INA2205

1U Network Appliance with Intel® Atom® Processor (formerly Amston Lake) & up to 8 GbE ports

User's Manual

Version 1.0
February 2026

iBASE

Copyright

Disclaimer

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

Trademarks

All the trademarks 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 regulatory limits and environmental requirements. 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 be valid.

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 or industrial environment. 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

RoHS Compliant

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

iBASE

Important Safety Information

Carefully read the following safety information before using the device.

Setting up your system:

- Put the device on a stable and solid surface.
- 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.
- Avoid placing this device in environments where the storage temperature may fall below -20˚C or exceed 70˚C, as this could damage the device. The device must be operated in a controlled environment.

Care During Use:

- Do not place heavy objects on the top of the device.
- Make sure to connect the correct voltage to the device. Failure to supply the correct voltage could damage the unit.
- Do not walk on the power cord or allow anything to rest on it.
- If you use an extension cord, make sure the total ampere rating of all devices plugged into the extension cord does not exceed the cord's ampere rating.
- Do not spill water or any other liquids on your device.
- Always unplug the power cord from the wall outlet before cleaning the device.
- Only use cleaning agents with a neutral pH level to clean the device.
- Vacuum dust and particles from the vents by using a computer vacuum cleaner.

Warranty Policy

- **IBASE standard products:**

  24-month (2-year) warranty from the date of shipment. If the date of shipment cannot be ascertained, customers can use the product serial numbers to approximate the 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, HDD, power adapter, panel and touchscreen.

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

Technical Support & Services

- Visit the IBASE website at www.ibase.com.tw to find the latest information about the product.
- If you encounter any technical problems and require assistance from your distributor or sales representative, please prepare and send the following information:

  - Product model name
  - Product serial number
  - Detailed description of the problem
  - Error messages in text or in screenshot form, if there any
  - The arrangement of the peripherals
  - Software in use (such as OS and application software, including the version numbers)

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

iBASE

Table of Contents

Chapter 1
General Information

The information provided in this chapter includes:

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

1.1 Introduction

The INA2205 is a compact 1U rackmount network appliance designed for wired networking applications in enterprise, industrial, and edge environments. It is powered by the Intel® Atom® x7405C processor (4 cores, up to 3.40 GHz) (formerly *Amston Lake*), delivering energy-efficient performance for firewall, routing, and network security deployments. The system supports one DDR5-4800 SO-DIMM slot with a maximum capacity of 16GB (Non-ECC). Storage options include support for one 2.5-inch SATA HDD/SSD and one M.2 2242 SATA storage slot, allowing flexible system and data storage configurations.

For networking, the INA2205 provides up to eight Ethernet ports, including four 2.5GbE RJ45 ports, two 1GbE RJ45 ports, and two 1GbE SFP ports. A hardware LAN bypass function is available on one Ethernet segment to maintain network connectivity during system failure. The front panel features an LCM display, status LEDs, USB ports, and a Reset button for system monitoring and maintenance. The system is housed in a 1U chassis and is designed for reliable operation in professional network environments.

1.2 Features

- Intel® Atom® x7405C Processor
- 1x DDR5-4800 SO-DIMM, Max. 16GB (Non-ECC)
- 4x 2.5G LAN RJ45 ports with 1 pair bypass on board and 2x 1G RJ45 LAN ports
- 2x SFP ports
- Supports open-frame 65W power supply

1.3 Packing List

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

- INA2205 System Unit
- Power Adapter
- AC Power Cord
- M.2 Screw Kit
- 2 x Rack ear Bracket

1.4 Optional Accessories

The following items are available depending on system configuration or sales package:

- SATA Data Cable

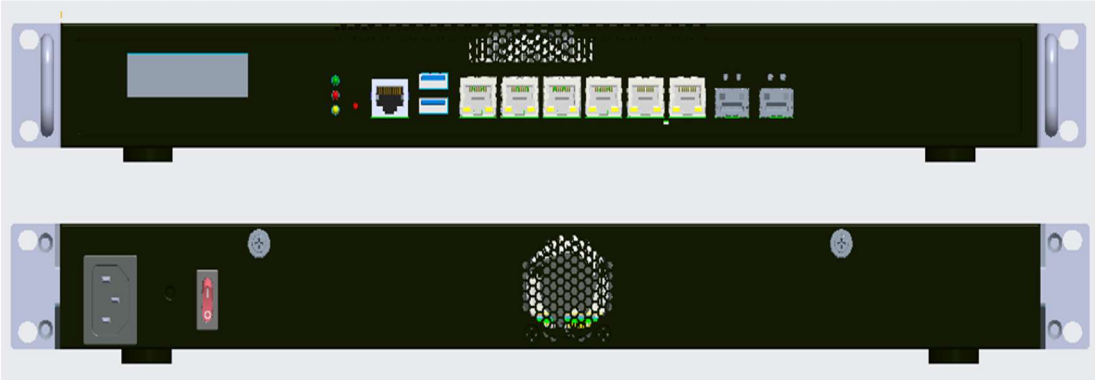
1.5 INA2205 Specifications

CPU	Intel® Atom® x7405C Processor (6M Cache, up to 3.40 GHz), FCBGA1264
Chipset	N/A
Memory	1x DDR5-4800 SO-DIMM (Non-ECC)
Maximum Memory	16GB
Display	1x LCM
Ethernet	4x Intel® i226V RJ45 ports (2.5GbE); 2x Intel® i350-AM4 RJ45 ports (1GbE); 2x Intel® i350-AM4 SFP ports (1GbE)
LAN Bypass	1x Segment (LAN5 / LAN6)
Expansion	N/A
IPMI	N/A
Storage	1x 2.5” SATA HDD/SSD; 1x M.2 2242 SATA SSD (SATA only)
TPM	TPM 2.0
I/O	• 1x LCM • 3x LED (Status / HDD / Power) • 4x 2.5G RJ45 LAN • 2x 1G RJ45 LAN • 2x SFP • 2x USB 3.0 • 1x Reset Button
Power Supply	Open-frame 65W power supply
Dimensions	438 (W) x 180 (D) x 43.5 (H) mm
Weight	6.5 kg
Operating Temperature	0°C to 40°C
Storage Temperature	-20°C to 70°C
Operating Humidity	10% to 90% (non-condensing)
Certification	CE / FCC

All specifications are subject to change without prior notice.

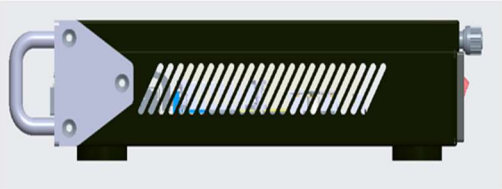
1.6 Product View

FRONT



BACK

LEFT



RIGHT

Front Panel I/O Connectors (Arranged from Left to Right)

No.	Connector	Name	Description
1	LED5	LED Indicators	Front-panel LED indicators (Status/HDD/ Power)
2	SW1	Digital I/O / Control Switch	GPIO control switch (refer to Digital I/O section)
3	RJ45COM1	Console Port	RJ45 serial console port
4	CN5	USB Ports	2x USB 3.0 Type-A ports
5	CN6	LAN Port	RJ45 LAN port
6	CN7	LAN Port	RJ45 LAN port
7	CN8	LAN Port	RJ45 LAN port
8	CN9	LAN Port	RJ45 LAN port
9	CN10	LAN Port	RJ45 LAN port
10	CN11	LAN Port	RJ45 LAN port
11	CN3	SFP Port	SFP Ethernet port
12	CN4	SFP Port	SFP Ethernet port

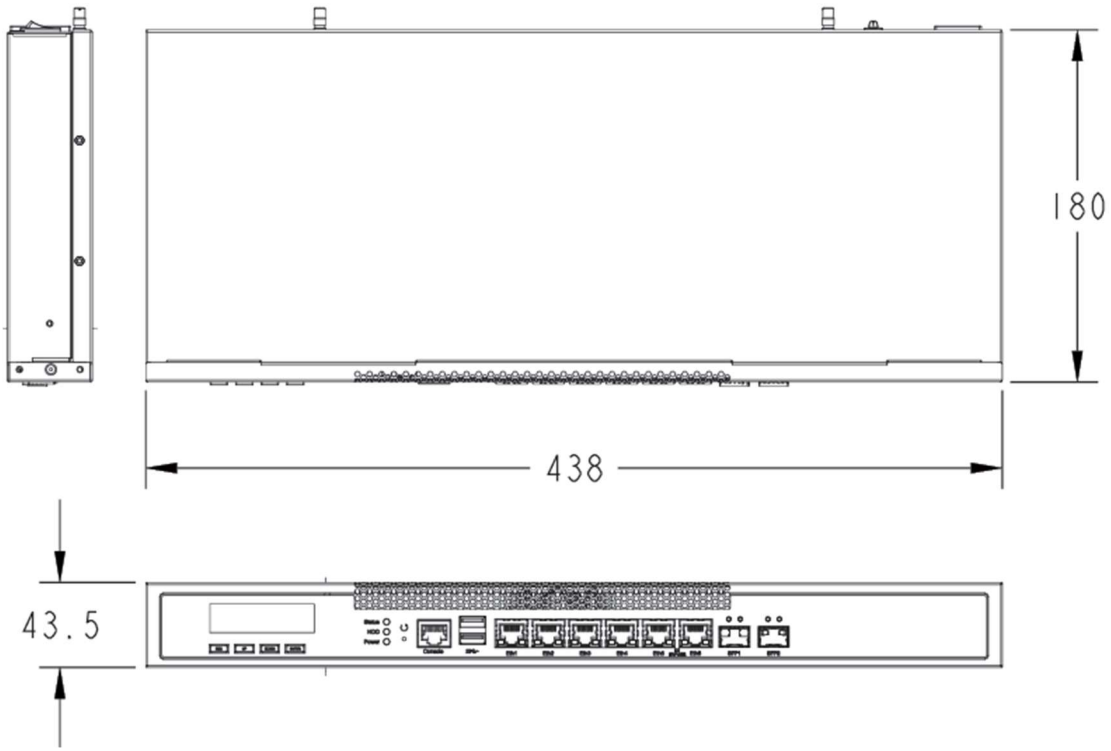
Note: LAN port speed and controller assignment depend on system configuration. Refer to the Specifications section for Ethernet controller details.

Rear Panel I/O (Arranged from Left to Right)

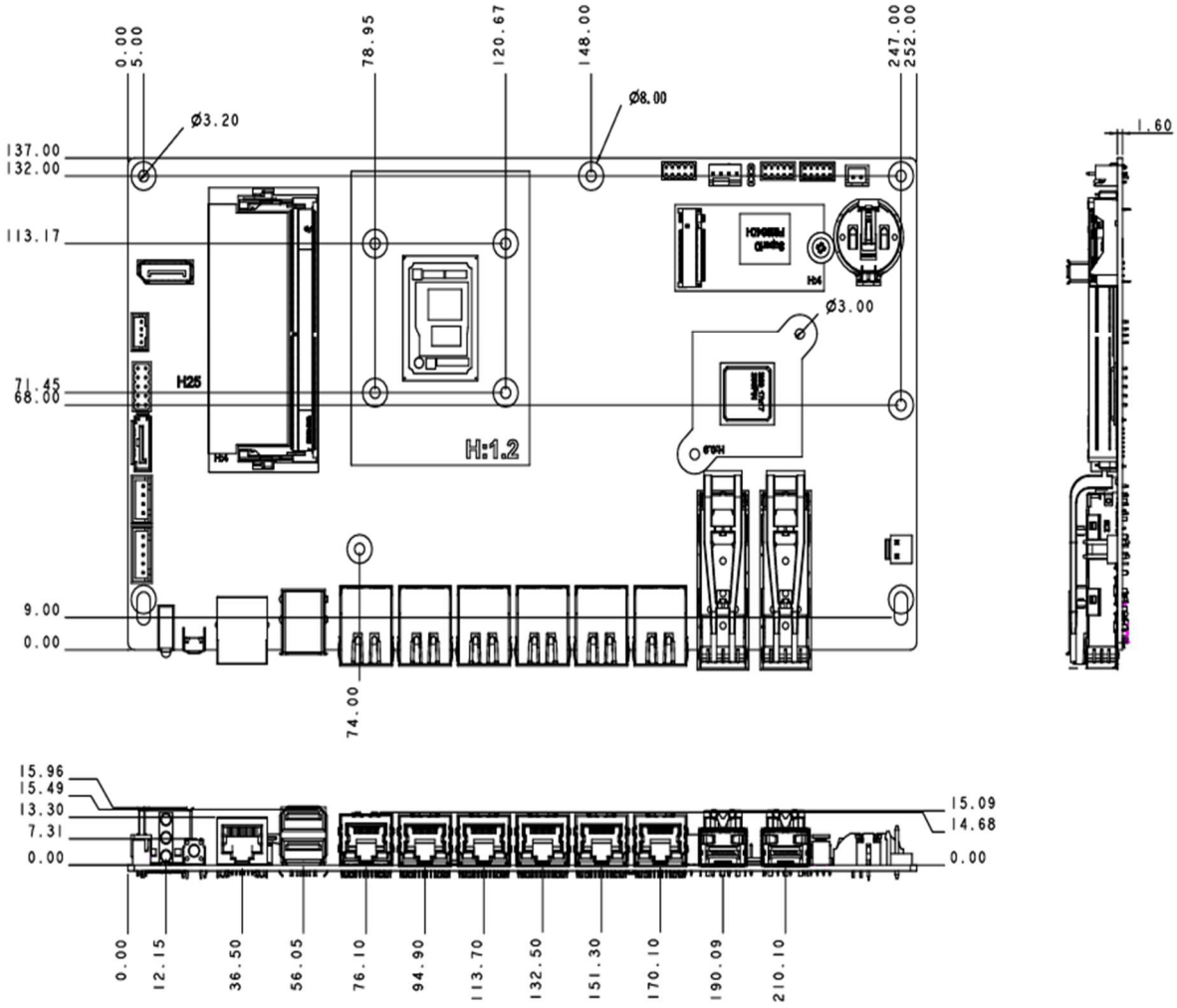
No.	Connector	Name	Description
1	AC_IN	AC Power Inlet	AC power input connector
2	SW_PWR	Power Switch	System power on/off switch
3	FAN_SYS	System Fan	System cooling fan with ventilation grille

1.7 Dimensions

INA2205 Dimensions



MBN2205 Motherboard Dimensions



Chapter 2
Hardware Configuration

The information provided in this chapter includes:

- Installation and Disassembly
- Rack Mount and Handle Removal (Optional)
- Top Cover Removal
- Power Board and HDD Module Removal
- Cooling Fan Removal
- LCM Module Removal
- Motherboard Removal
- Cable Fixing and Reassembly Notes
- Reassembly
- Component Installation

2.1 Installation and Disassembly

This section describes the recommended procedures for installing, removing, and servicing internal components of the INA2205 system.
Follow the steps in the order presented to avoid damage to the chassis or internal assemblies.

⚠ **Important**

Before performing any installation or disassembly procedure:

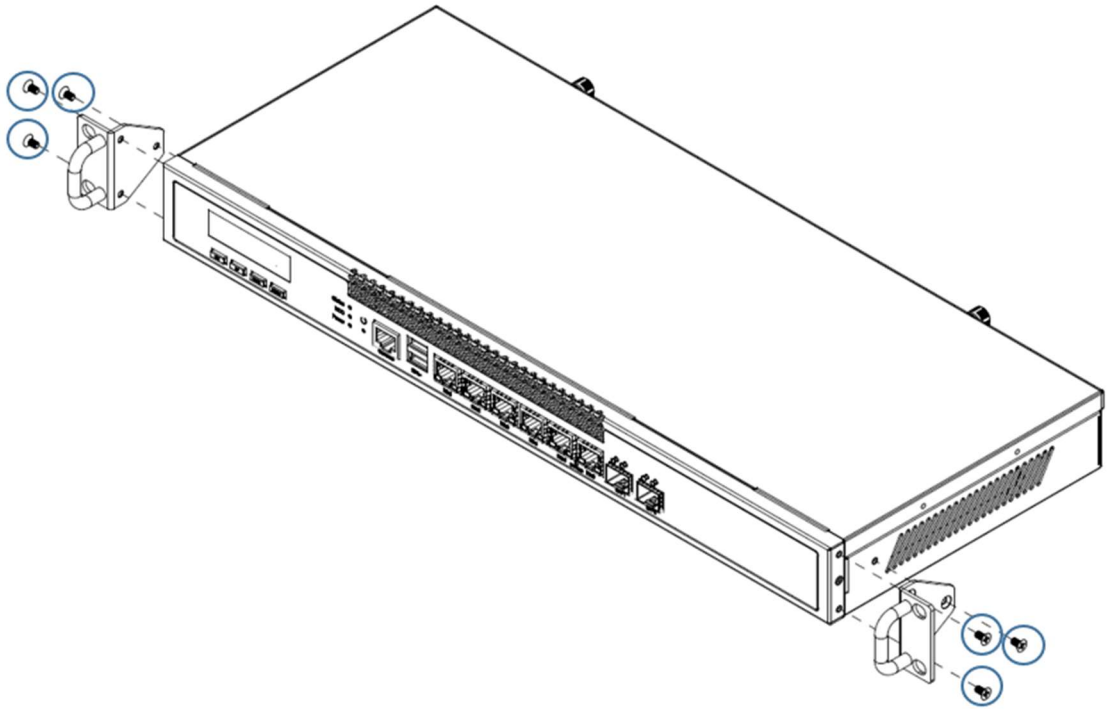
- Power off the system.
- Disconnect the power adapter and all external cables.
- Place the system on a clean, flat, and static-free surface.

