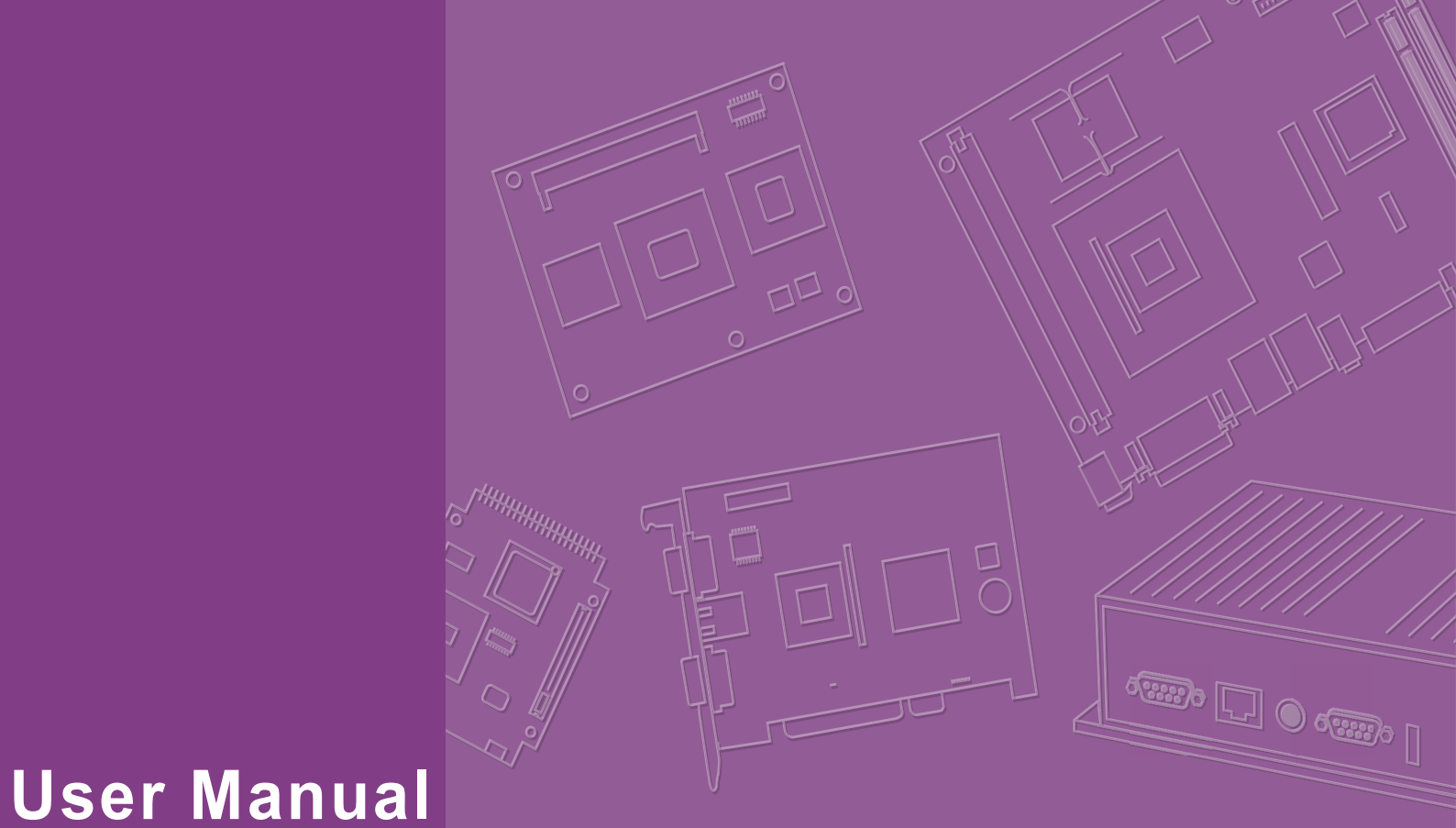




User Manual

ARK-2252

Fanless Embedded Box Computer

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2026 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice.

No part of this manual may be reproduced, copied, translated, or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. 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/>

For technical support and service, please visit our support website at: <https://www.advantech.com/en/support>

This manual is for the ARK-2252.

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 out-of-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.
3. If your product is diagnosed as defective, obtain a return merchandise authorization (RMA) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a 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!*



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



Note! *Notes provide optional additional information.*



Packing List

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

- 1 x ARK-2252 Unit
- 1 x User Manual (Simplified Chinese)
- 1 x China RoHS
- 1 x 4-pin plug-in block for power in
- 1 x 4-pin plug-in block for remote switch
- 2 x mounting bracket
- 2 x second memory pad
- 1 x Trellix, Acronis
- 1 x WISE-PaaS/DeviceOn Client Bundle

Ordering Information

Model Number	Description
ARK-2252-U1A1	Intel PTL U5-325 2HDMI+1typeC+4GbE+6USB+6COM
ARK-2252-S9A1	Intel PTL U7-358H 2HDMI+1typeC+4GbE+6USB+6COM
ARK-2252-U1A1U	Intel PTL U5-325 2HDMI+1typeC+4GbE+6USB+6COM MIT
ARK-2252-S9A1U	Intel PTL U7-358H 2HDMI+1typeC+4GbE+6USB+6COM MIT

Optional Accessories

Part Number	Description
96PSA-A230W24P4-3	ADP A/D 100-240V 230W 24V C14 TERMINAL BLOCK 4P
1702002600	Power cable 3-pin 183cm, USA type
1702002605	Power cable 3-pin 183cm, EU type
1702031801-11	Power cable 3-pin 183cm, UK type
1700000237	Power cable 3-pin 183cm, PSE type
1700001714	Power cable 3-pin 183cm, Taiwan BSMI
AMK-V019E	VESA mount kits
AMK-R005E	DIN Rail mount kits

Optional iDoor Modules

Part Number	Description
PCM-34D4R2-AE	Non-Isolated RS-232, DB37x1, M.2 Bkey(2242, USB)
PCM-34D2R2-AE	Isolated RS-232, DB9 x2, M.2 Bkey(2242, USB)
PCM-34R1TP-AE	Intel I225, 2.5Gb/s, IEEE 1588, TSN, RJ45*1, M.2
PCM-34R2GL-AE	2 Port Giga LAN Intel i350, M.2 B+M key
AMK-A0066	ARK-2252 2xUSB ports expansion module

Note! 1: PCM IO module need to add side bracket



a. 1x 1960065854N002 (side bracket)

b. 2x 19310305C0 (screw)

2. PCN M.2 2242/3042 idoor main board need to assembled with expansion bracket

a. 1x 1960110006N010 (expansion bracket)

b. 1x 193B0305E2 (M3x5L screw)

3. Cannot co-exist w/ internal USB 2.0 or PoE

Optional POE Modules

Part Number	Description
AMO-M021	POE Module A1 Single 30W w/ Heatsink
AMO-M022	POE Module A1 dual 15.4W w/ Heatsink

- Note!** 1: 30W PoE can be supported by LAN4 only
2: 15W PoE can be supported by LAN3 and LAN4
3: Cannot co-exist w/ internal USB 2.0 or iDoor



Optional Thermal Kit for 5g and Hailo Module

Part Number	Description
AMK-A0067	Thermal kit of ARK-2252 for 5G and Hailo AI B Key

- Note!** Condition may apply, contact your representative for further information.



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 openings on the enclosure are for air convection and protect the equipment from overheating. Do not cover the openings.
8. Ensure that the voltage of the power source is correct before connecting the equipment to a power outlet.
9. Position the power cord away from high-traffic areas. Do not place anything over the power cord.
10. All cautions and warnings on the equipment should be noted.
11. If the equipment is not used for a long time, disconnect the equipment from the power source to avoid damage from transient over-voltage.
12. Never pour liquid into an opening as this can cause fire or electrical shock.
13. Never open the equipment. For safety reasons, only qualified service personnel should open the equipment.

14. 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.
15. Do not leave the equipment in an environment with a storage temperature of below -40°C (-40°F) or above 85°C (185°F) as this may cause damage. The equipment should be stored in a controlled environment.
16. Any unverified component may cause unexpected damage. To ensure correct installation, always use the components (e.g., screws) provided in the accessory box.
17. **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.
18. 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.
19. In accordance with IEC 704-1:1982 specifications, the sound pressure level at the operator's position should not exceed 70 dB (A).
20. **DISCLAIMER:** These instructions are provided according to IEC 704-1 specifications.
Advantech disclaims all responsibility for the accuracy of any statements contained herein.
21. This product is intended to be supplied by an UL Listed power Adapter, or DC power source, rated: 12~24Vdc, 19.16-9.58A min, Tma=60°C min for DC power source, Tma= 40°C min for power adapter. Altitude: 2000 m maximum, if need further assistance, please contact Advantech for further information.
22. **RESTRICTED ACCESS AREA:** The equipment should only be installed in a Restricted Access Area.
23. While using optional PoE module, this equipment is only to be connected to PoE networks without routing to outside plants.

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. Les ouvertures sur le boîtier sont destinées à la convection d'air, protégeant ainsi l'équipement de la surchauffe. **NE COUVREZ PAS LES OUVERTURES.**
8. Au moyen d'un cordon d'alimentation connecté à une prise de courant avec mise à la terre.
9. Placez le cordon d'alimentation de sorte que personne ne puisse marcher dessus. Ne placez rien sur le cordon d'alimentation.
10. Tous les avertissements et mises en garde sur l'équipement doivent être notés.
11. Si l'appareil n'est pas utilisé pendant une longue période, débranchez-le du secteur pour ne pas être endommagé par une surtension transitoire.
12. Ne jamais verser de liquide dans les ouvertures de ventilation; Cela pourrait provoquer un incendie ou un choc électrique.
13. N'ouvrez jamais l'équipement. Pour des raisons de sécurité, seul le personnel de maintenance qualifié doit ouvrir l'équipement.
14. 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.
15. 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.
16. 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.
17. **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.
18. 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.
19. Niveau de pression acoustique au poste de l'opérateur selon la norme CEI 704-1: 1982 n'est pas supérieur à 70 dB (A).

20. **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.
21. Ce produit est conçu pour être alimenté par un adaptateur secteur homologué UL ou une source d'alimentation CC, caractéristiques: 12 à 24 Vcc, 19,16 à 9,58 A min, Tma = 60 °C min pour la source d'alimentation CC, Tma = 40 °C min pour l'adaptateur secteur. Altitude: 2 000 m maximum. Pour toute assistance supplémentaire, veuillez contacter Advantech.
22. **ZONE D'ACCES RESTREINTE:** L'équipement ne doit être installé que dans une zone d'accès restreint.
23. Lors de l'utilisation du module PoE optionnel, cet équipement doit uniquement être connecté à des réseaux PoE sans routage vers des installations extérieures.

Contents

Chapter 1 General Introduction1

1.1	Introduction	2
1.2	Specifications	3
	Table 1.1: Specifications	3
1.3	Mechanical Drawing	5
1.3.1	Dimensions	5
	Figure 1.1 ARK-2252 Mechanical Diagram	5

Chapter 2 Jumpers and Connectors7

2.1	Introduction	8
2.2	Jumper & Switches	8
2.2.1	Jumper Description	8
2.2.2	Jumper List	8
	Table 2.1: Jumper List	8
2.2.3	Jumper Locations.....	9
	Figure 2.1 Jumper Layout.....	9
2.2.4	Jumper Settings	9
	Table 2.2: SW_FUN_SEL: HW Function Select.....	9
	Table 2.3: JCMOS1: Clear CMOS.....	10
	Table 2.4: COM3 Mode Select (JSETCOM3).....	10
	Table 2.5: COM4 Mode Select (JSETCOM4).....	10
	Table 2.6: COM5 Mode Select (JSETCOM5).....	10
	Table 2.7: COM6 Mode Select (JSETCOM6).....	11
2.3	Connectors.....	11
2.3.1	External I/O Locations.....	11
	Figure 2.2 Front I/O Connector Diagram	11
	Figure 2.3 Rear I/O Connector Diagram.....	11
2.4	Connector Pin Definition	12
2.4.1	USB 3.2 - Gen2.....	12
	Table 2.8: USB 3.2 Gen2 Connector Pin Assignments	12
2.4.2	USB 2.0.....	12
	Table 2.9: USB 2.0 Connector Pin Assignments.....	12
2.4.3	Type C	13
	Table 2.10: Type C Connector Pin Assignments.....	13
2.4.4	DIO (GPIO)	14
	Table 2.11: GPIO Connector Pin Assignments	14
	Table 2.12: ARK-2252 GPIO Spec.	14
2.4.5	Ethernet Connector (2.5G LAN).....	15
	Table 2.13: Ethernet Connector Pin Assignments.....	15
2.4.6	Remote Switch Connector	15
	Table 2.14: Remote Switch Connector Pin Assignments	15
2.4.7	COM Connector	16
	Table 2.15: COM Port Connector Pin Assignments	16
2.4.8	CANBus Connector.....	17
	Table 2.16: CANBus Connector Pin Assignments	17
2.4.9	HDMI 2.1 Connector	18
	Table 2.17: HDMI Connector Pin Assignments	18
2.4.10	POE Pin Header (POE_PWR1) (Optional)	18
	Table 2.18: POE Pin Header (Optional) Pin Assignments	18
2.4.11	Dual USB Module (INT_USB1/2) (Optional)	19
	Table 2.19: Dual USB 2.0 Module (Optional) Pin Assignments ..	19
2.4.12	Phoenix Terminal Connector	19
	Table 2.20: Phoenix Terminal Connector	19

	2.4.13	Power On/ Off Button.....	20
	2.4.14	Audio Connector	20
2.5		Installation	20
	2.5.1	Expanded View.....	20
	2.5.2	Remove the Bottom Cover	21
	2.5.3	Memory Installation.....	22
	2.5.4	M.2 Module Installation.....	24
	2.5.5	Wall Mount Kit Installation (Optional).....	25
	2.5.6	VESA Mounting Installation (Optional)	25
	2.5.7	DIN Rail Kit Installation (Optional)	26
	2.5.8	PoE Module Installation (Optional)	27
	2.5.9	Expansion iDoor module Installation (Optional).....	28

Chapter 3 AMI BIOS Settings 31

3.1		Introduction	32
3.2		Entering BIOS Setup.....	32
	3.2.1	Main Setup.....	32
	3.2.2	Advanced BIOS Features Setup.....	33
	3.2.3	Security.....	93
	3.2.4	Boot	98
	3.2.5	Save & Exit	99

Chapter 1

General Introduction

This chapter details background information on the ARK-2252 series.

1.1 Introduction

ARK-2252 is an intelligent fanless embedded system powered by Intel® Core™ Ultra 3 Series (Panther Lake) processors. Featuring the latest hybrid-core architecture, the platform integrates CPU, GPU, and NPU technologies to deliver high performance with exceptional power efficiency. ARK-2252 accelerates edge AI workloads and is ideal for applications such as automated optical inspection (AOI), collaborative robots (cobots), autonomous mobile robots (AMRs), machine automation, and intelligent edge computing.

Rugged with Rich IO interface

ARK-2252 is equipped with dual-channel memory slots and supports up to 128 GB DDR5-7200 MT/s SODIMM memory. Designed for harsh industrial environments, the ruggedized system supports a wide operating temperature range of -20 ~ 60°C (-4 ~ 140°F) and a wide input voltage range of 12 ~ 24 VDC. The system I/O includes:

- 4 x USB 3.2 Gen2, 5V-0.9A
- 2 x USB 2.0, 5V-0.5A
- 6 x COM ports, (2 x full-function with RS-232/422/485, and 4 x RS-232/485)
- 1 x Type C w/ USB4, DP alt mode, 5V-3A
- 4 x 10/100/1000/2500 Mbps,
- 1 x Mic In/ Line Out,
- 2 x HDMI.
- 3 x M.2 slots, (1 x E key, 1 x M key, 1 x B key with SIM card slot)
- 2 x CANBus 2.0
- 1 x 8-bit DIO
- 1 x internal USB2.0, 5V-0.5A

ARK-2252 meets a wide range of international certifications, including CE, FCC Class B, CB, UL, CCC, BSMI, and UKCA.

Triple Displays Support

ARK-2252 supports high-resolution display with 2 x HDMI and 1 x Type C (DP alt mode), each capable of 4K resolution at up to 3840x2160@ 60Hz. The system's graphics are powered by integrated Intel® Xe 3 LPG

Built-In Intelligent Management Tools - Advantech SUSI API and DeviceOn

The Advantech SUSI API is an intelligent, cross-platform self-management tool that monitors system status and takes action when abnormalities are detected. It offers a valuable suite of programmable APIs, including multi-level watchdog timers, hardware monitoring, and other user-friendly interfaces. SUSI API enhances overall system reliability and intelligence. ARK-2252 also supports Advantech's WISE-DeviceOn solution, which enables easy remote management, allowing users to monitor, configure, and control a large number of devices-streamlining maintenance and recovery.

1.2 Specifications

Table 1.1: Specifications

Processor System	CPU	Intel® Core™ Ultra 7 358H (12Xe)	Intel® Core™ Ultra 5 325 (4Xe)
	Frequency	1.9GHz up to 4.8GHz	2.1GHz up to 4.5GHz
	Core Number	16	8
	BIOS	AMI EFI 512Mbit	
	AI Capability	180 TOPS	95 TOPS
Memory	Technology	DDR5 6400/7200 MT/s CSOD-IMM	DDR5 6400 MT/s CSODIMM
	Max capacity	up to 128GB	
	Socket	2x 262-pin SODIMM (no support ECC)	
Graphic	Chipset	Intel® Xe 3 LPG up to 192EU (12Xe) Intel® Xe 3 LPG (4Xe)	
	HDMI	2x HDMI 2.1 TMDs: 3840x2160@ 60Hz	
	Type C DP	1x DP via USB Type C Alt mode: 3840x2160@ 60Hz	
	Triple Display	2 x HDMI + 1 x Type C DP	
Ethernet	LAN1	10/100/1000/2500 Mbps Intel i226V GbE, support Wake On LAN	
	LAN2	10/100/1000/2500 Mbps Intel i226V GbE, support Wake On LAN	
	LAN3	10/100/1000/2500 Mbps Intel i226V GbE, support Wake On LAN, (support PoE module)	
	LAN4	10/100/1000/2500 Mbps Intel i226V GbE, support Wake On LAN, (support PoE module)	
Audio	Interface	1x, (Mic-in and Line-out by Realtek ALC888S by OS)	
I/O Interface	Serial Ports	2 x RS232/422/485 (COM1/2) (Default: RS-232, support High speed COM), Emodified by BIOS	
		4 x RS232/485 (COM3/4/5/6), (Default: RS-485), modified by jumper and BIOS	
	USB Ports Type A	4 x USB3.2 Gen2 (w/ Cable locking mechanism)	
		2 x USB2.0 (w/ Cable locking mechanism)	
		1 x internal USB 2.0 Type A for security dongle (cannot co-exist w/ iDoor or PoE)	
	USB Port Type C	1x USB Type C w/ USB4, DP alt mode, 5V-3A	
	GPIO	1x, 8-bit Programmable GPIO	
	CANBus	2x, DB9 (CANBus 2.0)	
Expansion	M.2	Remote Switch	1x 4pin connector
		3x, Key-B 3042/ 3052 (PCIe Gen4 x2, USB3.2) w/ 1 x SIM card slot, for 5G/AI/iDoor module, (modified by jumper) Key-E 2230 (PCIe Gen4 x1, USB2.0), for WiFi module Key-M 2280 (PCIe Gen5 x4)	
Storage	M.2	Default: 1x M.2 2280 M key (PCIe Gen5 x4) Optional: 1x M.2 2242 B key (PCIe Gen4x2) support Intel SW RAID, up to 512G	
Other	TPM	TPM2.0, on board	
	Watch dog	255 levels timer interval, setup by software	
Software Support	Microsoft Windows	Windows 11 Enterprise (LTSC)	
	Linux	By project support	

Table 1.1: Specifications

Power Requirement	Connector	1x, 4pin Phoenix Contact
	Power Type	AT/ATX (default ATX)
	Power Input Voltage	12~24V
	Power Adapter (optional)	230W (96PSA-A230W24P4-3)
Power Consumption	Typical	358H: 16.8W; 325:18.3W
	Max	358H: 36.7W; 325: 34.1W
Mechanical	Construction	Aluminum top + metal bottom
	Mounting	Default: Wall Mount
Optional: DIN-rail / VESA Mount	Dimensions (W x H x D)	260 x 60 x 145.2 mm
	Weight	2.675kg
Environment	Operating Temperature	With extended temperature 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, 1hr/axis (with Wall Mount and SSD)
	Shock during Operation	30 G, IEC-60068-2-27, half sine, 11 ms duration (with Wall Mount and SSD)
Certification	EMC	CE/FCC Class B, CCC, BSMI, UKCA
	Safety	CB, UL, CCC, UKCA

1.3 Mechanical Drawing

1.3.1 Dimensions

W/O Mounting: 260 x 60 x 145.2 mm (W x H x D)

W/ Mounting: 288 x 60.5 x 145.2 mm (W x H x D)

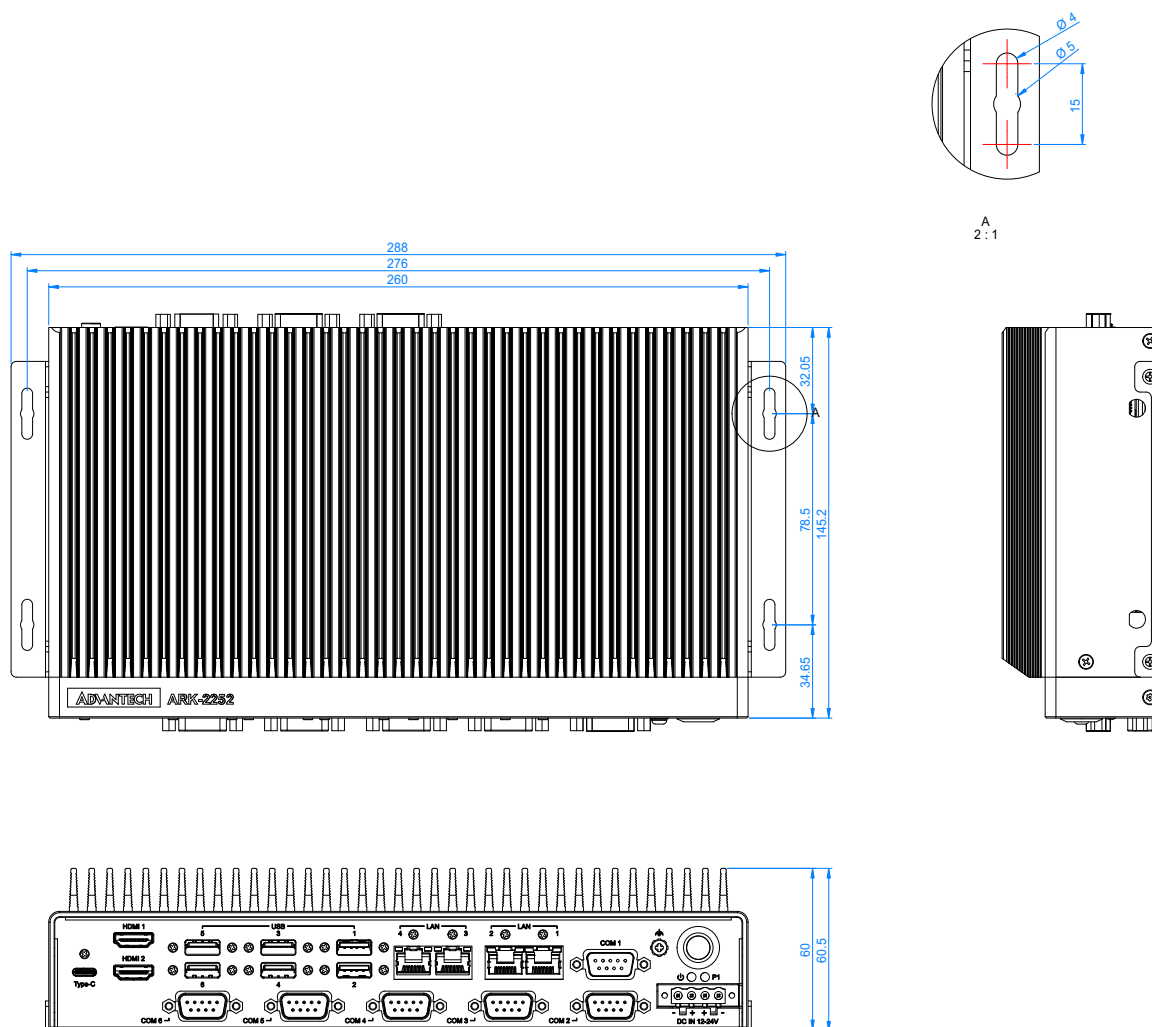


Figure 1.1 ARK-2252 Mechanical Diagram

Chapter 2

Jumpers and Connectors

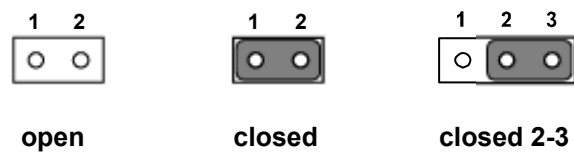
2.1 Introduction

The following sections show the internal jumper settings and the external connector pin assignments for different applications.

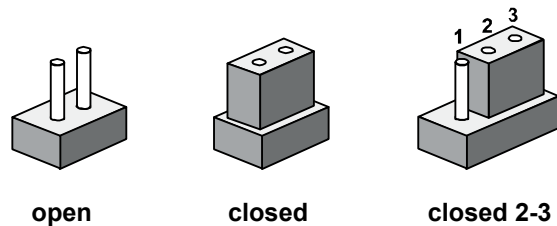
2.2 Jumper & Switches

2.2.1 Jumper Description

You may configure ARK-2252 to match the needs of your application by setting jumpers. A jumper is a metal bridge used to close an electric circuit. It consists of two metal pins and a small metal clip (often protected by a plastic cover) that slides over the pins to connect them. To close a jumper, you connect the pins with the clip. To open a jumper, remove the clip. Sometimes a jumper will have three pins, labeled 1, 2, and 3. In this case you would 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
SW_FUN_SEL	ATX / AT select and M.2 Key B interface Selection
JCMOS1	Clear CMOS
JSETCOM3	COM3 Mode Select
JSETCOM4	COM4 Mode Select
JSETCOM5	COM5 Mode Select
JSETCOM6	COM6 Mode Select

2.2.3 Jumper Locations

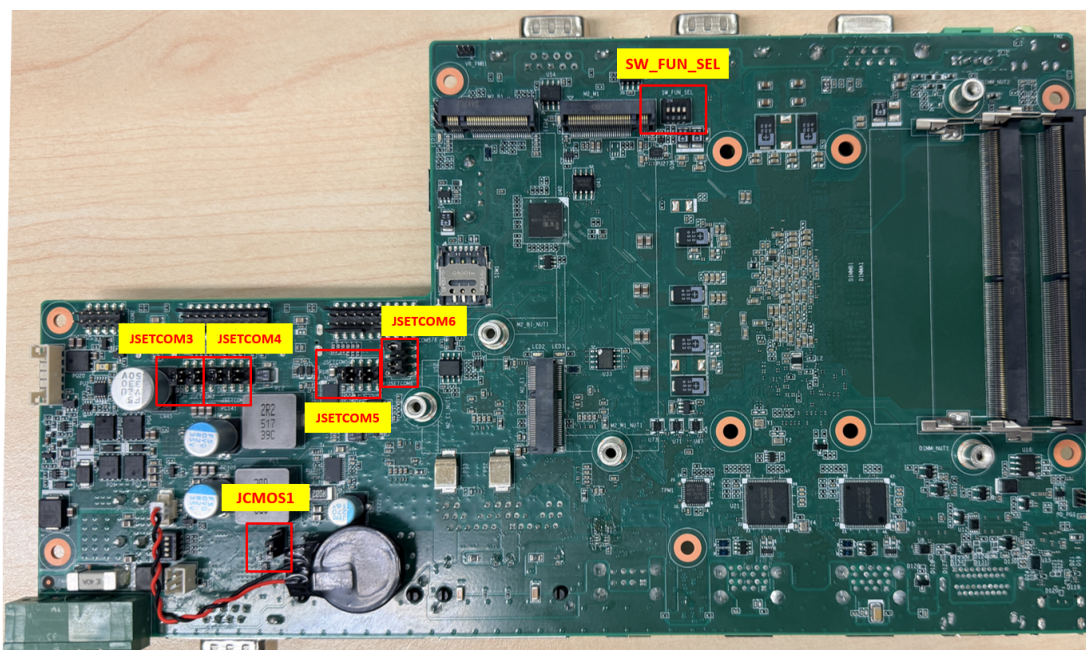


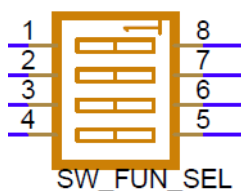
Figure 2.1 Jumper Layout

2.2.4 Jumper Settings

2.2.4.1 Function Select (SW_FUN_SEL)

Table 2.2: SW_FUN_SEL: HW Function Select

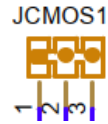
Pin	Description
(1-8)	ATX / AT select Off: ATX mode (default), On: AT mode
(2-7)	M.2 Key B interface Selection Off: USB3 (default), On: PCIe
(3-6)	Reserved Off (default)
(4-5)	Reserved Off (default)



2.2.4.2 Clear CMOS (JCMOS1)

Table 2.3: JCMOS1: Clear CMOS

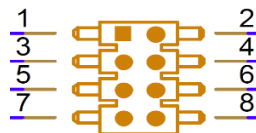
Pin	Description
(1-2) closed	Normal Operation (Default)
(2-3) closed	Clear CMOS



2.2.4.3 COM3 Mode Select (JSETCOM3)

Table 2.4: COM3 Mode Select (JSETCOM3)

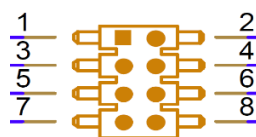
Pin	Description
(1-2) & (5-6) closed	RS-232
(3-4) & (7-8) closed	RS-485 (Default)



2.2.4.4 COM4 Mode Select (JSETCOM4)

Table 2.5: COM4 Mode Select (JSETCOM4)

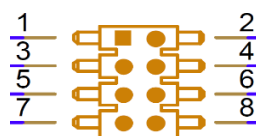
Pin	Description
(1-2) & (5-6) closed	RS-232
(3-4) & (7-8) closed	RS-485 (Default)



2.2.4.5 COM5 Mode Select (JSETCOM5)

Table 2.6: COM5 Mode Select (JSETCOM5)

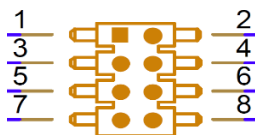
Pin	Description
(1-2) & (5-6) closed	RS-232
(3-4) & (7-8) closed	RS-485 (Default)



2.2.4.6 COM6 Mode Select (JSETCOM6)

Table 2.7: COM6 Mode Select (JSETCOM6)

Pin	Description
(1-2) & (5-6) closed	RS-232
(3-4) & (7-8) closed	RS-485 (Default)



2.3 Connectors

2.3.1 External I/O Locations

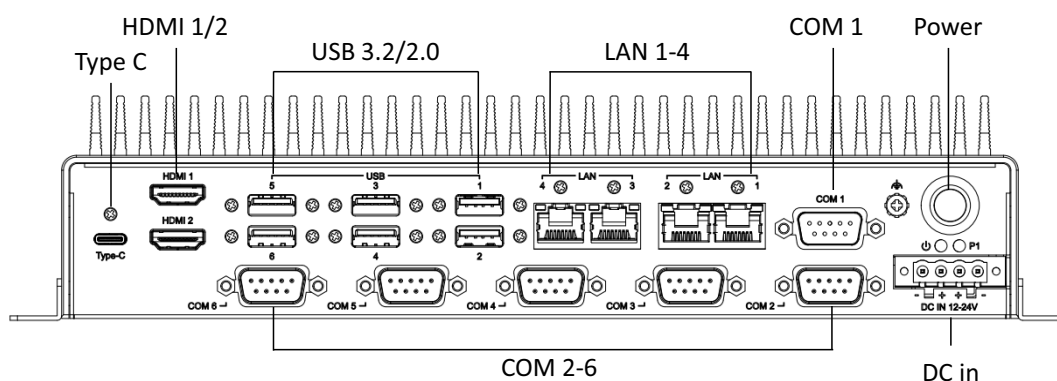


Figure 2.2 Front I/O Connector Diagram

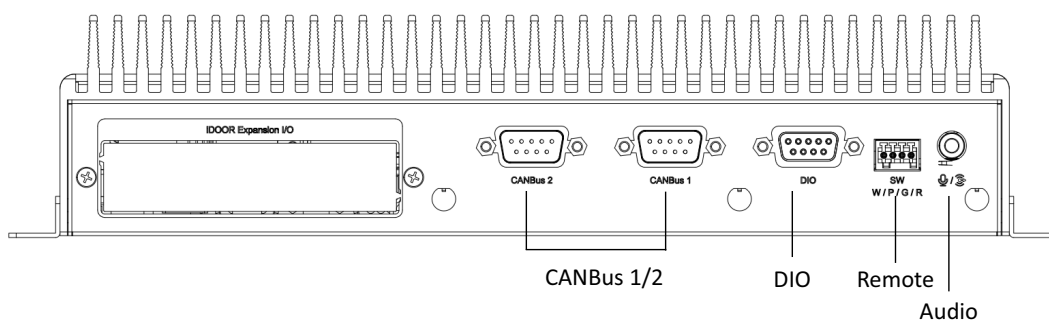


Figure 2.3 Rear I/O Connector Diagram

2.4 Connector Pin Definition

2.4.1 USB 3.2 - Gen2

The ARK-2252 supports 4 x USB 3.2 Gen2, w/ 5V-0.9A. Compliant with the USB XHCI, Rev. 3.2 revision standard. The USB 3.2 Gen2 connectors include both legacy pins for compatibility with USB 2.0 devices and additional pins to support full USB 3.2 functionality.

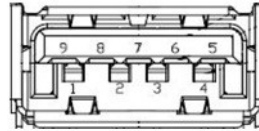


Table 2.8: USB 3.2 Gen2 Connector Pin Assignments

Pin	Signal Name	Pin	Signal Name
1	+5V	2	USB_data-
3	USB_data+	4	GND
5	SSRX-	6	SSRX+
7	GND	8	SSTX-
9	SSTX+		

2.4.2 USB 2.0

The ARK-2252 supports 2 x USB 2.0, w/ 5V-0.5A, and 1 x internal USB 2.0 Type A for security dongle, 5V-0.5A.

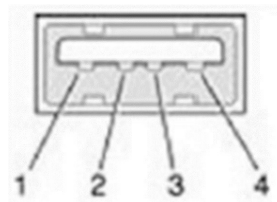


Table 2.9: USB 2.0 Connector Pin Assignments

Pin	Signal Name	Pin	Signal Name
1	+5V	2	USB_data-
3	USB_data+	4	GND

2.4.3 Type C

ARK-2252 provides 1 x USB Type C w/ USB4, DP alt mode, 5V-3A.



Table 2.10: Type C Connector Pin Assignments

Pin	Signal Definition
A1	GND
A2	TX1+
A3	TX1-
A4	VBUS
A5	CC1
A6	D+
A7	D-
A8	SBU1
A9	VBUS
A10	RX2-
A11	RX2+
A12	GND
B1	GND
B2	TX2+
B3	TX2-
B4	VBUS
B5	VCONN
B6	NC
B7	NC
B8	SBU2
B9	VBUS
B10	RX1-
B11	RX1+
B12	GND

2.4.4 DIO (GPIO)

ARK-2252 provides a programmable GPIO by D-sub 9 interface ports.

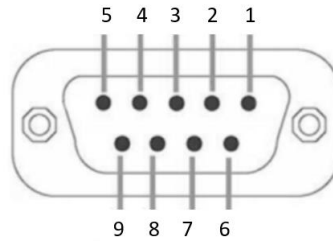


Table 2.11: GPIO Connector Pin Assignments

Pin	Signal Definition
1	EC_B_GPIO1
2	EC_B_GPIO2
3	EC_B_GPIO3
4	EC_B_GPIO4
5	EC_B_GPIO5
6	EC_B_GPIO6
7	EC_B_GPIO7
8	EC_B_GPIO8
9	GND

Table 2.12: ARK-2252 GPIO Spec.

Item	Description
Output Type	Open-Drain with 4.7K ohm pull-up resistor (depending on EC settings)
VIH (Input High Voltage)	$\geq 2.0V$ (typical)
VIL (Input Low Voltage)	$\leq 0.8V$ (typical)
VOH (Output High Voltage)	$\geq 2.4V$ @ IOH = 2~16 mA (typical for 5V IO)
VOL (Output Low Voltage)	$\leq 0.4V$ @ IOL = -2~-24 mA
IOH / IOL (Output Current Drive)	± 4 mA (typical; some pins support up to ± 8 mA)

2.4.5 Ethernet Connector (2.5G LAN)

The ARK-2252 is equipped with 4 x Ethernet controllers that are fully compliant with IEEE 802.3u 10/100/1000/2500 Mbps CSMA/CD standards. These Ethernet ports provide a standard RJ-45 jack connector with LED indicators on the front side.

Left LED behavior: Speed status

1. 10/100 Mbps: Off
2. 1000 Mbps: Solid orange
3. 2500 Mbps: Solid green

Right LED behavior: Link status

1. Link (without any loading): Solid green
2. Active (loading): Flashing green

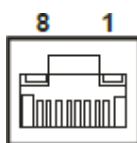


Table 2.13: Ethernet Connector Pin Assignments

Pin	10/100/1000/2500 BaseT Signal Name
1	TX+
2	TX-
3	RX+
4	MDI2+
5	MDI2-
6	RX-
7	MDI3+
8	MDI3-

2.4.6 Remote Switch Connector

ARK-2252 provides a remote switch connector for power control. From left to right, the pins are Reset, GND, Power Switch, and WDT.

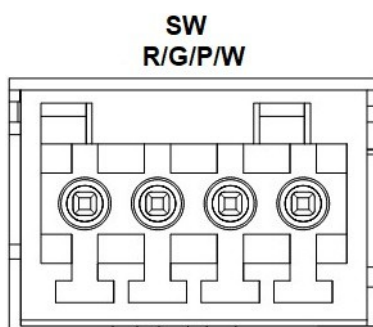


Table 2.14: Remote Switch Connector Pin Assignments

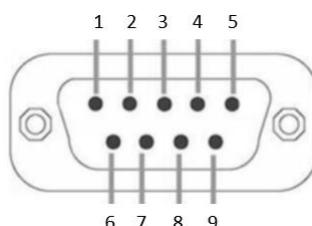
Pin	Signal Definition
W	W = WDT

Table 2.14: Remote Switch Connector Pin Assignments

P	P = Power Button
G	G = GND
R	R = Reset Button

2.4.7 COM Connector

ARK-2252 provides two full-function COM ports (COM1 and COM2) supporting RS-232/422/485 via DB9 connectors. The default setting is RS-232. RS-232, RS-422, or RS-485 mode can be configured through the BIOS. The system also provides four additional COM ports supporting RS-232/485 via DB9 connectors. The default setting is RS-232. RS-485 mode can be enabled through switch and BIOS settings.

