ASB110-PI900

Palm-Sized Box PC
with IBASE PI900 Pico-ITX Board

User Manual

Version 1.0
November 2026

Copyright

© 2026 IBASE Technology, Inc. All rights reserved.
No part of this publication may be reproduced, copied, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, photocopying, or otherwise, without the prior written consent of IBASE Technology, Inc. (hereinafter referred to as “IBASE”).

Disclaimer

IBASE reserves the right to make changes and improvements to the products described in this document without prior notice. Every effort has been made to ensure the information in the document is correct; however, IBASE does not guarantee this document is error-free. IBASE assumes no liability for incidental or consequential damages resulting from misapplication or inability to use the product or the information contained herein, nor for any infringements of rights of third parties, which may result from its use.

Trademarks

All the trademarks, registrations, and brands mentioned herein are used for identification purposes only and may be trademarks and/or registered trademarks of their respective owners.

Compliance

CE

This product has passed CE tests for environmental specifications and limits. This product is in accordance with the directives of the European Union (EU). If users modify and/or install other devices in this equipment, the CE conformity declaration may no longer apply.

FC

This product has been tested and found to comply with the limits for a Class B 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 manufacturer's instructions, may cause harmful interference to radio communications.

WEEE



This product must not be disposed of as normal household waste, in accordance with the EU directive for Waste Electrical and Electronic Equipment (WEEE – 2012/19/EU). Instead, it should be disposed of by returning it to a municipal recycling collection point. Check local regulations for disposal of electronic products.

Green IBASE



This product is compliant with the current RoHS 2 restrictions and prohibits use of the following substances in concentrations exceeding 0.1% by weight (1000 ppm) except for cadmium, limited to 0.01% by weight (100 ppm).

- Hexavalent chromium: 1,000 ppm
- Polybrominated biphenyls (PBBs): 1,000 ppm
- Polybrominated diphenyl ethers (PBDEs): 1,000 ppm
- Cadmium: 100 ppm
- Mercury: 1,000 ppm
- Lead: 1,000 ppm
- Bis(2-ethylhexyl) phthalate (DEHP): 1,000 ppm
- Butyl benzyl phthalate (BBP): 1,000 ppm
- Dibutyl phthalate (DBP): 1,000 ppm
- Diisobutyl phthalate (DIBP): 1,000 ppm

iBASE

Important Safety Information

Carefully read the precautions before using the device.

Environmental conditions:

- Place the device horizontally on a stable, solid surface to prevent it from falling and causing damage.
- Leave plenty of space around the device and do not block the openings for ventilation. Never drop or insert any objects of any kind into the ventilation openings.

Care for your IBASE products:

- Before cleaning the device, turn it off and unplug all cables, including the power cord, to prevent electrical current from flowing.
- Use neutral cleaning agents or diluted alcohol to clean the device chassis with a cloth. Then wipe the chassis with a dry cloth.
- Vacuum the dust with a computer vacuum cleaner to prevent the air vent or slots from being clogged.



WARNING

Attention during use:

- Do not use this product near water.
- Do not spill water or any other liquids on your device.
- Do not place heavy objects on the top of the device.
- Operate this device from the type of power indicated on the marking label. If you are not sure of the type of power available, consult your distributor or local power company.
- Do not walk on the power cord or allow anything to rest on it.
- If you use an extension cord, make sure that the total ampere rating of the product plugged into the extension cord does not exceed its limits.

Avoid Disassembly

Users are not advised to disassemble, repair or make any modification to the device. Disassembly, modification, or any attempt at repair could generate hazards and cause damage to the device, even bodily injury or property damage, and will void any warranty.



CAUTION

Danger of explosion if the internal battery is replaced with an incorrect type. Replace only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.

Warranty Policy

- **IBASE standard products:**

  24-month (2-year) warranty from the date of shipment. If the date of shipment cannot be ascertained, the product serial numbers can be used to determine the approximate shipping date.

- **3rd-party parts:**

  12-month (1-year) warranty from delivery for the 3rd-party parts that are not manufactured by IBASE, such as CPU, memory, SSD/HDD, power adapter, panel and touchscreen.

* *Products that fail due to misuse, accident, improper installation or unauthorized repair shall be treated as out of warranty and customers shall be billed for repair and shipping charges.*

Technical Support & Services

1. Visit the IBASE website at www.ibase.com.tw to find the latest information about the product.
2. If you need any further assistance from your distributor or sales representative, prepare the following information of your product and elaborate upon the problem.
   - Product model name
   - Product serial number
   - Detailed description of the problem
   - Error messages in text or screenshots, if any
   - The arrangement of the peripherals
   - Software in use (such as OS and application software, including the version numbers)
3. If repair service is required, you can download the RMA form at the website of IBASE. Fill out the form and contact your distributor or sales representative.

iBASE

Table of Contents

Chapter 1 General Information 1

1.1 Introduction 2
1.2 Features 3
1.3 Packing List 3
1.4 Optional Accessory 3
1.5 Specifications 4
1.6 Product View 5
1.7 Dimensions 8

Chapter 2 Hardware Configuration 9

2.1 Installation 10
2.1.1 System Disassembly Procedure 11
2.1.2 Memory Module Installation 15
2.1.3 M.2 Card Installation 15
2.1.4 Antenna Installation 16

Chapter 3 Driver Installation 17

3.1 Introduction 18
3.2 Intel® Chipset Software Installation Utility 18
3.3 Graphics Driver Installation 20
3.4 Realtek HD Audio Driver Installation 21
3.5 Realtek Audio DCH Driver Installation 22
3.6 Intel® Management Engine Driver Installation 23
3.7 Intel(R) Serial IO Driver Installation 24
3.8 Intel(R) PMT Driver Installation 25
3.9 Intel(R) NPU IO Driver Installation 26
3.10 Realtek LAN Driver Installation 27

Chapter 4 BIOS Setup 28

Appendix 50

A. I/O Port Address Map 51
B. Interrupt Request Lines (IRQ) 52

Chapter 1
General Information

The information provided in this chapter includes:

- Features
- Packing List
- Specifications
- Product View
- Dimensions

1.1 Introduction

The ASB110-PI900 is a compact, embedded system based on the IBASE PI900 PICO-ITX motherboard, powered by an Intel® Core™ Ultra 100U processor with integrated Intel® graphics. It supports one DDR5-5600 SO-DIMM slot, up to 48GB, and provides one M.2 2280 M-Key slot for NVMe/SATA storage and one M.2 2230 E-Key slot for Wi-Fi/Bluetooth connectivity. The system provides three USB 3.2 ports, one 2.5GbE LAN port, HDMI, and DisplayPort output through USB Type-C. It also supports a 12V DC power input, wall mounting, and optional DIN-rail mounting.
The ASB110-PI900 is suitable for industrial and embedded applications.



1.2 Features

- Palm-Sized System with IBASE PI900 Pico-ITX Board (TDP 15W)
- Onboard Intel® Core™ Ultra 100U Processor
- 1x DDR5 SO-DIMM, Max. 48GB
- Supports HDMI, DP thru USB Type-C
- 3x USB 3.2, 1x 2.5 GbE
- Supports 2x M.2 sockets (E2230 and M2280)
- 12V DC-in power input
- Supports Wall mounting, DIN-rail mounting and TPM (2.0)

1.3 Packing List

Your product package should include the items listed below.

- ASB110-PI900M

1.4 Optional Accessory

- 120W (12V@10A) power adaptor
- DIN-rail
- Wall mount bracket

The user's manual can be downloaded from the IBASE website.

1.5 Specifications

ASB110-PI900M-155	Palm-Sized box PC with PI900F-155U, Onboard Intel® Core™ Ultra 7 155U CPU, 3x USB 3.2, w/o memory/ SSD
ASB110-PI900M-125	Palm-Sized box PC with PI900F-125U, Onboard Intel® Core™ Ultra 5 125U CPU, 3x USB 3.2, w/o memory/ SSD
System Mainboard	IBASE PI900F
CPU Type	Intel® Core™ Ultra 100U Processor
Memory	1 x DDR5-5600 SO-DIMM, Max. 48GB
Storage	1 x M.2-M-Key (2280)
Front Panel I/O	• 1 x DC-jack • 1 x 2.5G LAN • 1 x HDMI • 1 x USB Type-C • 1 x Power button • 3 x USB 3.2 ports
Rear Panel I/O	N/A
Left Panel I/O	1 x Antenna hole
Right Panel I/O	2 x Antenna holes
Expansion Slots	• 1 x M.2 2230 (E-key) supports WiFi/ BT
Mounting	Optional for Wall mount / DIN-rail / VESA mount (75 x 75)
Dimensions	140mm (W) x 95mm (D) x 60mm (H) 5.52” (W) x 3.74” (D) x 2.36” (H)
Weight	1.2 kg
Certification	CE / FCC Class B / LVD
Regulation	RoHS 2.0
Environment	
Operating Temperature	0°C~55°C (32°F~131°F) *with airflow 0.9m/s
Storage Temperature	-20°C~80°C (-4°F~176°F)
Relative Humidity	5%~90%@45°C (non-condensing)
Vibration	Operating: 1 Grms / 3~500Hz
Shock	Operating: 20G / 11ms Non-operating: 40G / 11ms

All specifications are subject to change without prior notice.

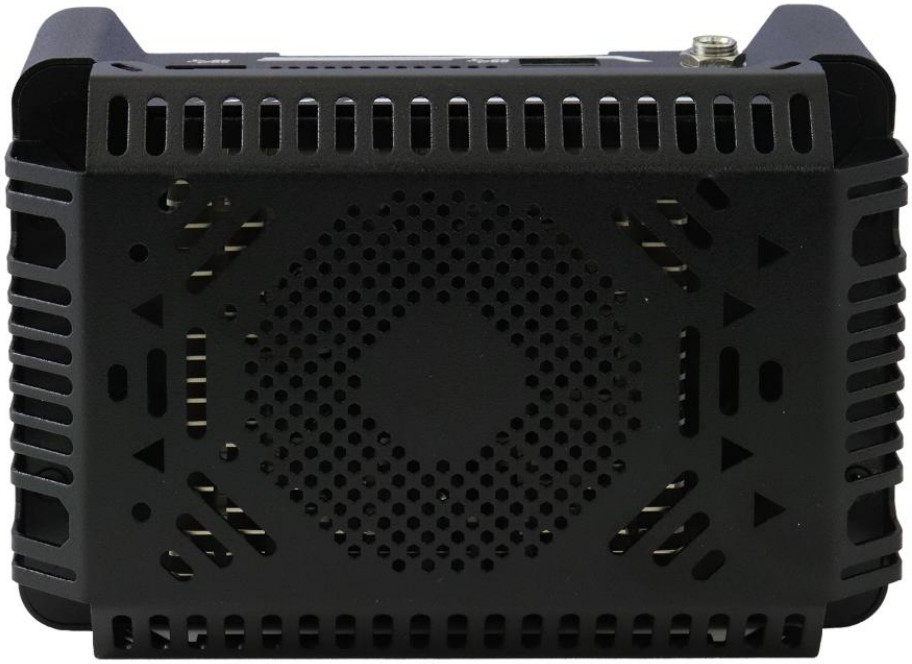
1.6 Product View

Front View



Front Panel External I/O	• 1 x DC-jack • 1x 2.5 GbE • 3x USB 3.2 • 1x HDMI • 1 x USB Type-C • 1 x Power button

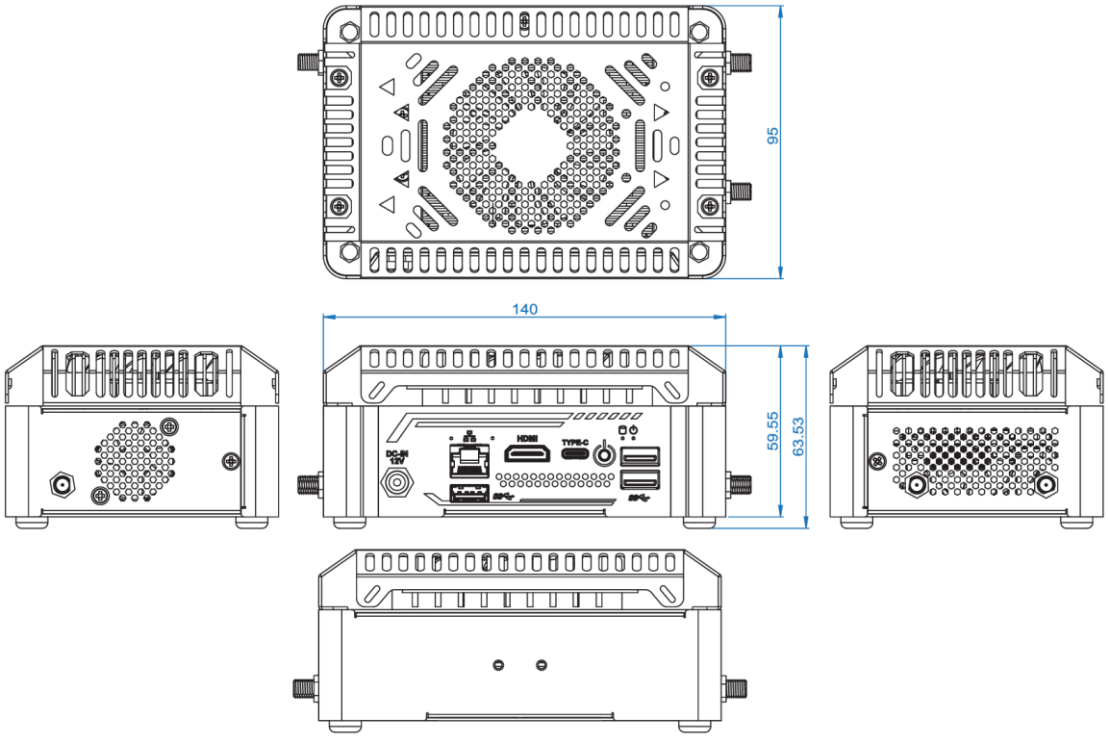
Top View



Oblique View



1.7 Dimensions



Chapter 2
Hardware Configuration

The information provided in this chapter includes:

- System disassembly procedure
- Memory and M.2 device installation
- Antenna installation

2.1 Installation

Before installing or replacing internal components, turn off the system and disconnect the power adapter and all peripheral cables.

