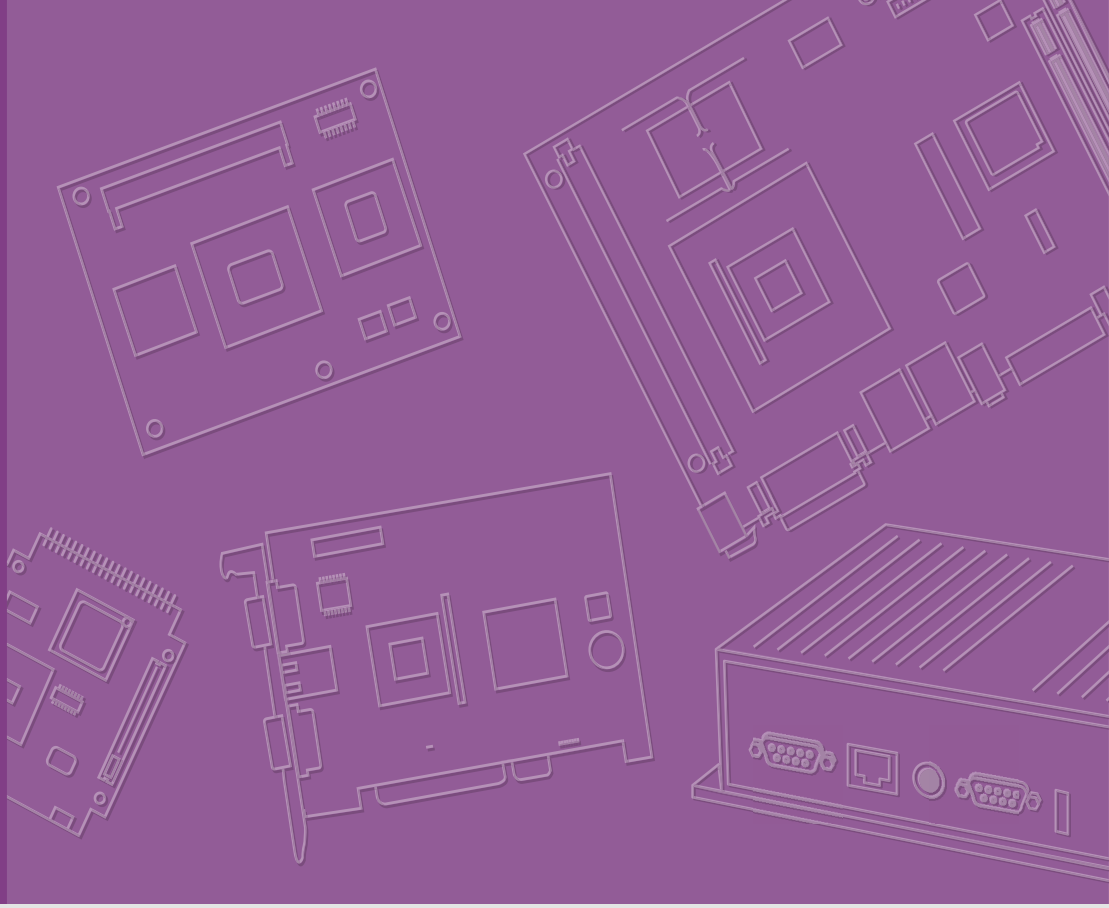


User Manual

ARK-1251

Fanless Embedded Box PC

ADVANTECH

Enabling an Intelligent Planet

Attention!

Please note this package contains a hard-copy user manual in Chinese for China CCC certification purposes. Please disregard the Chinese hard-copy user manual if the product is not to be sold and/or installed in China.

Attention!

Veuillez noter que ce paquet contient un manuel d'utilisation papier en chinois à des fins de certification China CCC. Veuillez ne pas tenir compte du manuel d'utilisation chinois sur papier si le produit ne doit pas être vendu et/ou installé en Chine.

Copyright

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 Semiconductor 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: http://support.advantech.com.tw/support

Part No. 2006125100 Edition 1

Printed in China January 2025

Product Warranty (2 Years)

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

This warranty does not apply to any products that have been repaired or altered by persons other than repair personnel authorized by Advantech, or products that have been subject to misuse, abuse, accident, or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced free of charge during the warranty period. For out-of-warranty repairs, customers will be billed according to the cost of replacement materials, service time, and freight. Please consult your dealer for more details.

If you believe your product to be defective, follow the steps outlined below.

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

Declaration of Conformity

FCC Class B

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

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

Technical Support and Assistance

1. Visit the Advantech website at http://support.advantech.com where you can find the latest information about the product.
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 that 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 loss.

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

Note! Notes provide additional, optional information.

Les remarques fournissent des informations supplémentaires facultatives.

Packing List

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

- 1 x ARK-1251 Unit
- 1 x User Manual (Simplified Chinese)
- 1 x Wrench for top cover
- 1 x 4-pin terminal block for switch
- 1 x 3-pin plug-in block for power in
- 1 x DIN-rail bracket
- 1 x WISE-PaaS/DeviceOn Quick Start Guide
- 1 x M.2 PCIe 2280 SSD thermal kit
- 1 x RAM thermal pad 59x13x1.0mm
- 1 x RAM thermal pad 59x23x1.5mm
- 1 x CPU thermal pad 25x20x0.21mm

Ordering Information

Model Number	Description
ARK-1251-S3A1	Intel Core Ultra 5-125U HDMI+DP+3*GbE+4*COM
ARK-1251-S3A1U	Intel Core Ultra 5-125U HDMI+DP+3*GbE+4*COM MIT
ARK-1251-S7A1	Intel Core Ultra 7-155U HDMI+DP+3*GbE+4*COM
ARK-1251-S7A1U	Intel Core Ultra 7-155U HDMI+DP+3*GbE+4*COM MIT

Optional Items for Default SKU

Part Number	Description
96PSA-A120W24T2-4	AC to DC adapter, 24V/120W
1702002600	Power cable 3-pin 183cm, USA type
11702002605	Power cable 3-pin 183cm, EU type
1702031801	Power cable 3-pin 183cm, UK type
1700000237	Power cable 3-pin 183cm, PSE type
1700030518-01	CANBus Cable (replacing GPIO)
1960103315N010	M.2 3052 Extend Bracket
AMK-W006	Wall mount kit
AMK-V023E	VESA mount kit

Safety Instructions

1. Read these safety instructions carefully.
2. Retain this user manual for future reference.

3. Disconnect the equipment from all power outlets before cleaning. Use only a damp cloth for cleaning. Do not use liquid or spray detergents.
4. For pluggable equipment, the power outlet socket must be located near the equipment and easily accessible.
5. Protect the equipment from humidity.
6. Place the equipment on a reliable surface during installation. Dropping or letting the equipment fall may cause damage.
7. Ensure that the voltage of the power source is correct before connecting the equipment to a power outlet.
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 it from the power source to avoid damage from transient overvoltage.
11. Never pour liquid into an opening. This may cause fire or electrical shock.
12. Never open the equipment. For safety reasons, the equipment should be opened only by qualified service personnel.
13. If any of the following occurs, have the equipment checked by service personnel:
    - The power cord or plug is damaged.
    - Liquid has penetrated the equipment.
    - The equipment has been exposed to moisture.
    - The equipment is malfunctioning, or does not operate according to the user manual.
    - The equipment has been dropped and damaged.
    - The equipment shows obvious signs of breakage.
14. 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 damage the components. The equipment should be kept in a controlled environment.
15. CAUTION: Batteries are at risk of exploding if incorrectly replaced. Replace only with the same or equivalent type as recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.
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 the 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 con- tained herein.
21. Use a power cord connected to a socket-outlet with a grounded connection.
22. This product is intended to be supplied by a UL-Listed power supply suitable for use at minimum Tma 60°C (140°F) whose output is rated at 24V, 5A. Please contact Advantech for further information

23. **RESTRICTED ACCESS AREA**: The equipment should only be installed in a Restricted Access Area.

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. Assurez-vous que la tension de la source d'alimentation est correcte avant de connecter l'équipement à la prise de courant.
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'appareilest 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. Au moyen d'un cordon d'alimentation connecté à une prise de courant avec mise à la terre.
21. Ce produit est destiné à être alimenté par une alimentation homologuée UL adaptée à une utilisation à une température minimale de Tma de 60°C (140°F) dont la sortie est nominale de 24V, 5A. Veuillez contacter Advantech pour plus d'informations.
22. ZONE D'ACCÈS RESTREINT: L'équipement ne doit être installé que dans une zone d'accès restreint.

Contents

Chapter 1

General Information

This chapter details background information on the ARK-1251 series.

1.1 Introduction

ARK-1251 is a compact and multifunctional fanless embedded system which powers by Intel® Core™ Ultra Processor 125U and 155U, which combine CPU, GPU, and NCU as performance hybrid SoC to offer high performance in low-power processing. ARK-1251 also offers sufficient I/O ports for different applications, targeted in market like Machine Automation, AI Inspection, Cobots/AMR and Edge Computing.

Rugged, Compact Design

ARK-1251 is equipped with dual channel memory slot, and supports up to 96GB of DDR5 5600 MHz SO-DIMM. The compact design is suitable for installation in environments with limited space, and this ruggedized system also designed for operation in harsh industrial environments for equipped with a wide operating temperature range (-20 ~ 60°C/-4 ~ 140°F), wide input power range (12 ~ 28 VDC) and multiple IO solution. It includes 4x USB 2.0, 2x USB 3.2 (Gen2), 2x full COM (RS-232/422/485), 2x COM (RS-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, 1x HDMI, and 1x DP. ARK-1251 also features 1x M.2 2280 M key, 1x M.2 2230 E-Key, and 1x M.2 2280 B-Key. ARK-1251 passes worldwide certification including CE, FCC Class B, CB, UL, CCC, BSMI, and UKCA.

Multiple Display Support

In ARK-1251, system offers 1x 8K HDMI displays, which support up to 7680 x 4320 @60Hz, and 1x 8K DP, which support up to 7680 x 4320 @60Hz. The graphic engine is Intel® Graphics.

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

The Advantech SUSI API is an intelligent self-management cross-platform tool that monitors the system's status for problems and take action in the event of abnormalities, and provides a valuable suite of programmable APIs such as multi-level watchdog, hardware monitoring, and other user-friendly interfaces. SUSI API makes the entire system more reliable and intelligent. ARK-1251 also supports Advantech's own WISE-DeviceOn solution either in-band or out-of-band. DeviceOn provides easy remote management so users can monitor, configure, and control a large number of terminals to ensure easy maintenance and recovery.

1.2 Product Features

1.2.1 Processor System

- **CPU:**
  - Core Ultra 5-125U
  - Core Ultra 7-155U
- **Frequency:**
  - Core Ultra 5-125U: 1.3Ghz
  - Core Ultra 7-155U: 1.7Ghz
- **Core Number:**
  - Core Ultra 5-125U: 12
  - Core Ultra 7-155U: 12
- **BIOS:** AMI EFI 256 Mbit

1.2.2 Memory

- **Technology:** DDR5 5600MHz
- **Max capacity:** Up to 96GB
- **Socket:** 2 x Channel DDR5 5600 MHz 262-pin SO-DIMM (no support ECC)

1.2.3 Graphic

- **Chipset:** Intel® Graphics
- **HDMI 2.1:** Up to 4096 x 2160 @ 60Hz
- **DP:** Up to 4096 x 2160 @ 60Hz
- **Dual Display:** HDMI + DP

1.2.4 Ethernet

- **LAN1:** 10/100/1000/2500 Mbps Intel i226-LM GbE, support Wake On LAN
- **LAN2:** 10/100/1000/2500 Mbps Intel i226-LM GbE, support Wake On LAN
- **LAN3:** 10/100/1000 Mbps Intel i210 GbE, support Wake On LAN

1.2.5 Audio

- **Interface:** Realtek ALC888S, Mic-in and Line-out

1.2.6 I/O Interface

- **Serial Ports:**
  - 2 x RS-232/422/485, with auto flow control
  - 2 x RS-422/485, with auto flow control
- **USB Ports:** 2 x USB 3.2 Gen 2, 4 x USB 2.0.
- **GPIO:** 8-bit Programmable DIO
- **Optional CAN Bus:** 1 x CAN Bus 2.0 (DB9 connector, replacing GPIO)

1.2.7 Expansion

- **M.2:**
  - 1x M.2 2230 E key (NVMe, PCIe x2)
  - 1x M.2 2280 B key with nano SIM holder (NVMe, PCIe x2, SATA)
  - 1x M.2 2280 M key (NVMe, PCIe x4)

1.2.8 Storage

- **NVMe/SATA:**
  - 1x M.2 2280 M key (NVMe, PCIe x4) (default)
  - 1x M.2 2280 B key with nano SIM holder (NVMe, PCIe x2 / SATA)

1.2.9 Other

- **TPM:** NPCT764AABYX FW7.2.3.1
- **Watchdog Timer:** 255 levels timer interval, setup by software

1.2.10 Software Support

- **Microsoft Windows:** Windows 10 Enterprise, Windows 11 Enterprise
- **Linux:** Ubuntu 24.04

1.2.11 Power Requirement

- **Power Type:** ATX/AT
- **Power Input Voltage:** 12 ~ 28 V_{DC}
- **Power Adapter:** AC to DC, 120W adapter

1.2.12 Power Consumption

- **Core Ultra 5-125U**
  - Typical: 17.83W
  - Max: 59.44W
- **Core Ultra 7-155U**
  - Typical: 18.19W
  - Max: 61.74W

1.2.13 Mechanical

- **Construction:** Aluminum housing
- **Mounting:** DIN-Rail/Wall Mount
- **Dimensions (W x H x D):** 173 x 60 x 141 mm (6.73 x 2.36 x 5.55 in)
- **Weight:** 1.5 kg

1.2.14 Environment

- **Operating Temperature:** With extended temp. peripherals: -20 ~ 60°C with 0.7m/s airflow (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:** With SSD: 3 Grms, IEC60068-2-64, random, 5~500 Hz, and 1hr/axis (with Wall Mount)
- **Shock During Operation:** With SSD: 30 G, IEC-60068-2-27, half sine, 11 ms duration (with Wall Mount)
- **EMC:** CE/FCC Class B, CCC, UKCA, and BSMI
- **Safety:** UL, CB, CCC, and UKCA

1.3 Mechanical Diagrams

Din Rail: 173 x 60 x 141 mm (6.73 x 2.36 x 5.55 in) (W x H x D)

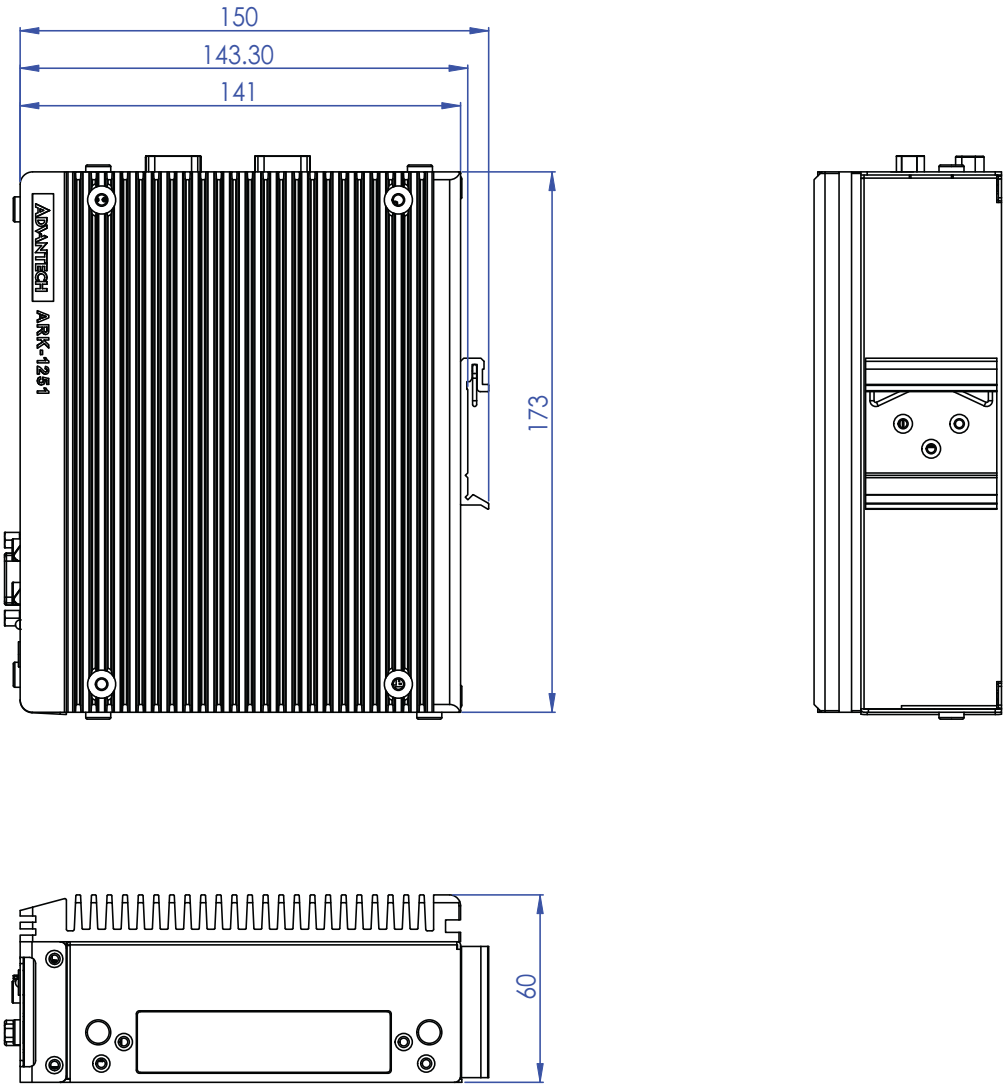


Figure 1.1 ARK-1251 Mechanical Dimensions Diagram

Wall Mount:

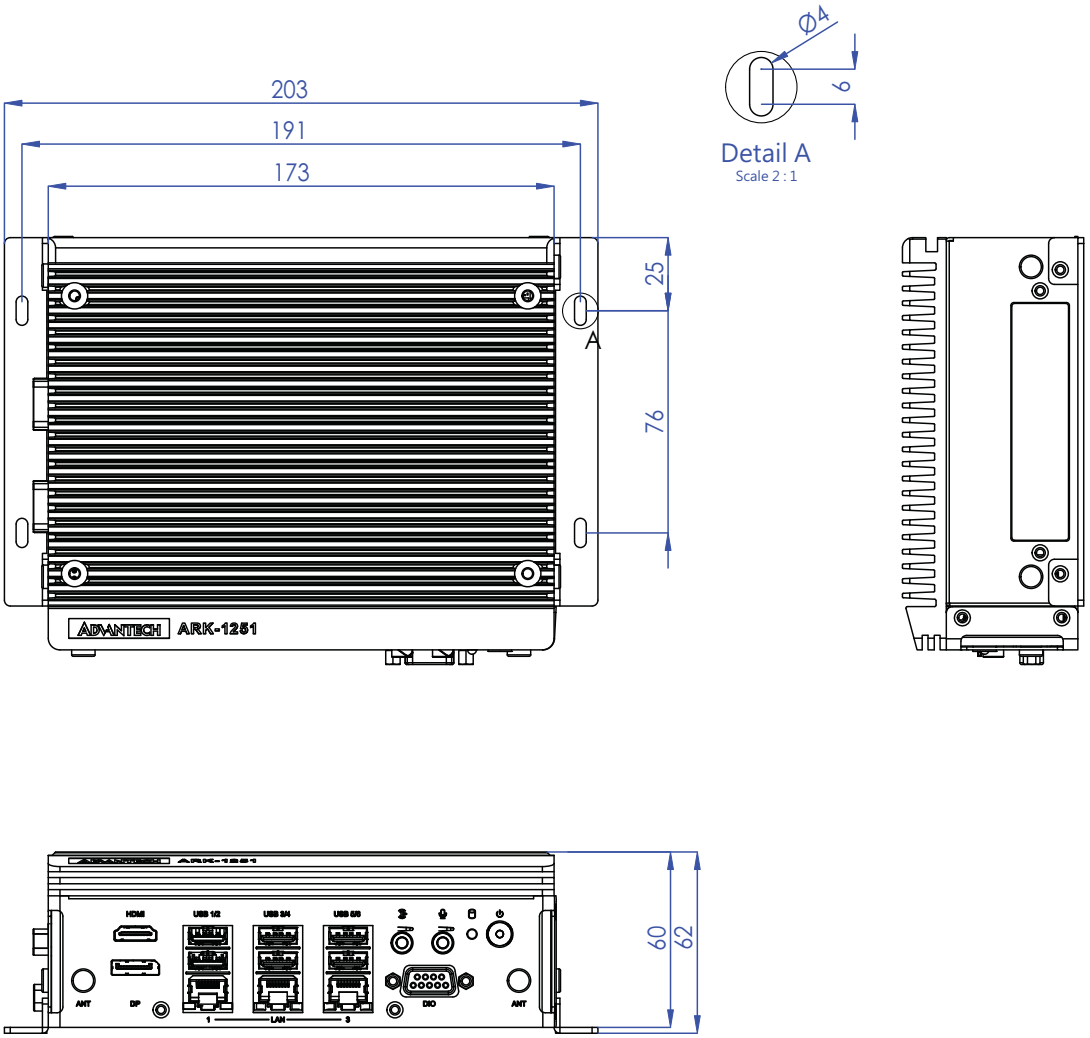


Figure 1.2 ARK-1251 Mechanical Dimensions Diagram With Wall Mount

1.4 Optional MOS Modules for iDoor Expansion

Table 1.1: Optional MOS Modules for iDoor Expansion	
Part-Number	Description
MOS-2120-Z1101E	Giga LAN Ethernet module, 1-Ch, PCIe I/F,
MOS-1130Y-0202	Isolated CANBus, 2-Ch, DB9, PCIe I/F
MOS-1110Y-0101E	Isolated 16 DI/8 DO, 1-Ch, DB37, PCIe I/F
MOS-2120-Z1201	Dual Intel I210 GbE LAN iDoor, 2-Ch, PCIe I/F
MOS-1120Y-0202E	Isolated RS-232, 2-Ports, DB9, PCIe I/F
MOS-1120Y-1402E	Non-Isolated RS-232, 4-Ports, DB37, PCIe I/F
MOS-2110Z-1201E	USB module, 2-Ch, PCIe I/F
AMO-I032	Expansion kit M.2 B key for mPCIe idoor

Note!

1. *You need to order the AMO-I032 together with MOS modules.*
2. *M.2 E Key cannot be used when adding any MOS module due to mechanical interference.*

Chapter 2

Hardware Configuration

This chapter details instructions for installing the ARK-1251 series.

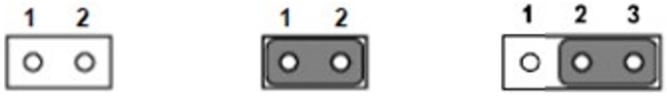
2.1 Introduction

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

2.2 Jumper

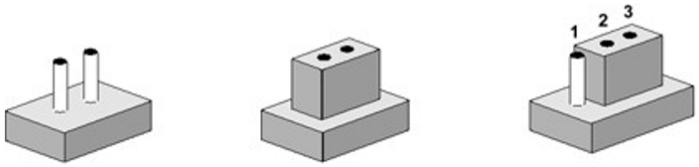
2.2.1 Jumper Description

You may configure ARK-1251 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.



Open Closed Closed 2-3

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



Open Closed Closed 2-3

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/Fail Safe

Table 2.1: Jumper List	
JCMOS1	Clear CMOS
SW4001	HW AT/ATX Mode setting
M2_SEL1	M.2 Key B Device selection
M2_LED_SEL	M.2 SSD LED Selection
SW_422_485_1	RS-485/RS-422 Failsafe
SW_422_485_2	RS-485/RS-422 Failsafe

2.2.3 Jumper Locations

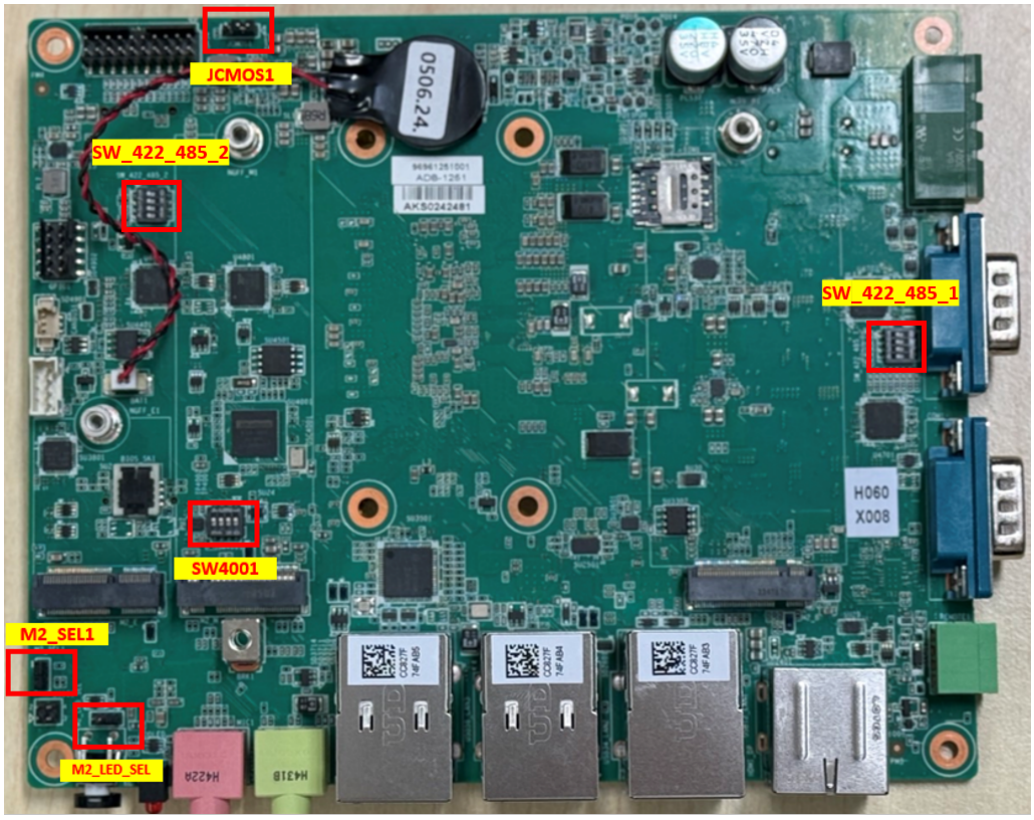


Figure 2.1 ARK-1251 Jumper Location

2.2.4 Jumper Settings

2.2.4.1 Clear CMOS (JCMOS1)

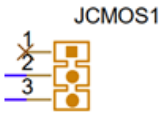


Table 2.2: JCMOS1 Clear CMOS	
Setting	**Function**
(1-2 Closed)	Normal operation (Default)
(2-3 Closed)	Clear CMOS

2.2.4.2 HW AT/ATX Mode DIP Switch (SW4001)

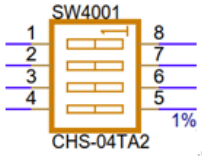


Table 2.3: SW4001 AT/ATX Mode Switch	
Setting	**Function**
(1-8)	Pin 1 represents Off: ATX mode(default), Pin 8 represents On: AT mode

Table 2.3: SW4001 AT/ATX Mode Switch	
(2-7)	Reserved Pin 2 represents Off (default), Pin 7 represents On
(3-6)	Reserved Pin 3 represents Off (default), Pin 6 represents On
(4-5)	Reserved Pin 4 represents Off (default), Pin 5 represents On

2.2.4.3 M.2 Key B Device selection (M2_SEL1)

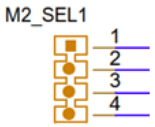


Table 2.4: M2_SEL1 M.2 Key B Device Selection	
Setting	**Function**
(1-2 Closed)	SSD with USB 2.0
(1-2 Open)	SSD with USB 3.0 (for 4G/5G) (default)
(3-4 Closed)	SSD – SATA type (default)
(3-4 Open)	SSD – PCIE type

2.2.4.4 M.2 SSD LED Selection (M2_LED_SEL)

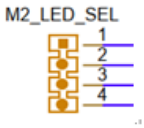


Table 2.5: M2_LED_SEL M.2 SSD LED Mode Jumper	
Setting	**Function**
(1-2 Closed)	Key B SSD LED
(3-4 Closed)	Key M SSD LED (default)

2.2.4.5 RS-422/RS-485 Failsafe (SW_422_485_1)

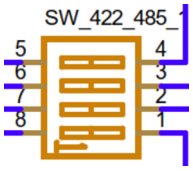


Table 2.6: SW_422_485_1 RS-485/RS-422 Failsafe	
Setting	**Function**
(1-8), (2-7)	Pin 1/2 represents Off: Disable COM2 failsafe (default), Pin 7/8 represents On: Enable COM2 failsafe
(3-6), (4-5)	Pin 3/4 represents Off: Disable COM1 failsafe (default), Pin 5/6 represents On: Enable COM1 failsafe

2.2.4.6 RS-422/RS-485 Failsafe (SW_422_485_2)

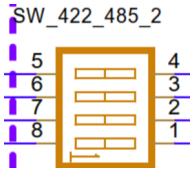
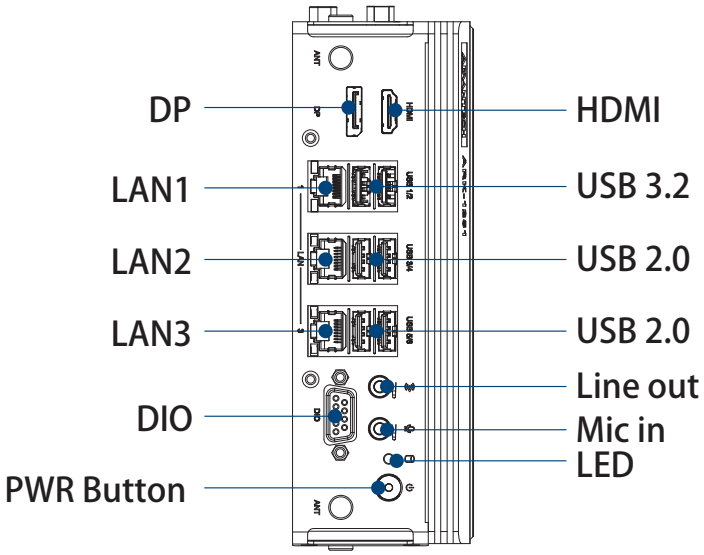
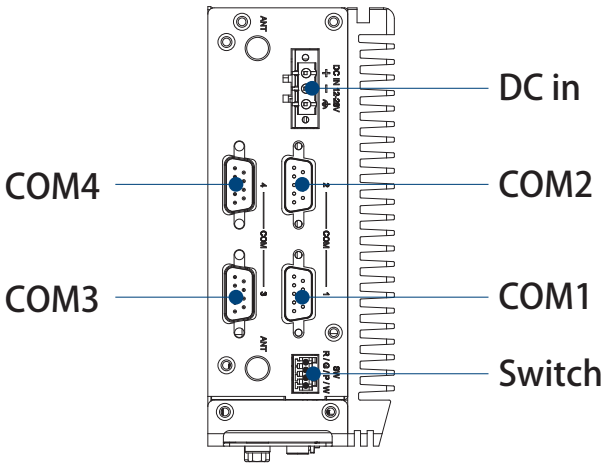


Table 2.7: SW_422_485_2 RS-485/RS-422 Failsafe

Setting	Function
(1-8), (2-7)	Pin 1/2 represents Off: Disable COM4 failsafe (default), 7/8 represents On: Enable COM4 failsafe
(3-6), (4-5)	Pin 3/4 represents Off: Disable COM3 failsafe (default), 5/6 represents On: Enable COM3 failsafe

2.3 System I/O





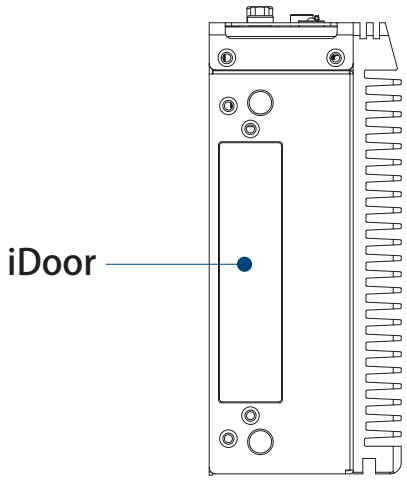


Figure 2.2 ARK-1251 Front and Rear I/O Connector Diagram

2.4 External I/O

2.4.1 Power On/Off Button

ARK-1251 has a Power On/Off button with LED indicators that show on status (Green LED).

Figure 2.3 Power On/Off Button

2.4.2 Power Input Connector

The power input connector supports 12 ~ 28V. The 3 pins are defined as +, -, and Ground.

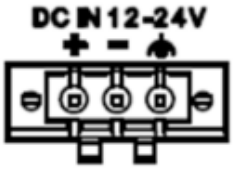


Figure 2.4 Power Input Connector

2.4.3 M.2 SSD LED Indicator

ARK-1251 provides one LED that indicates M.2 M Key or B key by jumper, and compact flash disk status.

Figure 2.5 SSD LED Indicator

2.4.4 Antenna Hole

ARK-1251 reserves 4 antenna holes for wireless antenna installation. Each of antenna hole mark “ANT” to let antenna hold easy to be recognized.

Figure 2.6 Antenna Hole

2.4.5 Audio Connector

ARK-1251 offers stereo audio ports by two phone jack connectors of Line Out and Mic In. The audio chip is controlled by Realtek ALC888S, and it’s compliant with Azalea standard.

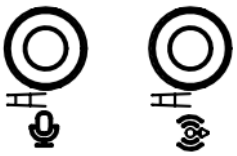


Figure 2.7 Audio Connector

2.4.6 DIO Connector

ARK-1251 provides 1x DIO connector.

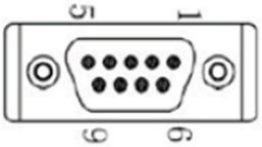


Figure 2.8 DIO Connector

Table 2.8: DIO Connector Pin Define

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

2.4.7 COM Connector

ARK-1251 provides offer 2 x RS-232/422/485 D-sub 9 serial communication interface ports, and the default setting is RS-232, the mode RS-422/ 485 can be supported via the BIOS settings. Also provide 2 x RS-422/485 D-sub 9 serial communication interface ports, and the default setting is RS-485.

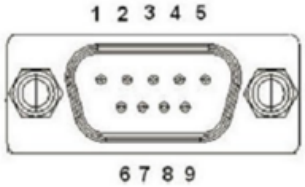


Figure 2.9 COM Connector

Table 2.9: COM Connector Pin Define

	RS-232	RS-422	RS-485
Pin	**Signal Name**	**Signal Name**	**Signal Name**
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

2.4.8 Ethernet Connector (1G LAN)

ARK-1251 is equipped with one Intel® i210-IT Ethernet controllers connected to LAN3. These Ethernet ports provide a standard RJ-45 jack connector with LED indicators. Right side LED shows Link status (Green LED) and Active status (flashing Green LED), and left side LED shows Speed status (Green LED for 1Gbps/Orange LED for 10 or 100 Mbps).

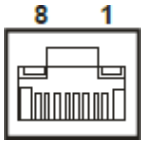


Figure 2.10 Ethernet Connector

Table 2.10: 1G Ethernet Connector (LAN) Pin Define

Pin	10/100/1000 BaseT Signal Name
1	BI_DA+(GHz)
2	BI_DA-(GHz)
3	BI_DB+(GHz)
4	BI_DB-(GHz)
5	BI_DC+(GHz)
6	BI_DC-(GHz)
7	BI_DD+(GHz)

Table 2.10: 1G Ethernet Connector (LAN) Pin Define	
8	BI_DD-(GHz)
H3	GND
H4	GND

2.4.9 Ethernet Connector (2.5G LAN)

ARK-1251 is equipped with two Intel® i226-LM Ethernet controllers connected to LAN1 and LAN2. These Ethernet ports provide a standard RJ-45 jack connector with LED indicators. Right side LED shows Link status (Green LED) and Active status (flashing Green LED), and left side LED shows Speed status (Green LED for 2.5Gbps/Orange LED for 1Gbps/no-flashing for 10 or 100 Mbps).

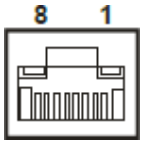


Figure 2.11 Ethernet Connector

Table 2.11: 2.5G Ethernet Connector (LAN) Pin Define	
Pin	**10/100/1000/2500 BaseT Signal Name**
1	BI_DA+(GHz)
2	BI_DA-(GHz)
3	BI_DB+(GHz)
4	BI_DB-(GHz)
5	BI_DC+(GHz)
6	BI_DC-(GHz)
7	BI_DD+(GHz)
8	BI_DD-(GHz)
H3	GND
H4	GND

2.4.10 HDMI Connector

ARK-1251 is equipped with 1 x 19-pin HDMI Type A interface. The HDMI link supports resolutions up to 7680 x 4320 @ 60 Hz.

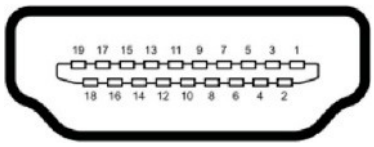


Figure 2.12 HDMI Receptacle Connector

Table 2.12: HDMI Connector Pin Define			
Pin	**Signal Name**	**Pin**	**Signal Name**
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-

Table 2.12: HDMI Connector Pin Define			
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		

2.4.11 DP

ARK-1251 is equipped with 1 x 20-pin DP connector, supports up to 7680 x 4320 @ 60 Hz.

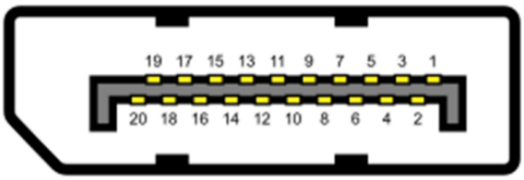


Figure 2.13 DP Receptacle Connector

Table 2.13: DP Connector Pin Define			
Pin	**Signal Name**	**Pin**	**Signal Name**
20	ML_Lane 0 (p)	21	GND
22	ML_Lane 0 (n)	23	ML_Lane 1 (p)
24	GND	25	ML_Lane 1 (n)
26	ML_Lane 2 (p)	27	GND
28	ML_Lane 2 (n)	29	ML_Lane 3 (p)
30	GND	31	ML_Lane 3 (n)
32	CONFIG1	33	CONFIG2
34	AUX CH (p)	35	GND
36	AUX CH (n)	34	Hot plug
38	Hot Plug Detect	39	DP_PWR

2.4.12 USB 3.2 - Gen2

ARK-1251 supports 2 x USB 3.2 interface. The USB interfaces comply with USB XHCI, Rev. 3.2 standards. USB 3.2 Gen2 connectors contain legacy pins to interface with USB 2.0 devices, and a new set of pins for USB 3.2 connectivity.

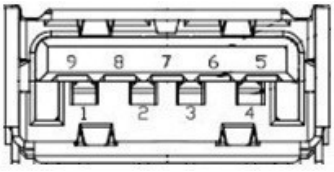


Figure 2.14 USB 3.2 Connector

Table 2.14: USB 3.2 Connector Pin Define			
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+		

2.4.13 USB 2.0

ARK-1251 supports 4 x USB 2.0.

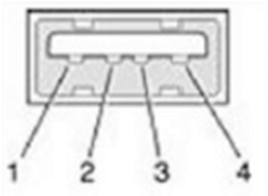


Figure 2.15 USB 2.0 Connector

Table 2.15: USB 2.0 Connector Pin Define	
Pin	**Signal Name**
1	VCC
2	USB Data -
3	USB Data +
4	GND

2.4.13.1 Remote Switch Connector

ARK-1251 provides the remote switch connector for power on/off. From the left to the right are WDT, Power Switch, GND, and Reset.

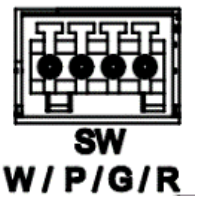


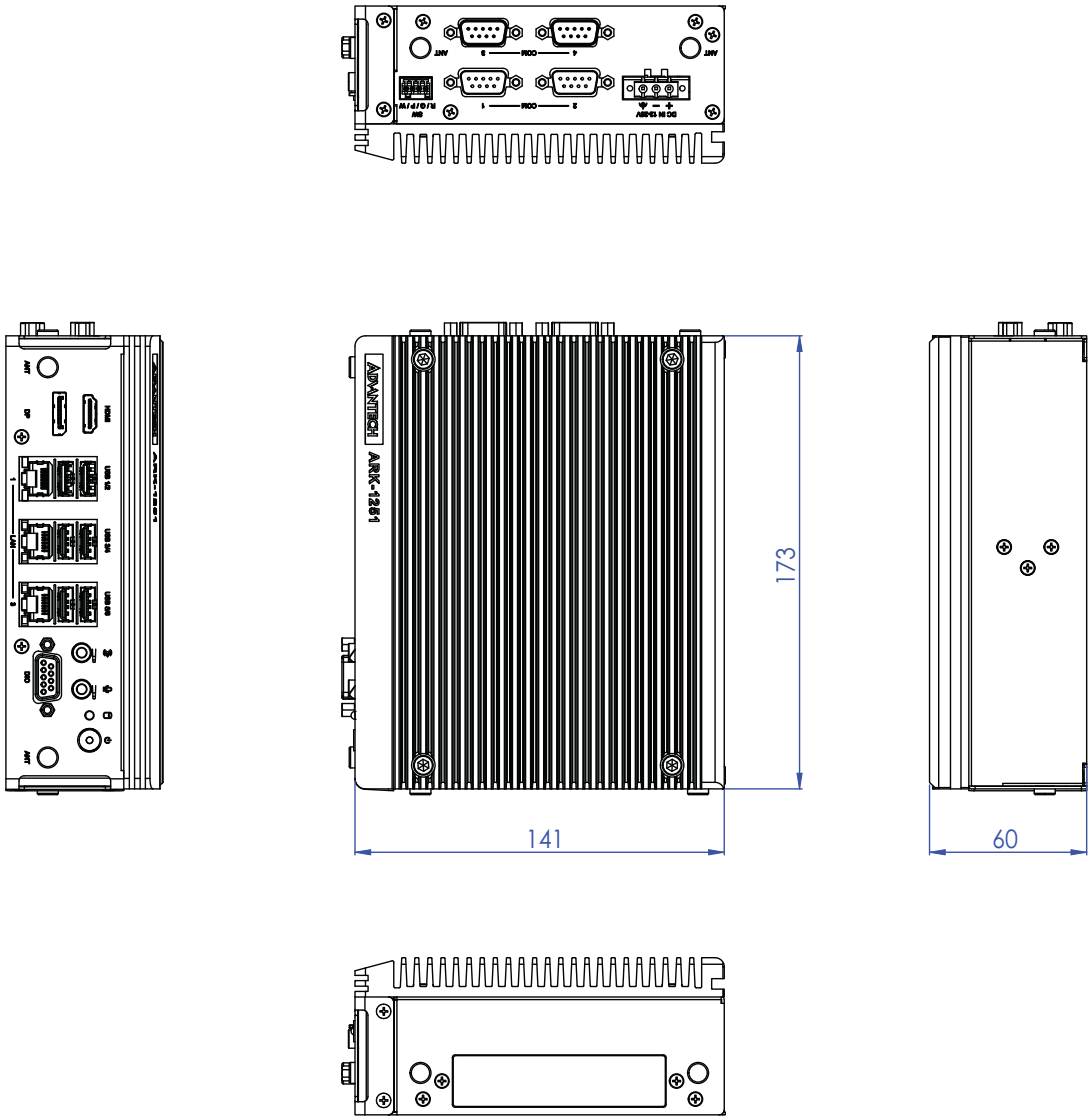
Figure 2.16 Remote Switch Connector

Table 2.16: Remote Connector Pin Define	
Pin	**Signal Name**
1	WDT
2	Power button
3	GND
4	Reset button

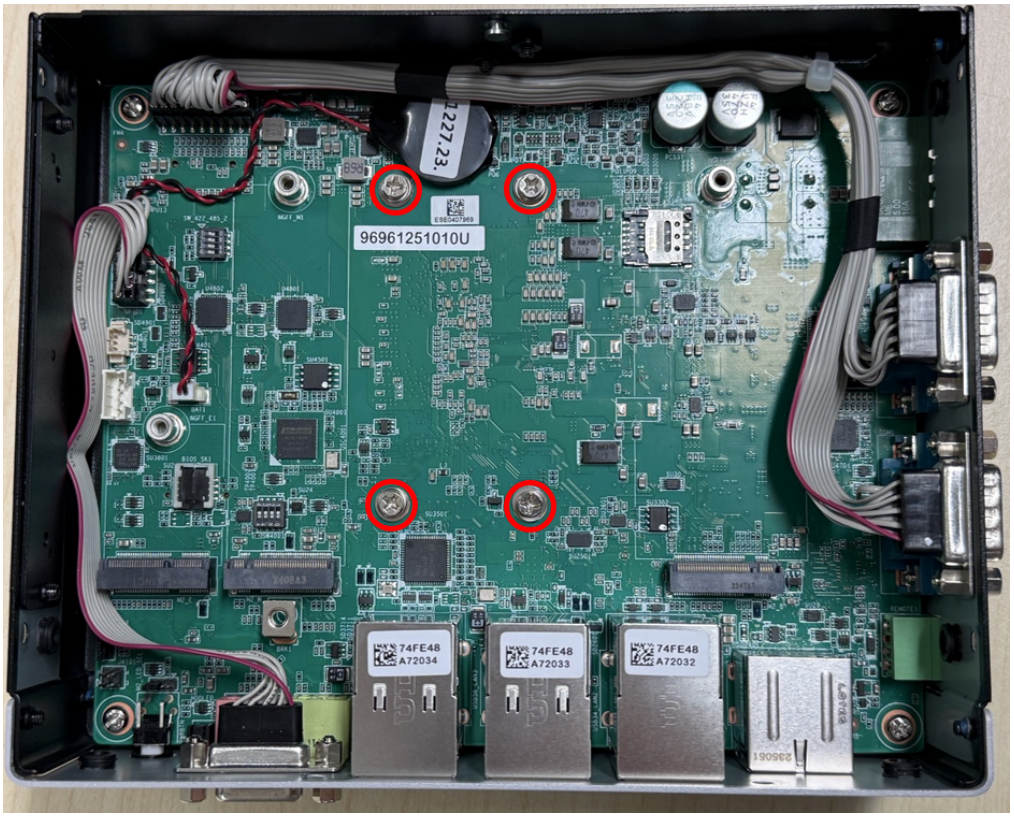
2.5 Installation

2.5.1 Memory and CPU Thermal Pad Installation

1. Loosen the 6 screws on the front/sides and remove the bottom cover

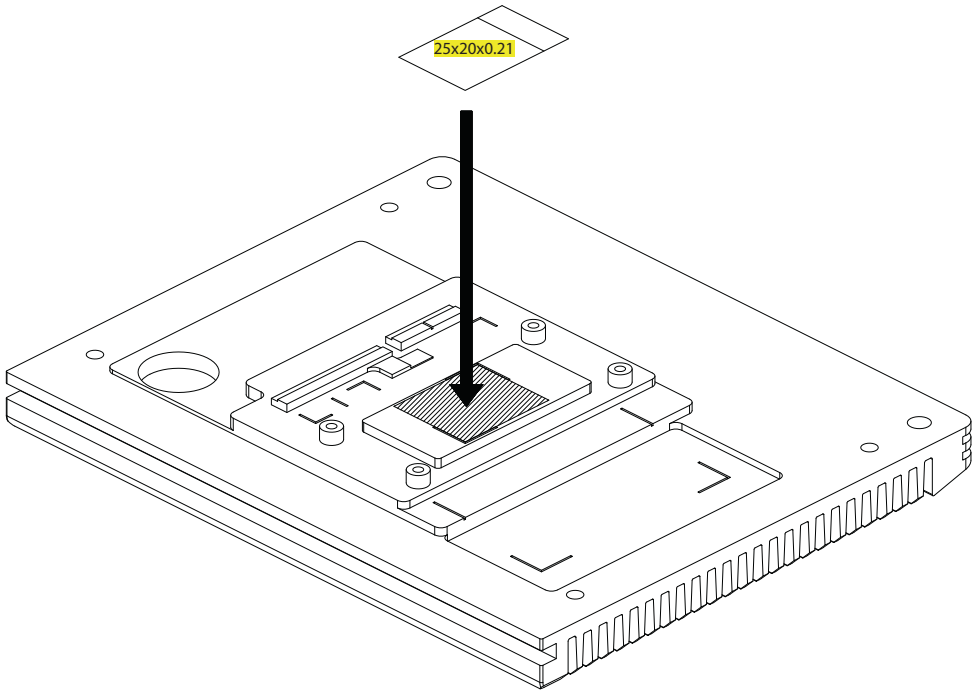


2. Loosen the 4 spring screws on main board.



3. Loosen the 4 screws on the top cover, and remove the top cover.

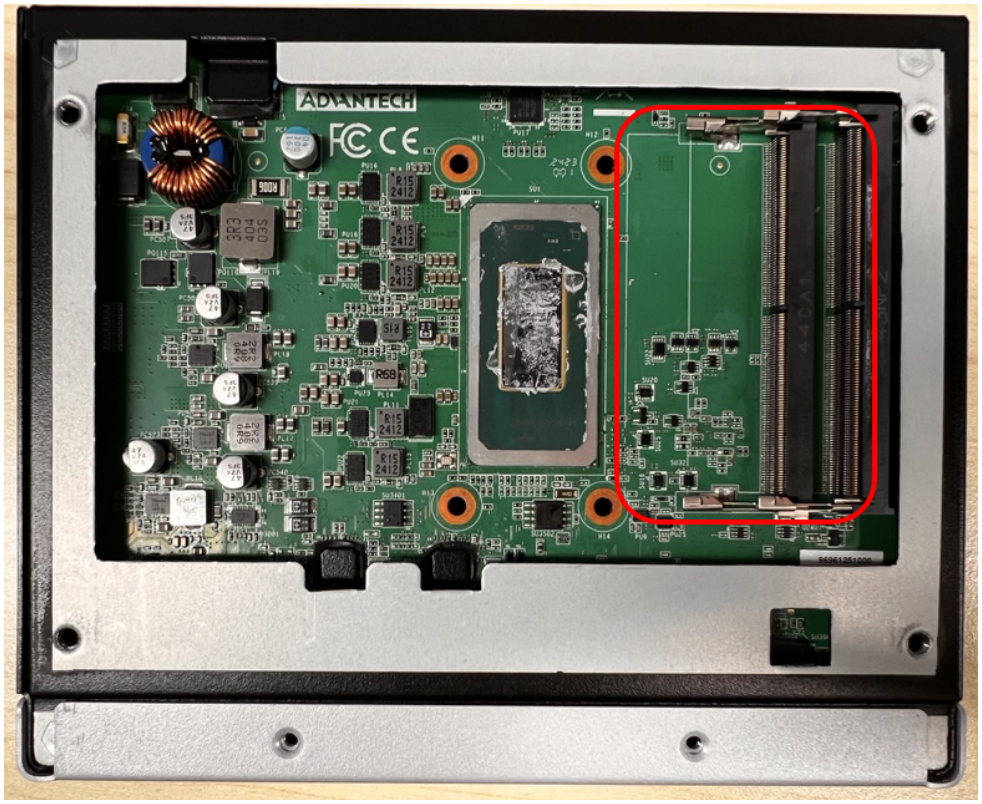
4. Install CPU thermal pad on top cover



Note! *The release paper must be removed when installing thermal pad for CPU.*

5. Install the memory into the slots.

6. Replace the top cover with the 6 screws.

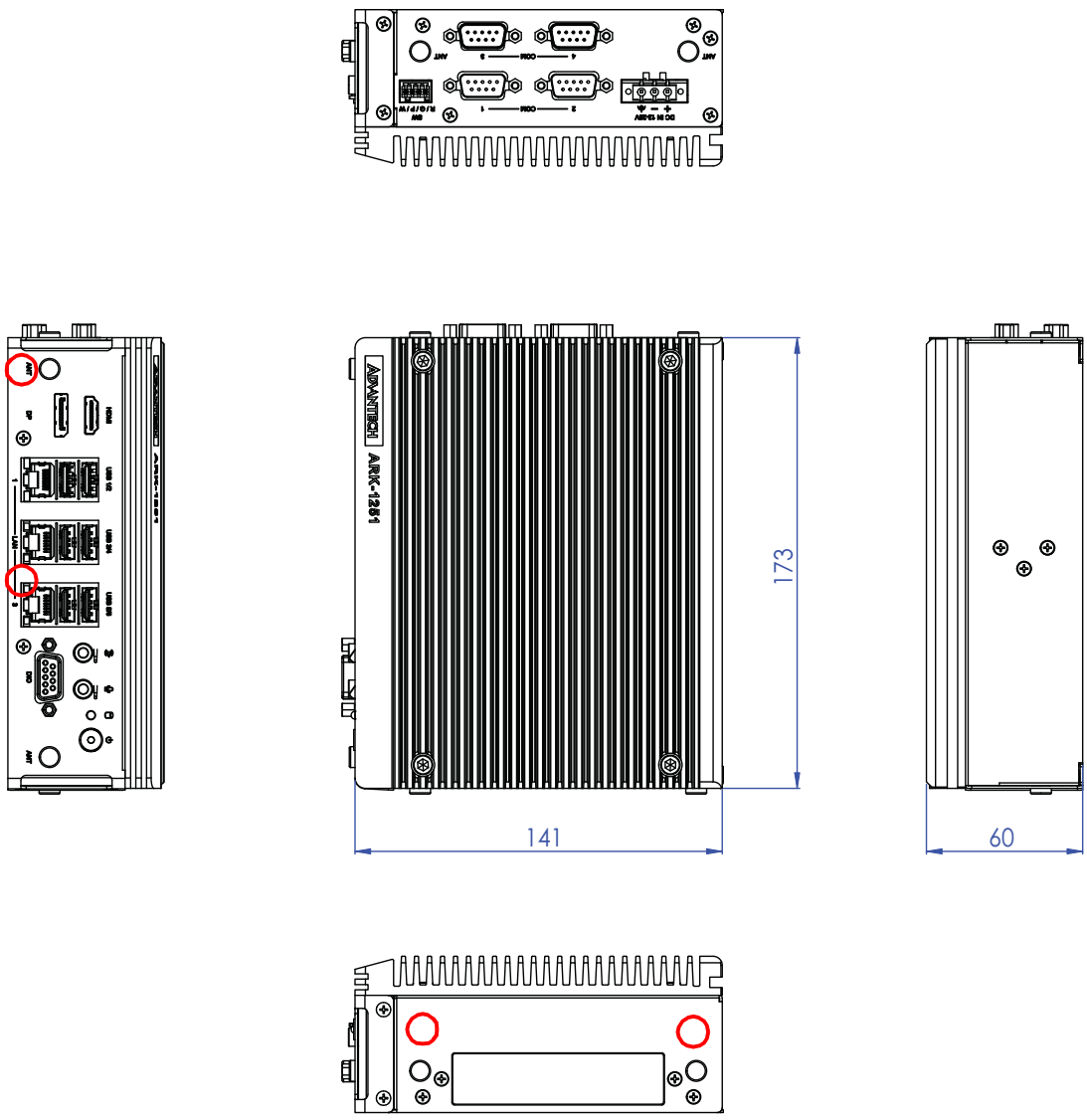


Note! *There are two thermal pads for second RAM in the accessory box. Please do place the thermal pad for second RAM if needed.*

