MS-C936

Industrial Data Machine

User Guide

Contents

Revision

V1.0, 2026/05

Regulatory Notices

CE Conformity

This product has been tested and found to comply with the harmonized standards for Information Technology Equipment published under Directives of Official Journal of the European Union.

FCC-B Radio Frequency Interference Statement

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 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 measures listed below:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and 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/television 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.

Notice 2

Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

WEEE Statement

European Union: This symbol on the product indicates that this product cannot be discarded as municipal waste. Instead, it is your responsibility to dispose of your waste electrical and electronic equipment by handing it over to a designated collection point for recycling. For more information about where you can drop off your waste equipment for recycling, please contact your local city office, your household waste disposal service or the shop where you purchased the product.

Chemical Substances Information

In compliance with chemical substances regulations, such as the EU REACH Regulation (Regulation EC No. 1907/2006 of the European Parliament and the Council), MSI provides the information of chemical substances in products at:

https://csr.msi.com/global/index

Battery Information

Please take special precautions if this product comes with a battery.

- Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer.
- Avoid disposal of a battery into fire or a hot oven, or mechanically crushing or cutting of a battery, which can result in an explosion.
- Avoid leaving a battery in an extremely high temperature or extremely low air pressure environment that can result in an explosion or the leakage of flammable liquid or gas.
- Do not ingest battery. If the coin/button cell battery is swallowed, it can cause severe internal burns and can lead to death. Keep new and used batteries away from children.

European Union:

Batteries, battery packs, and accumulators should not be disposed of as unsorted household waste. Please use the public collection system to return, recycle, or treat them in compliance with the local regulations.

BSMI:

廢電池請回收
For better environmental protection, waste batteries should be collected separately for recycling or special disposal.

California, USA:

The button cell battery may contain perchlorate material and requires special handling when recycled or disposed of in California.
For further information please visit:
http://www.dtsc.ca.gov/hazardouswaste/perchlorate/

Environmental Policy

- The product has been designed to enable proper reuse of parts and recycling and should not be thrown away at its end of life.
- Users should contact the local authorized point of collection for recycling and disposing of their end-of-life products.
- Visit the MSI website <https://csr.msi.com/global/pevn_ewaste> and locate a nearby distributor for further recycling information.
- Please visit <https://us.msi.com/page/recycling> for information regarding the recycling of your product in the US.

Copyright and Trademarks Notice

Technical Support

If a problem arises with your product and no solution can be obtained from the user' s manual, please contact your place of purchase or local distributor. Alternatively, please visit https://www.msi.com/support/ for further guidance.

Safety Information

Please read and follow these safety instructions carefully before installing, operating or performing maintenance on the equipment.

General Safety Instructions

- Always read the safety instructions carefully.
- Keep this User’ s Manual for future reference.
- Keep this equipment in a dry, humidity-free environment.
- Ensure that all components are securely connected to prevent issues during operation.
- Do not cover the air openings to prevent overheating.
- Avoid spilling liquids into the equipment to prevent damage or electrical shock.
- Do not leave the equipment in an unconditioned environment. Storage temperatures above 60°C (140°F) may cause damage.

Electrostatic Discharge (ESD) Precautions

The components included in this package are sensitive to electrostatic discharge. Follow these guidelines to prevent ESD-related damage:

- Hold the motherboard by the edges to avoid touching sensitive components.
- Wear an ESD wrist strap. If not available, discharge static electricity by touching a metal object before handling.
- When not installed, store the motherboard in an electrostatic shielding container or place it on an anti-static pad.

Power Safety

- Always turn off the power supply and unplug the power cord from the outlet before installing or removing any component.
- Ensure the electrical outlet provides the same voltage as indicated on the PSU before connecting.
- Arrange the power cord to avoid tripping hazards or damage. Do not place objects over the power cord.

Installation Instructions

- Lay the equipment on a stable, flat surface before setting it up.
- Before turning on the system, ensure there are no loose screws or metal components on the motherboard or within the system case.
- Do not boot the computer before completing all installations. Premature booting can cause permanent damage to components and pose safety risks.

When to Contact Service Personnel

Immediately consult service personnel if any of the following situations arise:

- The power cord or plug is damaged.
- Liquid has entered the equipment.
- The equipment has been exposed to moisture.
- The equipment does not function as described in the User Guide.
- The equipment has been dropped or physically damaged.
- The equipment shows visible signs of breakage.

Specifications

Model	MS-C936
Processor	**13th Gen** Intel® **Raptor Lake-P** Platform U-Series Processor Core™ 5 processor 120U, 15W
Memory	• 2 x DDR5 SO-DIMM slots (262-pin) - Dual Channel for DDR5, Non-ECC - Up to 5200 MT/s - Up to 96 GB
Network	2 x Intel® I226-LM 2.5GbE RJ-45 LAN (Co-lay I226-V)
Audio	Realtek® ALC897 High Definition Audio codec (Co-lay ALC888S)
Graphics	Engine within processor • 2 x HDMI™ 2.0b up to 4096x2304 @60Hz • 2 x USB Type-C support DP 1.4a up to 7680 x 4320 @60Hz - Supports DP++, High Bit Rate 3 • 4 independent display modes (2 x HDMI™, 2 x DP)
Storage	• 1 x SATA 3.0 (6Gb/s) port - Hot-plug supported • 1 x M.2 M Key (2242/ 2280) slot - With PCIe Gen 4 x4 NVMe & SATA 3.0 signal - Supports M/ B + M Key SSD devices • AHCI/ RAID 0/ RAID 1 - For SATA storage + M.2 M Key storage devices
Expansion Slots	• 1 x M.2 B Key (2242/ 3042) slot - With PCIe x1, USB 3.2 Gen 2, USB 2.0 signal - Shared with Nano SIM Holder • 1 x M.2 E Key (2230) slot - With PCIe x1 & USB 2.0 signal - Supports CNVi modules • 1 x Nano SIM Holder - Shared with M.2 B key slot
Wireless Connection	• 4 x Openings reserved for antennas - Supports Wi-Fi/ BT/ 4G LTE/ 5G
Power Solution	• 12V/ 19V DC-in power connector, lockable

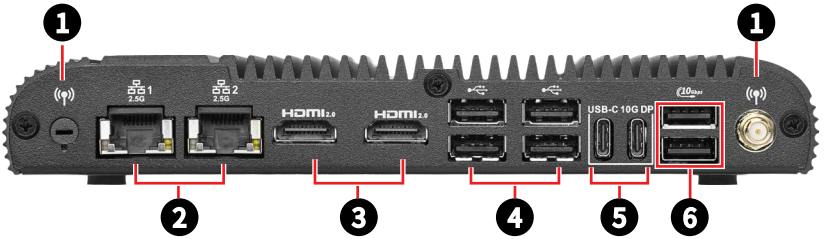
Continued on next column

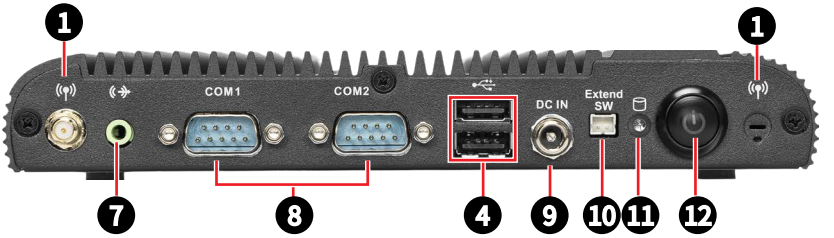
Model	MS-C936
Right Panel I/O	• 2 x Antenna connectors • 2 x RJ-45 2.5 GbE LAN ports • 2 x HDMI™ connectors • 4 x USB 2.0 Type-A connectors (5V/0.5A) • 2 x USB Type-C 10Gbps connectors (5V/3.0A) - support DisplayPorts 1.4a • 2 x Dual USB Type-A 10Gbps connectors (5V/0.9A)
Left Panel I/O	• 2 x Antenna connectors • 1 x Line-Out jack • 2 x RS232/ 422/ 485 Serial ports - 0V/ 5V/ 12V, 0.5A each port (selection by BIOS control, default: 0V) • 2 x USB 2.0 Type-A connectors (5V/0.5A) • 1 x DC power jack • 1 x Extend switch header • 1 x M.2 SSD Activity LED • 1 x Power button/ Power LED
Dimension	285mm (W) x 196mm (D) x 29mm (H)
Weight	2.22kg
Mounting	VESA mount
Accessories	• 1 x 19V, 90W Power Adapter • 1 x EU Power Cord (by BOM option) • 1 x USA Power Cord (by BOM option) • 1 x VESA Mounting Bracket • 4 x VESA Mounting Screws • 2 x Antennas for WiFi/ BT Module
OS Support	• Windows 10 IoT Enterprise 21H2 LTSC (64-Bit) • Windows 11 IoT Enterprise 24H2 LTSC (64-Bit)
Regulatory Compliance	FCC Class B/ CE/ RCM/ BSMI/ VCCI/ UKCA/ IC/ IEC 62368: CE(LVD)

Continued on next column

Model	MS-C936
Environment	• Operating Temperature - -10 ~ 50°C (w/ 2.5” SATA SSD <Ta: 85°C>, w/ M.2 NVMe SSD <Ta: 85°C>, w/ WT MEM) - Note: Thermal w/ Airflow: 0.7m/s • Storage Temperature - -20 ~ 80°C • Humidity: 10 ~ 90%, non-condensing • Vibration: IEC 60068-2-64: 2 Grms, 5 ~500 Hz, 1hr/axis (w/ SSD) • Shock: IEC 60068-2-27: 50G, half sine, 11ms (w/ SSD)

System Overview



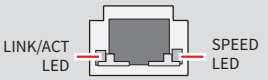


1 **Wi-Fi Antenna Connectors**

These connectors allow you to connect external antennas for wireless communication. User may find two on each side of the system.

2 **2.5 Gbps LAN Jacks**

These standard RJ-45 LAN jacks are provided for connection to the Local Area Network (LAN). They can be connected to network cable.



LED	Status	Description
Link/ Activity LED	○ Off	No link
	● Yellow	Linked
	◐ Blinking	Data activity
Speed LED	○ Off	10/100 Mbps
	● Green	1 Gbps
	● Orange	2.5 Gbps

3 **HDMI™ Connector**

Supports 4096x2304 @60Hz as specified in HDMI™ 2.0b.

4 **USB 2.0 Ports**

These connectors are provided for USB peripheral devices, providing power up to 5V/0.5A. (Speed up to 480 Mbps)

5 **USB 3.2 Gen 2 Ports (Type-C)**

These connectors are provided for USB peripheral devices, providing power up to 5V/3.0A. (Speed up to 10 Gbps)

6 **USB 3.2 Gen 2 Ports**

These connectors are provided for USB peripheral devices, providing power up to 5V/0.9A. (Speed up to 10 Gbps)

7 **Line-Out Jack**

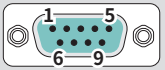
This connector is provided for headphones or speakers.