Remove the system covers as described in the following section to access the DDR5 SO-DIMM socket and M.2 expansion slots on the PI900F motherboard.

The accessible internal connectors include:

- **DDR5 SO-DIMM Socket (J1)**
- **M.2 M-Key Slot (J5)**
- **M.2 E-Key Slot (J6)**

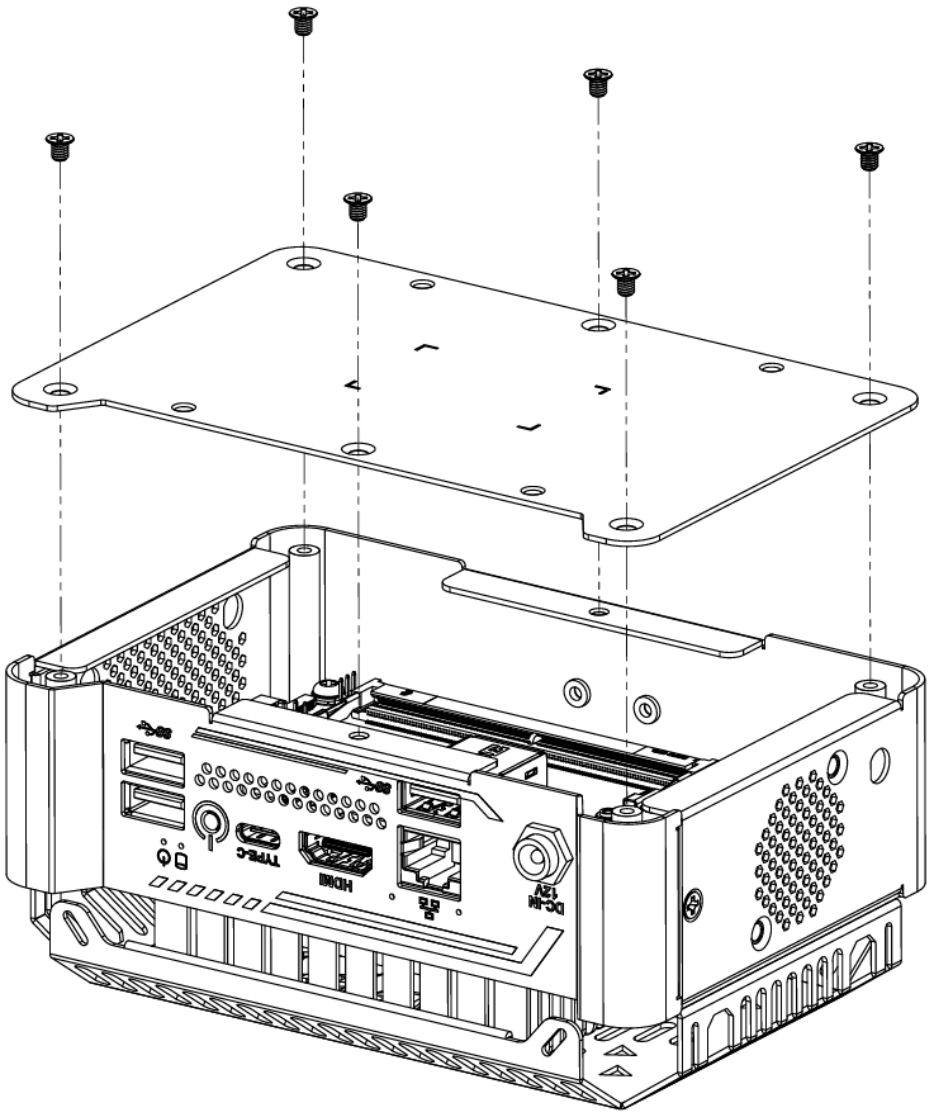
2.1.1 System Disassembly Procedure

Follow the steps below to remove the bottom covers and access the internal components.

Step 1: Remove the Outer Bottom Cover

Remove the **six screws** securing the outer bottom cover.

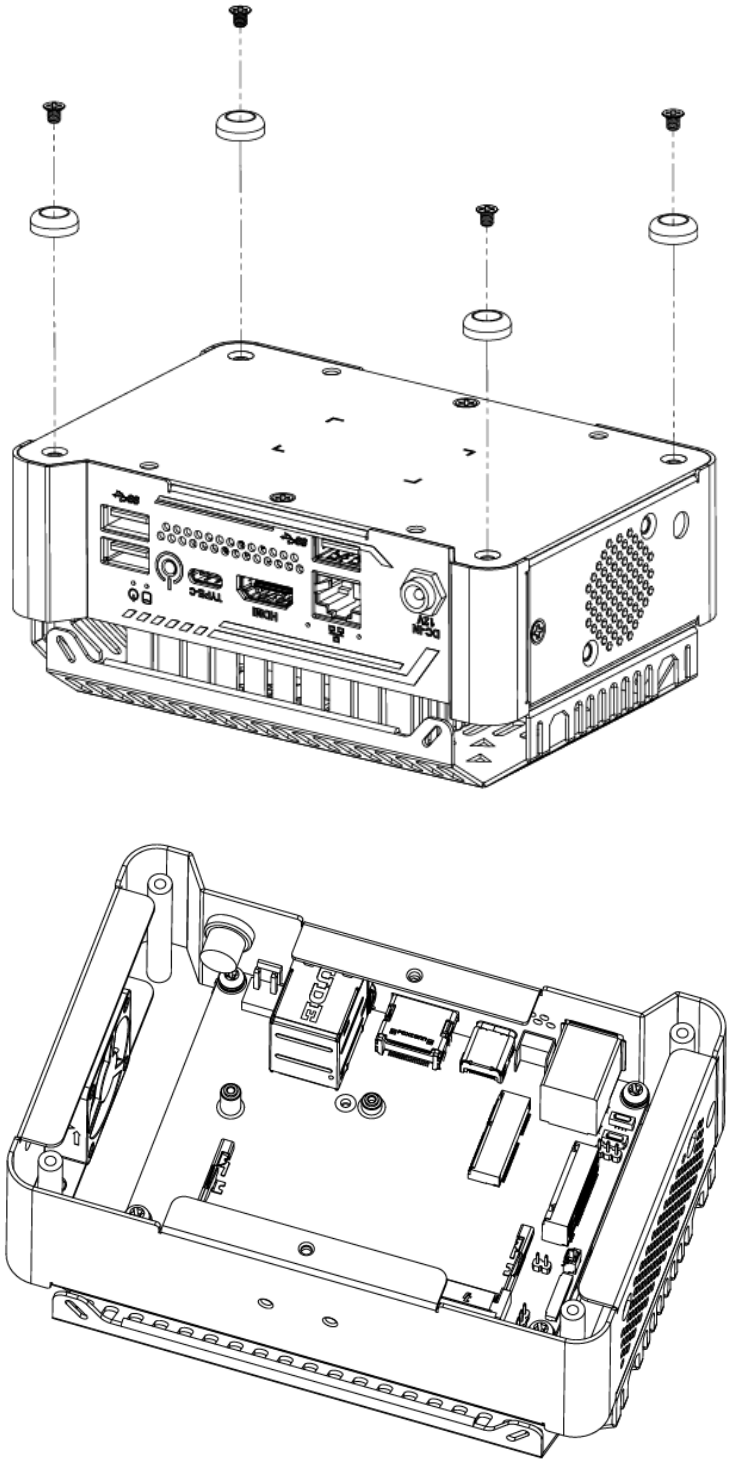
Carefully remove the cover from the system.



Step 2: Remove the Inner Bottom Cover

Remove the four screws located beneath the rubber feet.

Remove the rubber feet as necessary to access the screws, then carefully remove the inner bottom cover.



Internal Components

Step 3: Access the Internal Components

After removing both bottom covers, the PI900F motherboard and its internal sockets are accessible.

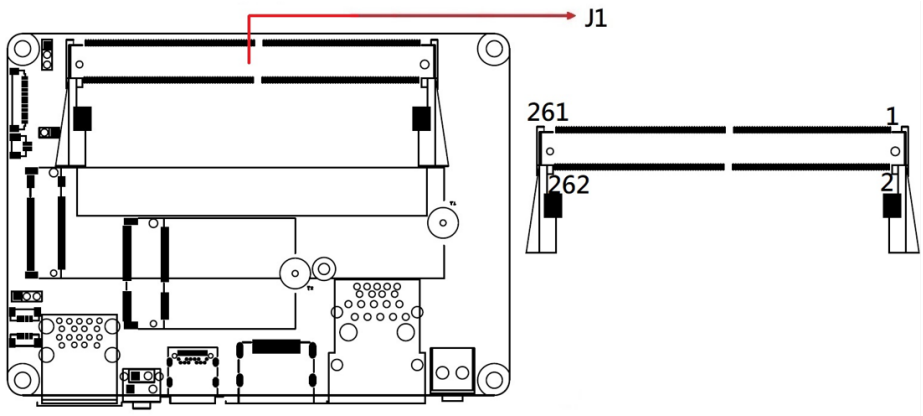
The following components can then be accessed for installation or replacement:

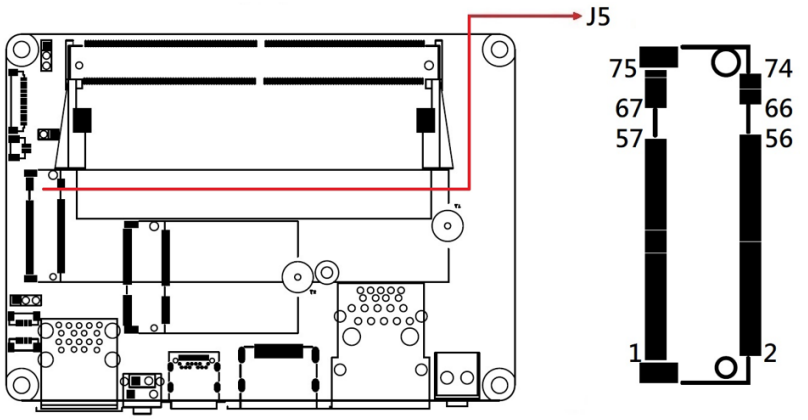
- **J1: DDR5 SO-DIMM Socket**

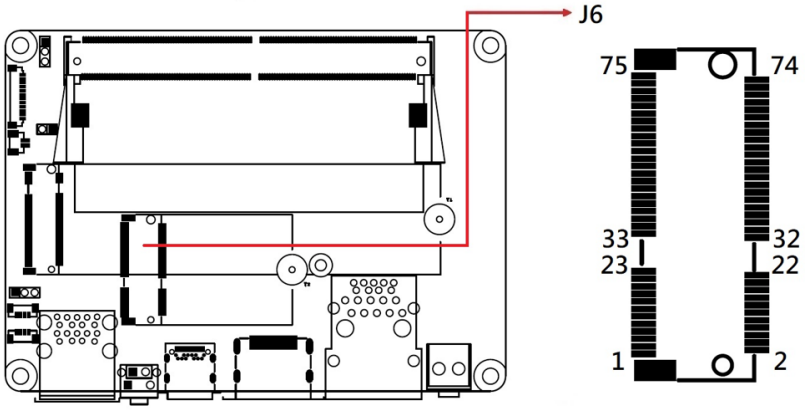
  Used for installation of the system memory module.
- **J5: M.2 M-Key Slot**

