

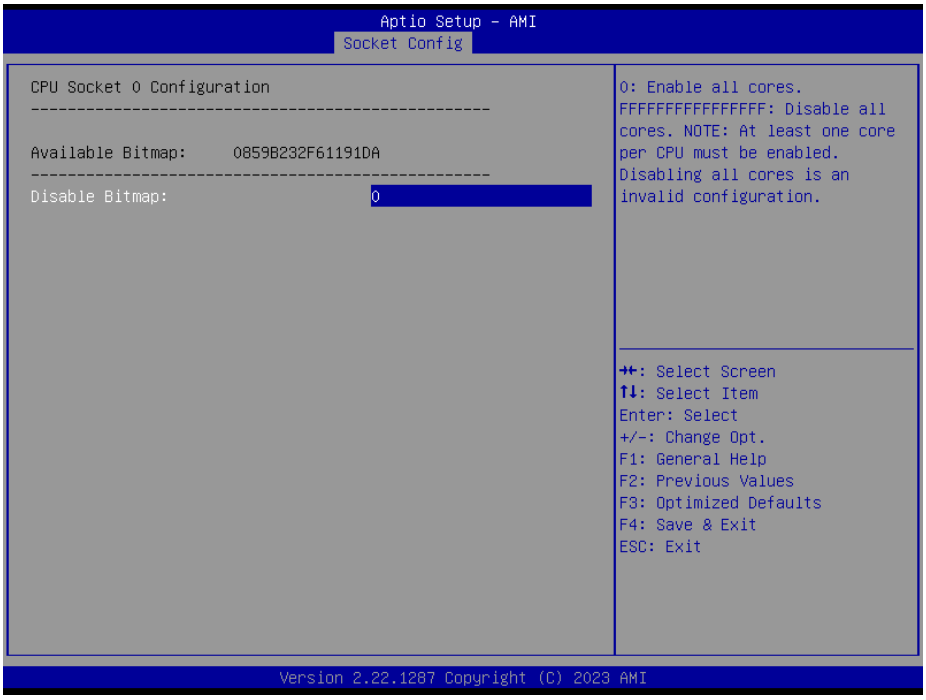


Item	Option	Description
Extended APIC	Disable Enable**[Default]**	Enable/disable extended APIC support. Note: When enabled, VT-d_Interrupt Remapping will be automatically enabled.

3.6.4.1.1 Per-Socket Configuration

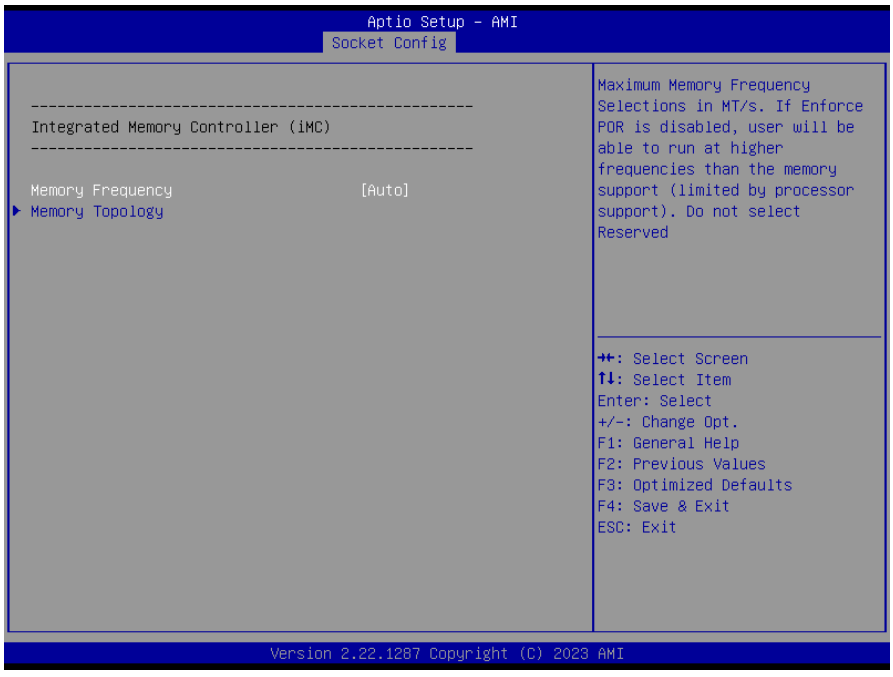


3.6.4.1.1.1 CPU Socket 0 Configuration



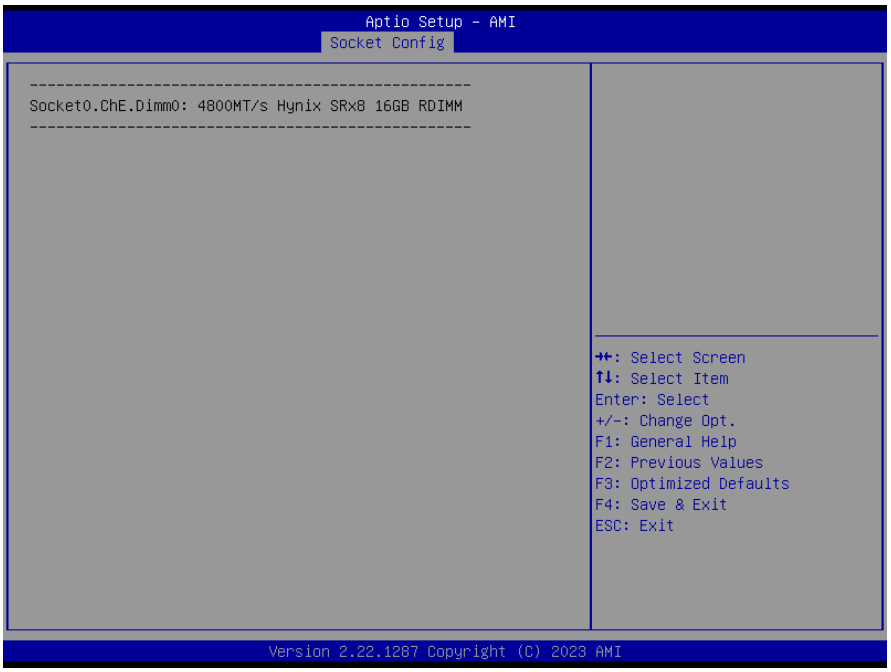
Item	Option	Description
Disable Bitmap:	0	0: Enable all cores. FFFFFFFFFFFFFFF: Disable all cores. NOTE: AT least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

3.6.4.2 Memory Configuration

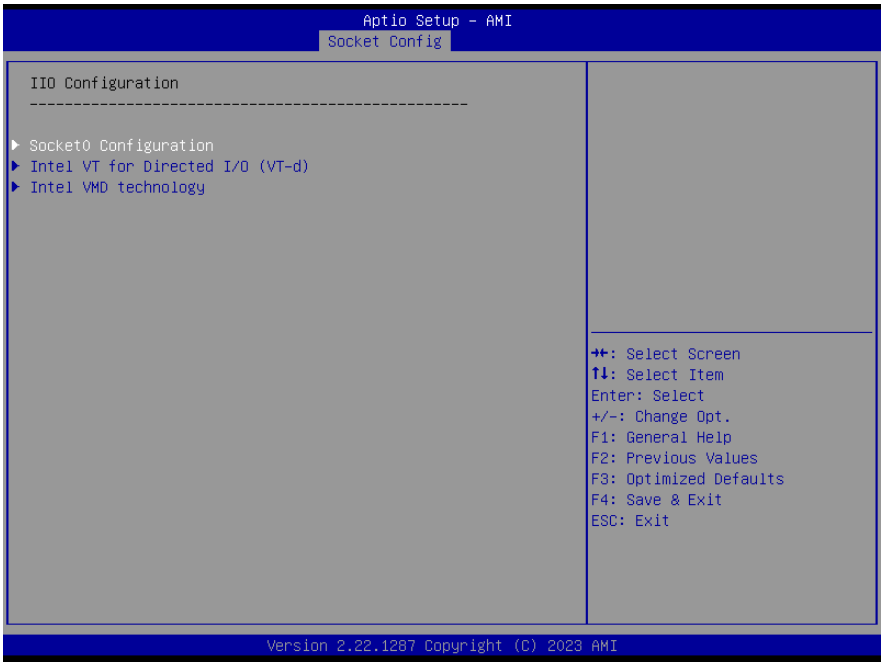


Item	Option	Description
Memory Frequency	Auto**[Default]** 3200 3600 4000 4400 4800 5200 5600	Maximum Memory Frequency Selections in MT/s. If Enforce POR is disabled, user will be able to run at higher frequencies than the memory suppot (limited by processor support). Do not select Reserved.

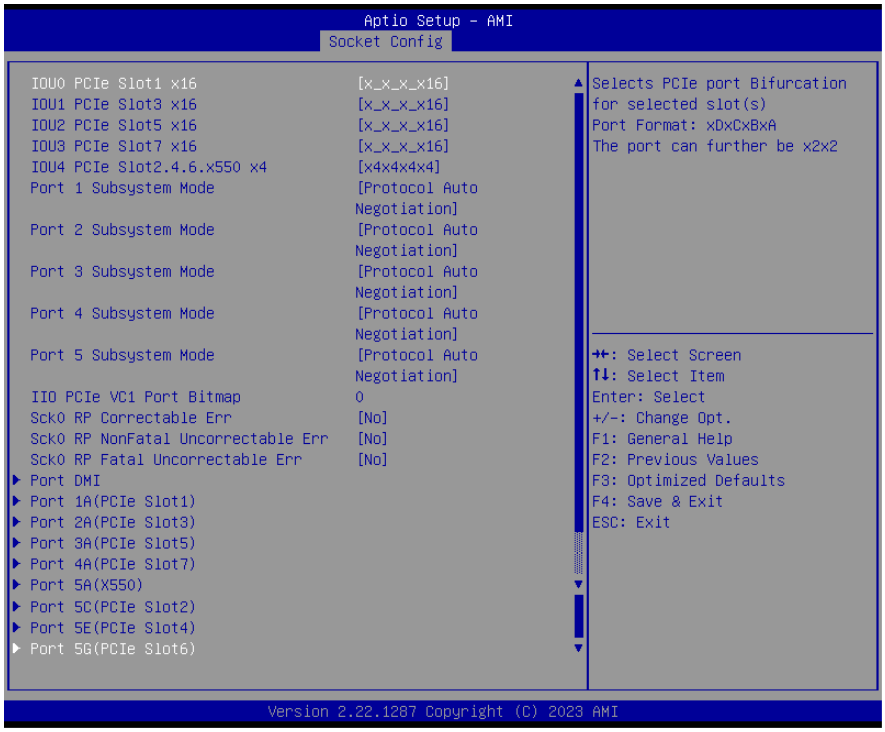
3.6.4.2.1 Memory Topology



3.6.4.3 IIO Configuration



3.6.4.3.1 Socket0 Configuration



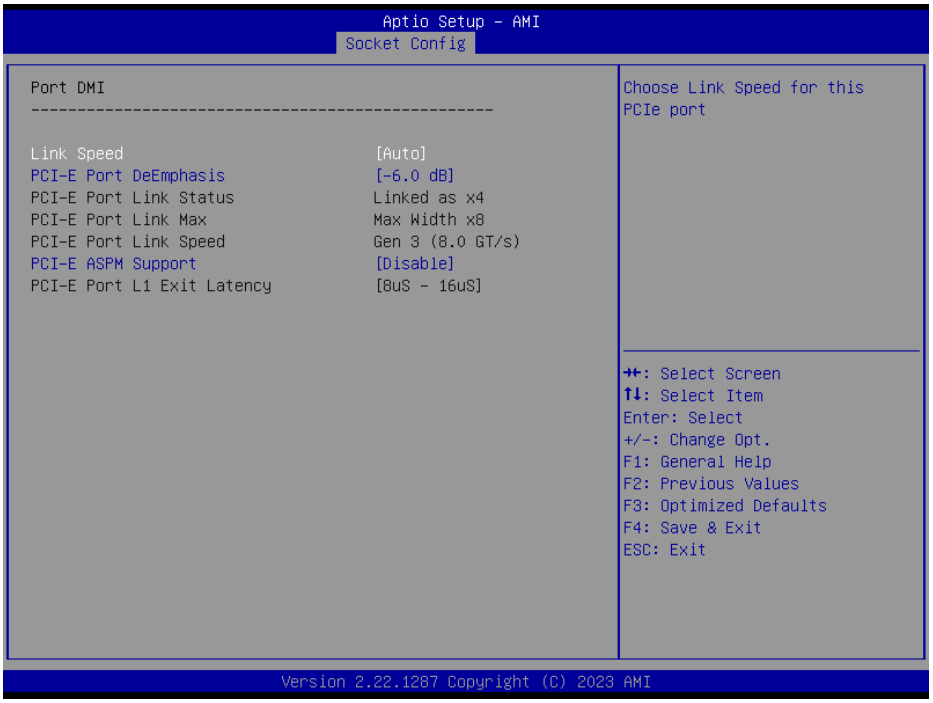
Item	Options	Description
IOU0 PCIe Slot1 x16	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16**[Default]** x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2 x2x2x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xDxCxBxA The port can further be x2x2.
IOU1 PCIe Slot3 x16	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8	Selects PCIe port Bifurcation for selected slot(s) Port Format: xDxCxBxA The port can further be x2x2.

	x_x_x_x16**[Default]** x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2 x2x2x2x2x2x2x2x2	
IOU2 PCIe Slot5 x16	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16**[Default]** x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2 x2x2x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xDxCxBxA The port can further be x2x2.
IOU3 PCIe Slot7 x16	Auto x4x4x4x4 x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16**[Default]** x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4	Selects PCIe port Bifurcation for selected slot(s) Port Format: xDxCxBxA The port can further be x2x2.

	x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2 x2x2x2x2x2x2x2x2	
IOU4 PCIe Slot2.4.6x550 x4	Auto x4x4x4x4**[Default]** x4x4x_x8 x_x8x4x4 x_x8x_x8 x_x_x_x16 x2x2x4x_x8 x4x2x2x_x8 x_x8x2x2x4 x2x2x4x4x4 x4x2x2x4x4 x4x4x2x2x4 x2x2x2x2x_x8 x2x2x2x2x4x4 x2x2x4x2x2x4 x4x2x2x2x2x4 x2x2x2x2x2x2x4 x_x8x4x2x2 x4x4x4x2x2 x_x8x2x2x2x2 x2x2x4x4x2x2 x4x2x2x4x2x2 x4x4x2x2x2x2 x2x2x2x2x4x2x2 x2x2x4x2x2x2x2 x4x2x2x2x2x2x2 x2x2x2x2x2x2x2x2	Selects PCIe port Bifurcation for selected slot(s) Port Format: xDxCxBxA The port can further be x2x2.
Port 1 Subsystem Mode	Gen5 Protocol Auto Negotiation**[Default]**	Select PCIe Subsystem Mode for selected slot(s) Gen4: Gen4 controller only Gen5: Gen5 with or without mix mode Auto: Auto select Force CXL: There is no training discovery, the attached device must also supports this mode.
Port 2 Subsystem Mode	Gen5 Protocol Auto Negotiation**[Default]**	Select PCIe Subsystem Mode for selected slot(s) Gen4: Gen4 controller only Gen5: Gen5 with or without mix mode Auto: Auto select Force CXL: There is no training discovery, the attached

