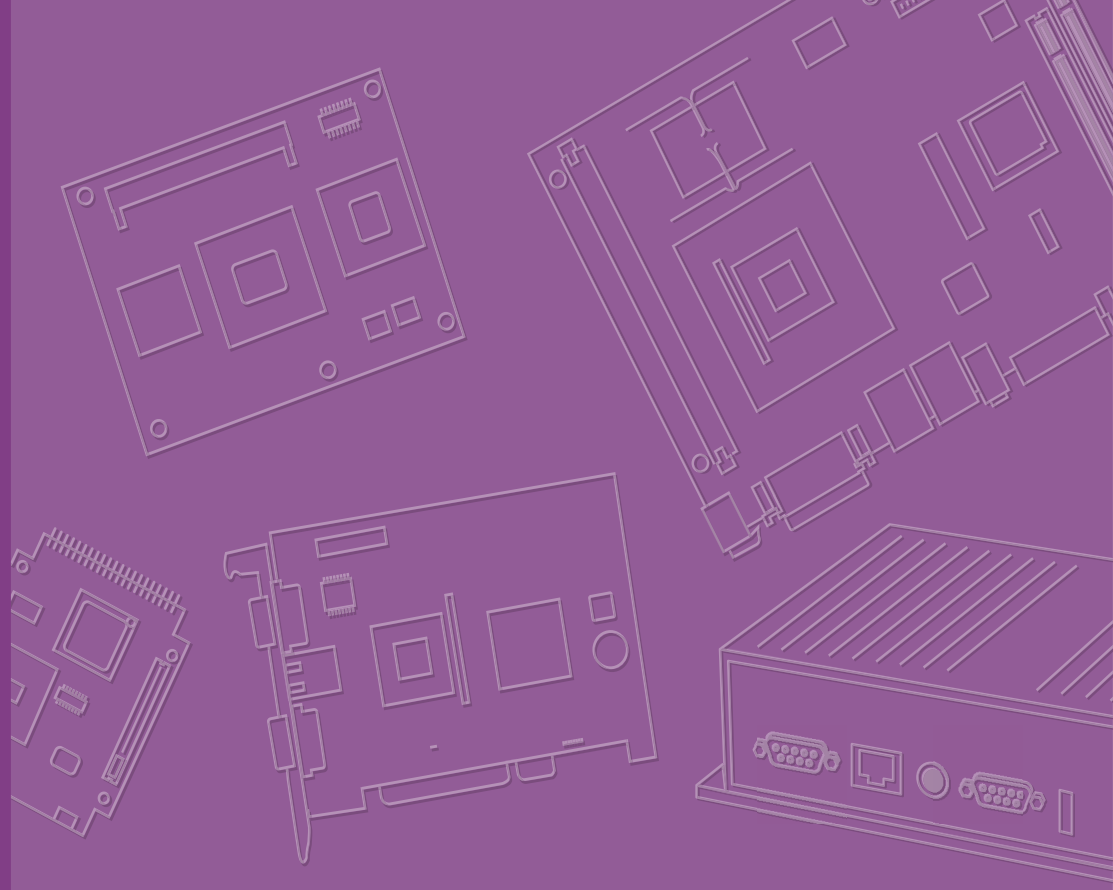




SOM-5886

**Intel® Core Ultra Processors
(Panther Lake)
COM Express Basic Type-6
Module**

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2026 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 the 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.

Declaration of Conformity

CE

This product has passed the CE test for environmental specifications. Test conditions for passing include the equipment being operated within an industrial enclosure. In order to protect the product from damage caused by electrostatic discharge (ESD) or 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 the FM certification. According to the National Fire Protection Association, work sites are classified into different classes, divisions and groups, based on hazard considerations. This equipment is compliant with the specifications of 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 if not observed can cause personal injury!



Caution! Cautions are included to help you avoid damaging hardware or losing data. e.g.:



There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.

Note! Notes provide optional additional 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.

CPU	Cores (P+E+LPE)	Base Freq. (GHz)	P-Core Max Turbo Freq. (GHz)	LLC	NPU PTOPS	GPU Xe Cores	GPU Max Freq. (GHz) / PTOPS	vPro	FuSa	PCIe Lanes	Memory	Default TDP	cTDP	Operating Temp.
Intel Core Ultra X9 388H	16C (4P+8E+4LPE)	2.1GHz	5.0GHz	18MB	50	12Xe	2.5GHz /122	Yes	No	12	DDR5 7200	25W	15W-65W	0~60°C
Intel Core Ultra 9 386H	16C (4P+8E+4LPE)	2.1GHz	4.8GHz	18MB	50	4Xe	2.5GHz /40	Yes	No	20	DDR5 7200	25W	15W-65W	0~60°C
Intel Core Ultra X7 358H	16C (4P+4E+4LPE)	1.9GHz	4.7GHz	18MB	50	12Xe	2.5GHz /122	No	No	12	DDR5 7200	25W	15W-65W	0~60°C
Intel Core Ultra 7 356H	16C (4P+8E+4LPE)	1.9GHz	4.6GHz	18MB	50	4Xe	2.45GHz /40	No	No	20	DDR5 7200	25W	15W-65W	0~60°C
Intel Core Ultra 5 325	8C (4P+0E+4LPE)	2.1GHz	4.4GHz	12MB	47	4Xe	2.45GHz /40	No	No	12	DDR5 6400	25W	12W-55W	0~60°C
Intel Core Ultra X7 368HR	16C (4P+8E+4LPE)	TBD	TBD	18MB	50	12Xe	TBD	Yes	Yes	12	DDR5 7200	25W	15W-65W	0~60°C
Intel Core Ultra 5 336HRE	12C (4P+4E+4LPE)	TBD	TBD	18MB	47	4Xe	TBD	Yes	Yes	20	DDR5 7200	25W	15W-65W	-40~85°C

Packing List

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

Part No.	Description	Quantity
-	SOM-5886 COM module	1
1970006397T001	Heatspreader for the SOM-5886	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
1970006409T001	QFCS 125 x 95 x 26.2 mm

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 your PC chassis before you work on it. Don't touch any components on the CPU card or other cards while the PC is on.
- Disconnect power before making any configuration changes. The sudden rush of power as you connect a jumper or install 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 does not exceed 70 dB (A).

DISCLAIMER: These instructions are provided according to IEC 704-1 standards. 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.....	2
1.2	Functional Block Diagram	3
	Figure 1.1 SOM-5886 Block Diagram	3
1.3	Product Specifications.....	3
1.3.1	Compliance	3
1.3.2	Feature List.....	4
	Table 1.2: Feature List.....	4
1.3.3	Processor System.....	5
	Table 1.3: Processor System	5
1.3.4	Memory	5
1.3.5	Graphics/Audio	5
	Table 1.4: Table 1.4: Graphics/Audio	5
1.3.6	Expansion Interfaces	5
	Table 1.5: PEG	6
	Table 1.6: PCI Express.....	6
1.3.7	LPC	6
1.3.8	Serial Bus.....	6
1.3.9	I/O	6
	Table 1.7: USB 2.0	7
	Table 1.8: BIOS	7
1.3.10	Power Management.....	8
1.3.11	Environmental Specifications	9
1.3.12	MTBF	9
1.3.13	OS Support	9
1.3.14	Advantech iManager	9
1.3.15	Power Consumption.....	10
	Table 1.9: Power Consumption Table (Watts).....	10
1.3.16	Performance	10
1.3.17	Pin Descriptions	10

Chapter 2 Mechanical Information 11

2.1	Board Information.....	12
	Figure 2.1 Board Chips ID – Front.....	12
	Figure 2.2 Board Chips ID – Rear	12
2.2	Mechanical Diagram	13
	Figure 2.3 Board Mechanical Diagram - Front.....	13
	Figure 2.4 Board Mechanical Diagram - Rear	13
	Figure 2.5 Board Mechanical Diagram – Side	14
2.3	Assembly Diagram	15
	Figure 2.6 Assembly Diagram	15
2.4	Assembly Diagram	16
	Figure 2.7 CPU Height and Tolerance (H12Xe)	16
	Figure 2.8 CPU Height and Tolerance (H404).....	16
	Figure 2.9 CPU Height and Tolerance (H484).....	16

Chapter 3 AMI BIOS 17

3.1	Introduction	18
	Figure 3.1 Setup Program Initial Screen.....	18
3.2	Entering Setup	19

3.3	Main Setup	19
	Figure 3.2 Main Setup Screen	19
3.4	Advanced BIOS Features Setup	20
	Figure 3.3 Advanced Features Setup Screen	20
3.4.1	RC ACPI Settings	21
	Figure 3.4 RC ACPI Settings	21
3.4.2	CPU Configuration	23
	Figure 3.5 CPU Configuration	23
	Figure 3.6 CPU Configuration	23
	Figure 3.7 Efficient-core Information	25
	Figure 3.8 Performance-core	25
3.4.3	Power & Performance	26
	Figure 3.9 Power & Performance	26
	Figure 3.10 CPU - Power Management Control	27
	Figure 3.11 Current Turbo Settings	28
	Figure 3.12 Current Turbo Ratio Limit Settings	29
	Figure 3.13 Config Base Power Configurations	30
3.4.4	System Agent (SA) Configuration	31
	Figure 3.14 System Agent (SA) Configuration	31
	Figure 3.15 Memory Configurations	32
	Figure 3.16 Graphics Configurations	33
	Figure 3.17 Display Configurations	34
	Figure 3.18 GT Configurations	35
	Figure 3.19 Media Configurations	36
	Figure 3.20 VMD Setup Menu	37
	Figure 3.21 VT-d Setup Menu	37
3.4.5	PCIe Configuration	38
	Figure 3.22 PCIe Configuration	38
	Figure 3.23 PCI Express Root Port PXPd	39
	Figure 3.24 PCIe Clocks	41
3.4.6	PCH-I/O Configuration	42
	Figure 3.25 PCH-I/O Configuration	42
	Figure 3.26 USB Configuration	44
	Figure 3.27 Security Configuration	45
	Figure 3.28 HD Audio Configuration Settings	46
3.4.7	PCH-FW Configuration	47
	Figure 3.29 PCH-FW Configuration	47
3.4.8	ACPI D3Cold Settings	48
	Figure 3.30 ACPI D3Cold Settings	48
	Figure 3.31 Intel® Ultrabook Event Support	49
3.4.9	AMT Configuration	50
	Figure 3.32 AMT Configuration	50
	Figure 3.33 ASF Configuration	51
3.4.10	Trusted Computing	52
	Figure 3.34 Trusted Computing	52
3.4.11	JMicron AHCI Controller	53
	Figure 3.35 JMicron AHCI Controller	53
3.4.12	ACPI Settings	53
	Figure 3.36 ACPI Settings	53
3.4.13	Embedded Controller	54
	Figure 3.37 Embedded Controller	54
	Figure 3.38 Serial Port 1 Configuration	55
	Figure 3.39 Serial Port 2 Configuration	56
	Figure 3.40 ACPI Report Method Configuration	57
3.4.14	Serial Port Console Redirection	58
	Figure 3.41 Serial Port Console Redirection	58
	Figure 3.42 Console Redirection Settings	59
3.4.15	USB Configuration	59
	Figure 3.43 USB Configuration	59
3.4.16	Network Stack Configuration	60

	Figure 3.44 Network Stack Configuration	60
3.4.17	NVMe Configuration.....	61
	Figure 3.45 NVMe Configuration	61
3.4.18	Option ROM Dispatch Policy	62
	Figure 3.46 Option ROM Dispatch Policy	62
3.5	Security Chipset.....	63
	Figure 3.47 Security Chipset	63
3.5.1	Secure Boot.....	64
	Figure 3.48 Secure Boot.....	64
3.6	Boot.....	65
	Figure 3.49 Boot Configuration.....	65
3.7	Save & Exit.....	66
	Figure 3.50 Save & Exit.....	66
3.8	MEBx.....	67
	Figure 3.51 MEBx	67

Chapter 4 S/W Introduction & Installation 69

4.1	S/W Introduction.....	70
4.2	Driver Installation	70
	4.2.1 Windows Driver Setup	70
	4.2.2 Other OS.....	70
4.3	Advantech iManager	71

Appendix A Pin Assignment 73

A.1	SOM-5886 Pin Assignments	74
	Table A.1: SOM-5886 Pin Assignments	74

Appendix B Watchdog Timer 79

B.1	Programming the Watchdog Timer	80
	Table B.1: Programming the Watchdog Timer.....	80

Appendix C Programming GPIO 81

C.1	GPIO Register.....	82
	Table C.1: GPIO Register	82

Appendix D System Assignments 83

D.1	System I/O Ports	84
	Table D.1: System I/O Port	84
D.2	Interrupt Assignments	85
	Table D.2: Interrupt Assignments.....	85
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-5886 CPU Computer on Module.

Sections include:

- Introduction
- Functional Block Diagram
- Product Specifications

1.1 Introduction

The Advantech SOM-5886 is a COM Express Type-6 Basic Module with a Intel® Core Ultra Processors (Series 3). It delivers octa-core computing performance with 45W TDP, while providing IXe LPG graphics, and Advantech's Edge AI Suite software toolkit.

The SOM-5886 supports up to 128GB DDR5 6400 RAM, offering a 2x increase in computing performance and 4X 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/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-5886 comes with a heat spreader and QFCS solution.

Table 1.1: Acronyms

Term	Definition
AC'97	Audio CODEC (Coder-Decoder)
ACPI	Advanced Configuration Power Interface – standard to implement power saving modes in PC-AT systems
BIOS	Basic Input Output System – firmware in 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 function ■ System information ■ Watchdog timer ■ I2C 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
I2C	Inter Integrated Circuit – 2 wire (clock and data) signaling scheme allowing communication between integrated circuit, 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 computer in 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, chip to enhance the security features of a computer system

Table 1.1: Acronyms

UEFI	Unified Extensible Firmware Interface
WDT	Watchdog Timer

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.

1.2 Functional Block Diagram

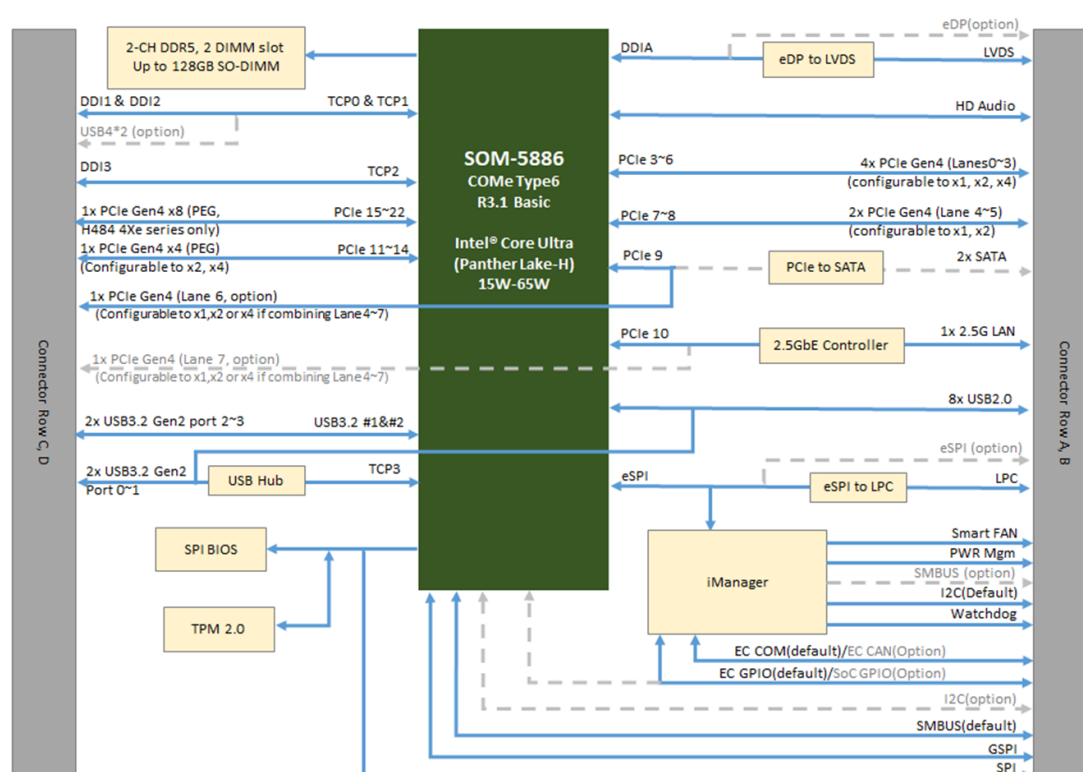


Figure 1.1 SOM-5886 Block Diagram

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	Feature	Type 6 Define		SOM-5886
			Min.	Max.	
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	C-D	PCI Express Lanes 16 - 31	0	16	12
Expansion	A-B	LPC Bus or eSPI	1	1	1
IO	A-B	NBASE-T LAN Port 0	1	1	1
IO	A-B	SATA Ports	1	4	2
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	C-D	USB 3.0 Ports	0	4	4
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)	TDP(W)
Intel Core Ultra X9 388H	2.1GHz	2.5GHz/122	16C (4P+8E+4LPE)	18	15-65W
Intel Core Ultra 9 386H	2.1GHz	2.5GHz/40	16C (4P+8E+4LPE)	18	15-65W
Intel Core Ultra X7 358H	1.9GHz	2.5GHz/122	16C (4P+4E+4LPE)	18	15-65W
Intel Core Ultra 7 356H	1.9GHz	2.45GHz/40	16C (4P+8E+4LPE)	18	15-65W
Intel Core Ultra 5 325	2.1GHz	2.45GHz/40	8C (4P+0E+4LPE)	12	12-55W

1.3.4 Memory

There are a total of 2 memory sockets on the SOM-5886. The topside has 2 by default. This solution supports max 128GB capacity (non-ECC memory modules with all SKUs.) with 262-pin SODIMM sockets (dual-channel).

1.3.5 Graphics/Audio

Graphics Core: Intel® Xe3 supports DX12.2, OGL4.6, Vulkan 1.2, and AVC/HEVC/VP9/SCC/AV1 HW decode/encode acceleration.

Table 1.4: Table 1.4: Graphics/Audio

CPU	Graphics Core	Base Freq.	Max Freq.
Intel Core Ultra X9 388H	Intel® Xe3	2.1GHz	2.5GHz/122
Intel Core Ultra 9 386H	Intel® Xe3	2.1GHz	2.5GHz/40
Intel Core Ultra X7 358H	Intel® Xe3	1.9GHz	2.5GHz/122
Intel Core Ultra 7 356H	Intel® Xe3	1.9GHz	2.45GHz/40
Intel Core Ultra 5 325	Intel® Xe3	2.1GHz	2.45GHz/40

- 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 12 lanes by default, compliant with PCIe Gen4 (16.0 GT/s) specifications, configurable to PEG x8, x4, x2.

*Note: Only H484 series has PEGx8.

Table 1.5: PEG

Type 6		Row C, D											
		P8	P9	P10	P11	P0	P1	P2	P3	P4	P5	P6	P7
Default	Config.	x4				x8							
option		x4				x8							

1.3.6.2 PC Express

PCI Express: Supports 8 lanes by default, PCIe x1 compliant to 6 x PCIe x1 Gen4 (x1, x2, x4) (16.0 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		Row A				Row B			
		P0	P1	P2	P3	P4	P5	P6	P7
Default	Config	x1	x1	x1	x1	x1	x1	Colay SATA	Colay LAN
Option		x4				x4			

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

Support SMBus 2.0 specification.

1.3.8.2 I2C Bus

Supports I2C bus 7-bit address modes. Support standard mode up to 100 Kb/s, 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 ports 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. Supports AHCI 1.3.1 mode (does not support IDE mode).

1.3.9.3 USB 4.0 /USB 3.2 / USB 2.0

SOM-5886 supports 2 x USB 4.0 (option), 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#	USB OCO#				USB OC3#			

1.3.9.5 SPI Bus

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

1.3.9.6 GPIO

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

1.3.9.7 Watchdog

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 Port

2 x 2-wire serial port (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

Support 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

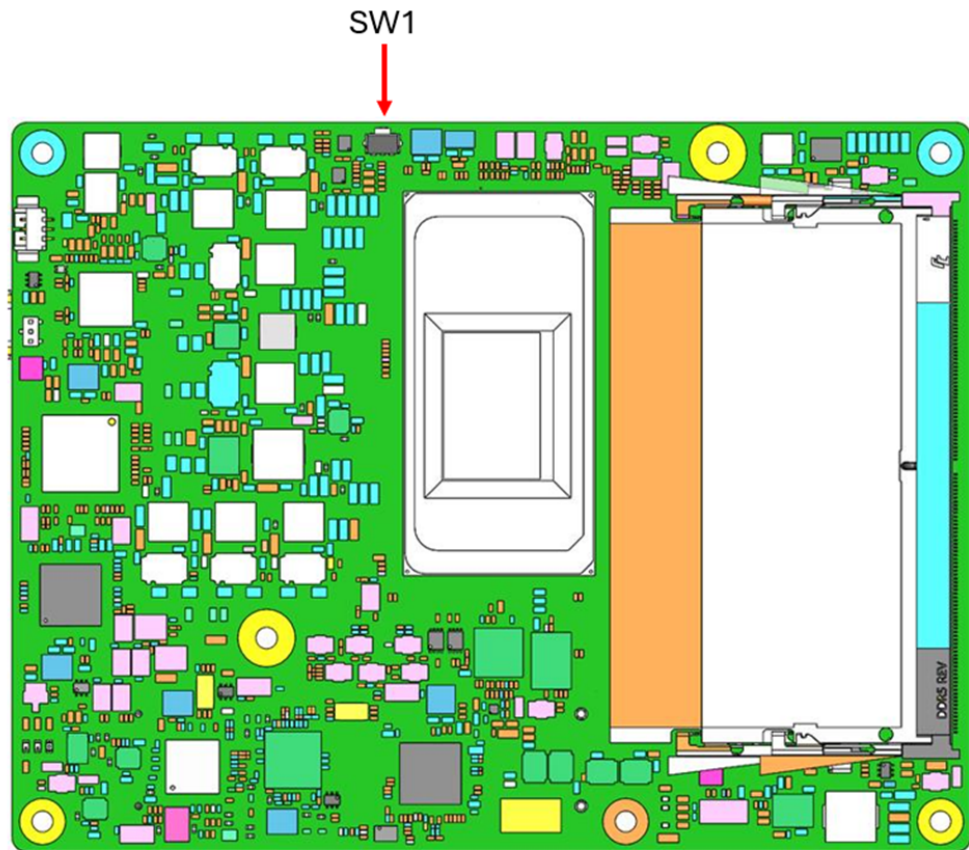
The BIOS chip is on module by default. Users can place BIOS chip on the carrier board with appropriate design and jumper setting in BIOS_DIS#[1:0].

Table 1.8: BIOS

BIOS_DIS#0	BIOS_DIS#1	Boot-Up Destination/Funtion
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. Put Button on SW1.
3. Turn on power supply.
4. The system will boot up a few times.
5. The BIOS will load default setting successfully.

1.3.10 Power Management

1.3.10.1 Power Supply

Supports both ATX and AT power modes. VSB is for suspended power and is optional if not required by standby (suspend-to-RAM) support. RTC battery is optional if date/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 allowing Carrier- based FPGAs or other configurable devices time to be programmed.