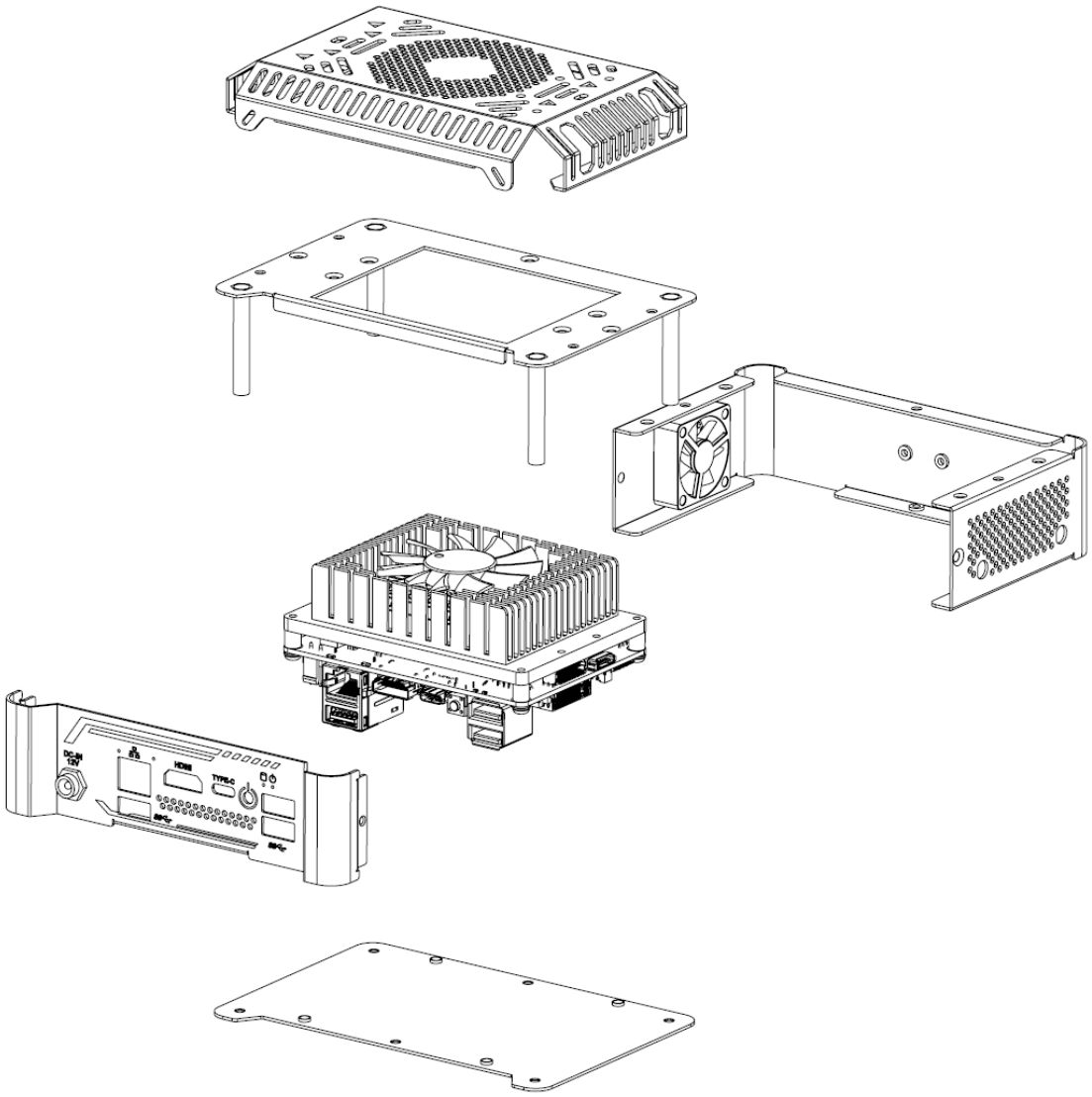
  Used for installation of an M.2 storage device.
- **J6: M.2 E-Key Slot**

  Used for installation of a wireless communication module such as Wi-Fi/Bluetooth.







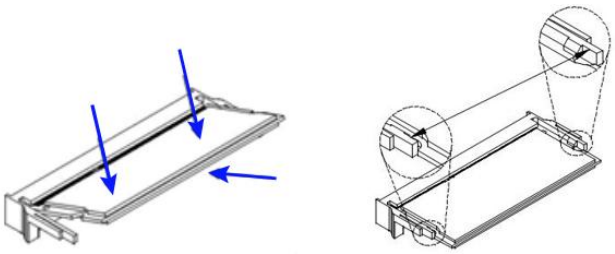


System Exploded View

2.1.2 Memory Module Installation

1. Locate the DDR5 SO-DIMM socket and align the notch on the memory module with the key in the socket.
2. Insert the memory module into the socket at an angle, then gently press it downward until the retaining clips lock the module in place.

   To remove the memory module, push the retaining clips outward. The module will release from the socket.



2.1.3 M.2 Card Installation

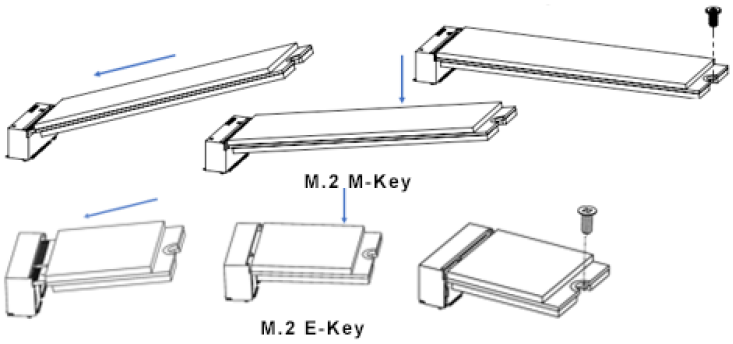
The ASB110-PI900 provides one M.2 M-Key slot and one M.2 E-Key slot on the PI900F motherboard:

- **J5: M.2 2280 M-Key slot, supports NVMe/SATA SSD.**
- **J6: M.2 2230 E-Key slot, supports Wi-Fi/Bluetooth.**

To install an M.2 card:

1. Locate the appropriate M.2 slot on the motherboard.
2. Align the key of the M.2 card with the key in the slot.
3. Insert the M.2 card into the slot at an angle.
4. Gently press the card downward until it lies flat.
5. Secure the M.2 card to the mounting standoff with the retaining screw.

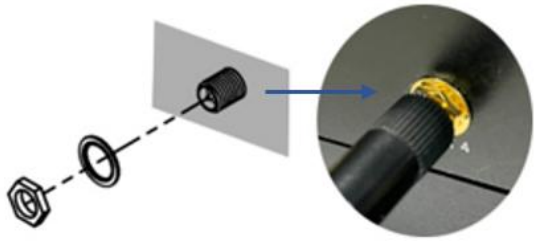
To remove an M.2 card, remove the retaining screw, allow the card to rise slightly, and carefully pull it out of the slot.



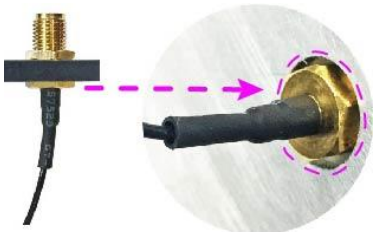
2.1.4 Antenna Installation

Route the antenna extension cable through the antenna mounting hole on the system chassis. Secure the antenna connector with the washer and hex nut as shown below.

1. Thread and fasten the hex nut and the washer. Then install the antenna.



2. Apply adhesive around here.



Info: The diameter of the nut is approximately 6.35 mm (0.25"-36UNC).

After installing the internal components and completing the antenna installation, reinstall the bottom covers by reversing the disassembly procedure described in Section 2.1.1.

Chapter 3
Driver Installation

This chapter introduces installation of the Intel(R) Meteor Lake-P/PS/U Chipset Drivers:

1. Intel(R) Chipset Software Installation
2. Intel(R) HD Graphics
3. Realtek Audio
4. Intel(R) ME
5. Intel(R) Serial IO
6. Intel(R) PMT
7. Intel(R) NPU
8. Realtek RTL8125BG 2.5G

3.1 Introduction

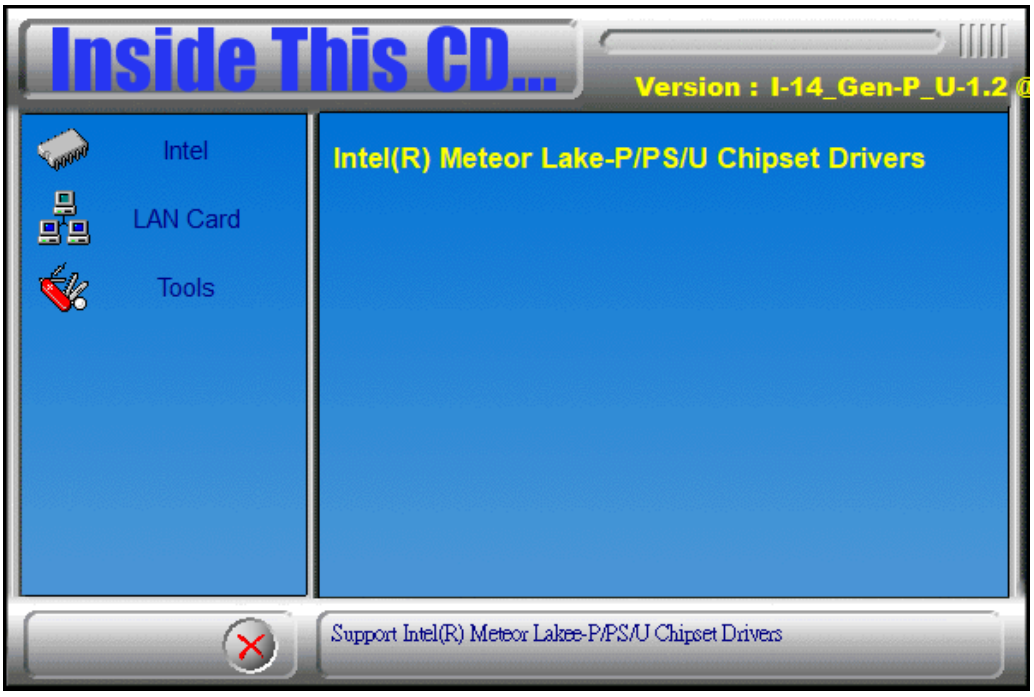
This section describes the installation procedures for software and drivers.

Note: After installing your Windows operating system, you must install the Intel® Chipset Software Installation Utility first before proceeding with the driver installation.

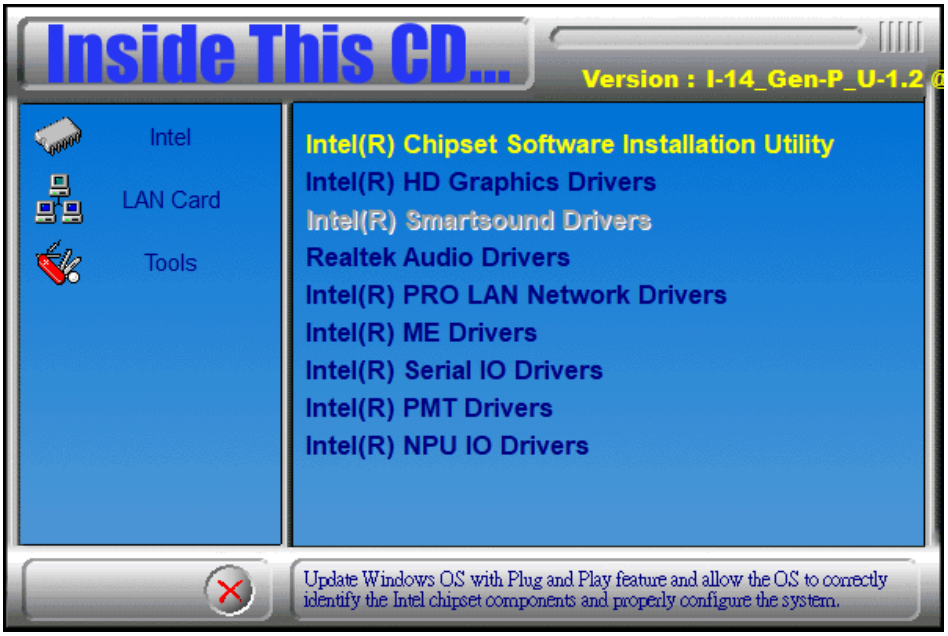
3.2 Intel® Chipset Software Installation Utility

The Intel® Chipset drivers should be installed first before the software drivers to install INF files for Plug & Play function for Intel chipset components. Follow the instructions below to complete the installation.