2.1.1 Rack Mount and Handle Removal (Optional)

If rack brackets or handles are installed, remove them before opening the chassis.

Procedure:

1. Place the system on a stable surface.
2. Remove the M3 screws securing the rack mount brackets and handles on both sides.
3. Detach the rack mount brackets and handles from the chassis.



2.1.2 Top Cover Removal

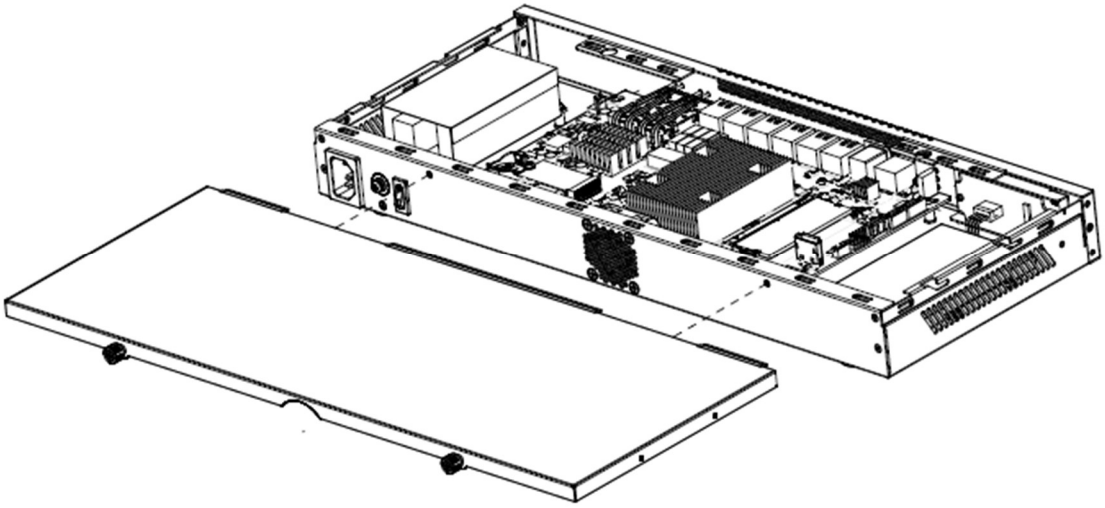
Removing the top cover provides access to internal serviceable components.

Procedure:

1. Loosen the hand-tightened screws securing the top cover.
2. Slide the top cover backward slightly.
3. Lift the top cover upward and remove it from the chassis.

After removing the top cover, the following components are accessible:

- Motherboard
- Memory module
- M.2 storage
- SATA HDD module
- Power board
- Cooling fan
- LCM module



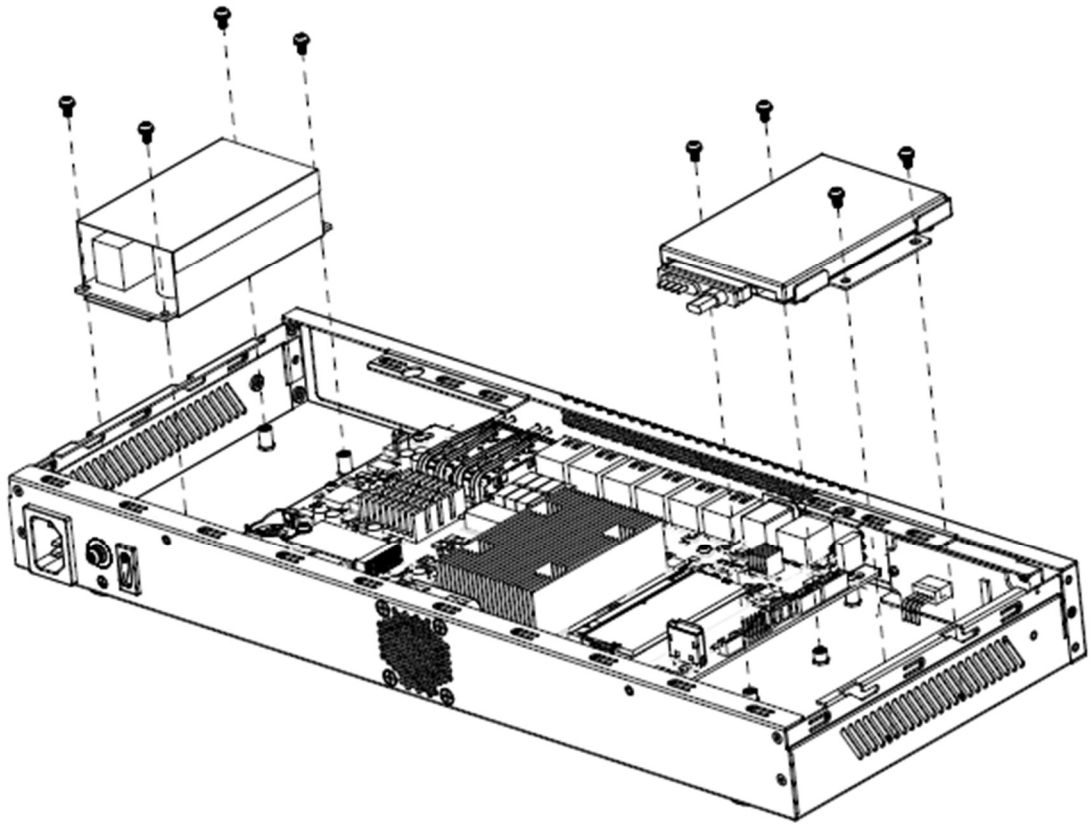
2.1.3 Power Board and HDD Module Removal

Remove the power board and HDD module if motherboard access or replacement is required.

Procedure:

1. Remove the M3 screws securing the power board.
2. Lift the power board carefully and disconnect its cables if necessary.
3. Remove the M3 screws securing the HDD module.
4. Lift the HDD module from the chassis.

⚠ Handle cables gently to prevent connector damage.

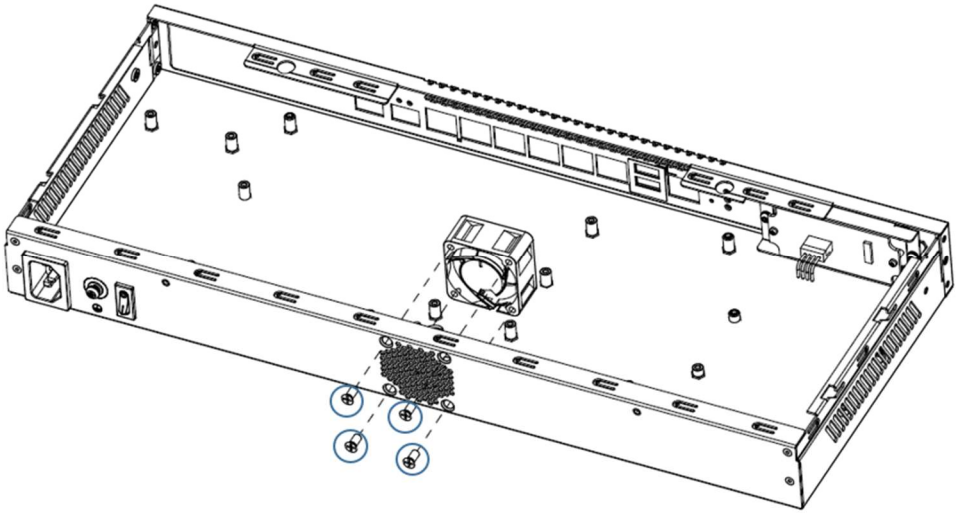


2.1.4 Cooling Fan Removal

Procedure:

1. Disconnect the fan power cable from the motherboard.
2. Remove **four (4) black Ø4 × 8 mm countersunk self-tapping screws (TP-3, BLACK, RoHS2)** securing the cooling fan.
3. Lift the cooling fan upward and remove it from the chassis.

⚠ Ensure the fan cable is fully disconnected before removing the fan.

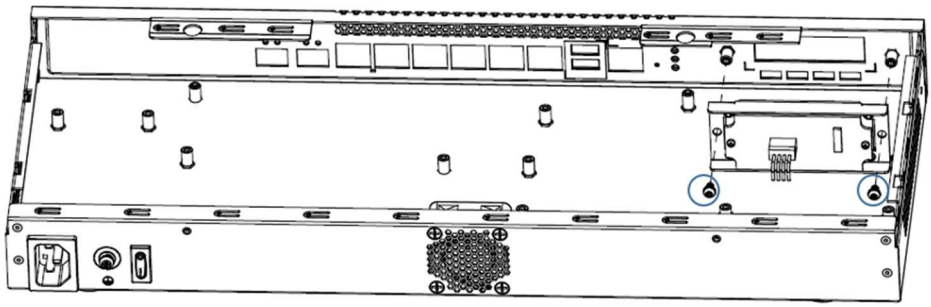


2.1.5 LCM Module Removal

Procedure:

1. Disconnect the LCM cable from the motherboard.
2. Remove **two (2) M3 × 6 mm pan head screws** securing the LCM module.
3. Carefully lift the LCM module out of the chassis.

⚠ Handle the LCM module carefully to avoid damaging the cable or display panel.



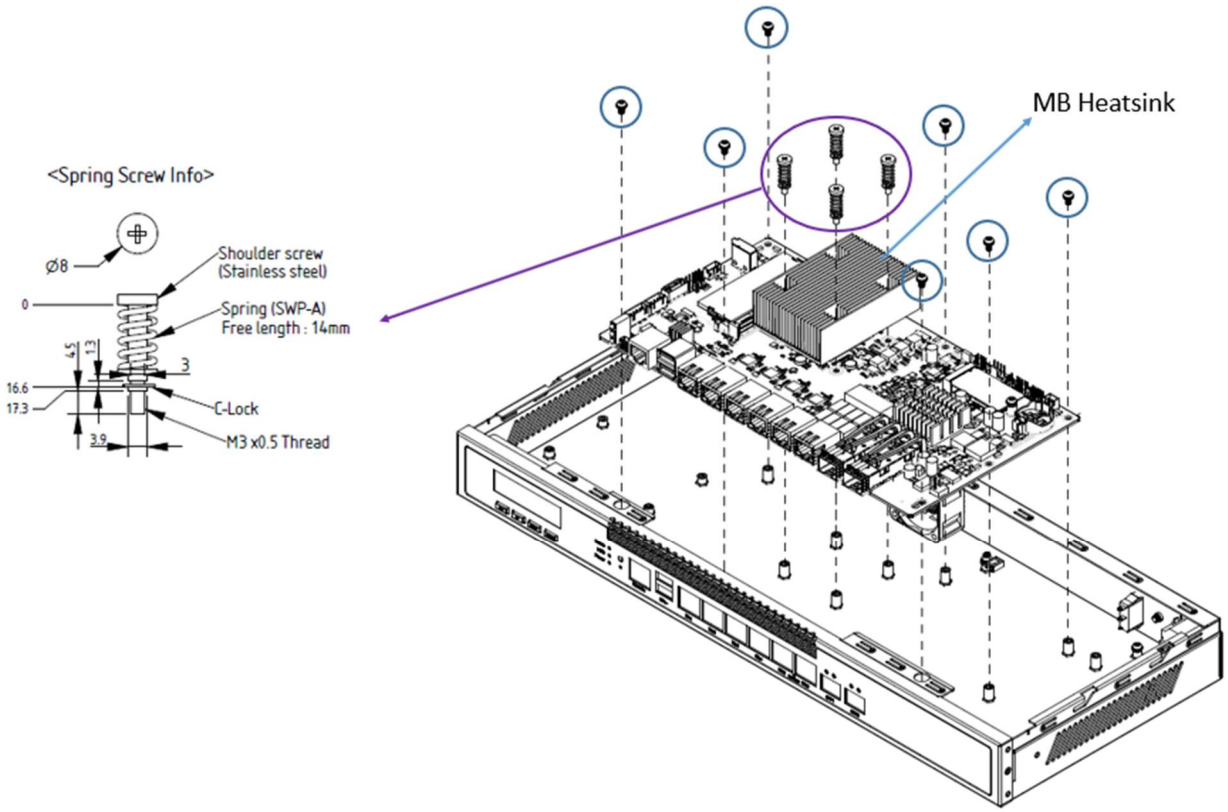
2.1.6 Motherboard Removal

Remove the motherboard only after all attached modules and cables have been disconnected.

Procedure:

1. Disconnect all motherboard cables (power, fan, front panel, storage).
2. Remove the M3 screws securing the motherboard to the chassis.
3. Remove the heatsink screws and detach the heatsink if required.
4. Lift the motherboard vertically and remove it from the chassis.

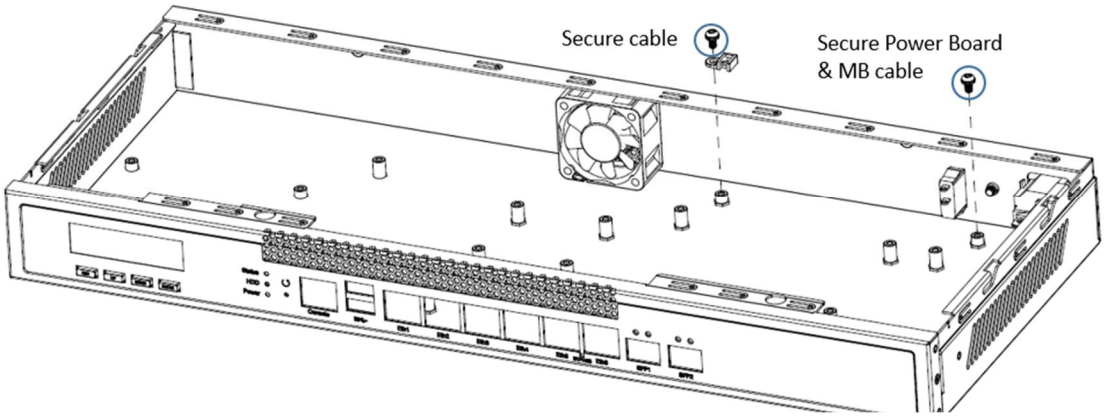
⚠ Avoid bending the motherboard during removal.



2.1.7 Cable Fixing and Reassembly Notes

During reassembly:

- Route all internal cables neatly along the chassis edges.
- Use **two (2) M3 × 6 mm pan head screws** to secure the cable fixing clamp.
- Fix both the **power board cable** and the **motherboard cable** using the cable fixing clamp.
- Ensure all cables are firmly secured and do not interfere with:
  - The cooling fan
  - Ventilation openings
  - The top cover during reinstallation



2.1.8 Reassembly

Reassemble the system by reversing the disassembly steps:

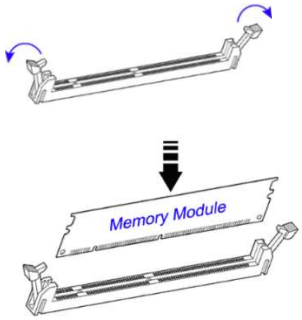
1. Reinstall the motherboard and heatsink.
2. Reinstall the fan, LCM module, power board, and HDD module.
3. Secure all cables and verify connections.
4. Reinstall the top cover and tighten screws.
5. Reattach rack mount brackets and handles if required.

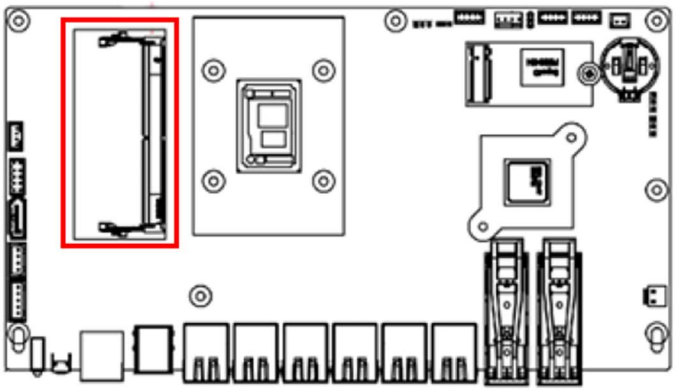
2.1.9 Component Installation

A. Memory Installation (DDR5 SO-DIMM)

1. Locate the **DDR5 SO-DIMM socket (J7)** on the motherboard.
2. Push the metal **retention clips outward** on both sides of the socket.
3. Align the notch on the DDR5 SO-DIMM module with the key in the socket.
4. Insert the module at approximately a **30-degree angle**.
5. Press the module downward until the retention clips snap into place.

