DFI

EC70A-ADP

Fanless Robust Embedded System

User's Manual

Copyright

This publication contains information that is protected by copyright. No part of it may be reproduced in any form or by any means or used to make any transformation/adaptation without the prior written permission from the copyright holders.

This publication is provided for informational purposes only. The manufacturer makes no representations or warranties with respect to the contents or use of this manual and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The user will assume the entire risk of the use or the results of the use of this document. Further, the manufacturer reserves the right to revise this publication and make changes to its contents at any time, without obligation to notify any person or entity of such revisions or changes.

Changes after the publication's first release will be based on the product's revision. The website will always provide the most updated information.

Trademarks

Product names or trademarks appearing in this manual are for identification purpose only and are the properties of the respective owners.

FCC and DOC Statement on Class A

This equipment has been tested and found to comply with the limits for a Class A 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 retrieved 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 arises 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.

About this 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 EC70A-ADP system unit

   ·   Remote switch cable

   ·   3 M.2 slot slot screws

   ·   4 Foot screws & Rubber foot

   ·   1 Grounding screw

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

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 Precautions

- Use the correct DC / AC input voltage range.

- Unplug the power cord before removing the system chassis cover for installation or servicing. After installation or servicing, cover the system chassis before plugging in the power cord.

- There is danger of explosion if battery incorrectly replaced.

- Replace only with the same or equivalent specifications of batteries recommend by the manufacturer.

- Dispose of used batteries according to local ordinance.

- Keep this system away from humid environments.

- Make sure the system is placed or mounted correctly and stably to prevent the chance of dropping or falling may cause damage.

- The openings on the system shall not be blocked and shall be kept in distance from other objects to make sure of proper air ventilation to protect the system from overheating.

- Dress the cables, especially the power cord, so they will not be stepped on, in contact with high temperature surfaces, or cause any tripping hazards.

- Do not place anything on top of the power cord. Use a power cord that has been approved for use with the system and is compliant with the voltage and current ranges required by the system's electrical specifications.

- If the system is to be unused or stored for a long time, disconnect it from the power source to avoid damage by transient overvoltage.

- If one of the following occurs, consult a service personnel:

  - The power cord or plug is damaged.

  - Liquid has penetrated the system.

  - The system has been exposed to moisture.

  - The system is not working properly.

  - The system is physically damaged.

- The unit uses a three-wire ground cable which is equipped with a third pin to ground the unit and prevent electric shock. Do not defeat the purpose of this pin. If your outlet does not support this kind of plug, contact your electrician to replace the outlet.

- Disconnect the system from the electricity outlet before cleaning. Use a damp cloth for cleaning the surface. Do not use liquid or spray detergents for cleaning.

- Before connecting, make sure that the power supply voltage is correct. The device is connected to a power outlet which should be grounded connection.

The system may burn fingers while running.

Wait for 30 minutes to handle electronic parts after power off.

Chapter 1 - Introduction

▶ Overview

Front View
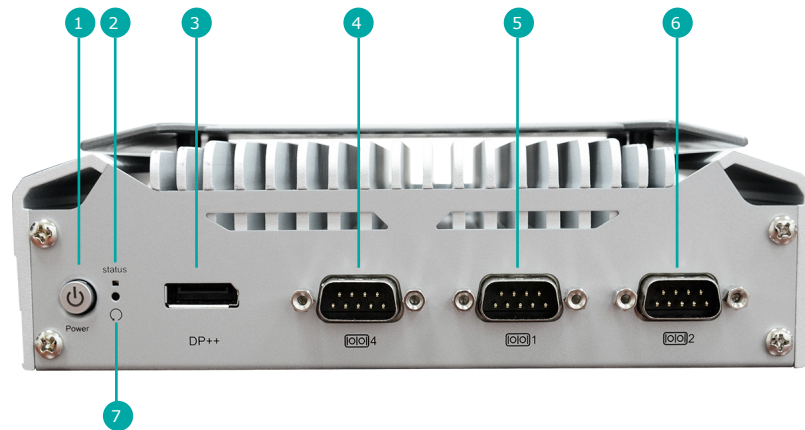
Rear View

1	Power Button
2	Status LED
3	DP++
4	COM4
5	COM1
6	COM2
7	Reset Button
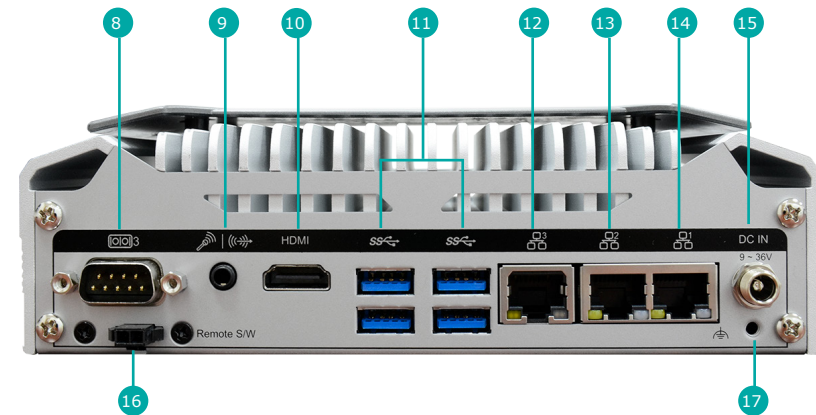
8	COM3
9	Line-out / Mic-in
10	HDMI
11	USB3.2
12	2.5 LAN3
13	LAN2
14	LAN1
15	DC Jack (9-36V)
16	Remote Switch
17	Grounding

▶ **Dimensions**

Front View

9.10

118.40

Left View

181.60

56.80

Rear View

Right View
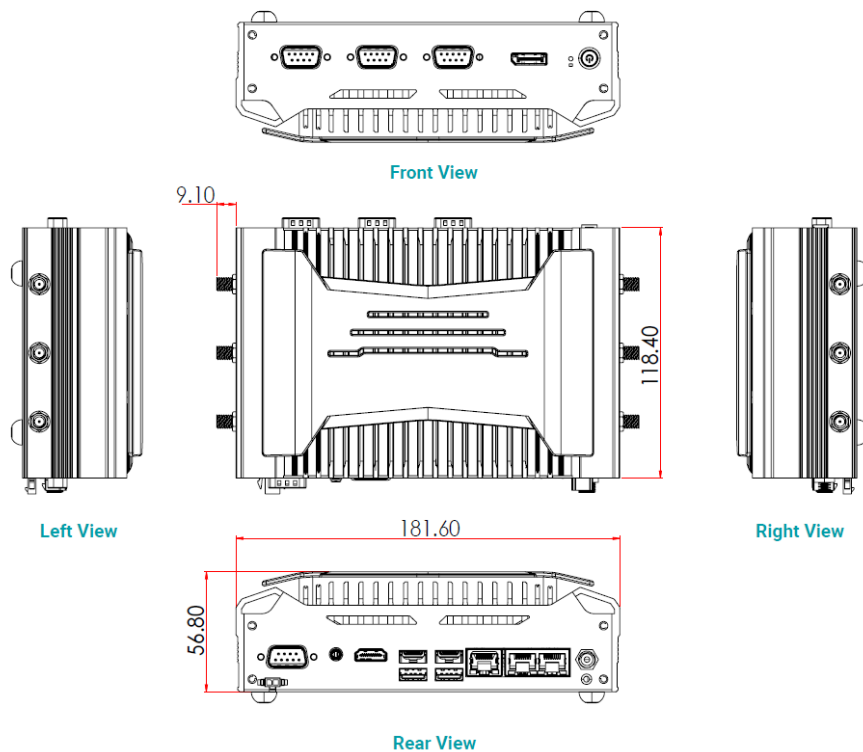
▶ **Key Features**

Alder Lake-P:
Intel® 12th Gen CoreTM Alder Lake-P Processor, TDP=15W for Fanless, TDP=28W for w/Fan.

Dual Displays:
HDMI (4K@30Hz) + DP (4K@60Hz)

On Board Memory:
On board memory and 1 SO-DIMM DDR4

5G Support:
Support M.2 B key 3042/3052 5G-NR module

Rich I/O:
Up to 3 LAN & 4 USB 3.2 (or 2 USB 3.2 + 2 USB type-C)

▶ **Specifications**

SYSTEM	Processor	12th Gen Intel® Core™ Processors, BGA 1744 (Alder Lake-P, 15W for Fanless model, 28W for with Fan model) Intel® Core™ i7-1265UE Processor, 10C12T, 12M Cache, 1.7GHz (4.7GHz) Intel® Core™ i5-1245UE Processor, 10C12T, 12M Cache, 1.5GHz (4.4GHz) Intel® Core™ i3-1215UE Processor, 6C8T, 10M Cache, 1.2GHz (4.4GHz)
	Memory	8GB On-board memory & one SO-DIMM DDR4 up to 32GB Dual Channel DDR4 3200MHz
	BIOS	AMI SPI 256Mbit
GRAPHICS	Controller	Intel® Iris® Xe Graphics for i7/i5 Processors Intel® UHD Graphics for i3/Celeron Processors
	Feature	DirectX 12, Open GL 4.6, Vulkan 1.2 HW Decode: AV1, AVC/H.264, MJPEG, HEVC/H.265, VP9, SCC HW Encode: MJPEG, AVC/H.264, HEVC/H.265, VP9, SCC
	Display	1 x HDMI, 1 x DP DP: resolution up to 4096x2304 @60Hz HDMI: resolution up to 4096x2160@30Hz
	Multiple Displays	HDMI + DP + 2 Type-C DP Alt. Mode
STORAGE	Internal	1 x M.2 2280 M key (PCIe x4/SATA)
EXPANSION	Interface	1 x M.2 M Key 2280 (PCIex4/SATA) 1 x M.2 B Key 3042/3052 (USB3.0/USB2.0/PCIex1), 1 x SIM slot for 4G/5G 1 x M.2 E Key 2230 (PCIex1/USB2.0)
AUDIO	Audio Codec	Realtek ALC888 5.1-channel
ETHERNET	Controller	1 x Intel® I225IT (10/100/1000/2500Mbps) 2 x Intel® I225IT (10/100/1000Mbps, connector speed limit) (Only Core i7/i5 supports iAMT)
LED	Indicators	1 x Power LED 1 x HDD LED
Front I/O	Serial	2 x RS-232/422/485 (DB-9, COM 1~2) 1 x RS232 (DB9, COM 4)
	Display	1 x DP (optional VGA by request)
	Buttons	1 x Power button 1 x Reset button

Rear I/O	Ethernet	1 x 2.5GHz (RJ-45) + 2 x GbE (RJ-45)
	Seial	1 x RS-232 or 8bit DIO (DB-9, COM 3, default is RS232, 8bit DIO can set by jumper setting)
	USB	4 x USB 3.2 **EC70A-ADP4043/EC70A-ADP4043F:** 4 x Type A connector **EC70A-ADP4022TC3/EC70A-4022TC3F:** 2 x Type C + 2 x Type A connector
	Display	1 x HDMI 2 x Type-C DP Alt. Mode(for EC70A-ADP4022TC3 & EC70A-ADP4022TC3F)
	Audio	1 x Audio Combo Phone Jack (Line-out/Mic-in)
WATCHDOG TIMER	Output & Interval	System Reset, Programmable via Software from 1 to 255 Seconds
SECURITY	TPM	TPM2.0
POWER	Type	Wide range 9~36V
	Connector	DC Jack
OS SUPPORT	Microsoft	Windows 10 IoT Enterprise 64-bit
	Linux	Linux
MECHANISM	Construction	Aluminum + Metal Aluminum
	Mounting	Wall/VESA/DIN rail mount
	Dimensions (W x H x D)	181.6mm x 57mm x 118.4mm
	Weight	TBD
ENVIRONMENT	Operating Temperature	Fanless(CPU TDP 15W): -20 to 60°C (wide-temp SSD)
	Storage Temperature	-20 to 85°C
	Relative Humidity	5 to 95% RH (non-condensing)
STANDARDS AND CERTIFI-CATIONS	Shock	Operating: IEC 60068-2-27 Test Ea: Shock Test Half-Sine, 3G @ 11ms, 18 Shock ±X, ±Y, ±Z (each axis 3 times)
	Vibration	Operating: IEC 60068-2-64 Test Fh: Vibration Board-Band Random Test Random, 1Grms @ 5~500 Hz, 30min Non-Operating: IEC 60068-2-6 Test Fc: Vibration Sinusoidal Test Sweep Sine, 3Grms @ 10~500Hz, 30min
	Certifications	CE, FCC Class A, RoHS, UKCA

Chapter 2 - Hardware Installations

▶ Removing the Chassis Cover

Please read and follow the instructions below to open the system.

