DFI

HPT193

Mini-ITX Industrial Motherboard

User's Manual

Copyright

Trademarks

FCC and DOC Statement on Class B

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio TV technician for help.

Notice:

1. The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
2. Shielded interface cables must be used in order to comply with the emission limits.

Table of Contents

About this Manual

This manual can be downloaded from the website.

The manual is subject to change and update without notice, and may be based on editions that do not resemble your actual products. Please visit our website or contact our sales representatives for the latest editions.

Warranty

1. Warranty does not cover damages or failures that arise from misuse of the product, inability to use the product, unauthorized replacement or alteration of components and product specifications.
2. The warranty is void if the product has been subjected to physical abuse, improper installation, modification, accidents or unauthorized repair of the product.
3. Unless otherwise instructed in this user's manual, the user may not, under any circumstances, attempt to perform service, adjustments or repairs on the product, whether in or out of warranty. It must be returned to the purchase point, factory or authorized service agency for all such work.
4. We will not be liable for any indirect, special, incidental or consequential damages to the product that has been modified or altered.

Static Electricity Precautions

It is quite easy to inadvertently damage your PC, system board, components or devices even before installing them in your system unit. Static electrical discharge can damage computer components without causing any signs of physical damage. You must take extra care in handling them to ensure against electrostatic build-up.

1. To prevent electrostatic build-up, leave the system board in its anti-static bag until you are ready to install it.
2. Wear an antistatic wrist strap.
3. Do all preparation work on a static-free surface.
4. Hold the device only by its edges. Be careful not to touch any of the components, contacts or connections.
5. Avoid touching the pins or contacts on all modules and connectors. Hold modules or connectors by their ends.

Important:

Electrostatic discharge (ESD) can damage your processor, disk drive and other components. Perform the upgrade instruction procedures described at an ESD workstation only. If such a station is not available, you can provide some ESD protection by wearing an antistatic wrist strap and attaching it to a metal part of the system chassis. If a wrist strap is unavailable, establish and maintain contact with the system chassis throughout any procedures requiring ESD protection.

Safety Measures

- To avoid damage to the system, use the correct AC input voltage range.
- To reduce the risk of electric shock, unplug the power cord before removing the system chassis cover for installation or servicing. After installation or servicing, cover the system chassis before plugging the power cord.

About the Package

The package contains the following items. If any of these items are missing or damaged, please contact your dealer or sales representative for assistance.

- 1 HPT193 motherboard
- 1 I/O shield

Note: The items are subject to change in the developing stage.

The board and accessories in the package may not come similar to the information listed above. This may differ in accordance with the sales region or models in which it was sold. For more information about the standard package in your region, please contact your dealer or sales representative.

Before Using the System Board

When installing the system board in a new system, you will need at least the following internal components.

- Power adapter

External system peripherals may also be required for navigation and display, including at least a keyboard, a mouse and a video display monitor.

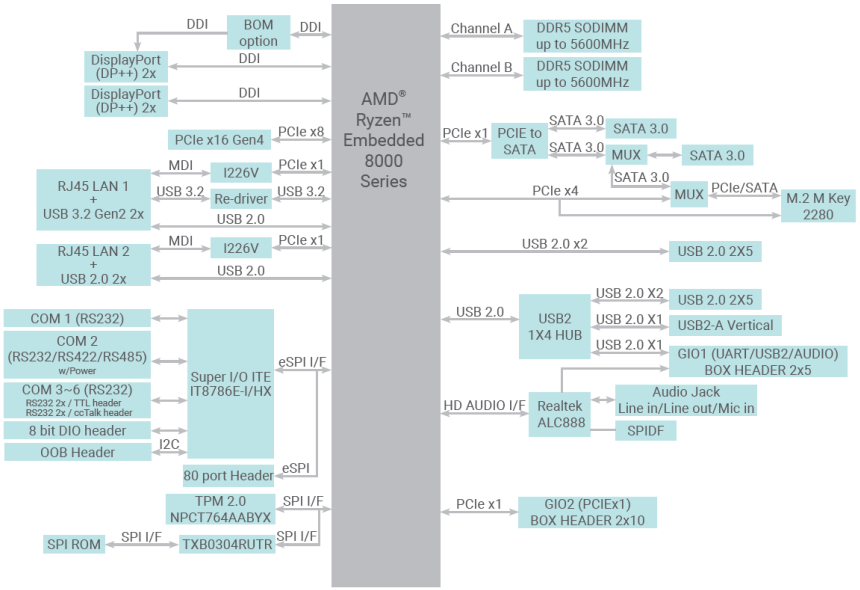
Chapter 1 - Introduction

▶ Specifications

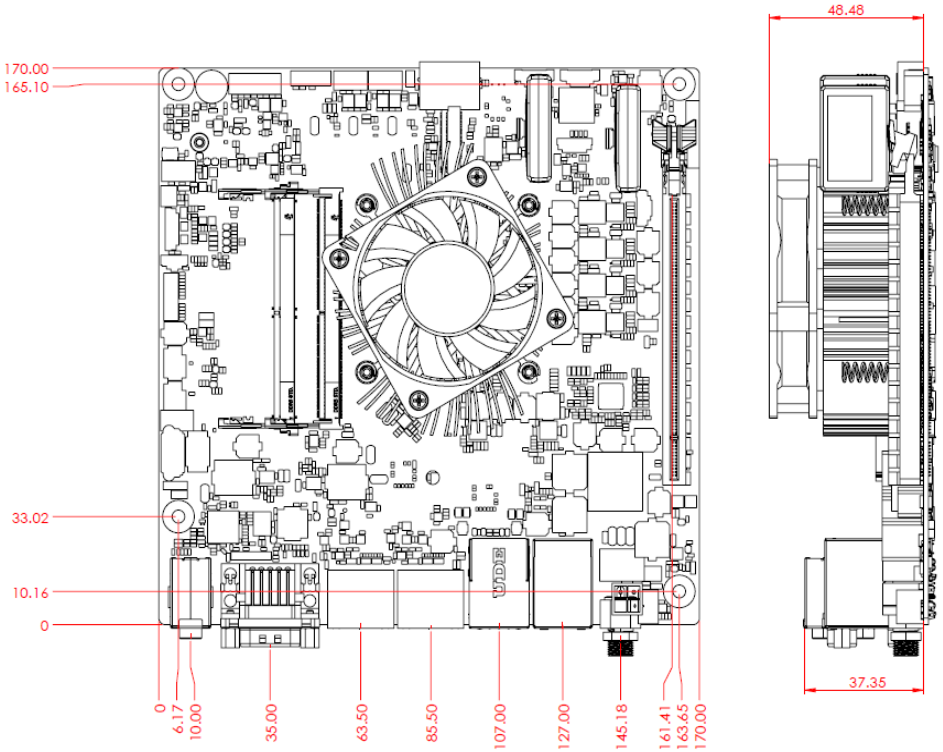
SYSTEM	Processor	AMD® Ryzen™ Embedded 8000 Series Processors, TDP up to 54W AMD® Ryzen™ Embedded 8845HS, 8C/16T, 8MB Cache, 3.8GHz (5.1GHz), 45W (35-54W) AMD® Ryzen™ Embedded 8645HS, 6C/12T, 6MB Cache, 4.3GHz (5.0GHz), 45W (35-54W) AMD® Ryzen™ Embedded 8840U, 8C/16T, 8MB Cache, 3.3GHz (5.1GHz), 28W (15-30W) AMD® Ryzen™ Embedded 8640U, 6C/12T, 6MB Cache, 3.5GHz (4.9GHz), 28W (15-30W)
	Memory	2 x 262-pin dual-channel SODIMM DDR5 5600/5200/4800MHz with ECC/non-ECC support up to 96GB (48GB per Dimm)
	BIOS	AMI SPI 256Mbit
GRAPHICS	Controller	RDNA3 graphics with up to 6 WGPs (Work Group processors)
	Display	4 x DP++ display **DP1.2**: resolution up to 3840x2160@60Hz
	Quad Displays	4 x DP++ display
EXPANSION	PCIE Slot	1 x PCIE Gen4 x16 slot (x8 Signal)
	M.2	1 x M.2 M Key 2280 slot (PCIE Gen4 x4 or SATA3)
	eMMC	1 x eMMC B2B header, Support DFI eMMC module
	Gaming I/O	GIO1 (UART, USB2, AUDIO R/L) GIO2 (PCIE x1)
AUDIO	Audio Codec	1 x Realtek ALC888S
ETHERNET	Controller	2 x Intel I226-V (10/100/1000/2500 Mbps)
REAR I/O	Ethernet	2 x 2.5GbE (RJ-45)
	USB	2 x USB 3.2 Gen2 2 x USB 2.0
	Display	4 x DP++ display
	Audio	1 x Front audio (Line-out, Line-in, Mic-in)
	Serial	1 x Full RS232 1 x RS232/RS422/RS485

INTERNAL I/O	Serial	2 x RS232 / TTL header 2 x RS232 / ccTalk header
	USB	4 x USB 2.0 port (pitch 2.0mm) 1 x USB 2.0 vertical Type A
	SATA	2 x SATA3 (6Gb/s) (one signal shared with M.2 M key, selected by BIOS) 2 x SATA Power
	DIO	1 x 8-bit header with power
	Case Open	1 1x2p header
	Audio	1 x S/PDIF (audio in & out) (Signal from ALC888S)
	SMBus/ I2C	2 x I2C 1 x SPI
WATCHDOG TIMER	Output & Interval	System Reset, Programmable via Software from 1 to 255 Seconds
SECURITY	TPM	dTPM 2.0(Default), fTPM (Option)
POWER	Type	Single 12~24V +/-5% DC
	Connector	DC-in Jack (Request) Straight Type Connector (4-pin) (Default)
	Consumption	TBD
	RTC Battery	CR2032 coin cell
OS SUPPORT	Microsoft	Windows 11 22H2 GAC Windows 11 LTSC
	Linux	Ubuntu 22.04
ENVIRONMENT	Temperature	Operating: -5 to 65°C Storage: -40 to 85°C
	Humidity	10 to 90% RH
	MTBF	TBD
MECHANICAL	Dimensions	Mini-ITX Form Factor 195mm (7.7") x 170mm (6.7")
	Height	PCB: 1.6mm Top Side: TBD Bottom Side: TBD
CERTIFICATIONS	Certifications	CE, FCC, RoHS

▶ Block Diagram

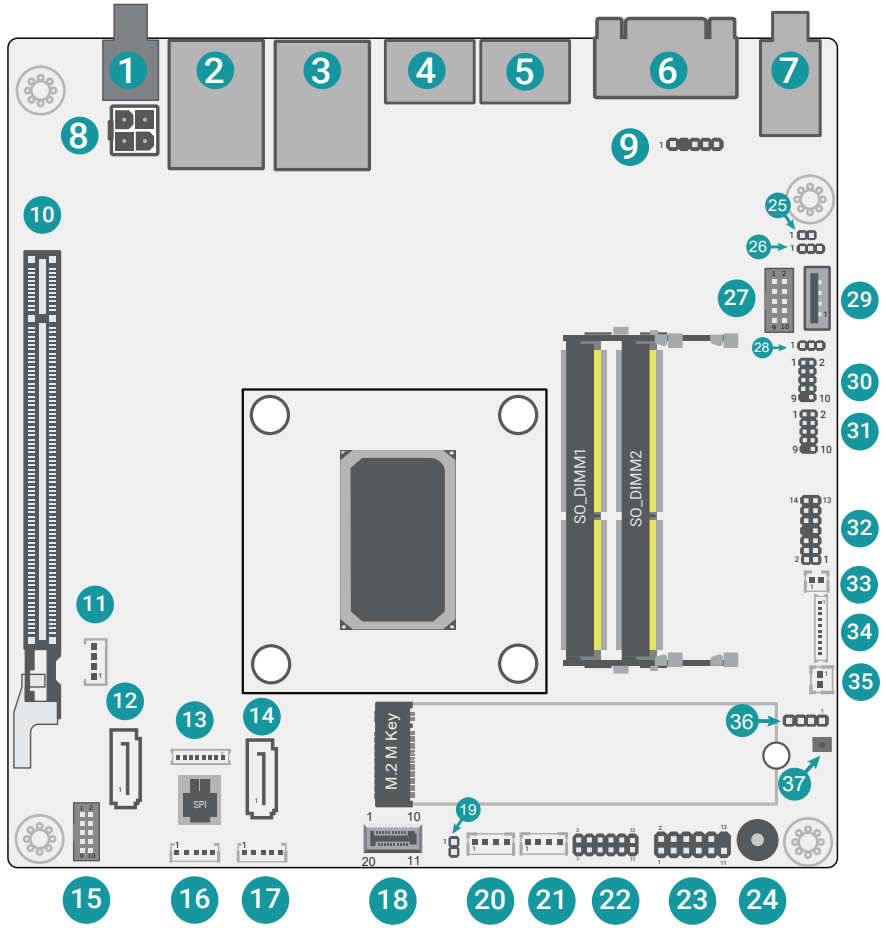


▶ Dimension



Chapter 2 - Hardware Installation

▶ Board Layout



1. 12~24V DC-in (BOM optional)
2. ▲LAN1
   ▼USB3.2 Gen2
3. ▲LAN2
   ▼USB2.0
4. 2xDP++
5. 2xDP++
6. ▲COM1
   ▼COM2
7. ▲Line In
   ▼Line Out
   ▼Mic In
8. 12~24V ATX
9. S/PDIF
10. PCIex8 Gen4
11. CPU Fan
12. SATA1
13. SMB & I2C
14. SATA0
15. COM3/4/5
16. SATA Power
17. SATA Power
18. PCIex1 with PWR
19. BIOS W/P function
20. C.C.Talk2
21. C.C.Talk1
22. COM3/4/5 (Jumper Setting)
23. Front Panel
24. Buzzer
25. COM2 Output (Jumper Setting)
26. COM2 Output (Jumper Setting)
27. for GM903 (USB2.0/UART/AUDIO)
28. COM6 (Jumper Setting)
29. USB2_1
30. USB2_6/7
31. USB2_8/9
32. eSPI
33. RTC Battery
34. DIO
35. CaseOpen
36. System FAN
37. Clear CMOS

▶ Installing the heat sink

Installing the Heat Sink

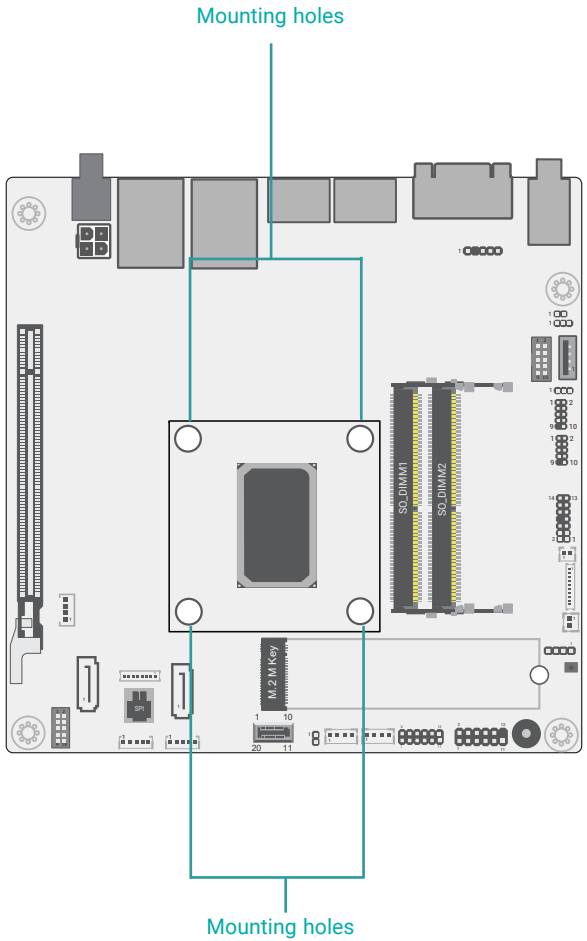
The CPU must be kept cool by using a heat sink, otherwise the CPU will overheat damaging both the CPU and system board.