1.3.10.3 Power Sequence

According to PICMG COM Express COM.0 R 3.1 specification

1.3.10.4 Wake Event

- Various wake event support allows users to apply different scenarios.
- Wake-on-LAN(WOL): Wake to S0 from S3/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 Environmental Specifications

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 non-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 EN55032 Class B and FCC Certifications: validate with standard development boards in Advantech chassis

1.3.12 MTBF

Please refer Advantech SOM-5886 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 the 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

Supports APIs for GPIO, smart fan control, multi-stage watchdog timer, temperature sensor, and hardware monitoring. 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 (uA)
SOM-5886C9H-U1A1	41.68W	42.30W	8.58W	0.73W	0.74W	2.86 uA

Hardware Configuration:

1. MB: SOM-5886C9H-U1A1
2. DRAM: 128GB DDR5 6400MHz x 2 pcs
3. Carrier board: SOM-DB5830-00A3

Test Conditions:

1. Test temperature: room temperature (about 25 °C)
2. Test voltage: rated voltage DC +12V
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, 2&3D Graphics, and Disk with 100%)
 - Idle mode: DUT power management off and not running any program.
4. OS: Windows 11 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 them 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 nearest Advantech branch office or call for getting the design documents and further advance supports.

Chapter 2

Mechanical Information

This chapter details mechanical information on the SOM-5886 CPU Computer on Module.

Sections include:

- Board Information
- Mechanical Diagrams
- Assembly Diagram

2.1 Board Information

The figures below demonstrate the main chips on the SOM-5886 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.

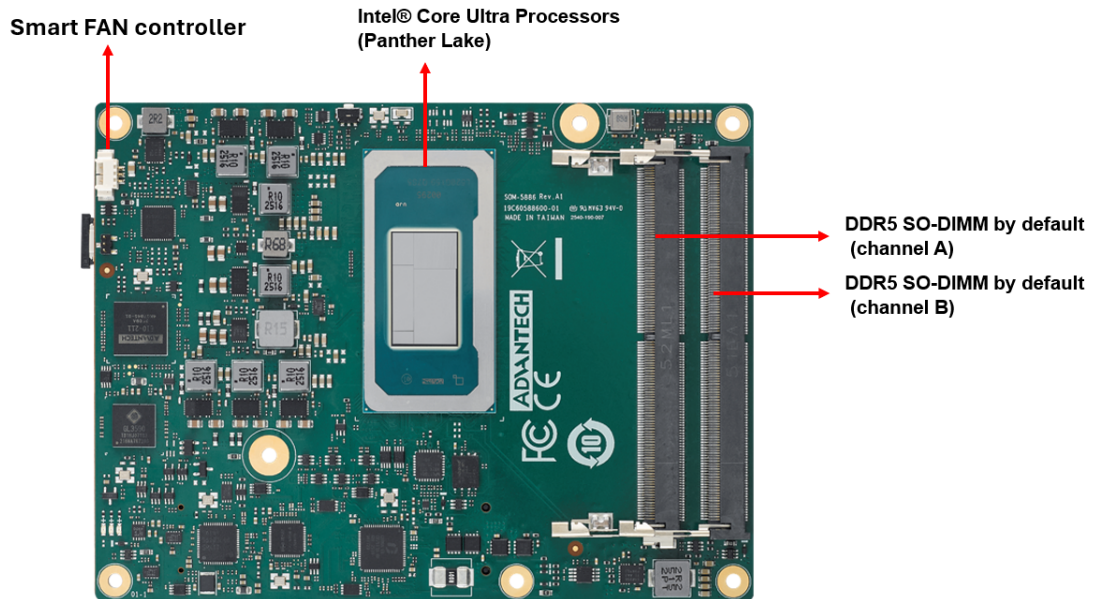


Figure 2.1 Board Chips ID – Front

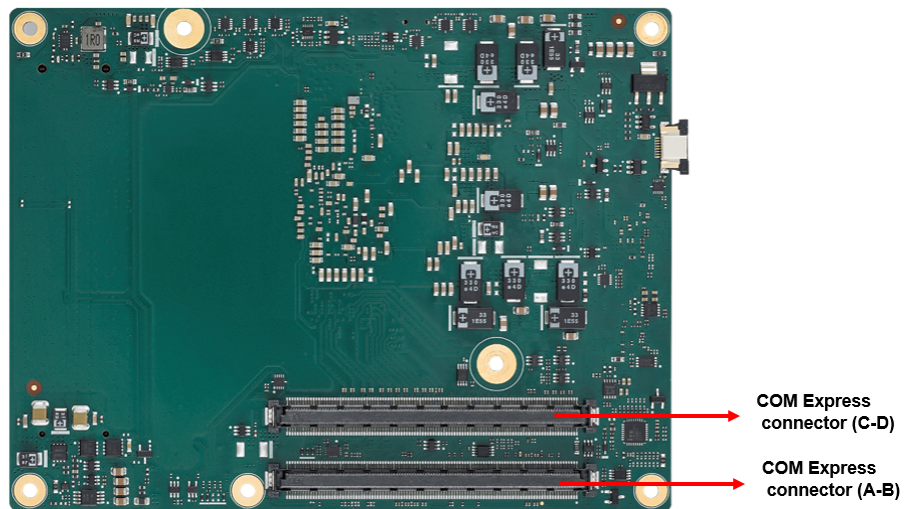


Figure 2.2 Board Chips ID – Rear

2.2 Mechanical Diagram

For more details about 2/3D models, please find on Advantech COM support service website <http://com.advantech.com>.

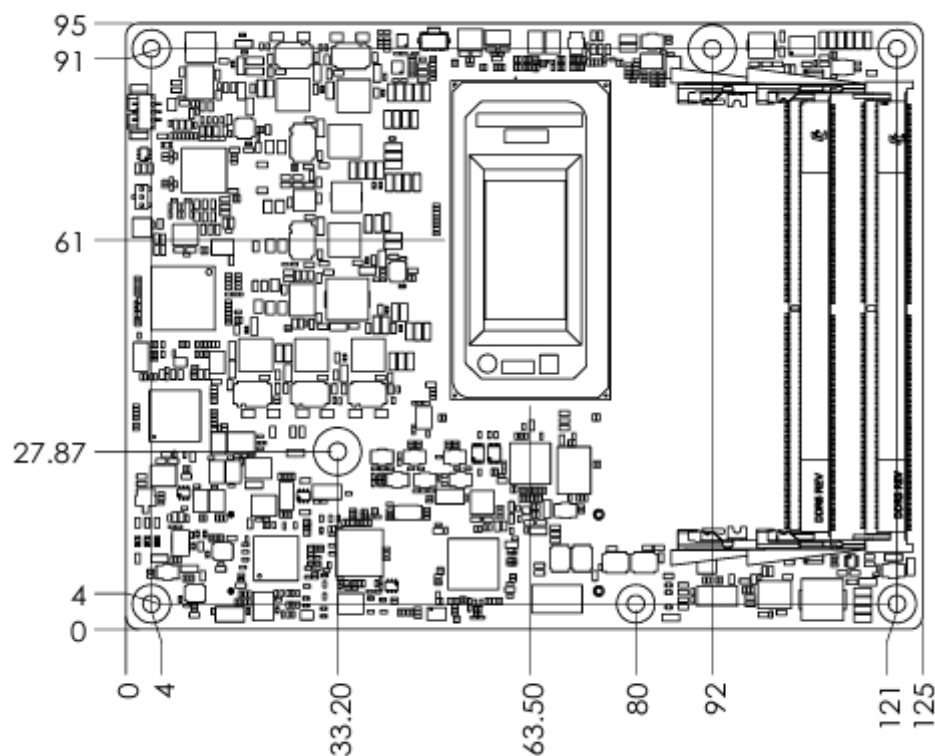


Figure 2.3 Board Mechanical Diagram - Front

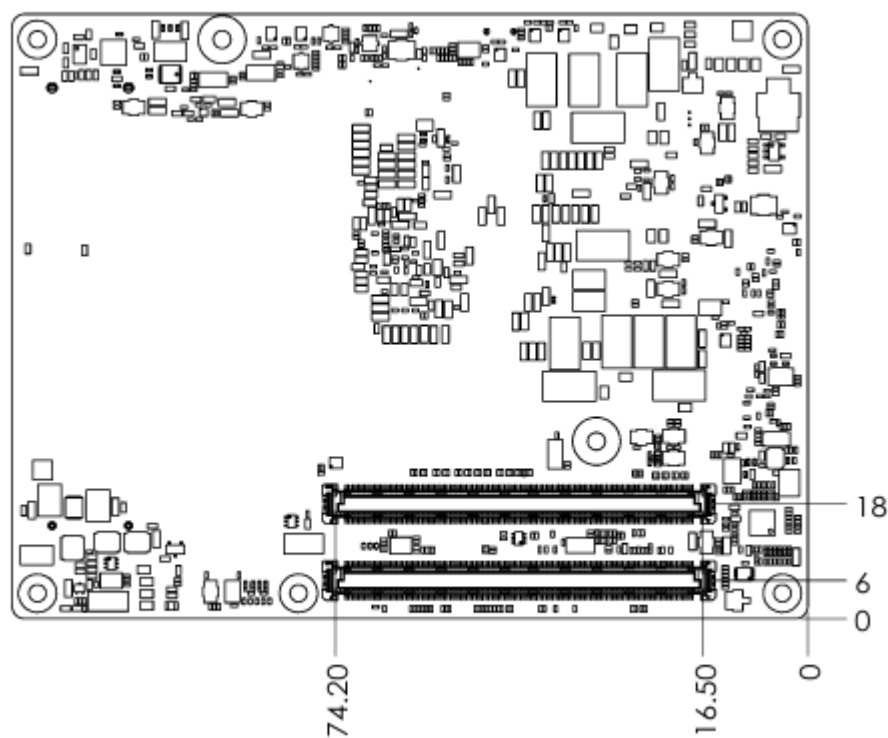


Figure 2.4 Board Mechanical Diagram - Rear

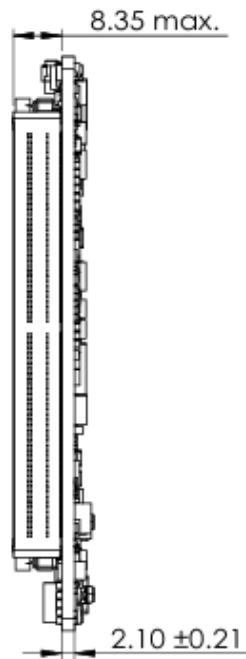


Figure 2.5 Board Mechanical Diagram – Side

2.3 Assembly Diagram

These figures demonstrate the assembly order from the thermal module, the COM module, and to the carrier board.

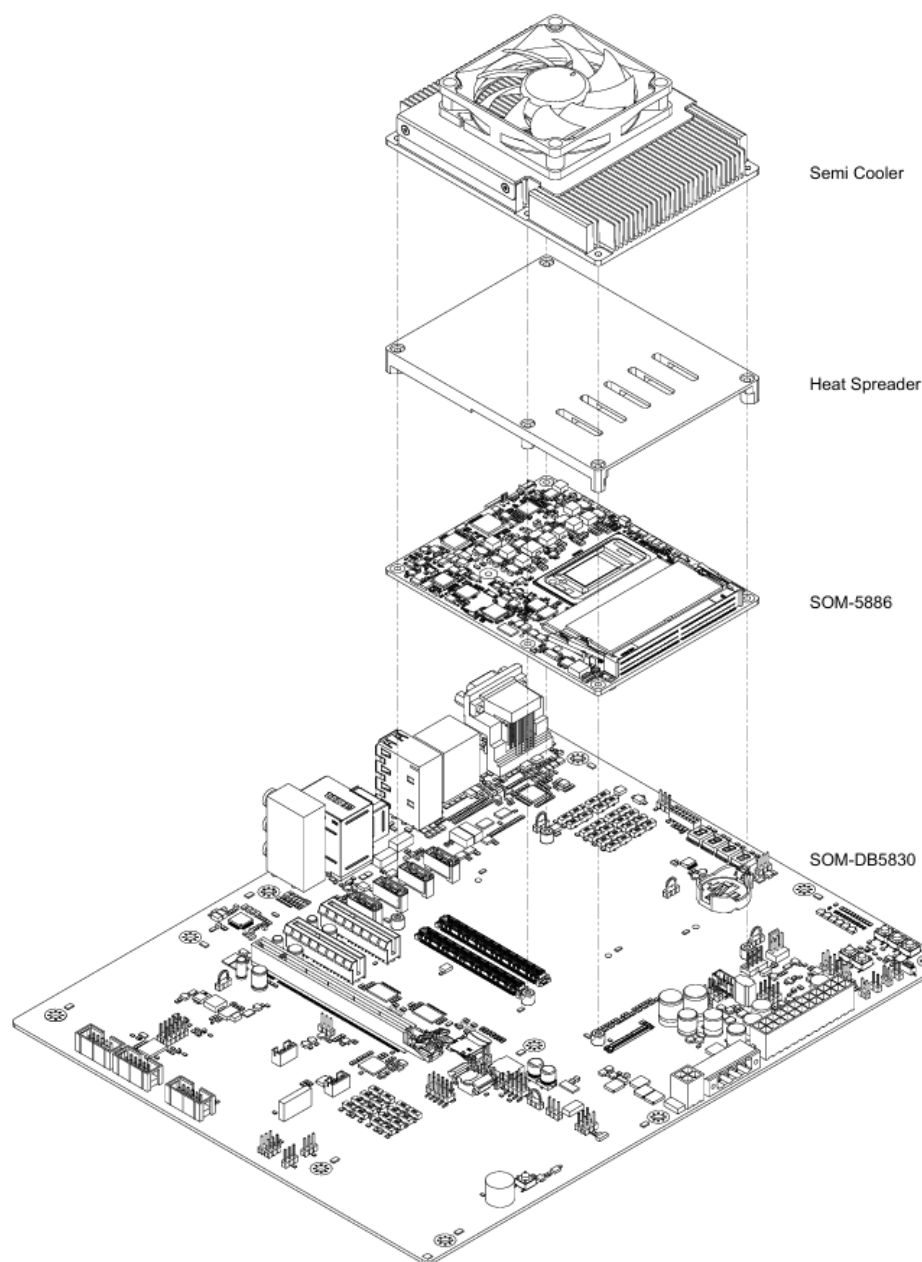


Figure 2.6 Assembly Diagram

There are 5 reserved screw holes for SOM-5886 to be pre-assembled with heat spreader.

2.4 Assembly Diagram

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

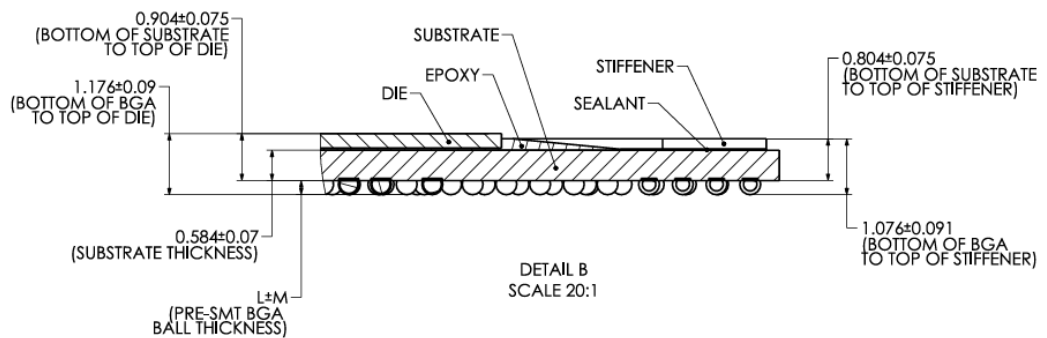


Figure 2.7 CPU Height and Tolerance (H12Xe)

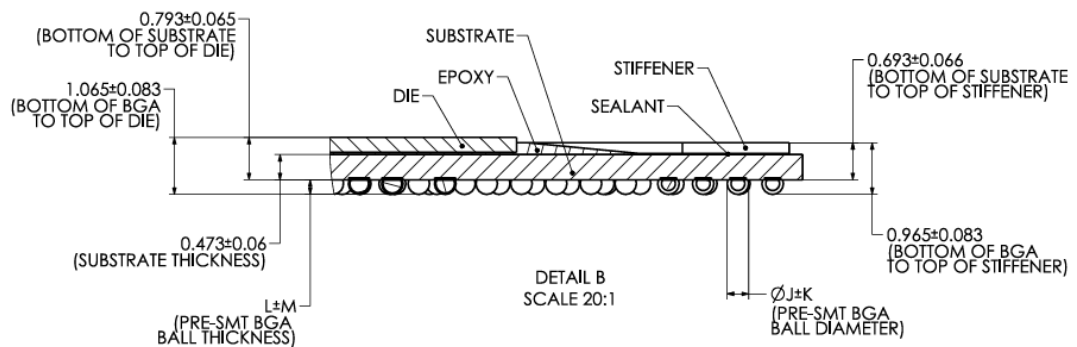


Figure 2.8 CPU Height and Tolerance (H404)

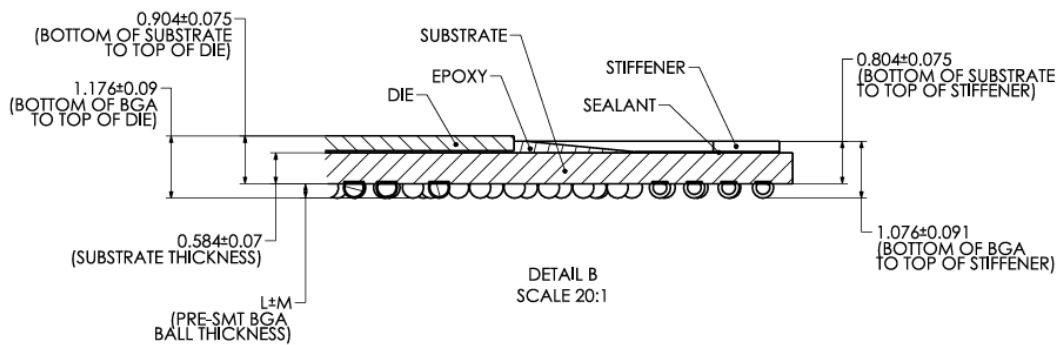


Figure 2.9 CPU Height and Tolerance (H484)

Chapter 3

AMI BIOS

This chapter gives BIOS setup information for the SOM-5886 CPU computer-on module.

Sections include:

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

3.1 Introduction

The AMI BIOS has been integrated into many motherboards for over a decade. With the AMI BIOS Setup Utility, users can modify 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 Date

Set the Date. Use Tab to switch between Date elements. Default Ranges:

Year: 1998-9999

Months: 1-12

Days: Dependent on month Range of Years may vary.

■ System Time

Set the Time. Use Tab to switch between Time elements.

3.4 Advanced BIOS Features Setup

Select the Advanced tab from the SOM-5886 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 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.

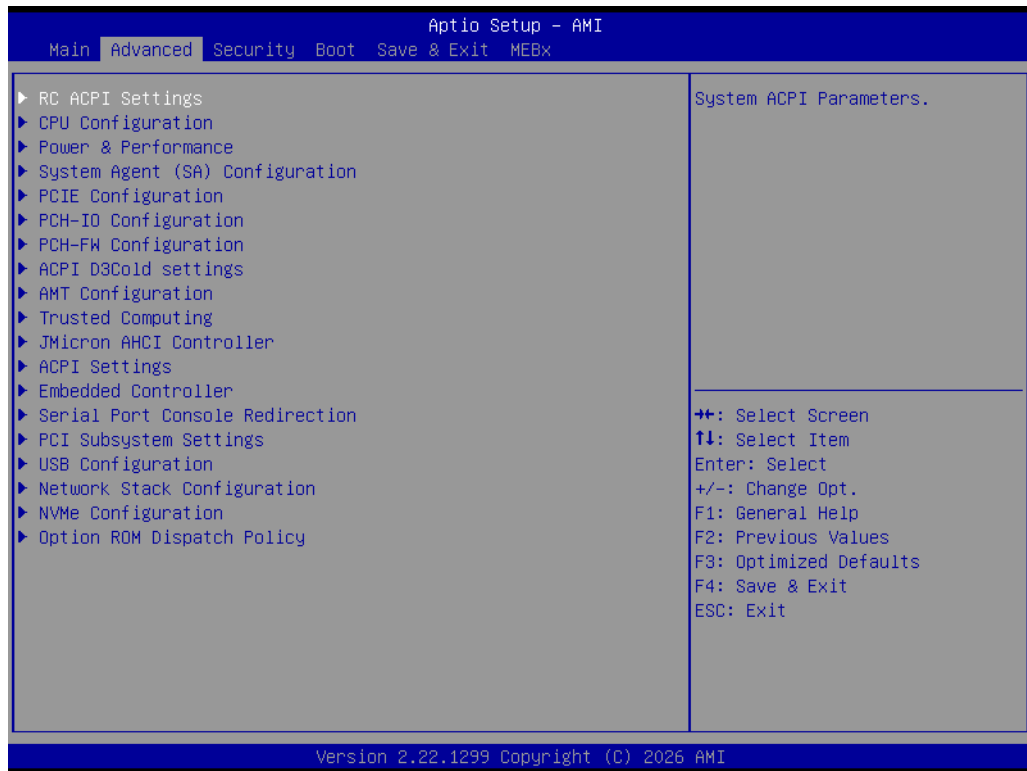


Figure 3.3 Advanced Features Setup Screen

- **RC ACPI Settings**
System ACPI Parameters.
- **CPU Configuration**
CPU Configuration Parameters.
- **Power & Performance**
Power & Performance Options.
- **System Agent (SA) Configuration**
System Agent (SA) Parameters.
- **PCIe Configuration**
PCIE Parameters
- **PCH-IO Configuration**
PCH Parameters
- **PCH-FW Configuration**
Configure Management Engine Technology Parameters.
- **ACPI D3Cold Settings**
ACPI D3Cold related settings
- **AMT Configuration**
Configure Intel® Active Management Technology Parameters.

