SI-663-N

12th Gen Intel® Core™ Processor Fanless Signage Player with HDMI / DP / DVI-D

User's Manual

Version 1.0
(May 2024)

iBASE

Copyright

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 arising 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

In a domestic environment, this product may cause radio interference in which case users may be required to take adequate measures.

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 Restriction of Hazardous Substances (RoHS) 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).

- Lead (Pb)
- Mercury (Hg)
- Cadmium (Cd)
- Hexavalent chromium (Cr6+)
- Polybrominated biphenyls (PBB)
- Polybrominated diphenyl ether (PBDE)

iBASE

Important Safety Information

Carefully read the precautions before using the device.

Environmental conditions:

- Lay the device horizontally on a stable and solid surface in case the device may fall, causing serious 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.
- Use this product in environments with ambient temperatures between 0˚C and 45˚C.
- DO NOT LEAVE THIS DEVICE IN AN ENVIRONMENT WHERE THE STORAGE TEMPERATURE MAY FALL BELOW -20° C OR RISE ABOVE 80° C. This could damage the device. The device must be used in a controlled environment.

Care for your IBASE products:

- Before cleaning the device, turn it off and unplug all cables such as power in case a small amount of electrical current may still flow.
- 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 place heavy objects on the top of the device.
- Operate this device using 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 products plugged into the extension cord does not exceed the cord's limits.

Avoid Disassembly

Do not disassemble, repair or make any modification to the device. Doing so could generate hazards and cause damage to the device, even bodily injury or property damage, and will void any warranty.

CAUTION

There is danger of explosion if internal lithium-ion battery is replaced by an incorrect type. Only replace with the same or 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, CPU cooler, memory, storage devices, power adapter, panel and touchscreen.

* PRODUCTS, HOWEVER, 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 about your product and elaborate upon the problem.

   - Product model name
   - Product serial number
   - Detailed description of the problem
   - The error messages in text or in screenshots if there is 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, visit the eRMA page in the IBASE's website and follow the instructions to obtain RMA authorization or contact your distributor / sales representative for assistance.

iBASE

Table of Contents

Chapter 1 General Information 1

1.1 Introduction 2
1.2 Features 2
1.3 Packing List 3
1.4 Specifications 3
1.5 Product View 5
1.6 Dimensions 7

Chapter 2 Hardware Installation & Motherboard Information 8

2.1 Installation / Replacement 9
2.1.1 Memory 12
2.1.2 Mini-PCIe & M.2 Cards 13
2.1.3 WiFi / 3G / 4G Antenna Installation 13
2.2 Setting the Jumpers 14
2.3 Motherboard Dimensions 15
2.4 Jumper & Connector Locations 16
2.4.1 Jumper Quick Reference 17
2.4.2 Sierra EM9191 5G Card USB/PCIe Select (JP1) 17
2.4.3 Clear ME Contents (JP3) 18
2.4.4 Clear CMOS Contents (JP4) 19
2.4.5 ATX & AT Power Mode Selection (JP5) 20
2.4.6 Flash Descriptor Security Override(J6) 21
2.4.7 PWM Programming (J7) 22
2.4.8 Connector Quick Reference 23
2.4.9 2.5 Gigabit LAN (Intel I226-LM) (CN1) 24
2.4.10 DisplayPort (CN2) 24
2.4.11 HDMI Connector (CN3) 25
2.4.12 DVI-D Connector (CN4) 25
2.4.13 DC_IN Connector (CN5) 26
2.4.14 USB 3.2 Connector (CN6, CN7, CN8) 26
2.4.15 USB 2.0 Connector (CN9) 27
2.4.16 COM1 Ports (CN10) 28
2.4.17 Front Panel Connector (JP2) 29
2.4.18 DDR5 SO-DIMM Slot (J5 / J13) 30
2.4.19 80 Port Debug (J8) 31
2.4.20 M.2 M2280 Slot (J3) 31
2.4.21 M.2 E2230 Slot (J12) 32

2.4.22 SPI Flash Connector (J11) 32
2.4.23 SIM Slot (J15).....33
2.4.24 M.2 B-key 3052 Slot (J14) 33
2.4.25 Fan Power Connectors (CPU_FAN1, SYS_FAN1) 34

Chapter 3 Driver Installation 35

3.1 Introduction 36
3.2 Intel® Chipset Software Installation Utility 36
3.3 VGA Driver Installation.....37
3.4 Realtek HD Audio Driver Installation 39
3.5 LAN Drivers Installation.....41
3.6 Intel® Management Engine Components Drivers Installation.....43
3.7 Intel® Serial I/O Drivers Installation.....44
3.8 Intel® Thunderbolt Drivers Installation 45

Chapter 4 BIOS Setup 47

4.1 Introduction 48
4.2 BIOS Setup.....48
4.3 Main Settings 49
4.4 Advanced Settings 49
4.5 Chipset Settings.....61
4.6 Security Settings 65
4.7 Boot Settings.....67
4.8 Save & Exit Settings.....68
4.9 MEBx 69

Appendix 70

A. I/O Port Address Map.....71
B. Interrupt Request Lines (IRQ) 74

Chapter 1
General Information

The information provided in this chapter includes:

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

1.1 Introduction

Introducing the SI-663-N, a cutting-edge 12th Gen Intel® Core™ Processor Fanless Signage Player from IBASE. Equipped with Intel® SoC Integrated Graphics, this powerhouse boasts unrivaled performance for dynamic signage applications. Featuring iSMART intelligent energy-saving technology, it facilitates seamless power on/off scheduling and power resume functions, ensuring optimal energy efficiency. Supporting 12th Gen Intel® Core™ processors, it delivers fast processing power for demanding tasks. With versatile connectivity options including 1x HDMI 2.0, 1x DP++ 1.4, and 1x DVI-D, alongside 2x DDR5-4800 SO-DIMM slots for a maximum of 64GB RAM, this signage player offers unparalleled versatility. Additionally, it comes equipped with TPM 2.0, vPro, and a watchdog timer for enhanced security and reliability. Designed with industrial-grade robustness and a compact, fanless form factor, the SI-663-N ensures seamless operation in diverse environments, making it the ultimate solution for signage applications requiring reliability, performance, and flexibility.

1.2 Features

- iSMART intelligent energy-saving technology - enables power on/off scheduling and power resume functions
- Supports 12th Gen Intel® Core™ processors
- 1x HDMI 2.0 / 1x DP++ 1.4 / 1x DVI-D
- 2x DDR5-4800 SO-DIMM, dual channel, Max. 64GB
- 1x M.2 B-Key (3052) for 5G connectivity
- 1x M.2 E-Key (2230) for WiFi, Bluetooth or capture card options
- TPM 2.0, vPro and watchdog timer
- Industrial-grade robust, fanless and compact design

1.3 Packing List

Your product package should include the items listed below. If any of the items below is missing, contact the distributor or the dealer from whom you purchased the product.

- SI-663-N Digital Signage Player
- Power Adapter
- Power Cord

1.4 Specifications

Product	SI-663-N
System	
Mainboard	MBD663
CPU	12th Gen Intel® Core™ series (Alder Lake PS) processor TDP<=28W
CPU Socket	LGA1700
Chipset	Integrated
Memory	2x DDR5 4800 SODIMM / Max. = 64GB (ECC not supported)
Graphics	Intel® Iris® Xe Graphics, up to 96EU
LAN Controller	1x Gigabit LAN (Isolation/PXE support) (Intel® 226LM 2.5Gb with Wake-on-Lan)
Expansion Slots	1x M.2 E-Key (2230) (WiFi-6E support) (2x PCI-E x1, USB 2.0) 1x M.2 B-Key (3052) (PCI-E x1; USB 2.0, USB 3.x) (supports Sierra LTE module) 1x UIM / SIM card slot 1x M.2 M-Key (2280) (PCIE4.0 X4) 1x M.2 NVMe (PCI-E 4.0 x4 / SATA)
I/O Interface	1x HDMI 2.0 / 1x DP++ 1.4 / 1x DVI-D 3x USB 3.2 (USB Type-A) 1x USB 2.0 (USB Type-A) 1x RJ45 for Gigabit LAN 1x DB9 for RS232 serial port 2x Audio connectors for Line in/Line out 1x Power button 1x Power switch connector 1x Power jack (+12V DC) 2x LED for power & storage
Storage	1x M.2 M-key (2280)

Watchdog	Watchdog Timer: 256 segments, 0, 1, 2…255 (sec)
Power Requirement	+12V DC
Construction	Aluminum + SGCC
Chassis Color	Black & White
Power Supply	84W power adaptor
Mounting	Standard system bracket
Dimensions (W x H x D)	175mm(W) x 212mm(D) x 37mm(H)
Certificate	CE, FCC Class-B, cULus & CCC
Operating System	Windows 10 IoT Enterprise RS5(64-bit) Linux Ubuntu(64-bit)
Environment	
Temperature	• Operating: 0 ~ 45 °C (32 ~ 113 °F) • Storage: -20 ~ 80 °C (-4 ~ 176 °F)
Relative Humidity	5 ~ 90% at 45 °C (non-condensing)
Vibration Protection	M.2: random operation 5 grms, 5~500 Hz

All specifications are subject to change without prior notice.

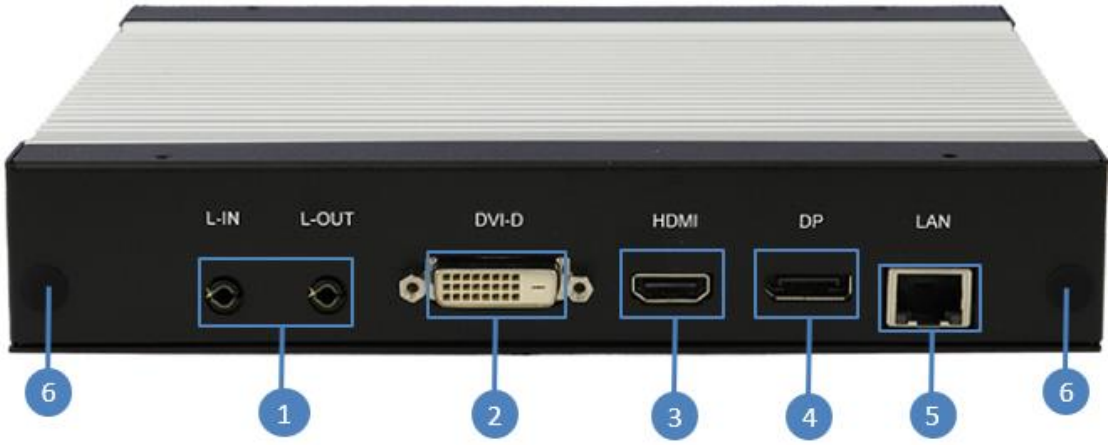
Note: The product performance relies on the system functioning as a whole. The level of CPU/APU/GPU processor, the interaction among the processor and the memory and storage bandwidth, or the functionality of the digital signage application software may affect the product performance.

1.5 Product View

Front View

No.	Function	No.	Function
1	DC-in Connector	5	Power Button
2	USB Ports	6	Power LED
3	COM Port	7	Extension Power Button
4	HDD Status LED	8	Antenna Holes

Rear View

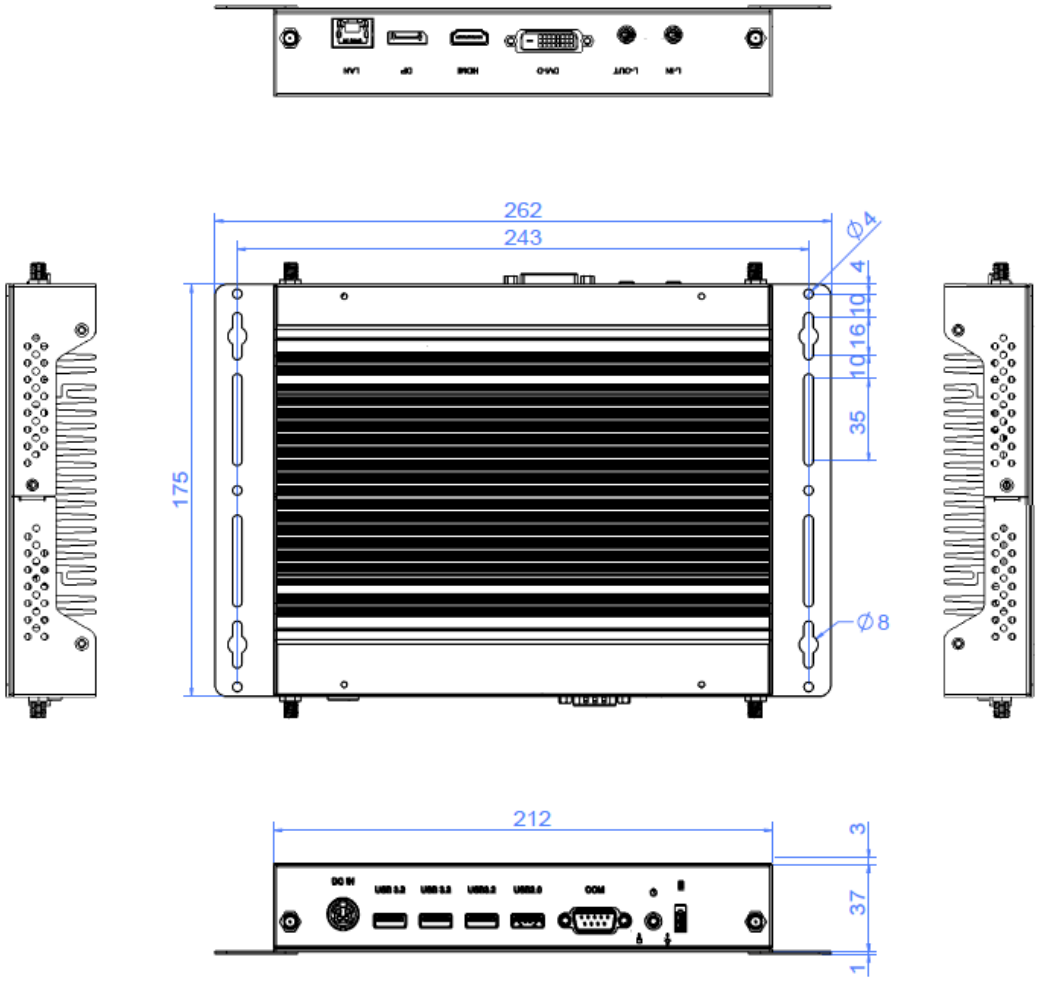


No.	Function	No.	Function
1	Line-in and Line-out	4	DP Port
2	DVI-D Port	5	LAN Port
3	HDMI Port	6	Antenna Holes

Oblique View

1.6 Dimensions

Unit: mm



Chapter 2
Hardware Installation & Motherboard Information

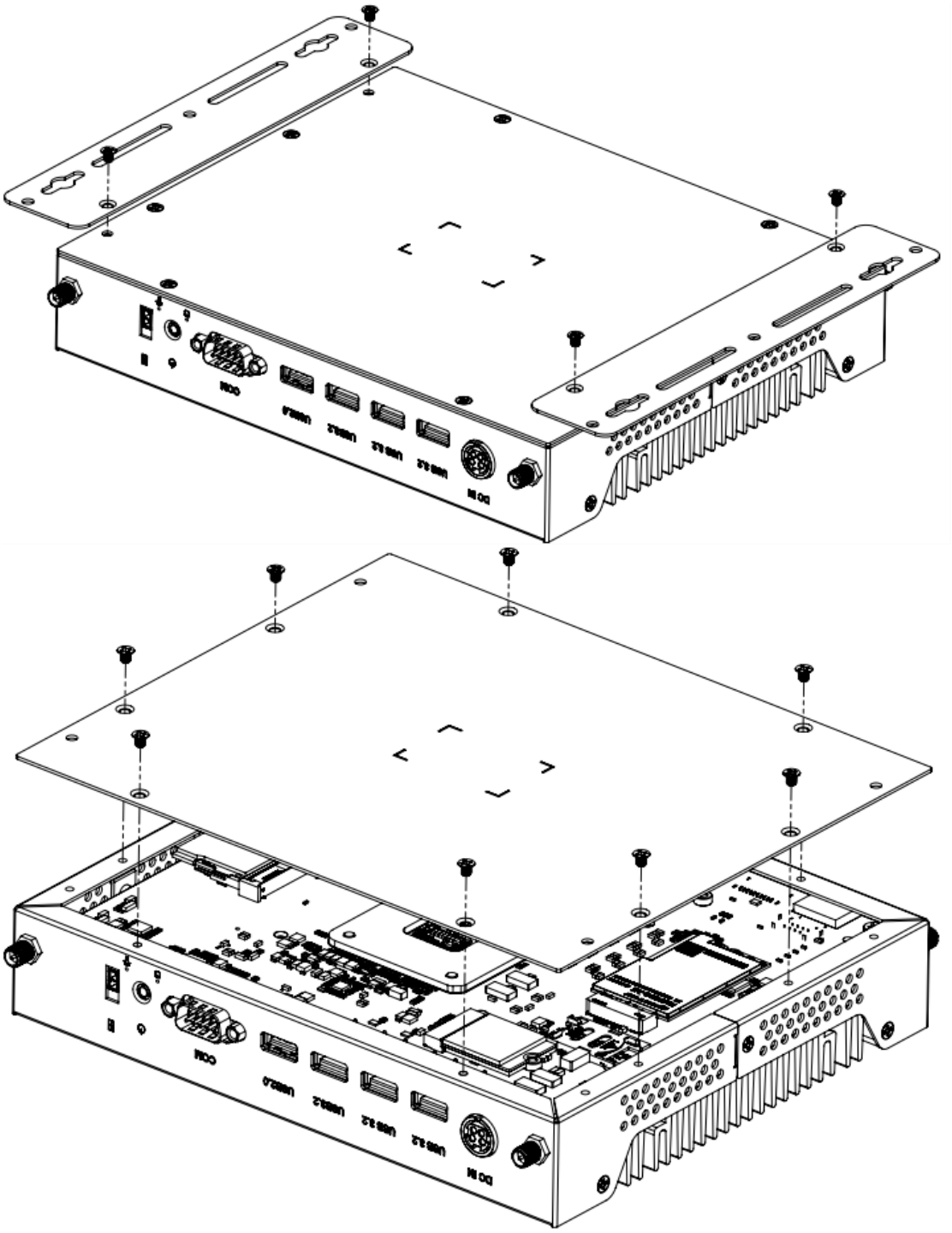
The information provided in this chapter includes:

- Installation /Replacement
- Jumpers and Connectors

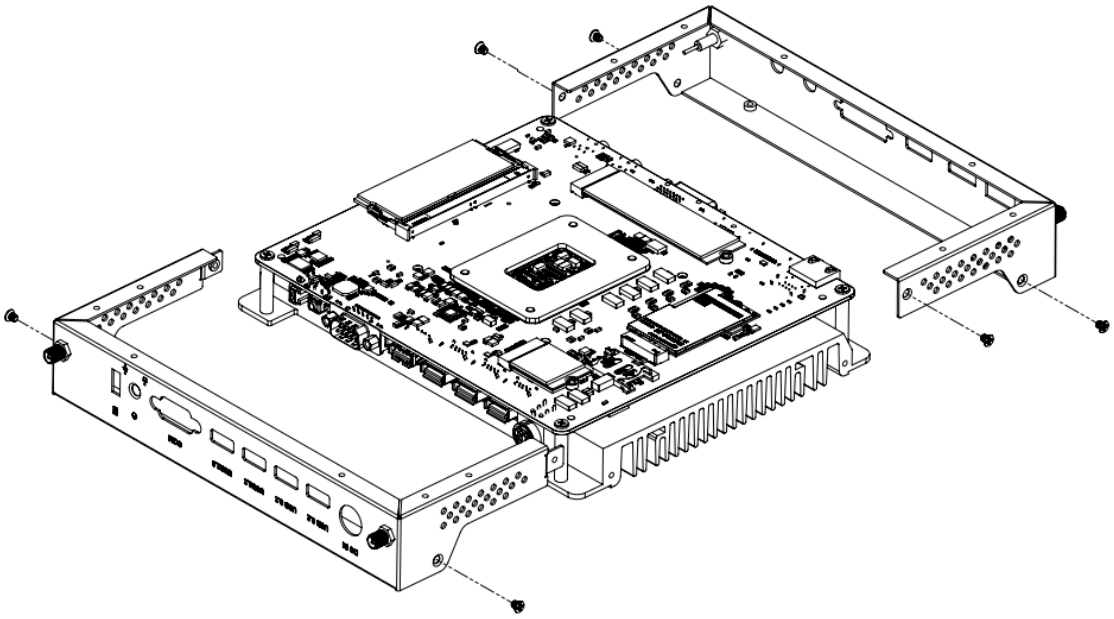
2.1 Installation / Replacement

The following pictures show how to disassemble the SI-663-N.

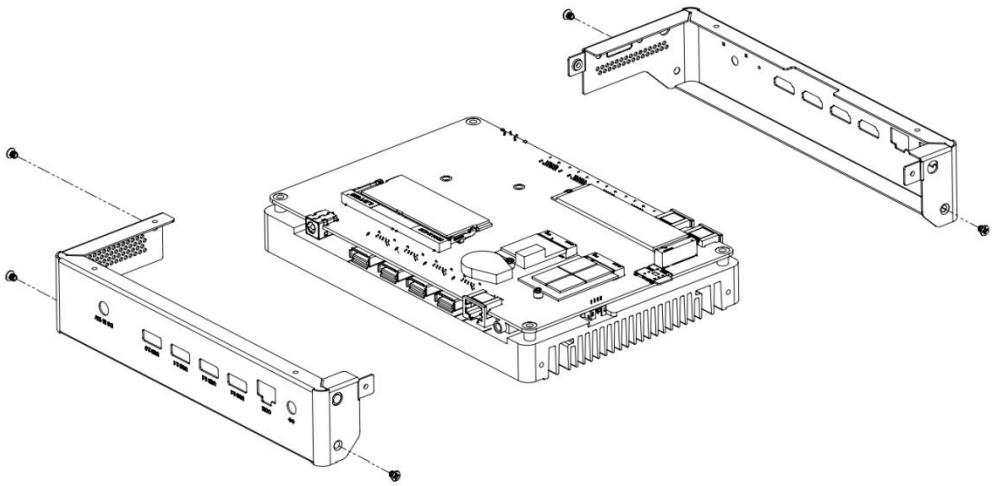
1. Remove the bracket screws and then the cover plate screws as shown below.



