IB96W

13th Gen Intel® Core™ i Mobile Wide-Temp Processor (RPL-P Platform) 3.5" Disk-Size SBC

User's Manual

Version 1.0
(July 2025)

iBASE

Compliance

CE

This product has passed CE tests for environmental specifications and limits and complies with applicable EU directives. In a domestic environment, it may cause radio interference, requiring users to take appropriate measures."

FC

This product complies with Class B limits under Part 15 of the FCC Rules, providing reasonable protection against harmful interference in residential installations. It generates, uses, and can radiate radio frequency energy. If not installed and used according to the manufacturer's instructions, it 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 on 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 complies with RoHS 2 restrictions, which prohibit the use of certain hazardous substances in electrical and electronic equipment. The following substances must not exceed the specified concentrations:

- 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

Important Safety Information

Carefully read the precautions before using the board.

Care for your IBASE products:

- Before cleaning the PCB, ensure the device is unplugged and powered off
- Use circuit board cleaner or alcohol carefully to avoid damage to sensitive components.
- Vacuum the dust with a computer vacuum cleaner to prevent the fan from being clogged.

WARNING

Attention during use:

- Do not use this product near water.
- Do not spill water or any other liquids on this product.
- Do not place heavy objects on the *product, as it may damage internal components or affect performance.*

Anti-static precautions

- Wear an anti-static wrist strap to avoid electrostatic discharge.
- Place the PCB on an anti-static mat.
- Hold the edges of the PCB when handling.
- When handling, avoid touching the surface of the PCB and hold it by its edges or non-metallic components.
- Ground yourself by touching a grounded metal object, such as a metal pipe or grounded equipment, to discharge static.

Caution:

Danger of explosion if the internal lithium-ion battery is replaced by an incorrect type. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions or recycle them at a local recycling facility or battery collection point.

Warranty Policy

- **IBASE standard products:**

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

- **3rd-party parts:**

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

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

Technical Support & Services

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

Table of Contents

Chapter 1
General Information

The information provided in this chapter includes:

- Features
- Packing List
- Optional Accessories
- Specifications
- Block Diagram
- Board Pictures
- Board Dimensions

1.1 Introduction

Powered by the latest 13th Gen Intel® Core™ i7/i5/i3 mobile wide-temp processors, the IB96W ensures high performance and exceptional efficiency for a wide range of applications. Accompanied by a DDR5 SO-DIMM socket with a 32GB capacity, the motherboard guarantees seamless multitasking and improved system responsiveness. Graphics support is provided by 2x DP++, LVDS, and eDP for independent display outputs. Two Intel® PCI-E 2.5G LAN ensures high-speed networking for seamless data transfer. Equipped with 3x USB 2.0, 3x USB 3.2, 2x COM, and 2x SATA III ports, the IB96W offers exceptional peripheral connectivity, and 3x M.2 slots (M-Key + E-key + B-key) enhances expandability options.

1.2 Features

- Onboard 13th Gen Intel® Core™ i7-1370PRE mobile processor, supports wide-temp.
- 1x DDR5 SO-DIMM, up to 32GB, supports IBECC
- Supports 2x DP++, LVDS, and eDP
- 2x Intel® I226IT PCIe 2.5G LAN
- 3x USB 2.0, 3x USB 3.2, 2x COM, 2x SATA III
- 3x M.2 slots (M-Key + E-key + B-key)
- Supports digital I/O (4-in/4-out), fTPM, and watchdog timer

1.3 Packing List

Your IB96W package should include the items listed below. If any of the items below is missing, contact the distributor or dealer from whom you purchased the product.

- IB96W SBC
- Disk
  (including chipset drivers and flash memory utility)
- This User's Manual

1.4 Optional Accessories

IBASE provides the following optional accessories:

- Cable Kit (IB76A-2)

  Including:

DC-In power cable (PW592)	x1
COM ports cable (PK1H)	x1
SATA & HDD power cable (SATA-53A)	x1
USB 2.0 cable (USB29)	x1

- Audio cable (Audio-18)
- Heat spreader (HSIB96W-1)
- Heat sink (HSIB96W-A), aluminum based heatsink + CPU cooler
- Heat sink (HSIB96W-B), aluminum & cooper based heatsink + CPU cooler

1.5 Specifications

Model	
IB96WVF-I7PRE	Intel® Core™ I7-1370PRE 3.5" SBC w/ I226IT 2.5G LAN, VGA (2x DisplayPort(1.4) + eDP + LVDS), 2x SATA III, 2x COM, 3x M.2 (M2280/E2230 & B3052), DC in (12V~24V), iAMT, fTPM (RoHS 2)

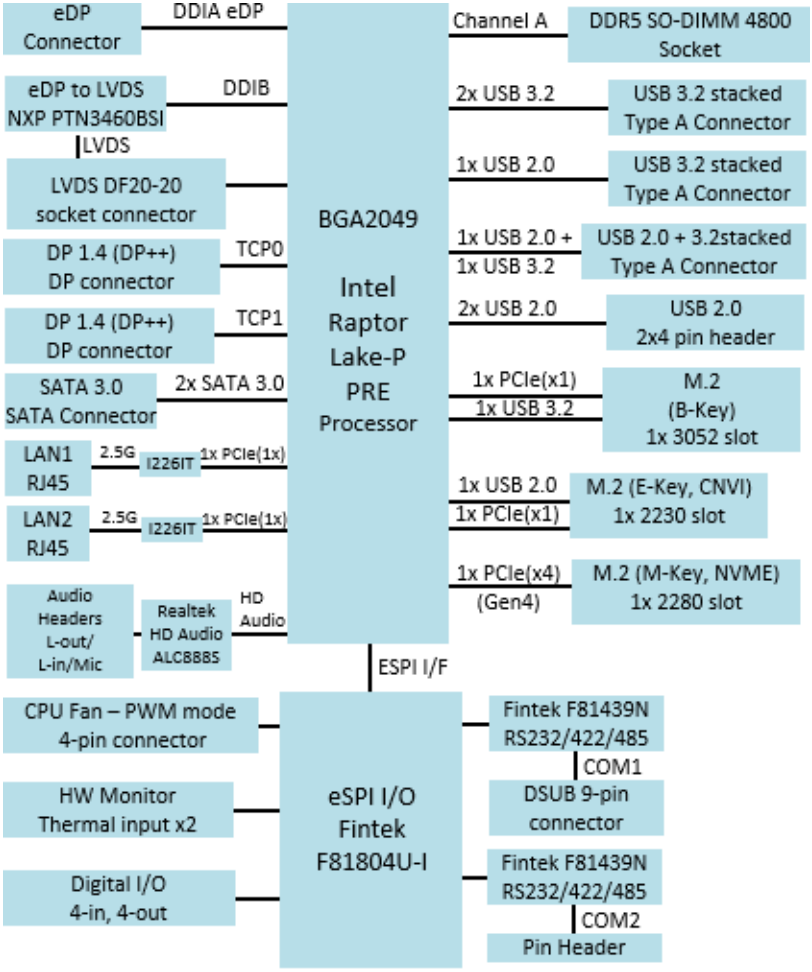
Specifications	
CPU	Onboard 13th Gen Intel® Core™ P-Series processors
Form Factor	3.5" disk-size SBC
Memory	1x DDR5 SO-DIMM, Max. 32GB, supports IBECC
BIOS	AMI
Graphics	13th Gen Intel® processor integrated graphics
Display Output	2x DisplayPort, eDP & LVDS
LAN	Intel® I226IT (1st LAN / 2nd LAN)
Super I/O	Fintek F81804U-I
Storage Interface	M.2 (M2280 for NVMe)
Mini Type Slots	1x M.2 (M-Key, Type:2280, with PCIe (4x) signal only, supports NVMe) 1x M.2 (E-Key, Type:2230, with PCIe (1x) & USB 2.0 signal, supports CNVi) 1x M.2 (B-Key, Type:3052, with PCIe (1x) & USB 3.2 signal, supports 5G/LTE
Audio	Built-in HD audio with Realtek AL888S-VD2-GR
Watchdog Timer	Yes (256 segments, 0, 1, 2…255 sec / min)
H/W Monitor	Yes
Power Requirement	+12V (-10% tolerance) ~ +24V (+10% tolerance) DC-in
fTPM	Yes
iAMT	16.1
Dimensions	102.22 x 147.01 mm (4.02" x 5.8")
RoHS 2	Yes
Certification	CE, FCC Class B

I/O Ports	
Display	• 2x DisplayPort • eDP • 24-bit dual-channel LVDS
LAN	2 x RJ45 for 2.5 Gigabit Ethernet
USB	• 3x USB 2.0 (1x Type-A, 2x via pin header) • 3x USB 3.2 (Type-A)
Serial	• 2x RS232/422/485
SATA	2 x SATA III
Digital IO	4-In & 4-Out
Operating System	Windows 11 LTSC Windows 10 (For Intel® Smart Sound Technology only) Ubuntu Linux (64bit)

Environmental	
Temperature	• Operating: -40~75°C (-40~167°F) • Storage: -40~80 °C (-40~176 °F)
Relative Humidity	0 ~ 90 %, non-condensing at 60 °C

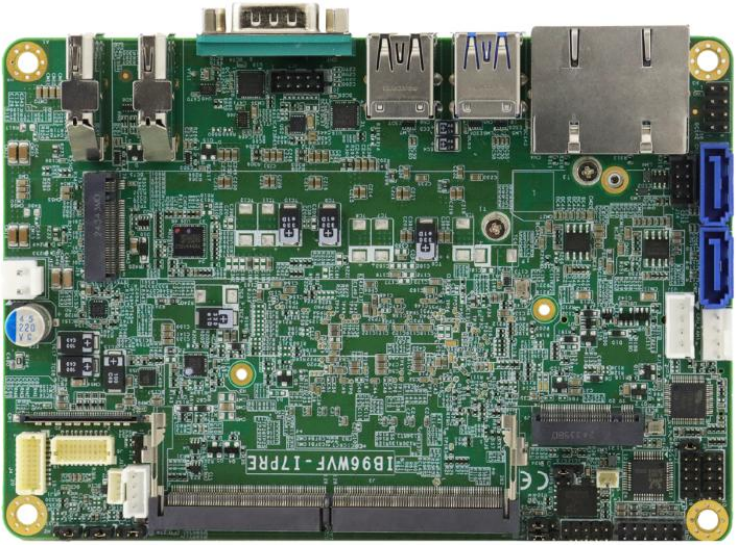
All specifications are subject to change without prior notice.

1.6 Block Diagram

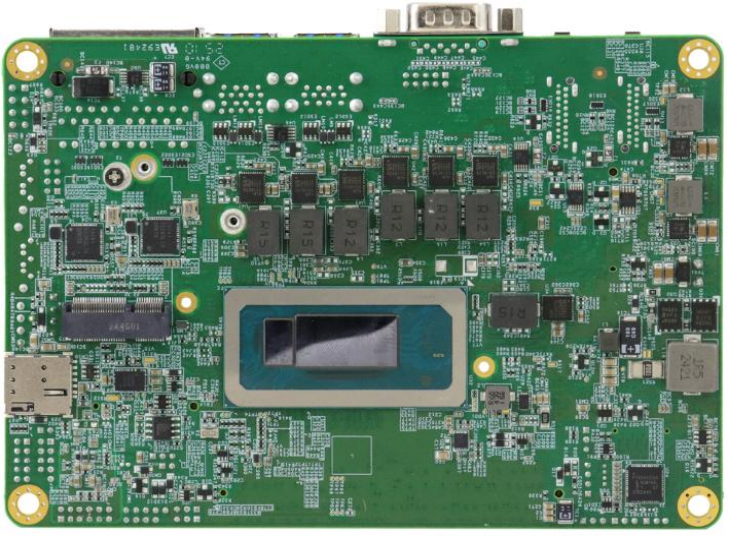


1.7 Board Pictures

Top View

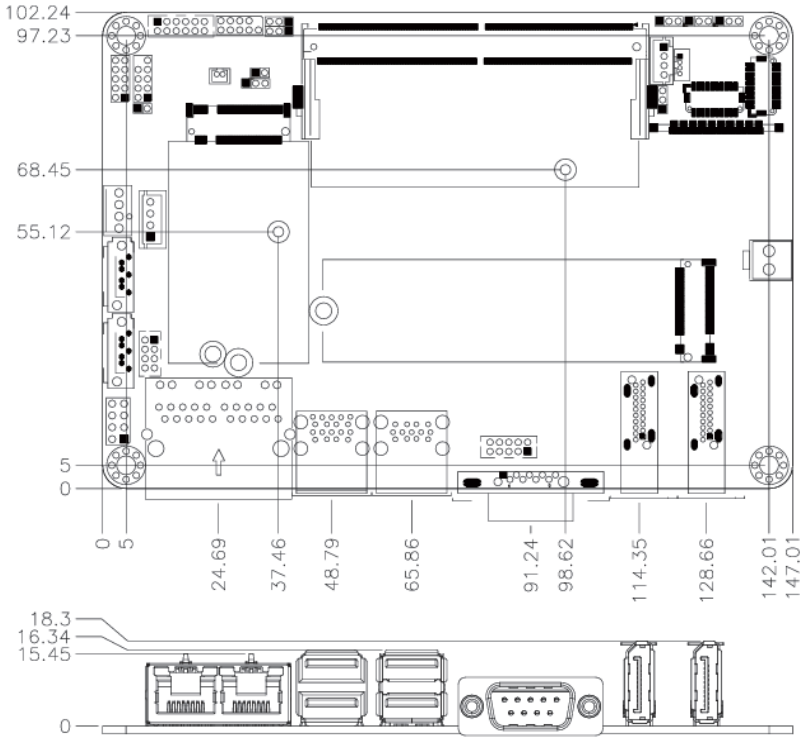


Bottom View



I/O View

1.8 Dimensions



Chapter 2
Hardware Configuration

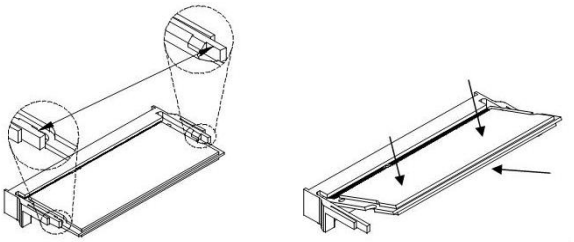
This section provides information on jumper settings and connectors on the IB96W in order to set up a workable system. On top of that, you will also need to install crucial pieces such as the CPU and the memory before using the product. The topics covered are:

- Essential installations
- Jumpers and connectors

2.1 Essential Installations

2.1.1 Installing the Memory

The IB96W supports one memory socket for DDR5 modules. To install a module, locate the memory slot on the board and perform the following steps:



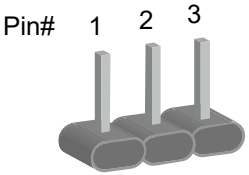
1. Align the key of the memory module with that on the memory slot and insert the module slantwise.
2. Gently push the module in an upright position until the clips of the slot close to hold the module in place when the module touches the bottom of the slot.

To remove the module, press the clips outwards with both hands, and the module will pop-up.

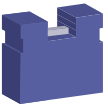
2.2 Setting the Jumpers

Set up and configure your IB96W by using jumpers for various settings and features according to your needs and applications. Contact your supplier if you have doubts about the best configuration for your use.

