

# ROC280-BB

### 1U 19"AC-DC Redundant Fanless Server With Intel 14<sup>th</sup> /13<sup>th</sup> Processor

SSD



USB2.0

HDD PWR

User's Manual Revision Date: Feburary ,7, 2025 Revision Date: Feburary, 7, 2025

### **Safety 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 Date: Feburary, 7, 2025

### **Revision History**

Revision	Date (mm.dd.yyyy)	Changes
V1.0	2.7.2025	First release

### **Packing list**

Item	Description	Q'ty
1	ROC288-BB 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.



Revision Date: Feburary, 7, 2025

### **Table of Contents**

Safety Information1
<b>Electrical safety</b> 1
Operation safety1
Statement
Revision History
Packing list
Chapter 1 : Product Information
<b>1.1 Key Feature</b>
<b>1.2 I/O Placement</b>
Chapter 2 : I/O Connector & SSD Tray Door
<b>2.1 2.5GbE RJ-45 LAN Jack</b>
<b>2.2 USB 10Gbps Port</b>
<b>2.3 Display Port</b>
<b>2.3 HDMI™ Connector</b>
<b>2.4 Mic-in Jack</b>
<b>2.5 Line-Out Jack</b>
<b>2.6 Line-Out Jack</b>
Chapter 3 : BIOS Setup
<b>3.1 The Menu Bar</b>
<b>3.2 Main</b>
<b>3.3 Advanced</b>
<b>3.4 Boot</b>

Revision Date: Feburary, 7, 2025

3.5 Security	
3.6 Chipset	
3.7 Power	
3.8 Save & Exit	

Revision Date: Feburary, 7, 2025

# **Chapter 1 : Product Information**

### **1.1 Key Feature**

**7**STARLAKE

SYSTEM

SYSTEM			
HighPerformance	14th/13th Gen Intel® Raptor Lake-R/Raptor Lake-S LGA1700 Socket Processor / Core		
Processor	i9/i7/i5/i3 Processor / TDP 65W		
Memory type	DDR5 4800 MHz / 2 x 262-pin SO-DIMM / Max. 64 GB (Non-ECC)		
Chipset	Intel® Q670 Chipset		
Expansion Slot	1 x PCIe expansion slot(PCIe x 16 FHHL)		
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			
1 x Intel <sup>®</sup> I226-LM 2.5Giga LAN Ethernet			
Linemet	2 x Intel <sup>®</sup> 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)		

Revision Date: Feburary, 7, 2025

7STARLAKE

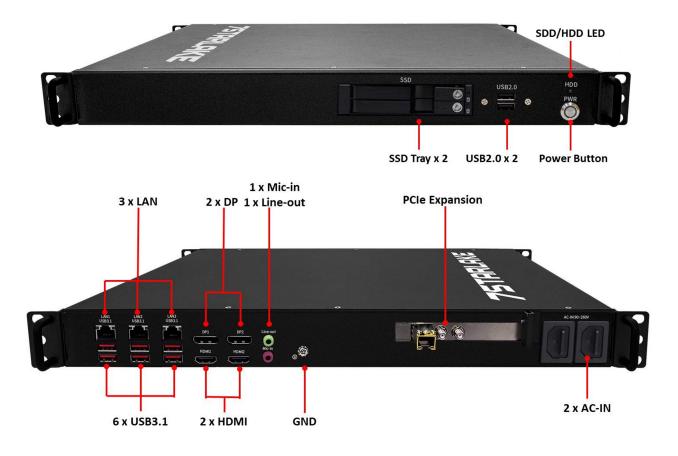
DC-IN	2 x AC plug	
	MENT	
Power Input	AC-IN 90~260V w/Redundant	
PHYSICAL		
Dimension (W x D x H)	430 x 450 x 44.4 mm	
Chassis	SECC	
ENVIRONMENT		
Green Product	RoHS compliance	
Operating Temperature	-20 to 60°C (Options for -40°C)	
Storage Temperature	-40 to 85°C	
Relative Humidity	5% to 95%, non-condensing	
EMC	CE and FCC compliance	
OPERATION SYST	EM	
OS	Windows®10/11 64-bit	
	Linux (Support by request)	