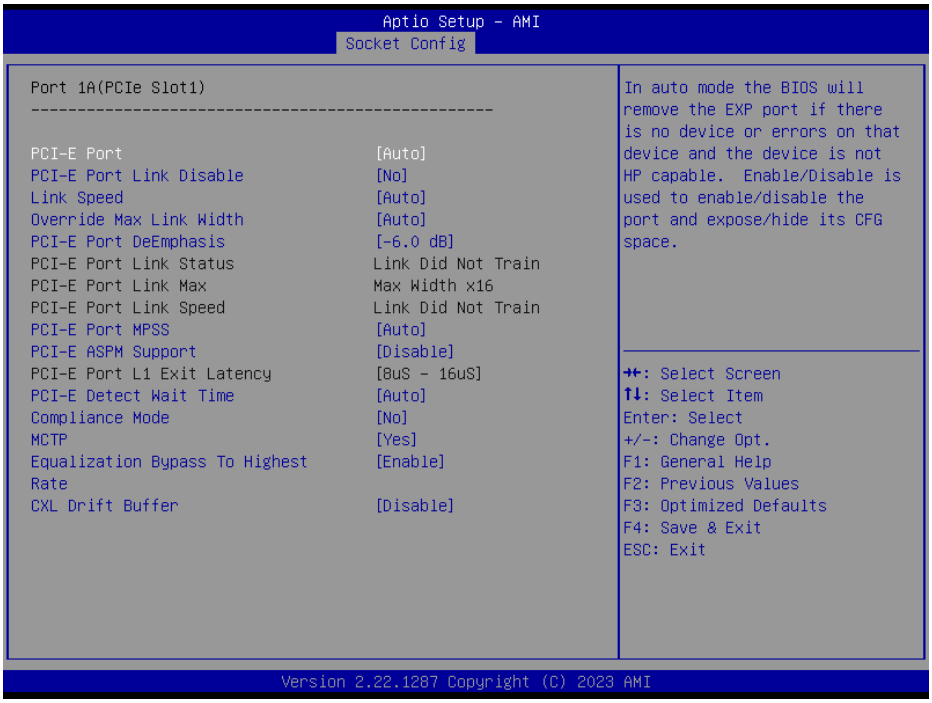
		device must also supports this mode.
Port 3 Subsystem Mode	Gen5 Protocol Auto Negotiation**[Default]**	Select PCIe Subsystem Mode for selected slot(s) Gen4: Gen4 controller only Gen5: Gen5 with or without mix mode Auto: Auto select Force CXL: There is no training discovery, the attached device must also supports this mode.
Port 4 Subsystem Mode	Gen5 Protocol Auto Negotiation**[Default]**	Select PCIe Subsystem Mode for selected slot(s) Gen4: Gen4 controller only Gen5: Gen5 with or without mix mode Auto: Auto select Force CXL: There is no training discovery, the attached device must also supports this mode.
Port 5 Subsystem Mode	Gen5 Protocol Auto Negotiation**[Default]**	Select PCIe Subsystem Mode for selected slot(s) Gen4: Gen4 controller only Gen5: Gen5 with or without mix mode Auto: Auto select Force CXL: There is no training discovery, the attached device must also supports this mode.
IIO PCIe VC1 Port Bitmap	0	Enable/Disable PCIe Port VC1 support. Port 0 is allocated to DMI or DMI as PCIe. Port 0 bit will have no effect in DMI mode. 0-VC1 support disabled. 1-VC1 support enabled. Example: bit 0= IIO PCIe Port 0…bit n = IIO PCIe Portn.
Sck0 RP Correctable Err	No**[Default]** Yes	Applies to root ports only. Enabled interrupt on correctable errors.
Sck0 RP NonFatal Uncorrectable Err	No**[Default]** Yes	Applies to root ports only. Enabled interrupt on a non-fatal error.
Sck0 RP Fatal Uncorrectable Err	No**[Default]** Yes	Applies to root ports only. Enabled MSI/INTx interrupt on fatal errors.

3.6.4.3.1.1 Port DMI



Item	Option	Description
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.

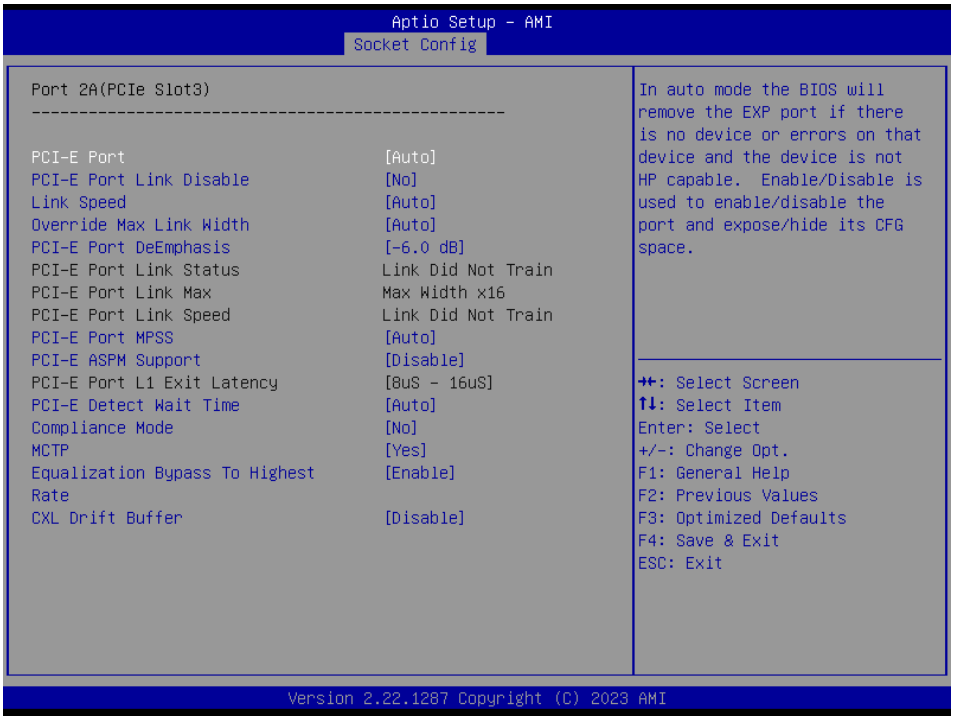
3.6.4.3.1.2 Port 1A(PCIe Slot1)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation.
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.

PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

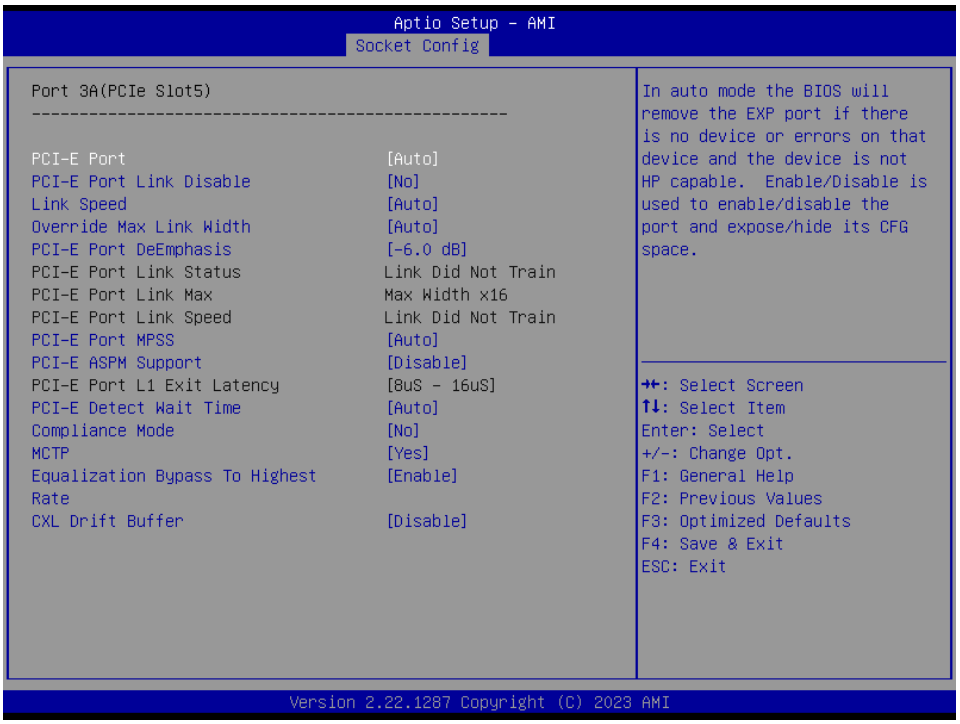
3.6.4.3.1.3 Port 2A(PCIe Slot3)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2	Override the max link width that was set by bifurcation.

	x4 x8 x16	
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.
PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

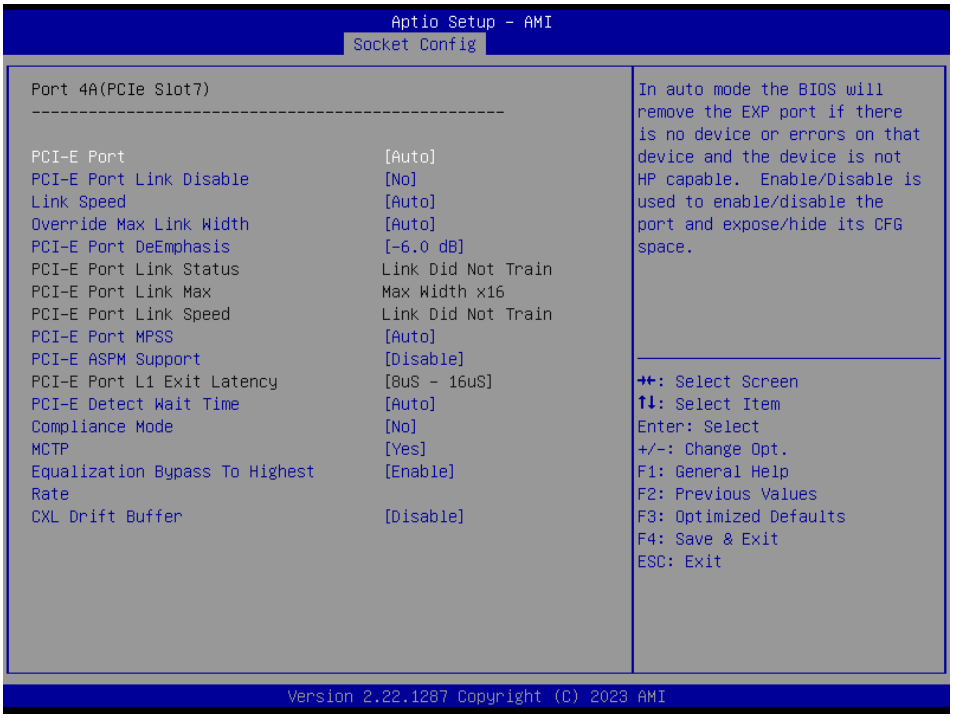
3.6.4.3.1.4 Port 3A(PCIe Slot5)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.

PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation.
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.
PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

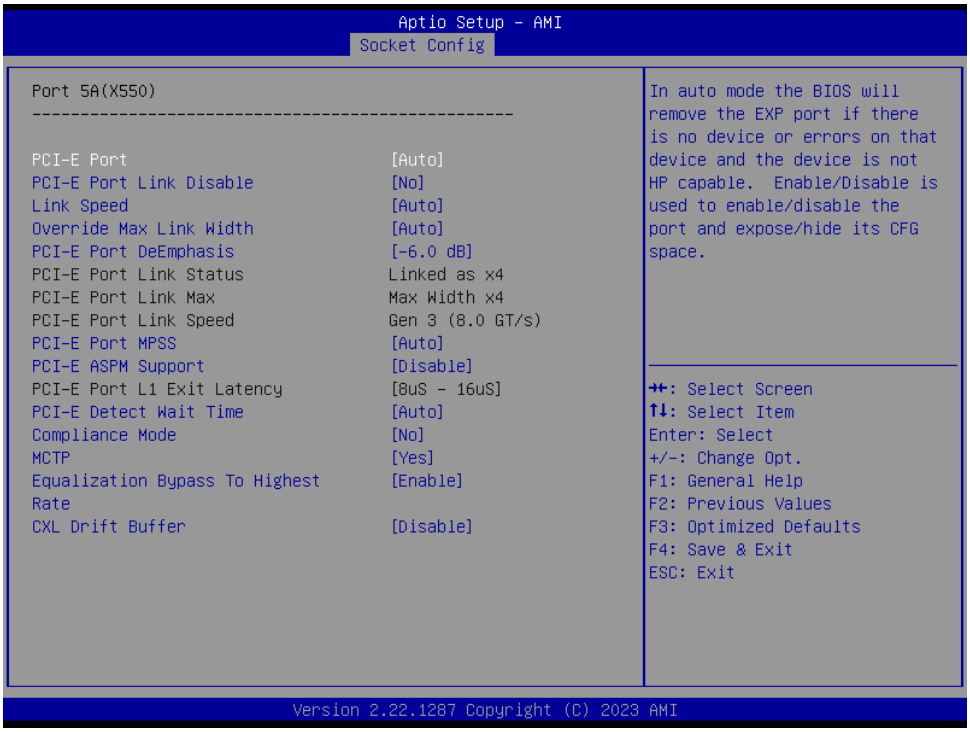
3.6.4.3.1.5 Port 4A(PCIe Slot7)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation.
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.

PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

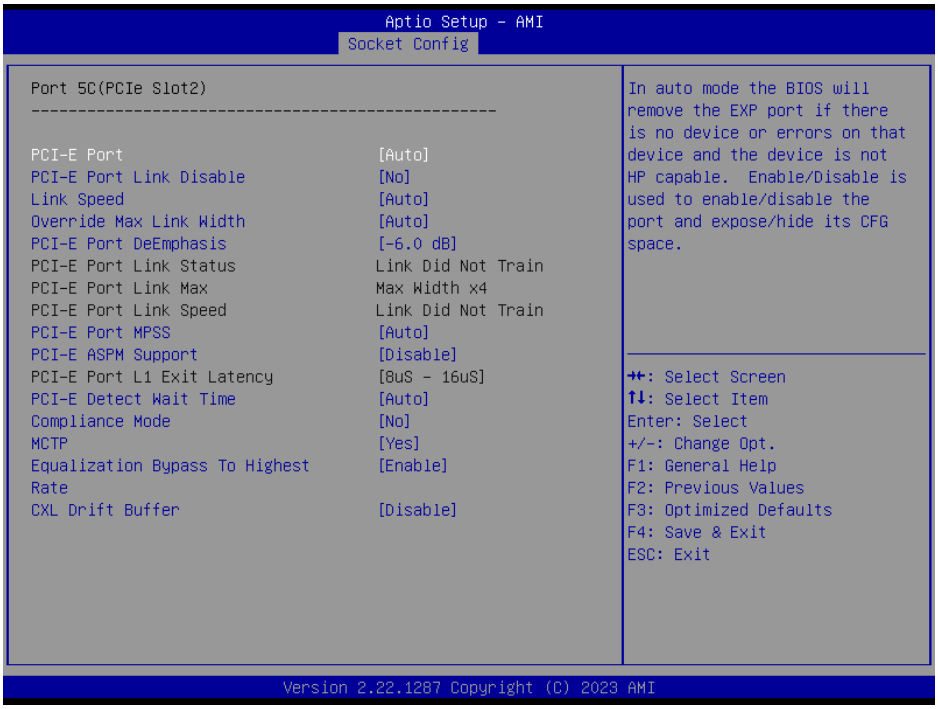
3.6.4.3.1.6 Port 5A(X550)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1	Override the max link width that was set by bifurcation.

	x2 x4 x8 x16	
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.
PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

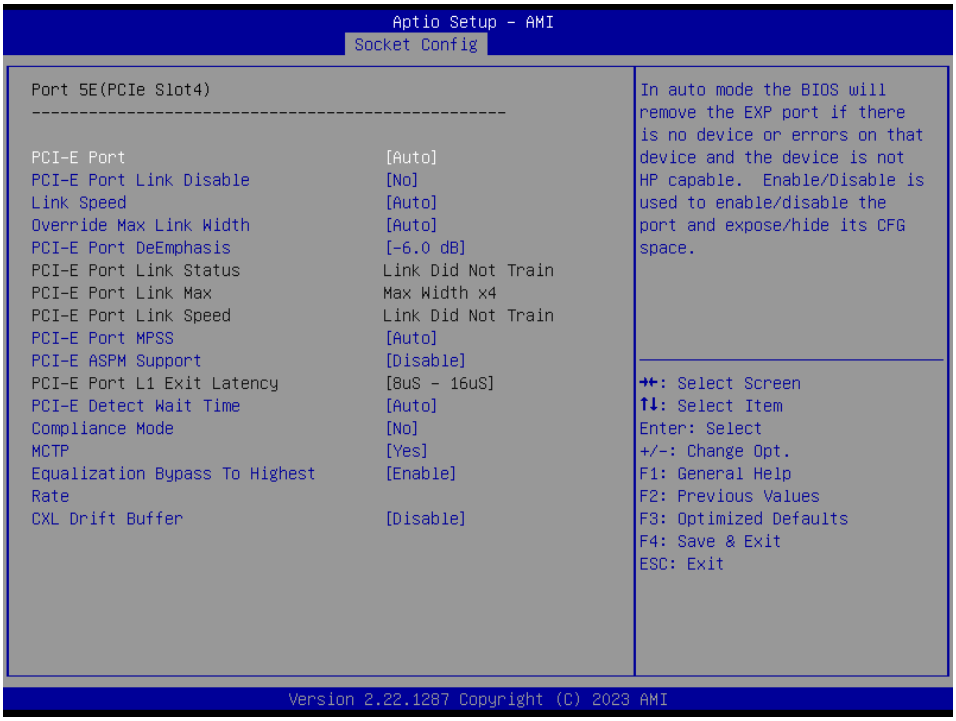
3.6.4.3.1.7 Port 5C(PCIe Slot2)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG

		space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation.
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.
PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

