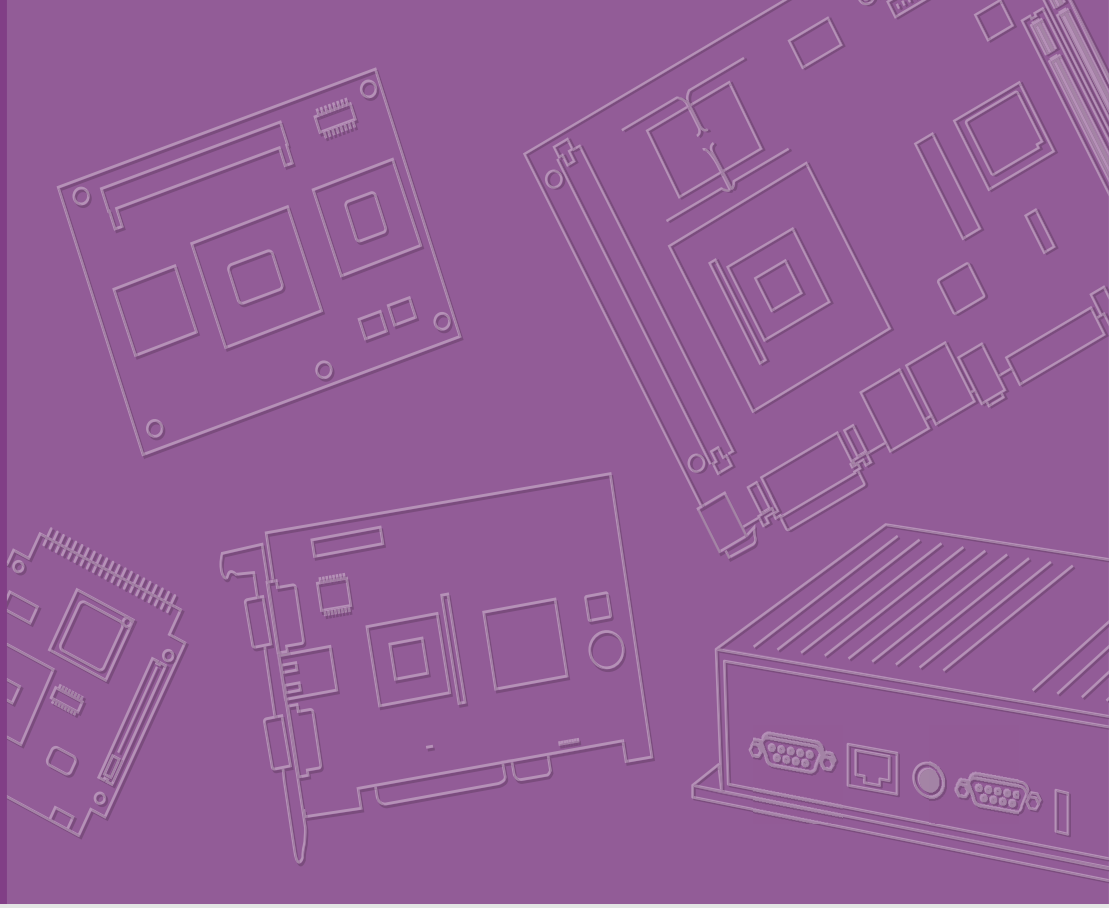


User Manual

SOM-5885

CPU Computer on Module

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2024 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated, or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. The information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties that may result from its use.

Acknowledgments

AMD is a trademark of AMD Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (2 Years)

Advantech warrants 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 that have been repaired or altered by persons other than repair personnel authorized by Advantech, or products that have been subject to misuse, abuse, accident, or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced free of charge during the warranty period. For out-of-warranty repairs, customers will be billed according to the cost of replacement materials, service time, and freight. Please consult your dealer for more details.

If you believe your product to be defective, follow the steps outlined below.

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any onscreen messages displayed when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain a return merchandise authorization (RMA) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a completed Repair and Replacement Order Card, and a proof of purchase date (such as a photocopy of your sales receipt) into a shippable container. Products returned without a proof of purchase date are not eligible for warranty service.
5. Write the RMA number clearly on the outside of the package and ship the package prepaid to your dealer.

Part No. 2006588503 Edition 4

Printed in Taiwan March 2026

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications when shielded cables are used for external wiring. We recommend the use of shielded cables. This type of cable is available from Advantech. Please contact your local supplier for ordering information.

Test conditions for passing also include the equipment being operated within an industrial enclosure. In order to protect the product from damage caused by electrostatic discharge (ESD) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class B

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

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

FM

This equipment has passed FM certification. According to the National Fire Protection Association, work sites are categorized into different classes, divisions, and groups based on hazard considerations. This equipment is compliant with the specifications for Class I, Division 2, Groups A, B, C, and D indoor hazards.

Technical Support and Assistance

1. Visit the Advantech website at www.advantech.com/support to obtain the latest product information.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before calling:
   - Product name and serial number
   - Description of your peripheral attachments
   - Description of your software (operating system, version, application software, etc.)
   - A complete description of the problem
   - The exact wording of any error messages

Warnings, Cautions, and Notes

Warning! *Warnings indicate conditions that could cause personal injury if not observed!*



Caution! *Cautions are included to help prevent hardware damage and data loss. For example,*



"Batteries are at risk of exploding if incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type as recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions."

Note! *Notes provide additional and/or optional information.*



Document Feedback

To assist us with improving this manual, we welcome all comments and constructive criticism. Please send all feedback in writing to support@advantech.com.

Selection Guide Including Part Numbers

Part No.	CPU	Cores	Base Freq	Max Boost Freq	Default TDP	cTDP	LLC	DDR5 SODIMM	PCIe Switch	iBECC	Thermal solution	Operating Temp
SOM-5885C7HV-S4A1	Core™ Ultra 7 165H	16	1.4GHz / 0.9GHz	5GHz	45W	20W-45W	24M	Non-ECC	Yes	Yes	Active	0 ~ 60°C
SOM-5885C7H-S4A1	Core™ Ultra 7 155H	16	1.4GHz / 0.9GHz	4.8GHz	45W	20W-45W	24M	Non-ECC	No	Yes	Active	0 ~ 60°C
SOM-5885C5H-S2A1	Core™ Ultra 5 125H	14	1.2GHz / 0.7GHz	4.5GHz	45W	20W-45W	18M	Non-ECC	No	Yes	Active	0 ~ 60°C
SOM-5885C7UV-S7A1	Core™ Ultra 7 165U	12	1.7GHz / 1.2GHz	4.9GHz	28W	12W-28W	12M	Non-ECC	No	Yes	Active	0 ~ 60°C
SOM-5885C5HA-S2A1	Core™ Ultra 5 125H	14	1.2GHz / 0.7GHz	4.5GHz	45W	20W-45W	18M	Non-ECC	No	Yes	Active	0 ~ 60°C

Packing List

Before system installation, check that the items listed below are included and in good condition. If any item does not accord with the list, contact your dealer immediately.

Part No.	Description	Quantity
-	SOM-5885 COM module	1
1970005918T001	Heatspreader for the SOM-5885	1

Development Board

Part No.	Description
SOM-DB5830-00A3	COMe Devel. Board COMe R3.1 Type6 pin-out (LVDS) 0 ~ 60°C
SOM-DB5830A-00A3	COMe Devel. Board COMe R3.1 Type6 pin-out (eDP) 0 ~ 60°C

Optional Accessories

Part No.	Description
1970005036T011	Semi-Cooler 125 x 95 x 33.2 mm with 12V Fan
1970005940T031	QFCS 125x95x26.2mm
SOM-MZ20-01A1	USB4.0 card for SOM-5885

Safety Precautions - Static Electricity

Follow these simple precautions to protect yourself from harm and the products from damage.

- To avoid electrical shock, always disconnect the power from the PC chassis before manual handling. Do not touch any components on the CPU card or other cards while the PC is powered on.
- Disconnect the power before making any configuration changes. A sudden rush of power after connecting a jumper or installing a card may damage sensitive electronic components.

Safety Instructions

1. Read these safety instructions carefully.
2. Retain this user manual for future reference.
3. Disconnect the equipment from all power outlets before cleaning. Use only a damp cloth for cleaning. Do not use liquid or spray detergents.
4. For pluggable equipment, the power outlet socket must be located near the equipment and easily accessible.
5. Protect the equipment from humidity.
6. Place the equipment on a reliable surface during installation. Dropping or letting the equipment fall may cause damage.
7. The openings on the enclosure are for air convection. Protect the equipment from overheating. Do not cover the openings.
8. Ensure that the voltage of the power source is correct before connecting the equipment to a power outlet.
9. Position the power cord away from high-traffic areas. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect it from the power source to avoid damage from transient overvoltage.
12. Never pour liquid into an opening. This may cause fire or electrical shock.
13. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
14. If any of the following occurs, have the equipment checked by service personnel:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture.
    - The equipment is malfunctioning, or does not operate according to the user manual.
    - The equipment has been dropped and damaged.
    - The equipment shows obvious signs of breakage.
15. Do not leave the equipment in an environment with a storage temperature of below -20°C (-4°F) or above 60°C (140°F) as this may damage the components. The equipment should be kept in a controlled environment.
16. CAUTION: Batteries are at risk of exploding if incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.
17. In accordance with IEC 704-1:1982 specifications, the sound pressure level at the operator's position should not exceed 70 dB (A).

DISCLAIMER: This set of instructions is given according to IEC 704-1. Advantech disclaims all responsibility for the accuracy of any statements contained herein.

Contents

Chapter 1 General Information 1

1.1 Introduction 2
Table 1.1: Acronyms 3
1.2 Functional Block Diagram 4
1.3 Product Specifications 5
1.3.1 Compliance 5
1.3.2 Feature List 5
Table 1.2: Feature List 5
1.3.3 Processor System 6
Table 1.3: Processor System 6
1.3.4 Memory 6
1.3.5 Graphics/Audio 6
Table 1.4: Graphics/Audio 6
1.3.6 Expansion Interfaces 7
Table 1.5: PEG 7
Table 1.6: PCI Express 7
1.3.7 LPC 7
1.3.8 Serial Bus 7
1.3.9 I/O 8
Table 1.7: USB 2.0 8
Table 1.8: BIOS 9
1.3.10 Power Management 9
1.3.11 Environment 10
1.3.12 MTBF 10
1.3.13 OS Support 11
1.3.14 Advantech iManager 11
1.3.15 Power Consumption 11
Table 1.9: Power Consumption Table (Watts) 11
1.3.16 Performance 11
1.3.17 Pin Descriptions 12

Chapter 2 Mechanical Information 13

2.1 Board Information 14
Figure 2.1 Board Chips – Front 14
Figure 2.2 Board Chips – Rear 14
2.2 Mechanical Diagram 15
Figure 2.3 Board Mechanical Diagram – Front 15
Figure 2.4 Board Mechanical Diagram – Rear 15
Figure 2.5 Board Mechanical Diagram – Side 1 16
Figure 2.6 Board Mechanical Diagram – Side 2 16
2.3 Assembly Diagram 17
Figure 2.7 Assembly Diagram 17
2.4 Assembly Diagram 18
Figure 2.8 CPU Height and Tolerance 18

Chapter 3 AMI BIOS 19

3.1 Introduction 20
Figure 3.1 Setup Program Initial Screen 20
3.2 Entering Setup 20
3.3 Main Setup 21
Figure 3.2 Main Setup Screen 21

3.4 Advanced BIOS Features Setup 22
Figure 3.3 Advanced BIOS Features Setup Screen 22
3.4.1 RC ACPI Settings 23
Figure 3.4 RC ACPI Settings 23
3.4.2 CPU Configuration 25
Figure 3.5 CPU Configuration 25
Figure 3.6 CPU Configuration 25
Figure 3.7 Efficient-core Information 27
Figure 3.8 Performance-core 27
3.4.3 Power & Performance 28
Figure 3.9 Power & Performance 28
Figure 3.10 CPU-Power Management Control 29
Figure 3.11 Current Turbo Settings 31
Figure 3.12 Current Turbo Ratio Limit Settings 32
Figure 3.13 Config TDP Configurations 32
Figure 3.14 GT/Media-Power Management Control 34
3.4.4 PCH-FW Configuration 35
Figure 3.15 PCH-FW Configuration 35
3.4.5 ACPI D3Cold Settings 36
Figure 3.16 ACPI D3Cold settings 36
3.4.6 AMT Configuration 38
Figure 3.17 AMT Configuration 38
Figure 3.18 ASF Configuration 39
Figure 3.19 Secure Erase Configuration 40
Figure 3.20 One Click Recovery (OCR) Configuration 41
3.4.7 Trusted Computing 42
Figure 3.21 Trusted Computing 42
3.4.8 ACPI Settings 43
Figure 3.22 ACPI Settings 43
3.4.9 SMART Settings 44
Figure 3.23 SMART Settings 44
3.4.10 Embedded Controller 45
Figure 3.24 Embedded controller 45
3.4.11 Serial Port Console Redirection 46
Figure 3.25 Serial Port 1 Configuration 46
Figure 3.26 Serial Port 2 Configuration 47
Figure 3.27 Serial Port Console Redirection 48
Figure 3.28 Console Redirection Settings 49
3.4.12 PCI Subsystem Settings 50
Figure 3.29 ACPI Report Method Configuration 50
3.4.13 USB Configuration 51
Figure 3.30 USB Configuration 51
3.4.14 Network Stack Configuration 52
Figure 3.31 Network Stack Configuration 52
3.4.15 NVMe Configuration 53
Figure 3.32 NVMe Configuration 53
3.4.16 Dual BIOS Configuration 54
Figure 3.33 Dual BIOS Configuration 54
3.4.17 Intel® Ethernet Controller I226-LMvP 55
Figure 3.34 Intel® Ethernet Controller I226-LMvP 55
3.5 Chipset Setup 56
Figure 3.35 Chipset Setup 56
3.5.1 System Agent (SA) Configuration 57
Figure 3.36 System Agent (SA) Configuration 57
Figure 3.37 Memory Configuration 58
Figure 3.38 Graphics Configuration 59
Figure 3.39 VMD Setup Menu 60
3.5.2 PCI Express Configuration 61
Figure 3.40 PCI Express Configuration 61
Figure 3.41 PCIE Clocks 62

Figure 3.42PCIE Root Port 63
Figure 3.43SATA Drives 64
Figure 3.44USB Configuration 65
Figure 3.45Security Configuration 66
Figure 3.46HD Audio Subsystem Configuration Settings 67
3.5.3 PCH-IO Configuration 68
Figure 3.47PCH-IO Configuration 68
3.6 Security Chipset 69
Figure 3.48Security Chipset 69
3.6.1 Secure Boot 70
Figure 3.49Secure Boot 70
3.6.2 Boot Setup 71
Figure 3.50Boot Setup 71
3.7 Save & Exit 72
Figure 3.51Save & Exit 72
3.8 MEBx 73
Figure 3.52MEBx 73

Chapter 4 S/W Introduction & Installation 75

4.1 S/W Introduction 76
4.2 Driver Installation 76
4.2.1 Windows Driver Setup 76
4.2.2 Other OS 76
4.3 Advantech iManager 77

Appendix A Pin Assignment 79

A.1 SOM-5885 Pin Assignment 80
Table A.1: SOM-5885 Pin Assignments 80

Appendix B Watchdog Timer 87

B.1 Programming the Watchdog Timer 88
Table B.1: Programming the Watchdog Timer 88

Appendix C Programming GPIO 89

C.1 GPIO Register 90
Table C.1: GPIO Register 90

Appendix D System Assignments 91

D.1 System I/O Ports 92
Table D.1: System I/O Ports 92
D.2 Interrupt Assignments 93
Table D.2: Interrupt Assignments 93
D.3 1st MB Memory Map 94
Table D.3: 1st MB Memory Map 94

Chapter 1

General Information

This chapter details background information on the SOM-5885 CPU Computer on Module.

Sections include:

- Introduction
- Functional Block Diagram
- Product Specifications

1.1 Introduction

The SOM-5885 is a COM Express Type 6 Basic Module with a 14th Gen Intel® Core™ processor. It delivers octa-core computing performance with 45W TDP, while providing IXe LPG graphics, and Advantech's Edge AI Suite software toolkit.

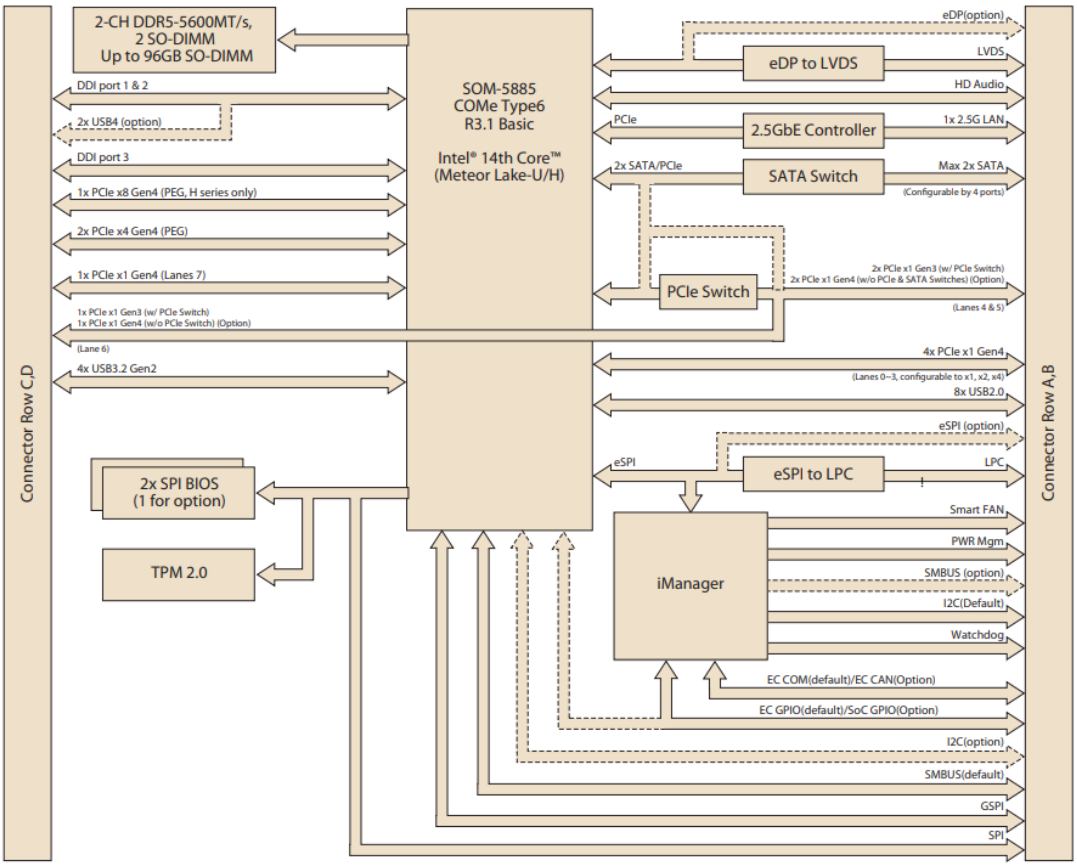
The SOM-5885 supports up to 96GB DDR5 5600 RAM, offering a 1.7x increase in computing performance and 1.5x increase in 3D graphics performance compared to previous generations. It supports numerous high-speed I/O interfaces such as PCIe Gen4 (16GT/s), 2.5GBase-T, and USB 3.2 Gen2 (10Gbps). The module can support four independent 4K displays via three DisplayPort 1.4 / HDMI 2.1 ports and one optional eDP or LVDS. It can also be configured with up to two 8K HDR outputs. Additional features include TPM 2.0 on-board, 8.5 to 20V power input, and a wide operating temperature range of 0 ~ 60°C (32 ~ 140°F). The SOM-5885 comes with a heat spreader and QFCS solution.

Advantech iManager (SUSI 4) meets diverse embedded application requirements by providing a multi-level watchdog timer, voltage and temperature monitoring, thermal protection through processor throttling, LCD backlight control, and embedded storage for customized information. When combined with Advantech WISE-PaaS/RMM, it allows for remote device monitoring and control over the Internet, facilitating easy maintenance. All Advantech Basic modules integrate iManager and WISE-PaaS/RMM providing added value for a wide range of customer applications.

Table 1.1: Acronyms

Term	Define
AC'97	Audio CODEC (Coder-Decoder)
ACPI	Advanced Configuration Power Interface – standard for implementation of power saving modes in PC-AT systems
BIOS	Basic Input Output System – firmware in a PC-AT system that is used to initialize system components before handing control over to the operating system
CAN	Controller-area network (CAN or CAN bus) is a vehicle bus standard designed to allow microcontrollers to communicate with each other within a vehicle without a host computer.
DDI	Digital Display Interface – containing DisplayPort, HDMI/DVI, and SDVO
EAPI	Embedded Application Programmable Interface Software interface for COM Express® specific industrial functions – System information – Watchdog timer – I^2C Bus – Flat-panel brightness control – User storage area – GPIO
GbE	Gigabit Ethernet
GPIO	General purpose input output
HDA	Intel High Definition Audio (HD Audio) refers to the specification released by Intel in 2004 for delivering high-definition audio that is capable of playing back more channels at higher quality than AC'97.
I^2C	Inter Integrated Circuit – 2-wire (clock and data) signaling scheme allowing communication between integrated circuits, primarily used to read and load register values
ME	Management Engine
PC-AT	"Personal Computer – Advanced Technology" – an IBM trademark term used to refer to Intel-based personal computers in the 1990s
PEG	PCI Express Graphics
RTC	Real Time Clock – battery-backed circuit in PC-AT systems that keeps system time and date as well as certain system setup parameters
SPD	Serial Presence Detect – refers to serial EEPROM on DRAMs that has DRAM Module configuration information
TPM	Trusted Platform Module – a chip to enhance the security features of a computer system
UEFI	Unified Extensible Firmware Interface
WDT	Watch Dog Timer

1.2 Functional Block Diagram



1.3 Product Specifications

1.3.1 Compliance

- PICMG COM.0 (COM Express) Revision 3.1
- Basic Size - 125 x 95 mm (4.9 x 3.7 in)
- Pin-out Type 6 compatible

1.3.2 Feature List

Table 1.2: Feature List

Feature Type	Connector Row	Feature	Type 6 Definition Min/Max	SOM-5885
Display	C-D	DDIs 1 - 3	0 / 3	3
Display	A-B	LVDS Channel A	0 / 1	1
Display	A-B	LVDS Channel B	0 / 1	1
Display	A-B	eDP on LVDS CH A pins	0 / 1	1
Display	A-B	VGA Port	0 / 1	0
Expansion	A-B	PCI Express Lanes 0 - 5	1 / 6	6
Expansion	A-B	PCI Express Lanes 6 - 15	0 / 2	2
Expansion	A-B	PCI Express Lanes 16 - 31	0 / 16	0
Expansion	C-D	PCI Express Graphics (PEG)	0 / 1	1
Expansion	A-B	LPC Bus or eSPI	1 / 1	1
IO	A-B	1Gb LAN Port 0	1 / 1	1
IO	A-B	SATA Ports	1 / 4	4
IO	A-B	HDA Digital Interface	0 / 1	1
IO	A-B	USB 2.0 Ports	4 / 8	8
IO	A-B	USB0 Client	0 / 1	0
IO	A-B	USB 3.0 Ports	0 / 2	2
IO	C-D	USB 3.0 Ports	0 / 2	2
IO	C-D	Rapid Shutdown	0 / 1	1
IO	A-B	SDIO (muxed on GPIO)	0 / 1	0
IO	A-B	General Purpose I/O	8 / 8	8
IO	A-B	Watchdog Timer	0 / 1	1
IO	A-B	Speaker Out	1 / 1	1
IO	A-B	Carrier Board BIOS Flash Support	0 / 1	1
IO	A-B	Reset Functions	1 / 1	1
IO	A-B	Trusted Platform Module (TPM_PP)	0 / 1	1
Serial	A-B	Serial Ports 1 - 2	0 / 2	2
Serial	A-B	CAN interface on SER1	0 / 1	1
Serial	A-B	SPI (Devices)	1 / 2	1
Serial	A-B	SMBus	1 / 1	1
Serial	A-B	I2C	1 / 1	1

1.3.3 Processor System

Table 1.3: Processor System

CPU	Std. Freq.	Max. Turbo Freq.	Cores	Cache (MB)	cTDP(W)
Core® Ultra 7-165H	1.4GHz/0.9GHz	5GHz	16C (6P+8E+2LPE)	24	20W-45W
Core® Ultra 7-155H	1.4GHz/0.9GHz	4.8GHz	16C (6P+8E+2LPE)	24	20W-45W
Core® Ultra 5-125H	1.2GHz/0.7GHz	4.5GHz	14C (4P+8E+2LPE)	18	20W-45W
Core® Ultra 7-165U	1.7GHz/1.2GHz	4.9GHz	12C (2P+8E+2LPE)	12	12W-28W
Core® Ultra 7-155U	1.7GHz/1.2GHz	4.8GHz	12C (2P+8E+2LPE)	12	12W-28W
Core® Ultra 5-125U	1.3GHz/0.8GHz	4.3GHz	12C (2P+8E+2LPE)	12	12W-28W

1.3.4 Memory

There are a total of 2 memory sockets on the SOM-5885. The topside has 2 by default. This solution supports max 96GB capacity (non-ECC memory modules with all SKUs.) with 260-pin SODIMM sockets (dual-channel).

1.3.5 Graphics/Audio

Graphics Core: Intel® Xe LPG supports DX12.2, OGL4.6, OCL3.0, and MPEG2/ AVC/HEVC/VP9/JPEG/AV1 HW decode/encode/transcode acceleration.

Table 1.4: Graphics/Audio

CPU	Graphics Core	Base Freq.	Max Freq.
Core® Ultra 7-165H	Intel® Xe LPG	1.4GHz	2.3GHz
Core® Ultra 7-155H	Intel® Xe LPG	1.4GHz	2.25GHz
Core® Ultra 5-125H	Intel® Xe LPG	1.2GHz	2.2GHz
Core® Ultra 7-165U	Intel® Xe LPG	1.7GHz	2.1GHz
Core® Ultra 7-155U	Intel® Xe LPG	1.7GHz	1.95GHz
Core® Ultra 5-125U	Intel® Xe LPG	1.3GHz	1.85GHz

- **Dual display:**
  - LVDS+DDI1
  - LVDS+DDI2
  - LVDS+DDI3
- **Triple display:**
  - DDI1+DDI2+LVDS
  - DDI1+DDI2+DDI3
- **Quad display**:
  - LVDS+DDI1+DDI2+DDI3

1.3.6 Expansion Interfaces

1.3.6.1 PEG

PEG: Supports 16 lanes by default, compliant with PCIe Gen4 (16.0 GT/ s) specifications, configurable to PEG x8, x4, x1.

*Note: The U series has no PEGX8.

Table 1.5: PEG

Type 6		Row C, D															
		P0	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
Default	Config	x8								x4				x4			
Option 1		x4				-				x2		-		x2		-	
Option 2		x1	-	-	-	-	-	-	-	x1	-	-	-	x1	-	-	-

1.3.6.2 PCI Express

PCI Express: Supports 8 lanes by default, PCIe x1 compliant to 4 x PCIe x1 Gen4 (x1, x2, x4) (16.0 GT/s), 1 x PCIe x1 Gen4 and 3 x PCIe x1 Gen3 (8.0 GT/s) specifications. Several configurable combinations may need BIOS modification. Please contact Advantech sales or FAE for more details.

Table 1.6: PCI Express

Type 6		Rows A, B						Rows C, D	
		P0	P1	P2	P3	P4	P5	P6	P7
Default	Config	x1	x1	x1	x1	x1 (Gen3)	x1 (Gen3)	x1 (Gen3)	x1 (Gen4)
Option 1		x2		x1	x1	-	-	x1 (Gen4)	x1 (Gen4)
Option 2		x2		x2		-		x2 (Gen4)	

*Note: In the default configuration, only SOM-5885C7HV-S4A1 has both a PCIe switch and a SATA switch. The SOM-5885C7H-S4A1 has no PCIe switch, and can use option 1 and option 2 configurations.

1.3.7 LPC

Supports Low Pin Count (LPC) 1.1 specifications, without DMA or bus mastering. It enables connection to Super I/O, an embedded controller, or TPM. The clock is 24MHz LPC.