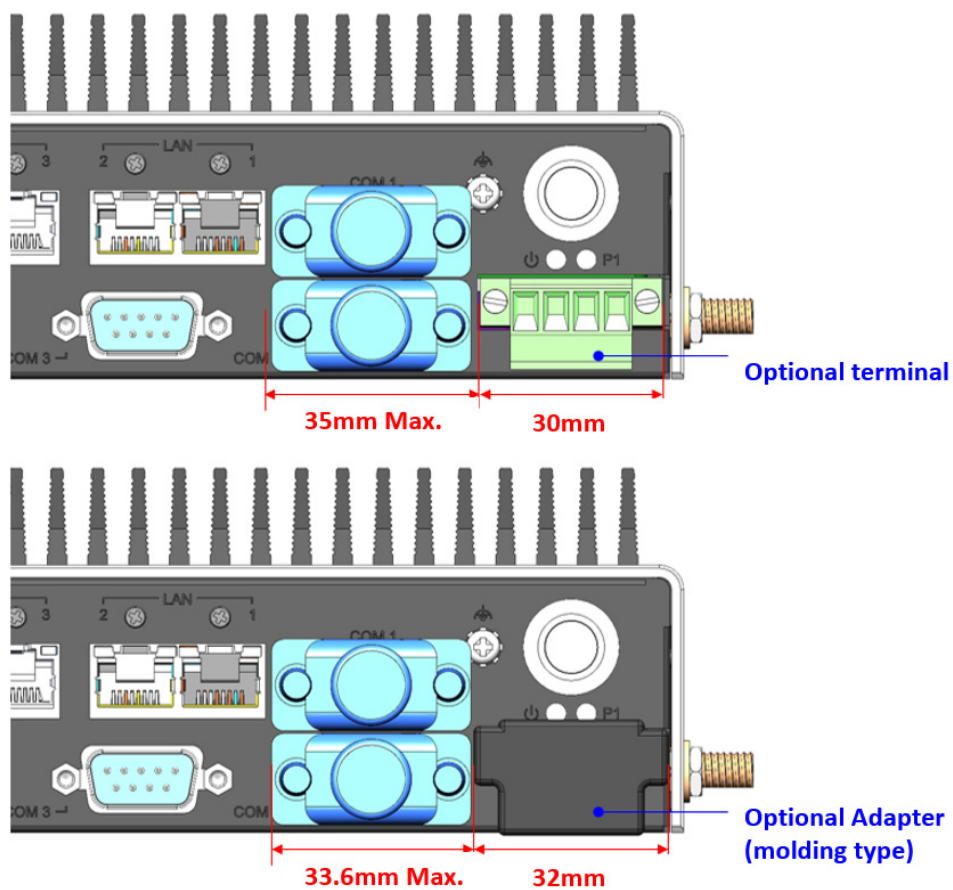
**Table 2.15: COM Port Connector Pin Assignments**

	RS-232	RS-422	RS-485
Pin	Signal Definition	Signal Definition	Signal Definition
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

Note!



1. The width of the device connected to COM2 must not exceed 35 mm when the optional terminal block in the accessory box is used.
2. The width of the device connected to COM2 must not exceed 33.6 mm when the optional adapter specified in the datasheet is used.



2.4.8 CANBus Connector

ARK-2252 provides 2 x CANBus by D-sub 9 interface ports.

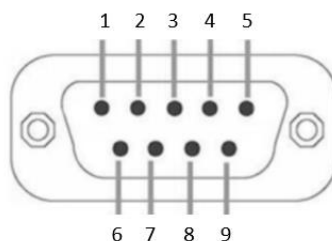


Table 2.16: CANBus Connector Pin Assignments

Pin	Signal Definition
1	NC
2	CAN1_D-
3	GND
4	NC
5	NC
6	NC
7	CAN1_D+
8	NC
9	NC

2.4.9 HDMI 2.1 Connector

ARK-2252 is equipped with 2 x 19-pin HDMI Type-A interface. The HDMI link supports resolutions up to 3840x2160@ 60Hz.

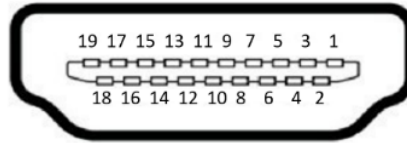


Table 2.17: HDMI Connector Pin Assignments

Pin	Signal Definition	Pin	Signal Definition
1	TMDS Data 2+	2	TMDS Data 2 shield
3	TMDS Data 2-	4	TMDS Data 1+
5	TMDS Data 1 shield	6	TMDS Data 1-
7	TMDS Data 0+	8	TMDS Data 0 shield
9	TMDS Data 0-	10	TMDS clock+
11	TMDS clock shield	12	TMDS clock-
13	CEC	14	Reserved
15	SCL	16	SDA
17	DDC/CEC Ground	18	+5V
19	Hot Plug Detect		

2.4.10 POE Pin Header (POE_PWR1) (Optional)

ARK-2252 provides 1 x POE pin header for optional POE module.

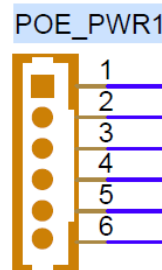


Table 2.18: POE Pin Header (Optional) Pin Assignments

Pin	Signal Definition	Pin	Signal Definition
1	+V48_LAN1+	2	+V48_LAN1-
3	+V48_LAN2+	4	+V48_LAN2-
5	GND	6	+VDCIN_POE

2.4.11 Dual USB Module (INT_USB1/2) (Optional)

ARK-2252 provides 1 x dual USB 2.0 module pin header.

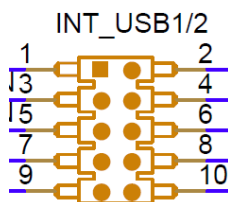
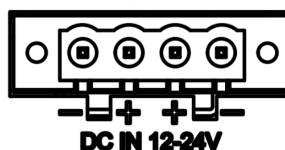


Table 2.19: Dual USB 2.0 Module (Optional) Pin Assignments

Pin	Signal Name	Pin	Signal Name
1	+5V_INT_USB	2	+5V_INT_USB
3	HUB2_DN3_CN	4	HUB2_DN4_CN
5	HUB2_DP3_CN	6	HUB2_DP4_CN
7	GND	8	GND
9	GND_USBIO	10	GND_USBIO

2.4.12 Phoenix Terminal Connector

ARK-2252 supports a 12–24 VDC power input through a 4-pin Phoenix terminal block connector. Connect the positive (+) and negative (-) power wires to the corresponding terminals on the power connector.



Note!



1. Use power supply wires rated for at least 115°C.
2. The terminal block supports up to 14 AWG wire. Tighten the terminal screws to 7 lb-in. Use copper conductors only. Installation must be performed by qualified service personnel.
3. To meet the maximum current requirement, both sets of terminal block connections must be used simultaneously. The current through any single pin must not exceed 16 A.
4. The equipment power cord must be connected to a properly grounded power outlet.

Table 2.20: Phoenix Terminal Connector

Pin	Signal Name	Pin	Signal Name
-	GND	+	V-in

2.4.13 Power On/ Off Button

The ARK-2252 power button supports dual functions: Power On and Power Off.

Pressing and holding the button for 4 seconds will power off the system. Additional power button functions can be configured via the operating system.



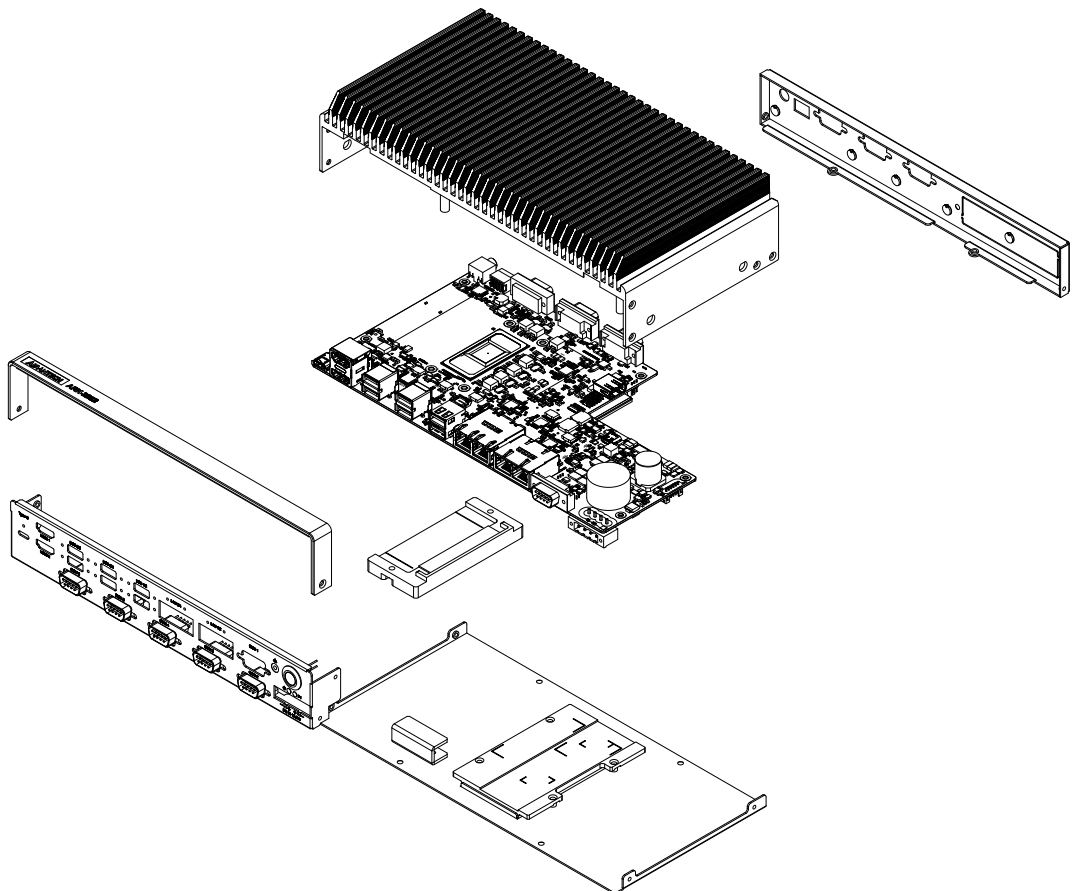
2.4.14 Audio Connector

The ARK-2252 features one audio jack that supports either Line-Out or Mic-In. The function can be configured through the operating system. The audio interface is controlled by the ALC888S codec and complies with the Azalia HD Audio specification.



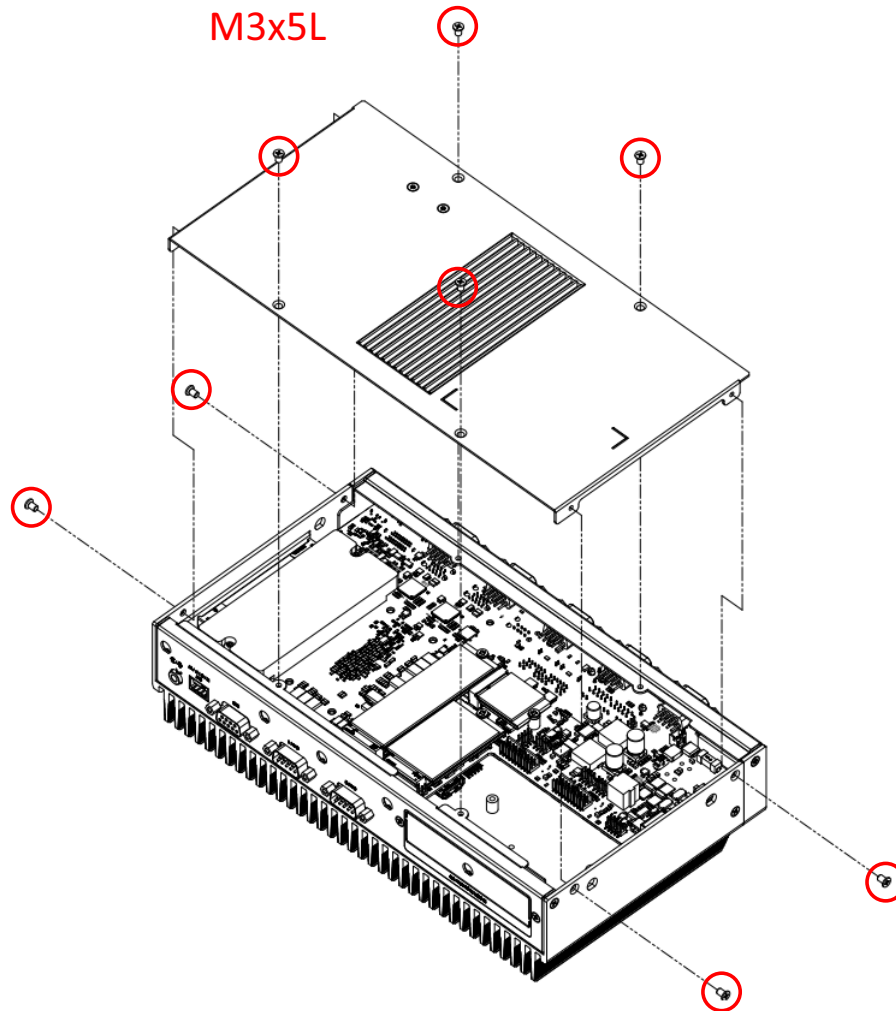
2.5 Installation

2.5.1 Expanded View



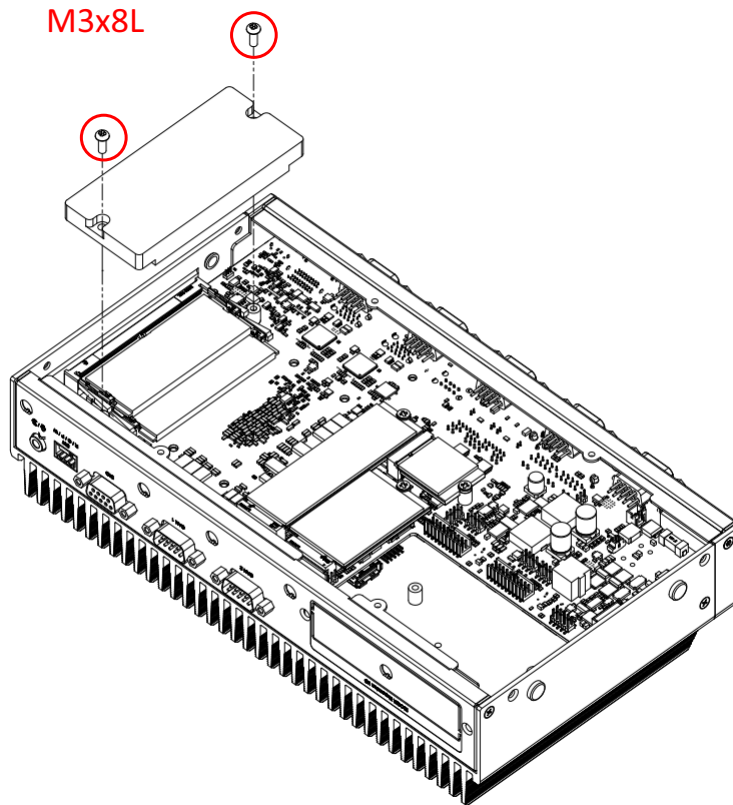
2.5.2 Remove the Bottom Cover

1. Unscrew the four M3x5L screws on the bottom cover.
Dévissez les 4 vis M3x5L du couvercle inférieur.
2. Unscrew the four M3x5L screws on the sides of the casing.
Dévissez les 4 vis M3x5L sur les côtés du boîtier.



2.5.3 Memory Installation

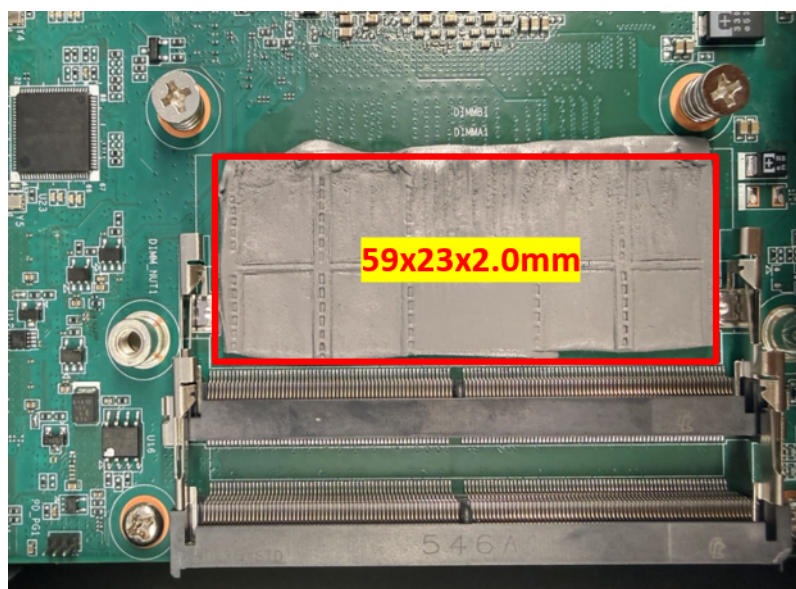
1. Remove the bottom cover. (2.5.2)
Retirez le couvercle inférieur (2.5.2).
2. Remove the memory heatsink by unscrewing the two M3x8L screws.
Retirez le dissipateur thermique de la mémoire en dévissant les 2 vis M3x8L.
3. Install the memory in the upper slot, and reinstall the heat sink and the bottom cover using the same screws.
Installez la mémoire dans l'emplacement supérieur, remettez en place le dissipateur thermique et le couvercle inférieur à l'aide des mêmes vis.



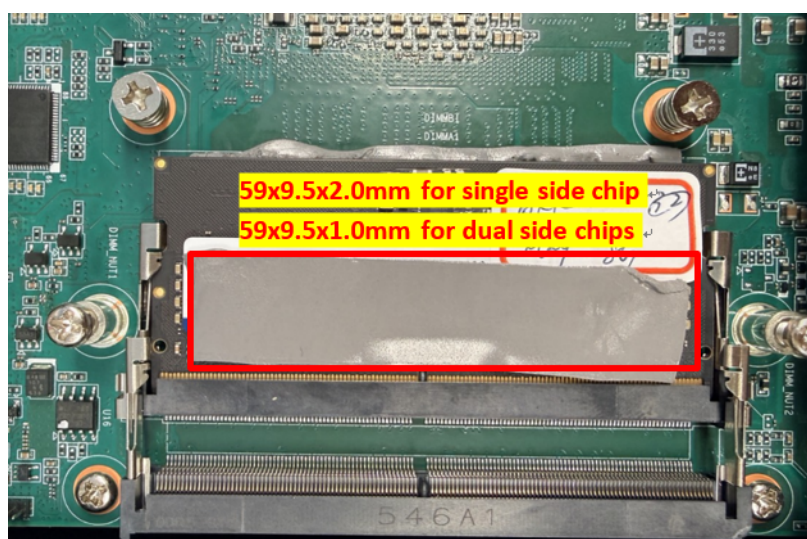
Note! There are two thermal pads for the second memory in the accessory box. Please install the thermal pad for the second RAM if needed
Deux pads thermiques pour la seconde barrette de mémoire sont fournis dans la boîte d'accessoires. Veuillez installer le pad thermique correspondant si nécessaire.

Pad for 2nd RAM *Module pour 2e RAM*

1. Thermal pad on the board
Coussinet sur la planche



2. Thermal pad on 2nd memory
Pad sur la 2ème mémoire

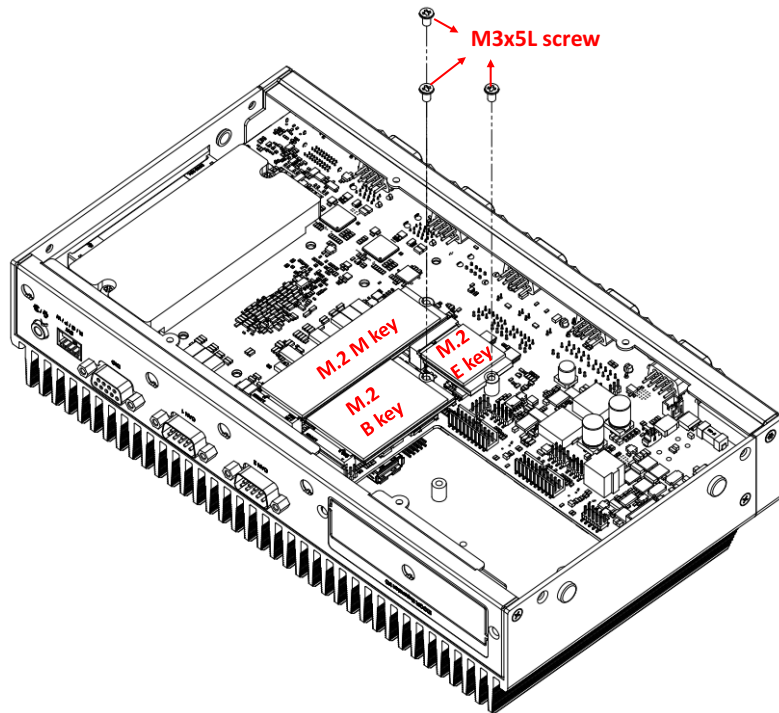


2.5.4 M.2 Module Installation

1. Remove the bottom cover (2.5.2).
Retirez le couvercle inférieur (2.5.2).
2. Install the M.2 module using the M3x5L screws from the accessory box.
Installez le module M.2 avec la vis M3x5L dans la boîte d'accessoires.
3. Replace the bottom cover using same screws.
Remettez le capot inférieur en place en utilisant les mêmes vis.

M.2 Module Diagram.

Schéma du module M.2.



Note!

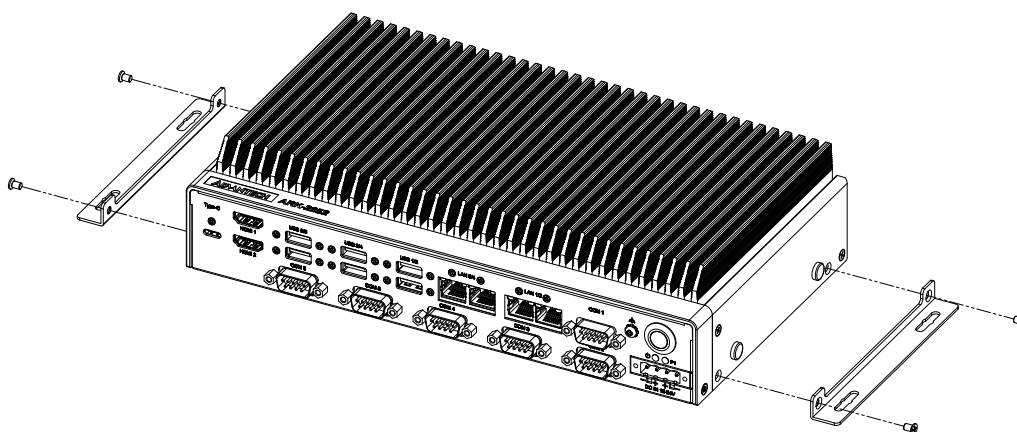


The M-Key is used by default for storage devices, the E-Key is designated for Wi-Fi modules, and the B-Key supports 5G, AI cards, or iDoor modules.

La clé M est utilisée par défaut pour les périphériques de stockage, la clé E est destinée aux modules Wi-Fi et la clé B prend en charge la 5G, les cartes IA ou les modules iDoor.

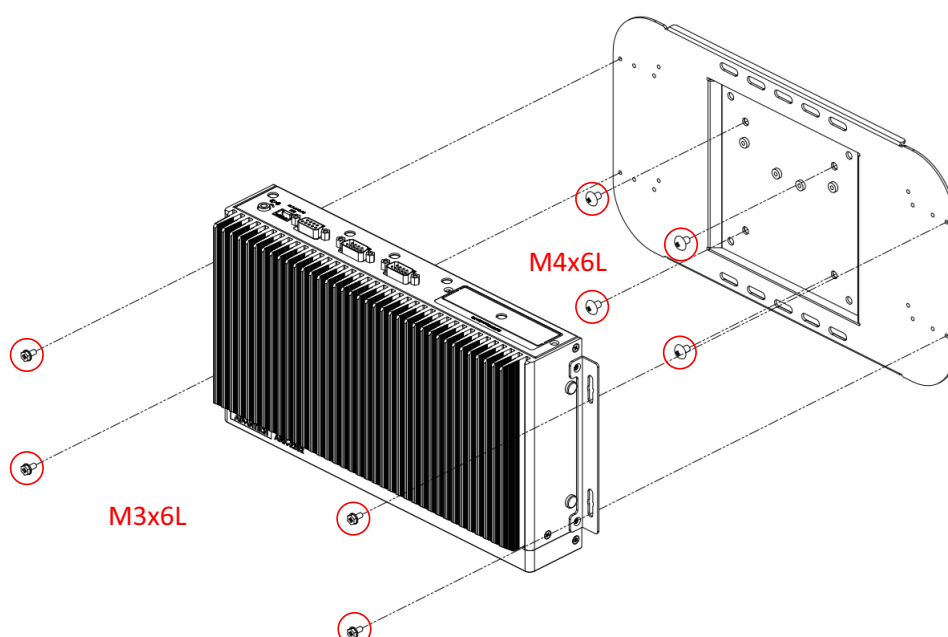
2.5.5 Wall Mount Kit Installation (Optional)

1. Unscrew the four M3x5L screws on the sides of the housing.
Dévissez les 4 vis M3x5L sur les côtés du boîtier.
2. Attach the two wall-mounting brackets from the accessory box using the same screws as those used for the side housing.
Fixez les 2 supports de montage mural dans la boîte d'accessoires avec les mêmes vis que celles du boîtier latéral.



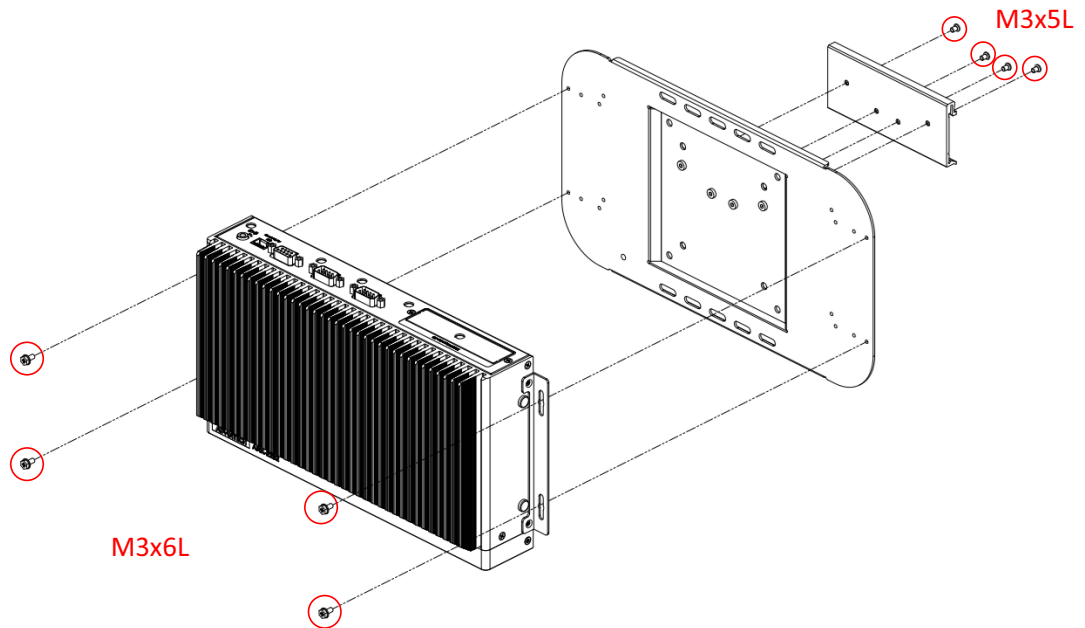
2.5.6 VESA Mounting Installation (Optional)

1. Install wall mount kit (2.5.5).
Installer le kit de montage mural (2.5.5).
2. Install the VESA mount onto the designated surface or object using the four M4x6L screws provided in the VESA mount accessory box.
Installez le support VESA sur la surface ou l'objet désigné à l'aide des 4 vis M4x6L fournies dans la boîte d'accessoires pour support VESA.
3. Install ARK-2252 onto the VESA mount with the four M3x6L screws from the VESA mount accessory box.
Installez l'ARK-2252 sur le support VESA avec 4 vis M3x6L provenant de la boîte d'accessoires du support VESA.



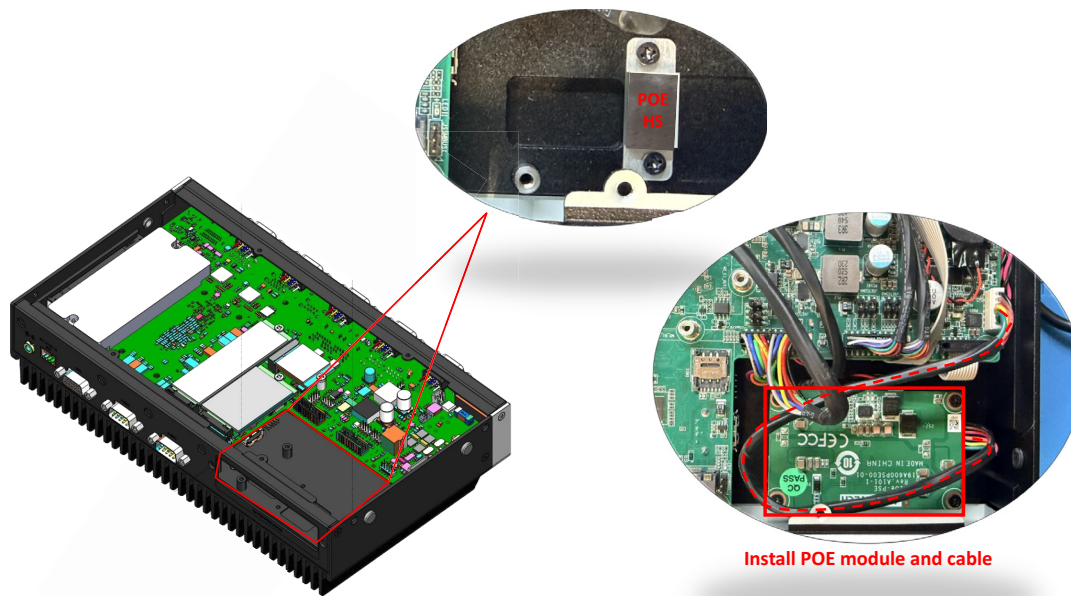
2.5.7 DIN Rail Kit Installation (Optional)

1. Install wall mount kit (2.5.5).
Installer le kit de montage mural (2.5.5).
2. Install the DIN-rail bracket at the back of VESA mount with the four M3x5L screws in the Din-rail accessory box.
Installez le support pour rail DIN à l'arrière du support VESA à l'aide des 4 vis M3x5L fournies dans la boîte d'accessoires du rail DIN.
3. Install ARK-2252 onto the VESA mount with the four M3x6L screws from the VESA mount accessory box.
Installez l'ARK-2252 sur le support VESA avec 4 vis M3x6L provenant de la boîte d'accessoires du support VESA.



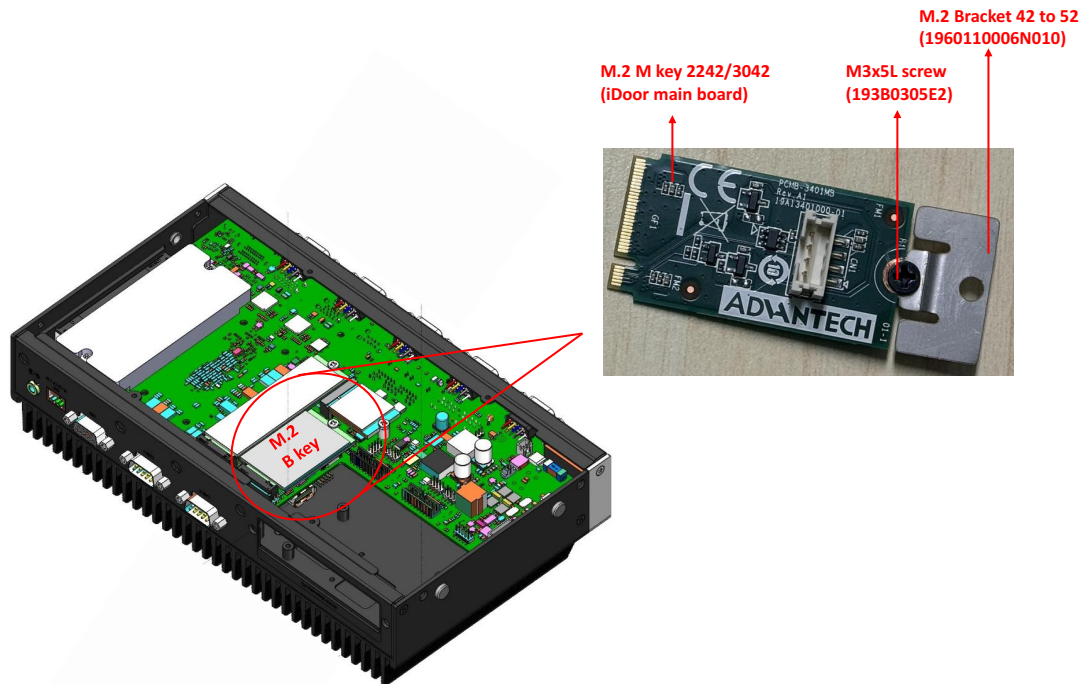
2.5.8 PoE Module Installation (Optional)

1. Remove the bottom cover. (2.5.2)
Retirez le couvercle inférieur (2.5.2).
2. Install POE heatsink on the top cover using two M3x5 screws.
Installez le dissipateur thermique POE sur le couvercle supérieur avec 2 vis M3x5.
3. Connect the POE module to the cable, then install it on the heatsink using the four M3x5 screws.
Connectez le module POE au c?ble, puis installez-le sur le dissipateur thermique avec 4 vis M3x5.
4. Reinstall the bottom cover and secure it using the original screws.
Réinstallez le couvercle inférieur et fixez-le à l'aide des vis d'origine.



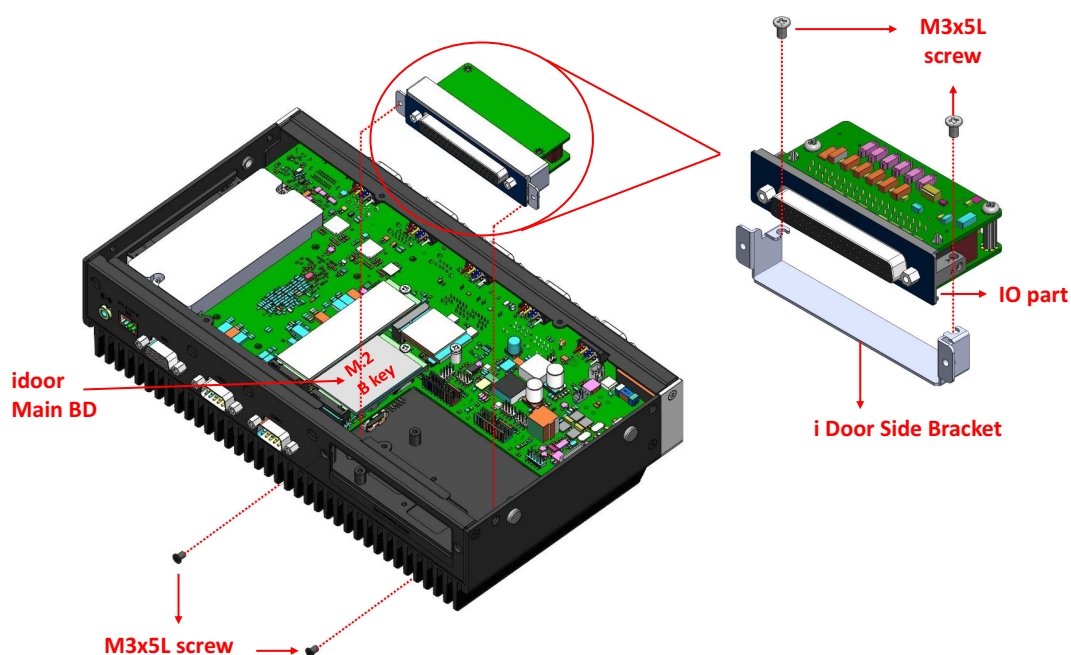
2.5.9 Expansion iDoor module Installation (Optional)

1. Remove the bottom cover. (2.5.2)
Retirez le couvercle inférieur (2.5.2).
2. Fasten the iDoor motherboard to the extension bracket using an M3x5L screw, then install the assembly into the M.2 B-key slot of the ARK-2252 using an M3x5L screw.
Vissez la carte mère idoor avec le support d'extension à l'aide d'une vis M3x5L, puis installez-les sur l'emplacement de clé M.2 B de l'ARK-2252 à l'aide d'une vis M3x5L.

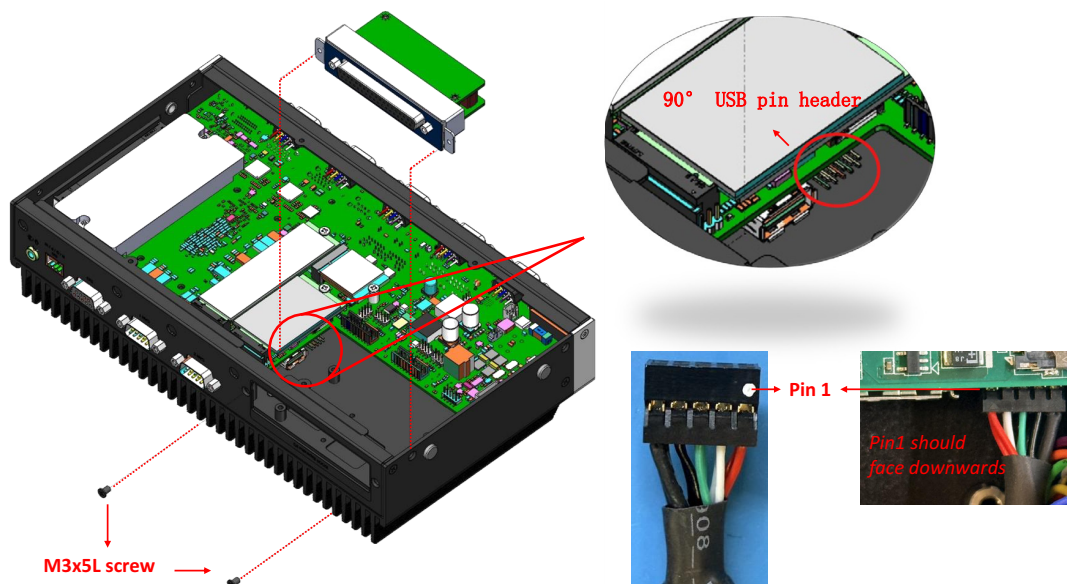


3. Screw the iDoor IO part to side bracket using two M3x5L screws.
Vissez la partie idoor IO au support latéral avec 2 vis M3x5L.
4. Install the iDoor cable, then install the iDoor I/O module into the ARK-2252 chassis.
Installez le cable idoor, puis installez la partie idoor IO dans le bo?tier de l'ARK-2252.

5. Replace the bottom cover using the same screws.
Remettez le capot inférieur en place en utilisant les mêmes vis.



6. For optional USB idoor (AMK-A0066) there is no M.2 main board, only a cable with connectors. Please connect this cable to the internal 90° USB pin header connector on the ARK-2252 main board.
Pour le module USB idoor optionnel (AMK-A0066), il n'y a pas de carte mère M.2 mais uniquement un câble avec connecteurs. Veuillez installer ce câble sur le connecteur USB interne à 90° de la carte mère ARK-2252.



Note! The white dot represents pin1 and should face downwards.
Le point blanc représente la broche 1 et doit être orienté vers le bas.



Chapter 3

AMI BIOS Settings

This chapter details instructions of setting BIOS configuration data.

3.1 Introduction

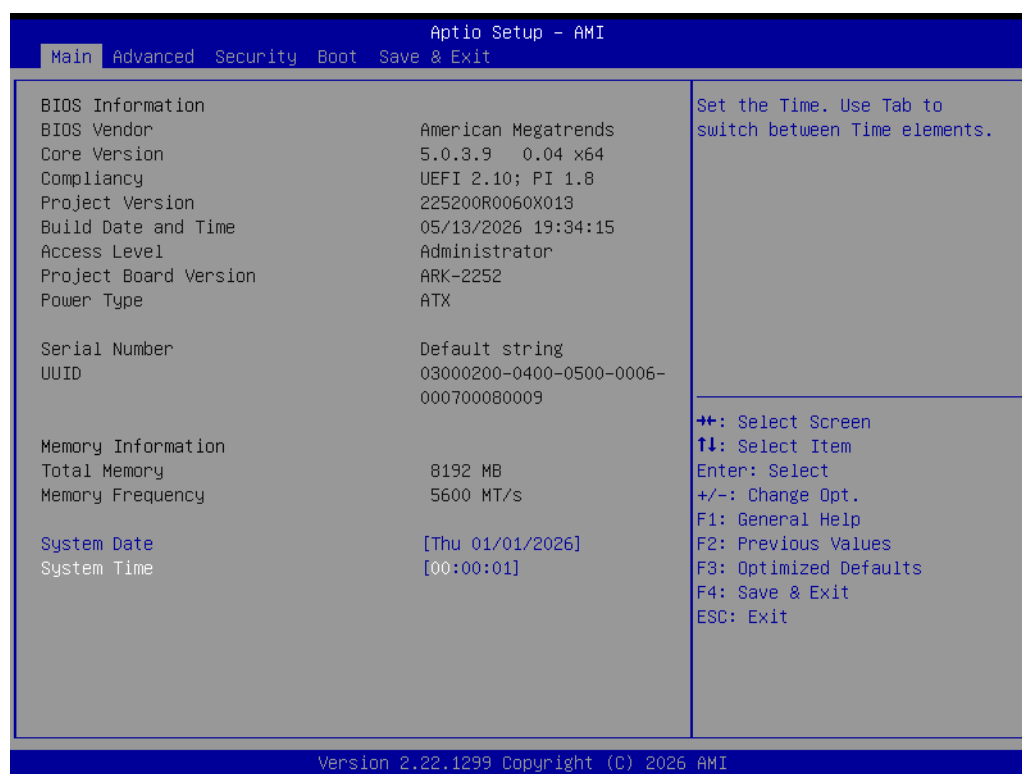
AMI BIOS ROM has a built-in setup program that allows users to modify the basic system configuration. This information is stored in battery-backed CMOS so it retains the Setup information when the power is turned off. This chapter describes the basic navigation of the ARK-2252 BIOS setup screens.