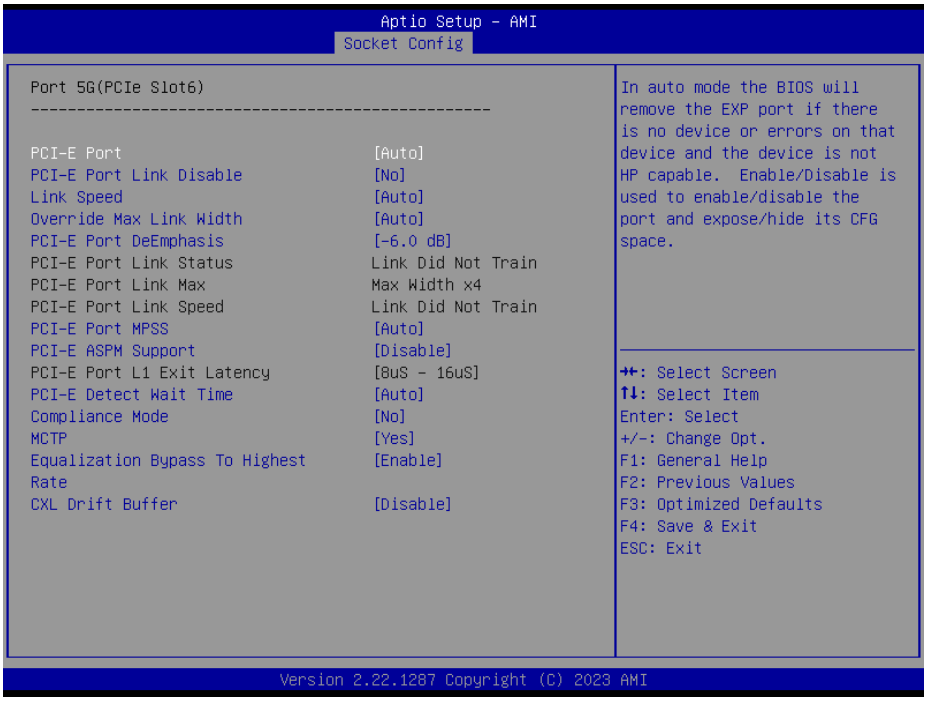
3.6.4.3.1.8 Port 5E(PCIe Slot4)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2 x4 x8 x16	Override the max link width that was set by bifurcation.
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.

PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

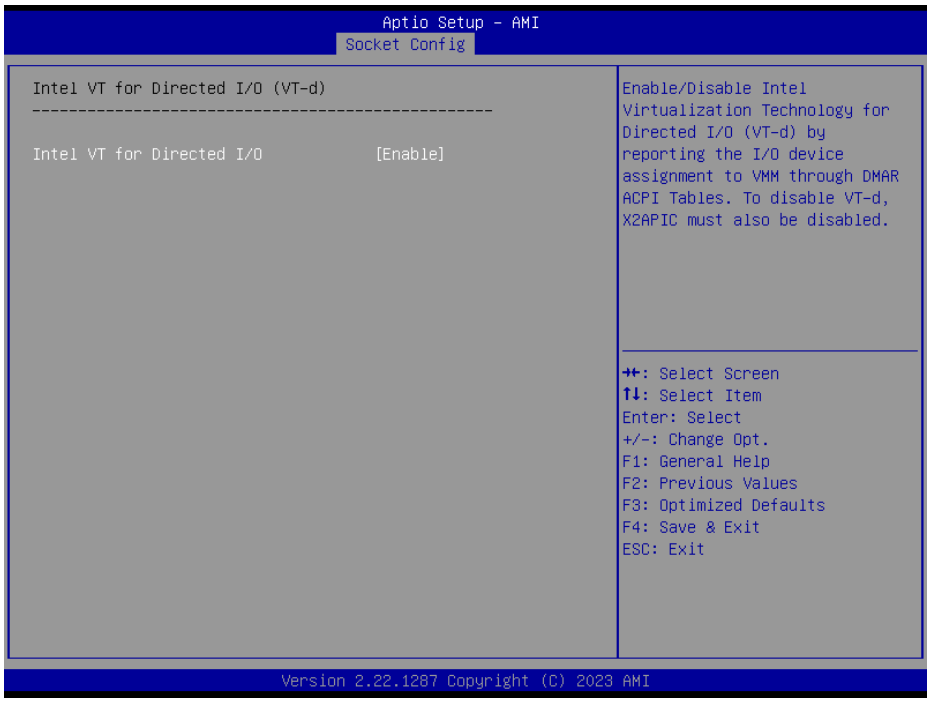
3.6.4.3.1.9 Port 5G(PCIe Slot6)



Item	Option	Description
PCI-E Port	Auto**[Default]** No Yes	In auto mode the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
PCI-E Port Link Disable	No**[Default]** Yes	This option disables the link so that the no training occurs but the CFG space is still active.
Link Speed	Auto**[Default]** Gen 1 (2.5 GT/s) Gen 2 (5 GT/s) Gen 3 (8 GT/s) Gen 4 (16 GT/s) Gen 5 (32 GT/s)	Choose Link Speed for this PCIe port.
Override Max Link Width	Auto**[Default]** x1 x2	Override the max link width that was set by bifurcation.

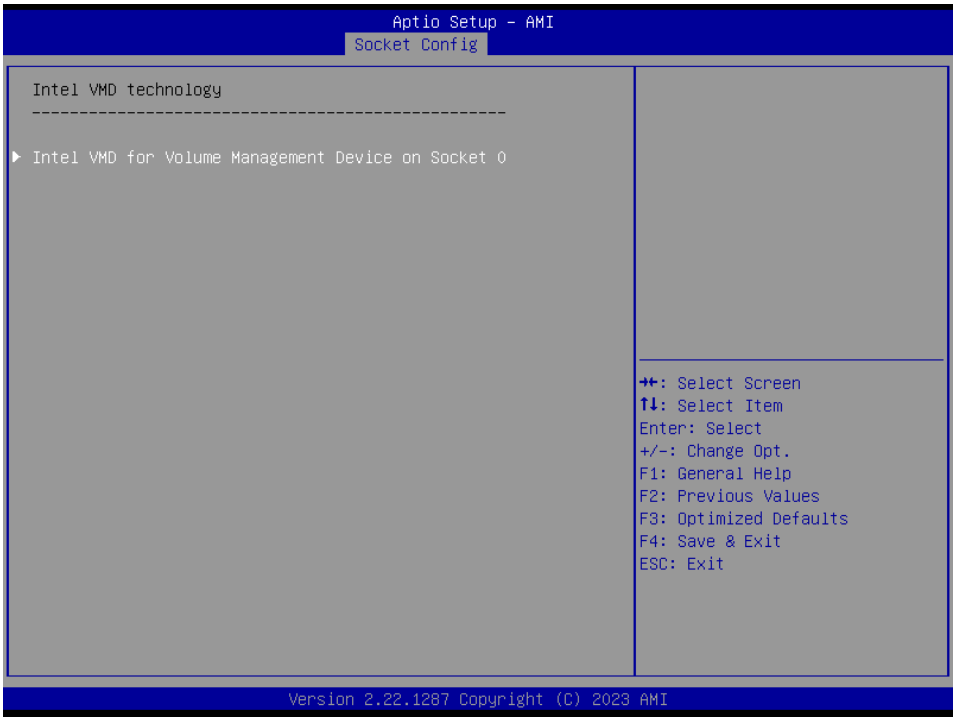
	x4 x8 x16	
PCI-E Port DeEmphasis	-6.0 dB**[Default]** -3.5 dB	De-Emphais control (LNKCON2[6]) for this PCIe port.
PCI-E Port MPSS	128B 256B 512B Auto**[Default]**	Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps hardware default.
PCI-E ASPM Support	Disabled**[Default]** Auto	This option can disable ASPM support in a PCIe root port. 'Auto' keeps hardware default.
PCI-E Detect Wait Time	Disable 500ms Auto**[Default]**	Set PCIe port TxRx detect polling.
Compliance Mode	No**[Default]** Yes	Enable/Disable Complicance Mode for this PCIe port.
MCTP	No Yes**[Default]**	Enable/Disable MCTP.
Equalization Bypass To Highest Rate	Disable Enable**[Default]**	Equalization Bypass To Highest Rate Support Enable/Disable.
CXL Drift Buffer	Disable**[Default]** Enable	Enable/Disable CXL Drift Buffer if there is a common referecne clock.

3.6.4.3.2 Intel VT for Directed I/O (VT-d)

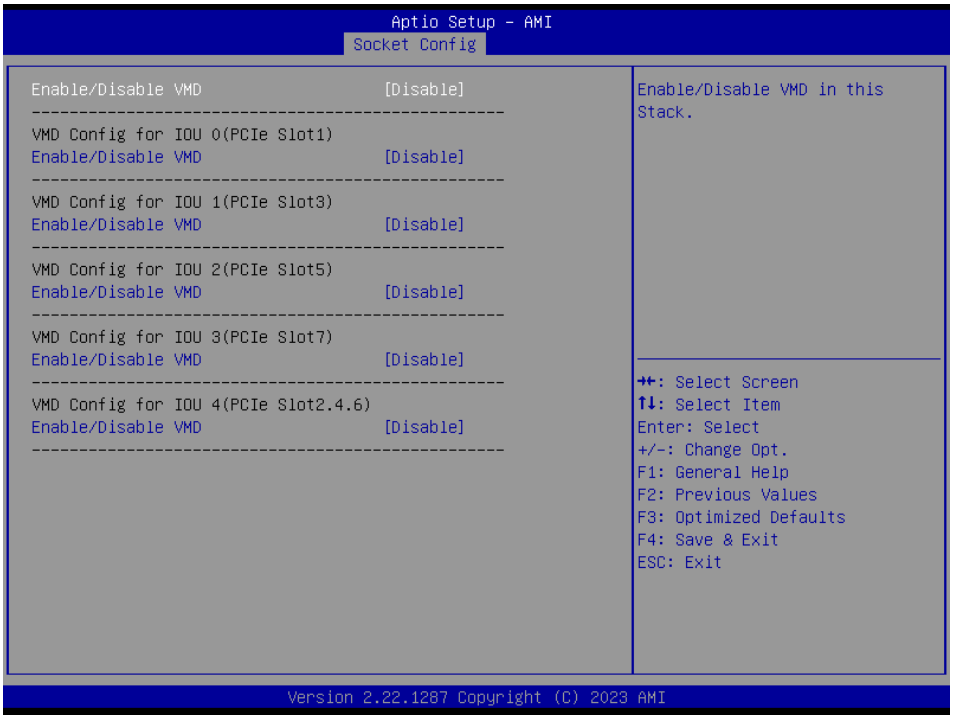


Item	Options	Description
Intel VT for Directed I/O	Enable**[Default]** Disable	Eneble/Disable Intel Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables. To disable VT-d, X2APIC must also be disabled.

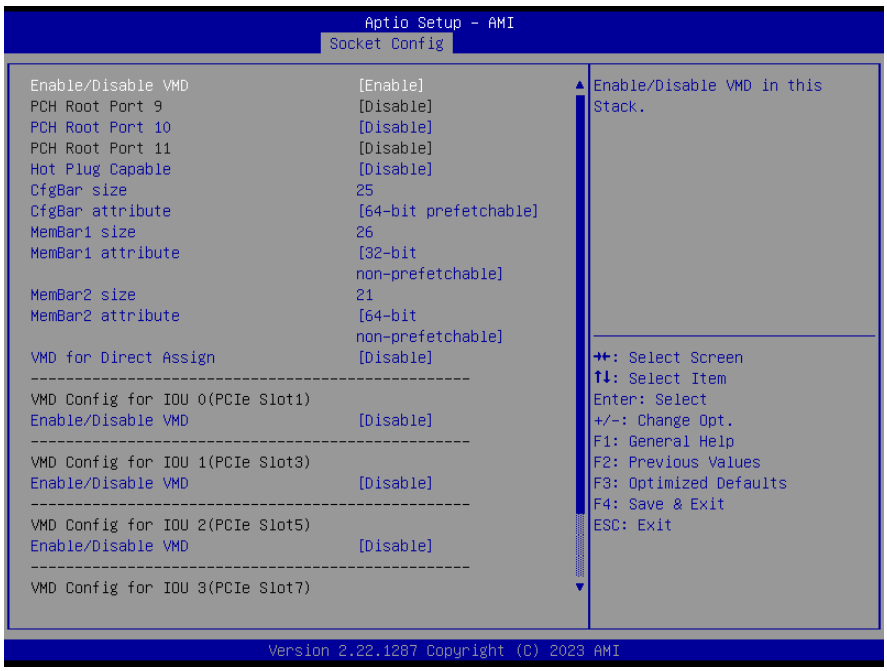
3.6.4.3.3 Intel VMD technology



3.6.4.3.3.1 Intel VMD for Volume Management Device on Socket 0

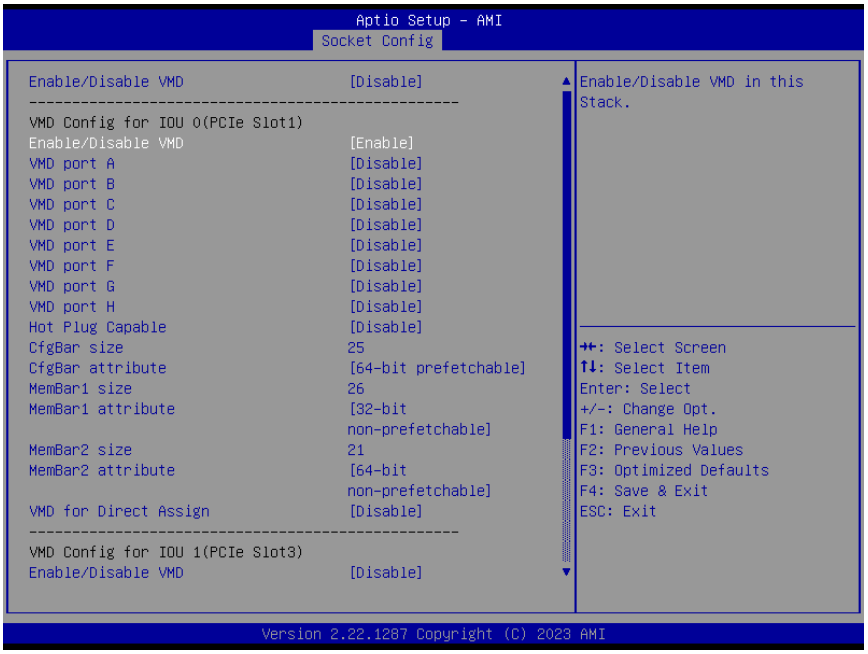


Item	Option	Description
Enable/Disable VMD	Disable**[Default]** Enable	Enable/Disable VMD in this Stack.