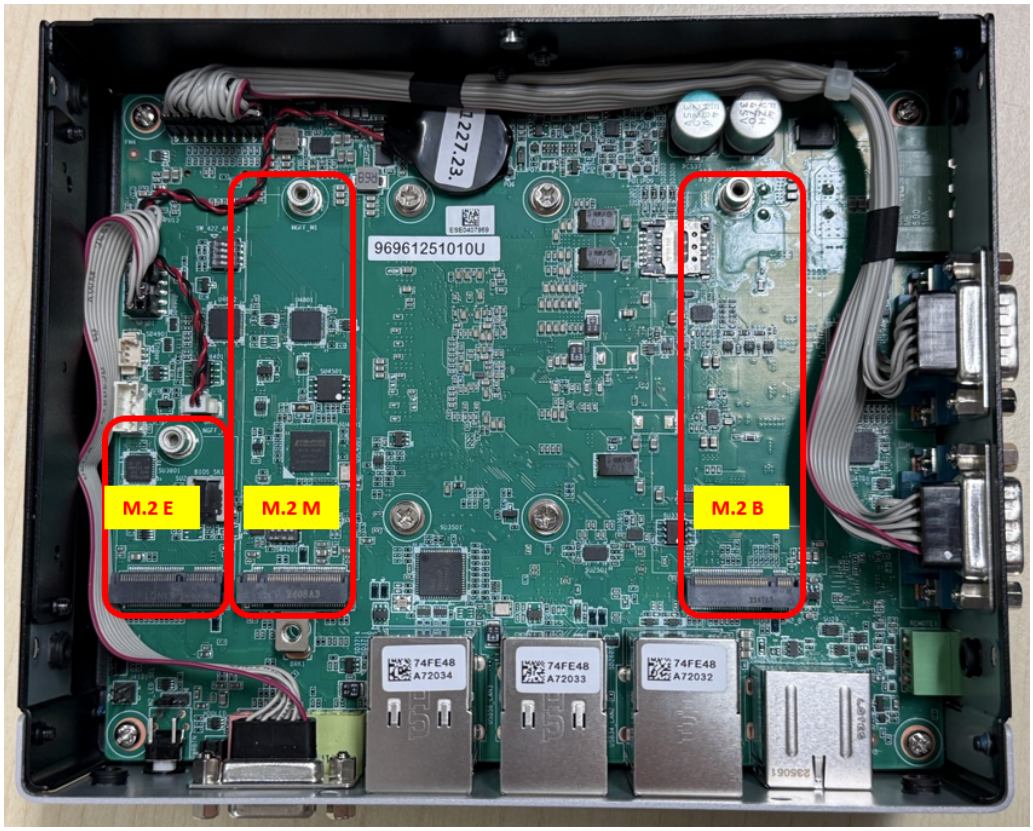
Note! *The release paper must be removed when installing thermal pad for memory.*

2.5.2 M.2 Module Installation

1. Loosen the 6 screws on the front/sides and remove the bottom cover.



2. Install the M.2 module into the system.
3. Replace the bottom cover with the 6 screws.



Note! *M key is default for storage, E key is for WiFi module, and B key is for 5G/AI card/ iDoor module.*

4. Using 4pcs M3.5 screws in accessory box to install the M.2 SSD thermal kit and thermal pad for M.2 2280 PCIe module.

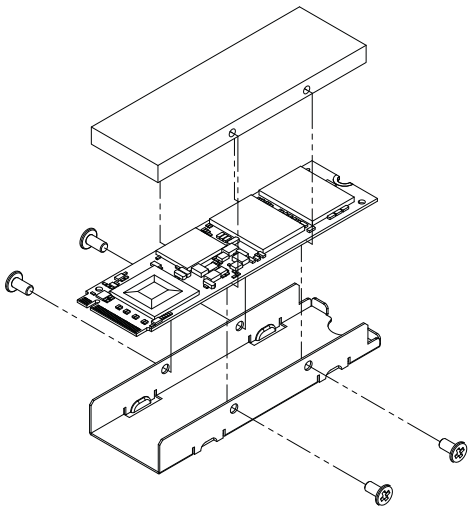


Figure 2.17 M.2 2280 SSD thermal kit

Note! *The release paper must be removed when installing thermal pad for SSD.*

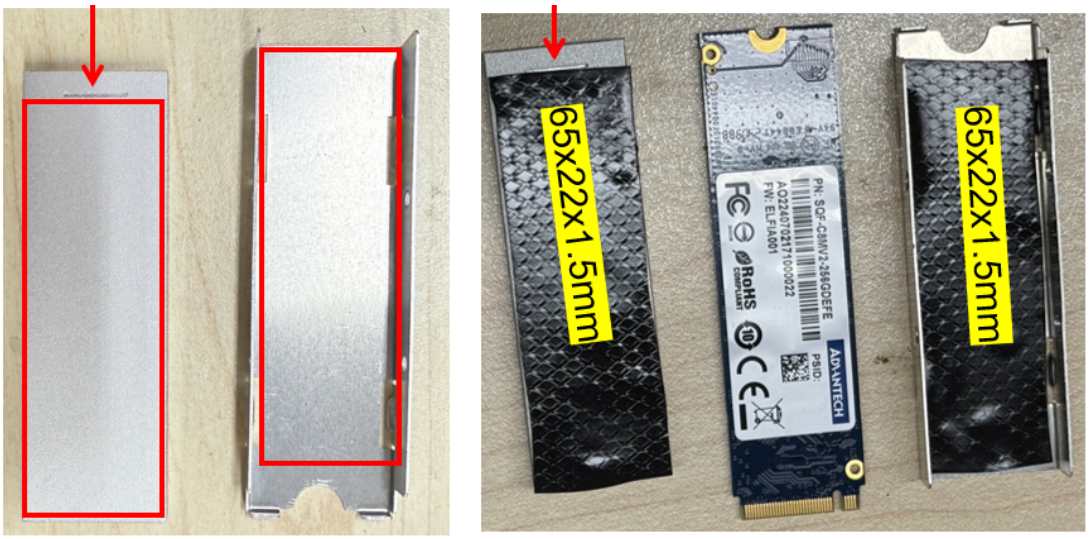


Figure 2.18 Placing thermal pad along with the mark

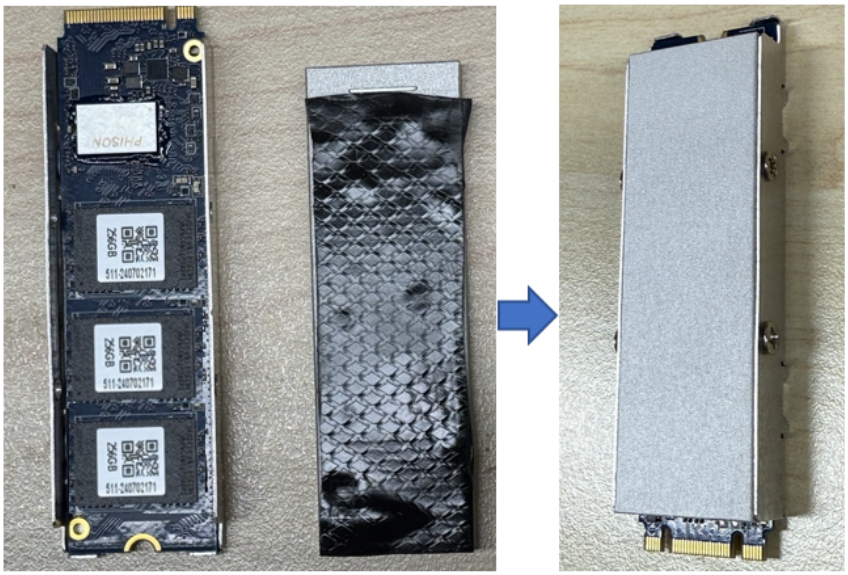
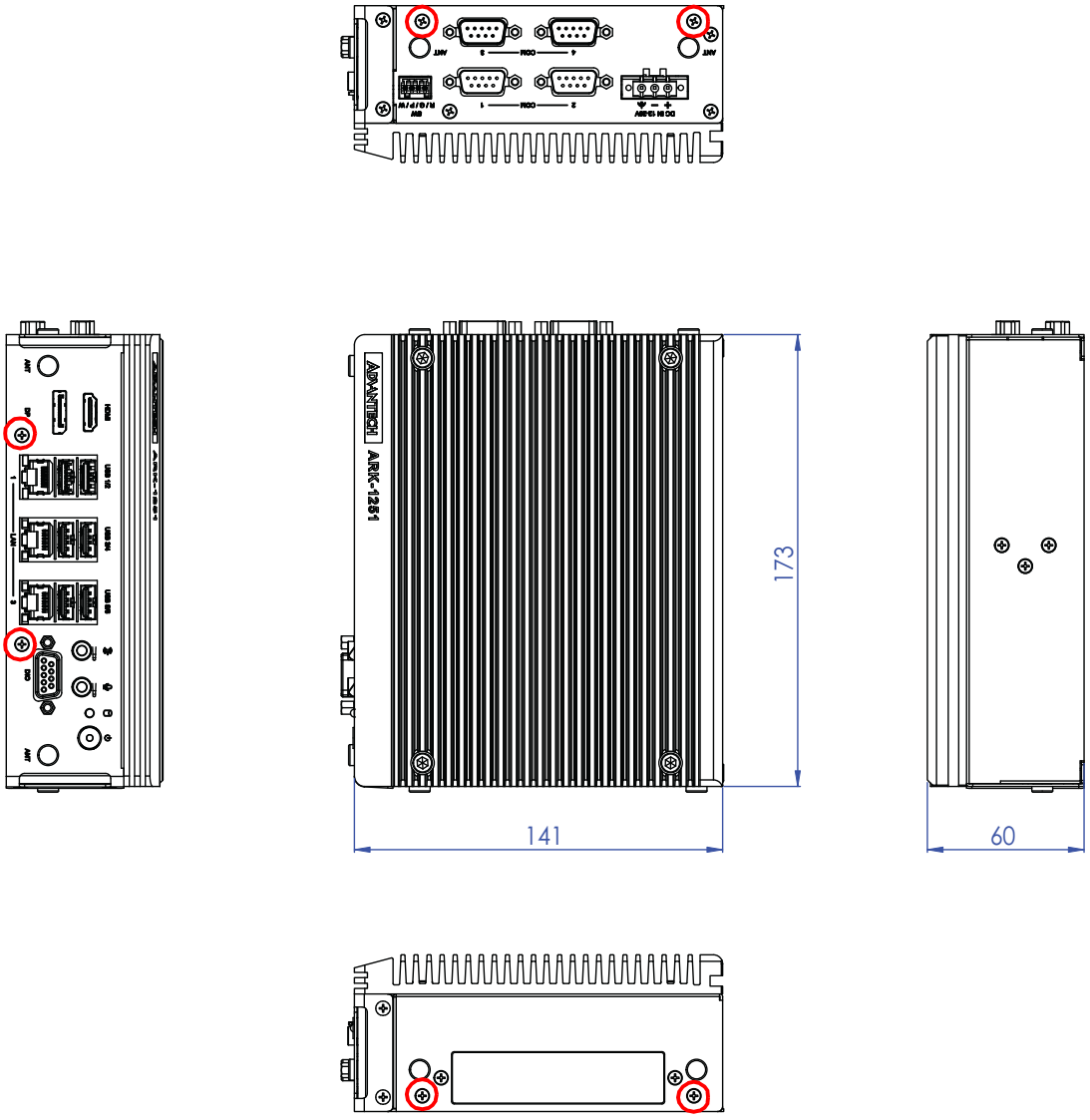


Figure 2.19 Cover up the kit with M3.5 screws

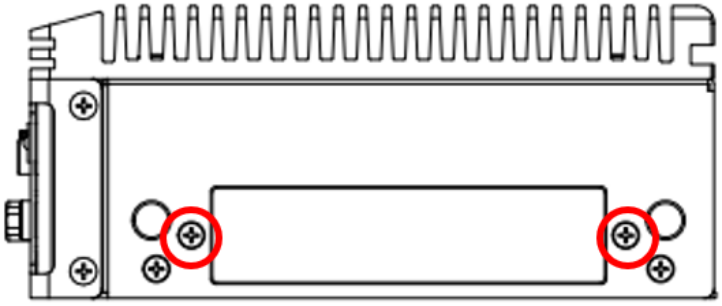
2.5.3 AMO I032 + Idoor Installation

AMO-I032 is the expansion kit (M.2 B-Key to mPCIe) for installing iDoor modules on ARK-1251. Users need to install AMO-I032 together with the iDoor module.

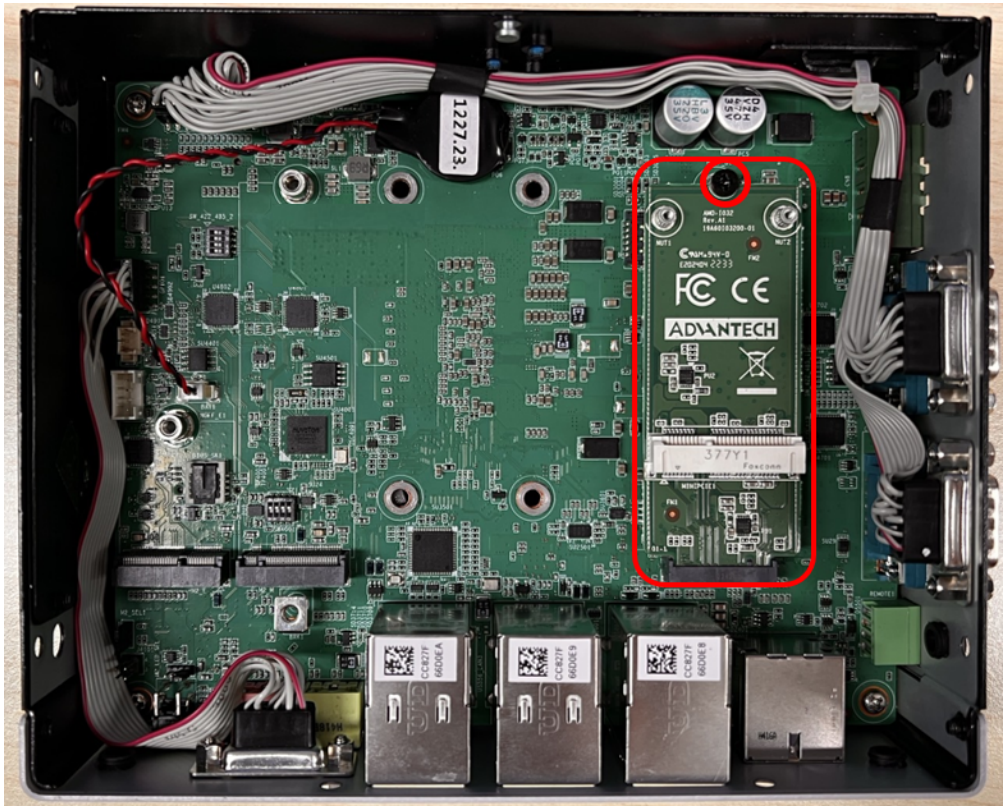
1. Loosen the 6 screws on the front/sides and remove the bottom cover.



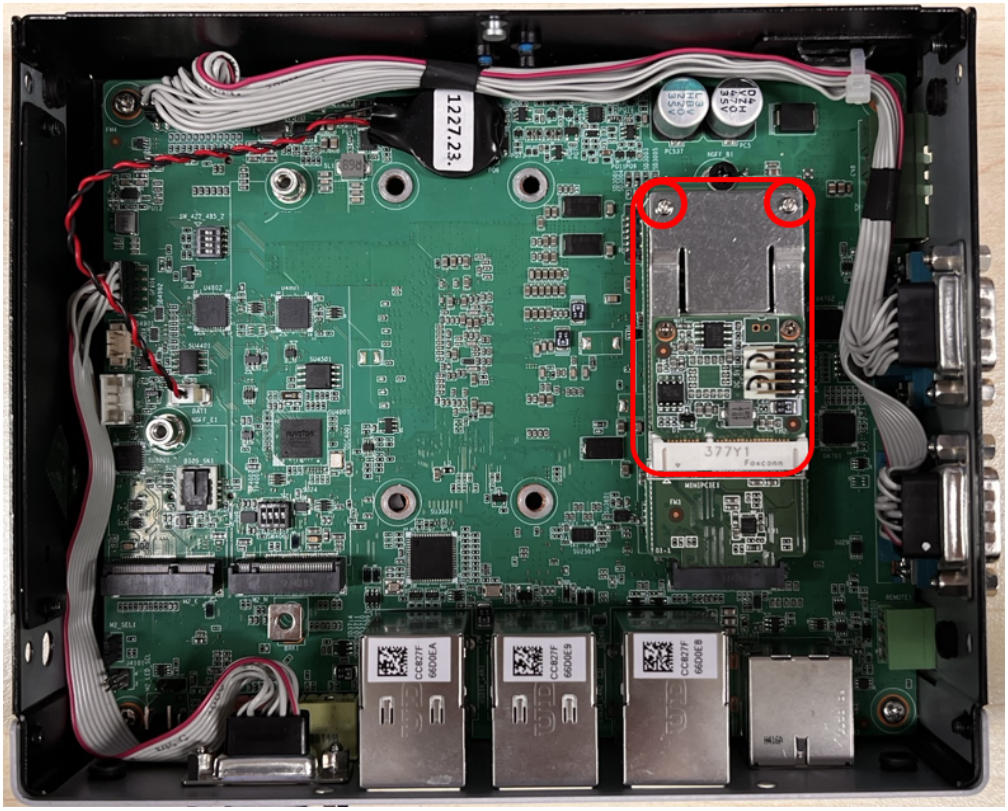
2. Loosen the 2 screws on the sides and remove the idoor cover



3. Install AMO-I032 on B key and screw it with a M3x5L screw.



4. The iDoor module board can then be installed on the AMO-I032.
5. Replace the bottom cover with the 6 screws.

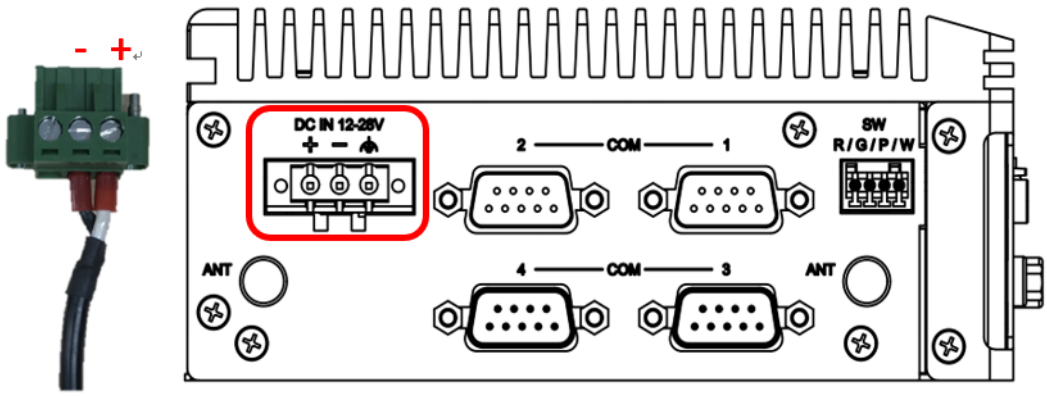


Note!

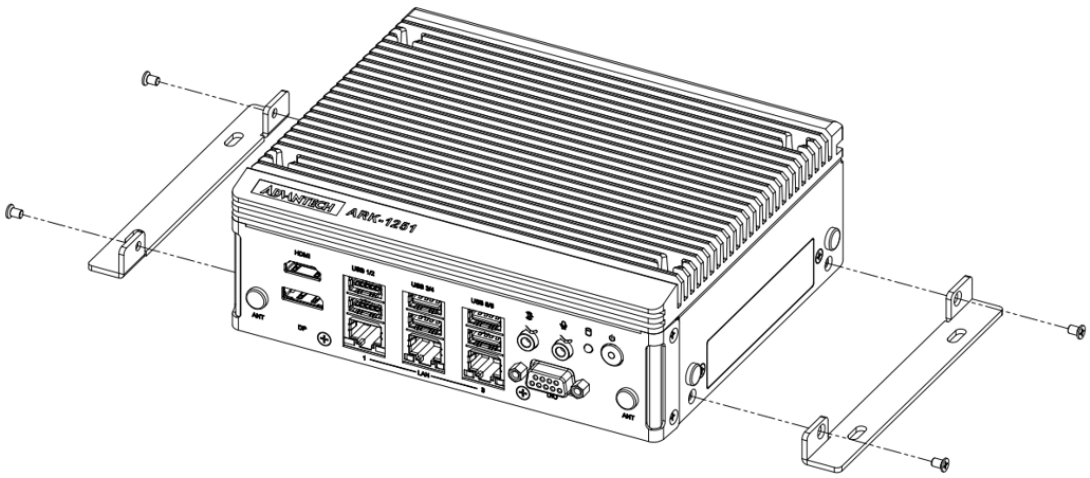
1. *You need to order the AMO-I032 together with MOS modules.*
2. *M.2 E Key cannot be used when adding any MOS module due to mechanical interference.*

2.5.4 Adapter Installation

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



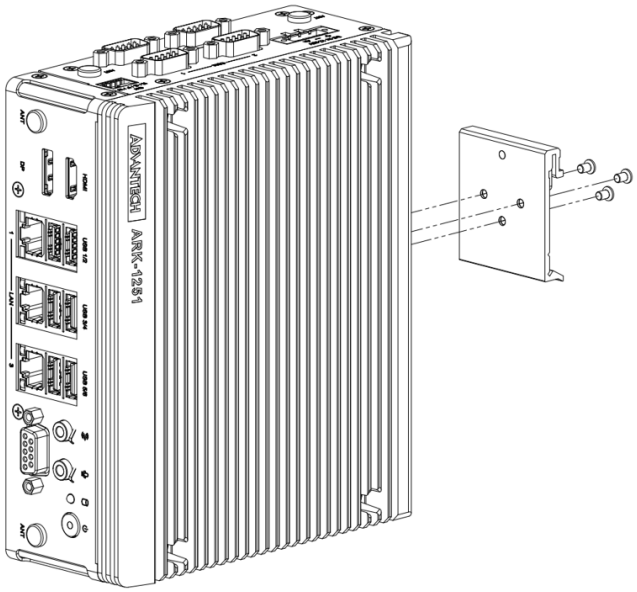
2.5.5 Wall mount Installation



1. Unscrew the 4 x M3x5L screws on both sides of ARK-1251.
2. Using the 4 screws removed in the above step to secure the wall mount brackets on both sides of ARK-1251

1. *Dévissez les 4x vis M3x5L ou des deux côtés de l'ARK-1251.*
2. *Vissez les supports de montage mural des deux côtés de l'ARK-1251 avec les quatre vis à l'arrière.*

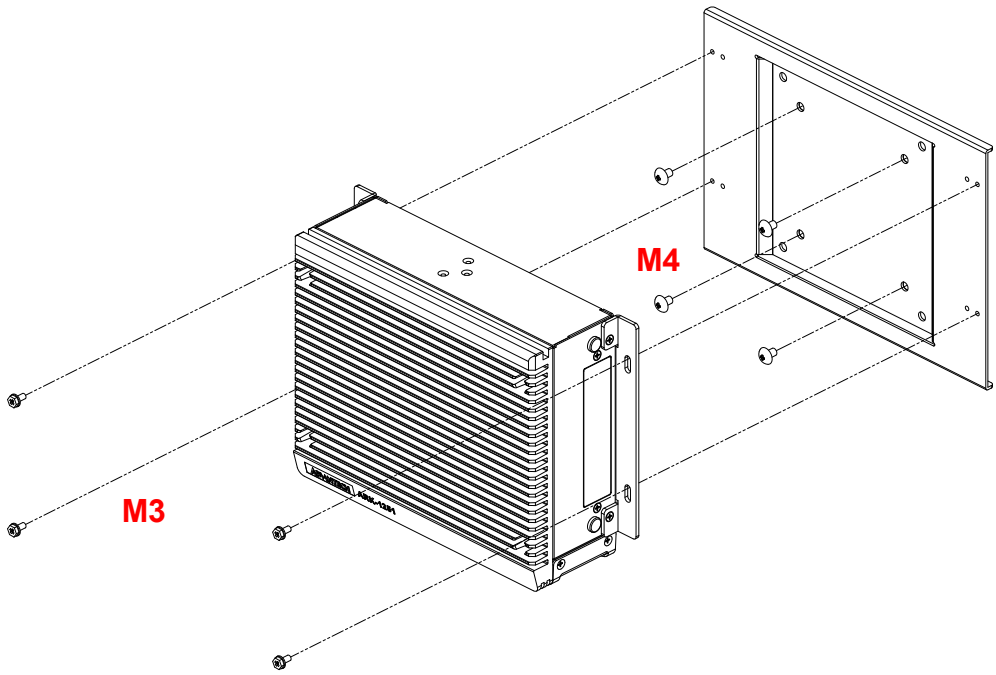
2.5.6 Din Rail Installation



1. Unscrew the 3 x M3x5L screws from the back side of ARK-1251.
2. Using 3 screws to secure the DIN-rail bracket on the back.

1. *Dévissez les 3 vis M3x5L à l'arrière de l'ARK-1251.*
2. *Revissez le support du rail DIN avec les trois vis*

2.5.7 VESA Mount Installation



1. Unscrew the 4 x M3x5L screws on both sides of ARK-1251.
2. Using the 4 screws removed in the above step to secure the wall mount brackets on both sides of ARK-1251
3. Using 4 x M4x6L in VESA mount accessory box to install VESA mount on certain object
4. Using 4 x M3x6L in VESA mount accessory box to install ARK-1251 on VESA mount.

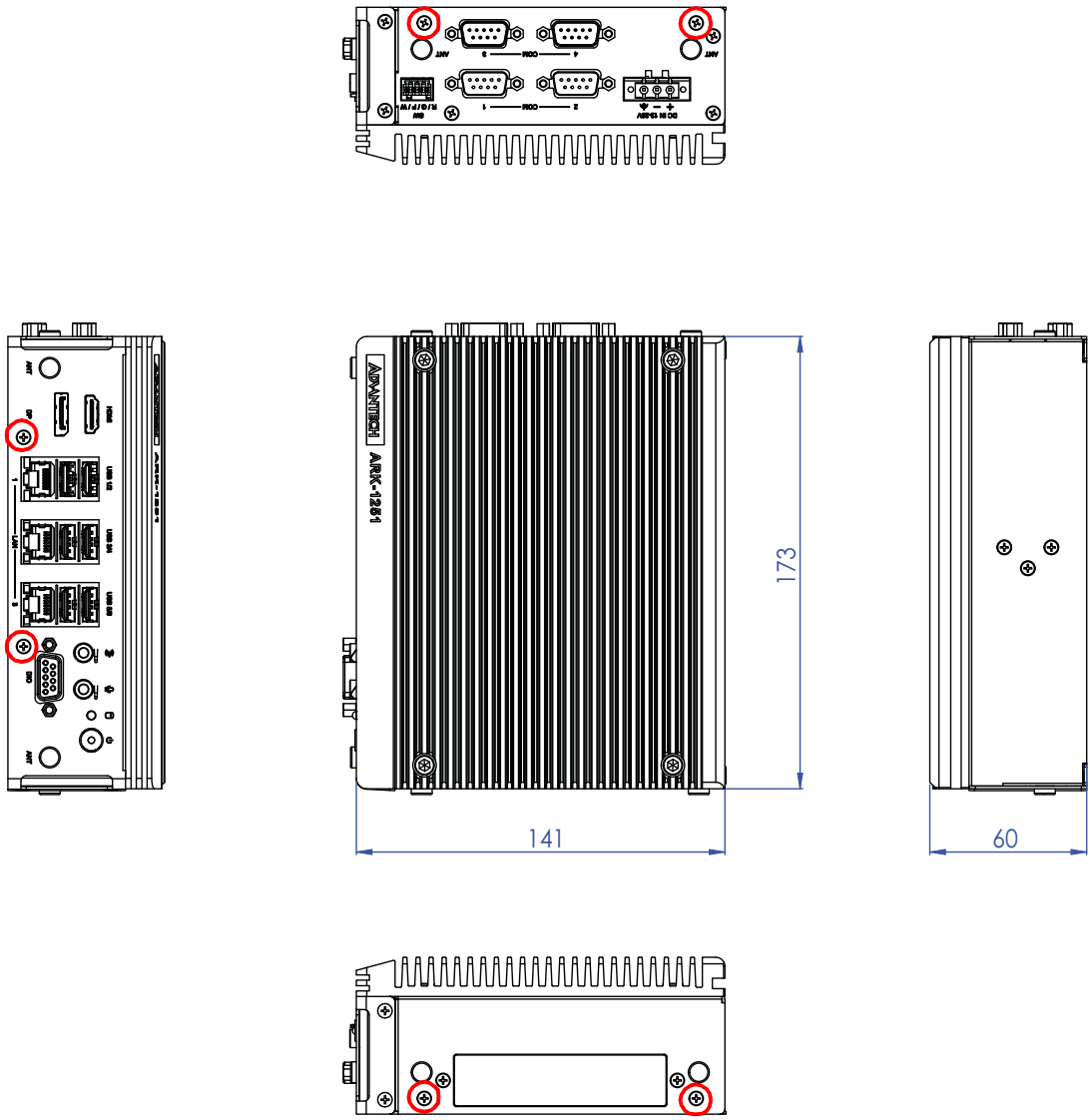
Note! *Wall mount kit AMK-W006 must be used along with VESA mount.*

1. *Dévissez les 4x vis M3x5L ou des deux côtés de l'ARK-1251.*
2. *Vissez les supports de montage mural des deux côtés de l'ARK-1251 avec les quatre vis à l'arrière.*
3. *Utilisation de 4 x M4x6L dans la boîte d'accessoires de montage VESA pour installer le support VESA sur certains objets*
4. *Utilisation de 4 x M3x6L dans la boîte d'accessoires de montage VESA pour installer l'ARK-1251 sur le support VESA.*

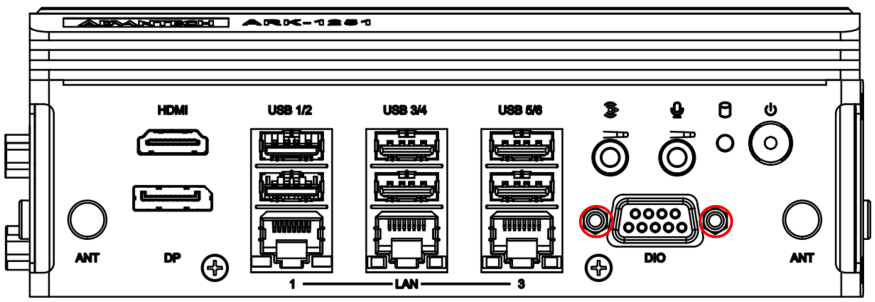
Note! *Les utilisateurs ont besoin d'un support mural lorsqu'ils utilisent le support VESA.*

2.5.8 Optional CAN Bus Installation

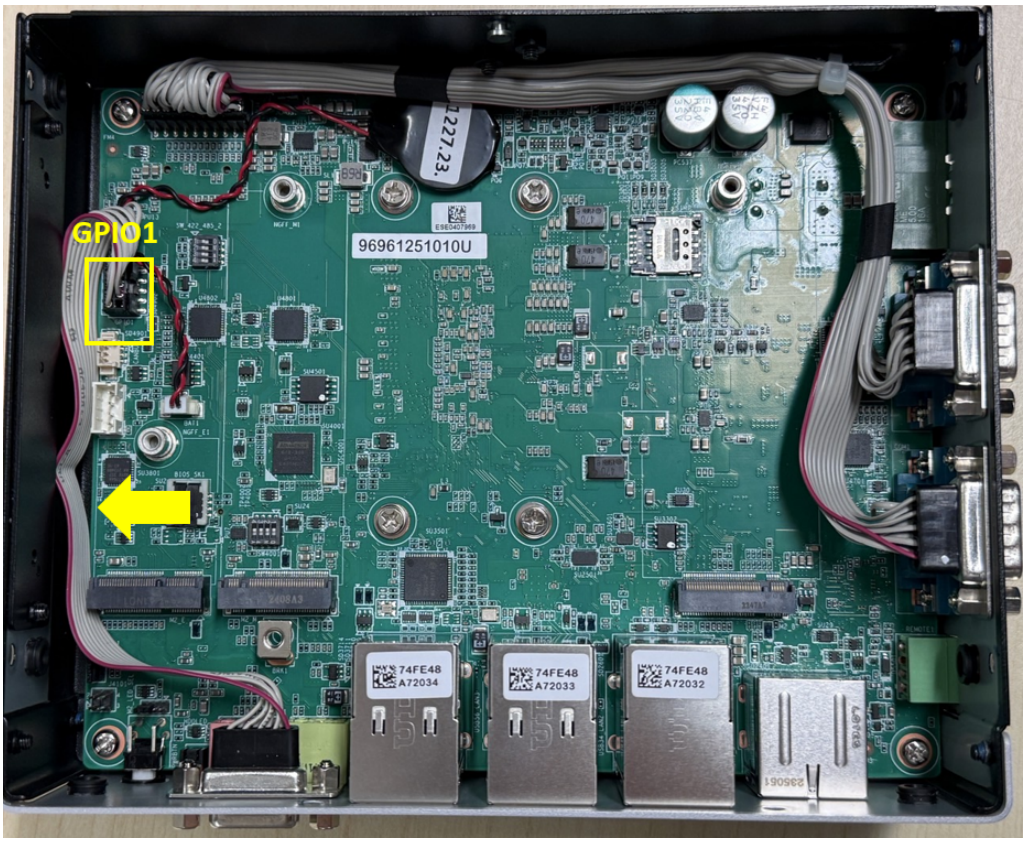
1. Loosen the 6 screws on the front/sides and remove the bottom cover.



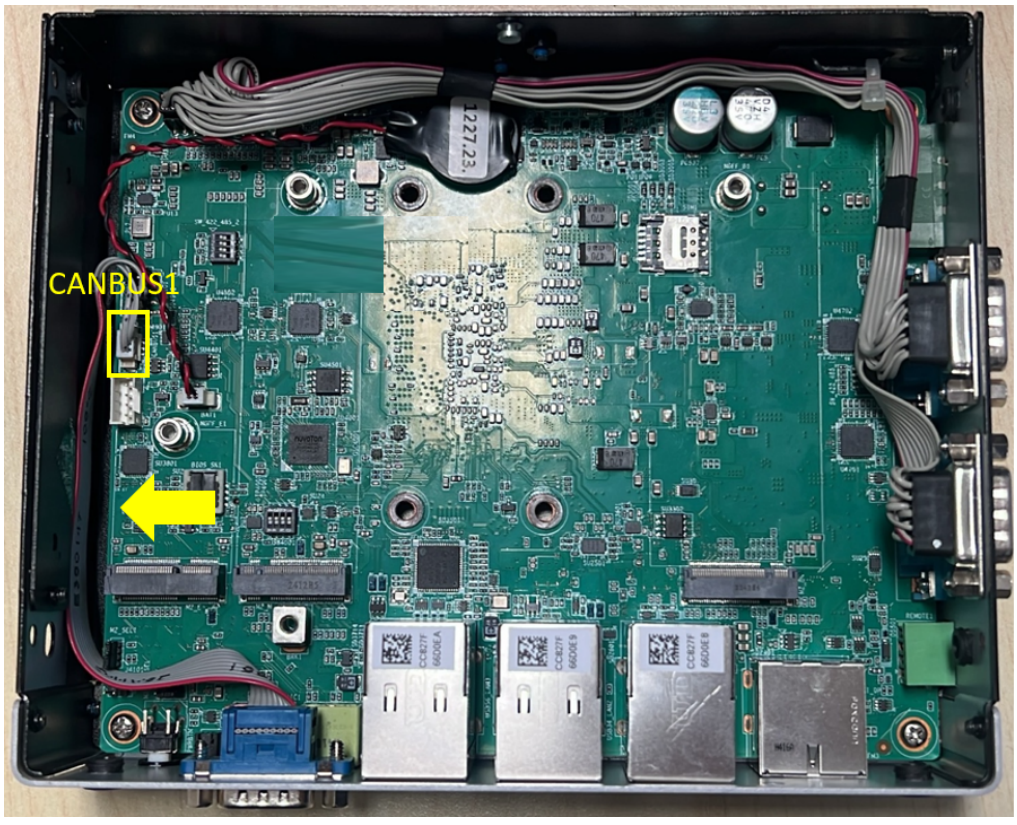
2. Loosen 2 screws of the DIO cable



3. Remove the DIO cable.



4. Install the CAN Bus cable and bottom cover back. (Advantech Part Number 1700030518-01).



5. CAN Bus cable pin definitions are shown below.

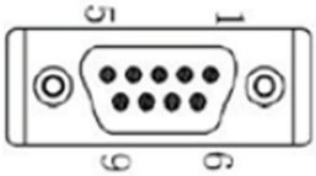
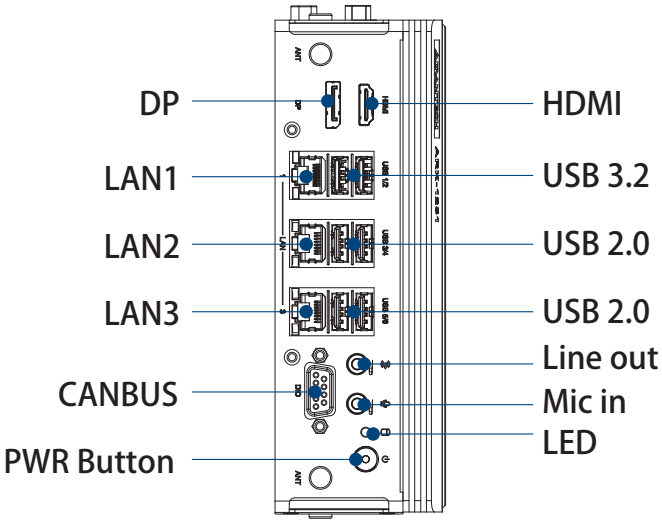


Figure 2.20 CAN Bus Connector

Table 2.17: CAN Bus Connector Pin Define

Pin	Signal Name
1	NC
2	CAN_L
3	GND
4	NC
5	NC
6	NC
7	CAN_H
8	NC
9	NC

ARK-1251 I/O image with optional CAN Bus port.



Chapter 3

BIOS Setting

This chapter details instructions for Setting BIOS configuration data.

3.1 Introduction

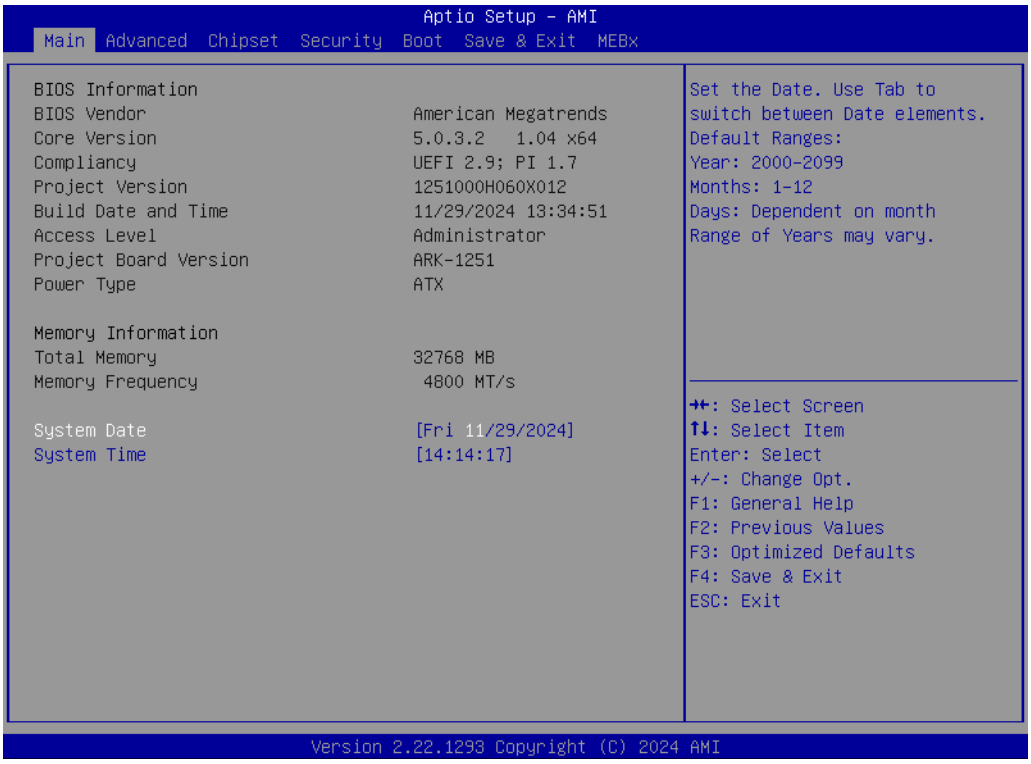
The AMI BIOS ROM has a built-in setup program — the BIOS Setup Utility — that allows users to modify the basic system configuration. All configuration data is stored in battery-backed CMOS to ensure the setup information is retained when the power is turned off. This chapter describes the basic navigation of the ARK-1251 BIOS setup screens.

3.2 Entering BIOS Setup

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

3.2.1 Main Setup

Upon accessing the BIOS Setup Utility, users are presented with the Main setup page. Users can always return to the Main Setup page by selecting the Main tab. The Main BIOS Setup page is shown below.



The Main BIOS setup page has two main frames. The left frame displays all the items accessible on the Main page. Items that are grayed out cannot be configured, whereas items presented in blue text can be configured. The right frame displays the key legend.

Located above the key legend is an area reserved for a text message. When an item is selected in the left frame, the item is presented in white text and often accompanied by a text message.

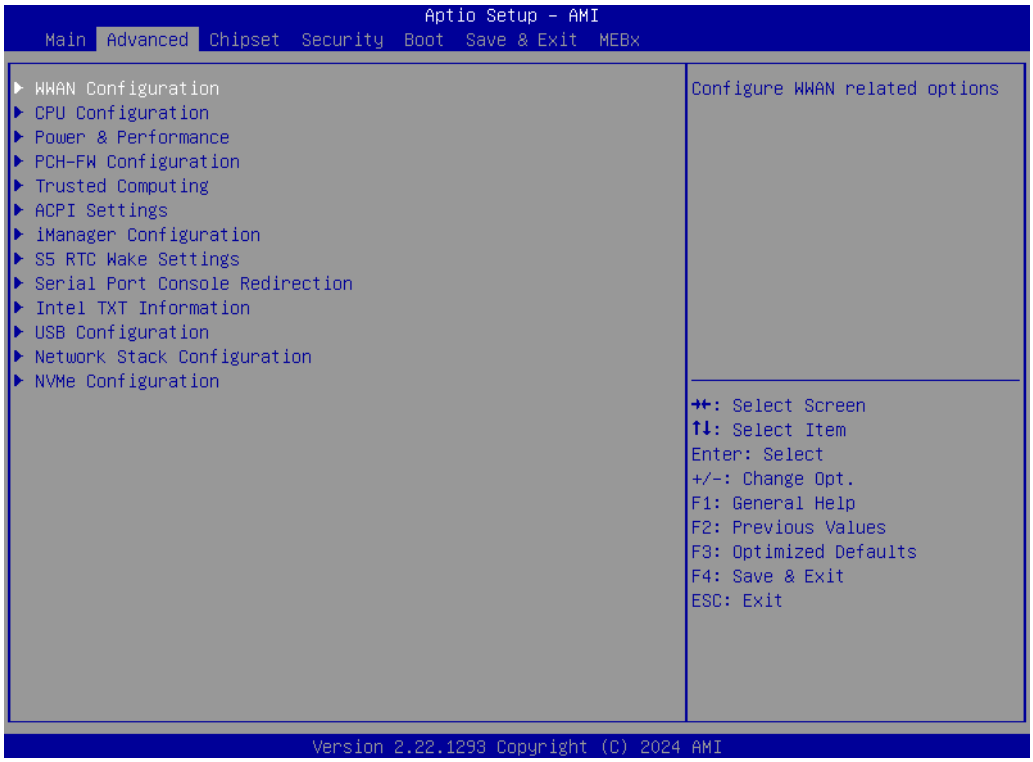
- **System Date / System Time**

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

3.2.2 Advanced Setup

Select the Advanced tab from the BIOS Setup Utility to enter the Advanced BIOS Setup page. Select any of the items in the left frame of the screen, such as CPU Configuration, to access the sub-menu for that item. The options for any of the Advanced BIOS Setup items can be displayed by highlighting the item using the <Arrow> keys.