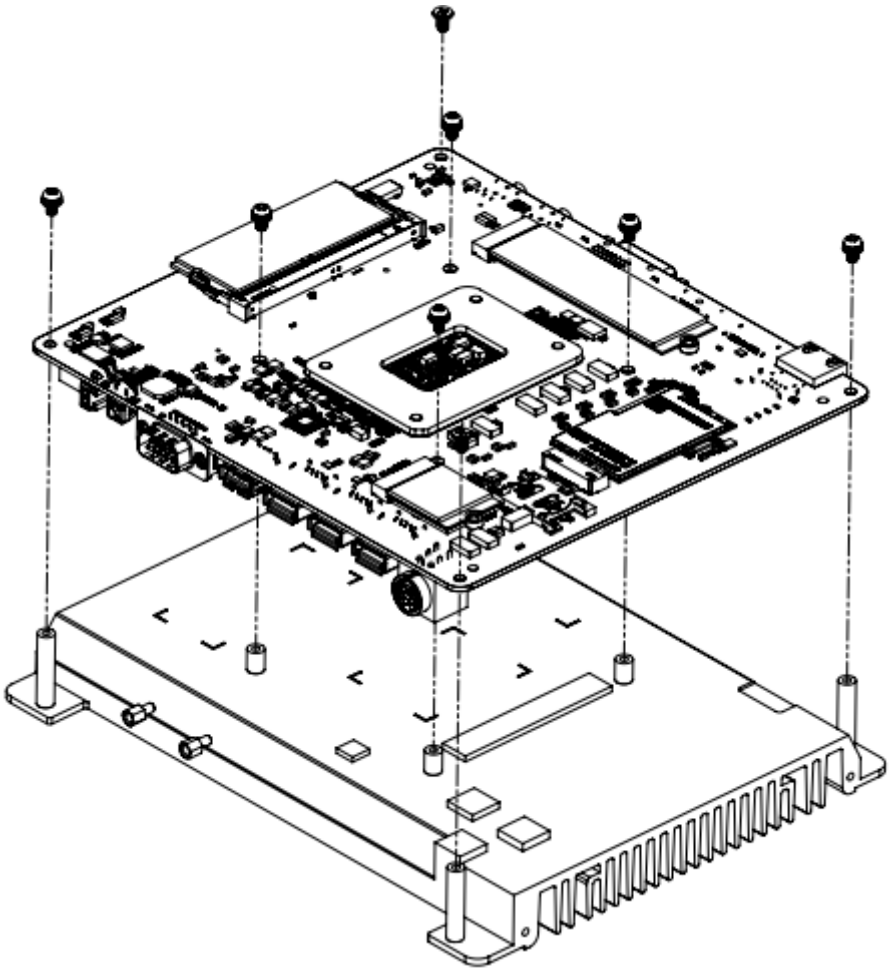
2. Remove the side plate by releasing the screws and chassis-side brackets shown below.



3. Remove the I/O connector cover plates by releasing the five (5) screws shown below.

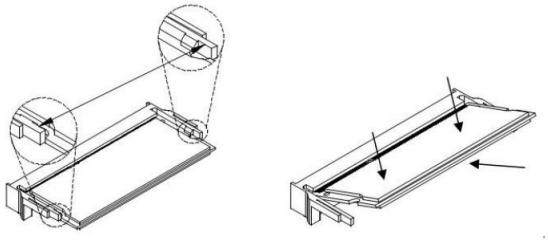


4. Separate the system board from the base heat sink by releasing the seven (7) screws shown below.



2.1.1 Memory

To install the modules, locate the memory slot on the motherboard.
The MBD663 supports two DDR5 memory sockets. To install the modules, locate the memory slot on the board and perform the following steps:



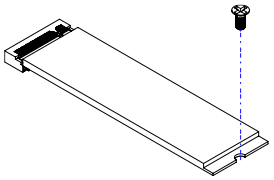
1. Align the key of the memory module with that on the memory slot and insert the module slantwise.
2. Gently push the module in an upright position until the clips of the slot close to hold the module in place when the module touches the bottom of the slot.
3. To remove the module, press the ejector tabs outwards with your fingertips to eject the module.

2.1.2 Mini-PCIe & M.2 Cards

1. Locate the M.2 slot inside the device.

2. Align the key of the M.2 card to the interface, and insert the card slantwise.
3. Fix the M.2 card with an M3 screw.

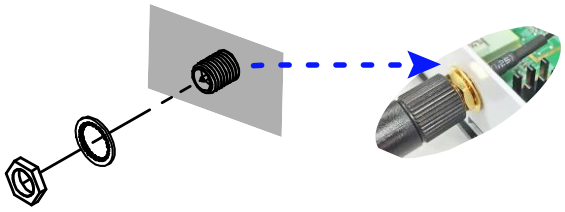
M.2:



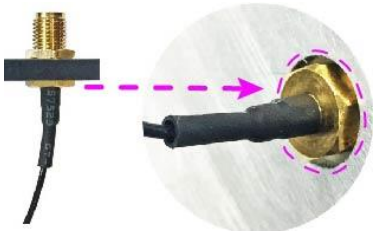
2.1.3 WiFi / 3G / 4G Antenna Installation

Thread the WiFi / 3G / 4G antenna extension cable through an antenna hole of the front I/O cover and fasten the antenna as shown below. Then apply adhesive to the edge of the hex nut behind the front I/O cover to prevent the extension cable from falling if the cable becomes loose.

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



2. Apply adhesive around here.



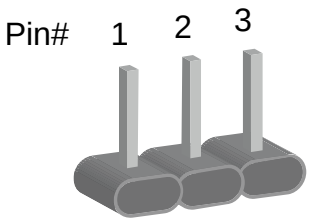
Info: The diameter of the nut is around 6.35 mm (0.25”-36UNC).

2.2 Setting the Jumpers

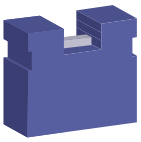
Set up and configure your SI-663-N by using jumpers for various settings and features according to your needs and applications. Contact your supplier if you have doubts about the best configuration for your use.

2.2.1 How to Set Jumpers

Jumpers are short-length conductors consisting of several metal pins with a non-conductive base mounted on the circuit board. Jumper caps are used to have the functions and features enabled or disabled. If a jumper has 3 pins, you can connect either PIN1 to PIN2 or PIN2 to PIN3 by shorting.

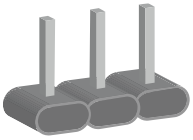
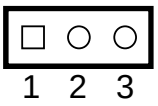
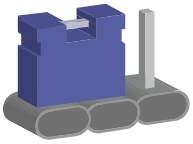
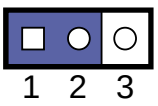
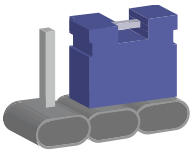
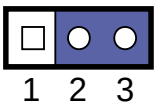


A 3-pin jumper



A jumper cap

Refer to the illustration below to set jumpers.

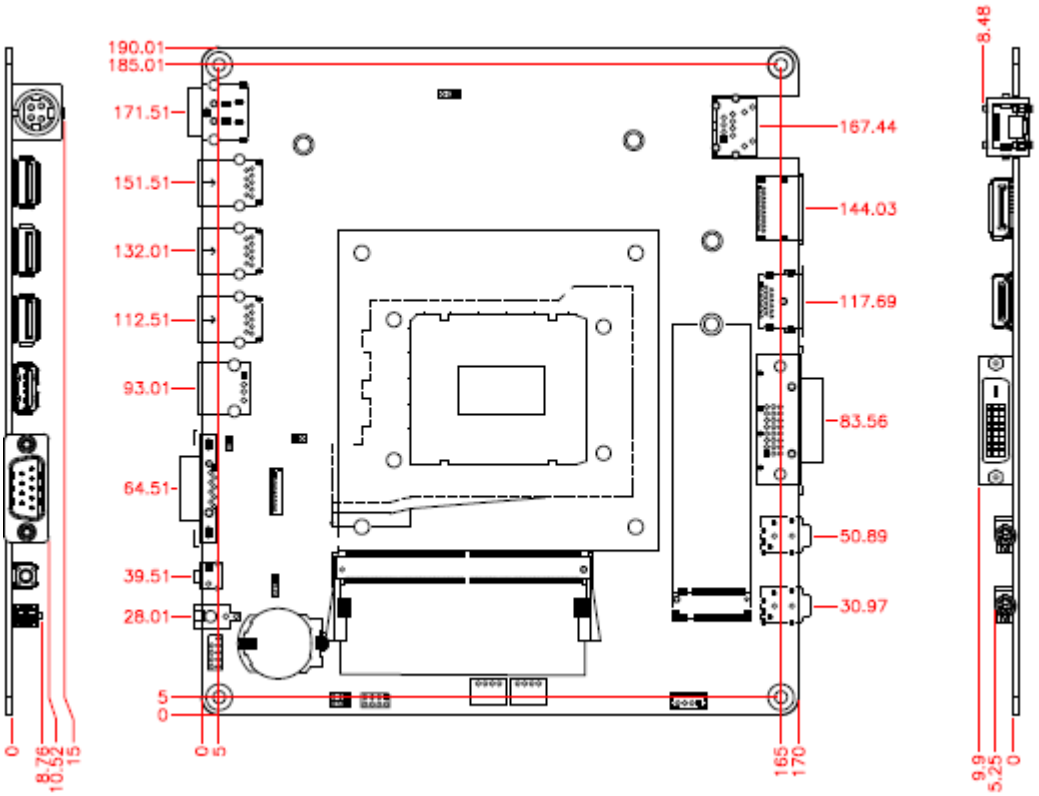
Pin closed	Oblique view	Illustration
Open		
1-2		
2-3		

When two pins of a jumper are encased in a jumper cap, this jumper is **closed**, i.e. turned **On**.

When a jumper cap is removed from two jumper pins, this jumper is **open**, i.e. turned **Off**.

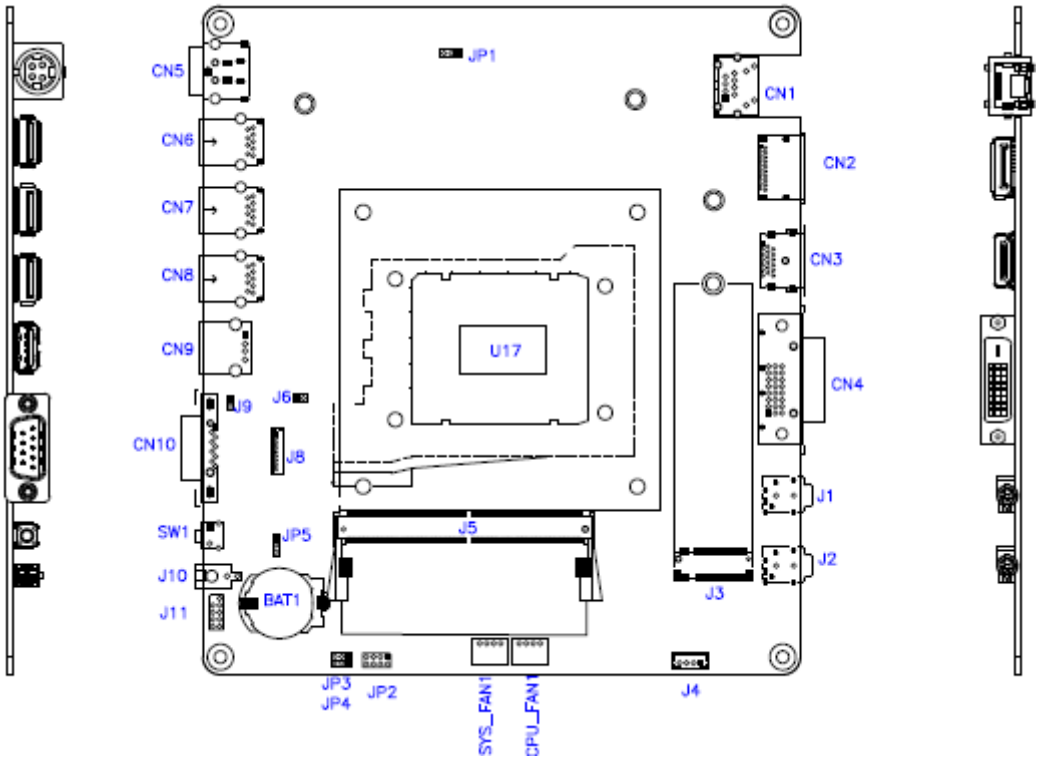
2.3 Motherboard Dimensions

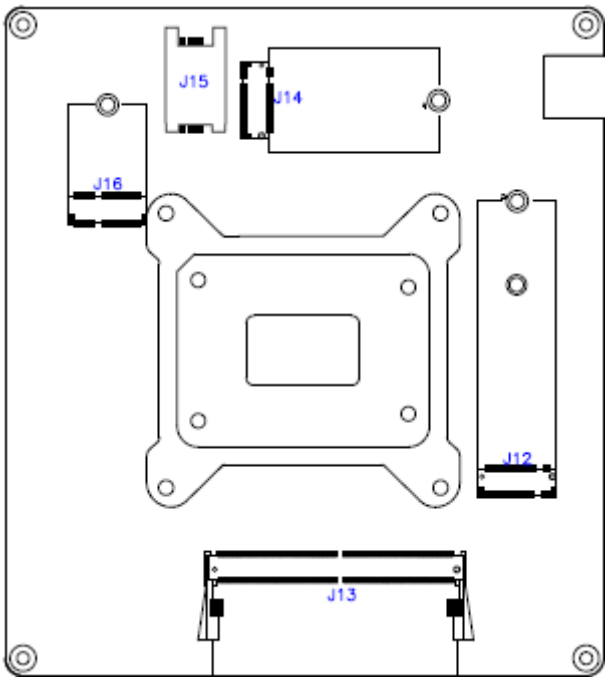
Motherboard: MBD663



2.4 Jumper & Connector Locations

Motherboard: MBD663

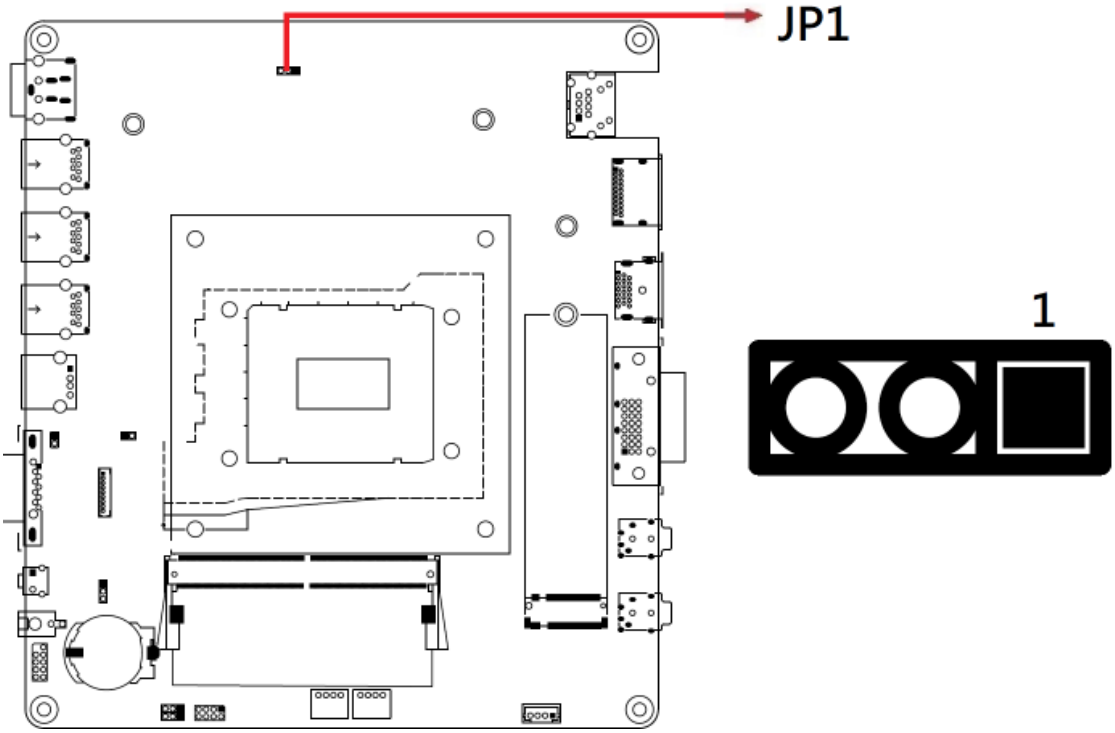




2.4.1 Jumper Quick Reference

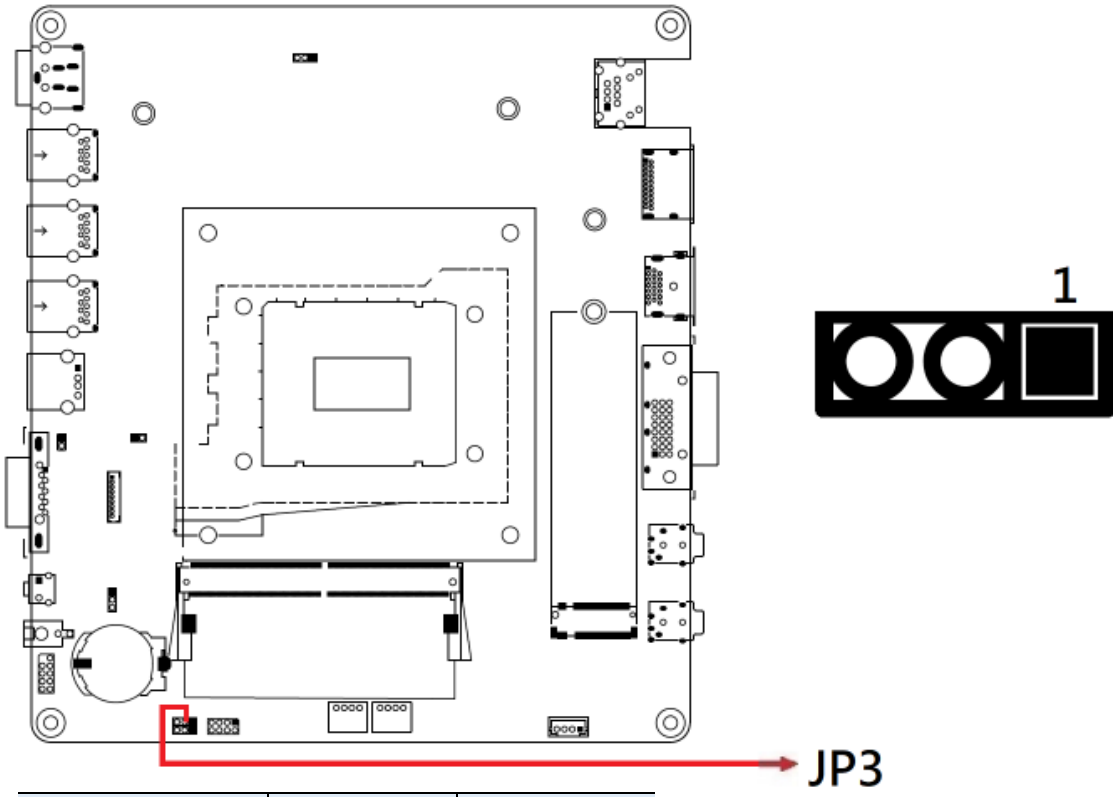
Jumper	Function
JP1	Sierra EM919x 5G card USB/PCIe Select
JP3	Clear ME
JP4	Clear CMOS
JP5	AT/ATX Select
J6	Flash Descriptor Security Override
J7	PWM Programming

2.4.2 Sierra EM9191 5G Card USB/PCIe Select (JP1)



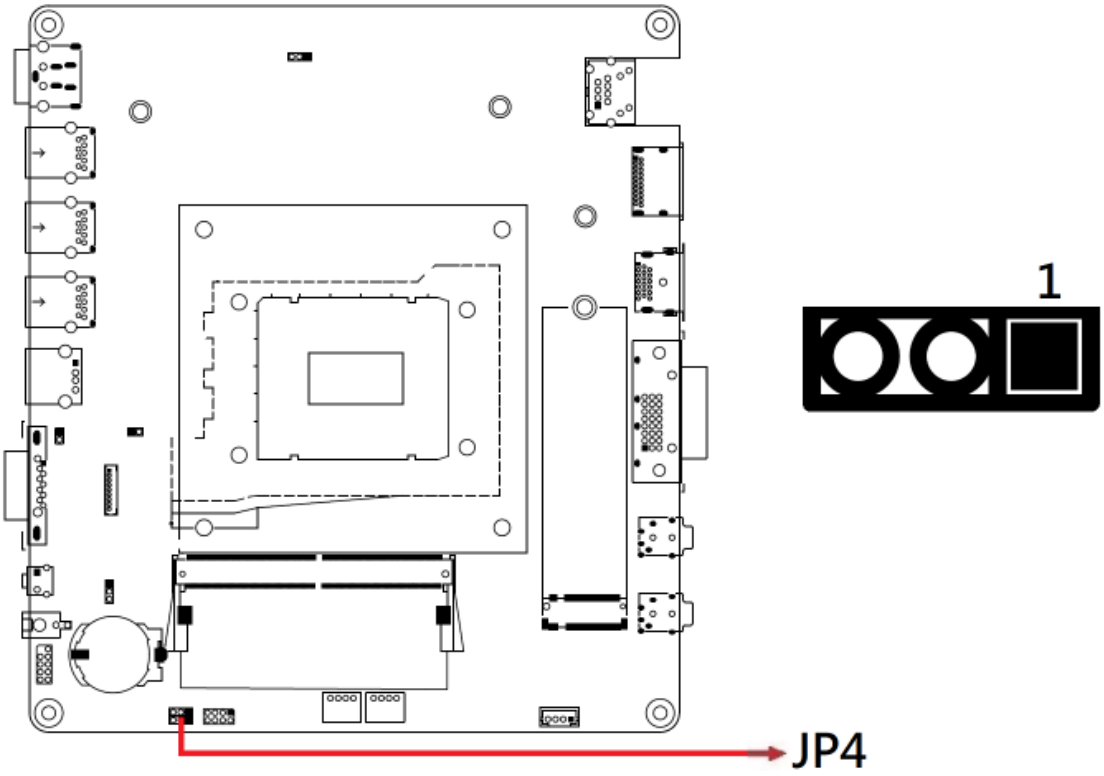
Function	Pin closed	Illustration
USB	1-2	
PCIe (default)	2-3	