Item	Option	Description
Enable/Disable VMD	Disable Enable**[Default]**	Enable/Disable VMD in this Stack.
PCH Root Port 10	Disable**[Default]** Enable	Configuration PCH root port: Enable – VMD ownership root port.
Hot Plug Capable	Disable**[Default]** Enable	Enable/Disable Hot Plug for PCIe Root Ports.
CfgBar Size	25	Setup VMD Config BAR size (in bits Min=20, Max=27), ex:20bits=1MB, 27bits=128MB.
CfgBar attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR attribute, like 64-bit or prefectchable.
MemBar1 size	26	Setup VMD Memory BAR1 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar1 attribute	32-bit non-prefetchable**[Default]** 64-bit non-prefetchable 64-bit prefetchable	Setup VMD Config BAR1 attribute, like 64-bit or prefectchable.
MemBar2 size	21	Setup VMD Memory BAR2 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar2 attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR2 attribute, like 64-bit or prefectchable.
VMD for Direct Assign	Disable**[Default]** Enable	Enable/Disable VMD for Direct Assign.

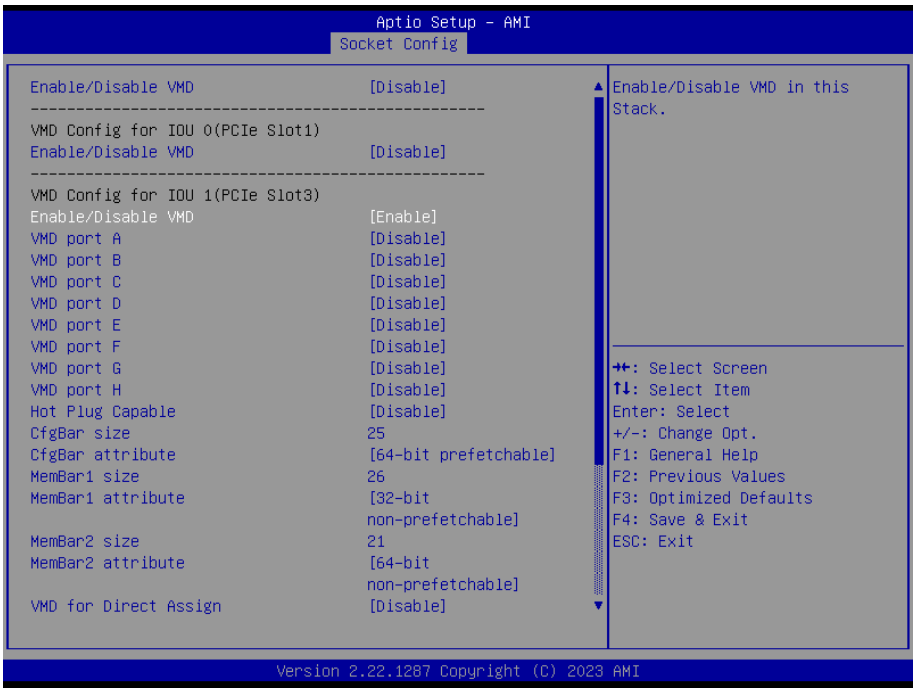
VMD Config for IOU 0(PCIe Slot1)



Item	Option	Description
Enable/Disable VMD	Disable**[Default]** Enable	Enable/Disable VMD in this Stack.
VMD port A	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port B	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port C	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port D	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port E	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port F	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port G	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port H	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
Hot Plug Capable	Disable**[Default]** Enable	Enable/Disable Hot Plug for PCIe Root Ports.

CfgBar Size	25	Setup VMD Config BAR size (in bits Min=20, Max=27), ex:20bits=1MB, 27bits=128MB.
CfgBar attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR attribute, like 64-bit or prefectchable.
MemBar1 size	26	Setup VMD Memory BAR1 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar1 attribute	32-bit non-prefetchable**[Default]** 64-bit non-prefetchable 64-bit prefetchable	Setup VMD Config BAR1 attribute, like 64-bit or prefectchable.
MemBar2 size	21	Setup VMD Memory BAR2 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar2 attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR2 attribute, like 64-bit or prefectchable.
VMD for Direct Assign	Disable**[Default]** Enable	Enable/Disable VMD for Direct Assign.

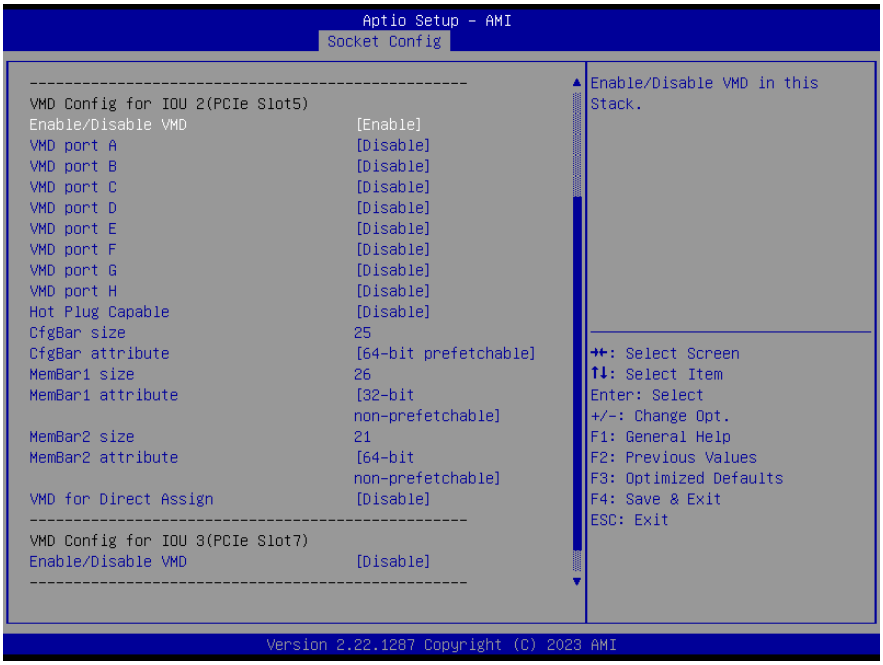
VMD Config for IOU 1(PCIe Slot3)



Item	Option	Description
Enable/Disable VMD	Disable**[Default]** Enable	Enable/Disable VMD in this Stack.
VMD port A	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port B	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on

		specific root port.
VMD port C	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port D	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port E	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port F	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port G	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port H	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
Hot Plug Capable	Disable**[Default]** Enable	Enable/Disable Hot Plug for PCIe Root Ports.
CfgBar Size	25	Setup VMD Config BAR size (in bits Min=20, Max=27), ex:20bits=1MB, 27bits=128MB.
CfgBar attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR attribute, like 64-bit or prefectchable.
MemBar1 size	26	Setup VMD Memory BAR1 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar1 attribute	32-bit non-prefetchable**[Default]** 64-bit non-prefetchable 64-bit prefetchable	Setup VMD Config BAR1 attribute, like 64-bit or prefectchable.
MemBar2 size	21	Setup VMD Memory BAR2 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar2 attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR2 attribute, like 64-bit or prefectchable.
VMD for Direct Assign	Disable**[Default]** Enable	Enable/Disable VMD for Direct Assign.

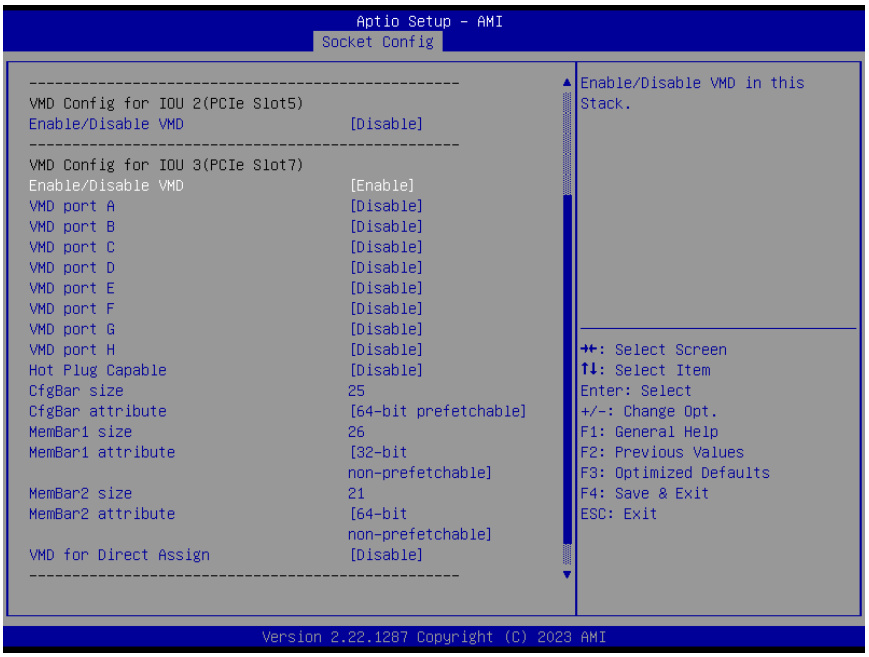
VMD Config for IOU 2(PCIe Slot5)



Item	Option	Description
Enable/Disable VMD	Disable**[Default]** Enable	Enable/Disable VMD in this Stack.
VMD port A	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port B	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port C	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port D	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port E	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port F	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port G	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port H	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
Hot Plug Capable	Disable**[Default]** Enable	Enable/Disable Hot Plug for PCIe Root Ports.

CfgBar Size	25	Setup VMD Config BAR size (in bits Min=20, Max=27), ex:20bits=1MB, 27bits=128MB.
CfgBar attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR attribute, like 64-bit or prefectchable.
MemBar1 size	26	Setup VMD Memory BAR1 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar1 attribute	32-bit non-prefetchable**[Default]** 64-bit non-prefetchable 64-bit prefetchable	Setup VMD Config BAR1 attribute, like 64-bit or prefectchable.
MemBar2 size	21	Setup VMD Memory BAR2 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar2 attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR2 attribute, like 64-bit or prefectchable.
VMD for Direct Assign	Disable**[Default]** Enable	Enable/Disable VMD for Direct Assign.

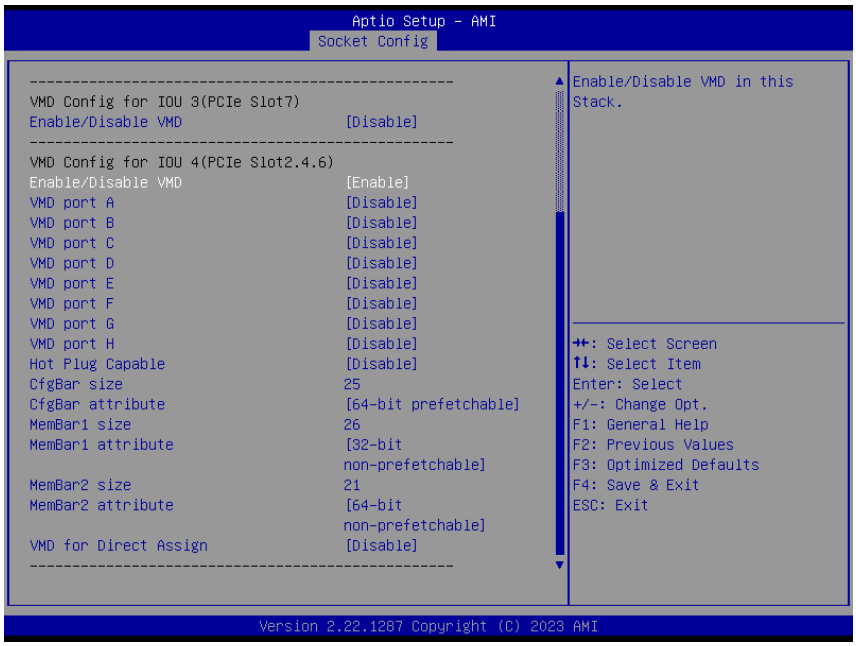
VMD Config for IOU 3(PCIe Slot7)



Item	Option	Description
Enable/Disable VMD	Disable Enable**[Default]**	Enable/Disable VMD in this Stack.
VMD port A	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port B	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.

VMD port C	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port D	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port E	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port F	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port G	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port H	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
Hot Plug Capable	Disable**[Default]** Enable	Enable/Disable Hot Plug for PCIe Root Ports.
CfgBar Size	25	Setup VMD Config BAR size (in bits Min=20, Max=27), ex:20bits=1MB, 27bits=128MB.
CfgBar attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR attribute, like 64-bit or prefectchable.
MemBar1 size	26	Setup VMD Memory BAR1 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar1 attribute	32-bit non-prefetchable**[Default]** 64-bit non-prefetchable 64-bit prefetchable	Setup VMD Config BAR1 attribute, like 64-bit or prefectchable.
MemBar2 size	21	Setup VMD Memory BAR2 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar2 attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR2 attribute, like 64-bit or prefectchable.
VMD for Direct Assign	Disable**[Default]** Enable	Enable/Disable VMD for Direct Assign.

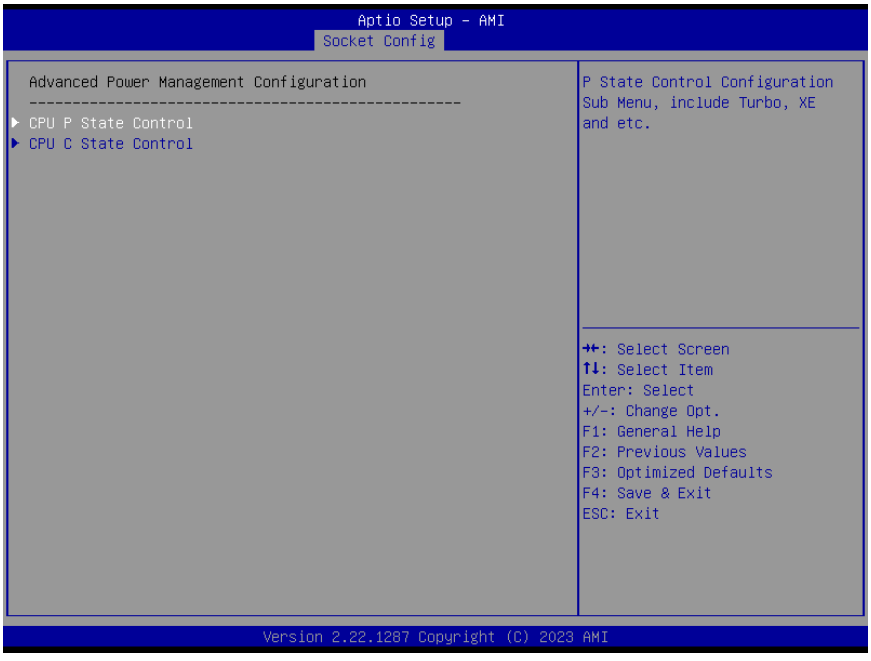
VMD Config for IOU 4(PCIe Slot2.4.6)



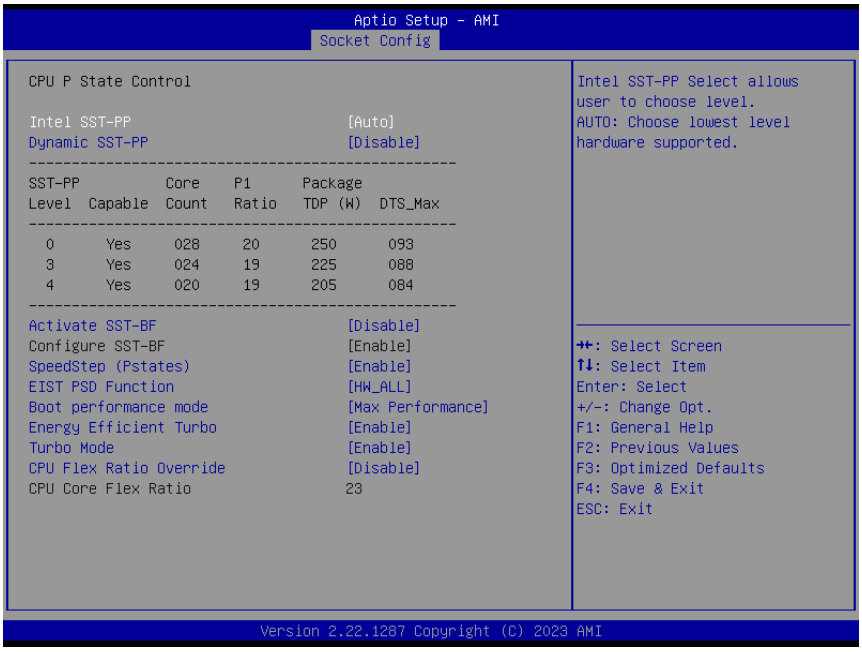
Item	Option	Description
Enable/Disable VMD	Disable**[Default]** Enable	Enable/Disable VMD in this Stack.
VMD port A	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port B	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port C	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port D	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port E	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port F	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port G	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
VMD port H	Disable**[Default]** Enable	Enable/Disable Intel Volume Management Device Technology on specific root port.
Hot Plug Capable	Disable**[Default]** Enable	Enable/Disable Hot Plug for PCIe Root Ports.