The Advanced BIOS Setup page is shown below:

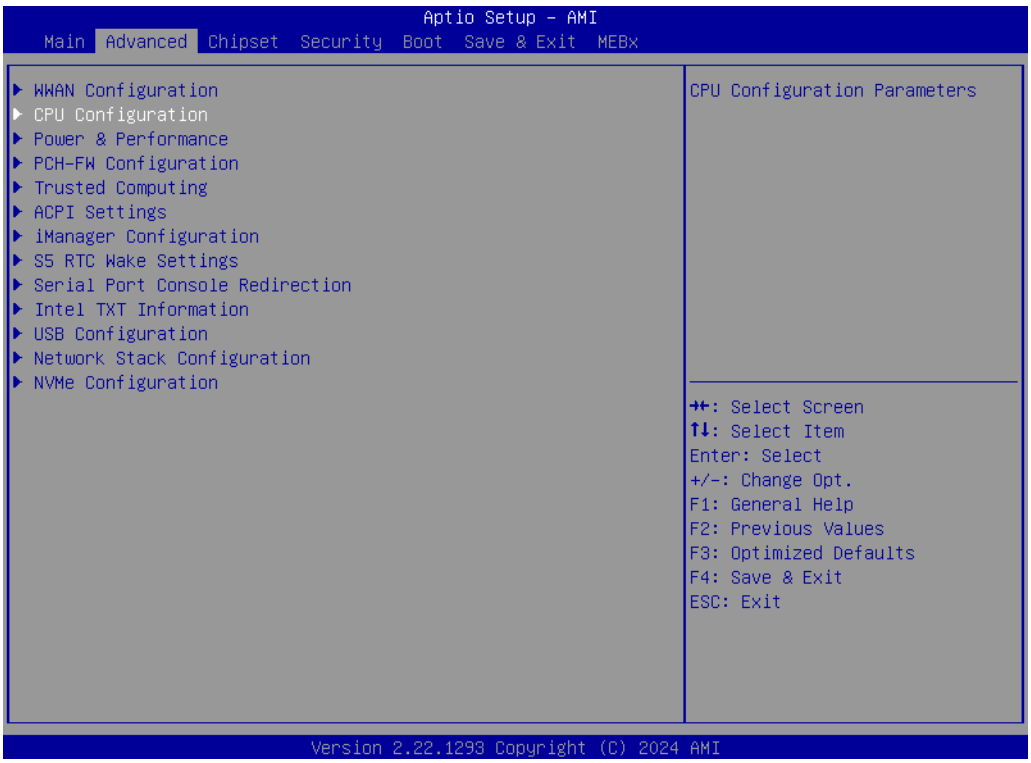


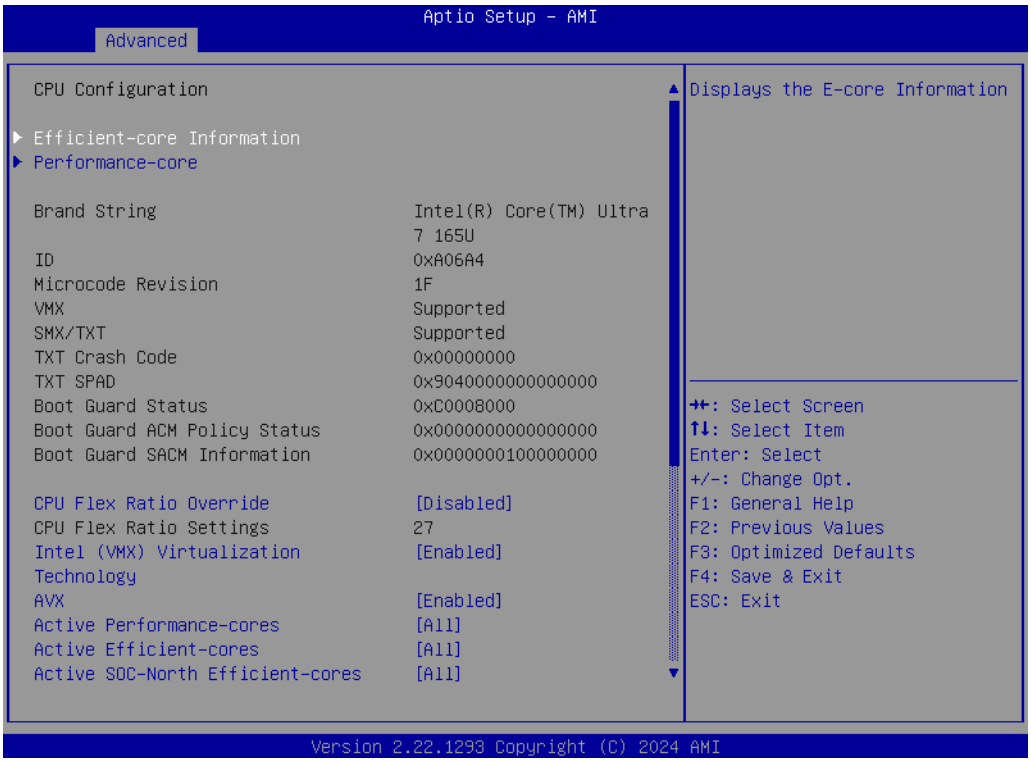
3.2.2.1 WWAN Configuration

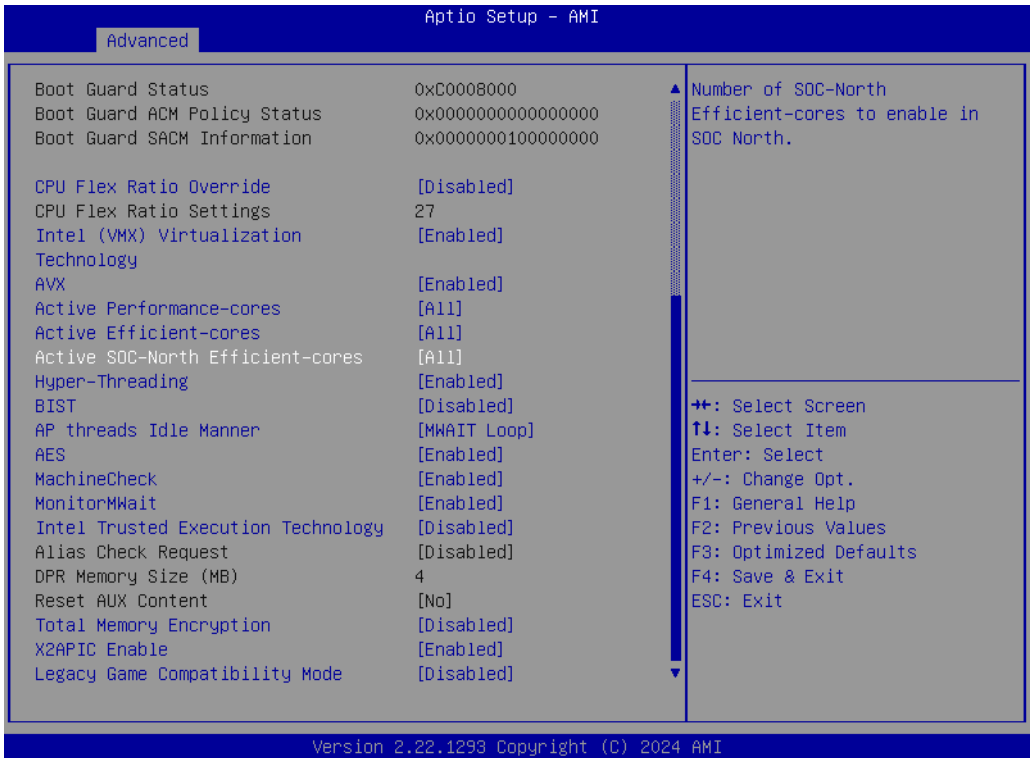
■ **WWAN Device**

Enable or disable M.2 WWAN Device

3.2.2.2 CPU Configuration



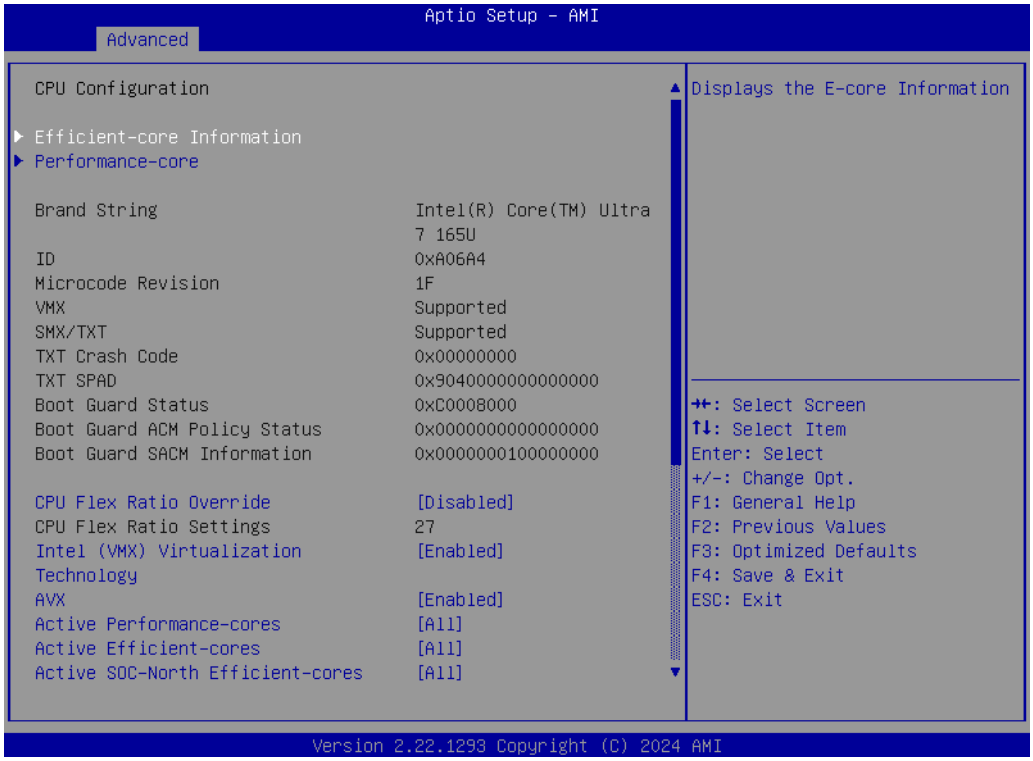


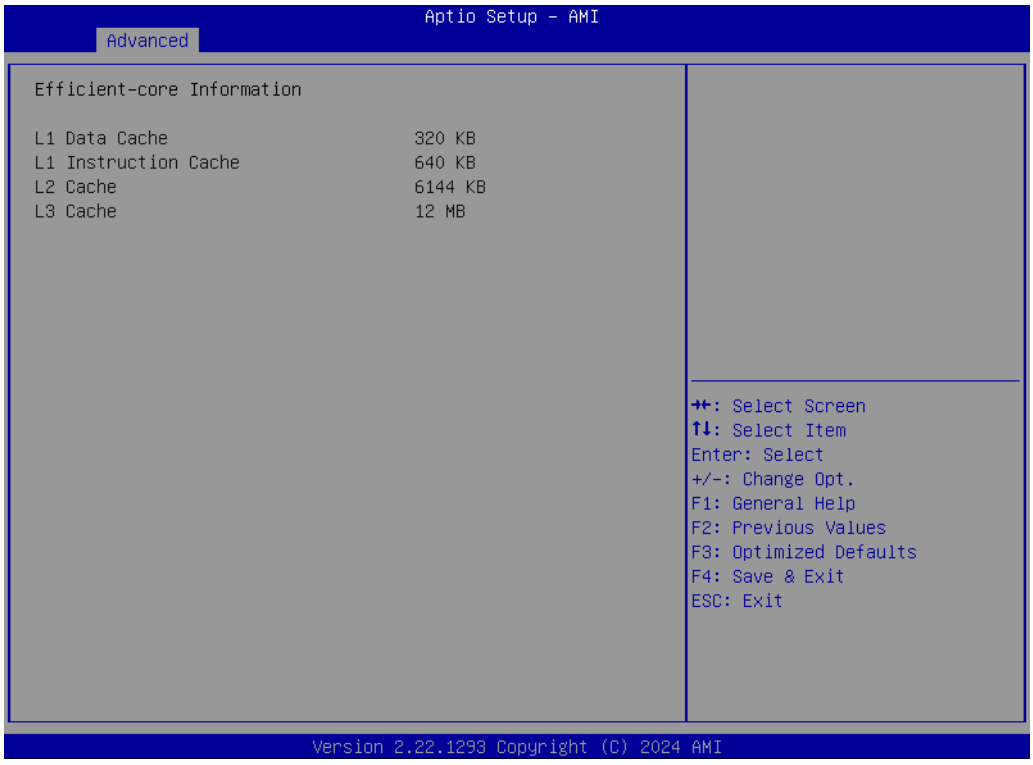


- **Efficient-core Information**
  Displays the Efficient-core Information.
- **Performance-core**
  Displays the P-core Information.
- **CPU Flex Ratio Override**
  Enable or Disable CPU Flex Ratio Programming.
- **CPU Flex Ratio Settings**
  This value must be between the Max Efficiency Ratio (LFM) and the Maximum non-turbo ratio set by hardware (HFM).
- **Intel® (VMX) Virtualization Technology**
  When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
- **AVX**
  Enable/Disable the Avx 2 Instructions. This is applicable for Performance-core only.
- **Active Performance-cores**
  Number of P-cores to enable in each processor package. Note: Number of Cores and E-Cores are looked at together. When both are {0,0}, Pcode will enable all cores.
- **Active Efficient-cross**
  Enable/Disable Per Core Disable. When Per Core Disable Configuration is enabled, selection of Active Cores and Active Efficient-cores will be disabled.
- **Active SOC-North Efficient-cores**
  Number of SOC-North Efficient-cores to enable in SOC North
- **Hyper-Threading**
  Enable or Disable Hyper-Threading Technology.
- **BIST**
  Enable/Disable BIST (Built-in Self Test) on reset.

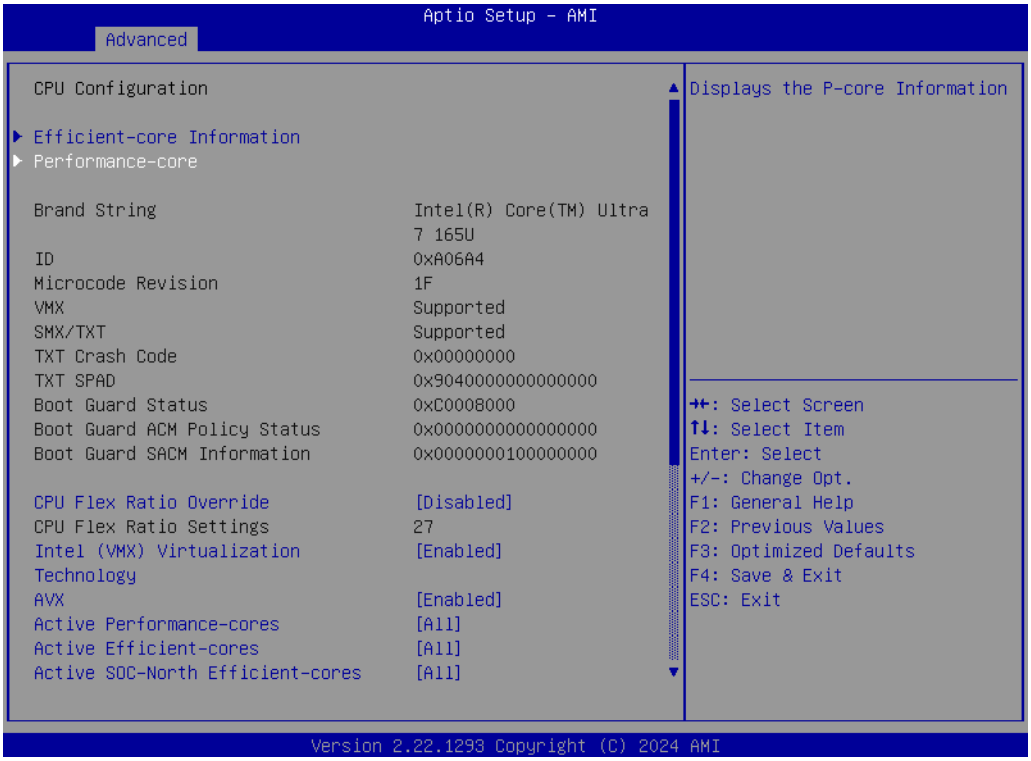
- **AP threads Idle Manner**
  AP threads Idle Manner for waiting signal to run.
- **AES**
  Enable/Disable AES. (Advanced Encryption Standard)
- **MachineCheck**
  Enable/Disable Machine Check.
- **MonitorMWait**
  Enable/Disable MonitorMWait. If Disabled, the AP threads Idle Manner should not be set to MWAIT Loop.
- **Intel Trusted Execution Technology**
  Intel® Trusted Execution Technology Enable utilization of additional hardware capabilities provided by Intel® Trusted Execution Technology. Changes require a full power cycle to take effect
- **Alias Check Request**
  Enable Txt Alias Checking capability. Changes require full Txt capability before it will take effect. It is a one-time only change, and on the next reboot it will be reset.
- **DPR Memory Size (MB)**
  Reserve DPR memory size (0-255) MB.
- **Reset AUX Content**
  Reset TPM Aux content. Txt may not be functional after AUX content gets reset.
- **Total Memory Encryption**
  Configure Total Memory Encryption (TME) to protect DRAM data from physical attacks. When this option is configured as 'Enabled', 'VT-d' option must be 'Enabled'. This option will be grayed out when 'VT-d' option is configured as 'Disabled'.
- **X2APIC Enable**
  Enable/Disable X2APIC Operating Mode. When this option is configured as 'Enabled', 'VT-d' option must be 'Enabled' and 'X2APIC Opt Out' option must be 'Disabled' as well. This option will be grayed out when 'VT-d' option is configured as 'Disabled'.
- **Legacy Game Compatibility Mode**
  When enabled, Pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when LED is off.

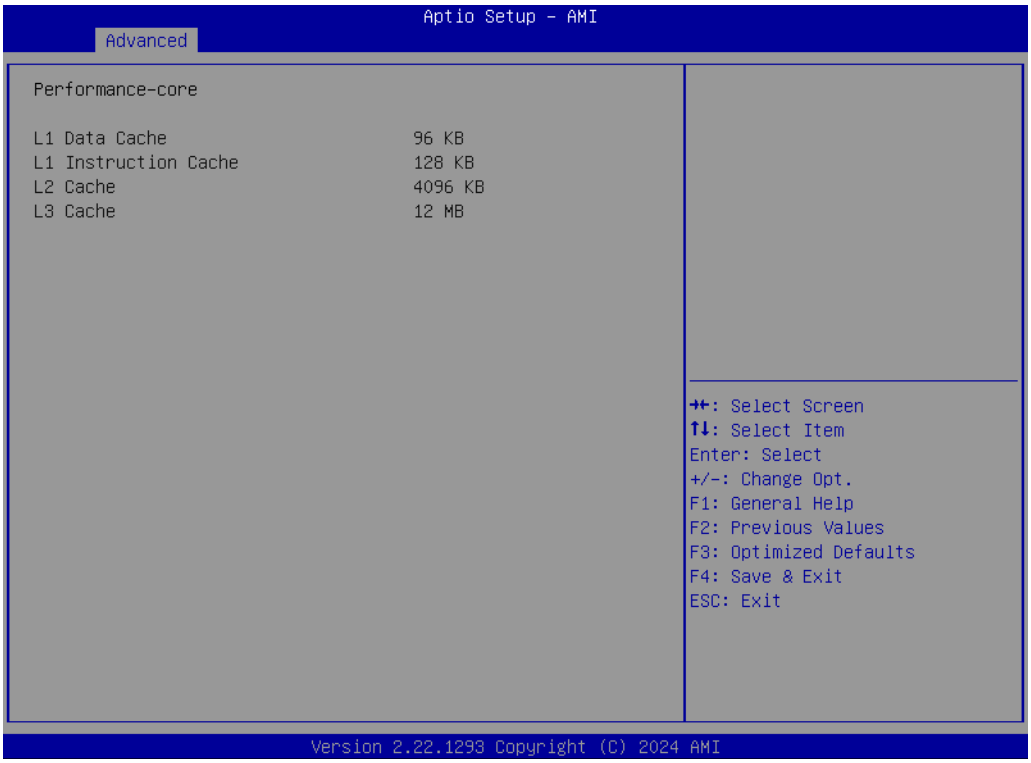
Efficient-core Information



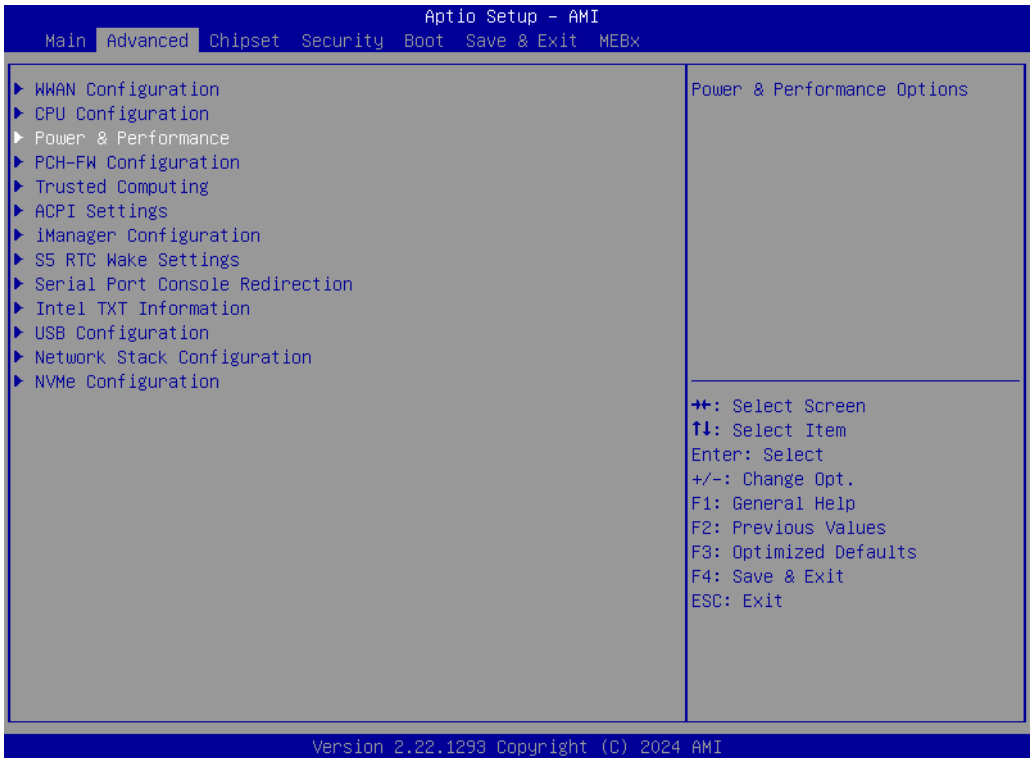


Performance-core





3.2.2.3 Power & Performance

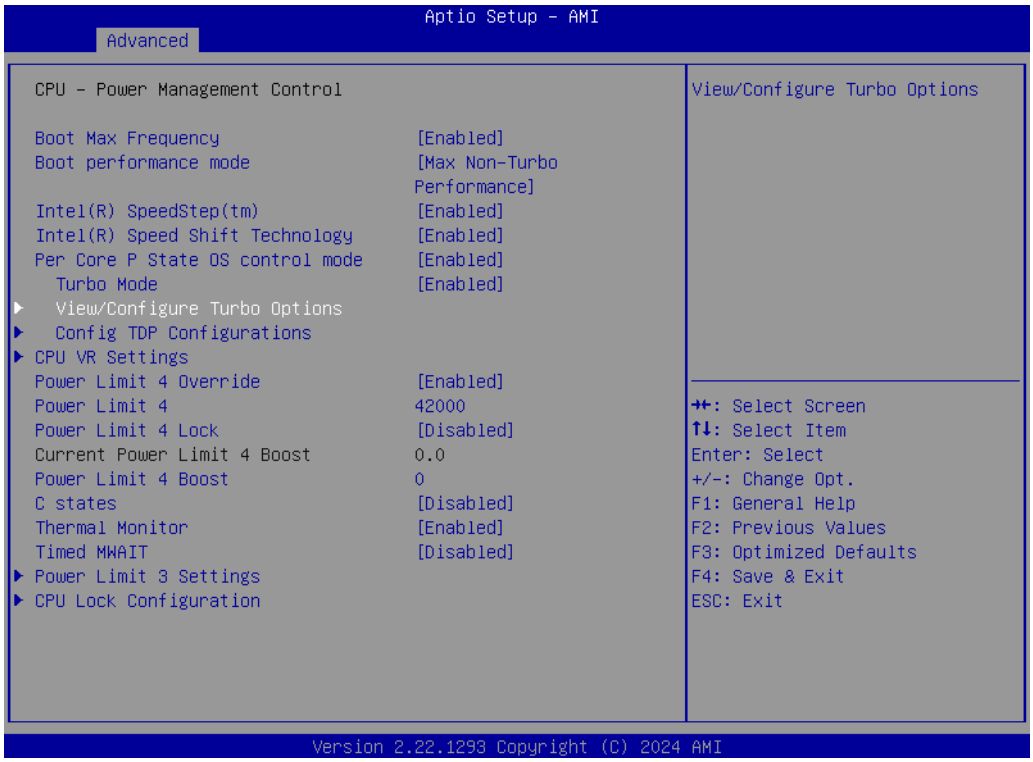


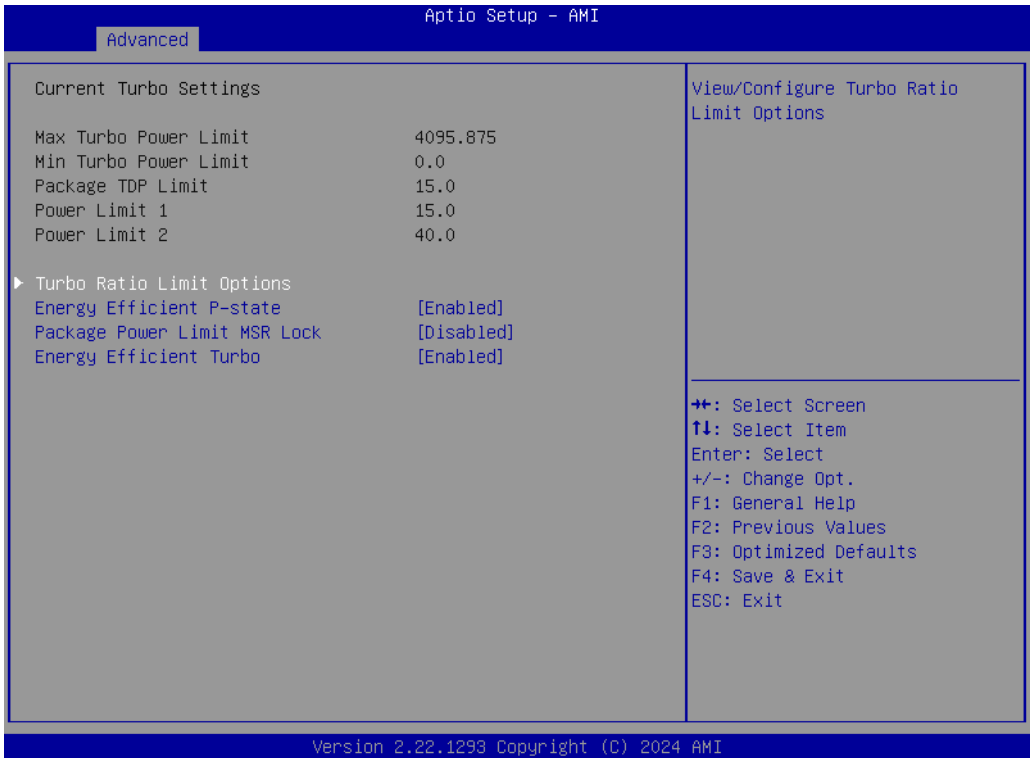
CPU - Power Management Control

- **Boot Max Frequency**
  Enable/Disable Boot Maximum Frequency in CPU strap.
- **Boot performance mode**
  Select the performance state that the BIOS will set before OS hand-off.
- **Intel® Speedstep™**
  Allows more than two frequency ranges to be supported.
- **Intel® Speed 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.
- **Turbo Mode**
  Enable/Disable processor Turbo Mode (requires Intel Speed Step or Intel Speed Shift to be available and enabled).
- **Power Limit 4 Override**
  Enable/Disable Power Limit 4 override.
- **Power Limit 4**
  Power Limit 4 in Milli Watts. BIOS will round to the nearest 1/8W when programming. For 12.50W, enter 12500. If the value is 0, BIOS leaves default value.
- **Power Limit 4 Lock**
  Power Limit 4 Lock. When enabled PL4 configurations are locked during OS. When disabled PL4 configuration can be changed during OS.
- **Power Limit 4 Boots**
  Configure Power Limit 4 Boost in Watts. The value 0 means disable.
- **C states**
  Enable/Disable CPU Power Management.

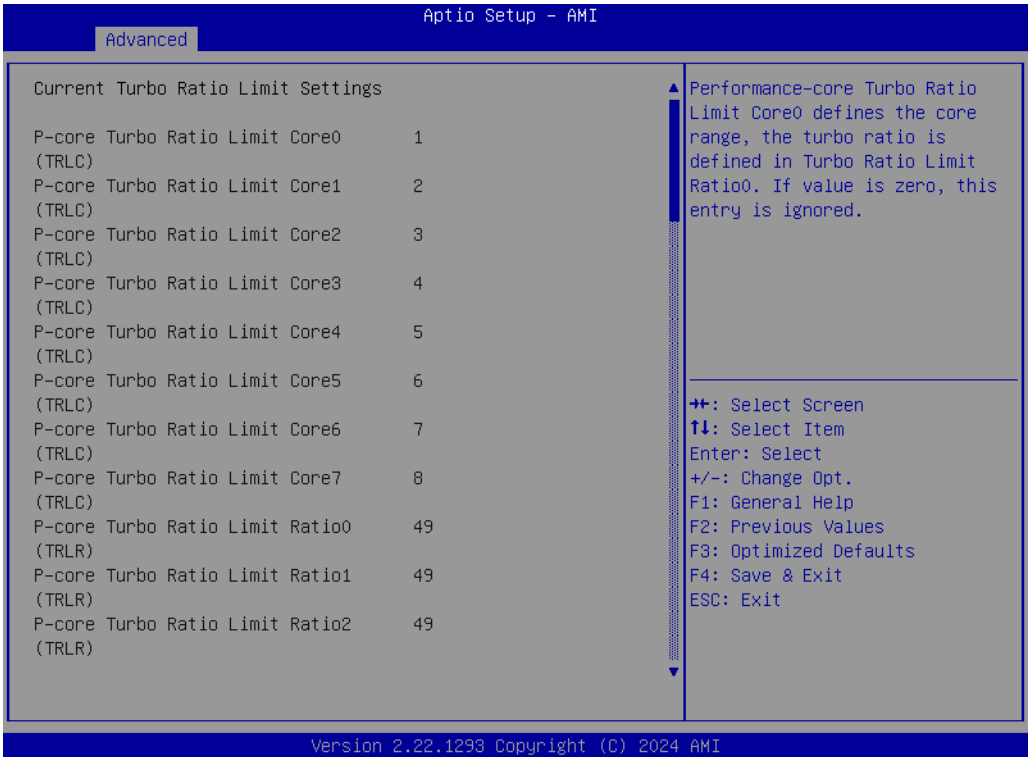
- **Thermal Monitor**
  Enable/Disable Thermal Monitor.
- **Timed MWAIT**
  Enable/Disable Timed MWAIT Support.

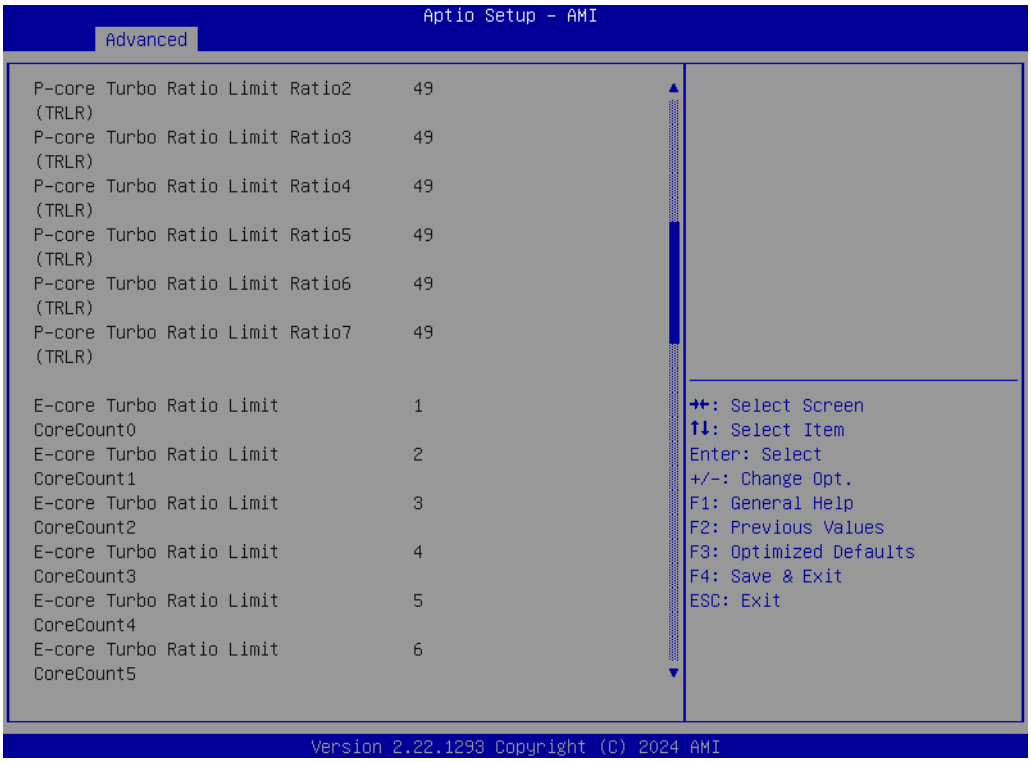
View/Configure Turbo Options

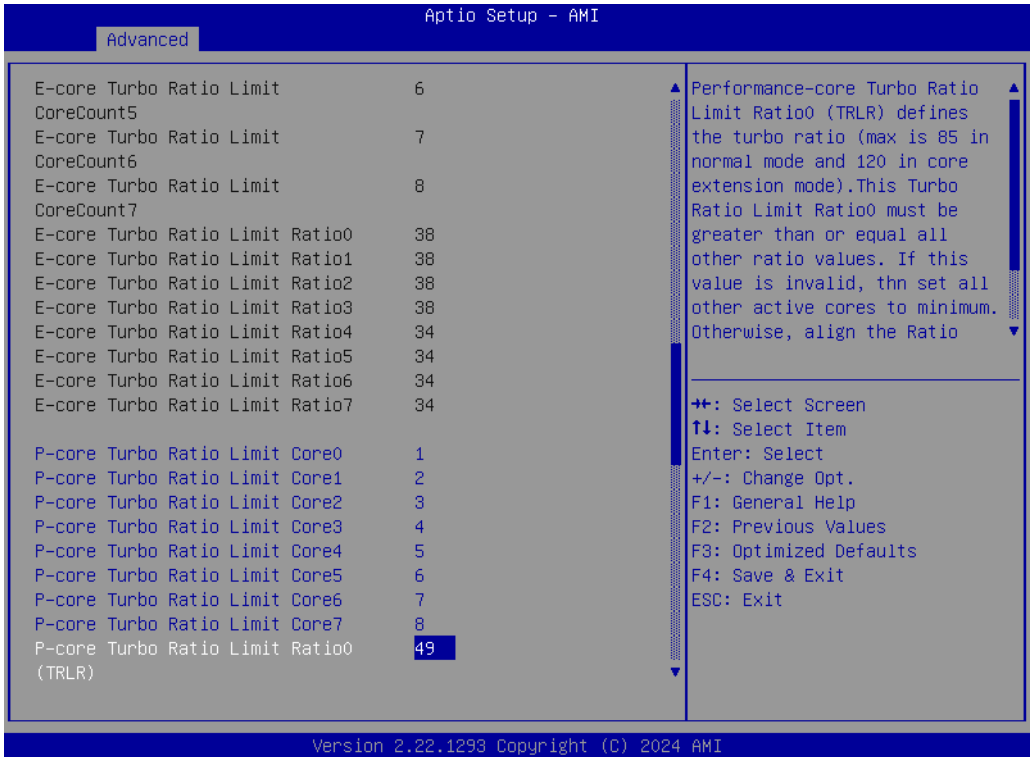


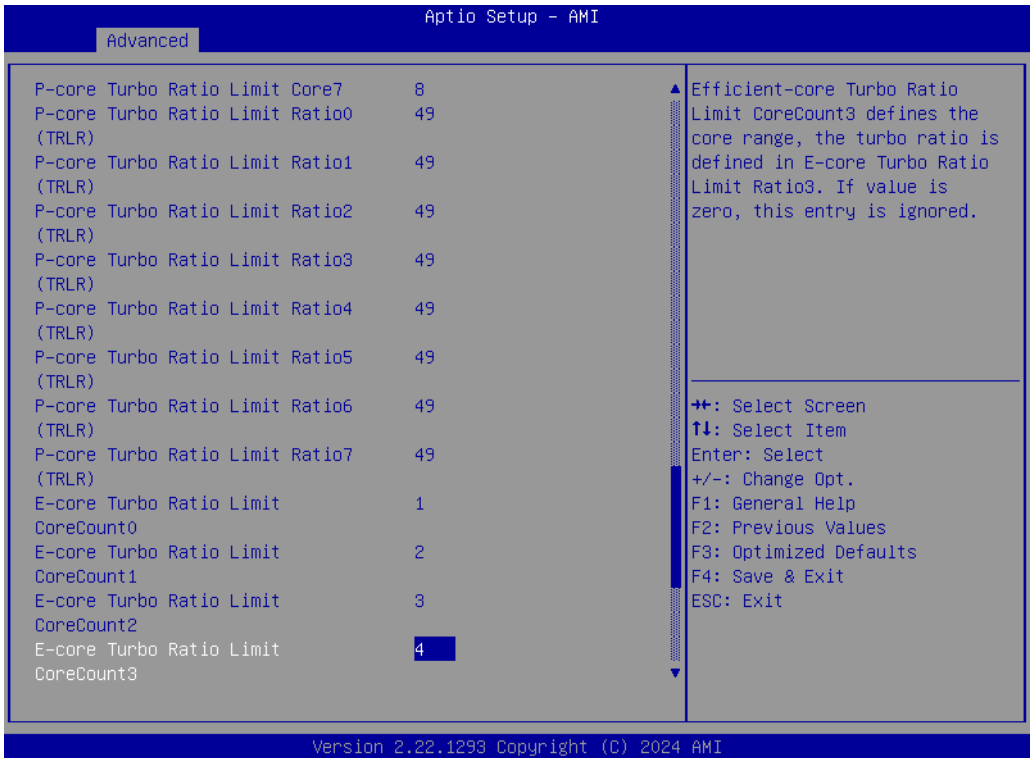


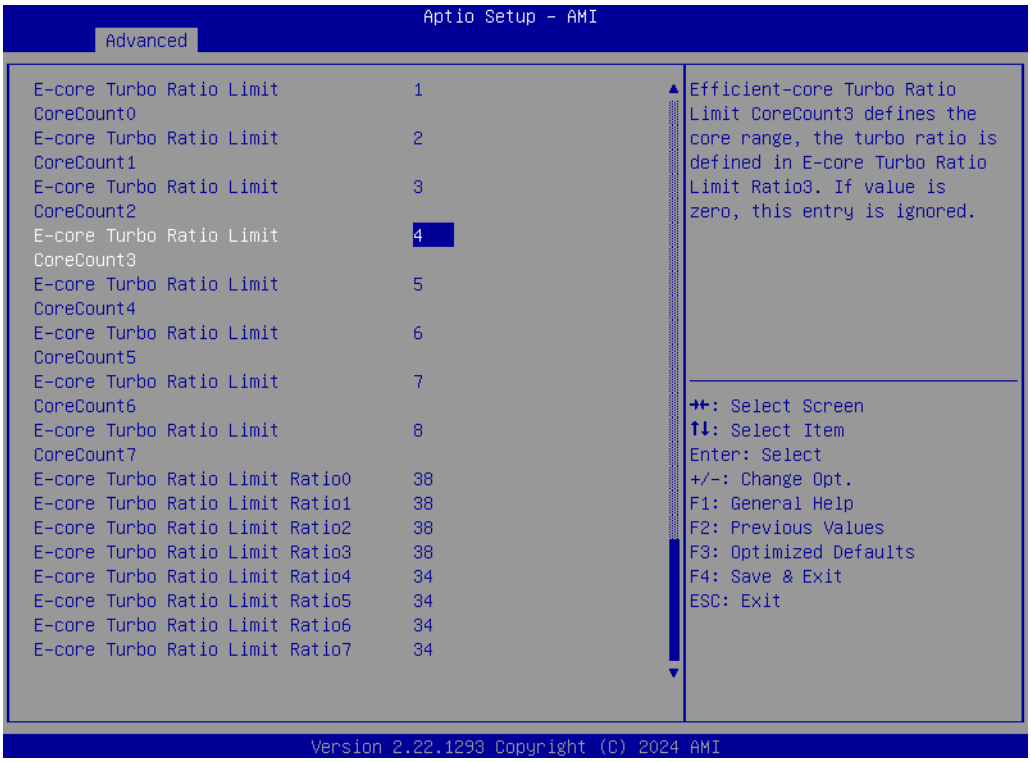
- **Energy Efficient P-state**
  Enable/Disable Energy Efficient P-state feature.
- **Package Power Limit MSR Lock**
  Enable/Disable locking of Package Power Limit settings.
- **Energy Efficient Turbo**
  Enable/Disable Energy Efficient Turbo Feature. This feature will opportunistically lower the turbo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






Aptio Setup – AMI
Advanced
E-core Turbo Ratio Limit CoreCount5 6
E-core Turbo Ratio Limit CoreCount6 7
E-core Turbo Ratio Limit CoreCount7 8
E-core Turbo Ratio Limit Ratio0 38
E-core Turbo Ratio Limit Ratio1 38
E-core Turbo Ratio Limit Ratio2 38
E-core Turbo Ratio Limit Ratio3 38
E-core Turbo Ratio Limit Ratio4 34
E-core Turbo Ratio Limit Ratio5 34
E-core Turbo Ratio Limit Ratio6 34
E-core Turbo Ratio Limit Ratio7 34
P-core Turbo Ratio Limit Core0 1
P-core Turbo Ratio Limit Core1 2
P-core Turbo Ratio Limit Core2 3
P-core Turbo Ratio Limit Core3 4
P-core Turbo Ratio Limit Core4 5
P-core Turbo Ratio Limit Core5 6
P-core Turbo Ratio Limit Core6 7
P-core Turbo Ratio Limit Core7 8
P-core Turbo Ratio Limit Ratio0 (TRLR) 49
Performance-core Turbo Ratio Limit Ratio0 (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode).This Turbo Ratio Limit Ratio0 must be greater than or equal all other ratio values. If this value is invalid, thn set all other active cores to minimum. Otherwise, align the Ratio
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1293 Copyright (C) 2024 AMI


Aptio Setup – AMI
Advanced
P-core Turbo Ratio Limit Core7 8
P-core Turbo Ratio Limit Ratio0 (TRLR) 49
P-core Turbo Ratio Limit Ratio1 (TRLR) 49
P-core Turbo Ratio Limit Ratio2 (TRLR) 49
P-core Turbo Ratio Limit Ratio3 (TRLR) 49
P-core Turbo Ratio Limit Ratio4 (TRLR) 49
P-core Turbo Ratio Limit Ratio5 (TRLR) 49
P-core Turbo Ratio Limit Ratio6 (TRLR) 49
P-core Turbo Ratio Limit Ratio7 (TRLR) 49
E-core Turbo Ratio Limit CoreCount0 1
E-core Turbo Ratio Limit CoreCount1 2
E-core Turbo Ratio Limit CoreCount2 3
E-core Turbo Ratio Limit CoreCount3 4
Efficient-core Turbo Ratio Limit CoreCount3 defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio3. If value is zero, this entry is ignored.
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1293 Copyright (C) 2024 AMI



- **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 value is zero, this entry is ignored.

- **P-Core Turbo Ratio Limit Ratio**

  Performance-core Turbo Ratio Limit Ratio(x) (TRLR) defines the turbo ratio (max is 85 in normal mode and 120 in core extension mode).

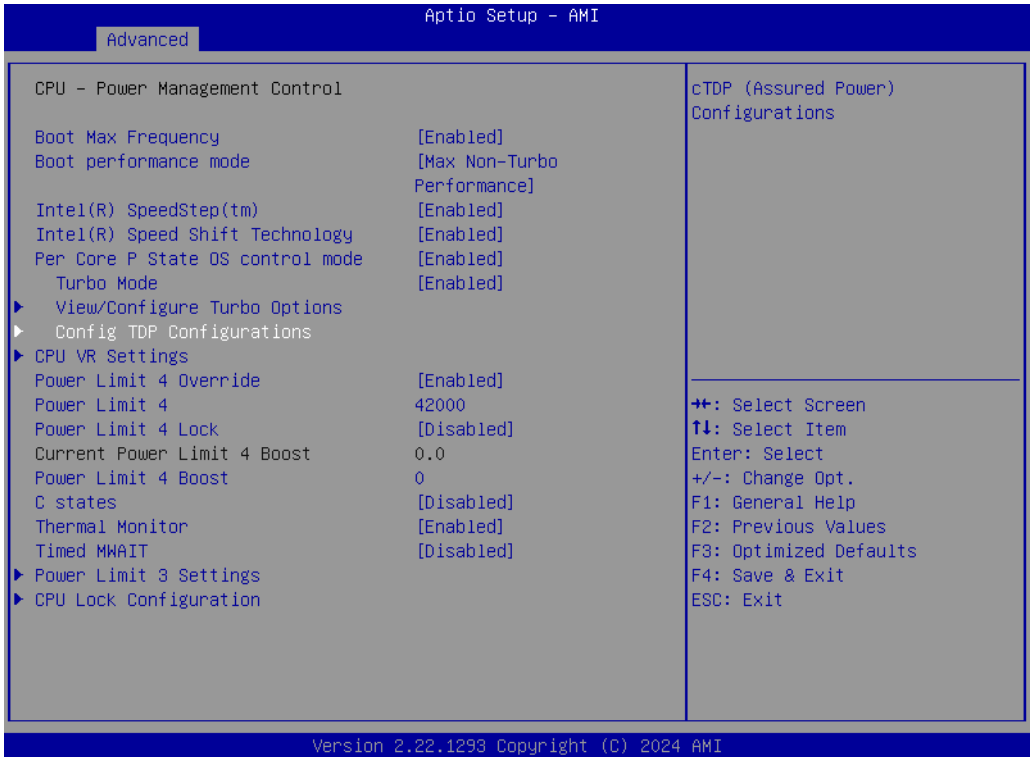
- **E-Core Turbo Ratio Limit CoreCount**

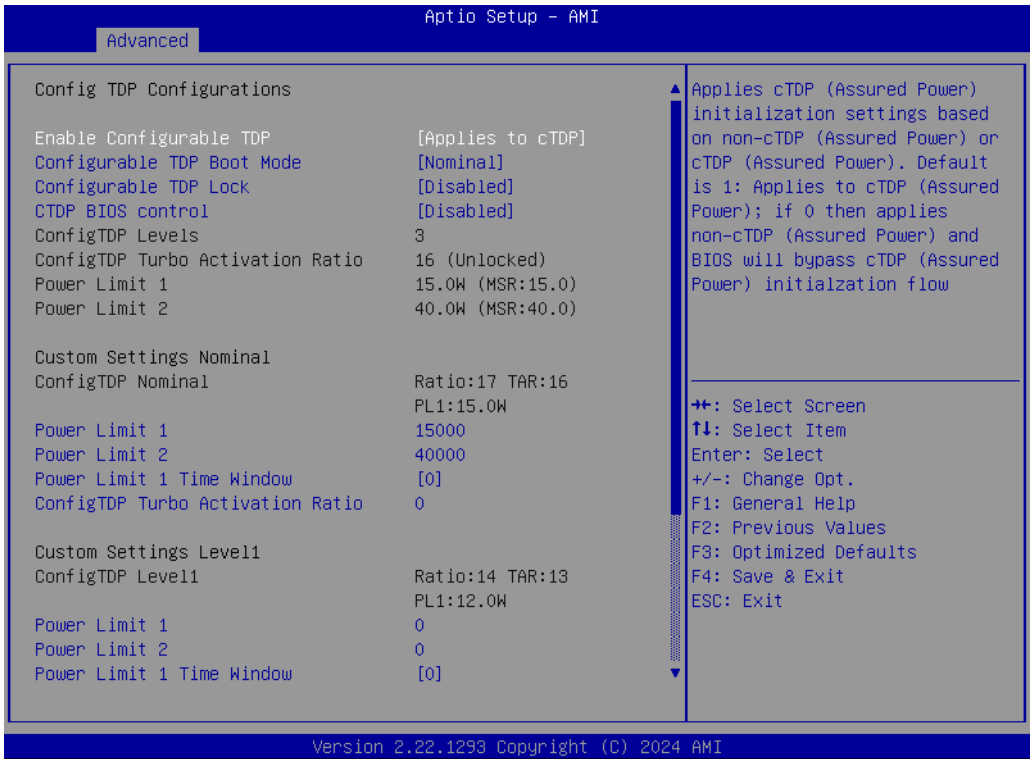
  Efficient-core Turbo Ratio Limit CoreCount(x) defines the core range, the turbo ratio is defined in E-core Turbo Ratio Limit Ratio(x). If value is zero, this entry is ignored.