1. Make sure the system and all other peripheral devices connected to it have been powered off.

2. Disconnect all power cords and cables.

Step 1:

The 2 screws on the bottom of the system are used to secure the bottom cover to the chassis. Remove the screws and put them in a safe place for later use. Lift the bottom cover upward to open the system.

Step 2:

The heat shield can be easily accessed after the chassis cover is removed.
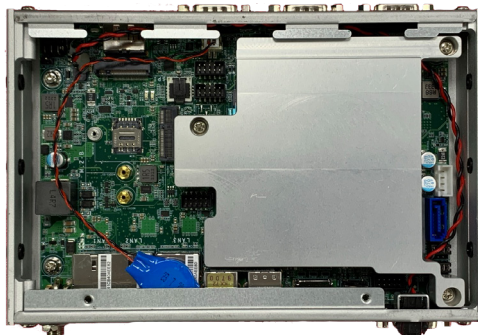
Step 3:

Remove the 3 screws of the heat shield and put them in a safe place for later use. The mainboard is readily accessible.

Heat shield
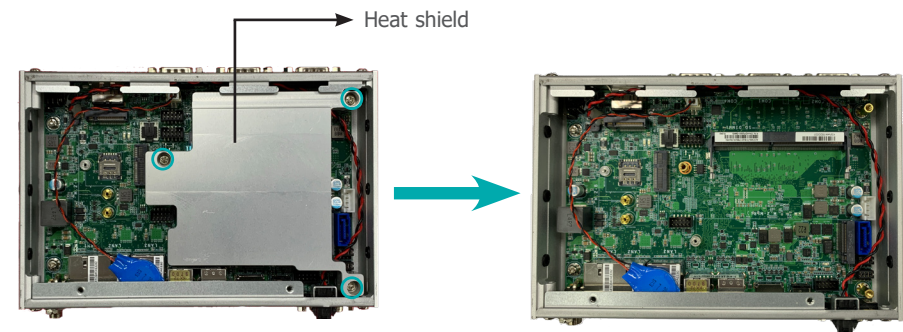
▶ Installing the SO-DIMM Module

Before installing the memory module, please read and follow the safety cautions below.

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.

Step 1:

Remove the 3 screws of the heat shield and put them in a safe place for later use.
Remove the heat shield and the SO-DIMM socket is readily accessible.
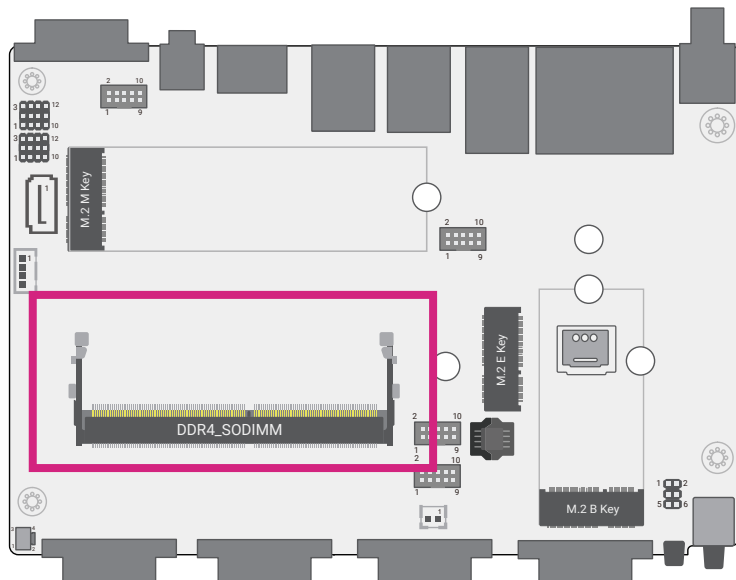
Step 2:
Insert the memory card into the slot while making sure 1) the notch and the key are aligned, and 2) the non-connector end rises approximately 45 degrees horizontally. Press the card firmly into the socket while applying and maintaining even pressure on both ends.

45°

Step 2

Retention Notch
↓ Notch
≪ **DDR3 SO-DIMM**

Retention Clip
↓ Key
≪ **Socket Top View**
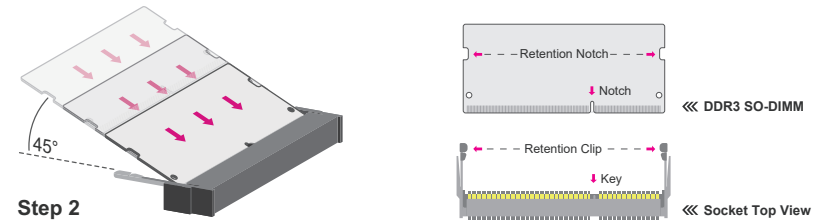
Step 3:
Press the end of the card far from the socket down while making sure the retention notch and the clip align as indicated by the dotted line in the illustration. If the retention notch and the clip do not align, please remove the card and re-insert it. Press the card all the way down.

Step 3
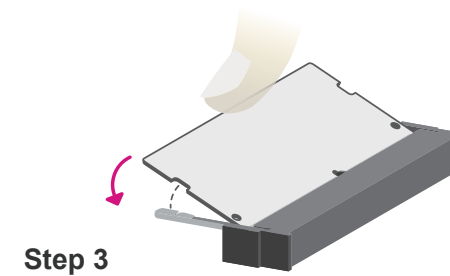
Step 4:
The clips snap automatically and abruptly to the retention notches of the card sounding a distinctive click, and lock the card in place. Inspect that the clip sits in the notch. If not, please pull the clips outward, release and remove the card, and mount it again.

Step 4
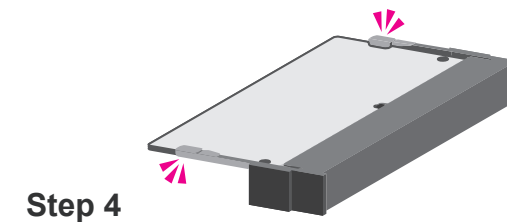
▶ **Installing the M.2 Module**

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.
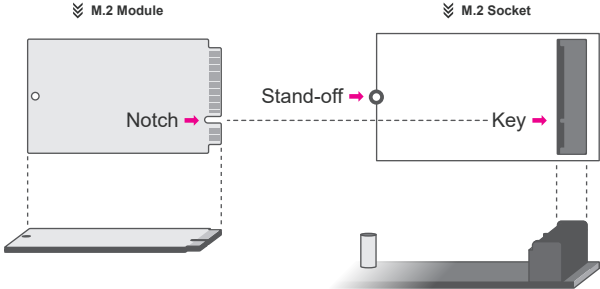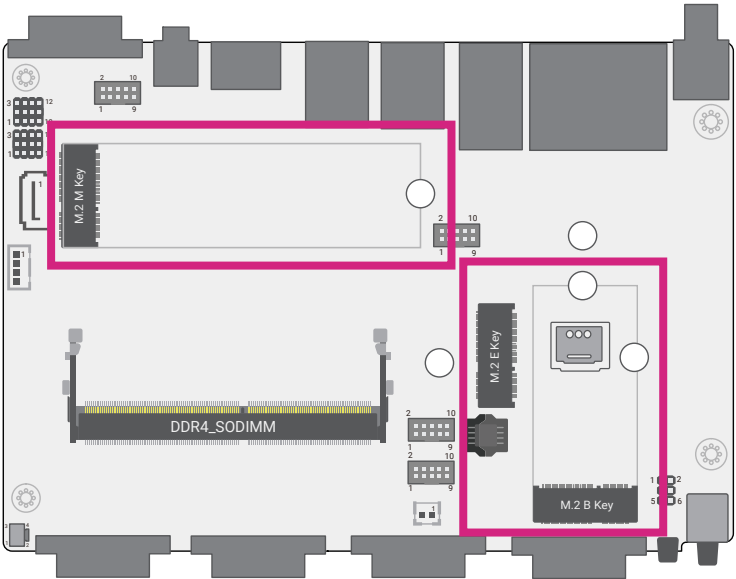
Please follow the steps below to install the card into the socket.
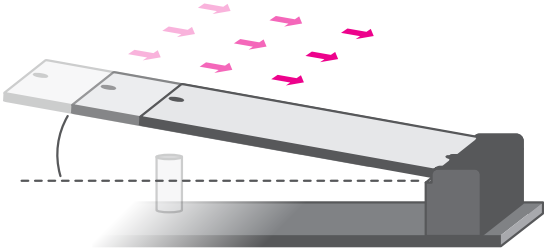
Step 1:
Insert the card into the socket at an angle while making sure the notch and key are perfectly aligned.
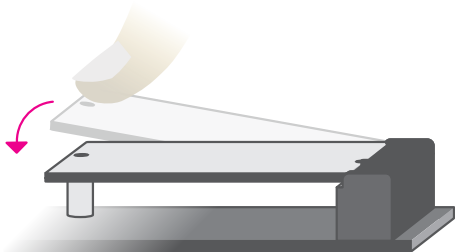
Step 2:
Press the end of the card far from the socket down until against the stand-off.
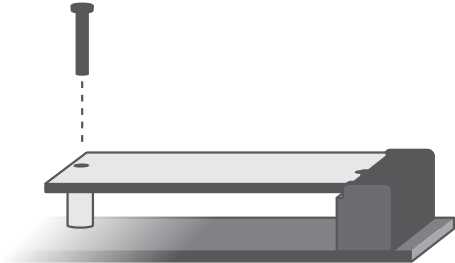
Step 3:
Screw tight the card onto the stand-off with a screw driver and a stand-off screw until the gap between the card and the stand-off closes up. The card should be lying parallel to the board when it's correctly mounted.

Chapter 3 - System Settings

▶ System Layout
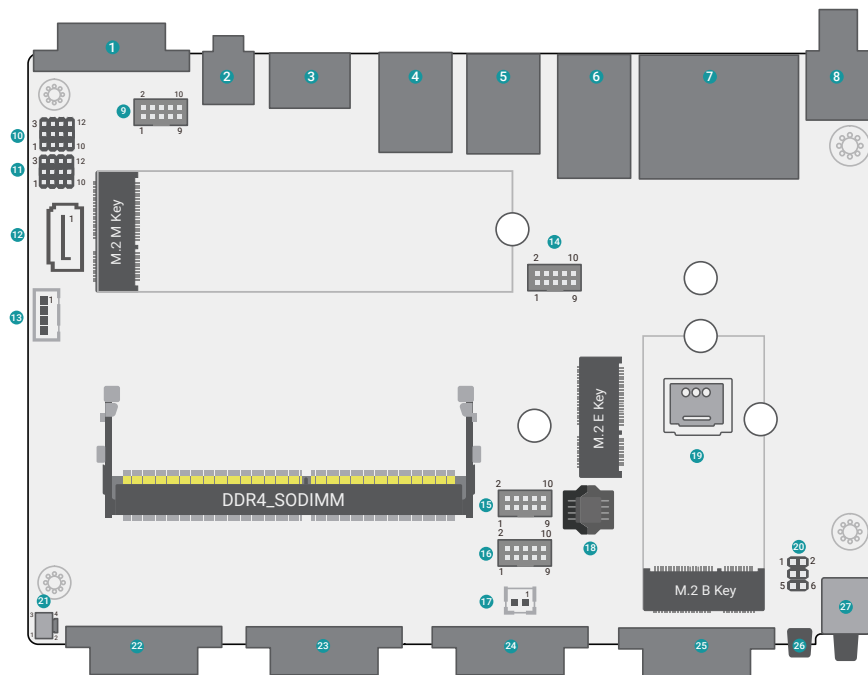
1	COM3 (RS232) / DIO (Optional)
2	Audio
3	HDMI
4	▲USB3.2 Type A ▼USB3.2 Type C
5	▲USB3.2 Type A ▼USB3.2 Type C
6	2.5G LAN3
7	LAN2 / LAN1
8	DC-IN
9	Front Audio
10	COM Serial / DIO Switch (JP8)
11	COM Serial / DIO Switch (JP9)
12	SATA
13	SATA Power
14	USB2.0
15	COM6
16	COM5
17	RTC Battery
18	SPI
19	SIM Slot
20	Front Panel