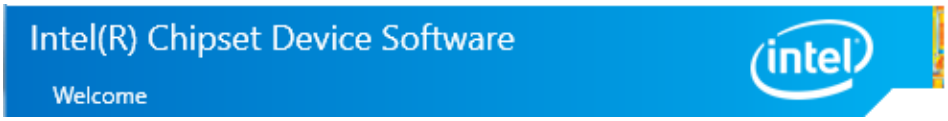
1. Go to the download page of the product. Copy the compressed drivers file to your computer. Double-click the file to extract its contents. Run "CDGuide" to go to the main drivers page as shown below. Click **Intel** on the left pane and then **Intel(R) Meteor Lake-P/PS/U Chipset Drivers** on the right pane.



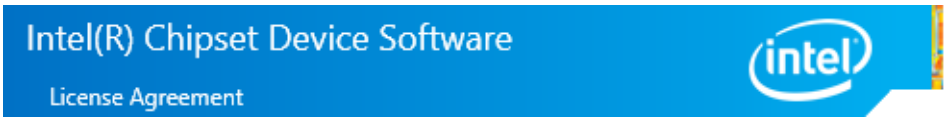
2. Click **Intel(R) Chipset Software Installation Utility**.



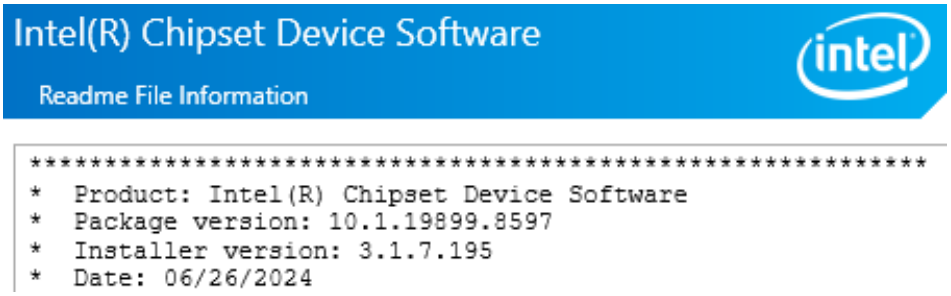
3. When the *Welcome* screen to the Intel® Chipset Device Software appears, click **Next** to continue.



4. Accept the software license agreement and proceed with the installation process.



5. On the *Readme File Information* screen, click **Install**.



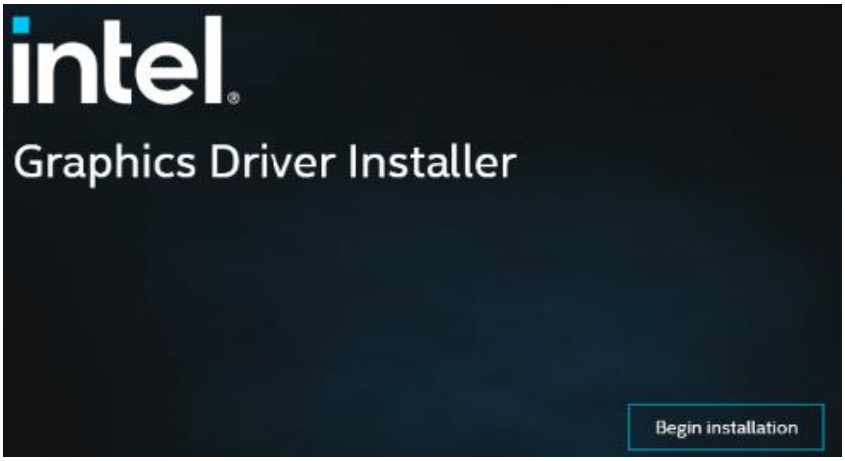
6. Click **Finish** to complete the setup process.

3.3 Graphics Driver Installation

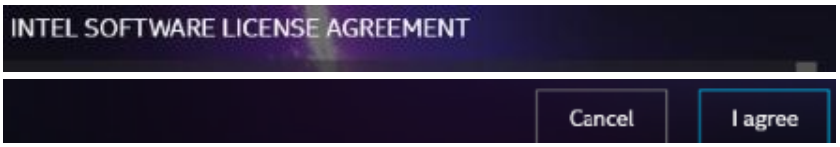
1. Click **Intel** on the left pane and then **Intel(R) Meteor Lake-P/PS/U Chipset Drivers** on the right pane.
2. Click **Intel(R) HD Graphics Driver**.



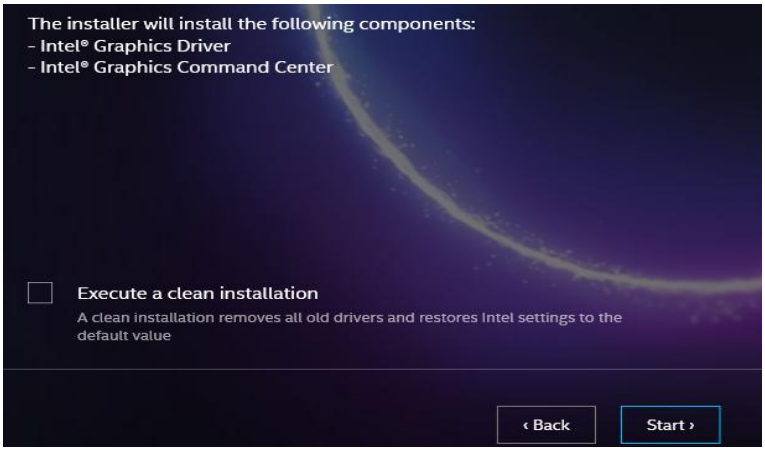
3. Click **Begin installation**.



4. Click **I agree** to accept the license agreement.



5. On the next screen, click **Start and** then click **Finish** when installation has been completed.



3.4 Realtek HD Audio Driver Installation

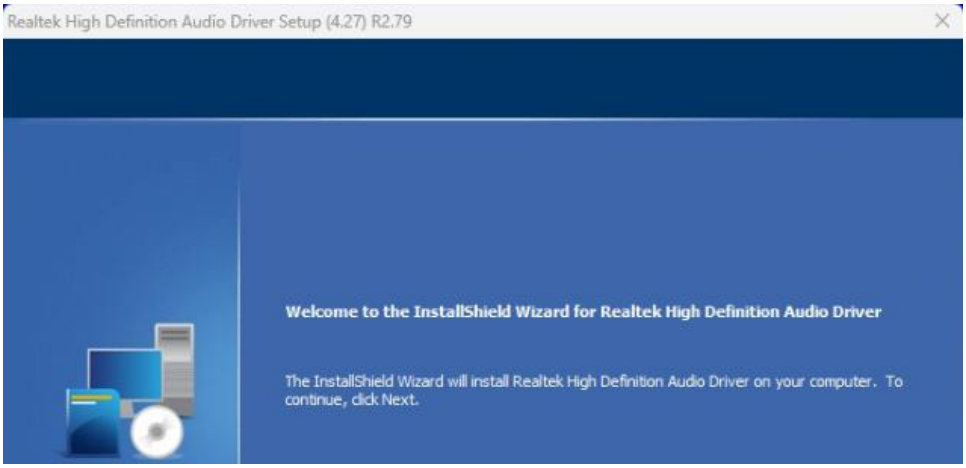
1. Click **Intel** on the left pane and then **Realtek Audio Drivers** on the right pane.



2. Click **Realtek High Definition Audio Driver**.



3. When the *Welcome* screen appears, click **Next** to start the installation.



4. After installation has been completed, restart the computer for changes to take effect.



3.5 Realtek Audio DCH Driver Installation

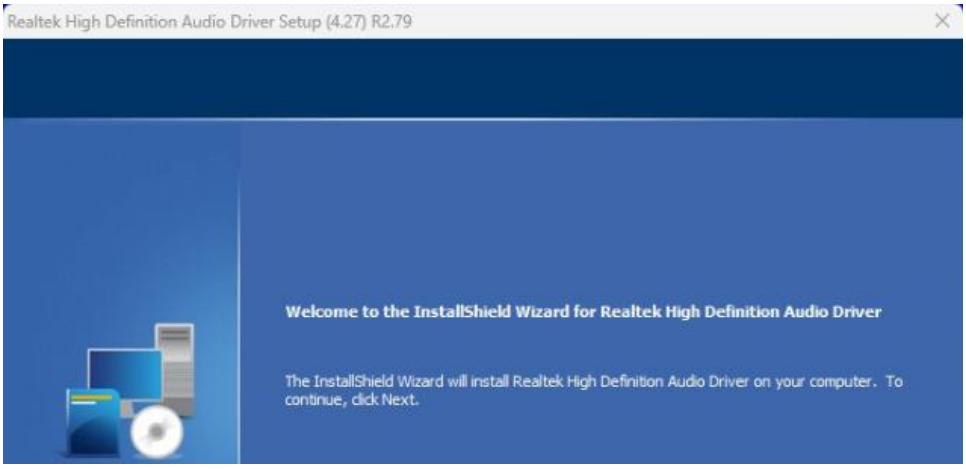
1. Click **Intel** on the left pane and then **Realtek Audio Drivers** on the right pane.



2. Click **Realtek Audio DCH Drivers**.



3. When the *Welcome* screen appears, click **Next** to start the installation.

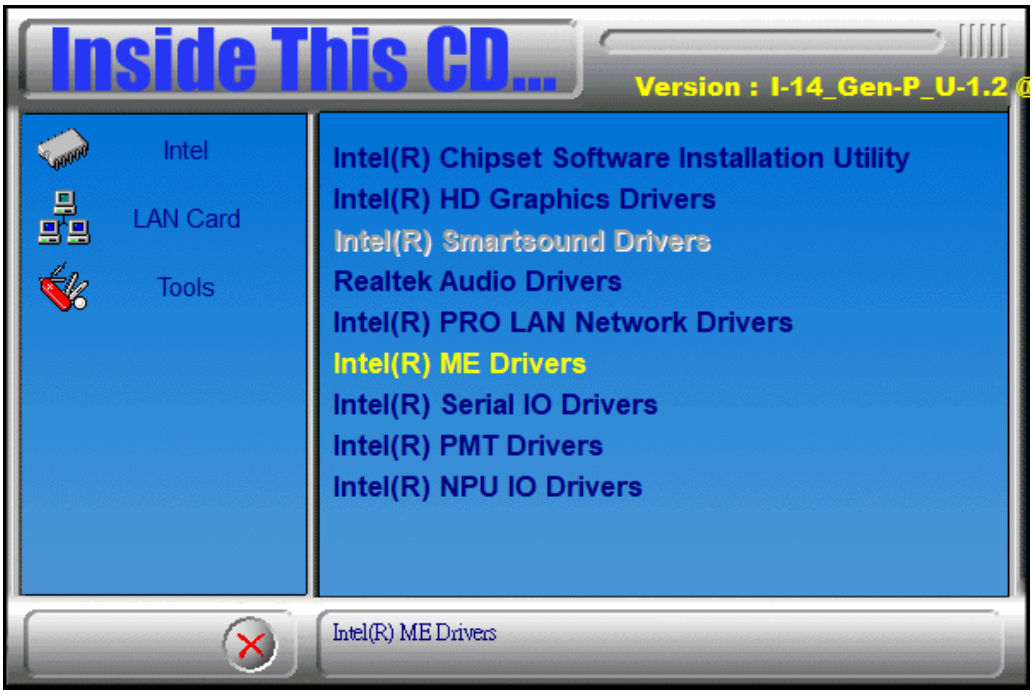


4. After installation has been completed, restart the computer for changes to take effect.

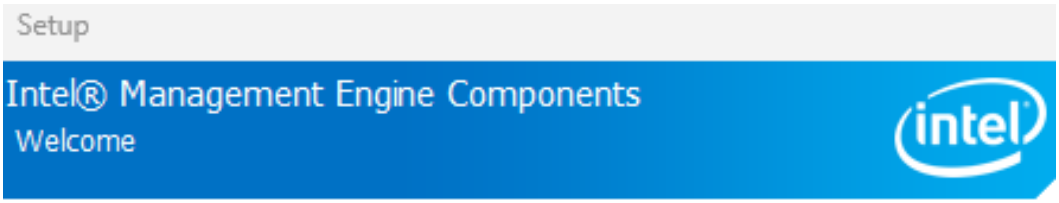


3.6 Intel® Management Engine Driver Installation

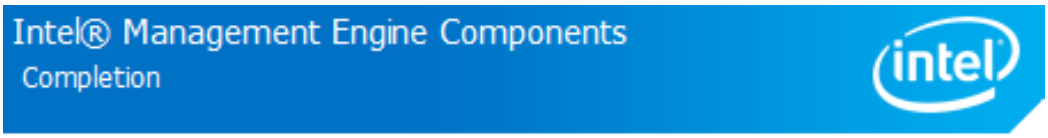
1. Click **Intel** on the left pane and then **Intel(R) Meteor Lake-P/PS/U Chipset Drivers** on the right pane.
2. Click **Intel(R) ME Drivers**.