- **Trusted Computing**
Trusted Computing Settings.
- **JMicron AHCI Controller**
JMicron AHCI Controller.
- **ACPI Settings**
System ACPI Parameters.
- **Embedded Controller**
Embedded Controller Parameters.
- **Serial Port Console Redirection**
Serial Port Console Redirection.
- **PCI Subsystem Settings**
PCI Subsystem Settings.
- **USB Configuration**
USB Configuration Parameters.
- **Network Stack Configuration**
Network Stack Settings.
- **NVMe Configuration**
NVMe Device Options Settings.
- **Option ROM Dispatch Policy**
Option ROM Dispatch Policy

3.4.1 RC ACPI Settings

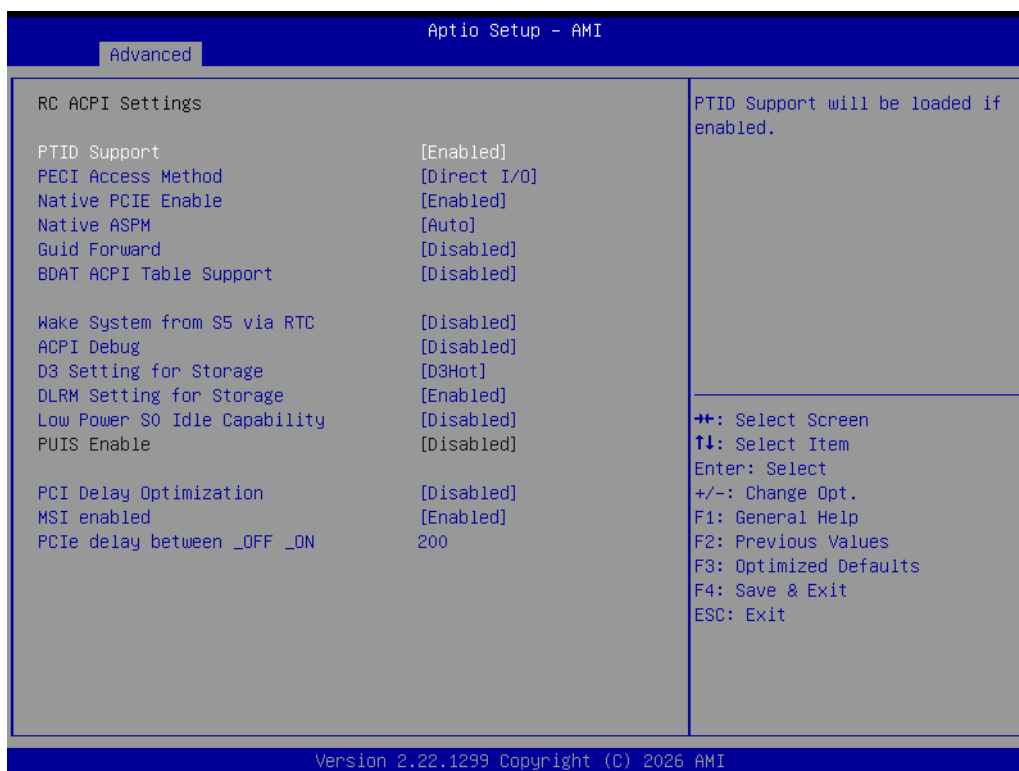


Figure 3.4 RC ACPI Settings

- **PTID Support**
PTID Support will be loaded if enabled.
- **PCIe Access Method**

PCIe Access Method is Direct I/O or ACPI.

■ **Native PCIe Enable**

When Enabled, Enables below OSPM capabilities

Bit-PCIe Native*control

0~Hot Plug

1-SHPC Native Hot Plug control

2~Power Management Events

■ **Native ASPM**

Enabled-OS Controlled ASPM, Disabled-BIOS Controlled ASPM.

■ **Guid Forward**

Forward PPI/Protocol Guid, status code to scratch.

■ **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 method ADBG to write strings to 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 Constraints Configuration->PEP PCIe Storage) when this setup is disabled/D3Hot.

■ **DLRM Setting for Storage**

Dynamic Link (PCIe) Rate management (DLRM) for Storage to reduce active power usage in D0.

■ **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.

3.4.2 CPU Configuration

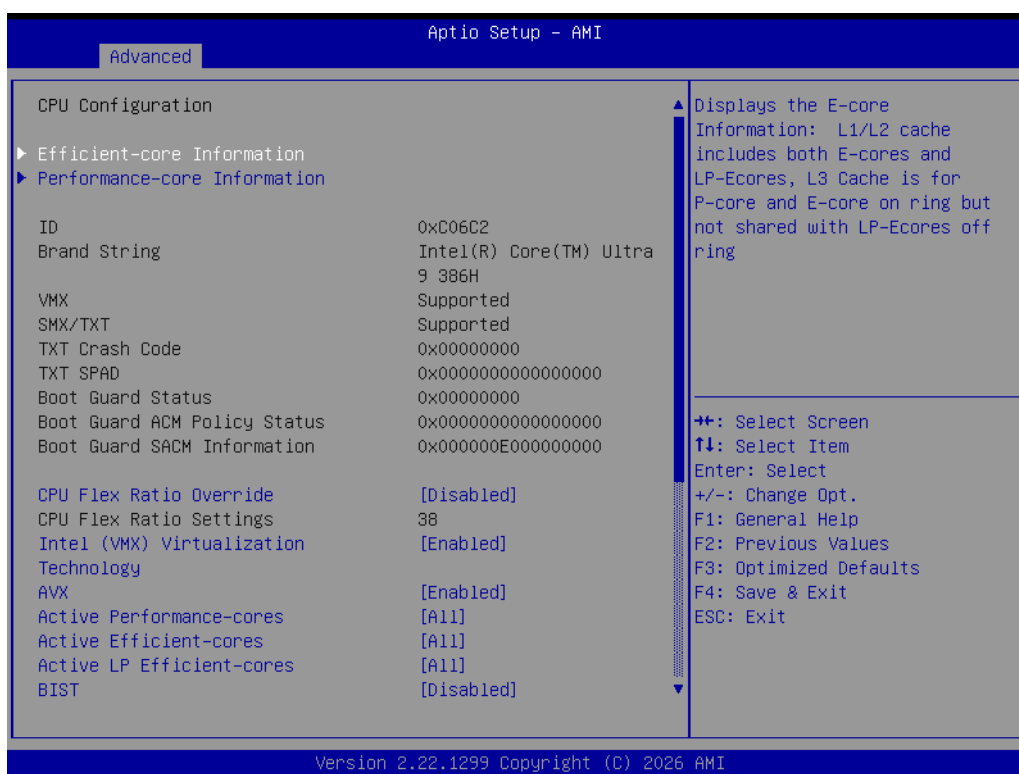


Figure 3.5 CPU Configuration

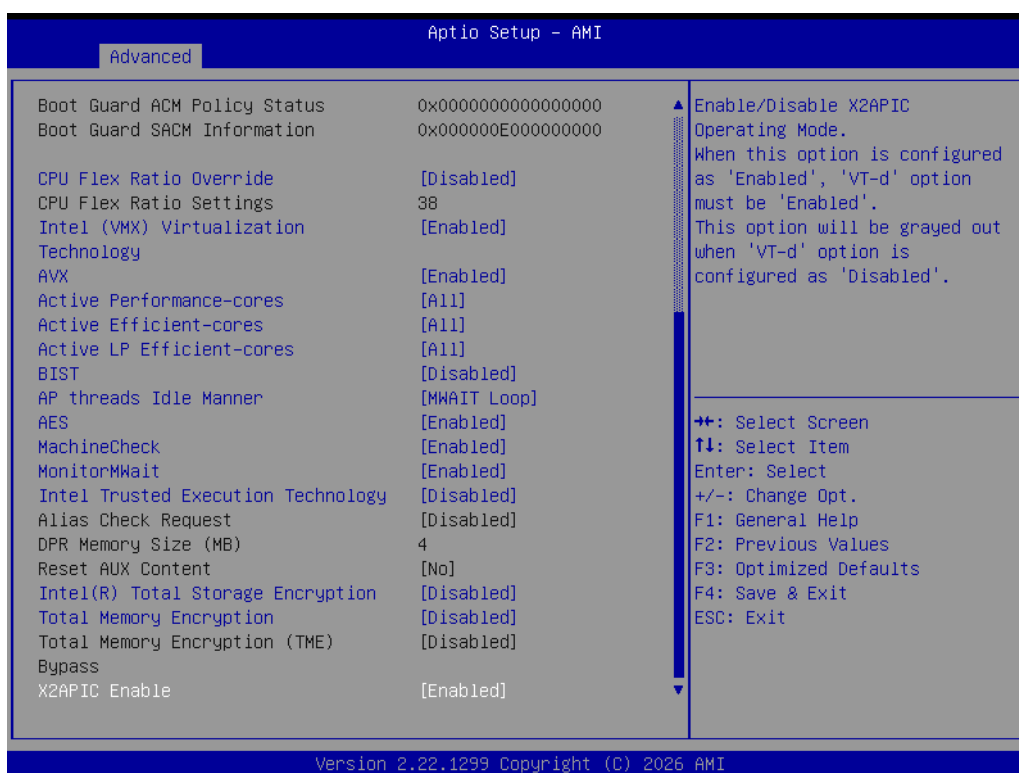
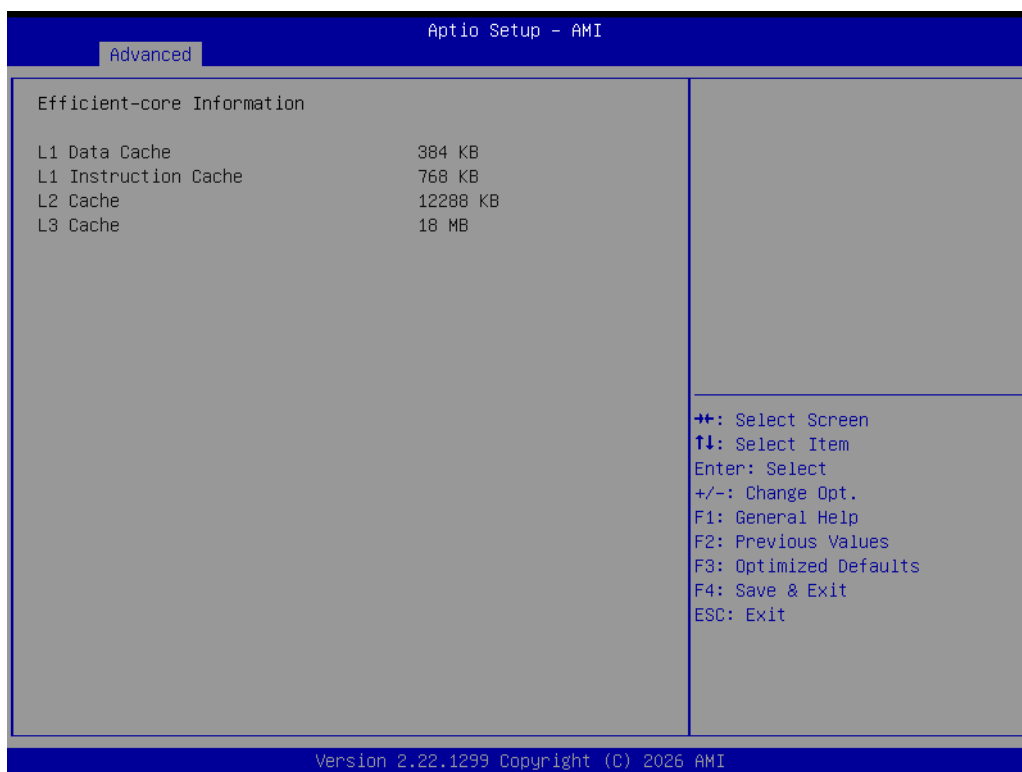


Figure 3.6 CPU Configuration

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

Information: L1/L2 cache includes both E-cores and LP-Ecores, L3 Cache is for P-core and E-core on ring but not shared with LP-Ecores off ring.

- **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: P-Cores must be greater than zero as per Reset HAS.
- **Active Efficient-cores**
Number of E-cores to enable in each processor package. Note: Number of P-Cores, E-cores and LP E-cores are looked at together. When all are {0,0,0}, Pcode will enable all cores.
- **Active LP Efficient-cores**
Number of LP E-cores off ring. Note: Number of P-Cores, E-cores and LP E-cores are looked at together. When all are {0,0,0}, Pcode will enable all cores.
- **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 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'.

**Figure 3.7 Efficient-core Information****Figure 3.8 Performance-core**

3.4.3 Power & Performance

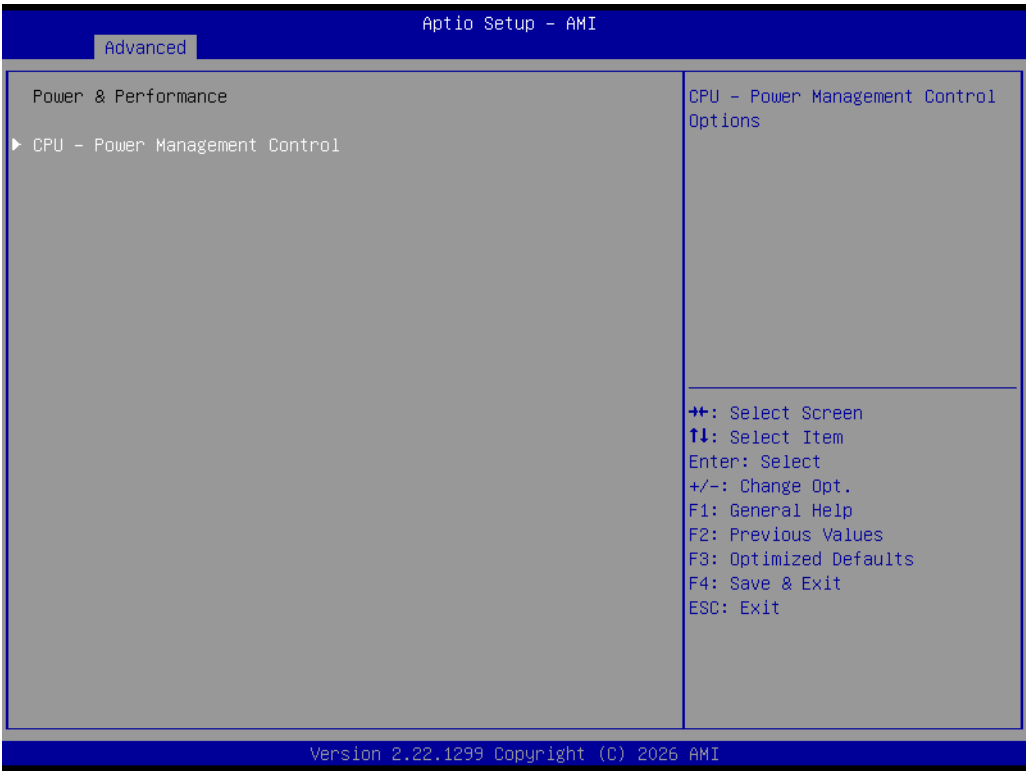


Figure 3.9 Power & Performance

- **CPU - Power Management Control**
CPU - Power Management Control Options

3.4.3.1 CPU - Power Management Control

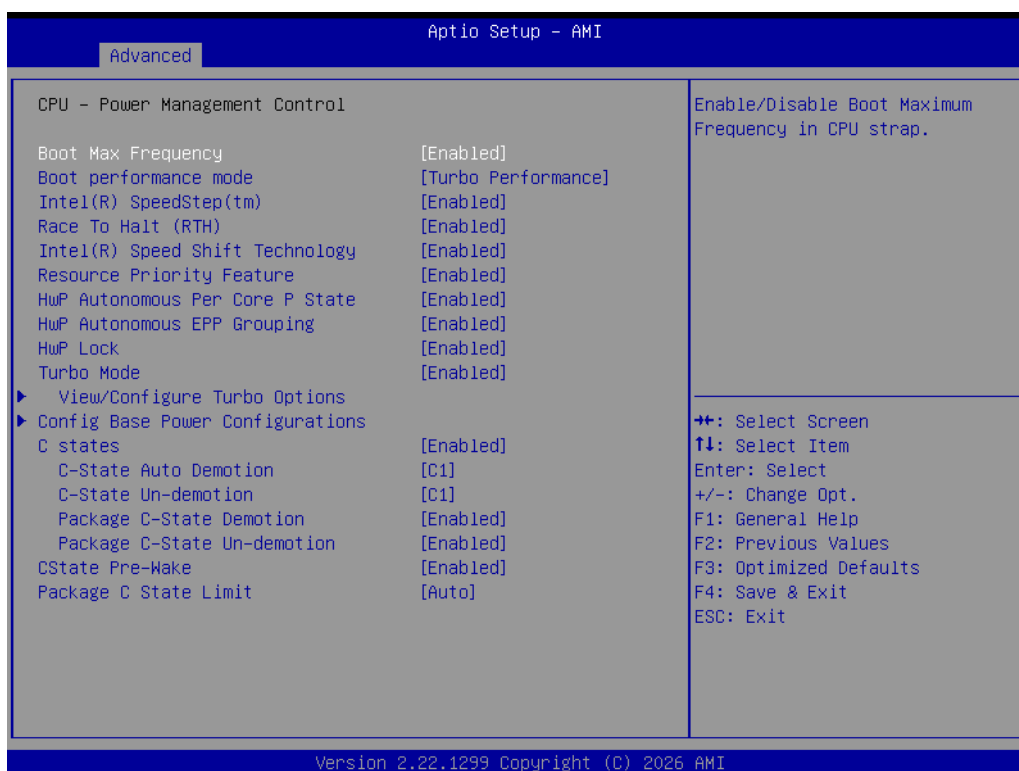


Figure 3.10 CPU - Power Management Control

- **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.
- **Resource Priority Feature**
Enable/Disable Resource Priority Feature support.
- **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 Base Power Configurations**
Assured Power (cTDP) Configurations.
- **C States**
Enable/Disable CPU Power Management. Allows CPU to go to C states when it's not 100% utilized.
- **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.
- **Package C State Limit**
Maximum Package C State Limit Setting. CPU Default: Leaves to Factory default value. Auto: Initializes to deepest available Package C State Limit.

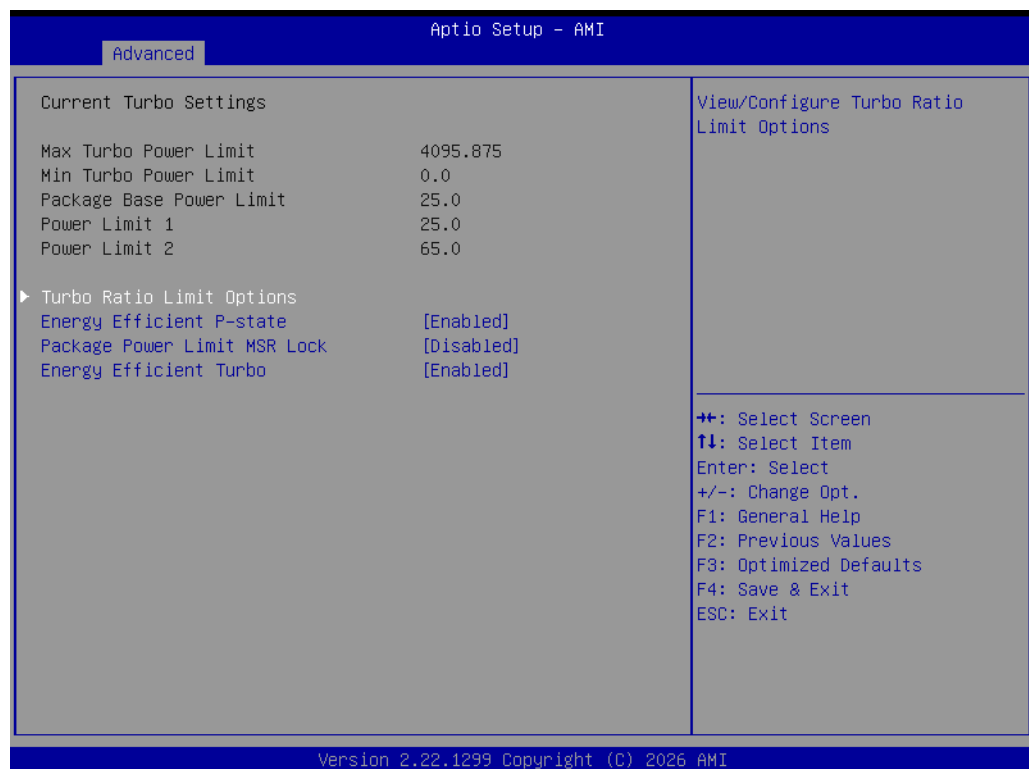


Figure 3.11 Current Turbo Settings

- **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, will disable access to the ENERGY_PERFORMANCE_BIAS MSR and CPUID Function 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. Recommended only to disable it in overclocking situations where turbo frequency must remain constant. Otherwise, leave it as enabled.

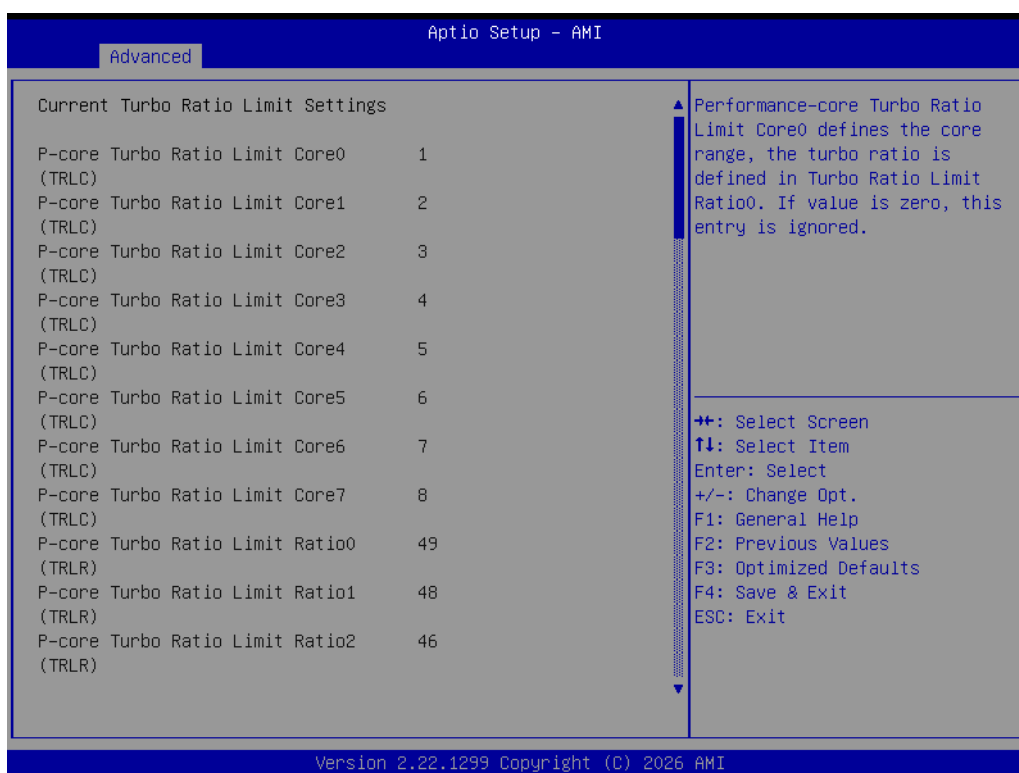


Figure 3.12 Current Turbo Ratio Limit Settings

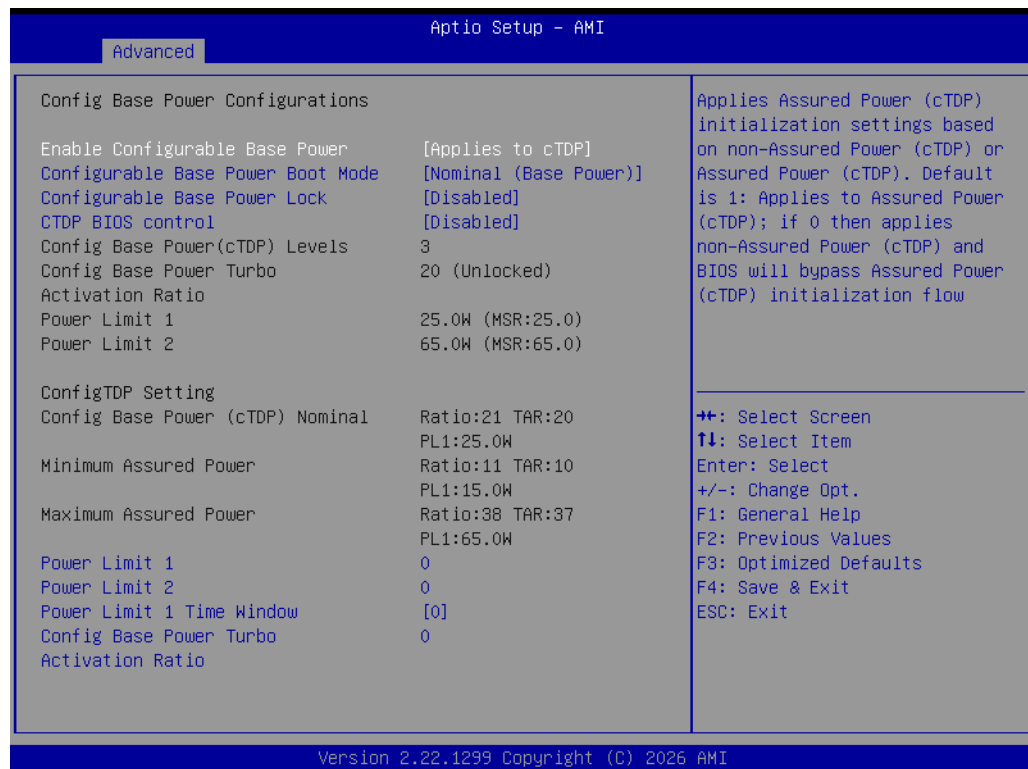


Figure 3.13 Config Base Power Configurations

- **Enable Configurable TDP**
Applies Assured Power (cTDP) initialization settings based on non-Assured Power (cTDP) or Assured Power (cTDP). Default is 1: Applies to Assured Power (cTDP); if 0 then applies non- Assured Power (cTDP) and BIOS will bypass Assured Power (cTDP) initialization flow.
- **Configurable Base Power Boot Mode**
Assured Power (cTDP) Mode as Nominal/Maximum/Minimum Base Power (TDP) selection.
- **Configurable Base Power Lock**
Assured Power (cTDP) Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and BASE_POWER_CONTROL. Note: When cTDP (Assured Power) Lock is enabled, Custom Config Base Power (cTDP) Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.
- **CTDP BIOS Control**
Enables Assured Power (cTDP) control via runtime ACPI BIOS methods. This 'BIOS only' feature does not require EC or driver support.
- **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 value in milliwatts. BIOS will round to the nearest 1/8W when programming. 0=no custom override. For 12.50W, enter 12500. 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). Defines time window which Processor Base Power (TDP) value should be maintained.