21	Clear CMOS
22	COM2
23	COM1
24	COM4
25	VGA
26	Reset Button
27	Power Button

▶ **Jumper Settings**

▶ **Pin Assignment**

COM Serial / DIO Switch

RTC Battery

JP8

JP9

3 12
1 10

3 12
1 10
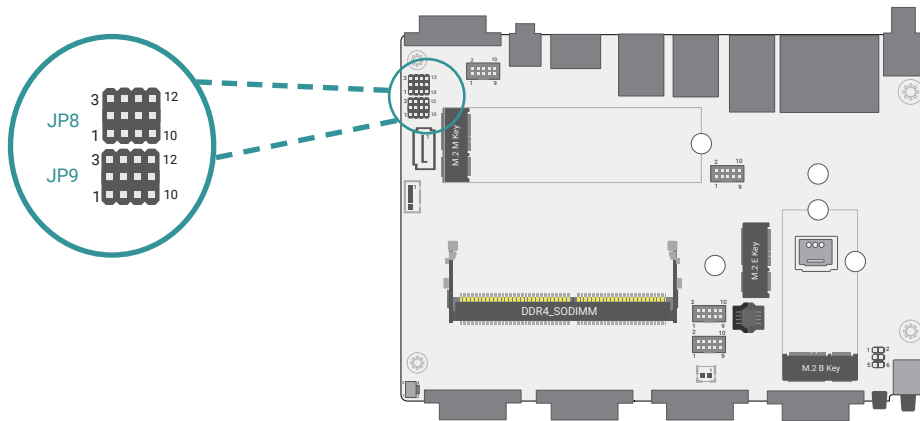
3 12
1 10
■ Serial COM Signal (Default)

3 12
1 10
■ DIO Signal (Opt.)

1
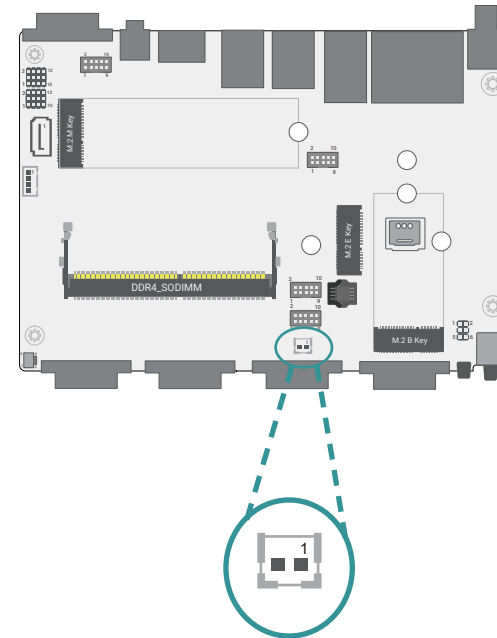
Pin	Assignment
1	V_BAT
2	GND

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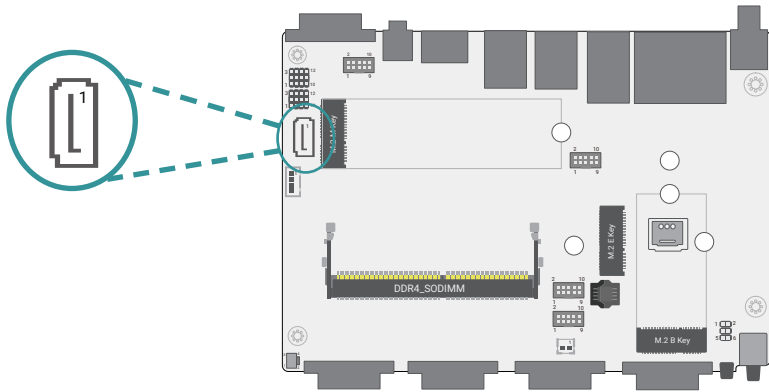
Pin	Assignment
1	GND
2	TX+
3	TX-
4	GND
5	RX-
6	RX+
7	GND

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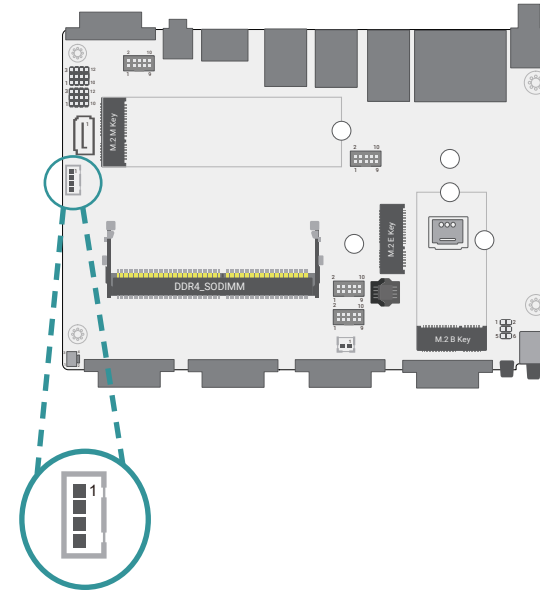
Pin	Assignment
1	12V
2	GND
3	GND
4	5V

Front Panel
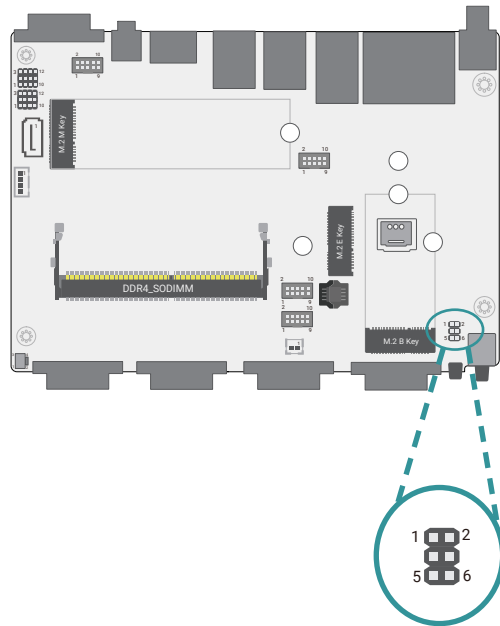
Pin	Assignment	Pin	Assignment
1	PWR_BTN0	2	V_SUS_LED
3	GND	4	SUS_LED#
5	SYS_RST0	6	HD_LED#

COM1 & COM2
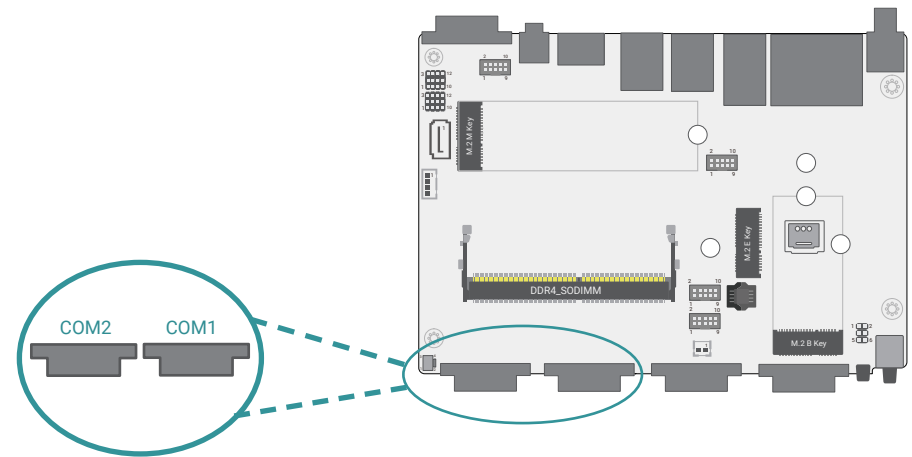
Pin	RS232	RS422	RS485
1	DCD-	TXD-	Data-
2	RD	TXD+	Data+
3	TD	RXD+	N.C.
4	DTR-	RXD-	N.C.
5	GND	GND	GND
6	DSR-	N.C.	N.C.
7	RTS-	N.C.	N.C.
8	CTS-	N.C.	N.C.
9	RI-	N.C.	N.C.

COM4 & COM5 & COM6
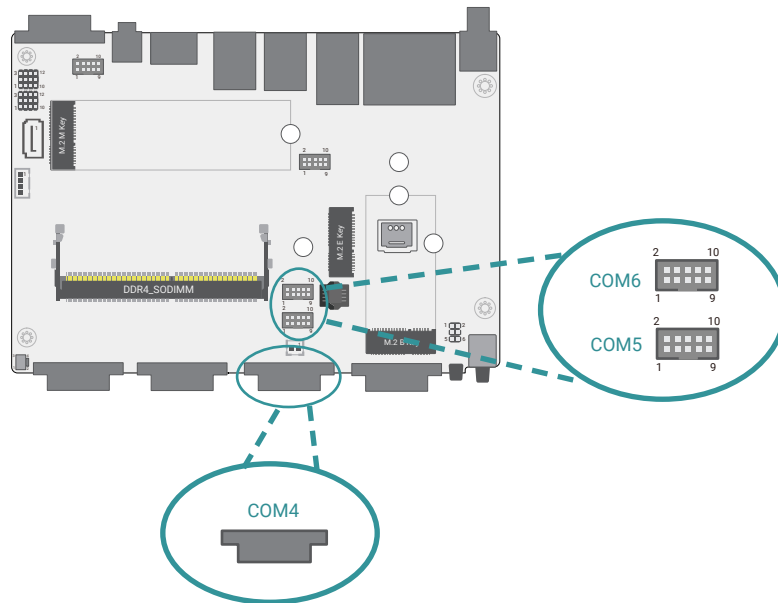
COM3/DIO (Optional)

Pin	Assignment	Pin	Assignment
1	MDCD-	2	MSIN-
3	MSO-	4	MDTR-
5	GND	6	MDSR-
7	MRTS-	8	MCTS-
9	MRI-	10	NC
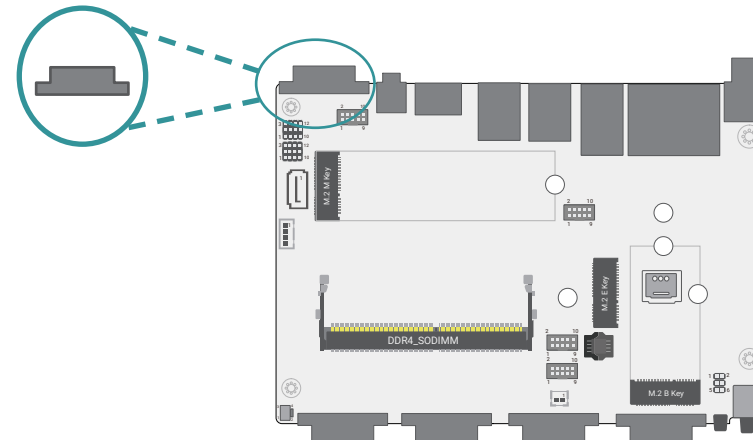
■ COM3 Pin Assignment

Pin	Assignment	Pin	Assignment
1	MDCD-	2	MSIN-
3	MSO-	4	MDTR-
5	GND	6	MDSR-
7	MRTS-	8	MCTS-
9	MRI-	10	NC

■ DIO Pin Assignment (Optional)

Pin	Assignment	Pin	Assignment
1	DIOA0	2	DIOA1
3	DIOA2	4	DIOA3
5	GND	6	DIOA6
7	DIOA7	8	DIOA4
9	DIOA5		

Chapter 4 - 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.