2.4.3 Clear ME Contents (JP3)



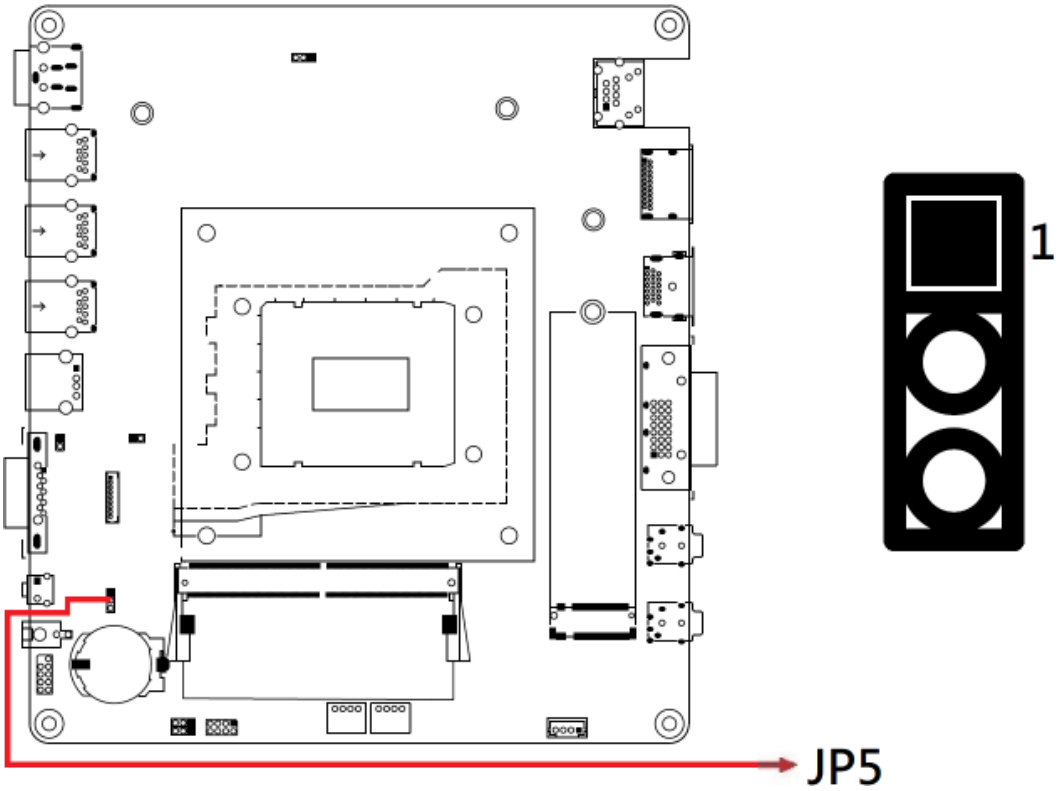
Function	Pin closed	Illustration
Normal(default)	1-2	
Clear ME	2-3	

2.4.4 Clear CMOS Contents (JP4)



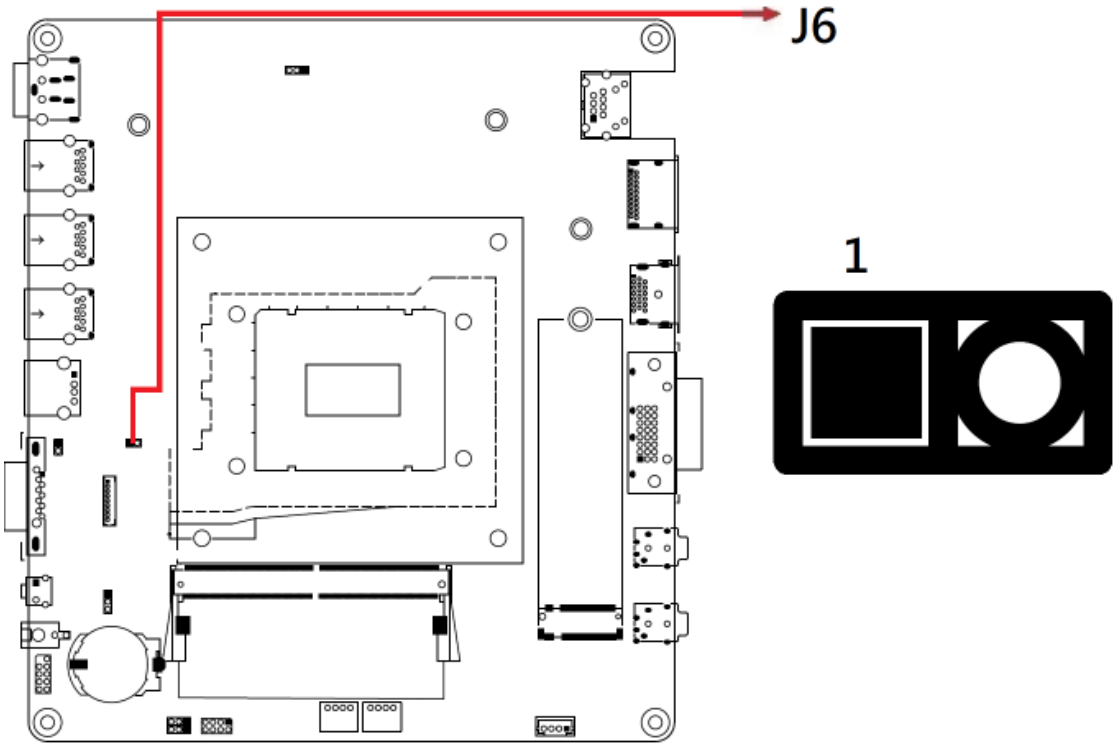
Function	Pin closed	Illustration
Normal(default)	1-2	
Clear CMOS	2-3	

2.4.5 ATX & AT Power Mode Selection (JP5)



Function	Pin closed	Illustration
ATX (default)	1-2	
AT	2-3	

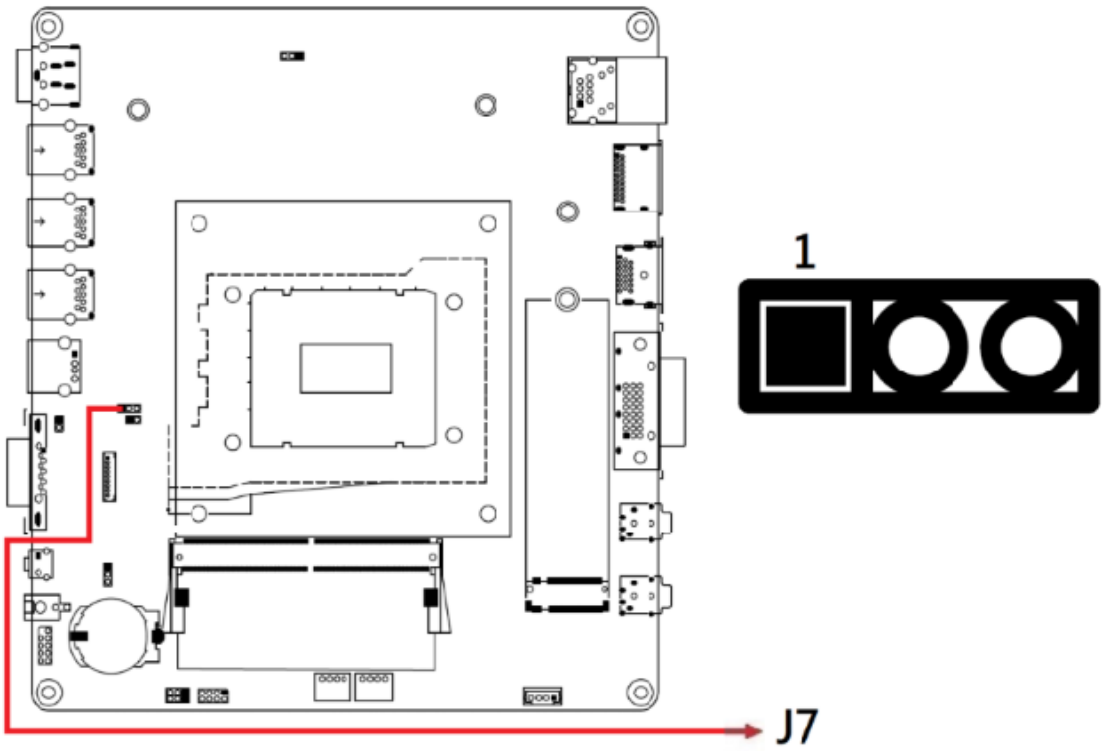
2.4.6 Flash Descriptor Security Override(J6)



Flash Descriptor Security Override	Pin	Illustration
Disabled (default)	Open	1
Enabled	Close	1

Note: J6 is for factory use only.

2.4.7 PWM Programming (J7)

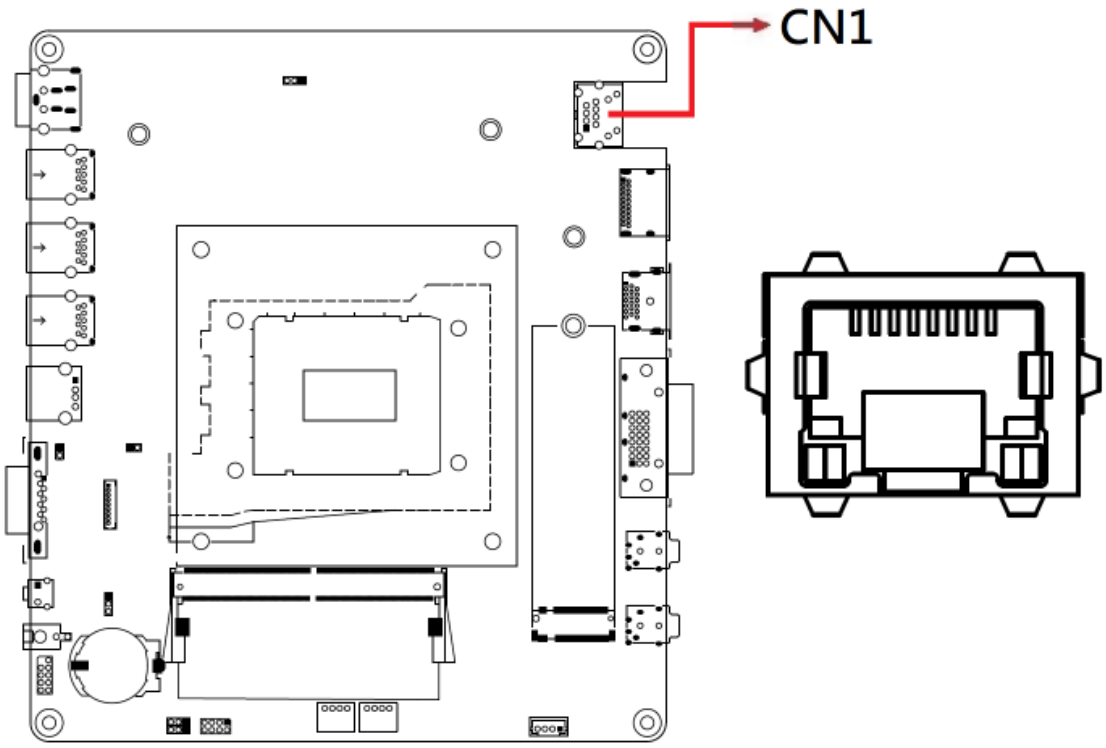


Note: J7 is for factory use only.

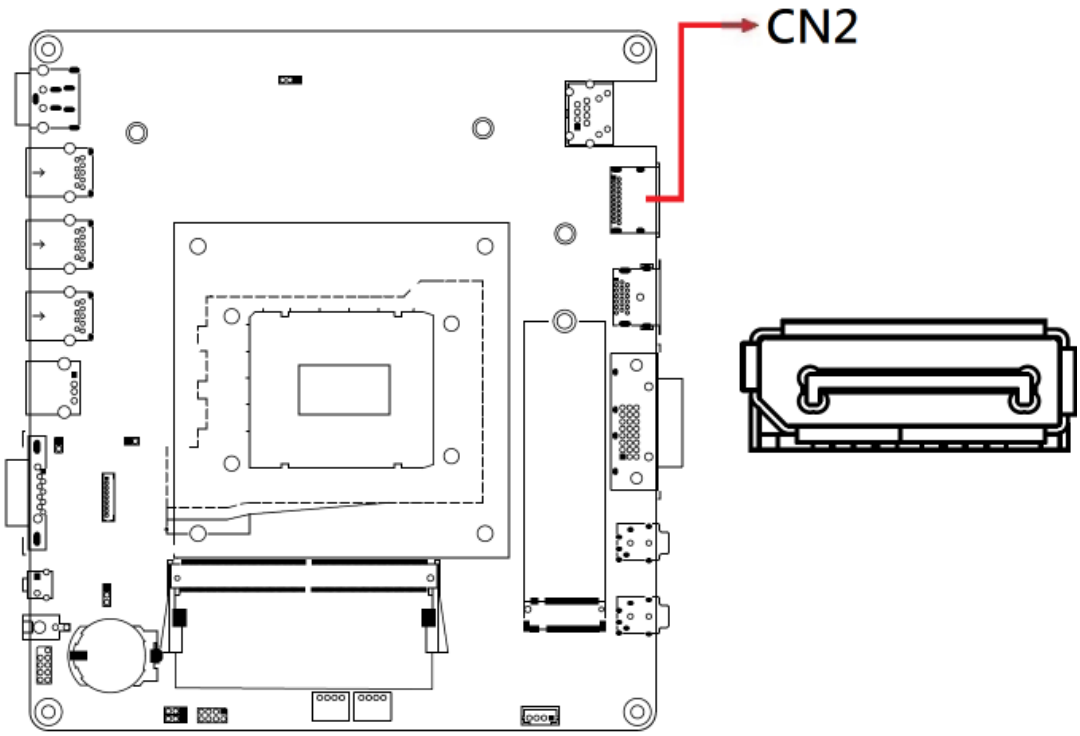
2.4.8 Connector Quick Reference

Connector	Function
CN1	2.5 Gigabit LAN (Intel I226-LM)
CN2	DisplayPort
CN3	HDMI Connector
CN4	DVI-D Connector
CN5	DC_IN Connector
CN6, CN7, CN8	USB3.1 Connector
CN9	USB2.0 Connector
CN10	COM1 Connector
J1	LINE OUT Connector
J2	LINE IN Connector
J14	M.2 B-key 3052 Slot
J4	iSMART PROG
J5, J13	DDR5 SO-DIMM Slots
J11	SPI Flash Connector (Factory use only)
J8	80 Port Debug (Factory use only)
J3, J12	M.2 M2280 Slots
J15	SIM Slot
J16	M.2 E2230 Slot
JP2	Front Panel Connector
SW1, J10	Power Buttom
CPU_FAN1, SYS_FAN1	Fan Power Connectors

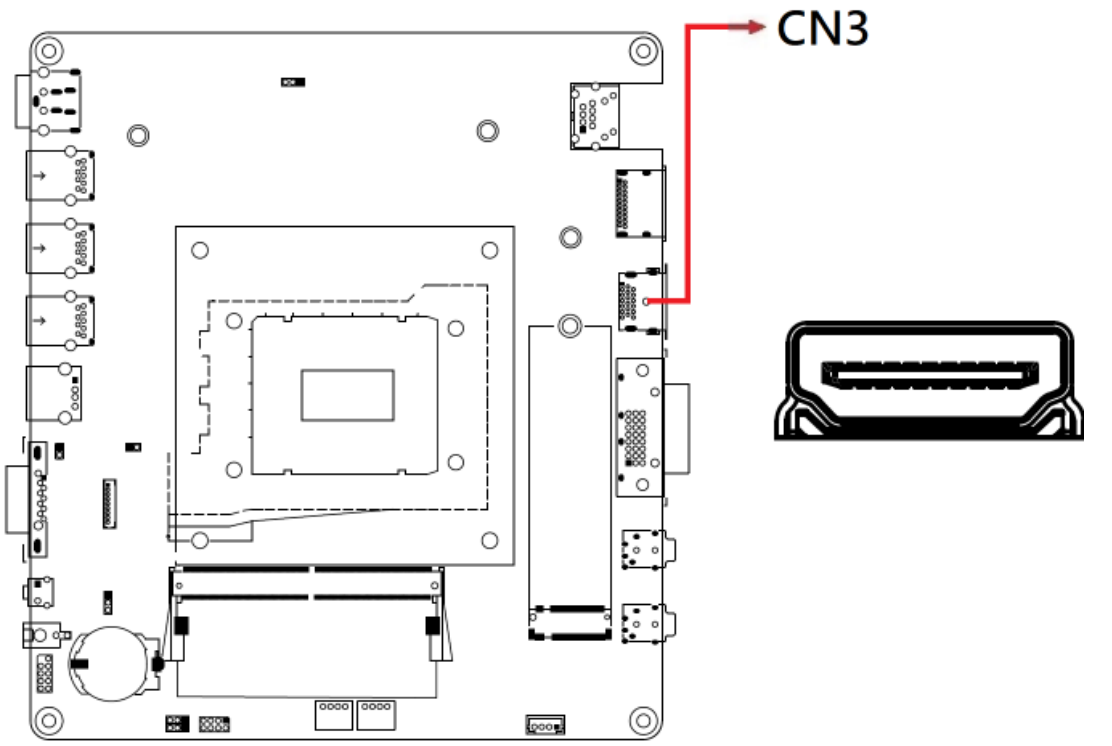
2.4.9 2.5 Gigabit LAN (Intel I226-LM) (CN1)



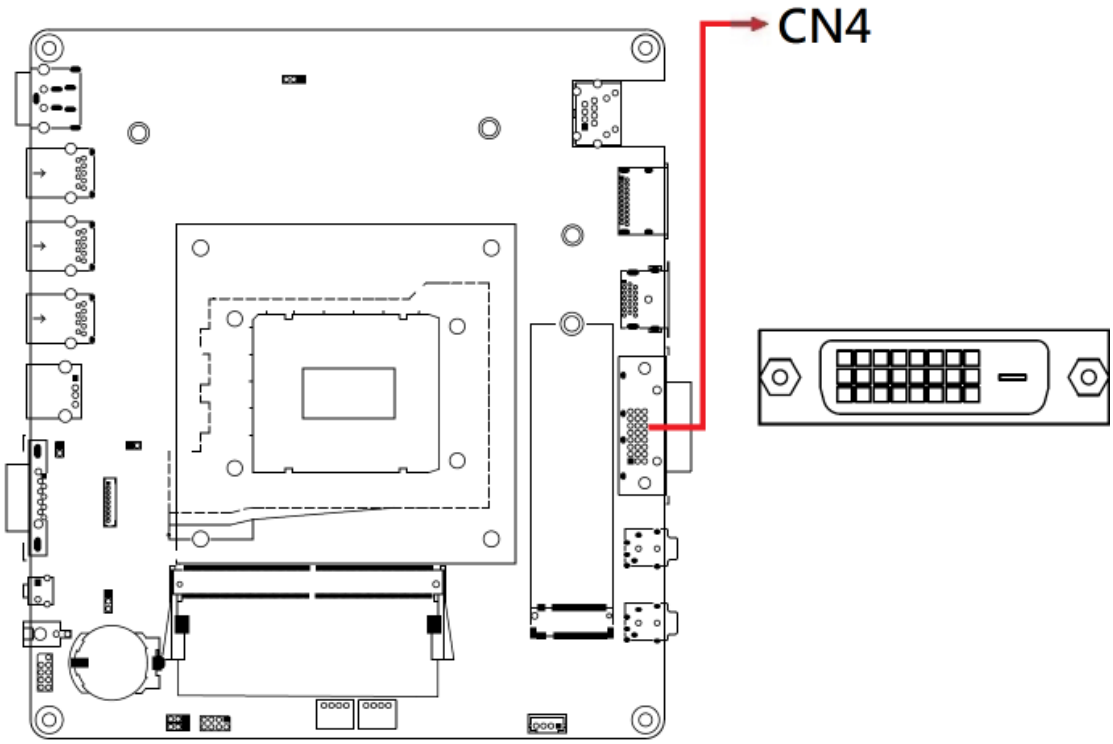
2.4.10 DisplayPort (CN2)



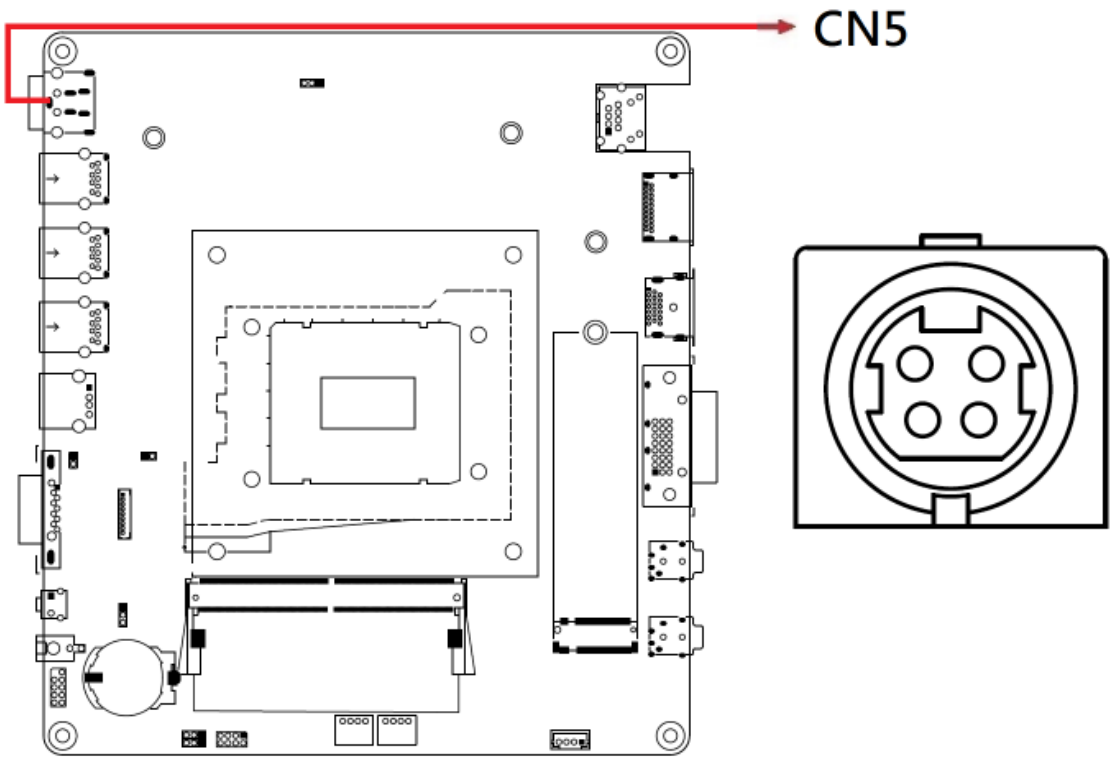
2.4.11 HDMI Connector (CN3)