Continued on next column

8

RS232/422/485 Serial Port

The serial port is a 16550A high speed communications port that sends/ receives 16 bytes FIFOs. It supports barcode scanners, barcode printers, bill printers, credit card machine, etc.



RS232		
PIN	SIGNAL	DESCRIPTION
1	NDCD	Data Carrier Detect
2	NSIN	Signal In
3	NSOUT	Signal Out
4	NDTR	Data Terminal Ready
5	GND	Signal Ground
6	NDSR	Data Set Ready
7	NRTS	Request To Send
8	NCTS	Clear To Send
9	VCC_COM	VCC_COM

RS422		
PIN	SIGNAL	DESCRIPTION
1	422 TXD-	Transmit Data, Negative
2	422 TXD+	Transmit Data, Positive
3	422 RXD+	Receive Data, Positive
4	422 RXD-	Receive Data, Negative
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

RS485		
PIN	SIGNAL	DESCRIPTION
1	D-	Data, Negative
2	D+	Data, Positive
3	NC	No Connection
4	NC	No Connection
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

9

DC Power Jack

Power supplied through this jack supplies power to the system.

Continued on next column

10 **Extend Switch Header**

This header is provided for power switches.

11 **M.2 SSD Activity LED (Supports by SSD)**

This indicator shows the activity status of the **M.2 M key PCIe SSD**. It flashes when the system is accessing data on the SSD and remains off when no disk activity is detected.

12 **Power Button/ Power LED**

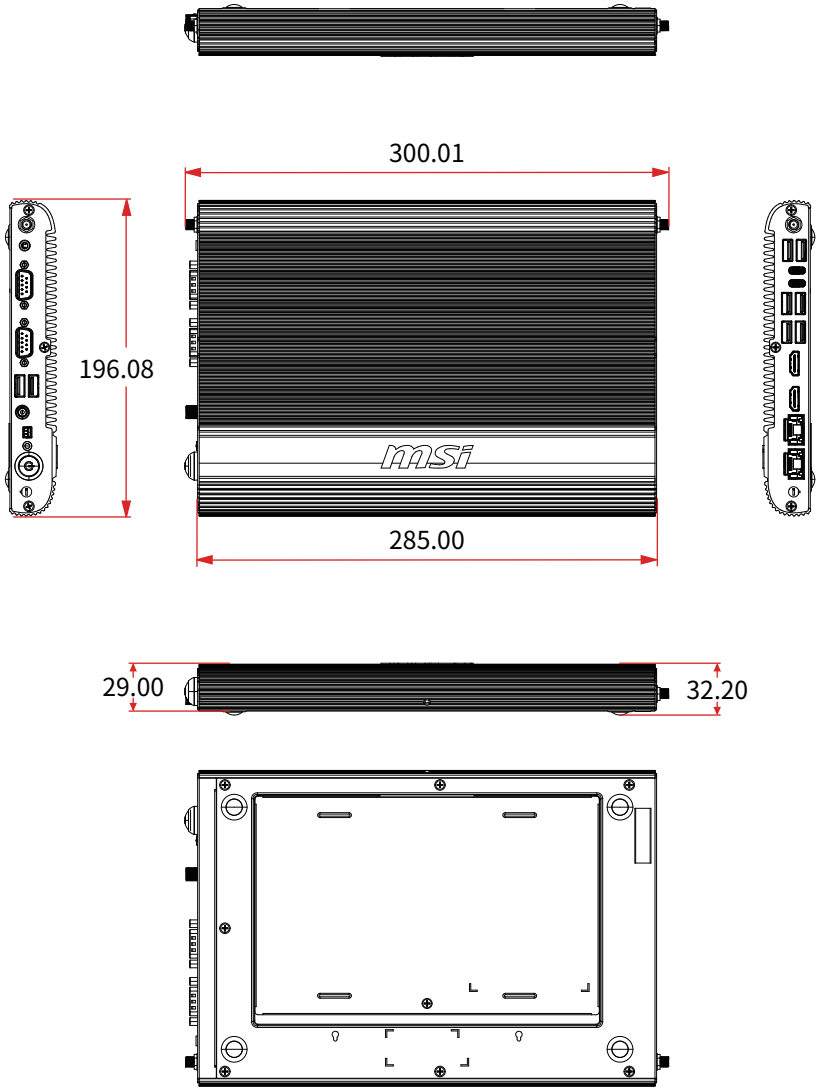
Press the button to turn the system on or off.

LED Status	Description
Off	ACPI S4/ S5/ Deep S5, Power Off
Blinking	ACPI S3
Green	ACPI S0

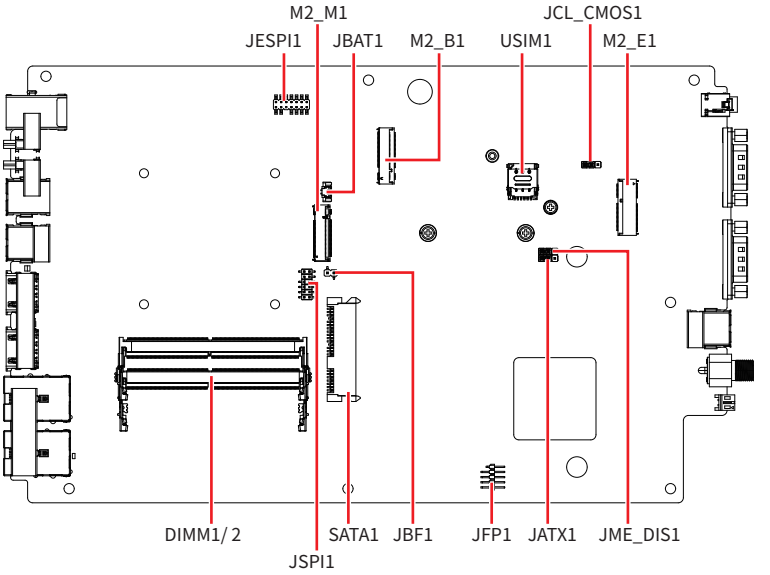
ME Overview

System Dimensions

Unit of measurement: mm



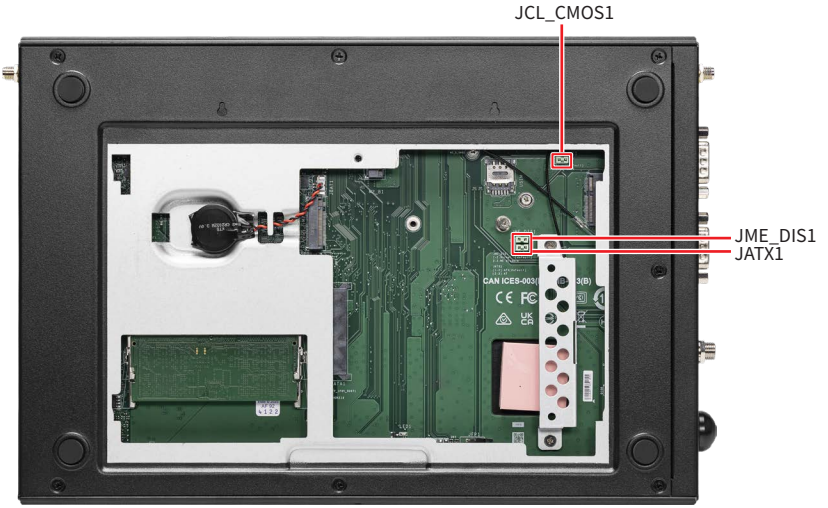
Motherboard Overview



Motherboard Jumper

Important

Avoid adjusting jumpers when the system is on; it will damage the motherboard.



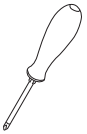
Jumper Name	Default Setting	Description
JCL_CMOS1	1	Clear CMOS Jumper
		1-2: Normal (Default) 2-3: Clear CMOS
JME_DIS1	1	ME Jumper
		1-2: Normal (Default) 2-3: ME disable
JATX1	1	ATX Mode Select Jumper
		1-2: ATX mode (Default) 2-3: AT mode

Getting Started

Important

All information is subject to change without prior notice.

Necessary Tools



Screwdriver

Pliers

Tweezers

Anti-Static Gloves

Safety Precautions

The following precautions should be observed while handling the system:

- Place the system on a flat and stable surface.
- Do not place the system in environments subject to mist, smoke, vibration, excessive dust, salty or greasy air, or other corrosive gases and fumes.
- Do not drop or jolt the system.
- Do not use another power adapter other than the one enclosed with the system.
- Disconnect the power cord before performing any installation procedures on the system.
- Do not perform any maintenance with wet hands.
- Prevent foreign substances, such as water, other liquids or chemicals, from entering the system while performing installation procedures on the system.
- Use a grounded wrist strap before handling system components such as CPU, Memory, SSD, expansion cards, etc.
- Place system components on a grounded antistatic pad or on the bed that came with the components whenever the components are separated from the system.

Important

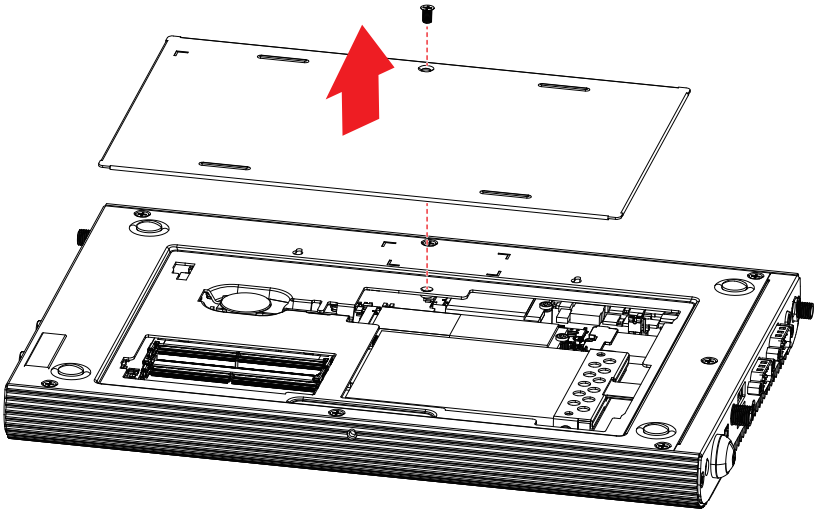
The system photos are provided for demonstration of system assembly only. The internal view of your system may vary depending on the model you purchased.