1. Before you install the fan / heat sink, you must apply a thermal paste onto the top of the CPU. The thermal paste is usually supplied when you purchase the fan / heat sink assembly. Do not spread the paste all over the surface. When you later place the heat sink on top of the CPU, the compound will disperse evenly.

   Some heat sinks come with a patch of preapplied thermal paste. Do not apply thermal paste if the fan / heat sink already has a patch of thermal paste on its underside. Peel the strip that covers the paste before you place the fan / heat sink on top of the CPU.

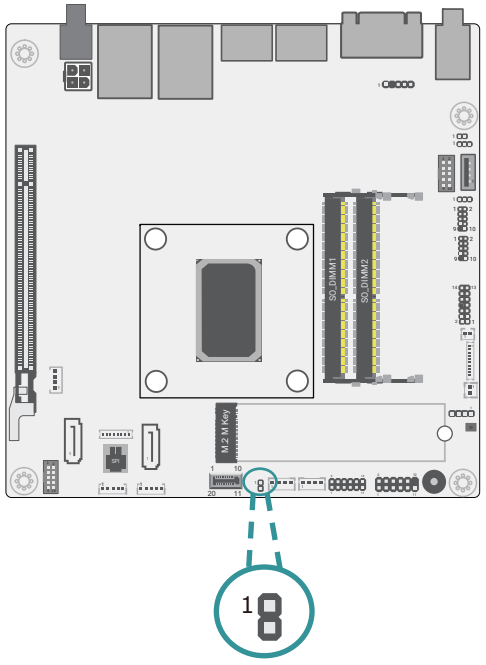
2. Place the heat sink on top of the CPU. The 4 spring screws around the heat sink, which are used to secure the heat sink onto the system board, must match the 4 mounting holes around the board.

3. Screw tight two of the spring screws at opposite corners into the mounting holes. And then proceed with the other two spring screws.



▶ Jumper Settings

BIOS W/P Function (JBJ1)

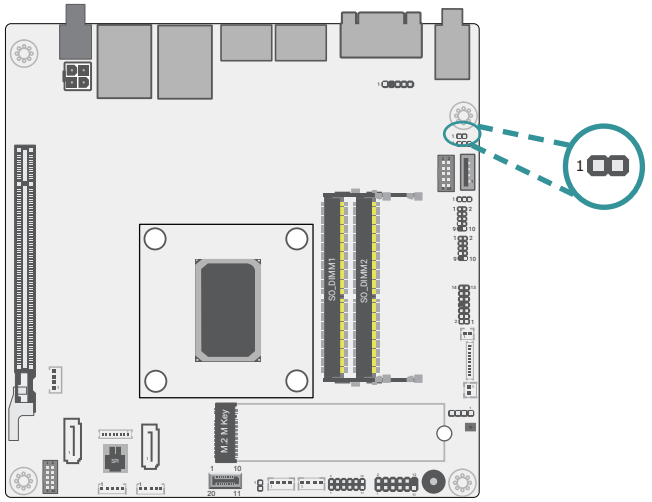


- 1-2 On: R/W
- 2-3 Off: Read only (@W/P)

Note:

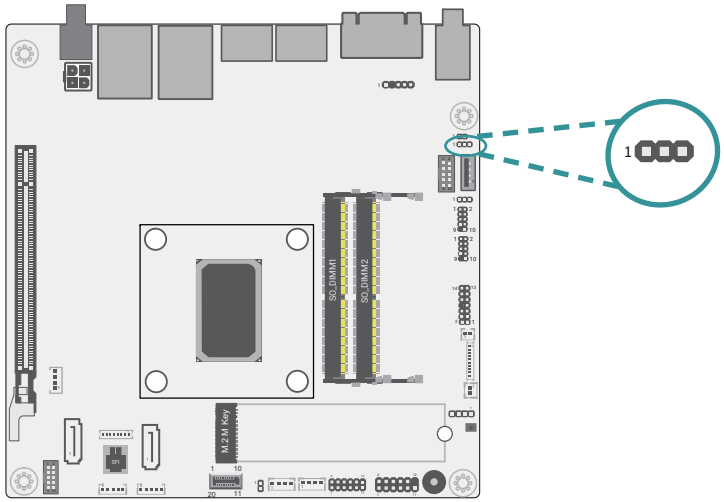
Please remove JBJ1 to activate BIOS W/P function. Please be noted that if there is any changes of W/P status, from Enable to Disable or from Disable to Enable, the system must be SHUT DOWN first before adjusting JBJ1.
BIOS cannot be updated when W/P is activated.

COM2 Output (RIJ1)



- 1-2 On: RI-

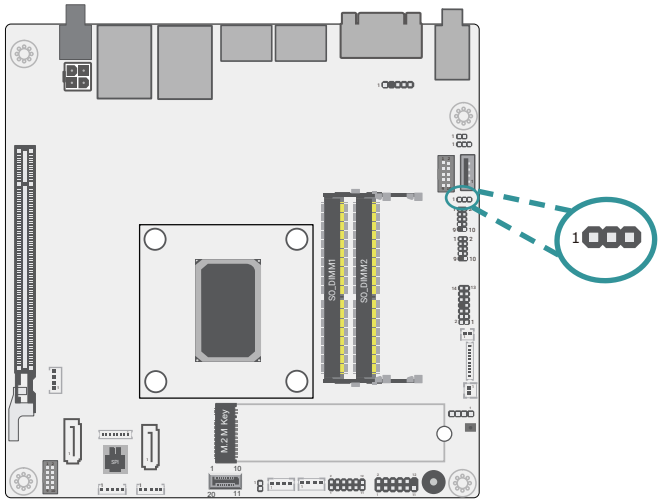
COM2 Output (JP16)



■ 1-2 On: 5V (Default)

■ 2-3 On: 12V

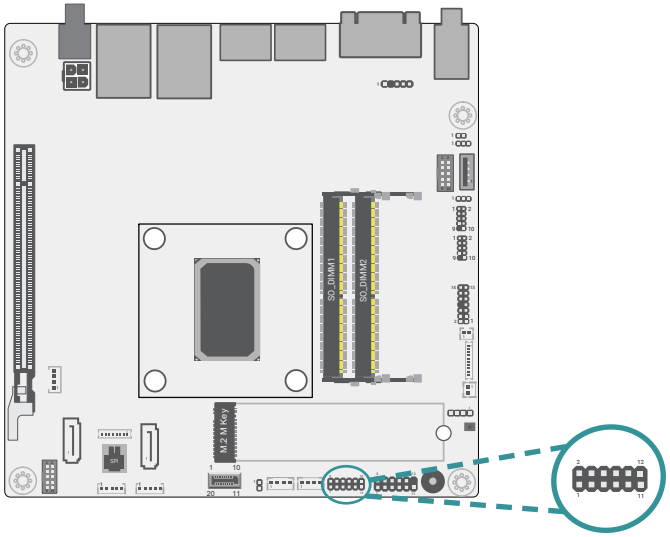
COM6 (JP5)



■ 1-2 On: Simple RS232 @TSJ1

■ 2-3 On: GM903 Host-Link (default)

COM3/4/5 (JPS1)



■ 1-3, 2-4 On:
RS232(COM3) (Default)

■ 3-5, 4-5 On:
TTL-5V(COM3)

■ 7-9 On:
RS232(COM4) (Default)

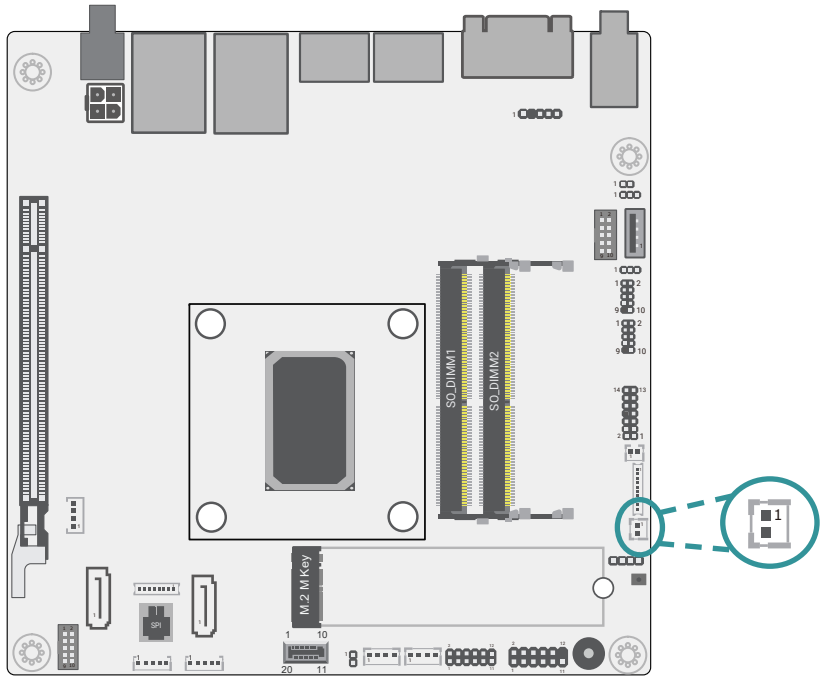
■ 8-10 On:
RS232(COM5) (Default)

■ 9-11On:
C.C.Talk(COM4)

■ 10-12 On:
C.C.Talk(COM5)

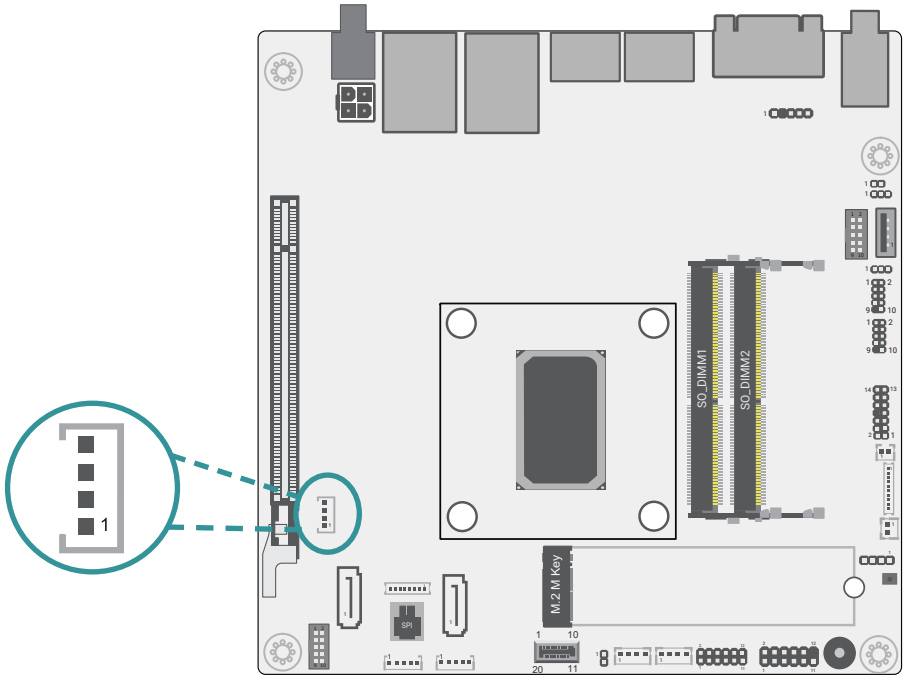
▶ PIN Assignment

CASEOPEN (SOJ1)



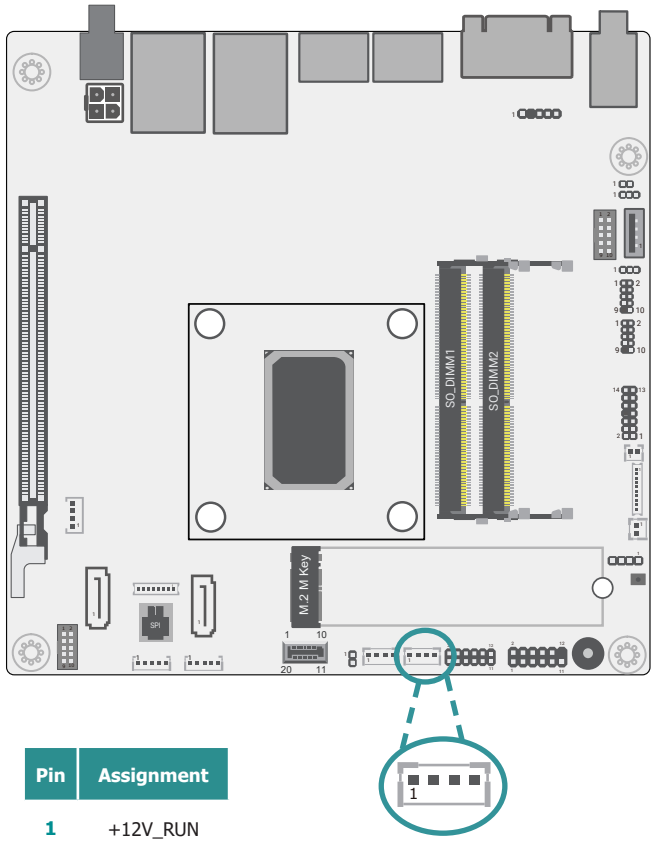
Pin	Function	Pin	Function
1	CASEOPEN#	2	GND

CPU Fan (CN10)



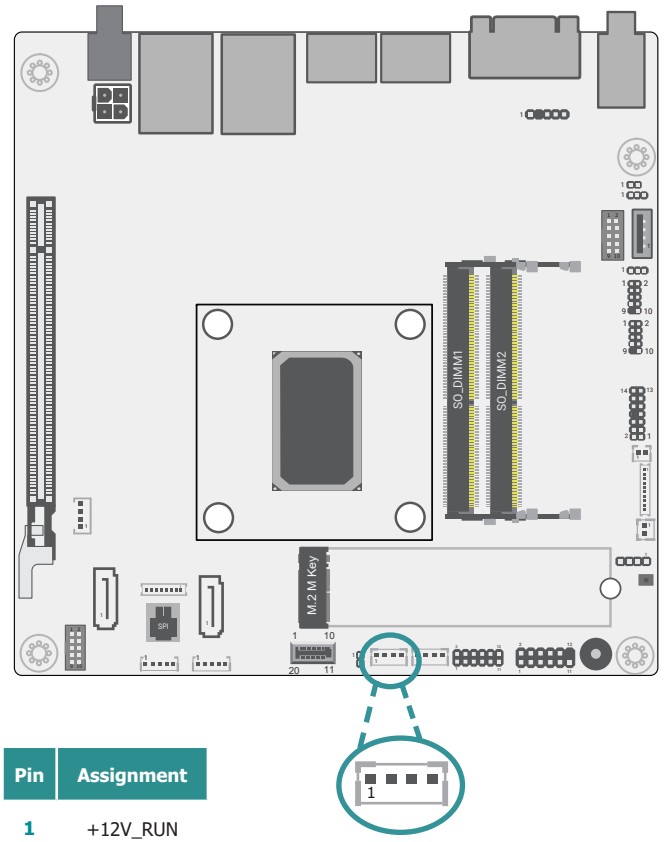
Pin	Assignment
1	GND
2	12V
3	RPM
4	CTRL

C.C.Talk (CN8)



