

# **User Manual**

# ARK-2251

Fanless Embedded Box Computer



# Attention!

Please note:

This package contains a hard-copy user manual in Chinese for China CCC certification purposes. There is an English user manual included as a PDF file on the CD. Please disregard the Chinese hard copy user manual if the product is not to be sold and/or installed in China.

# Copyright

The documentation and the software included with this product are copyrighted 2023 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. 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, which may result from its use.

# **Acknowledgments**

Award is a trademark of Award Software International, Inc.

VIA is a trademark of VIA Technologies, Inc.

IBM, PC/AT, PS/2 and VGA are trademarks of International Business Machines Corporation.

Intel® and Pentium® are trademarks of Intel Corporation.

Microsoft Windows® is a registered trademark of Microsoft Corp.

RTL is a trademark of Realtek Semi-Conductor Co., Ltd.

ESS is a trademark of ESS Technology, Inc.

UMC is a trademark of United Microelectronics Corporation.

SMI is a trademark of Silicon Motion, Inc.

Creative is a trademark of Creative Technology LTD.

CHRONTEL is a trademark of Chrontel Inc.

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

For more information about this and other Advantech products, please visit our website at:

http://www.advantech.com/

https://www.advantech.com/products/fanless-embedded-computers/sub\_1-2jkeuf

For technical support and service, please visit our support website at: http://support.advantech.com.tw/support/

Part No. 2006225101

Edition 2 January 2024

# **Product Warranty (2 years)**

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

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which 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 of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For outof-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

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

# **Declaration of Conformity**

### FCC Class B

Note: 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 instructions, 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 help.

# **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 you call:
  - 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, which if not observed, can cause personal injury!



Les avertissements indiquent des conditions qui, si elles ne sont pas respectées, peuvent entra?ner des blessure!



**Caution!** Cautions are included to help prevent hardware damage and data losses.



Des précautions sont incluses pour vous aider à éviter d'endommager le matériel ou de perdre Les données.



Notes provide optional additional information.

Les remarques fournissent des informations supplémentaires facultatives.

# **Packing List**

Before installation, please ensure the following items have been shipped:

- 1 x ARK-2251 Unit
- 1 x User Manual (Simplified Chinese)
- 1 x Wrench for top cover
- 1 x Mounting kit
- 1 x Bracket & thermal pad for M.2 M Key SSD (NVMe)
- 1 x WISE-DeviceOn
- 1 x McAfee Application Control Lite/Acronis Backup 11.7 for Windows PC
- 1 x 3-pin plug-in block for power in
- 1 x 4-pin terminal block for switch
- 1 x 6-pin terminal block for Canbus

# **Ordering Information**

Model Number	Description
ARK-2251-S2A1	Intel® Core™ i3-1315UE 1.2G+3GbE+6USB+6COM
ARK-2251-S2A1U	Intel® Core™ i3-1315UE 1.2G+3GbE+6USB+6COM
ARK-2251-S3A1	Intel® Core™ i5-1335UE 1.3G+3GbE+6USB+6COM
ARK-2251-S3A1U	Intel® Core™ i5-1335UE 1.2G+3GbE+6USB+6COM

# **Optional Accessories**

Part Number	Description
96PSA-A120W24T2-4	AC to DC adapter, 24V/120W
96PSA-A150W24T2-4	AC to DC adapter, 24V/150W
1702002600	Power cable 3-pin 183 cm, USA type
1702002605	Power cable 3-pin 183 cm, EU type
1702031801	Power cable 3-pin 183 cm, UK type
170000237	Power cable 3-pin 183 cm, PSE type
1700024369-01	1M HDMI cable
1700031560-01	1.8M HDMI cable

# **Safety Instructions**

- 1. Read these safety instructions carefully.
- 2. Retain this user manual for future reference.
- 3. Disconnect the equipment from all AC outlets before cleaning. Use only a damp cloth for cleaning. Do not use liquid or spray detergent.
- 4. For pluggable equipment, the power outlet should be 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 power outlet sockets should have grounded connections.
- 8. Position the power cord away from high-traffic areas. Do not place anything over the power cord.
- 9. All cautions and warnings on the equipment should be noted.
- 10. If the equipment is not used for a long time, disconnect the equipment from the power source to avoid damage from transient over-voltage.
- 11. Never pour liquid into an opening as this can cause fire or electrical shock.
- 12. Never open the equipment. For safety reasons, only qualified service personnel should open the equipment.
- 13. If one of the following occurs, have the equipment checked by service personnel:
  - The power cord or plug is damaged.
  - Liquid has penetrated into 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.
- 14. 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 cause damage. The equipment should be stored in a controlled environment.
- 15. Any unverified component may cause unexpected damage. To ensure correct installation, always use the components (e.g., screws) provided in the accessory box.
- 16. CAUTION: The equipment is equipped with a battery-powered real-time clock circuit. There is a risk of explosion if a battery is incorrectly replaced. Replace only with same or equivalent type as recommended by the manufacturer. Discard all used batteries according to the manufacturer's instructions.
- 17. Always disconnect the power cord from the chassis before manually handling the hardware. Do not implement connections or configuration changes while the device is powered on. Sudden power surges may damage sensitive electronic components.
- 18. In accordance with IEC 704-1:1982 specifications, the sound pressure level at the operator's position should not exceed 70 dB (A).
- 19. DISCLAIMER: These instructions are provided according to IEC 704-1 specifications.

Advantech disclaims all responsibility for the accuracy of any statements contained herein.

20. The product is intended to be supplied by an UL listed power Supply suitable for use at minimum Tma 60 °C which output is rated: 12-24Vdc, 7.5-3.75A min. If need further assistance, please contact Advantech for further information.

- 21. RESTRICTED ACCESS AREA: The equipment should only be installed in a Restricted Access Area.
- 22. The PoE is to be connected only to PoE networks without routing to the outside plant.

# **Consignes de Sécurité**

- 1. Veuillez lire attentivement ces instructions de sécurité.
- 2. Veuillez conserver ce manuel de l'utilisateur pour référence ultérieure.
- 3. Veuillez débrancher cet équipement de la prise secteur avant le nettoyage. Utilisez un chiffon humide. Ne pas utiliser de détergent liquide ou pulvérisé pour le nettoyage. Utilisez une feuille ou un chiffon humide pour le nettoyage.
- 4. Pour les équipements enfichables, la prise de courant doit être à proximité de l'équipement et doit être facilement accessible.
- 5. S'il vous plaît garder cet équipement de l'humidité.
- 6. Posez cet équipement sur une surface fiable lors de l'installation. Une chute ou une chute pourrait causer des blessures.
- 7. Au moyen d'un cordon d'alimentation connecté à une prise de courant avec mise à la terre.
- 8. Placez le cordon d'alimentation de sorte que personne ne puisse marcher dessus. Ne placez rien sur le cordon d'alimentation.
- 9. Tous les avertissements et mises en garde sur l'équipement doivent être notés.
- 10. Si l'appareil n'est pas utilisé pendant une longue période, débranchez-le du secteur pour ne pas être endommagé par une surtension transitoire.
- 11. Ne jamais verser de liquide dans les ouvertures de ventilation; Cela pourrait provoquer un incendie ou un choc électrique.
- 12. N'ouvrez jamais l'équipement. Pour des raisons de sécurité, seul le personnel de maintenance qualifié doit ouvrir l'équipement.
- 13. Si l'une des situations suivantes se présente, faites vérifier le matériel par le personnel de service:
  - Le cordon d'alimentation ou la fiche est endommagé.
  - Un liquide a pénétré dans l'appareil.
  - L'équipement a été exposé à l'humidité.
  - L'équipement ne fonctionne pas bien ou vous ne pouvez pas le faire. fonctionner conformément au manuel d'utilisation.
  - Equipment L'équipement est tombé et a été endommagé.
  - Equipment L'équipement présente des signes évidents de rupture.
- 14. Ne laissez pas cet équipement dans un environnement où la température de stockage peut être inférieure à -40 °C (-40 °F) ou supérieure à 85 °C (185 °F). Cela pourrait endommager l'équipement. L'équipement doit être dans un environnement contrôlé.
- 15. Tout composant non vérifié peut causer des dommages inattendus. Pour garantir une installation correcte, veuillez toujours utiliser les composants (ex. Vis) fournis avec la boîte d'accessoires.
- 16. ATTENTION: L'ordinateur est équipé d'un circuit d'horloge temps réel alimenté par batterie. Il y a un risque d'explosion si la batterie est remplacée de manière incorrecte. Remplacez uniquement avec le même type ou un type équivalent recommandé par le fabricant. Jetez les piles usagées conformément aux instructions du fabricant.
- 17. Débranchez toujours complètement le cordon d'alimentation de votre châssis lorsque vous utilisez du matériel. Ne faites pas de connexion quand l'appareil

est sous tension. Les composants électroniques sensibles peuvent être endommagés par des surtensions soudaines.

- 18. Niveau de pression acoustique au poste de l'opérateur selon la norme CEI 704-1: 1982 n'est pas supérieur à 70 dB (A).
- 19. AVERTISSEMENT: Cet ensemble d'instructions est donné conformément à la norme CEI 704-1. Advantech décline toute responsabilité quant à l'exactitude des déclarations contenues dans ce.
- 20. Ce produit est destiné à être alimenté par un bloc d'alimentation homologué UL adapté à une utilisation à Tma 50 degrés C min. dont la sortie est conforme à PS2 (ou LPS), ES1 (ou SELV) et dont la sortie est nominale: 9-36Vdc, 16.65-4.16A, si besoin d'aide supplémentaire, veuillez contacter Advantech pour plus d'informations.
- N'ouvrez jamais l'équipement. Pour des raisons de sécurité, l'équipement ne doit être ouvert que par du personnel de service qualifié (Par personne qualifiée).
- 22. Le PoE doit être connecté uniquement aux réseaux PoE sans routage vers l'installation extérieure.

# Contents

Chapter	1	General Introduction1
	11	Introduction 2
	1.2	Product Specifications
		1.2.1 Processor System
		1.2.2 Memory
		1.2.3 Socket
		1.2.4 Graphics
		1.2.5 Ethernet
		1.2.6 Audio
		1.2.7 I/O Interface
		1.2.8 Expansion
		1.2.9 Storage
		1.2.10 Other
		1.2.11 Software Support
		1.2.12 Power Requirements
		1.2.13 Power Consumption
		1.2.14 Mechanical
	4.0	1.2.15 Environment
	1.3	Mechanical Drawing
	1.4	Optional MOS Modules for iDoor Expansion
		Table 1.1: Optional MOS Modules for iDoor Expansion
Chapter	2	Hardware Installation7
	2.1	Introduction
	2.2	Jumpers8
		2.2.1 Jumper Description
		2.2.2 Jumper List
		Table 2.1: Jumper List8
		2.2.3 Jumper Locations
		Figure 2.1 Jumper Layout9
		2.2.4 Jumper Settings
		Table 2.2: CN22 Jumper Setting: AT/ATX Mode
		Table 2.3: JCMOS1 Jumper Setting:Clear CMOS
		Table 2.4: J1 Jumper Setting: Mini PCIe/M.2 E PCIe Switch 10
		Table 2.5: ERP1 Jumper Setting: Power Saving for ERP 10
		Table 2.6: CN20 Jumper Setting: Mini PCIe Power Selection10
		Table 2.7: SW_422_3 Setting: RS-485/RS-422 Failsafe11
		Table 2.8: SW_422_4 Setting: RS-485/RS-422 Failsafe11
		Table 2.9: SW_422_5 Setting: RS-485/RS-422 Failsafe11
		Table 2.10:SW_422_6 Setting: RS-485/RS-422 Failsafe 12
	2.3	System IO
	<b>.</b>	Figure 2.2 ARK-2251 Front and Rear I/O Connector Diagram 12
	2.4	External I/O
		2.4.1 Power Un/Uff Button
		Figure 2.3 Power UN/UFF Button
		2.4.2 Power input Connector
		Figure 2.4 Power input Connector
		2.4.3 Etnernet Connector (LAN)
		Figure 2.5 Ethernet Connector (LAN)
		apie 2.11: Etnemet Connector (LAN) PIN Definition
		2.4.4 USB 3.1 Connector
		14 I able 2.12.056 3.1 PIN Definition

2.4.5	Audio Connector	14
	Figure 2.7 Audio Connector	14
2.4.6	COM Connector	14
	Figure 2.8 COM Connector	14
	Table 2.13: COM Connector PIN Definition	15
2.4.7	HDMI Connector	15
	Figure 2.9 HDMI Connector	15
	Table 2.14: HDMI Connector PIN Definition	15
2.4.8	DIO Connector	16
	Figure 2.10DIO Connector	16
	Table 2.15: DIO Connector PIN Definition	16
2.4.9	Remote Switch Connector	16
	Figure 2.11Remote Switch Connector	16
	Table 2.16: Remote Switch Connector PIN Definition	16
2.4.10	CANBus	17
	Figure 2.12Canbus Connector	17
	Table 2.17: CANBus Connector PIN Definition	17
Installa	tion	17
2.5.1	M.2 Installation	17
2.5.2	Memory Installation	20
2.5.3	mPCIe/mSATA Installation	21
2.5.4	Adapter Installation	22
2.5.5	Wall Mount Installation	23
2.5.6	PoE Installation	24

# 

Introdu	ction	. 28
Enterin	g BIOS Setup	. 28
3.2.1	Main Setup	. 28
3.2.2	Advanced BIOS Features Setup	. 29
3.2.3	Chipset Configuration	. 82
3.2.4	Security	. 98
3.2.5	Boot	100
3.2.6	Save & Exit	101
3.2.7	MEBx	102

2.5

3.1 3.2



# **General Introduction**

This chapter details background information on the ARK-2251 series.