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 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.



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.

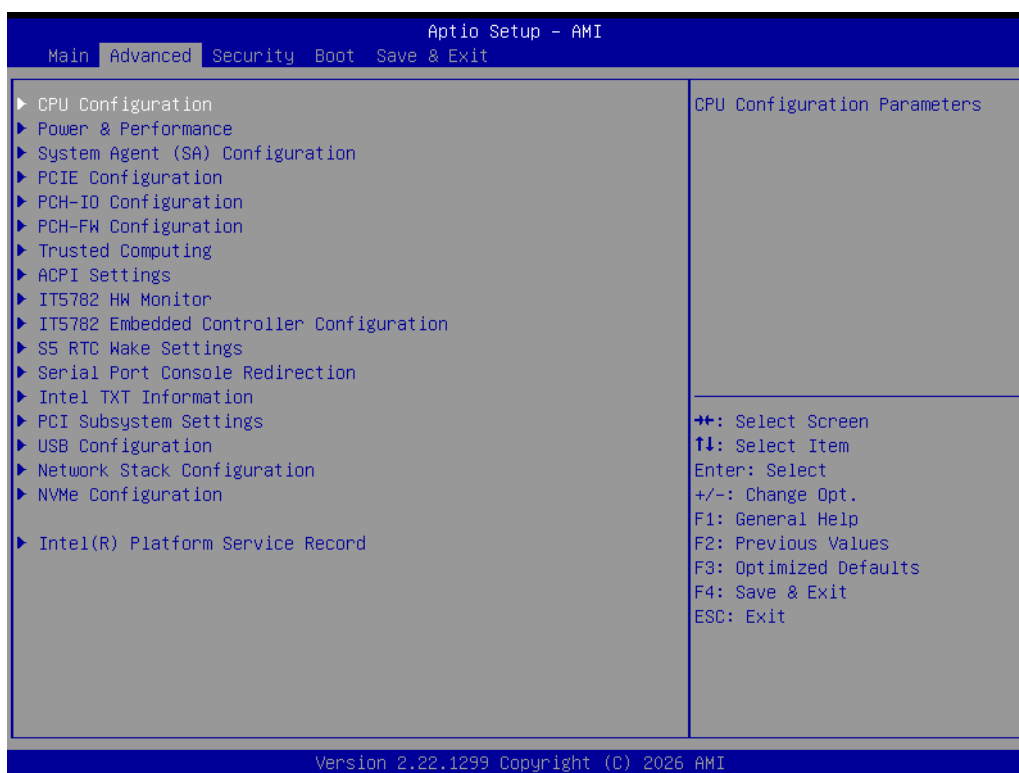
Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it.

System time / System date

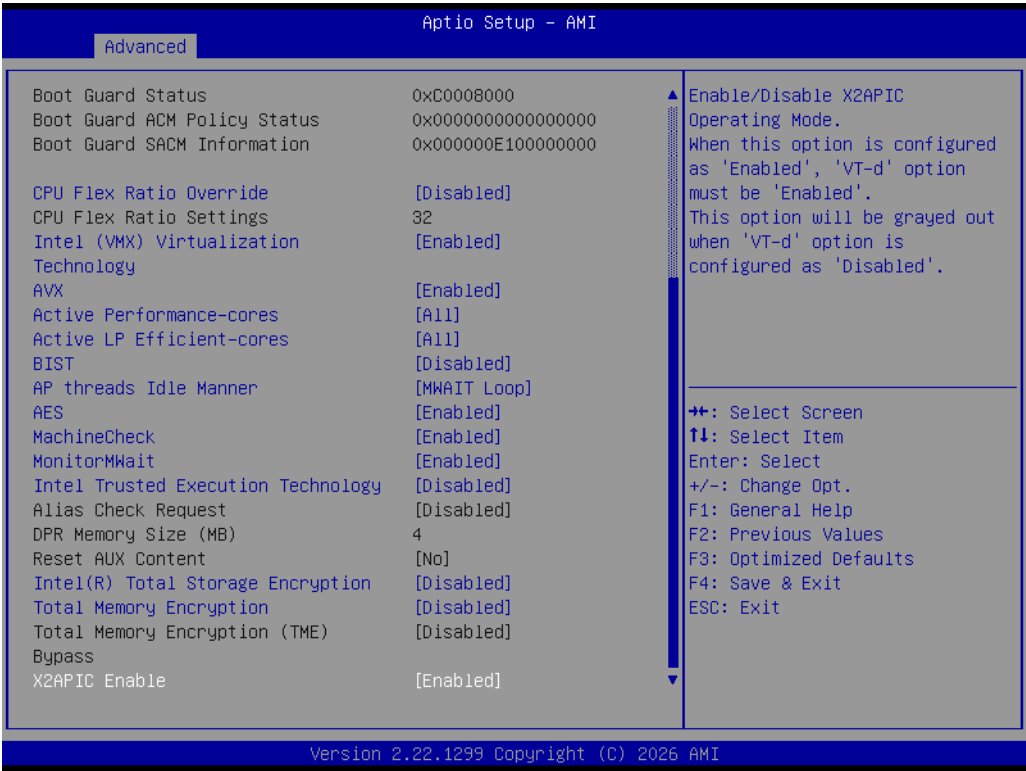
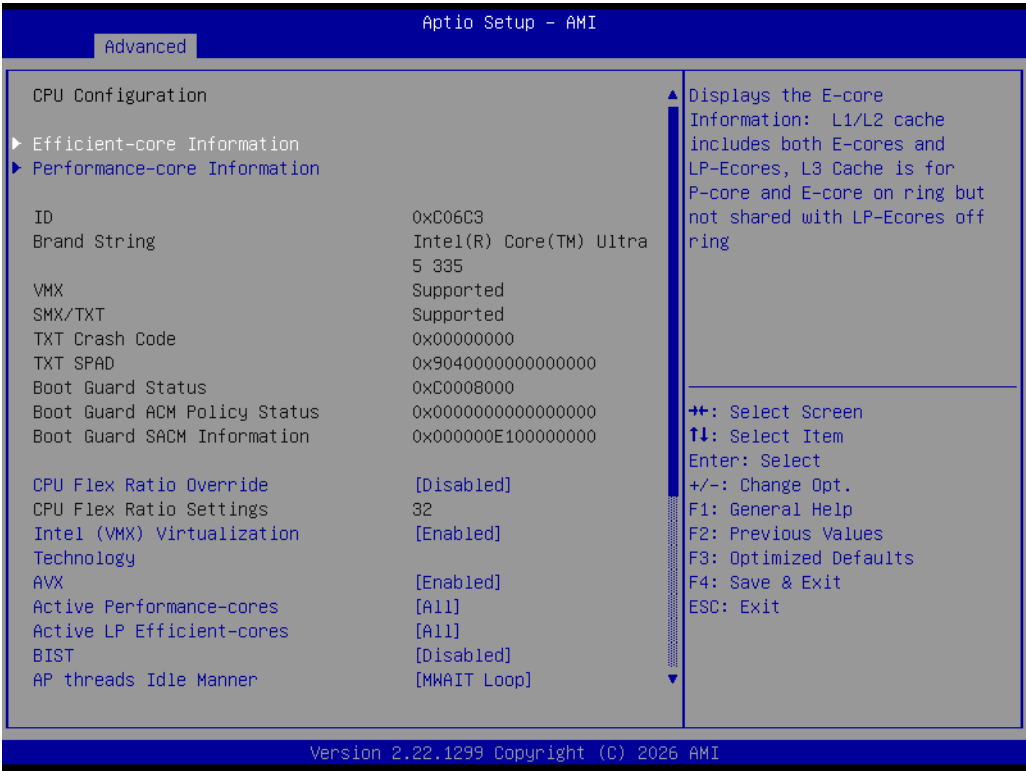
Use this option to change the system time and date. Highlight System Time or System Date using the <Arrow> keys. Enter new values through the keyboard. Press the <Tab> key or the <Arrow> keys to move between fields. The date must be entered in MM/DD/YY format. The time must be entered in HH:MM:SS format.

3.2.2 Advanced BIOS Features Setup

Select the Advanced tab from the ARK-2252 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.



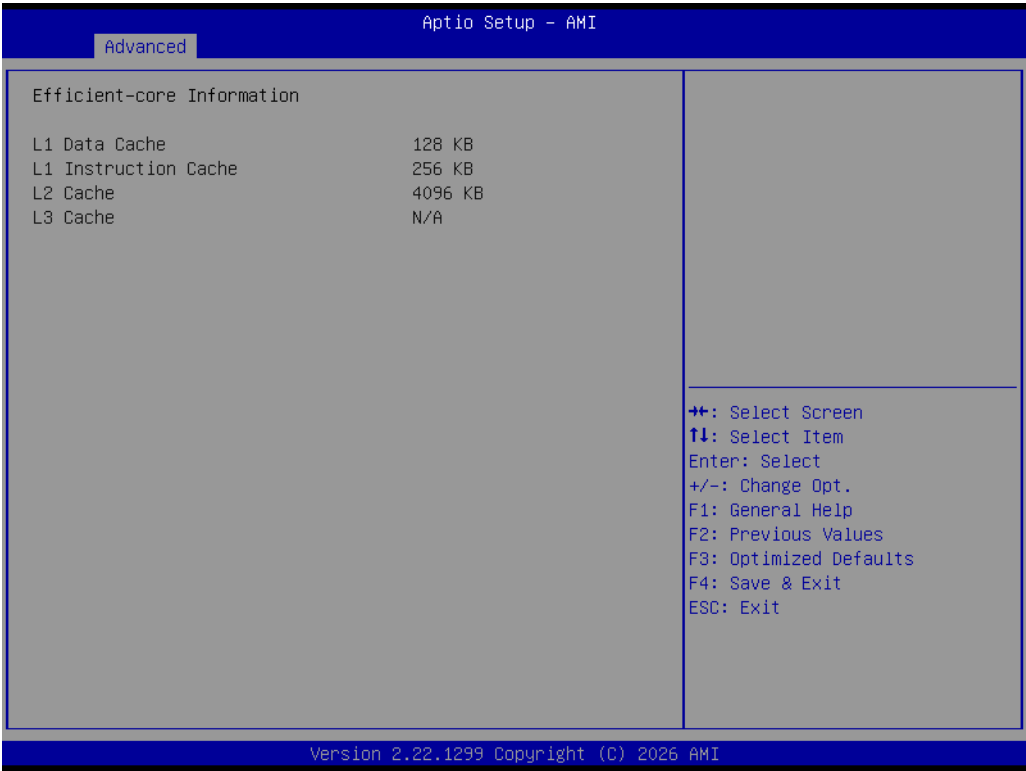
3.2.2.1 CPU Configuration



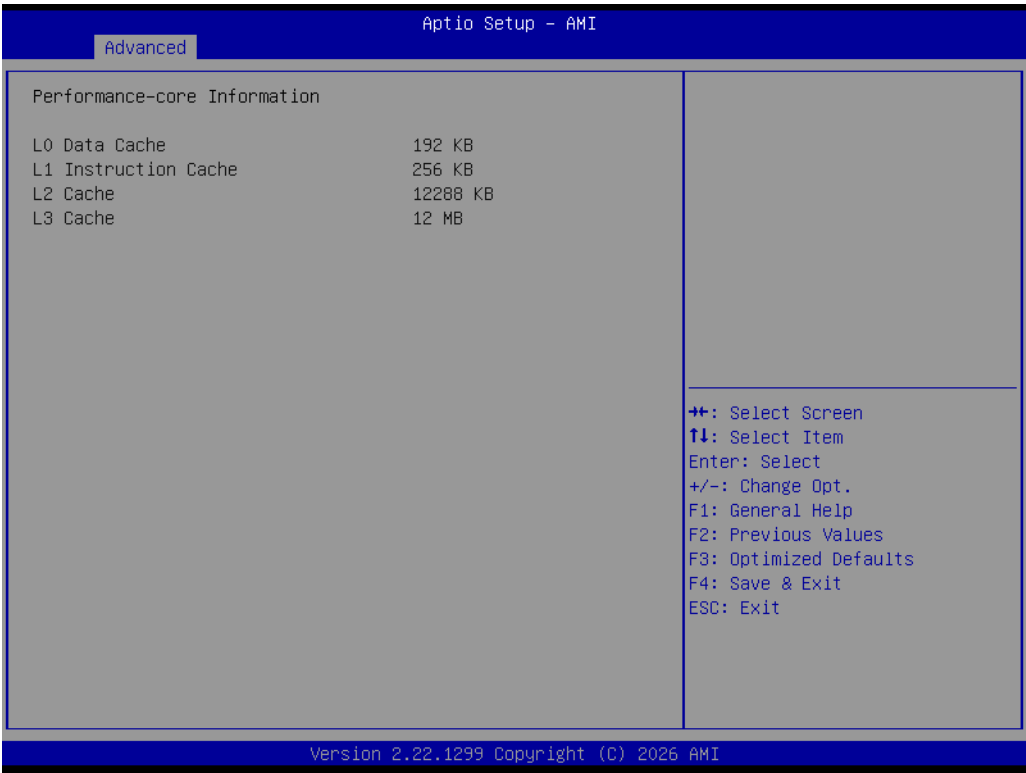
- **CPU Flex Ratio Override**
Enables/Disables CPU Flex Ratio programming.
- **CPU Flex Ratio Setting**
This value must be between the Max Efficiency Ratio (LFM) and the Maximum non-turbo ratio set by hardware (HFM).

- **Intel (VMX) Virtualization Technology**
When Enabled, a VMM can utilize the additional hardware capability provided by Vanderpool Technology.
- **AVX**
Enables/Disables the AVX 2/3 Instructions. This is applicable for performance-core only.
- **Active Performance-cores**
Number of P-cores to enable in each processor package.
- **Active Efficient-cores**
The number of P-Cores an E-Cores are looked at together. When both are {0,0}, Pcode will enable all cores.
- **Active LP Efficient-cores**
Number of LP E-cores off ring. Note: Number of P-cores, E-cores and LP E-cores are looked at together. When all are {0,0,0}, Pcode will enable all cores.
- **BIST**
Enables/Disables BIST (Built-in Self Test) on reset.
- **AP threads Idle Manner**
Specifies how AP threads behave while waiting for a signal to run.
- **AES**
Enables/Disables AES (Advanced Encryption Standard).
- **MachineCheck**
Enables/Disables Machine Check.
- **MonitorMWait**
Enables/Disables MonitorMWait. If Disabled, the AP threads Idle Manner should not be set to MWAIT Loop.
- **Intel Trusted Execution Technology**
Intel® Trusted Execution Technology Enables utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology. Changes require a full power cycle to take effect.
- **Intel® Total Storage Encryption**
Configure Intel(R) Total Storage Encryption.
- **Total Memory Encryption**
Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks. When this option is configured as 'Enabled', the 'VT-d' option must be 'Enabled'. This option will be grayed out when the 'VT-d' option is configured as 'Disabled'.
- **X2APIC Enable**
Enables/Disables X2APIC Operating Mode. When this option is configured as 'Enabled', the 'VT-d' option must be 'Enabled' and the 'X2APIC Opt Out' option must be 'Disabled' as well. This option will be grayed out when the 'VT-d' option is configured as 'Disabled'.

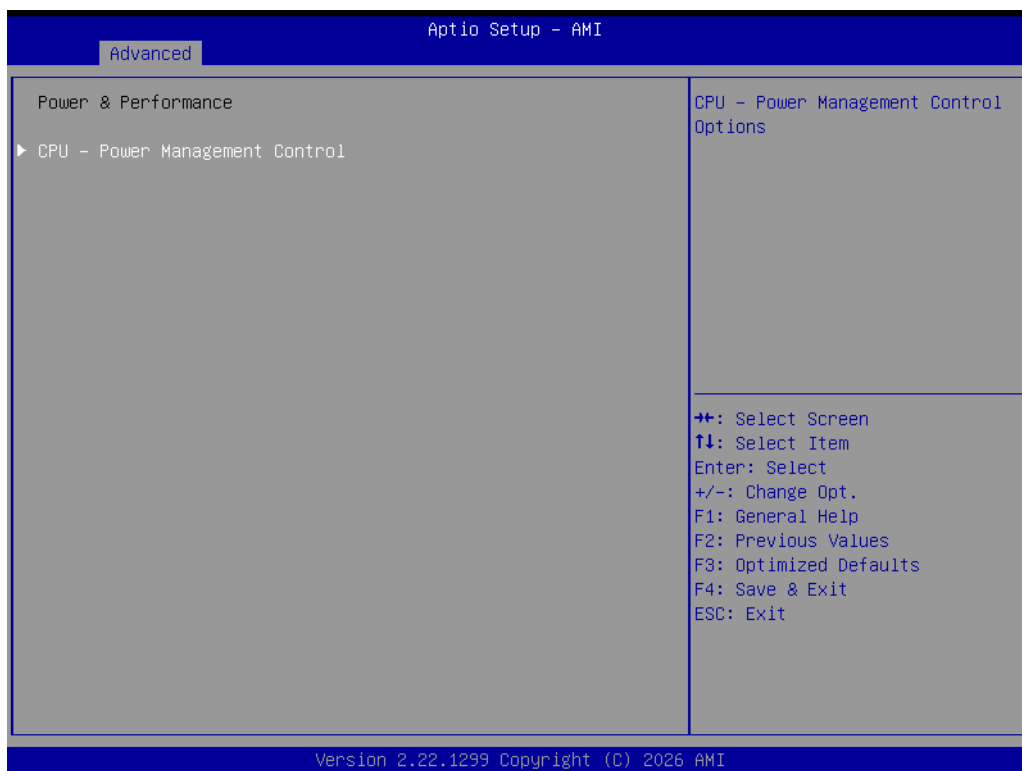
Efficient-core Information



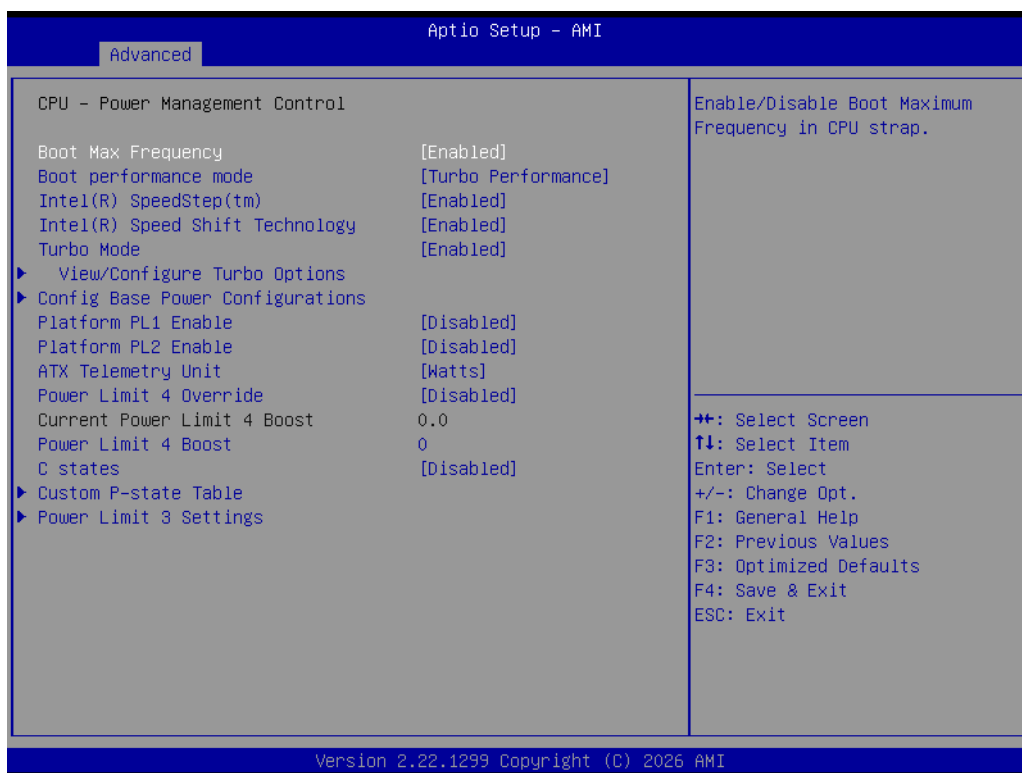
Performance-core Information



3.2.2.2 Power & Performance



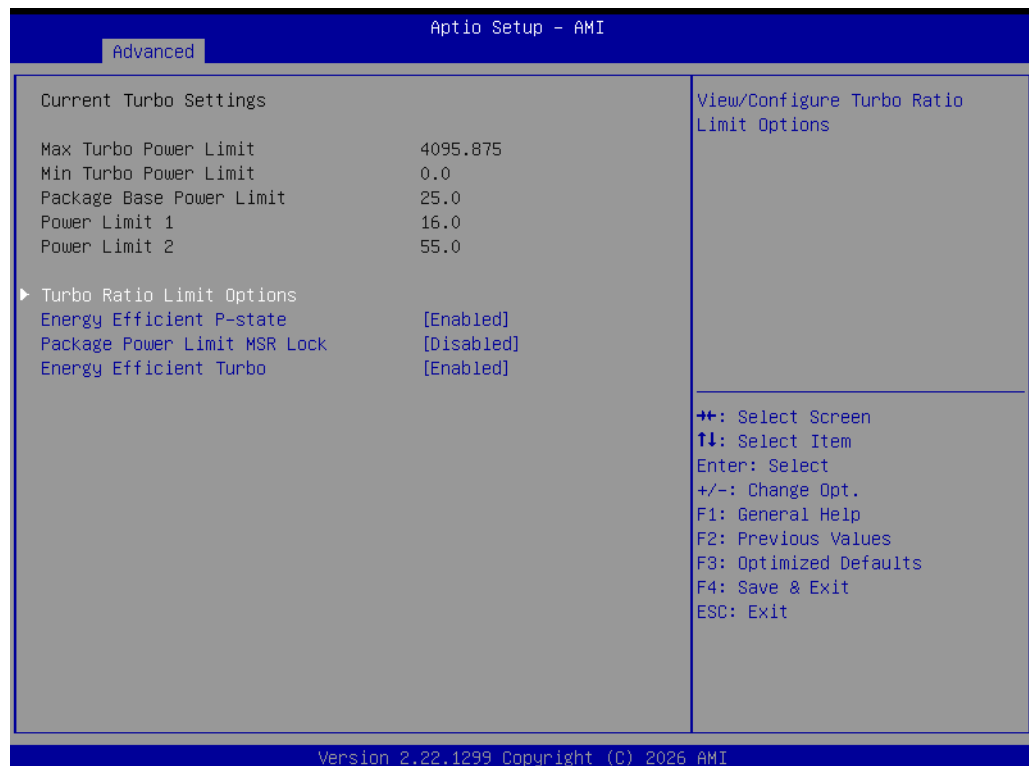
CPU - Power Management Control



- **Boot Max Frequency**
Enables/Disables Boot Maximum Frequency in CPU strap.
- **Boot performance mode**
Select the performance state that the BIOS will set before OS hand-off.

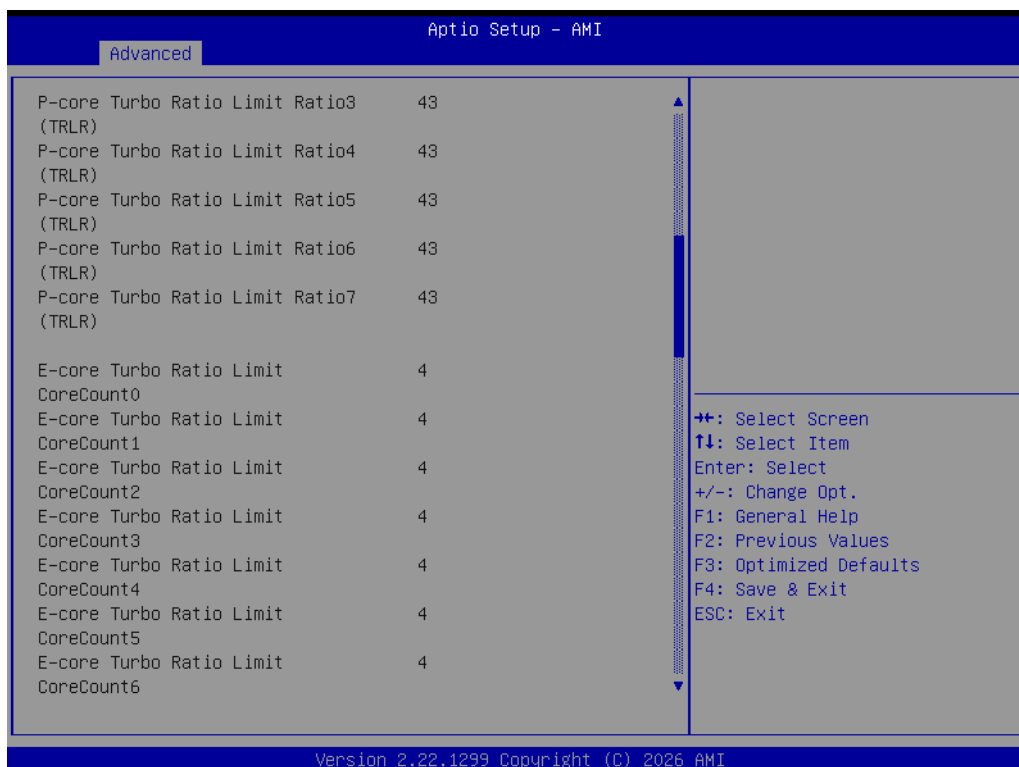
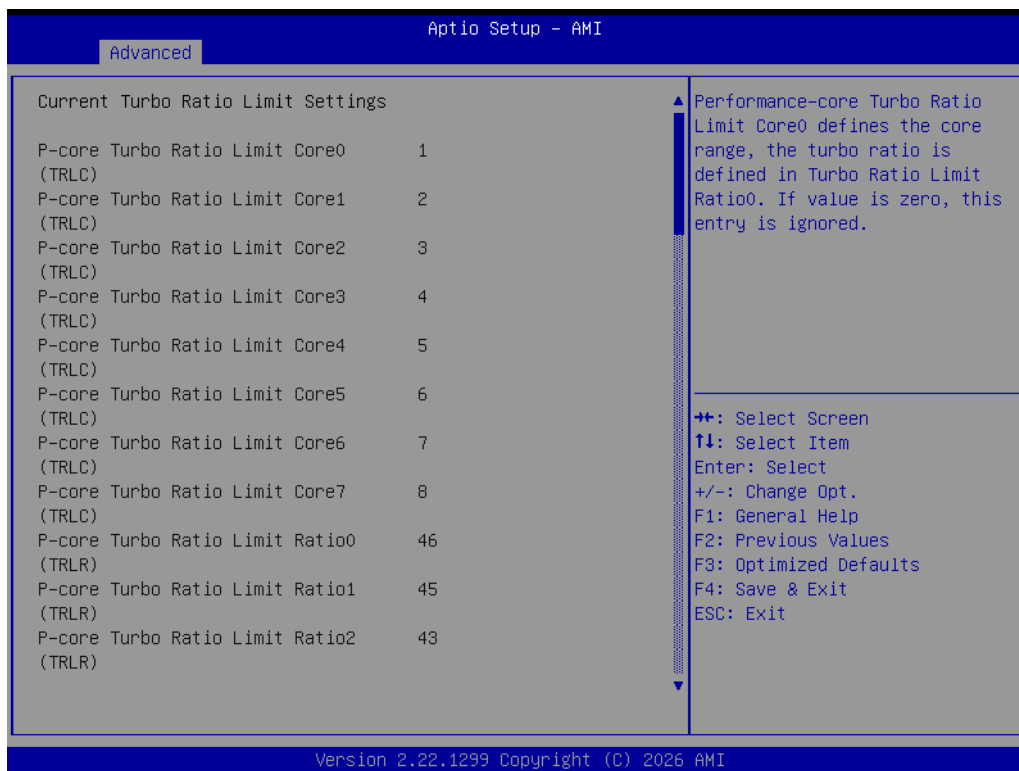
- **Intel® SpeedStep™**
Allows more than two frequency ranges to be supported.
- **Intel® Speed Shift Technology**
Enables/Disables Intel® Speed Shift Technology support.
- **Turbo Mode**
Enables/Disables Intel® Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
- **Platform PL1 Enable**
Enables/Disables Platform Power Limit 1 programming.
- **Platform PL2 Enable**
Enables/Disables Platform Power Limit 2 programming.
- **ATX Telemetry Unit**
ATX Telemetry Unit in Watts or Percentage, it indicates the telemetry type for Psys support. Psys data is in Unitless format when selecting Percentage, it is a relative % from P100%PSU rated power. Default is Watts, recommended to select Percentage when plug-in ATX12VO PSU.
- **Power Limit 4 Override**
Enables/Disables Power Limit 4 override.
- **Power Limit 4 Boost**
Configure Power Limit 4 Boost in watts. The value 0 means disabled.
- **C states**
Enables/Disables CPU Power Management.

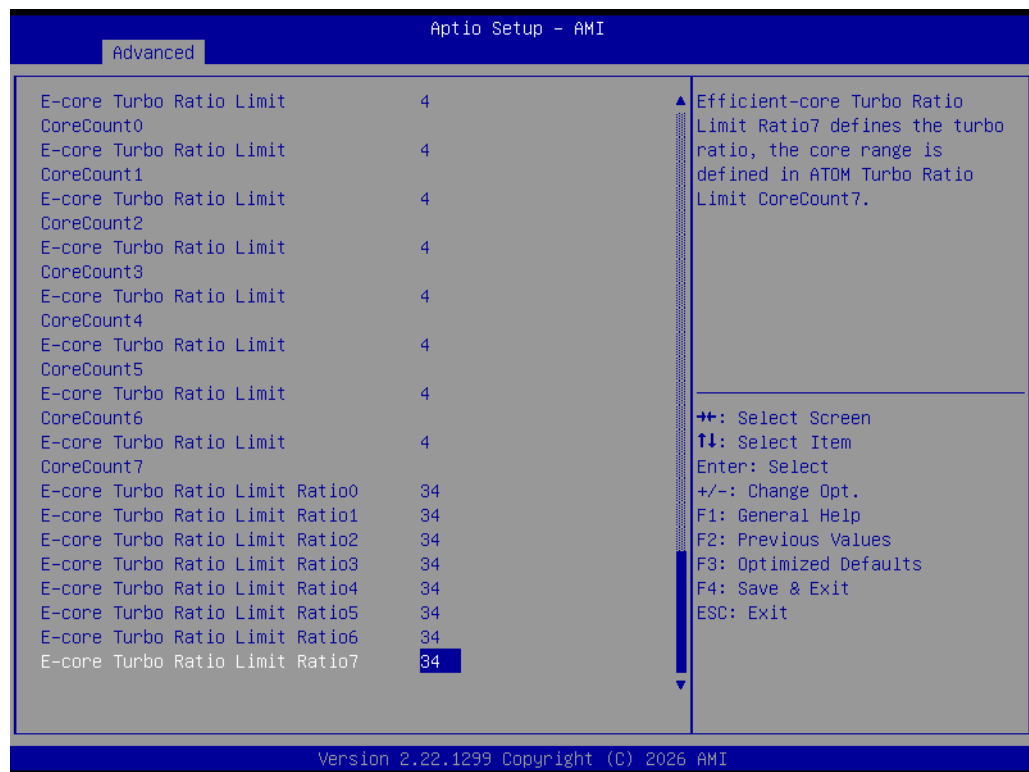
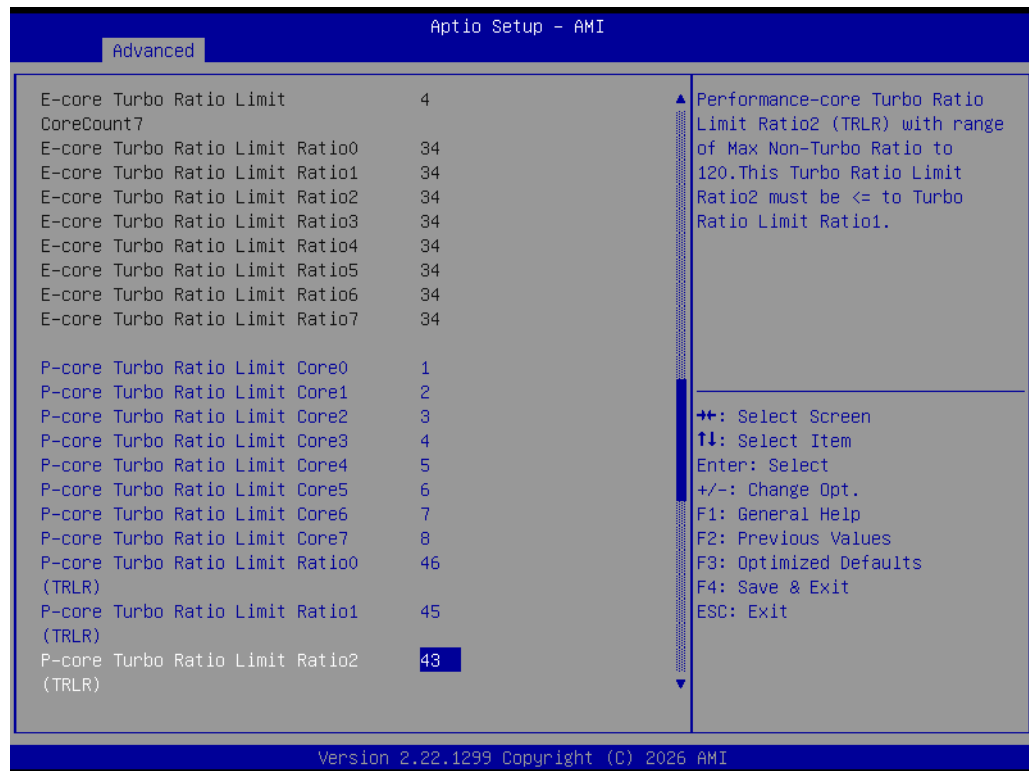
View/Configure Turbo Options



- **Turbo Ratio Limit Options**
View/Configure Turbo Ratio Limit Options.
- **Energy Efficient P-state**
Enables/Disables Energy Efficient P-state feature.

- **Package Power Limit MSR Lock**
Enables/Disables locking of Package Power Limit settings.
- **Energy Efficient Turbo**
Enables/Disables the energy efficient turbo feature. This feature will opportunistically lower the turbo frequency to increase efficiency.
- **Turbo Ratio Limit Options**

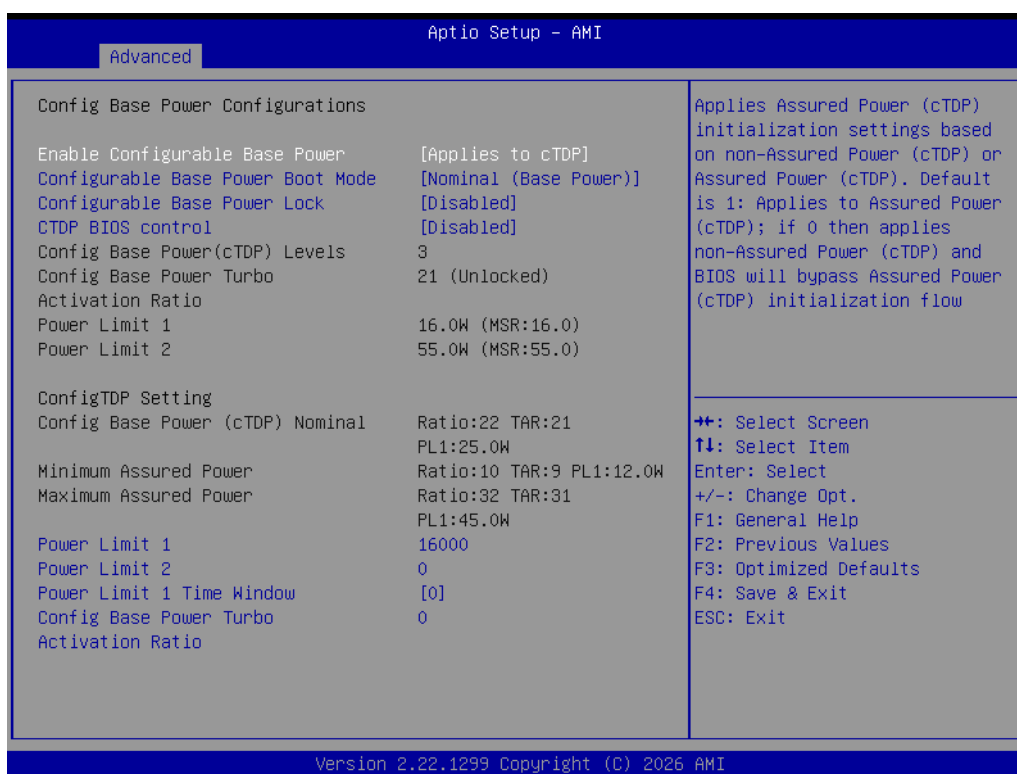




- P-Core Turbo Ratio Limit Core
Performance-core Turbo Ratio Limit Core(x) defines the core range, the turbo ratio is defined in Turbo Ratio Limit Ratio(x). If the value is zero, this entry is ignored.
- P-Core Turbo Ratio Limit Ratio (TRLR)
Performance-core Turbo Ratio Limit Ratio(x) (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode).

- E-Core Turbo Ratio Limit CoreCount
Efficient-core Turbo Ratio Limit CoreCount(x) defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio(x). If the value is zero, this entry is ignored.
- E-Core Turbo Ratio Limit Ratio
Efficient-core Turbo Ratio Limit Ratio(x) defines the turbo ratio (max is 85 irrespective of the core extension mode), the core range is defined in E-core Turbo Ratio Limit CoreCount(x).