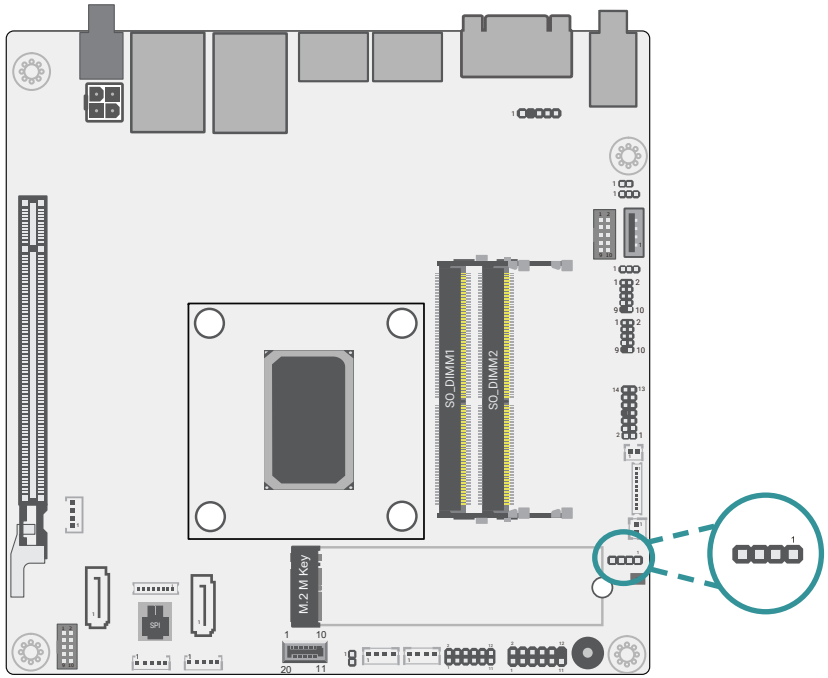
Pin	Assignment
1	+12V_RUN
2	+12V_RUN
3	GND
4	CCTALK_CH1

C.C.Talk (CN9)



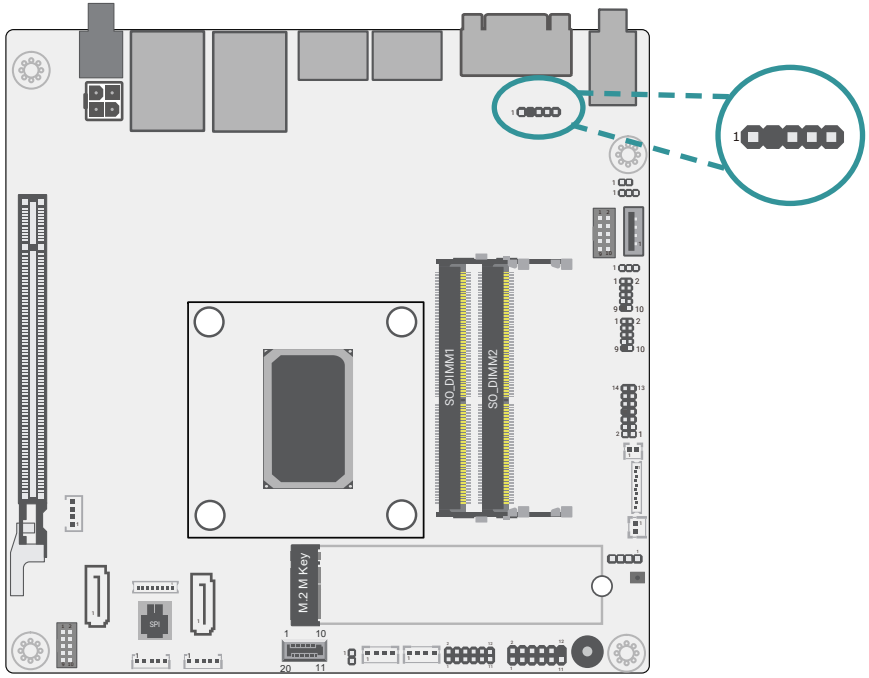
Pin	Assignment
1	+12V_RUN
2	+12V_RUN
3	GND
4	CCTALK_CH2

System Fan (J16)



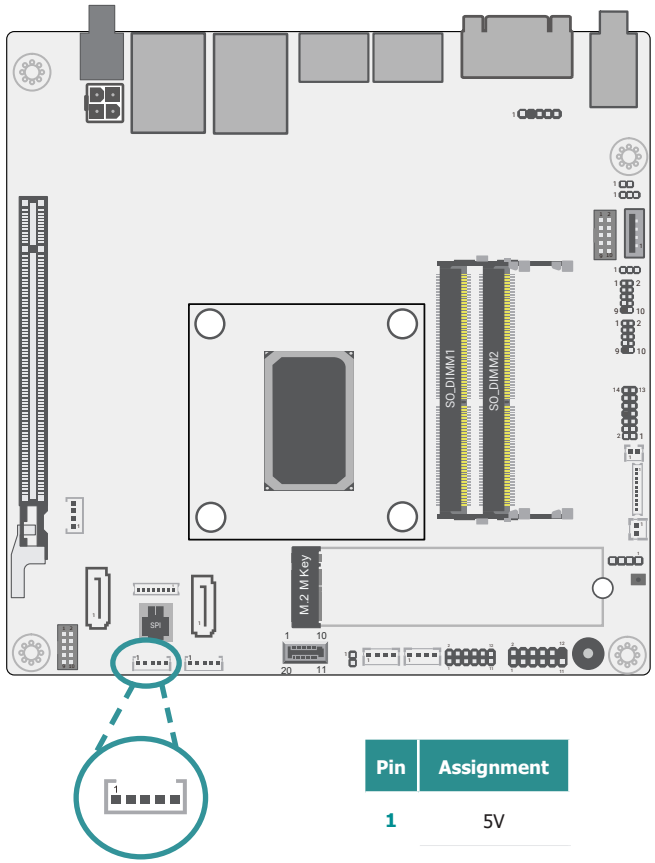
Pin	Assignment
1	GND
2	12V
3	RPM
4	CTRL

SPDIF (AUJ1)



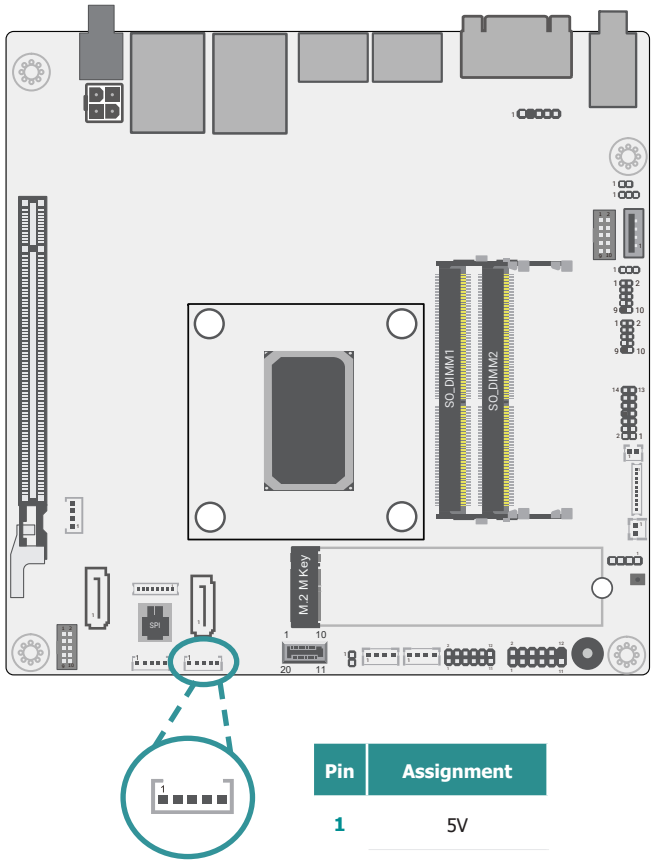
Pin	Assignment
1	+5V_RUN
2	NA
3	S/PDIF-OUT
4	GND
5	S/PDIF-IN

SATA POWER (J6)



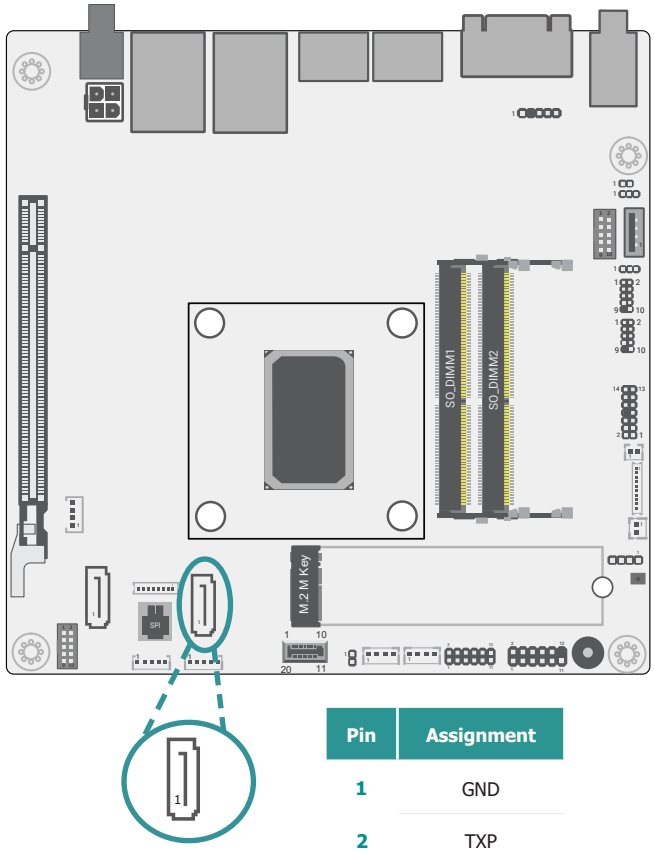
Pin	Assignment
1	5V
2	5V
3	12V
4	GND
5	GND

SATA POWER (J9)



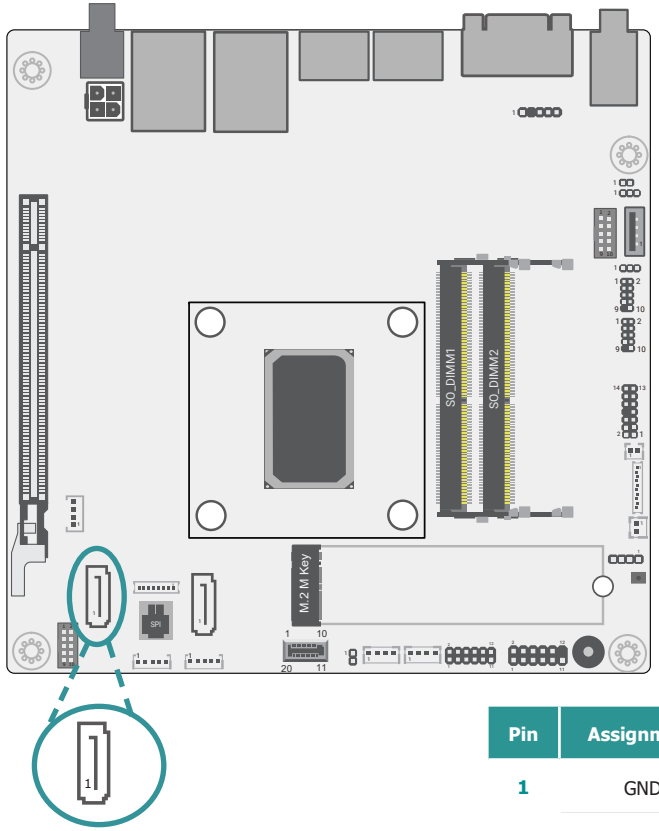
Pin	Assignment
1	5V
2	5V
3	12V
4	GND
5	GND

SATA0 (J7)



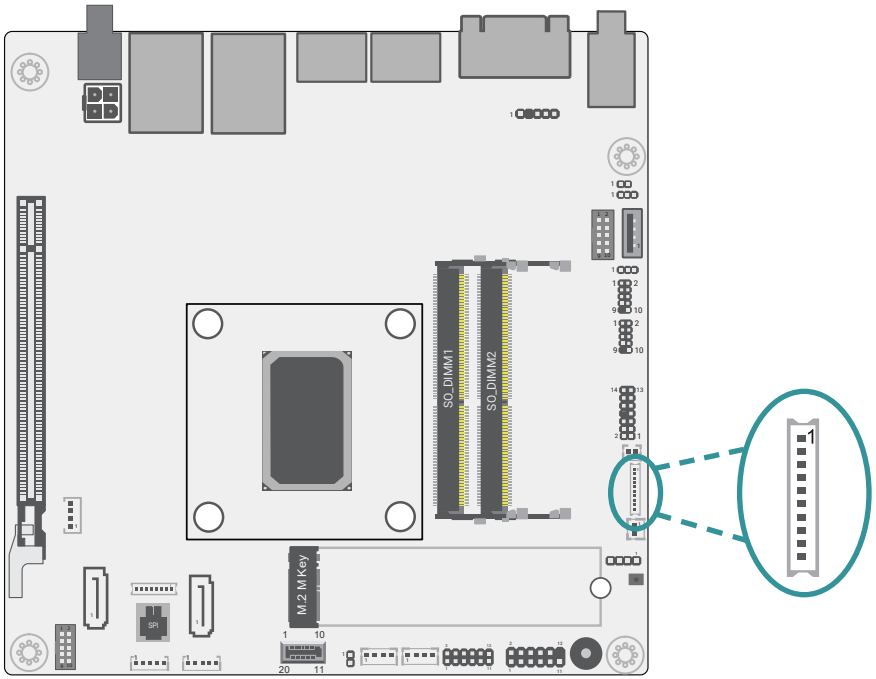
Pin	Assignment
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND or +5V(SATADOM)

SATA1 (J8)



