ROC288A

1U 19”DC-DC Fanless Server With Intel 14th /13th Processor

13th Raptor lake

14th Raptor Lake Refresh

User’s Manual

Revision Date: May ,13, 2025

sSafety Information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

Statement

- All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- All trademarks are the properties of the respective owners.
- All product specifications are subject to change without prior notice

Revision History

Revision	Date (mm.dd.yyyy)	Changes
V1.0	5.13.2025	First release

Packing list

Item	Description	Q'ty
1	ROC288-A System	1
2	CD(Drivier + User's manual)	1
3	Ear mounting & Screw	1 Set

If any of the above items is damaged or missing, please contact your local distributor.

Table of Contents

Safety Information....1
Electrical safety....1
Operation safety....1
Statement....1
Revision History....2
Packing list....2
Chapter 1 : Product Information....5
1.1 Key Feature....5
1.2 I/O Placement....7
Chapter 2 : I/O Connector & SSD Tray Door....8
2.1 2.5GbE RJ-45 LAN Jack....8
2.2 USB 10Gbps Port....8
2.3 Display Port....8
2.3 HDMI™ Connector....8
2.4 Mic-in Jack....8
2.5 Line-Out Jack....8
2.6 Line-Out Jack....8
Chapter 3 : BIOS Setup....10
3.1 The Menu Bar....12
3.2 Main....13
3.3 Advanced....16
3.4 Boot....23

3.5 Security 24

3.6 Chipset 33

3.7 Power 34

3.8 Save & Exit 35

Chapter 1 : Product Information

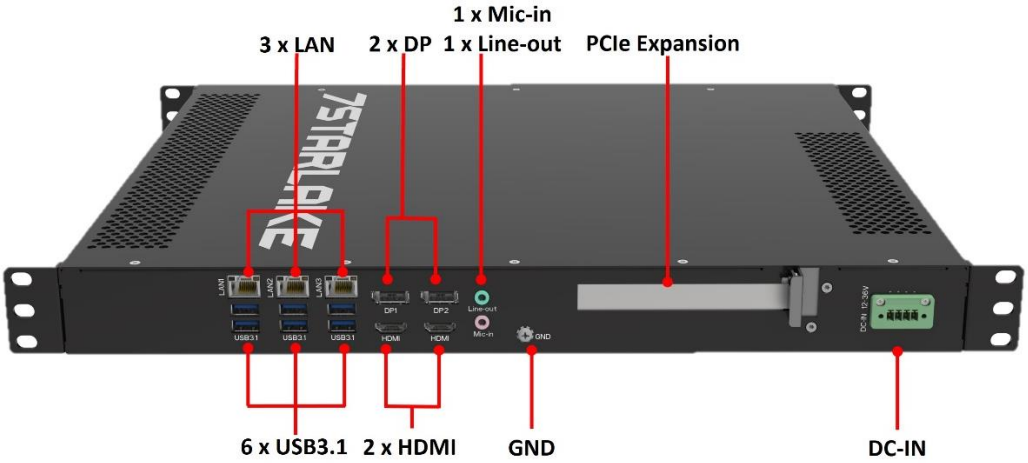
1.1 Key Feature

System	
HighPerformance Processor	14th/13th Gen Intel® Raptor Lake-R/Raptor Lake-S LGA1700 Socket Processor / Core i9/i7/i5/i3 Processor / TDP 65W
Memory type	DDR5 5200 MHz / 2 x 262-pin SO-DIMM / Max. 64 GB (Non-ECC/ECC)
Chipset	Intel® Q670E/R680E Chipset
Expansion Slot	1 x PCIe expansion slot(PCIe x 16 HHHL)
Display	
DP	Resolution up to 4096 x 2304 @60Hz
HDMI	Resolution up to 4096 x 2304 @60Hz
Storage	
HDD/SDD	2 x 2.5" Solid State Disk (SSD) 2 x SATAIII
Ethernet	
Ethernet	1 x Intel® I226-LM 2.5Giga LAN 2 x Intel® I226-V 2.5Giga LAN
Front I/O	
Easy Swap SSD Tray	2
Button	1 x Power Button w/Indicator LED
Indicator LED	SSD
Rear I/O	
DisplayPort	2 x DP
HDMI	2 x HDMI
Ethernet	3 x 2.5GbE RJ45
Audio	1 x Mic-in, 1 x Line-out
USB Port	6 x USB 3.1
PCIe expansion	1 x PCIe expansion slot (PCIe x 16 FHHL)

DC-IN	1 x DC plug
Power Requirement	
Power Input	DC-IN 12~36V
Physical	
Dimensions (W x D x H)	430 x 370 x 44.4 mm
Chassis	SECC
Environment	
Green Product	RoHS design to meet
Operating Temperature	ET : -20°C to +50°C UT : -30°C to +60°C
Storage Temperature	-40 to 85°C
Relative Humidity	5% to 95%, non-condensing
EMC	CE and FCC design to meet
Operation System	
OS	Windows®10/11 64-bit Linux(Support by request)

***All specifications and photos are subject to change without notice.**

1.2 I/O Placement

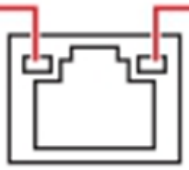


Chapter 2 : I/O Connector & SSD Tray Door

2.1 2.5GbE RJ-45 LAN Jack

The standard single RJ45 LAN jack is provided for connection to the Local Area Network (LAN). You can connect a network cable to it.

Link/ Activity LED	
Status	Description
Off	No link
Yellow	Linked
Blinking	Data activity



Speed LED	
Status	Description
Off	10/100 Mbps
Green	1000 Mbps
Orange	2.5 Gbps

2.2 USB 10Gbps Port

USB 10Gbps, delivers high-speed data transfer for various devices, such as storage devices, hard drives, video cameras, etc.

2.3 Display Port

DisplayPort is a digital display interface standard. This connector is used to connect a monitor with DisplayPort inputs.

2.3 HDMI™ Connector

HDMI™ is a digital interface for uncompressed audio/video streams, accommodating all TV formats and multi-channel audio on a single cable. It supports 4096x2304@60Hz as specified in HDMI™ 2.0b.

2.4 Mic-in Jack

This connector is provided for microphones.

2.5 Line-Out Jack

This connector is provided for headphones or speakers.

2.6 Line-Out Jack

ROC280-A support Two 2.5" Easy Swap SSD :

Use cross pliers to open screw and pull out the 2.5" SSD Tray

Put 2.5" SSD on the tray and make sure SSD is fixed and push the tray back

Usecross pliers to lock the tray door

Chapter 3 : BIOS Setup

This chapter provides information on the BIOS Setup program and allows users to configure the system for optimal use.

Users may need to run the Setup program when:

· An error message appears on the screen at system startup and requests users to run SETUP.

· Users want to change the default settings for customized features.

Important

· Please note that BIOS update assumes technician-level experience.

· AsthesystemBIOSisundercontinuousupdateforbettersystemperformance,the illustrations in this chapter should be held for reference only.

Entering Setup

Power on the computer and the system will start POST (Power On Self Test) process. When the message below appears on the screen, press <DEL> or <F2> key to enter Setup, <F11> key to Boot Menu, <F12> key to PXE Boot .

Press <DEL> or <F2> to enter SETUP

If the message disappears before you respond and you still wish to enter Setup, restart the system by turning it **OFF** and **On** or pressing the **RESET** button. You may also restart the system by simultaneously pressing <**Ctrl**>, <**Alt**>, and <**Delete**> keys.

Important

The item sunder each BIOS category described in this chapter are under continuous update for better system performance. Therefore, the description may be slightly different from the latest BIOS and should be held for reference only.

Control Keys

←→	Select Screen
↑ ↓	Select Item
Enter	Select
+ -	Change Value
Esc	Exit
F1	General Help
F7	Previous Values
F9	Optimized Defaults
F10	Save & Reset*
F12	Screenshot capture
<K>	Scroll help area upwards
<M>	Scroll help area downwards

* When you press <F10>, a confirmation window appears and it provides the modification information. Select between Yes or No to confirm your choice.

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

The main menu lists the setup functions you can make changes to. You can use the arrow keys (↑↓) to select the item. The on-line description of the highlighted setup function is displayed at the bottom of the screen.

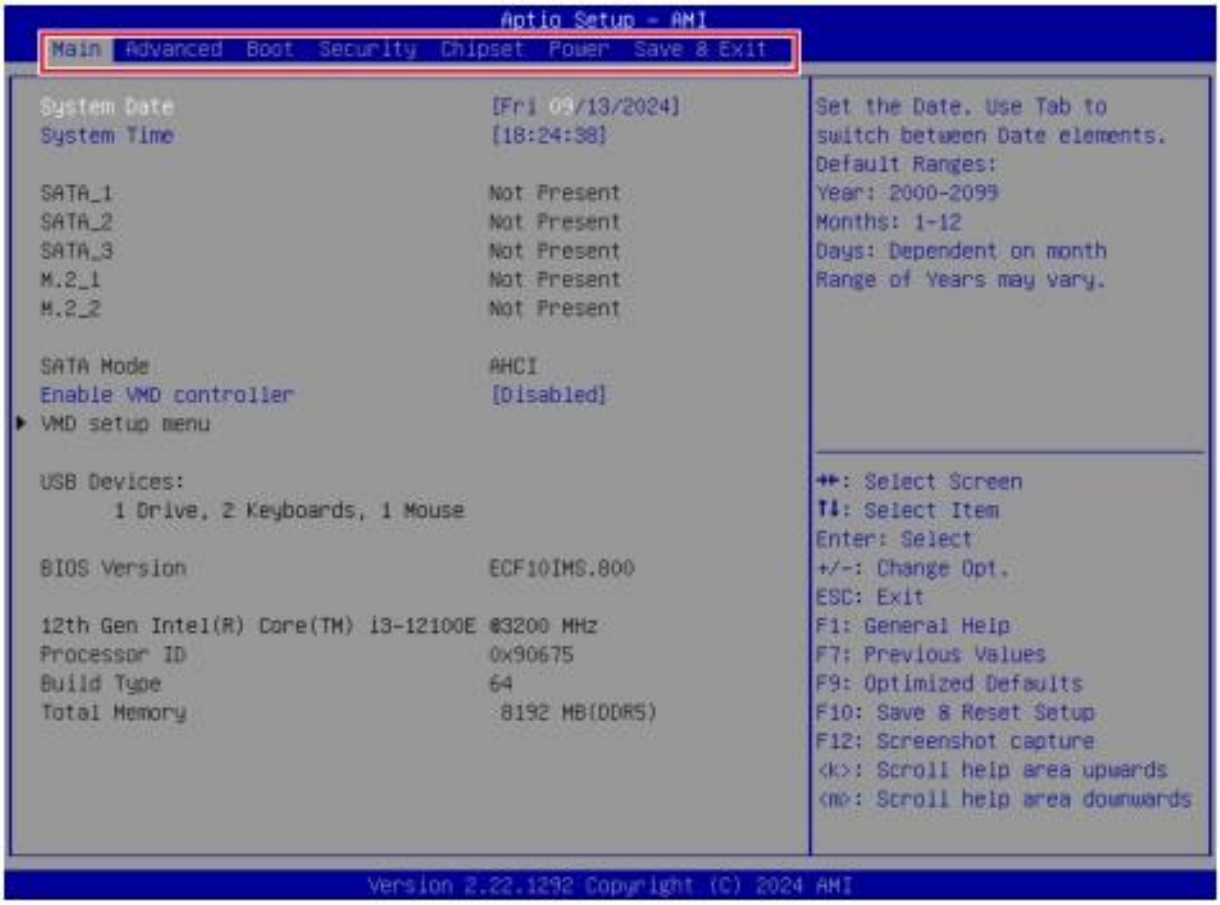
Sub-Menu

If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use arrow keys (↑↓) to highlight the field and press <Enter> to call up the sub-menu. Then you can use the control keys to enter values and move from field to field within a sub-menu. If you want to return to the main menu, just press the <Esc>.