1.3.8 Serial Bus

1.3.8.1 SMBus

Supports SMBus 2.0 specifications.

1.3.8.2 I^2C Bus

Supports I²C bus 7-bit and 10-bit address modes. It supports standard mode up to 100 Kb/s, and fast mode up to 400 Kb/s.

1.3.9 I/O

1.3.9.1 Gigabit Ethernet

Ethernet: Intel® I226 Gigabit LAN supports 10/100/1000 Mbps & 2.5 Gbps Speed.

1.3.9.2 SATA

Supports 2 x SATA Gen3 (6.0 Gb/s), backward-compliant to SATA Gen2 (3.0 Gb/s) and Gen1 (1.5 Gb/s). The maximum data rate is 600 MB/s. It supports AHCI 1.3.1 mode (It does not support IDE mode).

1.3.9.3 USB 4.0 / USB 3.2 / USB 2.0

SOM-5885 supports 2 x USB 4.0, 4 x USB 3.2 Gen2 (10 Gbps) ports and 8 x USB 2.0 (480 Mbps) ports which are reverse compatible to USB 1.x. For USB 3.2, it supports LPM (U0, U1, U2, and U3) for power efficiency.

Notice: To meet USB 3.2 Gen2 performance, Advantech strongly recommends using a certified cable.

1.3.9.4 USB 2.0

Table 1.7: USB 2.0

Type 6	**P0**	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**
SoC	P0	P1	P2	P3	P4	P5	P6	P7
Type 6	OC_01		OC_23		OC_45		OC_67	
SoC USB_OC#	OC_0		OC_1		OC_1		OC_3	

1.3.9.5 SPI Bus

Supports BIOS flash only. The SPI clock can be 14MHz, with capacity up to 256Mb.

1.3.9.6 GPIO

8 x programmable general purpose input or output (GPIO).

1.3.9.7 Watchdog Timer

It supports multi-level watchdog time-out output. it provides 1-65535 levels, from 100ms to 109.22 minute intervals.

1.3.9.8 Serial Ports

2 x 2-wire serial ports (Tx/Rx) supports 16550 UART compliance:

- Programmable FIFO or character mode
- 16-byte FIFO buffer on transmitter and receiver in FIFO mode
- Programmable serial-interface characteristics: 5-, 6-, 7-, or 8-bit character
- Even, odd, or no parity bit selectable
- 1, 1.5, or 2 stop bit selectable
- Baud rate up to 115.2K

1.3.9.9 TPM

Supports TPM 2.0 module by default.

1.3.9.10 Smart Fan

There is support for 2 x Fan PWM control signals and 2 x tachometer inputs for fan speed detection. There is one on the module via the connector and the other on the carrier board following PICMG COM Express R3.1 specifications.

1.3.9.11 BIOS

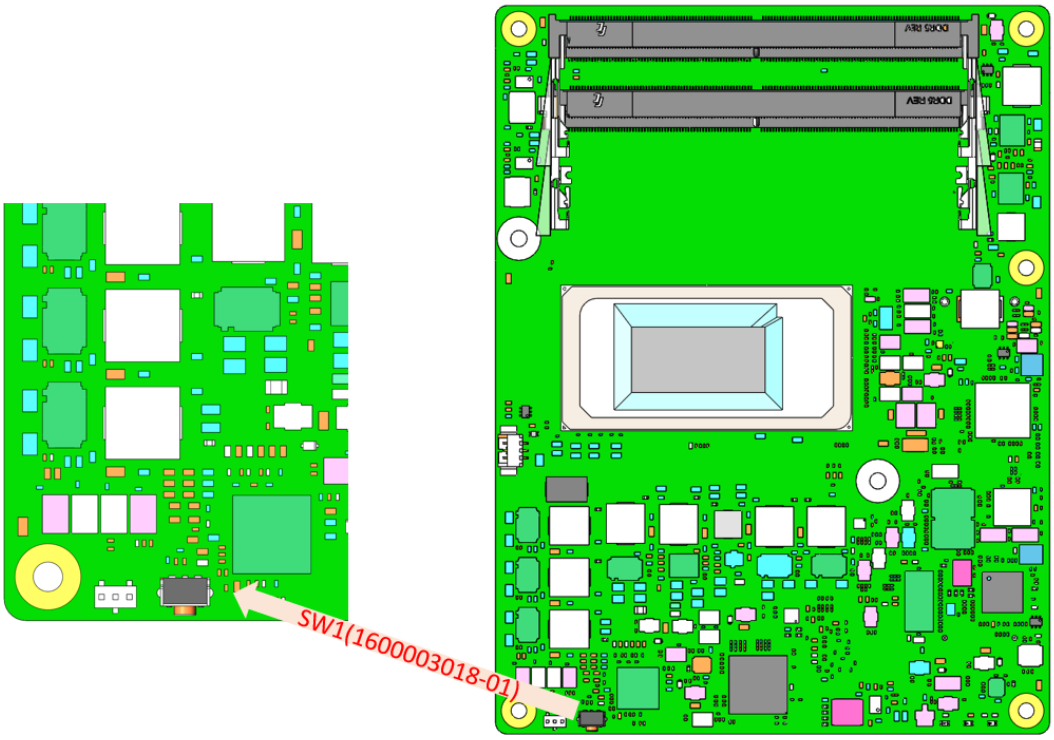
The BIOS chip is placed on the module by default. Users can place the BIOS chip on the carrier board with the appropriate design and jumper setting in BIOS_DIS#[1:0].

Table 1.8: BIOS

BIOS_DIS#0	BIOS_DIS#1	Boot-Up Destination/Function
Open	Open	Boot from the Module's SPI BIOS
Open	GND	SPI_CS0# to Carrier Board, SPI_CS1# to Module
GND	GND	SPI_CS0# to Module, SPI_CS1# to Carrier Board

Note: If system COMS is cleared, Advantech strongly suggests going to the BIOS setup menu and loading the default settings on the first boot-up.

The standard module has no jumper at SW1, so BIOS settings are kept without an RTC coin battery. If you need to restore the BIOS to default settings, follow the steps below:



1. Remove the coin battery.
2. Push the button on SW1.
3. Turn on the power supply.
4. The system will boot up a few times.
5. The BIOS will load the default settings.

1.3.10 Power Management

1.3.10.1 Power Supply

Both ATX and AT power modes are supported. VSB is for suspended power and is optional if not required by standby (suspend-to-RAM) support. The RTC battery is optional if datekeeping/timekeeping is not required.

- **VCC:** 8.5V (9V-5%) – 20V (19V+5%)
- **VSB:** 5V +/- 5% (Suspend power)
- **RTC Battery Power:** 2.0V – 3.3V

1.3.10.2 PWROK

Power-good from the main power supply. A high value indicates the power level is good. This signal can be used to postpone module startup to allow carrier-based FPGAs or other configurable devices to have the time programmed.

1.3.10.3 Power Sequence

According to PICMG COM Express COM.0 R 3.1 specifications.

1.3.10.4 Wake Event

Various wake event support allows users to apply different scenarios.

- **Wake-on-LAN (WOL):** Wake to S0 from S4/S5
- **USB Wake:** Wake to S0 from S4
- **PCIe Device Wake:** depends on user inquiry and may need customized BIOS
- **LPC Wake:** depends on user inquiry and may need customized BIOS

1.3.10.5 Advantech S5 ECO Mode (Deep Sleep Mode)

Advantech iManager provides additional features allowing the system to enter a very low suspended power mode – S5 ECO mode. In this mode, the module will cut all power, including suspended and active power to the chipset, and keep an on-module controller active. Only power under 50mW will be consumed, meaning user battery packs can last longer. While this mode is enabled in the BIOS, the system (or module) only allows power button boot instead of other methods such as WOL.

1.3.11 Environment

1.3.11.1 Temperature

- **Operating:** 0 ~ 60°C (32 ~ 140°F)
- **Storage:** -40 ~ 85°C (-40 ~ 185°F)

1.3.11.2 Humidity

- **Operating:** 40°C @ 95% relative humidity, non-condensing
- **Storage:** 60°C @ 95% relative humidity, non-condensing

1.3.11.3 Vibrations

IEC60068-2-64: Random vibration test under operation mode, 3.5 Grms.

1.3.11.4 Drop Test (Shock)

Federal Standard 101 Method 5007 test procedure with standard packing.

1.3.11.5 EMC

CE EN55022 Class B and FCC Certifications: validated with standard development boards in the Advantech chassis.

1.3.12 MTBF

Please refer to the Advantech SOM-5885 Refresh Series Reliability Prediction report on the website: Link: http://com.advantech.com

1.3.13 OS Support

The mission of Advantech Embedded Software Services is to "Enhance quality of life with Advantech platforms and Microsoft Windows Embedded technology." We enable Windows Embedded software products on Advantech platforms to more effectively support the embedded computing community. Customers are freed from the hassle of dealing with multiple vendors (hardware suppliers, system integrators, embedded OS distributors) for projects. Our goal is to make Windows Embedded software solutions easily and widely available to the embedded computing community.

To install drivers, please connect to the website http://support.advantech.com.tw to download the setup file.

1.3.14 Advantech iManager

iManager supports APIs for GPIO, smart fan control, a multi-stage watchdog timer, temperature sensor, and hardware monitoring. It follows PICMG EAPI 1.0 specifications with backward compatibility.

1.3.15 Power Consumption

Table 1.9: Power Consumption Table (Watts)

VCC=12V, VSB=5V	Active Power Domain			Suspend Power Domain		Mechanical Off
Power State	S0 Max. Load	S0 Burn-in	S0 Idle	S5	S5 Deep Sleep	RTC (μA)
SOM-5885C7HV-S4A1	81.18W	66.05W	9.86W	0.74W	0.29W	4.54μA

Hardware Configuration:

1. MB: SOM-5885C7HV-S4A1
2. DRAM: 48GB DDR5 5600MHz x 2pcs.
3. Carrier board: SOM-DB5830-00A3, SOM-DB5830A-00A3

Test Condition:

1. Test temperature: room temperature (about 25°C)
2. Test voltage: rated voltage DC +12.0V
3. Test loading:
   - Maximum load mode: According to Intel thermal/power test tools.
   - Burn-in mode: Burn-in test V8.1 Pro (1023) for 64-bit Windows. (CPU, RAM, 2D&3D Graphics and Disk with 100%)
   - Idle mode: DUT power management off and not running any programs.
4. OS: Windows 10 Enterprise

1.3.16 Performance

To compare performance or benchmark data with other modules, please refer to the “Advantech COM Performance & Power Consumption Table.”

1.3.17 Pin Descriptions

Advantech provides useful checklists for schematic design and layout routing. The schematic checklist will specify details about each pin's electrical properties and how to connect it in different scenarios. The layout checklist will specify the layout constraints and recommendations for trace length, impedance, and other necessary information during design.

Please contact your regional Advantech branch office to acquire design documents and further advanced support.

Chapter 2

Mechanical Information

This chapter details mechanical information for the SOM-5885 CPU Computer on Module.

Sections include:

- Board Information
- Mechanical Drawings
- Assembly Drawings

2.1 Board Information

The figures below demonstrate the main chips on the SOM-5885 Computer on Module.

Be aware of these positions when designing your customer's carrier board to avoid mechanical damage and to improve thermal dissipation performance.

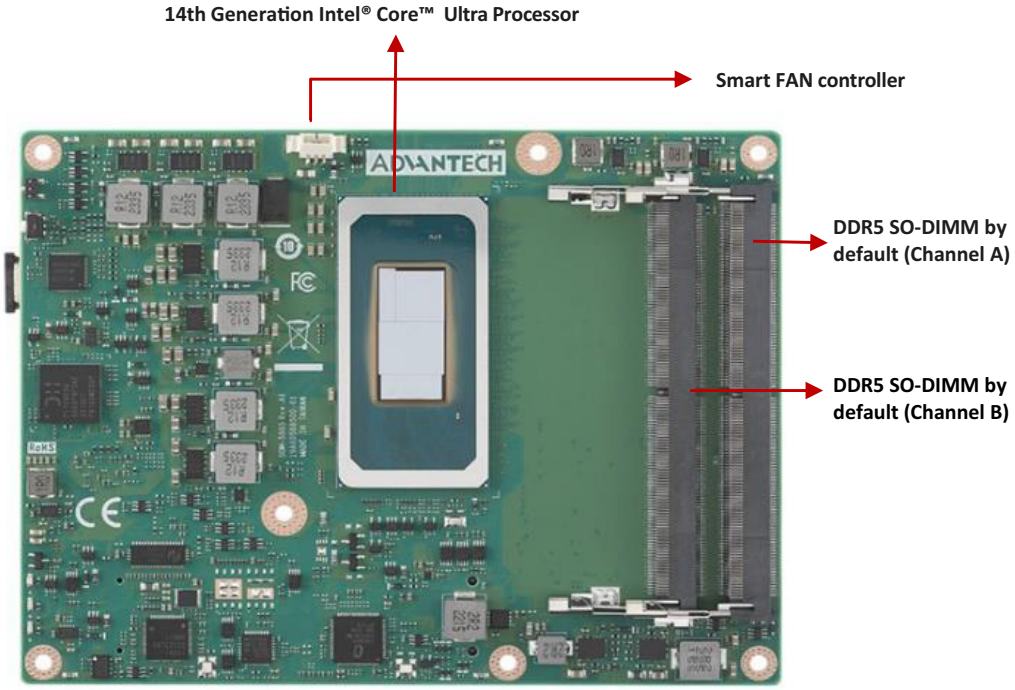


Figure 2.1 Board Chips – Front

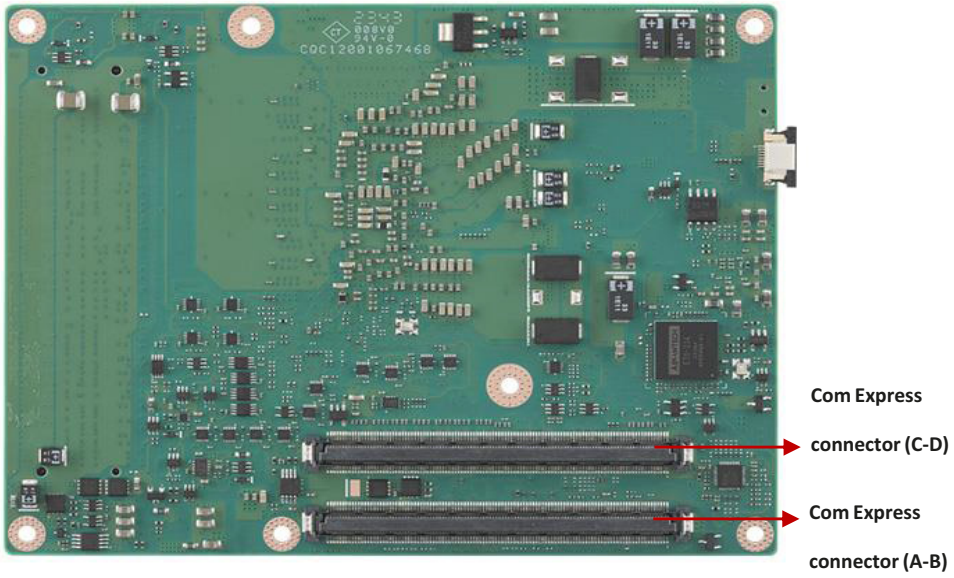


Figure 2.2 Board Chips – Rear

2.2 Mechanical Diagram

For more details regarding 2D/3D models, please visit the Advantech COM support service website: http://com.advantech.com.

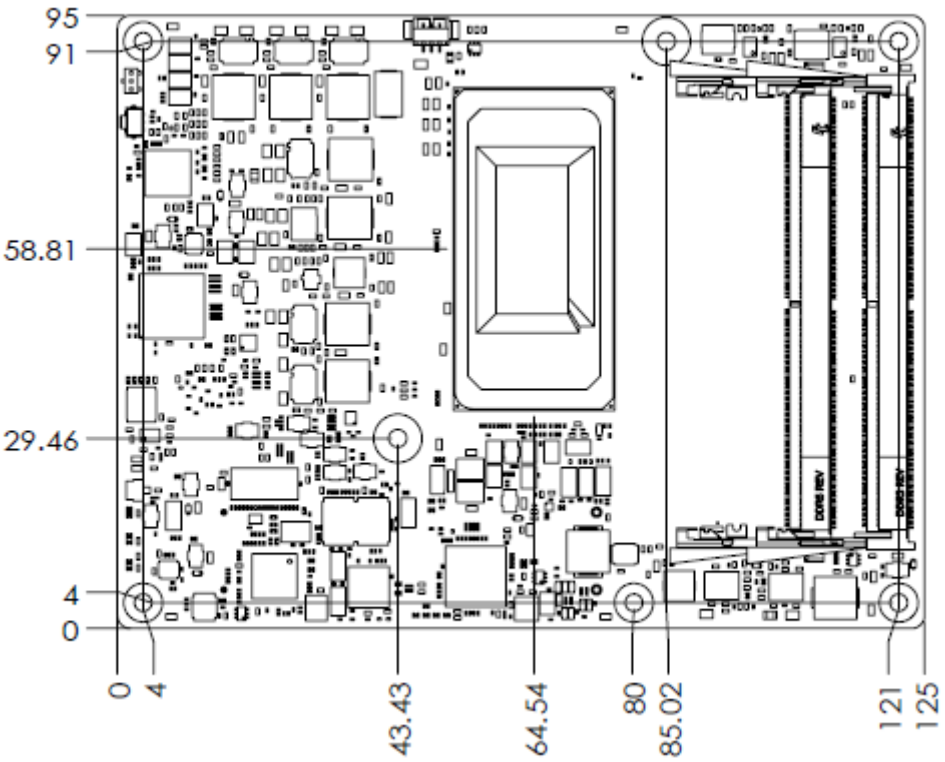


Figure 2.3 Board Mechanical Diagram – Front



Figure 2.4 Board Mechanical Diagram – Rear



Figure 2.5 Board Mechanical Diagram – Side 1

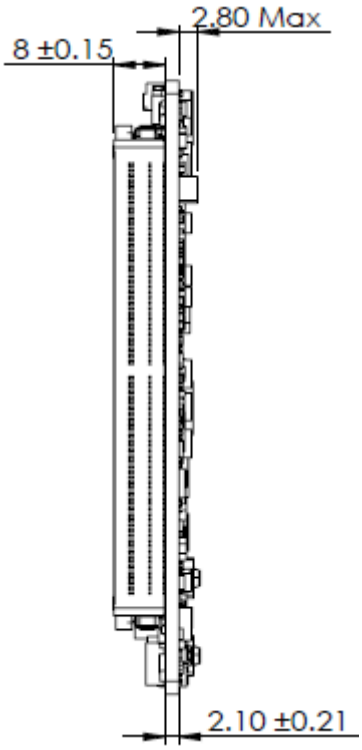


Figure 2.6 Board Mechanical Diagram – Side 2

2.3 Assembly Diagram

These figures demonstrate the order of assembly needed when attaching the thermal module and COM module to the carrier board.

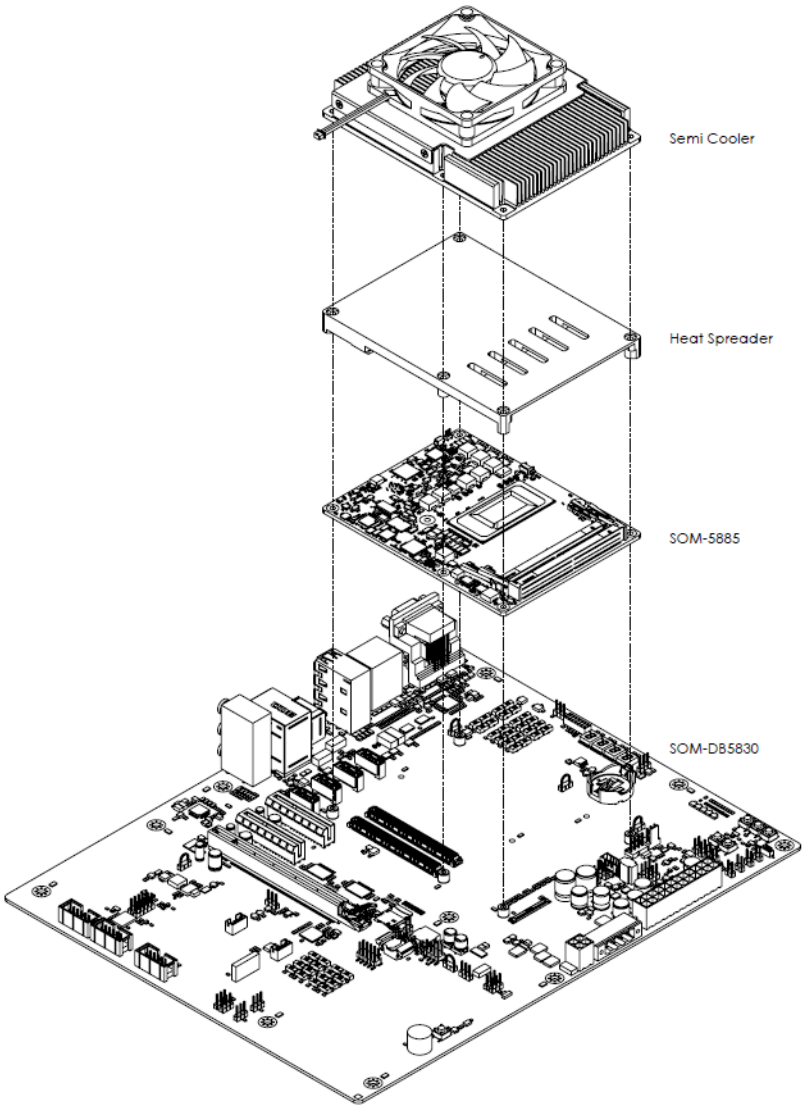


Figure 2.7 Assembly Diagram

There are 5 x reserved screw holes for the SOM-5885 used to assemble the heat spreader.

2.4 Assembly Diagram

Consider the CPU and chip height tolerance when designing your thermal solution.

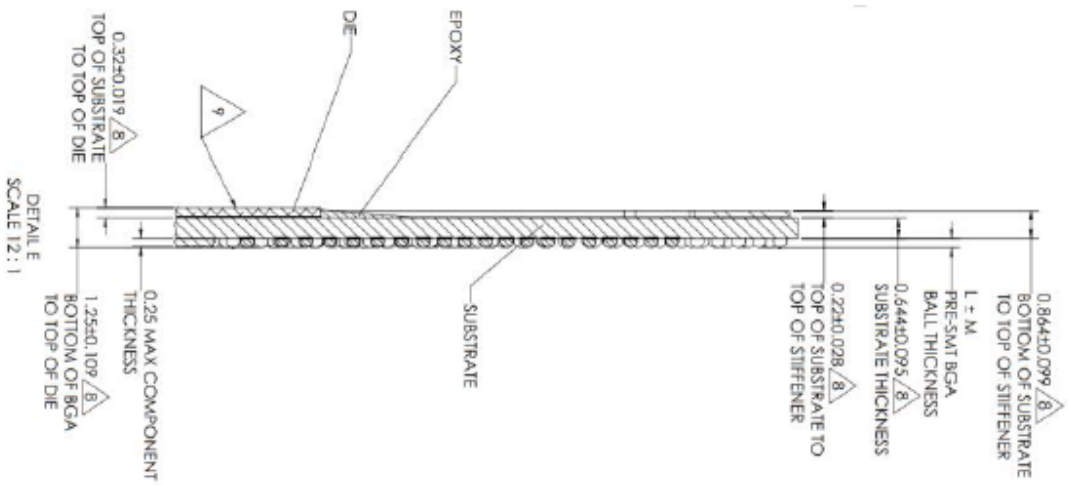


Figure 2.8 CPU Height and Tolerance

Chapter 3

AMI BIOS

This chapter details BIOS setup information for the SOM-5885 CPU Computer on Module.

Sections include:

- Introduction
- Entering Setup
- Hot/Operation Keys
- Exit BIOS Setup Utility

3.1 Introduction

AMI BIOS has been integrated into many motherboards for over a decade. The AMI BIOS Setup Utility enables users to modify the BIOS settings and control various system features. This chapter describes the basic navigation of the BIOS Setup Utility.



Figure 3.1 Setup Program Initial Screen

AMI's BIOS ROM has a built-in Setup program that allows users to modify the basic system configuration. This information is stored in flash ROM so it retains the Setup information when the power is turned off.

3.2 Entering Setup

Turn on the computer and then press <DEL> or <ESC> to enter the Setup menu.

3.3 Main Setup

When users first enter the BIOS Setup Utility, users will see the Main setup screen.

Users can always return to the Main setup screen by selecting the Main tab. There are two Main Setup options. They are described in this section. The Main BIOS Setup screen is shown below.



Figure 3.2 Main Setup Screen

The Main BIOS setup screen has two main frames. The left frame displays all the options that can be configured. Grayed-out options cannot be configured; options in blue can. The right frame displays the key legend.

Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it.

- **System Time / System Date**
  Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time must be entered in HH:MM:SS format.

3.4 Advanced BIOS Features Setup

Select the Advanced tab from the SOM-7533 setup screen to enter the Advanced BIOS Setup screen. Users can select any item in the left frame of the screen, such as CPU Configuration, to go to the sub-menu for that item. Users can display an Advanced BIOS Setup option by highlighting it using the <Arrow> keys. All Advanced BIOS Setup options are described in this section. The Advanced BIOS Setup screens are shown below. The sub-menus are described on the following pages.

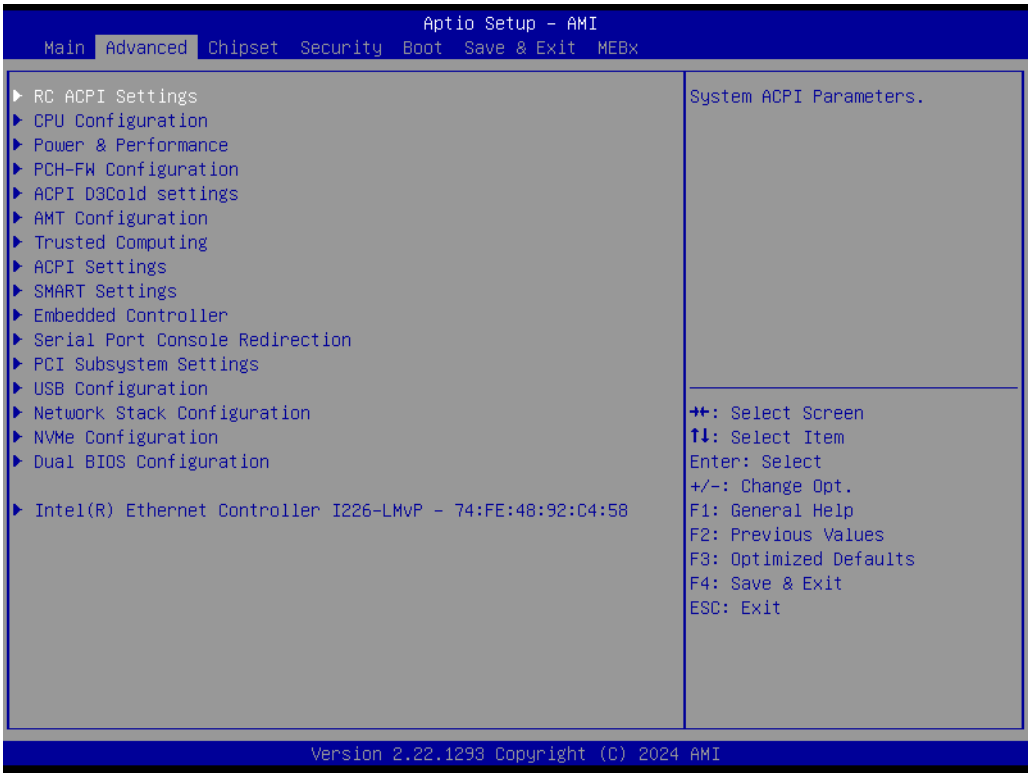


Figure 3.3 Advanced BIOS Features Setup Screen

- **RC ACPI Settings**
  System ACPI Parameters.
- **CPU Configuration**
  CPU Configuration Parameters.
- **Power & Performance**
  Power & Performance Options.
- **PCH-FW Configuration**
  Configure Management Engine Technology Parameters.
- **AMT Configuration**
  Configure Intel® Active Management Technology Parameters.
- **Trusted Computing**
  Trusted Computing Settings.
- **ACPI Settings**
  ACPI Sleep State.
- **SMART Settings**
  System SMART Settings.
- **Embedded Controller**
  Embedded Controller Parameters.
- **Serial Port Console Redirection**
  Console Redirection Settings.