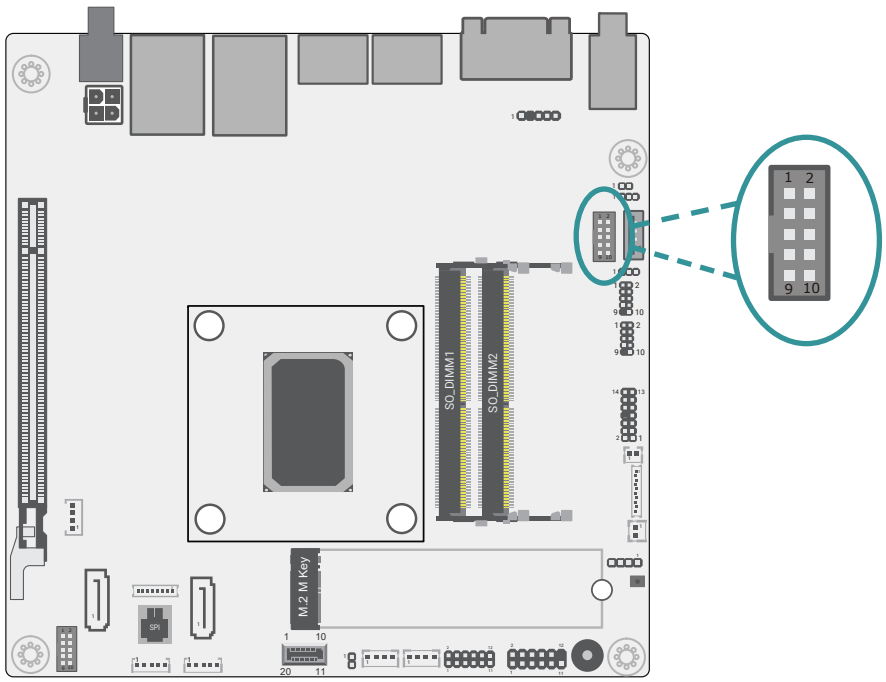
Pin	Assignment
1	GND
2	TXP
3	TXN
4	GND
5	RXN
6	RXP
7	GND or +5V(SATADOM)

DIO (J18)



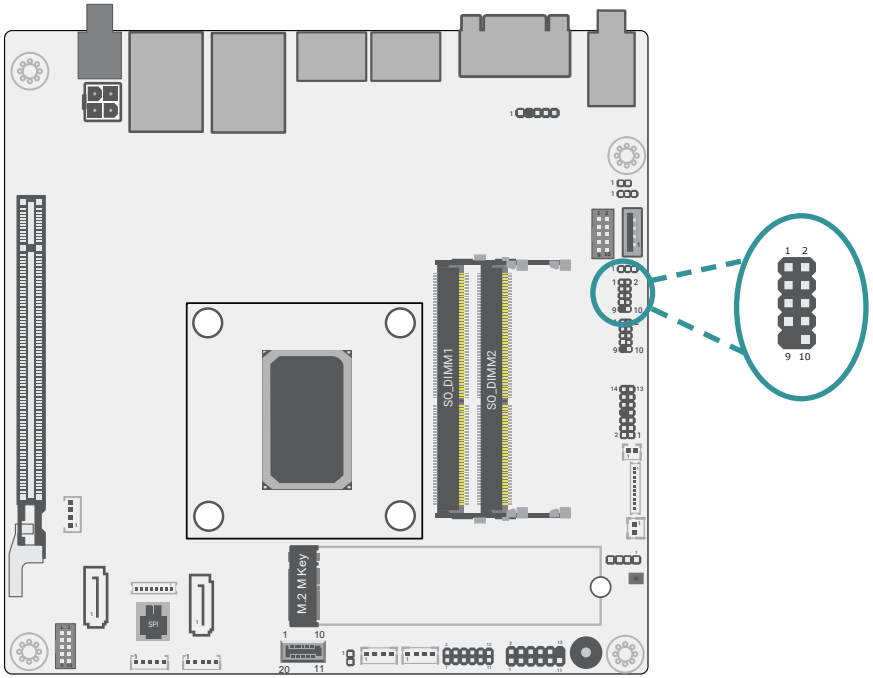
Pin	Assignment
1	DI3
2	DI2
3	DI1
4	DI0
5	DO3
6	DO2
7	DO1
8	DO0
9	+5V_ALW
10	GND

For GM903 (USB2.0/UART/AUDIO) (J20)



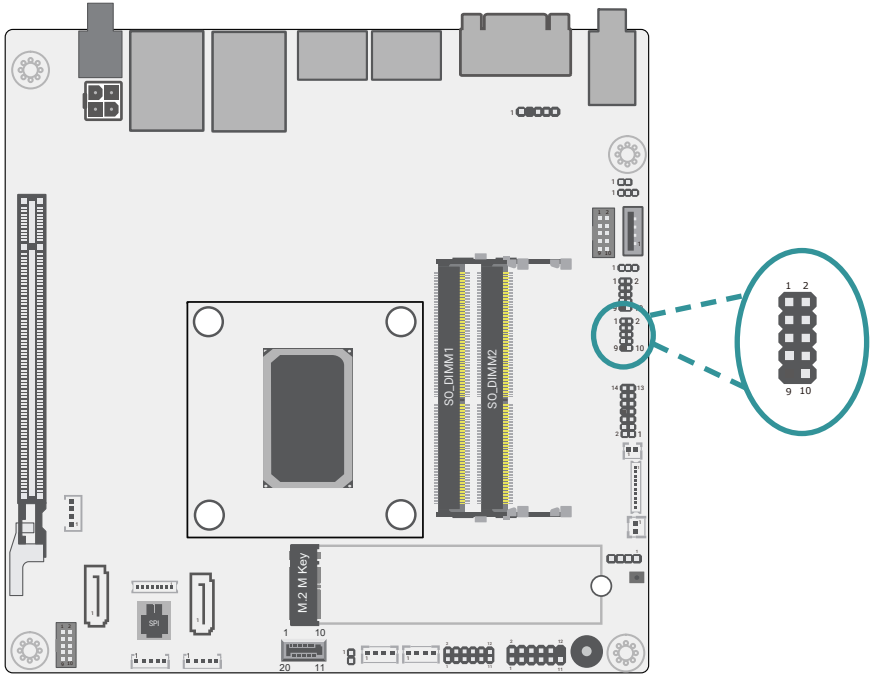
Pin	Assignment	Pin	Assignment
1	GND	2	GND
3	USBD-	4	AUDIO-R
5	USBD+	6	AUDIO-L
7	GND	8	GND
9	UART-RX (Host<-GM903)	10	UART-TX (Host->GM903)

USB2_6/7 (UBJ1)



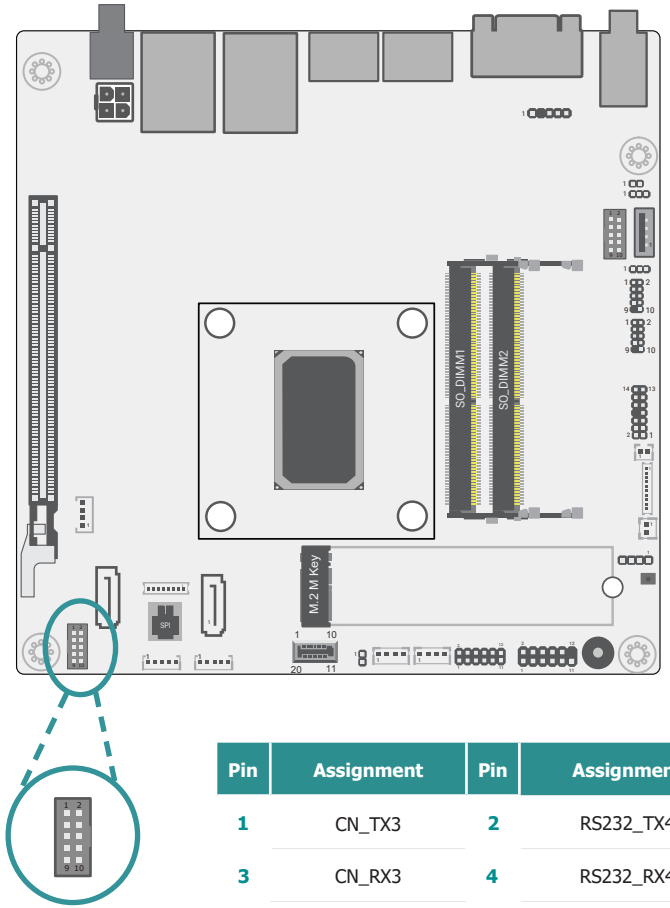
Pin	Assignment
1	+5V_RUN
2	+5V_RUN
3	USB_6N
4	USB_7N
5	USB_6P
6	USB_7P
7	GND
8	GND
9	NA
10	NC

USB2_8/9 (UBJ2)



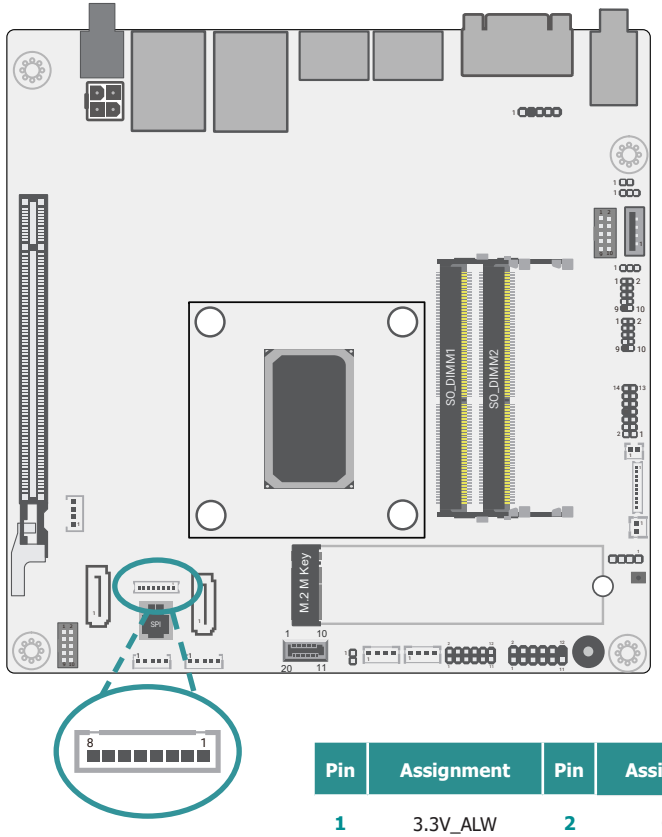
Pin	Assignment
1	+5V_RUN
2	+5V_RUN
3	USB_8N
4	USB_9N
5	USB_8P
6	USB_9P
7	GND
8	GND
9	NA
10	NC

COM3/4/5 (TSJ1)



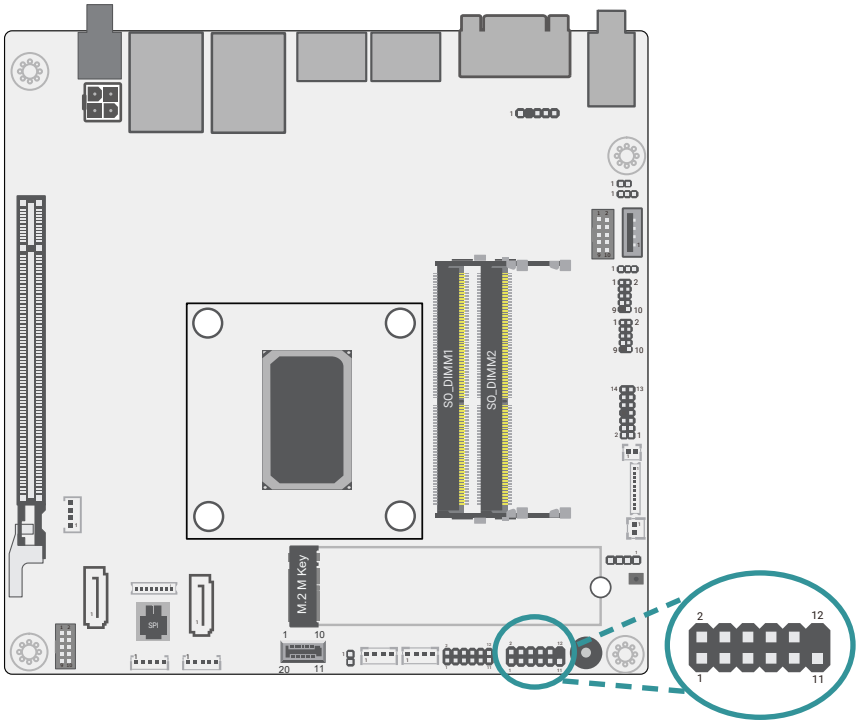
Pin	Assignment	Pin	Assignment
1	CN_TX3	2	RS232_TX4
3	CN_RX3	4	RS232_RX4
5	GND	6	GND
7	RS232_TX5	8	RS232_TX6
9	RS232_RX5	10	RS232_RX6

SMBus / I2C (J2)



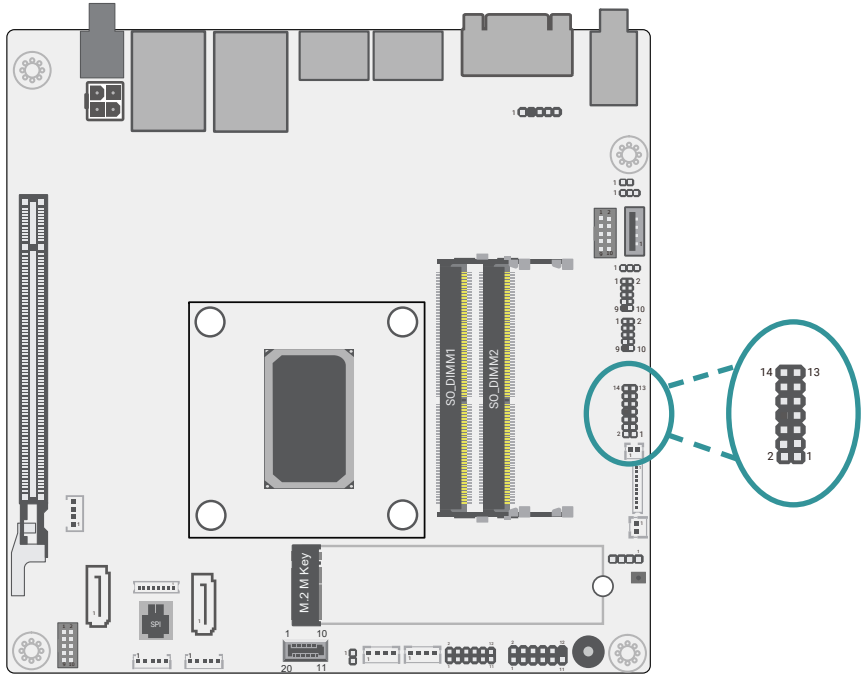
Pin	Assignment	Pin	Assignment
1	3.3V_ALW	2	GND
3	SMB_CLK	4	SMB_DATA
5	SMB_INT	6	I2C_SCL
7	I2C_SDA	8	I2C_INT

Front Panel (J14)



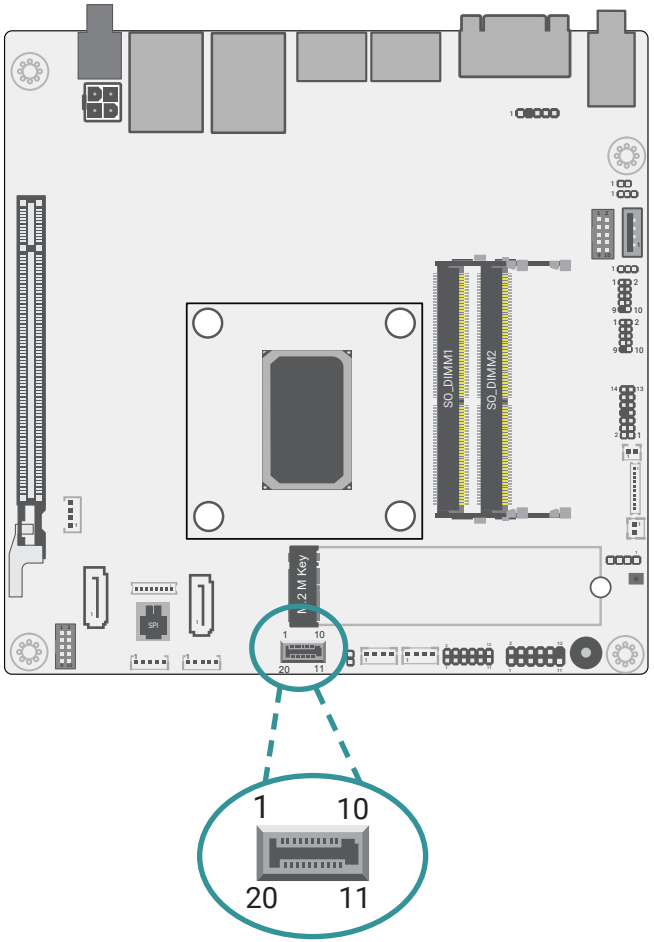
Pin	Assignment	Pin	Assignment
1	NC	2	3V3SB
3	3V3_RUN	4	3V3SB
5	HDD_LED	6	SUS_LED
7	GND	8	GND
9	SYS_RST-	10	PWR_BTN-
11	NC	12	NA

eSPI Header (J17)