CfgBar Size	25	Setup VMD Config BAR size (in bits Min=20, Max=27), ex:20bits=1MB, 27bits=128MB.
CfgBar attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR attribute, like 64-bit or prefectchable.
MemBar1 size	26	Setup VMD Memory BAR1 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar1 attribute	32-bit non-prefetchable**[Default]** 64-bit non-prefetchable 64-bit prefetchable	Setup VMD Config BAR1 attribute, like 64-bit or prefectchable.
MemBar2 size	21	Setup VMD Memory BAR2 size (in bits Min=20), ex:20bits=1MB, 22bits=4MB, 26bits=64MB.
MemBar2 attribute	32-bit non-prefetchable 64-bit non-prefetchable 64-bit prefetchable**[Default]**	Setup VMD Config BAR2 attribute, like 64-bit or prefectchable.
VMD for Direct Assign	Disable**[Default]** Enable	Enable/Disable VMD for Direct Assign.

3.6.4.4 Advanced Power Management Configuration

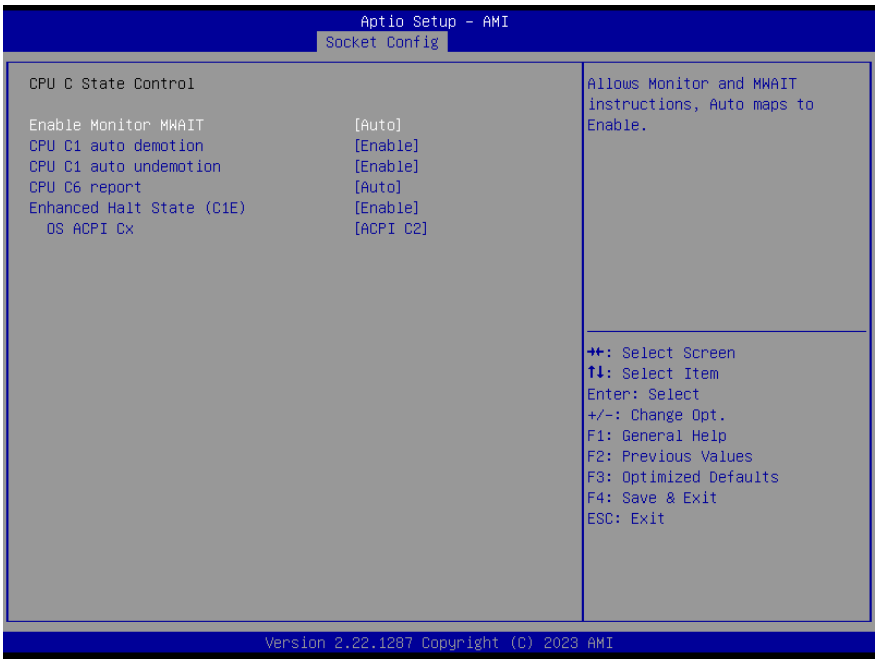


3.6.4.4.1 CPU P State Control



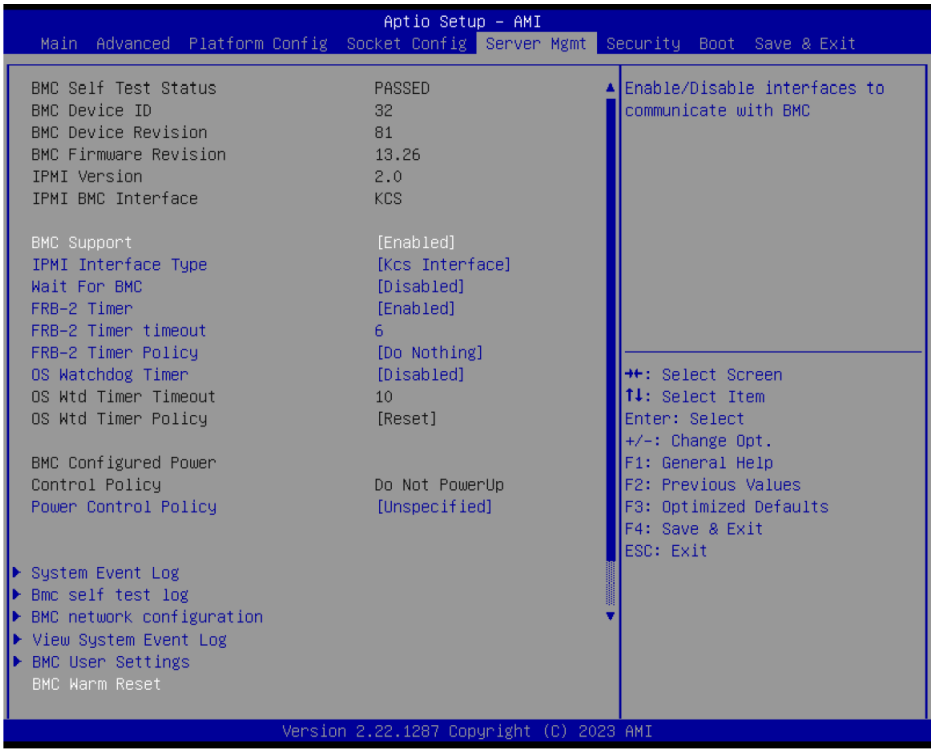
Item	Option	Description
Intel SST-PP	Auto**[Default]** Level0 Level1 Level2 Level3 Level4	Intel SST-PP Select allows user to choose level. AUTO: Choose lowest level hardware supported.
Dynamic SST-PP	Disable**[Default]** Enable	Support Dynamic SST-PP selection NOTE: HWP Native Mode is a pre-requisite for enabling Dynamic SST-PP.
Activate SST-BF	Disable**[Default]** Enable	This Option allows SST-BF to be enabled. NOTE: 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.
SpeedStep (Pstates)	Disable Enable**[Default]**	Enable/Disable EIST (P-States).
EIST PSD Function	HW_ALL**[Default]** SW_ALL	Choose HW_ALL/SW_ALL in _PSD return.
Boot performance mode	Max Performance**[Default]** Max Efficient Set by Intel Node Manager	Select the performance state that the BIOS will set before OS hand off.
Energy Efficient Turbo	Enable**[Default]** Disable	Energy Efficient Turbo Disable, MSR 0x1FC[19].
Turbo Mode	Disable Enable**[Default]**	Enable/Disable processor Turbo Mode (requires EMTTM enabled too).
CPU Flex Ratio Override	Disable**[Default]** Enable	Enable/Disable CPU Flex Ratio Programming.

3.6.4.4.2 CPU C State Control



Item	Option	Description
Enable Monitor MWAIT	Disable Enable Auto**[Default]**	Allows Monitor and MWAIT instructions, Auto maps to Enable.
CPU C1 auto demotion	Disable Enable**[Default]**	Allows CPU to automatically demote to C1. Takes effect after reboot.
CPU C1 auto undemotion	Disable Enable**[Default]**	Allows CPU to automatically undemote from C1. Takes effect after reboot.
CPU C6 report	Disable Enable Auto**[Default]**	Enable/Disable CPU C6(ACPI C3) report to OS, Auto maps to enable.
Enhanced Halt State (C1E)	Disable Enable**[Default]**	Core C1E auto promotion Control. Takes effect after reboot. Will be enforced to enable when Optimized Power Mode is enabled.
OS ACPI Cx	ACPI C2**[Default]** ACPI C3	Report CC3/CC6 to OS ACPI C2 or ACPI C3.

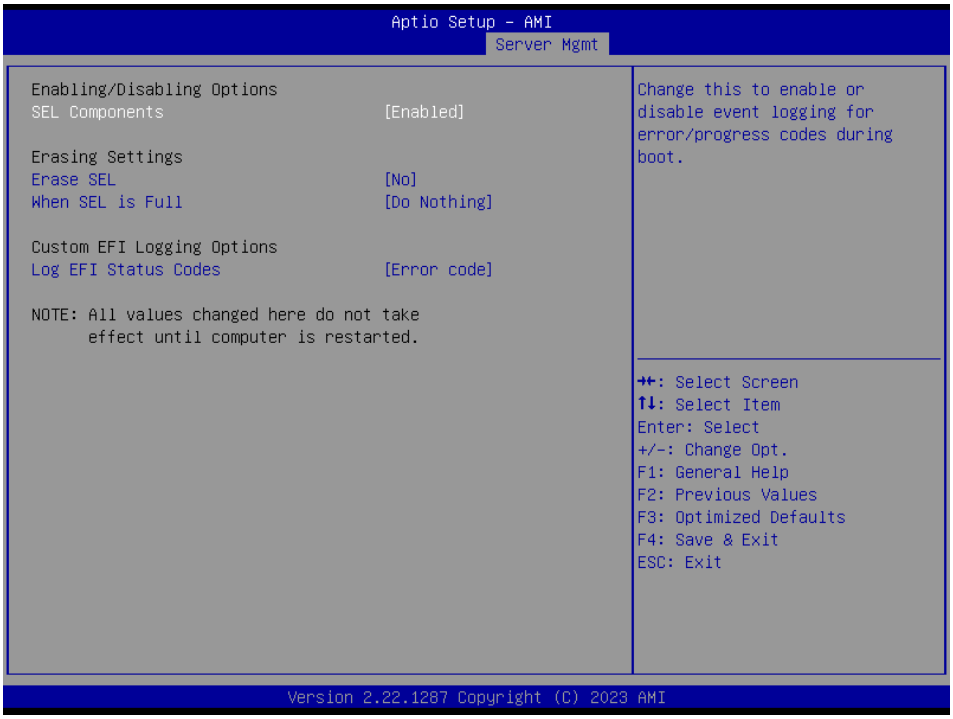
3.6.5 Server Mgmt



Item	Options	Description
BMC Support	Enabled**[Default]** Disabled	Enable/Disable interfaces to communicate with BMC.
IPMI Interface Type	Kcs Interface**[Default]** Ssif Interface Ipmb Interface Usb Interface Oem1 Interface Oem2 Interface	Type of Interface to communicate BMC from HOST.
Wait For BMC	Enabled Disabled**[Default]**	Wait For BMC response for specified time out. BMC starts at the same time when BIOS starts during AC power ON. It takes around 30 seconds to initialize Host to BMC interfaces.
FRB-2 Timer	Enabled**[Default]** Disabled	Enable or Disable FRB-2 time (POST timer).
FRB-2 Timer timeout	6	Enter value Between 3 to 6 min for FRB-2 Timer Expiration value.
FRB-2 Timer Policy	Do Nothing**[Default]** Reset Power Down Power Cycle	Configure how the system should respond if the FRB-2 Timer expires. Not available if FRB-2 Timer is disabled.
OS Watchdog Timer	Enabled Disabled**[Default]**	If enabled, starts a BIOS timer which can only be shut off by Management Software after the OS loads. Helps determine that the OS successfully loaded or follows

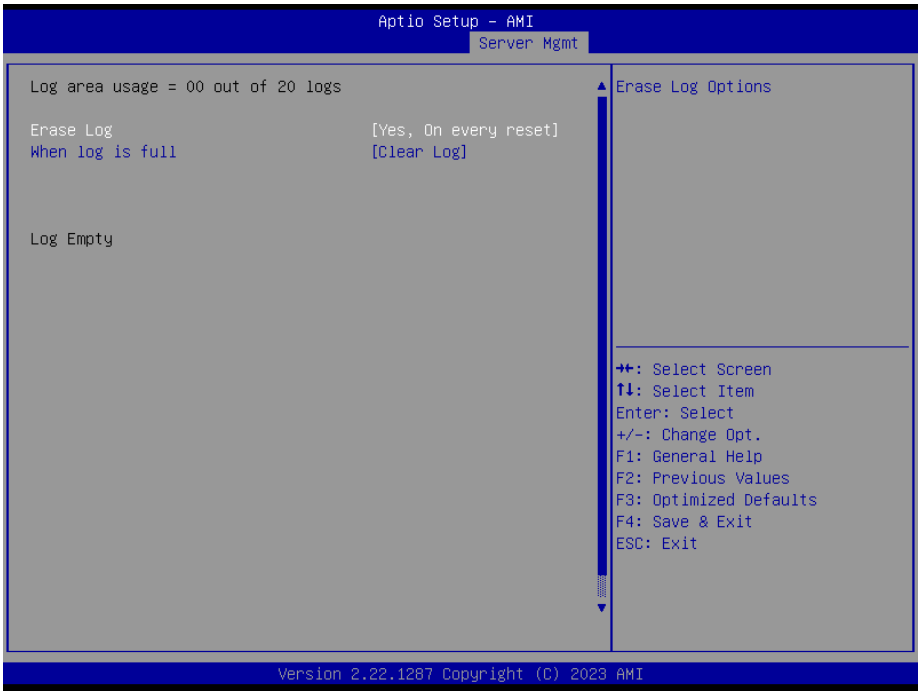
		the OS Boot Watchdog Timer policy.
Power Control Policy	Do Not PowerUp Last Power State Power Restore Unspecified**[Default]**	Configure how the system should respond if AC Power is lost, Reset not required as selected Power policy will be set in BMC when policy is saved.
BMC Warm Reset	Press <Enter> to do Warm Reset BMC.	

3.6.5.1 System Event Log



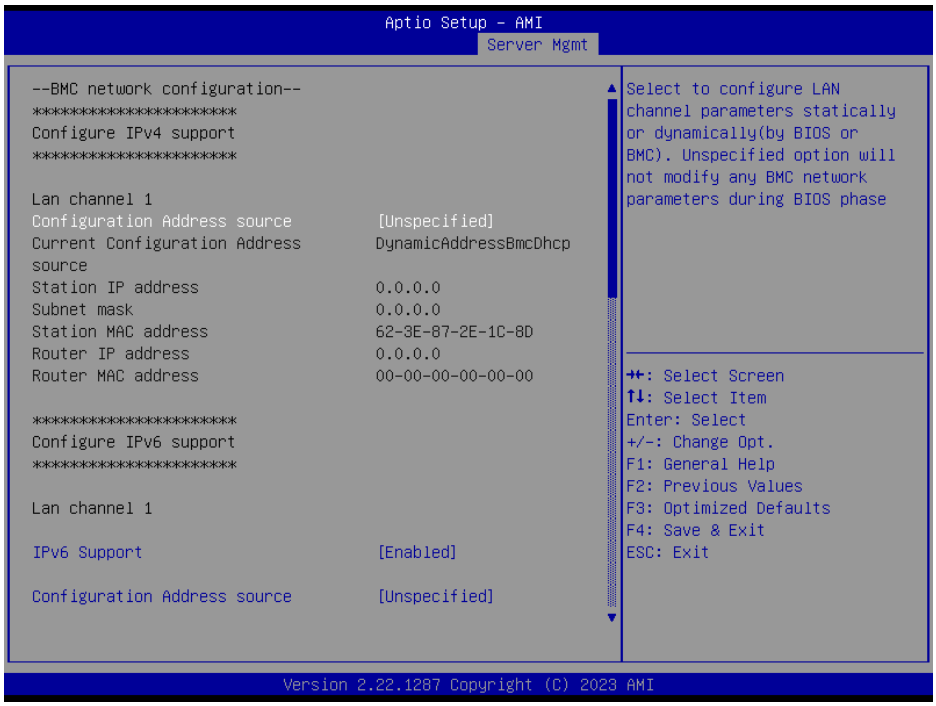
Item	Option	Description
SEL Components	Enabled**[Default]** Disabled	Change this to enable or disable event logging for error/progress codes during boot.
Erase SEL	No**[Default]** Yes, On next reset Yes, On every reset	Choose options for erasing SEL.
When SEL is Full	Do Nothing**[Default]** Erase Immediately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

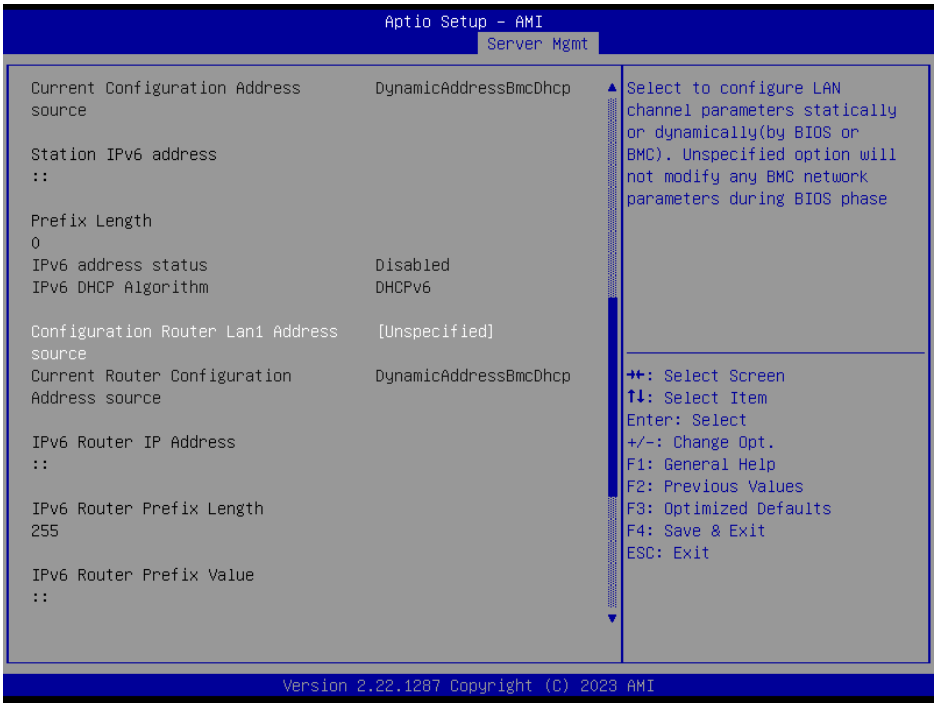
3.6.5.2 Bmc self test log



Item	Option	Description
Erase Log	Yes, On every reset**[Default]** No	Erase Log Options.
When log is full	Clear Log**[Default]** Do not log any more	Select the action to be taken when log is full.