- **PCI Subsystem Settings**
  PCI Subsystem Settings.
- **USB Configuration**
  USB Configuration Parameters.
- **Network Stack Configuration**
  Network Stack Settings.
- **NVMe Configuration**
  NVMe Device Options Settings.
- **Dual BIOS Configuration**
  Dual BIOS configuration. (If the module is equipped with 2 flashes.)
- **Intel® Ethernet Controller I226-LMvP**
  Configure Gigabit Ethernet device parameters.

3.4.1 RC ACPI Settings



Figure 3.4 RC ACPI Settings

- **PTID Support**
  PTID Support will be loaded if enabled.
- **PCIE Access Method**
  PCIE Access Method is Direct I/O or ACPI.
- **Native PCIE Enable**
  Bit-PCIe Native*control
  0-~Hot Plug
  1-SHPC Native Hot Plug control
  2-2-~Power Management Events
  3-3-PCIe Advanced Error Reporting control
  4-4-PCIe Capability Structure control
  5-Latency Tolerance Reporting control

- **Native ASPM**
  Enabled-OS Controlled ASPM, Disabled-BIOS Controlled ASPM.
- **BDAT ACPI Table Support**
  Enables support for the BDAT ACPI table.
- **Wake System from S5 via RTC**
  Enable or Disable system wake-on-alarm event. When enabled, the system will wake on the hr:min:sec specified.
- **ACPI Debug**
  Open a memory buffer for storing debug strings. Reenter SETUP after enabling to see the buffer address. Use the ADBG method to write strings to the buffer.
- **D3 Setting for Storage**
  RTD3 support for Storage. PCIE storage PEP constraint needs to be set as D0/F1 (Intel Advanced->ACPI Settings->PEP PCIe Storage) when this setup is disabled/D3Hot.
- **Low Power S0 Idle Capability**
  This variable determines if we enable ACPI Lower Power S0 Idle Capability (Mutually exclusive with Smart connect). While this is enabled, it also disables 8524 timer for SLP_S0 support.
- **PCI Delay Optimization**
  Experimental ACPI additions for FW latency optimizations.
- **MSI enabled**
  When disabled, MSI support is disabled in FADT.
- **PCIe delay between_OFF_ON**
  PCIe delay between _OFF _ON.

3.4.2 CPU Configuration

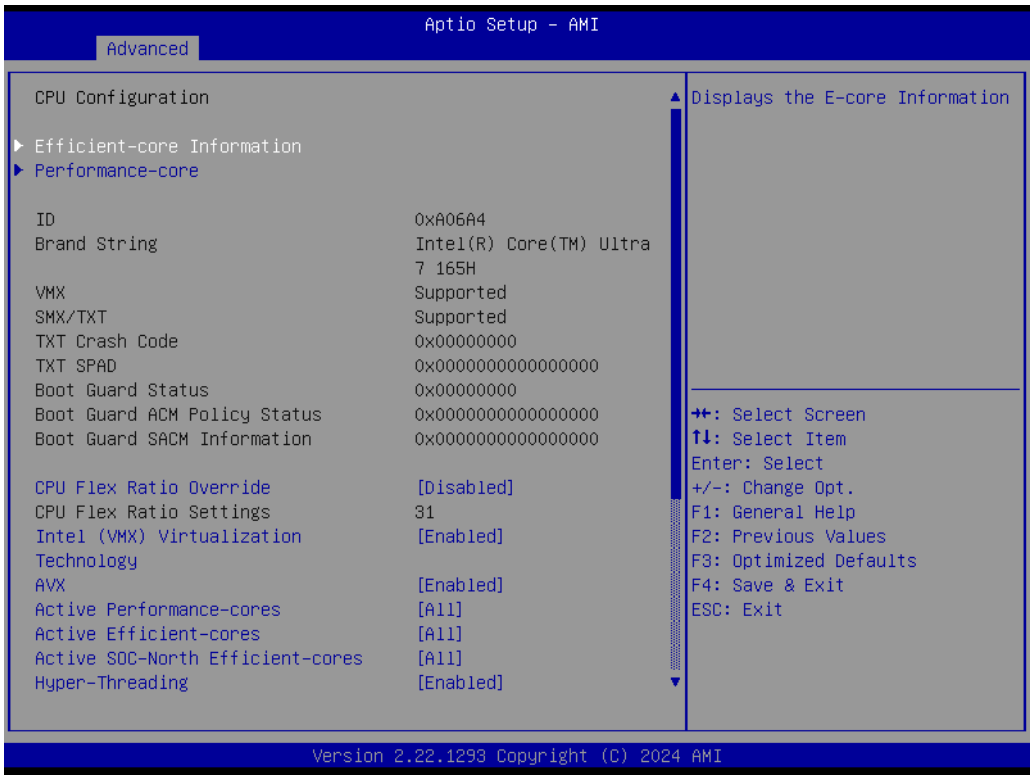


Figure 3.5 CPU Configuration

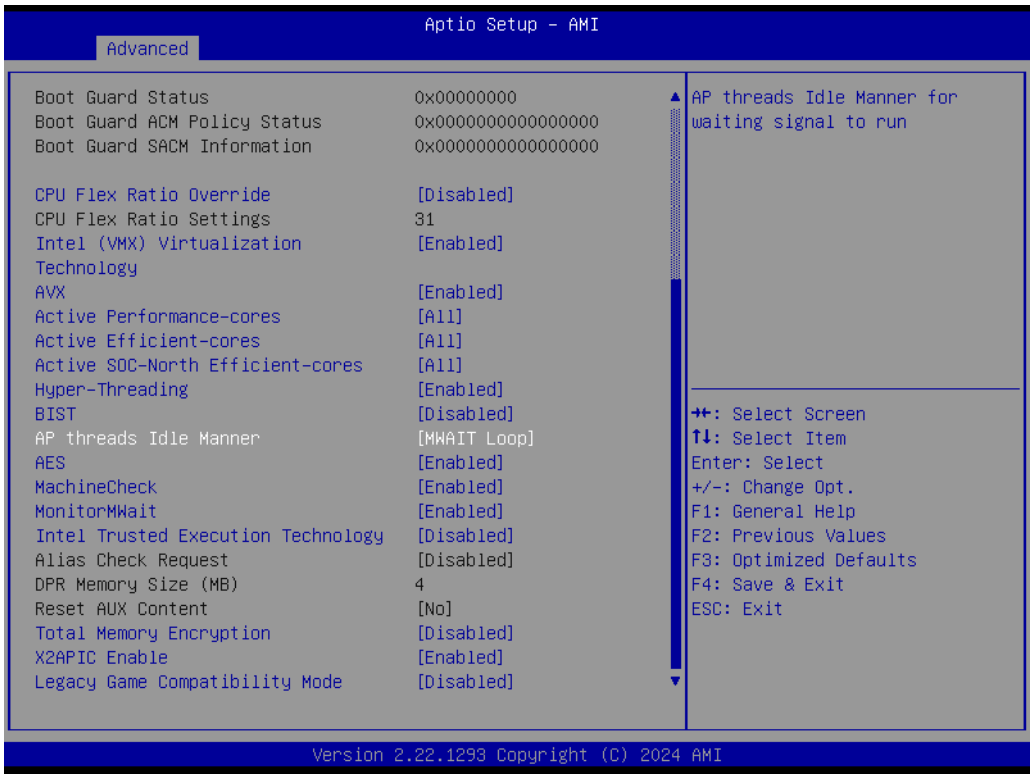


Figure 3.6 CPU Configuration

- **Efficient-core Information**
  Displays the E-core Information.

- **Performance-core**
  Displays the P-core Information.
- **CPU Flex Ratio Override**
  Enable or Disable CPU Flex Ratio Programming.
- **Intel (VMX) Virtualization Technology**
  When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
- **AVX**
  Enable/Disable the AVX and AVX2 Instructions.
- **Active Performance-cores**
  Number of P-cores to enable in each processor package. Note: The number of Cores and E-cores are considered together. When both are {0,0}, Pcode will enable all cores.
- **Active Efficient-cores**
  The number of E-cores to enable in each processor package. Note: the number of Cores and E-cores are considered together. When both are {0,0}, Pcode will enable all cores.
- **Active SOC-North Efficient-cores**
  The number of SOC-North Efficient-cores to enable in SOC North.
- **Hyper-Threading**
  Enable or Disable Hyper-Threading Technology.
- **BIST**
  Enable/Disable BIST (Built-In Self Test) on reset.
- **AP threads Idle Manner**
  AP threads Idle Manner for waiting signal to run.
- **AES**
  Enable/Disable AES (Advanced Encryption Standard).
- **MachineCheck**
  Enable/Disable Machine Check.
- **MonitorMWait**
  Enable/Disable MonitorMwait. If you Disable MonitorMwait, the AP threads Idle Manner should not be set in MWAIT Loop.
- **Intel Trusted Execution Technology**
  Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology. Changes require a full power cycle to take effect.
- **Total Memory Encryption**
  Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks. When this option is configured as ‘Enabled’, ‘VT-d’ option must be ‘Enabled’. This option will be grayed out when ’VT-d’ option is configured as ‘Disabled’.
- **X2APIC Enable**
  Enable/Disable X2APIC Operating Mode. When this option is configured as ‘Enabled’, ‘VT-d’ option must be ‘Enabled’ and ‘X2APIC’ Opt Out ‘option must be ‘Disabled’ as well. This option will be grayed out when ’VT-d’ option is configured as ‘Disabled’.
- **Legacy Game Compatibility Mode**
  When enabled, pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when the LED is off.

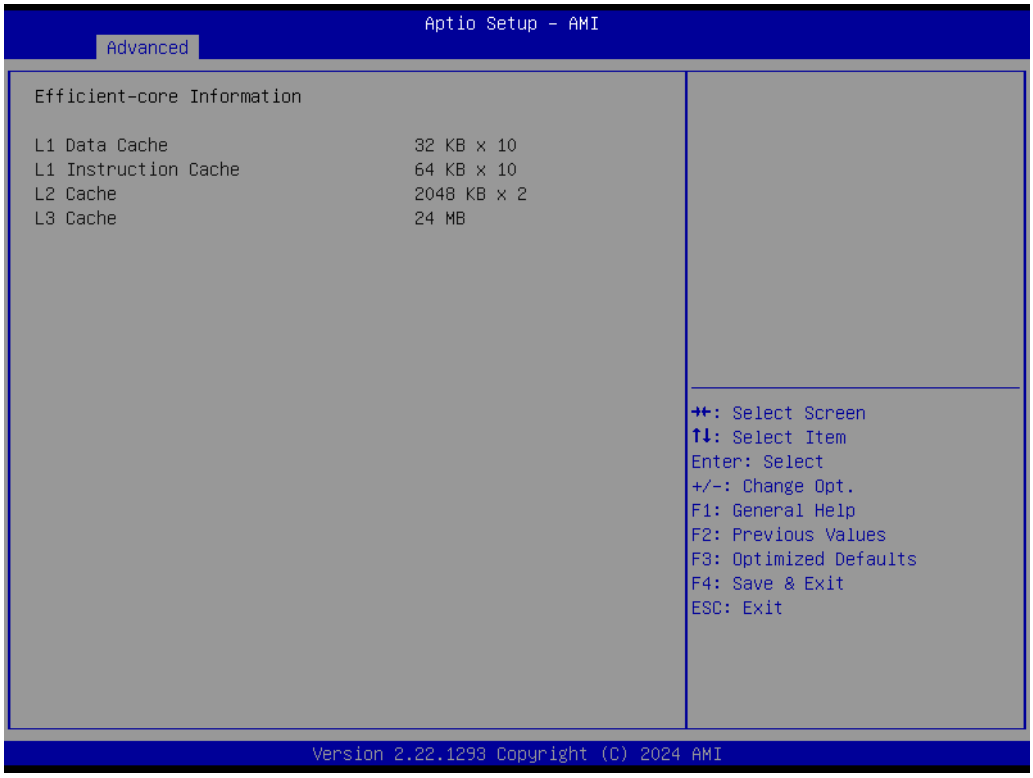


Figure 3.7 Efficient-core Information

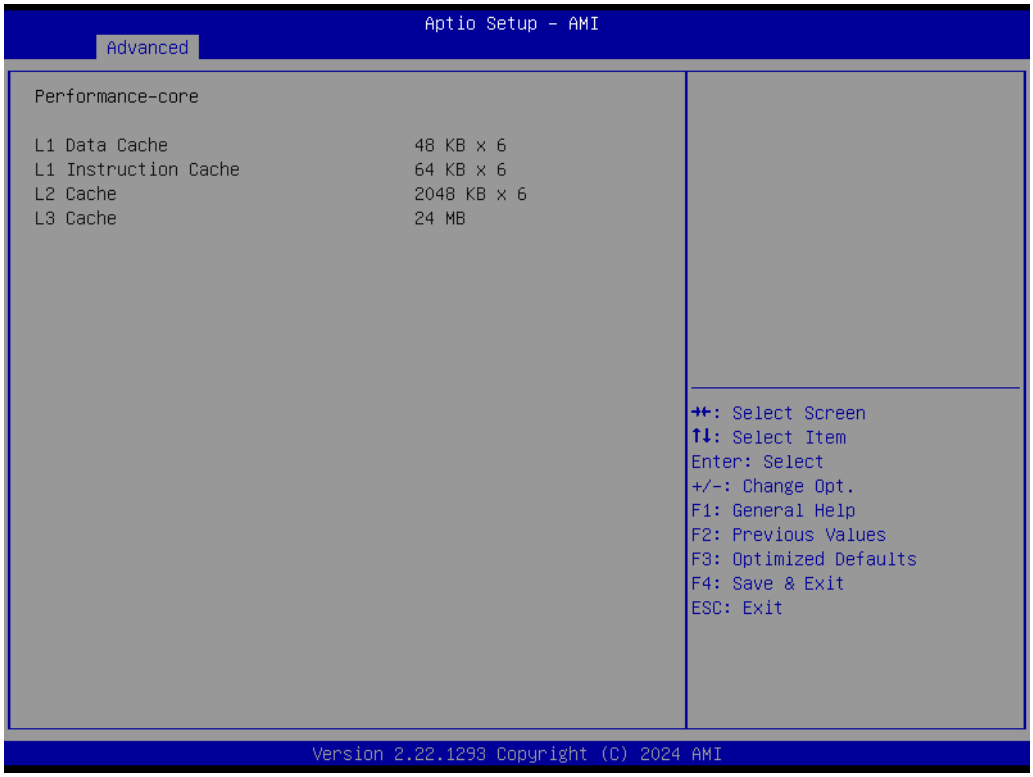


Figure 3.8 Performance-core

3.4.3 Power & Performance

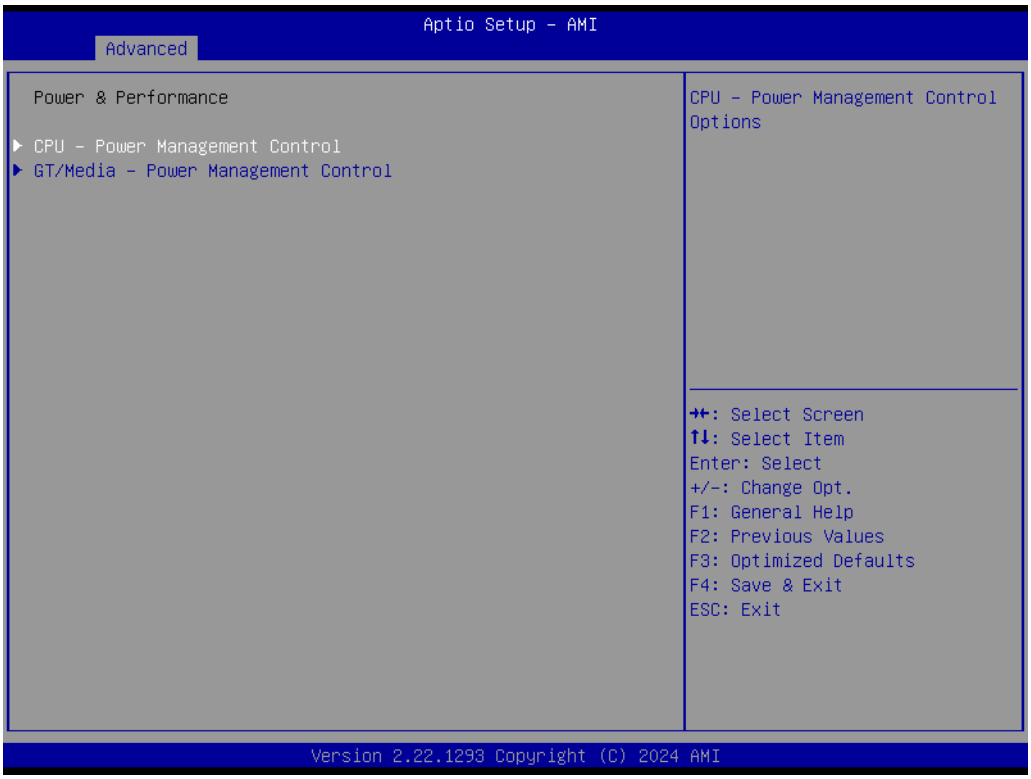


Figure 3.9 Power & Performance

- **CPU - Power Management Control**
  CPU - Power Management Control Options.
- **GT/Media - Power Management Control**
  GT/Media - Power Management Control Options.

3.4.3.1 CPU - Power Management Control

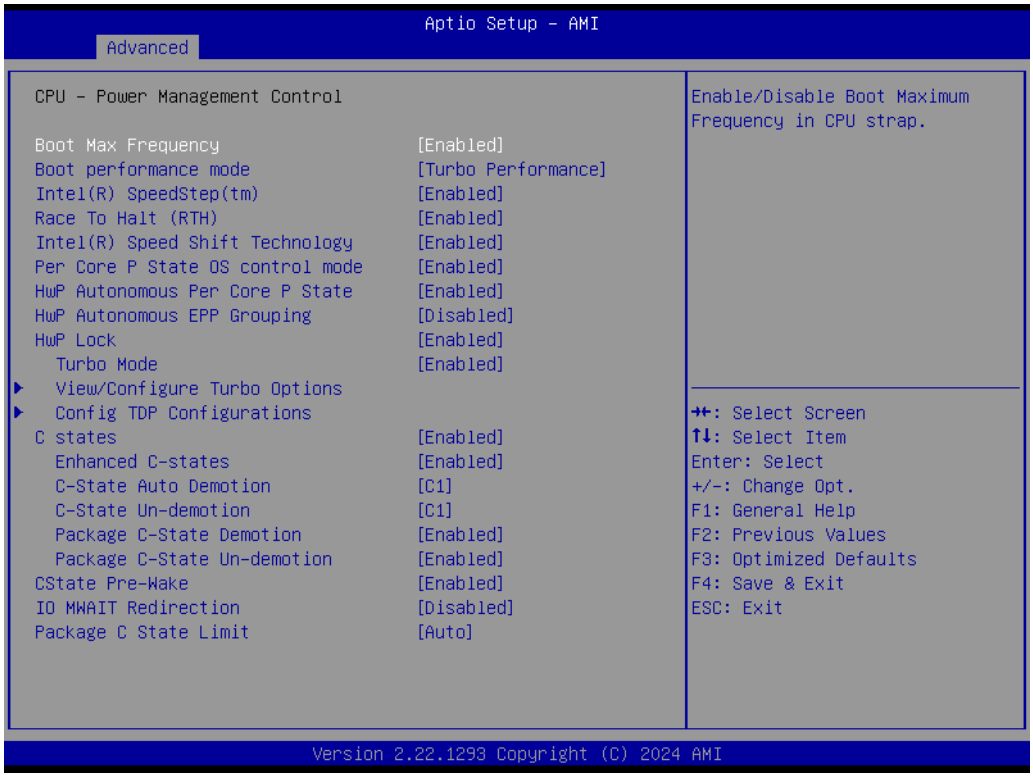


Figure 3.10 CPU-Power Management Control

- **Boot Max Frequency**
  Enable/Disable Boot Maximum Frequency in CPU strap.
- **Boot performance mode**
  Select the performance state that the BIOS will set starting from the reset vector.
- **Intel(R) SpeedStep(tm)**
  Allows more than two frequency ranges to be supported.
- **Race To Halt (RTH)**
  Enable/Disable the Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power.
- **Intel(R) Speed Shift Technology**
  Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
- **Per Core P State OS control mode**
  Enable/Disable Per Core state OS control mode. When set, the highest core request is used for all other core requests.
- **HwP Autonomous Per Core P State**
  Disable Autonomous PCPS Autonomous will request the same value for all cores all the time.
- **HwP Autonomous EPP Grouping**
  Enable EPP grouping Autonomous will request the same values for all cores with same EPP. Disable EPP grouping autonomous will not necessarily request same values for all cores with same EPP.
- **HwP Lock**
  Enable/Disable HWP Lock support in Misc Power Management MSR.
- **Turbo Mode**
  Enable/Disable processor Turbo Mode.

- **View/Configure Turbo Options**
  View/Configure Turbo Options.
- **Config TDP Configurations**
  cTDP (Assured Power) Configurations.
- **C states**
  Enable/Disable CPU Power Management. Allows the CPU to go to C states when it's not 100% utilized.
- **Enhanced C-states**
  Enable/Disable C1E. When enabled, the CPU will switch to minimum speed when all cores enter C-State.
- **C-State Auto Demotion**
  Configure C-State Auto Demotion
- **C-State Un-demotion**
  Configure C-State Un-demotion.
- **Package C-State Demotion**
  Package C-State Demotion.
- **Package C-State Un-demotion**
  Package C-State Un-demotion.
- **CState Pre-Wake**
  Disable-to 1 to disable the Cstate Pre-Wake.
- **IO MWAIT Redirection**
  When set, it will map IO_read instructions sent to IO registers PMG_IO_BASE_ADDRBASE+offset to MWAIT(offset).
- **Package C State Limit**
  Maximum Package C State Limit Setting. CPU Default: Leaves it as Factory default value. Auto: Initializes to deepest available Package C State Limit.

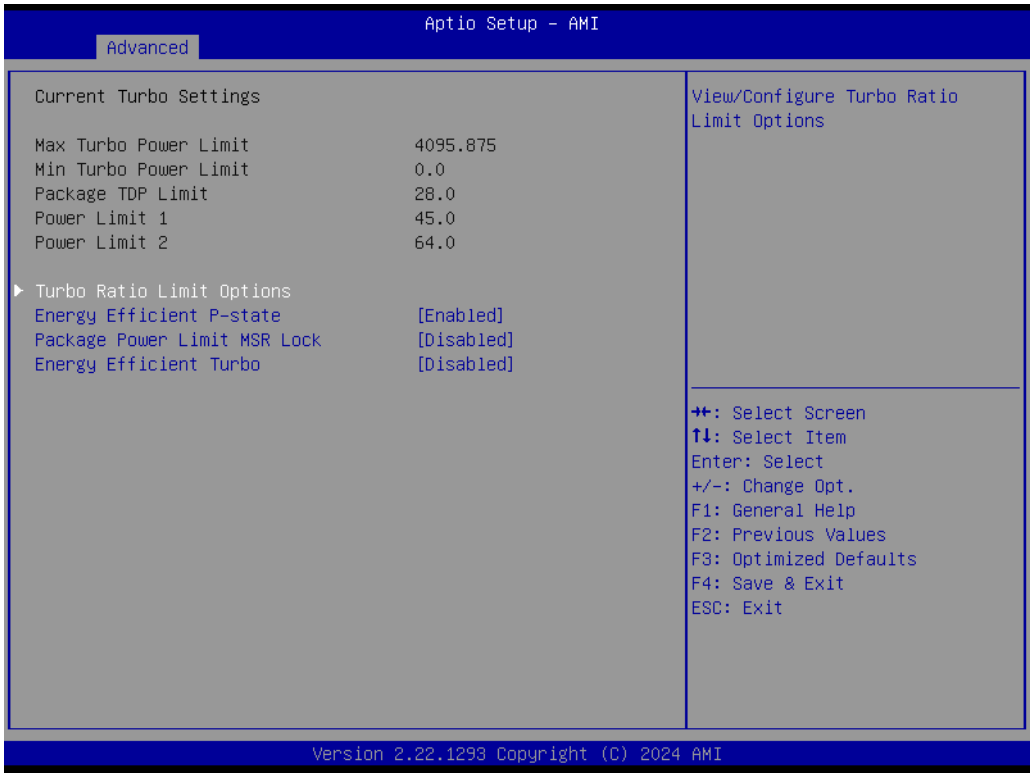


Figure 3.11 Current Turbo Settings

- **Turbo Ratio Limit Options**
  View/Configure Turbo Ratio Limit Options.
- **Energy Efficient P-state**
  Enable/Disable the Energy Efficient P-state feature. When set to 0, it will disable access to the ENERGY_PERFORMANCE_BIAS MSR and CPUID Function. It will read 0, indicating no support for Energy Efficient policy setting. When set to 1, it will enable access to ENERGY_PERFORMANCE_BIAS MSR and the CPUID Function will read 1, indicating the Energy Efficient policy setting is supported.
- **Package Power Limit MSR Lock**
  Enable/Disable locking of Package Power Limit settings. When enabled, PACKAGE_POWER_LIMIT MSR will be locked and a reset will be required to unlock the register.
- **Energy Efficient Turbo**
  Enable/Disable the Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency. It is recommended only to disable it in overclocking situations where turbo frequency must remain constant. Otherwise, leave it as enabled.