# 1.1 Introduction

ARK-2251 is a compact, fanless, embedded system that features an 13th Gen Intel® Core™ i processor and essential I/O for easy access and installation.

### **Rugged Design with Compact Dimension**

ARK-2251 is equipped with a dual channel memory slot that supports up to 64GB of DDR5 4800 MHz SO-DIMM. Designed for operation in harsh industrial environments, this ruggedized system supports a wide operating temperature range (-20 ~ 60°C/-4 ~ 140°F) and wide input power range (12 ~ 24 VDC). The system I/O includes 6 x USB 3.1 Gen1 (2 x are independent), 6 x RS232/422/485, 2 x 10/100/1000/2500 Mbps LAN ports, and 1 x 10/100/1000 Mbps LAN port, as well as 1 x Mic In and Line Out, 2 x HDMI. ARK-2251 also features 1 x full-sized mPCIe, 1 x mSATA (shared with mPCIe), 1 x M.2 2230 E key, 1 x M.2 2280 M key which support NVME.

### Built-In Intelligent Management Tools – Advantech iEdge

Advantech's iEdge platform, together with McAfee and Acronis, provides a valuable suite of programmable APIs - such as a multi-level watchdog, hardware monitor, system restore, and other user-friendly interfaces. With the inclusion of iEdge, ARK-2251 can be used for remotely managing, monitoring, configuring, and controlling numerous terminals to ensure easy maintenance and recovery.

# **1.2 Product Specifications**

# 1.2.1 Processor System

- CPU:
  - Core i3-1315UE
  - Core i5-1335UE

### Frequency:

- Core i3-1315UE: 1.2 GHz turbo boost up to 4.5 GHz
- Core i5-1335UE: 1.3 GHz turbo boost up to 4.5 GHz
- Core Number:
  - Core i3-1315UE: 2P + 4E
  - Core i5-1335UE: 2P + 8E
- BIOS: AMI EFI 256 Mbit

### 1.2.2 Memory

- Technology: DDR5 4800 Mhz
- Max capacity: Up to 64 GB

### **1.2.3 Socket**

Socket: 2 x Dual Channel DDR5 4800 MHz 262 pin SO-DIMM (no support ECC)

### **1.2.4 Graphics**

- Chipset: Intel® Iris® Xe graphics
- **HDMI 2.0b:** Up to 4096 x 2160 @ 60Hz
- Dual Display: 2 x HDMI

# 1.2.5 Ethernet

- LAN1: 10/100/1000 Mbps Intel i219 GbE, supports Wake On LAN
- LAN2: 10/100/1000/2500 Mbps Intel i226 GbE, supports Wake On LAN
- LAN3: 10/100/1000/2500 Mbps Intel i226 GbE, supports Wake On LAN
- POE Load (optional): LAN2 & LAN3: 15.4W per port

# 1.2.6 Audio

Interface: Realtek ALC888S, High Definition Audio, Mic-in, Line-out

### 1.2.7 I/O Interface

- Serial Ports: 6 x RS-232/422/485 with auto flow control
- **USB Ports:** 6 x USB 3.1 Gen1 (2 x are independent)
- **GPIO:** 8-bit programmable DIO
- CANbus: 2 x CANBus

### 1.2.8 Expansion

- Mini PCle: 1 x full-sized mPCle
- M.2: 1 x M2. 2230 E key and 1 x M.2 2280 M key

### 1.2.9 Storage

- **NVME:** 1x M.2 M Key supporting NVME
- mSATA: Shared with mPCle

### 1.2.10 Other

- WatchDog Timer: 255 levels timer interval, setup by software
- **TPM:** TPM 2.0 (project supported by AMO-I029)

### 1.2.11 Software Support

- Microsoft Windows: Windows 10
- Linux: Ubuntu 22.04, others by project support

### **1.2.12 Power Requirements**

- Power Type: ATX/AT
- Power Input Voltage: 12-24 V<sub>DC</sub>, 10A- 5A
- Power Adapter: AC to DC, 12-24 V<sub>DC</sub>,10A- 5A, 120W (150W for adding PoE Module)

### **1.2.13 Power Consumption**

- Typical: (OS idle mode) 19.05W for ARK-2251-S2A1, 19.30W for ARK-2251-S3A1, 19.47W for ARK-2251-S7A1
- Max.: (full loading) 38.21W for ARK-2251-S2A1, 41.23W for ARK-2251-S3A1, 42.13W for ARK-2251-S7A1

# 1.2.14 Mechanical

- **Construction:** Aluminum housing
- Mounting: Wall mounting
- Dimensions (W x H x D): 260 x 54 x 140.2 mm (10.24" x 2.13" x 5.52")
- Weight: 2.3KG

# 1.2.15 Environment

- Operating Temperature: With extended temp. peripherals: -20 ~ 60°C with 0.7m/s air flow (only up to 40°C when using with the adapter).
- **Storage Temperature:** -40~85°C (-40 ~ 185°F)
- **Relative Humidity:** 95% @ 40 °C (non-condensing)
- Vibration during Operation: 3 Grms, IEC60068-2-64, random, 5~500 Hz, and 1hr/axis (with Wall Mount)
- Shock during Operation: 30 G, IEC-60068-2-27, half sine, 11 ms duration (with Wall Mount)
- EMC: CE/FCC Class B, CCC, and BSMI
- Safety: UL, CB, CCC, and BSMI

# **1.3 Mechanical Drawing**







# **1.4 Optional MOS Modules for iDoor Expansion**

# Table 1.1: Optional MOS Modules for iDoor Expansion

Part Number	Description
MOS-2230-Z1201E	CANBus module, 2-Ch, USB Interface
MOS-2220-X1101E	Parallel LPT module, 1-Ch, USB Interface
MOS-2110Z-1201E	USB module, 2-Ch, PCle Interface
MOS-2120-Z1101E	Giga LAN Ethernet module, 1-Ch, PCIe Interface
MOS-1120Y-0202E	Isolated RS-232, 2-Ch, DB9, PCIe Interface
MOS-1121Y-0202E	Isolated RS-422/485, 2-Ch, DB9, PCIe Interface
MOS-1120Y-1402E	Non-Isolated RS-232, DB37, 4-Ch, PCIe Interface
MOS-1130Y-0201E	Isolated CANBus, 2-Ch, DB9, PCIe Interface
MOS-1110Y-0101E	Isolated 16 DI/8 DO, 1-Ch, DB37, PCIe Interface
MOS-2120-Z1201	Dual Intel I210 GbE LAN iDoor, 2-Ch, PCle I/F
MOS-2220-Z1101E	High-speed Serial COM module, 1-Ch, USB Interface

6



Hardware Installation

# 2.1 Introduction

This chapter details instructions for installing the ARK-2251 series. The following sections show the internal jumper settings and the external connector pin assignments.

**Note!** Hardware installation must be performed by the skilled personnel



# 2.2 Jumpers

# 2.2.1 Jumper Description

Configure the ARK-2251 to meet specific application needs by adjusting jumpers. A jumper, functioning as a metal bridge, closes an electric circuit. It typically comprises two metal pins and a small metal clip, often protected by plastic. To close a jumper, connect the pins with the clip, and to open it, remove the clip. In cases where a jumper has three pins labeled 1, 2, and 3, connect either pins 1 and 2 or 2 and 3.



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



A pair of needle-nose pliers may be helpful when working with jumpers. If you have any doubts about the best hardware configuration for your application, contact your local distributor or sales representative before you make any changes. Generally, you simply need a standard cable to make most connections.

# 2.2.2 Jumper List

Table 2.1: Jumper List			
Location	Function		
CN22	AT/ATX Mode		
JCMOS1	Clear CMOS		
J1	Mini PCIe/M.2 E PCIe Switch		
ERP1	Power Saving for ERP		
CN20	Mini PCIe Power Selection		
SW_422_3	RS-485/RS-422 Failsafe		
SW_422_4	RS-485/RS-422 Failsafe		
SW_422_5	RS-485/RS-422 Failsafe		
SW_422_6	RS-485/RS-422 Failsafe		

# 2.2.3 Jumper Locations



Figure 2.1 Jumper Layout

0

SW\_422-5 SW\_422-6

000

# 2.2.4 Jumper Settings

Table 2.2: CN22 Jumper Setting: AT/ATX Mode			
Pin	Description		
1-2	ATX Mode (default)		
3-4	AT Mode		



A

CN20

3

0

Table 2.3: JCMOS1 Jumper Setting:Clear CMOS			
PIN	Description		
1-2	Normal (default)		
2-3	Clear CMOS		



Table 2.4: J1 Jumper Setting: Mini PCle/M.2 E PCle Switch			
PIN	Description		
1-2	Mini PCIe		
2-3	M.2 E (default)		



Table 2.5: ERP	Jumper Set	ting: Power	Saving for ERP
----------------	------------	-------------	----------------

PIN	Description
1-2	ERP Disable (default)
3-4	ERP Enable



Table 2.6: CN20 Jumper Setting: Mini PCIe Power Selection		
PIN	Description	
1-2	Mini PCIe VCC=3.8V	
3-4	Mini PCIe VCC=3.3V (default)	



# Table 2.7: SW\_422\_3 Setting: RS-485/RS-422 Failsafe

PIN	Description	
1-8, 2-7, 3-6, 4-5	Enable COM3 failsafe	
1-8, 2-7, 3-6, 4-5	Disable COM3 failsafe (default)	



### Table 2.8: SW\_422\_4 Setting: RS-485/RS-422 Failsafe

PIN	Description
1-8, 2-7, 3-6, 4-5	Enable COM4 failsafe
1-8, 2-7, 3-6, 4-5	Disable COM4 failsafe (default)



Table 2.9: SW_422_5 Setting: RS-485/RS-422 Failsafe		
PIN	Description	
1-8, 2-7, 3-6, 4-5	Enable COM5 failsafe	
1-8, 2-7, 3-6, 4-5	Disable COM5 failsafe (default)	

5	 4
6	3
7	2
8	1

PIN	Description	
1-8, 2-7, 3-6, 4-5	Enable COM6 failsafe	
1-8, 2-7, 3-6, 4-5	Disable COM6 failsafe (default)	



# 2.3 System IO



Figure 2.2 ARK-2251 Front and Rear I/O Connector Diagram

# 2.4 External I/O

# 2.4.1 Power On/Off Button

ARK-2251 features a power on/off button with an LED indicator on top that shows on status (ON: Green LED, OFF: Orange LED).



# 2.4.2 Power Input Connector

The power input connector supports 12  $\sim$  24 V. The 3 pins are defined as +, -, and GND.



### Figure 2.4 Power Input Connector

# 2.4.3 Ethernet Connector (LAN)

ARK-2251 is equipped with two Intel® i226-LM Ethernet controllers connected to LAN2 and LAN3 (Optional for PoE), as well as Intel® i219 Ethernet controllers connected to LAN1. The Ethernet ports provide standard RJ45 jack connectors with LED indicators on the sides to show Active/Link status (Green LED) and speed status (Yellow LED). LAN2 and LAN3 support PoE function by additional MIOe-PSE module(optional). The maximum voltage and rated current output for each PoE port is 50V/ 0.308A, 15.4W.



Figure 2.5 Ethernet Connector (LAN)

Table 2.11: Etherne	et Connector (LAN) PIN Definition
Pin	10/100/1000/2500 Mbps Signal Name
1	BI_DA+(GHz)
2	BI_DA+(GHz)
3	BI_DB+(GHz)
4	BI_DC+(GHz)
5	BI_DC-(GHz)
6	BI_DB-(GHz)
7	BI_DD+(GHz)
8	BI_DD-(GHz)
H3	GND
H4	GND

\* LAN 2 and 3 are up to 2.5G, while LAN 1 is up to 1G.

# 2.4.4 USB 3.1 Connector

ARK-2251 supports 6 x USB 3.1 Gen 1 (2x are independent) interfaces, which support plug-and-play functionality and hot swapping for external devices. The USB interfaces comply with USB UHCI, Rev. 3.0.



### Figure 2.6 USB 3.1 Connector

Table 2.12: USB 3.1 PIN Definition		
Pin	Signal Name	
1	+5V	
2	D0	
3	D+_0	
4	GND	
5	USB0_SSRX-	
6	USB0_SSRX+	
7	GND	
8	USB0_SSTX-	
9	USB0_SSTX+	

### 2.4.5 Audio Connector

ARK-2251 supports stereo Line-Out and Mic- In audio ports. The audio chip is controlled by ALC888S and compliant with Azalea standards.



### Figure 2.7 Audio Connector

### 2.4.6 COM Connector

ARK-2251 provides six 9-pin D-sub connectors, which support RS-232/422/485 serial communication interface ports. The default setting is RS-232, if you want to use RS-422/485, you can change the setting in BIOS.



Figure 2.8 COM Connector

Table 2.13: COM Connector PIN Definition			
Pin	RS-232	RS-422	RS-485
1	DCD	Tx-	DATA-
2	RxD	Tx+	DATA+
3	TxD	Rx+	NC
4	DTR	Rx-	NC
5	GND	GND	GND
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

NC represents "No Connection"

# 2.4.7 HDMI Connector

ARK-2251 offers 2 x integrated 19-pin receptacle connector HDMI 2.0b interfaces. The HDMI link supports resolutions up to 4096x2160 @60 Hz.