Removing System Cover

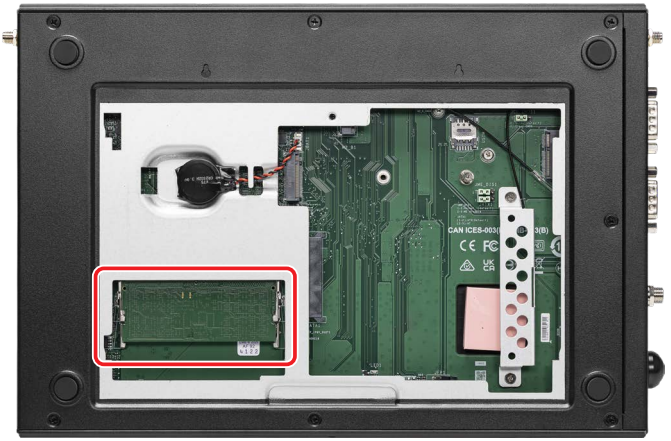
Important

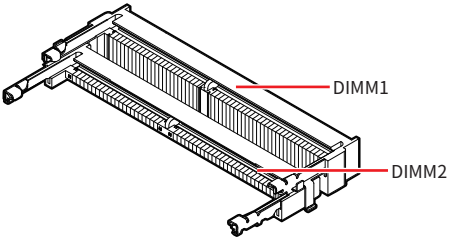
Before you remove or install any components, make sure the system is not turned on or connected to the AC power.

1. Place the system on a flat and steady surface. Locate the screw on the back side, and slightly pull aside to uncover the system.
2. Remove the cover carefully, and set the cover and screw aside for later use.



Memory Module





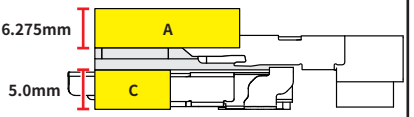
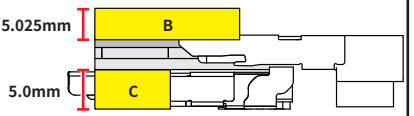
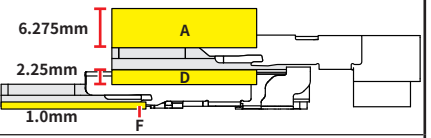
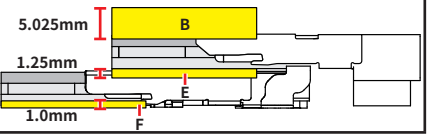
Important

- *Always insert memory module in the higher slot first.*
- *To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.*

Applying Thermal Pad for the Memory

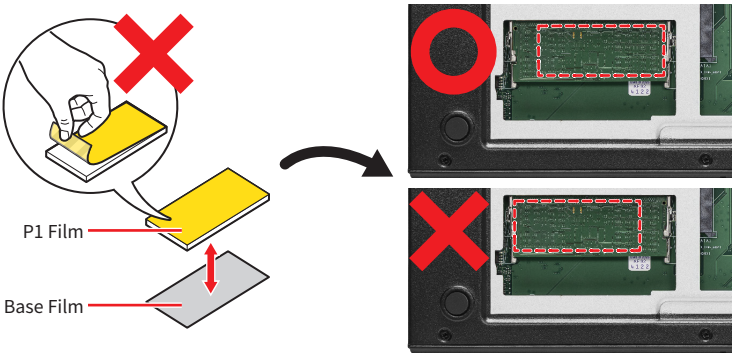
Refer to the table below for the correct placement and size of thermal pads based on the memory types and number of memory installed in your system.

Memory Thermal Pad Application Table

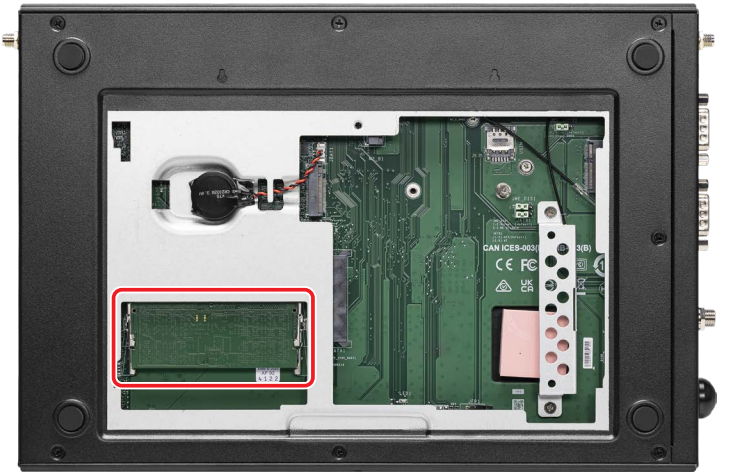
Memory Type / Q'ty	Pad Size	M.2 SSD & Thermal Pad Side View
Single-sided (chips on 1 side) / 1 memory (top)	A. 20 x 55 x **6.275mm** C. 10 x 60 x **5.0mm**	
Double-sided (chips on 2 sides) / 1 memory (top)	B. 20 x 55 x **5.025mm** C. 10 x 60 x **5.0mm**	
Single-sided (chips on 1 side) / 2 memories	A. 20 x 55 x **6.275mm** D. 20 x 60 x **2.25mm** F. 20 x 60 x **1.0mm**	
Double-sided (chips on 2 sides) / 2 memories	B. 20 x 55 x **5.025mm** E. 20 x 60 x **1.25mm** F. 20 x 60 x **1.0mm**	

Important

- *The thermal pad between the case and the memory (A and B) has no protective tape. Attach the pad with the non-adhesive side (P1 film) facing the case and the adhesive side facing the memory.*
- *To prevent interference with system cover closure, apply the thermal pad A and B towards the center of the system.*



Installing Memory Module



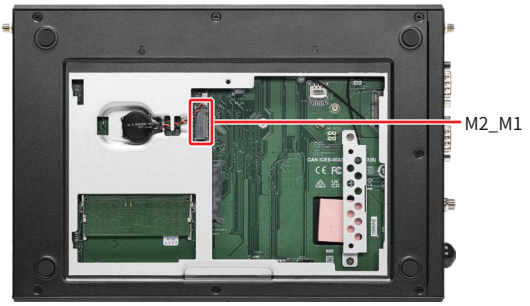
1. Align the notch on the memory module with the key on the slot and insert the memory module into the slot at a 45-degree angle.
2. Push the memory module gently downwards until the slot clips click and lock the memory module in place.
3. Install more DIMMs if necessary.

- *To uninstall the DIMM, flip the slot levers outwards and the DIMM will be released instantly.*

Important

You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.

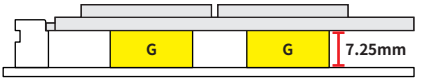
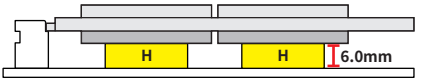
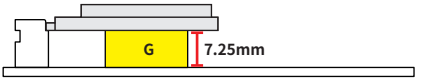
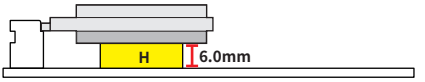
M.2 SSD (M-Key)



Applying Thermal Pad for the M.2 SSD

Refer to the table below for the correct placement and size of thermal pads based on the M.2 SSD types installed in your system.

M.2 SSD Thermal Pad Application Table

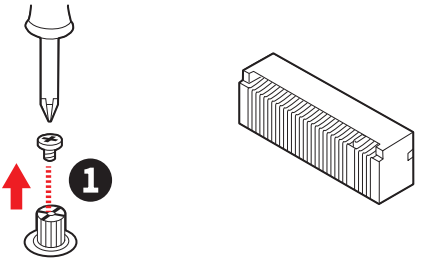
M.2 SSD Type	Pad Q'ty / Size	M.2 SSD & Thermal Pad Side View
2280, Single-sided (chips on 1 side)	Pad x1 or x2 G. 20 x 25 x **7.25mm**	
2280, Double-sided (chips on 2 sides)	Pad x1 or x2 H. 20 x 25 x **6.0mm**	
2242, Single-sided (chips on 1 side)	Pad x1 G. 20 x 25 x **7.25mm**	
2242, Double-sided (chips on 2 sides)	Pad x1 H. 20 x 25 x **6.0mm**	

Installing M.2 SSD (M-Key)

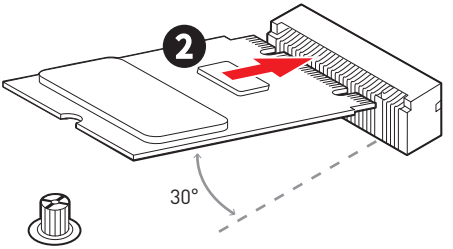
Video Demonstration

Watch the video to learn how to Install M.2 SSD.

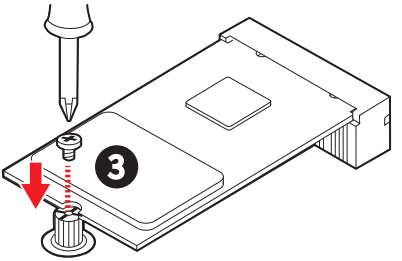
1. Loosen the M.2 screw from the motherboard.



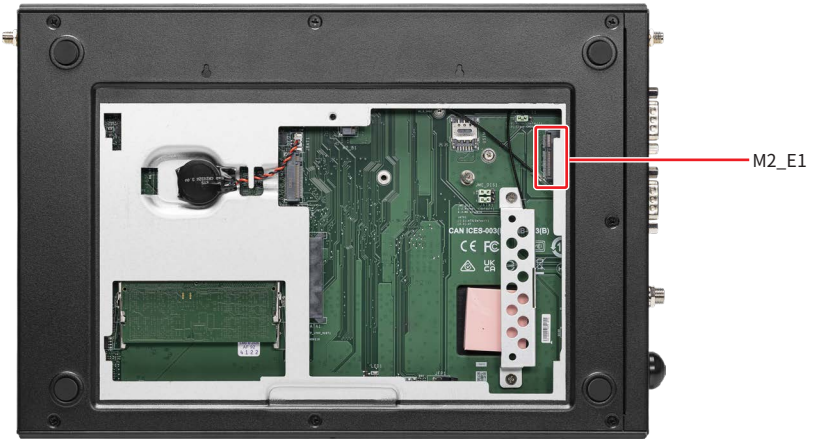
2. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.



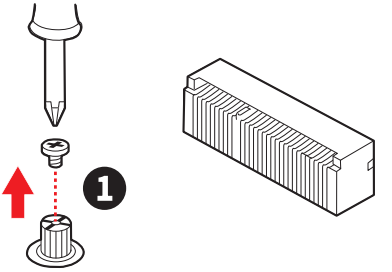
3. Secure the M.2 SSD in place with the supplied M.2 screw.



Installing M.2 Wi-Fi Card (E-Key)



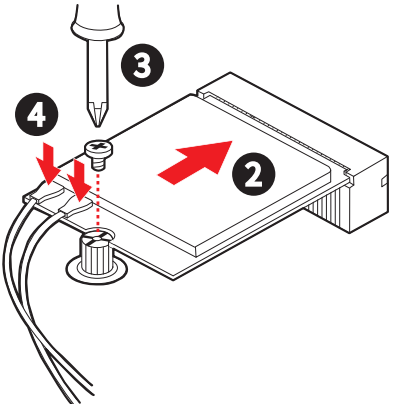
1. Loosen the M.2 screw from the motherboard.