3. When the *Welcome* screen appears, click **Next**.

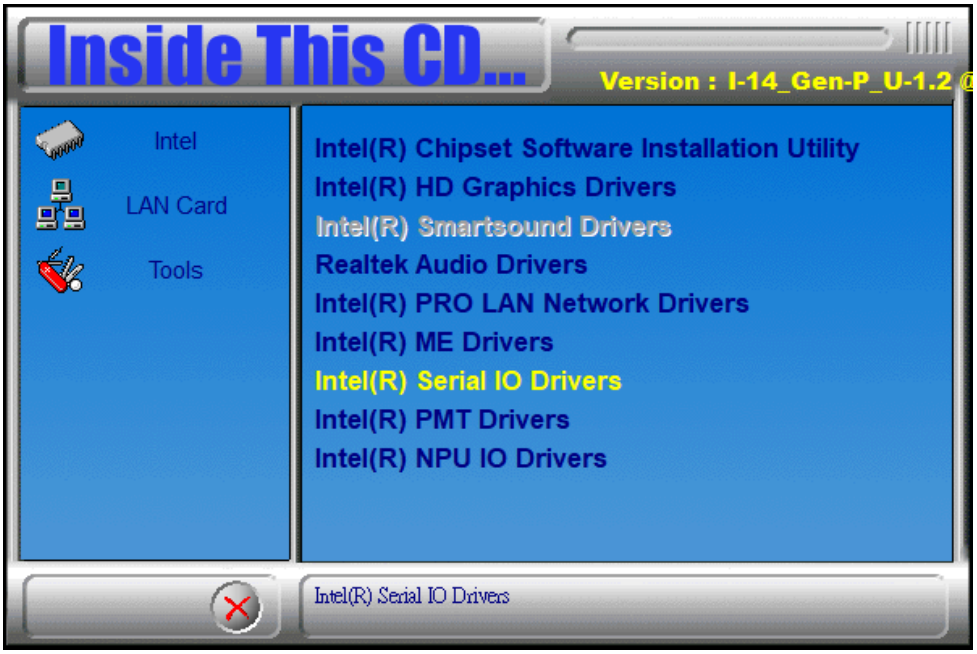


4. Accept the license agreement and click **Next**.
5. Click **Next** to install to the default folder, or click Change to choose another destination folder.
6. After Intel Management Engine Components have been successfully installed, click **Finish**.



3.7 Intel(R) Serial IO Driver Installation

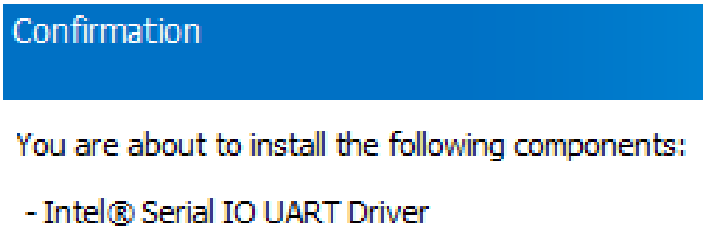
1. Click **Intel** on the left pane and then **Intel(R) Meteor Lake-P/PS/U Chipset Drivers** on the right pane.
2. Click **Intel(R) Serial IO Drivers**.



3. In the Welcome screen, click **Next**.



4. In the next screen, accept the license agreement and click **Next**.
5. In the Readme File Information screen, click **Next**.
6. In the Confirmation screen, click **Next**.

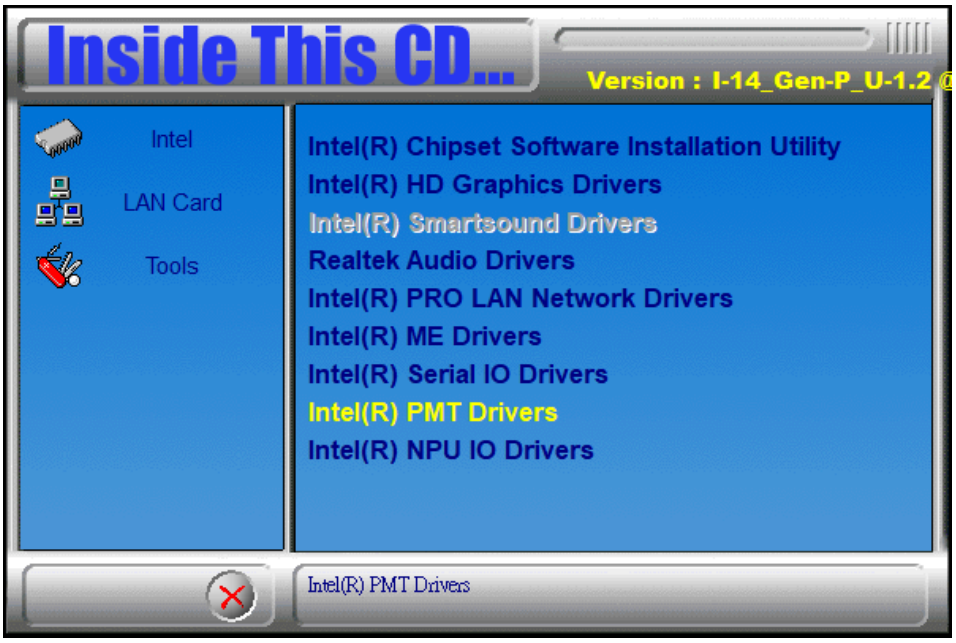


7. When installation has been completed, click **Finish**.

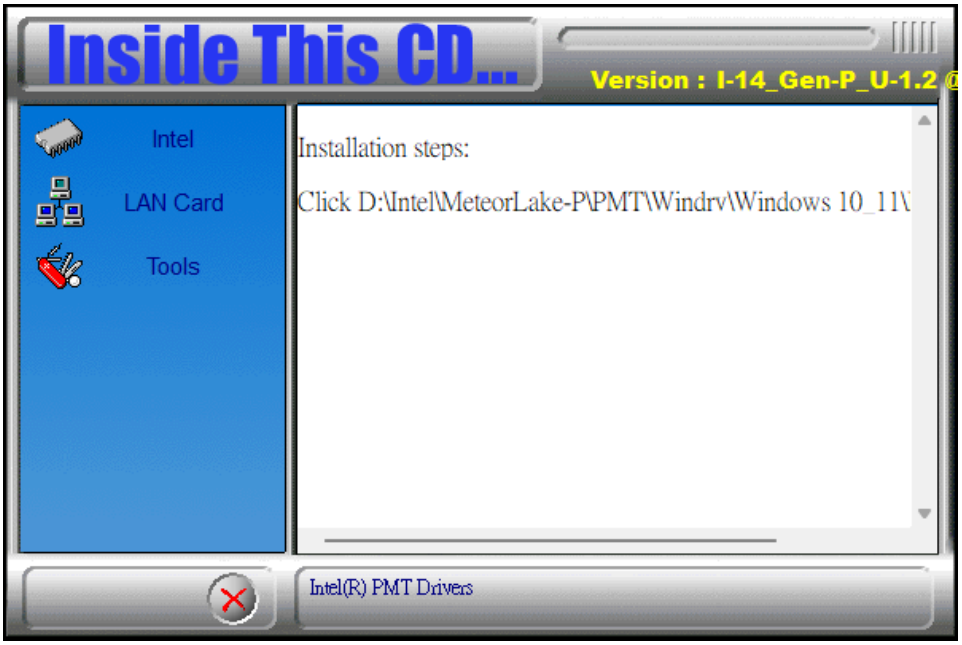


3.8 Intel(R) PMT Driver Installation

1. Click **Intel** on the left pane and then **Intel(R) Meteor Lake-P/PS/U Chipset Drivers** on the right pane.
2. Click **Intel(R) PMT Drivers**.

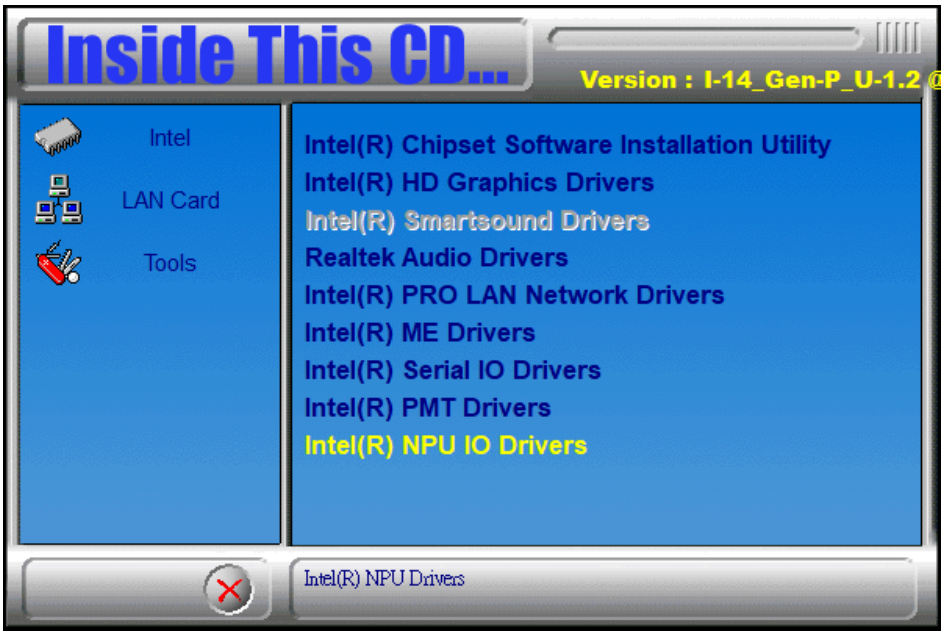


3. Follow the steps until InstallShield Wizard completes the installation.

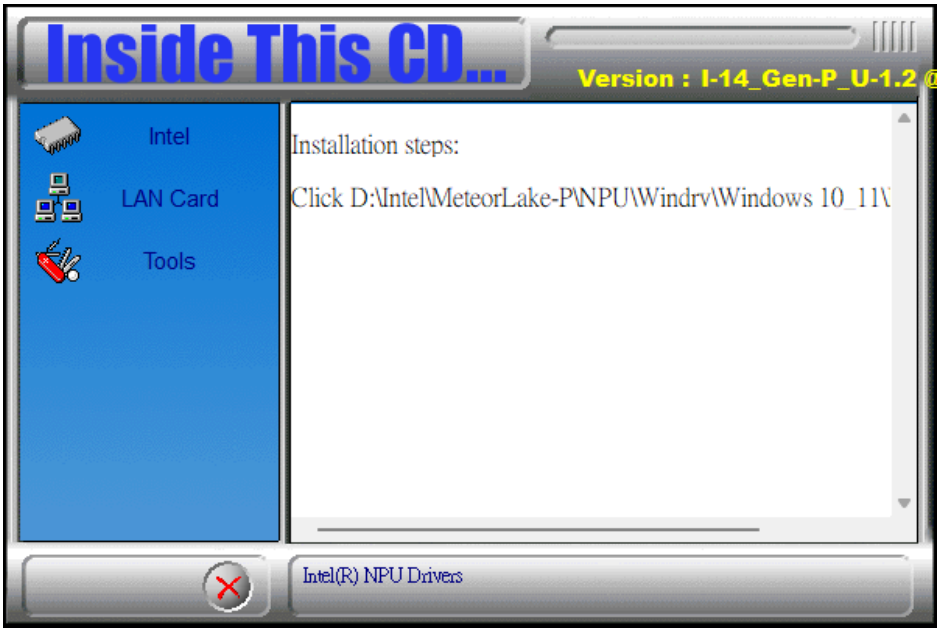


3.9 Intel(R) NPU IO Driver Installation

1. Click **Intel** on the left pane and then **Intel(R) Meteor Lake-P/PS/U Chipset Drivers** on the right pane.
2. Click **Intel(R) NPU IO Drivers**.