3.6.5.3 BMC network configuration

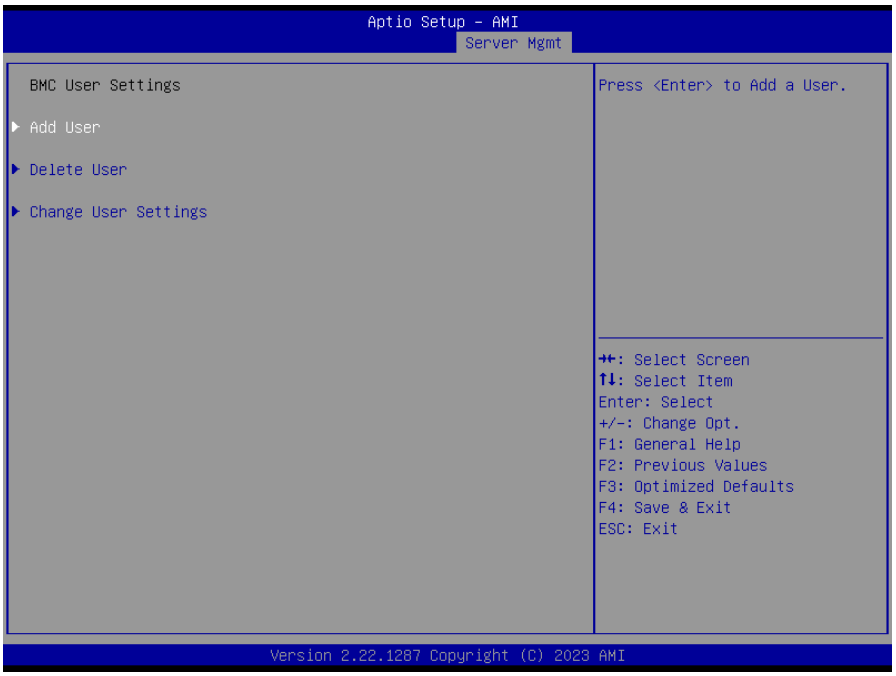




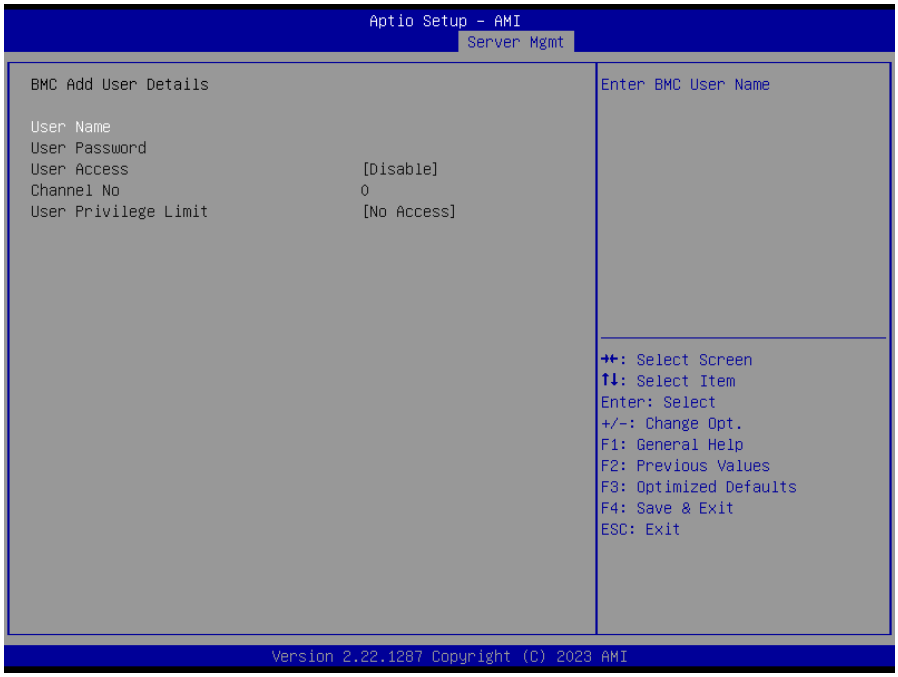
Item	Option	Description
Configuration Address source	Unspecified**[Default]** Static DynamicBmcDhcp DynamicBmcNonDhcp	Select configure LAN channel parameters statically or dynamically(by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase.
IPV6 Support	Enabled**[Default]** Disabled	Enable or Disable LAN1 IPv6 Support.

Configuration Address source	Unspecified**[Default]** Static DynamicBmcDhcp	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.
Configuration Router Lan1 Address source	Unspecified**[Default]** Static DynamicBmcDhcp	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.

3.6.5.4 BMC User Settings

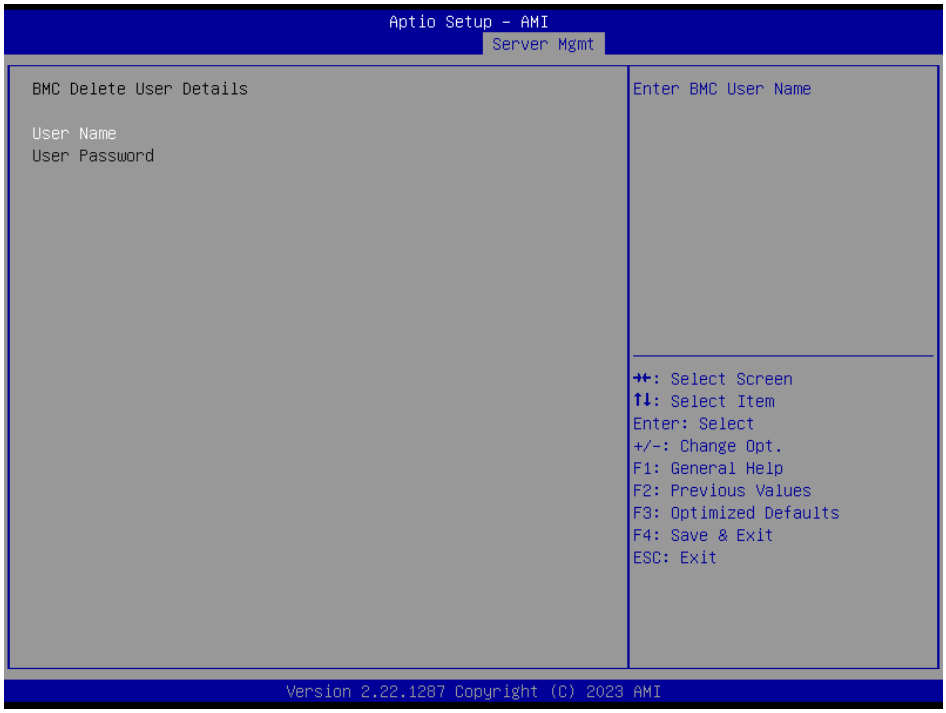


3.6.5.4.1 BMC Add User Details



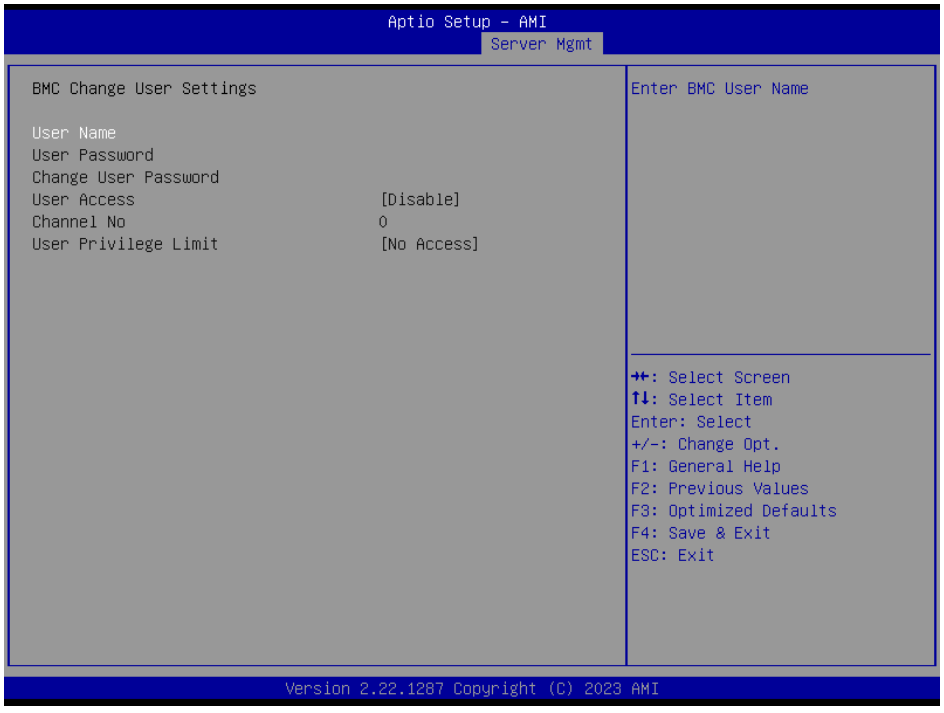
Item	Description
User Name	Enter BMC User Name.

3.6.5.4.2 BMC Delete User Details



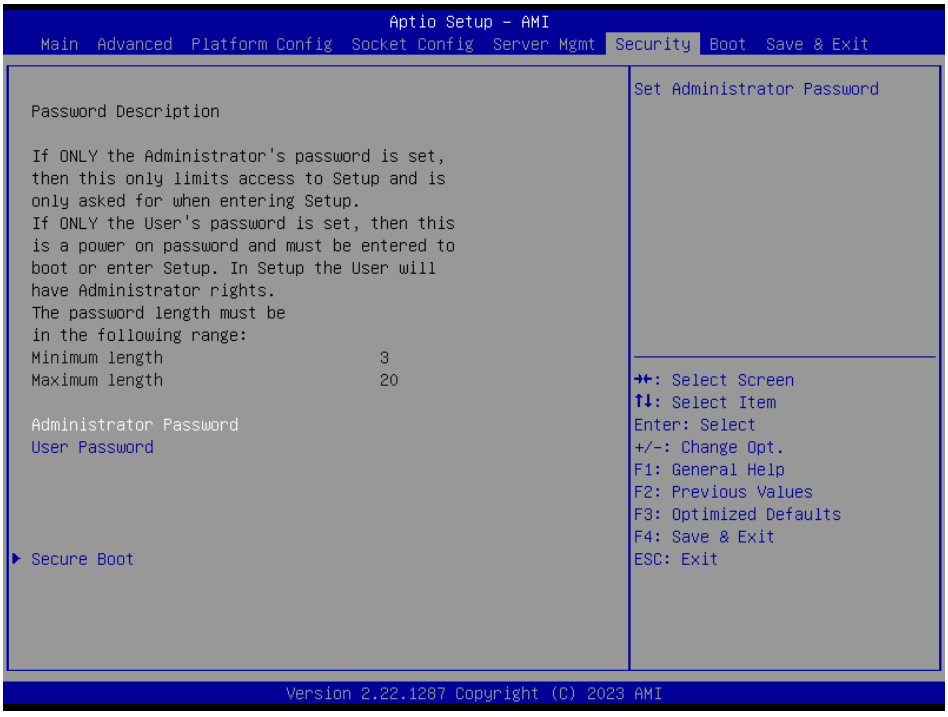
Item	Description
User Name	Enter BMC User Name.

3.6.5.4.3 BMC Change User Settings



Item	Description
User Name	Enter BMC User Name.

