



User Manual

SOM-D580

**Intel® Xeon® D-2700 Processor
(Ice Lake-D HCC)
COM-HPC® Server Size D**

ADVANTECH

Enabling an Intelligent Planet

Copyright

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

Acknowledgments

AMD® is a trademark of 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 could cause personal injury if not observed!



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



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

Note! Notes provide additional and/or optional information.



Document Feedback

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

Packing List

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

- SOM-D580 CPU module

Selection Guide w/ P/N

Part No.	SoC	Cores	Base Freq.	Max Turbo Freq.	SoC TDP	LLC	DDR4 RDIMM/ LRDIMM	Ethernet Mode	PCIe Gen. 4 Lanes	Power	Thermal Solution	Operating Temp.
SOM-D580D20-U0A1	D-2796TE	20	2.0 GHz	3.1 GHz	118W	30MB	2933MT/s	100G	32	AT/ATX	Active * Optional Accessories	0~60°C
SOM-D580D16-U0A1	D-2775TE	16	2.0 GHz	3.1 GHz	100W	25MB	2933MT/s	100G	32	AT/ATX	Active * Optional Accessories	0~60°C
SOM-D580D12-S8A1	D-2752TE R	12	1.8 GHz	2.8 GHz	77W	20MB	2667MT/s	50G	32	AT/ATX	Active * Optional Accessories	0~60°C
SOM-D580D8-U1A1	D-2733NT	8	2.1 GHz	3.2 GHz	80W	15MB	2667MT/s	50G	32	AT/ATX	Active * Optional Accessories	0~60°C
SOM-D580D4-S9A1	D-2712T	4	1.9 GHz	3.0 GHz	65W	15MB	2667MT/s	50G	32	AT/ATX	Active * Optional Accessories	0~60°C
SOM-D580D20X-U0A1	D-2796TE	20	2.0 GHz	3.1 GHz	118W	30MB	2933MT/s	100G	32	AT/ATX	Active * Optional Accessories	-40~85°C
SOM-D580D16X-U0A1	D-2775TE	16	2.0 GHz	3.1 GHz	100W	25MB	2933MT/s	100G	32	AT/ATX	Active * Optional Accessories	-40~85°C
SOM-D580D12X-S8A1	D-2752TE R	12	1.8 GHz	2.8 GHz	77W	20MB	2667MT/s	50G	32	AT/ATX	Active * Optional Accessories	-40~85°C

Development Board

Part No.	Description
SOM-DH5000-00A1	COM-HPC Size D Development Board A1 With 10GBASE-KR OCP cards (SOM-EA70 + SOM-EA64)
SOM-DH5000-01A1	COM-HPC Size D Development Board A1 With 25GBASE-KR OCP card (SOM-EA71)

Optional Accessories

Part No.	Description
1970005587T001	One-piece heatsink, H.S R4 Intel® Xeon® D HCC 118W 120x98x23.5 mm
1970005122N001	Add-on fan module, CL R3 160x160 SC for SOM-D580

Safety Instructions

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

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

Safety Precautions - Static Electricity

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

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

Acronyms

Term	Definition
AC'97	Audio CODEC (Coder-Decoder)
ACPI	Advanced Configuration Power Interface – standard to implement power saving modes in PC-AT systems
BIOS	Basic Input Output System – firmware in PC-AT 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 – containing DisplayPort, HDMI/DVI, and SDVO
EAPI	<p>Embedded Application Programmable Interface Software interface for COM Express® specific industrial function</p> <ul style="list-style-type: none"> ■ 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 system time and date as well as certain system setup parameters
SPD	Serial Presence Detect – refers to serial EEPROM on DRAM that has DRAM Module configuration information
TPM	Trusted Platform Module - a chip to enhance the security features of a computer system
UEFI	Unified Extensible Firmware Interface
WDT	Watchdog Timer

Contents

Chapter 1	General Information	1
1.1	Introduction	2
1.2	Functional Block Diagram	3
	Figure 1.1 Block Diagram	3
1.3	Product Specifications.....	4
1.3.1	Compliance.....	4
1.3.2	Feature List.....	4
	Table 1.1: Feature List.....	4
1.3.3	Processor System.....	5
	Table 1.2: Processor System	5
1.3.4	Memory	5
1.3.5	Expansion Interface	5
	Table 1.3:	5
	Table 1.4:	5
	Table 1.5:	5
1.3.6	Serial Bus.....	6
1.3.7	I/O	6
	Table 1.6: USB 3.2 Gen1	6
	Table 1.7: USB 2.0	6
	Table 1.8:	7
	Table 1.9:	7
1.3.8	Power Management.....	8
1.3.9	Advantech S5 ECO Mode (Deep Sleep Mode).....	9
1.3.10	Environmental Specifications.....	9
1.3.11	MTBF	9
1.3.12	OS Support	9
1.3.13	Advantech iManager	10
1.3.14	Power Consumption.....	10
	Table 1.10: Power Consumption Table (Watts).....	10
1.3.15	Performance	10
1.3.16	Pin Descriptions	10
Chapter 2	Mechanical Information	11
2.1	Board Information.....	12
	Figure 2.1 Board Chips ID – Front.....	12
	Figure 2.2 Board Chips ID – Rear	13
2.2	Mechanical Diagrams.....	14
	Figure 2.3 Board Mechanical Diagram – Front.....	14
	Figure 2.4 Board Mechanical Diagram – Rear	14
	Figure 2.5 Board Mechanical Diagram – Side	15
2.3	Assembly Diagram	16
	Figure 2.6 Assembly Drawing	16
2.4	Assembly Drawings.....	17
2.4.1	Allowable Initial Angular Misalignment.....	17
	Figure 2.7 Initial Angular Misalignment.....	17
2.4.2	Allowable Final Angular Misalignment	17
	Figure 2.8 Final Angular Misalignment	17
2.5	CPU Package Design	18
	Table 2.1: CPU Package Design	18
Chapter 3	AMI BIOS	19

3.1	Introduction	20
	Figure 3.1 Setup Program Initial Screen	20
3.2	Entering Setup	21
3.2.1	Main Setup.....	21
	Figure 3.2 Main Setup Screen	21
3.2.2	Advanced BIOS Features Setup.....	22
	Figure 3.3 Advanced BIOS Features Setup Screen.....	22
	Figure 3.4 Trusted Computing.....	23
	Figure 3.5 ACPI Settings.....	24
	Figure 3.6 Embedded Controller	25
	Figure 3.7 Serial Port 1 Configuration	26
	Figure 3.8 Serial Port 2 Configuration	27
	Figure 3.9 Hardware Monitor.....	28
	Figure 3.10Serial Port Console Redirection	29
	Figure 3.11Console Redirection Settings.....	30
	Figure 3.12PCI Subsystem Settings.....	31
	Figure 3.13PCI Express Settings	32
	Figure 3.14PCI Express GEN2 Settings.....	33
	Figure 3.15USB Configuration.....	35
	Figure 3.16PCI Network Stack Configuration.....	36
	Figure 3.17NVMe Configuration	37
	Figure 3.18Option ROM Dispatch Policy.....	38
	Figure 3.19TIs Auth Configuration.....	41
	Figure 3.20Enroll Cert	42
	Figure 3.21Enroll Cert Using File	43
	Figure 3.22Emulation Configuration	44
	Figure 3.23Port Option Configuration.....	45
	Figure 3.24Port Options	46
	Figure 3.25Chipset	47
	Figure 3.26Socket Configuration	48
	Figure 3.27Processor Configuration.....	49
	Figure 3.28Chipset	50
	Figure 3.29Chipset	52
	Figure 3.30CPU Socket 0 Configuration	53
	Figure 3.31CPU Socket 0 Configuration	54
	Figure 3.32Global PSMI	55
	Figure 3.33Socket 0 Configuration	56
	Figure 3.34Processor Dfx Configuration	57
	Figure 3.35IIO Configuration	58
	Figure 3.36Socket 0 Configuration	59
	Figure 3.37Trace Hub Configuration	60
	Figure 3.38R-Link.....	61
	Figure 3.39Chipset.....	62
	Figure 3.40Port 1A	63
	Figure 3.41Port 1A	64
	Figure 3.42Port 2A	66
	Figure 3.43Port 2A	67
	Figure 3.44Port 2C	69
	Figure 3.45Port 2C	70
	Figure 3.46Intel® VT for Directed I/O (VT-d).....	72
	Figure 3.47Intel® VMD technology.....	73
	Figure 3.48VMD Config	74
	Figure 3.49Package C State Control.....	75
	Figure 3.50Latency Tolerance Requirement	76
	Figure 3.51PkgC SA PS Criteria Power Management Control... 77	
	Figure 3.52CPU0 PKGC_SA_PS_CRITERIA	78
	Figure 3.53PKGc Interrupt Response Time	79
	Figure 3.54ACPI Sx State Control.....	80
	Figure 3.55Memory Power & Thermal Configuration	81
	Figure 3.56DRAM RAPL Configuration	82

Figure 3.57	Memory Thermal Configuration	83
Figure 3.58	Memory Power & Thermal Configuration	84
Figure 3.59	PCH-IO Configuration.....	85
Figure 3.60	PCI Express Configuration	86
Figure 3.61	PCI Express Configuration	87
Figure 3.62	PCI Express Configuration	88
Figure 3.63	PCI Express Configuration	89
Figure 3.64	PCI Express Configuration	90
Figure 3.65	PCI Express Configuration	91
Figure 3.66	PCI Express Configuration	92
Figure 3.67	PCI Express Configuration	93
Figure 3.68	PCI Express Configuration	94
Figure 3.69	PCI Express Configuration	95
Figure 3.70	PCI Express Configuration	96
Figure 3.71	PCI Express Configuration	97
Figure 3.72	PCI Express Configuration	98
Figure 3.73	Fia Mux Configuration	99
Figure 3.74	SATA Configuration.....	102
Figure 3.75	Controller SATA Configuration	103
Figure 3.76	USB Configuration.....	104
Figure 3.77	USB Configuration.....	105
Figure 3.78	Security Configuration	106
Figure 3.79	System Event Log	107
Figure 3.80	eMCA Settings.....	108
Figure 3.81	Whea Settings	109
Figure 3.82	Error Injection Settings	110
Figure 3.83	Memory Error Enabling.....	111
Figure 3.84	IIO Error Enabling.....	112
Figure 3.85	IIO Error Enabling.....	113
Figure 3.86	PCIe Error Enabling.....	114
Figure 3.87	PCIe Error Enabling.....	116
Figure 3.88	Error Control Setting.....	117
Figure 3.89	Server Mgmt.....	118
3.2.3	Security Chipset.....	123
Figure 3.90	Security Chipset	123
Figure 3.91	Secure Boot.....	125
Figure 3.92	Boot Setup.....	126
3.2.4	Save & Exit	127
Figure 3.93	Save & Exit.....	127
3.2.5	MEBx Login.....	128

Chapter 4 S/W Introduction & Installation129

4.1	S/W Introduction.....	130
4.2	Driver Installation	130
4.2.1	Windows Driver Setup	130
4.2.2	Other OS.....	130
4.3	Advantech iManager	131

Appendix A Pin Assignment133

A.1	SOM-D580 Pin Assignment	134
	Table A.1: J1 Connector Rows A and B	134
	Table A.2: J1 Connector Rows C and D	137
	Table A.3: J2 Connector Rows E and F.....	140
	Table A.4: J2 Connector Rows G and H.....	143

Appendix B	Watchdog Timer	147
B.1	Programming the Watchdog Timer	148
	Table B.1: Programming the Watchdog Timer	148
Appendix C	Programming GPIO.....	149
C.1	GPIO Register.....	150
	Table C.1: GPIO Register	150
Appendix D	System Assignments.....	151
D.1	System I/O Ports.....	152
	Table D.1: System I/O Ports	152
D.2	Interrupt Assignments	153
	Table D.2: Interrupt Assignments	153
D.3	1st MB Memory Map.....	164
	Table D.3: 1st MB Memory Map	164

Chapter 1

General Information

This chapter details background information on the SOM-D580 CPU Computer-on-Module.

Sections include:

- Introduction
- Functional Block Diagram
- Product Specifications

1.1 Introduction

The Advantech SOM-D580 is a COM-HPC Server Type Size D module with superior performance based on an Intel® Xeon® D-2700 processor (Intel Ice Lake-D HCC). These Xeon® processors offer up to 20 cores of computing power under 118-Watt TDP. They can be deployed for such applications as 5G base stations, in-flight entertainment, in-vehicle radar, cloud storage, and high-end testing applications. SOM-D580 supports Advantech's ready-to-use Edge AI Suite software toolkit.

In terms of memory, SOM-D580 supports either 4 x RDIMM (up to 256GB) or 4 x LRDIMM (up to 512GB). There is additional expansion room for 32 x PCIe Gen 4 and 17 x PCIe Gen 3 lanes. High-bandwidth Ethernet Connectivity is also integrated with 8 x 10G or 4 x 25G Intel integrated Ethernet (according to CPU SKU) for particular applications. It also comes equipped with high-speed I/O expansion consisting of 2 x SATA 3.0, 4 x USB 3.2 Gen1, and 4 x USB 2.0.

SOM-D580 is suitable for use in rugged outdoor applications due to its wide operating temperature range (-40~85°C) and we offer the QFCS 2.0 advanced thermal solution for enhanced thermal performance in a slimmer and lighter form factor.

SOM-D580 also supports IPMB for BMC remote control, and onboard TPM with advanced security. Additionally, it supports both secure boot and fast boot which can be changed in the BIOS settings.

Advantech iManager (SUSI4) satisfies diverse requirements by supporting multi-level watchdog timers, voltage and temperature monitoring, thermal protection and mitigation, LCD backlight on/off and brightness control, and embedded storage. All Advantech COM-HPC modules integrate iManager and WISE-PaaS/RMM.

1.2 Functional Block Diagram

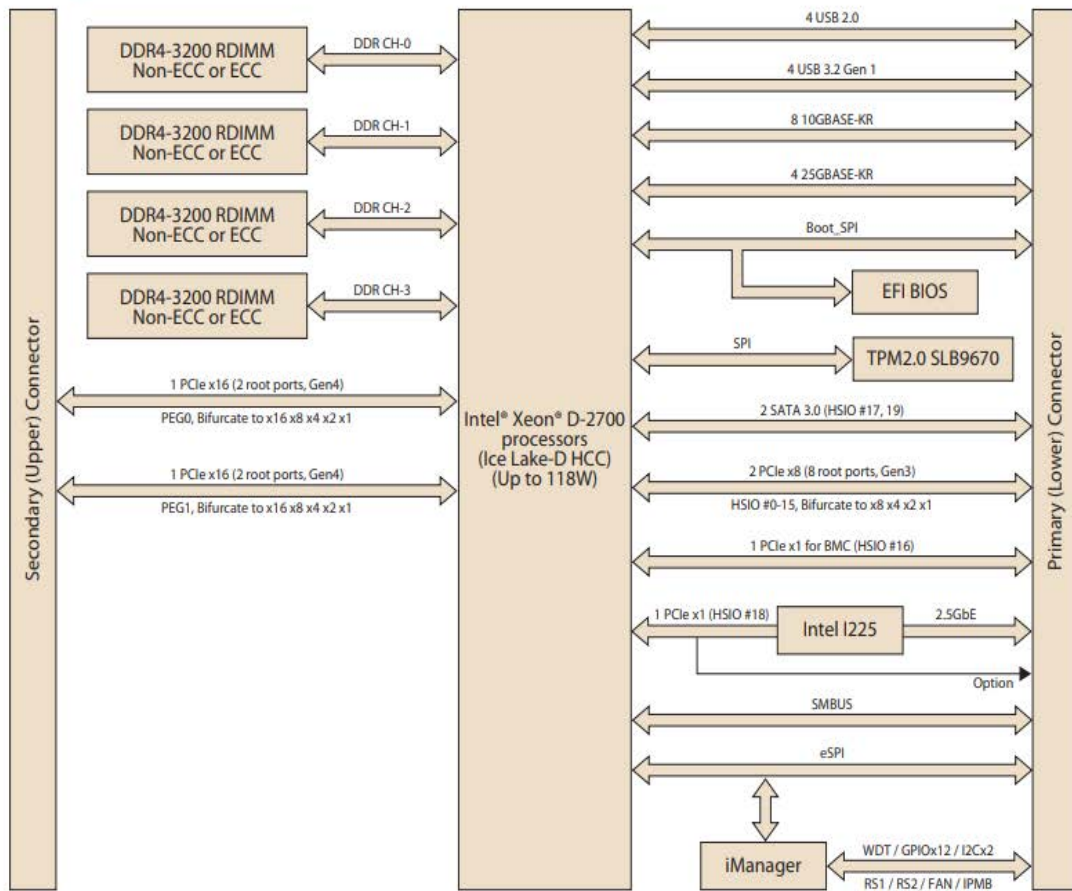


Figure 1.1 Block Diagram

1.3 Product Specifications

1.3.1 Compliance

- PICMG COM-HPC Revision 1.10
- COM-HPC® Size D - 160 x 160 mm
- Pinout Server Type compatible

1.3.2 Feature List

Table 1.1: Feature List

Feature	Server Module Min/Max	SOM-D580
NBASE-T	1/1	1
Ethernet KR/KX	2/8	8
SATA	0/2	2
PCIe 0:47	4/48	48
PCIe 48:63	0/16	0
PCIe BMC	1/1	1
PCIe Target on Module Support	0/2	0
USB 2.0 Ports 0:7	4 / 8	4
USB 3.2 Gen 1 or Gen 2	0/4	4
USB 3.2 Gen 2x2	0/2	0
USB 4.0	0/2	0
eSPI	0/1	1
Boot SPI Interface	1/1	1
BIOS Select Options	1/1	1
Digital Display Interfaces (DDI)	N/A	N/A
eDP	N/A	N/A
MIPI Display Serial Interface (DSI)	N/A	N/A
MIPI Camera Serial Interface (CSI)	N/A	N/A
Audio	N/A	N/A
I2S Audio /2nd SoundWire/HDA	N/A	N/A
Asynchronous Serial Ports	1/2	2
I2C Ports	2/2	2
IPMB	0/1	1
General Purpose SPI Port	1/1	1
Power and System Management	1/1	1
Rapid Shutdown	0/1	1
Thermal Protection	1/1	1
System Management Bus	1/1	1
GPIO	12/12	12
FuSa Set of Signals	0/1	0
Module Type Pin Support	1/1	1
Watchdog Timer	0/1	1
Secondary Fan Tach and PWM	1/1	1
VCC	28/28	28
VCC_5V_SBY support	0/2	2
VCC_RTC	1/1	1
Connector J1	1/1	1
Connector J2	1/1	1
GND	All	All

1.3.3 Processor System

Table 1.2: Processor System

SoC	Cores	Base Freq.	Max Turbo Freq.	SoC TDP	Catch (MB)
D-2796TE	20	2.0 GHz	3.1 GHz	118W	30MB
D-2775TE	16	2.0 GHz	3.1 GHz	100W	25MB
D-2752TER	12	1.8 GHz	2.8 GHz	77W	20MB
D-2733NT	8	2.1 GHz	3.2 GHz	80W	15MB
D-2712T	4	1.9 GHz	3.0 GHz	65W	15MB

1.3.4 Memory

There are a total of 4 memory sockets on SOM-D580.

4 x RDIMM, 1 x DPC, 3200 MT/s, max DIMM capacity 64GB, up to 256GB.

4 x LRDIMM, 1 x DPC, 3200 MT/s, max DIMM capacity 128GB, up to 512GB.

1.3.5 Expansion Interface

32 x PCIe Gen 4 and 17 x PCIe Gen 3 (1 x PCIe x1 Gen 3 for BMC) for a total of 49 lanes.

1.3.5.1 PCIe Gen 3 x1

PCI Express x1: Supports 17 x PCIe Gen 3 (1 x PCIe x1 Gen 3 for BMC). Several configurable combinations may need BIOS modification. Please contact Advantech sales or FAE for more details.

Table 1.3:

Server Type	Primary J1							
PCIe Lane	PCIe0	PCIe1	PCIe2	PCIe3	PCIe4	PCIe5	PCIe6	PCIe7
Default/Option	PCIe x4_Slot1				PCIe x4_Slot2			

Table 1.4:

Server Type	Primary J1				
PCIe Lane	PCIe8-11	PCIe12	PCIe13	PCIe14	PCIe15
Default	PCIe x4_Slot3	PCIe x4_Slot0		I210	NA
Option	PCIe x4_Slot3	PCIe x4_Slot0			

Table 1.5:

Server Type	Primary J2
PCIe Lane	PCIe16~31
Default/Option	PCIe x16 (for PEG)

1.3.6 Serial Bus

1.3.6.1 SMBus

Supports the SMBus 2.0 specification.

1.3.6.2 I²C Bus

Supports 2 x I2C bus. In standard mode, it supports up to 100 Kb/s, and in fast mode up to 400 Kb/s.

1.3.7 I/O

1.3.7.1 Gigabit Ethernet

Ethernet: Intel® I225IT Gigabit LAN Controller supports 10/100/1000 Mbps & 2.5 Gbps speeds.

1.3.7.2 SATA

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

1.3.7.3 USB 3.2 / USB 2.0

Supports 4 x USB 3.2 Gen1 (5 Gbps) and 4 x USB 2.0 (480 Mbps).

Notice: Advantech strongly recommends using a certified cable to maximize USB 3.2 Gen2 performance.

1.3.7.4 USB 3.2 Gen1

Table 1.6: USB 3.2 Gen1

Server Type	P00	P01	P10	P11	P2	P3
SoC	P0	NA	P1	NA	P2	P3
Server Type	OC_01				OC_23	
SoC USB_OC#	OC_01				OC_23	

1.3.7.5 USB 2.0

Table 1.7: USB 2.0

Server Type	P00	P01	P02	P03	P04	P05	P06	P07
SoC	P1	P2	P3	P4	NA			
Server Type	OC_01		OC_23		NA			
SoC USB_OC#	OC_01		OC_23		NA			

1.3.7.6 SPI Bus

Supports BIOS flash only. The SPI clock can be 50MHz, with a capacity up to 256Mb.

1.3.7.7 GPIO

12 programmable general purpose inputs or outputs (GPIO).

1.3.7.8 Watchdog

Supports multi-level watchdog time-out output. Provides 1-65535 levels, from 100ms to 109.22 minute intervals.

1.3.7.9 Serial Ports

2 x 2-wire serial ports (Tx/Rx) supporting 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 bits selectable
- Baud rate up to 115.2K

1.3.7.10 TPM

Supports a TPM 2.0 module.

1.3.7.11 Smart Fan

Supports 1 Fan PWM control signal and 1 tachometer input for fan speed detection. There is 1 connector on the module with 1 other connector on the carrier board, following PICMG COM HPC R1.10 specifications.

1.3.7.12 BIOS

The BIOS chip is on the module by default. Users can place a BIOS chip on the carrier board with the appropriate design and jumper settings for BSEL#[2:0].

Table 1.8:

BSEL #2	BSEL #1	BSEL S#0	Bootup Destination/Function
NA	NA	Open	Boot from Module SPI BIOS
NA	NA	GND	Boot from Carrier SPI BIOS

Note! *If system COMS is cleared, it is strongly suggested to go to the BIOS setup menu and load the default settings when booting up for the first time.*



The standard module has no jumper at SCN2, so BIOS settings are kept without an RTC coin battery. If you need to restore the BIOS to default settings, follow the steps below.

Table 1.9:

Pin	Function
NA	N/A [Default]
1-2	BIOS clear CMOS, load default settings

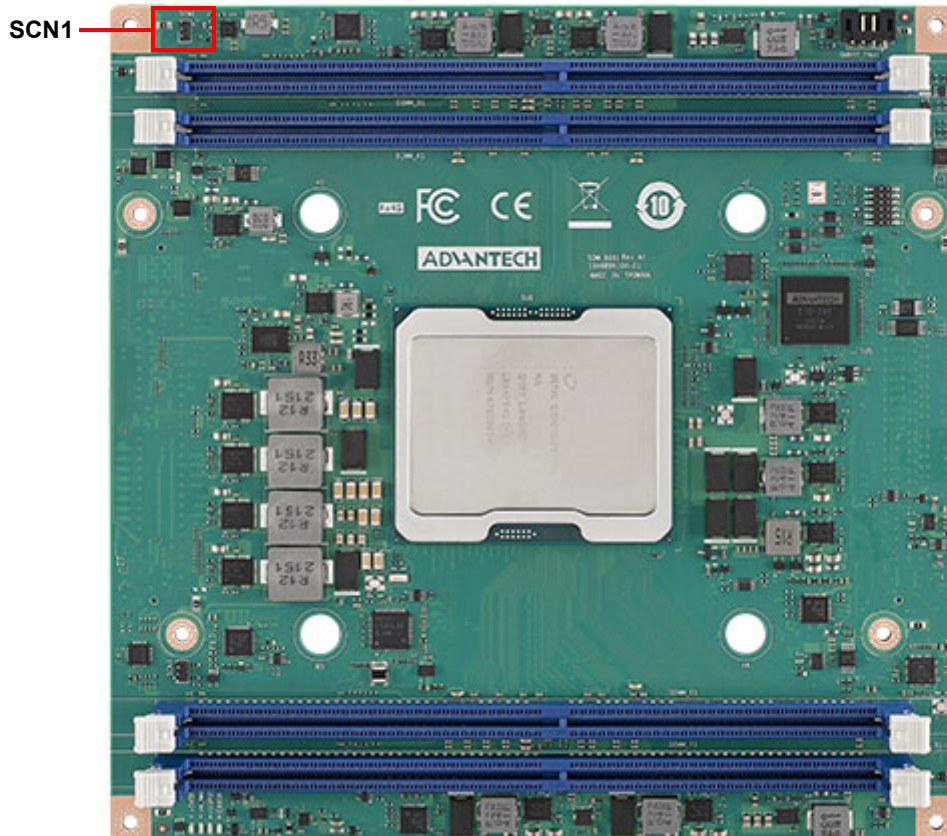


Reserved

Or



BIOS Default Settings



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

1.3.8 Power Management

1.3.8.1 Power Supply

Supports both ATX and AT power modes. VSB is for suspended power and can be optional if not required by standby (suspend-to-RAM) support. The RTC battery may be optional if date/timekeeping is not required.

- **Vin:** 12V +/- 5%
- **VSB:** 5V +/- 5% (suspend power)
- **RTC Battery Power:** 2.0V - 3.3V

1.3.8.2 PWROK

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

1.3.8.3 Power Sequence

According to PICMG COM Express R1.10 specifications.

1.3.8.4 Wake Event

Various wake event support allows users to apply it to different scenarios.

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

1.3.9 Advantech S5 ECO Mode (Deep Sleep Mode)

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

1.3.10 Environmental Specifications

1.3.10.1 Temperature

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

1.3.10.2 Humidity

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

1.3.10.3 Vibrations

IEC60068-2-64: Random vibration test under non-operation mode, 3.5 Grms. For operation, please contact Advantech sales or FAE for more details.

1.3.10.4 Drop Test (Shock)

Federal Standard 101 Method 5007 test procedure with standard packing.

1.3.10.5 EMC

CE EN55032 Class B and FCC Certifications: validated with standard development boards in the Advantech chassis.

1.3.11 MTBF

Please refer to the Advantech SOM-D580 Refresh Series Reliability Prediction report on the website: Link: <http://com.advantech.com>

1.3.12 OS Support

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

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

1.3.13 Advantech iManager

Supports APIs for GPIO, smart fan control, multi-stage watchdog timer, temperature sensor, and hardware monitoring. Follows PICMG EAPI 1.0 specifications with backward compatibility.

1.3.14 Power Consumption

Table 1.10: 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	
SOM-D580D20-U0A1	178.12	147.47	71.06	7.63	0.35	2.54
SOM-D580D4-S9A1	100.73	96.30	67.45	6.89	0.32	4.55
SOM-D580D12-S8A1	124.88	110.38	68.30	6.46	0.33	4.23
SOM-D580D8-U1A1	123.29	108.84	67.50	6.86	0.35	8.3
SOM-D580D16-U0A1	157.98	137.35	72.67	8.49	1.04	7.91

1.3.14.1 Hardware Configuration

- **MB:** SOM-D580D20-U0A1
- **DRAM:** 512GB DDR4 3200MHz x 4pcs
- **Carrier board:** SOM-DH5000-00A1/SOM-DH5000-01A1

1.3.14.2 Test Conditions

- **Test temperature:** room temperature (about 25°C)
- **Test voltage:** rated voltage DC +12V
- **Test loading:**
 - Maximum load mode: According to Intel thermal/power test tools.
 - Burn-in mode: Burn-in test V8.1 Pro (1023) for 64-bit Windows. (CPU, RAM, 2D&3D Graphics, and Disk with 100%)
 - Idle mode: DUT power management off and not running any programs

1.3.15 Performance

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

1.3.16 Pin Descriptions

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

Please contact your nearest Advantech branch office or call to obtain design documents and further support.

Chapter 2

Mechanical Information

This chapter details mechanical information for the SOM-D580 CPU Computer-on-Module.

Sections include:

- Board Information
- Mechanical Diagrams
- Assembly Diagrams

2.1 Board Information

The figures below indicate the main chips on the SOM-D580 Computer-on-Module. Please be aware of these positions while designing your own carrier board to avoid mechanical issues and ensure there is sufficient space for thermal solution contact points for best thermal dissipation performance.

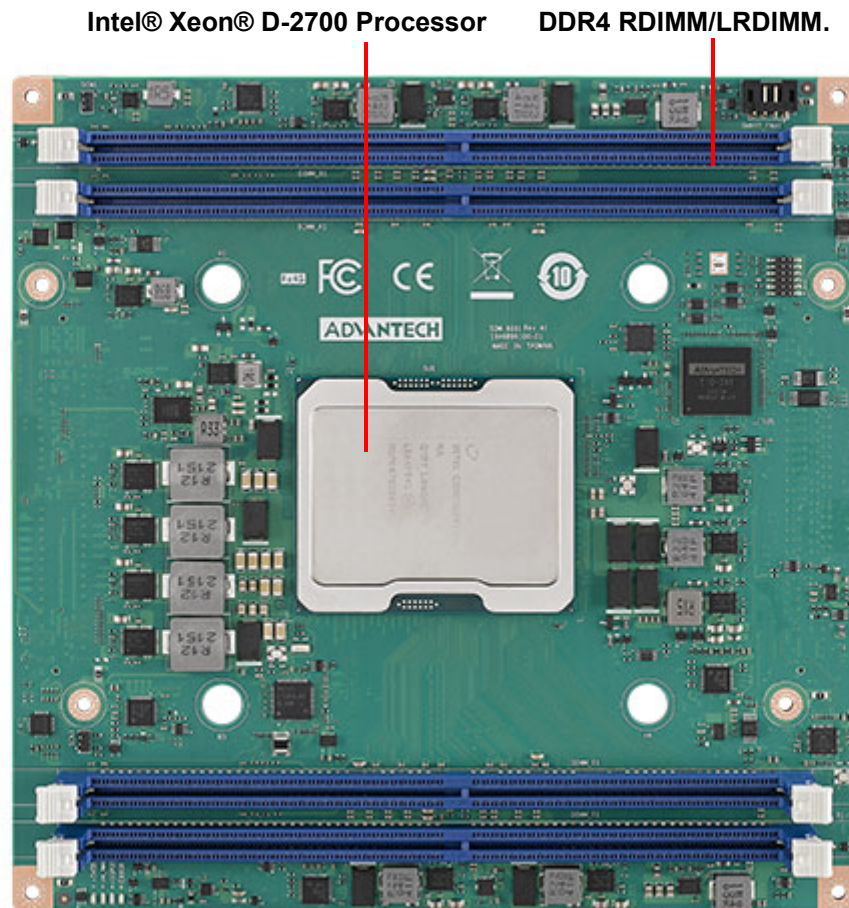
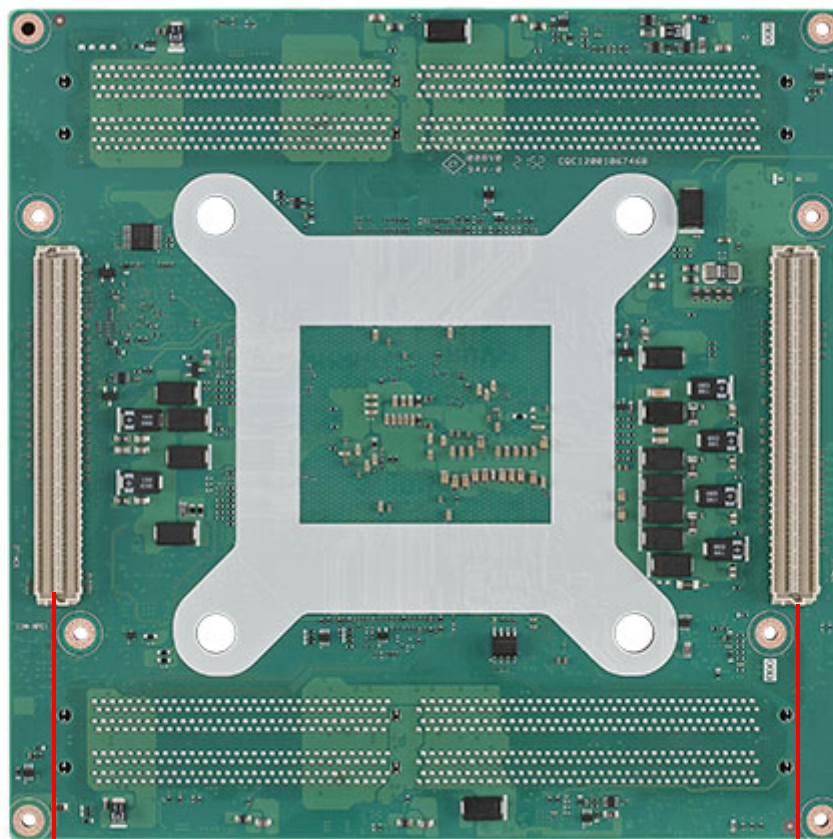


Figure 2.1 Board Chips ID – Front



COM HPC Connector (Primary J2)

COM HPC Connector (Primary J1)

Figure 2.2 Board Chips ID – Rear

2.2 Mechanical Diagrams

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

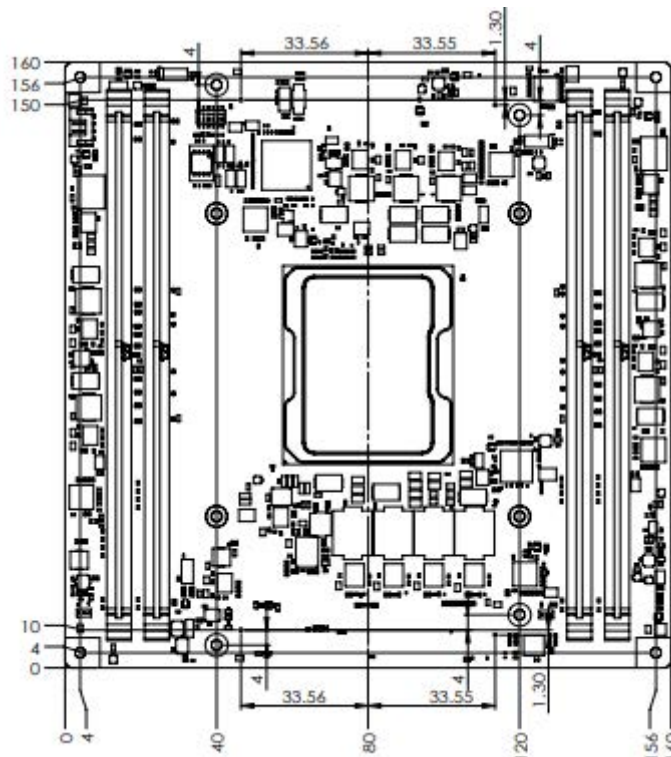


Figure 2.3 Board Mechanical Diagram – Front

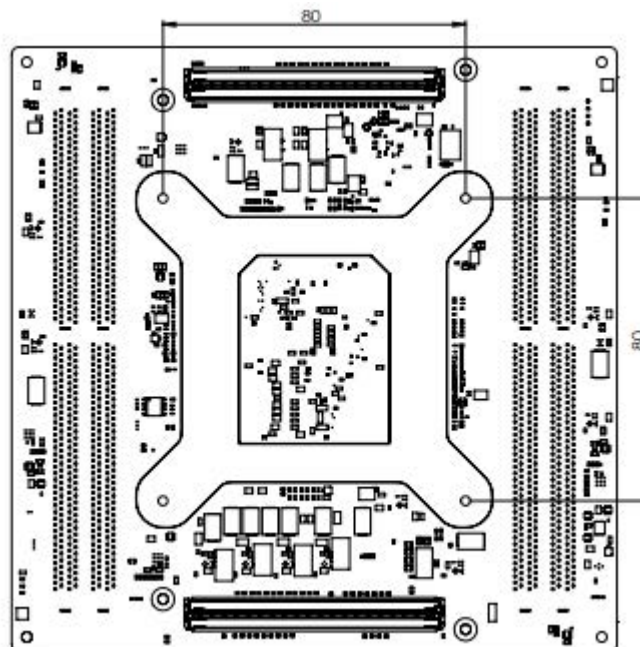


Figure 2.4 Board Mechanical Diagram – Rear

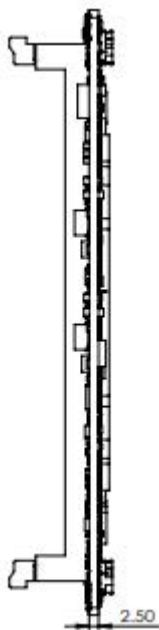


Figure 2.5 Board Mechanical Diagram – Side

2.3 Assembly Diagram

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

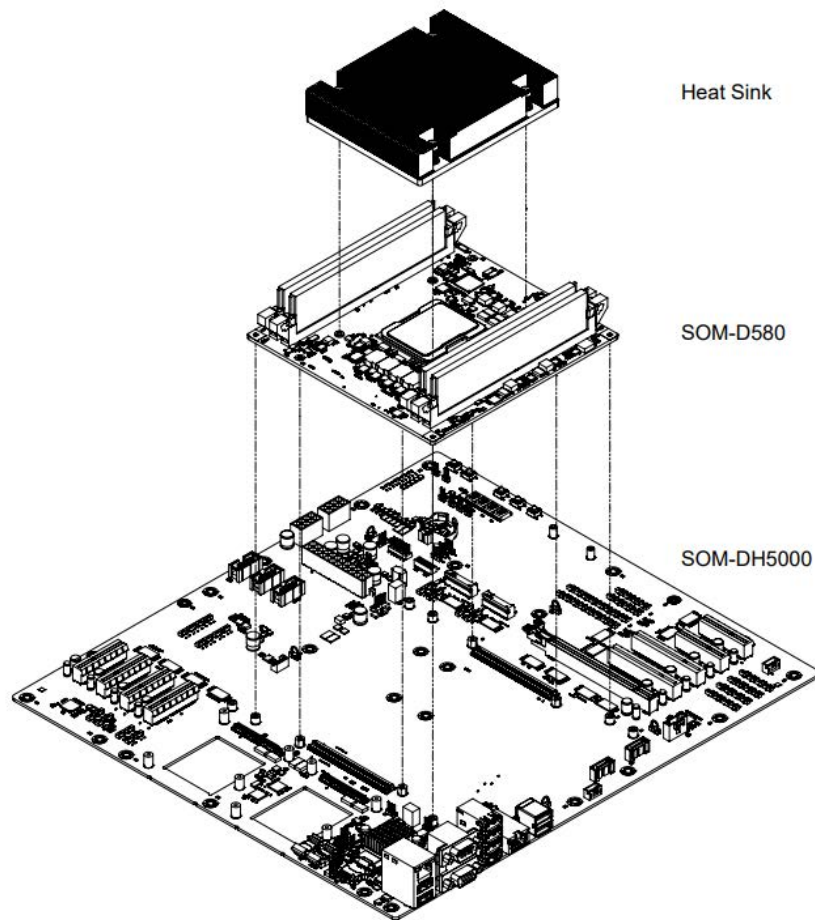


Figure 2.6 Assembly Drawing

There are 4 reserved screw holes for heat spreader pre-assembly on the SOM-2533.

2.4 Assembly Drawings

The board to board connector of the COM-HPC is a 400-pin connector, so please vertically assemble the module and carrier board and follow the allowable angle of the board to board connector as demonstrated in the following figures to avoid damaging the connector.

Mating Angle Requirements:

2.4.1 Allowable Initial Angular Misalignment

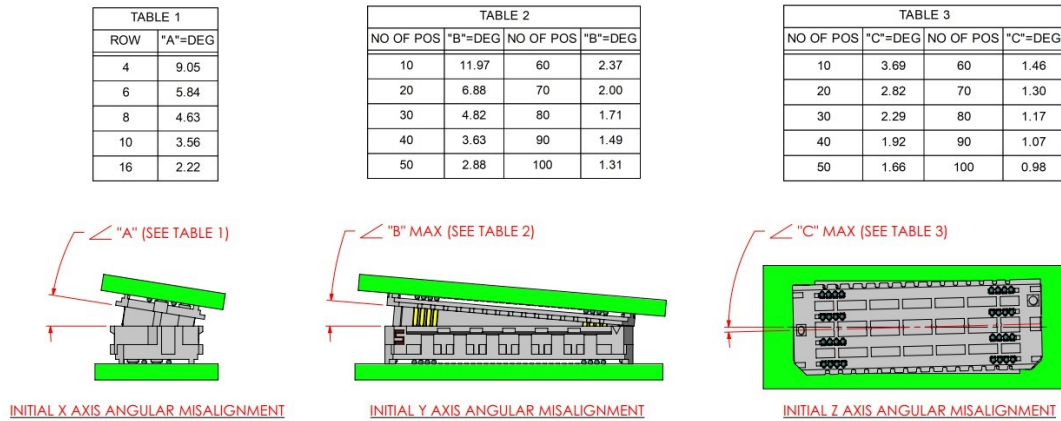


Figure 2.7 Initial Angular Misalignment

2.4.2 Allowable Final Angular Misalignment

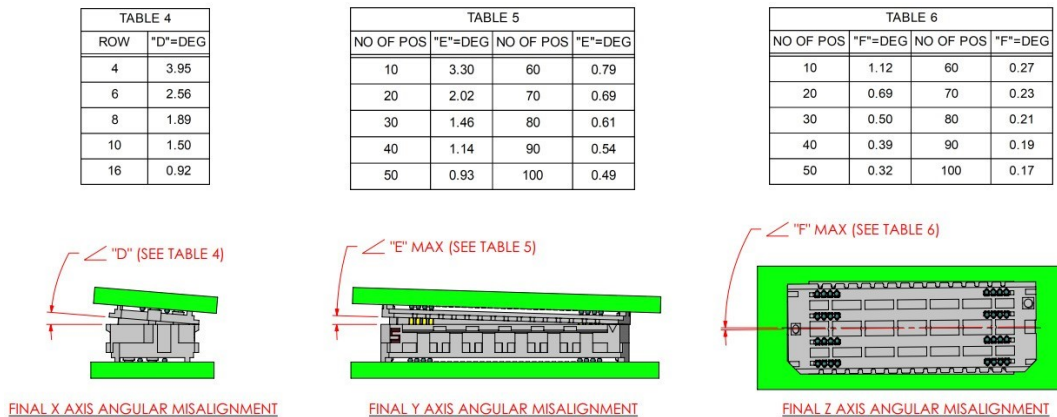


Figure 2.8 Final Angular Misalignment

2.5 CPU Package Design

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

Table 2.1: CPU Package Design

Item	PRE-SMT STACK-UP THICKNESS
IHS to MB Height (validated range)	4.217~4.517 mm

Figure 2.9 CPU and CPU Socket Height and Tolerance

Chapter 3

AMI BIOS

This chapter details BIOS setup information for the SOM-D580 CPU Computer-on-Module.

Sections include:

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

3.1 Introduction

AMI BIOS has been integrated into many motherboards for over a decade. 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 BIOS ROM has a built-in setup program that allows users to modify basic system configuration. This information is stored in flash ROM so it retains setup information when the power is turned off.

3.2 Entering Setup

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

3.2.1 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.

