AES100

Advanced Expandable Edge AI Computer With 350W NVIDIA® RTX™ GPU Card

User Manual

Version 1.0
January 2026

Copyright

Disclaimer

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

Trademarks

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

Compliance

CE

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

FC

This product has been tested and found to comply with the limits for a **Class 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 and prohibits use of the following substances in concentrations exceeding 0.1% by weight (1000 ppm) except for cadmium, limited to 0.01% by weight (100 ppm).

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

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 power and signal cables to prevent electrical hazards.
- Use neutral cleaning agents or diluted alcohol to clean the device chassis with a cloth. Then wipe the chassis with a dry cloth.
- Vacuum the dust with a computer vacuum cleaner to prevent the air vent or slots from being clogged.

WARNING

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

Avoid Disassembly

Users are not advised to disassemble, repair, or 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.

CAUTION

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

Warranty Policy

- **IBASE standard products:**

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

- **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, prepare the following information:
   - Product model name
   - Product serial number
   - Detailed description of the problem
   - The error messages in text or in screenshots if there is any
   - The arrangement of the peripherals
   - Software in use (such as OS and application software, including the version numbers)
3. If repair service is required, you can download the RMA form at the website of IBASE. Fill out the form and contact your distributor or sales representative.

iBASE

Table of Contents

Chapter 1
General Information

The information provided in this chapter includes:

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

1.1 Introduction

AES100 is an advanced expandable Edge AI computer based on 14th/13th Gen Intel® Core™ desktop processors (65W/35W) and supports a single 350W NVIDIA® RTX™ GPU (configuration dependent). It provides rich connectivity including 3x 2.5GbE, 6x USB 3.2, triple-display options (DP++ / HDMI 2.0 / optional VGA), built-in 8-in & 8-out isolated DIO, and flexible storage expansion with 2x removable 2.5” drive bays (RAID 0/1) plus an optional front-accessible M.2 NVMe tray. It also supports TPM 2.0 and Intel iAMT (16.1), and uses 8V–48V DC input with ignition control.

1.2 Features

- 14th/13th Gen Intel® Core™ i9/i7/i5/i3 Desktop Processors
- 3x 2.5GbE LAN ports & 6x USB 3.2
- 1x DisplayPort (DP++) + 1x HDMI 2.0 + 1x VGA(optional)
- Built-in 8-in & 8-out isolated Digital I/O
- 2x removable drive bays for SSD with RAID0/1
- 1x accessible M.2 NVMe SSD (optional)
- Supports iAMT(16.1) & TPM (2.0)
- 8V~48V DC input with ignition control

1.3 Packing List

Item	Q'ty	IBASE P/N
AES100	1	
Manual @ Driver download instruction	1	D2MANUAL--0000100P
Wall mount bracket	2	H06Z1AES10001000AP
DC-input Matching Connector(4 pins)	1	C1216EC7604107000P
DC-in GND Matching Connector(3 pins)	1	C1216EC7603107000P
GPIO Matching Connector (20 pins)	1	C1216015620103000P
Remote SW Matching Connector (2pins)	1	C1216EC3502103200P
Screw for SSD (if not pre-installed)	8	H0230461012200000P
Screw for wall mount	8	H0240813012200000P

1.4 Optional Items

Item	IBASE P/N
AES100 Power supply kit	SC2AES100--0A1100R
M.2 2280 NVMe SSD tray kit	SC2AES100--0A1200R
VGA internal cable	C501VGA1215302000P

1.5 Specifications

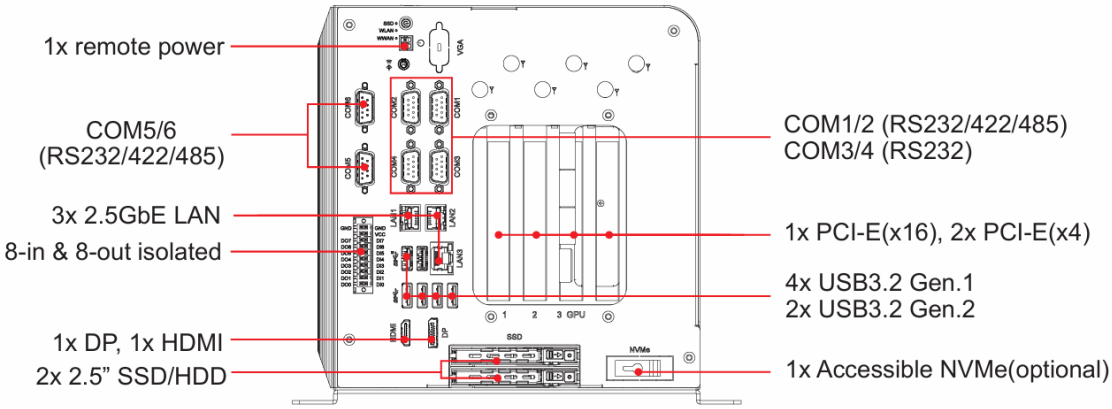
Product Name	AES100 Advanced Expandable Edge AI Computer
Chipset / PCH	Intel® R680E PCH
Mainboard	MBA-100
CPU Type	14th/13th Gen Intel® Core™ i9/i7/i5/i3 desktop processors (65W/35W)
System Speed	Up to 5.0 GHz
Memory	2x DDR5-4800/5600 SO-DIMM, Max. 64GB
Front Panel External I/O	• 1x DisplayPort (DP++) + 1x HDMI 2.0 + 1x VGA (optional) • 3x RJ45 2.5GbE • 2x USB 3.2 Gen.2 + 4x USB 3.2 Gen.1 • 4x COM (RS232/422/485) + 2x COM (RS232) • 8-in & 8-out isolated DIO • 1x Line-out + 1x MIC-in • 6x antenna holes • 1x remote power switch • 1x power button; LEDs: storage / WLAN / WWAN • 1x PCIe (x16) Gen4 + 2x PCIe (x4) Gen4
Rear Panel External I/O	• 1x 4-pin for 8V–48V DC input w/ ignition • 1x 3-pin for IGN
Side Panel I/O	2x external-accessible Nano SIM sockets
Expansion (M.2 / Mini PCIe)	• 1x M.2 2230 E-key (PCIe + USB 2.0 + SMBus) • 1x M.2 3042/3052 B-key (PCIe + USB 3.2 Gen1) • 1x M.2 2280 M-key (PCIe x4 Gen4) • 2x Mini PCIe full-size (PCIe + USB 2.0 + SMBus)
Storage (2.5”)	2x 2.5” HDD/SSD (front-accessible, removable bays)
Storage (Optional)	1x front-accessible M.2 2280 NVMe SSD tray (PCIe x4 Gen4)
Construction	Aluminum & steel
Chassis Color	Silver & Gray
Mounting	Wall mount
Dimensions	213.8mm (W) x 363.6mm (D) x 215mm (H) 8.4” (W) x 14.3” (D) x 8.46” (H)
Weight	9.4 kg
Power Input	8V–48V DC input with ignition control
Certification	CE (EN 62368-1 / EN55032 / EN55035), FCC Class A

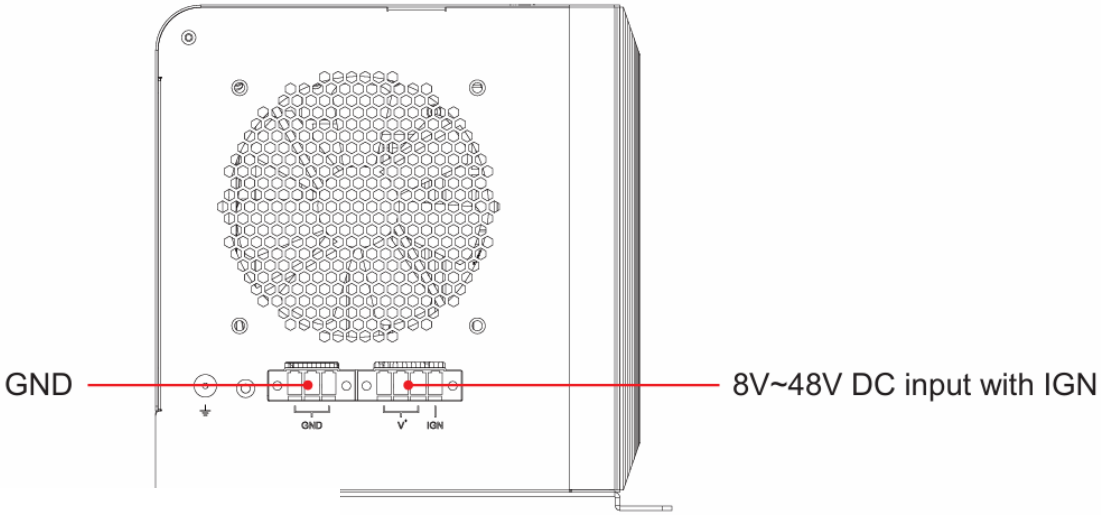
Environment	
Operating Temperature	-20°C to 60°C (-4°F to 140°F) *with airflow
Storage Temperature	-40°C to 70°C (-40°F to 158°F)
Relative Humidity	5–90% @ 45°C (non-condensing)
Vibration	MIL- STD-810H Operating (SSD): 2.26 Grms (5~500 Hz)
Shock	MIL-STD-810H Operating: Sawtooth: 20G, 11msec (Z-axis)

All specifications are subject to change without prior notice.

1.6 Product View

Front and Rear View





GND

Pin	Assignment
1	Ground
2	Ground
3	Ground

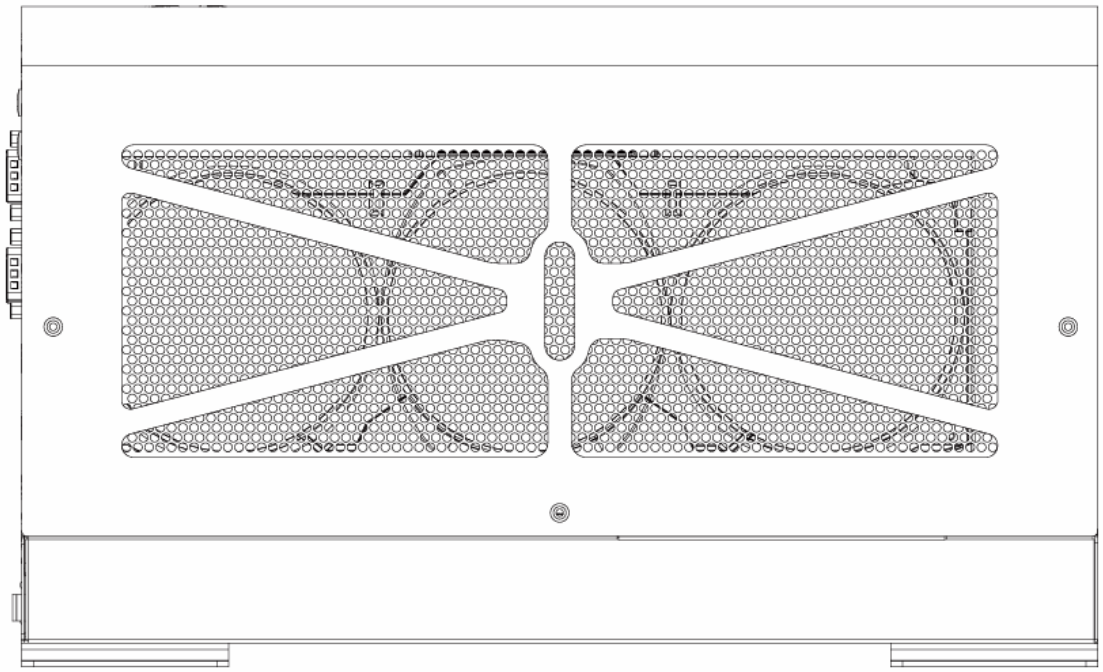
Power Input (Positive)

Pin	Assignment
1	DC IN+
2	DC IN+
3	DC IN+
4	IGN

Note: Marked in Red is IGN(PIN 4)

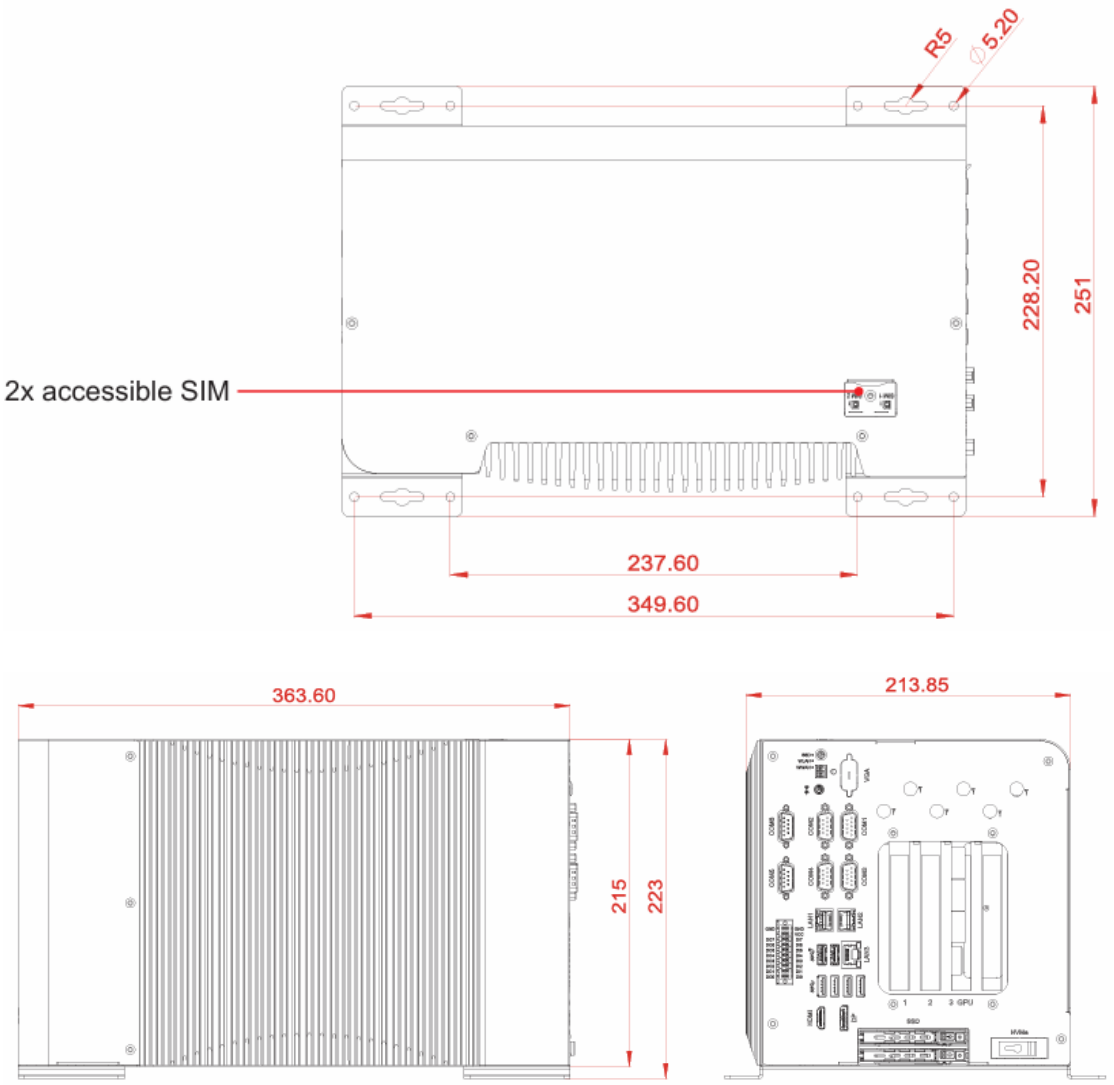
Side View

Side Panel External I/O	● 2x External accessible Nano SIM sockets



Oblique View

1.7 Dimensions



Chapter 2
Hardware Configuration

The information provided in this chapter includes:

- installations
- Information and locations of connectors

2.1 Installation

The **AES100 Expandable Edge AI System** is designed with a modular mechanical structure that allows users to access internal components—such as system memory, storage devices, and expansion modules—by removing the external chassis covers. This chapter provides step-by-step instructions for disassembling the system to safely access internal installation areas.

Before performing any installation, disassembly, or maintenance operation, ensure that the system is completely powered off and disconnected from all power sources.

After completing the disassembly steps described in this chapter, users will be able to access internal installation points, including:

- DDR5 SO-DIMM slots for system memory installation
- M.2 expansion slots, including:
    - M-Key (for NVMe SSD installation)
    - E-Key / B-Key (for wireless or other supported expansion modules, depending on configuration)
- 2.5-inch SSD/HDD mounting bays
- Other user-serviceable expansion areas as supported by the system configuration

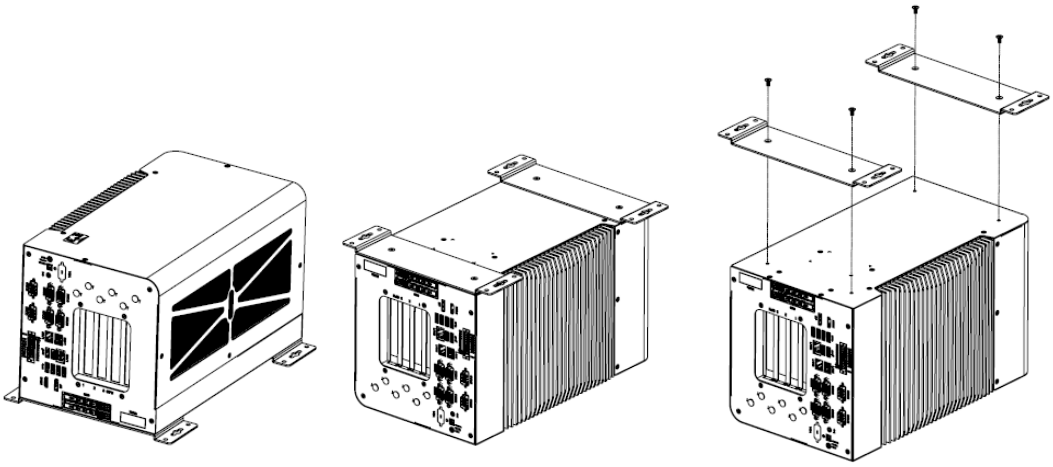
Reassembly should be performed by reversing the disassembly steps in the order described.

2.1.1 Installation and Disassembly Instructions

Purpose
This section describes the required disassembly steps to access internal motherboard slots, including memory, M.2 storage, and wireless module sockets. Only components that physically obstruct access to the motherboard are covered.

Safety Notice
Before proceeding:
• Power off the system
• Disconnect the DC power input
• Allow the system to cool completely

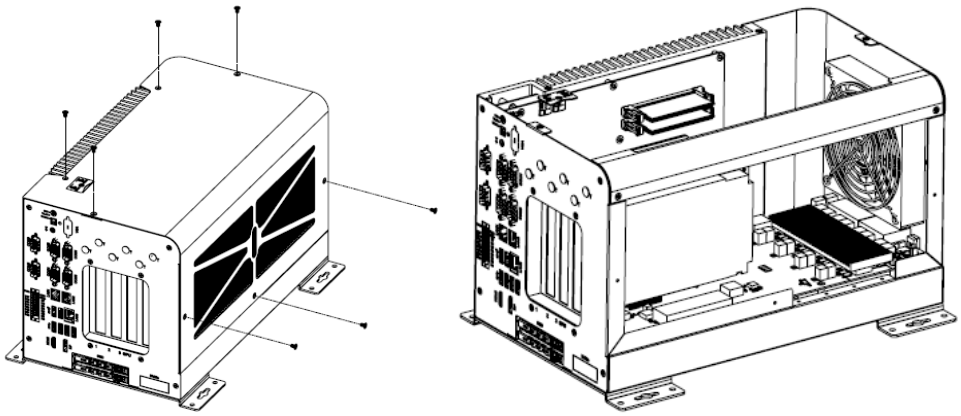
Step 1 – Remove Wall Mount Bracket (If Installed)



(Figure1 : Wall Mount Bracket Removal)

1. Place the system upside down on a stable, flat surface.
2. If a wall mount bracket is installed, locate the bracket attached to the bottom of the chassis.
3. Remove four mounting screws securing the wall mount bracket (Screw D13 ×4).
4. Remove the wall mount bracket and set it aside.

Step 2 – Remove Top System Cover

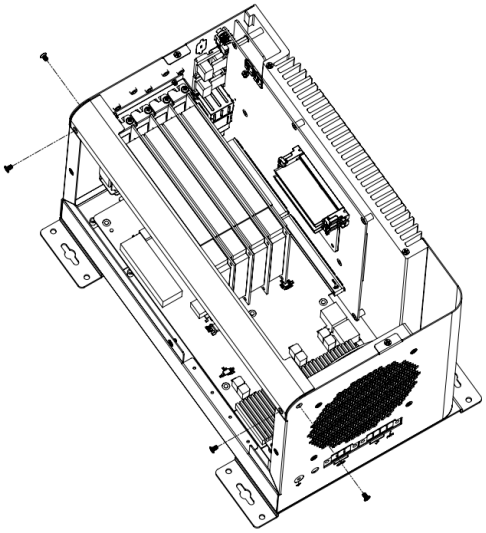


(Figure 2: Top Cover Removal)

1. Return the system to its normal upright position.
2. Locate the top system cover.
3. Remove seven screws securing the top cover to the chassis (Screw B30-N ×7).
4. Lift the top cover upward and remove it completely.

After this step, the internal structure of the system becomes visible.

Step 3 – Remove Base Bracket



(
Figure 3: Base Bracket Removal)

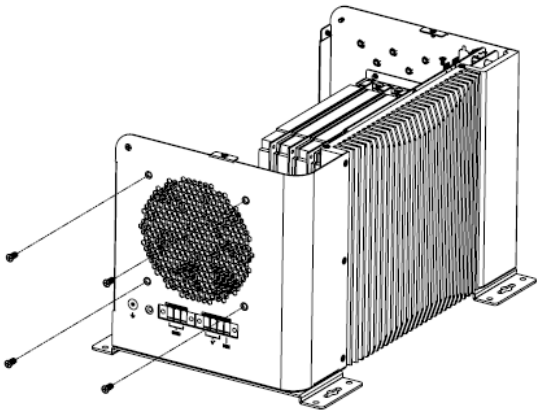
Purpose

The base bracket is a long internal support bracket installed along the side of the chassis.
It must be removed after the top system cover is taken off to allow access to the motherboard slots.

Procedure

1. With the top system cover already removed, locate the base bracket inside the chassis.
   The base bracket runs along the side of the internal frame and is clearly visible in the internal view.
2. Identify the four screws securing the base bracket to the chassis.
3. Remove all four screws (Screw B30-N ×4).
4. Carefully lift the base bracket upward and remove it from the chassis.
   After removing the base bracket, the motherboard area becomes further exposed, allowing subsequent access to internal components.

Step 4 – Remove Cooling Fan Assembly



(Figure 4: Fan Removal)

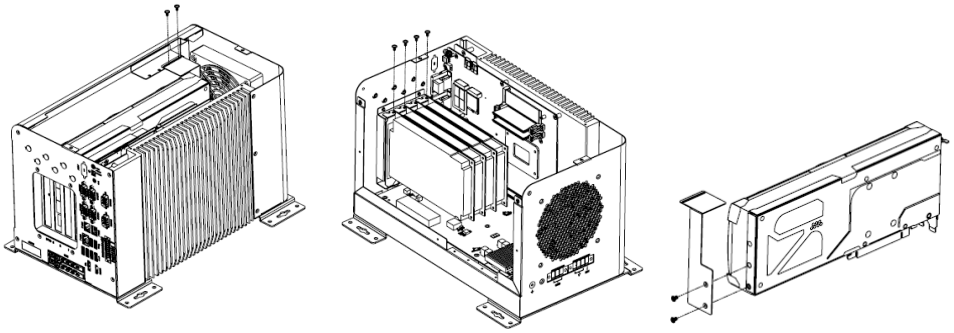
Purpose
The cooling fan assembly is installed above the motherboard and must be removed to provide clearance for accessing memory slots and other onboard connectors.

Procedure

1. Locate the cooling fan assembly mounted above the motherboard.
2. Disconnect the fan cable from the motherboard fan connector.
3. Remove the four screws securing the fan to the chassis (Screw E2 ×4).
4. Carefully lift the fan assembly upward and remove it from the system.

After removing the fan assembly, the motherboard slots and internal connectors are fully accessible.