2. Insert your M.2 Wi-Fi card into the M.2 slot at a 30-degree angle.

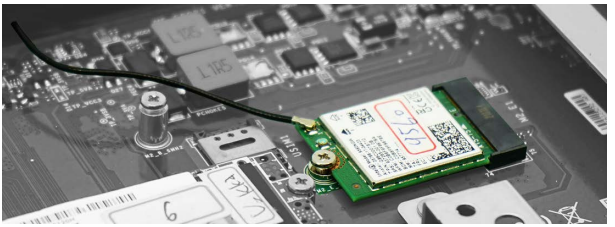
3. Secure the M.2 Wi-Fi card in place with the supplied M.2 screw.

4. Locate the antenna cables and gently connect them to the Wi-Fi card.

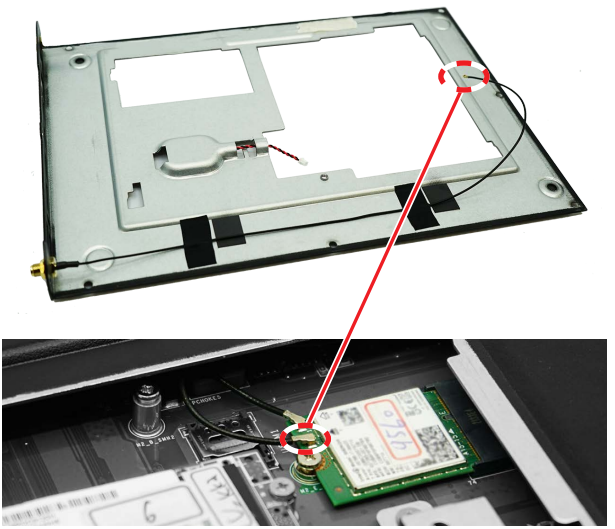


Cable Connection for Wi-Fi Card (M.2 E-Key Slot)

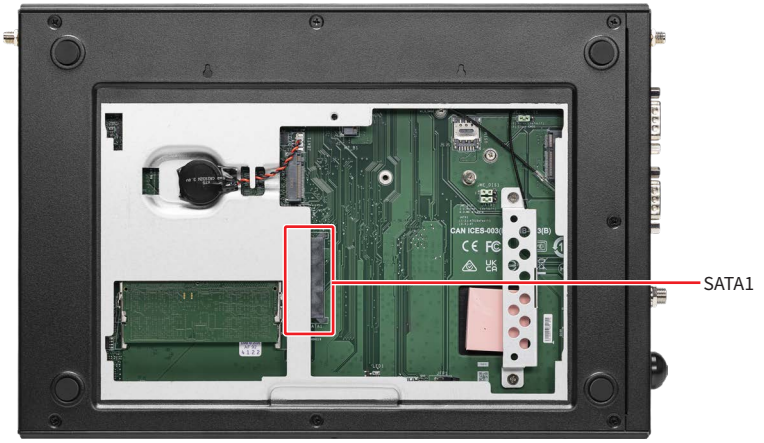
1. Find the antenna cable, gently push down to connect it.



2. Use acetate cloth electrical tape to secure another antenna cable on the back side of the case, then connect it to the Wi-Fi card.



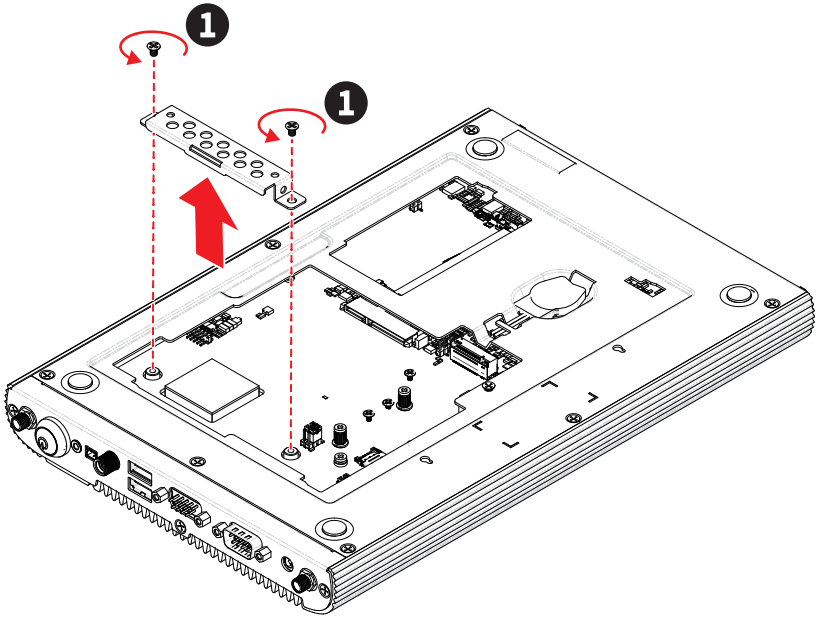
Installing 2.5" SSD (7mm)



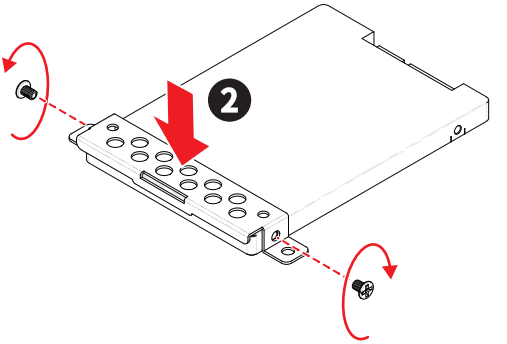
Important

Before assembly, please make sure the SSD is compatible.

1. Remove the bracket by unlocking 2 screws, and keep the screws for later use.

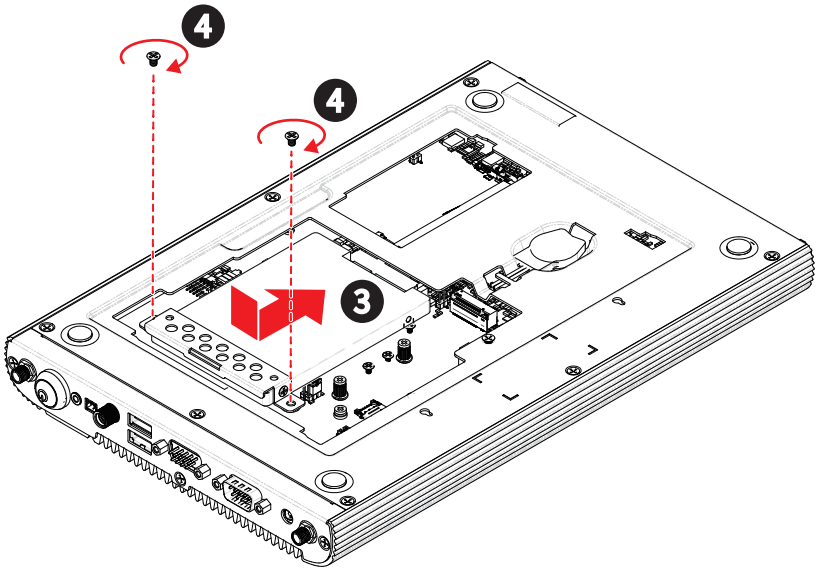


2. Put the SSD into the bracket with screw holes aligned. Tighten the screws to fix the SSD to the bracket.



3. Align the SATA data & power connectors and connect the SSD to the system.

4. Fasten the bracket to the system with 2 screws.

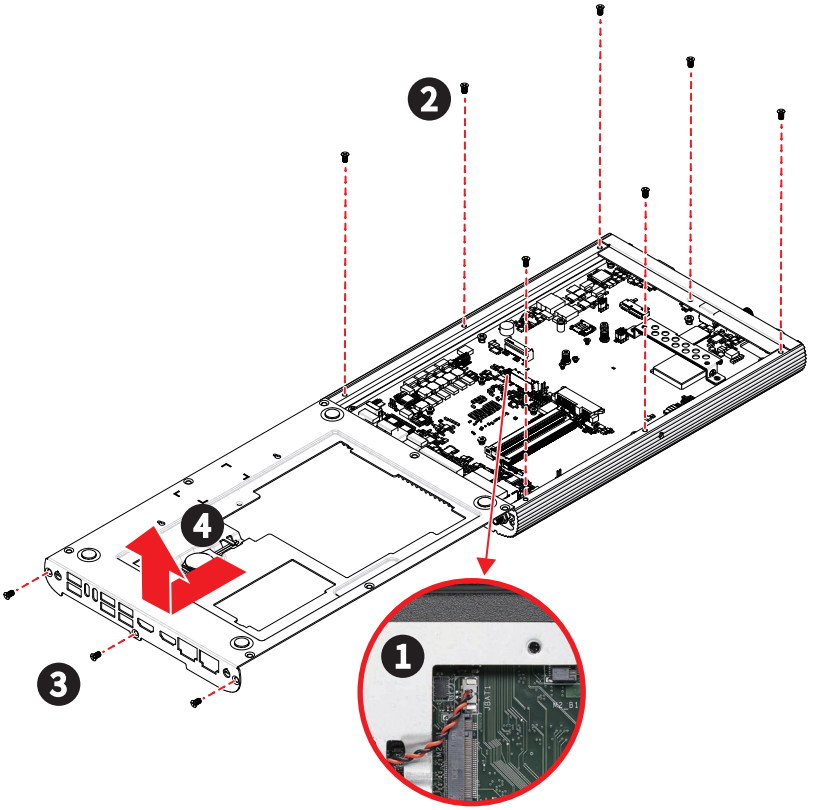


- *Please make sure the SSD is properly and completely fixed.*
- *Follow the above procedures in reverse order to replace the SSD if needed.*

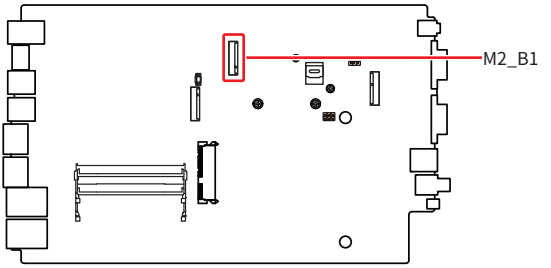
Removing System Case

1. Unplug the battery connector.
2. Remove the screws on the back side.
3. Remove the screws on the right side.
4. Carefully pull to remove the case, and set the case and screws aside for later use.

