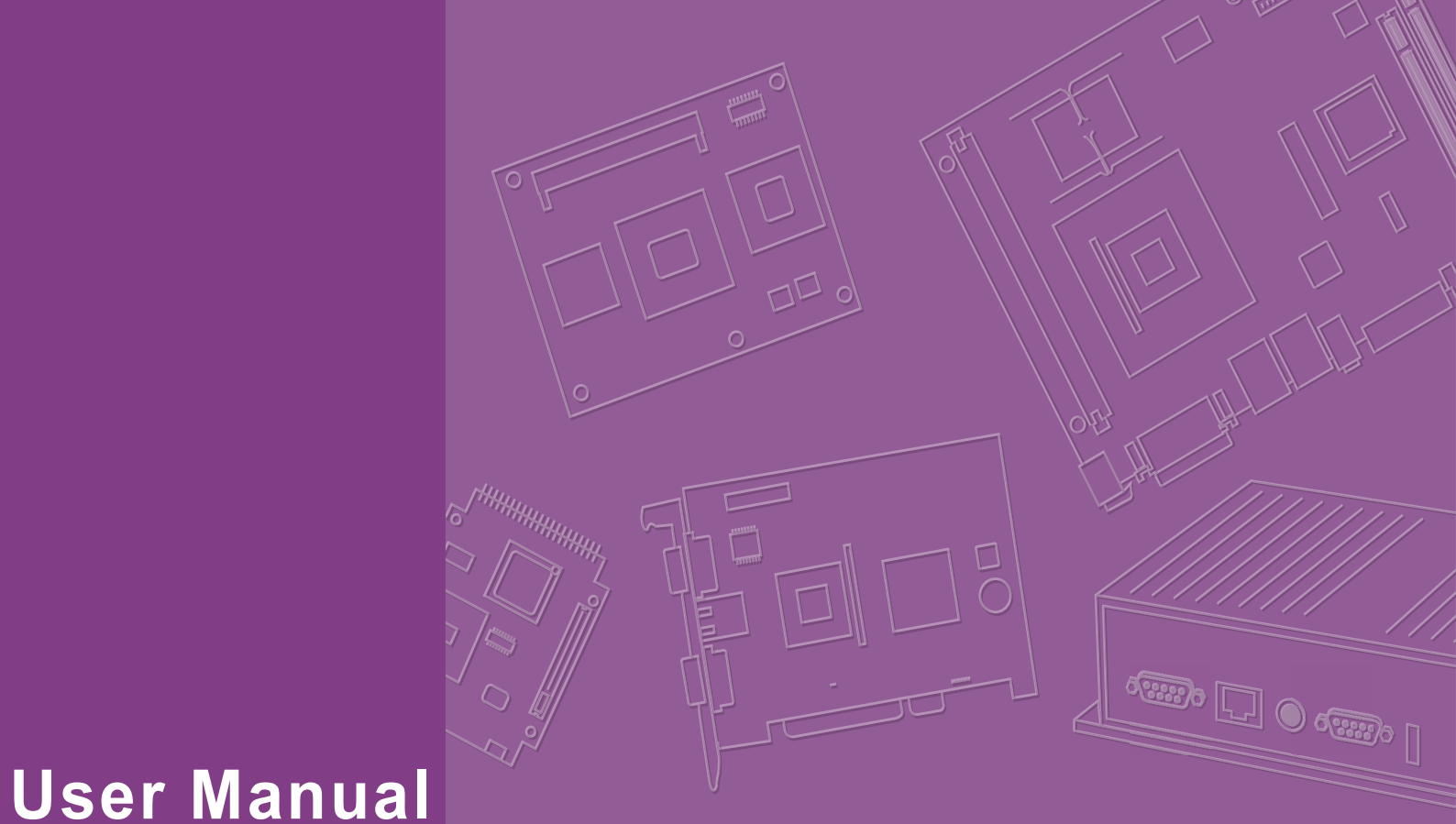




User Manual

SOM-5993

CPU Computer on 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 when shielded cables are used for external wiring. We recommend the use of shielded cables. This type of cable is available from Advantech. Please contact your local supplier for ordering information.

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

FCC Class B

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

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

FM

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

Technical Support and Assistance

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

Warnings, Cautions, and Notes

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



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



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

Note! Notes provide additional optional information.



Document Feedback

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

Selection Guide w/ P/N

Part No.	CPU	Cores	Freq.	CPU TDP	LLC	DDR4 SODIMM	Giga LAN	10G Base-KR	PEG X16	PEG X8	PEG X1	USB 2.0	USB 3.0	SATA III	LPC	Power	Thermal Solution	Operating Temp.
SOM-5993D10-U0A1	D-1746TE-R	10	2.0G	67W	15MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C
SOM-5993D8-U2A1	D-1735TR	8	2.2G	59W	15MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C
SOM-5993D8-S9A1	D-1732TE	8	1.9G	25W	15MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C
SOM-5993D4-U4A1	D-1715TE-R	4	2.4G	50W	10MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C
SOM-5993D4-U0A1	D-1712TR	4	2.0G	40W	10MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C
SOM-5993D10X-U0A1	D-1746TE-R	10	2.0G	67W	15MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	-40 ~ 85°C
SOM-5993D8X-S9A1	D-1732TE	8	1.9G	52W	15MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	-40 ~ 85°C
SOM-5993D4X-U4A1	D-1715TE-R	4	2.4G	50W	10MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	-40 ~ 85°C
SOM-5993D4-U2A1	D-1713NT	4	2.2G	45W	10MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C
SOM-5993RD4-U2A1	D-1813NT	4	2.2G	42W	10MB	ECC/non ECC	1	4	1	1	4	4	4	2	Yes	AT/ATX	Active	0 ~ 60°C

Packing List

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

Part No.	Description	Quantity
-	SOM-5993 Module	1
1970005371T001	Standard Heatspreader	1

Development Board

Part No.	Description
SOM-DB5920-01A2	COMe Type 7 Devel.. Board Rev.A2 w/10G PHY EA64 (4-port, Copper)
SOM-DB5920-F1A2	COMe Type 7 Devel. Board Rev.A2 w/10G PHY EA65 (4-port, Fiber)

Optional Accessories

Part No.	Description
1970005036T001	Semi-Cooler 125 x 95 x 33 mm with 12V Fan
1970005514T001	QFCS

Safety Precaution - Static Electricity

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

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

Safety Instructions

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

	Table 1.1: Acronyms.....	2
1.1	Introduction	3
1.2	Functional Block Diagram	4
1.3	Product Specifications.....	5
1.3.1	Compliance	5
1.3.2	Feature List.....	5
	Table 1.2: Feature List.....	5
1.3.3	Processor System.....	6
	Table 1.3: Processor System	6
1.3.4	Memory	7
1.3.5	Graphics/Audio	7
1.3.6	Expansion Interface	7
	Table 1.4: PCIe x16 [31:16]	7
	Table 1.5: PCIe x8, [7:0].....	8
	Table 1.6: PCIe x8, [15:8].....	8
1.3.7	LPC	8
1.3.8	Serial Bus.....	9
1.3.9	I/O	9
	Table 1.7: USB 3.0	9
	Table 1.8: USB 2.0	9
	Table 1.9: BIOS	10
	Table 1.10: Clear CMOS	10
1.3.10	Power Management.....	11
1.3.11	Environment.....	12
1.3.12	MTBF	12
1.3.13	OS Support (duplicate with SW chapter)	12
1.3.14	Advantech iManager	12
1.3.15	Power Consumption.....	13
	Table 1.11: Power Consumption Table (Watts).....	13
1.3.16	Performance	13
1.3.17	Pin Definitions	13

Chapter 2 Mechanical Information 15

2.1	Board Information.....	16
	Figure 2.1 Board Chip Identification – Front	16
	Figure 2.2 Board Chip Identification – Back	16
2.1.1	Connector List.....	17
	Table 2.1: FAN1 Fan	17
2.2	Mechanical Diagram	17
	Figure 2.3 Board Mechanical Diagram — Front	17
	Figure 2.4 Board Mechanical Diagram – Back	18
	Figure 2.5 Board Mechanical Diagram – Side	18
2.3	Assembly Diagram	19
	Figure 2.6 Assembly Diagram	19
2.4	Assembly Diagram	20
	Figure 2.7 Main Chip Height and Tolerances	20

Chapter 3 AMI BIOS 21

3.1	Introduction	22
	Figure 3.1 Setup Program Initial Screen.....	22

3.2	Entering the Setup	23
3.3	Main Setup	23
	Figure 3.2 Main Setup Screen	23
3.4	Advanced BIOS Features Setup	24
	Figure 3.3 Advanced BIOS Features Setup Screen	24
3.4.1	Trusted Computing	25
	Figure 3.4 Trusted Computing	25
3.4.2	ACPI Settings	26
	Figure 3.5 ACPI Settings	26
3.4.3	Embedded Controller	27
	Figure 3.6 Embedded Controller	27
	Figure 3.7 Serial Port 1 Configuration	28
	Figure 3.8 Serial Port 2 Configuration	29
	Figure 3.9 Hardware Monitor	30
3.4.4	Serial Port Console Redirection	31
	Figure 3.10 Serial Port Console Redirection	31
	Figure 3.11 Console Redirection Settings	32
3.4.5	PCI Subsystem Settings	33
	Figure 3.12 PCI Subsystem Settings	33
	Figure 3.13 PCI Express Settings	34
	Figure 3.14 PCI Express GEN 2 Settings	35
3.4.6	USB Configuration	37
	Figure 3.15 USB Configuration	37
3.4.7	Network Stack Configuration	38
	Figure 3.16 Network Stack Configuration	38
3.4.8	NVMe Configuration	38
	Figure 3.17 NVMe Configuration	38
3.5	Chipset	39
	Figure 3.18 Chipset	39
3.5.1	Socket Configuration	40
	Figure 3.19 Socket Configuration	40
	Figure 3.20 Processor Configuration	41
	Figure 3.21 Processor Configuration	41
	Figure 3.22 Processor Configuration	42
	Figure 3.23 Per-Socket Configuration	44
	Figure 3.24 CPU Socket 0 Configuration	45
	Figure 3.25 PSMI Configuration	46
	Figure 3.26 Socket 0 Configuration	47
	Figure 3.27 IIO Configuration	48
	Figure 3.28 Socket0 Configuration	49
	Figure 3.29 TraceHub Configuration Menu	50
	Figure 3.30 R-Link	51
	Figure 3.31 R-Link	51
	Figure 3.32 Port 1A	53
	Figure 3.33 Port 1A	54
	Figure 3.34 Advanced Power Management Configuration	56
	Figure 3.35 CPU P State Configuration	57
	Figure 3.36 Perf P-Limit	58
	Figure 3.37 CPU C State Configuration	59
	Figure 3.38 Package C State Control	60
	Figure 3.39 Latency Tolerance Requirement (LTR)	61
	Figure 3.40 PkgC SA PS Criteria Power Management Control	62
	Figure 3.41 CPU0 PKGC_SA_PS_CRITERIA	63
	Figure 3.42 PKGc Interrupt Response Time	64
	Figure 3.43 Memory Topology	65
3.5.2	Platform Configuration	66
	Figure 3.44 Platform Configuration	66
	Figure 3.45 PCH-IO Configuration	67
	Figure 3.46 PCI Express Configuration	68
	Figure 3.47 PCI Express Root Port 1	69

	Figure 3.48 PCI Express Root Port 2	70
	Figure 3.49 PCI Express Root Port 3	71
	Figure 3.50 PCI Express Root Port 4	72
	Figure 3.51 PCI Express Root Port 5	73
	Figure 3.52 PCI Express Root Port 6	74
	Figure 3.53 PCI Express Root Port 7	75
	Figure 3.54 PCI Express Root Port 8	76
	Figure 3.55 PCI Express Root Port 9	77
	Figure 3.56 PCI Express Root Port 10	78
	Figure 3.57 PCI Express Root Port 11	79
	Figure 3.58 PCI Express Root Port 12	80
	Figure 3.59 Fia Mux Configuration	81
	Figure 3.60 Fia Mux Configuration	81
	Figure 3.61 Fia Mux Configuration	82
	Figure 3.62 Fia Mux Configuration	82
	Figure 3.63 Fia Mux Configuration	83
	Figure 3.64 SATA Configuration	85
	Figure 3.65 Controller 3 SATA Configuration	86
	Figure 3.66 USB Configuration	87
	Figure 3.67 Security Configuration	88
	Figure 3.68 System Event Log	89
	Figure 3.69 eMCA Settings	90
	Figure 3.70 Whea Settings	91
	Figure 3.71 Error Injection Settings	92
	Figure 3.72 Memory Error Enabling	93
	Figure 3.73 IIO Error Enabling	94
	Figure 3.74 IIO Error Enabling	94
	Figure 3.75 PCIe Error Enabling	96
	Figure 3.76 PCIe Error Enabling	97
	Figure 3.77 Error Control Settings	99
3.6	Server Mgmt	100
	Figure 3.78 Server Mgmt	100
3.7	Security	101
	Figure 3.79 Security	101
3.7.1	Secure Boot	102
	Figure 3.80 Secure Boot	102
3.8	Boot	103
	Figure 3.81 Boot	103
3.9	Save and Exit	104
	Figure 3.82 Save and Exit	104

Chapter 4 S/W Introduction & Installation 105

4.1	S/W Introduction	106
4.2	Driver Installation	106
4.3	Windows Driver Setup	106
4.4	Other OS	106
4.5	Advantech iManager	107

Appendix A Pin Assignment 109

A.1	SOM-5993 Type 7 Pin Assignment	110
	Table A.1: SOM-5993 ROWS A, B	110
	Table A.2: SOM-5993 ROWS C, D	112

Appendix B Watchdog Timer 115

B.1	Programming the Watchdog Timer	116
-----	--------------------------------------	-----

	Table B.1: Programming the Watchdog Timer	116
Appendix C	Programming GPIO.....	117
C.1	GPIO Register.....	118
	Table C.1: GPIO Register	118
Appendix D	System Assignments.....	119
D.1	System I/O Ports.....	120
	Table D.1: System I/O Ports	120
D.2	DMA Channel Assignments	121
	Table D.2: DMA Channel Assignments	121
D.3	Interrupt Assignments	122
	Table D.3: Interrupt Assignments	122
D.4	1st MB Memory Map.....	122
	Table D.4: 1st MB Memory Map	122

Chapter 1

General Information

This chapter details background information on the SOM-5993 CPU Computer on Module.

Sections include:

- Introduction
- Functional Block Diagram
- Product Specifications

Table 1.1: Acronyms

Term	Definition
AC'97	Audio CODEC (Encoder-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 systems 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 micro-controllers to communicate with each other within a vehicle without a host computer.
DDI	Digital Display Interface – including DisplayPort, HDMI/DVI, and SDVO
EAPI	Embedded Application Programmable Interface Software interface for COM Express® specific industrial functions – 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 circuits, primarily used to read and load register values
ME	Management Engine
PC-AT	“Personal Computer – Advanced Technology” – an IBM trademark term used to refer to Intel-based personal computers in the 1990s
PEG	PCI Express Graphics
RTC	Real Time Clock – battery-backed circuit in PC-AT systems that keeps the 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
UEFI	Unified Extensible Firmware Interface
WDT	Watchdog Timer

1.1 Introduction

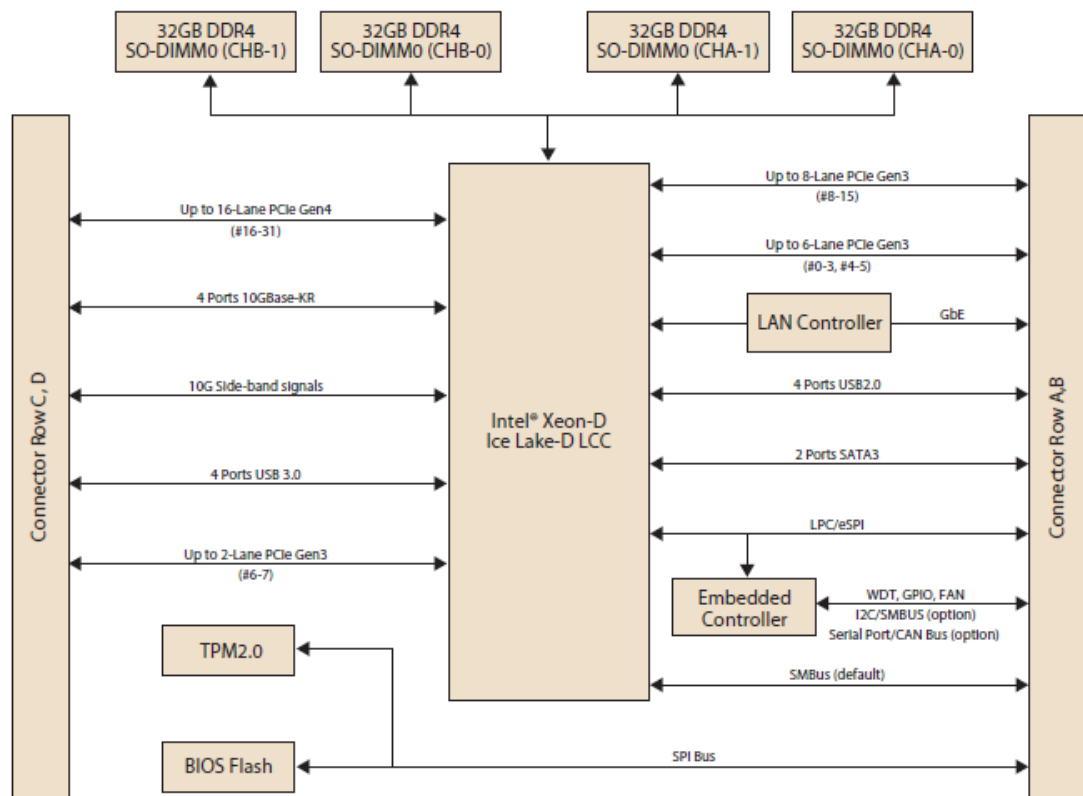
The Advantech SOM-5993 leverages 128GB of memory to support Intel® Xeon® 10-core processors in a 125 x 95 mm COM Express basic module form factor. It offers a wide spectrum of performance options enabling its users to configure the CPU and RAM based on their system specifications.

The SOM-5993 is capable of full performance without throttling when the SoC is at 69W TDP. This is achieved using Advantech's patented thermal solution—the Quadro Flow Cooling System (QFCS). SOM-5993 uses multiple TDP options (39 ~ 69W) to fulfill the needs of middle/high-end systems.

In addition, SOM-5993 features a reliable design that adapts to diverse applications. It also features ruggedized SODIMM for improved vibration and shock resistance; and supports TPM 2.0 onboard chips for cyber-security. Likewise, its wide power input and temperature range support (9 ~ 12V; -40 ~ 85°C) is ideal for diverse applications. In terms of software, SOM-5993 supports WISE-DeviceOn for remote hardware monitoring and over-the-air software updates.

SOM-5993 features 4 screw holes near the CPU, positioned in compliance with the Intel® standard thermal design guide. The thermal module is attached to the CPU using a balanced torque design. It is the first COM Express to add a backplane to increase the rigidity of the single board. This means that the thermal module makes tight contact with the CPU without the board bending. This results in highly efficient heat dissipation and outstanding computing performance. Advantech also offers SOM-5993 thermal solution pre-assembly services that make system-level assembly easy.

1.2 Functional Block Diagram



1.3 Product Specifications

1.3.1 Compliance

- PICMG COM.0 (COM Express) Revision 3.0
- Basic Size – 125 x 95 mm
- Pin-out Type 7 compatible

1.3.2 Feature List

Table 1.2: Feature List			
Row	System I/O	R3.0 Type 7	SOM-5993
A-B	PCI Express Lanes 0 - 5	6/6	6
	PCI Express Lanes 8 - 15 (Type 7)	0/8	8
	LVDS Channel A	N/A	N/A
	LVDS Channel B	N/A	N/A
	eDP on LVDS CH A Pins	N/A	N/A
	VGA Port	N/A	N/A
	Serial Ports 1 - 2	0/2	2
	CAN Interfaces on SER1	0/1	1 (Optional)
	SATA/SAS Ports	0/2	2
	HDA Digital Interface	N/A	N/A
	USB 2.0 Ports (Host)	4/4	4
	USB0 Client (USB 2.0)	0/1	0
	1Gb LAN Port 0	1/1	1
	LPC Bus	1/1	1 (LPC)
	SPI	1/2	1
Row	System Management	R3.0 Type 7	SOM-5993
A-B	SDIO (Muxed on GPIO)	0/1	0
	General Purpose I/O	8/8	8
	SMBus	1/1	1
	I2C	1/1	1 (Optional)
	Watchdog Timer	0/1	1
	Speaker Out	1/1	1
	External BIOS ROM Support	0/1	1
	Reset Function	1/1	1
	Trusted Platform Modules	0/1	1
Row	Power Management	R3.0 Type 7	SOM-5993

A-B	Thermal Protection	0/1	1
	Battery Low Alarm	0/1	1
	Suspend/Wake Signals	0/3	2
	Power Button Support	1/1	1
	Power Good	1/1	1
	VCC_5V_SBY Contacts	4/4	4
	Sleep Input	0/1	1
	Lid Input	0/1	1
	Carrier Board Fan Control	0/1	1
Row	Power	R3.0 Type 7	SOM-5993
A-B	VCC_12V Contacts	12/12	12
Row	System I/O	R3.0 Type 7	SOM-5993
C-D	PCI Express Lanes 16 - 31 (PEG)	0/16	16
	PCI Express Lanes 6 - 7	0/2	2
	10G LAN Port 0-3	0/4	4
	Digital Display Interfaces 1 - 3	N/A	N/A
	USB 3.0 Ports	0/4	4
	Rapid Shutdown	0/1	1
Row	Power	R3.0 Type 7	SOM-5993
C-D	VCC_12V Contacts	12/12	12

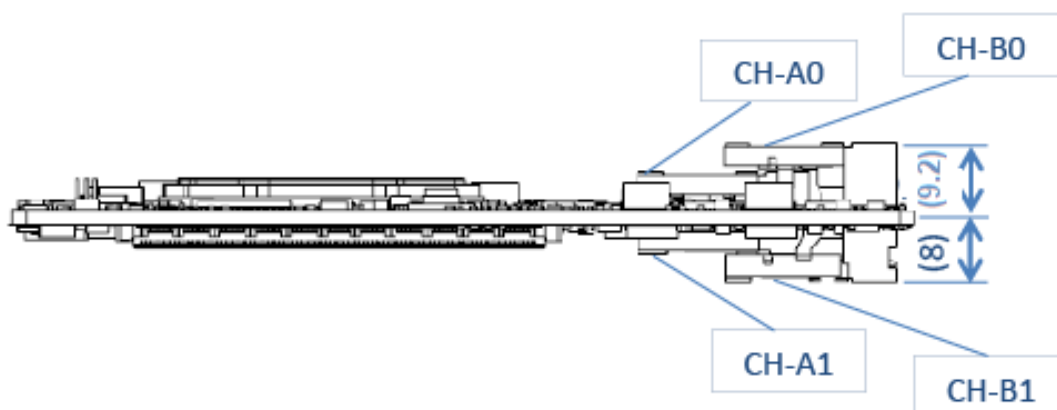
1.3.3 Processor System

Table 1.3: Processor System

CPU	Std. Freq.	Max. Turbo Freq.	Core/Thread	LLC Cache	TDP (W)
Xeon® D-1746TER	2.0 GHz	3.1 GHz	10/20	15MB	67W
Xeon® D-1735TR	2.2 GHz	3.4 GHz	8/16	15MB	59W
Xeon® D-1732TE	1.9 GHz	3.0 GHz	8/16	15MB	52W
Xeon® D-1715TER	2.4 GHz	3.5 GHz	4/8	10MB	50W
Xeon® D-1712TR	2.0 GHz	3.1 GHz	4/8	10MB	40W
Xeon® D-1713TR	2.2 GHz	3.5 GHz	4/8	10MB	45W
Xeon® D-1813TR	2.2 GHz	2.4 GHz	4/8	10MB	42W

1.3.4 Memory

Dual-channel 4 x sockets supporting DDR4 2400MHz up to 2666MHz (ECC supported) with maximum support for 32GB in each socket (Total=128GB).



Note! Installing memory modules in pairs on SOM-5993 requires filling the lowest numbered slots first.
For example, the SOM-5993 has two slots each for channel A (CH-A) and channel B (CH-B), numbered 0 and 1. Fill the slots for CH-A0 and CH-B0 first, then CH-A1 and CH-B1 second.

1.3.5 Graphics/Audio

The Intel® Xeon® Processor D family lacks graphics. Likewise, SOM-5993 does not support display and audio. Graphics are defined according to specific user scenarios based on system specifications. Please contact Advantech sales or FAE for further details.

1.3.6 Expansion Interface

PCIe x16 [31:16]

Intel® Xeon® Processor D natively integrates 1 x PCIe x16 interface with support for up to 4 devices at up to Gen4 speeds (8 GHz). SOM-5993 supports 1 x (PCIe x16), and is configurable to 4 x (PCIe x4), 2 x (PCIe x4) and 1 x (PCIe x8), or 1 x (PCIe x8) and 2 x (PCIe x4), or 2 (PCIe x8).

Table 1.4: PCIe x16 [31:16]

Type 7	Rows C, D															
	P0	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15
Default	X16															
Option 1	X4				X4				X4				X4			
Option 2 Config	X4				X4								X8			
Option 3					X8				X4				X4			
Option 4					X8								X8			

PCIe x8, [7:0]

Intel® Xeon® Processor D natively integrates 1 x PCIe x8 lane and up to 4 devices at up to Gen3 speeds (8.0 GT/s).

The SOM-5993 supports 1 x (PCIe x4) and 2 x (PCIe x2) as default, and is configurable to 4 x (PCIe x2), 1 x (PCIe x4) and 2 x (PCIe x2), 2 x (PCIe x2) and 1 x (PCIe x4), or 2 x (PCIe x4) and 1 x (PCIe x8).

Table 1.5: PCIe x8, [7:0]

Type 7	Row A, B				Rows C, D			
	P0	P1	P2	P3	P4	P5	P6	P7
Default		X4			X2		X2	
Option 1	X2		X2		X2		X2	
Option 2		X4			X2		X2	
Option 3	X2		X2			X4		
Option 4		X4				X4		
Option 5				X8				

PCIe x8, [15:8]

Intel® Xeon® Processor D natively integrates 1 x PCIe x8 lanes and up to 4 devices at up to Gen3 speed (8.0 GT/s).

The SOM-5993 supports 1 x (PCIe x8) by default, and is configurable to 4 x (PCIe x2), 1 x (PCIe x4) and 2 x (PCIe x2), 2 x (PCIe x2) and 1 x (PCIe x4), or 2 x (PCIe x4).

Table 1.6: PCIe x8, [15:8]

Type 7	Rows A, B							
	P8	P9	P10	P11	P12	P13	P14	P15
Default				X8				
Option 1	X2		X2		X2		X2	
Option 2		X4			X2		X2	
Option 3	X2		X2			X4		
Option 4		X4				X4		
Option 5				X8				

1.3.7 LPC

This solution supports Low Pin Count (LPC) 1.1 specifications, without DMA or bus mastering. This allows it to connect super I/O, embedded controllers, or TPM. The LPC clock is 24MHz.

1.3.8 Serial Bus

1.3.8.1 SMBus

Support for SMBus 2.0 specifications with alert pins.

1.3.8.2 I2C Bus

Support for I2C bus 8-bit and 10-bit address modes, at both 100KHz and 400KHz.

1.3.9 I/O

1.3.9.1 Gigabit Ethernet

On-module Intel i225IT supports the standard IEEE802.3 Ethernet interface for 2500BASE-T, 1000BASE-T, 100BASE-TX, and 10BASE-T connections (IEEE 802.3, 802.3u, and 802.3ab). There is support for TCP/UDP (for both IPv4, IPv6) checksum calculations and performing TCP segmentation.

1.3.9.2 SATA

Support for 2 x SATA Gen 3 (6.0 Gb/s) ports, backwards compliant to SATA Gen 2 (3.0 Gb/s) and Gen1 (1.5 Gb/s). The maximum data rate is 600 MB/s. There is support for AHCI 1.3 mode.

1.3.9.3 USB 3.0 / USB 2.0

4 x USB 3.0 ports (5.0 Gbps) and 4 x USB 2.0 ports (480 Mbps) which are backward compatible to USB 1.x. It supports LPM (U0, U1, U2, and U3) for USB 3.0 to save power.

1.3.9.4 USB 3.0

Table 1.7: USB 3.0

Type 7	P0	P1	P2	P3
SoC	P0	P1	P2	P3
Type 7	USB_0_1_OC#		USB_2_3_OC#	
SOC_USBOC#	USB_OC#01		USB_OC#23	

1.3.9.5 USB 2.0

Table 1.8: USB 2.0

Type 7	P0	P1	P2	P3
SoC	P0	P1	P2	P3
Type 7	USB_0_1_OC#		USB_2_3_OC#	
SOC_USBOC#	USB_OC#01		USB_OC#23	

1.3.9.6 SPI Bus

Support for BIOS flash only. The SPI clock can be 50MHz, 33MHz, or 20MHz, with capacity up to 16MB.

1.3.9.7 GPIO

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

1.3.9.8 Watchdog

There is support for multi-level watchdog time-out output. It provides 1-65535 levels, from 100ms to 109.22-minute intervals.

1.3.9.9 Serial Ports

- 2 x ports, 2-wire serial port (Tx/Rx) support 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 characters
- Even, odd, or no parity bit selectable
- 1, 1.5, or 2 stop bit selectable
- Baud rate up to 115.2K

1.3.9.10 TPM

TPM 2.0 module by optional support.

1.3.9.11 Smart Fan

There is support for 2 x fan PWM control signals and 2 x tachometers for input for fan speed detection. There is 1 fan on the module with a connector and 1 on the carrier board following PICMG COM Express R3.0 specifications.

1.3.9.12 BIOS

BIOS chips are on the module by default. This allows the user to have a BIOS chip on the carrier board with the appropriate design and jumper settings on BIOS_DIS#[1:0].

Table 1.9: BIOS

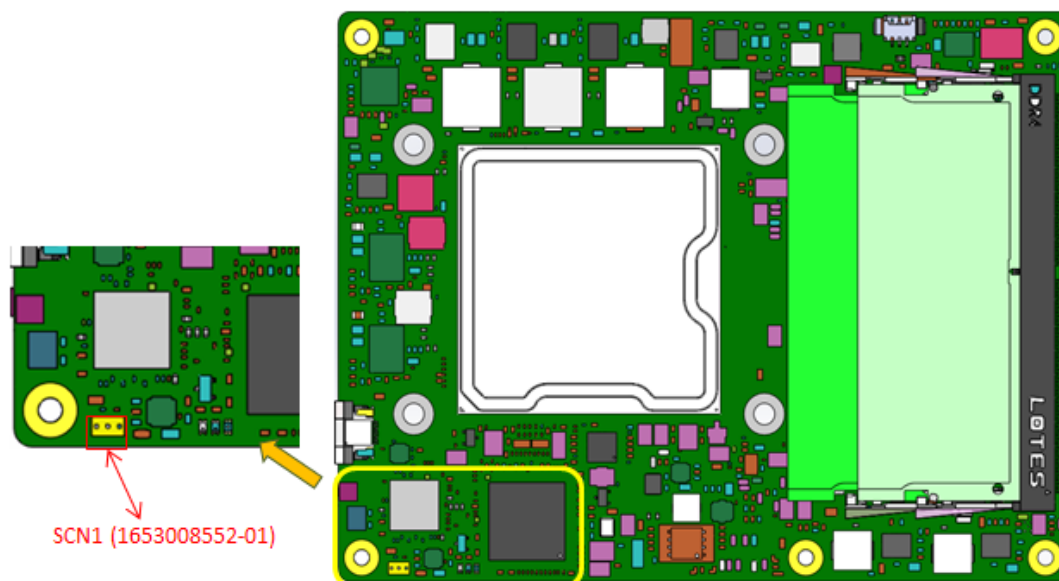
BIOS_DIS0#	BIOS_DIS#1	Boot Up Destination/Function
Open	Open	Boot from the Module's SPI BIOS
GND	Open	Boot from the Carrier Board LPC/FWH BIOS
Open	GND	SPI_CS0# to Carrier Board, SPI_CS1# to Module
GND	GND	SPI_CS0# to Module, SPI_CS1# to Carrier Board

Notice: If the system CMOS is cleared, we strongly suggest going to the BIOS setup menu and loading default settings following the first bootup.

Table 1.10: Clear CMOS

Setting Type	Jumper Setting	Clear RTC CMOS (Time & Date)	BIOS Setting Load Default
Default Setting	Without jumper	V	NA
Optional Setting	Jumper 1-2	V	V

Purpose: The standard module has no jumper at SCN1. Therefore, the BIOS settings are maintained without an RTC coin battery. If you need to restore the BIOS default settings, please follow the steps below:



1. Remove the coin battery.
2. Put the jumper on SCN1 pin1-2.
3. Turn on the power supply.
4. The system will boot up a few times.
5. The BIOS will load default settings successfully.

1.3.10 Power Management

1.3.10.1 Power Supply

The power supply supports both ATX and AT power modes. VSB is to suspend power and can be an option if the user does not require standby (suspend-to-RAM) support. An RTC Battery is optional if keeping the time/date is not required.

- VCC: 9V ~ 12V (+/-5%) power input
- VSB: 5V (+/- 5%) suspend power
- RTC battery Power: 2.0 ~ 3.3V

1.3.10.2 PWROK

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

1.3.10.3 Power Sequence

According to PICMG COM Express R3.0 specifications

1.3.10.4 Wake Event

Diverse wake-up events support different scenarios.

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

1.3.10.5 Advantech S5 ECO Mode (Deep Sleep Mode)

Advantech iManager provides additional features that allow systems to enter a very low suspend power mode – S5 ECO mode. The module will cut all power including suspend and active power into the chipset and keep an on-module controller active in this mode. In such cases, under 50mW of power will be consumed. This means user battery packs can last longer. When enabled in BIOS, this mode only allows the system (or module) to boot from the power button, and does not support WOL.

1.3.11 Environment

1.3.11.1 Temperature

- Standard: 0 ~ 60°C (32 ~ 140°F), with an active heat sink under 0.7m/s air flow chamber
- Extend: -40 ~ 85°C (-40 ~ 185°F)
- Storage: -40 ~ 85°C (-40 ~ 185°F)

1.3.11.2 Humidity

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

1.3.11.3 Vibrations

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

1.3.11.4 Drop Test (Shock)

Federal Standard 101 Method 5007 test procedure with standard packing

1.3.11.5 EMC

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

1.3.12 MTBF

Please refer Advantech SOM-5993 Series Reliability Prediction Report No: CERT-22-01345.

Link: <http://com.advantech.com>

1.3.13 OS Support (duplicate with SW chapter)

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

To install the drivers for Linux or other OS, please connect to the Internet to download the setup file.

Link: <http://support.advantech.com.tw>

1.3.14 Advantech iManager

iManager supports APIs for GPIO, smart fan control, multi-stage watchdog timer output, temperature sensor, hardware monitor, etc. It follows PICMG EAPI 1.0 specifications and provides backward compatibility.

1.3.15 Power Consumption

Table 1.11: 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	RTC (uA)
SOM-5993D10-U0A1	84.229 W	70.586 W	34.504 W	5.834 W	4.79 uA

Hardware Configurations:

1. MB: SOM-5993D10-U0A1 (PCB_A101-1, CPU: Intel® Xeon® D-1746TER)
2. DRAM: 2 x 32GB DDR4 2666MHz ECC SODIMM
3. Carrier board: SOM-DB5920_A201-1

Test Conditions:

1. Test temperature: room temperature
2. Test voltage: rated voltage DC +12.0V
3. Test loading:
 - Idle mode: DUT power management off and not running any programs
 - Maximum load mode: Running programs
4. OS: Windows Server 2012 R2 Standard
5. Test software:
 - Burn-In Test V8.1 Pro (1022) for 64-Bit Windows
 - Intel® Power Thermal Utility Tool Rev1.1

1.3.16 Performance

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

1.3.17 Pin Definitions

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

Please contact your nearest Advantech branch office to receive design documents and advanced support.