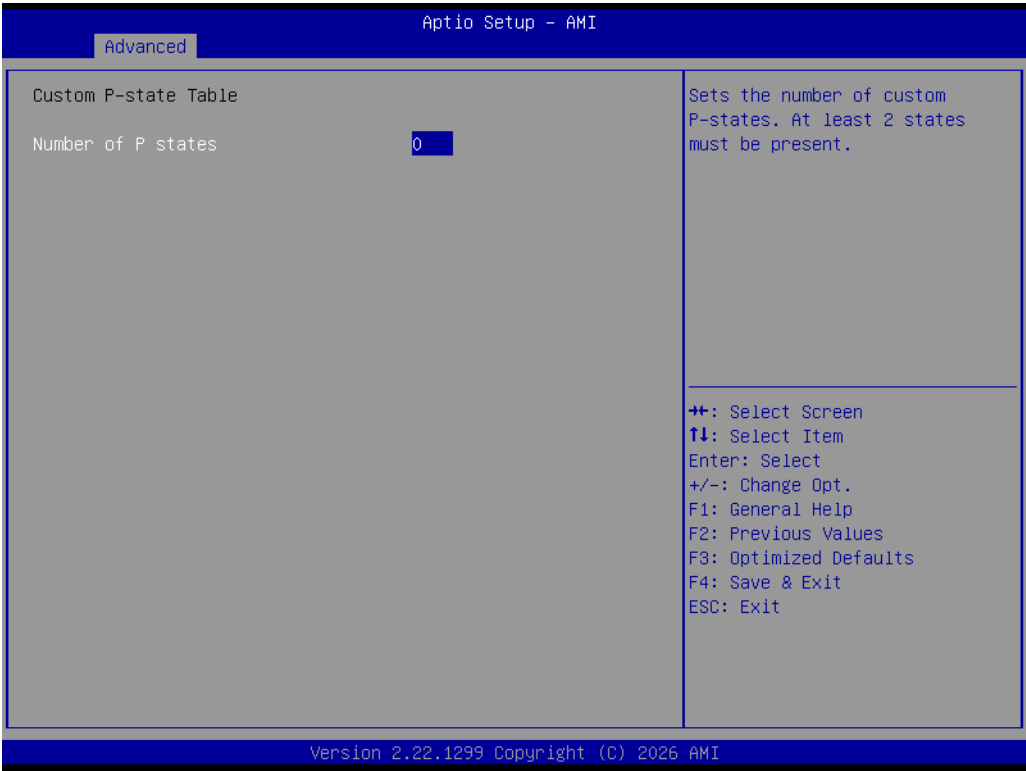
Config Base Power Configuration



- **Enable Configuration Base Power**
Applies Assured Power (cTDP) initialization settings based on non-Assured Power (cTDP) or Assured Power (cTDP). Default is 1: Applies to Assured Power (cTDP); if 0 then applies non-Assured Power (cTDP) and BIOS will bypass Assured Power (cTDP) initialization flow.
- **Configuration Base Power Boot mode**
Assured Power (cTDP) Mode as Nominal/Maximum/Minimum Base Power (TDP) selection.
- **Configuration Base Power Lock**
Assured Power (cTDP) Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and BASE_POWER_CONTROL.
Note: When CTD (Assured Power) Lock is enabled Custom Config Base Power (cTDP) Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.
- **CTDP BIOS Control**
Enables CTD control via runtime ACPI BIOS method.
- **Power Limit 1**
Power Limit 1 in milliwatts.
- **Power Limit 2**
Power Limit 2 in milliwatts.

- **Power Limit 1 Time Window**
Power Limit 1 Time Window value in seconds.
- **Config Base Power Turbo Activation Ratio**
Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.

Custom P-state Table



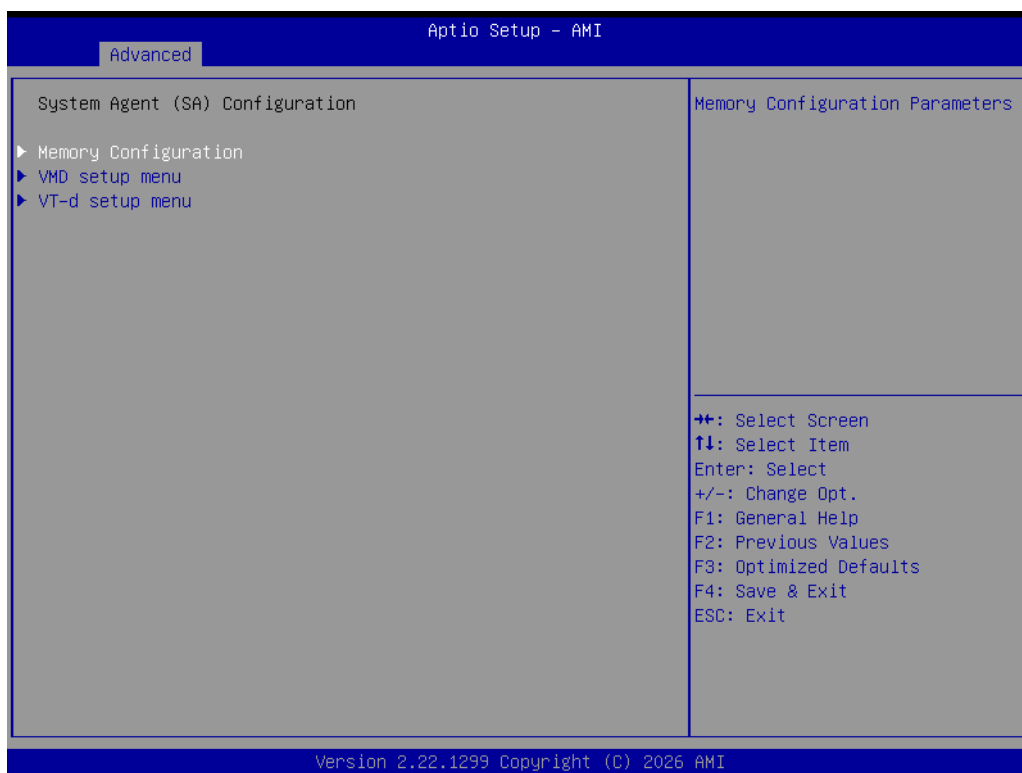
- **Number of P States**
Sets the number of custom P-states. At least 2 states must be present.

Custom P-state Table

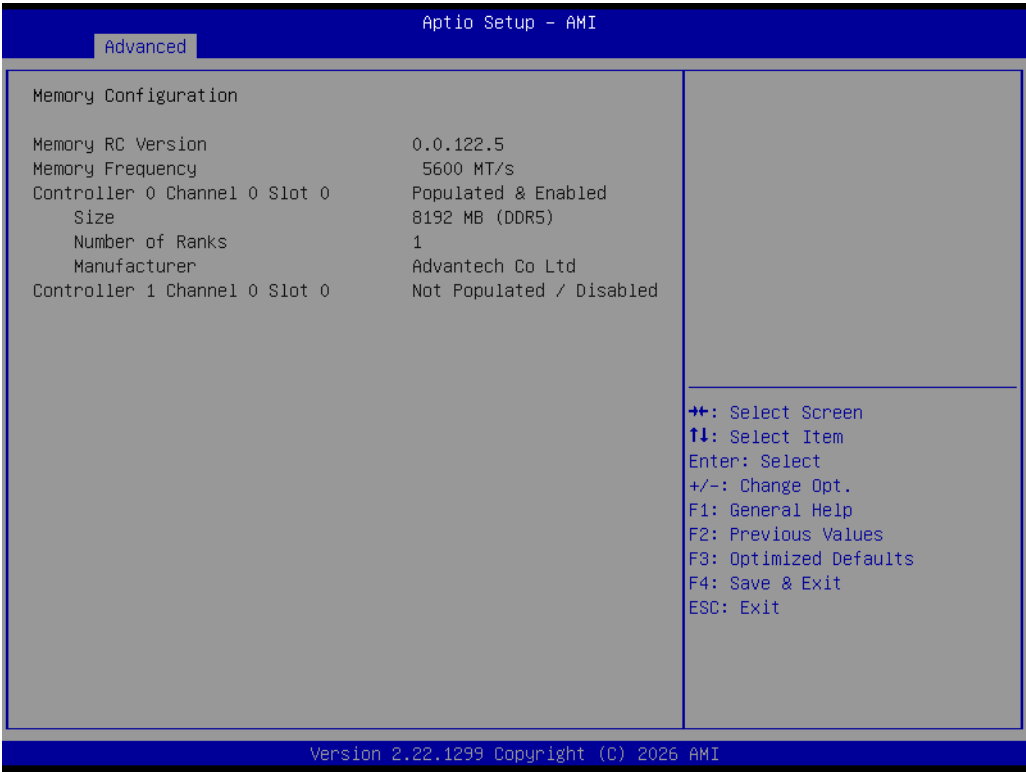


- **Power Limit 3 Override**
Enables/Disables Power Limit 3 override.

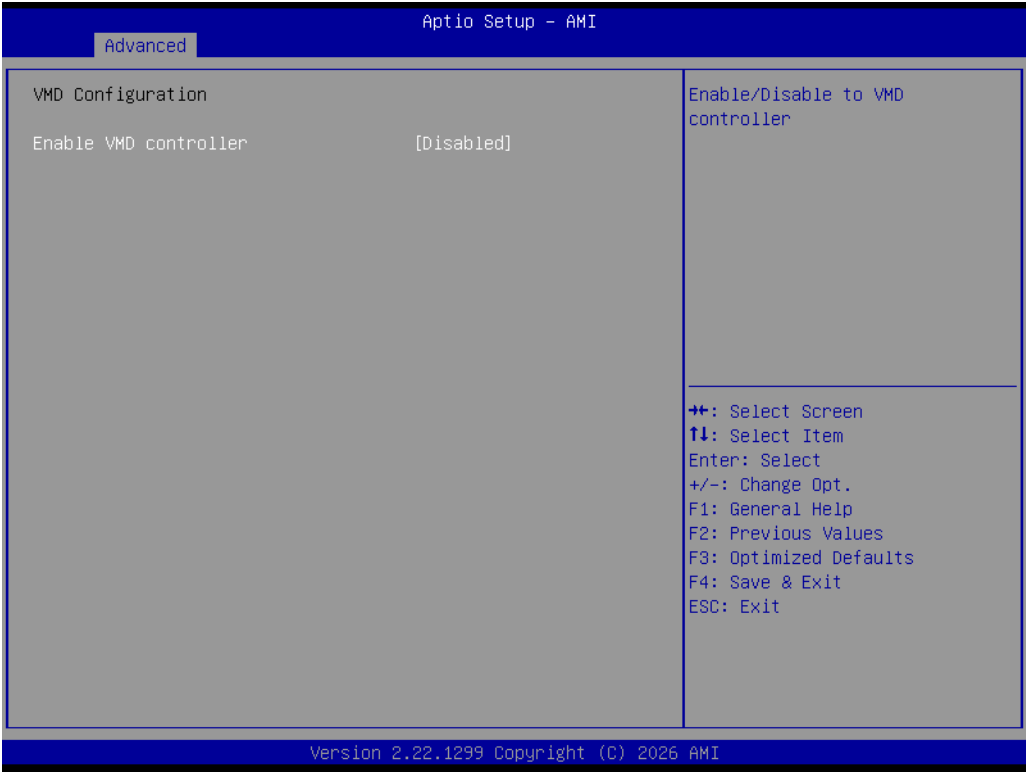
3.2.2.3 System Agent (SA) Configuration



Memory Configuration

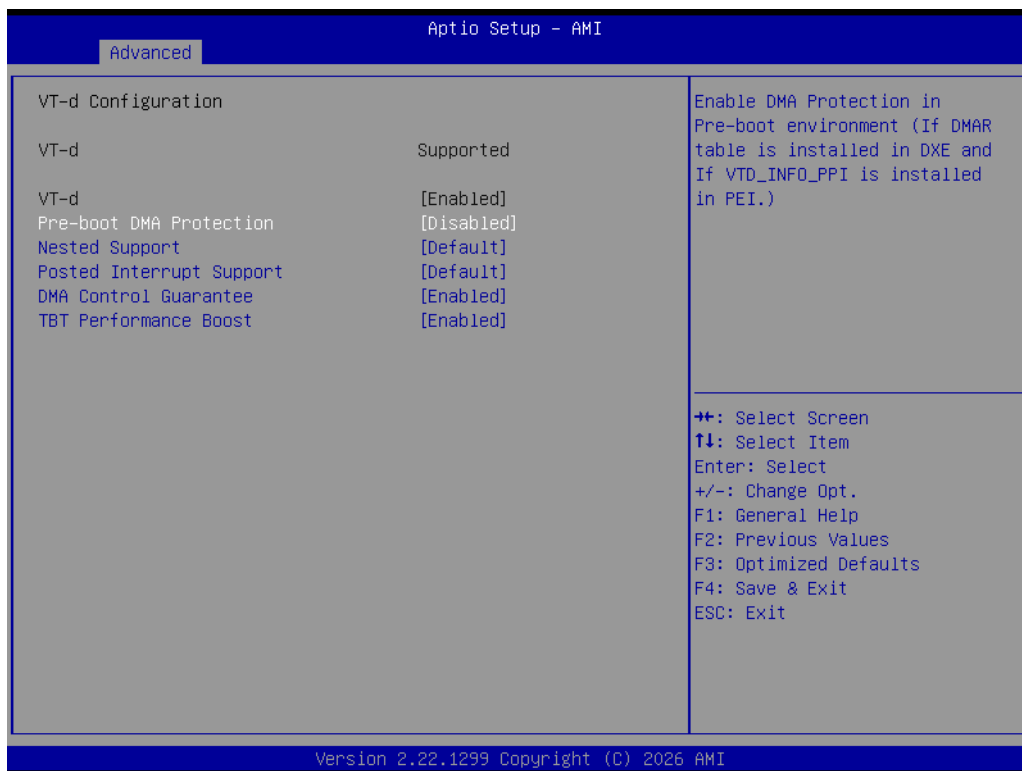


VMD Configuration



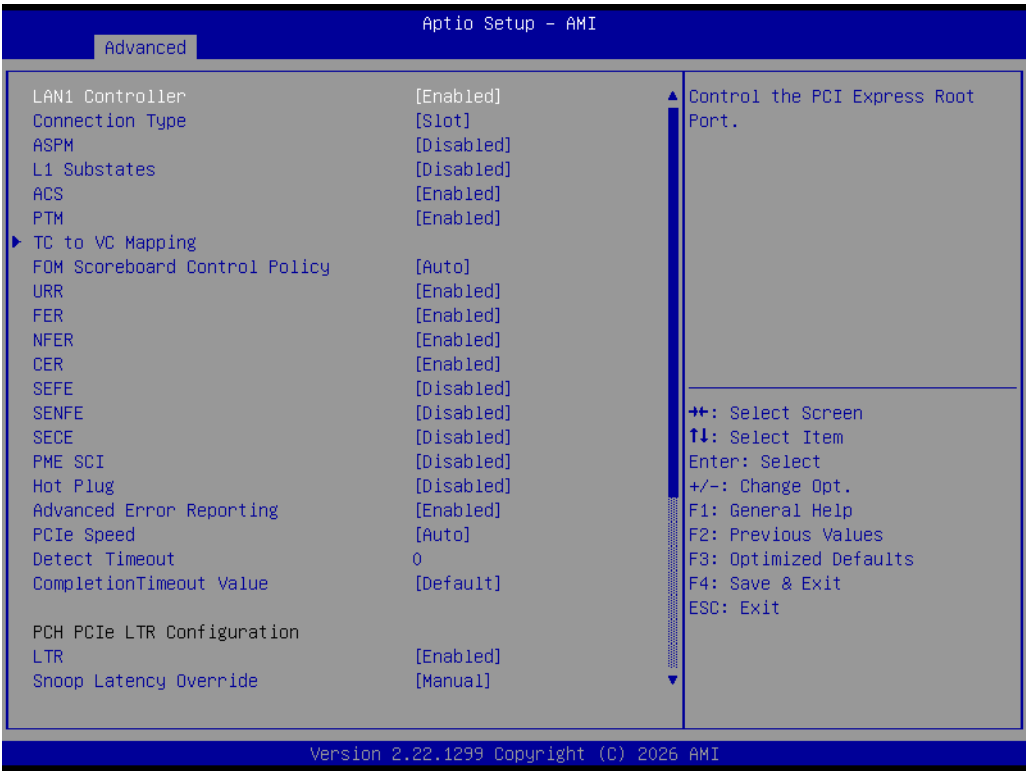
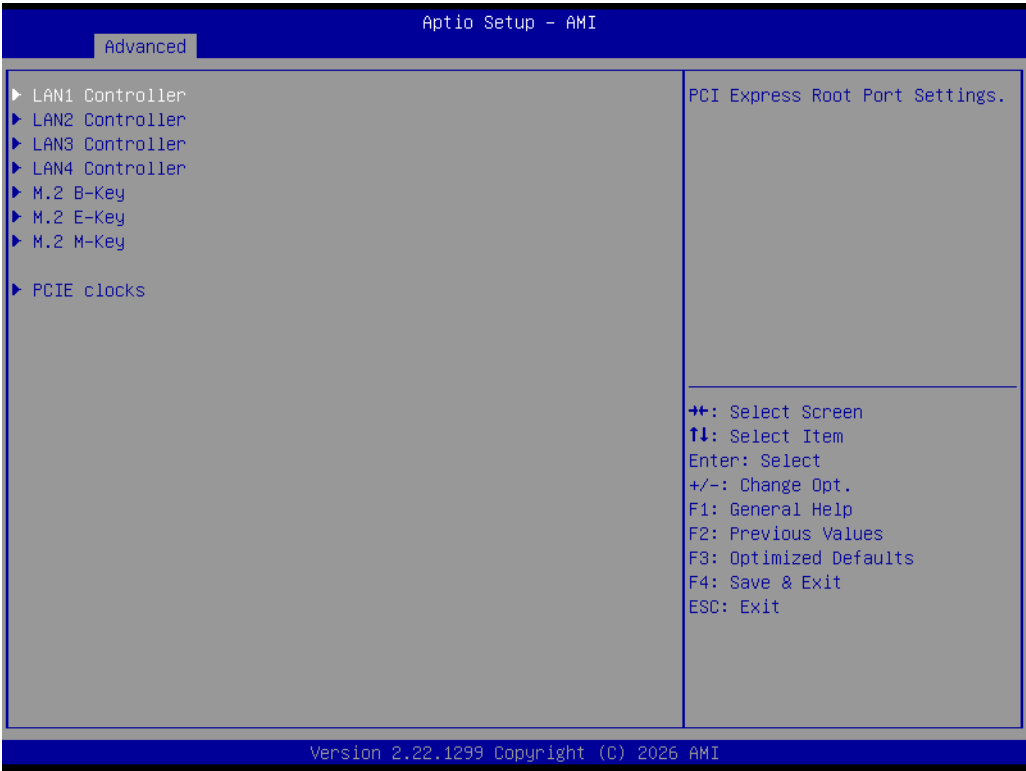
- **Enable VMD Controller**
Enables/Disables VMD controller.

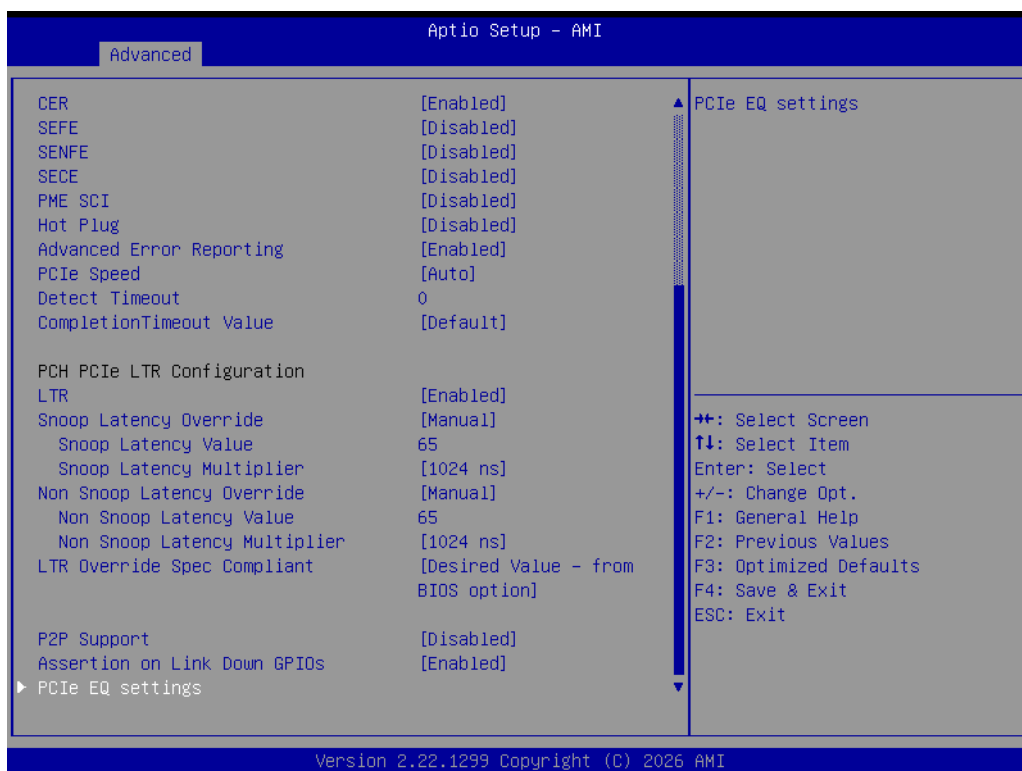
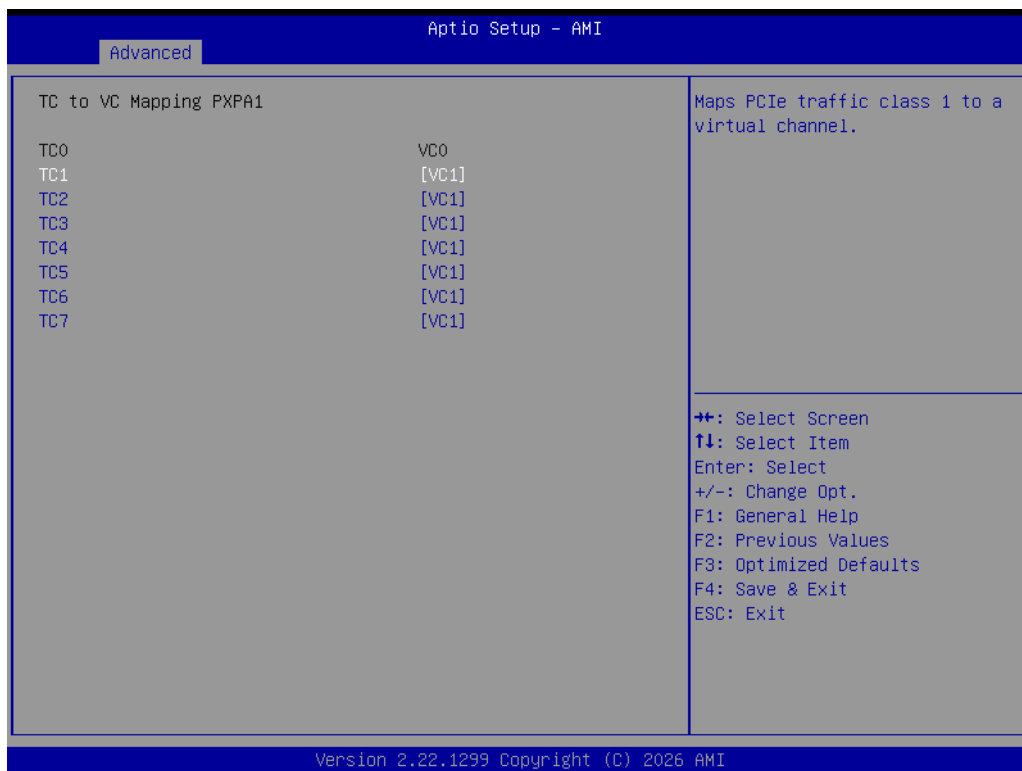
VT-d Setup Menu

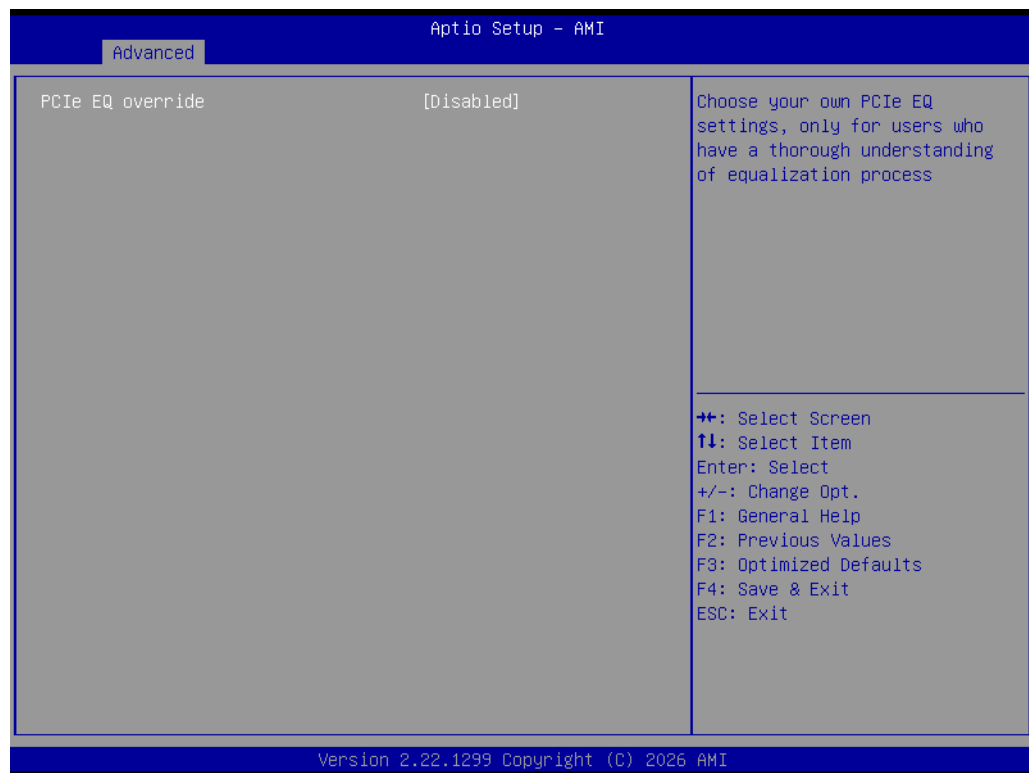


- **VT-d**
Check to enable the VT-d function on MCH. This option will be grayed out when the 'X2APIC Enable' option is configured as 'Enabled'.
- **Pre-Boot DMA Protection**
Enables DMA Protection in the Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.).
- **Nested Support** |
Enables/Disables nested support capability.
- **Posted Interrupt Support**
Enables/Disables the posted interrupt support capability.
- **DMA Control Guarantee**
Enables/Disables DMA control guarantee: DMA_CONTROL_GUARANTEE bit.
- **TBT Performance Boost**
Enables/Disables TBT performance boost through PCode mailbox.

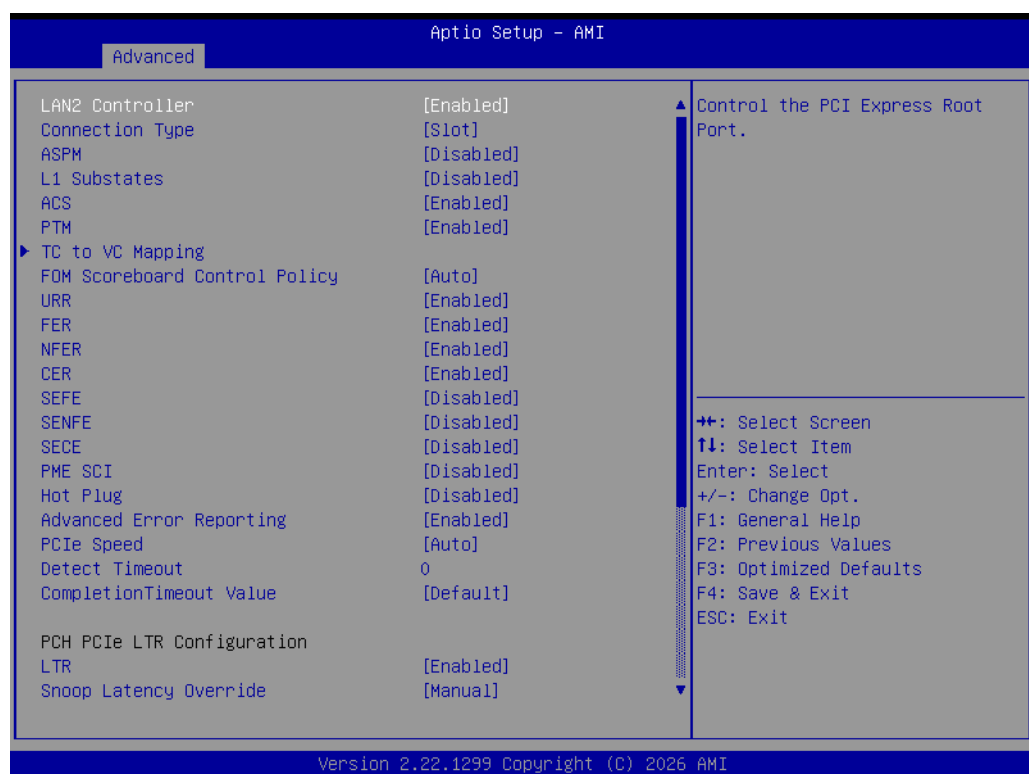
3.2.2.4 PCIE Configuration
VT-d Setup Menu

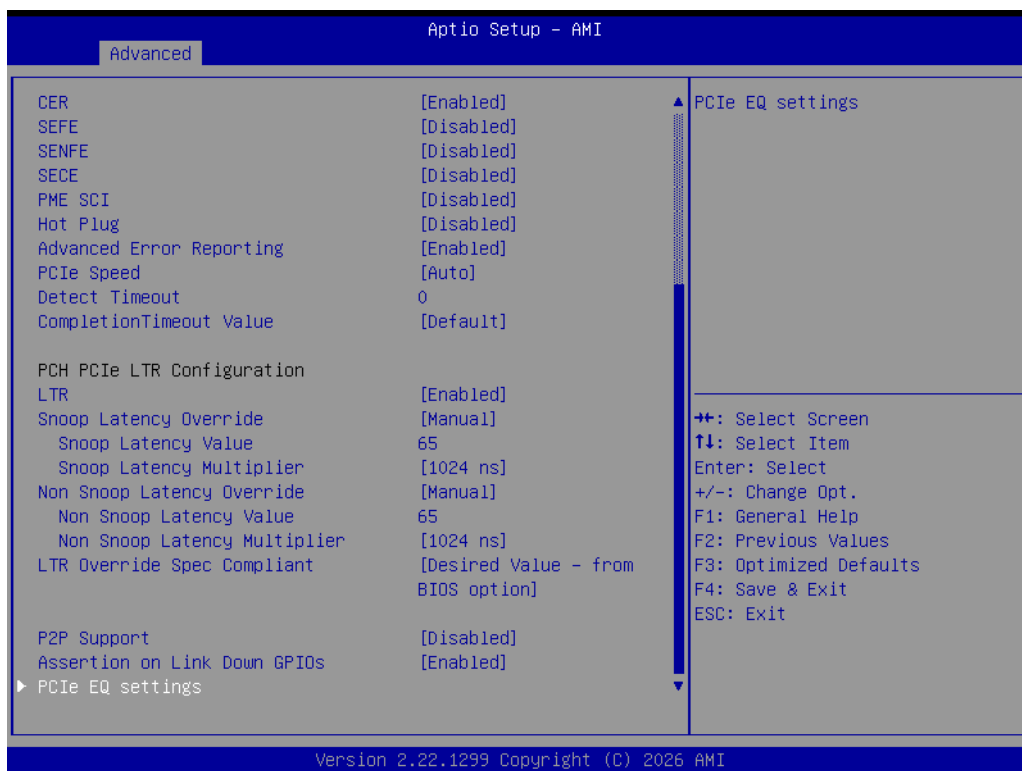
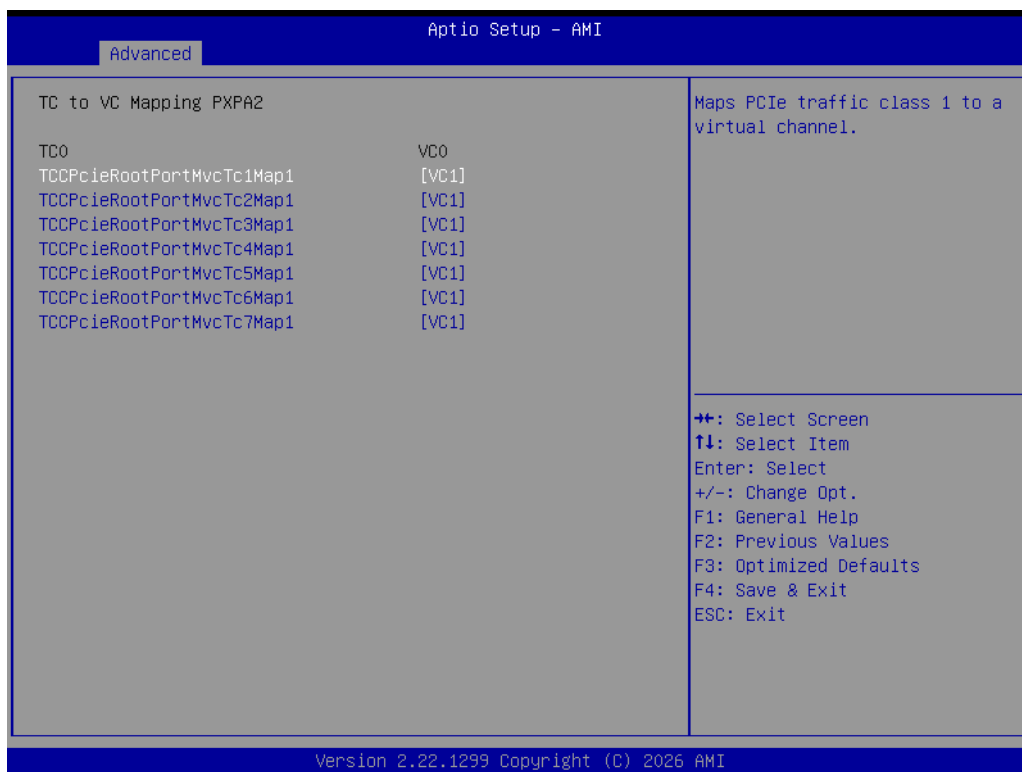






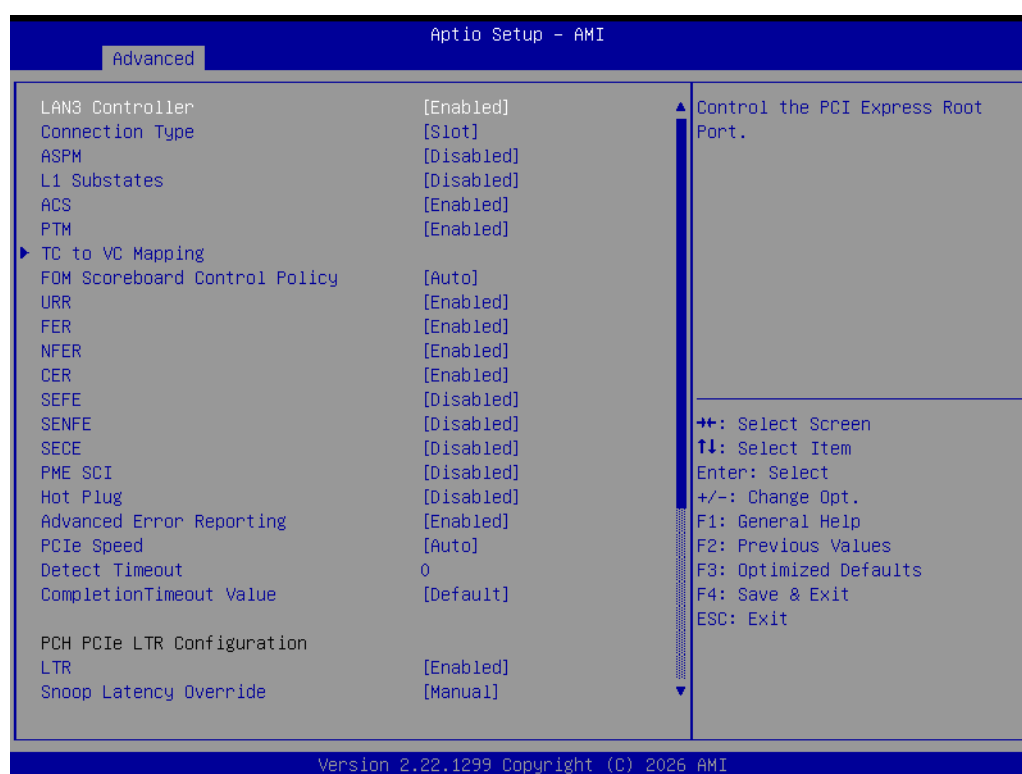
LAN2 Controller

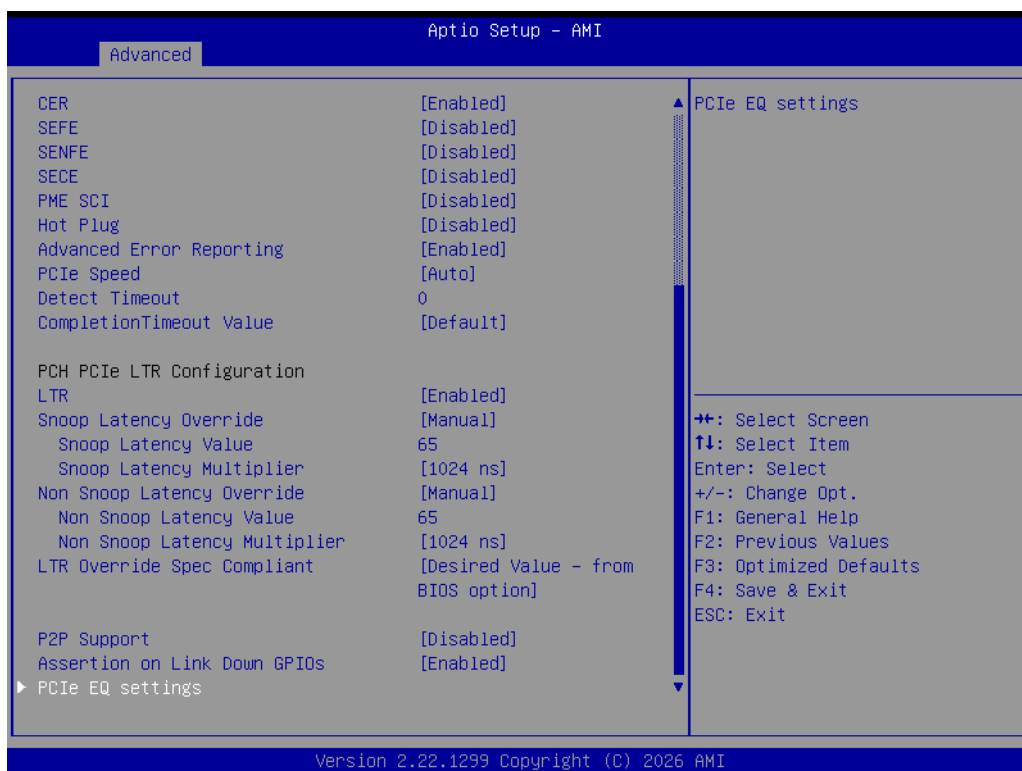
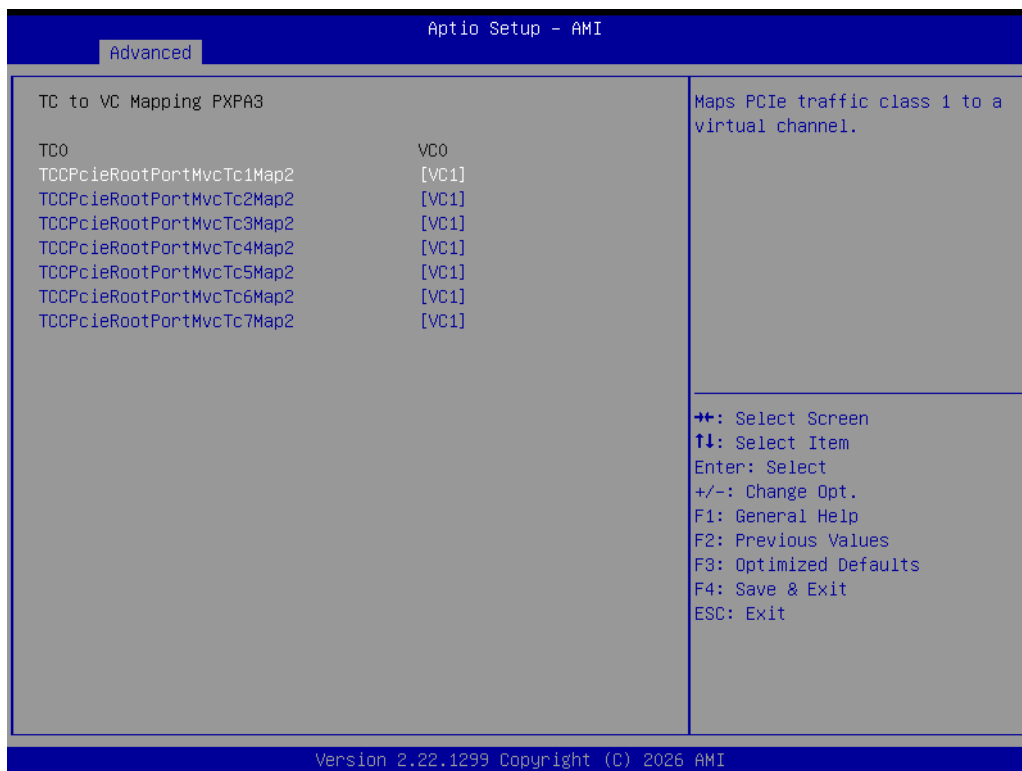