✓ The memory module should lie flat and be firmly locked.



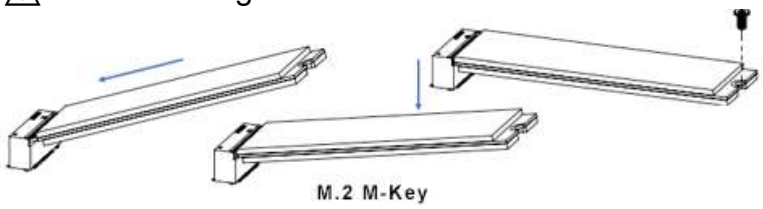


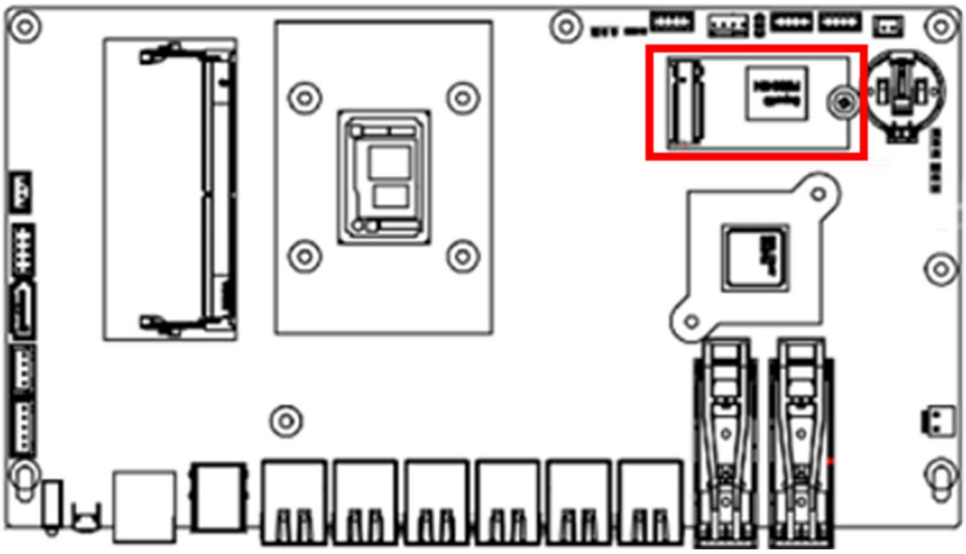
B. M.2 SSD Installation (M-Key, 2242)

The INA2205 provides **one M.2 M-Key slot (2242)** for SATA SSD storage.

1. Locate the **M.2 M-Key slot** on the motherboard.
2. If a standoff screw is pre-installed, remove it temporarily.
3. Insert the M.2 SSD into the slot at approximately a **30-degree angle**.
4. Push the SSD downward so that it aligns with the standoff.
5. Secure the SSD using the supplied **M.2 mounting screw**.

⚠ Do not overtighten the screw.





.

C. SATA III Drive Installation (2.5” SSD / HDD)

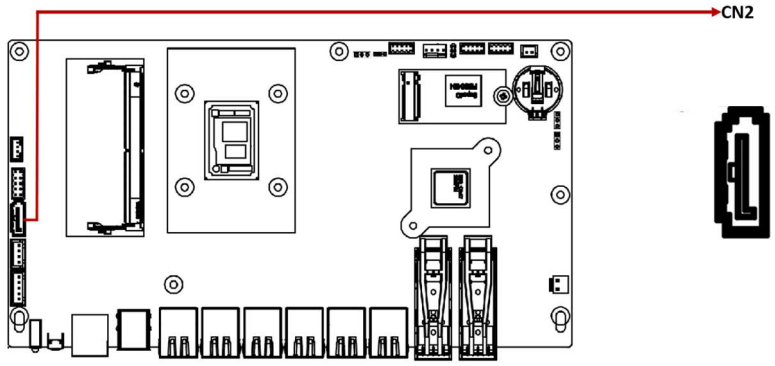
The INA2205 supports a 2.5” SATA storage device using a dedicated data and power connector.

1. SATA Data Connection
Locate the SATA III port on the motherboard.
Connect one end of the SATA data cable to the SATA III port.

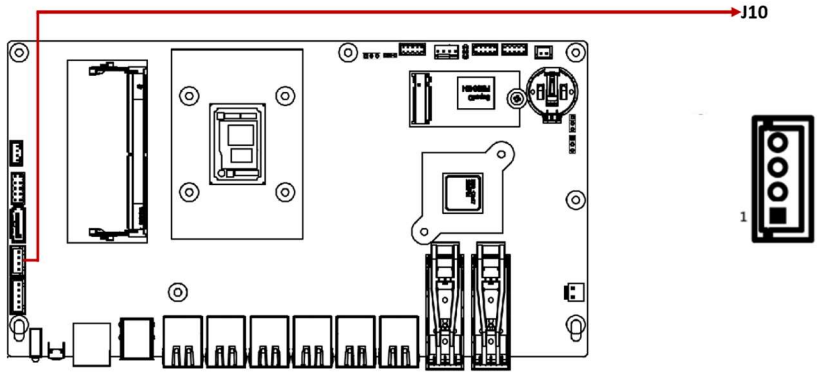
2. SATA Power Connection
Locate the SATA III power connector on the motherboard.
Connect the SATA power cable directly from this connector to the drive.

3. Drive Mounting
Mount the 2.5” drive in the designated internal drive bracket (if present).
Secure the drive using the appropriate screws.
✓ Ensure both data and power cables are fully seated.

CN2: SATA III Port Connector



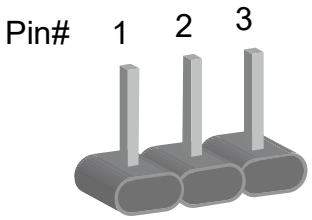
J10: SATA III Power Connector



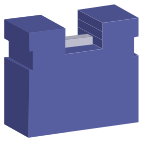
2.2 Setting the Jumpers

Set up and configure your device 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, shorting either PIN1 to PIN2 or PIN2 to PIN3 will enable the desired function or feature.

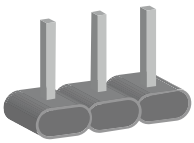
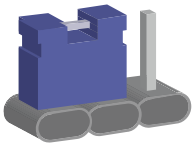
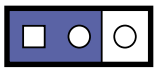
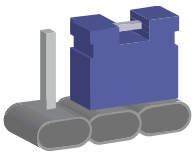
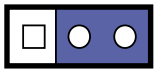


A 3-pin jumper



A jumper cap

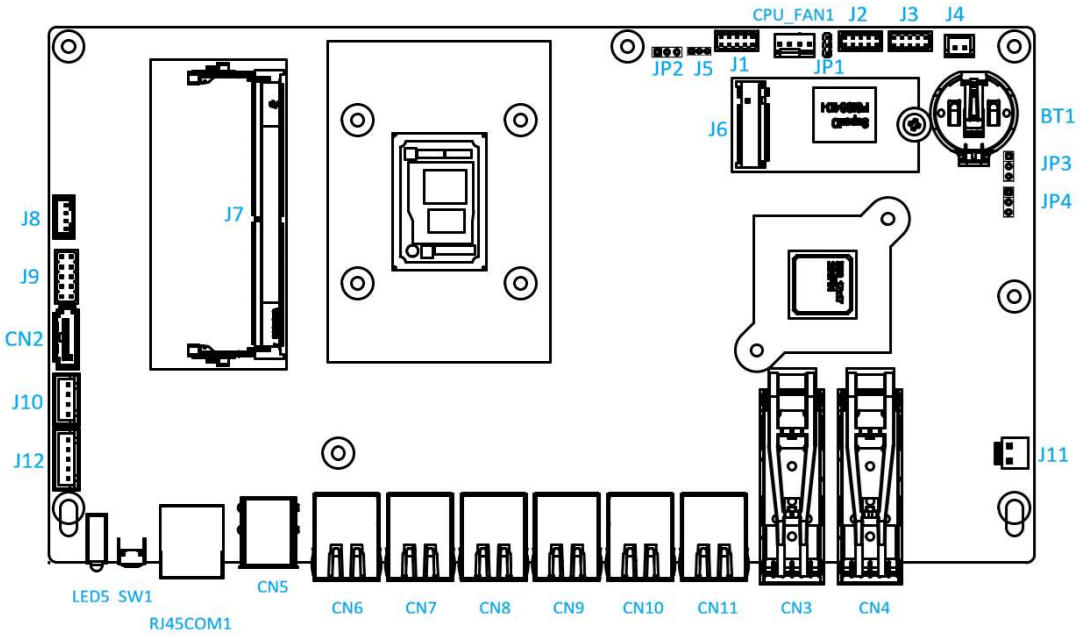
Refer to the illustration below to set jumpers.

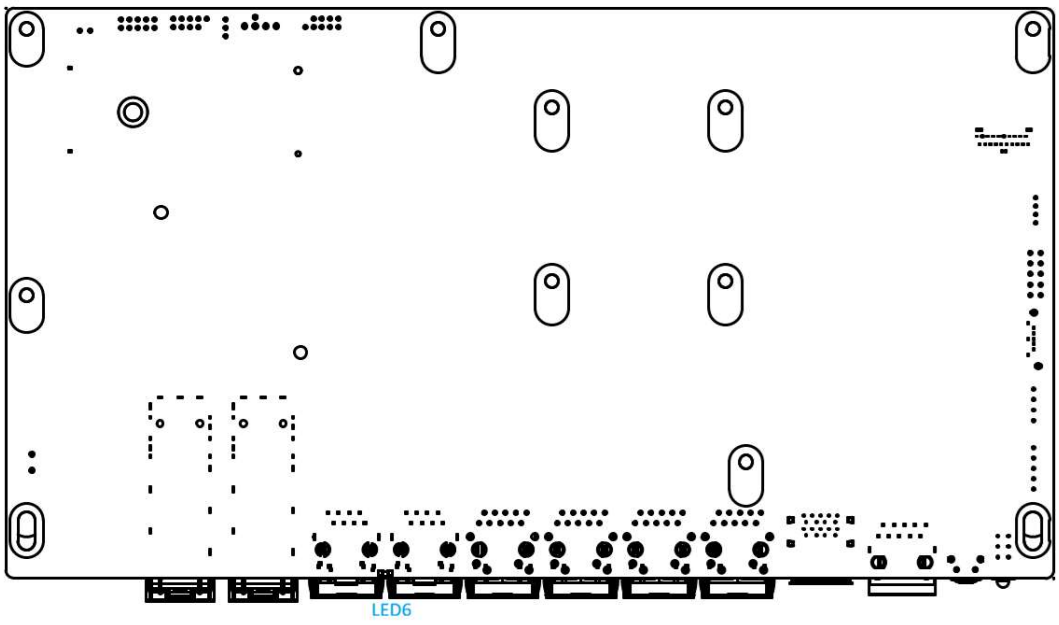
Pin closed	Oblique view	Jumper Settings
Open		
1-2		
2-3		

- Closed: Jumper cap encased in pins (turned On).
- Open: Jumper cap removed from pins (turned Off).

2.3 Jumper & Connector Locations on Motherboard

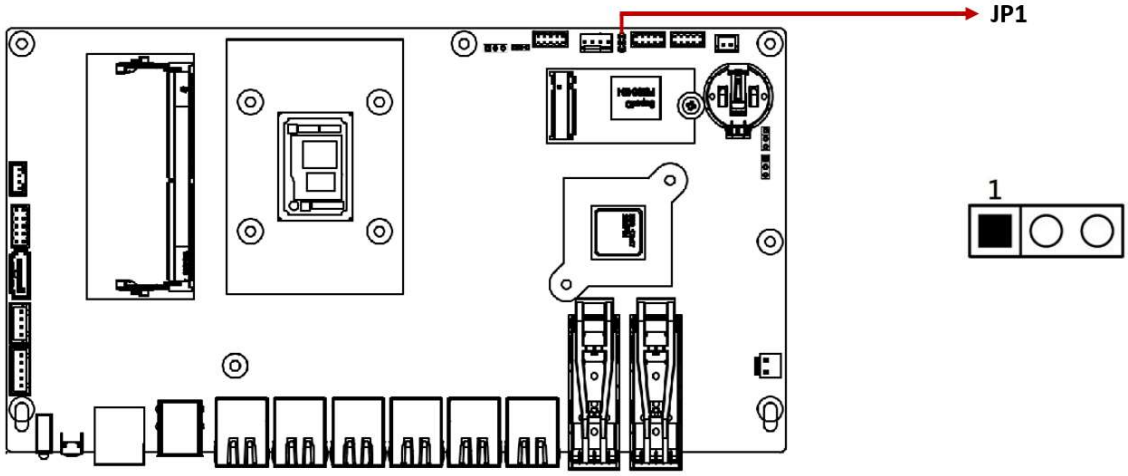
Motherboard: MBN2205

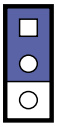




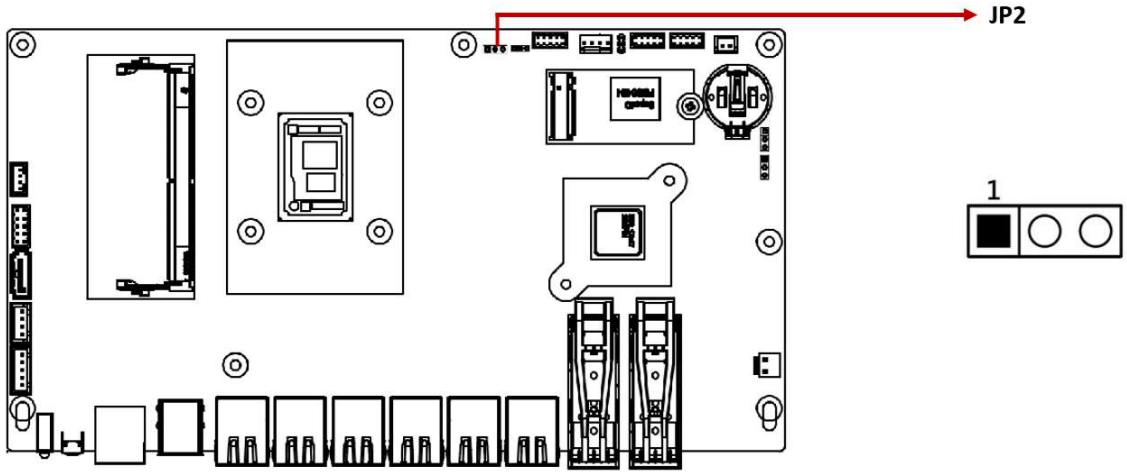
2.4 Jumpers, Switches and LEDs

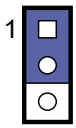
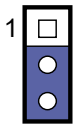
2.4.1 JP1: ATX / AT Mode Select



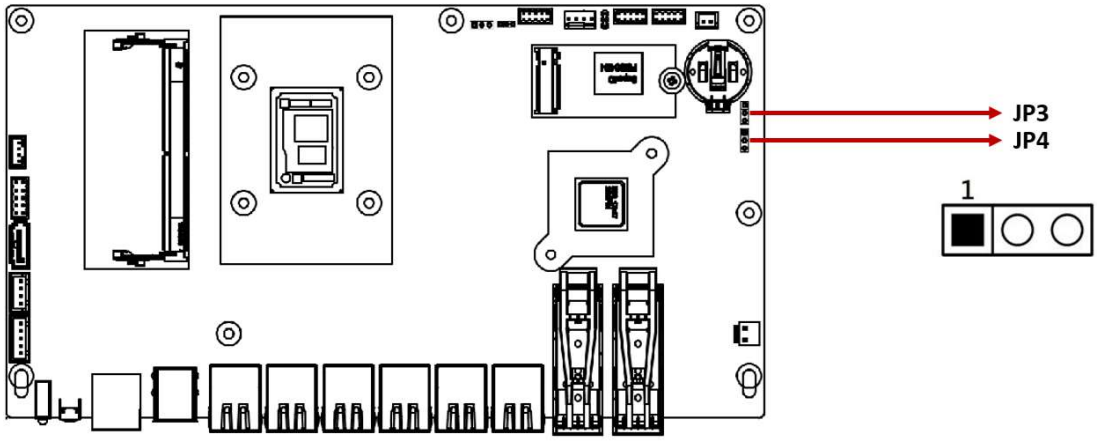
Pin closed	Setting	Function
1-2		ATX Mode (Default)
2-3		AT Mode

2.4.2 JP2: Flash Descriptor

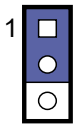
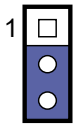