### Figure 2.9 HDMI Connector

Table 2.14: HDMI Connector PIN Definition		
Pin	Signal Name	
1	HDMI_TX2+	
2	GND	
3	HDMI_TX2-	
4	HDMI_TX1+	
5	GND	
6	HDMI_TX1-	
7	HDMI_TX0+	
8	GND	
9	HDMI_TX0-	
10	HDMI_CLK+	
11	GND	
12	HDMI_CLK-	
13	NC	
14	NC	
15	HDMI_DCLK	
16	HDMI_DDAT	
17	GND	
18	+V5_HDMI-HPD	
19	DDP0_HPD	

NC represents "No Connection"

# 2.4.8 DIO Connector

ARK-2251 provides 1 x 8-bit DIO connector.



### Figure 2.10 DIO Connector

Table 2.15: DIO Connector PIN Definition		
Pin	Signal Name	
1	DIO bit 0	
2	DIO bit 1	
3	DIO bit 2	
4	DIO bit 3	
5	DIO bit 4	
6	DIO bit 5	
7	DIO bit 6	
8	DIO bit 7	
9	GND	

# 2.4.9 Remote Switch Connector

ARK-2251 provides a remote switch connector for power on/off via an external cable.



### Figure 2.11 Remote Switch Connector

Table 2.16: Remote Switch Connector PIN Definition			
Pin	Signal Name		
1	WDT		
2	PWRBTN		
3	GND		
4	SYSRST		

# Chapter 2 Hardware Installation

# 2.4.10 CANBus

ARK-2251 provides a 6-pin terminal block for Canbus.



### Figure 2.12 Canbus Connector

Table 2.17: CANBus Connector PIN Definition		
Pin	Signal Name	
1	CAN0_D-	
2	CAN1_D+	
3	GND	
4	GND	
5	CAN0_D+	
6	CAN1_D-	

# 2.5 Installation

This should be performed by skilled personnel.



?!

# 2.5.1 M.2 Installation

For the M.2 E KEY

Loosen the 8 x screws (M3x5L) on the bottom/sides and remove the bottom 1. cover.



- 2. Install the M.2 E Key Module with the screw.
- 3. Put the bottom cover back and secure it with the 8 x screws (M3x5L).



### For the M.2 M KEY

1. Loosen the 8 x screws on the front/sides and remove the bottom cover.



2. Take the bracket with thermal pad and the screw(M3\*5L) out from the accessory box then install it on the right position.



3. Install the M.2 M Key Device on the bracket.



4. Put the bottom cover back and secure it with the 8 x screws.

# 2.5.2 Memory Installation

1. Remove the top cover with the wrench in the accessory box.



2. Carefully install RAM memory into the slots



3. To install a second memory module, apply the thermal pad (located in the accessory box) before installing the memory.



4. Put the top cover back and secure it with the 8x screws

# 2.5.3 mPCIe/mSATA Installation

1. Loosen the 8 x screws on the front/sides and remove the bottom cover.



2. Install mPCLe/mSATA module.



3. Put the bottom cover back and secure it with the 8 x screws.

# 2.5.4 Adapter Installation

1. Connect the 3-pin Phoenix connector to the DC input.





# 2.5.5 Wall Mount Installation

- 1. Unscrew the 4 x M3x5L screws on both sides of ARK- 2251.
- 2. Secure the wall mount brackets on both sides of ARK-2251 using the 4 x screws removed as shown in the above step.
- 1. Dévissez les 4x vis M3x5L ou des deux côtés de l'ARK-2251.
- 2. Vissez les supports de montage mural des deux côtés de l'ARK-2251 avec les quatre vis à l'arrière.



# 2.5.6 **PoE Installation**

1. Remove the top cover with the wrench in the accessory box.


2. Loosen the 8 x screws on the front/sides and remove the bottom cover.



3. Attach the PoE module and then connect the cable to the ARK-2251.







## **BIOS Settings**

This chapter details instructions of setting BIOS configuration data.

## 3.1 Introduction

The AMI BIOS ROM has a built-in setup program - the BIOS Setup Utility - that allows users to modify the basic system configuration. All configuration data is stored in battery-backed CMOS to ensure the setup information is retained when the power is turned off. This chapter describes the basic navigation of the ARK-2251 BIOS setup screens.

## 3.2 Entering BIOS Setup

Turn on the computer and check for the patch code. If there is a number assigned to the patch code, it means that BIOS supports your CPU. If there is no number assigned to the patch code, please contact an Advantech application engineer to obtain an up-to-date patch code file. This will ensure that your CPU's system status is valid. After ensuring that you have a number assigned to the patch code, press <DEL> and you will immediately be allowed to enter Setup.

### 3.2.1 Main Setup

When users first enter the BIOS Setup Utility, they 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.

Main Advanced Chipset	Aptio Setup – AMI Security Boot Save & Exit NVMe RPM	B Key Migration MEBx
BIOS Information BIOS Vendor Core Version Compliancy Project Version Build Date and Time Access Level Project Board Version Power Type Memory Information Total Memory Memory Frequency System Date System Time	American Megatrends 5.0.2.7 0.14 x64 UEFI 2.8; PI 1.7 2251000R060X014 08/14/2023 12:17:14 Administrator ARK-2251 ATX 16384 MB 4800 MT/s [Mon 08/14/2023] [13:21:09]	Set the Date. Use Tab to switch between Date elements. Default Ranges: Year: 2000-2099 Months: 1-12 Days: Dependent on month Range of Years may vary. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	Version 2.22.1290 Copyright (C) 2023	AMI

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 ARK-2251 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.

### 3.2.2.1 WWAN Configuration

	Apt	io Setup – AM	I	
Main Advanced Chipset Security	Boot	Save & Exit	NVMe RPM	B Key Migration MEBx
<ul> <li>&gt; HWAN Configuration</li> <li>&gt; CPU Configuration</li> <li>&gt; Power &amp; Performance</li> <li>&gt; PCH-FW Configuration</li> <li>&gt; Trusted Computing</li> <li>&gt; ACPI Settings</li> <li>&gt; iManager Configuration</li> <li>&gt; NCT5124DSEC Super IO Configuration</li> <li>&gt; SS RTC Wake Settings</li> <li>&gt; Serial Port Console Redirection</li> <li>&gt; Intel TXT Information</li> <li>&gt; PCI Subsystem Settings</li> <li>&gt; USB Configuration</li> <li>&gt; Network Stack Configuration</li> <li>&gt; CSM Configuration</li> <li>&gt; NVMe Configuration</li> </ul>				Configure WWAN related options ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2 22 1	290 Copuright	(0) 2023	амт



### WWAN DEVICE

Select the M.2 WWAN Device options to enable 4G - 7360/7560 (Intel), 5G - M80 (MediaTek) Modems

### 3.2.2.2 CPU Configuration

Main Advanced Chipset Security	Aptio Setup – AMI Boot Save & Exit N\	VMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>OPU Configuration</li> <li>POUPT Series A Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>		CPU Configuration Parameters ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1290 Copyright ((	C) 2023 AMI

### **Efficient-core Information**

Advanced	Aptio Setup – AMI	
CPU Configuration		Displays the E-core Information
CPU Configuration Efficient-core Information Performance-core Information Brand String ID Microcode Revision VMX SMX/TXT TXT Crash Code TXT SPAD Boot Guard Status Boot Guard Status Boot Guard SACM Information C6DRAM CPU Elevy Batic Queppide	13th Gen Intel(R) Core(TM) 15-1335UE 0x806A3 4114 Supported Supported 0x0000000 0x9040000000000000 0x0000000000	<ul> <li>▲ Displays the E-core Information</li> <li>★+: Select Screen</li> <li>↑↓: Select Item</li> <li>Enter: Select</li> <li>+/-: Change Opt.</li> <li>F1: General Help</li> <li>F2: General Help</li> <li>F3: General Help</li> </ul>
CPU Flex Ratio Override CPU Flex Ratio Settings Hardware Prefetcher Adjacent Cache Line Prefetch Intel (VMX) Virtualization Technology PECI	[Disabled] 25 [Enabled] [Enabled] [Enabled] [Enabled]	F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit

### Version 2.22.1290 Copyright (C) 2023 AMI

Advanced	Aptio Setup - AMI	
Boot Guard ACM Policy Status Boot Guard SACM Information C6DRAM CPU Flex Ratio Override CPU Flex Ratio Settings Hardware Prefetcher Adjacent Cache Line Prefetch Intel (VMX) Virtualization Technology	0x000000000000000000000000000000000000	Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only
PECT AVX Active Performance-cores Active Efficient-cores Hyper-Threading BIST AP threads Idle Manner AES MachineCheck MonitorMWait Intel Trusted Execution Technology Alias Check Request DPR Memory Size (MB) Reset AUX Content ► CPU SMM Enhancement	[Enabled] [Enabled] [A11] [Enabled] [Disabled] [MWAIT Loop] [Enabled] [Enabled] [Enabled] [Disabled] [Disabled] 4 [no]	<pre> ++: Select Screen  14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Conuright (C) 2023	R AMT

# Chapter 3 BIOS Settings



### C6DRAM

Enable/Disable moving of DRAM contents to PRM memory when CPU is in C6 state.

### CPU Flex Ratio Override

Enable/Disable CPU Flex Ratio Programming.

### CPU Flex Ratio Settings

This value must be between Max Efficiency Ratio (LFM) and Maximum nonturbo ratio set by Hardware (HFM).

### Hardware Prefetcher

To turn on/off the MLC streamer prefetcher.

### Adjacent Cache Line Prefetch

To turn on/off prefetching of adjacent cache lines.

### Intel (VMX) Virtualization Technology

When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

PECI

Enable/Disable PECI.

### AVX

Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only

### Active Performance-Cores

Number of cores to enable in each processor package.

### Active Efficient-cores

Enable/Disable Per Core Disable. When Per Core Disable Configuration is enabled, selction of Active Cores and Active Efficient-cores will be disabled.

### Hyper-Threading

Enable/Disable Hyper-Threading Technology.

BIST

Enable/Disable BIST (Built-in Self Test) on reset

AP threads Idle Manner

AP threads Idle Manner for waiting signal to run.

AES

Enable/Disable AES (Advanced Encryption Standard)

MachineCheck

Enable/Disable Machine Check.

- MonitorMWait Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop
- Intel Trusted Execution Technology Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology.
- Alias Check Request Enables Txt Alias Checking capability.
- DPR memory size (MB)
   Reserve DPR memory size (0-255) MB
- Reset AUX Content Reset TPM Aux content. Txt may not functional after AUX content gets reset.
- L1 Data Cache
   Displays the Efficient-core L1 Data Cache size.
- L1 Instruction Cache
   Displays the Efficient-core L1 Instruction Cache size.
- L2 Cache Displays the Efficient-core L2 Cache size.
- L3 Cache
   Displays the Performance-core L3 Cache size.

### Power and Performance – CPU Power Management Control

Advanced	Aptio Setup – AMI	
CPU Configuration		▲ Displays the P-core Information
<ul> <li>Efficient-core Information</li> <li>Performance-core Information</li> </ul>		
Brand String ID Microcode Revision VMX SMX/TXT TXT Crash Code TXT SPAD Boot Guard Status Boot Guard ACM Policy Status Boot Guard ACM Information C6DRAM CPU Flex Ratio Override CPU Flex Ratio Settings Hardware Prefetcher Odiscent Scaba Line Designth	13th Gen Intel(R) Core(TM) 15-1335UE 0x806A3 4114 Supported Supported 0x00000000 0x9040000000000000 0x0000000000	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit F4: Save &amp; Exit</pre>
Intel (VMX) Virtualization	[Enabled]	E30. EXIL
PECI	[Enabled]	
Versio	n 2.22.1290 Copyright (C)	2023 AMI

Advanced	Aptio Setup – AMI	
Boot Guard ACM Policy Status Boot Guard SACM Information C6DRAM CPU Flex Ratio Override CPU Flex Ratio Settings Hardware Prefetcher Adjacent Cache Line Prefetch Intel (VMX) Virtualization Technology PECI AVX Active Performance-cores Active Efficient-cores Hyper-Threading BIST AP threads Idle Manner AES MachineCheck MonitorMWait Intel Trusted Execution Technology Alias Check Request DPR Memory Size (MB) Reset AUX Content > CPU SMM Enhancement	Ox000000000000000 Ox00000110000000 [Enabled] 25 [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [All] [All] [All] [Disabled] [Disabled] [Enabled] [Enabled] [Enabled] [Enabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled]	<ul> <li>▲ CPU SMM Enhancement</li> <li>★+: Select Screen</li> <li>↓1: Select Item</li> <li>Enter: Select</li> <li>+/-: Change Opt.</li> <li>F1: General Help</li> <li>F2: Previous Values</li> <li>F3: Optimized Defaults</li> <li>F4: Save &amp; Exit</li> <li>ESC: Exit</li> </ul>
United and a second and a	22 4000 Conuniatet (C)	DODD ANT



Advanced	Aptio Setup – AMI		
CPU SMM Enhancement SMM Use Delay Indication SMM Use Block Indication SMM Use SMM en-US Indication	[Enabled] [Enabled] [Enabled]	Enable/Disable usage of SMM_DELAYED MSR for MP sync in SMI	
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>	
Version 2.22.1290 Copyright (C) 2023 AMI			

### C6DRAM

Enable/Disable moving of DRAM contents to PRM memory when CPU is in C6 state.