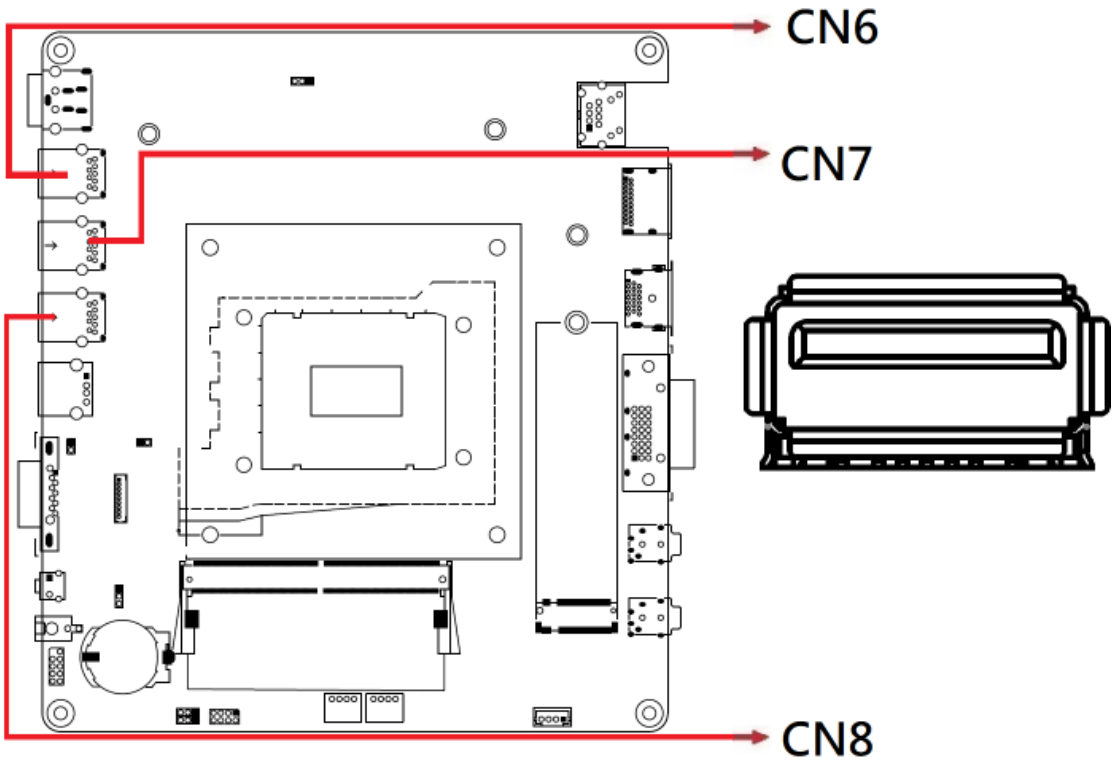
2.4.12 DVI-D Connector (CN4)



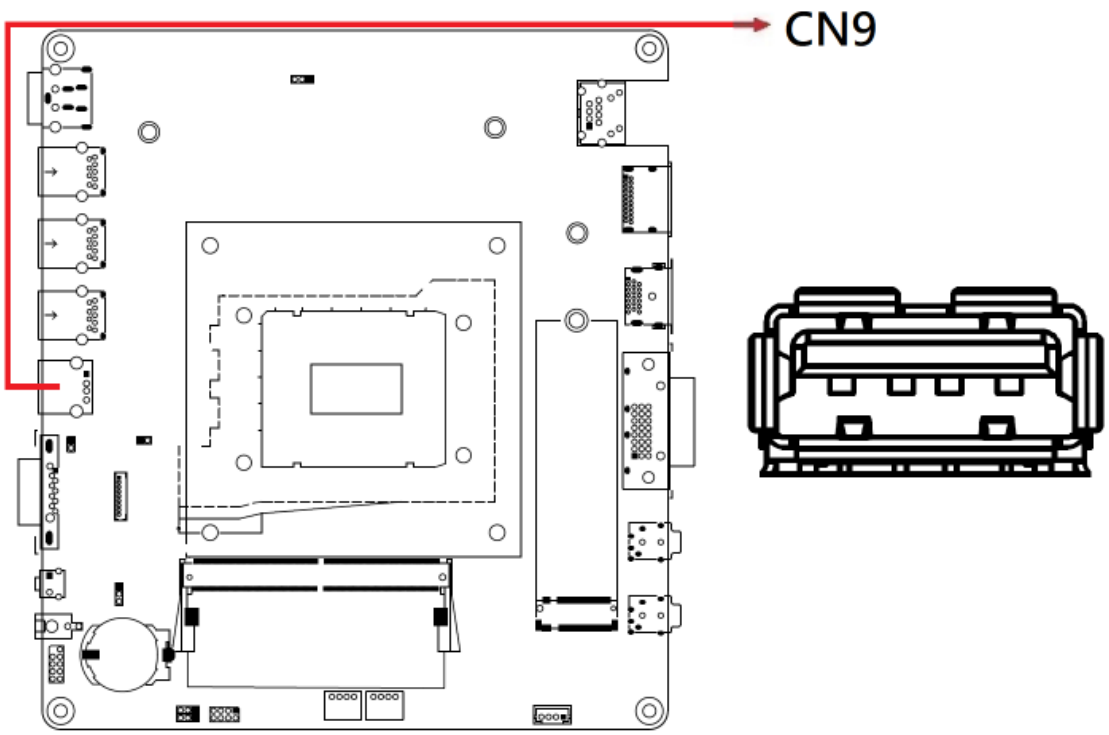
2.4.13 DC_IN Connector (CN5)



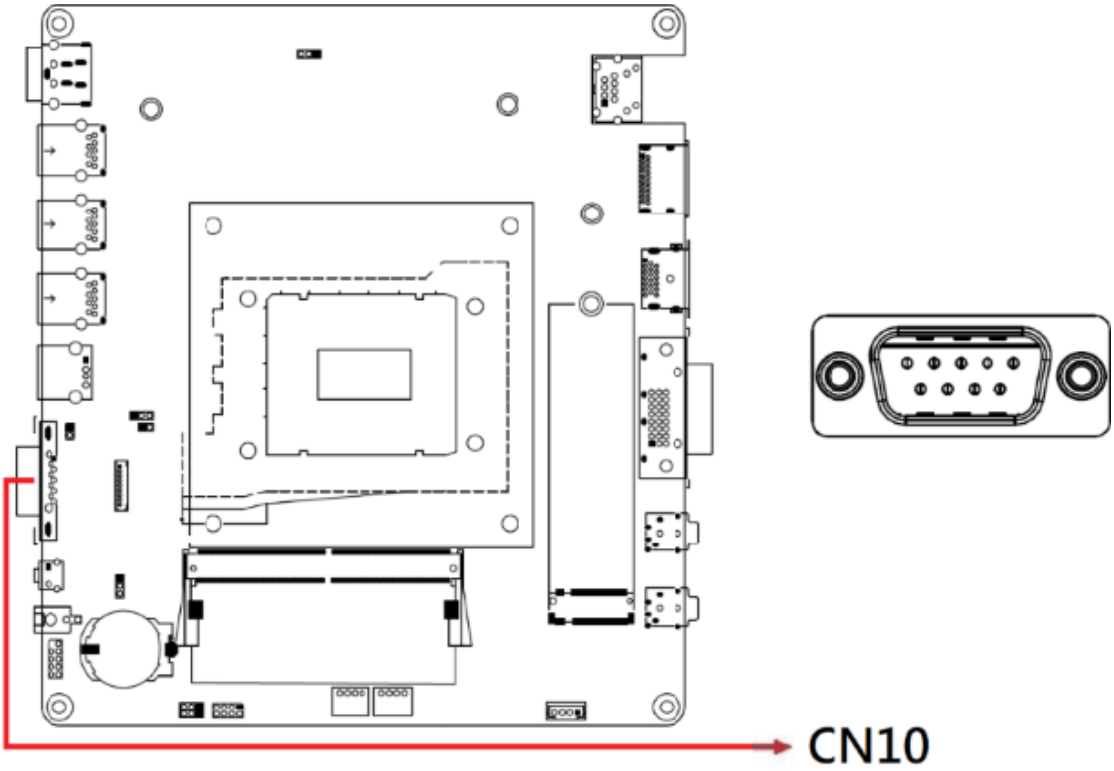
2.4.14 USB 3.2 Connector (CN6, CN7, CN8)



2.4.15 USB 2.0 Connector (CN9)

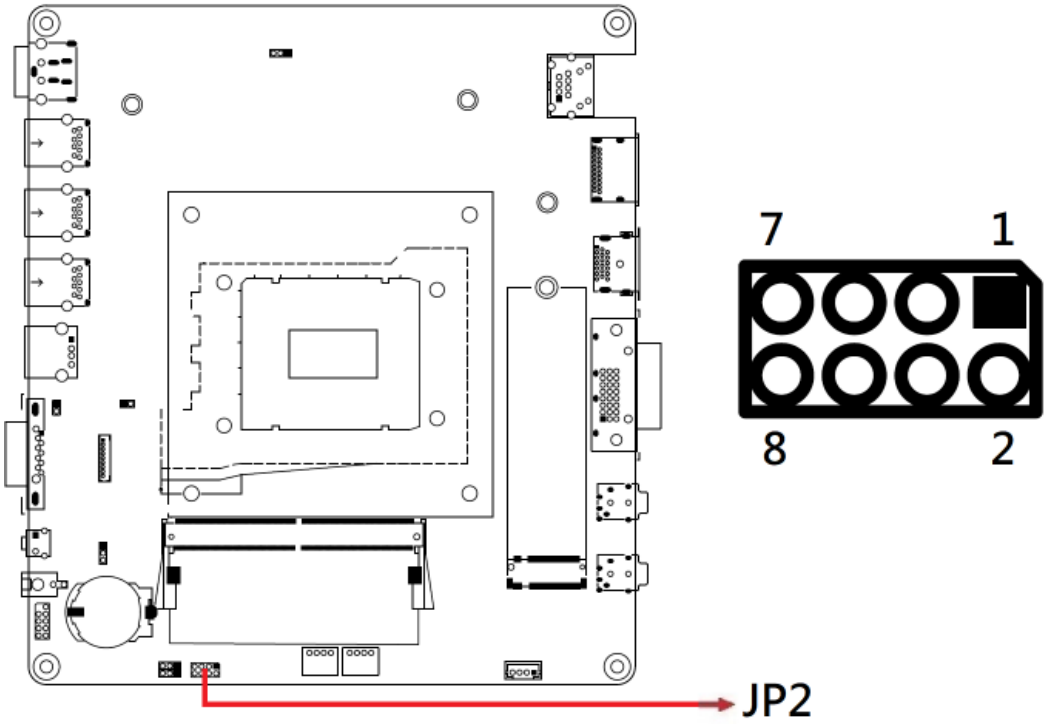


2.4.16 COM1 Ports (CN10)



Pin	Signal Name	Pin	Signal Name
1	DCD, Data carrier detect	6	DSR, Data set ready
2	RXD, Receive data	7	RTS, Request to send
3	TXD, Transmit data	8	CTS, Clear to send
4	DTR, Data terminal ready	9	RI, Ring indicator
5	Ground		

2.4.17 Front Panel Connector (JP2)



Pin	Signal	Pin	Signal
1	Power BTN-	2	Power BTN+
3	HDD LED+	4	HDD LED-
5	Reset BTN-	6	Reset BTN+
7	Power LED+	8	Power LED-

JP2 is utilized for system indicators to provide light indication of the computer activities and switches to change the computer status. It provides interfaces for the following functions:

ATX Power ON Switch (Pins 1 and 2)

Pins 1 and 2 make an “ATX Power Supply On/Off Switch” for the system that connects to the power switch on the case. When pressed, the power switch will force the system to power on. When pressed again, it will power off the system.

Hard Disk Drive LED Connector (Pins 3 and 4)

This connector connects to the hard drive activity LED on control panel. This LED will flash when the HDD is being accessed.

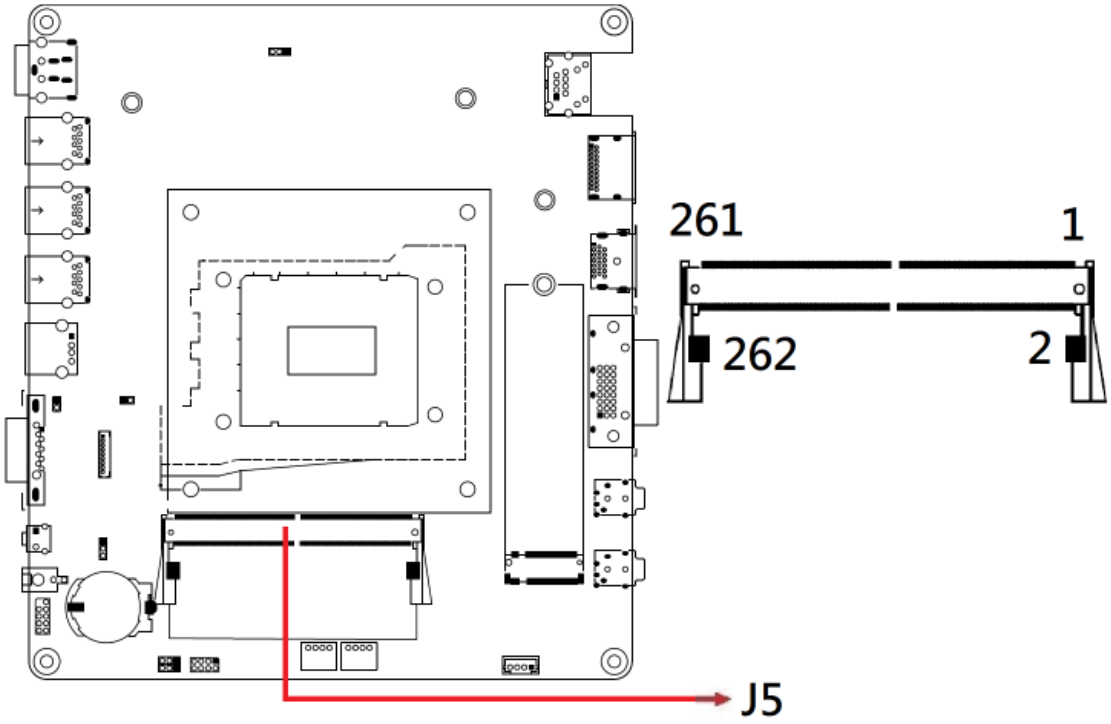
Reset Switch (Pins 5 and 6)

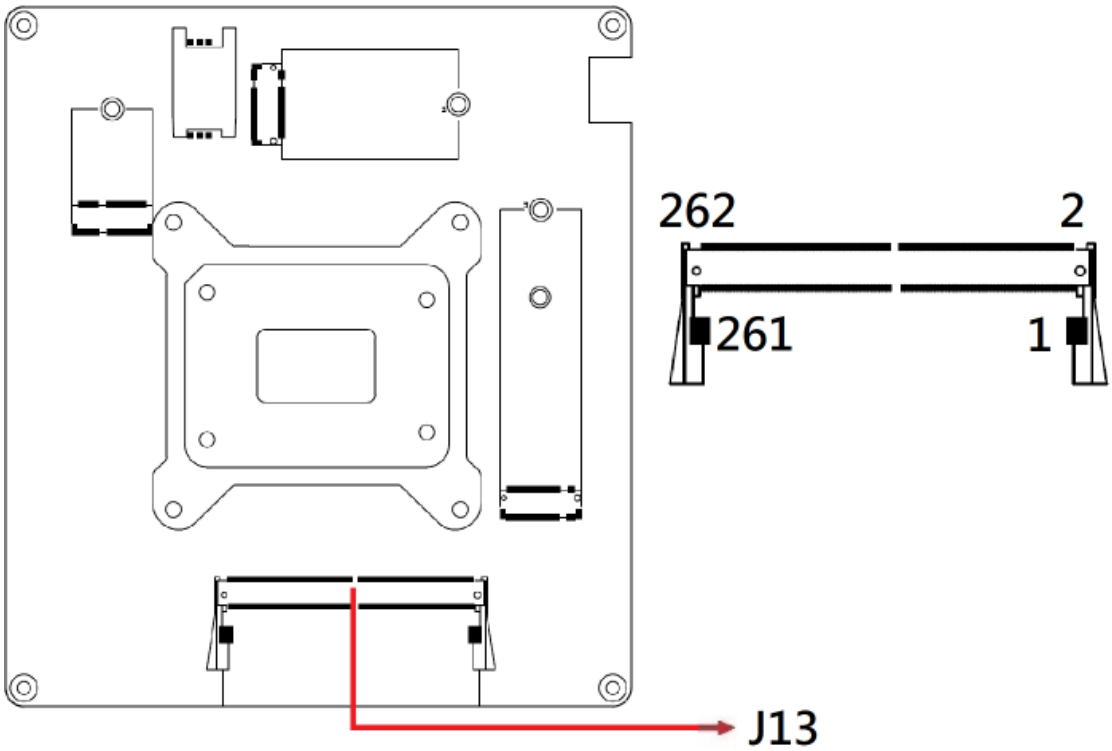
The reset switch allows you to reset the system without turning the main power switch off and then on again. Orientation is not required when making a connection to this header.

Power LED (Pins 7 and 8)

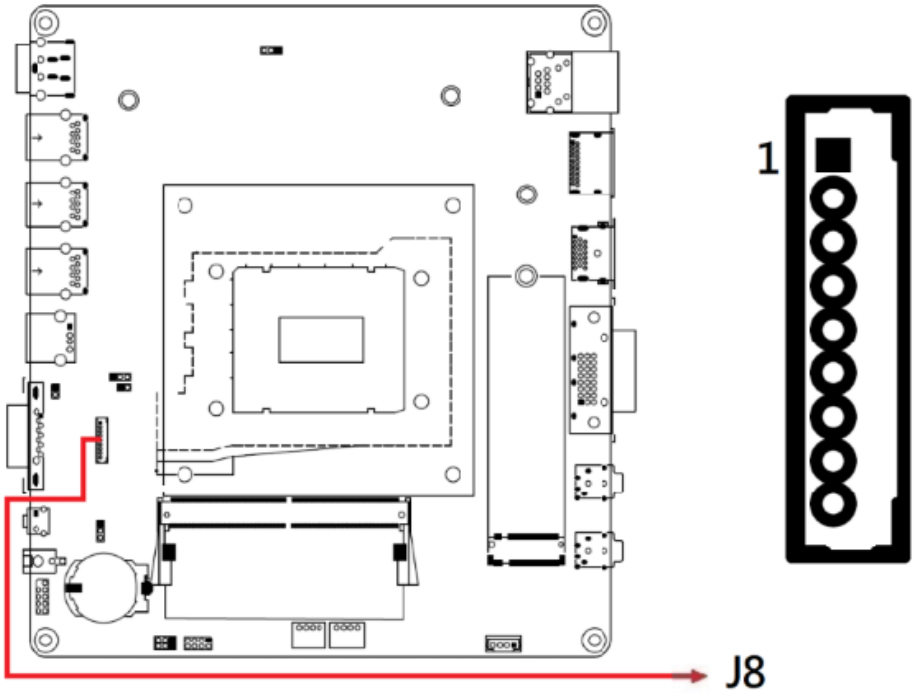
This connector connects to the system power LED on control panel. This LED will light when the system turns on.