- *Follow the above procedures in reverse order to install the cover.*



Installing M.2 Expansion Card (B-Key)

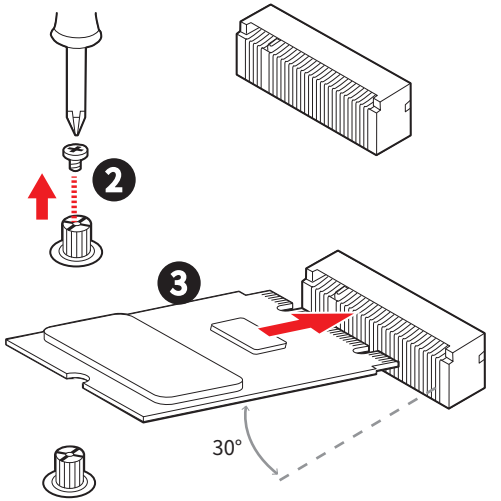


1. Open the case.

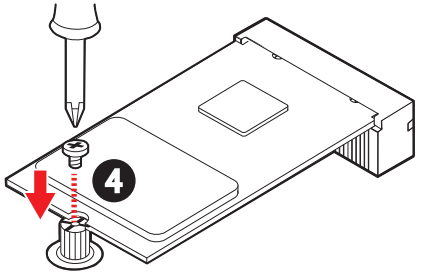
- *Please refer to the previous page for instructions on removing the system case.*

2. Loosen the M.2 screw from the motherboard.

3. Insert your M.2 SSD into the M.2 slot at a 30-degree angle.



4. Secure the M.2 SSD in place with the supplied M.2 screw.



Important

When adding or removing expansion cards, make sure that you unplug the power supply first. Meanwhile, read the documentation for the expansion card to configure any necessary hardware or software settings for the expansion card, such as jumpers, switches or BIOS configuration.

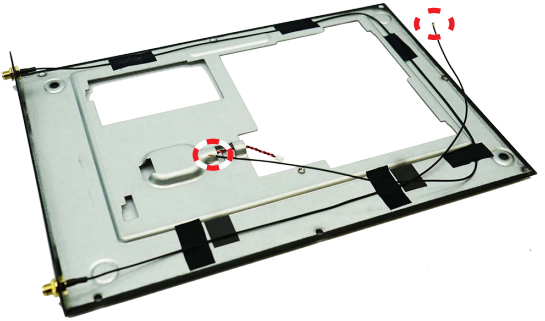
Cable Connection for 5G Card (M.2 B-Key Slot)

1. Open the case.

- *For instructions, please refer to **Removing System Case** chapter.*

2. Find two antenna cables, gently push down to connect it.

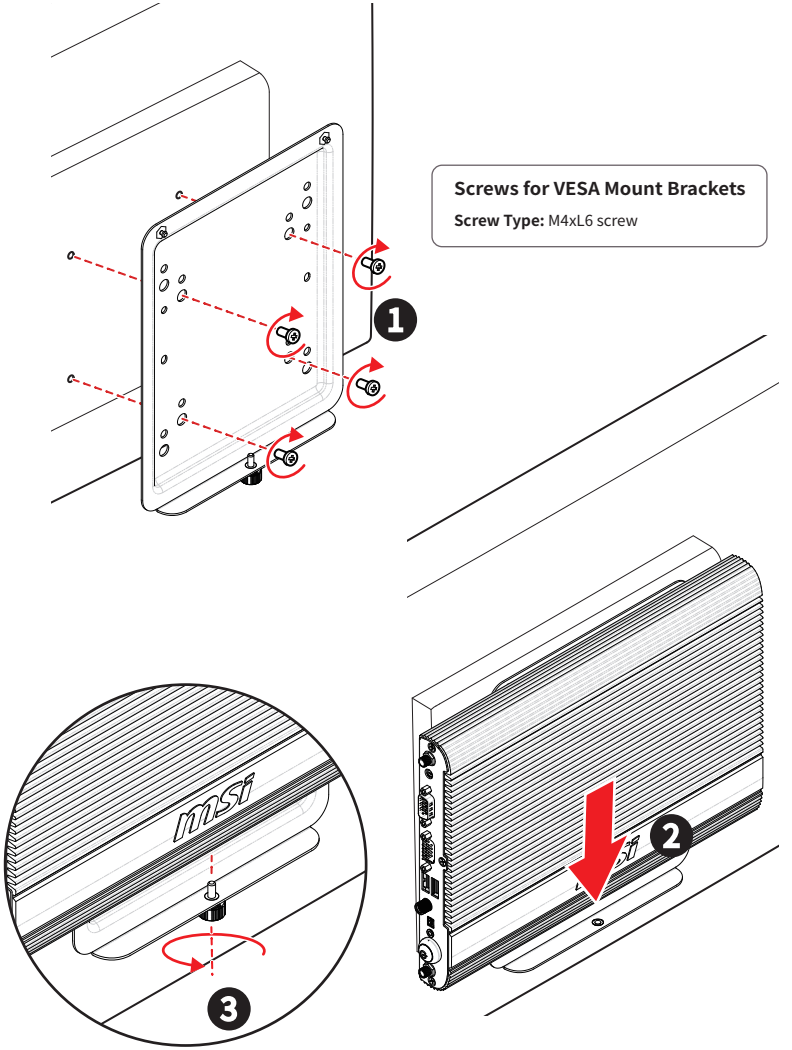
3. Use acetate cloth electrical tape to secure the other two antenna cables on the back side of the case, then connect them to the 5G card.



VESA Mount Plate

Installing VESA Mount Plate

1. Fasten the **VESA mount plate** to the monitor with the supplied screws.
2. Mount the system onto the VESA mount plate.
3. Tighten the **thumbscrew** at the bottom of the VESA mount plate to secure the system.



BIOS Setup

This chapter provides information on the BIOS Setup program and allows users to configure the system for optimal use.

Users may need to run the Setup program when:

- An error message appears on the screen at system startup and requests users to run SETUP.
- Users want to change the default settings for customized features.

Important

- *Please note that BIOS update assumes technician-level experience.*
- *As the system BIOS is under continuous update for better system performance, the illustrations in this chapter should be held for reference only.*

Entering Setup

Power on the computer and the system will start POST (Power On Self Test) process. When the message below appears on the screen, press **<DEL>** or **<F2>** key to enter Setup, **<F11>** to Boot Order Menu.

Press <DEL> or <F2> to enter SETUP

If the message disappears before you respond and you still wish to enter Setup, restart the system by turning it **OFF** and **On** or pressing the **RESET** button. You may also restart the system by simultaneously pressing **<Ctrl>, <Alt>, and <Delete>** keys.

Important

The items under each BIOS category described in this chapter are under continuous update for better system performance. Therefore, the description may be slightly different from the latest BIOS and should be held for reference only.

Control Keys

← →	Select Screen
↑ ↓	Select Item
Enter	Select
+ -	Change Value
Esc	Exit
F1	General Help
F7	Previous Values
F8	Search setup items
F9	Optimized Defaults
F10	Save & Reset*
F12	Screenshot capture
<K>	Scroll help area upwards
<M>	Scroll help area downwards

* When you press **<F10>**, a confirmation window appears and it provides the modification information. Select between **Yes** or **No** to confirm your choice.

Getting Help

Upon entering setup, you will see the Main Menu.

Main Menu

The main menu lists the setup functions you can make changes to. You can use the **arrow keys (↑ ↓)** to select the item. The on-line description of the highlighted setup function is displayed at the bottom of the screen.

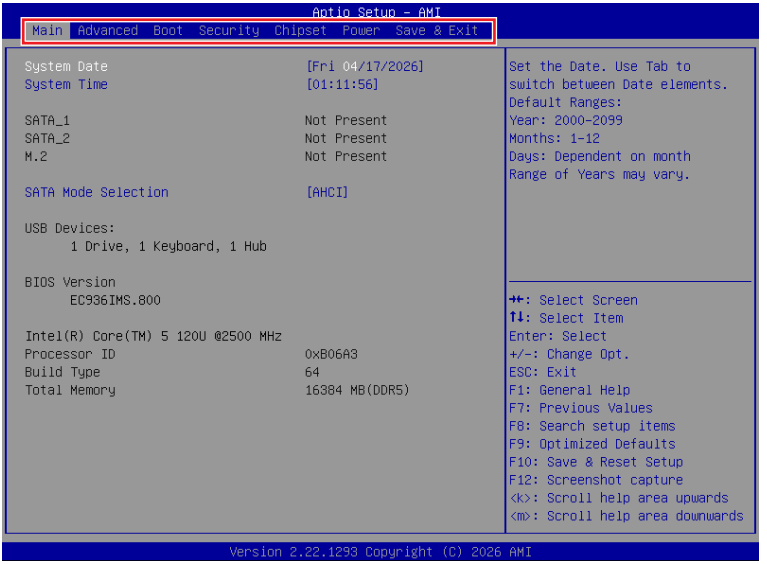
Sub-Menu

If you find a right pointer symbol appears to the left of certain fields that means a sub-menu can be launched from this field. A sub-menu contains additional options for a field parameter. You can use **arrow keys (↑ ↓)** to highlight the field and press **<Enter>** to call up the sub-menu. Then you can use the **control keys** to enter values and move from field to field within a sub-menu. If you want to return to the main menu, just press the **<Esc>.**

General Help <F1>

The BIOS setup program provides a General Help screen. You can call up this screen from any menu by simply pressing **<F1>**. The Help screen lists the appropriate keys to use and the possible selections for the highlighted item. Press **<Esc>** to exit the Help screen.

The Menu Bar



- **Main**

  Use this menu for basic system configurations, such as time, date, etc.

- **Advanced**

  Use this menu to set up the items of special enhanced features.

- **Boot**

  Use this menu to specify the priority of boot devices.

- **Security**

  Use this menu to set supervisor and user passwords.

- **Chipset**

  This menu controls the advanced features of the on-board chipsets.

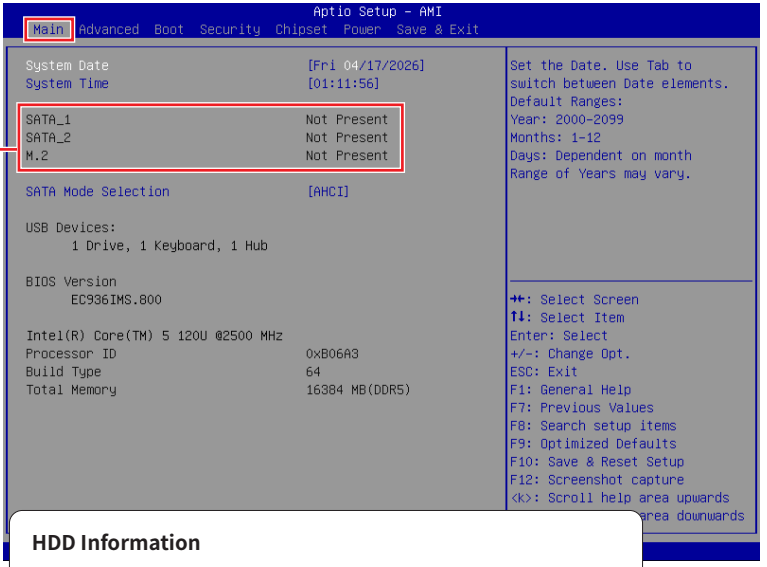
- **Power**

  Use this menu to specify your settings for power management.

- **Save & Exit**

  This menu allows you to load the BIOS default values or factory default settings into the BIOS and exit the BIOS setup utility with or without changes.