# CPU Flex Ratio Override Enable/Disable CPU Flex Ratio Programming.

### CPU Flex Ratio Settings

This value must be between Max Efficiency Ratio (LFM) and Maximum non-turbo ratio set by Hardware (HFM).

### Hardware Prefetcher

To turn on/off the MLC streamer prefetcher.

### Adjacent Cache Line Prefetch

To turn on/off prefetching of adjacent cache lines.

### Intel (VMX) Virtualization Technology

When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

### PECI

Enable/Disable PECI.

### AVX

Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only

### Active Performance-Cores

Number of cores to enable in each processor package.

### Active Efficient-cores

Enable/Disable Per Core Disable. When Per Core Disable Configuration is enabled, selction of Active Cores and Active Efficient-cores will be disabled.

### Hyper-Threading

Enable/Disable Hyper-Threading Technology.

### BIST

Enable/Disable BIST (Built-in Self Test) on reset

### AP threads Idle Manner

AP threads Idle Manner for waiting signal to run.

### AES

Enable/Disable AES (Advanced Encryption Standard)

### MachineCheck

Enable/Disable Machine Check.

### MonitorMWait

Enable/Disable MonitorMWait, if Disable MonitorMwait, the AP threads Idle Manner should not set in MWAIT Loop

### Intel Trusted Execution Technology

Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology.

### Alias Check Request

Enables Txt Alias Checking capability.

### DPR memory size (MB)

Reserve DPR memory size (0-255) MB

### Reset AUX Content Reset TPM Aux content. Txt may not functional after AUX content gets reset.

### L1 Data Cache

Displays the Efficient-core L1 Data Cache size.

### L1 Instruction Cache

Displays the Efficient-core L1 Instruction Cache size.

### L2 Cache

Displays the Efficient-core L2 Cache size.

# Chapter 3 BIOS Settings

### CPU SMM Enhancement

- SMM Use Delay Indication Enable/Disable usage of SMM\_DELAYED MSR for MP sync in SMI.
- SMM Use Block Indication
   Enable/Disable usage of SMM BLOCKED MSR for MP sync in SMI.
- SMM Use SMM en-US Indication
   Enable/Disable usage of SMM\_ENABLE MSR for MP sync in SMI

### 3.2.2.3 Power & Performance



### **CPU - Power Management Control**



	Advanced	Aptio Setup – AMI	
Γ	CPU – Power Management Control		Select the performance state
	Boot performance mode	[Max Non-Turbo Performance]	starting from reset vector.
	Intel(R) SpeedStep(tm)	[Enabled]	
	Race IO Hait (RIH)	[Enabled]	
	Pap Capa B State OS control mode	[Enabled]	
	HuP Autonomous Per Core P State	[Enabled]	
	HuP Autonomous FPP Grouning	[Enabled]	
	EPB override over PECI	[Disabled]	
	HwP Lock	[Enabled]	
	HDC Control	[Enabled]	
	Turbo Mode	[Enabled]	↔: Select Screen
	View/Configure Turbo Options		†↓: Select Item
	CPU VR Settings		Enter: Select
	C states	[Disabled]	+/-: Change Opt.
	Thermal Monitor	[Enabled]	F1: General Help
	Interrupt Redirection Mode	[Fixed Priority]	F2: Previous Values
	Selection		F3: Optimized Defaults
	Timed MWAIT	[Disabled]	F4: Save & Exit
P	Custom P-state Table		ESC: Exit
	EU Turbo Control Mode	[Disabled]	
	Energy Performance Gain		
	EFG DIMM IQUON	20	
	Version 2	2 22 1290 Copunight (C) 2023	ANT

Advanced	Aptio Setup – AMI	
Boot performance mode Intel(R) SpeedStep(tm) Race To Halt (RTH) Intel(R) Speed Shift Technology Per Core P State OS control mode HwP Autonomous Per Core P State HwP Autonomous EPP Grouping EPB override over PECI HwP Lock HDC Control Turbo Mode	[Max Non-Turbo Performance] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Disabled] [Enabled] [Enabled] [Enabled]	▲ Enable/disable Energy Performance Gain.
<ul> <li>View Configure (drbd) options</li> <li>CPU VR Settings</li> <li>C states</li> <li>Thermal Monitor</li> <li>Interrupt Redirection Mode</li> <li>Selection</li> <li>Timed MWAIT</li> <li>Custom P-state Table</li> <li>EC Turbo Control Mode</li> <li>Energy Performance Gain</li> <li>EPG DIMM Idd3N</li> <li>EPG DIMM Idd3P</li> <li>CPU Lock Configuration</li> </ul>	[Disabled] [Enabled] [Fixed Priority] [Disabled] [Disabled] 26 11	<pre></pre>

### Version 2.22.1290 Copyright (C) 2023 AMI

Advanced	Aptio Setup — AMI	
Current Turbo Settings Max Turbo Power Limit Min Turbo Power Limit Package TDP Limit Power Limit 1 Power Limit 2 > Turbo Ratio Limit Options Energy Efficient P-state Package Power Limit MSR Lock Energy Efficient Turbo	4095.875 0.0 15.0 15.0 55.0 [Enabled] [Disabled] [Enabled]	View/Configure Turbo Ratio Limit Options
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version	2.22.1290 Copyright (C) 202	3 AMI

Advanced	Aptio Setup – AMI	
CPU VR Settings Current VccIn Aux Icc Max PSYS Slope PSYS Offset PSYS Prefix PSYS PMax Power Min Voltage Override VccIn Aux ICC Max VccIn Aux IMON Slope VccIN Aux IMON Slope VccIN Aux IMON Prefix Vsys/Psys Critical Assertion Deglitch Mantissa Assertion Deglitch Exponent De assertion Deglitch Exponent De assertion Deglitch Exponent VR Power Delivery Design Acoustic Noise Settings Core/IA VR Settings RFI Settings	128 0 (+) 0 [Disabled] 0 100 0 (+) [Disabled] 1 1 0 13 2 [AUTO]	<pre>PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9.  ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Versio	n 2.22.1290 Copyright (C) 20	23 AMI

Advanced	Aptio Setup – AMI	
Acoustic Noise Settings		Enabling this option will help
Acoustic Noise Mitigation	[Disabled]	certain SKUs when the CPU is
Pre Wake Time	0	in deeper C state
Ramp Up Time	0	
Ramp Down Time	0	
IA VR Domain		
Disable Fast PKG C State Ramp for	[FALSE]	
IA Domain Slav Slav Data (an IS Damain	[[/0]	
Slow Slew Rate for IA Domain	[Fast/2]	
GT VR Domain		
Disable Fast PKG C State Ramp for	[FALSE]	↔: Select Screen
GT Domain		↑↓: Select Item
Slow Slew Rate for GT Domain	[Fast/2]	Enter: Select
		+/-: Change Opt.
		F1: General Help
		F2: Previous Values
		F3: Optimized Defaults
		F4: Save & Exit
		ESC: Exit
Version 2	2.22.1290 Copyright (C) 2023	AMI

Advanced	Aptio Setup – AMI	
Core/IA VR Domain		▲ VR Config Enable
VR Config Enable Current AC Loadline Current DC Loadline Current Psil Threshold Current Psi2 Threshold Current Psi3 Threshold Current Imon Slope Current Imon Offset Current VR Current Limit Current VR Current Limit Current Voltage Limit AC Loadline DC Loadline PS Current Threshold1 PS Current Threshold2 PS Current Threshold3 PS3 Enable PS4 Enable IMON Slope IMON Offset IMON Prefix VR Current Limit Core VR Fast Vmode	[Enabled] 280 80 20 4 0 1 320 384 1600 0 0 80 20 4 [Enabled] [Enabled] 0 1 [Enabled]	<pre>**: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>

Advanced	Aptio Setup — AMI	
Current Psi3 Threshold Current Imon Slope Current Imon Offset Current VR Current Limit Current Tdc Current Limit Current Voltage Limit AC Loadline DC Loadline PS Current Threshold1 PS Current Threshold2 PS Current Threshold3 PS3 Enable PS4 Enable	4 ▲ 0 1 320 384 1600 0 0 80 20 4 [Enabled] [Enabled]	Enable/Disable IRMS – Current root mean square
IMON Slope IMON Offset IMON Prefix VR Current Limit Core VR Fast Vmode Fast Vmode Itrip ICC Limit VR Voltage Limit TDC Enable TDC Current Limit TDC Time Window TDC Lock IRMS	0 0 [+] 0 [Enabled] 260 0 [Enabled] 0 [1 sec] [Disabled] [Disabled]	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>

	Aptio Setup – AMI	
Advanced		
GT Domain		▲ VR Config Enable
VR Config Enable Current AC Loadline Current DC Loadline Current Psil Threshold Current Psil2 Threshold Current Psil3 Threshold Current Tmon Slope Current Imon Offset Current VR Current Limit Current VR Current Limit Current Voltage Limit AC Loadline DC Loadline PS Current Threshold1 PS Current Threshold2 PS Current Threshold3 PS3 Enable PS4 Enable IMON Slope IMON Offset IMON Offset IMON Prefix VR Current Limit GT VR Fast Vmode	[Enabled] 320 320 80 20 4 0 1 160 184 1500 0 0 80 20 4 [Enabled] [Enabled] 0 0 [+] 0 [Disabled]	<pre>**: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>

Version 2.22.1290 Copyright (C) 2023 AMI

Advanced	Aptio Setup – AMI	
Current Psi1 Threshold Current Psi2 Threshold Current Psi3 Threshold Current Imon Slope Current Imon Offset Current VR Current Limit Current VG Current Limit Current Voltage Limit AC Loadline DC Loadline PS Current Threshold1 PS Current Threshold2 PS Current Threshold3 PS3 Enable PS4 Enable IMON Slope IMON Offset IMON Offset IMON Offset IMON Prefix VR Current Limit GT VR Fast Vmode VR Voltage Limit TDC Enable TDC Current Limit TDC Time Window TDC Lock	80 20 4 0 1 160 184 1500 0 0 80 20 4 [Enabled] [Enabled] 0 [Lisabled] 0 [Enabled] 0 [Lisabled] [Lisabl	<ul> <li>TDC Lock</li> <li>TDC Lock</li> <li>**: Select Screen</li> <li>11: Select Item</li> <li>Enter: Select</li> <li>+/-: Change Opt.</li> <li>F1: General Help</li> <li>F2: Previous Values</li> <li>F3: Optimized Defaults</li> <li>F4: Save &amp; Exit</li> <li>ESC: Exit</li> </ul>
	Vancian 2 22 1280 Conunight (C	THA COOL





Advanced	Aptio Setup — AMI	
CFG Lock Overclocking Lock	[Enabled] [Enabled]	Configure MSR OxE2[15], CFG Lock bit
		++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1290 Copyright (C) 2023	AMI

### Boot performance mode

Select the performance state that the BIOS will set before OS hand-off.

### Intel ® SpeedStep (tm)

Allows more than two frequency ranges to be supported.

### Race To Halt (RTH)

Enable/Disable Race To Halt feature. RTH will dynamically increase CPU frequency in order to enter pkg C-State faster to reduce overall power. (RTH is controlled through MSR 1FC bit 20)

### Intel ® SpeedStep Shift Technology

Enable/Disable Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.

### Per Core P State OS Control mode

Enable/Disable Per Core P state OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core requests.

### HwP Autonomous Per Core P State

Disable Autonomous PCPS (Bit 30 = 1, command 0x11) Autonomous will request the same value for all cores all the time. Enable PCPS (default Bit 30 = 0, command 0x11)

### HwP Autonomous EPP Grouping

Enable EPP grouping (default Bit 29 =0, command 0x11) Autonomous will request the same values for all cores with same EPP. Disable EPP grouping (Bit 29 =1, command 0x11) autonomous will not necessarily request same values for all cores with

### EPB Override over PECI

Enable/Disable EPB override over PECI. Enable by sending pcode command 0x2b, subcommand 0x3 to 1. This will allow OOB EPB PECI override control

### HwP Lock

Enable/Disable HWP Lock support in Misc Power Management MSR.

### HDC Control

This option allows HDC configuration.

### Turbo Mode

Enable/Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).

### View/Configure Turbo Options

- Turbo Ratio Limit Options
   View/Configure Turbo Ratio Limit Options
- Energy Efficient P-state
   Enable/Disable Energy Efficient P-state feature.
- Package Power Limit MSR Lock
   Enable/Disable locking of Package Power Limit settings.
- Energy Efficient Turbo
   Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo frequency to increase efficiency.

### CPU VR Setting

- Current VccIn AUX Icc Max Current VccIn Aux Icc Max
- PSYS Slope
   PSYS Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x9.
- PSYS offset
   PSYS Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. PSYS Uses BIOS VR mailbox command 0x4.
- PSYS Prefix Sets the offset value as positive or negative.

PSYS Pmax Power

PSYS PMax power, defined in 1/8 Watt increments. Range 0-8191. For a PMax of 125W, enter 1000. 0 = AUTO. Uses BIOS VR mailbox command 0xB.