Chapter 2

Mechanical Information

This chapter details mechanical information for the SOM-5993 CPU Computer on Module.

Sections include:

- Board Information
- Mechanical Diagram
- Assembly Diagram

2.1 Board Information

The figures below indicate the main chips on the SOM-5993 Computer-on-Module. Please be aware of these positions while designing customer carrier boards to avoid mechanical problems. Use thermal solution contacts for improved thermal performance.

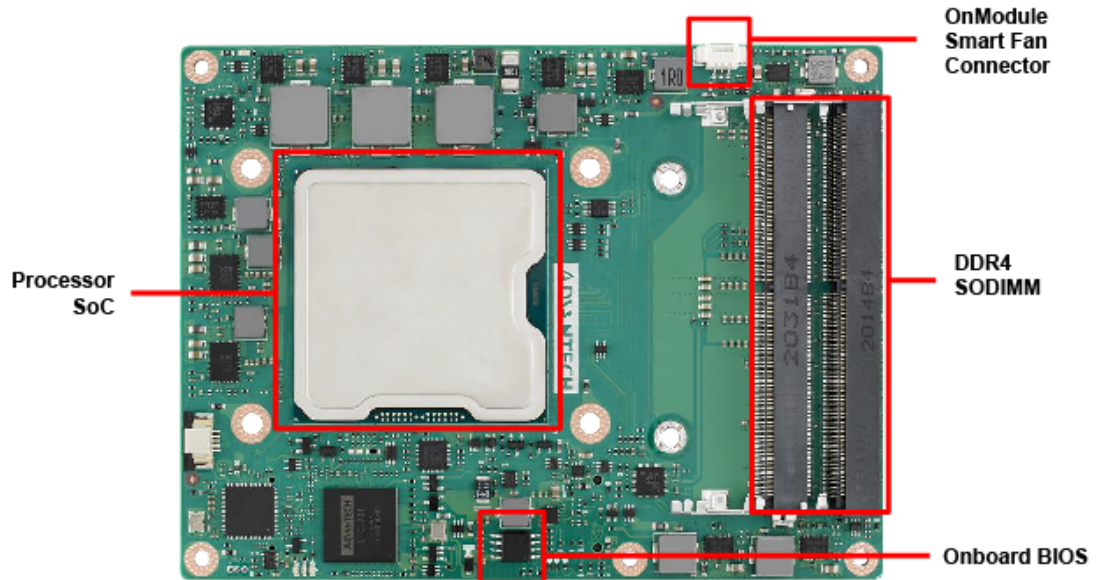


Figure 2.1 Board Chip Identification – Front

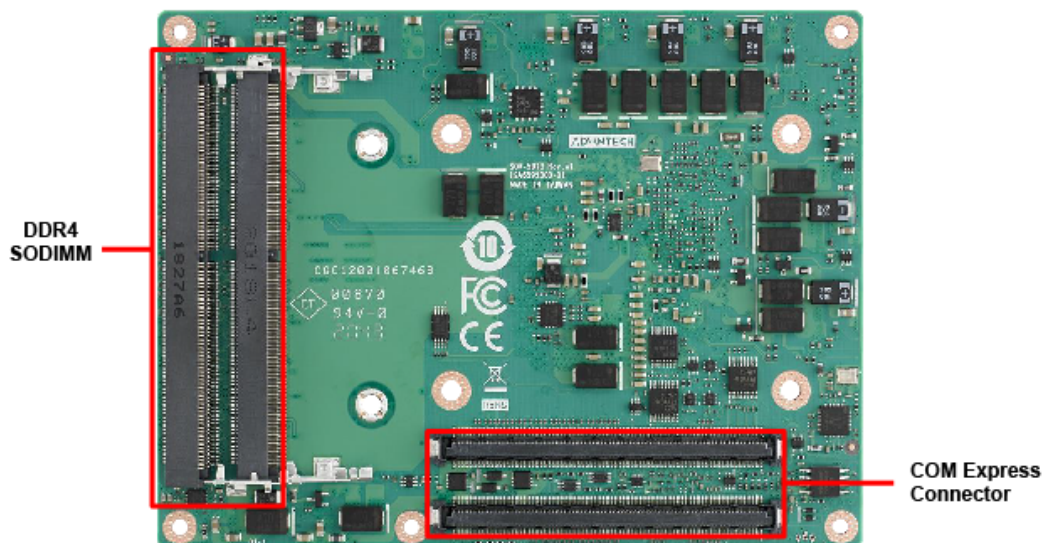
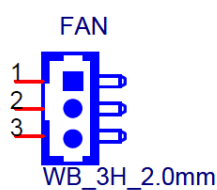


Figure 2.2 Board Chip Identification – Back

2.1.1 Connector List

Table 2.1: FAN1 Fan

FAN1	Fan
Description	Wafer 2.0 mm 3P 90D(M)DIP 2001-WR-03-LF W/Lock
Pin	Pin Name
1	Fan Tacho-Input
2	Fan Out
3	GND



2.2 Mechanical Diagram

For more information on 2/3D models, please visit the Advantech COM support service website at: <http://com.advantech.com>.

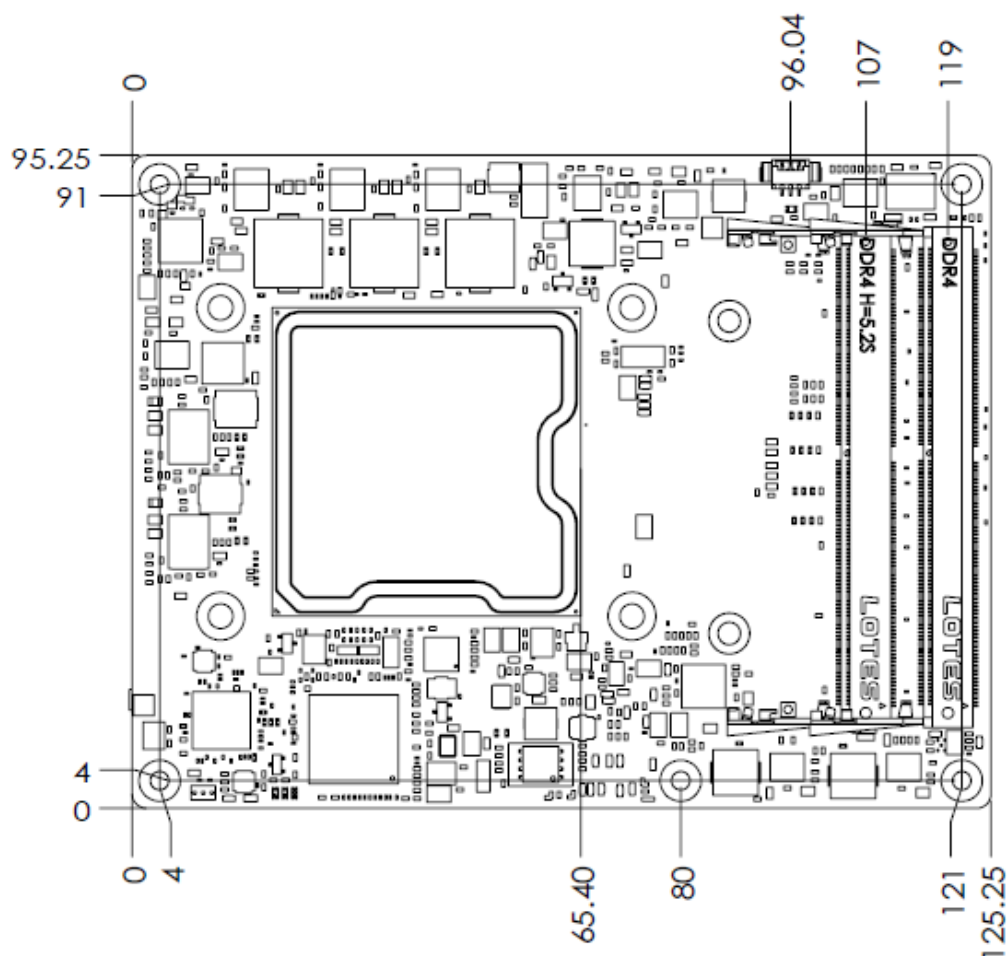


Figure 2.3 Board Mechanical Diagram — Front

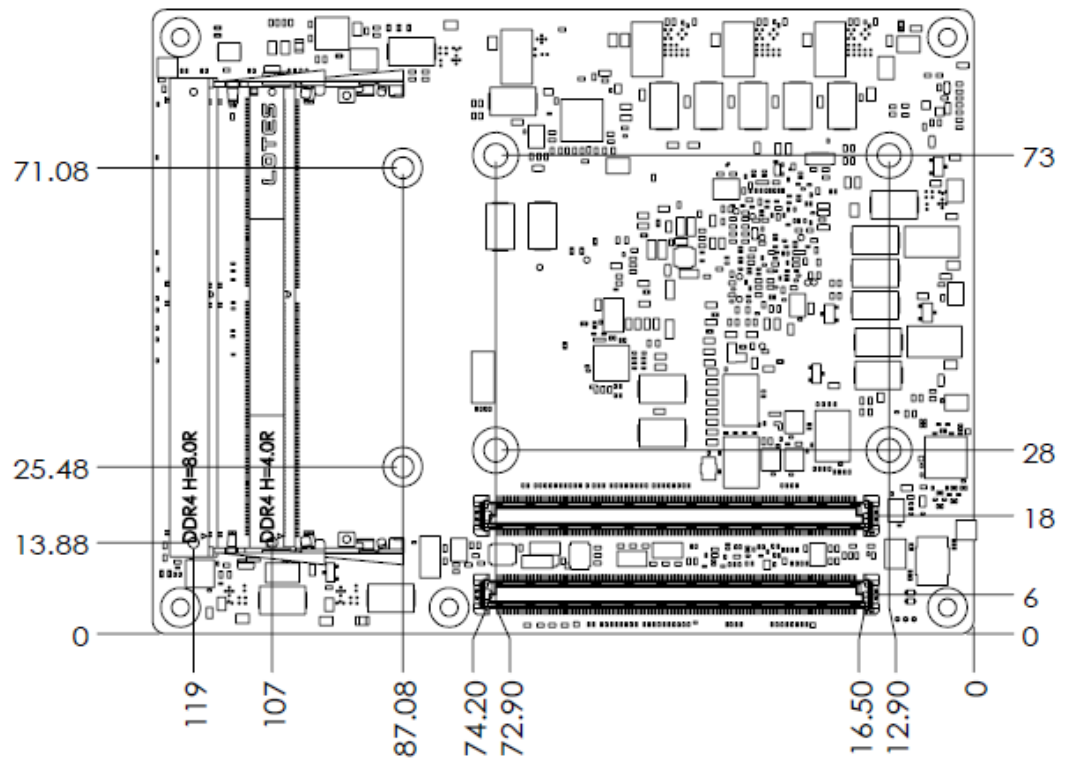


Figure 2.4 Board Mechanical Diagram – Back

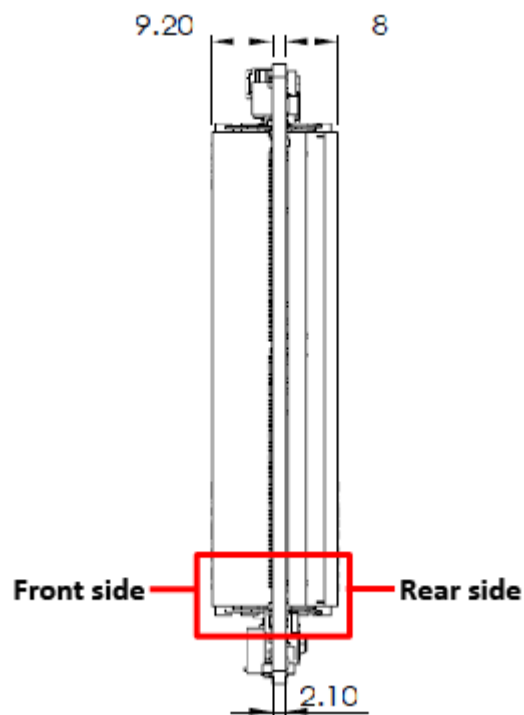


Figure 2.5 Board Mechanical Diagram – Side

2.3 Assembly Diagram

This figure demonstrates the assembly order of the thermal module, COM module, and carrier board.

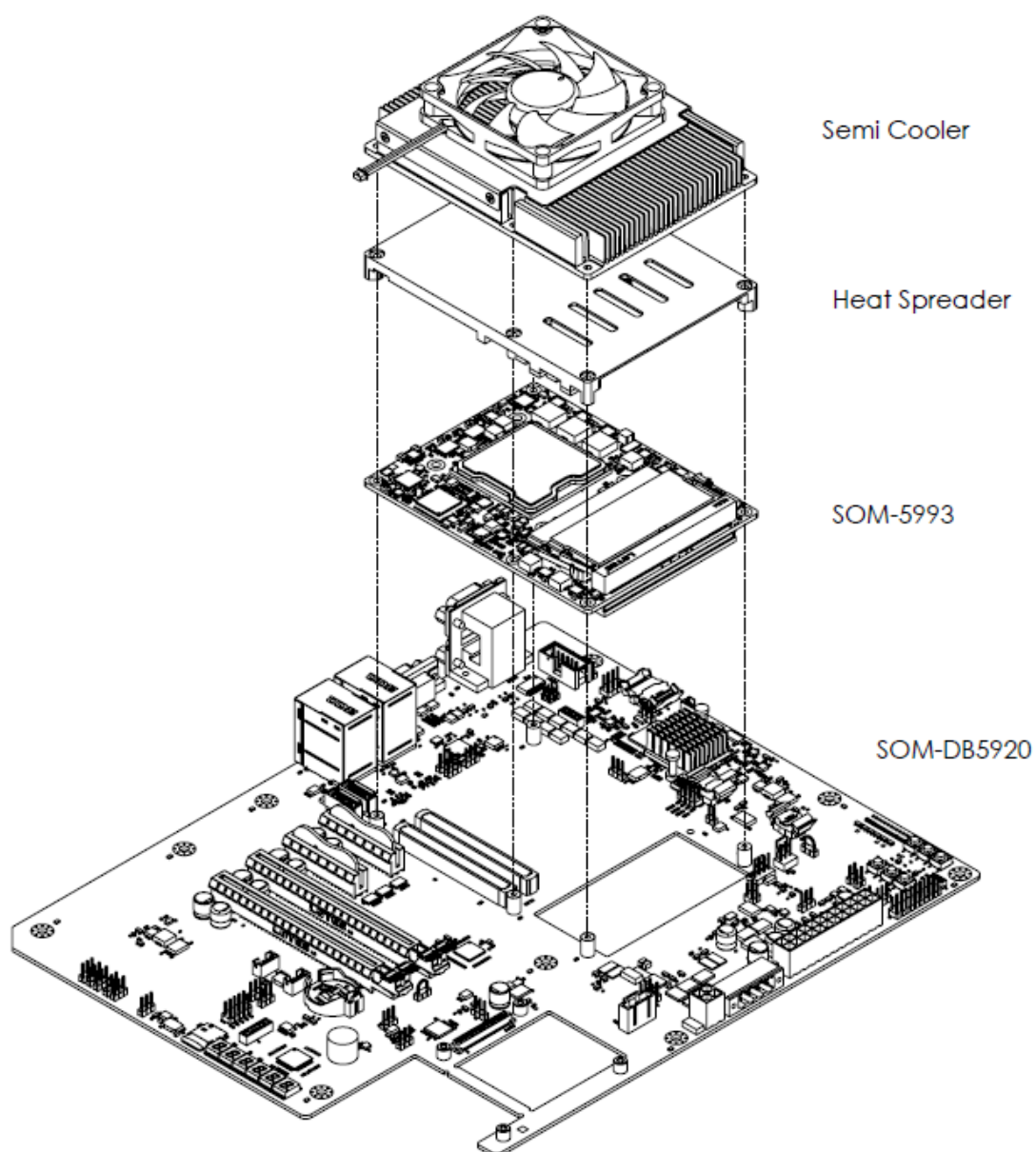


Figure 2.6 Assembly Diagram

There are 4 reserved screw holes on SOM-5993 for pre-assembly with a heat spreader.

2.4 Assembly Diagram

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

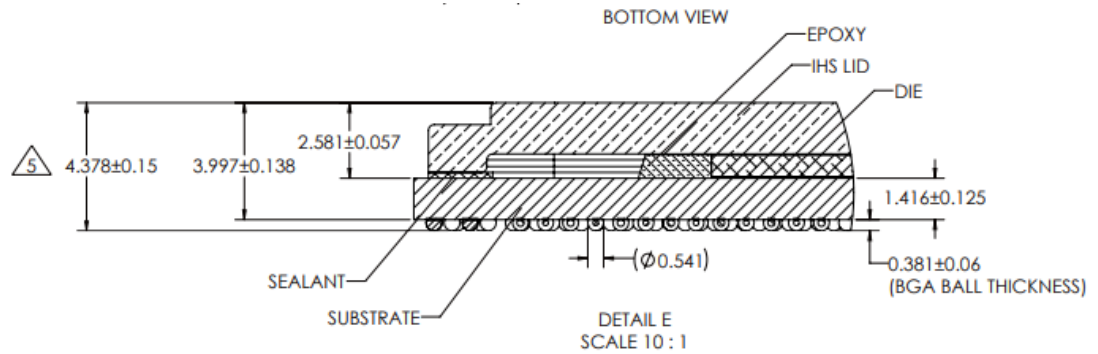


Figure 2.7 Main Chip Height and Tolerances

Package height: 4.378 mm TOL: ± 0.242 mm

(Post SMT stackup height based on limited data from Intel reference board design)

Chapter 3

AMI BIOS

This chapter details BIOS setup information for the SOM-5993 CPU computer-on module.

Sections include:

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

3.1 Introduction

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 the 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 enter the Main setup screen.

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



Figure 3.2 Main Setup Screen

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

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

■ System Time / System Date

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

3.4 Advanced BIOS Features Setup

Select the Advanced tab from the SOM-5993 setup screen to enter the Advanced BIOS Setup screen. Users can select any item in the left frame of the screen, such as CPU Configuration, to go to the sub-menu for that item. Users can display an Advanced BIOS Setup option by highlighting it using the <Arrow> keys. All Advanced BIOS Setup options are described in this section. The Advanced BIOS Setup screens are shown below. The sub-menus are described on the following pages.

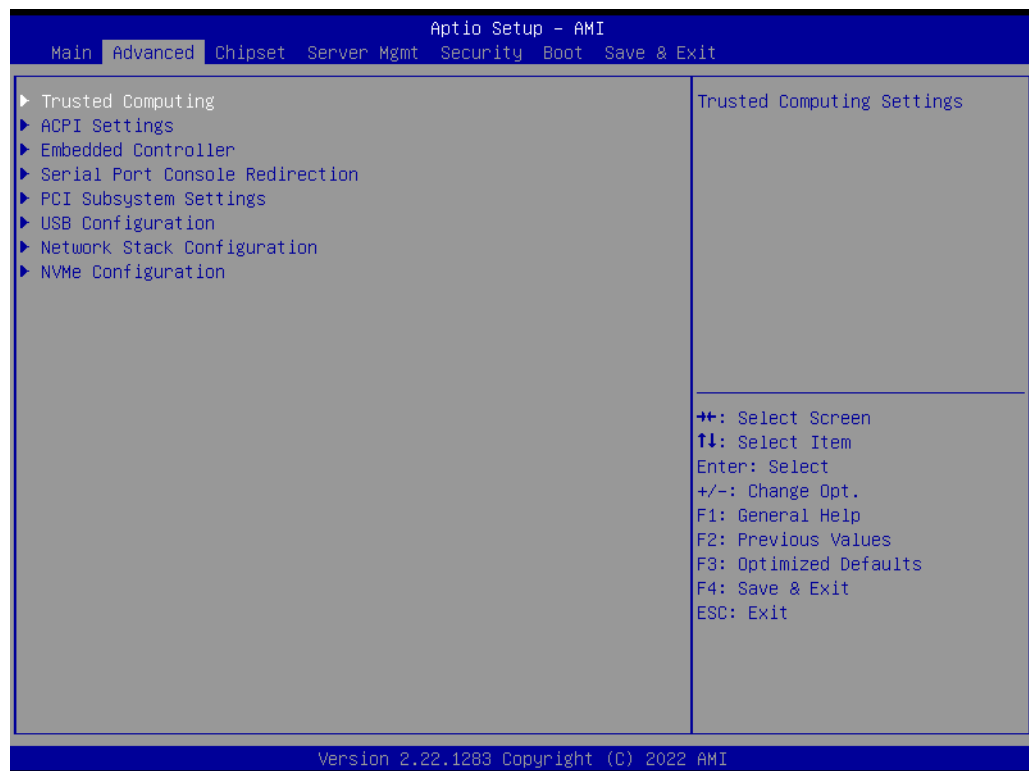


Figure 3.3 Advanced BIOS Features Setup Screen

3.4.1 Trusted Computing

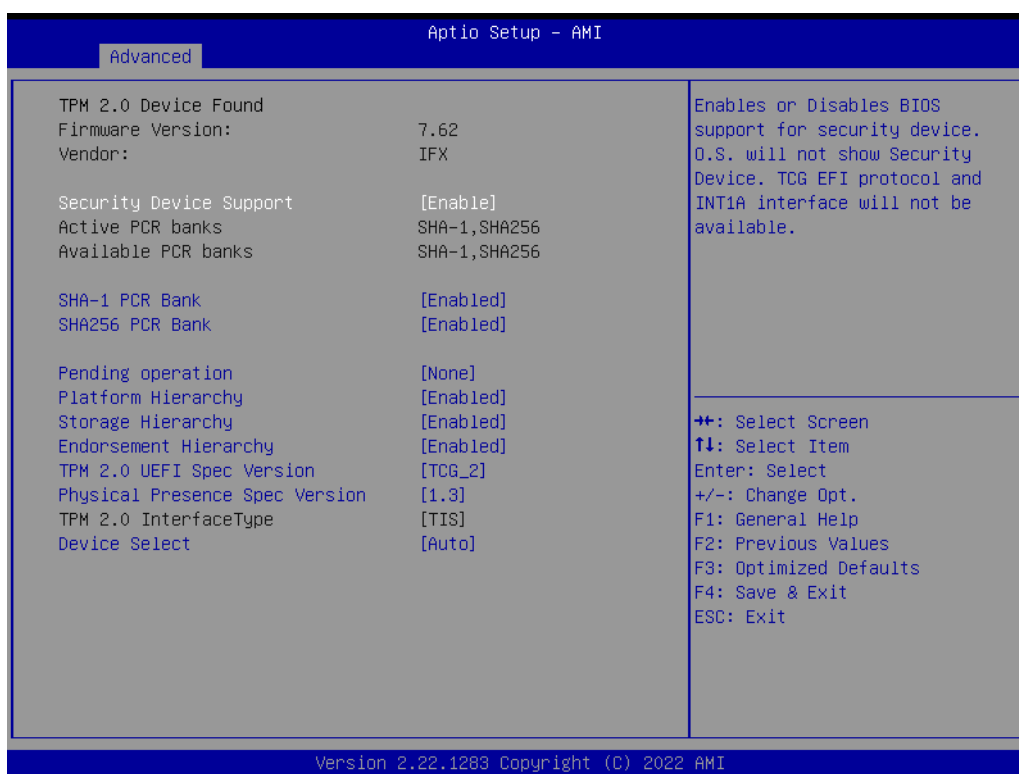


Figure 3.4 Trusted Computing

- **Security Device Support**
Enables or Disables BIOS support for the security device. The OS will not show the security Device. TCG EFI protocol and the INT1A interface will not be available.
- **SHA-1 PCR Bank**
Enable or Disable SHA-1 PCR Bank.
- **SHA256 PCR Bank**
Enable or Disable SHA256 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.
- **TPM 2.0 UEFI Spec Version**
Select the TCG2 Spec Version Support,
TCG_1_2: the compatible mode for Win8/Win10
TCG_2: Supports the new TCG2 protocol and event format for Win10 or later
- **Physical Presence Spec Version**
Select to tell the OS to support PPI Spec Version 1.2 or 1.3. Note: some HCK tests might not support 1.3.
- **Device Select**
TPM 1.2 will restrict support to TPM 1.2 devices. TPM 2.0 will restrict support to

TPM 2.0 devices. Auto will support both with the default set to TPM 2.0 devices if not found. TPM 2.0 devices will be enumerated.

3.4.2 ACPI Settings

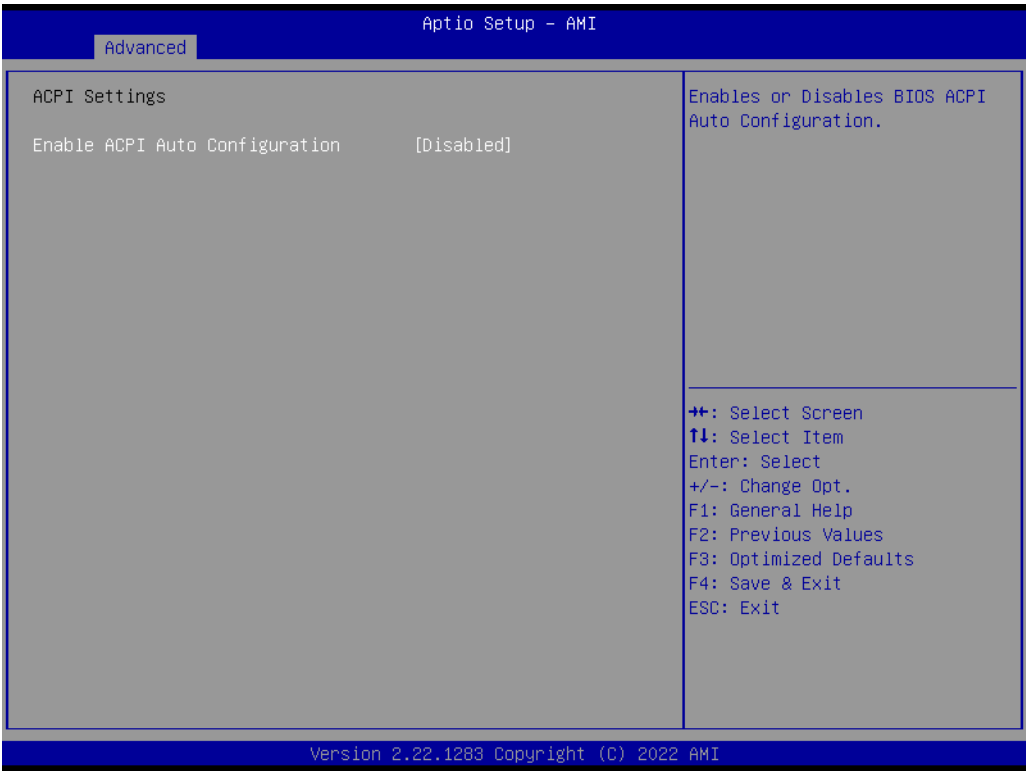


Figure 3.5 ACPI Settings

- **Enable ACPI Auto Configuration**
Enables or disables BIOS ACPI Auto Configuration.

3.4.3 Embedded Controller

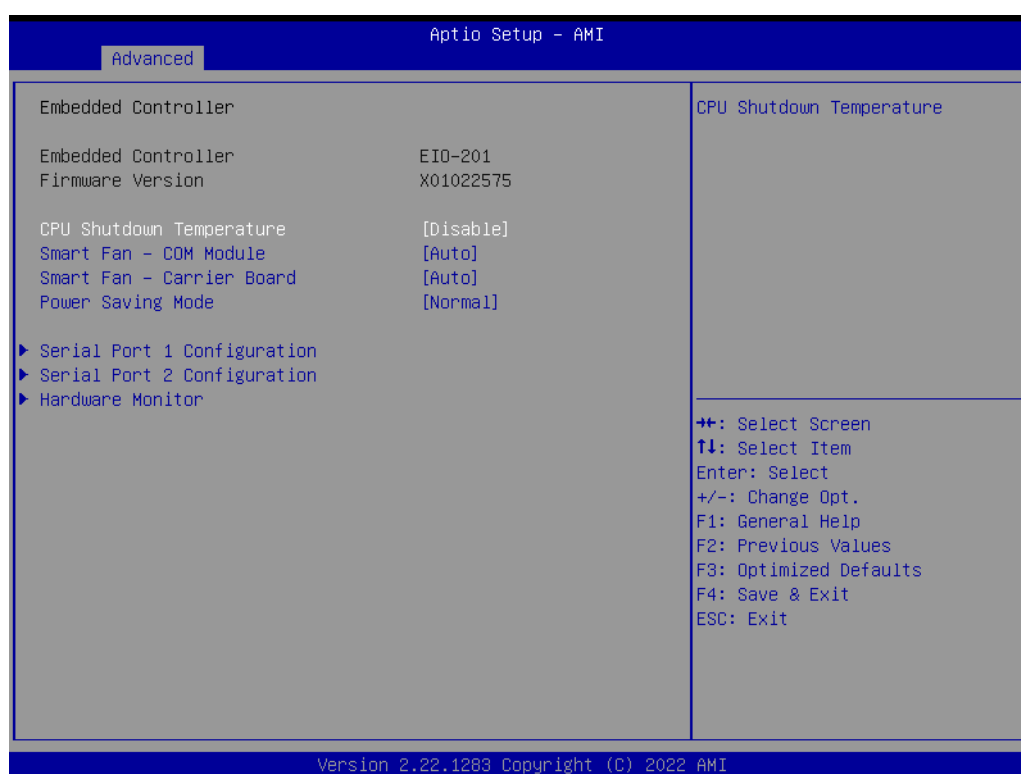


Figure 3.6 Embedded Controller

- **CPU Shutdown Temperature**
CPU Shutdown Temperature.
- **Smart Fan – COM Module**
Control the COM Module Smart FAN function. Get the value from EC and only set the value when you save changes.
- **Smart Fan – Carrier Board**
Control the Carrier Board Smart FAN function. Get the value from EC and only set the value when you save changes.
- **Power Saving Mode**
Select Power Saving Mode.
- **Serial Port 1 Configuration**
Set Parameters of Serial Port 1(COMG).
- **Serial Port 2 Configuration**
Set Parameters of Serial Port 2(COMH).
- **Hardware Monitor**
Monitor hardware status.

3.4.3.1 Serial Port 1 Configuration

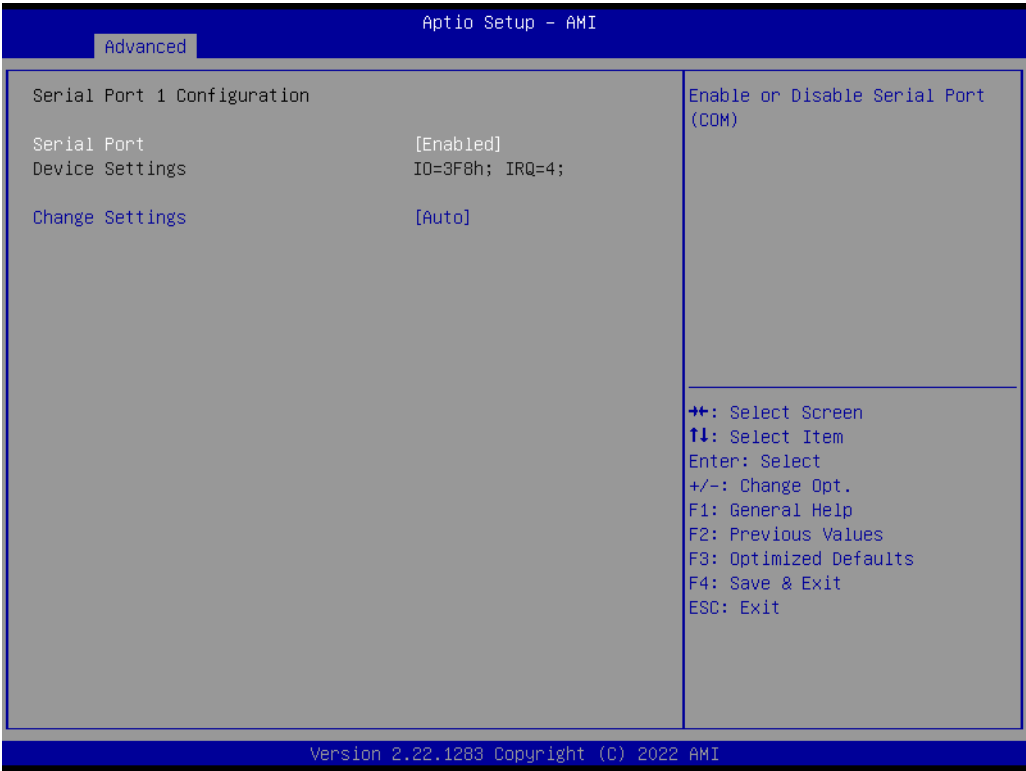


Figure 3.7 Serial Port 1 Configuration

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

3.4.3.2 Serial Port 2 Configuration

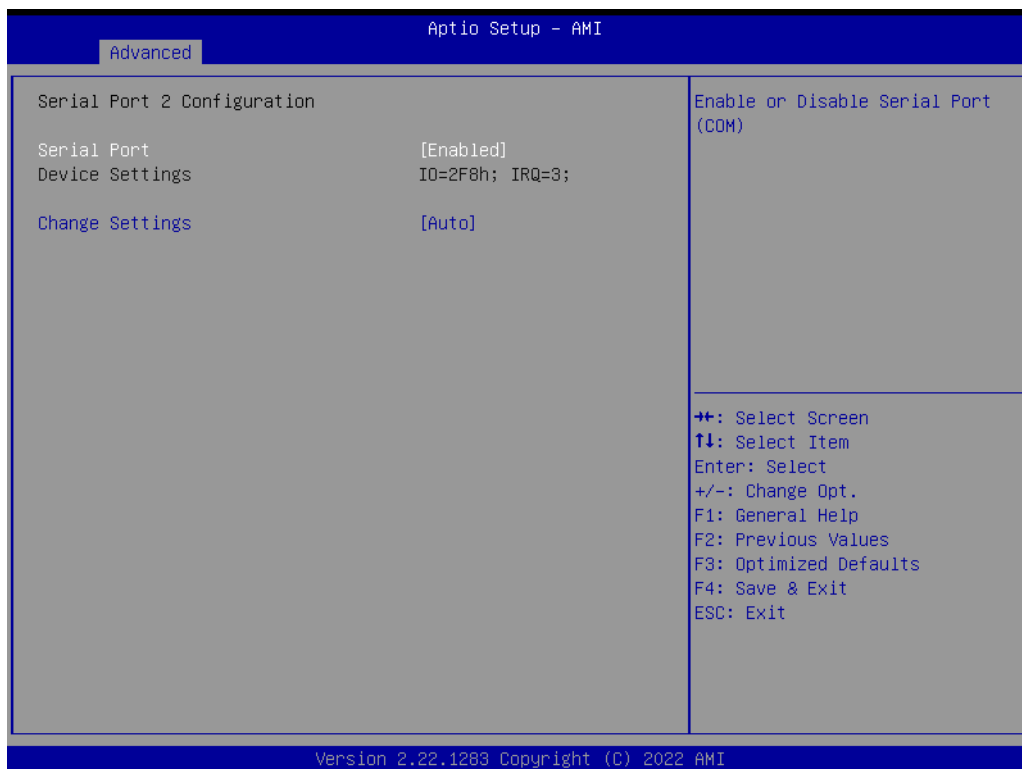


Figure 3.8 Serial Port 2 Configuration

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

3.4.3.3 Hardware Monitor

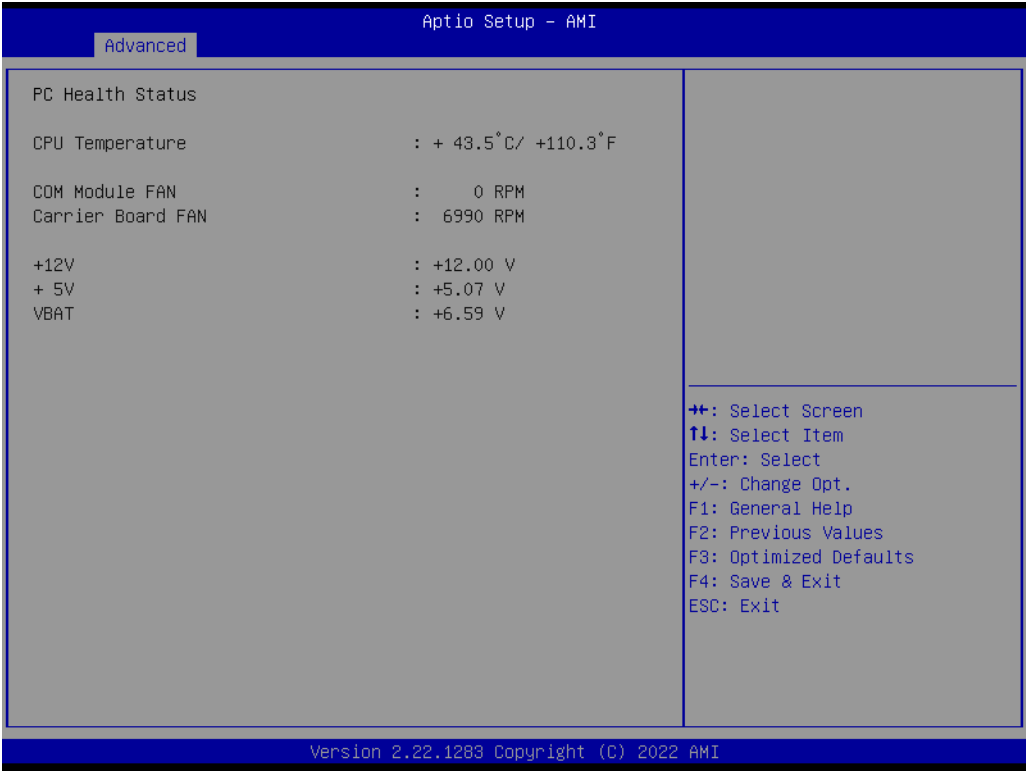


Figure 3.9 Hardware Monitor

3.4.4 Serial Port Console Redirection



Figure 3.10 Serial Port Console Redirection

- **Console Redirection**
Console Redirection Enable or Disable.
- **Console Redirection Settings**
The settings specify how the host computer and remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.
- **Console Redirection**
Console Redirection Enable or Disable.
- **Console Redirection EMS**
Console Redirection Enable or Disable.