Step 5 – Remove GPU Card and GPU Bracket (If Installed)



(Figure 5: GPU Card and Bracket Removal)

Purpose
If a discrete GPU card is installed, it must be removed to fully clear the motherboard area and allow unobstructed access to motherboard slots.

Procedure

1. Locate the GPU card installed along the side of the chassis.
2. Identify the **GPU bracket** securing the GPU card to the chassis.
3. Remove the **two GPU bracket mounting screws** securing the bracket to the chassis *(Screw B16C ×2, per screw table)*.
4. Remove the **four screws securing the GPU card to the GPU bracket** *(Screw B28I ×4)*.
5. Carefully slide the GPU card straight out of the connector and remove it from the system.
6. Set the GPU card and GPU bracket aside on an anti-static surface.

After completing the above disassembly steps and removing any installed GPU card(s), the motherboard expansion areas are fully exposed. The following section identifies the user-accessible slots on the MBA100 motherboard that can be serviced or upgraded after disassembly. Only expansion slots intended for user access are listed. Jumper settings, pin definitions, and factory-reserved connectors are not included.
User-Accessible Slots (MBA100)

- DDR5 SO-DIMM Memory Slots
  DDR5 SO-DIMM Socket (J6, J7)
- M.2 Expansion Slots
  M.2 M-key 2280 Slot (PCIe x4) (J9)
  M.2 E-key 2230 Slot (Wi-Fi / Bluetooth) (J15)
  M.2 B-key 3052 Slot (Cellular / WWAN) (J18)
- Mini PCIe Slots
  MiniCard Slot (J12, J14)
- PCI Express Slots
  PCI Express x16 Slot (PCIE1)
  PCI Express x4 Slots (PCIE2, PCIE3)

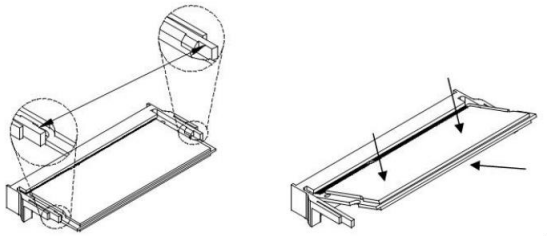
2.1.2 Memory Module Installation

Before proceeding, ensure that the system covers have been removed and the memory slot(s) are accessible.

The AES100 system supports DDR5 SO-DIMM memory modules.

Steps

1. Identify the memory slot on the motherboard.
2. Align the key of the memory module with the key in the slot and insert the module into the slot at an angle.
3. Gently press the module downward until it is fully seated and the retention clips on both sides lock into place.



To remove the memory module, gently push the retention clips outward until the module is released, then remove the module from the slot.

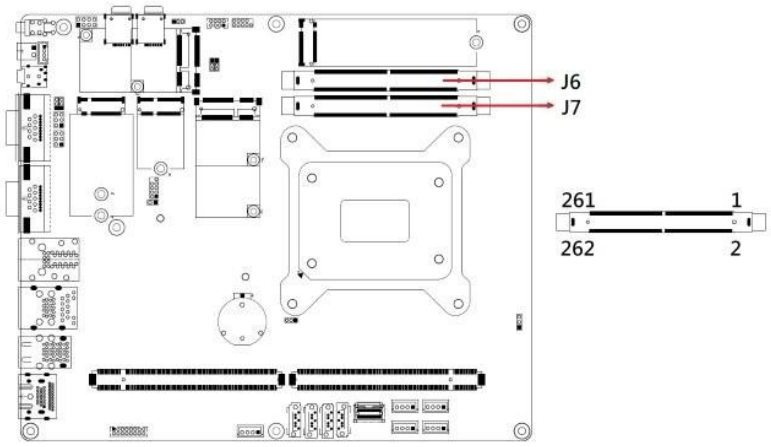


Figure: DDR5 SO-DIMM Location

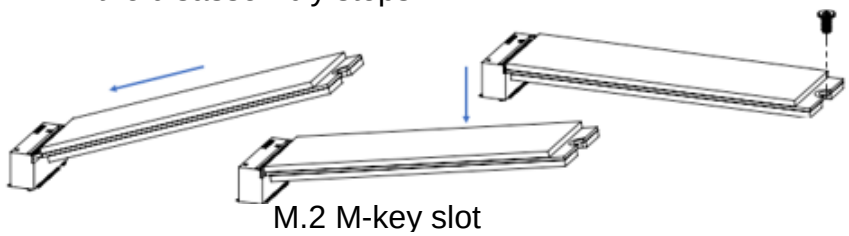
2.1.3 Expansion Card Installation (M.2 / Mini PCIe)

Before proceeding, ensure that the system covers have been removed and the internal expansion slots are accessible.

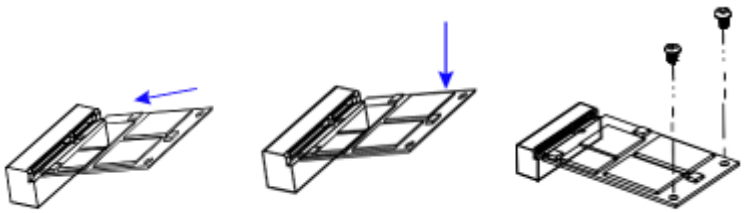
The AES100 system supports multiple internal expansion slots, including M.2 (M-Key, B-Key, E-Key) and Mini PCIe slots. Installation procedures are identical in principle and are illustrated in the accompanying figures.

Steps

1. Ensure the system is powered off and disconnected from the DC power input. Place the system on a flat, stable surface.
2. Identify the appropriate expansion slot according to the module type to be installed.
3. Align the connector key of the module with the slot. Insert the module into the slot at an angle, as shown in the figure.
4. Gently press the module downward until it is level with the mounting surface.
5. Secure the module to the standoff using the provided screw.
6. If required, connect antenna or auxiliary cables according to the module type.
7. After installation is complete, reinstall all removed covers by reversing the disassembly steps.



M.2 M-key slot



mini-PCIe slot

Expansion Slots on the MBA100 Motherboard

1. M-key 2280 Slot (PCIe x4) (J9)
2. M.2 E-key 2230 Slot (Wi-Fi / Bluetooth) (J15)
3. M.2 B-key 3052 Slot (Cellular / WWAN) (J18)
4. Mini PCIe Slots
5. MiniCard Slot (J12, J14)

Note: Refer to section 2.2

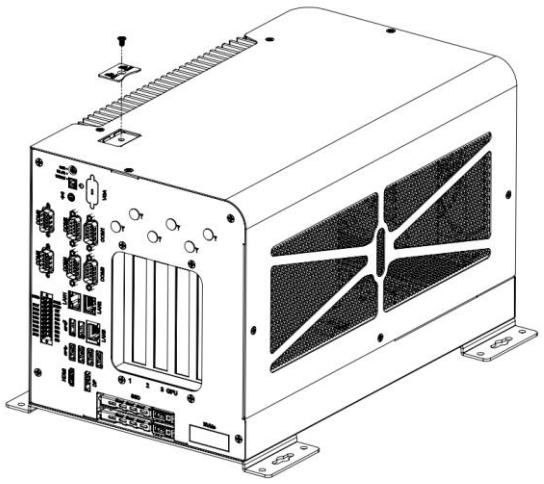
2.1.4 SIM Card Installation (External)

Before proceeding, ensure that the system is powered off and all external power sources are disconnected.
The AES100 system provides an externally accessible SIM card slot, allowing SIM installation without opening the chassis.

Steps

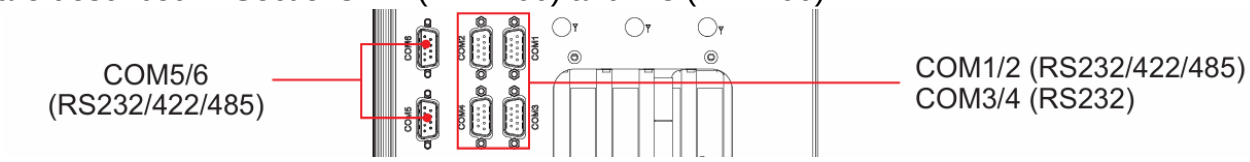
1. Locate the SIM card cover on the system chassis.
2. Remove the retaining screw securing the SIM cover (B30-N ×1).
3. Remove the SIM cover to expose the SIM card slot.
4. Insert the SIM card into the slot, ensuring correct orientation according to the slot marking.
5. Reinstall the SIM cover and secure it with the original screw.

To remove the SIM card, power off the system, remove the SIM cover, gently press the SIM card inward to release it, then pull the card out of the slot.



2.1.5 Pinout for COM Ports & GPIO Connector

Note: This section provides an overview of COM port signal pinouts and GPIO availability. Detailed connector locations and full GPIO pin definitions are described in Sections 2.2 (MBA100) and 2.3 (IDA-100).

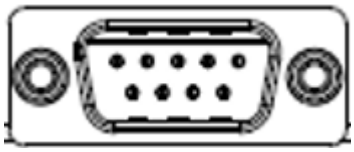


COM1/COM2/COM3/COM4 are provided by the MBA100 mainboard. COM5/COM6 and the GPIO signals are provided by the IDA-100 function board.

Port	Interface support	Notes
COM1 / COM2	RS-232 / RS-422 / RS-485	Mode is configurable in BIOS
COM3 / COM4	RS-232	Fixed RS-232
COM5 / COM6	RS-232 / RS-422 / RS-485	Provided by IDA-100

Note: RS-485 interfaces are implemented as 2-wire (half-duplex). Termination resistors and biasing are not provided on-board and must be implemented externally if required by the application.

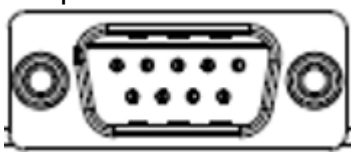
COM1/COM2 are RS-232/422/485 configurable in BIOS.
Note: Only one interface type (RS-232, RS-422, or RS-485) can be active at a time. Changing the interface type requires BIOS configuration and a system reboot.



Pin	Assignment	Pin	Assignment
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		

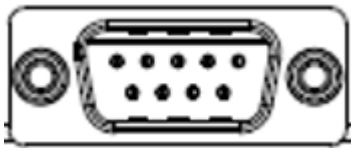
Pin	Assignment		
	RS-232	RS-422	RS-485
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	TX	RX+	NC
4	DTR	RX-	NC
5	Ground	NC	NC
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

COM3/COM4 are RS-232 ports.



Pin	Assignment	Pin	Assignment
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		

COM5/COM6 and the GPIO signals are provided by the IDA-100 function board.
Note: COM5 and COM6 are independent serial interfaces. GPIO signals are provided through a separate GPIO connector on the IDA-100 board and do not share pins with COM5/COM6.
Note: COM5 and COM6 correspond to COM A and COM B on the IDA-100 board.



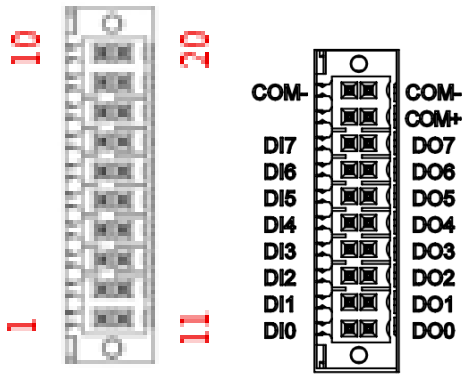
Pin	Assignment	Pin	Assignment
1	DCD, Data carrier detect	6	DSR, Data set ready
2	RXD, Receive data	7	RTS, Request to send
3	TXD, Transmit data	8	CTS, Clear to send
4	DTR, Data terminal ready	9	RI, Ring indicator
5	Ground		

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	NC	NC
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

GPIO Connector (IDA-100)

The AES100 provides eight channels of isolated DI, eight channels of isolated DO, (isolation voltage 2.5 KV). Pin definition and reference wiring diagrams are as follows:

Isolation 8 DI+ 8 DO



Pin	Signal	Pin	Signal
1	DI0	11	DO0
2	DI1	12	DO1
3	DI2	13	DO2
4	DI3	14	DO3
5	DI4	15	DO4
6	DI5	16	DO5
7	DI6	17	DO6
8	DI7	18	DO7
9	N.C	19	COM+
10	COM-	20	COM-

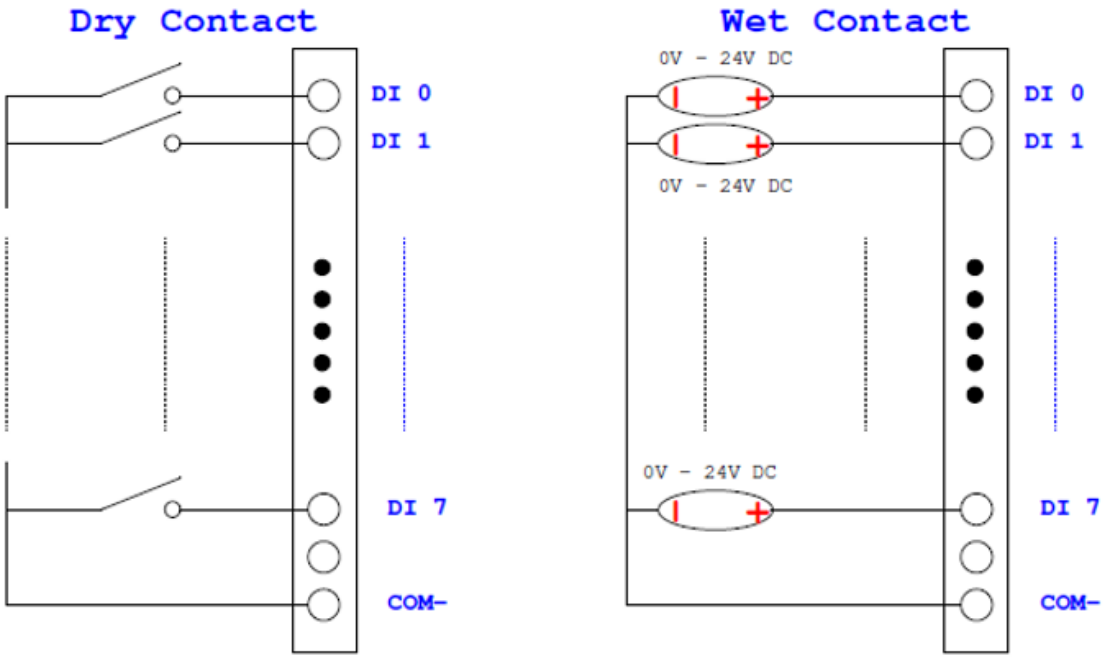
8 x insulated DI

- Maximum input range • 24 V, non-polarity
- Digital logic levels • 0-24 V, non-polarity
- Input high voltage: 5-24 V
- Input low voltage: 0-1.5 V
- Input resistance: 1.2 kΩ@ 0.5 W
- Isolation voltage: 2500 VRMS

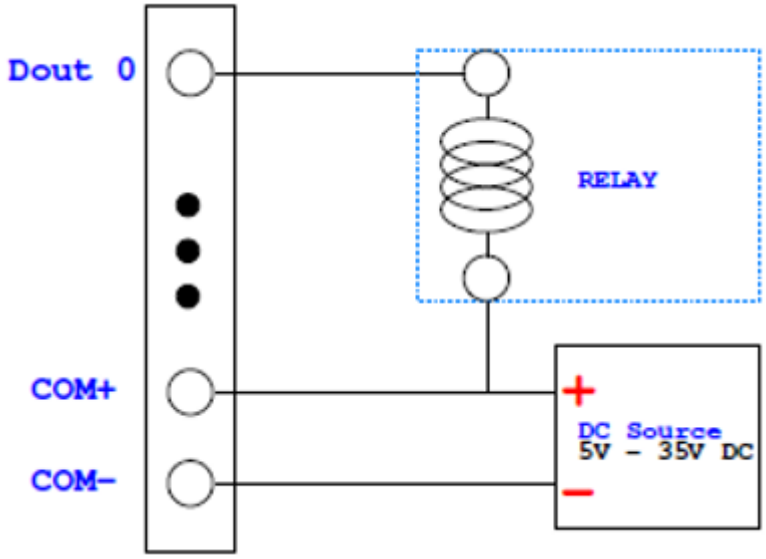
8 x insulated DO

- Output type: Darlington transistor
- Sink current • 200 mA for one channel @ 100% duty
- Source current • 200 mA for one channel @100% duty cycle
- Supply voltage: 5-35 VDC
- Isolation voltage: 2500 VRMS

DI (Dry & Wet contact)



DO Ex: Relay control



2.1.6 Antenna Installation

This section applies only when a wireless module (WiFi, LTE, or 5G) is installed.
The AES100 system provides pre-installed antenna mounting holes on the chassis. These holes are typically covered with protective plugs when not in use.

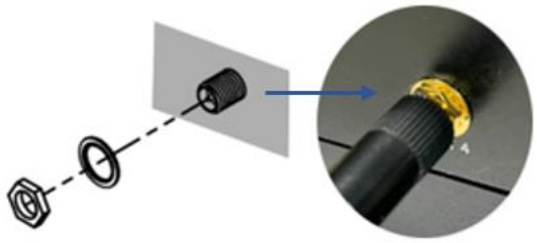
Steps

1. Remove the protective plug from the antenna mounting hole.
2. Insert the antenna cable connector through the hole from the inside of the chassis.
3. Place the washer and nut on the connector from the outside.
4. Tighten the nut securely to fix the antenna connector in place.
5. Attach the external antenna to the connector.

Note

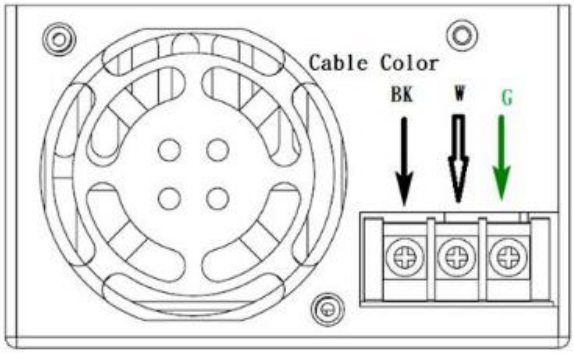
Ensure the antenna connector is firmly secured to prevent loosening during operation.

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



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

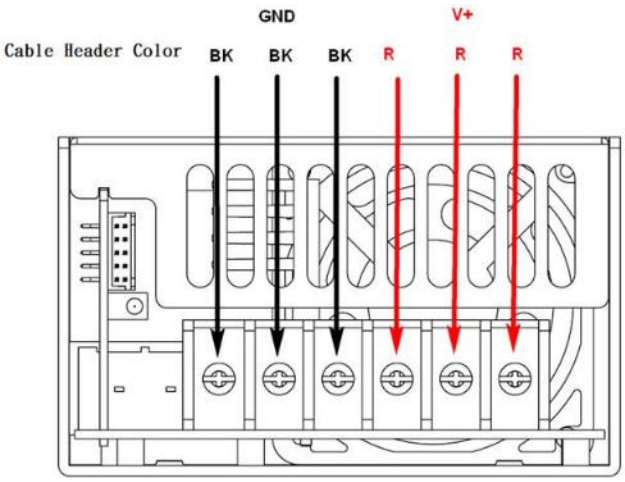
2.1.7 Extend PSU Installation

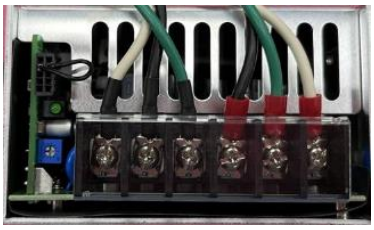


PSU AC INPUT Installation

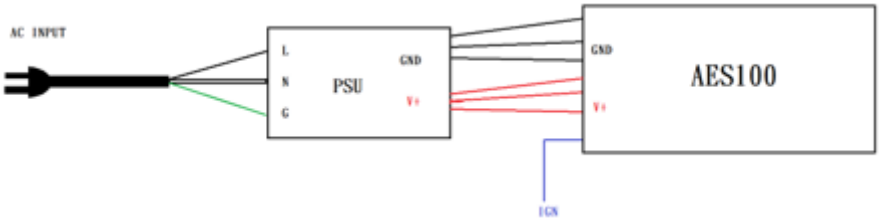
Steps:

1. Turn OFF AC power and confirm no power is present.
2. Identify the AC INPUT terminal block labeled L / N / G.
3. Identify each wire by its insulation color:
   - Black: Live (L)
   - White: Neutral (N)
   - Green: Ground (G)





4. Insert each wire into the corresponding terminal.
5. Tighten all terminal screws securely.
6. Verify that all wires are firmly fixed and no copper is exposed.

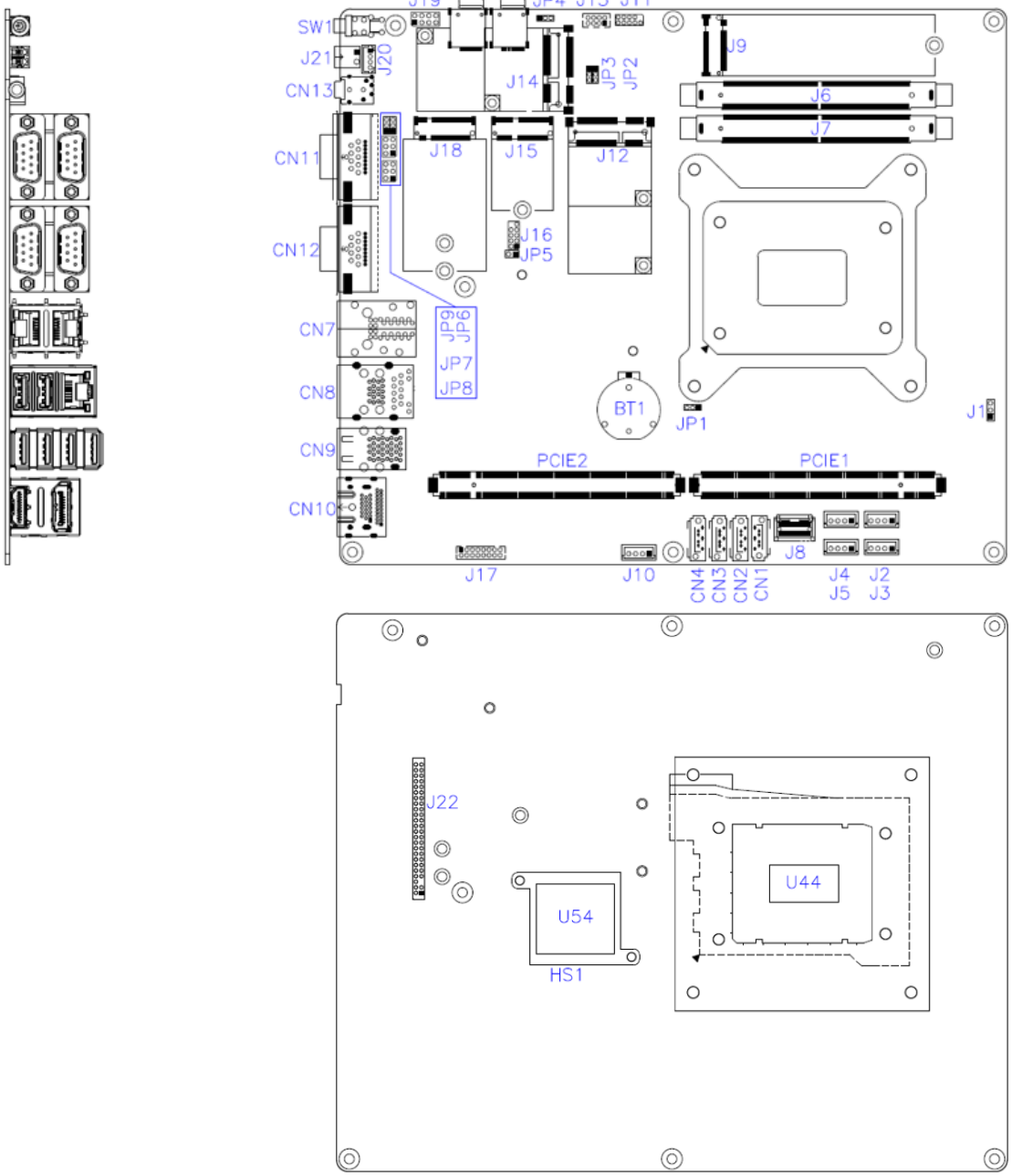


Complete Wiring Diagram (AC Input to AES100 via PSU)

2.2 Mainboard (MBA100)

The MBA100 is the mainboard of the **AES100** system. It integrates the CPU, memory, chipset, storage interfaces, and core I/O functions. The MBA100 is responsible for system processing, data handling, and communication with expansion boards. Other system boards, including the **IDA-100** and **IPA-100**, connect to the **MBA100** through dedicated board-to-board connectors to extend I/O capability and power management functions.