- Min Voltage Override
   Min Voltage Override. Enable to override minimum voltage for runtime and for C8.
- VccIn Aux Icc Max
   Sets the Max Icc VccIn Aux value defined in 1/4A increments. Range is 0-512. For an IccMax 32A, enter 128(32\*4).
- VccIn Aux IMON Slpoe
   VccIN Aux IMON Slope defined in 1/100 increments. Range is 0-200. For a 1.25 slope, enter 125. 0 = AUTO. Uses BIOS VR mailbox command 0x18.
- VccIn Aux IMON Offset
   VccIN Aux IMON Offset defined in 1/1000 increments. Range is 0-63999. For an offset of 25.348, enter 25348. IMON Uses BIOS VR mailbox command 0x18.
- VccIn Aux IMON Prefix
   Sets the offset value as positive or negative.
- Vsys/Psys Critical
   Vsys Critical Enable/Disable.
- Assertion Deglitch Mantissa
   Assertion Deglitch Mantissa 0x4F[7-3]. Assertion Deglitch = 2µs \* Mantissa \* 2<sup>(</sup>Exponent)
- Assertion Deglitch Exponent Assertion Deglitch Exponent 0x4F[3-0]. Assertion Deglitch = 2µs \* Mantissa \* 2^(Exponent)
- De assertion Deglitch Mantissa
   De Assertion Deglitch Mantissa 0x49[7-3]. Assertion Deglitch = 2µs \* Mantissa \* 2<sup>(</sup>Exponent)
- De assertion Deglitch Exponent
   De Assertion Deglitch Exponent 0x49[3-0]. Assertion Deglitch = 2µs \* Mantissa \* 2<sup>(</sup>Exponent)
- VR Power Delivery Design

Specifies the ADL Desktop board design used for the VR settings override values. By default, BIOS will override the default Desktop VR settings based on the board design. A value of AUTO(0) will use the board ID to determine the board design. Any other value will override the board id logic to provide a custom VR Power Delivery Design value. This is intended primarily for validation.

Acoustic Noise Settings

(i) Acoustic Noise Mitigation

Enabling this option will help mitigate acoustic noise on certain SKUs when the CPU is in deeper C state

(ii) Pre Wake Time

Set the maximum Pre Wake randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.

(iii) Ramp Up Time

Set the maximum Ramp Up randomization time in micro ticks. Range is 0-255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning

(iv) Ramp Down Time

Set the maximum Ramp Down randomization time in micro ticks. Range is 0-

255. This is for acoustic noise mitigation Dynamic Perodicity Alteration (DPA) tuning.

(v) Disable Fast PKG C State Ramp for IA Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state

(vi) Slow Slew Rate for IA Domain

Set VR IA Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8, 16 to slow down the slew rate to help minimize acoustic noise.

(vii) Disable Fast PKG C State Ramp for GT Domain

This option needs to be configured to reduce acoustic noise during deeper C states. False: Don't disable Fast ramp during deeper C states; True: Disable Fast ramp during deeper C state.

(viii) Slow Slew Rate for GT Domain

Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled

- Core/IA VR Settings
  - (i) VR Config Enable
  - (ii) Current AC loadline
  - (iii) Current DC loadline
  - (iv) Current Psi1 Threshold
  - (v) Current Psi2 Threshold
  - (vi) Current Psi3 Threshold
  - (vii) Current Imon Slope
  - (viii) Current Imon offset
  - (ix) Current VR Current Limit
    - Current VR Current Limit (Current IccMax Value)
  - (x) Current TDC Current Limit
  - (xi) Current Voltage Limit
  - (xii) AC Loadline
    - AC Loadline defined in 1/100 mOhms.
  - (xiii) DC Loadline
    - DC Loadline defined in 1/100 mOhms.
  - (xiv) PS Current Threshold1
    - PS Current Threshold1, defined in 1/4 A increments.
  - (xv) PS Current Threshold2
    - PS Current Threshold2, defined in 1/4 A increments.
  - (xvi) PS Current Threshold3

PS3 Enable/Disable. 0 - Disabled, 1 - Enabled.Uses BIOS VR mailbox command 0x3

(xvii) PS4 Enable

PS4 Enable/Disable. 0 - Disabled, 1 - Enabled.Uses BIOS VR mailbox command 0x3

(xviii) IMON Slope

IMON Slope defined in 1/100 increments.

(xix) IMON Offset

IMON Offset defined in 1/1000 increments.

(xx) IMON Prefix

Sets the offset value as positive or negative.

(xxi) VR Current Limit

Current VR Current Limit (Current IccMax Value)

(xxii) Core VR Fast Vmode

Core VR Fast Vmode. Use to control Core Fast Vmode Enable/Disable. The value will only be effective by enabling the corresponding CEP.

(xxiii) Fast Vmode Itrip ICC Limit

Voltage Regulator Fast Vmode Itrip ICC Limit.

(xxiv) VR Voltage Limit

Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV. Uses BIOS VR mailbox command 0x8.

(xxv) TDC Enable

TDC Enable. 0- Disable, 1 - Enable

(xxvi) TDC Current Limit

TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.

(xxvii) TDC Time Window

VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.

(xxviii) TDC Lock

(xxix) IRMS

Enable/Disable IRMS - Current root mean square

- GT VR Settings
  - (i) VR Config Enable
    - VR Config Enable
  - (ii) Current AC loadline
  - (iii) Current DC loadline
  - (iv) Current Psi1 Threshold
  - (v) Current Psi2 Threshold
  - (vi) Current Psi3 Threshold
  - (vii) Current Imon Slope
  - (viii) Current Imon offset
  - (ix) Current VR Current Limit

Current VR Current Limit (Current IccMax Value)

- (x) Current TDC Current Limit
- (xi) Current Voltage Limit
- (xii) AC Loadline
  - AC Loadline defined in 1/100 mOhms.
- (xiii) DC Loadline
  - DC Loadline defined in 1/100 mOhms.
- (xiv) PS Current Threshold1
  - PS Current Threshold1, defined in 1/4 A increments.
- (xv) PS Current Threshold2
  - PS Current Threshold2, defined in 1/4 A increments.
- (xvi) PS Current Threshold3

PS Current Threshold3, defined in 1/4 A increments.

(xvii) PS4 Enable

PS4 Enable/Disable. 0 - Disabled, 1 - Enabled.Uses BIOS VR mailbox command 0x3

- (xviii) IMON Slope
  - IMON Slope defined in 1/100 increments.
- (xix) IMON Offset

IMON Offset defined in 1/1000 increments.

- (xx) IMON Prefix
  - Sets the offset value as positive or negative.
- (xxi) VR Current Limit

Voltage Regulator Current Limit (IccMax).

(xxii) VR Voltage Limit

Voltage Limit (VMAX). This value represents the Maximum instantaneous voltage allowed at any given time. Range is 0 - 7999mV. Uses BIOS VR mailbox command 0x8.

(xxiii) TDC Enable

TDC Enable. 0- Disable, 1 - Enable

(xxiv) TDC Current Limit

TDC Current Limit, defined in 1/8A increments. Range 0-32767. For a TDC Current Limit of 125A, enter 1000. 0 = 0 Amps. Uses BIOS VR mailbox command 0x1A.

(xxv) TDC Time Window

VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.

(xxvi) TDC Lock

- RFI Settings
  - (i) RFI Current Frequency
  - (ii) RFI Frequency

Set desired RFI frequency, in increments of 100KHz. (For a frequency of 100.6MHz, enter 1006.)

- (iii) FIVR Spread Spectrum
  - Enable/Disable the FIVR Spread Spectrum.
- (iv) RFI Spread spectrum
  - Set the Spread Spectrum.

### C States

Enable/Disable CPU Power Management.

Thermal Monitor

Enable/Disable CPU Power Management.

Interrupt Redirection Mode

Enable/Disable Thermal Monitor

### Timed MWAIT

Enable/Disable Timed MWAIT Support

### Custom P-state Table

Number of P states
 Sets the number of custom P-states. At least 2 states must be present.

- EC Turbo Control Mode
   Enable/Disable EC Turbo Control mode
- Energy Performance Gain Enable/disable Energy Performance Gain.

### EPG DIM Idd3N

Active standby current (Idd3N) in milliamps from datasheet. Must be calculated on a per DIMM basis.

### EPG DIM Idd3P

Active power-down current (Idd3P) in milliamps from datasheet. Must be calculated on a per DIMM basis.

### CPU Lock Configuration

CFG Lock

Configure MSR 0xE2[15], CFG Lock bit.

Overclocking Lock
 Enable/Disable Overclocking Lock (BIT 20) in FLEX\_RATIO(194) MSR.

### **GT - Power Management Control**



Advanced	Aptio Setup – AMI	
GT – Power Management Control RC6(Render Standby) Maximum GT frequency Disable Turbo GT frequency	[Enabled] [Default Max Frequency] [Disabled]	Check to enable render standby support.
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	2.22.1290 Copyright (C) 2023	AMI

### RC6 (Render Standby)

Check to enable render standby support.

# Maximum GT frequency Maximum GT frequency limited by the user

Disable Turbo GT frequency
 Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited.

# Chapter 3 BIOS Settings

### 3.2.2.4 PCH-FW Configuration

Aptio Setup – AMI		
Main Advanced Chipset Security	oot Save & Exit NVMe RPMB Key Migration MEBx	
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>POWER &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>S5 RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> </ul>	Configure Management Engine Technology Parameters	
<ul> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>	
Version (	22.1290 Copyright (C) 2023 AMI	

### **ME State**

When Disabled ME will be put into ME Temporarily Disabled Mode.

### **Mamageability Features State**

Enable/Disable Intel Manageability features.

### **AMT BIOS Features**

When disabled AMT BIOS Features are no longer supported and user is no longer able to access MEBx Setup.

### **AMT** Configuration

Advanced	Aptio Setup — AMI	
ME Firmware Version ME Firmware Mode ME Firmware SKU ME Firmware Status 1 ME Firmware Status 2 ME Firmware Status 3 ME Firmware Status 4 ME Firmware Status 5 ME Firmware Status 6	16.1.27.2225 Normal Mode Corporate SKU 0x390000255 0x39858106 0x00000030 0x00004000 0x0000103 0x80400002	Configure Intel(R) Active Management Technology Parameters
ME State Manageability Features State AMT BIOS Features AMT Configuration Local Platform Erase Configuration ME Unconfig on RTC Clear Core Bios Done Message CSE Data Resilience Support Firmware Update Configuration PTT Configuration DEM Key Revocation Configuration Extend CSME Measurement to TPM-PCR	[Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

### USB Provisioning of AMT

Enable/Disable of AMT USB Provisioning.

### MAC Pass Through

Enable/Disable MAC Pass Through function.

### Dynamic LAN Switch

Allow switching AMT support from Integrated LAN to Discrete LAN.

### Activate Remote Assistance Process

Trigger CIRA boot\n\nNote:\nNetwork Access must be activated first from MEBx Setup.

### Unconfigure ME

OEMFlag Bit 15. Unconfigure ME with resetting MEBx password to default.

### Secure Erase Configuration

- Secure Erase mode
   Change Secure Erase module behavior. Simulated: Performs SE flow without erasing SSD\nReal: Erase SSD. If SATA device is used, OEM could use SECURE\_ERASE\_HOOK\_PROTOCOL to remove SATA power to skip G3 cycle.
- Force Secure Erase
   Force Secure Erase on next boot

Advanced	Aptio Setup – AMI	
ME Firmware Version ME Firmware Mode ME Firmware SKU ME Firmware Status 1 ME Firmware Status 2 ME Firmware Status 3 ME Firmware Status 4 ME Firmware Status 5 ME Firmware Status 6	16.1.27.2225 Normal Mode Corporate SKU 0x90000255 0x39858106 0x00000030 0x00004000 0x0000103 0x80400002	Configure Intel(R) Active Management Technology Parameters
ME State Manageability Features State AMT BIOS Features AMT Configuration Local Platform Erase Configuration ME Unconfig on RTC Clear Core Bios Done Message CSE Data Resilience Support	(Enabled) (Enabled) (Enabled) (Enabled) (Enabled) (Enabled)	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values</pre>
<ul> <li>Firmware Update Configuration</li> <li>PTT Configuration</li> <li>OEM Key Revocation Configuration Extend CSME Measurement to TPM-PCR</li> </ul>	[Disabled]	F3: Optimized Defaults F4: Save & Exit ESC: Exit

Version 2.22.1290 Copyright (C) 2023 AMI

Advanced	Aptio Setup – AMI	
USB Provisioning of AMT MAC Pass Through Dynamic Lan Switch Activate Remote Assistance Process Unconfigure ME ▶ Secure Erase Configuration	[Disabled] [Disabled] [As defined in FIT] [Disabled] [Disabled]	Enable/Disable of AMT USB Provisioning.
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

Advanced	Aptio Setup — AMI	
USB Provisioning of AMT MAC Pass Through Dynamic Lan Switch Activate Remote Assistance Process Unconfigure ME > Secure Erase Configuration	[Disabled] [Disabled] [As defined in FIT] [Disabled] [Disabled]	Secure Erase configuration menu ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	2.22.1290 Copyright (C) 2023	AMI

Advanced	Aptio Setup – AMI	
Secure Erase mode Force Secure Erase	[Simulated] [Disabled]	Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD Real: Erase SSD. *** If SATA device is used, OEM could use SECURE_ERASE_HOOK_PROTOCOL to remove SATA power to skip G3 CyCle. ***
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Ve	ersion 2.22.1290 Copyright (C	) 2023 AMI

### Local Platform Erase Configuration

Advanced	Aptio Setup – AMI	
Advanced Perform Platform Erase Operations	[Disabled]	Enabling this Feature will trigger Platform Erase Operations on the Next Boot ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1290 Copyright (C) 2023	AMI

### Perform Platform Erase Operations

Enabling this Feature will trigger Platform Erase Operations on the Next Boot

### ME Unconfig on RTC Clear

When Disabled ME will not be unconfigured on RTC Clear. **Core Bios Done Message** Enable/Disable Core Bios Done message sent to ME **CSE Data Resilience Support** Enable/Disable CSE Data Resilience Support

### Firmware Update Configuration

Advanced	Aptio Setup — AMI	
Me FW Image Re-Flash FW Update	[Disabled] [Enabled]	Enable/Disable Me FW Image Re-Flash function.
		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

### ME FW Image Re-Flash

Enable/Disable Me FW Image Re-Flash function.