- **Config Base Power Turbo Activation Ratio**

Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.

3.4.4 System Agent (SA) Configuration



Figure 3.14 System Agent (SA) Configuration

- **Memory Configuration**
Memory Configuration Parameters
- **Graphics Configuration**
Graphics Configuration
- **VMD Setup Menu**
VMD Configuration settings
- **VT-d Setup Menu**
VT-d Configuration settings

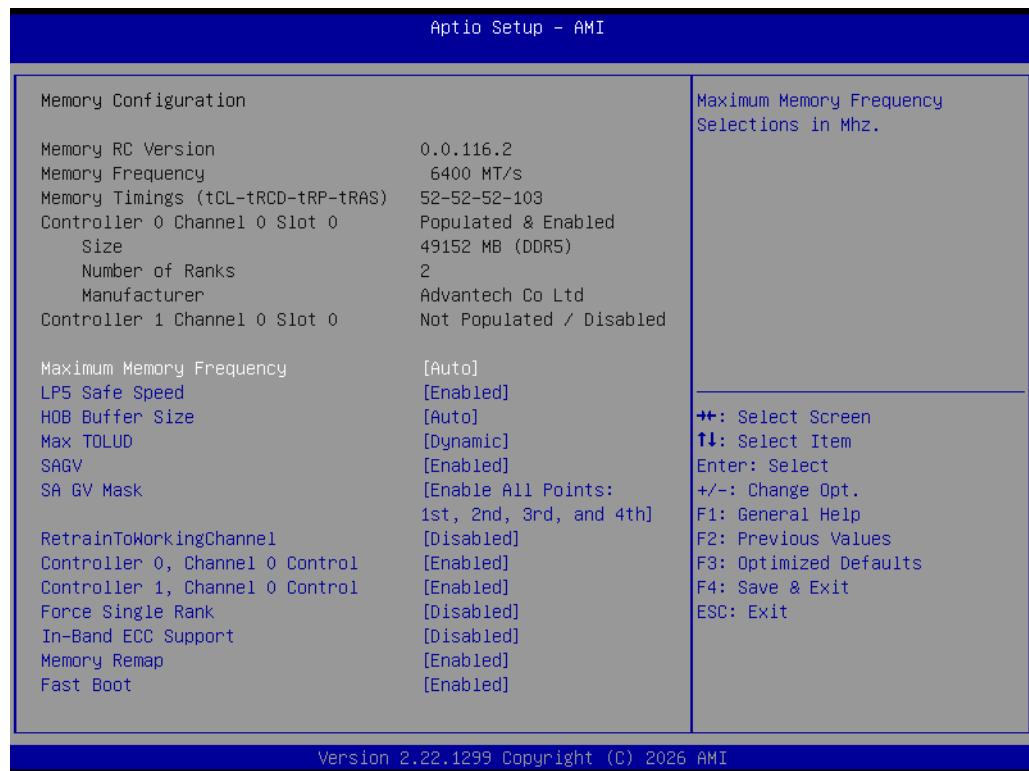


Figure 3.15 Memory Configurations

- **Maximum Memory Frequency**
Maximum Memory Frequency Selection in Mhz.
- **LP5 Safe Speed**
Limit RVP3 to 8533 and RVP1 to 7467, when using internal SPD, FreqMax is Auto and DRAM doesn't support higher speed.
- **HDB Buffer Size**
Size to set HDB Buffer
- **Max TOLUD**
Maximum Value of TOLUD. Dynamic assignment would adjust TOLUD automatically based on target MMIO length of installed graphic controller.
- **SAGV**
System Agent Geyserville. Disabled or Enabled.
- **SA GV Mask**
System Agent Geyserville. Set the BIT(s) for which points to use in frequency switching.
- **RetrainToWorkingChannel**
Retrain To Working Channel.
- **Controller 0, Channel 0 Control**
Controller 0, Channel 0 Control – Enable or Disable Controller 0, Channel 0.
- **Controller 1, Channel 0 Control**
Controller 1, Channel 0 Control – Enable or Disable Controller 1, Channel 0.
- **Force Single Rank**
When enabled, only Rank 0 will be used in each DIMM.
- **In-Band ECC Support**

Enable/Disable InBand ECC. Will be enabled if memory has symmetric configuration.

- **Memory Remap**

Enable/Disable Memory Remap above 4GB.

- **Fast Boot**

Enable/Disable fast path thru the MRC.

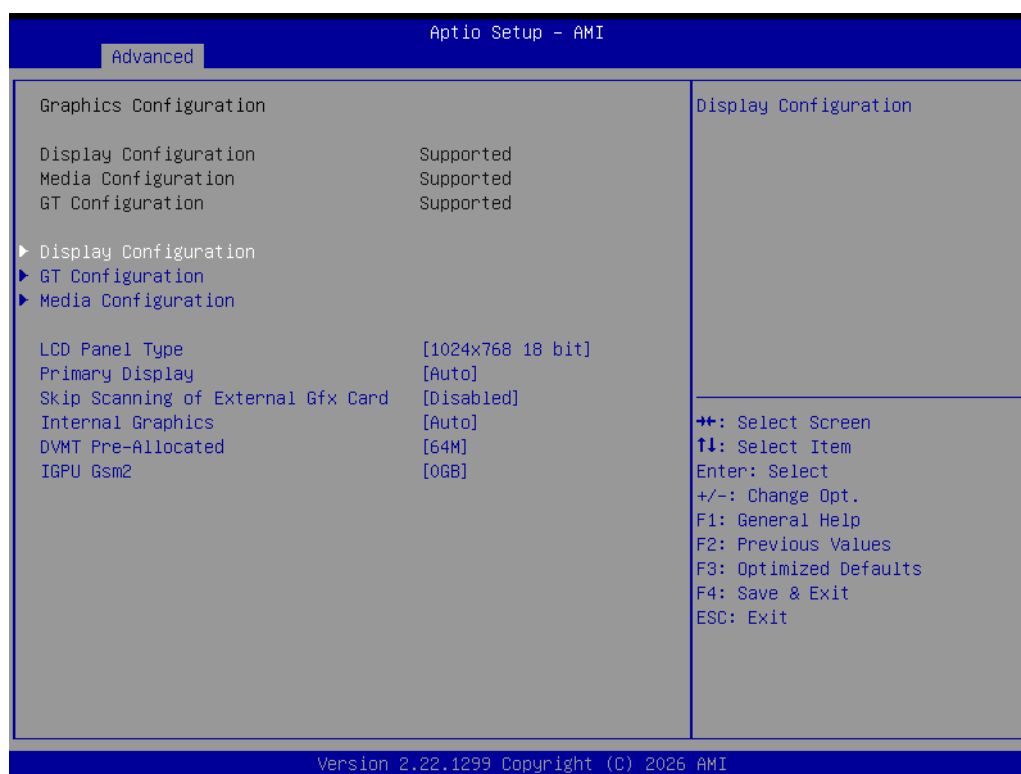


Figure 3.16 Graphics Configurations

- **Display Configuration**

Display Configuration.

- **GT Configuration**

GT Configuration.

- **Media Configuration**

Media Configuration.

- **LCD Panel Type**

Select LCD panel used by Internal Graphics Device by selecting the appropriate setup item.

- **Primary Display**

Select AUTO set IGD to be Primary Display if no external Graphics Device connected otherwise external Graphics Device detected on first PCIe port will be Primary Display or Select IGPU for IGD to be Primary Display or Select HG for Hybrid Gfx

- **Skip Scanning of External Gfx Card**

If Enable, it will not scan for External Gfx Card on PCIe Ports.

- **Internal Graphics**

Keep IGPU enabled based on the setup options.

- **DVMT Pre-Allocated**

Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.

- **IGPU Gsm2**
Graphics Stolen Memory 2

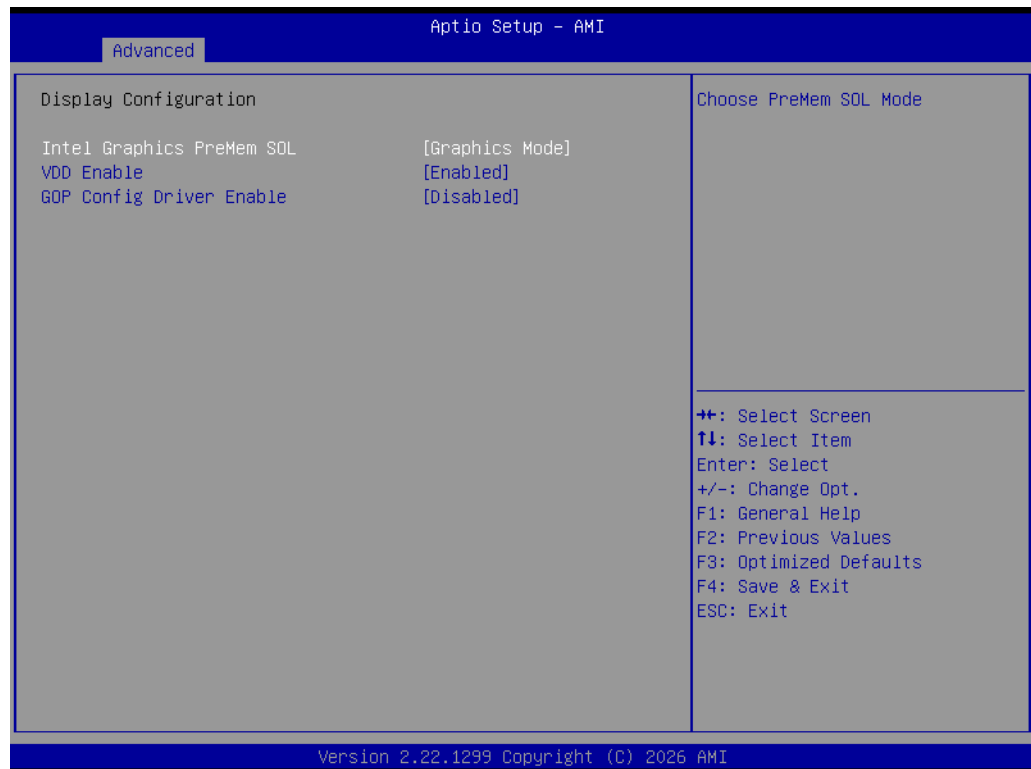


Figure 3.17 Display Configurations

- **Intel Graphics PreMem SOL**
Choose PreMem SOL Mode.
- **VDD Enable**
Enable/Disable forcing of VDD in the BIOS.
- **GOP Config Driver Enable**
Enable/Disable GOP Config Driver.



Figure 3.18 GT Configurations

- **Configure GT for Use**
Enable/Disable GT configuration in BIOS.
- **GT RC1p Support**
Enable/Disable RC1p support.If GT RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met.
- **RC6(Render Standby)**
Check to enable render standby support.
- **Reduce XeCores**
Enable/Disable Reduce XeCores.

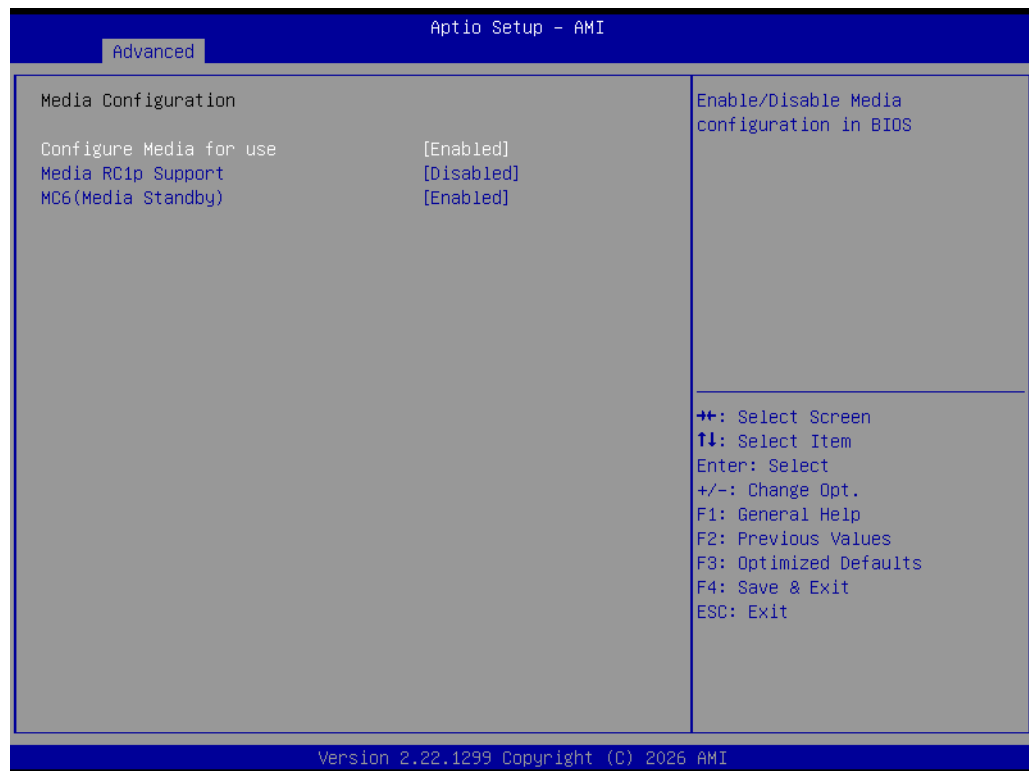


Figure 3.19 Media Configurations

- **Configure Media for Use**
Enable/Disable Media configuration in BIOS.
- **Media RC1p Support**
Enable/Disable RC1p support.If Media RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met.
- **MC6(Media Standby)**
Check to enable Media standby support.



Figure 3.20 VMD Setup Menu

- **Enable VMD Controller**
Enable/Disable to VMD controller.



Figure 3.21 VT-d Setup Menu

- **Pre-boot DMA Protection**
Enabled DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
- **Nested Support**
Defeature Nested Capability.
- **Posted Interrupt Support**
Defeature Posted Interrupt Capability.
- **DMA Control Guarantee**
Enable/Disable DMA_CONTROL_GUARANTEE bit.
- **TBT Performance Boost**
Enable/Disable TBT Performance Boost through PCode mailbox.

3.4.5 PCIe Configuration

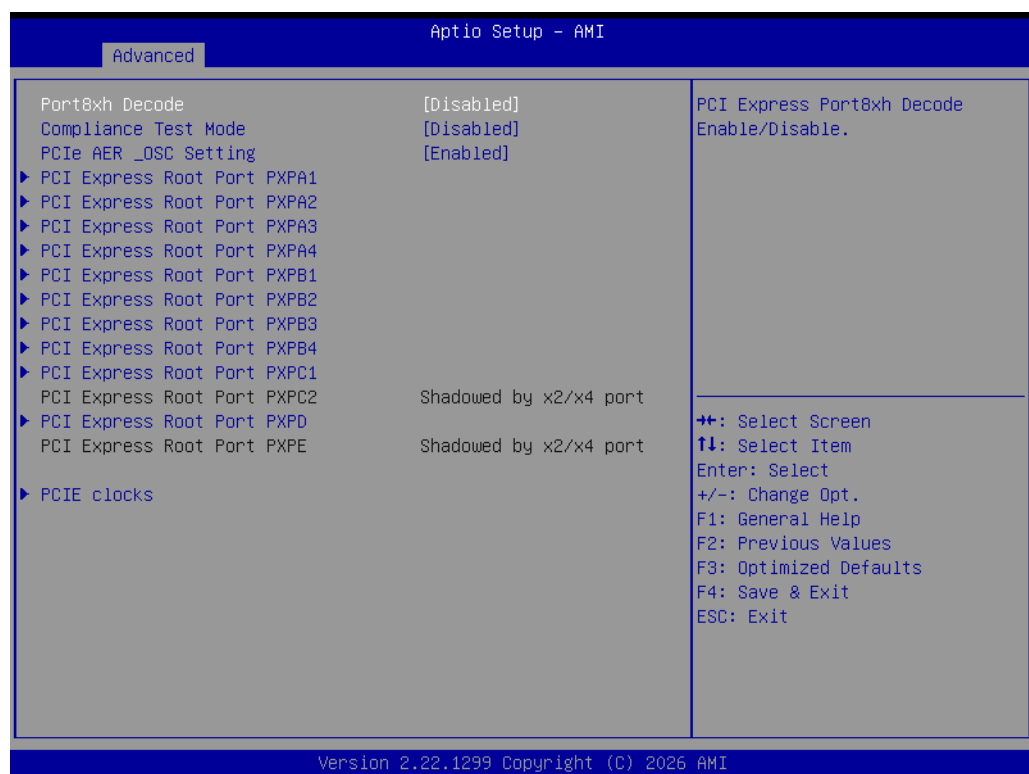


Figure 3.22 PCIe Configuration

- **Port18xh Decode**
PCI Express Port8xh Decode Enable/Disable.
- **Compliance Test Mode**
Enable when using Compliance Load Board.
- **PCIe AER _OSC Setting**
Enable/Disable Platform-wide PCIe Advanced Error Reporting via ACPI _OSC method.
- **PCI Express Root Port PXPA1**
PCI Express Root Port Settings. COM Express PCIE0.
- **PCI Express Root Port PXPA2**
PCI Express Root Port Settings. COM Express PCIE1.
- **PCI Express Root Port PXPA3**

- PCI Express Root Port Settings. COM Express PCIE2.
- **PCI Express Root Port PXPA4**
PCI Express Root Port Settings. COM Express PCIE3.
- **PCI Express Root Port PXPB1**
PCI Express Root Port Settings. COM Express PCIE4.
- **PCI Express Root Port PXPB2**
PCI Express Root Port Settings. COM Express PCIE5.
- **PCI Express Root Port PXPB3**
PCI Express Root Port Settings. COM Express PCIE6.
- **PCI Express Root Port PXPB4**
PCI Express Root Port Settings. COM Express PCIE7.
- **PCI Express Root Port PXPC1**
PCI Express Root Port Settings. COM Express PEG8-11/PCIE24-27.
- **PCI Express Root Port PXPD**
PCI Express Root Port Settings. COM Express PEG0-7/PCIE16-23.
- **PCIe Clocks**
PCIe clocks

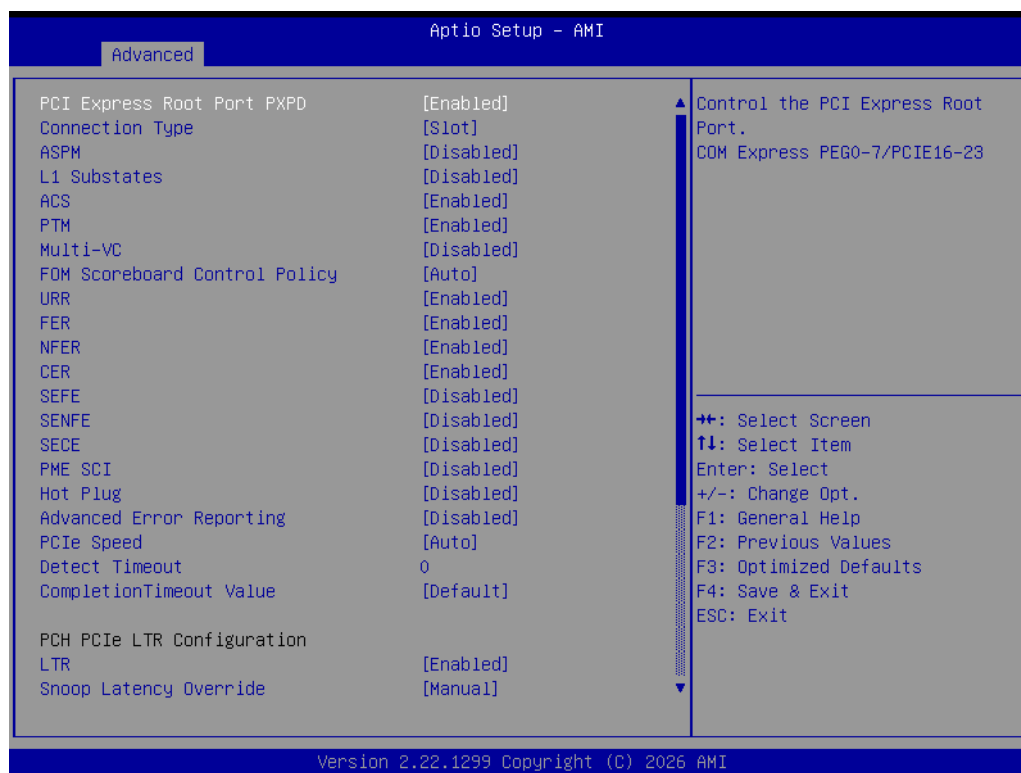


Figure 3.23 PCI Express Root Port PXPD

- **PCI Express Root Port PXPD**
Control the PCI Express Root Port. COM Express PCIE6.
- **Connect Type**
Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.
- **ASPM**
Set the ASPM Level: Force L0s – Force all links to L0s State

AUTO – BIOS auto configure

DISABLE – Disables ASPM.