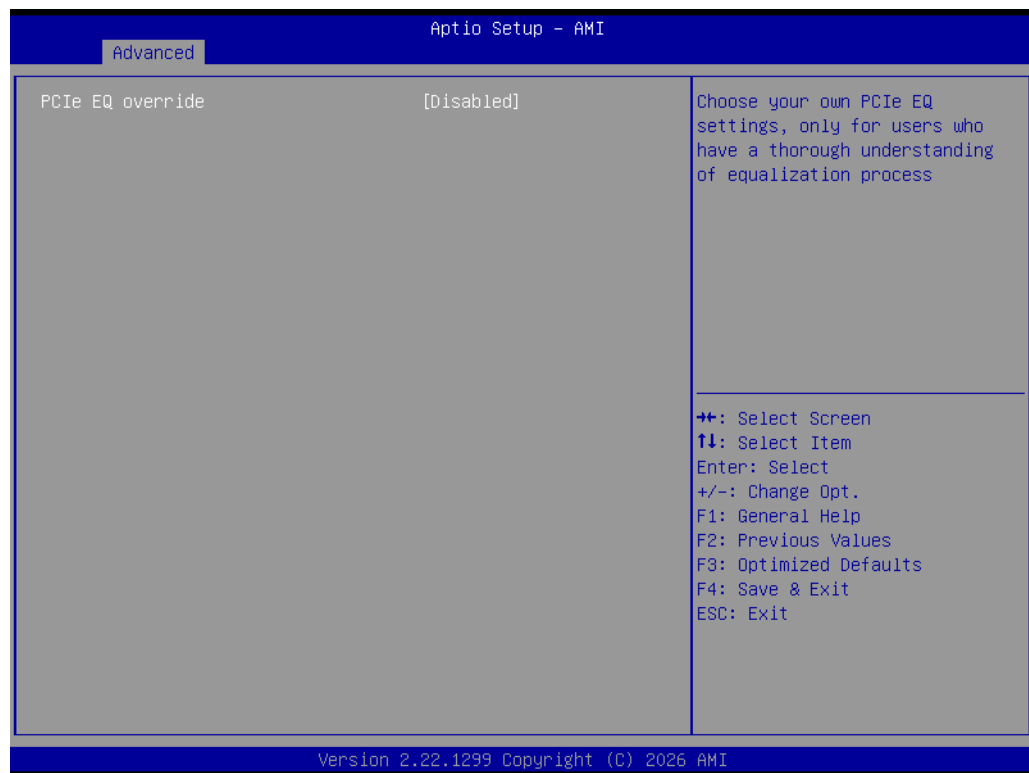




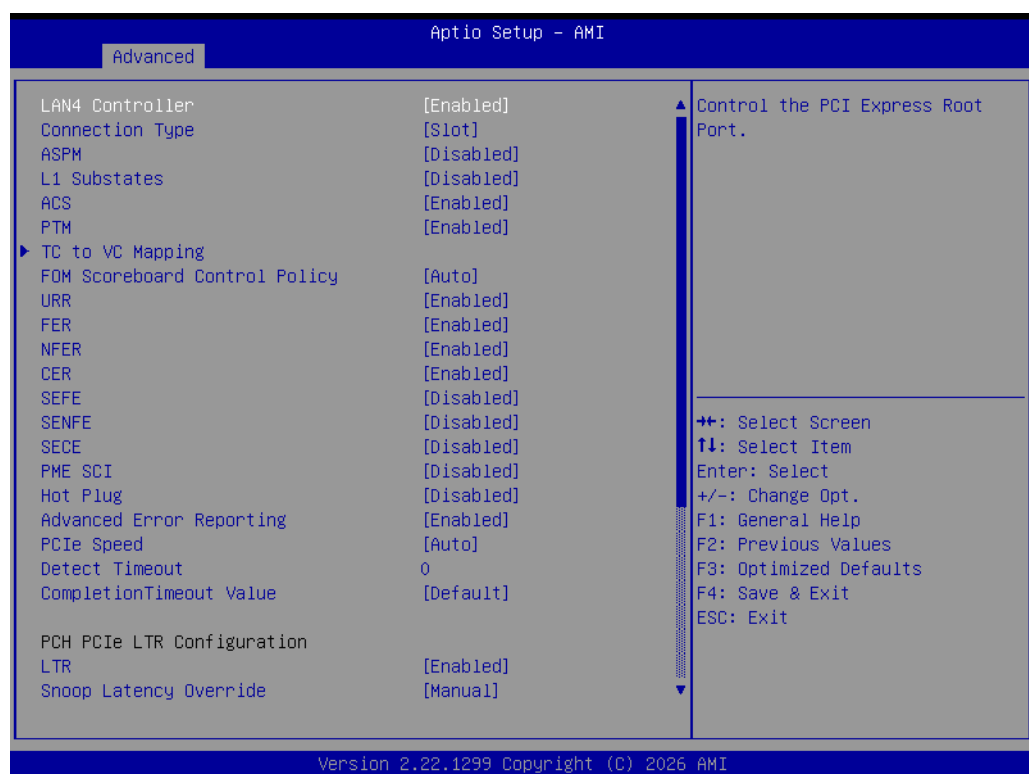
LAN2 Controller

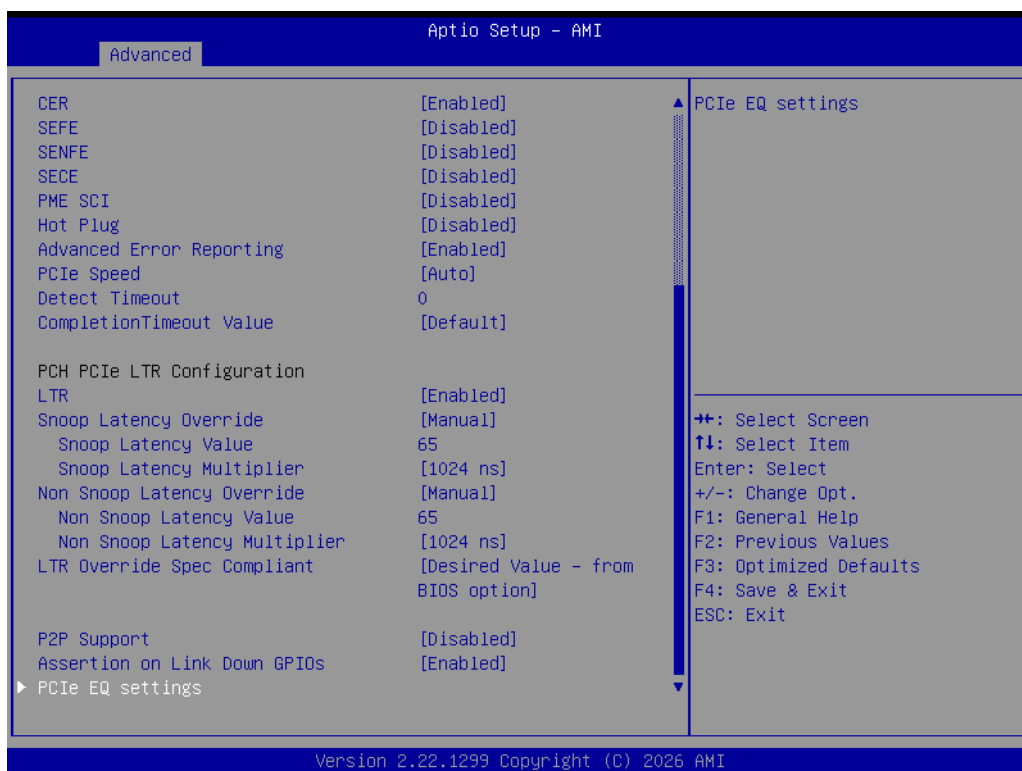
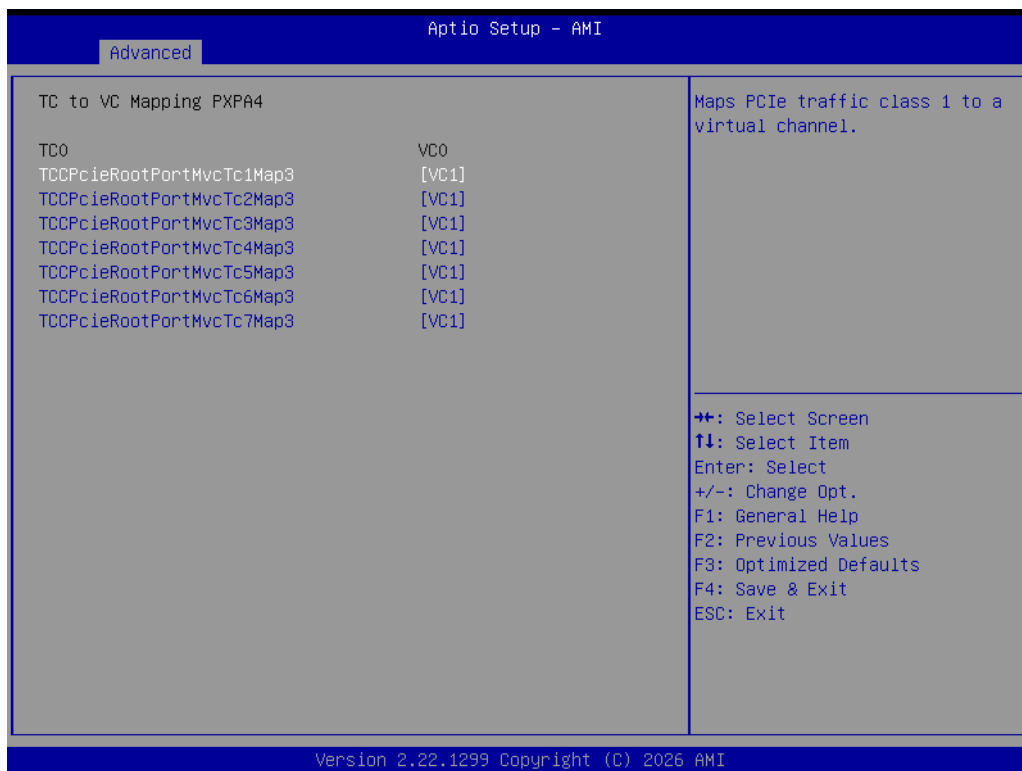


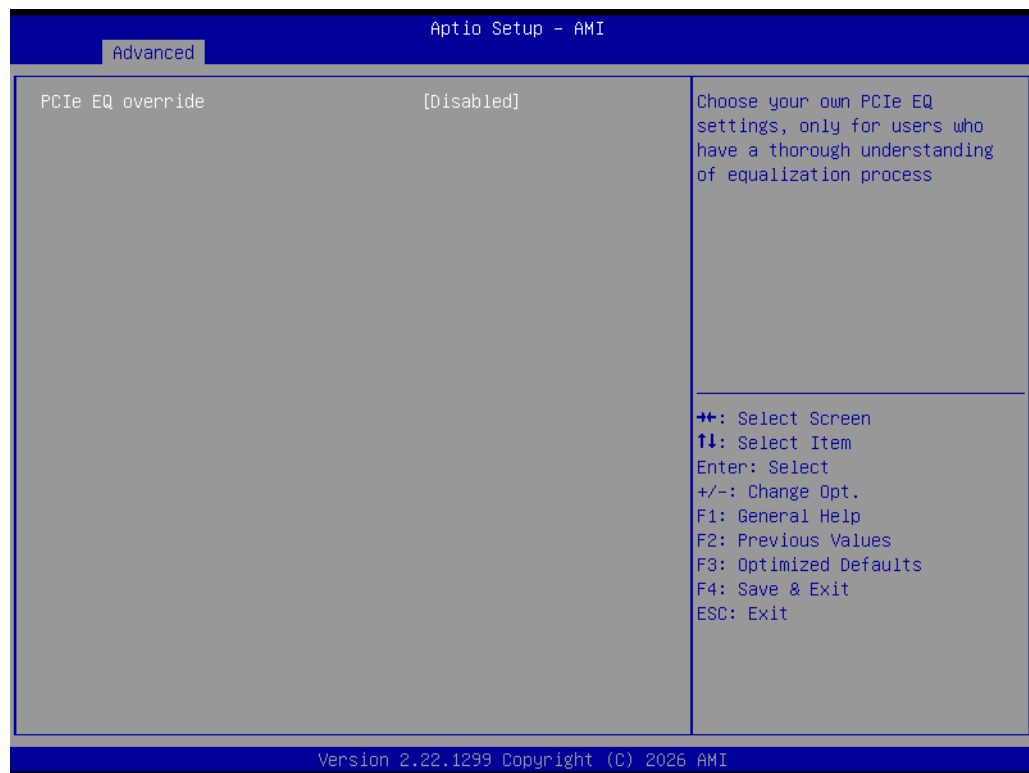




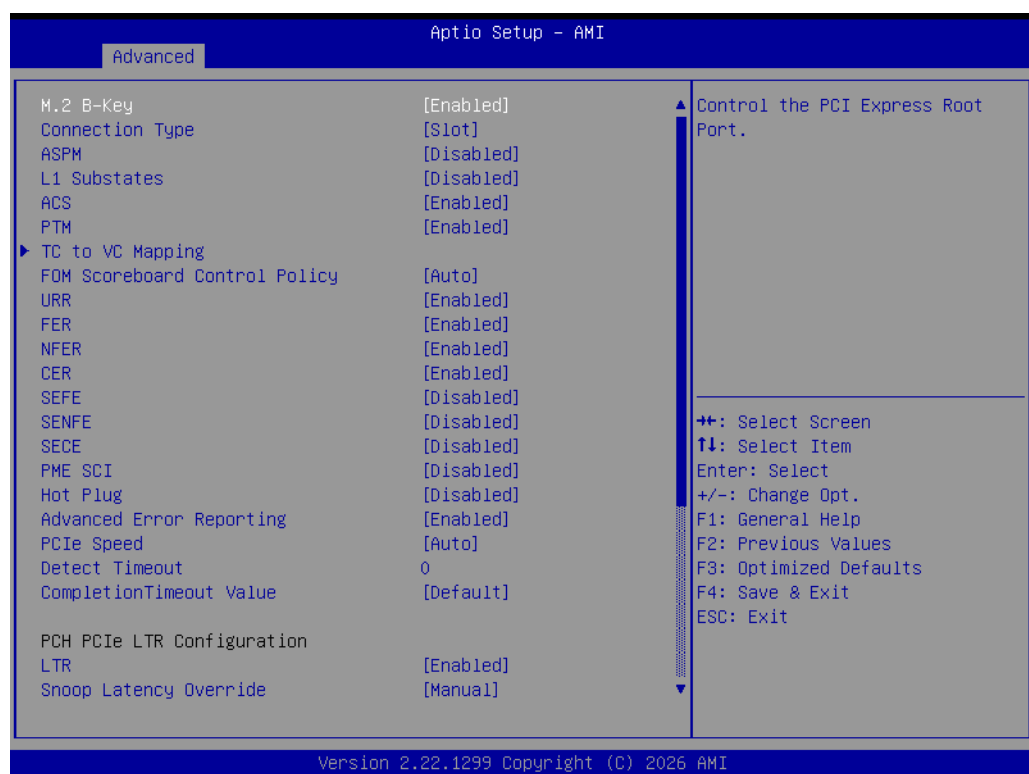
LAN4 Controller

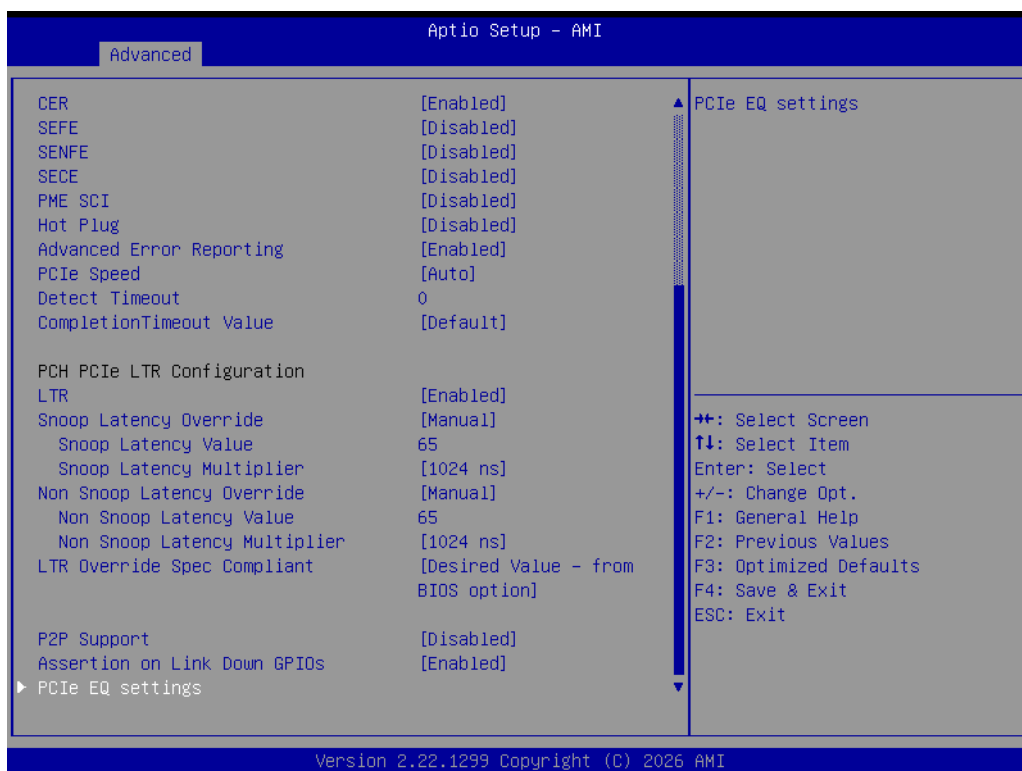
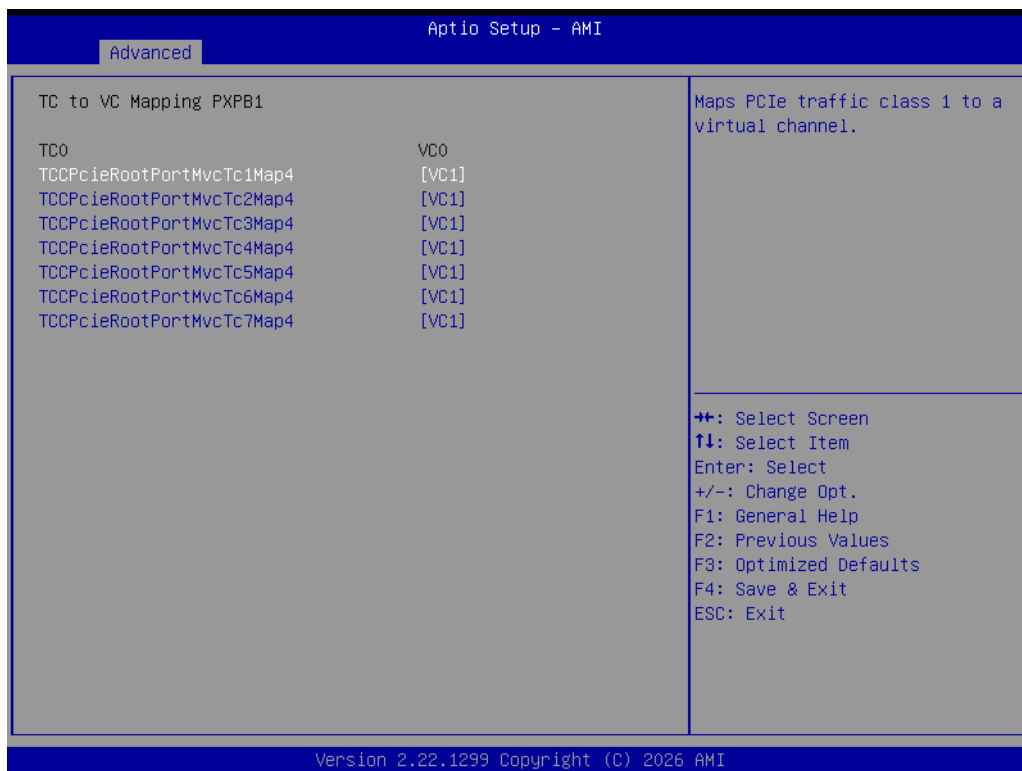


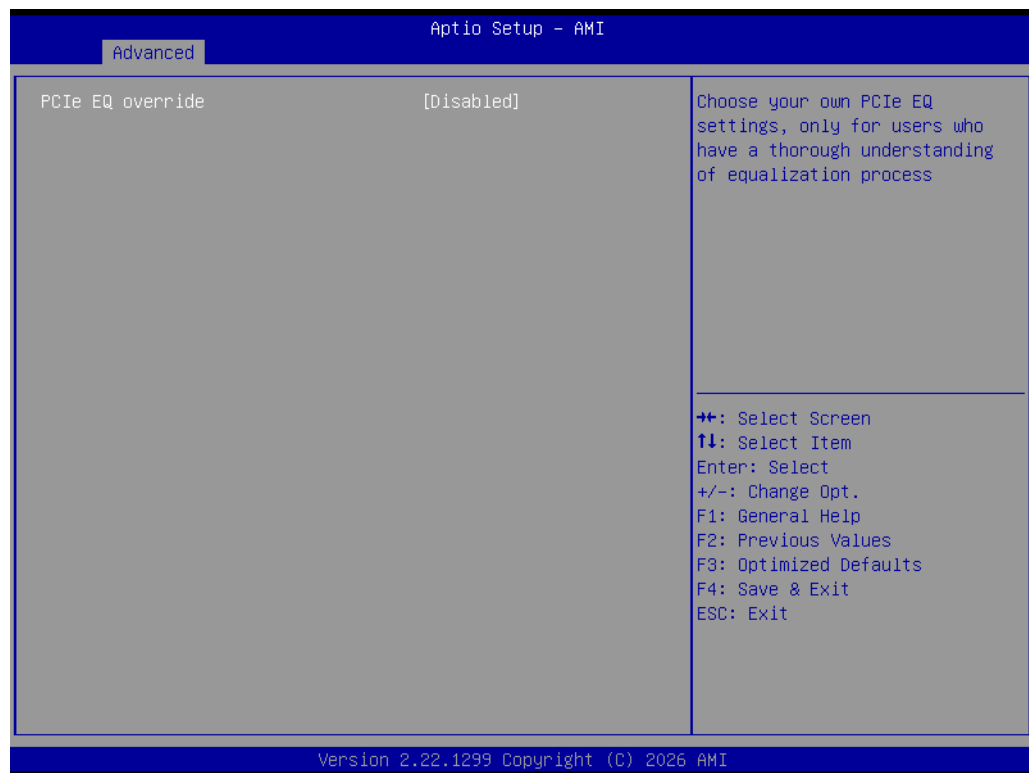




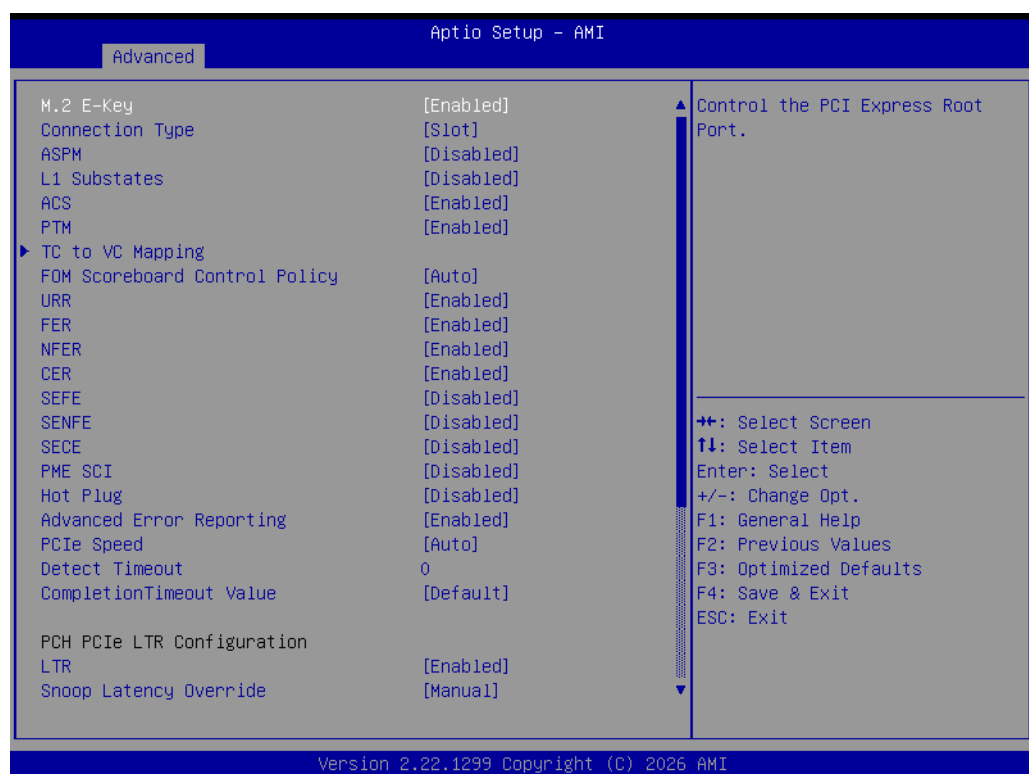
M.2 B-Key

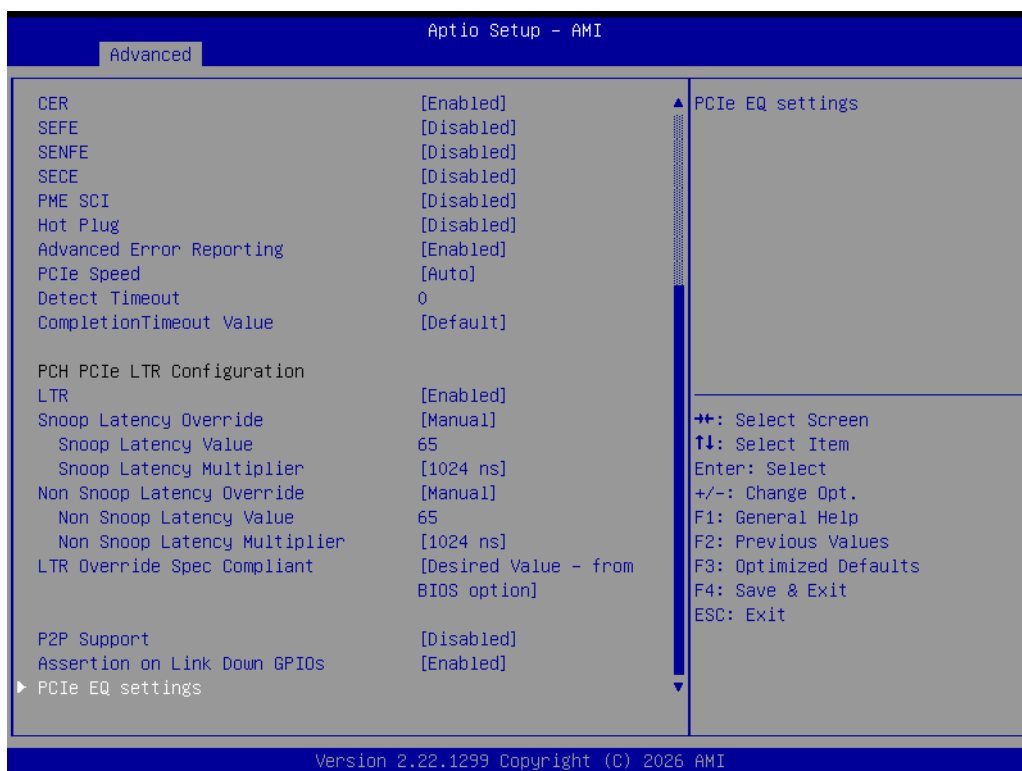
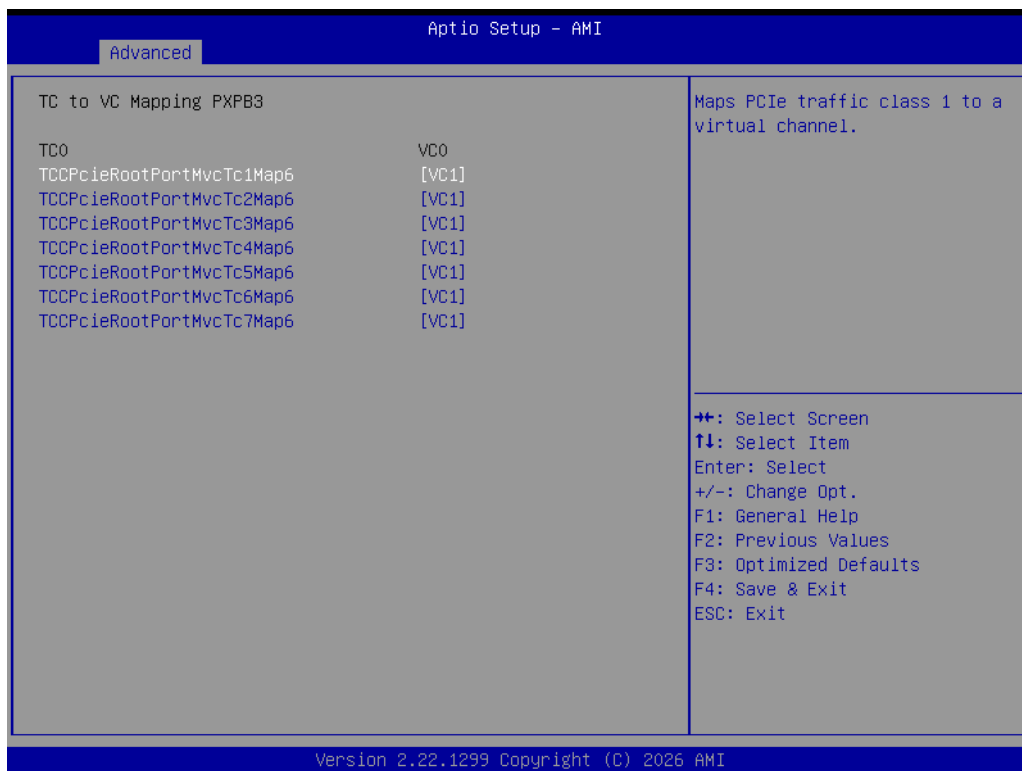


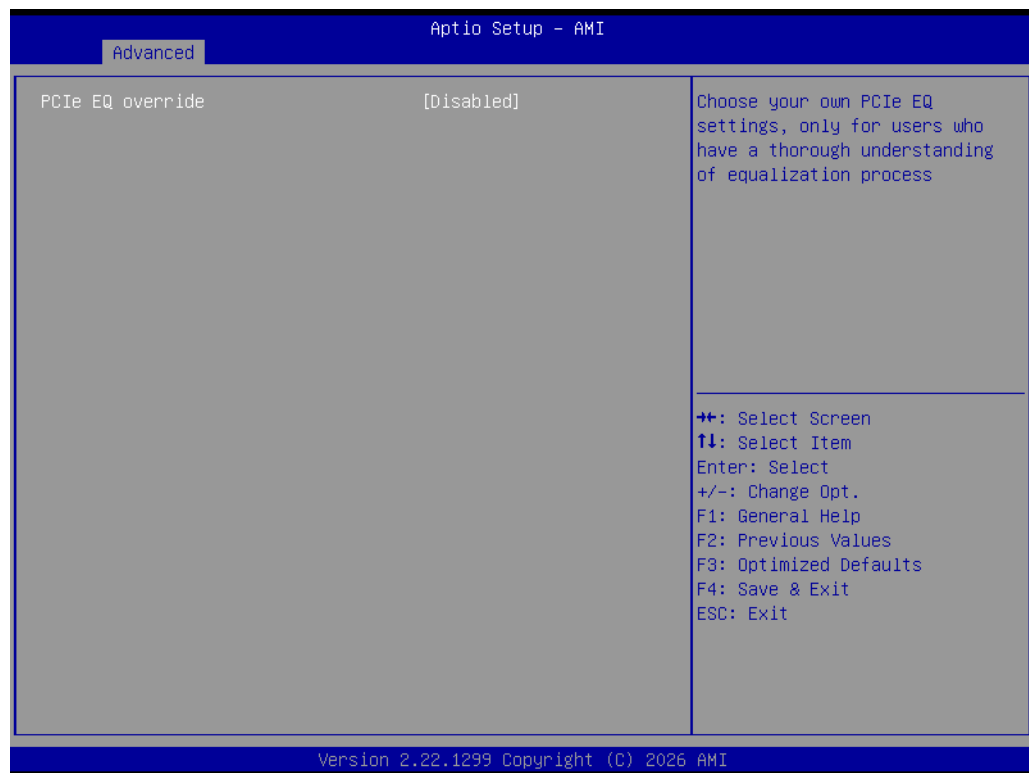




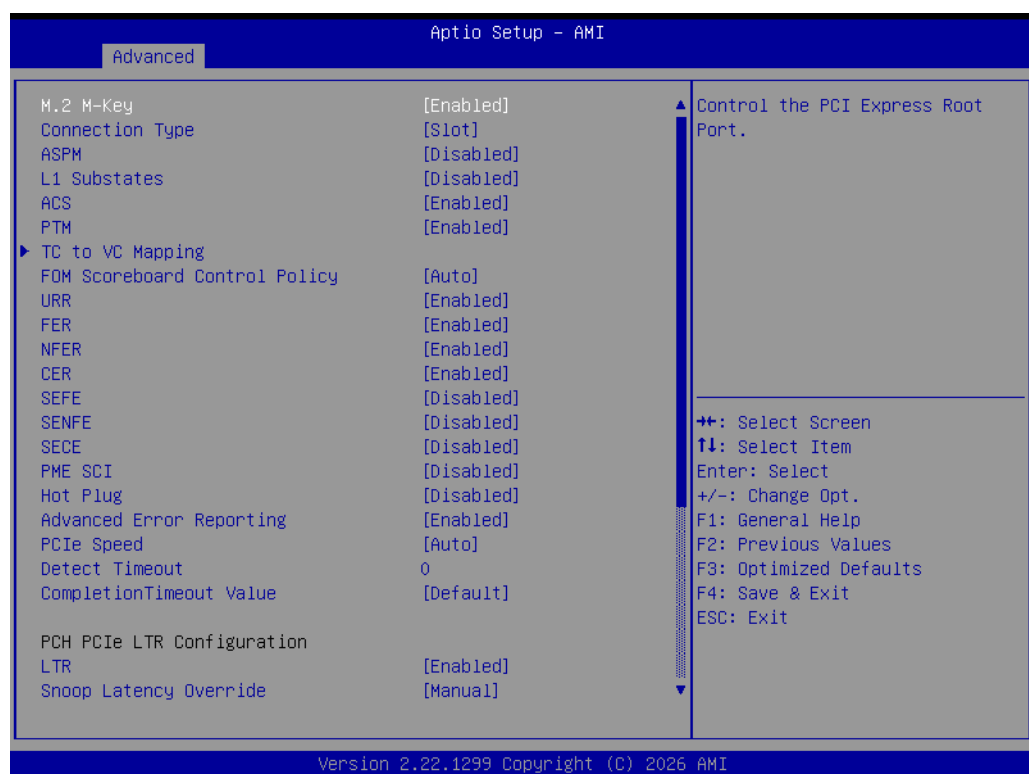
M.2 E-Key

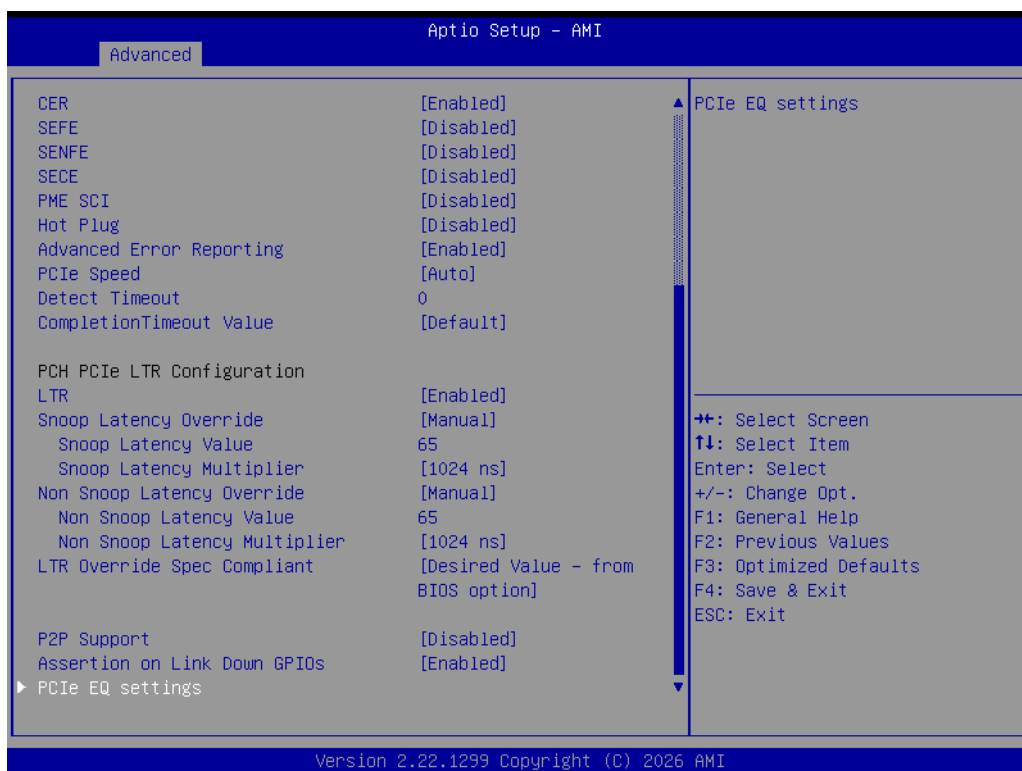
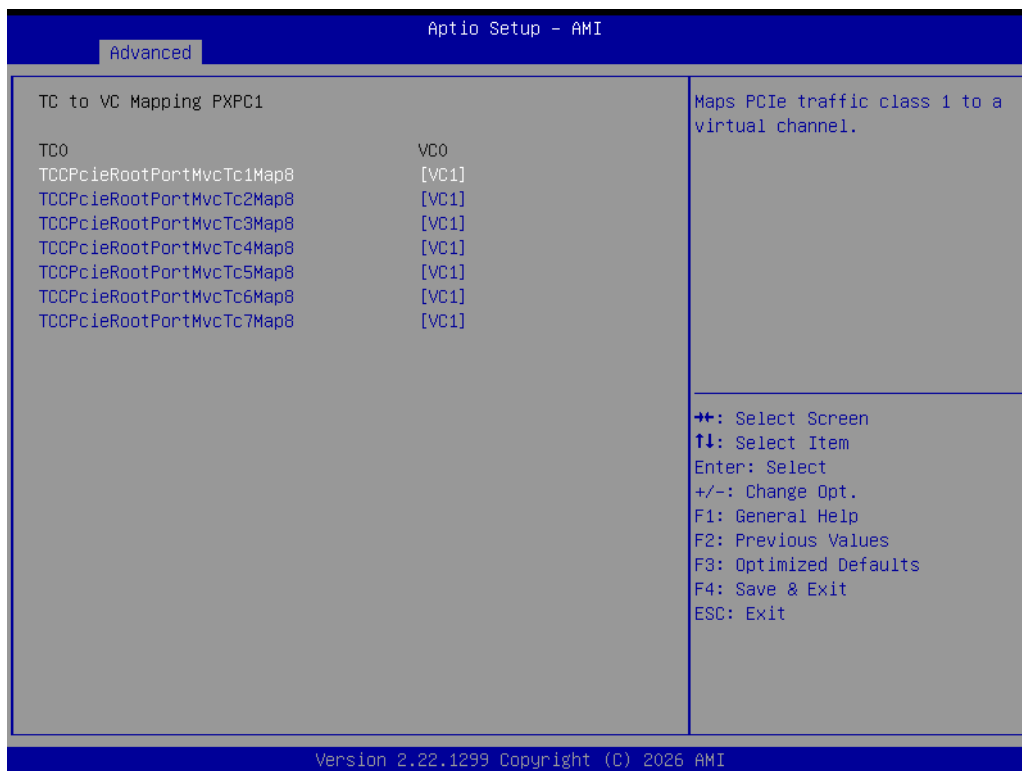