Main



HDD Information

- **RAID (VMD) Disabled:** Display HDD information as plugging in status.
- **RAID (VMD) Enabled:** Display "Not Present" only.

*__SATA_2__ is for M.2 M key (SATA signal)

▸ System Date

This setting allows you to set the system date. Use <Tab> key to switch between Date elements.

Format: <Day> <Month> <Date> <Year>.

▸ System Time

This setting allows you to set the system time. Use <Tab> key to switch between Time elements.

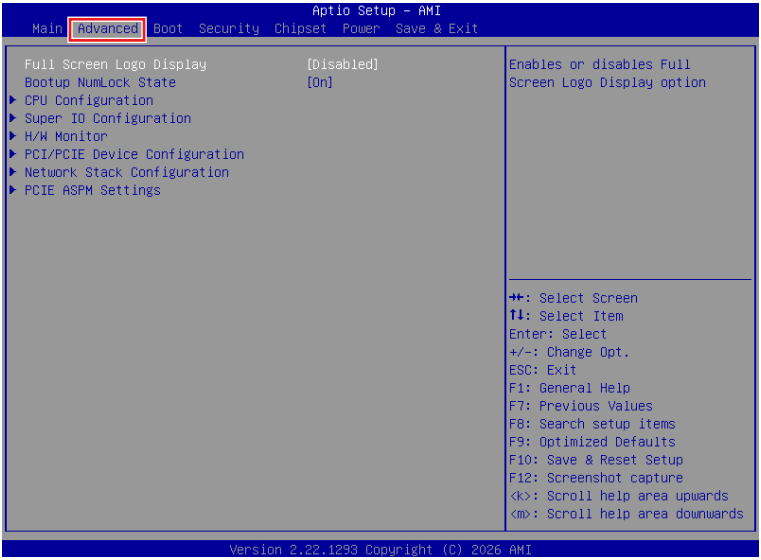
Format: <Hour> <Minute> <Second>.

▸ SATA Mode Selection

This setting specifies SATA controller mode.

[AHCI]	AHCI (Advanced Host Controller Interface), is a technical standard for an interface that allows the software to communicate with Serial ATA (SATA) devices. It offers advanced SATA features such as Native Command Queuing (NCQ) and hot-plugging.
[RAID]	RAID (Redundant Array of Independent Disks) is a virtual disk storage technology that combines multiple physical disks into one unit for data redundancy, performance improvement, or both.

Advanced



▸ Full Screen Logo Display

This BIOS feature determines if the BIOS should hide the normal POST messages with the motherboard or system manufacturer' s full-screen logo.

[Enabled] BIOS will display the full-screen logo during the boot-up sequence, hiding normal POST messages.

[Disabled] BIOS will display the normal POST messages, instead of the full-screen logo.

Please note that enabling this BIOS feature often adds 2-3 seconds to the booting sequence. This delay ensures that the logo is displayed for a sufficient amount of time. Therefore, **it is recommended to disable this BIOS feature for faster boot-up.**

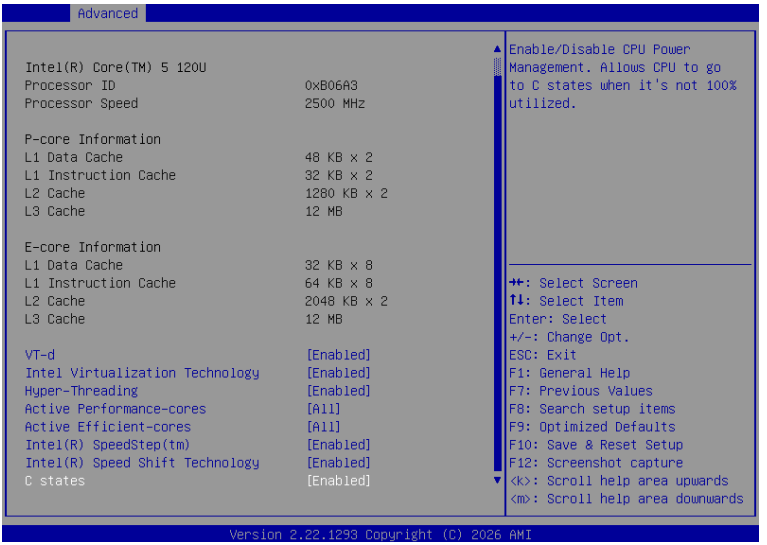
▸ Bootup NumLock State

This setting is to set the state of the Num Lock key on the keyboard when the system is powered on.

[On] Turn on the Num Lock key when the system is powered on.

[Off] Allow users to use the arrow keys on the numeric keypad.

▸ CPU Configuration



Important

The following items are displayed based on the supported CPU.

- **VT-d**

  Enables or disables Intel® VT-D (Intel® Virtualization for Directed I/O) technology.

- **Intel Virtualization Technology (VT-x)**

  Enables or disables Intel Virtualization technology.

  [Enabled] Enables Intel Virtualization technology and allows a platform to run multiple operating systems in independent partitions. The system can function as multiple systems virtually.

  [Disabled] Disables this function.

- **Hyper-Threading (HT Function)**

  Enables or disables Intel Hyper-Threading technology.
  The processor uses Hyper-Threading technology to improve utilization of the CPU resources and potentially increasing overall performance by allowing it to handle multiple threads simultaneously. If you disable the function, it will restricts the CPU to operate as a single-threaded processor, with only one logical core per physical core. Please disable this item if your operating system does not support HT Function or unreliability and instability may occur.

- **Active Performance-cores**

  Select the number of active Performance-cores (P-cores).

▸ **Active Efficient-cores**

Select the number of active Efficient-cores (E-cores).

▸ **Intel(R) SpeedStep(tm)**

Enhanced Intel SpeedStep® Technology enables the OS to control and activate performance states (P-States) of the processor.

[Enabled] When enabled, Intel SpeedStep® technology is activated. This technology allows the processor to manage its power consumption via performance state (P-State) transitions.

[Disabled] Disables this function

▸ **Intel(R) Speed Shift Technology**

Intel® Speed Shift Technology is an energy-efficient method that allows frequency control by hardware rather than the OS.

[Enabled] When enabled, Intel® Speed Shift Technology is activated. The technology enables the management of processor power consumption via hardware performance state (P-State) transitions.

[Disabled] Disable this function.

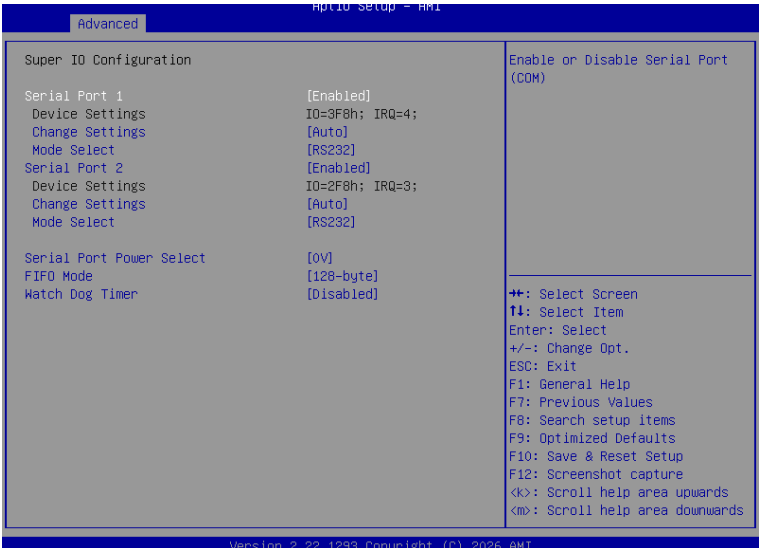
▸ **C States**

This setting controls the C-States (CPU Power states).

[Enabled] Detects the idle state of system and reduce CPU power consumption accordingly.

[Disabled] Disable this function.

▸ Super IO Configuration



▸ Serial Port 1/ 2

This setting enables or disables the specified serial port.

» **Change Settings**

This setting is used to change the address & IRQ settings of the specified serial port.

» **Mode Select**

Select an operation mode for Serial Port 1/ 2.

▸ Serial Port Power Select

Choose from [0V], [5V], or [12V] for the serial port power.

▸ FIFO Mode

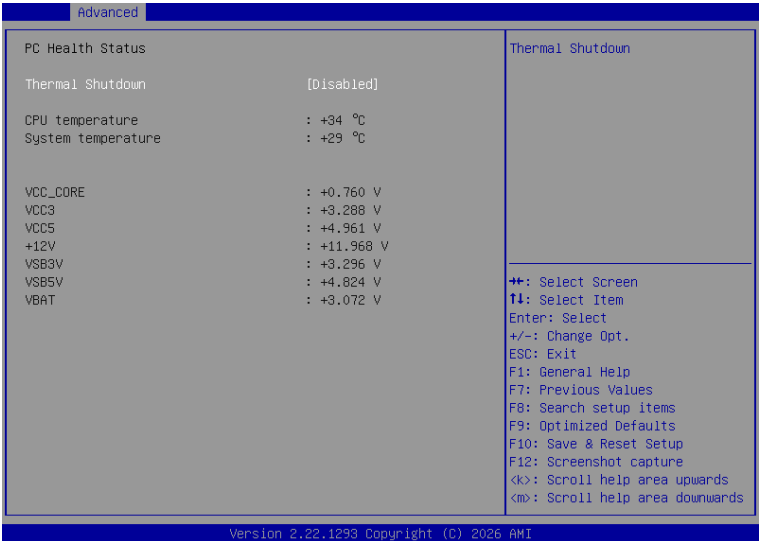
This setting controls the FIFO (First In First Out) data transfer mode.

▸ Watch Dog Timer

You can enable the system watchdog timer, a hardware timer that generates a reset when the software that it monitors does not respond as expected each time the watchdog polls it.

▸ H/W Monitor (PC Health Status)

These items display the current status of all monitored hardware devices/ components such as voltages, temperatures and all fans' speeds.



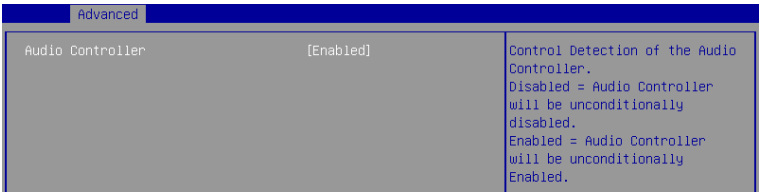
▸ Thermal Shutdown

This setting determines the behavior of the system when the CPU temperature reaches a predefined threshold.

[Enabled] Initiate an automatic shutdown of the system to protect from potential damage due to overheating.

[Disabled] Disable this function.