General Help <F1>

The BIOS setup program provides a General Help screen. You can call up this screen from any menu by simply pressing <F1>. The Help screen lists the appropriate keys to use and the possible selections for the highlighted item. Press <Esc> to exit the Help screen.

3.1 The Menu Bar



- Main

  Use this menu for basic system configurations, such as time, date, etc.

- Advanced

  Use this menu to set up the items of special enhanced features.

- Boot

  Use this menu to specify the priority of boot devices.

- Security

Use this menu to set supervisor and user passwords.

- Chipset

This menu controls the advanced features of the on-board chipsets

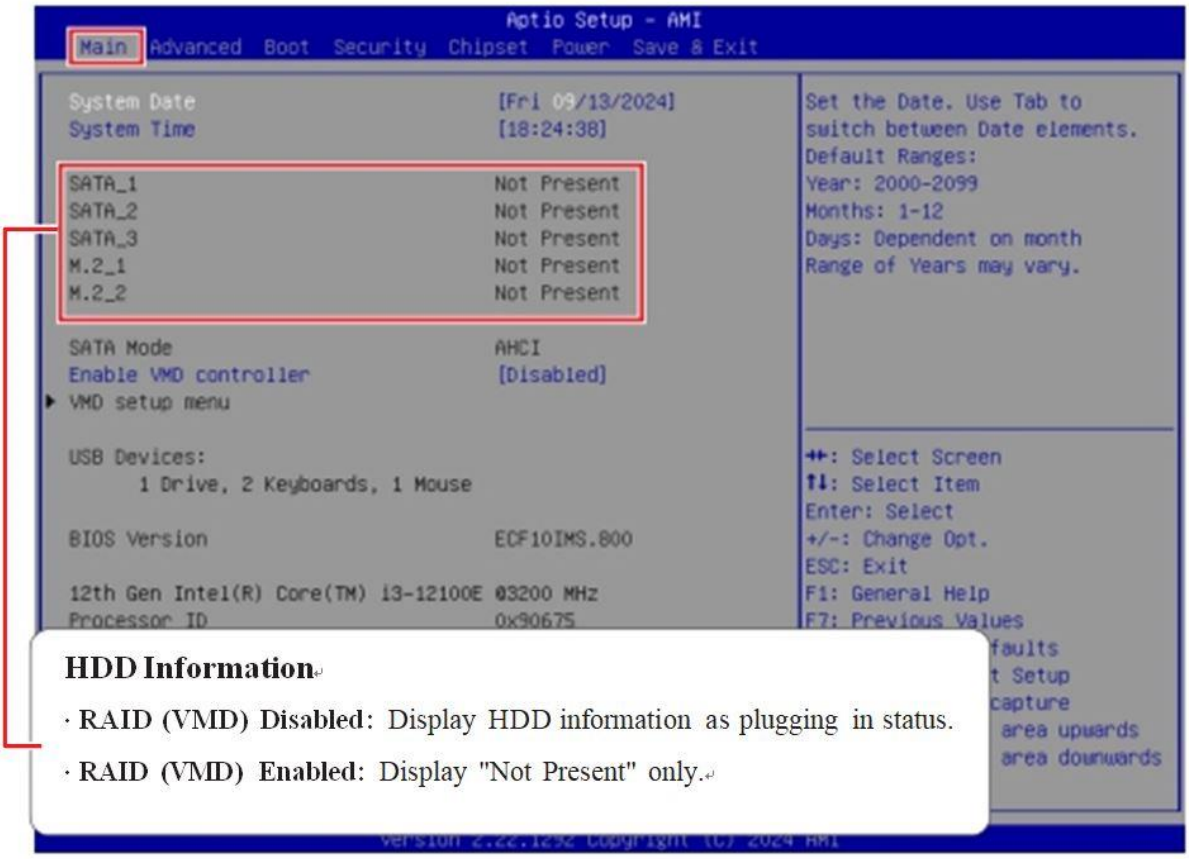
- Power

Use this menu to specify your settings for power management.

- Save & Exit

This menu allows you to load the BIOS default values or factory default settings into the BIOS and exit the BIOS setup utility with or without changes.

3.2 Main



- System Date

This setting allows you to set the system date.

Format: <Day> <Month> <Date> <Year>.

- System Time

This setting allows you to set the system time.

Format: <Hour> <Minute> <Second>.

- SATA Mode Selection

This setting specifies SATA controller mode.

[AHCI] AHCI (Advanced Host Controller Interface), is a technical standard for an interface that allows the software to communicate with Serial ATA (SATA) devices. It offers advanced SATA features such as Native Command Queuing (NCQ) and hot-plugging.

[RAID] RAID (Redundant Array of Independent Disks) is a virtual disk storage technology that combines multiple physical disks into one unit for data redundancy, performance improvement, or both.

- Enable VMD controller

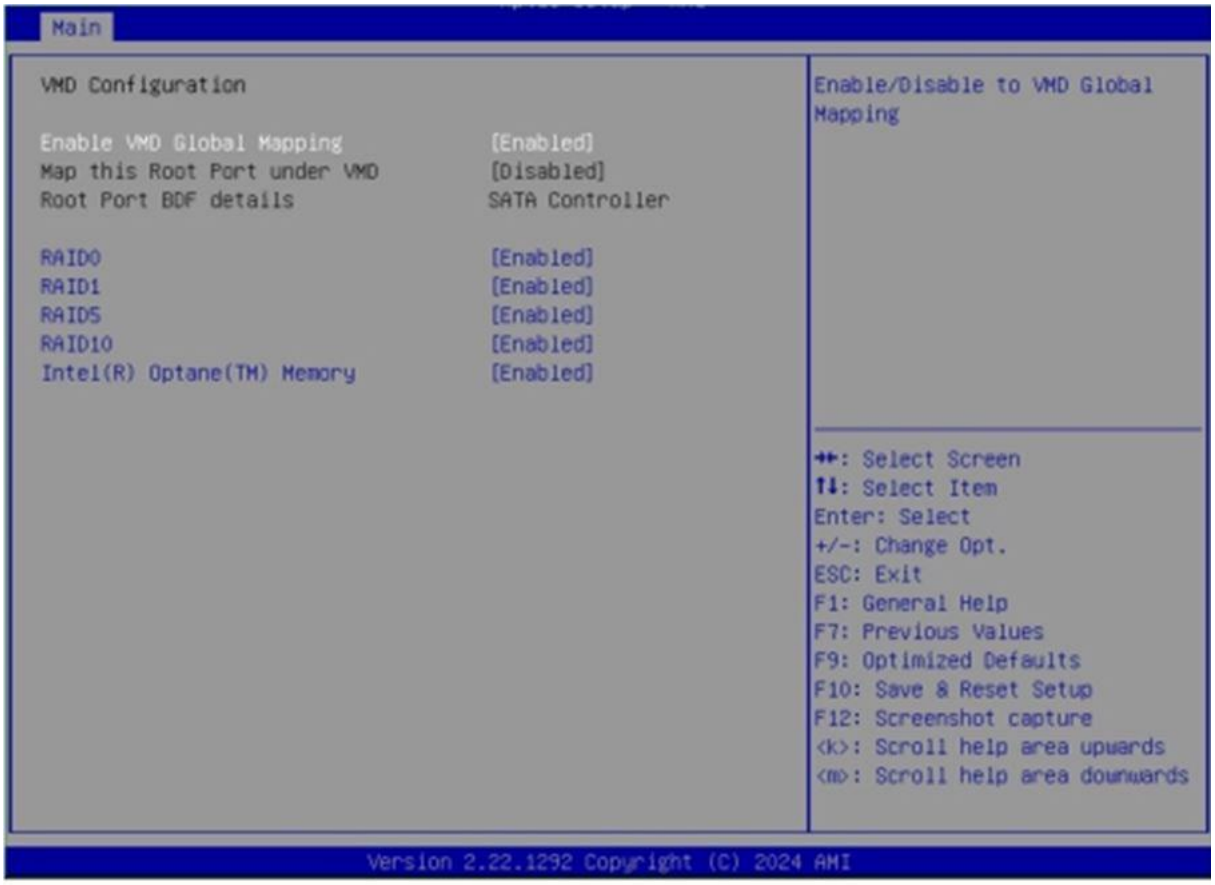
Enables or disables VMD (RAID) controller.

Important

· "SATA_3"isM.2MKeywithSATAsignal,andthe"M.2_2" isM.2BKey.

- VMD Setup Menu (VMD Configuration)

In AHCI mode, this menu will be grayed out and can not be selected.



- Enabled VMD Global Mapping

  Enables or disables Intel VMD mapping. Intel VMD enables direct control and management of NVMe SSDs from the PCIe bus without additional hardware adapters.