2.4.18 DDR5 SO-DIMM Slot (J5 / J13)



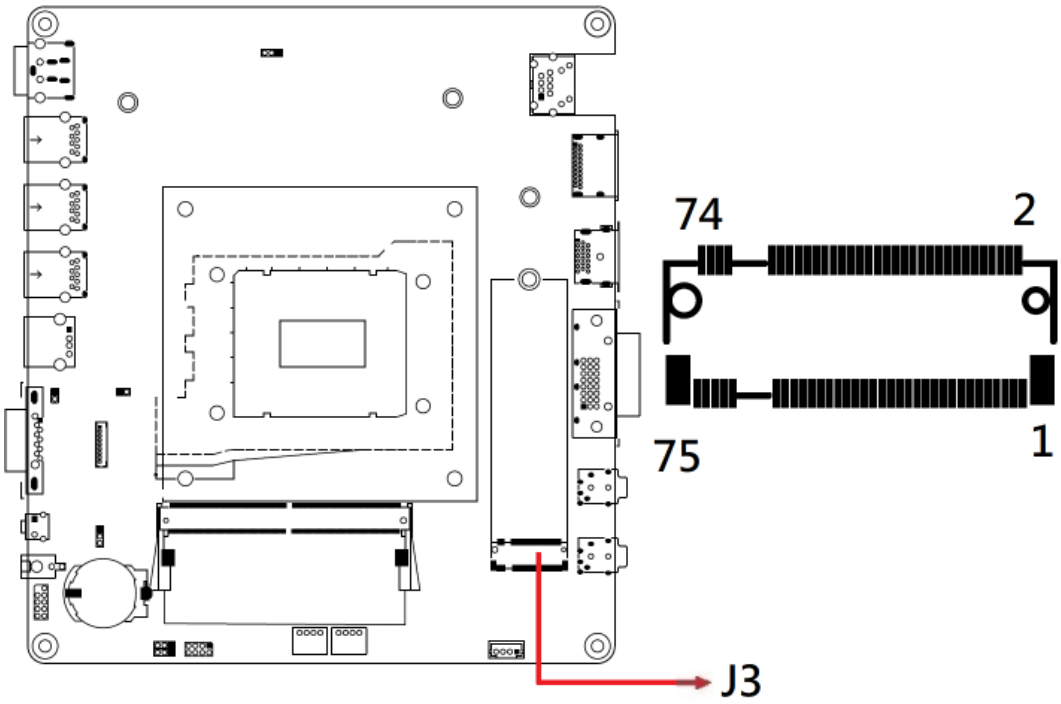


2.4.19 80 Port Debug (J8)



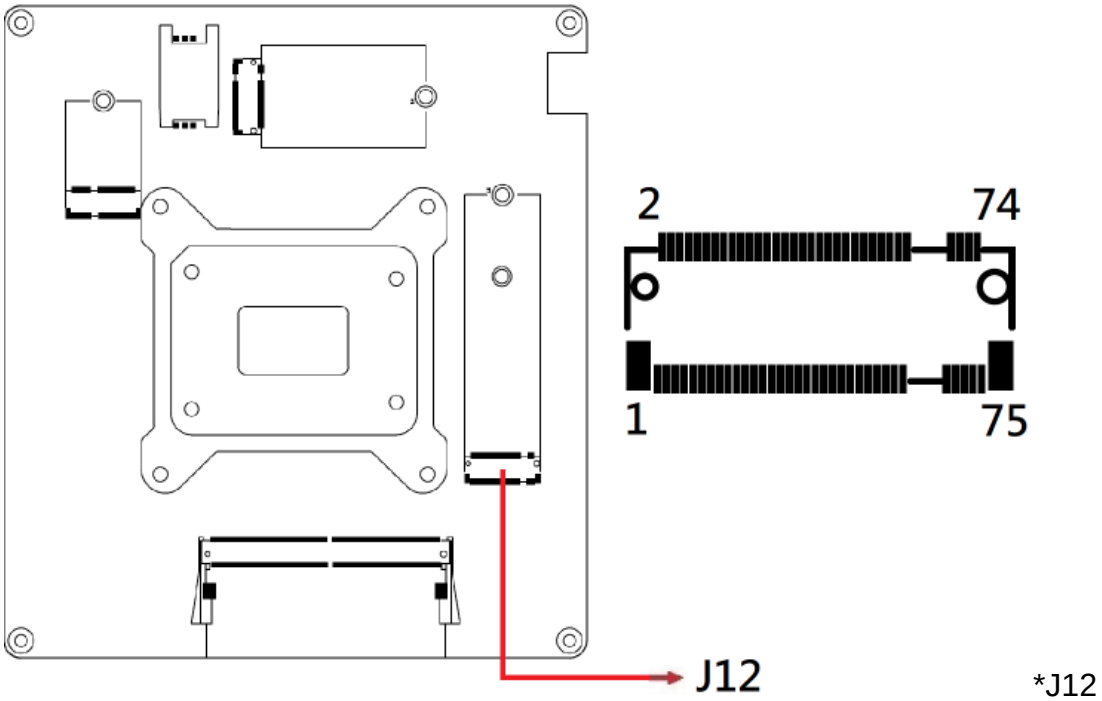
Note: J8 is for factory use only.

2.4.20 M.2 M2280 Slot (J3)



*J3/J12 supports NVME

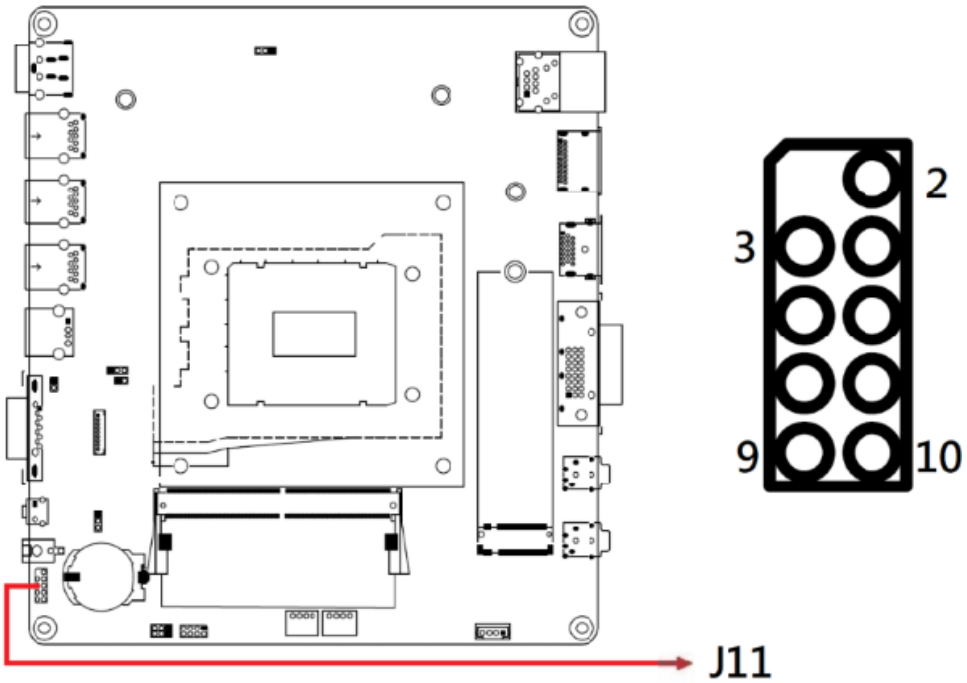
2.4.21 M.2 E2230 Slot (J12)



*J12

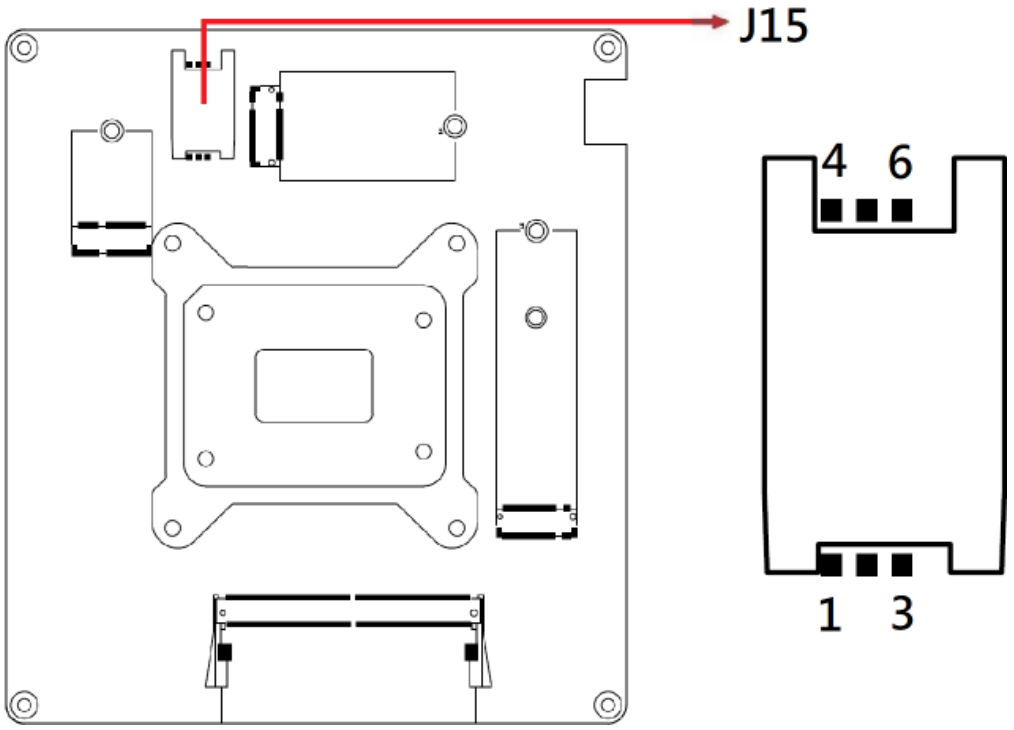
* supports USB2.0 & PCIE x1

2.4.22 SPI Flash Connector (J11)

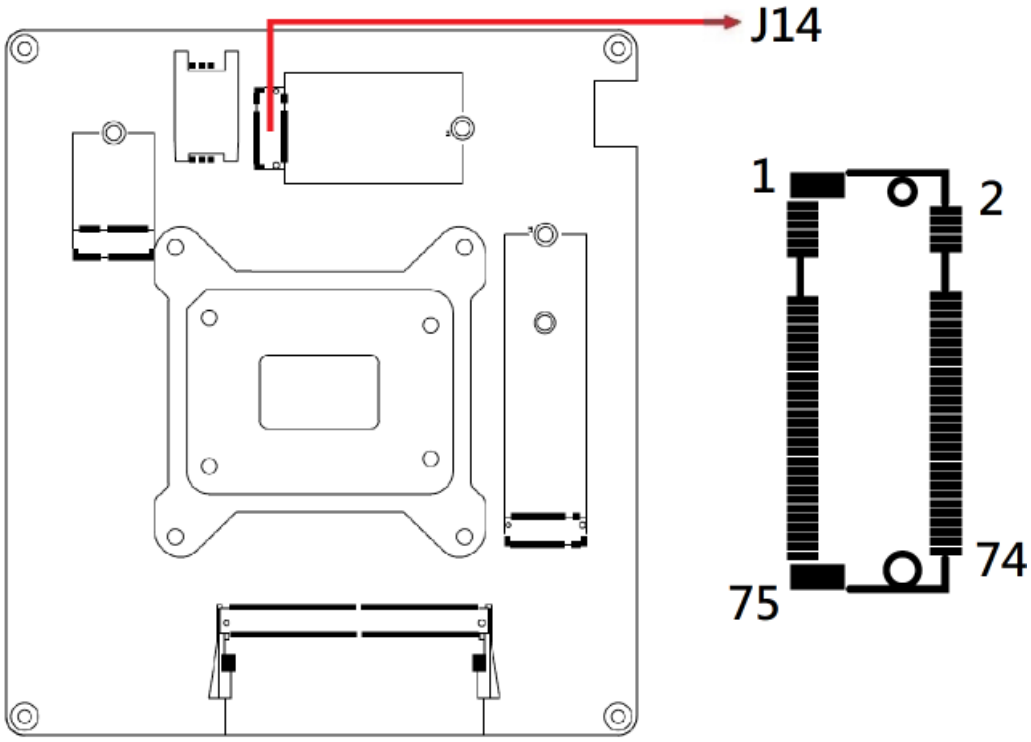


Note: J11 is for factory use only.

2.4.23 SIM Slot (J15)

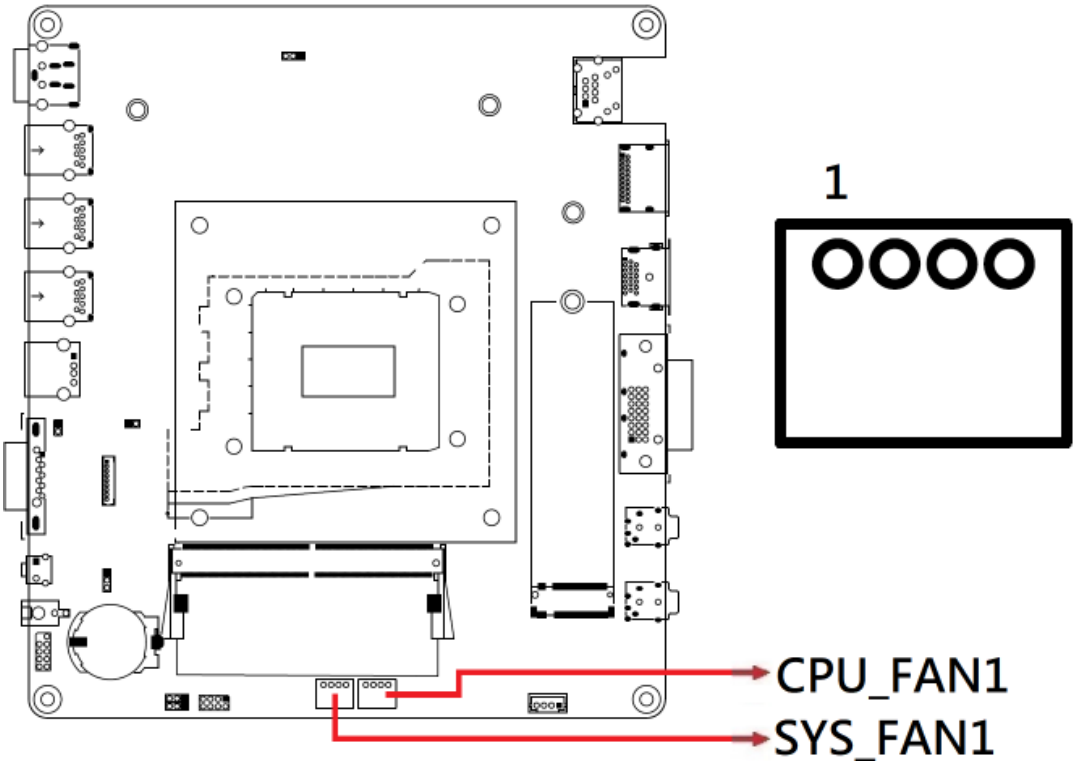


2.4.24 M.2 B-key 3052 Slot (J14)



*J14 supports Sierra EM9191 5G modules.

2.4.25 Fan Power Connectors (CPU_FAN1, SYS_FAN1)



Pin	Signal Name
1	Ground
2	+12V
3	Rotation detection
4	Control

Chapter 3
Driver Installation

The information provided in this chapter includes:

- Intel® Chipset Software Installation Utility
- HD Audio Driver Installation
- LAN Driver Installation
- Intel® Management Engine Components Drivers Installation

3.1 Introduction

This section describes the installation procedures for software drivers. The software drivers are available on IBASE website www.ibase.com.tw.

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

3.2 Intel® Chipset Software Installation Utility

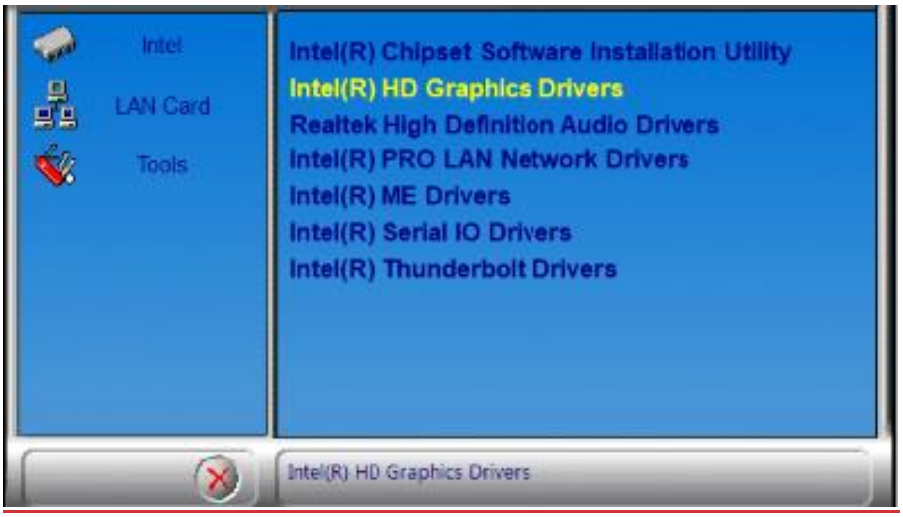
The Intel® Chipset drivers should be installed first before the software drivers to install INF files for Plug & Play function for the chipset components. Follow the instructions below to complete the installation.

1. Run the disk enclosed with the board package. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers** on the right pane, and click **Intel(R) Chipset Software Installation Utility**.

2. When the *Welcome* screen for the Intel® Chipset Device Software appears, click **Next** to continue.
3. **Accept** the software license agreement.
4. On the *Readme File Information* screen, click **Install**.
5. After the installation has been completed, click **Finish** to complete the setup process.

3.3 VGA Driver Installation

1. Run the disk enclosed with the board package. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers** on the right pane. Run the drivers disk. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers**, and **Intel(R) HD Graphics Driver** on the right pane.

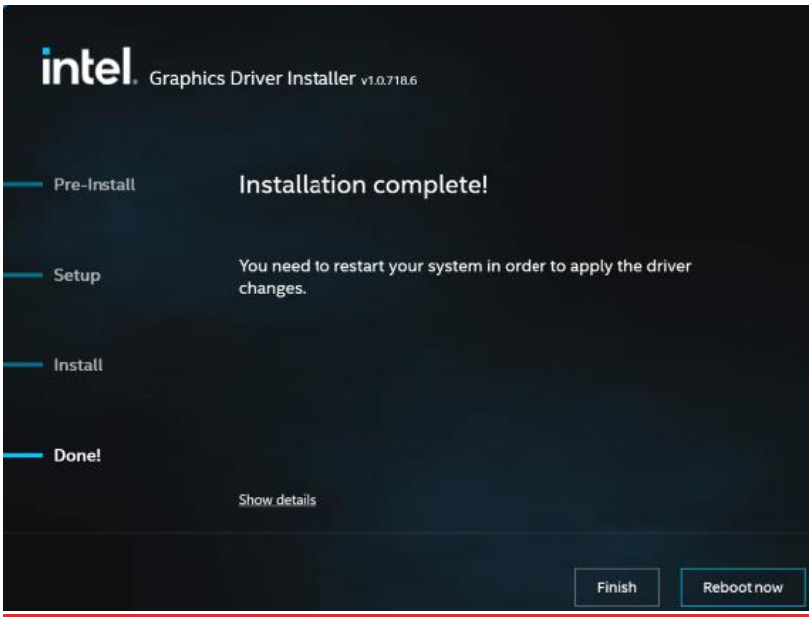


2. When the ***Intel Graphics Driver Installer*** screen appears, click **Begin installation**.

3. Click **I agree** to accept the INTEL SOFTWARE LICENSE AGREEEMENT.

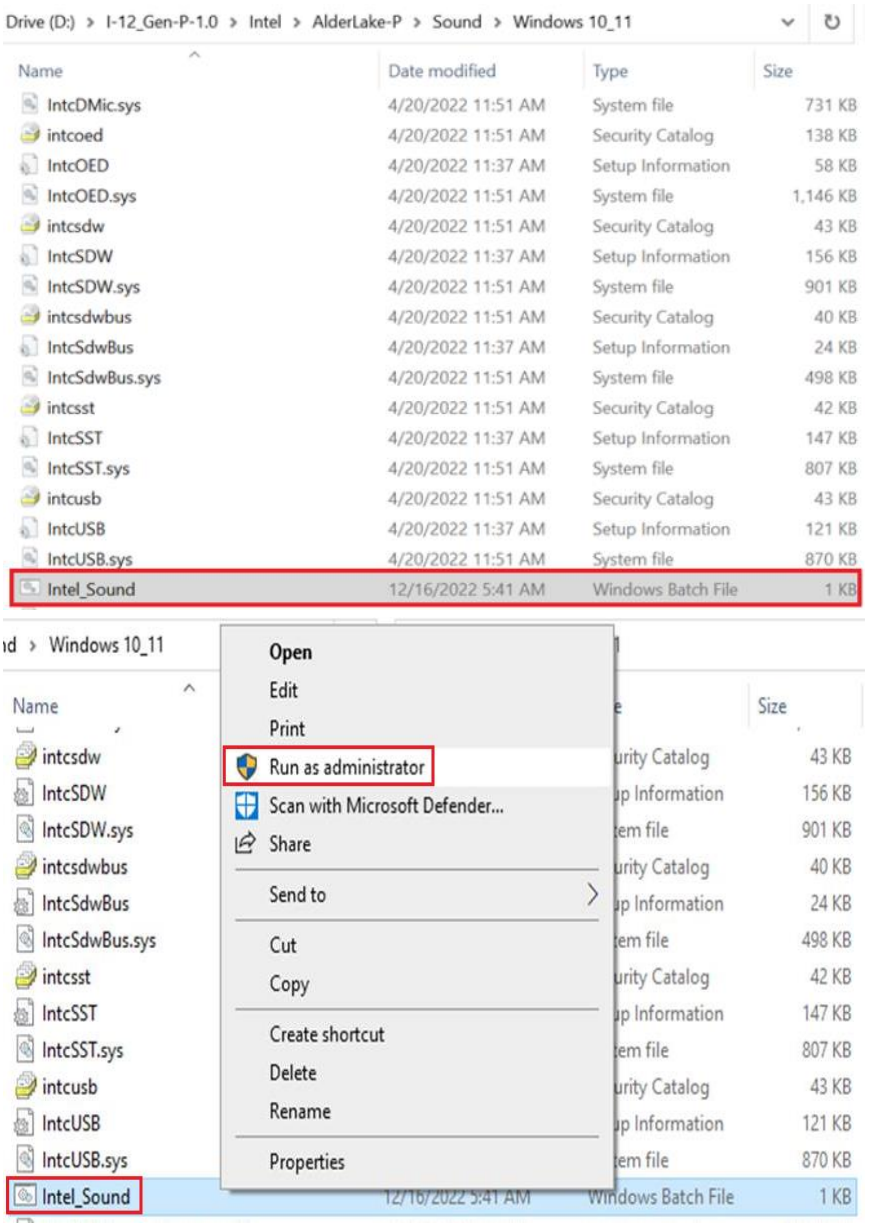
4. In the Pre-Install stage, “The installer will install the following components:
   - Intel® Graphics Driver
   - Intel® Graphics Command Center
   Click **Start** to start installing the new graphics driver.

5. The next screen will indicate that the new graphics driver is being installed. When the message “**Installation complete!**” appears, restart your system in order to apply the driver changes.