3.2.2 Advanced BIOS Features Setup

Select the Advanced tab from the SOM-D580 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.

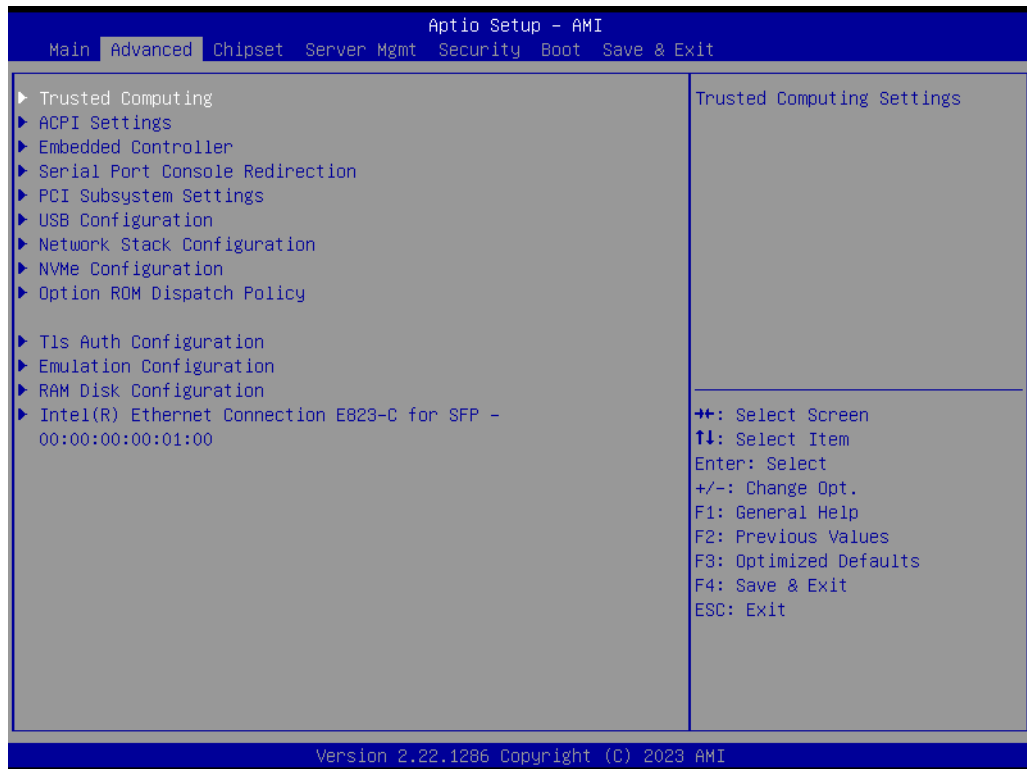


Figure 3.3 Advanced BIOS Features Setup Screen

- **Trusted Computing**
Trusted computing settings.
- **ACPI Settings**
System ACPI parameters.
- **Embedded Controller**
Embedded Controller parameters.
- **Serial Port Console Redirection**
Serial Port Console Redirection.
- **PCI Subsystem settings**
PCI, PCI-X, and PCI Express settings.
- **USB Configuration**
USB Configuration parameters.
- **Network Stack Configuration**
Network Stack settings.
- **NVMe Configuration**
NVMe Device Options settings.
- **Option ROM Dispatch Policy**
Option ROM Dispatch Policy.
- **Tls Auth Configuration**
Press <Enter> to select Tls Auth Configuration.

- **Emulation Configuration**
Displays and provides options to change the DFX Emulation settings.
- **RAM Disk Configuration**
Press <Enter> to add/remove RAM disks.
- **Intel® I210 Gigabit Network Connection - 00:A0:C9:00:00:00**
Configure Gigabit Ethernet device parameters.
- **Intel® Ethernet Controller (3) I225-IT - 74:FE:48:8A:44:57**
Configure Gigabit Ethernet device parameters.

3.2.2.1 Trusted Computing



Figure 3.4 Trusted Computing

- **Security Device Support**
Enables or Disables BIOS Support for a security device. The OS will not show the Security Device. TCG EFI protocol and the INT1A interface will not be available.
- **SHA256 PCR Bank**
Enable or Disable SHA256 PCR Bank.
- **SHA384 PCR Bank**
Enable or Disable SHA384 PCR Bank.
- **Pending operation**
Schedule an Operation for the Security Device. NOTE: Your Computer will reboot during restart in order to change state if a security device is found.
- **Platform Hierarchy**
Enable or Disable Platform Hierarchy.
- **Storage Hierarchy**
Enable or Disable Storage Hierarchy.
- **Endorsement Hierarchy**
Enable or Disable Endorsement Hierarchy.

- **Physical Presence Spec Version**
Select to tell the OS to support PPI Spec Version 1.2 or 1.3. Note: some HCK tests might not support 1.3.
- **Device Select**
TPM 1.2 will restrict support to TPM 1.2 devices. TPM 2.0 will restrict support to TPM 2.0 devices. Auto will support both with the default set to TPM 2.0 devices if not found. TPM 1.2 devices will be enumerated.

3.2.2.2 ACPI Settings

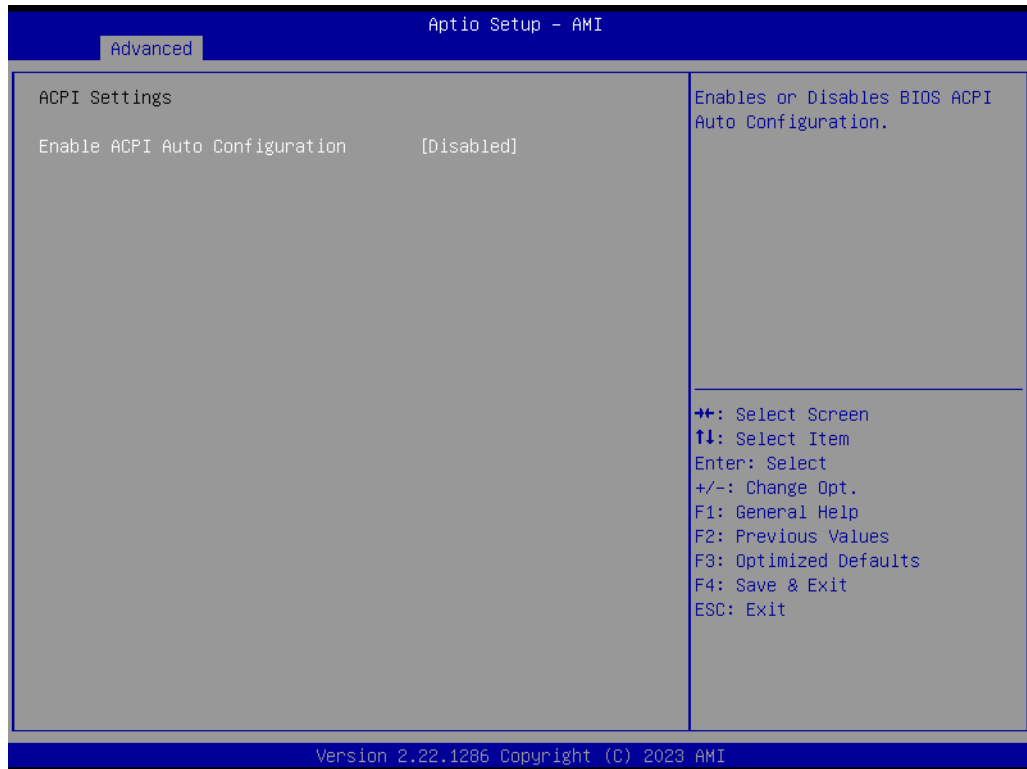


Figure 3.5 ACPI Settings

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

3.2.2.3 Embedded Controller

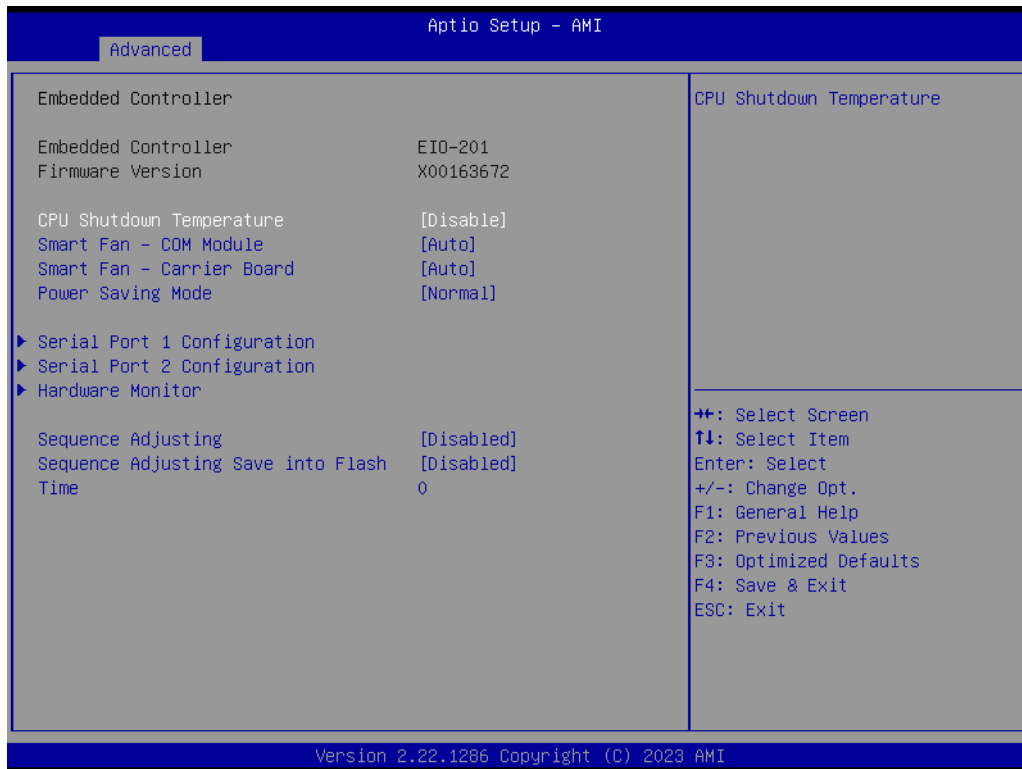


Figure 3.6 Embedded Controller

- **CPU Shutdown Temperature**
CPU Shutdown Temperature.
- **Smart Fan – COM Module**
Control the COM Module Smart FAN function.
Get the value from EC and only save the value when you Save Changes.
- **Smart Fan- Carrier Board**
Control the Carrier Board Smart FAN function.
Get the value from EC and only save the value when you Save Changes.
- **Power Saving Mode**
Select Power Saving Mode.
- **Serial Port 1 Configuration**
Set Parameters of Serial Port 1 (COMA).
- **Serial Port 2 Configuration**
Set Parameters of Serial Port 2 (COMB).
- **Hardware Monitor**
Monitor hardware status.
- **Sequence Adjusting**
Delay the startup time.
- **Sequence Adjusting Save into Flash**
Save the Sequence Adjusting setting into Flash.
- **Time**
Timing for the delay can be adjusted within the range of 0 to 10000ms.

3.2.2.4 Serial Port 1 Configuration

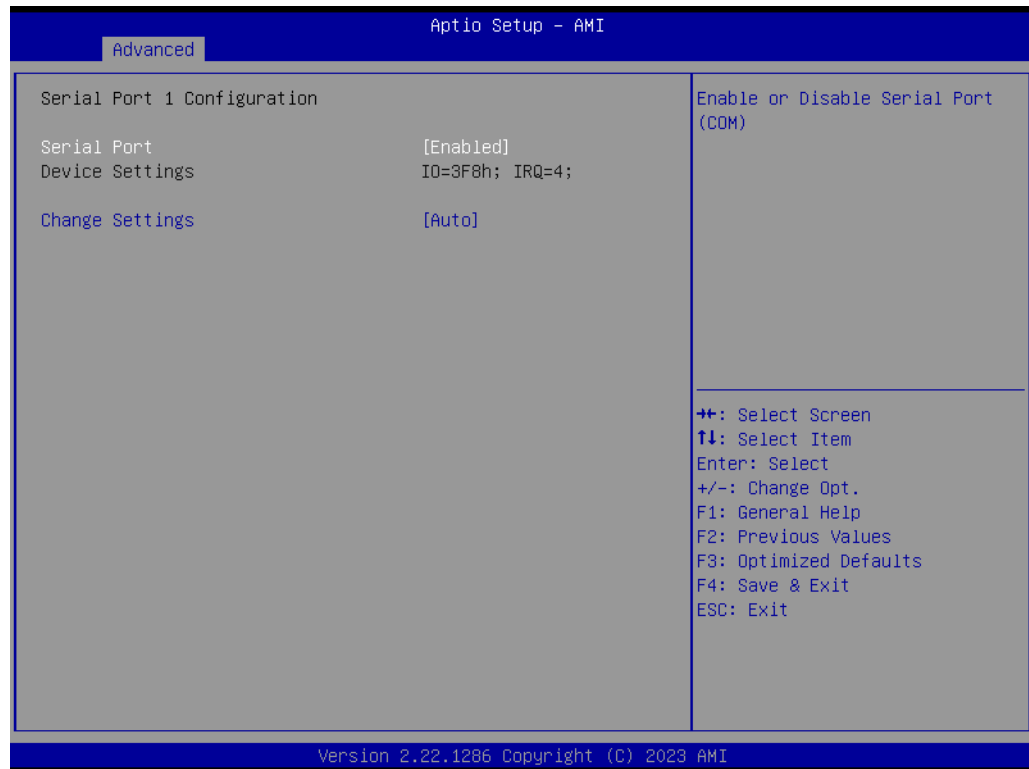


Figure 3.7 Serial Port 1 Configuration

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

3.2.2.5 Serial Port 2 Configuration

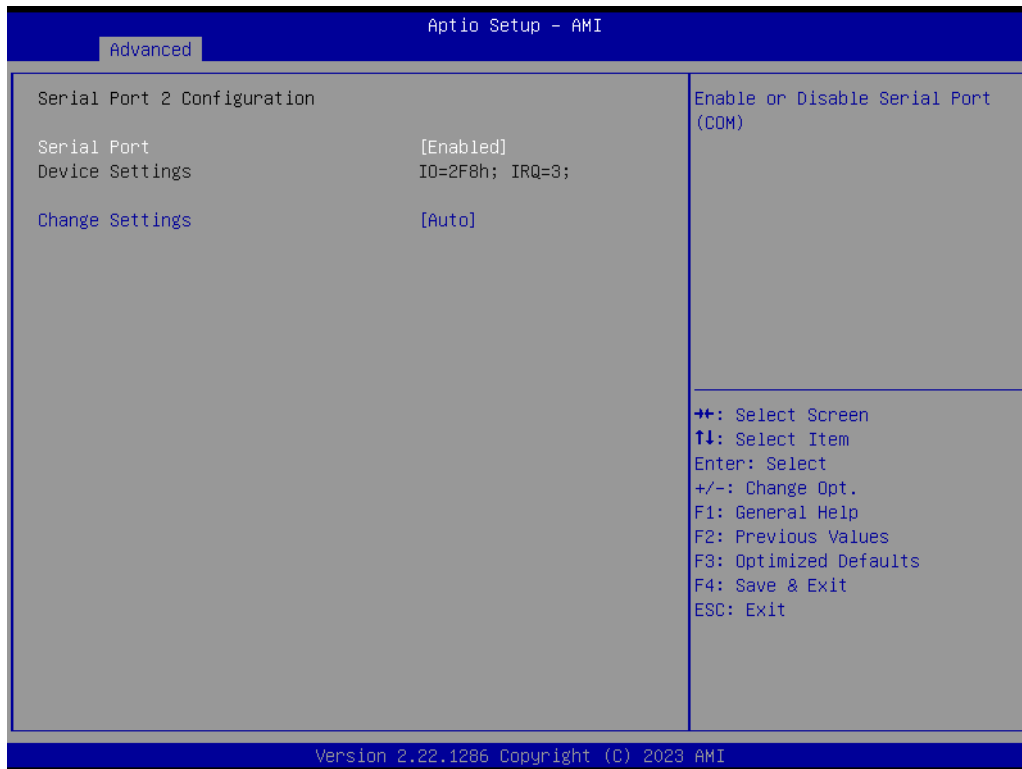


Figure 3.8 Serial Port 2 Configuration

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

3.2.2.6 Hardware Monitor

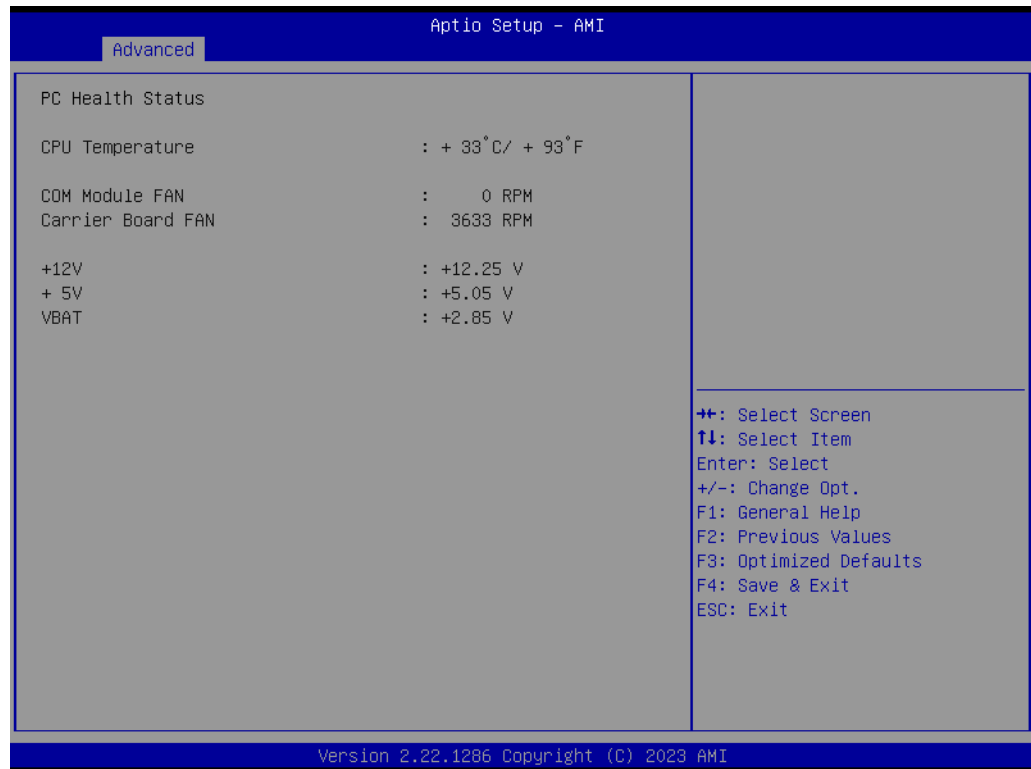


Figure 3.9 Hardware Monitor

Monitor hardware status.

3.2.2.7 Serial Port Console Redirection

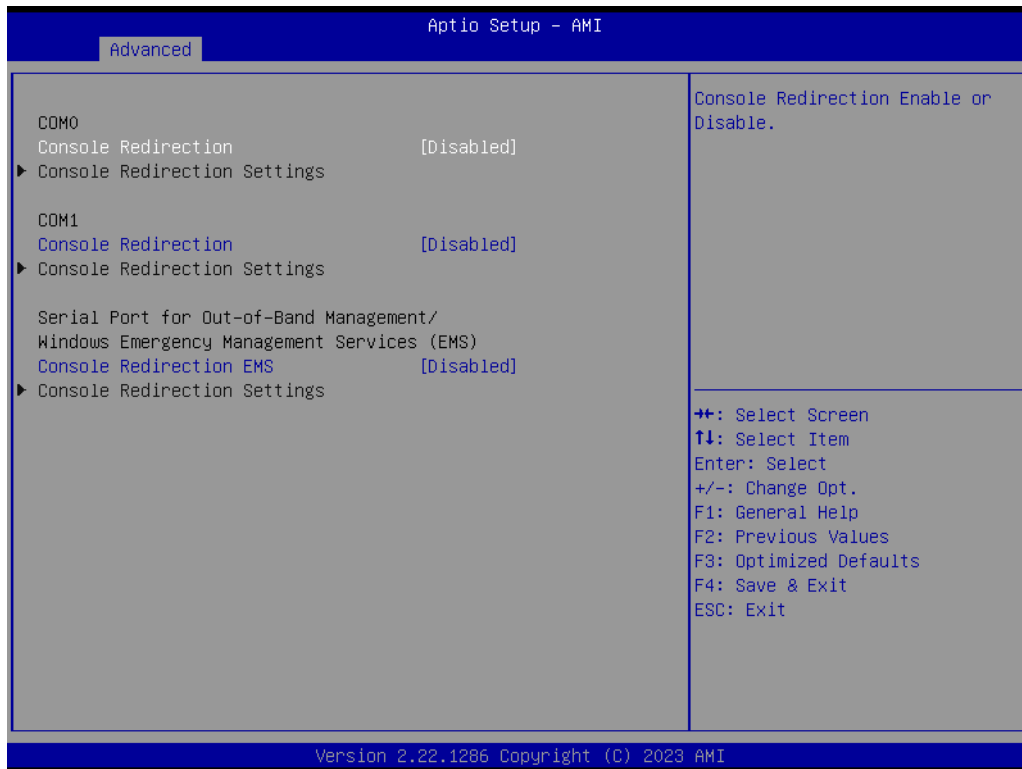


Figure 3.10 Serial Port Console Redirection

COM0

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

COM1

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

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

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

3.2.2.8 Console Redirection Settings (COM0)

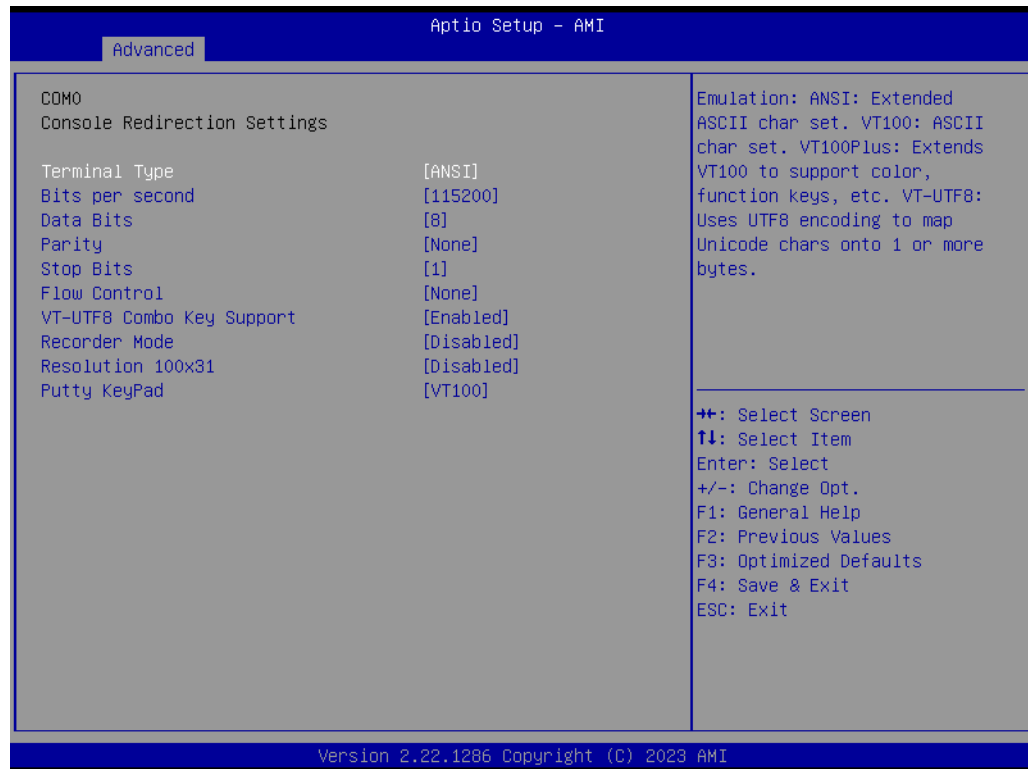


Figure 3.11 Console Redirection Settings

- **Terminal Type**
Emulation: ANSI: Extended ASCII char set.
VT100: ASCII char set.
VT100Plus: Extends VT100 to support color, function keys, etc.
VT-UTF8: Uses UTF8 encoding to map Unicode characters onto 1 or more bytes.
- **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 transmission errors. Even: Parity bit is 0 if the num of 1s in the data bit is even.
Odd: parity bit is 0 if num of 1s in the data bits is odd.
Mark: parity bit is always 1.
Space: Parity bit is always 0.
Mark and Space Parity do not allow for error detection.
They can be used as an additional data bit.
- **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. Communication with slow devices may require more than 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.

Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

- **VT-UTF8 Combo Key Support**
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 100x31**
Enables or disables extended terminal resolution.
- **Putty KeyPad**
Select FunctionKey and KeyPad on Putty.

3.2.2.9 PCI Subsystem Settings

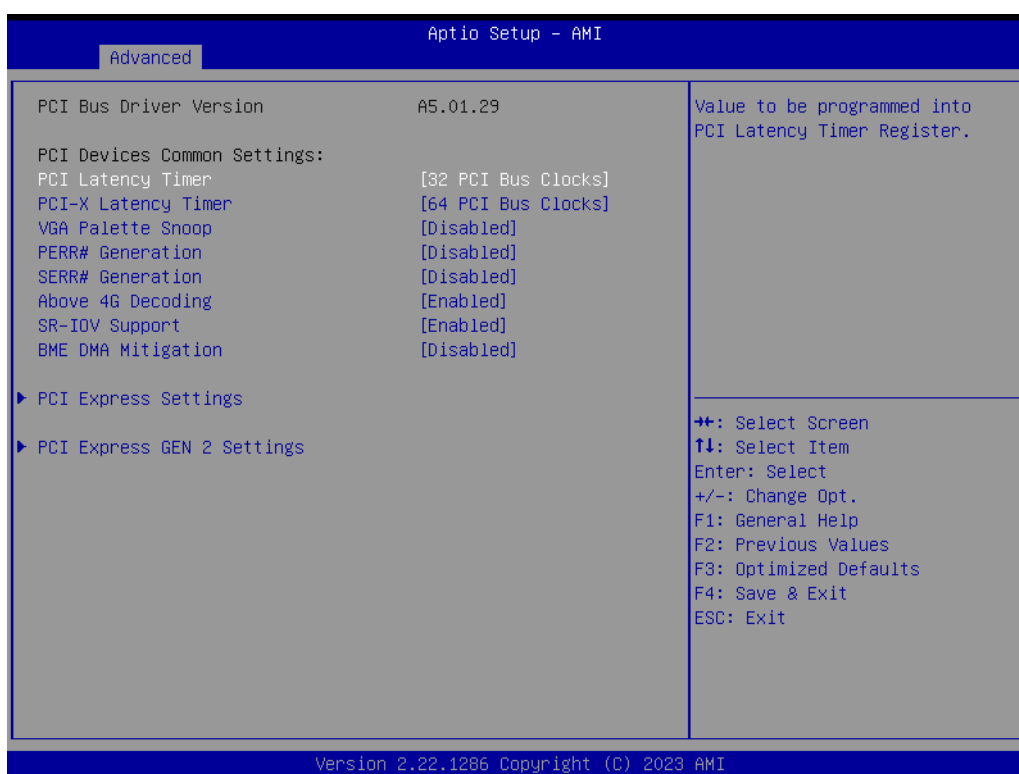


Figure 3.12 PCI Subsystem Settings

- **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**
Enables or Disables VGA Palette Register Snooping.
- **PERR# Generation**
Enables or Disables a PCI Device to Generate PERR#.
- **SERR# Generation**
Enables or Disables a PCI Device to Generate SERR#.
- **Above 4G Decoding**
Enables or Disables 64-bit capable devices to be decoded in 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 from disable during PCI enumeration for PCI Bridges after SMM is locked.
- **PCI Express Settings**
Change PCI Express Device Settings.
- **PCI Express Gen 2 Settings**
Change PCI Express Gen Device Settings.

3.2.2.10 PCI Express Settings

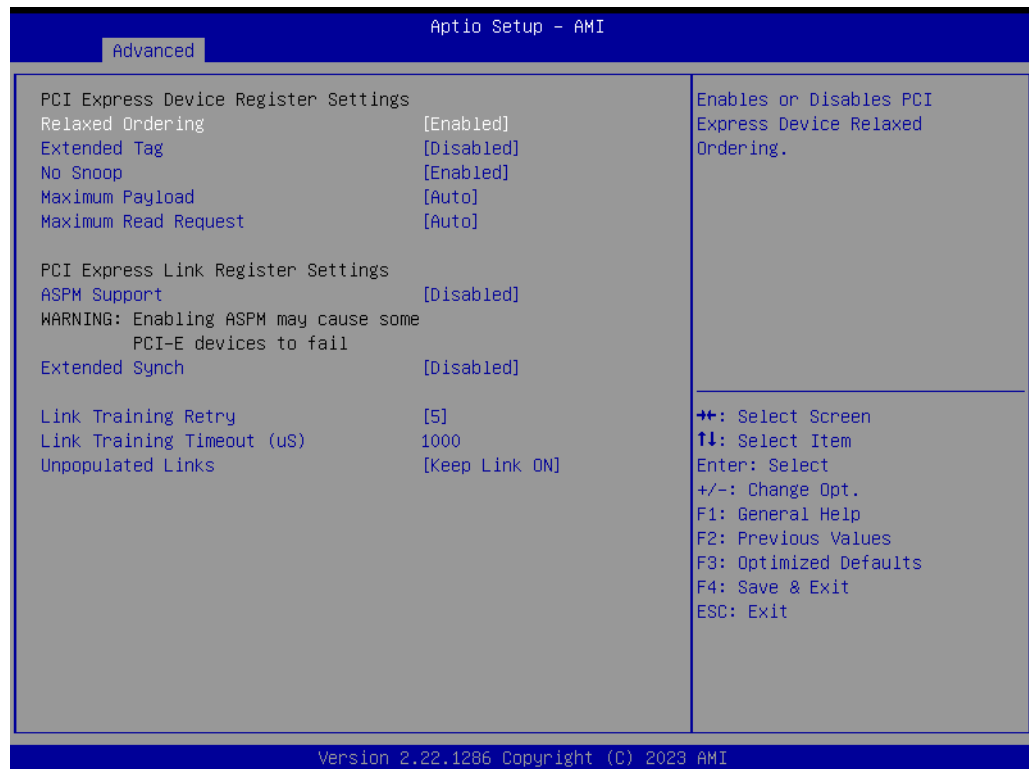


Figure 3.13 PCI Express Settings

- **Relaxed Ordering**
Enables or Disables PCI Express Device Relaxed Ordering.
- **Extended Tag**
If Enabled, it allows a 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 the Maximum Payload of a PCI Express Device or allow System BIOS to select the value.
- **Maximum Read Request**
Set Maximum Read Request Size of a 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- Disable ASPM.
- **Extended Synch**
If Enabled, it allows generation of Extended Synchronization patterns.

- **Link Training Retry**
Defines the number of Retry Attempts software will take to retrain the link if a previous training attempt was unsuccessful.
- **Link Training Timeout (uS)**
Defines the number of Microseconds software will wait before polling 'Link Training' bit in Link Status register.
Value range from 10 to 10000 μ s.
- **Unpopulated Links**
In order to save power, software will disable unpopulated PCI Express links if the option set to 'Disable Link'.

3.2.2.11 PCI Express GEN 2 Settings

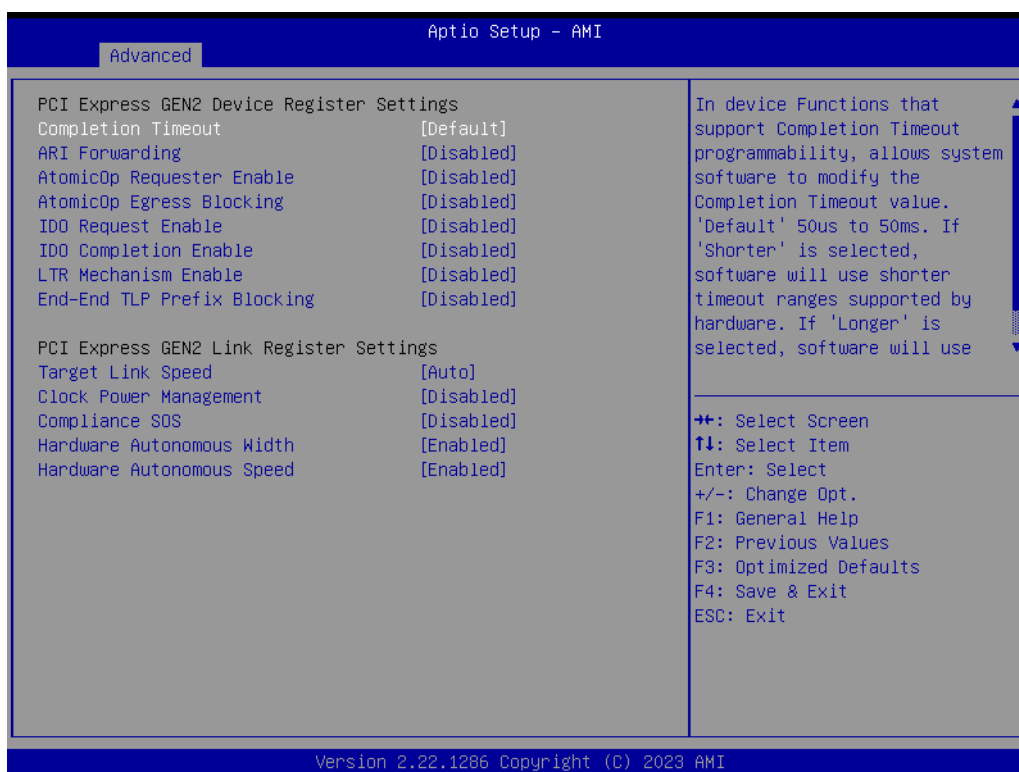


Figure 3.14 PCI Express GEN2 Settings

- **Completion Timeout**
In device Functions that support completion time out programmability, this allows system software to modify the completion time out value.
The Default is 50 μ s to 50ms. If 'Shorter' is selected, the software will use shorter timeout ranges supported by hardware.
If 'Longer' is selected, the 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 to be 0 enforcement when turning a Type1 Configuration Request into a Type 0 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.

-
- **Atomic0p Egress Blocking**
If supported by hardware and set to 'Enabled', outbound Atomic0p Requests via Egress Ports will be blocked.
 - **ID0 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.
 - **ID0 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 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.

3.2.2.12 USB Configuration

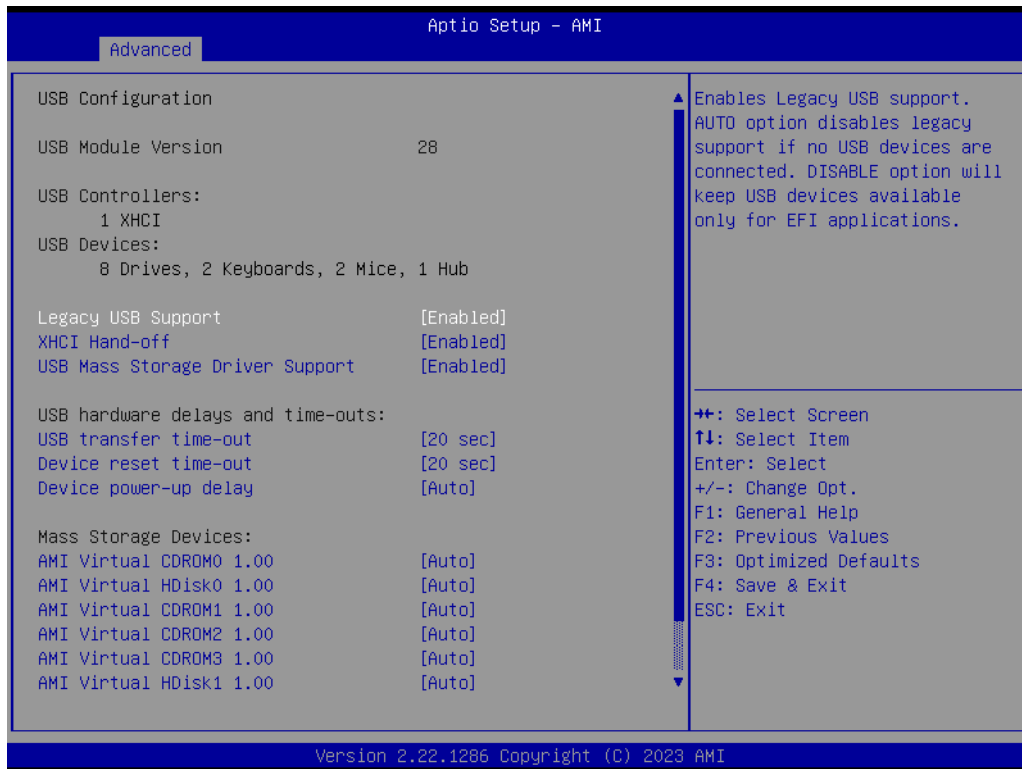


Figure 3.15 USB Configuration

- **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 OSes without XHCI hand-off support. The XHCI ownership change should be claimed by the XHCI driver.
- **USB Mass Storage Driver Support**
 Enable/Disable USB Mass Storage Driver Support.
- **USB transfer time-out**
 The time-out value for control, bulk, and interrupt transfers.
- **Device reset time-out**
 USB mass storage device start unit command time-out.
- **Device power-up delay**
 Maximum time the device will take before it properly reports itself to the Host Controller.
 'Auto' uses the default value: for a Root port it is 100ms, for a hub port the delay is taken from the Hub descriptor.
- **AMI Virtual CDROM0 1.00**
 Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM', drives with no media emulated according to drive type.
- **AMI Virtual HDisk0 1.00**
 Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM' drives with no media emulated according to drive type.

- **AMI Virtual CDROM1 1.00**
Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM' drives with no media emulated according to drive type.
- **AMI Virtual CDROM2 1.00**
Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM' drives with no media emulated according to drive type.
- **AMI Virtual CDROM3 1.00**
Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM' drives with no media emulated according to drive type.
- **AMI Virtual HDisk1 1.00**
Mass storage device emulation type. 'AUTO' enumerates devices according to their media format. Optical drives are emulated as 'CDROM' drives with no media emulated according to drive type.

3.2.2.13 Network Stack Configuration



Figure 3.16 PCI Network Stack Configuration

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

3.2.2.14 NVMe Configuration

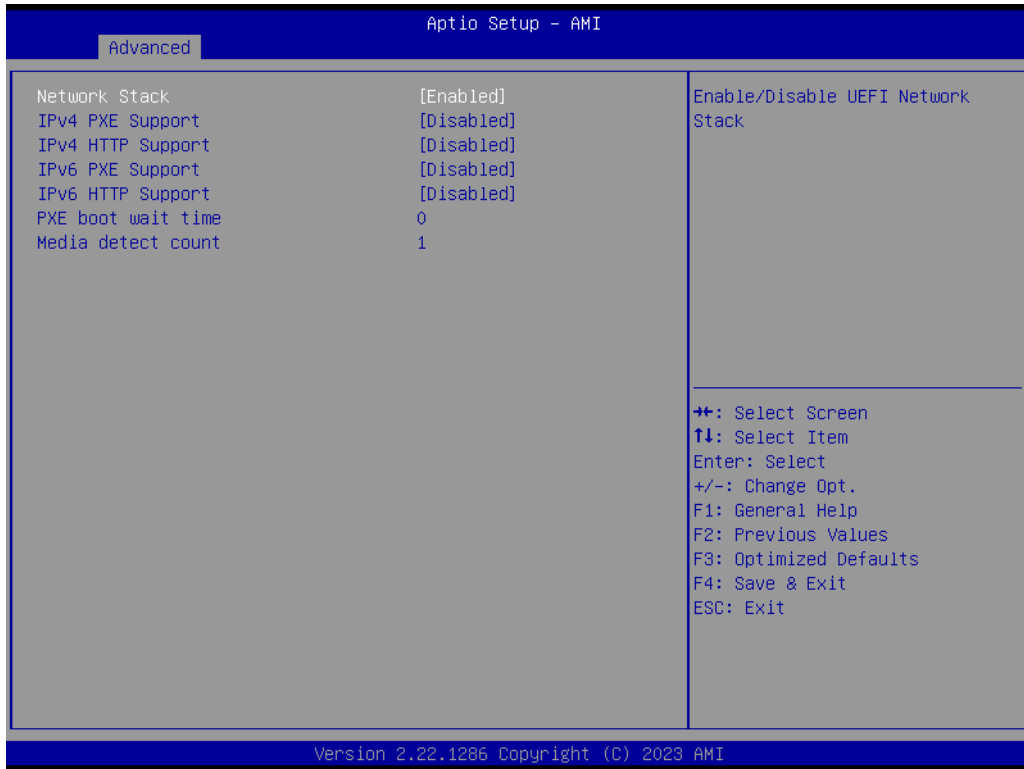


Figure 3.17 NVMe Configuration

- **Network Stack**
Enable/Disable UEFI Network Stack.
- **IPv4 PXE Support**
- **IPv4 HTTP Support**
- **IPv6 PXE Support**
- **IPv6 HTTP Support**
- **PXE boot wait time**
- **Media detect count**

3.2.2.15 Option ROM Dispatch Policy

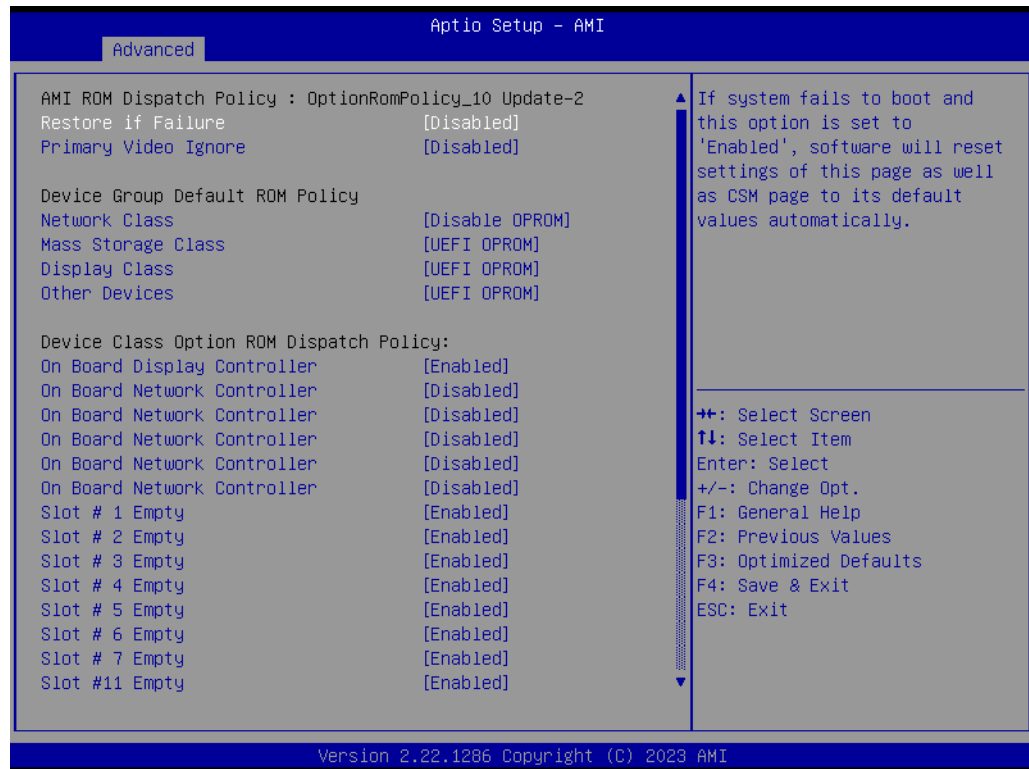


Figure 3.18 Option ROM Dispatch Policy

- **Restore if Failure**
If the system fails to boot and this option is set to 'Enabled', the software will reset the settings of this page as well as the CSM page to default values automatically.
- **Primary Video Ignore**
If software detects that due to the Policy settings, Option ROM of the Primary Video Device will not dispatch, it will ignore the device policy settings and restore it to 'Enable' automatically.
- **Network Class**
Controls the execution of UEFI and Legacy Network OpROM.
- **Mass Storage Class**
Controls the execution of UEFI and Legacy Storage OpROM.
- **Display Class**
Controls the execution of UEFI and Legacy Video OpROM.
- **Other Devices**
Determines OpROM execution policy for devices other than Network, Storage, or Video.
- **On Board Display Controller**
Onboard Device has:
UEFI [X]
Legacy [X]
Embedded ROM(s).
VIDx1A03; DIDx2000; Class:3/0/0
@Sx0|Bx3|Dx0|Fx0
t:2Sx0|Bx2|Dx0|Fx0
t:2Sx0|Bx0|Dx14|Fx0
t: 1Sx0|Bx3|Dx0|Fx0

- As1Name:ASVD
SMBIOS:AST2500 BMC
- **On Board Network Controller**
Onboard Device has:
UEFI [X]
Legacy [X]
Embedded ROM(s).
VIDx1A03; DIDx1533;Class:2/0/0
@Sx0|Bx1|Dx0|Fx0
t:2Sx0|Bx0|Dx13|Fx0
t: 1Sx0|Bx0|Dx0|Fx0
As1Name:I210
SMBIOS:I210 PCIE 14
 - **On Board Network Controller**
Onboard Device has:
UEFI [X]
Legacy [X]
Embedded ROM(s).
VIDx1A03; DIDx0D9F;Class:2/0/0
@Sx0|Bx4|Dx0|Fx0
t:2Sx0|Bx0|Dx15|Fx0
t: 1Sx0|Bx0|Dx0|Fx0
As1Name:I225
SMBIOS:I225 HSIO 18
 - **On Board Network Controller**
Onboard Device has:
UEFI [X]
Legacy [X]
Embedded ROM(s).
VIDx1A03; DIDx188D;Class:2/0/0
@Sx0|Bx89|Dx0|Fx1
t:2Sx0|Bx88|Dx4|Fx0
t: 1Sx0|Bx88|Dx0|Fx0
As1Name:CPK1
SMBIOS: Intel CPK1
 - **On Board Network Controller**
Onboard Device has:
UEFI [X]
Legacy [X]
Embedded ROM(s).
VIDx1A03; DIDx188D;Class:2/0/0
@Sx0|Bx89|Dx0|Fx2
t:2Sx0|Bx88|Dx4|Fx0
t: 1Sx0|Bx88|Dx0|Fx0
As1Name:CPK2
SMBIOS: Intel CPK2
 - **On Board Network Controller**
Onboard Device has:
UEFI [X]
Legacy [X]
Embedded ROM(s).
VIDx1A03; DIDx188D;Class:2/0/0
@Sx0|Bx89|Dx0|Fx3
t:2Sx0|Bx88|Dx4|Fx0
t: 1Sx0|Bx88|Dx0|Fx0

As1Name:CPK3
SMBIOS: Intel CPK3

- **Slot # 1 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 2 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 3 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 4 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 5 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 6 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 7 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 11 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 12 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 13 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 21 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 31 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 41 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 51 Empty**
Enable or Disable option ROM execution for selected slot.
- **Slot # 61 Empty**
Enable or Disable option ROM execution for selected slot.