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

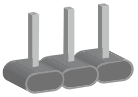
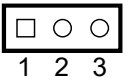
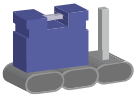
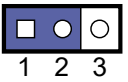
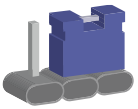
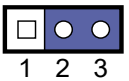


A 3-pin jumper



A jumper cap

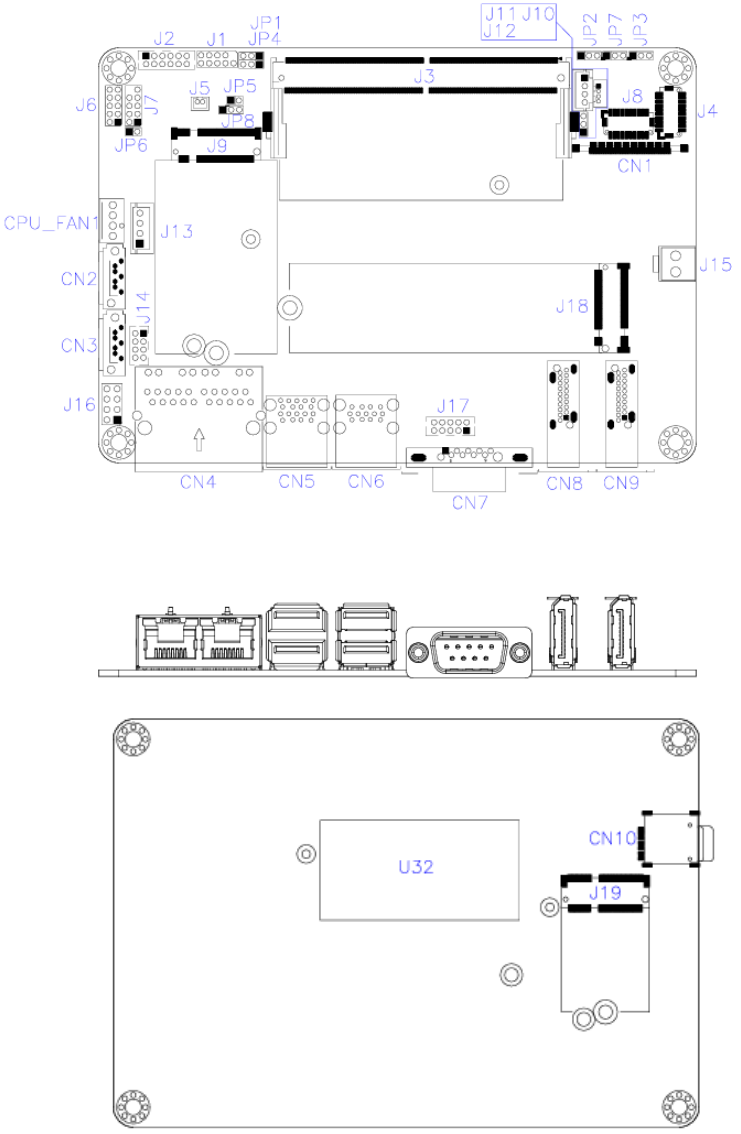
Refer to the illustration below to set jumpers.

Pin closed	Jumper	Setting
Open		
1-2		
2-3		

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

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

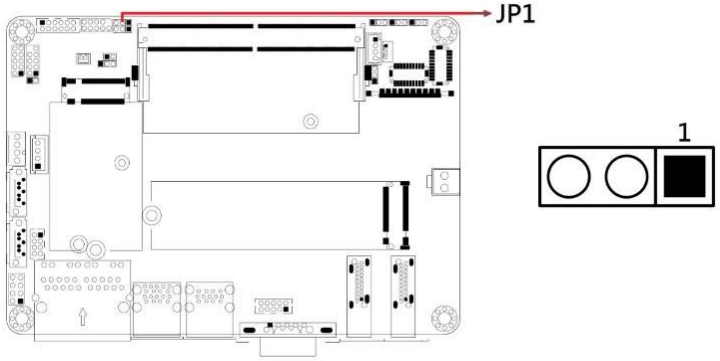
2.3 Jumper & Connector Locations



2.4 Jumpers Quick Reference

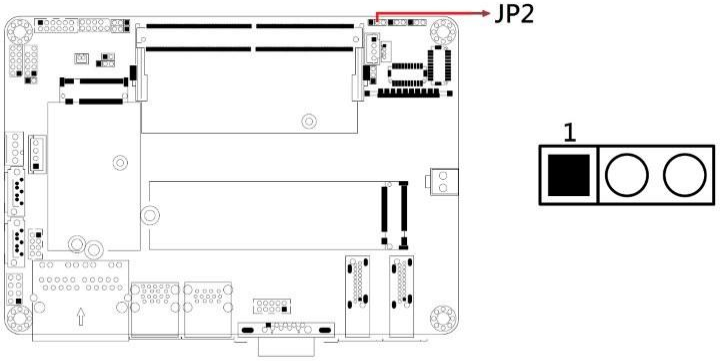
Jumper	Function
JP1	Clear RTC Data
JP2	eDP Power Selection
JP3	LVDS Power Selection
JP4	Clear CMOS Data
JP5	Flash Descriptor Security Override
JP6	AT/ATX Selection
JP7	LVDS Brightness Power Selection
JP8	Sierra EM9 Series 5G card USB/PCIe Select

2.4.1 JP1: Clear RTC Data



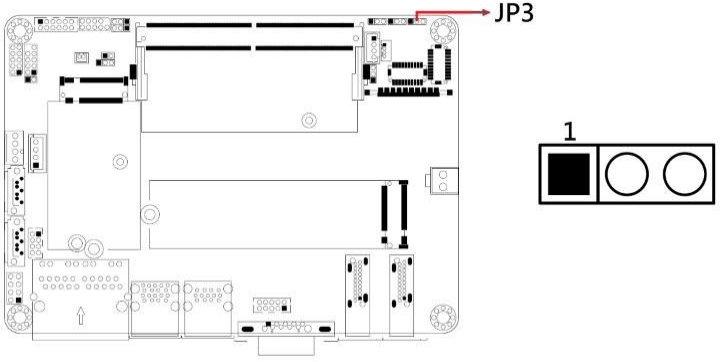
Function	Pin closed	Setting
Normal	1-2	1
Clear RTC	2-3	1

2.4.2 JP2: eDP Power Selection



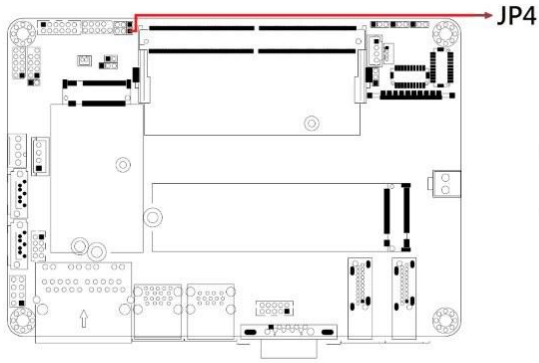
Function	Pin closed	Setting
3.3V (default)	1-2	1
5V	2-3	1

2.4.3 JP3: LVDS Power Selection



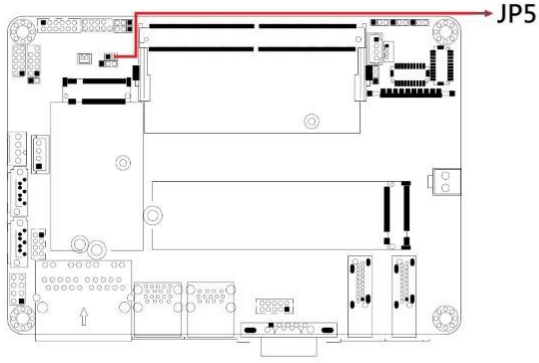
Function	Pin closed	Setting
3.3V (default)	1-2	1
5V	2-3	1

2.4.4 JP4: Clear CMOS Data



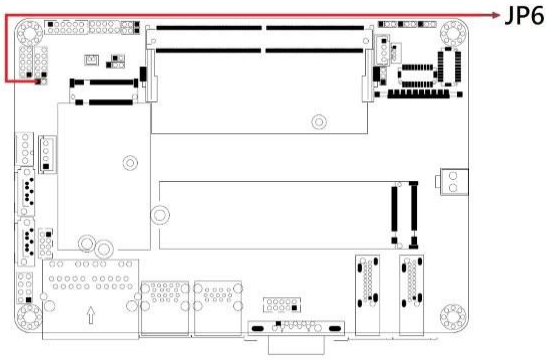
Function	Pin closed	Setting
Normal	1-2	1
Clear CMOS	2-3	1

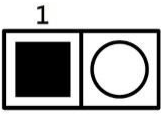
2.4.5 JP5: Flash Descriptor Security Override



Remarks: Factory use only

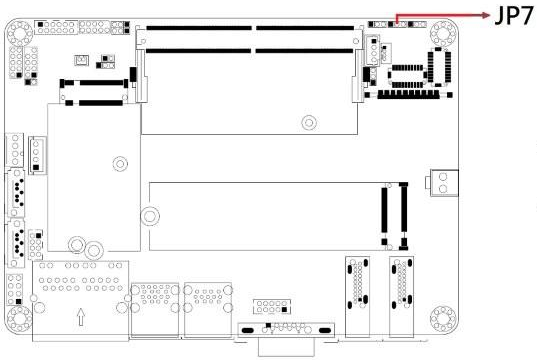
2.4.6 JP6: AT/ATX Selection





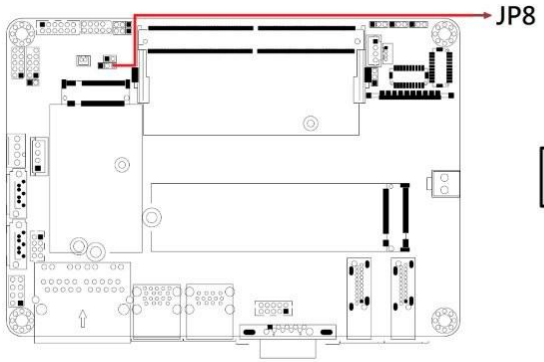
Function	Pin closed	Setting
ATX	Open (default)	
AT	Close	

2.4.7 JP7: LVDS Brightness Power Selection



Function	Pin closed	Setting
3.3V (default)	1-2	1 
5V	2-3	1 

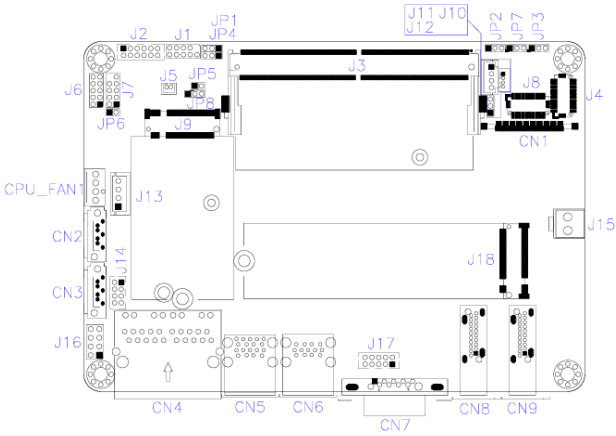
2.4.8 JP8: Sierra EM9 Series 5G card USB/PCIe Select

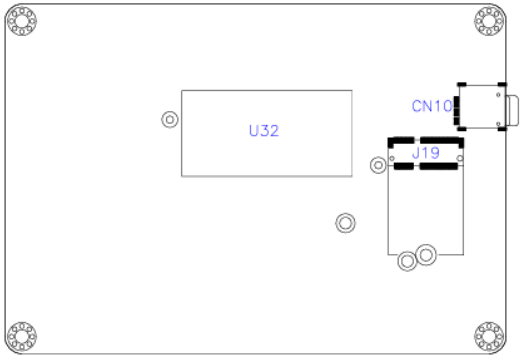


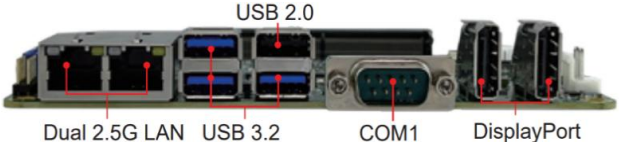
Function	Pin closed	Setting
USB (default)	1-2	1 
PCIe	2-3	1 

2.5 Connectors Quick Reference

Connector	Function
CN1	eDP Connector
CN2, CN3	SATA #0 / #1 Ports
CN4	2.5G LAN i226IT Ports
CN5	USB3 #1 / #2 Ports
CN6	USB3 #3 / USB2 #4 Ports
CN7	COM1 Serial Port
CN8, CN9	DP++ Ports
CN10	SIM Socket
J1	SPI Flash Connector
J2	Audio Connector
J3	DDR5 SO-DIMM Socket
J4	LVDS CH-B Connector
J5	Battery Connector
J6	Digital I/O (4in, 4out) Connector
J7	eSPI Debug Connector
J8	LVDS CH-A Connector
J9	M.2 B-Key 3052 Socket
J10	SMBUS Connector
J11	LVDS Backlight Connector
J13	SATA Power Connector
J14	USB2 #5/#6 Connectors
J15	DC-In Connector
J16	Front Panel Connector
J17	COM2 Serial Port
J18	M.2 M-Key 2280 Socket
J19	M.2 E-Key 2230 Socket
CPU_FAN1	CPU Fan Power Connector

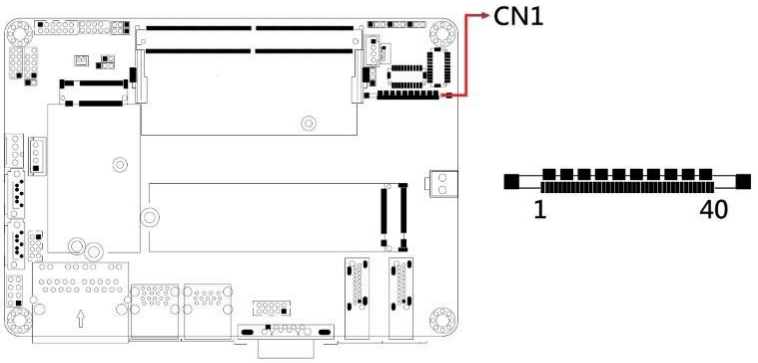






Function	Connector
Dual 2.5 GbE Ports	CN4
USB Ports	CN6, CN5
COM1 Serial Port	CN7
DisplayPort	CN8, CN9

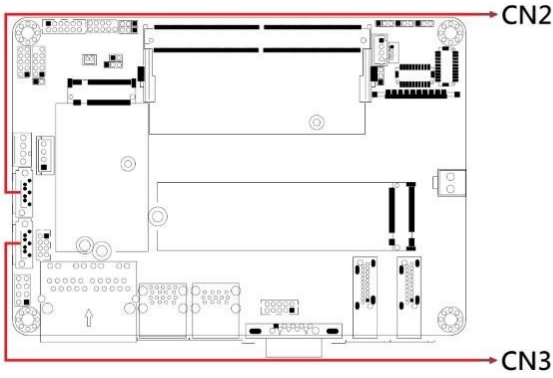
2.5.1 CN1: eDP Connector

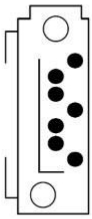


* KEL_SSL00-40S

Pin	Assignment	Pin	Assignment
1	eDP Vcc	21	TXN0
2	eDP Vcc	22	TXP0
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

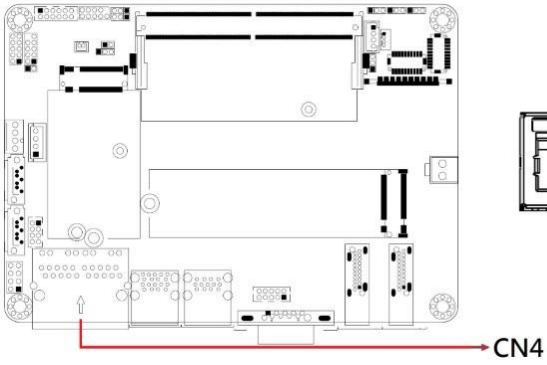
2.5.2 CN2, CN3: SATA #0 / #1 Ports

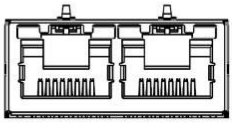




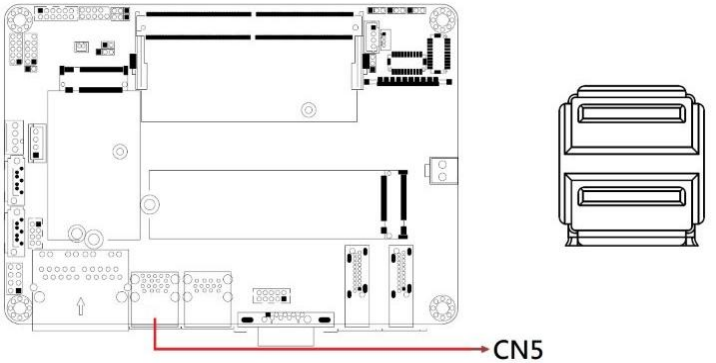
Pin	Assignment	Pin	Assignment
1	Ground	4	Ground
2	TX+	5	RX-
3	TX-	6	RX+
4	Ground	7	Ground

