CMI211-1005

Intel® Core™ Ultra 200H Mini-ITX Systems

User's Manual

Version 1.0
(February 2026)

iBASE

iBASE

Copyright

Disclaimer

Trademarks

iBASE

Compliance

CE

This product has passed CE tests for environmental specifications and regulatory 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 A device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the 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, which prohibit the 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 on a stable, level surface to prevent it from falling, causing serious damage.

- Slots and openings on the chassis are for ventilation. Do not block or cover these openings. Make sure you leave plenty of space around the device for ventilation. Never insert 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 cable, as 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.

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:

Do not disassemble, repair, or modify 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.

Danger of explosion

Replace only with the same or an equivalent type recommended by the manufacturer. Dispose of used batteries according to local regulations.

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.

- Third-party parts:

12-month (1-year) warranty from delivery for the third-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 for 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)

If repair service is required, you can download the RMA form from the IBASE website. Fill out the form and contact your distributor or sales representative.

iBASE

Table of Contents

Chapter 1
General Information

The information provided in this chapter includes:

- Features
- Specifications
- Product View
- Dimensions

1.1 Introduction

The CMI211-1005 is a compact and expandable Mini-ITX industrial system built on an IBASE Mini-ITX motherboard and powered by Intel® Core™ Ultra 200H series mobile processors with a thermal design power of up to 65W. It supports up to 96GB of DDR5 cSO-DIMM memory and offers flexible expansion with PCIe Gen4 x4 and three M.2 slots (E-Key and dual M-Key). The system provides rich I/O connectivity, including USB Type-C, USB 3.2, USB 2.0, COM ports, HDMI, and DisplayPort (DP++), along with dual/tri 2.5GbE LAN configurations using Intel® I226 controllers with optional iAMT support. Designed for space-constrained industrial and embedded applications, the CMI211-1005 delivers a balanced combination of performance, expandability, and connectivity in a rugged, compact form factor.

1.2 Features

- Mini-ITX system with MI1005AF Mini-ITX motherboard
- Intel® Core™ Ultra 200H series mobile onboard processors, up to 65W
- 2x DDR5 cSO-DIMM, Max. 96GB, Non-ECC
- Supports 2x Type-C, 1x HDMI and 1x DisplayPort(DP++)
- LAN 1: Intel® I226LM, supports 2.5G and iAMT
- LAN 2 / LAN 3: Intel® I226V, supports 2.5G only
- 4x USB 3.2, 2x USB Type-C, 4x USB 2.0, 2x COM
- Supports 1x PCIe (x4) [Gen4.0]
- 3x M.2 (E-Key @2230 and 2x M-Key @2280 & 2242)

1.3 Specifications

Model CMI211-1005AFM	Barebone system with MI1005AF+ IP201 riser card, w/o SSD, memory, w/ 250W PSU, 2.5" storage holder, 1x PCI-E (x4) expansion slot (RoHS2)
System	
System	• CMI211-1005
Mainboard	• MI1005AF
Processor	• Intel® Core™ Ultra 200H series mobile Processors
PCH	• N/A
System Speed	• Up to 5.4 GHz (Core™ Ultra 9 285H)
Memory	• 2x DDR5 SO-DIMM sockets, Up to DDR5-6400 cSO-DIMM memory module, Max. 96GB
I/O Interface	
Front-side Panel I/O	• 2x USB 2.0 ports • 2x Antenna holes
Rear-side Panel I/O	• 1x AC-inlet • 1x Power switch (rocker switch) • 1x Power LED indicator • 1x Storage LED indicator • 2x USB 2.0 ports • 2x DB9 for COM#1/COM#2 (COM#1 with RS232/422/485, select from BIOS) • 1x DP + 1x HDMI • 2x (USB Type-C + USB 3.2 Type-A + RJ45 connector) • 1x (Dual USB 3.2 Type-A + RJ45 connector) • 1x triple type jack for Audio connector • 2x Antenna holes
Storage Interface	
SATA	• 1x 2.5" storage drive bay
M.2	• 2x M.2 (M2280 & M2242)

Expansion	
PCIe Expansion	• 1x PCI-E (x4) [Gen.4.0] expansion slot
M.2	• 1x E-key E2230; 2x M-key (M2280 & M2242)
Add-on card Max. Size	• 111mm (W) x 168mm (D) x 18mm (H)
Power	
ATX Power	• Industrial 250W ATX power supply
	• Input voltage: 100V ~ 240V
	• Input frequency: 47Hz ~ 63Hz
	• Compatible with IEC62368-1 / EN62368-1
Mechanical	
Construction	• SECC
Chassis Color	• Black
Mounting Type	• Wall mount & Desktop
Dimensions	• 300mm (W) x 205mm (D) x 72mm (H)
	• 11.81" (W) x 8.07" (D) x 2.83" (H)
Weight	• 3.2 kg
Environment	
Operating Temperature	• 0°C ~ 45°C (32°F ~ 113°F)
Storage Temperature	• -20°C ~ 80°C (-4°F ~ 176°F)
Humidity	• 5% ~ 90% @45°C (non-condensing)
Vibration	• Non-operating: 1.0 grms / 5~500Hz / random
	• Operating: 0.25 grms / 5~500Hz / random
Certification	
Certification	• CE / LVD / FCC Class B

All specifications are subject to change without prior notice.

1.4 System View

Top View
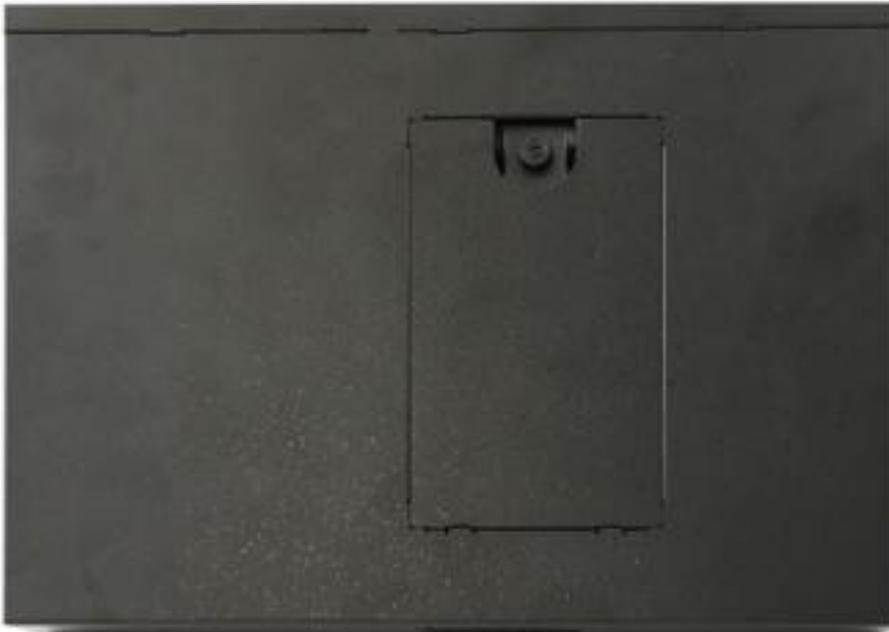
Rear View

Rear Side Panel I/O View
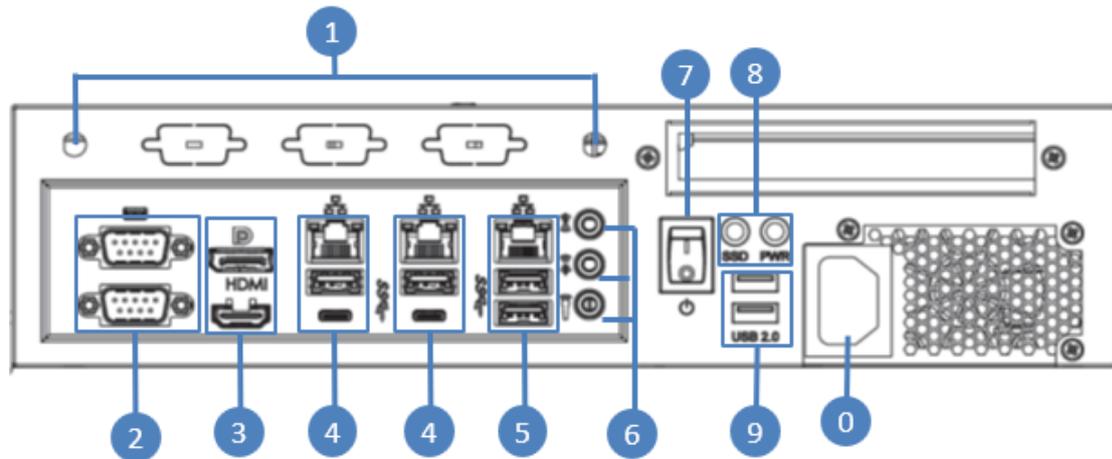
No.	Name	No.	Name
1	Antenna Holes	6	Audio Jacks (From top to bottom: Line-In, Line-Out, Mic)
2	COM#1/COM#2 (COM#1 with RS232/422/485	7	Power switch (rocker switch)
3	DP (top) HDMI (bottom)	8	SSD LED indicator Power LED indicator
4	USB Type-C + USB 3.2 Type-A + RJ45	9	2x USB 2.0 ports
5	Dual USB 3.2 Type-A + RJ45	0	AC-inlet

Side View View

1.5 Dimensions

Unit: mm
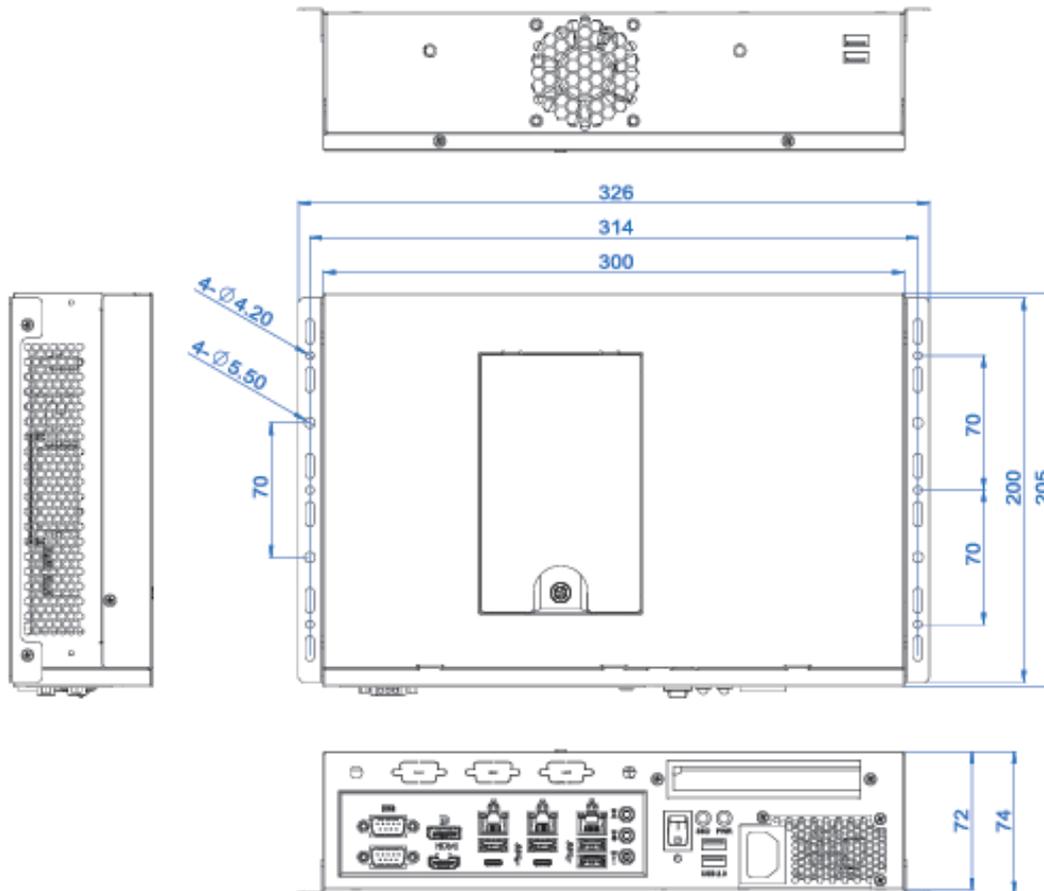
Chapter 2
Hardware Installation

The information provided in this chapter includes:

- Essential installations
  - HDD Installation
  - Memory Installation
  - WiFi / 4G / 5G Antenna Installation
  - PCIe Expansion Card Installation
  - Fan Replacement
  - Mounting Brackets Installation

IBASE

2.1 Essential Installations

Release the four screws shown below to remove the cover for all installations except for that of the HDD. After installation, secure the device cover.
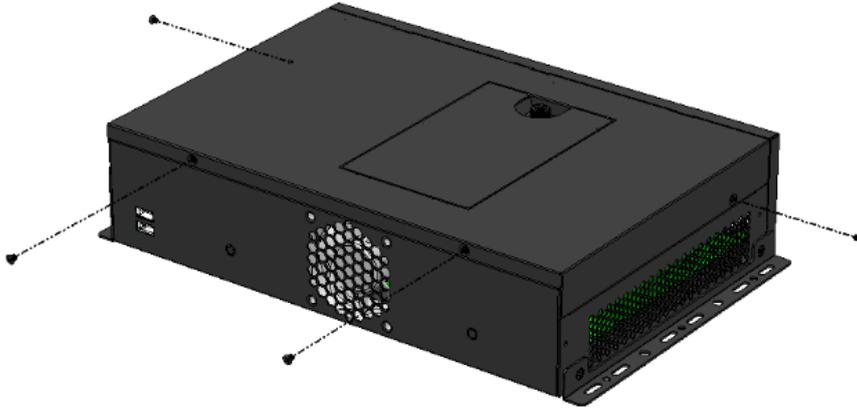
Note: This illustration is for reference only. The I/O connectors may not match the actual system configuration. The image is intended solely to show the screw locations required for disassembly.

2.1.1   HDD Installation

1. Loosen the single screw to release the HDD tray. Loosen the 4 screws holding the HDD. Install the HDD by fixing it with the screws that have been removed and connect the related cables. Close and secure the tray.

2.1.2 Memory Installation

1. Remove the system cover, locate the memory slot.

2. Open the retaining clips at both ends of the socket. Align the notch on the memory module with the key in the socket. Insert the module vertically and press firmly until both retaining clips lock into place.
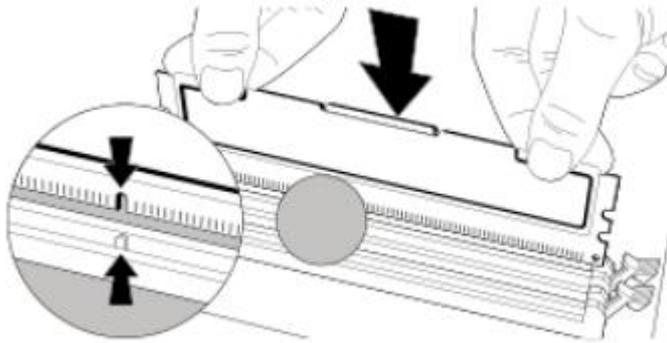
To remove the module, press the clips outwards with both hands.

2.1.3 WiFi / 4G / 5G Antenna Installation

Thread the WiFi / 4G / 5G 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. After installation, secure the device cover.

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

2. Apply adhesive around here.
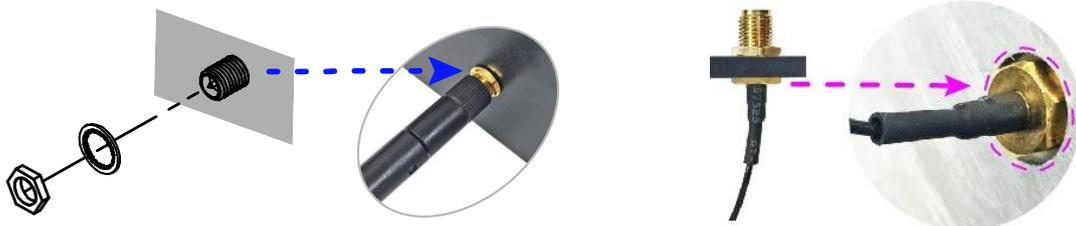
Info: The diameter of the nut is around 6.35 mm (0.25"-36UNC).