■ **L1 Substates**

PCI Express L1 Substates settings.

■ **ACS**

Enable/Disable Access Control Services Extended Capability.

■ **PTM**

Enable/Disable Precision Time Measurement.

■ **Multi-VC**

Enable/Disable Multi Virtual Channel.

■ **FOM Scoreboard Control Policy**

Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS.

■ **URR**

PCI Express Unsupported Request Reporting Enable/Disable.

■ **FER**

PCI Express Device Fatal Error Request Enable/Disable.

■ **NFER**

PCI Express Device Non-Fatal Error Reporting Enable/Disable.

■ **CER**

PCI Express Device Correctable Error Reporting Enable/Disable.

■ **SEFE**

Root PCI Express System Error on Fatal Error Enable/Disable.

■ **SENFE**

Root PCI Express System Error on Non-Fatal Error Enable/Disable.

■ **SECE**

Root PCI Express System Error on Correctable Error Enable/Disable.

■ **PME SCI**

PCI Express PME SCI Enable/Disable.

■ **Advanced Error Reporting**

Advanced Error Reporting Enable/Disable.

■ **PCIe Speed**

Configure PCIe Speed.

■ **Detect Timeout**

The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.

■ **Completion Timeout Value**

PCH PCIe Completion Timeout Value.

■ **LTR**

PCH PCIe Latency Reporting Enable/Disable.

■ **Snoop Latency**

Snoop Latency Override for PCH PCIe.

■ **Disabled: Disable override.**

Manual: Manually enter override values..

■ **Snoop Latency Value**

LTR Snoop Latency value of PCIe, recommended value is 65us so default value to this BIOS knob is 65..

- **Snoop Latency Multiplier**

LTR Snoop Latency Multiplier of PCIe, recommended value is 65us so default value to this BIOS knob is 1024ns which will be multiplied with LTR Value.

- **Non Snoop Latency Override**

Non Snoop Latency Override for PCH PCIe.

- **Disabled: Disable override.**

Manual: Manually enter override values.

- **Non Snoop Latency Value**

LTR Non Snoop Latency Value of PCIe, recommended value is 65us so default value to this BIOS knob is 65.

- **Non Snoop Latency Multiplier**

LTR Non Snoop Latency Multiplier of PCIe, recommended value is 65us.

- **LTR Override Spec Compliant**

By default is Desired Value. When Desired Value is selected, LTR value will be programmed with recommended value. When Spec Compliant is selected, it will program 400ns LTR value and may block platform PG.

- **PP2P Support**

Program P2P Support Registers according to setup option.

- **Assertion on Link Down GPIOs**

GPIO Assertion on Link Down.

- **PCIe EQ Settings**

PCIe EQ settings.

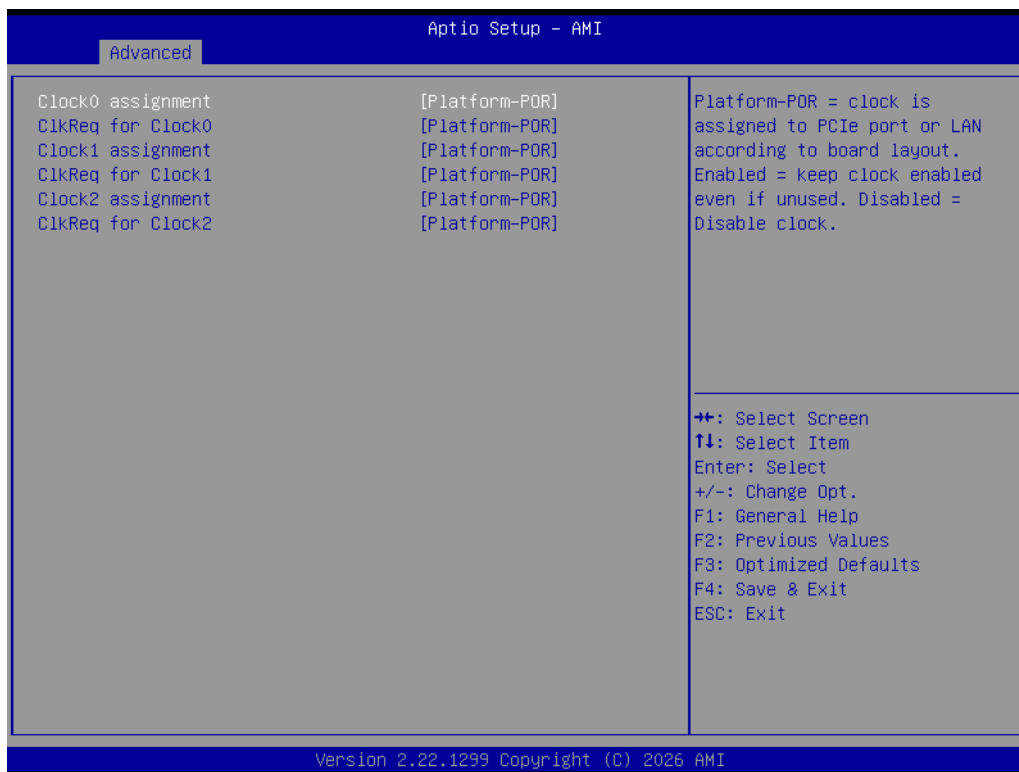


Figure 3.24 PCIe Clocks

- **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.

3.4.6 PCH-I/O Configuration



Figure 3.25 PCH-I/O Configuration

- **USB Configuration**
USB Configuration settings.
- **Security Configuration**
Security Configuration settings.
- **HD Audio Configuration**
HD Audio Configuration settings.

- **Wake on LAN Support**
Enable/Disable Intel Foxville Wake on LAN Support.
- **State After G3**
Specify what state to go to when power is re-applied after a power failure (G3 state).
- **PCIe Device Initial Delay**
The PCIe device initial delay 0~30 second.
- **Enhance Port 80th LPC Decoding**
Support the word/dword decoding of port 80h behind LPC Disable for CS1 (0-base) to validate DPRE.
- **Legacy IO Low Latency**
Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.
- **Enable TCO Timer**
Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDATtable will not be published.
- **Enable 8254 Clock Gate**
Enable/Disable 8254 clock gate in early phase. Set 8254CGE is necessary for SLP_S0 support. Platform is able to disable this policy and set 8254CGE in late phase.
- **Lock PCH Sideband Access**
Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g.PSFx). The option is invalid if POST-BOOT SAI is set.
- **Flash Protection Range Registers(FPRR)**
Enable Flash Protection Range Registers.
- **SPD Write Disable**
Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.
- **LGMR**
64KB memory block for LGMR (LPC Memory Range Decode)

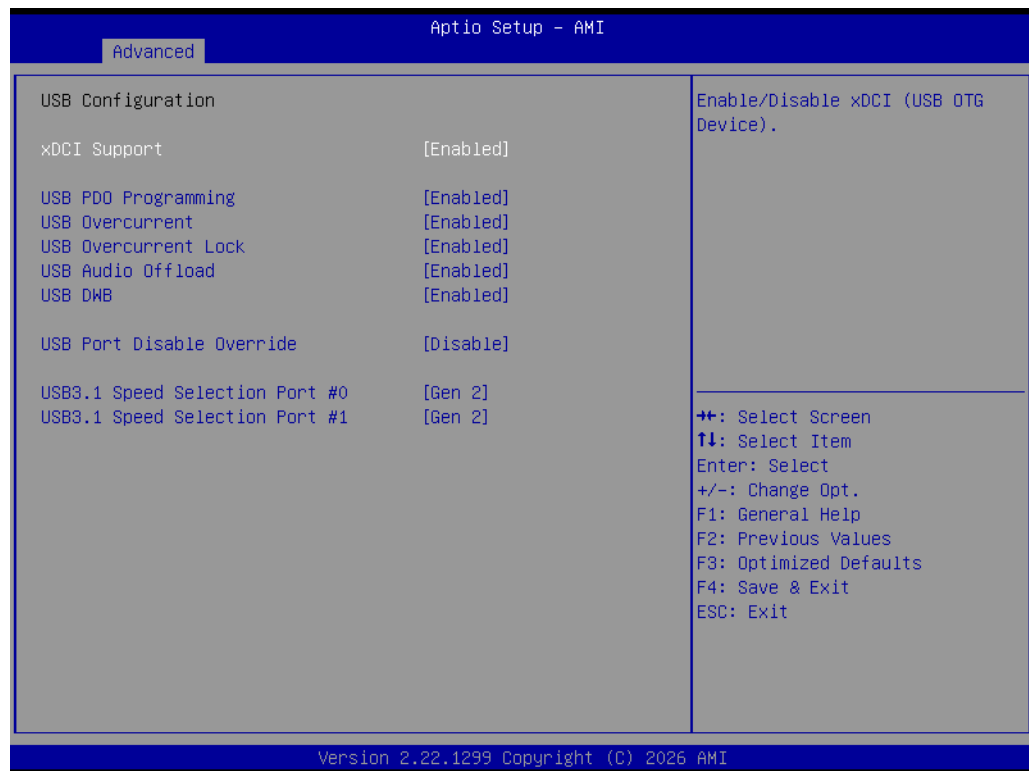


Figure 3.26 USB Configuration

- **xDCI Support**
Enable/Disable Xdci (USB OTG Device).
- **USB PDO Programming**
Select 'Enabled' if Port Disable Override functionality is used.
- **USB Overcurrent**
Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
- **USB Overcurrent Lock**
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 Offload functionality.
- **USB DWB**
Enable/Disable USB Deferred Write Buffer feature.
- **USB Port Disable Override**
Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
- **USB3.1 Speed Selection Port #0**
USB3.1 Speed selection; Gen1 or Gen2
- **USB3.1 Speed Selection Port #1**
USB3.1 Speed selection; Gen1 or Gen2



Figure 3.27 Security Configuration

- **RTC Memory Lock**
Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.
- **BIOS Lock**
Enable/Disable the PCH BIOS Lock Enable feature. 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 unlocked state.

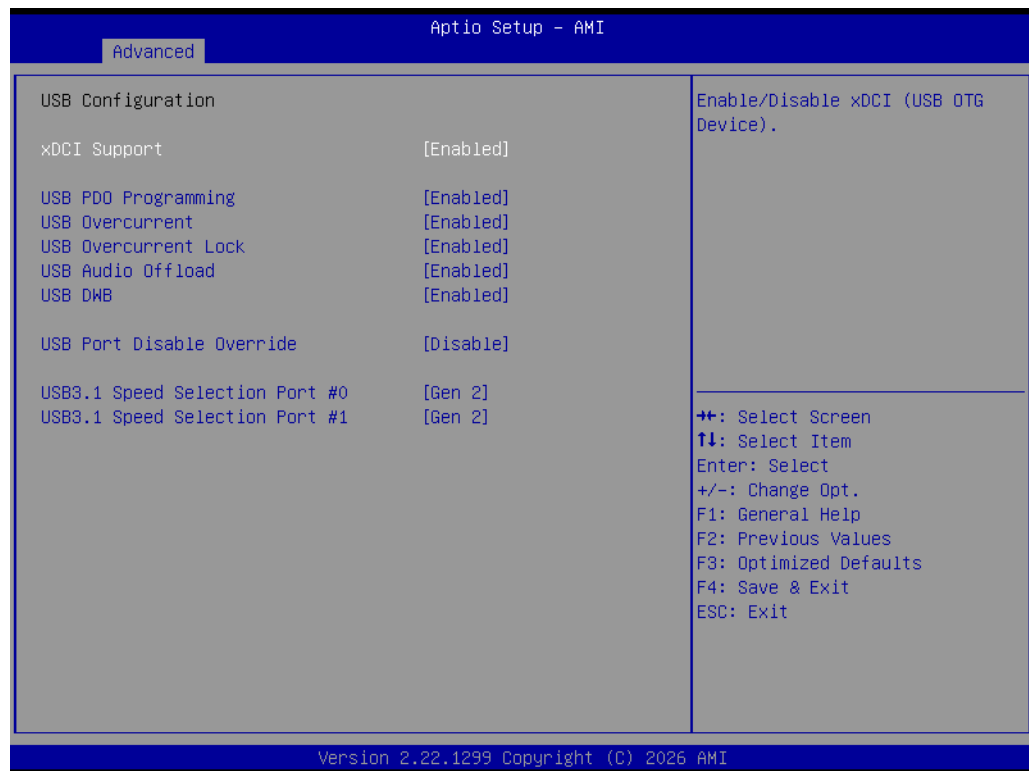


Figure 3.28 HD Audio Configuration Settings

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

3.4.7 PCH-FW Configuration

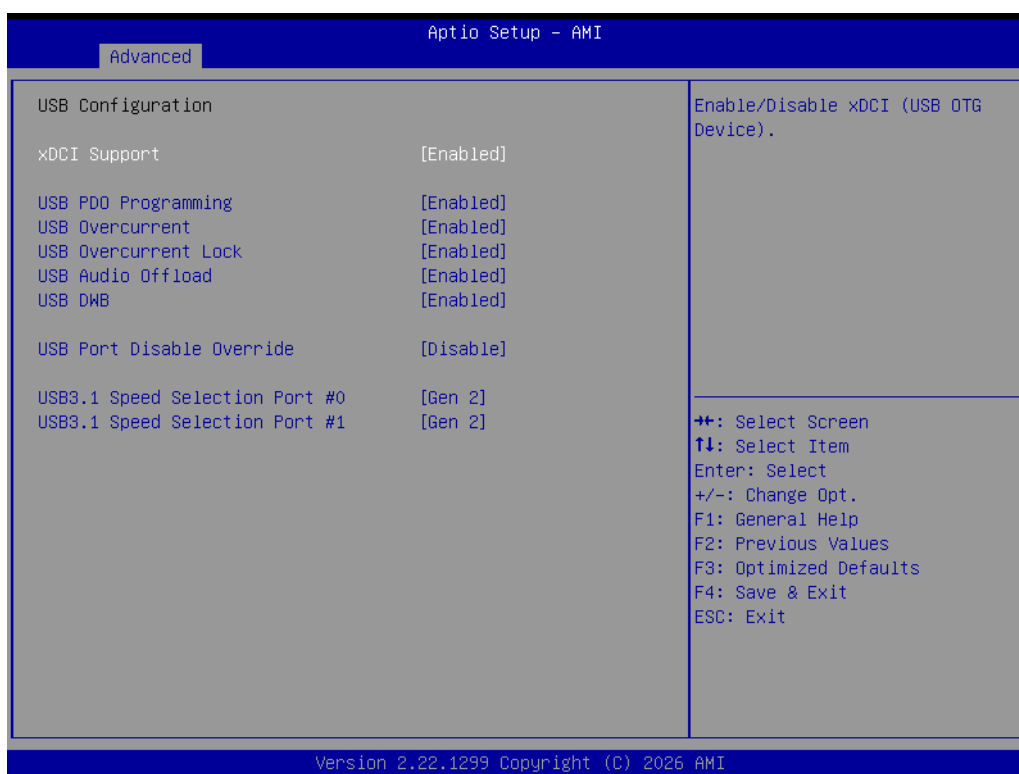


Figure 3.29 PCH-FW Configuration

- **ME State**
When Disabled, ME will be put into ME Temporarily Disabled Mode .
NOTE:
Once this option is changed and saved, it is grayed out to prevent command been sent again before reset.
- **Manageability Features State**
Enable/Disable Inter® Manageability features.
NOTE:
This option disables/enables Manageability Features support in FW.
To disable support platform must be in an unprovisioned state first.
- **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**
Disable: Disable CSE Data Resilience Support.
Enable: Enable CSE Data Resilience Support in PEI.
Enable and defer: Handle CSE Data Clear in DXE.
- **PSE EOM Flow Enable**
Enable/Disable PSE EOM Flow.
- **Firmware Update Configuration**
Configure Management Engine Technology Parameters.
- **Extend CSME Measurement to TPM-PCR**

Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1].

3.4.8 ACPI D3Cold Settings

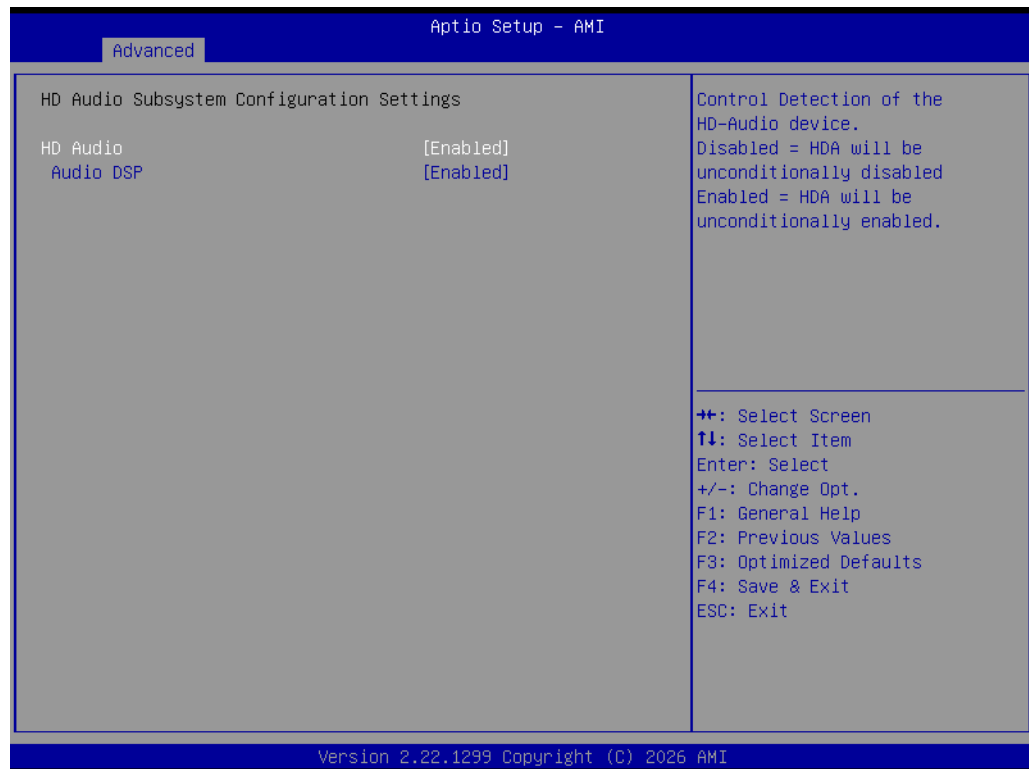


Figure 3.30 ACPI D3Cold Settings

- **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 Device Power-on Delay in ms**
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.
- **RTD3 Support for PCIe Root Ports**
Enable/Disable PCIe RTD3 Support.
- **IUER Button Enable**

- **Intel® Ultrabook Event Support**
Enable/Disable IUER Button Functionality.
Intel® Ultrabook Event Support.

Figure 3.31 Intel® Ultrabook Event Support

- **IUER Slate Enable**
Enable/Disable IUER Slate Functionality.
- **IUER Dock Enable**
Enable/Disable IUER Dock Functionality.

3.4.9 AMT Configuration



Figure 3.32 AMT Configuration

- **USB Provisioning of AMT**
Enable/Disable of AMT USB Provisioning.
- **MAC Pass Through**
Enable/Disable MAC Pass Through function.
- **Dynamic Lan Switch**
Allow switching AMT support from Integrated LAN to Discrete LAN.
- **Activate Remote Assistance Process**
Trigger CIRA boot
Note:
Network Access must be activated first from MEBx Setup.
- **Unconfigure ME**
Unconfigure ME with resetting MEBx password to default on next boot.
- **ASF Configuration**
Configure Alert Standard Format parameters.



Figure 3.33 ASF Configuration

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

3.4.10 Trusted Computing



Figure 3.34 Trusted Computing

- **Security Device Support**
Enables or Disables BIOS support for security device. When its disabled, 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 O.S. 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.

3.4.11 JMicron AHCI Controller

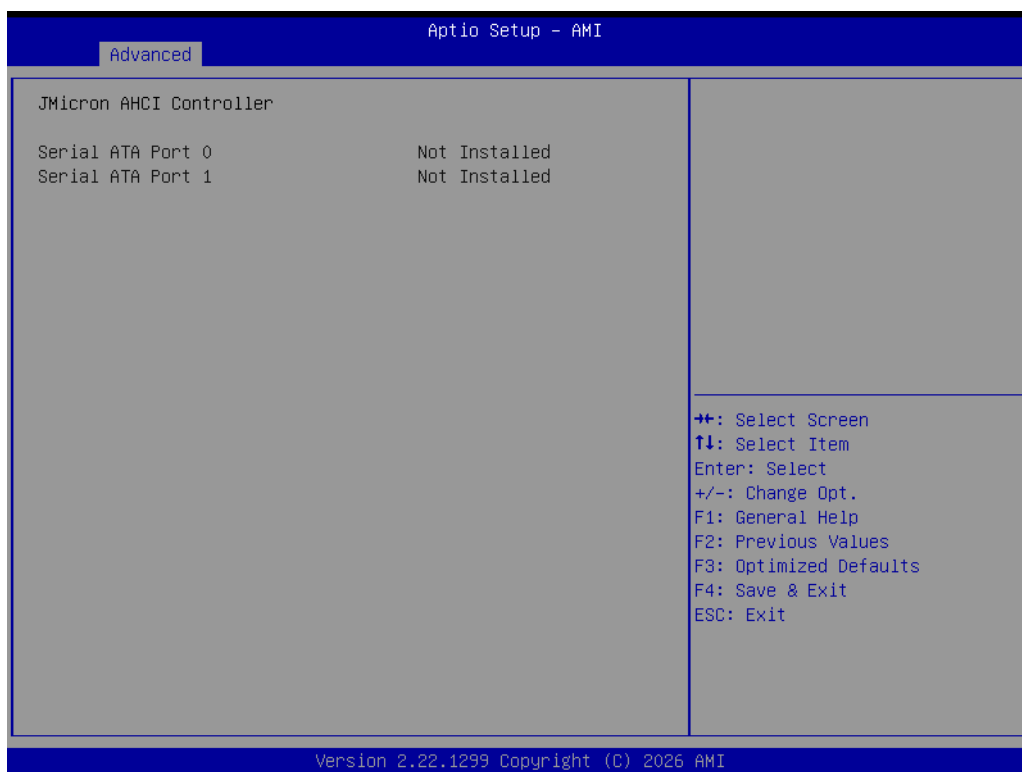


Figure 3.35 JMicron AHCI Controller

3.4.12 ACPI Settings

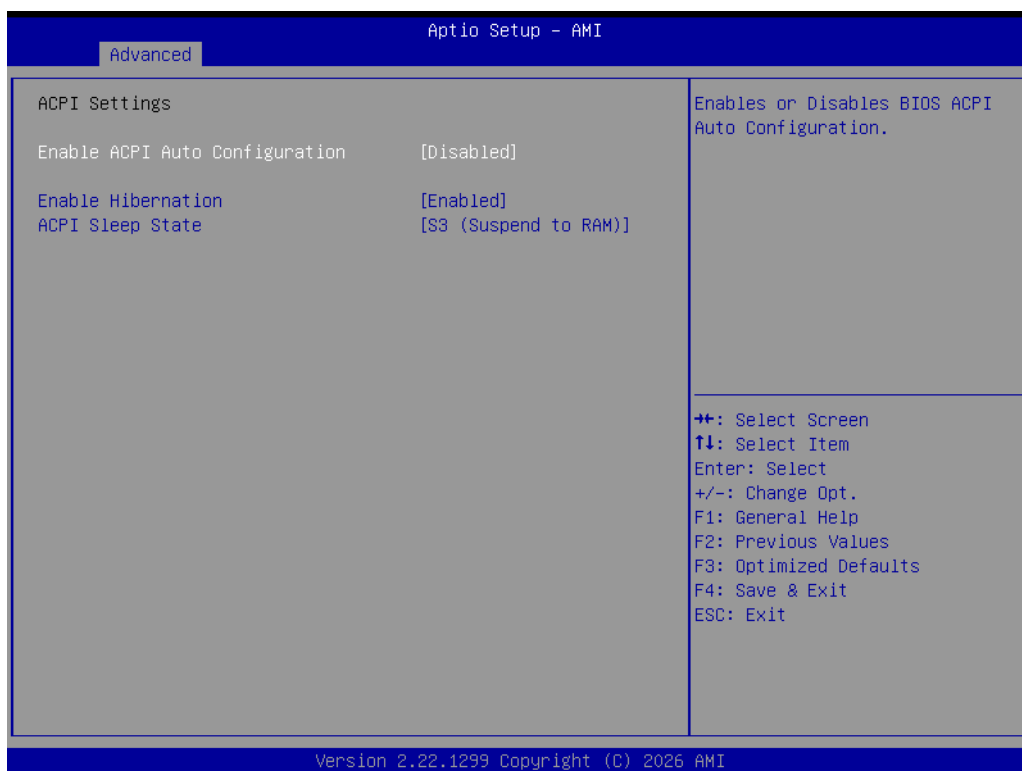


Figure 3.36 ACPI Settings

- **Enable ACPI Auto Configuration**
Enable or Disable BIOS ACPI Auto Configuration.
- **Enable Hibernation**
Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.
- **ACPI Sleep State.**
Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.