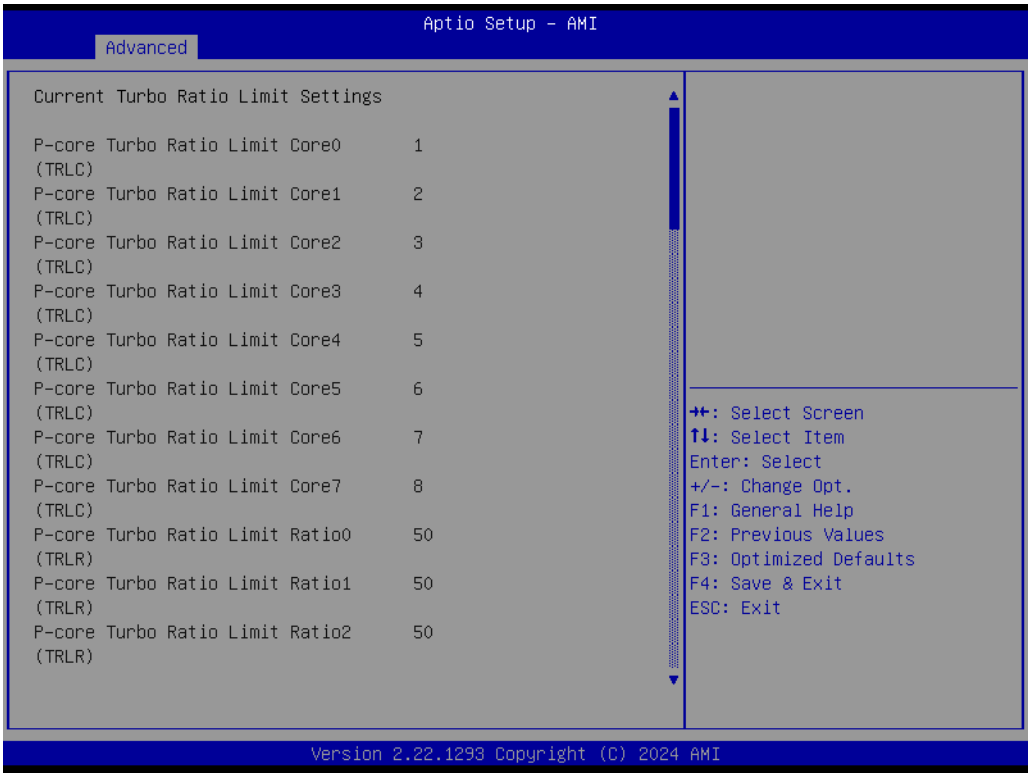


Figure 3.12 Current Turbo Ratio Limit Settings

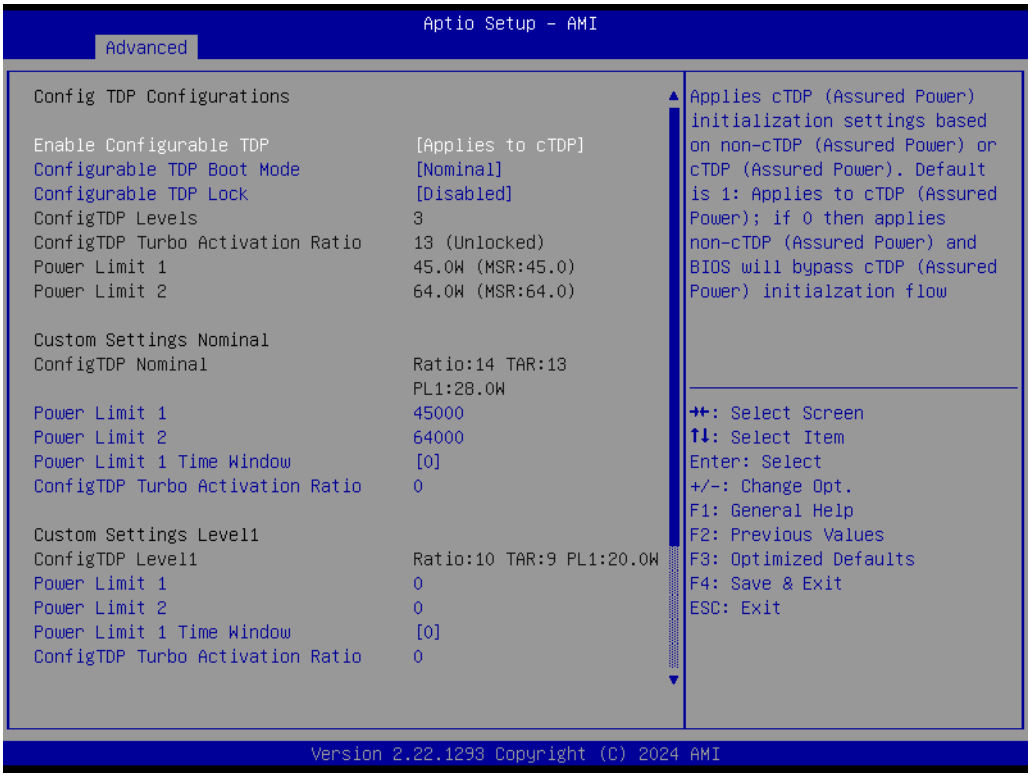


Figure 3.13 Config TDP Configurations

- **Enable Configurable TDP**
  Applies cTDP (Assured Power) initialization settings based on non-cTDP (Assured Power) or cTDP (Assured Power). Default is 1: Applies to cTDP

(Assured Power); if 0 then applies non-cTDP (Assured Power) and BIOS will bypass cTDP (Assured Power) initialization flow.

- **Configurable TDP Boot Mode**
  cTDP (Assured Power) Mode as Nominal/Level1/Level2/Deactivate TDP (Base Power) selection. The Deactivate option will set MSR to Nominal and MMIO to Zero.
- **Configurable TDP Lock**
  cTDP (Assured Power) Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL. Note: When cTDP (Assured Power) Lock is enabled, Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.
- **Power Limit 1**
  Power Limit 1 in milliwatts. BIOS will round to the nearest 1/8W when programming. 0=no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits. Other SKUs: This value must be between Min Power Limit and Processor Base (TDP) Limit.
- **Power Limit 2**
  Power Limit 2 in milliwatts. The BIOS will round to the nearest 1/8W when programming. 0=no custom override. For 12.50W, enter 12500. The processor applies control policies such that the package power does not exceed this limit.
- **Power Limit 1 Time Window**
  Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0=default value (28 sec for Mobile and 8 sec for Desktop). It defines the time window in which Processor Base Power (TDP) value should be maintained.
- **ConfigTDP Turbo Activation Ratio**
  Custom value for Turbo Activation Ratio. It needs to be configured with valid values from LFM to Max Turbo. 0 means it is not using a custom value.
- **Power Limit 1**
  Power Limit 1 in milliwatts. The BIOS will round to the nearest 1/8W when programming. 0=no custom override. For 12.50W, enter 12500. Overclocking SKU: the value must be between Max and Min Power Limits. Other SKUs: This value must be between the Min Power Limit and Processor Base (TDP) Limit.
- **Power Limit 2**
  Power Limit 2 in milliwatts. The BIOS will round to the nearest 1/8W when programming. 0=no custom override. For 12.50W, enter 12500. The processor applies control policies such that the package power does not exceed this limit.
- **Power Limit 1 Time Window**
  Power Limit 1 Time Window value in seconds. The value may vary from 0 to 128. 0=default value (28 sec for Mobile and 8 sec for Desktop). It defines the time window in which the Processor Base Power (TDP) value should be maintained.
- **ConfigTDP Turbo Activation Ratio**
  Custom value for Turbo Activation Ratio. It needs to be configured with valid values from LFM to Max Turbo. 0 means it is not using a custom value.

3.4.3.2 GT/Media-Power Management Control

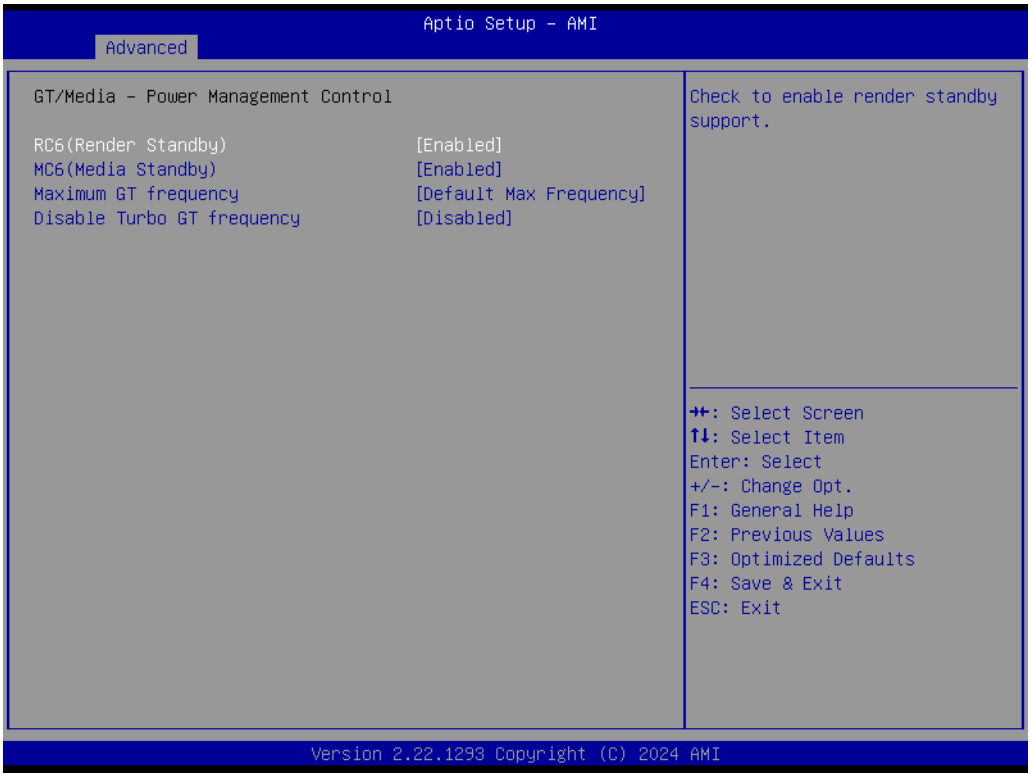


Figure 3.14 GT/Media-Power Management Control

- **RC6(Render Standby)**
  Check to enable render standby support.
- **MC6(Media Standby)**
  Check to enable Media standby support.
- **Maximum GT frequency**
  Maximum GT frequency limited by the user. Choose between 2400MHx (RPN) and 6900MHz (RP0). A value beyond the range will be clipped to the min/max supported by the SKU.
- **Disable Turbo GT frequency**
  Enabled: Disable Turbo GT frequency. Disabled: GT frequency is not limited.

3.4.4 PCH-FW Configuration

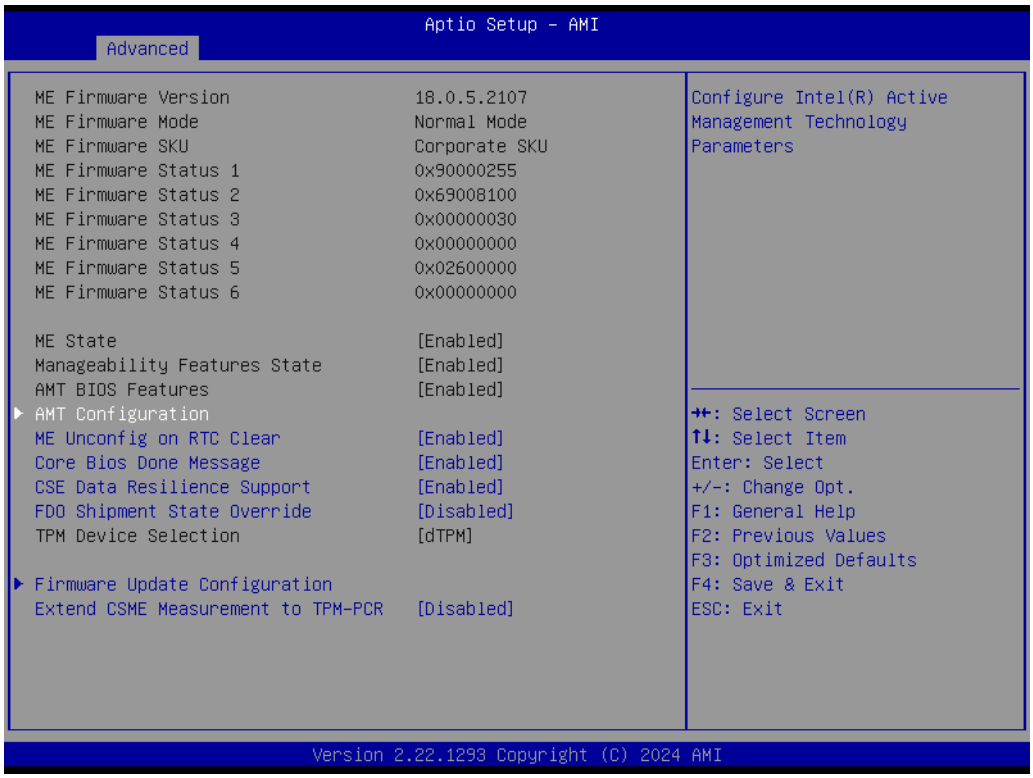


Figure 3.15 PCH-FW Configuration

- **AMT Configuration**
  Configure Intel(R) Active Management Technology Parameters.
- **ME Unconfig on RTC Clear**
  When Disabled, ME will not be unconfigured on RTC clear.
- **Core Bios Done Message**
  Enable/Disabled Core Bios Done message sent to ME.
- **CSE Data Resilience Support**
  Enable/Disable CSE Data Resilience Support.
- **FD0 Shipment State Override**
  Enable/Disable FD0 Shipment State Override. The BIOS will override the soft strap setting when enabled.
- **Firmware Update Configuration**
  Configure Intel(R) Active Management Technology Parameters.
- **Extend CSME Measurement to TPM-PCR**
  Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1].

3.4.5 ACPI D3Cold Settings

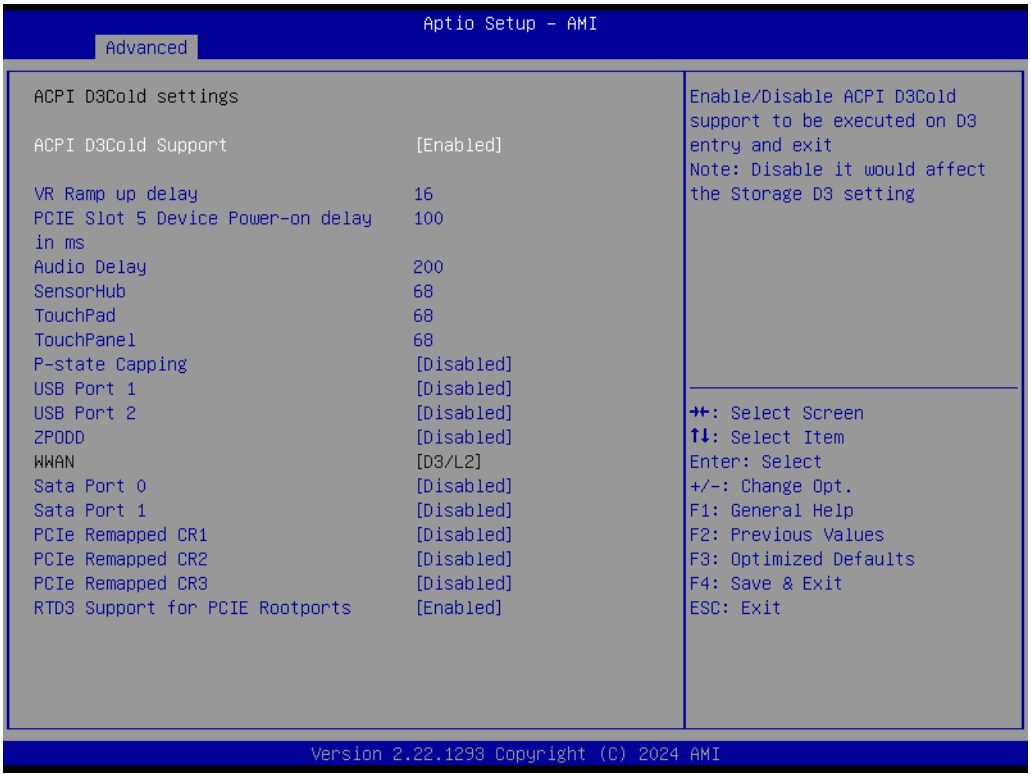


Figure 3.16 ACPI D3Cold settings

- **ACPI D3Cold Support**
  Enable/Disable ACPI D3Cold support to be executed on D3 entry and exit. Note: Disable it would affect the storage D3 setting.
- **VR Ramp up to delay**
  Delay between subsequent VR ramp up if they are all Turn ON at the same time.
- **PCIE Slot 5 Device Power-on delay**
  Delay between applying core power and Deasserting PERST#
- **Audio Delay**
  Delay after applying power to HD Audio (Realtek) codec device.
- **SensorHub**
  Delay after applying power to SensorHub device.
- **TouchPad**
  Delay after applying power to Touchpad device.
- **TouchPanel**
  Delay in PR-ON after applying power to TouchPanel device.
- **P-state Capping**
  Set _PPC and send ACPI notification.
- **USB Port 1**
  USB RTD3 support. Super Speed: USB 3.0 devices will be exposed as RTD3 capable. High Speed: USB 2.0 devices will be exposed as RTD3 capable. Disabled: USB RTD3 support disabled. For SawtoothPeak USB Port1 (Below) is Superspeed and Port2 (Top) is HighSpeed. Check the respective board configuration to see the USB port position.
- **USB Port 1**
  USB RTD3 support. Super Speed: USB 3.0 devices will be exposed as RTD3

capable. High Speed: USB 2.0 devices will be exposed as RTD3 capable. Disabled: USB RTD3 support disabled. For SawtoothPeak USB Port1 (Below) is Superspeed and Port2 (Top) is HighSpeed. Check the respective board configuration to see the USB port position.

- **USB Port 2**
  USB RTD3 support. Super Speed: USB 3.0 devices will be exposed as RTD3 capable. High Speed: USB 2.0 devices will be exposed as RTD3 capable. Disabled: USB RTD3 support disabled. For SawtoothPeak USB Port1 (Below) is Superspeed and Port2 (Top) is HighSpeed. Check the respective board configuration to see the USB port position.
- **ZPODD**
  The Zero Power ODD option is applicable only for the board with ZPODD support.
- **Sata Port 0**
  Setup option to control the SATA port RTD3 functionality.
- **Sata Port 1**
  Setup option to control the SATA port RTD3 functionality.
- **PCIe Remapped CR1**
  PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
- **PCIe Remapped CR2**
  PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
- **PCIe Remapped CR3**
  PCIe RTD3 setup conflicts with SATA RTD3. Platform specific.
- **RTD3 Support for PCIE Rootports**
  Enable/Disable PCIE RTD3 Support.

3.4.6 AMT Configuration

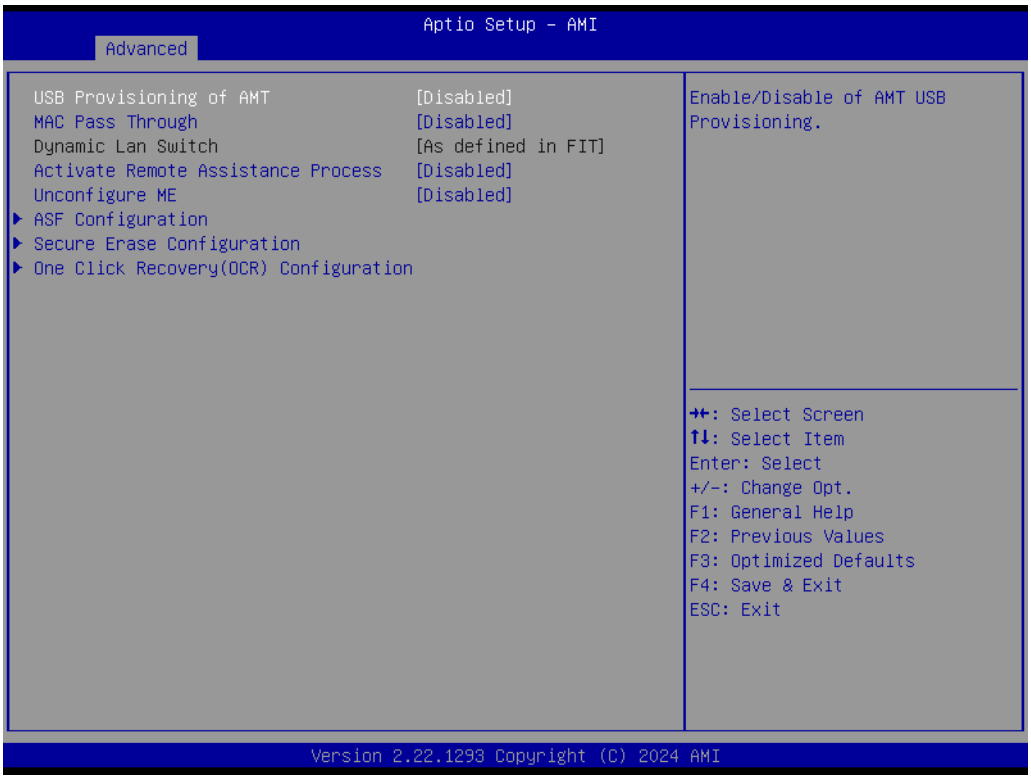


Figure 3.17 AMT Configuration

- **USB Provisioning of AMT**
  Enable/Disable AMT USB Provisioning.
- **MAC Pass Through**
  Enable/Disable the MAC Pass Through function.
- **Activate Remote Assistance Process**
  Tiger CIRA boot Note: Network Access must be activated first from the MEBx Setup.
- **Unconfigure ME**
  Unconfigure ME with resetting MEBx password to default on next boot.
- **ASF Configuration**
  Configure Alert Standard Format parameters.
- **Secure Erase Configuration**
  Secure Erase configuration menu.
- **One Click Recovery(OCR) Configuration**
  Configuration setting for One Click Recovery. This allows access for AMT to boot a recovery IS application.

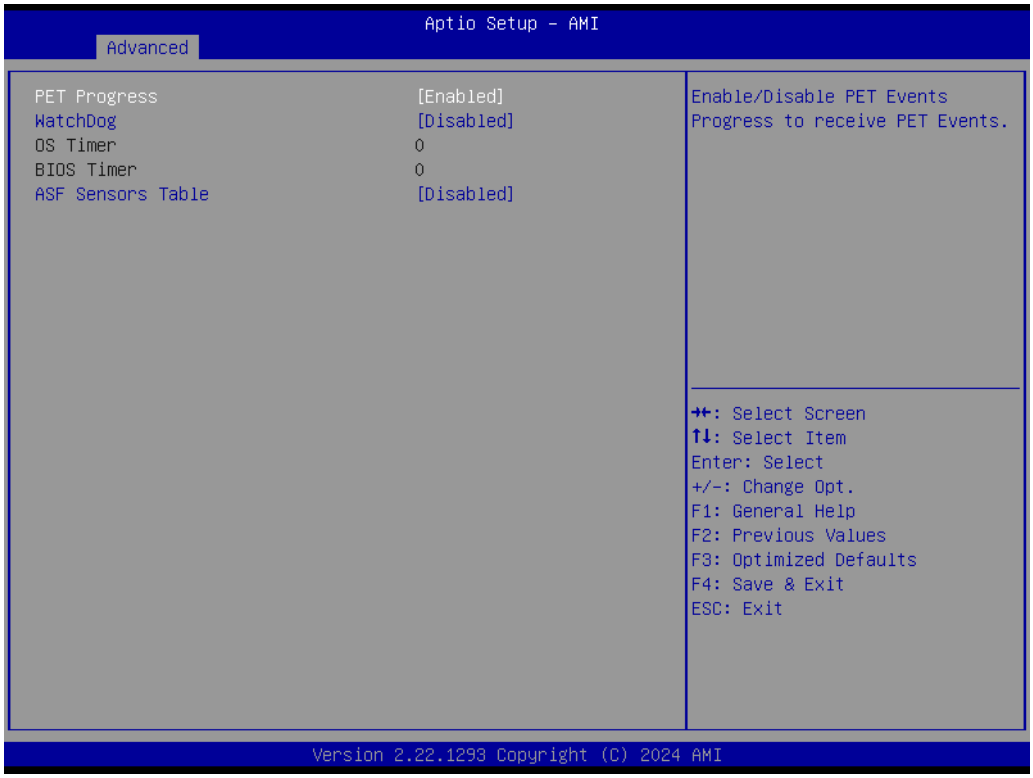


Figure 3.18 ASF Configuration

- **PET Process**
  Enable/Disable PET Events Progress to receive PET Events.
- **WatchDog**
  Enable/Disable the WatchDog Timer.
- **ASF Sensors Table**
  Adds the ASF Sensor Table into the ASF! ACPI Table.

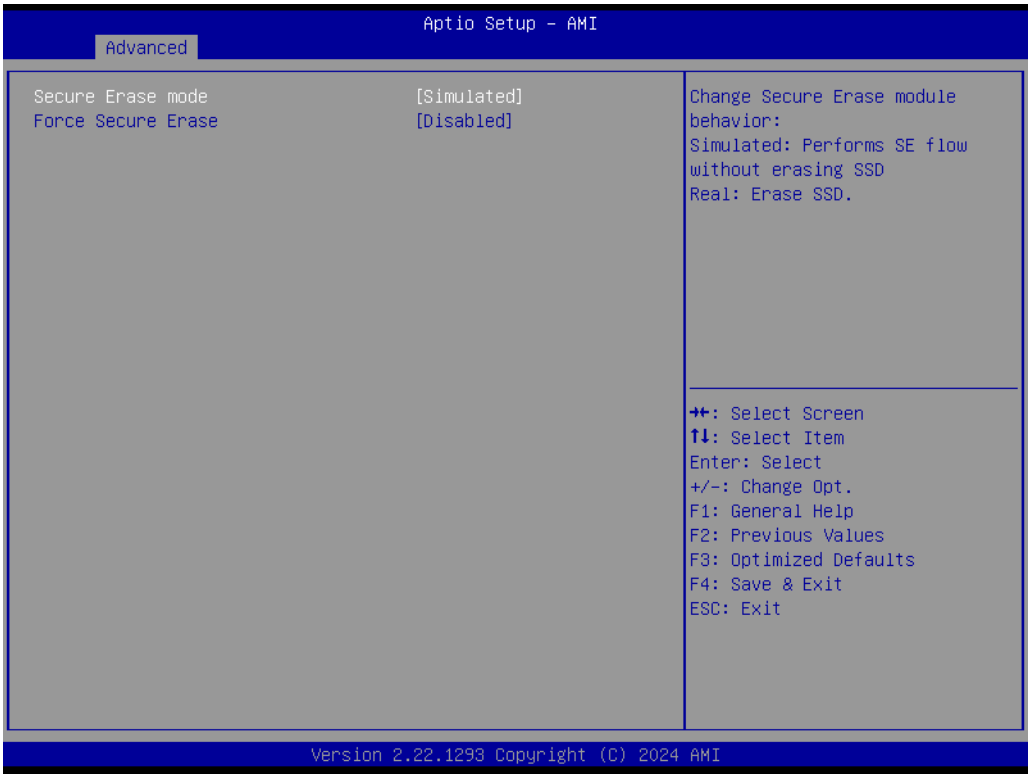


Figure 3.19 Secure Erase Configuration

- **Secure Erase mode**
  Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD Real: Erase SSD.
- **Force Secure Erase**
  Force Secure Erase on next boot.

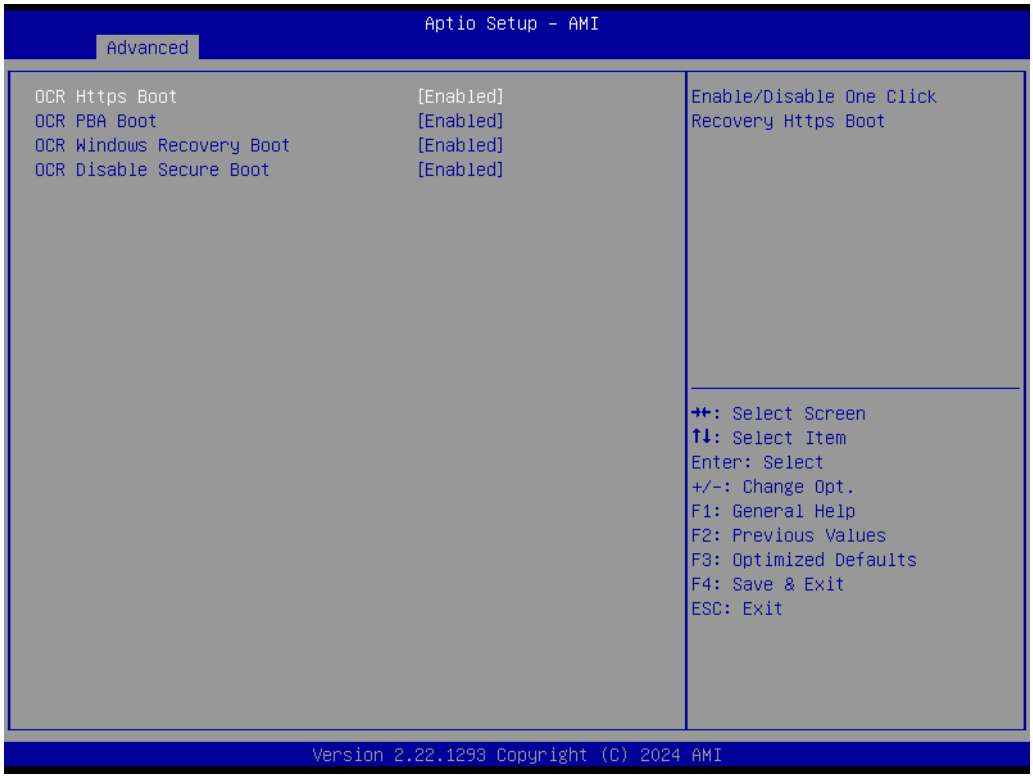


Figure 3.20 One Click Recovery (OCR) Configuration

- **OCR Https Boot**
  Enable/Disable One Click Recovery Https Boot.
- **OCR PBA Boot**
  Enable/Disable One Click Recovery PBA Boot.
- **OCR Windows Recovery Boot**
  Enable/Disable One Click Recovery Windows Recovery Boot.
- **OCR Disable Secure Boot**
  Allows CSME to request SecureBoot to be disabled for One Click Recovery.