# FW Update Enable/Disable ME FW Update function.

### **PTT Configuration**

Advanced	Aptio Setup – AMI	
PTT Capability / State	1 / 1	
TPM Device Selection	[ftpm]	
		<pre> ++: Select Screen  1↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version :	2.22.1290 Copyright (C) 2023	AMI

### PTT Capability

# TPM Device Selection Configure TPM device

**OEM Key Revocation configuration** 

### Extend CSME Measurement to TPM-PCR

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

Advanced	Aptio Setup — AMI	
Automatic OEM Key Revocation Invoke OEM Key Revocation	[Disabled] [Disabled]	When enabled, BIOS will automatically send HECI command to revoke OEM keys. ++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1290 Copyright (C) 2023	AMI

### Automatic OEM Key Revocation

When enabled, BIOS will automatically send HECI command to revoke OEM keys.

### Invoke OEM Key Revocation

A HECI command will be sent to revoke OEM key

### 3.2.2.5 Trusted Computing

Main Advanced Chipset Security	Aptio Setup – AMI Boot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>POUET &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	Trusted Computing Settings ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1290 Copyright (C) 2023 AMI

- Security Device Support
   Enable/Disable BIOS support for security device
- Active PCR banks
- Available PCR banks
- SHA256 PCR Bank Enable/Disable SHA256 PCR Bank
- SHA384 PCR Bank Enable/Disable SHA384 PCR Bank
- SM3\_256 PCR Bank Enable/Disable SM3\_256 PCR Bank
- Pending Operation
   Schedule an Operation for the security device
- Platform Hierarchy
   Enable/Disable Platform Hierarchy
- Storage Hierarchy
   Enable/Disable Storage Hierarchy
- Endorsement Hierarchy Enable/Disable Endorsement Hierarchy
- Physical Presence Spec Version Tells OS to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 1.3.
- TPM 2.0 Interface Type
- Device Select

	Υ.
	_
- n'	<u>۱</u>
-	
	5
$\sim$	
	le.
<u> </u>	
1.20	
	5 -
- C .	<u>_</u>
- 0	9
- 57	-
	-
	- ))
	1
	_
- 6 (	
- ( /	
	1
	_
- 17	л
- UL	
	-
_	la.
- E	
	5
-	
-	6
- ( <i>Г</i>	)

Advanced	Aptio Setup – AMI	
TPM Device Selection	[fTPM]	Selects TPM device: fTPM or dTPM _ FTPM _ Enables fTPM
TPM 2 0 Device Found		dTPM - Disables fTPM and
Firmware Version:	600.18	Enable dTPM, Warning !
Vendor:	INTC	fTPM/dTPM will be disabled and all data saved on it will be
Security Device Support	[Enable]	lost.
Active PCR banks	SHA256	
Available PCR banks	SHA256,SHA384,SM3	
SHA256 PCR Bank	[Enabled]	
SHA384 PCR Bank	[Disabled]	
SM3_256 PCR Bank	[Disabled]	
		↔: Select Screen
Pending operation	[None]	↑↓: Select Item
Platform Hierarchy	[Enabled]	Enter: Select
Storage Hierarchy	[Enabled]	+/-: Change Opt.
Endorsement Hierarchy	[Enabled]	F1: General Help
Physical Presence Spec Version	[1.3]	F2: Previous Values
TPM 2.0 InterfaceType	[CRB]	F3: Optimized Defaults
Device Select	[Auto]	F4: Save & Exit
		ESU: EXIT
Version	2.22.1290 Copyright (C)	2023 AMI

### 3.2.2.6 ACPI Settings

Main Advanced Chipset Security	Aptio Setup – AMI Boot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>POWER &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	System ACPI Parameters. **: Select Screen 1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1290 Copyright (C) 2023 AMI

- Enable ACPI Auto Configuration
  - Enables/Disables BIOS ACPI Auto Configuration.

# Enable Hibernation Enable/Disable System's ability to Hibernate (OS/S4 Sleep State)

### ACPI Sleep State

Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.



### 3.2.2.7 iManager Configuration


# **Serial Port 1 Configuration**

Advanced	Aptio Setup — AMI	
Serial Port 1 Configuration		Enable or Disable Serial Port
Serial Port Device Settings	[Enabled] IO=3F8h; IRQ=4;	(COM)
Change Settings COM Port Mode	[Auto] [RS-232 Mode]	
		↔: Select Screen ↑↓: Select Item Enter: Select
		+/-: Change Opt. F1: General Help F2: Previous Values
		F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1290 Copyright (C) 2023	AMI

- Serial Port
- Device Settings
- Change Settings
- COM Port Mode

# Serial Port 2 Configuration

Advanced	Aptio Setup — AMI	
Serial Port 2 Configuration		Enable or Disable Serial Port
Serial Port Device Settings	[Enabled] IO=2F8h; IRQ=3;	(600)
Change Settings COM Port Mode	[Auto] [RS-232 Mode]	
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

- Serial Port
- Device Settings
- Change Settings
- COM Port Mode

# **Serial Port 3 Configuration**



- Serial Port
- Device Settings
- Change Settings
- COM Port Mode

# Serial Port 4 Configuration

Advanced	Aptio Setup – AMI	
Serial Port 4 Configuration		Enable or Disable Serial Port
Serial Port Device Settings Change Settings	[Enabled] IO=2E8h; IRQ=7; [Auto]	(COM)
		<pre>++: Select Screen 1↓: Select Item Enter: Select +/-: Change Opt.</pre>
		F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version :	2.22.1290 Copyright (C) 2023	) AMI

- Serial Port
- Device Settings
- Change Settings
- COM Port Mode

### Hardware Monitor

Advanced	Aptio Setup – AMI	
PC Health Status		
CPU Temperature	: + 60°C⁄ + 140°F	
+3.3V + 5V VBAT Vcore	: +3.27 V : +5.03 V : +2.93 V : +0.76 V	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version :	2.22.1290 Copyright (C) 2023	AMI

- CPU Temperature
- +3.3V
- +5V
- VBAT
- Vcore

### Watch Dog Timer Configuration



### Watch Dog Timer Hidden

Enabled or Disabled Watch Dog Timer Hidden

### Watch Dog Timer

Enabled or Disabled Watch Dog Timer function (Start before boot to OS and must stop by self)

# **GPIO Configuration**

Advanced	Aptio Setup – AMI	
GPIO Configuration		Choose to control GPIO by EC
GPIO Control Enable	[By EC]	or user override during POST stage. →+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. 5↓: Common Post
		F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1290 Copyright (C) 2023 AMI		

# GPIO Control Enable

Choose to control GPIO by EC or user override during POST stage.

### **ACPI Report Method Configuration**



### ACPI Report Method Control

Select ACPI Reporting Method for EC Devices.

# Active High-Speed COM Port

Standard -> Standard COM Port. High Speed -> High Speed COM Port. (Driver installation is necessary.)

### iManager I2C0 Control

Enable/Disable SMBus0 controller on RDC

# iManager SMBus Control

Advanced	Aptio Setup – AMI	
Advanced iManager Configuration iManager Chipset Firmware Version DEM Group GPIO Number Available Serial Port 1 Configuration Serial Port 2 Configuration Serial Port 3 Configuration Serial Port 4 Configuration Hardware Monitor Hardware Monitor Hardware Monitor ACPI Report Method Configuration	EID-201 V01004027 8	Select ACPI Reporting Method for EC Devices. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
	.22.1290 Copyright (C) 2023	AMI

# 3.2.2.8 NCT5124DSEC Super IO Configuration

Main Advanced Chipset Security	Apt Boot	t <b>io Setup – A⊬</b> Save & Exit	II NVMe RPM	B Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>				System Super ID Chip Parameters. 
Version	2.22.1	1290 Copyright	: (C) 2023	AMI

# Super IO Chip Serial Port 5 Configuration

[Enabled] IO=C80h; IRQ=10; [Auto] [RS-232 Mode]	Enable or Disable Serial Por (COM)
[Enabled] IO=C80h; IRQ=10; [Auto] [RS-232 Mode]	
[Auto] [RS-232 Mode]	
	<pre>++: Select Screen  f↓: Select Item Enter: Select +/-: Change Opt.</pre>
	F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
sion 2 22 1290 Converget (P)	2023 AMT
	3ion 2.22.1290 Copyright (C)

- Device Settings
- Change Settings
- COM Port Mode

# **Serial Port 6 Configuration**

Advanced	Aptio Setup — AMI	
Serial Port 6 Configuration		Enable or Disable Serial Port
Serial Port Device Settings Change Settings COM Port Mode	[Enabled] IO=C68h; IRQ=11; [Auto] [RS-232 Mode]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Helm</pre>
Vancian 2	22, 1990, Conunidat (C), 2022	F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1290 Copyright (C) 2023	AMI

- Serial Port
- Device Settings
- Change Settings
- COM Port Mode

# 3.2.2.9 S5 RTC Wake Settings

Main Advanced Chinset Security	Apt Boot	io Setup – AM Save & Exit	II NVMe	RPMB Key Migration MEBy
<ul> <li>NHAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS FTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>				<pre>HTTP: Key Higherton HEDX Enable system to wake from S5 using RTC alarm  ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version	2.22.1	250 Copyright	. (b) Z	1020 HM1

# Wake system from S5

Advanced	Aptio Setup – AMI	
Wake system from S5	[Disabled]	Enable or disable System wake on alarm event. Select FixedTime, system will wake on the hr::min::sec specified. Select DynamicTime , System will wake on the current time + Increase minute(s) **: Select Screen 11: Select Item Enter: Select t+-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
V	ersion 2.22.1290 Copyright (	C) 2023 AMI

# 3.2.2.10 Serial Port Console Redirection

Main Advanced Chipset Security	Aptio Setup – AMI Boot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>IManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	Serial Port Console Redirection ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
· Version :	.22.1290 Copyright (C) 2023 AMI

### Console Redirection

Console Redirection Enable/Disable

### Console Redirection Settings

The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

### COM1(Pci Bus, Dev0, Func0)

### Console Redirection

Console Redirection Enable/Disable.



### Legacy Console Redirection Settings



- Redirection COM Port Select a COM port to display redirection of Legacy OS and Legacy OPROM Messages
- Resolution
   Enable/Disable extended terminal resolution

- Redirect After Post

When Bootloader is selected, then Legacy Console Redirection is disabled before booting to legacy OS. When Always Enable is selected, then Legacy Console Redirection is enabled for legacy OS. Default setting for this option is set to Always

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

Console Redirection Enable/Disable.

### Console Redirection Settings

The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.

### 3.2.2.11 Intel TXT Information

		f	ptio Setup – Ak	4I	
Main	Advanced <u>Chipset</u>	Security Boo	t Save & Exit	NVMe RPM	18 Key Migration MEBX
WWAN ( CPU CC) POWER PCH-FF Trusta ACPI S iManag NCT512 SS RTIC Seria. Intel PCI S( VUSB CC) Networ CSM CC NVME ( NVME ()	Configuration onfiguration & Performance A Configuration ed Computing Settings ger Configuration 24DSEC Super IO Conf 2 Wake Settings 1 Port Console Redir TXT Information ubsystem Settings onfiguration ~k Stack Configurati onfiguration Configuration	iguration ection on			<pre>Display Intel TXT information ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
		Version 2 22	1290 Conuright	t (C) 2029	AMT

- Chipset
- BiosAcm
- Chipset TxT
- CPU TxT
- Error Code
- Class Code
- Major Code
- Minor Code

### PCI Subsystem Settings

Main Advanced Chipset Security	Aptio Setup – AMI oot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	PCI Subsystem Settings ++: Select Screen 1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	22.1290 Copyright (C) 2023 AMI

- Re-Sized BAR Support
- If system has Resizable BAR capable PCIe Devices, this option Enables or Disables Resizable BAR Support.
- BME DMA Mitigation
   Re-enable Bus Master Attribute disabled during PCI enumeration for PCI
   Bridges after SMM Locked



### 3.2.2.12 USB Configuration

Main Advanced Chipset Security	Aptio Setup – AMI ot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	USB Configuration Parameters ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version :	2.1290 Copyright (C) 2023 AMI

#### Legacy USB Support

Enables Legacy USB support.

# XHCI Hand-off This is a workaround for OS without XHCI hand-off support.

- USB Mass Storage Device Configuration Configure the USB Mass Storage Devices.
- 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.