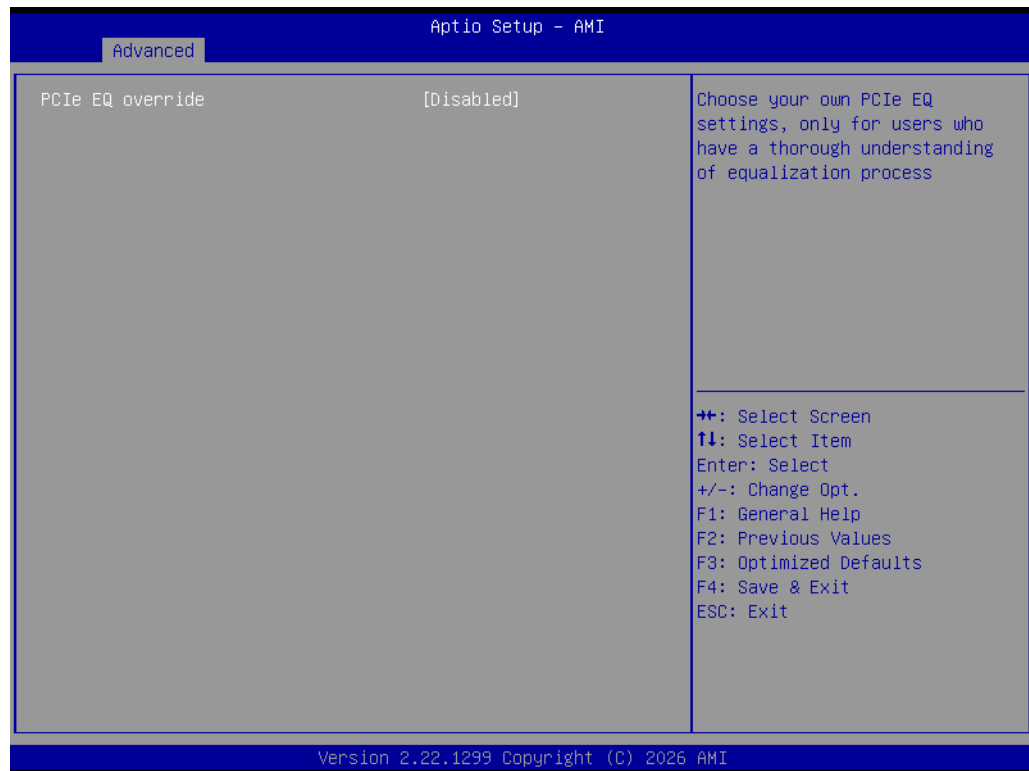




M.2 M-Key





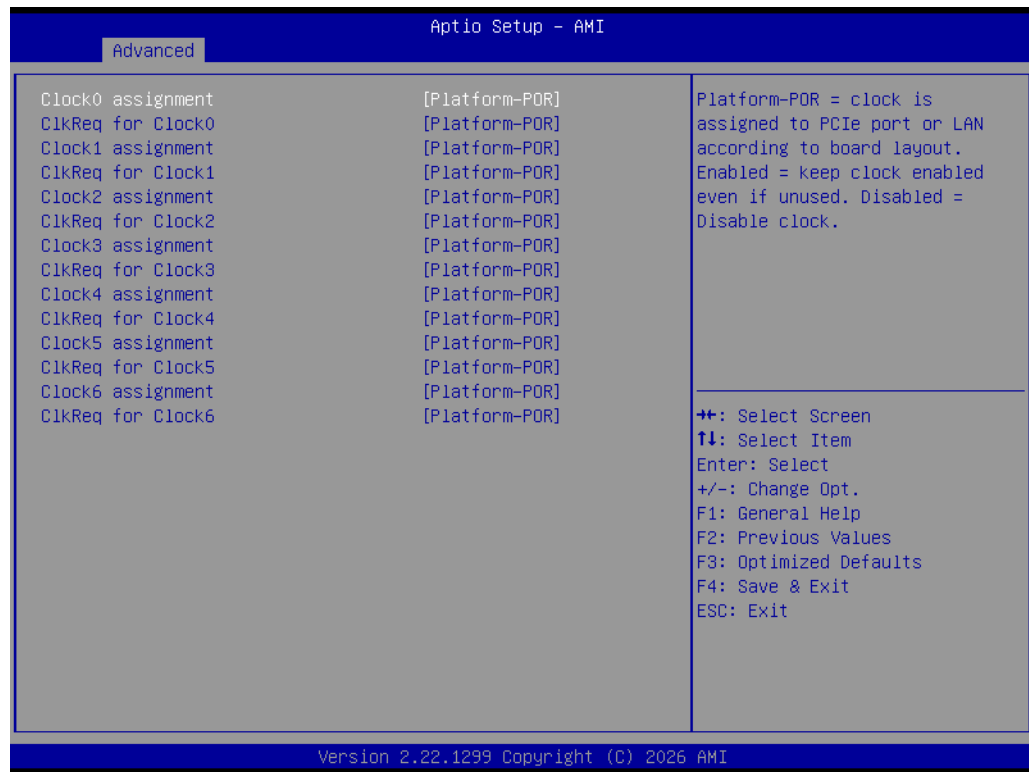


- **LAN1/2/3/4 Controller**
Enables/Disables onboard LAN1/2/3/4.
- **M.2 B/E/M-Key**
Enables/Disables onboard M.2 B/E/M key.
- **Connection Type**
Built-In: A built-in device is connected to this root port. The Slot Implemented bit is clear. Slot: This root port is connected to a user-accessible slot. The Slot Implemented bit is set.
- **ASPM**
PCI Express Active State Power Management settings.
- **L1 Substates**
PCI Express L1 Substates settings. L1SS cannot be enabled when CLKREQMSG is disabled.
- **ACS**
Enables/Disables Access Control Services Extended Capability.
- **PTM**
Enables/Disables Precision Time Measurement.
- **TC to VC Mapping**
PCIe Traffic Class to Multi Virtual Channel (TC->VC) mapping.
- **FOM Scoreboard Control Policy**
Select the FOM Scoreboard Control Policy, when set to Auto, speed is based on TLS.
- **URR**
Enables/Disables PCI Express Unsupported Request Reporting.
- **FER**
Enables/Disables PCI Express device Fatal Error Reporting.
- **NFER|**
Enables/Disables PCI Express device Non-Fatal Error Reporting.

- **CER**
Enables/Disables PCI Express Device Correctable Error Reporting.
- **SEFE**
Enables/Disables Root PCI Express System Error On Fatal Error.
- **SENF**
Enables/Disables Root PCI Express System Error On Non-fatal Error.
- **SECE**
Enables/Disables Root PCI Express System Error On Correctable Error.
- **PME SCI**
Enables/Disables PCI Express PME SCI.
- **Hot Plug**
Enables/Disables PCI Express hot plug.
- **Advanced Error Reporting**
Enables/Disables advanced error reporting.
- **PCIe Speed**
Configure PCIe speed.
- **Detect Timeout**
The number of milliseconds reference code will wait for link to exit detect state for enabled ports before assuming there is no device and potentially disabling the port.
- **Completion Timeout Value**
PCH PCIE Completion Timeout Value
- **LTR**
Enables/Disables SA PCIE latency reporting.
- **Snoop Latency Override**
Snoop Latency Override for SA PCIE.
- **Snoop Latency Value**
LTR Snoop Latency value for PCIe. The recommended value is 65 μ s. The default value for this BIOS option is 65 μ s.
- **Snoop Latency Multiplier**
LTR Snoop Latency Multiplier for PCIe. The recommended LTR Snoop Latency is 65 μ s. The default value for this BIOS option is 1024 ns, which is multiplied by the LTR Snoop Latency value.
- **Non Snoop Latency Override**
Non Snoop Latency Override for SA PCIE.
- **Non Snoop Latency Value**
LTR Non Snoop Latency value for PCIe. The recommended value is 65 μ s. The default value for this BIOS option is 65 μ s.
- **Non Snoop Latency Multiplier**
LTR Non Snoop Latency Multiplier of PCIE, recommended value is 65us.
- **LTR Override Spec Compliant**
By default, Desired Value is selected. Desired Value programs the LTR value with the recommended setting. Spec Compliant programs the LTR value to 400 ns and may prevent the platform from entering power-gating (PG) states.
- **P2P Support**
Programs the P2P support registers based on the selected options.
- **Assertion on Link Down GPIOs**
GPIO Assertion on Link Down.
- **TC0(~7)**
(TC0) Traffic Class 0 is always mapped to virtual channel 0.
(~7, x = 1~7) Maps PCIe traffic class x to a virtual channel.

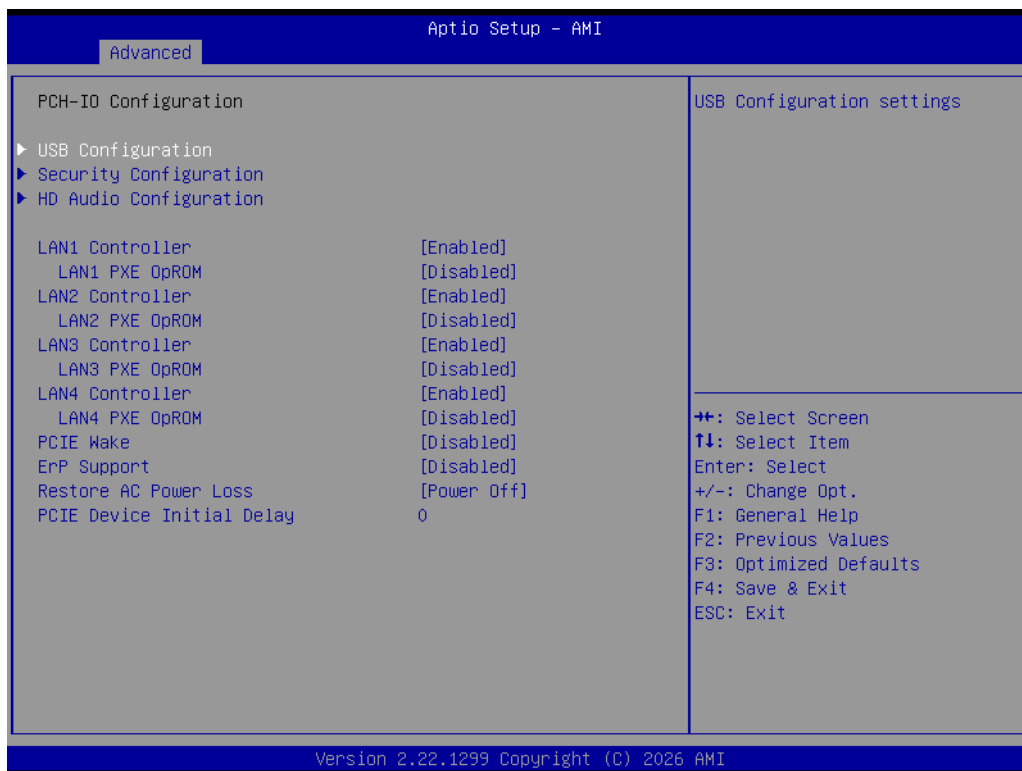
- **TCC PCIe Root Port MVC TC1–TC7 Map1–Map8**
(Tx= 1~7) Maps PCIe traffic class x to a virtual channel.
- **PCIe EQ Override**
Choose your own PCIe EQ settings, only for users who have a thorough understanding of equalization process.

PCIE Clocks



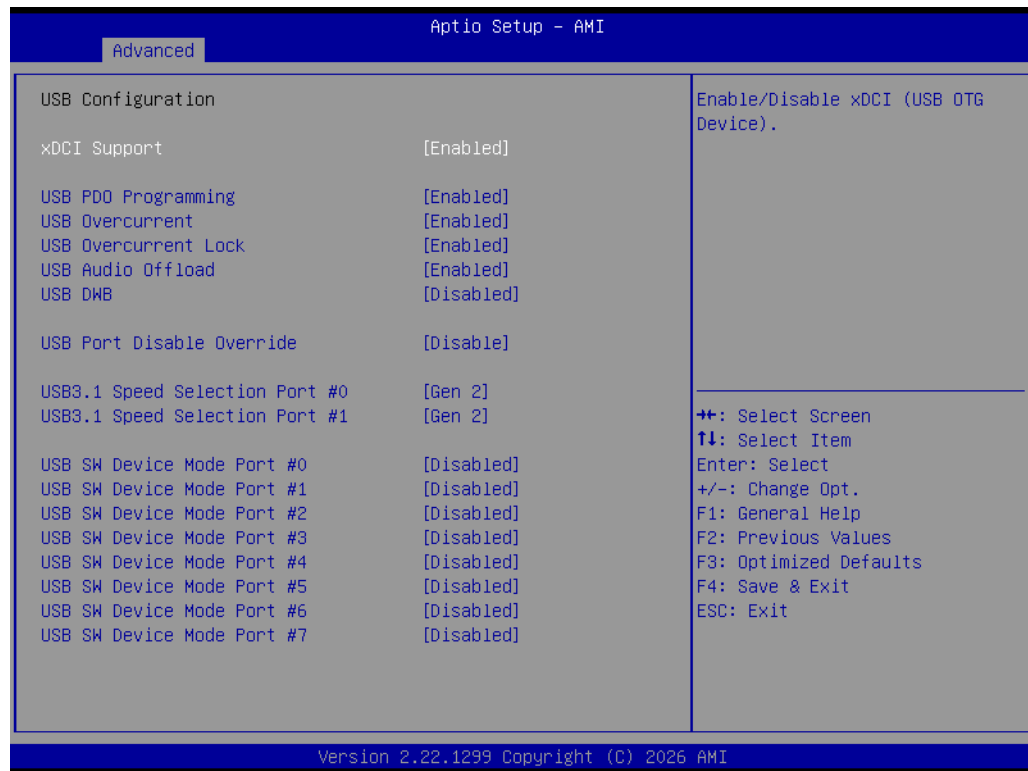
- **ClockX assignment**
Platform-POR = clock is assigned to a PCIe port or LAN according to board layout. Enabled = keep clock enabled even if unused. Disabled = Disable clock.
- **C1kReq for ClockX**
Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will not be used.

3.2.2.5 PCH-IO Configuration



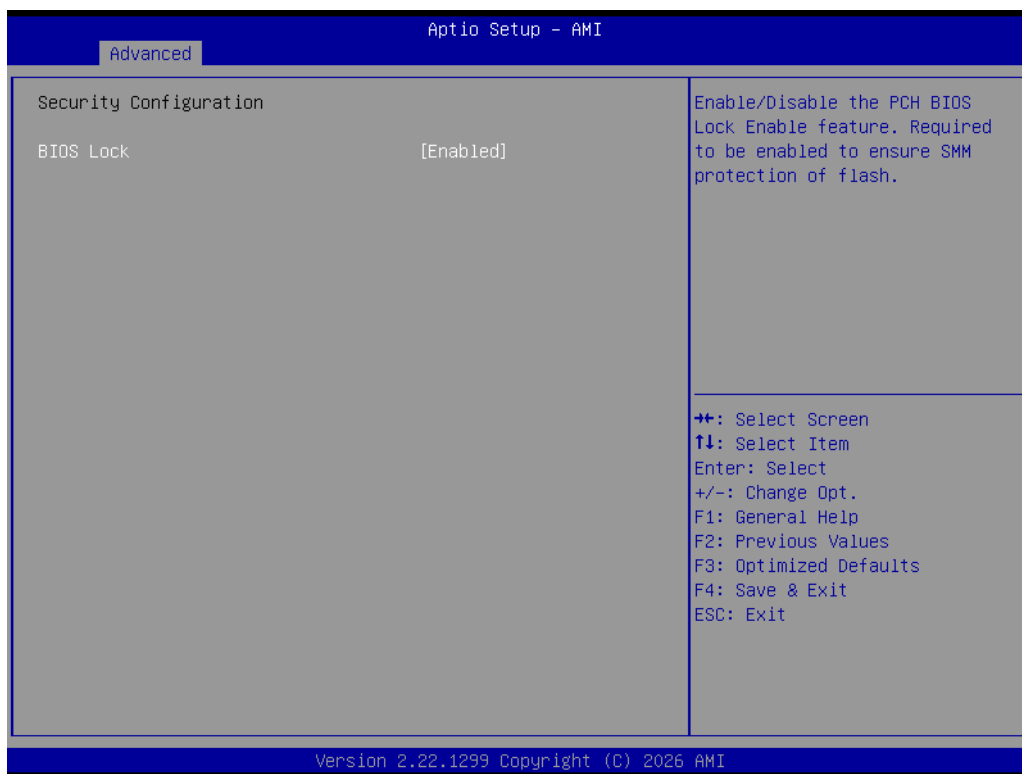
- **LAN1/2/3/4 Controller**
Enables/Disables onboard LAN1/2/3/4.
- **LAN1/2/3/4 PXE OpROM**
Enables/Disables boot option ROM for LAN1 controller.
- **PCIe Wake**
Enables/Disables PCIe to wake the system from S5.
- **ErP Support**
Enables/Disables ErP support under S5.
- **Restore AC Power Loss**
Specify what state to go to when power is re-applied after a power failure (G3 state).
- **PCIe Device Initial Delay**
The PCIe device initial delay 0~30 seconds.

USB Configuration



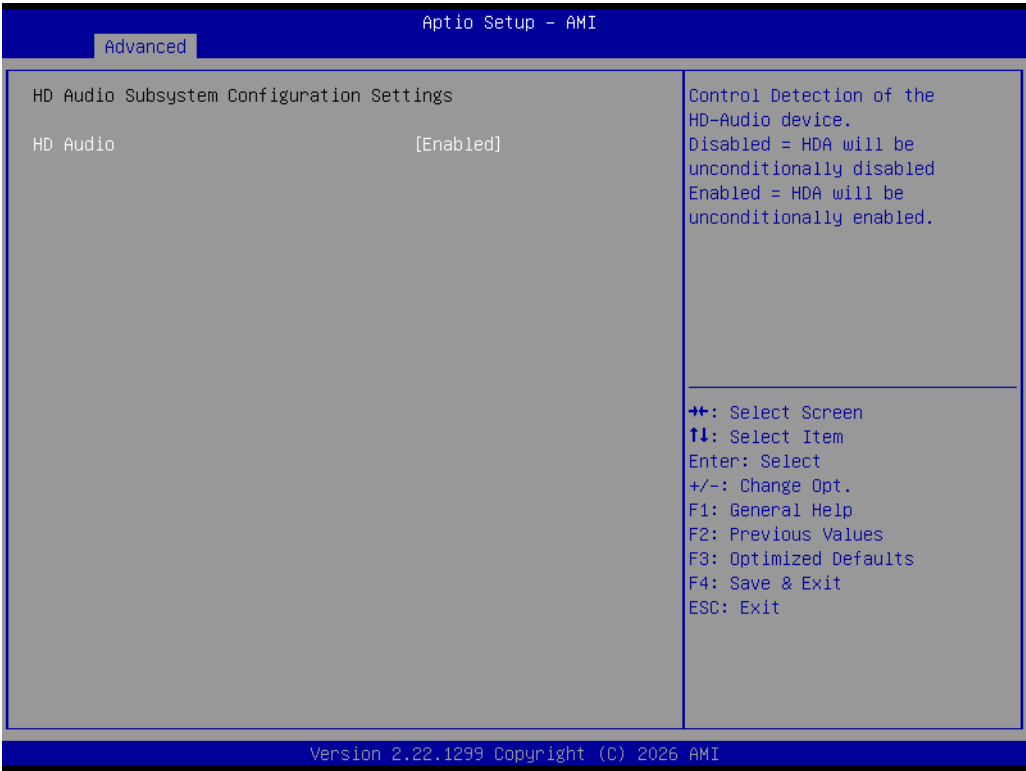
- **xHCI Support**
Enables/Disables xHCI (USB OTG device).
- **USB PDO Programming**
Select 'Enabled' if Port Disable Override functionality is used.
- **USB Overcurrent**
Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data. 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**
Selectively Enables/Disables the corresponding USB port from reporting a device connection to the controller.
- **USB Audio Offload**
Enables/Disables USB Audio Offload functionality.
- **USB DWB**
Enables/Disables USB Deferred Write Buffer feature.
- **USB Port Disable Override**
Selectively Enables/Disables the corresponding USB Port from reporting a device connection to the controller.
- **USB3.1 Speed Selection Port #0/1**
USB3.1 Speed Selection; Gen1 or Gen2.
- **USB SW Device Mode Port #0~7**
Enable connector event for device subscription.

Security Configuration



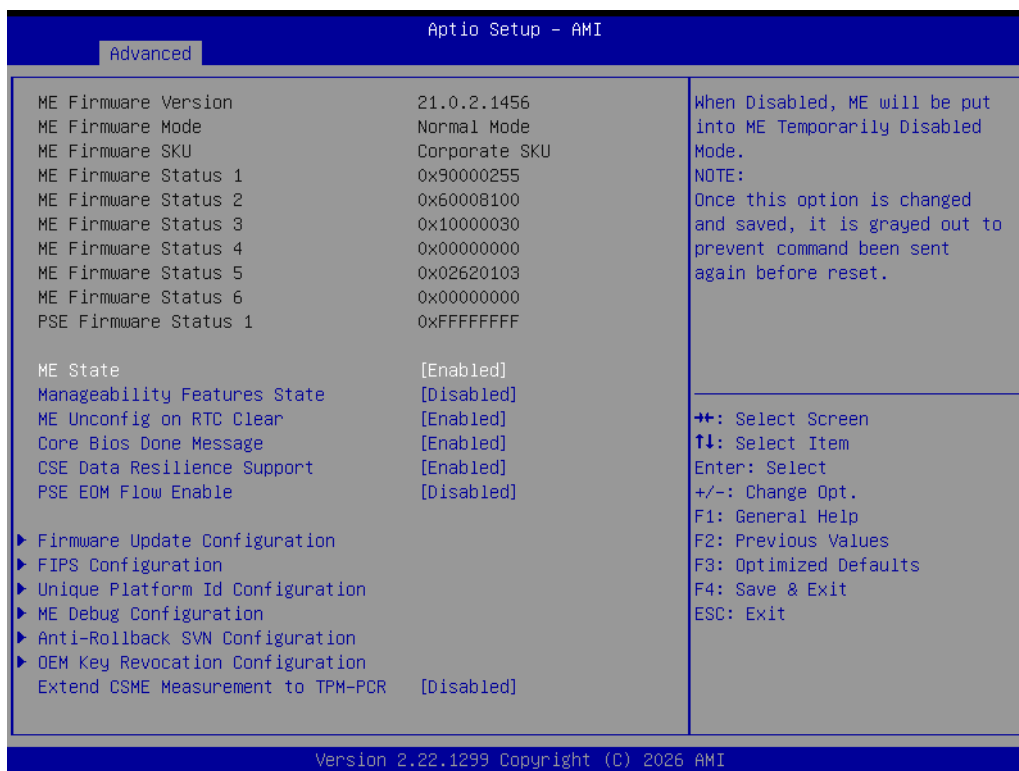
- **BIOS Lock**
Enables/Disables the PCH BIOS Lock enable feature. This is required to be enabled to ensure SMM protection of flash.

HD Audio Subsystem Configuration Settings



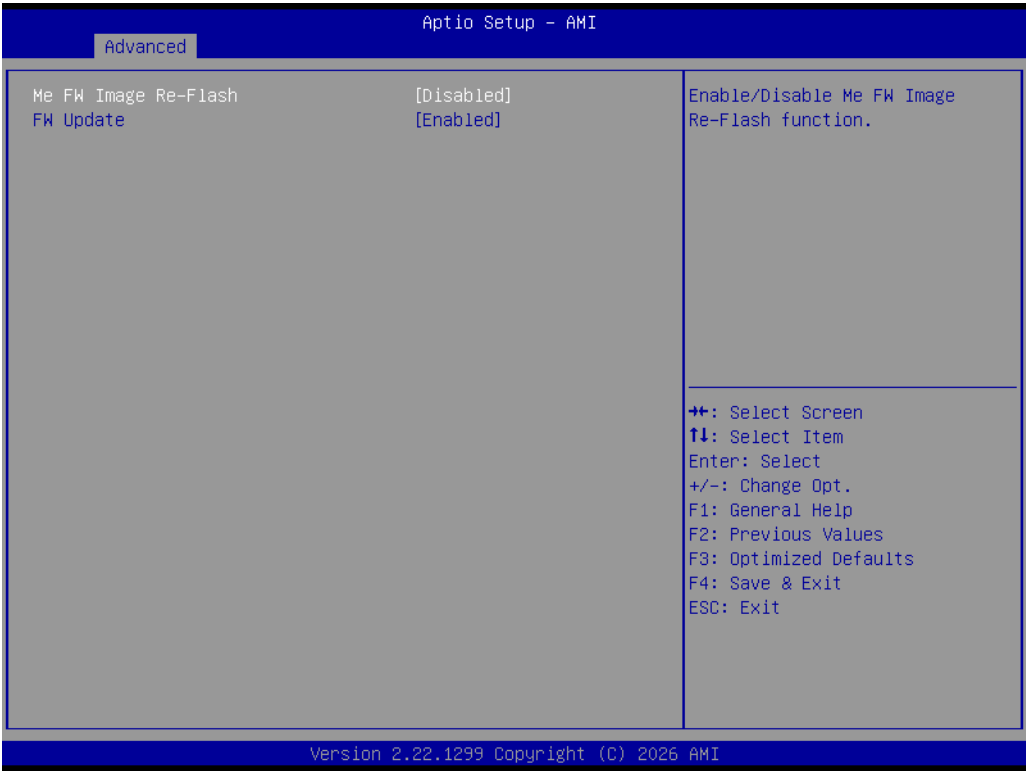
- **HD Audio**
Control Detection of the HD-Audio device. Disabled = HDA will be unconditionally disabled. Enabled = HDA will be unconditionally Enabled.

3.2.2.6 PCH-FW Configuration



- **ME State**
When disabled ME will be put into ME temporarily disabled mode.
- **Manageability Features State**
Enables/Disables Intel Manageability features.
- **ME Unconfig on RTC Clear**
When Disabled ME will not be unconfigured on RTC Clear.
- **Core BIOS Done Message**
Enables/Disables core BIOS Done message sent to ME.
- **CSE Data Resilience Support**
Enables/Disables CSE Data Resilience support.
- **PSE EOM Flow Enable**
Enables/Disables PSE EOM flow.
- **Extend CSME Measurement to TPM-PCR**
Enables/Disables Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1].

Firmware Update Configuration



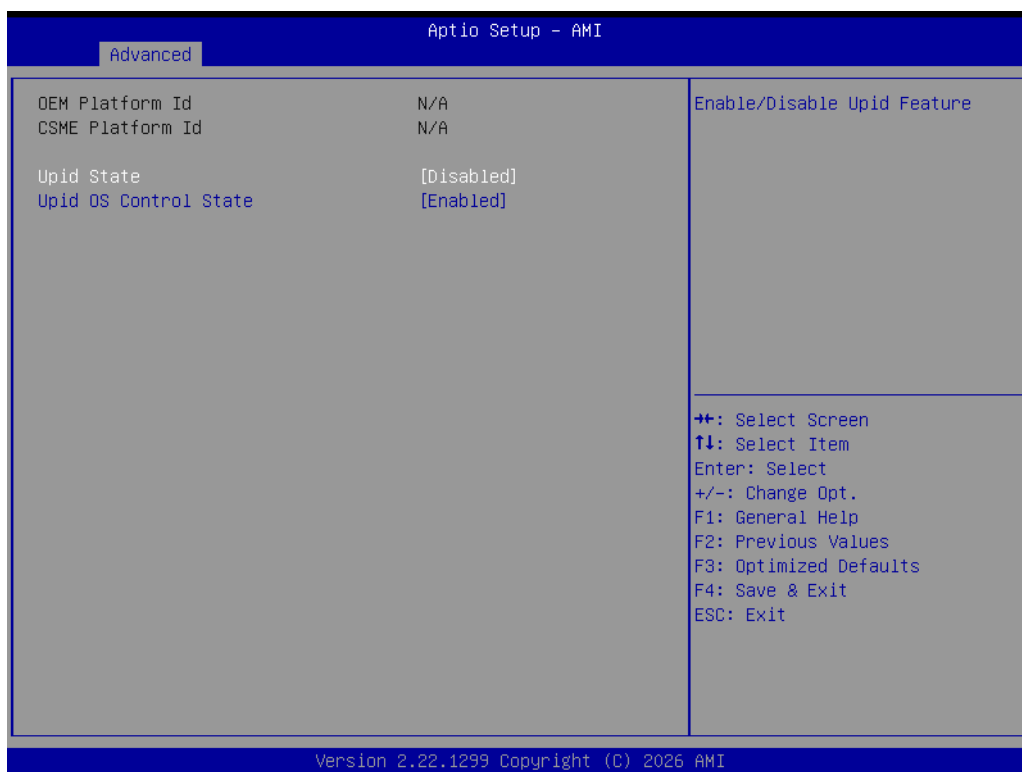
- **Me FW Image Re-Flash**
Enables/Disables Me FW Image Re-Flash function.
- **FW Update**
Enables/Disables ME FW Update function. Enables/Disables ME FW Update function.

FIPS Configuration



- **FIPS Mode Select**
FIPS Mode configuration.

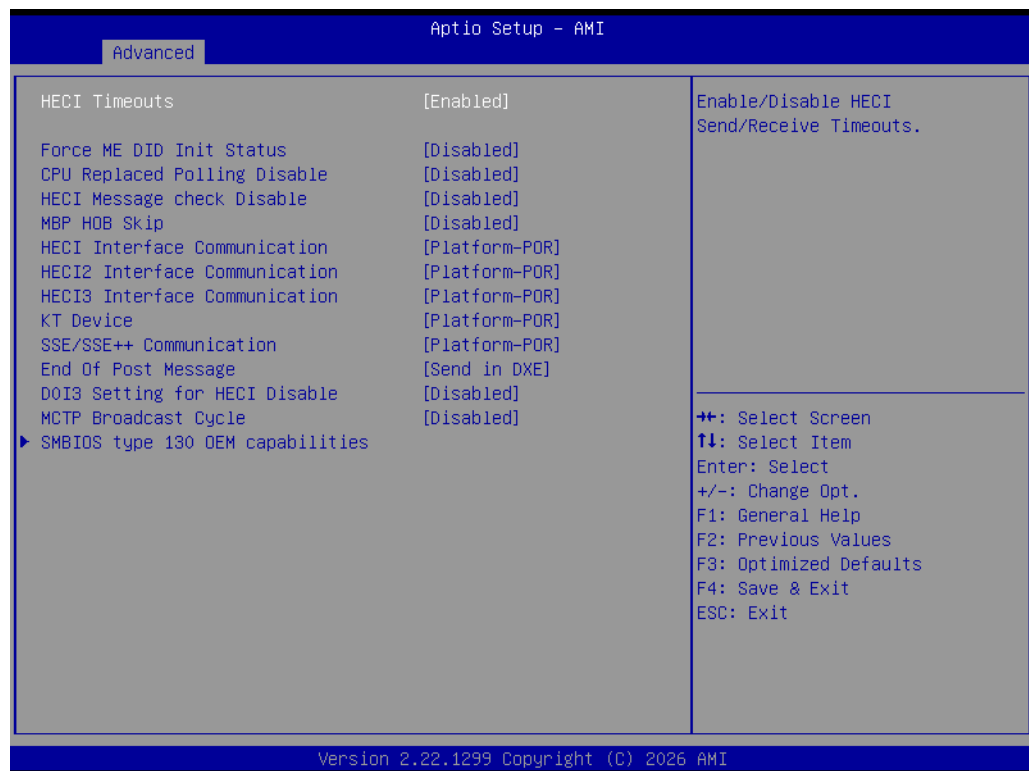
Unique Platform ID Configuration



- **Upid State**
Enables/Disables Upid Feature.

- **Upid OS Control State**
Allows the OS to enable or disable the UPID feature state.

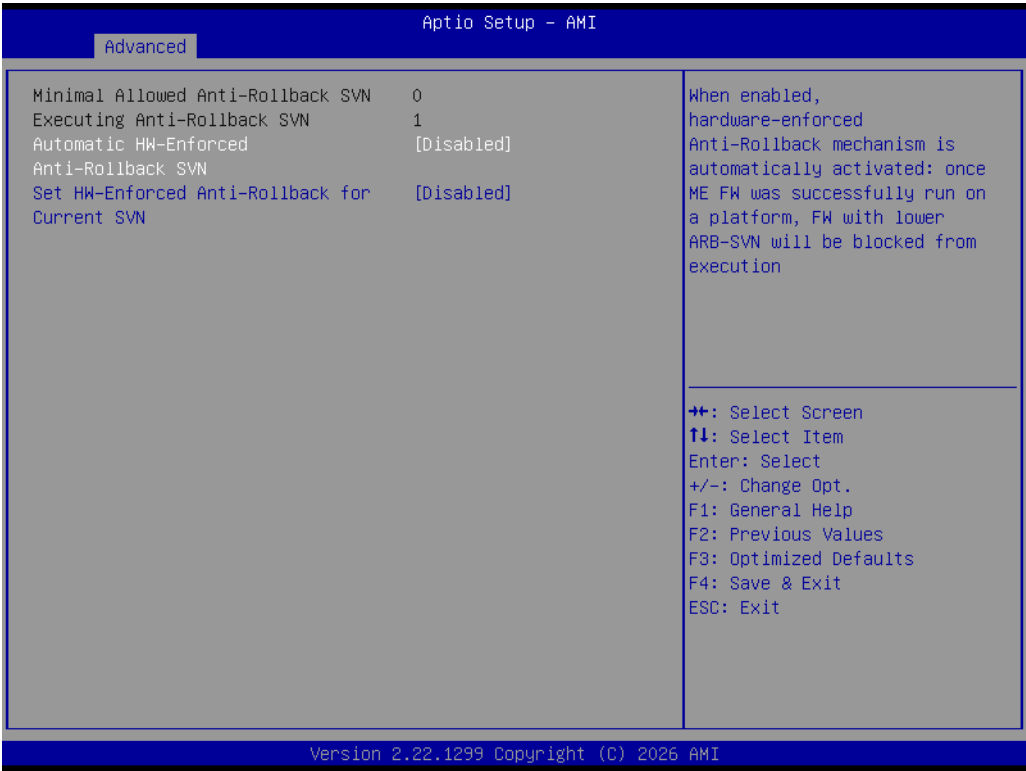
ME Debug Configuration



- **HECI Timeouts**
Enables/Disables HECI, send/receive timeout.

- **Force ME DID Init Status**
Force the DID initialization status value.
- **CPU Replaced Polling Disable**
Setting this option disables CPU replacement polling loop.
- **HECI Message Check Disable**
Setting this option disables message check for BIOS boot path when sending.
- **HBP HOB Skip**
Setting this option will skip MBP HOB.
- **HECI Interface Communication**
Adds or removes the HECI Device from the PCI space.
- **KT Device**
Enables/Disables KT Device.
- **SSE/SSE++ Communication**
Enables/Disables SSE/SSE++ Devices from PCI config space.
- **End of Post Message**
Enables/Disables End of Post message sent to ME.
- **DOI3 Setting for HECI Disable**
Setting this option disables setting DOI3 bit for all HECI devices.
- **MCTP Broadcast Cycle**
Enables or disables the Management Component Transport Protocol (MCTP) broadcast cycle and sets PMT as the bus owner.
- **BIOS Reflash Capability State**
Change BIOS Reflash Capability State.
- **BIOS Boot to Setup Capability State**
Change BIOS Boot to Setup Capability State.
- **BIOS Pause Before Booting Capability State**
Change BIOS Pause Before Booting Capability State.
- **BIOS Secure Boot Capability Exposure to FW State**
Change BIOS Secure Capability Exposure State to FW. This does not affect SecureBoot as such.
- **vPro TBT Support**
Enables or disables vPro Thunderbolt (TBT) dock support. Note: For the change to take effect, place the system into the G3 state, then power it on again.

Anti-Rollback SVN Configuration



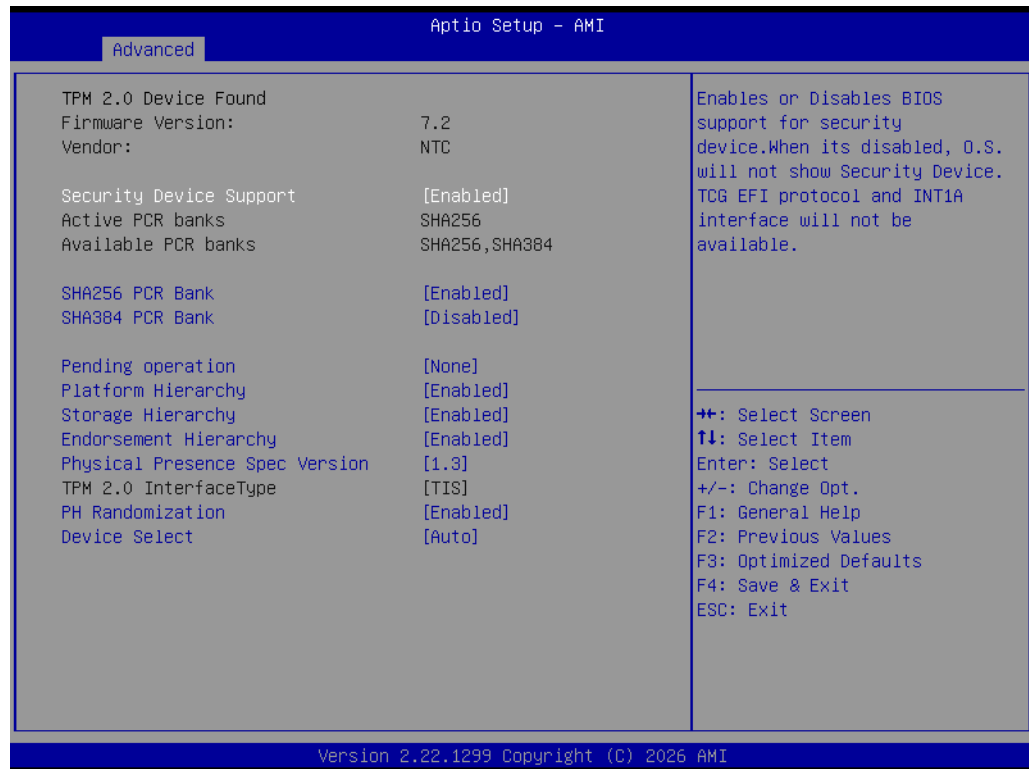
- **Automatic HW-Enforced Anti-Rollback SW**
When enabled, the hardware-enforced anti-rollback mechanism is automatically activated: once ME FW is successfully run on a platform, FW with lower ARB-SVN will be blocked from execution.
- **Set HW-Enforced Anti-Rollback for Current SVN**
Enable hardware-enforced Anti-Rollback mechanism for current ARB-SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent.