2.5.3 CN4: 2.5G LAN 226IT Ports

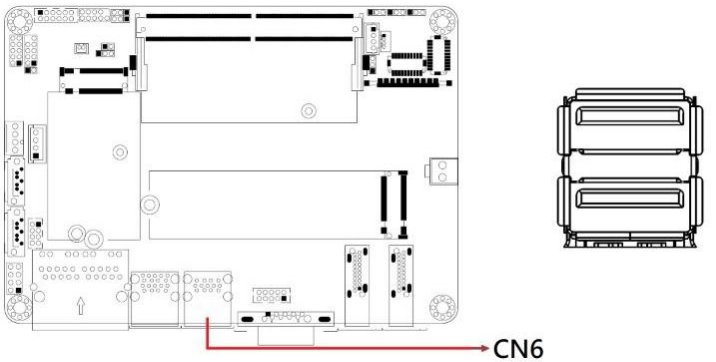




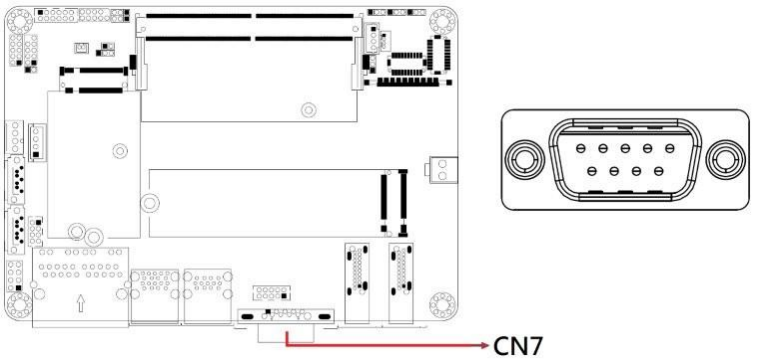
2.5.4 CN5: USB3 #1 / #2 Ports



2.5.5 CN6: USB3 #3 / USB2 #4 Ports

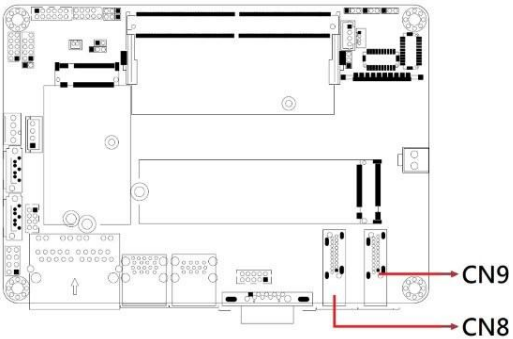


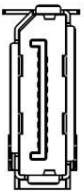
2.5.6 CN7: COM1 Serial Port



Pin	Assignment		
	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

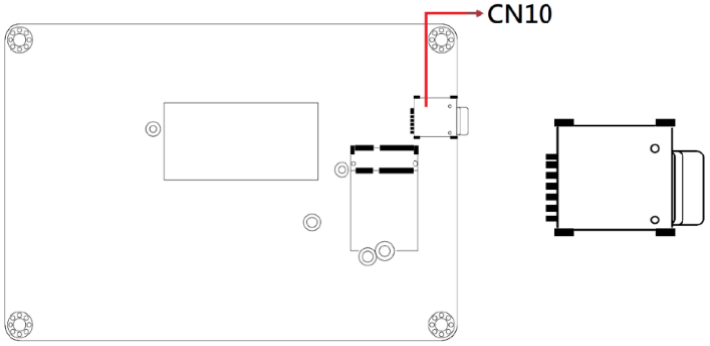
2.5.7 CN8, CN9: DP++ Ports





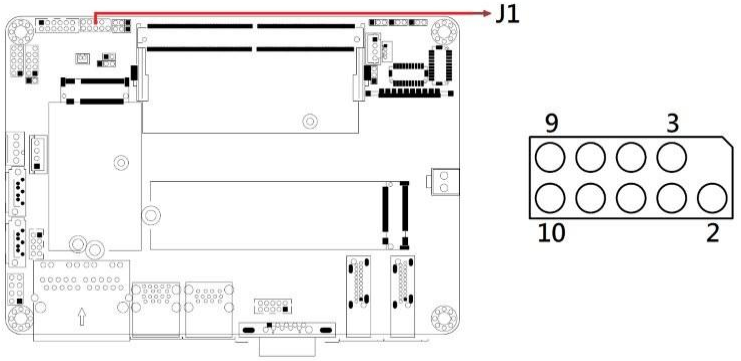
Pin	Assignment	Pin	Assignment
1	LAN0_P	11	GND
2	GND	12	LAN3_N
3	LAN0_N	13	CONFIG
4	LAN1_P	14	GND
5	GND	15	AUXP
6	LAN1_N	16	GND
7	LAN2_P	17	AUXN
8	GND	18	Hot Plug
9	LAN2_N	19	GND
10	LAN3_P	20	+5V

2.5.8 CN10: SIM Socket

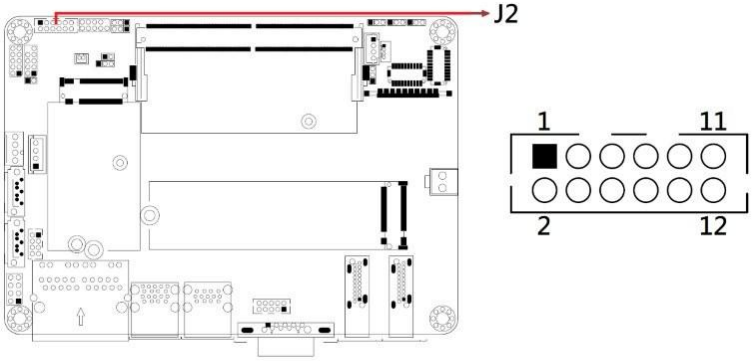


2.5.9 J1: SPI Flash Connector

* Factory use only



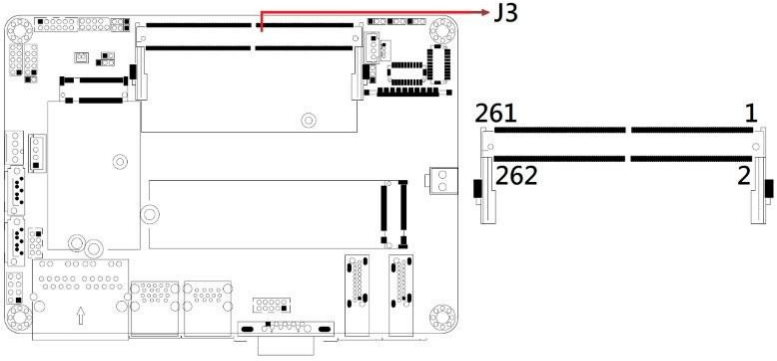
2.5.10 J2: Audio Connector



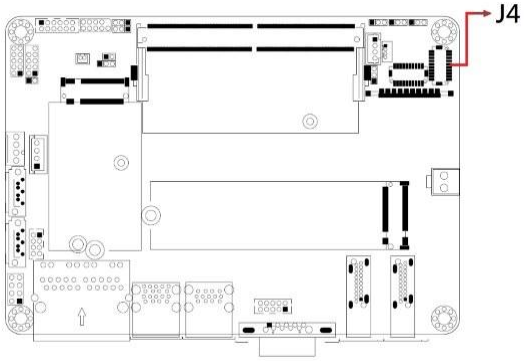
* HK_DF11-12S-PA66H

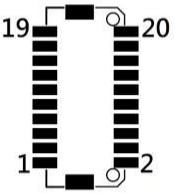
Pin	Assignment	Pin	Assignment
1	LINE OUT_L	2	LINE OUT_R
3	FRONT_JD	4	GND
5	LINE IN_L	6	LINE IN_R
7	LINE _JD	8	GND
9	MIC_L	10	MIC_R
11	MIC_JD	12	GND

2.5.11 J3: DDR5 SO-DIMM Socket



2.5.12 J4: LVDS CH-B Connector

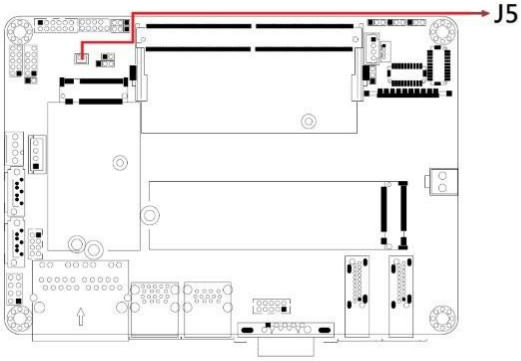


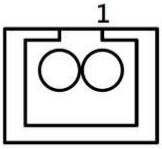


* Hirose_DF20G-20DP-1V(56

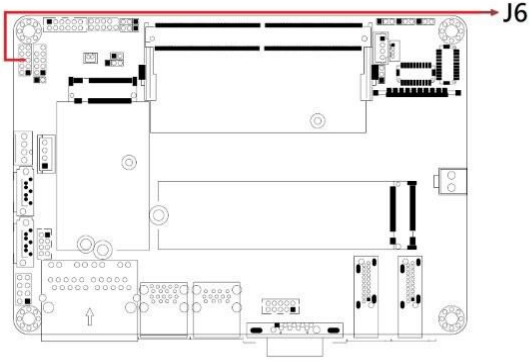
Pin	Assignment	Pin	Assignment
1	TX0P	2	TX0N
3	GND	4	GND
5	TX1P	6	TX1N
7	GND	8	GND
9	TX2P	10	TX2N
11	GND	12	GND
13	CLKP	14	CLKN
15	GND	16	GND
17	TX3P	18	TX3N
19	+3.3V	20	+3.3V

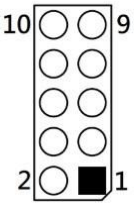
2.5.13 J5: Battery Connector





2.5.14 J6: Digital I/O (4in, 4out) Connector



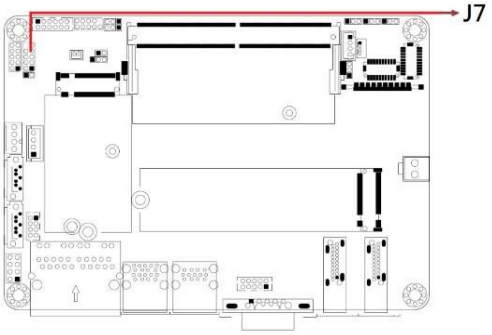


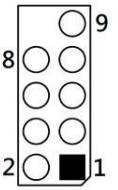
* E-Call_0196-01-200-100

Pin	Assignment	Pin	Assignment
1	Ground	2	+5V
3	Out3	4	Out1
5	Out2	6	Out0
7	IN3	8	IN1
9	IN2	10	IN0

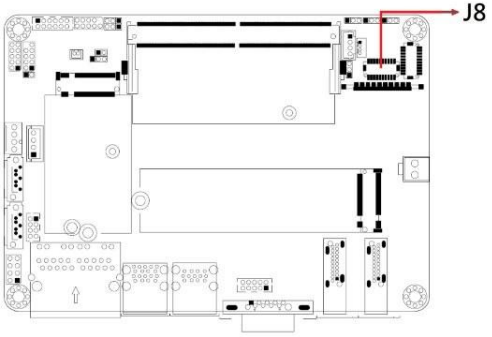
2.5.15 J7: eSPI Debug Connector

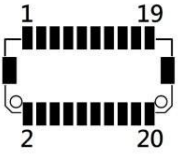
* Factory use only





2.5.16 J8: LVDS CH-A Connector

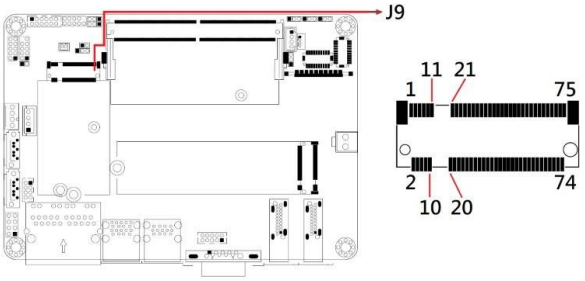




* Hirose_DF20G-20DP-1V(56

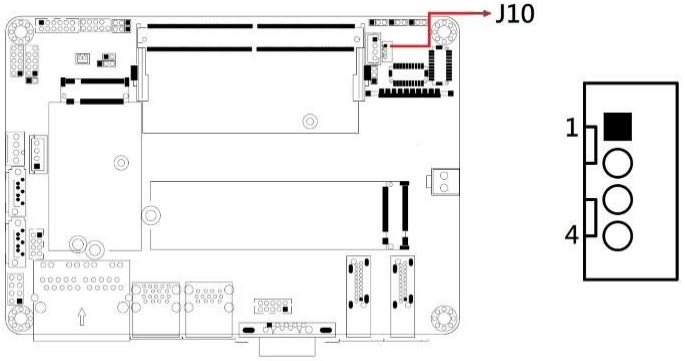
Pin	Assignment	Pin	Assignment
1	TX0P	2	TX0N
3	GND	4	GND
5	TX1P	6	TX1N
7	GND	8	GND
9	TX2P	10	TX2N
11	GND	12	GND
13	CLKP	14	CLKN
15	GND	16	GND
17	TX3P	18	TX3N
19	+3.3V	20	+3.3V

2.5.17 J9: M.2 B-Key 3052 Socket



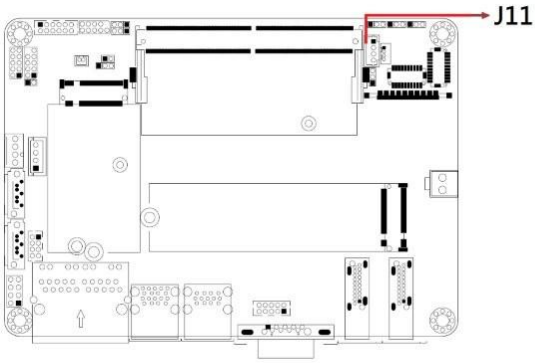
Pin	Assignment	Pin	Assignment
1	NC	2	3.3V
3	GND	4	3.3V
5	GND	6	FULL_CARD_POWER_OFF#
7	USB_D+	8	W_DISABLE1#
9	USB_D-	10	NC
11	GND	12	NC
13	NC	14	NC
15	NC	16	NC
17	NC	18	NC
19	NC	20	GPIO5
21	NC	22	GPIO6
23	NC	24	GPIO7
25	NC	26	NC
27	GND	28	NC
29	USB3_RXN	30	SIM_RST#
31	USB3_RXP	32	SIM_CLK
33	GND	34	SIM_IO
35	USB3_TXN	36	SOM_VCC
37	USB3_TXP	38	NC
39	GND	40	NC
41	PCIE_RXN	42	NC
43	PCIE_RXP	44	NC
45	GND	46	NC
47	PCIE_TXN	48	NC
49	PCIE_TXP	50	PCIE_RST#
51	GND	52	CLK_REQ#
53	PCIE_CLK_N	54	PCIE_WAKE#
55	PCIE_CLK_P	56	NC
57	GND	58	NC
59	NC	60	NC
61	NC	62	NC
63	NC	64	NC
65	NC	66	SIM_CD
67	NC	68	SUS_CLK
69	NC	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	NC		