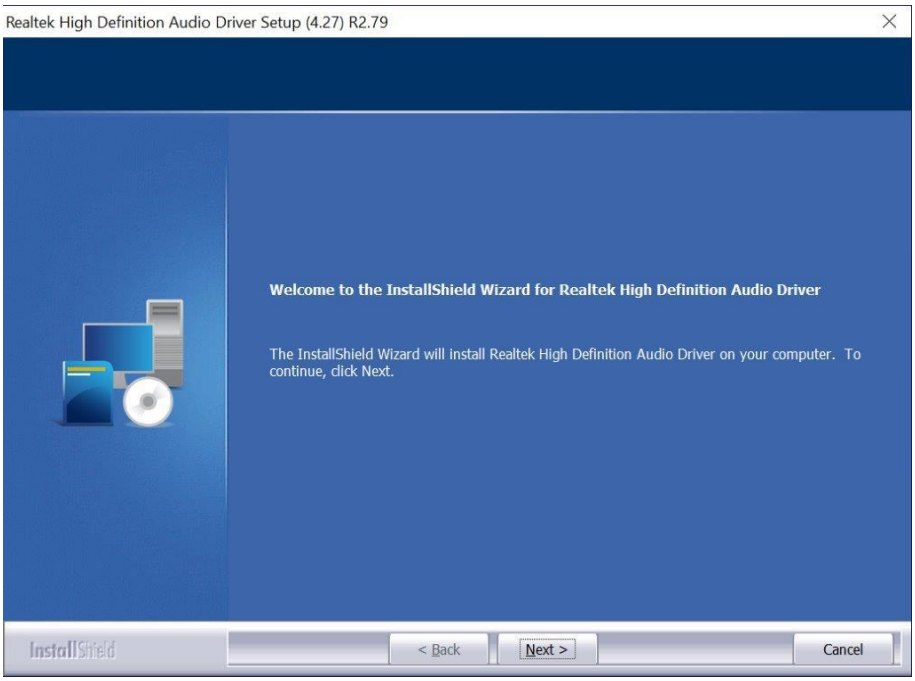
3.4 Realtek HD Audio Driver Installation

1. Before installing the audio drivers in the disk provided, run the batch file - **Intel_Sound.bat** in the directory shown in the picture below:
   I-12_Gen-P-1.0\Intel\AlderLake-P\Sound\Windows 10_11
   Right-click Intel_Sound.bat and **run the batch file as administrator**.



2. After running the batch file, install the audio drivers. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers** on the right.Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers**, and **Realtek High Definition Audio Driver** on the right pane.

3. On the *Welcome* screen of the InstallShield Wizard, click **Next** to install the drivers.

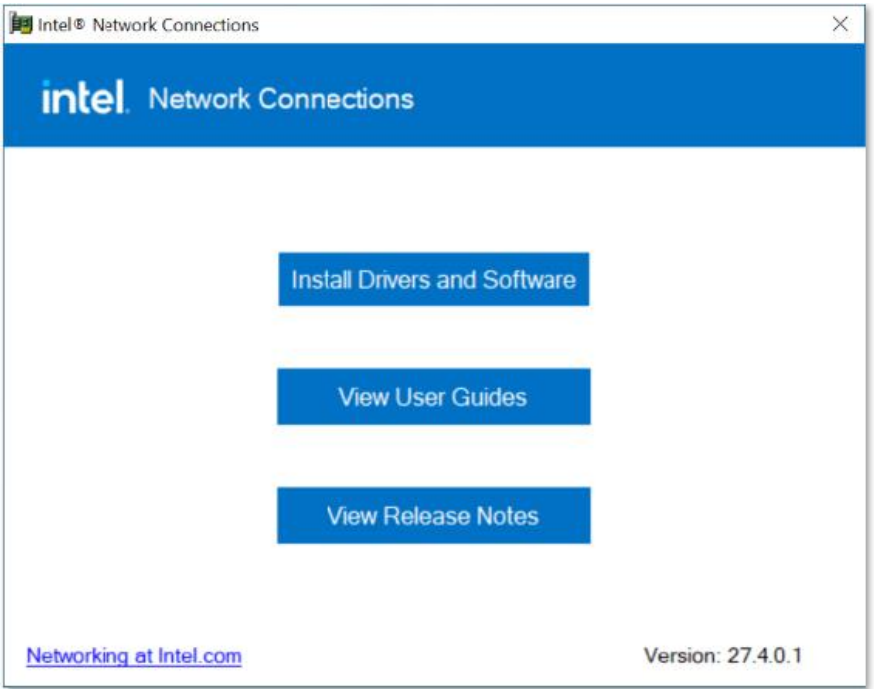


4. When the audio driver has been installed, click **Finish** to restart the computer.

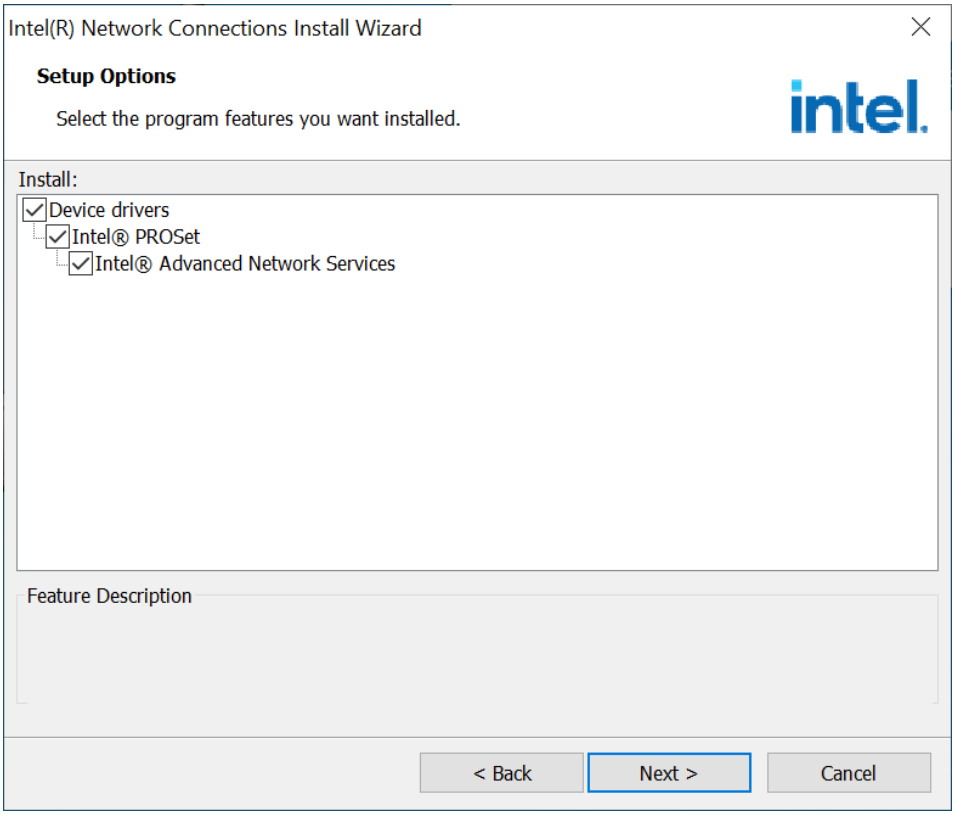
3.5 LAN Drivers Installation

1. Run the disk enclosed with the board package. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers**, and **Intel PRO LAN Network Drivers** on the right pane.

2. Click **Intel Drivers and Software**.



3. When the *Welcome to the install wizard for Intel(R) Network Connection* screen appears, click **Next**. On the next screen, accept the terms in the License Agreement and click **Next**.
4. On the *Setup Options* screen, select the program features you want to be installed. Then click **Next** to continue.

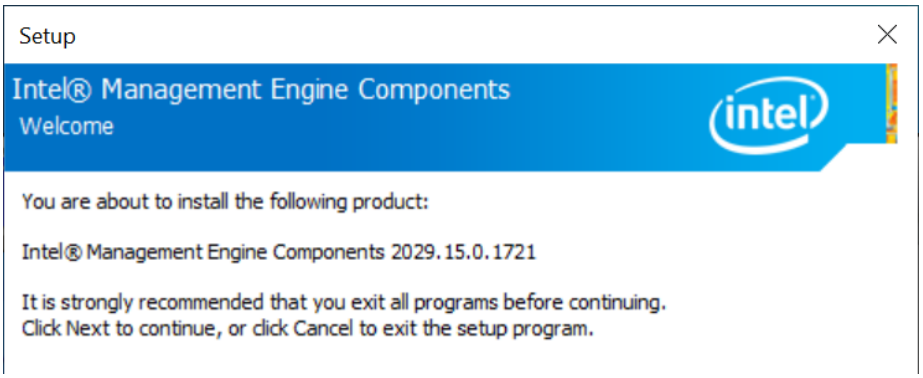


5. On the *Ready to Install the Program* screen, click **Install** to begin the installation. When the *Install wizard Completed* screen appears, click **Finish**.

3.6 Intel® Management Engine Components Drivers Installation

1. Run the disk enclosed with the board package. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers,** and **Intel(R) ME Drivers** on the right pane..

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

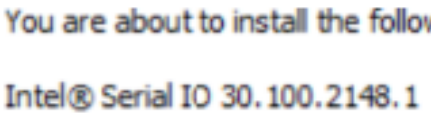


3. Accept the license agreement and click **Next**.
4. On the Destination Folder screen, click **Next**.
5. After Intel Management Engine Components have been successfully installed, click **Finish**.

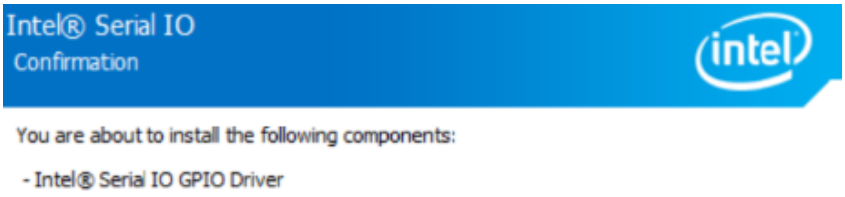
3.7 Intel® Serial I/O Drivers Installation

1. Run the disk enclosed with the board package. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers,** and **Intel(R) Serial IO Drivers** on the right pane.

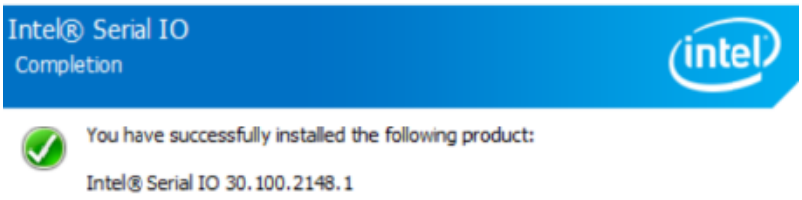
2. When the *Welcome* screen to the Intel® Serial IO appears, click **Next**.



3. Accept the terms in the license agreement and click **Next**.
4. On the **Readme File Information** and **Confirmation** screens, click **Next**.



5. Click **Finish** when the **Completion** screen appears.

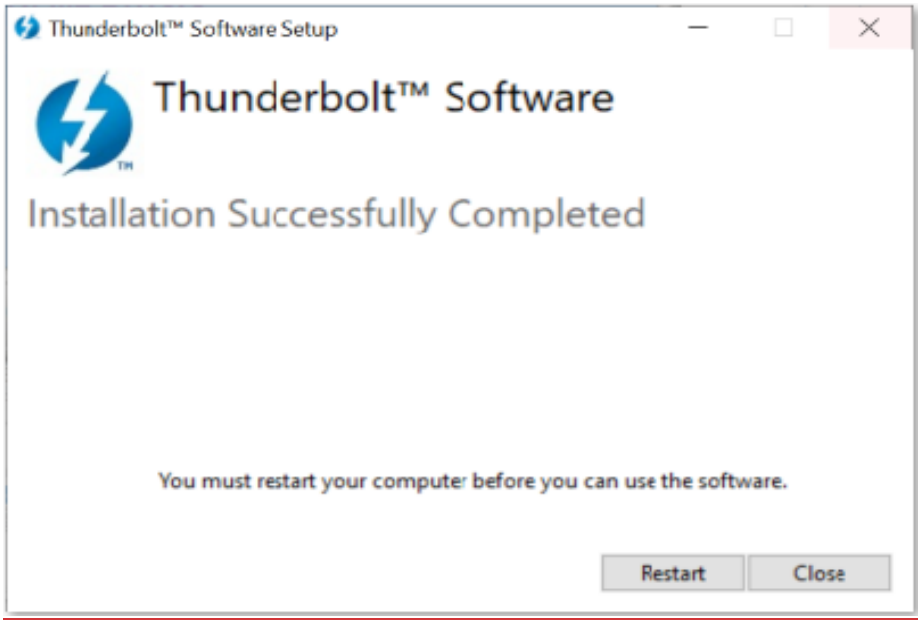


3.8 Intel® Thunderbolt Drivers Installation

1. Run the disk enclosed with the board package. Click **Intel** on the left pane and then **Intel(R) AlderLake-P/PS/U Chipset Drivers,** and **Intel(R) Thunderbolt Drivers** on the right pane.

2. Accept the terms in the license agreement and click **Install**.

3. When installation has been completed, click **Restart**.



Chapter 4
BIOS Setup

This chapter describes the different settings available in the AMI BIOS that comes with the board. The topics covered in this chapter are as follows:

- Main Settings
- Advanced Settings
- Chipset Settings
- Security Settings
- Boot Settings
- Save & Exit