3.6.6 Security



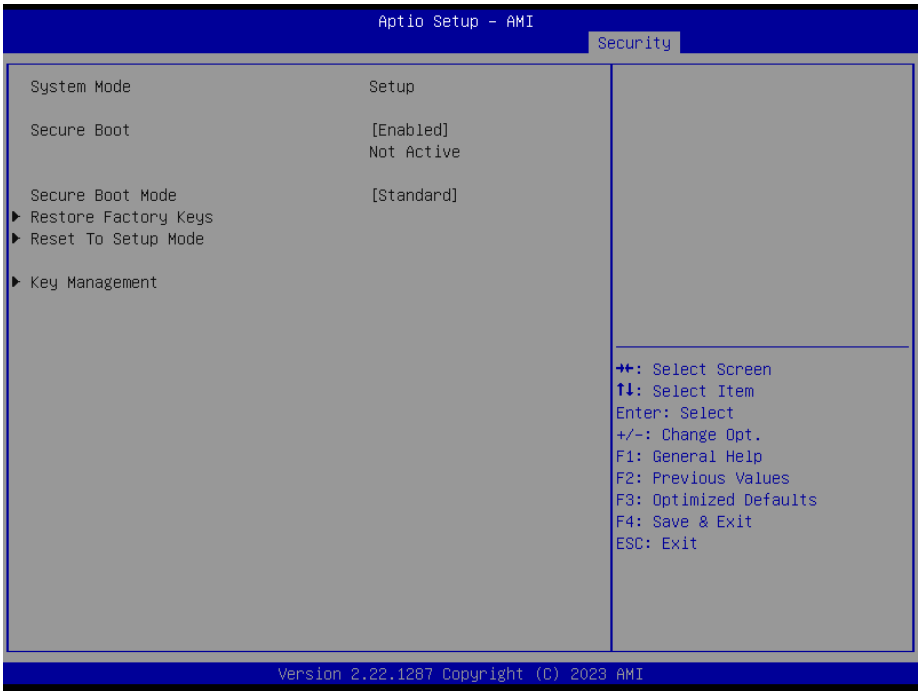
- **Administrator Password**

Set setup Administrator Password

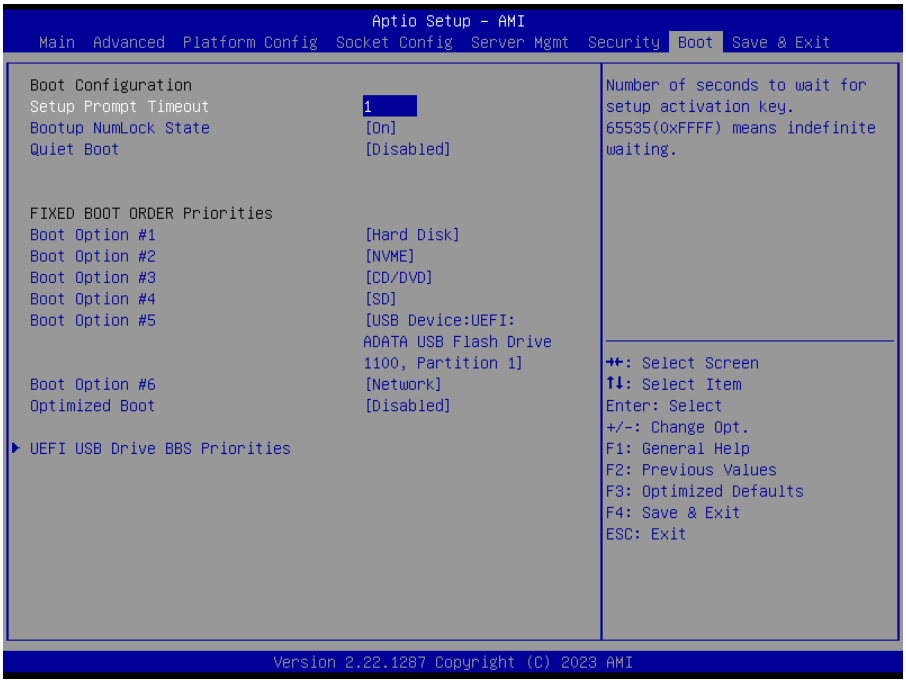
- **User Password**

Set User Password

3.6.6.1 Secure Boot



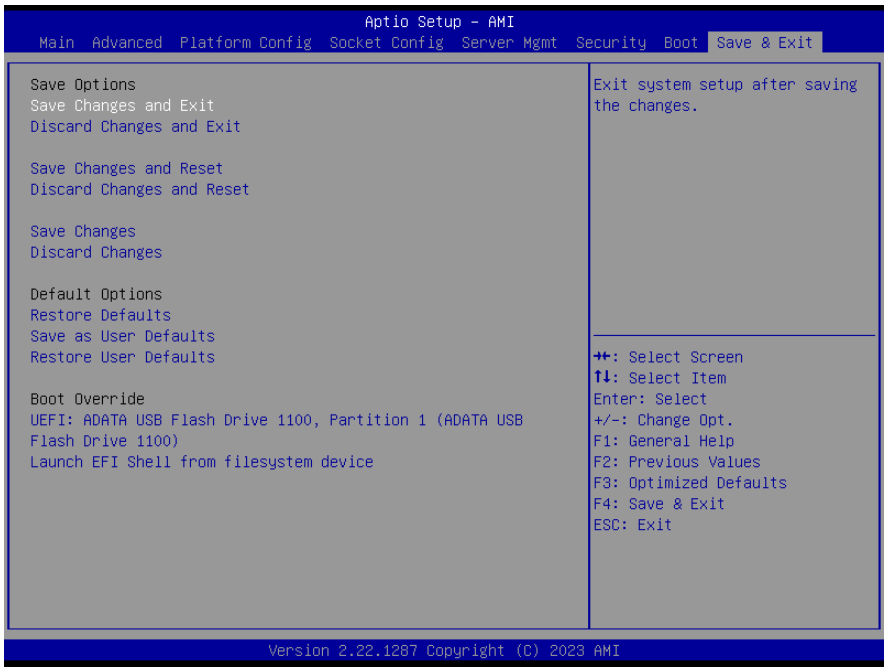
3.6.7 Boot



Item	Option	Description
Setup Prompt Timeout	1~ 65535	Set the default timeout before system boot. A value of 65535 will disable the timeout completely.
Bootup NumLock State	On**[Default]** Off	Select the keyboard NumLock state
Quiet Boot	Disabled**[Default]** Enabled	Enables or disables Quiet Boot option
Boot Option #1	Hard Disk**[Default]** NVME CD/DVD SD USB Device Network Disabled	Set the system boot order.
Boot Option #2	Hard Disk NVME**[Default]** CD/DVD SD USB Device Network Disabled	Set the system boot order.
Boot Option #3	Hard Disk NVME CD/DVD**[Default]** SD USB Device Network Disabled	Set the system boot order.
Boot Option #4	Hard Disk NVME	Set the system boot order.

	CD/DVD SD**[Default]** USB Device Network Disabled	
Boot Option #5	Hard Disk NVME CD/DVD SD USB Device**[Default]** Network Disabled	Set the system boot order.
Boot Option #6	Hard Disk NVME CD/DVD SD USB Device Network**[Default]** Disabled	Set the system boot order.
Optimized Boot	Disabled**[Default]** Enabled	Enables or disables Optimized Boot. Enabling Optimized Boot will disable Csm support and disable connecting Network devices to decrease boot time. While disabling Optimized Boot, make sure to restore Csm Support option to previous value before enabling Optimized Boot.

3.6.8 Save and exit



3.6.8.1 Save Changes and Exit

Use the save changes and reset option to save the changes made to the BIOS options and to exit the BIOS configuration setup program.

3.6.8.2 Discard Changes and Exit

Use the Discard changes and Exit option to exit the system without saving the changes made to the BIOS configuration setup program.

3.6.8.3 Save Changes and Reset

Reset the system after saving the changes.

3.6.8.4 Discard Changes and Reset

Any changes made to BIOS settings during this session of the BIOS setup program are discarded. The setup program then exits and reboots the controller.

3.6.8.5 Save Changes

Changes made to BIOS settings during this session are committed to NVRAM. The setup program remains active, allowing further changes.

3.6.8.6 Discard Changes

Any changes made to BIOS settings during this session of the BIOS setup program are discarded. The BIOS setup continues to be active.

3.6.8.7 Restore Defaults

This option restores all BIOS settings to the factory default. This option is useful if the controller exhibits unpredictable behavior due to an incorrect or inappropriate BIOS setting.

3.6.8.8 Save as User Defaults

This option saves a copy of the current BIOS settings as the User Defaults. This option is useful for preserving custom BIOS setup configurations.

3.6.8.9 Restore User Defaults

This option restores all BIOS settings to the user defaults. This option is useful for restoring previously preserved custom BIOS setup configurations.

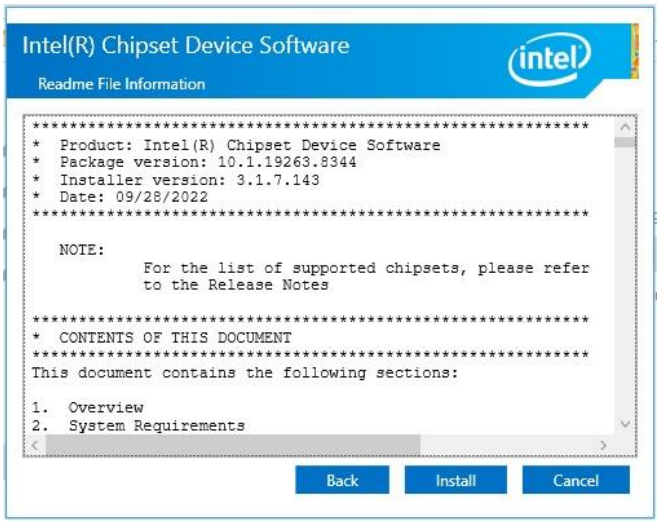
4. Drivers Installation

Note: Installation procedures and screen shots in this section are for your reference and may not be exactly the same as shown on your screen.

4.1 Install Chipset Driver

All drivers can be found on the Avalue Official Website: http://www.avalue.com.tw.

Note: The installation procedures and screen shots in this section are based on Windows 10 operation system. If the warning message appears while the installation process, click Continue to go on.



Step 3. Click **Install**.

Step1. Click **Next**.

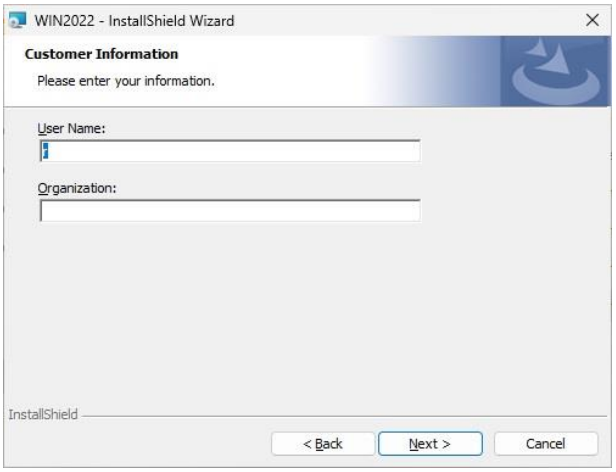
Step 4. Setup completed.

Step 2. Click **Accept**.

4.2 Install VGA Driver

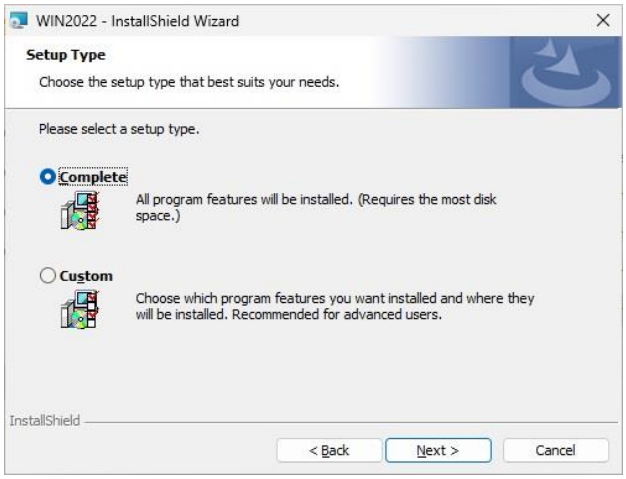
All drivers can be found on the Avalue Official Website: **http://www.avalue.com.tw**.

Note: The installation procedures and screen shots in this section are based on Windows 10 operation system.

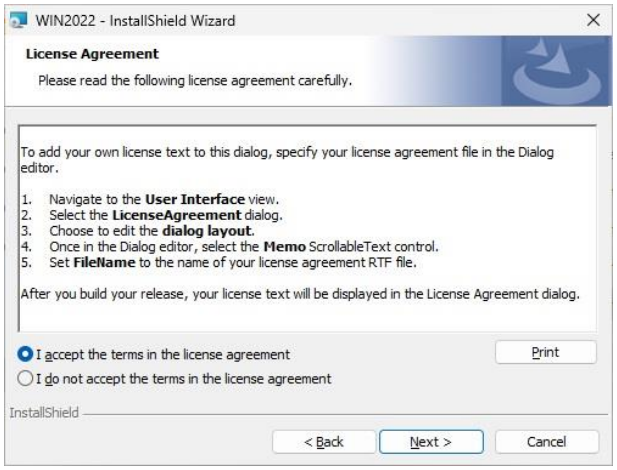


Step 3. Click **Next.**

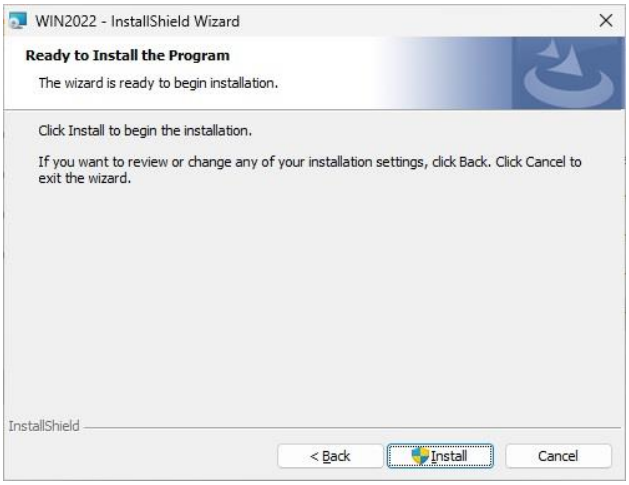
Step 1. Click **Next** to continue installation.



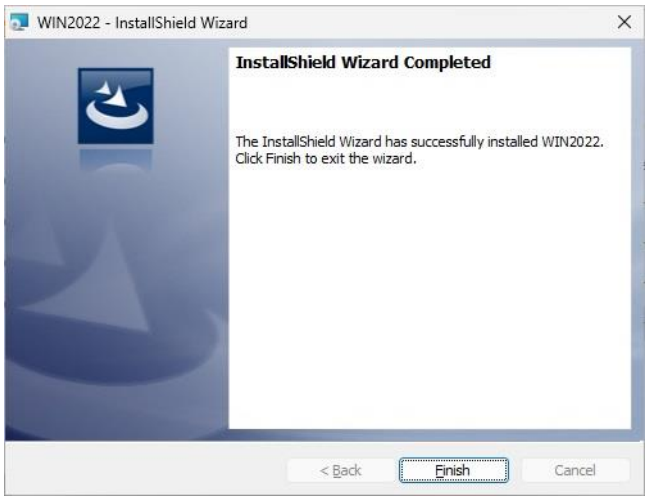
Step 4. Click **Next**.



Step 2. Click **Next**.



Step 5. Click **Install**.



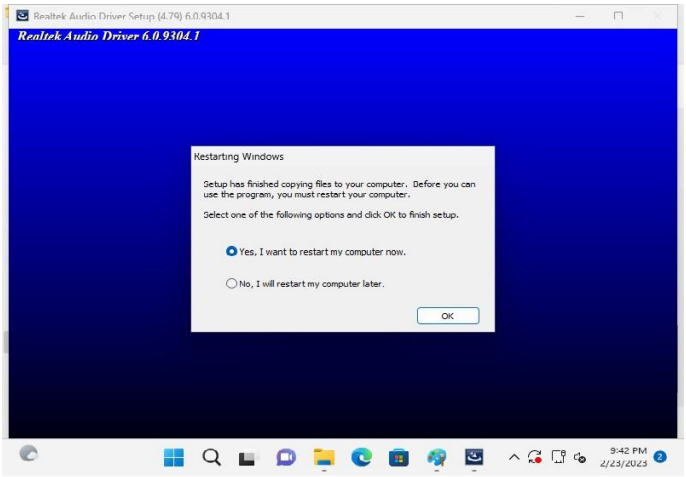
Step 6. Click **Finish** to complete setup.

4.3 Install Audio Driver

All drivers can be found on the Avalue Official Website:
http://www.avalue.com.tw.

Note: The installation procedures and screen shots in this section are based on Windows 10 operation system.

Step 1. Click **Yes** to continue installation.



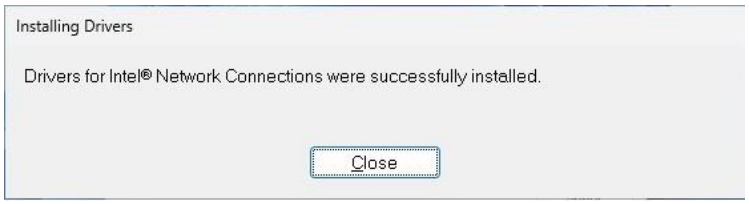
Step 2. Setup completed.

4.4 Install Ethernet Driver

All drivers can be found on the Avalue Official Website:
http://www.avalue.com.tw.

Note: The installation procedures and screen shots in this section are based on Windows 10 operation system.

Step 1. Click **OK** to continue installation.