3.4.7 Trusted Computing



Figure 3.21 Trusted Computing

- **Security Device Support**
  Enables or Disables BIOS support for a security device. The OS will not show the Security Device. TCG EFI protocol and INT1A interface will not be available.
- **SHA256 PCR Bank**
  Enable or Disable SHA256 PCR Bank.
- **SHA384 PCR Bank**
  Enable or Disable SHA384 PCR Bank.
- **Pending operation**
  Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change the State of Security Device.
- **Platform Hierarchy**
  Enable or Disable Platform Hierarchy.
- **Storage Hierarchy**
  Enable or Disable Storage Hierarchy.
- **Endorsement Hierarchy**
  Enable or Disable Endorsement Hierarchy.
- **Physical Presence Spec Version**
  Select to tell the OS to support PPI Spec Version 1.2 or 1.3. Note: some HCK tests might not support 1.3.
- **Device Select**
  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.

3.4.8 ACPI Settings

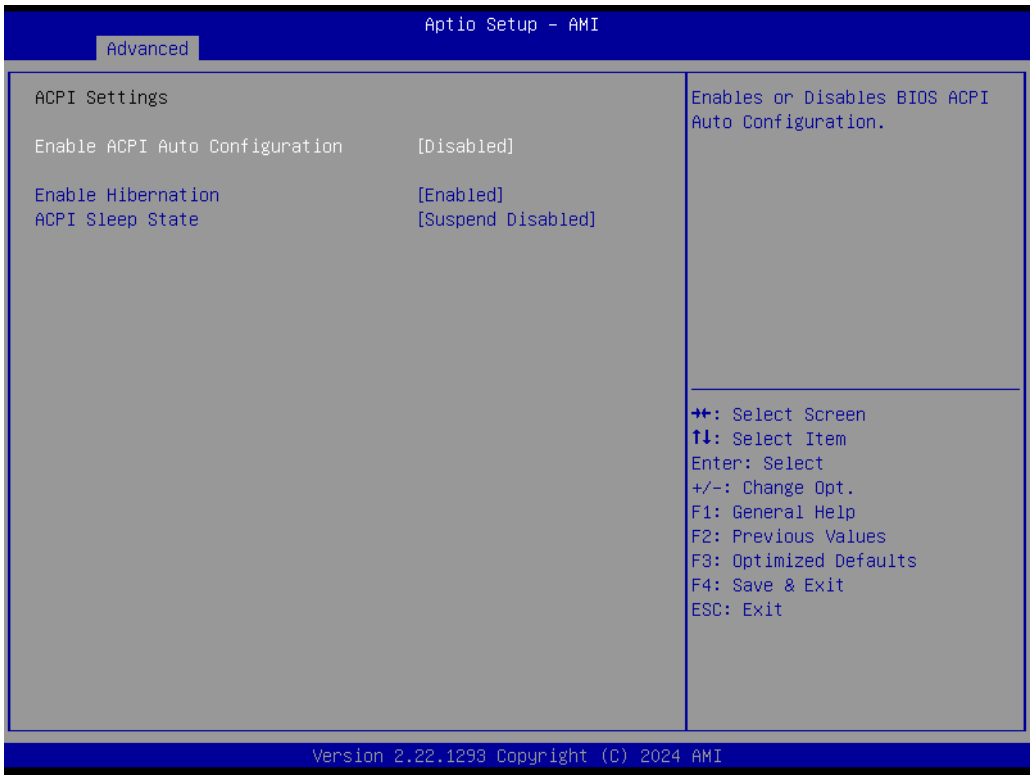


Figure 3.22 ACPI Settings

- **Enable ACPI Auto Configuration**
  Enable or Disable BIOS ACPI Auto Configuration.
- **Enable Hibernation**
  ACPI Sleep State.

3.4.9 SMART Settings

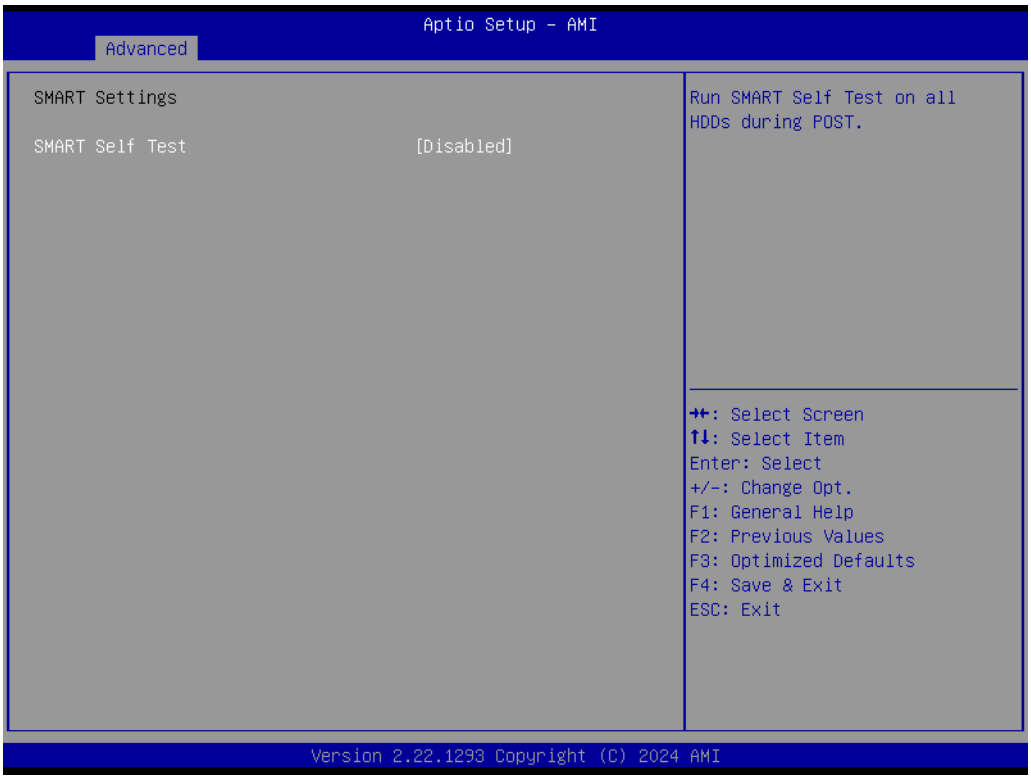


Figure 3.23 SMART Settings

- **SMART Self Test**
  Run SMART Self Test on all HDDs during POST.

3.4.10 Embedded Controller

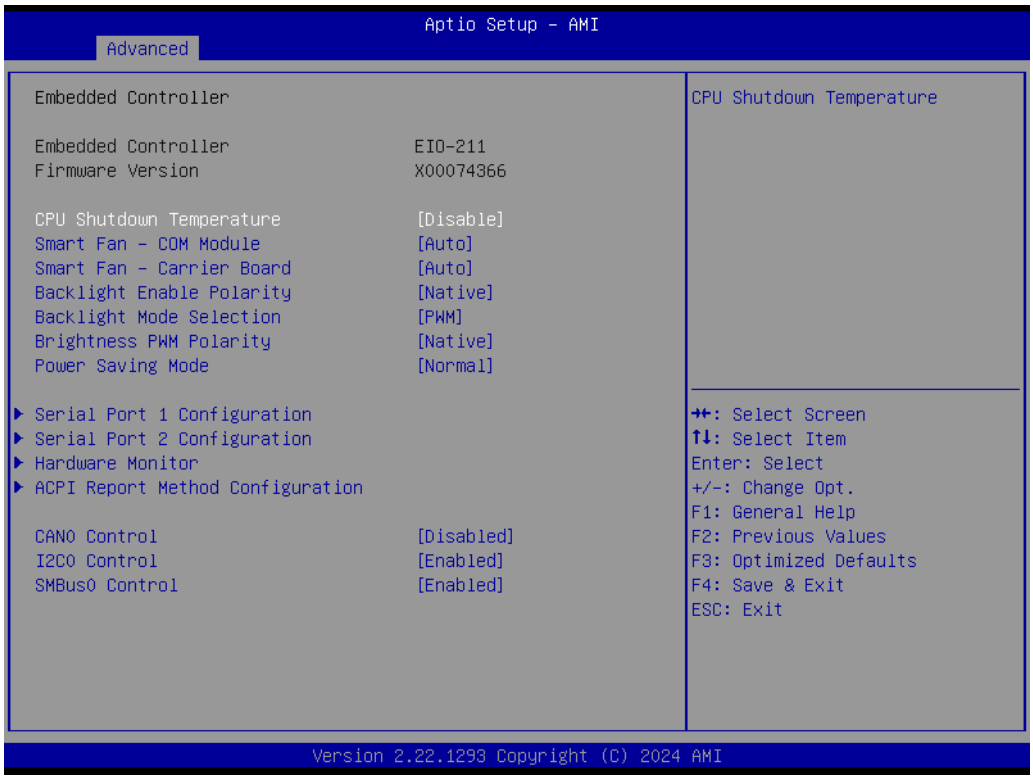


Figure 3.24 Embedded controller

- **CPU Shutdown Temperature**
  CPU Shutdown Temperature.
- **Smart Fan - COM Module**
  Control COM Module Smart FAN function.
- **Smart Fan - Carrier Board**
  Control Carrier Board Smart FAN function. It gets the value from EC and only sets the value when you Save Changes.
- **Backlight Enable Polarity**
  Switch Backlight Enable Polarity for Native or Invert.
- **Backlight Mode Selection**
  Switch Backlight Control to PWM or DC mode.
- **Brightness PWM Polarity**
  Backlight Control Brightness PWM Polarity for Native or Invert.
- **Power Saving Mode**
  Select Power Saving Mode.
- **Serial Port 1 Configuration**
  Set Parameters of Serial Port 1 (COMA).
- **Serial Port 2 Configuration**
  Set Parameters of Serial Port 2 (COMB).
- **Hardware Monitor**
  Monitor hardware status.
- **ACPI Report Method Configuration**
  Select ACPI Reporting Method for EC Devices.
- **CAN0 Control**
  Enable/Disable CAN0 controller on RDC-IS200.

- **I2C0 Control**
  Enable/Disable I2C0 controller on RDC-IS200.
- **SMBus0 Control**

3.4.11 Serial Port Console Redirection

3.4.11.1 Serial Port 1 Configuration

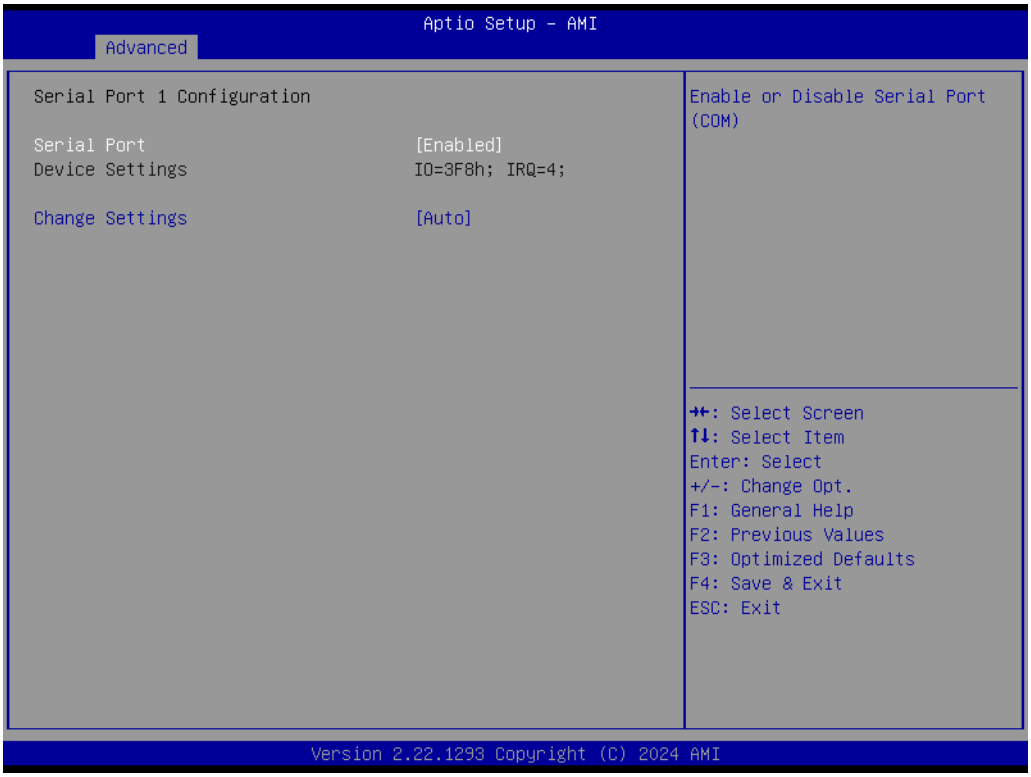


Figure 3.25 Serial Port 1 Configuration

- **Serial Port**
  Enable or Disable Serial Port (COM).
- **Change Settings**
  Select an optimal settings for a Super IO Device.

3.4.11.2 Serial Port 2 Configuration

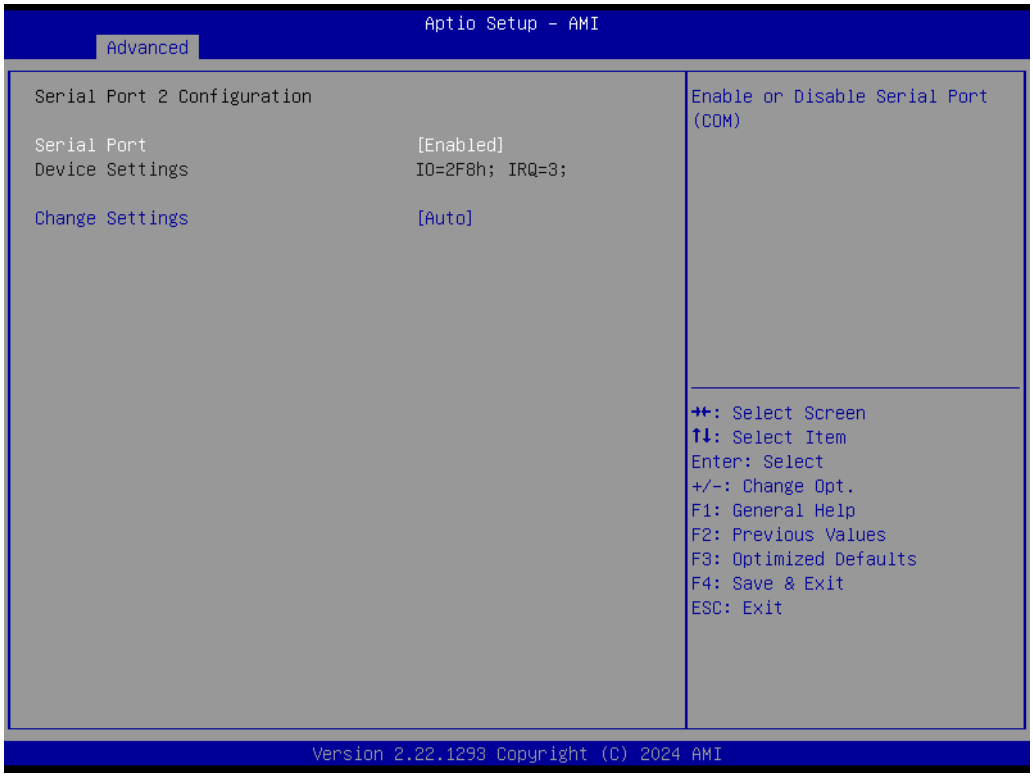


Figure 3.26 Serial Port 2 Configuration

- **Serial Port**
  Enable or Disable Serial Port (COM).
- **Change Settings**
  Select optimal settings for a Super IO Device.

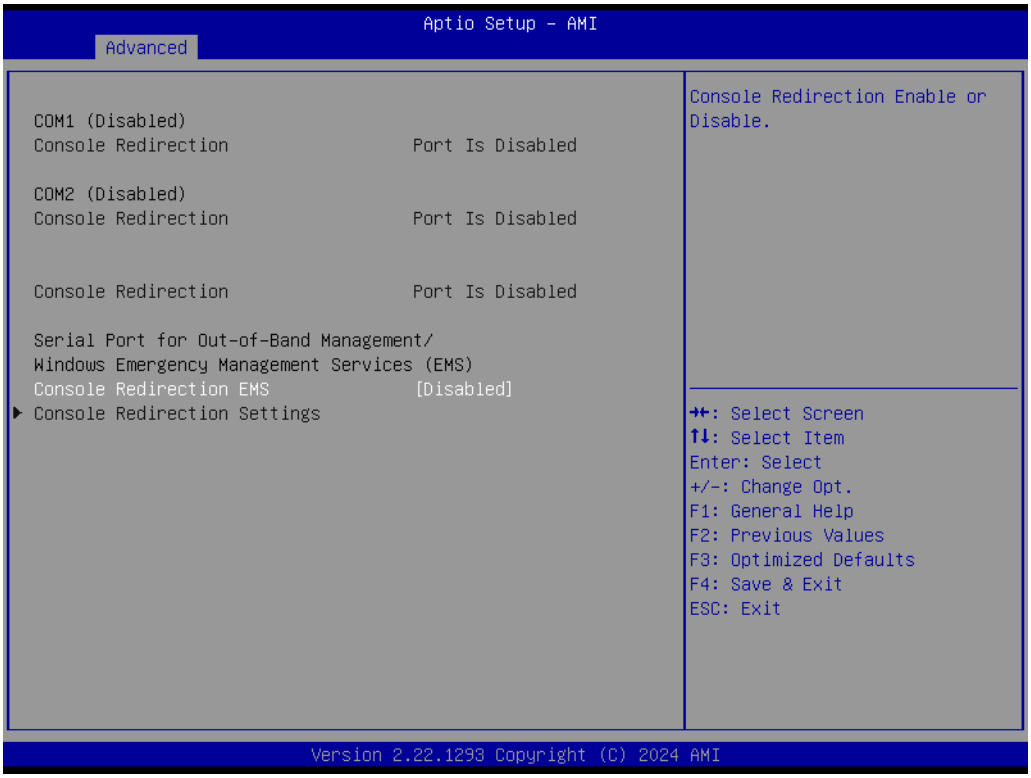


Figure 3.27 Serial Port Console Redirection

- **COM1 Console Redirection**
  Console Redirection Enable or Disable.
- **COM2 Console Redirection**
  Console Redirection Enable or Disable.
- **Console Redirection EMS**
  Console Redirection Enable or Disable.

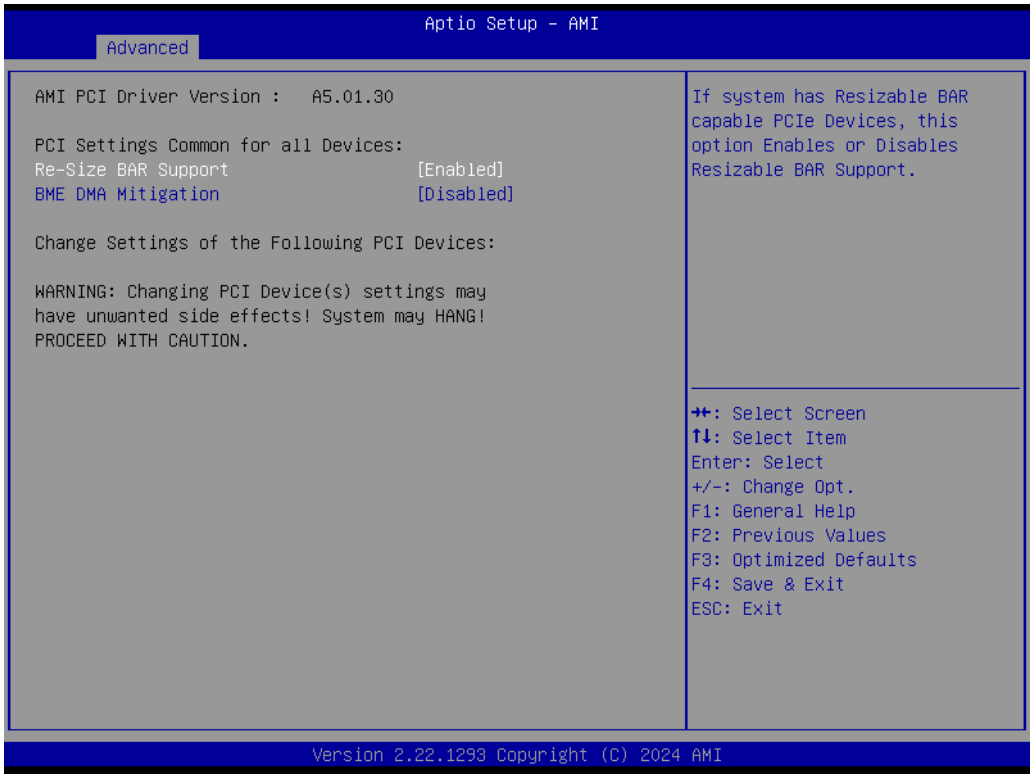


Figure 3.28 Console Redirection Settings

3.4.12 PCI Subsystem Settings

3.4.12.1 ACPI Report Method Configuration

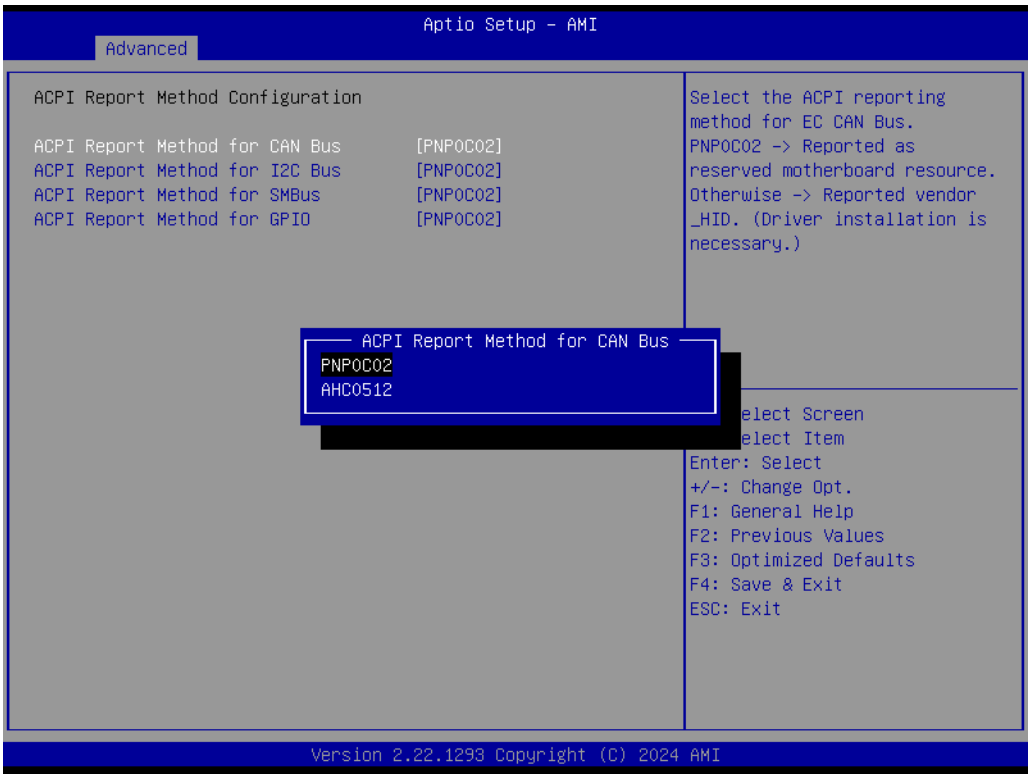


Figure 3.29 ACPI Report Method Configuration

- **ACPI Report Method for CAN Bus**
  Select the ACPI reporting method for EC CAN Bus. PNP0C02 -> Reported as reserved motherboard resource.
  Otherwise -> Reported vendor _HID. (Driver installation is necessary.)
- **ACPI Report Method for I2C Bus**
  Select the ACPI reporting method for EC I2C Bus. PNP0C02 -> Reported as reserved motherboard resource.
  Otherwise -> Reported vendor _HID. (Driver installation is necessary.)
- **ACPI Report Method for SMBus**
  Select the ACPI reporting method for EC SMBus. PNP0C02 -> Reported as reserved motherboard resource.
  Otherwise -> Reported vendor _HID. (Driver installation is necessary.)
- **ACPI Report Method for GPIO**
  Select the ACPI reporting method for EC GPIO.
  PNP0C02 -> Reported as reserved motherboard resource.
  Otherwise -> Reported vendor _HID. (Driver installation is necessary.)

3.4.13 USB Configuration

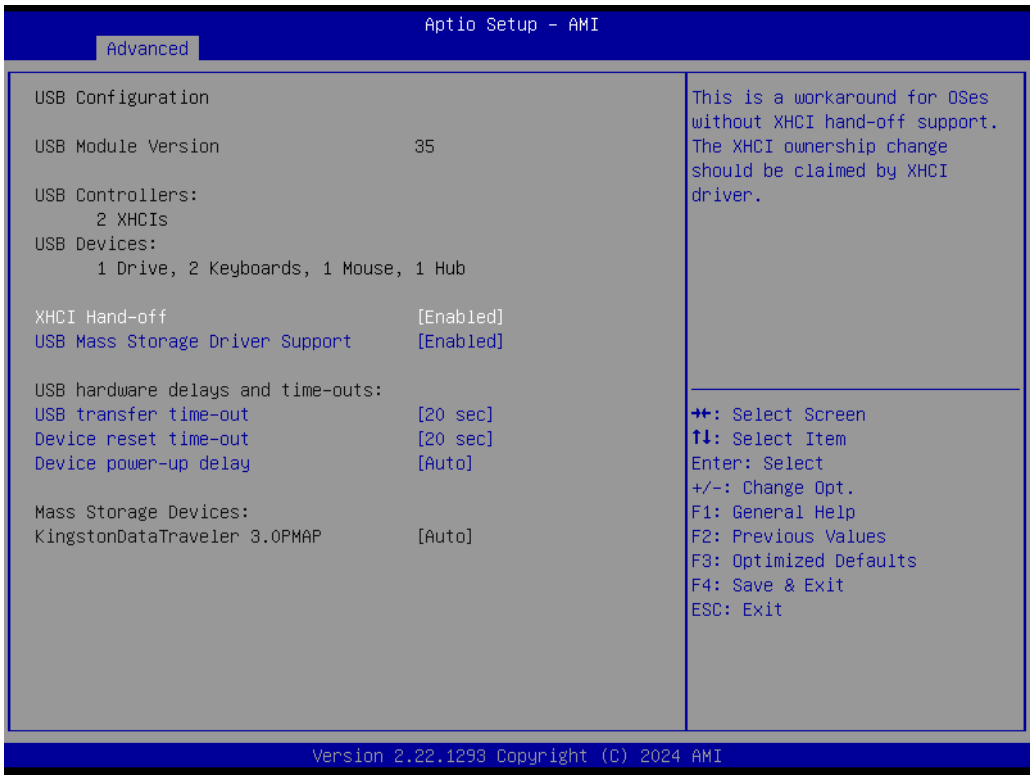


Figure 3.30 USB Configuration

- **XHCI Hand-off**
  This is a workaround for OS without XHCI hand-off support. The XHCI ownership change should be claimed by the XHCI driver.
- **USB Mass Storage Driver Support**
  Enable/Disable USB Mass Storage Driver Support.
- **USB transfer time-out**
  The time-out value for Control, Bulk, and Interrupt transfers.
- **Device reset time-out**
  USB mass storage device Start Unit command time-out.
- **Device power-up delay**
  Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses the default value: for a Root port it is 100 ms, for a Hub port the delay is taken from the Hub descriptor.