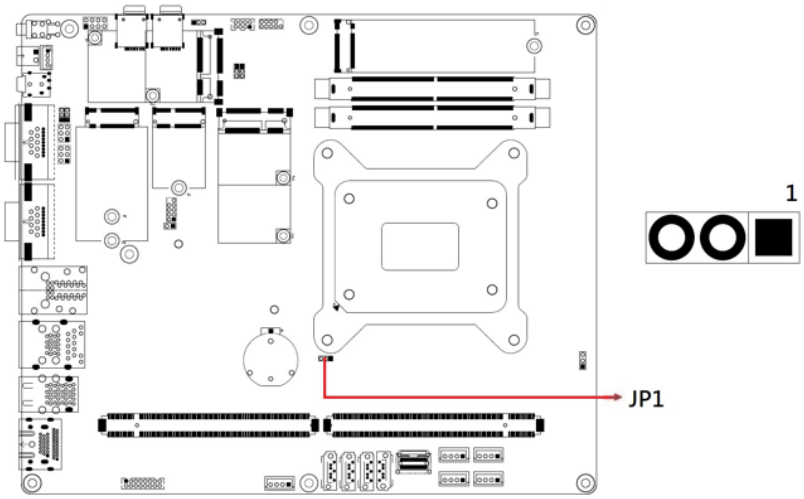
Board Layout



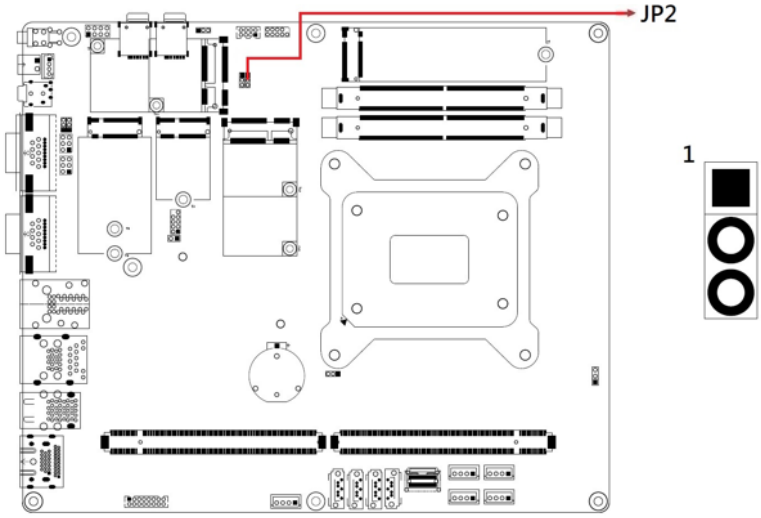
Jumper and Connector Quick Reference

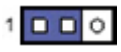
Function (MBA100)	Jumper / Connector
Factory Use Only	JP1
Clear ME Contents	JP2
Clear CMOS Contents	JP3
SIM Card Select	JP4
Flash Descriptor Security Override	JP5
Sierra EM9191 5G Card USB/PCIe Select	JP6
COM1/COM2 RS232 RI/+5V/+12V Power Setting	JP7, JP8
ATX & AT Power Mode Selection	JP9
SATA Power Connector	J2, J3, J4, J5, J10
SlimSAS	J8
DDR5 SO-DIMM Socket	J6, J7
M.2 M-key 2280 (PCIe x4)	J9
SPI Flash Connector	J11
MiniCard Slot	J12, J14
2× USB 2.0	J13
M.2 E2230 Slot	J15
80 Port Debug	J16
VGA	J17
M.2 B-key 3052 Slot	J18
Front Panel Signals	J19
Speaker Out	J20
Remote Power Switch	J21
Board to Board Connector	J22
SATA III 7-pin Connector	CN1, CN2, CN3, CN4
Nano SIM Card 2 / Nano SIM Card 1 Slots	CN5, CN6
2× 2.5 Gigabit LAN (Intel I226-IT) Stack Connector	CN7
2.5 Gigabit LAN (Intel I226-LM) + USB 3.2 Gen 2	CN8
4× USB 3.2 Gen 1 Type-A	CN9
DisplayPort (Top) + HDMI (Bottom)	CN10
COM1/COM2 Ports	CN11
COM3 & COM4 RS-232 Ports	CN12
Audio Jack (Line out + MIC IN)	CN13
Power Button	SW1
Coin Battery Socket	BT1
Non-Standard High-speed Board-to-Board Slots	PCIE1, PCIE2

JP1: Factory Use Only

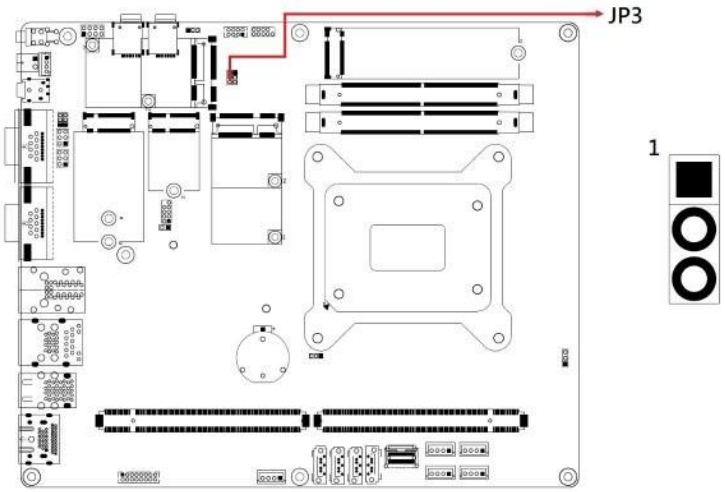


JP2: Clear ME Contents



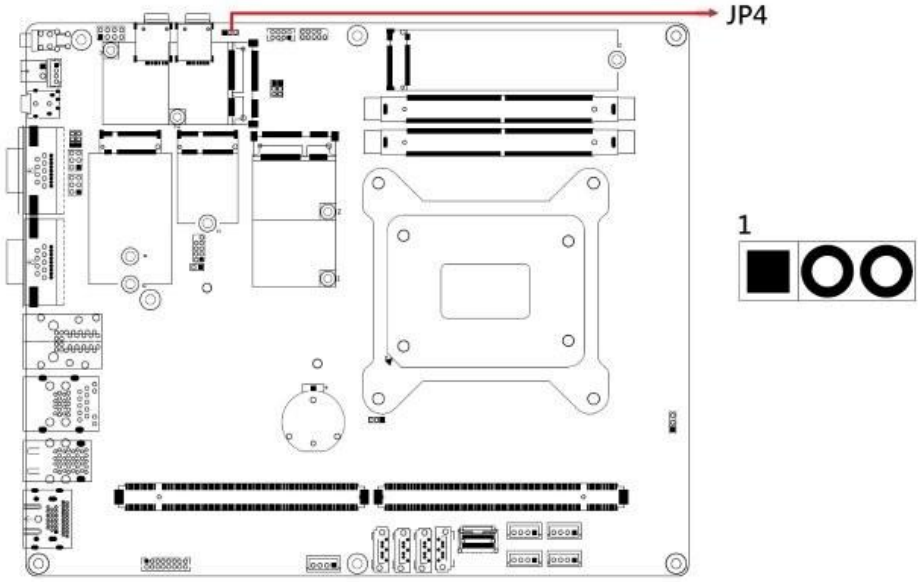
Function	Pin closed	Illustration
Normal	1-2	
Clear ME	2-3	

JP3: Clear CMOS Contents



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

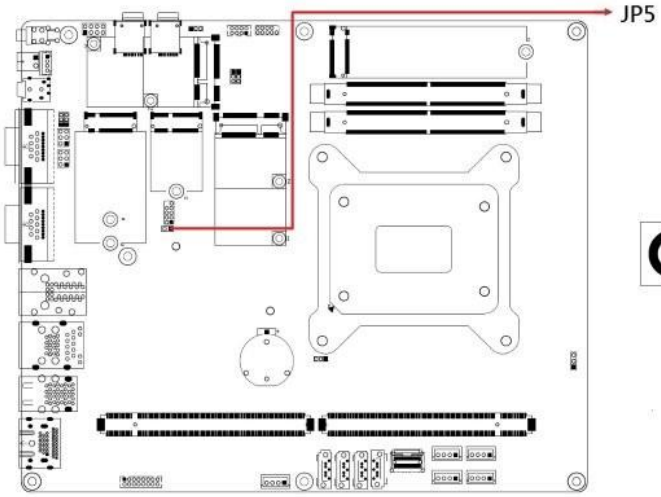
JP4: SIM Card Select



Function	Pin closed	Illustration
M.2 (J18)	1-2	
Minicard (J14)	2-3	

Note: SIM Slot (CN5) selected to match the module used.

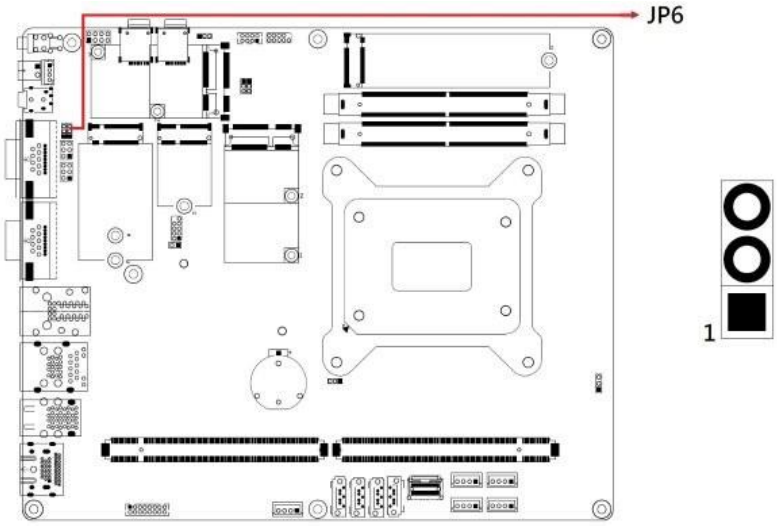
JP5: Flash Descriptor Security Override



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

Note: JP5 is for factory use only

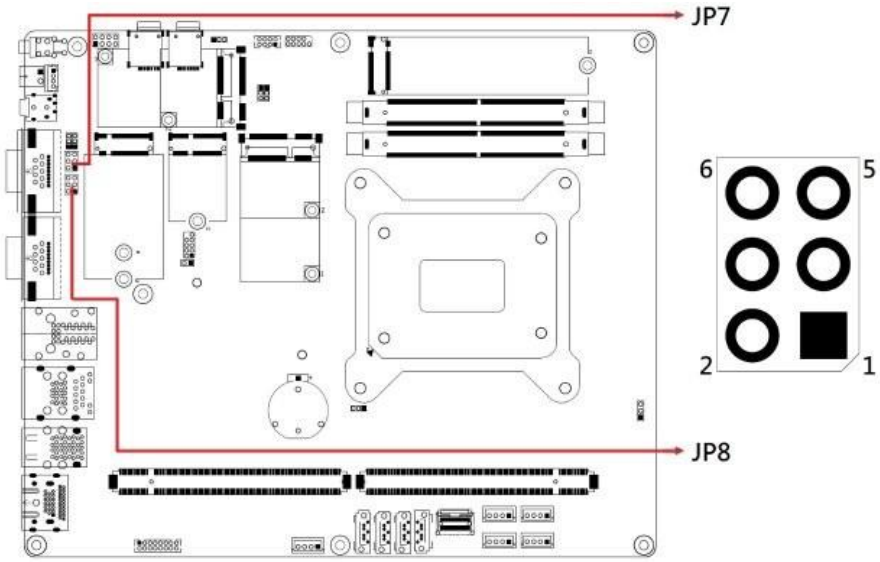
JP6: Sierra EM9191 5G Card USB/PCIe Select

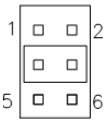


Function	Pin closed	Illustration
USB(default)	1-2	1
PCIe	2-3	1

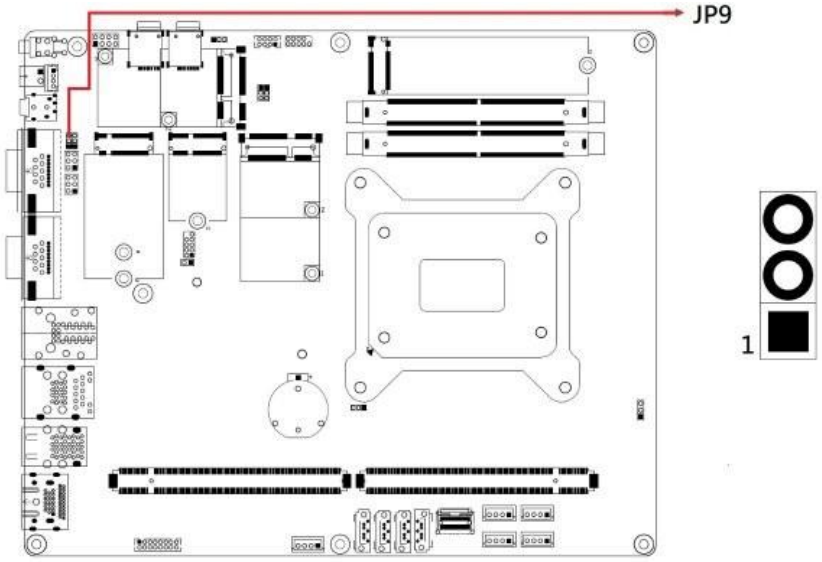
Note: This setting is for J18 only.

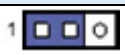
JP7, JP8: COM1/COM2 RS232 RI/+5V/+12V Power Setting



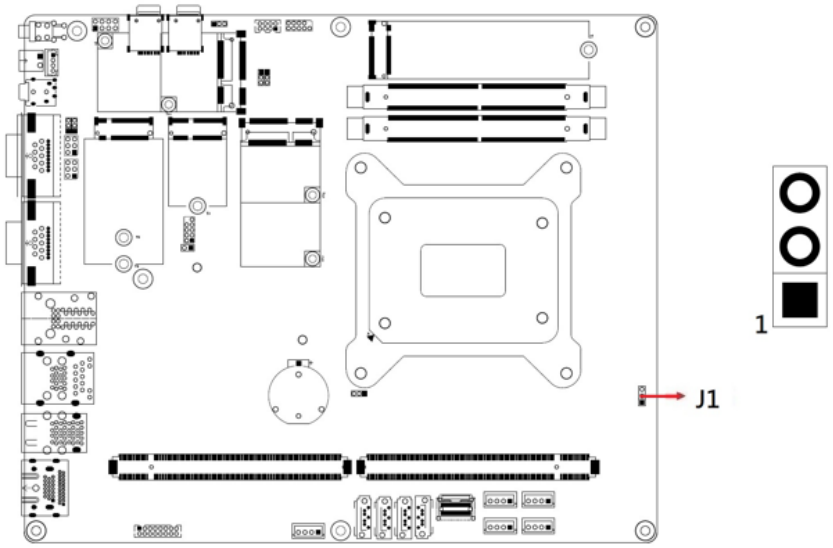
Function	Pin closed	Illustration
+12V	Pin 1-3, Short/Closed	
RI (Default)	Pin 3-4, Short/Closed	
+5V	Pin 3-5, Short/Closed	

JP9: ATX & AT Power Mode Selection

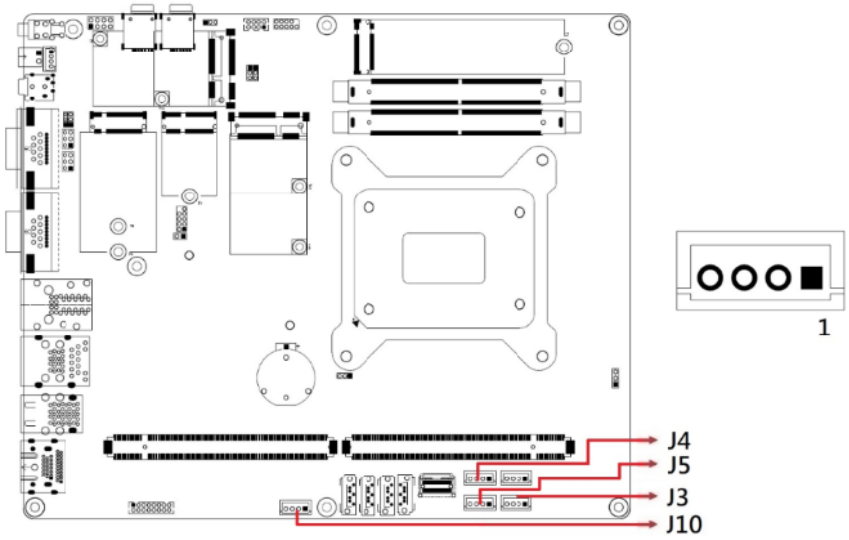


Function	Pin closed	Illustration
ATX (default)	1-2	
AT	2-3	

J1: Factory Use Only

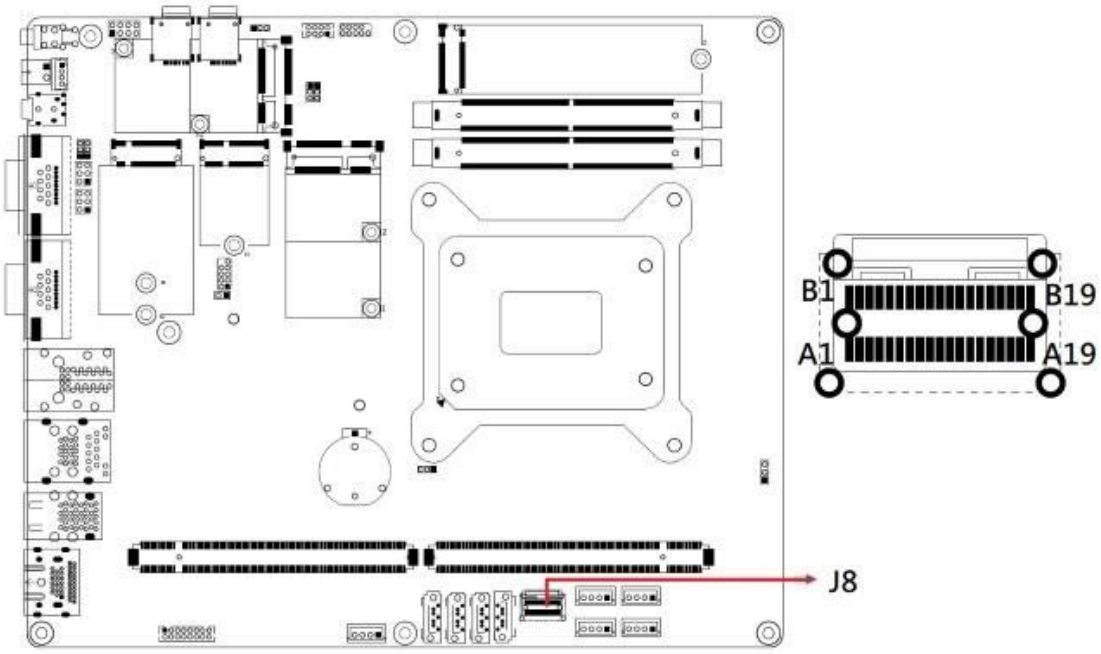


J3, J4, J5, J10: SATA Power Connector



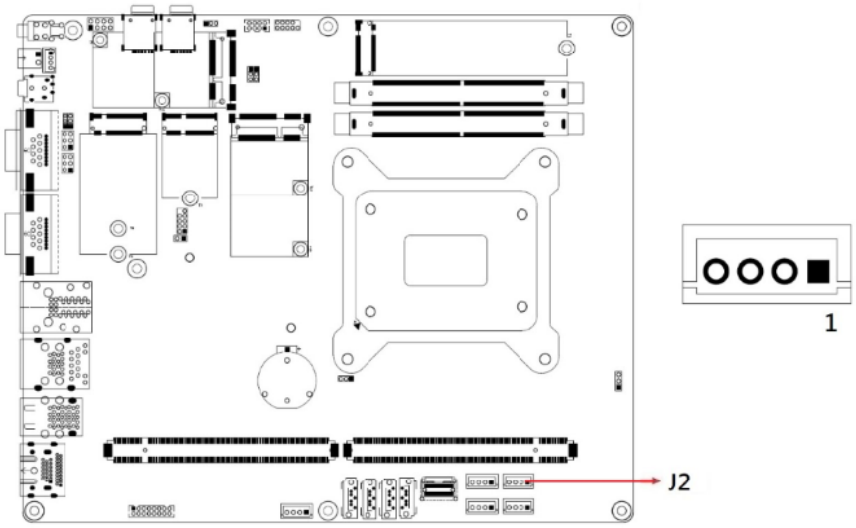
Pin	Assignment
1	+5V
2	Ground
3	Ground
4	NC

J8: SlimSAS



Pin	Assignment	Pin	Assignment
A1	Ground	B1	+5V(0.5A)
A2	RX0+	B2	TX1+
A3	RX0-	B3	TX0-
A4	Ground	B4	Ground
A5	RX1+	B5	TX1+
A6	RX1-	B6	TX1-
A7	Ground	B7	Ground
A8	NC	B8	NC
A9	NC	B9	NC
A10	Ground	B10	Ground
A11	CLK_P	B11	PLTRST
A12	CLK_N	B12	PRSNT
A13	Ground	B13	Ground
A14	RX2+	B14	TX2+
A15	RX2-	B15	TX2-
A16	Ground	B16	Ground
A17	RX3+	B17	TX3+
A18	RX3-	B18	TX3-
A19	Ground	B19	Ground

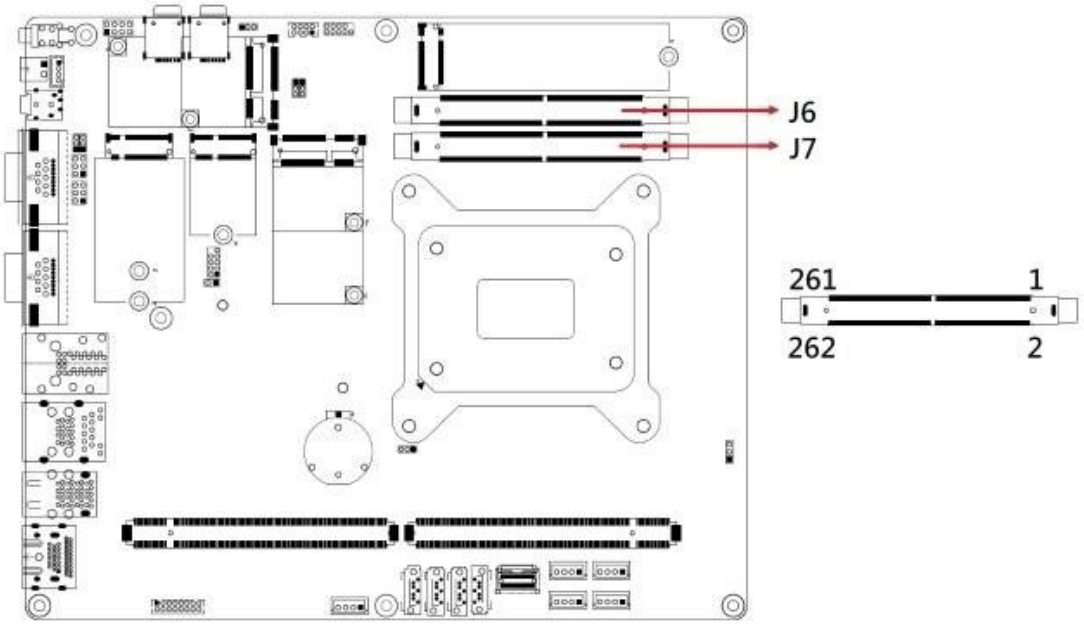
J2: SATA Power Connector



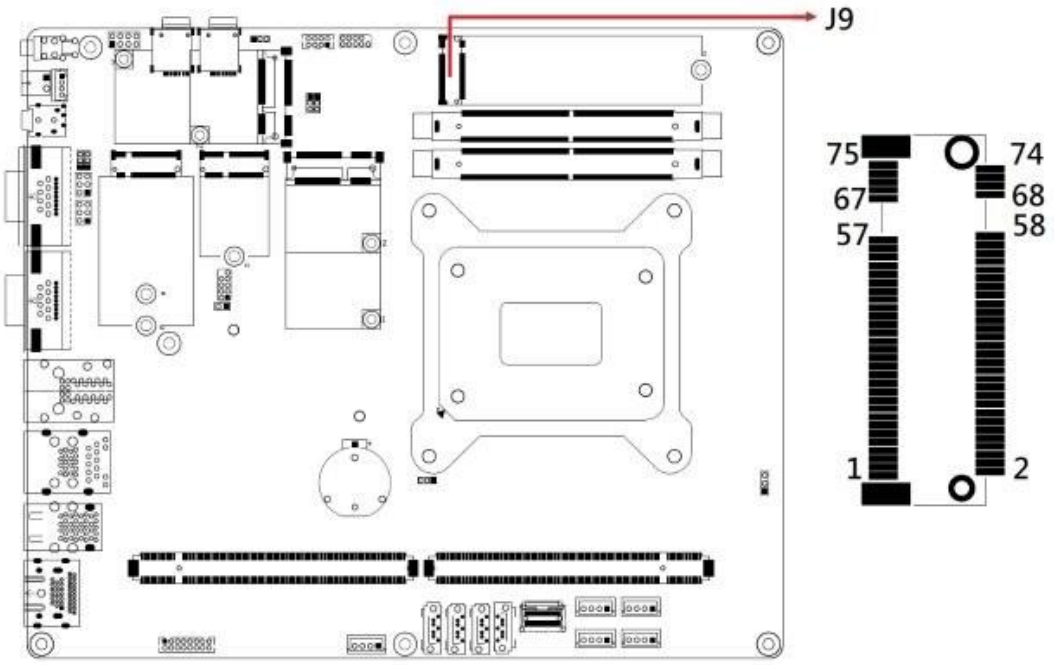
Pin	Assignment
1	+5V
2	Ground
3	Ground
4	+12V