2.1.4   PCIe Expansion Card Installation

Release the screw holding the expansion slot bracket after removing the system chassis cover. Then install the expansion card and fix it with the screw that we removed earlier. Secure the system cover.
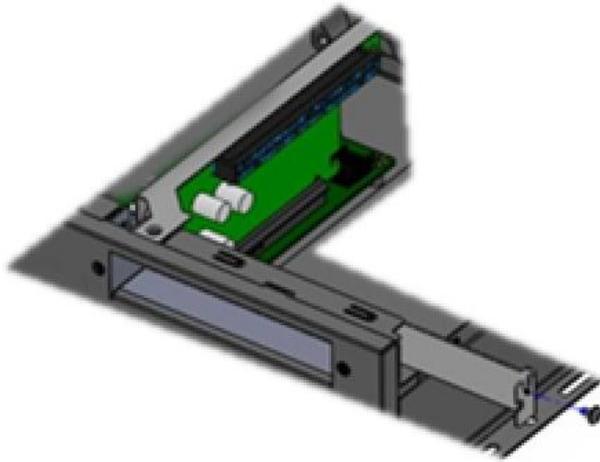
Note: The figure is for screw-location reference only; I/O layout may differ.

2.1.5   Fan Replacement

Remove the system cover and release the 4 fan screws. Replace the fan and tighten it with the screws that were removed. Replace the system cover.
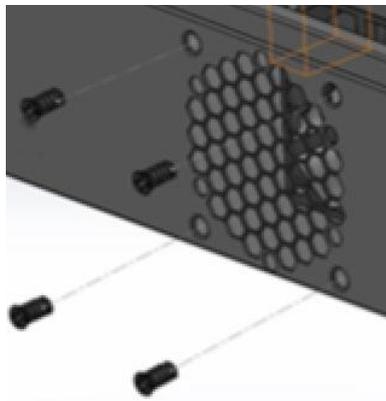
2.1.6   Mounting Brackets Installation

Wall Mount Installation:

Attach the wall mounting brackets to your CMI211-1005 System, and secure them with the supplied screws as shown below.

Note: The figure is for screw-location reference only; I/O layout may differ.

Prepare at least four screws (M3, 6 mm) to mount the device on wall .

2.2 Setting Jumpers

Configure your MI1005AF by setting jumpers according to your specific needs and applications. If you are unsure about the optimal configuration, please contact your supplier for assistance.

Jumpers are short-length conductors consisting of metal pins mounted on a non-conductive base on the circuit board. Jumper caps are used to enable or disable certain functions and features. For 3-pin jumpers, you can short either **Pin 1–2** or **Pin 2–3** depending on the required setting.

Pin#   1   2   3
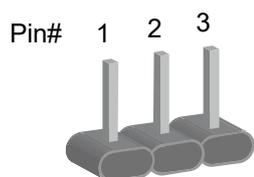
A 3-pin jumper   **A jumper cap**

Refer to the illustration below to set jumpers.

Position	Oblique view	Illustration
Open		□ ○ ○ 1 2 3
1-2		■ ● ○ 1 2 3
2-3		□ ● ● 1 2 3
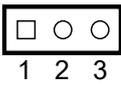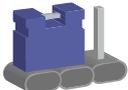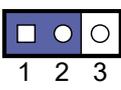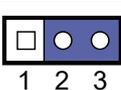
When two pins of a jumper are covered by a jumper cap, the jumper is **closed** (i.e., turned **On**).
When the jumper cap is removed, the jumper is **open** (i.e., turned **Off**).

2.3 Jumper and Connector Locations
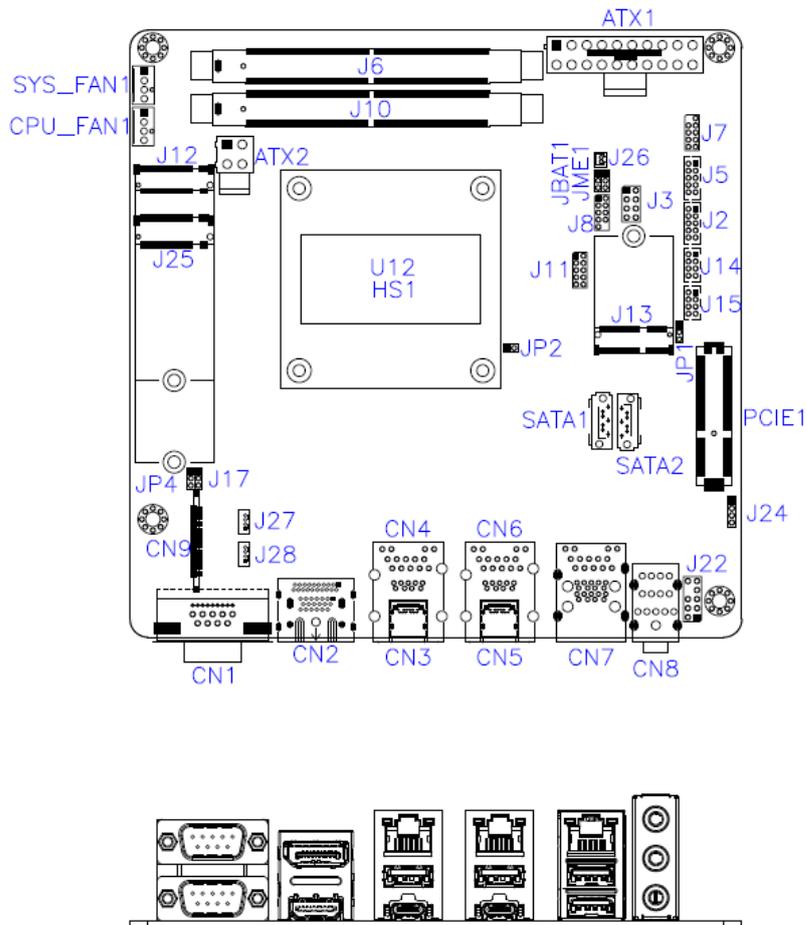
2.4 Jumpers Quick Reference

Jumper	Function
JBAT1	Clear CMOS
JME1	Clear ME
JP1	AT/ATX Select
JP4	EDP Panel Power Select

2.4.1 Clear CMOS Contents (JBAT1)
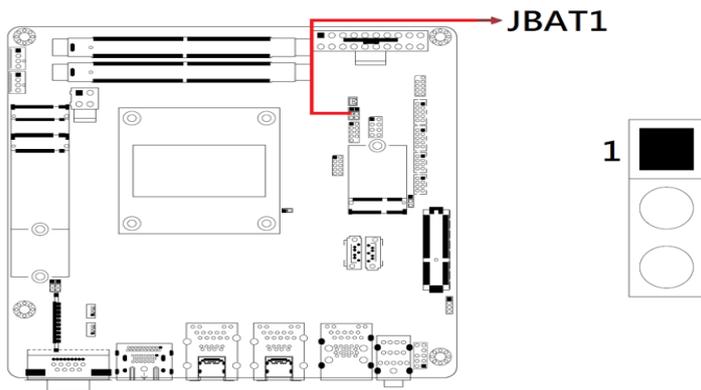
Function	Pin closed	Illustration
Normal	1-2	
Clear CMOS	2-3	

2.4.2   Clear ME Contents (JME1)
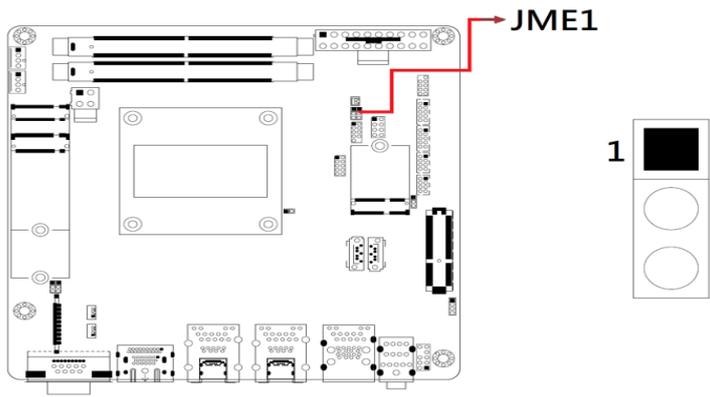
Function	Pin closed	Illustration
Normal	1-2	
Clear ME	2-3	

2.4.3   ATX & AT Power Mode Selection (JP1)
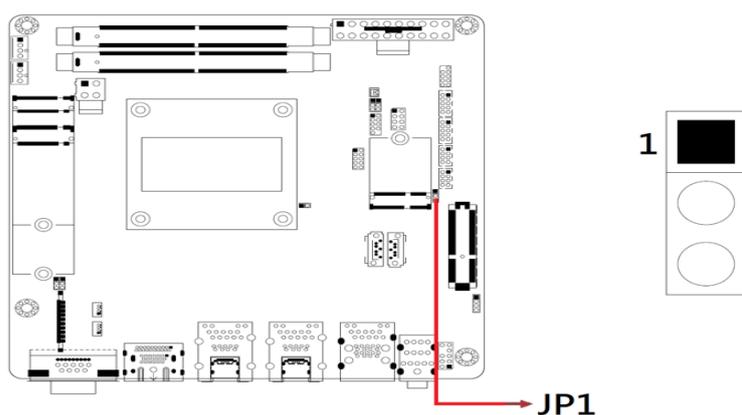
Function	Pin closed	Illustration
ATX (default)	1-2	
AT	2-3	

2.4.4   EDP Panel Power Select (JP4)
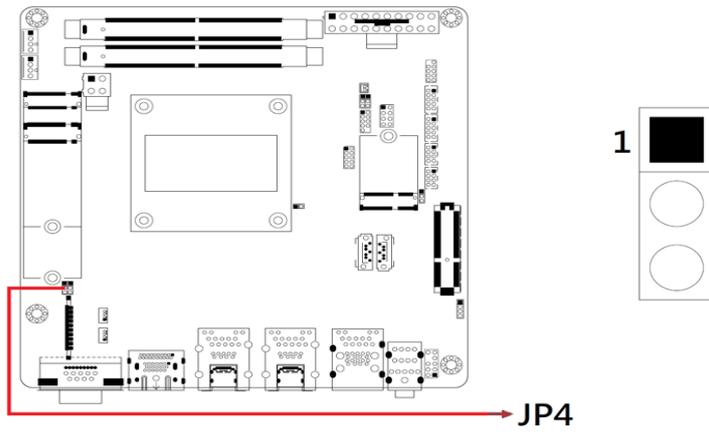
Function	Pin closed	Illustration
+3.3V(default)	1-2	
+5V	2-3	

2.5 Connectors Quick Reference

Connector	Function
CN1	COM1 & COM2 RS-232/422/485 Ports
CN2	DisplayPort & HDMI Port
CN3, CN5	USB Type-C Connector
CN4	2.5 Gigabit LAN (Intel I226-V) + USB 3.2
CN6	2.5 Gigabit LAN (Intel I226-LM) + USB 3.2
CN7	2.5 Gigabit LAN (Intel I226-V) + USB 3.2
CN8	HD Audio Connector
CN9	EDP Panel Connector
J2, J5	COM3 & COM4 RS-232 Ports
J3	Front Panel Settings Connector
J6, J10	DDR5 SO-DIMM Slots
J7	SPI Flash Connector (Factory use only)
J8	80 Port Debug (Factory use only)
J11	Digital I/O Connector
J12	M.2 M2280 Slot
J13	M.2 E2230 Slot
J25	M.2 M2242 Slot
J14, J15	USB 2.0 Connector (DF11-8S-PA66H)
J26	Battery Connector
ATX1	ATX Power Connector
J22	Audio Pin Header for Chassis Front Panel
ATX2	CPU Power Connector
J24, J27, J28	Factory use only
SATA1, SATA2	SATA III Connectors
CPU_FAN1, SYS_FAN1	Fan Power Connectors
PCIE1	PCIe (x4) Slot

2.5.1 COM1 & COM2 RS-232/422/485 Ports (CN1)

CN1
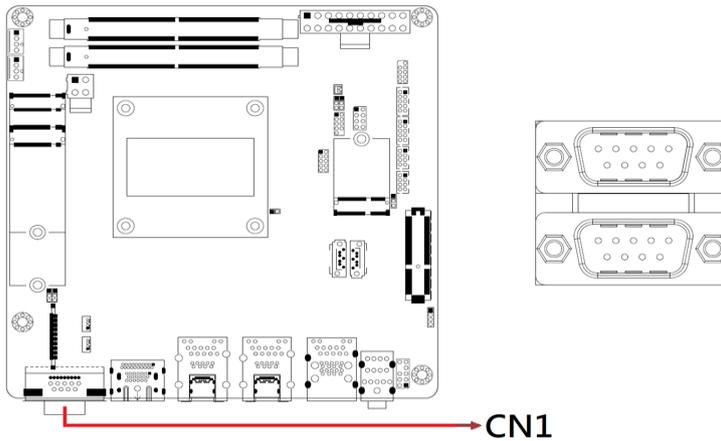
Pin	Signal Name	Pin	Signal Name
1	DCD, Data carrier detect	6	DSR, Data set ready
2	RXD, Receive data	7	RTS, Request to send
3	TXD, Transmit data	8	CTS, Clear to send
4	DTR, Data terminal ready	9	RI, Ring indicator
5	Ground		

COM1/COM2 RS-232/422/485 are jumperless, configurable in BIOS.

Pin	Signal Name		
	RS-232	**RS-422**	**RS-485**
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	TX	RX+	NC
4	DTR	RX-	NC
5	Ground	Ground	Ground
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

2.5.2 DisplayPort & HDMI Port (CN2)

CN2
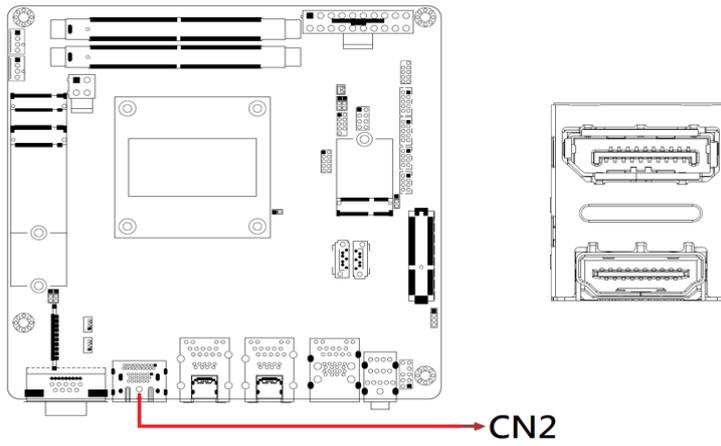
2.5.3 USB Type-C Connector (CN3, CN5)

CN5
CN3
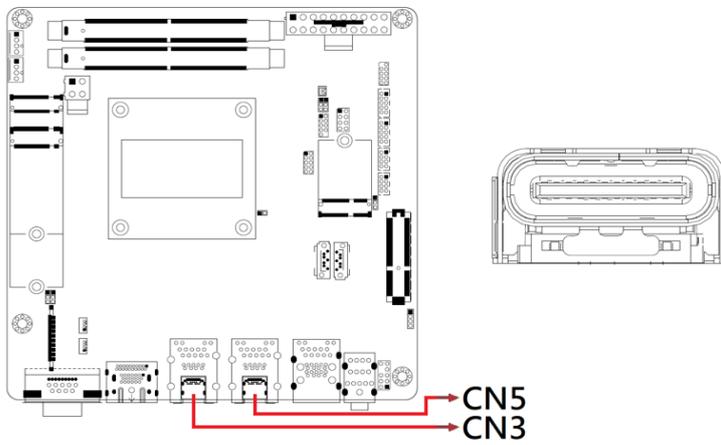
2.5.4　2.5 Gigabit LAN (Intel I226-V) + USB3.2 (CN4, CN6)

CN6

CN4
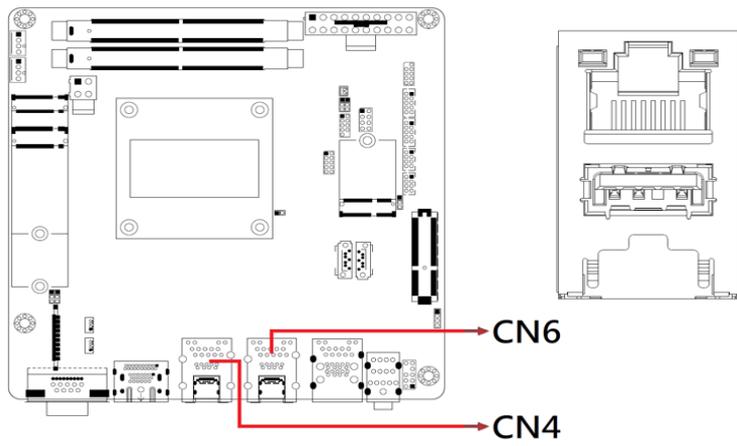
2.5.5　2.5 Gigabit LAN (Intel I226-LM) + USB3.2 (CN7)