3.4.4.1 Console Redirection Settings

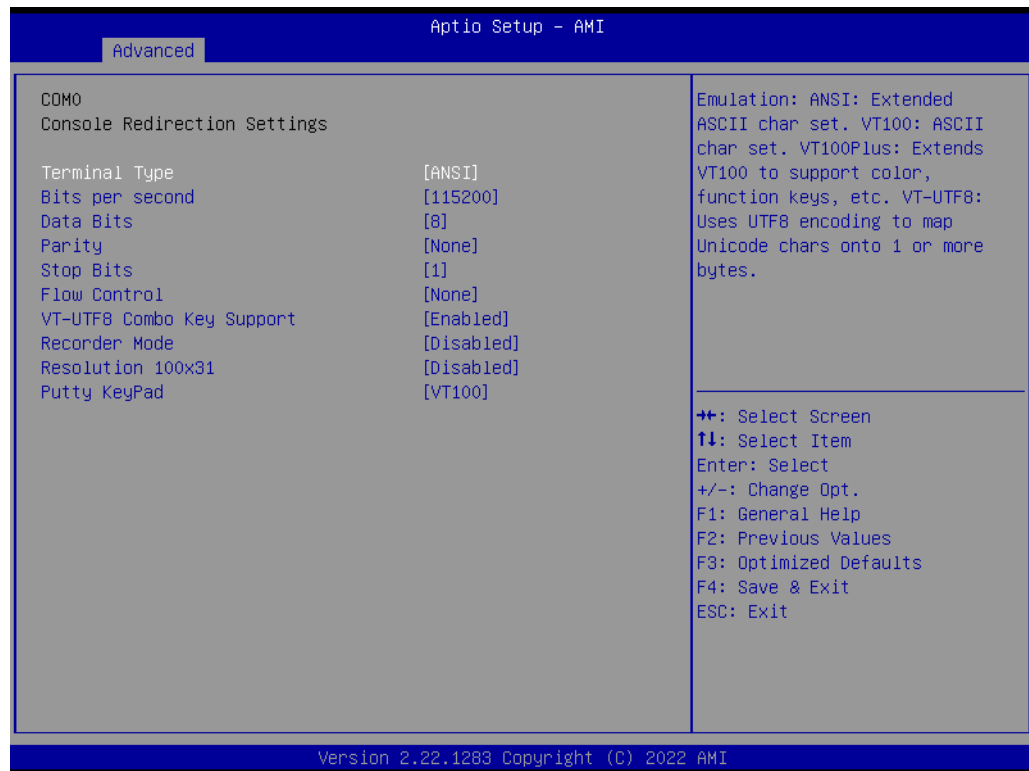


Figure 3.11 Console Redirection Settings

- **Terminal Type**
Emulation: ANSI: Extended ASCII charset. VT100: ASCII charset. VT100Plus: Extends VT100 to support color, function keys, etc.
- **Bits per second**
Selects serial port transmission speed. The speed must be matched on the other side.
Long or noisy lines may require lower speeds.
- **Data Bits**
Data Bits.
- **Parity**
A parity bit can be sent with the data bits to detect some transmission errors.
Even: Parity bit is 0 if the number of 1s in the data bits is even.
- **Stop Bits**
Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning).
The standard setting is 1 stop bit.
- **Flow Control**
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow.
- **VT-UTF8 Combo Key Support**
Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
- **Recorder Mode**
With this mode enabled only text will be sent. This is to capture Terminal data.
- **Resolution 100 x 31**
Enable or disable extended terminal resolution.
- **Putty KeyPad**
Select FunctionKey and KeyPad on Putty.

3.4.5 PCI Subsystem Settings

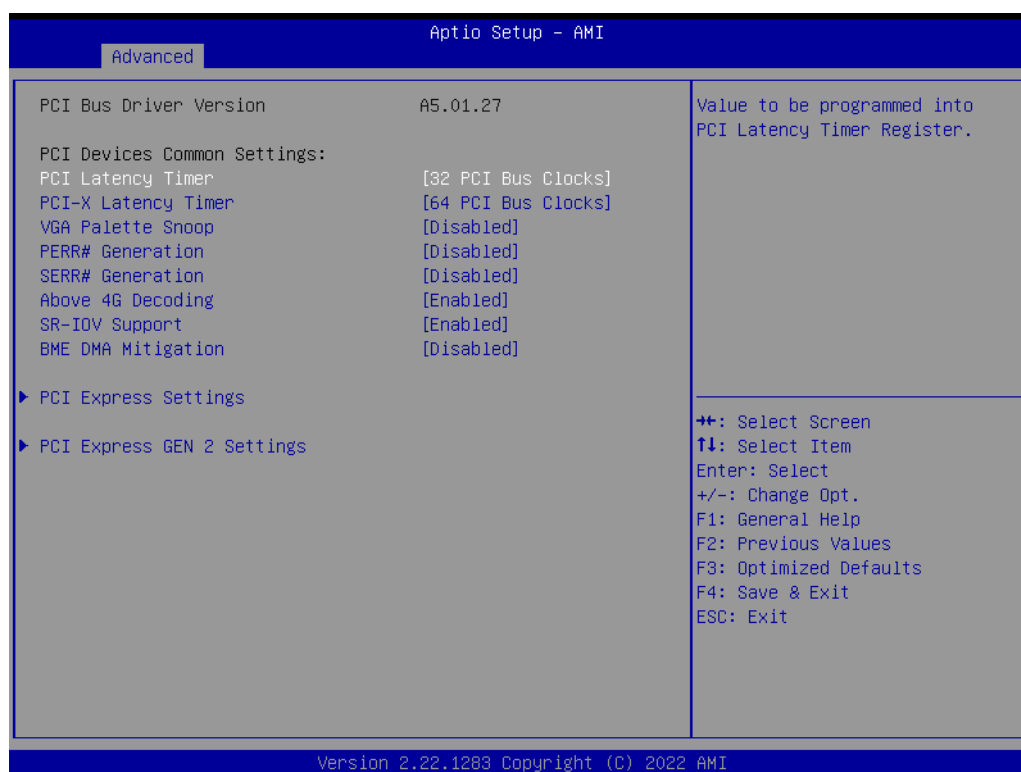


Figure 3.12 PCI Subsystem Settings

- **PCI Latency Timer**
Value to be programmed into the PCI Latency Timer Register.
- **PCI-X Latency Timer**
Value to be programmed into the PCI Latency Timer Register.
- **VGA Palette Snoop**
Enable or Disable VGA Palette Register Snooping.
- **PERR# Generation**
Enable or Disable PCI Device to Generate PERR#.
- **SERR# Generation**
Enable or Disable PCI Device to Generate SERR#.
- **Above 4G Decoding**
Enable or Disable 64-bit capable devices to be decoded in the above 4G address space (Only if the system supports 64-bit PCI decoding).
- **SR-IOV Support**
If the system has SR-IOV capable PCIe devices, this option Enables or Disables single root IO Virtualization support.
- **BME DMA Mitigation**
Re-enable Bus Master Attribute if disabled during PCI enumeration for PCI Bridges after SMM Locked.
- **PCI Express Settings**
Changes PCI Express device settings.
- **PCI Express GEN 2 Settings**
Changes PCI Express GEN device settings.

3.4.5.1 PCI Express Settings

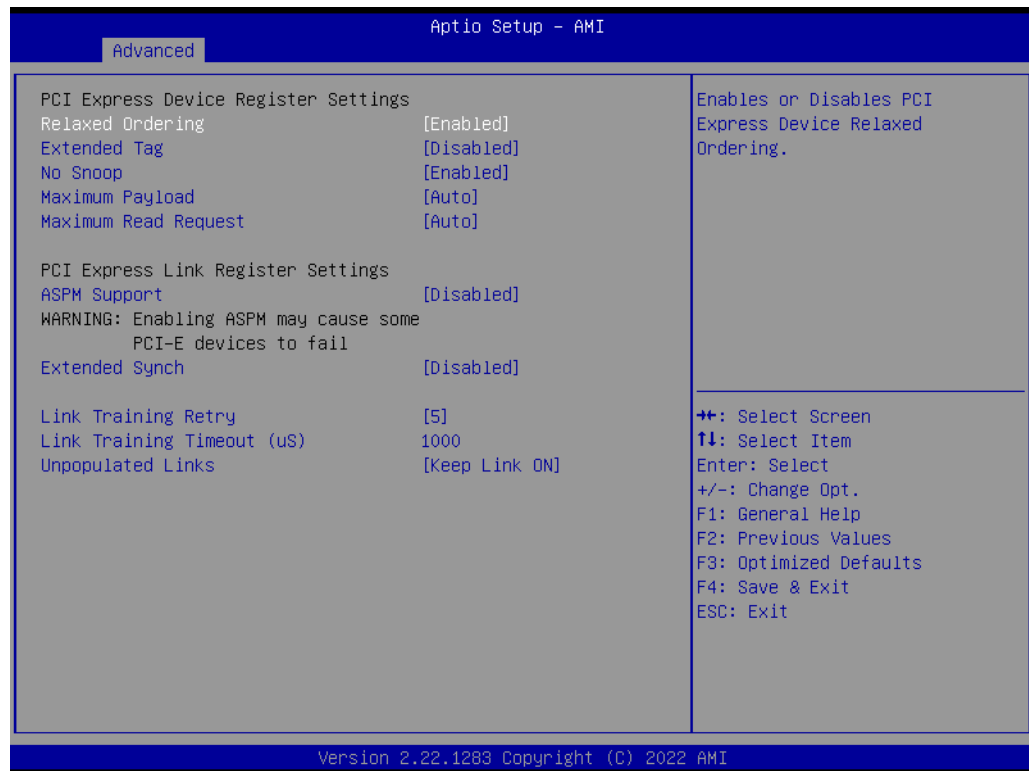


Figure 3.13 PCI Express Settings

- **Relaxed Ordering**
Enables or Disables PCI Express Device Relaxed Ordering.
- **Extended Tag**
If Enabled, it allows the device to use an 8-bit Tag field as a requester.
- **No Snoop**
Enables or Disables the PCI Express device No Snoop option.
- **Maximum Payload**
Set Maximum Payload of the PCI Express device or allow System BIOS to select the value.
- **Maximum Read Request**
Set Maximum Read Request Size of the PCI Express device or allow System BIOS to select the value.
- **ASPM Support**
Set the ASPM Level: Force L0s-Force all links to L0s State AUTO-BIOS auto configure DISABLE-Disables ASPM.
- **Extended Synch**
If Enabled, it allows generation of Extended Synchronization patterns.
- **Link Training Retry**
Defines number of Retry Attempts software will take to retrain the link if previous training attempts were unsuccessful.
- **Link Training Timeout (uS)**
Defines the numbers of microseconds software will wait before polling the 'Link Training' bit in the Link Status register. Values range from 10 to 10000 uS.
- **Unpopulated Links**
In order to save power, software will disable unpopulated PCI Express links if this option set to 'Disable Link'.

3.4.5.2 PCI Express GEN 2 Settings

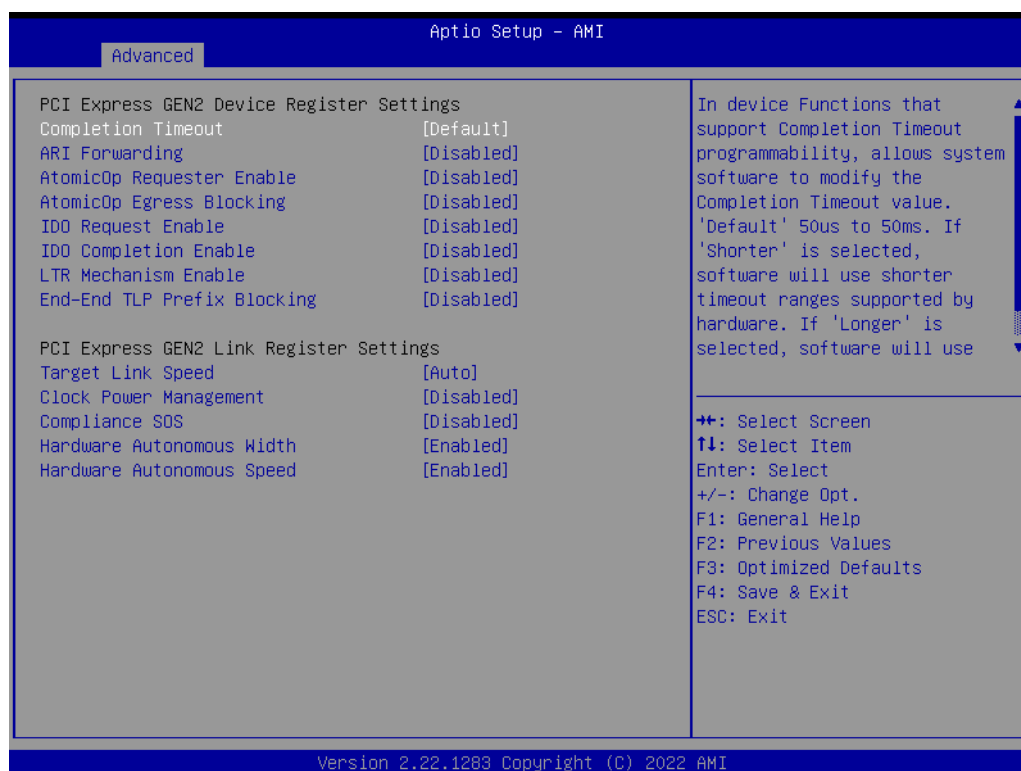


Figure 3.14 PCI Express GEN 2 Settings

- **Complete Timeout**
For device functions that support Completion Timeout programmability, it allows system software to modify the Completion Timeout value. The 'Default' is 50us to 50ms. If 'Shorter' is selected, software will use shorter timeout ranges supported by hardware. If 'Longer' is selected, software will use longer timeout ranges.
- **ARI Forwarding**
If supported by hardware and set to 'Enabled', the Downstream Port disables its traditional Device Number field with 0 enforcement when turning a Type1 Configuration Request into a Type0 Configuration Request, permitting access to Extended Functions in an ARI Device immediately below the Port. Default value: Disabled.
- **AtomicOp Requester Enable**
If supported by hardware and set to 'Enabled', this function initiates AtomicOp Requests only if the Bus Master Enable bit is in the Command Register Set.
- **AtomicOp Egress Blocking**
If supported by hardware and set to 'Enabled', outbound AtomicOp Requests via Egress Ports will be blocked.
- **IDO Request Enable**
If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (ID0) bit (Attribute [2]) requests to be initiated.
- **IDO Completion Enable**
If supported by hardware and set to 'Enabled', this permits setting the number of ID-Based Ordering (ID0) bit (Attribute [2]) requests to be initiated.
- **LTR Mechanism Enable**
If supported by hardware and set to 'Enabled', this enables the Latency Tolerance Reporting (LTR) Mechanism.

-
- **End-End TLP Prefix Blocking**
If supported by hardware and set to 'Enabled', this function will block forwarding of TLPs containing End-End TLP Prefixes.
 - **Target Link Speed**
If supported by hardware and set to 'Force to X.X GT/s' for Downstream Ports, this sets an upper limit on link operational speed by restricting the values advertised by the upstream component in its training sequences. When 'Auto' is selected, HW initialized data will be used.
 - **Clock Power Management**
If supported by hardware and set to 'Enabled', the device is permitted to use the CLKREQ# signal for power management of the link clock in accordance with protocol defined in the appropriate form factor specification.
 - **Compliance SOS**
If supported by hardware and set to 'Enabled', this will force LTSSM to send SKP Ordered Sets between sequences when sending a Compliance Pattern or Modified Compliance Pattern.
 - **Hardware Autonomous Width**
If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation.
 - **Hardware Autonomous Speed**
If supported by hardware and set to 'Disabled', this will disable the hardware's ability to change link speed except speed rate reduction for the purpose of correcting unstable link operation.

3.4.6 USB Configuration

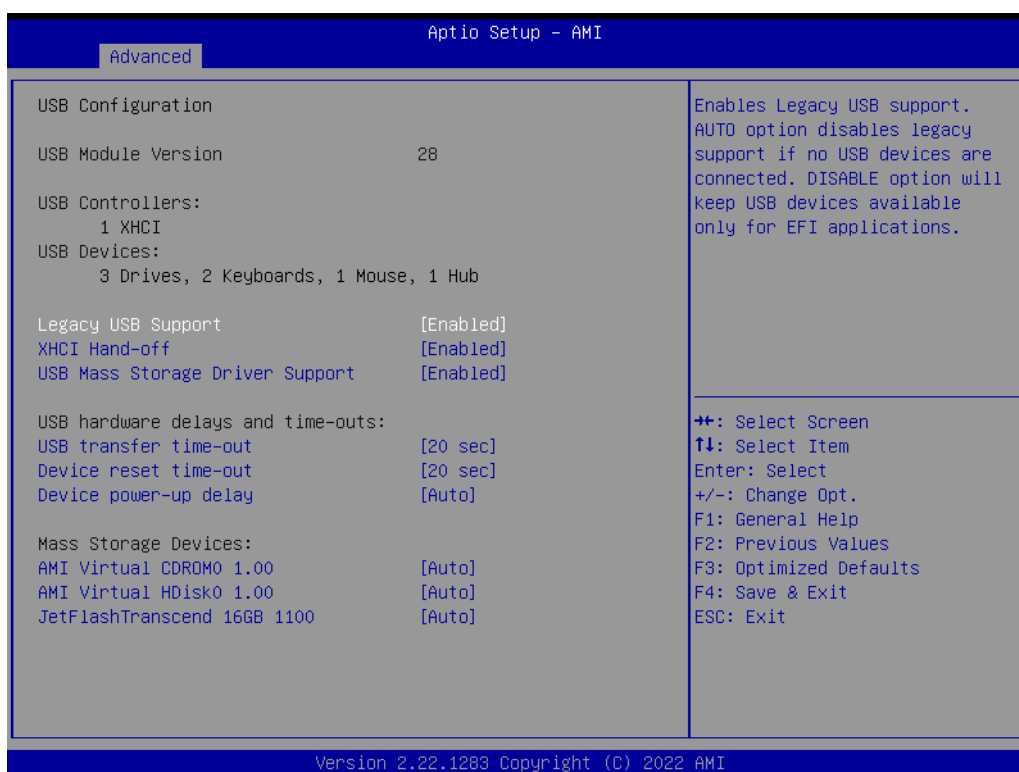


Figure 3.15 USB Configuration

- **Legacy USB Support**
Enables Legacy USB support. The Auto option disables legacy support if no USB devices are connected. The Disable option will keep USB devices available only for EFI applications.
- **XHCI Hand-off**
This is a workaround for OS without XHCI hand-off support. The XHCI ownership change should be claimed by the XHCI driver.
- **USB Mass Storage Driver Support**
Enable/Disable USB Mass Storage Driver Support.
- **USB transfer time-out**
This is 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.
- **AMI Virtual CDROM 1.00**
- **AMI Virtual HDISK0 1.00**

3.4.7 Network Stack Configuration

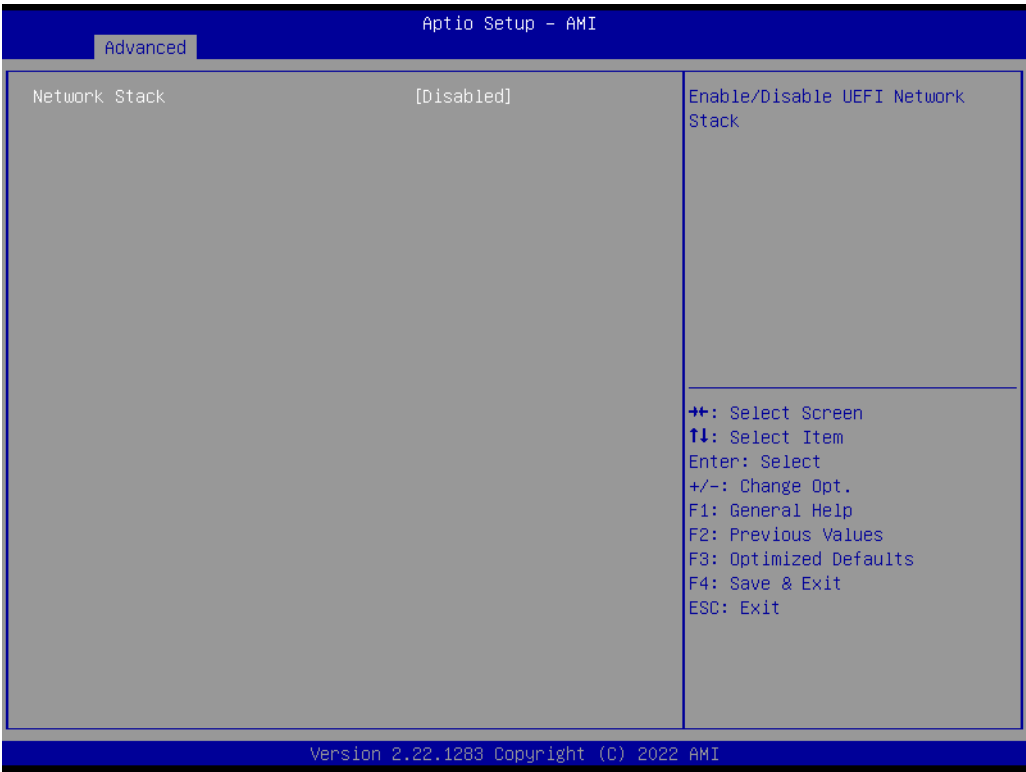


Figure 3.16 Network Stack Configuration

- **Network Stack**
Enable/Disable UEFI Network Stack.

3.4.8 NVMe Configuration

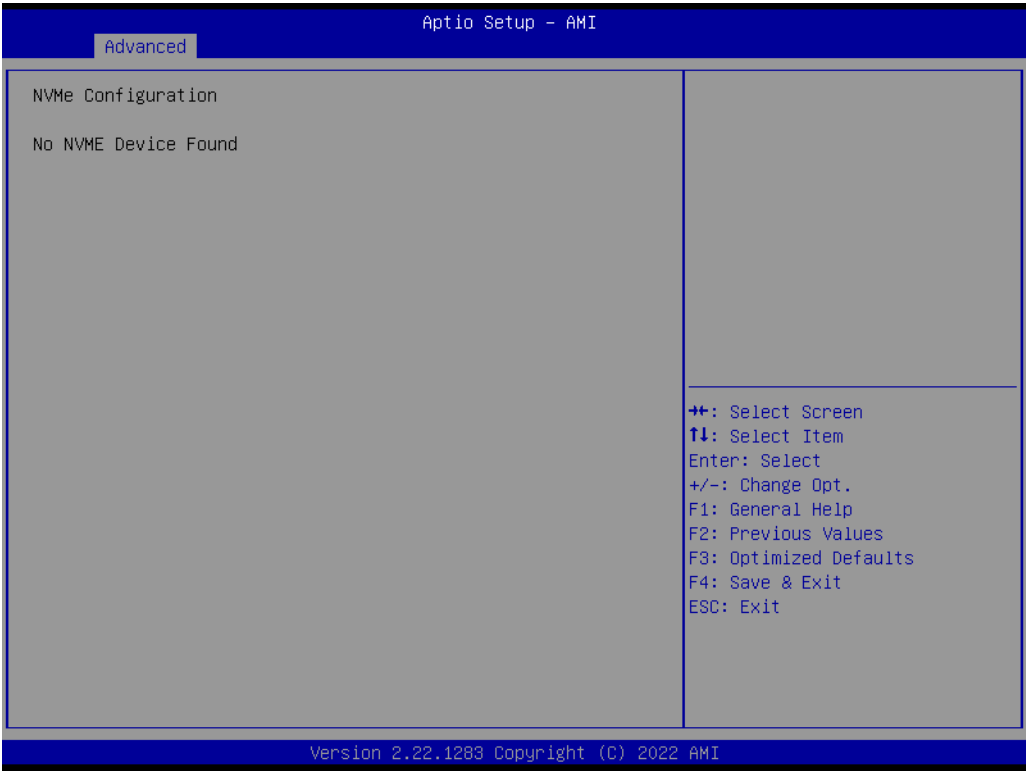


Figure 3.17 NVMe Configuration

3.5 Chipset

Select the Chipset tab from the SOM-5993 setup screen to enter the BIOS Setup screen. You can select the items by highlighting them using the <Arrow> keys. All Plug and Play BIOS Setup options are described in this section. The Plug and Play BIOS Setup screen is shown below. It provides the option to change the Processor Settings.



Figure 3.18 Chipset

- **Socket Configuration**
Displays and provides the option to change the Socket Settings.
- **Platform Configuration**
Press <Enter> to select the Platform System Setup options.

3.5.1 Socket Configuration

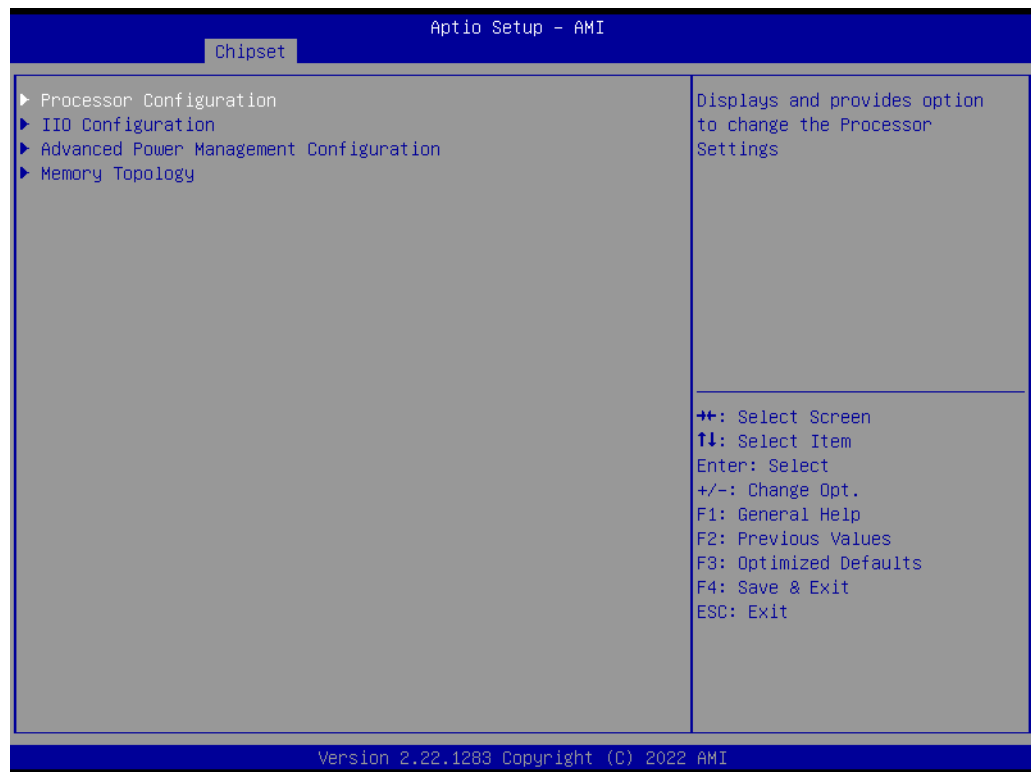


Figure 3.19 Socket Configuration

- **Processor Configuration**
Displays and provides the option to change the Processor Settings.
- **IIO Configuration**
Displays and provides the option to change the IIO Settings.
- **Advanced Power Management Configuration**
Displays and provides the option to change the Power Management Settings.
- **Memory Topology**
Displays memory topology with DIMM population information.

3.5.1.1 Processor Configuration



Figure 3.20 Processor Configuration

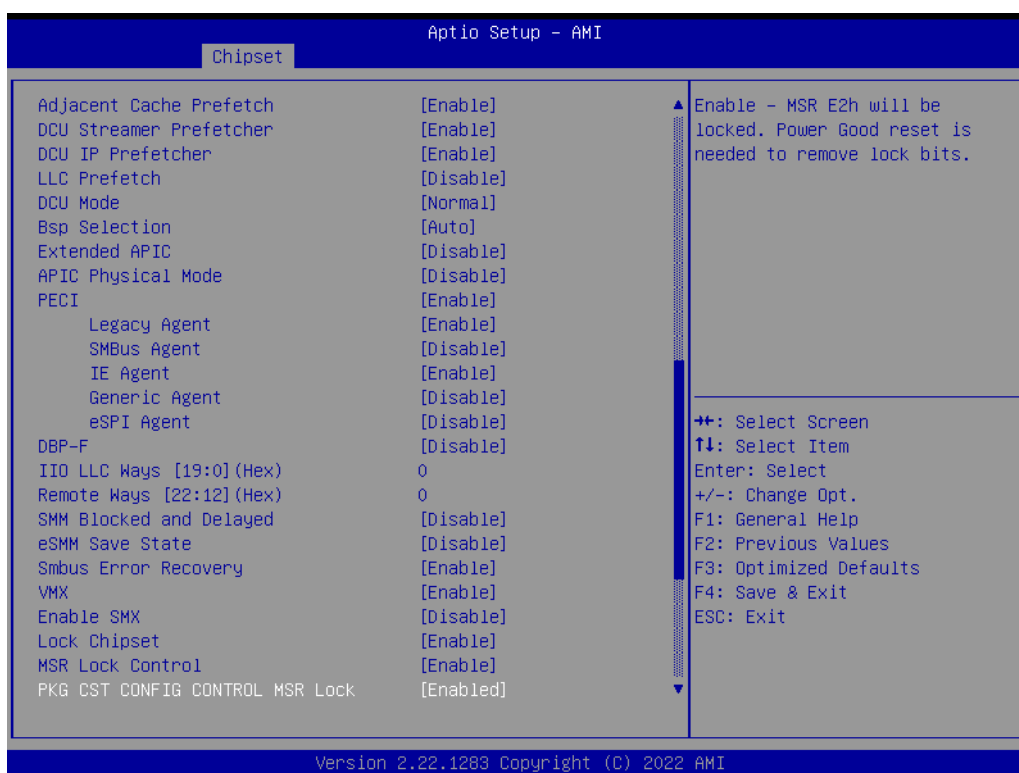


Figure 3.21 Processor Configuration

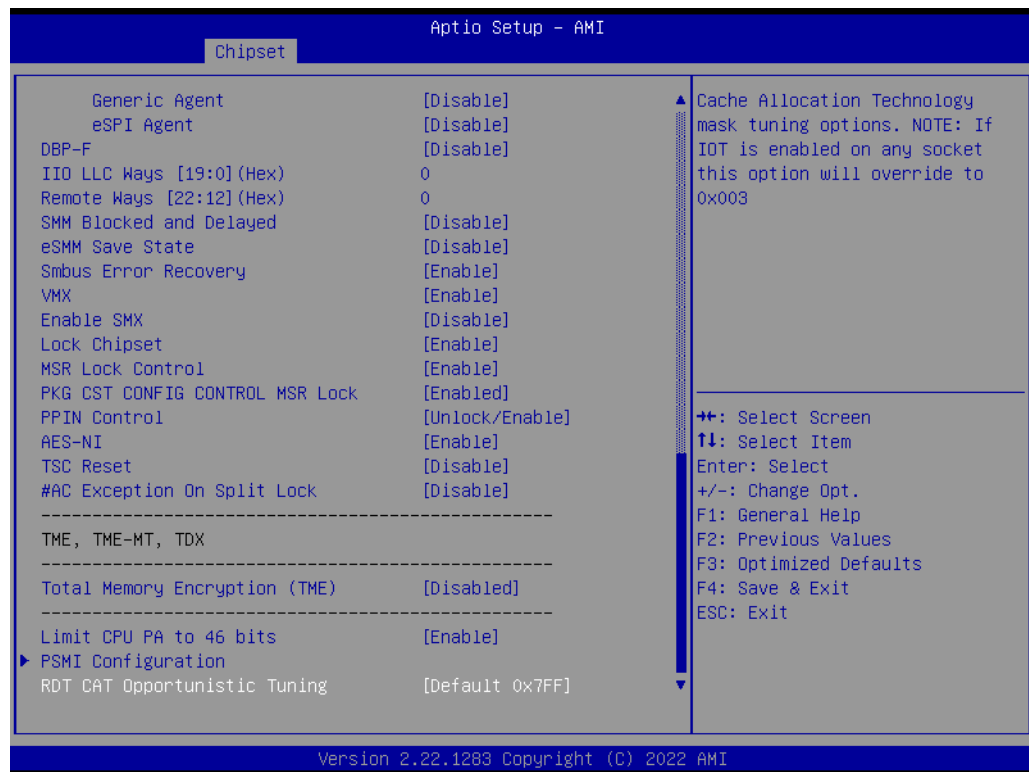


Figure 3.22 Processor Configuration

- **Per-Socket Configuration**
Change Per-Socket Settings.
- **Hyper-Threading [ALL]**
Enables Hyper-Threading (Software Method to Enable/Disable Logical Processor threads).
- **IED Trace memory**
Options to allocate memory for PSMI trace.
- **Skip Flex Ratio Override**
Skip Flex Ratio overrides to use power-on default Flex Ratio values. In multi-socket systems, this will allow mixed flex ratio limits.
- **Check CPU BIST Result**
Disable failed BIST core when enabled, otherwise, ignore the BIST result.
- **3StrikerTimer**
The 3 strike counter can be turned off by writing into the MISC_FEATURE_CONTROL_DISABLE_THREE_STRIKE_CNT(MSR 0x01a4).
- **Fast String**
When enabled, enable fast strings for REP MOVSt/STOS.
- **Machine Check**
Enable or Disable the Machine Check.
- **Max CPUID Value Limit**
This should be enabled in order to boot legacy OS that cannot support CPUs with extended CPUID functions.
- **Hardware Prefetcher**
= MLC Streamer Prefetcher (MSR 1A4h Bit [0]).
- **Adjacent Cache Prefetch**
=MLC Spatial Prefetcher (MSR 1A4h Bit [1]).