### ■ JetFlashTS4GJFV30 8.07

Advanced	Aptio Setup – AMI	
USB Configuration		Enables Legacy USB support.
USB Module Version	31	support if no USB devices are connected. DISABLE option will
USB Controllers: 4 XHCIs		keep USB devices available only for EFI applications.
USB Devices: 1 Drive, 1 Keyboard, 1 Mouse,	1 Hub	
Legacy USB Support XHCI Hand-off USB Mass Storage Driver Support	[Enabled] [Enabled] [Enabled]	
USB hardware delays and time-outs:		↔: Select Screen
USB transfer time-out	[20 sec]	†↓: Select Item Enter: Select
Device power-up delay	[Auto]	+/-: Change Opt.
Mass Storage Devices:		F1: General Help F2: Previous Values
JetFlashTS4GJFV30 8.07	[Auto]	F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	2.22.1290 Copyright (C) 2023	AMI

# Chapter 3 BIOS Settings

# 3.2.2.13 Network Stack Configuration

Main Advanced Chipset Security	Aptio Setup – AMI Boot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>SS RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>CSM Configuration</li> <li>NVMe Configuration</li> </ul>	<pre>Network Stack Settings  ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version -	2.22.1290 Copyright (C) 2023 AMI

## Network Stack

Advanced	Aptio Setup – AMI	
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack **: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Ver	sion 2.22.1290 Copyright (C) :	2023 AMI

### 3.2.2.14 CSM Configuration

Main Advanced Chipset Security	Aptio Setup – AMI Boot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>WWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>S5 RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>NCME Configuration</li> <li>NVME Configuration</li> </ul>	CSM configuration: Enable/Disable, Option ROM execution settings, etc. ++: Select Screen fl: Select Item Enter: Select
	+/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1290 Copyright (C) 2023 AMI

## CSM Support

Enable/Disable CSM Support.



# Chapter 3 BIOS Settings

# 3.2.2.15 NVMe Configuration

Main Advanced Chipset Security	Aptio Setup – AMI oot Save & Exit NVMe RPMB Key Migration MEBx
<ul> <li>NWAN Configuration</li> <li>CPU Configuration</li> <li>Power &amp; Performance</li> <li>PCH-FW Configuration</li> <li>Trusted Computing</li> <li>ACPI Settings</li> <li>iManager Configuration</li> <li>NCT5124DSEC Super IO Configuration</li> <li>S5 RTC Wake Settings</li> <li>Serial Port Console Redirection</li> <li>Intel TXT Information</li> <li>PCI Subsystem Settings</li> <li>USB Configuration</li> <li>Network Stack Configuration</li> <li>NVMe Configuration</li> </ul>	ANCE & LAIT       NVHE NUME NUME NUME NUME NUME         NVHE Device Options Settings         **: Select Screen         11: Select Item         Enter: Select         +/-: Change Opt.         F1: General Help         F2: Previous Values         F3: Optimized Defaults         F4: Save & Exit         ESC: Exit
Version	22.1290 Copyright (C) 2023 AMI

Aptio Setup – AMI Advanced	
NVMe Configuration	
No NVME Device Found	
	t↓: Select Item Enter: Select
	+/-: Change Opt. E1: General Help
	F2: Previous Values F3: Ontimized Defaults
	F4: Save & Exit
Version 2.22.1290 Copyright (C) 2023	AMI

# 3.2.3 Chipset Configuration

Select the Chipset tab from the ARK-2251 setup screen to enter the Chipset BIOS Setup screen. You can display a Chipset BIOS Setup option by highlighting it using the <Arrow> keys. All Plug and Play BIOS Setup options are described in this section. The Plug and Play BIOS Setup screen is shown below.

### 3.2.3.1 System Agent Configuration

	Main	Advanced	Chipset	Security	Apt Boot	io Setup – AM Save & Exit	I NVMe RPME	3 Key Migration MEBx
•	Main System PCH-IO	Advanced Agent (SA Configura	Chipset ) Configu tion	security	Boot	Save & Exit	NVME RPME	System Agent (SA) Parameters System Agent (SA) Parameters ++: Select Screen 14: Select Item Enter: Select +/-: Select Opt
								+/-: Change Upt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
				Version	2.22.1	290 Copyright	(0) 2023	AMI

	Chipset	Aptio Setup – AMI	
Γ	System Agent (SA) Configuration		Memory Configuration Parameters
	VT-d	Supported	
	Memory Configuration Graphics Configuration VMD setup menu PCI Express Configuration		
	VT-d Control Iommu Pre-boot Behavior Above 4GB MMIO BIOS assignment IPU Device (B0:D5:F0) IPU 1181 Dash Camera	[Enabled] [Disable IOMMU] [Enabled] [Disabled] [Disabled]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
	Version 2	.22.1290 Copyright (C) 2023	AMI

# Memory Configuration

Chipset	Aptio Setup – AMI	
Memory Configuration Memory RC Version Memory Frequency DIMM1 DIMM2 Size Number of Ranks Manufacturer SAM Overlaoding	0.0.4.133 4800 MT/s Not Populated / Disabled Populated & Enabled 16384 MB (DDR5) 1 Advantech Co Ltd [Disabled]	Enable: copy the sagv frequency point. Disable: not copy.
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version	2.22.1290 Copyright (C) 2023	AMI

 SAM Overloading Enable/Disable SAM Overloading

# Graphics Configuration

Chipset	Aptio Setup – AMI	
Graphics Configuration		Graphics turbo IMON current values supported (14–31)
Graphics Turbo IMON Current Skip Scaning of External Gfx Card	<mark>31 [</mark> Disabled]	
<ul> <li>Primary Display</li> <li>External Gfx Card Primary Display Constraints</li> <li>GTT Size</li> <li>Aperture Size</li> <li>DVMT Pre-Allocated</li> <li>DVMT Total Gfx Mem</li> <li>Intel Graphics Pei Display Peim</li> <li>VDD Enable</li> <li>Configure GT for use</li> <li>RC1p Support</li> <li>PAVP Enable</li> </ul>	[Auto] onfiguration [Auto] [8MB] [256MB] [60M] [256M] [Disabled] [Enabled] [Enabled] [Disabled] [Enabled]	<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
LVersion 2	2.22.1290 Copyright (C) 2023	AMI

- Graphics Turbo IMON current Graphics turbo IMON current values supported (14-31)
- Skip Scanning of External Gfx Card If Enabled, it will not scan for External Gfx Card on PEG and PCH PCIE Ports.
- Primary Display Select which of IGFX/PEG/PCI Graphics device should be Primary Display or select SG for Switchable Gfx.
- External Gfx Card Primary Display Configuration Select the card used on the platform.
- Internal Graphics
  - Keep IGFX enabled based on the setup options.
- GTT Size Select the GTT Size.
- Aperture Size
   Select the Aperture Size.
- Dvmt Pre-Allocated Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
- Dvmt Total Gfx Mem
   Select DVMT5.0 Total Graphic Memory size used by the Internal Graphics
   Device.
- DVMT Pre-Allocated Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
- Intel Graphics Pel Display Peim Enable/Disable Pei (Early) Display
- VDD Enable
   Enable/Disable forcing of VDD in the BIOS
- Configure GT for use Enable/Disable GT configuration in BIOS
- RC1p Support
   Enable/Disable RC1p support. If RC1p is enabled, send a RC1p frequency request to PMA based other conditions being met
- PAVP Enable
   Enable/Disable PAVP

## VMD Setup Menu

Chipset	Aptio Setup — AMI	
VMD Configuration		Enable/Disable to VMD
Enable VMD controller	[Disabled]	Controller
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

- Enable VMD Controller
   Enable/Disable to VMD controller
- PCI Express Configuration
- VT-d

VT-d capability

- Control Iommu Pre-boot Behavior Control Iommu Pre-boot Behavior
- Above 4GB MMIO BIOS assignment Enable/Disable above 4GB Memory Mapped I/O BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB.
- IPU Device (B0:D5:F0)
   Enable/Disable SA IPU Device.

### IPU 1181 Dash Camera

Chipset	Aptio Setup — AMI	
System Agent (SA) Configuration		PCI Express Configuration
VT-d	Supported	oo ta maa
<ul> <li>Memory Configuration</li> <li>Graphics Configuration</li> <li>VMD setup menu</li> <li>PCI Express Configuration</li> </ul>		
VT-d Control Iommu Pre-boot Behavior Above 4GB MMIO BIOS assignment IPU Device (B0:D5:F0) IPU 1181 Dash Camera	[Enabled] [Disable IOMMU] [Enabled] [Disabled] [Disabled]	★: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2	.22.1290 Copyright (C) 2023	AMI

Aptio Setup - AMI Chipset	
PCI Express Configuration	PCI Express Root Port Settings.
▶ PCI Express Root Port 1	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2.22.1290 Copyright (C) 2023	AMI

Chipset	Aptio Setup – AMI	
PCI Express Root Port 1 Connection Type PCI Express Clock Gating PCI Express Power Gating ASPM L1 Substates Gen3 Eq Phase3 Method Gen4 Eq Phase3 Method ACS PTM DPC FOM Scoreboard Control Policy Multi-VC EDPC URR FER NFER CER CTO SEFFE SENFE SECE PME SCI Advanced Error Reporting PCIE Speed	[Enabled] [Slot] [Enabled] [Enabled] [Disabled] [Disabled] [Hardware] [Hardware] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Enabled] [Disabled]	<ul> <li>Control the PCI Express Root Port.</li> <li>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</li> </ul>

#### Version 2.22.1290 Copyright (C) 2023 AMI

Chipset	Aptio Setup – AMI	
PME SCI Advanced Error Reporting PCIe Speed Enable ClockReq Messaging Transmitter Half Swing Detect Timeout P2P Support CPU PCIE Func0 Link Disable	[Enabled] [Disabled] [Auto] [Enabled] [Disabled] O [Disabled] [Disabled]	Enable or Disable ClockReq Messaging
SA PCIe LTR Configuration LTR Snoop Latency Override Non Snoop Latency Override Force LTR Override LTR Lock	(Enabled) [Auto] [Auto] [Disabled] [Disabled]	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Unt</pre>
CPU PCIE Gen3 HWEQ Config UPTP DPTP CPU PCIE Gen4 HWEQ Config	5 7	F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
UPTP DPTP	8 9	

# PCI Express Root Port 1

- PCI Express Root Port 1 Control the PCI Express Root Port.
- Connection Type Built-In: a built-in device is connected to this rootport. SlotImplemented bit

will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.

- PCI Express Clock Gating PCI Express Clock Gating Enable/Disable for each root port.
- PCI Express Power Gating
   PCI Express Power Gating Enable/Disable for each root port.
- ASPM
  - PCI Express Active State Power Management settings
- L1 Substates
   PCI Express L1 Substates settings.L1SS cannot be enabled when CLKREQMSG is disabled
- Gen3 EQ Phase3 Method
   PCIe Gen3 Equalization Phase 3 Method
- Gen4 EQ Phase3 Method
   PCIe Gen4 Equalization Phase 3 Method
- ACS
  - Enable/Disable Access Control Services Extended Capability
- PTM Enable (Disable Decision T
- Enable/Disable Precision Time Measurement
- DPC
  - Enable/Disable Downstream Port Containment
- FOM Scoreboard Control Policy Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS
- Multi-VC
   Enable/Disable Multi Virtual Channel
- EDPC
   Enable/Disable Rootport extensions for Downstream Port Containment
- URR
  - PCI Express Unsupported Request Reporting Enable/Disable.
- FER
  - PCI Express Device Fatal Error Reporting Enable/Disable.
- NFER
  - PCI Express Device Non-Fatal Error Reporting Enable/Disable
- CER
  - PCI Express Device Correctable Error Reporting Enable/Disable.
- CTO
  - PCI Express Device Correctable Error Reporting Enable/Disable.
- SEFE
  - Root PCI Express System Error on Fatal Error Enable/Disable.
- SENFE
  - Root PCI Express System Error on Non-Fatal Error Enable/Disable.
- SECE
  - Root PCI Express System Error on Correctable Error Enable/Disable
- PME SCI
   PCI Express PME SCI Enable/Disable.
- Advanced Error Reporting
   Advanced Error Reporting Enable/Disable.
- PCIe Speed
   Configure PCIe Speed
- Enable ClockReq Messaging
   Enable/Disable ClockReq Messaging

- Transmitter Half Swing
   Transmitter Half Swing Enable/Disable.
- Detect Timeout The number of milliseconds reference code will wait for link to exit Detect state for enabled ports before assuming there is no device and potentially disabling the port.
- P2P Support
   Program P2P Support Registers according to setup option
- CPU PCIE Func0 Link Disable
   CPU PCIE Func0 Link Disable while Device attached into Port having Func0 and FuncN
- SA PCIe LTR Configuration
   SA PCIE Latency Reporting Enable/Disable
- LTR

SA PCIE Latency Reporting Enable/Disable

- Snoop Latency Override
   Snoop Latency Override for SA PCIE.
- Non Snoop Latency Override Non Snoop Latency Override for SA PCIE.
- Force LTR Override
   Force LTR Override for SA PCIE.
- LTR Lock
   PCIE LTR Configuration Lock

# 3.2.3.2 PCH-IO Configuration

Main Advanced Chipset Security	Ap <sup>:</sup> Boot	tio Setup – AMI Save & Exit NVMe	RPMB Key Migration MEBx
<ul> <li>System Agent (SA) Configuration</li> <li>PCH-ID Configuration</li> </ul>			PCH Parameters ++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.	1520 CobALISUI (C)	2023 HM1

Chipset	Aptio Setup – AMI	
<ul> <li>PCH-IO Configuration</li> <li>PCI Express Configuration</li> <li>SATA Configuration</li> <li>USB Configuration</li> <li>Security Configuration</li> <li>HD Audio Configuration</li> </ul>		PCI Express Configuration settings
LAN1 Controller Wake on LAN Enable LAN1 PXE OpROM LAN2 Controller LAN2 PXE OpROM LAN3 Controller LAN3 PXE OpROM PCIE Wake Restore AC Power Loss Flash Protection Range Registers (FPRR) SPD Write Disable	[Enabled] [Disabled] [Disabled] [Enabled] [Disabled] [Disabled] [Disabled] [Power Off] [Disabled] [TRUE]	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version	2.22.1290 Copyright (C) 202	23 AMI

### LAN1 Controller

Control Detection of the HD-Audio device.