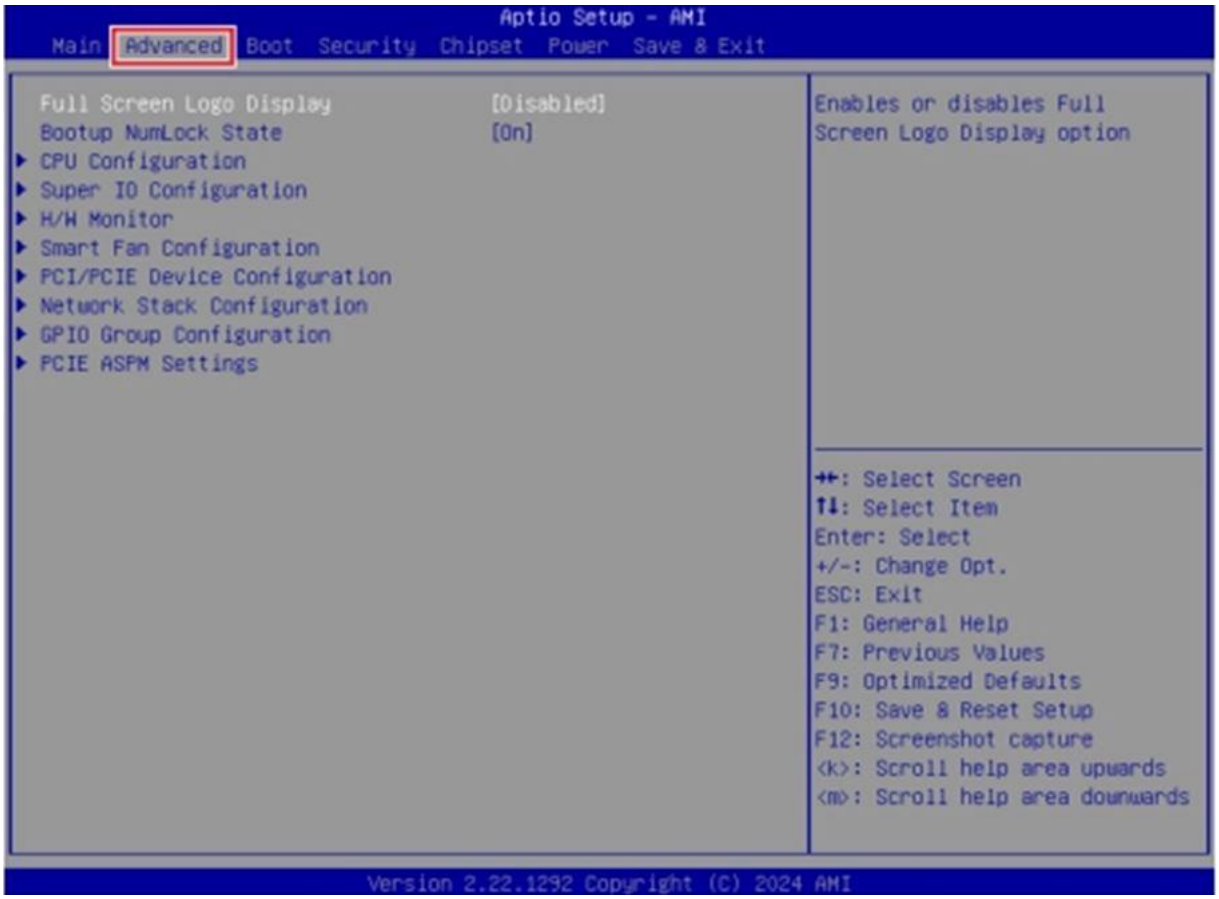
- Map This Root Port under VMD

  Enables or disables the mapping of the specified PCIe root port under Intel VMD control.

- RAID0/ 1/ 5/ 10/ Intel ® Optane™ Memory

  Enables or disables RAID 0/ 1/ 5/ 10/ Intel ® Optane™ Memory.

3.3 Advanced



- Full Screen Logo Display

  This BIOS feature determines if the BIOS should hide the normal POST messages with the motherboard or system manufacturer's full-screen logo.

  [Enabled] BIOS will display the full-screen logo during the boot-up sequence, hiding normal POST messages.

  [Disabled] BIOS will display the normal POST messages, instead of the full-screen logo.

  Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, it is recommended to disable this BIOS feature for faster boot-up.

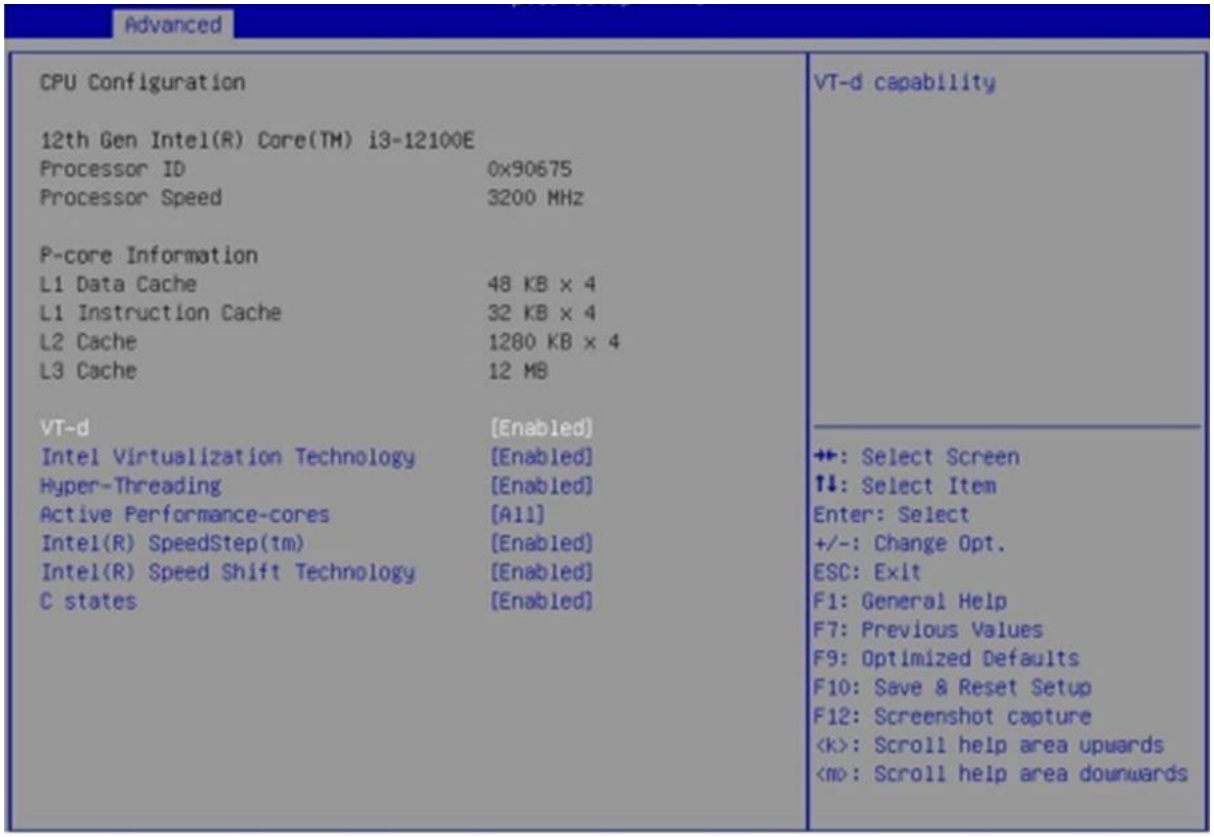
- Bootup NumLock State

  This setting is to set the state of the Num Lock key on the keyboard when the system is powered on.

  [On] Turn on the Num Lock key when the system is powered on..

  [Off] Allow users to use the arrow keys on the numeric keypad.

- CPU Configuration



- VT-d

  Enables or disables Intel VT-D (Intel Virtualization for Directed I/O) technology.

- Intel Virtualization Technology

  Enables or disables Intel Virtualization technology.

  [Enabled] Enables Intel Virtualization technology and allows a platform to run multiple operating systems in independent partitions. The system can function as multiple systems virtually.

  [Disabled] Disables this function.

- Hyper-Threading (HT Function)

  Enables or disables Intel Hyper-Threading technology. The processor uses Hyper-Threading technology to improve utilization of the CPU resources and potentially increasing overall performance by allowing it to handle multiple threads simultaneously. If you disable the function, it will restricts the CPU to operate as a single-threaded processor, with only one logical core per physical core. Please disable this item if your

operating system does not support HT Function or unreliability and instability may occur.

- Active Performance-cores

  Select the number of active Performance-cores (P-cores).

- Intel(R) SpeedStep(TM)

  Enhanced Intel SpeedStep® Technology enables the OS to control and activate performance states (P-States) of the processor.

  [Enabled] When enabled, Intel SpeedStep® technology is activated. This technology allows the processor to manage its power consumption via performance state (P-State) transitions.

  [Disabled] Disables this function.

- Intel(R) Speed Shift Technology

  Intel® Speed Shift Technology is an energy-efficient method that allows frequency control by hardware rather than the OS.

  [Enabled] When enabled, Intel® Speed Shift Technology is activated.The technology enables the management of processor power consumption via hardware performance state (P-State) transitions.

  [Disabled] Disables this function

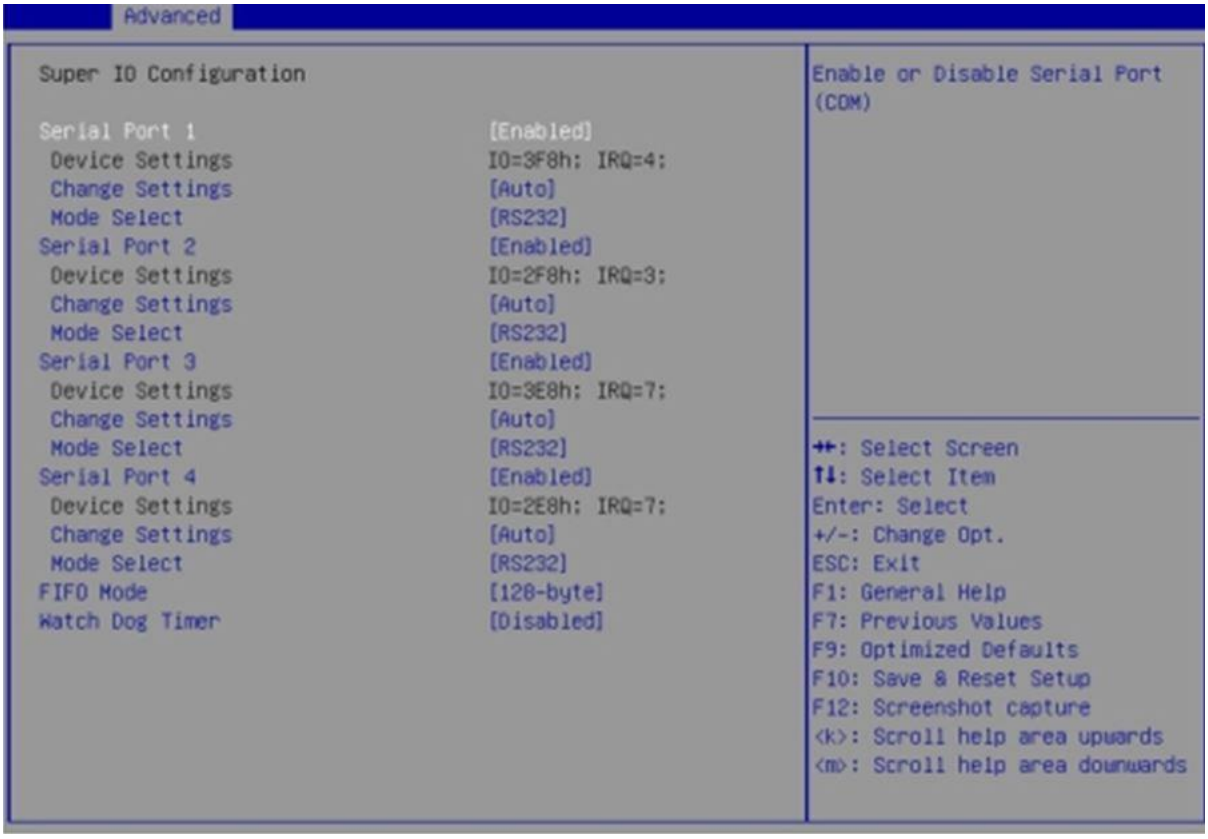
- C States

  This setting controls the C-States (CPU Power states).