Note: J2 connector is used with J8, if needed.
(JST_B4B-XH-A → Compatible Mating JST_XHP-4)
※ Only J2 has +12V at PIN 4

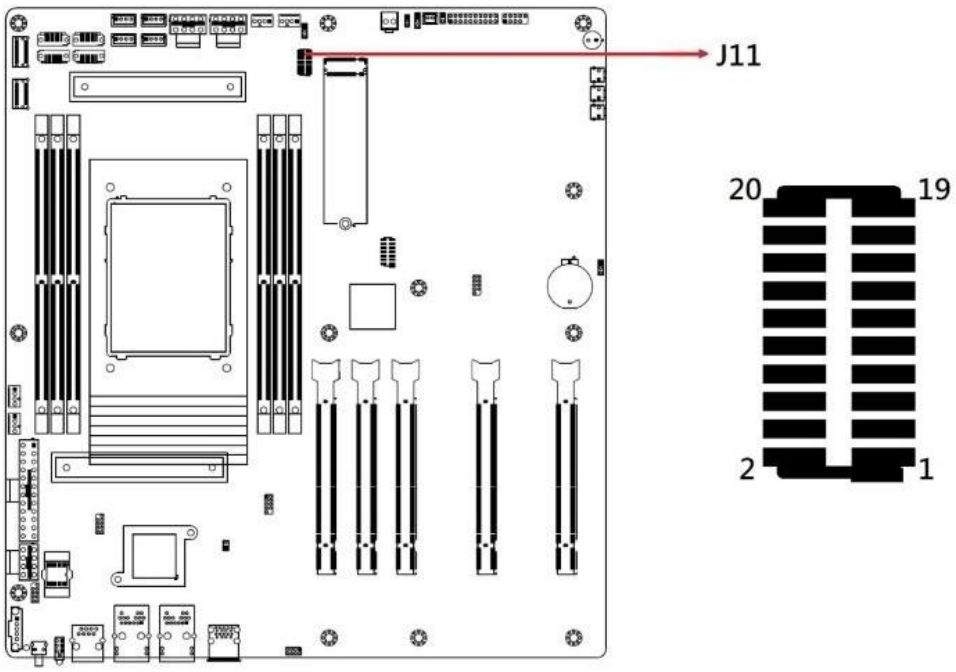
J6, J7: DDR5 SO-DIMM Socket



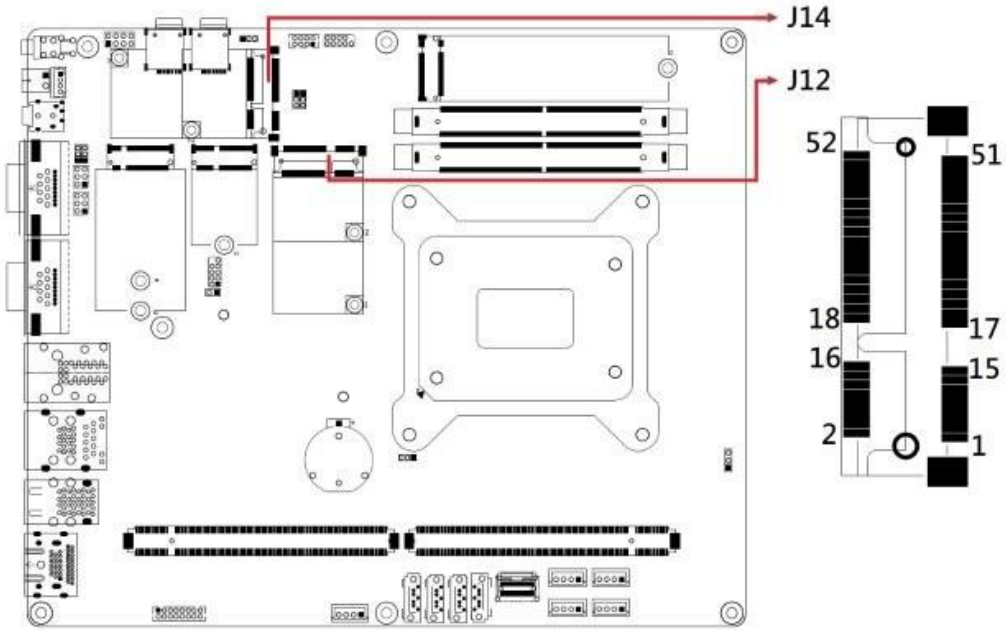
J9: M.2 M-key 2280 (PCIex4)



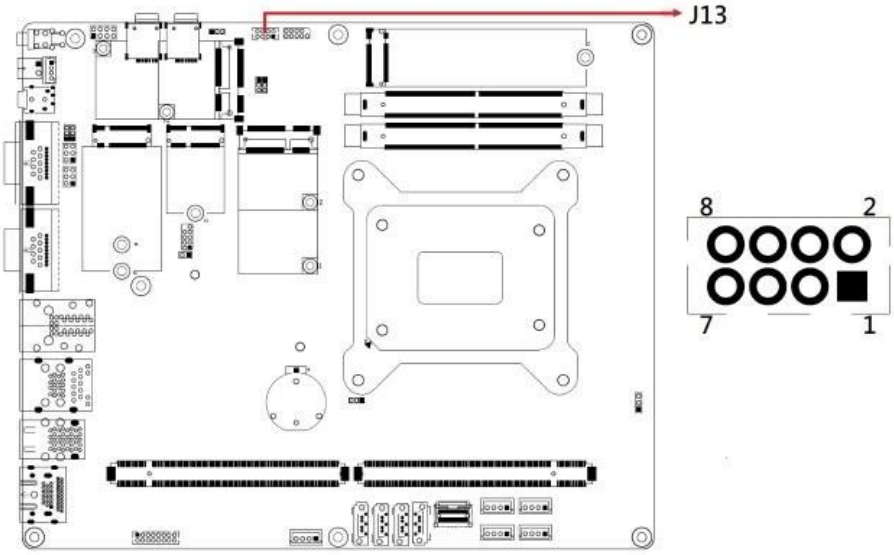
J11: SPI Flash Connector



J12, J14: MiniCard Slot

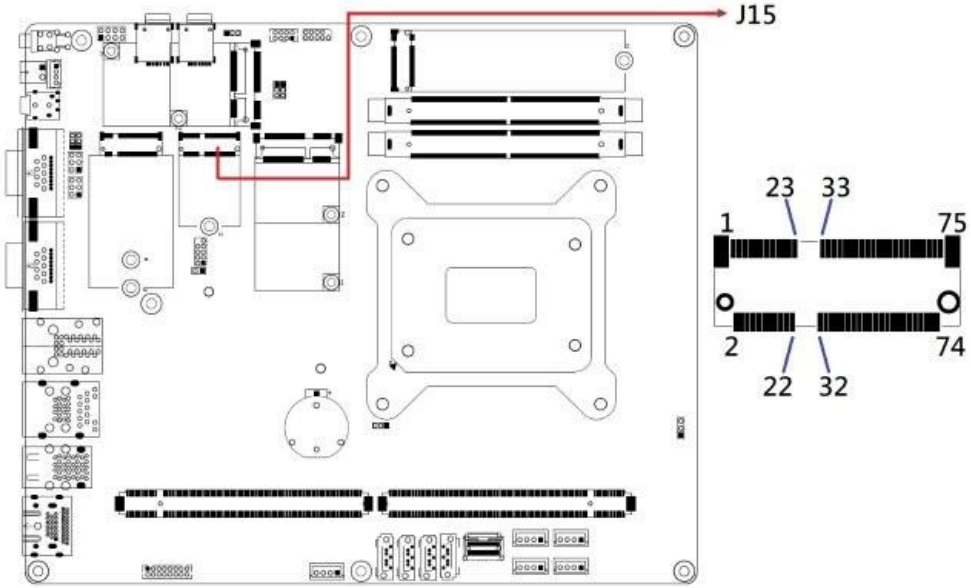


J13: 2x USB2.0 (DF11-8S-PA66H)



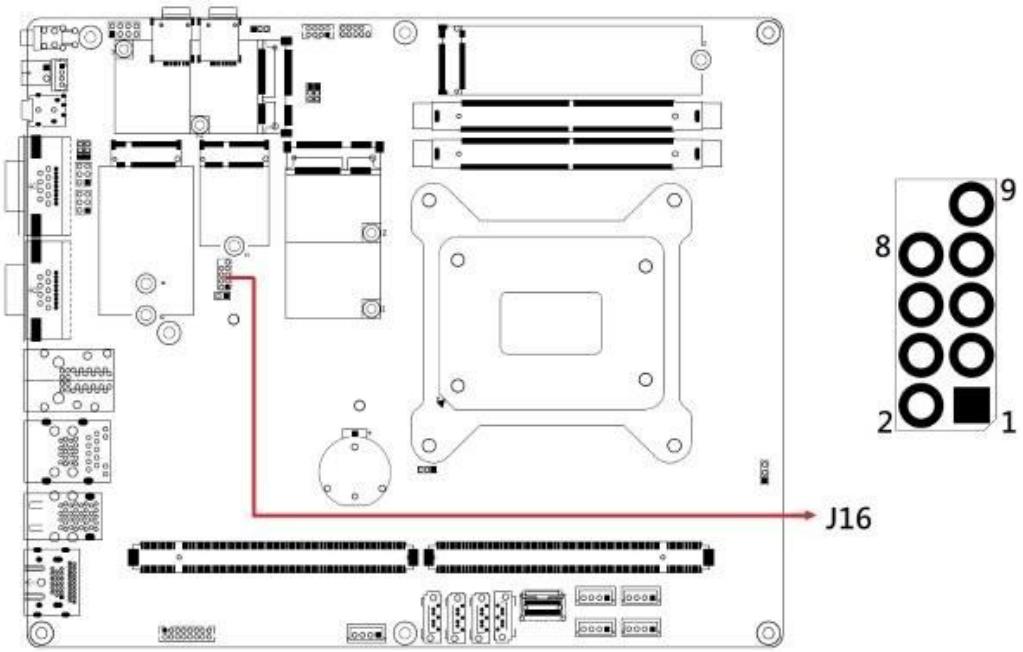
Pin	Signal	Pin	Signal
1	USBPWR	2	Ground
3	D-	4	D+
5	D+	6	D-
7	Ground	8	USBPWR

J15: M.2 E2230 Slot



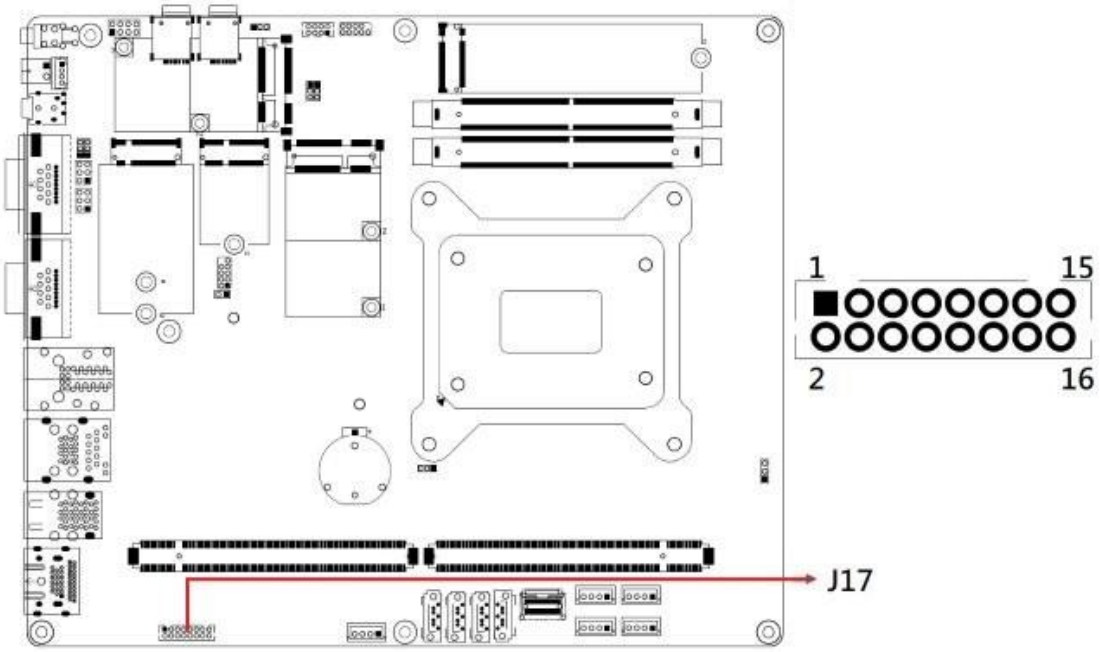
Note: J15 supports CNVi / PCIe(1x) / USB2.0

J16: 80 Port Debug



Note: Factory use only.

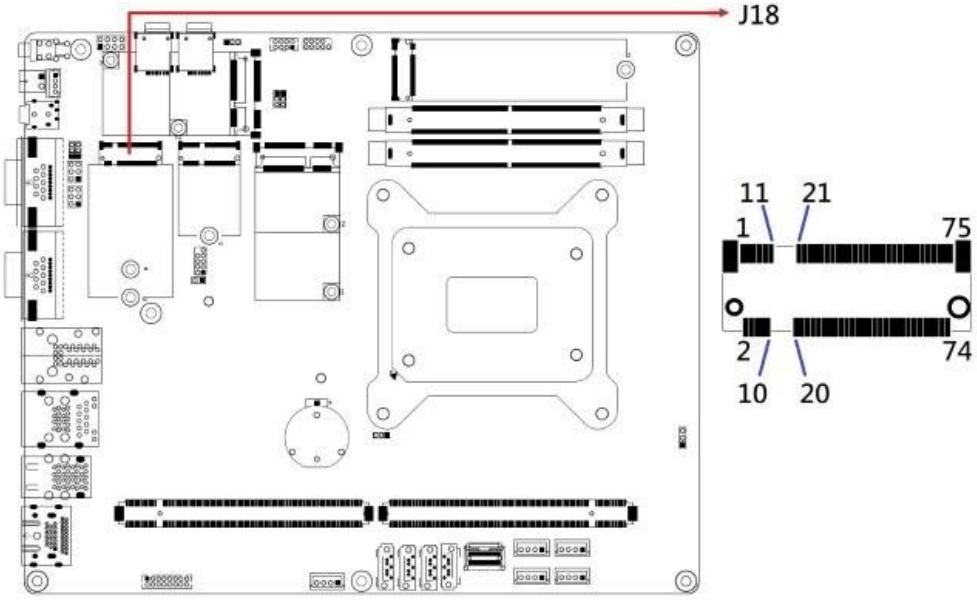
J17: VGA



Note: HRS DF11-16DP-2DSA

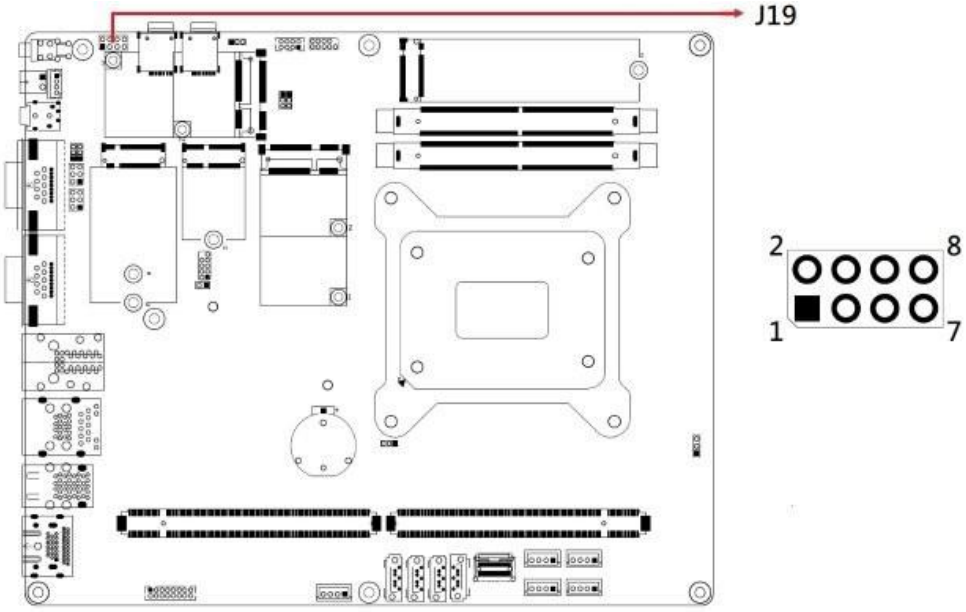
Pin	Signal	Pin	Signal
1	Red	2	+5V(0.5A)
3	Green	4	Ground
5	Blue	6	NC
7	NC	8	DDC_DATA
9	Ground	10	HSYN
11	Ground	12	VSYN
13	Ground	14	DDC_CLK
15	Ground	16	NC

J18: M.2 B-key 3052 Slot



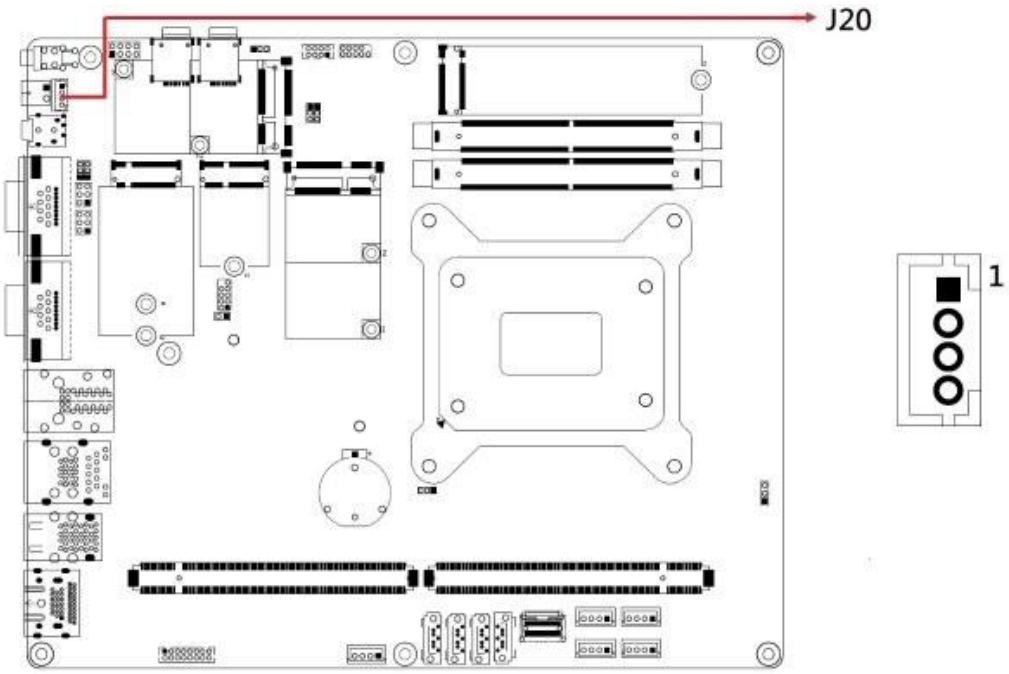
Note: J18 supports PCIe(1x) + USB3.2 for 5G Sierra EM9191 5G modules

J19: Front Panel Signals



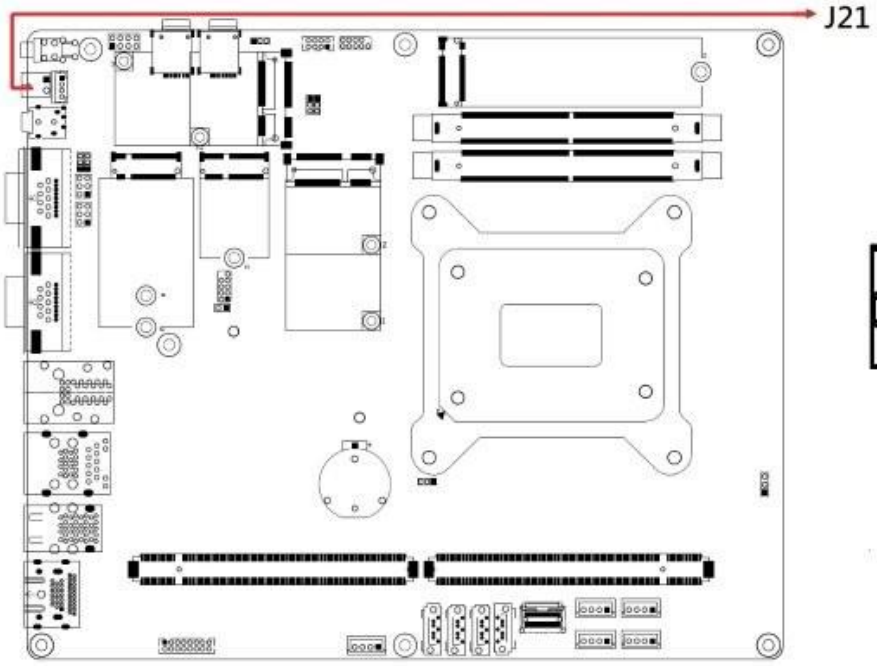
Pin	Signal Name	Pin	Signal Name
1	PWR_SW-	2	PWR_SW+
3	HDD_LED+	4	HDD_LED-
5	Ground	6	RESET+
7	PWR_LED+	8	Ground

J20: Speaker Out



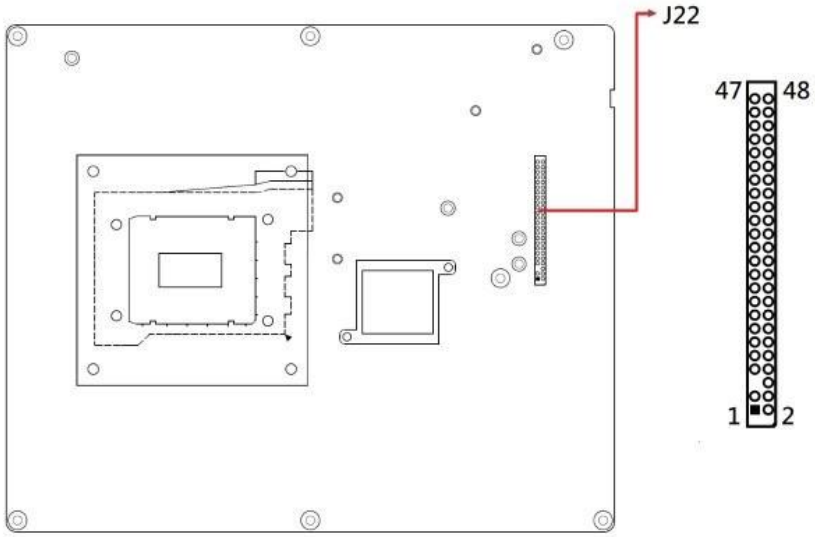
Pin	Assignment
1	Line out Left+
2	Line out Left-
3	Line out Right-
4	Line out Right+