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

    Project Name                EC70A-ADP          Set the Date. Use Tab to
    BIOS Version                B23A.26A           switch between Date elements.
                                                   Default Ranges:
    FSP version                 0C.01.73.10        Year: 1998-2121
    RC version                  0C.E0.73.10        Months: 1-12
                                                   Days: Dependent on month
    12th Gen Intel(R) Core(TM) i7-1265UE           Range of Years may vary.
    ID                          0x906A4
    Stepping                    R0
    Number of Efficient-cores   8Core(s) / 8Thread(s)
    Number of Performance-cores 2Core(s) / 4Thread(s)
    Microcode Revision          423

    Memory RC Version           0.0.4.60           →←: Select Screen
    Total Memory                8192 MB            ↑↓: Select Item
    Memory Frequency            3200 MHz           Enter: Select
                                                   +/- : Change Opt.
    PCH SKU                     PCH-P P Premium    F1: General Help
    ME FW Version               16.1.25.2020       F2: Previous Values
    ME Firmware SKU             Corporate SKU      F9: Optimized Defaults
    PMC FW Version              160.1.0.1028       F10: Save & Reset
                                                   ESC: Exit
    System Date                 [Mon 07/15/2024]
    System Time                 [02:48:35]

                    Version 2.22.1287 Copyright (C) 2023 AMI
```

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.

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

    ▶ CPU Configuration                            CPU Configuration Parameters
    ▶ Power & Performance
    ▶ PCH-FW Configuration
    ▶ Trusted Computing
    ▶ IT8786 Super IO Configuration
    ▶ IT8786 Hardware Monitor
    ▶ Serial Port Console Redirection
    ▶ ACPI Settings
    ▶ Network Stack Configuration
    ▶ NVMe Configuration
    ▶ DFI WDT Configuration
    ▶ USB Power Control

    ▶ Tls Auth Configuration

                                                   →←: Select Screen
                                                   ↑↓: Select Item
                                                   Enter: Select
                                                   +/- : Change Opt.
                                                   F1: General Help
                                                   F2: Previous Values
                                                   F9: Optimized Defaults
                                                   F10: Save & Reset
                                                   ESC: Exit

                    Version 2.22.1287 Copyright (C) 2023 AMI
```

▶ **Advanced**

▶ **Advanced**

CPU Configuration

Power & Performance

```
                           Aptio Setup - AMI
   Advanced

   CPU Configuration                                    When enabled, a VMM can
                                                        utilize the additional
   Intel (VMX) Virtualization        [Enabled]          hardware capabilities provided
   Technology                                           by Vanderpool Technology.
   Hyper-Threading                   [Enabled]
   AES                               [Enabled]




                                                        ↔: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/- : Change Opt.
                                                        F1: General Help
                                                        F2: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset
                                                        ESC: Exit



                     Version 2.22.1287 Copyright (C) 2023 AMI
```

```
                           Aptio Setup - AMI
      Advanced

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




                                                        ↔: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/- : Change Opt.
                                                        F1: General Help
                                                        F2: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset
                                                        ESC: Exit



                     Version 2.22.1287 Copyright (C) 2023 AMI
```

Intel (VMX) Virtualization Technology

When this field is set to Enabled, the VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.

Hyper-threading

Enables this field for Windows XP and Linux which are optimized for Hyper-Threading technology. Select disabled for other OSes not optimized for Hyper-Threading technology. When disabled, only one thread per enabled core is enabled.

AES

Enable / Disable AES (Advanced Encryption Standard)

▶ **Advanced**

Power & Performance ▶ **CPU- Power Management Control**

```
                          Aptio Setup - AMI
      Advanced
┌─────────────────────────────────────────┬──────────────────────────┐
│  CPU - Power Management Control          │Enable/Disable processor Turbo│
│                                          │Mode (requires EMTTM enabled│
│    Turbo Mode              [Enabled]     │too). AUTO means enabled.  │
│  ▶ Config TDP Configurations             │                          │
│  C states                  [Enabled]     │                          │
│                                          │                          │
│                                          │                          │
│                                          │                          │
│                                          │                          │
│                                          ├──────────────────────────┤
│                                          │→←: Select Screen         │
│                                          │↑↓: Select Item           │
│                                          │Enter: Select             │
│                                          │+/- : Change Opt.         │
│                                          │F1: General Help          │
│                                          │F2: Previous Values       │
│                                          │F9: Optimized Defaults    │
│                                          │F10: Save & Reset         │
│                                          │ESC: Exit                 │
│                                          │                          │
└─────────────────────────────────────────┴──────────────────────────┘
              Version 2.22.1287 Copyright (C) 2023 AMI
```
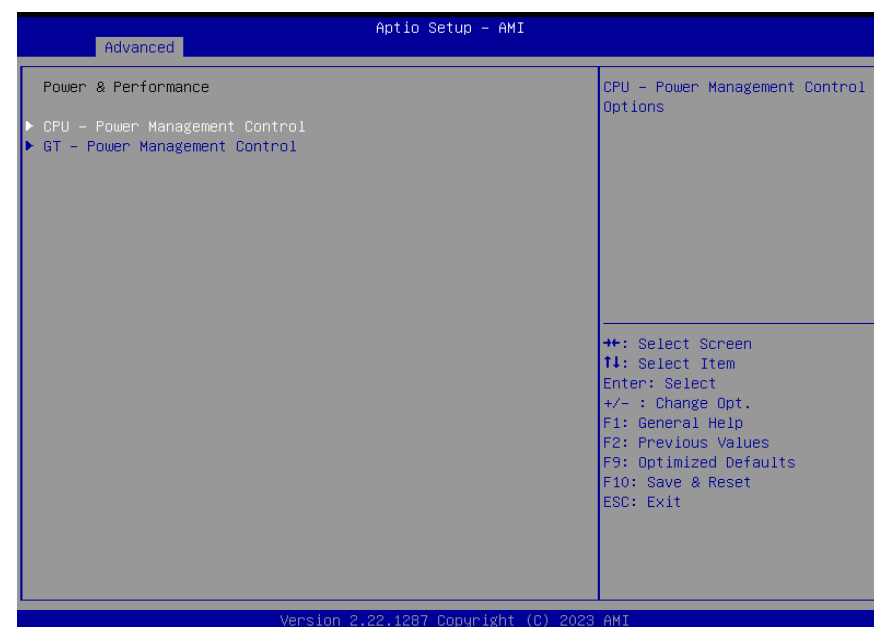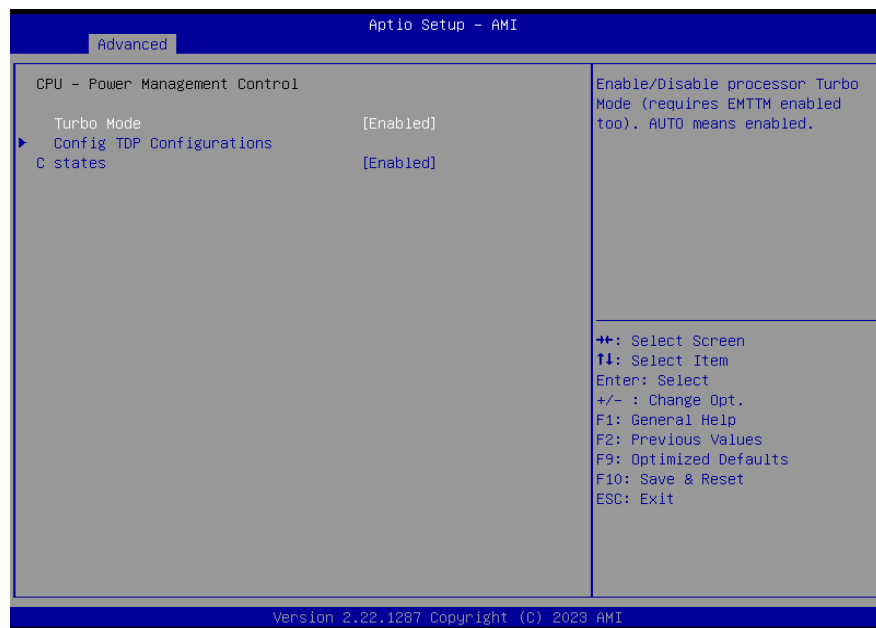
Turbo Mode

Enable/Disable processor Turbo Mode (requires EMTTM enabled too). AUTO means enabled.

Configure Turbo Options

Configure Turbo Options.

C states

Enable or disable CPU Power Management. It allows CPU to enter "C states" when it's idle and nothing is executing.

▶ **Advanced**

Power & Performance ▶ **GT- Power Management Control**

```
                          Aptio Setup - AMI
      Advanced
┌─────────────────────────────────────────┬──────────────────────────┐
│  GT - Power Management Control           │Check to enable render standby│
│                                          │support.                  │
│  RC6(Render Standby)       [Enabled]     │                          │
│                                          │                          │
│                                          │                          │
│                                          │                          │
│                                          │                          │
│                                          │                          │
│                                          │                          │
│                                          ├──────────────────────────┤
│                                          │→←: Select Screen         │
│                                          │↑↓: Select Item           │
│                                          │Enter: Select             │
│                                          │+/- : Change Opt.         │
│                                          │F1: General Help          │
│                                          │F2: Previous Values       │
│                                          │F9: Optimized Defaults    │
│                                          │F10: Save & Reset         │
│                                          │ESC: Exit                 │
│                                          │                          │
└─────────────────────────────────────────┴──────────────────────────┘
              Version 2.22.1287 Copyright (C) 2023 AMI
```
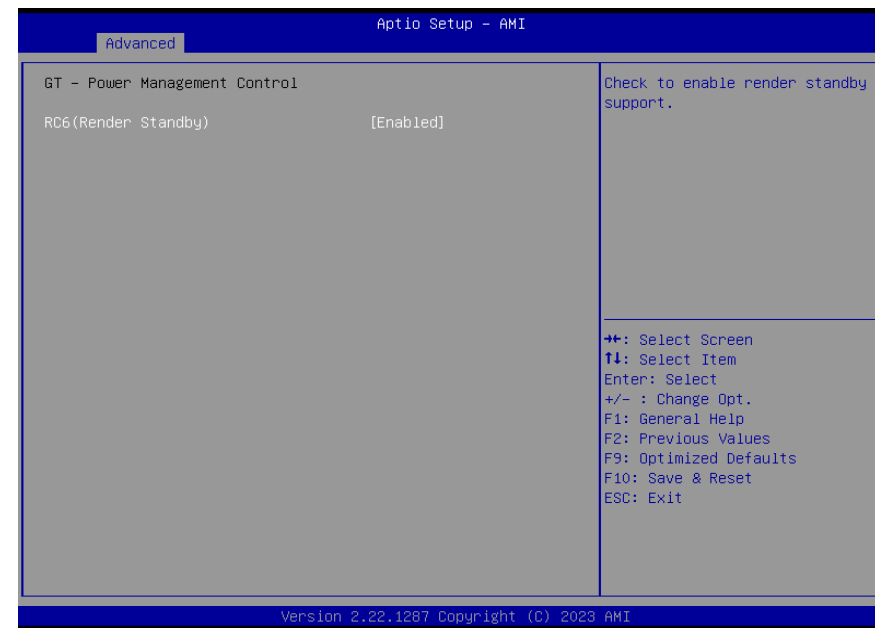
RC6 (Render Standby)
Check to enable render standby support.

▶   Advanced

PCH-FW Configuration

```
                            Aptio Setup - AMI
    Advanced

 ME State                         [Enabled]          When Disabled ME will be put
 Manageability Features State     [Enabled]          into ME Temporarily Disabled
 AMT BIOS Features                [Enabled]          Mode.
 ME Unconfig on RTC Clear         [Enabled]

 ▶ Firmware Update Configuration




                                                     →←: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
                                                     +/- : Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F9: Optimized Defaults
                                                     F10: Save & Reset
                                                     ESC: Exit



               Version 2.22.1287 Copyright (C) 2023 AMI
```

ME State

When this field is set to Disabled, ME will be put into ME Temporarily Disabled Mode.