3.2.2.16 Tls Auth Configuration

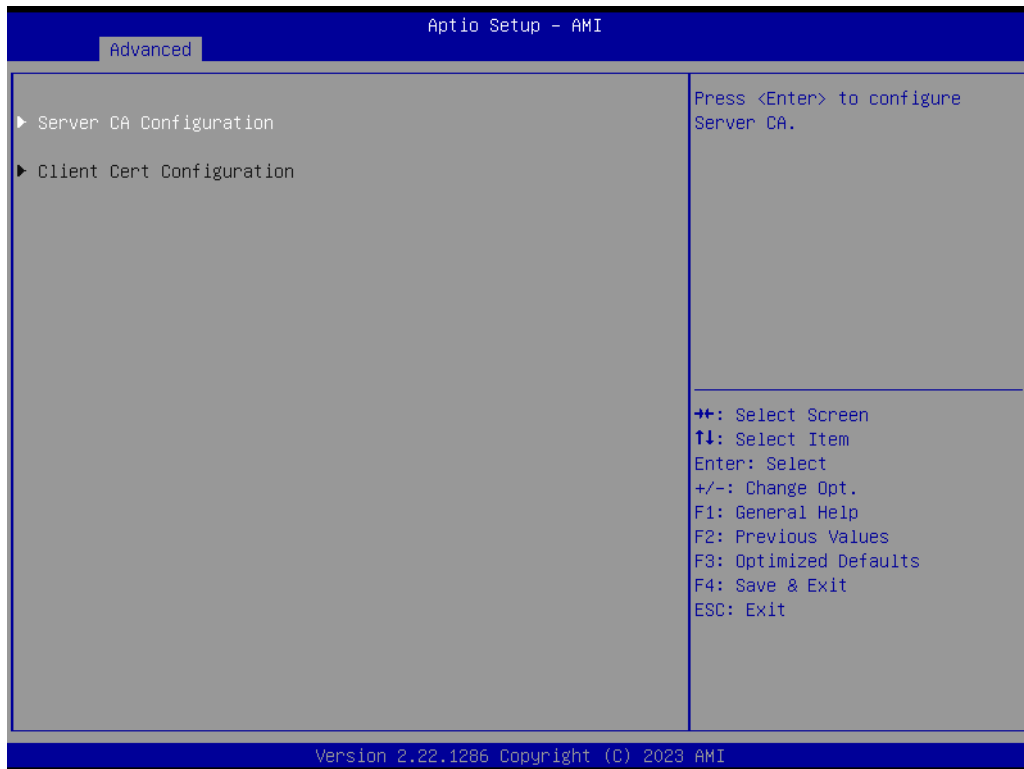


Figure 3.19 Tls Auth Configuration

- **Server CA Configuration**
Press <Enter> to configure Server CA.
- **Client Cert Configuration**
Press <Enter> to configure Client Cert.

3.2.2.17 Enroll Cert

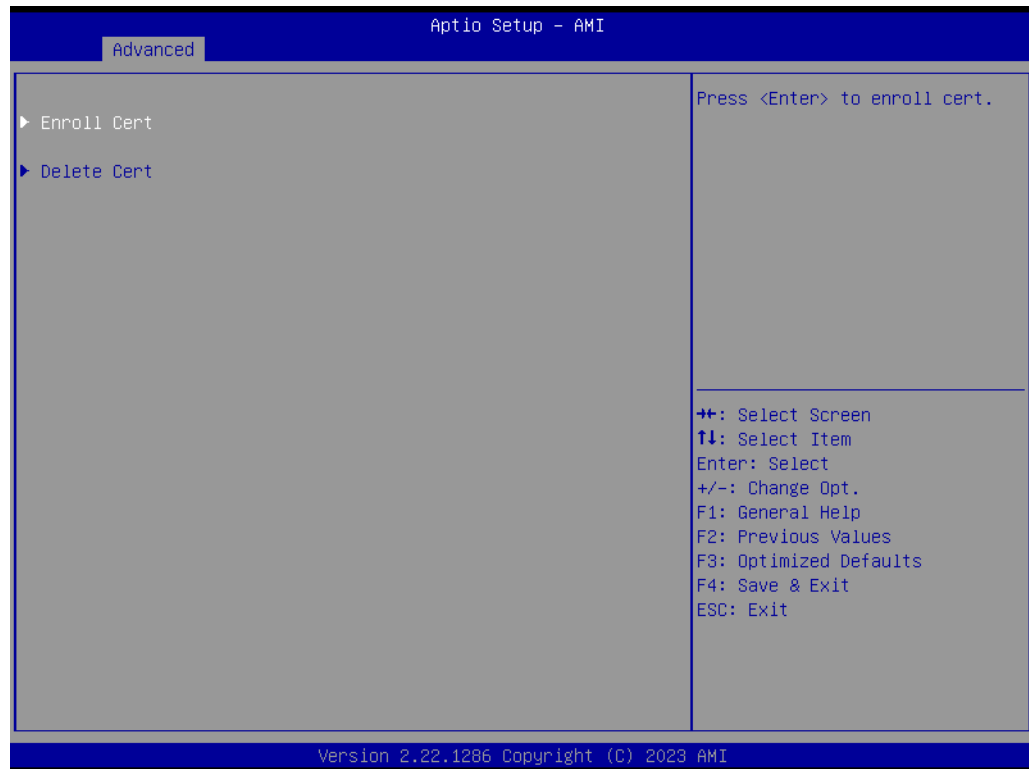


Figure 3.20 Enroll Cert

- **Enroll Cert**
Press <Enter> to enroll cert.
- **Delete Cert**
Press <Enter> to delete cert.

3.2.2.18 Enroll Cert Using File



Figure 3.21 Enroll Cert Using File

- **Enroll Cert Using File**
Enroll Cert Using File.
- **Cert GUID**
Input digit characters in 11111111-2222-3333-4444-1234567890ab format.
- **Commit Changes and Exit**
Commit Changes and Exit.
- **Discard Changes and Exit**
Discard Changes and Exit.

3.2.2.19 Emulation Configuration

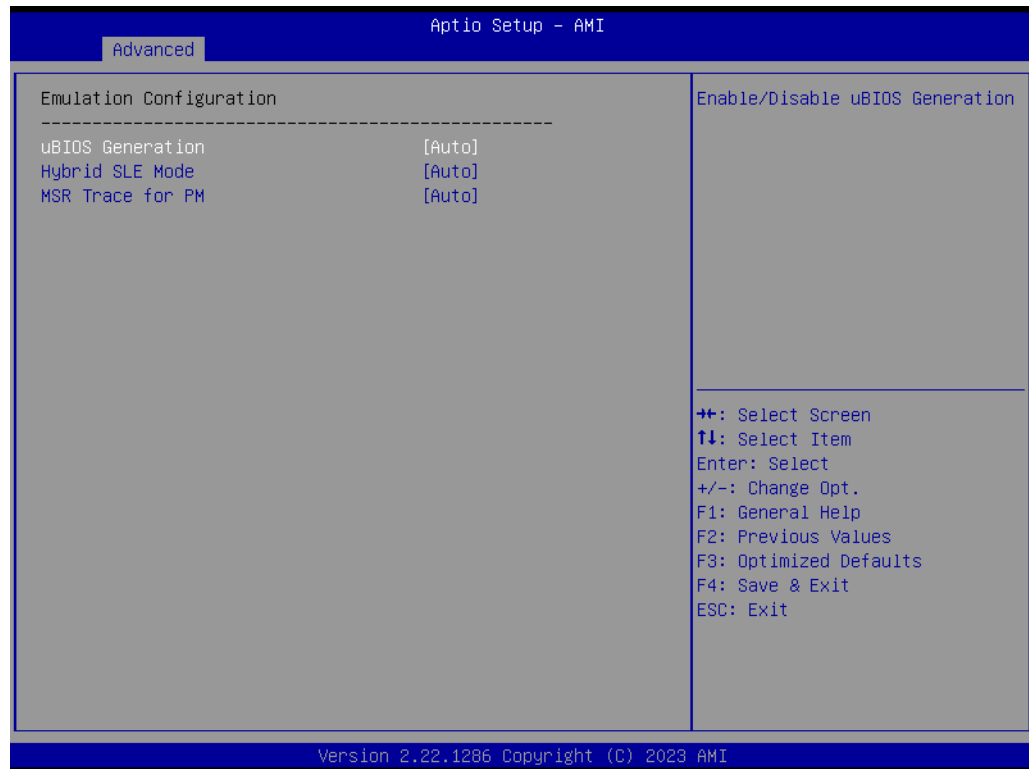


Figure 3.22 Emulation Configuration

- **uBIOS Generation**
Enable/Disable uBIOS Generation.
- **Hybrid SLE Mode**
Enable/Disable Hybrid Level Emulation Mode.
- **MSR Trace for PM**
Enable/Disable MSR Trace for Power management in uBIOS.

3.2.2.20 Intel® Ethernet Connection

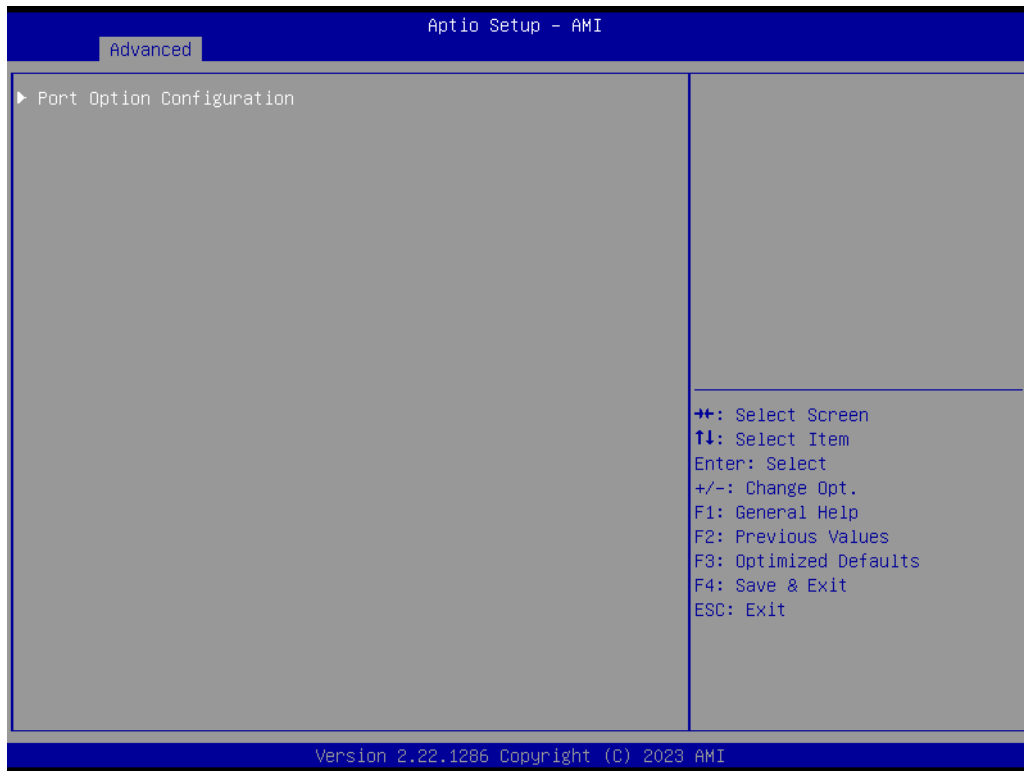


Figure 3.23 Port Option Configuration

■ Port Option Configuration

3.2.2.21 Port Options



Figure 3.24 Port Options

- **Port Option**
Configure the port option of the device. The Option string is defined as follows:
- **Option 0: 4x25G**
- **Option 1: 2x4x10G**
- **Option 2: 4x10G**
- **Option 3: -4 x1G**
- **Option 4: 2x25G**
- **Option 5: -4x10G**
- **Option 6: 1x100G**

3.2.2.22 Chipset



Figure 3.25 Chipset

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

3.2.2.23 Socket Configuration

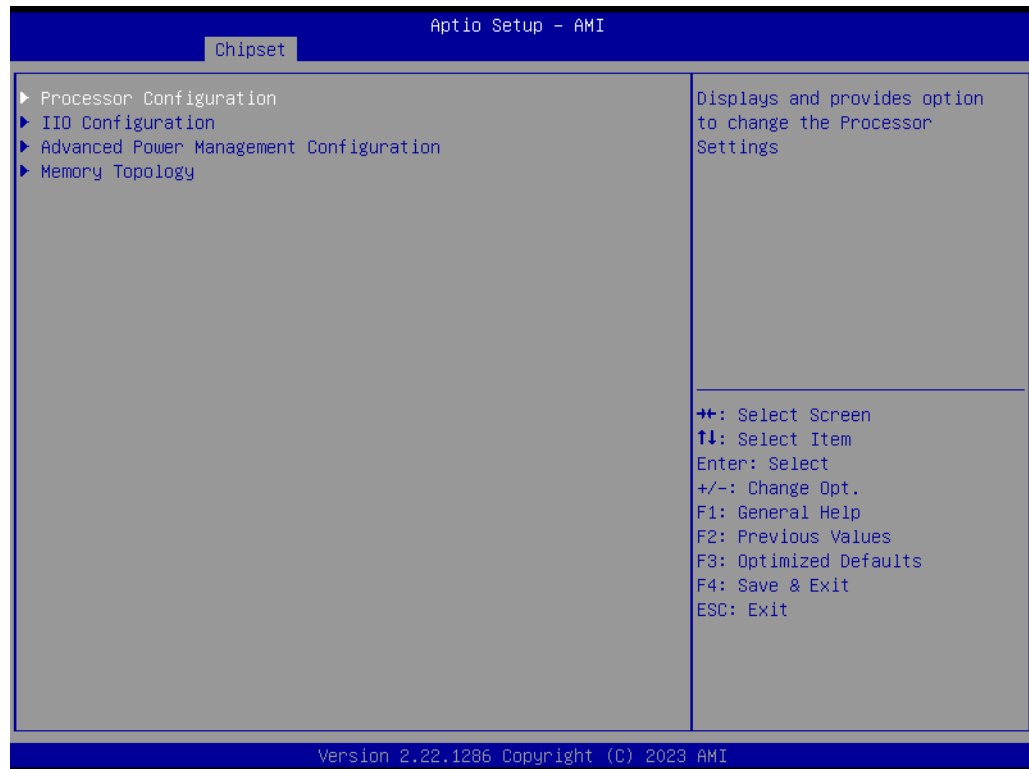


Figure 3.26 Socket Configuration

- **Process Configuration**
Displays and provides the option to change processor settings.
- **IIO Configuration**
Displays and provides the option to change IIO Settings.
- **Advanced Power Management Configuration**
Displays and provides the option to change Power Management Settings.
- **Memory Topology**
Displays memory topology with Dimm population information.

3.2.2.24 Processor Configuration

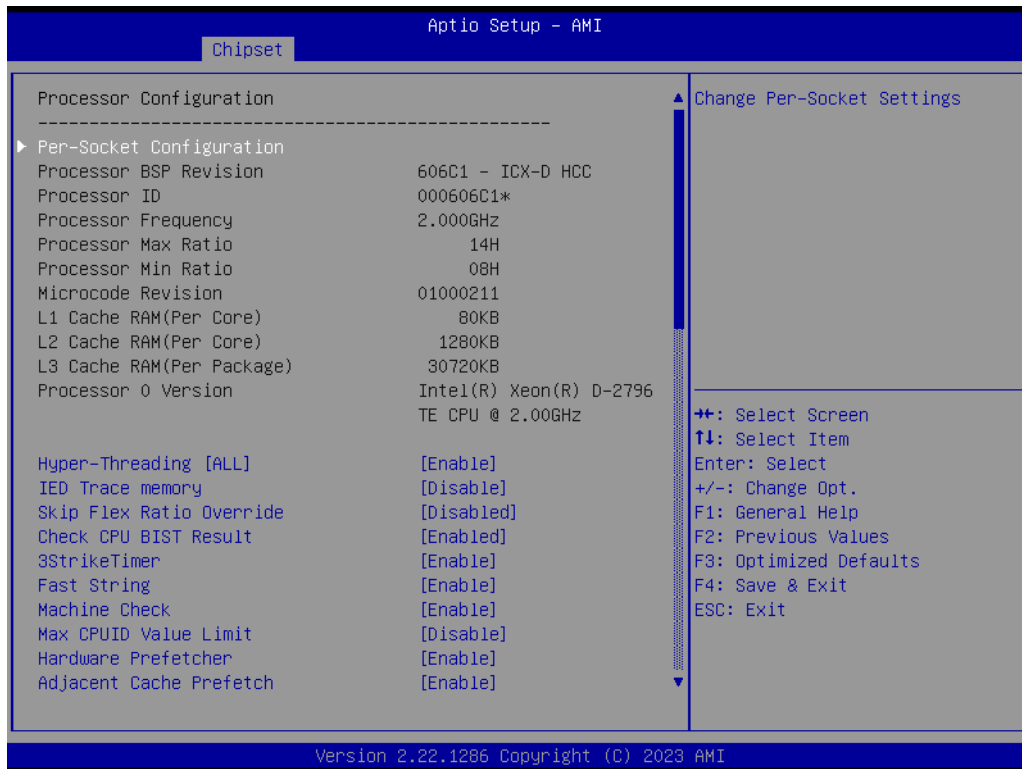


Figure 3.27 Processor Configuration

- **Per-Socket Configuration**
Change Per-Socket settings.
- **Hyper-Threading [ALL]**
Enables Hyper-Threading (Software Method to Enable/Disable Logical Processor threads).
- **IED Trace memory**
Option 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.
- **3StrikeTimer**
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, it enables 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]).

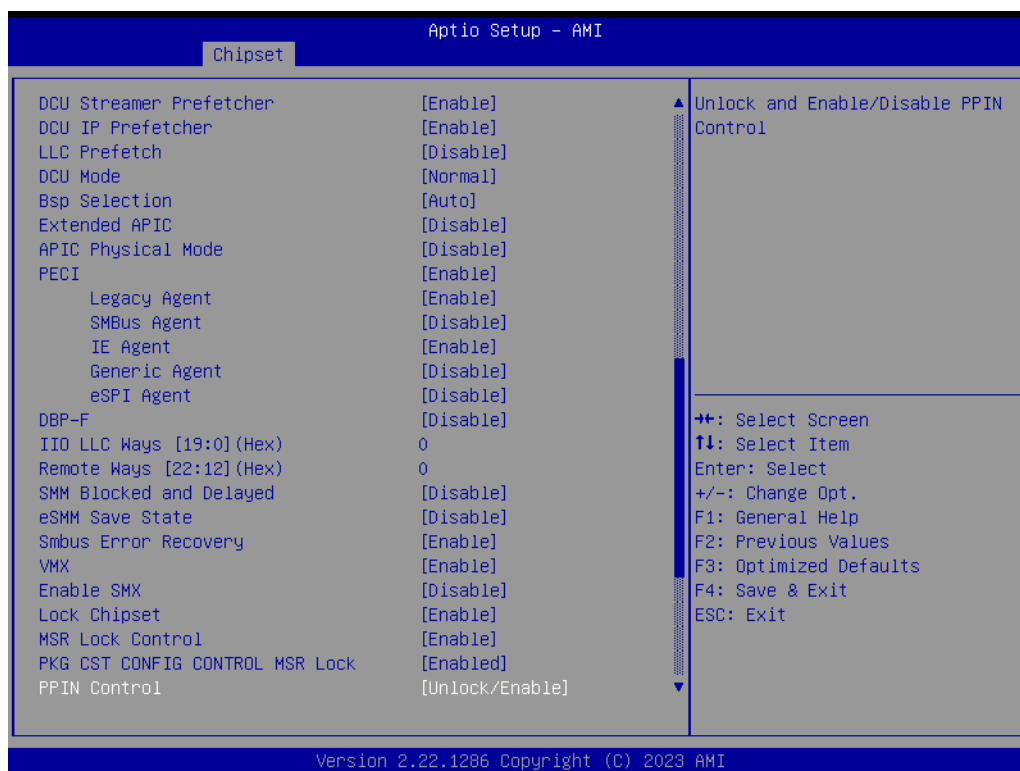


Figure 3.28 Chipset

- **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 Prefetch**
Enable/Disable LLC Prefetcher 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 PECl 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 LCC Ways [19:0](Hex)**
MSR CBO_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; takes effect after reboot.
- **Enable SMX**
Enables Safer Mode Extensions.
- **Lock Chipset**
Lock or Unlock 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.

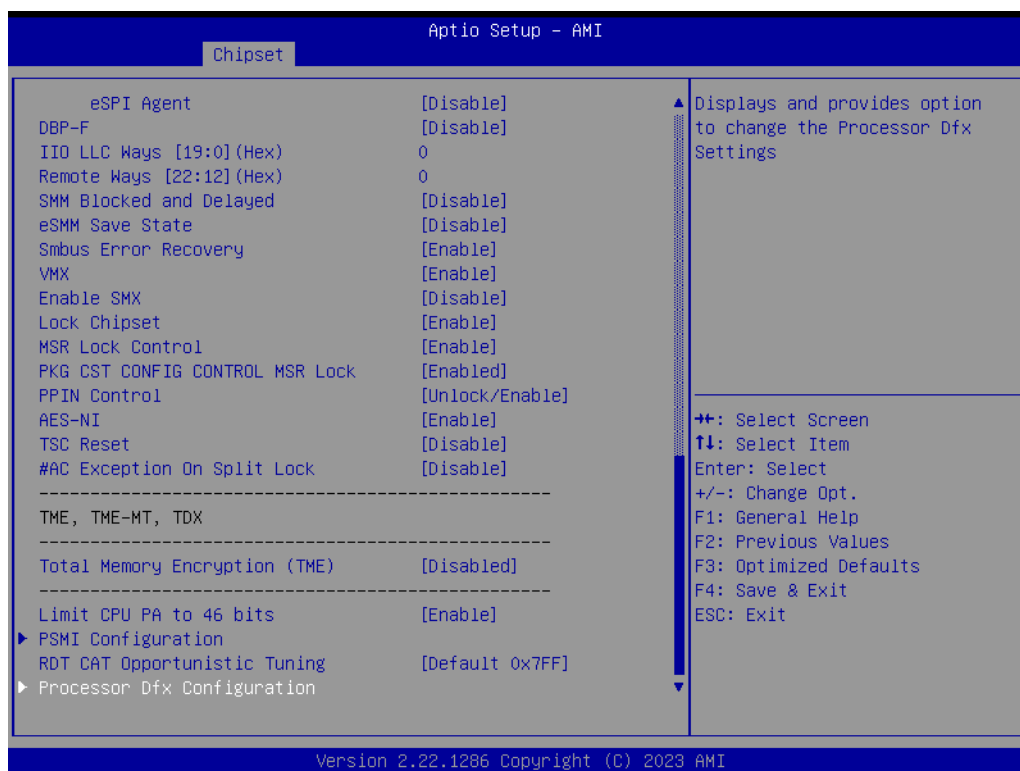


Figure 3.29 Chipset

- **AES-NI**
Enable/Disable AES-NI support.
- **TSC Reset**
Enable/Disable TSC reset during warm reboot.
- **#AC Exception On Split Lock**
Enable/Disable #AC (Alignment Check) Exception On Split Lock.
- **Total Memory Encryption (TME)**
Enable/Disable Total Memory Encryption (TME).
- **Limit CUP PA to 46 bits**
Limit CPU physical address to 46 bits to support older Hyper-V. If enabled, it automatically disables TME-MT.
- **PSMI Configuration**
PSMI Configuration.
- **Processor Dfx Configuration**
Displays and provides the option to change Processor Dfx Settings.

3.2.2.25 Pre-Socket Configuration

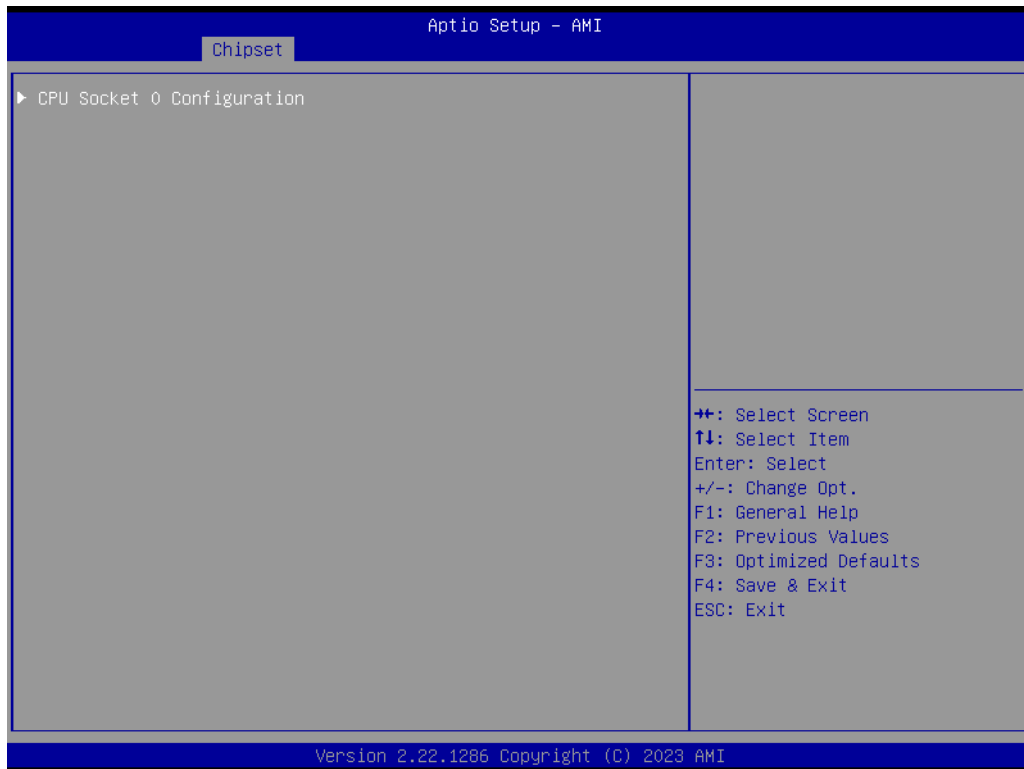


Figure 3.30 CPU Socket 0 Configuration

- CPU Socket 0 Configuration

3.2.2.26 CPU Socket 0 Configuration

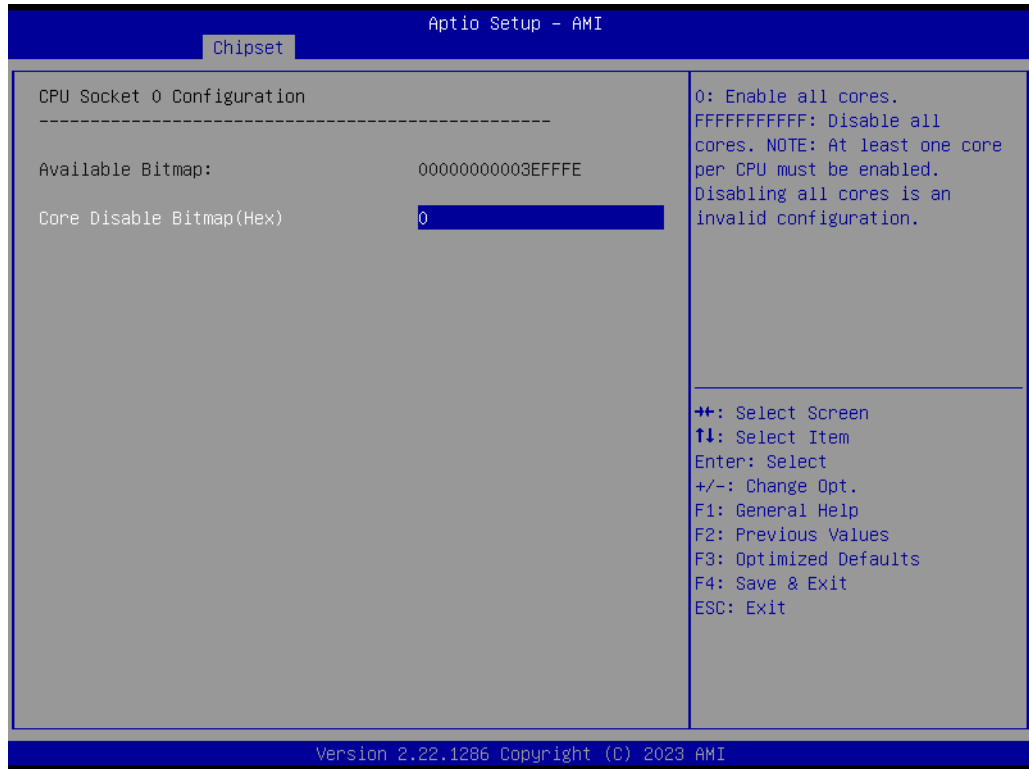


Figure 3.31 CPU Socket 0 Configuration

- **Core Disable Bitmap (Hex)**
0: Enable all cores.
FFFFFFFF: Disable all cores.
Note: At least one core per CPU must be enabled.
Disabling all cores is an invalid configuration.

3.2.2.27 PSMI Configuration

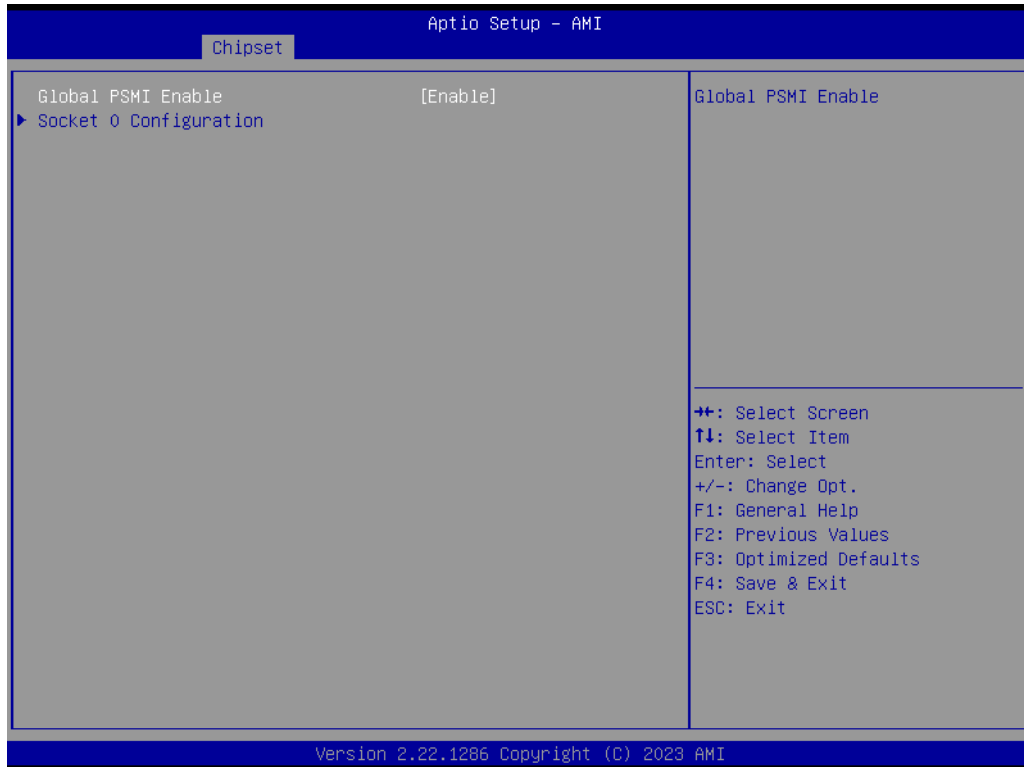


Figure 3.32 Global PSMI

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

3.2.2.28 Socket 0 Configuration

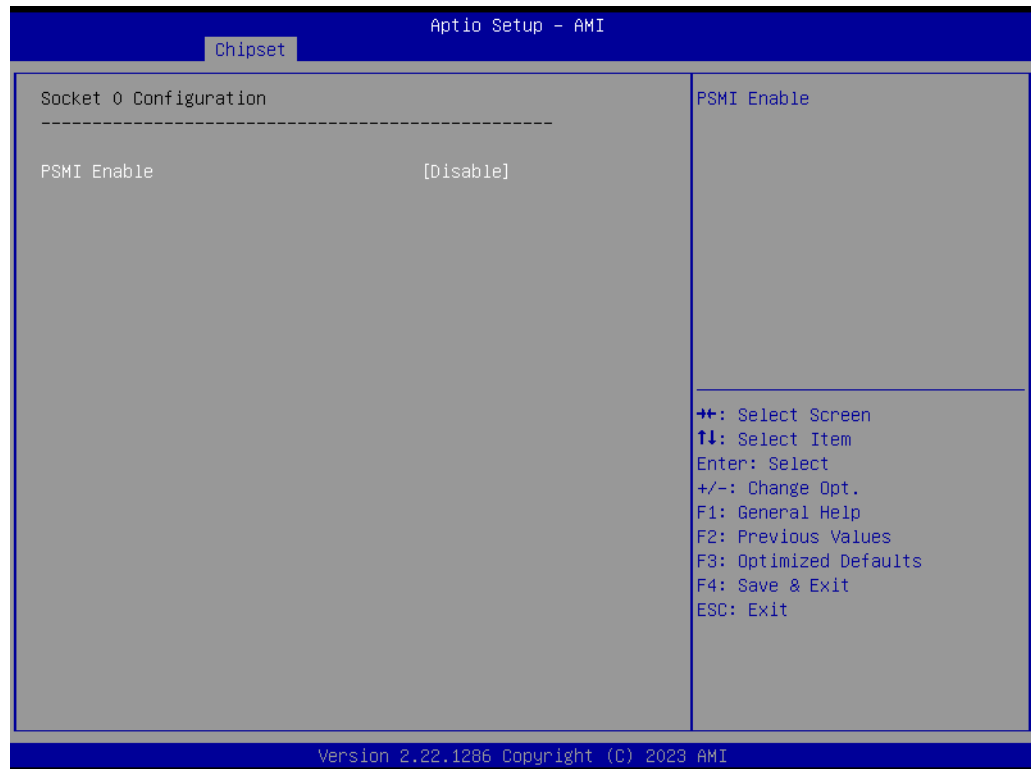


Figure 3.33 Socket 0 Configuration

- **PSMI Enable**
PSMI Enable.

3.2.2.29 Processor Dfx Configuration

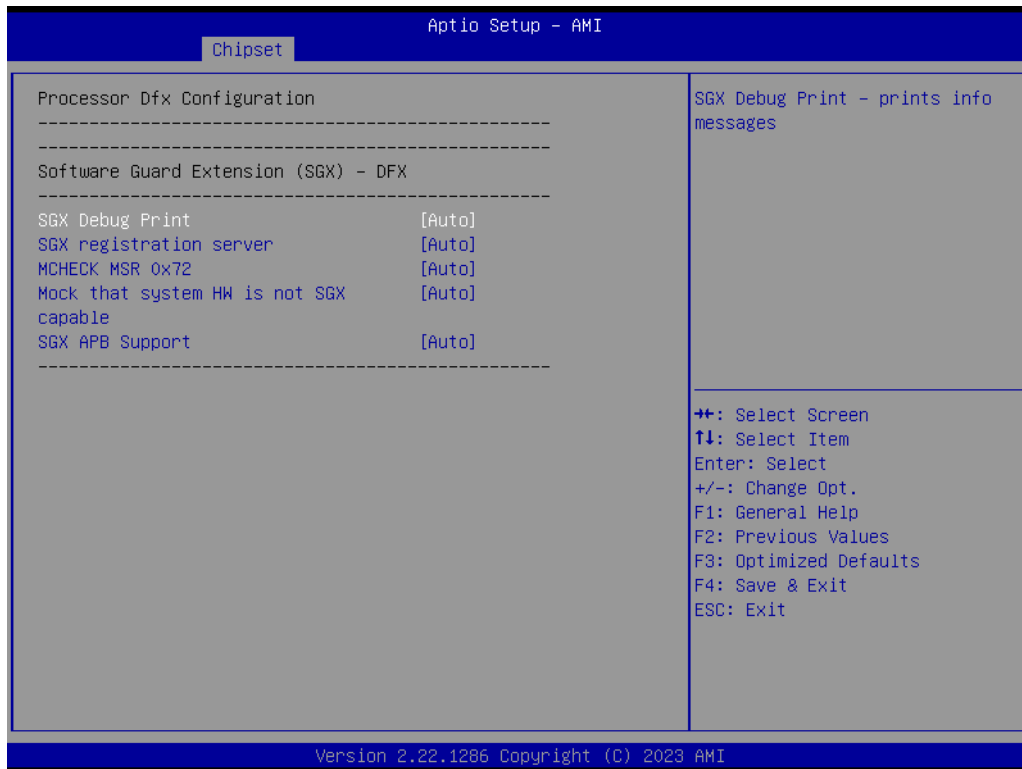


Figure 3.34 Processor Dfx Configuration

- **SGX Debug Print**
SGX Debug Print – prints info messages.
- **SGX registration server**
Choose which server should be used for SGX registration.
- **MCHECK MSR 0x72**
Triggers MCHECK with MSR 0x72, support for Simics.
- **Mock that system HW is not SGX capable**
Mock that system HW is not SGX capable: allows to test suppress in the BIOS menu.
- **SGX APB Support**
FPE on APB.

3.2.2.30 IIO Configuration

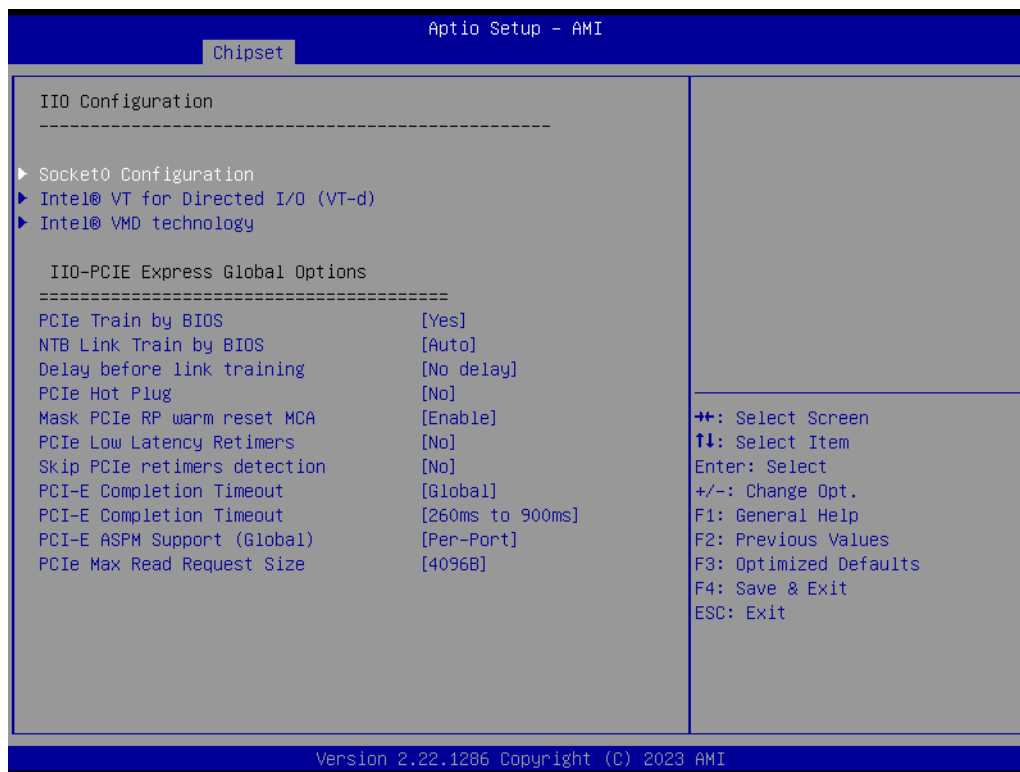


Figure 3.35 IIO Configuration

- **Socket0 Configuration**
- **Intel® VT for Directed I/O (VT-d)**
Press <Enter> to bring up the Intel® Virtualization for Directed I/O (VT-d) Configuration menu.
- **Intel® VMD technology**
Press <Enter> to bring up the Intel® VMD for Volume Management Device Configuration menu.
- **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 link.
- **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 speed up the boot. Retimers are present only in specific HW configurations.
- **PCI-E Completion Timeout**
Configure PCIe Completion Timeout in the Device Control2 register.

- **PCI-E Completion Timeout**
Configure PCIe Completion Timeout in the 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.