J21: Remote Power Switch



Pin	Assignment
1	SW+
2	SW-

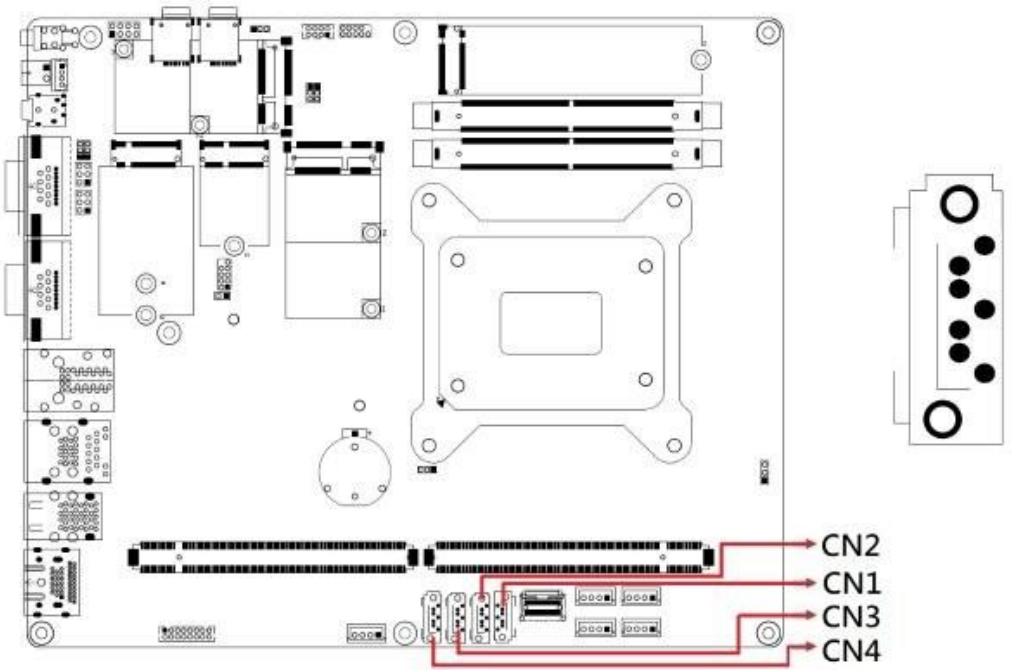
J22: Board to Board Connector



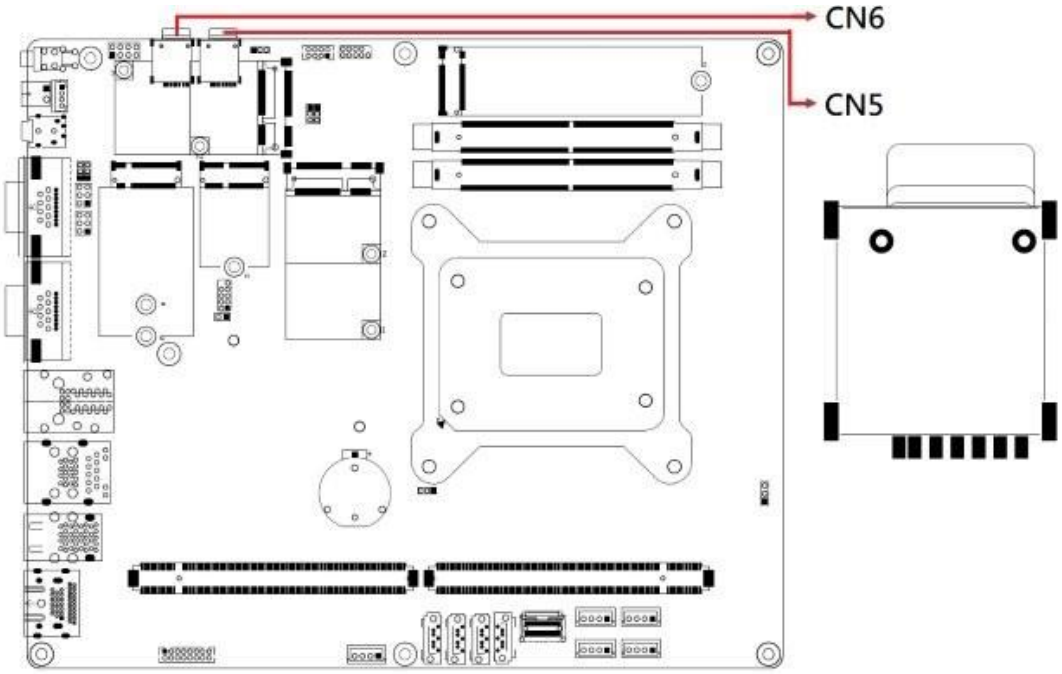
Pin	Signal	Pin	Signal
1	Ground	2	Ground
3	GPP_C21	4	RTS#E
		6	GPP_C22
7	GPP_C23	8	SIN#E
9	RTS#F	10	SOUT#E
11	SIN#F	12	DSR#E
13	SOUT#F	14	DTR#E
15	DCD#F	16	CTS#E
17	RI#F	18	RI#E
19	CTS#F	20	DCD#E
21	DTR#F	22	GPP_C18
23	DSR#F	24	GPP_C19
25	Ground	26	GPP_C20
27	GPIO70	28	Ground
29	GPIO71	30	GPIO80
31	GPIO72	32	GPIO81
33	GPIO73	34	GPIO85
35	GPIO74	36	GPIO82
37	GPIO75	38	GPIO86
39	GPIO76	40	GPIO83
41	GPIO77	42	GPIO87
43	+5V	44	GPIO84
45	+5V	46	Ground
47	+5V	48	Ground

Note: For IDA100

CN1, CN2, CN3, CN4: SATA III 7-pin Connector

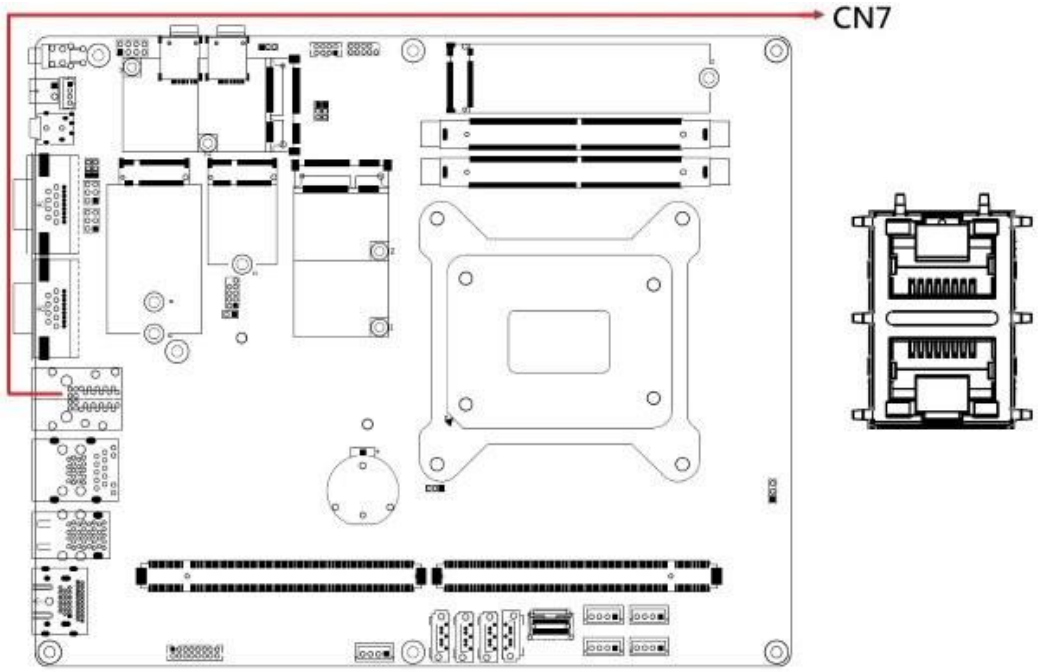


CN5, CN6: Nano SIM Card 2, Nano SIM Card 1 Slots

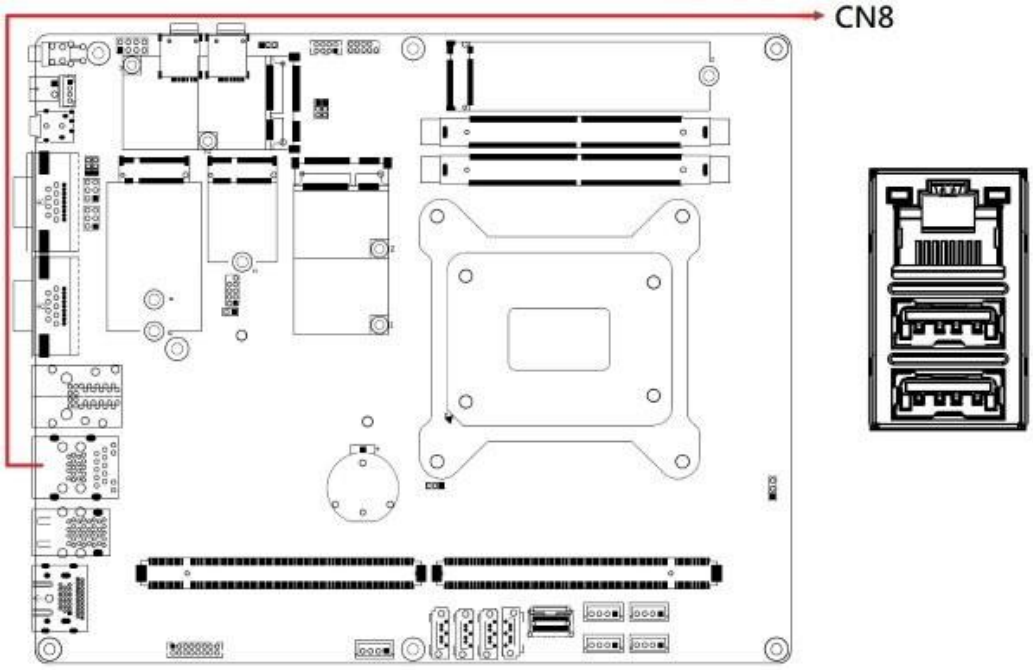


Note: Nano SIM card 2 is shared for CN5 and J18

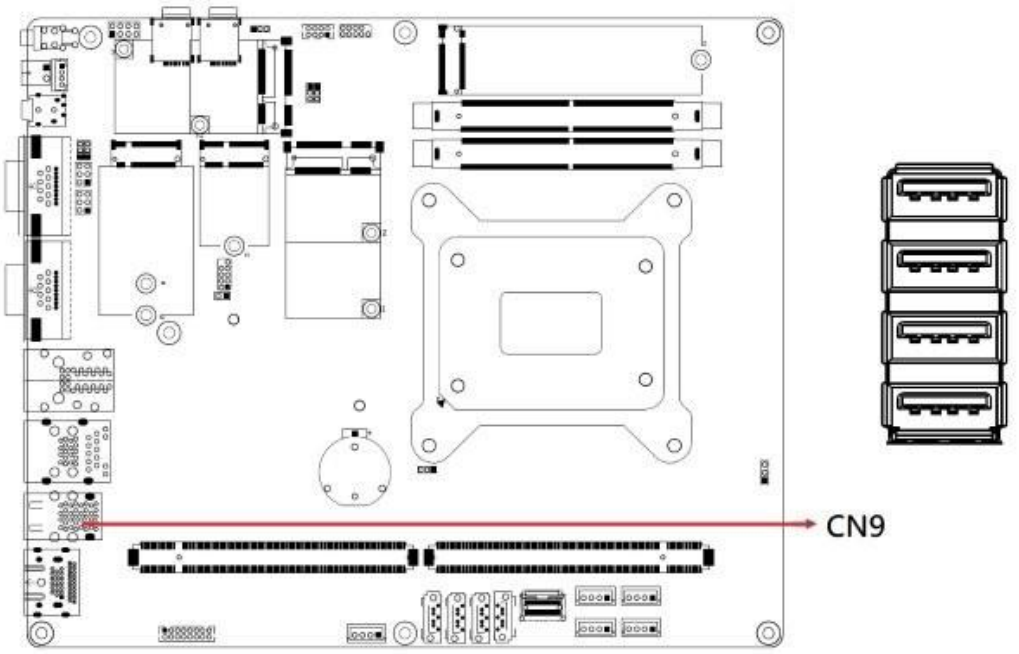
CN7: 2x 2.5 Gigabit LAN (Intel I226-IT) Stack Connector



CN8: 2.5 Gigabit LAN (Intel I226-LM) + USB3.2 Gen 2

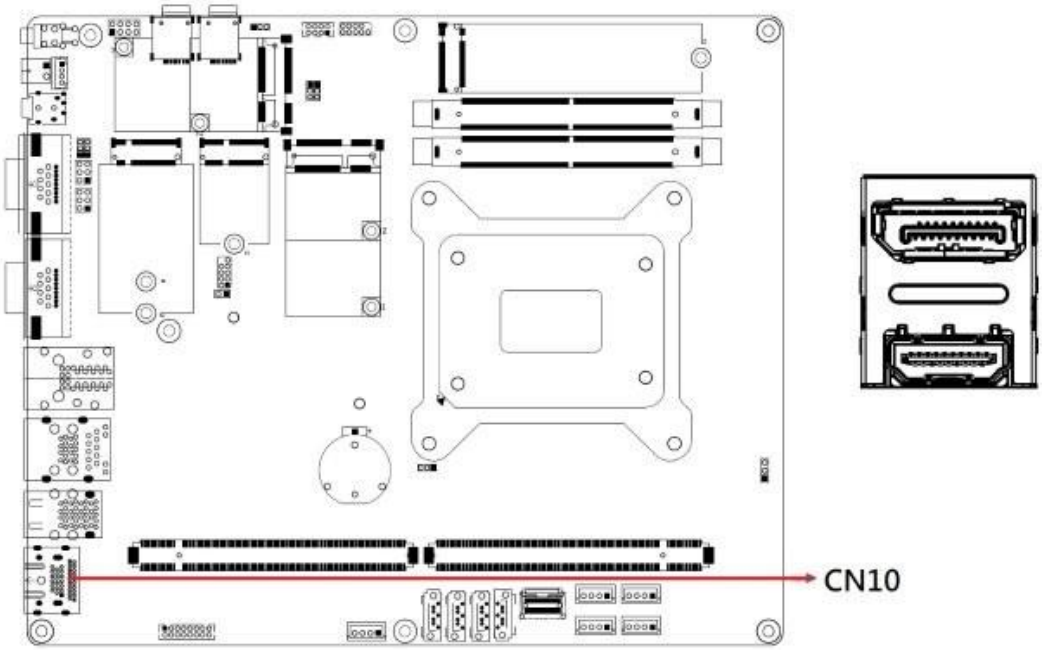


CN9: 4x USB3.2 Gen 1 Type-A

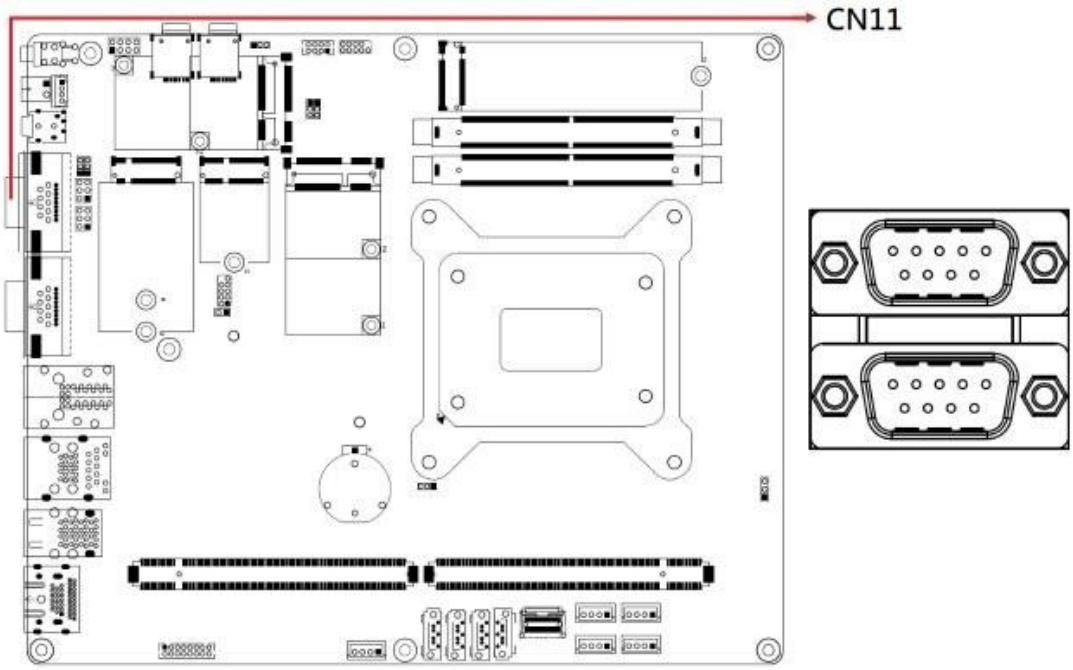


Note: The bottom port supports PDPC by software.

CN10: Display Port(Top) + HDMI (Bottom)



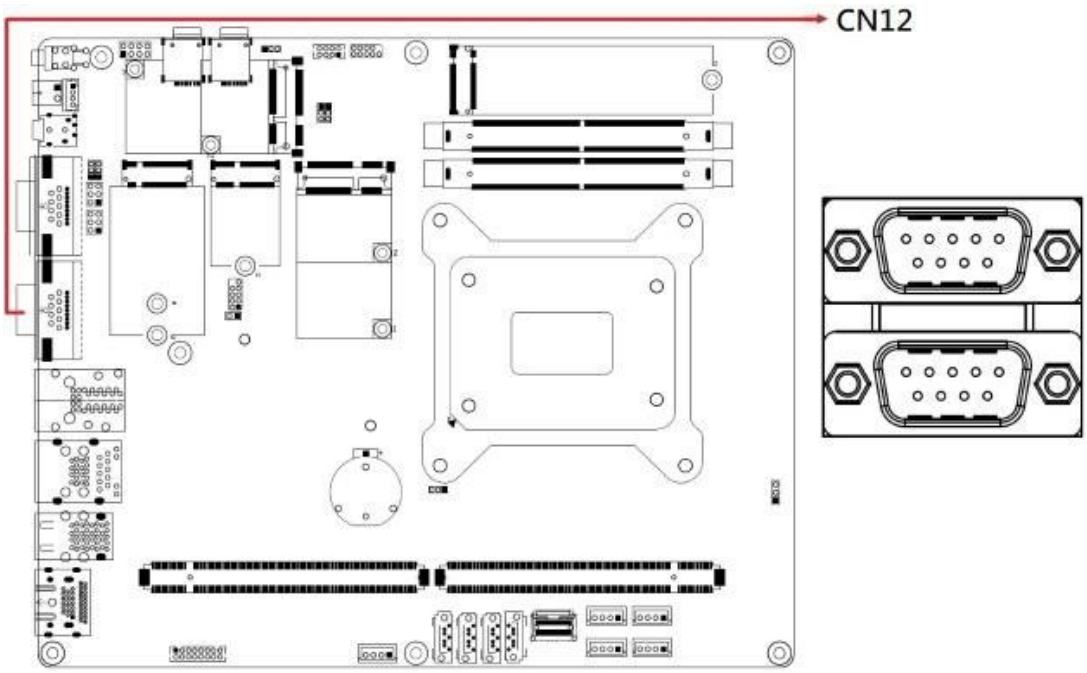
CN11: COM1/COM2 Ports



RS-232/422/485 configurable in BIOS.

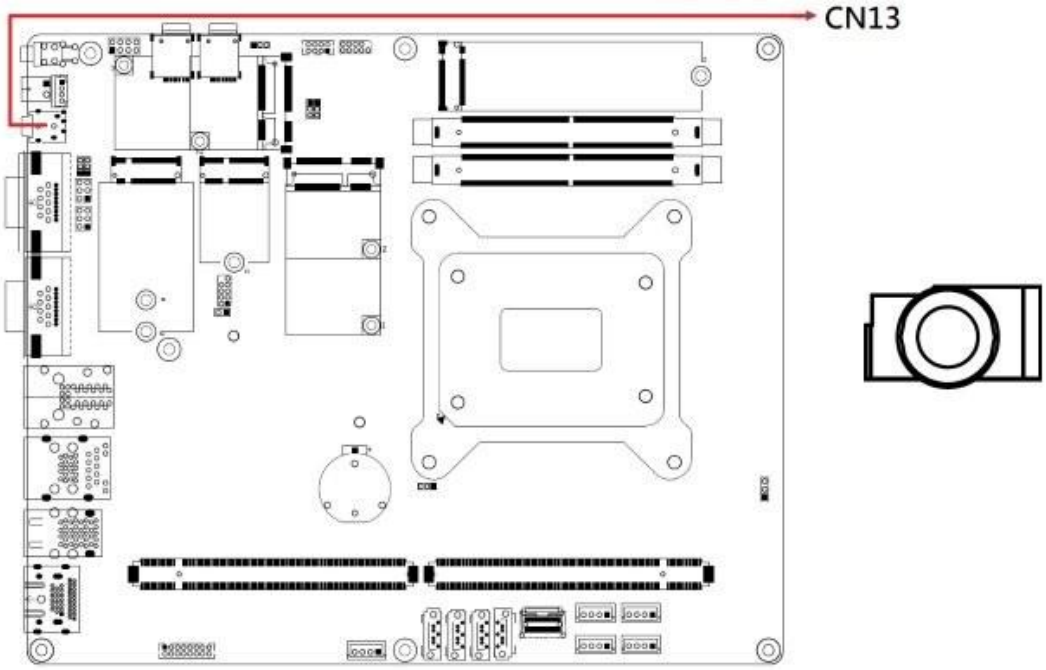
Pin	Signal Name		
	RS-232	RS-422	RS-485
1	DCD	TX-	DATA-
2	RX	TX+	DATA+
3	TX	RX+	NC
4	DTR	RX-	NC
5	Ground	NC	NC
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

CN12: COM3 & COM4 RS-232 Ports

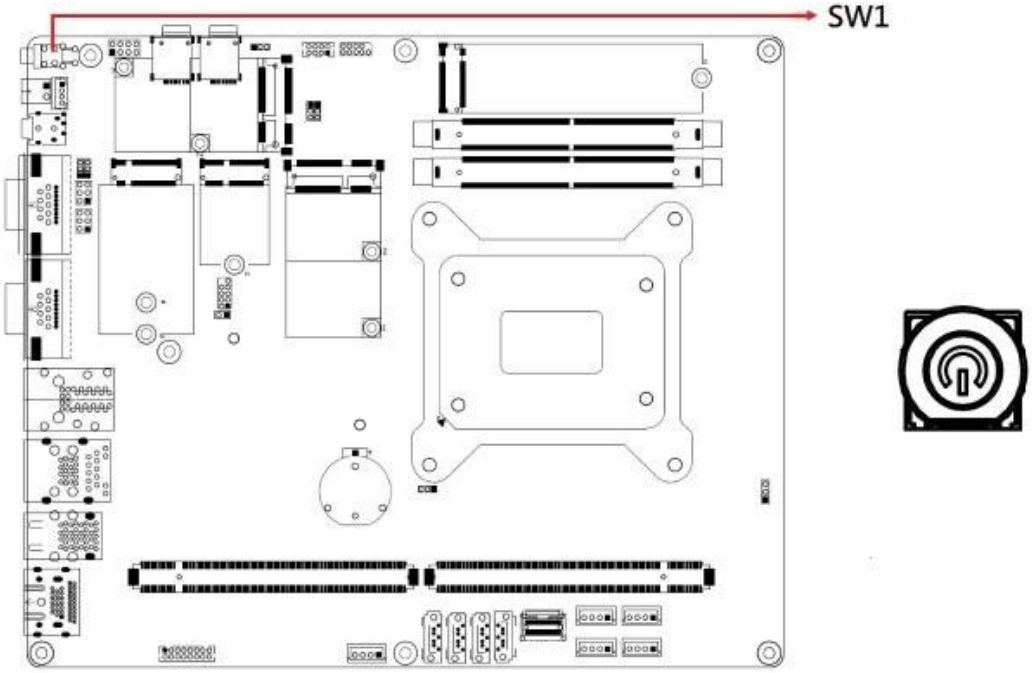


Pin	Signal Name	Pin	Signal Name
1	DCD, Data carrier detect	6	DSR, Data set ready
2	RXD, Receive data	7	RTS, Request to send
3	TXD, Transmit data	8	CTS, Clear to send
4	DTR, Data terminal ready	9	RI, Ring indicator
5	Ground		