3. Follow the steps until InstallShield Wizard completes the installation.



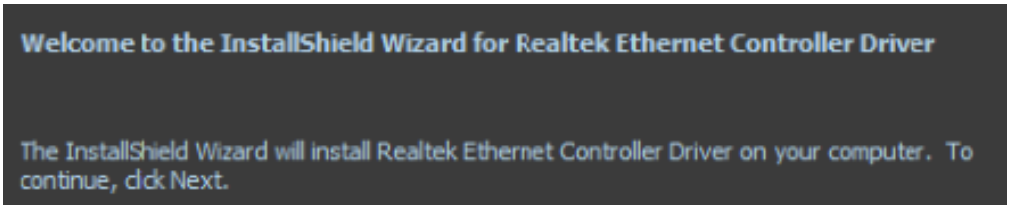
3.10 Realtek LAN Driver Installation

1. Click **LAN Card** on the left pane and then **Realtek LAN Controller Drivers**. Click **Realtek RTL8125BG 2.5G LAN Drivers**.

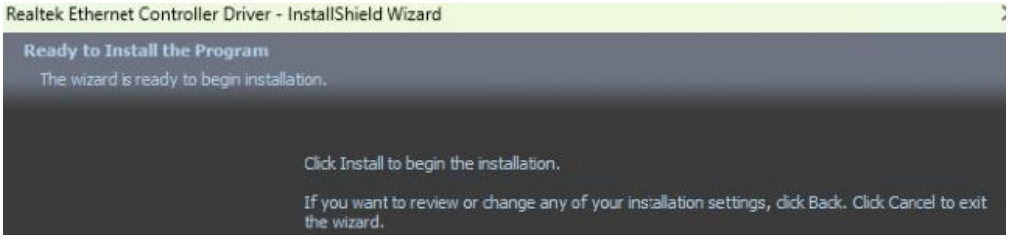




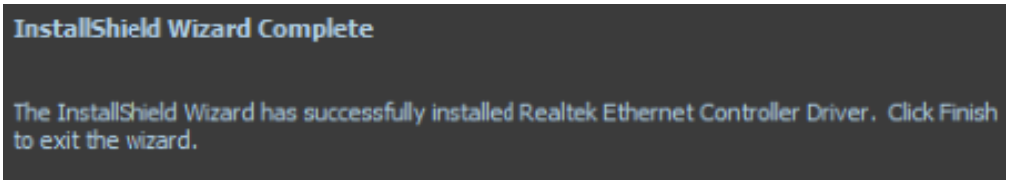
2. When the Welcome screen appears, click **Next**.



3. When the Ready to Install the Program screen appears, click **Install**.



4. When the InstallShield Wizard has completed the installation, click **Finish**.



Chapter 4
BIOS Setup

4.1 Introduction

The BIOS (Basic Input/Output System) installed in the ROM of your computer system provides critical low-level support for standard devices such as disk drives, and serial ports. It also provides password protection as well as special support for detailed fine-tuning of the chipset controlling the entire system.

4.2 BIOS Setup

The BIOS provides a Setup utility program for specifying the system configurations and settings. The BIOS ROM of the system stores the Setup utility. When you turn on the computer, the BIOS is immediately activated. Press the <Del> key immediately to enter the Setup utility. If you are a little bit late pressing the <Del> key, POST (Power On Self Test) will continue with its test routines, thus preventing you from invoking the Setup.

If you still need to enter Setup, restart the system by simultaneously pressing the <Ctrl>, <Alt> and <Delete> keys.
You can also restart by turning the system Off and back On again.

The following message will appear on the screen:

```
Press <DEL> to Enter Setup
```

In general, press the arrow keys to highlight items, <Enter> to select, the <PgUp> and <PgDn> keys to change entries, <F1> for help, and <Esc> to quit.

When you enter the BIOS Setup utility, the *Main Menu* screen will appear on the screen. The Main Menu allows you to select from various setup functions and exit choices.

Warning: It is strongly recommended that you avoid making any changes to the chipset defaults.

These defaults have been carefully chosen by both AMI and your system manufacturer to provide the absolute maximum performance and reliability. Changing the defaults could make the system unstable and crash in some cases.

4.3 Main Settings



BIOS Setting	Description
System Date	Sets the date. Use the <Tab> key to switch between the date elements.
System Time	Set the time. Use the <Tab> key to switch between the time elements.

4.4 Advanced Settings

This section allows you to configure system features according to your preference.

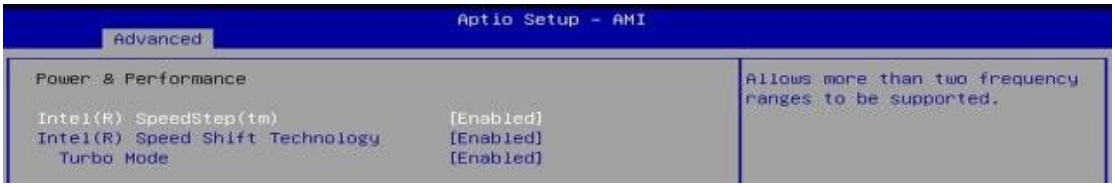


4.4.1 CPU Configuration



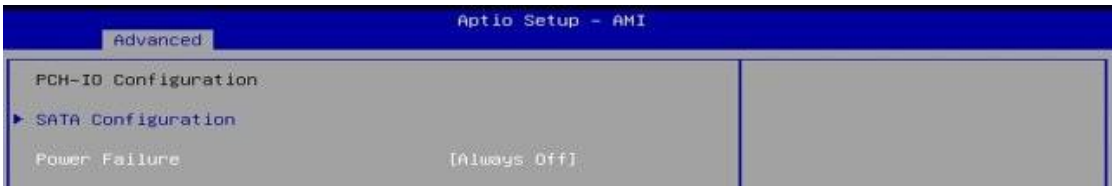
BIOS Setting	Description
Intel (VMX) Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Performance-cores	Number of P-cores to enable in each processor package. Note: Number of cores and E-cores are looked at together. When both are (0,0), Pcode will enable all cores.
Active Efficient-cores	Number of E-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 SOC-North Efficient-cores	Number of SOC-North Efficient-cores to enable in SOC North.
Hyper-Threading	Enable or Disable Hyper-Threading Technology.

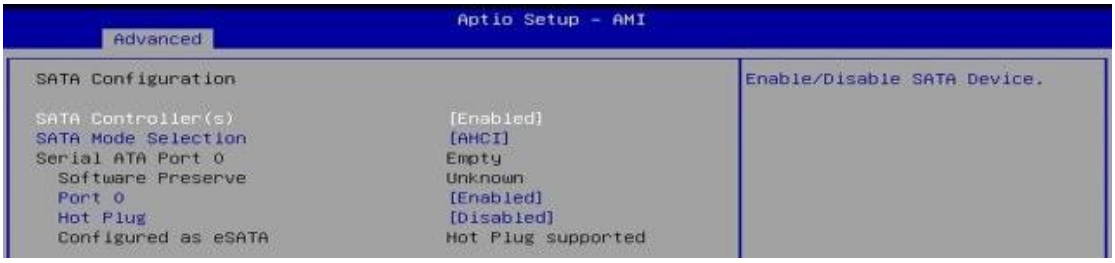
4.4.2 Power & Performance

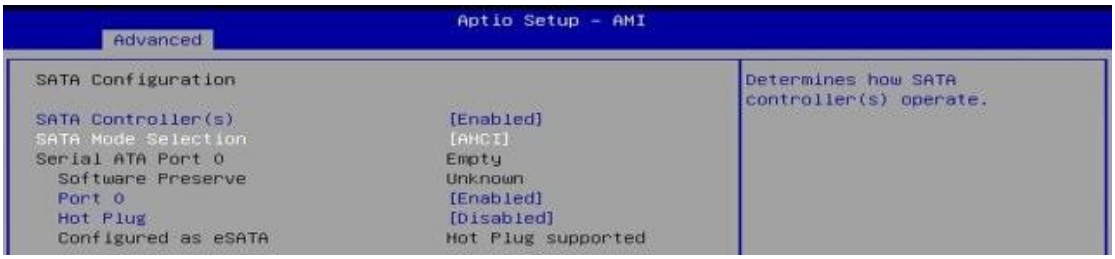


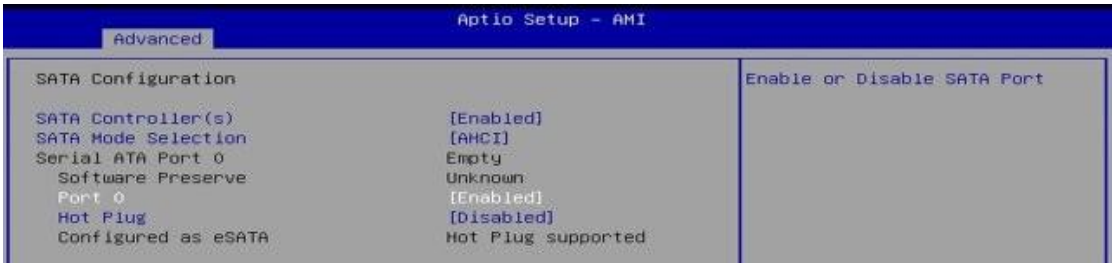
BIOS Setting	Description
Intel SpeedStep	Allows more than two frequency ranges to be supported
Intel Speed Shift Technology	Enable/Disable Intel Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Turbo Mode	Enable/Disable processor Turbo Mode (requires EMTTM enabled too). Auto means enabled.

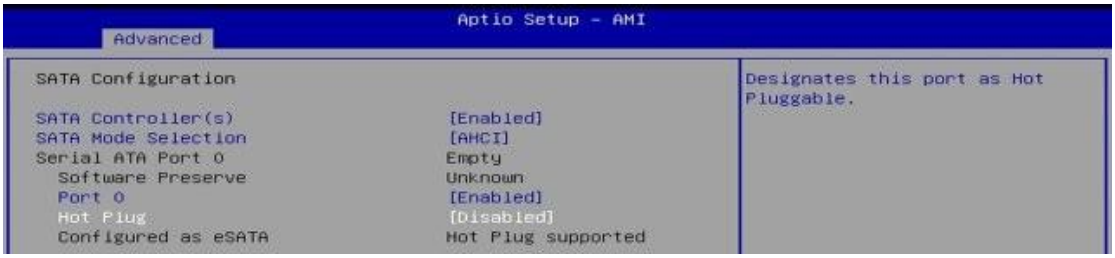
4.4.3 PCH-IO Configuration











4.4.4 PCH-FW Configuration



4.4.5 Trusted Computing



BIOS Setting	Description
Security Device Support	Enables / Disables BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.
SHA256 PCR Bank	Options: Enabled / Disabled
SHA384 PCR Bank	Options: Enabled / Disabled
Pending operation	Schedule an operation for the security device. Note: Your computer will reboot during restart in order to change state of security device.
Platform Hierarchy	Enables / Disables platform hierarchy.
Storage Hierarchy	Enables / Disables storage hierarchy.
Endorsement Hierarchy	Enables / Disables endorsement hierarchy.
Physical Presence Spec Version	Select to tell O.S. to support PPI Spec Version 1.2 or 1.3. Note some HCK tests might not support 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. Auto will support both with the default set to TPM 2.0 devices if not found, TPM 1.2 devices will be enumerated.