Linux(Support by request)

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

Revision Date: Feburary, 7, 2025

### **1.2 I/O Placement**



Revision Date: Feburary, 7, 2025

### 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		Speed LED	
<b>Status</b> .	<b>Description</b> .	<b>Status</b> <i>₀</i>	<b>Description</b> <sub>*</sub>
O Off.∕	No link.	O Off.∕	10/100 Mbps.
⊖ Yellow	Linked	Green	1000 Mbps+
Blinking	Data activity.	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<sup>™</sup> Connector

HDMI<sup>™</sup> 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<sup>™</sup> 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

Revision Date: Feburary, 7, 2025

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



Revision Date: Feburary, 7, 2025

### **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.
- $\cdot$  Users want to change the default settings for customized features.

### **M**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.

### Mmportant

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.



Revision Date: Feburary, 7, 2025

#### **Control Keys**

$\leftrightarrow$	Select Screen		
$\uparrow \downarrow$	Select Item		
Enter	Select		
+-	Change Value		
Esc	Exit		
F1	General Help		
F7	Previous Values		
F9	Optimized Defaults		
F10	Save & Reset*		
F12	Screenshot capture		
<К>	Scroll help area upwards		
<m></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 (  $\uparrow \downarrow$  ) 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 ( $\uparrow \downarrow$ ) 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>.

Revision Date: Feburary, 7, 2025

#### 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**

Aptio Setup - AMI				
Main Advanced Boot Security Chi	pset Power Save & Exit			
System Date	[Fri 09/13/2024]	Set the Date, Use Tab to		
System Time	[18:24:38]	switch between Date elements. Default Ranges:		
SATA_1	Not Present	Yean: 2000-2099		
SATA_2	Not Present	Nonths: 1-12		
SATA_3	Not Present	Days: Dependent on month		
M.2_1	Not Present	Range of Years may vary.		
M.2_2	Not Present			
SATA Mode	AHCI			
Enable VMD controller	[Disabled]			
VMD setup menu	(			
USB Devices:		++: Select Screen		
1 Drive, 2 Keyboards, 1 Mouse		14: Select Item		
		Enter: Select		
BIOS Version	ECF10IMS.800	+/-: Change Opt.		
		ESC: Exit		
12th Gen Intel(R) Core(TM) 13–12100E		F1: General Help		
Processor ID	0x90675	F7: Previous Values		
Build Type	64	F9: Optimized Defaults		
Total Memory	8192 MB(DDR5)	F10: Save & Reset Setup		
		F12: Screenshot capture		
		<k>: Scroll help area upwards</k>		
		<m>: Scroll help area downwards</m>		
Version 2	.22.1292 Copyright (C) 2024	AMI		

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

Revision Date: Feburary, 7, 2025

Use this menu to set supervisor and user passwords.

Chipset

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

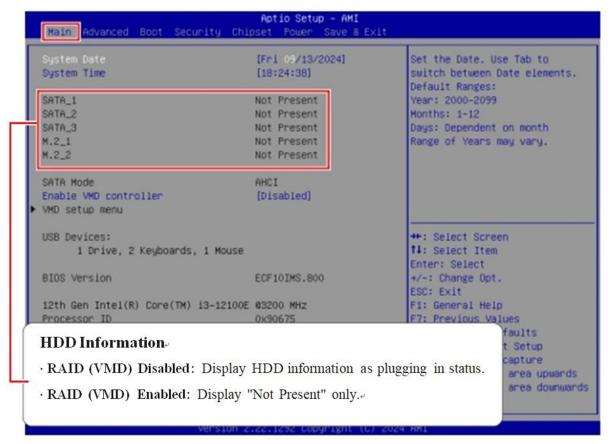
Power

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

**7**STARLAKE

This setting allows you to set the system date.

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

Revision Date: Feburary, 7, 2025

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.