OEM Key Recovery Configuration



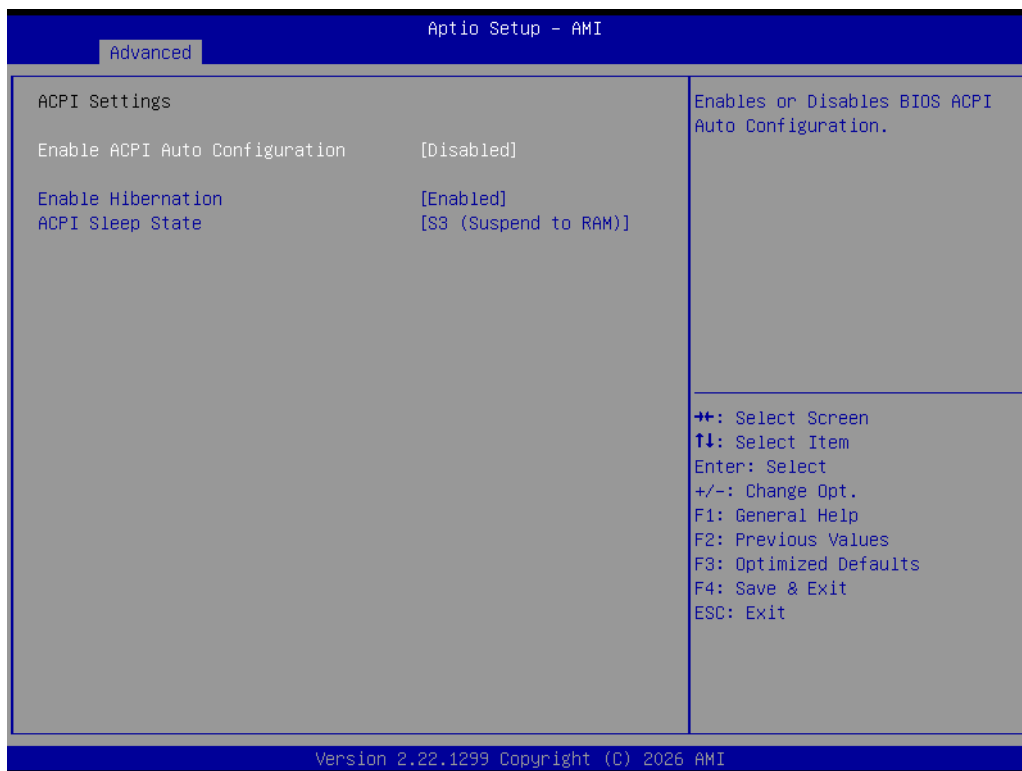
- **Automatic OEM Key Revocation**
When enabled, BIOS will automatically send HECI command to revoke OEM keys.
- **Invoke OEM Key Revocation**
Sends a HECI command to revoke the OEM key.

3.2.2.7 Trusted Computing



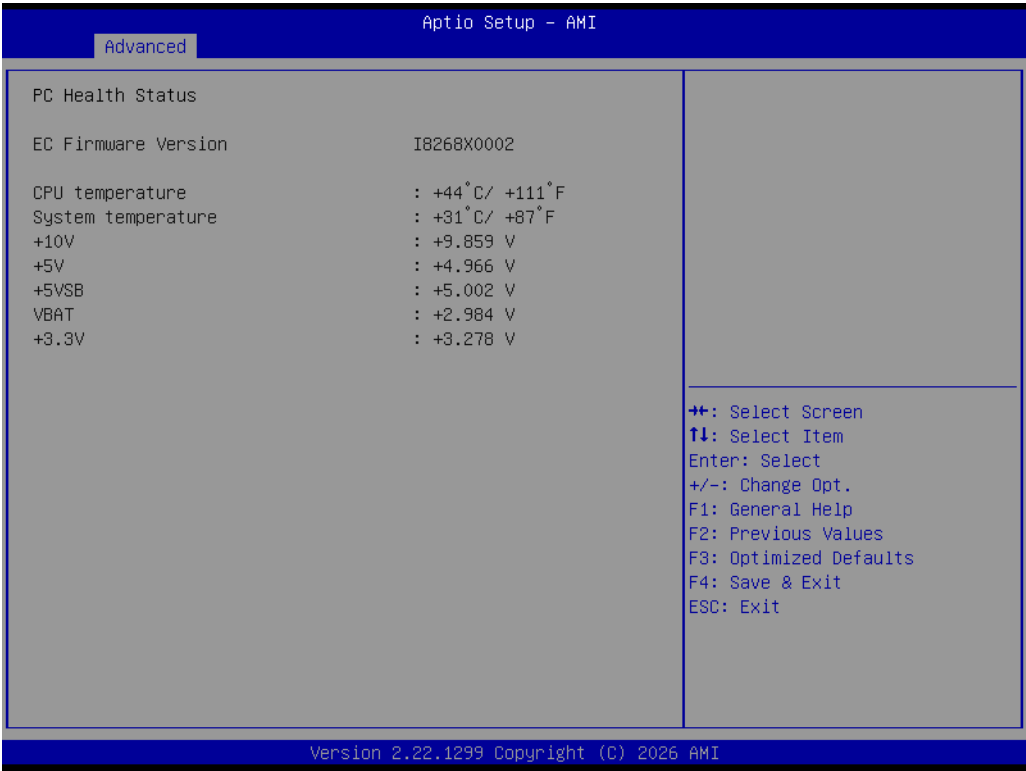
- **Security Device Support**
Enables/Disables BIOS support for security device.
- **SHA256 PCR Bank**
Enables/Disables SHA256 PCR Bank.
- **SHA384 PCR Bank**
Enables/Disables SHA384 PCR Bank.
- **Pending Operation**
Schedule an operation for the security device.
- **Platform Hierarchy**
Enables/Disables Platform Hierarchy.
- **Storage Hierarchy**
Enables/Disables Storage Hierarchy.
- **Endorsement Hierarchy**
Enables/Disables 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.
- **PH Randomization**
Enables/Disables Platform Hierarchy randomization. Do not enable this option on production platforms. This option is intended for development and testing only. Override the ChangePlatformAuth ELINK setting on production platforms that support TXT.
- **Device Select**
TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices.

3.2.2.8 ACPI Setting

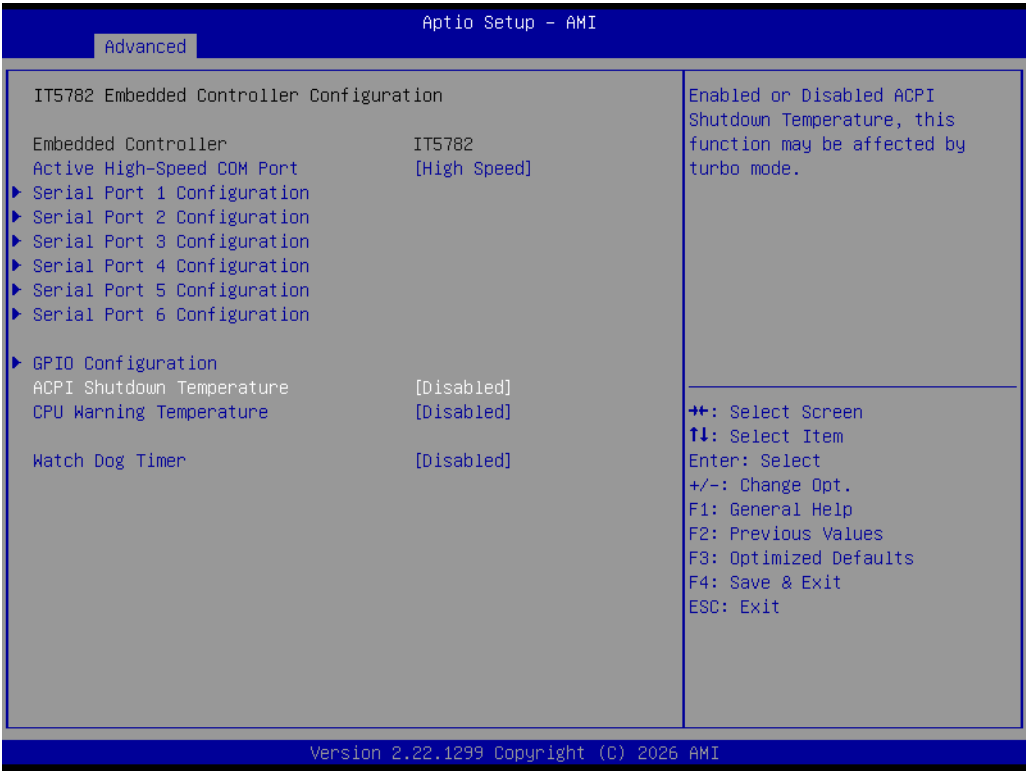


- **Enable ACPI Auto Configuration**
Enables/Disables BIOS ACPI Auto Configuration.
- **Enable Hibernation**
Enables or disables the system's ability to hibernate (OS/S4 sleep state).
- **ACPI Sleep State**
Selects the highest ACPI sleep state the system enters when the Suspend button is pressed.

3.2.2.9 IT5782 HW Monitor



3.2.2.10 IT5782 Embedded Controller Configuration



- **Active High-Speed COM Port**
Standard: Uses a standard COM port. High Speed: Uses a high-speed COM port. Driver installation is required.
- **ACPI Shutdown Temperature**
Enables/Disables ACPI Shutdown Temperature.

- **CPU Warning Temperature**
Enables/Disables CPU Warning Temperature function.
- **Watchdog Timer**
Enables/Disables Watch Dog Timer function (Start before boot to OS and must stop by self).

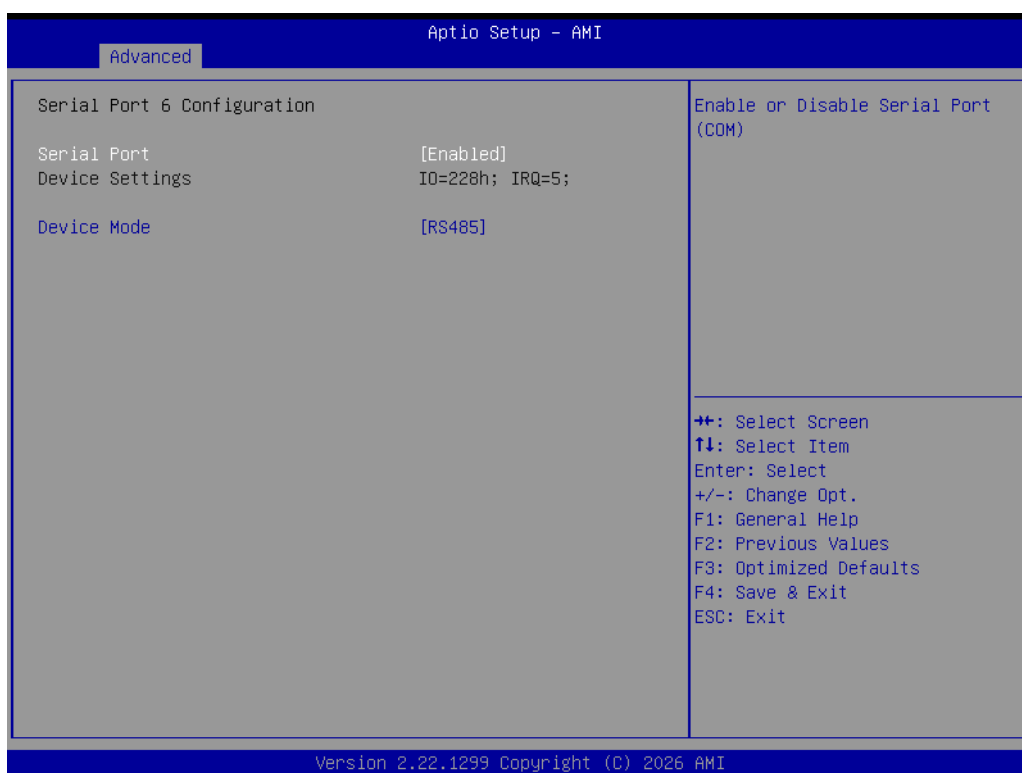
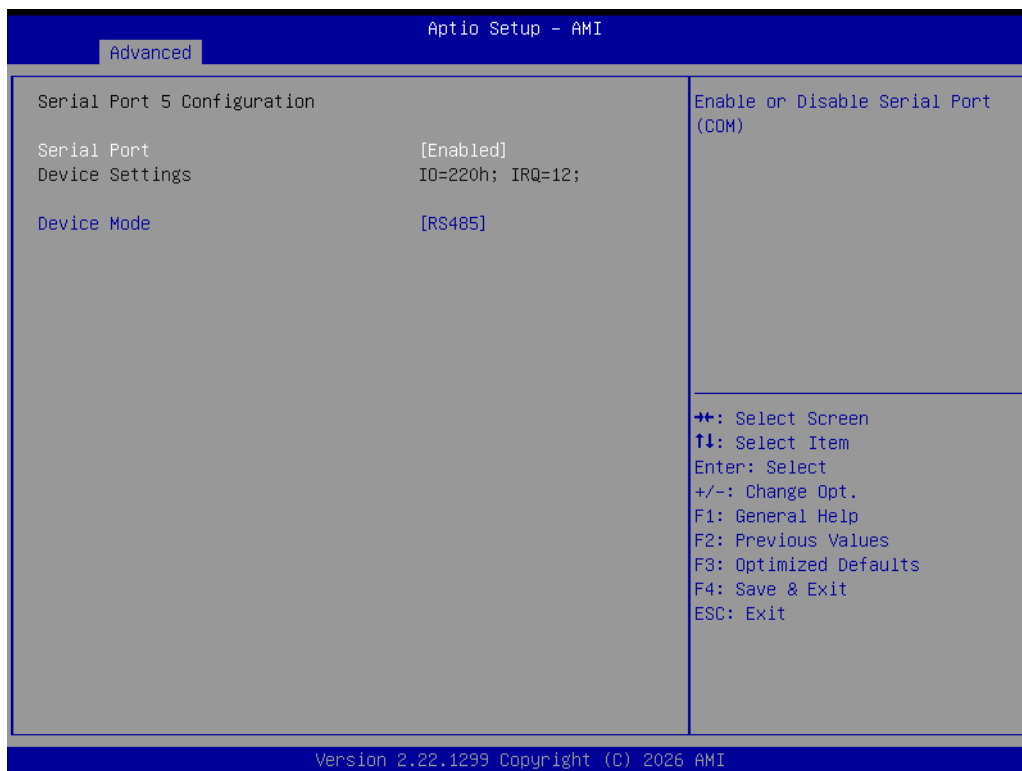
Serial Port 1~6 Configuration

Aptio Setup - AMI	
Advanced	
Serial Port 1 Configuration	
Serial Port	[Enabled]
Device Settings	I0=3F8h; IRQ=4;
Device Mode	[RS232]
Enable or Disable Serial Port (COM)	
↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1299 Copyright (C) 2026 AMI	

Aptio Setup - AMI	
Advanced	
Serial Port 2 Configuration	
Serial Port	[Enabled]
Device Settings	I0=2F8h; IRQ=3;
Device Mode	[RS232]
Enable or Disable Serial Port (COM)	
↔: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit	
Version 2.22.1299 Copyright (C) 2026 AMI	

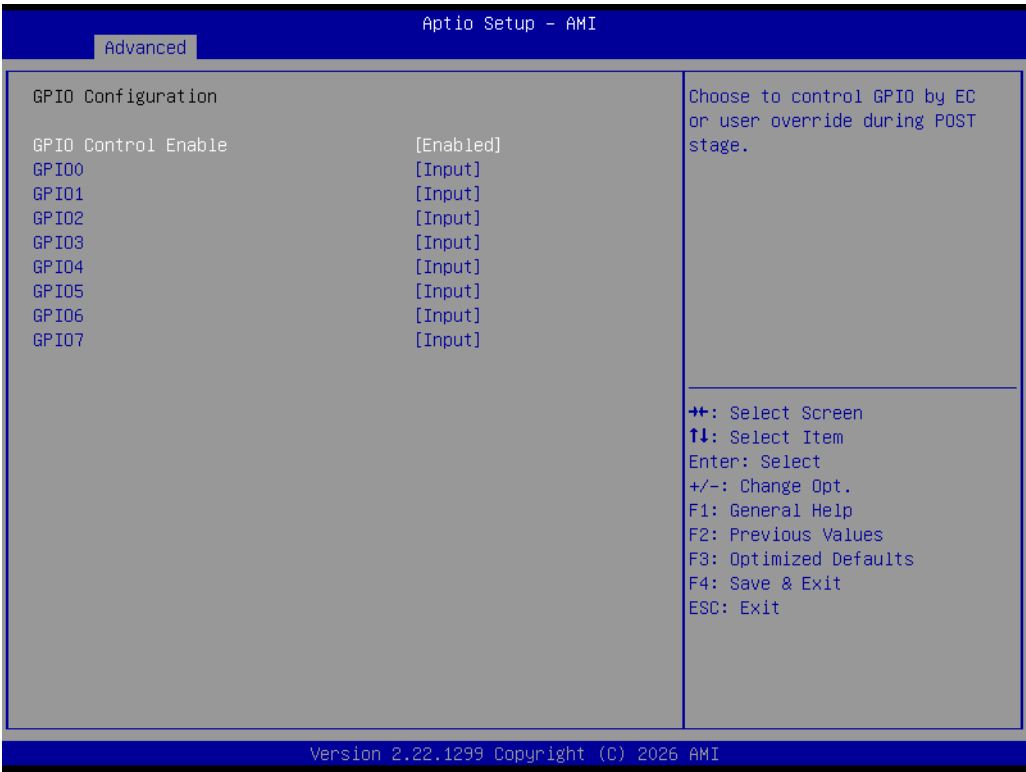
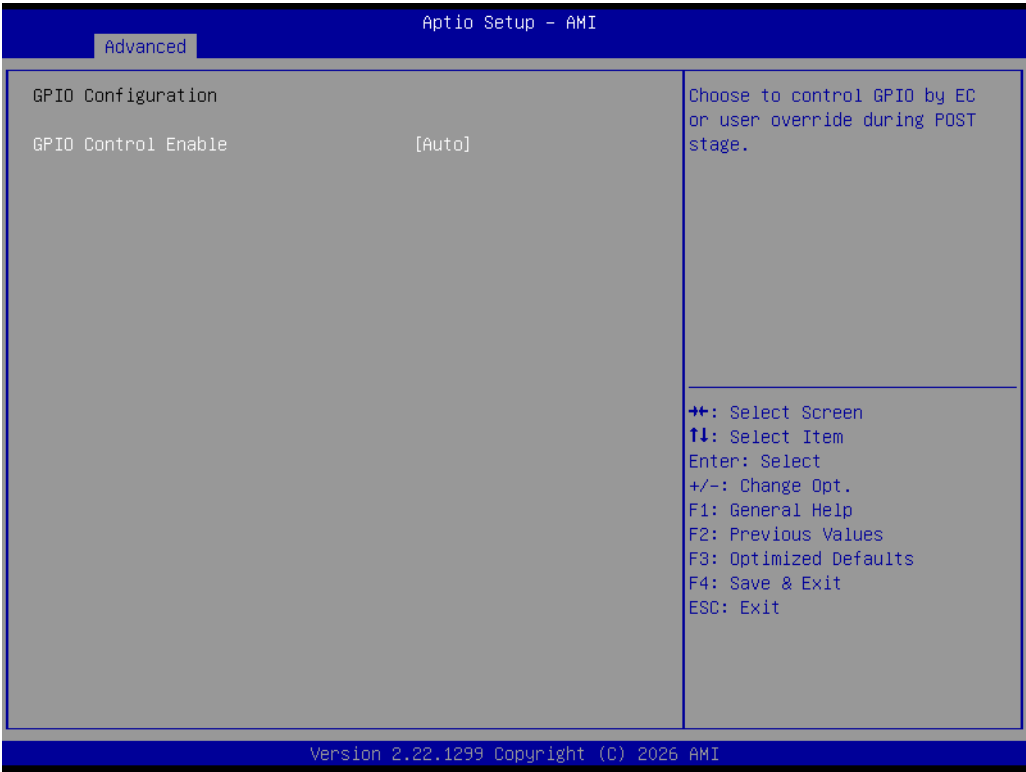
Aptio Setup - AMI		
Advanced		
Serial Port 3 Configuration		Enable or Disable Serial Port (COM)
Serial Port	[Enabled]	
Device Settings	IO=3E8h; IRQ=10;	
Device Mode	[RS485]	
		++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1299 Copyright (C) 2026 AMI		

Aptio Setup - AMI		
Advanced		
Serial Port 4 Configuration		Enable or Disable Serial Port (COM)
Serial Port	[Enabled]	
Device Settings	IO=2E8h; IRQ=11;	
Device Mode	[RS485]	
		++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Version 2.22.1299 Copyright (C) 2026 AMI		



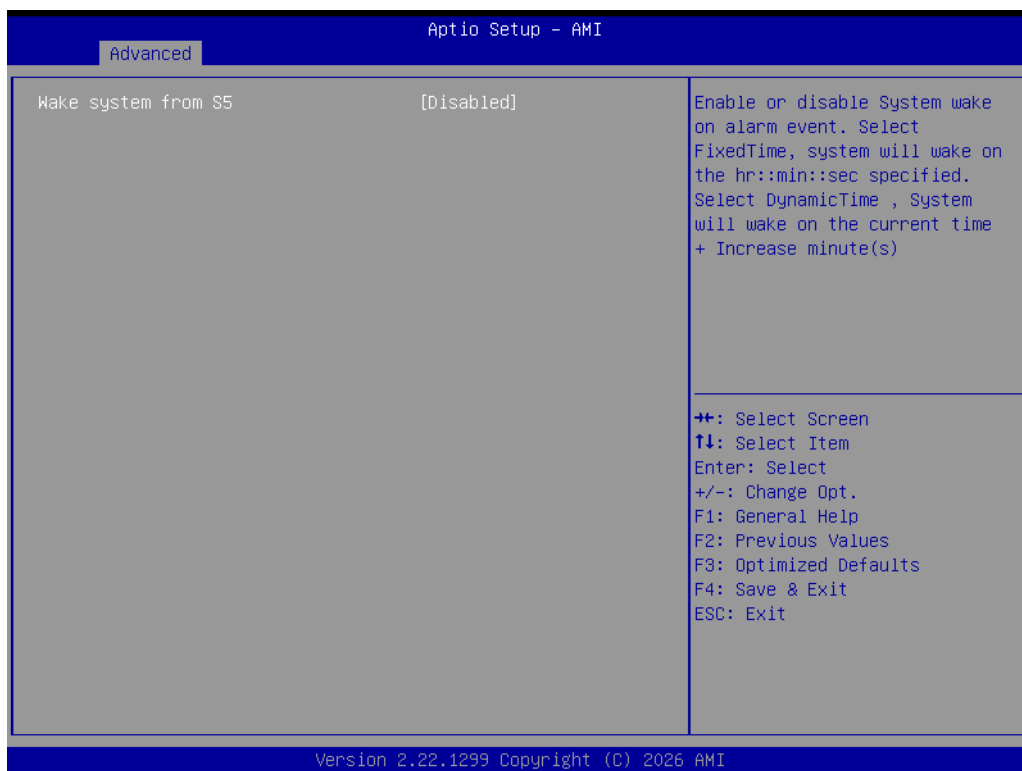
- **Serial Port**
Enables/Disables the serial port.
- **Device Mode**
Serial port mode select.

GPIO Configuration



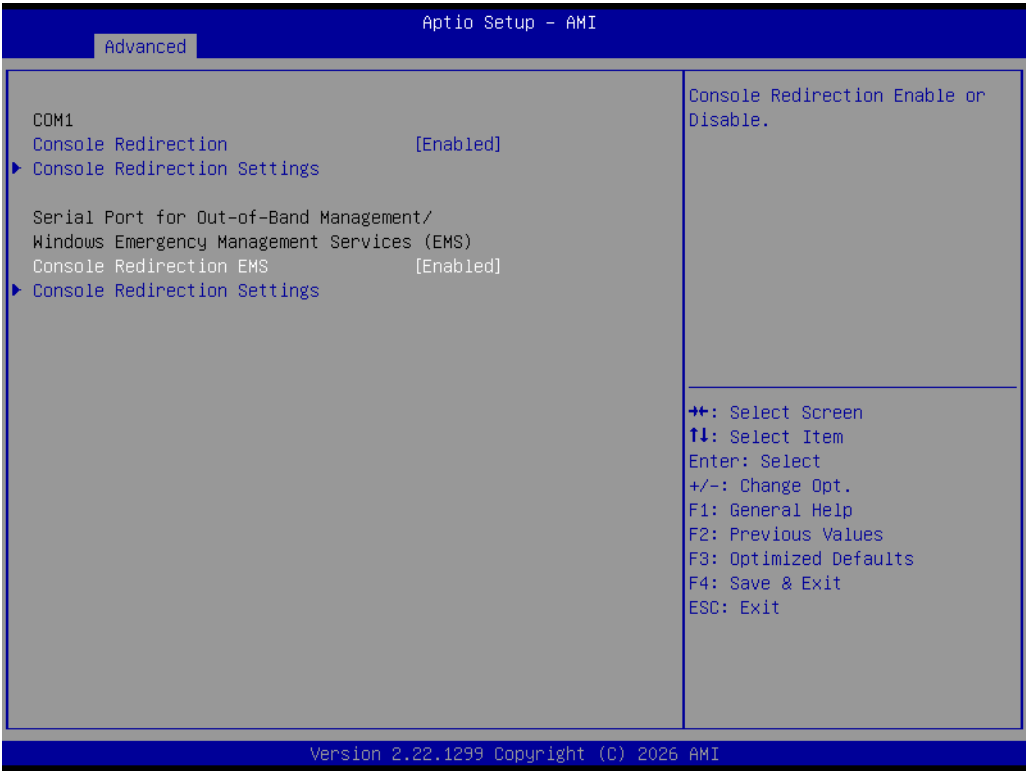
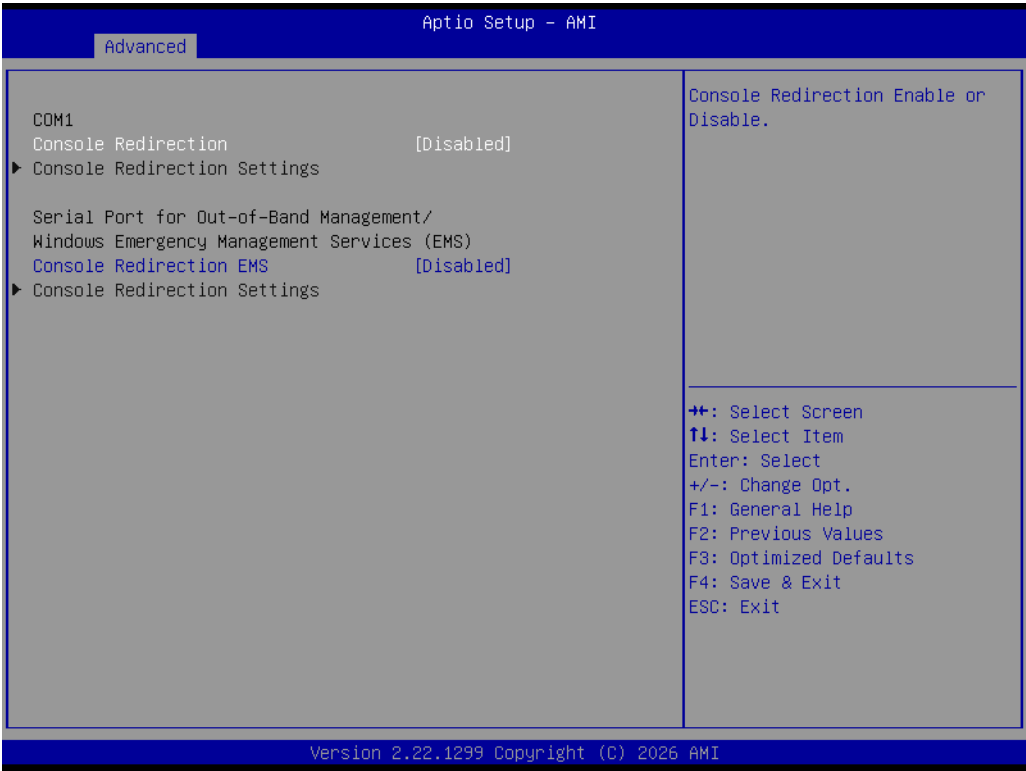
- **GPIO control Enable**
Select to control GPIO by EC or user override during the POST stage.

3.2.2.11 S5 RTC Wake Setting

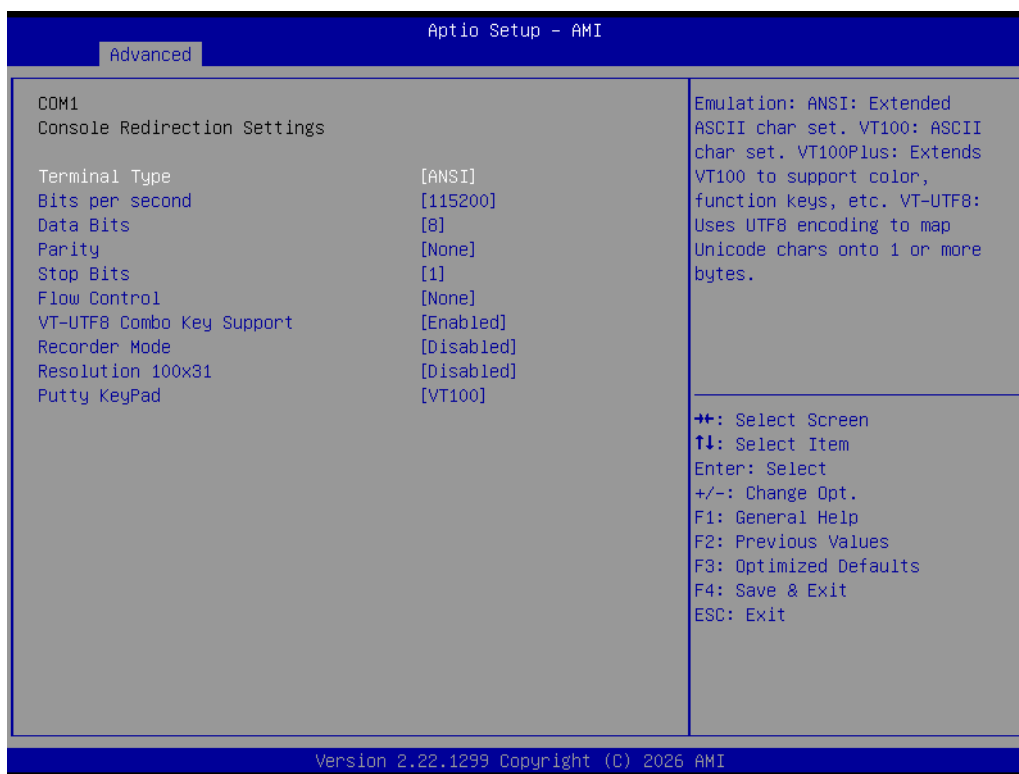


- **Wake system from S5**
Wake system from S5

3.2.2.12 Serial Port Console Redirection



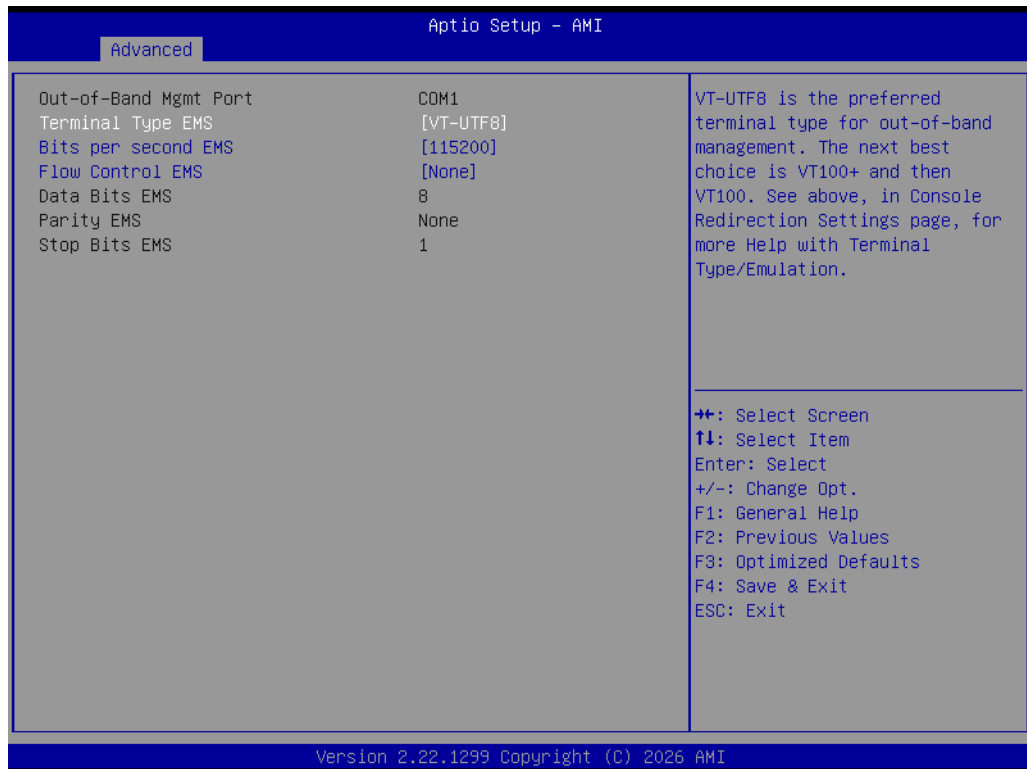
Console Redirection Settings



- **Terminal Type**
Emulation: ANSI: Extended ASCII char set. VT100: ASCII char set. VT100Plus: Extends VT100 to support color, function keys, etc. VT-UTF8: Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
- **Bits per second**
Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
- **Data Bits**
Specifies the number of data bits.
- **Parity**
A parity bit can be transmitted with the data bits to detect certain transmission errors. Even: The parity bit is 0 if the number of 1s in the data bits is even. Odd: The parity bit is 1 if the number of 1s in the data bits is odd. Mark: The parity bit is always 1. Space: The parity bit is always 0. Mark and Space parity do not provide error detection and can be used as an additional data bit.
- **Stop Bits**
Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Communication with slow devices may require more than 1 stop bit.
- **Flow Control**
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.
- **VT-UTF8 Combo Key Support**
Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
- **Recorder Mode**
When enabled, only text is sent. Use this mode to capture terminal data.

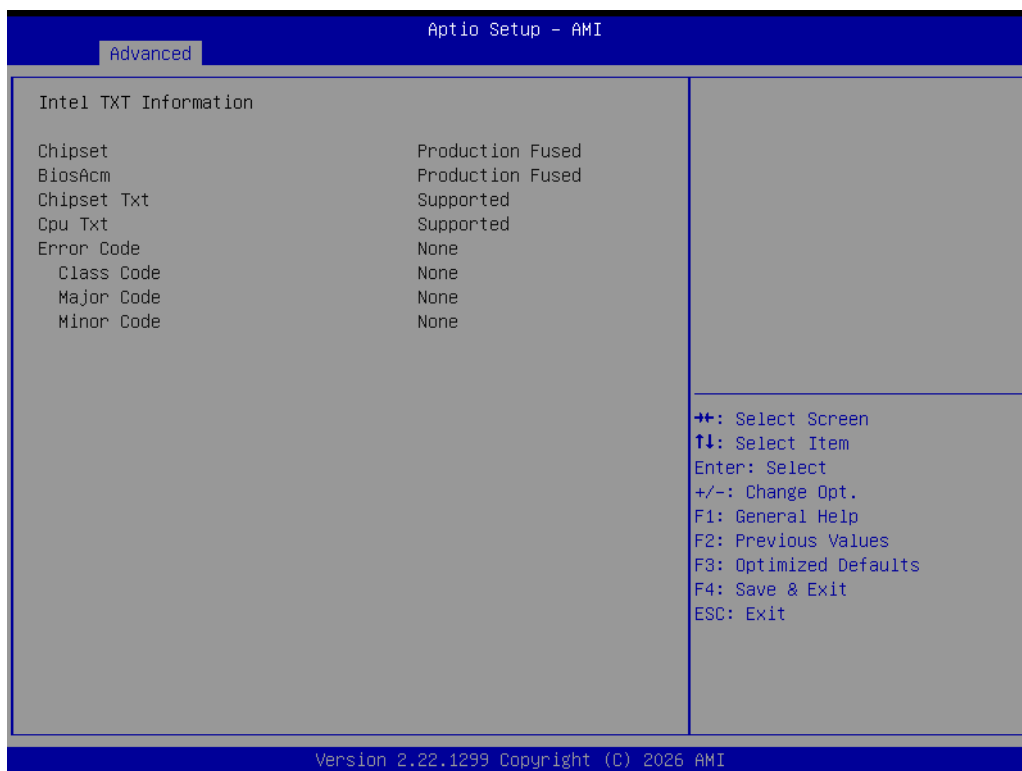
- **Resolution 100x31**
Enables/Disables extended terminal resolution.
- **Putty Keypad**
Select FunctionKey and KeyPad on Putty.

Console Redirection EMS

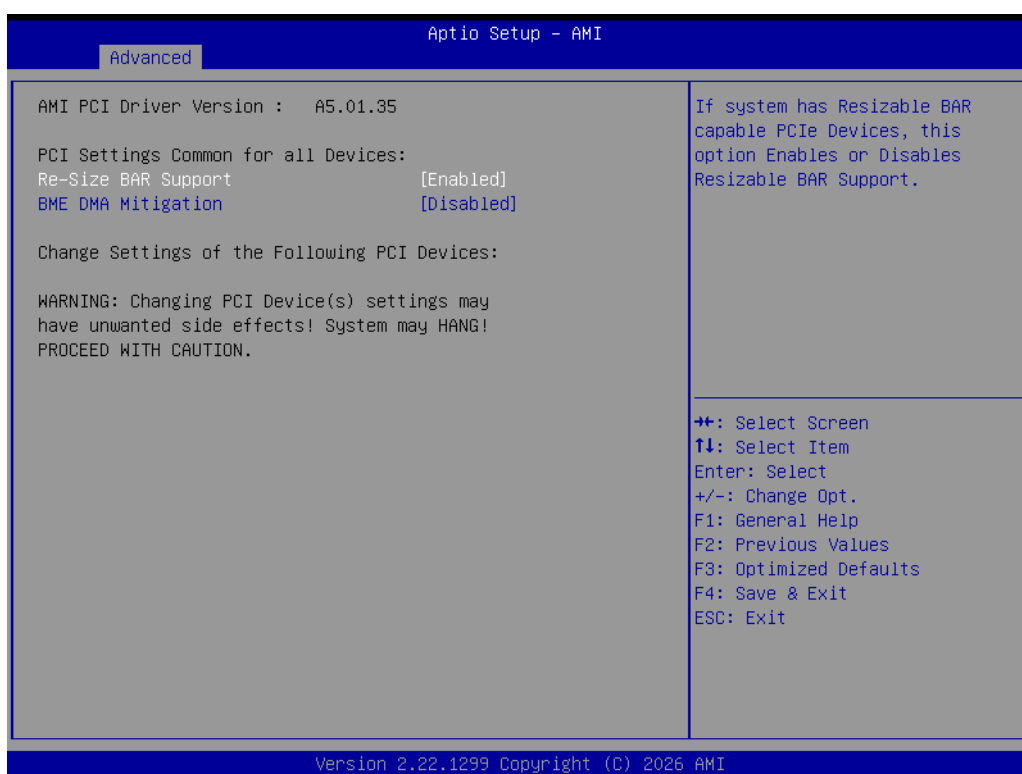


- **Terminal Type EMS**
VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+, followed by VT100. See the Console Redirection Settings page above for more information about Terminal Type/Emulation.
- **Bits per second EMS**
Specifies the baud rate for EMS serial port console redirection.
- **Flow Control EMS**
Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a 'stop' signal can be sent to stop the data flow. Once the buffers are empty, a 'start' signal can be sent to re-start the flow. Hardware flow control uses two wires to send start/stop signals.