Manageability Features State

Enable or disable Intel(R) Manageability features. This option disables/enables Manageability Features support in FW. To disable, support platform must be in an unprovisioned state first.

AMT BIOS Features

When disabled, AMT BIOS features are no longer supported and user is no longer able to access MEBx Setup. This option does not disable manageability features in FW.

ME Unconfig on RTC Clear

When disabled, ME will not be unconfigured on RTC Clear.

Firmware Update Configuration

Configure Management Engine Technology Parameters.

> **Note:**
> The sub-menus are detailed in following sections.

▶ **Advanced**

Trusted Computing

```
                              Aptio Setup - AMI
    ┌──────────┐
    │ Advanced │
    └──────────┘
    ┌─────────────────────────────────────────────────┬───────────────────────────┐
    │  TPM 2.0 Device Found                            │ Enables or Disables BIOS  │
    │  Firmware Version:             7.2               │ support for security device.│
    │  Vendor:                       NTC               │ O.S. will not show Security │
    │                                                  │ Device. TCG EFI protocol and│
    │  Security Device Support       [Enable]          │ INT1A interface will not be │
    │  Active PCR banks              SHA256            │ available.                  │
    │  Available PCR banks           SHA256,SHA384     │                             │
    │                                                  │                             │
    │                                                  │                             │
    │  Pending operation             [None]            │                             │
    │                                                  │                             │
    │                                                  │                             │
    │                                                  │ →←: Select Screen           │
    │                                                  │ ↑↓: Select Item             │
    │                                                  │ Enter: Select               │
    │                                                  │ +/- : Change Opt.           │
    │                                                  │ F1: General Help            │
    │                                                  │ F2: Previous Values         │
    │                                                  │ F9: Optimized Defaults      │
    │                                                  │ F10: Save & Reset           │
    │                                                  │ ESC: Exit                   │
    │                                                  │                             │
    └─────────────────────────────────────────────────┴───────────────────────────┘
                    Version 2.22.1287 Copyright (C) 2023 AMI
```

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**

NCT5525D Super IO Configuration

```
                              Aptio Setup - AMI
    ┌──────────┐
    │ Advanced │
    └──────────┘
    ┌─────────────────────────────────────────────────┬───────────────────────────┐
    │  IT8786 Super IO Configuration                   │ Set Parameters of Serial Port│
    │                                                  │ 1 (COMA)                  │
    │  Super IO Chip                 IT8786            │                             │
    │ ▶ Serial Port 1 Configuration                    │                             │
    │ ▶ Serial Port 2 Configuration                    │                             │
    │ ▶ Serial Port 3 Configuration                    │                             │
    │ ▶ Serial Port 4 Configuration                    │                             │
    │ ▶ Serial Port 5 Configuration                    │                             │
    │ ▶ Serial Port 6 Configuration                    │                             │
    │                                                  │                             │
    │                                                  │ →←: Select Screen           │
    │                                                  │ ↑↓: Select Item             │
    │                                                  │ Enter: Select               │
    │                                                  │ +/- : Change Opt.           │
    │                                                  │ F1: General Help            │
    │                                                  │ F2: Previous Values         │
    │                                                  │ F9: Optimized Defaults      │
    │                                                  │ F10: Save & Reset           │
    │                                                  │ ESC: Exit                   │
    └─────────────────────────────────────────────────┴───────────────────────────┘
                    Version 2.22.1287 Copyright (C) 2023 AMI
```

▶ **Advanced**

NCT5525D Super IO Configuration ▶ **Serial Port 1, 2 Configuration**
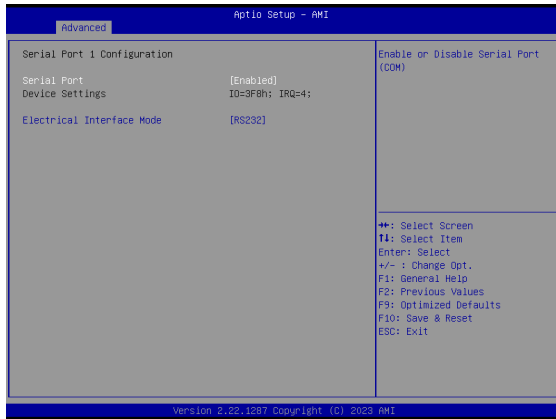
Serial Port
Enable or disable serial port.

▶ **Advanced**

NCT5525D Super IO Configuration ▶ **Serial Port 3, 4 Configuration**
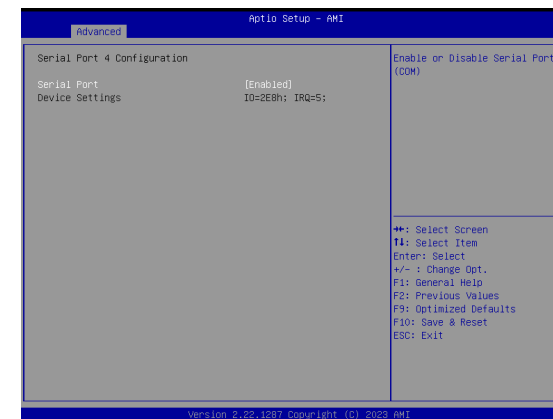
Serial Port
Enable or disable serial port.

▶ **Advanced**

NCT5525D Super IO Configuration   ▶ **Serial Port 5, 6 Configuration**
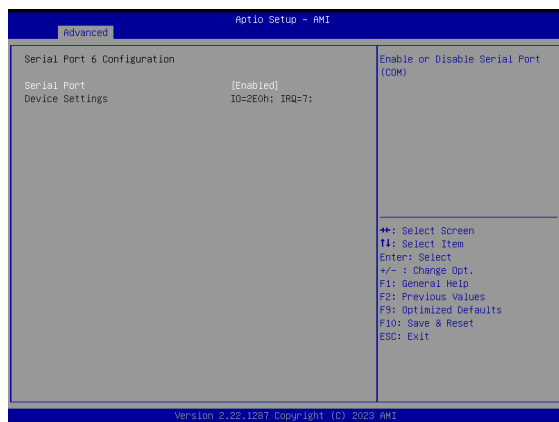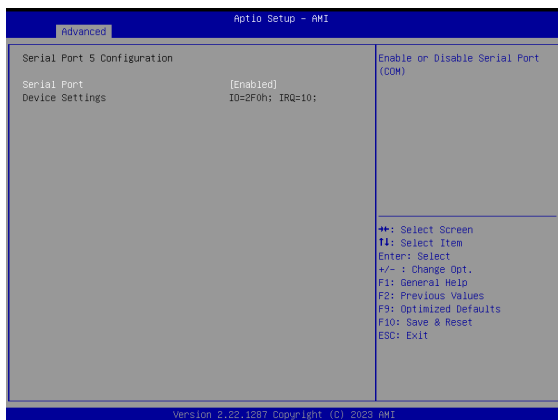
▶ **Advanced**

NCT5525D HW Monitor
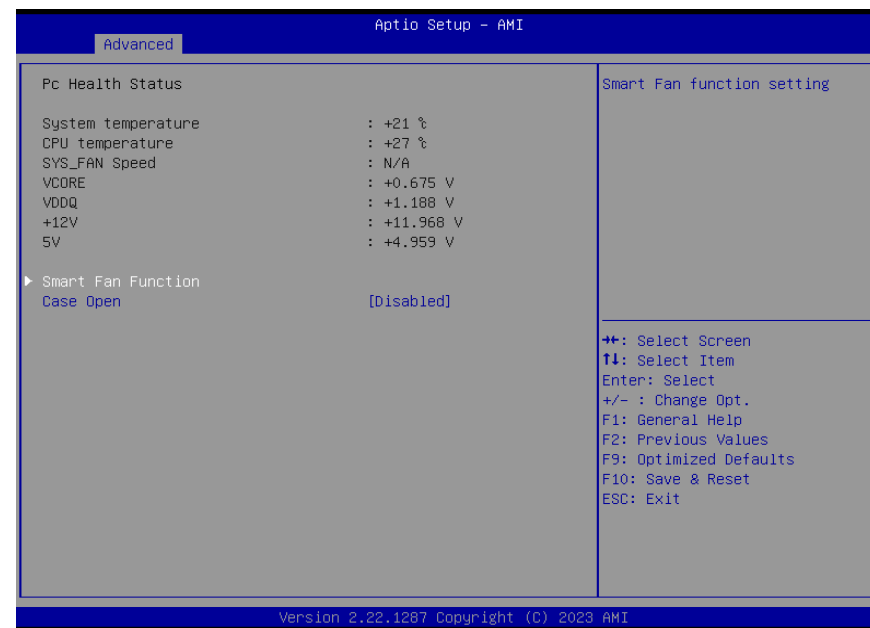
This section displays the system's health information, i.e. voltage readings, CPU and system temperatures, and fan speed readings

Smart Fan Function

Smart Fan Function Setting.

Case Open

Enable or disable the case open detection function.

Serial Port

Enable or disable serial port.

▶ **Advanced**

NCT5525D HW Monitor ▶ **Smart FAN Function**

```
                        Aptio Setup – AMI
      Advanced
┌─────────────────────────────────────────────────────────────────┐
│ ▶ SYS_FAN Setting                    │ Smart Fan function setting │
│                                      │                            │
│                                      │                            │
│                                      │                            │
│                                      │                            │
│                                      │                            │
│                                      │                            │
│                                      ├────────────────────────────┤
│                                      │ →←: Select Screen          │
│                                      │ ↑↓: Select Item            │
│                                      │ Enter: Select              │
│                                      │ +/– : Change Opt.          │
│                                      │ F1: General Help           │
│                                      │ F2: Previous Values        │
│                                      │ F9: Optimized Defaults     │
│                                      │ F10: Save & Reset          │
│                                      │ ESC: Exit                  │
│                                      │                            │
└─────────────────────────────────────────────────────────────────┘
           Version 2.22.1287 Copyright (C) 2023 AMI
```
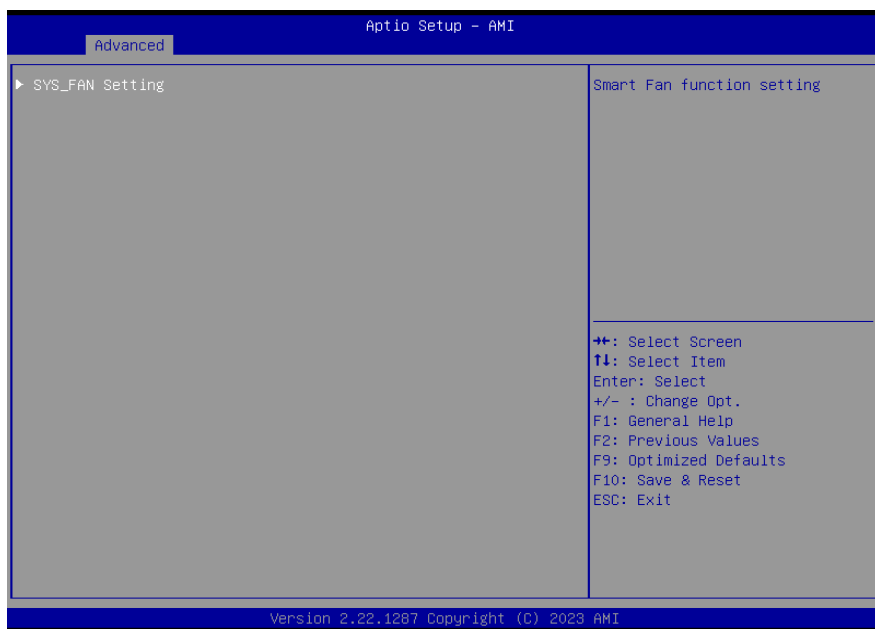
▶ **Advanced**

NCT5525D HW Monitor ▶ **Smart FAN Function** ▶ **SYS FAN Setting**

```
                        Aptio Setup – AMI
      Advanced
┌─────────────────────────────────────────────────────────────────┐
│ SYS_FAN Setting                              │ Smart Fan Mode Select│
│ SYS_FAN Mode              [Automatic Mode]   │                      │
│ Fan off temperature limit      0             │                      │
│ Fan start temperature limit    60            │                      │
│ Fan full speed temperature limit  85         │                      │
│ Fan start PWM                  51            │                      │
│                                              │                      │
│                                              ├──────────────────────┤
│                                              │ →←: Select Screen    │
│                                              │ ↑↓: Select Item      │
│                                              │ Enter: Select        │
│                                              │ +/– : Change Opt.    │
│                                              │ F1: General Help     │
│                                              │ F2: Previous Values  │
│                                              │ F9: Optimized Defaults│
│                                              │ F10: Save & Reset    │
│                                              │ ESC: Exit            │
│                                              │                      │
└─────────────────────────────────────────────────────────────────┘
           Version 2.22.1287 Copyright (C) 2023 AMI
```

SYS_FAN Mode

Smart Fan Mode Select

Fan off temperature limit

Fan will be turned off when the temperature is lower than this limit.