  [Enabled] Detects the idle state of system and reduce CPU power consumption accordingly.

  [Disabled] Disables this function

■ Super IO Configuration



- Serial Port 1/ 2/ 3/ 4

  This setting enables or disables the specified serial port.

  » Device Settings

  This setting shows the address & IRQ of the specified serial port.

  » Change Settings

  This setting is used to change the address & IRQ settings of the specified serial port.

  » Mode Select

  Select an operation mode for Serial Port 1/ 2/ 3/ 4.

- FIFO Mode

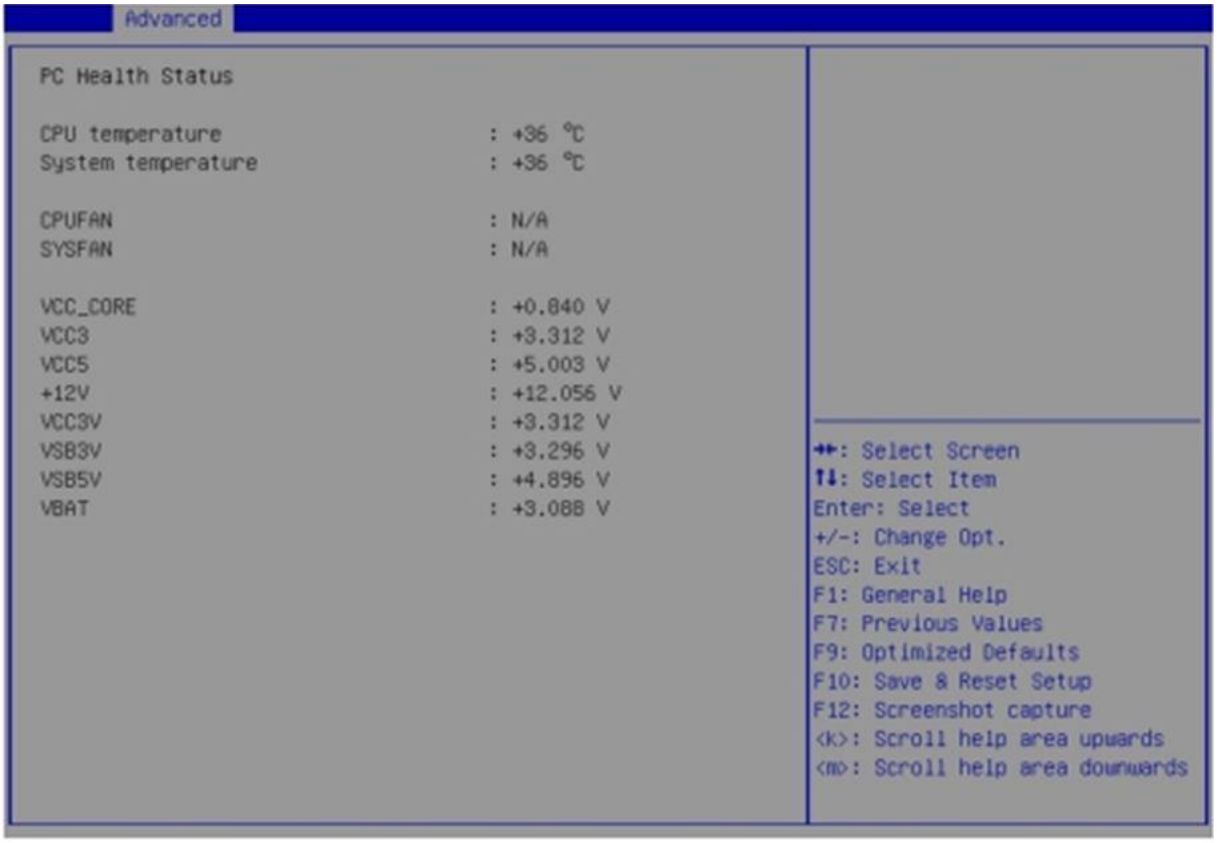
  This setting controls the FIFO (First In First Out) data transfer mode.

- Watch Dog Timer

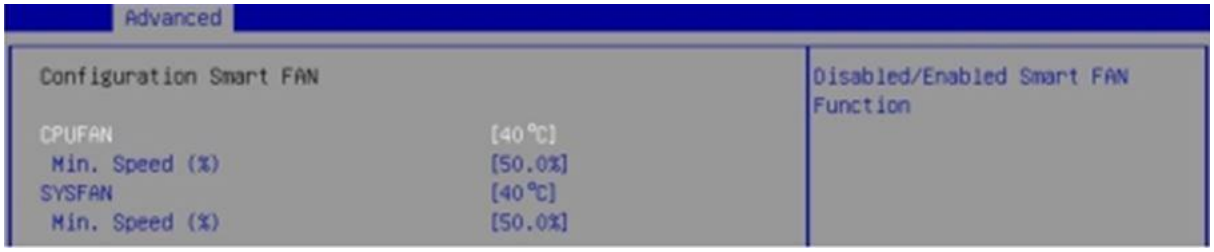
  You can enable the system watchdog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watchdog polls it.

- H/W Monitor (PC Health Status)

  These items display the current status of all monitored hardware devices/ components such as voltages, temperatures and all fans' speeds.



■ Smart Fan Configuration



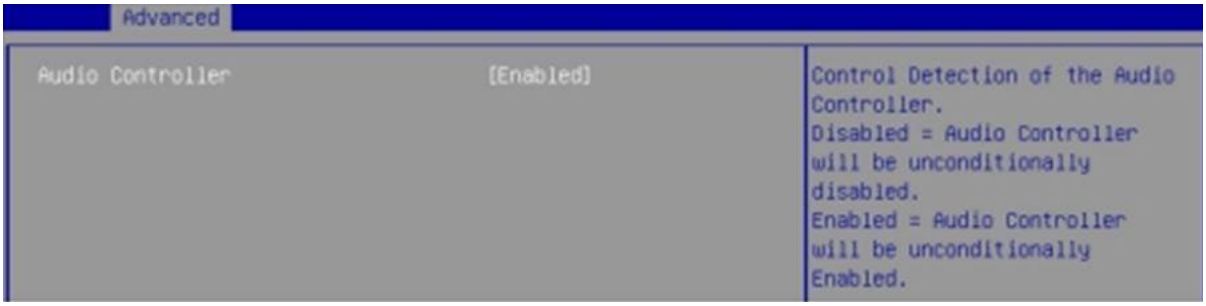
➢ CPUFAN/ SYSFAN

This setting enables or disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the CPU/system fan speed automatically depending on the current CPU/system temperature, avoiding the overheating to damage your system. The following item will display when CPUFAN/ SYSFAN is enabled.

» Min. Speed (%)

The beginning speed of the System fan.

■ PCI/PCIE Device Configuration

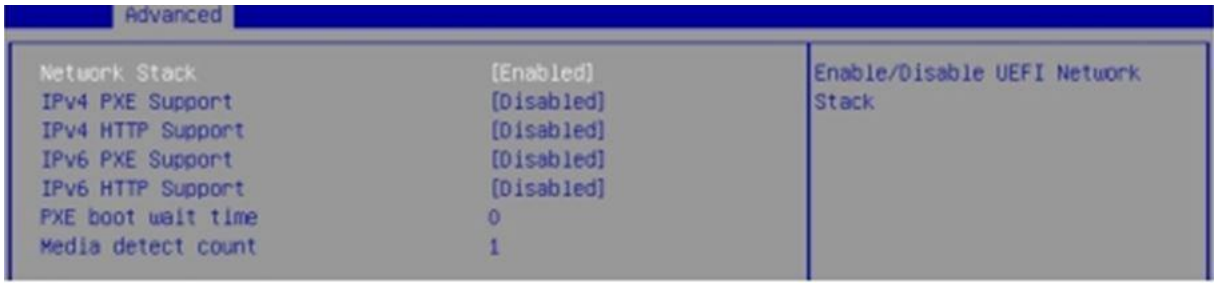


➢ Audio Controller

This setting enables or disables the detection of the onboard audio controller.

■ Network Stack Configuration

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS.



➢ Network Stack

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS. The following items will display when Network Stak is enabled.

» IPV4 PXE Support

Enables or disables IPv4 PXE boot support.

» IPV4 HTTP Support

Enables or disables Ipv4 HTTP Support.

» IPV6 PXE Support

Enables or disables Ipv6 PXE Support.

» IPV6 HTTP Support

Enables or disables Ipv6 HTTP Support.

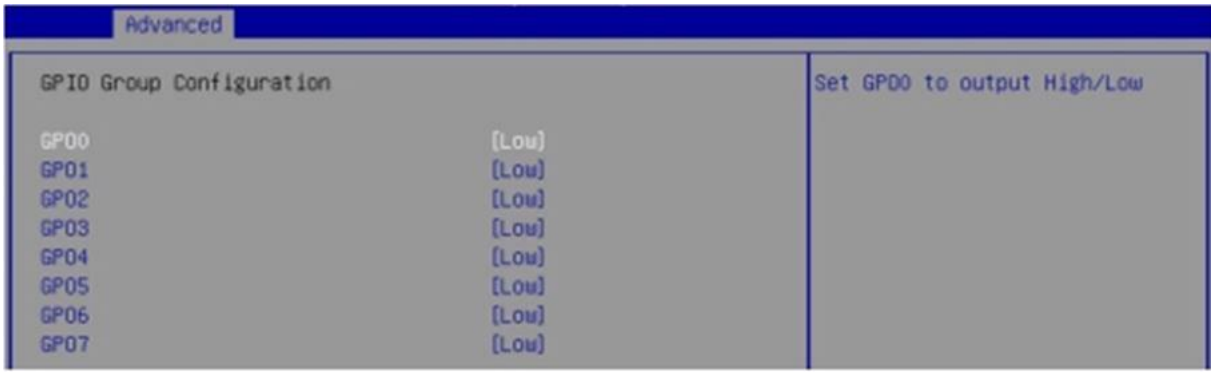
» PXE boot wait time

Use this option to specify the wait time to press the ESC key to abort the PXE boot. Press "+" or "-" on your keyboard to change the value. The default setting is 0.

» Media detect count

Use this option to specify the number of times media will be checked. Press "+" or "-" on your keyboard to change the value. The default setting is 1.

■ GPIO Group Configuration



➢ GPO0 ~ GPO7

These settings control the operation mode of the specified GPIO.

■ PCIE ASPM settings

This menu provide settings for PCIe ASPM (Active State Power Management) level for different installed devices.

➢ M2_B1, M2_E1, M2_M1, PCIE1

Sets PCI Express ASPM (Active State Power Management) state for power saving.

Lanes form PCH :

[Disabled] Disables this function

[L1] Higher latency, lower power "standby" state.

[Auto] Set the best state supported by the system.