3.4.14 Network Stack Configuration

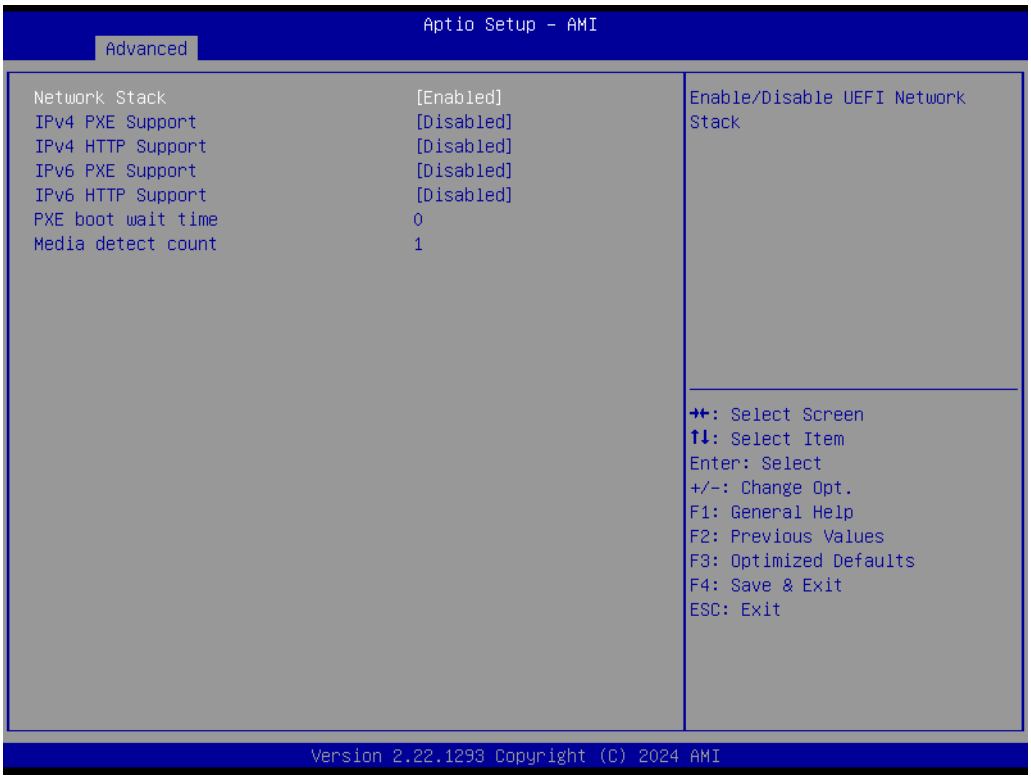


Figure 3.31 Network Stack Configuration

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

3.4.15 NVMe Configuration

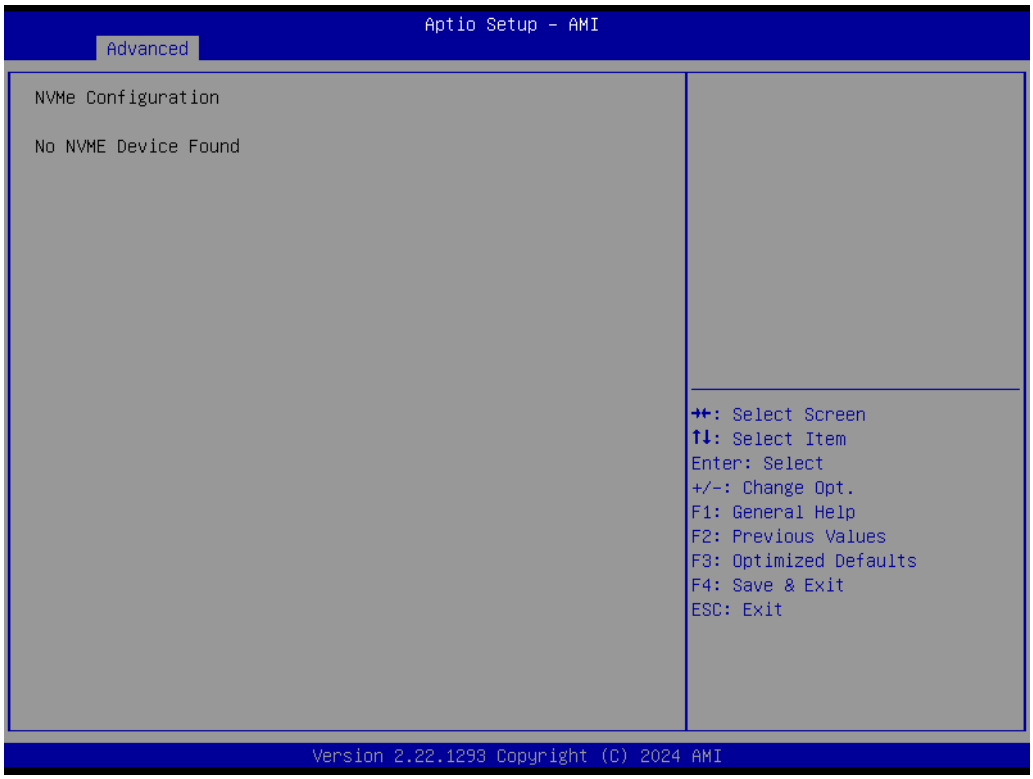


Figure 3.32 NVMe Configuration

3.4.16 Dual BIOS Configuration

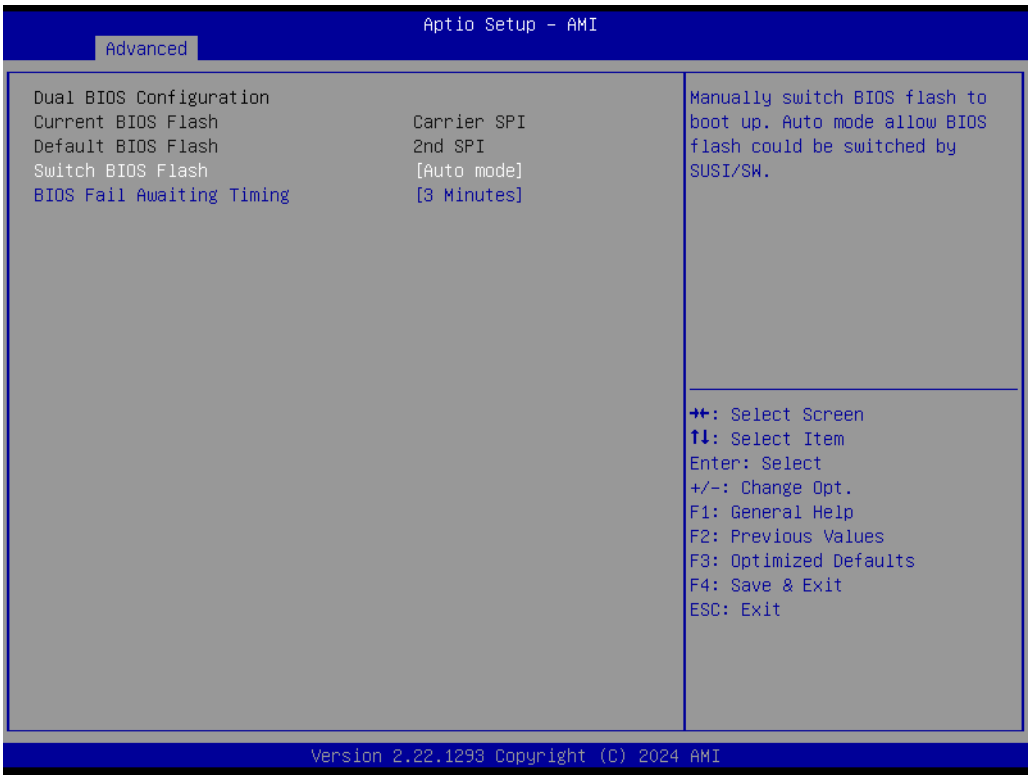


Figure 3.33 Dual BIOS Configuration

- **Switch BIOS Flash**
  Manually switch BIOS flash to boot up. Auto mode allows BIOS flash to be switched by SUSI/SW.
- **BIOS Fail Awaiting Timing**
  Determine specific timing to monitor if BIOS hasn't yet booted up successfully; then BIOS will be switched to another one.

3.4.17 Intel® Ethernet Controller I226-LMvP

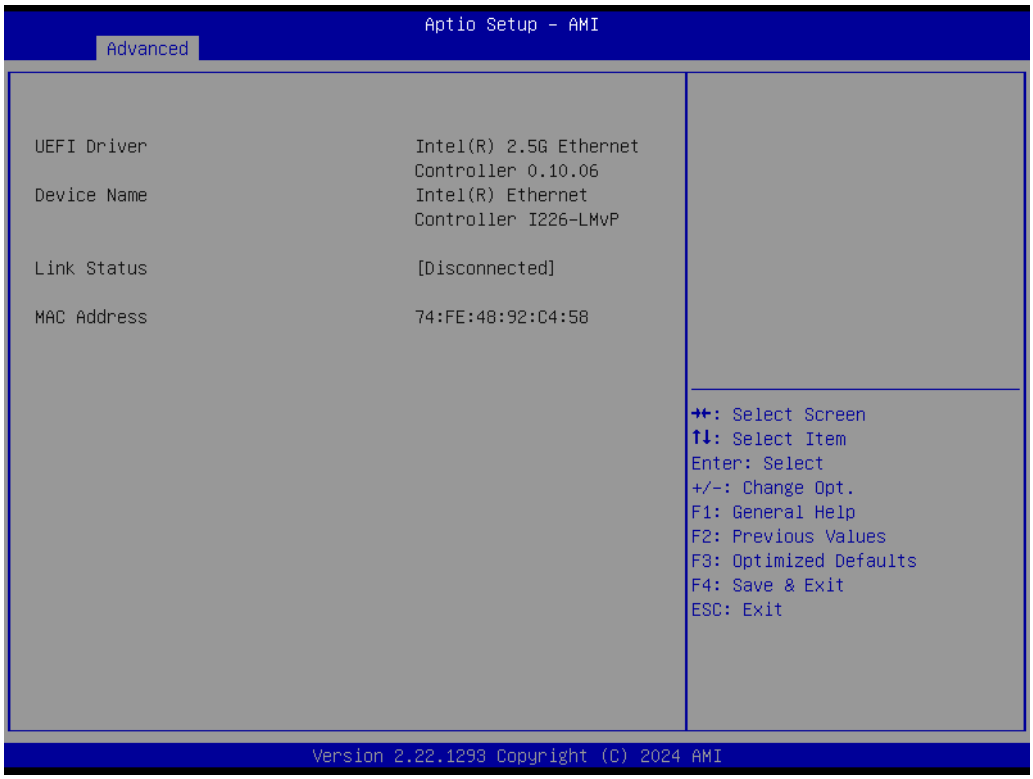


Figure 3.34 Intel® Ethernet Controller I226-LMvP

3.5 Chipset Setup

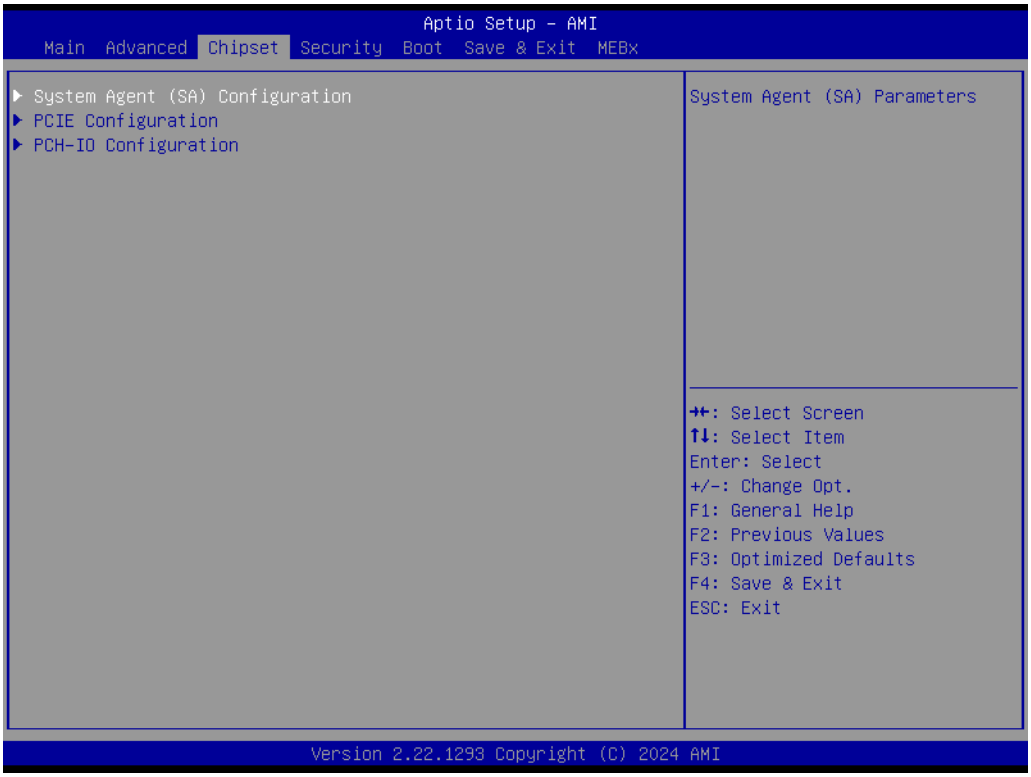


Figure 3.35 Chipset Setup

- **System Agent (SA) Configuration**
  System Agent Parameters.
- **PCIE Configuration**
  PCIE Parameters.
- **PCH-IO Configuration**
  PCH Parameters.

3.5.1 System Agent (SA) Configuration



Figure 3.36 System Agent (SA) Configuration

- **Memory Configuration**
  Memory Configuration Parameters.
- **Graphics Configuration**
- **VMD setup menu**
  VMD Configuration.
- **VT-d**
  VT-d capability.
- **Above 4GB MMIO BIOS assignment**
  Enable/Disable above 4GB memory-mapped IO BIOS assignment. This is enabled automatically when aperture size is set to 2048MB.

3.5.1.1 Memory Configuration

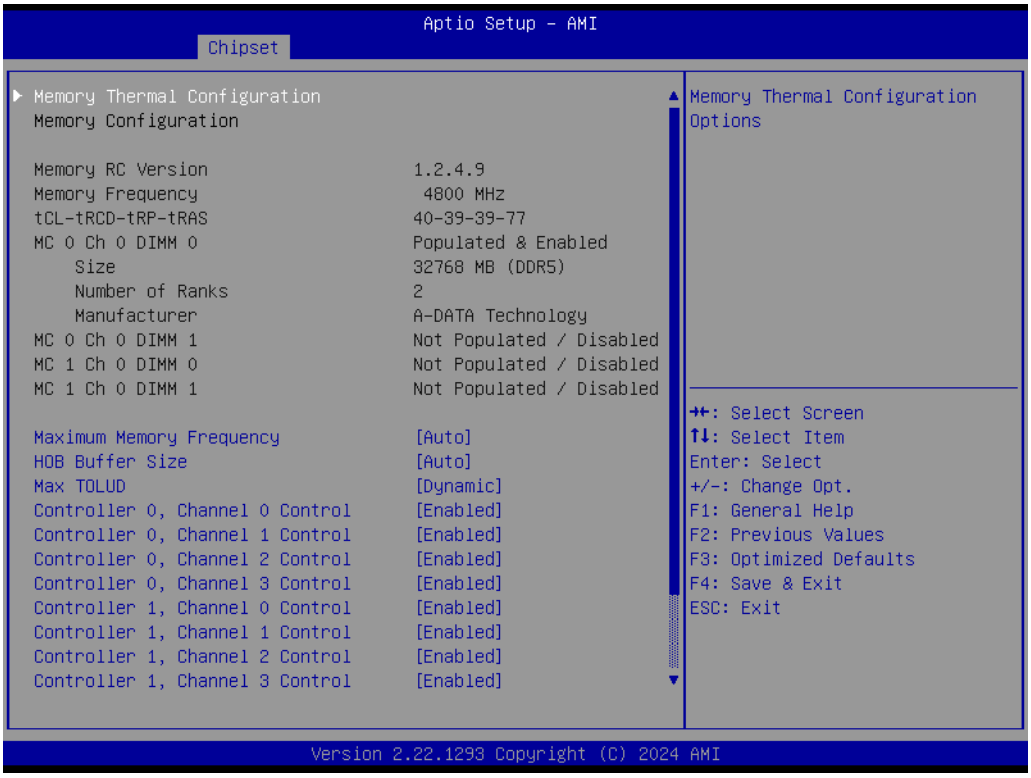


Figure 3.37 Memory Configuration

- **Maximum Memory Frequency**
  Maximum Memory Frequency Selections in MHz.
- **HOB Buffer Size**
  Size to set HOB Buffer.
- **Max TOLUD**
  Maximum value of TOLUD. Dynamic assignment will adjust TOLUD automatically based on the largest MMIO length of the installed graphics controller.
- **Fast Boot**
  Enable/Disable fast path through the MRC.

3.5.1.2 Graphics Configuration

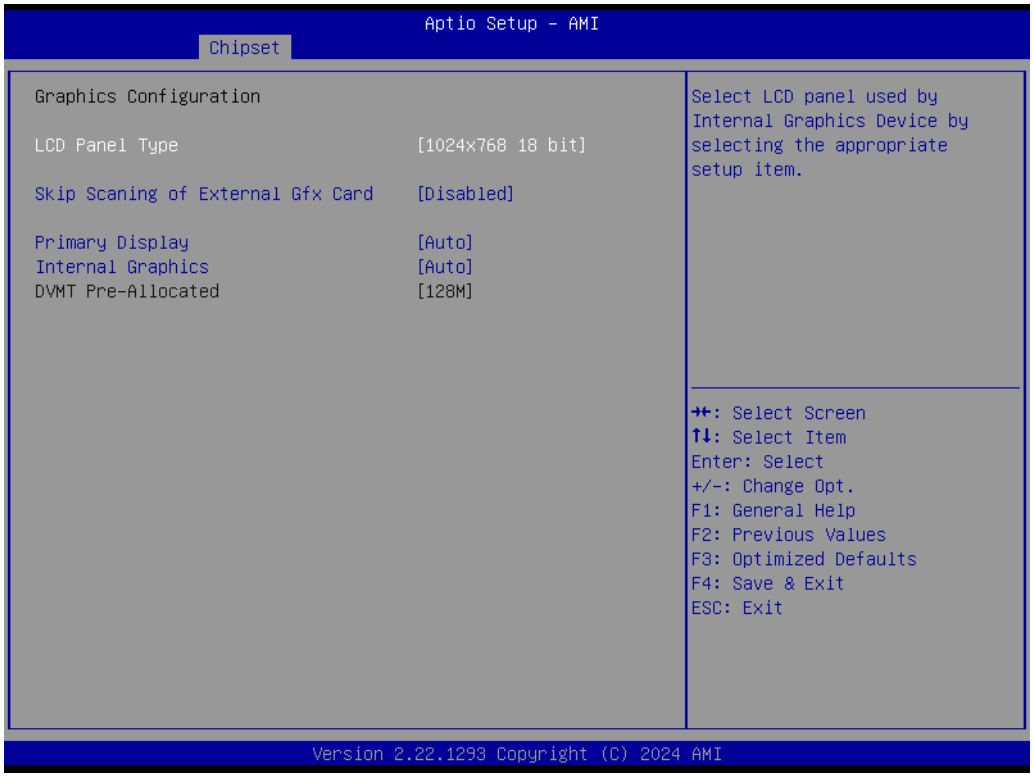


Figure 3.38 Graphics Configuration

- **LCD Panel Type**
  Select the LCD panel used by the Internal Graphics Device by selecting the appropriate setup item.
- **Skip Scanning of External Gfx Card**
  If Enabled, it will not scan for an External Gfx Card on PEG and PCH PCIE Ports.
- **Primary Display**
  Select which of IGFX/PEG/PCI Graphics devices should be the Primary Display Or select HG for Hybrid Gfx.
- **Internal Graphics**
  Keep IGFX enabled based on the setup options.
- **DVMT Pre-Allocated**
  Select DVMT5.0 pre-allocated (fixed) Graphics Memory size used by the internal graphics device.

3.5.1.3 VMD Setup Menu

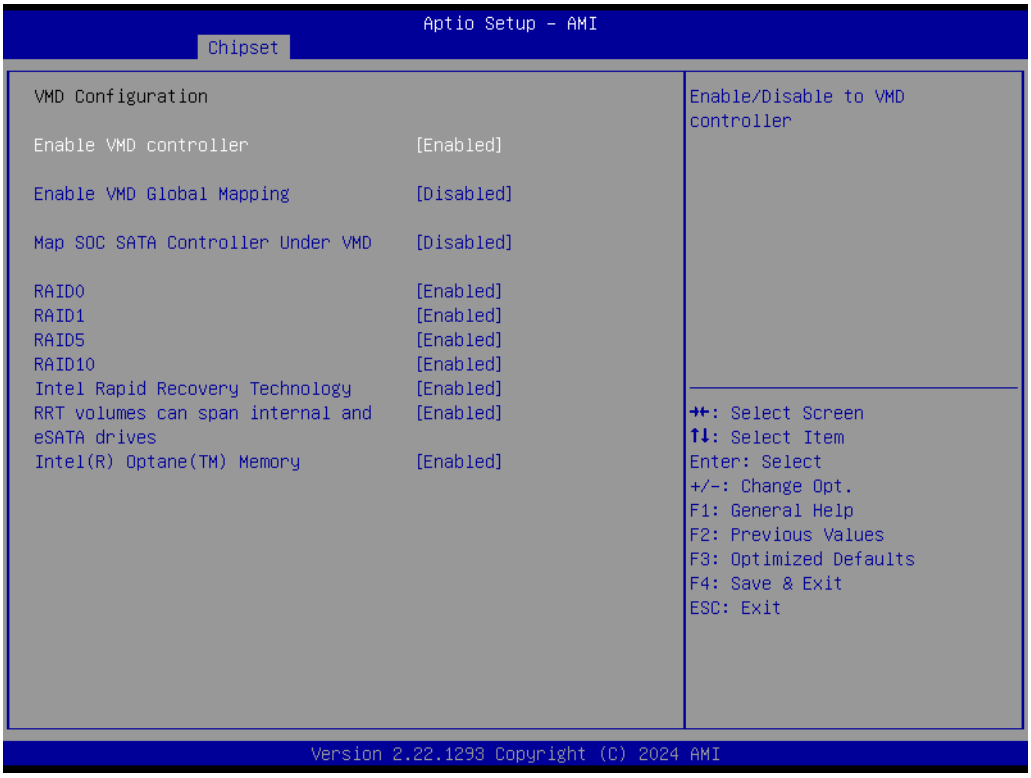


Figure 3.39 VMD Setup Menu

- **Enable VMD controller**
  Enable/Disable to VMD controller.
- **Enable VMD Global Mapping**
  Enable/Disable to VMD Global Mapping.
- **Map SOC SATA Controller Under VMD**
- **RAID0**
  Enable/Disable RAID0 feature.
- **RAID1**
  Enable/Disable RAID1 feature.
- **RAID5**
  Enable/Disable RAID5 feature.
- **RAID10**
  Enable/Disable RAID10 feature.
- **Intel Rapid Recovery Technology RRT volumes can span internal and eSATA drivers**
- **Intel(R) Optane(TM) Memory**
  Enable/Disable System Acceleration with the Intel(R) Optane(TM) Memory feature.

3.5.2 PCI Express Configuration

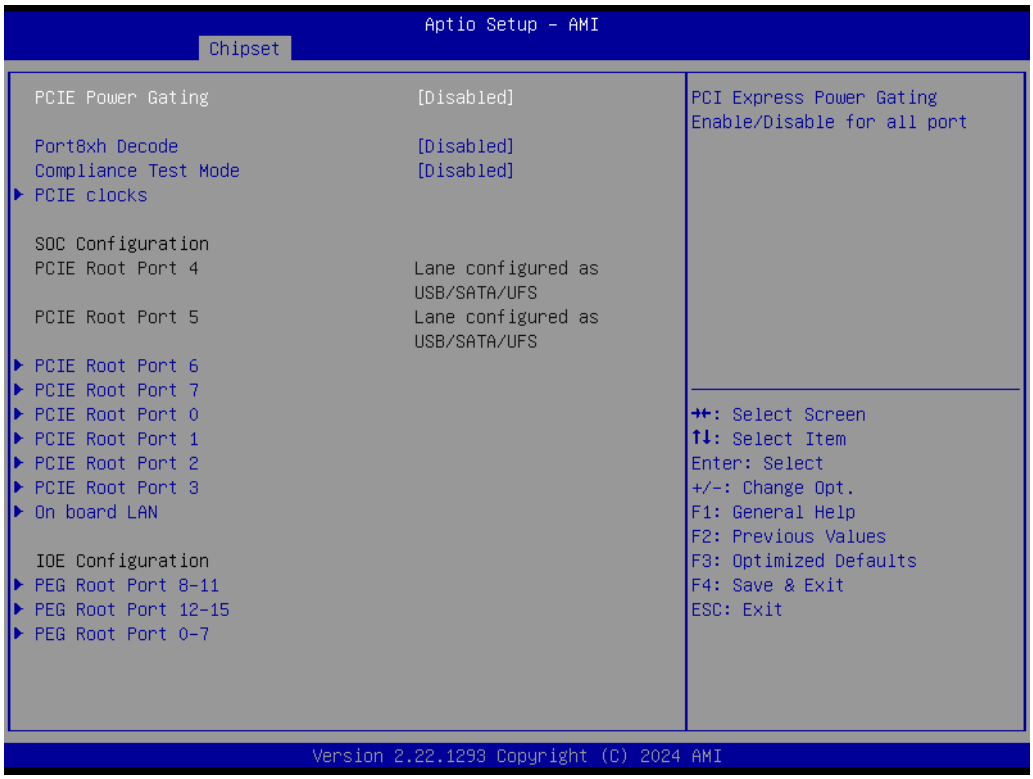


Figure 3.40 PCI Express Configuration

- **PCIE Power Gating**
  PCIe Express Power Gating Enable/Disable for all ports.
- **PCIE clocks**
- **PCIE Root Port 6**
- **PCIE Root Port 7**
- **PCIE Root Port 0**
- **PCIE Root Port 1**
- **PCIE Root Port 2**
- **PCIE Root Port 3**
- **On board LAN**
- **PEG Root Port 8-11**
- **PEG Root Port 12-15**
- **PEG Root Port 0-7**

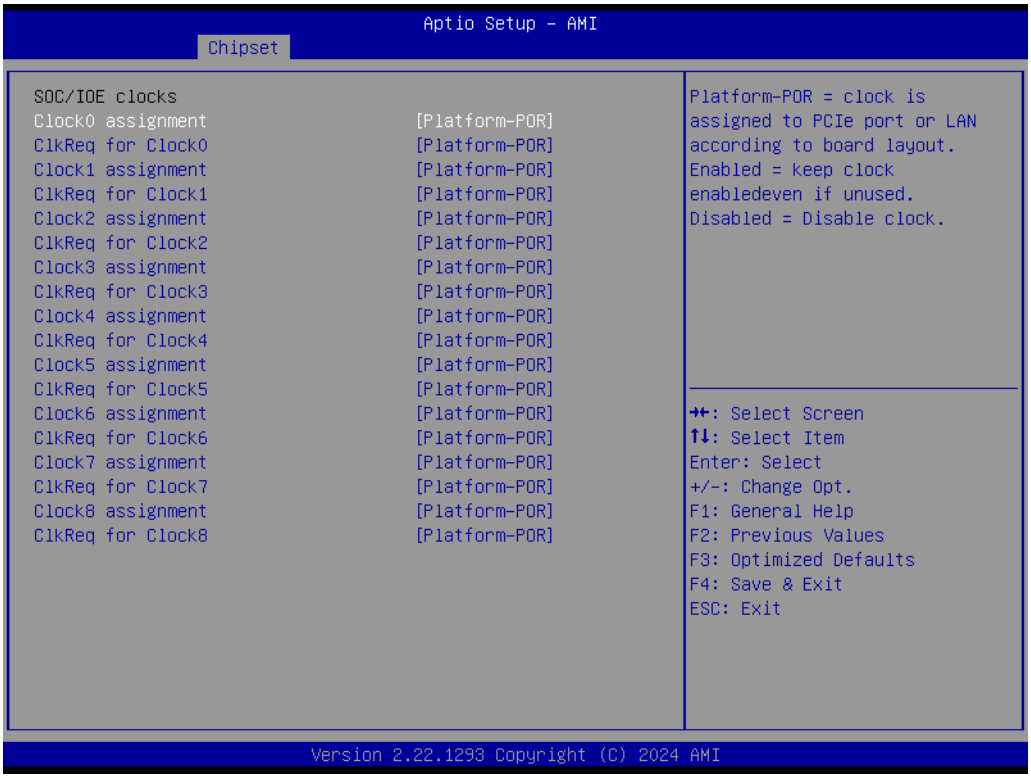


Figure 3.41 PCIE Clocks

- **Clock0 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock0**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock1 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock1**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock2 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock2**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock3 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock3**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock4 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.