▸ PCI/PCIE Device Configuration

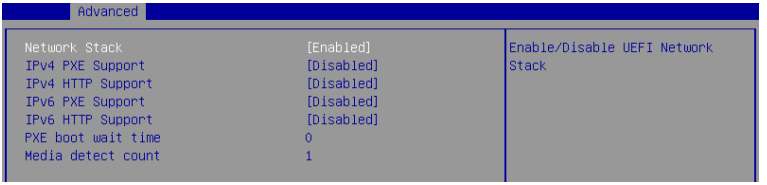


▸ Audio Controller

This setting enables or disables the detection of the onboard audio controller.

▸ Network Stack Configuration

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS.



▸ Network Stack

This menu provides Network Stack settings for users to enable or disable the network stack function, which allows the system to boot from a network device using protocols such as PXE (Preboot Execution Environment) and HTTP. The following items will display when **“Network Stack”** is enabled.

» **IPV4 PXE Support**

Enables or disables support for IPv4-based PXE booting.

» **IPV4 HTTP Support**

Enables or disables for IPv4-based HTTP booting.

» **IPV6 PXE Support**

Enables or disables for IPv6-based PXE booting.

» **IPV6 HTTP Support**

Enables or disables for IPv6-based HTTP booting.

» **PXE boot wait time**

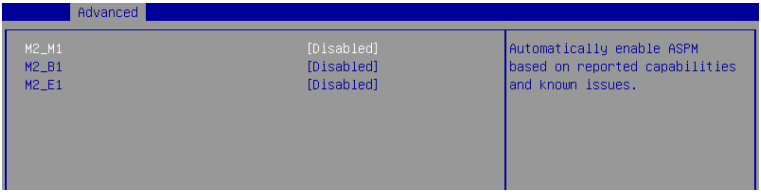
Use this option to specify the wait time to press the **<ESC>** key to abort the PXE boot. Press “+” or “-” on your keyboard to change the value. The default setting is 0.

» **Media detect count**

Use this option to specify the number of times media will be checked. Press “+” or “-” on your keyboard to change the value. The default setting is 1.

▸ PCIE ASPM settings

This menu provide settings for PCIe ASPM (Active State Power Management) level for different installed devices.

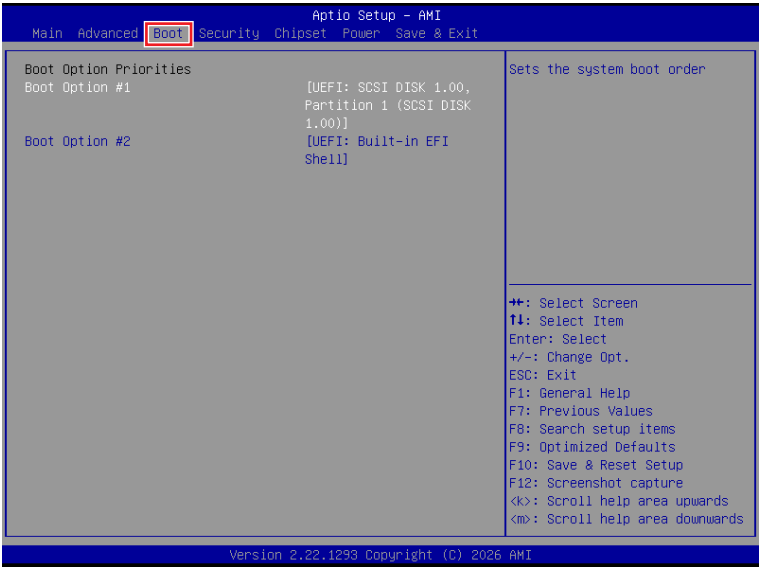


▸ M2_M1/ M2_B1/ M2_E1

Sets PCI Express ASPM (Active State Power Management) state for power saving.

[L0s]	Initiate an automatic shutdown of the system to protect from potential damage due to overheating.
[L1]	Higher latency, lower power “standby” state **(optional)**.
[L0sL1]	Activate both L0s and L1 support.
[Disabled]	Disable this function.

Boot



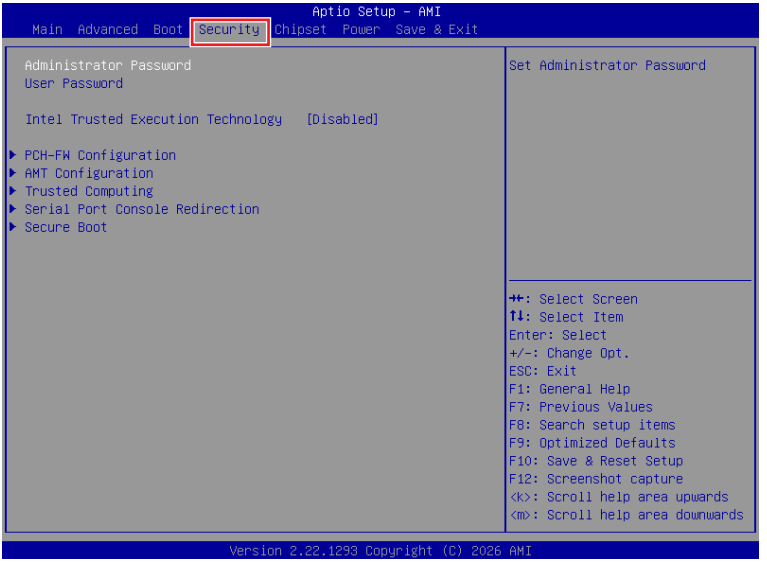
- **Boot Option #1-2**

  This setting allows users to set the sequence of boot devices where BIOS attempts to load the disk operating system.

Important

Disabled all boot option will return BIOS Setup.

Security



- **Administrator Password**

  Sets administrator password for system security. User has full rights to change the BIOS items with administrator password.

- **User Password**

  Sets User Password for system security. User has limited rights to change the BIOS items with user password. This item will be available when administrator password is set.

Important

- *When selecting the **Administrator / User Password** items, a password box will appear on the screen. Type the password then press **<Enter>.** The password typed now will replace any previous set password from CMOS memory. You will be prompted to confirm the password. You may also press **<Esc>** key to abort the selection.*
- *It is standard practice to erase passwords after clearing CMOS, but for some customized productions, passwords will be kept even after CMOS memory has been cleared.*

- **Intel Trusted Execution Technology**

  Enables or disables the Intel Trusted Execution Technology. Intel® Trusted Execution Technology (Intel® TXT) is a security feature that provides hardware-based security to protect the system and maintain the confidentiality and integrity of data stored or created on the system.

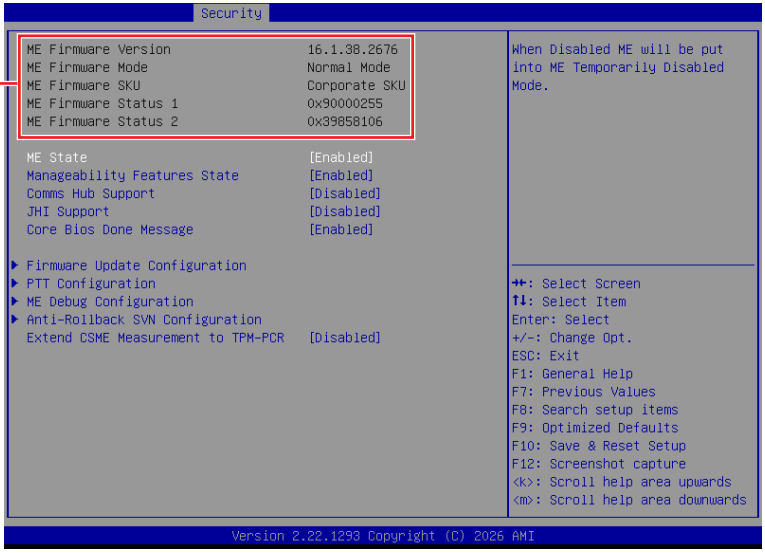
Important

The following items must be enabled before "Intel Trusted Execution Technology" can be enabled:

- *All Intel processor cores*
- *Hyper-threading*
- *Intel Virtualization Technology (VT-x)*
- *Trusted Platform Module (TPM)*
- *Secure Boot*

▸ PCH-FW Configuration

This menu allows you to configure settings related to the Platform Controller Hub (PCH) Firmware.



Firmware Information

ME Firmware Version	ME Firmware Status 1	These settings show the firmware information of the Intel ME (Management Engine).
ME Firmware Mode	ME Firmware Status 2	
ME Firmware SKU		

▸ ME State

This menu controls the Intel® Management Engine State (ME state) parameters, which provides various management and security capabilities. The following items will display when **“ME State”** is enabled.

▸ Manageability Feature State

Enables or disables Manageability Feature State. Enabling this item for remote management capabilities.

▸ Comms Hub Support

Enables or disables the communications hub support.

▸ JHI Support

Enables or disables JHI Support. JHI stands for Intel® Dynamic Application Loader Host Interface Service (Intel® DAL HIS) and is the engineering name for this feature. Enabling JHI Support in the BIOS settings allows the system to utilize this interface for communication between trusted applications and host-based applications.

▸ **Core BIOS Done Message**

Enables or disables Core BIOS Done Message sent to ME.

▸ **Extend CSME Measurement to TPM-PCR**

This setting enables or disables Intel® Converged Security and Management Engine (CSME) measurement extend to TPM-PCR.

Important

*Please note that for **"Extend CSME Measurement to TPM-PCR"** function to work, your system should have a **TPM module** installed and enabled in the BIOS, which is a separate hardware component providing secure storage and cryptographic functions.*

▸ **Firmware Update Configuration**

» **ME FW Image Re-Flash**

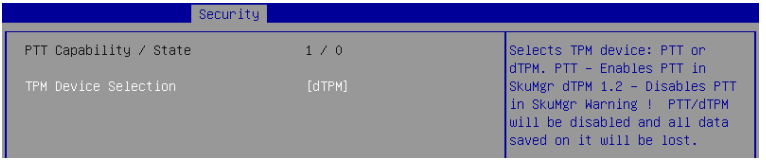
Enables or disables the ME Firmware Image Re-flashing**.**

» **Local FW Update**

Enables or disables the capability to perform a firmware update of the ME locally.

▸ **PTT Configuration**

Intel® Platform Trust Technology (PTT) is a platform functionality for credential storage and key management used by Microsoft Windows. This menu will display when **ME State** is enabled.



» **TPM Device Selection**

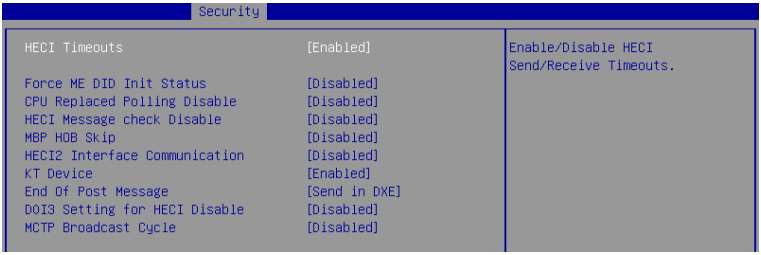
Select TPM (Trusted Platform Module) devices from PTT or dTPM (Discrete TPM).