Lanes form SA :

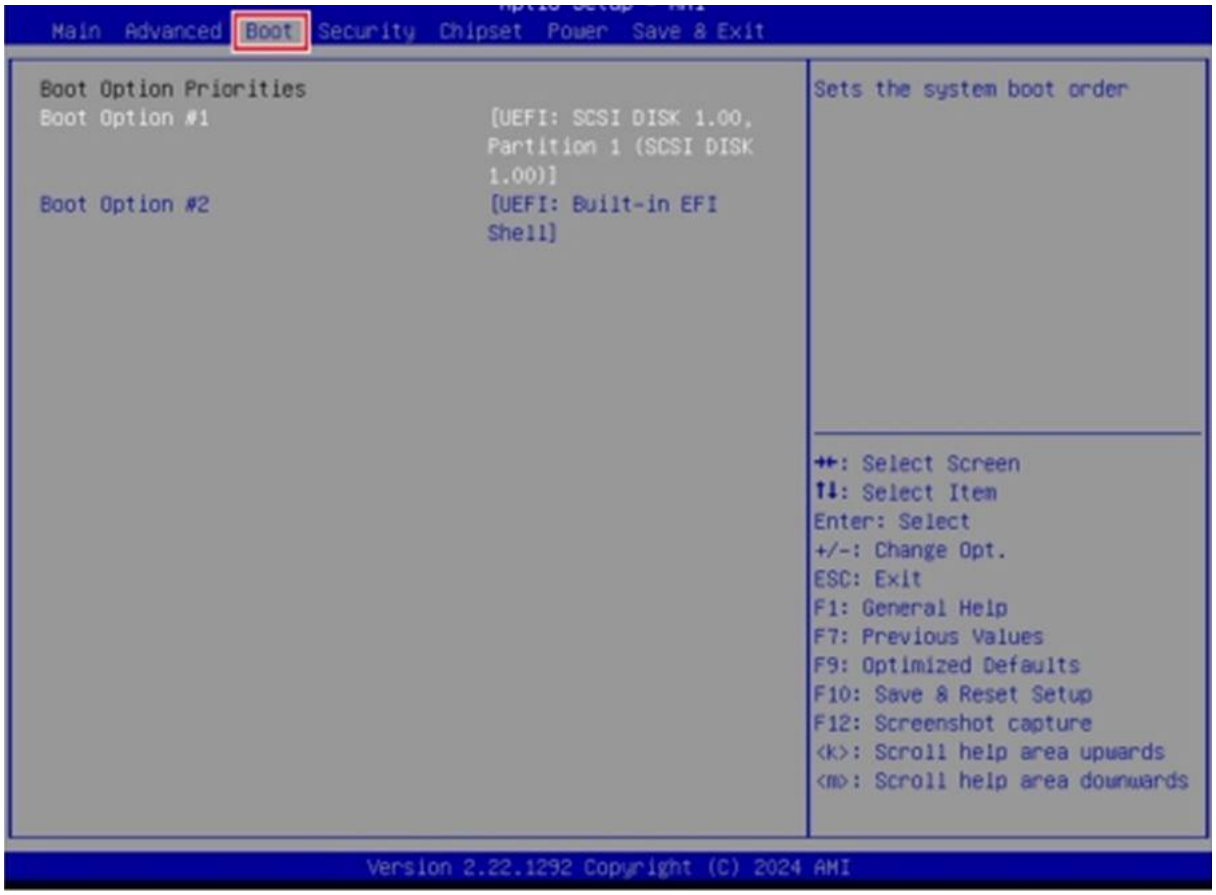
[Disabled] Disables this function

[L0s] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.

[L1] Higher latency, lower power "standby" state.

[L0sL1] Activate both L0s and L1 support.

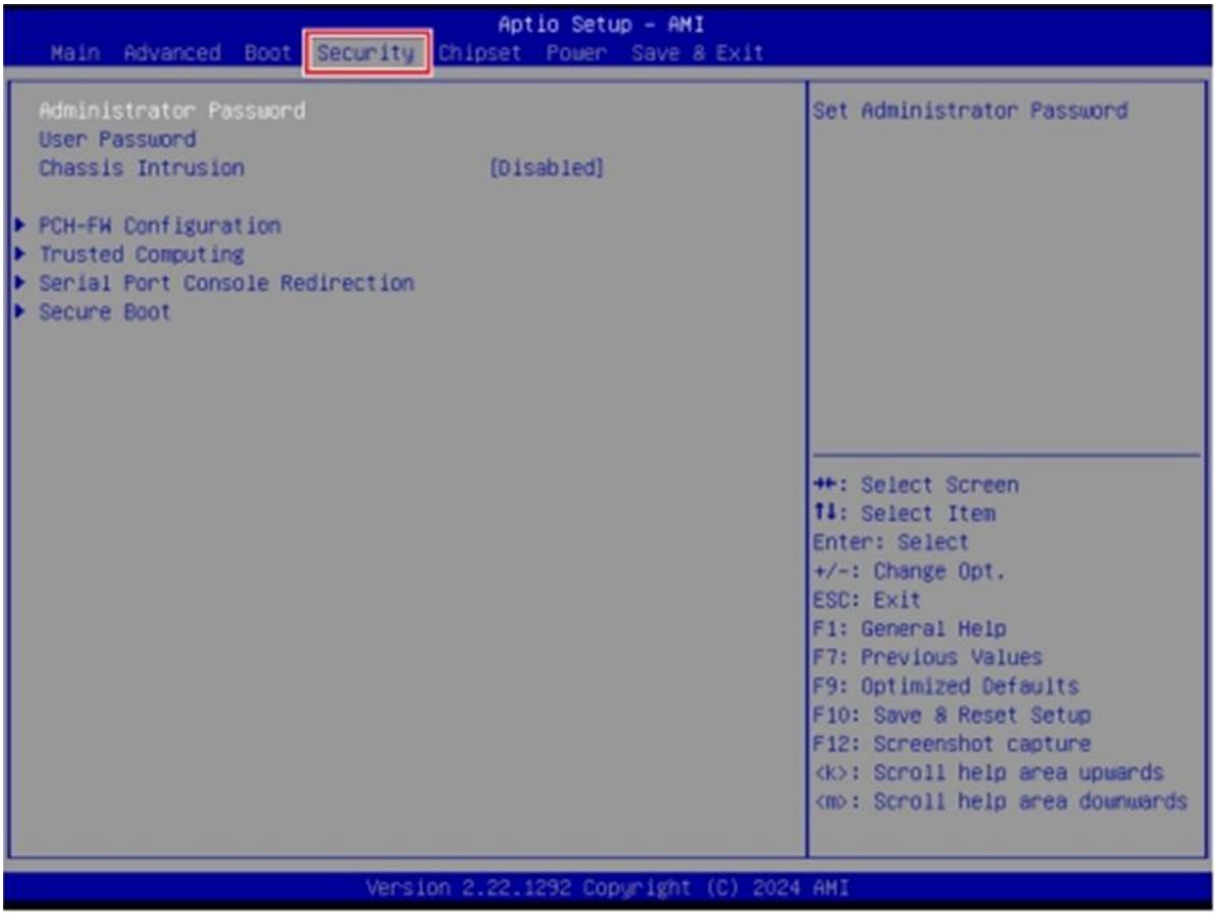
3.4 Boot



- Boot Option #1-2

  This setting allows users to set the sequence of boot devices where BIOS attempts to load the disk operating system.

3.5 Security



- Administrator Password

  Administrator Password controls access to the BIOS Setup utility.

- User Password

  User Password controls access to the system at boot and to the BIOS Setup utility.

- Chassis Intrusion

  Enables or disables recording messages while the chassis is opened. This function is ready for the chassis equips a chassis intrusion jumper(switch).

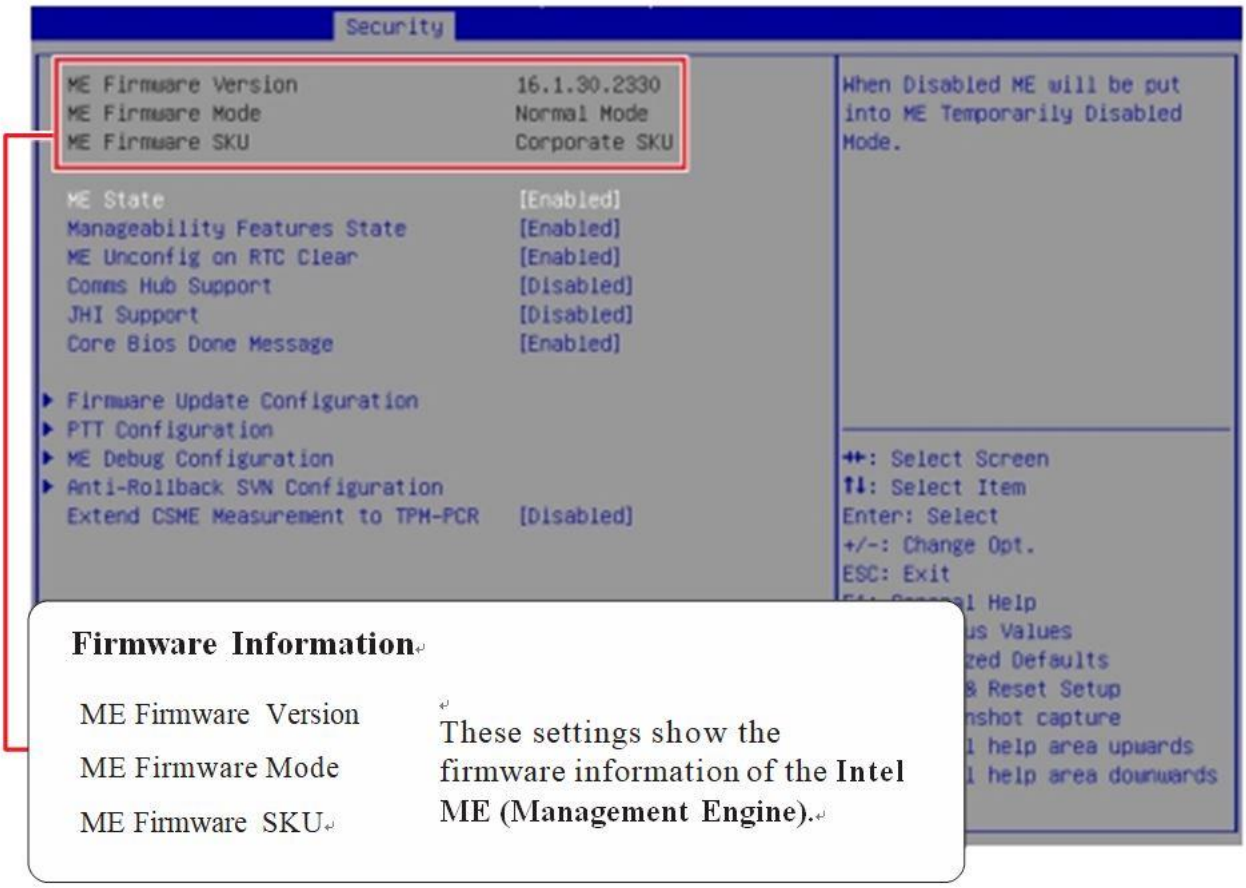
  [Enabled] Disables this function Once the chassis is opened, the system will record and issue a warning message. A beep sound will be emitted before this function is reset.