4.1 Introduction

The BIOS (Basic Input/Output System) installed in the ROM of your computer system supports Intel® processors. The BIOS provides critical low-level support for standard devices such as disk drives, serial ports and parallel 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 allows you 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 pressing the ”Reset” button or 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
```

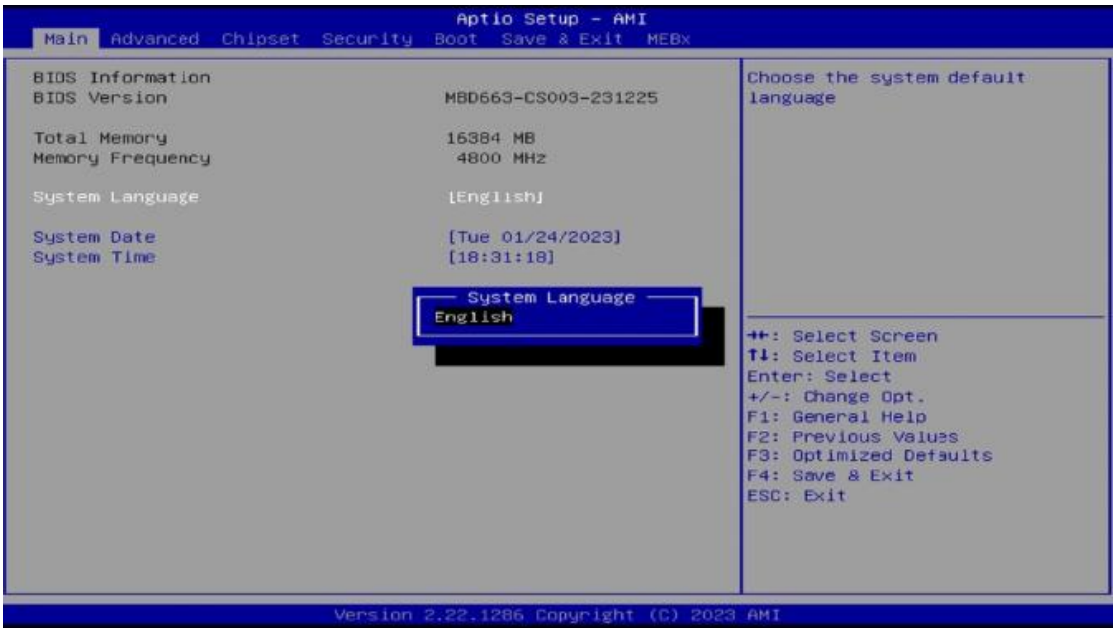
In general, press the arrow keys to highlight items, <Enter> to select, the <PgUp> and <PgDn> keys to change entries, <F1> for help, and <Esc> to quit.

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.

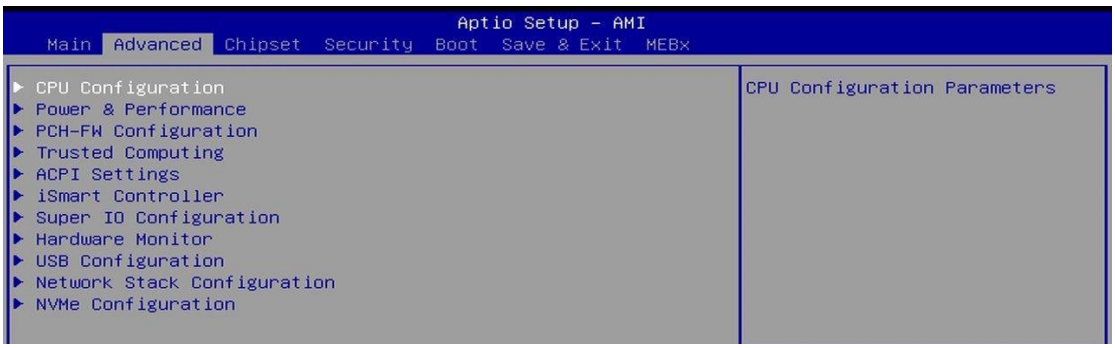
4.3 Main Settings



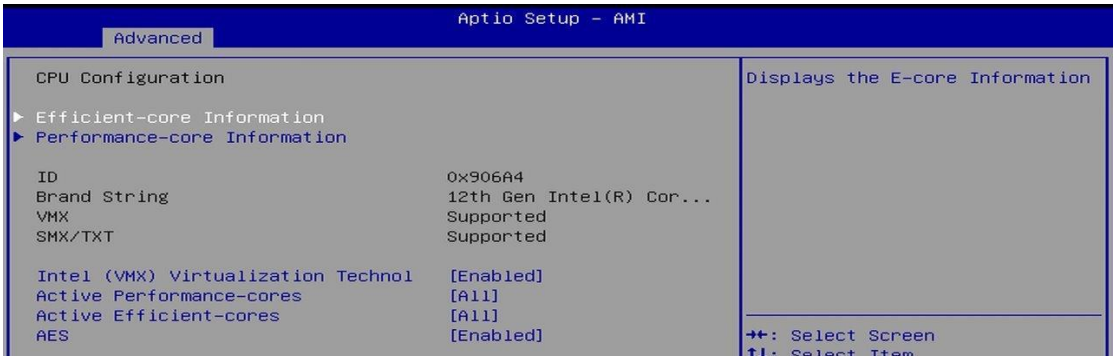
BIOS Setting	Description
System Date	Sets the date. Use the <Tab> key to switch between the date elements.
System Time	Set the time. Use the <Tab> key to switch between the time elements.

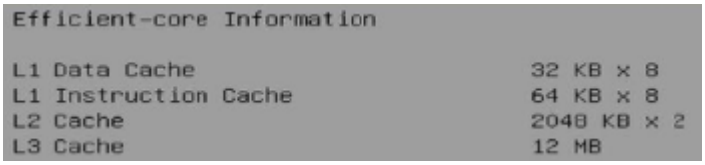
4.4 Advanced Settings

This section allows you to configure, improve your system and allows you to set up some system features according to your preference.



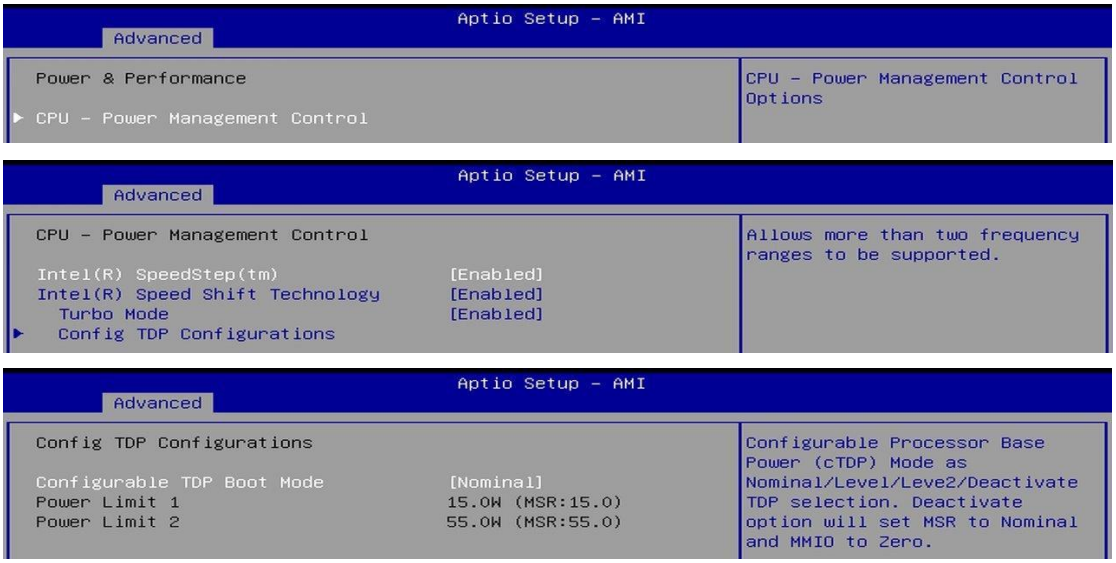
4.4.1 CPU Configuration





BIOS Setting	Description
Efficient-core Information	Displays the E-core information.
Performance-core Information	Displays the P-core information.
Intel (VMX) Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Procesor Cores	Number of cores to enable in each processor package. Number of Core and E-cores are looked at together. When both are [0,0], Pcode will enable all cores.
Hyper-Threading	Enable or Disable Hyper-Threading Technology
AES	Enable/Disable AES (Advanced Encryption Standard)

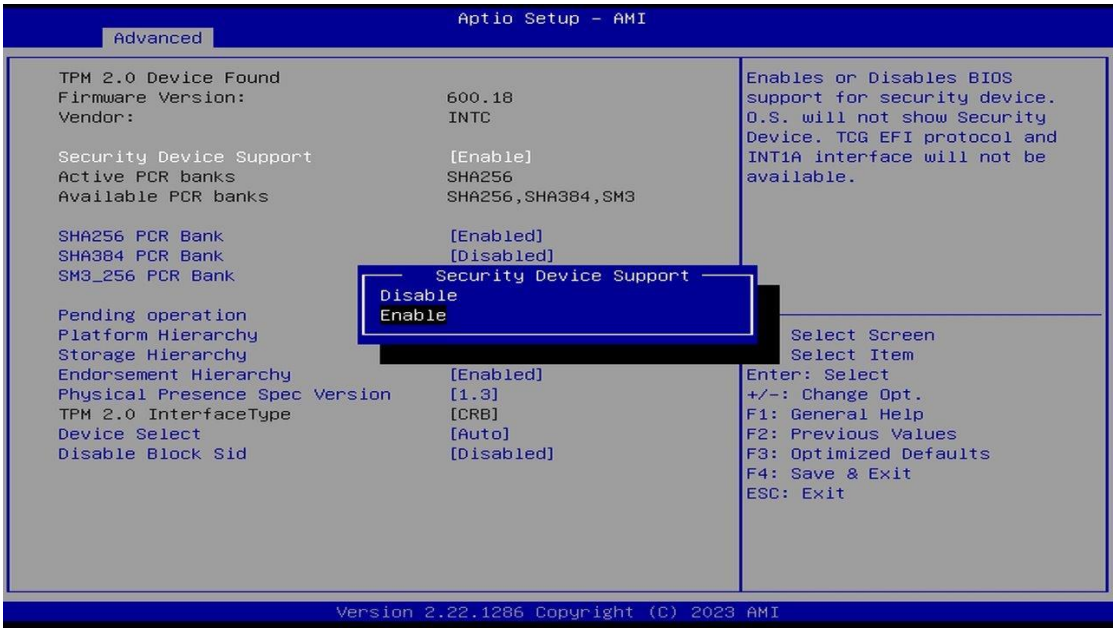
4.4.2 Power & Performance



BIOS Setting	Description
CPU – Power Management Control	CPU power management control options.
Intel(R) SpeedStep(tm)	Allows more than two frequency ranges to be supported
Intel(R) Speed Shift Technology	Enable/Disable Intel(R) Speed Shift Technology support. Enabling will expose the CPPC V2 interface to allow for hardware controlled P-states.
Tubo Mode	Enable/Disable processor Tubo mode (requires EMTTM enabled too). AUTO means enabled.
Config TDP Configuration	Configurable processor base power (cTDP) configuration

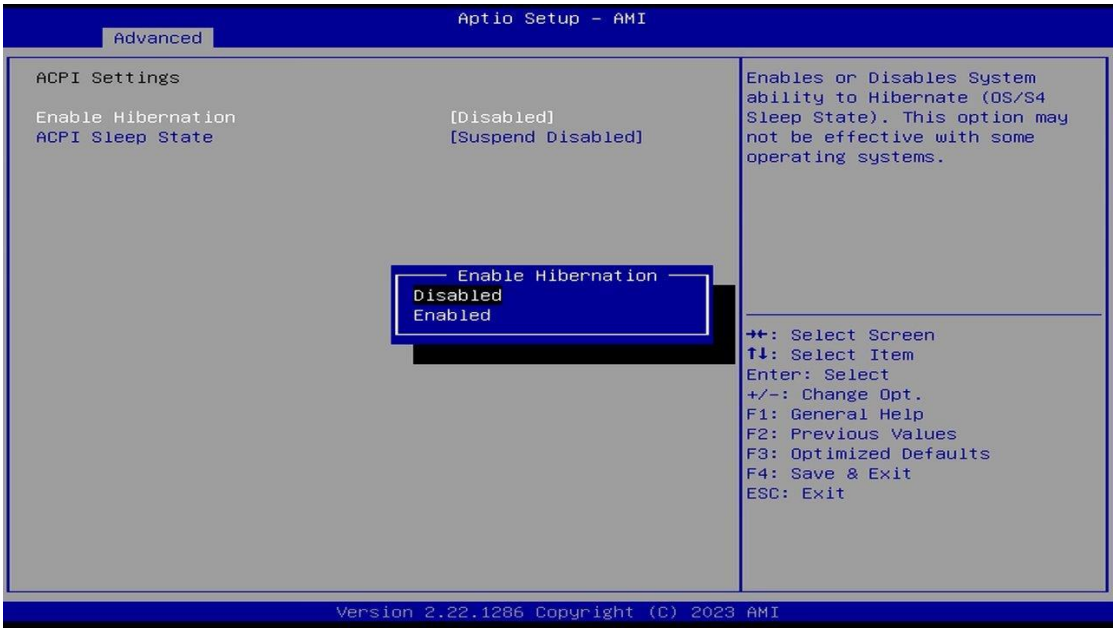
4.4.3 PCH-FW Configuration

4.4.4 Trusted Computing



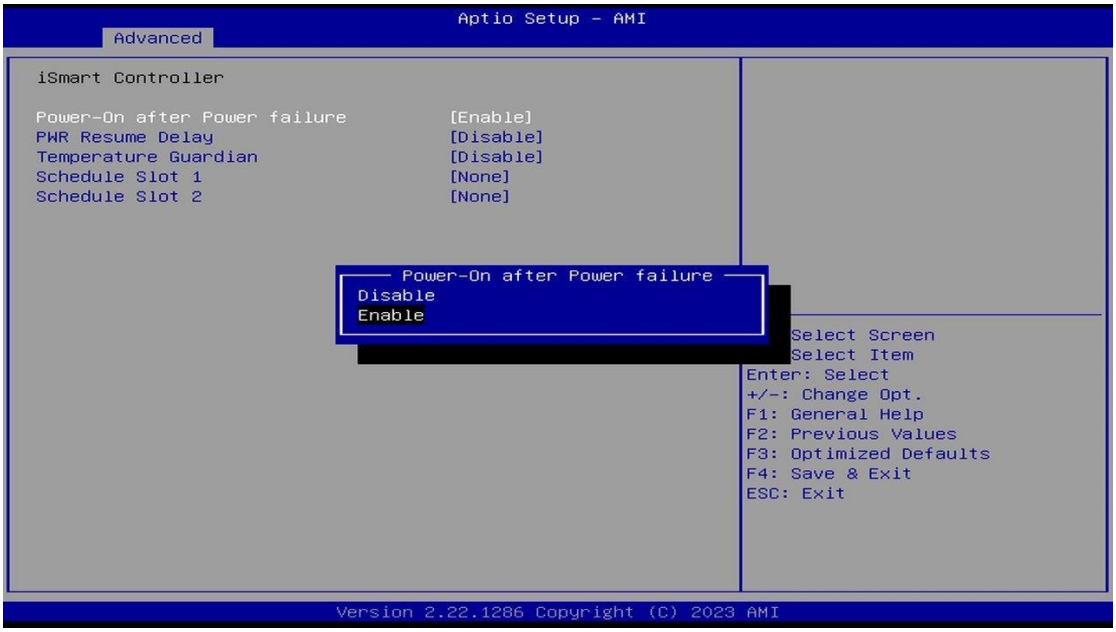
BIOS Setting	Description
Security Device Support	Enables / Disables BIOS support for security device. OS will not show security device. TCG EFI protocol and INTIA interface will not be available.
SHA256 PCR Bank SHA384 PCR Bank SM3_256 PCR Bank	Options: Enable / Disable
Pending operation	Schedule an operation for the security device. Note: Your computer will reboot during restart in order to change state of security device.
Platform / Storage / Endorsement Hierarchy	Options: Enable / Disable
TPM2.0 UEFI Spec Version	Select the TCG2 Spec Version Support. TCG_1_2: the compatible mode for Win8/Win10 TCG_2: Support new TCG2 protocol and event format for Win10 or later
Physical Presence Spec Version	Select to tell OS to support PPI Spect Version 1.2 or 1.3. 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.
Disable Block Sid	Overried to allow SID authentication in TCG storage device.

4.4.5 ACPI Settings



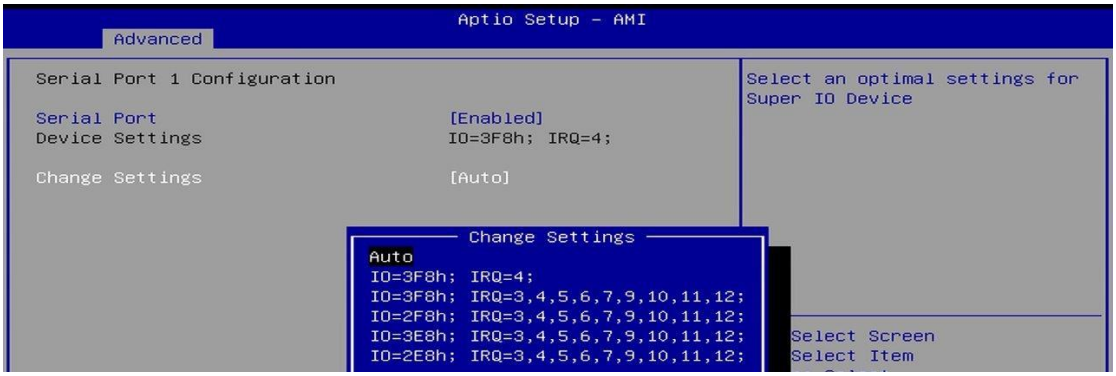
BIOS Setting	Description
Enable Hibernation	Enables / Disables system ability to hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.
ACPI Sleep State	Select the highest ACPI sleep state the system will enter when the SUSPEND button is pressed.

4.4.6 iSmart Controller



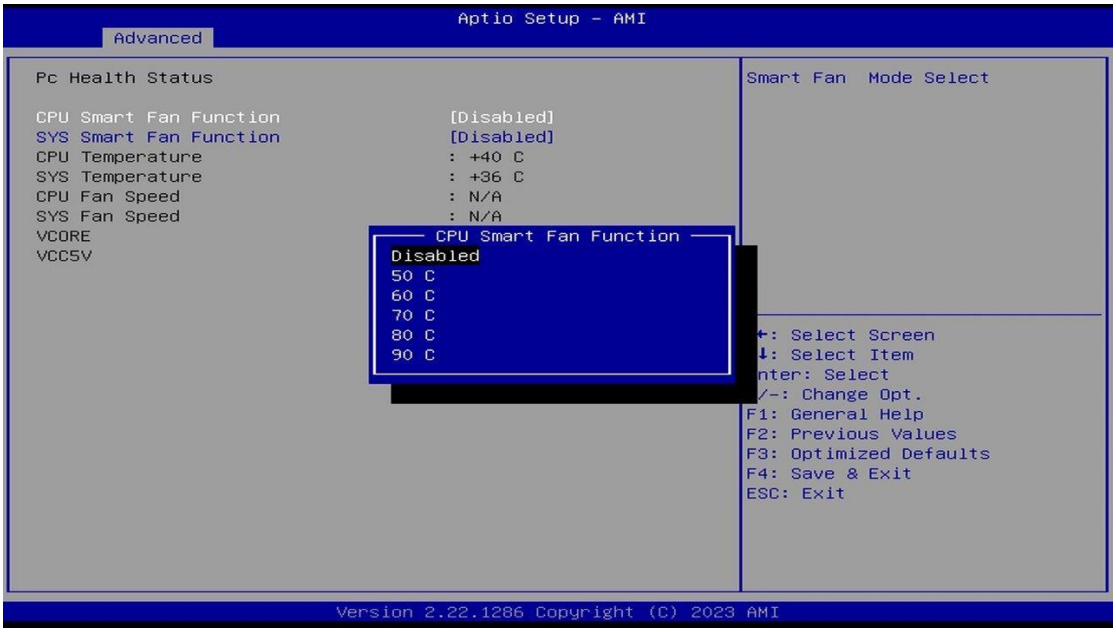
BIOS Setting	Description
Power-On after Power failure	Enables / Disables the system to be turned on automatically after a power failure.
PWR Resume Delay	Enables / Disables Power on resume delay.
Temperature Guardian	Options: Disable / Enable
Schedule Slot 1 / 2	Sets up the hour / minute for system powe-on. **Important:** If you would like to set up a schedule between adjacent days, configure two schedule slots. For example, if setting up a schedule from Wednesday 5 p.m. to Thursday 2 a.m., configure two schedule slots. But if setting up a schedule from 3 p.m to 5 p.m. on Wednesday, configure only a schedule slot.

4.4.7 F81804 Super IO Configuration



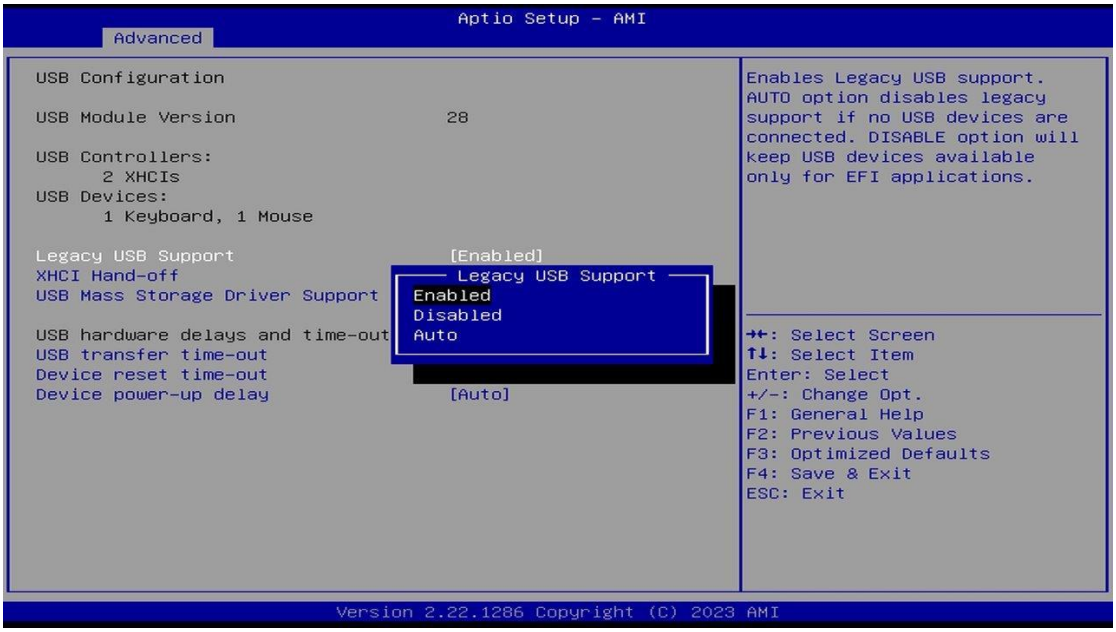
BIOS Setting	Description
Serial Port 1 Configuration	Sets parameters of Serial Port 1 (COMA).
Serial Port	Enable / Disable the serial port.
Change Settings	Select an optimal setting for the Super IO device.

4.4.8 Hardware Monitor



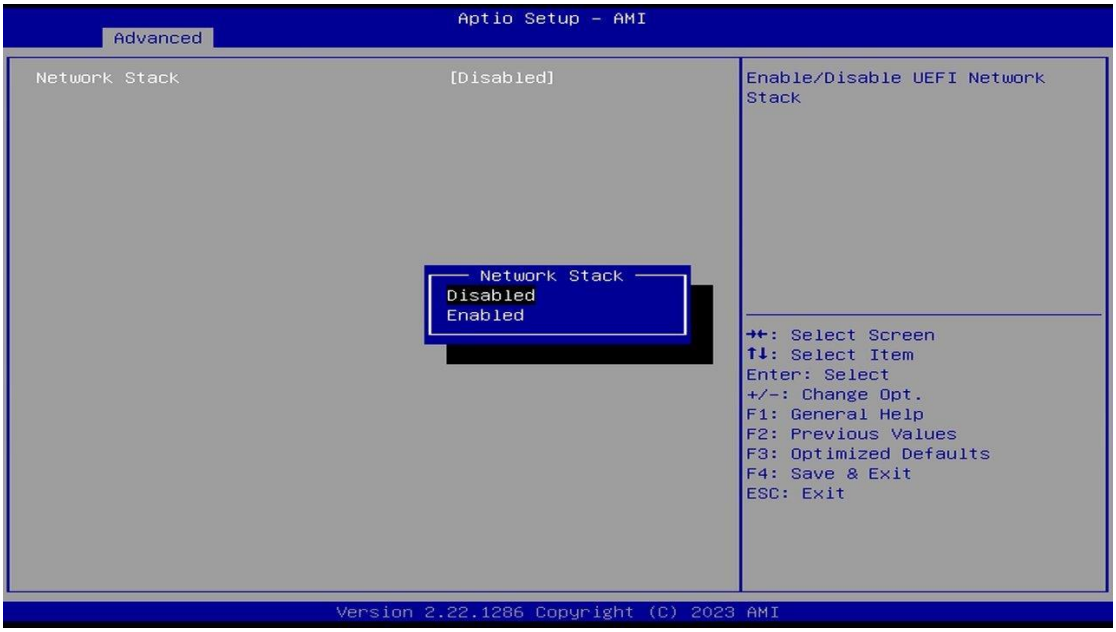
BIOS Setting	Description
Temperatures / Voltages	These fields are the parameters of the hardware monitoring function feature of the motherboard. The values are read-only values as monitored by the system and show the PC health status.
CPU Smart Fan Function SYS Smart Fan Function	Smart Fan Mode Select

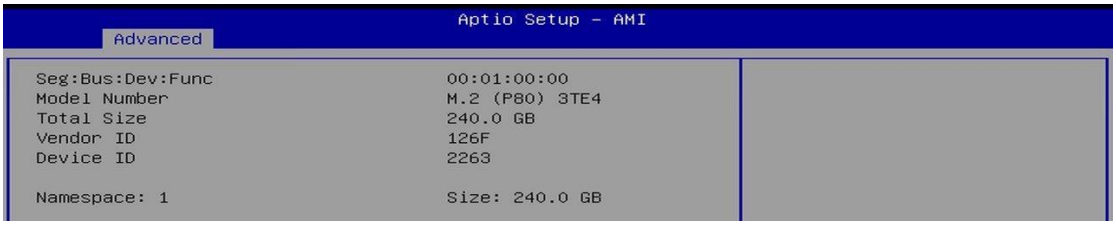
4.4.9 USB Configuration



BIOS Setting	Description
Legacy USB Support	• **Enable:** Enables Ledacy USB Support. • **Auto:** Disables legacy support if no USB devices are connected. • **Disable:** Keeps USB devices available only for EFI applications.
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 for Control, Bulk, and Interrupt transfers.
Device reset time-out	Seconds of delaying execution of start unit command to USB mass storage device.
Device power-up delay	The 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. But for a Hub port, the delay is taken from Hub descriptor.

4.4.10 Network Stack Configuration

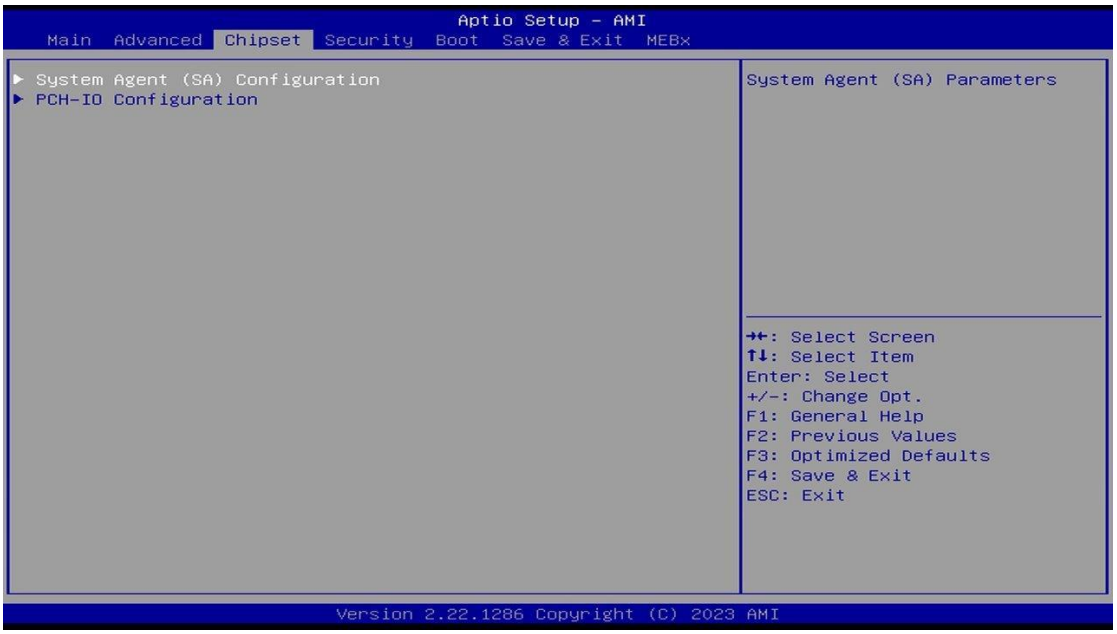




BIOS Setting	Description
Network Stack	Enables / Disables UEFI Network Stack.

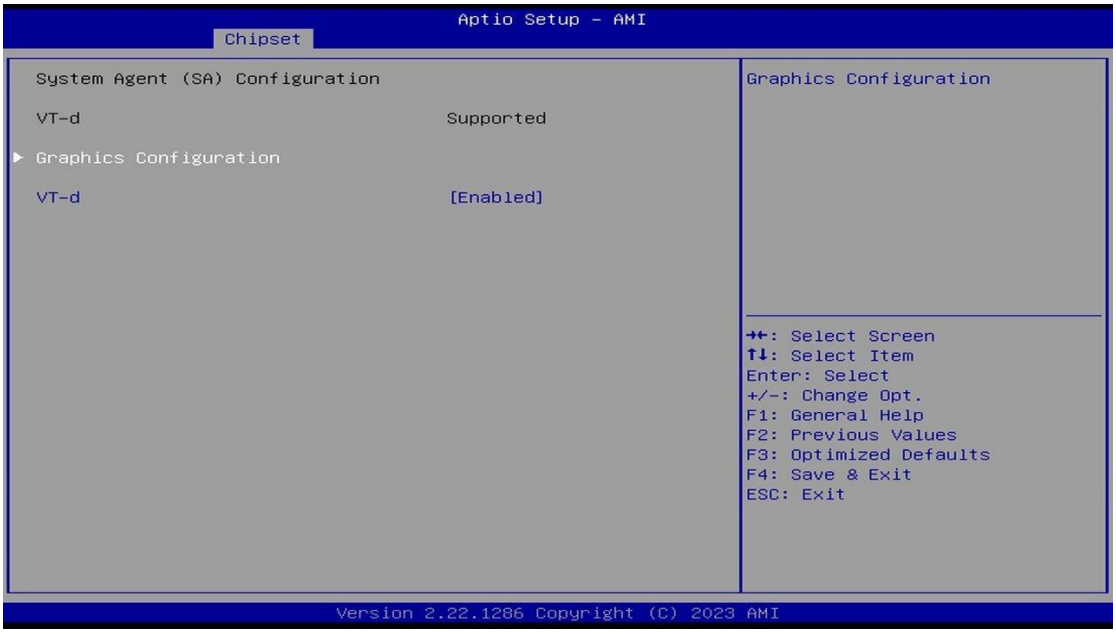
4.4.11 NVMe Configuration

4.5 Chipset Settings



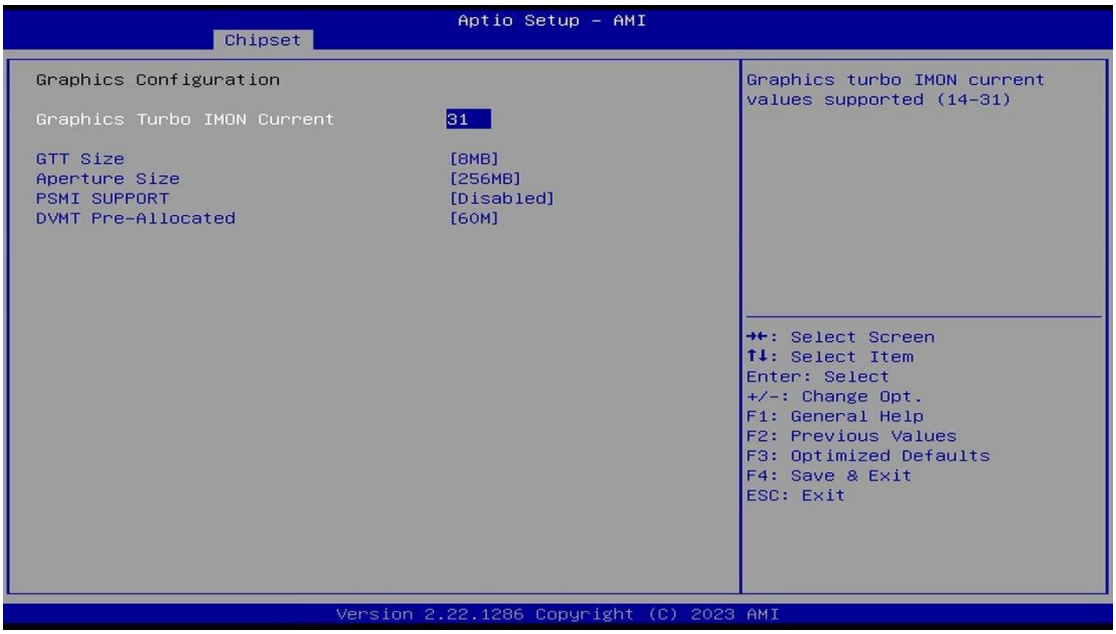
BIOS Setting	Description
System Agent (SA) Configuration	System Agent (SA) parameters
PCH-IO Configuration	PCH parameters

4.5.1 System Agent (SA) Configuration



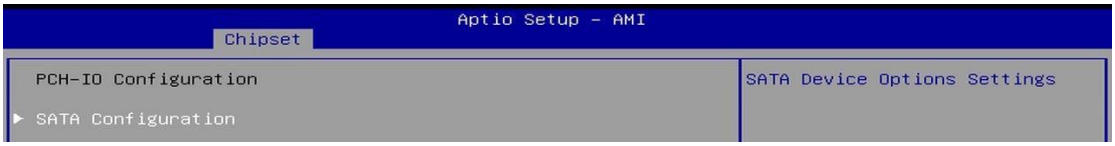
BIOS Setting	Description
System Agent (SA) Configuration	System Agent (SA) Parameters
Graphics Configuration	Configures the graphics settings.
VT-d	Checks if VT-d function on MCH is supported.

4.5.1.1. Graphics Configuration



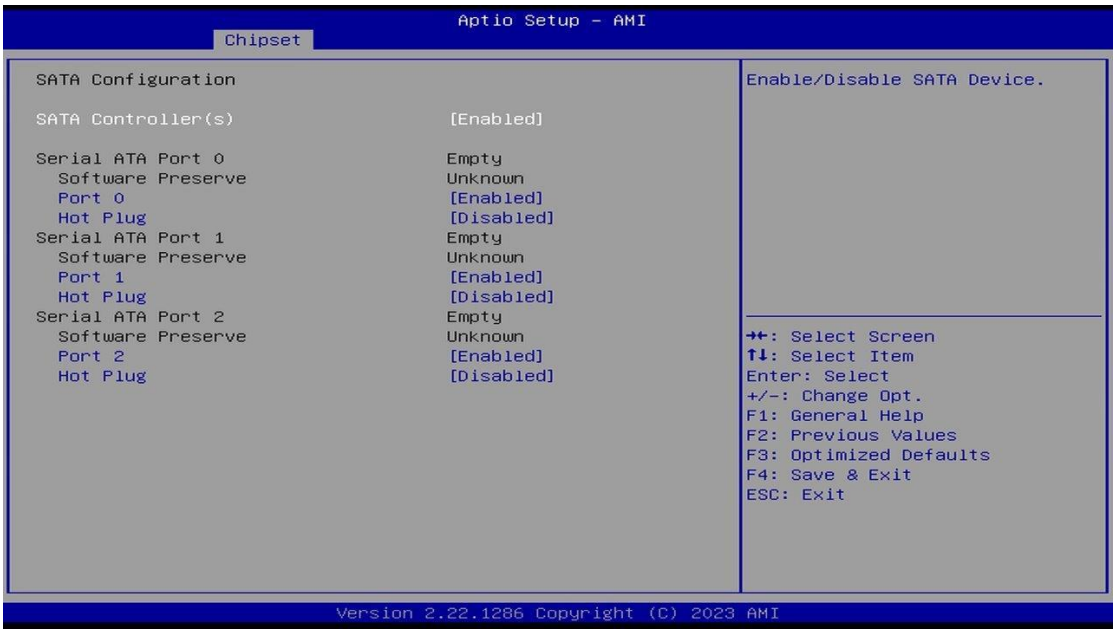