### <u>M</u>mportant

- · "SATA\_3" is M.2MKeywith SATA signal, and the "M.2\_2" is M.2BKey.
- VMD Setup Menu (VMD Configuration)

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



Revision Date: Feburary, 7, 2025

Main Nain		
VMD Configuration Enable VMD Global Mapping Map this Root Port under VMD Root Port BDF details RAIDO	SATA Controller	Enable/Disable to VMD Global Mapping
RAID1 RAID5	(Enabled) (Enabled)	
RAIDIO	[Enabled]	
Intel(R) Optane(TM) Memory	(Enabled)	
		<pre>**: Select Screen f4: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save &amp; Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <mp: area="" downwards<="" help="" pre="" scroll=""></mp:></k></pre>
Versi	on 2.22.1292 Copyright (C)	2024 AMI

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 <sup>®</sup> Optane<sup>™</sup> Memory

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

Revision Date: Feburary, 7, 2025

### **3.3 Advanced**

Main Advanced Boot Security	Aptio Setup – AMI Chipset Power Save & E	xit
Full Screen Logo Display Bootup NumLock State CPU Configuration Super ID Configuration H/W Monitor Smart Fan Configuration PCI/PCIE Device Configuration Network Stack Configuration GPID Group Configuration PCIE ASPM Settings	[Oisabled] [On]	Enables or disables Full Screen Logo Display option
		<pre>++: Select Screen fl: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save &amp; Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>
Vers	ion 2.22.1292 Copyright (C	) 2024 AMI

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

**7**STARLAKE

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.

Revision Date: Feburary, 7, 2025

#### CPU Configuration

Advanced		
CPU Configuration		VT-d capability
CPU Configuration 12th Gen Intel(R) Core(TM) 13-1210 Processor ID Processor Speed P-core Information L1 Data Cache L1 Instruction Cache L2 Cache L3 Cache VT-d Intel Virtualization Technology Hyper-Threading Active Performance-cores Intel(R) SpeedStep(tm) Intel(R) Speed Shift Technology C states	0E 0x90675 3200 MHz 48 KB × 4 32 KB × 4 1280 KB × 4 12 MB (Enabled) (Enabled) (Enabled) (Enabled) (Enabled) (Enabled) (Enabled) (Enabled) (Enabled)	<pre>VT-d capability  ++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save &amp; Reset Setup</pre>
		F12: Screenshot capture (k): Scroll help area upwards (m): Scroll help area downwards

#### ≻ 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)

**7**STARLAKE

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

Revision Date: Feburary, 7, 2025

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<sup>®</sup> Technology enables the OS to control and activate performance states (P-States) of the processor.

[Enabled] When enabled, Intel SpeedStep<sup>®</sup> 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<sup>®</sup> 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



Revision Date: Feburary, 7, 2025

Super IO Configuration		Enable or Disable Serial Port (COM)
Senial Port 1 Device Settings Change Settings Mode Select Senial Port 2 Device Settings Change Settings Mode Select Senial Port 3 Device Settings Change Settings Mode Select Senial Port 4 Device Settings Change Settings Mode Select FIFO Mode Watch Dog Timer	<pre>[Enabled] I0=3F8h: IRQ=4; [Auto] [RS232] [Enabled] I0=2F8h: IRQ=3; [Auto] [RS232] [Enabled] I0=3E8h: IRQ=7; [Auto] [RS232] [Enabled] I0=2E8h; IRQ=7; [Auto] [RS232] [128-byte] [Disabled]</pre>	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save &amp; Reset Setup F12: Screenshot capture <kb: <mb:="" area="" downwards<="" help="" pre="" scroll="" upwards=""></kb:></pre>

#### 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

**7**STARLAKE

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.

Revision Date: Feburary, 7, 2025

PC Health Status		
PC Health Status CPU temperature System temperature CPUFAN SYSFAN VCC_CORE VCC3 VCC5 +12V VCC3V VSB3V VSB3V VSB5V VBAT	: +36 °C : +36 °C : N/A : N/A : +0.840 V : +3.312 V : +5.003 V : +12.056 V : +3.312 V : +3.296 V : +4.896 V : +3.088 V	<pre>**: Select Screen f1: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save &amp; Reset Setup</pre>

#### Smart Fan Configuration

Configuration Smart FAN			
		Disabled/Enabled Smart FAN Function	
CPUFAN	[40 °C]		
Min. Speed (%)	[50.0%]		
SYSFAN	(40 °C)		
Min. Speed (%)	[50.0%]		

#### CPUFAN/ SYSFAN

**7**STARLAKE

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

Revision Date: Feburary, 7, 2025

Advanced		
Audio Controller	[Enabled]	Control Detection of the Audio Controller. Disabled = Audio Controller will be unconditionally disabled. Enabled = Audio Controller will be unconditionally Enabled.