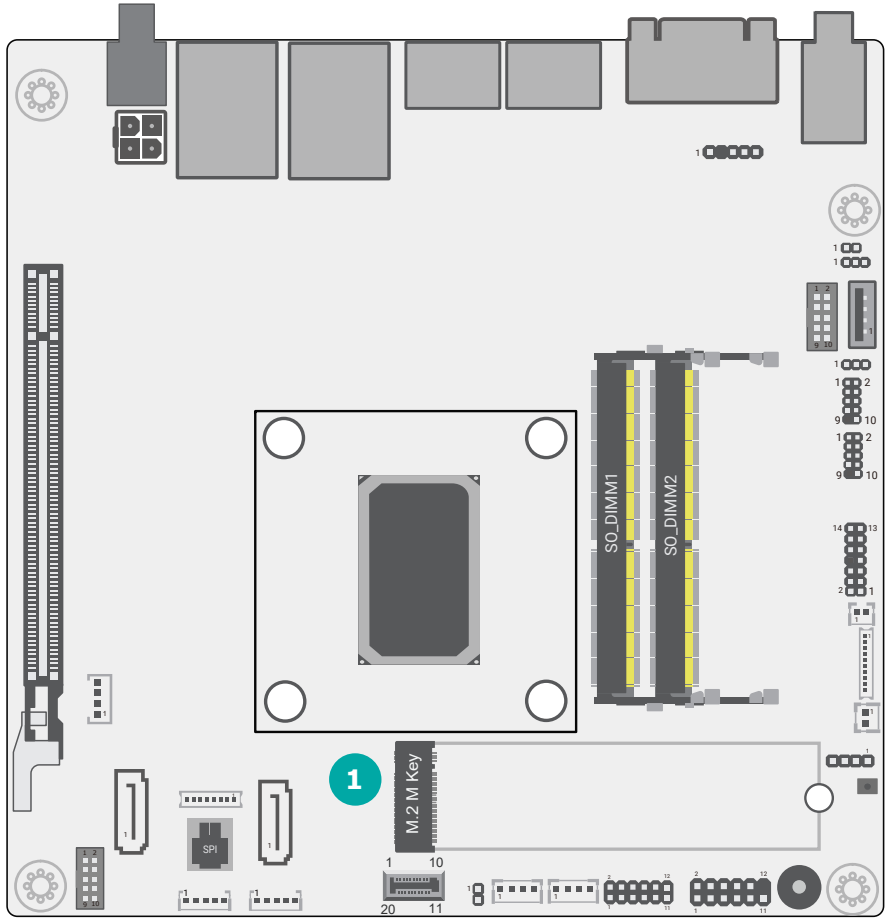
Pin	Assignment	Pin	Assignment
1	+3.3V_ALW	2	ESPI_CLK
3	ESPI_RESET#	4	GND
5	ESPI_ALT#	6	UART0_TX
7	ESPI_D0	8	NA
9	ESPI_D1	10	ESPI_CS
11	ESPI_D2	12	UART0_RX
13	ESPI_D3	14	+3.3V_ALW

PCIex1 with +12V & +3.3V (J19)



Pin	Assignment	Pin	Assignment
1	GND	2	PCIE_CLK+
3	PCIE_CLK-	4	GND
5	PCIE_TX+	6	PCIE_TX-
7	GND	8	PCIE_RX+
9	PCIE_RX-	10	+12V
11	GND	12	+3.3V
13	+3.3V	14	GND
15	(reserved) PowerSource	16	NC
17	GND	18	+12V
19	PCIE_RST#	20	+12V

▶ Expansion Slots

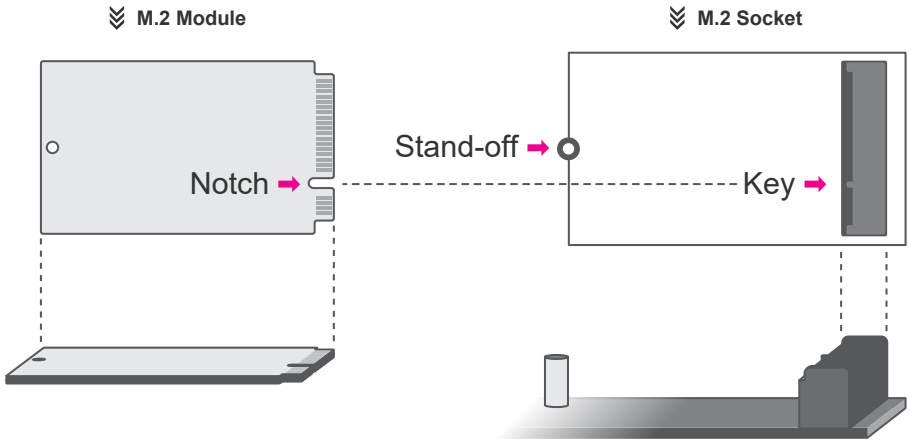


1 M.2 M-Key

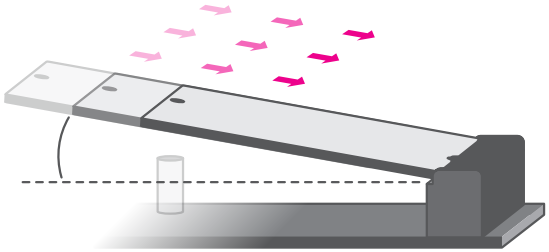
Installing the M.2 Module

Before installing the M.2 module into the M.2 socket, please make sure that the following safety cautions are well-attended.

1. Make sure the PC and all other peripheral devices connected to it has been powered down.
2. Disconnect all power cords and cables.
3. Locate the M.2 socket on the system board
4. Make sure the notch on card is aligned to the key on the socket.
5. Make sure the standoff screw is removed from the standoff.

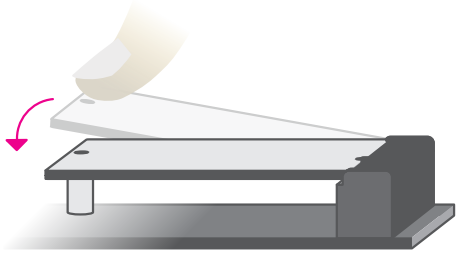


Please follow the steps below to install the card into the socket.



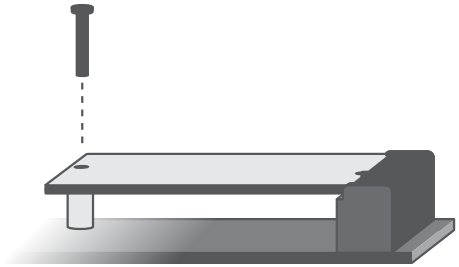
Step 1:

Insert the card into the socket at an angle while making sure the notch and key are perfectly aligned.



Step 2:

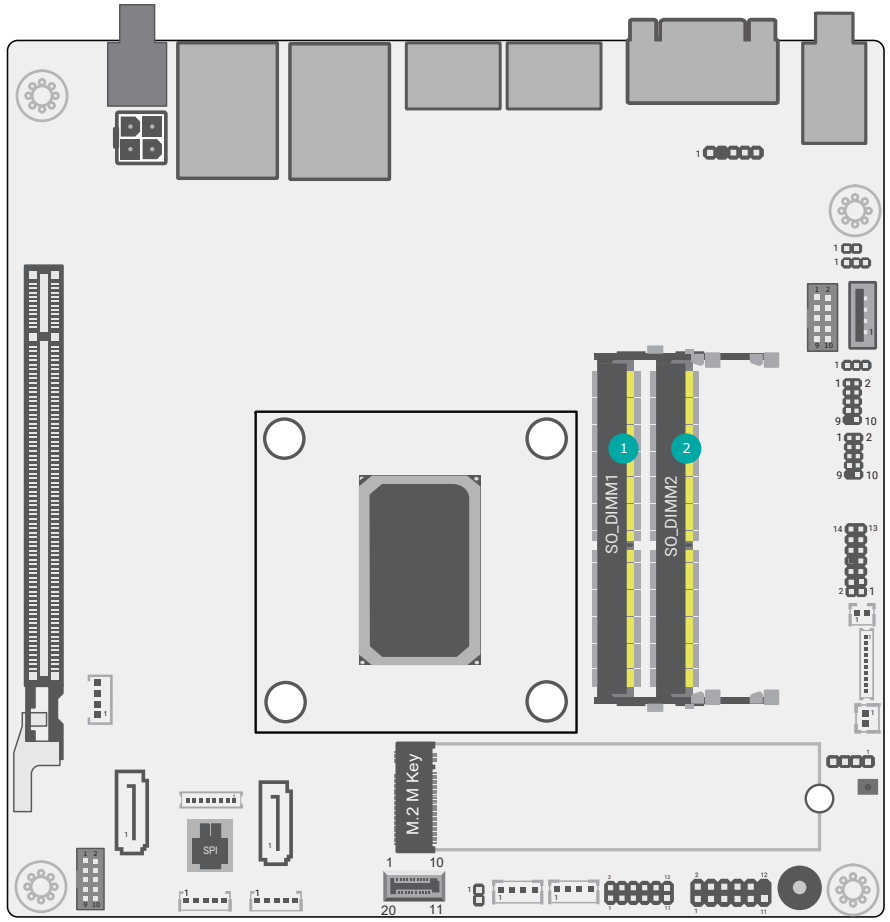
Press the end of the card far from the socket down until against the stand-off.



Step 3:

Screw tight the card onto the stand-off with a screw driver and a stand-off screw until the gap between the card and the stand-off closes up. The card should be lying parallel to the board when it's correctly mounted.

Installing the SO-DIMM Module

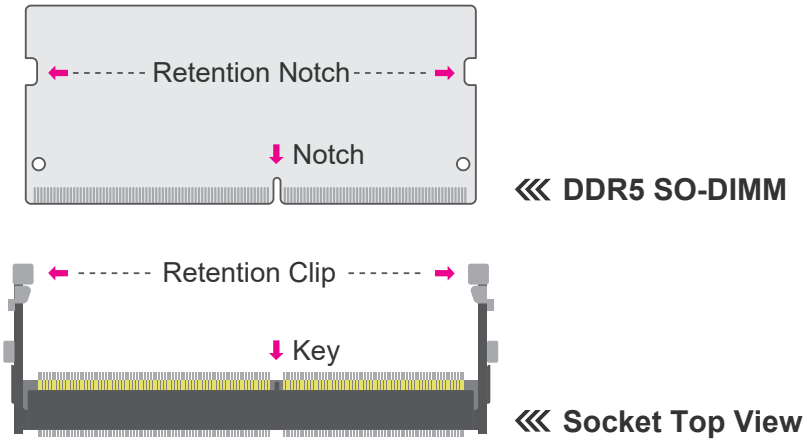


1 DDR5-1 SODIMM

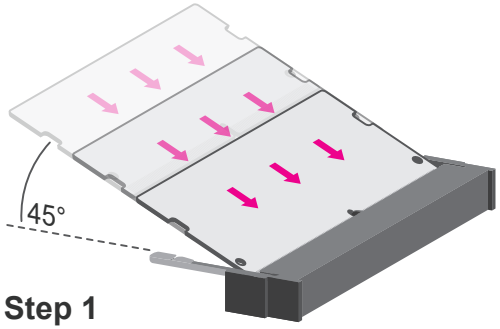
2 DDR5-2 SODIMM

Before installing the memory module, please make sure that the following safety cautions are well-attended.

1. Make sure the PC and all other peripheral devices connected to it has been powered down.
2. Disconnect all power cords and cables.
3. Locate the SO-DIMM socket on the system board
4. Make sure the notch on memory card is aligned to the key on the socket.



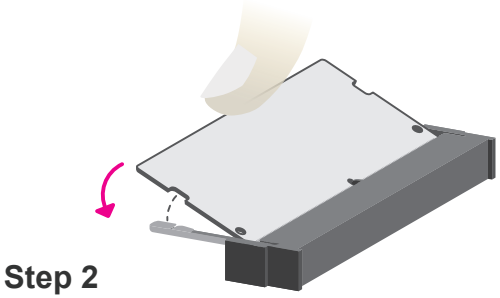
Please follow the steps below to install the memory card into the socket.



Step 1

Step 1:

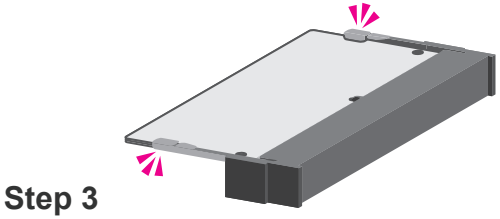
Insert the memory card into the slot while making sure 1) the notch and the key are aligned, and 2) the non-connector end rises approximately 45 degrees horizontally. Press the card firmly into the socket while applying and maintaining even pressure on both ends.



Step 2

Step 2:

Press the end of the card far from the socket down while making sure the retention notch and the clip align as indicated by the dotted line in the illustration. If the retention notch and the clip do not align, please remove the card and re-insert it. Press the card all the way down.



Step 3

Step 3:

The clips snap automatically and abruptly to the retention notches of the card sounding a distinctive click, and lock the card in place. Inspect that the clip sits in the notch. If not, please pull the clips outward, release and remove the card, and mount it again.

Chapter 3 - BIOS Settings

▶ Overview

The BIOS is a program that takes care of the basic level of communication between the CPU and peripherals. It contains codes for various advanced features found in this system board. The BIOS allows you to configure the system and save the configuration in a battery-backed CMOS so that the data retains even when the power is off. In general, the information stored in the CMOS RAM of the EEPROM will stay unchanged unless a configuration change has been made such as a hard drive replaced or a device added.

It is possible that the CMOS battery will fail causing CMOS data loss. If this happens, you need to install a new CMOS battery and reconfigure the BIOS settings.

Note:

The BIOS is constantly updated to improve the performance of the system board; therefore the BIOS screens in this chapter may not appear the same as the actual one. These screens are for reference purpose only.

Default Configuration

Most of the configuration settings are either predefined according to the Load Optimal Defaults settings which are stored in the BIOS or are automatically detected and configured without requiring any actions. There are a few settings that you may need to change depending on your system configuration.

Entering the BIOS Setup Utility

The BIOS Setup Utility can only be operated from the keyboard and all commands are keyboard commands. The commands are available at the right side of each setup screen.