- **DCU Streamer Prefetcher**
DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).
- **DCU IP Prefetcher**
DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).
- **LLC Prefetcher**
Enable/Disable LLC Prefetch on all threads.
- **DCU Mode**
Normal: The whole DCU is used for caching; Mirror-Mode: DCU is organized as 2x16KB mirrored copies.
- **Bsp Selection**
Choose the method to select BSP.
- **Extended APIC**
Enable/disable extended APIC support. Note: This will enable VT-d automatically if x2APIC is enabled.
- **APIC Physical Mode**
Enable/Disable the APIC physical destination mode.
- **PECI**
PECI in trust bit enable.
- **Legacy Agent**
Legacy Peci agent in trust bit enable.
- **SMBus Agent**
SMBus Peci agent in trust bit enable.
- **IE Agent**
IE Peci agent in trust bit enable.
- **Generic Agent**
Generic Peci agent in trust bit enable.
- **eSPI Agent**
ESPI Peci agent in trust bit enable.
- **DBP-F**
The DBP-F can be turned off by writing into the (MSR 792h [5:6] for CLX, CPX, and MSR 6Dh// [2:3] for ICX).
- **IIO LLC Ways [19:0] (Hex)**
MSR CB0_SLICE0_CR_IIO_LLC_WAYS bitmask.
- **Remote Ways [22:12] (Hex)**
MSR INGRESS_SPARE bitmask [26:16], Value 0 means no override.
- **SMM Blocked and Delayed**
Enable/Disable SMM Blocked and Delayed.
- **eSMM Save State**
Enable or Disable the eSMM Save State Feature.
- **Smbus Error Recovery**
Enable or Disable Smbus Error Recovery.
- **VMX**
Enables Vanderpool Technology. It takes effect after reboot.
- **Enable SMX**
Enables Safer Mode Extensions.
- **Lock Chipset**
Lock or Unlock the chipset.
- **MSR Lock Control**
Enable – MSR 3Ah and CSR 80h will be locked. Power Good reset is needed to remove lock bits.

- **PKG CST CONFIG CONTROL MSR Lock**
Enable – MSR E2h will be locked. Power Good reset is needed to remove lock bits.
 - **PPIN Control**
Unlock and Enable/Disable PPIN Control.
 - **AES-NI**
Enable/disable AES-NI support.
 - **TSC Reset**
Enable or Disable TSC reset during a warm reboot.
 - **#AC Exception On Split Lock**
Enable or Disable #AC (Alignment Check) Exception On Split Lock.
 - **Total Memory Encryption (TME)**
Enable/Disable Total Memory Encryption (TME).
 - **Limit CPU PA to 46 bits**
Limit the CPU physical address to 46 bits to support older Hyper-v. If enabled, it automatically disables TME-MT.
 - **PSMI Configuration**
PSMI Configuration.
 - **RDT CAT Opportunistic Tuning**
Cache Allocation Technology mask turning options. NOTE: If IOT is enabled on any socket, this option will override to 0x003.
- **Per-Socket Configuration**



Figure 3.23 Per-Socket Configuration

■ CPU Socket 0 Configuration

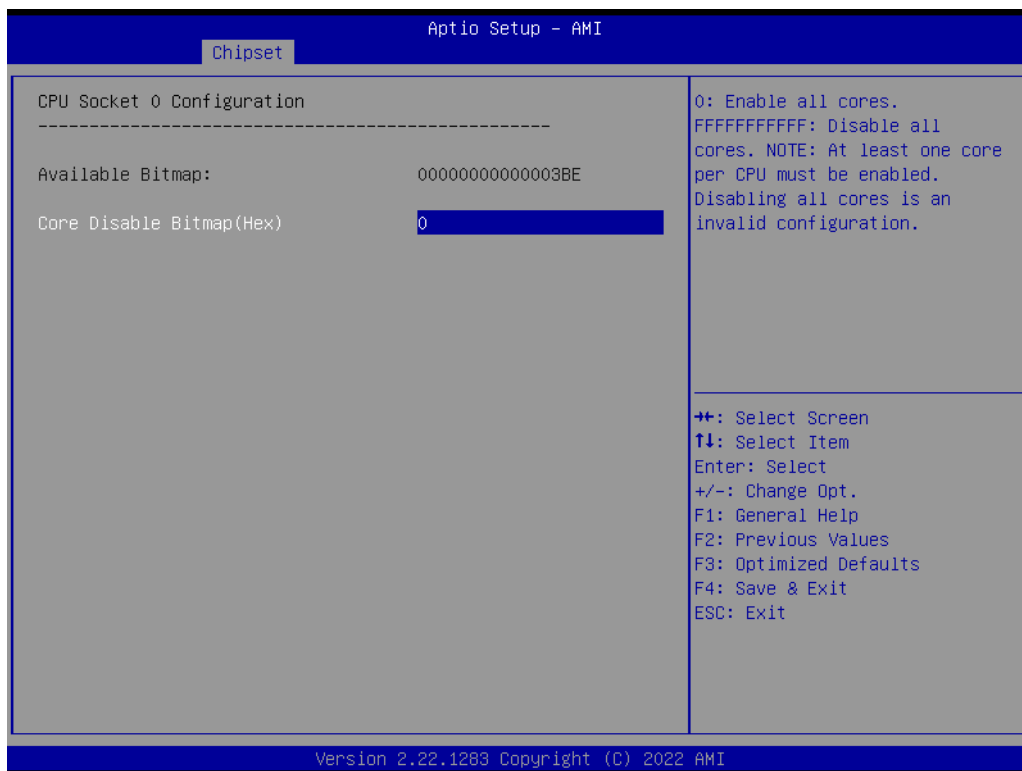


Figure 3.24 CPU Socket 0 Configuration

■ Core Disable Bitmap (Hex)

0: Enable all cores. FFFFFFFFFF: Disable all cores. NOTE: At least one core per CPU must be enabled. Disabling all cores is an invalid configuration.

■ PSMI Configuration

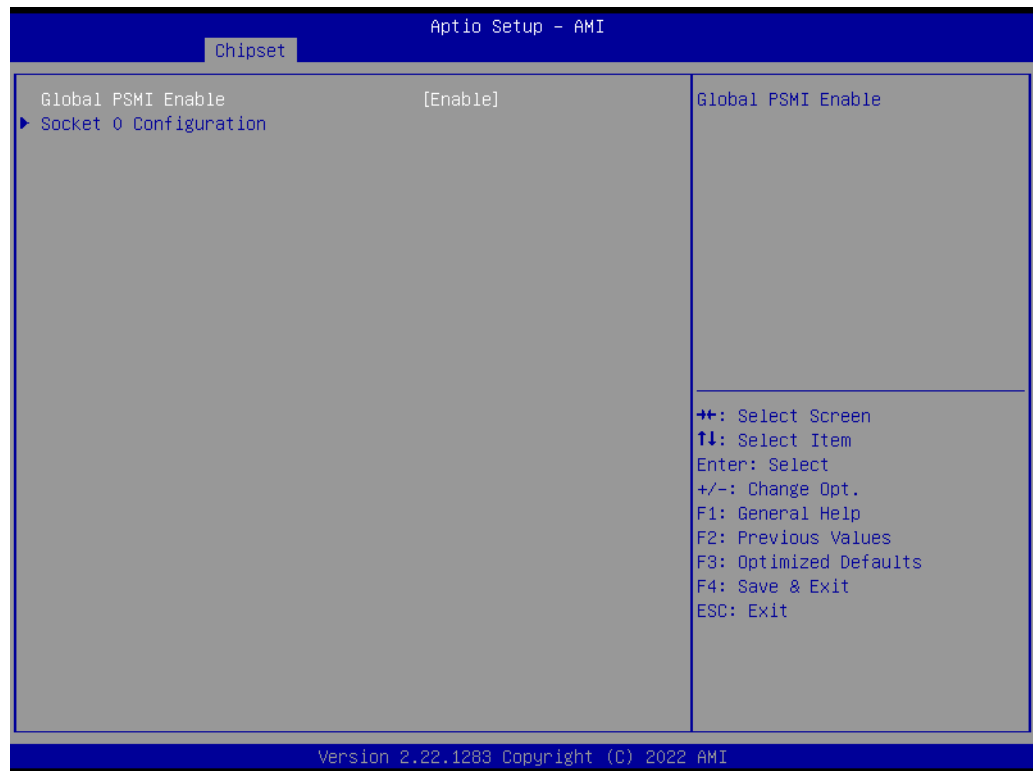


Figure 3.25 PSMI Configuration

- **Global PSMI Enable**
Global PSMI Enable.
- **Socket 0 Configuration**

Socket 0 Configuration

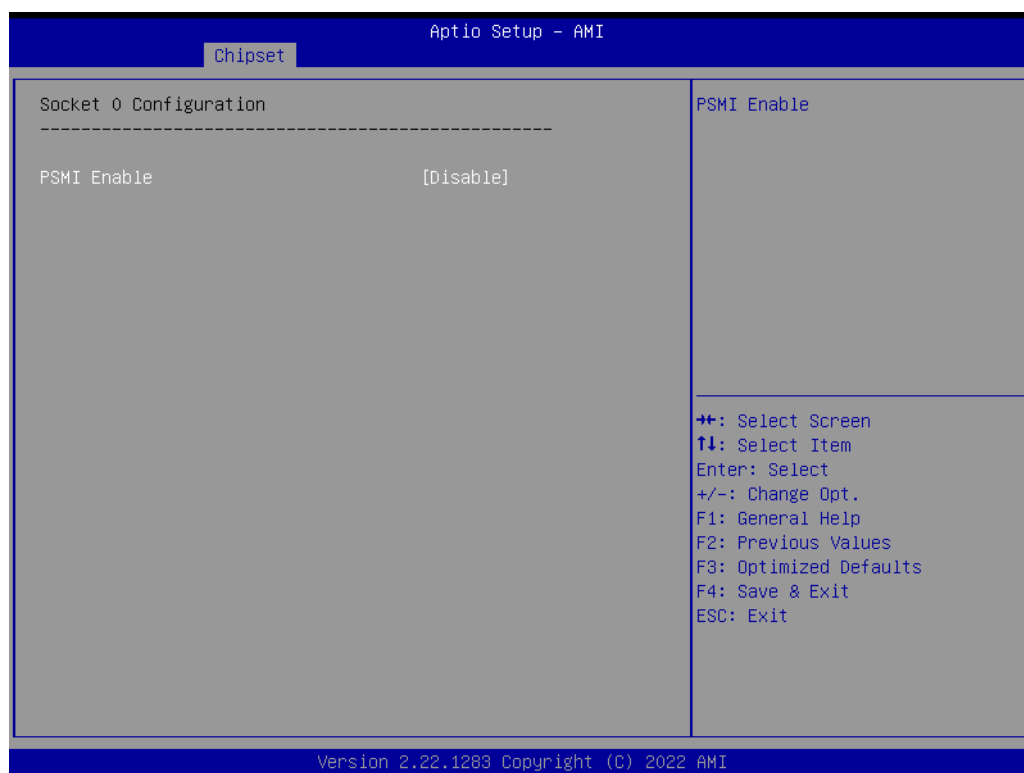


Figure 3.26 Socket 0 Configuration

- **PSMI Enabled**

3.5.1.2 IIO Configuration

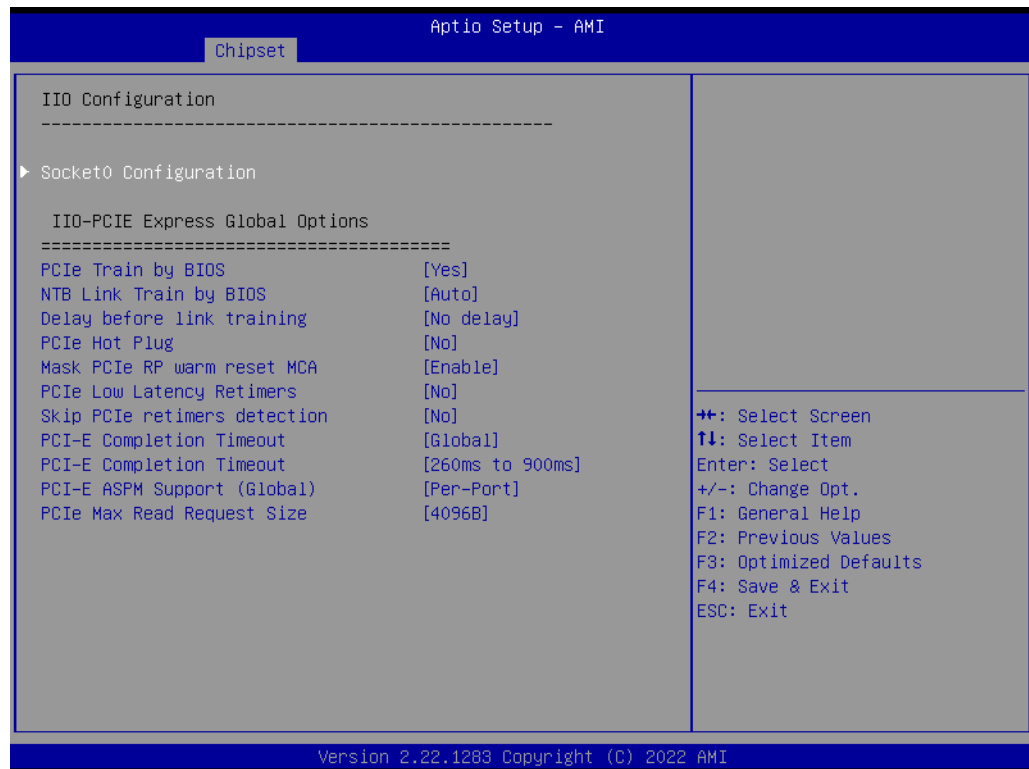


Figure 3.27 IIO Configuration

- **Socket0 Configuration**
- **PCIe Train by BIOS**
Assume IIO is strapped for wait-for-BIOS because straps are unreliable in A-0 Silicon.
- **NTB Link Train by BIOS**
This knob enables or disables the BIOS to train the NTB links.
- **Delay before link training**
Custom delay before PCIe link training on IIO ports.
- **PCIe Hot Plug**
Enable/Disable PCIe Hot Plug globally.
- **Mask PCIe RP warm reset MCA**
Enable/Disable Mask CPU Complex PCIe Root Port warm reset MCA.
- **PCIe Low Latency Retimers**
Enable/Disable PCIe low Latency retimers.
- **Skip PCIe retimers detection**
Skip PCIe retimers detection to speedup the boot.
- **PCI-E Completion Timeout**
Configure PCIe Completion Timeout in Device Control2 register.
- **PCI-E Completion Timeout [260ms to 900ms]**
Configure PCIe Completion Timeout in Device Control2 register.
- **PCI-E ASPM Support (Global)**
This option can disable ASPM support in all PCIe root ports.
- **PCIe Max Read Request Size**
This option can set the requested Max Read Request Size in the PCI Hierarchy. 'Default' keeps the hardware default.

■ Socket0 Configuration



Figure 3.28 Socket0 Configuration

- **IOU0 (IIO PCIe Port 1)**
Selects PCIe port Bifurcation for selected slot(s).
- **Sck0 RP Correctable Err**
Applies to root ports only. Enable interrupt on correctable errors.
- **Sck0 RP NonFatal Uncorrectable Err**
Applies to root ports only. Enable interrupt on a non-fatal error.
- **Sck0 RP Fatal Uncorrectable Err**
Applies to root ports only. Enable MSI/INTx interrupt on fatal errors.
- **TraceHub Configuration Menu**
TraceHub Configuration Settings.
- **R-Link**
Settings related to PCI Express Ports(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).
- **Port 1A**
Settings related to PCI Express Ports(0/1A/1B/1C/1D/2A/2B/2C/2D/3A/3B/3C/3D/4A/4B/4C/4D/5A/5B/5C/5D).

TraceHub Configuration Menu

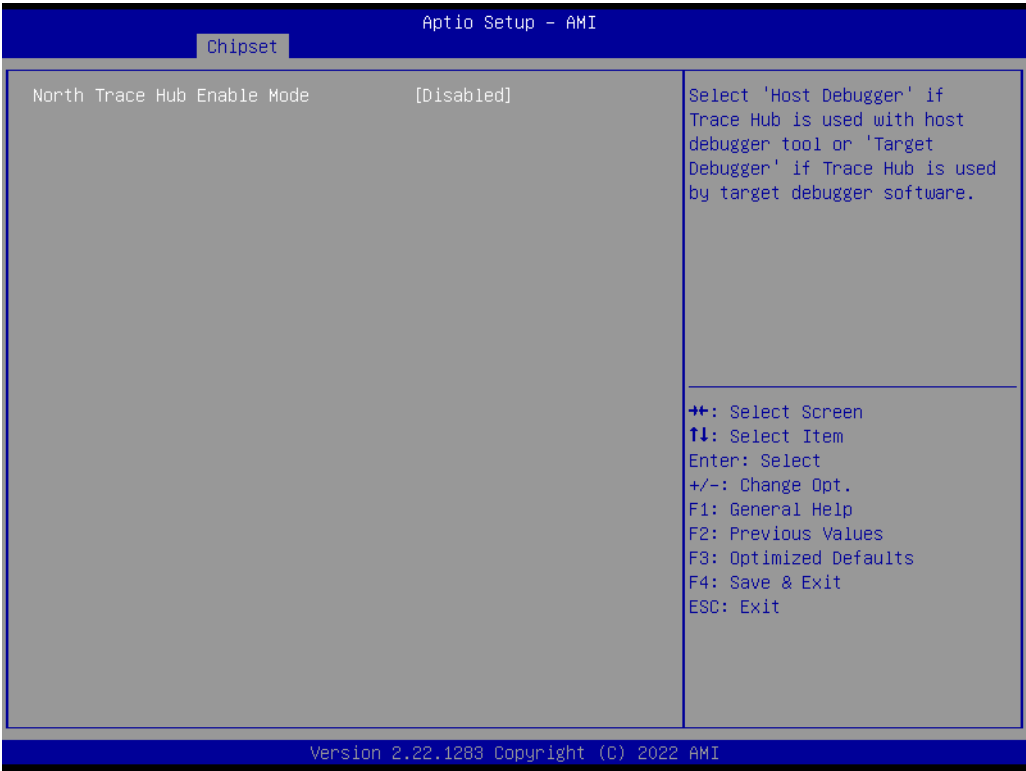


Figure 3.29 TraceHub Configuration Menu

- **North Trace Hub Enable Mode**
Select 'Host Debugger' if Trace Hub is used with the host debugger tool or 'Target Dubugger' if Trace Hub is used by target debugger software.

■ R-Link

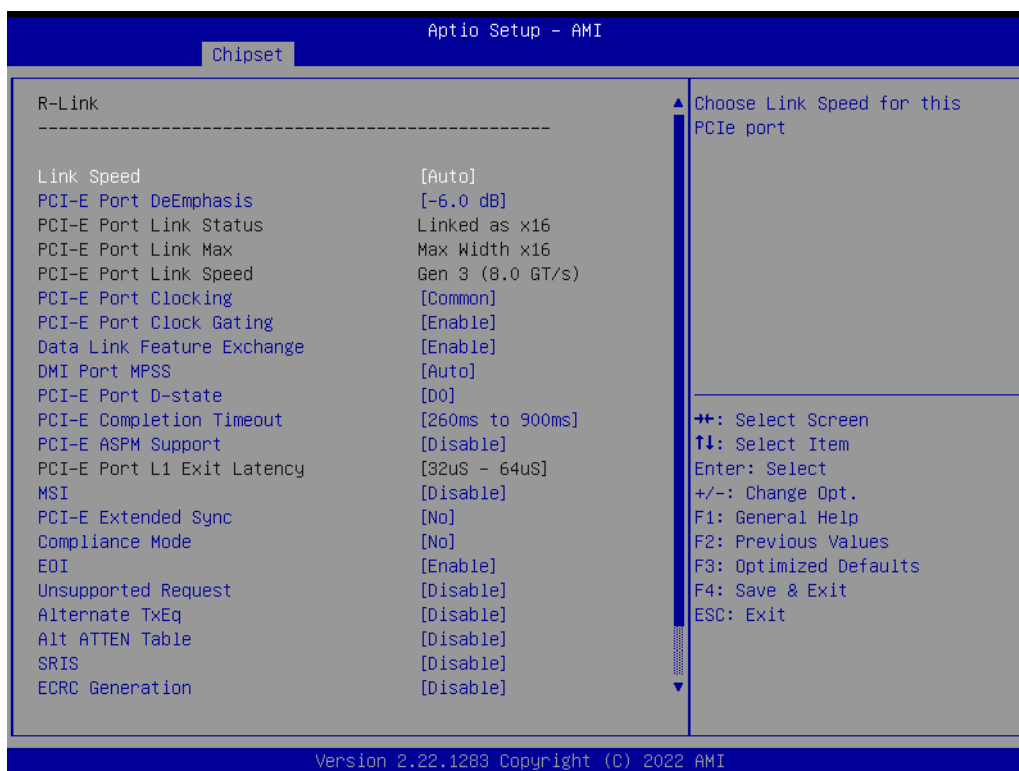


Figure 3.30 R-Link

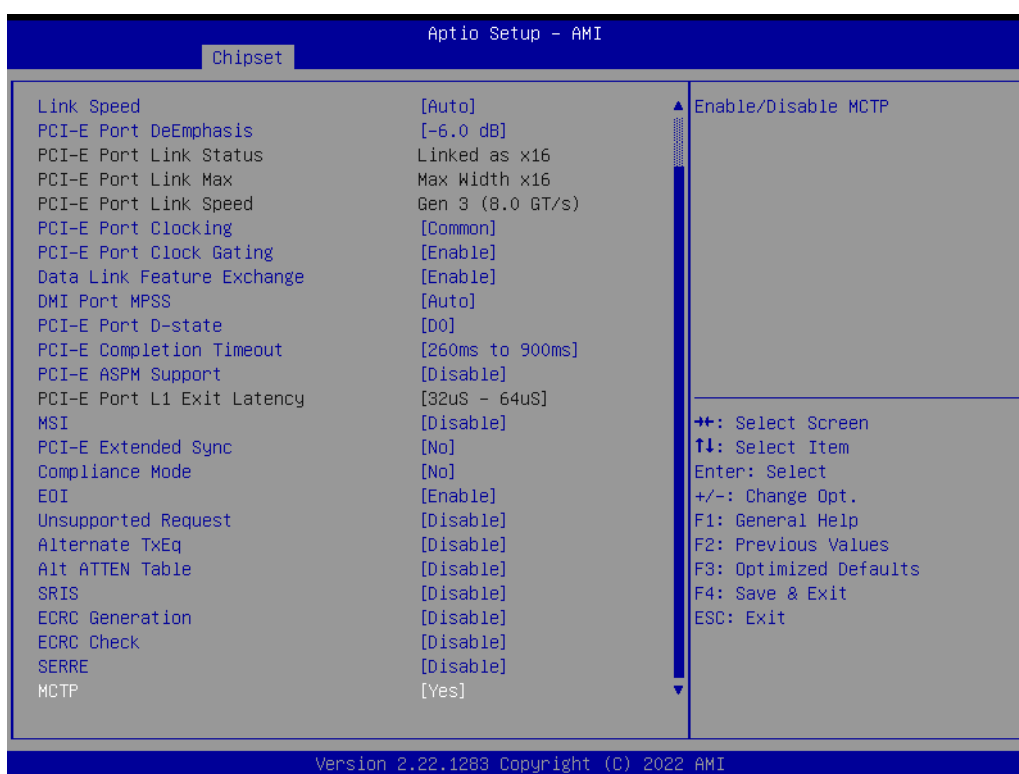


Figure 3.31 R-Link

■ Link Speed

Choose Link Speed for this PCIe port.

- **PCI-E Port DeEmphasis**
De-Emphasis control (LNKCON2[6]) for this PCIe port.
- **PCI-E Port Clocking**
Configure port clocking via LNKCON[6]. This refers to the components and the downstream component.
- **PCI-E Port Clock Gating**
Enable/Disable Clock Gating for this PCIe port.
- **Data Link Feature Exchange**
Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
- **DMI Port MPSS**
Configure Max Payload Size Supported in DMI Device Capabilities register. 'Auto' keeps the hardware default. If 'Auto' is not used, make sure MPSS in PCH root ports is updated to the same or smaller value.
- **PCI-E Port D-state**
Set to D0 for normal operation. D3Hot to be in low-power state.
- **PCI-E Completion Timeout**
Configure PCIe Completion Timeout in Device Control2 register.
- **PCI-E ASPM Support**
This option can disable ASPM support in a PCIe root port. 'Auto' keeps the hardware default.
- **MSI**
BUS0 DEVx FUN0 OFF 0x5A bit 0, where X is 0-3.
- **PCI-E Extend Sync**
Enable/disable the Extended Sync Mode (D:x F:0 0:7Ch B:7) where x is 0-9.
- **Compliance Mode**
Enable/Disable Compliance Mode for this PCIe port.
- **EOI**
Dev 0,2,3 MISCCTRLSTS (Reg 0x188) Bit 26.
- **Unsupported Request**
Controls the reporting of unsupported requests that IIO itself detects on requests its receives from a PCI Express/DMI port.
- **Alternate TxEq**
Enable or Disable TxEq.
- **Alt ATTEN Table**
Enable/Disable Alternate Attenuator Table.
- **SRIS**
Enable or Disable SRIS.
- **ECRC Generation**
Enable or Disable ECRC Generation (Error Capabilities and Control Register).
- **ECRC Check**
Enable or Disable ECRC Check (Error Capabilities and Control Register).
- **SERRE**
Enable or Disable SERRE (SERR Reporting Enable).
- **MCTP**
Enable/Disable MCTP.

Port 1A

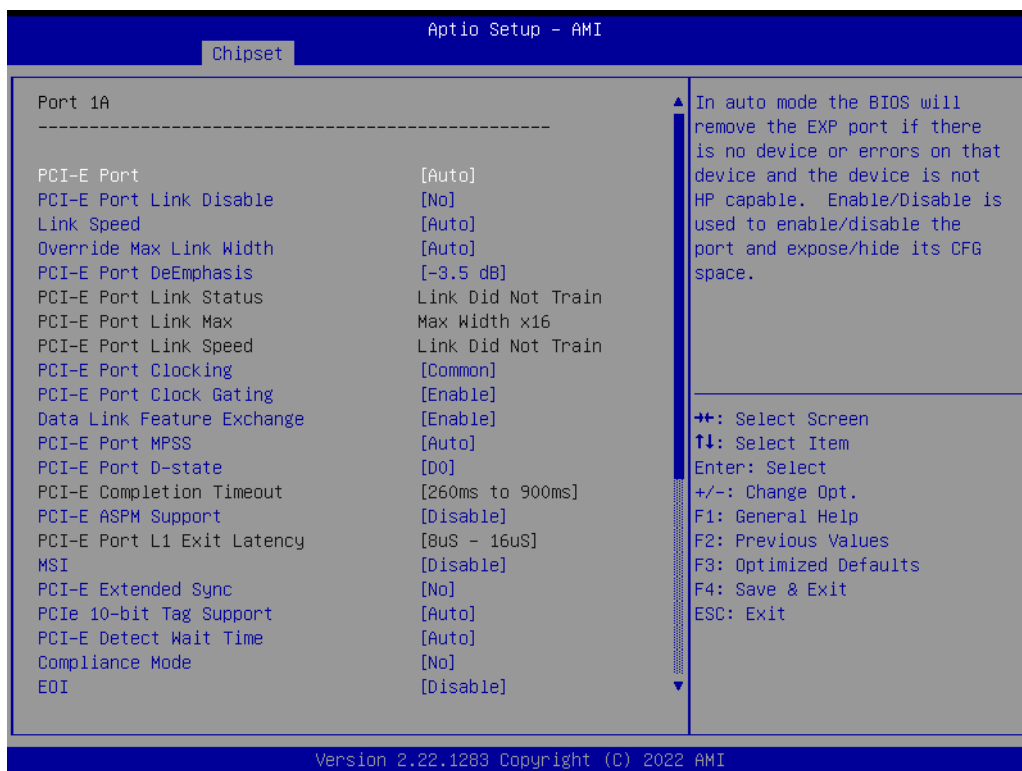


Figure 3.32 Port 1A

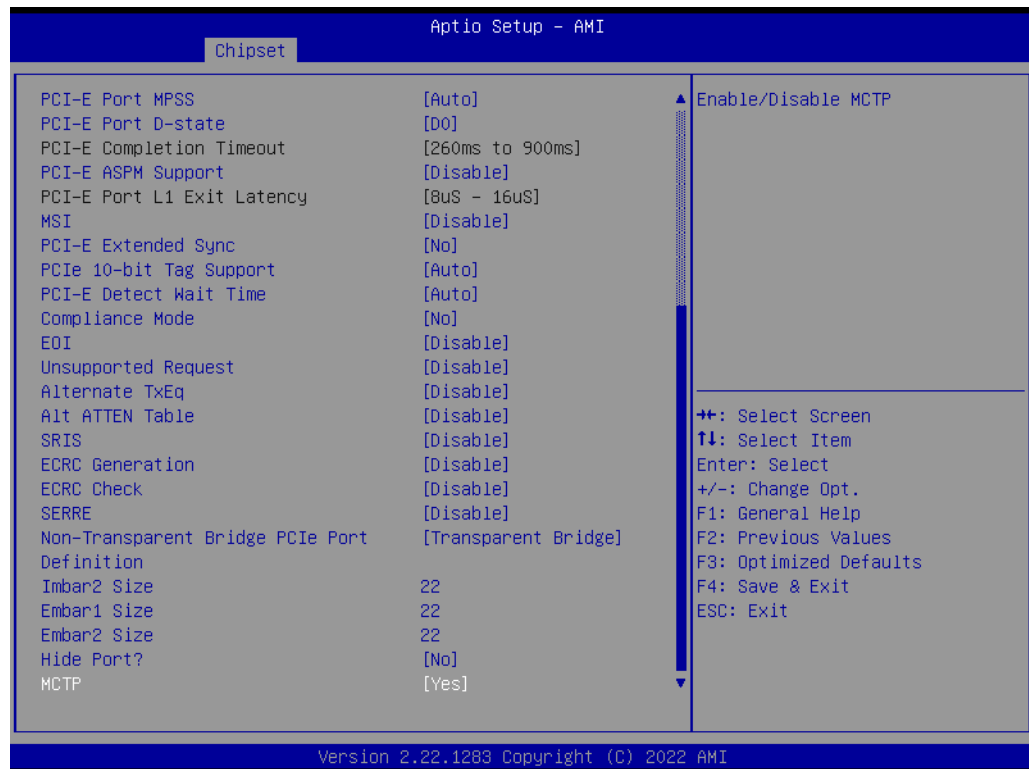


Figure 3.33 Port 1A

- **PCI-E Port**
In auto mode, the BIOS will remove the EXP port if there is no device or errors on that device and the device is not HP capable. Enable/Disable is used to enable/disable the port and expose/hide its CFG space.
- **PCI-E Port Link Disable**
This option disables the link so that the no training occurs but the CFG space is still active.
- **Link Speed**
Choose Link Speed for this PCIe port.
- **Override Max Link Width**
Override the max link width that was set by bifurcation.
- **PCI-E Port DeEmphasis**
De-Emphasis control (LNKCON2[6]) for this PCIe port.
- **PCI-E Port Clocking**
Configure port clocking via LNKCON[6]. This refers to this components and the downstream component.
- **PCI-E Port Clock Gating**
Enable/Disable Clock Gating for this PCIe port.
- **Data Link Feature Exchange**
Enable/Disable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register.
- **DMI Port MPSS**
Configure Max Payload Size Supported in PCIe Device Capabilities register. 'Auto' keeps the hardware default.
- **PCI-E Port D-state**
Set to D0 for normal operation, with D3Hot to be in low-power state.
- **PCI-E Completion Timeout**
- **PCI-E ASPM Support**

- This option can disable ASPM support in a PCIe root port. 'Auto' keeps the hardware default.
- **MSI**
BUS0 DEVx FUN0 OFF 0x5A bot 0, Where X is 0-3.
- **PCI-E Extend Sync**
Enable/Disable the Extended Sync Mode (D:z F:0 0:7Ch B:7) where x is 0-9.
- **PCIe 10-bit Tag Support**
The 'Disable' option can disable PCIe 10-bit Tag Requester support in a PCIe root port hierarchy. 'Auto' keeps the hardware default. Advanced users may use the 'Force Enable' option to enforce enabling the 10-bit Tag Requester in an hierarchy where the Root Port is 10-bit Tag Completer capable, but not all nodes support the 10-bit Tag Completer. The user assures there will be no peer to peer traffic from node with 10-bit Tag Requester capability to a node without 10-bit Tag Completer capability. In such an hierarchy, the 10-bit Tag Requester is not enabled in the Root Port regardless of Root Port capability.
- **PCI-E Detect Wait Time**
Set PCIe port TxRx detect polling.
- **Compliance Mode**
Enable/Disable Compliance Mode for this PCIe port.
- **EOI**
Dev 0,2,3 MISCCTRLSTS (Reg 0x188) Bit 26.
- **Unsupported Request**
Controls the reporting of unsupported requests that I/O itself detects on requests it receives from a PCI Express/DMI port.
- **Alternate TxEq**
Enable or Disable TxEq.
- **Alt ATTN Table**
Enable/Disable the Alternative Attenuator Table.
- **SRIS**
Enable or Disable SRIS.
- **ECRC Generation**
Enable or Disable ECRC Generation (Error Capabilities and Control Register).
- **ECRC Check**
Enable or Disable ECRC Check (Error Capabilities and Control Register).
- **SERRE**
Enable or Disable SERRE (SERR Reporting Enable).
- **Non-Transparent Bridge PCIe Port Definition**
[EMBAR1XBASE, EMBAR2XBASE] Configures port as TB, NTB-NTB, or NTB-RP (DON'T SELECT NTB-RP for legacy I/O on A0 Si!).
- **Imbar2 Size**
[IMBAR2SZ] Used to set the prefetchable Imbar2 size on primary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.
- **Embar1 Size**
[EMBAR1SZ] Used to set the prefetchable Embar1 size on secondary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.
- **Embar2 Size**
[EMBAR2SZ] Used to set the prefetchable Embar2 size on secondary side of NTB. Value range <12...51> representing BAR sizes <4KB...128PB>.
- **Hide Port**
The user can force to hide this root port from OS.
- **MCTP**
Enable/Disable MCTP.