CN7
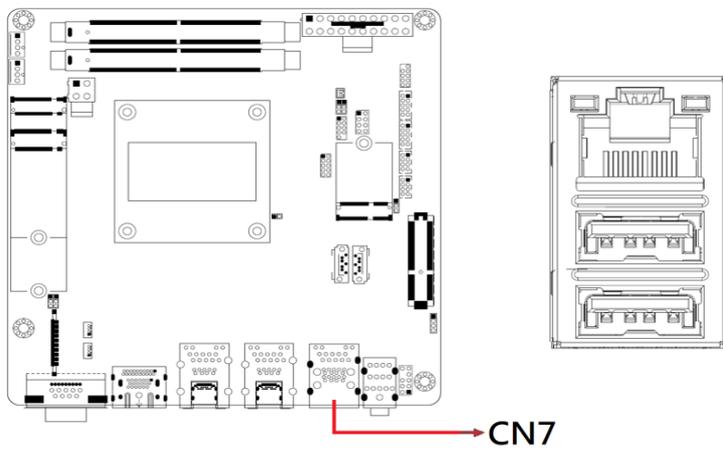
2.5.6　HD Audio Connector (CN8)

CN8
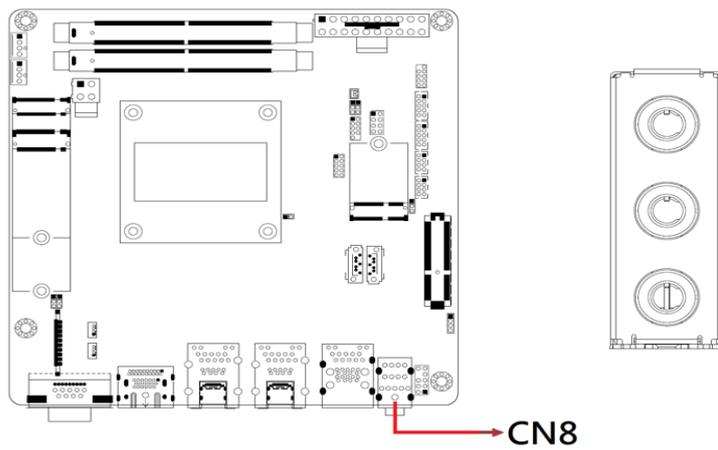
2.5.7   EDP Panel Connector (CN9)
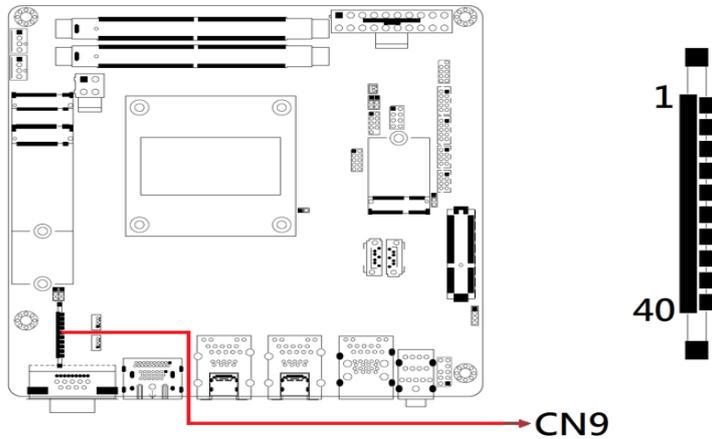
Remarks: KEL_SSL00-40S

Pin	Signal Name	Pin	Signal Name
1	eDP Vcc	21	TXN0
2	eDP Vcc	22	TXP1
3	eDP Vcc	23	Ground
4	eDP Vcc	24	AUXP
5	eDP Vcc	25	AUXN
6	Ground	26	NC
7	Ground	27	+3.3V
8	Ground	28	EDP BKLT (+12V)
9	Ground	29	NC
10	Hot Plug detect	30	Ground
11	Ground	31	+5V
12	TXN3	32	NC
13	TXP3	33	Back Light Control
14	Ground	34	Back Light Enable
15	TXN2	35	EDP BKLT (+12V)
16	TXP2	36	+3.3V
17	Ground	37	Ground
18	TXN1	38	NC
19	TXP1	39	NC
20	Ground	40	NC

2.5.8   Front Panel Settings Connector (J3)
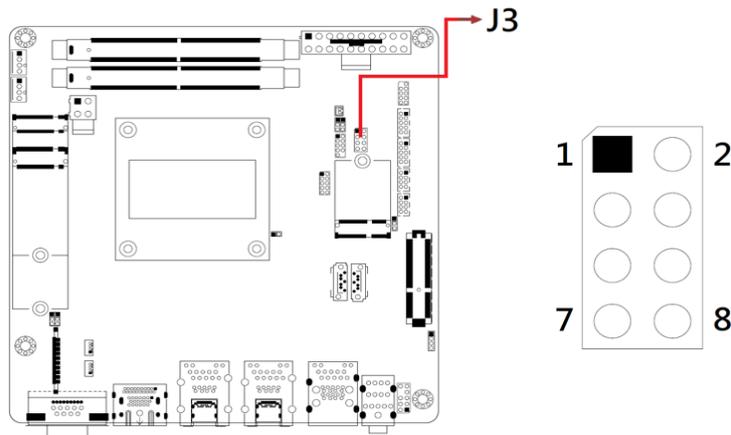
Pin	Signal	Pin	Signal
1	Power BTN-	2	Power BTN+
3	HDD LED+	4	HDD LED-
5	Reset BTN-	6	Reset BTN+
7	Power LED+	8	Power LED-

J3 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)
The 2 pins 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 lights up when the system turns on.

2.5.9 COM3 (J2) & COM4 (J5) RS-232 Ports
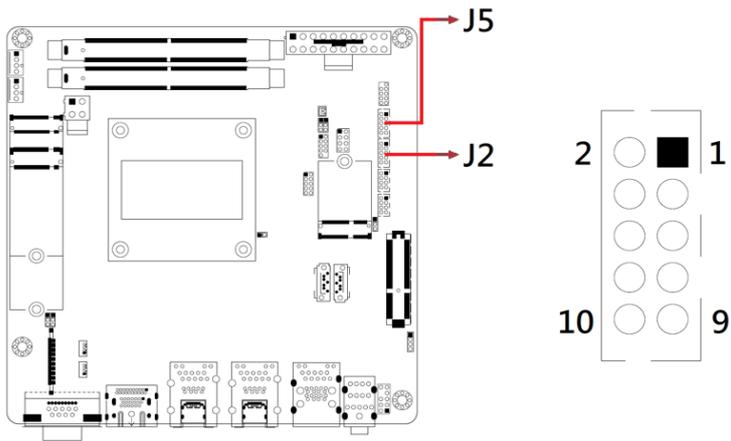
Pin	Signal Name	Pin	Signal Name
1	DCD, Data carrier detect	2	RXD, Receive data
3	TXD, Transmit data	4	DTR, Data terminal ready
5	Ground	6	DSR, Data set ready
7	RTS, Request to send	8	CTS, Clear to send
9	RI, Ring indicator	10	Not Used

2.5.10 DDR5 SO-DIMM Slot (J6 / J10)
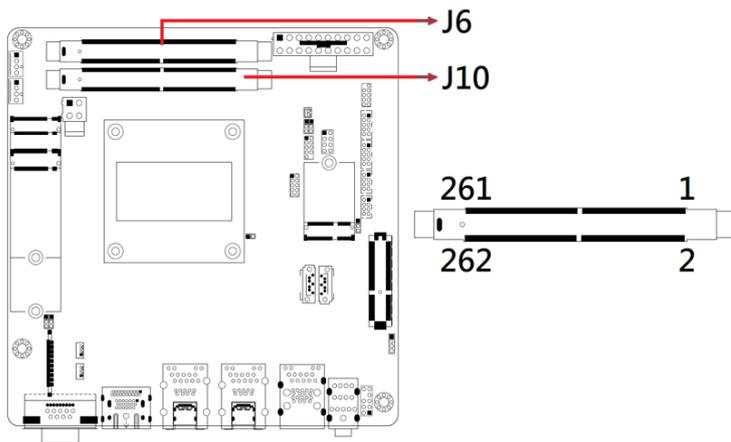
2.5.11 SPI Flash Connector (J7)
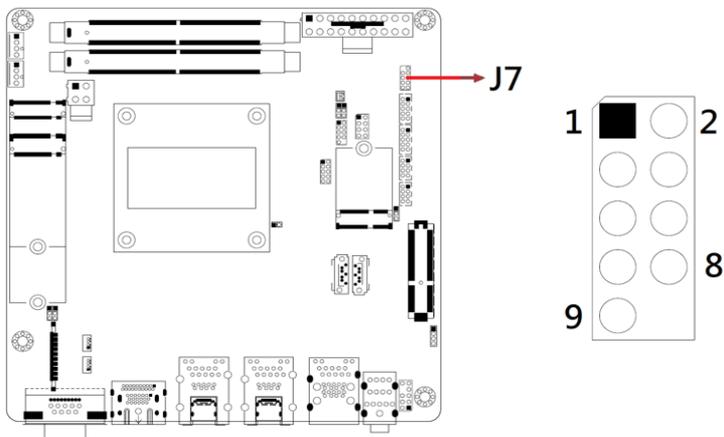
Note: J7 is for Factory use only.

2.5.12 80 Port Debug (J8)
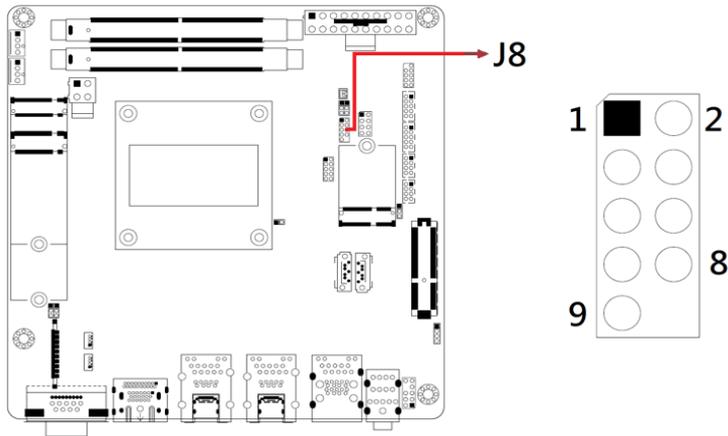
Note: J8 is for factory use only.

2.5.13 Digital I/O Connector (J11)
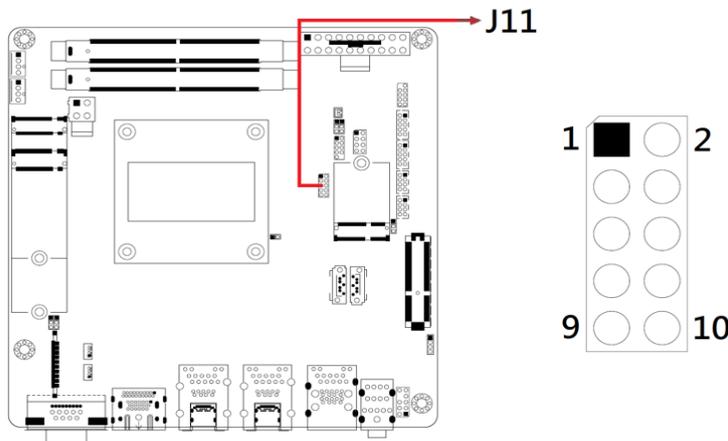
Pin	Signal	Pin	Signal
1	Ground	2	+5V(0.5A)
3	OUT3	4	OUT1
5	OUT2	6	OUT0
7	IN3	8	IN1
9	IN2	10	IN0

2.5.14   M.2 M2280 Slot (J12)
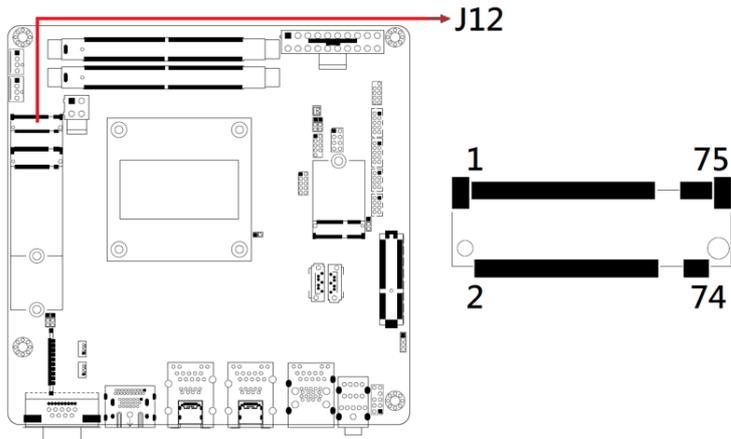
*J12 supports NVME

2.5.15   M.2 E2230 Slot (J13)
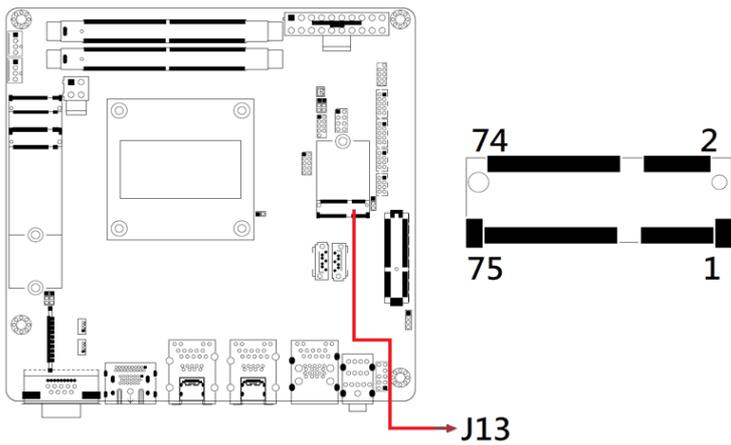
*J13 supports USB2.0 & PCIE x1

2.5.16 USB 2.0 Connector (J14, J15)
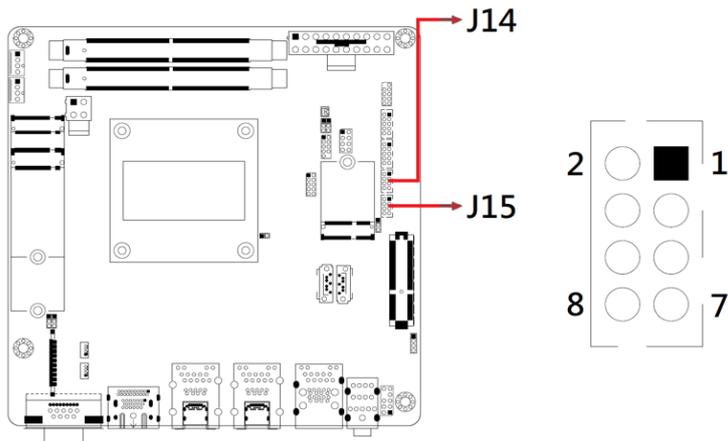
* Connector type: DF11-8S-PA66H

Pin	Signal	Pin	Signal
1	VCC(0.5A)	2	Ground
3	D0-	4	D1+
5	D0+	6	D1-
7	Ground	8	VCC(0.5A)