2.5.18 J10: SMBUS Connector



Pin	Assignment
1	VCC3
2	SMB_CLK
3	SMB_Data
4	Ground

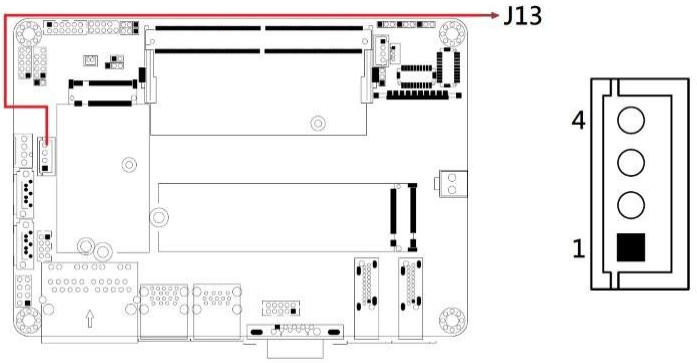
2.5.19 J11: LVDS Backlight Connector



* E-Call_0110-161-040

Pin	Assignment
1	+12V
2	Backlight Enable
3	Brightness Control
4	GND

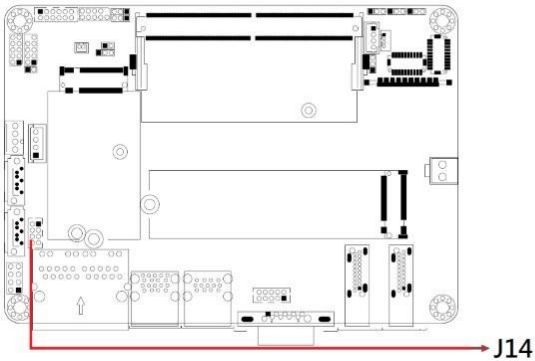
2.5.20 J13: SATA Power Connector

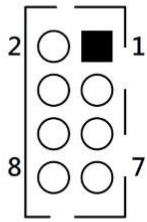


* E-Call_0110-071-040

Pin	Assignment
1	+5V
2	GND
3	GND
4	+12V

2.5.21 J14: USB2 #5/#6 Connectors

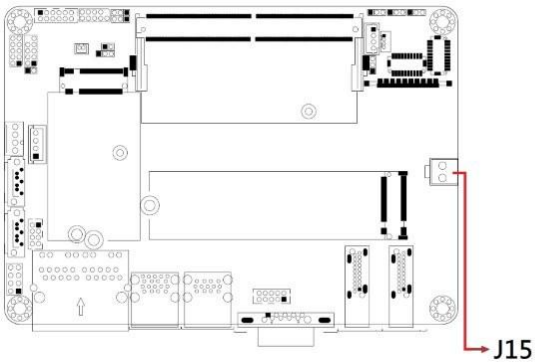


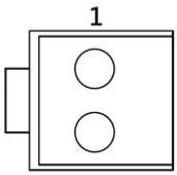


* HK_DF11-8S-PA66H

Pin	Assignment	Pin	Assignment
1	+5V	2	GND
3	USB_PN	4	USB_PP
5	USB_PP	6	USB_PN
7	GND	8	+5V

2.5.22 J15: DC-In Connector

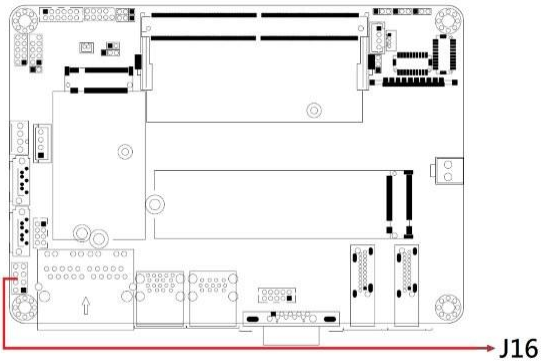


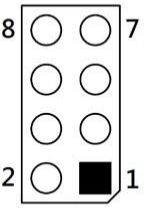


* HK_WAFER396-2S-WV

Pin	Assignment
1	DC_IN
2	GND

2.5.23 J16: Front Panel Connector





* E-Call_0126-01-203-080

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

This connector provides interfaces for the following functions.

- **ATX Power ON Switch (Pins 1 and 2)**

  These pins make an “ATX Power Supply On/Off Switch” for the system, connecting to the power switch on the case. Pressing this switch powers on the system, and pressing it again powers it off.

- **Hard Disk Drive LED Connector (Pins 3 and 4)**

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

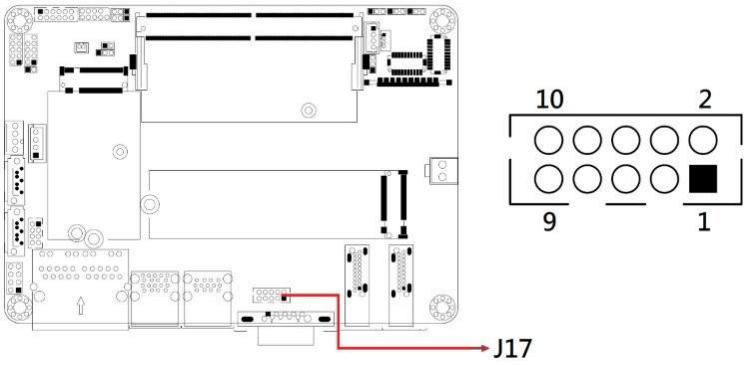
- **Reset Switch (Pins 5 and 6)**

  The reset switch allows you to reset the system without toggling the main power switch. Orientation is not required when making a connection to this header.

- **Power LED: Pins 7 and 8**

  This connector attaches to the system power LED on control panel. This LED illuminates when the system turns on.

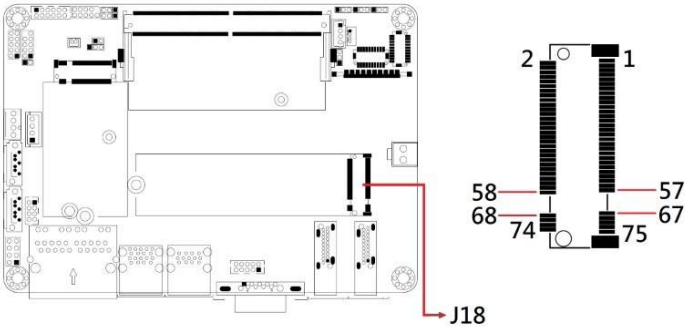
2.5.24 J17: COM2 Serial Port



* HK_DF11-10S-PA66H

Pin	Assignment		
	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
10	NC	NC	NC

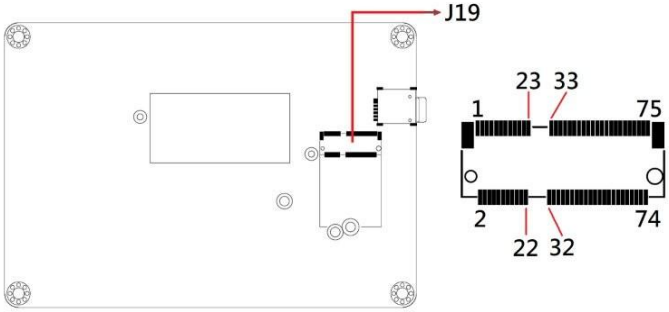
2.5.25 J18: M.2 M-Key 2280 Socket



Pin	Assignment	Pin	Assignment
1	GND	2	3.3V
3	GND	4	3.3V
5	PCIE_RXN3	6	NC
7	PCIE_RXP3	8	NC
9	GND	10	SSD_LED
11	PCIE_TXN3	12	3.3V
13	PCIE_TXP3	14	3.3V
15	GND	16	3.3V
17	PCIE_RXN2	18	3.3V
19	PCIE_RXP2	20	NC
21	GND	22	NC
23	PCIE_TXN2	24	NC
25	PCIE_TXP2	26	NC
27	GND	28	NC
29	PCIE_RXN1	30	NC
31	PCIE_RXP1	32	NC
33	GND	34	NC
35	PCIE_TXN1	36	NC
37	PCIE_TXP1	38	NC
39	GND	40	NC
41	PCIE_RXN0	42	NC
43	PCIE_RXP0	44	NC
45	GND	46	NC
47	PCIE_TXN0	48	NC
49	PCIE_TXP0	50	PCIE_RST#
51	GND	52	CLK_REQ#
53	PCIE_CLK_N	54	PCIE_WAKE#
55	PCIE_CLK_P	56	NC
57	GND	58	NC
59	NC	60	NC
61	NC	62	NC
63	NC	64	NC
65	NC	66	NC
67	NC	68	SUS_CLK
69	NC	70	3.3V
71	GND	72	3.3V
73	GND	74	3.3V
75	GND		

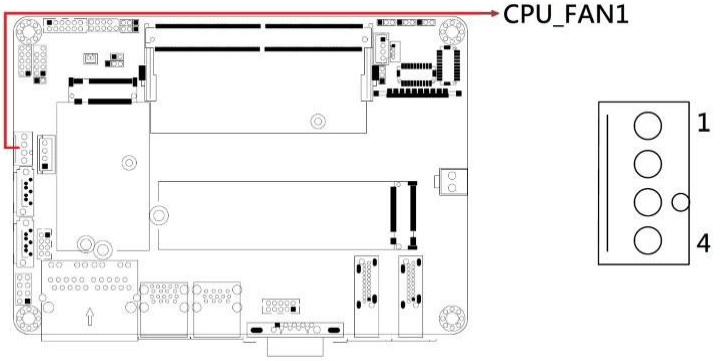
2.5.26 J19: M.2 E-Key 2230 Socket

* With CNVI support



Pin	Assignment	Pin	Assignment
1	GND	2	3.3V
3	USB_D+	4	3.3V
5	USB_D-	6	NC
7	GND	8	NC
9	CNV_WR_D1_DN	10	M.2_BT_PCMFRM
11	CNV_WR_D1_DP	12	NC
13	GND	14	M.2_BT_PCMOUT
15	CNV_WR_D0_DN	16	NC
17	CNV_WR_D0_DP	18	GND
19	GND	20	UART_BT_WAKE#
21	CNV_WR_CLK_DN	22	CNV_BRI_RSP
23	CNV_WR_CLK_DN	24	NC
25	NC	26	NC
27	NC	28	NC
29	NC	30	NC
31	NC	32	CNV_RGI_DT
33	GND	34	CNV_RGI_RSP
35	PCIE_TXP	36	CNV_BRI_DT
37	PCIE_TXN	38	CNV_WLAN_CLINK_RST_N
39	GND	40	CNV_WLAN_CLINK_DATA
41	PCIE_RXP	42	CNV_WLAN_CLINK_CLK
43	PCIE_RXN	44	NC
45	GND	46	NC
47	PCIE_CLK_P	48	NC
49	PCIE_CLK_N	50	SUS_CLK
51	GND	52	PCIE_RST#
53	CLK_REQ#	54	BT_RF_OFF
55	PCIE_WAKE#	56	WIFI_RF_OFF
57	GND	58	NC
59	CNV_WT_D1_DN	60	NC
61	CNV_WT_D1_DP	62	NC
63	GND	64	NC
65	CNV_WT_D0_DN	66	PCIE_RST#
67	CNV_WT_D0_DP	68	NC
69	GND	70	PCIE_WAKE#
71	CNV_WT_CLK_DN	72	3.3V
73	CNV_WT_CLK_DN	74	3.3V
75	GND		

2.5.27 CPU_FAN1: CPU Fan Power Connector



* PWM Only

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

Chapter 3
Drivers Installation

This chapter introduces installation of the following drivers:

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

3.1 Introduction

This section describes the installation procedures for software drivers. The software drivers are available on the IBASE website. Go to the product's download page. Copy the compressed drivers file to your computer. Double-click the file to extract it. Run "CDGuide" to access the main drivers page.

Note: After installing your Windows 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

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

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

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

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

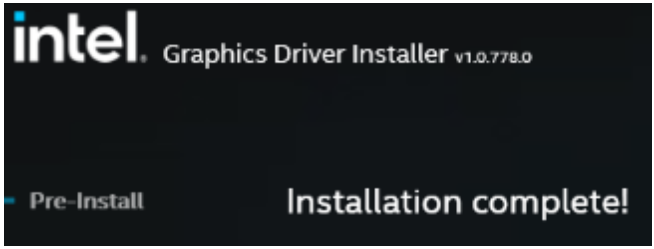
3.3 VGA Driver Installation

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

2. Click **Begin installation**.

3. Click **I agree** in the INTEL SOFTWARE LICENSE AGREEMENT screen.
4. Click **Start** to install the graphics driver.

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



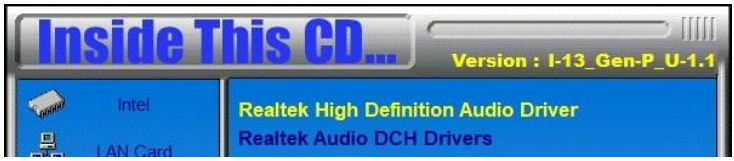
3.4 Intel(R) Smartsound Driver Installation

1. The **Intel(R) Smartsound Drivers** are applicable to Windows 10 only. Click **Intel** and then **Intel(R) Smartsound Drivers o**n the left pane and then **Intel(R) RaptorLake-P/PS/U Chipset Drivers** on the right pane. Click **Intel(R) HD Graphics Driver**.

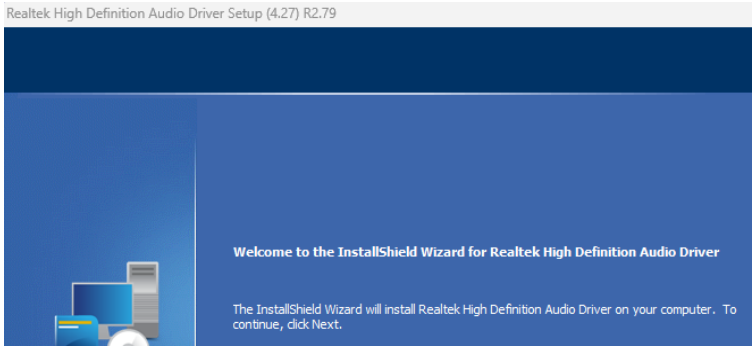
2. As shown in the image below, locate the executable file to proceed with the installation process.

3.5 HD Audio Driver Installation

1. Click **Intel** on the left pane and then **Intel(R) RaptorLake-P/PS/U Chipset Drivers** on the right.
2. Click **Realtek Audio Drivers**, then **Realtek High Definition Audio Drivers**.



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

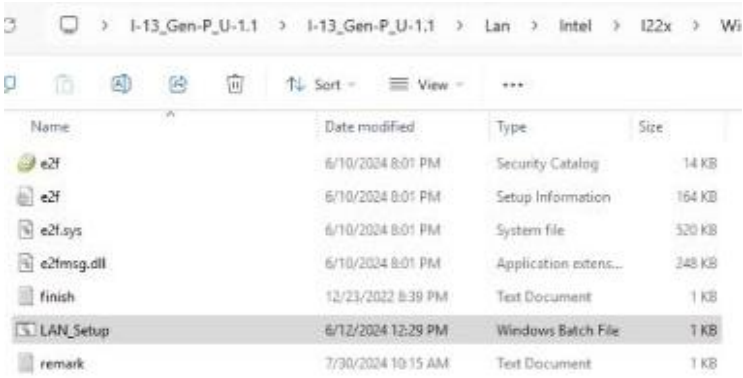


4. Click **Next** to continue the driver installation process.
5. After completing the installation, click **Finish** to restart the computer.

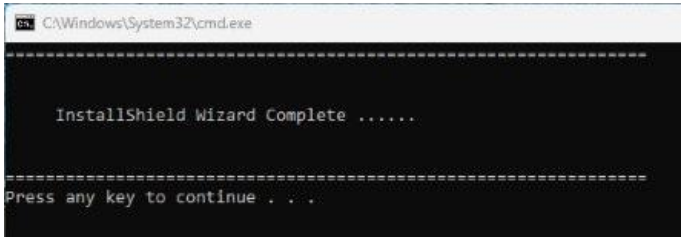
3.6 LAN Driver Installation

1. Click **Intel** on the left pane and then **Intel(R) RaptorLake-P/PS/U Chipset Drivers** on the right pane.
2. Click **Intel(R) PRO LAN Network Drivers**..

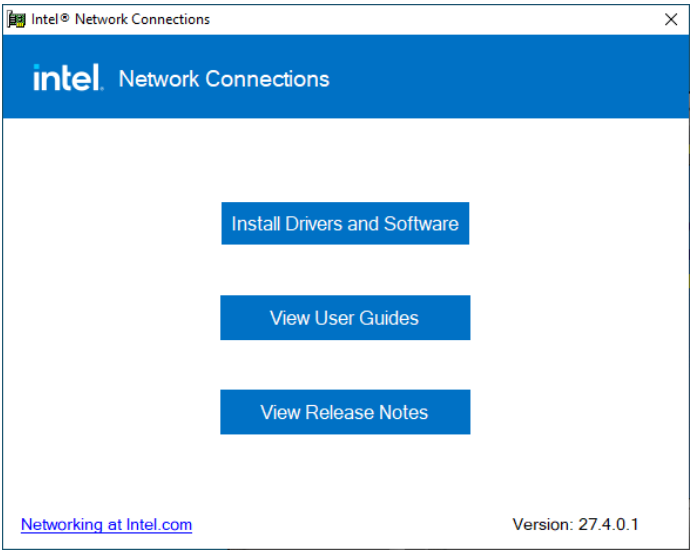
3. Follow the steps on the screen to run the necessary LAN_Setup file. **These steps apply for Windows 11. For Windows 10, the steps are discussed in 5 after the images for Windows 11.**



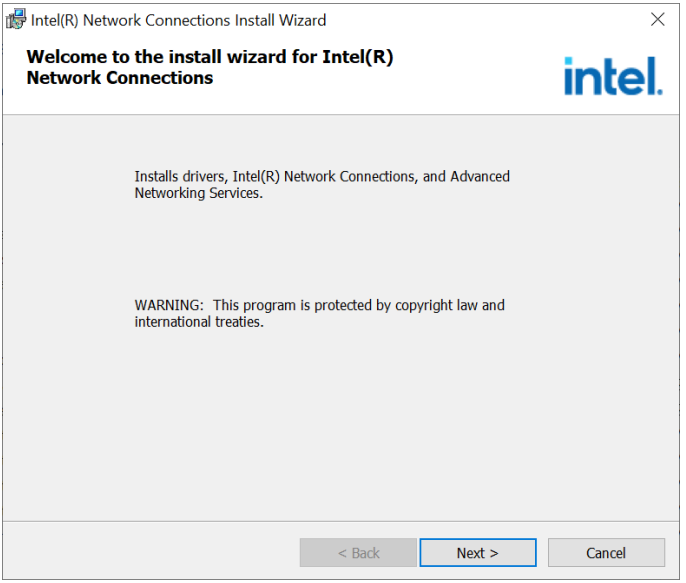
4. InstallShield Wizard has completed installation.