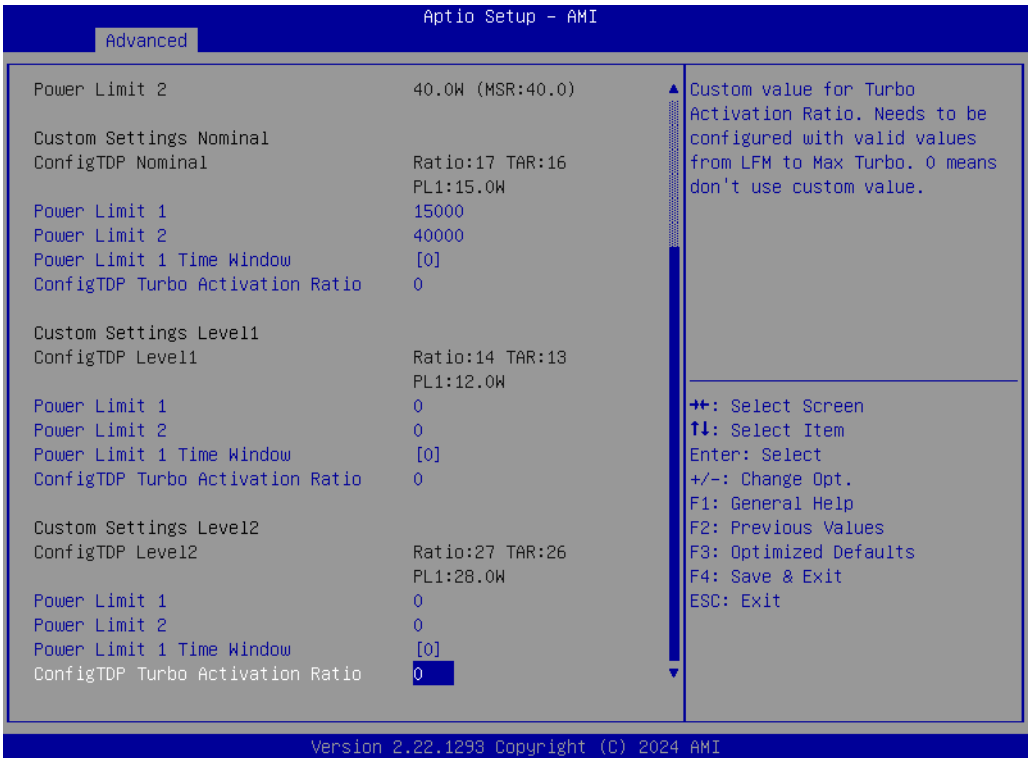
- **E-Core Turbo Ratio Limit Ratio**

  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 TDP Configurations

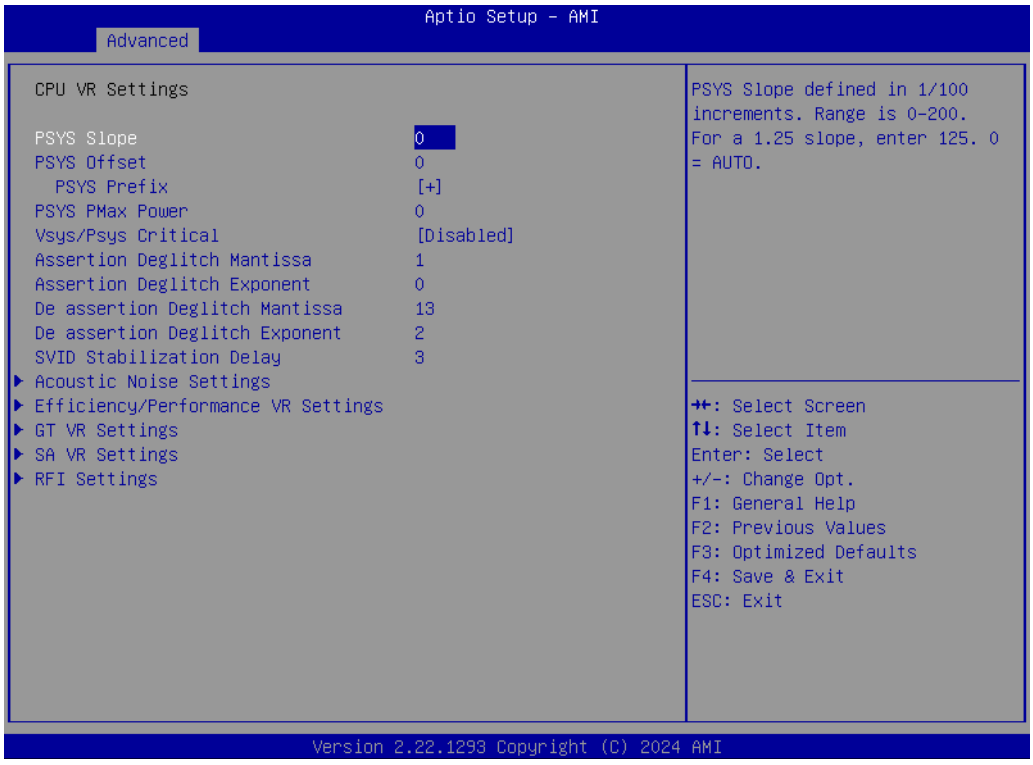






- **Enable Configurable TDP**
  Applies TDP initialization settings based on non-cTDP or cTDP
- **Configurable TDP Boot Mode**
  Configurable TDP Mode as Nominal/Up/Down/Deactivate TDP selection.
- **Configurable TDP Lock**
  Configurable TDP Mode Lock sets the Lock bit.
- **CTDP BIOS control**
  Enables CTDP control via runtime ACPI BIOS method.
- **Power Limit 1**
  Power Limit 1 in Milli Watts.
- **Power Limit 2**
  Power Limit 2 in Milli Watts.
- **Power Limit 1 Time Window**
  Power Limit 1 Time Window value in seconds.
- **ConfigTDP Turbo Activation Ratio**
  Custom value for Turbo Activation Ratio.

CPU VR Settings



- **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.

- **Vsys/Psys Critical**

  Vsys/Psys Critical Enable or disable.

- **Assertion Deglitch Mantissa**

  Assertion Deglitch Mantissa 0x4F[7-3]. Assertion Deglitch = 2µs * Mantissa * 2^(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^(Exponent).

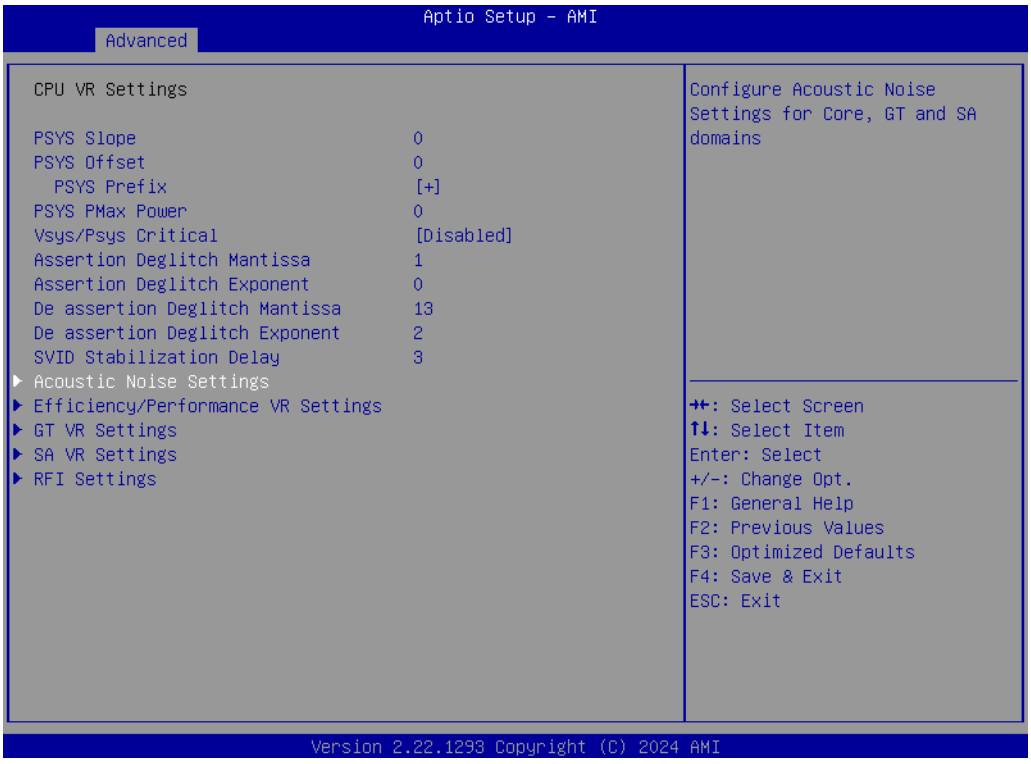
- **De assertion Deglitch Exponent**

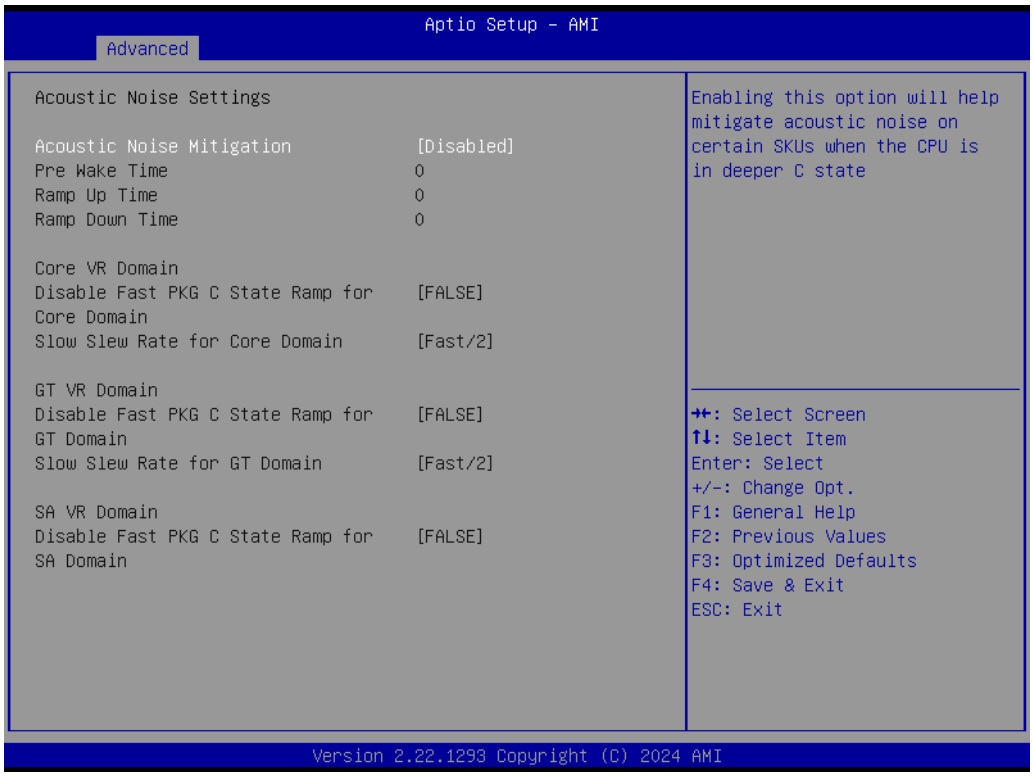
  De Assertion Deglitch Exponent 0x49[3-0]. Assertion Deglitch = 2µs * Mantissa * 2^(Exponent).

- **SVID Stabilization Delay**

  Configure SVID Stabilization Delay (in us) being used for the FVM feature when it is enabled. Note that this delay applies to all SVID domains equally (no unique values possible for IA/GT/SA).

Acoustic Noise Settings





- **Acoustic Noise Mitigation**

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

- **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.

- **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.

- **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.

- **Disable Fast PKG C State Ramp for Core 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.

- **Slow Slew Rate for Core Domain**

  Set VR Core 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.

- **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.

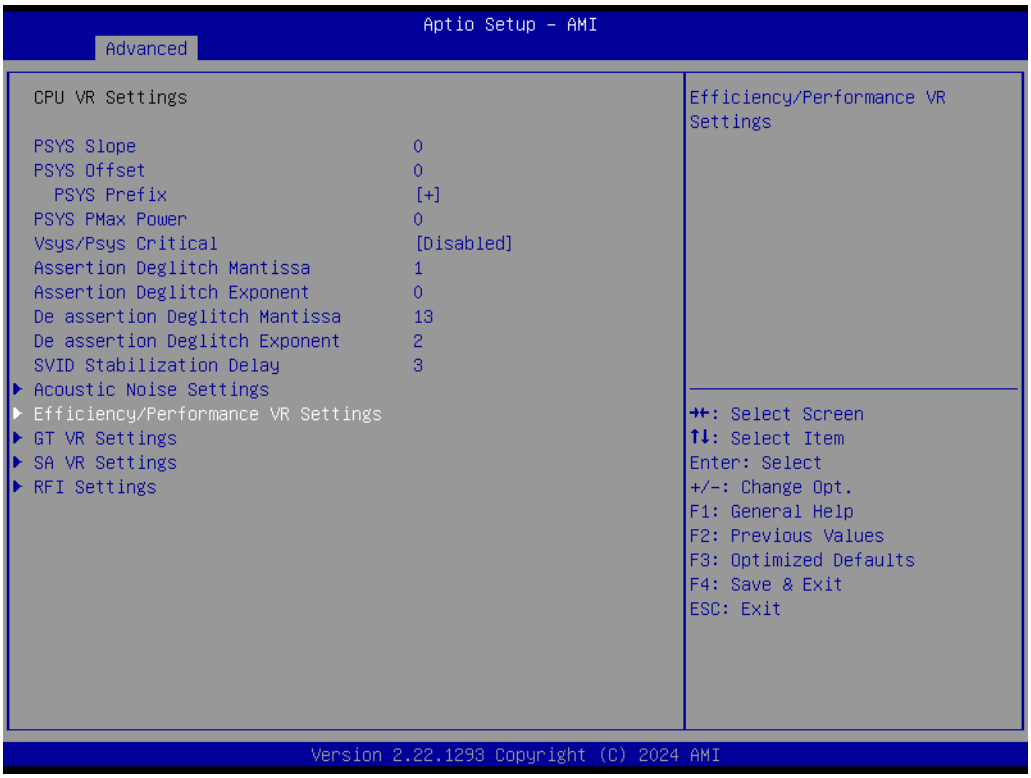
- **Slow Slew Rate for GT Domain**

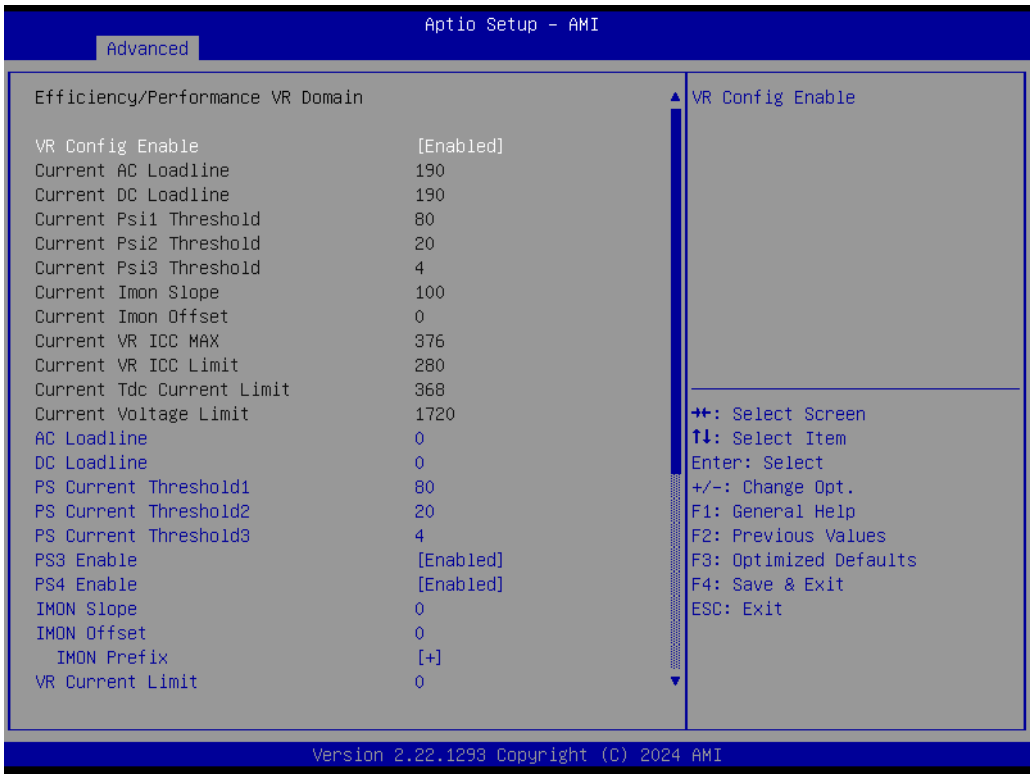
Set VR GT Slow Slew Rate for Deep Package C State ramp time; Slow slew rate equals to Fast divided by number, the number is 2, 4, 8 to slow down the slew rate to help minimize acoustic noise; divide by 16 is disabled.

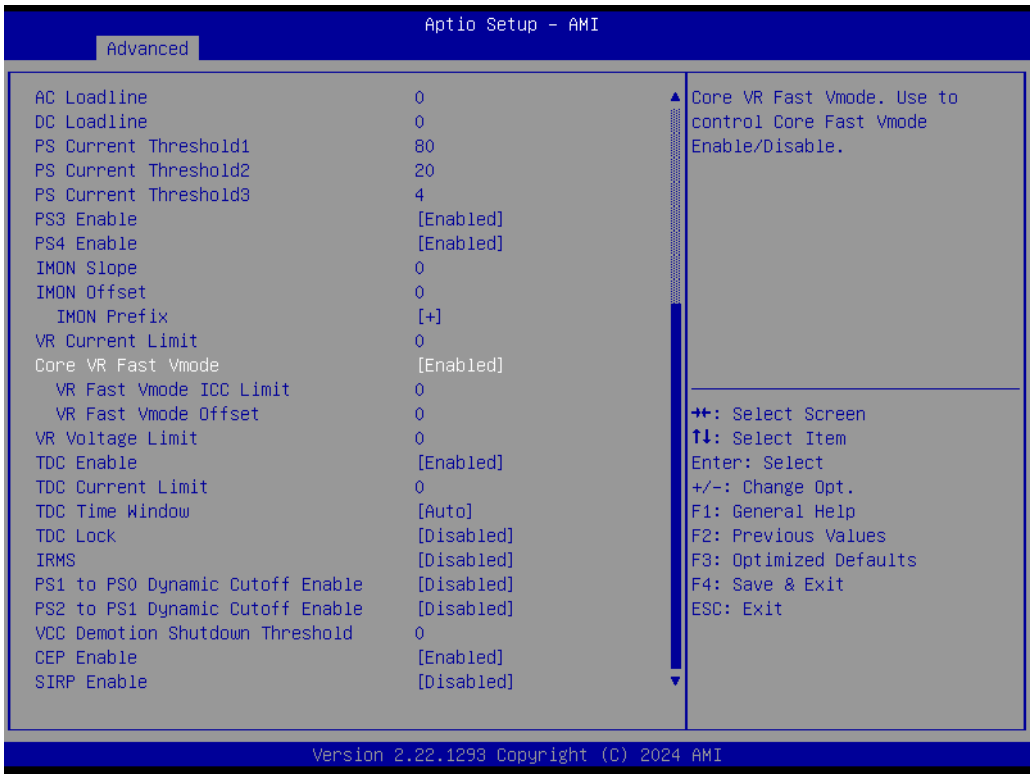
- **Disable Fast PKG C State Ramp for SA Domain**

  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.

Efficiency/Performance VR Settings





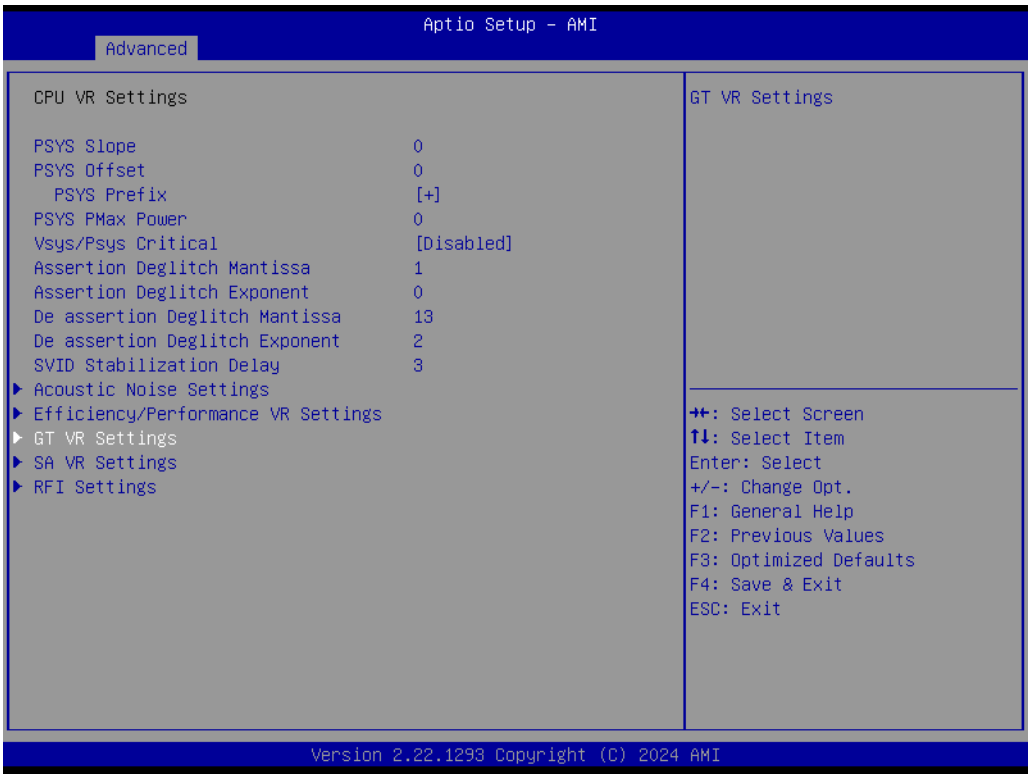


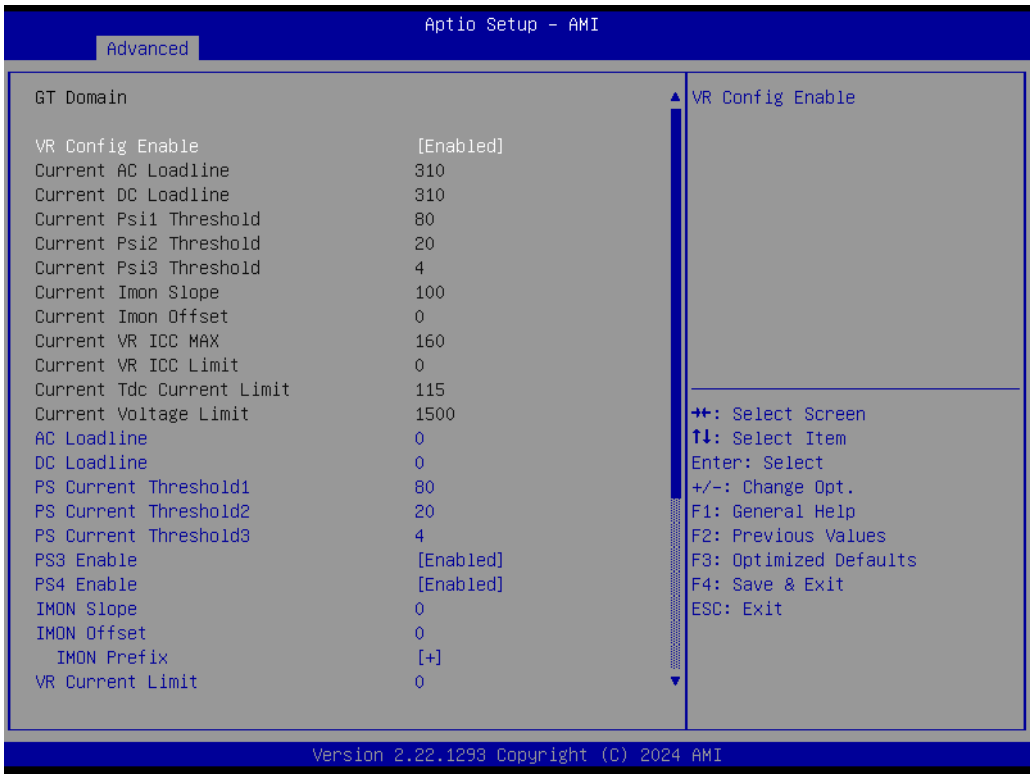
- **VR Config Enable**
  VR Config Enable.
- **PS3 Enable**
  PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
- **PS4 Enable**

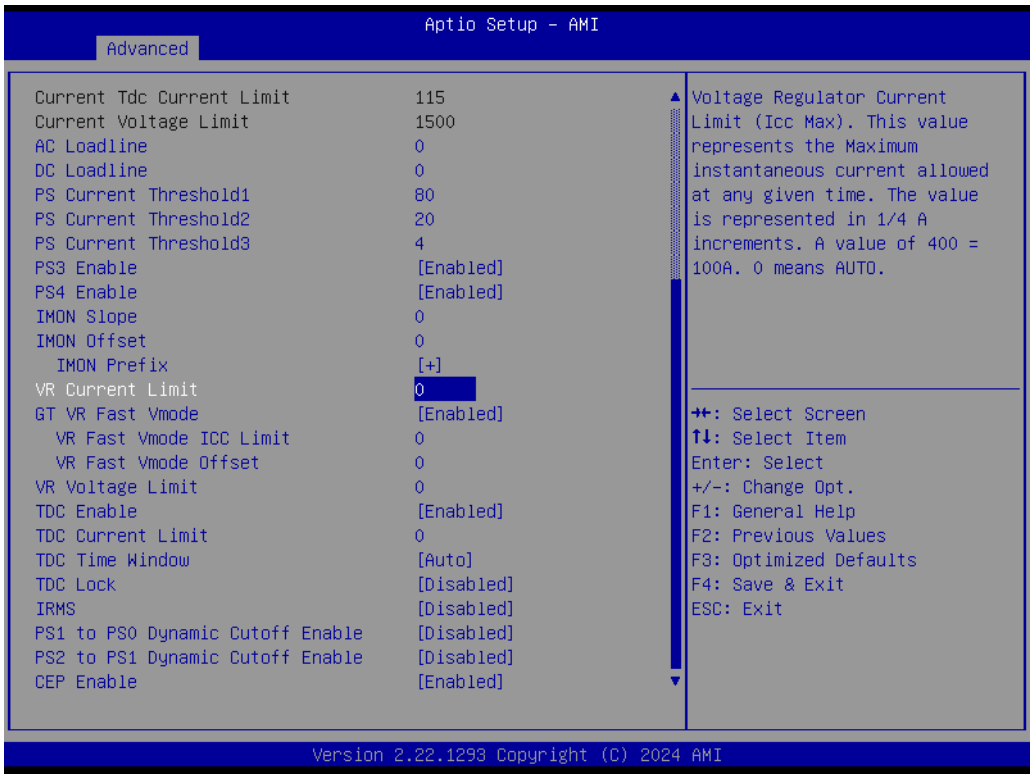
PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.

- **IMON Prefix**
  Sets the offset value as positive or negative.
- **Core VR Fast Vmode**
  Core VR Fast Vmode. Use to control Core Fast Vmode Enable/Disable.
- **TDC Enable**
  TDC Enable. 0- Disable, 1 – Enable
- **TDC Time Window**
  VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.
- **TDC Lock**
  Enable/Disable TDC Lock.
- **IRMS**
  Enable/Disable IRMS - Current root mean square.
- **PS1 to PS0 Dynamic Cutoff Enable**
  PS1 to PS0 Dynamic Cutoff Enable/Disable.
- **PS2 to PS1 Dynamic Cutoff Enable**
  PS2 to PS1 Dynamic Cutoff Enable/Disable.
- **CEP Enable**
  Enable/Disable SIRP (SoC Iccmax Reactive Protection) Support.
- **SIRP Enable**
  Enable/Disable SIRP (SoC Iccmax Reactive Protection) Support

GT VR Settings





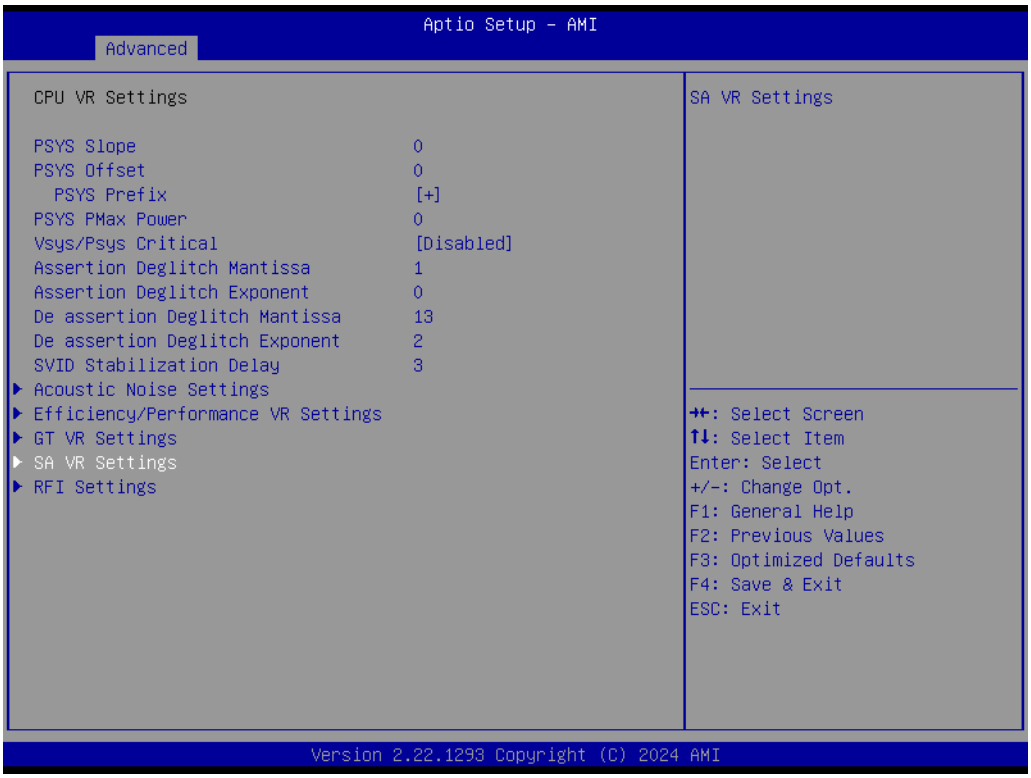


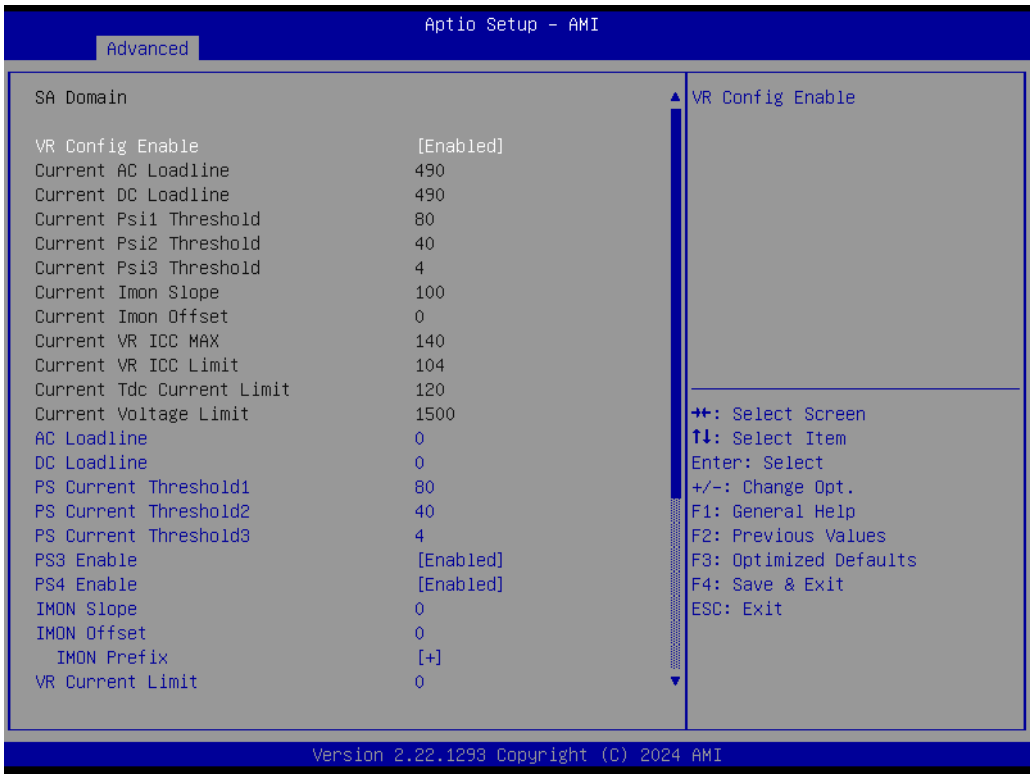
- **VR Config Enable**
  VR Config Enable.
- **PS3 Enable**
  PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
- **PS4 Enable**

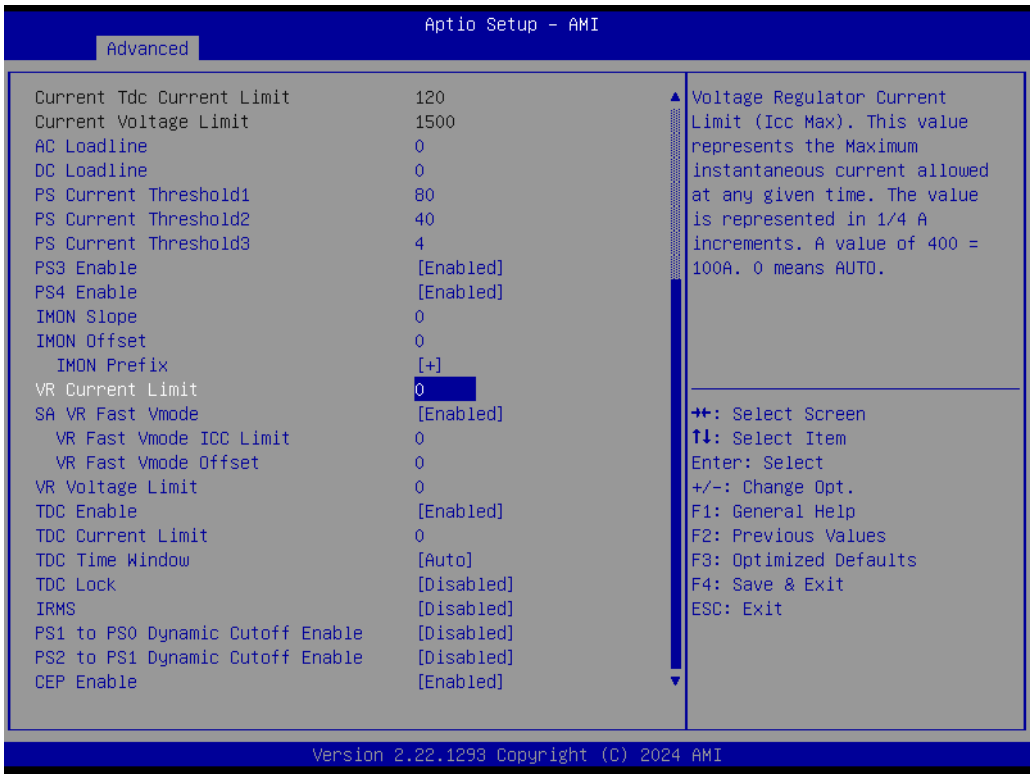
PS4 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.

- **IMON Prefix**
  Sets the offset value as positive or negative.
- **GT VR Fast Vmode**
  GT VR Fast Vmode. Use to control GT Fast Vmode Enable/Disable.
- **TDC Enable**
  TDC Enable. 0- Disable, 1 – Enable
- **TDC Time Window**
  VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.
- **TDC Lock**
  Enable/Disable TDC Lock.
- **IRMS**
  Enable/Disable IRMS - Current root mean square.
- **PS1 to PS0 Dynamic Cutoff Enable**
  PS1 to PS0 Dynamic Cutoff Enable/Disable.
- **PS2 to PS1 Dynamic Cutoff Enable**
  PS2 to PS1 Dynamic Cutoff Enable/Disable.
- **CEP Enable**
  Enable/Disable CEP (Current Excursion Protection) Support.

SA VR Settings





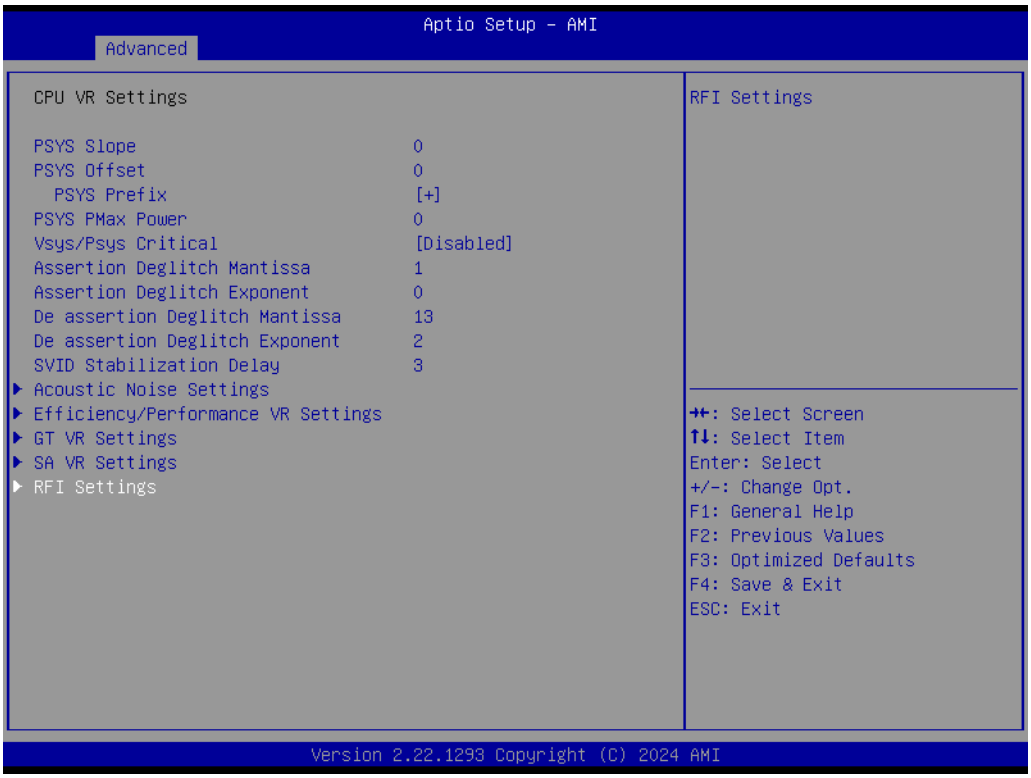


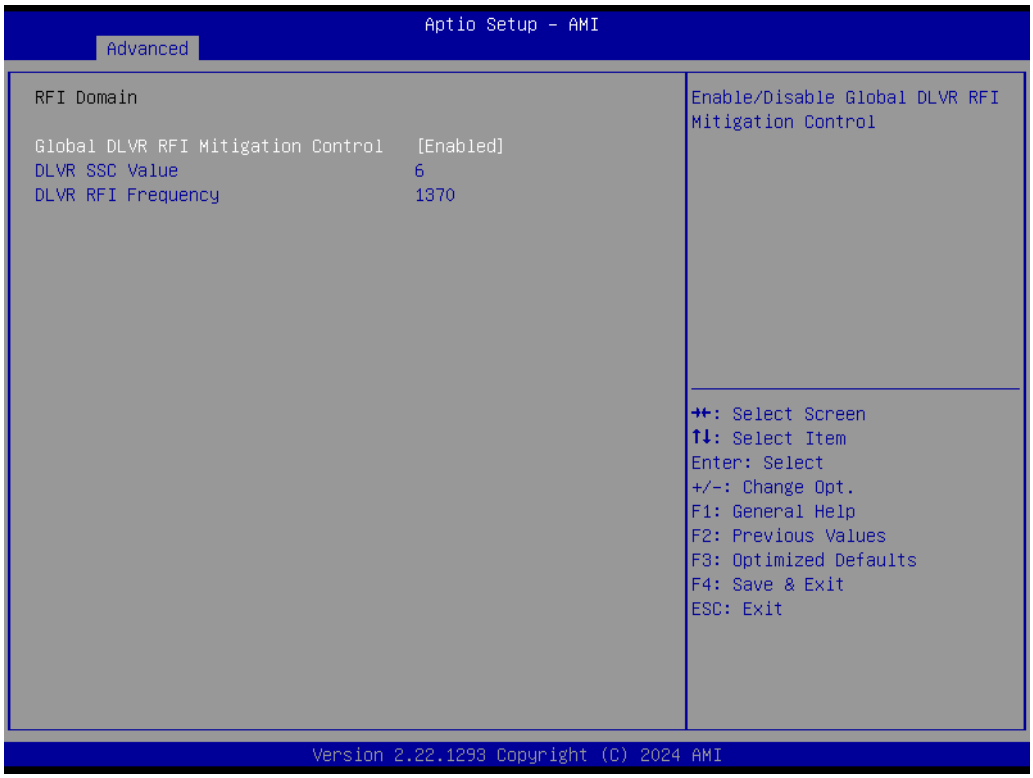
- **VR Config Enable**
  VR Config Enable.
- **PS3 Enable**
  PS3 Enable/Disable. 0 - Disabled, 1 - Enabled. Uses BIOS VR mailbox command 0x3.
- **PS4 Enable**

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

- **IMON Prefix**
  Sets the offset value as positive or negative.
- **SA VR Fast Vmode**
  SA VR Fast Vmode. Use to control SA Fast Vmode Enable/Disable.
- **TDC Enable**
  TDC Enable. 0- Disable, 1 – Enable
- **TDC Time Window**
  VR TDC Time Window, value in seconds. 1s is default. Range from 1s to 448s.
- **TDC Lock**
  Enable/Disable TDC Lock.
- **IRMS**
  Enable/Disable IRMS - Current root mean square.
- **PS1 to PS0 Dynamic Cutoff Enable**
  PS1 to PS0 Dynamic Cutoff Enable/Disable.
- **PS2 to PS1 Dynamic Cutoff Enable**
  PS2 to PS1 Dynamic Cutoff Enable/Disable.
- **CEP Enable**
  Enable/Disable CEP (Current Excursion Protection) Support.

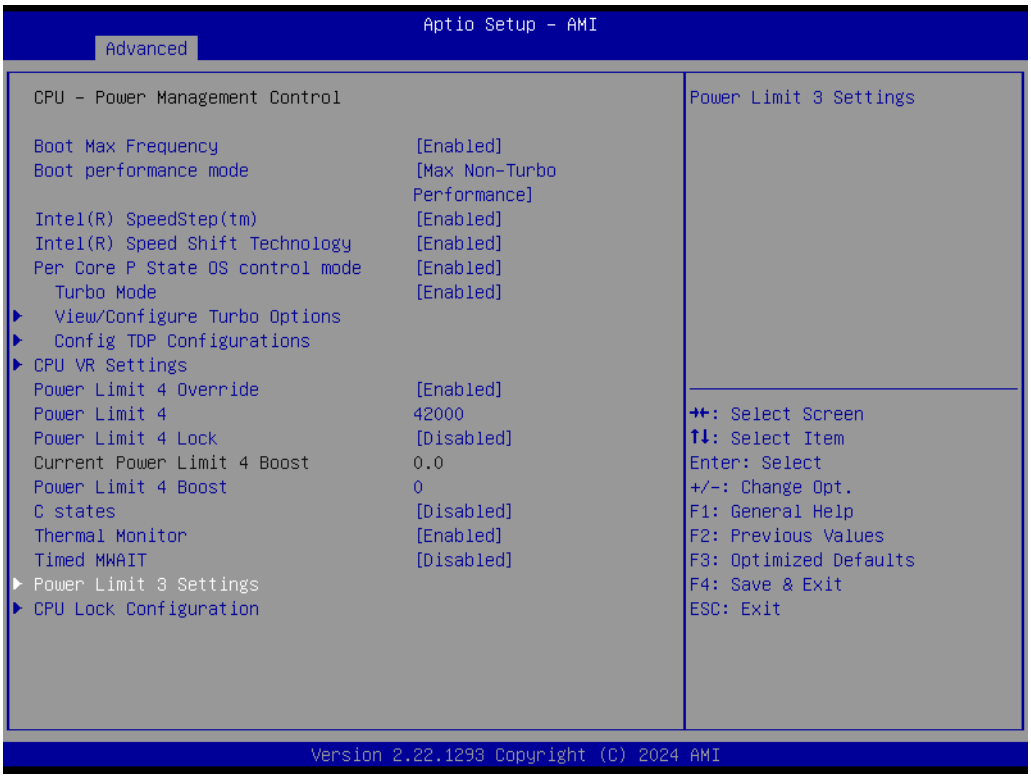
RFI Settings





- **Global DLVR RFI Mitigation Control**
  Enable/Disable Global DLVR RFI Mitigation Control.
- **DLVR SSC Value**
  DLVR SSC in percentage with multiple of 0.25%. 0 = 0%, 31 = 7.75%.
- **DLVR RFI Frequency**
  DLVR RFI Frequency in MHz.

Power Limit 3 Settings



- **Power Limit 3 Override**
  Enable/Disable Power Limit 3 override.
- **Power Limit 3**
  Power Limit 3 in Milli Watts/Percent. BIOS will round to the nearest 1/8W when programming. For example, if 12.50W, enter 12500, if 12%, enter 12000, if 50%, enter 50000. If the value is 0, BIOS leaves the hardware default value.

- **Power Limit 3 Time Window**

  Power Limit 3 Time Window value in Milli seconds. The value may vary from 3 to 64(max). Indicates the time window over which Power Limit 3 value should be maintained. If the value is 0, BIOS leaves the hardware default value.

- **Power Limit 3 Duty Cycle**

  Specify the duty cycle in percentage that the CPU is required to maintain over the configured time window. Range is 0-100.

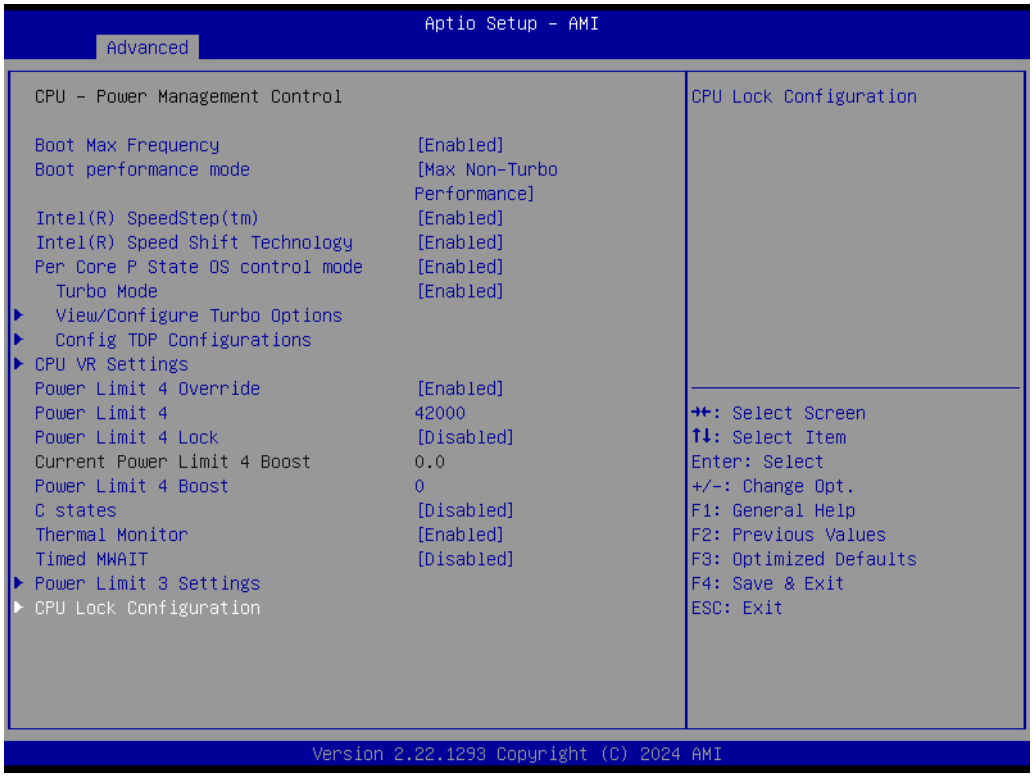
- **Response Mode**

  Use Response Mode to adjust Psys_PL3 power reduction behavior. Battery-enabled systems use Gradual Power Reduction.

- **Power Limit 3 Lock**

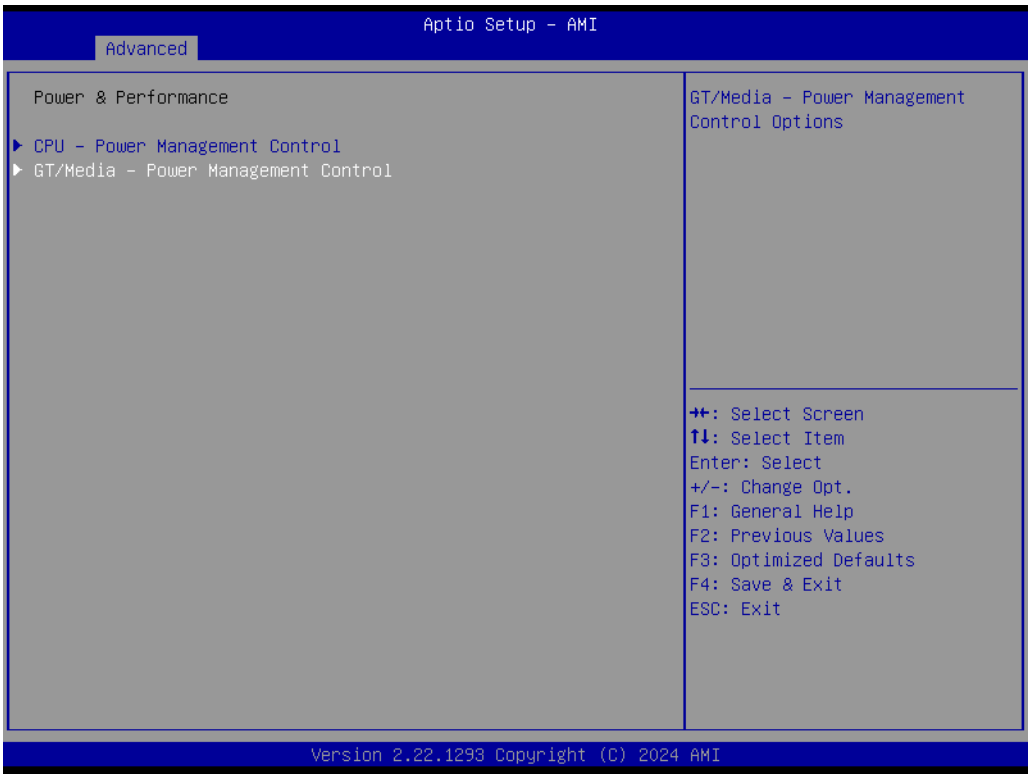
  Power Limit 3 Lock. When enabled PL3 configurations are locked during OS. When disabled PL3 configuration can be changed during OS.