3.4.13 Embedded Controller

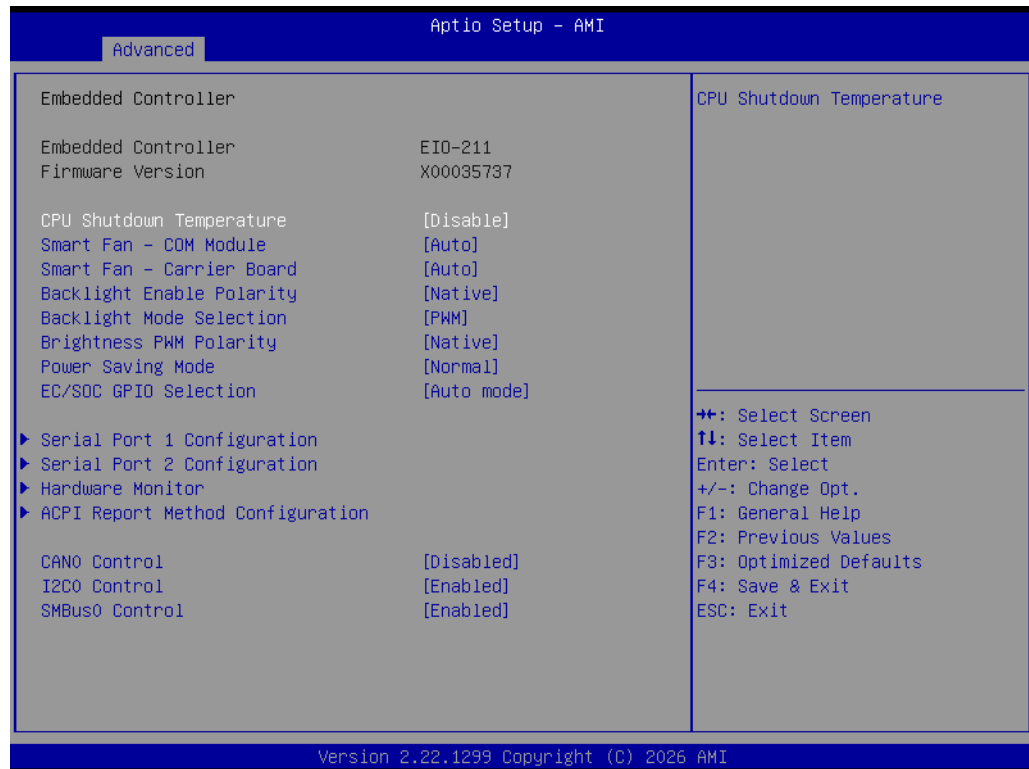


Figure 3.37 Embedded Controller

- **CPU Shutdown Temperature**
CPU Shutdown Temperature.
- **Smart Fan – COM Module**
Control COM Module Smart FAN function. Get value from EC and only sets value when Save Changes.
- **Smart Fan - Carrier Board**
Control Carrier Board Smart FAN function. Get value from EC and only sets value when Save Changes.
- **Backlight Enable Polarity**
Switch Backlight Enable Polarity for Native or Invert.
- **Brightness PWM Polarity**
Backlight Control Brightness PWM Polarity for Native or Invert.
- **Power Saving Mode**
Select Power Saving Mode.
- **EC/SOC GPIO Selection**

- EC/SOC GPIO Selection.
- **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**
Enable/Disable SMBus0 controller on RDC-IS200.

Serial Port 1 Configuration

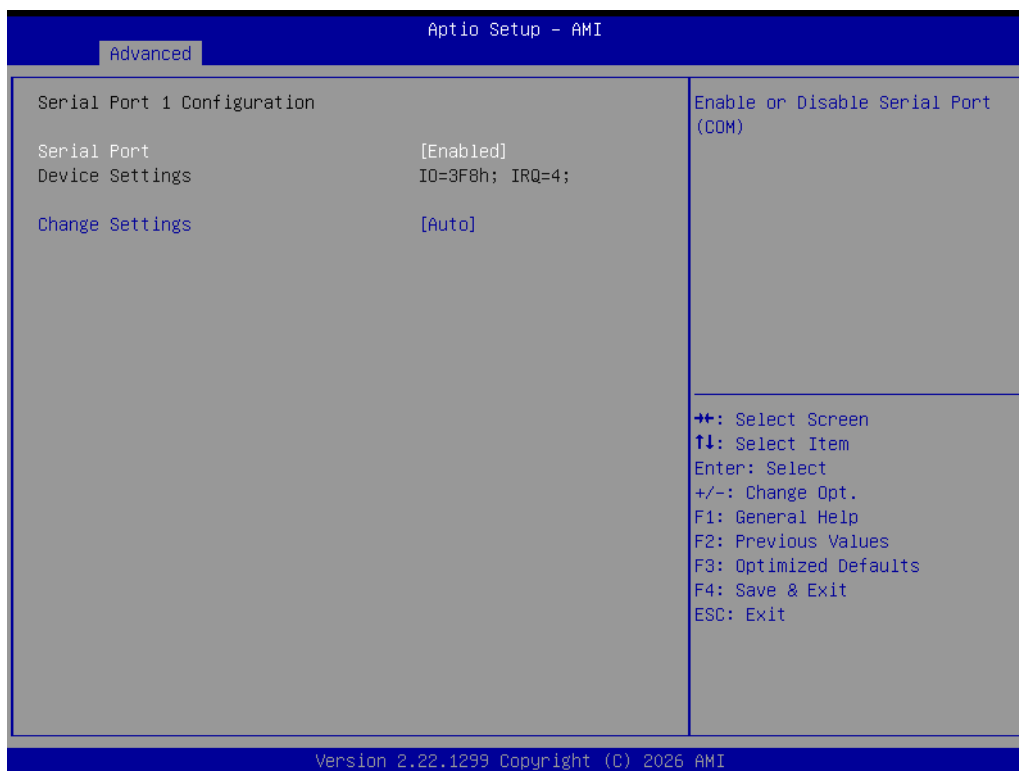


Figure 3.38 Serial Port 1 Configuration

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

Serial Port 2 Configuration

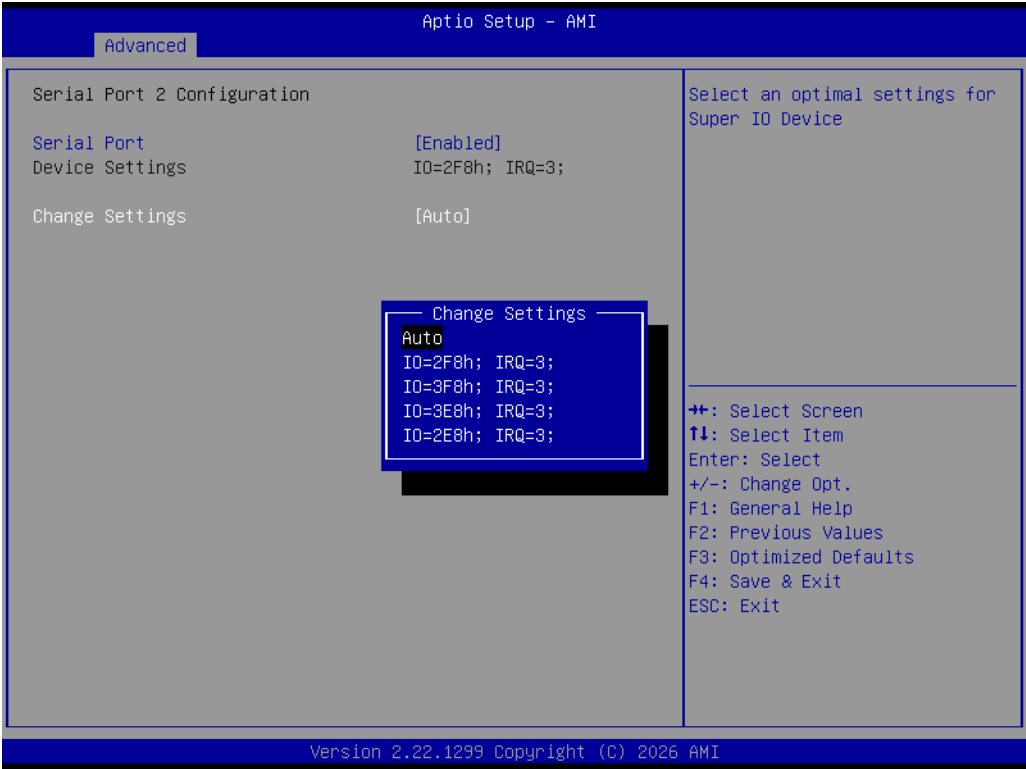


Figure 3.39 Serial Port 2 Configuration

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

ACPI Report Method Configuration



Figure 3.40 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 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.)

3.4.14 Serial Port Console Redirection

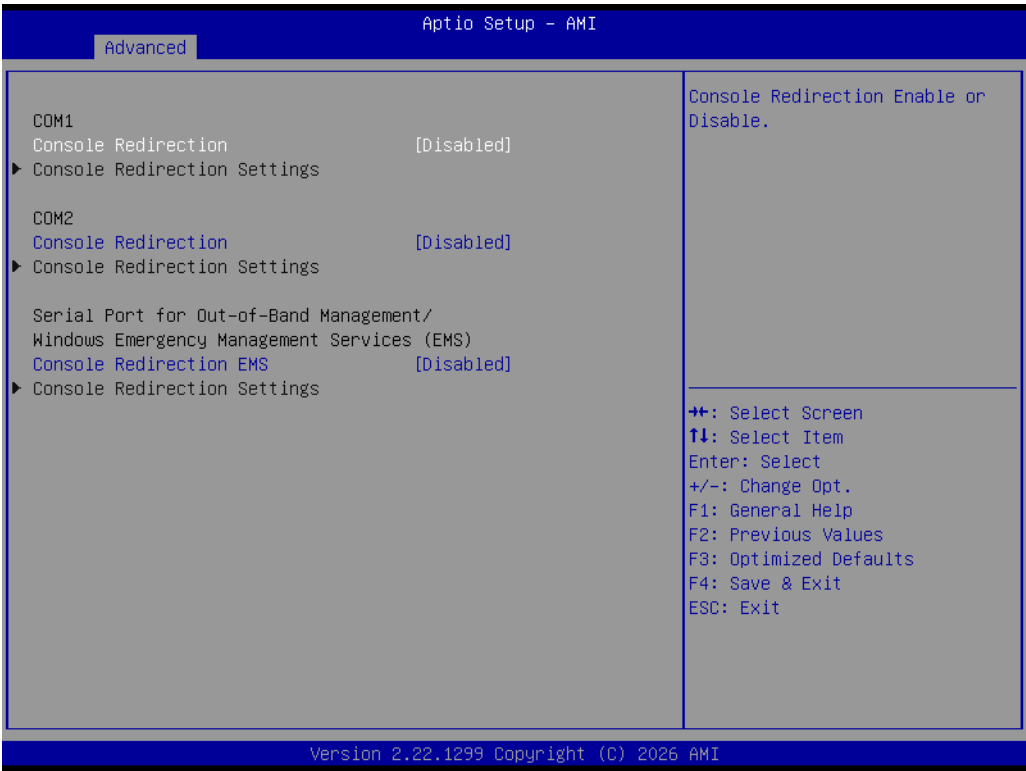


Figure 3.41 Serial Port Console Redirection

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

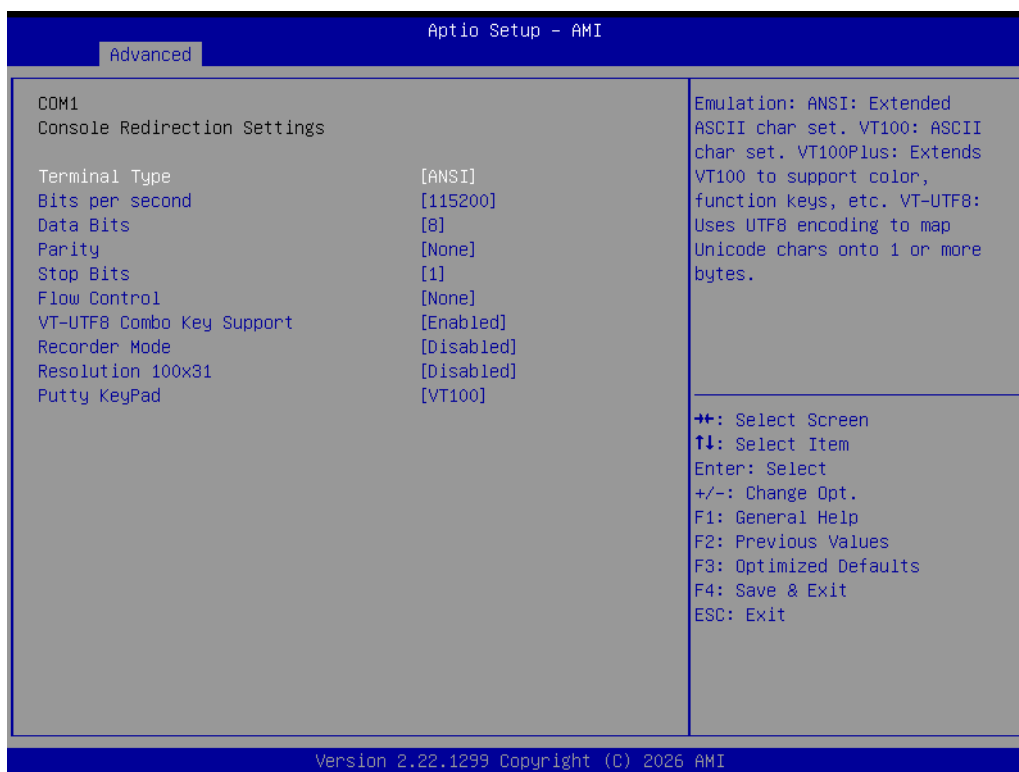


Figure 3.42 Console Redirection Settings

3.4.15 USB Configuration



Figure 3.43 USB Configuration

- **Legacy USB Support**
Enables legacy USB support. AUTO option disables legacy support if no USB devices are connected. DISABLE option will keep USB devices available only for EFI applications..
- **XHCI Hand-off**
This is a workaround for OSes 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.

3.4.16 Network Stack Configuration

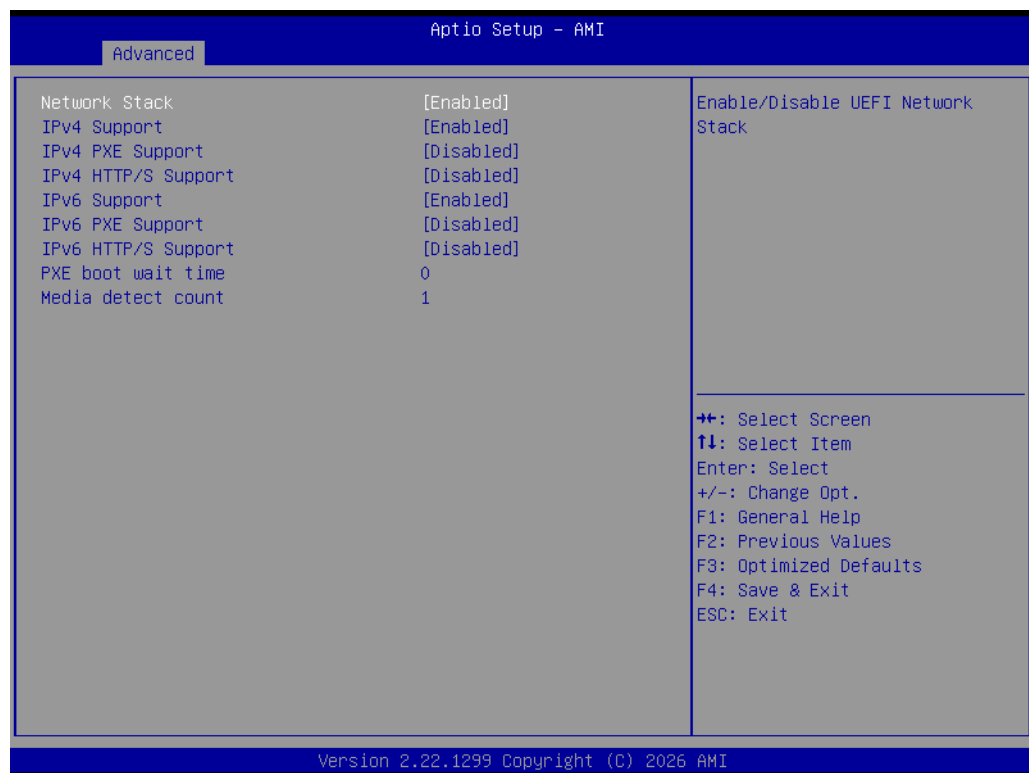


Figure 3.44 Network Stack Configuration

- **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.

3.4.17 NVMe Configuration



Figure 3.45 NVMe Configuration

3.4.18 Option ROM Dispatch Policy

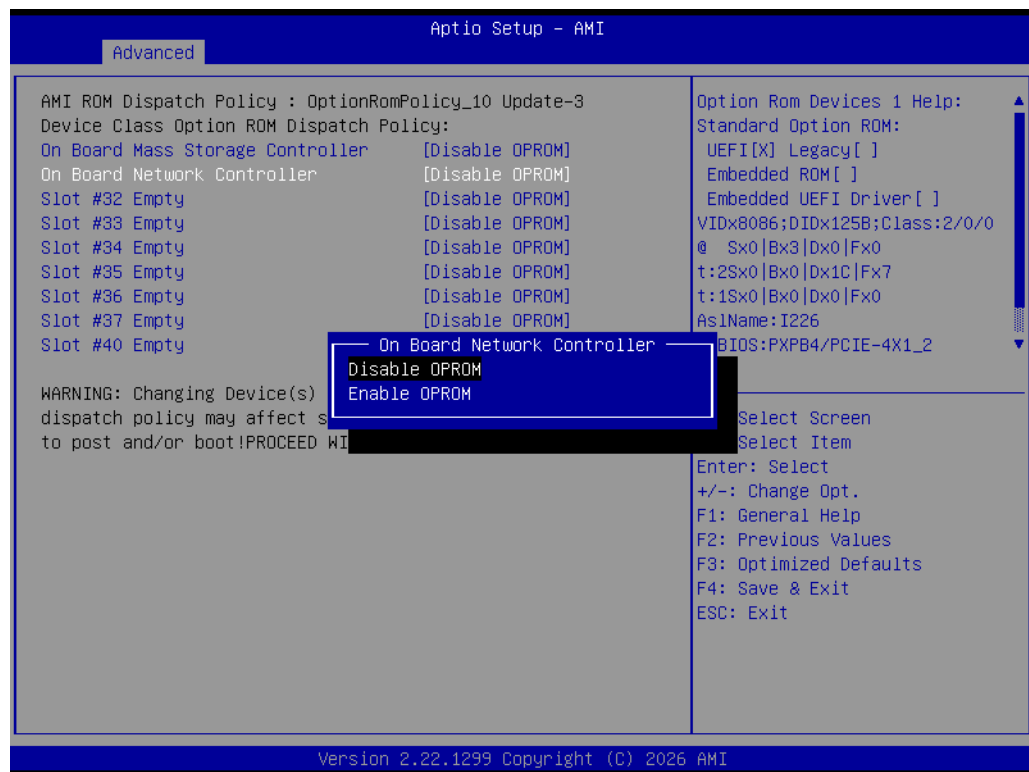


Figure 3.46 Option ROM Dispatch Policy

■ On Board Mass Storage Controller

Option Rom Devices 0 Help:

Standard Option ROM:

UEFI [] Legacy []

Embedded ROM []

Embedded UEFI Driver []

VIDx197B;DIDX0585;Class:1/6/1

@ Sx0|Bx1|Dx0|Fx0

t:2Sx0|Bx0|Dx1C|Fx0

t:1Sx0|Bx0|Dx0|Fx0

AslName: J58x

SMBIOS: PXPB3/PCIE-4X1_2?

■ OnBoard NOT FOUND

Option Rom Devices 1 Help.

■ Slot #32 Empty

Option Rom Devices 2 Help.

■ Slot #33 Empty

Option Rom Devices 3 Help.

■ Slot #34 Empty

Option Rom Devices 4 Help.

■ Slot #35 Empty

Option Rom Devices 5 Help.

■ Slot #36 Empty

- Option Rom Devices 6 Help.
- **Slot #37 Empty**
Option Rom Devices 7 Help.
- **Slot #40 Empty**
Option Rom Devices 8 Help.