Pin closed	Setting	Function
1-2		Flash descriptor security override
2-3		Flash descriptor no security override (default)

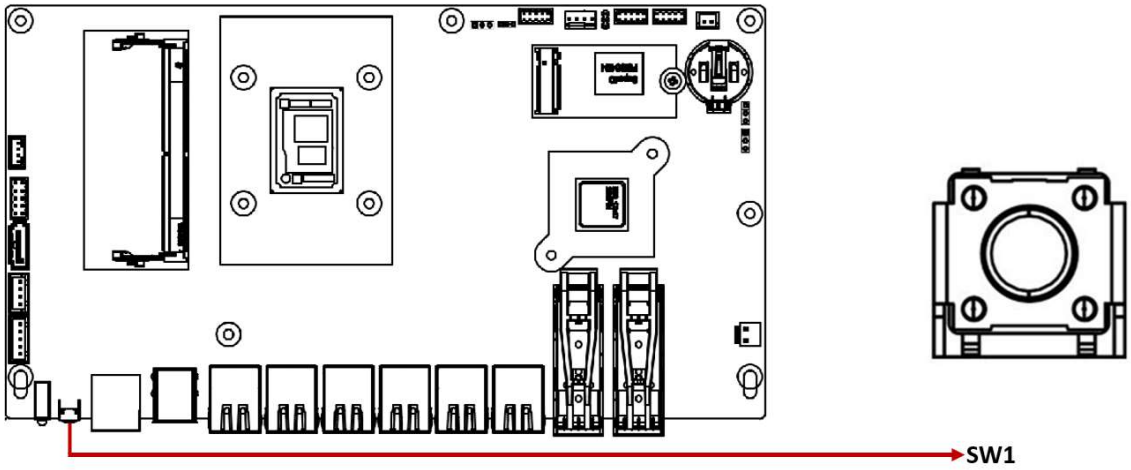
2.4.3 JP3, JP4: Clear CMOS



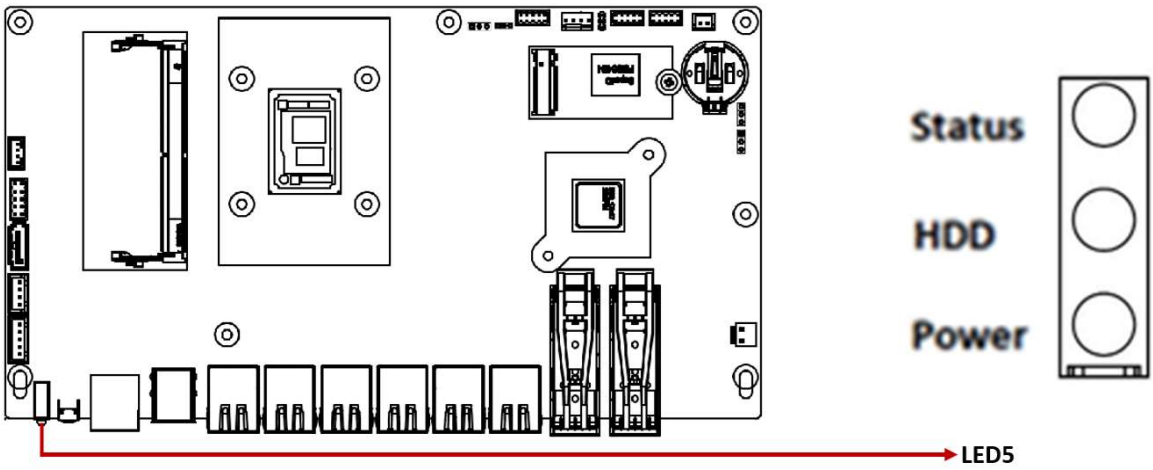
***Remark**: Use JP3, JP4 to clear the CMOS contents. Note that the ATX-power connector should be disconnected from the board before clearing CMOS.*

Pin closed	Setting	Function
1-2		Normal (Default)
2-3		Clear CMOS

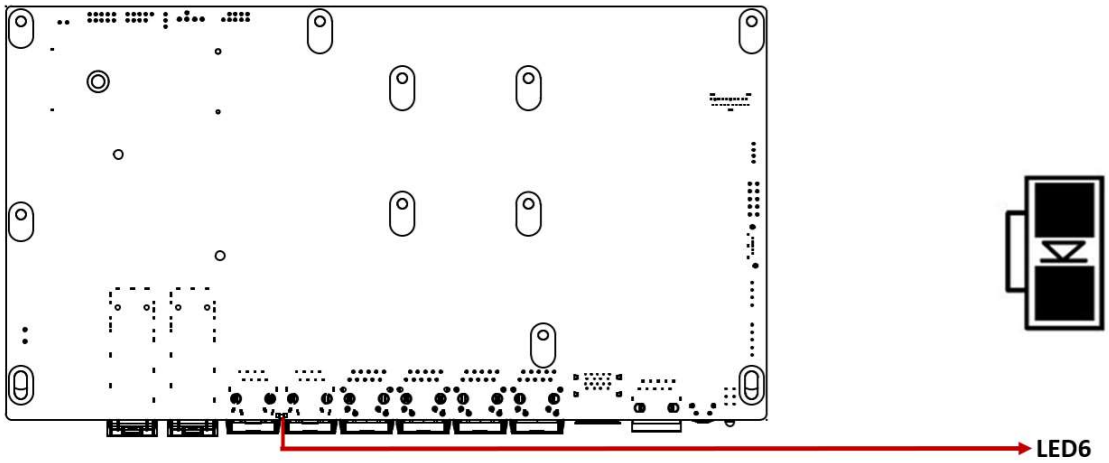
2.4.4 SW1: GPIO Button



2.4.5 LED5: Power (Green)/HDD (Green)/Status (Yellow/Red)

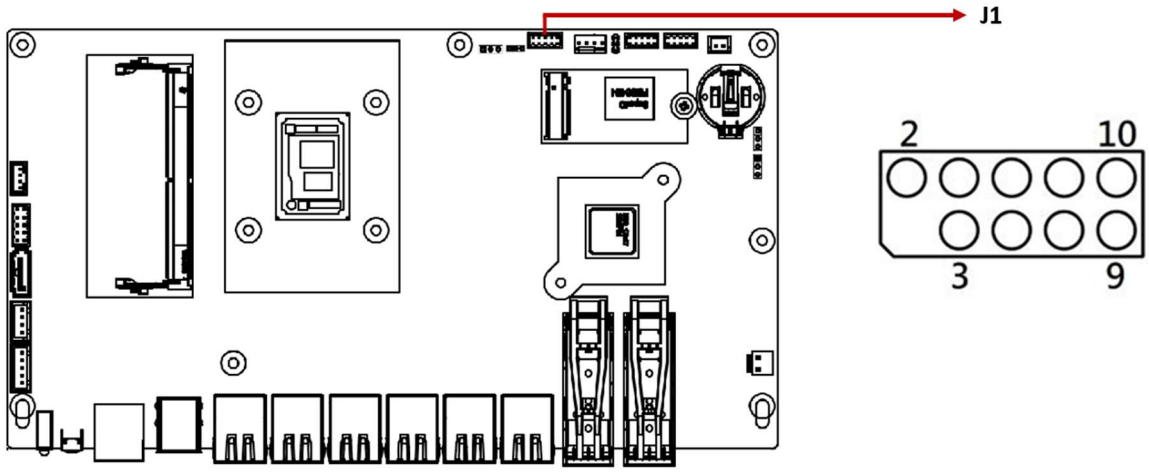


2.4.6 LED6: Bypass LED

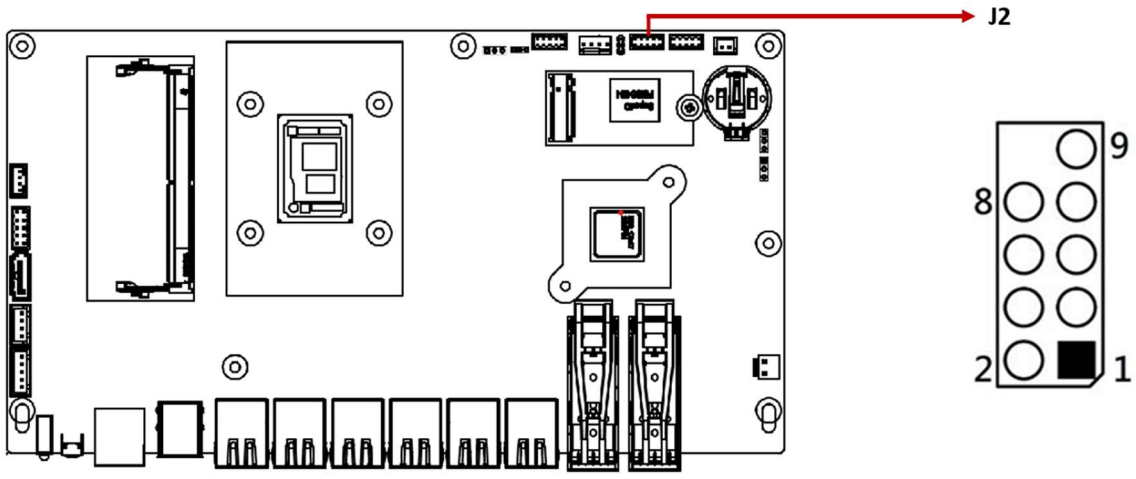


2.5 Connectors Quick Reference

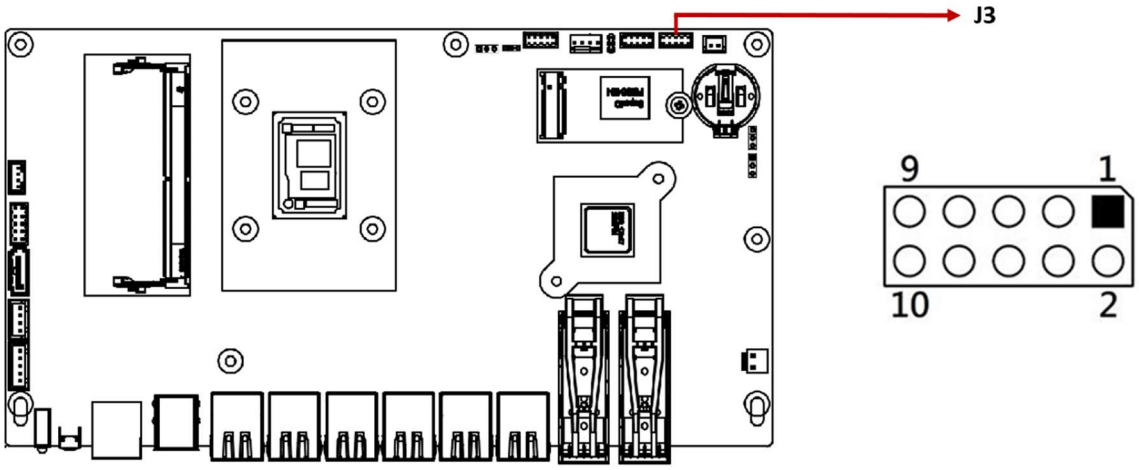
2.5.1 J1: SPI Debug Port (Factory use only)



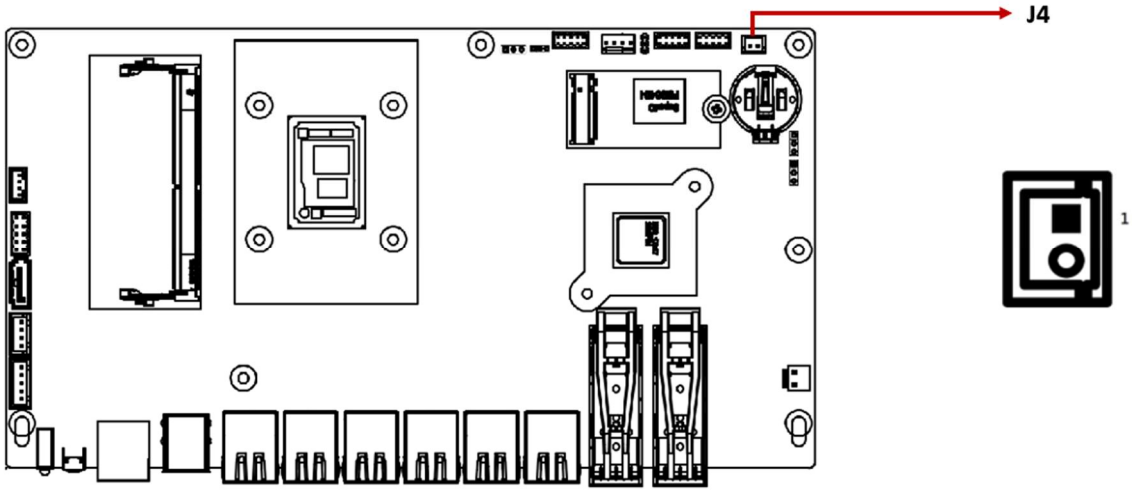
2.5.2 J2: eSPI Debug Port (Factory use only)