3.5.1.3 Advanced Power Management Configuration

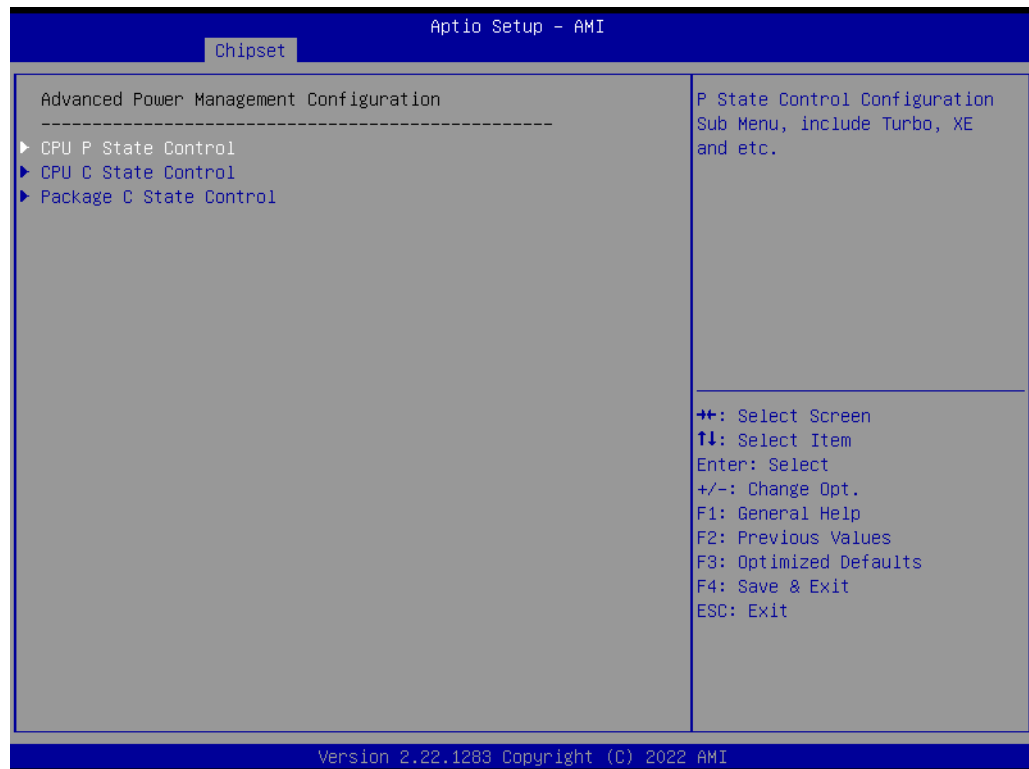


Figure 3.34 Advanced Power Management Configuration

- **CPU P State Control**
P State Control Configuration sub-menu, including Turbo, XE and etc.
- **CPU C State Control**
CPU C State setting.
- **Package C State Control**
Package C State setting.

■ CPU P State Control

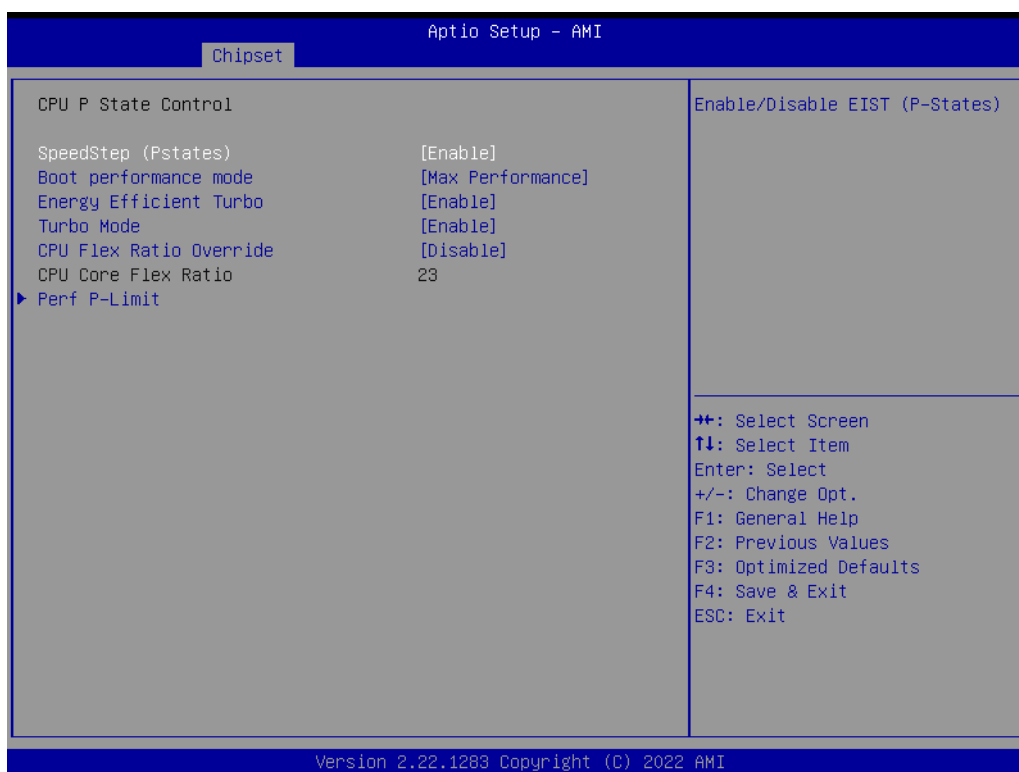


Figure 3.35 CPU P State Configuration

- **SpeedStep (Pstates)**
Enable/Disable EIST (P-States).
- **Boot performance mode**
Select the performance state that the BIOS will set before OS hand-off.
- **Energy Efficient Turbo**
Energy Efficient Turbo Disable, MSR 0x1FC [19].
- **Turbo Mode**
Enable/Disable processor Turbo Mode (requires EMTTM enabled too).
- **CPU Flex Ratio Override**
Enable/Disable CPU Flex Ratio Programming.
- **Perf P-Limit**
Program PERF_P_LIMIT 1:30:2:0xe4 sub-menu.

Perf P-Limit

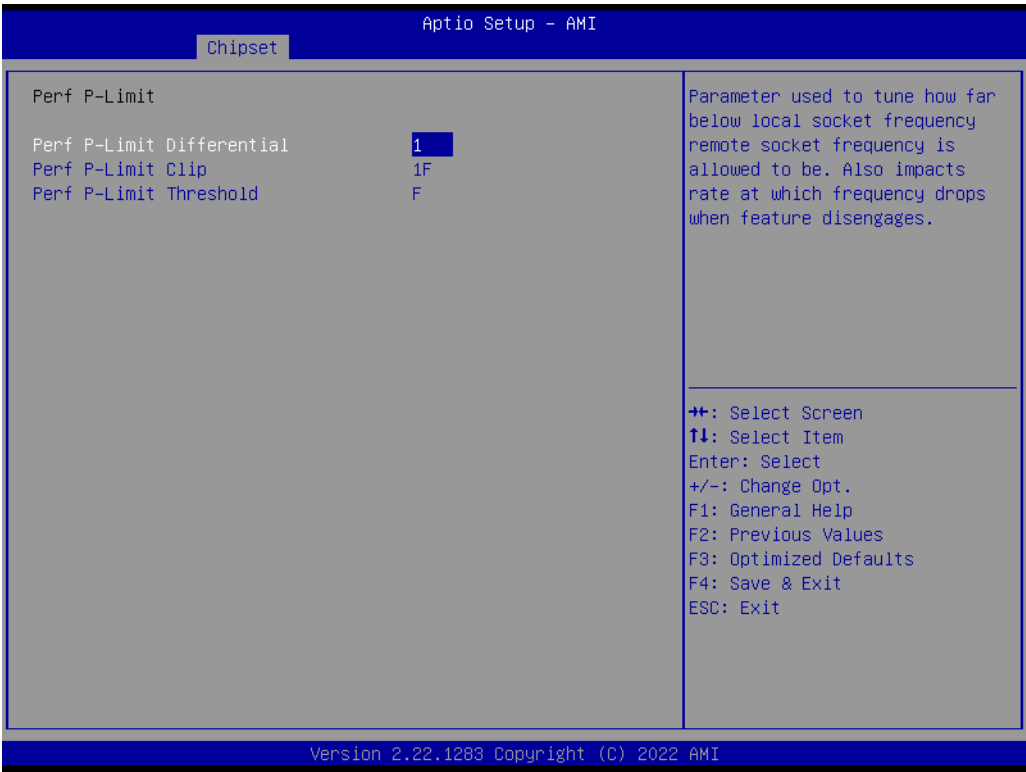


Figure 3.36 Perf P-Limit

- **Perf P-Limit Differential**
Parameter used to tune how far below local socket frequency remote socket frequency is allowed to be. It also impacts the rate at which frequency drops when the feature disengages.
- **Perf P-Limit Clip**
Maximum value the floor is allowed to be set to for Perf P-Limit.
- **Perf P-Limit Threshold**
Uncore frequency threshold above which this socket will trigger the feature and start trying to raise the frequency of other sockets.

■ CPU C State Control

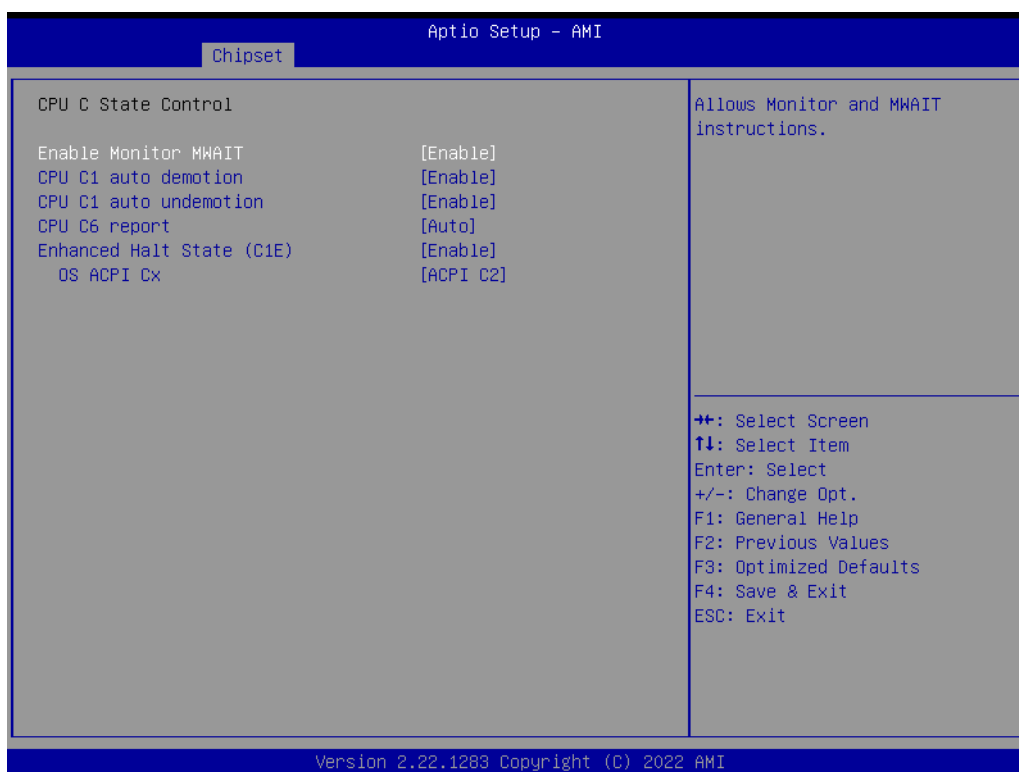


Figure 3.37 CPU C State Configuration

- **Enable Monitor MWAIT**
Allows Monitor and MWAIT instructions.
- **CPU C1 auto demotion**
Allows CPU to automatically demote to C1. Takes effect after reboot.
- **CPU C1 auto undemotion**
Allows CPU to be automatically undemoted from C1. It takes effect after reboot.
- **CPU C6 report**
Enable/Disable CPU C6 (ACPI C3) report to OS.
- **Enhanced Halt State (C1E)**
Core C1E auto promotion Control. Takes effect after reboot.
- **OS ACPI CX**
Report CC3/CC6 OS ACPI C2 or ACPI C3.

■ Package C State Control

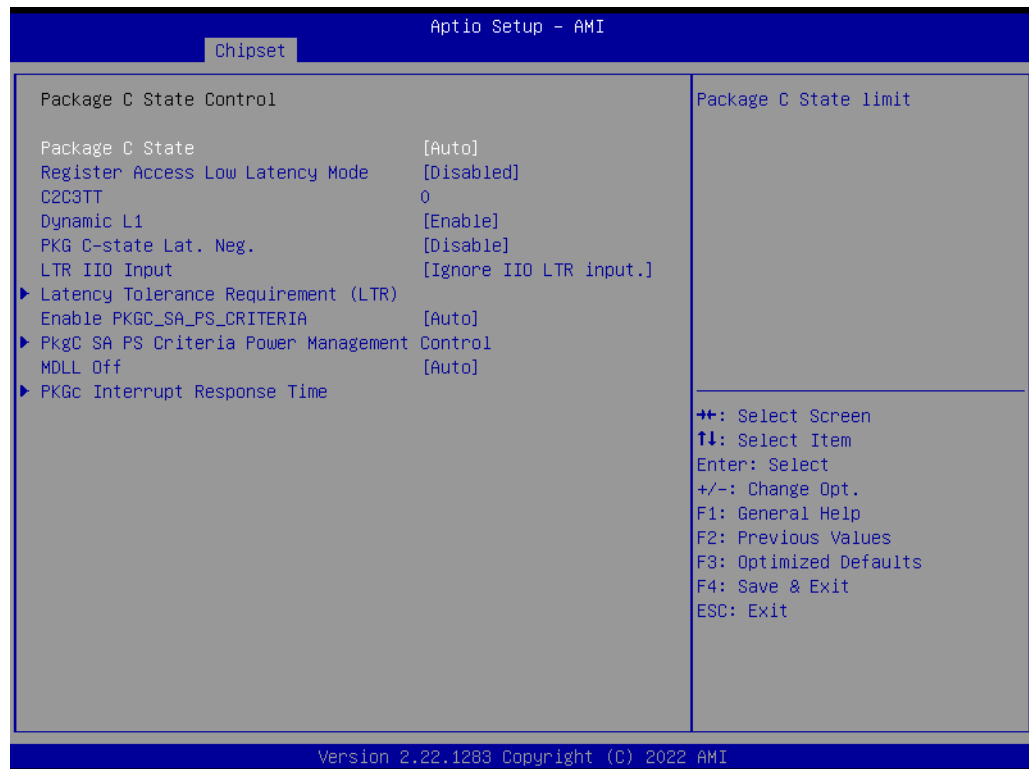


Figure 3.38 Package C State Control

- **Package C State**
Package C State limit.
- **Register Access Low Latency Mode [Disabled]**
Enable lower latency mode for register access. NOTE: Enabling this mode will prevent PkgC6 as register access fabric is prevented from going into idle.
- **C2C3TT**
Default = 0, means [AUTO]. C2 to C3 Transition Timer, PPDN_INIT = 1:10:1:74 Bit [11:0].
- **Dynamic L1**
PCU_MISC_CONFIG Bit [21] = dynamic L1 enable.
- **PKG C-state Lat. Neg.**
MSR 1FCh Bit [30] = PCH_NEG_DISABLE.
- **LTR IIO Input**
MSR 1FCh Bit [29] = LTR_IIO_DISABLE. Disable = Ignore IIO LTR input.
- **Latency Tolerance Requirement (LTR)**
Program PCIE_ILTR_OVRD 1:30:1:0xFC sub-menu.
- **PKGC SA PS Criteria Power Management Control**
Program WRITE_PKGC_SA_PS_CRITERIA sub-menu.
- **PKGc Interrupt Response Time**
Programmable Package C-state interrupt response time setup control.

Latency Tolerance Requirement (LTR)

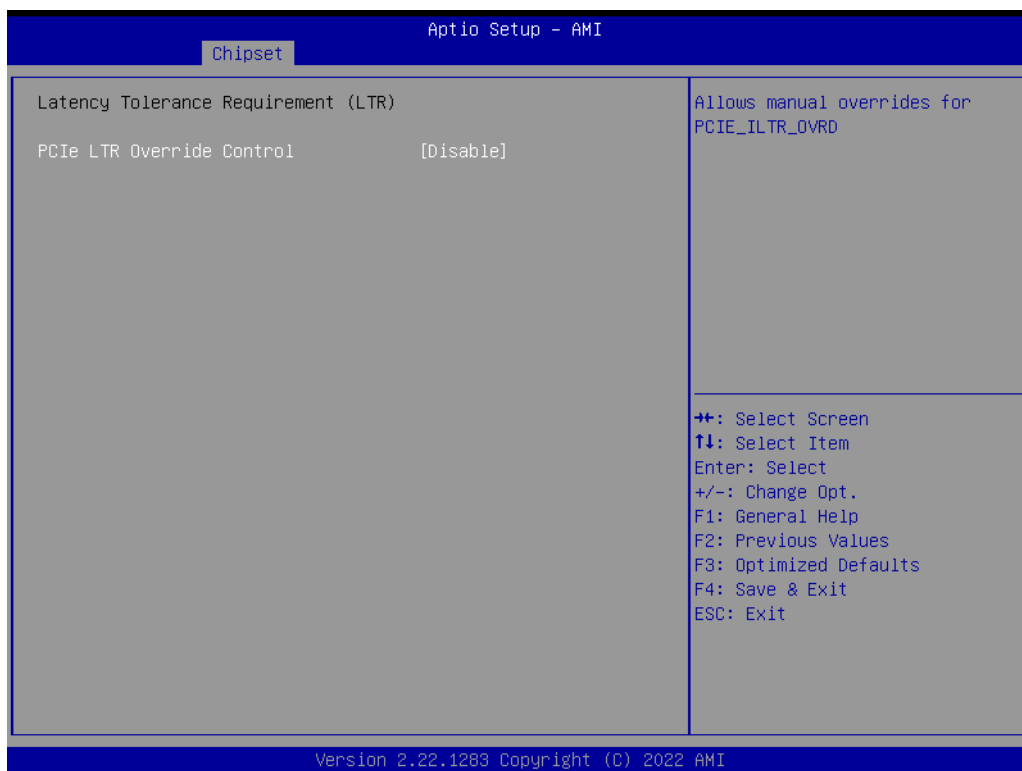


Figure 3.39 Latency Tolerance Requirement (LTR)

- **PCIe LTR Override Control**
Allows manual overrides for PCIE_ILTR_OVRD.

PkgC SA PS Criteria Power Management Control

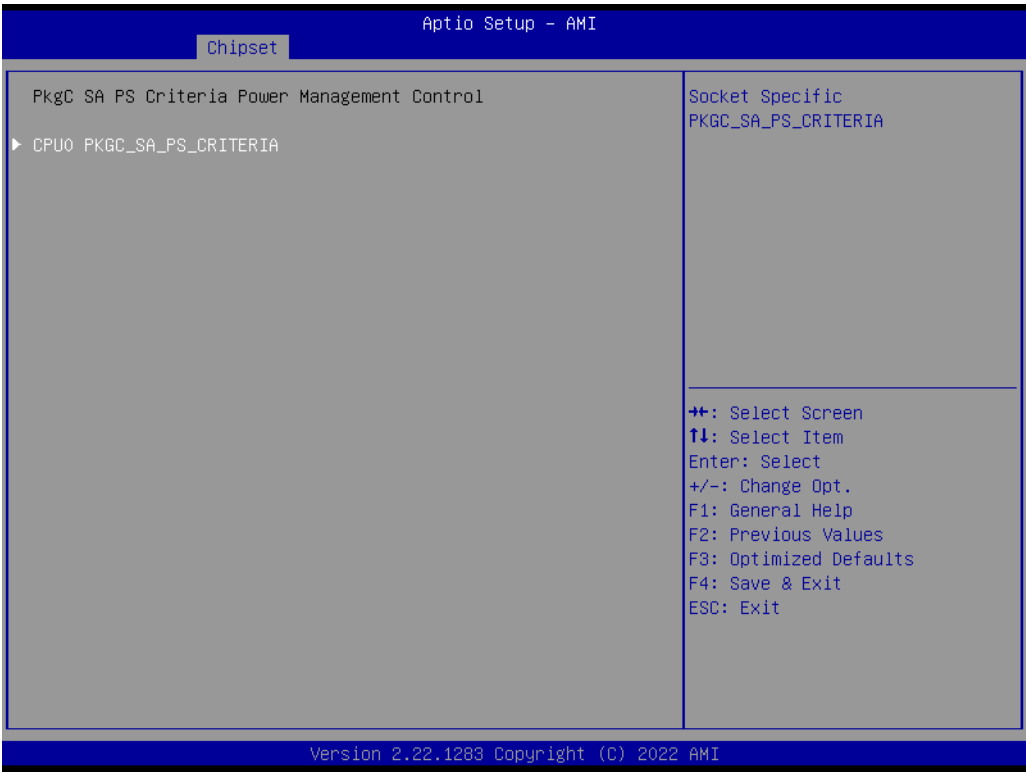


Figure 3.40 PkgC SA PS Criteria Power Management Control

- **CPU0 PKGC_SA_PS_CRITERIA**
Socket Specific PKGC_SA_PS_CRITERIA.

CPU0 PKGC_SA_PS_CRITERIA

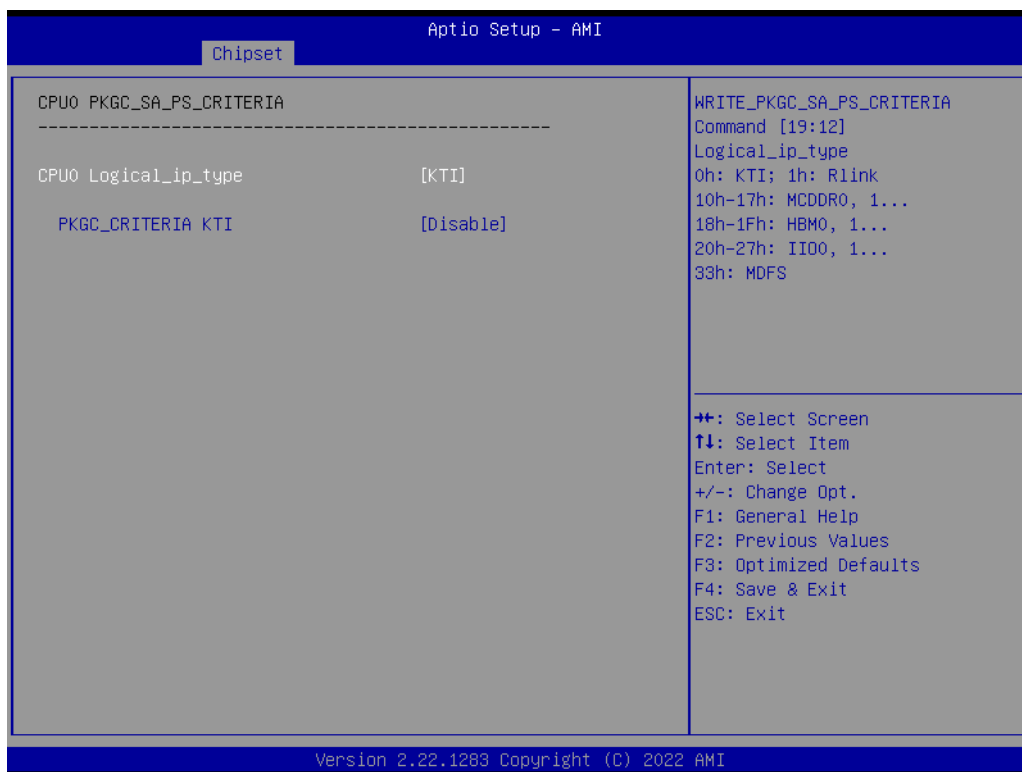


Figure 3.41 CPU0 PKGC_SA_PS_CRITERIA

- **CPU0 Logical_ip_type**
WRITE_PKGC_SA_PS_CRITERIA Command [19:12] Logical_ip_type 0h: KTI?1h:Rlink 10h-17h: MCDDR0, 1...
18h-1Fh: HBM0, 1...
20h-27h: IIO0, 1...
33h: MDFS.
- **PKGCRITERIA KTI**

PKGc Interrupt Response Time

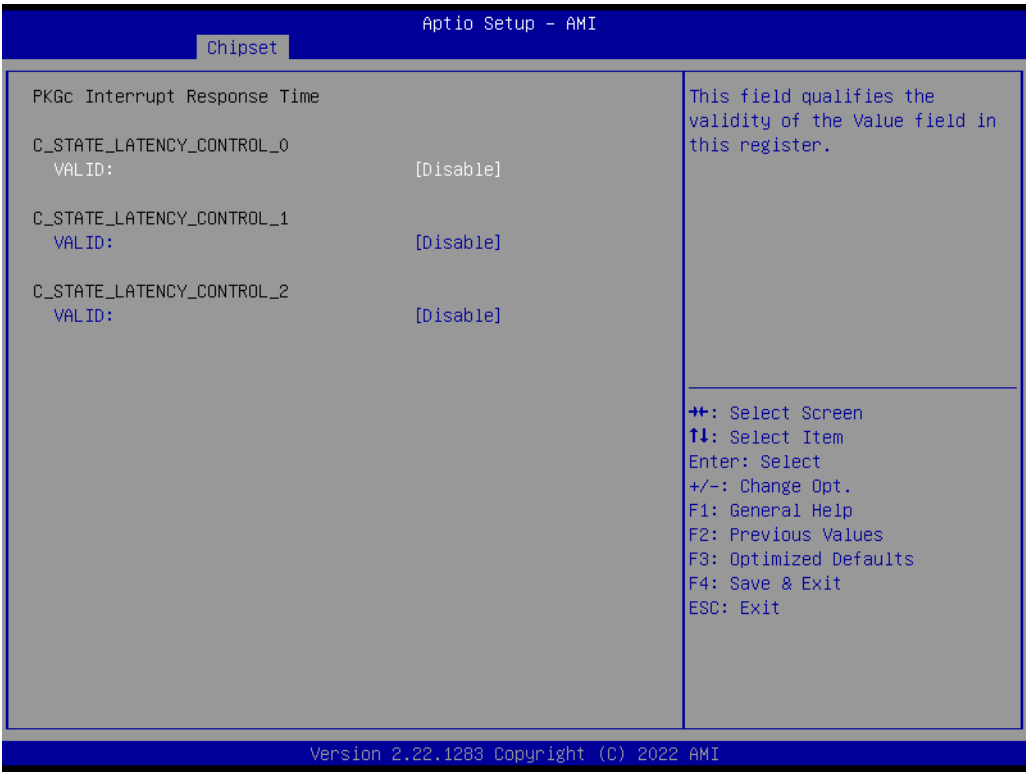


Figure 3.42 PKGc Interrupt Response Time

- **VALID**
This field qualifies the validity of the Value field in this register.

3.5.1.4 Memory Topology

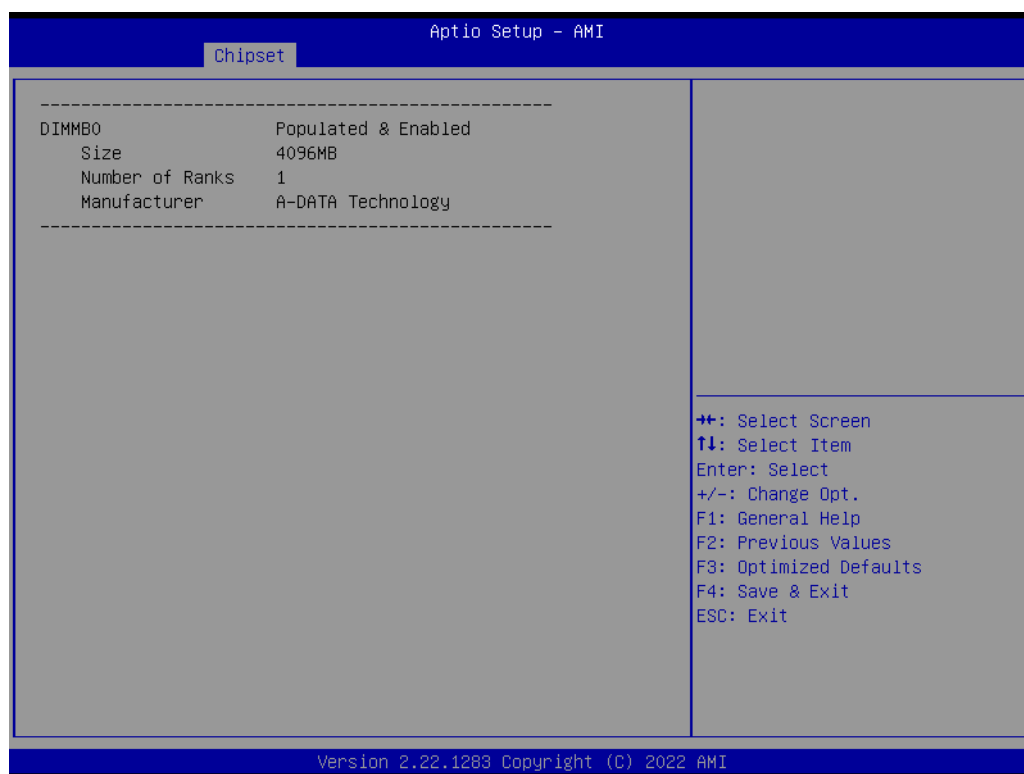


Figure 3.43 Memory Topology

3.5.2 Platform Configuration

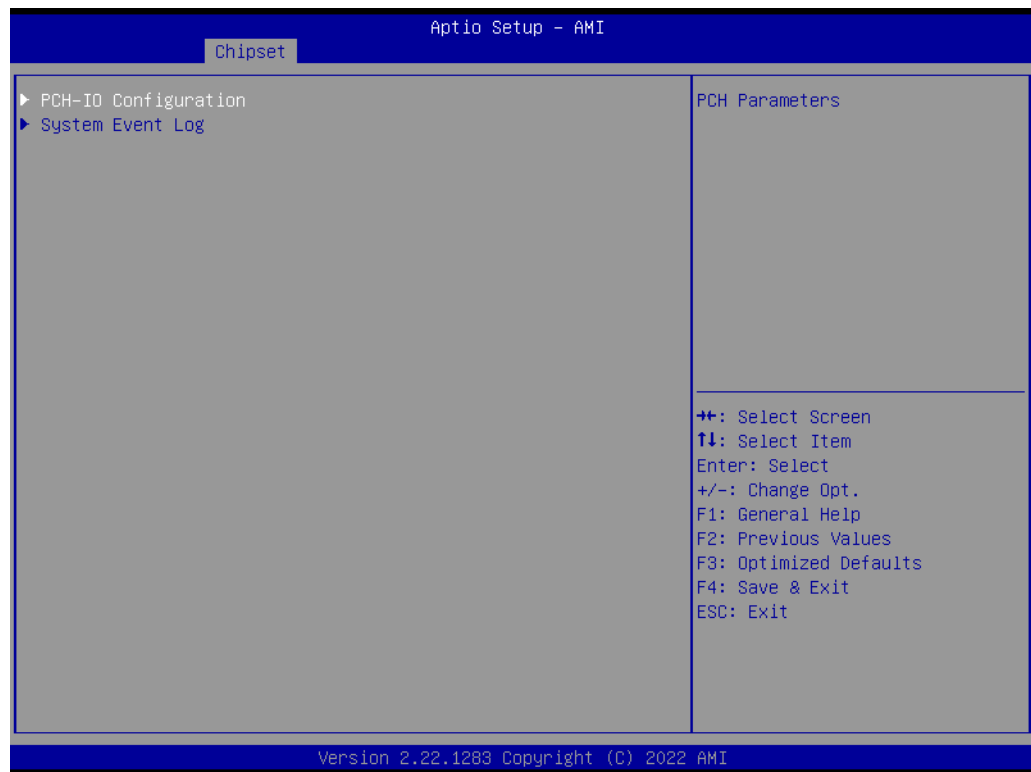


Figure 3.44 Platform Configuration

- **PCH-IO Configuration**
PCH Parameters.
- **System Event Log**
Press <Enter> to view or change the event log configuration.

3.5.2.1 PCH-IO Configuration



Figure 3.45 PCH-IO Configuration

- **PCI Express Configuration**
PCI Express Configuration settings.
- **Fia Mux Configuration**
Configuration of FIA Mux.
- **SATA Configuration**
Device Options Settings.
- **USB Configuration**
USB Configuration settings.
- **Security Configuration**
Security Configuration settings.
- **State After G3**
Specify what state to go to when power is re-applied after a power failure (G3 state).
- **Pcie Pll SSC**
PCIe Pll SSC percentage. AUTO-Keep hw default, no BIOS override. Setting AUTO reveals an option for CSME programming of SSC.
- **Flash Protection Range Registers (FPRR)**
Enable Flash Protection Range Registers.

■ PCI Express Configuration

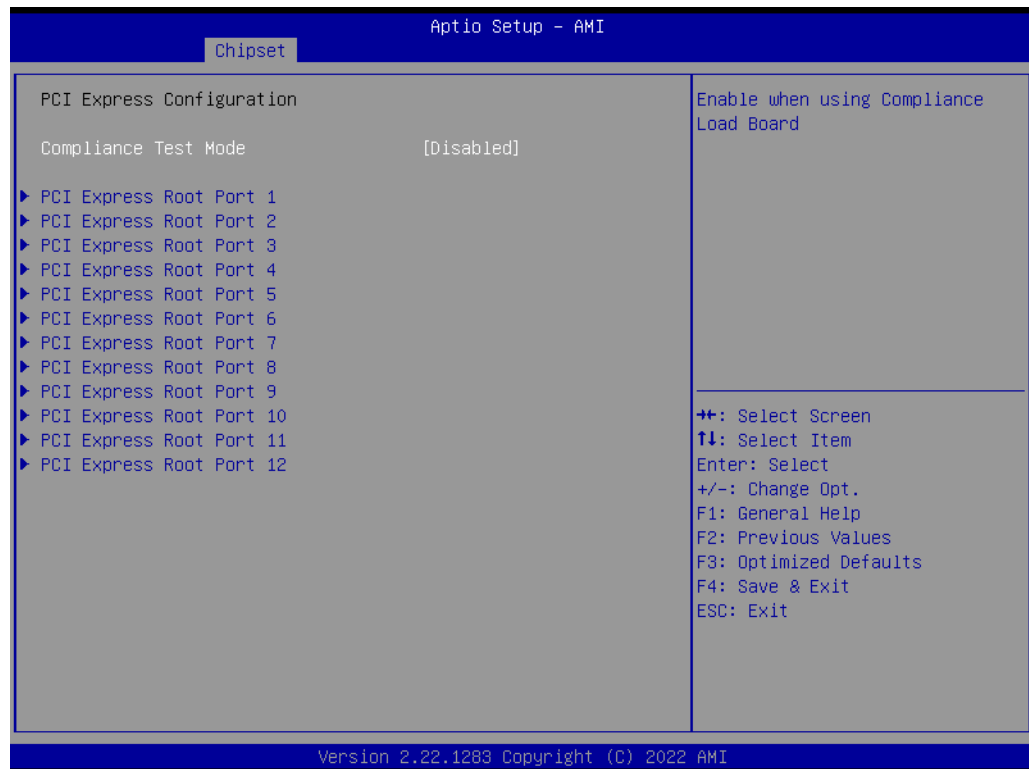


Figure 3.46 PCI Express Configuration

- **Compliance Test Mode**
Enable when using Compliance Load Board.
- **PCI Express Root Port 1**
PCI Express Root Port Settings.
- **PCI Express Root Port 2**
PCI Express Root Port Settings.
- **PCI Express Root Port 3**
PCI Express Root Port Settings.
- **PCI Express Root Port 4**
PCI Express Root Port Settings.
- **PCI Express Root Port 5**
PCI Express Root Port Settings.
- **PCI Express Root Port 6**
PCI Express Root Port Settings.
- **PCI Express Root Port 7**
PCI Express Root Port Settings.
- **PCI Express Root Port 8**
PCI Express Root Port Settings.
- **PCI Express Root Port 9**
PCI Express Root Port Settings.
- **PCI Express Root Port 10**
PCI Express Root Port Settings.
- **PCI Express Root Port 11**
PCI Express Root Port Settings.
- **PCI Express Root Port 12**
PCI Express Root Port Settings.