2.5.17 M.2 M-key 2242 Slot (J25)
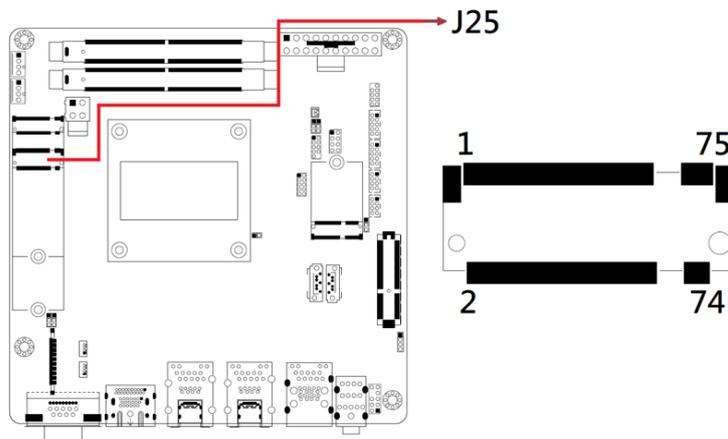
*J25 supports NVME

2.5.18 Battery Connector (J26)
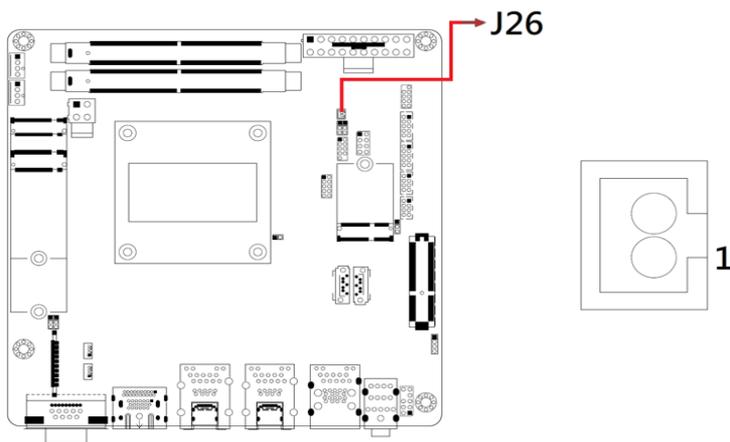
Pin	Signal Name	Pin	Signal Name
1	Battery (3V)	2	Ground

2.5.19 ATX Power Connector (ATX1)
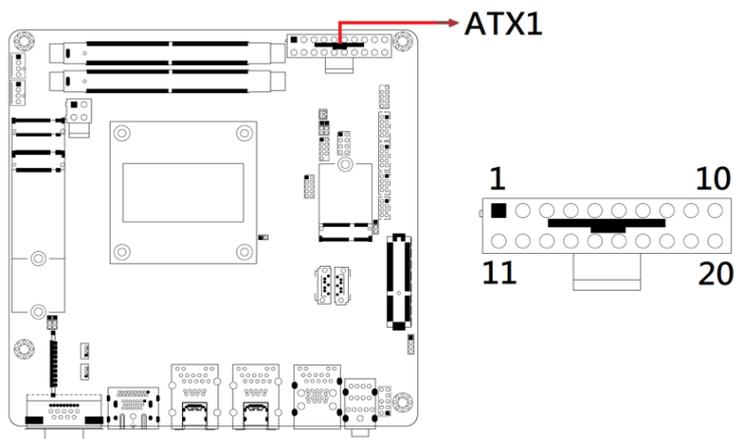
Pin	Signal Name	Pin	Signal Name
1	3.3V	11	3.3V
2	3.3V	12	-12V
3	Ground	13	Ground
4	+5V	14	PS-ON
5	Ground	15	Ground
6	+5V	16	Ground
7	Ground	17	Ground
8	Power good	18	-5V
9	5VSB	19	+5V
10	+12V	20	+5V

2.5.20 Audio Pin Header for Chassis Front Panel (J22)
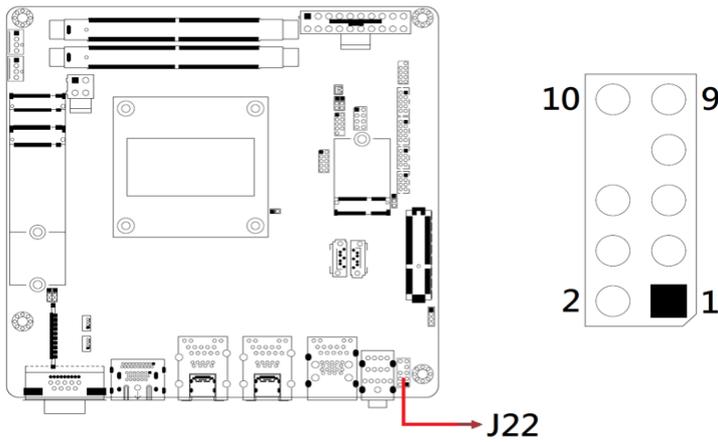
Pin	Signal Name	Pin	Signal Name
1	MIC IN_L	2	Ground
3	MIC IN_R	4	DET
5	LINE_R	6	Sense Ground
7	Sense	8	KEY
9	LINE_L	10	Sense Ground

2.5.21 CPU Power Connector (ATX2)
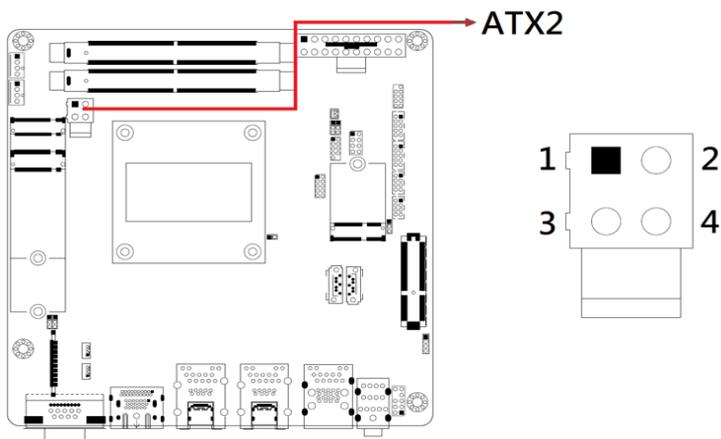
Pin	Signal Name	Pin	Signal Name
1	Ground	2	Ground
3	+12 V	4	+12V

2.5.22 SATA III Connector (SATA1, SATA2)
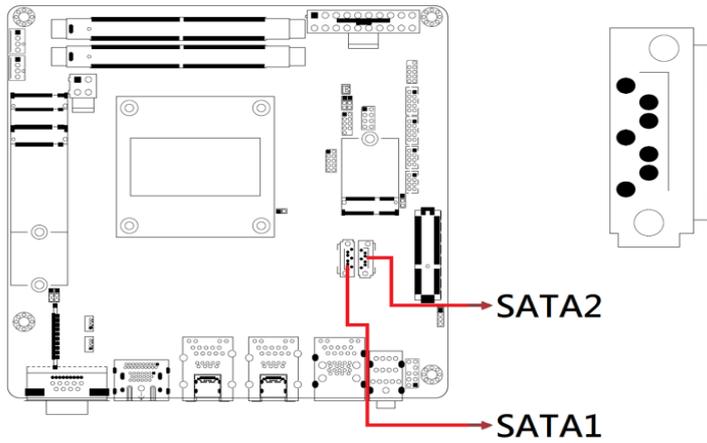
2.5.23 Fan Power Connectors (CPU_FAN1, SYS_FAN1)
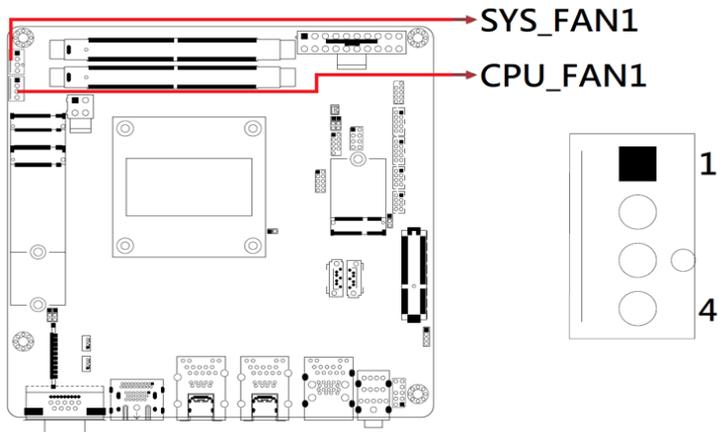
Pin	Signal Name
1	Ground
2	+12V
3	Rotation detection
4	Control

2.5.24 PCIe (x4) Slot (PCIE1)

A32 B32

A1 B1

PCIE1
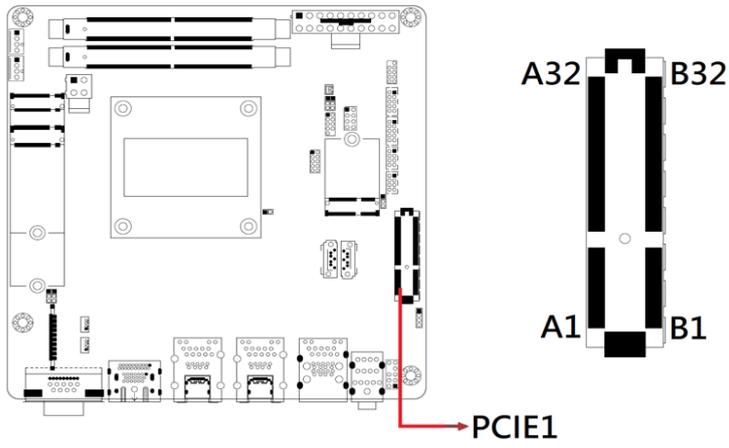
This page is intentionally left blank.

Chapter 3
Driver Installation

The information provided in this chapter includes:

- Intel Chipset Software Installation Utility
- VGA Driver Installation
- Intel Smartsound Drivers Installation
- Realtek Audio DCH Drivers Installation
- LAN Driver Installation
- Intel ME Drivers Installation
- Intel PMT Drivers Installation
- Intel NPU IO Drivers Installation
- Intel GNA IO Drivers Installation

iBASE

3.1 Introduction

This section describes the installation procedures for software and drivers under Windows 11.

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

3.2 Intel® Chipset Software Installation Utility

Intel® Chipset Software Installation Utility must be installed first to properly configure INF files for Plug & Play functionality of Intel chipset components. Follow the steps below:

1. Visit the IBASE website and navigate to the product's Download page. Download the compressed driver file to your computer. Double-click the file to extract it. Run CDGuide.exe to open the main driver interface. In the interface, click Intel on the left pane, then select Intel® Arrow Lake-P/U/H Chipset Drivers on the right.

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

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

4. Accept the software license agreement.

5. On the *Readme File Information* screen, click *Install*.
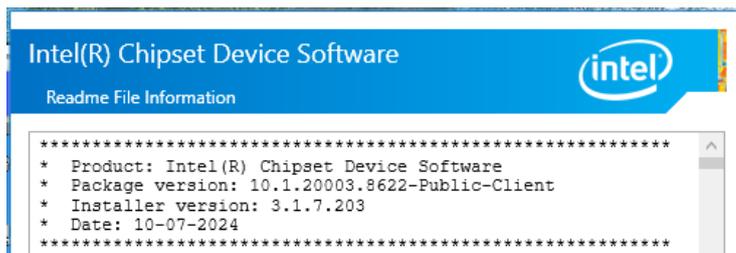
6. After the utility has been installed, click *Finish*.

iBASE

3.3 Graphics Drivers Installation

1. Click **Intel** on the left pane and then **Intel(R) Arrow Lake-P/U/H Chipset Drivers** on the right.
2. Click **Intel(R) HD Graphics Driver**.
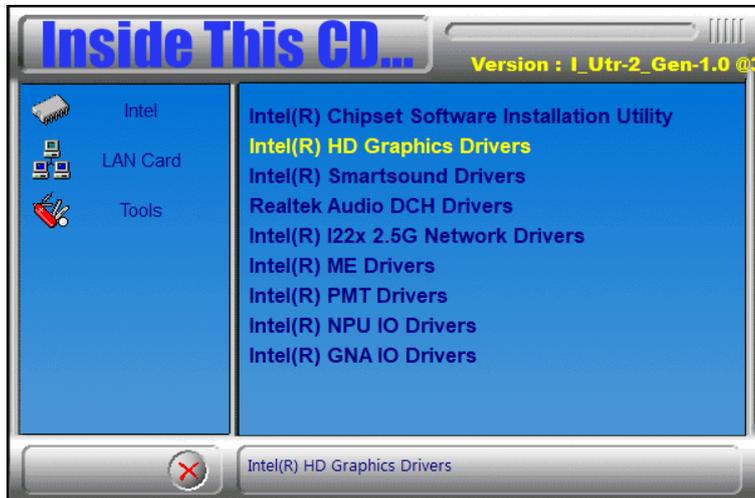
3. When the *Welcome* screen appears, click *Next*.
4. Click *I Agree* to continue the installation.
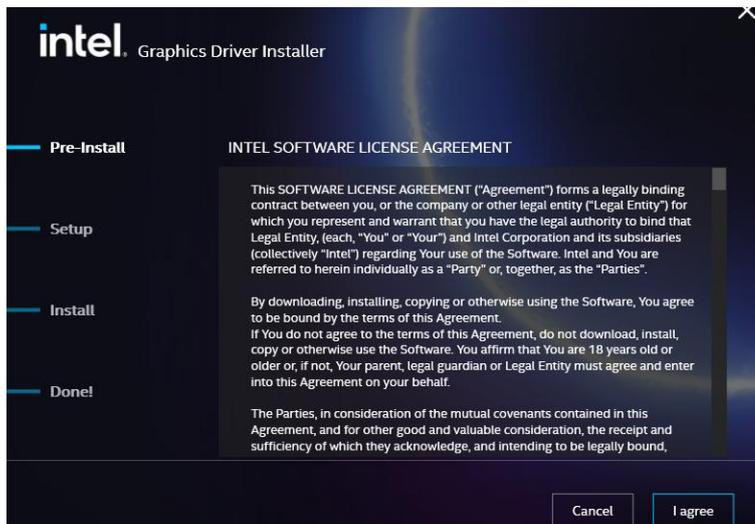
5. Click **Start** for the installer to install the following components:
   - Intel Graphics Driver
   - Intel Graphics Command Center
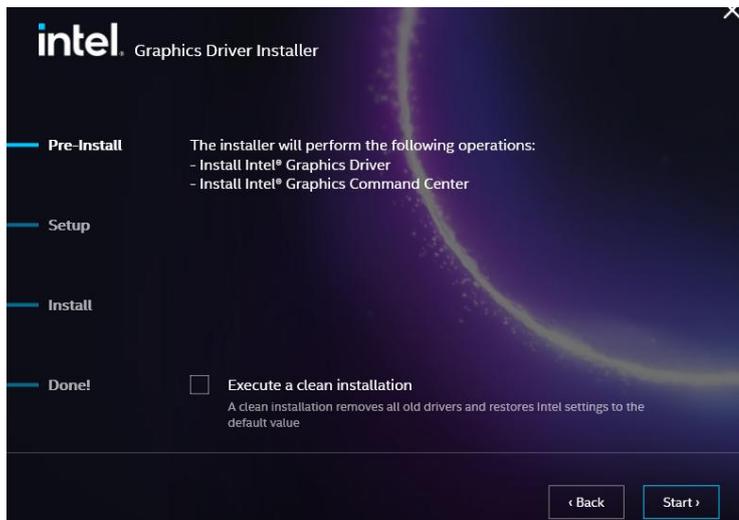
6. When installation has been completed, click *Finish*.

iBASE
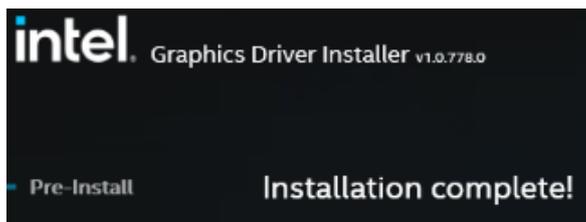
3.4 Intel(R) Smartsound Drivers Installation

1. Click **Intel** on the left pane and then **Intel(R) Arrow Lake-P/U/H Chipset Drivers** on the right pane. Click **Intel(R) Smartsound Drivers** on the right.
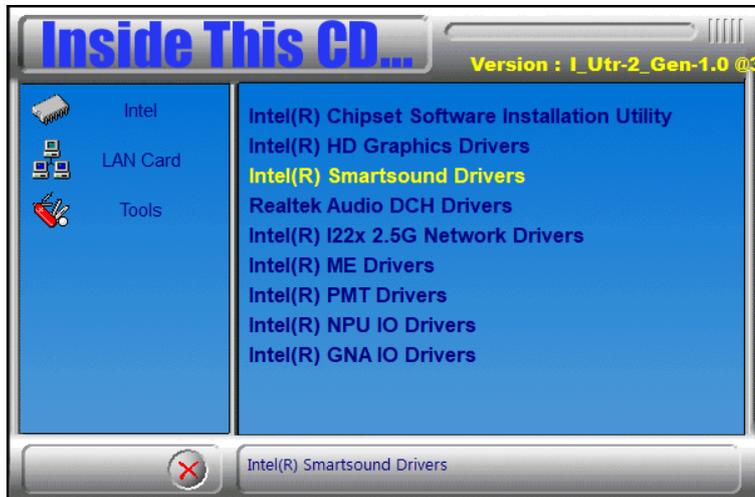
2. Run the file in the path shown below for the InstallShield Wizard to start and complete the installation of the Intel Smartsound drivers. When installation has been completed, press any key to continue.
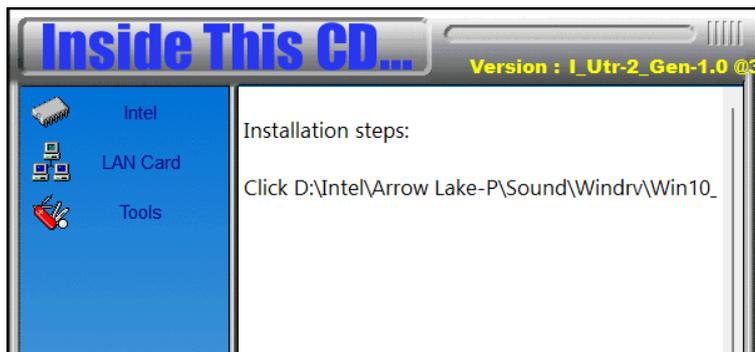
3.5 Realtek Audio DCH Drivers Installation

1. Click **Intel** on the left pane and then **Intel(R) Arrow Lake-P/U/H Chipset Drivers** on the right. Click **Realtek Audio DCH Drivers**.