2.5.3 J3: DIO Header

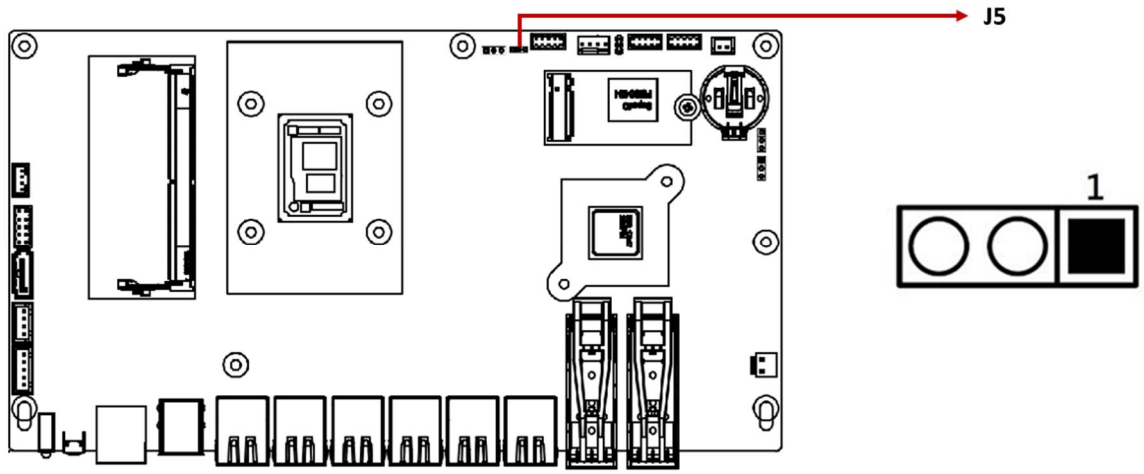


2.5.4 J4: PSU Simulated Connector

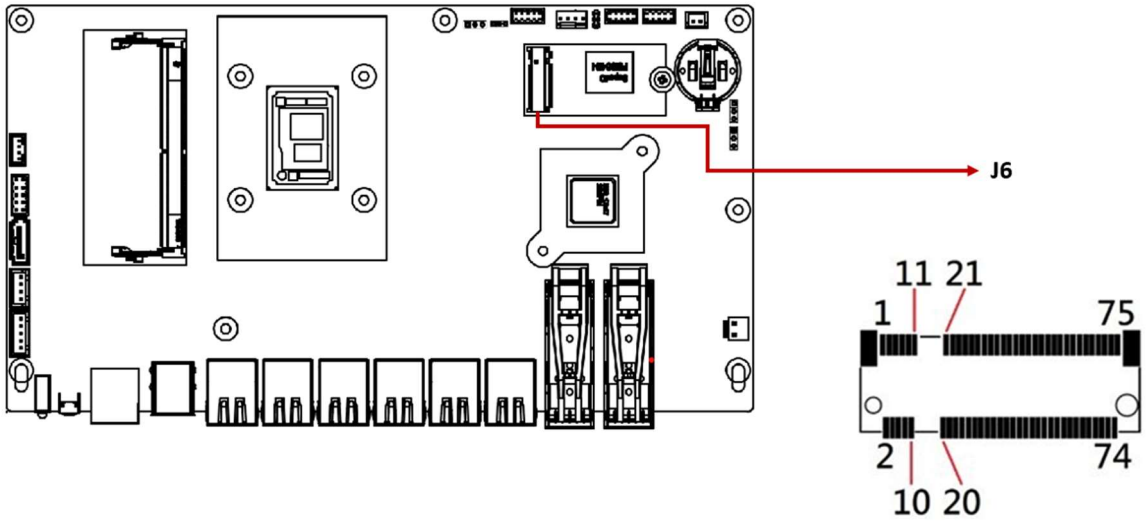


Signal Name	Pin	Pin	Signal Name
P_BTN-	1	2	P_BTN+

2.5.5 J5: Power Debug Port (Factory use only)

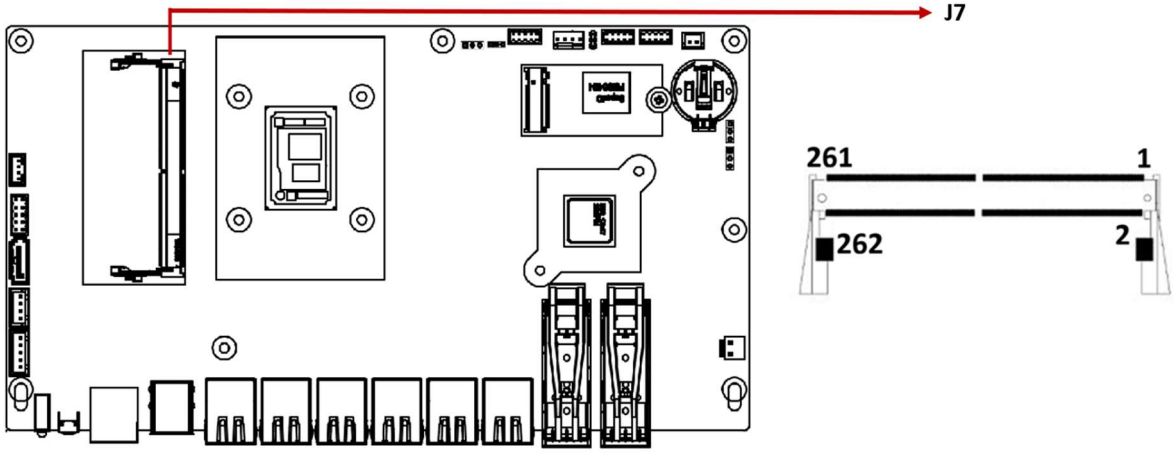


2.5.6 J6: M.2 M-Key Slot (2280)

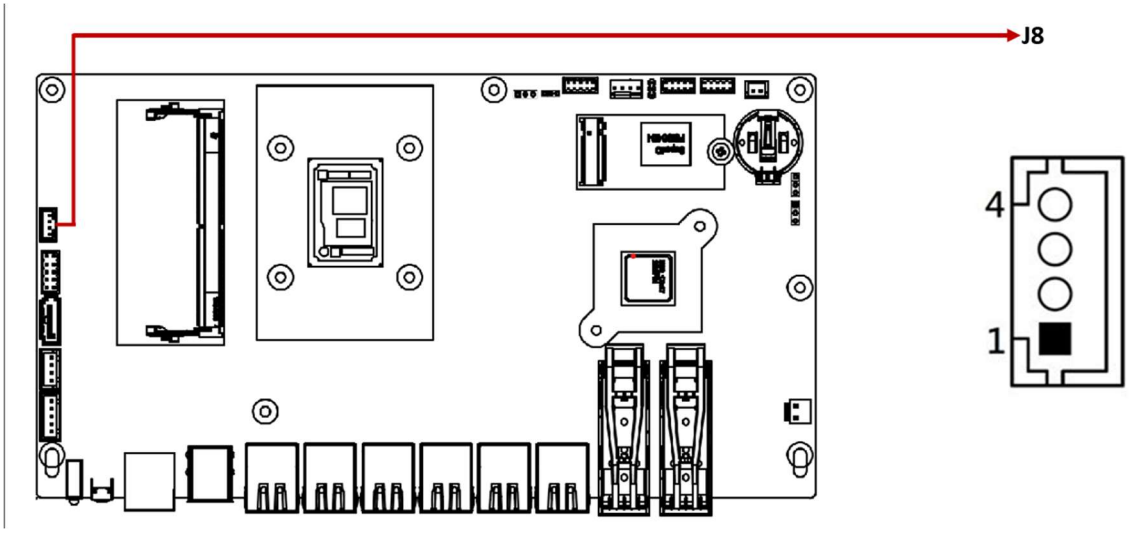


Remarks: Supports SATA III only

2.5.7 J7: DDR5 SO-DIMM Socket

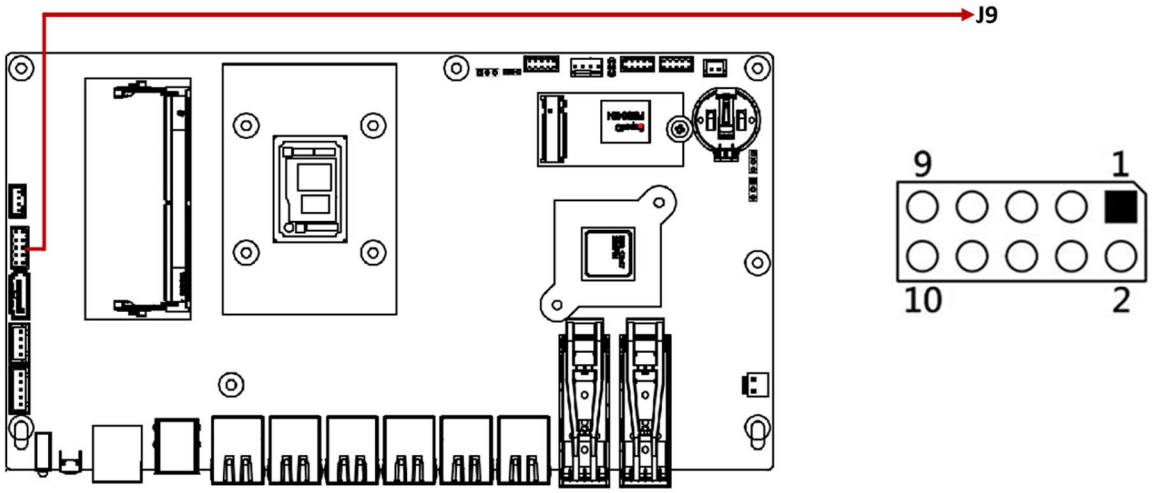


2.5.8 J8: MCU Debug Port (Factory use only)



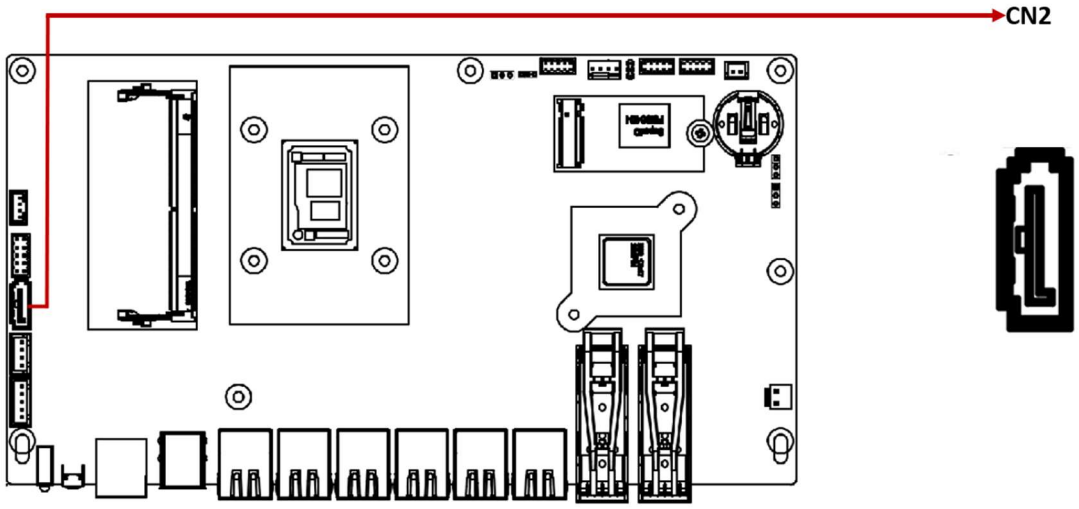
Pin	Signal Name
1	MCU_3V
2	SBWTCK
3	SBWTDIO
4	Ground

2.5.9 J9: Front Panel Function Connector

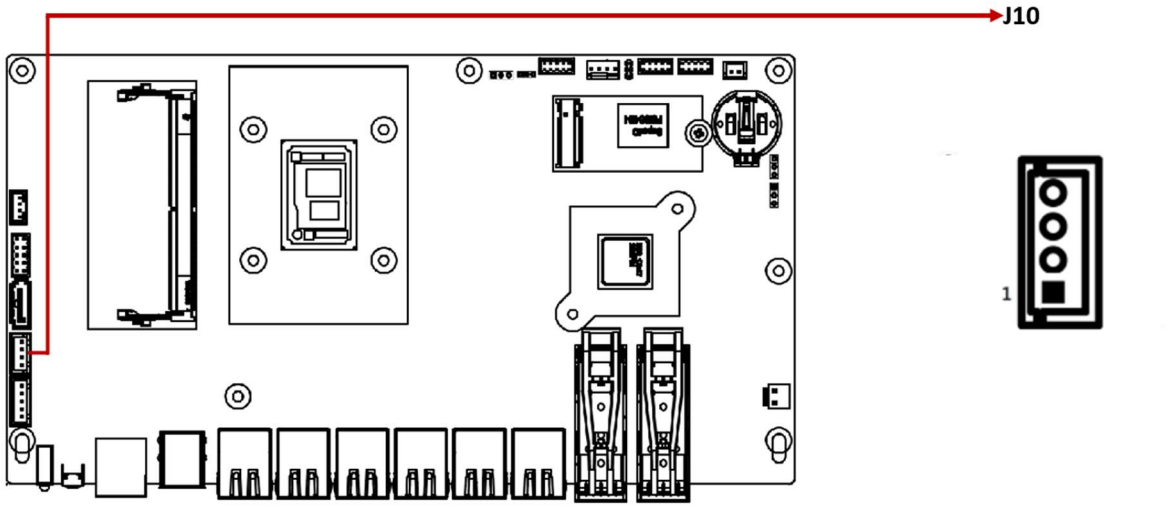


Signal Name	Pin	Pin	Signal Name
Ground	1	2	Power On
Ground	3	4	PM_SYSRST#
+5V	5	6	Ground
+3.3V	7	8	HDD LED
+3.3V	9	10	Bypass LED