3.2.2.31 Socket0 Configuration

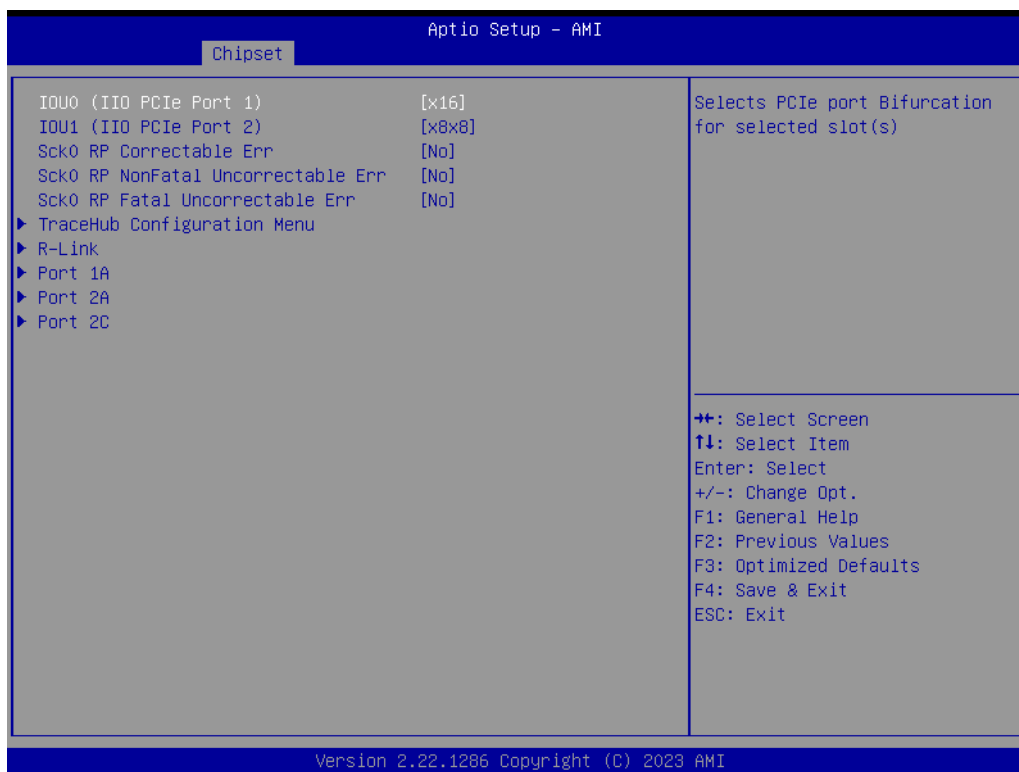


Figure 3.36 Socket 0 Configuration

- **IOU0 (IIO PCIe Port 1)**
Selects PCIe port Bifurcation for selected slot(s).
- **IOU1 (IIO PCIe Port 2)**
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 non-fatal errors.
- **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).

- **Port 2A**
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 2C**
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).

3.2.2.32 Trace Hub Configuration Menu

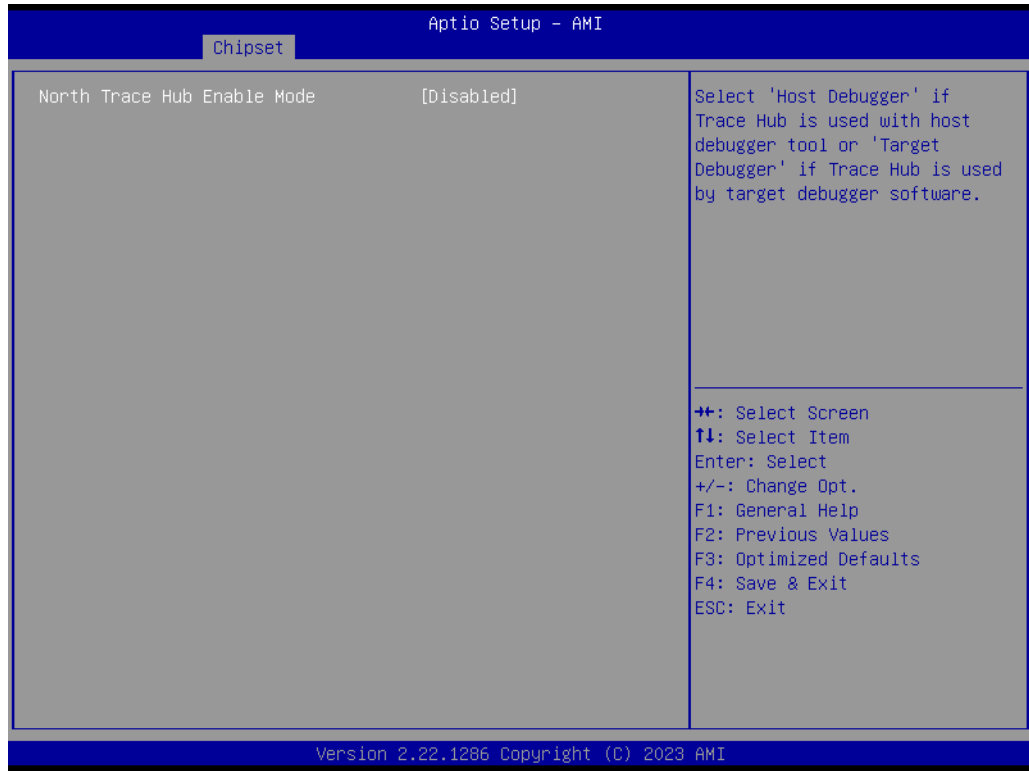


Figure 3.37 Trace Hub Configuration

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

3.2.2.33 R-Link

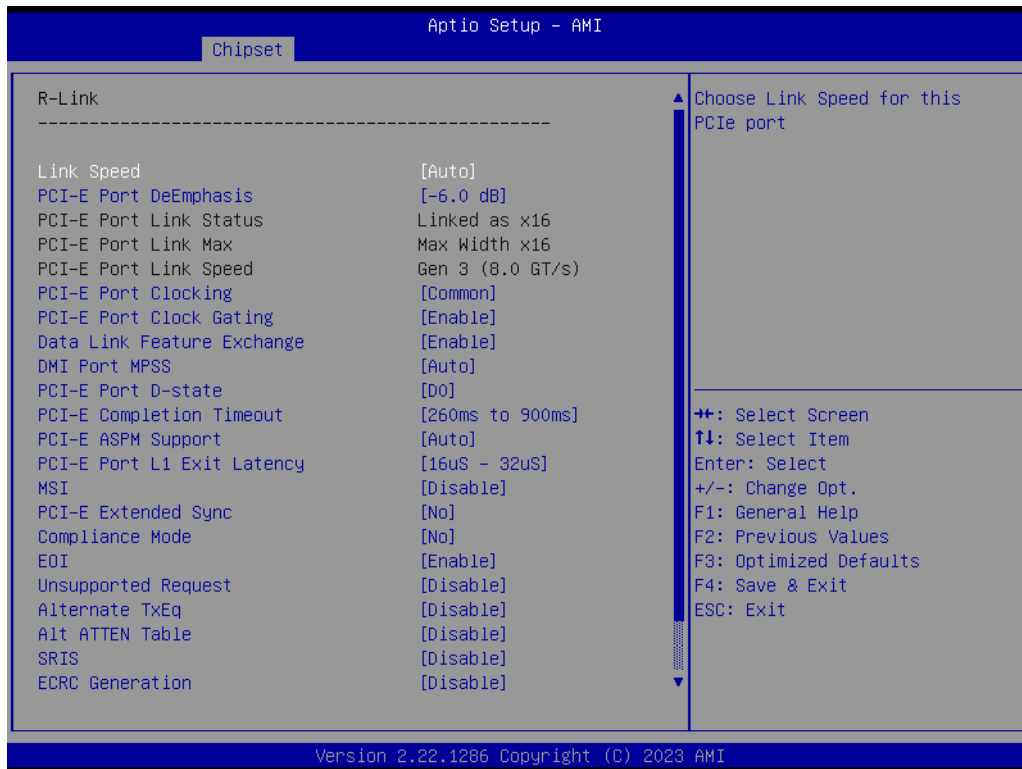


Figure 3.38 R-Link

- **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**
Configuration port clocking via LNKCON2[6]. This refers to this component 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 the 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 a low-power state.
- **PCI-E Completion Timeout**
Configure PCIe Completion Timeout in the Device Control2 register.
- **PCI-E ASPM Support**
This option can disable ASPM support in a PCIe root port. 'AUTO' keeps the hardware default.
- **PCI-E Port L1 Exit Latency**
The length of time this port requires to complete transition from L1 to L0.
- **MSI**
BUS0 DEVx FUN0 OFF 0x5A bit 0, where X is 0-3.

- **PCI-E Extended Sync**
Enable/Disable Extended Sync Mode (D:x F:0 O: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 it receives from a PCI Express/DMI port.
- **Alternate TxEq**
Enable/Disable TxEq.
- **Alt ATTEN Table**
Enable/Disable the Alternate Attenuator Table.
- **SRIS**
Enable/Disable SRIS.
- **ECRC Generation**
Enable/Disable ECRC Generation (Error Capabilities and Control Register).

3.2.2.34 R-Link

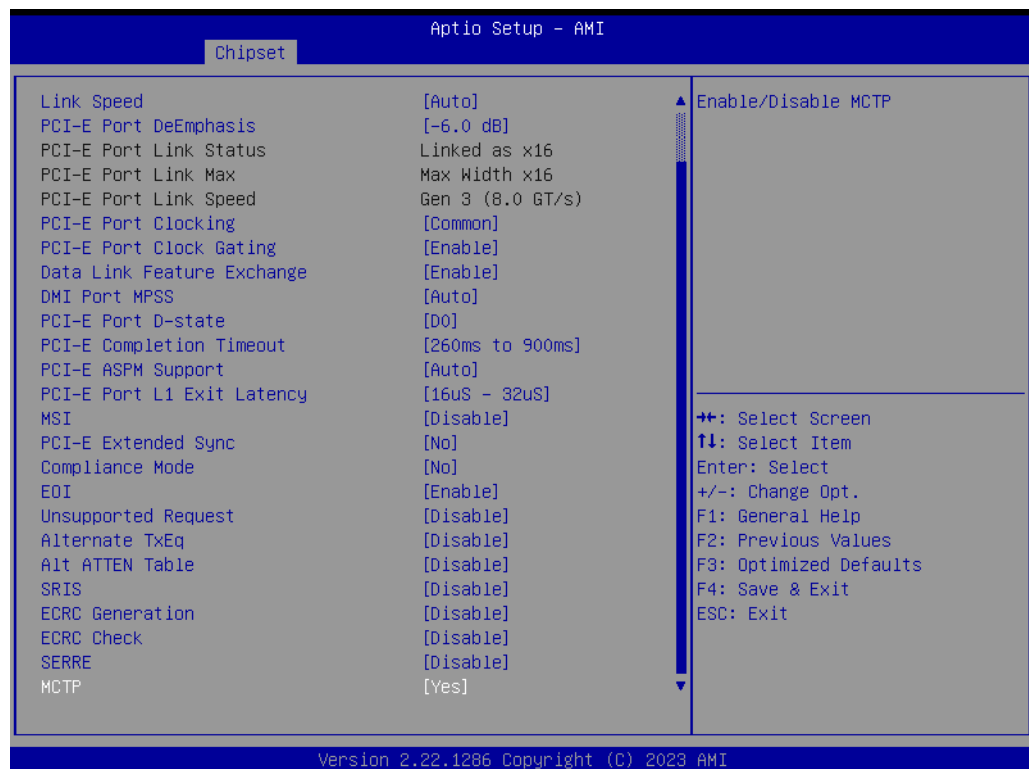


Figure 3.39 Chipset

- **ECRC Check**
Enable/Disable ECRC Check (Error Capabilities and Control Register).
- **SERRE**
Enable/Disable SERRE (SERR Reporting Enable).
- **MCTP**
Enable/Disable MCTP.

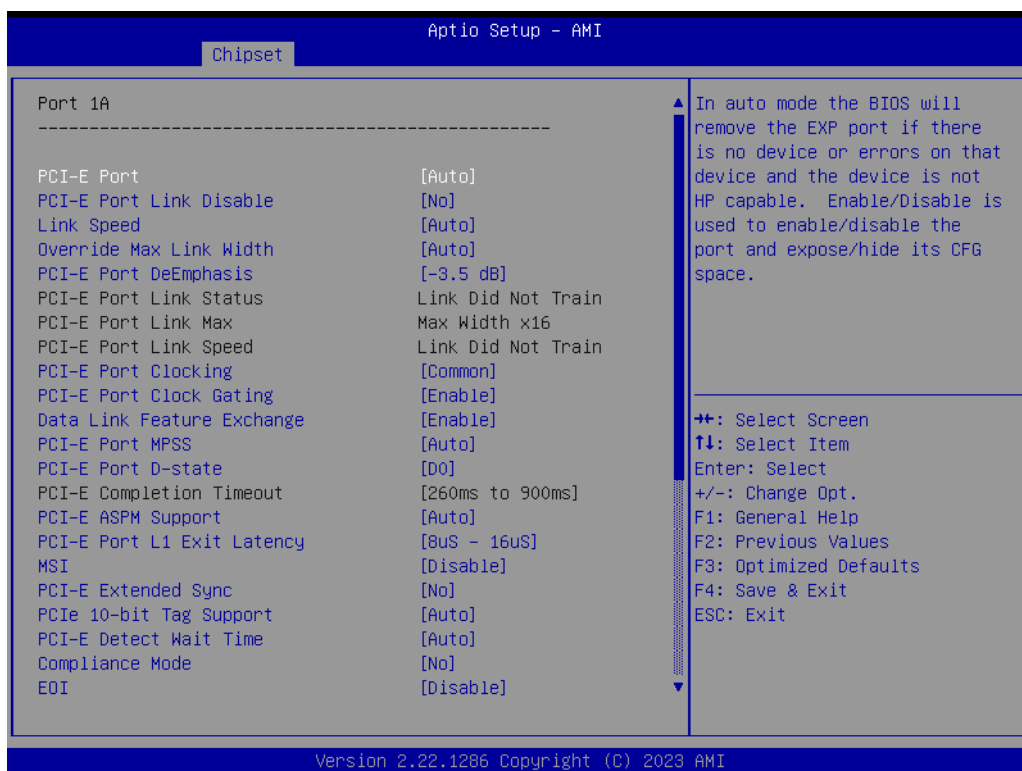


Figure 3.40 Port 1A

- **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 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**
Configuration port clocking via LNKCON2[6]. This refers to this component 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 the PCIe Capabilities register. 'AUTO' keeps the hardware default.
- **PCI-E Port D-state**
Set to D0 for normal operation, D3Hot to be in the 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.
- **PCI-E Port L1 Exit Latency**
The length of time this port requires to complete transition from L1 to L0.
- **MSI**
BUS0 DEVx FUN0 OFF 0x5A bit 0, where X is 0-3.
- **PCI-E Extended Sync**
Enable/Disable the Extended Sync Mode (D:x F:0 O: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 a 10-bit Tag Requester in the hierarchy where the Root Port is 10-bit Tag Completer capable, but not all nodes support a 10-bit Tag Completer. The user assures there will be no peer-to-peer traffic from a node with 10-bit Tag Requester capability to a node without 10-bit tag Completer capability. In such an hierarchy, a 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.

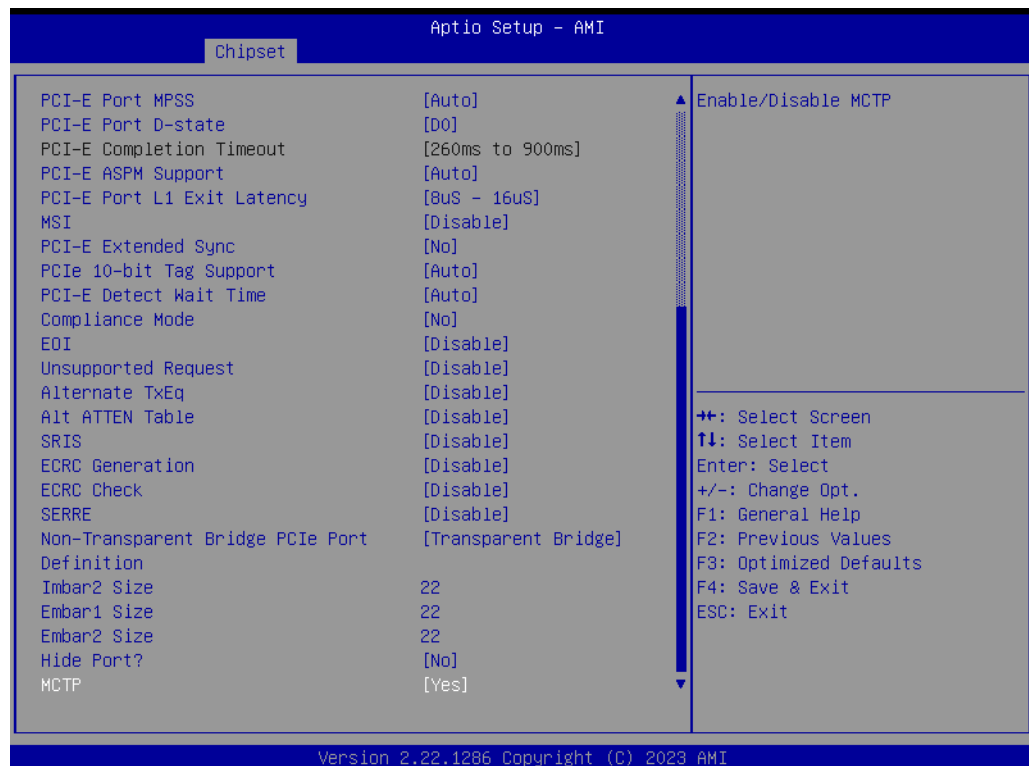


Figure 3.41 Port 1A

- **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/Disable TxEq.
- **Alt ATTEN Table**
Enable/Disable the Alternate Attenuator Table.
- **SRIS**
Enable/Disable SRIS.
- **ECRC Generation**
Enable/Disable ECRC Generation (Error Capabilities and Control Register).
- **ECRC Check**
Enable/Disable ECRC Check (Error Capabilities and Control Register).
- **SERRE**
Enable/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 IIO 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 hide this root port from the OS.
- **MCTP**
Enable/Disable MCTP.

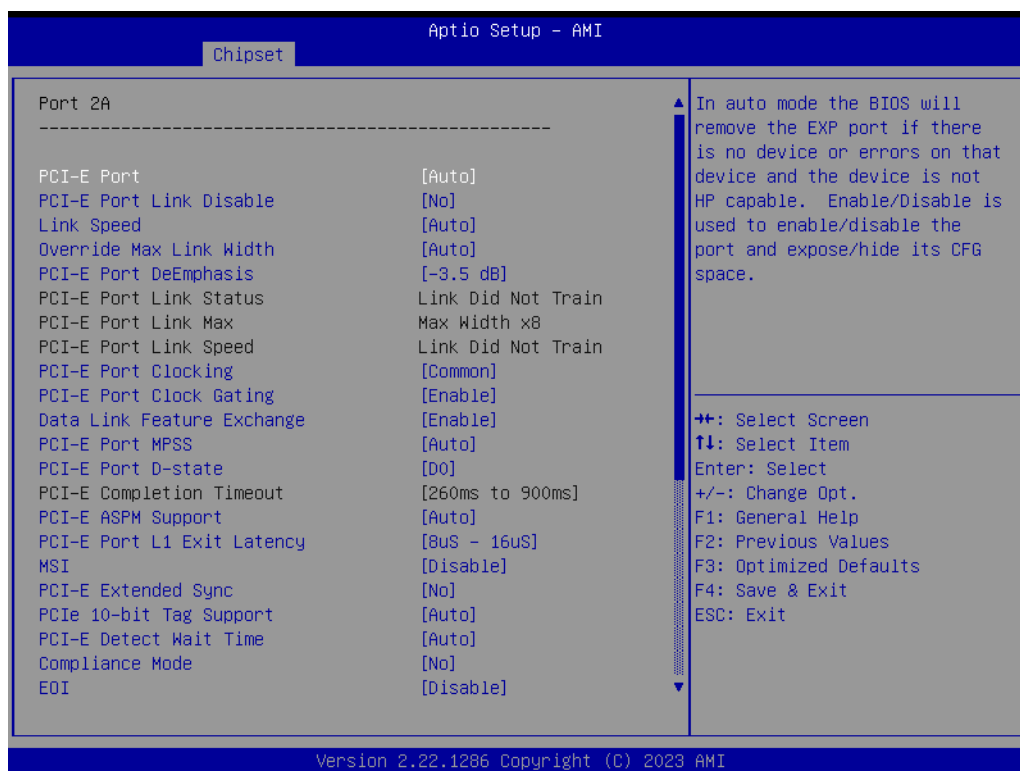


Figure 3.42 Port 2A

- **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 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**
Configuration port clocking via LNKCON2[6]. This refers to this component 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 the PCIe Capabilities register. 'AUTO' keeps the hardware default.
- **PCI-E Port D-state**
Set to D0 for normal operation, D3Hot to be in a 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.
- **PCI-E Port L1 Exit Latency**
The length of time this port requires to complete the transition from L1 to L0.
- **MSI**
BUS0 DEVx FUN0 OFF 0x5A bit 0, where X is 0-3
- **PCI-E Extended Sync**
Enable/Disable the Extended Sync Mode (D:x F:0 O: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 the hierarchy where the Root Port is 10-bit Tag Completer capable, but not all nodes support a 10-bit Tag Completer. The user assures there will be no peer-to-peer traffic from a node with 10-bit Tag Requester capability to a node without 10-bit tag Completer capability. In such an hierarchy, a 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.

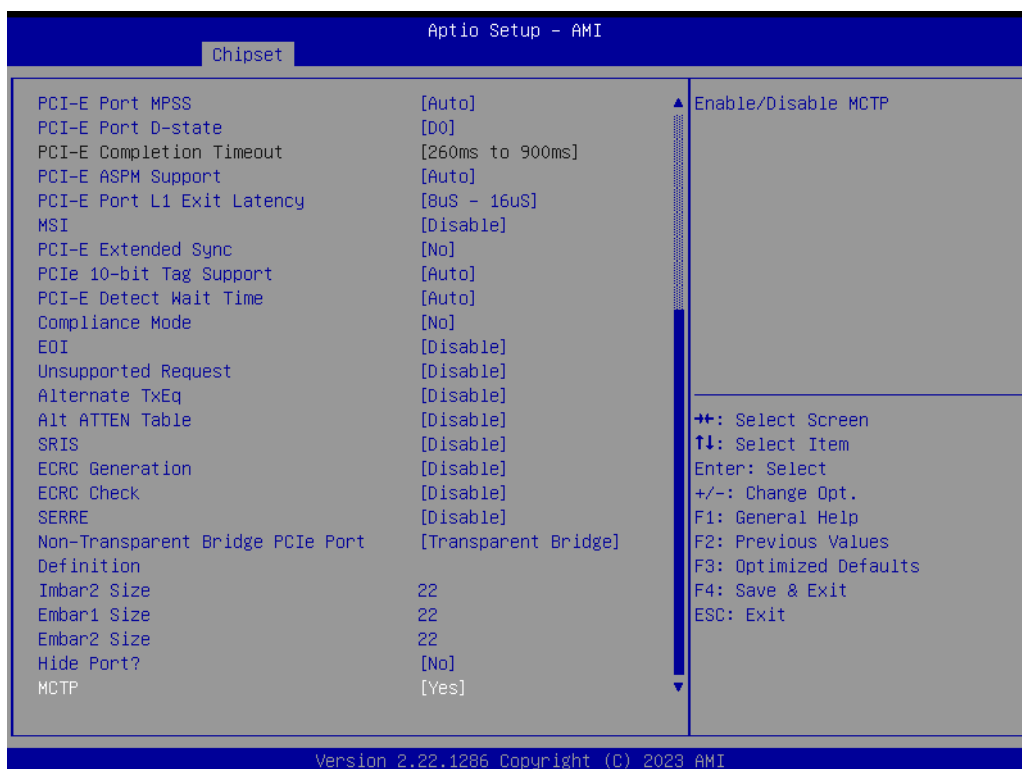


Figure 3.43 Port 2A

- **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/Disable TxEq.
 - **Alt ATTEN Table**
Enable/Disable the Alternate Attenuator Table.
 - **SRIS**
Enable/Disable SRIS.
 - **ECRC Generation**
Enable/Disable ECRC Generation (Error Capabilities and Control Register).
 - **ECRC Check**
Enable/Disable ECRC Check (Error Capabilities and Control Register).
 - **SERRE**
Enable/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 IIO 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 hide this root port from the OS.
 - **MCTP**
Enable/Disable MCTP.

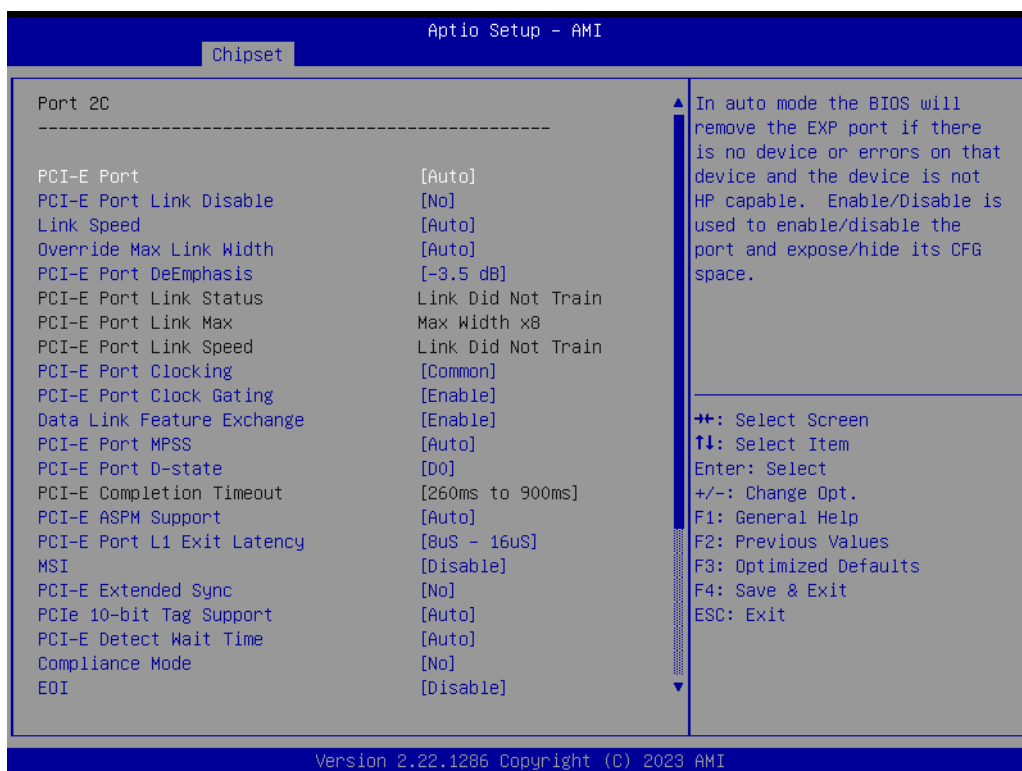


Figure 3.44 Port 2C

- **PCI-E Port**
In auto mode the BIOS will remove the EXP port if there is no device or there are 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**
Configuration port clocking via LNKCON2[6]. This refers to this component 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 the PCIe Capabilities register. 'AUTO' keeps the hardware default.
- **PCI-E Port D-state**
Set to D0 for normal operation, 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.
- **PCI-E Port L1 Exit Latency**
The length of time this port requires to complete transition from L1 to L0.
- **MSI**
BUS0 DEVx FUN0 OFF 0x5A bit 0, where X is 0-3.
- **PCI-E Extended Sync**
Enable/Disable Extended Sync Mode (D:x F:0 O: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 a 10-bit Tag Requester in the hierarchy where the Root Port is 10-bit Tag Completer capable, but not all nodes support a 10-bit Tag Completer. The user assures there will be no peer-to-peer traffic from a node with a 10-bit Tag Requester capability to a node without 10-bit tag Completer capability. In such an hierarchy, a 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.

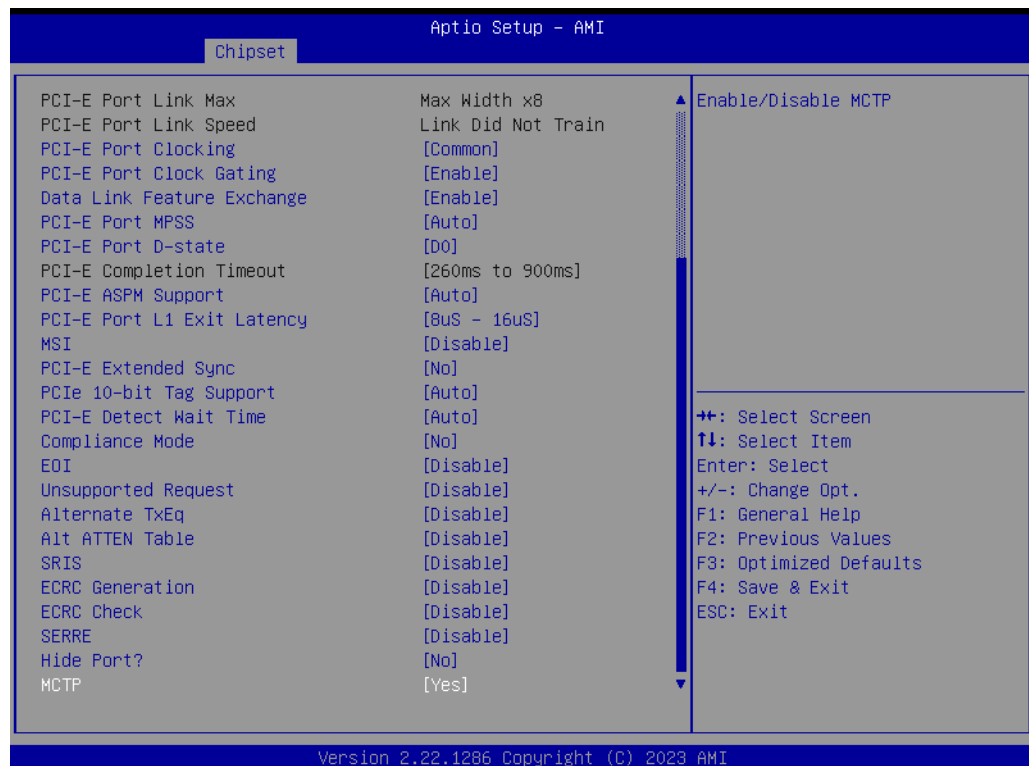


Figure 3.45 Port 2C

- **Unsupported Request**
Controls the reporting of unsupported requests that IIO itself detects on requests it receives from a PCI Express/DMI port.

- **Alternate TxEq**
Enable/Disable TxEq.
- **Alt ATTEN Table**
Enable/Disable Alternate Attenuator Table.
- **SRIS**
Enable/Disable SRIS.
- **ECRC Generation**
Enable/Disable ECRC Generation (Error Capabilities and Control Register).
- **ECRC Check**
Enable/Disable ECRC Check (Error Capabilities and Control Register).
- **SERRE**
Enable/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 IIO 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 hide this root port from the OS.
- **MCTP**
Enable/Disable MCTP.

3.2.2.35 Intel® Ethernet Connection

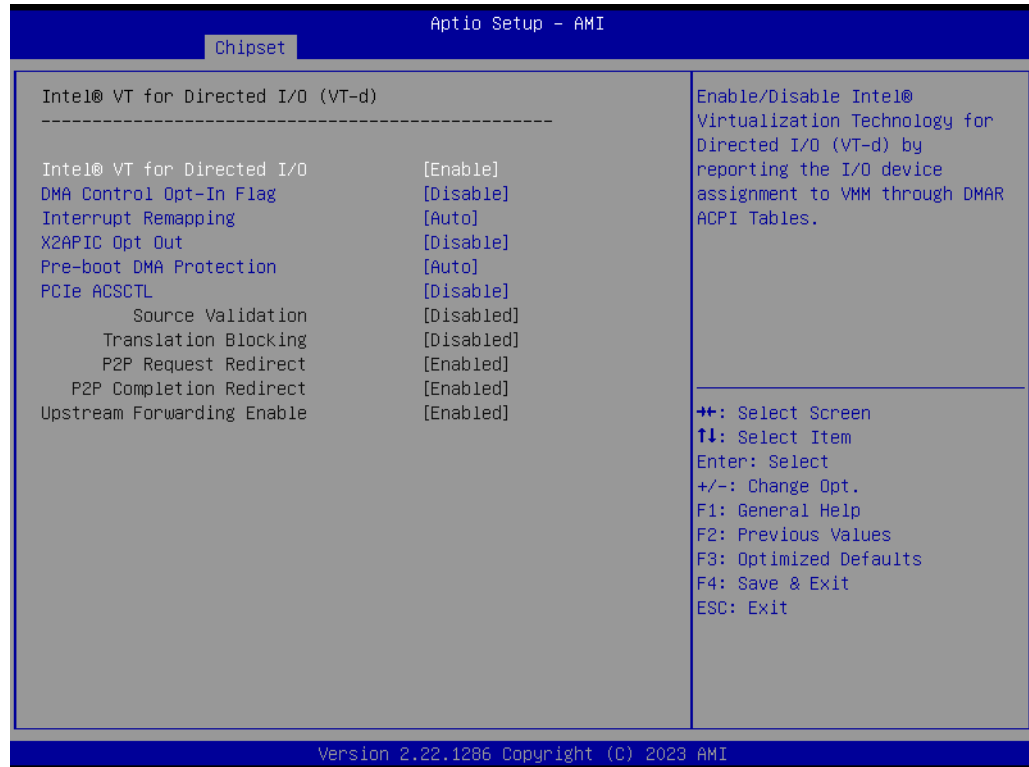


Figure 3.46 Intel® VT for Directed I/O (VT-d)

- **Intel VT for Directed I/O**
Enable/Disable Intel® Virtualization Technology for Directed I/O (VT-d) by reporting the I/O device assignment to VMM through DMAR ACPI Tables.
- **DMA Control Opt-In Flag**
Enable/Disable DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR table in ACPI. It is not compatible with Direct Device Assignment (DDA).
- **Interrupt Remapping**
Enable/Disable VT-d Interrupt Remapping Support.
- **X2APIC Opt Out**
Enable/Disable X2APIC_OPT_OUT bit.
- **Pre-boot DMA Protection**
Enable DMA Protection in the Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)
- **PCIe ACSCTL**
Enable/Disable overwrite of PCI Access Control Services Control register in PCI root ports.
- **Source Validation**
When set, the component validates the Bus Number from the Requester ID of upstream Requests against the secondary/subordinate Bus Numbers.
- **Translation Blocking**
When set, the component blocks all upstream Memory Requests whose Address Translation (AT) field is not set to the default value.
- **P2P Request Redirect**
This bit determines when the component redirects peer-to-peer Requests upstream.

- **P2P Completion Redirect**
Determines when the component redirects peer-to-peer Completions upstream, applicable only to Read Completions whose Relaxed Ordering Attribute is clear.
- **Upstream Forwarding Enable**
When set, the component forwards upstream any Request or Completion TLPs it receives that were redirected upstream by a component lower in the hierarchy.

3.2.2.36 Intel® VMD technology

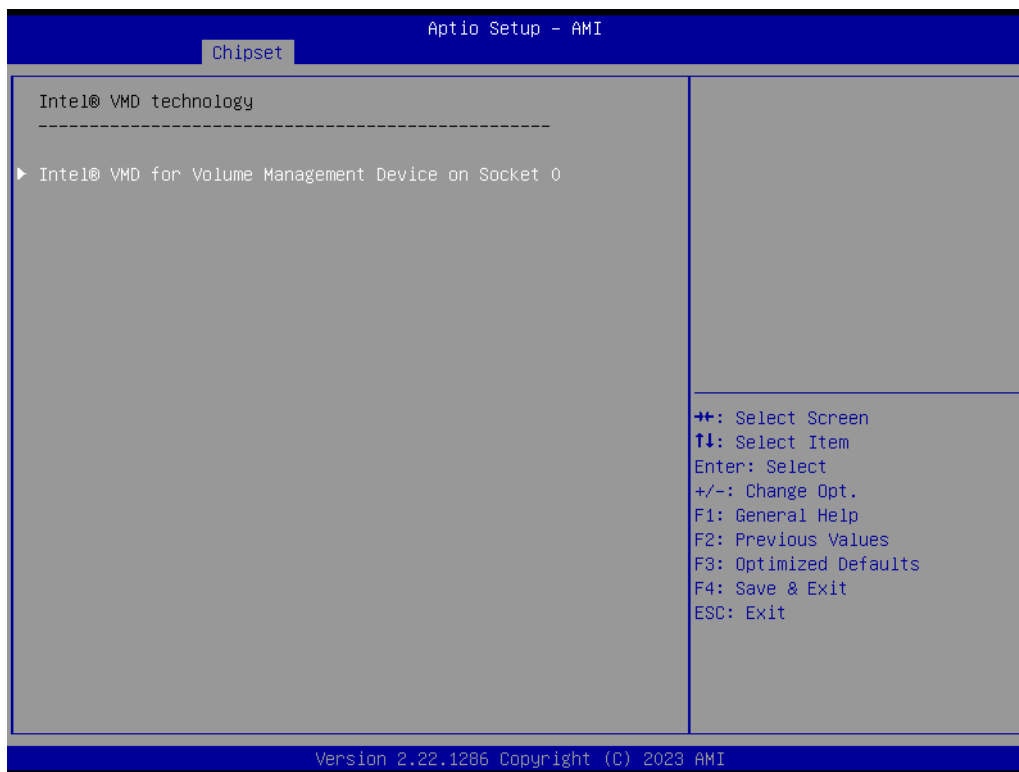


Figure 3.47 Intel® VMD technology

- **Intel® VMD for Volume Management Device on Socket 0**

3.2.2.37 VMD Config

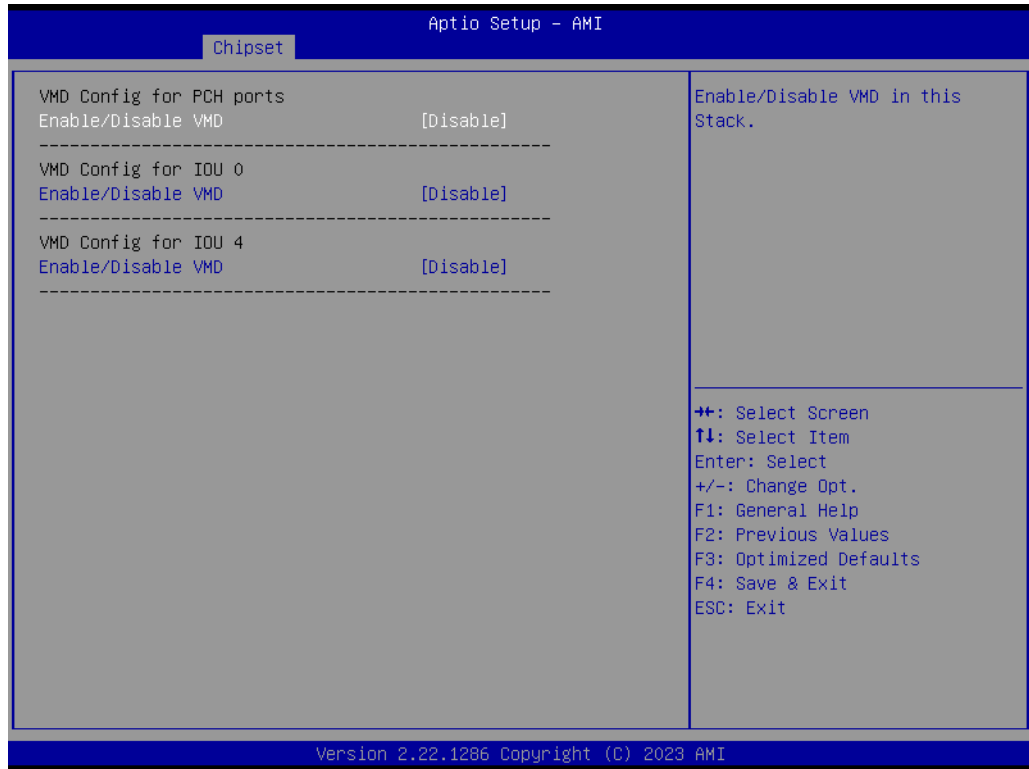


Figure 3.48 VMD Config

- **VMD Config for PCH Ports**
Enable/Disable VMD in the stack.
- **VMD Config for IOU 0**
Enable/Disable VMD in the stack.
- **VMD Config for IOU 4**
Enable/Disable VMD in the stack.

3.2.2.38 Package C State Control

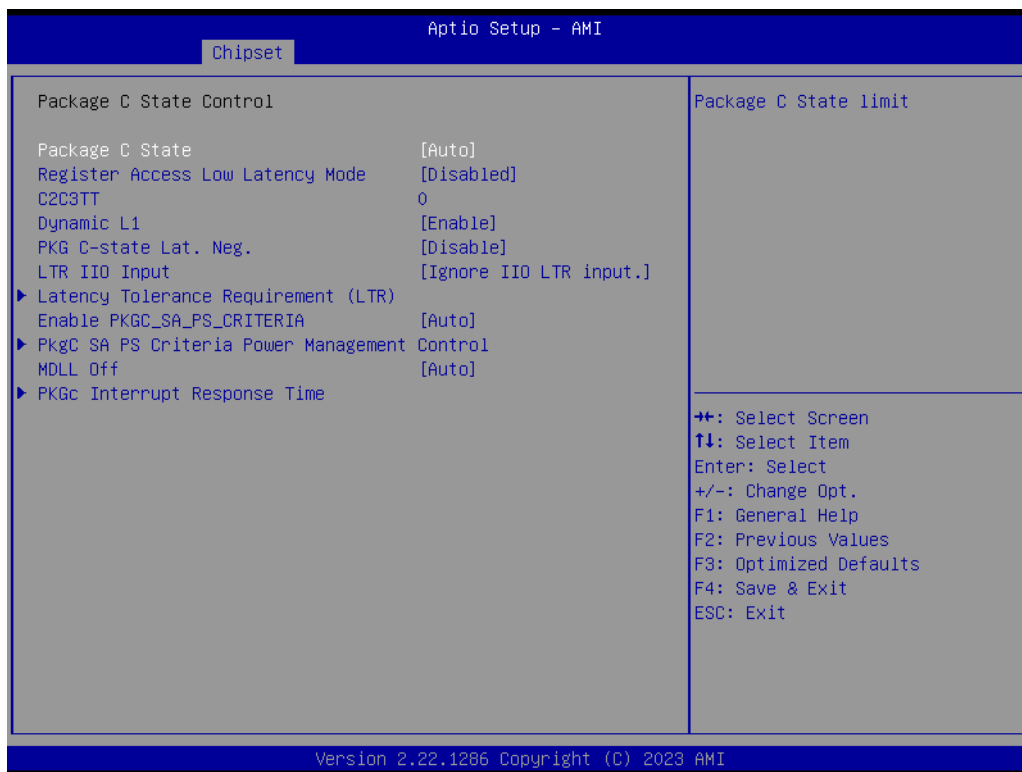


Figure 3.49 Package C State Control

- **Package C State**
Package C State Limit.
- **Register Access Low Latency Mode**
Enable lower latency mode for register access. Note: Enabling this mode will prevent PkgC6 as register access fabric and prevent it 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.
- **Enable PKGC_SA_PS_CRITERIA**
Program WRITE_PKGC_SA_PS_CRITERIA Sub Menu.
- **PkgC SA PS Criteria Power Management Control**
Program WRITE_PKGC_SA_PS_CRITERIA Sub Menu.
- **MDLL Off**
Enable shutdown of MDLL during SR.
- **PKGc Interrupt Response Time**
Programmable Package C-state interrupt response time setup control.