- **ClkReq for Clock4**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock5 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock5**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock6 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock6**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock7 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock7**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.
- **Clock8 assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled=keep clock enabled even if unused. Disabled=Disable clock.
- **ClkReq for Clock8**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.

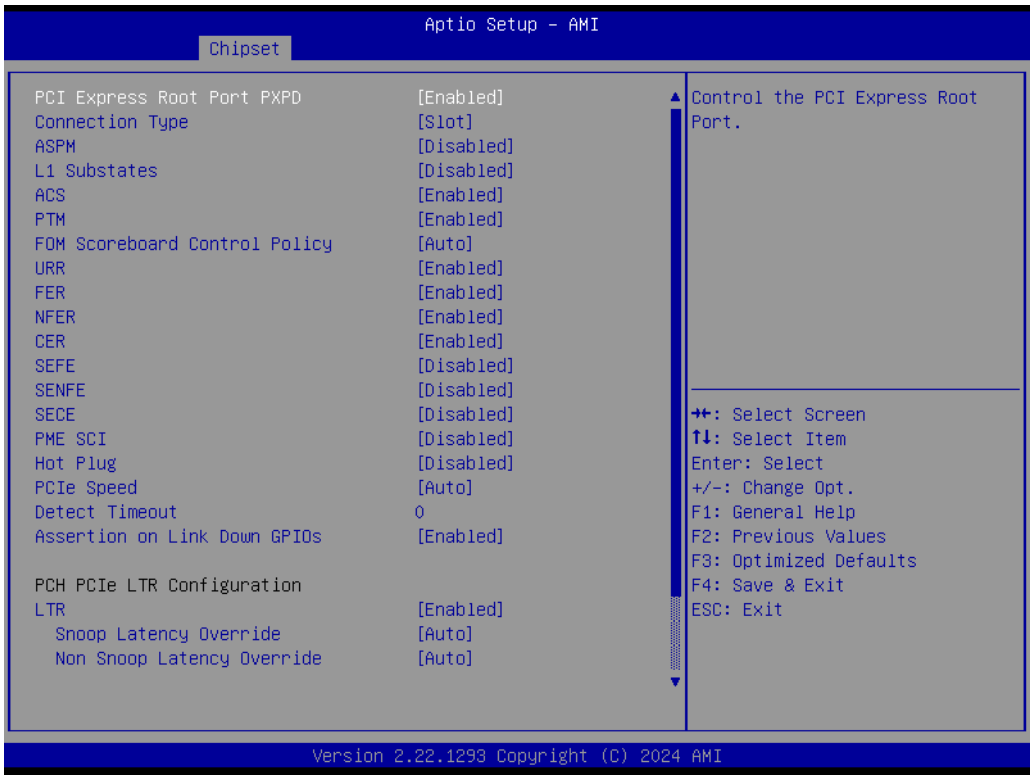


Figure 3.42 PCIE Root Port

- **PCI Express Root Port PXPD**
  Control the PCI Express Root Port.

3.5.2.1 SATA Drives

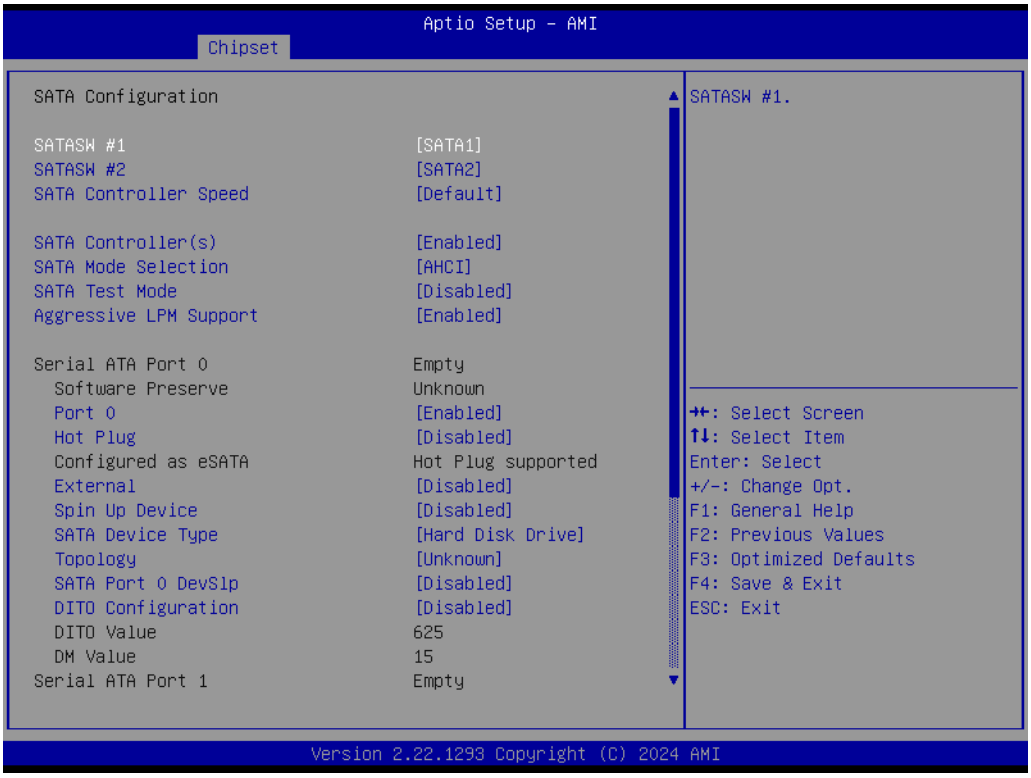


Figure 3.43 SATA Drives

- **SATASW#1**
  SATASW#1.
- **SATASW#2**
  SATASW#2.
- **SATA Controller(s)**
  Enable/Disable SATA Device.
- **SATA Mode Selection**
  Determines how SATA controller(s) operate.
- **SATA Test Mode**
  Test Mode Enable/Disable (Loop Back).
- **Aggressive LPM Support**
  Enable PCH to aggressively enter link power state.
- **SATA Controller Speed**
  Indicates the maximum speed the SATA controller can support.
- **Port 0**
  Enable or Disable SATA Port.
- **Hot Plug**
- **External**
- **Spin up Device**
- **SATA Device Type**
  Identify if the SATA port is connected to a Solid State Drive or Hard Disk Drive.
- **Topology**
- **SATA Port 0 DevSlp**
- **DIT0 Configuration**
  Enable/Disable DIT0 Configuration.

3.5.2.2 USB Configuration

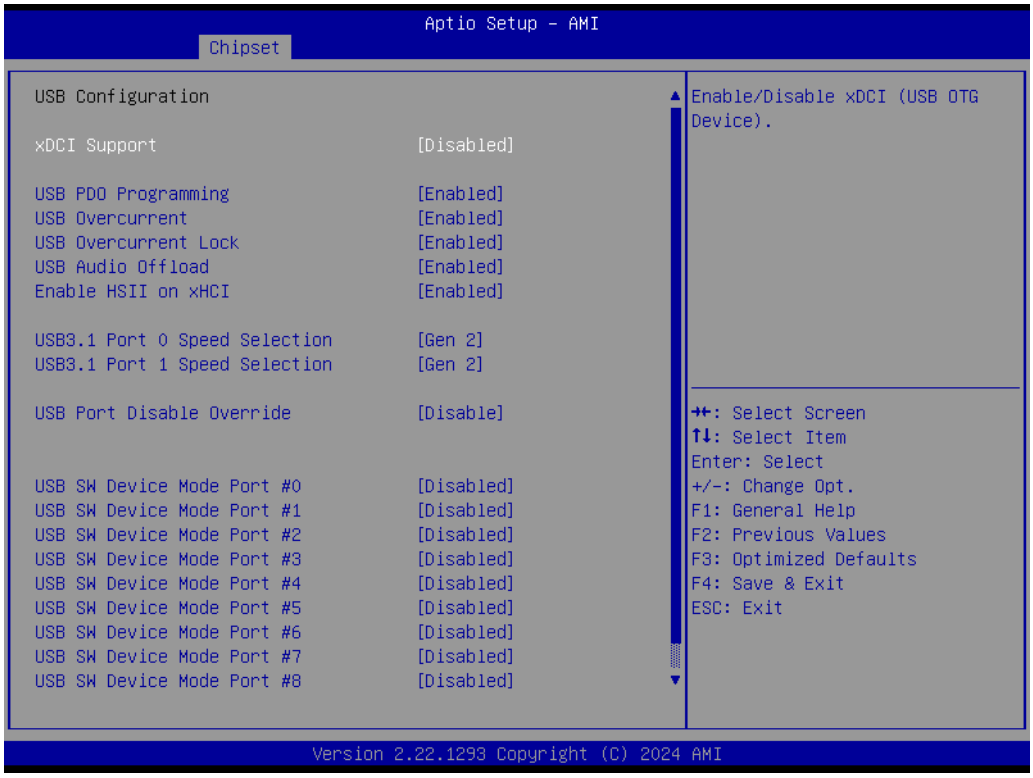


Figure 3.44 USB Configuration

- **xDCI Support**
  Enable/Disable xDCI (US OTG Device).
- **USB PD0 Programming**
  Select ‘Enable’ if Port Disable Override functionality is used.
- **USB Overcurrent**
  Select ‘Disabled’ for pin-based debug. If pin-based debug is enabled bit USB overcurrent is not disabled, USB Dbc does not work.
- **USB Overcurrent Lock**
  Select ‘Enabled’ if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.
- **USB Audio offload**
  Enable/Disable USB Audio Offlaid functionality.
- **Enable HSII on xHCI**
  Enable/Disable HSII feature. It may lead to increased power consumption.
- **USB3.1 Port 0 Speed Selection**
  USB 3.1 Speed selection; Gen1 or Gen2.
- **USB3.1 Port 1 Speed Selection**
  USB 3.1 Speed selection; Gen1 or Gen2.
- **USB Port Disable Override**
  Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
- **USB SW Device Mode Port #0**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #1**
  Enable Connector Event for device subscription.

- **USB SW Device Mode Port #2**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #3**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #4**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #5**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #6**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #7**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #8**
  Enable Connector Event for device subscription.
- **USB SW Device Mode Port #9**
  Enable Connector Event for device subscription.

3.5.2.3 Security Configuration

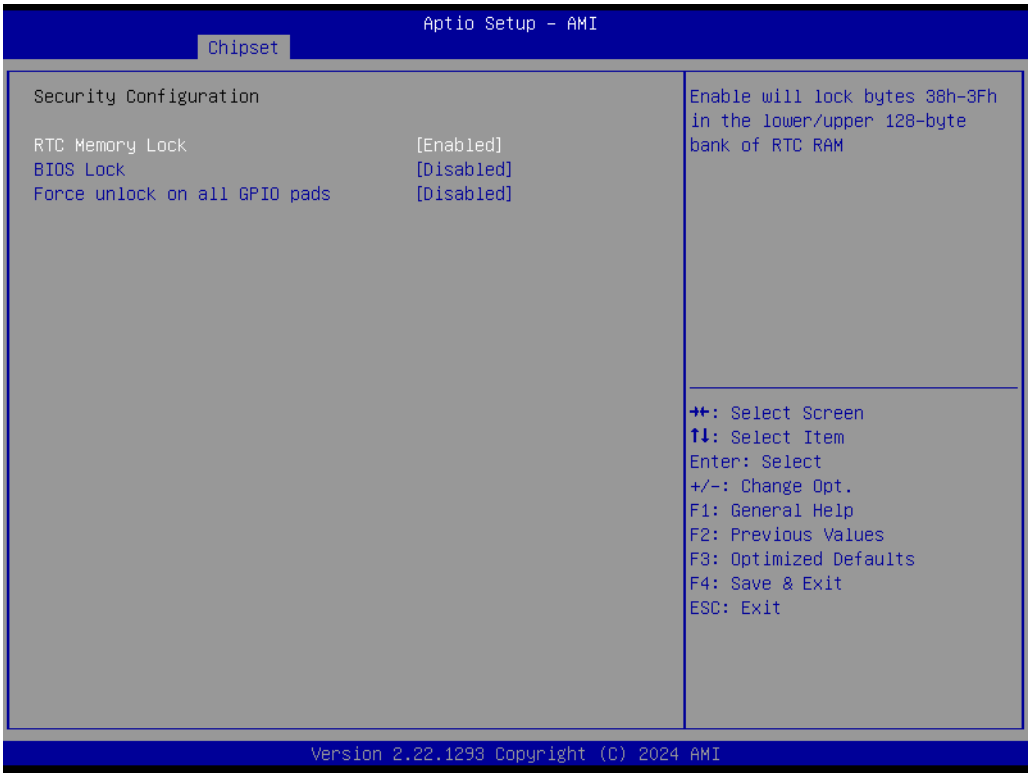


Figure 3.45 Security Configuration

- **RTC Memory Lock**
  Enable will lock bytes 38h-3Fh in the lower/upper 126 –byte bank of RTC RAM.
- **BIOS Lock**
  Enable/Disable the PCH BIOS lock enable feature. it is required to be enabled to ensure SMM protection of flash.
- **Force unlock on all GPIO pads**
  If Enabled, BIOS will force all GPIO pads to be in an unlocked state.

3.5.2.4 HD Audio Subsystem Configuration Settings

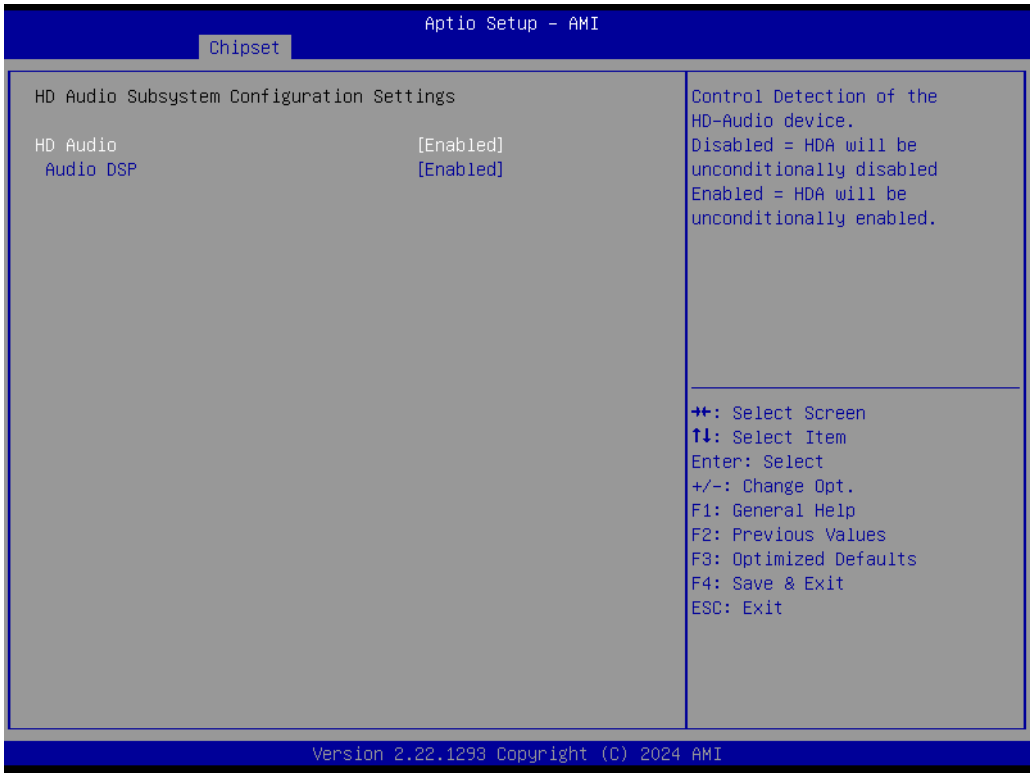


Figure 3.46 HD Audio Subsystem Configuration Settings

- **HD Audio**
  Control Detection of the HD-Audio device. Disabled=HDA will be unconditionally disabled. Enabled=HDA will be unconditionally enabled.
- **Audio DSP**
  Enable/Disable Audio DSP.

3.5.3 PCH-IO Configuration

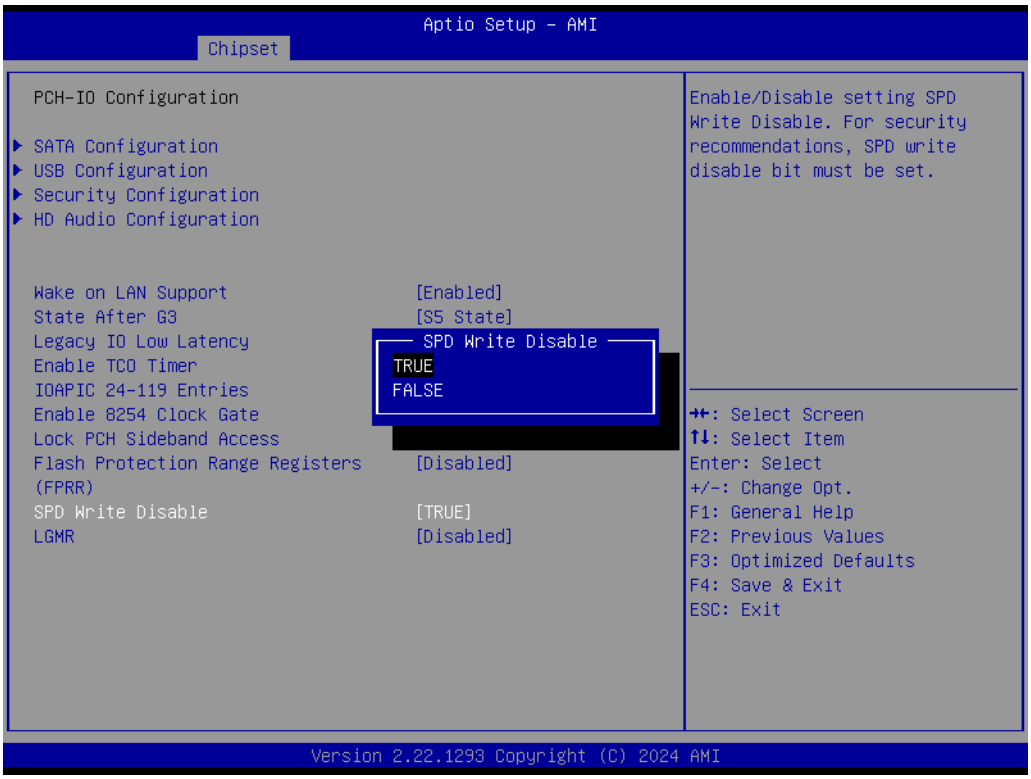


Figure 3.47 PCH-IO Configuration

- **SATA Configuration**
  SATA device option settings.
- **USB Configuration**
  USB Configuration settings.
- **Security Configuration**
  Security Configuration settings.
- **HD Audio Configuration**
  HD audio subsystem configuration settings.
- **Wake on LAN Support**
  Seriallo configuration settings.
- **State After G3**
  Specify what state to go to when power is re-applied after a power failure (G3 state).
- **Legacy IO Low Latency**
- **Enable TC0 Timer**
  PCIe Ref.5%.
- **I0APIC 24-119 Entries**
- **Enable 8254 Clock Gate**
- **Lock PCH Sideband Access**
- **Flash Protection Range Registers (FPRR)**
- **SPD Write Disable**
  Enable/Disable setting SPD Write Disable. For security recommendations, the SPD write disable bit must be set.
- **LGMR**

3.6 Security Chipset



Figure 3.48 Security Chipset

- **Administrator Password**
  Set Setup Administrator Password.
- **User Password**
  Set User Password.
- **Secure Boot**
  Secure Boot Configuration.

3.6.1 Secure Boot



Figure 3.49 Secure Boot

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

3.6.2 Boot Setup

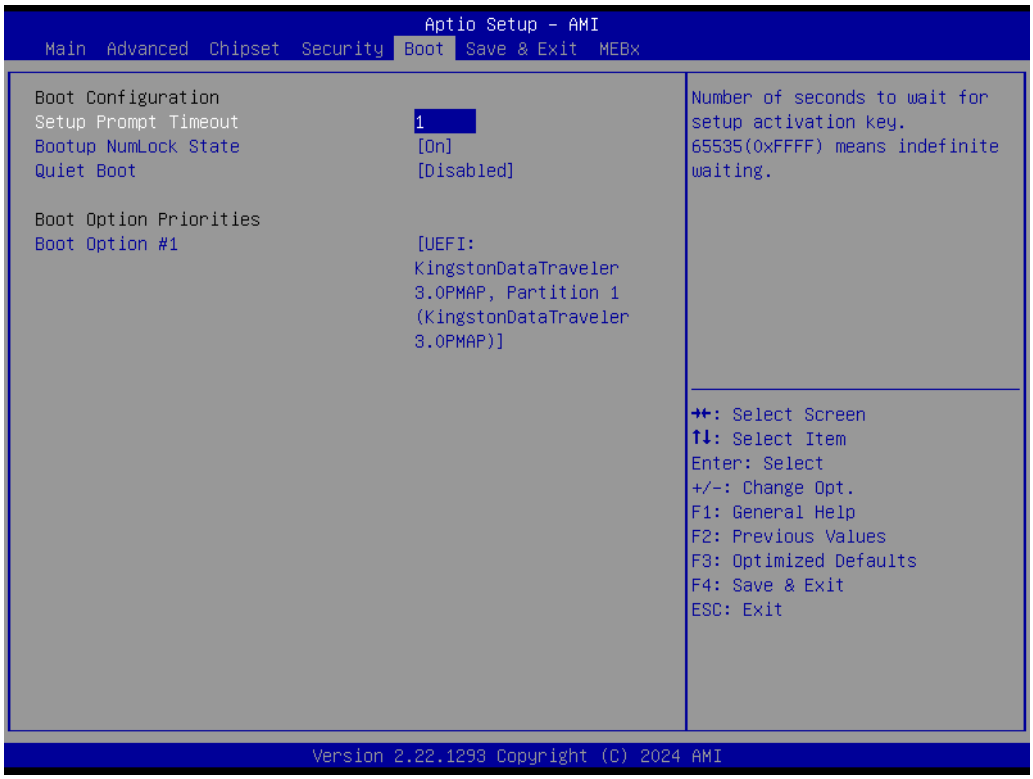


Figure 3.50 Boot Setup

- **Setup Prompt Timeout**
  Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
- **Bootup NumLock State**
  Select the keyboard NumLock state.
- **Quiet Boot**
  Enables or disables the Quiet Boot option.
- **Boot Option #1**
  Sets the system boot order.

3.7 Save & Exit

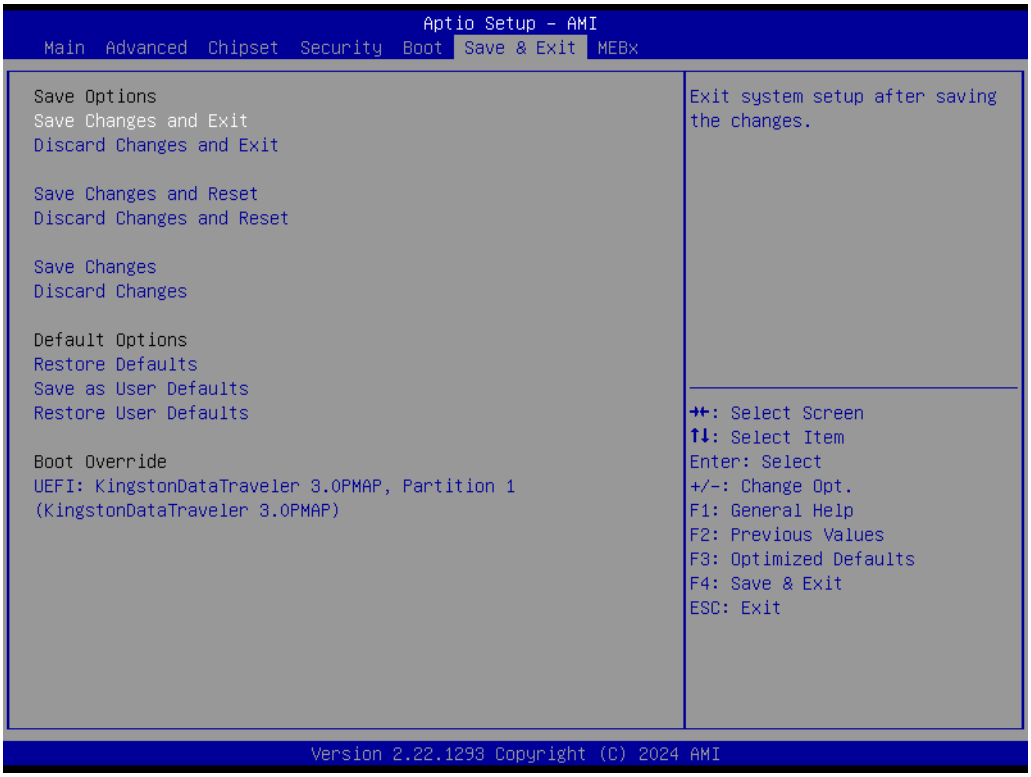


Figure 3.51 Save & Exit

- **Save Changes and Exit**
  Exit system setup after saving the changes.
- **Discard Changes and Exit**
  Exit system setup without saving any changes.
- **Save Changes and Reset**
  Reset the system after saving the changes.
- **Discard Changes and Reset**
  Reset system setup without saving any changes.
- **Save Changes**
  Save Changes done so far to any of the setup options.
- **Discard Changes**
  (005B) Discard Changes done so far to any of the setup options.
- **Restore Defaults**
  Restore/Load Default values for all the setup options.
- **Save as User Defaults**
  Save the changes done so far as User Defaults.
- **Restore User Defaults**
  Restore the User Defaults to all the setup options.
- **Boot Override**

3.8 MEBx



Figure 3.52 MEBx

Chapter 4

S/W Introduction & Installation

- S/W Introduction
- Driver Installation
- Advantech iManager

4.1 S/W Introduction

The mission of Advantech Embedded Software Services is to “Enhance quality of life with Advantech platforms and Microsoft Windows embedded technology”. We enable Windows Embedded software products on Advantech platforms to more effectively support the embedded computing community. Customers are freed from the hassle of dealing with multiple vendors (Hardware suppliers, System integrators, Embedded OS distributors) for projects. Our goal is to make Windows Embedded Software solutions easily and widely available to the embedded computing community.

4.2 Driver Installation

The Intel Chipset Software Installation (CSI) utility installs the Windows INF files that explain how chipset components are configured to the operating system.

4.2.1 Windows Driver Setup

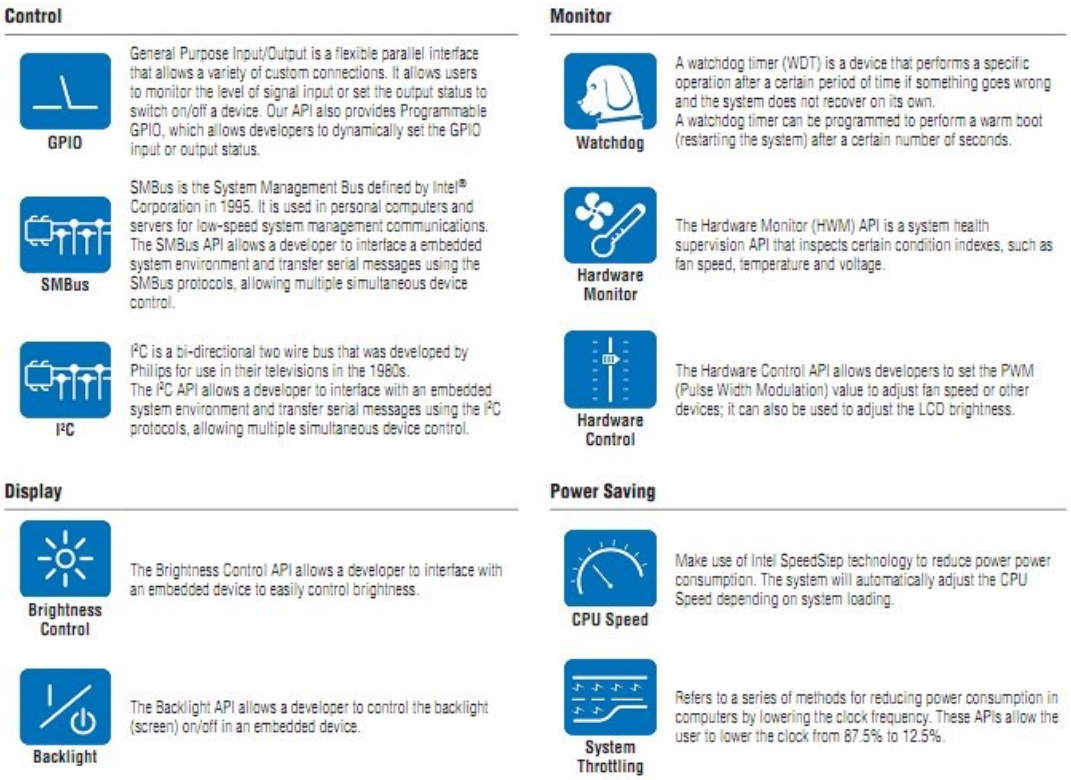
To install the drivers on a Windows-based operating system, please connect to the Internet and navigate to the website http://support.advantech.com.tw. Next, download the drivers that you want to install. Then follow the Driver Setup instructions to complete the installation.