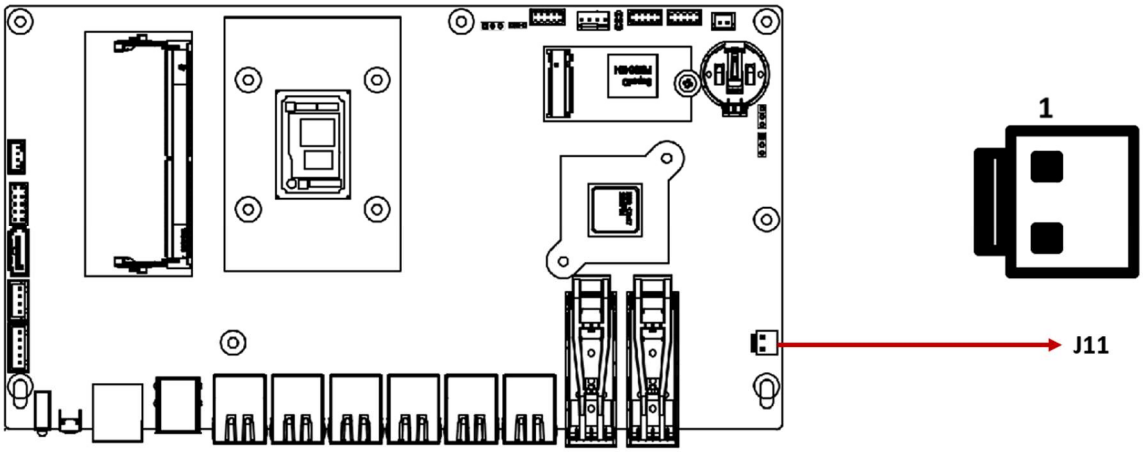
2.5.10 CN2: SATA III Port Connector



2.5.11 J10: SATA III Power Connector

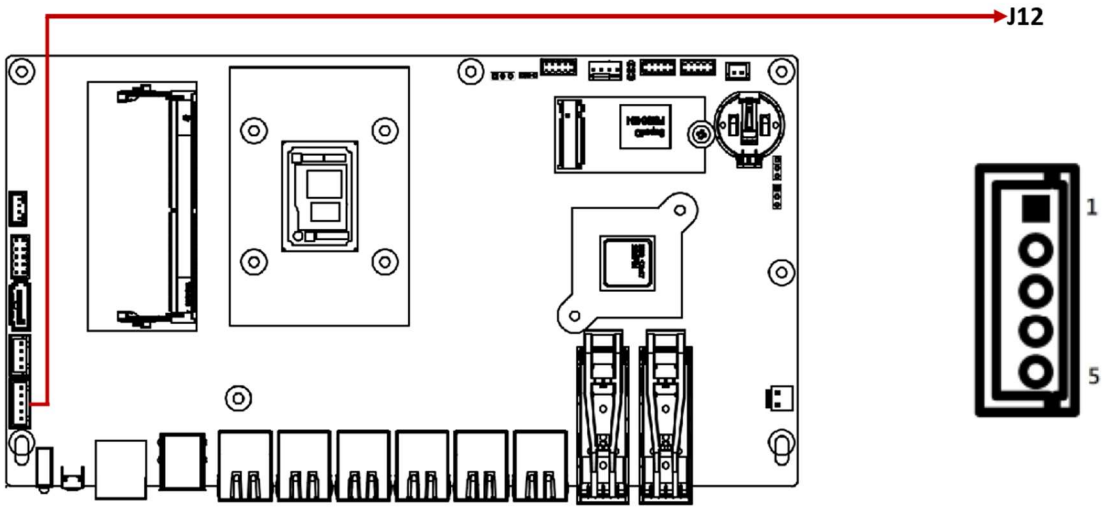


2.5.12 J11: Power Adapter Connector

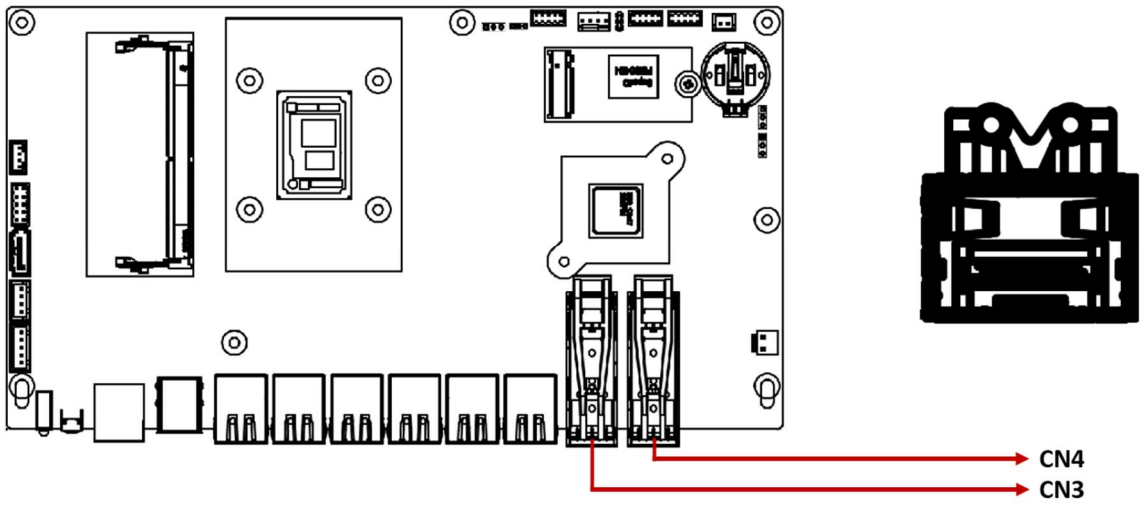


Pin	Signal Name
1	DC_In
2	Ground

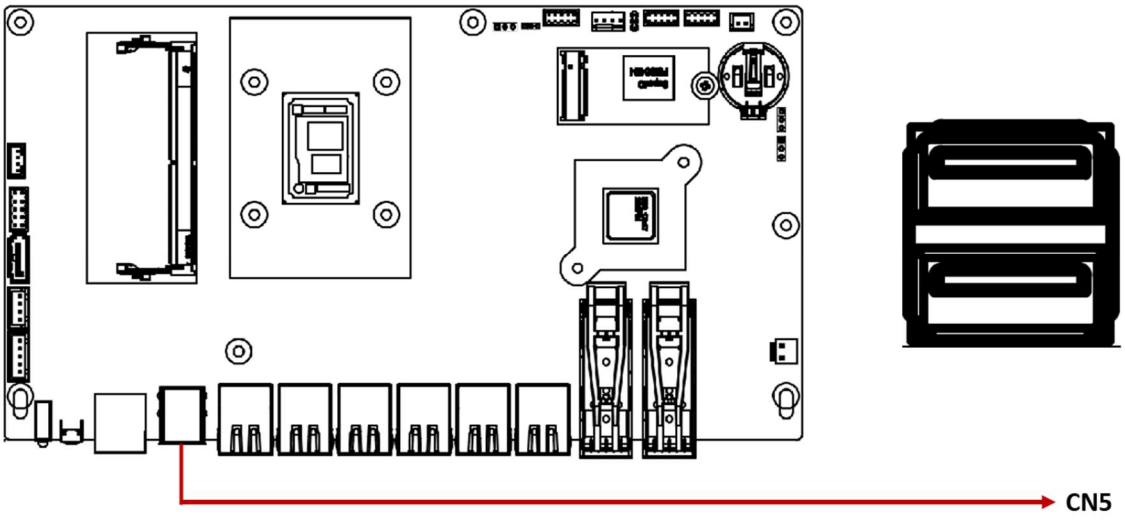
2.5.13 J12: LCM Connector



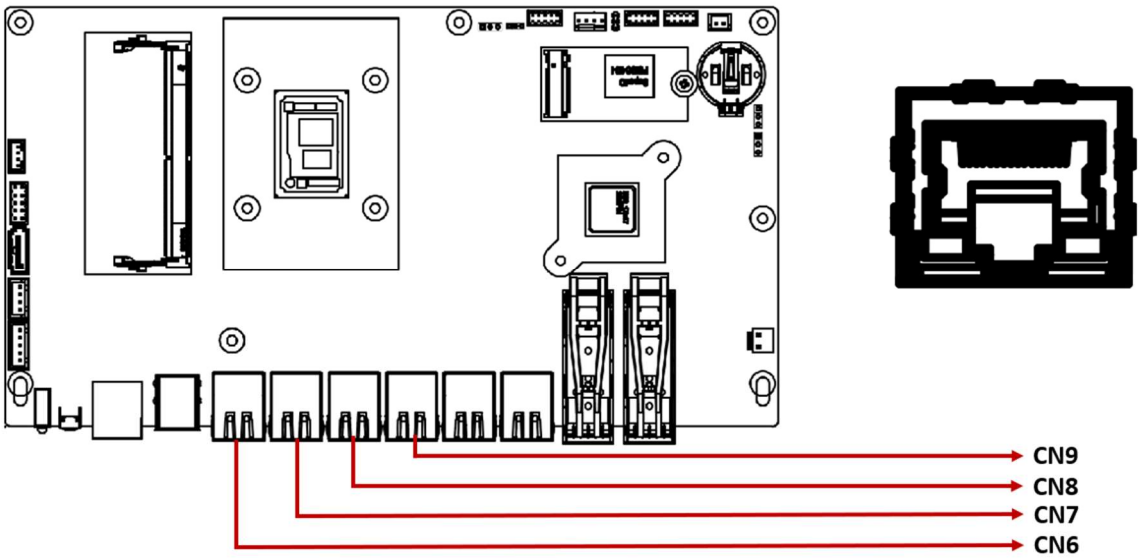
2.5.14 CN3, CN4: 2 x 1G Single Port SFP Connectors



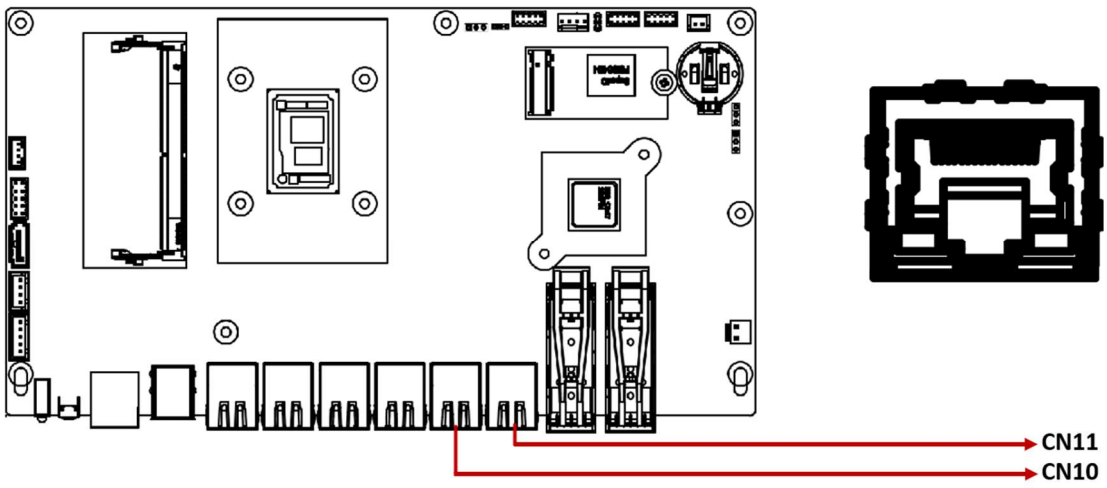
2.5.15 CN5: Dual Port USB 3.0/2.0 Connectors



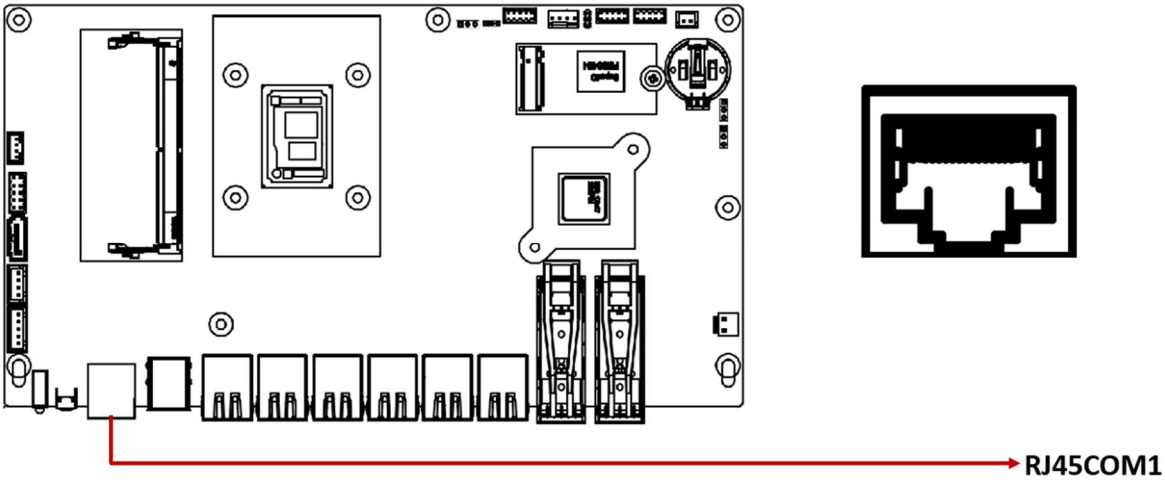
2.5.16 CN6, CN7, CN8, CN9:4 x 2.5G Single Port RJ45 Connectors



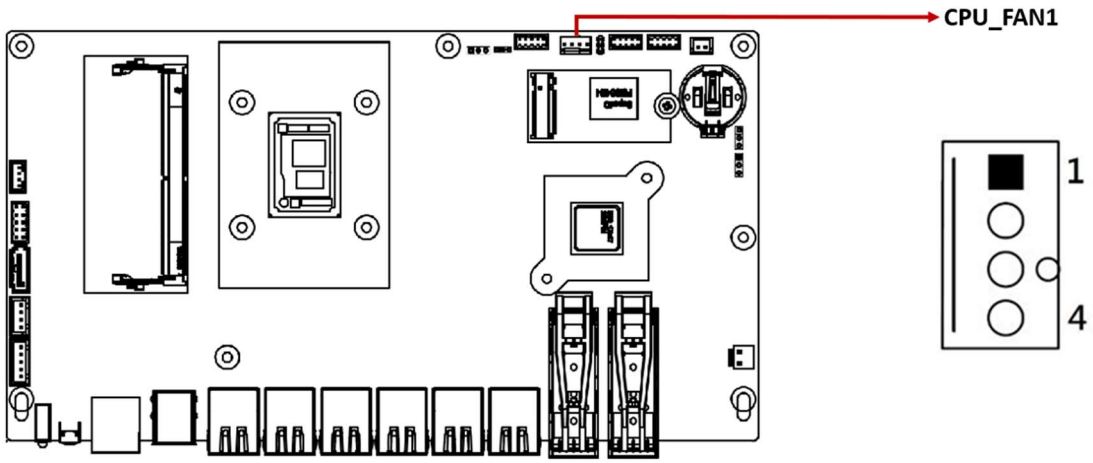
2.5.17 CN10, CN11: 2 x 1G Single Port RJ45 Connectors



2.5.18 RJ45COM1: Console Connector



2.5.19 CPU_FAN1: CPU Fan Power Connector



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

Chapter 3
BIOS Setup

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

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

3.1 Introduction

The BIOS (Basic Input/Output System) installed in the ROM of your computer system supports Intel® processors. The BIOS provides low-level support for standard devices such as disk drives and serial ports. It also includes password protection and options for fine-tuning the chipset that controls the entire system.

3.2 BIOS Setup

The BIOS includes a Setup utility program for specifying system configuration and settings. The Setup utility is stored in the system's BIOS ROM. When the computer is powered on, the BIOS is activated immediately. Pressing the <Del> key during startup allows you to enter the Setup utility. If you do not press the <Del> key in time, POST (Power-On Self Test) will continue and the Setup utility will not be invoked.

If you still need to enter Setup, restart the system by pressing the Reset button, pressing <Ctrl>+<Alt>+<Delete>, or by turning the system off and then back on.

The following message will appear on the screen:
Press <DEL> to Enter Setup

In general:

- Use the arrow keys to highlight items.
- Press <Enter> to select.
- Use <PgUp> and <PgDn> to change entries.
- Press <F1> for help.
- Press <Esc> to quit.

Warning: It is strongly recommended not to change the chipset defaults. These settings have been carefully chosen by AMI and your system manufacturer to ensure maximum performance and reliability. Modifying them may cause the system to become unstable or crash.

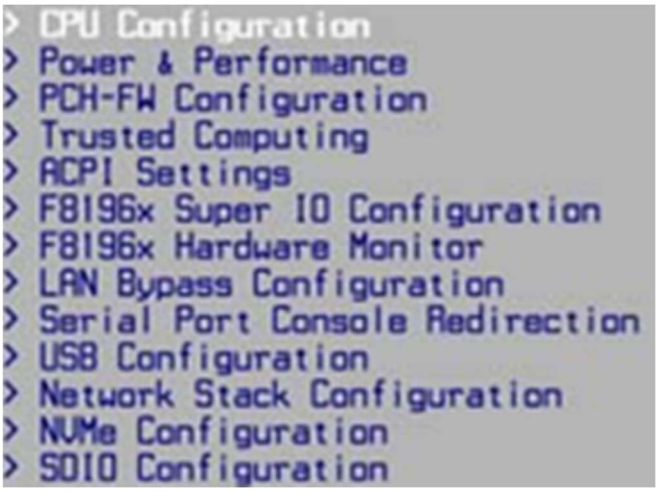
3.3 Main Settings

In the main settings section, the BIOS version and system memory information are shown. It also allows you to configure the date and time settings.

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

3.4 Advanced Settings

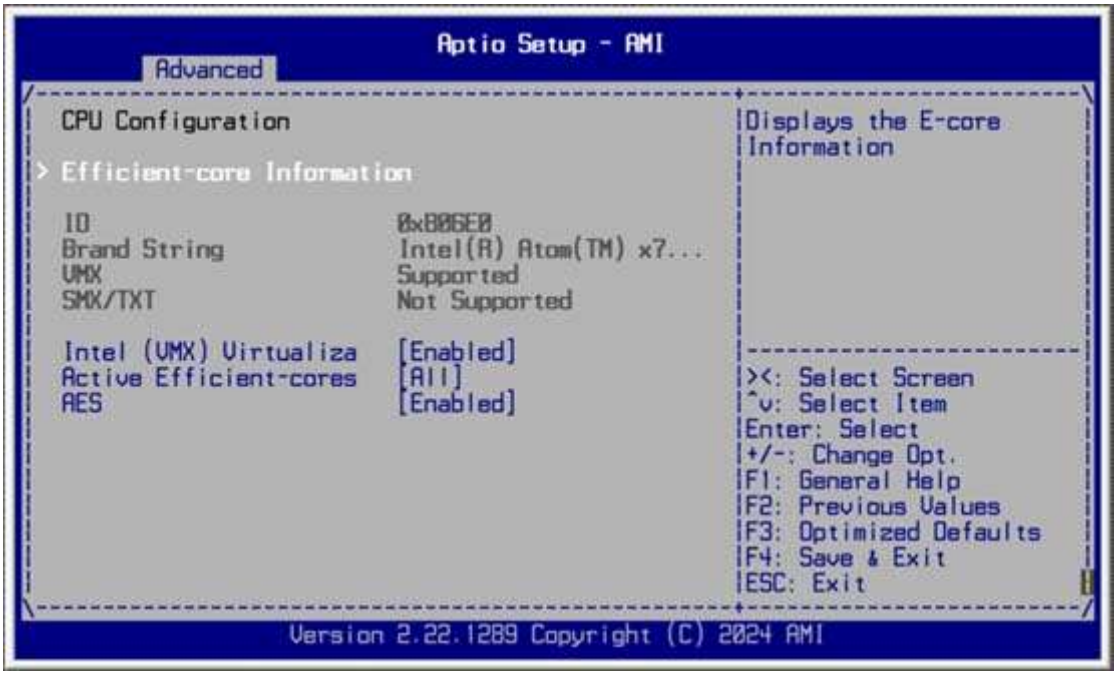
This section allows you to configure, improve your system and allows you to set up some system features according to your preference.



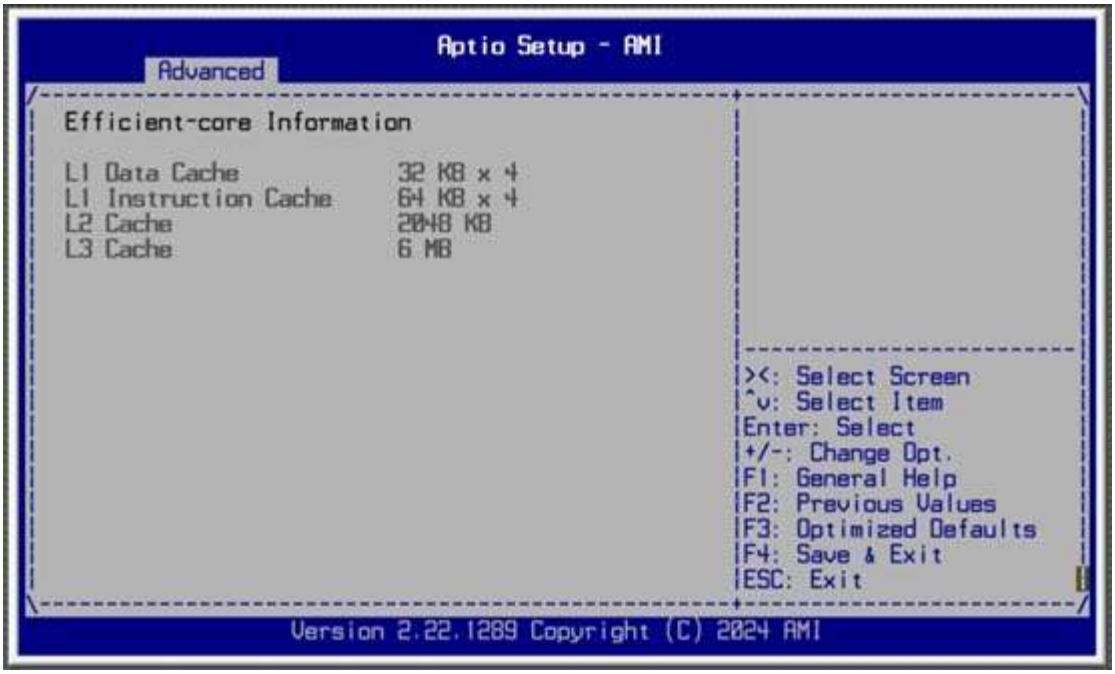
Advanced Menu (Top-Level Items)

1. CPU Configuration – Opens settings for CPU features such as virtualization, power-saving states, and core management.
2. Power & Performance – Adjusts processor power technology, speed scaling, and performance modes.
3. PCH-FW Configuration – Provides options for Intel® Management Engine (ME) firmware and related security features.
4. Trusted Computing – Configures TPM (Trusted Platform Module) settings for security and encryption.
5. ACPI Settings – Sets system power management behavior, such as sleep states and wake-up events.
6. F8196x Super IO Configuration – Configures Super I/O chip functions, such as serial/parallel ports and watchdog timer.
7. F8196x Hardware Monitor – Displays and controls system health information like temperatures, voltages, and fan speeds.
8. LAN Bypass Configuration – Configures LAN bypass functionality, used in network appliances to keep traffic flowing even during system faults.
9. Serial Port Console Redirection – Redirects BIOS and OS-level text output to a serial port for headless management.
10. USB Configuration – Manages USB ports, legacy USB support, and hand-off between BIOS and OS.
11. Network Stack Configuration – Enables network booting via PXE, with IPv4/IPv6 support.
12. NVMe Configuration – Displays attached NVMe SSDs and allows NVMe controller settings. (BIOS menu, if supported by firmware)
13. SDIO Configuration – Configures the Secure Digital I/O controller, used for SD/SDIO cards in embedded systems.