The BIOS Setup Utility does not require an operating system to run. After you power up the system, the BIOS message appears on the screen and the memory count begins. After the memory test, the message “Press DEL to run setup” will appear on the screen. If the message disappears before you respond, restart the system or press the “Reset” button. You may also restart the system by pressing the <Ctrl> <Alt> and <Del> keys simultaneously.

Legends

Keys	Function
Right / Left arrow	Move the highlight left or right to select a menu
Up / Down arrow	Move the highlight up or down between submenus or fields
<Enter>	Enter the highlighted submenu
+ (plus key)/F6	Scroll forward through the values or options of the highlighted field
- (minus key)/F5	Scroll backward through the values or options of the highlighted field
<F1>	Display general help
<F2>	Display previous values
<F7>	Popup Boot Device List
<F9>	Optimized defaults
<F10>	Save and Exit
<Esc>	Return to previous menu

Scroll Bar

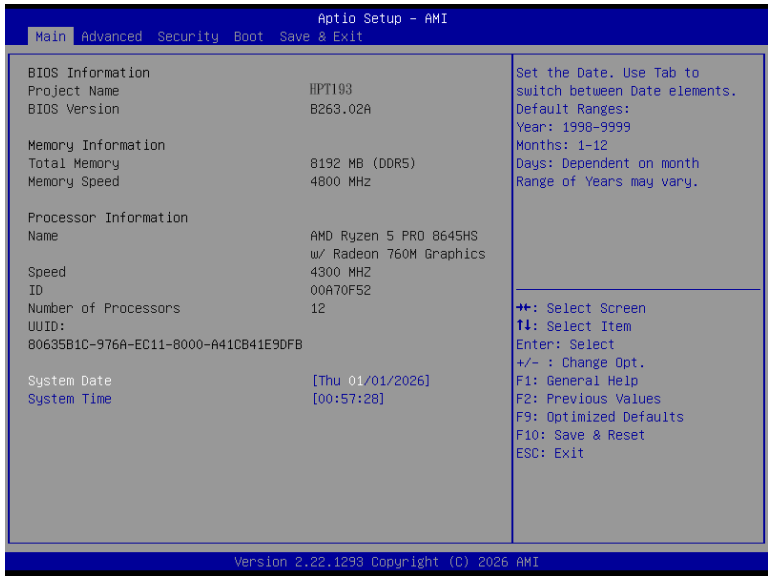
When a scroll bar appears to the right of the setup screen, it indicates that there are more available fields not shown on the screen. Use the up and down arrow keys to scroll through all the available fields.

Submenu

When “▶” appears on the left of a particular field, it indicates that a submenu which contains additional options are available for that field. To display the submenu, move the highlight to that field and press <Enter>.

▶ Main

The Main menu is the first screen that you will see when you enter the BIOS Setup Utility.



System Date

The date format is <month>, <date>, <year>. Press "Tab" to switch to the next field and press "-" or "+" to modify the value.

System Time

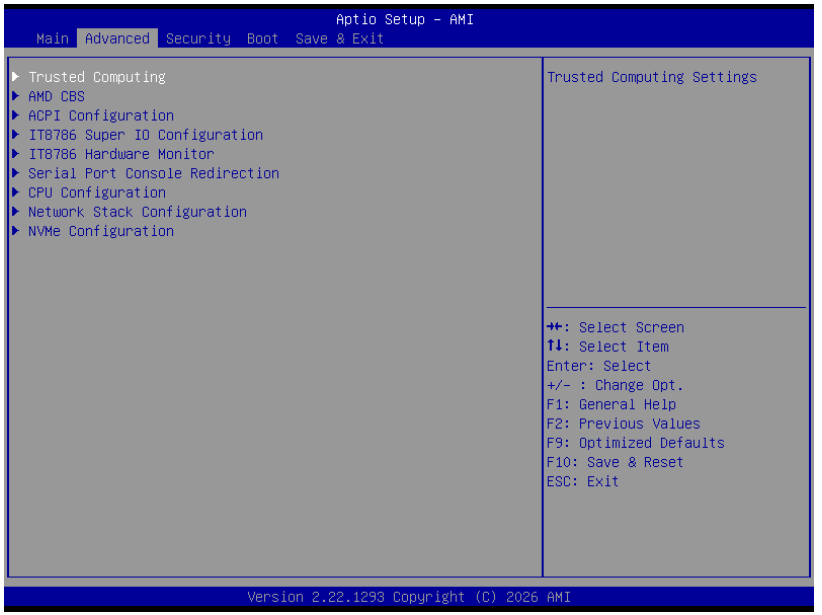
The time format is <hour>, <minute>, <second>. The time is based on the 24-hour military-time clock. For example, 1 p.m. is 13:00:00. Hour displays hours from 00 to 23. Minute displays minutes from 00 to 59. Second displays seconds from 00 to 59.

▶ Advanced

The Advanced menu allows you to configure your system for basic operation. Some entries are defaults required by the system board, while others, if enabled, will improve the performance of your system or let you set some features according to your preference.

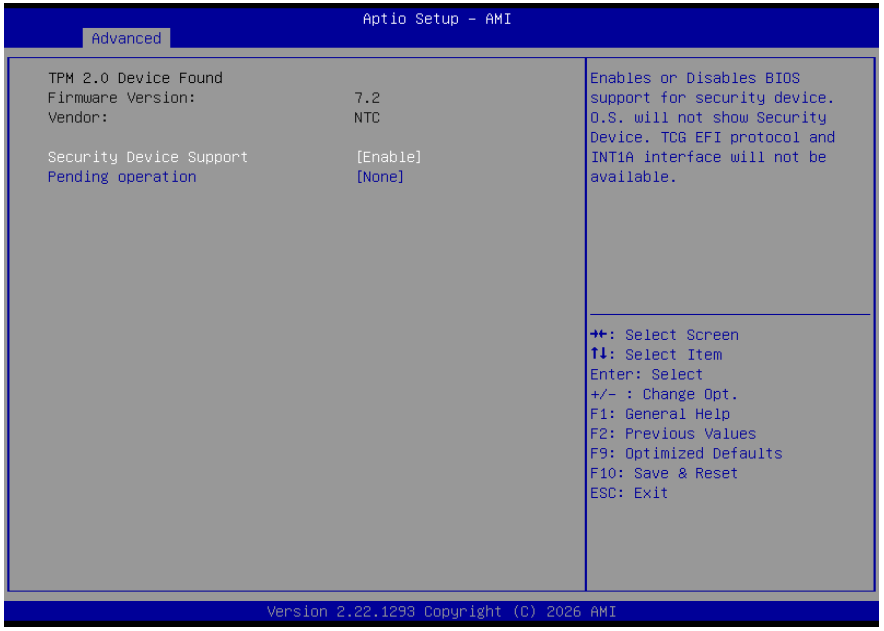
Important:

Setting incorrect field values may cause the system to malfunction.



▶ Advanced

Trusted Computing



Security Device Support

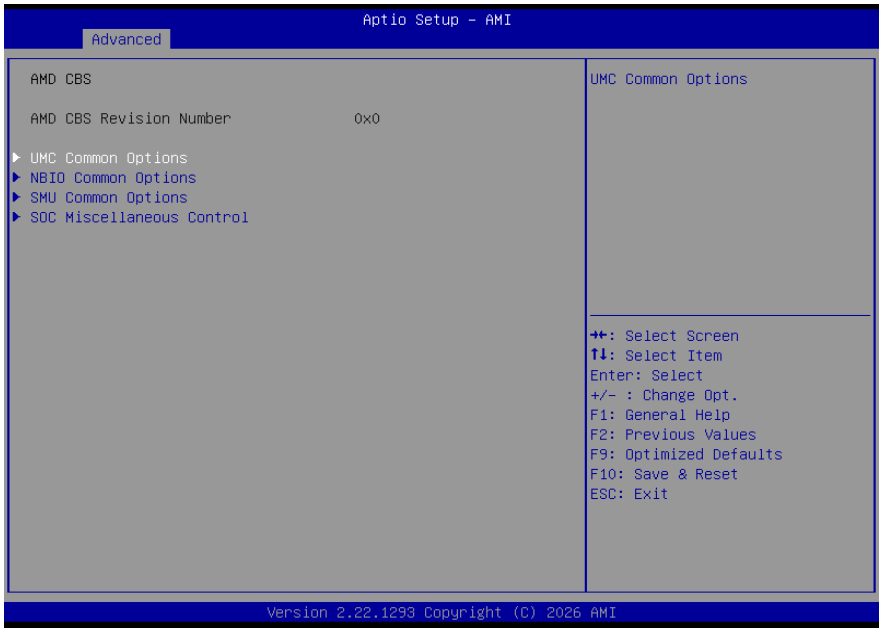
This field is used to enable or disable BIOS support for the security device such as an TPM 2.0 to achieve hardware-level security via cryptographic keys.

Pending operation

To clear the existing TPM encryption, select "TPM Clear" and restart the system. This field is not available when "Security Device Support" is disabled.