3.2.2.39 Latency Tolerance Requirement (LTR)

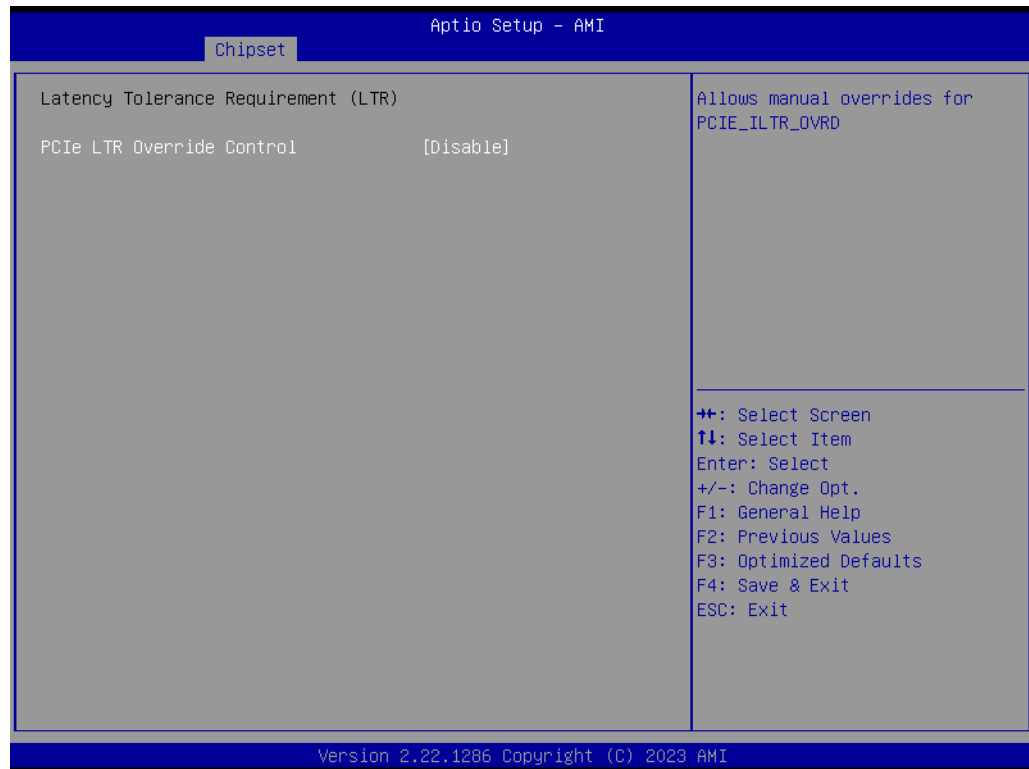


Figure 3.50 Latency Tolerance Requirement

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

3.2.2.40 PkgC SA PS Criteria Power Management Control

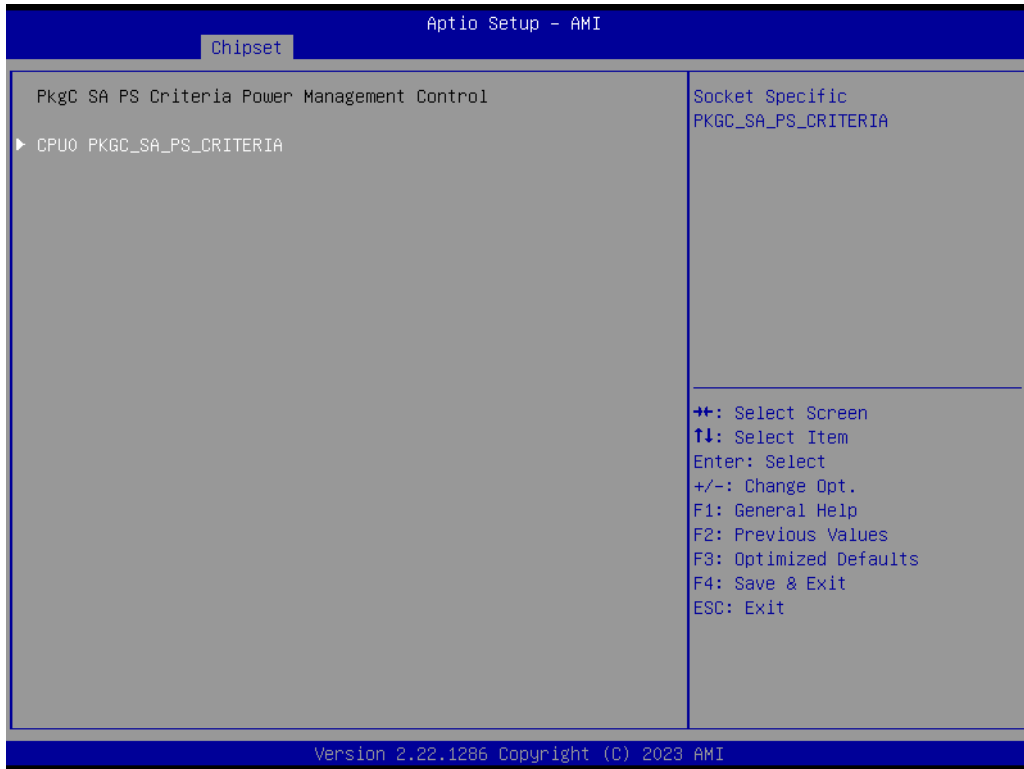


Figure 3.51 PkgC SA PS Criteria Power Management Control

- **CPU0 PKGC_SA_PS_CRITERIA**
Socket-Specific PKGC_SA_PS_CRITERIA.

3.2.2.41 CPU0 PKGC_SA_PS_CRITERIA

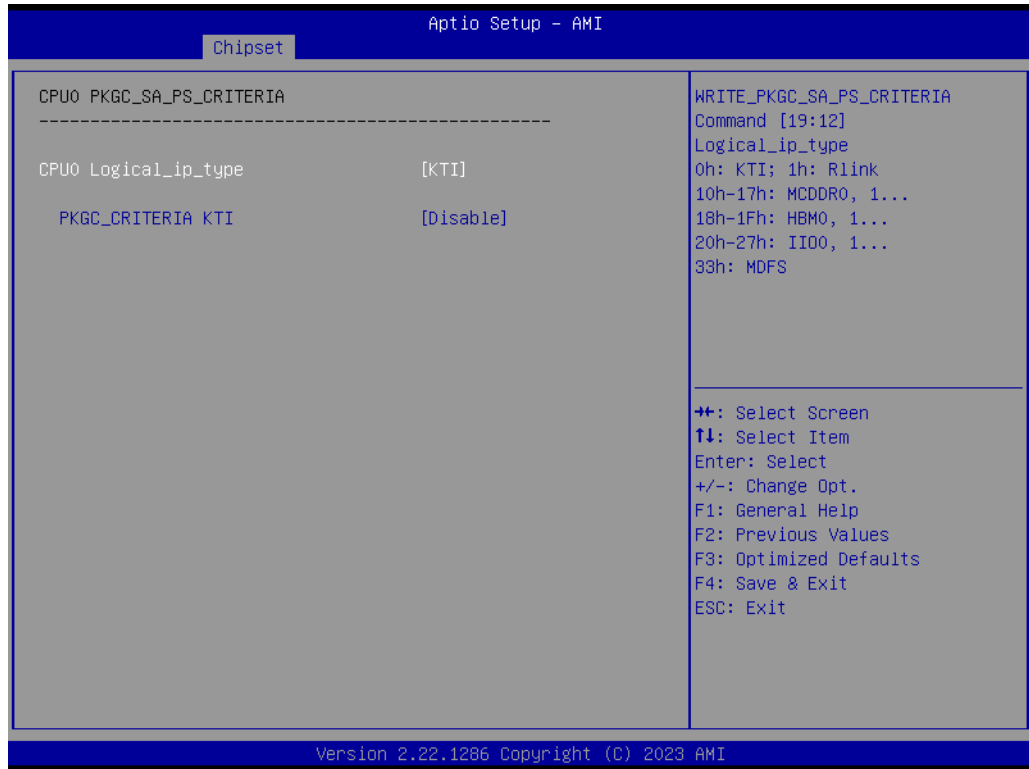


Figure 3.52 CPU0 PKGC_SA_PS_CRITERIA

- **CPU0 Logical_ip_type**
WRITE_PKGC_SA_PS_CRITERIA Command [19:12]
Logical_ip_type oh:KTI; 1H: RINK
10h-17h: MCDDR0, 1...
18h-1Fh: HBMO, 1...
20h-27h: IIO0, 1...
33h: MDFS
- **PKGCRITERIA KTI**
Enable: B2P WRITE_PKGC_SA_PS_CRITERIA accepts input value.

3.2.2.42 PKGc Interrupt Response Time

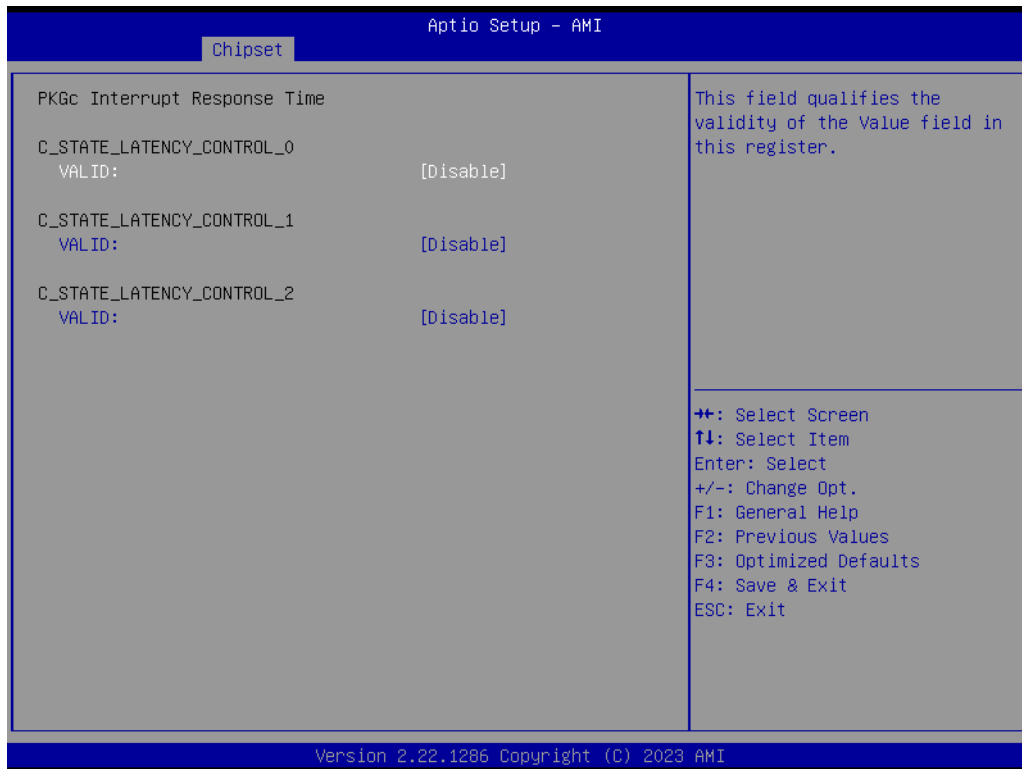


Figure 3.53 PKGc Interrupt Response Time

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

3.2.2.43 ACPI Sx State Control

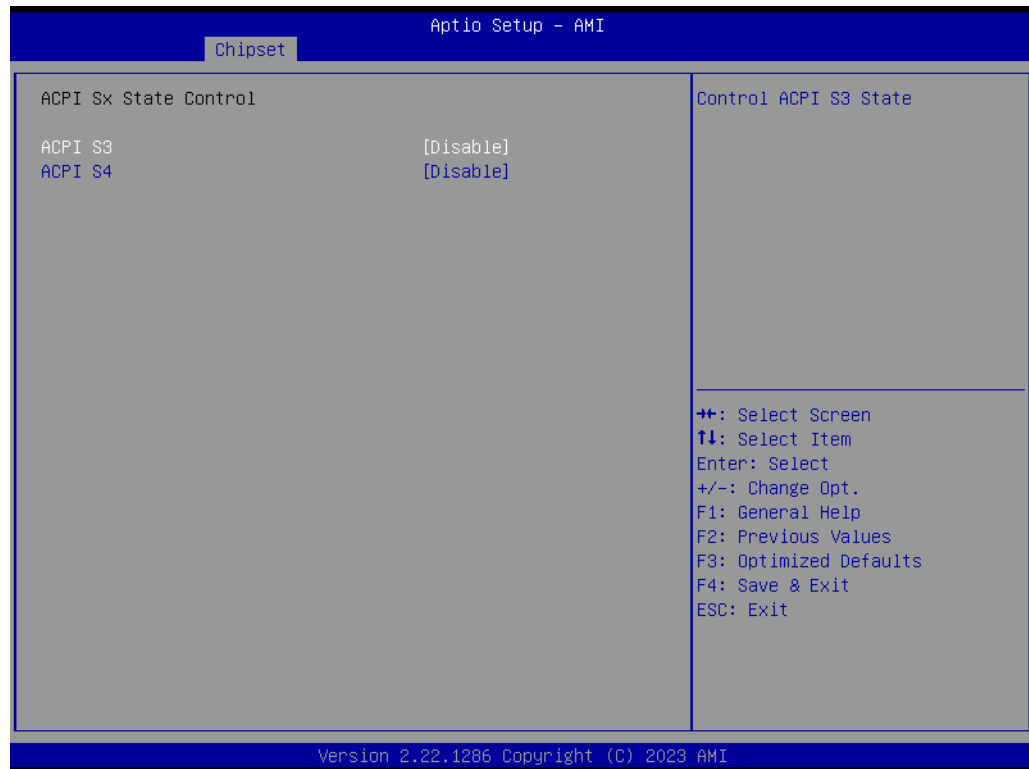


Figure 3.54 ACPI Sx State Control

- **ACPI S3**
Controls ACPI S3 State.
- **ACPI S4**
Controls ACPI S4 State.

3.2.2.44 Memory Power & Thermal Configuration

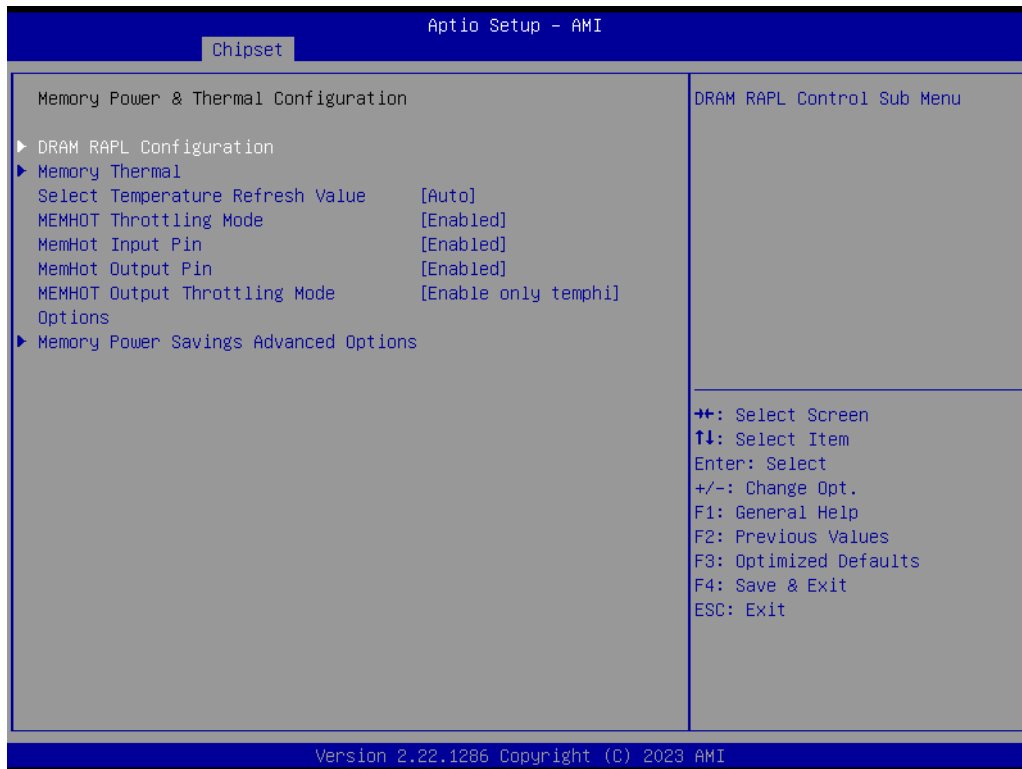


Figure 3.55 Memory Power & Thermal Configuration

- **DRAM RAPL Configuration**
DRAM RAPL Control Sub-Menu.
- **Memory Thermal**
Set memory thermal settings.
- **Select Temperature Refresh Value**
Option to manually enter a Temperature refresh value. Select Manual to enter a value, Auto for default.
- **MEMHOT Throttling Mode**
Configure MEMHOT Input and Output Mode: Mem Hot Sense Therm Throt or Mem Hot Output Therm Throt.
- **MemHot Input Pin**
Configure Memhot input.
- **MemHot Output Pin**
Configure Memhot output.
- **MEMHOT Output Throttling Mode Options**
Configure MEMHOT Output Mode options: Enable/Disable the Throt Output high, mid and low bit fields.
- **Memory Power Savings Advanced Options**
Advanced Settings for CKE and related Memory Power Savings Features.

3.2.2.45 DRAM RAPL Configuration

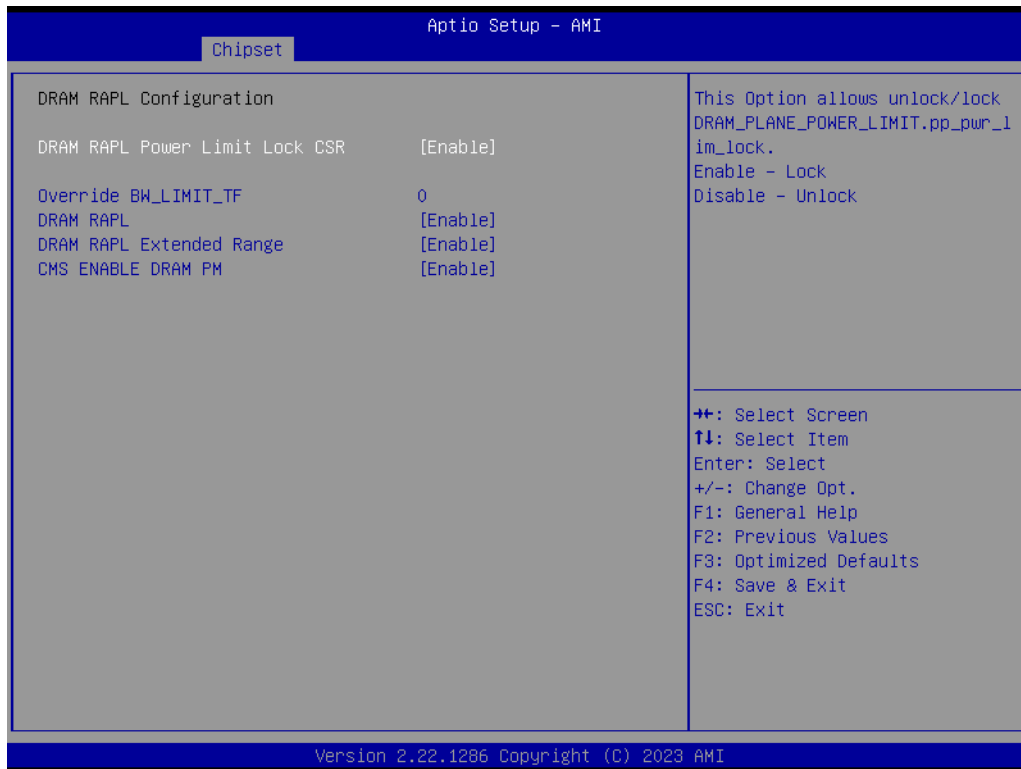


Figure 3.56 DRAM RAPL Configuration

- **DRAM RAPL Power Limit Lock CSR**
 This Option allows unlock/lock DRAM_PLANE_POWER_LIMIT.pp_pwr_lim_lock.
 Enable-Lock
 Disable-Unlock
- **Override BW_LIMIT_TF**
 Allows custom tuning of BW_LIMIT_TF when DRAM RAPL is enabled.
- **DRAM RAPL**
 Enable\Disable DRAM Rapl.
- **DRAM RAPL Extended Range**
 Select DRAM RAPL Extended Range.
- **CMS ENABLE DRAM PM**
 CMS ENABLE DRAM PM.

3.2.2.46 Memory Thermal Management

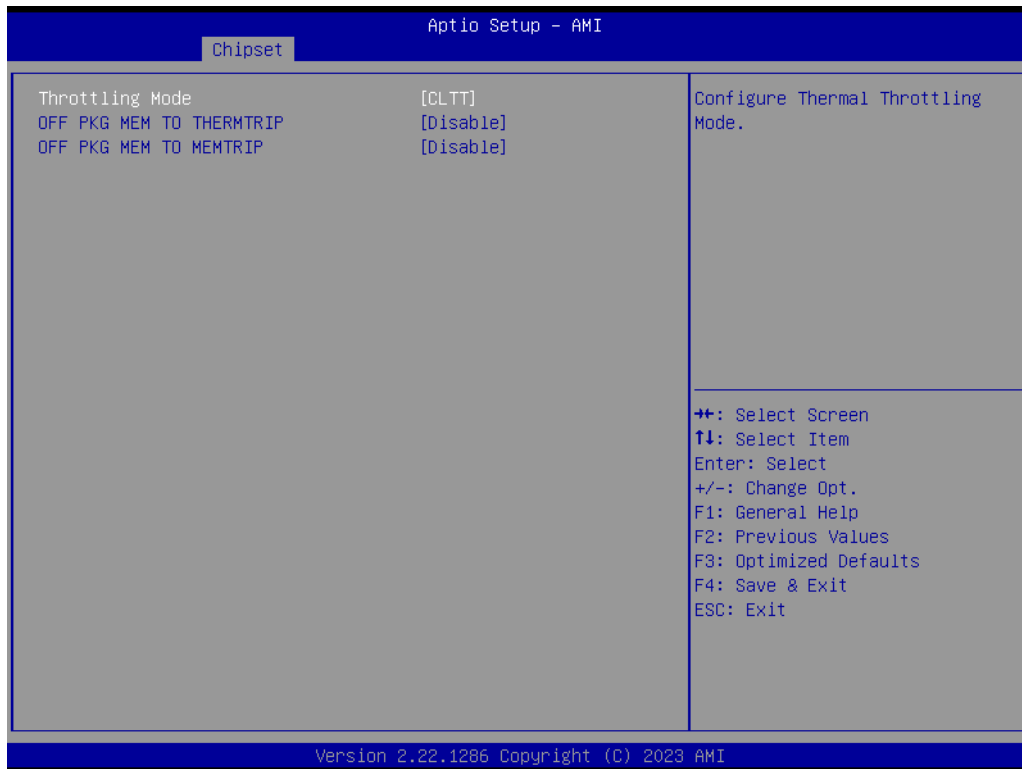


Figure 3.57 Memory Thermal Configuration

- **Throttling Mode**
Configure Thermal Throttling Mode.
- **OFF PKG MEM TO THERMTRIP**
If set to 0, the processor will ignore offpkg Memtrip to thermtrip tree. If set to 1, the processor will include offpkg Memtrip to thermtrip tree.
- **OFF PKG MEM TO MEMTRIP**
If set to 0, the processor will ignore offpkg memtrip to memtrip tree. If set to 1, the processor will include offpkg memtrip to memtrip tree.

3.2.2.47 Memory Power & Thermal Configuration

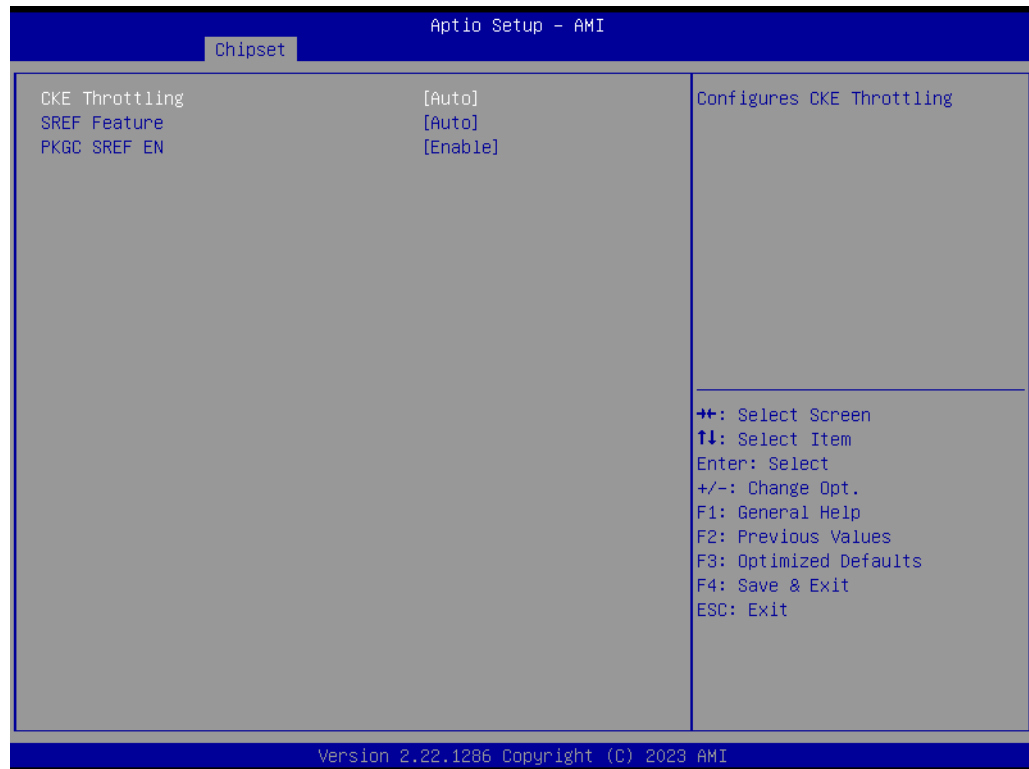


Figure 3.58 Memory Power & Thermal Configuration

- **CKE Throttling**
Configures CKE Throttling.
- **SREF Feature**
Select the manual or auto programming Self Refresh feature.
- **PKGC SREF EN**
Enable/Disable PKGC Self Refresh.

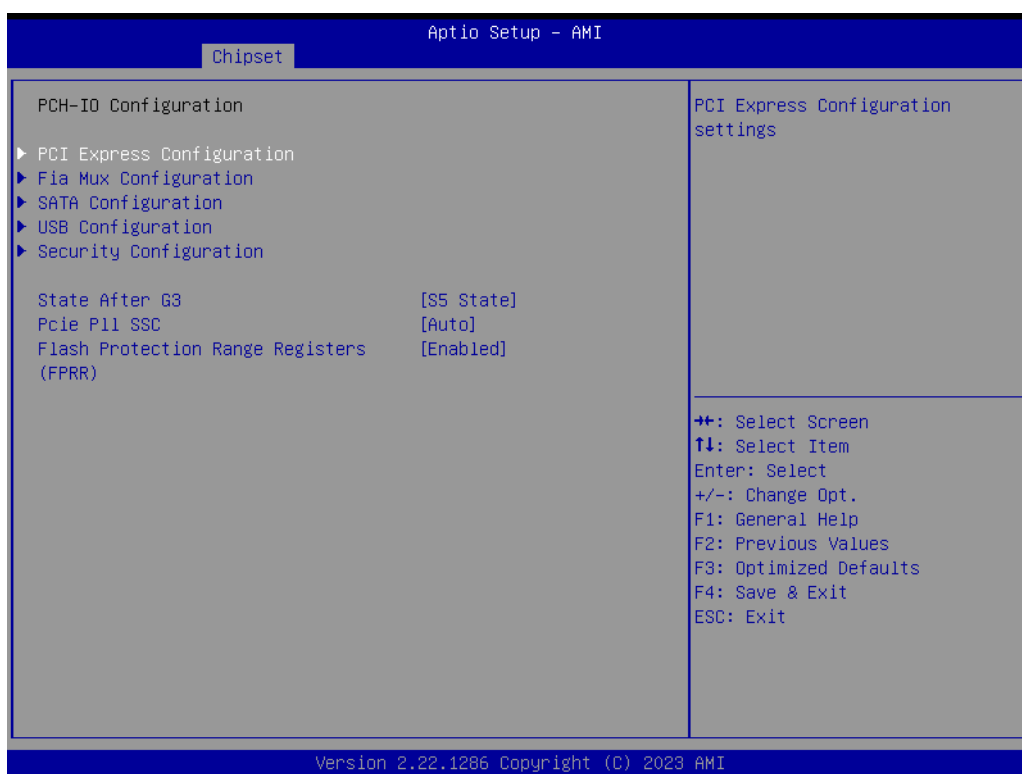
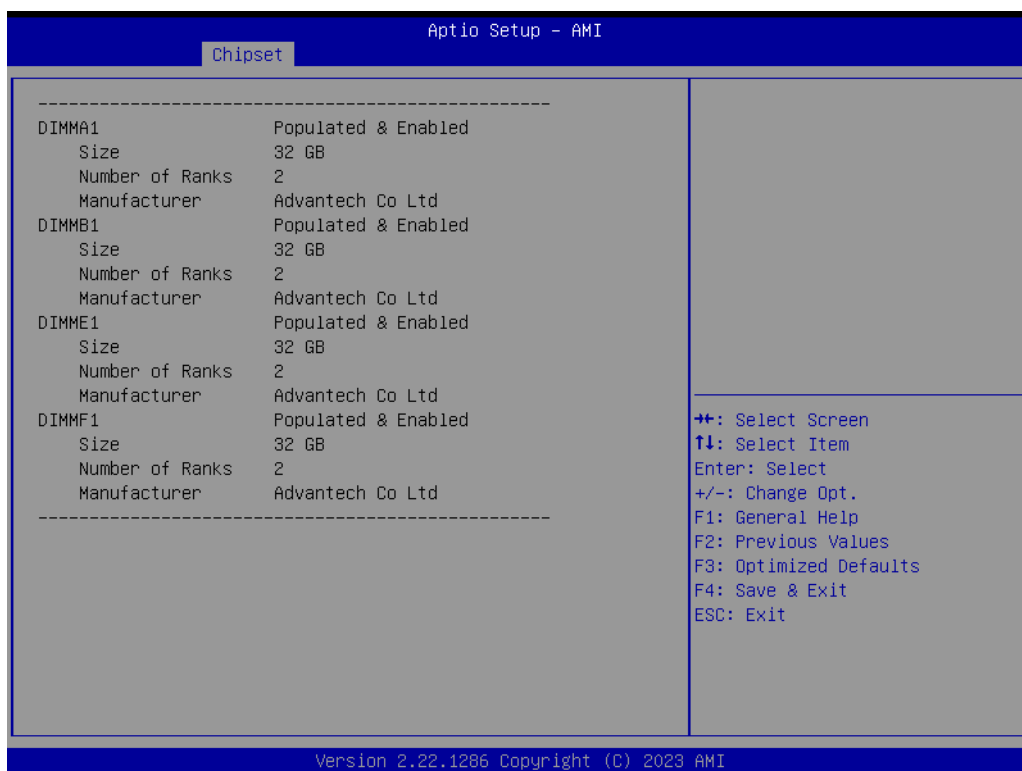


Figure 3.59 PCH-IO Configuration

- **PCI Express Configuration**
PCI Express Configuration settings.
- **Fia Mux Configuration**
Configuration of FIA Mux.

- **SATA Configuration**
Device Options Settings.
- **USB Configuration**
Configuration of FIA Mux.
- **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.

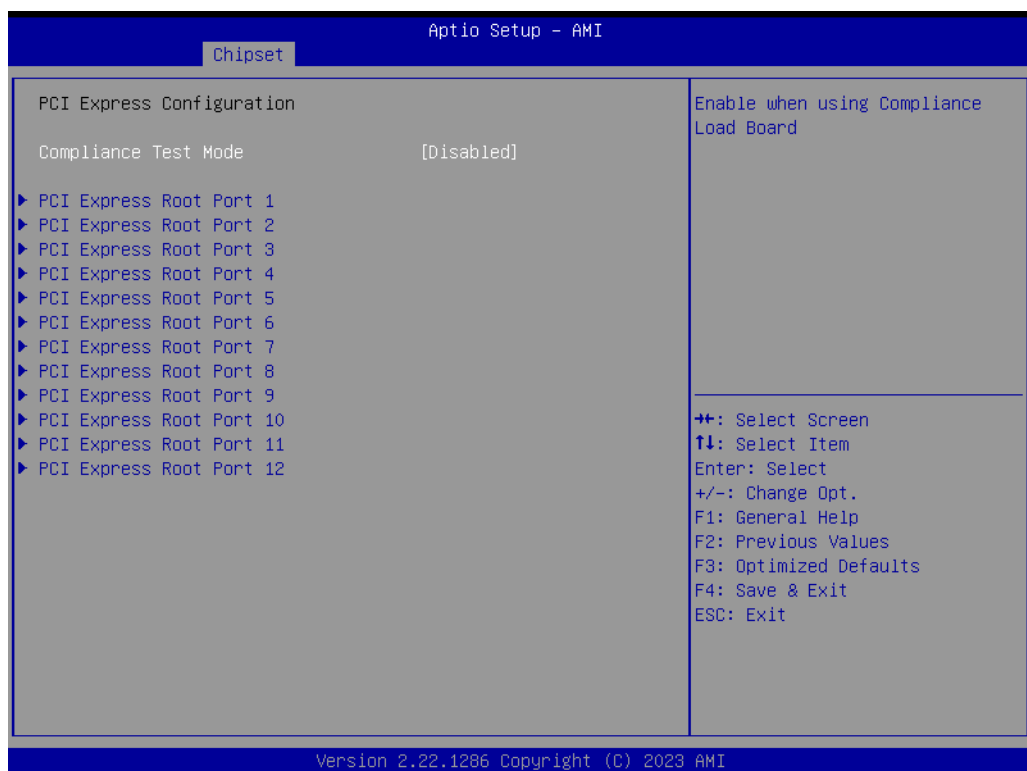


Figure 3.60 PCI Express Configuration

- **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.



Figure 3.61 PCI Express Configuration

- **PCI Express Root Port 1**
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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.62 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.63 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.64 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.65 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.66 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.

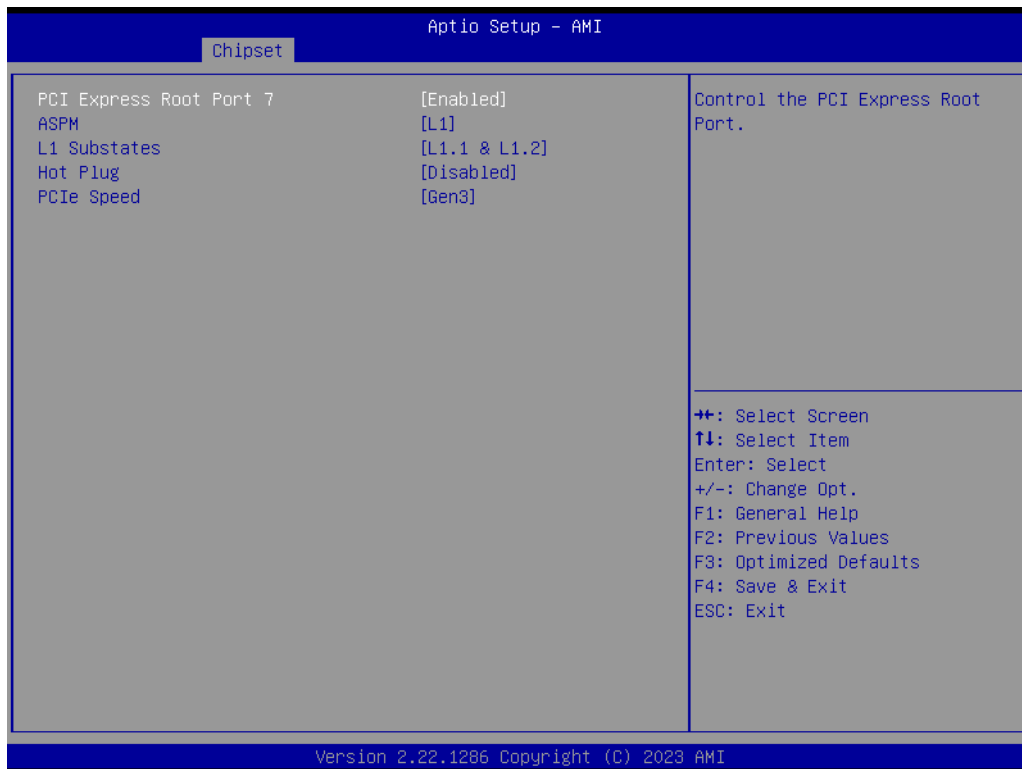


Figure 3.67 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.68 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.69 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.70 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.71 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.



Figure 3.72 PCI Express Configuration

- **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 is equal to Gen2 or Gen3 depending on DTR soft strap.

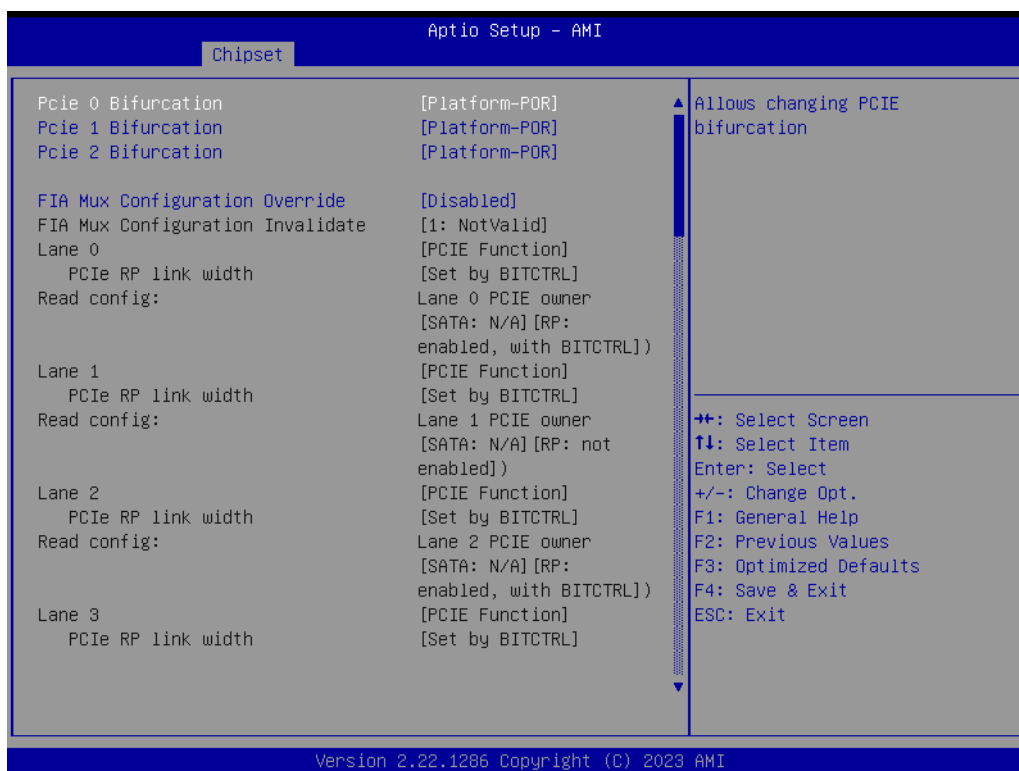
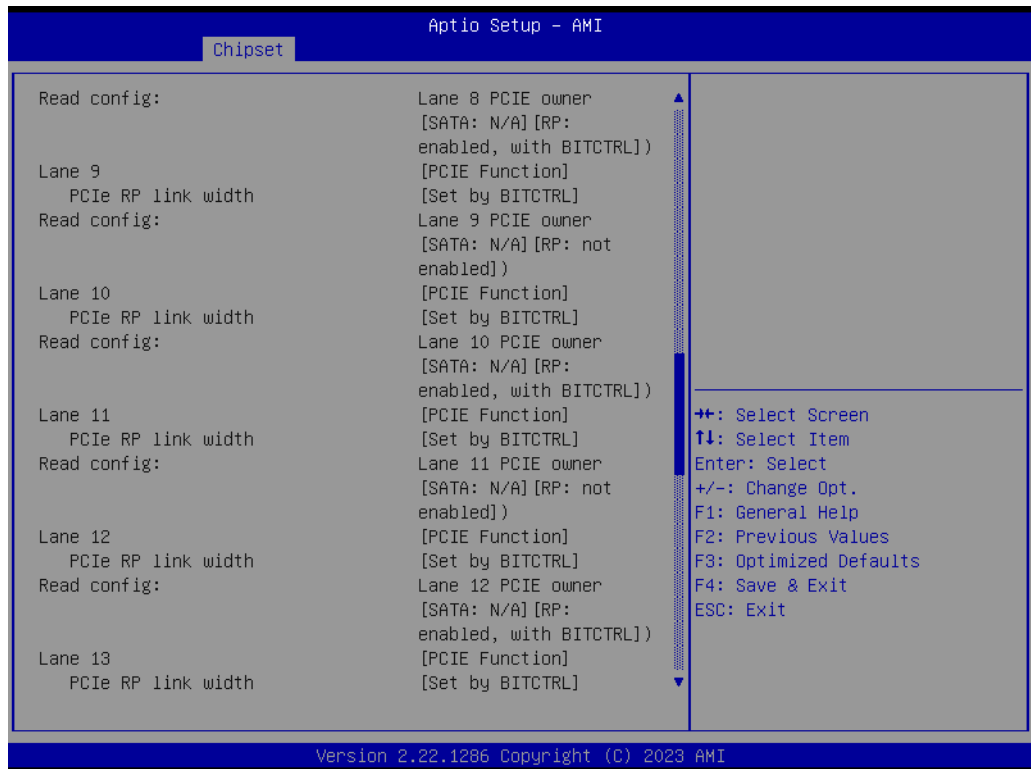
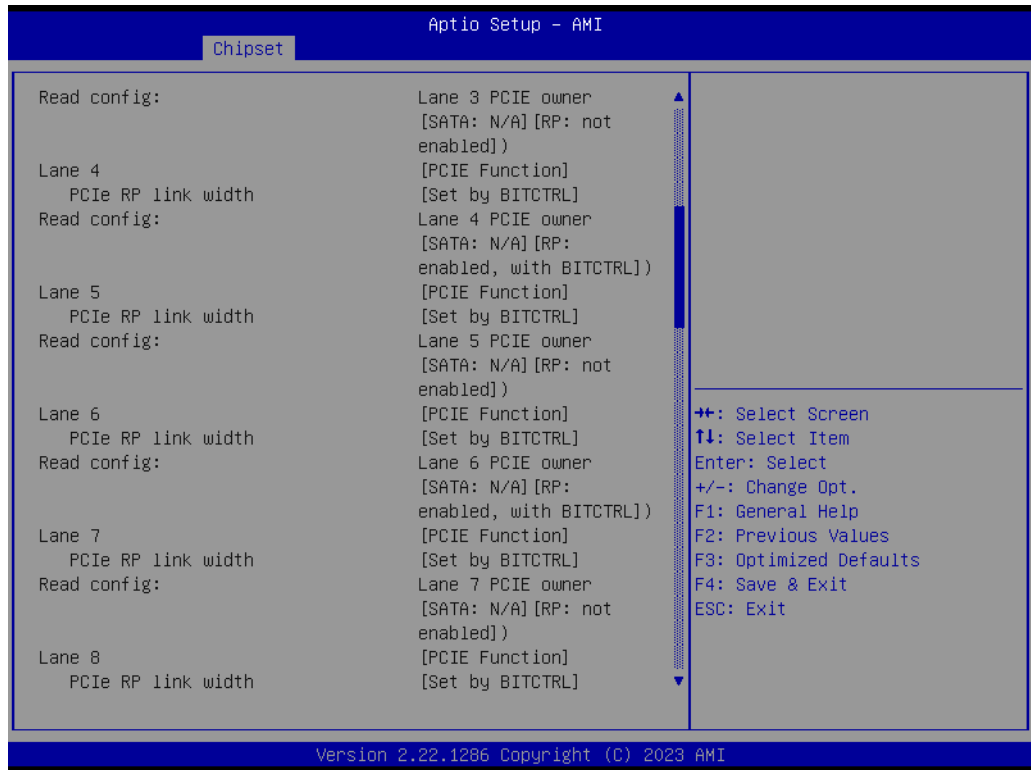
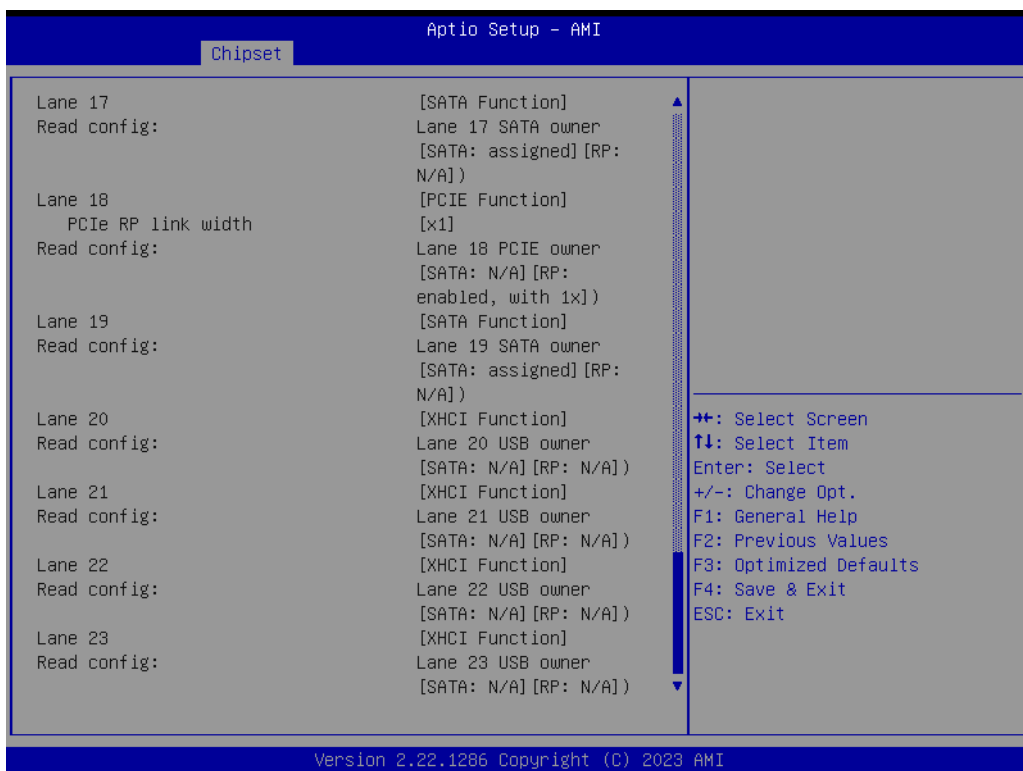
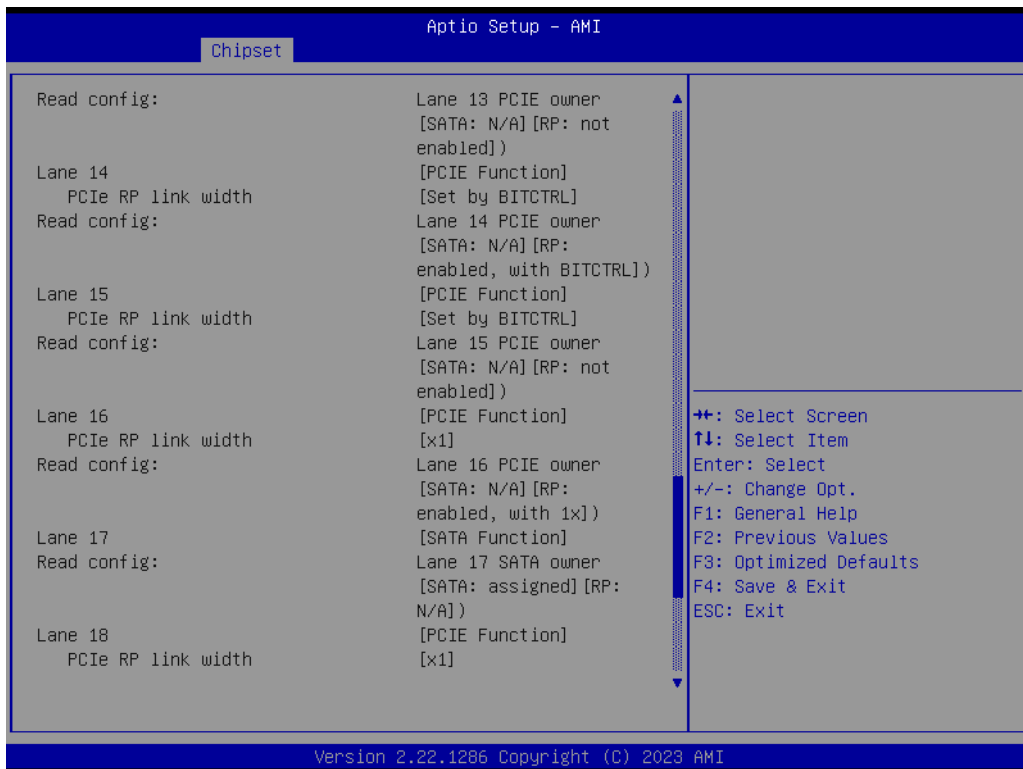


Figure 3.73 Fia Mux Configuration

- **Pcie 0 Bifurcation**
Allow changing PCIE bifurcation.
- **Pcie 1 Bifurcation**
Allow changing PCIE bifurcation.
- **Pcie 2 Bifurcation**
Allow changing PCIE bifurcation.
- **FIA Mux Configuration Override**
By Enabling this you override the platform configuration on FIA/WM.