3.4.1 CPU Configuration

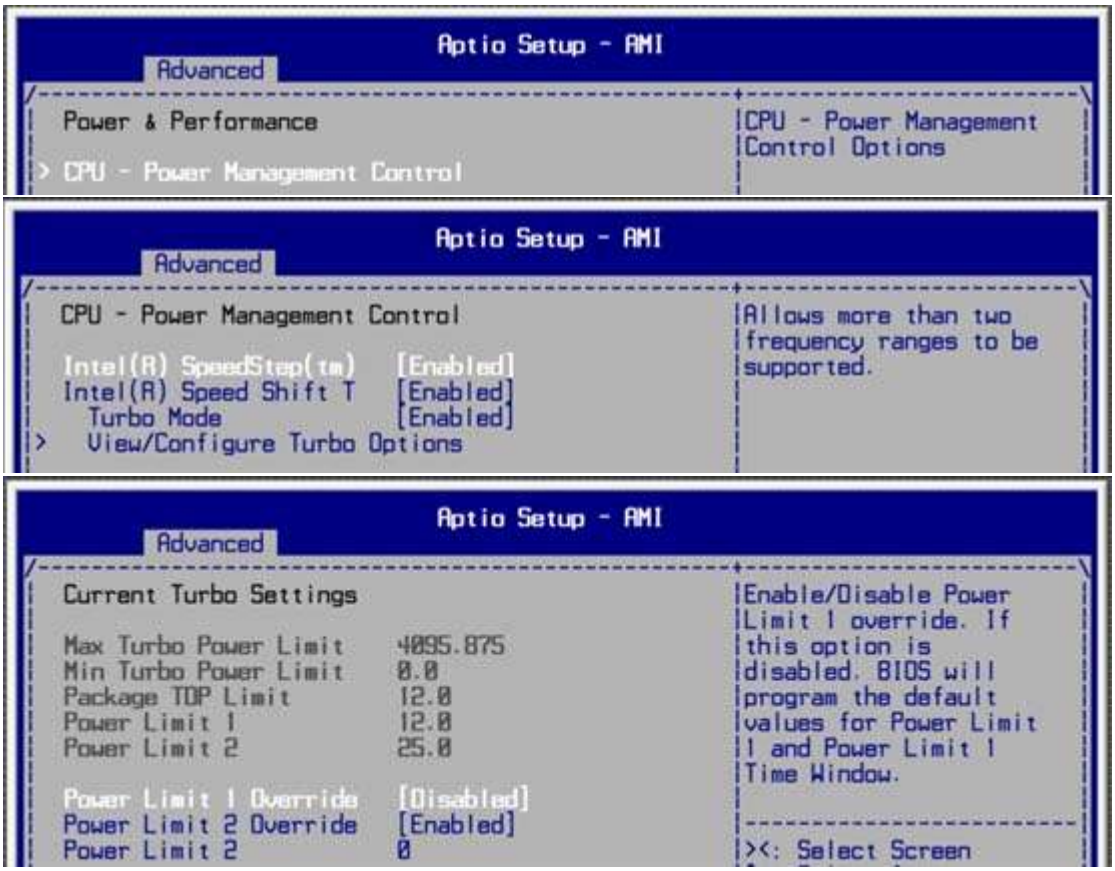


BIOS Setting	Description
Efficient-core Information	Displays details about the system's Efficient-cores (E-cores).
ID	Shows the processor identification number (hex value).
Brand String	Displays the processor model name (e.g., Intel® Atom™).
VMX	Indicates whether Intel® Virtualization Technology (VMX) is supported.
SMX/TXT	Indicates whether Intel® Trusted Execution Technology (TXT) is supported.
Intel (VMX) Virtualization Technology	Enables or disables Intel Virtualization Technology for running virtual machines.
Active Efficient-cores	Allows enabling or disabling specific Efficient-cores (E-cores) for power or performance optimization.
AES	Enables or disables the processor's AES (Advanced Encryption Standard) instruction set for hardware-accelerated encryption.



BIOS Setting	Description
L1 Data Cache	Shows the size of the Level 1 (L1) data cache per core (e.g., 32 KB × 4).
L1 Instruction Cache	Shows the size of the Level 1 (L1) instruction cache per core (e.g., 64 KB × 4).
L2 Cache	Displays the size of the Level 2 (L2) cache, typically shared by core clusters (e.g., 2048 KB).
L3 Cache	Displays the size of the Level 3 (L3) cache (Last Level Cache), shared among all cores (e.g., 6 MB).

3.4.2 Power & Performance



BIOS Setting	Description
Power & Performance	Opens the menu for processor power and performance settings.
CPU - Power Management Control	Opens options to configure CPU power management features.
Intel SpeedStep	Enables or disables Intel SpeedStep technology, which dynamically adjusts CPU frequency and voltage for power efficiency.
Intel Speed Shift	Enables or disables Intel Speed Shift technology, allowing the processor to control frequency and voltage for faster responsiveness.
Turbo Mode	Enables or disables Turbo Mode, which allows processor cores to run above their base operating frequency.
View/Configure Turbo Options	Opens submenu for viewing or configuring CPU Turbo settings.

Power Limit 1 Override	Enables/disables manual override of Power Limit 1 (PL1). If disabled, BIOS uses default PL1 value and time window.
Power Limit 2 Override	Enables/disables manual override of Power Limit 2 (PL2). If disabled, BIOS uses default PL2 value.
Power Limit 2	Sets the value for Power Limit 2 (PL2), the maximum turbo power limit the processor can draw for short durations.

3.4.3 PCH-FW Configuration

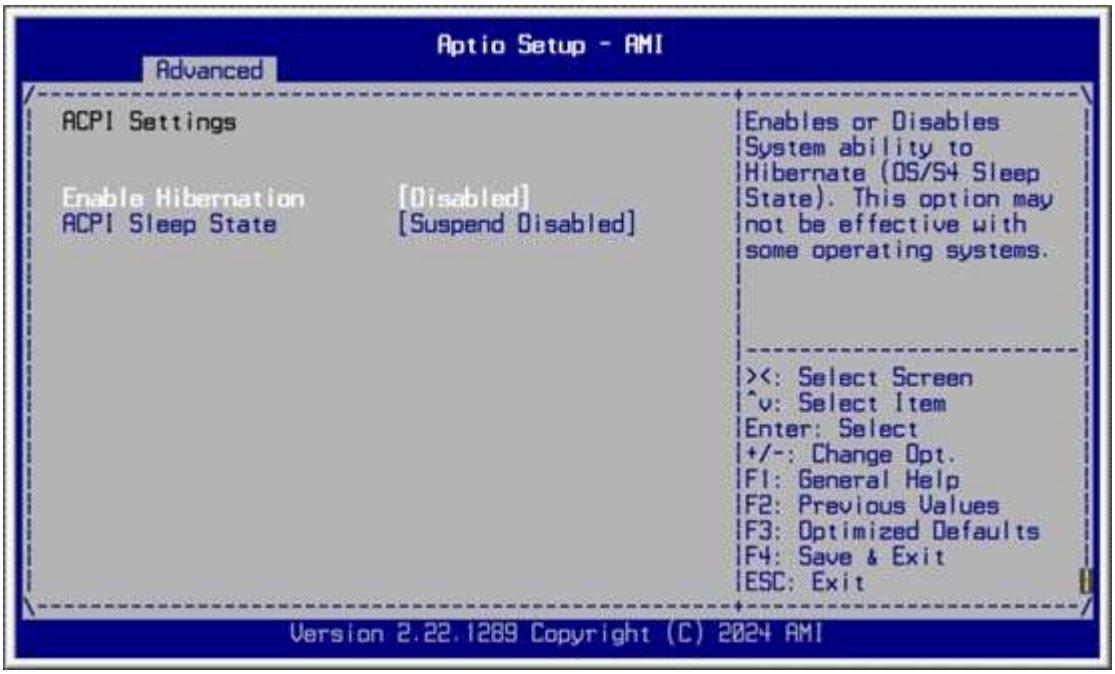
BIOS Setting	Description
ME Firmware Version	Displays the version number of the Intel Management Engine (ME) firmware installed on the system.
ME Firmware Mode	Indicates the current operating mode of the Intel ME firmware (e.g., Normal Mode, Recovery Mode).
ME Firmware SKU	Displays the SKU (Stock Keeping Unit) type of the ME firmware, which defines its feature set (e.g., Consumer, Corporate).

3.4.4 Trusted Computing

BIOS Setting	Description
TPM 2.0 Device Found	Indicates whether a TPM 2.0 device is detected in the system.
Firmware Version	Displays the firmware version of the TPM device.
Vendor	Shows the vendor or manufacturer of the TPM device (e.g., IFX).
Security Device Support	Enables or disables BIOS support for the TPM security device.
Active PCR Banks	Lists the currently active PCR (Platform Configuration Register) banks used for measurements.
Available PCR Banks	Displays the available PCR banks supported by the TPM device.
SHA256 PCR Bank	Enables or disables the SHA256 PCR bank for TPM measurements.
SHA384 PCR Bank	Enables or disables the SHA384 PCR bank for TPM measurements.
Pending Operation	Specifies if there is a pending TPM operation, such as clearing ownership.
Platform Hierarchy	Enables or disables the TPM platform hierarchy, which controls overall TPM access.
Storage Hierarchy	Enables or disables the TPM storage hierarchy for managing TPM storage keys.
Endorsement Hierarchy	Enables or disables the TPM endorsement hierarchy for authentication and identity keys.
Physical Presence Spec Version	Displays the version of the physical presence interface specification supported (e.g., 1.3).
TPM 2.0 Interface Type	Specifies the TPM interface type used (e.g., TIS).

Device Select	Selects which TPM device to use when multiple are available.

3.4.5 ACPI Settings

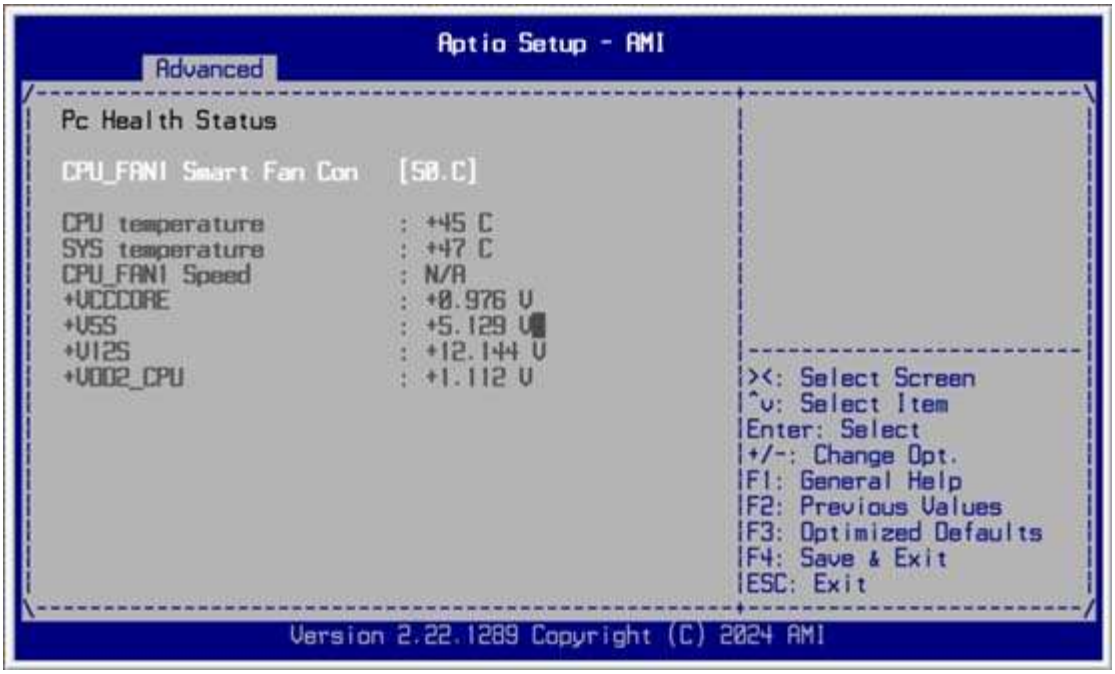


BIOS Setting	Description
Enable Hibernation	Enables or Disables System ability to Hibernate (OS/S4 Sleep State). This option may not be effective with some operating systems.
ACPI Sleep State	Suspend Disabled

3.4.6 F8196x Super IO Configuration

BIOS Setting	Description
F8196x Super IO Configuration	Opens configuration options for the Super IO chip (F8196x) and Serial Port (COMA).
Super IO Chip	Identifies the installed Super IO chip. (Fixed value: F8196x.)
Serial Port 1 Configuration	Opens settings for configuring Serial Port 1 (COMA).
Serial Port	Enables or disables Serial Port (COMA). Options: Enabled / Disabled. Default: Enabled.
Device Settings	Shows and allows adjustment of I/O address and IRQ used by the serial port. Default: I/O = 3F8h; IRQ = 4.
Change Settings	Sets how serial port resources are configured. Options: Auto (BIOS assigns resources) / Manual. Default: Auto.

3.4.7 F8196x Hardware Monitor

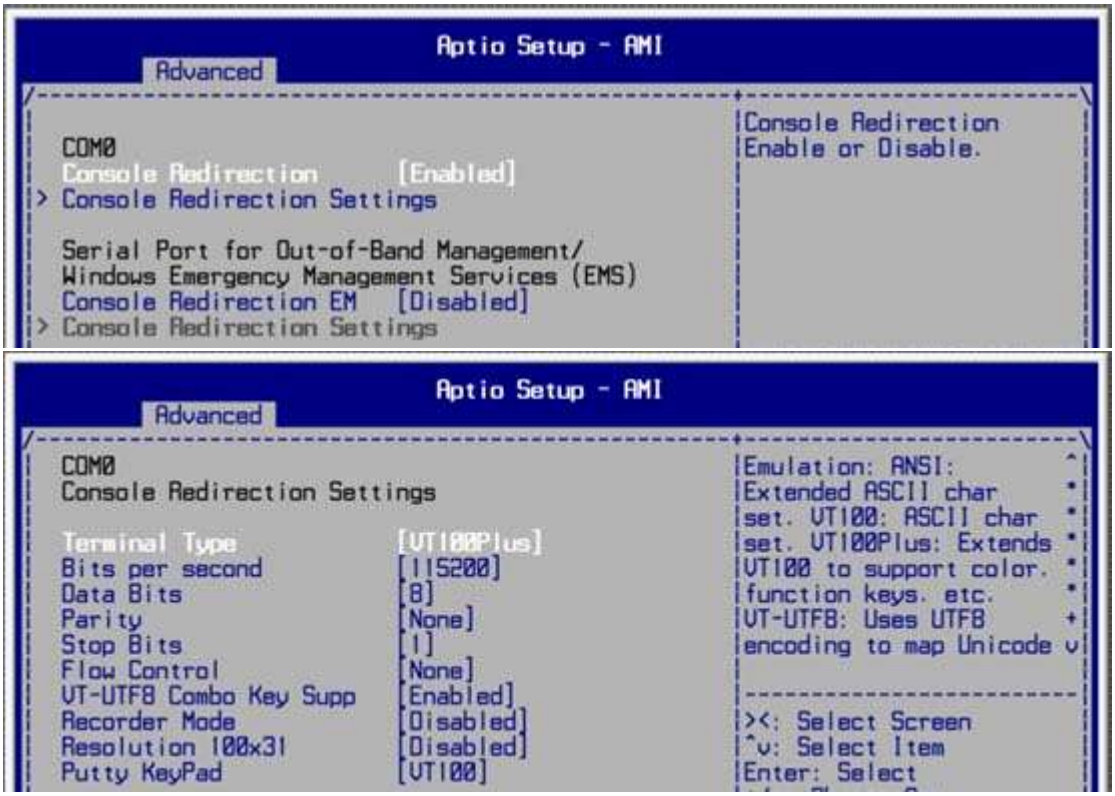


BIOS Setting	Description
Smart Fan Control	Disable or setting smart fan control start up temperature.
Temperatures / Voltages	These fields are the parameters of the hardware monitoring function feature of the motherboard. The values are read-only values as monitored by the system and show the PC health status.

3.4.8 LAN Bypass Configuration

BIOS Setting	Description
LAN Bypass Configuration	Opens configuration options for LAN bypass behavior.
Bypass Quick Setting	Sets LAN port behavior mode. Options: - Normal: All LAN ports operate normally. Watchdog Timer (WDT) monitors system hang and initiates a reboot. - Bypass: All LAN ports switch to bypass mode during power-off or when the WDT initiates a bypass.