3.5 Security Chipset



Figure 3.47 Security Chipset

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

3.5.1 Secure Boot

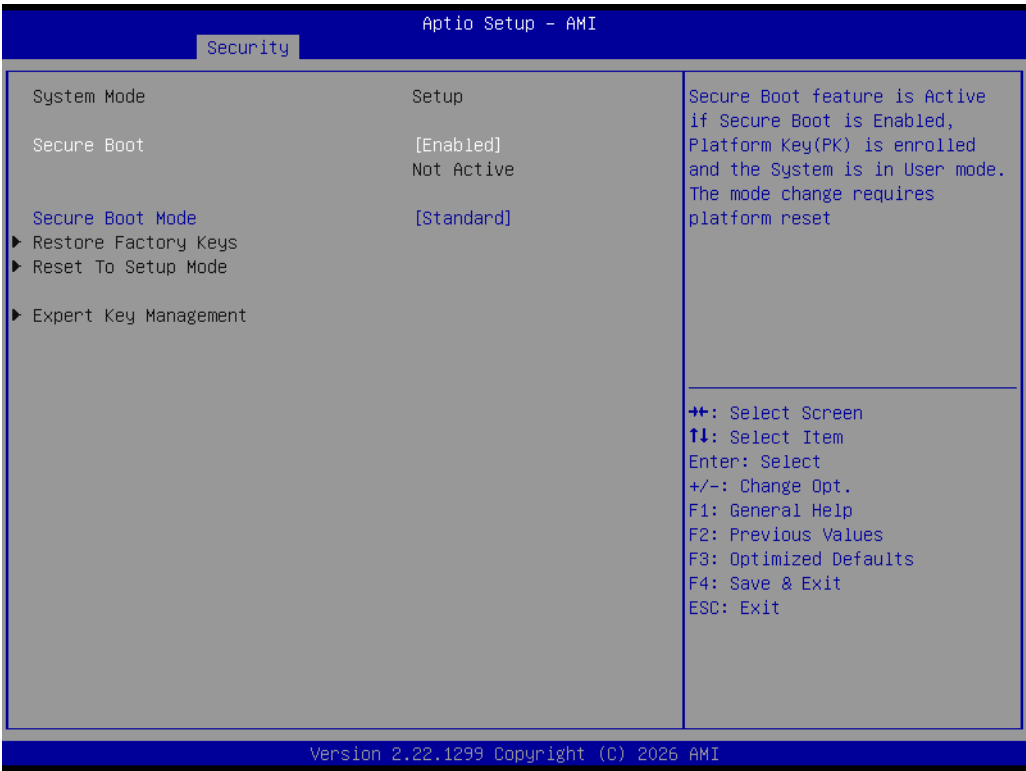


Figure 3.48 Secure Boot

- **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 Boot

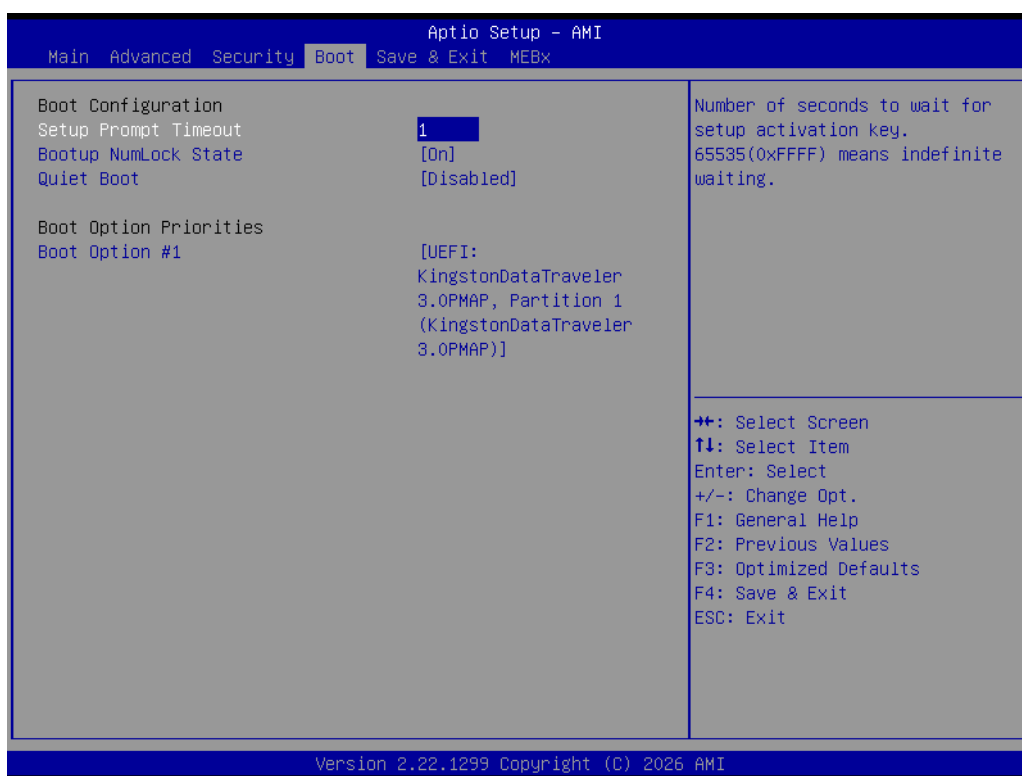


Figure 3.49 Boot Configuration

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

3.7 Save & Exit

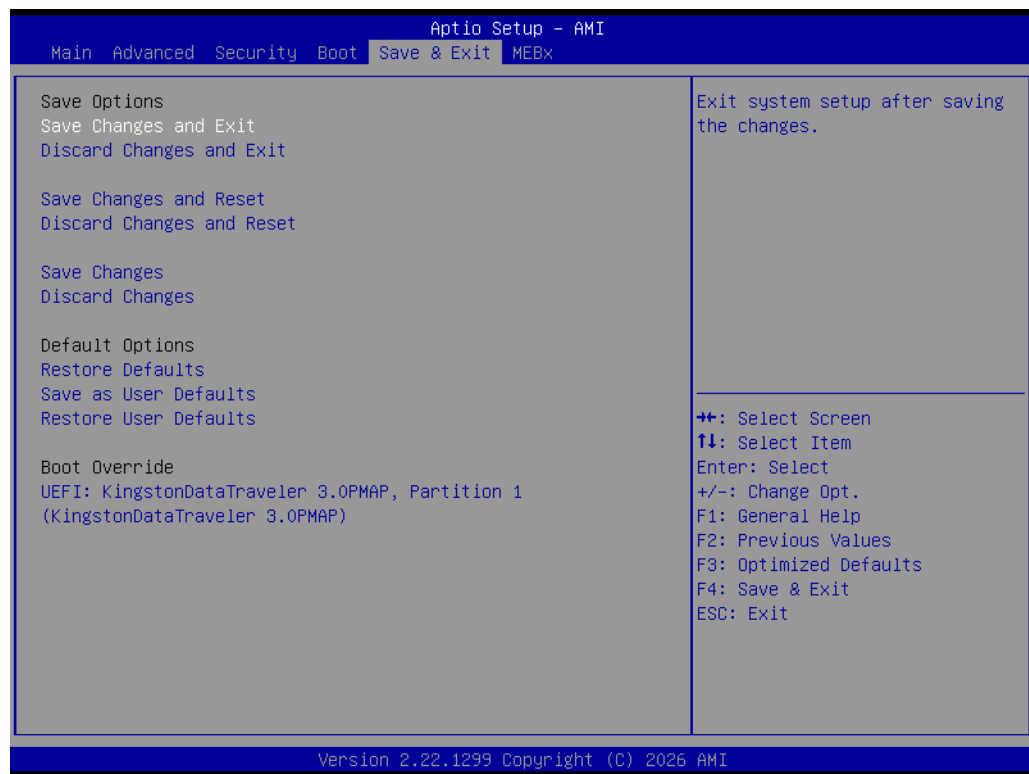


Figure 3.50 Save & Exit

- **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**
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 3.51 MEBx

Chapter 4

S/W Introduction & Installation

Sections include:

- 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 outline to the operating system how the chipset components will be configured.

4.2.1 Windows Driver Setup

To install the drivers on a windows-based OS, please connect to the internet and go to <http://support.advantech.com.tw> to download the drivers that you want to install and follow Driver Setup instructions to complete the installation.

4.2.2 Other OS

Linux Ubuntu

4.3 Advantech iManager

Advantech platforms come equipped with iManager, a micro-controller 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 as they happen. iManager also comes with a secure & encrypted EEPROM for storing important security keys or other customer information. All the embedded functions are configured through the API and provide corresponding utilities to demonstrate. These APIs comply with PICMG EAPI (Embedded Application Programmable Interface) specifications and makes these embedded features easier to integrate, speed development schedules, and provide customer's with software continuity while upgrading hardware. More details of how to use the APIs and utilities, please refer to the Advantech iManager 2.0 Software API User Manual.

Control	Monitor
 GPIO General Purpose Input/Output is a flexible parallel interface that allows a variety of custom connections. It allows users to monitor the level of signal input or set the output status to switch on/off a device. Our API also provides Programmable GPIO, which allows developers to dynamically set the GPIO input or output status.	 Watchdog A watchdog timer (WDT) is a device that performs a specific operation after a certain period of time if something goes wrong and the system does not recover on its own. A watchdog timer can be programmed to perform a warm boot (restarting the system) after a certain number of seconds.
 SMBus SMBus is the System Management Bus defined by Intel® Corporation in 1995. It is used in personal computers and servers for low-speed system management communications. The SMBus API allows a developer to interface an embedded system environment and transfer serial messages using the SMBus protocols, allowing multiple simultaneous device control.	 Hardware Monitor The Hardware Monitor (HWM) API is a system health supervision API that inspects certain condition indexes, such as fan speed, temperature and voltage.
 I2C I2C is a bi-directional two wire bus that was developed by Philips for use in their televisions in the 1980s. The I2C API allows a developer to interface with an embedded system environment and transfer serial messages using the I2C protocols, allowing multiple simultaneous device control.	 Hardware Control The Hardware Control API allows developers to set the PWM (Pulse Width Modulation) value to adjust fan speed or other devices; it can also be used to adjust the LCD brightness.
Display	Power Saving
 Brightness Control The Brightness Control API allows a developer to interface with an embedded device to easily control brightness.	 CPU Speed Make use of Intel SpeedStep technology to reduce power power consumption. The system will automatically adjust the CPU Speed depending on system loading.
 Backlight The Backlight API allows a developer to control the backlight (screen) on/off in an embedded device.	 System Throttling Refers to a series of methods for reducing power consumption in computers by lowering the clock frequency. These APIs allow the user to lower the clock from 87.5% to 12.5%.

Appendix **A**

Pin Assignment

This appendix details information about the hardware pin assignment of the SOM-5886 CPU System on Module.

Sections include:

- SOM-5886 Type 6-Pin Assignment

A.1 SOM-5886 Pin Assignments

This section gives SOM-5886 pin assignment on COM Express connector which compliant with COMR.0 R3.1 Type 6 pin-out definitions. More details about how to use these pins and get design reference, please contact to Advantech for design guide, checklist, reference schematic, and other hardware/software supports.

Table A.1: SOM-5886 Pin Assignments

SOM-5886 Rows A, B			
A1	GND (FIXED)	B1	GND (FIXED)
A2	GBE0_MDI3-	B2	GBE0_ACT#
A3	GBE0_MDI3+	B3	LPC_FRAME#/ESPI_CS0#
A4	GBE0_LINK100#	B4	LPC_AD0/ESPI_IO_0
A5	GBE0_LINK1000#	B5	LPC_AD1/ESPI_IO_1
A6	GBE0_MDI2-	B6	LPC_AD2/ESPI_IO_2
A7	GBE0_MDI2+	B7	LPC_AD3/ESPI_IO_3
A8	GBE0_LINK#	B8	LPC_DRQ0#/ESPI_ALERT0#
A9	GBE0_MDI1-	B9	LPC_DRQ1#/ESPI_ALERT1#
A10	GBE0_MDI1+	B10	LPC_CLK/ESPI_CK
A11	GND (FIXED)	B11	GND (FIXED)
A12	GBE0_MDI0-	B12	PWRBTN#
A13	GBE0_MDI0+	B13	SMB_CK
A14	GBE0_CTREF	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#/ESPI_RESET#
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	HDA_SDIN2/SNDW0_CLK
A29	HDA_SYNC	B29	HDA_SDIN1/SNDW0_DAT
A30	HDA_RST#	B30	HDA_SDIN0
A31	GND (FIXED)	B31	GND (FIXED)
A32	HDA_BITCLK	B32	SPKR
A33	HDA_SDOUT	B33	I2C_CK
A34	BIOS_DIS0#/ESPI_SAFS	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-5886 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	USB0_HOST_PRSENT
A49	GBE0_SDP	B49	SYS_RESET#
A50	LPC_SERIRQ/ESPI_CS1#	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-
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
A87	eDP_HPD	B87	VCC_5V_SBY

Table A.1: SOM-5886 Pin Assignments

A88	PCIE_CLK_REF+	B88	BIOS_DIS1#
A89	PCIE_CLK_REF-	B89	VGA_RED
A90	GND (FIXED)	B90	GND (FIXED)
A91	SPI_POWER	B91	VGA_GRN
A92	SPI_MISO	B92	VGA_BLU
A93	GPO0	B93	VGA_HSYNC
A94	SPI_CLK	B94	VGA_VSYNC
A95	SPI_MOSI	B95	VGA_I2C_CK
A96	TPM_PP	B96	VGA_I2C_DAT
A97	TYPE10#	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-5886 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	USB4_1_LSTX	D15	DDI1_CTRLCLK_AUX+/ USB4_1_AUX+
C16	USB4_1_LSRX	D16	DDI1_CTRLCLK_AUX-/ USB4_1_AUX-
C17	USB4_RT_ENA	D17	USB4_PD_I2C_ALERT#
C18	GND	D18	PMCALERT#
C19	PCIE_RX6+	D19	PCIE_TX6+
C20	PCIE_RX6-	D20	PCIE_TX6-
C21	GND (FIXED)	D21	GND (FIXED)

Table A.1: SOM-5886 Pin Assignments			
C22	PCIE_RX7+	D22	PCIE_TX7+
C23	PCIE_RX7-	D23	PCIE_TX7-
C24	DDI1_HPD	D24	GND
C25	SML0_CLK	D25	GND
C26	SML0_DAT	D26	DDI1_PAIR0+/USB4_1_SSTX0+
C27	SML1_CLK	D27	DDI1_PAIR0-/USB4_1_SSTX0-
C28	SML1_DAT	D28	GND
C29	USB4_PD_I2C_CLK	D29	DDI1_PAIR1+/USB4_1_SSRX0+
C30	USB4_PD_I2C_DAT	D30	DDI1_PAIR1-/USB4_1_SSRX0-
C31	GND (FIXED)	D31	GND (FIXED)
C32	DDI2_CTRLCLK_AUX+/USB4_2_AUX+	D32	DDI1_PAIR2+/USB4_1_SSTX1+
C33	DDI2_CTRLDATA_AUX-/USB4_2_AUX-	D33	DDI1_PAIR2-/USB4_1_SSTX1-
C34	DDI2_DDC_AUX_SEL	D34	DDI1_DDC_AUX_SEL
C35	USB4_2_LSTX	D35	USB4_2_LSRX
C36	DDI3_CTRLCLK_AUX+	D36	DDI1_PAIR3+/USB4_1_SSRX1+
C37	DDI3_CTRLDATA_AUX-	D37	DDI1_PAIR3-/USB4_1_SSRX1-
C38	DDI3_DDC_AUX_SEL	D38	GND
C39	DDI3_PAIR0+	D39	DDI2_PAIR0+/USB4_2_SSTX0+
C40	DDI3_PAIR0-	D40	DDI2_PAIR0-/USB4_2_SSTX0-
C41	GND (FIXED)	D41	GND (FIXED)
C42	DDI3_PAIR1+	D42	DDI2_PAIR1+/USB4_2_SSRX0+
C43	DDI3_PAIR1-	D43	DDI2_PAIR1-/USB4_2_SSRX0-
C44	DDI3_HPD	D44	DDI2_HPD
C45	GP_SPI_CS#	D45	GND
C46	DDI3_PAIR2+	D46	DDI2_PAIR2+/USB4_2_SSTX1+
C47	DDI3_PAIR2-	D47	DDI2_PAIR2-/USB4_2_SSTX1-
C48	RSVD	D48	GND
C49	DDI3_PAIR3+	D49	DDI2_PAIR3+/USB4_2_SSRX1+
C50	DDI3_PAIR3-	D50	DDI2_PAIR3-/USB4_2_SSRX1-
C51	GND (FIXED)	D51	GND (FIXED)
C52	PEG_RX0+	D52	PEG_TX0+
C53	PEG_RX0-	D53	PEG_TX0-
C54	TYPE0#	D54	PEG_LANE_RV#
C55	PEG_RX1+	D55	PEG_TX1+
C56	PEG_RX1-	D56	PEG_TX1-
C57	TYPE1#	D57	TYPE2#
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	RSVD	D63	GND
C64	RSVD	D64	GND
C65	PEG_RX4+	D65	PEG_TX4+
C66	PEG_RX4-	D66	PEG_TX4-

Table A.1: SOM-5886 Pin Assignments

C67	RAPID_SHUTDOWN	D67	GND
C68	PEG_RX5+	D68	PEG_TX5+
C69	PEG_RX5-	D69	PEG_TX5-
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)

Appendix **B**

Watchdog Timer

This appendix gives you the information about the watchdog timer programming on the SOM-5886 CPU System on Module.

Sections include:

- Programming the Watchdog Timer

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	Power button event
Power Off	Support
H/W Restart	Support
WDT Pin Activate	Support

** WDT new driver support automatically select available IRQ number from BIOS, and then set to EC. Only Win8.1 and Win10 support it.

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

Appendix **C**

Programming GPIO

This Appendix details illustration of 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	GPO3

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

Appendix **D**

System Assignments

This appendix gives you the information about the system resource allocation on the SOM-5886 CPU System on Module.

Sections include:

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

D.1 System I/O Ports

Table D.1: System I/O Port

Addr.Range(Hex)	Device
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
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
0x00000062-0x00000062	Microsoft ACPI-Compliant Embedded Controller
0x00000066-0x00000066	Microsoft ACPI-Compliant Embedded Controller
0x00001854-0x00001857	Motherboard resources
0x0000EFA0-0x0000EFBF	Intel(R) SMBus Controller - E322
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
0x000000B4-0x000000B5	Programmable interrupt controller
0x000000B8-0x000000B9	Programmable interrupt controller

Table D.1: System I/O Port

0x000000BC-0x000000BD	Programmable interrupt controller
0x000004D0-0x000004D1	Programmable interrupt controller
0x00000000-0x000000CF7	PCI Express Root Complex
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x000000F0-0x000000F0	Numeric data processor
0x00002000-0x000020FE	Motherboard resources
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer