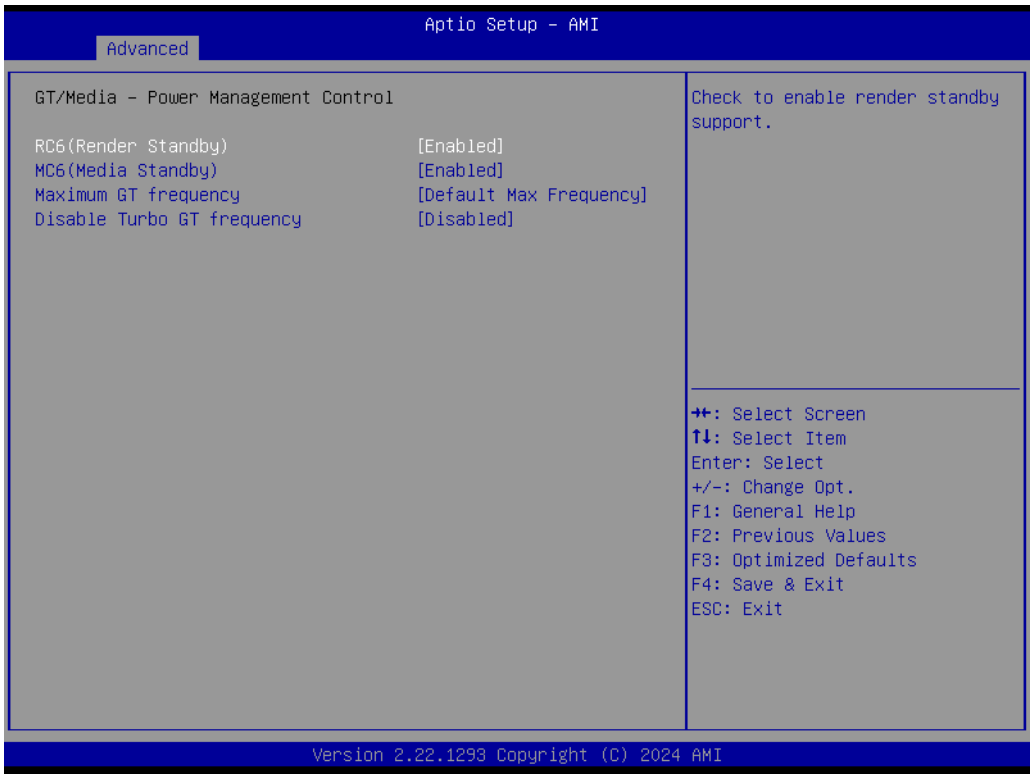
CPU Lock Configuration



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

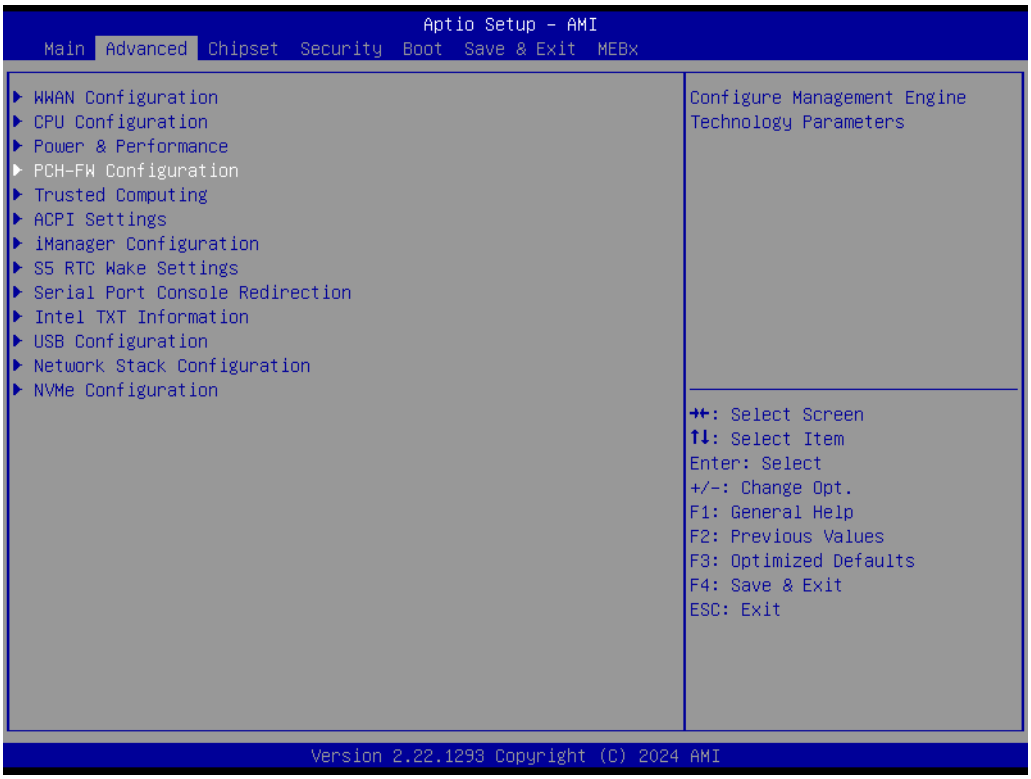
GT/Media - Power Management Control

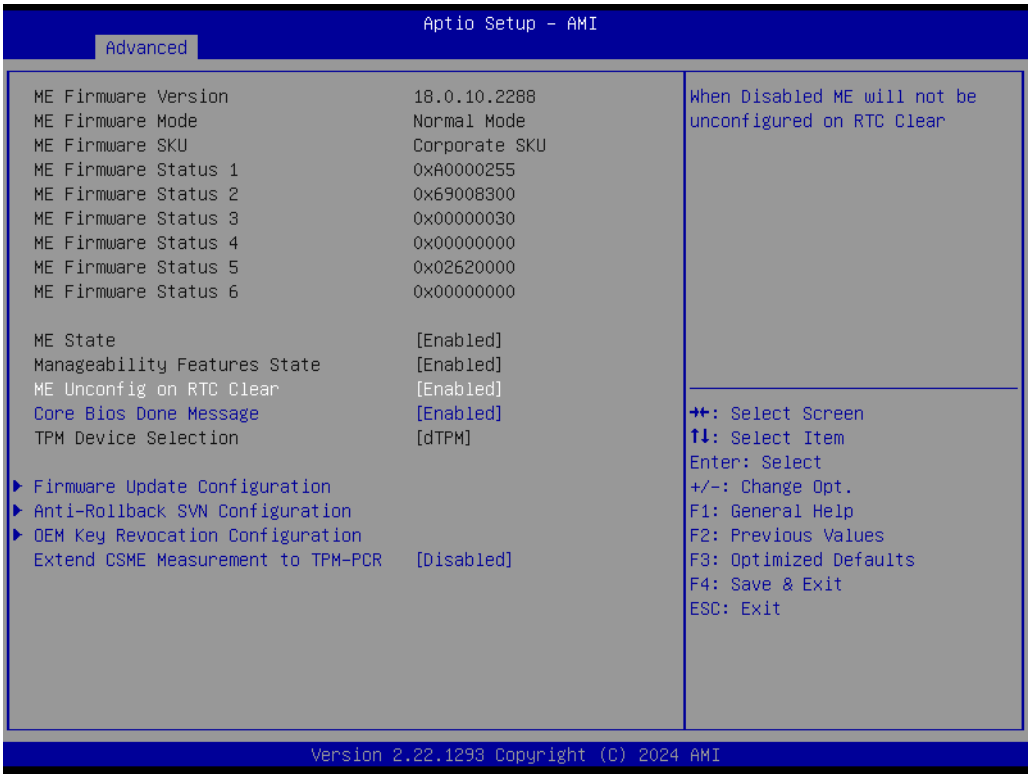




- **RC6 (Render Standby)**
  Check to enable render standby support.
- **MC6 (Media Standby)**
  Check to enable Media standby support.
- **Maximum GT frequency**
  Maximum GT frequency limited by the user.
- **Disable Turbo GT frequency**
  Enabled: Disables Turbo GT frequency. Disabled: GT frequency is not limited.

3.2.2.4 PCH-FW Configuration



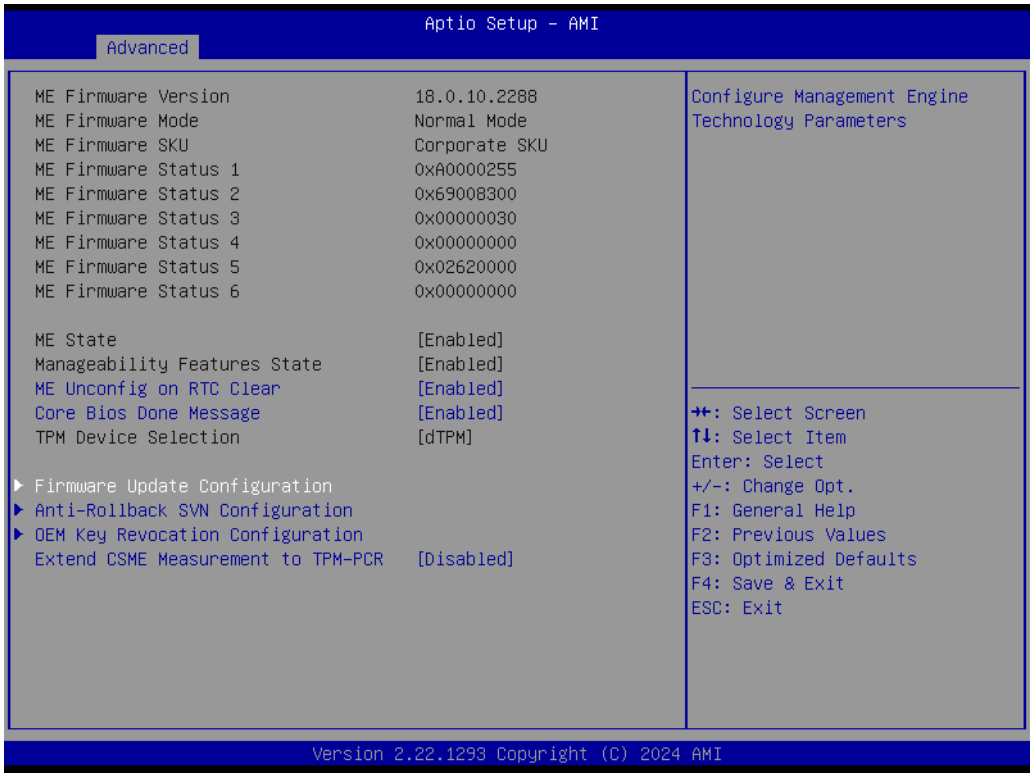


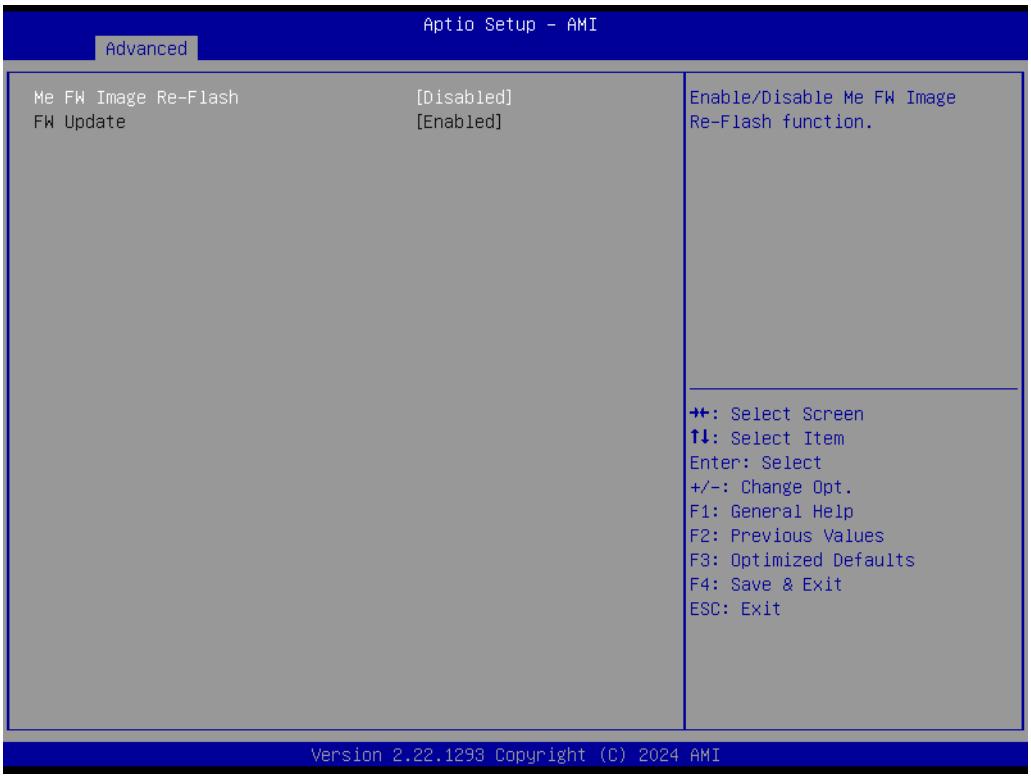
- **ME State**
  When Disabled, ME will be put into ME Temporarily Disabled Mode.
- **Manageability Features State**
  When Disabled, ME will not be unconfigured on RTC Clear.
- **ME Unconfig on RTC Clear**

When Disabled, ME will not be unconfigured on RTC Clear.

- **Core BIOS Done Message**
  Enable/Disable Core BIOS Done message sent to ME.
- **TPM Device Selection**
  Selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr dTPM 1.2 - Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost.
- **Extend CSME Measurement to TPM-PCR**
  Enable/Disable Extend CSME Measurement to TPM-PCR[0] and AMT Config to TPM-PCR[1].

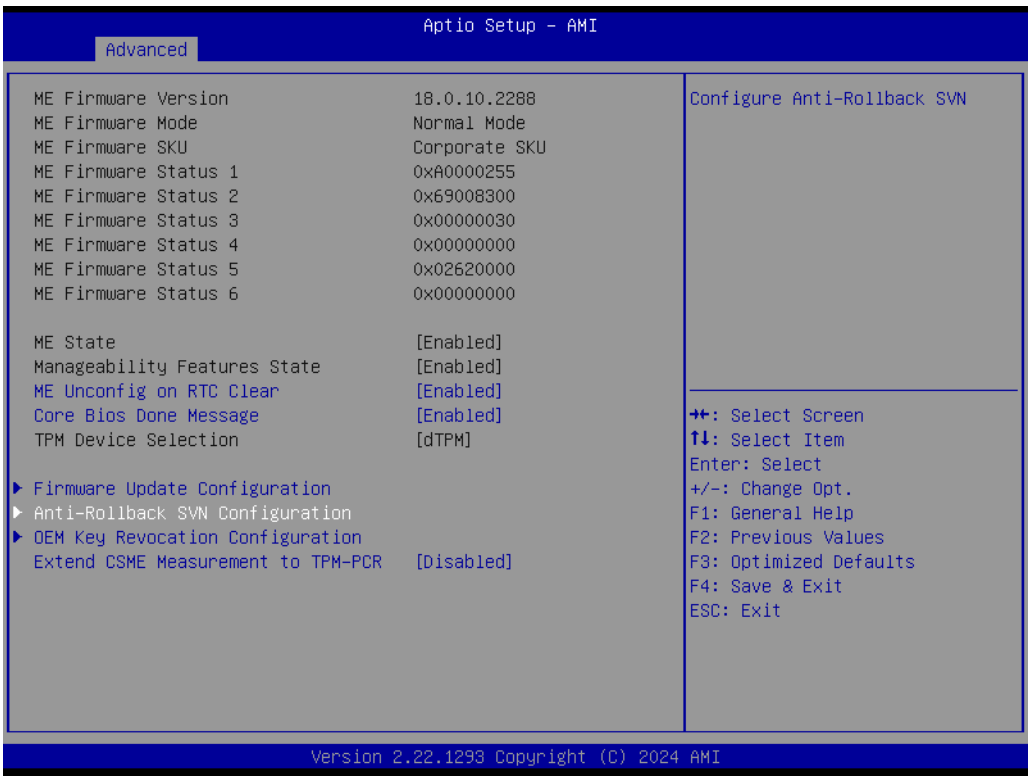
Firmware Update Configuration

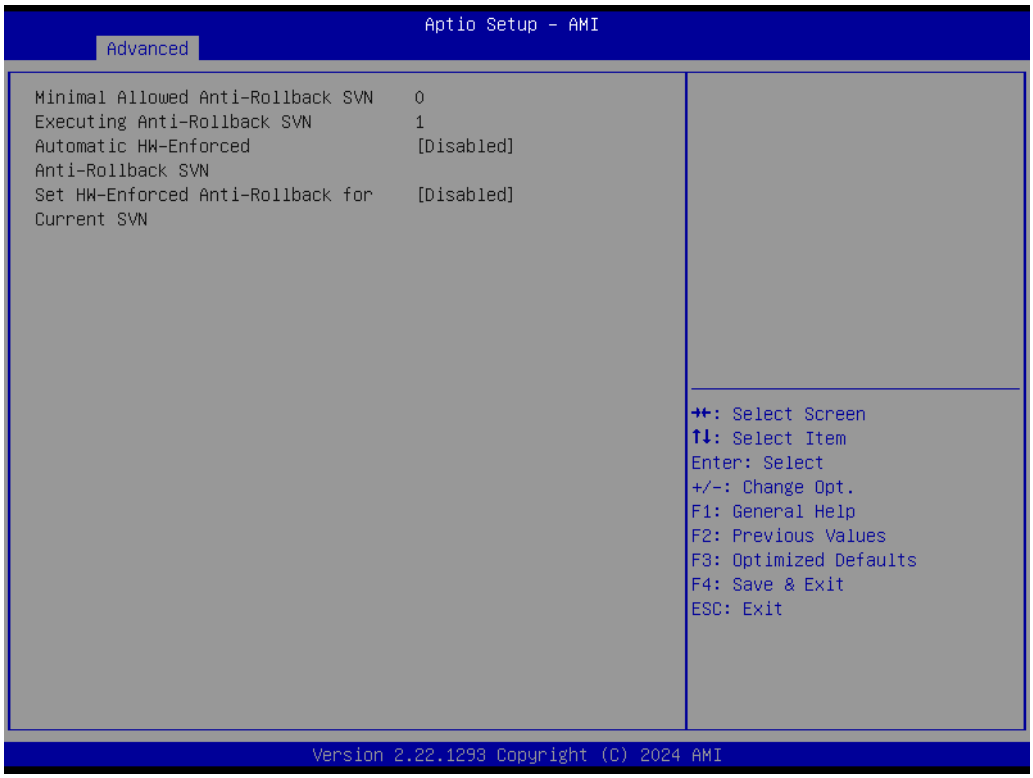




- **ME FW Image Re-Flash**
  Enable/Disable ME FW Image Re-Flash function.
- **FW Update**
  Enable/Disable ME FW Update function

Anti-Rollback SW Configuration





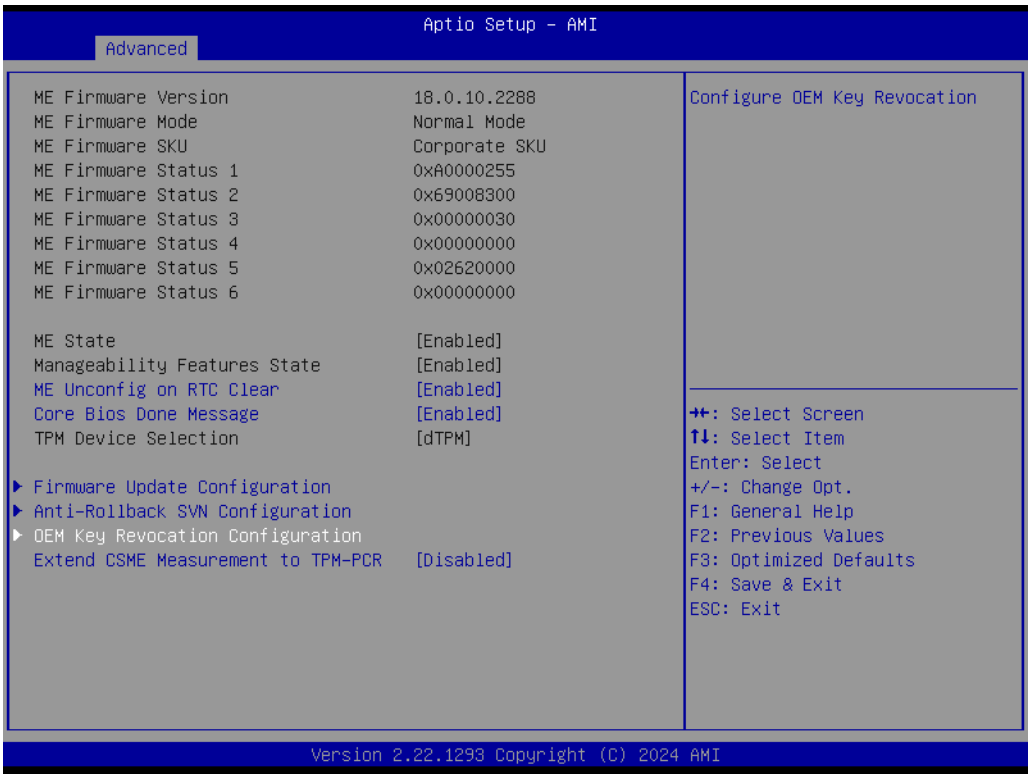
- **Automatic HW-Enforced Anti-Rollback SVN**

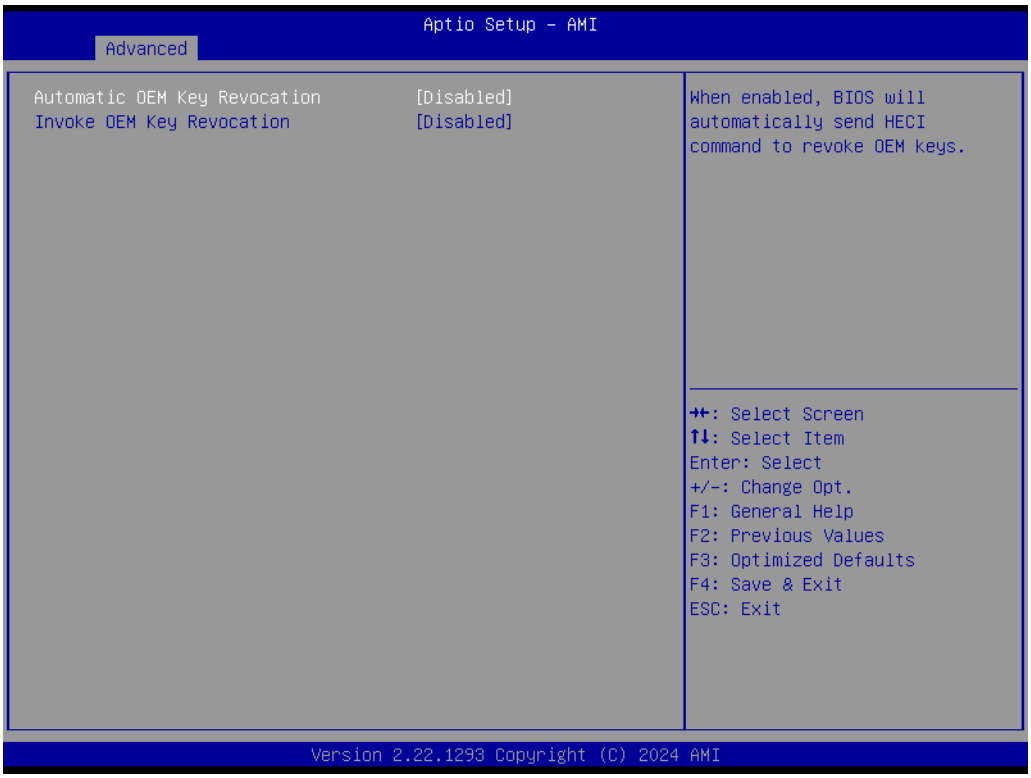
  When enabled hardware-enforced Anti-Rollback mechanism is automatically activated: once ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution.

- **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.

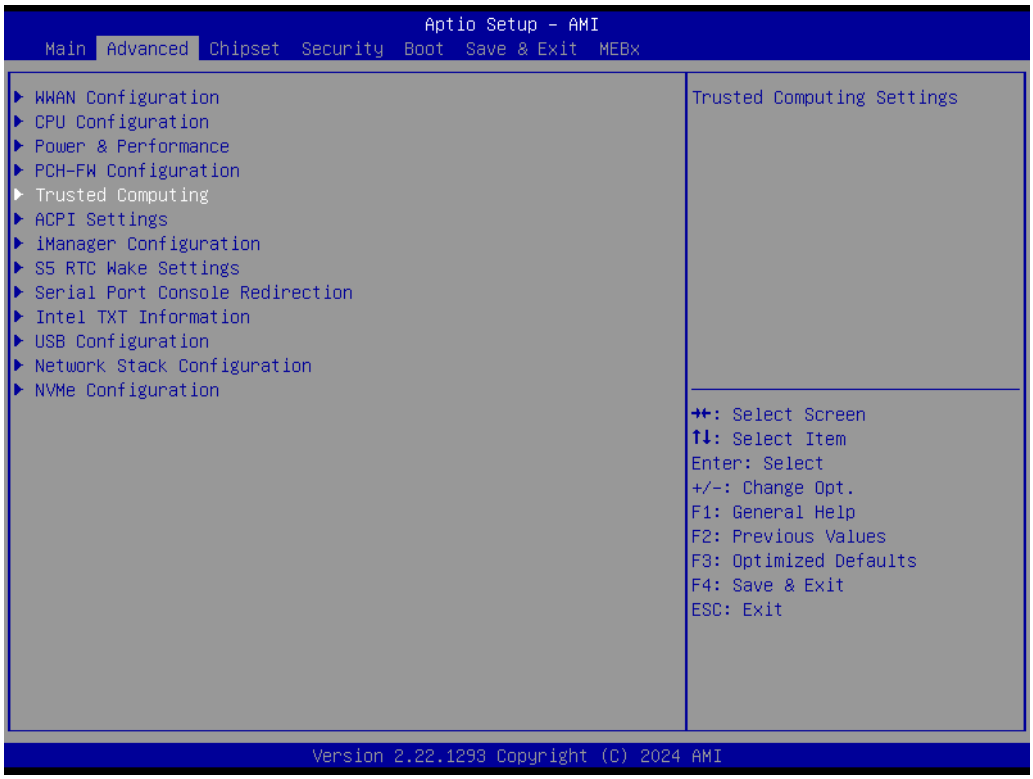
OEM Key Revocation Configuration

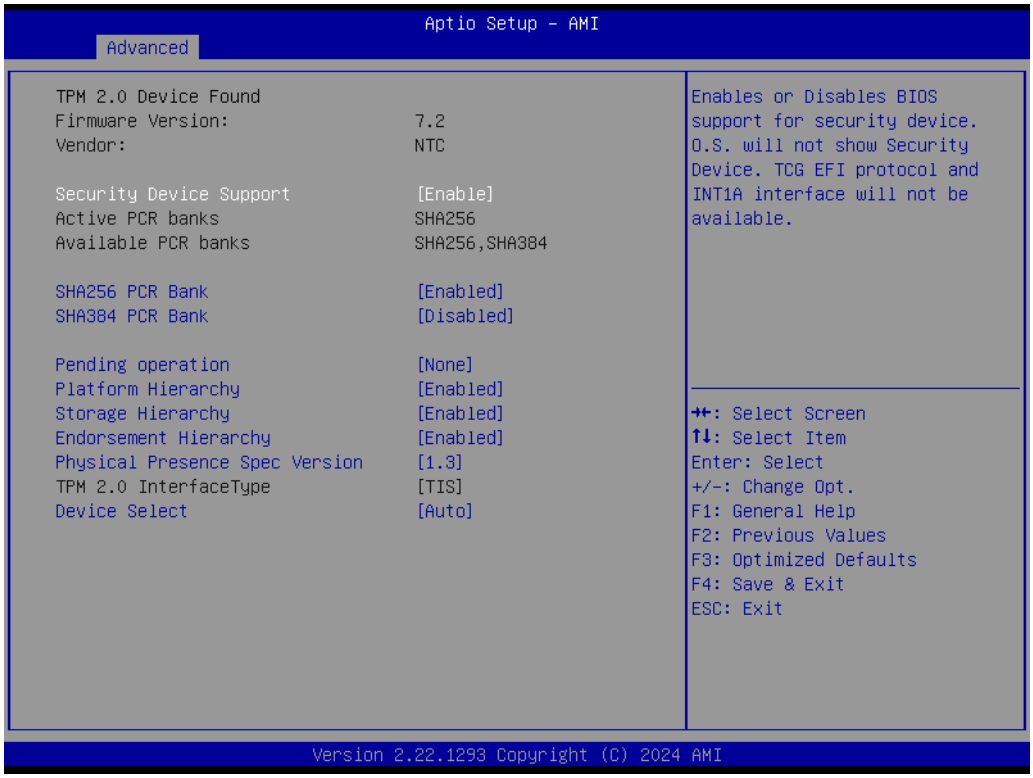




- **Automatic OEM Key Revocation**
  When enabled, the BIOS will automatically send HECI command to revoke OEM keys.
- **Invoke OEM Key Revocation**
  A Heci command will be send to revoke the OEM key.

3.2.2.5 Trusted Computing



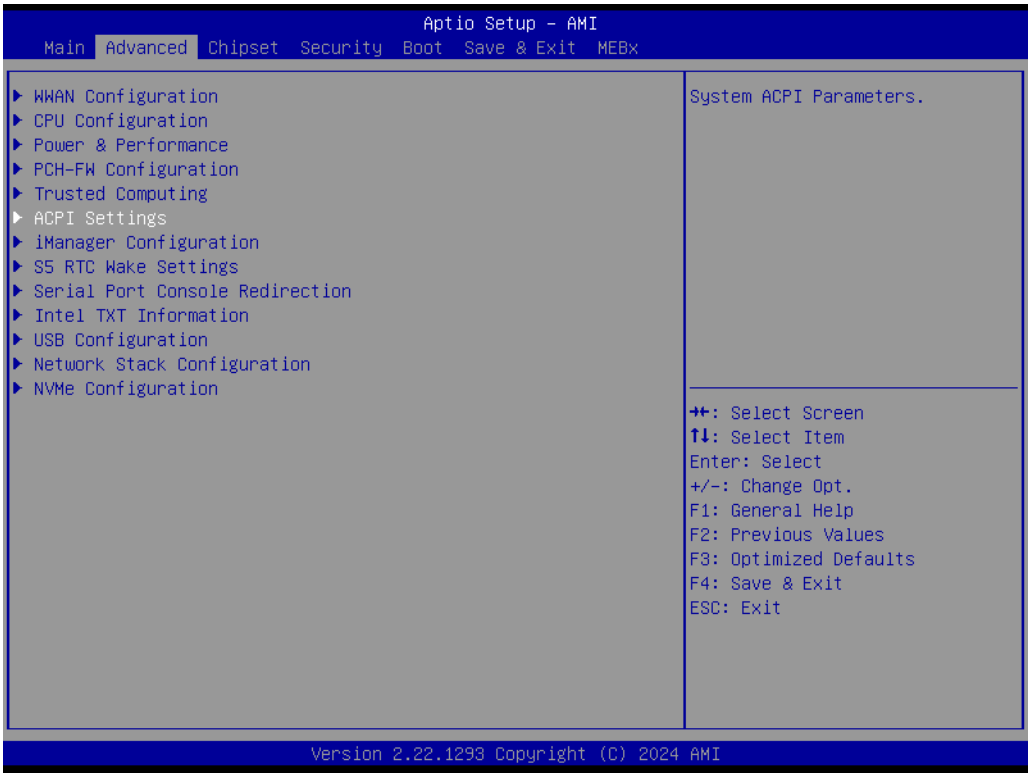


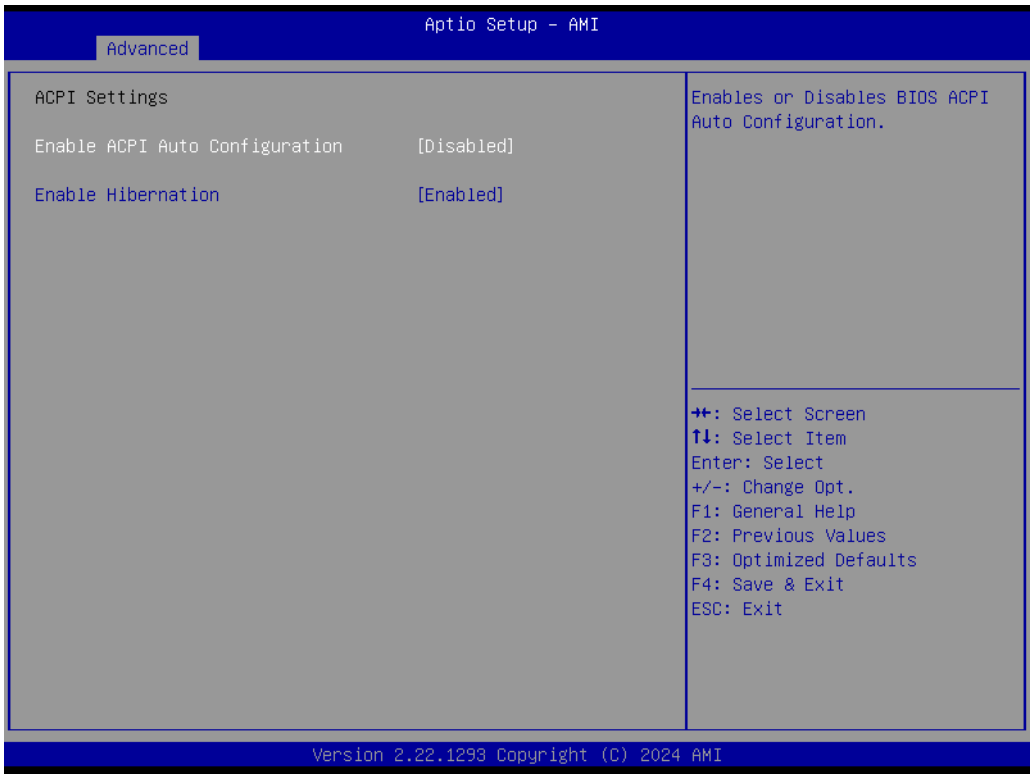
- **Security Device Support**
  Enable or disable BIOS support for security device.
- **SHA256 PCR Bank**
  Enable or Disable SHA256 PCR Bank.
- **SHA384 PCR Bank**

Enable or Disable SHA384 PCR Bank.

- **Pending operation**
  Schedule an Operation for the Security Device.
- **Platform Hierarchy**
  Enable or Disable Platform Hierarchy.
- **Storage Hierarchy**
  Enable or Disable Storage Hierarchy.
- **Endorsement Hierarchy**
  Enable or Disable Endorsement Hierarchy.
- **Physical Presence Spec Version**
  Select to Tell O.S. to support PPI Spec Version 1.2 or 1.3.
- **Device Select**
  TPM 1.2 will restrict support to TPM 1.2 devices, TPM 2.0 will restrict support to TPM 2.0 devices

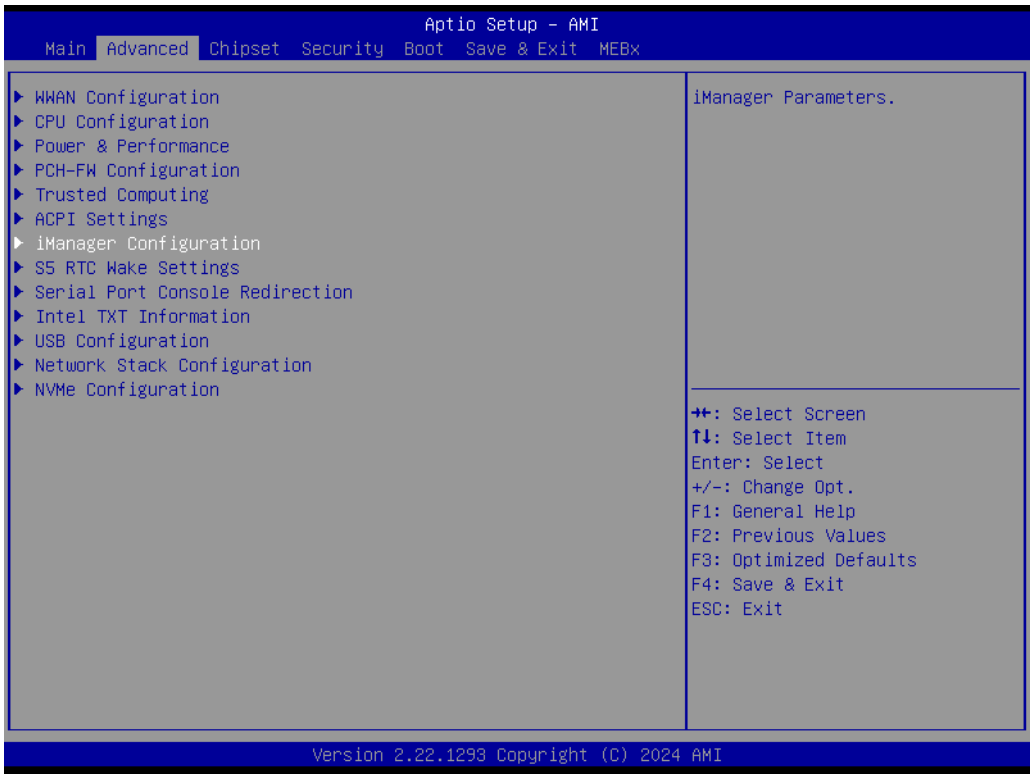
3.2.2.6 ACPI Setting

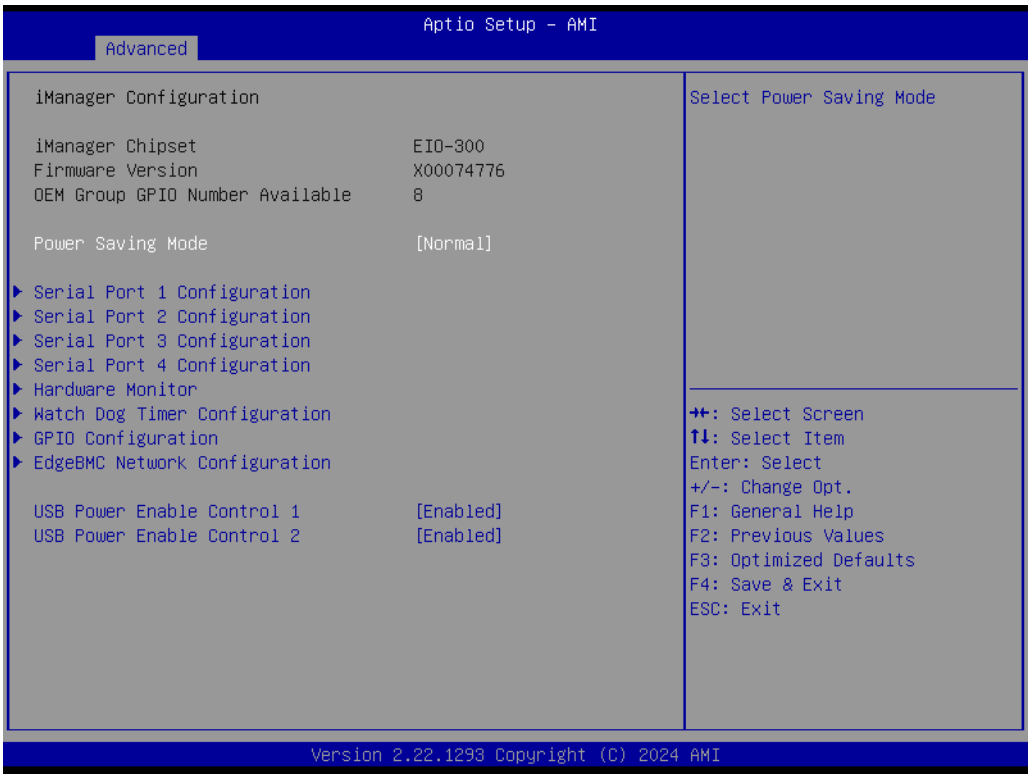




- **Enable ACPI Auto Configuration**
  Enables or Disables BIOS ACPI Auto Configuration.
- **Enable Hibernation**
  Enables or Disables System's ability to Hibernate (OS/S4 Sleep State).

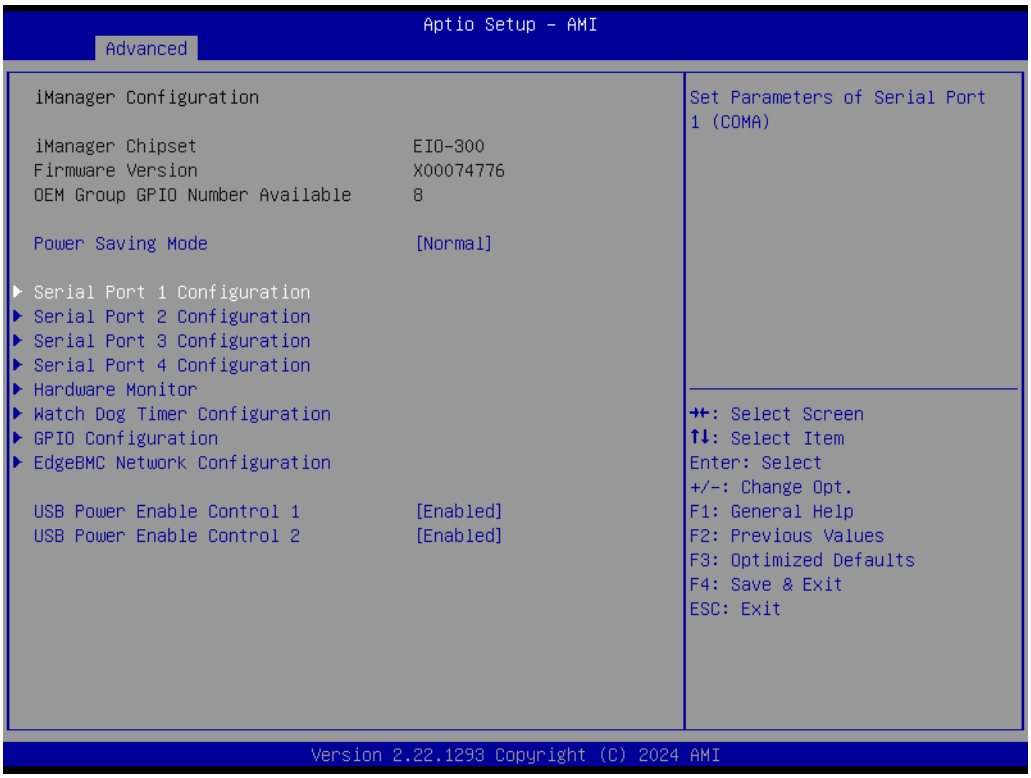
3.2.2.7 iManager Configuration

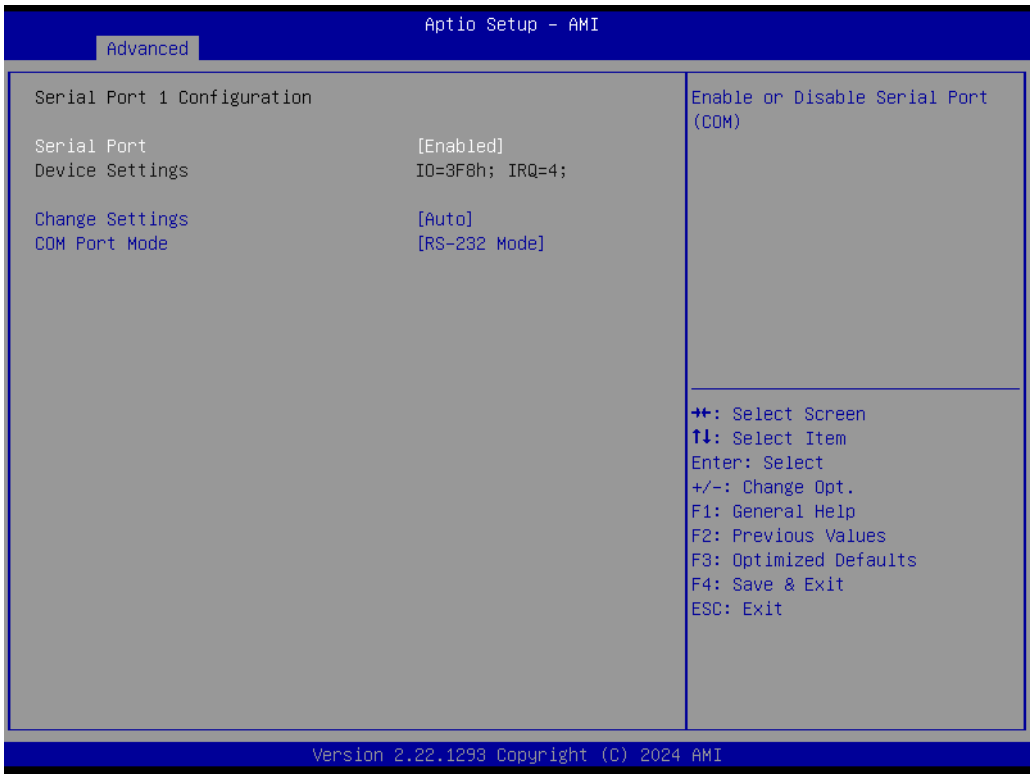




- **Power Saving Mode**
  Enable/Disable power saving mode.