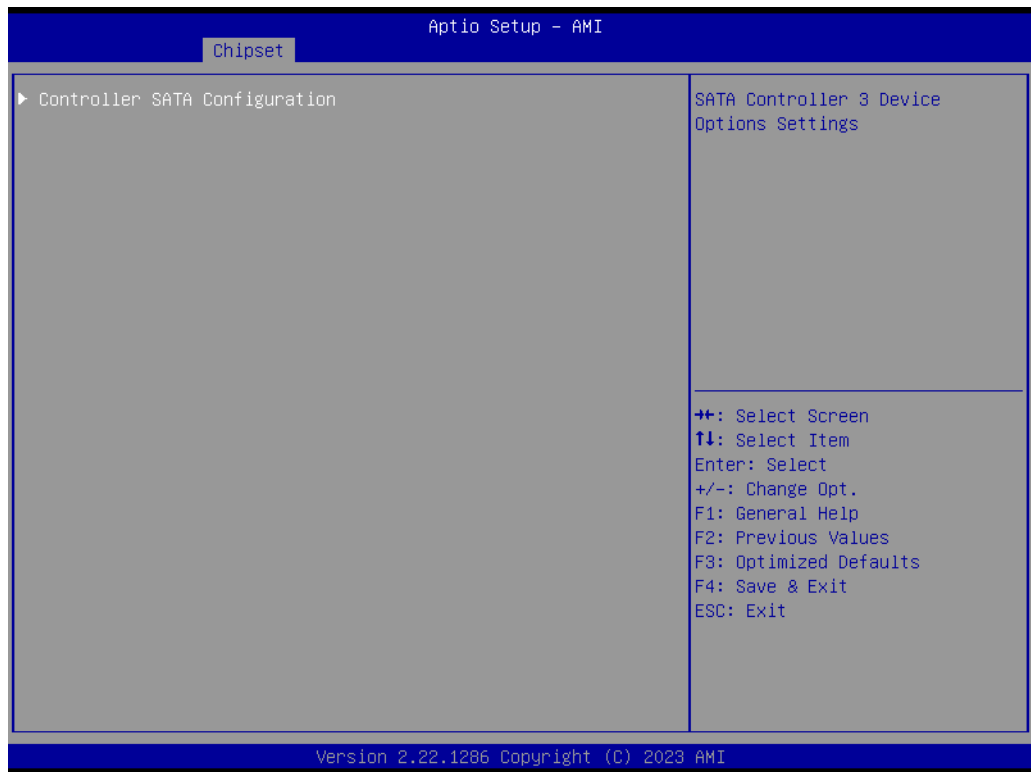


Figure 3.74 SATA Configuration

- **Controller SATA Configuration**
SATA Controller 3 Device Options Settings.



Figure 3.75 Controller SATA Configuration

- **SATA Configuration**
SATA test Settings.
- **SATA Controller Speed**
Indicates the maximum speed the SATA controller can support.
- **Aggressive LPM Support**
Enable PCH to aggressively enter link power state.
- **Port 0**
Enable or Disable SATA Port.
DH5000 Mapping:SATA1.
- **Port 1**
Enable or Disable SATA Port.
DH5000 Mapping:SATA2.

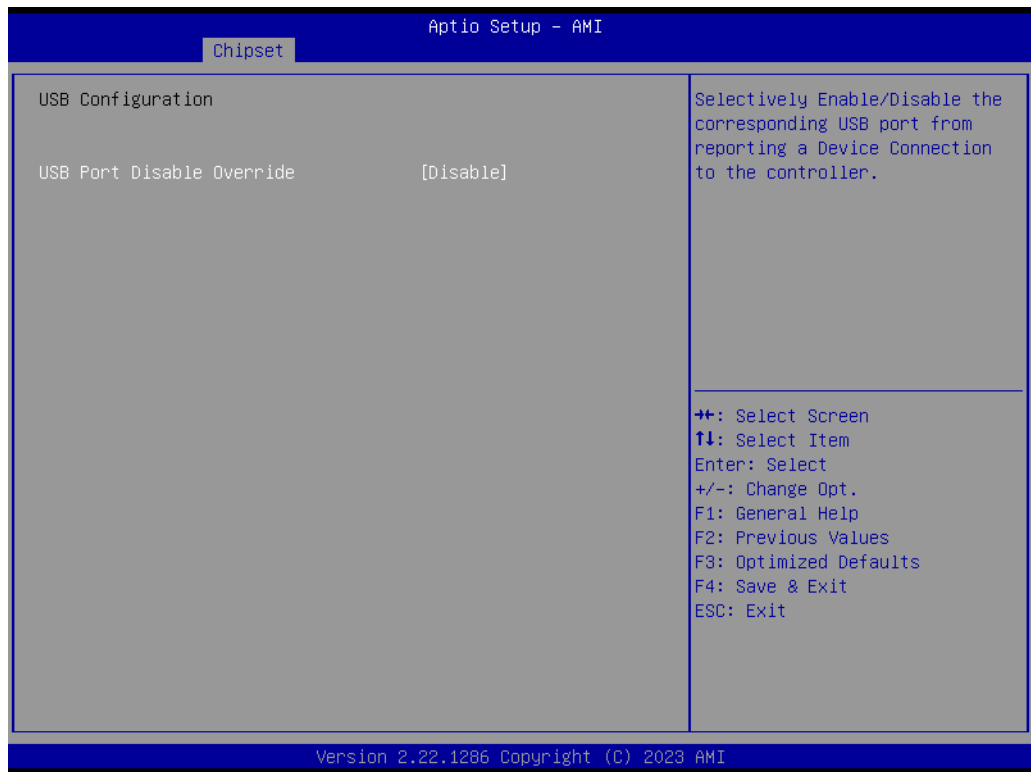


Figure 3.76 USB Configuration

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

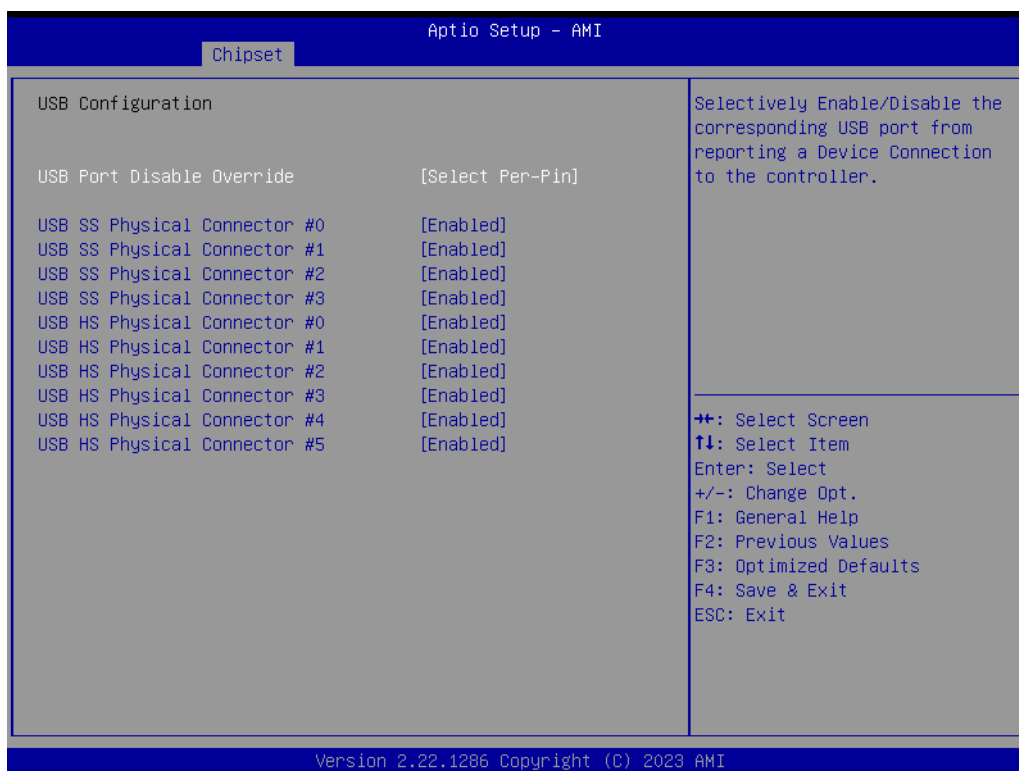


Figure 3.77 USB Configuration

- **USB Port Disable Override**
Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
- **USB SS Physical Connector #0**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB SS Physical Connector #1**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB SS Physical Connector #2**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB SS Physical Connector #3**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB HS Physical Connector #0**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB HS Physical Connector #1**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.

- **USB HS Physical Connector #2**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB HS Physical Connector #3**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB HS Physical Connector #4**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.
- **USB HS Physical Connector #5**
Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plugged into the connector will not be detected by the BIOS or OS.

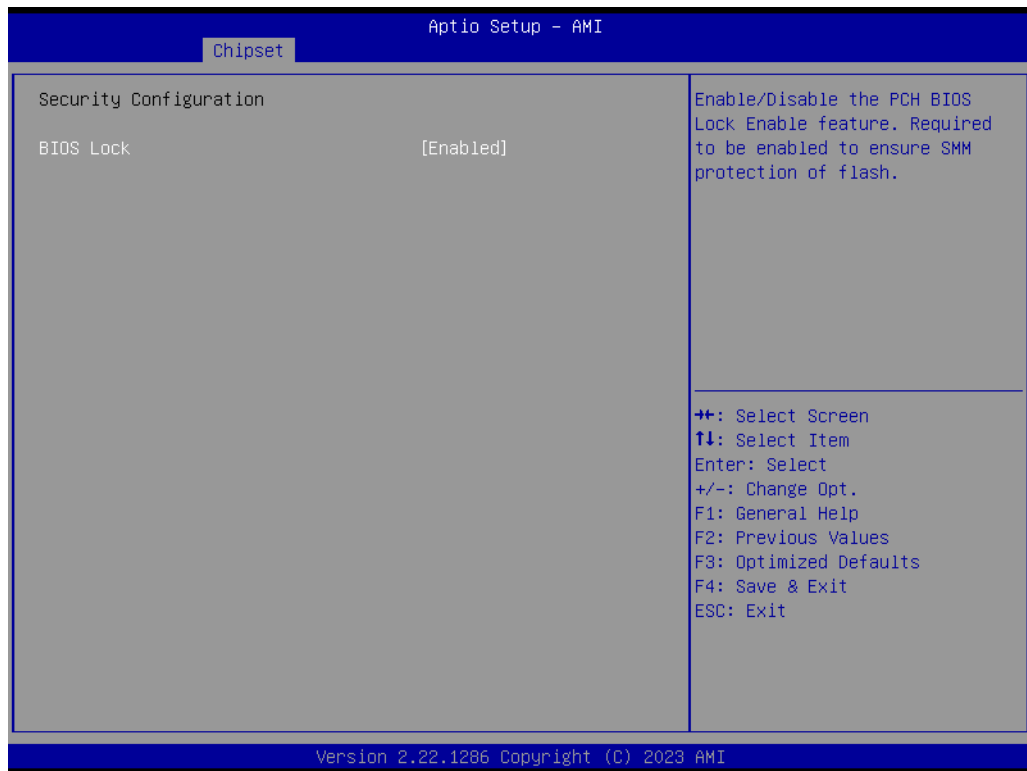


Figure 3.78 Security Configuration

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

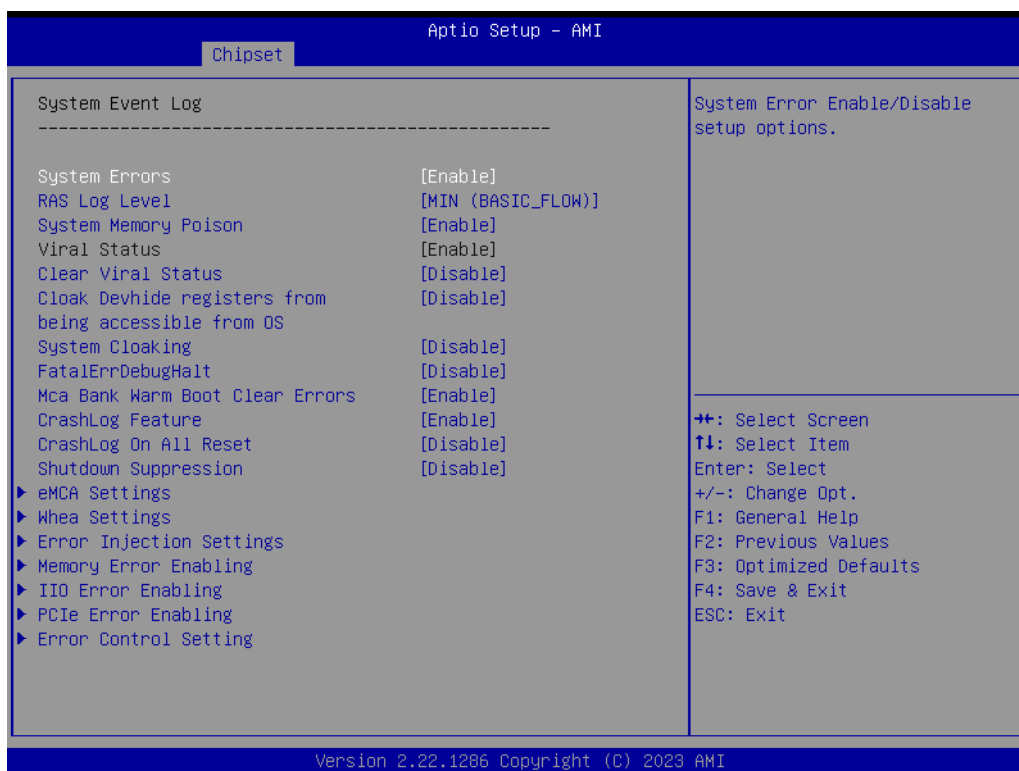


Figure 3.79 System Event Log

- **System Errors**
System Error Enable/Disable setup options.
- **RAS Log Level**
RAS Log setup options.
- **System Memory Poison**
Enable/Disable System Memory Poison.
- **Viral Status**
- **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 collect crash data from PMC SSRAM.
- **CrashLog On All Reset**
Option to invoke CrashLog collection on all reset.
- **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.

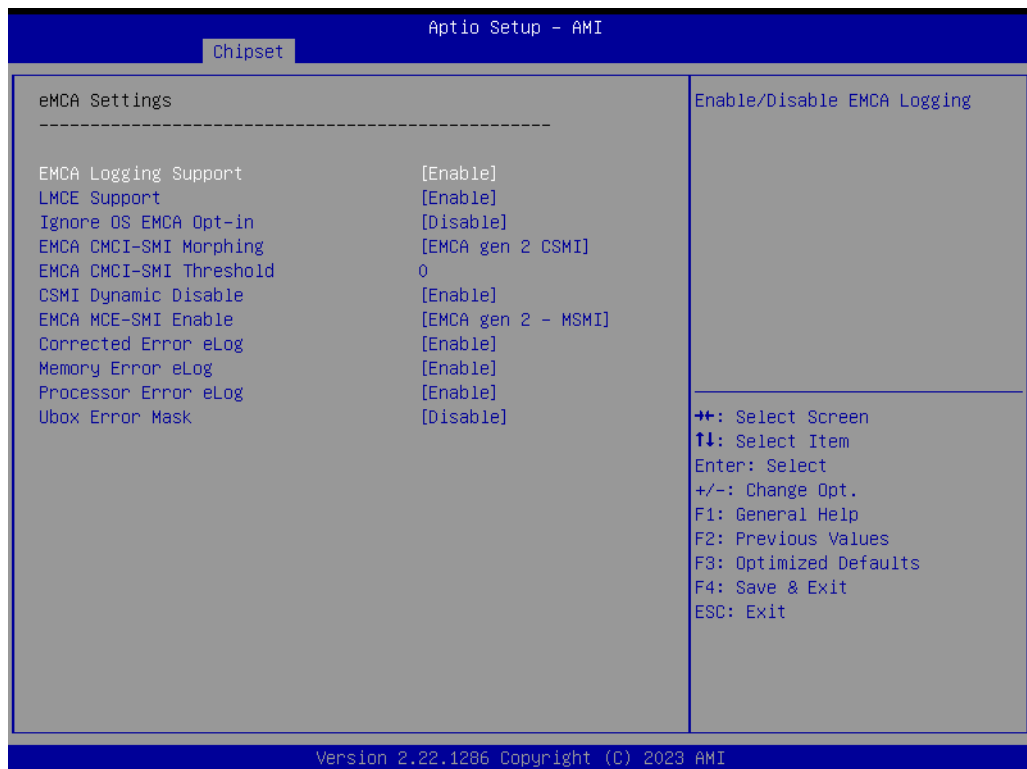


Figure 3.80 eMCA Settings

- **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 the error threshold is reached.
- **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.

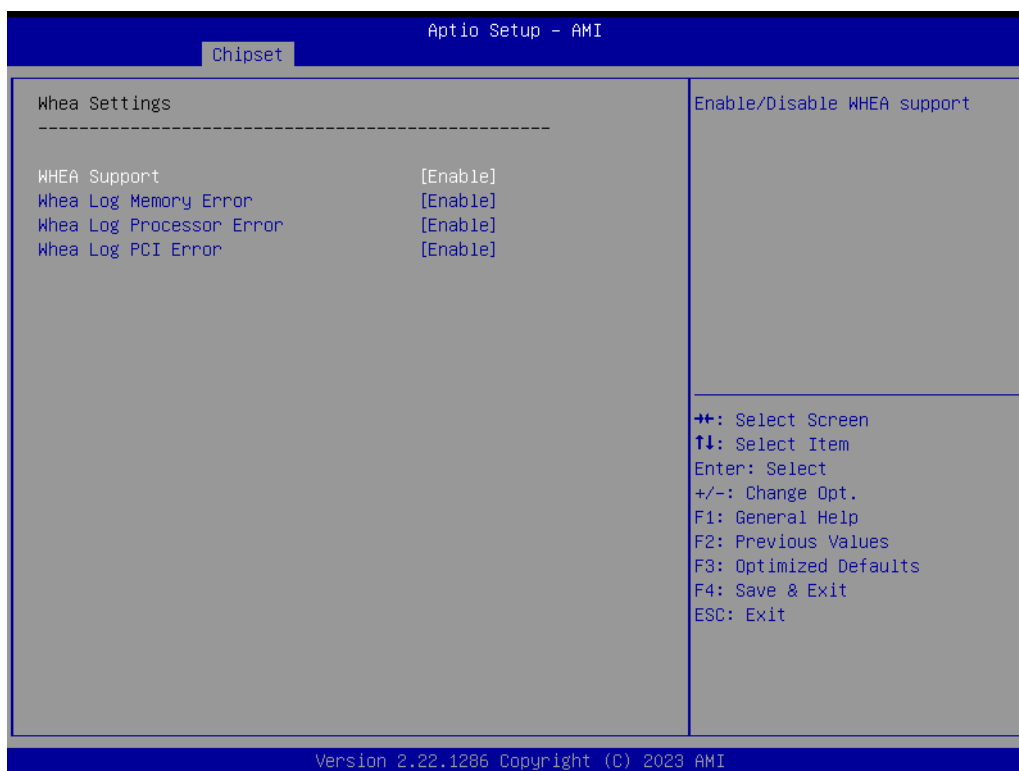


Figure 3.81 Whea Settings

- **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.

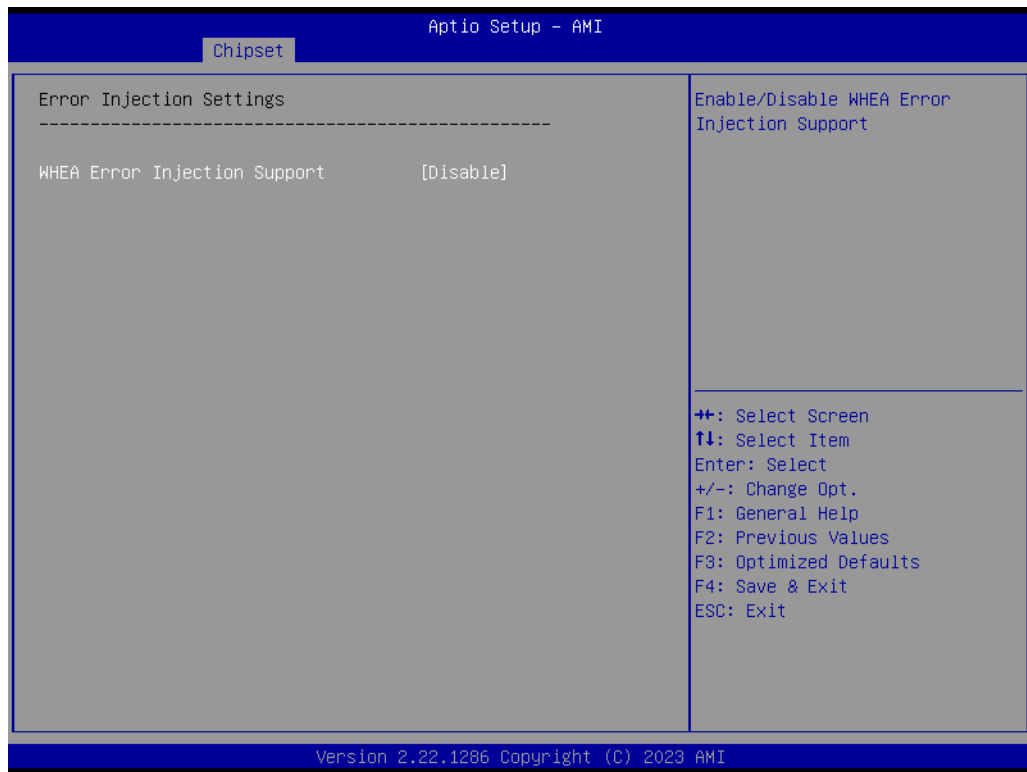


Figure 3.82 Error Injection Settings

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

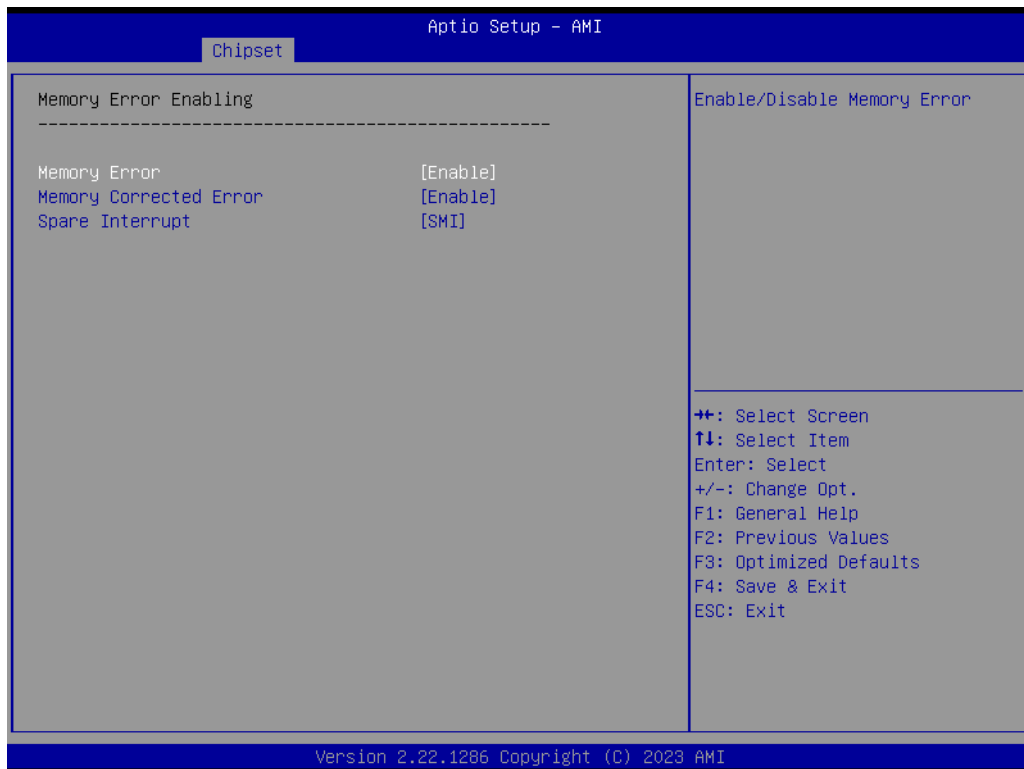


Figure 3.83 Memory Error Enabling

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

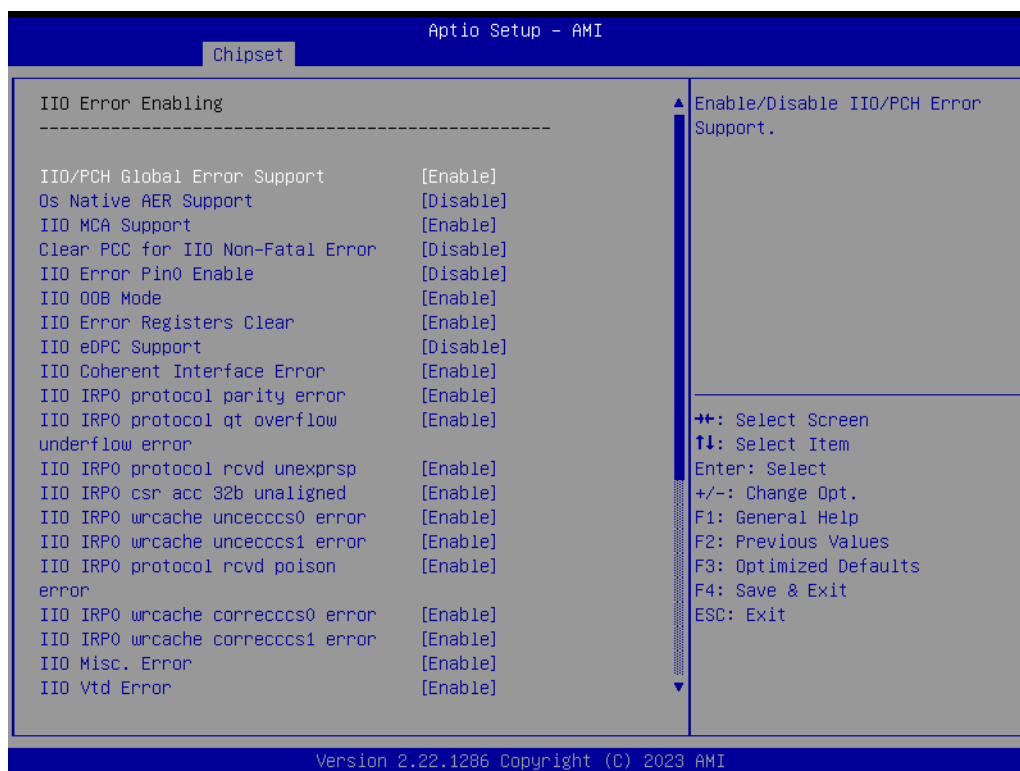


Figure 3.84 IIO Error Enabling

- **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 OS native is selected, the BIOS will also initialize 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 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/Disable IIO Coherent Interface protocol queue table overflow or underflow error reporting.
- **IIO IRP0 protocol rcvd unexprsp**
Enable/Disable IIO Coherent Interface protocol layer received unexpected response or completion error reporting.

- **IIO IRP0 csr acc 32b unaligned**
Enable/Disable IIO Coherent Interface CSR Access Crossing 32-bit Boundary error reporting.
- **IIO IRP0 wrcache uncecccs0 error**
Enable/Disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
- **IIO IRP0 wrcache uncecccs1 error**
Enable/Disable IIO Coherent Interface Write Cache Un-correctable ECC error reporting.
- **IIO IRP0 protocol rcvd poison error**
Enable/Disable IIO Coherent Interface Protocol Layer Received Poisoned Packet error reporting.
- **IIO IRP0 wrcache correcccs0 error**
Enable/Disable IIO Coherent Interface Write Cache Correctable ECC error reporting.
- **IIO IRP0 wrcache correcccs1 error**
Enable/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.



Figure 3.85 IIO Error Enabling

- **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.

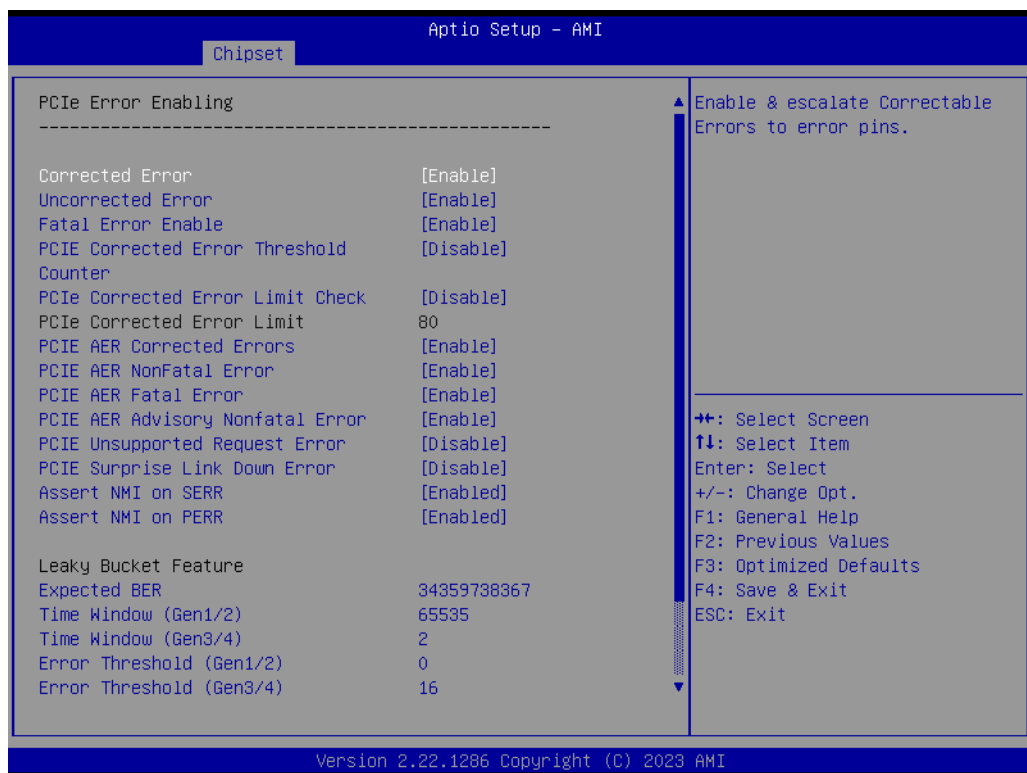


Figure 3.86 PCIe Error Enabling

- **Corrected Error**
Enable & escalate Correctable Errors to error pins.
- **Uncorrected Error**
Enable & escalate Uncorrectable/Recoverable to error pins.
- **Fatal Error Enable**
Enable & escalate fatal errors to error pins.
- **PCIE Corrected Error Threshold Counter**
Enable/Disable PCIE Corrected Error 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 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.

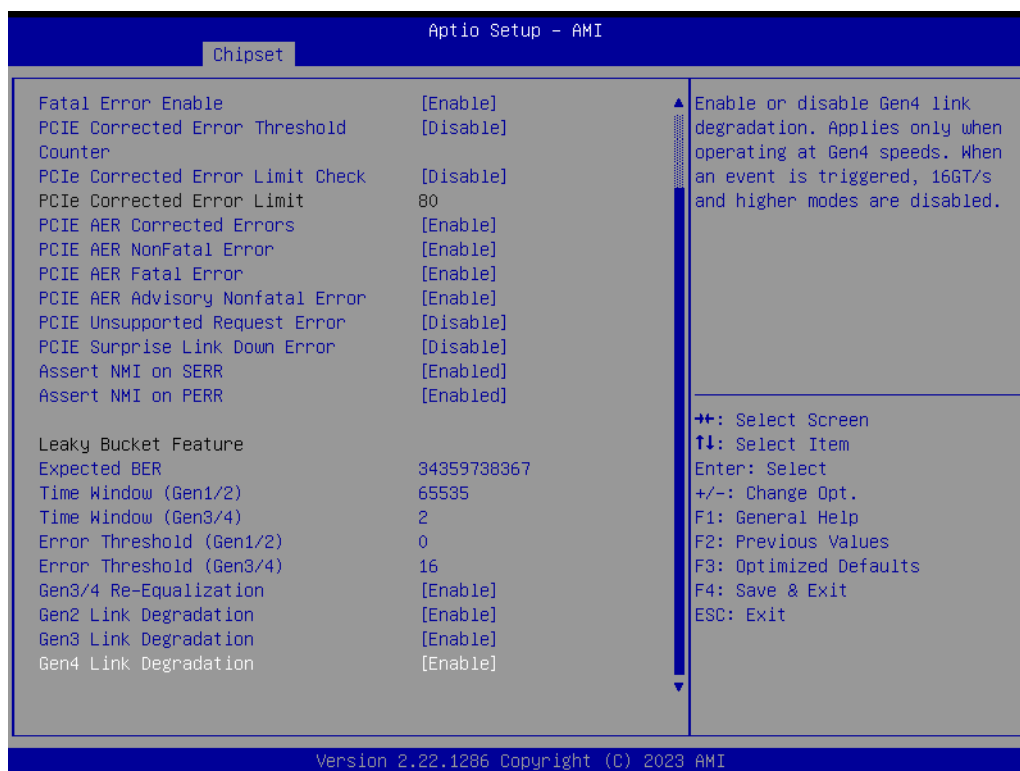


Figure 3.87 PCIe Error Enabling

- **Gen3/4 Re-Equalization**
Enable/Disable Gen3 and Gen4 re-equalization. This applies only when operating at Gen2 or Gen4 speeds. When an event is triggered, equalization is re-run.
- **Gen2 Link Degradation**
Enable/Disable Gen2 link degradation. This applies only when operating at Gen2 speeds. When an event is triggered, 5GT/s and higher modes are disabled.
- **Gen3 Link Degradation**
Enable/Disable Gen3 link degradation. This applies only when operating at Gen3 speeds. When an event is triggered, 8GT/s and higher modes are disabled.
- **Gen4 Link Degradation**
Enable/Disable Gen4 link degradation. This applies only when operating at Gen4 speeds. When an event is triggered, 16GT/s and higher modes are disabled.



Figure 3.88 Error Control Setting

- **Latch First Corrected Error in KTI**
Enable/Disable latch first corrected error in KTI.
- **Patrol Scrub Error Reporting**
Patrol Scrub Error type selection.