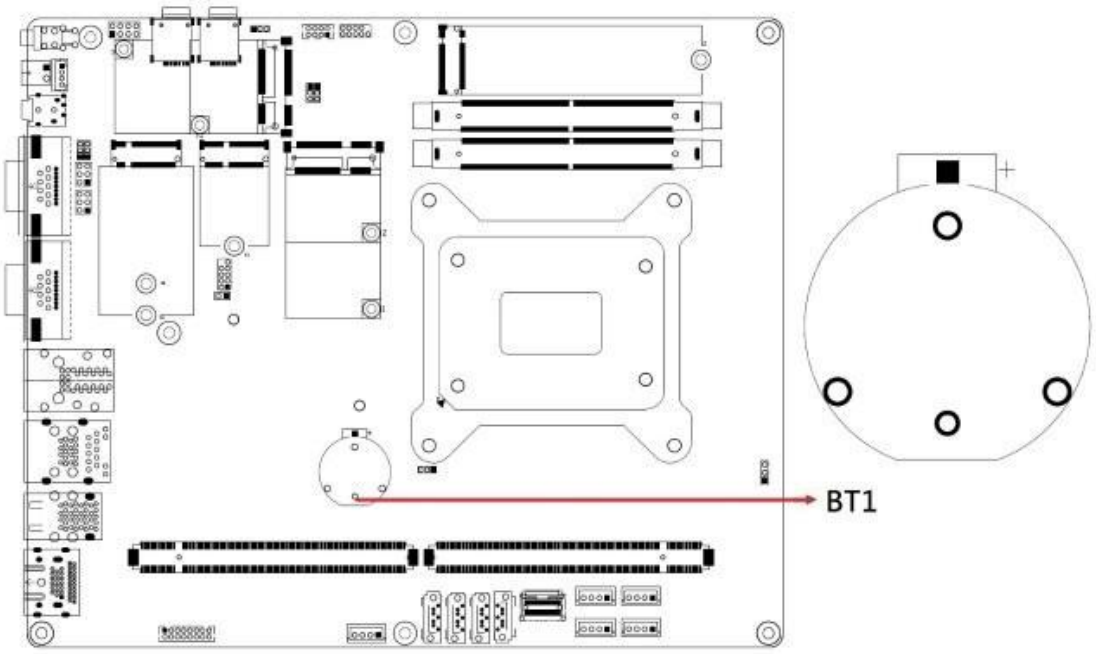
CN13: Audio Jack (Line out + MIC IN)



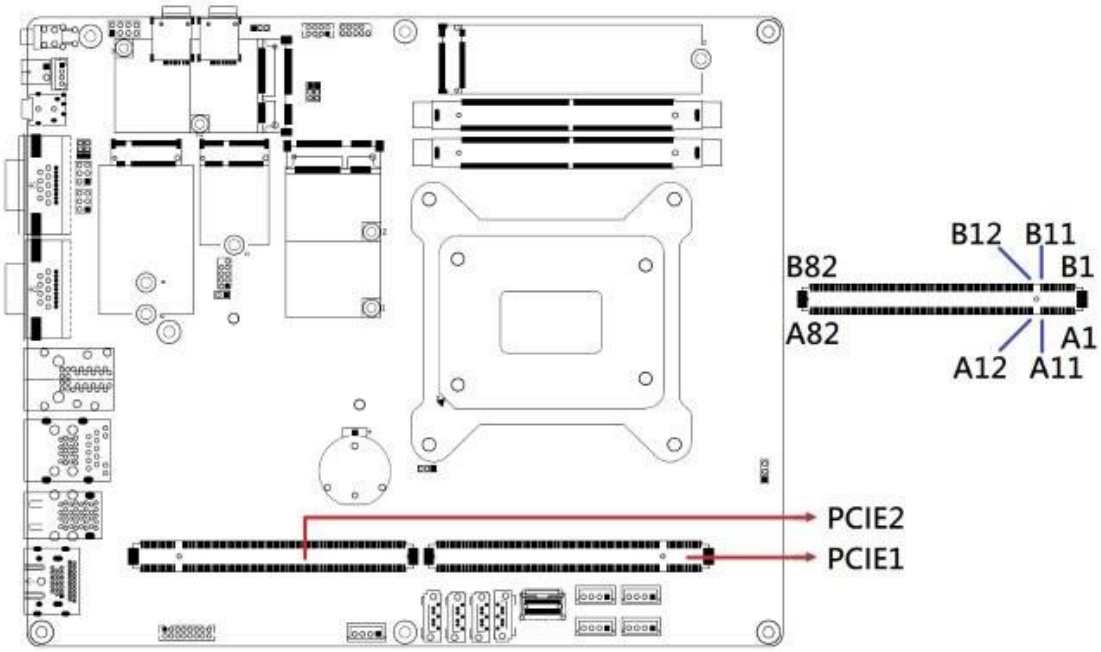
SW1: Power Button



BT1: Coin battery Socket



PCIE1, PCIE2: Non-Standard High-speed Board to Board Slots



Note: For IPA100

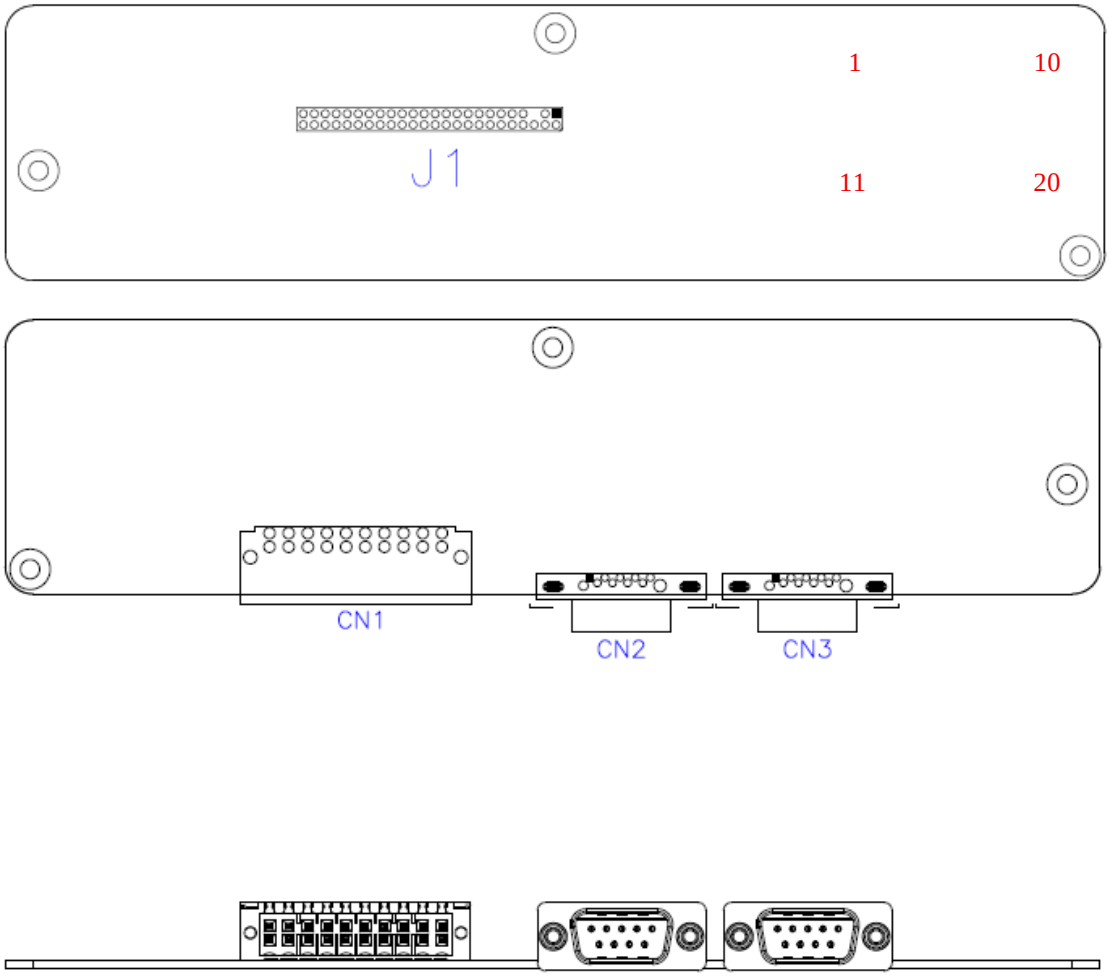
2.3 I/O Expansion Board (IDA-100)

The IDA-100 is an I/O expansion and isolation board designed to extend the AES100 system's connectivity. It provides isolated digital input and output channels as well as additional serial communication ports supporting RS-232, RS-422, and RS-485 standards.

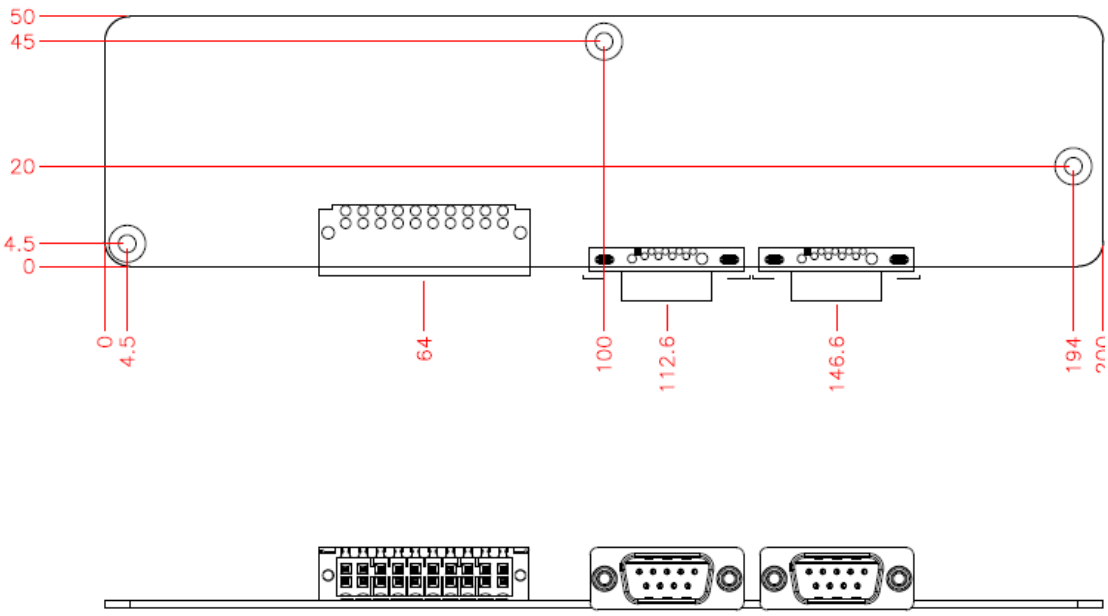
The IDA-100 connects to the MBA100 mainboard through a high-speed board-to-board connector, enabling reliable signal transmission while maintaining electrical isolation for industrial applications.

This design improves system robustness by protecting the mainboard from electrical noise, voltage spikes, and ground potential differences commonly found in industrial and vehicle environments.

Board Layout



Board Dimensions

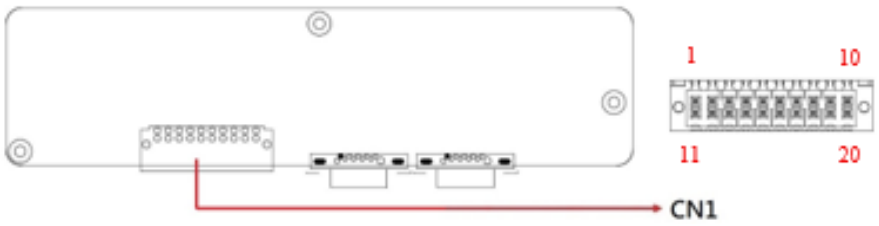


Jumper and Connector Quick Reference

Function (*IDA-100*)	Connector
Isolation 8 DI + 8 DO	CN1
COM A / COM B RS-232 / RS-422 / RS-485	CN2, CN3
Board-to-Board Connector	J1

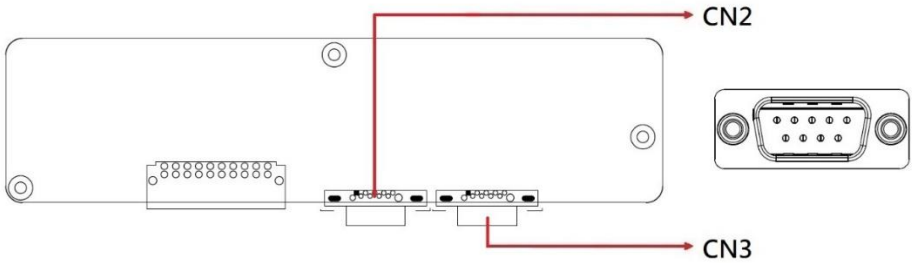
IDA-100 Pin Definitions

CN1: Isolation 8 DI+ 8 DO



Pin	Signal	Pin	Signal
1	DI0	11	DO0
2	DI1	12	DO1
3	DI2	13	DO2
4	DI3	14	DO3
5	DI4	15	DO4
6	DI5	16	DO5
7	DI6	17	DO6
8	DI7	18	DO7
9	NC	19	COM+
10	COM-	20	COM-

CN2, CN3: COM A/COM B RS-232/422/485



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	NC	NC
6	DSR	NC	NC
7	RTS	NC	NC
8	CTS	NC	NC
9	RI	NC	NC

J1: Board to Board Connector

Pin	Signal	Pin	Signal
1	Ground	2	Ground
3	GPP_C21	4	RTS#E
		6	GPP_C22
7	GPP_C23	8	SIN#E
9	RTS#F	10	SOUT#E
11	SIN#F	12	DSR#E
13	SOUT#F	14	DTR#E
15	DCD#F	16	CTS#E
17	RI#F	18	RI#E
19	CTS#F	20	DCD#E
21	DTR#F	22	GPP_C18
23	DSR#F	24	GPP_C19
25	Ground	26	GPP_C20
27	GPIO70	28	Ground
29	GPIO71	30	GPIO80
31	GPIO72	32	GPIO81
33	GPIO73	34	GPIO85
35	GPIO74	36	GPIO82
37	GPIO75	38	GPIO86
39	GPIO76	40	GPIO83
41	GPIO77	42	GPIO87
43	+5V	44	GPIO84
45	+5V	46	Ground
47	+5V	48	Ground

Note: Connected to MBA100 J22

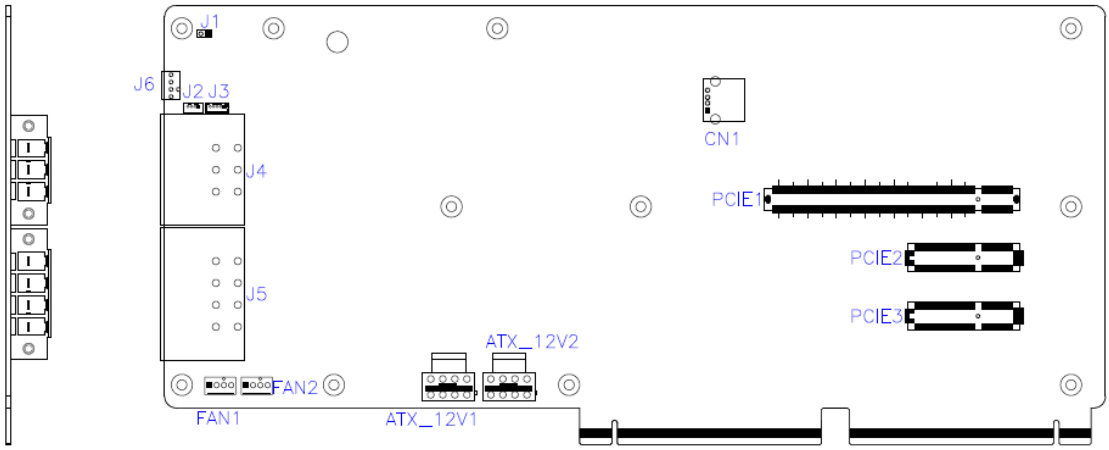
2.4 Power and Ignition Board (IPA-100)

The IPA-100 is a power and ignition control board designed to manage system power for the AES100 platform. It supports wide-range DC power input and provides regulated power outputs to the mainboard and system components.

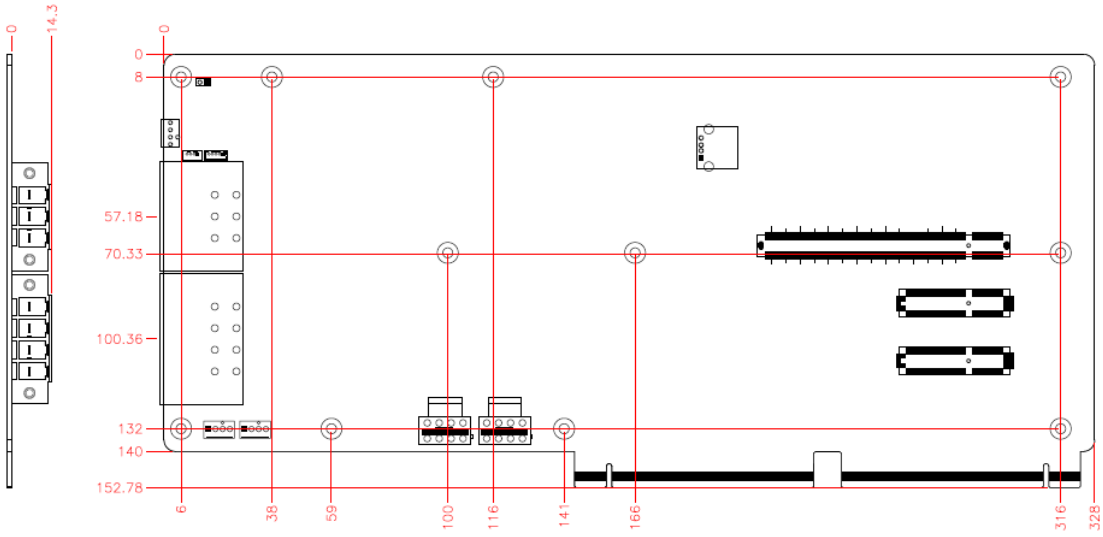
The IPA-100 connects to the MBA100 mainboard through a board-to-board interface, enabling stable power delivery and coordinated power control across the system.

This design supports ignition-based power on and off control, power delay, and power protection features, ensuring reliable operation in vehicle and industrial environments.

Board Layout



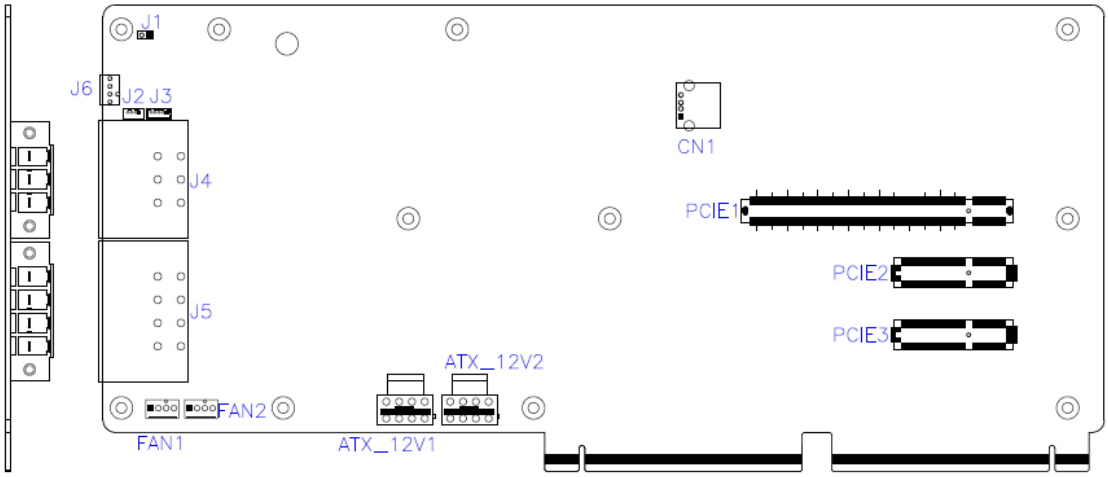
Board Dimensions



Jumper and Connector Quick Reference

Function (*IPA-100*)	Connector
Power Input (Ground)	J4
Power Input (Positive)	J5
IGN Mode Selection	J6
Power Output	ATX1_12V1
Power Output	ATX1_12V2
USB 2.0 Type-A	CN1
System Fan / CPU Fan	FAN1, FAN2
PCI Express x16 Slot	PCIE1
PCI Express x4 Slot	PCIE2, PCIE3

IPA-100 Pin Definitions



J1, J2, J3: Factory Use Only

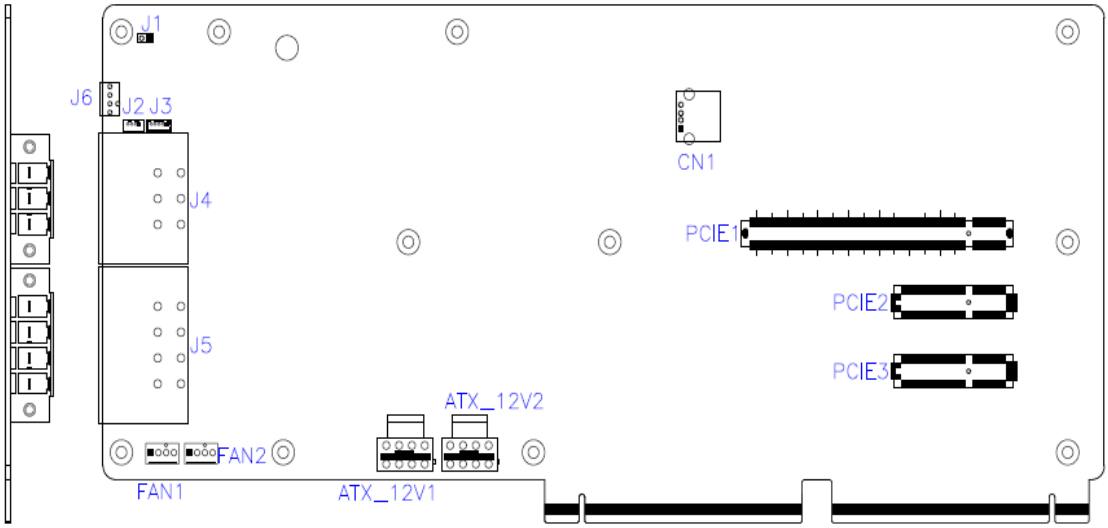
J4: Power Input (Ground)

Pin	Assignment
1	Ground
2	Ground
3	Ground

J5: Power Input (Positive)

Pin	Assignment
1	DC IN+
2	DC IN+
3	DC IN+
4	IGN

Note: Marked in Red is IGN(PIN 4)

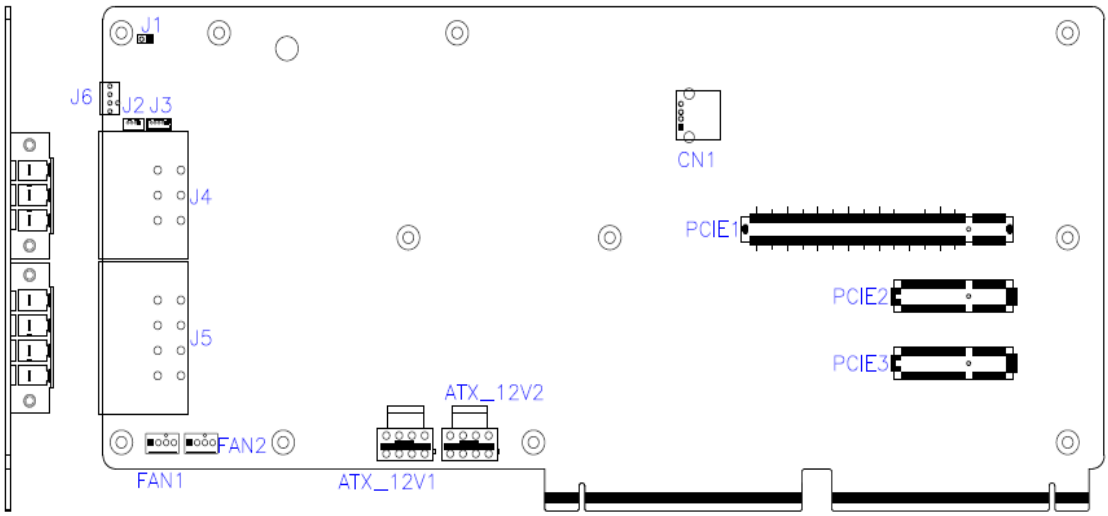


J6: IGN Mode Selection

Default: Mode 0
Mode selection from 0 to F
This is power on/off delay control
Note: J5 pin-4 should be connected DC 8V~48V (Not limited at Mode 0)

Mode	Power-on Delay	Power-off Delay	Hard-off Timeout
0	N/A	N/A	N/A
1	10 Seconds	10 Seconds	10 Minutes
2	10 Seconds	30 Seconds	10 Minutes
3	10 Seconds	1 Minute	10 Minutes
4	10 Seconds	5 Minutes	10 Minutes
5	20 Seconds	10 Seconds	10 Minutes
6	20 Seconds	30 Seconds	10 Minutes
7	20 Seconds	1 Minute	10 Minutes
8	20 Seconds	5 Minutes	10 Minutes
9	30 Seconds	30 Seconds	10 Minutes
A	30 Seconds	1 Minute	10 Minutes
B	30 Seconds	5 Minutes	10 Minutes
C	5 Minutes	10 Minutes	10 Minutes
D	5 Minutes	30 Minutes	10 Minutes
E	10 Minutes	10 Minutes	10 Minutes
F	10 Minutes	30 Minutes	10 Minutes

The IGN (Ignition) function allows the system to power on/off based on vehicle ignition status. When enabled, the system follows programmable power-on delay, power-off delay, and hard-off timeout settings.