Fan start temperature limit
Fan will start working when the temperature is higher than this limit.

Fan full speed temperature limit

Fan will be full speed when the temperature is higher than this limit.

Fan start PWM

Fan will start with this PWM value.

▶ **Advanced**

Serial Port Console Redirection

```
                        Aptio Setup - AMI
      Advanced
  ┌────────────────────────────────────────┬─────────────────────────┐
  │                                         │ Console Redirection Enable or │
  │  COM1                                   │ Disable.                │
  │  Console Redirection        [Disabled]  │                         │
  │ ▶ Console Redirection Settings          │                         │
  │                                         │                         │
  │  COM2                                   │                         │
  │  Console Redirection        [Disabled]  │                         │
  │ ▶ Console Redirection Settings          │                         │
  │                                         │                         │
  │                                         ├─────────────────────────┤
  │                                         │ →←: Select Screen       │
  │                                         │ ↑↓: Select Item         │
  │                                         │ Enter: Select           │
  │                                         │ +/- : Change Opt.       │
  │                                         │ F1: General Help        │
  │                                         │ F2: Previous Values     │
  │                                         │ F9: Optimized Defaults  │
  │                                         │ F10: Save & Reset       │
  │                                         │ ESC: Exit               │
  │                                         │                         │
  └────────────────────────────────────────┴─────────────────────────┘
              Version 2.22.1287 Copyright (C) 2023 AMI
```
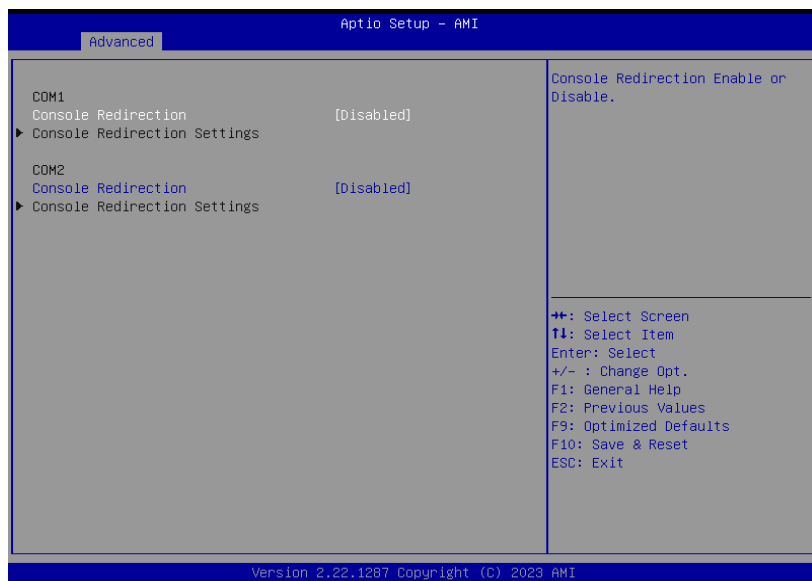
Console Redirection

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**

```
                        Aptio Setup - AMI
      Advanced
  ┌──────────────────────────────────────────┬──────────────────────────┐
  │  COM1                                     │ Emulation: ANSI: Extended │
  │  Console Redirection Settings             │ ASCII char set. VT100: ASCII │
  │                                           │ char set. VT100Plus: Extends │
  │  Terminal Type            [VT100Plus]     │ VT100 to support color,  │
  │  Bits per second          [115200]        │ function keys, etc. VT-UTF8: │
  │  Data Bits                [8]             │ Uses UTF8 encoding to map │
  │  Parity                   [None]          │ Unicode chars onto 1 or more │
  │  Stop Bits                [1]             │ bytes.                   │
  │  Flow Control             [None]          │                          │
  │  VT-UTF8 Combo Key Support [Enabled]      │                          │
  │  Recorder Mode            [Disabled]      │                          │
  │  Resolution 100x31        [Enabled]       │                          │
  │  Putty KeyPad             [VT100]         ├──────────────────────────┤
  │                                           │ →←: Select Screen        │
  │                                           │ ↑↓: Select Item          │
  │                                           │ Enter: Select            │
  │                                           │ +/- : Change Opt.        │
  │                                           │ F1: General Help         │
  │                                           │ F2: Previous Values      │
  │                                           │ F9: Optimized Defaults   │
  │                                           │ F10: Save & Reset        │
  │                                           │ ESC: Exit                │
  └──────────────────────────────────────────┴──────────────────────────┘
              Version 2.22.1287 Copyright (C) 2023 AMI
```

```
                        Aptio Setup - AMI
      Advanced
  ┌──────────────────────────────────────────┬──────────────────────────┐
  │  COM2                                     │ Emulation: ANSI: Extended │
  │  Console Redirection Settings             │ ASCII char set. VT100: ASCII │
  │                                           │ char set. VT100Plus: Extends │
  │  Terminal Type            [VT100Plus]     │ VT100 to support color,  │
  │  Bits per second          [115200]        │ function keys, etc. VT-UTF8: │
  │  Data Bits                [8]             │ Uses UTF8 encoding to map │
  │  Parity                   [None]          │ Unicode chars onto 1 or more │
  │  Stop Bits                [1]             │ bytes.                   │
  │  Flow Control             [None]          │                          │
  │  VT-UTF8 Combo Key Support [Enabled]      │                          │
  │  Recorder Mode            [Disabled]      │                          │
  │  Resolution 100x31        [Enabled]       │                          │
  │  Putty KeyPad             [VT100]         ├──────────────────────────┤
  │                                           │ →←: Select Screen        │
  │                                           │ ↑↓: Select Item          │
  │                                           │ Enter: Select            │
  │                                           │ +/- : Change Opt.        │
  │                                           │ F1: General Help         │
  │                                           │ F2: Previous Values      │
  │                                           │ F9: Optimized Defaults   │
  │                                           │ F10: Save & Reset        │
  │                                           │ ESC: Exit                │
  └──────────────────────────────────────────┴──────────────────────────┘
              Version 2.22.1287 Copyright (C) 2023 AMI
```

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.

Flow Control

Select flow control type: None or Hardware RTS/CTS. Flow Control is for RS485 mode and is only supported by Serial Port 1 (COM1).

VT-UTF8 Combo Key Support

Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.

Recorder Mode

With this mode enbaled only text will be sent. This is to capture Terminal data.

Resolution 100x31

Enables or disables extended terminal resolution

Putty KeyPad

Select FunctionKey and KeyPad on Putty.

▶ **Advanced**

ACPI Settings

```
                                    Aptio Setup - AMI
     Advanced

     ACPI Settings                                        Enable or disable System wake
                                                          on alarm event. When enabled,
     Wake System from S5 via RTC        [Disabled]        System will wake on the
     State After G3                     [S0 State]        hr::min::sec specified




                                                          →←: Select Screen
                                                          ↑↓: Select Item
                                                          Enter: Select
                                                          +/- : Change Opt.
                                                          F1: General Help
                                                          F2: Previous Values
                                                          F9: Optimized Defaults
                                                          F10: Save & Reset
                                                          ESC: Exit



                            Version 2.22.1287 Copyright (C) 2023 AMI
```
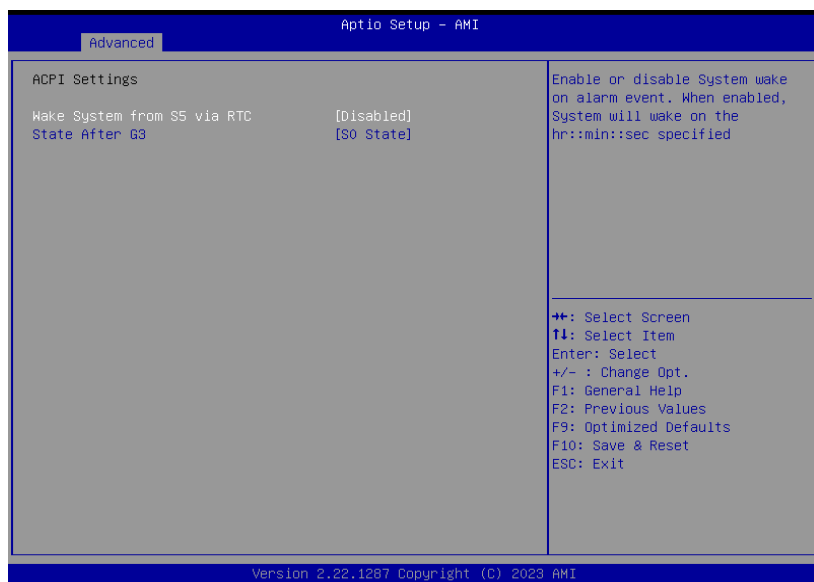
Wake system from S5 via RTC

When Enabled, the system will automatically power up at a designated time every day. Once it's switched to [Enabled], please set up the time of day — hour, minute, and second — for the system to wake up.

State After G3

Select between S0 State, and S5 State. This field is used to specify what state the system is set to return to when power is re-applied after a power failure (G3 state).

• **S0 State**   The system automatically powers on after power failure.

• **S5 State**   The system enter soft-off state after power failure. Power-on signal input is required to power up the system.

▶ **Advanced**

Network Stack Configuration

```
                                    Aptio Setup - AMI
     Advanced

     Network Stack                      [Enabled]         Enable/Disable UEFI Network
       IPv4 PXE Support                 [Disabled]        Stack
       IPv4 HTTP Support                [Disabled]
       IPv6 PXE Support                 [Disabled]
       IPv6 HTTP Support                [Disabled]
       PXE boot wait time               0
       Media detect count               1


                                                          →←: Select Screen
                                                          ↑↓: Select Item
                                                          Enter: Select
                                                          +/- : Change Opt.
                                                          F1: General Help
                                                          F2: Previous Values
                                                          F9: Optimized Defaults
                                                          F10: Save & Reset
                                                          ESC: Exit

                            Version 2.22.1287 Copyright (C) 2023 AMI
```

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.

Ipv4 HTTP Support

Enable or disable IPv4 HTTP boot support. If disabled, IPv4 HTTP 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.