3.4.9 Serial Port Console Redirection



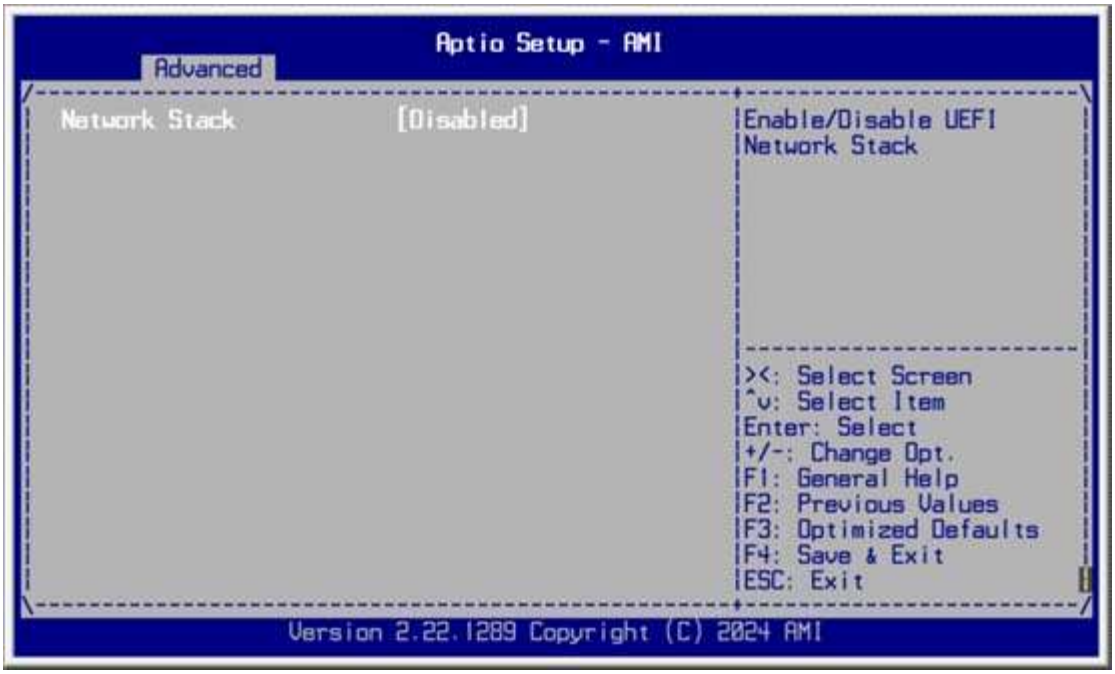
BIOS Setting	Description
Console Redirection	Allows you to enable or disable the console redirection feature.
Console Redirection Settings	These items become configurable only when you enable the Console Redirection item. The settings specify how the host computer and the remote computer (which the user is using) will exchange data. Both computers should have the same or compatible settings.
Terminal Type	Emulation: **ANSI:** Extended ASCII charset. **VT100:** ASCII charset. **VT100+:** Extends VT100 to support color, function keys, etc. **VT-UTF8:** Uses UTF8 encoding to map Unicode.
Bits per second	Selects serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds. Options: 9600, 19200, 38400, 57600, 115200
Data Bits	Options: 7, 8

Parity	A parity bit can be sent with the data bits to detect some transmission errors. Even: parity bit is 0 if the number of 1's in the data bits is even. Options: None, Even, Odd, Mark, Space
Stop Bits	Stop bits indicate the end of a serial data packet. (A start bit indicates the beginning). The standard setting is 1 stop bit. Options: 1, 2
Flow Control	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Options: None, Hardware RTS/CTS
VT-UTF8 Combo Key Support	Enables / Disables VT-UTFB combination key support for ANSI/VT100 terminals.
Recorder Mode	With this mode enabled, only text will be sent. This is to capture terminal data.
Resolution 100x31	Enables / Disables extended terminal resolution.
Putty Keypad	Select FunctionKey and keyPad on Putty. Options: VT100, LINUX, XTERMR6, SC0, ESCN, VT400

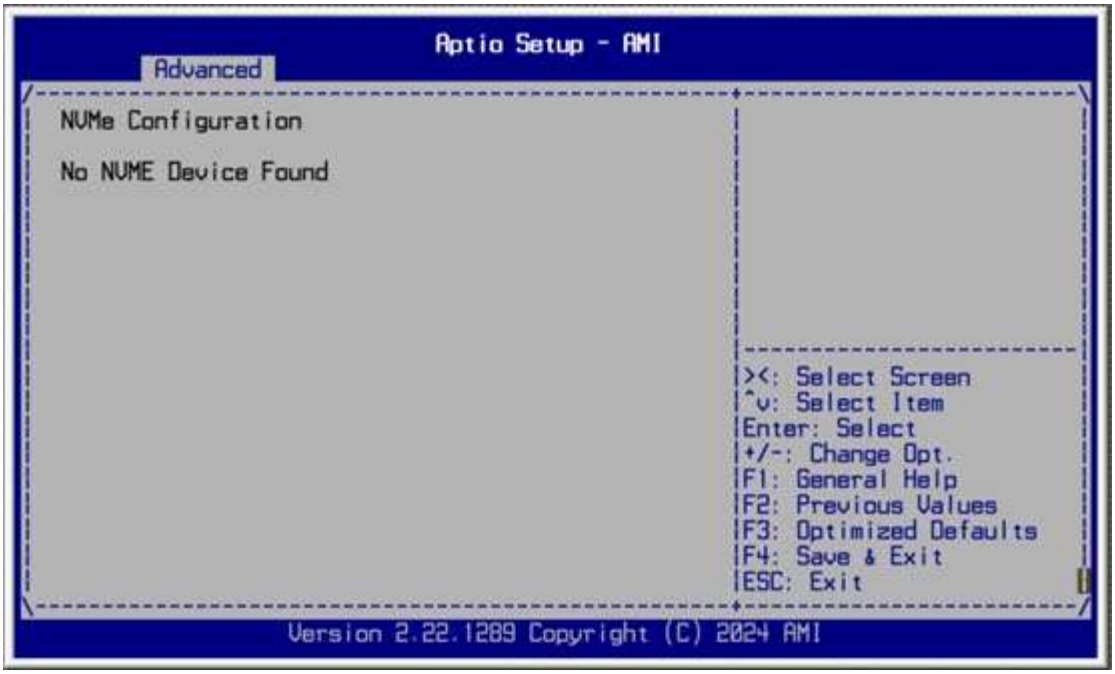
3.4.10 USB Configuration

BIOS Setting	Description
Legacy USB Support	• **Enable:** Enables Legacy USB Support. • **Auto:** Disables legacy support if no USB devices are connected. • **Disable:** Keeps USB devices available only for EFI applications.
XHCI Hand-off	This is a workaround for OSes without XHCI hand-off support. The XHCI ownership change should be claimed by XHCI driver.
USB Mass Storage Driver Support	Enables / Disables the support for USB mass storage driver.
USB Transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.
Device reset time-out	Seconds of delaying execution of start unit command to USB mass storage device.
Device power-up delay	The maximum time the device will take before it properly reports itself to the Host Controller. “Auto” uses default value for a Root port it is 100ms. But for a Hub port, the delay is taken from Hub descriptor.

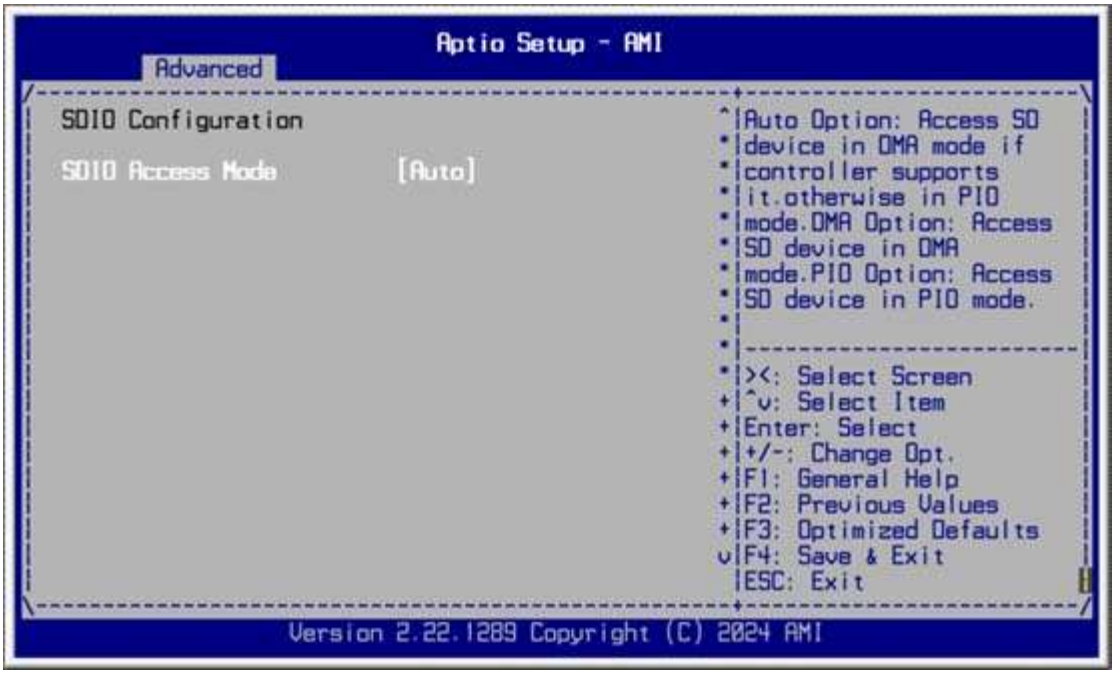
3.4.11 Network Stack



3.4.12 NVMe Configuration (BIOS menu, if supported by firmware)



3.4.13 SDIO Configuration



BIOS Setting	Description
SDIO Configuration	Opens configuration options for Secure Digital Input Output (SDIO) device settings.
SDIO Access Mode	Selects the access mode for SDIO devices. Options: - Auto: Uses DMA mode if supported by the controller; otherwise falls back to PIO mode. - DMA: Forces SDIO device to use Direct Memory Access mode. - PIO: Forces SDIO device to use Programmed Input/Output mode.

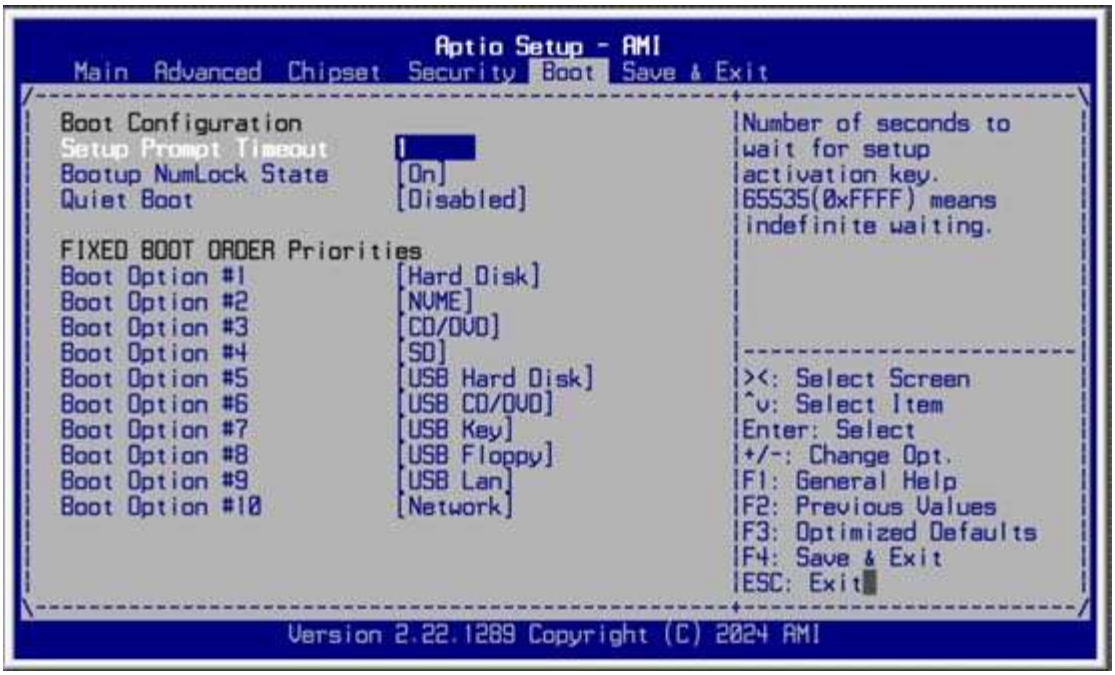
3.5 Chipset Configuration

BIOS Setting	Description
System Agent (SA) Configuration	Enables or disables Intel® Virtualization Technology for Directed I/O. Required for advanced virtualization and passthrough.
VT-d	Displays the current IMON value used for graphics turbo power management (read-only).
Graphics Configuration	Sets the Graphics Translation Table (GTT) memory size. Options: 2 MB / 4 MB / 8 MB.
Graphics Turbo IMON Current Value	Sets the aperture size for the graphics translation lookaside buffer (GTLB). Options typically: 128 MB / 256 MB / 512 MB.
GTT Size	Enables or disables PSMI (Power Saving Mode Interface) support for integrated graphics.
Aperture Size	Pre-allocates a fixed amount of system memory for integrated graphics. Options: 32 MB / 64 MB / 128 MB.
PSMI Support	Enables or disables the onboard SATA controller.
DVMT Pre-Allocated	Enables or disables Serial ATA Port 0.
PCH-IO Configuration	Enables or disables Serial ATA Port 1.
SATA Configuration	Selects the mode for the SATA controller. Options: AHCI / RAID (if supported).
SATA Controller(s)	Enables or disables hot-plug capability for SATA Port 0.
Serial ATA Port 0	Enables or disables hot-plug capability for SATA Port 1.
Serial ATA Port 1	Enables or disables the embedded MultiMediaCard (eMMC) 5.1 controller.
SATA Mode Selection	Enables or disables Intel® Virtualization Technology for Directed I/O. Required for advanced virtualization and passthrough.
Port 0 Hot Plug	Displays the current IMON value used for graphics turbo power management (read-only).
Port 1 Hot Plug	Sets the Graphics Translation Table (GTT) memory size. Options: 2 MB / 4 MB / 8 MB.
SCS Configuration	Sets the aperture size for the graphics translation lookaside buffer (GTLB). Options typically: 128 MB / 256 MB / 512 MB.
eMMC 5.1 Controller	Enables or disables PSMI (Power Saving Mode Interface) support for integrated graphics.

3.6 Security Settings

BIOS Setting	Description
Administrator Password	Sets a password that restricts access to the BIOS setup. If only the Administrator password is set, it limits access to setup only (prompted when entering BIOS). Password length: 3–20 characters.
User Password	Sets a power-on password that must be entered to boot or enter setup. When set, the user has Administrator rights inside BIOS. Password length: 3–20 characters.
Secure Boot	Enables or disables Secure Boot feature. Options: Enabled / Disabled. Default: Disabled. Requires platform keys to be enrolled.
Secure Boot Mode	Defines Secure Boot mode. Options: Standard / Custom. In Custom mode, keys can be manually managed.
Restore Factory Keys	Restores default Secure Boot keys.
Reset To Setup Mode	Clears Secure Boot keys and places the system in Setup Mode. Requires reboot.
Key Management	Opens the Secure Boot Key Management menu for enrolling, deleting, or viewing keys.
Platform Key (PK)	Defines the Platform Key (PK), which establishes the trust relationship for Secure Boot. Only one PK can be installed.
Key Exchange Keys (KEK)	Stores Key Exchange Keys (KEK), which are used to update PK and db/dbx contents. Multiple KEKs may be enrolled.
Authorized Signatures (db)	Contains the database of authorized signatures (db). Only signed executables and drivers listed here are allowed to run when Secure Boot is enabled.
Forbidden Signatures (dbx)	Contains the database of forbidden signatures (dbx). Executables or drivers listed here are blocked from loading.

3.7 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	Turns on/off the keyboard NumLock state.
Quiet Boot	Enables / Disables Quiet Boot option.
FIXED BOOT ORDER PRIORITIES	Sets the system boot order.

3.8 Save & Exit Settings

BIOS Setting	Description
Save Changes and Exit	Exit system setup after saving the changes.
Discard Changes and Exit	Exit system setup without saving the changes.
Save Changes and Reset	Save changes and reset the system.
Discard Changes and Reset	Discard changes and reset the system.
Save Changes	Save changes without exiting the setup.
Discard Changes	Discard changes without exiting the setup.
Restore Defaults	Restore factory default settings.
Save as User Defaults	Save current settings as user defaults.
Restore User Defaults	Restore previously saved user defaults.
Launch EFI Shell from filesystem device	Boots directly into the EFI shell if available on a filesystem device.