2. Click **Next** when the Welcome to the InstallShield Wizard for Realtek Audio Driver screen appears.

3. After the InstallShield Wizard has completed the installation, restart the computer.

iBASE
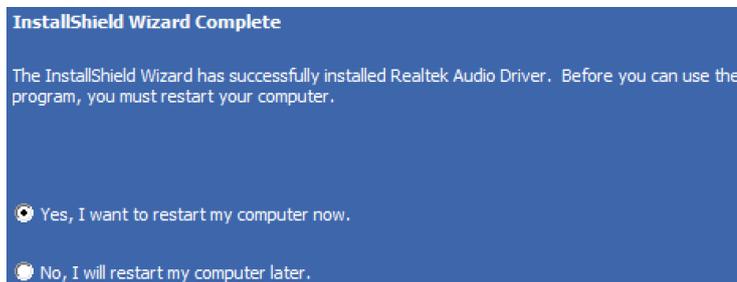
3.6 LAN Drivers Installation

1. Click **Intel** on the left pane and then **Intel(R) Arrow Lake-P/U/H Chipset Drivers** on the right.
2. Click **Intel(R) I22x 2.5G Network Drivers**.
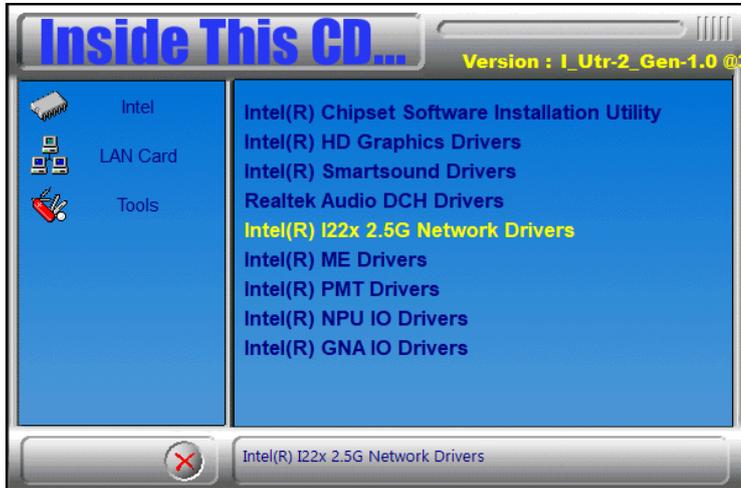
3. Follow the steps until InstallShield Wizard completes the installation.

3.7 Intel® Management Engine Drivers Installation

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

3. When the Welcome screen appears, click **Next**.
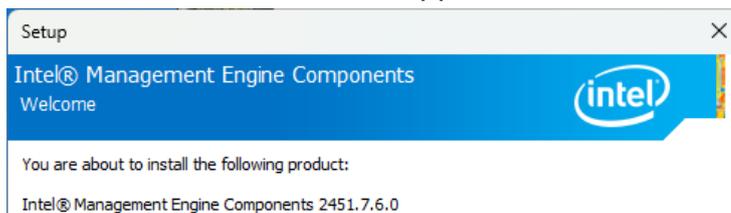
4. Accept the terms in the license agreement and click **Next**.
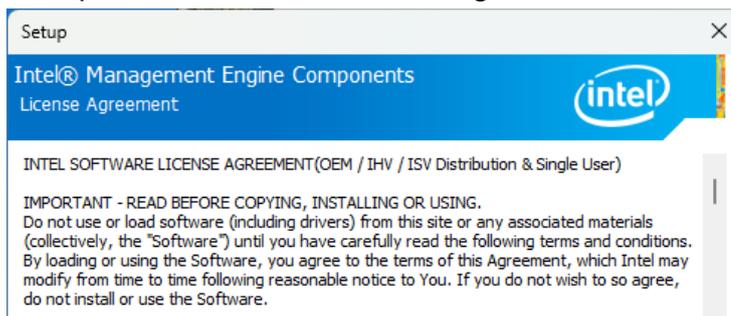
iBASE

5. In the Destination Folder screen, click **Next** to install to the default folder, or click Change to choose another destination folder.
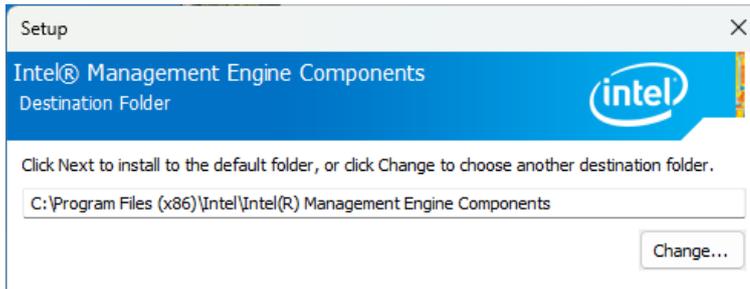
6. When installation is complete, click **Finish**.
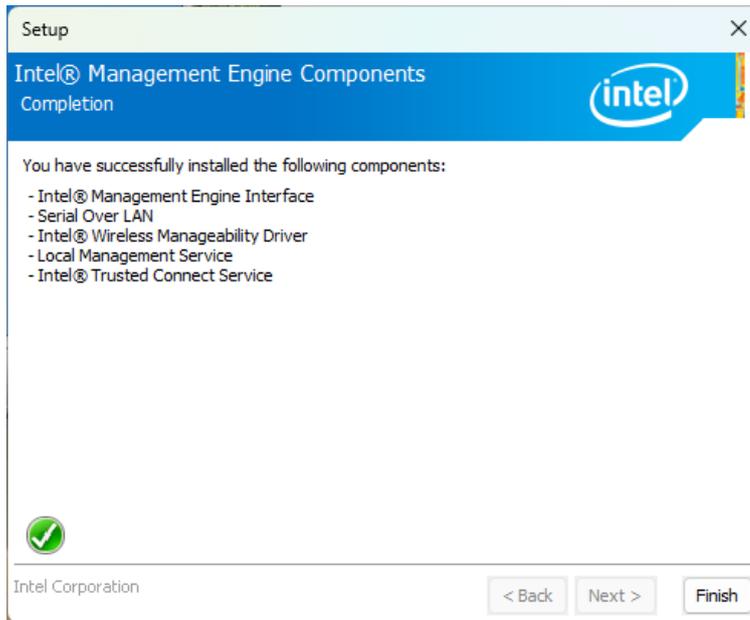
3.8 Intel® PMT Drivers Installation

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

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

iBASE
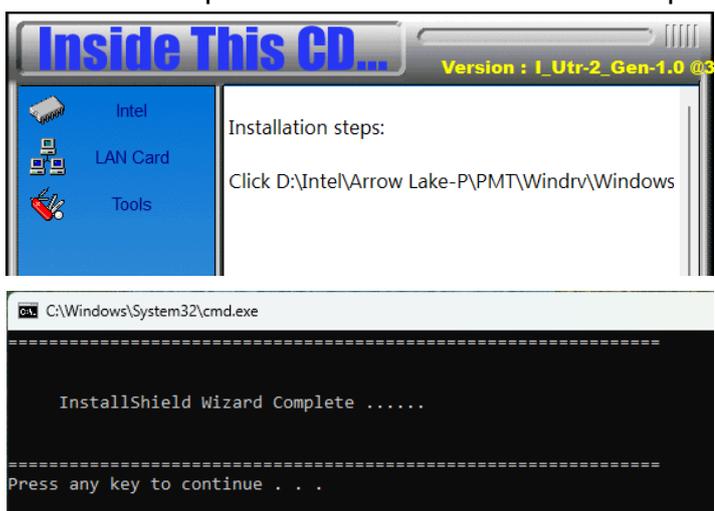
3.9 Intel® NPU IO Drivers Installation

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

3. Follow the steps until InstallShield Wizard completes the installation.
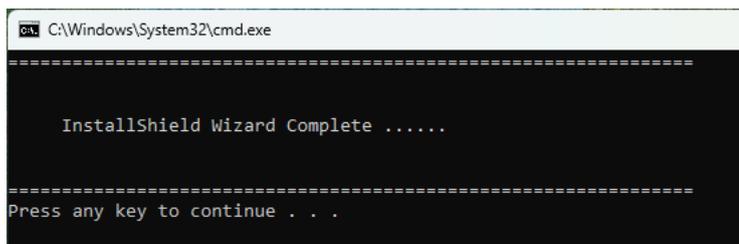
3.10 Intel® GNA IO Drivers Installation

1. Click **Intel** on the left pane and then **Intel(R) Arrow Lake-P/U/H Chipset Drivers** on the   right.
2. Click **Intel(R) GNA IO Drivers**.
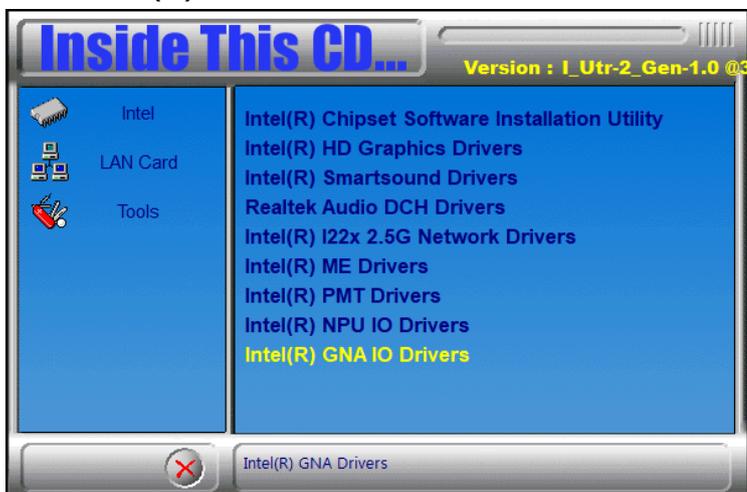
3. Follow the steps until InstallShield Wizard completes the installation.
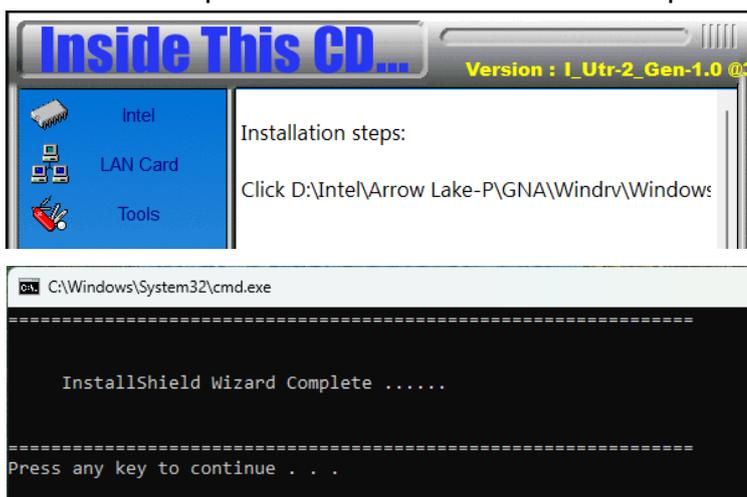
Chapter 4
BIOS Setup

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

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

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 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. Pressing 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.

---

iBASE

4.3 Main Settings

```
                              Aptio Setup – AMI
 Main  Advanced  Security  Boot  Save & Exit

 BIOS Version                   MI1005AF-AS003-250328...       Set the Date. Use Tab to
                                                               switch between Date elements.
 Total Memory                   8192 MB                        Default Ranges:
 Memory Frequency               5600 MHz                       Year: 1998-9999
                                                               Months: 1-12
                                                               Days: Dependent on month
 System Date                    [Tue 08/15/2124]               Range of Years may vary.
 System Time                    [03:41:05]



                                                               ++: Select Screen
                                                               ↑↓: Select Item
                                                               Enter: Select
                                                               +/-: Change Opt.
                                                               F1: General Help
                                                               F2: Previous Values
                                                               F3: Optimized Defaults
                                                               F4: Save & Exit
                                                               ESC: Exit




                    Version 2.22.1297 Copyright (C) 2025 AMI
```

BIOS Setting	Description
System Date	Sets the system date. Use **<Tab>** to navigate fields.
System Time	Sets the system time. Use **<Tab>** to navigate fields.

4.4 Advanced Settings

This section covers system configurations.

```
                              Aptio Setup – AMI
    Main  Advanced  Security  Boot  Save & Exit

  ▶ CPU Configuration                           CPU Configuration Parameters
  ▶ Power & Performance
  ▶ System Agent (SA) Configuration
  ▶ PCH-IO Configuration
  ▶ PCH-FW Configuration
  ▶ Trusted Computing
  ▶ ACPI Settings
  ▶ F8196x Super IO Configuration
  ▶ F8196x Hardware Monitor
  ▶ USB Configuration
  ▶ Network Stack Configuration
  ▶ NVMe Configuration

                                                ↔: Select Screen
                                                ↑↓: Select Item
                                                Enter: Select
                                                +/-: Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit

                    Version 2.22.1297 Copyright (C) 2025 AMI
```

iBASE

CPU Configuration

```
                          Aptio Setup - AMI
   ┌─────────────┐
   │  Advanced   │
   └─────────────┘
   CPU Configuration                               Displays the E-core Information

 ► Efficient-core Information
 ► Performance-core

   ID                         0xB0650
   Brand String               Intel(R) Core(TM) Ult...
   VMX                        Supported
   SMX/TXT                    Supported

   Intel (VMX) Virtualization Technol   [Enabled]
   Active Performance-cores             [All]
   Active Efficient-cores               [All]
   Active SOC-North Efficient-cores     [All]      →←: Select Screen
   Hyper-Threading                      [Enabled]  ↑↓: Select Item
   AES                                  [Enabled]  Enter: Select
   X2APIC Enable                        [Enabled]  +/-: Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit



                    Version 2.22.1297 Copyright (C) 2025 AMI
```

BIOS Setting	Description
Efficient/Performance-core Information	Displays the E-core / P-core Information
Intel (VMX) Virtualization Technology	When enabled, a VMX 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/Disable Hyper-Threading Technology.
AES	Enable/Disable AES (Advanced Encryption Standard).
X2APIC Enable	Enable/Disable X2APIC Operating Mode. When this option is configured as 'Enabled', 'VT-d' option must be 'Enabled' and 'X2APIC Opt Out' option must be 'Disabled' as well. This option will be grayed out when 'VT-d' option is configured as 'Disabled'.