ATX1_12V1: Power output

Pin	Signal	Pin	Signal
1	Ground	5	+12V
2	Ground	6	+12V
3	Ground	7	+12V
4	Ground	8	+12V

ATX1_12V2: Power output

Pin	Signal	Pin	Signal
1	Ground	5	+12V_SENSE 0
2	Ground	6	+12V_SENSE 1
3	Ground	7	+12V
4	Ground	8	+12V

CN1: USB2.0 Type A

FAN1, FAN2: System Fan, CPU Fan

PCIE1: PCIEx16 Slot

PCIE2, PCIE3: PCIEx4 Slot

Chapter 3
Drivers Installation

This chapter introduces installation of the following drivers:

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

3.1 Introduction

This section describes the installation procedures for software and drivers.

Note: After installing your Windows operating system, you must install the Intel® Chipset Software Installation Utility first before proceeding with the 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 the chipset components. Follow the instructions below to complete the installation.

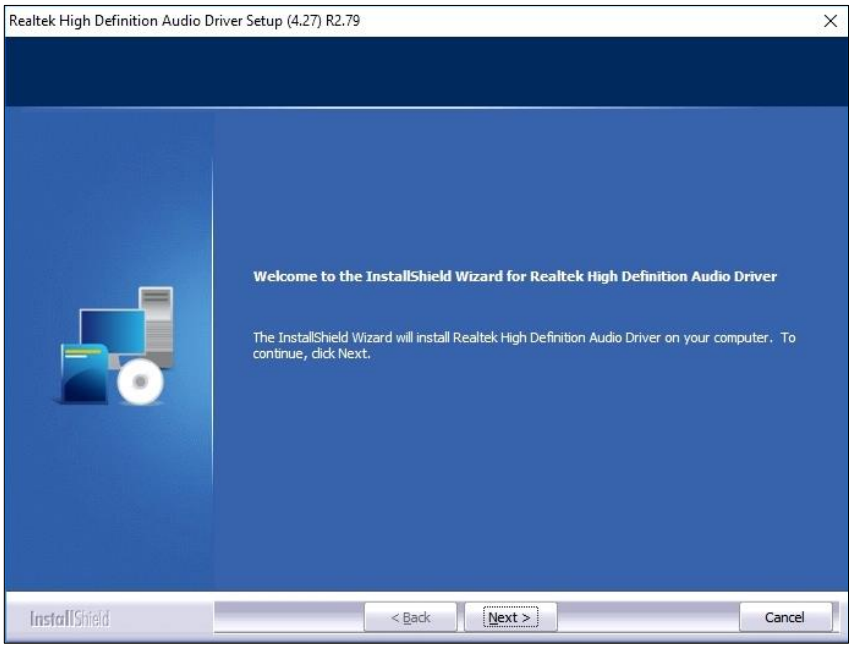
1. Run the **Setup.exe** file.

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

3. Accept the license agreement and proceed with the installation process.
4. When the driver is completely installed, restart the computer for changes to take effect.

3.3 HD Audio Driver Installation

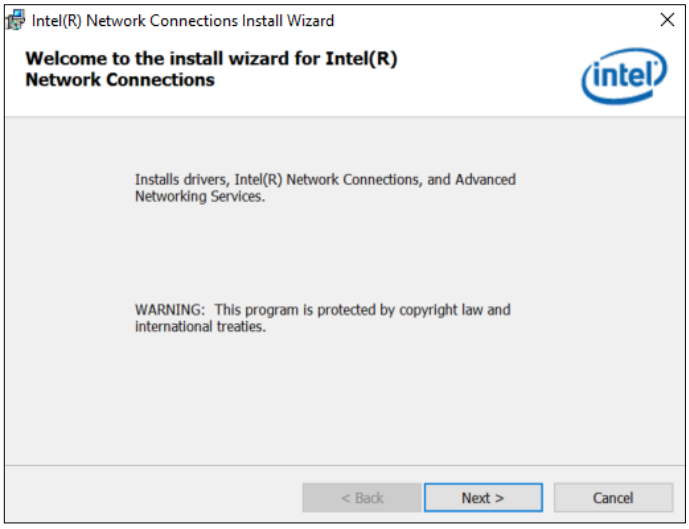
1. Run the **Setup.exe** file.
2. On the Welcome screen of the InstallShield Wizard, click Next.



3. When the driver is completely installed, restart the computer for changes to take effect.

3.4 LAN Driver Installation

1. Run the **Setup.exe** file.
2. On the Welcome screen of the InstallShield Wizard, click Next.

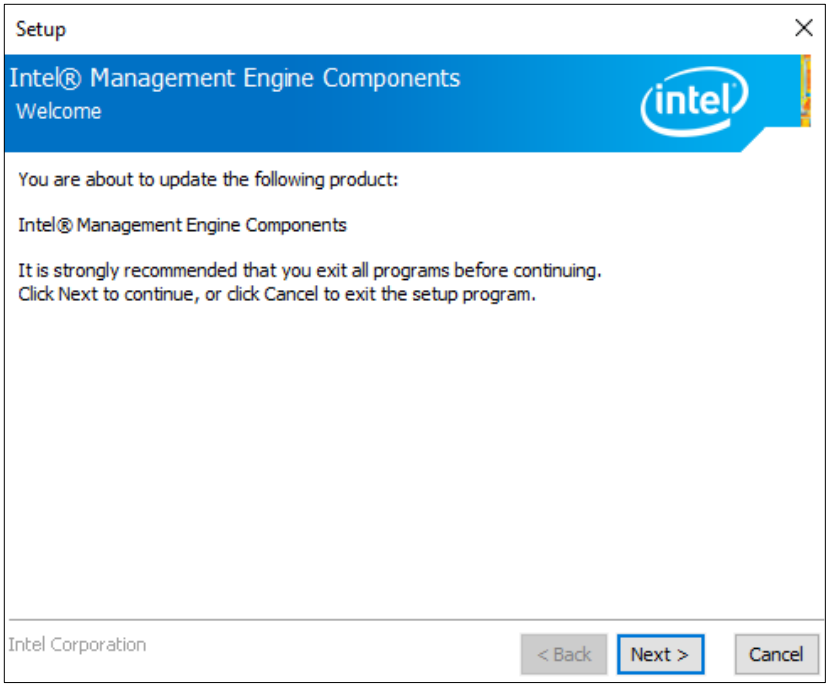


3. Accept the license agreement and click Next to continue.

   On the *Setup Options* screen, tick the checkbox to select the desired driver(s) and click **Next** for installation. When the driver is completely installed, restart the computer for changes to take effect.

3.5 Intel® Management Engine Components Drivers Installation

1. Run the **Setup.exe** file.
2. When the *Welcome* screen appears, click **Next**.



3. Accept the license agreement and click **Next** for installation.
4. The driver has been completely installed. Restart the computer for changes to take effect.

Chapter 4
BIOS Setup

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. 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.

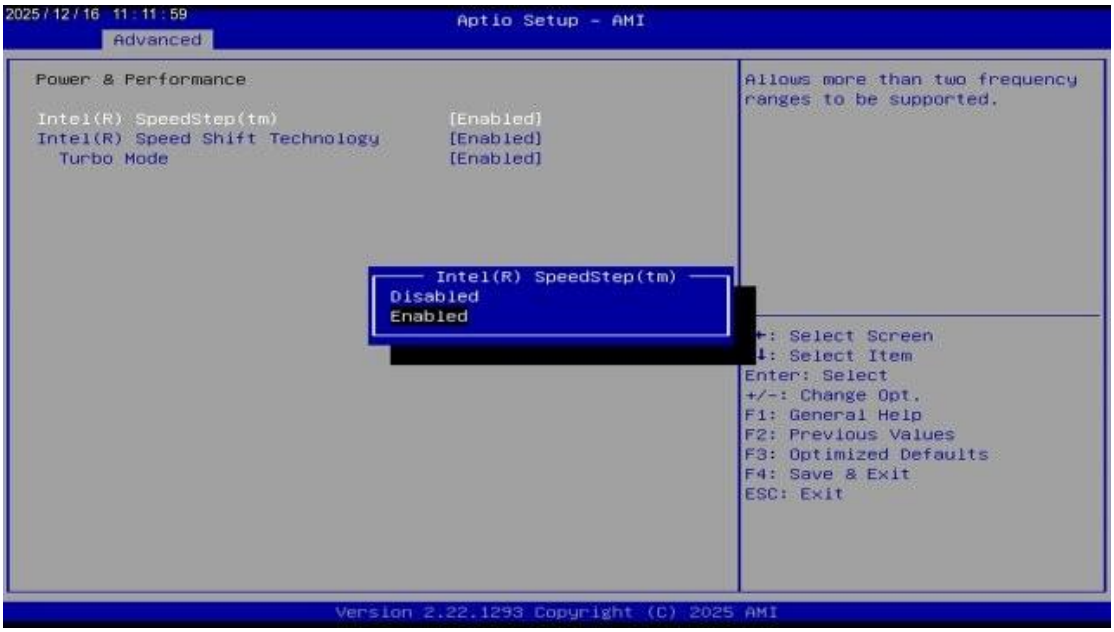
4.4.1 Connectivity Configuration

BIOS Setting	Description
BT Audio Offload	This is an option to enable/disable BT audio offload which enables audio input from BT device to the audio DSP and enables power efficient audio output to BT device.
RFI Mitigation	This is an option intended to enable/disable DDR-RFIM feature for connectivity. This RFI mitigation feature may result in temporary slowdown of the DDR speed.
DLVR RFI Mitigation	This is an option intended to enable /disable DLVR RFIM. This option is only valid when global DLVR is enabled.
Preboot BLE	This will be used to enable Preboot Bluetooth function
Discrete Bluetooth Interface	SerialIo UART0 needs to be enabled to select BT interface.
BT Tile Mode	Enable/Disable Tile
Advanced settings	Configure ACPI objects for wireless devices.
WWAN Configuration	Configure WWAN related options
WWAN Device	Select the M.2 WWAN device options to enable 4G – 7360/7560 (Intel), 5G – MB0 (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 P-cores are looked at together. When both are (o,o), 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 (o,o), Pcode will enable all cores.
Hyper-Threading	Enable/Disable Hyper-Threading
Legacy Game Compatibility	When enabled, pressing the scroll lock key will toggle the Efficient-cores between being parked when Scroll Lock LED is on and un-parked when LED is off.

4.4.3 Power & Performance



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

4.4.4 PCH-FW Configuration

4.4.5 Trusted Computing

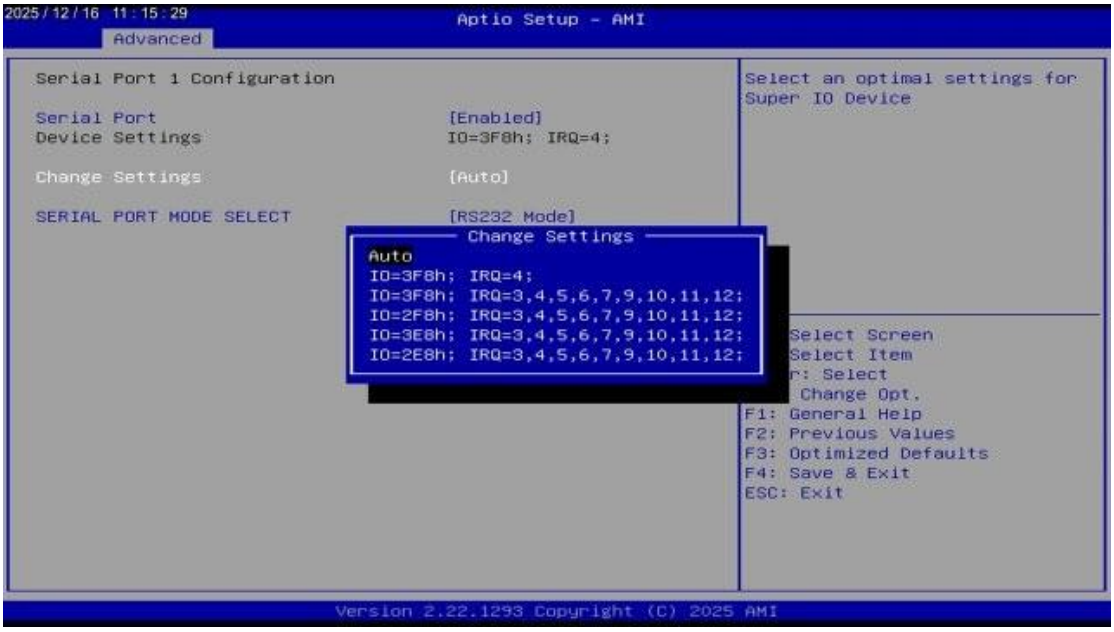
BIOS Setting	Description
Security Device Support	Enables / Disables BIOS support for security device. OS will not show security device. TCG EFI protocol and INT1A interface will not be available.
SHA256 PCR Bank	Options: Enabled / Disabled
SHA384 PCR Bank	Options: Enabled / Disabled
Pending operation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

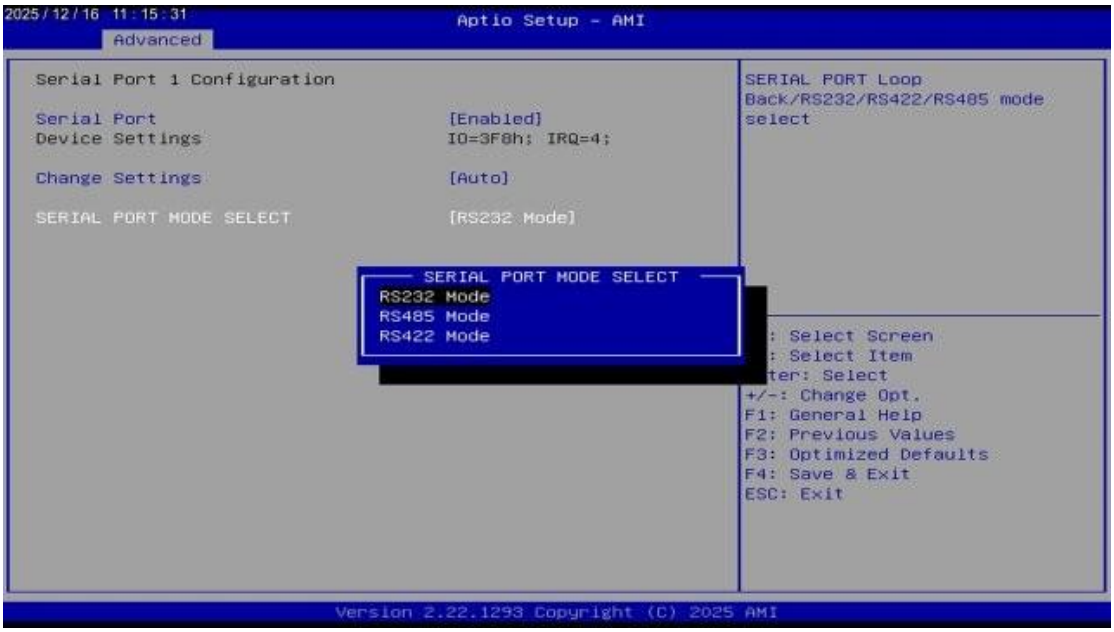
4.4.6 ACPI Settings

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 the SUSPEND button is pressed.

4.4.8 F81966 Super IO Configuration

BIOS Setting	Description
Serial Port 1/2/3/4/5/6 Configuration	Sets parameters of Serial Port 1/2/3/4/5/6


2025/12/16 11:15:29
Aptio Setup - AMI
Advanced
Serial Port 1 Configuration
Serial Port [Enabled]
Device Settings IO=3F8h; IRQ=4;
Change Settings [Auto]
SERIAL PORT MODE SELECT [RS232 Mode]
Change Settings
Auto
IO=3F8h; IRQ=4;
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;
IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;
Select an optimal settings for Super IO Device
Select Screen
Select Item
r: Select
Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1293 Copyright (C) 2025 AMI


2025/12/16 11:15:31
Aptio Setup - AMI
Advanced
Serial Port 1 Configuration
Serial Port [Enabled]
Device Settings IO=3F8h; IRQ=4;
Change Settings [Auto]
SERIAL PORT MODE SELECT [RS232 Mode]
SERIAL PORT MODE SELECT
RS232 Mode
RS485 Mode
RS422 Mode
SERIAL PORT Loop Back/RS232/RS422/RS485 mode select
: Select Screen
: Select Item
ter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.22.1293 Copyright (C) 2025 AMI

4.4.9 Hardware Monitor

BIOS Setting	Description
Smart Fan Function	Options: Disabled, 50C, 60C, 70C, 80C, and 90C.
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.

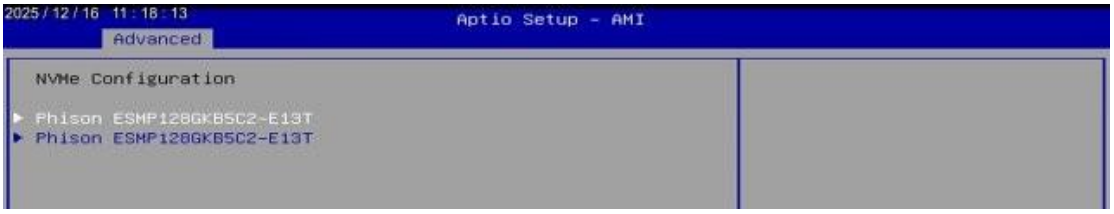
4.4.10 USB Configuration

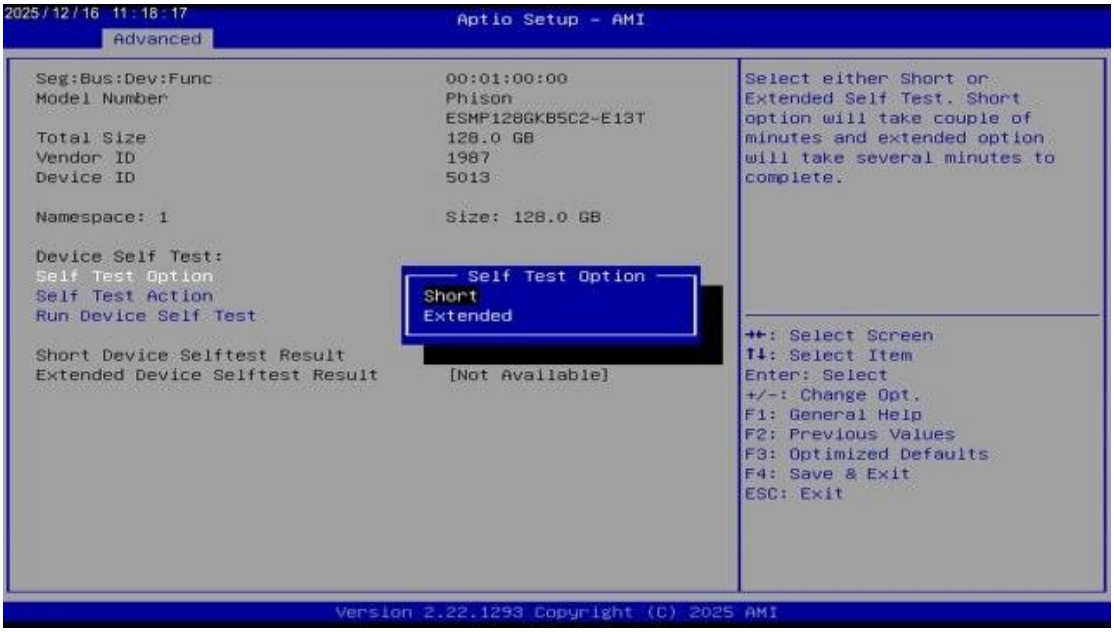
BIOS Setting	Description
Legacy USB Support	• **Enabled** enables Legacy USB support. • **Auto** disables legacy support if there is no USB device connected. • **Disabled** keeps USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. 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	USB mass storage device Start Unit command time-out (10/20/30/40 sec).
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.