  [Disabled] Once the chassis is closed, the system will record and issue a warning message.

  [Reset] Clear the warning message. After clearing the message, please return to Enabled or Disabled.

- PCH-FW Configuration

This menu allows you to configure settings related to the PCH firmware.



➢ ME State

This menu controls the Intel® Management Engine State (ME state) parameters, which provides various management and security capabilities. The following items will display when ME State is enabled.

» Manageability Feature State

Enables or disables Manageability Feature State. Enabling this item for remote management capabilities.

» ME Unconfig on RTC Clear

Enables or disables ME Unconfig on RTC Clear. Enabling this item resets the ME configuration to its default state, removing any customizations or settings applied.

» Comms Hub Support

Enables or disables the communications hub support.

» JHI Support

Enables or disables JHI Support. JHI stands for Intel® Dynamic Application Loader Host Interface Service (Intel® DAL HIS) and is the engineering name for this feature. Enabling JHI Support in the BIOS settings allows the system to utilize this interface for communication between trusted applications and host-based applications.

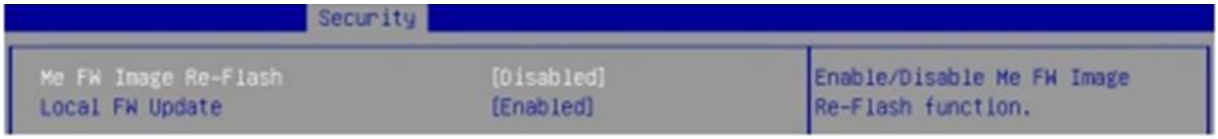
» Core BIOS Done Message

Enables or disables Core BIOS Done Message sent to ME.

- Extend CSME Measurement to TPM-PCR

This setting enables or disables Intel® Converged Security and Management Engine (CSME) measurement extend to TPM-PCR.

- Firmware Update Configuration



» ME FW Image Re-Flash

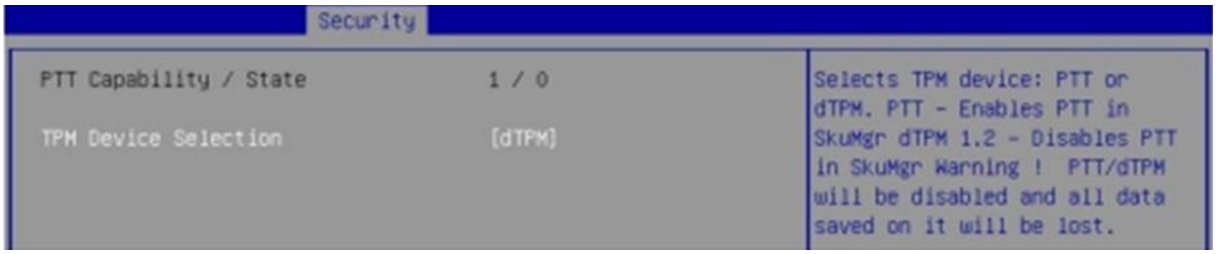
Enables or disables the ME Firmware Image Re-flashing.

» Local FW Update

Enables or disables the capability to perform a firmware update of the ME locally.

- PTT Configuration

Intel® Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows.



» TPM Device Selection

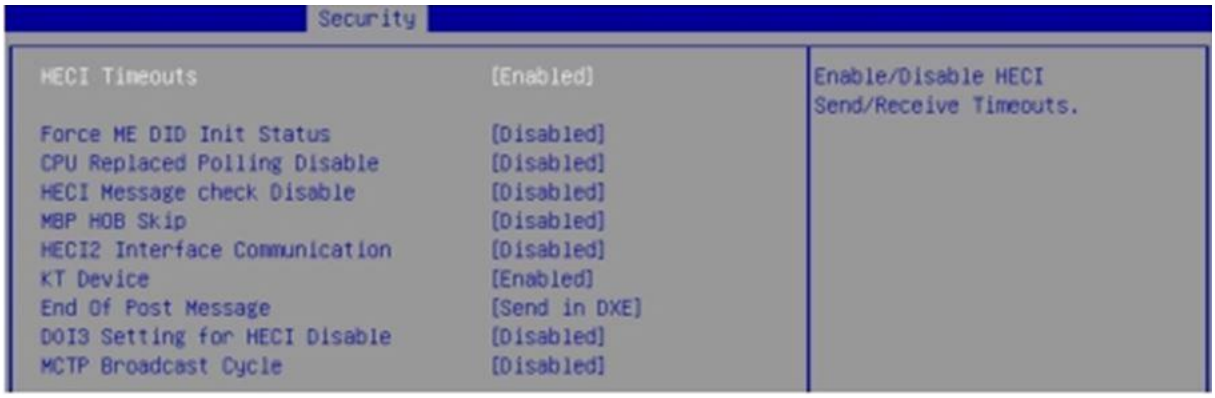
Select TPM (Trusted Platform Module) devices from PTT or dTPM (Discrete TPM).

[PTT] Enables PTT in SkuMgr.

[dTPM] Disables PTT in SkuMgr. Warning! PTT/ dTPM will be disabled and all data saved on it will be lost.

- ME Debug Configuration

This menu allows you to configure debug-related options for the Intel® Management Engine (ME).



» HECI Timeouts

This setting enables/ disables the HECI (Host Embedded Controller Interface) send/ receive timeouts.

» Force ME DID Init Status

Forces the ME Device ID (DID) initialization status value.

» CPU Replaced Polling Disable

Setting this option disables the CPU replacement polling loop.

» HECI Message Check Disable

This setting disables message check for BIOS boot path when sending messages.

» MBP HOB Skip

Setting this option will skip ME's Memory-Based Protection (MBP) H0B region.

» HECI2 Interface Communication

This setting Adds/ Removes HECI2 device from PCI space.

» KT Device

Enables or disables Key Transfer (KT) Device.

» End of Post Message

Enables or disables End of Post Message sent to ME.

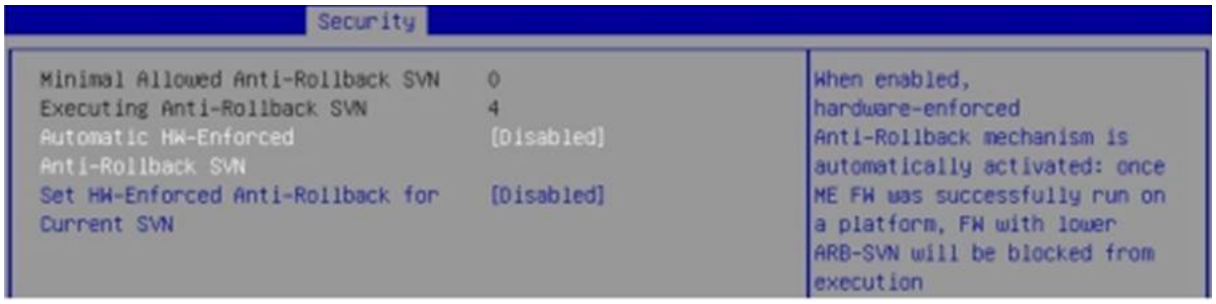
» DOI3 Setting for HECI Disable

Setting this option disables setting DOI3 bit for all HECI devices.

» MCTP Broadcast Cycle

Enables or disables Management Component Transport Protocol (MCTP) Broadcast Cycle.

➢ Anti-Rollback SVN Configuration



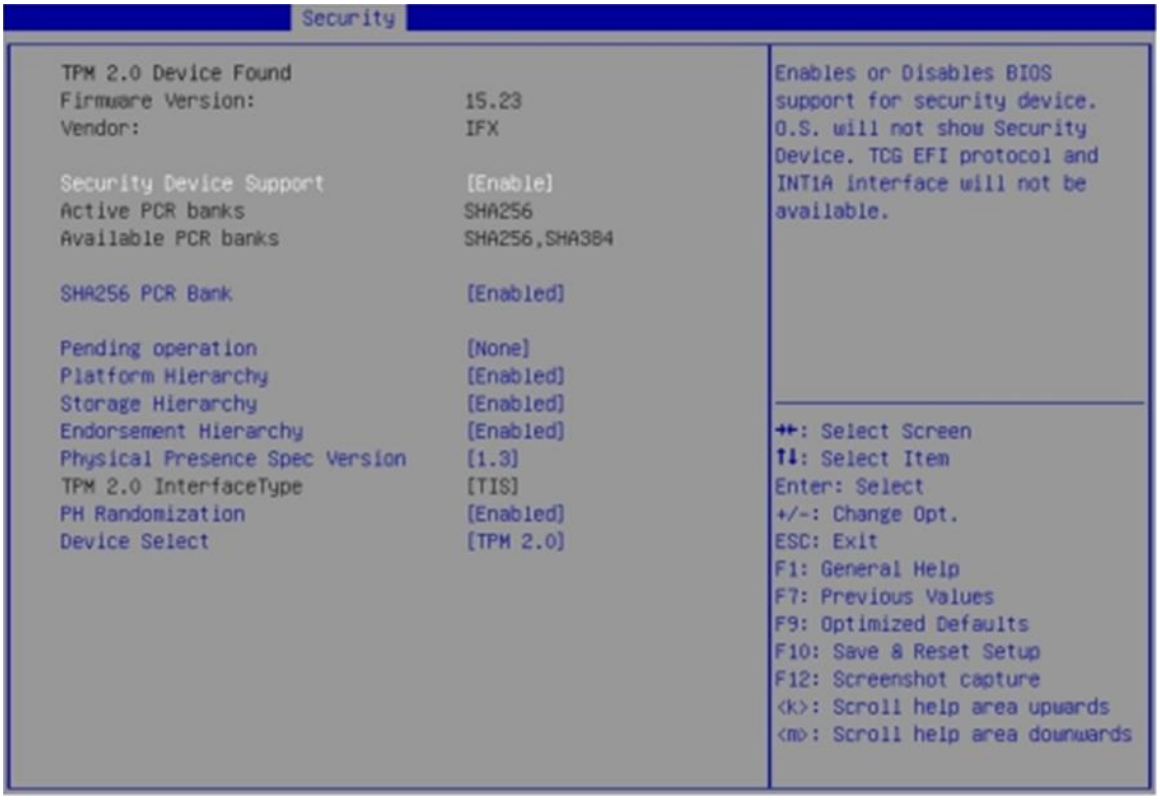
» Automatic HW-Enforced Anti-Rollback SVN

Setting this item enables will automatically activate the hardware-enforced anti-rollback protection based on the Secure Version Number (SVN). Once enabled, the hardware will enforce that only firmware updates with an SVN equal to or higher than the current SVN can be installed.

» Set HW-Enforced Anti-Rollback for Current SVN

Enable HW ERB 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. This item will display when Automatic HW-Enforced Anti-Rollback SVN is enabled.

■ Trusted Computing



- Security Device Support

  This item enables or disables BIOS support for security device. When set to [Disable], the OS will not show security device.

- SHA256 PCR Bank

  These settings enables or disables the SHA256 PCR Bank.