4.4.2 Power & Performance

```
                        Aptio Setup - AMI
    Main  Advanced  Security  Boot  Save & Exit

 ▶ CPU Configuration                           Power & Performance Options
 ▶ Power & Performance
 ▶ System Agent (SA) Configuration
 ▶ PCH-IO Configuration
 ▶ PCH-FW Configuration
 ▶ Trusted Computing
 ▶ ACPI Settings
 ▶ F8196x Super IO Configuration
 ▶ F8196x Hardware Monitor
 ▶ USB Configuration
 ▶ Network Stack Configuration
 ▶ NVMe Configuration
                                               ↔: Select Screen
                                               ↑↓: Select Item
                                               Enter: Select
                                               +/-: Change Opt.
                                               F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit
```

```
                        Aptio Setup - AMI
        Advanced

  Power & Performance                          CPU - Power Management Control
                                               Options
 ▶ CPU - Power Management Control
```

```
                        Aptio Setup - AMI
        Advanced

  CPU - Power Management Control               Allows more than two frequency
                                               ranges to be supported.
    Intel(R) SpeedStep(tm)        [Enabled]
    Intel(R) Speed Shift Technology [Enabled]
      Turbo Mode                   [Enabled]
 ▶    Config TDP Configurations
```

```
                        Aptio Setup - AMI
        Advanced

  CPU - Power Management Control               Enable/Disable Intel(R) Speed
                                               Shift Technology support.
    Intel(R) SpeedStep(tm)        [Enabled]    Enabling will expose the CPPC
    Intel(R) Speed Shift Technology [Enabled]  v2 interface to allow for
      Turbo Mode                   [Enabled]   hardware controlled P-states.
 ▶    Config TDP Configurations
```

```
                        Aptio Setup - AMI
        Advanced

  CPU - Power Management Control               Enable/Disable processor Turbo
                                               Mode.
    Intel(R) SpeedStep(tm)        [Enabled]
    Intel(R) Speed Shift Technology [Enabled]
      Turbo Mode                   [Enabled]
 ▶    Config TDP Configurations
```

```
                        Aptio Setup - AMI
        Advanced

  CPU - Power Management Control               cTDP (Assured Power)
                                               Configurations
    Intel(R) SpeedStep(tm)        [Enabled]
    Intel(R) Speed Shift Technology [Enabled]
      Turbo Mode                   [Enabled]
 ▶    Config TDP Configurations
```

```
                        Aptio Setup - AMI
        Advanced

  Config TDP Configurations                    cTDP (Assured Power) Mode as
                                               Nominal/Level1/Level2/Deactivat
    Configurable TDP Boot Mode     [Nominal]   e TDP (Base Power) selection.
    Power Limit 1          28.0W (MSR:28.0)    Deactivate option will set MSR
    Power Limit 2          60.0W (MSR:60.0)    to Nominal and MMIO to Zero.
```

iBASE

4.4.3 System Agent (SA) Configuration

```
                              Aptio Setup - AMI
        Main  Advanced  Security  Boot  Save & Exit

   ▶ CPU Configuration                                System Agent (SA) Parameters
   ▶ Power & Performance
   ▶ System Agent (SA) Configuration
   ▶ PCH-IO Configuration
   ▶ PCH-FW Configuration
   ▶ Trusted Computing
   ▶ ACPI Settings
   ▶ F8196x Super IO Configuration
   ▶ F8196x Hardware Monitor
   ▶ USB Configuration
   ▶ Network Stack Configuration
   ▶ NVMe Configuration
                                                     →←: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
                                                     +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit


                    Version 2.22.1297 Copyright (C) 2025 AMI
```

```
   System Agent (SA) Configuration                    VMD Configuration settings

   ▶ VMD setup menu
   ▶ VT-d setup menu

     NPU Device (B0:D11:F0)           [Enabled]
```

```
   VMD Configuration                                  Enable/Disable to VMD
                                                      controller
   Enable VMD controller              [Disabled]
```

```
   VMD Configuration                                  Enable/Disable to VMD
                                                      controller
   Enable VMD controller              [Enabled]

   Enable VMD Global Mapping          [Disabled]

   Map SOC SATA Controller Under VMD  [Disabled]

   RAID0                              [Enabled]
   RAID1                              [Enabled]
   RAID5                              [Enabled]
   RAID10                             [Enabled]
```

```
   VMD Configuration                                  Enable/Disable to VMD Global
                                                      Mapping
   Enable VMD controller              [Enabled]

   Enable VMD Global Mapping          [Disabled]
```

```
   VMD Configuration                                  Map/UnMap this Root Port to VMD

   Enable VMD controller              [Enabled]

   Enable VMD Global Mapping          [Disabled]

   Map SOC SATA Controller Under VMD  [Disabled]
```

```
VMD Configuration                                      Enable/Disable RAID0 support

Enable VMD controller           [Enabled]

Enable VMD Global Mapping       [Disabled]

Map SOC SATA Controller Under VMD   [Disabled]

RAID0                           [Enabled]
RAID1                           [Enabled]
RAID5                           [Enabled]
RAID10                          [Enabled]
```

```
System Agent (SA) Configuration                        VT-d Configuration settings

▶ VMD setup menu
▶ VT-d setup menu

  NPU Device (B0:D11:F0)            [Enabled]
```

```
VT-d Configuration

  VT-d                              Supported

  VT-d                              [Enabled]
```

```
System Agent (SA) Configuration                        Enable/Disable NPU (Neural
                                                       Processing Unit) Device.
▶ VMD setup menu
▶ VT-d setup menu

  NPU Device (B0:D11:F0)            [Enabled]



                        ┌── NPU Device (B0:D11:F0) ──┐
                        │ Enabled                    │
                        │ Disabled                   │
                                                       ←: Select Screen
```

iBASE

4.4.4 PCH-IO Configuration

2.5.25

```
                          Aptio Setup – AMI
    Main  Advanced  Security  Boot  Save & Exit

  ▶ CPU Configuration                              PCH Parameters
  ▶ Power & Performance
  ▶ System Agent (SA) Configuration
  ▶ PCH-IO Configuration
  ▶ PCH-FW Configuration
  ▶ Trusted Computing
  ▶ ACPI Settings
  ▶ F8196x Super IO Configuration
  ▶ F8196x Hardware Monitor
  ▶ USB Configuration
  ▶ Network Stack Configuration
  ▶ NVMe Configuration
```

2.5.26

```
  PCH-IO Configuration                             SATA Device Options Settings

  ▶ SATA Configuration

  Power-On after Power failure          [Power Off]
```

2.5.27

```
  SATA Configuration                               Enable/Disable SATA Device.

  SATA Controller(s)                    [Enabled]
  SATA Mode Selection                   [AHCI]
  Serial ATA Port 0                     Empty
    Software Preserve                   Unknown
    Port 0                              [Enabled]
    Hot Plug                            [Disabled]
    Configured as eSATA                 Hot Plug supported
  Serial ATA Port 1                     Empty
    Software Preserve                   Unknown
    Port 1                              [Enabled]
    Hot Plug                            [Disabled]
    Configured as eSATA                 Hot Plug supported    ↔: Select Screen
```

2.5.28

```
  SATA Configuration                               Determines how SATA
                                                   controller(s) operate.
  SATA Controller(s)                    [Enabled]
  SATA Mode Selection                   [AHCI]
```

2.5.29

```
  SATA Configuration                               Enable or Disable SATA Port

  SATA Controller(s)                    [Enabled]
  SATA Mode Selection                   [AHCI]
  Serial ATA Port 0                     Empty
    Software Preserve                   Unknown
    Port 0                              [Enabled]
```

2.5.30

```
  SATA Configuration                               Designates this port as Hot
                                                   Pluggable.
  SATA Controller(s)                    [Enabled]
  SATA Mode Selection                   [AHCI]
  Serial ATA Port 0                     Empty
    Software Preserve                   Unknown
    Port 0                              [Enabled]
    Hot Plug                            [Disabled]
```

2.5.31

```
  PCH-IO Configuration                             Specify what state to go to
                                                   when power is re-applied after
  ▶ SATA Configuration                             a power failure (G3 state).

  Power-On after Power failure          [Power Off]



                  ┌─── Power-On after Power failure ───┐
                  │ Power On                           │
                  │ Power Off                          │
```

4.4.5 PCH-FW Configuration

```
                          Aptio Setup - AMI
   Main  Advanced  Security  Boot  Save & Exit

 ▶ CPU Configuration                         Configure Management Engine
 ▶ Power & Performance                       Technology Parameters
 ▶ System Agent (SA) Configuration
 ▶ PCH-IO Configuration
 ▶ PCH-FW Configuration
 ▶ Trusted Computing
 ▶ ACPI Settings
 ▶ F8196x Super IO Configuration
 ▶ F8196x Hardware Monitor
 ▶ USB Configuration
 ▶ Network Stack Configuration
 ▶ NVMe Configuration
                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

              Version 2.22.1297 Copyright (C) 2025 AMI
```

```
                          Aptio Setup - AMI
   Advanced

 ME Firmware Version       18.1.15.2481
 ME Firmware Mode          Normal Mode
 ME Firmware SKU           Corporate SKU




                                             →←: Select Screen
                                             ↑↓: Select Item
                                             Enter: Select
                                             +/-: Change Opt.
                                             F1: General Help
                                             F2: Previous Values
                                             F3: Optimized Defaults
                                             F4: Save & Exit
                                             ESC: Exit

              Version 2.22.1297 Copyright (C) 2025 AMI
```

iBASE

4.4.6 Trusted Computing

```
                            Aptio Setup - AMI
     Main  Advanced  Security  Boot  Save & Exit

   ▶ CPU Configuration                               Trusted Computing Settings
   ▶ Power & Performance
   ▶ System Agent (SA) Configuration
   ▶ PCH-IO Configuration
   ▶ PCH-FW Configuration
   ▶ Trusted Computing
   ▶ ACPI Settings
   ▶ F8196x Super IO Configuration
   ▶ F8196x Hardware Monitor
   ▶ USB Configuration
   ▶ Network Stack Configuration
   ▶ NVMe Configuration

   TPM 2.0 Device Found
   Firmware Version:                   15.23
   Vendor:                             IFX

   Security Device Support             [Enabled]
   Active PCR banks                    SHA256
   Available PCR banks                 SHA256,SHA384

   SHA256 PCR Bank                     [Enabled]
   SHA384 PCR Bank                     [Disabled]

   Pending operation                   [None]
   Platform Hierarchy                  [Enabled]
   Storage Hierarchy                   [Enabled]
   Endorsement Hierarchy               [Enabled]
   Physical Presence Spec Version      [1.3]
   TPM 2.0 InterfaceType               [TIS]
   Device Select                       [Auto]
```

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.
SHA256/384 PCR Bank	Enables / Disables PCR Bank.
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.

4.4.7 ACPI Settings
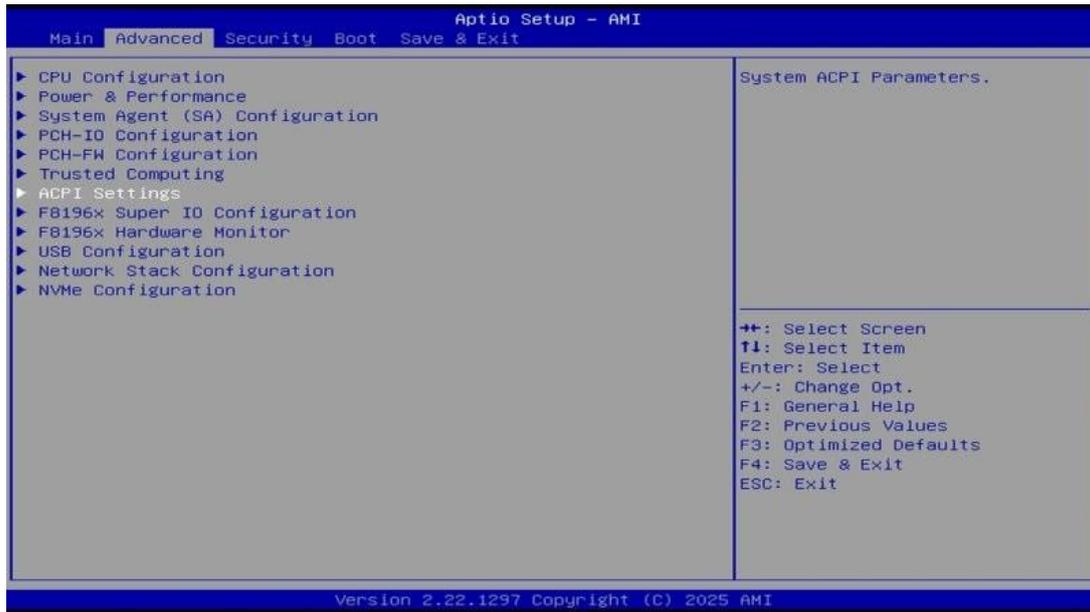
```
                        Aptio Setup - AMI
   Main  Advanced  Security  Boot  Save & Exit

 ▶ CPU Configuration                              System ACPI Parameters.
 ▶ Power & Performance
 ▶ System Agent (SA) Configuration
 ▶ PCH-IO Configuration
 ▶ PCH-FW Configuration
 ▶ Trusted Computing
 ▶ ACPI Settings
 ▶ F8196x Super IO Configuration
 ▶ F8196x Hardware Monitor
 ▶ USB Configuration
 ▶ Network Stack Configuration
 ▶ NVMe Configuration

                                                 ➤←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit


               Version 2.22.1297 Copyright (C) 2025 AMI
```

```
                        Aptio Setup - AMI
        Advanced

   ACPI Settings                                  Enables or Disables System
                                                  ability to Hibernate (OS/S4
                                                  Sleep State). This option may
   Enable Hibernation          [Enabled]          not be effective with some
                                                  operating systems.



                      ┌── Enable Hibernation ──┐
                      │ Disabled               │
                      │ Enabled                │
                      └────────────────────────┘      ➤←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit


               Version 2.22.1297 Copyright (C) 2025 AMI
```