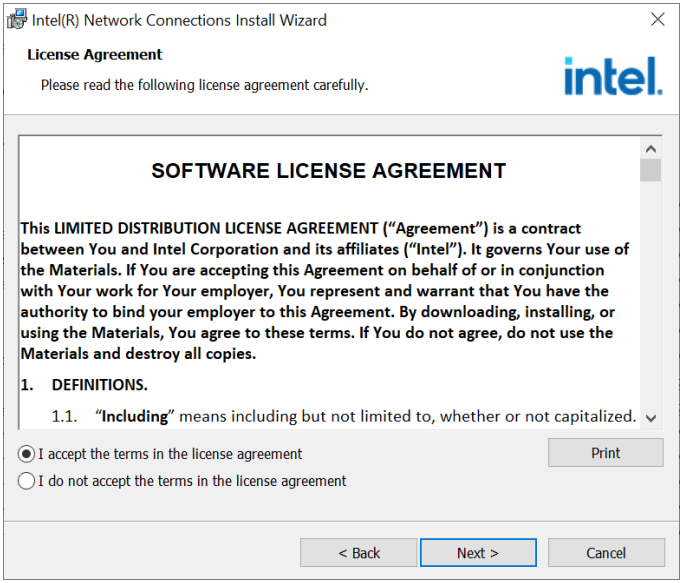
5. **The** following images applies to LAN installation under **Windows 10**. Click **Install Drivers and Software**.



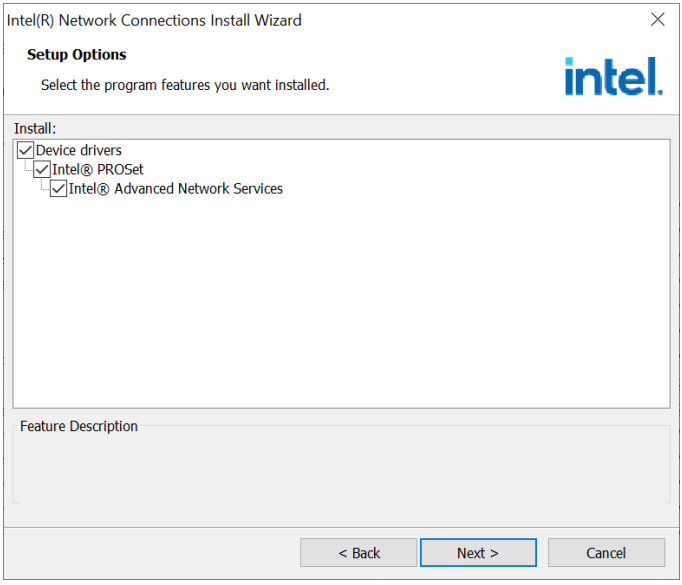
6. In the **Welcome** screen, click **Next**.



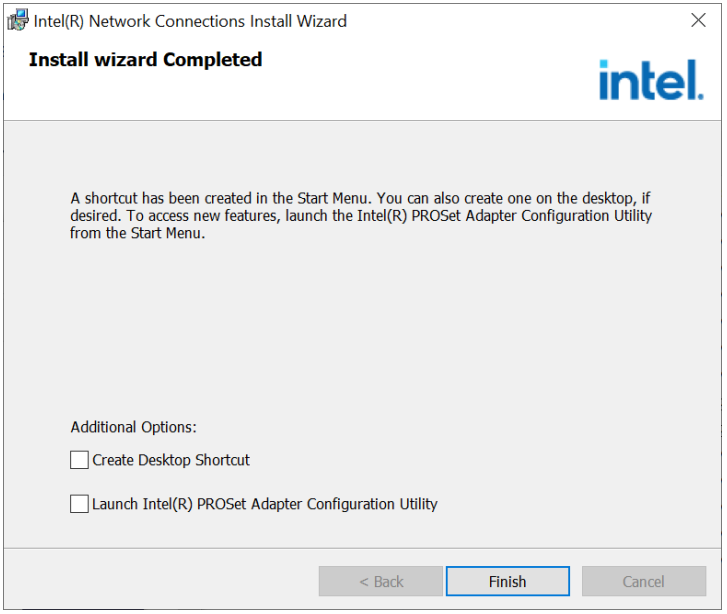
7. Accept the terms of the licence agreement.



8. In the **Setup Options** screen, click **Next**.



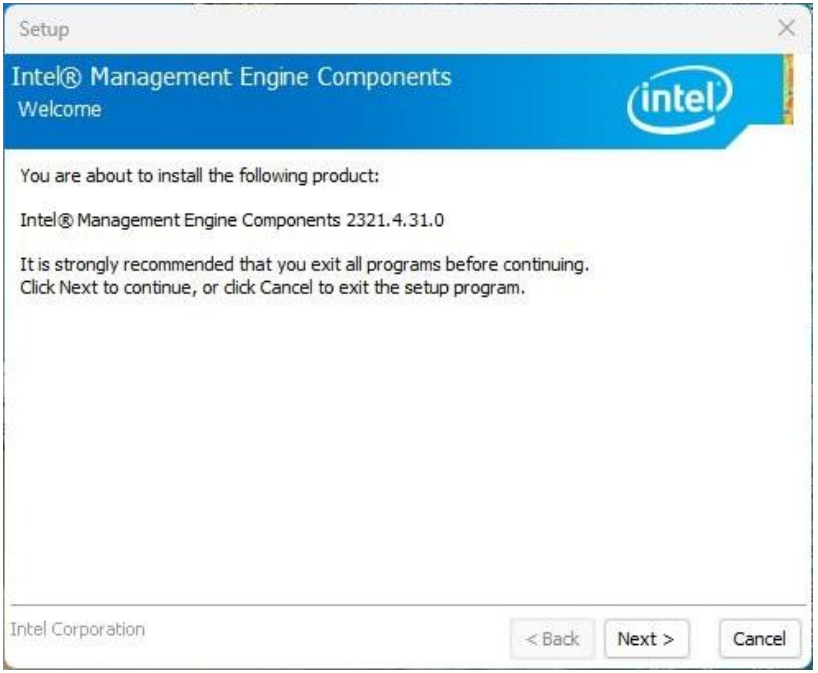
9. When **Install wizard** has completed installation, click **Finish**.



3.7 Intel® Management Engine Components Drivers Installation

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

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



4. Accept the terms in the license agreement and click **Next**.

5. In the Destination Folder, click **Next** to install to the default folder, or click **Change** to choose another destination folder.

6. After Intel Management Engine Components have been successfully installed, click **Finish**.

Chapter 4
BIOS Setup

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

- Main Settings
- Advanced Settings
- Chipset Settings
- Security Settings
- Boot Settings
- Save & Exit
- 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, serial ports and parallel ports. It also provides password protection as well as special support for detailed fine-tuning of the chipset controlling the entire system.

4.2 BIOS Setup

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

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

The following message will appear on the screen:

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

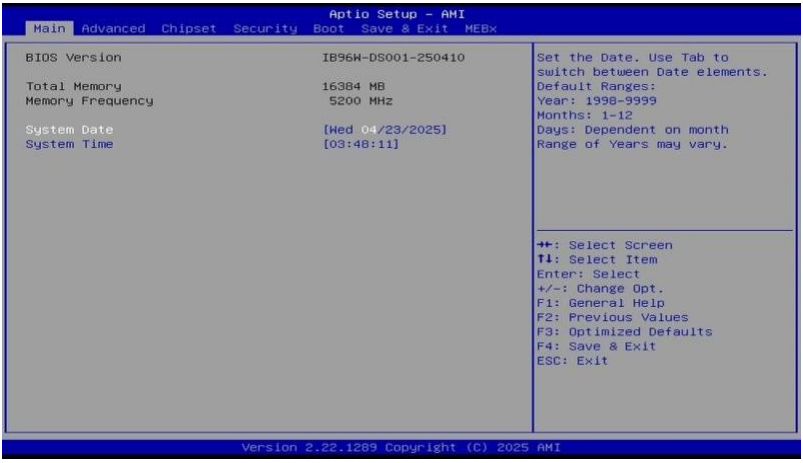
In general, press the arrow keys to highlight items, <Enter> to select, the <PgUp> and <PgDn> keys to change entries, <F1> for help, and <Esc> to quit.

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

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

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

4.3 Main Settings



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

4.4 Advanced Settings

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

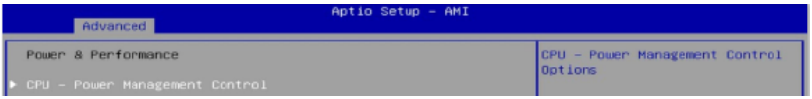
4.4.1 Connectivity Configuration

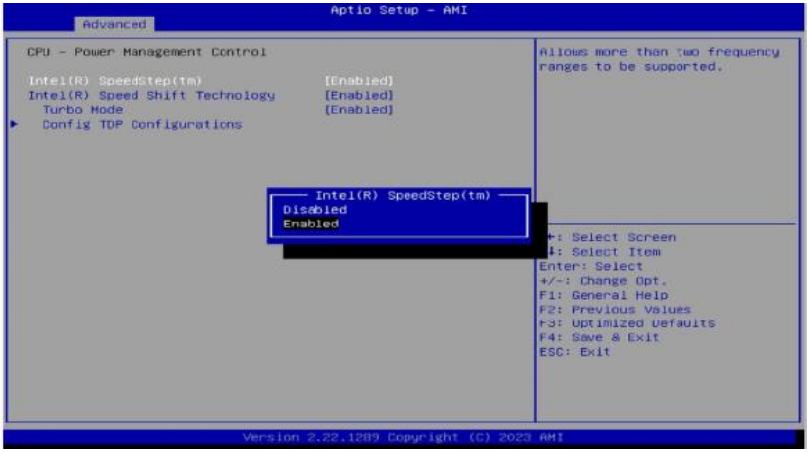
BIOS Setting	Description
CNVI Mode	This option configures Connectivity. ***Auto Detection*** – means that if Discrete solution is discovered it will be enabled by default. Otherwise Integrated solution (CNVi) will be enabled; ***Disable Integrated*** – disables Integrated Solution.
RFI Mitigation	This is an option intended to enable/disable DDR-RFIM feature for connecivity. This feature may result in temporary slowdown of the DR speed.
Preboot BLE	This will be used to enable Preboot Bluetooth function.
Discrete Bluetooth Module	Seiral IO UART0 needs to be enabled to select BT Module. Default: Disabled
BT Tile Mode	Enable/Disable Tile
Advanced Settings	Configure ACPI objects for wireless devices Default: Disabled
WWAN Configuration	Configure WWAN related options. WWAN Device: enable or disable M.2 WWAN device
WWAN Device	Select the M.2 WWAN device options to enable 4G-7360/7560 (Intel) 5G – M80 (MediaTek) modems.

4.4.2 CPU Configuration

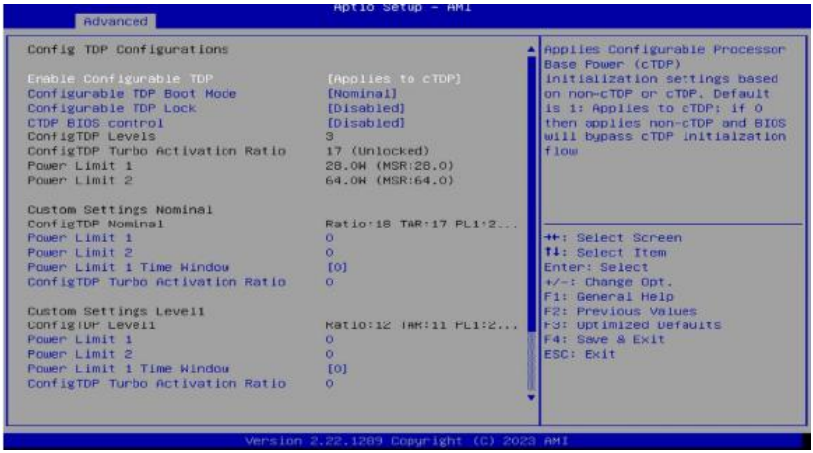
BIOS Setting	Description
Intel (VMX) Virtualization Technology	When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.
Active Performance Cores	Number of P-cores to enable in each processor package. Note: Number of cores and E-cores are looked at together.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

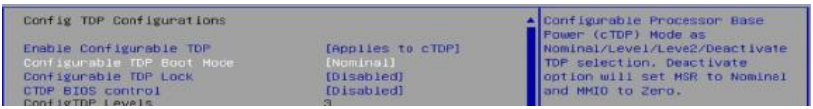
4.4.3 Power & Performance

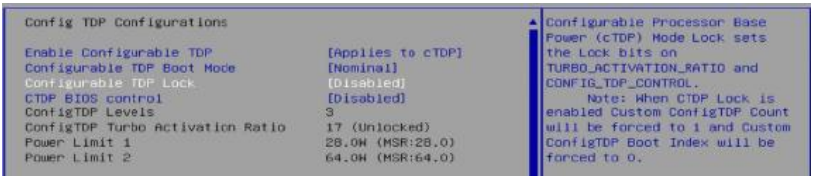


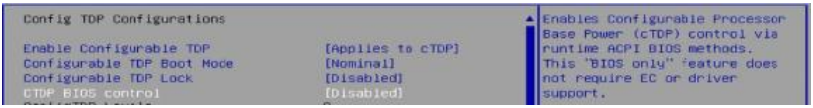


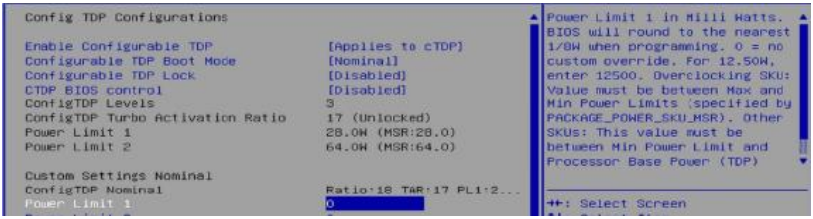
BIOS Setting	Description
Intel Speedstep	Allows more than two frequency ranges to be supported
Intel Speed Shift Technology	Enable/Disable Intel Speed Shift Technology support. Enabling will expose the CPPC v2 interface to allow for hardware controlled P-states.
Turbo Mode	Enable/disable processor turbo mode (requires EMTTM enabled too. AUTO means enabled.
Config TDP Configuration	Configurable processor base power (cTDP) configurations.