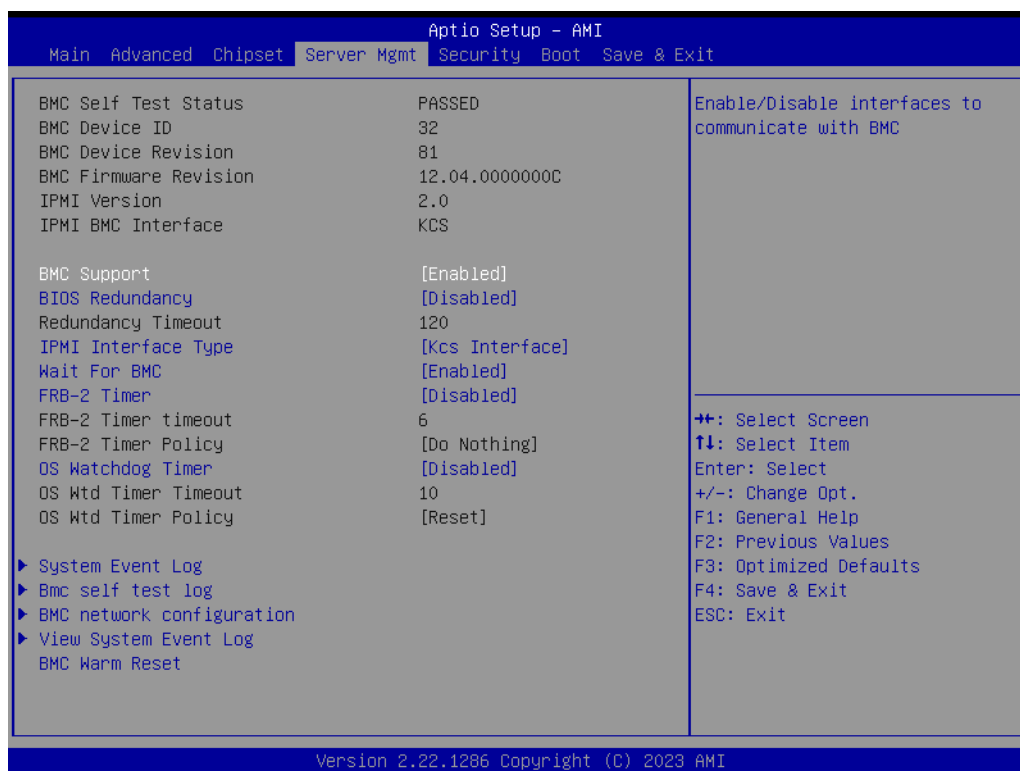
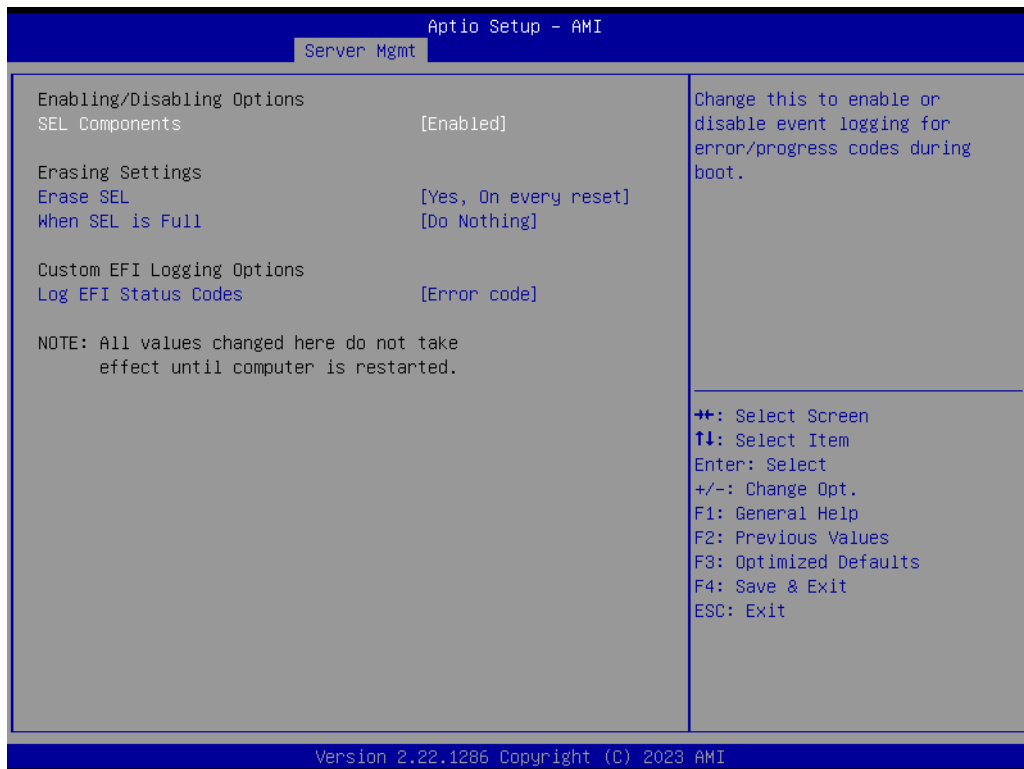
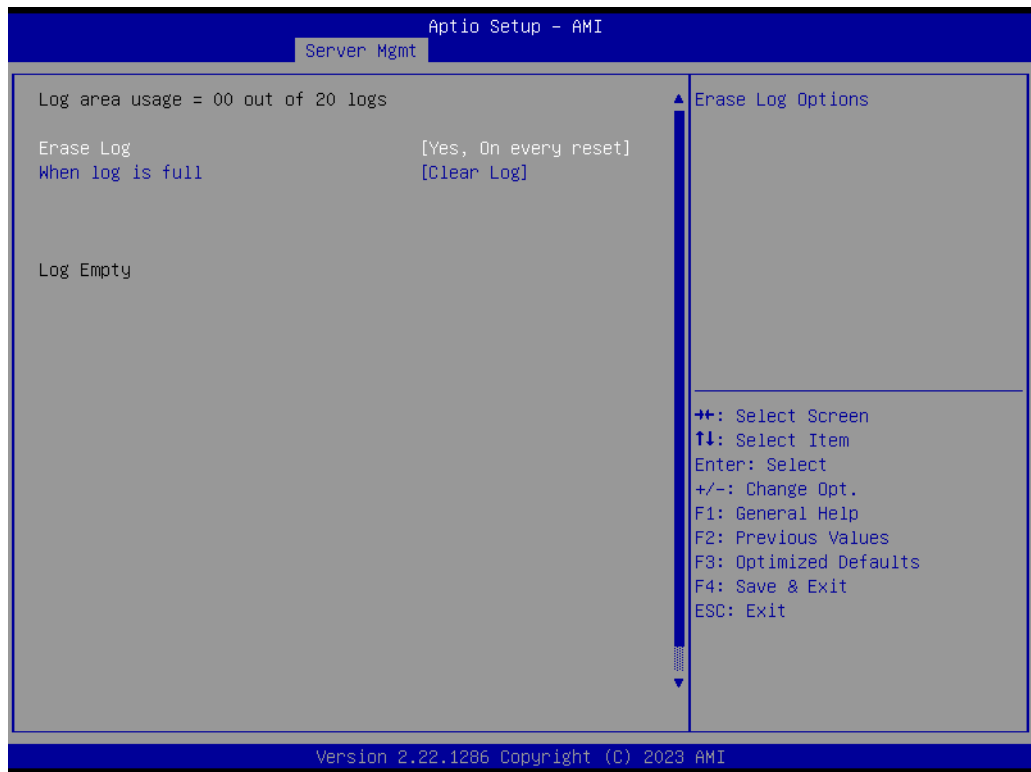


Figure 3.89 Server Mgmt

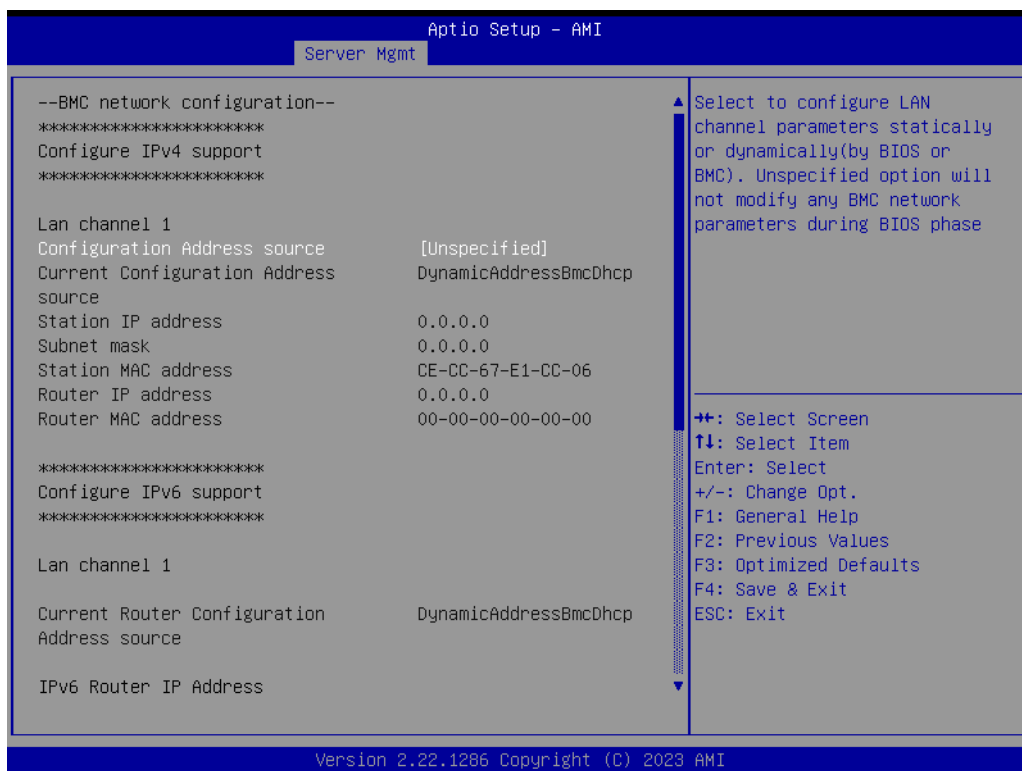
- **BMC Support**
Enable/Disable interfaces to communicate with BMC.
- **BIOS Redundancy**
Enable/Disable the BIOS Redundancy feature.
- **IPMI Interface Type**
Type of Interface to communicate BMC from HOST.
- **Wait For BMC**
Wait For BMC response for specified time out. In ASPEED 2500 ESPI mode, BMC starts at the same time when BIOS starts during AC power ON. It takes around 60 seconds to initialize Host to BMC interfaces.
- **FRB-2 Timer**
Enable/Disable FRB-2 timer (POST timer).
- **OS Watchdog Timer**
If enabled, it starts a BIOS timer which can only be shut off by Management Software after the OS loads. It helps determine if the OS successfully loaded or follows the OS Boot Watchdog Timer policy.
- **System Event Log**
Press <Enter> to change the SEL event log configuration.
- **Bmc self test log**
Logs the report returned by the BMC self test command.
- **BMC network configuration**
Configure BMC network parameters.
- **View System Event Log**
Press <Enter> to view the System Event Log Records.
- **BMC Warm Reset**
Press <Enter> to do a BMC Warm Reset.



- **SEL Components**
Change this to enable or disable event logging for error/progress codes during bootup.
- **Erase SEL**
Choose options for erasing SEL.
- **When SEL is Full**
Choose options for reactions to a full SEL.
- **Log EFI Status Codes**
Disable the logging of EFI Status Codes or log only the error code, only the progress code, or both.

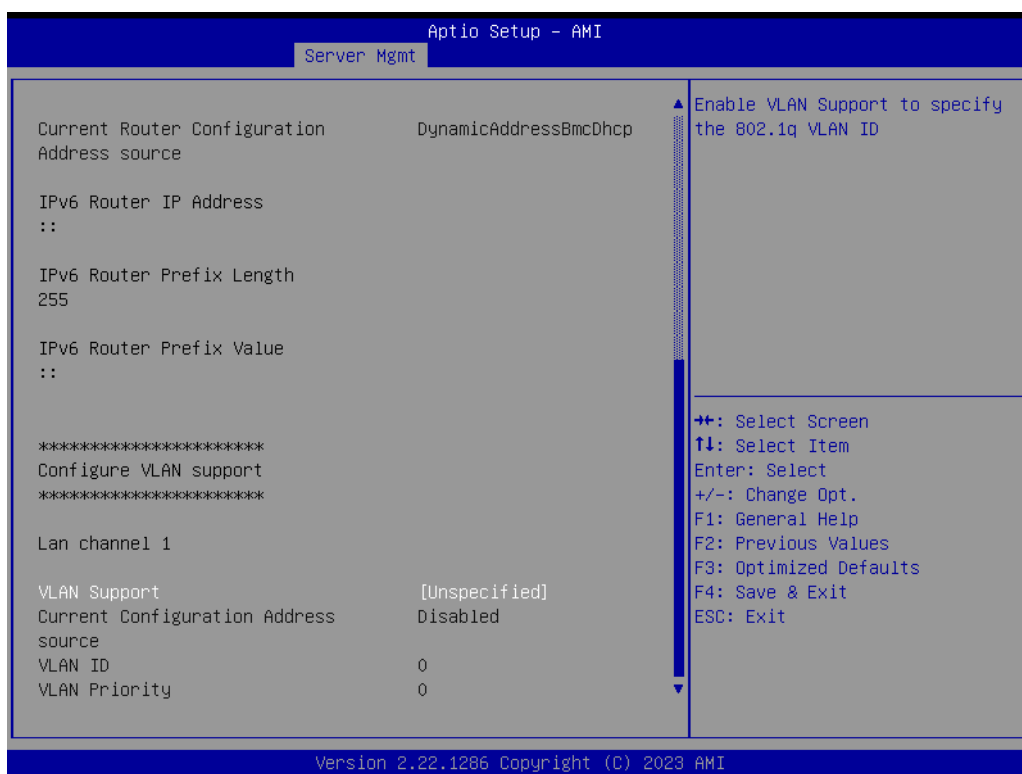


- **Erase Log**
Erase Log Options.
- **When log is full**
Select the action to be taken when the log is full.



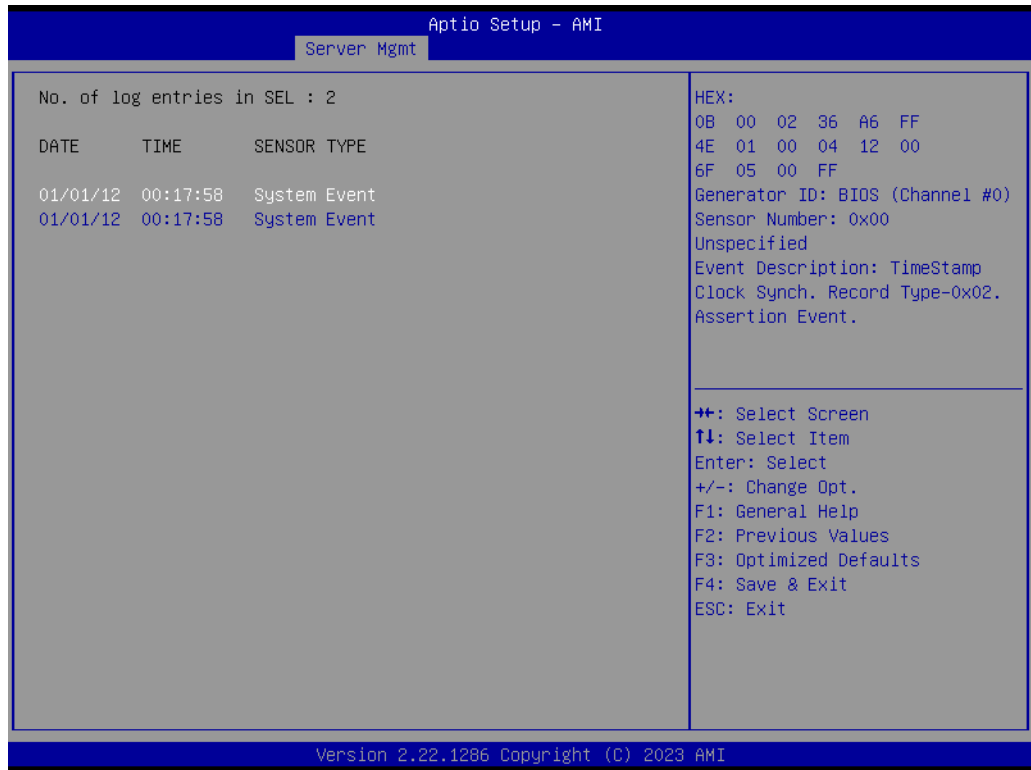
■ SEL Components

Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). The Unspecified option will not modify any BMC network parameters during the BIOS phase.



■ VLAN Support

Enable VLAN Support to specify the 802.1q VLAN ID.



- **01/01/12 00:17:58 System Event**
 HEX:
 0B 00 02 36 A6 FF
 4E 01 00 04 12 00
 6F 05 00 FF
 Generator ID: BIOS (Channel #0)
 Sensor Number: 0x00
 Unspecified Event Description: TimeStamp Clock Synch. Record Type-0x02.
 Assertion Event.
- **01/01/12 00:17:58 System Event**
 HEX:
 0B 00 02 36 A6 FF
 4E 01 00 04 12 00
 6F 05 00 FF
 Generator ID: BIOS (Channel #0)
 Sensor Number: 0x00
 Unspecified Event Description: TimeStamp Clock Synch. Record Type-0x02.
 Assertion Event.

3.2.3 Security Chipset

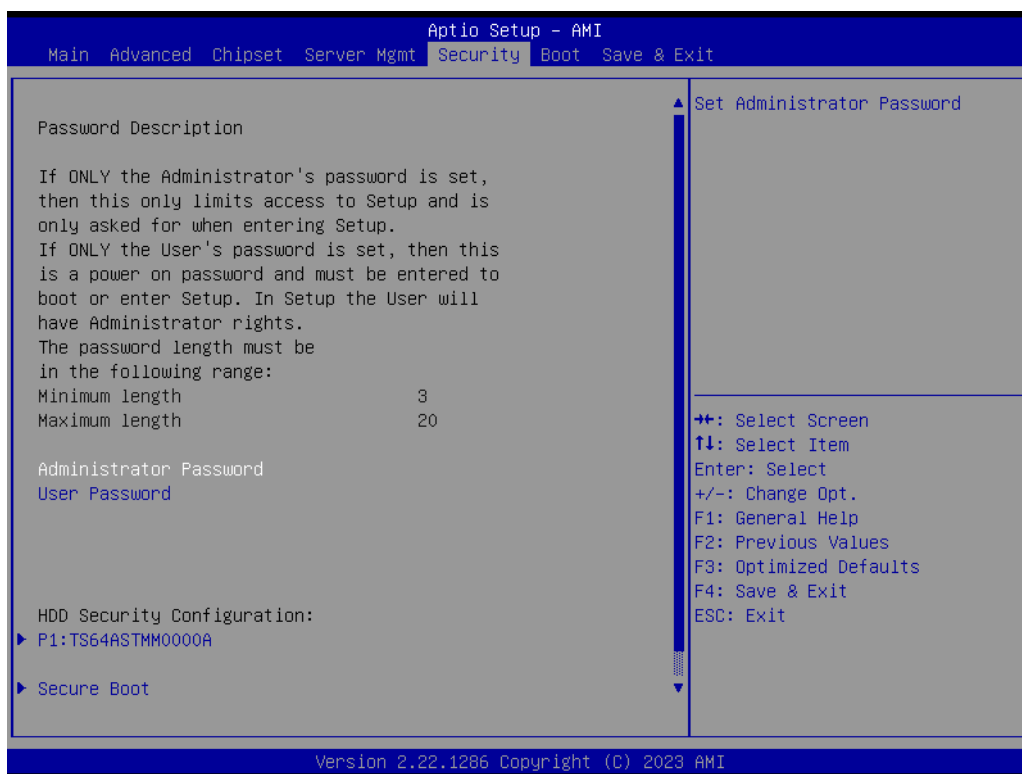
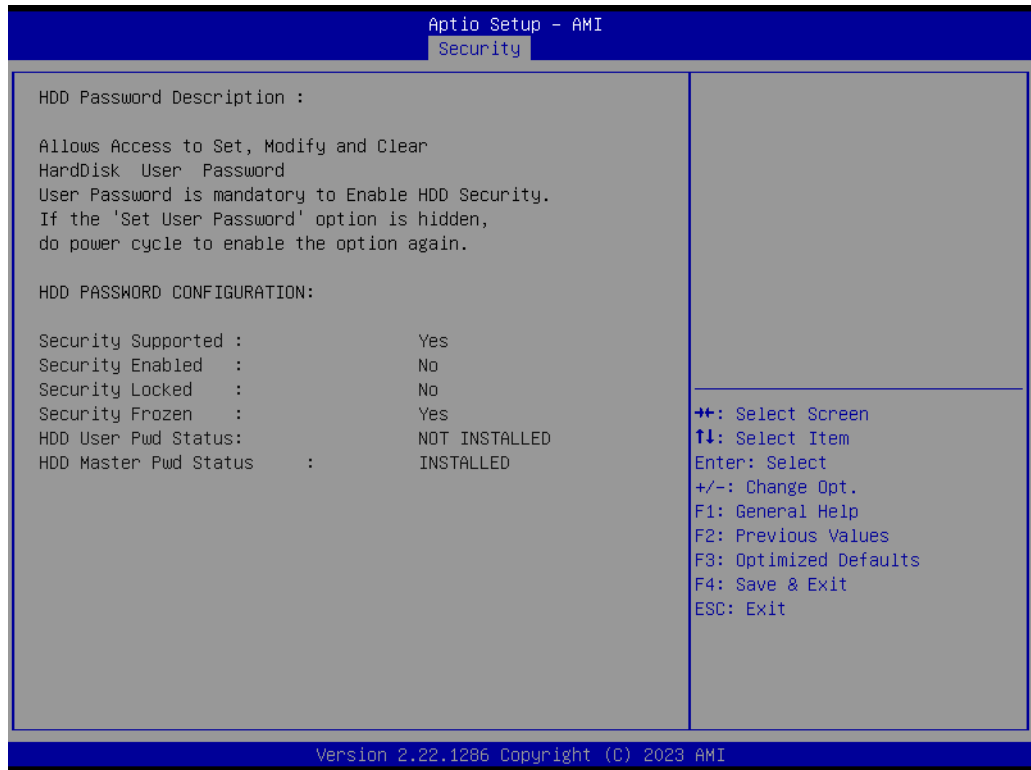


Figure 3.90 Security Chipset

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



3.2.3.1 Secure Boot

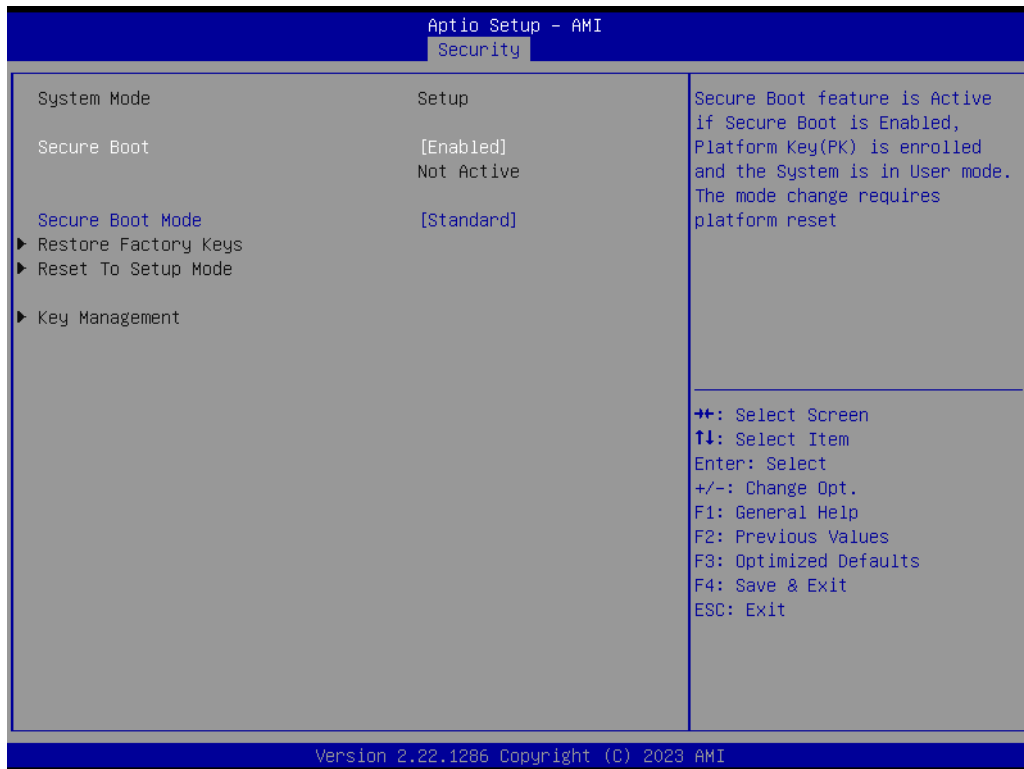


Figure 3.91 Secure Boot

- **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.

3.2.3.2 Boot Setup



Figure 3.92 Boot Setup

- **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/Disables the Quiet Boot option.
- **Boot Option #1**
Sets the system boot order.

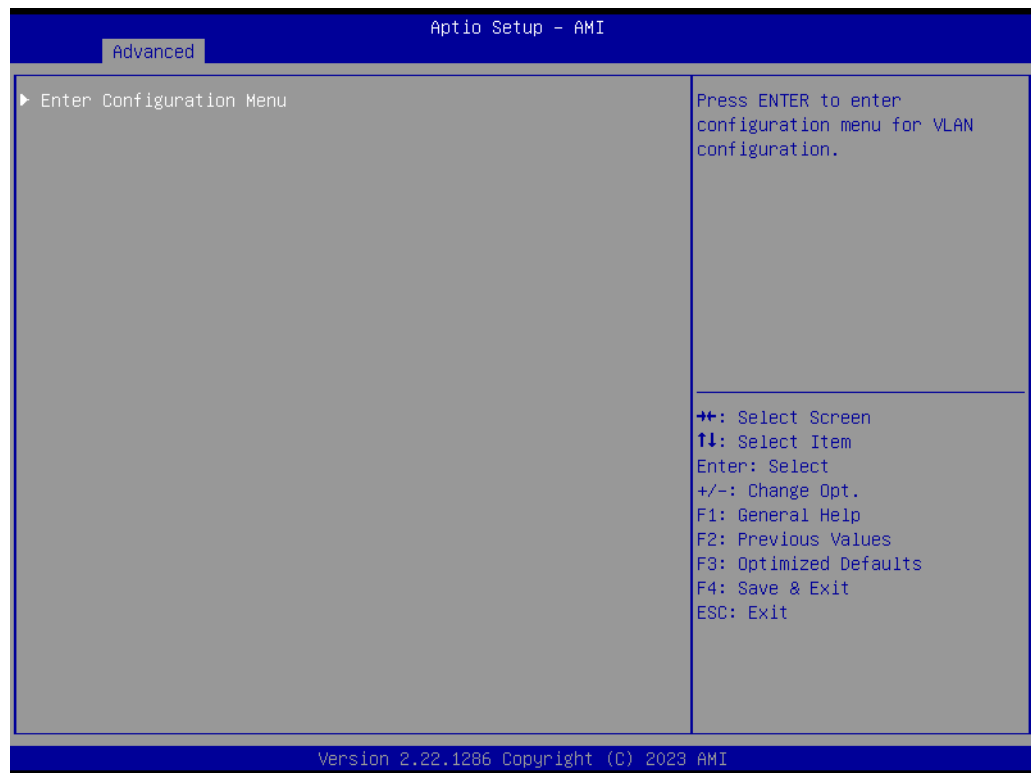
3.2.4 Save & Exit



Figure 3.93 Save & Exit

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

3.2.5 MEBx Login



- **Intel® ME Password**
MEBx Login.

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.

4.2.1 Windows Driver Setup

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











4.2.2 Other OS

Linux Ubuntu.

4.3 Advantech iManager

Advantech'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 information. All the embedded functions are configured through the API and provide corresponding utilities to demonstrate. These APIs comply with PICMG EAPI (Embedded Application Programmable Interface) specifications and make these embedded features easier to integrate, speed development schedules, and provide customers with software continuity while upgrading hardware. For more details on how to use the APIs and utilities, please refer to the Advantech iManager 2.0 Software API User Manual.

Control	Monitor
 <p>GPIO</p> <p>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.</p>	 <p>Watchdog</p> <p>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.</p>
 <p>SMBus</p> <p>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.</p>	 <p>Hardware Monitor</p> <p>The Hardware Monitor (HWM) API is a system health supervision API that inspects certain condition indexes, such as fan speed, temperature and voltage.</p>
 <p>I2C</p> <p>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.</p>	 <p>Hardware Control</p> <p>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.</p>
Display	Power Saving
 <p>Brightness Control</p> <p>The Brightness Control API allows a developer to interface with an embedded device to easily control brightness.</p>	 <p>CPU Speed</p> <p>Make use of Intel SpeedStep technology to reduce power power consumption. The system will automatically adjust the CPU Speed depending on system loading.</p>
 <p>Backlight</p> <p>The Backlight API allows a developer to control the backlight (screen) on/off in an embedded device.</p>	 <p>System Throttling</p> <p>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 67.5% to 12.5%.</p>

Appendix **A**

Pin Assignment

This appendix details information about the hardware pin assignments of the SOM-D580 CPU Computer-on-Module.

Sections include:

- SOM-D580 Client Size Pin Assignment

A.1 SOM-D580 Pin Assignment

This section gives SOM-D580 pin assignments on the COM HPC connector, which are compliant with COM-HPC Revision 1.10 Client Type pin-out definitions. For more details about how to use these pins and to obtain a design reference, please contact Advantech for a design guide, checklist, reference schematic, and other hardware/software support.

Table A.1: J1 Connector Rows A and B

Pin#	Row A Description	SOM-D580 Difference	Pin#	Row B Description	SOM-D580 Difference
J1.A1	VCC	+VIN_12V	J1.B1	VCC	
J1.A2	VCC	+VIN_12V	J1.B2	PWRBTN#	
J1.A3	VCC	+VIN_12V	J1.B3	VCC	
J1.A4	VCC	+VIN_12V	J1.B4	THERMTRIP#	
J1.A5	VCC	+VIN_12V	J1.B5	VCC	
J1.A6	VCC	+VIN_12V	J1.B6	TAMPER#	
J1.A7	VCC	+VIN_12V	J1.B7	VCC	
J1.A8	VCC	+VIN_12V	J1.B8	SUS_S3#	
J1.A9	VCC	+VIN_12V	J1.B9	VCC	
J1.A10	GND	GND	J1.B10	WD_STROBE#	
J1.A11	BATLOW#	PM_BATLOW#	J1.B11	WD_OUT	
J1.A12	PLTRST#	PLTRST_CB#	J1.B12	GND	
J1.A13	GND	GND	J1.B13	USB5-	
J1.A14	USB7-	USB20_BMC_D-	J1.B14	USB5+	
J1.A15	USB7+	USB20_B-MC_D+	J1.B15	GND	
J1.A16	GND	GND	J1.B16	USB4-	
J1.A17	USB6-	NC	J1.B17	USB4+	
J1.A18	USB6+	NC	J1.B18	GND	
J1.A19	GND	GND	J1.B19	I2S_LRCLK/ SNDW_CLK3/ HDA_SYNC	
J1.A20	ETH4_RX-	LAN_KR_RX4-	J1.B20	I2S_DOUT/ SNDW_DAT3/ HDA_SDO	
J1.A21	ETH4_RX+	LAN_KR_RX4+	J1.B21	I2S_MCLK/ HDA_RST	
J1.A22	GND	GND	J1.B22	I2S_DIN/ SNDW_DAT2/ HDA_SDI	
J1.A23	ETH5_RX-	LAN_KR_RX5-	J1.B23	I2S_CLK/ SNDW_CLK2/ HDA_BCLK	
J1.A24	ETH5_RX+	LAN_KR_RX5+	J1.B24	VCC_5V_SBY	
J1.A25	GND	GND	J1.B25	USB67_OC#	
J1.A26	ETH6_RX-	LAN_KR_RX6-	J1.B26	USB45_OC#	
J1.A27	ETH6_RX+	LAN_KR_RX6+	J1.B27	USB23_OC#	
J1.A28	GND	GND	J1.B28	USB01_OC#	
J1.A29	ETH7_RX-	LAN_KR_RX7-	J1.B29	SML1_CLK	

Table A.1: J1 Connector Rows A and B

J1.A30	ETH7_RX+	LAN_KR_RX7+	J1.B30	SML1_DAT	
J1.A31	GND	GND	J1.B31	PMCALERT#	
J1.A32	RSVD	NC	J1.B32	SML0_CLK	
J1.A33	RSVD	NC	J1.B33	SML0_DAT	
J1.A34	GND		J1.B34	USB_P-D_ALERT#	NC
J1.A35	ETH4_TX-		J1.B35	USB_PD_I2C_-CLK	CB_SML0_CLK
J1.A36	ETH4_TX+		J1.B36	USB_PD_I2C_-DAT	CB_SML0_DAT
J1.A37	GND		J1.B37	USB_RT_ENA	NC
J1.A38	ETH5_TX-		J1.B38	USB1_LSRX	PD
J1.A39	ETH5_TX+		J1.B39	USB1_LSTX	PD
J1.A40	GND		J1.B40	USB0_LSRX	PD
J1.A41	ETH6_TX-		J1.B41	USB0_LSTX	PD
J1.A42	ETH6_TX+		J1.B42	GND	
J1.A43	GND		J1.B43	USB0_AUX-	NC
J1.A44	ETH7_TX-		J1.B44	USB0_AUX+	NC
J1.A45	ETH7_TX+		J1.B45	RSVD	
J1.A46	GND		J1.B46	RSVD	EC_ESPI_CS#
J1.A47	USB1_AUX-	NC	J1.B47	VCC_BOOT_SPI	
J1.A48	USB1_AUX+	NC	J1.B48	BOOT_SPI_CS#	
J1.A49	GND		J1.B49	BSEL0	
J1.A50	eSPI_IO0		J1.B50	BSEL1	
J1.A51	eSPI_IO1		J1.B51	BSEL2	
J1.A52	eSPI_IO2		J1.B52	eSPI_ALERT0#	
J1.A53	eSPI_IO3		J1.B53	eSPI_ALERT1#	NC
J1.A54	eSPI_CLK		J1.B54	eSPI_CS0#	
J1.A55	GND		J1.B55	eSPI_CS1#	NC
J1.A56	PCIe_-CLKREQ0_LO#		J1.B56	eSPI_RST#	
J1.A57	PCIe_-CLKREQ0_HI#		J1.B57	GND	
J1.A58	GND		J1.B58	PCIe_BMC_RX-	
J1.A59	PCIe_BMC_TX-		J1.B59	PCIe_BMC_RX+	
J1.A60	PCIe_BMC_TX+		J1.B60	GND	
J1.A61	GND		J1.B61	PCIe08_RX-	
J1.A62	PCIe08_TX-		J1.B62	PCIe08_RX+	
J1.A63	PCIe08_TX+		J1.B63	GND	
J1.A64	GND		J1.B64	PCIe09_RX-	
J1.A65	PCIe09_TX-		J1.B65	PCIe09_RX+	
J1.A66	PCIe09_TX+		J1.B66	GND	
J1.A67	GND		J1.B67	PCIe10_RX-	
J1.A68	PCIe010_TX-		J1.B68	PCIe10_RX+	
J1.A69	PCIe010_TX+		J1.B69	GND	
J1.A70	GND		J1.B70	PCIe11_RX-	
J1.A71	PCIe11_TX-		J1.B71	PCIe11_RX+	
J1.A72	PCIe11_TX+		J1.B72	GND	

Table A.1: J1 Connector Rows A and B

J1.A73	GND	J1.B73	PCle12_RX-
J1.A74	PCle12_TX-	J1.B74	PCle12_RX+
J1.A75	PCle12_TX+	J1.B75	GND
J1.A76	GND	J1.B76	PCle13_RX-
J1.A77	PCle13_TX-	J1.B77	PCle13_RX+
J1.A78	PCle13_TX+	J1.B78	GND
J1.A79	GND	J1.B79	PCle14_RX-
J1.A80	PCle14_TX-	J1.B80	PCle14_RX+
J1.A81	PCle14_TX+	J1.B81	GND
J1.A82	GND	J1.B82	PCle15_RX-
J1.A83	PCle15_TX-	J1.B83	PCle15_RX+
J1.A84	PCle15_TX+	J1.B84	GND
J1.A85	GND	J1.B85	TEST# PU
J1.A86	VCC_RTC	J1.B86	RSMRST_OUT#
J1.A87	SUS_CLK	J1.B87	UART1_TX
J1.A88	GPIO_00	J1.B88	UART1_RX
J1.A89	GPIO_01	J1.B89	UART1_RTS#
J1.A90	GPIO_02	J1.B90	UART1_CTS#
J1.A91	GPIO_03	J1.B91	IPMB_CLK
J1.A92	GPIO_04	J1.B92	IPMB_DAT
J1.A93	GPIO_05	J1.B93	GP_SPI_MOSI NC
J1.A94	GPIO_06	J1.B94	GP_SPI_MISO NC
J1.A95	GPIO_07	J1.B95	GP_SPI_CS0# NC
J1.A96	GPIO_08	J1.B96	GP_SPI_CS1# NC
J1.A97	GPIO_09	J1.B97	GP_SPI_CS2# NC
J1.A98	GPIO_10	J1.B98	GP_SPI_CS3# NC
J1.A99	GPIO_11	J1.B99	GP_SPI_CLK NC
J1.A100	TYPE0 GND	J1.B100	GP_SPI_ALERT# NC

Table A.2: J1 Connector Rows C and D

Pin#	Row C Description	SOM-D580 Difference	Pin#	Row D Description	SOM-D580 Difference
J1.C1	VCC		J1.D1	VCC	
J1.C2	RSTBTN#		J1.D2	VCC	
J1.C3	VCC		J1.D3	VCC	
J1.C4	CARRIER_HOT#		J1.D4	VCC	
J1.C5	VCC		J1.D5	VCC	
J1.C6	VIN_PWROK		J1.D6	VCC	
J1.C7	VCC		J1.D7	VCC	
J1.C8	SUS_S4_S5#		J1.D8	VCC	
J1.C9	VCC		J1.D9	VCC	
J1.C10	GND		J1.D10	WAKE0#	
J1.C11	FAN_PWMOUT		J1.D11	WAKE1#	
J1.C12	FAN_TACHIN		J1.D12	GND	
J1.C13	GND		J1.D13	USB1-	
J1.C14	USB3-		J1.D14	USB1+	
J1.C15	USB3+		J1.D15	GND	
J1.C16	GND		J1.D16	USB0-	
J1.C17	USB2-		J1.D17	USB0+	
J1.C18	USB2+		J1.D18	GND	
J1.C19	GND		J1.D19	ETH0_RX-	
J1.C20	ETH0_TX-		J1.D20	ETH0_RX+	
J1.C21	ETH0_TX+		J1.D21	GND	
J1.C22	GND		J1.D22	ETH1_RX-	
J1.C23	ETH1_TX-		J1.D23	ETH1_RX+	
J1.C24	ETH1_TX+		J1.D24	GND	
J1.C25	GND		J1.D25	ETH2_RX-	
J1.C26	ETH2_TX-		J1.D26	ETH2_RX+	
J1.C27	ETH2_TX+		J1.D27	GND	
J1.C28	GND		J1.D28	ETH3_RX-	
J1.C29	ETH3_TX-		J1.D29	ETH3_RX+	
J1.C30	ETH3_TX+		J1.D30	GND	
J1.C31	GND		J1.D31	USB3_SSTX-	
J1.C32	USB3_SSRX-		J1.D32	USB3_SSTX+	
J1.C33	USB3_SSRX+		J1.D33	GND	
J1.C34	GND		J1.D34	USB2_SSTX-	
J1.C35	USB2_SSRX-		J1.D35	USB2_SSTX+	
J1.C36	USB2_SSRX+		J1.D36	GND	
J1.C37	GND		J1.D37	USB1_SSTX0-	
J1.C38	USB1_SSRX0-		J1.D38	USB1_SSTX0+	
J1.C39	USB1_SSRX0+		J1.D39	GND	
J1.C40	GND		J1.D40	USB1_SSTX1-	NC
J1.C41	USB1_SSRX1-	NC	J1.D41	USB1_SSTX1+	NC
J1.C42	USB1_SSRX1+	NC	J1.D42	GND	
J1.C43	GND		J1.D43	USB0_SSTX0-	

Table A.2: J1 Connector Rows C and D

J1.C44	USB0_SSRX0-	J1.D44	USB0_SSTX0+
J1.C45	USB0_SSRX0+	J1.D45	GND
J1.C46	GND	J1.D46	USB0_SSTX1- NC
J1.C47	USB0_SSRX1- NC	J1.D47	USB0_SSTX1+ NC
J1.C48	USB0_SSRX1+ NC	J1.D48	GND
J1.C49	GND	J1.D49	SATA0_RX-
J1.C50	BOOT_SPI_IO0	J1.D50	SATA0_RX+
J1.C51	BOOT_SPI_IO1	J1.D51	GND
J1.C52	BOOT_SPI_IO2	J1.D52	SATA0_TX-
J1.C53	BOOT_SPI_IO3	J1.D53	SATA0_TX+
J1.C54	BOOT_SPI_CLK	J1.D54	GND
J1.C55	GND	J1.D55	SATA1_RX-
J1.C56	PCIe_REF-CLK0_HI-	J1.D56	SATA1_RX+
J1.C57	PCIe_REF-CLK0_HI+	J1.D57	GND
J1.C58	GND	J1.D58	SATA1_TX-
J1.C59	PCIe_REF-CLK0_LO-	J1.D59	SATA1_TX+
J1.C60	PCIe_REF-CLK0_LO+	J1.D60	GND
J1.C61	GND	J1.D61	PCIe00_TX-
J1.C62	PCIe00_RX-	J1.D62	PCIe00_TX+
J1.C63	PCIe00_RX+	J1.D63	GND
J1.C64	GND	J1.D64	PCIe01_TX-
J1.C65	PCIe01_RX-	J1.D65	PCIe01_TX+
J1.C66	PCIe01_RX+	J1.D66	GND
J1.C67	GND	J1.D67	PCIe02_TX-
J1.C68	PCIe02_RX-	J1.D68	PCIe02_TX+
J1.C69	PCIe02_RX+	J1.D69	GND
J1.C70	GND	J1.D70	PCIe03_TX-
J1.C71	PCIe03_RX-	J1.D71	PCIe03_TX+
J1.C72	PCIe03_RX+	J1.D72	GND
J1.C73	GND	J1.D73	PCIe04_TX-
J1.C74	PCIe04_RX-	J1.D74	PCIe04_TX+
J1.C75	PCIe04_RX+	J1.D75	GND
J1.C76	GND	J1.D76	PCIe05_TX-
J1.C77	PCIe05_RX-	J1.D77	PCIe05_TX+
J1.C78	PCIe05_RX+	J1.D78	GND
J1.C79	GND	J1.D79	PCIe06_TX-
J1.C80	PCIe06_RX-	J1.D80	PCIe06_TX+
J1.C81	PCIe06_RX+	J1.D81	GND
J1.C82	GND	J1.D82	PCIe07_TX-
J1.C83	PCIe07_RX-	J1.D83	PCIe07_TX+
J1.C84	PCIe07_RX+	J1.D84	GND
J1.C85	GND	J1.D85	NBASET0_MDIO-
J1.C86	SMB_CLK	J1.D86	NBASET0_M-DIO+

Table A.2: J1 Connector Rows C and D				
J1.C87	SMB_DAT		J1.D87	GND
J1.C88	SMB_ALERT#		J1.D88	NBASET0_MDI1-
J1.C89	UART0_TX		J1.D89	NBASET0_MDI1+
J1.C90	UART0_RX		J1.D90	GND
J1.C91	UART0_RTS#		J1.D91	NBASET0_MDI2-
J1.C92	UART0_CTS#		J1.D92	NBASET0_MDI2+
J1.C93	I2C0_CLK		J1.D93	GND
J1.C94	I2C0_DAT		J1.D94	NBASET0_MDI3-
J1.C95	I2C0_ALERT#		J1.D95	NBASET0_MDI3+
J1.C96	I2C1_CLK		J1.D96	GND
J1.C97	I2C1_DAT		J1.D97	NBASET0_LINK_MAX#
J1.C98	NBASET0_SDP		J1.D98	NBASET0_LINK_MID#
J1.C99	NBASET0_C-TREF	NC	J1.D99	NBASET0_LINK_ACT#
J1.C100	TYPE1	GND	J1.D100	TYPE2 NC

Table A.3: J2 Connector Rows E and F

Pin#	Row E Description	SOM-D580 Difference	Pin#	Row F Description	SOM-D580 Difference
J2.E1	RAPID_SHUT-DOWN		J2.F1	ETH2_SDP	
J2.E2	GND		J2.F2	ETH3_SDP	
J2.E3	RSVD		J2.F3	ETH4_SDP	NC
J2.E4	RSVD		J2.F4	ETH5_SDP	NC
J2.E5	GND		J2.F5	ETH6_SDP	NC
J2.E6	RSVD		J2.F6	ETH7_SDP	NC
J2.E7	RSVD		J2.F7	ETH4-7_I2C_-CLK	LAN_KR_I2C1_SCL
J2.E8	GND		J2.F8	ETH4-7_I2C_-DAT	LAN_KR_I2C1_SDA
J2.E9	RSVD		J2.F9	ETH4-7_INT#	
J2.E10	RSVD		J2.F10	ETH4-7_MDIO_-CLK	
J2.E11	GND		J2.F11	ETH4-7_MDIO_-DAT	
J2.E12	RSVD		J2.F12	ETH4-7_PHY_INT#	
J2.E13	RSVD		J2.F13	ETH4-7_PHY_RST#	
J2.E14	GND		J2.F14	ETH4-7_PRSNT#	
J2.E15	RSVD		J2.F15	RSVD	
J2.E16	RSVD		J2.F16	RSVD	
J2.E17	GND		J2.F17	RSVD	
J2.E18	RSVD		J2.F18	RSVD	
J2.E19	RSVD		J2.F19	GND	
J2.E20	GND		J2.F20	PCle32_RX-	
J2.E21	PCle32_TX-		J2.F21	PCle32_RX+	
J2.E22	PCle32_TX+		J2.F22	GND	
J2.E23	GND		J2.F23	PCle33_RX-	
J2.E24	PCle33_TX-		J2.F24	PCle33_RX+	
J2.E25	PCle33_TX+		J2.F25	GND	
J2.E26	GND		J2.F26	PCle34_RX-	
J2.E27	PCle34_TX-		J2.F27	PCle34_RX+	
J2.E28	PCle34_TX+		J2.F28	GND	
J2.E29	GND		J2.F29	PCle35_RX-	
J2.E30	PCle35_TX-		J2.F30	PCle35_RX+	
J2.E31	PCle35_TX+		J2.F31	GND	
J2.E32	GND		J2.F32	PCle36_RX-	
J2.E33	PCle36_TX-		J2.F33	PCle36_RX+	
J2.E34	PCle36_TX+		J2.F34	GND	
J2.E35	GND		J2.F35	PCle37_RX-	
J2.E36	PCle37_TX-		J2.F36	PCle37_RX+	
J2.E37	PCle37_TX+		J2.F37	GND	