iBASE

4.4.8 F8196x Super IO Configuration

```
                              Aptio Setup - AMI
       Main  Advanced  Security  Boot  Save & Exit

    ▶ CPU Configuration                              System Super IO Chip
    ▶ Power & Performance                            Parameters.
    ▶ System Agent (SA) Configuration
    ▶ PCH-IO Configuration
    ▶ PCH-FW Configuration
    ▶ Trusted Computing
    ▶ ACPI Settings
    ▶ F8196x Super IO Configuration
    ▶ F8196x Hardware Monitor
    ▶ USB Configuration
    ▶ Network Stack Configuration
    ▶ NVMe Configuration
```
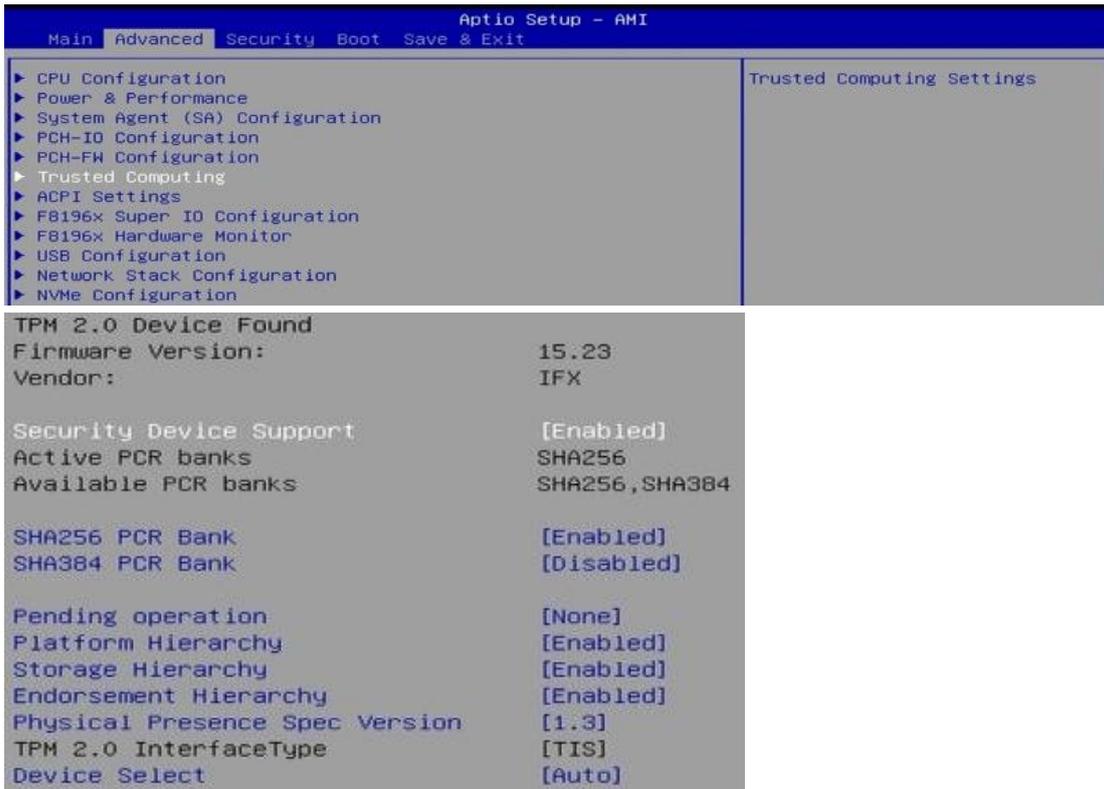
```
    F8196x Super IO Configuration                    Set Parameters of Serial Port
                                                     1 (COMA)
      Super IO Chip                       F8196x
    ▶ Serial Port 1 Configuration
    ▶ Serial Port 2 Configuration
    ▶ Serial Port 3 Configuration
    ▶ Serial Port 4 Configuration
```

```
    Serial Port 1 Configuration                      Change the Serial Port mode.

      Serial Port                   [Enabled]
      Device Settings               IO=3F8h; IRQ=4;

      Change Settings               [Auto]
      Device Mode                   [RS232]

                    ┌──────────── Device Mode ────────────┐
                    │ RS232                                │
                    │ RS485 TX Low  Active                 │
                    │ RS485 with Termination TX Low Active │
                    │ RS422                                │      elect Screen
                    │ RS422 with Termination               │      elect Item
                    └──────────────────────────────────────┘
```

```
    F8196x Super IO Configuration                    Set Parameters of Serial Port
                                                     2 (COMB)
      Super IO Chip                       F8196x
    ▶ Serial Port 1 Configuration
    ▶ Serial Port 2 Configuration
    ▶ Serial Port 3 Configuration
    ▶ Serial Port 4 Configuration
```

```
    Serial Port 2 Configuration                      Select an optimal settings for
                                                     Super IO Device
      Serial Port                   [Enabled]
      Device Settings               IO=2F8h; IRQ=3;

      Change Settings               [Auto]
      Device Mode                   [RS232]

                  ┌───────────── Change Settings ──────────────┐
                  │ Auto                                        │
                  │ IO=2F8h; IRQ=3;                             │
                  │ IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;          │
                  │ IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;          │
                  │ IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;          │  Select Screen
                  │ IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;          │  Select Item
                  └─────────────────────────────────────────────┘
```

```
    Serial Port 2 Configuration                      Change the Serial Port mode.

      Serial Port                   [Enabled]
      Device Settings               IO=2F8h; IRQ=3;

      Change Settings               [Auto]
      Device Mode                   [RS232]

                    ┌──────────── Device Mode ────────────┐
                    │ RS232                                │
                    │ RS485 TX Low  Active                 │
                    │ RS485 with Termination TX Low Active │
                    │ RS422                                │      elect Screen
                    │ RS422 with Termination               │      elect Item
                    └──────────────────────────────────────┘
```

```
F8196x Super IO Configuration                          Set Parameters of Serial Port
                                                       3 (COMC)
Super IO Chip                        F8196x
► Serial Port 1 Configuration
► Serial Port 2 Configuration
► Serial Port 3 Configuration
► Serial Port 4 Configuration
```

```
Serial Port 3 Configuration                            Select an optimal settings for
                                                       Super IO Device
Serial Port                          [Enabled]
Device Settings                      IO=3E8h; IRQ=7;

Change Settings                      [Auto]

                    ┌──────── Change Settings ────────┐
                    │ Auto                            │
                    │ IO=3E8h; IRQ=7;                 │
                    │ IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; │
                    │ IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12; │
                    │ IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Screen
                    │ IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Item
```

```
F8196x Super IO Configuration                          Set Parameters of Serial Port
                                                       4 (COMD)
Super IO Chip                        F8196x
► Serial Port 1 Configuration
► Serial Port 2 Configuration
► Serial Port 3 Configuration
► Serial Port 4 Configuration
```

```
Serial Port 4 Configuration                            Select an optimal settings for
                                                       Super IO Device
Serial Port                          [Enabled]
Device Settings                      IO=2E8h; IRQ=6;

Change Settings                      [Auto]

                    ┌──────── Change Settings ────────┐
                    │ Auto                            │
                    │ IO=2E8h; IRQ=7;                 │
                    │ IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12; │
                    │ IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12; │
                    │ IO=2F0h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Screen
                    │ IO=2E0h; IRQ=3,4,5,6,7,9,10,11,12; │ Select Item
```

iBASE

4.4.9 F8196x Hardware Monitor

```
                          Aptio Setup - AMI
    Main  Advanced  Security  Boot  Save & Exit

  ▶ CPU Configuration                              Monitor hardware status
  ▶ Power & Performance
  ▶ System Agent (SA) Configuration
  ▶ PCH-IO Configuration
  ▶ PCH-FW Configuration
  ▶ Trusted Computing
  ▶ ACPI Settings
  ▶ F8196x Super IO Configuration
  ▶ F8196x Hardware Monitor
  ▶ USB Configuration
  ▶ Network Stack Configuration
  ▶ NVMe Configuration

                                                 ←→: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

                 Version 2.22.1297 Copyright (C) 2025 AMI
```

```
                          Aptio Setup - AMI
    Advanced

  Pc Health Status

  CPU_FAN1 Smart Fan Control          [Disabled]
  SYS_FAN1 Smart Fan Control          [Disabled]
  CPU temperature                     : +30 C
  System temperature                  : +30 C
  CPU Fan1 Speed                      : 7936 RPM
  SYS Fan1 Speed                      : N/A
  VCORE                               : +1.168 V
  +5V            ┌──── SYS_FAN1 Smart Fan Control ────┐
  +12V           │ Disabled                           │
  Memory Voltage │ 50°C                               │
                 │ 60°C                               │
                 │ 70°C                        Select Screen
                 │ 80°C                        Select Item
                 └────────────────────────────┘er: Select
                                                 : Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

                 Version 2.22.1297 Copyright (C) 2025 AMI
```

BIOS Setting	Description
CPU Smart Fan Control	Enables / Disables smart fan control.
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 USB Configuration

```
                              Aptio Setup - AMI
    Advanced

 USB Configuration                              This is a workaround for OSes
                                                without XHCI hand-off support.
 USB Module Version              38             The XHCI ownership change
                                                should be claimed by XHCI
 USB Controllers:                               driver.
     2 XHCIs
 USB Devices:
     1 Keyboard, 1 Mouse, 2 Hubs

 XHCI Hand-off                   [Enabled]
 USB Mass Storage Driver Support [Enabled]

 USB hardware delays and time-outs:
 USB transfer time-out           [20 sec]       →←: Select Screen
 Device reset time-out           [20 sec]       ↑↓: Select Item
 Device power-up delay           [Auto]         Enter: Select
                                                +/-: Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F3: Optimized Defaults
                                                F4: Save & Exit
                                                ESC: Exit



                     Version 2.22.1297 Copyright (C) 2025 AMI
```

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 support.
USB Transfer time-out	The time-out value (1 / 5 10 / 20 secs) for Control, Bulk, and Interrupt transfers.
Device reset time-out	Gives seconds (10 / 20 / 30 / 40 secs) to delay execution of Start Unit command to USB mass storage device.
Device power-up delay	Max.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.

iBASE

4.4.11 Network Stack Configuration
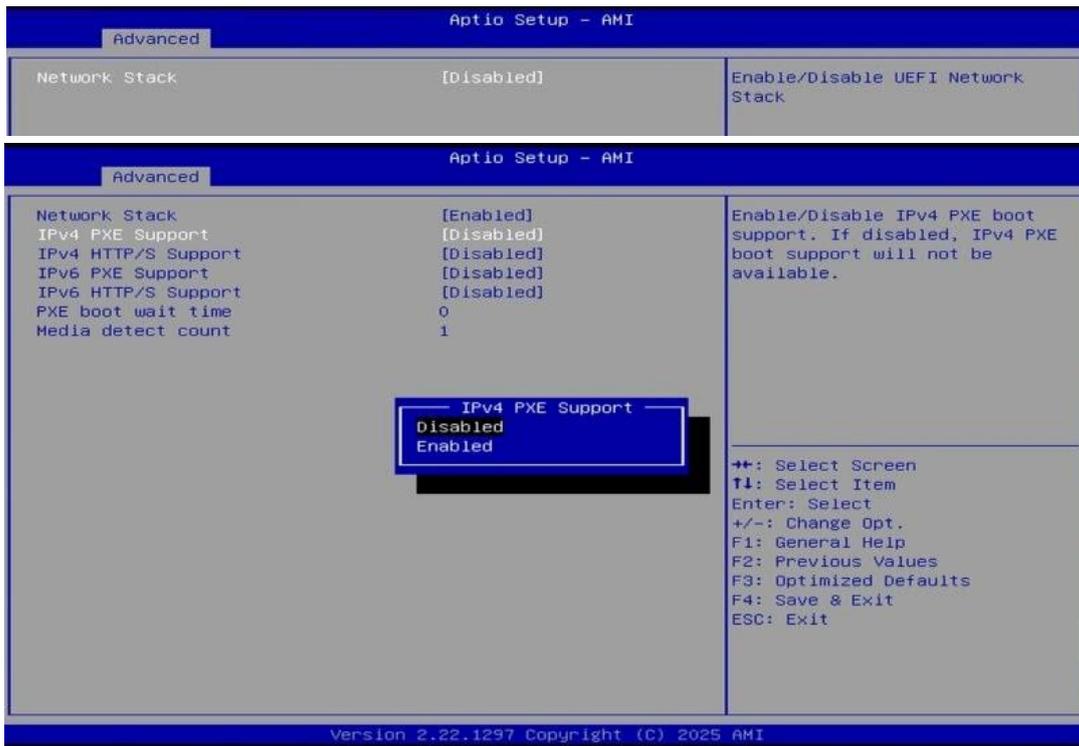
BIOS Setting	Description
Network Stack	Enable/Disable UEFI Network Stack
IPv4 PXE Support	If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	If disabled, IPv4 HTTP boot support will not be available.
IPv6 PXE Support	If disabled, IPv6 PXE boot support will not be available.
IPv6 HTTP Support	If disabled, IPv6 HTTP boot support will not be available.
PXE boot wait time	Wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value
Media detect count	Number of times the presence of media will be checked. Use either +/- numeric keys to set the value.

4.4.12 NVME Configuration

2.5.32

2.5.33

iBASE
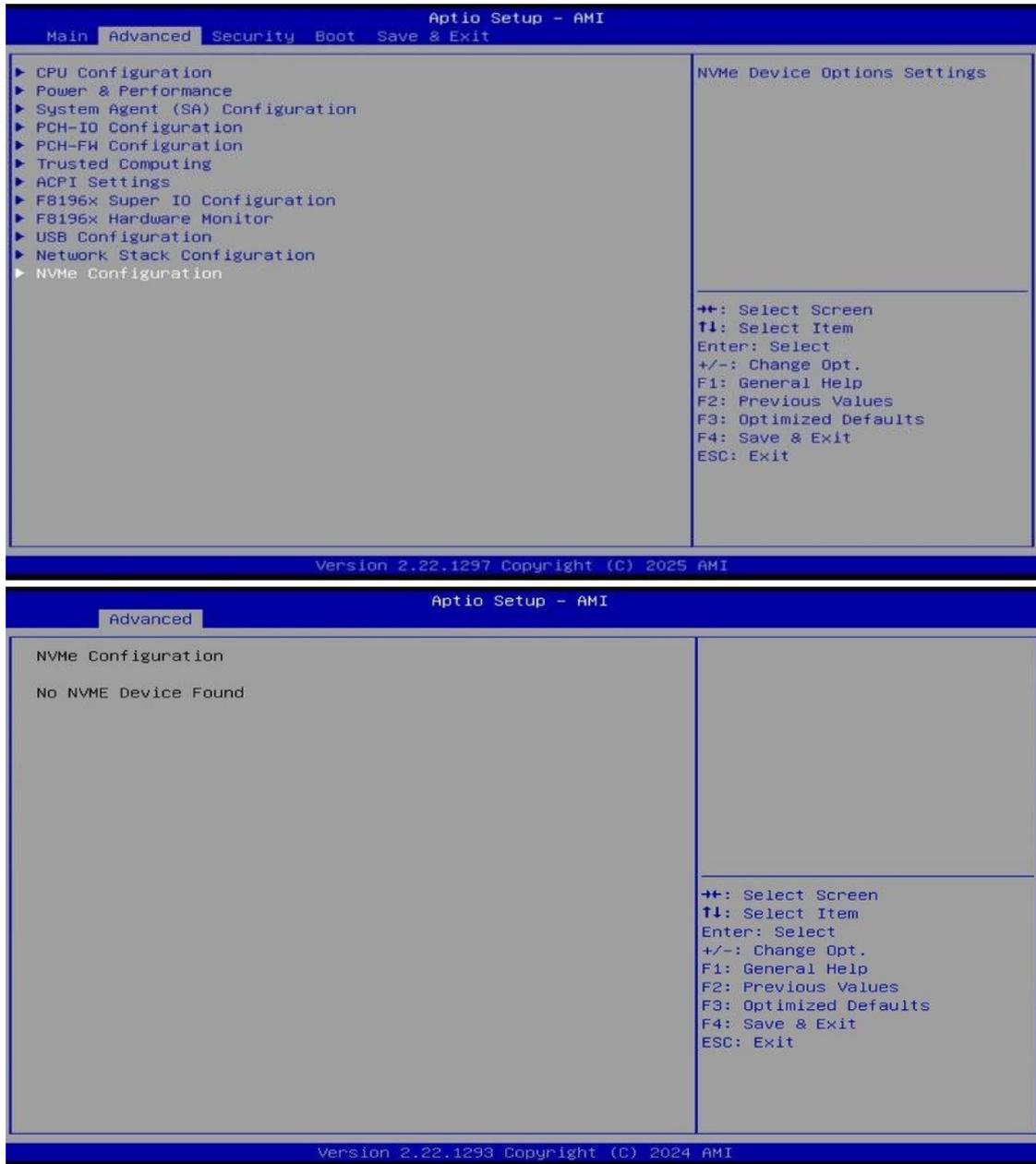
4.5 Security Settings

```
                        Aptio Setup - AMI
    Main  Advanced  Security  Boot  Save & Exit

    Password Description                              Set Administrator Password

    If ONLY the Administrator's password is set,
    then this only limits access to Setup and is
    only asked for when entering Setup.
    If ONLY the User's password is set, then this
    is a power on password and must be entered to
    boot or enter Setup. In Setup the User will
    have Administrator rights.
    The password length must be
    in the following range:
    Minimum length              3
    Maximum length              20              ↔: Select Screen
                                                ↑↓: Select Item
    Administrator Password                      Enter: Select
    User Password                               +/-: Change Opt.
                                                F1: General Help
  ▶ Secure Boot                                 F2: Previous Values
                                                F3: Optimized Defaults
```

```
    System Mode                 Setup           Secure Boot feature is Active
                                                if Secure Boot is Enabled,
    Secure Boot                 [Disabled]      Platform Key(PK) is enrolled
                                Not Active      and the System is in User mode.
                                                The mode change requires
    Secure Boot Mode            [Custom]        platform reset
```

```
    System Mode                 Setup           Secure Boot mode options:
                                                Standard or Custom.
    Secure Boot                 [Disabled]      In Custom mode, Secure Boot
                                Not Active      Policy variables can be
                                                configured by a physically
    Secure Boot Mode            [Custom]        present user without full
  ▶ Restore Factory Keys                        authentication
  ▶ Reset To Setup Mode

  ▶ Expert Key Management
                            ┌─── Secure Boot Mode ───┐
                            │ Standard               │
                            │ Custom                 │
```

```
    System Mode                 Setup           Force System to User Mode.
                                                Install factory default Secure
    Secure Boot                 [Disabled]      Boot key databases
                                Not Active

    Secure Boot Mode            [Custom]
  ▶ Restore Factory Keys
  ▶ Reset To Setup Mode

  ▶ Expert Key Management   ┌──── Install factory defaults ────┐
                           │ Press 'Yes' to proceed 'No' to cancel │
                           │                                   │
                           │  Yes                 No           │  elect Screen
                                                                  elect Item
```

```
    System Mode                 Setup           Enables expert users to modify
                                                Secure Boot Policy variables
    Secure Boot                 [Disabled]      without variable authentication
                                Not Active

    Secure Boot Mode            [Custom]
  ▶ Restore Factory Keys
  ▶ Reset To Setup Mode

  ▶ Expert Key Management
```
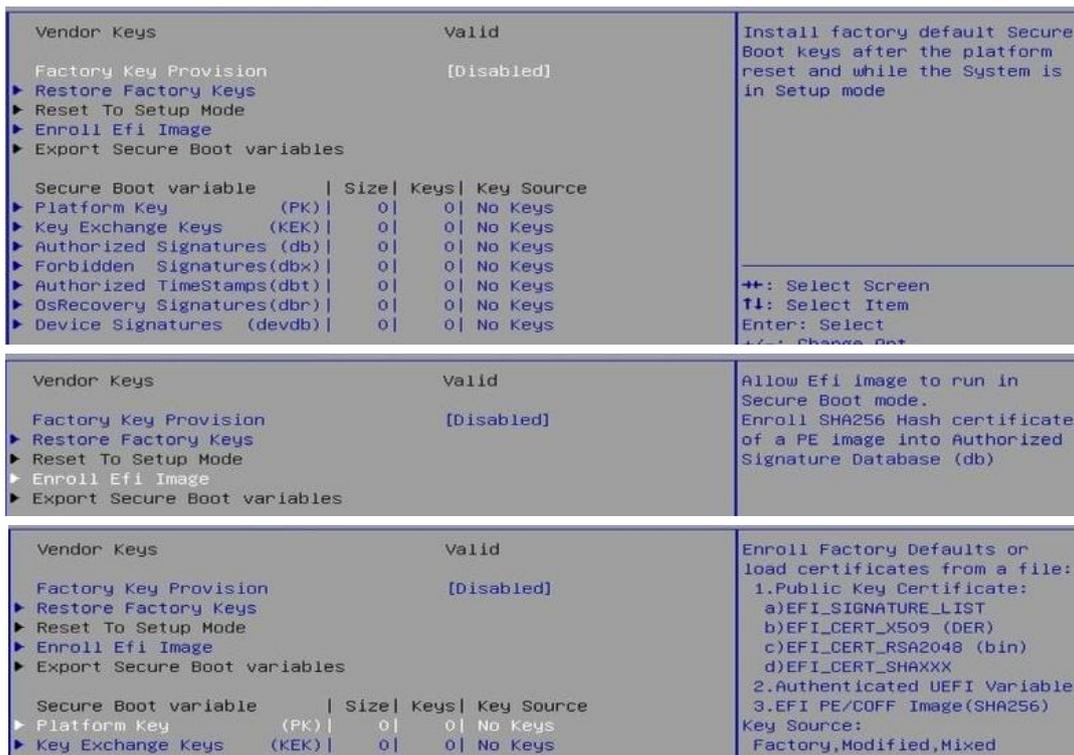
BIOS Setting	Description
Setup Administrator Password	Sets an administrator password for the setup utility.
User Password	Sets a user password.
Secure Boot	Secure Boot feature is Active if Secure Boot is enabled. Platform Key(PK) is enrolled and the system is in user mode. The mode change requires platform 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.
Restore Factory Keys	Forces system to user mode. Install factory default Secure Boot key databases.
Reset to Setup Mode	Delete all Secure Boot key databases from NVRAM
Expert Key Management	Enables expert users to modify Secure Boot Policy variables without full authentication.