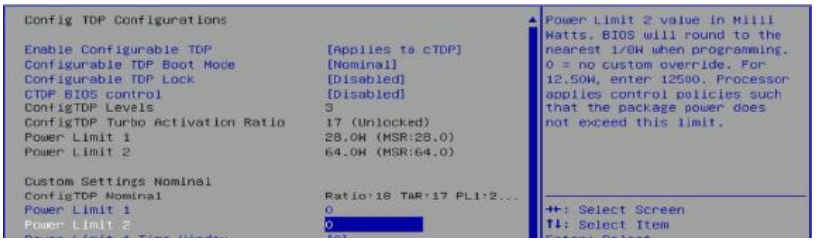

Aptio Setup – AMI
Advanced
Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
ConfigTDP Levels 3
ConfigTDP Turbo Activation Ratio 17 (Unlocked)
Power Limit 1 28.0W (MSR:28.0)
Power Limit 2 64.0W (MSR:64.0)
Custom Settings Nominal
ConfigTDP Nominal Ratio:18 TAR:17 PL1:2...
Power Limit 1 0
Power Limit 2 0
Power Limit 1 Time Window [0]
ConfigTDP Turbo Activation Ratio 0
Custom Settings Level1
ConfigTDP Level1 Ratio:12 TAR:11 PL1:2...
Power Limit 1 0
Power Limit 2 0
Power Limit 1 Time Window [0]
ConfigTDP Turbo Activation Ratio 0
Applies Configurable Processor Base Power (cTDP) initialization settings based on non-cTDP or cTDP. Default is 1: Applies to cTDP; if 0 then applies non-cTDP and BIOS will bypass cTDP initialzation flow
→←: 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) 2023 AMI

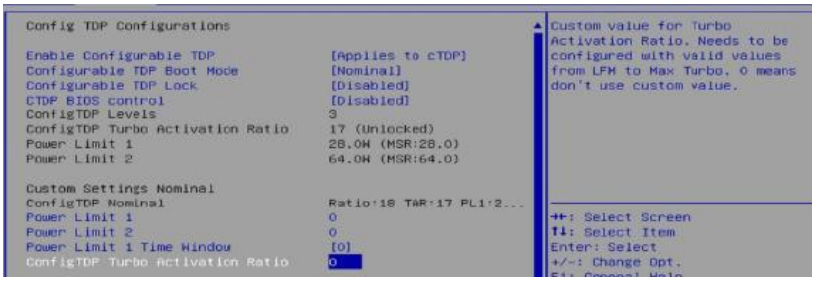

Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
Configurable Processor Base Power (cTDP) Mode as Nominal/Level1/Leve2/Deactivate TDP selection. Deactivate option will set MSR to Nominal and MMIO to Zero.

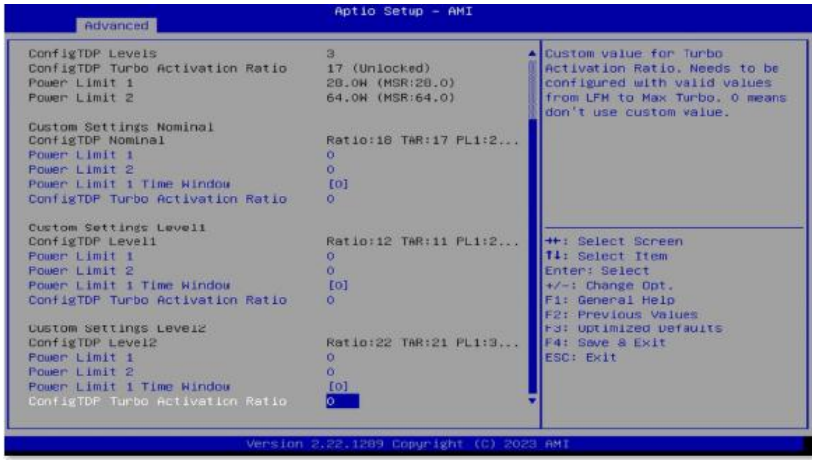

Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
ConfigTDP Levels 3
ConfigTDP Turbo Activation Ratio 17 (Unlocked)
Power Limit 1 28.0W (MSR:28.0)
Power Limit 2 64.0W (MSR:64.0)
Configurable Processor Base Power (cTDP) Mode Lock sets the Lock bits on TURBO_ACTIVATION_RATIO and CONFIG_TDP_CONTROL.
Note: When CTDP Lock is enabled Custom ConfigTDP Count will be forced to 1 and Custom ConfigTDP Boot Index will be forced to 0.


Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
Enables Configurable Processor Base Power (cTDP) control via runtime ACPI BIOS methods. This "BIOS only" feature does not require EC or driver support.

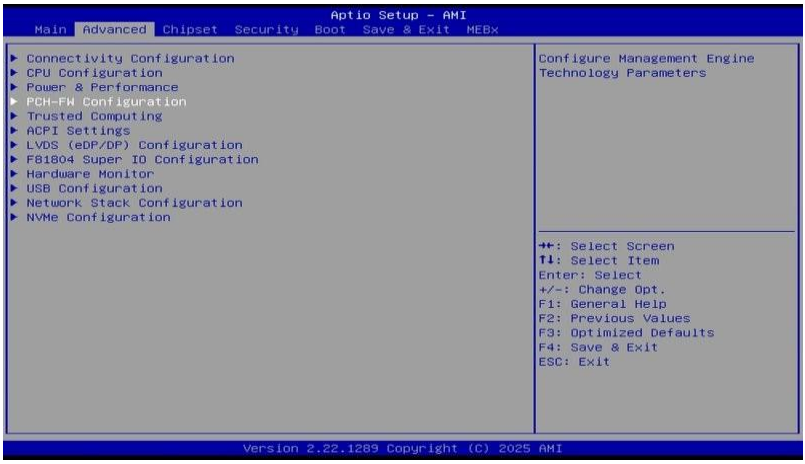

Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
ConfigTDP Levels 3
ConfigTDP Turbo Activation Ratio 17 (Unlocked)
Power Limit 1 28.0W (MSR:28.0)
Power Limit 2 64.0W (MSR:64.0)
Custom Settings Nominal
ConfigTDP Nominal Ratio:18 TAR:17 PL1:2...
Power Limit 1 0
Power Limit 1 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Overclocking SKU: Value must be between Max and Min Power Limits (specified by PACKAGE_POWER_SKU_MSR). Other SKUs: This value must be between Min Power Limit and Processor Base Power (TDP)
→←: Select Screen

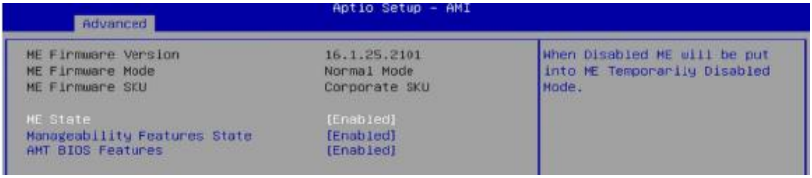

Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
ConfigTDP Levels 3
ConfigTDP Turbo Activation Ratio 17 (Unlocked)
Power Limit 1 28.0W (MSR:28.0)
Power Limit 2 64.0W (MSR:64.0)
Custom Settings Nominal
ConfigTDP Nominal Ratio:18 TAR:17 PL1:2...
Power Limit 1 0
Power Limit 2 0
Power Limit 2 in Milli Watts. BIOS will round to the nearest 1/8W when programming. 0 = no custom override. For 12.50W, enter 12500. Processor applies control policies such that the package power does not exceed this limit.
++: Select Screen
↑↓: Select Item

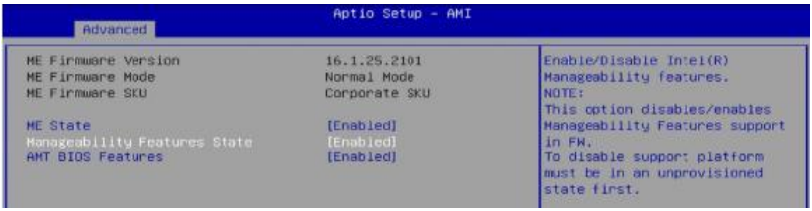

Config TDP Configurations
Enable Configurable TDP [Applies to cTDP]
Configurable TDP Boot Mode [Nominal]
Configurable TDP Lock [Disabled]
CTDP BIOS control [Disabled]
ConfigTDP Levels 3
ConfigTDP Turbo Activation Ratio 17 (Unlocked)
Power Limit 1 28.0W (MSR:28.0)
Power Limit 2 64.0W (MSR:64.0)
Custom Settings Nominal
ConfigTDP Nominal Ratio:18 TAR:17 PL1:2...
Power Limit 1 0
Power Limit 2 0
Power Limit 1 Time Window [0]
ConfigTDP Turbo Activation Ratio 0
Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.
++: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.

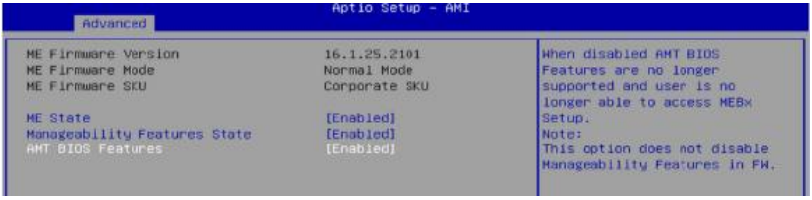

Aptio Setup – AMI
Advanced
ConfigTDP Levels 3
ConfigTDP Turbo Activation Ratio 17 (Unlocked)
Power Limit 1 28.0W (MSR:28.0)
Power Limit 2 64.0W (MSR:64.0)
Custom Settings Nominal
ConfigTDP Nominal Ratio:18 TAR:17 PL1:2...
Power Limit 1 0
Power Limit 2 0
Power Limit 1 Time Window [0]
ConfigTDP Turbo Activation Ratio 0
Custom Settings Level1
ConfigTDP Level1 Ratio:12 TAR:11 PL1:2...
Power Limit 1 0
Power Limit 2 0
Power Limit 1 Time Window [0]
ConfigTDP Turbo Activation Ratio 0
Custom Settings Level2
ConfigTDP Level2 Ratio:22 TAR:21 PL1:3...
Power Limit 1 0
Power Limit 2 0
Power Limit 1 Time Window [0]
ConfigTDP Turbo Activation Ratio 0
Custom value for Turbo Activation Ratio. Needs to be configured with valid values from LFM to Max Turbo. 0 means don't use custom value.
++: 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) 2023 AMI

4.4.4 PCH-FW Configuration





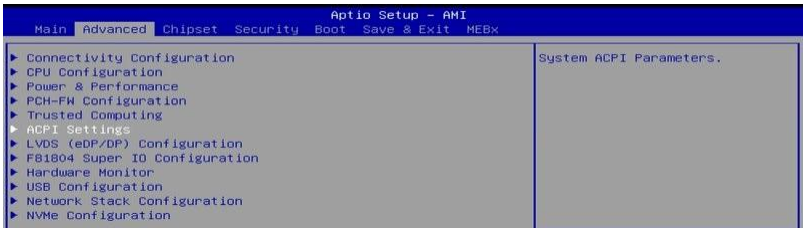




4.4.5 Trusted Computing

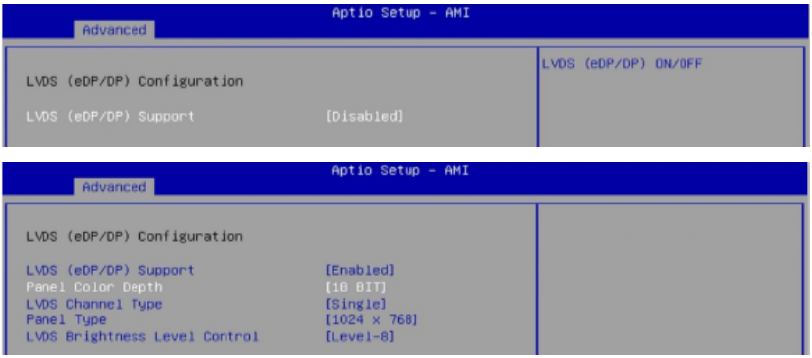
BIOS Setting	Description
Security Device Support	Enables / Disables BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.
SHA256/384, SM3_256 PCR Bank	Enables / Disables PCR Bank.
Pending operation	Schedule an operation for the 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.

4.4.6 ACPI Settings



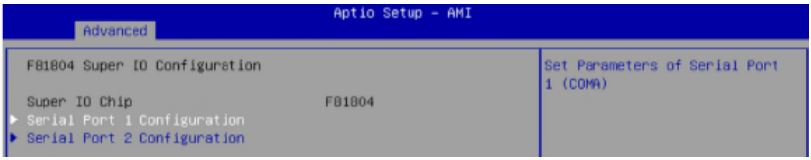
BIOS Setting	Description
Enable Hibernation	Enables / Disables the system ability to hibernate (OS/S4 Sleep State). This option may be not effective with some OS.
ACPI Sleep State	Select the highest ACPI sleep state the system will enter when SUSPEND button is pressed.

4.4.7 LVDS (eDP/DP) Configuration



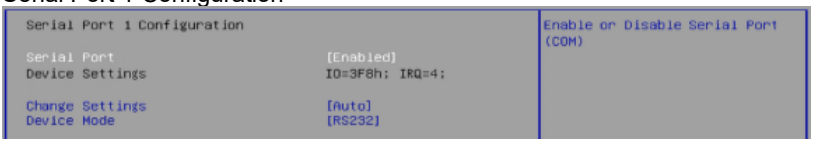
BIOS Setting	Description
LVDS (eDP/DP) Support	*LVDS (eDP/DP) ON/OFF*
Panel Color Depth	Selects the panel color depth. Options: 18 bit, 24bit (VESA/JEIDA)
LVDS Channel Type	Chooses the LVDS as single or dual channel.
Panel Type	Panel Type (Resolution) Options: 800 x 480, 800 x 600, 1024 x 768, 1280 x 768, 1280 x 800, 1280 x 960, 1280 x 1024, 1366 x 768, 1440 x 900, 1600 x 900, 1600 x 1200, 1680 x 1050, 1920 x 1080, 1920 x 1200
LVDS Brightness Level Control	Options: Level-1 to Level-8

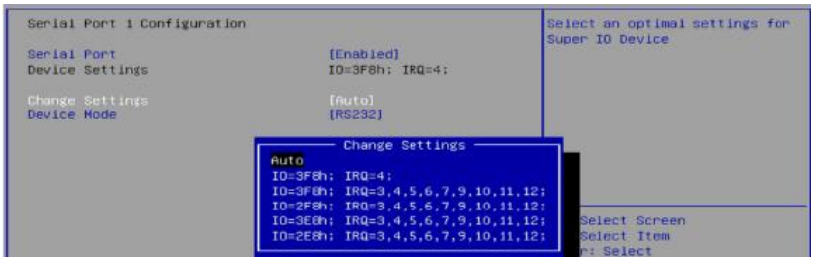
4.4.8 F81804 Super IO Configuration



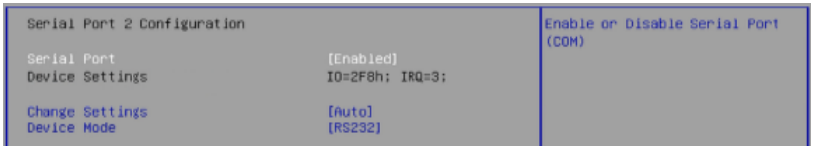
BIOS Setting	Description
Serial Ports Configuration	Sets parameters of serial ports. Enables / Disables the serial port and select an optimal setting for the Super IO device.