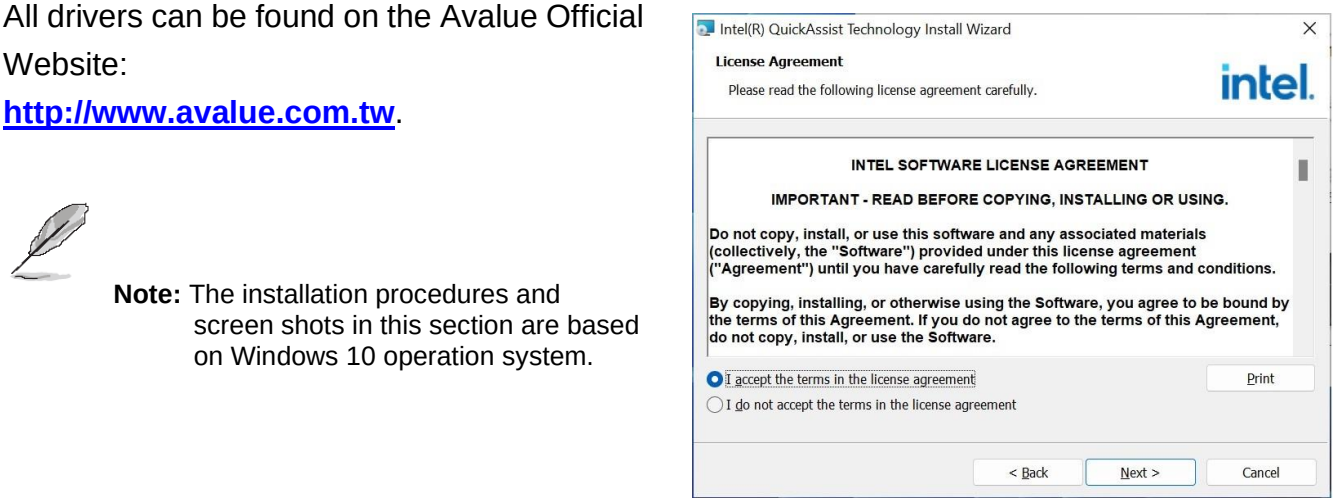


Step 2. Setup completed.

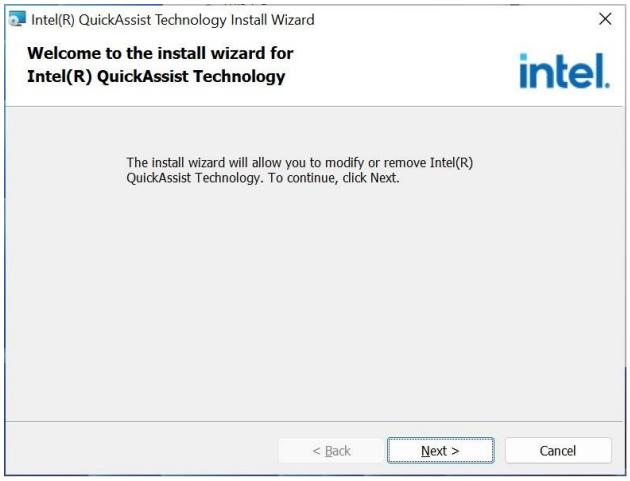
4.5 Install QuickAssist Technology Driver

All drivers can be found on the Avalue Official Website:
http://www.avalue.com.tw.

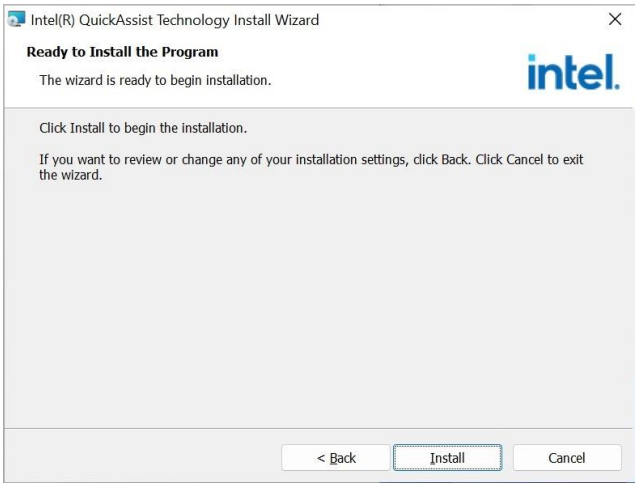
Note: The installation procedures and screen shots in this section are based on Windows 10 operation system.



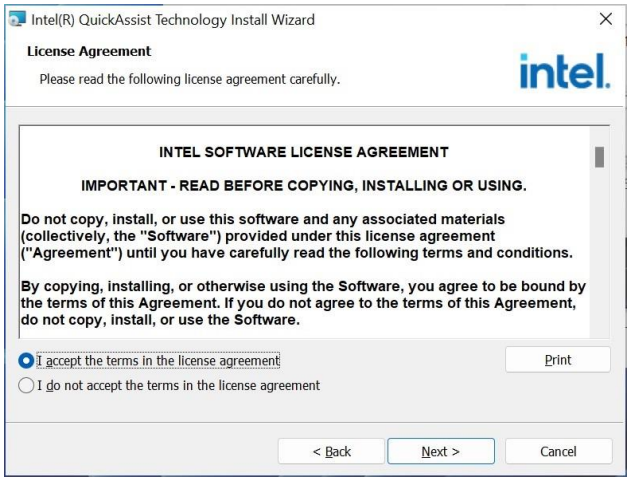
Step 3. Click **Next**.



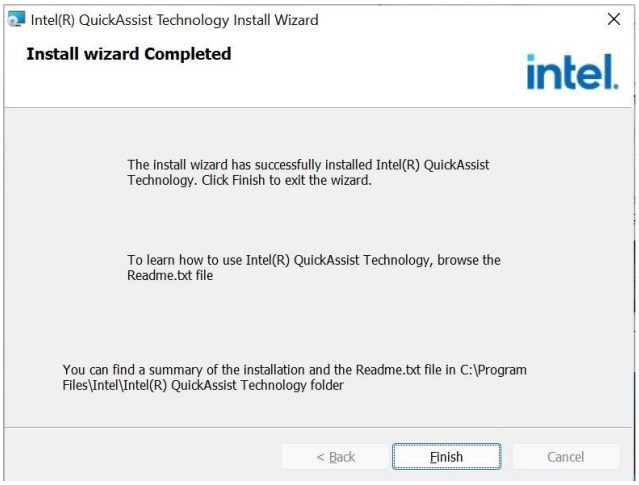
Step 1. Click **Next** to continue installation.



Step 4. Click **Install**.



Step 2. Click **Next**.

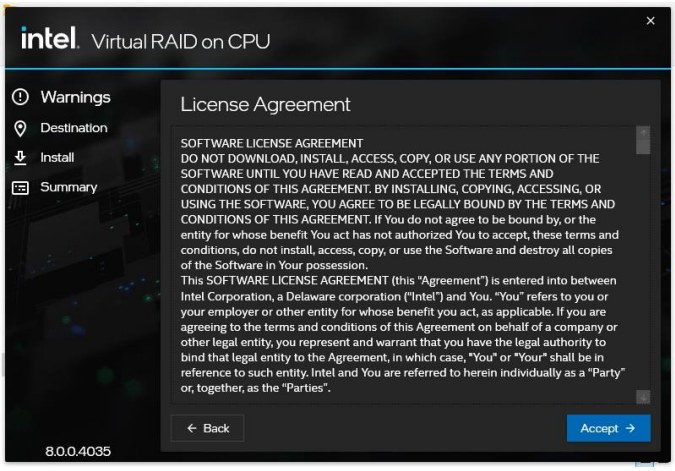


Step 5. Click **Finish** to complete setup.

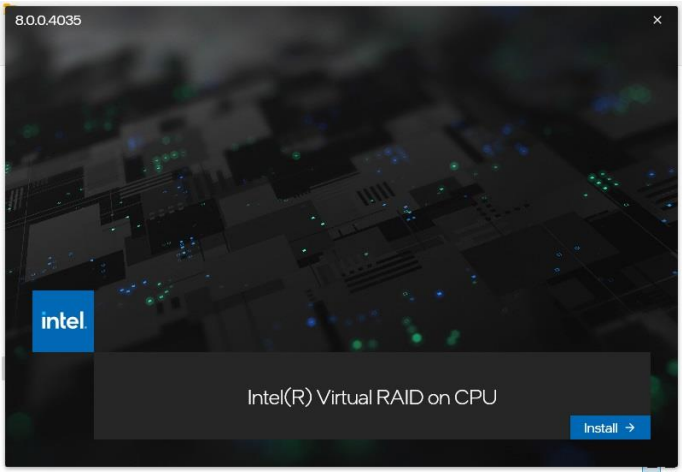
4.6 Install VROC Driver

All drivers can be found on the Avalue Official Website:
http://www.avalue.com.tw.

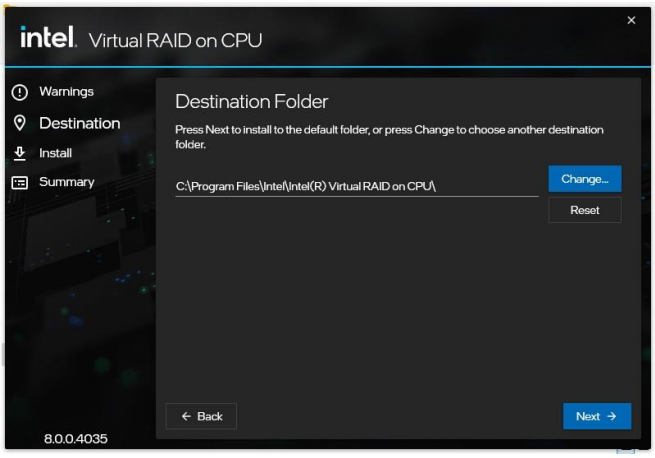
Note: The installation procedures and screen shots in this section are based on Windows 10 operation system.



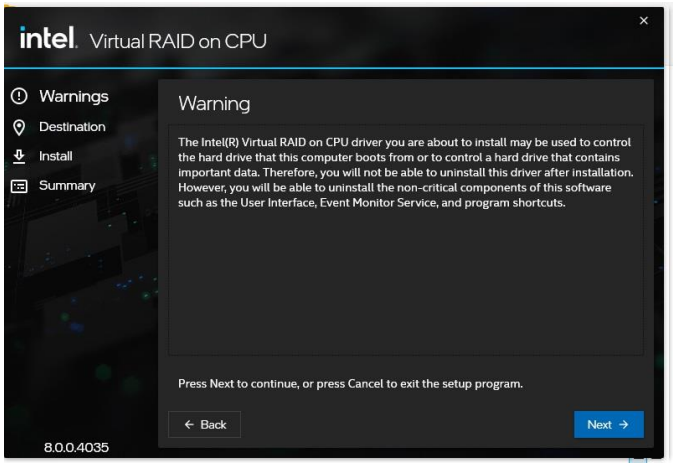
Step 3. Click **Accept**.



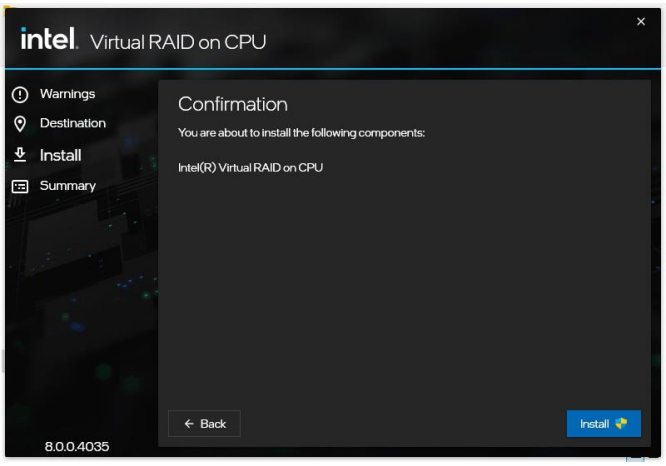
Step 1. Click **Install** to continue installation.



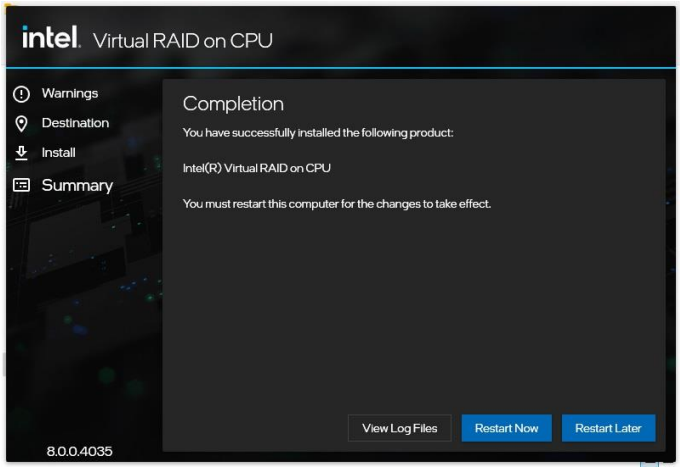
Step 4. Click **Next**.



Step 2. Click **Next**.

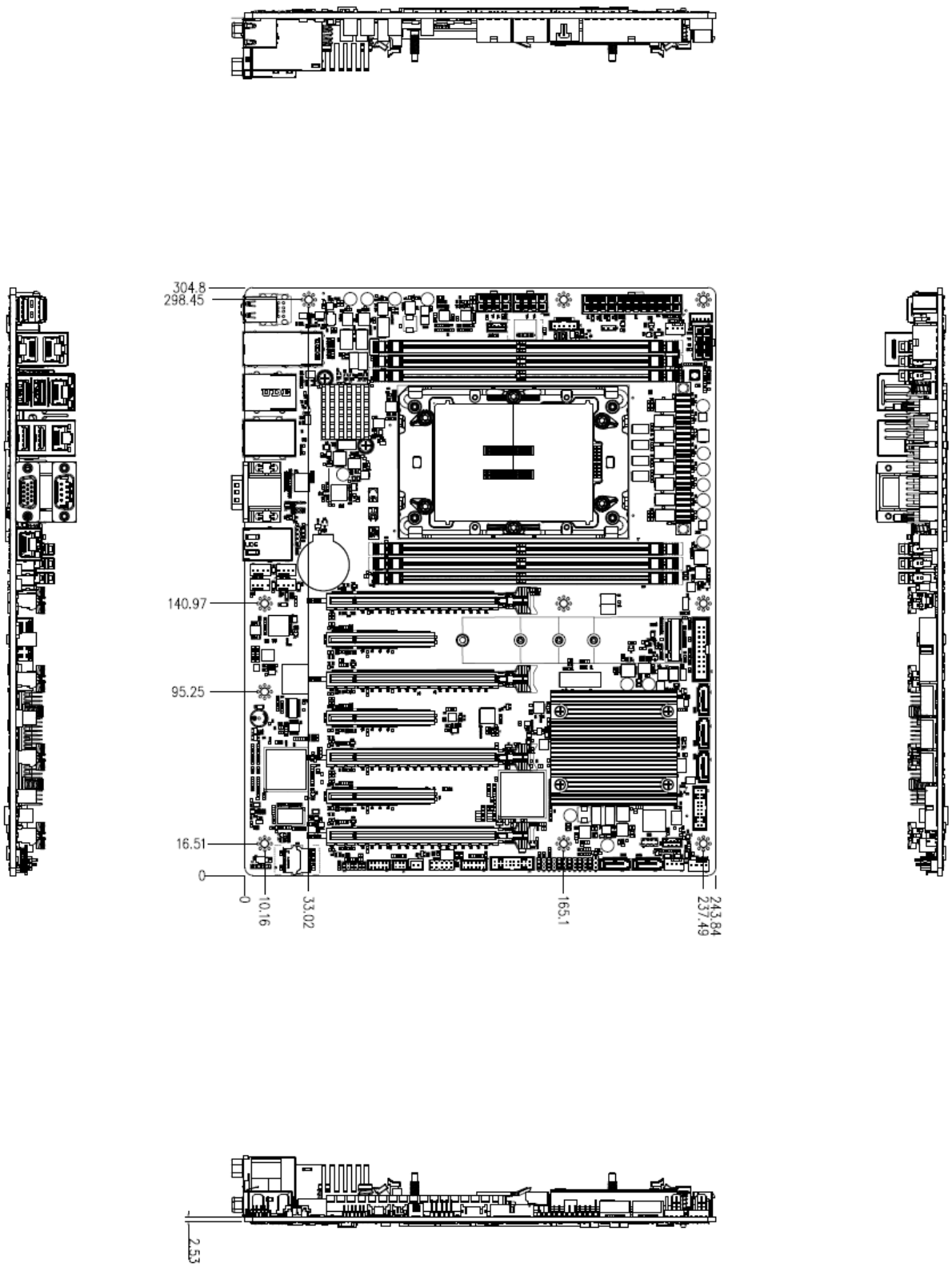


Step 5. Click **Install**.



Step 6. Setup completed.

5. Mechanical Drawing



Unit: mm