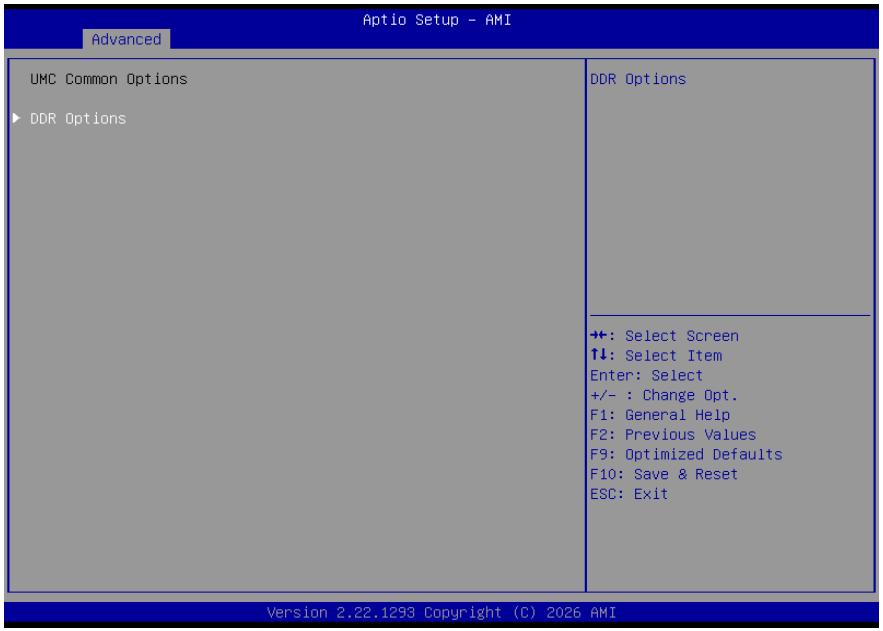
▶ Advanced

AMD CBS



▶ Advanced

AMD CBS ▶ UMC Common Options

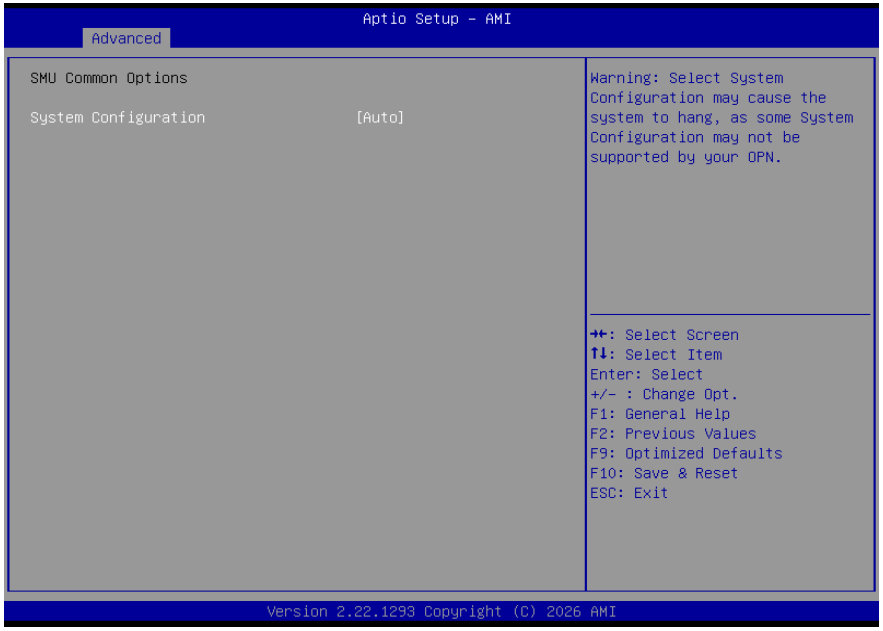


▶ Advanced

AMD CBS ▶ NBIO Common Options

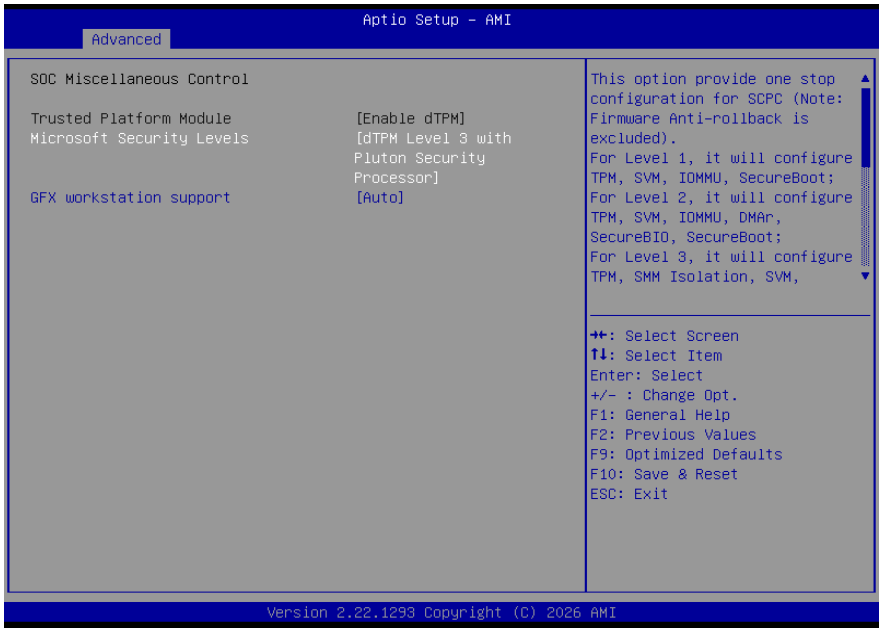
▶ Advanced

AMD CBS ▶ SMU Common Options



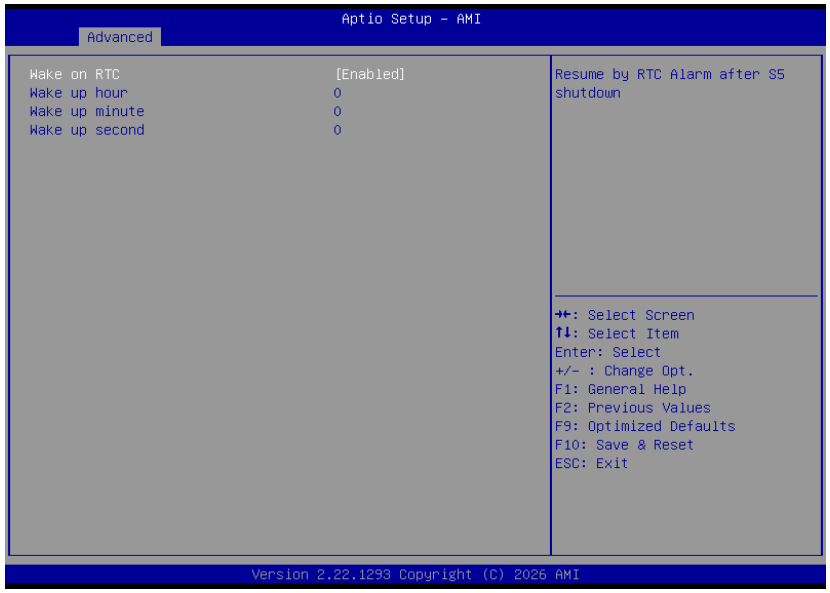
▶ Advanced

AMD CBS ▶ SOC Miscellaneous Control



▶ Advanced

ACPI Settings

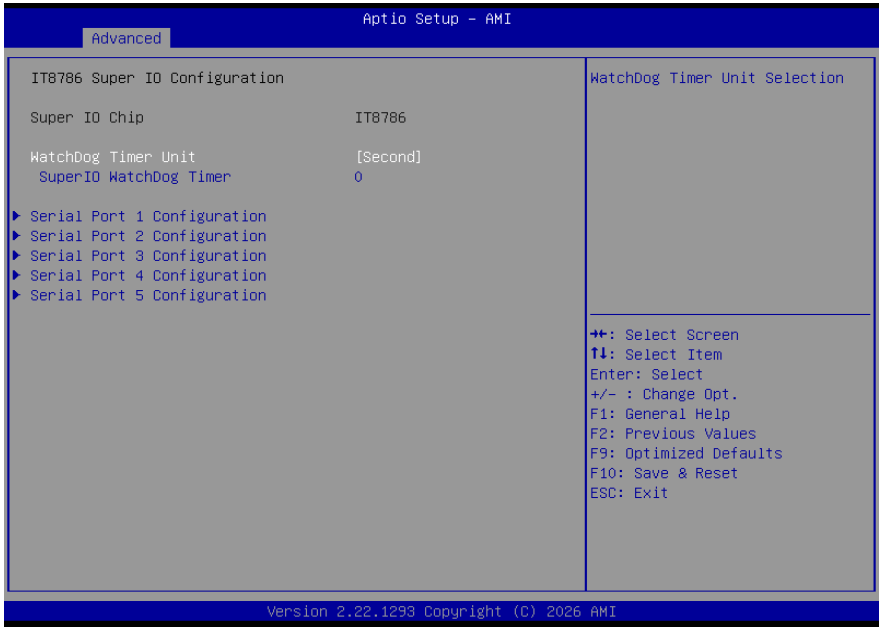


Wake On RTC

Resume by RTC Alarm after S5 shutdown.

▶ Advanced

IT8786 Super IO Configuration

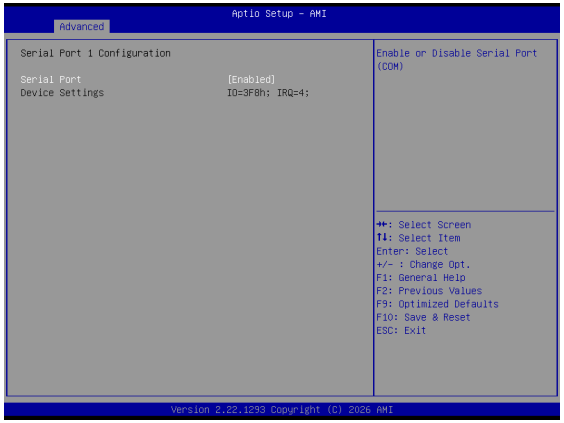


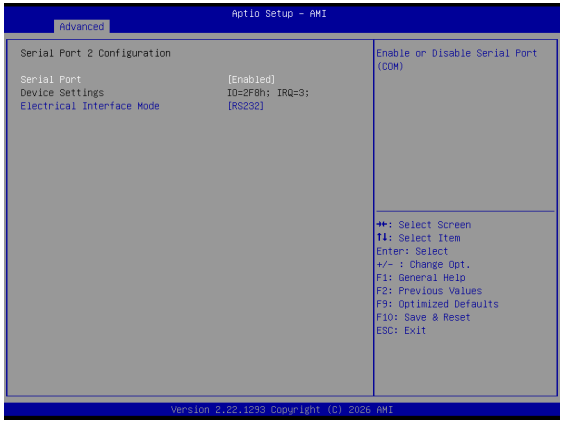
Note:

The sub-menus are detailed in following sections.

▶ Advanced

IT8786 Super IO Configuration ▶ Serial Port 1, 2 Configuration



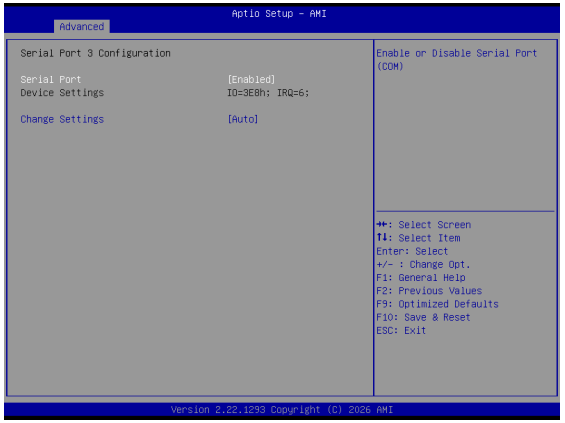


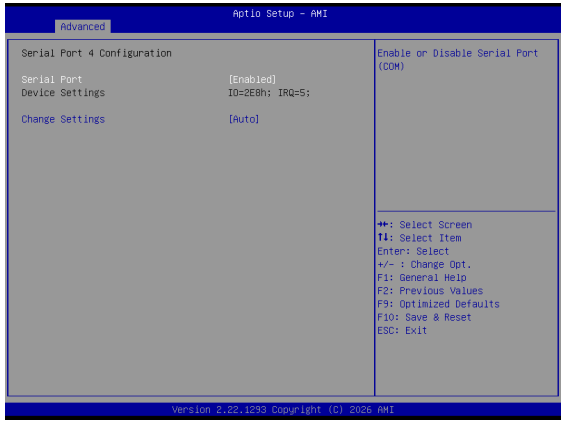
Serial Port

Enable or disable serial port.

▶ Advanced

IT8786 Super IO Configuration ▶ Serial Port 3, 4 Configuration



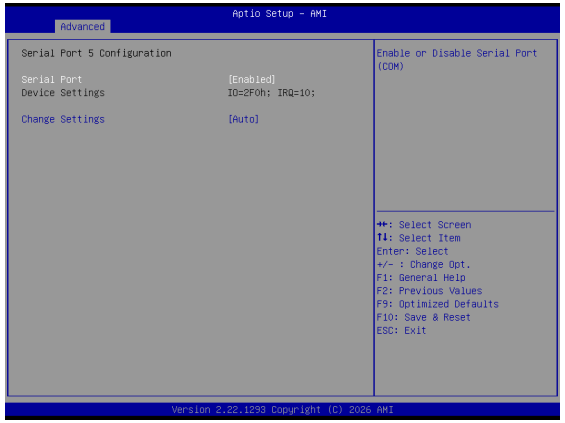


Serial Port

Enable or disable serial port.

▶ Advanced

IT8786 Super IO Configuration ▶ Serial Port 5 Configuration

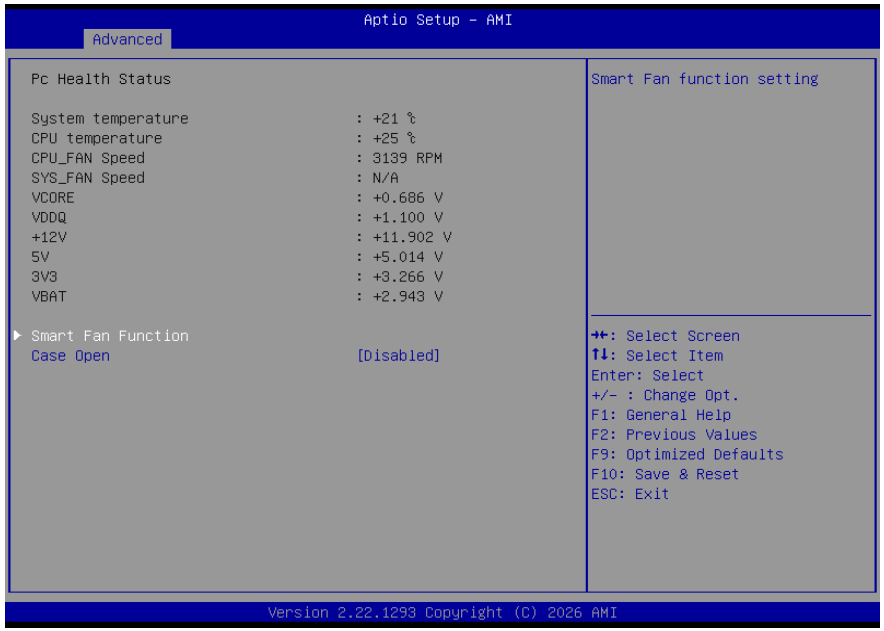


Serial Port

Enable or disable serial port.

▶ Advanced

IT8786 Hardware Monitor



This section displays the system's health information, i.e. voltage readings, CPU and system temperatures, and fan speed readings

Smart Fan Function

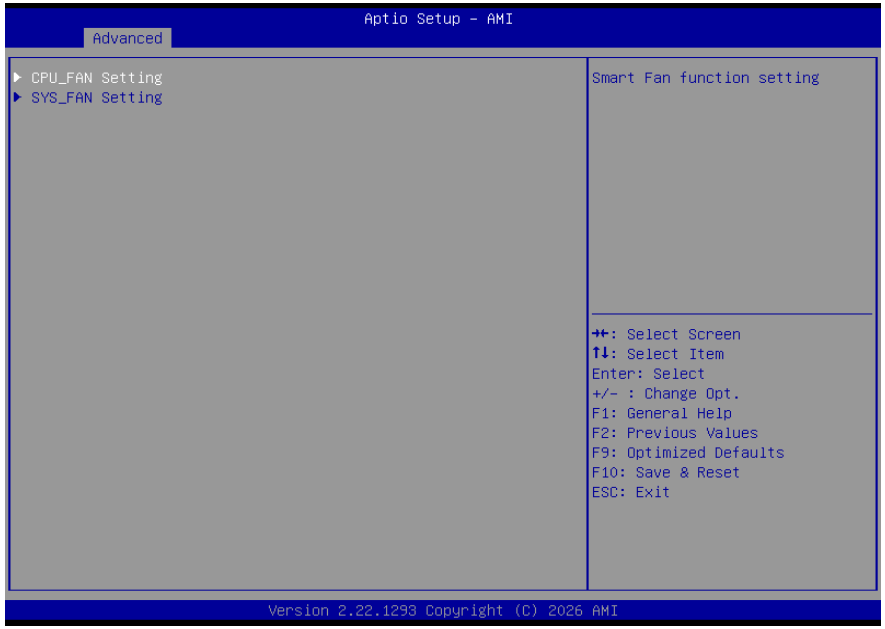
Smart Fan Function Setting.

Case Open

Enable or disable the case open detection function.

▶ Advanced

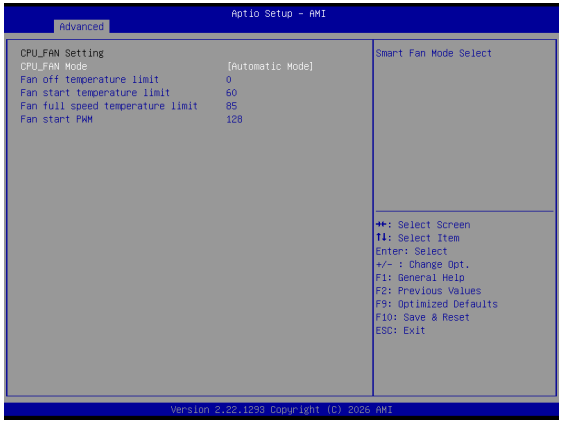
IT8786 Hardware Monitor ▶ Smart FAN Function

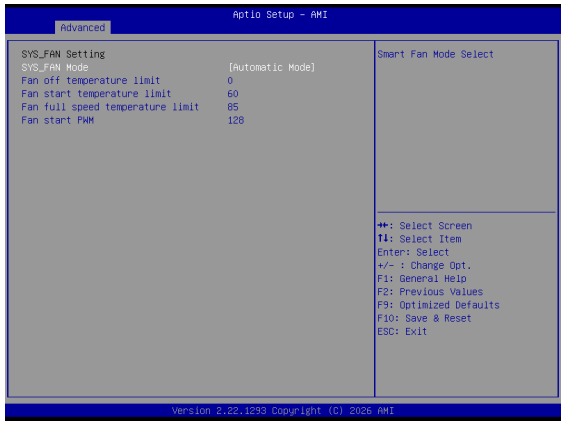


Smart Fan is a fan speed moderation strategy dependent on the current system temperature. When the system temperature goes higher than the Boundary setting, the fan speed will be turned up to the setting of the Fan Speed Count that bears the same index as the Boundary field.

▶ Advanced

IT8786 Hardware Monitor ▶ Smart FAN Function





Smart FAN Mode

Smart Fan Mode Select.

Fan off temperature limit

Fan will off when temperature lower than this limit.

Fan start temperature limit

Fan will work when temperature higher than this limit.

Fan full speed temperature limit

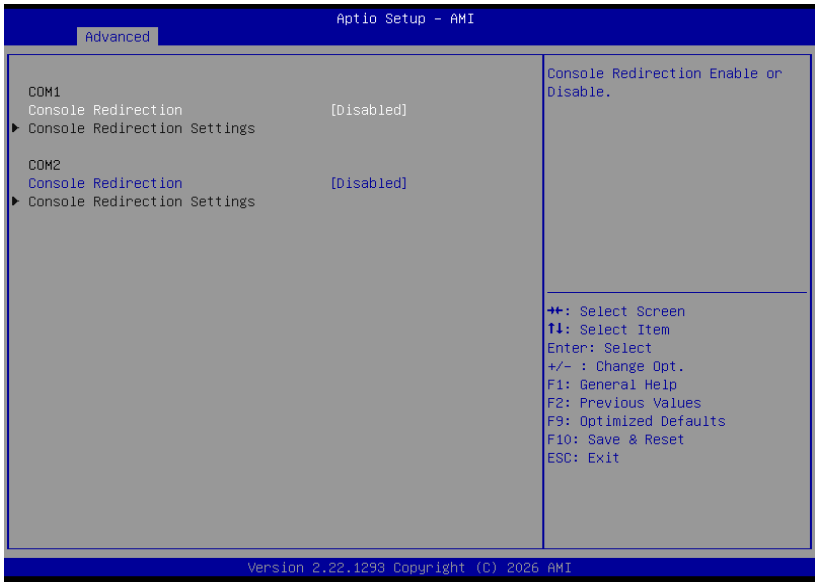
Fan will full speed when temperature higher than this limit.

Fan start PWM

Fan will start with this PWM value.