#### 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.

Advanced		
Network Stack IPv4 PXE Support IPv4 HTTP Support	(Enabled) (Disabled) (Disabled)	Enable/Disable UEFI Network Stack
IPv6 PXE Support IPv6 HTTP Support	[Disabled] [Disabled]	
PXE boot wait time	0	
Media detect count	1	

#### 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.

Revision Date: Feburary, 7, 2025

■ GPIO Group Configuration

Advanced		
GPIO Group Configuration	on	Set GPD0 to output High/Low
GPOO	(LOW)	
GP01	(Lou)	
6P02	[Lou]	
6P03	(Lou)	
GP04	(Lou)	
6P05	[Lou]	
GP06	(Lou)	
GP07	(Lou)	

➢ 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.

Huvanceu		
M2_B1 M2_E1 M2_M1 PCIE1	(Disabled) [Disabled] [Disabled] [Disabled]	PCI Express Active State Power Management settings.

#### 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 :

**7**STARLAKE

[Disabled] Disables this function

- [LOs] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.
- [L1] Higher latency, lower power "standby" state.
- [LOsL1] Activate both LOs and L1 support.

Revision Date: Feburary, 7, 2025

### **3.4 Boot**

Nain Advanced Boot Security	Chipset Power Save & Exit	
Boot Option Priorities Boot Option #1	[UEFI: SCSI DISK 1.00, Partition 1 (SCSI DISK 1.00)]	Sets the system boot order
Boot Option #2	[UEFI: Built-in EFI Shell]	<pre>++: Select Screen 14: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save &amp; Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards</m></k></pre>
Vers	ion 2.22.1292 Copyright (C) 202	4 AMI

#### ■ Boot Option #1-2

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



Revision Date: Feburary, 7, 2025

### **3.5 Security**

	Chipset Power Save &	ana t
Administrator Password		Set Administrator Password
User Password		
Chassis Intrusion	[Disabled]	
PCH-FH Configuration		
Trusted Computing		
Serial Port Console Redirection		
Secure Boot		
		++: Select Screen
		14: Select Item
		Enter: Select
		+/-: Change Opt.
		ESC: Exit
		F1: General Help
		F7: Previous Values
		F9: Optimized Defaults
		F10: Save & Reset Setup
		F12: Screenshot capture
		<k>: Scroll help area upwards</k>
		<mp: area="" downward<="" help="" scroll="" td=""></mp:>

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

24

Revision Date: Feburary, 7, 2025

ME Firmware Version	16.1.30.2330	When Disabled ME will be put
ME Firmware Mode	Normal Mode	into ME Temporarily Disabled
ME Firmware SKU	Corporate SKU	Mode.
ME State	[Enabled]	
Manageability Features State	[Enabled]	
ME Unconfig on RTC Clear	[Enabled]	
Commis Hub Support	[Disabled]	
JHI Support	[Disabled]	
Core Bios Done Message	[Enabled]	
Firmware Update Configuration	1	
PTT Configuration		
ME Debug Configuration		++: Select Screen
Anti-Rollback SVN Configurat.	ion	11: Select Item
Extend CSNE Measurement to Th	PM-PCR [Disabled]	Enter: Select
		+/-: Change Opt.
		ESC: Exit
		Help
<b>Firmware Information</b>	lψ	us Values zed Defaults
		& Reset Setup
ME Firmware Version		ashat canture
	These settings show th	1e 1 help area upward
ME Firmware Mode	firmware information of	
ME FIIIIWale Mode	minimate information o	i the interior a near or co uour and

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

#### ME State

This menu controls the Intel<sup>®</sup> 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

**7**STARLAKE

Enables or disables JHI Support. JHI stands for Intel<sup>®</sup> Dynamic Application Loader Host Interface Service (Intel<sup>®</sup> 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

Revision Date: Feburary, 7, 2025

Enables or disables Core BIOS Done Message sent to ME.