Ipv6 HTTP Support

Enable or disable IPv6 HTTP boot support. If disabled, IPv6 HTTP 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**

DFI WDT Configuration

```
                          Aptio Setup - AMI
        Advanced

   DFI WDT Configuration                          Enable/Disable Watchdog Timer

   Watchdog Timer                 [Enabled]
      Timeout Delay               15



                                                →←: Select Screen
                                                ↑↓: Select Item
                                                Enter: Select
                                                +/- : Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F9: Optimized Defaults
                                                F10: Save & Reset
                                                ESC: Exit


              Version 2.22.1287 Copyright (C) 2023 AMI
```
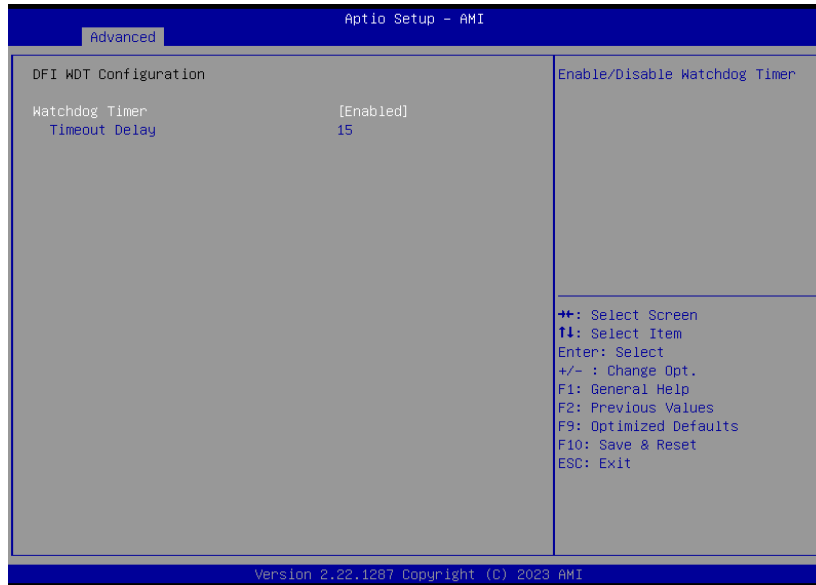
Watchdog Timer

Enable or disable Watchdog Timer.

▶ **Advanced**

USB Power Control

```
                          Aptio Setup - AMI
        Advanced

   USB3_TypeA_UBCN1              [5V_Dual]       5V_Dual: Support system wake
   USB3_TypeA_UBCN2              [5V_Dual]       up from S3/S4 by USB KB&MS
   USB2_5/6                      [5V_Dual]       5V: No support system wake up
                                                from S3/S4 by USB KB&MS



                                                →←: Select Screen
                                                ↑↓: Select Item
                                                Enter: Select
                                                +/- : Change Opt.
                                                F1: General Help
                                                F2: Previous Values
                                                F9: Optimized Defaults
                                                F10: Save & Reset
                                                ESC: Exit


              Version 2.22.1287 Copyright (C) 2023 AMI
```
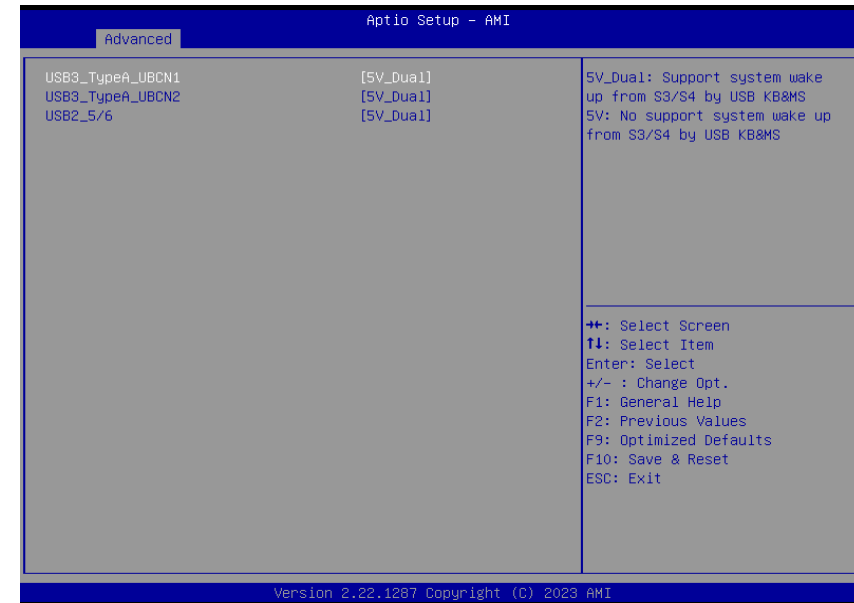
Server CA Configuration

5_Dual: Support system wake up from S3/S4 by USB KB&MS

5V: No support system wake up from S3/S4 by USB KB&MS

▶ **Advanced**

Tls Auth Configuration

```
                          Aptio Setup - AMI
         Advanced

   ▶ Server CA Configuration              Press <Enter> to configure
                                          Server CA.
   ▶ Client Cert Configuration




                                          →←: Select Screen
                                          ↑↓: Select Item
                                          Enter: Select
                                          +/- : Change Opt.
                                          F1: General Help
                                          F2: Previous Values
                                          F9: Optimized Defaults
                                          F10: Save & Reset
                                          ESC: Exit


              Version 2.22.1287 Copyright (C) 2023 AMI
```

Server CA Configuration

Press <Enter> to configure Server CA.

▶ **Chipset**

System Agent (SA) Configuration

Please select a submenu and press Enter. The submenus are detailed in the following pages.
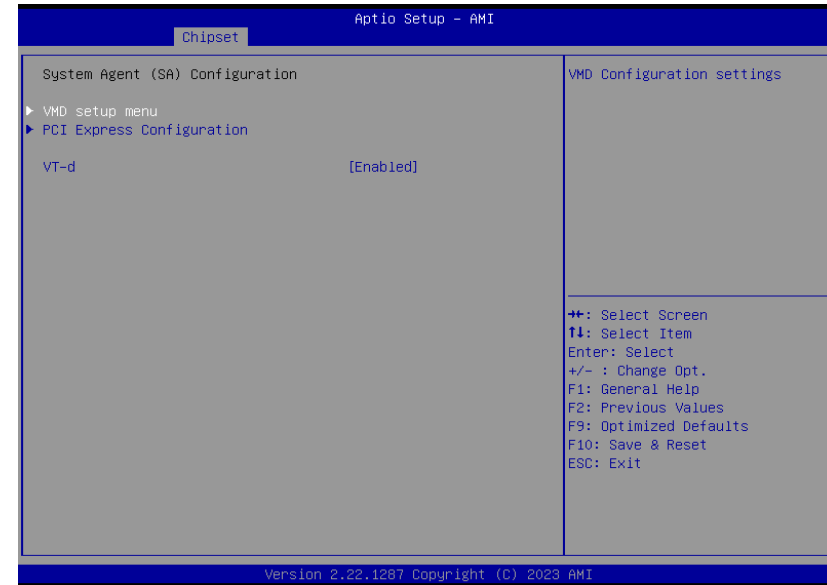
VMD setup menu
VMD Configuration Settings

PCI Express Configuration :

VT-d
VT-d capability.

▶ **Chipset**

PCH-IO Configuration

```
                     Aptio Setup - AMI
          ┌─────────┐
          │ Chipset │
          └─────────┘

   PCH-IO Configuration                      │ PCI Express Configuration
                                             │ settings
 ▶ PCI Express Configuration                 │
 ▶ SATA Configuration                        │
 ▶ HD Audio Configuration                    │
                                             │
                                             │
                                             │
                                             │
                                             │
                                             │ →←: Select Screen
                                             │ ↑↓: Select Item
                                             │ Enter: Select
                                             │ +/- : Change Opt.
                                             │ F1: General Help
                                             │ F2: Previous Values
                                             │ F9: Optimized Defaults
                                             │ F10: Save & Reset
                                             │ ESC: Exit
                                             │
                                             │
                                             │
         Version 2.22.1287 Copyright (C) 2023 AMI
```
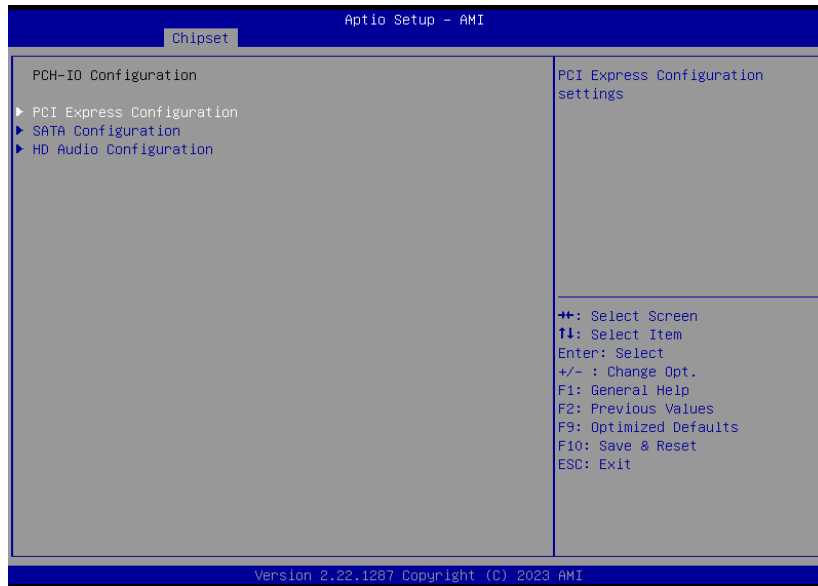
PCI Express Configuration

PCI Express Configuration Settings

SATA Configuration

SATA Device Otpions Settings

HD Audio Configuration

HD Audio Subsystem Configuration Settings

▶ **Chipset**

PCH-IO Configuration▶ **PCI Express Configuration**

```
                     Aptio Setup - AMI
          ┌─────────┐
          │ Chipset │
          └─────────┘

   PCI Express Configuration                 │ PCI Express Root Port Settings.
                                             │
 ▶ M.2-B                                     │
 ▶ LAN1                                      │
 ▶ LAN2                                      │
 ▶ LAN3                                      │
 ▶ M.2-E                                     │
                                             │
                                             │
                                             │
                                             │ →←: Select Screen
                                             │ ↑↓: Select Item
                                             │ Enter: Select
                                             │ +/- : Change Opt.
                                             │ F1: General Help
                                             │ F2: Previous Values
                                             │ F9: Optimized Defaults
                                             │ F10: Save & Reset
                                             │ ESC: Exit
                                             │
                                             │
                                             │
         Version 2.22.1287 Copyright (C) 2023 AMI
```

Select one of the PCI Express channels and press enter to configure the following settings.

LAN1,LAN2, LAN3, M.2-E, M.2-B

Control the PCI Express Root Port.

▶ **Chipset**

PCH-IO Configuration▶ **SATA Configuration**

```
                         Aptio Setup - AMI
              Chipset

   SATA Configuration                              Enable/Disable SATA Device.

   SATA Controller(s)           [Enabled]
   SATA Speed                   [Auto]

   SATA0(R0)                    Empty
     Port 0                     [Enabled]
     Hot Plug                   [Disabled]
   M.2-M(R1)                    Empty
     Port 1                     [Enabled]
     Hot Plug                   [Disabled]

                                            →←: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/- : Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F9: Optimized Defaults
                                            F10: Save & Reset
                                            ESC: Exit

              Version 2.22.1287 Copyright (C) 2023 AMI
```

SATA Controller(s)

This field is used to enable or disable the Serial ATA controller.

SATA Speed

This field is used to select SATA speed generation limit: Auto, Gen1, Gen2 or Gen3.

Ports and Hot Plug

Enable or disable the Serial ATA port and its hot plug function.