4.4.6 LVDS (eDP/DP) Configuration

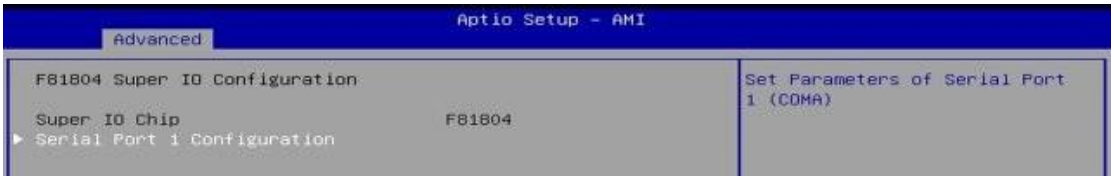


4.4.7 ACPI Settings

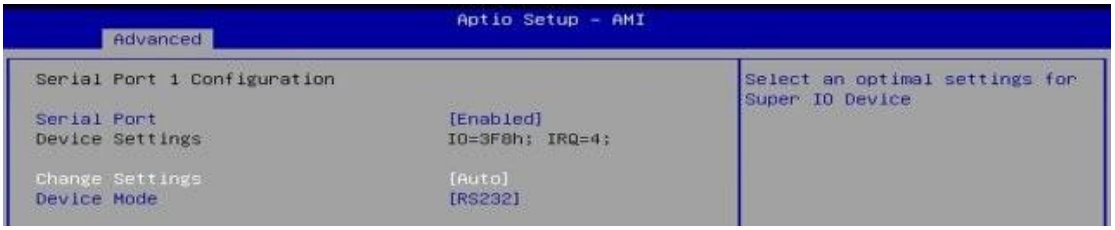


BIOS Setting	Description
Enable Hibernation	Enables / Disables the system ability to hibernate (OS/S4 Sleep State). This option may be not effective with some OS.

4.4.8 F81804 Super IO Configuration









4.4.9 F81804 Hardware Monitor



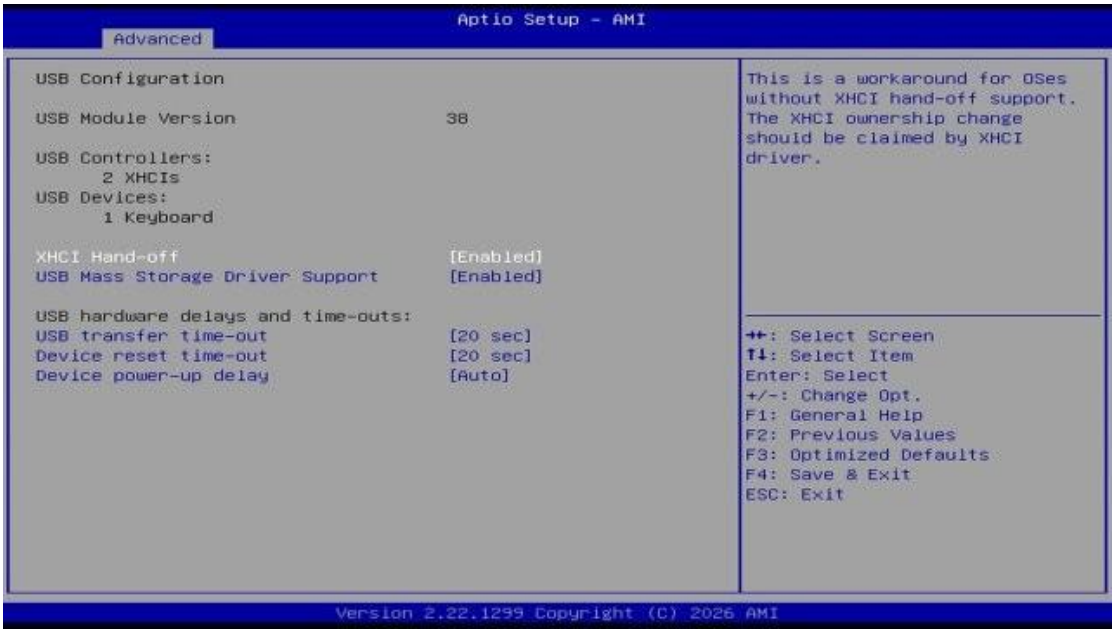


BIOS Setting	Description
Temperatures / Voltages	These fields are the parameters of the hardware monitoring function feature of the motherboard. The values are read-only values as monitored by the system and show the PC health status.

4.4.10 Intel TXT Information

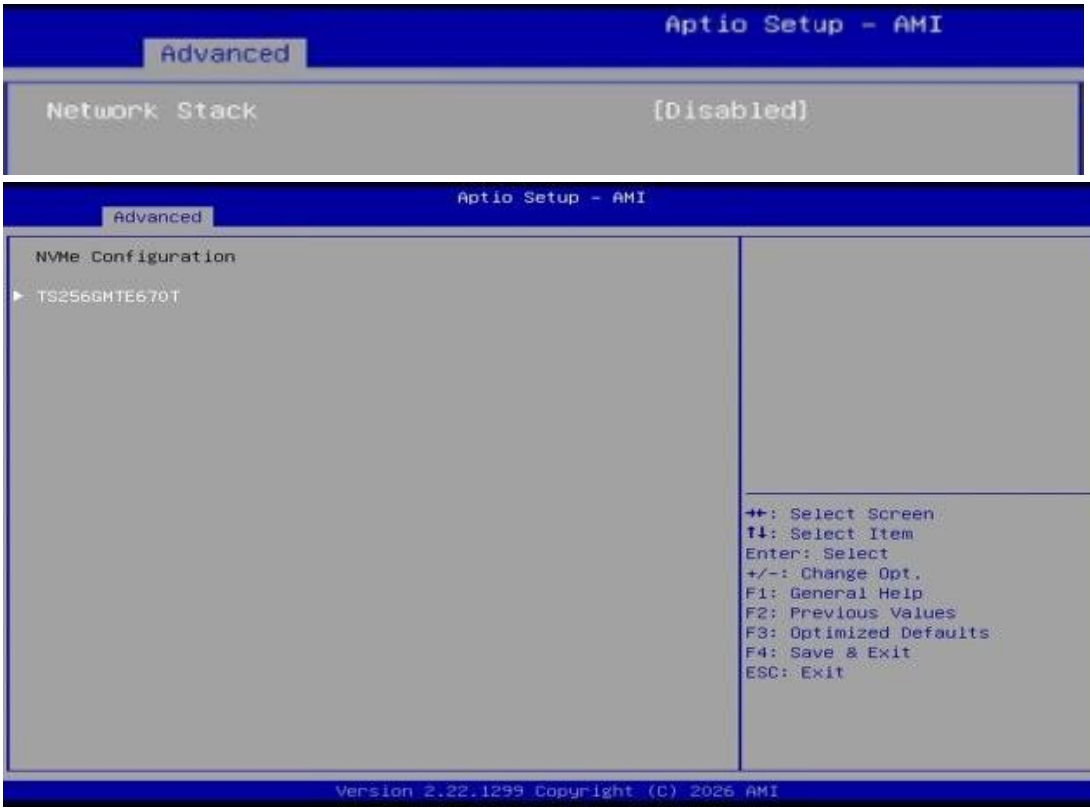


4.4.11 USB Configuration



BIOS Setting	Description
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enables / Disables the support for USB mass storage driver.
USB Transfer time-out	The time-out value (1 / 5 / 10 / 20 secs) for Control, Bulk, and Interrupt transfers.
Device reset time-out	USB mass storage device Start Unit command time-out (10/20/30/40 sec).
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. '**Auto**' uses default value: for a Root port it is 100ms, for a Hub port the delay is taken from Hub descriptor.

4.4.12 Network Stack Configuration



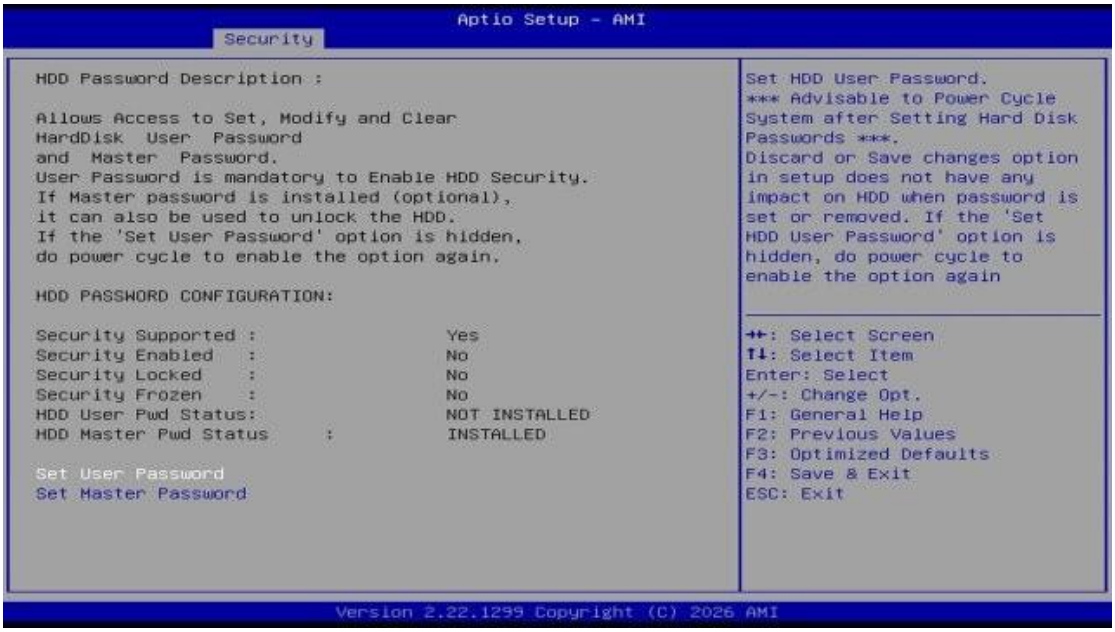
4.4.13 NVMe Configuration

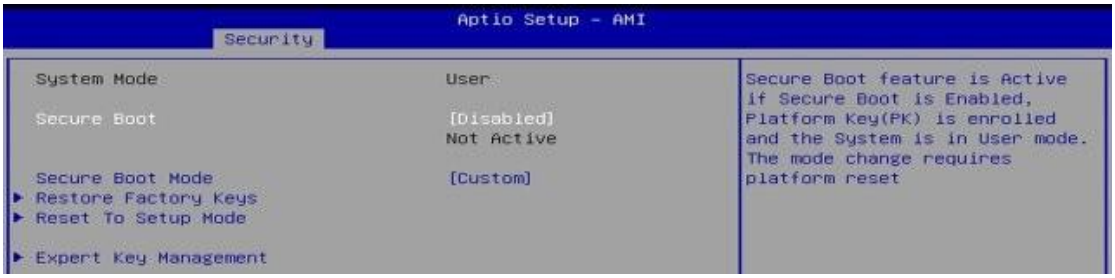


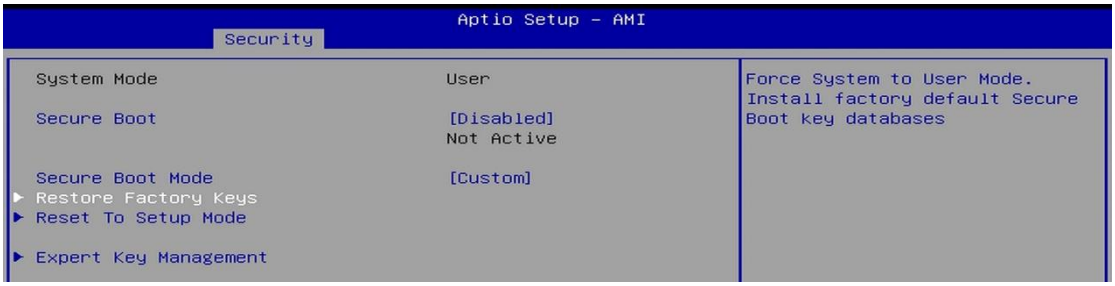
4.5 Security Settings

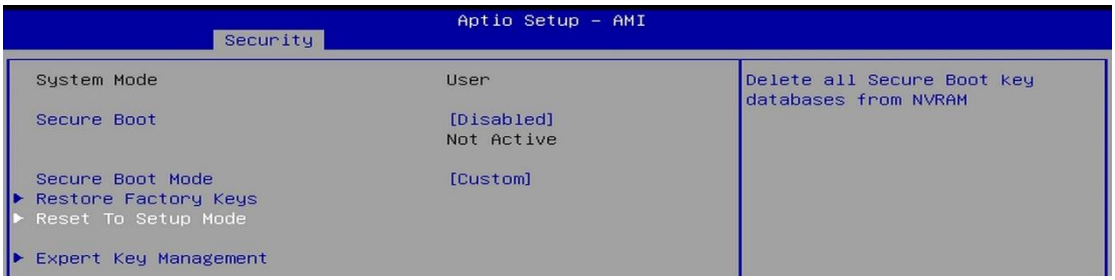


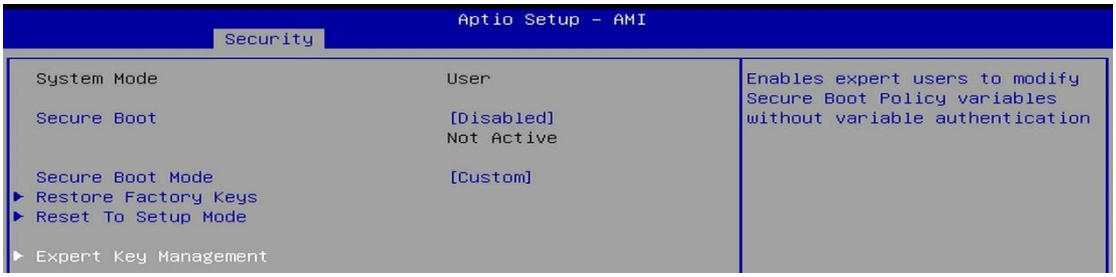
BIOS Setting	Description
Setup Administrator Password	Sets an administrator password for the setup utility.
User Password	Sets a user password.
Secure Boot	Secure Boot feature is Active if Secure Boot is enabled. Platform Key(PK) is enrolled and the system is in user mode. The mode change requires platform reset.
Secure Boot Mode	Secure Boot mode options: Standard or Custom. In Custom mode, Secure Boot Policy variables can be configured by a physically present user without full authentication