Extend CSME Measurement to TPM-PCR

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

Firmware Update Configuration

Security		
Me FW Inage Re-Flash	[0isabled]	Enable/Disable Me FW Image
Local FW Update	[Enabled]	Re-Flash function.

» 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<sup>®</sup> Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows.

Security		
PTT Capability / State	1 / 0	Selects TPM device: PTT or dTPM. PTT - Enables PTT in
TPM Device Selection	[dTPM]	SkuMgr dTPM 1.2 - Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost.

#### » 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).



Revision Date: Feburary, 7, 2025

Security		
HECI Timeouts	(Enabled)	Enable/Disable HECI Send/Receive Timeouts.
Force ME DID Init Status	(Disabled)	
CPU Replaced Polling Disable	[Disabled]	
HECI Message check Disable	[Disabled]	
MBP HOB Skip	(Disabled)	
HECI2 Interface Communication	[Disabled]	
KT Device	[Enabled]	
End Of Post Message	(Send in DXE)	
DOI3 Setting for HECI Disable	(Disabled)	
MCTP Broadcast Cycle	[Disabled]	

» 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) HOB 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

Revision Date: Feburary, 7, 2025

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

#### Anti-Rollback SVN Configuration

Security		
Minimal Allowed Anti-Rollback SVN	0	When enabled,
Executing Anti-Rollback SVN Automatic HW-Enforced	(Disabled)	hardware-enforced Anti-Rollback mechanism is
Anti-Rollback SVN		automatically activated: once
Set HW-Enforced Anti-Rollback for Current SVN	[Disabled]	ME FW was successfully run on a platform, FW with lower ARB-SVN will be blocked from execution

#### » 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



Revision Date: Feburary, 7, 2025

Security		
TPM 2.0 Device Found Firmware Version: Vendor:	15.23 IFX	Enables or Disables BIOS support for security device. 0.S. will not show Security
Security Device Support	[Enable]	Device. TCG EFI protocol and INTIA interface will not be
Active PCR banks Available PCR banks	SHA256 SHA256, SHA384	available.
SHA256 PCR Bank	[Enabled]	
Pending operation	(None)	
Platform Hierarchy Storage Hierarchy	[Enabled] [Enabled]	and the second
Endorsement Hierarchy	(Enabled)	++: Select Screen
Physical Presence Spec Version		11: Select Item
TPM 2.0 InterfaceType	[TIS]	Enter: Select
PH Randomization	(Enabled)	+/-: Change Opt.
Device Select	(TPM 2.0)	ESC: Exit
		F1: General Help
		F7: Previous Values F9: Optimized Defaults
		F10: Save & Reset Setup
		F12: Screenshot capture
		<pre> K&gt;: Scroll help area upwards</pre>
		<m>: Scroll help area downwar</m>

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

**7**STARLAKE

This settings show the Physical Presence Spec Version.

Revision Date: Feburary, 7, 2025

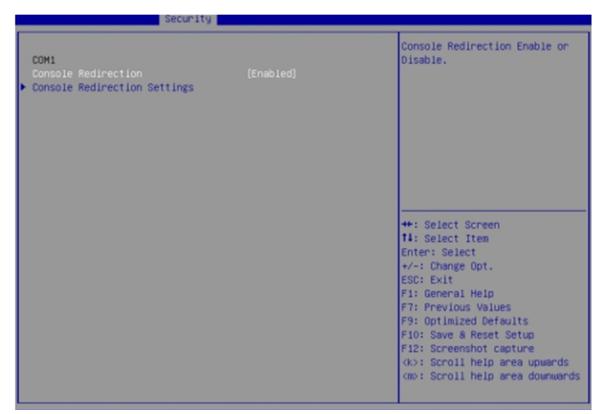
TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

Device Select

Select your TPM device through this setting.

Serial Port Console Redirection



#### Console Redirection

**7**STARLAKE

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.