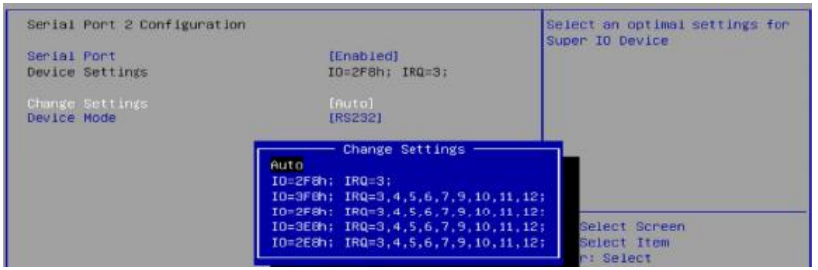
Serial Port 1 Configuration



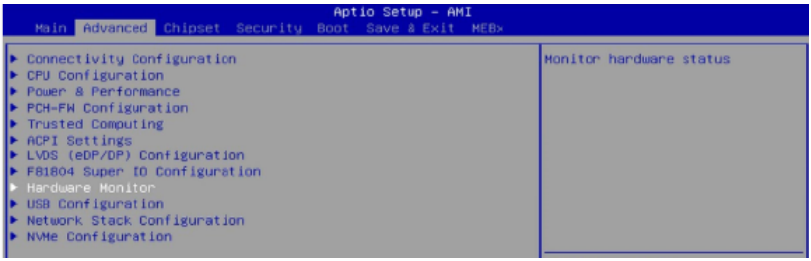


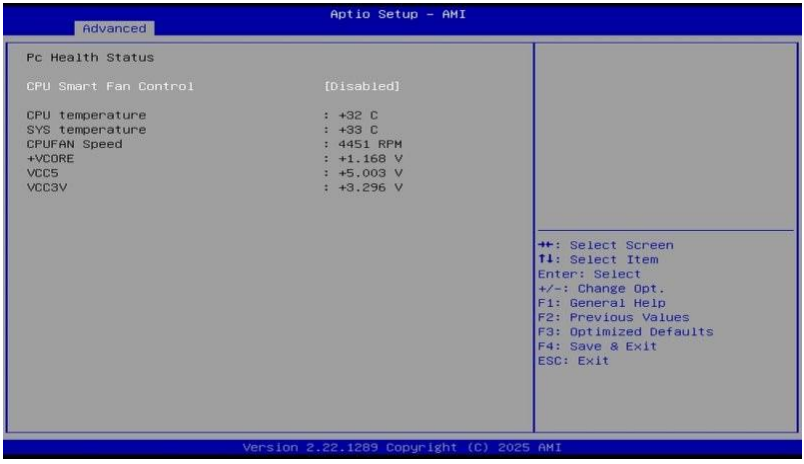
Serial Port 2 Configuration





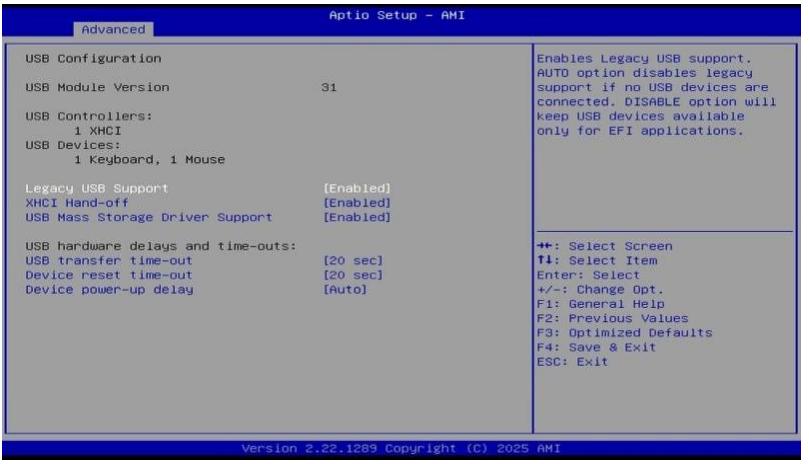
4.4.9 Hardware Monitor





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



BIOS Setting	Description
Legacy USB Support	• **Enabled** enables Legacy USB support. • **Auto** disables legacy support if there is no USB device connected. • **Disabled** keeps USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enables / Disables the support for USB mass storage driver.
USB Transfer time-out	The time-out value (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.

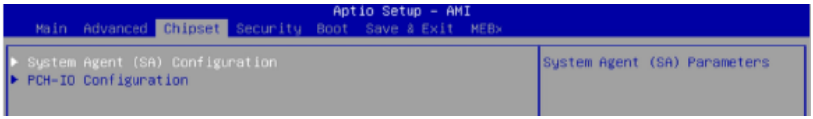
4.4.11 Network Stack Configuration

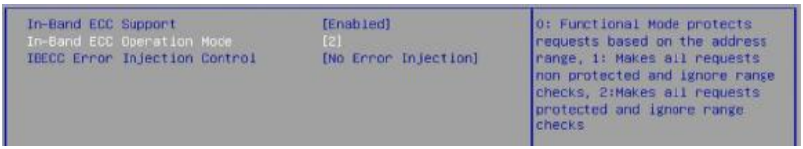
BIOS Setting	Description
Network Stack	Enable/Disable UEFI Network Stack
IPv4 PXE Support	If disabled, IPv4 PXE boot support will not be available.
IPv4 HTTP Support	If disabled, IPv4 HTTP boot support will not be available.
Ipv6 PXE Support	If disabled, IPv6 PXE boot support will not be available.
Ipv6 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 +/- nurmeric keys to set the value.

4.4.12 NVMe Configuration

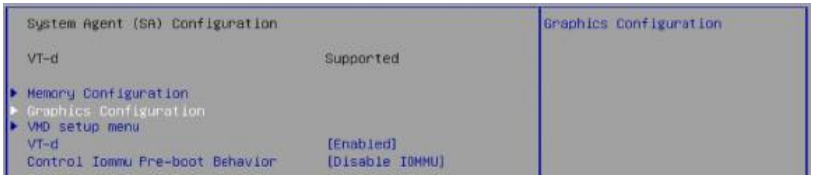
4.5 Chipset Settings

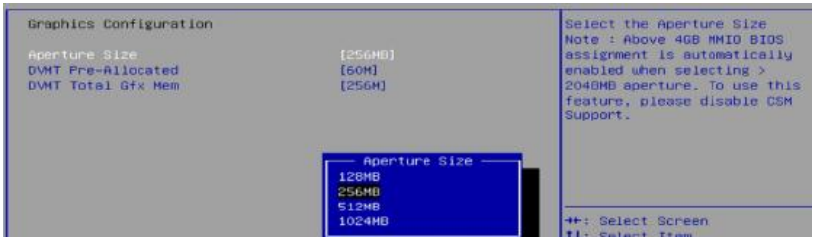
4.5.1 System Agent (SA) Configuration

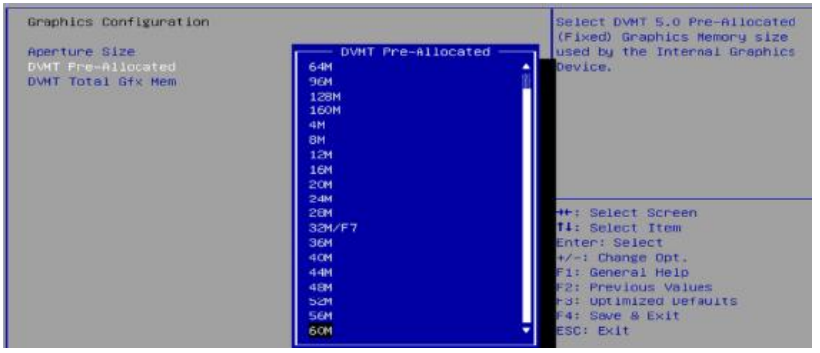




4.5.1.1. Graphics Configuration and VMD Setup



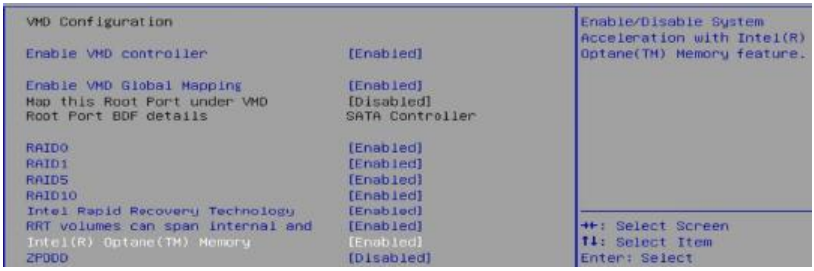




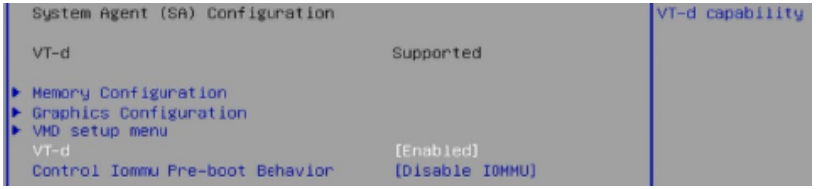

VMD Configuration
Enable VMD controller [Disabled]
Enable/Disable to VMD controller


VMD Configuration
Enable VMD controller [Enabled]
Enable VMD Global Mapping [Enabled]
Map this Root Port under VMD [Disabled]
Root Port BDF details SATA Control
RAID0 [Enabled]
RAID1 [Enabled]
RAID5 [Enabled]
RAID10 [Enabled]
Intel Rapid Recovery Technology [Enabled]
RRT volumes can span internal and [Enabled]
Intel(R) Optane(TM) Memory [Enabled]
ZPODD [Disabled]

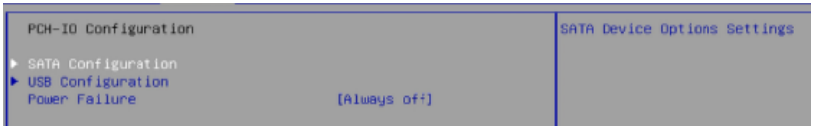

VMD Configuration
Enable VMD controller [Enabled]
Enable VMD Global Mapping [Enabled]
Map this Root Port under VMD [Disabled]
Root Port BDF details SATA Controller
RAID0 [Enabled]
RAID1 [Enabled]
RAID5 [Enabled]
RAID10 [Enabled]
Intel Rapid Recovery Technology [Enabled]
RRT volumes can span internal and [Enabled]
Intel(R) Optane(TM) Memory [Enabled]
ZPODD [Disabled]
Enable/Disable RRT volumes can span internal and eSATA drives.
→←: Select Screen
↑↓: Select Item
Enter: Select


VMD Configuration
Enable VMD controller [Enabled]
Enable VMD Global Mapping [Enabled]
Map this Root Port under VMD [Disabled]
Root Port BDF details SATA Controller
RAID0 [Enabled]
RAID1 [Enabled]
RAID5 [Enabled]
RAID10 [Enabled]
Intel Rapid Recovery Technology [Enabled]
RRT volumes can span internal and [Enabled]
Intel(R) Optane(TM) Memory [Enabled]
ZPODD [Disabled]
Enable/Disable System Acceleration with Intel(R) Optane(TM) Memory feature.
→←: Select Screen
↑↓: Select Item
Enter: Select

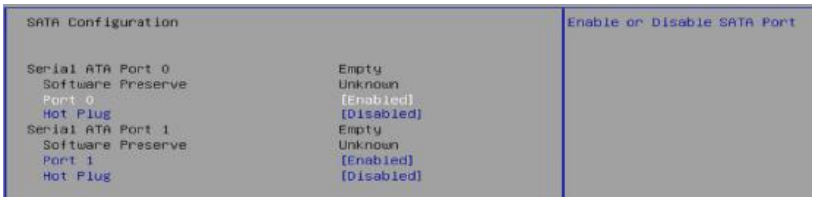

VMD Configuration
Enable VMD controller [Enabled]
Enable VMD Global Mapping [Enabled]
Map this Root Port under VMD [Disabled]
Root Port BDF details SATA Controller
RAID0 [Enabled]
RAID1 [Enabled]
RAID5 [Enabled]
RAID10 [Enabled]
Intel Rapid Recovery Technology [Enabled]
RRT volumes can span internal and [Enabled]
Intel(R) Optane(TM) Memory [Enabled]
ZPODD [Disabled]
Enable/Disable ZPODD. The option is only needed to be enabled when ZPODD is connected in VMD mode
→←: Select Screen
↑↓: Select Item
Enter: Select



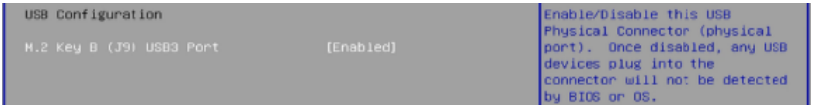
4.5.2 PCH-IO Configuration



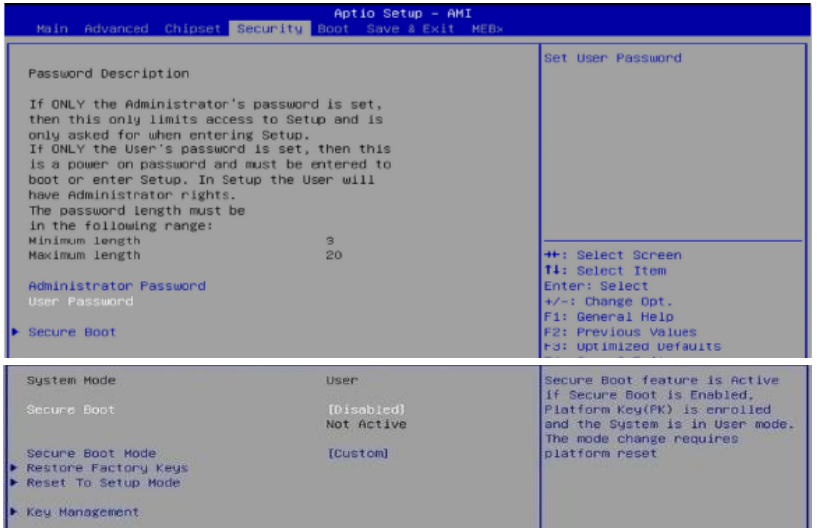
4.5.2.1 SATA and RST Configuration:



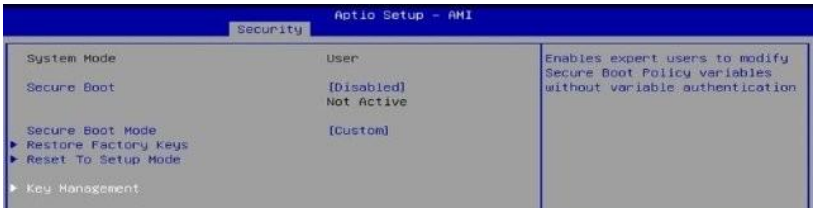
BIOS Setting	Description
SATA and RST Configuration	SATA device options and settings
SATA Controller(s)	Enables / Disables the Serial ATA.
USB Configuration	USB Configuration Settings
M.2 Key B (J9) USB3 Port	Enable/Disable this USB physical connector. Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.
Power-On after Power failure	Specify what state to go to when power is re-applied after a power failure (G3 state).

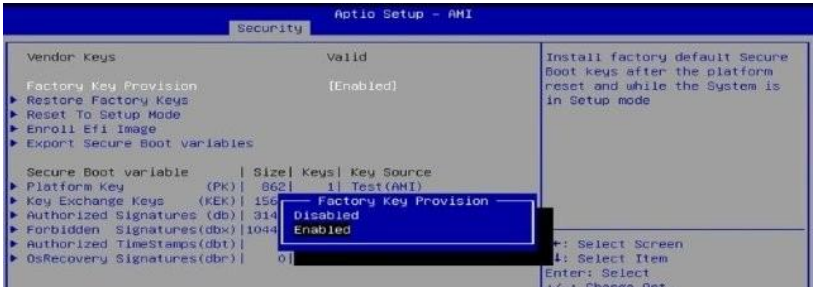


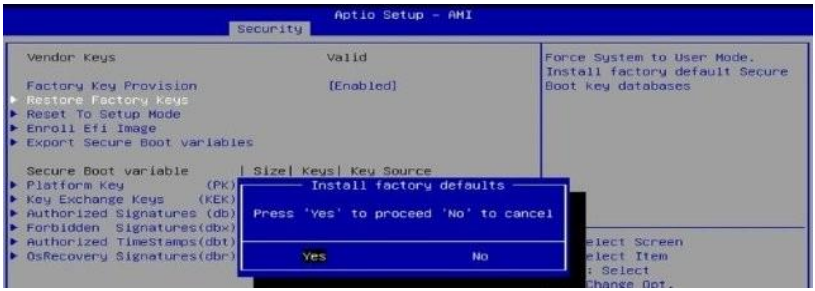
4.6 Security Settings



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


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


Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Size
Keys
Key Source
Platform Key (PK)
862
1
Test(AMI)
Key Exchange Keys (KEK)
156
Authorized Signatures (db)
314
Forbidden Signatures(dbx)
1044
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
0
Factory Key Provision
Disabled
Enabled
Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode
Select Screen
Select Item
Enter: Select

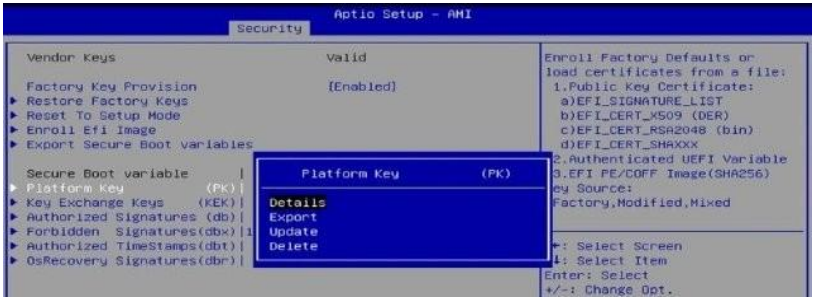

Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Size
Keys
Key Source
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
Install factory defaults
Press 'Yes' to proceed 'No' to cancel
Yes
No
Force System to User Mode. Install factory default Secure Boot key databases
Select Screen
Select Item
Select


Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
Reset To Setup Mode
Deleting all variables will reset the System to Setup Mode
Do you want to proceed?
Yes
No
Delete all Secure Boot key databases from NVRAM
Select Screen
Select Item
Select
Change Opt.
General Help
F2: Previous Values


Aptio Setup - AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Size
Keys
Key Source
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
File System
No Valid File System Available
Ok
Allow Efi image to run in Secure Boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db)
: Select Screen
: Select Item
ter: Select
-: Change Opt.
F1: General Help


Aptio Setup - AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Size
Keys
Key Source
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
File System
No Valid File System Available
Ok
Save NVRAM content of Secure Boot variable to a file
: Select Screen
: Select Item
ter: Select
-: Change Opt.