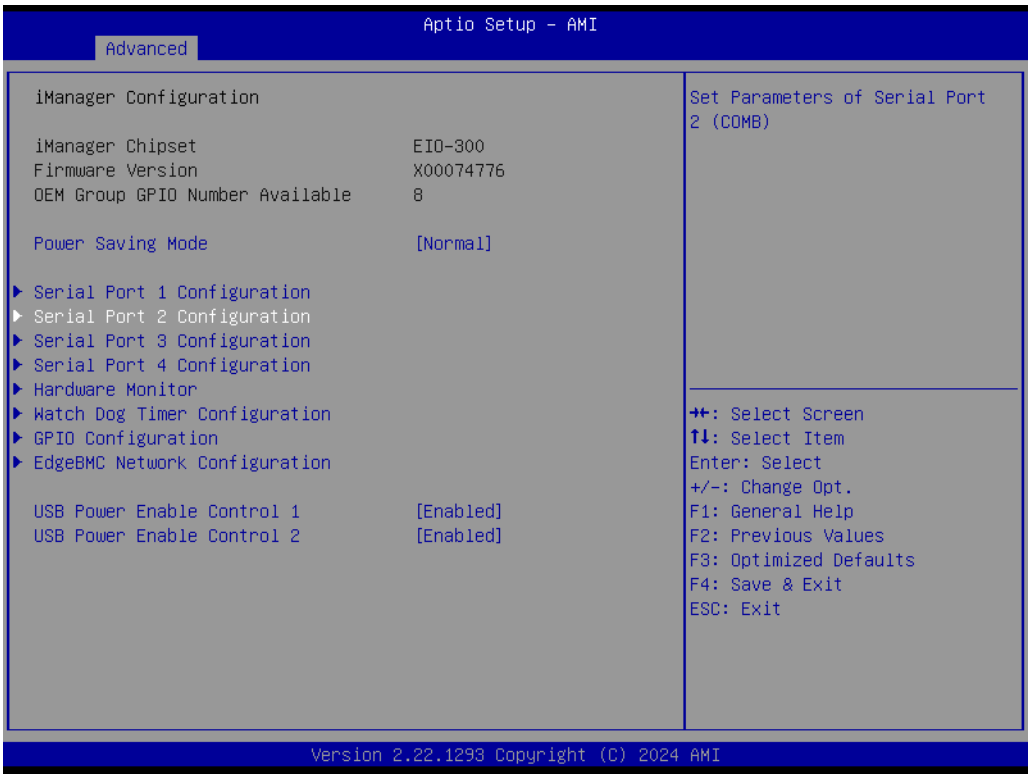
Serial Port 1 Configuration

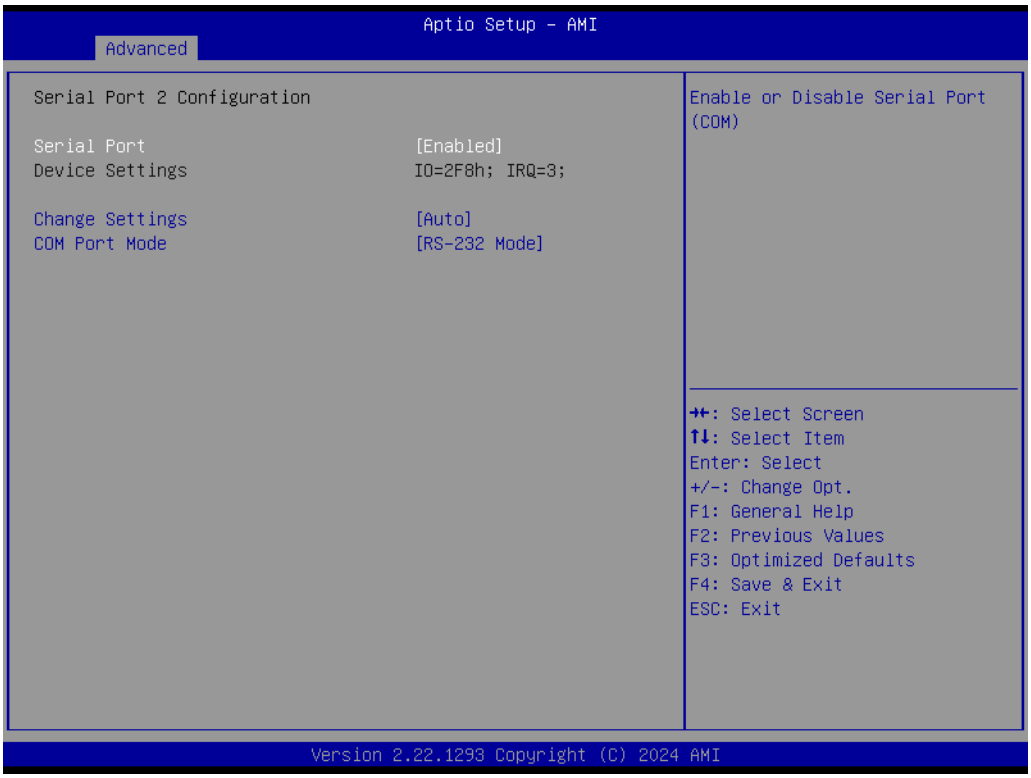




- **Serial Port**
  Enable/Disable serial port.
- **Change Settings**
  Select optimal settings for Super IO device.
- **COM port mode**
  COM Port Mode Select

Serial Port 2 Configuration

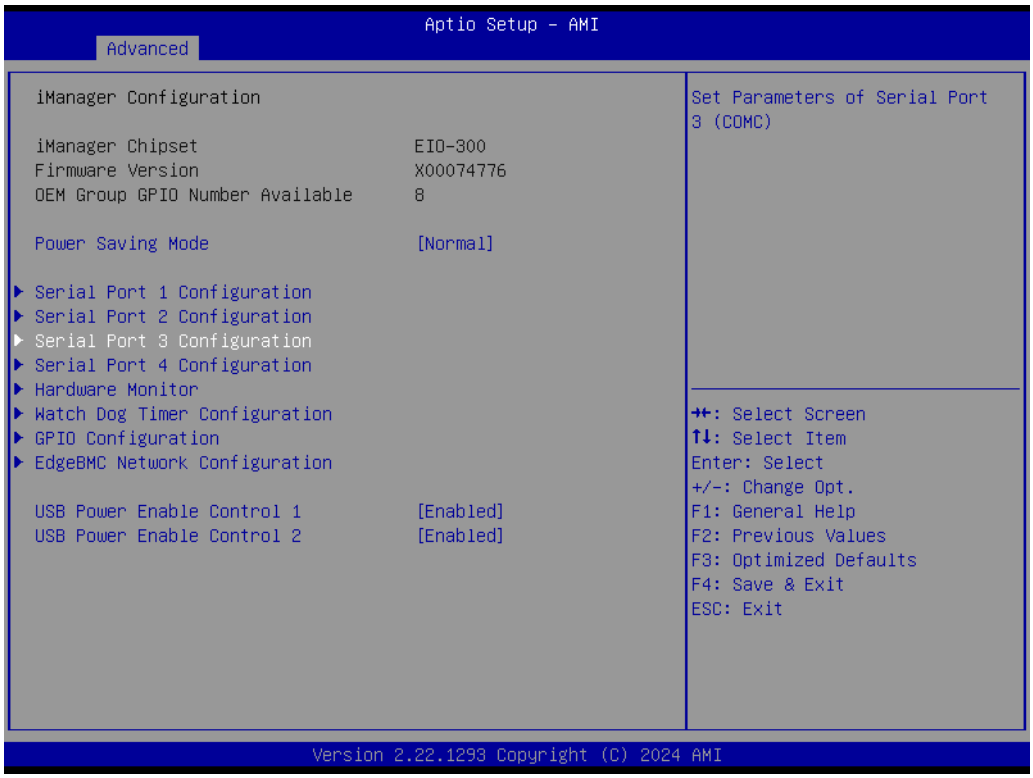


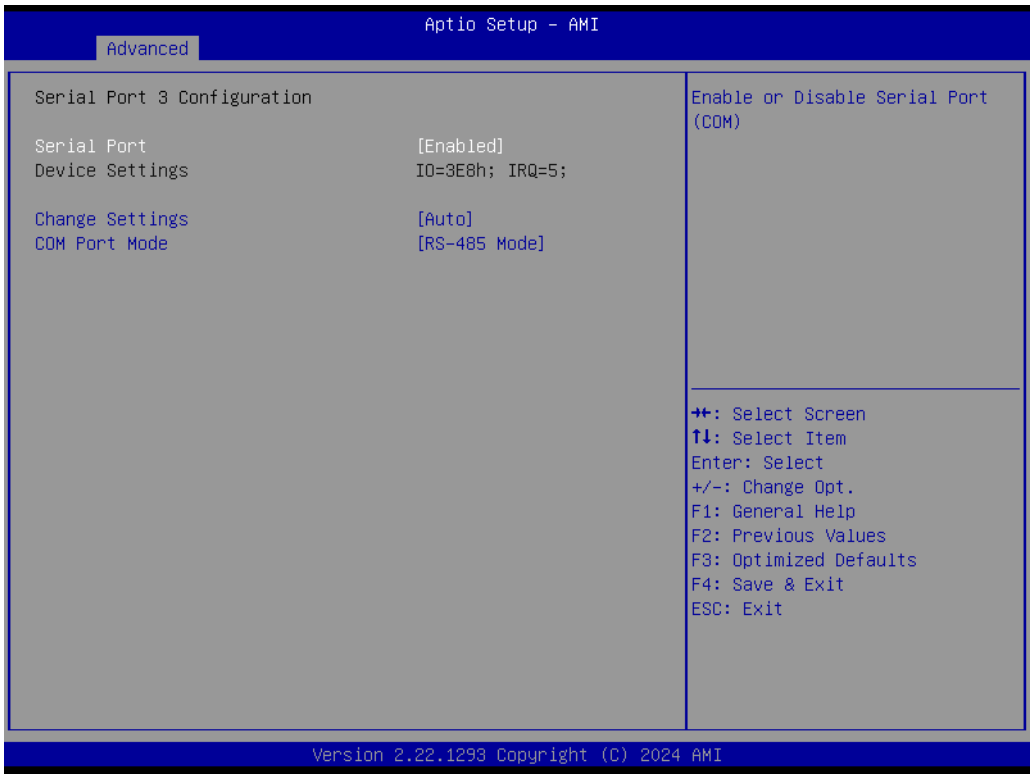


- **Serial Port**
  Enable/Disable serial port.
- **Change Settings**
  Select optimal settings for Super IO device.
- **COM port mode**

COM Port Mode Select

Serial Port 3 Configuration



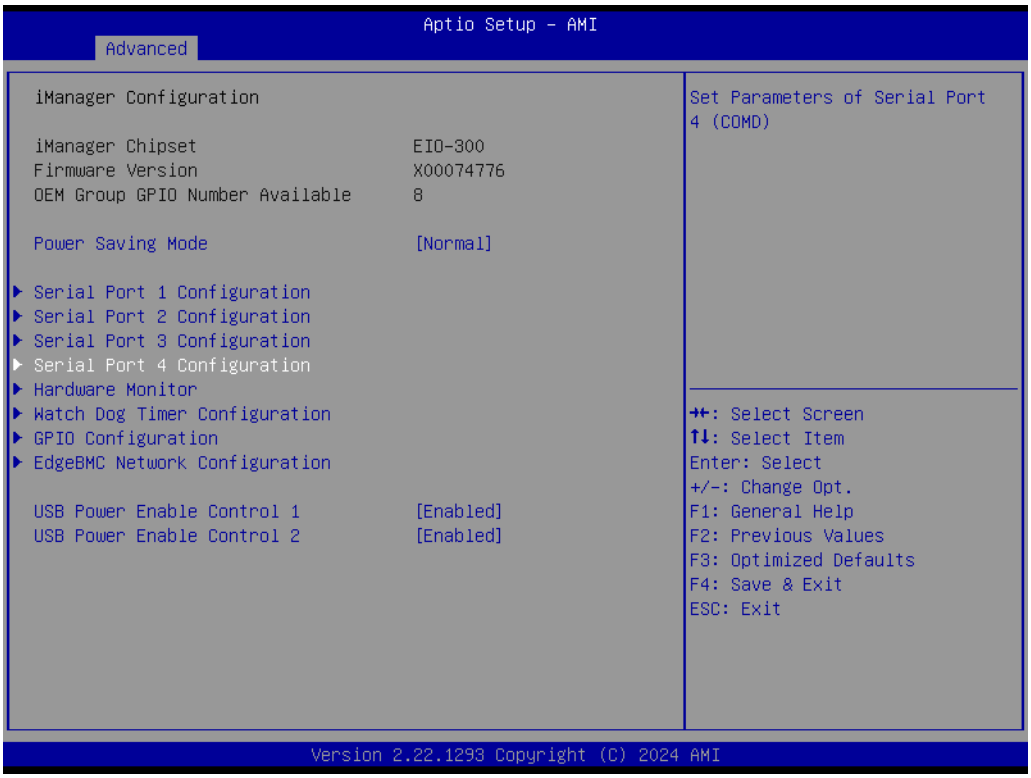


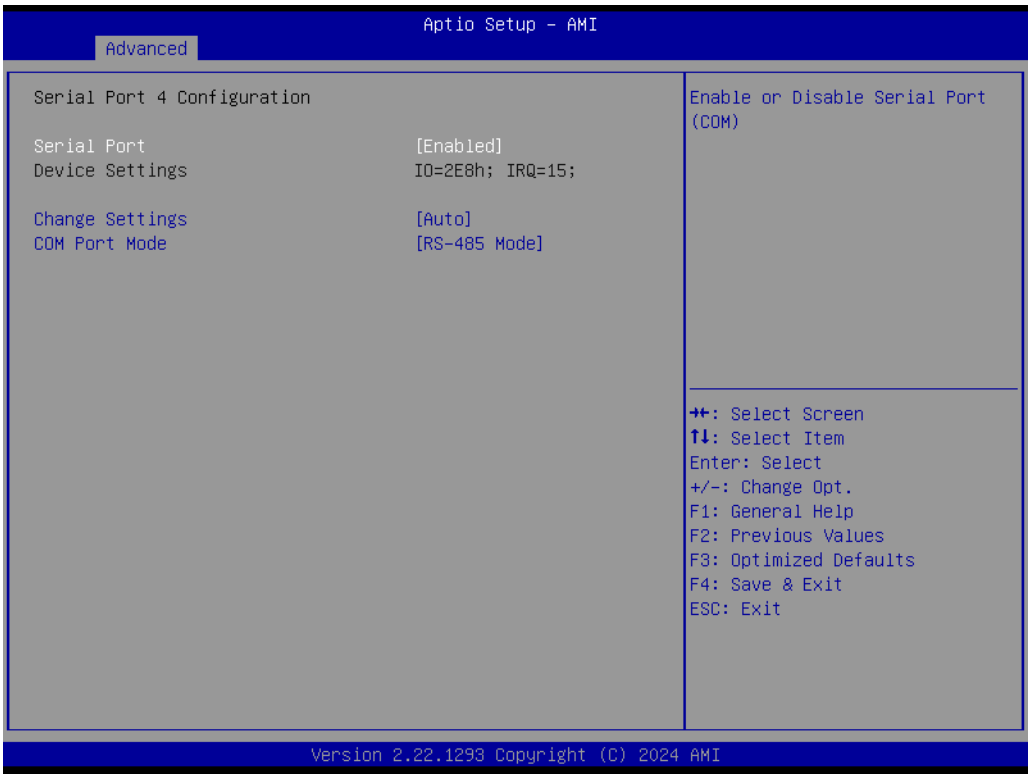
- **Serial Port**
  Enable/Disable serial port.
- **Change Settings**

Select optimal settings for Super IO device.

- **COM port mode**
  COM Port Mode Select

Serial Port 4 Configuration



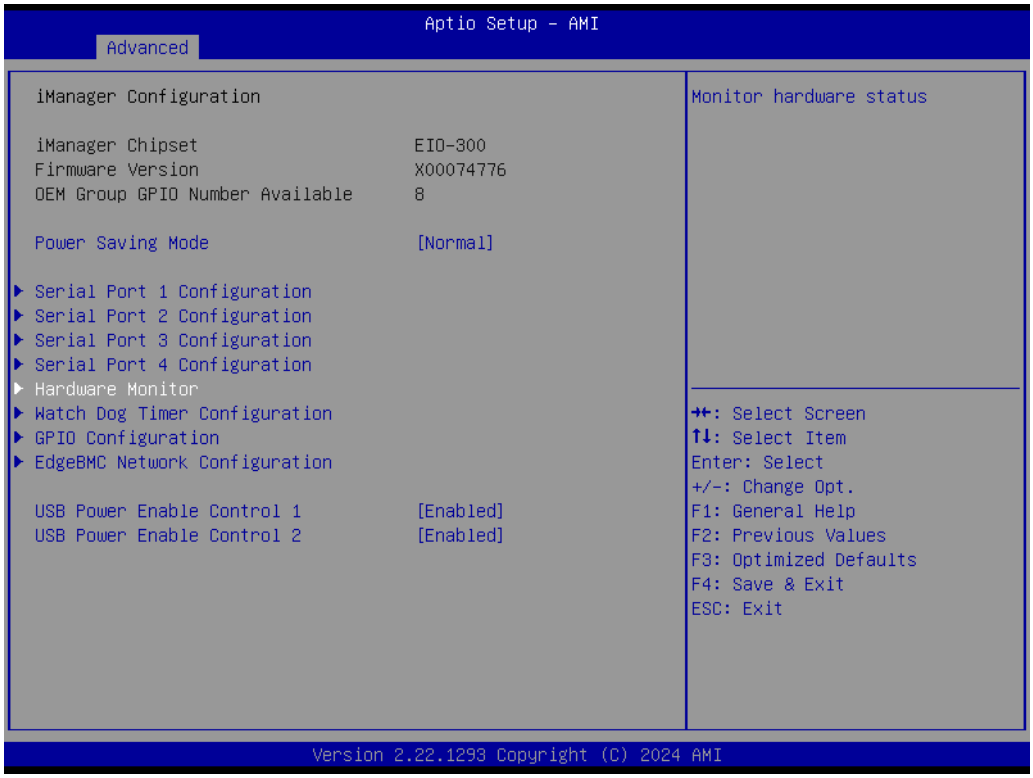


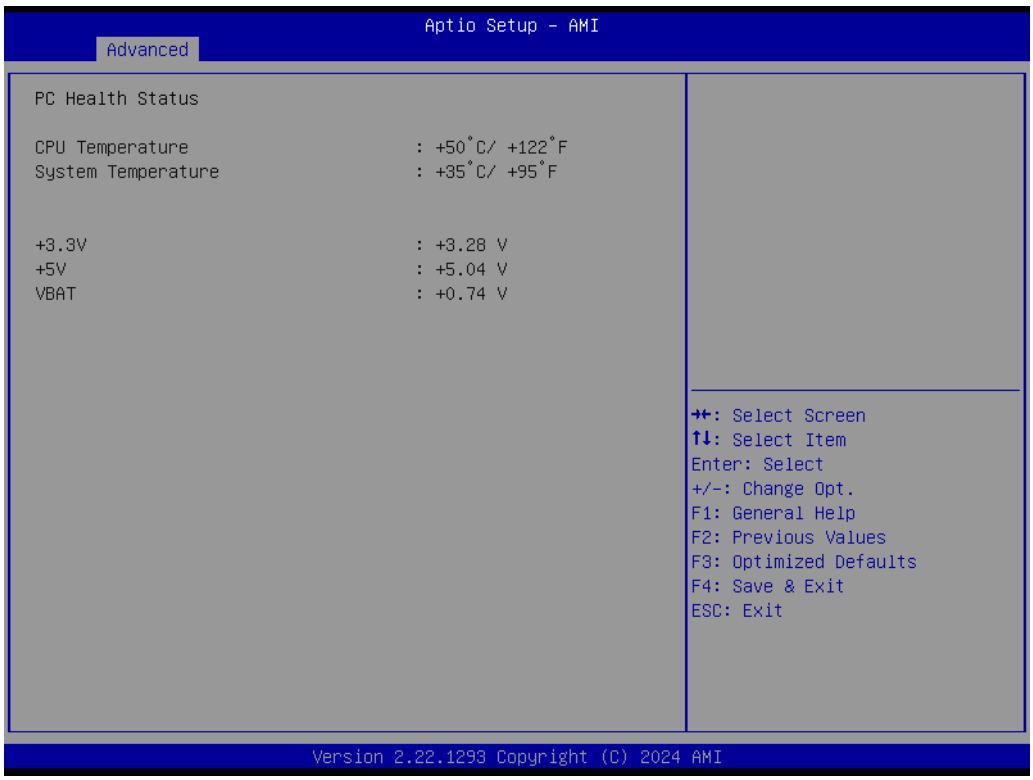
- **Serial Port**

Enable/Disable serial port.

- **Change Settings**
  Select optimal settings for Super IO device.
- **COM port mode**
  COM Port Mode Select

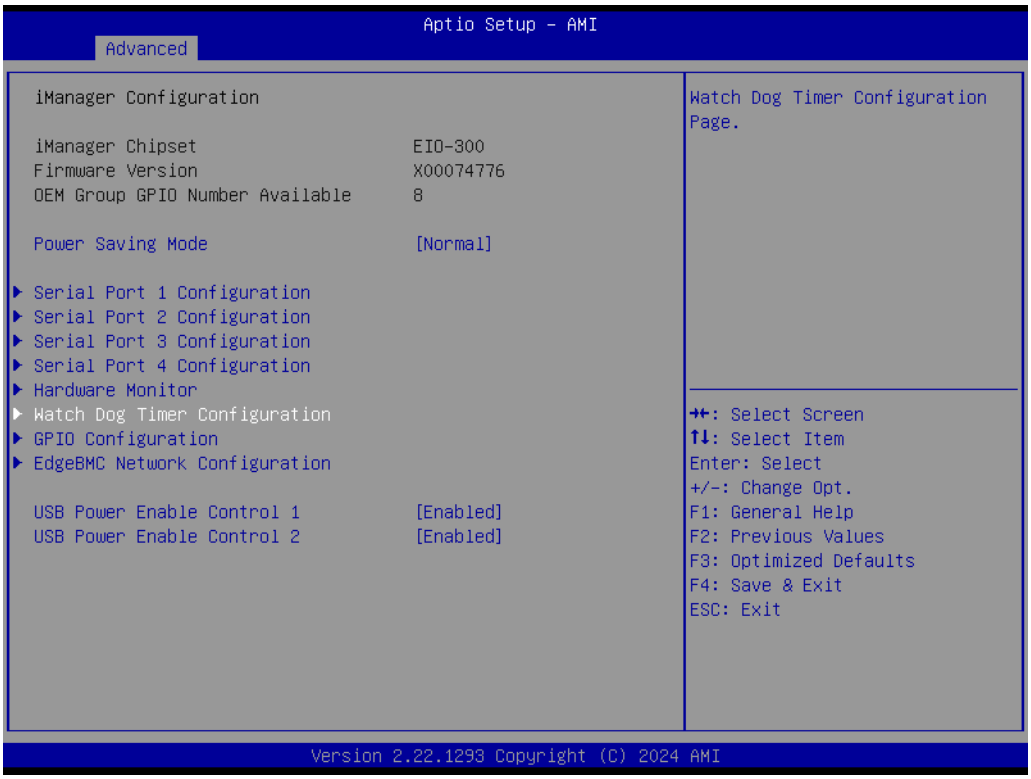
Hardware Monitor

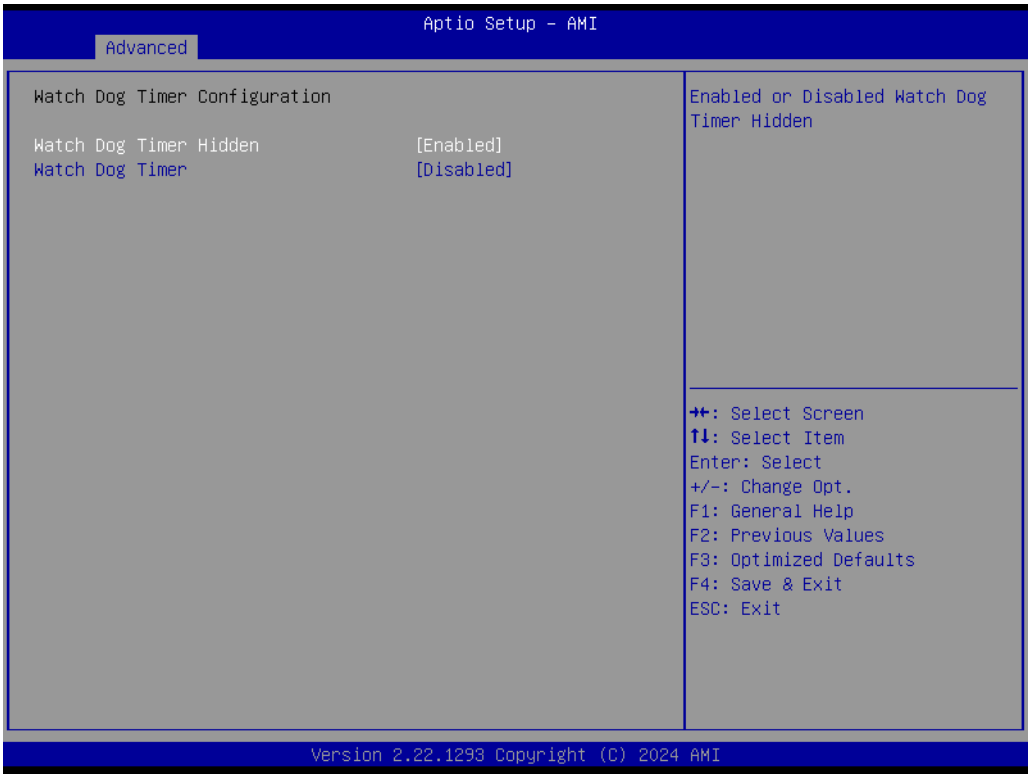




- **Hardware Monitor**
  Provides hardware monitoring information

Watch Dog Timer Configuration

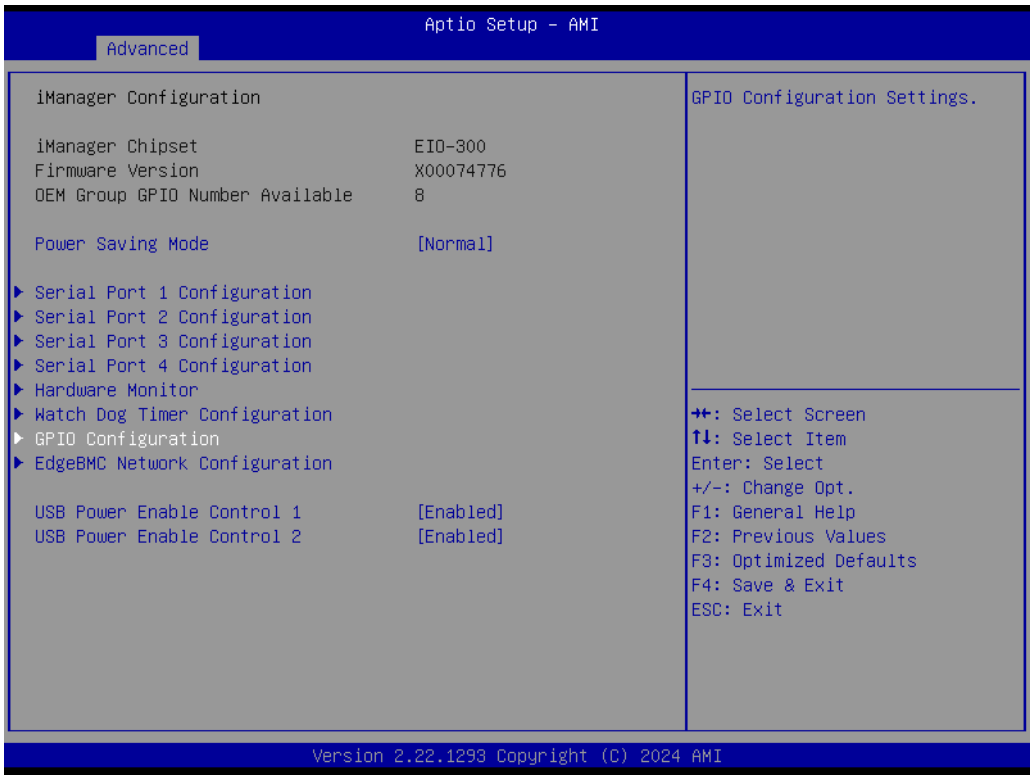


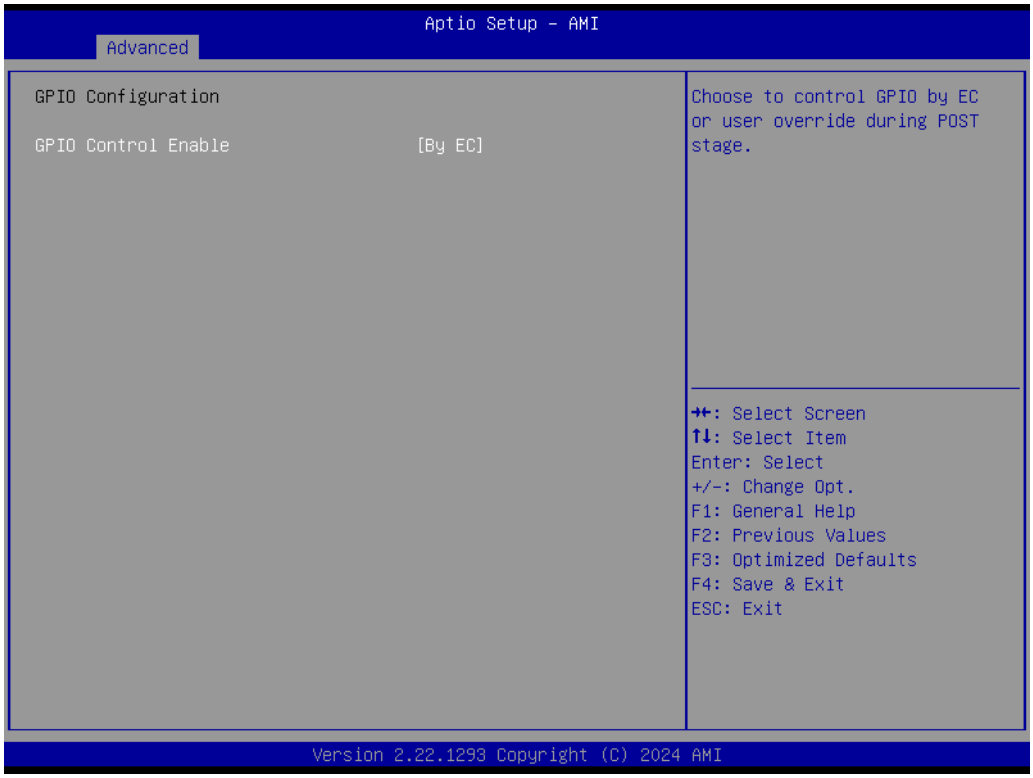


- **Watch Dog Timer Hidden**
  Enabled or Disabled Watch Dog Timer Hidden.

- **Watch Dog Timer**
  Enable or Disable the Watch Dog Timer function

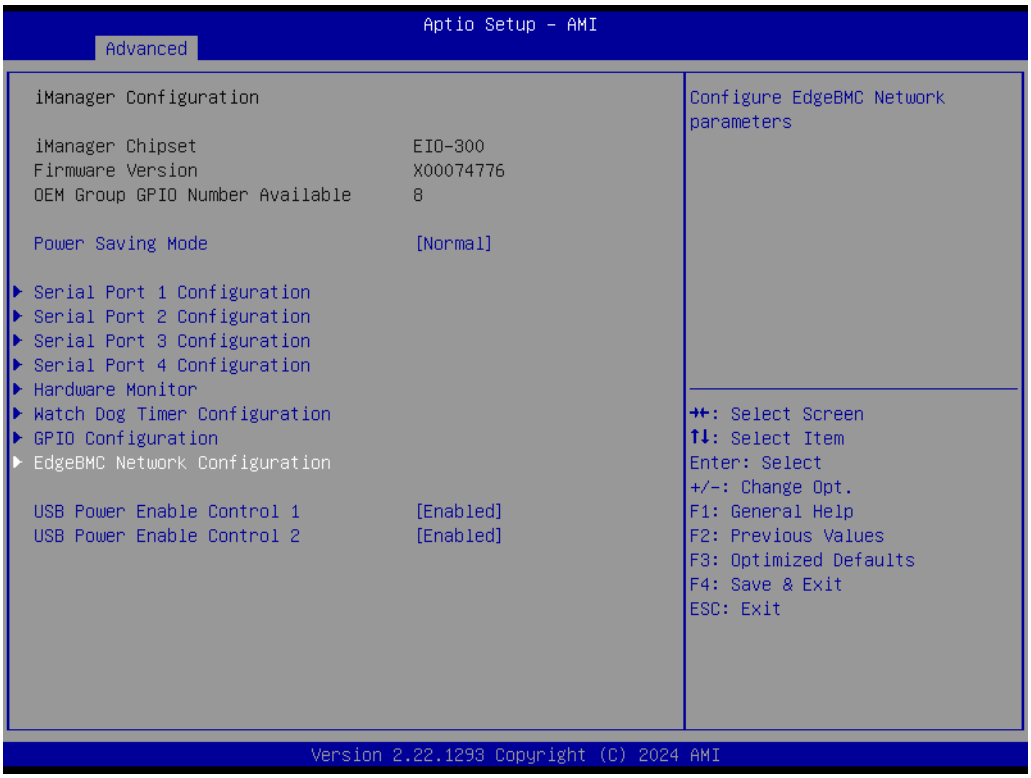
GPIO Configuration

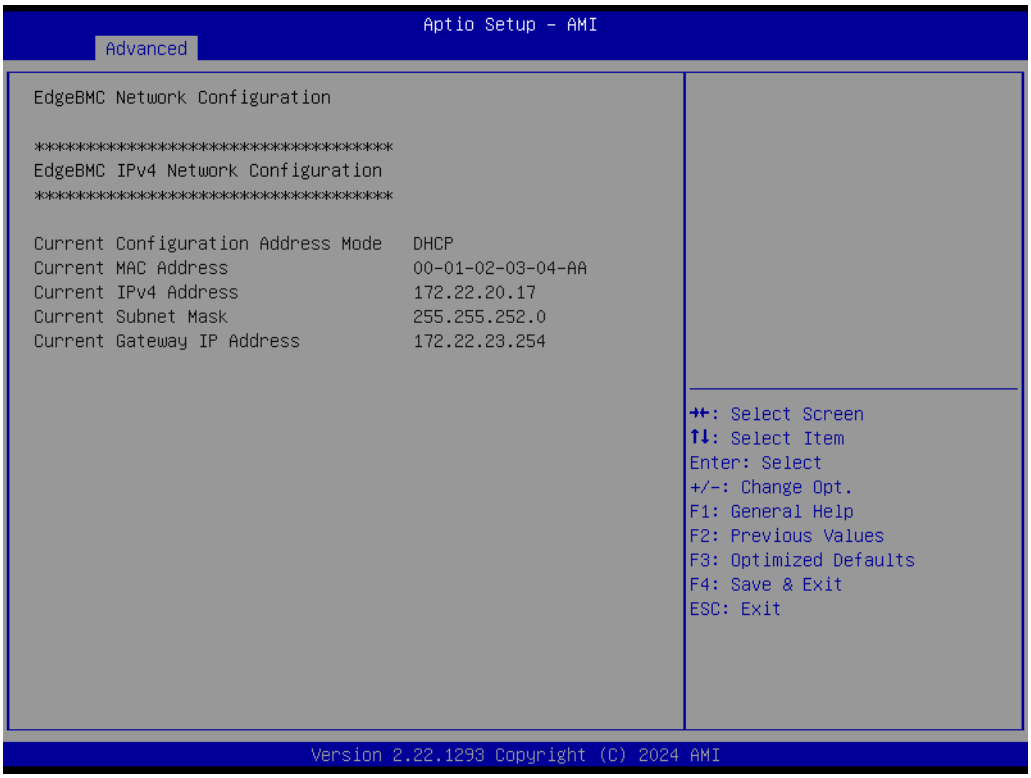




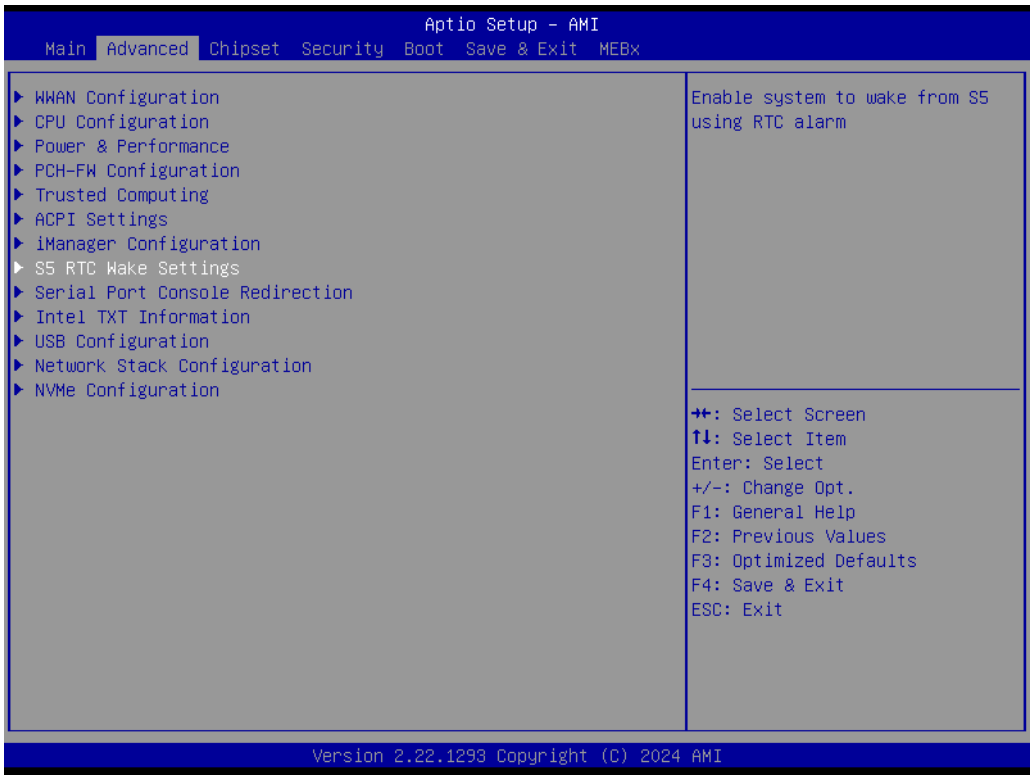
- **GPIO Control Enable**
  Select to control GPIO by EC or user override during the POST stage.

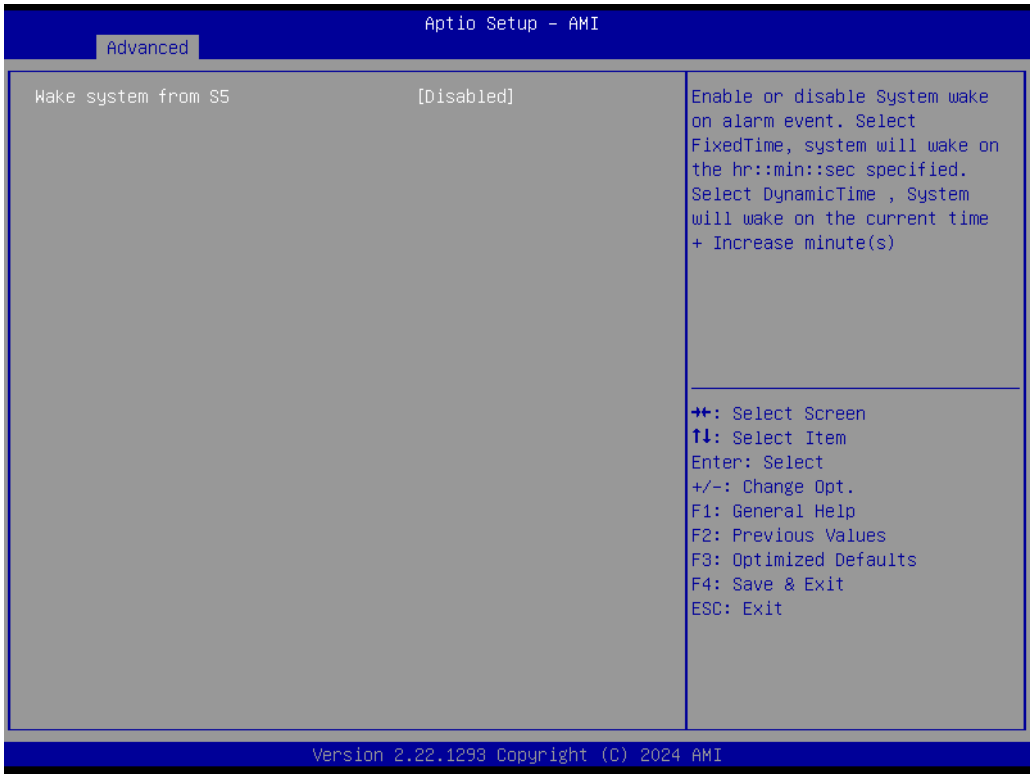
EdgeBMC Network Configuration





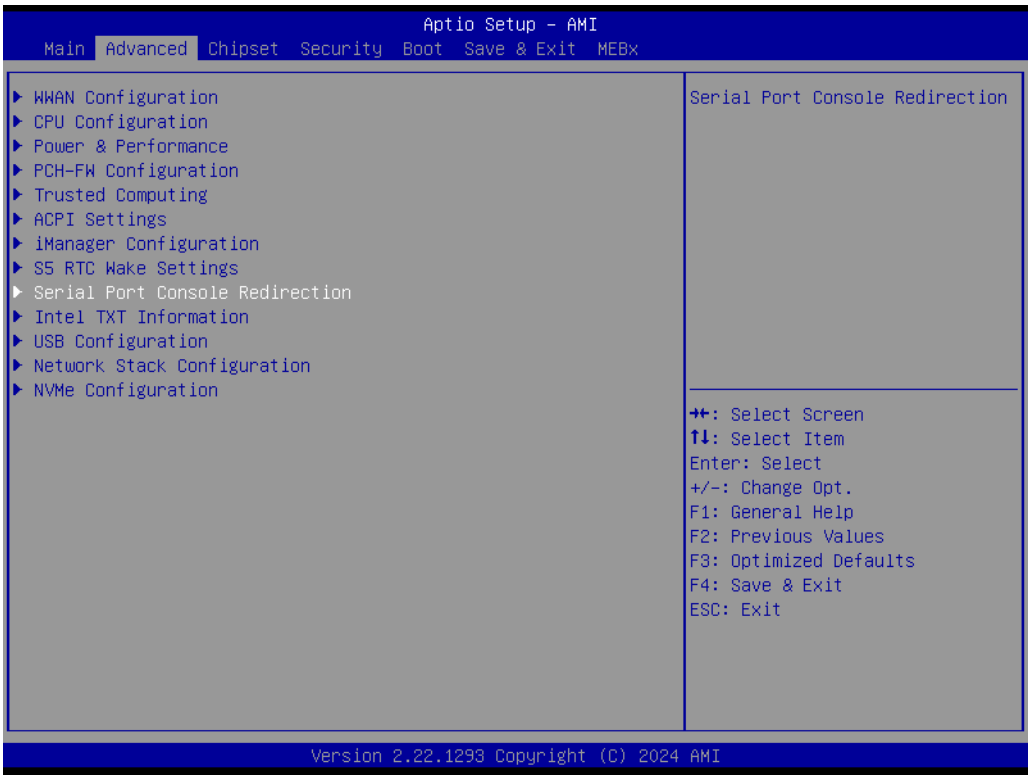
3.2.2.8 S5 RTC Wake Settings

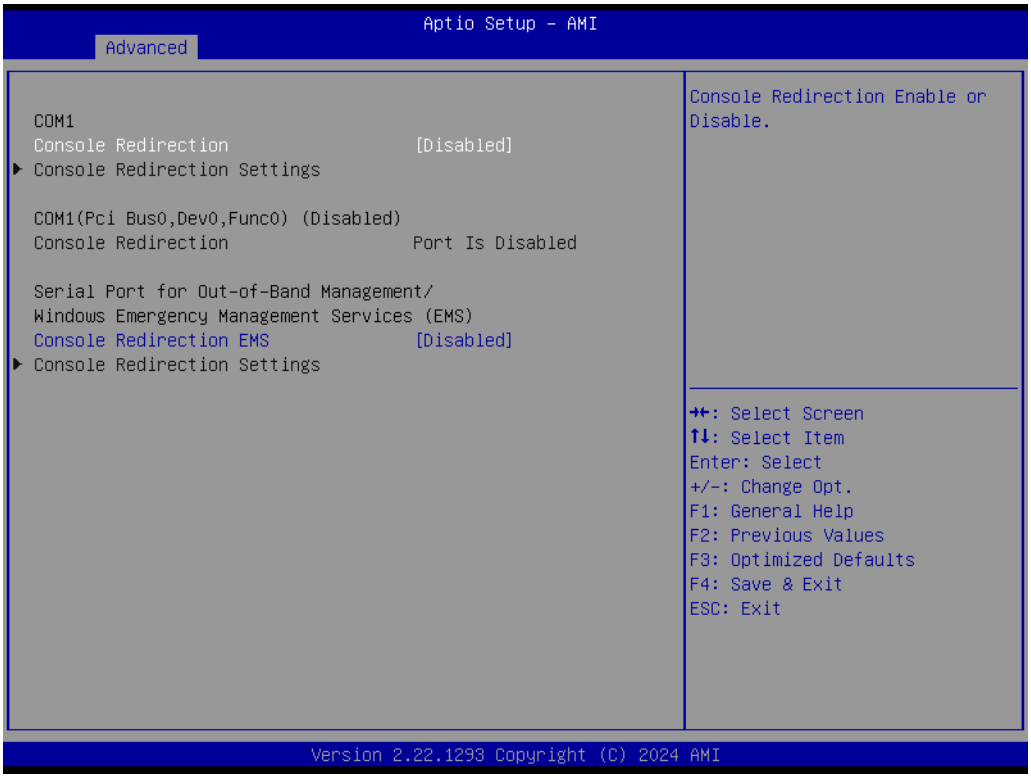




- **Wake system from S5**
  Enable or disable system wake on alarm event.

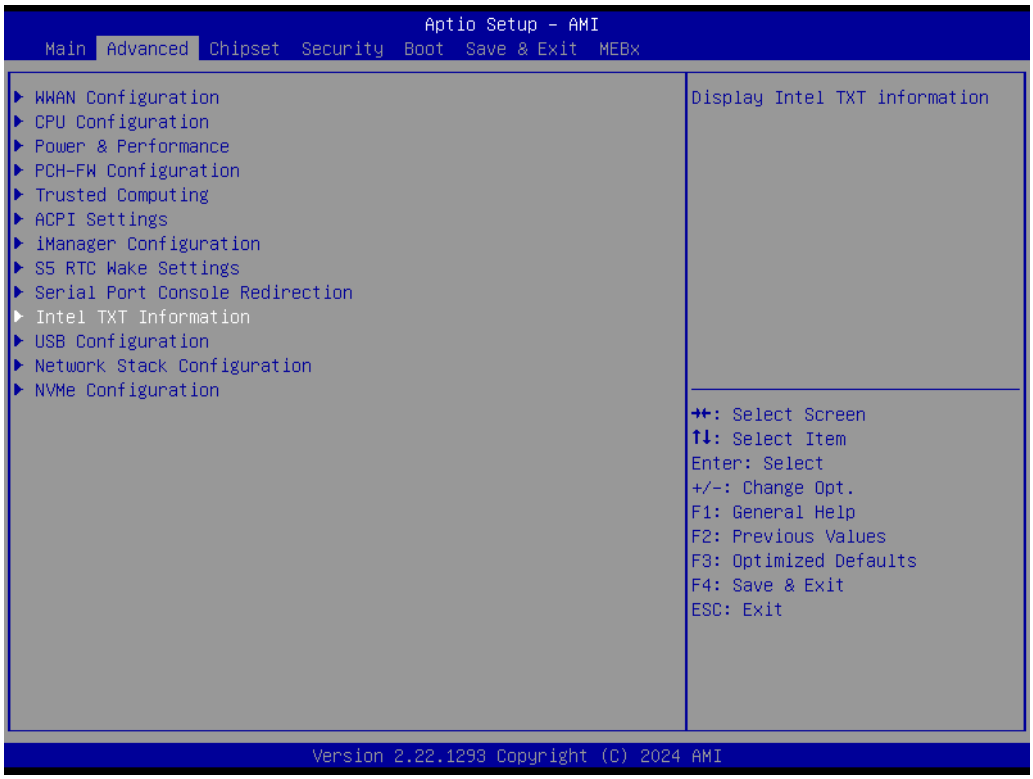
3.2.2.9 Serial Port Console Redirection

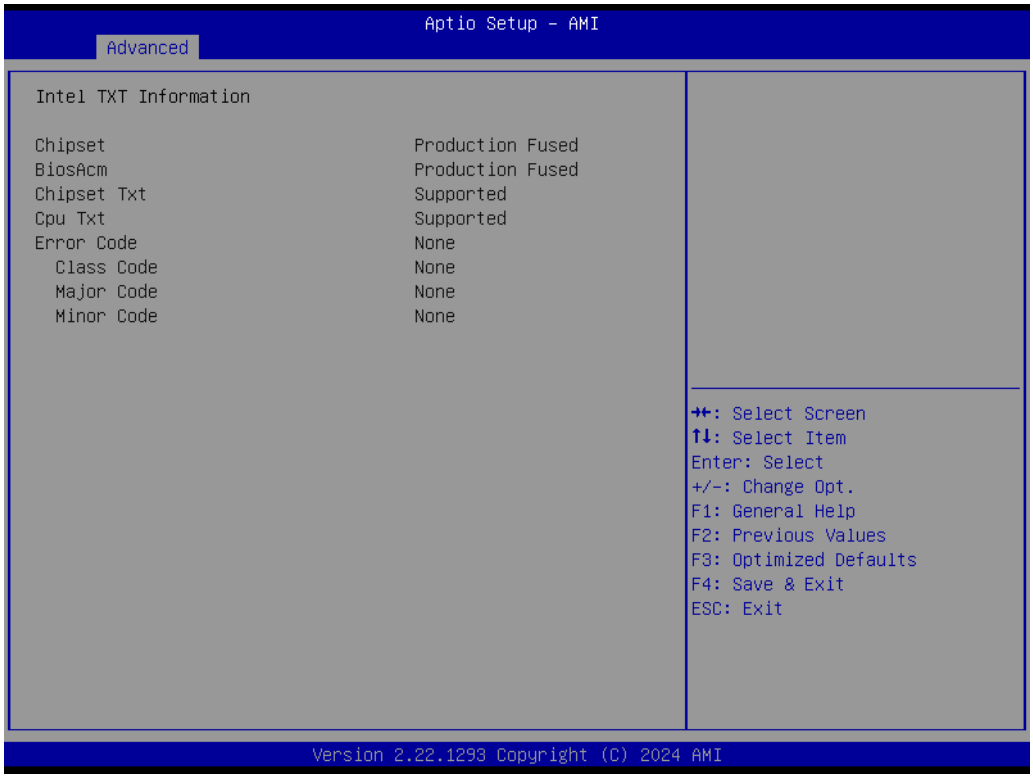




- **Console Redirection**
  Console Redirection Enable or Disable.
- **Console Redirection EMS**
  Console Redirection Enable or Disable.