Revision Date: Feburary, 7, 2025

COM1		Emulation: ANSI: Extended
Console Redirection Settings		ASCII char set. VT100: ASCII char set. VT100Plus: Extends
Terminal Type	[ANSI]	VT100 to support color,
Bits per second	[115200]	function keys, etc. VT-UTF8:
Data Bits	[8]	Uses UTF8 encoding to map
Parity	[None]	Unicode chars onto 1 or more
Stop Bits	[1]	bytes.
Flow Control	[None]	
VT-UTF8 Combo Key Support	[Enabled]	
Recorden Node	[Disabled]	
Resolution 100x31	[Disabled]	
Putty KeyPad	[VT100]	

» 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

Revision Date: Feburary, 7, 2025

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

Secure Boot

Secur	ity	
System Mode	Setup	Secure Boot feature is Active if Secure Boot is Enabled.
Secure Boot	[Disabled] Not Active	Platform Key(PK) is enrolled and the System is in User mode. The mode change requires
Secure Boot Mode ► Restore Factory Keys ► Reset To Setup Mode	(Custom)	platform reset
Key Management		
		++: Select Screen 14: Select Item
		Enter: Select +/-: Change Opt. ESC: Exit
		F1: General Help F7: Previous Values F9: Optimized Defaults
		F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards</k>
		<m>: Scroll help area downwards</m>

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

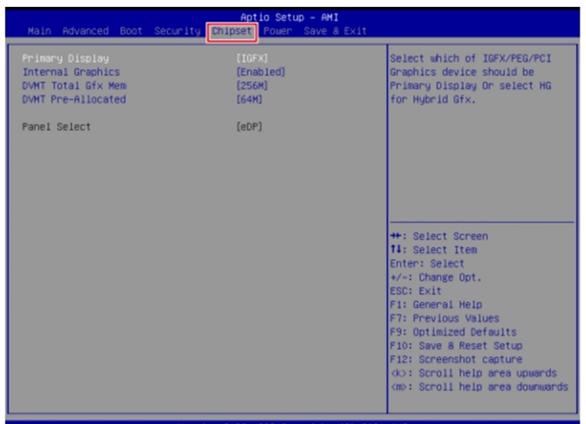
Allows you to delete all the Secure Boot keys (PK,KEK,db,dbt,dbx). The settings will be applied after reboot or at the next reboot. This item appears when "Secure Boot Mode" sets to [Custom].

Key Management

Revision Date: Feburary, 7, 2025

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

7STARLAKE

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

Revision Date: Feburary, 7, 2025

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**

Deep Sleep Mode [S4 + S5] p Advanced Resume Events Control USB [Enabled] PCIE PME/Ring [Disabled] RTC [Disabled] 	elect AC power state when ower is re-applied after a ower failure.
t E +	
F F F F	<pre>:: Select Screen L: Select Item nter: Select /-: Change Opt. SC: Exit L: General Help 7: Previous Values 3: Optimized Defaults 10: Save &amp; Reset Setup 12: Screenshot capture O: Scroll help area upwards mo: Scroll help area downward</pre>

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

**7**STARLAKE

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

Revision Date: Feburary, 7, 2025

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

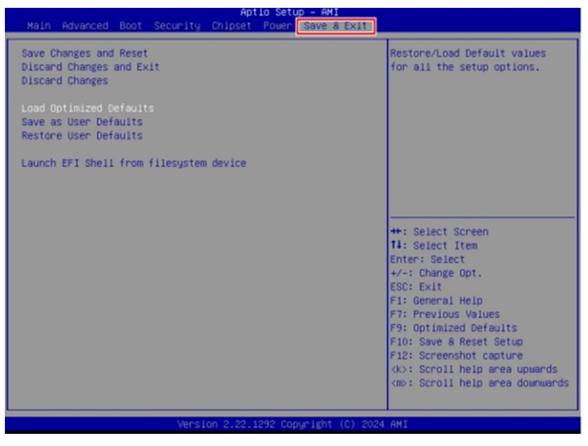
The setting allows the activity of the specified device to wake up the system from power saving modes.

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

**7**STARLAKE

Save changes to CMOS and reset the system.

Revision Date: Feburary, 7, 2025

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.