Table A.3: J2 Connector Rows E and F

J2.E38	GND		J2.F38	PCle38_RX-	
J2.E39	PCle38_TX-		J2.F39	PCle38_RX+	
J2.E40	PCle38_TX+		J2.F40	GND	
J2.E41	GND		J2.F41	PCle39_RX-	
J2.E42	PCle39_TX-		J2.F42	PCle39_RX+	
J2.E43	PCle39_TX+		J2.F43	GND	
J2.E44	GND		J2.F44	PCle16_RX-	
J2.E45	PCle16_TX-		J2.F45	PCle16_RX+	
J2.E46	PCle16_TX+		J2.F46	GND	
J2.E47	GND		J2.F47	PCle17_RX-	
J2.E48	PCle17_TX-		J2.F48	PCle17_RX+	
J2.E49	PCle17_TX+		J2.F49	GND	
J2.E50	GND		J2.F50	PCle18_RX-	
J2.E51	PCle18_TX-		J2.F51	PCle18_RX+	
J2.E52	PCle18_TX+		J2.F52	GND	
J2.E53	GND		J2.F53	PCle19_RX-	
J2.E54	PCle19_TX-		J2.F54	PCle19_RX+	
J2.E55	PCle19_TX+		J2.F55	GND	
J2.E56	GND		J2.F56	PCle20_RX-	
J2.E57	PCle20_TX-		J2.F57	PCle20_RX+	
J2.E58	PCle20_TX+		J2.F58	GND	
J2.E59	GND		J2.F59	PCle21_RX-	
J2.E60	PCle21_TX-		J2.F60	PCle21_RX+	
J2.E61	PCle21_TX+		J2.F61	GND	
J2.E62	GND		J2.F62	PCle22_RX-	
J2.E63	PCle22_TX-		J2.F63	PCle22_RX+	
J2.E64	PCle22_TX+		J2.F64	GND	
J2.E65	GND		J2.F65	PCle23_RX-	
J2.E66	PCle23_TX-		J2.F66	PCle23_RX+	
J2.E67	PCle23_TX+		J2.F67	GND	
J2.E68	GND		J2.F68	PCle48_RX-	NC
J2.E69	PCle48_TX-	NC	J2.F69	PCle48_RX_	NC
J2.E70	PCle48_TX_	NC	J2.F70	GND	
J2.E71	GND		J2.F71	PCle49_RX-	NC
J2.E72	PCle49_TX-	NC	J2.F72	PCle49_RX_	NC
J2.E73	PCle49_TX_	NC	J2.F73	GND	
J2.E74	GND		J2.F74	PCle50_RX-	NC
J2.E75	PCle50_TX-	NC	J2.F75	PCle50_RX+	NC
J2.E76	PCle50_TX+	NC	J2.F76	GND	
J2.E77	GND		J2.F77	PCle51_RX-	NC
J2.E78	PCle51_TX-	NC	J2.F78	PCle51_RX+	NC
J2.E79	PCle51_TX+	NC	J2.F79	GND	
J2.E80	GND		J2.F80	PCle52_RX-	NC
J2.E81	PCle52_TX-	NC	J2.F81	PCle52_RX+	NC
J2.E82	PCle52_TX+	NC	J2.F82	GND	
J2.E83	GND		J2.F83	PCle53_RX-	NC
J2.E84	PCle53_TX-	NC	J2.F84	PCle53_RX+	NC

Table A.3: J2 Connector Rows E and F

J2.E85	PCIe53_TX+	NC	J2.F85	GND	
J2.E86	GND		J2.F86	PCIe54_RX-	NC
J2.E87	PCIe54_TX-	NC	J2.F87	PCIe54_RX+	NC
J2.E88	PCIe54_TX+	NC	J2.F88	GND	
J2.E89	GND		J2.F89	PCIe55_RX-	NC
J2.E90	PCIe55_TX-	NC	J2.F90	PCIe55_RX+	NC
J2.E91	PCIe55_TX+	NC	J2.F91	GND	
J2.E92	GND		J2.F92	PCIe_REFCLK2-	
J2.E93	PCIe_REF-CLK1-		J2.F93	PCIe_REFCLK2+	
J2.E94	PCIe_REF-CLK1+		J2.F94	GND	
J2.E95	GND		J2.F95	PCIe_-CLKREQ3#	
J2.E96	PCIe_-CLKREQ1#		J2.F96	ETH0-3_PRSENT#	
J2.E97	PCIe_-CLKREQ2#		J2.F97	ETH0-3_PHY_RST#	
J2.E98	PCIe_-CLKREQ_OUT0 #	PD	J2.F98	ETH0_SDP	
J2.E99	PCIe_-CLKREQ_OUT1 #	PD	J2.F99	ETH1_SDP	
J2.E100	PCIe_PER-ST_IN0#	PD	J2.F100	PCIe_PER-ST_IN1#	PD

Table A.4: J2 Connector Rows G and H

Pin#	Row G Description	SOM-D580 Difference	Pin#	Row H Description	SOM-D580 Difference
J2.G1	VCC_5V_SBY		J2.H1	RSVD	NC
J2.G2	RSVD	NC	J2.H2	RSVD	NC
J2.G3	RSVD	NC	J2.H3	RSVD	NC
J2.G4	RSVD	NC	J2.H4	RSVD	NC
J2.G5	RSVD	NC	J2.H5	RSVD	NC
J2.G6	RSVD	NC	J2.H6	RSVD	NC
J2.G7	RSVD	NC	J2.H7	RSVD	NC
J2.G8	RSVD	NC	J2.H8	RSVD	NC
J2.G9	RSVD	NC	J2.H9	RSVD	NC
J2.G10	RSVD	NC	J2.H10	RSVD	NC
J2.G11	RSVD	NC	J2.H11	RSVD	NC
J2.G12	RSVD	NC	J2.H12	RSVD	NC
J2.G13	RSVD	NC	J2.H13	RSVD	NC
J2.G14	GND		J2.H14	RSVD	NC
J2.G15	RSVD	NC	J2.H15	RSVD	NC
J2.G16	RSVD	NC	J2.H16	RSVD	NC
J2.G17	RSVD	NC	J2.H17	RSVD	NC
J2.G18	RSVD	NC	J2.H18	RSVD	NC
J2.G19	RSVD	NC	J2.H19	GND	
J2.G20	GND		J2.H20	PCIe40_TX-	
J2.G21	PCIe40_RX-		J2.H21	PCIe40_TX+	
J2.G22	PCIe40_RX+		J2.H22	GND	
J2.G23	GND		J2.H23	PCIe41_TX-	
J2.G24	PCIe41_RX-		J2.H24	PCIe41_TX+	
J2.G25	PCIe41_RX+		J2.H25	GND	
J2.G26	GND		J2.H26	PCIe42_TX-	
J2.G27	PCIe42_RX-		J2.H27	PCIe42_TX+	
J2.G28	PCIe42_RX+		J2.H28	GND	
J2.G29	GND		J2.H29	PCIe43_TX-	
J2.G30	PCIe43_RX-		J2.H30	PCIe43_TX+	
J2.G31	PCIe43_RX+		J2.H31	GND	
J2.G32	GND		J2.H32	PCIe44_TX-	
J2.G33	PCIe44_RX-		J2.H33	PCIe44_TX+	
J2.G34	PCIe44_RX+		J2.H34	GND	
J2.G35	GND		J2.H35	PCIe45_TX-	
J2.G36	PCIe45_RX-		J2.H36	PCIe45_TX+	
J2.G37	PCIe45_RX+		J2.H37	GND	
J2.G38	GND		J2.H38	PCIe46_TX-	
J2.G39	PCIe46_RX-		J2.H39	PCIe46_TX+	
J2.G40	PCIe46_RX+		J2.H40	GND	
J2.G41	GND		J2.H41	PCIe47_TX-	
J2.G42	PCIe47_RX-		J2.H42	PCIe47_TX+	
J2.G43	PCIe47_RX+		J2.H43	GND	
J2.G44	GND		J2.H44	PCIe24_TX-	

Table A.4: J2 Connector Rows G and H

J2.G45	PCIe24_RX-		J2.H45	PCIe24_TX+	
J2.G46	PCIe24_RX+		J2.H46	GND	
J2.G47	GND		J2.H47	PCIe25_TX-	
J2.G48	PCIe25_RX-		J2.H48	PCIe25_TX+	
J2.G49	PCIe25_RX+		J2.H49	GND	
J2.G50	GND		J2.H50	PCIe26_TX-	
J2.G51	PCIe26_RX-		J2.H51	PCIe26_TX+	
J2.G52	PCIe26_RX+		J2.H52	GND	
J2.G53	GND		J2.H53	PCIe27_TX-	
J2.G54	PCIe27_RX-		J2.H54	PCIe27_TX+	
J2.G55	PCIe27_RX+		J2.H55	GND	
J2.G56	GND		J2.H56	PCIe28_TX-	
J2.G57	PCIe28_RX-		J2.H57	PCIe28_TX+	
J2.G58	PCIe28_RX+		J2.H58	GND	
J2.G59	GND		J2.H59	PCIe29_TX-	
J2.G60	PCIe29_RX-		J2.H60	PCIe29_TX+	
J2.G61	PCIe29_RX+		J2.H61	GND	
J2.G62	GND		J2.H62	PCIe30_TX-	
J2.G63	PCIe30_RX-		J2.H63	PCIe30_TX+	
J2.G64	PCIe30_RX+		J2.H64	GND	
J2.G65	GND		J2.H65	PCIe31_TX-	
J2.G66	PCIe31_RX-		J2.H66	PCIe31_TX+	
J2.G67	PCIe31_RX+		J2.H67	GND	
J2.G68	GND		J2.H68	PCIe56_TX-	NC
J2.G69	PCIe56_RX-	NC	J2.H69	PCIe56_TX+	NC
J2.G70	PCIe56_RX+	NC	J2.H70	GND	
J2.G71	GND		J2.H71	PCIe57_TX-	NC
J2.G72	PCIe57_RX-	NC	J2.H72	PCIe57_TX+	NC
J2.G73	PCIe57_RX+	NC	J2.H73	GND	
J2.G73	GND		J2.H74	PCIe58_TX-	NC
J2.G75	PCIe58_RX-	NC	J2.H75	PCIe58_TX+	NC
J2.G76	PCIe58_RX+	NC	J2.H76	GND	
J2.G77	GND		J2.H77	PCIe59_TX-	NC
J2.G78	PCIe59_RX-	NC	J2.H78	PCIe59_TX+	NC
J2.G79	PCIe59_RX+	NC	J2.H79	GND	
J2.G80	GND		J2.H80	PCIe60_TX-	NC
J2.G81	PCIe60_RX-	NC	J2.H81	PCIe60_TX+	NC
J2.G82	PCIe60_RX+	NC	J2.H82	GND	
J2.G83	GND		J2.H83	PCIe61_TX-	NC
J2.G84	PCIe61_RX-	NC	J2.H84	PCIe61_TX+	NC
J2.G85	PCIe61_RX+	NC	J2.H85	GND	
J2.G86	GND		J2.H86	PCIe62_TX-	NC
J2.G87	PCIe62_RX-	NC	J2.H87	PCIe62_TX+	NC
J2.G88	PCIe62_RX+	NC	J2.H88	GND	
J2.G89	GND		J2.H89	PCIe63_TX-	NC
J2.G90	PCIe63_RX-	NC	J2.H90	PCIe63_TX+	NC
J2.G91	PCIe63_RX+	NC	J2.H91	GND	

Table A.4: J2 Connector Rows G and H

J2.G92	GND		J2.H92	PCIe_REF-CLKIN0-	NC
J2.G93	PCIe_REF-CLK3-		J2.H93	PCIe_REF-CLKIN0+	NC
J2.G94	PCIe_REF-CLK3+		J2.H94	GND	
J2.G95	GND		J2.H95	PCIe_REF-CLKIN1-	NC
J2.G96	ETH0-3_I2C_-CLK		J2.H96	PCIe_REF-CLKIN1+	NC
J2.G97	ETH0-3_I2C_-DAT		J2.H97	GND	
J2.G98	ETH0-3_PHY_INT#	PU	J2.H98	ETH0-3_MDIO_-CLK	
J2.G99	ETH0-3_INT#		J2.H99	ETH0-3_MDIO_-DAT	
J2.G100	PCIe_WAKE_OUT0#	PU	J2.H100	PCIe_WAKE_OUT1#	PU

Note!

1. A86 can be an optional pin reserved for CB_I2C_ALERT#. Please contact FAE for details.
2. 2C15 can be an optional pin reserved for SML0_CLK. Please contact FAE for details.
3. C16 can be an optional pin reserved for SML0_DATA. Please contact FAE for details.
4. C17 can be an optional pin reserved for SML0ALERT#. Please contact FAE for details.
5. C18 can be an optional pin reserved for PMC_ALERT#. Please contact FAE for details.
6. C25 can be an optional pin reserved for AUXDDI1_TBT_AUX+. Please contact FAE for details.
7. C26 can be an optional pin reserved for AUXDDI1_TBT_AUX-. Please contact FAE for details.
8. C27 can be an optional pin reserved for SML1_CLK. Please contact FAE for details.
9. C28 can be an optional pin reserved for SML1_DATA. Please contact FAE for details.
10. C29 can be an optional pin reserved for AUXDDI2_TBT_AUX+. Please contact FAE for details.
11. C30 can be an optional pin reserved for AUXDDI2_TBT_AUX-. Please contact FAE for details.
12. D17 can be an optional pin reserved for DDI1_CTRLCLK. Please contact FAE for details.
13. D18 can be an optional pin reserved for DDI1_CTRLDATA. Please contact FAE for details.
14. D63 can be an optional pin reserved for DDI2_CTRLCLK. Please contact FAE for details.
15. D64 can be an optional pin reserved for DDI2_CTRLDATA. Please contact FAE for details.

Appendix **B**

Watchdog Timer

This appendix details information about watchdog timer programming on the SOM-D580 CPU Computer-on-Module.

Sections include:

- Watchdog Timer Programming

B.1 Programming the Watchdog Timer

Table B.1: Programming the Watchdog Timer

Trigger Event	Note
IRQ	BIOS setting default disable**
NMI	N/A
SCI	Power button event
Power Off	Support
H/W Restart	Support
External WDT	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 this.

On 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 details illustration of the General Purpose Input and Output pin settings.

Sections include:

- GPIO Register

C.1 GPIO Register

Table C.1: GPIO Register

GPIO Byte Mapping	H/W Pin Name
BIT0	GPI0
BIT1	GPI1
BIT2	GPI2
BIT3	GPI3
BIT4	GPI4
BIT5	GPI5
BIT6	GPI6
BIT7	GPI7
BIT8	GPI8
BIT9	GPI9
BIT10	GPI10
BIT11	GPI11

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

Appendix **D**

System Assignments

This appendix gives you information about system resource allocation on the SOM-D580 CPU Computer-on-Module.

Sections include:

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

D.1 System I/O Ports

Table D.1: System I/O 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
0x000003F8-0x000003FF	Communications Port (COM1)
0x00000400-0x0000041F	Motherboard resources
0x000004D0-0x000004D1	Programmable interrupt controller
0x00000500-0x000005FE	Motherboard resources
0x00000500-0x000005FE	Motherboard resources

Table D.1: System I/O Ports

0x0000CA2-0x0000CA2	Microsoft Generic IPMI Compliant Device
0x0000CA3-0x0000CA3	Microsoft Generic IPMI Compliant Device
0x00001000-0x00005FFF	PCI Express Root Complex
0x00003000-0x00003FFF	CDF PCIeRP[8] - 18AD
0x00003000-0x00003FFF	PCI Express to PCI/PCI-X Bridge
0x00003000-0x00003FFF	ASPEED Graphics Family (WDDM)
0x00004000-0x00004FFF	CDF PCIeRP[7] - 18AB
0x00005020-0x0000503F	Standard SATA AHCI Controller
0x00005070-0x00005073	Standard SATA AHCI Controller
0x00005080-0x00005087	Standard SATA AHCI Controller
0x00005FE8-0x00005FEF	CDF HSUART - 18D8 (COM5)
0x00005FF0-0x00005FF7	CDF HSUART - 18D8 (COM4)
0x00005FF8-0x00005FFF	CDF HSUART - 18D8 (COM3)
0x00006000-0x00008FFF	PCI Express Root Complex
0x00009000-0x0000BFFF	PCI Express Root Complex
0x0000C000-0x0000DFFF	PCI Express Root Complex
0x0000E000-0x0000FFFF	PCI Express Root Complex

D.2 Interrupt Assignments

Table D.2: Interrupt Assignments

Interrupt#	Interrupt Source
IRQ 0	System timer
IRQ 100	Microsoft ACPI-Compliant System
IRQ 101	Microsoft ACPI-Compliant System
IRQ 102	Microsoft ACPI-Compliant System
IRQ 103	Microsoft ACPI-Compliant System
IRQ 104	Microsoft ACPI-Compliant System
IRQ 105	Microsoft ACPI-Compliant System
IRQ 106	Microsoft ACPI-Compliant System
IRQ 107	Microsoft ACPI-Compliant System
IRQ 108	Microsoft ACPI-Compliant System
IRQ 109	Microsoft ACPI-Compliant System
IRQ 110	Microsoft ACPI-Compliant System
IRQ 111	Microsoft ACPI-Compliant System
IRQ 112	Microsoft ACPI-Compliant System
IRQ 113	Microsoft ACPI-Compliant System
IRQ 114	Microsoft ACPI-Compliant System
IRQ 115	Microsoft ACPI-Compliant System
IRQ 116	Microsoft ACPI-Compliant System
IRQ 117	Microsoft ACPI-Compliant System
IRQ 118	Microsoft ACPI-Compliant System
IRQ 119	Microsoft ACPI-Compliant System
IRQ 120	Microsoft ACPI-Compliant System
IRQ 121	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 122	Microsoft ACPI-Compliant System
IRQ 123	Microsoft ACPI-Compliant System
IRQ 124	Microsoft ACPI-Compliant System
IRQ 125	Microsoft ACPI-Compliant System
IRQ 126	Microsoft ACPI-Compliant System
IRQ 127	Microsoft ACPI-Compliant System
IRQ 128	Microsoft ACPI-Compliant System
IRQ 129	Microsoft ACPI-Compliant System
IRQ 13	Numeric data processor
IRQ 130	Microsoft ACPI-Compliant System
IRQ 131	Microsoft ACPI-Compliant System
IRQ 132	Microsoft ACPI-Compliant System
IRQ 133	Microsoft ACPI-Compliant System
IRQ 134	Microsoft ACPI-Compliant System
IRQ 135	Microsoft ACPI-Compliant System
IRQ 136	Microsoft ACPI-Compliant System
IRQ 137	Microsoft ACPI-Compliant System
IRQ 138	Microsoft ACPI-Compliant System
IRQ 139	Microsoft ACPI-Compliant System
IRQ 140	Microsoft ACPI-Compliant System
IRQ 141	Microsoft ACPI-Compliant System
IRQ 142	Microsoft ACPI-Compliant System
IRQ 143	Microsoft ACPI-Compliant System
IRQ 144	Microsoft ACPI-Compliant System
IRQ 145	Microsoft ACPI-Compliant System
IRQ 146	Microsoft ACPI-Compliant System
IRQ 147	Microsoft ACPI-Compliant System
IRQ 148	Microsoft ACPI-Compliant System
IRQ 149	Microsoft ACPI-Compliant System
IRQ 150	Microsoft ACPI-Compliant System
IRQ 151	Microsoft ACPI-Compliant System
IRQ 152	Microsoft ACPI-Compliant System
IRQ 153	Microsoft ACPI-Compliant System
IRQ 154	Microsoft ACPI-Compliant System
IRQ 155	Microsoft ACPI-Compliant System
IRQ 156	Microsoft ACPI-Compliant System
IRQ 157	Microsoft ACPI-Compliant System
IRQ 158	Microsoft ACPI-Compliant System
IRQ 159	Microsoft ACPI-Compliant System
IRQ 16	CDF HSUART - 18D8 (COM3)
IRQ 16	ASPEED Graphics Family (WDDM)
IRQ 160	Microsoft ACPI-Compliant System
IRQ 161	Microsoft ACPI-Compliant System
IRQ 162	Microsoft ACPI-Compliant System
IRQ 163	Microsoft ACPI-Compliant System
IRQ 164	Microsoft ACPI-Compliant System
IRQ 165	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 166	Microsoft ACPI-Compliant System
IRQ 167	Microsoft ACPI-Compliant System
IRQ 168	Microsoft ACPI-Compliant System
IRQ 169	Microsoft ACPI-Compliant System
IRQ 17	CDF HSUART - 18D8 (COM4)
IRQ 170	Microsoft ACPI-Compliant System
IRQ 171	Microsoft ACPI-Compliant System
IRQ 172	Microsoft ACPI-Compliant System
IRQ 173	Microsoft ACPI-Compliant System
IRQ 174	Microsoft ACPI-Compliant System
IRQ 175	Microsoft ACPI-Compliant System
IRQ 176	Microsoft ACPI-Compliant System
IRQ 177	Microsoft ACPI-Compliant System
IRQ 178	Microsoft ACPI-Compliant System
IRQ 179	Microsoft ACPI-Compliant System
IRQ 18	CDF HSUART - 18D8 (COM5)
IRQ 180	Microsoft ACPI-Compliant System
IRQ 181	Microsoft ACPI-Compliant System
IRQ 182	Microsoft ACPI-Compliant System
IRQ 183	Microsoft ACPI-Compliant System
IRQ 184	Microsoft ACPI-Compliant System
IRQ 185	Microsoft ACPI-Compliant System
IRQ 186	Microsoft ACPI-Compliant System
IRQ 187	Microsoft ACPI-Compliant System
IRQ 188	Microsoft ACPI-Compliant System
IRQ 189	Microsoft ACPI-Compliant System
IRQ 190	Microsoft ACPI-Compliant System
IRQ 191	Microsoft ACPI-Compliant System
IRQ 192	Microsoft ACPI-Compliant System
IRQ 193	Microsoft ACPI-Compliant System
IRQ 194	Microsoft ACPI-Compliant System
IRQ 195	Microsoft ACPI-Compliant System
IRQ 196	Microsoft ACPI-Compliant System
IRQ 197	Microsoft ACPI-Compliant System
IRQ 198	Microsoft ACPI-Compliant System
IRQ 199	Microsoft ACPI-Compliant System
IRQ 200	Microsoft ACPI-Compliant System
IRQ 201	Microsoft ACPI-Compliant System
IRQ 202	Microsoft ACPI-Compliant System
IRQ 203	Microsoft ACPI-Compliant System
IRQ 204	Microsoft ACPI-Compliant System
IRQ 21	CDF GPIO Controller - 3001
IRQ 256	Microsoft ACPI-Compliant System
IRQ 257	Microsoft ACPI-Compliant System
IRQ 258	Microsoft ACPI-Compliant System
IRQ 259	Microsoft ACPI-Compliant System
IRQ 260	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 261	Microsoft ACPI-Compliant System
IRQ 262	Microsoft ACPI-Compliant System
IRQ 263	Microsoft ACPI-Compliant System
IRQ 264	Microsoft ACPI-Compliant System
IRQ 265	Microsoft ACPI-Compliant System
IRQ 266	Microsoft ACPI-Compliant System
IRQ 267	Microsoft ACPI-Compliant System
IRQ 268	Microsoft ACPI-Compliant System
IRQ 269	Microsoft ACPI-Compliant System
IRQ 270	Microsoft ACPI-Compliant System
IRQ 271	Microsoft ACPI-Compliant System
IRQ 272	Microsoft ACPI-Compliant System
IRQ 273	Microsoft ACPI-Compliant System
IRQ 274	Microsoft ACPI-Compliant System
IRQ 275	Microsoft ACPI-Compliant System
IRQ 276	Microsoft ACPI-Compliant System
IRQ 277	Microsoft ACPI-Compliant System
IRQ 278	Microsoft ACPI-Compliant System
IRQ 279	Microsoft ACPI-Compliant System
IRQ 280	Microsoft ACPI-Compliant System
IRQ 281	Microsoft ACPI-Compliant System
IRQ 282	Microsoft ACPI-Compliant System
IRQ 283	Microsoft ACPI-Compliant System
IRQ 284	Microsoft ACPI-Compliant System
IRQ 285	Microsoft ACPI-Compliant System
IRQ 286	Microsoft ACPI-Compliant System
IRQ 287	Microsoft ACPI-Compliant System
IRQ 288	Microsoft ACPI-Compliant System
IRQ 289	Microsoft ACPI-Compliant System
IRQ 290	Microsoft ACPI-Compliant System
IRQ 291	Microsoft ACPI-Compliant System
IRQ 292	Microsoft ACPI-Compliant System
IRQ 293	Microsoft ACPI-Compliant System
IRQ 294	Microsoft ACPI-Compliant System
IRQ 295	Microsoft ACPI-Compliant System
IRQ 296	Microsoft ACPI-Compliant System
IRQ 297	Microsoft ACPI-Compliant System
IRQ 298	Microsoft ACPI-Compliant System
IRQ 299	Microsoft ACPI-Compliant System
IRQ 3	Communications Port (COM2)
IRQ 300	Microsoft ACPI-Compliant System
IRQ 301	Microsoft ACPI-Compliant System
IRQ 302	Microsoft ACPI-Compliant System
IRQ 303	Microsoft ACPI-Compliant System
IRQ 304	Microsoft ACPI-Compliant System
IRQ 305	Microsoft ACPI-Compliant System
IRQ 306	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 307	Microsoft ACPI-Compliant System
IRQ 308	Microsoft ACPI-Compliant System
IRQ 309	Microsoft ACPI-Compliant System
IRQ 310	Microsoft ACPI-Compliant System
IRQ 311	Microsoft ACPI-Compliant System
IRQ 312	Microsoft ACPI-Compliant System
IRQ 313	Microsoft ACPI-Compliant System
IRQ 314	Microsoft ACPI-Compliant System
IRQ 315	Microsoft ACPI-Compliant System
IRQ 316	Microsoft ACPI-Compliant System
IRQ 317	Microsoft ACPI-Compliant System
IRQ 318	Microsoft ACPI-Compliant System
IRQ 319	Microsoft ACPI-Compliant System
IRQ 320	Microsoft ACPI-Compliant System
IRQ 321	Microsoft ACPI-Compliant System
IRQ 322	Microsoft ACPI-Compliant System
IRQ 323	Microsoft ACPI-Compliant System
IRQ 324	Microsoft ACPI-Compliant System
IRQ 325	Microsoft ACPI-Compliant System
IRQ 326	Microsoft ACPI-Compliant System
IRQ 327	Microsoft ACPI-Compliant System
IRQ 328	Microsoft ACPI-Compliant System
IRQ 329	Microsoft ACPI-Compliant System
IRQ 330	Microsoft ACPI-Compliant System
IRQ 331	Microsoft ACPI-Compliant System
IRQ 332	Microsoft ACPI-Compliant System
IRQ 333	Microsoft ACPI-Compliant System
IRQ 334	Microsoft ACPI-Compliant System
IRQ 335	Microsoft ACPI-Compliant System
IRQ 336	Microsoft ACPI-Compliant System
IRQ 337	Microsoft ACPI-Compliant System
IRQ 338	Microsoft ACPI-Compliant System
IRQ 339	Microsoft ACPI-Compliant System
IRQ 340	Microsoft ACPI-Compliant System
IRQ 341	Microsoft ACPI-Compliant System
IRQ 342	Microsoft ACPI-Compliant System
IRQ 343	Microsoft ACPI-Compliant System
IRQ 344	Microsoft ACPI-Compliant System
IRQ 345	Microsoft ACPI-Compliant System
IRQ 346	Microsoft ACPI-Compliant System
IRQ 347	Microsoft ACPI-Compliant System
IRQ 348	Microsoft ACPI-Compliant System
IRQ 349	Microsoft ACPI-Compliant System
IRQ 350	Microsoft ACPI-Compliant System
IRQ 351	Microsoft ACPI-Compliant System
IRQ 352	Microsoft ACPI-Compliant System
IRQ 353	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 354	Microsoft ACPI-Compliant System
IRQ 355	Microsoft ACPI-Compliant System
IRQ 356	Microsoft ACPI-Compliant System
IRQ 357	Microsoft ACPI-Compliant System
IRQ 358	Microsoft ACPI-Compliant System
IRQ 359	Microsoft ACPI-Compliant System
IRQ 360	Microsoft ACPI-Compliant System
IRQ 361	Microsoft ACPI-Compliant System
IRQ 362	Microsoft ACPI-Compliant System
IRQ 363	Microsoft ACPI-Compliant System
IRQ 364	Microsoft ACPI-Compliant System
IRQ 365	Microsoft ACPI-Compliant System
IRQ 366	Microsoft ACPI-Compliant System
IRQ 367	Microsoft ACPI-Compliant System
IRQ 368	Microsoft ACPI-Compliant System
IRQ 369	Microsoft ACPI-Compliant System
IRQ 370	Microsoft ACPI-Compliant System
IRQ 371	Microsoft ACPI-Compliant System
IRQ 372	Microsoft ACPI-Compliant System
IRQ 373	Microsoft ACPI-Compliant System
IRQ 374	Microsoft ACPI-Compliant System
IRQ 375	Microsoft ACPI-Compliant System
IRQ 376	Microsoft ACPI-Compliant System
IRQ 377	Microsoft ACPI-Compliant System
IRQ 378	Microsoft ACPI-Compliant System
IRQ 379	Microsoft ACPI-Compliant System
IRQ 380	Microsoft ACPI-Compliant System
IRQ 381	Microsoft ACPI-Compliant System
IRQ 382	Microsoft ACPI-Compliant System
IRQ 383	Microsoft ACPI-Compliant System
IRQ 384	Microsoft ACPI-Compliant System
IRQ 385	Microsoft ACPI-Compliant System
IRQ 386	Microsoft ACPI-Compliant System
IRQ 387	Microsoft ACPI-Compliant System
IRQ 388	Microsoft ACPI-Compliant System
IRQ 389	Microsoft ACPI-Compliant System
IRQ 390	Microsoft ACPI-Compliant System
IRQ 391	Microsoft ACPI-Compliant System
IRQ 392	Microsoft ACPI-Compliant System
IRQ 393	Microsoft ACPI-Compliant System
IRQ 394	Microsoft ACPI-Compliant System
IRQ 395	Microsoft ACPI-Compliant System
IRQ 396	Microsoft ACPI-Compliant System
IRQ 397	Microsoft ACPI-Compliant System
IRQ 398	Microsoft ACPI-Compliant System
IRQ 399	Microsoft ACPI-Compliant System
IRQ 4	Communications Port (COM1)

Table D.2: Interrupt Assignments	
IRQ 400	Microsoft ACPI-Compliant System
IRQ 401	Microsoft ACPI-Compliant System
IRQ 402	Microsoft ACPI-Compliant System
IRQ 403	Microsoft ACPI-Compliant System
IRQ 404	Microsoft ACPI-Compliant System
IRQ 405	Microsoft ACPI-Compliant System
IRQ 406	Microsoft ACPI-Compliant System
IRQ 407	Microsoft ACPI-Compliant System
IRQ 408	Microsoft ACPI-Compliant System
IRQ 409	Microsoft ACPI-Compliant System
IRQ 410	Microsoft ACPI-Compliant System
IRQ 411	Microsoft ACPI-Compliant System
IRQ 412	Microsoft ACPI-Compliant System
IRQ 413	Microsoft ACPI-Compliant System
IRQ 414	Microsoft ACPI-Compliant System
IRQ 415	Microsoft ACPI-Compliant System
IRQ 416	Microsoft ACPI-Compliant System
IRQ 417	Microsoft ACPI-Compliant System
IRQ 418	Microsoft ACPI-Compliant System
IRQ 419	Microsoft ACPI-Compliant System
IRQ 420	Microsoft ACPI-Compliant System
IRQ 421	Microsoft ACPI-Compliant System
IRQ 422	Microsoft ACPI-Compliant System
IRQ 423	Microsoft ACPI-Compliant System
IRQ 424	Microsoft ACPI-Compliant System
IRQ 425	Microsoft ACPI-Compliant System
IRQ 426	Microsoft ACPI-Compliant System
IRQ 427	Microsoft ACPI-Compliant System
IRQ 428	Microsoft ACPI-Compliant System
IRQ 429	Microsoft ACPI-Compliant System
IRQ 4294967246	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967247	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967248	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967249	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967250	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967251	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967252	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967253	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967254	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967255	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967256	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967257	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967258	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967259	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967260	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967261	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967262	Intel® Ethernet Controller (3) I225-IT

Table D.2: Interrupt Assignments

IRQ 4294967263	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967264	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967265	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967266	Intel® Ethernet Controller (3) I225-IT
IRQ 4294967267	Intel® I210 Gigabit Network Connection
IRQ 4294967268	Intel® I210 Gigabit Network Connection
IRQ 4294967269	Intel® I210 Gigabit Network Connection
IRQ 4294967270	Intel® I210 Gigabit Network Connection
IRQ 4294967271	Intel® I210 Gigabit Network Connection
IRQ 4294967272	Intel® I210 Gigabit Network Connection
IRQ 4294967273	Intel® I210 Gigabit Network Connection
IRQ 4294967274	Intel® I210 Gigabit Network Connection
IRQ 4294967275	Intel® I210 Gigabit Network Connection
IRQ 4294967276	Intel® I210 Gigabit Network Connection
IRQ 4294967277	Intel® I210 Gigabit Network Connection
IRQ 4294967278	Intel® I210 Gigabit Network Connection
IRQ 4294967279	Intel® I210 Gigabit Network Connection
IRQ 4294967280	Intel® I210 Gigabit Network Connection
IRQ 4294967281	Intel® I210 Gigabit Network Connection
IRQ 4294967282	Intel® I210 Gigabit Network Connection
IRQ 4294967283	Intel® I210 Gigabit Network Connection
IRQ 4294967284	Intel® I210 Gigabit Network Connection
IRQ 4294967285	Intel® I210 Gigabit Network Connection
IRQ 4294967286	Intel® I210 Gigabit Network Connection
IRQ 4294967287	Intel® I210 Gigabit Network Connection
IRQ 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[9] - 18AE
IRQ 4294967293	CDF PCIeRP[8] - 18AD
IRQ 4294967294	CDF PCIeRP[7] - 18AB
IRQ 430	Microsoft ACPI-Compliant System
IRQ 431	Microsoft ACPI-Compliant System
IRQ 432	Microsoft ACPI-Compliant System
IRQ 433	Microsoft ACPI-Compliant System
IRQ 434	Microsoft ACPI-Compliant System
IRQ 435	Microsoft ACPI-Compliant System
IRQ 436	Microsoft ACPI-Compliant System
IRQ 437	Microsoft ACPI-Compliant System
IRQ 438	Microsoft ACPI-Compliant System
IRQ 439	Microsoft ACPI-Compliant System
IRQ 440	Microsoft ACPI-Compliant System
IRQ 441	Microsoft ACPI-Compliant System
IRQ 442	Microsoft ACPI-Compliant System
IRQ 443	Microsoft ACPI-Compliant System
IRQ 444	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 445	Microsoft ACPI-Compliant System
IRQ 446	Microsoft ACPI-Compliant System
IRQ 447	Microsoft ACPI-Compliant System
IRQ 448	Microsoft ACPI-Compliant System
IRQ 449	Microsoft ACPI-Compliant System
IRQ 450	Microsoft ACPI-Compliant System
IRQ 451	Microsoft ACPI-Compliant System
IRQ 452	Microsoft ACPI-Compliant System
IRQ 453	Microsoft ACPI-Compliant System
IRQ 454	Microsoft ACPI-Compliant System
IRQ 455	Microsoft ACPI-Compliant System
IRQ 456	Microsoft ACPI-Compliant System
IRQ 457	Microsoft ACPI-Compliant System
IRQ 458	Microsoft ACPI-Compliant System
IRQ 459	Microsoft ACPI-Compliant System
IRQ 460	Microsoft ACPI-Compliant System
IRQ 461	Microsoft ACPI-Compliant System
IRQ 462	Microsoft ACPI-Compliant System
IRQ 463	Microsoft ACPI-Compliant System
IRQ 464	Microsoft ACPI-Compliant System
IRQ 465	Microsoft ACPI-Compliant System
IRQ 466	Microsoft ACPI-Compliant System
IRQ 467	Microsoft ACPI-Compliant System
IRQ 468	Microsoft ACPI-Compliant System
IRQ 469	Microsoft ACPI-Compliant System
IRQ 470	Microsoft ACPI-Compliant System
IRQ 471	Microsoft ACPI-Compliant System
IRQ 472	Microsoft ACPI-Compliant System
IRQ 473	Microsoft ACPI-Compliant System
IRQ 474	Microsoft ACPI-Compliant System
IRQ 475	Microsoft ACPI-Compliant System
IRQ 476	Microsoft ACPI-Compliant System
IRQ 477	Microsoft ACPI-Compliant System
IRQ 478	Microsoft ACPI-Compliant System
IRQ 479	Microsoft ACPI-Compliant System
IRQ 480	Microsoft ACPI-Compliant System
IRQ 481	Microsoft ACPI-Compliant System
IRQ 482	Microsoft ACPI-Compliant System
IRQ 483	Microsoft ACPI-Compliant System
IRQ 484	Microsoft ACPI-Compliant System
IRQ 485	Microsoft ACPI-Compliant System
IRQ 486	Microsoft ACPI-Compliant System
IRQ 487	Microsoft ACPI-Compliant System
IRQ 488	Microsoft ACPI-Compliant System
IRQ 489	Microsoft ACPI-Compliant System
IRQ 490	Microsoft ACPI-Compliant System
IRQ 491	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments

IRQ 492	Microsoft ACPI-Compliant System
IRQ 493	Microsoft ACPI-Compliant System
IRQ 494	Microsoft ACPI-Compliant System
IRQ 495	Microsoft ACPI-Compliant System
IRQ 496	Microsoft ACPI-Compliant System
IRQ 497	Microsoft ACPI-Compliant System
IRQ 498	Microsoft ACPI-Compliant System
IRQ 499	Microsoft ACPI-Compliant System
IRQ 500	Microsoft ACPI-Compliant System
IRQ 501	Microsoft ACPI-Compliant System
IRQ 502	Microsoft ACPI-Compliant System
IRQ 503	Microsoft ACPI-Compliant System
IRQ 504	Microsoft ACPI-Compliant System
IRQ 505	Microsoft ACPI-Compliant System
IRQ 506	Microsoft ACPI-Compliant System
IRQ 507	Microsoft ACPI-Compliant System
IRQ 508	Microsoft ACPI-Compliant System
IRQ 509	Microsoft ACPI-Compliant System
IRQ 510	Microsoft ACPI-Compliant System
IRQ 511	Microsoft ACPI-Compliant System
IRQ 54	Microsoft ACPI-Compliant System
IRQ 55	Microsoft ACPI-Compliant System
IRQ 56	Microsoft ACPI-Compliant System
IRQ 57	Microsoft ACPI-Compliant System
IRQ 58	Microsoft ACPI-Compliant System
IRQ 59	Microsoft ACPI-Compliant System
IRQ 6	Motherboard resources
IRQ 6	Motherboard resources
IRQ 6	Motherboard resources
IRQ 60	Microsoft ACPI-Compliant System
IRQ 61	Microsoft ACPI-Compliant System
IRQ 62	Microsoft ACPI-Compliant System
IRQ 63	Microsoft ACPI-Compliant System
IRQ 64	Microsoft ACPI-Compliant System
IRQ 65	Microsoft ACPI-Compliant System
IRQ 66	Microsoft ACPI-Compliant System
IRQ 67	Microsoft ACPI-Compliant System
IRQ 68	Microsoft ACPI-Compliant System
IRQ 69	Microsoft ACPI-Compliant System
IRQ 70	Microsoft ACPI-Compliant System
IRQ 71	Microsoft ACPI-Compliant System
IRQ 72	Microsoft ACPI-Compliant System
IRQ 73	Microsoft ACPI-Compliant System
IRQ 74	Microsoft ACPI-Compliant System
IRQ 75	Microsoft ACPI-Compliant System
IRQ 76	Microsoft ACPI-Compliant System
IRQ 77	Microsoft ACPI-Compliant System

Table D.2: Interrupt Assignments	
IRQ 78	Microsoft ACPI-Compliant System
IRQ 79	Microsoft ACPI-Compliant System
IRQ 8	System CMOS/real time clock
IRQ 80	Microsoft ACPI-Compliant System
IRQ 81	Microsoft ACPI-Compliant System
IRQ 82	Microsoft ACPI-Compliant System
IRQ 83	Microsoft ACPI-Compliant System
IRQ 84	Microsoft ACPI-Compliant System
IRQ 85	Microsoft ACPI-Compliant System
IRQ 86	Microsoft ACPI-Compliant System
IRQ 87	Microsoft ACPI-Compliant System
IRQ 88	Microsoft ACPI-Compliant System
IRQ 89	Microsoft ACPI-Compliant System
IRQ 90	Microsoft ACPI-Compliant System
IRQ 91	Microsoft ACPI-Compliant System
IRQ 92	Microsoft ACPI-Compliant System
IRQ 93	Microsoft ACPI-Compliant System
IRQ 94	Microsoft ACPI-Compliant System
IRQ 95	Microsoft ACPI-Compliant System
IRQ 96	Microsoft ACPI-Compliant System
IRQ 97	Microsoft ACPI-Compliant System
IRQ 98	Microsoft ACPI-Compliant System
IRQ 99	Microsoft ACPI-Compliant System

D.3 1st MB Memory Map

Table D.3: 1st MB Memory Map

Addr. Range (Hex)	Device
0x90000000-0xA5FFFFFF	PCI Express Root Complex
0xA0000000-0xA40FFFFFF	CDF PCIeRP[8] - 18AD
0xA0000000-0xA40FFFFFF	PCI Express to PCI/PCI-X Bridge
0xA0000000-0xA40FFFFFF	ASPEED Graphics Family (WDDM)
0xA0000-0xBFFFF	PCI Express Root Complex
0xA4000000-0xA401FFFF	ASPEED Graphics Family (WDDM)
0xA4100000-0xA43FFFFFF	CDF PCIeRP[9] - 18AE
0xA42FC000-0xA42FFFFFF	Intel® Ethernet Controller (3) I225-IT
0xA4300000-0xA43FFFFFF	Intel® Ethernet Controller (3) I225-IT
0xA4400000-0xA44FFFFFF	CDF PCIeRP[7] - 18AB
0xA447C000-0xA447FFFF	Intel® I210 Gigabit Network Connection
0xA4480000-0xA44FFFFFF	Intel® I210 Gigabit Network Connection
0xA4580000-0xA45FFFFFF	Intel® PMON MSM Registers - 09A7
0xA4600000-0xA467FFFF	Intel® PMON MSM Registers - 09A7
0xA4680000-0xA4681FFF	Standard SATA AHCI Controller
0xA4682000-0xA4683FFF	Intel® MSM Registers - 09A6
0xA4687000-0xA46877FF	Standard SATA AHCI Controller
0xA4688000-0xA46880FF	Standard SATA AHCI Controller
0xA5FFFD00-0xA5FFFDFF	CDF HSUART - 18D8 (COM5)
0xA5FFFE00-0xA5FFFEFF	CDF HSUART - 18D8 (COM4)
0xA5FFFF00-0xA5FFFFFF	CDF HSUART - 18D8 (COM3)
0xA6000000-0xBB7FFFFFF	PCI Express Root Complex
0xBB800000-0xD0FFFFFF	PCI Express Root Complex
0xC8000-0xCFFFF	PCI Express Root Complex
0xD1000000-0xE67FFFFFF	PCI Express Root Complex
0xD8000000-0xFC4FFFFFF	PCI Express Root Port
0xE6300000-0xE66FFFFFF	PCI Express Root Port
0xE6800000-0xFB7FFFFFF	PCI Express Root Complex
0xFD000000-0xFD69FFFF	Motherboard resources
0xFD6F0000-0xFDFFFFFF	Motherboard resources
0xFDC20000-0xFDC21FFF	CDF GPIO Controller - 3001
0xFDC50000-0xFDC51FFF	CDF GPIO Controller - 3001
0xFE000000-0xFE01FFFF	Motherboard resources
0xFE010000-0xFE010FFF	CDF SPI - 18E0
0xFE010000-0xFE010FFF	PCI Express Root Complex
0xFE200000-0xFE7FFFFFF	Motherboard resources
0xFEC00000-0xFECFFFFFF	Advanced programmable interrupt controller
0xFED00000-0xFED003FF	High-precision event timer
0xFF000000-0xFFFFFFFF	Motherboard resources
0xFF000000-0xFFFFFFFF	Motherboard resources
0xFFA00000-0xFFA1FFFF	CDF PCIeRP[9] - 18AE
0xFFA20000-0xFFA3FFFF	CDF PCIeRP[8] - 18AD
0xFFA40000-0xFFA5FFFF	CDF PCIeRP[7] - 18AB

Table D.3: 1st MB Memory Map	
0xFFA80000-0xFFA8FFFF	Intel® USB 3.0 eXtensible Host Controller - 1.0 (Microsoft)
0xFFAB7000-0xFFAB7FFF	CDF ME:HECI#3 - 18D6
0xFFAB8000-0xFFAB8FFF	CDF ME:HECI#1 - 18D3

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com

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

All product specifications are subject to change without notice.

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

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

© Advantech Co., Ltd. 2024