4.2.2 Other OS

Linux Ubuntu

4.3 Advantech iManager

Advantech's platforms come equipped with iManager, a microcontroller that provides embedded features for system integrators. Embedded features have been moved from the OS/BIOS level to the board level, to increase reliability and simplify integration. iManager runs whether the operating system is running or not; it can count the boot times and running hours of the device, monitor device health, and provide an advanced watchdog to handle errors just as they happen. iManager also comes with a secure and encrypted EEPROM for storing important security key or other customer-defined information. All the embedded functions are configured through the API and provide corresponding utilities. These APIs comply with the PICMG EAPI (Embedded Application Programmable Interface) specification and utilize the same structures. It makes these embedded features easier to integrate, speeds up development schedules, and provides the customer with software continuity when upgrading hardware. For more details on how to use the APIs and utilities, please refer to the Advantech iManager 2.0 Software API User Manual.



Appendix A

Pin Assignment

This appendix provides you with information about the hardware pin assignment for the SOM-5885 CPU System on Module.

Sections include:

- SOM-5885 Type 6 Pin Assignment

A.1 SOM-5885 Pin Assignment

This section gives SOM-5885 pin assignment on the COM Express connector, compliant with COMR.0 R3.1 Type 6 pin-out definitions. For more details about how to use these pins and to obtain a design reference, please contact Advantech for a design guide, checklist, reference schematic, and other hardware/software support.

Table A.1: SOM-5885 Pin Assignments

SOM-5885 Rows A, B			
A1	GND (FIXED)	B1	GND (FIXED)
A2	GBE0_MDI3-	B2	GBE0_ACT#
A3	GBE0_MDI3+	B3	LPC_FRAME#
A4	GBE0_LINK100#	B4	LPC_AD0
A5	GBE0_LINK1000#	B5	LPC_AD1
A6	GBE0_MDI2-	B6	LPC_AD2
A7	GBE0_MDI2+	B7	LPC_AD3
A8	GBE0_LINK#	B8	N/A
A9	GBE0_MDI1-	B9	N/A
A10	GBE0_MDI1+	B10	LPC_CLK
A11	GND (FIXED)	B11	GND (FIXED)
A12	GBE0_MDI0-	B12	PWRBTN#
A13	GBE0_MDI0+	B13	SMB_CK
A14	N/A	B14	SMB_DAT
A15	SUS_S3#	B15	SMB_ALERT#
A16	SATA0_TX+	B16	SATA1_TX+
A17	SATA0_TX-	B17	SATA1_TX-
A18	SUS_S4#	B18	SUS_STAT#
A19	SATA0_RX+	B19	SATA1_RX+
A20	SATA0_RX-	B20	SATA1_RX-
A21	GND (FIXED)	B21	GND (FIXED)
A22	SATA2_TX+	B22	SATA3_TX+
A23	SATA2_TX-	B23	SATA3_TX-
A24	SUS_S5#	B24	PWR_OK
A25	SATA2_RX+	B25	SATA3_RX+
A26	SATA2_RX-	B26	SATA3_RX-
A27	BATLOW#	B27	WDT
A28	(S)ATA_ACT#	B28	N/A
A29	AC/HDA_SYNC	B29	AC/HDA_SDIN1
A30	AC/HDA_RST#	B30	AC/HDA_SDIN0
A31	GND (FIXED)	B31	GND (FIXED)
A32	AC/HDA_BITCLK	B32	SPKR
A33	AC/HDA_SDOUT	B33	I2C_CK
A34	BIOS_DIS0#	B34	I2C_DAT
A35	THRMTRIP#	B35	THRM#
A36	USB6-	B36	USB7-
A37	USB6+	B37	USB7+
A38	USB_6_7_OC#	B38	USB_4_5_OC#
A39	USB4-	B39	USB5-

Table A.1: SOM-5885 Pin Assignments			
A40	USB4+	B40	USB5+
A41	GND (FIXED)	B41	GND (FIXED)
A42	USB2-	B42	USB3-
A43	USB2+	B43	USB3+
A44	USB_2_3_OC#	B44	USB_0_1_OC#
A45	USB0-	B45	USB1-
A46	USB0+	B46	USB1+
A47	VCC_RTC	B47	ESPI_EN#
A48	RSMRST_OUT#	B48	N/A
A49	GBE0_SDP	B49	SYS_RESET#
A50	LPC_SERIRQ	B50	CB_RESET#
A51	GND (FIXED)	B51	GND (FIXED)
A52	PCIE_TX5+	B52	PCIE_RX5+
A53	PCIE_TX5-	B53	PCIE_RX5-
A54	GPI0	B54	GPO1
A55	PCIE_TX4+	B55	PCIE_RX4+
A56	PCIE_TX4-	B56	PCIE_RX4-
A57	GND	B57	GPO2
A58	PCIE_TX3+	B58	PCIE_RX3+
A59	PCIE_TX3-	B59	PCIE_RX3-
A60	GND (FIXED)	B60	GND (FIXED)
A61	PCIE_TX2+	B61	PCIE_RX2+
A62	PCIE_TX2-	B62	PCIE_RX2-
A63	GPI1	B63	GPO3
A64	PCIE_TX1+	B64	PCIE_RX1+
A65	PCIE_TX1-	B65	PCIE_RX1-
A66	GND	B66	WAKE0#
A67	GPI2	B67	WAKE1#
A68	PCIE_TX0+	B68	PCIE_RX0+
A69	PCIE_TX0-	B69	PCIE_RX0-
A70	GND (FIXED)	B70	GND (FIXED)
A71	LVDS_A0+	B71	LVDS_B0+
A72	LVDS_A0-	B72	LVDS_B0-
A73	LVDS_A1+	B73	LVDS_B1+
A74	LVDS_A1-	B74	LVDS_B1-
A75	LVDS_A2+	B75	LVDS_B2+
A76	LVDS_A2-	B76	LVDS_B2-
A77	LVDS_VDD_EN	B77	LVDS_B3+
A78	LVDS_A3+	B78	LVDS_B3-
A79	LVDS_A3-	B79	LVDS_BKLT_EN
A80	GND (FIXED)	B80	GND (FIXED)
A81	LVDS_A_CK+	B81	LVDS_B_CK+
A82	LVDS_A_CK-	B82	LVDS_B_CK-
A83	LVDS_I2C_CK	B83	LVDS_BKLT_CTRL
A84	LVDS_I2C_DAT	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	GP_SPI_MOSI	B86	VCC_5V_SBY

Table A.1: SOM-5885 Pin Assignments			
A87	eDP_HPD	B87	VCC_5V_SBY
A88	PCIE_CLK_REF+	B88	BIOS_DIS1#
A89	PCIE_CLK_REF-	B89	N/A
A90	GND (FIXED)	B90	GND (FIXED)
A91	SPI_POWER	B91	N/A
A92	SPI_MISO	B92	N/A
A93	GPO0	B93	N/A
A94	SPI_CLK	B94	N/A
A95	SPI_MOSI	B95	N/A
A96	TPM_PP	B96	N/A
A97	N/A	B97	SPI_CS#
A98	SER0_TX	B98	GP_SPI_MISO
A99	SER0_RX	B99	GP_SPI_CK
A100	GND (FIXED)	B100	GND (FIXED)
A101	SER1_TX	B101	FAN_PWMOUT
A102	SER1_RX	B102	FAN_TACHIN
A103	LID#	B103	SLEEP#
A104	VCC_12V	B104	VCC_12V
A105	VCC_12V	B105	VCC_12V
A106	VCC_12V	B106	VCC_12V
A107	VCC_12V	B107	VCC_12V
A108	VCC_12V	B108	VCC_12V
A109	VCC_12V	B109	VCC_12V
A110	GND (FIXED)	B110	GND (FIXED)
SOM-5885 Rows C, D			
C1	GND (FIXED)	D1	GND (FIXED)
C2	GND	D2	GND
C3	USB_SSRX0-	D3	USB_SSTX0-
C4	USB_SSRX0+	D4	USB_SSTX0+
C5	GND	D5	GND
C6	USB_SSRX1-	D6	USB_SSTX1-
C7	USB_SSRX1+	D7	USB_SSTX1+
C8	GND	D8	GND
C9	USB_SSRX2-	D9	USB_SSTX2-
C10	USB_SSRX2+	D10	USB_SSTX2+
C11	GND (FIXED)	D11	GND (FIXED)
C12	USB_SSRX3-	D12	USB_SSTX3-
C13	USB_SSRX3+	D13	USB_SSTX3+
C14	GND	D14	GND
C15	N/A(*Note)	D15	DDI1_CTRLCLK_AUX+
C16	N/A(*Note)	D16	DDI1_CTRLDATA_AUX-
C17	N/A(*Note)	D17	RSVD (*Note)
C18	GND	D18	RSVD (*Note)
C19	PCIE_RX6+	D19	PCIE_TX6+
C20	PCIE_RX6-	D20	PCIE_TX6-
C21	GND (FIXED)	D21	GND (FIXED)
C22	PCIE_RX7+	D22	PCIE_TX7+

Table A.1: SOM-5885 Pin Assignments			
C23	PCIE_RX7-	D23	PCIE_TX7-
C24	DDI1_HPD	D24	GND
C25	N/A(*Note)	D25	GND
C26	N/A(*Note)	D26	DDI1_PAIR0+
C27	N/A (*Note)	D27	DDI1_PAIR0-
C28	N/A (*Note)	D28	GND
C29	N/A(*Note)	D29	DDI1_PAIR1+
C30	N/A(*Note)	D30	DDI1_PAIR1-
C31	GND (FIXED)	D31	GND (FIXED)
C32	DDI2_CTRLCLK_AUX+	D32	DDI1_PAIR2+
C33	DDI2_CTRLDATA_AUX-	D33	DDI1_PAIR2-
C34	DDI2_DDC_AUX_SEL	D34	DDI1_DDC_AUX_SEL
C35	N/A(*Note)	D35	RSVD
C36	DDI3_CTRLCLK_AUX+	D36	DDI1_PAIR3+
C37	DDI3_CTRLDATA_AUX-	D37	DDI1_PAIR3-
C38	DDI3_DDC_AUX_SEL	D38	GND
C39	DDI3_PAIR0+	D39	DDI2_PAIR0+
C40	DDI3_PAIR0-	D40	DDI2_PAIR0-
C41	GND (FIXED)	D41	GND (FIXED)
C42	DDI3_PAIR1+	D42	DDI2_PAIR1+
C43	DDI3_PAIR1-	D43	DDI2_PAIR1-
C44	DDI3_HPD	D44	DDI2_HPD
C45	GP_SPI_CS#	D45	GND
C46	DDI3_PAIR2+	D46	DDI2_PAIR2+
C47	DDI3_PAIR2-	D47	DDI2_PAIR2-
C48	RSVD	D48	GND
C49	DDI3_PAIR3+	D49	DDI2_PAIR3+
C50	DDI3_PAIR3-	D50	DDI2_PAIR3-
C51	GND (FIXED)	D51	GND (FIXED)
C52	PEG_RX0+	D52	PEG_TX0+
C53	PEG_RX0-	D53	PEG_TX0-
C54	N/A	D54	N/A
C55	PEG_RX1+	D55	PEG_TX1+
C56	PEG_RX1-	D56	PEG_TX1-
C57	N/A	D57	GND (FIXED)
C58	PEG_RX2+	D58	PEG_TX2+
C59	PEG_RX2-	D59	PEG_TX2-
C60	GND (FIXED)	D60	GND (FIXED)
C61	PEG_RX3+	D61	PEG_TX3+
C62	PEG_RX3-	D62	PEG_TX3-
C63	GND	D63	GND
C64	GND	D64	GND
C65	PEG_RX4+	D65	PEG_TX4+
C66	PEG_RX4-	D66	PEG_TX4-
C67	RAPID_SHUTDOWN	D67	GND
C68	PEG_RX5+	D68	PEG_TX5+
C69	PEG_RX5-	D69	PEG_TX5-

Table A.1: SOM-5885 Pin Assignments			
C70	GND (FIXED)	D70	GND (FIXED)
C71	PEG_RX6+	D71	PEG_TX6+
C72	PEG_RX6-	D72	PEG_TX6-
C73	GND	D73	GND
C74	PEG_RX7+	D74	PEG_TX7+
C75	PEG_RX7-	D75	PEG_TX7-
C76	GND	D76	GND
C77	GND	D77	GND
C78	PEG_RX8+	D78	PEG_TX8+
C79	PEG_RX8-	D79	PEG_TX8-
C80	GND (FIXED)	D80	GND (FIXED)
C81	PEG_RX9+	D81	PEG_TX9+
C82	PEG_RX9-	D82	PEG_TX9-
C83	GND	D83	GND
C84	GND	D84	GND
C85	PEG_RX10+	D85	PEG_TX10+
C86	PEG_RX10-	D86	PEG_TX10-
C87	GND	D87	GND
C88	PEG_RX11+	D88	PEG_TX11+
C89	PEG_RX11-	D89	PEG_TX11-
C90	GND (FIXED)	D90	GND (FIXED)
C91	PEG_RX12+	D91	PEG_TX12+
C92	PEG_RX12-	D92	PEG_TX12-
C93	GND	D93	GND
C94	PEG_RX13+	D94	PEG_TX13+
C95	PEG_RX13-	D95	PEG_TX13-
C96	GND	D96	GND
C97	GND	D97	GND
C98	PEG_RX14+	D98	PEG_TX14+
C99	PEG_RX14-	D99	PEG_TX14-
C100	GND (FIXED)	D100	GND (FIXED)
C101	PEG_RX15+	D101	PEG_TX15+
C102	PEG_RX15-	D102	PEG_TX15-
C103	GND	D103	GND
C104	VCC_12V	D104	VCC_12V
C105	VCC_12V	D105	VCC_12V
C106	VCC_12V	D106	VCC_12V
C107	VCC_12V	D107	VCC_12V
C108	VCC_12V	D108	VCC_12V
C109	VCC_12V	D109	VCC_12V
C110	GND (FIXED)	D110	GND (FIXED)

*Note:

1. A50 could be an optional pin reserved for ESPI_CS1#. Please contact FAE for details.
2. A71 could be an optional pin reserved for eDP_TX2+. Please contact FAE for details.

3. A72 could be an optional pin reserved for eDP_TX2-. Please contact FAE for details.
4. A73 could be an optional pin reserved for eDP_TX1+. Please contact FAE for details.
5. A74 could be an optional pin reserved for eDP_TX1-. Please contact FAE for details.
6. A75 could be an optional pin reserved for eDP_TX0+. Please contact FAE for details.
7. A76 could be an optional pin reserved for eDP_TX0-. Please contact FAE for details.
8. A77 could be an optional pin reserved for eDP_VDD_EN. Please contact FAE for details.
9. A81 could be an optional pin reserved for eDP_TX3+. Please contact FAE for details.
10. A82 could be an optional pin reserved for eDP_TX3-. Please contact FAE for details.
11. A83 could be an optional pin reserved for eDP_AUX+. Please contact FAE for details.
12. A84 could be an optional pin reserved for eDP_AUX-. Please contact FAE for details.
13. A101 could be an optional pin reserved for CAN_TX. Please contact FAE for details.
14. A102 could be an optional pin reserved for CAN_RX. Please contact FAE for details.
15. B3 could be an optional pin reserved for ESPI_CS0#. Please contact FAE for details.
16. B4 could be an optional pin reserved for ESPI_IO_0. Please contact FAE for details.
17. B5 could be an optional pin reserved for ESPI_ IO_1. Please contact FAE for details.
18. B6 could be an optional pin reserved for ESPI_ IO_2. Please contact FAE for details.
19. B7 could be an optional pin reserved for ESPI_ IO_3. Please contact FAE for details.
20. B10 could be an optional pin reserved for ESPI_CK. Please contact FAE for details.
21. B79 could be an optional pin reserved for eDP_BKLT_EN. Please contact FAE for details.
22. B83 could be an optional pin reserved for eDP_BKLT_CTRL. Please contact FAE for details.
23. C15 could be an optional pin reserved for USB4_1_LSTX. Please contact FAE for details.
24. C16 could be an optional pin reserved for USB4_1_LSRX. Please contact FAE for details.
25. C17 could be an optional pin reserved for USB4_RT_ENA. Please contact FAE for details.
26. C25 could be an optional pin reserved for SML0_CLK. Please contact FAE for details.
27. C26 could be an optional pin reserved for SML0_DAT. Please contact FAE for details.
28. C27 could be an optional pin reserved for SML1_CLK. Please contact FAE for details.

29. C28 could be an optional pin reserved for SML1_DAT. Please contact FAE for details.
30. C29 could be an optional pin reserved for USB4_PD_I2C_CLK. Please contact FAE for details.
31. C30 could be an optional pin reserved for USB4_PD_I2C_DAT. Please contact FAE for details.
32. C32 could be an optional pin reserved for USB4_2_AUX+. Please contact FAE for details.
33. C33 could be an optional pin reserved for USB4_2_AUX-. Please contact FAE for details.
34. C35 could be an optional pin reserved for USB4_2_LSTX. Please contact FAE for details.
35. D15 could be an optional pin reserved for USB4_1_AUX+. Please contact FAE for details.
36. D16 could be an optional pin reserved for USB4_1_AUX-. Please contact FAE for details.
37. D17 could be an optional pin reserved for USB4_PD_I2C_ALERT#. Please contact FAE for details.
38. D18 could be an optional pin reserved for PMCALERT#. Please contact FAE for details.
39. D26 could be an optional pin reserved for USB4_1_SSTX0+. Please contact FAE for details.
40. D27 could be an optional pin reserved for USB4_1_SSTX0-. Please contact FAE for details.
41. D29 could be an optional pin reserved for USB4_1_SSRX0+. Please contact FAE for details.
42. D30 could be an optional pin reserved for USB4_1_SSRX0-. Please contact FAE for details.
43. D32 could be an optional pin reserved for USB4_1_SSTX1+. Please contact FAE for details.
44. D33 could be an optional pin reserved for USB4_1_SSTX1-. Please contact FAE for details.
45. D36 could be an optional pin reserved for USB4_1_SSRX1+. Please contact FAE for details.
46. D37 could be an optional pin reserved for USB4_1_SSRX1-. Please contact FAE for details.
47. D39 could be an optional pin reserved for USB4_2_SSTX0+. Please contact FAE for details.
48. D40 could be an optional pin reserved for USB4_2_SSTX0-. Please contact FAE for details.
49. D42 could be an optional pin reserved for USB4_2_SSRX0+. Please contact FAE for details.
50. D43 could be an optional pin reserved for USB4_2_SSRX0-. Please contact FAE for details.
51. D46 could be an optional pin reserved for USB4_2_SSTX1+. Please contact FAE for details.
52. D47 could be an optional pin reserved for USB4_2_SSTX1-. Please contact FAE for details.
53. D49 could be an optional pin reserved for USB4_2_SSRX1+. Please contact FAE for details.
54. D50 could be an optional pin reserved for USB4_2_SSRX1-. Please contact FAE for details.

Appendix B

Watchdog Timer

This appendix details information about the watchdog timer programming on the SOM-5885 CPU System on Module.

Sections include:

- Watchdog Timer Programming

B.1 Programming the Watchdog Timer

Table B.1: Programming the Watchdog Timer

Trigger Event	Note
IRQ	(BIOS setting default disable)**
NMI	N/A
SCI	Support
Power Off	Support
H/W Restart	Support
WDT Pin Activate	Support

** WDT new driver support automatically selects an available IRQ number from the BIOS, and then sets it to EC. Only Win10 supports this.

In other OS, it will still use an IRQ number from the BIOS settings as usual. For details, please refer to the iManager & Software API User Manual.

Appendix C

Programming GPIO

This Appendix illustrates the General Purpose Input and Output pin settings.

Sections include:

- GPIO Register

C.1 GPIO Register

Table C.1: GPIO Register

GPIO Byte Mapping	H/W Pin Name
BIT0	GPI0
BIT1	GPI1
BIT2	GPI2
BIT3	GPI3
BIT4	GPO0
BIT5	GPO1
BIT6	GPO2
BIT7	GPO4

For details, please refer to the iManager and Software API User Manual.

Appendix D

System Assignments

This appendix gives you information about the system resource allocation on the SOM-5885 CPU System on Module.

Sections include:

- System I/O Ports
- DMA Channel Assignments
- Interrupt Assignments
- 1st MB Memory Map

D.1 System I/O Ports

Table D.1: System I/O Ports

Addr. Range (Hex)	Device
0x0000EFA0-0x0000EFBF	Intel® SMBus - 7E22
0x00000299-0x0000029A	Motherboard resources
0x000002C0-0x000002DF	Motherboard resources
0x000002A0-0x000002BF	Motherboard resources
0x000002A0-0x000002BF	Motherboard resources
0x00000290-0x0000029F	Motherboard resources
0x0000029E-0x000002AD	Motherboard resources
0x00000060-0x0000006F	Motherboard resources
0x00000200-0x0000027F	Motherboard resources
0x00000300-0x0000037F	Motherboard resources
0x00000280-0x0000028F	Motherboard resources
0x00000280-0x0000028F	Motherboard resources
0x000002F0-0x000002F7	Motherboard resources
0x0000002E-0x0000002F	Motherboard resources
0x0000004E-0x0000004F	Motherboard resources
0x00000061-0x00000061	Motherboard resources
0x00000063-0x00000063	Motherboard resources
0x00000065-0x00000065	Motherboard resources
0x00000067-0x00000067	Motherboard resources
0x00000070-0x00000070	Motherboard resources
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
0x000000B2-0x000000B3	Motherboard resources
0x00000680-0x0000069F	Motherboard resources
0x0000164E-0x0000164F	Motherboard resources
0x00001854-0x00001857	Motherboard resources
0x00000062-0x00000062	Microsoft ACPI-Compliant Embedded Controller
0x00000066-0x00000066	Microsoft ACPI-Compliant Embedded Controller
0x000003F8-0x000003FF	Communications Port (COM1)
0x000002F8-0x000002FF	Communications Port (COM2)
0x00000020-0x00000021	Programmable interrupt controller
0x00000024-0x00000025	Programmable interrupt controller
0x00000028-0x00000029	Programmable interrupt controller
0x0000002C-0x0000002D	Programmable interrupt controller
0x00000030-0x00000031	Programmable interrupt controller
0x00000034-0x00000035	Programmable interrupt controller
0x00000038-0x00000039	Programmable interrupt controller
0x0000003C-0x0000003D	Programmable interrupt controller
0x000000A0-0x000000A1	Programmable interrupt controller
0x000000A4-0x000000A5	Programmable interrupt controller
0x000000A8-0x000000A9	Programmable interrupt controller
0x000000AC-0x000000AD	Programmable interrupt controller
0x000000B0-0x000000B1	Programmable interrupt controller

Table D.1: System I/O Ports	
0x000000B4-0x000000B5	Programmable interrupt controller
0x000000B8-0x000000B9	Programmable interrupt controller
0x000000BC-0x000000BD	Programmable interrupt controller
0x000004D0-0x000004D1	Programmable interrupt controller
0x00003050-0x00003057	Standard SATA AHCI Controller

D.2 Interrupt Assignments

Table D.2: Interrupt Assignments	
Addr. Range (Hex)	**Device**
IRQ 4294967294	PCI Express Root Port
IRQ 4294967271 - IRQ 4294967287	Intel® Ethernet Controller I226-LMvP
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 4294967292	Standard SATA AHCI Controller
IRQ 6	Motherboard resources
IRQ 4294967288	Intel® USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 34	Intel® Serial IO I2C Host Controller - 7E7A
IRQ 111	Trusted Platform Module 2.0
IRQ55 - IRQ 204	Microsoft ACPI-Compliant System
IRQ 256 - IRQ 511	Microsoft ACPI-Compliant System
IRQ 4294967290	Intel® Arc(TM) Graphics
IRQ 4294967290	Intel® Arc(TM) Graphics
IRQ 19	Intel® Active Management Technology - SOL (COM3)
IRQ 4294967289	Intel® USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967291	Intel® Management Engine Interface #1
IRQ 0	System timer
IRQ 32	Intel® Serial IO I2C Host Controller - 7E78
IRQ 14	Intel® Serial IO GPIO Host Controller - INTC1083
IRQ 4294967293	PCI Express Root Port

D.3 1st MB Memory Map

Table D.3: 1st MB Memory Map

Addr. Range (Hex)	Device
0x11268000-0x112680FF	Intel® SMBus - 7E22
0xFEDC0000-0xFEDC7FFF	Motherboard resources
0x0000-0x0FFF	Motherboard resources
0x0000-0x0FFF	Motherboard resources
0xC0000000-0xCFFFFFFF	Motherboard resources
0xFED20000-0xFED7FFFF	Motherboard resources
0xFC800000-0xFC81FFFF	Motherboard resources
0xFED45000-0xFED8FFFF	Motherboard resources
0xFEE00000-0xFEEFFFFF	Motherboard resources
0xBFFC0000-0xBFFFFFFF	Intel® Platform Monitoring Technology (PMT) Driver
0x80000000-0x802FFFFF	PCI Express Root Port
0x80000000-0x802FFFFF	PCI Express Root Complex
0x80100000-0x801FFFFF	Intel® Ethernet Controller I226-LMvP
0x80200000-0x80203FFF	Intel® Ethernet Controller I226-LMvP
0xFED00000-0xFED003FF	High precision event timer
0x80400000-0x80401FFF	Standard SATA AHCI Controller
0x80403000-0x804030FF	Standard SATA AHCI Controller
0x80402000-0x804027FF	Standard SATA AHCI Controller
0x11240000-0x1124FFFF	Intel® USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
0xA0000-0xBFFFF	PCI Express Root Complex
0x1126A000-0x1126AFFF	Intel® Serial IO I2C Host Controller - 7E7A
0x10000000-0x10FFFFFF	Intel® Arc(TM) Graphics
0x0000-0xFFFFFFF	Intel® Arc(TM) Graphics
0xFED40000-0xFED44FFF	Trusted Platform Module 2.0
0xFE010000-0xFE010FFF	Intel® SPI - 7E23
0x80300000-0x8037FFFF	PCI Express Upstream Switch Port
0x80300000-0x8037FFFF	PCI Express Root Port
0xBFFFF000-0xBFFFFFFF	Intel® Active Management Technology - SOL (COM3)
0x11250000-0x1125FFFF	Intel® USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
0x11269000-0x11269FFF	Intel® Management Engine Interface #1
0x1126B000-0x1126BFFF	Intel® Serial IO I2C Host Controller - 7E78
0xE0D10000-0xE0D1FFFF	Intel® Serial IO GPIO Host Controller - INTC1083
0xE0D20000-0xE0D2FFFF	Intel® Serial IO GPIO Host Controller - INTC1083
0xE0D30000-0xE0D3FFFF	Intel® Serial IO GPIO Host Controller - INTC1083
0xE0D40000-0xE0D4FFFF	Intel® Serial IO GPIO Host Controller - INTC1083
0xE0D50000-0xE0D5FFFF	Intel® Serial IO GPIO Host Controller - INTC1083
0xBFFBC000-0xBFFBFFFF	Intel® Smart Sound Technology BUS
0xBFC00000-0xBFDFFFFF	Intel® Smart Sound Technology BUS

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.

No part of this publication may be reproduced in any form or by any means, such as electronically, by photocopying, recording, or otherwise, without prior written permission from the publisher.

All brand and product names are trademarks or registered trademarks of their respective companies.

© Advantech Co., Ltd. 2026