iBASE

4.6 Boot Settings

```
                              Aptio Setup – AMI
    Main  Advanced  Security  Boot  Save & Exit

    Boot Configuration                                    Number of seconds to wait for
    Setup Prompt Timeout              1                   setup activation key.
    Bootup NumLock State              [On]                65535(0xFFFF) means indefinite
    Quiet Boot                        [Disabled]          waiting.


    FIXED BOOT ORDER Priorities
    Boot Option #1                    [Hard Disk]
    Boot Option #2                    [NVME]
    Boot Option #3                    [CD/DVD]
    Boot Option #4                    [SD]
    Boot Option #5                    [USB Hard Disk]
    Boot Option #6                    [USB CD/DVD]
    Boot Option #7                    [USB Key]          �→←: Select Screen
    Boot Option #8                    [USB Floppy]       ↑↓: Select Item
    Boot Option #9                    [USB Lan]          Enter: Select
    Boot Option #10                   [Network]          +/-: Change Opt.
                                                         F1: General Help
                                                         F2: Previous Values
                                                         F3: Optimized Defaults
                                                         F4: Save & Exit
                                                         ESC: Exit



                         Version 2.22.1297 Copyright (C) 2025 AMI
```
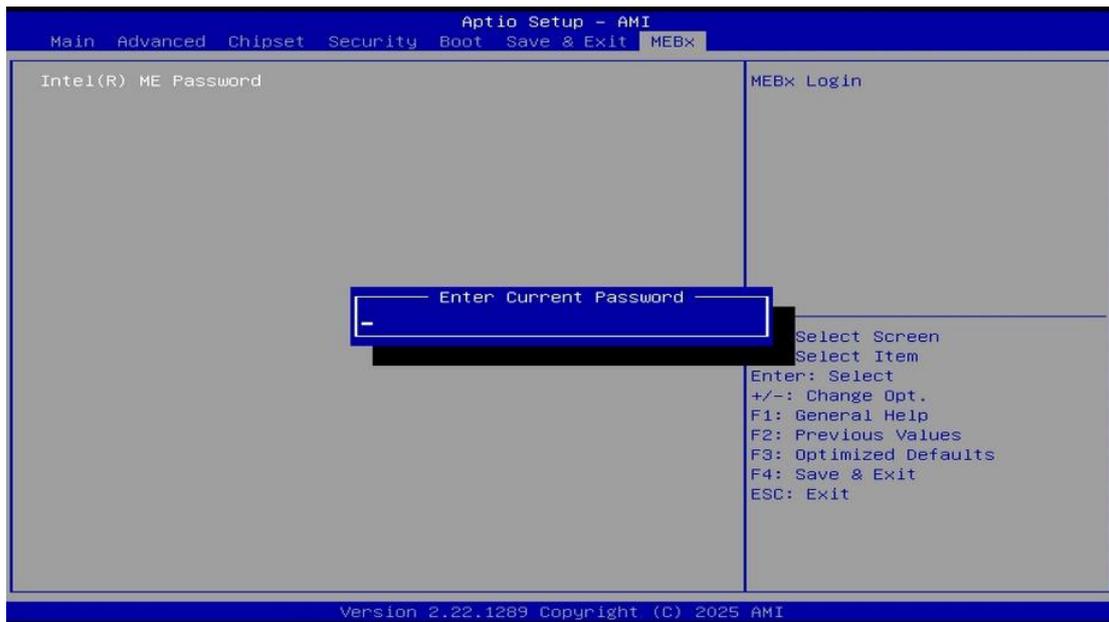
BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
FIXED BOOT ORDER Priorities	Sets the system boot order.

4.7 Save & Exit Settings

```
                          Aptio Setup - AMI
   Main  Advanced  Security  Boot  Save & Exit

 Save Options                                  Exit system setup after saving
 Save Changes and Exit                         the changes.
 Discard Changes and Exit

 Save Changes and Reset
 Discard Changes and Reset

 Save Changes
 Discard Changes

 Default Options
 Restore Defaults
 Save as User Defaults                         →←: Select Screen
 Restore User Defaults                         ↑↓: Select Item
                                               Enter: Select
 Boot Override                                 +/-: Change Opt.
 Launch EFI Shell from filesystem device       F1: General Help
                                               F2: Previous Values
                                               F3: Optimized Defaults
                                               F4: Save & Exit
                                               ESC: Exit


                   Version 2.22.1297 Copyright (C) 2025 AMI
```

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.
Launch EFI Shell from filesystem device	Attempts to launch EFI shell application (Shell.efi) from one of the available filesystem devices.

iBASE

4.8 MEBx Settings

```
                          Aptio Setup - AMI
        Main  Advanced  Chipset  Security  Boot  Save & Exit  MEBx

   Intel(R) ME Password                            MEBx Login








                                                  →←: Select Screen
                                                  ↑↓: Select Item
                                                  Enter: Select
                                                  +/-: Change Opt.
                                                  F1: General Help
                                                  F2: Previous Values
                                                  F3: Optimized Defaults
                                                  F4: Save & Exit
                                                  ESC: Exit




                     Version 2.22.1289 Copyright (C) 2025 AMI
```

```
                          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 2.22.1289 Copyright (C) 2025 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)
- Watchdog Timer Configuration

iBASE

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
0x00000080-0x00000080	Motherboard resources
0x00000092-0x00000092	Motherboard resources
0x000000B2-0x000000B3	Motherboard resources
0x00000680-0x0000069F	Motherboard resources
0x0000164E-0x0000164F	Motherboard resources
0x0000EFA0-0x0000EFBF	Intel (R) SMBus - 7722
0x000003F8-0x000003FF	Communications Port (COM1)
0x000002F8-0x000002FF	Communications Port (COM2)
0x000003E8-0x000003EF	Communications Port (COM3)
0x000002E8-0x000002EF	Communications Port (COM4)
0x00003050-0x00003057	Standard SATA AHCI Controller
0x00003040-0x00003043	Standard SATA AHCI Controller
0x00003020-0x0000303F	Standard SATA AHCI Controller
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer
0x00001854-0x00001857	Motherboard resources

Address	Device Description
0x00000000-0x00000CF7	PCI Express Root Complex
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x00002000-0x000020FE	Motherboard resources
0x0000FFF8-0x0000FFFF	Intel(R) Active Management Technology - SOL (COM5)
0x00000020-0x00000021	Programmable interrupt controller
0x00000024-0x00000025	Programmable interrupt controller
0x00000028-0x00000029	Programmable interrupt controller
0x0000002C-0x0000002D	Programmable interrupt controller
0x00000030-0x00000031	Programmable interrupt controller
0x00000034-0x00000035	Programmable interrupt controller
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

iBASE

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 4294967269-85	Intel(R) Ethernet Controller I226-V
IRQ 4294967252-68	Intel(R) Ethernet Controller I226-V #2
IRQ 4294967292	PCI Express Root Port
IRQ 4294967235-51	Intel(R) Ethernet Controller I226-LM
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 7	Communications Port (COM3)
IRQ 6	Communications Port (COM4)
IRQ 4294967290	Standard SATA AHCI Controller
IRQ 0	System timer
IRQ 4294967289	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 55-204	Microsoft ACPI-Compliant System
IRQ 256-511	Microsoft ACPI-Compliant System
IRQ 4294967293	PCI Express Root Port
IRQ 4294967232	Intel(R) GNA Scoring Accelerator module
IRQ 4294967287	Intel(R) Graphics
IRQ 19	Intel(R) Active Management Technology - SOL (COM5)
IRQ 4294967288	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967233	Intel(R) AI Boost
IRQ 4294967291	PCI Express Root Port
IRQ 4294967234	Intel(R) Management Engine Interface #1
IRQ 4294967286	Intel® Smart Sound Technology BUS
IRQ 4294967294	PCI Express Root Port

C. Watchdog Timer Configuration

The Watchdog Timer (WDT) is used to generate specific output signals after a user-programmable countdown. It is typically used to prevent system lock-up, such as when software becomes unresponsive or trapped in a deadlock. In such cases, the timer will count down to zero and trigger the designated output action.

Under normal circumstances, the WDT must be regularly reset or refreshed before the countdown reaches zero, ensuring that the system is functioning correctly.

Sample Code:

```
//-------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR
// PURPOSE.
//
//-------------------------------------------------------------------------
#include <dos.h>
#include <conio.h>
#include <stdio.h>
#include <stdlib.h>
#include "F81966.H"
//-------------------------------------------------------------------------
int main (int argc, char *argv[]);
void EnableWDT(int);
void DisableWDT(void);
//-------------------------------------------------------------------------
int main (int argc, char *argv[])
{
unsigned char bBuf;
unsigned char bTime;
char **endptr;

char SIO;

printf("Fintek 81966 watch dog program\n");
SIO = Init_F81966();
if (SIO == 0)
{
printf("Can not detect Fintek 81966, program abort.\n");
return(1);
}//if (SIO == 0)

if (argc != 2)
{
printf(" Parameter incorrect!!\n");
return (1);
}
```

```
bTime = strtol (argv[1], endptr, 10);
printf("System will reset after %d seconds\n", bTime);

if (bTime)
{      EnableWDT(bTime); }
else
{      DisableWDT();  }
return 0;
}
//---------------------------------------------------------------------------
void EnableWDT(int interval)
{
unsigned char bBuf;

bBuf = Get_F81966_Reg(0x2B);
bBuf &= (~0x20);
Set_F81966_Reg(0x2B,     bBuf);        //Enable WDTO

Set_F81966_LD(0x07);              //switch to logic device 7
Set_F81966_Reg(0x30,     0x01);        //enable timer

bBuf = Get_F81966_Reg(0xF5);
bBuf &= (~0x0F);
bBuf |= 0x52;
Set_F81966_Reg(0xF5,     bBuf);        //count mode is second

Set_F81966_Reg(0xF6,      interval);   //set timer

bBuf = Get_F81966_Reg(0xFA);
bBuf |= 0x01;
Set_F81966_Reg(0xFA,     bBuf);        //enable WDTO output

bBuf = Get_F81966_Reg(0xF5);
bBuf |= 0x20;
Set_F81966_Reg(0xF5,     bBuf);        //start counting
}
//---------------------------------------------------------------------------
void DisableWDT(void)
{
unsigned char bBuf;

Set_F81966_LD(0x07);              //switch to logic device 7

bBuf = Get_F81966_Reg(0xFA);
bBuf &= ~0x01;
Set_F81966_Reg(0xFA,     bBuf);        //disable WDTO output

bBuf = Get_F81966_Reg(0xF5);
bBuf &= ~0x20;
bBuf |= 0x40;
Set_F81966_Reg(0xF5,     bBuf);        //disable WDT
}
//---------------------------------------------------------------------------
```

```
//-------------------------------------------------------------------------
//
// THIS CODE AND INFORMATION IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY
// KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE
// IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A
PARTICULAR
// PURPOSE.
//
//-------------------------------------------------------------------------
#include "F81966.H"
#include <dos.h>
//-------------------------------------------------------------------------
unsigned int F81966_BASE;
void Unlock_F81966 (void);
void Lock_F81966 (void);
//-------------------------------------------------------------------------
unsigned int Init_F81966(void)
{
unsigned int result;
unsigned char ucDid;

F81966_BASE = 0x4E;
result = F81966_BASE;

ucDid = Get_F81966_Reg(0x20);
if   (ucDid == 0x07)          //Fintek 81966
{      goto     Init_Finish;    }

F81966_BASE = 0x2E;
result = F81966_BASE;

ucDid = Get_F81966_Reg(0x20);
if   (ucDid == 0x07)          //Fintek 81966
{      goto     Init_Finish;    }

F81966_BASE = 0x00;
result = F81966_BASE;

Init_Finish:
return (result);
}
//-------------------------------------------------------------------------
void Unlock_F81966 (void)
{
outportb(F81966_INDEX_PORT, F81966_UNLOCK);
outportb(F81966_INDEX_PORT, F81966_UNLOCK);
}
//-------------------------------------------------------------------------
void Lock_F81966 (void)
{
outportb(F81966_INDEX_PORT, F81966_LOCK);
}
```

iBASE

```
//--------------------------------------------------------------------------
void Set_F81966_LD( unsigned char LD)
{
Unlock_F81966();
outportb(F81966_INDEX_PORT, F81966_REG_LD);
outportb(F81966_DATA_PORT, LD);
Lock_F81966();
}
//--------------------------------------------------------------------------
void Set_F81966_Reg( unsigned char REG, unsigned char DATA)
{
Unlock_F81966();
outportb(F81966_INDEX_PORT, REG);
outportb(F81966_DATA_PORT, DATA);
Lock_F81966();
}
//--------------------------------------------------------------------------
unsigned char Get_F81966_Reg(unsigned char REG)
{
unsigned char Result;
Unlock_F81966();
outportb(F81966_INDEX_PORT, REG);
Result = inportb(F81966_DATA_PORT);
Lock_F81966();
return Result;
}
//--------------------------------------------------------------------------
```