BIOS Setting	Description
Graphics Turbo IMON Current	Graphics turbo IMON current values supported (14-31)
GTT Size	Sets the GTT size as 2 MB, 4 MB, or 8 MB.
Aperture Size	Sets the aperture size as 128 MB, 256 MB, 512 MB, 1024 MB or 2048 MB. **Note:** Above 4 GB MMIO BIOS assignment is automatically enabled when selecting 2048 MB aperture. To use this feature, disable CSM support.
PSMI Support	Options: Enable / Disable
DVMT Pre-Allocated	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the internal graphics device.

4.5.2 PCH-IO Configuration



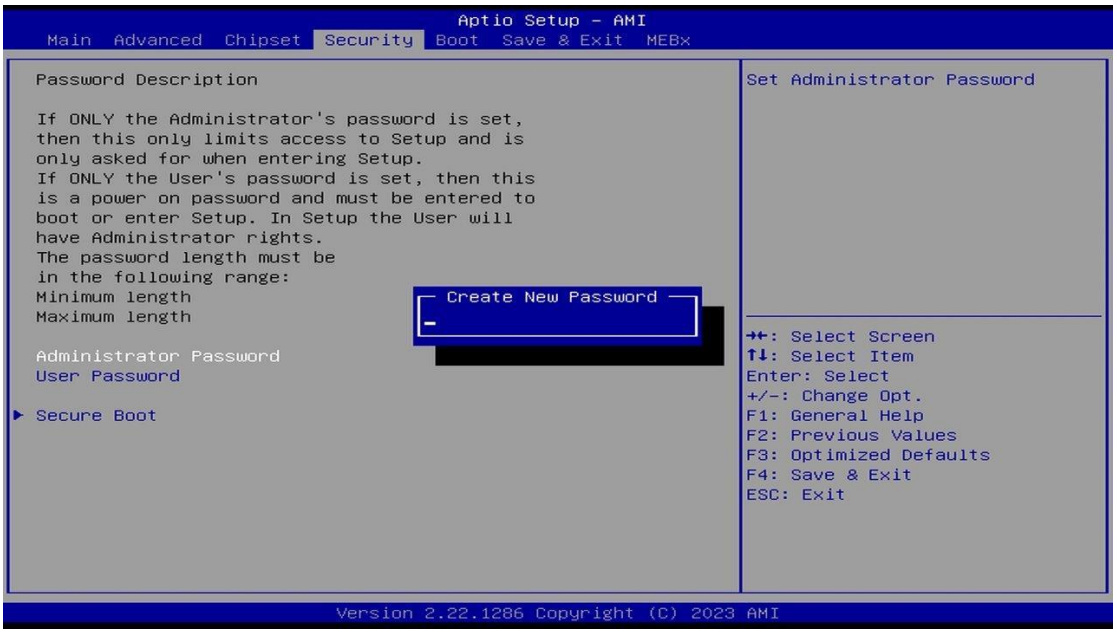
BIOS Setting	Description
SATA Configuration	Configures SATA devices.

4.5.2.1. SATA Configuration:



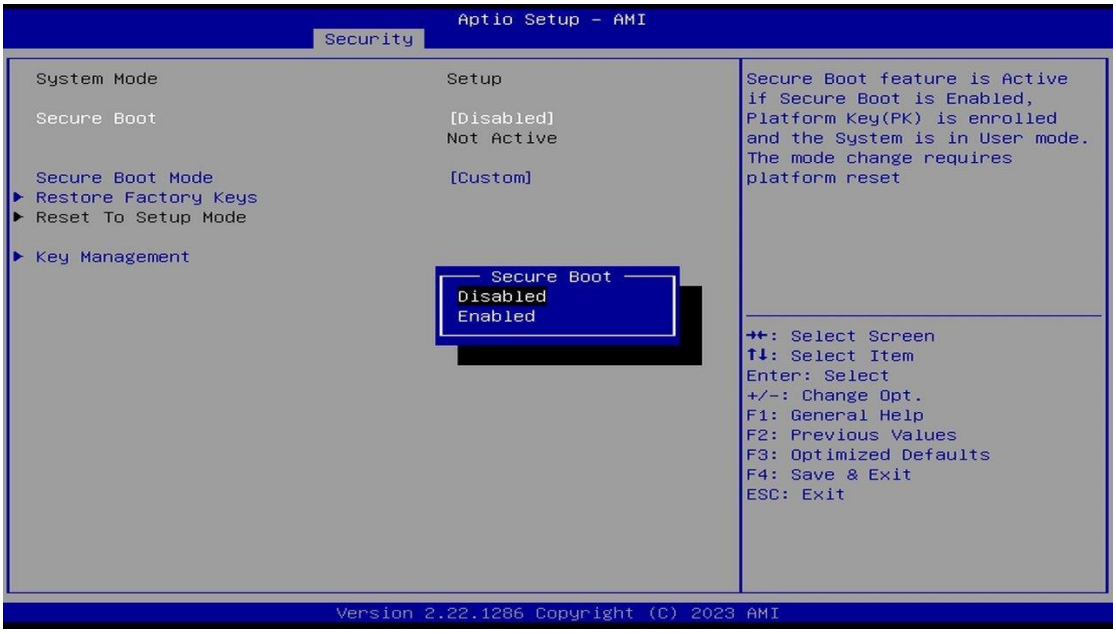
BIOS Setting	Description
SATA Controller(s)	Enables / Disables the SATA device.
Serial ATA Ports	Enables / Disables serial ports.
SATA Ports Hot Plug	Enables / Disables SATA Ports Hot Plug.

4.6 Security Settings

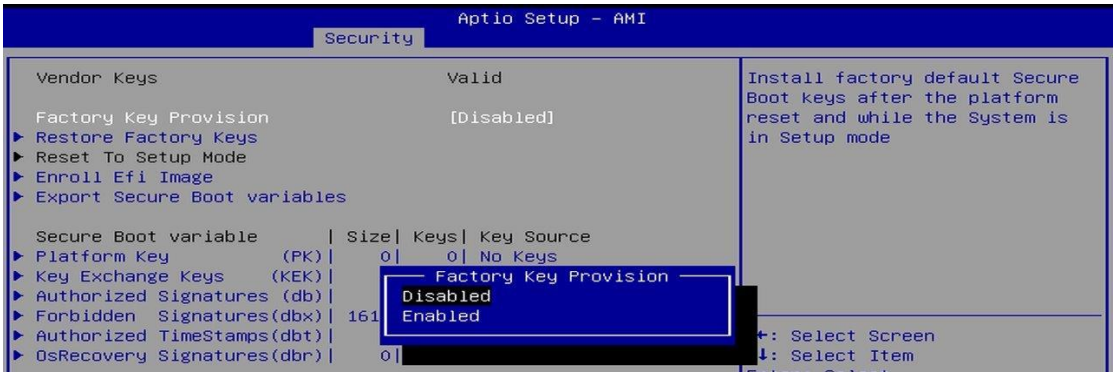


BIOS Setting	Description
Administrator Password	Sets an administrator password for the setup utility.
User Password	Sets a user password.
Secure Boot	Configures Secure Boot.

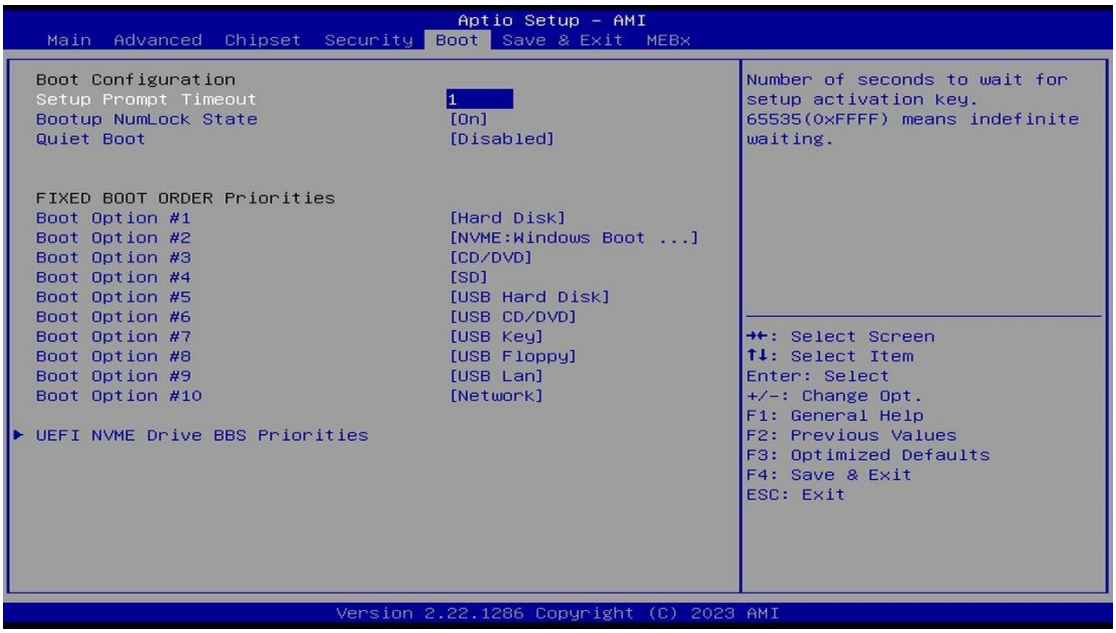
4.6.1 Secure Boot



BIOS Setting	Description
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.
Restore Factory Keys	Forces system to user mode. Install factory default Secure Boot key databases.
Key Management	Enables expert users to modify Secure Boot Policy variables without full authentication.



4.7 Boot Settings

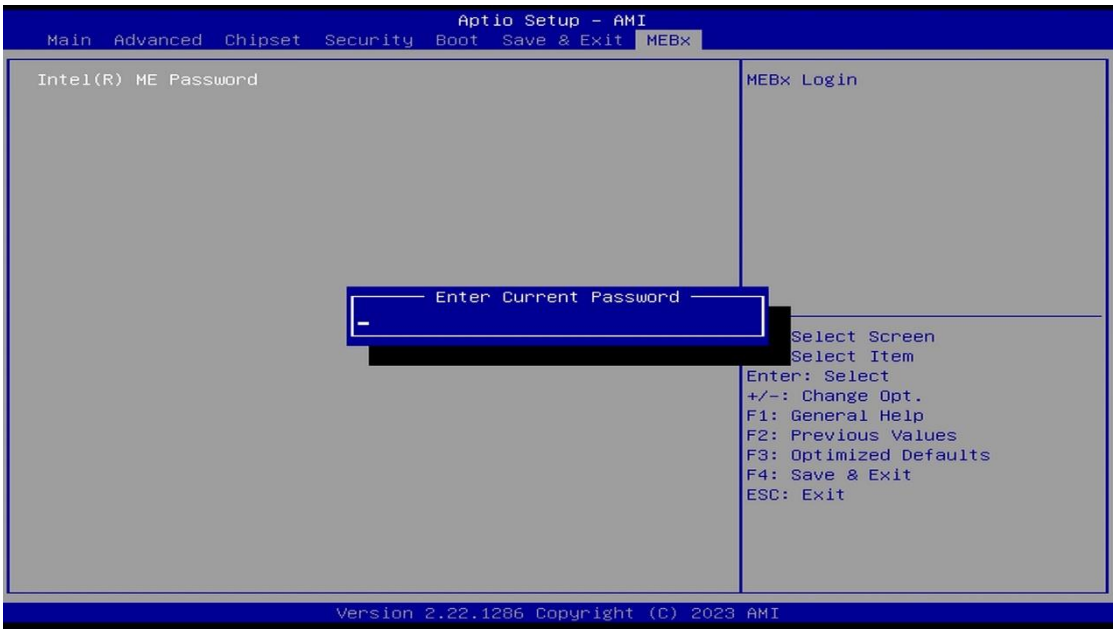


BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535(0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
Boot Option Priorities	Sets the system boot order.
UEFI NVME Drive BBS Priorities	Specifies the boot device priority sequence from available UEFI NVME drives.

4.8 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.

4.9 MEBx


Aptio Setup – AMI
Main Advanced Chipset Security Boot Save & Exit MEBx
Intel(R) ME Password
MEBx Login
Enter Current Password
Select Screen
Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1286 Copyright (C) 2023 AMI

Appendix

This section provides the mapping addresses of peripheral devices and the sample code of watchdog timer configuration.

- I/O Port Address Map
- Interrupt Request Lines (IRQ)

A. I/O Port Address Map

Each peripheral device in the system is assigned a set of I/O port addresses which also becomes the identity of the device. The following table lists the I/O port addresses used.

Address	Device Description
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	Motherboard resources
0x00000A20-0x00000A2F	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
0x00000070-0x00000070	System CMOS/real time clock
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
0x000000B2-0x000000B3	Motherboard resources
0x00000680-0x0000069F	Motherboard resources
0x0000FFFF-0x0000FFFF	Motherboard resources
0x0000FFFF-0x0000FFFF	Motherboard resources
0x0000FFFF-0x0000FFFF	Motherboard resources
0x00001800-0x000018FE	Motherboard resources
0x0000164E-0x0000164F	Motherboard resources
0x00000800-0x0000087F	Motherboard resources
0x000000F0-0x000000F0	Numeric data processor
0x0000F050-0x0000F057	Standard SATA AHCI Controller
0x0000F040-0x0000F043	Standard SATA AHCI Controller
0x0000F020-0x0000F03F	Standard SATA AHCI Controller
0x000003F8-0x000003FF	Communications Port (COM1)
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer

Address	Device Description
0x00000000-0x00000CF7	PCI Express Root Complex
0x00000020-0x00000021	Programmable interrupt controller
0x00000024-0x00000025	Programmable interrupt controller
0x00000028-0x00000029	Programmable interrupt controller
0x0000002C-0x0000002D	Programmable interrupt controller
0x0000002E-0x0000002F	Motherboard Resources
0x00000030-0x00000031	Programmable interrupt controller
0x00000034-0x00000035	Programmable interrupt controller
0x00000038-0x00000039	Programmable interrupt controller
0x0000003C-0x0000003D	Programmable interrupt controller
0x00000040-0x00000043	System timer
0x00000060-0x00000060	Standard PS/2 Keyboard
0x00000061-0x00000061	Motherboard resources
0x00000063-0x00000063	Motherboard resources
0x00000064-0x00000064	Standard PS/2 Keyboard
0x00000067-0x00000067	Motherboard resources
0x00000070-0x00000070	Motherboard resources
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
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
0x000000B2-0x000000B3	Motherboard resources
0x000000B4-0x000000B5	Programmable interrupt controller
0x000000B8-0x000000B9	Programmable interrupt controller
0x000000BC-0x000000BD	Programmable interrupt controller
0x000002F8-0x000002FF	Communication Port (COM2)
0x000003F8-0x000003FF	Communication Port (COM1)
0x000004D0-0x000004D1	Programmable interrupt controller
0x00000680-0x0000069F	Motherboard resources
0x00000A00-0x00000A0F	Motherboard resources

0x00000A20-0x00000A2F	Motherboard resources
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x0000164E-0x0000164F	Motherboard resources
0x00001800-0x000018FE	Motherboard resources
0x00001854-0x00001857	Motherboard resources
0x00002000-0x000020FE	Motherboard resources
0x00004000-0x0000403F	Intel(R) Iris (R) Xe Graphics
0x00004060-0x0000407F	Standard SATA AHCI Controller
0x00004080-0x00004083	Standard SATA AHCI Controller
0x00004090-0x00004097	Standard SATA AHCI Controller
0x00004060-0x0000407F	Standard SATA AHCI Controller
0x0000EFA0-0x0000EFBF	Intel(R) SMBus – A0A3
0x0000FFF8-0x0000FFFF	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 1	Standard PS/2 Keyboard
IRQ 3	Communications Port (COM2)
IRQ 4	Communications Port (COM1)
IRQ 12	Microsoft PS/2 Mouse
IRQ 14	Intel(R) GPIO Controller 34Cs
IRQ 16	High Definition Audio Controller
IRQ 17	USB Synopsys Controller
IRQ 19	Intel(R) Active Management Technology SOL (COM3)
IRQ 28	Trusted Platform Module 2.0
IRQ 55 ~ IRQ 204	Microsoft ACPI-Compliant System
IRQ 256 ~ IRQ 511	Microsoft ACPI-Compliant System
IRQ 4294967246	Intel(R) Management Engine Interface
IRQ 4294967247	Intel(R) Ethernet Connection (132) I219-V
IRQ 4294967248~53	Intel(R) I211 Gigabit Network Connection
IRQ 4294967254~85	Standard SATA AHCI Controller
IRQ 4294967256	Intel(R) Iris (R) Xe Graphics
IRQ 4294967287~88	Intel(R) USB 3.10 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967289	Intel(R) PCI Express Root Port #7 – A0Be
IRQ 4294967289	Intel(R) Management Engine Interface
IRQ 4294967291~94	PCI Express Root Port