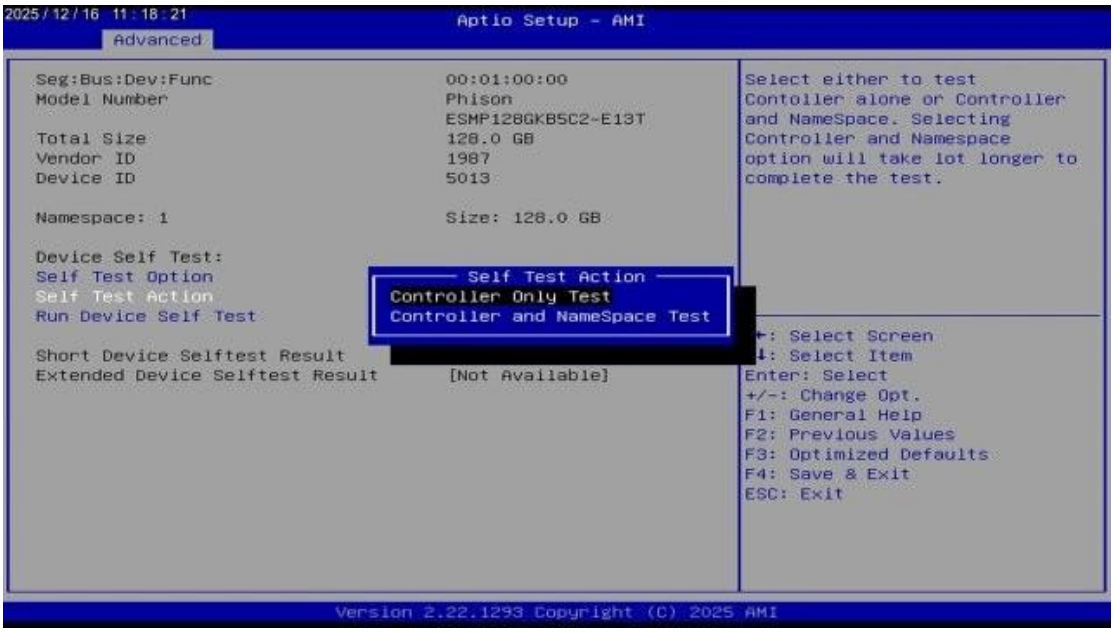
4.4.11 Network Stack Configuration

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

4.4.12 NVME Configuration

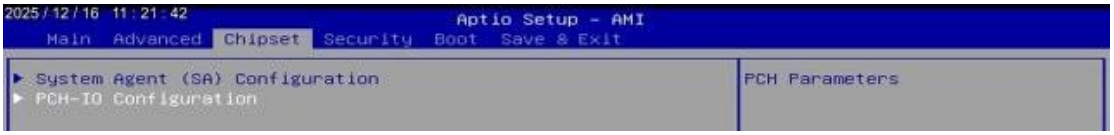




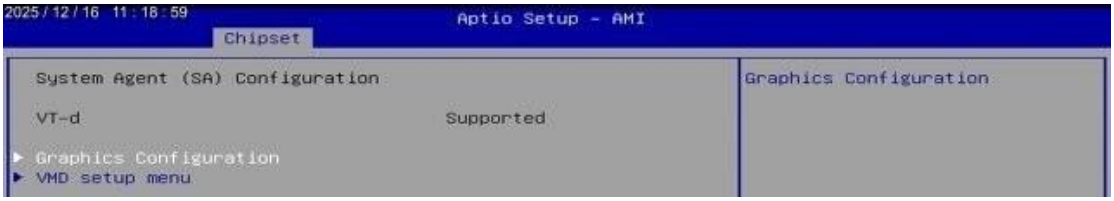


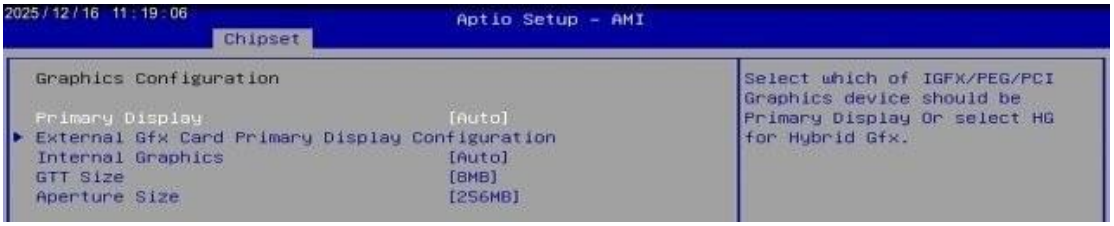
4.5 Chipset Settings

4.5.1 System Agent (SA) Configuration



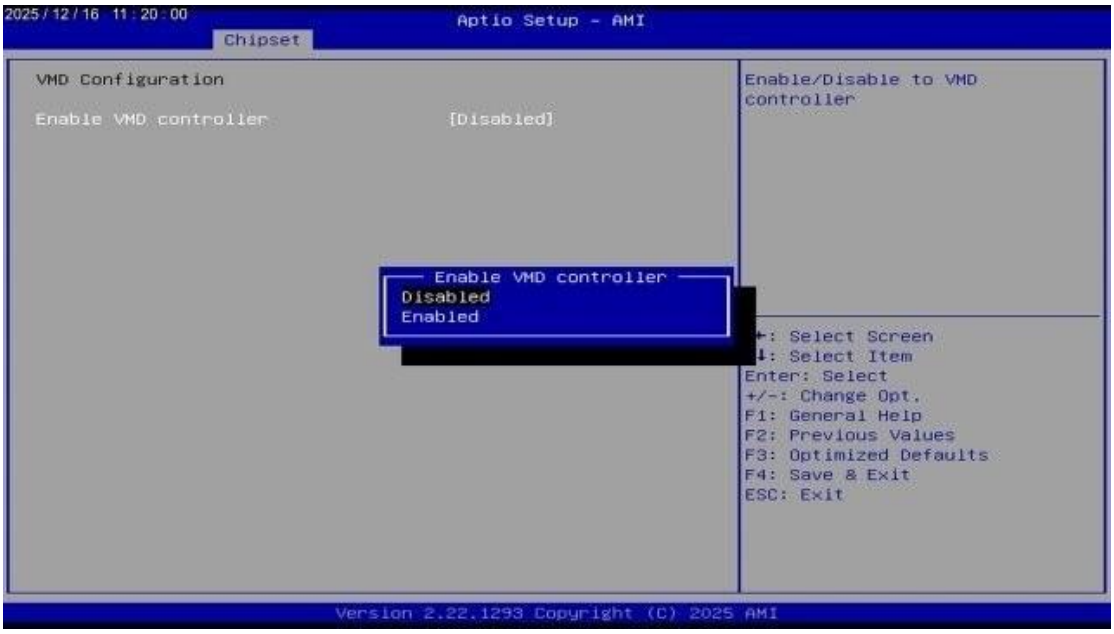
4.5.1.1. Graphics Configuration:



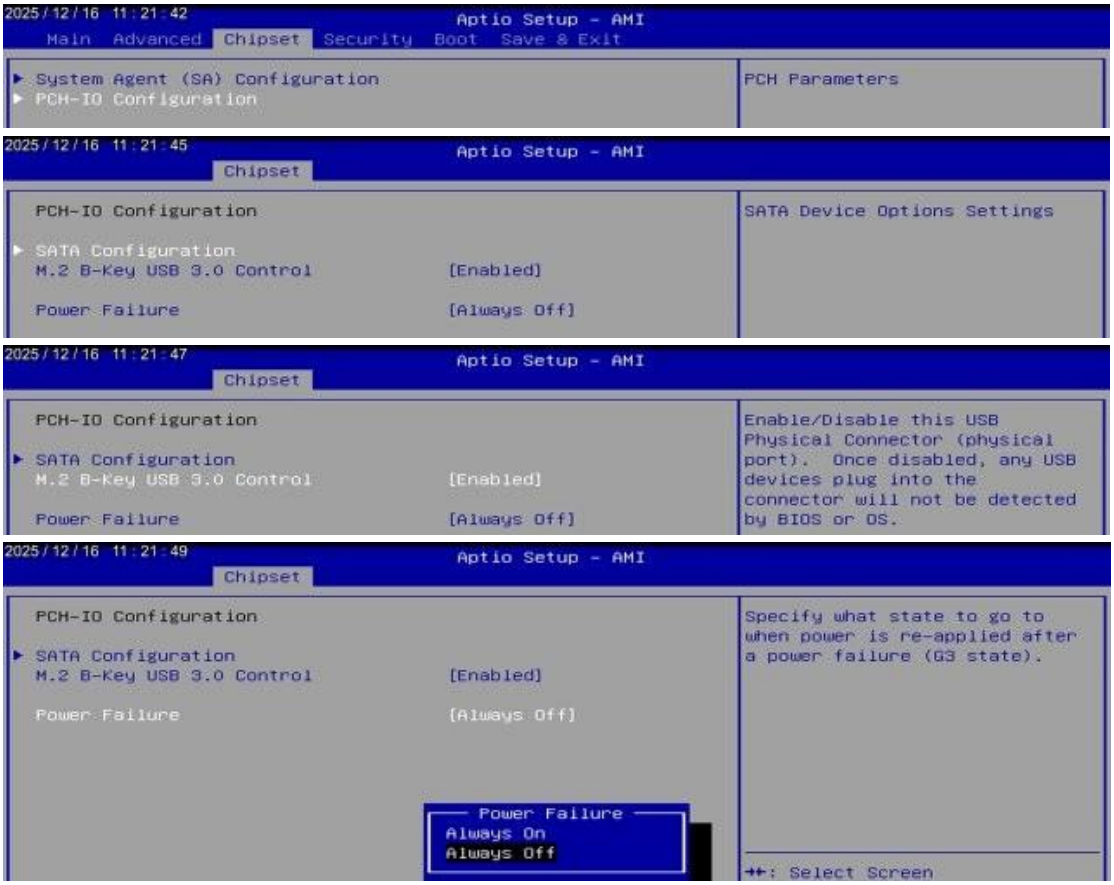


BIOS Setting	Description
Primary Display	Select which of the IGFX PEG PCI Graphics device should be Primary Display or select HG for Hybrid Gfx.
External Gfx Card Primary Display Configuration	Keep IGFX enabled based on setup options. **Primary PEG:** Select PEG0/PEG1/PEG2/PEG3 Graphics device should be Primary PEG. **Primary PCIE:** Select Auto/PCIE1/PCIE2/PCIE3/PCIE4/PCIE5/PCIE6/PCIE7 or D28:F0/F1/F2/F3/F4/F5/F6/F7, PCIE8/PCIE9/PCIE10/PCIE11/PCIE12/PCIE13/PCIE14/PCIE15 or D29:F0/F1/F2/F3/F4/F5/F6/F7, PCIE16/PCIE17/PCIE18/PCIE19 or D27:F0/F1/F2/F3, Graphics device should be Primary PCIE.
Internal Graphics	Keep IGFX enabled based on setup options.
GTT Size	Select the GTT Size (2MB / 4MB / 8MB).
Aperture Size	Select the Aperture Size (128MB/256MB/ 512MB/1024MB). Note: Above 4GB MMIO BIOS assignment is automatically enabled when selecting > 2048MB aperture. To use this feature, please disable CSM Support.
DVMT Pre-Allocated	Select DVMT 5.0 Pre-Allocated (Fixed) Graphics Memory size used by the Internal Graphics Device.
VT-d	Enable/Disable VT-d capability

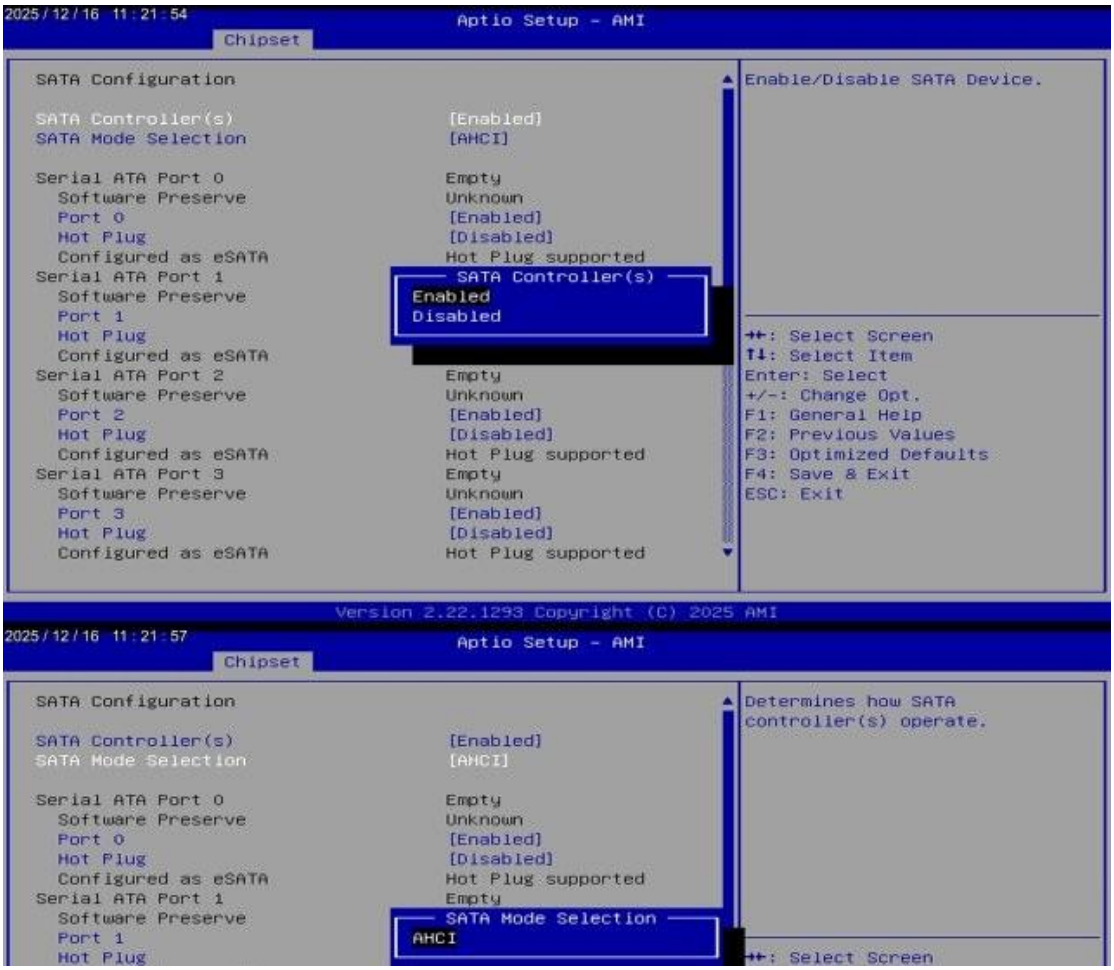
4.5.1.2. VMD Setup Menu:



4.5.2 PCH-IO Configuration

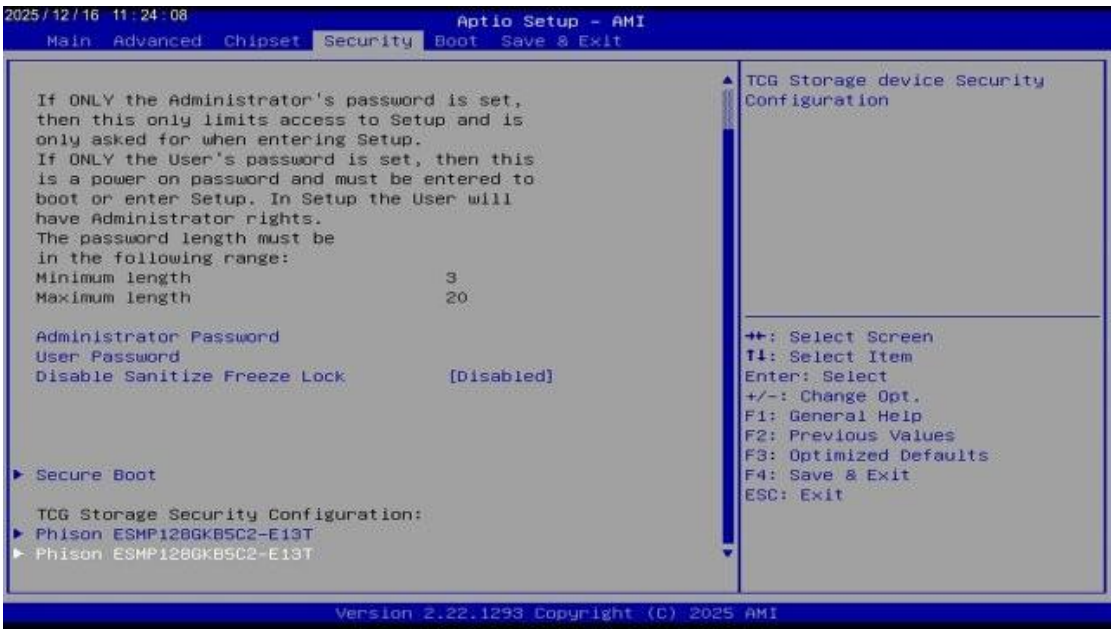


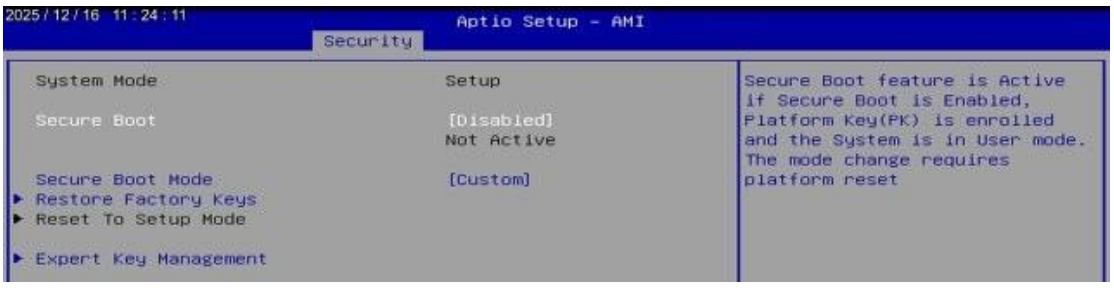
4.5.2.1 SATA Configuration:



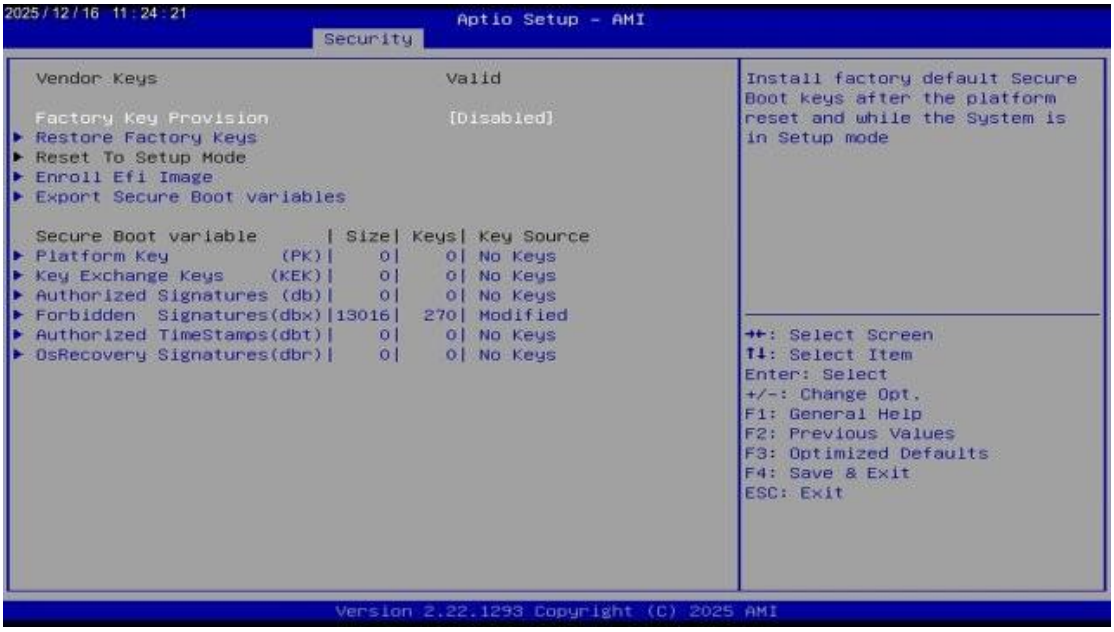
BIOS Setting	Description
SATA and RST Configuration	SATA device options and settings
SATA Controller(s)	Enables / Disables the SATA Device.
SATA Mode Selection	Determines how SATA controller(s) operate
Serial ATA Port 0~7	Enables / Disables Serial Port 0~7.
SATA Ports Hot Plug	Enables / Disables SATA Ports HotPlug.
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



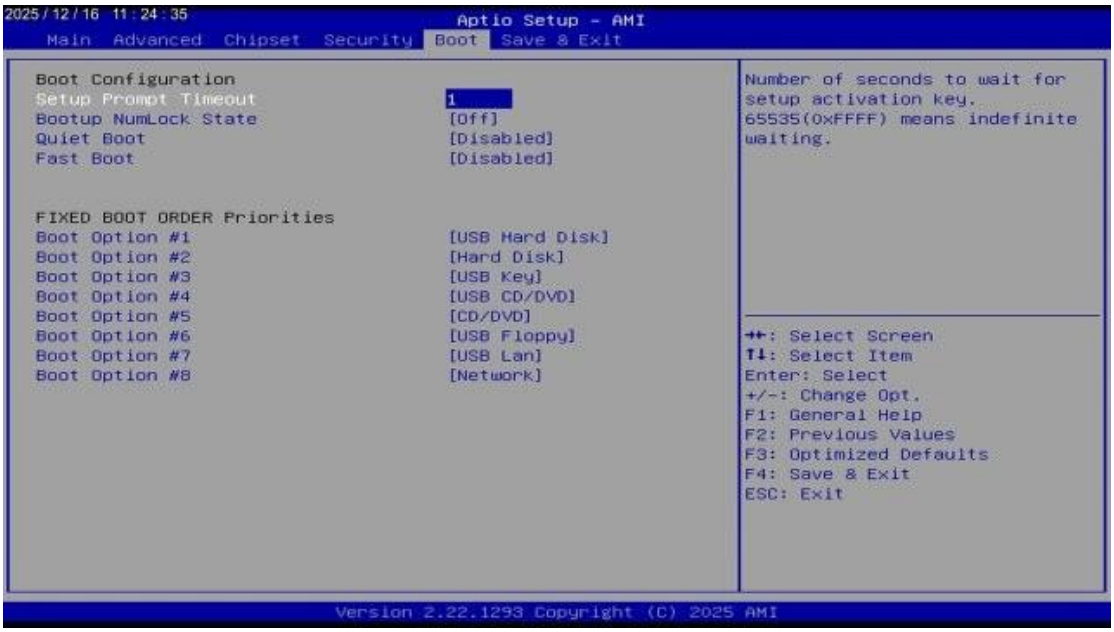


BIOS Setting	Description
Disable Block Sid and Freeze Lock	Override to allow SID authentication of TCG Storage device and to skip freeze lock command for SATA device. Modified value will be applicable only for next boot.
Setup Administrator Password	Sets an administrator password for the setup utility.
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
Expert Key Management	Enables expert users to modify Secure Boot Policy variables without variable authentication.



BIOS Setting	Description
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the system is in setup mode.
Restore Factory Keys	Force System to User Mode. Install factory default secure boot key databases.
Enroll Efi Image	Allow Efi image to run in secure boot mode. Enroll SHA256 Hash certificate of a PE image into Authorized Signature Database (db).
Platform Key Key Exchange Keys Authorized Signatures Forbidden Signatures Authorize TimeStamps OsRecovery Signatures	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

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.
Fast Boot	Enables / Disables boot with initialization of a minimal set of devices required to launch active boot option. Has no effect for BBS boot options.
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 from one of the available filesystem devices.

Appendix

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

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

A. I/O Port Address Map

Address	Device Description
0x00000A00-0x00000A0F	Motherboard resources
0x00000A10-0x00000A1F	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
0x00003000-0x0000303F	Intel(R) UHD Graphics 770

0x000003F8-0x000003FF	Communications Port (COM1)
0x000002F8-0x000002FF	Communications Port (COM2)
0x000003E8-0x000003EF	Communications Port (COM3)
0x000002E8-0x000002EF	Communications Port (COM4)
0x000002F0-0x000002F7	Communications Port (COM5)
0x000002E0-0x000002E7	Communications Port (COM6)
0x0000EFA0-0x0000EFBF	Intel(R) SMBus - 7AA3
0x00003090-0x00003097	Standard SATA AHCI Controller
0x00003080-0x00003083	Standard SATA AHCI Controller
0x00003060-0x0000307F	Standard SATA AHCI Controller
0x00000000-0x00000CF7	PCI Express Root Complex
0x00000D00-0x0000FFFF	PCI Express Root Complex
0x00001854-0x00001857	Motherboard resources
0x00000040-0x00000043	System timer
0x00000050-0x00000053	System timer
0x00002000-0x000020FE	Motherboard resources
0x00000060-0x00000060	Standard PS/2 Keyboard
0x00000064-0x00000064	Standard PS/2 Keyboard

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 4294967286	Intel(R) USB 3.20 eXtensible Host Controller - 1.20 (Microsoft)
IRQ 4294967290	Intel(R) PCI Express Root Port #4 - 7ABB
IRQ 4294967287	Intel(R) UHD Graphics 770
IRQ 4294967294	Intel(R) PCI Express Root Port #25 - 7AC8
IRQ 4	Communications Port (COM1)
IRQ 3	Communications Port (COM2)
IRQ 5	Communications Port (COM3)
IRQ 6	Communications Port (COM4)
IRQ 7	Communications Port (COM5)
IRQ 10	Communications Port (COM6)
IRQ 4294967288	Standard SATA AHCI Controller
IRQ 4294967289	Intel(R) PCI Express Root Port #13 - 7AB4
IRQ 16	Intel(R) Serial IO UART Host Controller - 7AA8
IRQ 4294967292	Intel(R) PCI Express Root Port #2 - 7AB9
IRQ 4294967253-57	Intel(R) Ethernet Controller I226-LM
IRQ 4294967291	Intel(R) PCI Express Root Port #3 - 7ABA
IRQ 55-204	Microsoft ACPI-Compliant System
IRQ 256-511	Microsoft ACPI-Compliant System
IRQ 0	System timer
IRQ 17	High Definition Audio Controller
IRQ 4294967277-85	Standard NVM Express Controller
IRQ 37	Intel(R) Serial IO SPI Host Controller - 7AAB
IRQ 1	Standard PS/2 Keyboard
IRQ 12	Microsoft PS/2 Mouse
IRQ 4294967251-52	Intel(R) Wi-Fi 6E AX210 160MHz
IRQ 4294967250	Intel(R) Wi-Fi 6E AX210 160MHz
IRQ 4294967293	Intel(R) PCI Express Root Port #1 - 7AB8
IRQ 14	Intel(R) Serial IO GPIO Host Controller - INTC1056
IRQ 4294967263-67	Intel(R) Ethernet Controller I226-IT
IRQ 4294967258-62	Intel(R) Ethernet Controller I226-IT #2
IRQ 4294967276	Standard NVM Express Controller
IRQ 4294967268-75	Standard NVM Express Controller