■ PCI Express Root Port 1

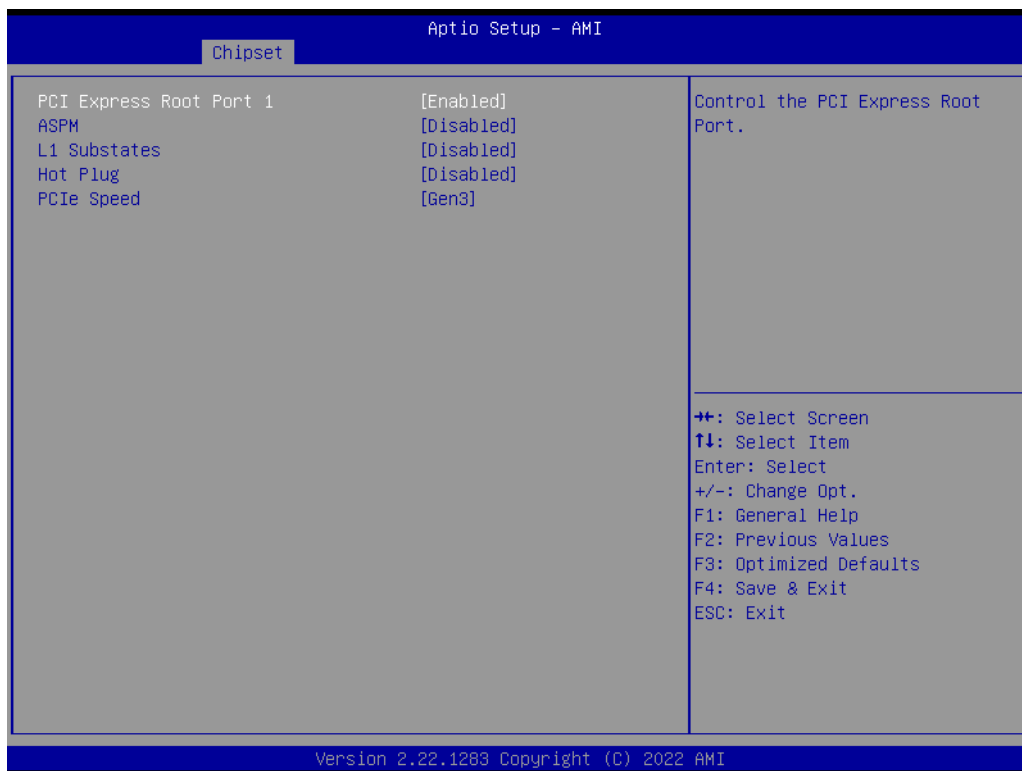


Figure 3.47 PCI Express Root Port 1

- **PCI Express Root Port 1**
Control the PCI Express Root Port.
- **ASPM**
- **L1 Substates**
- **Hot Plug**
- **PCIe Speed**

PCI Express Root Port 2

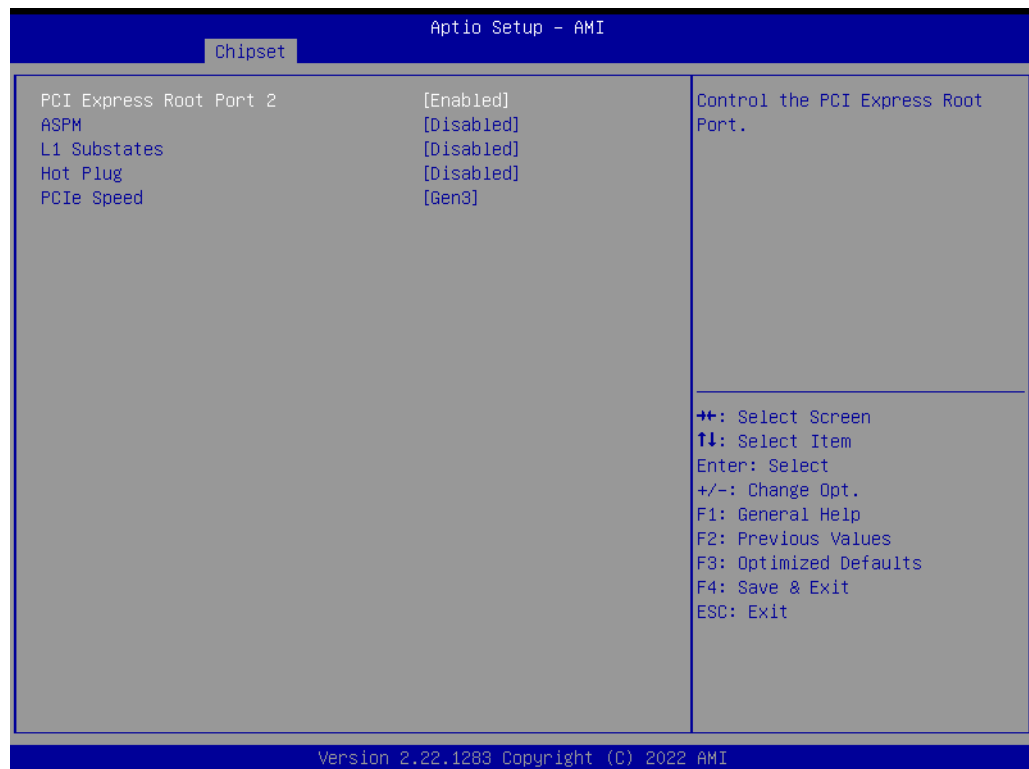


Figure 3.48 PCI Express Root Port 2

- **PCI Express Root Port 2**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 3

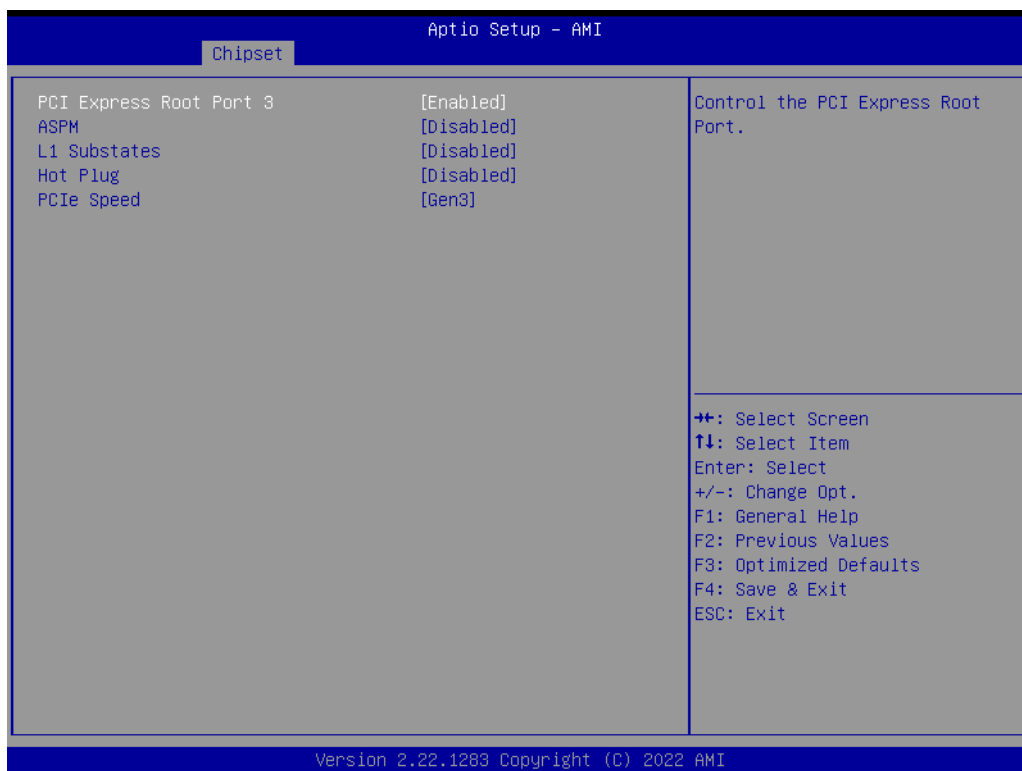


Figure 3.49 PCI Express Root Port 3

- **PCI Express Root Port 3**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 4

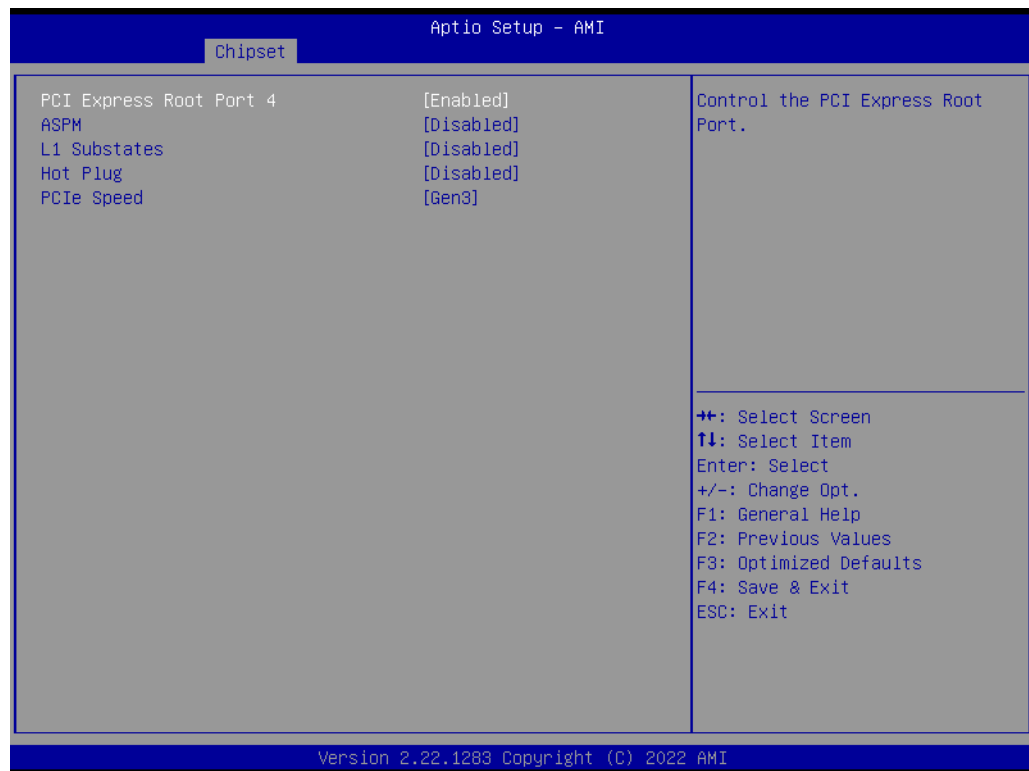


Figure 3.50 PCI Express Root Port 4

- **PCI Express Root Port 4**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 5

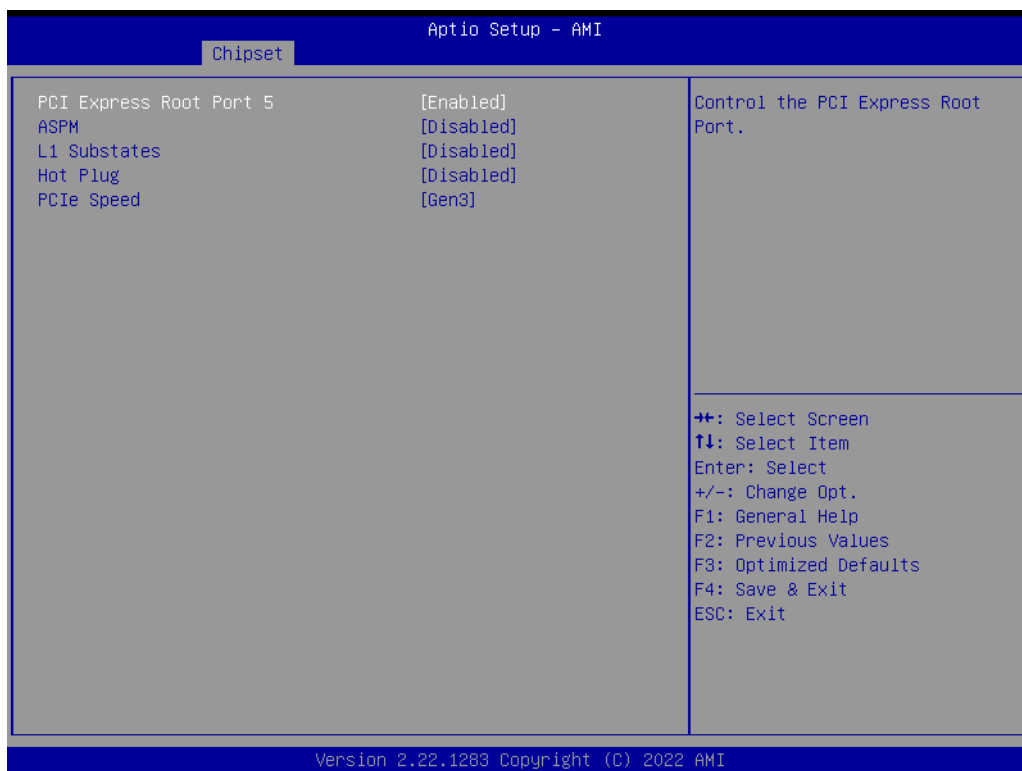


Figure 3.51 PCI Express Root Port 5

- **PCI Express Root Port 5**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 6

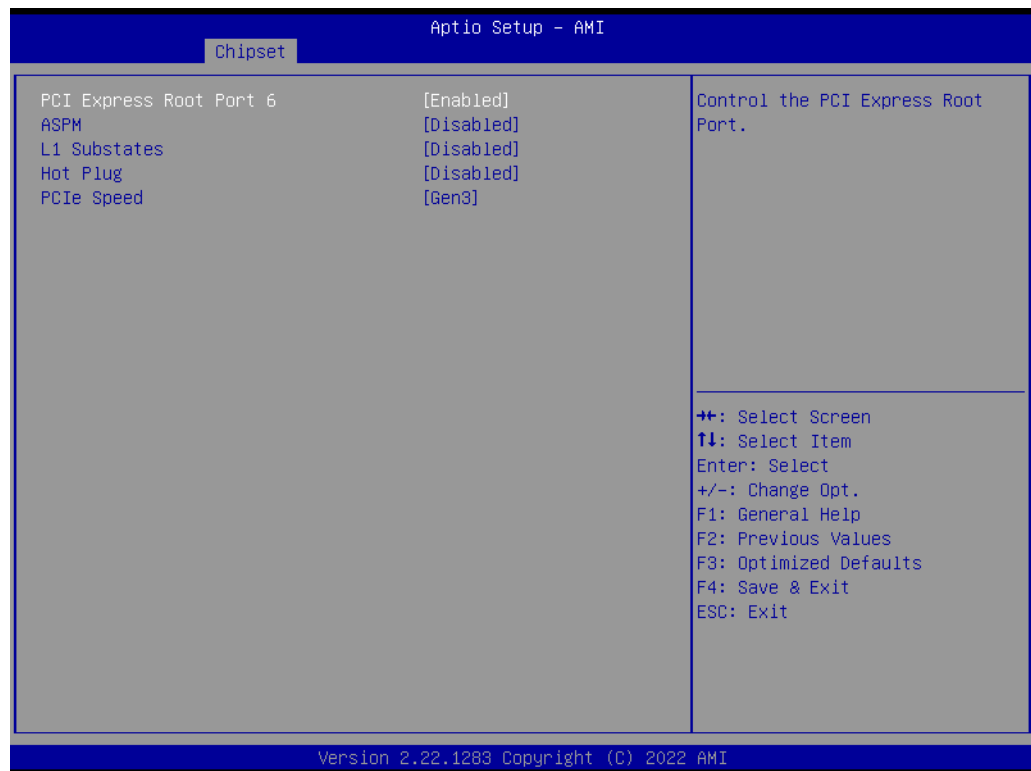


Figure 3.52 PCI Express Root Port 6

- **PCI Express Root Port 6**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 7

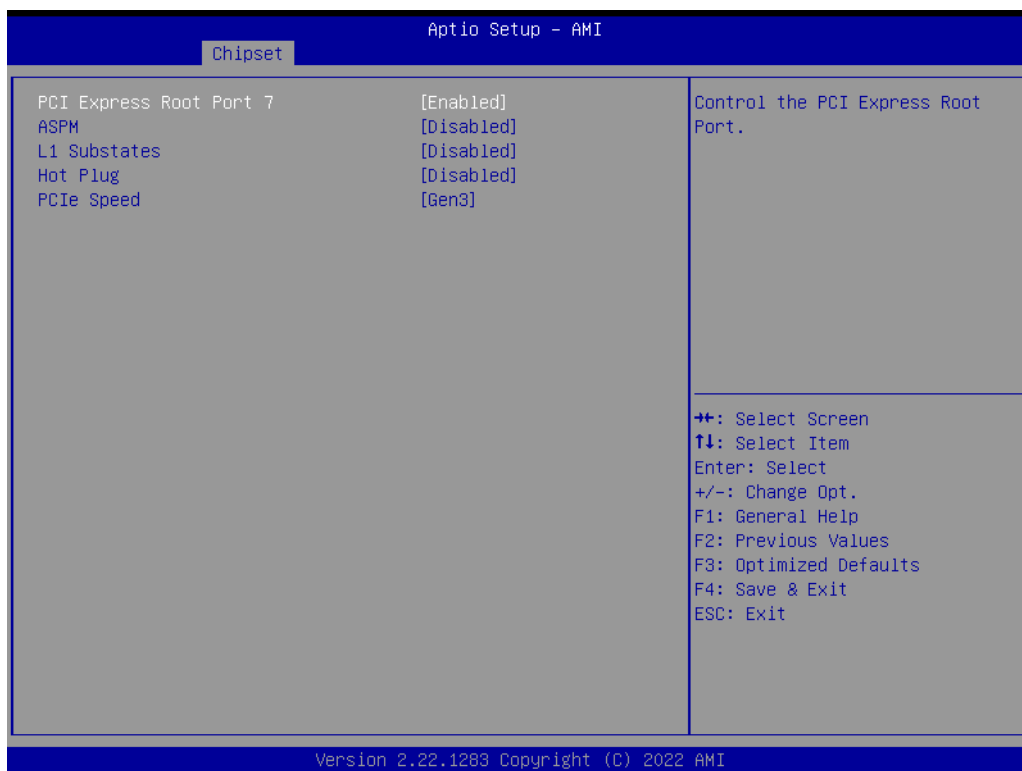


Figure 3.53 PCI Express Root Port 7

- **PCI Express Root Port 7**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 8

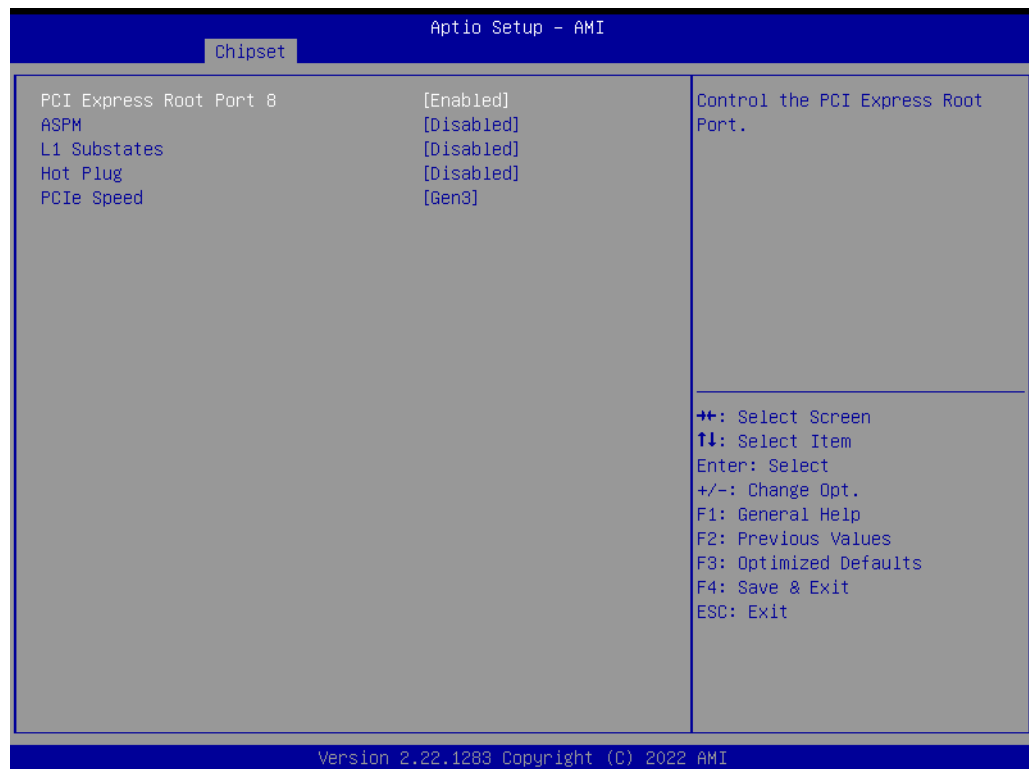


Figure 3.54 PCI Express Root Port 8

- **PCI Express Root Port 8**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 9

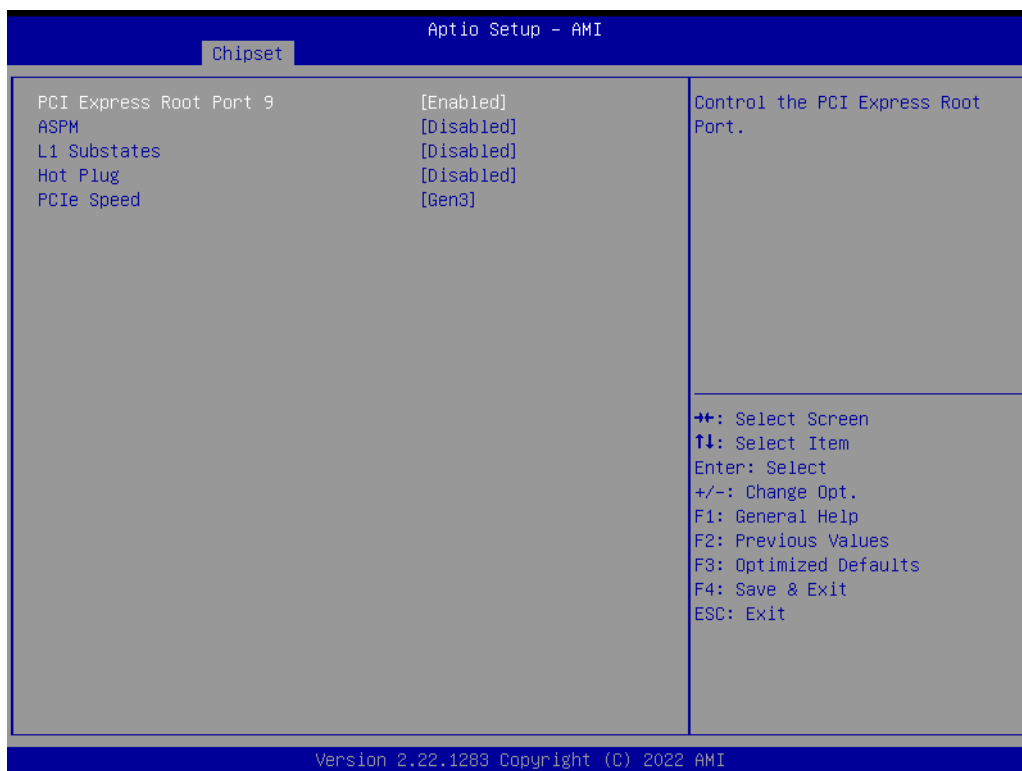


Figure 3.55 PCI Express Root Port 9

- **PCI Express Root Port 9**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 10

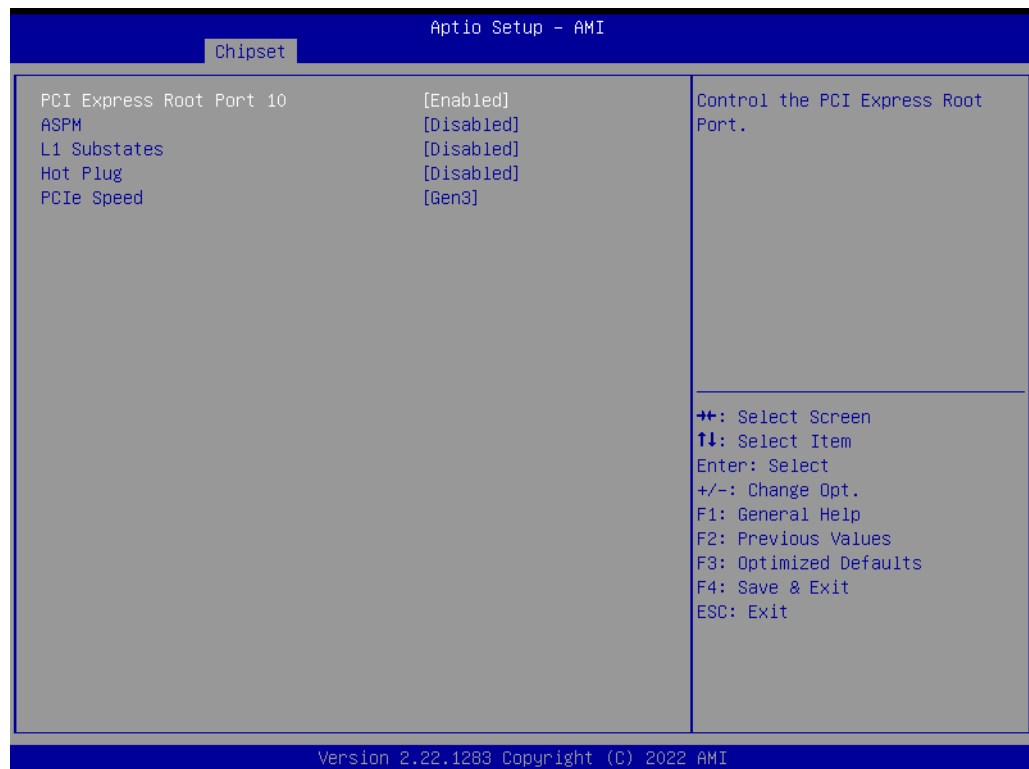


Figure 3.56 PCI Express Root Port 10

- **PCI Express Root Port 10**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 11

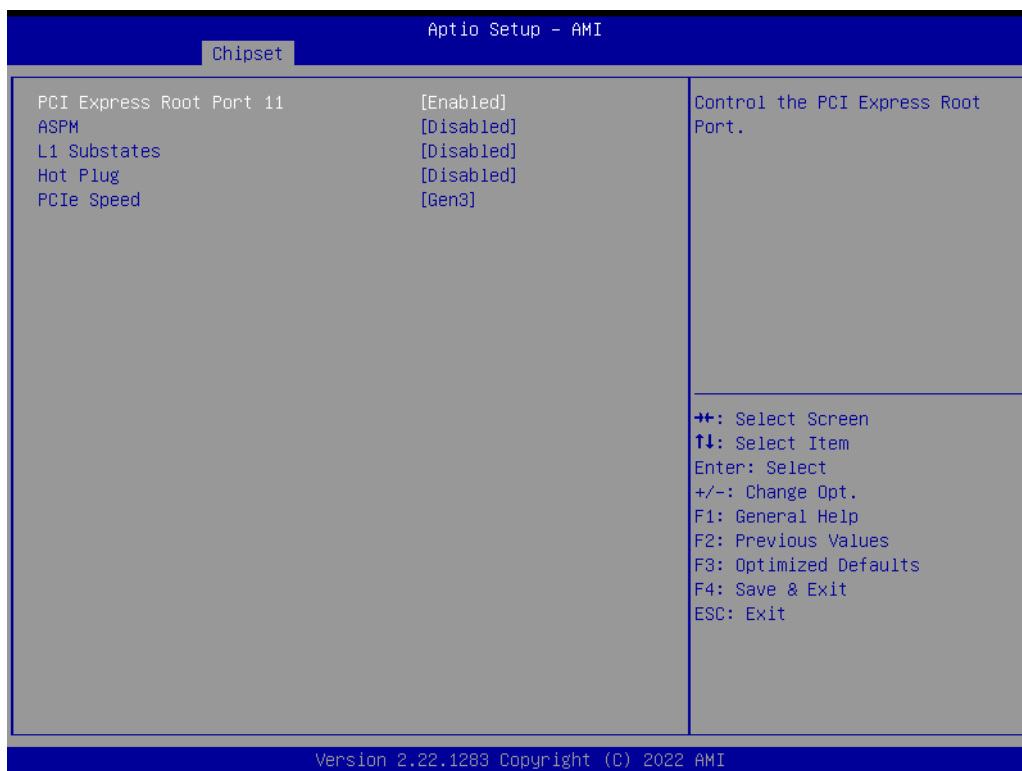


Figure 3.57 PCI Express Root Port 11

- **PCI Express Root Port 11**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

PCI Express Root Port 12

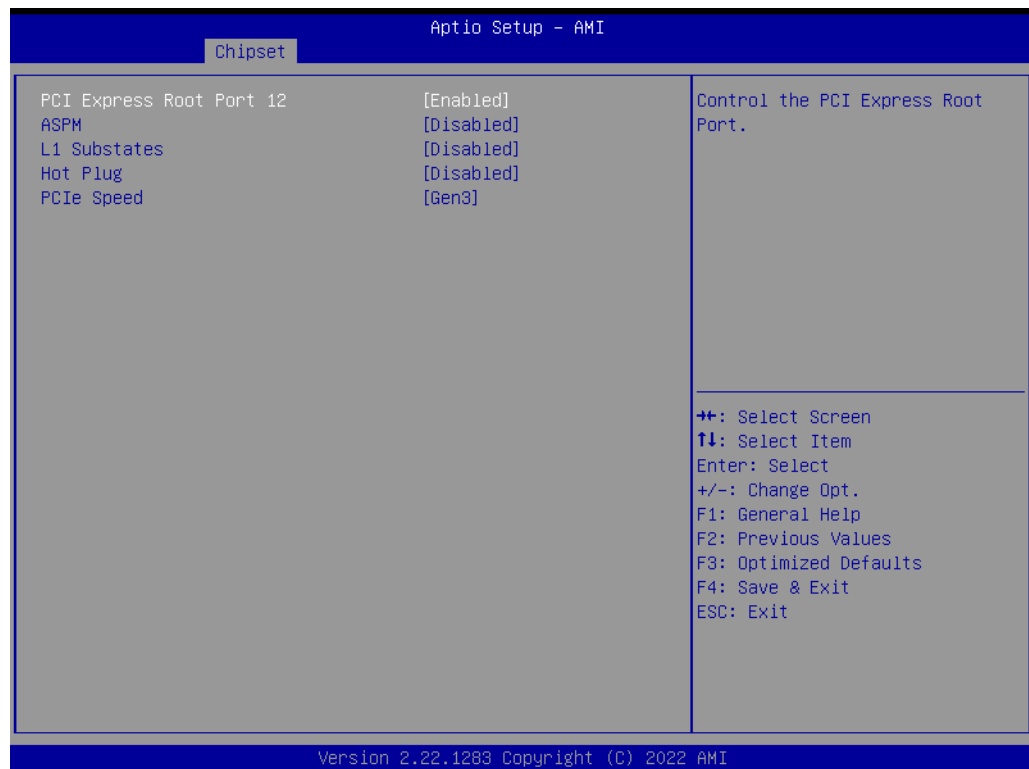


Figure 3.58 PCI Express Root Port 12

- **PCI Express Root Port 12**
Control the PCI Express Root Port.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings.
- **Hot Plug**
PCI Express Hot Plug Enable/Disable.
- **PCIe Speed**
Configure PCIe Speed Auto as equal to Gen2 or Gen3 depending on DTR soft strap.