- Pending Operation

  When Security Device Support is set to [Enable], Pending Operation will appear. It is advised that users should routinely back up their TPM secured data.

  [TPM Clear] Clear all data secured by TPM.

  [None] Discard the se lection.

- Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy

  These settings enables or disables the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

- Physical Presence Spec Version

  This settings show the Physical Presence Spec Version.

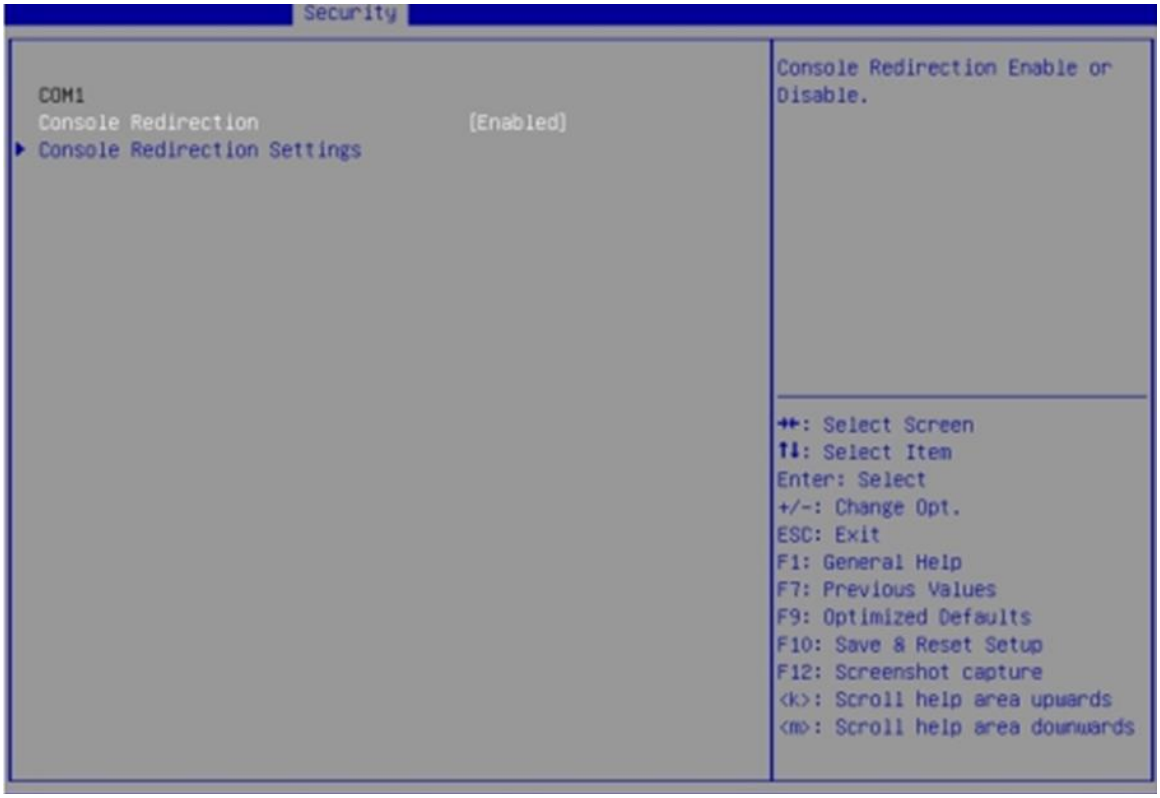
- TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

- Device Select

Select your TPM device through this setting.

■ Serial Port Console Redirection

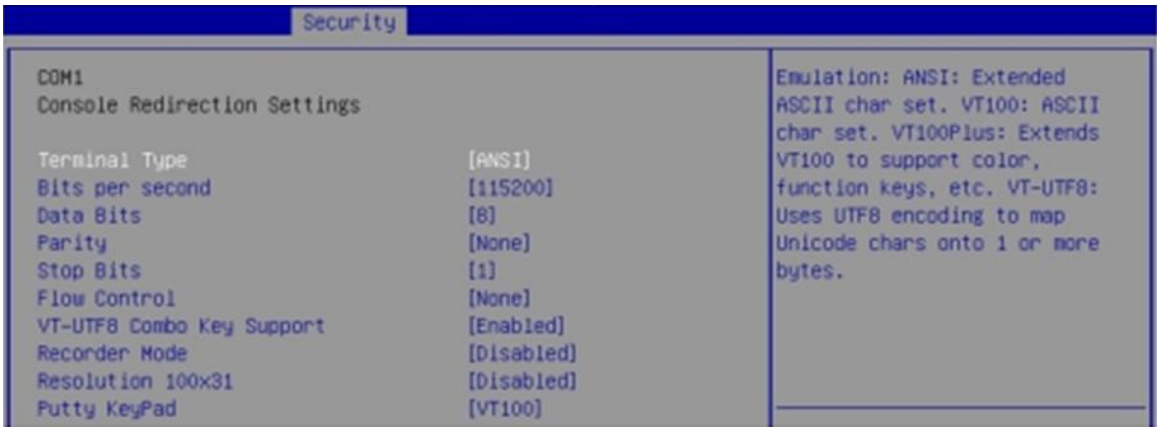


- Console Redirection

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables or disables the operation of console redirection. When set to [Enabled], BIOS redirects and sends all contents that should be displayed on the screen to the serial COM port for display on the terminal screen. Besides, all data received from the serial port is interpreted as keystrokes from a local keyboard.

- Console Redirection Settings (COM1)

This option appears when Console Redirection is enabled.



» Terminal Type

To operate the system's console redirection, you need a terminal supporting ANSI terminal protocol and a RS-232 null modem cable connected between the host system and terminal(s). You can select emulation for the terminal from this setting.

[ANSI] Extended ASCII character set.

[VT100] ASCII character set.

[VT100Plus] Extends VT100 to support color, function keys, etc.

[VT-UTF8] Uses UTF8 encoding to map Unicode characters onto one or more bytes.

» Bits per second, Data Bits, Parity, Stop Bits

These setting specifies the transfer rate (bits per second, data bits, parity, stop bits) of Console Redirection.

» Flow Control

Flow control is the process of managing the rate of data transmission between two nodes. It's the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

» VT-UTF8 Combo Key Support

This setting enables or disables the VT-UTF8 combination key support for ANSI/VT100 terminals.

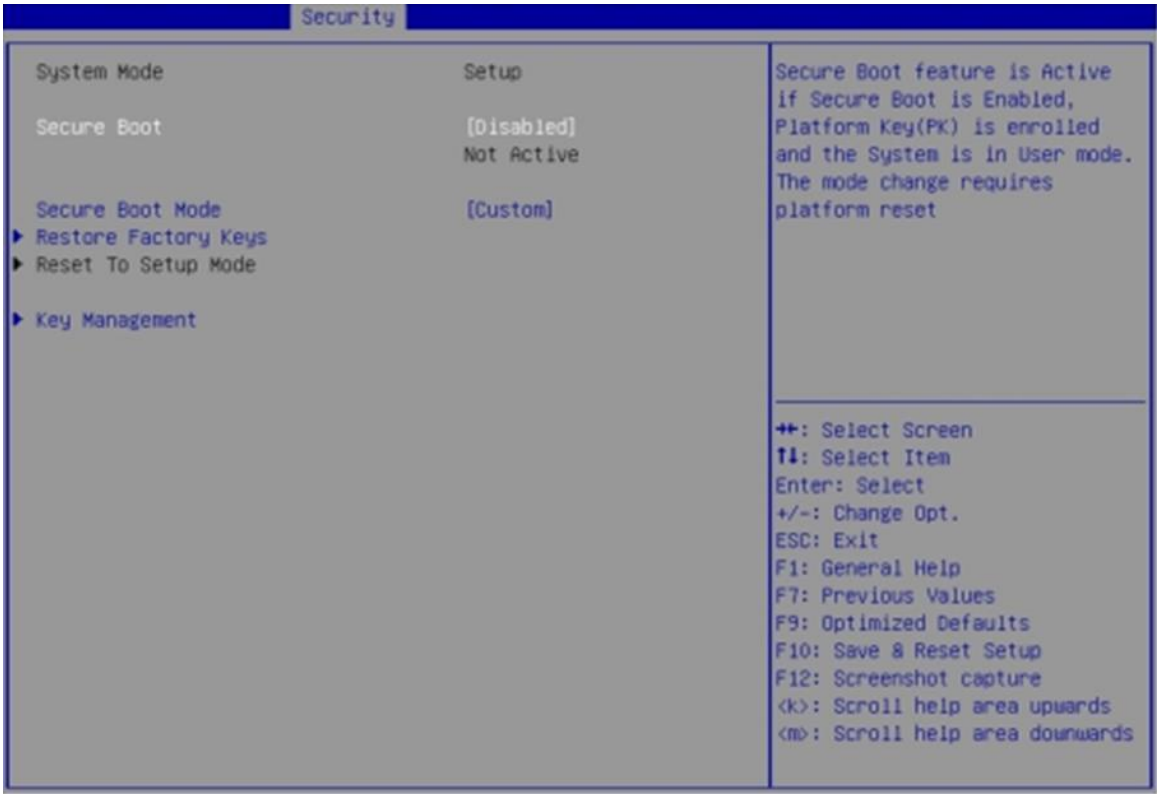
» Recorder Mode, Resolution 100x31

These settings enables or disables the recorder mode and the resolution 100x31.

» Putty KeyPad

PuTTY is a terminal emulator for Windows. This setting controls the numeric keypad for use in PuTTY.

- Secure Boot



- Secure Boot

Secure Boot function can be enabled only when the Platform Key (PK) is enrolled and running accordingly.

- Secure Boot Mode

Selects the secure boot mode. This item appears when Secure Boot is enabled.

[Standard] The system will automatically load the secure keys from BIOS.

[Custom] Allows user to configure the secure boot settings and manually load the secure keys.

- Restore Factory Keys

Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when "Secure Boot Mode" sets to [Custom].