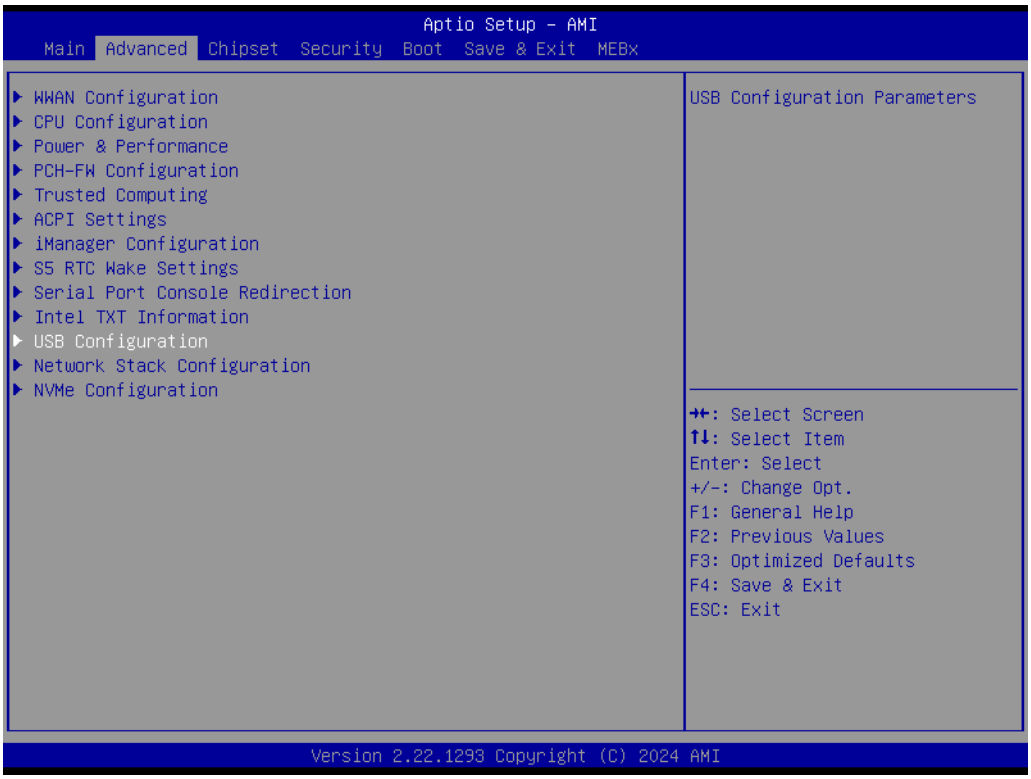
3.2.2.10 Intel TXT Information

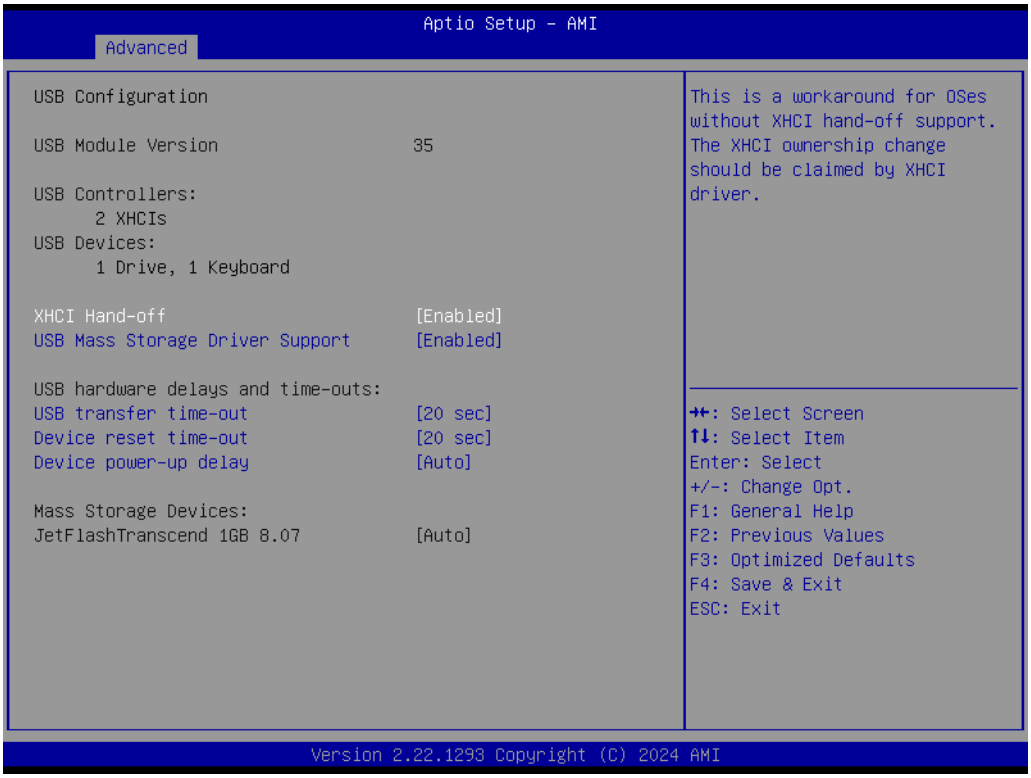




- **Intel TXT Information**
  Display Intel TXT information

3.2.2.11 USB Configuration



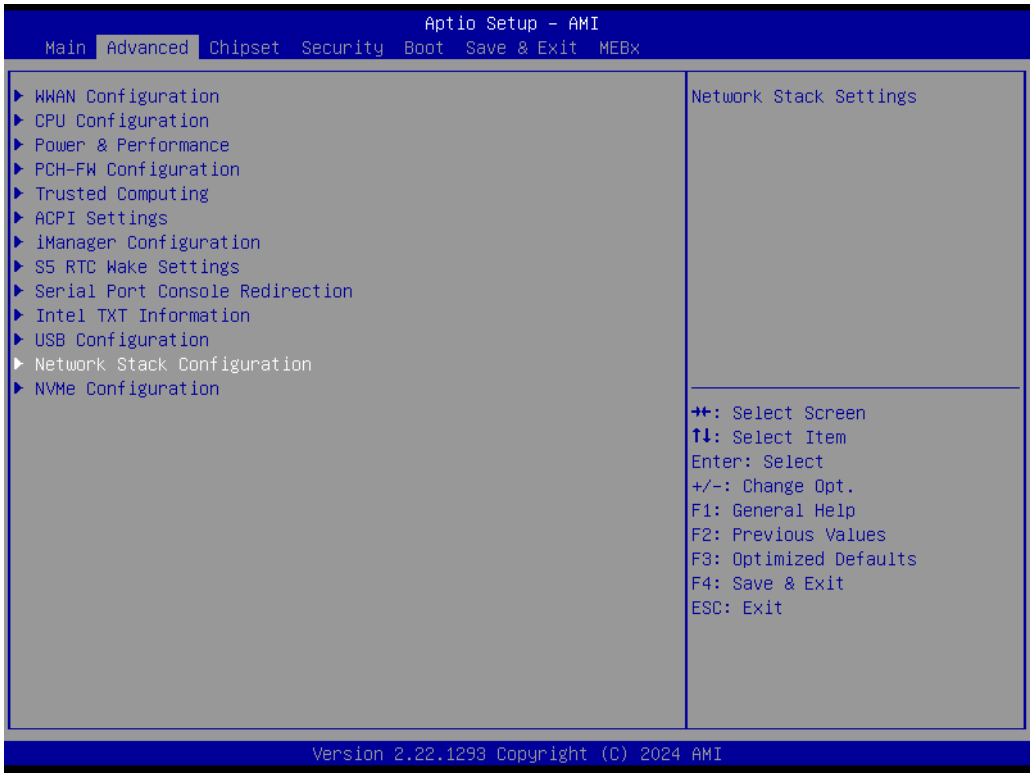


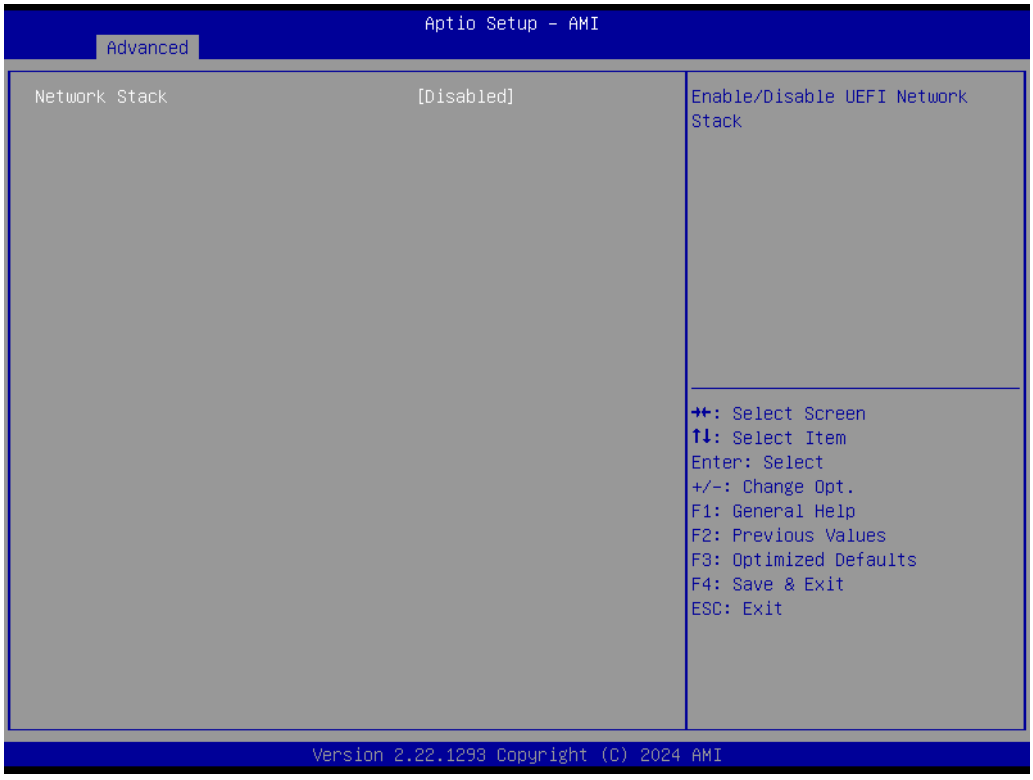
- **XHCI Hand-Off**
  This is a workaround for OS without XHCI hand-off support.
- **USB Mass Storage Driver Support**
  Enable/Disable USB Mass Storage Driver Support.
- **USB transfer time-out**

The time-out value for control, bulk, and interrupt transfers.

- **Device reset time-out**
  USB mass storage device Start Unit command time-out.
- **Device power-up delay**
  Maximum time the device will take before it properly reports itself to the Host Controller.

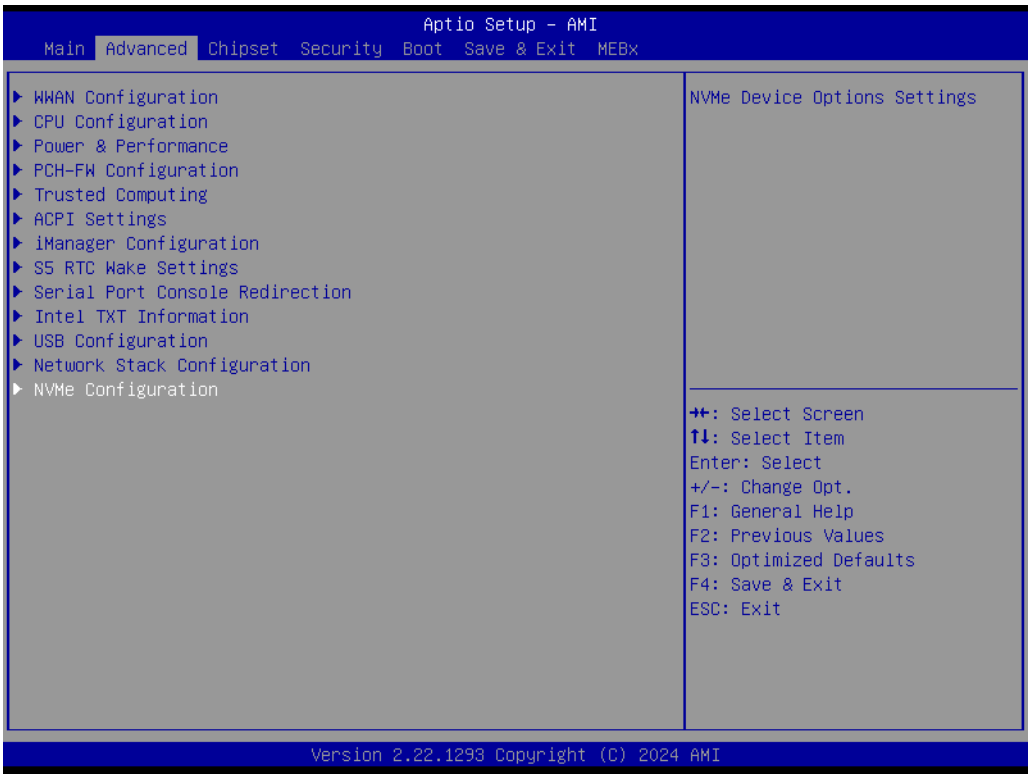
3.2.2.12 Network Stack Configuration

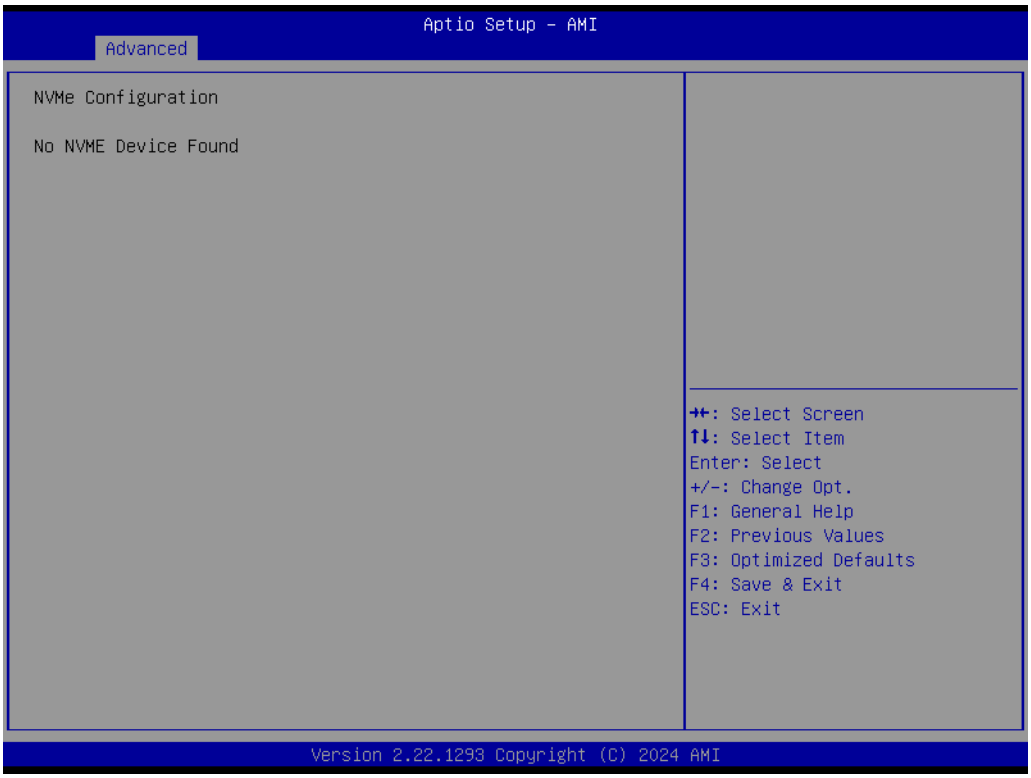




- **Network Stack**
  Enable/Disable UEFI Network Stack.

3.2.2.13 NVMe Configuration

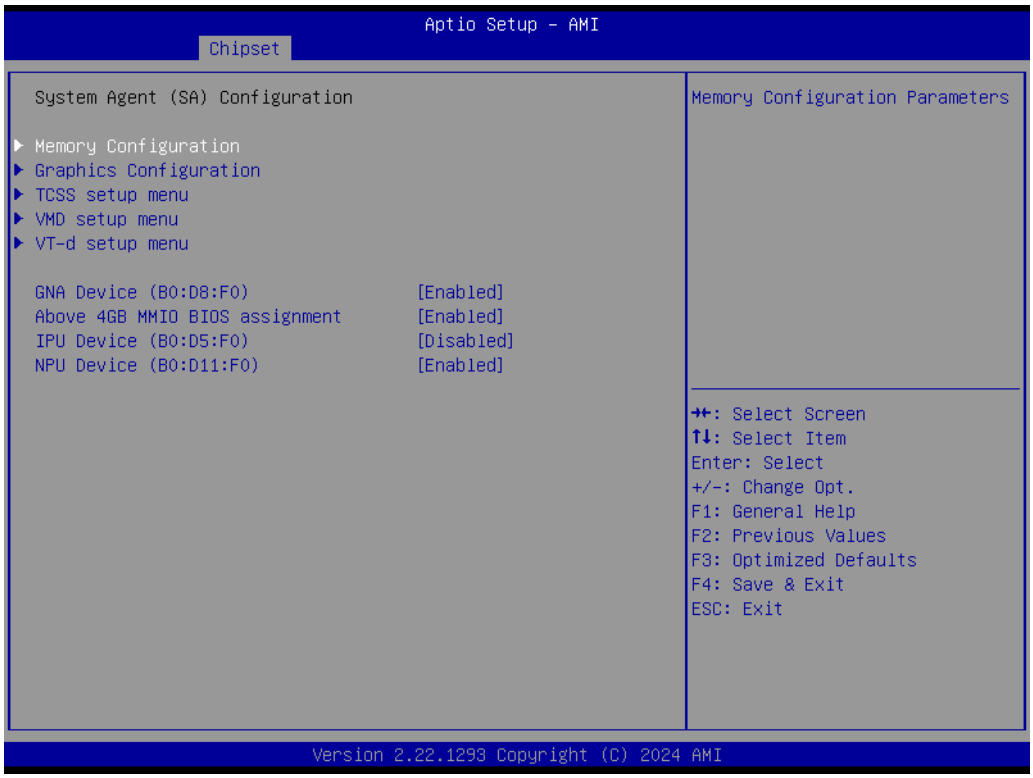




3.2.3 Chipset Configuration

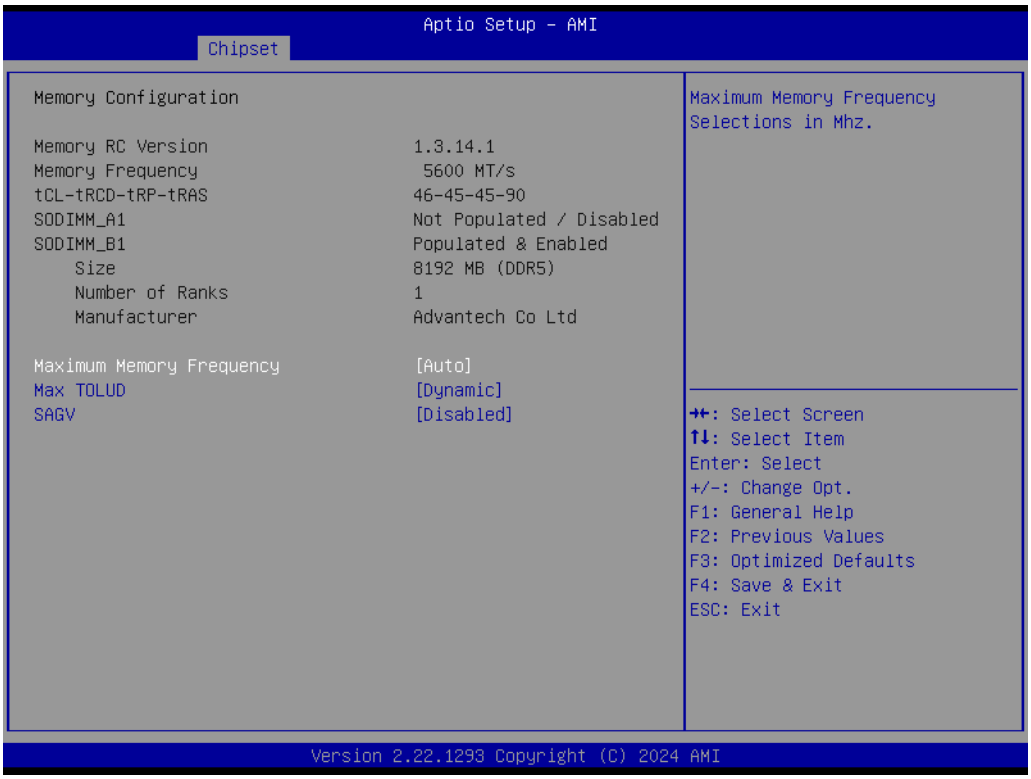
Select the Chipset tab from the ARK-1125 setup screen to enter the Chipset BIOS Setup screen. You can display a Chipset BIOS Setup option by highlighting it using the <Arrow> keys. All Plug-and-Play BIOS Setup options are described in this section. The Plug-and-Play BIOS Setup screen is shown below.

3.2.3.1 System Agent (SA) Configuration



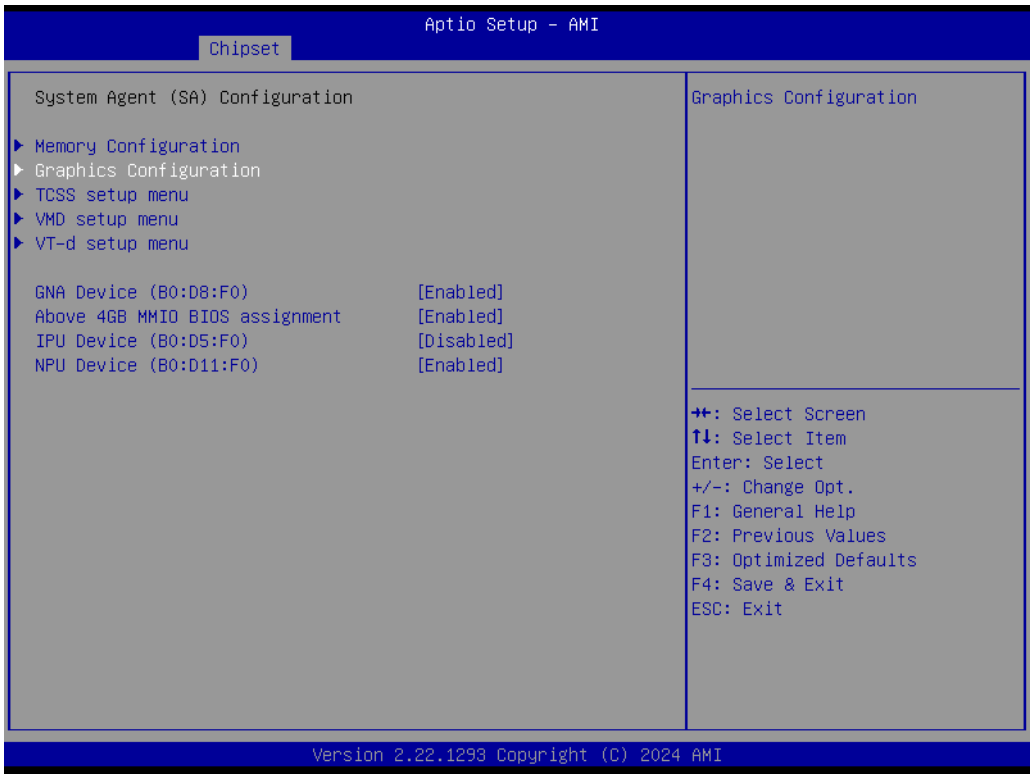
- **GNA Device**
  Enable/Disable SA GNA Device.
- **Above 4GB MMIO BIOS assignment**
  Enable/Disable above 4GB Memory Mapped I/O BIOS assignment. This is enabled automatically when Aperture Size is set to 2048MB
- **IPU Device**
  Enable/Disable SA IPU Device. This option will be grayed out when IPU is fused off from silicon.
- **NPU Device**
  Enable/Disable NPU (Neural Processing Unit) Device.

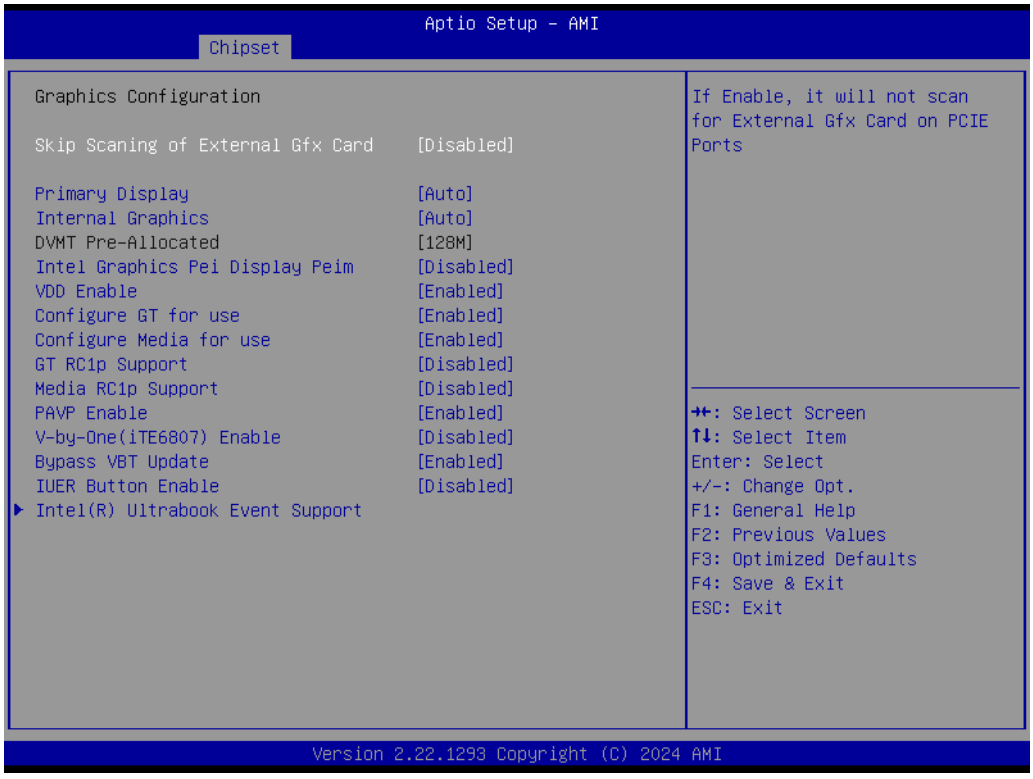
Memory Configuration



- **Maximum Memory Frequency**
  Maximum Memory Frequency Selections in Mhz
- **Max TOLUD**
  Maximum Value of TOLUD.
- **SAGV**
  System Agent Geysetville.

Graphics Configuration

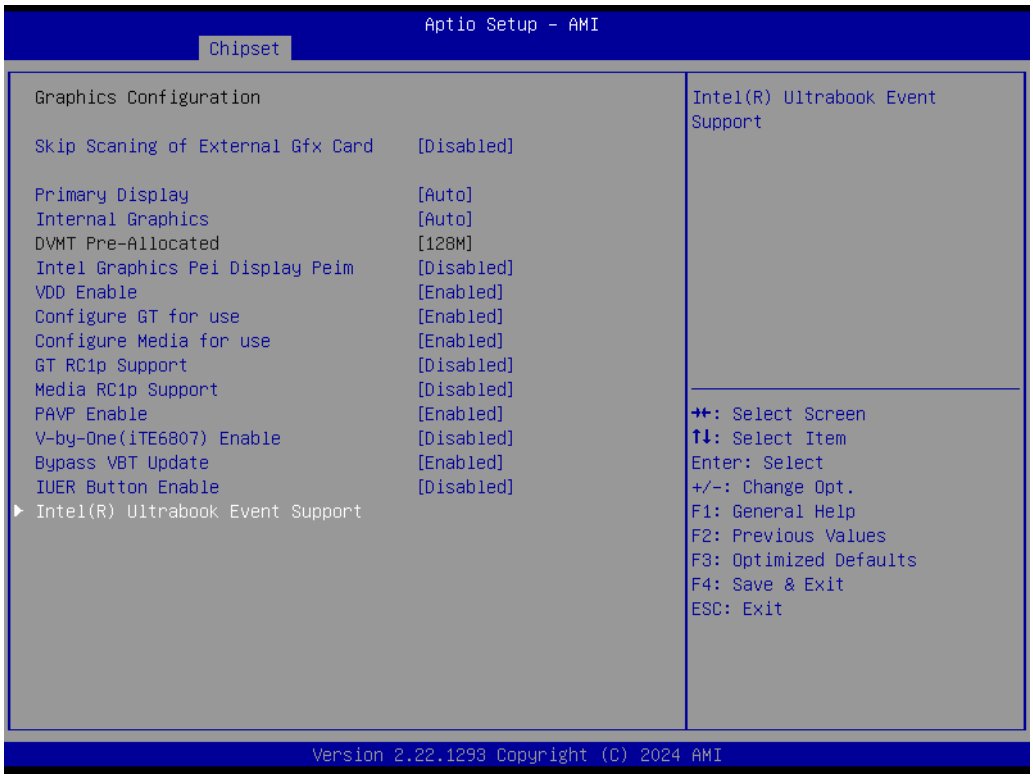


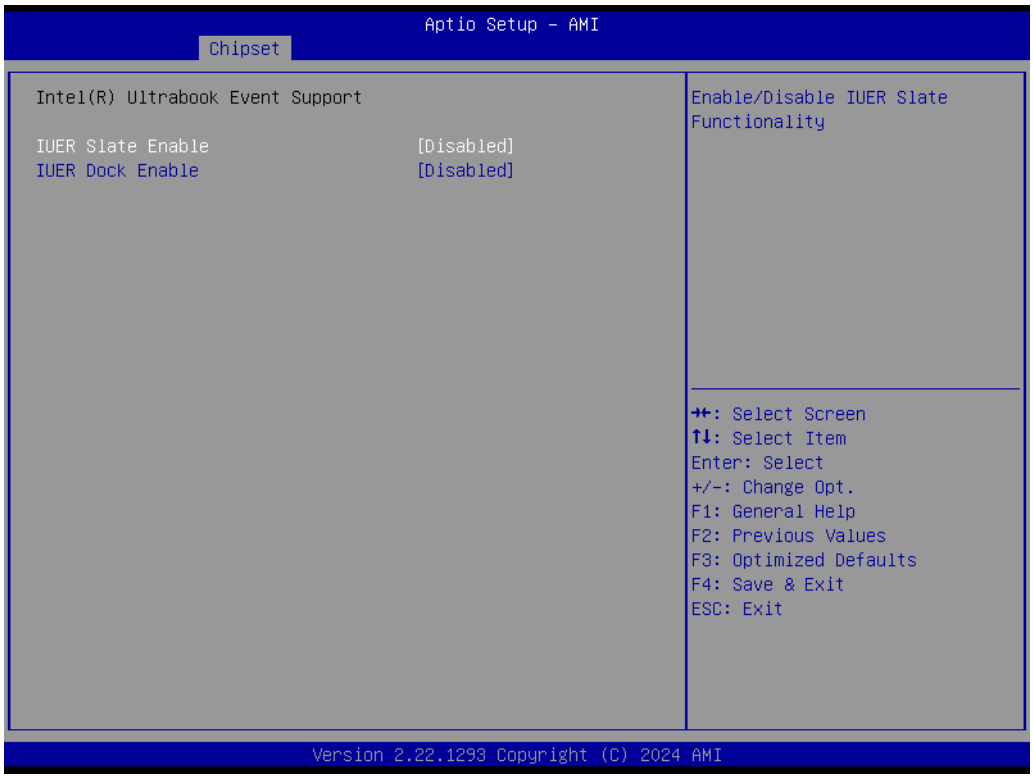


- **Skip Scaning of External Gfx Card**
  If Enable, it will not scan for External Gfx Card on PCIE Ports.
- **Primary Display**
  Select from IGFX/PEG/PCI, which graphics device should be Primary Dis- play or select SG for Switchable Gfx.

- **Internal Graphics**
  Keep IGFX enabled based on the setup options.
- **DVMT Pre-Allocated**
  Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
- **Intel Graphics Pei 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.
- **Configure Media for use**
  Enable/Disable Media configuration in BIOS.
- **GT RC1p Support**
  Enable/Disable RC1p support. If GT RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met.
- **Media RC1p Support**
  Enable/Disable RC1p support. If Media RC1p is enabled, send a RC1p frequency request to PMA if other conditions being met.
- **PAVP Enable**
  Enable/Disable PAVP.
- **V-by-One (iTE6807) Enable**
  Enable/Disable V-by-One(iTE6807)
- **Bypass VBT Update**
  Enable/Disable bypass VBT update.
- **IUER Button Enable**
  Enable/Disable IUER Button Functionality.

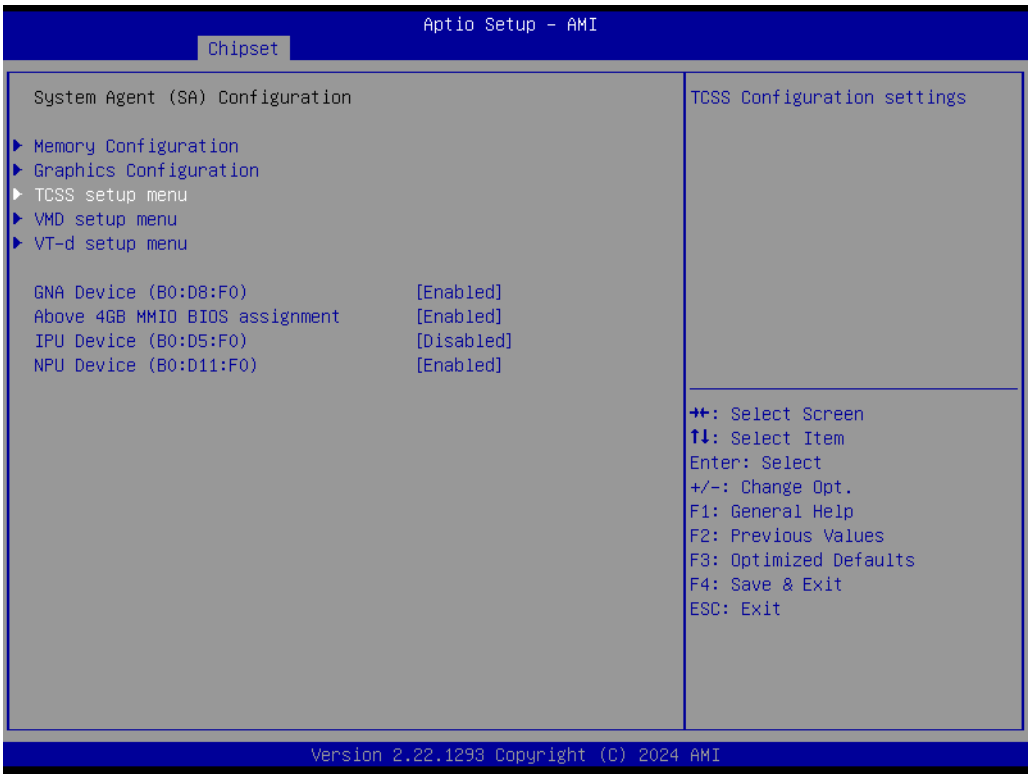
Intel® Ultrabook Event Support

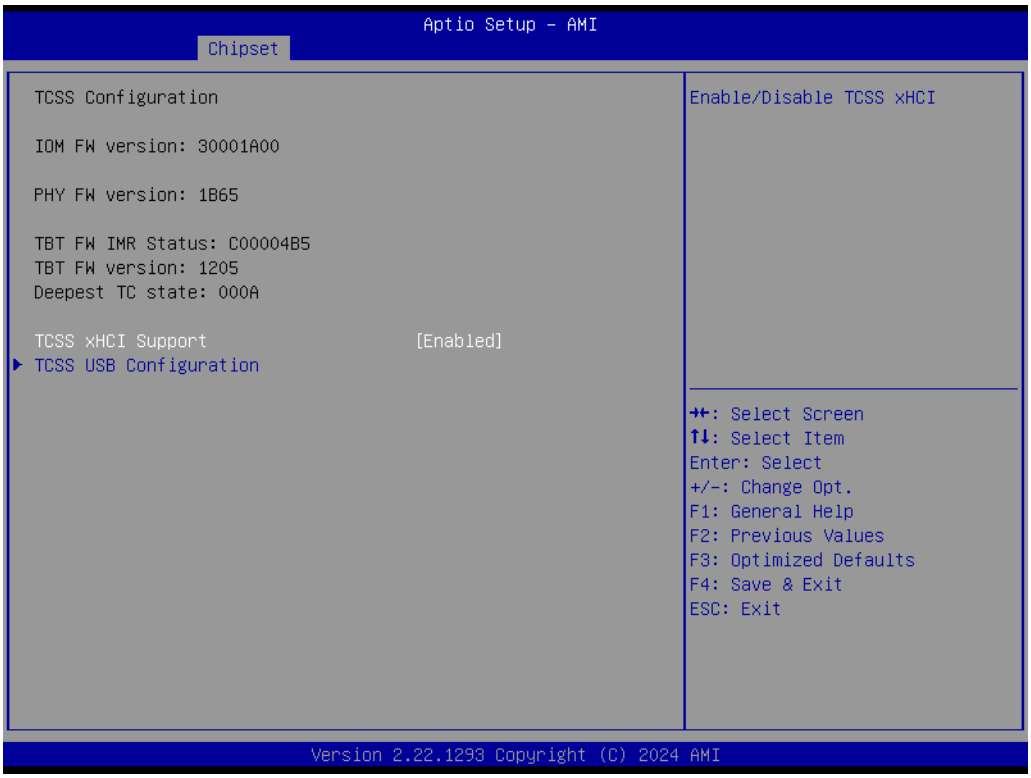




- **IUER Slate Enable**
  Enable/Disable IUER Slate Functionality.
- **IUER Dock Enable**
  Enable/Disable IUER Dock Functionality.

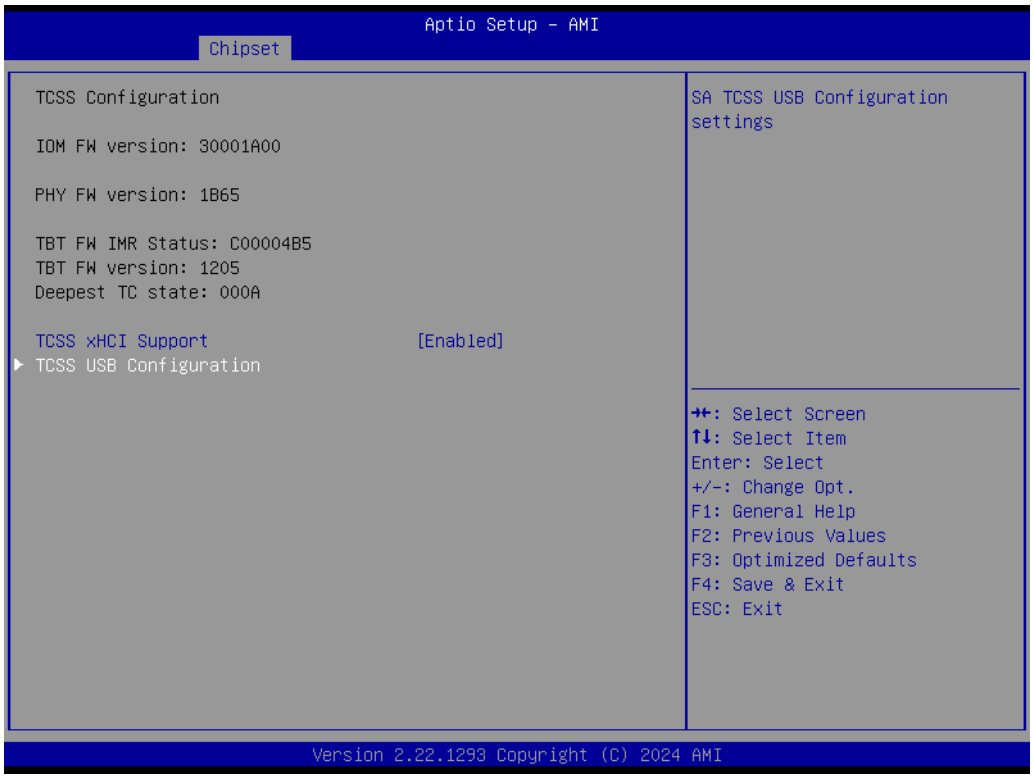
TCSS Setup Menu

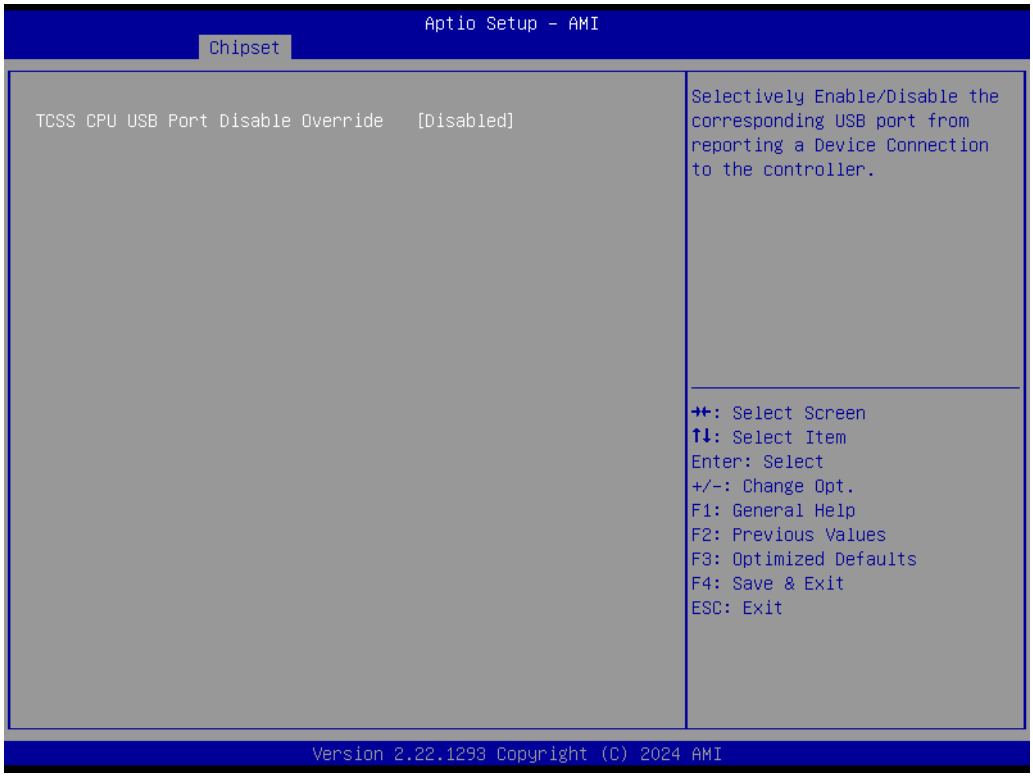




- **TCSS xHCI Support**
  Enable/Disable TCSS xHCI.

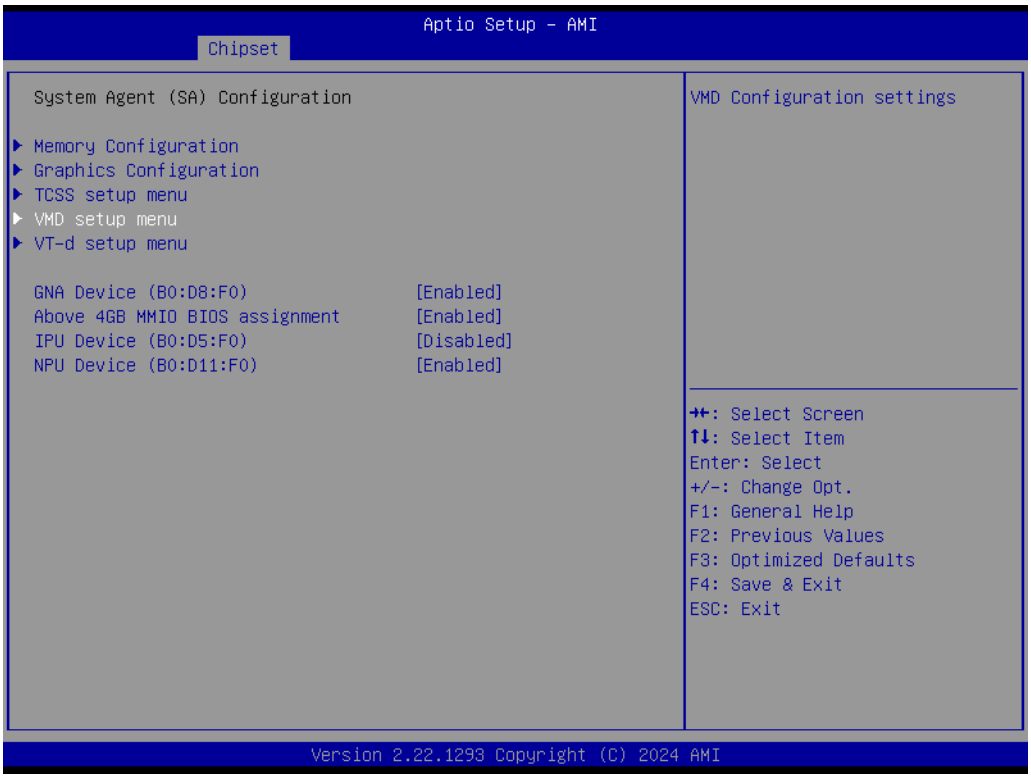
TCSS USB Configuration





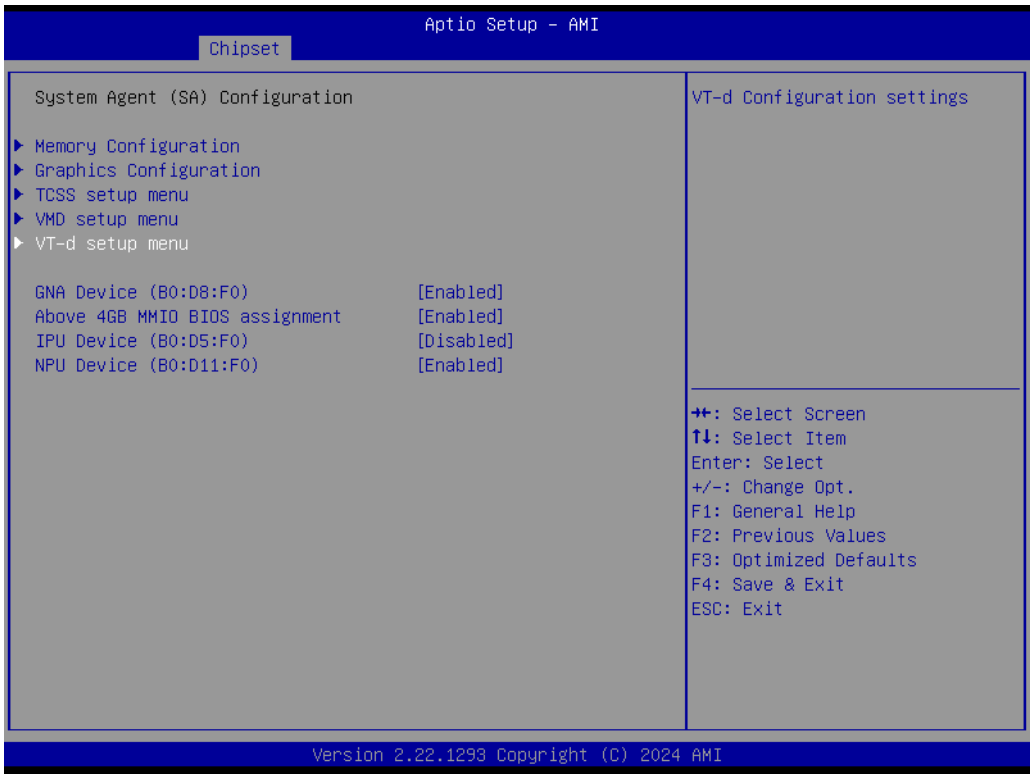
- **TCSS CPU USB Port Disable Override**
  Selectively Enable/Disable the corresponding USB port from reporting a Device Connection to the controller.

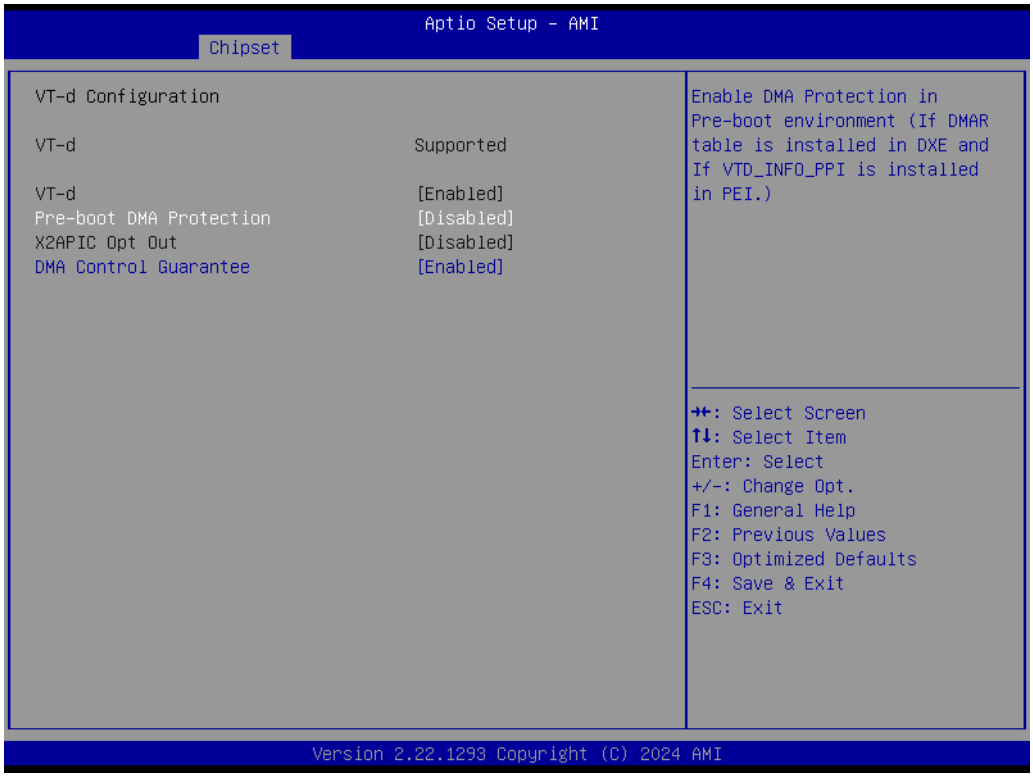
VMD Setup Menu



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

VT-d Setup Menu



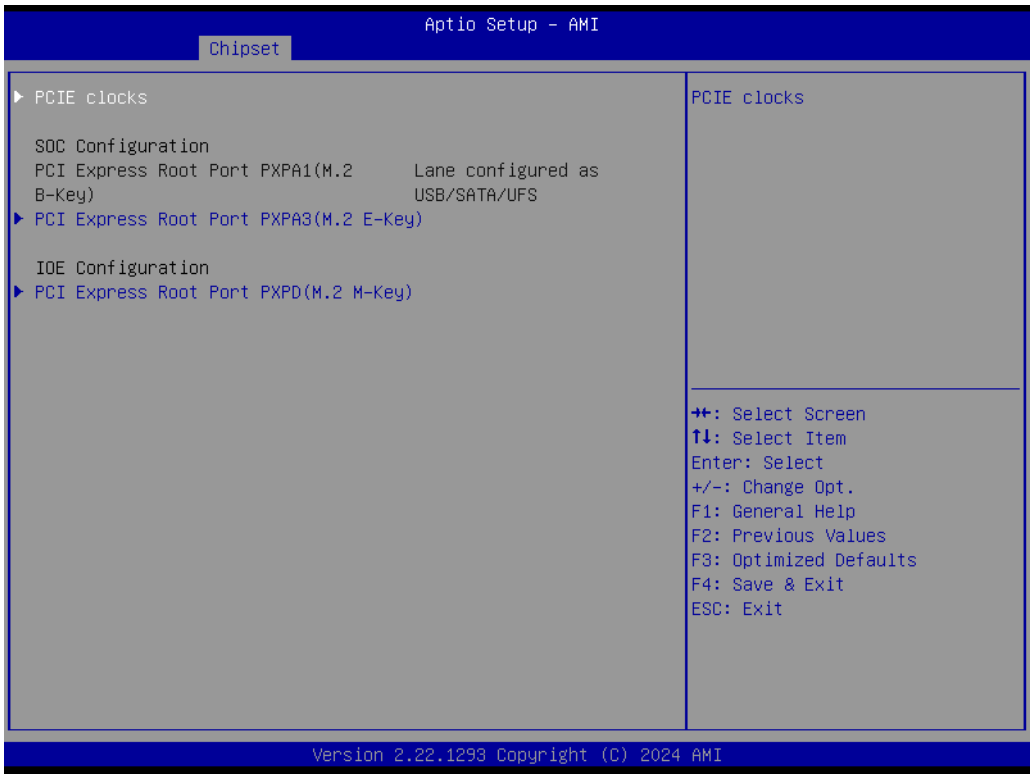


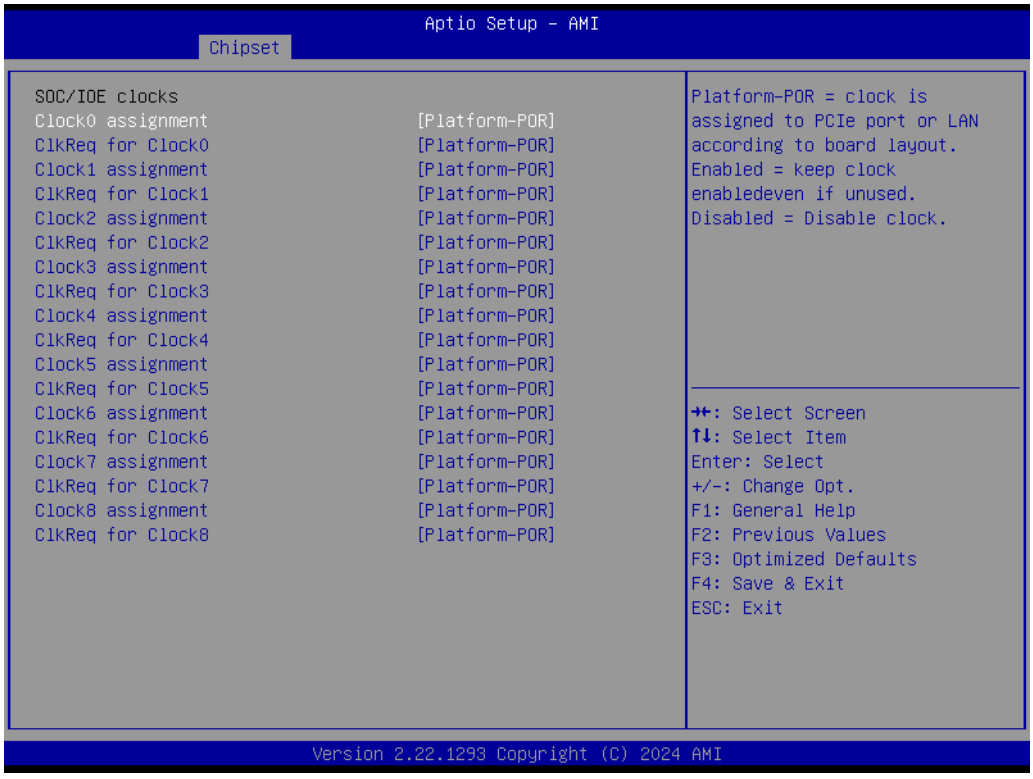
- **VT-d**
  Check to enable VT-d function on MCH.\nThis option will be grayed out when 'X2APIC Enable' option is configured as 'Enabled'.
- **Pre-boot DMA Protection**
  Enable DMA Protection in Pre-boot environment (If DMAR table is installed in DXE and If VTD_INFO_PPI is installed in PEI.)