■ Fia Mux Configuration

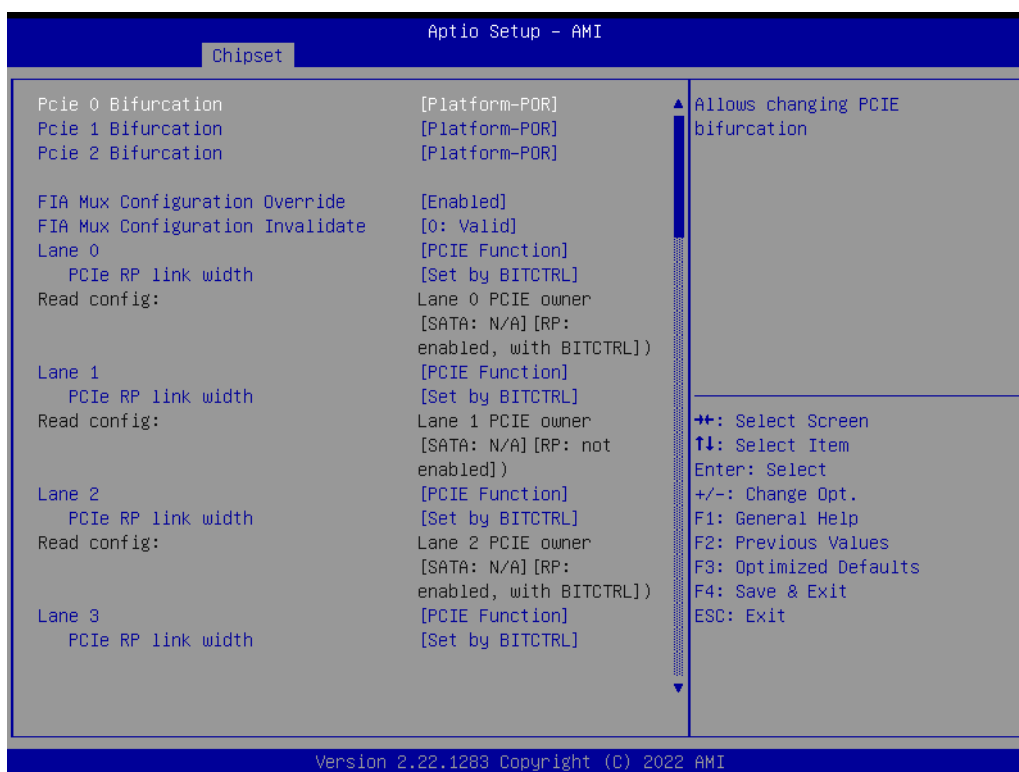


Figure 3.59 Fia Mux Configuration

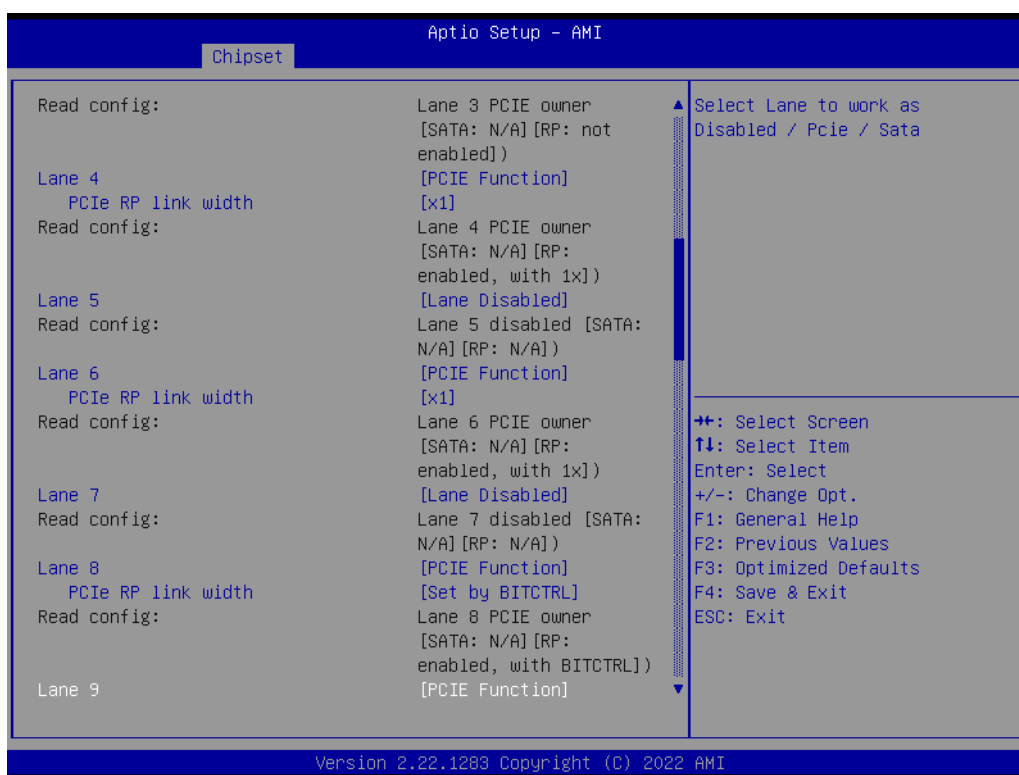


Figure 3.60 Fia Mux Configuration

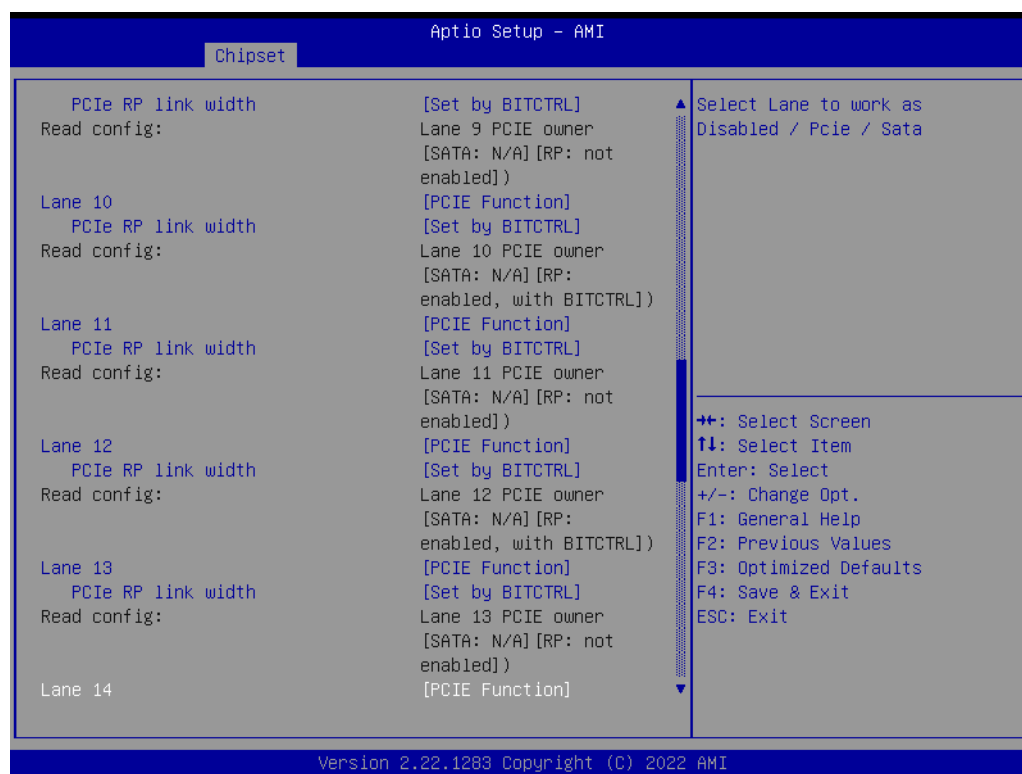


Figure 3.61 Fia Mux Configuration

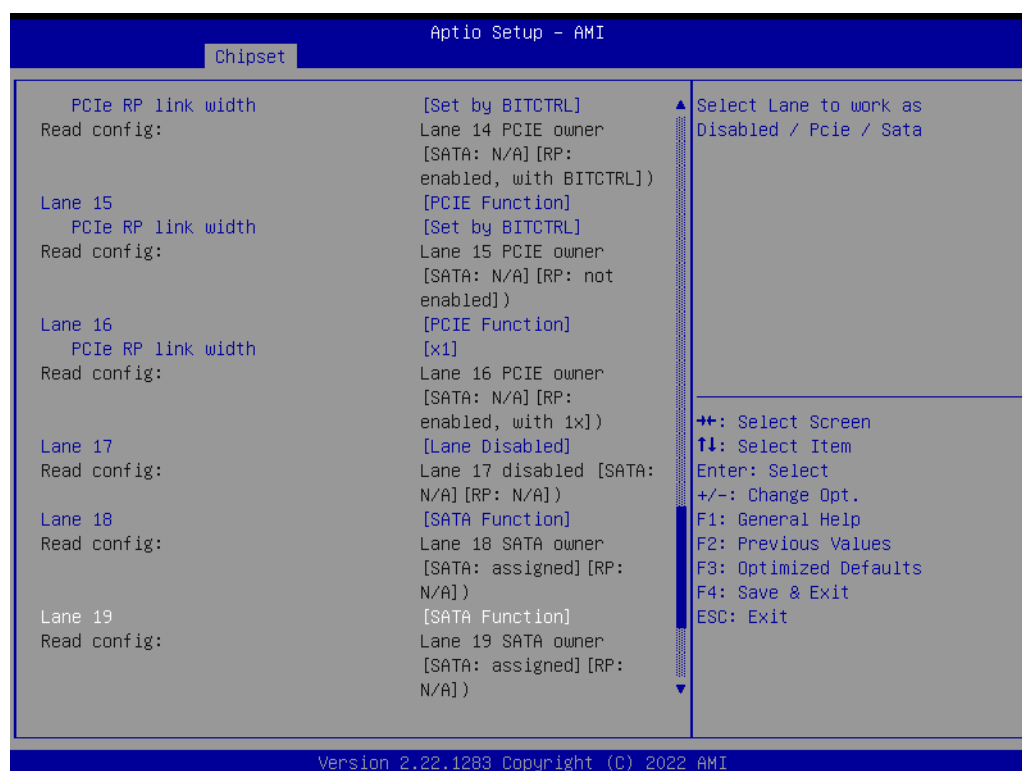


Figure 3.62 Fia Mux Configuration

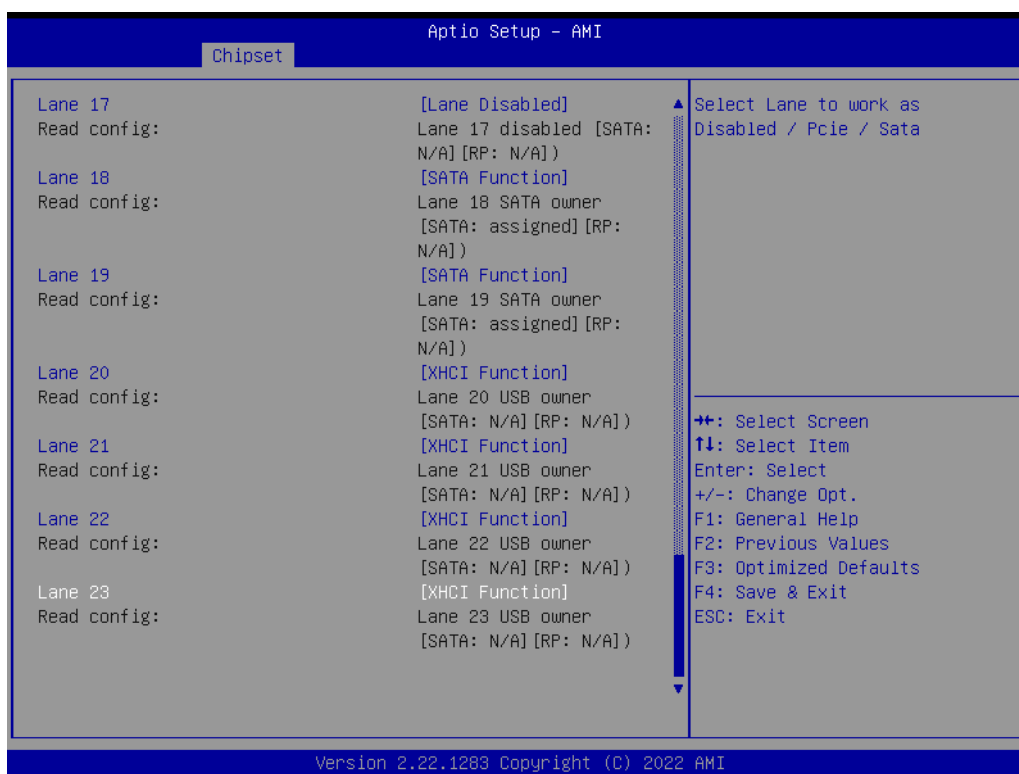


Figure 3.63 Fia Mux Configuration

- **Pcie 0 Bifurcation**
Allows changing PCIe bifurcation.
- **Pcie 1 Bifurcation**
Allows changing PCIe bifurcation.
- **Pcie 2 Bifurcation**
Allows changing PCIe bifurcation.
- **FIA Mux Configuration Override**
By Enabling this you override the platform configuration on FIA/WM.
- **FIA Mux Configuration Invalidate**
0: Valid – FIA Mux Configuration is Valid and should be stored on Flash, 1: Not-Valid – FIA Mux configuration on Intel ME Flash should be invalidated. This means that the Lanes configuration will be based on Soft Straps Settings.
- **Lane 0**
Select Lane to work as Disabled/PCie.
- **PCle RP link width**
Selects PCIe Root Port link width.
- **Lane 1**
Select Lane to work as Disabled/PCie.
- **PCle RP link width**
Selects PCIe Root Port link width.
- **Lane 2**
Select Lane to work as Disabled/PCie.
- **PCle RP link width**
Selects PCIe Root Port link width.
- **Lane 3**
Select Lane to work as Disabled/PCie.

- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 4**
Select Lane to work as Disabled/Pcie.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 5**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 6**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 7**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 8**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 9**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 10**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 11**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 12**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 13**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 14**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 15**
Select Lane to work as Disabled/Pcie/Sata.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 16**
Select Lane to work as Disabled/Sata/Xhci.
- **PCIe RP link width**
Selects PCIe Root Port link width.
- **Lane 17**
Select Lane to work as Disabled/Pcie/Sata.

- **Lane 18**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 19**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 20**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 21**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 22**
Select Lane to work as Disabled/Pcie/Sata.
- **Lane 23**
Select Lane to work as Disabled/Pcie/Sata.
- **SATA Configuration**



Figure 3.64 SATA Configuration

- **SATA Controller Speed**
Indicates the maximum speed the SATA controller can support.
- **Controller 3 SATA Configuration**
SATA controller 3 Device Options Settings.

Controller 3 SATA Configuration

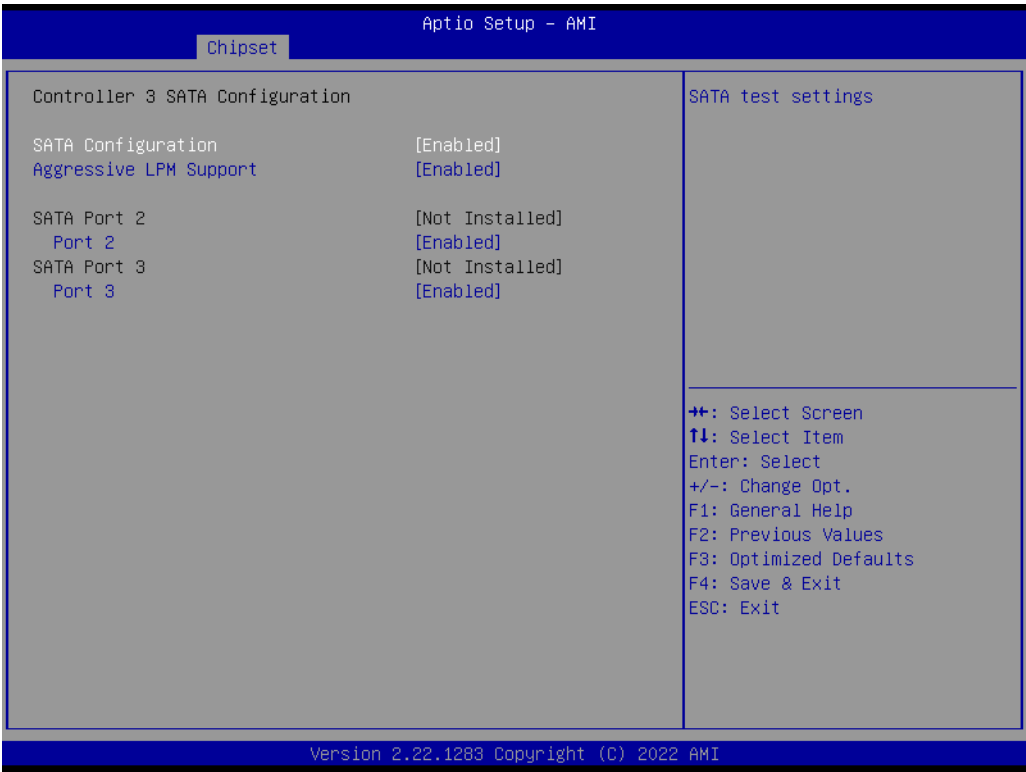


Figure 3.65 Controller 3 SATA Configuration

- **SATA Configuration**
SATA test settings.
- **Aggressive LPM Support**
Enable PCH to aggressively enter link power state.
- **Port 2**
Enable or Disable SATA Port.
- **Port 3**
Enable or Disable SATA Port.

USB Configuration

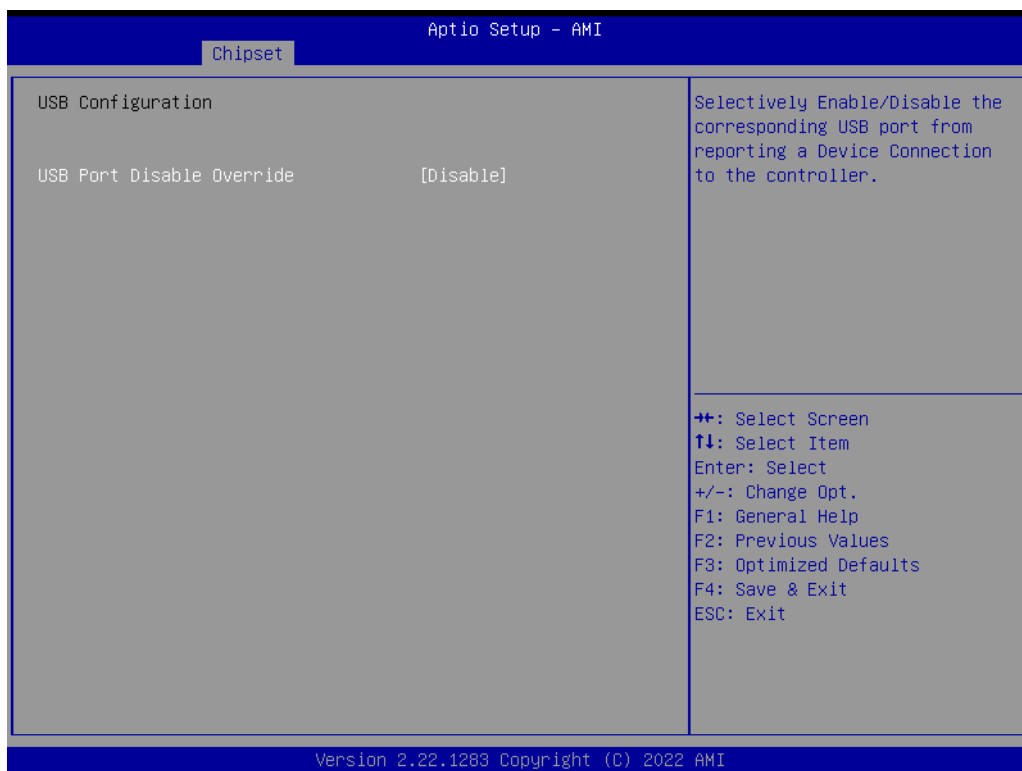


Figure 3.66 USB Configuration

- **USB Port Disable Override**
Selectively Enable/Disable the corresponding USB port from reporting a Device Connect to the controller.

Security Configuration

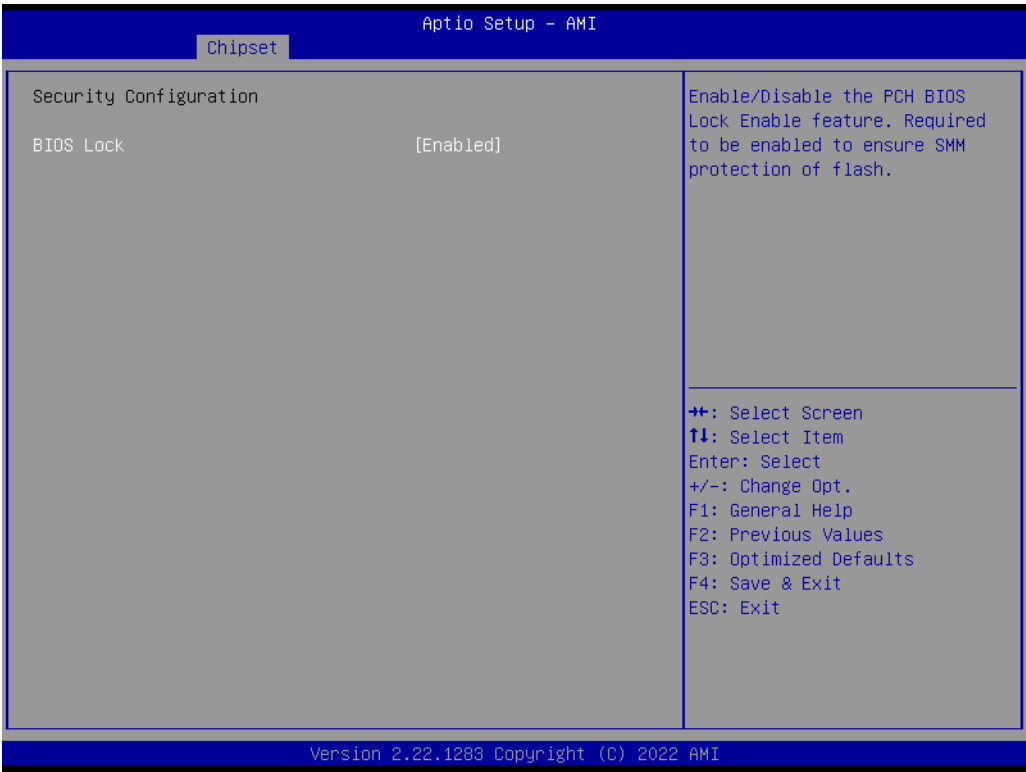


Figure 3.67 Security Configuration

- **BIOS Lock**
Enable/Disable the PCH BIOS Lock Enable feature. Required to be enabled to ensure SMM protection of flash.

3.5.2.2 System Event Log

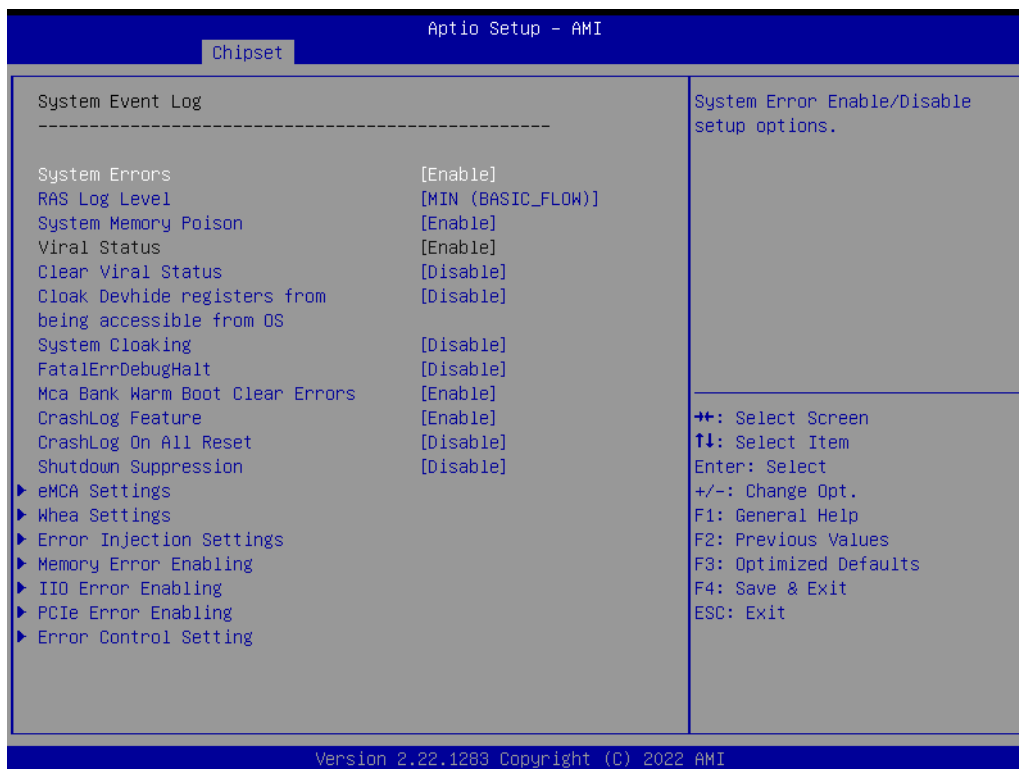


Figure 3.68 System Event Log

- **System Errors**
System Error Enable/Disable setup options.
- **RAS Log Level**
RAS Log setup options.
- **System Memory Poison**
Enable/Disable System Memory Poison.
- **Clear Viral Status**
Enable/Disable Clear Viral Status.
- **Cloak Devhide registers from being accessible from OS**
Enable/Disable OS to access Devhide registers.
- **System Cloaking**
When enabled, Corrected errors are masked from OS/SW visibility. This option is valid only when EMCA is enabled.
- **FatalErrDebugHalt**
DEBUG loop for McBank Fatal error case ONLY. Warning: Enable this knob only in conjunction with ITP as the thread will halt in Fatal error flow.
- **Mca Bank Warm Boot Clear Errors**
Enable/Disable Mca Bank Warm Boot Clear Errors.
- **CrashLog Feature**
The feature helps collecting crash data from PMC SSRAM.
- **CrashLog On All Reset**
Option to invoke CrashLog collection on all resets.
- **Shutdown Suppression**
Configures Shutdown Suppression and Log MCA IERR Support.
- **eMCA Settings**
Press <Enter> to view or change the eMCA configuration.

- **Whea Settings**
Press <Enter> to view or change the WHEA configuration.
- **Error Injection Settings**
Press <Enter> to view or change the Error Injection configuration.
- **Memory Error Enabling**
Press <Enter> to view or change the Memory error enabling options.
- **IIO Error Enabling**
Press <Enter> to view or change the IIO error enabling options.
- **PCIe Error Enabling**
Press <Enter> to view or change the PCIe error enabling options.
- **Error Control Setting**
Press <Enter> to view or change the Error Control Setting options.
- **eMCA Settings**

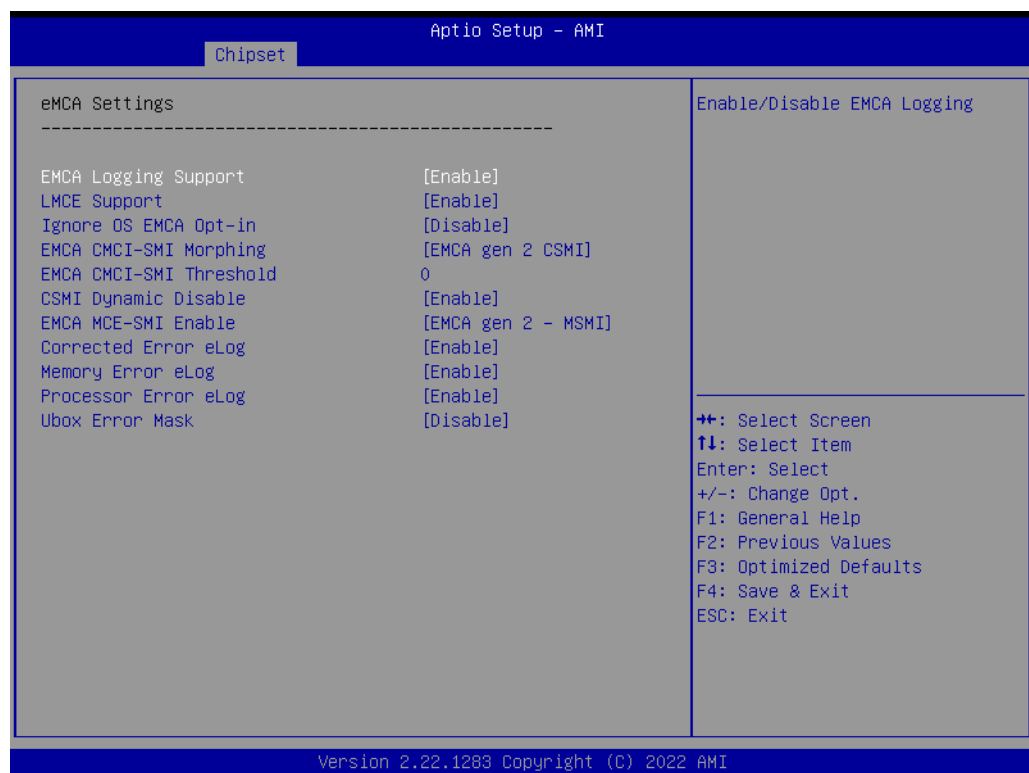


Figure 3.69 eMCA Settings

- **EMCA Logging Support**
Enable/Disable EMCA Logging.
- **LMCE Support**
Enable/Disable Local MCE firmware support.
- **Ignore OS EMCA Opt-in**
Enable/Disable Ignore OS EMCA Opt-in and log.
- **EMCA CMCI-SMI Morphing**
Enable/Disable EMCA CSMI.
- **EMCA CMCI-SMI Threshold**
Set the threshold of correctable error for signaling CMCI-CSMI.
- **CSMI Dynamic Disable**
[Enable] - BIOS disables CSMI when error threshold reached. [Disabled] – CSMI always on.

- **EMCA MCE-SMI Enable**
Enable/Disable EMCA Uncorrected SMI for Gen2.
- **Corrected Error eLog**
Enable/Disable Corrected Error eLog.
- **Memory Error eLog**
Enable/Disable Memory Error eLog.
- **Processor Error eLog**
Enable/Disable Processor Error eLog.
- **Ubox Error Mask**
Mask SMI generation for Ubox Error.
- **Whea Settings**

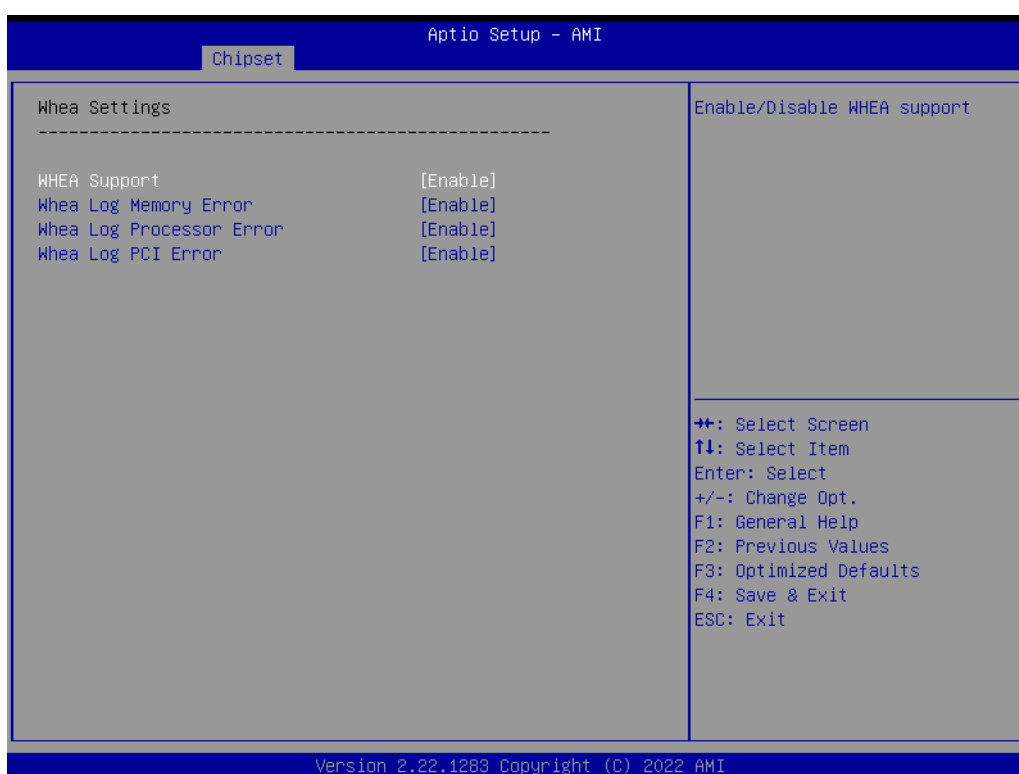


Figure 3.70 Whea Settings

- **WHEA Support**
Enable/Disable WHEA support.
- **Whea Log Memory Error**
Enable/Disable WHEA Log Memory Error.
- **Whea Log Processor Error**
Enable/Disable WHEA Log Processor Error.
- **Whea Log PCI Error**
Enable/Disable WHEA Log PCI Error.

■ Error Injection Settings

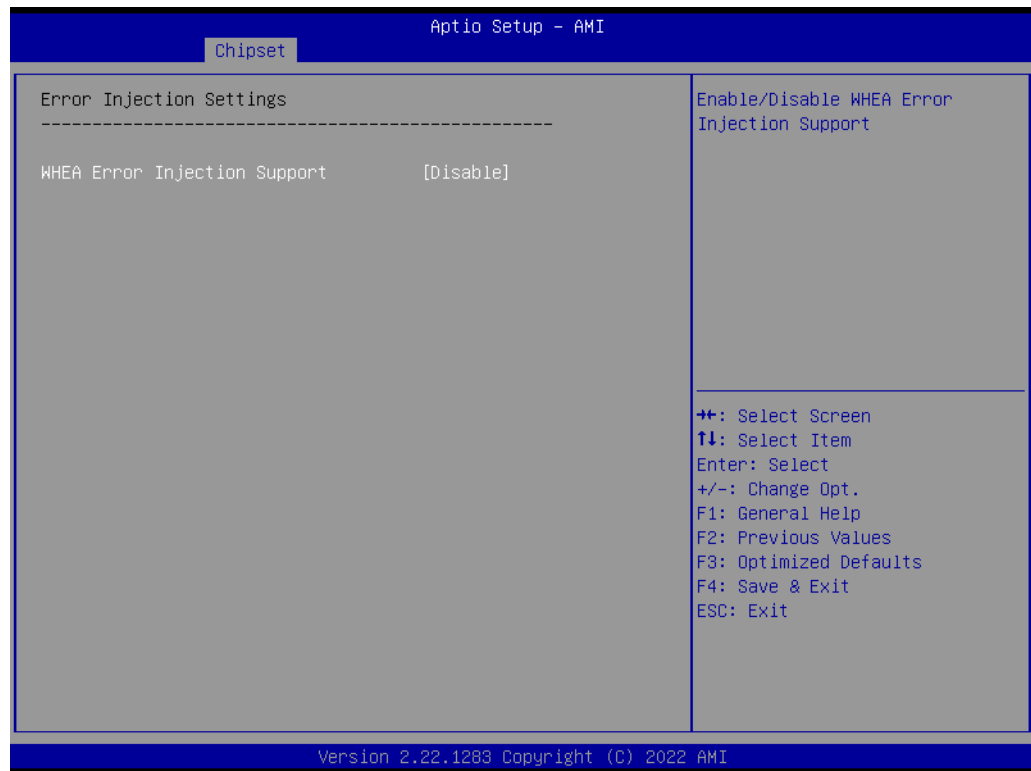


Figure 3.71 Error Injection Settings

- **WHEA Error Injection Support**
Enable/Disable WHEA Error Injection Support.

■ Memory Error Enabling



Figure 3.72 Memory Error Enabling

- **Memory Error**
Enable/Disable Memory Error.
- **Memory Corrected Error**
Enable/Disable Memory Corrected Error.
- **Spare Interrupt**
Spare Interrupt Selection.

■ IIO Error Enabling

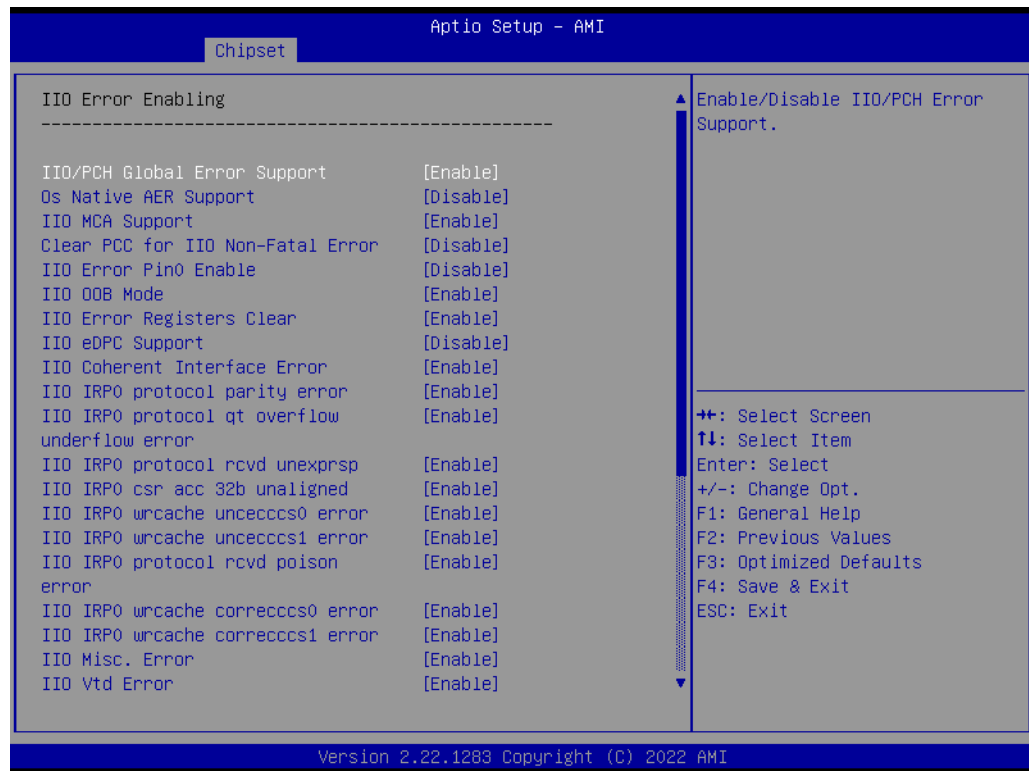


Figure 3.73 IIO Error Enabling



Figure 3.74 IIO Error Enabling

- **IIO/PCH Global Error Support**
Enable/Disable IIO/PCH Error Support.