D.2 Interrupt Assignments

Table D.2: Interrupt Assignments

Interrupt#	Interrupt Source
IRQ 4294967279	Intel(R) NPU
IRQ 4294967284	Intel(R) Platform Monitoring Technology (PMT) Driver
IRQ 4294967278	Intel® Smart Sound Technology BUS
IRQ 17	USB Synopsys Controller
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 4294967294	PCI Express Root Port
IRQ 6	Motherboard resources
IRQ 6	Motherboard resources
IRQ 4294967283	Intel(R) Graphics
IRQ 4294967281	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 14	Intel(R) Serial IO Generic GPIO Host Controller
IRQ 14	Intel(R) Serial IO Generic GPIO Host Controller
IRQ 14	Intel(R) Serial IO Generic GPIO Host Controller
IRQ 14	Intel(R) Serial IO Generic GPIO Host Controller
IRQ 14	Intel(R) Serial IO Generic GPIO Host Controller
IRQ 55	Microsoft ACPI-Compliant System
IRQ 56	Microsoft ACPI-Compliant System
IRQ 57	Microsoft ACPI-Compliant System
IRQ 58	Microsoft ACPI-Compliant System
IRQ 59	Microsoft ACPI-Compliant System
IRQ 60	Microsoft ACPI-Compliant System
IRQ 61	Microsoft ACPI-Compliant System
IRQ 62	Microsoft ACPI-Compliant System
IRQ 63	Microsoft ACPI-Compliant System
IRQ 64	Microsoft ACPI-Compliant System
IRQ 65	Microsoft ACPI-Compliant System
IRQ 66	Microsoft ACPI-Compliant System
IRQ 67	Microsoft ACPI-Compliant System
IRQ 68	Microsoft ACPI-Compliant System
IRQ 69	Microsoft ACPI-Compliant System
IRQ 70	Microsoft ACPI-Compliant System
IRQ 71	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 72	Microsoft ACPI-Compliant System
IRQ 73	Microsoft ACPI-Compliant System
IRQ 74	Microsoft ACPI-Compliant System
IRQ 75	Microsoft ACPI-Compliant System
IRQ 76	Microsoft ACPI-Compliant System
IRQ 77	Microsoft ACPI-Compliant System
IRQ 78	Microsoft ACPI-Compliant System
IRQ 79	Microsoft ACPI-Compliant System
IRQ 80	Microsoft ACPI-Compliant System
IRQ 81	Microsoft ACPI-Compliant System
IRQ 82	Microsoft ACPI-Compliant System
IRQ 83	Microsoft ACPI-Compliant System
IRQ 84	Microsoft ACPI-Compliant System
IRQ 85	Microsoft ACPI-Compliant System
IRQ 86	Microsoft ACPI-Compliant System
IRQ 87	Microsoft ACPI-Compliant System
IRQ 88	Microsoft ACPI-Compliant System
IRQ 88	Trusted Platform Module 2.0
IRQ 89	Microsoft ACPI-Compliant System
IRQ 90	Microsoft ACPI-Compliant System
IRQ 91	Microsoft ACPI-Compliant System
IRQ 92	Microsoft ACPI-Compliant System
IRQ 93	Microsoft ACPI-Compliant System
IRQ 94	Microsoft ACPI-Compliant System
IRQ 95	Microsoft ACPI-Compliant System
IRQ 96	Microsoft ACPI-Compliant System
IRQ 97	Microsoft ACPI-Compliant System
IRQ 98	Microsoft ACPI-Compliant System
IRQ 99	Microsoft ACPI-Compliant System
IRQ 100	Microsoft ACPI-Compliant System
IRQ 101	Microsoft ACPI-Compliant System
IRQ 102	Microsoft ACPI-Compliant System
IRQ 103	Microsoft ACPI-Compliant System
IRQ 104	Microsoft ACPI-Compliant System
IRQ 105	Microsoft ACPI-Compliant System
IRQ 106	Microsoft ACPI-Compliant System
IRQ 107	Microsoft ACPI-Compliant System
IRQ 108	Microsoft ACPI-Compliant System
IRQ 109	Microsoft ACPI-Compliant System
IRQ 110	Microsoft ACPI-Compliant System
IRQ 111	Microsoft ACPI-Compliant System
IRQ 112	Microsoft ACPI-Compliant System
IRQ 113	Microsoft ACPI-Compliant System
IRQ 114	Microsoft ACPI-Compliant System
IRQ 115	Microsoft ACPI-Compliant System
IRQ 116	Microsoft ACPI-Compliant System
IRQ 117	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 118	Microsoft ACPI-Compliant System
IRQ 119	Microsoft ACPI-Compliant System
IRQ 120	Microsoft ACPI-Compliant System
IRQ 121	Microsoft ACPI-Compliant System
IRQ 122	Microsoft ACPI-Compliant System
IRQ 123	Microsoft ACPI-Compliant System
IRQ 124	Microsoft ACPI-Compliant System
IRQ 125	Microsoft ACPI-Compliant System
IRQ 126	Microsoft ACPI-Compliant System
IRQ 127	Microsoft ACPI-Compliant System
IRQ 128	Microsoft ACPI-Compliant System
IRQ 129	Microsoft ACPI-Compliant System
IRQ 130	Microsoft ACPI-Compliant System
IRQ 131	Microsoft ACPI-Compliant System
IRQ 132	Microsoft ACPI-Compliant System
IRQ 133	Microsoft ACPI-Compliant System
IRQ 134	Microsoft ACPI-Compliant System
IRQ 135	Microsoft ACPI-Compliant System
IRQ 136	Microsoft ACPI-Compliant System
IRQ 137	Microsoft ACPI-Compliant System
IRQ 138	Microsoft ACPI-Compliant System
IRQ 139	Microsoft ACPI-Compliant System
IRQ 140	Microsoft ACPI-Compliant System
IRQ 141	Microsoft ACPI-Compliant System
IRQ 142	Microsoft ACPI-Compliant System
IRQ 143	Microsoft ACPI-Compliant System
IRQ 144	Microsoft ACPI-Compliant System
IRQ 145	Microsoft ACPI-Compliant System
IRQ 146	Microsoft ACPI-Compliant System
IRQ 147	Microsoft ACPI-Compliant System
IRQ 148	Microsoft ACPI-Compliant System
IRQ 149	Microsoft ACPI-Compliant System
IRQ 150	Microsoft ACPI-Compliant System
IRQ 151	Microsoft ACPI-Compliant System
IRQ 152	Microsoft ACPI-Compliant System
IRQ 153	Microsoft ACPI-Compliant System
IRQ 154	Microsoft ACPI-Compliant System
IRQ 155	Microsoft ACPI-Compliant System
IRQ 156	Microsoft ACPI-Compliant System
IRQ 157	Microsoft ACPI-Compliant System
IRQ 158	Microsoft ACPI-Compliant System
IRQ 159	Microsoft ACPI-Compliant System
IRQ 160	Microsoft ACPI-Compliant System
IRQ 161	Microsoft ACPI-Compliant System
IRQ 162	Microsoft ACPI-Compliant System
IRQ 163	Microsoft ACPI-Compliant System
IRQ 164	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 165	Microsoft ACPI-Compliant System
IRQ 166	Microsoft ACPI-Compliant System
IRQ 167	Microsoft ACPI-Compliant System
IRQ 168	Microsoft ACPI-Compliant System
IRQ 169	Microsoft ACPI-Compliant System
IRQ 170	Microsoft ACPI-Compliant System
IRQ 171	Microsoft ACPI-Compliant System
IRQ 172	Microsoft ACPI-Compliant System
IRQ 173	Microsoft ACPI-Compliant System
IRQ 174	Microsoft ACPI-Compliant System
IRQ 175	Microsoft ACPI-Compliant System
IRQ 176	Microsoft ACPI-Compliant System
IRQ 177	Microsoft ACPI-Compliant System
IRQ 178	Microsoft ACPI-Compliant System
IRQ 179	Microsoft ACPI-Compliant System
IRQ 180	Microsoft ACPI-Compliant System
IRQ 181	Microsoft ACPI-Compliant System
IRQ 182	Microsoft ACPI-Compliant System
IRQ 183	Microsoft ACPI-Compliant System
IRQ 184	Microsoft ACPI-Compliant System
IRQ 185	Microsoft ACPI-Compliant System
IRQ 186	Microsoft ACPI-Compliant System
IRQ 187	Microsoft ACPI-Compliant System
IRQ 188	Microsoft ACPI-Compliant System
IRQ 189	Microsoft ACPI-Compliant System
IRQ 190	Microsoft ACPI-Compliant System
IRQ 191	Microsoft ACPI-Compliant System
IRQ 192	Microsoft ACPI-Compliant System
IRQ 193	Microsoft ACPI-Compliant System
IRQ 194	Microsoft ACPI-Compliant System
IRQ 195	Microsoft ACPI-Compliant System
IRQ 196	Microsoft ACPI-Compliant System
IRQ 197	Microsoft ACPI-Compliant System
IRQ 198	Microsoft ACPI-Compliant System
IRQ 199	Microsoft ACPI-Compliant System
IRQ 200	Microsoft ACPI-Compliant System
IRQ 201	Microsoft ACPI-Compliant System
IRQ 202	Microsoft ACPI-Compliant System
IRQ 203	Microsoft ACPI-Compliant System
IRQ 204	Microsoft ACPI-Compliant System
IRQ 256	Microsoft ACPI-Compliant System
IRQ 257	Microsoft ACPI-Compliant System
IRQ 258	Microsoft ACPI-Compliant System
IRQ 259	Microsoft ACPI-Compliant System
IRQ 260	Microsoft ACPI-Compliant System
IRQ 261	Microsoft ACPI-Compliant System
IRQ 262	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 263	Microsoft ACPI-Compliant System
IRQ 264	Microsoft ACPI-Compliant System
IRQ 265	Microsoft ACPI-Compliant System
IRQ 266	Microsoft ACPI-Compliant System
IRQ 267	Microsoft ACPI-Compliant System
IRQ 268	Microsoft ACPI-Compliant System
IRQ 269	Microsoft ACPI-Compliant System
IRQ 270	Microsoft ACPI-Compliant System
IRQ 271	Microsoft ACPI-Compliant System
IRQ 272	Microsoft ACPI-Compliant System
IRQ 273	Microsoft ACPI-Compliant System
IRQ 274	Microsoft ACPI-Compliant System
IRQ 275	Microsoft ACPI-Compliant System
IRQ 276	Microsoft ACPI-Compliant System
IRQ 277	Microsoft ACPI-Compliant System
IRQ 278	Microsoft ACPI-Compliant System
IRQ 279	Microsoft ACPI-Compliant System
IRQ 280	Microsoft ACPI-Compliant System
IRQ 281	Microsoft ACPI-Compliant System
IRQ 282	Microsoft ACPI-Compliant System
IRQ 283	Microsoft ACPI-Compliant System
IRQ 284	Microsoft ACPI-Compliant System
IRQ 285	Microsoft ACPI-Compliant System
IRQ 286	Microsoft ACPI-Compliant System
IRQ 287	Microsoft ACPI-Compliant System
IRQ 288	Microsoft ACPI-Compliant System
IRQ 289	Microsoft ACPI-Compliant System
IRQ 290	Microsoft ACPI-Compliant System
IRQ 291	Microsoft ACPI-Compliant System
IRQ 292	Microsoft ACPI-Compliant System
IRQ 293	Microsoft ACPI-Compliant System
IRQ 294	Microsoft ACPI-Compliant System
IRQ 295	Microsoft ACPI-Compliant System
IRQ 296	Microsoft ACPI-Compliant System
IRQ 297	Microsoft ACPI-Compliant System
IRQ 298	Microsoft ACPI-Compliant System
IRQ 299	Microsoft ACPI-Compliant System
IRQ 300	Microsoft ACPI-Compliant System
IRQ 301	Microsoft ACPI-Compliant System
IRQ 302	Microsoft ACPI-Compliant System
IRQ 303	Microsoft ACPI-Compliant System
IRQ 304	Microsoft ACPI-Compliant System
IRQ 305	Microsoft ACPI-Compliant System
IRQ 306	Microsoft ACPI-Compliant System
IRQ 307	Microsoft ACPI-Compliant System
IRQ 308	Microsoft ACPI-Compliant System
IRQ 309	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 310	Microsoft ACPI-Compliant System
IRQ 311	Microsoft ACPI-Compliant System
IRQ 312	Microsoft ACPI-Compliant System
IRQ 313	Microsoft ACPI-Compliant System
IRQ 314	Microsoft ACPI-Compliant System
IRQ 315	Microsoft ACPI-Compliant System
IRQ 316	Microsoft ACPI-Compliant System
IRQ 317	Microsoft ACPI-Compliant System
IRQ 318	Microsoft ACPI-Compliant System
IRQ 319	Microsoft ACPI-Compliant System
IRQ 320	Microsoft ACPI-Compliant System
IRQ 321	Microsoft ACPI-Compliant System
IRQ 322	Microsoft ACPI-Compliant System
IRQ 323	Microsoft ACPI-Compliant System
IRQ 324	Microsoft ACPI-Compliant System
IRQ 325	Microsoft ACPI-Compliant System
IRQ 326	Microsoft ACPI-Compliant System
IRQ 327	Microsoft ACPI-Compliant System
IRQ 328	Microsoft ACPI-Compliant System
IRQ 329	Microsoft ACPI-Compliant System
IRQ 330	Microsoft ACPI-Compliant System
IRQ 331	Microsoft ACPI-Compliant System
IRQ 332	Microsoft ACPI-Compliant System
IRQ 333	Microsoft ACPI-Compliant System
IRQ 334	Microsoft ACPI-Compliant System
IRQ 335	Microsoft ACPI-Compliant System
IRQ 336	Microsoft ACPI-Compliant System
IRQ 337	Microsoft ACPI-Compliant System
IRQ 338	Microsoft ACPI-Compliant System
IRQ 339	Microsoft ACPI-Compliant System
IRQ 340	Microsoft ACPI-Compliant System
IRQ 341	Microsoft ACPI-Compliant System
IRQ 342	Microsoft ACPI-Compliant System
IRQ 343	Microsoft ACPI-Compliant System
IRQ 344	Microsoft ACPI-Compliant System
IRQ 345	Microsoft ACPI-Compliant System
IRQ 346	Microsoft ACPI-Compliant System
IRQ 347	Microsoft ACPI-Compliant System
IRQ 348	Microsoft ACPI-Compliant System
IRQ 349	Microsoft ACPI-Compliant System
IRQ 350	Microsoft ACPI-Compliant System
IRQ 351	Microsoft ACPI-Compliant System
IRQ 352	Microsoft ACPI-Compliant System
IRQ 353	Microsoft ACPI-Compliant System
IRQ 354	Microsoft ACPI-Compliant System
IRQ 355	Microsoft ACPI-Compliant System
IRQ 356	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 357	Microsoft ACPI-Compliant System
IRQ 358	Microsoft ACPI-Compliant System
IRQ 359	Microsoft ACPI-Compliant System
IRQ 360	Microsoft ACPI-Compliant System
IRQ 361	Microsoft ACPI-Compliant System
IRQ 362	Microsoft ACPI-Compliant System
IRQ 363	Microsoft ACPI-Compliant System
IRQ 364	Microsoft ACPI-Compliant System
IRQ 365	Microsoft ACPI-Compliant System
IRQ 366	Microsoft ACPI-Compliant System
IRQ 367	Microsoft ACPI-Compliant System
IRQ 368	Microsoft ACPI-Compliant System
IRQ 369	Microsoft ACPI-Compliant System
IRQ 370	Microsoft ACPI-Compliant System
IRQ 371	Microsoft ACPI-Compliant System
IRQ 372	Microsoft ACPI-Compliant System
IRQ 373	Microsoft ACPI-Compliant System
IRQ 374	Microsoft ACPI-Compliant System
IRQ 375	Microsoft ACPI-Compliant System
IRQ 376	Microsoft ACPI-Compliant System
IRQ 377	Microsoft ACPI-Compliant System
IRQ 378	Microsoft ACPI-Compliant System
IRQ 379	Microsoft ACPI-Compliant System
IRQ 380	Microsoft ACPI-Compliant System
IRQ 381	Microsoft ACPI-Compliant System
IRQ 382	Microsoft ACPI-Compliant System
IRQ 383	Microsoft ACPI-Compliant System
IRQ 384	Microsoft ACPI-Compliant System
IRQ 385	Microsoft ACPI-Compliant System
IRQ 386	Microsoft ACPI-Compliant System
IRQ 387	Microsoft ACPI-Compliant System
IRQ 388	Microsoft ACPI-Compliant System
IRQ 389	Microsoft ACPI-Compliant System
IRQ 390	Microsoft ACPI-Compliant System
IRQ 391	Microsoft ACPI-Compliant System
IRQ 392	Microsoft ACPI-Compliant System
IRQ 393	Microsoft ACPI-Compliant System
IRQ 394	Microsoft ACPI-Compliant System
IRQ 395	Microsoft ACPI-Compliant System
IRQ 396	Microsoft ACPI-Compliant System
IRQ 397	Microsoft ACPI-Compliant System
IRQ 398	Microsoft ACPI-Compliant System
IRQ 399	Microsoft ACPI-Compliant System
IRQ 400	Microsoft ACPI-Compliant System
IRQ 401	Microsoft ACPI-Compliant System
IRQ 402	Microsoft ACPI-Compliant System
IRQ 403	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 404	Microsoft ACPI-Compliant System
IRQ 405	Microsoft ACPI-Compliant System
IRQ 406	Microsoft ACPI-Compliant System
IRQ 407	Microsoft ACPI-Compliant System
IRQ 408	Microsoft ACPI-Compliant System
IRQ 409	Microsoft ACPI-Compliant System
IRQ 410	Microsoft ACPI-Compliant System
IRQ 411	Microsoft ACPI-Compliant System
IRQ 412	Microsoft ACPI-Compliant System
IRQ 413	Microsoft ACPI-Compliant System
IRQ 414	Microsoft ACPI-Compliant System
IRQ 415	Microsoft ACPI-Compliant System
IRQ 416	Microsoft ACPI-Compliant System
IRQ 417	Microsoft ACPI-Compliant System
IRQ 418	Microsoft ACPI-Compliant System
IRQ 419	Microsoft ACPI-Compliant System
IRQ 420	Microsoft ACPI-Compliant System
IRQ 421	Microsoft ACPI-Compliant System
IRQ 422	Microsoft ACPI-Compliant System
IRQ 423	Microsoft ACPI-Compliant System
IRQ 424	Microsoft ACPI-Compliant System
IRQ 425	Microsoft ACPI-Compliant System
IRQ 426	Microsoft ACPI-Compliant System
IRQ 427	Microsoft ACPI-Compliant System
IRQ 428	Microsoft ACPI-Compliant System
IRQ 429	Microsoft ACPI-Compliant System
IRQ 430	Microsoft ACPI-Compliant System
IRQ 431	Microsoft ACPI-Compliant System
IRQ 432	Microsoft ACPI-Compliant System
IRQ 433	Microsoft ACPI-Compliant System
IRQ 434	Microsoft ACPI-Compliant System
IRQ 435	Microsoft ACPI-Compliant System
IRQ 436	Microsoft ACPI-Compliant System
IRQ 437	Microsoft ACPI-Compliant System
IRQ 438	Microsoft ACPI-Compliant System
IRQ 439	Microsoft ACPI-Compliant System
IRQ 440	Microsoft ACPI-Compliant System
IRQ 441	Microsoft ACPI-Compliant System
IRQ 442	Microsoft ACPI-Compliant System
IRQ 443	Microsoft ACPI-Compliant System
IRQ 444	Microsoft ACPI-Compliant System
IRQ 445	Microsoft ACPI-Compliant System
IRQ 446	Microsoft ACPI-Compliant System
IRQ 447	Microsoft ACPI-Compliant System
IRQ 448	Microsoft ACPI-Compliant System
IRQ 449	Microsoft ACPI-Compliant System
IRQ 450	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 451	Microsoft ACPI-Compliant System
IRQ 452	Microsoft ACPI-Compliant System
IRQ 453	Microsoft ACPI-Compliant System
IRQ 454	Microsoft ACPI-Compliant System
IRQ 455	Microsoft ACPI-Compliant System
IRQ 456	Microsoft ACPI-Compliant System
IRQ 457	Microsoft ACPI-Compliant System
IRQ 458	Microsoft ACPI-Compliant System
IRQ 459	Microsoft ACPI-Compliant System
IRQ 460	Microsoft ACPI-Compliant System
IRQ 461	Microsoft ACPI-Compliant System
IRQ 462	Microsoft ACPI-Compliant System
IRQ 463	Microsoft ACPI-Compliant System
IRQ 464	Microsoft ACPI-Compliant System
IRQ 465	Microsoft ACPI-Compliant System
IRQ 466	Microsoft ACPI-Compliant System
IRQ 467	Microsoft ACPI-Compliant System
IRQ 468	Microsoft ACPI-Compliant System
IRQ 469	Microsoft ACPI-Compliant System
IRQ 470	Microsoft ACPI-Compliant System
IRQ 471	Microsoft ACPI-Compliant System
IRQ 472	Microsoft ACPI-Compliant System
IRQ 473	Microsoft ACPI-Compliant System
IRQ 474	Microsoft ACPI-Compliant System
IRQ 475	Microsoft ACPI-Compliant System
IRQ 476	Microsoft ACPI-Compliant System
IRQ 477	Microsoft ACPI-Compliant System
IRQ 478	Microsoft ACPI-Compliant System
IRQ 479	Microsoft ACPI-Compliant System
IRQ 480	Microsoft ACPI-Compliant System
IRQ 481	Microsoft ACPI-Compliant System
IRQ 482	Microsoft ACPI-Compliant System
IRQ 483	Microsoft ACPI-Compliant System
IRQ 484	Microsoft ACPI-Compliant System
IRQ 485	Microsoft ACPI-Compliant System
IRQ 486	Microsoft ACPI-Compliant System
IRQ 487	Microsoft ACPI-Compliant System
IRQ 488	Microsoft ACPI-Compliant System
IRQ 489	Microsoft ACPI-Compliant System
IRQ 490	Microsoft ACPI-Compliant System
IRQ 491	Microsoft ACPI-Compliant System
IRQ 492	Microsoft ACPI-Compliant System
IRQ 493	Microsoft ACPI-Compliant System
IRQ 494	Microsoft ACPI-Compliant System
IRQ 495	Microsoft ACPI-Compliant System
IRQ 496	Microsoft ACPI-Compliant System
IRQ 497	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 498	Microsoft ACPI-Compliant System
IRQ 499	Microsoft ACPI-Compliant System
IRQ 500	Microsoft ACPI-Compliant System
IRQ 501	Microsoft ACPI-Compliant System
IRQ 502	Microsoft ACPI-Compliant System
IRQ 503	Microsoft ACPI-Compliant System
IRQ 504	Microsoft ACPI-Compliant System
IRQ 505	Microsoft ACPI-Compliant System
IRQ 506	Microsoft ACPI-Compliant System
IRQ 507	Microsoft ACPI-Compliant System
IRQ 508	Microsoft ACPI-Compliant System
IRQ 509	Microsoft ACPI-Compliant System
IRQ 510	Microsoft ACPI-Compliant System
IRQ 511	Microsoft ACPI-Compliant System
IRQ 13	Numeric data processor
IRQ 4294967277	Intel(R) Silicon Security Engine Interface
IRQ 4294967293	Standard NVM Express Controller
IRQ 4294967292	Standard NVM Express Controller
IRQ 4294967291	Standard NVM Express Controller
IRQ 4294967290	Standard NVM Express Controller
IRQ 4294967289	Standard NVM Express Controller
IRQ 4294967288	Standard NVM Express Controller
IRQ 4294967287	Standard NVM Express Controller
IRQ 4294967286	Standard NVM Express Controller
IRQ 4294967285	Standard NVM Express Controller
IRQ 4294967282	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967280	Intel(R) Management Engine Interface #1
IRQ 0	System timer
IRQ 27	Intel(R) Serial IO I2C Host Controller - E378

D.3 1st MB Memory Map

Table D.3: 1st MB Memory Map

Addr. Range (Hex)	Device
0x00000000FEDC0000-0x00000000FEDC7FFF	Motherboard resources
0x00000000FA000000-0x00000000FA000FFF	Motherboard resources
0x0000000000000000-0x0000000000000FFF	Motherboard resources
0x00000000E0000000-0x00000000FFFFFF	Motherboard resources
0x00000000FED20000-0x00000000FED7FFFF	Motherboard resources
0x00000000FC800000-0x00000000FC81FFFF	Motherboard resources
0x00000000FED45000-0x00000000FED8FFFF	Motherboard resources
0x00000000FEE00000-0x00000000FEEFFFFF	Motherboard resources
0x0000000062056000-0x0000000062065FFF	Motherboard resources
0x000003FFFFC00000-0x000003FFFDFFFFFF	Intel(R) NPU
0x000003FFFFFEF000-0x000003FFFFFEFFFF	Intel(R) NPU

Table D.3: 1st MB Memory Map

0x000003FFFFFF0000-0x000003FFFFFFFFFFFF	Intel(R) Platform Monitoring Technology (PMT) Driver
0x000003FFFFFF0000-0x000003FFFFFF7FFFF	Intel® Smart Sound Technology BUS
0x000003FFFFFFC00000-0x000003FFFFDFFFFFFF	Intel® Smart Sound Technology BUS
0x00000100144B8000-0x00000100144B80FF	Intel(R) SMBus Controller - E322
0x000003FFFFFA00000-0x000003FFFFBFFFFFFF	USB Synopsys Controller
0x000003FFFFFED000-0x000003FFFFFEDFFF	USB Synopsys Controller
0x00000000FED00000-0x00000000FED003FF	High precision event timer
0x0000000080A00000-0x0000000080AFFFFF	PCI Express Root Port
0x0000000080A00000-0x0000000080AFFFFF	Standard NVM Express Controller
0x0000010010000000-0x0000010010FFFFFF	Intel(R) Graphics
0x0000010000000000-0x0000010000FFFFFF	Intel(R) Graphics
0x000000000000A0000-0x000000000000BFFFFF	PCI Express Root Complex
0x0000000080800000-0x00000000DFFFFFFF	PCI Express Root Complex
0x0000010014480000-0x000001001448FFFF	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
0x0000004000590000-0x000000400059FFFF	Intel(R) Serial IO Generic GPIO Host Controller
0x00000040005A0000-0x00000040005AFFFF	Intel(R) Serial IO Generic GPIO Host Controller
0x00000040005B0000-0x00000040005BFFFF	Intel(R) Serial IO Generic GPIO Host Controller
0x00000040005C0000-0x00000040005CFFFF	Intel(R) Serial IO Generic GPIO Host Controller
0x00000040005D0000-0x00000040005DFFFF	Intel(R) Serial IO Generic GPIO Host Controller
0x00000000FED40000-0x00000000FED44FFF	Trusted Platform Module 2.0
0x000003FFFFFEE000-0x000003FFFFFEEFFF	Intel(R) Silicon Security Engine Interface
0x00000000FE010000-0x00000000FE010FFF	Intel(R) SPI (flash) Controller - E323
0x0000010014490000-0x000001001449FFFF	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
0x00000100144BA000-0x00000100144BAFFF	Intel(R) Management Engine Interface #1
0x000003FFFFFEC000-0x000003FFFFFECFFF	Intel(R) Serial IO I2C Host Controller - E378
0x00000000FEDC0000-0x00000000FEDC7FFF	Motherboard resources
0x00000000FA000000-0x00000000FA000FFF	Motherboard resources
0x0000000000000000-0x00000000000000FF	Motherboard resources
0x00000000E0000000-0x00000000EFFFFFFF	Motherboard resources
0x00000000FED20000-0x00000000FED7FFFF	Motherboard resources



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