▶ **Chipset**

PCH-IO Configuration▶ **HD Audio Configuration**

```
                         Aptio Setup - AMI
              Chipset

   HD Audio Subsystem Configuration Settings        Control Detection of the
                                                    HD-Audio device.
   HD Audio                     [Enabled]           Disabled = HDA will be
                                                    unconditionally disabled
                                                    Enabled = HDA will be
                                                    unconditionally enabled.

                                            →←: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/- : Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F9: Optimized Defaults
                                            F10: Save & Reset
                                            ESC: Exit

              Version 2.22.1287 Copyright (C) 2023 AMI
```
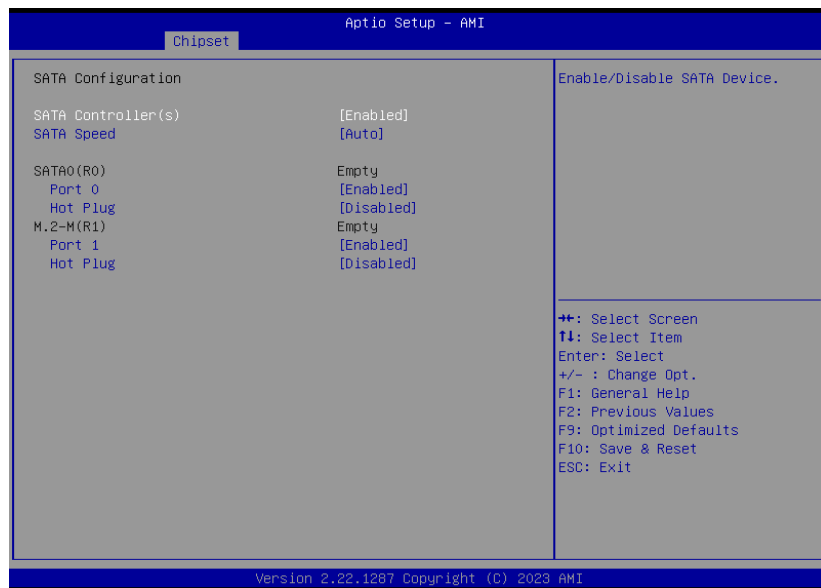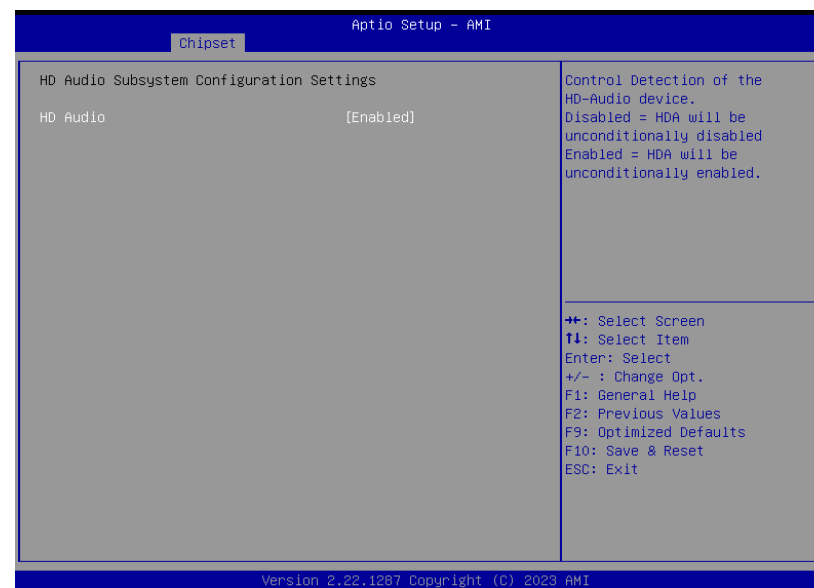
HD Audio

Control the detection of the HD Audio device.

• **Disabled** HDA will be unconditionally disabled.

• **Enabled** HDA will be unconditionally enabled.

▶ **Security**

Secure Boot

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

  Password Description                       Set Administrator Password

  Minimum length                 3
  Maximum length                 20

  Administrator Password

▶ Secure Boot

                                            ↔: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/- : Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F9: Optimized Defaults
                                            F10: Save & Reset
                                            ESC: Exit

               Version 2.22.1287 Copyright (C) 2023 AMI
```
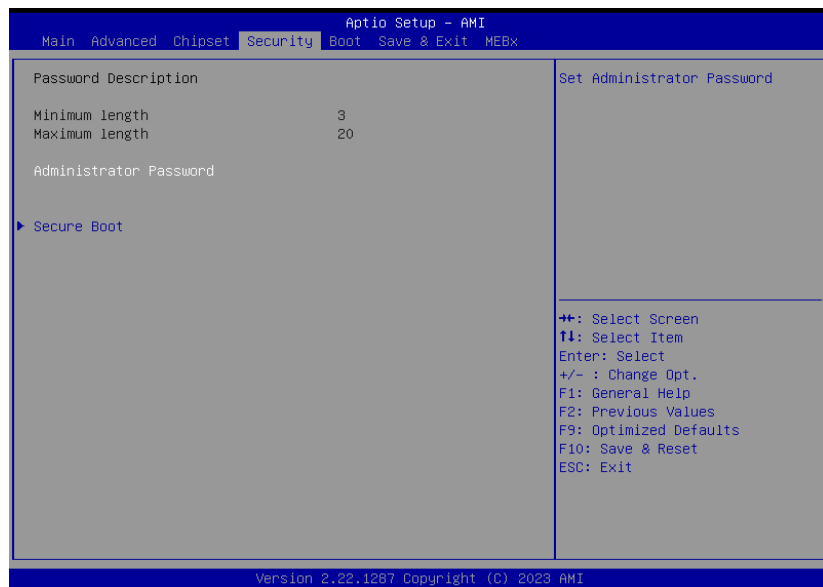
```
                          Aptio Setup - AMI
                            Security

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

▶ Key Management
                                            ↔: Select Screen
                                            ↑↓: Select Item
                                            Enter: Select
                                            +/- : Change Opt.
                                            F1: General Help
                                            F2: Previous Values
                                            F9: Optimized Defaults
                                            F10: Save & Reset
                                            ESC: Exit

               Version 2.22.1287 Copyright (C) 2023 AMI
```

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.

User Password

Set the user password. To clear the password, input nothing and press enter when a new password is asked. User Password will be required when powering up the system.

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.
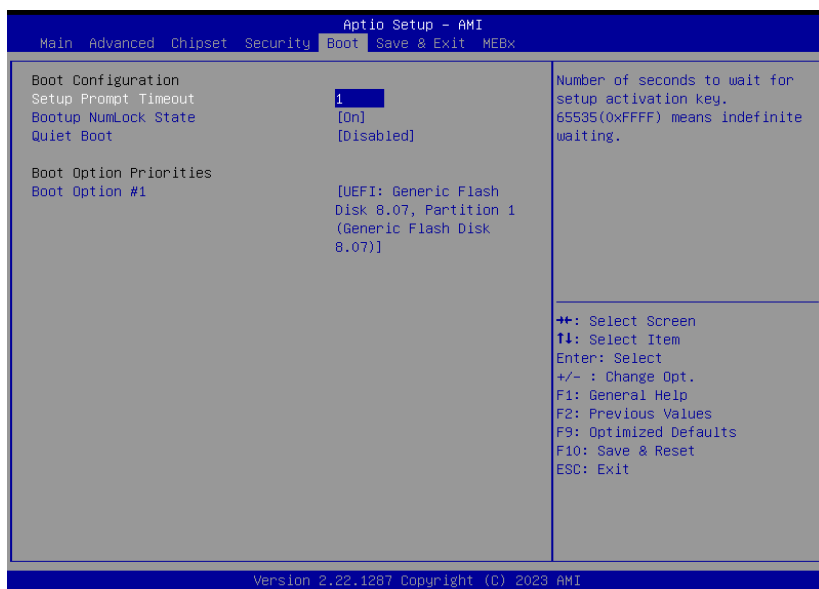
Reset To Setup Mode

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.

Key Management

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

▶ **Boot**

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

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

  Boot Option Priorities
  Boot Option #1                [UEFI: Generic Flash
                                Disk 8.07, Partition 1
                                (Generic Flash Disk
                                8.07)]

                                                        →←: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/- : Change Opt.
                                                        F1: General Help
                                                        F2: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset
                                                        ESC: Exit

                    Version 2.22.1287 Copyright (C) 2023 AMI
```

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.
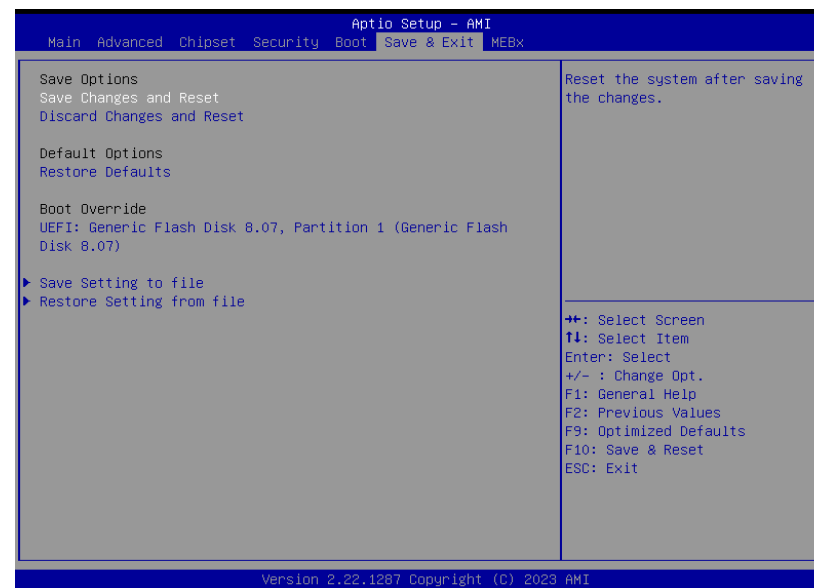
Boot Option Priorities

Rearrange the system boot order of available boot devices.

> **Note:**
> If "Boot option filter" of "CSM Configuration" is set to "UEFI and Legacy" or "UEFI only", and "Quiet Boot" is set to enabled, "BGRT Logo" will show up for configuration. Refer to the Advanced > CSM Configuration submenu for more information.

▶ **Save & Exit**

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

  Save Options                                          Reset the system after saving
  Save Changes and Reset                                the changes.
  Discard Changes and Reset

  Default Options
  Restore Defaults

  Boot Override
  UEFI: Generic Flash Disk 8.07, Partition 1 (Generic Flash
  Disk 8.07)

  ▶ Save Setting to file
  ▶ Restore Setting from file

                                                        →←: Select Screen
                                                        ↑↓: Select Item
                                                        Enter: Select
                                                        +/- : Change Opt.
                                                        F1: General Help
                                                        F2: Previous Values
                                                        F9: Optimized Defaults
                                                        F10: Save & Reset
                                                        ESC: Exit

                    Version 2.22.1287 Copyright (C) 2023 AMI
```

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 Reset

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.
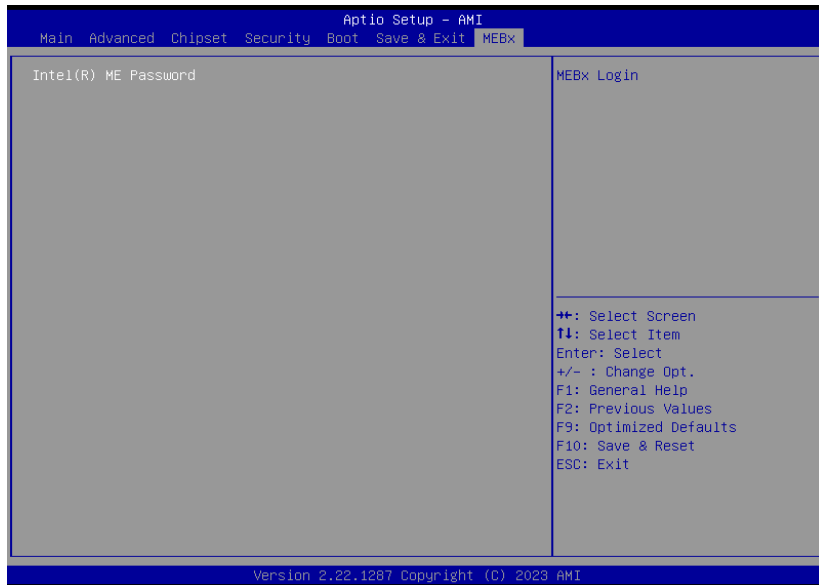
Restore Defaults

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.

Boot Override

Move the cursor to an available boot device and press Enter, and then the system will immediately boot from the selected boot device. The Boot Override function will only be effective for the current boot. The "Boot Option Priorities" configured in the Boot menu will not be changed.

• **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.

▶ **MEBx**

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

      Intel(R) ME Password                    MEBx Login




                                              ↔: Select Screen
                                              ↑↓: Select Item
                                              Enter: Select
                                              +/- : Change Opt.
                                              F1: General Help
                                              F2: Previous Values
                                              F9: Optimized Defaults
                                              F10: Save & Reset
                                              ESC: Exit


              Version 2.22.1287 Copyright (C) 2023 AMI
```

▶ **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 Intel® Management Engine 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 Intel® Management Engine 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.