Aptio Setup – AMI
Security
HDD Password Description :
Allows Access to Set, Modify and Clear
HardDisk User Password
and Master Password.
User Password is mandatory to Enable HDD Security.
If Master password is installed (optional),
it can also be used to unlock the HDD.
If the 'Set User Password' option is hidden,
do power cycle to enable the option again.
HDD PASSWORD CONFIGURATION:
Security Supported : Yes
Security Enabled : No
Security Locked : No
Security Frozen : No
HDD User Pwd Status: NOT INSTALLED
HDD Master Pwd Status : INSTALLED
Set User Password
Set Master Password
Set HDD User Password.
*** Advisable to Power Cycle
System after Setting Hard Disk
Passwords ***.
Discard or Save changes option
in setup does not have any
impact on HDD when password is
set or removed. If the 'Set
HDD User Password' option is
hidden, do power cycle to
enable the option again
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1299 Copyright (C) 2026 AMI

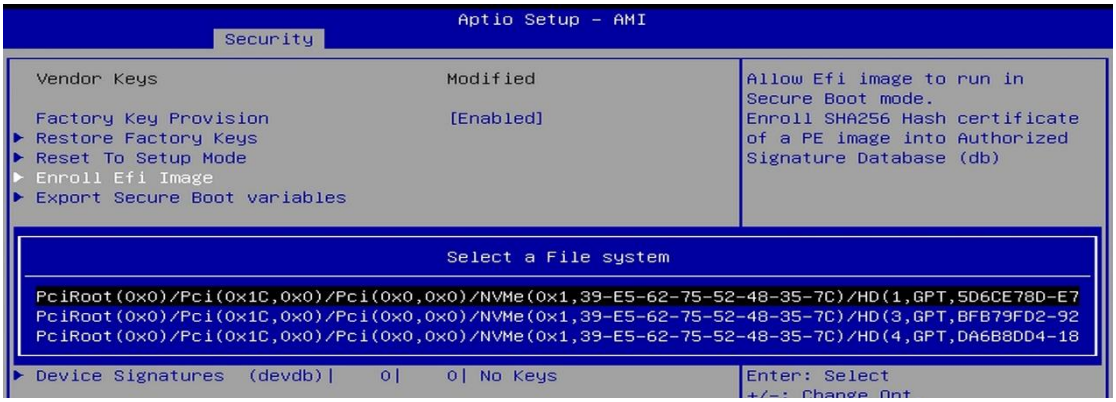

Aptio Setup – AMI
Security
System Mode User
Secure Boot [Disabled]
Not Active
Secure Boot Mode [Custom]
Restore Factory Keys
Reset To Setup Mode
Expert Key Management
Secure Boot feature is Active
if Secure Boot is Enabled,
Platform Key(PK) is enrolled
and the System is in User mode.
The mode change requires
platform reset

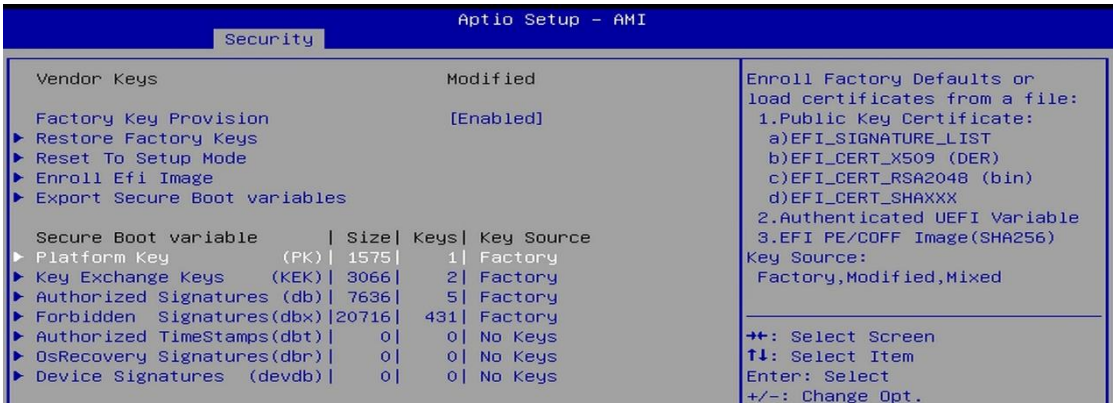

Aptio Setup – AMI
Security
System Mode User
Secure Boot [Disabled]
Not Active
Secure Boot Mode [Custom]
Restore Factory Keys
Reset To Setup Mode
Expert Key Management
Force System to User Mode.
Install factory default Secure
Boot key databases


Aptio Setup – AMI
Security
System Mode User
Secure Boot [Disabled]
Not Active
Secure Boot Mode [Custom]
Restore Factory Keys
Reset To Setup Mode
Expert Key Management
Delete all Secure Boot key
databases from NVRAM


Aptio Setup – AMI
Security
System Mode
User
Secure Boot
[Disabled]
Not Active
Secure Boot Mode
[Custom]
Restore Factory Keys
Reset To Setup Mode
Expert Key Management
Enables expert users to modify Secure Boot Policy variables without variable authentication


Aptio Setup – AMI
Security
Vendor Keys
Modified
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable | Size| Keys| Key Source
Platform Key (PK)| 1575| 1| Factory
Key Exchange Keys (KEK)| 3066| 2| Factory
Authorized Signatures (db)| 7636| 5| Factory
Forbidden Signatures(dbx)|20716| 431| Factory
Authorized TimeStamps(dbt)| 0| 0| No Keys
OsRecovery Signatures(dbr)| 0| 0| No Keys
Device Signatures (devdb)| 0| 0| No Keys
Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.


Aptio Setup – AMI
Security
Vendor Keys
Modified
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Allow Efi image to run in Secure Boot mode.
Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
Select a File system
PciRoot(0x0)/Pci(0x1C,0x0)/Pci(0x0,0x0)/NVMe(0x1,39-E5-62-75-52-48-35-7C)/HD(1,GPT,5D6CE78D-E7
PciRoot(0x0)/Pci(0x1C,0x0)/Pci(0x0,0x0)/NVMe(0x1,39-E5-62-75-52-48-35-7C)/HD(3,GPT,BFB79FD2-92
PciRoot(0x0)/Pci(0x1C,0x0)/Pci(0x0,0x0)/NVMe(0x1,39-E5-62-75-52-48-35-7C)/HD(4,GPT,DA6B8DD4-18
Device Signatures (devdb)| 0| 0| No Keys
Enter: Select


Aptio Setup – AMI
Security
Vendor Keys
Modified
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable | Size| Keys| Key Source
Platform Key (PK)| 1575| 1| Factory
Key Exchange Keys (KEK)| 3066| 2| Factory
Authorized Signatures (db)| 7636| 5| Factory
Forbidden Signatures(dbx)|20716| 431| Factory
Authorized TimeStamps(dbt)| 0| 0| No Keys
OsRecovery Signatures(dbr)| 0| 0| No Keys
Device Signatures (devdb)| 0| 0| No Keys
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,Modified,Mixed
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.

4.6 Boot Settings



BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
FIXED BOOT ORDER Priorities	Sets the system boot order.

4.7 Save & Exit Settings



BIOS Setting	Description
Save Changes and Exit	Exits system setup after saving the changes.
Discard Changes and Exit	Exits system setup without saving any changes.
Save Changes and Reset	Resets the system after saving the changes.
Discard Changes and Reset	Resets system setup without saving any changes.
Save Changes	Saves changes done so far to any of the setup options.
Discard Changes	Discards changes done so far to any of the setup options.
Restore Defaults	Restores / Loads defaults values for all the setup options.
Save as User Defaults	Saves the changes done so far as User Defaults.
Restore User Defaults	Restores the user defaults to all the setup options.

Appendix

This chapter introduces Hardware Resources including:

1. I/O
2. IRQs

A. I/O Port Address Map

Address	Device Description
0x0000EFA0-0x0000EFBF	Motherboard resources
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x00000290-0x0000029F	Motherboard resources
0x0000002E-0x0000002F	Motherboard resources
0x0000004E-0x0000004F	Motherboard resources
0x00000061-0x00000061	Motherboard resources
0x00000063-0x00000063	Motherboard resources
0x00000065-0x00000065	Motherboard resources
0x00000067-0x00000067	Motherboard resources
0x00000070-0x00000070	Motherboard resources
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
0x000000B2-0x000000B3	Intel(R) SMBus Controller - E422
0x00000680-0x0000069F	System timer
0x0000164E-0x0000164F	System timer
0x00000020-0x00000021	Communications Port (COM1)
0x00000024-0x00000025	Communications Port (COM2)
0x00000028-0x00000029	Motherboard resources
0x0000002C-0x0000002D	PCI Express Root Complex
0x00000030-0x00000031	PCI Express Root Complex
0x00000034-0x00000035	Motherboard resources
0x00000038-0x00000039	Programmable interrupt controller
0x0000003C-0x0000003D	Programmable interrupt controller
0x000000A0-0x000000A1	Programmable interrupt controller
0x000000A4-0x000000A5	Programmable interrupt controller
0x000000A8-0x000000A9	Programmable interrupt controller
0x000000AC-0x000000AD	Programmable interrupt controller
0x000000B0-0x000000B1	Programmable interrupt controller
0x000000B4-0x000000B5	Programmable interrupt controller
0x000000B8-0x000000B9	Programmable interrupt controller
0x000000BC-0x000000BD	Programmable interrupt controller
0x000004D0-0x000004D1	Programmable interrupt controller
0x000003F8-0x000003FF	Programmable interrupt controller
0x00000000-0x00000CF7	Programmable interrupt controller
0x00000D00-0x0000FFFF	Programmable interrupt controller
0x00000040-0x00000043	Programmable interrupt controller
0x00000050-0x00000053	Programmable interrupt controller
0x00002000-0x000020FE	Programmable interrupt controller
0x00003000-0x00003FFF	Standard PS/2 Keyboard
0x00003F00-0x00003FFF	Standard PS/2 Keyboard
0x00001854-0x00001857	Intel(R) Active Management Technology - SOL (COM3)

B. Interrupt Request Lines (IRQ)

Peripheral devices use interrupt request lines to notify CPU for the service required. The following table shows the IRQ used by the devices on board.

Level	Function
IRQ 0	System timer
IRQ 4	Communications Port (COM1)
IRQ 14	Intel(R) Serial IO GPIO Host Controller - INTC1083
IRQ 16	High Definition Audio Controller
IRQ 55-204	Microsoft ACPI-Compliant System
IRQ 256-511	Microsoft ACPI-Compliant System
IRQ 4294967293-94	PCI Express Root Port
IRQ 4294967273	Intel(R) Graphics
IRQ 4294967253-55	Intel(R) Wi-Fi 6E AX210 160MHz #2
IRQ 4294967275	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967272	Intel(R) AI Boost
IRQ 4294967277-91	Standard NVM Express Controller
IRQ 4294967292	PCI Express Root Port
IRQ 4294967274	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967276	Intel(R) Management Engine Interface #1
IRQ 4294967256-71	Realtek Gaming 2.5GbE Family Controller