▶ Advanced

Serial Port Console Redirection

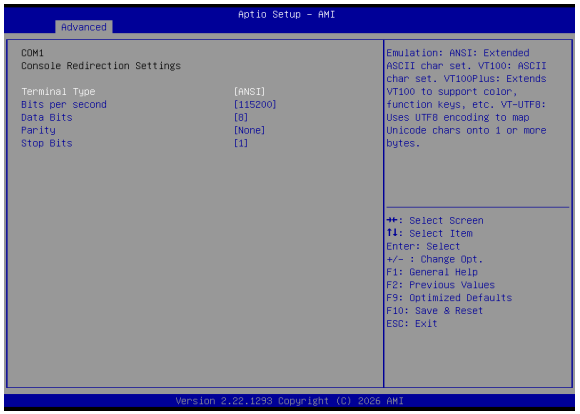


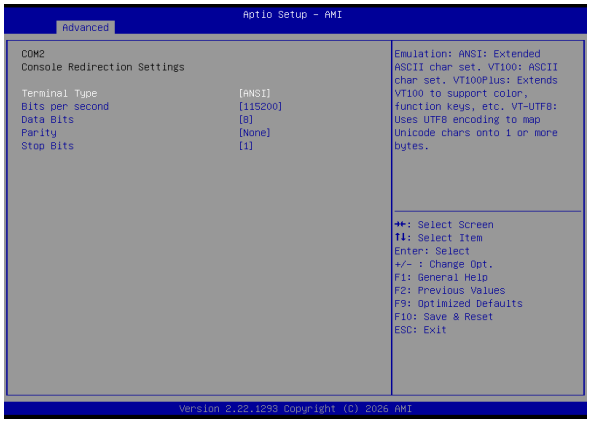
Console Redirection

By enabling Console Redirection of a COM port, the sub-menu of console redirection settings will become available for configuration as detailed in the following.

▶ Advanced

Serial Port Console Redirection ▶ Console Redirection Settings





Configure the serial settings of the current COM port.

Terminal Type

Select terminal type: VT100, VT100+, VT-UTF8 or ANSI.

Bits per second

Select serial port transmission speed: 9600, 19200, 38400, 57600 or 115200.

Data Bits

Select data bits: 7 bits or 8 bits.

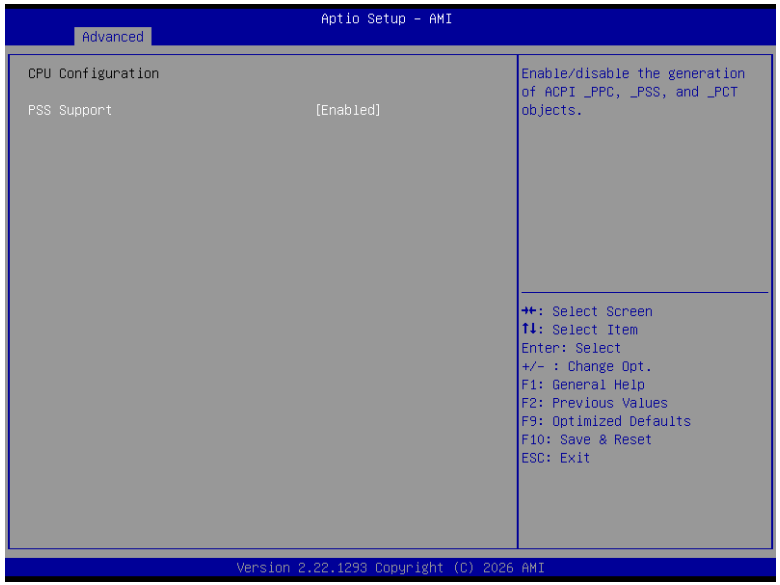
Parity

Select parity bits: None, Even, Odd, Mark or Space.

Stop Bits

Select stop bits: 1 bit or 2 bits.

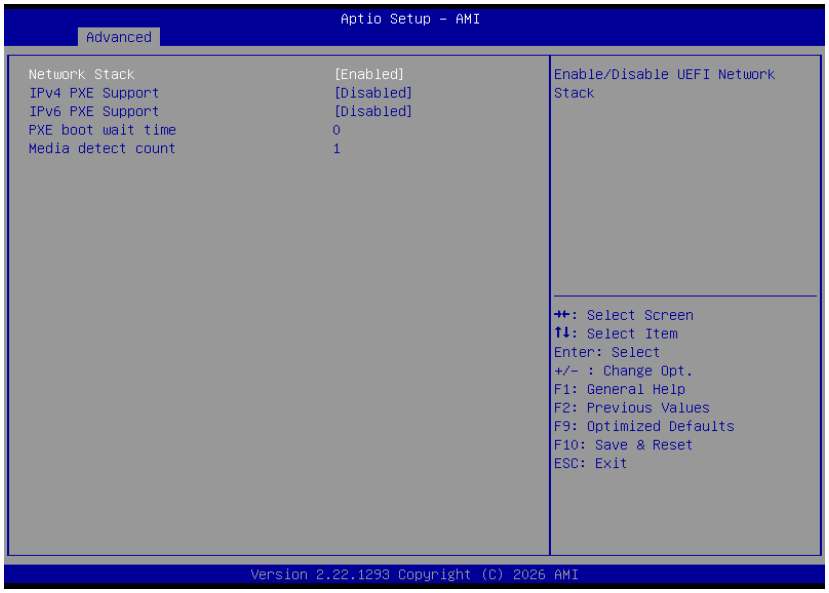
CPU Configuration



PSS Support

Enable or disable the generation of ACPI_PPC, _PSS, and _PCT objects.

Network Stack Configuration



Network Stack

Enable or disable UEFI network stack. The following fields will appear when this field is enabled.

Ipv4 PXE Support

Enable or disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.

Ipv6 PXE Support

Enable or disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.

PXE boot wait time

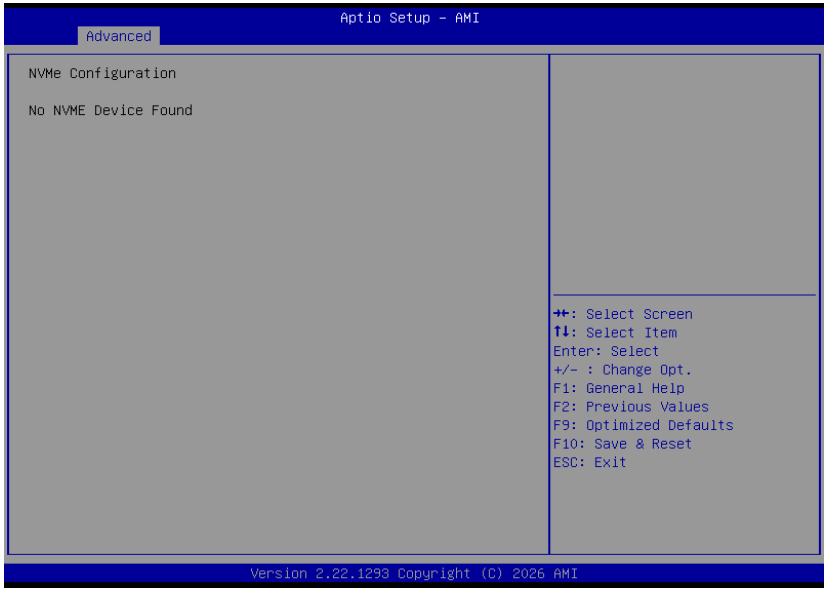
Set the wait time in seconds to press ESC key to abort the PXE boot. Use either +/- or numeric keys to set the value.

Media detect count

Set the number of times the presence of media will be checked. Use either +/- or numeric keys to set the value.

▶ Advanced

NvMe Configuration



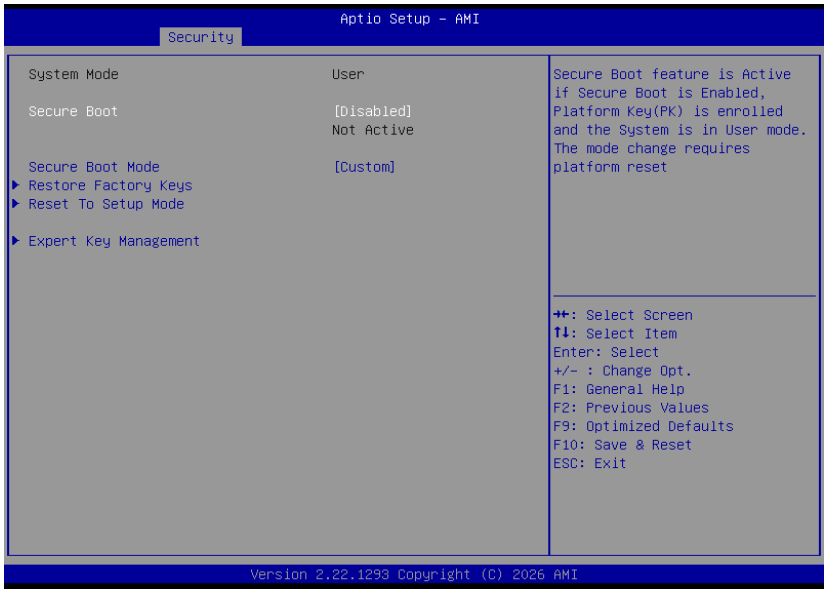
▶ Security

Administrator Password

Set the administrator password. To clear the password, input nothing and press enter when a new password is asked. Administrator Password will be required when entering the BIOS.

▶ Security

Secure Boot



Secure Boot

The Secure Boot store a database of certificates in the firmware and only allows the OSes with authorized signatures to boot on the system. To activate Secure Boot, please make sure that "Secure Boot" is "[Enabled]", Platform Key (PK) is enrolled, "System Mode" is "User", and CSM is disabled. After enabling/disabling Secure Boot, please save the configuration and restart the system. When configured and activated correctly, the Secure Boot status will be "Active".

Secure Boot Mode

Select the secure boot mode — Standard or Custom. When set to Custom, the following fields will be configurable for the user to manually modify the key database.

Restore Factory Keys

Force system to User Mode. Load OEM-defined factory defaults of keys and databases onto the Secure Boot. Press Enter and a prompt will show up for you to confirm.

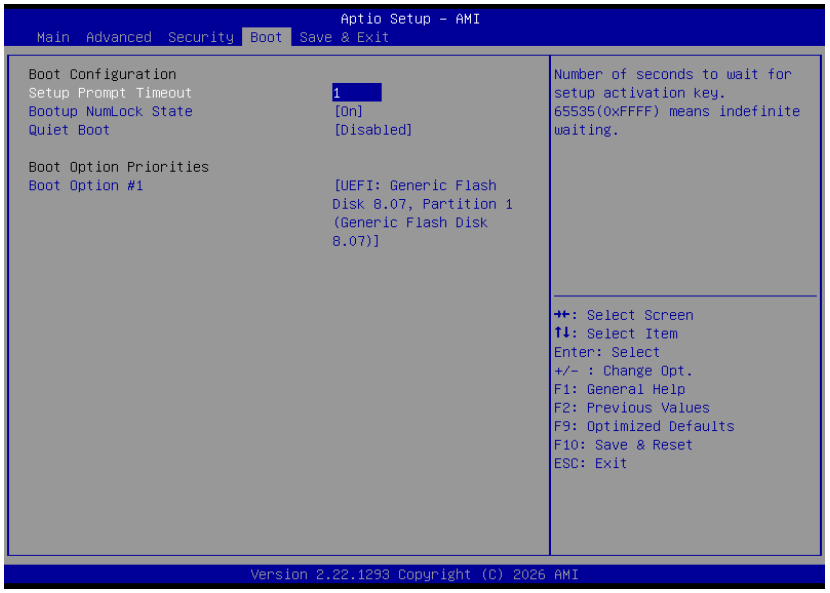
Reset To Setup Mode

Clear the database from the NVRAM, including all the keys and signatures installed in the Key Management menu. Press Enter and a prompt will show up for you to confirm.

Expert Key Management

Enables expert users to modify Secure Boot Policy variables without full authentication.

▶ Boot



Setup Prompt Timeout

Set the number of seconds to wait for the setup activation key. 65535 (0xFFFF) denotes indefinite waiting.

Bootup NumLock State

Select the keyboard NumLock state: On or Off.

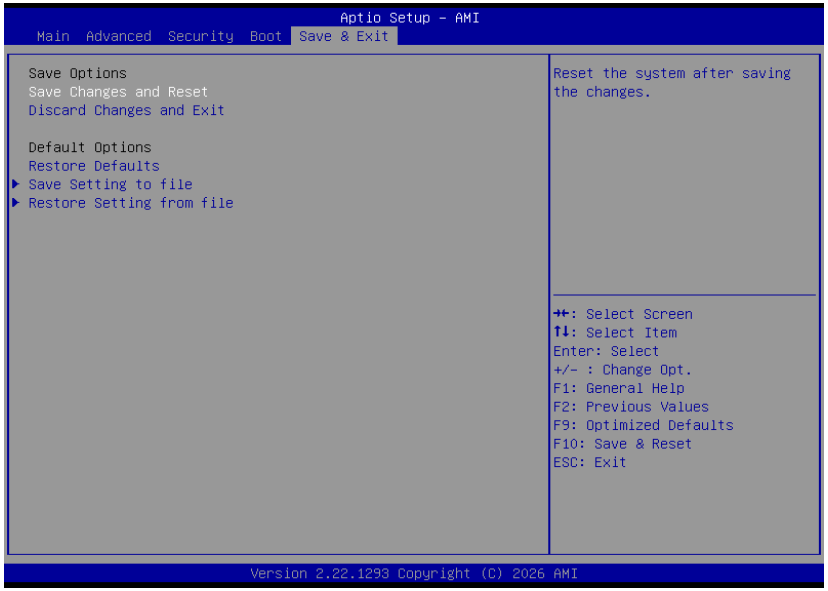
Quiet Boot

This section is used to enable or disable quiet boot option.

Boot Option Priorities

Rearrange the system boot order of available boot devices.

▶ Save & Exit



Save Changes and Reset

To save the changes, select this field and then press <Enter>. A dialog box will appear. Select Yes to reset the system after saving all changes made.

Discard Changes and Exit

To discard the changes, select this field and then press <Enter>. A dialog box will appear. Select Yes to reset the system setup without saving any changes.

Restore Defaults

To restore and load the optimized default values, select this field and then press <Enter>. A dia-log box will appear. Select Yes to restore the default values of all the setup options.

• **Save Setting to file** Select this option to save BIOS configuration settings to a USB flash device.

• **Restore Setting from file** This field will appear only when a USB flash device is detected. Select this field to restore set-ting from the USB flash device.

▶ Updating the BIOS

To update the BIOS, you will need the new BIOS file and a flash utility. Please contact technical support or your sales representative for the files and specific instructions about how to update BIOS with the flash utility.

▶ Notice: BIOS SPI ROM

1. The AMD Platform Security Processor has already been integrated into this system board. Due to the safety concerns, the BIOS (SPI ROM) chip cannot be removed from this system board and used on another system board of the same model.
2. The BIOS (SPI ROM) on this system board must be the original equipment from the factory and cannot be used to replace one which has been utilized on other system boards.
3. If you do not follow the methods above, the AMD Platform Security Processor will not be updated and will cease to be effective.

Note:

a. You can take advantage of flash tools to update the default configuration of the BIOS (SPI ROM) to the latest version anytime.

b. When the BIOS IC needs to be replaced, you have to populate it properly onto the system board after the EEPROM programmer has been burned and follow the technical person's instructions to confirm that the MAC address should be burned or not.

c. After updating unique MAC Address from manufacturing, NVM will be protected immediately after power cycle. Users cannot update NVM or MAC address.