- **OS Native AER Support**
Select FFM or OS native for AER error handling. If you select OS as native, BIOS also initializes FFM first until the handshake, which depends on the OS capability.
- **IIO MCA Support**
Enable/Disable IIO MCA Support.
- **Clear PCC for IIO Non-Fatal Error**
Enable/Disable PCC equal to 0 for IIO severity 1 error.
- **IIO Error Pin0 Enable**
Enable/Disable IIO Error Pin0.
- **IIO OOB Mode**
Enable/Disable System Event Generation when Error Pin is enabled.
- **IIO Error Registers Clear**
Enable/Disable Clear IIO Error Registers.
- **IIO eDPC Support**
Enable/Disable IIO eDPC Support.
- **IIO Coherent Interface Error**
Enable/Disable IIO Coherent Interface Error.
- **IIO IRP0 protocol parity error**
Enable or disable Coherent Interface protocol IIO parity error reporting.
- **IIO IRP0 protocol qt overflow underflow error**
Enable or disable IIO Coherent Interface protocol queue table overflow or underflow error reporting.
- **IIO IRP0 protocol rcvd unexprsp**
Enable or disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting.
- **IIO IRP0 csr acc 32b unaligned**
Enable or disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting.
- **IIO IRP0 wrcache uncecccs0 error**
Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
- **IIO IRP0 wrcache uncecccs1 error**
Enable or disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
- **IIO IRP0 protocol rcvd poison error**
Enable or disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting.
- **IIO IRP0 wrcache correcccs0 error**
Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.
- **IIO IRP0 wrcache correcccs1 error**
Enable or disable IIO Coherent Interface Write Cache Correctable ECC error reporting.
- **IIO Misc. Error**
Enable/Disable IIO Misc. Error.
- **IIO Vtd Error**
Enable/Disable IIO Vtd Error.
- **IIO Dma Error**
Enable/Disable IIO Dma Error.
- **IIO Dmi Error**
Enable/Disable IIO Dmi Error.

- **PCIE Error**
Enable/Disable PCIE Error.
- **IIO PCIE Additional Corrected Error**
Enable/Disable IIO PCIE Additional Corrected Error.
- **IIO PCIE Additional Uncorrected Error**
Enable/Disable IIO PCIE Additional Uncorrected Error.
- **IIO PCIE Additional Received Completion With UR**
Enable/Disable IIO PCIE Additional Received Completion with UR.
- **IIO PCIE AER Spec Compliant**
Enable/Disable IIO PCIE AER Spec Compliant.
- **ITC/OTC CA/MA Errors**
Enable/Disable Completer Abort and Master Abort (Unsupported Request) on ITC and OTC.
- **PSF UR Error**
Enable/Disable Unsupported Request Error on PSF.
- **PMSB Router Parity Error**
Enable/Disable PMSB Router Parity Error.

- **PCle Error Enabling**

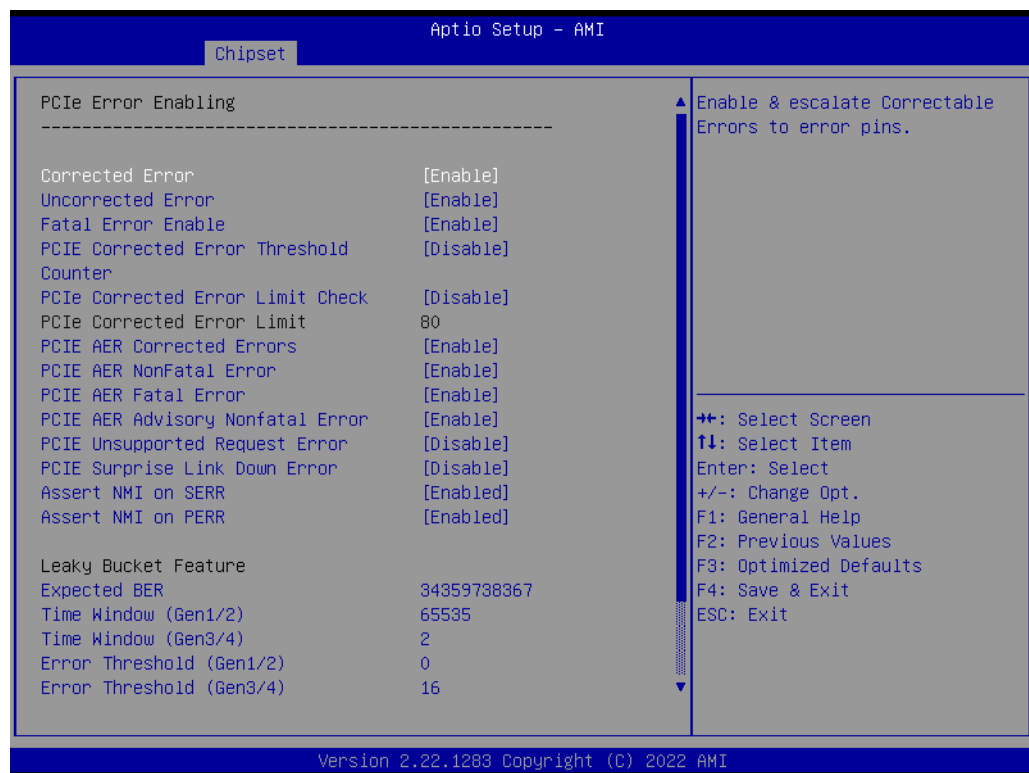


Figure 3.75 PCIe Error Enabling

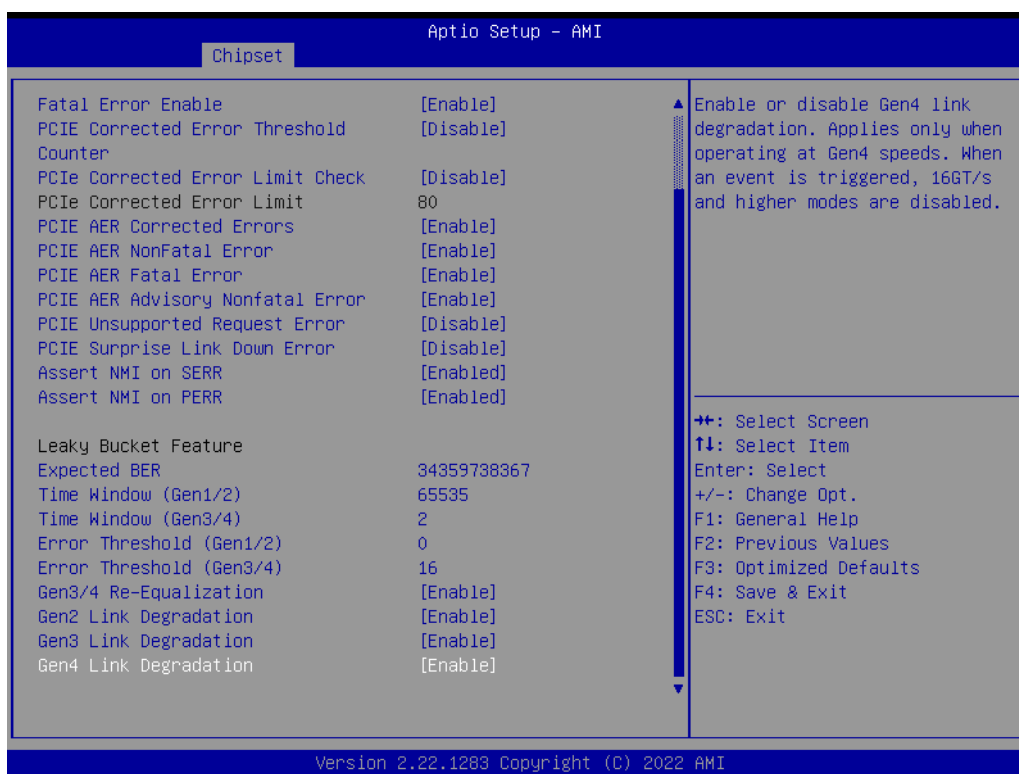


Figure 3.76 PCIe Error Enabling

- **Corrected Error**
Enable & escalate Correctable Errors to error pins.
- **Uncorrected Error**
Enable & escalate Uncorrectable/Recoverable to error pins.
- **Fatal Error Enable**
Enable & escalate fatal error to error pins.
- **PCIe Corrected Error Threshold Counter**
- **PCIe Corrected Error Limit Check**
Enable/Disable the feature to disable reporting PCIe corrected errors for a device if they exceed a given limit.
- **PCIe AER Corrected Errors**
Enable/Disable PCIe AER Corrected Errors.
- **PCIe AER NonFatal Error**
Enable/Disable PCIe AER NonFatal Error.
- **PCIe AER Fatal Error**
Enable/Disable PCIe AER Fatal Error.
- **PCIe AER Advisory Nonfatal Error**
Enable/Disable PCIe AER Advisory Nonfatal Error.
- **PCIe Unsupported Request Error**
Enable/Disable PCIe Unsupported Request Error.
- **PCIe Surprise Link Down Error**
Enable/Disable PCIe Surprise Link Down Error.
- **Assert NMI on SERR**
On SERR, generate an NMI and log an error. Note: [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.

-
- **Assert NMI ON PERR**
On PERR, generate an NMI and log an error. Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.
 - **Expected BER**
Set the expected Bit Error Rate for all speeds.
 - **Time Window (Gen1/2)**
Set the error burst protection time window for Gen1 and Gen2 speeds. A burst of errors within the window is counted as one.
 - **Time Window (Gen3/4)**
Set the error burst protection time window for Gen3 and Gen4 speeds. A burst of errors within the window is counted as one.
 - **Error Threshold (Gen1/2)**
Set the error threshold for Gen1 and Gen2 speeds. An event is triggered when the error count exceeds the threshold.
 - **Error Threshold (Gen3/4)**
Set the error threshold for Gen3 and Gen4 speeds. An event is triggered when the error count exceeds the threshold.
 - **Gen3/4 Re-Equalization**
Enable or disable Gen3 and Gen4 re-equalization. Applies only when operating at Gen2 or Gen4 speeds. When an event is triggered, equalization is re-run.
 - **Gen2 Link Degradation**
Enable or disable Gen2 link degradation. Applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.
 - **Gen3 Link Degradation**
Enable or disable Gen3 link degradation. Applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.
 - **Gen4 Link Degradation**
Enable or disable Gen4 link degradation. Applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.

■ Error Control Settings



Figure 3.77 Error Control Settings

- **Latch First Corrected Error in KTI**
Enable or disable Latch First Corrected Error in KTI.
- **Patrol Scrub Error Reporting**
Patrol Scrub Error type selection.

3.6 Server Mgmt



Figure 3.78 Server Mgmt

- **BMC Support**
Enable/Disable interfaces to communicate with BMC.

3.7 Security

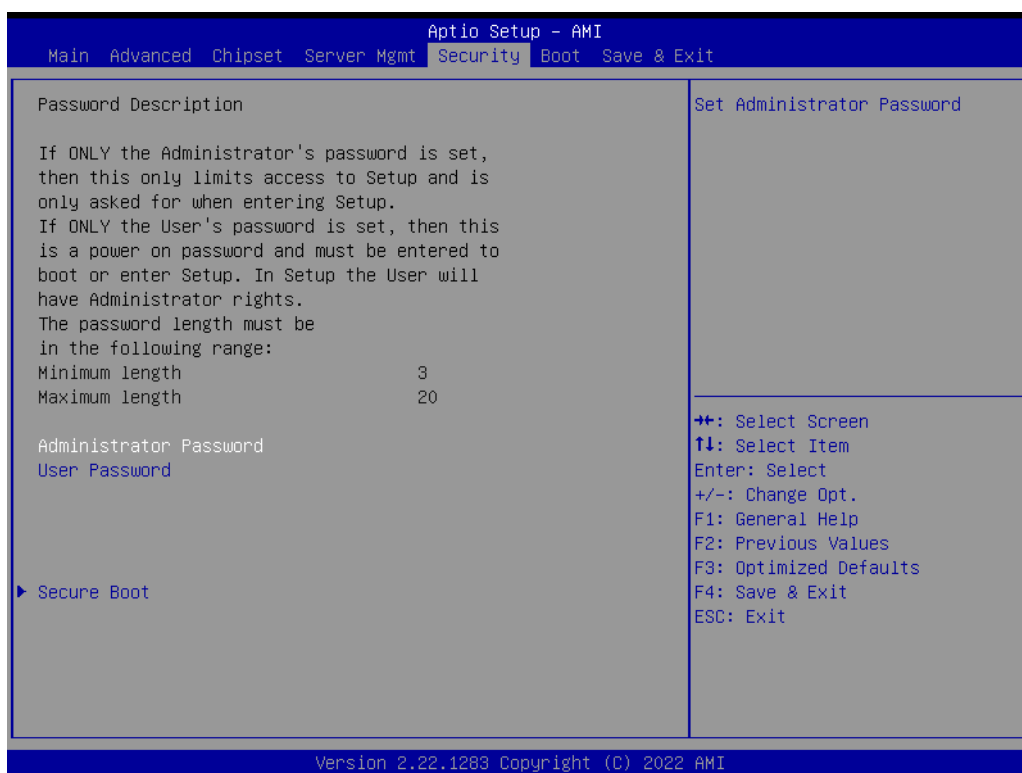


Figure 3.79 Security

- **Administration Password**
Set Administrator Password.
- **User Password**
Set User Password.
- **Secure Boot**
Secure Boot configuration.

3.7.1 Secure Boot

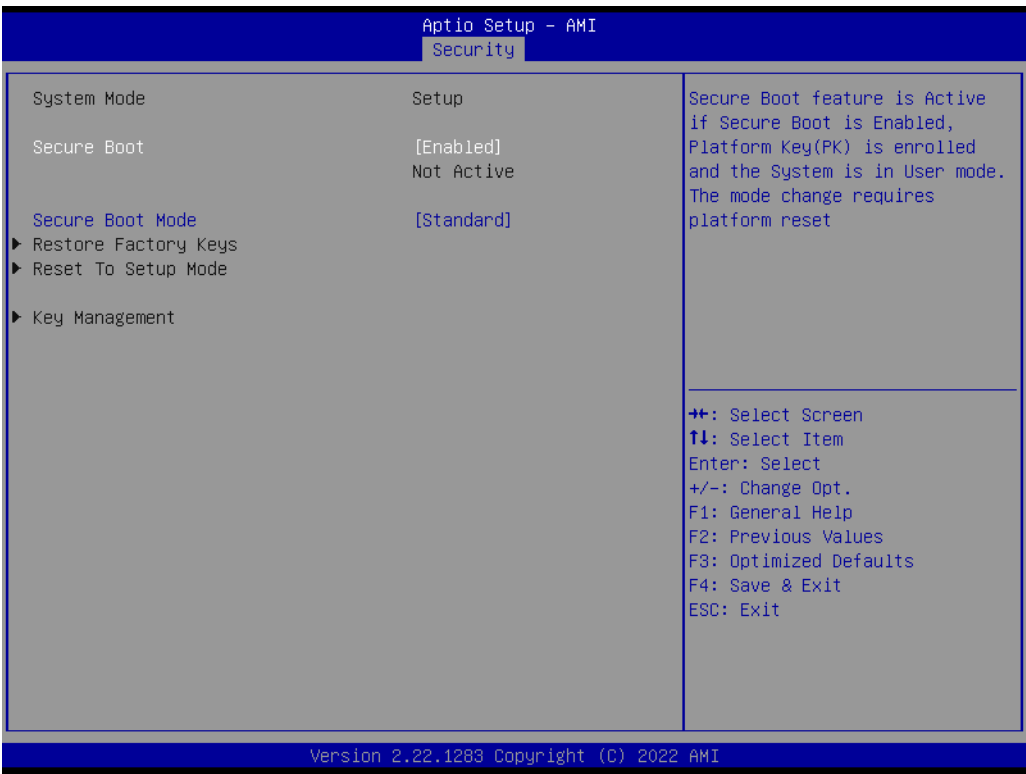


Figure 3.80 Secure Boot

- **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.

3.8 Boot



Figure 3.81 Boot

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

3.9 Save and Exit

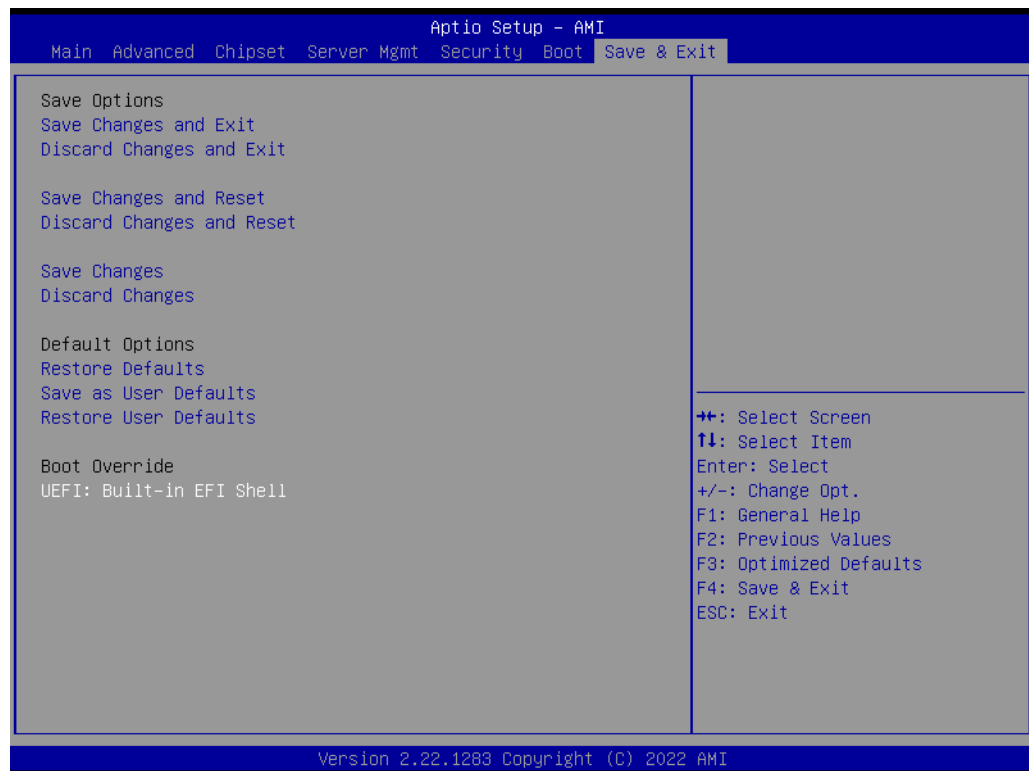


Figure 3.82 Save and Exit

- **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.

Chapter 4

S/W Introduction & Installation

- S/W Introduction
- Driver Installation
- Advantech iManager

4.1 S/W Introduction

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

4.2 Driver Installation

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

4.3 Windows Driver Setup

To install the drivers on a windows-based operating system, please connect to the Internet and go to the website: <http://support.advantech.com.tw>. Download the required drivers and follow the setup instructions to complete the installation.

4.4 Other OS

To install the drivers for Linux or other OS, please connect to the Internet and go to the following website: <http://support.advantech.com.tw> to download the setup file.

4.5 Advantech iManager

Advantech's 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-defined information. All the embedded functions are configured through API and provide corresponding utilities. These APIs comply with PICMG EAPI (Embedded Application Programmable Interface) specifications and unify in the same structures. It makes these embedded features easier to integrate while speeding up development schedules, and providing software continuity during hardware upgrades. For more details on 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 a 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 on the hardware pin assignment of the SOM-5993 CPU System on Module.

Sections include:

- SOM-5993 Type 7 Pin Assignment

A.1 SOM-5993 Type 7 Pin Assignment

This section details the SOM-5993 pin assignment on the COM Express connector which is compliant with COM Express R3.0 Type 7 pin-out definitions. To receive further details on using these pins, or to receive a design reference, please contact Advantech. We will provide a design guide, checklist, reference schematic, and other hardware/software support.

Table A.1: SOM-5993 ROWS A, B

A1	GND(FIXED)	B1	GND(FIXED)
A2	GBE0_MDI3-	B2	GBE0_ACT#
A3	GBE0_MDI3+	B3	LPC_FRAME#
A4	GBE0_LINK100#	B4	LPC_AD0
A5	GBE0_LINK1000#	B5	LPC_AD1
A6	GBE0_MDI2-	B6	LPC_AD2
A7	GBE0_MDI2+	B7	LPC_AD3
A8	GBE0_LINK#	B8	LPC_DRQ0#
A9	GBE0_MDI1-	B9	LPC_DRQ1#
A10	GBE0_MDI1+	B10	LPC_CLK
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#
A19	SATA0_RX+	B19	SATA1_RX+
A20	SATA0_RX-	B20	SATA1_RX-
A21	GND(FIXED)	B21	GND(FIXED)
A22	PCIE_TX15+	B22	PCIE_RX15+
A23	PCIE_TX15-	B23	PCIE_RX15-
A24	SUS_S5#	B24	PWR_OK
A25	PCIE_TX14+	B25	PCIE_RX14+
A26	PCIE_TX14-	B26	PCIE_RX14-
A27	BATLOW#	B27	WDT
A28	(S)ATA_ACT#	B28	GND
A29	RSVD	B29	PCIE1_CK_REF+
A30	RSVD	B30	PCIE1_CK_REF-
A31	GND(FIXED)	B31	GND(FIXED)
A32	IPMB_CLK	B32	SPKR
A33	IPMB_DAT	B33	I2C_CK
A34	BIOS_DIS0#	B34	I2C_DAT
A35	THRMTRIP#	B35	THRM#
A36	PCIE_TX13+	B36	PCIE_RX13+
A37	PCIE_TX13-	B37	PCIE_RX13-
A38	GND	B38	GND
A39	PCIE_TX12+	B39	PCIE_RX12+

A40	PCIE_TX12-	B40	PCIE_RX12-
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	RSVD	B48	-
A49	GBE0_SDP	B49	SYS_RESET#
A50	LPC_SERIRQ	B50	CB_RESET#
A51	GND(FIXED)	B51	GND(FIXED)
A52	PCIE_TX5+	B52	PCIE_RX5+
A53	PCIE_TX5-	B53	PCIE_RX5-
A54	GPI0	B54	GPO1
A55	PCIE_TX4+	B55	PCIE_RX4+
A56	PCIE_TX4-	B56	PCIE_RX4-
A57	GND	B57	GPO2
A58	PCIE_TX3+	B58	PCIE_RX3+
A59	PCIE_TX3-	B59	PCIE_RX3-
A60	GND(FIXED)	B60	GND(FIXED)
A61	PCIE_TX2+	B61	PCIE_RX2+
A62	PCIE_TX2-	B62	PCIE_RX2-
A63	GPI1	B63	GPO3
A64	PCIE_TX1+	B64	PCIE_RX1+
A65	PCIE_TX1-	B65	PCIE_RX1-
A66	GND	B66	WAKE0#
A67	GPI2	B67	WAKE1#
A68	PCIE_TX0+	B68	PCIE_RX0+
A69	PCIE_TX0-	B69	PCIE_RX0-
A70	GND(FIXED)	B70	GND(FIXED)
A71	PCIE_TX8+	B71	PCIE_RX8+
A72	PCIE_TX8-	B72	PCIE_RX8-
A73	GND	B73	GND
A74	PCIE_TX9+	B74	PCIE_RX9+
A75	PCIE_TX9-	B75	PCIE_RX9-
A76	GND	B76	GND
A77	PCIE_TX10+	B77	PCIE_RX10+
A78	PCIE_TX10-	B78	PCIE_RX10-
A79	GND	B79	GND
A80	GND(FIXED)	B80	GND(FIXED)
A81	PCIE_TX11+	B81	PCIE_RX11+
A82	PCIE_TX11-	B82	PCIE_RX11-
A83	GND	B83	GND
A84	NC	B84	VCC_5V_SBY
A85	GPI3	B85	VCC_5V_SBY
A86	RSVD	B86	VCC_5V_SBY
A87	RSVD	B87	VCC_5V_SBY

A88	PCIE_CK_REF+	B88	BIOS_DIS1#
A89	PCIE_CK_REF-	B89	NC
A90	GND(FIXED)	B90	GND(FIXED)
A91	SPI_POWER	B91	NC
A92	SPI_MISO	B92	NC
A93	GPO0	B93	NC
A94	SPI_CLK	B94	NC
A95	SPI_MOSI	B95	NC
A96	TPM_PP	B96	NC
A97	NC	B97	SPI_CS#
A98	SER0_TX	B98	NC
A99	SER0_RX	B99	NC
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)

Table A.2: SOM-5993 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	-	D15	-
C16	-	D16	-
C17	10G_SDP2	D17	10G_SDP3
C18	GND	D18	GND
C19	PCIE_RX6+	D19	PCIE_TX6+
C20	PCIE_RX6-	D20	PCIE_TX6-
C21	GND(FIXED)	D21	GND(FIXED)
C22	PCIE_RX7+	D22	PCIE_TX7+

C23	PCIE_RX7-	D23	PCIE_TX7-
C24	-	D24	-
C25	GND	D25	GND
C26	10G_KR_RX3+	D26	10G_KR_TX3+
C27	10G_KR_RX3-	D27	10G_KR_TX3-
C28	GND	D28	GND
C29	10G_KR_RX2+	D29	10G_KR_TX2+
C30	10G_KR_RX2-	D30	10G_KR_TX2-
C31	GND(FIXED)	D31	GND(FIXED)
C32	10G_SFP_SDA3	D32	10G_SFP_SCL3
C33	10G_SFP_SDA2	D33	10G_SFP_SCL2
C34	NC	D34	NC
C35	CEI_RST#	D35	CEI_PRSENT#
C36	10G_LED_SDA	D36	RSVD
C37	10G_LED_SCL	D37	RSVD
C38	10G_SFP_SDA1	D38	10G_SFP_SCL1
C39	10G_SFP_SDA0	D39	10G_SFP_SCL0
C40	10G_SDP0	D40	10G_SDP1
C41	GND(FIXED)	D41	GND(FIXED)
C42	10G_KR_RX1+	D42	10G_KR_TX1+
C43	10G_KR_RX1-	D43	10G_KR_TX1-
C44	GND	D44	GND
C45	-	D45	-
C46	CEI_MDC	D46	CEI_MDIO
C47	10G_INT0	D47	-
C48	GND	D48	GND
C49	10G_KR_RX0+	D49	10G_KR_TX0+
C50	10G_KR_RX0-	D50	10G_KR_TX0-
C51	GND(FIXED)	D51	GND(FIXED)
C52	PEG_RX0+	D52	PEG_TX0+
C53	PEG_RX0-	D53	PEG_TX0-
C54	GND	D54	-
C55	PEG_RX1+	D55	PEG_TX1+
C56	PEG_RX1-	D56	PEG_TX1-
C57	NC	D57	GND
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	RSVD
C64	RSVD	D64	RSVD
C65	PEG_RX4+	D65	PEG_TX4+
C66	PEG_RX4-	D66	PEG_TX4-
C67	RAPID_SHUTDOWN	D67	GND
C68	PEG_RX5+	D68	PEG_TX5+
C69	PEG_RX5-	D69	PEG_TX5-
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	RSVD	D77	RSVD
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	RSVD	D83	RSVD
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	RSVD	D97	RSVD
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 details information regarding watchdog timer programming for the SOM-5993 CPU System on Module.

- Section includes:
- Watchdog Timer Programming

B.1 Programming the Watchdog Timer

Table B.1: Programming the Watchdog Timer

Trigger Event	Note
IRQ	IRQ5, 7, 14 (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 selects an available IRQ number from the BIOS, and then sets it to EC. Only Win8.1 and Win10 support it.

In other OS, it will still use the IRQ number from the BIOS setting as usual.

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

Appendix **C**

Programming GPIO

This appendix provides a General Purpose Input and Output pin setting diagram.

Sections include:

- System I/O Ports

C.1 GPIO Register

Table C.1: GPIO Register

GPIO Byte Mapping	H/W Pin Name
BIT0	GPO0
BIT1	GPO1
BIT2	GPO2
BIT3	GPO3
BIT4	GPI0
BIT5	GPI1
BIT6	GPI2
BIT7	GPI3

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

Appendix **D**

System Assignments

This appendix details information on the system resource allocation of the SOM-5993 CPU System on Module.

Sections include:

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

D.1 System I/O Ports

Table D.1: System I/O Ports

Addr. Range(Hex)	Device
0x00000000-0x0000000F	Direct memory access controller
0x00000000-0x0000000F	PCI Express Root Complex
0x00000010-0x0000001F	Motherboard resources
0x00000020-0x0000003D	Programmable interrupt controller
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer
0x00000060-0x0000006F	Motherboard resources
0x00000061-0x00000061	System speaker
0x00000062-0x00000062	Microsoft ACPI-Compliant Embedded Controller
0x00000066-0x00000066	Microsoft ACPI-Compliant Embedded Controller
0x00000070-0x00000071	System CMOS/real time clock
0x00000072-0x00000073	System CMOS/real time clock
0x00000074-0x00000077	System CMOS/real time clock
0x00000080-0x00000080	Motherboard resources
0x00000081-0x00000083	Direct memory access controller
0x00000084-0x00000086	Motherboard resources
0x00000087-0x00000087	Direct memory access controller
0x00000088-0x00000088	Motherboard resources
0x00000089-0x0000008B	Direct memory access controller
0x0000008C-0x0000008E	Motherboard resources
0x0000008F-0x0000008F	Direct memory access controller
0x00000090-0x0000009F	Motherboard resources
0x000000A0-0x000000BD	Programmable interrupt controller
0x000000C0-0x000000DF	Direct memory access controller
0x000000F0-0x000000F0	Numeric data processor
0x00000200-0x0000027F	Motherboard resources
0x00000200-0x0000027F	Motherboard resources
0x00000280-0x0000028F	Motherboard resources
0x00000280-0x0000028F	Motherboard resources
0x00000290-0x0000029F	Motherboard resources
0x00000299-0x0000029A	Motherboard resources
0x0000029E-0x000002AD	Motherboard resources
0x000002A0-0x000002BF	Motherboard resources
0x000002A0-0x000002BF	Motherboard resources
0x000002C0-0x000002DF	Motherboard resources
0x000002F0-0x000002F7	Motherboard resources
0x000002F8-0x000002FF	Communications Port (COM2)
0x00000300-0x0000037F	Motherboard resources
0x000003B0-0x000003BB	CDF PCIeRP[2] - 18A6
0x000003B0-0x000003BB	PCI Express to PCI/PCI-X Bridge
0x00003000-0x00003FFF	CDF PCIeRP[3] - 18A7
0x000003C0-0x000003DF	CDF PCIeRP[2] - 18A6
0x000003C0-0x000003DF	PCI Express to PCI/PCI-X Bridge

Table D.1: System I/O Ports

0x000003F8-0x000003FF	Communications Port (COM1)
0x00000400-0x0000041F	Motherboard resources
0x000004D0-0x000004D1	Programmable interrupt controller
0x00000500-0x000005FE	Motherboard resources
0x00000500-0x000005FE	Motherboard resources
0x00001000-0x00005FFF	PCI Express Root Complex
0x00004000-0x00004FFF	CDF PCIeRP[2] - 18A6
0x00004000-0x00004FFF	PCI Express to PCI/PCI-X Bridge
0x00004000-0x00004FFF	ASPEED Graphics Family(WDDM)
0x00005000-0x0000501F	CDF LegacySMBus - 18DF
0x00005020-0x0000503F	Standard SATA AHCI Controller
0x00005040-0x00005047	CDF HSUART - 18D8
0x00005050-0x00005057	CDF HSUART - 18D8
0x00005060-0x00005067	CDF HSUART - 18D8
0x00005070-0x00005073	Standard SATA AHCI Controller
0x00005080-0x00005087	Standard SATA AHCI Controller
0x00006000-0x0000AFFF	PCI Express Root Complex
0x0000B000-0x0000FFFF	PCI Express Root Complex

D.2 DMA Channel Assignments

Table D.2: DMA Channel Assignments

Channel	Function
4	Direct memory access controller

D.3 Interrupt Assignments

Table D.3: Interrupt Assignments

Interrupt#	Interrupt Source
IRQ 0	System timer
IRQ 3	Communications Port (COM2)
IRQ 4	Communications Port (COM1)
IRQ 6	Motherboard resources
IRQ 8	System CMOS / real time clock
IRQ 13	Numeric data processor
IRQ 16	SDA Standard Compliant SD Host Controller
IRQ 16	ASPEED Graphics Family (WDDM)
IRQ 54~511	Microsoft ACPI-Compliant System
IRQ 4294967266~4294967276	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967277~ 4294967288	Intel® I210 Gigabit Network Connection
IRQ 4294967289	Intel® USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
IRQ 4294967290	Standard SATA AHCI Controller
IRQ 4294967291	PCI Express Root Port
IRQ 4294967292	CDF PCIeRP[8] - 18AD
IRQ 4294967293	CDF PCIeRP[3] - 18A7
IRQ 4294967294	CDF PCIeRP[2] - 18A6

D.4 1st MB Memory Map

Table D.4: 1st MB Memory Map

Addr. Range (Hex)	Device
0x90000000-0xB3FFFFFF	PCI Express Root Complex
0xA0000-0xBFFFF	CDF PCIeRP[2] - 18A6
0xA0000-0xBFFFF	PCI Express Root Complex
0xA0000-0xBFFFF	PCI Express to PCI/PCI-X Bridge
0xAC000000-0xB0FFFFFF	CDF PCIeRP[2] - 18A6
0xAC000000-0xB0FFFFFF	PCI Express to PCI/PCI-X Bridge
0xAC000000-0xB0FFFFFF	ASPEED Graphics Family (WDDM)
0xB0000000-0xB001FFFF	ASPEED Graphics Family (WDDM)
0xB0100000-0xB03FFFFFF	CDF PCIeRP[8] - 18AD
0xB02FC000-0xB02FFFFFF	Intel® Ethernet Controller (3) I225-IT
0xB0300000-0xB03FFFFFF	Intel® Ethernet Controller (3) I225-IT
0xB0400000-0xB04FFFFFF	CDF PCIeRP[3] - 18A7
0xB047C000-0xB047FFFF	Intel® I210 Gigabit Network Connection
0xB0480000-0xB04FFFFFF	Intel® I210 Gigabit Network Connection
0xB0580000-0xB05FFFFFF	Intel® PMON MSM Registers - 09A7
0xB0600000-0xB067FFFF	Intel® PMON MSM Registers - 09A7
0xB0680000-0xB0681FFF	Standard SATA AHCI Controller
0xB0682000-0xB0683FFF	Intel® MSM Registers - 09A6
0xB0687000-0xB06877FF	Standard SATA AHCI Controller

Table D.4: 1st MB Memory Map	
0xB0688000-0xB06880FF	Standard SATA AHCI Controller
0xB4000000-0xD7FFFFFF	PCI Express Root Complex
0xC8000-0xCFFFF	PCI Express Root Complex
0xD8000000-0xFB7FFFFF	PCI Express Root Complex
0xD8000000-0xFC4FFFFF	PCI Express Root Port
0xFB300000-0xFB6FFFFF	PCI Express Root Port
0xFD000000-0xFD69FFFF	Motherboard resources
0xFD6C0000-0xFD6CFFFF	Motherboard resources
0xFD6F0000-0xFDFFFFFF	Motherboard resources
0xFDC20000-0xFDC21FFF	
0xFDC50000-0xFDC51FFF	
0xFE000000-0xFE01FFFF	Motherboard resources
0xFE010000-0xFE010FFF	CDF SPI - 18E0
0xFE010000-0xFE010FFF	PCI Express Root Complex
0xFE200000-0xFE7FFFFF	Motherboard resources
0xFEC00000-0xFECFFFFF	Advanced programmable interrupt controller
0xFED00000-0xFED003FF	High precision event timer
0xFED40000-0xFED44FFF	Trusted Platform Module 2.0
0xFF000000-0xFFFFFFFF	Motherboard resources
0xFF000000-0xFFFFFFFF	Motherboard resources
0xFFA00000-0xFFA1FFFF	CDF PCIeRP[8] - 18AD
0xFFA20000-0xFFA3FFFF	CDF PCIeRP[3] - 18A7
0xFFA40000-0xFFA5FFFF	CDF PCIeRP[2] - 18A6
0xFFA80000-0xFFA8FFFF	Intel® USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
0xFFAB8000-0xFFAB8FFF	CDF ME:HECI#3 - 18D6
0xFFAB9000-0xFFAB9FFF	CDF ME:HECI#2 - 18D4
0xFFABA000-0xFFABAFFF	CDF ME:HECI#1 - 18D3
0xFFFFF000-0xFFFFFFFF	SDA Standard Compliant SD Host Controller



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