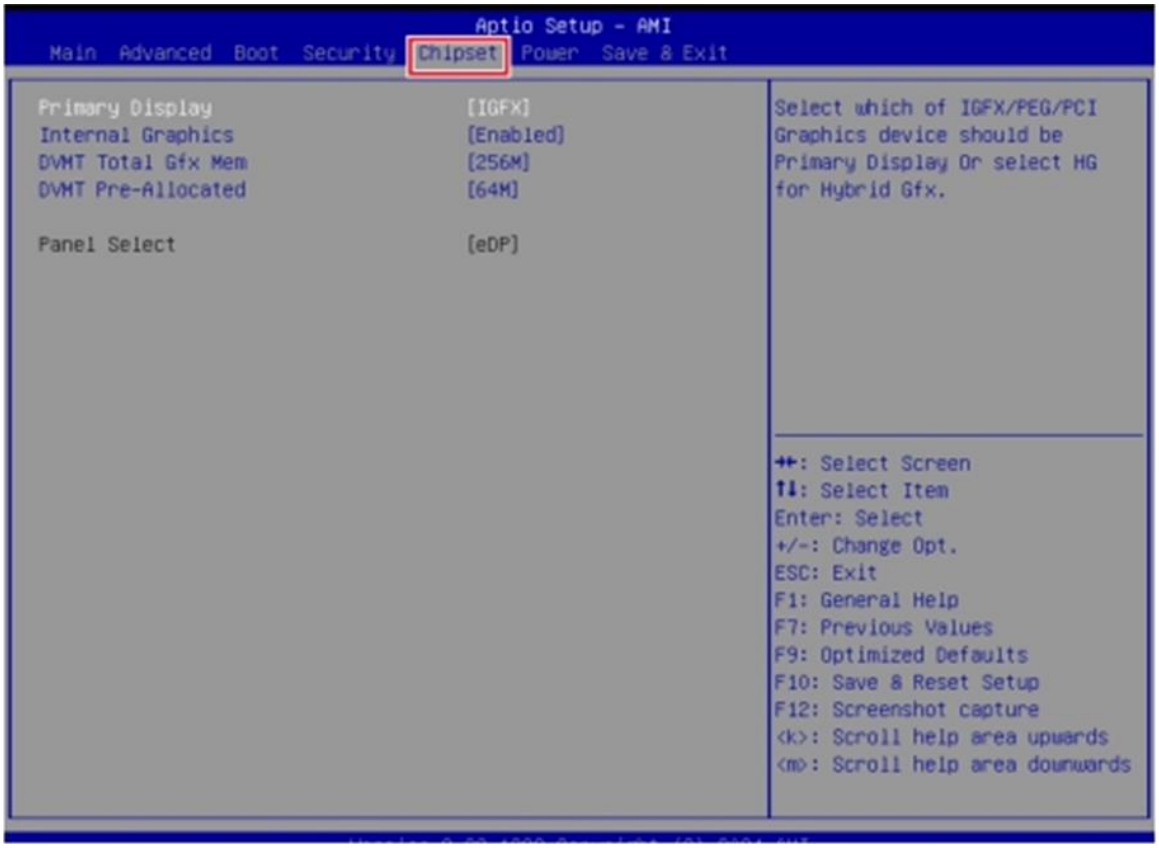
- Reset to setup Mode

Allows you to delete all the Secure Boot keys (PK,KEK,db,dbt,dbx). The settings will be applied after reboot or at the next reboot. This item appears when "Secure Boot Mode" sets to [Custom].

- Key Management

Press Enter key to enter the sub-menu. Manage the secure boot keys. This item appears when "Secure Boot Mode"sets to [Custom].

3.6 Chipset



- Primary Display

Secure Boot function can be enabled only when the Platform Key (PK) is enrolled and running accordingly.

- Internal Graphics

This setting enables or disables the internal graphics function. Available settings are:

[Auto] The internal graphics will be automatically enabled or disabled.

[Enable] Enables the internal graphics.

[Disable] Disables the internal graphics.

- DVMT Total Gfx Mem

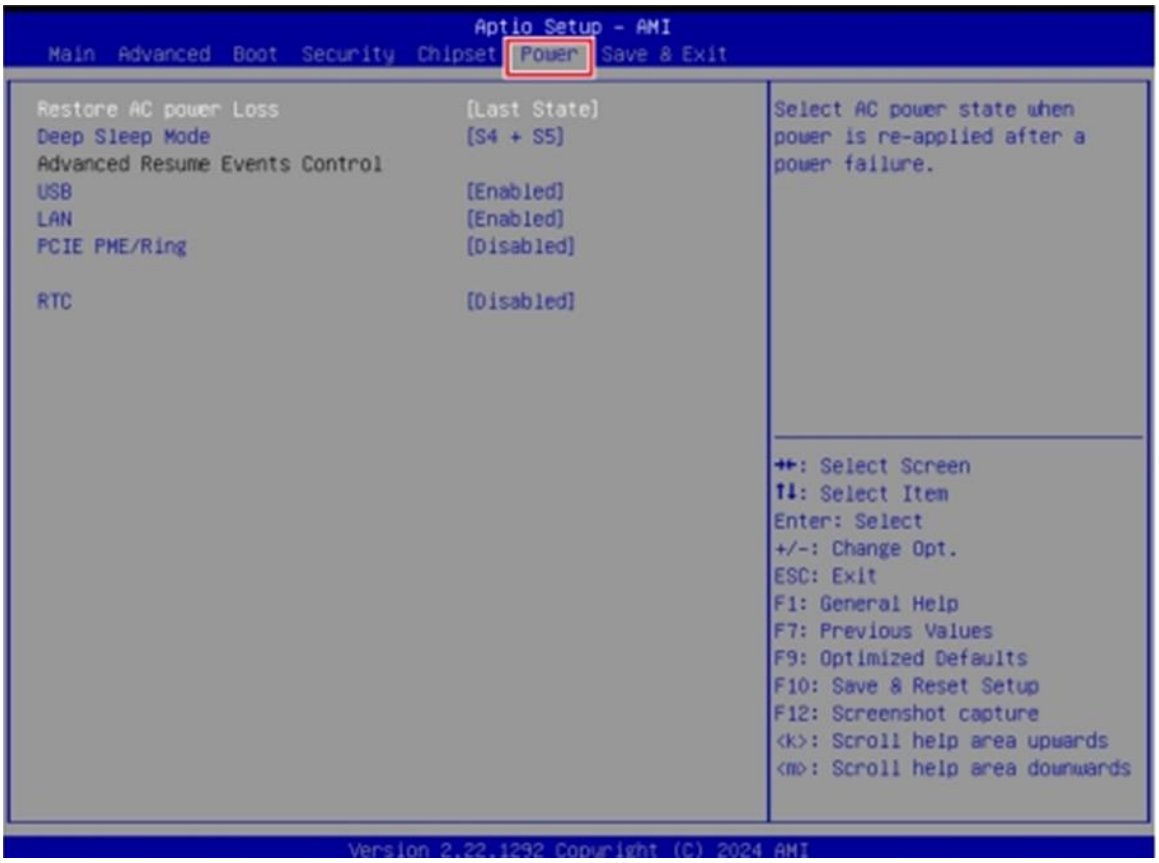
This setting specifies the total graphics memory size for Dynamic Video Memory Technology (DVMT).

- DVMT Pre-Allocated

This setting defines the DVMT pre-allocated memory. Pre-allocated memory is the small amount of

system memory made available at boot time by the system BIOS for video. Pre-allocated memory is also known as locked memory. This is because it is "locked" for video use only and as such, is invisible and unable to be used by the operating system.

3.7 Power



- Restore AC Power Loss

  This setting specifies whether your system will reboot after a power failure or interrupt occurs. Available settings are :

  [Power Off] Leaves the computer in the power off state.

  [Power On] Leaves the computer in the power on state.

  [Last State] Restores the system to the previous status before power failure or interrupt occurred.

- Deep Sleep Mode

  The setting enables or disables the Deep S5 power saving mode. S5 is almost the same as G3 Mechanical Off, except that the PSU still supplies power, at a minimum, to the power button to allow return to S0. A full reboot is

required. No previous content is retained. Other components may remain powered so the computer can "wake" on input from the keyboard, clock, modem, LAN, or USB device.

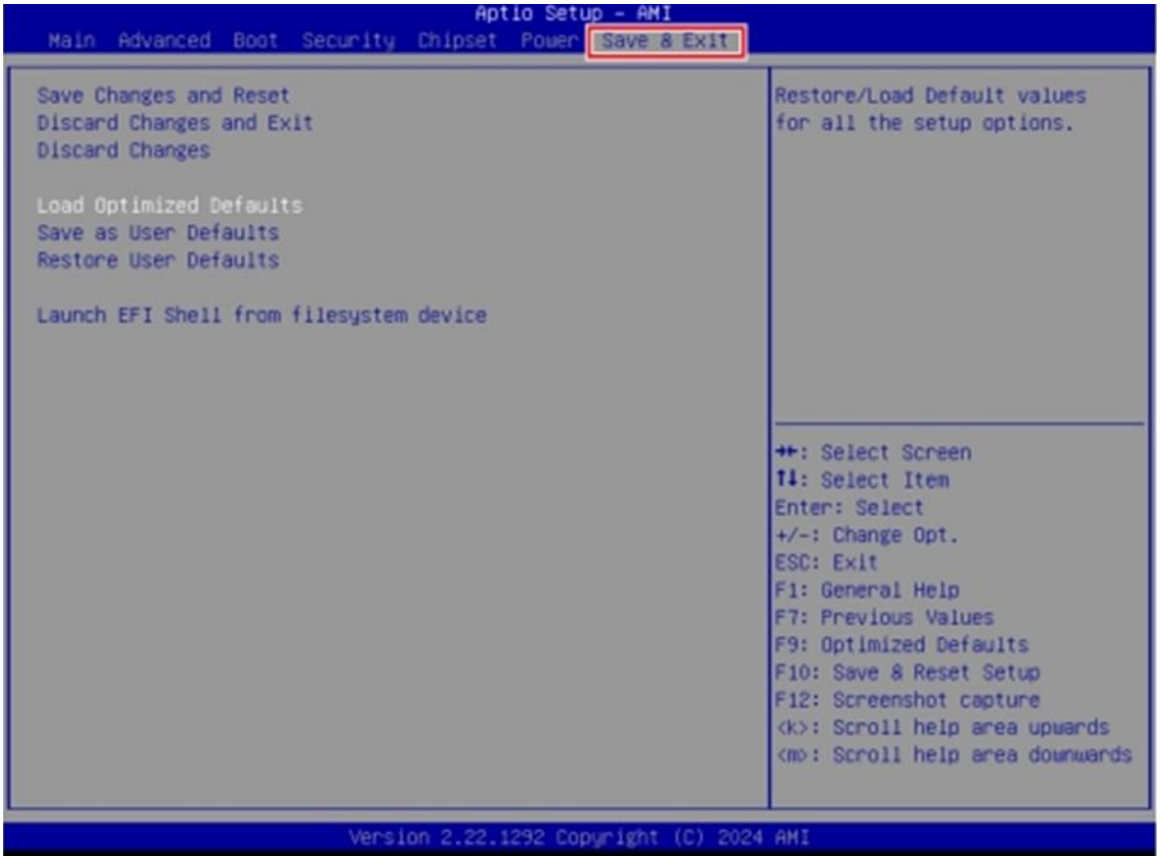
- USB, LAN, PCIE PME/ Ring

The setting allows the activity of the specified device to wake up the system from power saving modes.

- RTC

When [Enabled], your can set the date and time at which the RTC (real-time clock) alarm awakens the system from power saving modes.

3.8 Save & Exit



- Save Changes and Reset

Save changes to CMOS and reset the system.

- Discard Changes and Exit

  Abandon all changes and exit the Setup Utility.

- Discard Changes

  Abandon all changes.

- Load Optimized Defaults

  Use this menu to load the default values set by the motherboard manufacturer specifically for optimal performance of the motherboard.

- Save as User Defaults

  Save changes as the user's default profile.

- Restore User Defaults

  Restore the user's default profile.

- Launch EFI Shell from filesystem device

  This setting helps to launch the EFI Shell application from one of the available file system devices.