- **X2APIC Opt Out**
  Enable/Disable X2APIC_OPT_OUT bit. This option will be grayed out when 'X2APIC Enable' option is configured as 'Enabled'.
- **DMA Control Guarantee**
  Enable/Disable DMA_CONTROL_GUARANTEE bit.

3.2.3.2 PCIE Configuration

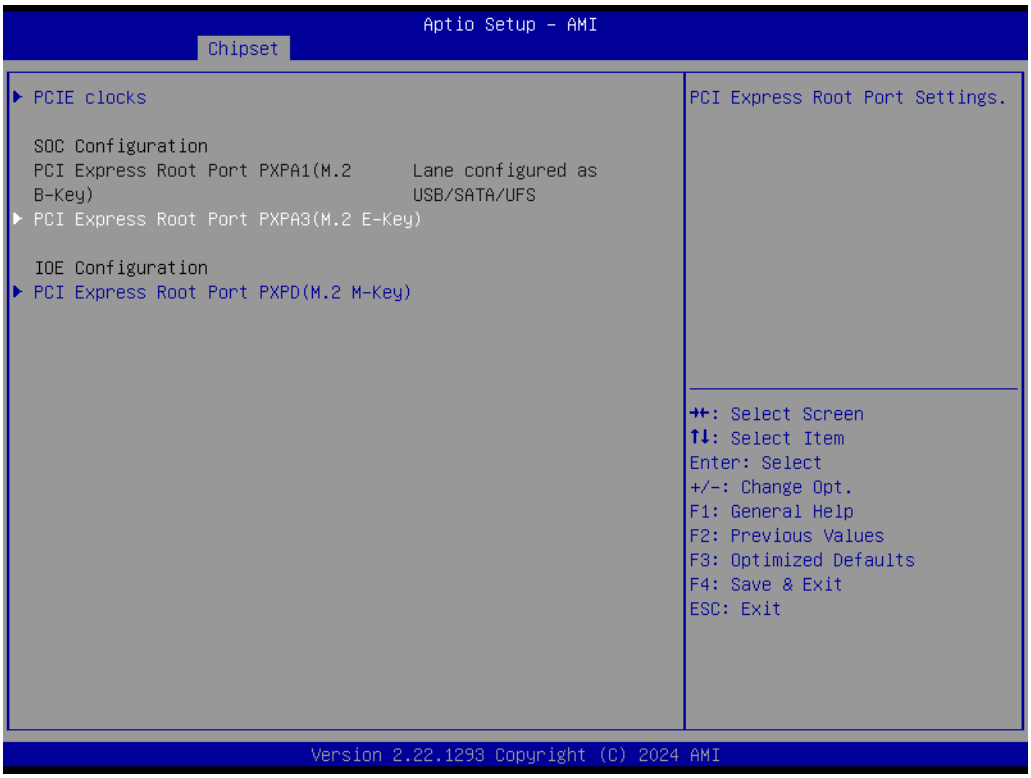
PCIE Clocks

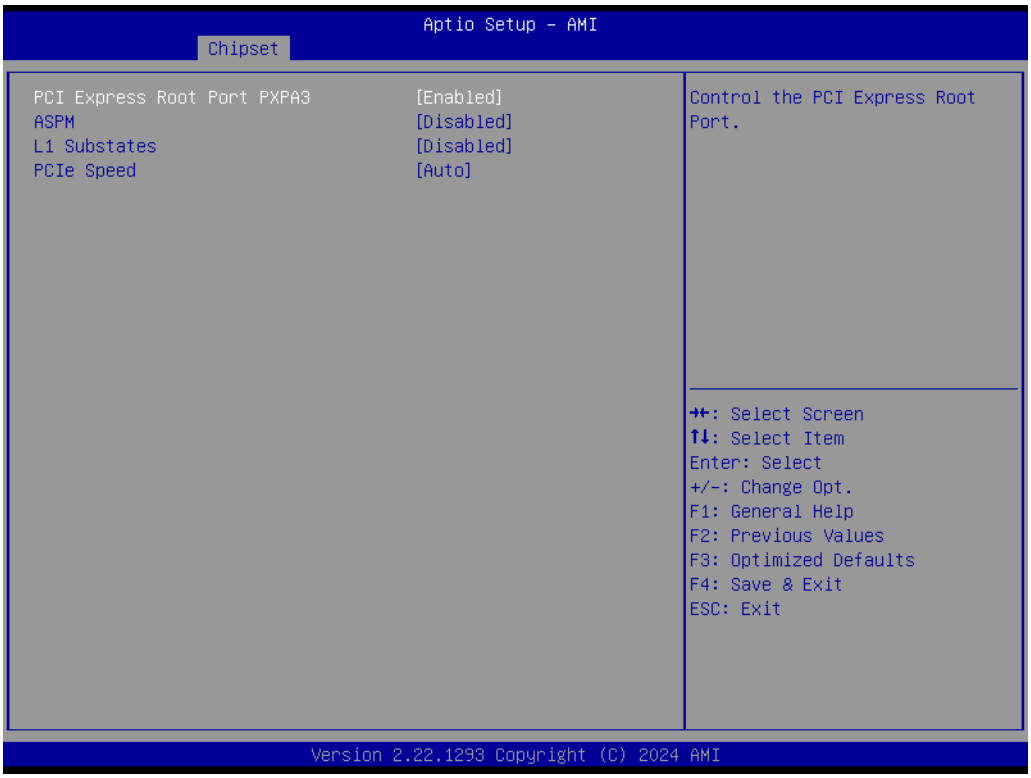




- **ClockX assignment**
  Platform-POR = clock is assigned to PCIe port or LAN according to board layout. Enabled = keep clock enabledeven if unused. Disabled = Disable clock.
- **C1kReq for ClockX**
  Platform-POR = CLKREQ signal is assigned to CLKSRC according to board layout. Disabled = CLKREQ will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

PCI Express Root Port PXPA3 (M.2 M-Key)

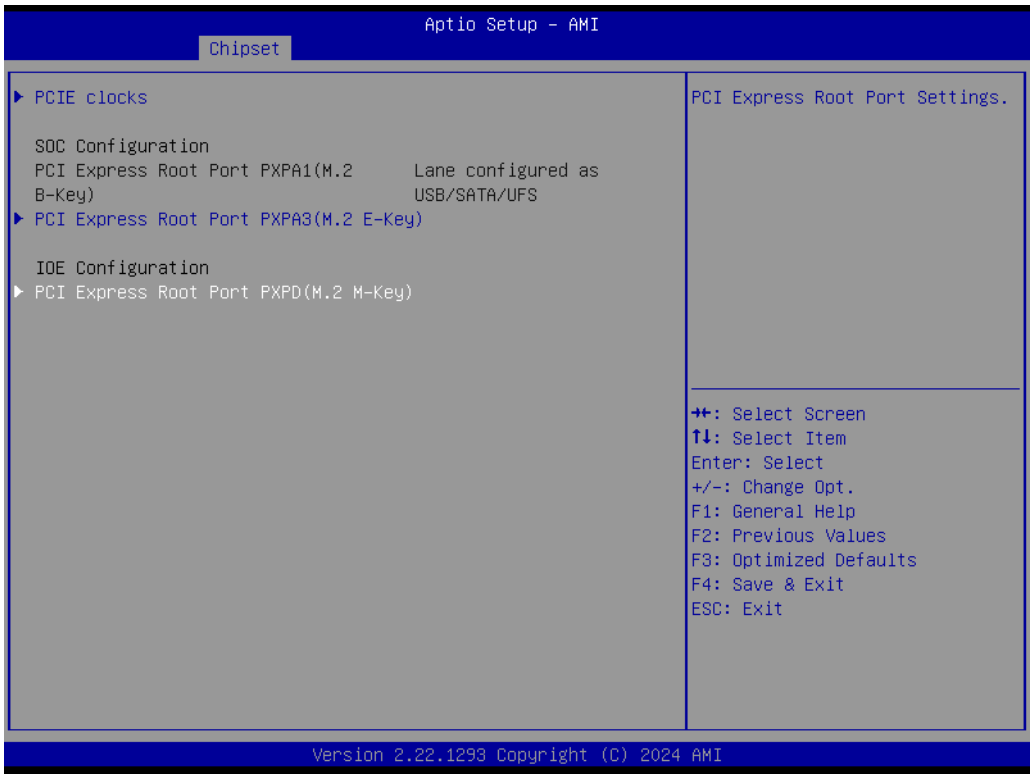


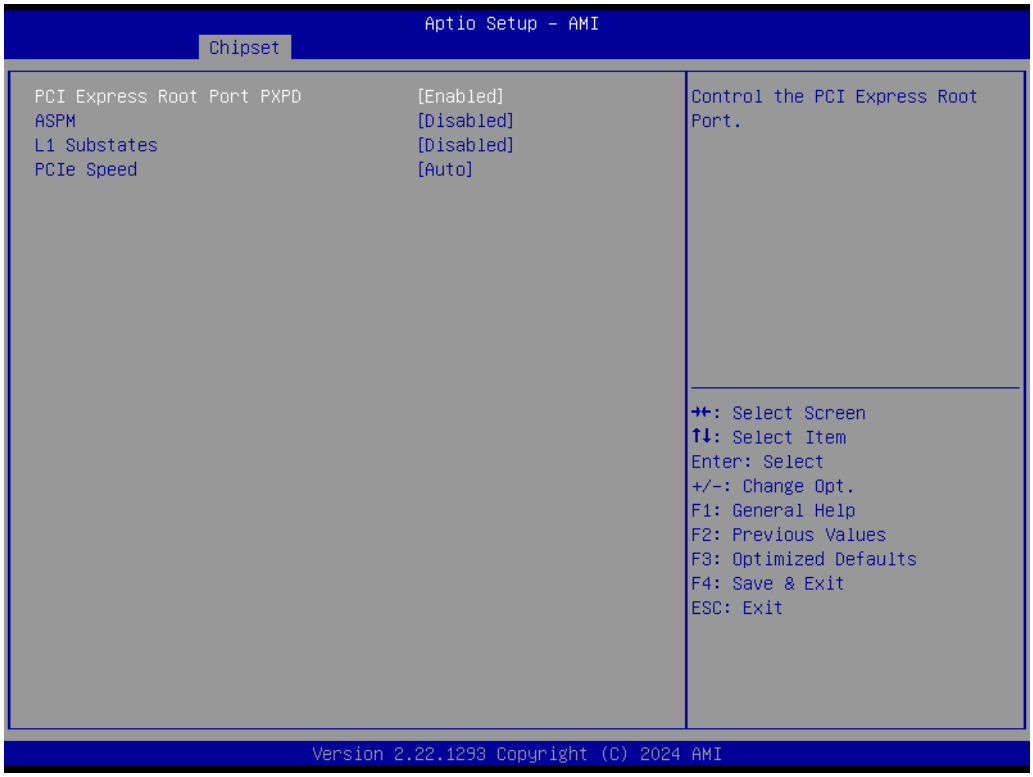


- **PCI Express Root Port PXPA3**
  Control the PCI Express Root Port.
- **ASPM**
  Set the ASPM Level: Force L0s - Force all links to L0s State. AUTO - BIOS auto configure. DISABLE - Disables ASPM

- **L1 Substates**
  PCI Express L1 Substates settings.
- **PCIe Speed**
  Configure PCIe Speed.

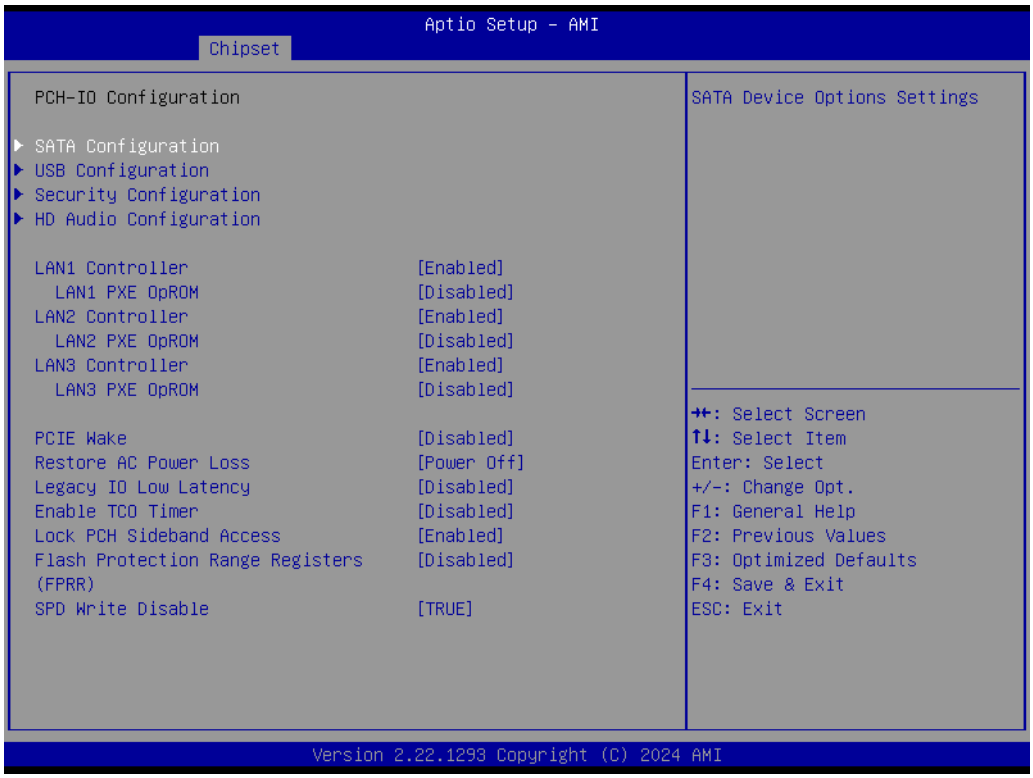
PCI Express Root Port PXPD(M.2 M-Key)





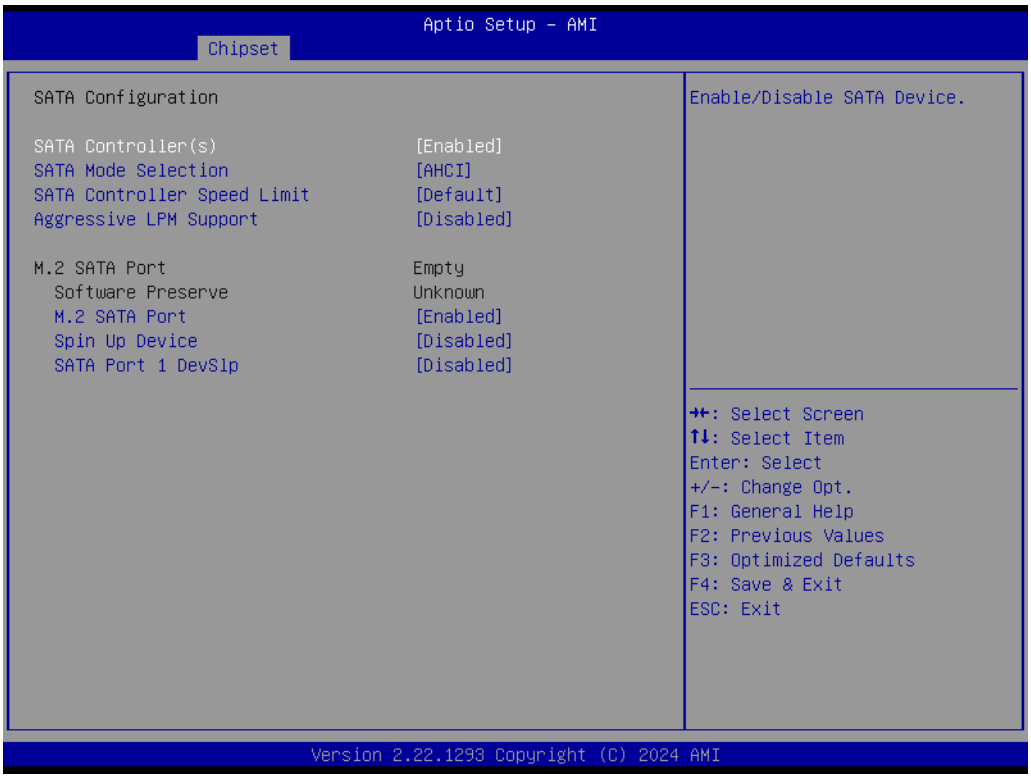
- **PCI Express Root Port PXPD**
  Control the PCI Express Root Port.
- **ASPM**
  Set the ASPM Level: Force L0s - Force all links to L0s State. AUTO - BIOS auto configure. DISABLE - Disables ASPM
- **L1 Substates**
  PCI Express L1 Substates settings.
- **PCIe Speed**
  Configure PCIe Speed.

3.2.3.3 PCH-IO Configuration



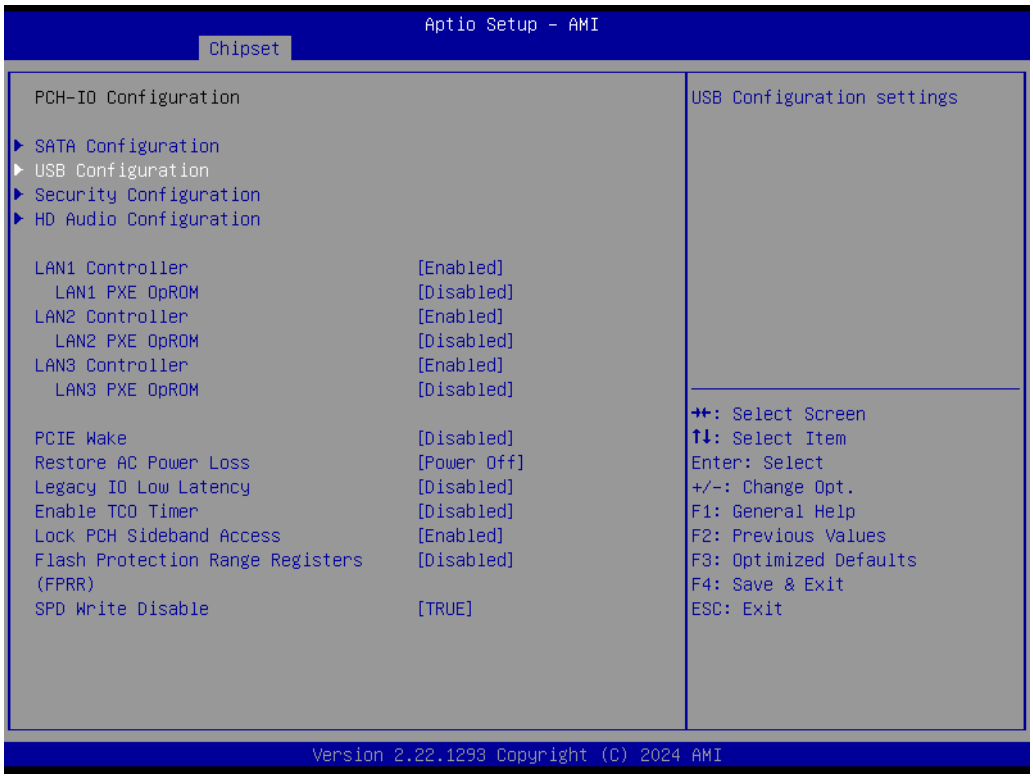
- **LAN Controller**
  Enable or Disable onboard NIC.
- **LAN PXE OpROM**
  Enable or disable boot option rom for LAN1 Controller.
- **PCIE Wake**
  Enable or disable PCIE to wake the system from S5.
- **Restore AC Power Loss**
  Specify what state to go to when power is re-applied after a power failure (G3 state).
- **Legacy IO LOW Latency**
  Set to enable low latency of legacy IO. Some systems require lower IO latency irrespective of power. This is a tradeoff between power and IO latency.
- **Enable TCO Timer**
  Enable/Disable TCO timer. When disabled, it disables PCH ACPI timer, stops TCO timer, and ACPI WDAT table will not be published.
- **Lock PCH Sideband Access**
  Lock PCH Sideband access, include SideBand interface lock and SideBand PortID mask for certain end point (e.g. PSFx). The option is invalid if POST-BOOT SAI is set.
- **Flash Protection Range Registers (FPRR)**
  Enable Flash Protection Range Registers.
- **SPD Write Disable**
  Enable/Disable setting SPD Write Disable. For security recommendations, SPD write disable bit must be set.

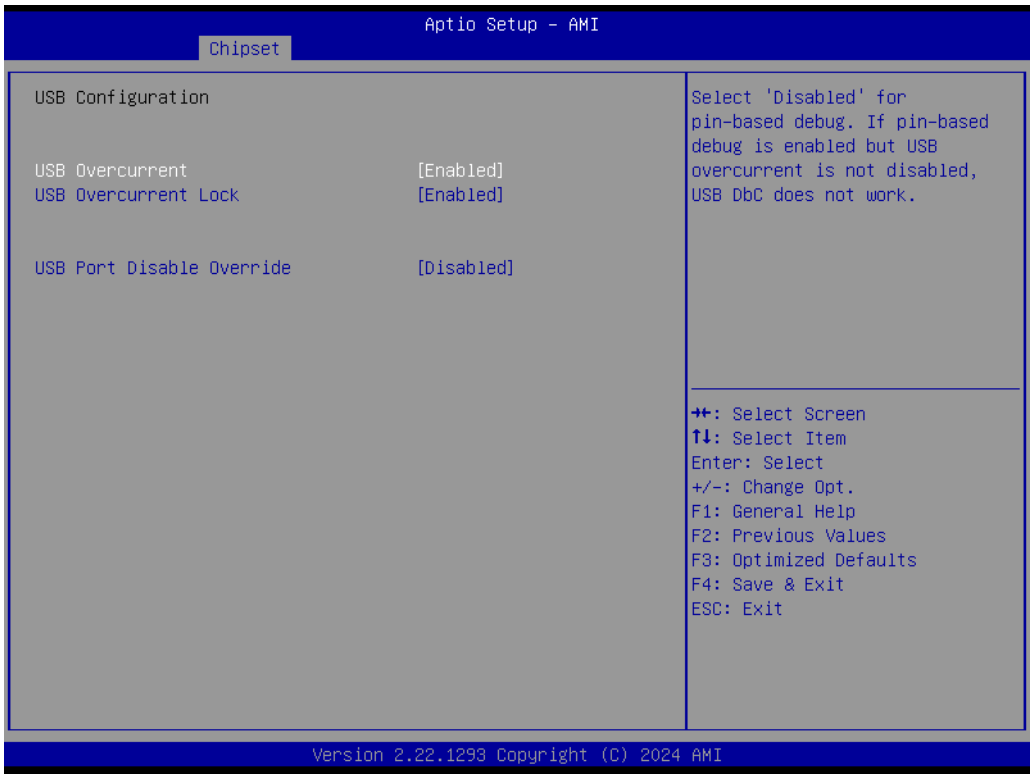
SATA Configuration



- **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**
  Disable/Enable PCH to aggressively enter link power state.
- **M.2 SATA Port**
  Enable or Disable SATA/mSATA Port.
- **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 Port 1 DevSlp**
  Enable/Disable SATA Port 1~2 DevSlp. For DevSlp to work, both the hard drive and SATA port need to support the DevSlp function; otherwise an unexpected behavior might happen. Please check the board design before enabling it.

USB Configuration

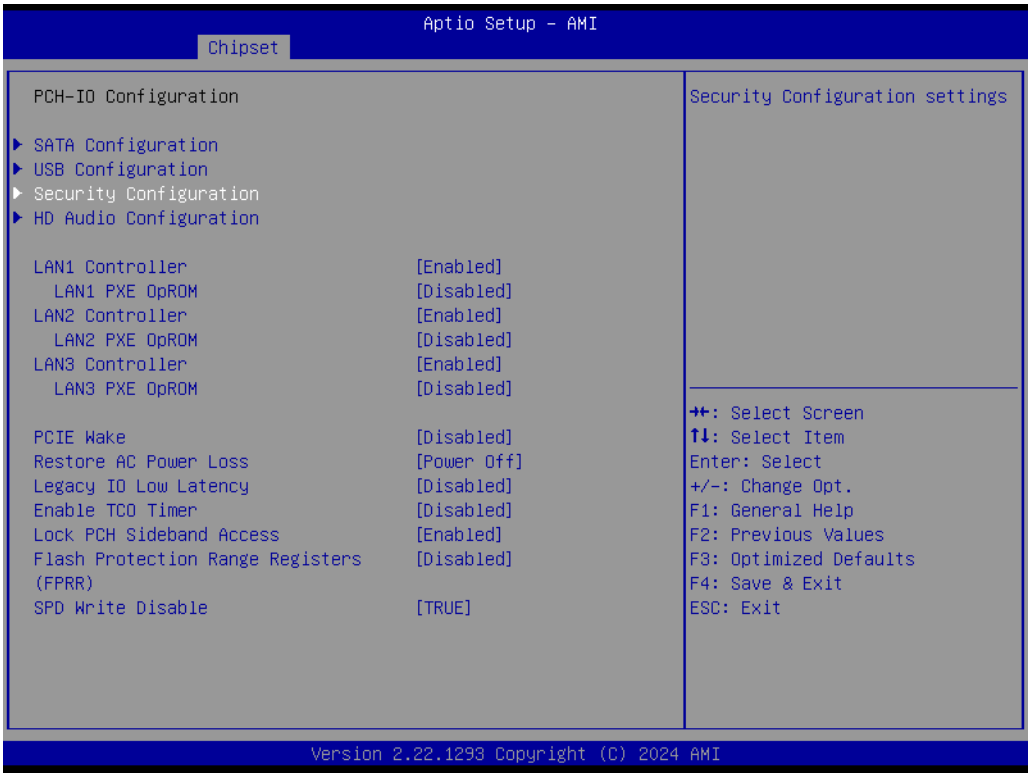


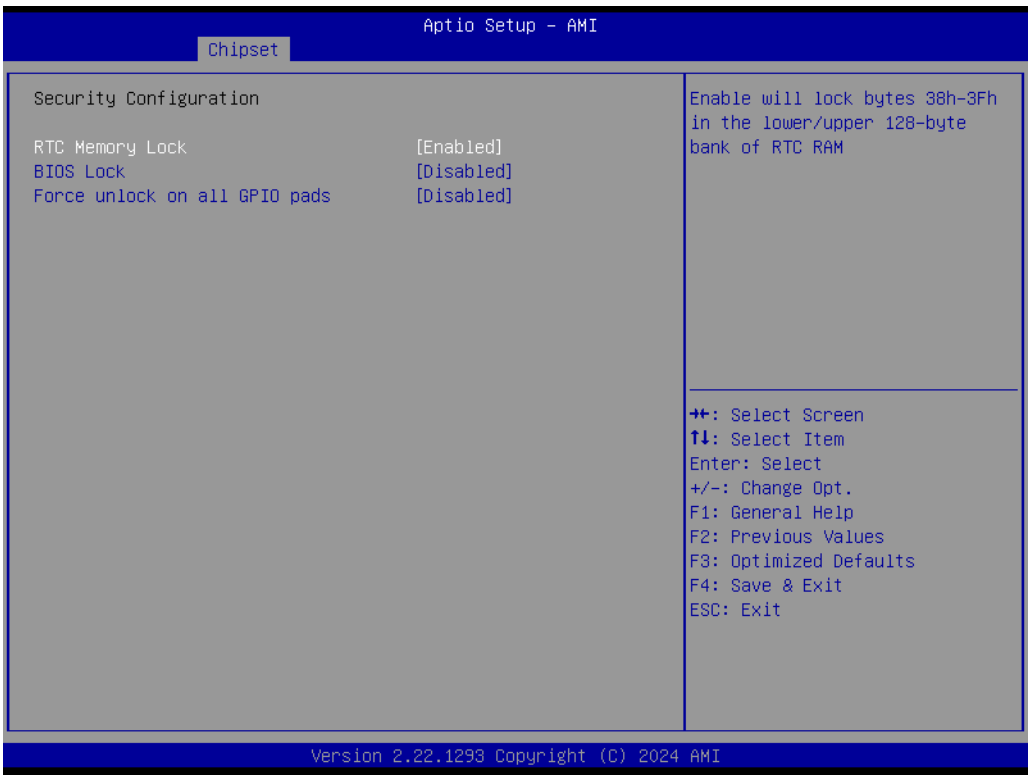


- **USB Overcurrent**
  Select 'Disabled' for pin-based debug. If pin-based debug is enabled but USB overcurrent is not disabled, USB DbC does not work.
- **USB Overcurrent Lock**
  Select 'Enabled' if Overcurrent functionality is used. Enabling this will make xHCI controller consume the Overcurrent mapping data.

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

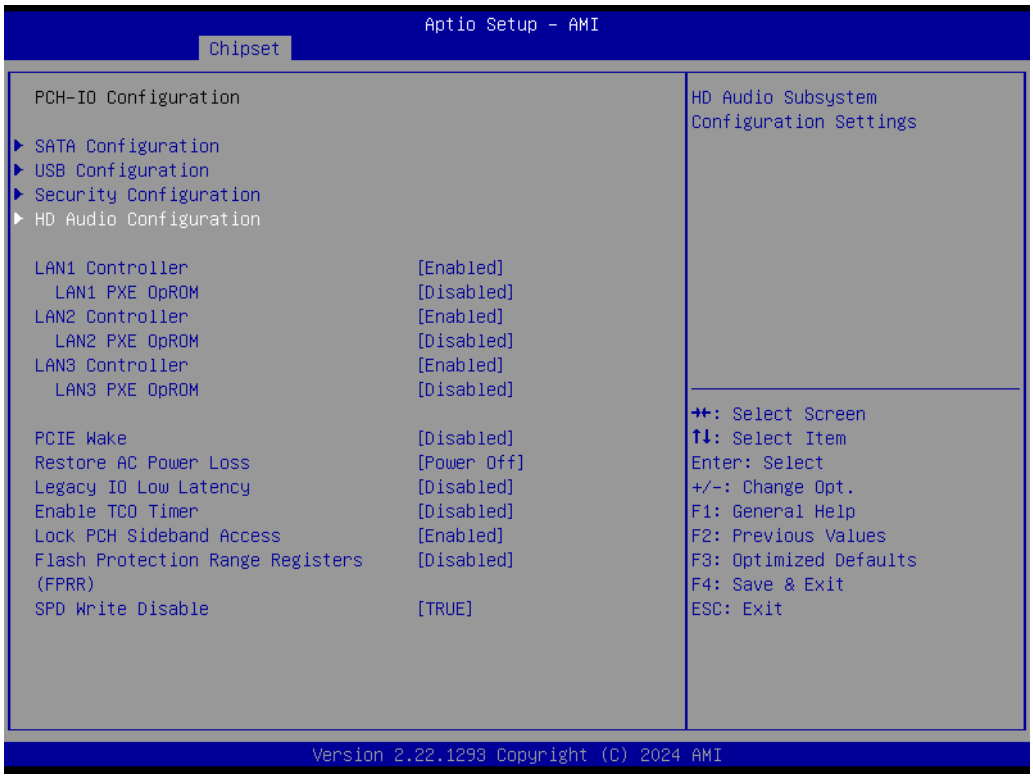
Security Configuration

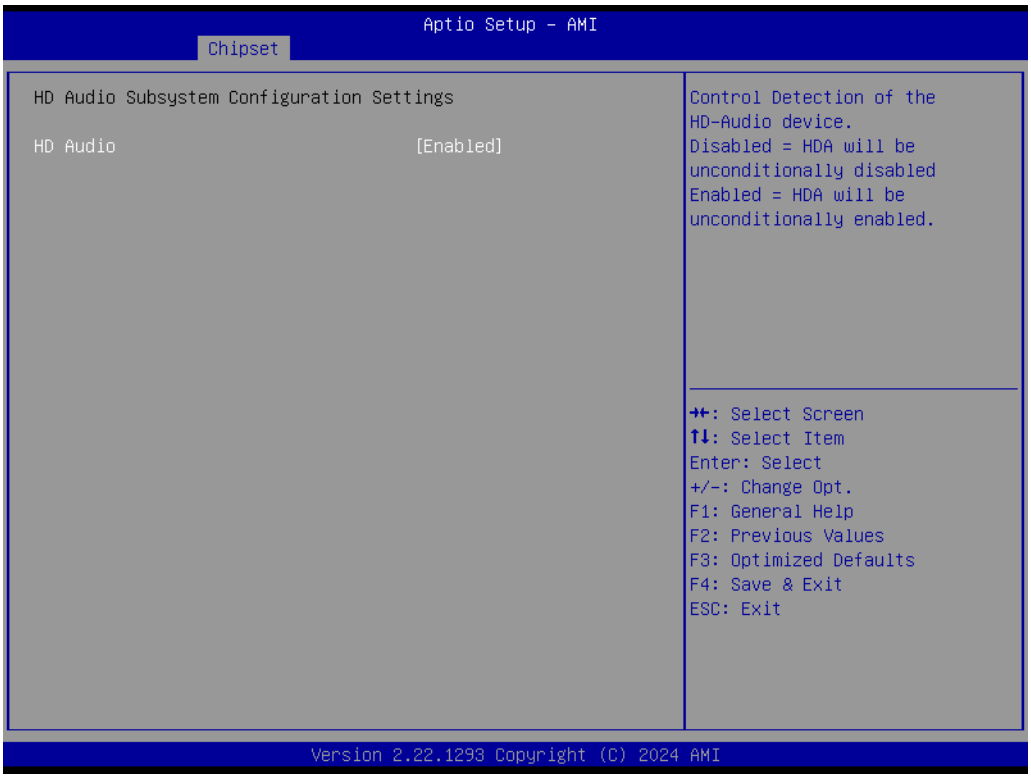




- **RTC Memory Lock**
  Enable will lock bytes 38h-3Fh in the lower/upper 128-byte bank of RTC RAM.
- **BIOS Lock**
  Enable/Disable the PCH BIOS Lock Enable feature. It is required to be enabled to ensure SMM protection of flash.
- **Force unlock on all GPIO pads**
  If Enabled, the BIOS will force all GPIO pads to be in the unlocked state.

HD Audio Configuration



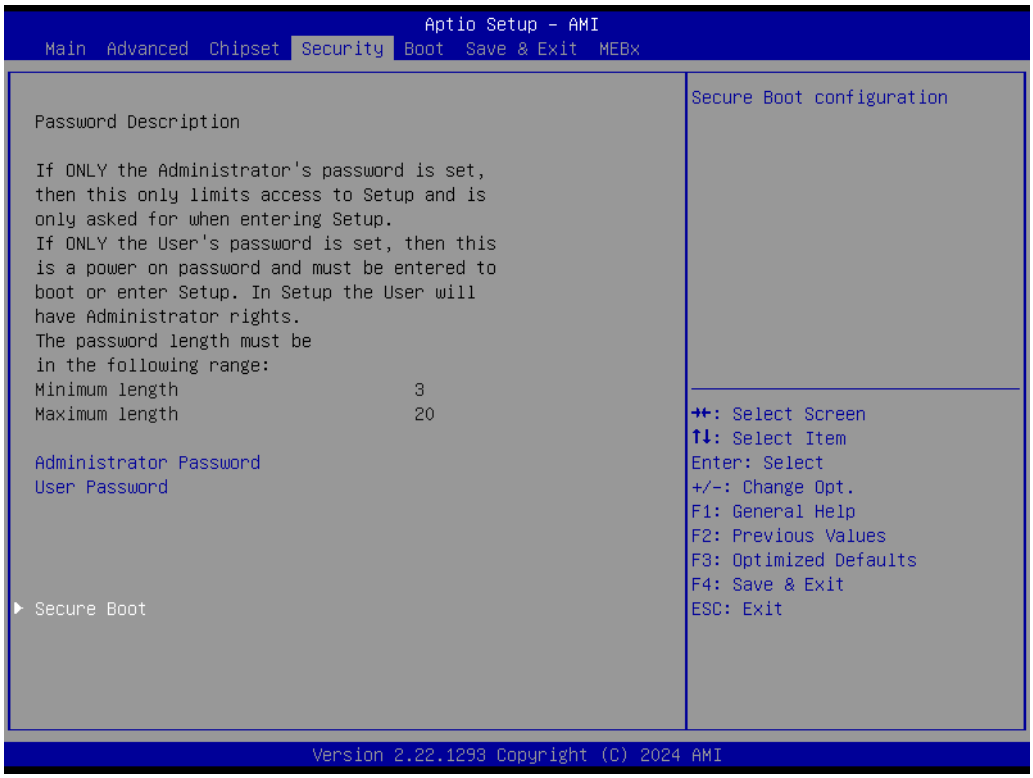


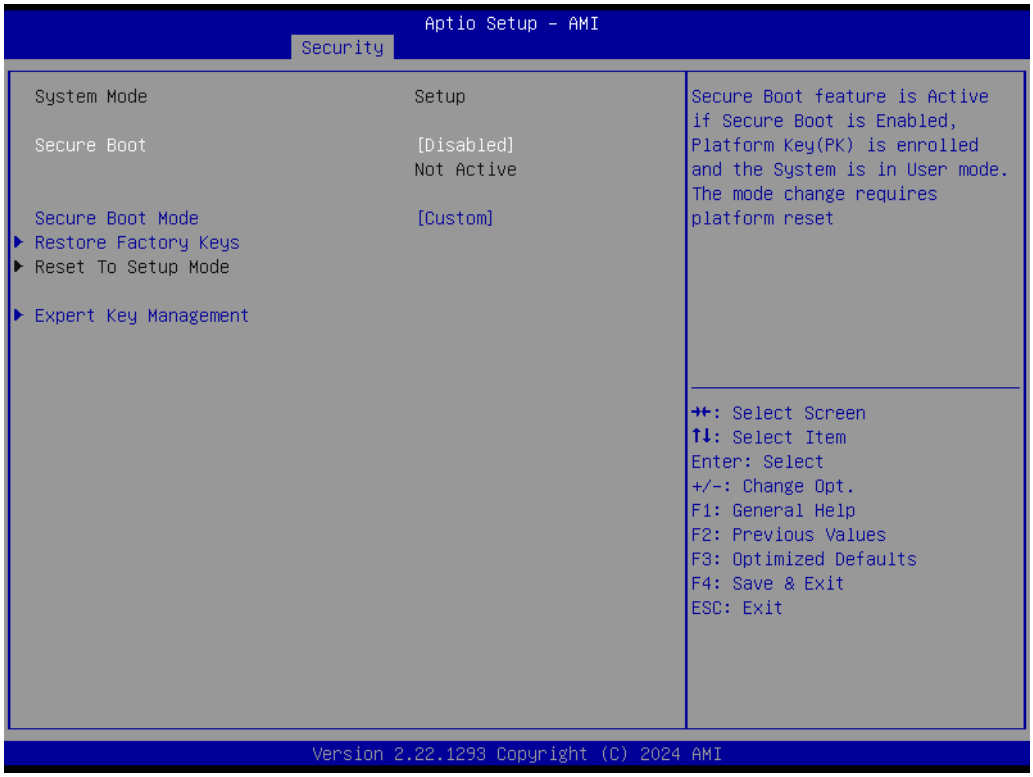
- **HD Audio**
  Control Detection of the HD-Audio device.

3.2.4 Security

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

Secure Boot





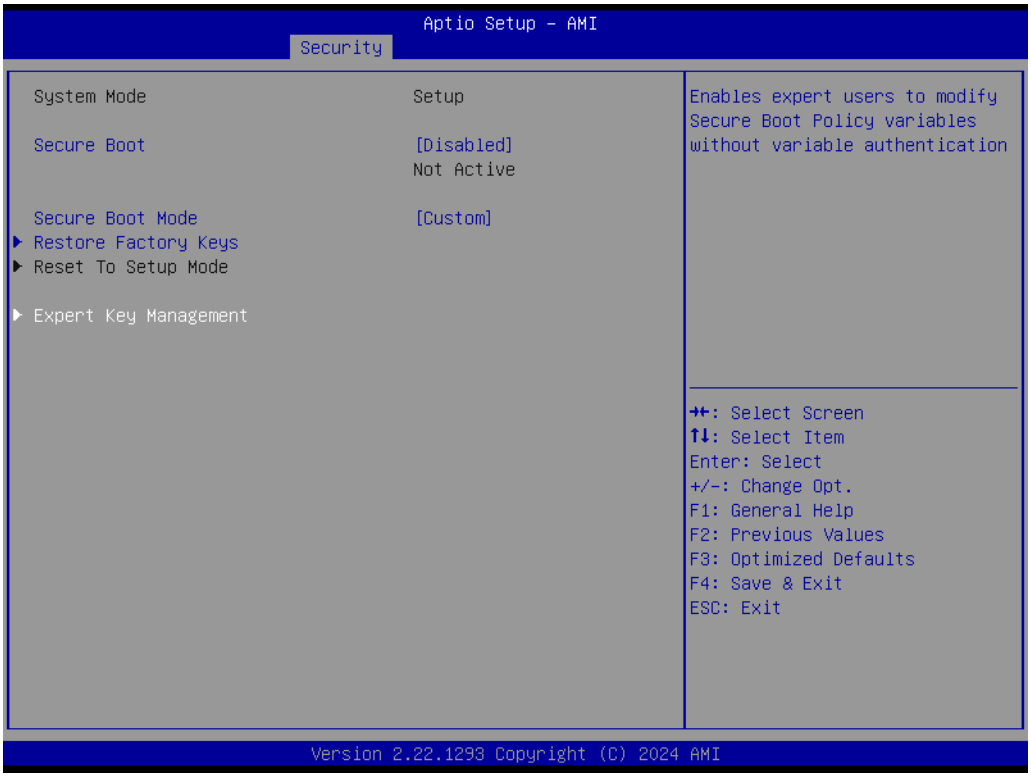
- **Secure Boot**

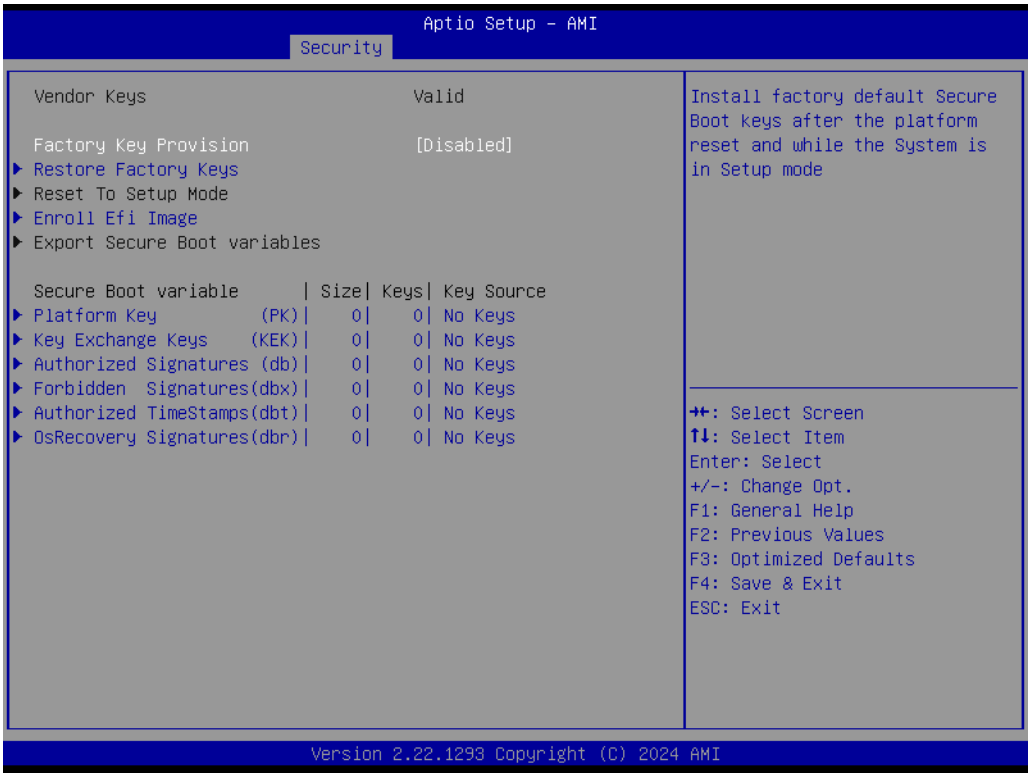
  The Secure Boot feature is Active if Secure Boot is Enabled, Platform Key (PK) is enrolled, and the System is in User mode. The mode change requires a platform reset.

- **Secure Boot Mode**

  Secure Boot mode options: Standard or Custom.

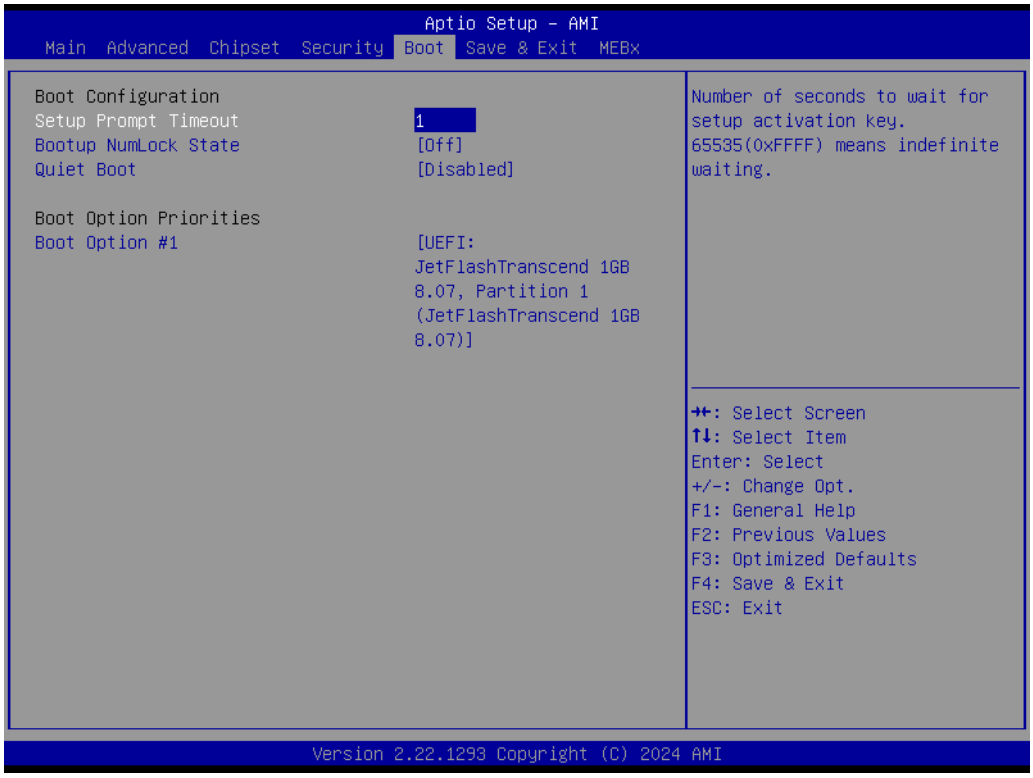
Expert Key Management





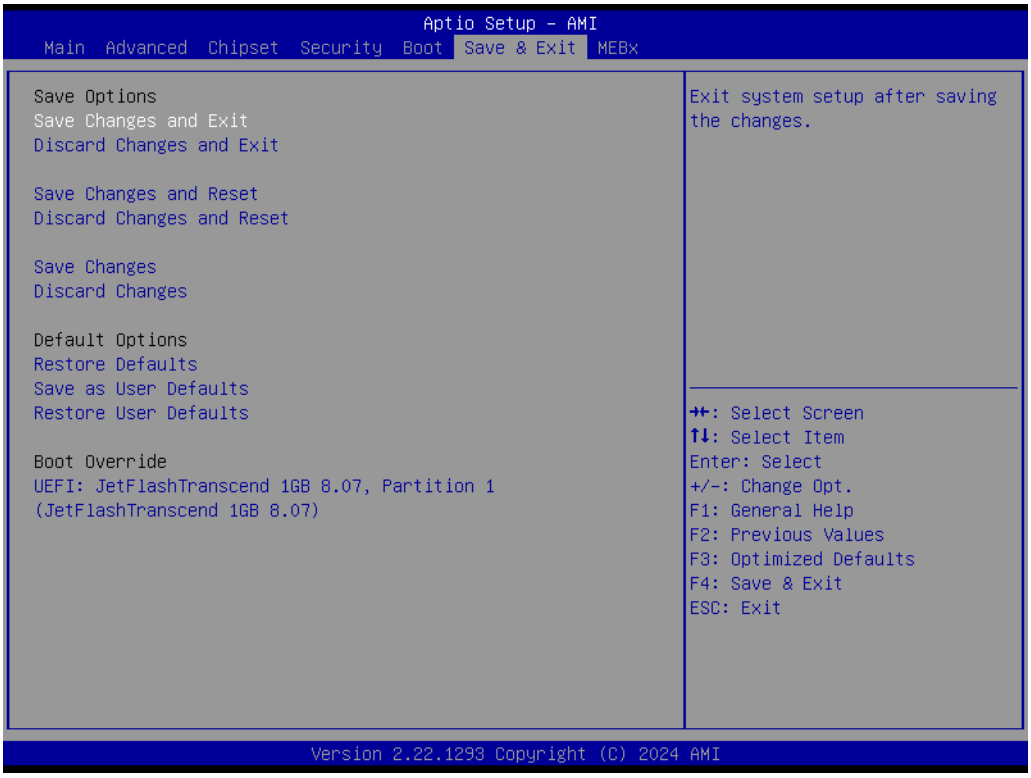
- **Factory Key Provision**
  Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.

3.2.5 Boot



- **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**
  Enables or disables the Quiet Boot option.

3.2.6 Save & Exit



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

3.2.7 MEBx


Aptio Setup – AMI
Main Advanced Chipset Security Boot Save & Exit MEBx
Configuration locked after
EndOfPost
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1293 Copyright (C) 2024 AMI

ADVANTECH

Enabling an Intelligent Planet

www.advantech.com