### Wake on LAN Enable

Enable/Disable integrated LAN to wake the system.

### LAN1 PXE 0Prom

Enable/Disable boot option rom for LAN1 Controller.

# LAN2 Controller

Enable/Disable onboard LAN2

### LAN2 PXE 0pROM

Enable/Disable boot option rom for LAN2 Controller.

# LAN3 Controller Enchla/Dischla anhaard LA

Enable/Disable onboard LAN3

### LAN3 PXE 0pROM

Enable/Disable boot option ROM for LAN2 Controller.

### PCIE Wake

Enable/Disable PCIE to wake the system from S5.

### Restore AC Power Loss

Specify what state to go to when power is re-applied after a power failure (G3 state).

# Flash Protection Range Registers (FPRR)

Enable Flash Protection Range Registers

## SPD Write Disable

Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

# PCI Express Configuration

Chipset	Aptio Setup – AMI	
PCI Express Configuration DMI Link ASPM Control PCIe function swap PCH PCIE Clock Gating PCH PCIE Power Gating ▶ PCIE EQ settings	[Auto] [Enabled] [Enabled] [Enabled]	The control of Active State Power Management of the DMI Link.
▶ PCI Express Root Port 12(mPCIe/M.2E)		<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

Chipset	Aptio Setup – AMI	
PCI Express Configuration DMI Link ASPM Control PCIe function swap PCH PCIE Clock Gating	[Auto] [Enabled] [Enabled]	This form contains options for controlling PCIe EQ process
<ul> <li>PCH PCIE Power Gating</li> <li>PCIE EQ settings</li> <li>PCI Express Root Port 12(mPCIe/M.2E)</li> </ul>	[Enabled]	
		<pre>++: Select Screen t1: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2.	.22.1290 Copyright (C) 2023	AMI

Chapter 3 BIOS Settings

Chipset	Aptio Setup – AMI	
PCIe EQ override	[Disabled]	Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Ve	ersion 2.22.1290 Copyright (C	) 2023 AMI

Chipset	Aptio Setup – AMI	
PCI Express Configuration		PCI Express Root Port Settings.
DMI Link ASPM Control PCIe function swap PCH PCIE Clock Gating PCH PCIE Power Gating ▶ PCIe EQ settings	[Auto] [Enabled] [Enabled] [Enabled]	
▶ PCI Express Root Port 12(mPCIe/M.2E)		
		<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

Chipset	Aptio Setup – AMI	
PCI Express Root Port 12 Connection Type ASPM L1 Substates L1 Low ACS PTM DPC EDPC URR FER NFER CER SEFE SENFE SECE PME SCI Advanced Error Reporting PCIe Speed Transmitter Half Swing Detect Timeout Extra Bus Reserved Reserved Memory Reserved I/O	[Enabled] [Slot] [Disabled] [Disabled] [Enabled] [Enabled] [Enabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Enabled] [Enabled] [Auto] [Disabled] 0 0 10 4	<ul> <li>Control the PCI Express Root Port.</li> <li>**: Select Screen</li> <li>**: Select Item Enter: Select</li> <li>*/-: Change Opt.</li> <li>F1: General Help</li> <li>F2: Previous Values</li> <li>F3: Optimized Defaults</li> <li>F4: Save &amp; Exit</li> <li>ESC: Exit</li> </ul>

Aptio Setup – AMI Chipset DPC [Disabled] Reserved I/O (4K/8K/12K/16K/20K) Range for EDPC [Enabled] LIRR [Disabled] this Root Bridge. FER [Disabled] NFER [Disabled] [Disabled] CER [Disabled] SEFE SENFE [Disabled] SECE [Disabled] PME SCI [Enabled] Advanced Error Reporting [Enabled] PCIe Speed [Auto] Transmitter Half Swing [Disabled] Detect Timeout ++: Select Screen 0 ↑↓: Select Item Extra Bus Reserved 0 Reserved Memory 10 Enter: Select +/-: Change Opt. 4 F1: General Help PCH PCIe LTR Configuration F2: Previous Values LTR [Enabled] F3: Optimized Defaults Snoop Latency Override [Auto] F4: Save & Exit ESC: Exit Non Snoop Latency Override [Auto] LTR Lock [Disabled] Peer Memory Write Enable [Disabled] Version 2.22.1290 Copyright (C) 2023 AMI

 DMI Link ASPM Control The control of Active State Power Management of the DMI Link.

- PCIe function swap
   Enable/Disable PCIe function swap
- PCH PCIE Clock Gating
   PCH PCI Express Clock Gating Enable/Disable for all port

- PCH PCIE Power Gating
   PCH PCI Express Power Gating Enable/Disable for all port
- PCIe EQ settings
  - PCIe EQ override Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process
- PCI Express Root Port 12(mPCIe/M.2E)
  - PCI Express Root Port 12
    - Control the PCI Express Root Port.
  - Connection Type

Built-In: a built-in device is connected to this rootport. SlotImplemented bit will be clear. Slot: this rootport connects to user-accessible slot. SlotImplemented bit will be set.

ASPM

PCI Express Active State Power Management settings.

• L1 Substates

PCI Express L1 Substates settings.L1SS cannot be enabled when CLKREQMSG is disabled

• L1 Low

PCI Express L1 Low Substate Enable/Disable.

- ACS
- Enable/Disable Access Control Services Extended Capability
- PTM

Enable/Disable Precision Time Measurement

• DPC

Enable/Disable Downstream Port Containment

EDPC

Enable/Disable Rootport extensions for Downstream Port Containment

• URR

PCI Express Unsupported Request Reporting Enable/Disable.

- FER
  - PCI Express Device Fatal Error Reporting Enable/Disable.
- NFER
  - PCI Express Device Non-Fatal Error Reporting Enable/Disable.
- CER
  - PCI Express Device Correctable Error Reporting Enable/Disable
- SEFE
- Root PCI Express System Error on Fatal Error Enable/Disable
- SENFE

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

- SECE
- Root PCI Express System Error on Correctable Error Enable/Disable.
- PME SCI

PCI Express PME SCI Enable/Disable.

- Advanced Error Reporting
  - Advanced Error Reporting Enable/Disable
- PCIe Speed

Configure PCIe Speed

- Transmitter Half Swing
- Transmitter Half Swing Enable/Disable
- Detect Timeout

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

• Extra Bus Reserved

Extra Bus Reserved (0-7) for bridges behind this Root Bridge.

- Reserved Memory
  - Reserved Memory for this Root Bridge (1-20) MB
- Reserved I/O Reserved I/O (4K/8K/12K/16K/20K) Range for this Root Bridge.
- LTR
- SA PCIE Latency Reporting Enable/Disable
- Snoop Latency Override Snoop Latency Override for SA PCIE.
- Non Snoop Latency Override
   Non Snoop Latency Override for SA PCIE
- LTR Lock PCIE LTR Configuration Lock
- Peer Memory Write Enable
   Peer Memory Write Enable/Disable

### SATA Configuration

Chipset	Aptio Setup — AMI	
Chipset SATA Configuration SATA Controller(s) SATA Mode Selection SATA Controller Speed Limit Aggressive LPM Support Serial ATA Port 1 Software Preserve Port 1 External Spin Up Device SATA Device Type Topology SATA Port 1 DevSIp DITO Configuration DITO Value DM Value	<pre>[Enabled] [AHCI] [Default] [Disabled] Empty Unknown [Enabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] [Disabled] 625 15</pre>	Enable/Disable SATA Device. ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Versia	on 2.22.1290 Copyright (C) :	2023 AMI

- SATA Controller(s)
  - Enable/Disable SATA Device.
- SATA Mode Selection Determines how SATA controller(s) operate.
- SATA Controller Speed Limit Indicates the maximum speed the SATA controller can support.
- Aggressive LPM Support
   Enable PCH to aggressively enter link power state
- Serial ATA Port 1
- Software Preserve
- Port 1
- External

Spin Up Device

If enabled for any of ports Staggered Spin Up will be performed and only the drives which have this option enabled will spin up at boot. Otherwise all drives spin up at boot.

- SATA Device Type Identify the SATA port is connected to Solid State Drive or Hard Disk Drive
- Topology Identify the SATA Topology if it is Default or ISATA or Flex or DirectConnect or M2
- SATA Port 1 DevSlp Enable/Disable SATA Port 1 DevSlp. For DevSlp to work, both hard drive and SATA port need to support DevSlp function, otherwise an unexpected behavior might happen. Please check board design before enabling it.
- DITO Configuration
- Enable/Disable DITO Configuration
- DITO Value
- DM Value

### USB Configuration



DM Value

Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC will not work.

- USB Overcurrent Lock
   Select 'Enabled' if Overcurrent functionality is used. Enabling this will make
   xHCI controller consume the Overcurrent mapping data.
- USB Overcurrent Lock Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.
#### Security Configuration

Chipset	Aptio Setup – AMI	
Security Configuration RTC Memory Lock BIOS Lock Force unlock on all GPIO pads	[Enabled] [Enabled] [Disabled]	Enable will lock bytes 38h–3Fh in the lower/upper 128–byte bank of RTC RAM
		++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values 52: Octimized Defende
		F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version	2.22.1290 Copyright (C) 2023	AMI

DM Value

Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC will not work.

- USB Overcurrent Lock
   Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.
- USB Overcurrent Lock Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

#### HD Audio Configuration



- HD Audio
  - Control Detection of the HD-Audio device.

## 3.2.4 Security

Aptio Setup – AMI Main Advanced Chipset <mark>Security </mark> Boot Save & Exit NVMe RPMB Key Migration MEBx		
Password Description		Set Administrator Password
If ONLY the Administrator's then this only limits acces only asked for when enterin If ONLY the User's password is a power on password and boot or enter Setup. In Set have Administrator rights. The password length must be in the following range: Wisiwm length	a password is set, is to Setup and is ig Setup. I is set, then this must be entered to up the User will	
Maximum length	3 20	↔: Select Screen
Administrator Password User Password		<pre>fl: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit</pre>
▶ Secure Boot	Version 2.22 1290 Convright	ESC: Exit

Aptio Setup – AMI Main Advanced Chipset <mark>Security</mark> Boot Save & Exit NVMe RPMB Key Migration MEBx		
Password Description		Secure Boot configuration
If ONLY the Administrator's p then this only limits access only asked for when entering If ONLY the User's password i is a power on password and mu boot or enter Setup. In Setup have Administrator rights. The password length must be in the following range:	assword is set, to Setup and is Setup. s set, then this st be entered to the User will	
Minimum length Maximum length Administrator Password User Password ▶ Secure Boot	3 20	<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Ve	rsion 2.22.1290 Copyright	(C) 2023 AMI

Security	Aptio Setup – AMI	
System Mode	Setup	
Secure Boot	[Disabled] Not Active	
Secure Boot Mode ▶ Restore Factory Keys ▶ Reset To Setup Mode ▶ Key Management	[Custom]	
		<pre>++: Select Screen 11: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2	.22.1290 Copyright (C) 2023	AMI

## Administrator Password

Set Administrator Password

User Password
 Set User Password

# Secure Boot Mode Secure Boot mode options: Standard or Custom.

#### Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot key databases

## Reset To Setup Mode Delete all Secure Reat key database

Delete all Secure Boot key databases from NVRAM

#### Key Management

Enables expert users to modify Secure Boot Policy variables without variable authentication.

## 3.2.5 Boot

Aptio Setup – AMI Main Advanced Chipset Security <mark>Boot</mark> Save & Exit NVMe RPMB Key Migration MEBx		
Boot Configuration Setup Prompt Timeout Bootup NumLock State Quiet Boot	<mark>1</mark> [On] [Disabled]	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Boot Option Priorities Boot Option #1	[UEFI: JetFlashTS4GJFV30 8.07, Partition 1 (JetFlashTS4GJFV30 8.07)] [UEFI: Built-in FFI	
Boot Uption #2 Driver Option Priorities	[UEF1: BUIIT-IN EF1 Shell]	<pre>++: Select Screen f↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>
Version 2.22.1290 Copyright (C) 2023 AMI		

#### Setup Prompt Timeout

Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.

- Bootup NumLock State
   Select the keyboard NumLock state.
- Quiet Boot
   Enable/Disable Quiet Boot option.

## 3.2.6 Save & Exit

Aptio Setup – AMI Main Advanced Chipset Security Boot <mark>Save &amp; Exit</mark> NVMe RPMB Key Migration MEBx		
Save Options Save Changes and Exit Discard Changes and Exit Save Changes and Reset Discard Changes and Reset Save Changes Discard Changes Default Options Restore Defaults	Exit system setup after saving the changes.	
Save as User Defaults Restore User Defaults Boot Override UEFI: JetFlashTS4GJFV30 8.07, Partition 1 (JetFlashTS4GJFV30 8.07) UEFI: Built-in EFI Shell	<pre> ++: Select Screen  14: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save &amp; Exit ESC: Exit</pre>	
Version 2.22.1290 Copyright (C) 2023	AMI	

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

## 3.2.7 MEBx



MEBx

Set ME configuration.



## 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, electronic, 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