3.2.2.13 Intel TXT Information

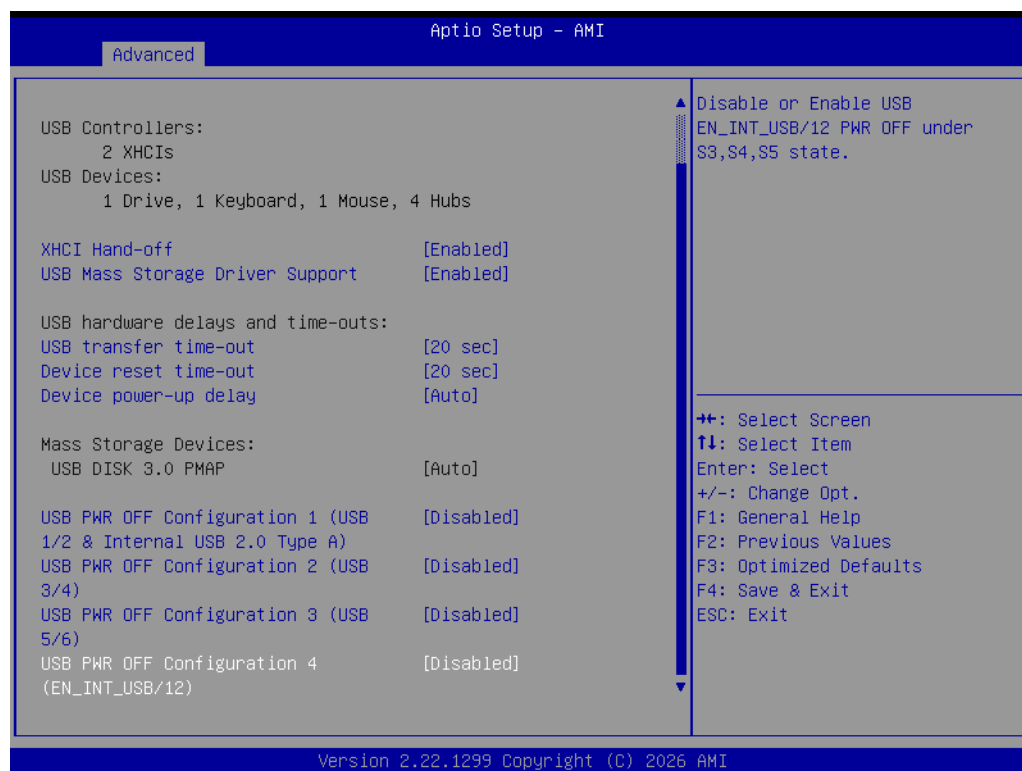
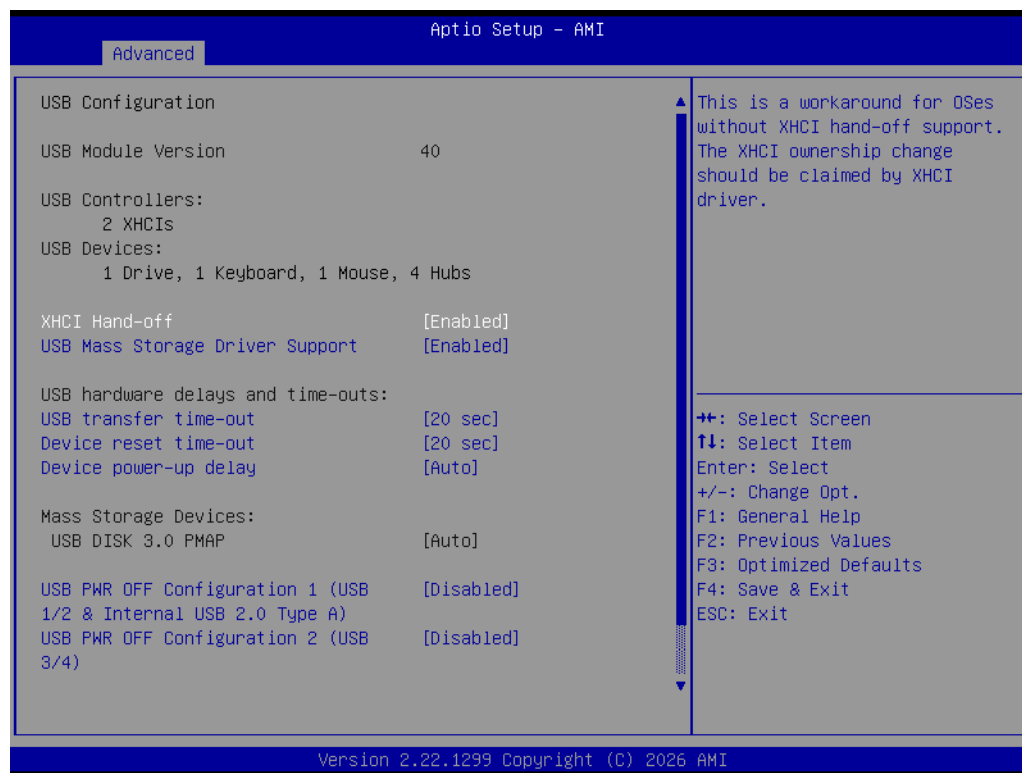


3.2.2.14 PCI Subsystem Settings



- **Re-Size BAR support**
If the system includes PCIe devices that support Resizable BAR, this option enables or disables Resizable BAR support.
- **BME DMA Mitigation**
Re-enables the Bus Master Enable (BME) attribute for PCI bridges after SMM lock.

3.2.2.15 USB Configuration



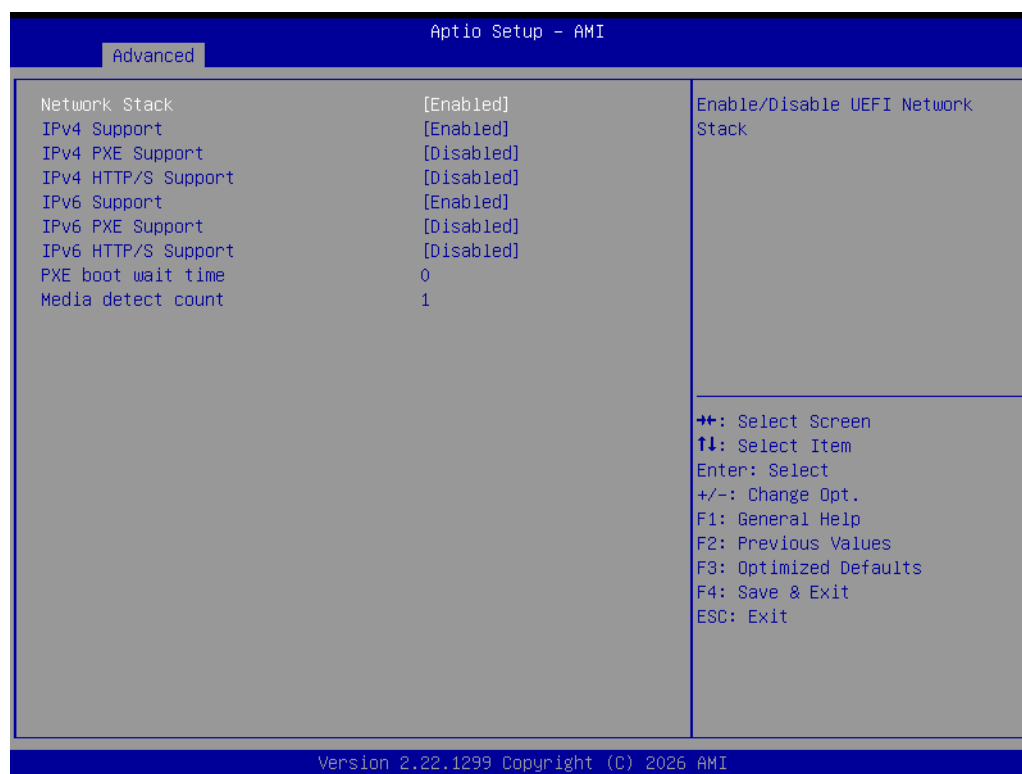
- **XHCI Hand-off**
This is a workaround for OS without XHCI hand-off support.
- **USB Mass Storage Driver Support**
Configure the USB Mass Storage Devices.
- **USB transfer time-out**
The time-out value for Control, Bulk, and Interrupt transfers. USB Mass Storage Driver Support

- **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.
- **USB PWR OFF Configuration**
Enables/Disables USB Power.

3.2.2.16 Network Stack Configuration

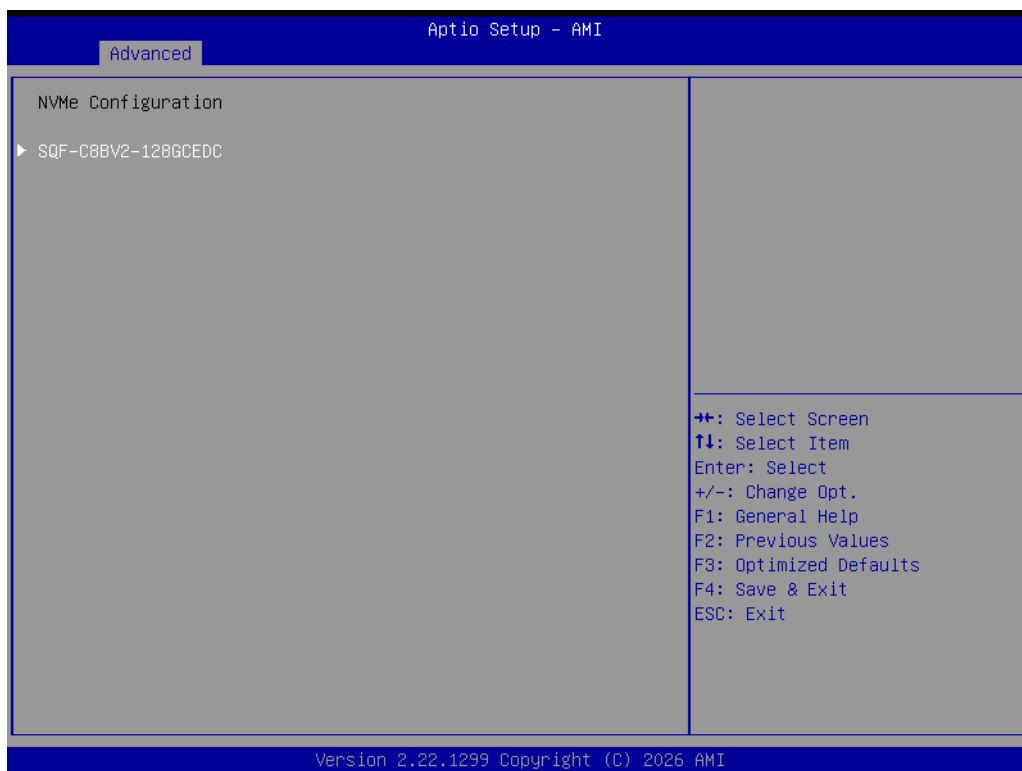


- **Network Stack**
Enables/Disables UEFI Network Stack.



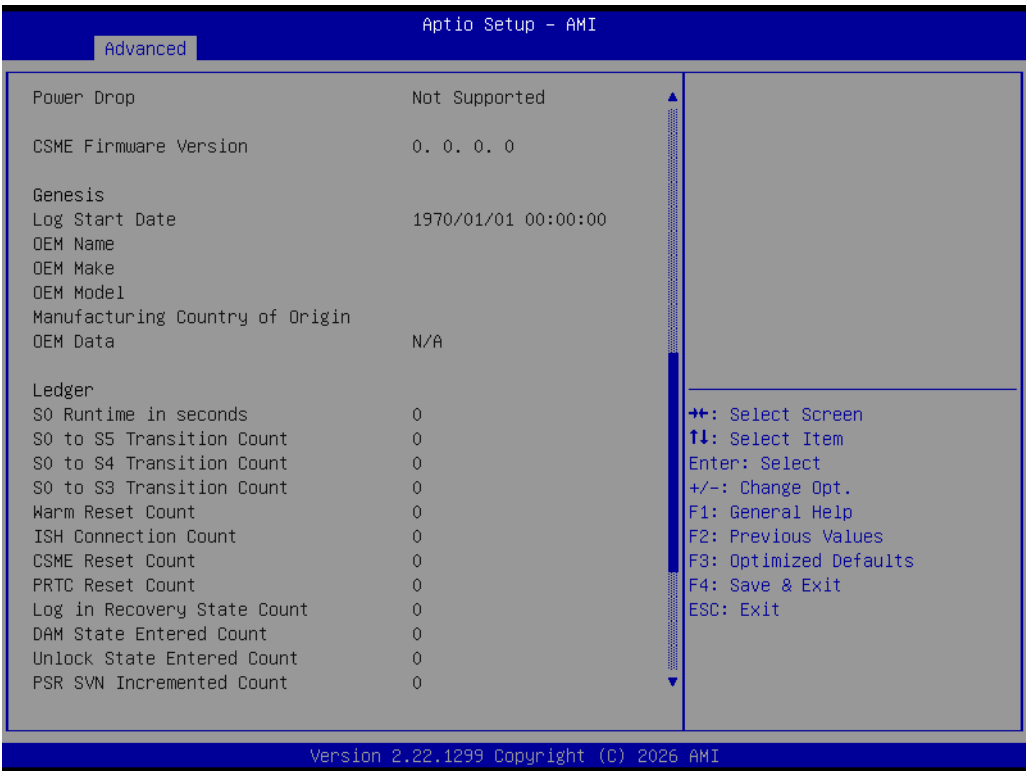
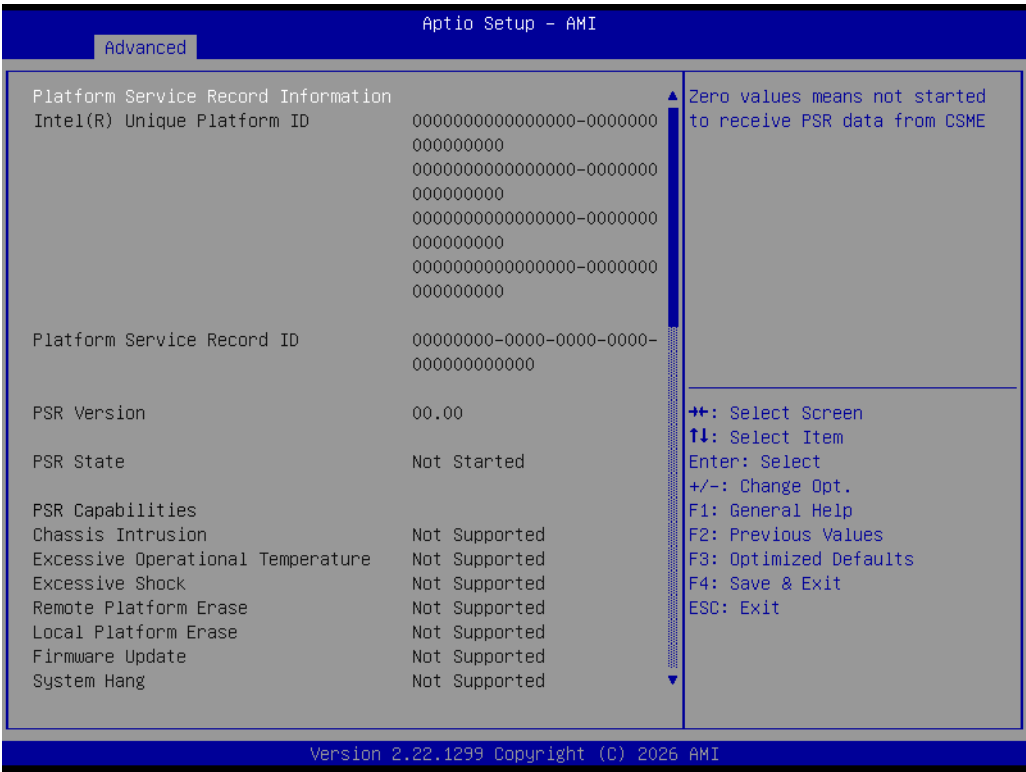
- **IPv4 Support**
Enables/Disables IPv4 support. If disabled, IPv4 support will not be available.
- **IPv4 PXE Support**
Enables/Disables IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.
- **IPv4 HTTP/S Support**
Enables/Disables IPv4 HTTP/HTTPS boot support. If disabled,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

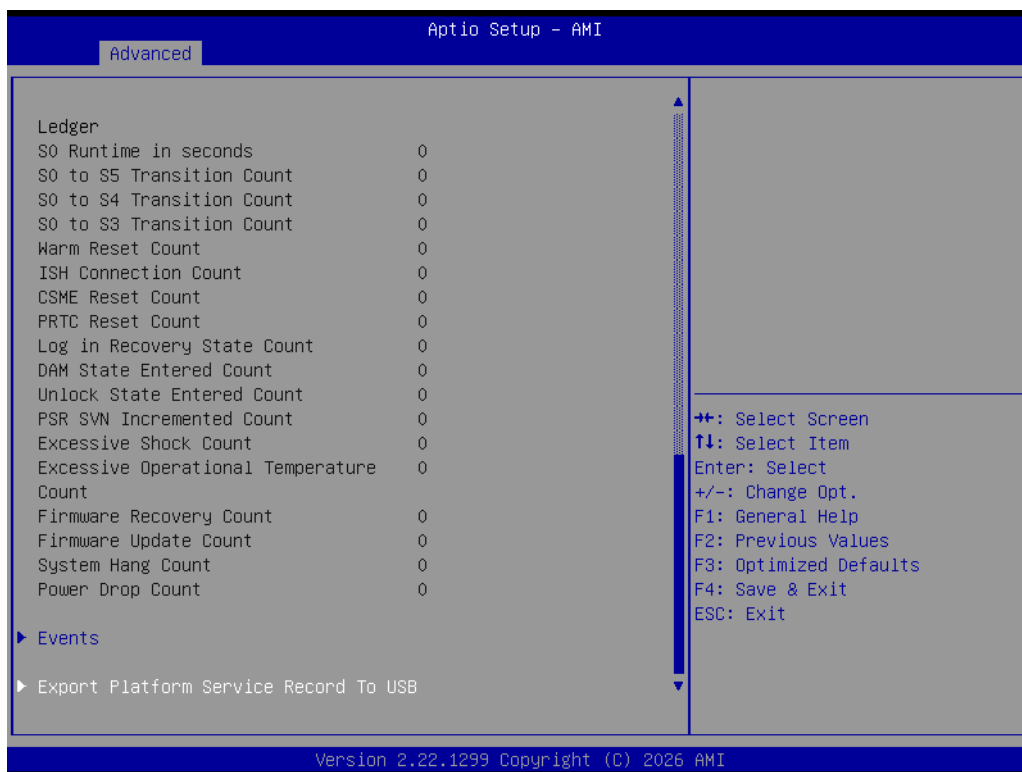
3.2.2.17 NVMe Configuration

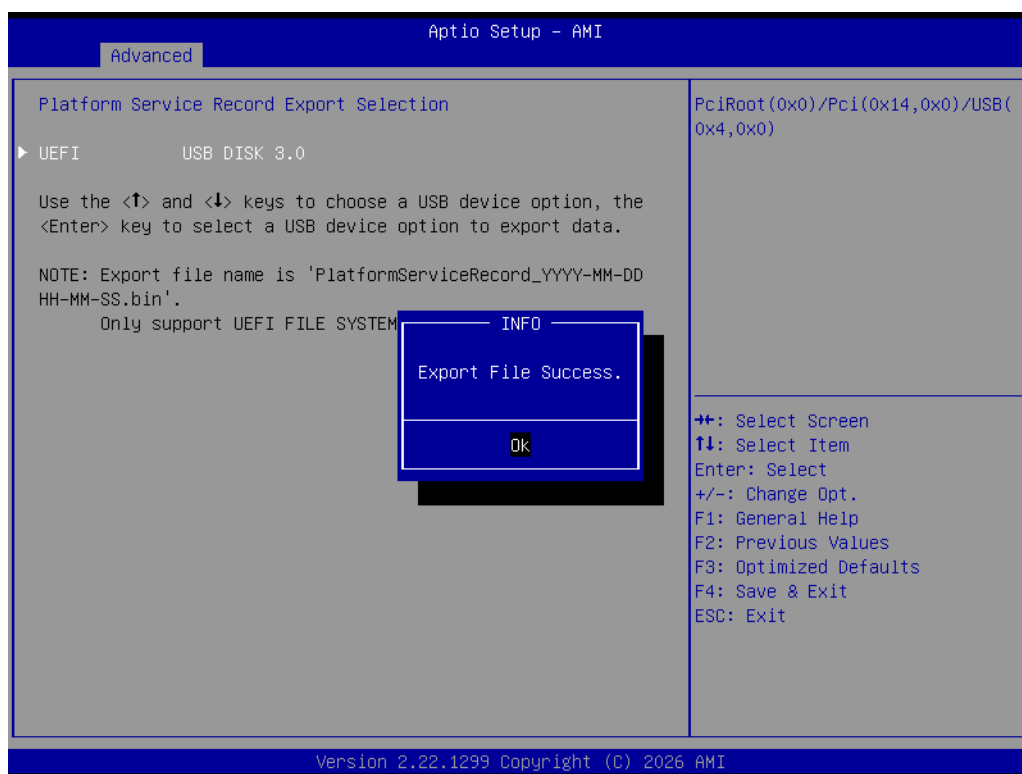
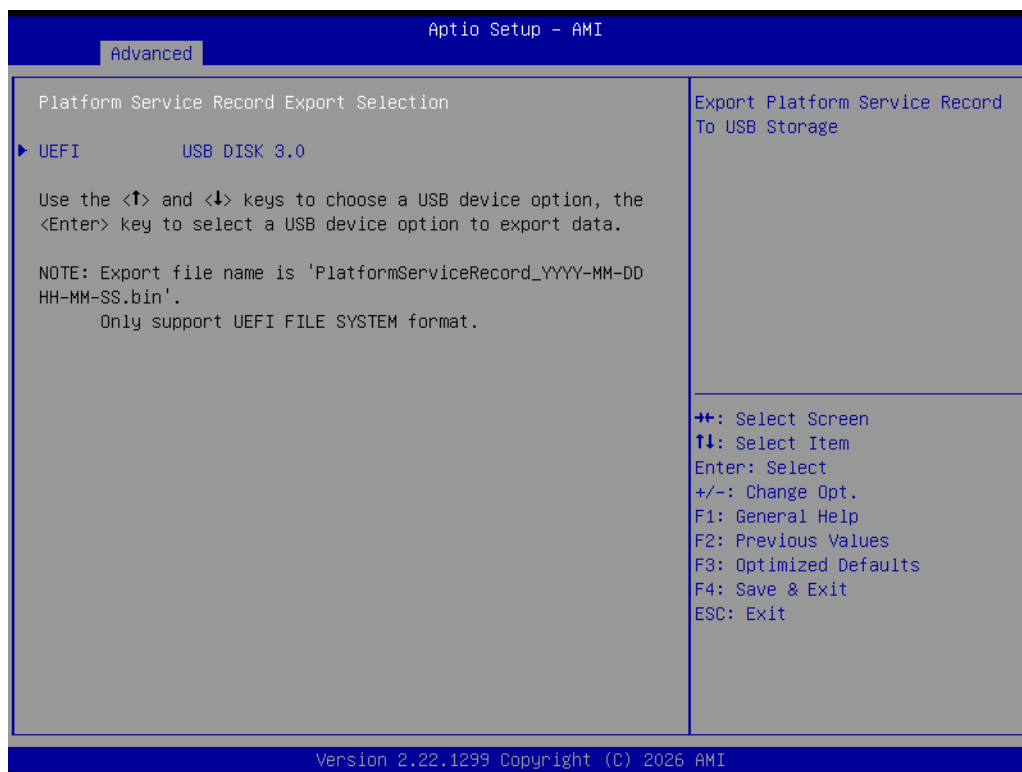


- **Self Test Option**
Select either Short or Extended Self Test. Short option will take couple of minutes and extended option will take several minutes to complete.
- **Self Test Action Run Device Self Test**
Select either to test Contoller alone or Controller and NameSpace. Selecting Controller and NameSpace option will take lot longer to complete the test.

3.2.2.18 NVMe Configuration







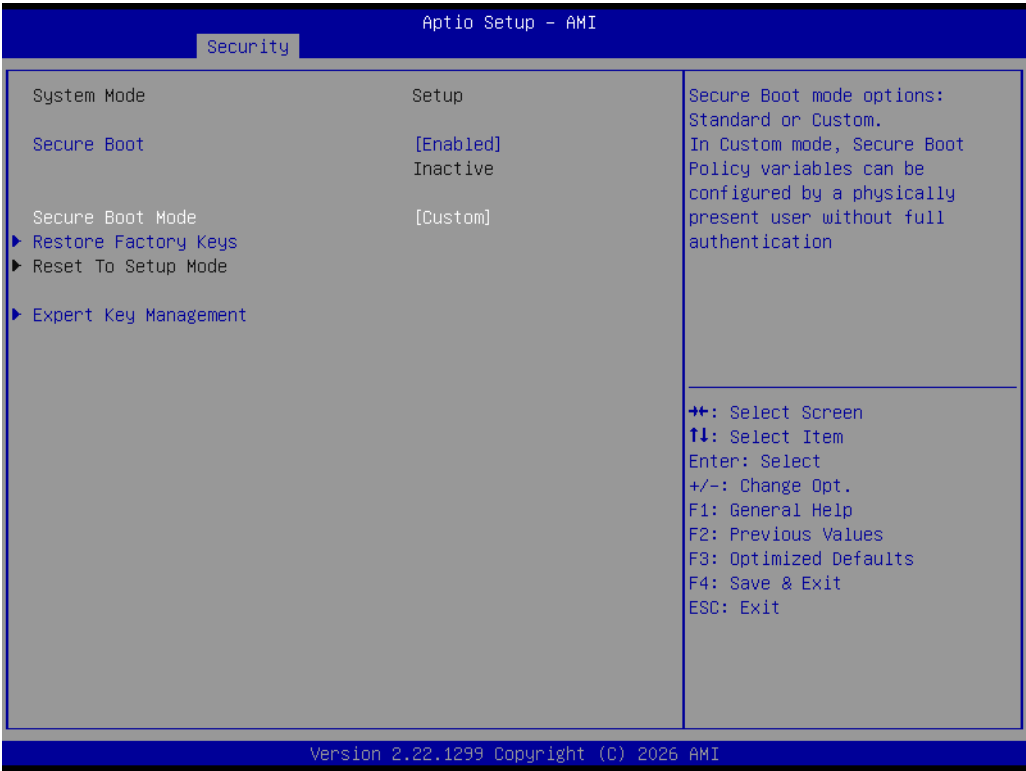
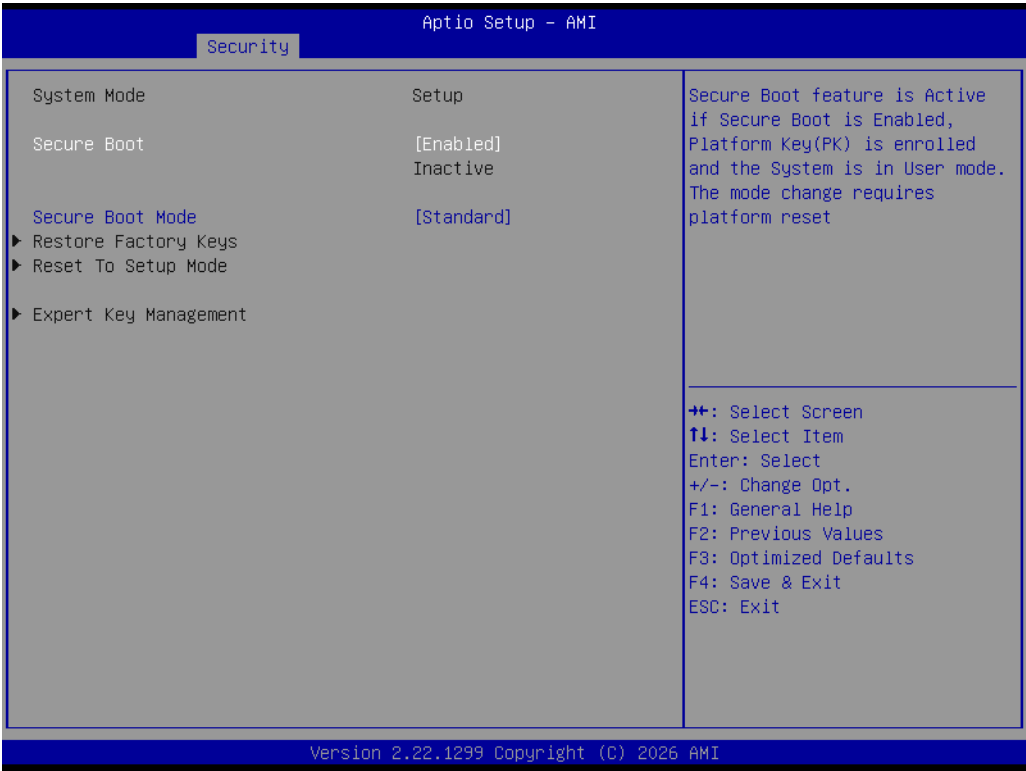
3.2.3 Security

Select Security Setup from the ARK-2252 Setup main BIOS setup menu. All Security Setup options, such as password protection and virus protection are described in this section. To access the sub menu for the following items, select the item and press <Enter>:



- **Administrator Password**
Set Administrator Password.
- **User Password**
Set User Password.

3.2.3.1 Security Boot



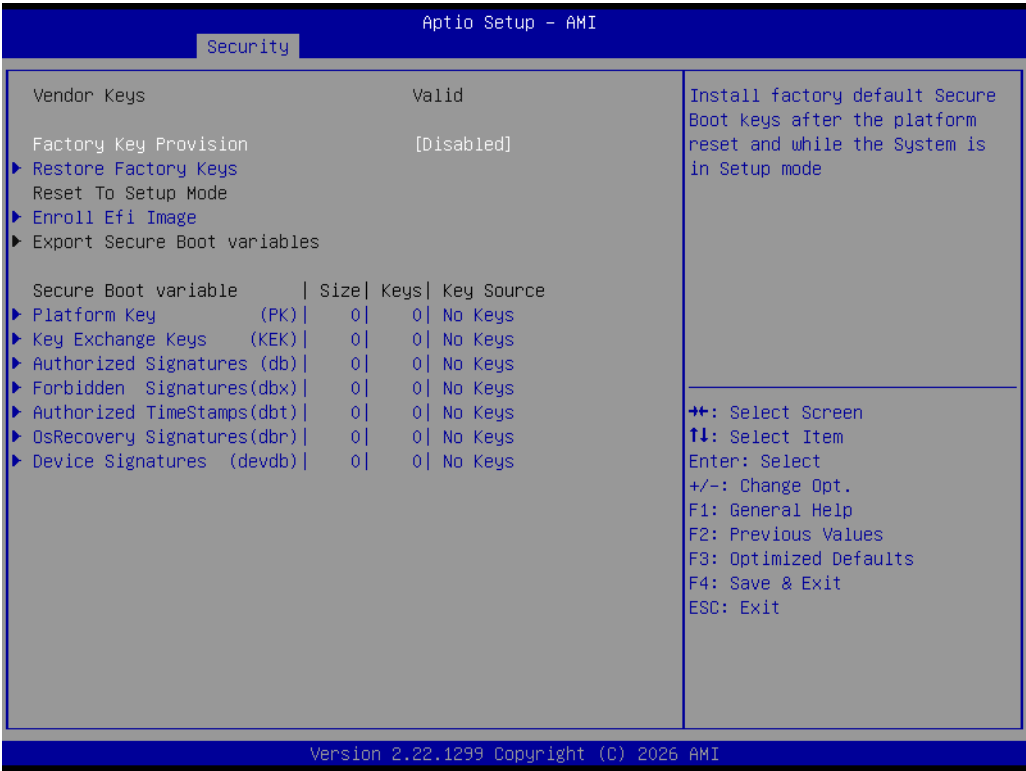
- **Secure Boot**
The Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled, and the System is in User mode. The mode change requires a platform reset.
- **Secure Boot Mode**
Secure Boot mode options: Standard or Custom.

- **Restore Factory Keys**
Forces the system into User Mode and installs the factory default Secure Boot key databases.
- **Expert Key Management**
Enables expert users to modify Secure Boot Policy variables without variable authentication.

Restore Factory Keys

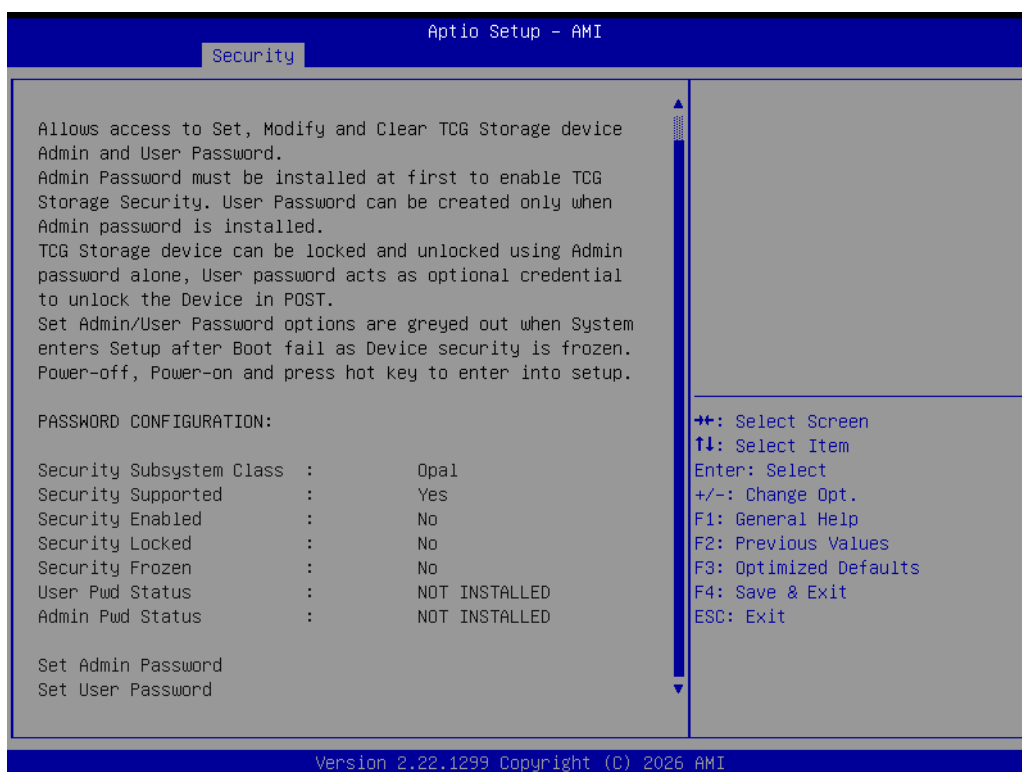
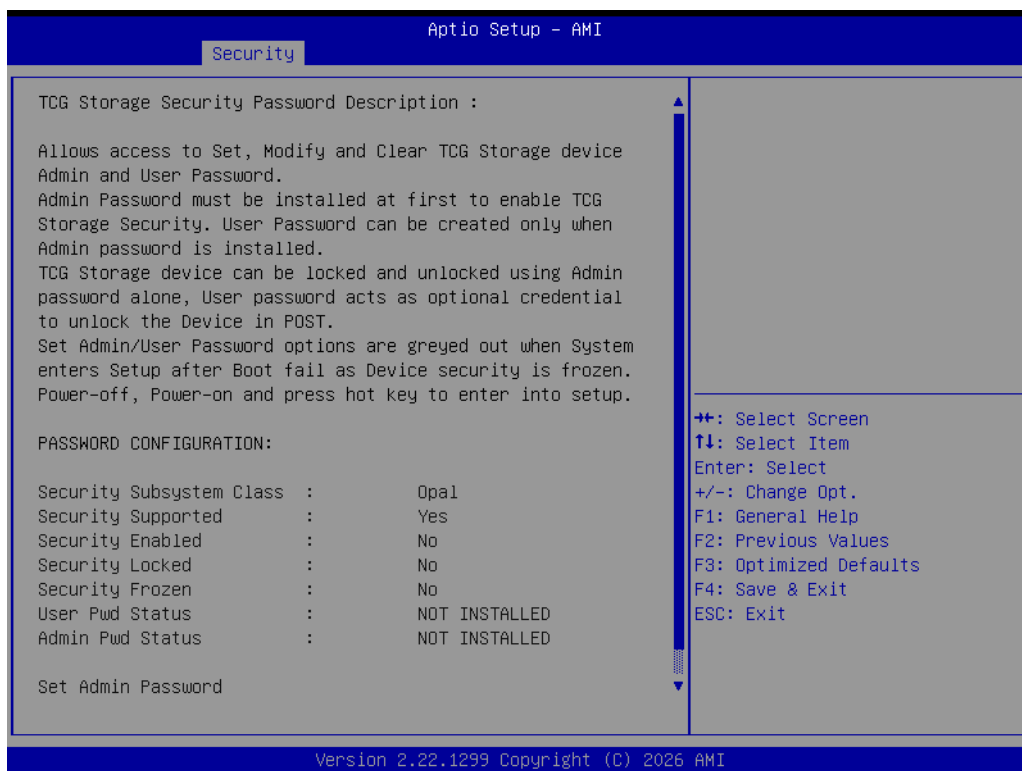


Expert Key Management



- **Factory Key Provision**
Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.
- **Restore Factory Keys**
Force System to User Mode.\nInstall factory default Secure Boot key data-bases.
- **Enroll EFI Image**
Allows an EFI image to run in secure boot mode. Enrolls the SHA-256 hash certificate of a PE image into the Authorized Signature Database (db).
- **Platform Key**
PK Key.
- **Key Exchange Keys**
KEK Key.
- **Authorizes Signatures**
db Key.
- **Forbidden Signatures**
dbx Key.
- **Authorizes TimeStamps**
dbt key.
- **OsRecovery Signatures**
dbr key.
- **Device Signatures**
devdb key.

3.2.3.2 SSD information

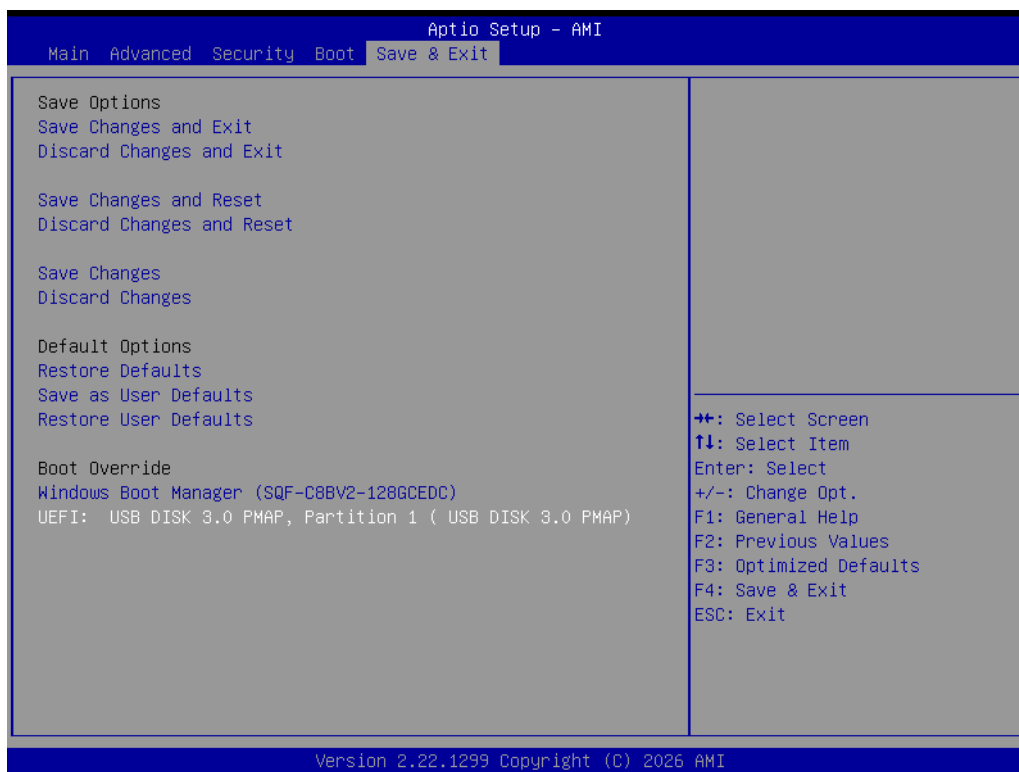


3.2.4 Boot



- **Setup Prompt Timeout**
Number of seconds that the firmware will wait before initiating the original default boot selection. A value of 0 indicates that the default boot selection is to be initiated immediately on boot. A value of 65535(0xFFFF) indicates that firmware will wait for user input before booting. This means the default boot selection is not automatically started by the firmware.
- **Bootup NumLock State**
Select the keyboard NumLock state.
- **Quiet Boot**
Enables/Disables Quiet Boot option.
- **Boot Option**
Sets the system boot order.

3.2.5 Save & Exit



- **Save Changes and Exit**
This item allows you to exit system setup after saving the changes.
- **Discard Changes and Exit**
This item allows you to exit system setup without saving any changes.
- **Save Changes and Reset**
This item allows you to reset the system after saving the changes.
- **Discard Changes and Reset**
This item allows you to reset system setup without saving any changes.
- **Save Changes**
This item allows you to save changes done so far to any of the options.
- **Discard Changes**
This item allows you to discard changes done so far to any of the options.
- **Restore Defaults**
This item allows you to restore/load default values for all the options.
- **Save as User Defaults**
This item allows you to save the changes done so far as user defaults.
- **Restore User Defaults**
This item allows you to restore the user defaults to all the options.
- **Boot Override**
Boot device select can override your boot priority.



Enabling an Intelligent Planet

www.advantech.com

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

All product specifications are subject to change without notice.

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

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

© Advantech Co., Ltd. 2026