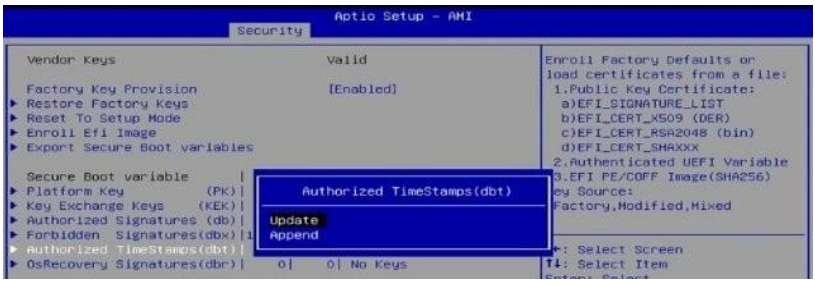

Aptio Setup - AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Size
Keys
Key Source
Platform Key (PK) 862 1 Test(AMI)
Key Exchange Keys (KEK) 1560 1 Factory
Authorized Signatures (db) 3143 2 Factory
Forbidden Signatures(dbx) 10444 217 Factory
Authorized TimeStamps(dbt) 0 0 No Keys
OsRecovery Signatures(dbr) 0 0 No Keys
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,Modified,Mixed
↔: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help

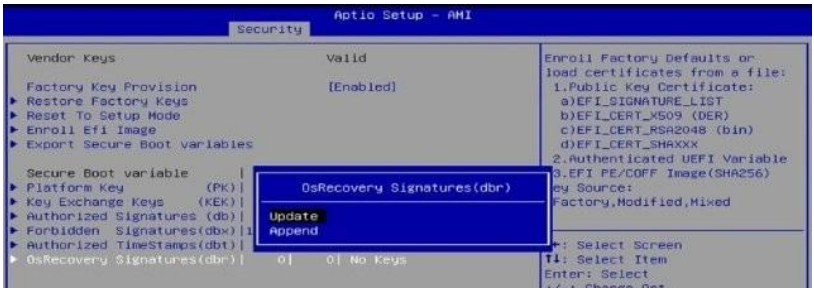

Aptio Setup - AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
Platform Key (PK)
Details
Export
Update
Delete
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Factory,Modified,Mixed
Enter: Select
+/-: Change Opt.


Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
Key Exchange Keys (KEK)
Details
Export
Update
Append
Delete
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,Modified,Mixed
: Select Screen
: Select Item
Enter: Select

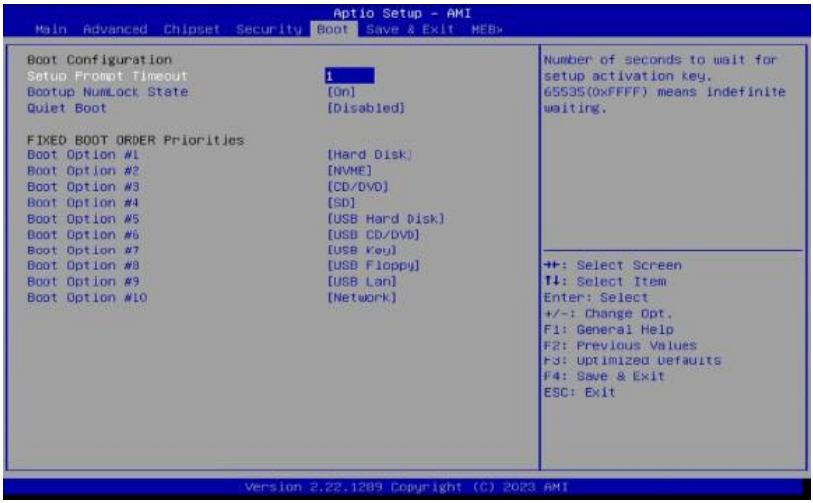

Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
Authorized Signatures (db)
Details
Export
Update
Append
Delete
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,Modified,Mixed
: Select Screen
: Select Item
Enter: Select
+/-: Change Opt.


Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
Forbidden Signatures(dbx)
Details
Export
Update
Append
Delete
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,Modified,Mixed
: Select Screen
: Select Item
Enter: Select


Aptio Setup – AMI
Security
Vendor Keys
Valid
Factory Key Provision
[Enabled]
Restore Factory Keys
Reset To Setup Mode
Enroll Efi Image
Export Secure Boot variables
Secure Boot variable
Platform Key (PK)
Key Exchange Keys (KEK)
Authorized Signatures (db)
Forbidden Signatures(dbx)
Authorized TimeStamps(dbt)
OsRecovery Signatures(dbr)
0
0 No Keys
Authorized TimeStamps(dbt)
Update
Append
Enroll Factory Defaults or load certificates from a file:
1.Public Key Certificate:
a)EFI_SIGNATURE_LIST
b)EFI_CERT_X509 (DER)
c)EFI_CERT_RSA2048 (bin)
d)EFI_CERT_SHAXXX
2.Authenticated UEFI Variable
3.EFI PE/COFF Image(SHA256)
Key Source:
Factory,Modified,Mixed
: Select Screen
: Select Item



4.7 Boot Settings



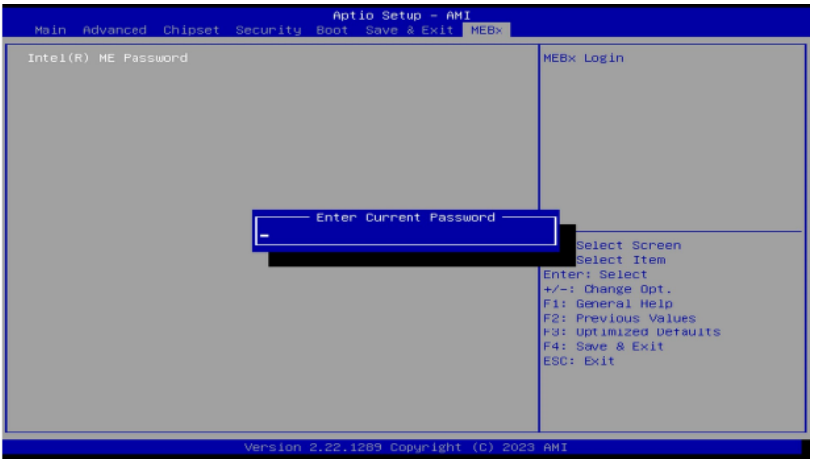
BIOS Setting	Description
Setup Prompt Timeout	Number of seconds to wait for setup activation key. 65535 (0xFFFF) means indefinite waiting.
Bootup NumLock State	Selects the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
FIXED BOOT ORDER Priorities	Sets the system boot order.

4.8 Save & Exit Settings

BIOS Setting	Description
Save Changes and Exit	Exits system setup after saving the changes.
Discard Changes and Exit	Exits system setup without saving any changes.
Save Changes and Reset	Resets the system after saving the changes.
Discard Changes and Reset	Resets system setup without saving any changes.
Save Changes	Saves changes done so far to any of the setup options.
Discard Changes	Discards changes done so far to any of the setup options.
Restore Defaults	Restores / Loads defaults values for all the setup options.
Save as User Defaults	Saves the changes done so far as User Defaults.
Restore User Defaults	Restores the user defaults to all the setup options.
Launch EFI Shell from filesystem device	Attempts to launch EFI shell application (Shell.efi) from one of the available filesystem devices.

4.9 MEBx


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) 2023 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) 2023 AMI

Appendix

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

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
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
0x0000FFF8-0x0000FFFF	Intel(R) Active Management Technology - SOL (COM3)
0x000003F8-0x000003FF	Communications Port (COM1)
0x000002F8-0x000002FF	Communications Port (COM2)
0x00001854-0x00001857	Motherboard resources

0x00000000-0x00000CF7	PCI Express Root Complex
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x0000EFA0-0x0000EFBF	Intel(R) SMBus - 51A3
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer
0x00002000-0x000020FE	Motherboard resources
0x00003090-0x00003097	Standard SATA AHCI Controller
0x00003080-0x00003083	Standard SATA AHCI Controller
0x00003060-0x0000307F	Standard SATA AHCI Controller
0x00003000-0x0000303F	Intel(R) UHD Graphics

B. Interrupt Request Lines (IRQ)

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

Level	Function
IRQ 0	System timer
IRQ 16	High Definition Audio Controller
IRQ 19	Intel(R) Active Management Technology - SOL (COM3)
IRQ 4294967294	Intel(R) PCI Express Root Port #7 - 51BE
IRQ 4294967259	Intel(R) Management Engine Interface #1
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 55-204	Microsoft ACPI-Compliant System
IRQ 256-511	Microsoft ACPI-Compliant System
IRQ 4294967275-89	Intel(R) Ethernet Controller I226-IT
IRQ 4294967260-74	Intel(R) Ethernet Controller I226-IT #2
IRQ 4294967292	Standard SATA AHCI Controller
IRQ 4294967290	Intel(R) UHD Graphics
IRQ 4294967291	Intel(R) USB 3.10 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967293	Intel(R) PCI Express Root Port #8 - 51BF

C. Watchdog Timer Configuration

The Watchdog Timer (WDT) is used to generate a variety of output signals after a user programmable count. The WDT is suitable for use in the prevention of system lock-up, such as when software becomes trapped in a deadlock. Under these sorts of circumstances, the timer will count to zero and the selected outputs will be driven.

Under normal circumstance, you will need to restart the WDT at regular intervals before the timer counts to zero.

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 " F81804.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 81866 watch dog program\n");
                SIO = Init_ F81804();
                if (SIO == 0)
                {
                                printf("Can not detect Fintek 81866, 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_ F81804_Reg(0x2B);
        bBuf &= (~0x20);
        Set_ F81804_Reg(0x2B,   bBuf);          //Enable WDTO

        Set_ F81804_LD(0x07);                   //switch to logic device  7
        Set_ F81804_Reg(0x30,   0x01);          //enable timer

        bBuf = Get_ F81804_Reg(0xF5);
        bBuf &= (~0x0F);
        bBuf |= 0x52;
        Set_ F81804_Reg(0xF5,   bBuf);          //count mode is second

        Set_ F81804_Reg(0xF6,   interval);      //set timer

        bBuf = Get_ F81804_Reg(0xFA);
        bBuf |= 0x01;
        Set_ F81804_Reg(0xFA,   bBuf);          //enable WDTO output

        bBuf = Get_ F81804_Reg(0xF5);
        bBuf |= 0x20;
        Set_ F81804_Reg(0xF5,   bBuf);          //start counting
}
//-----------------------------------------------------------------------------
void DisableWDT(void)
{
        unsigned char bBuf;

        Set_ F81804_LD(0x07);                   //switch to logic device 7

        bBuf = Get_ F81804_Reg(0xFA);
        bBuf &= ~0x01;
        Set_ F81804_Reg(0xFA,   bBuf);          //disable WDTO output

        bBuf = Get_ F81804_Reg(0xF5);
        bBuf &= ~0x20;
        bBuf |= 0x40;
        Set_ F81804_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 " F81804.H"
#include <dos.h>
//---------------------------------------------------------------------------
unsigned int F81804_BASE;
void Unlock_ F81804 (void);
void Lock_ F81804 (void);
//---------------------------------------------------------------------------
unsigned int Init_ F81804(void)
{
        unsigned int result;
        unsigned char ucDid;

         F81804_BASE = 0x4E;
        result = F81804_BASE;

        ucDid = Get_ F81804_Reg(0x20);
        if (ucDid == 0x07)                      //Fintek 81866
        {       goto Init_Finish;               }

         F81804_BASE = 0x2E;
        result = F81804_BASE;

        ucDid = Get_ F81804_Reg(0x20);
        if (ucDid == 0x07)                      //Fintek 81866
        {       goto Init_Finish;               }

         F81804_BASE = 0x00;
        result = F81804_BASE;

Init_Finish:
        return (result);
}
//---------------------------------------------------------------------------
void Unlock_ F81804 (void)
{
        outportb( F81804_INDEX_PORT, F81804_UNLOCK);
        outportb( F81804_INDEX_PORT, F81804_UNLOCK);
}
//---------------------------------------------------------------------------
void Lock_ F81804 (void)
{
        outportb( F81804_INDEX_PORT, F81804_LOCK);
}
//---------------------------------------------------------------------------
void Set_ F81804_LD( unsigned char LD)
{
        Unlock_ F81804();
        outportb( F81804_INDEX_PORT, F81804_REG_LD);
        outportb( F81804_DATA_PORT, LD);
        Lock_ F81804();
}
```

```
//---------------------------------------------------------------------------
void Set_ F81804_Reg( unsigned char REG, unsigned char DATA)
{
                Unlock_ F81804();
                outportb( F81804_INDEX_PORT, REG);
                outportb( F81804_DATA_PORT, DATA);
                Lock_ F81804();
}
//---------------------------------------------------------------------------
unsigned char Get_ F81804_Reg(unsigned char REG)
{
                unsigned char Result;
                Unlock_ F81804();
                outportb( F81804_INDEX_PORT, REG);
                Result = inportb( F81804_DATA_PORT);
                Lock_ F81804();
                return Result;
}
//---------------------------------------------------------------------------
```

```
//---------------------------------------------------------------------------
//
// 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.
//
//---------------------------------------------------------------------------
#ifndef    F81804_H
#define    F81804_H                         1
//---------------------------------------------------------------------------
#define          F81804_INDEX_PORT       ( F81804_BASE)
#define          F81804_DATA_PORT        ( F81804_BASE+1)
//---------------------------------------------------------------------------
#define          F81804_REG_LD           0x07
//---------------------------------------------------------------------------
#define          F81804_UNLOCK           0x87
#define          F81804_LOCK             0xAA
//---------------------------------------------------------------------------
unsigned int Init_ F81804(void);
void Set_ F81804_LD( unsigned char);
void Set_ F81804_Reg( unsigned char,
unsigned char); unsigned char
Get_ F81804_Reg( unsigned char);
//---------------------------------------------------------------------------
#endif  //    F81804_H
```

D. Onboard Connector Reference Types

Function	Connector	Onboard Type	Compatible Mating Type
Audio	J2	Hao Guo Xing Ye DF11-12S-PA66H	Hirose DF11-12DS-2C
SATA HDD Power	J13	E-CALL 0110-071-040	JST XHP-4
Front Panel Setting	J16	E-CALL 2.5 mm-pitch pin header (Male)	Dupont 2.5mm-pitch (Female)
USB 2.0	J14	Hao Guo Xing Ye DF11-8S-PA66H	Hirose DF11-8DS-2C
COM2 Serial Port	J7, J17	Hao Guo Xing Ye DF11-10S-PA66H	Hirose DF11-10DS-2C
DC Power Input	J15	Hao Guo Xing Ye WAFER396-2S-WV	JST VHR-2N
Digital I/O	J6	Dupont 2.00 mm-pitch pin header (Male)	Dupont 2.00 mm-pitch (Female)
LCD Backlight	J11	E-CALL 0110-161-040	JST PHR-4.
LVDS	J4, J8	Hirose DF20G-20DP-1V	Hirose DF20A-20DS-1C

E. USB Power Control Mapping

PDPC (Peripheral Device Power Control) allows users to turn off the external power and restart it via software, enabling the external device to recover and ensuring the system remains operational. Here are the bit-mapping for software SDK.

Function	Connector	Software Mapping
USB 3.1	CN6 (A, B)	Bit_0