[PTT] Enables PTT in SkuMgr.

[dTPM] Disables PTT in SkuMgr. **Warning! PTT/ dTPM will be disabled and all data saved on it will be lost.**

▸ **ME Debug Configuration**

This menu allows you to configure debug-related options for the Intel® Management Engine (ME).



» **HECI Timeouts**

This setting enables or disables the HECI (Host Embedded Controller Interface) send/ receive timeouts.

» **Force ME DID Init Status**

Forces the ME Device ID (DID) initialization status value.

» **CPU Replaced Polling Disable**

Setting this option disables the CPU replacement polling loop.

» **HECI Message Check Disable**

This setting disables message check for BIOS boot path when sending messages.

» **MBP HOB Skip**

Setting this option will skip ME' s Memory-Based Protection (MBP) HOB region.

» **HECI2 Interface Communication**

This setting Adds/ Removes HECI2 device from PCI space.

» **KT Device**

Enables or disables Key Transfer (KT) Device.

» **End of Post Message**

Choose between [disabled] and [Send in DXE] for the display of a message at the end of the Power-On Self-Test (POST) process. When set to **[disabled],** the end of POST message will not be displayed. However, when set to **[Send in DXE]**, the end of POST message will be displayed after the DXE (Driver Execution Environment) phase starts.

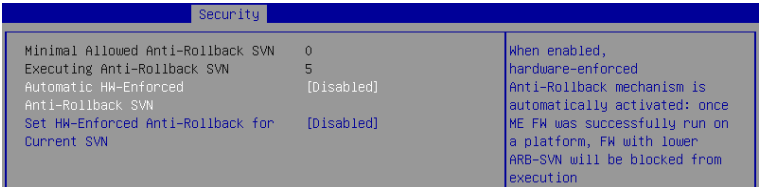
» **DOI3 Setting for HECI Disable**

Setting this option disables setting DOI3 bit for all HECI devices.

» **MCTP Broadcast Cycle**

Enables or disables Management Component Transport Protocol (MCTP) Broadcast Cycle.

▸ **Anti-Rollback SVN Configuration**



» **Automatic HW-Enforced Anti-Rollback SVN**

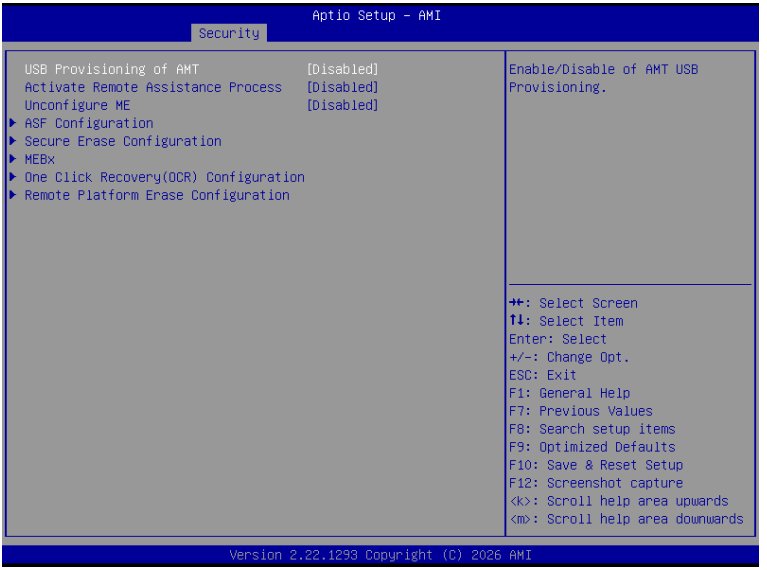
Setting this item enables will automatically activate the hardware-enforced anti-rollback protection based on the Secure Version Number (SVN). Once enabled, the hardware will enforce that only firmware updates with an SVN equal to or higher than the current SVN can be installed.

» **Set HW-Enforced Anti-Rollback for Current SVN**

Enable HW ERB mechanism for current ARB SVN value. FW with lower ARB-SVN will be blocked from execution. The value will be restored to disable after the command is sent. This item will display when **"Automatic HW-Enforced Anti-Rollback SVN"** is enabled.

▸ AMT Configuration

Intel® Active Management Technology (Intel® AMT) is hardware-based technology for remotely managing and securing PCs out-of-band (OOB).



▸ USB Provisioning of AMT

Enables or disables the ability to provision AMT using a USB device.

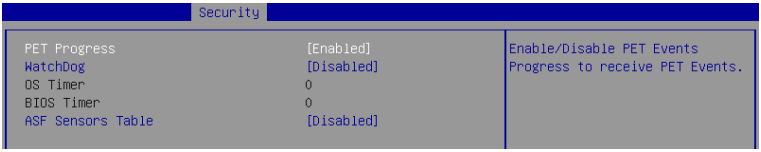
▸ Activate Remote Assistance Process

Enables or disables remote assistance sessions to be initiated on systems with AMT support.

▸ Unconfigure ME

Enables or disables the Unconfigure ME.

▸ ASF Configuration



» **PET Progress**

Enables or disable the this item to receive PET Events.

» **WatchDog**

Enables or disable the watchdog timer.

» **OS Timer**

This item displays OS Timer.

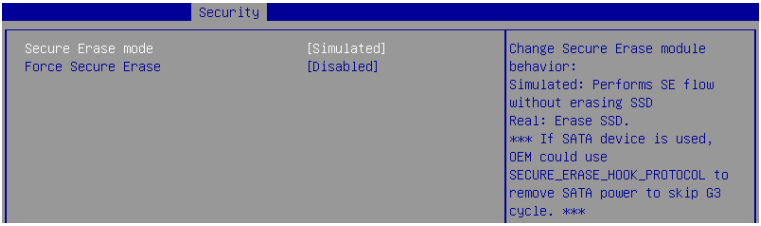
» **BIOS Timer**

This item displays BIOS Timer.

» **ASF Sensor Table**

Enables or disable the Alert Standard Format (ASF) Sensor Table.

▸ Secure Erase Configuration



» **Secure Erase Mode**

This setting change Secure Erase module behavior.

[Simulated]	Performs SE flow without erasing SSD.
[Real]	Erase SSD.

» **Force Secure Erase**

Setting this option enables or disables to force Secure Erase on next boot.

▸ **MEBx (Management Engine BIOS Extension)**

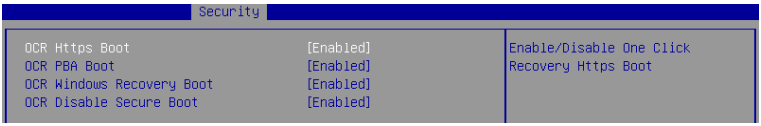
» **Intel(R) ME Password**

Set the Intel® ME Password for securing access to the ME configuration through the MEBx menu. For the first time setting the Intel® ME Password, type the default password: admin, then change to your own password.

Important

- *The **MEBx menu** can be accessed only by pressing the **<DEL> or <F2> key** during the process of booting up the system.*
- *Upon setting up Intel® ME Password for the first time, type "**admin**" as the **default password**, then enter your own.*

▸ **One Click Recovery (OCR) Configuration**



» **OCR Https Boot**

Enables or disables the use of HTTPS (Hypertext Transfer Protocol Secure) for the OCR boot process. When enabled, the OCR process will utilize HTTPS for enhanced security during the process of booting up the system.

» **OCR PBA Boot**

Enables or disables the PBA (Pre-Boot Authentication) for the OCR boot process. When enabled, users may be required to authenticate themselves before the OCR boot process begins, adding an extra layer of security.

» **OCR Windows Recovery Boot**

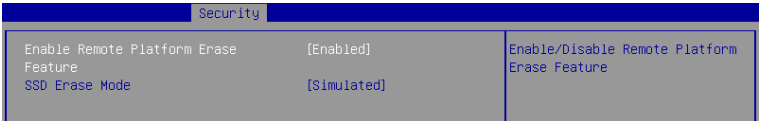
Enables or disables the Windows Recovery Boot for the OCR boot process. When enabled, the OCR boot process will prioritize Windows recovery options, allowing users to restore the system to a previous Windows state or initiate other Windows-specific recovery procedures.

» **OCR Disable Secure Boot**

Enabling this item will disable Secure Boot during the OCR process.

▸ **Remote Platform Erase Configuration**

Intel® Remote Platform Erase (Intel® RPE) Configuration provides settings for the remote erasure of the platform information or specific storage devices connected to the system.



» **Enable Remote Platform Erase Feature**

Enables or disables the ability to initiate the remote erasure process for the system or selected storage devices.

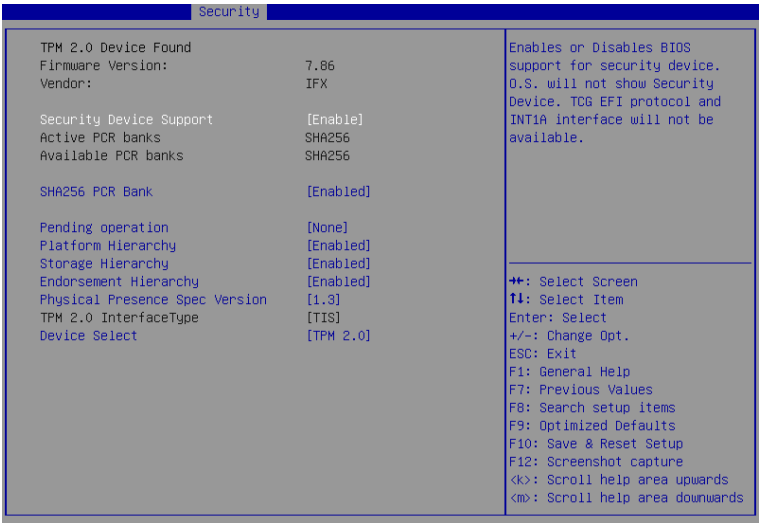
» **SSD Erase Mode**

This setting determines the erase mode to be used specifically for solid-state drives (SSDs) during the erasure process.

[Simulated] **Simulates** the erasure process **without permanently** deleting SSD data to estimate the time and resources required.

[Real] **Actual** erasure process that **permanently** deletes the SSD data to ensure that the data is no longer accessible.

▸ Trusted Computing



▸ Security Device Support

This item enables or disables BIOS support for security device. When set to [Disable], the OS will not show security device.

▸ Active PCR Banks

These settings enables or disables the SHA-1 PCR Bank and SHA256 PCR Bank.

▸ Pending Operation

When **Security Device Support** is set to [Enable], **Pending Operation** will appear. It is advised that users should routinely back up their TPM secured data.

[TPM Clear] Clear all data secured by TPM.

[None] Discard the se lection.

▸ Platform Hierarchy, Storage Hierarchy, Endorsement Hierarchy

These settings enables or disables the Platform Hierarchy, Storage Hierarchy and Endorsement Hierarchy.

▸ Physical Presence Spec Version

This settings show the Physical Presence Spec Version.

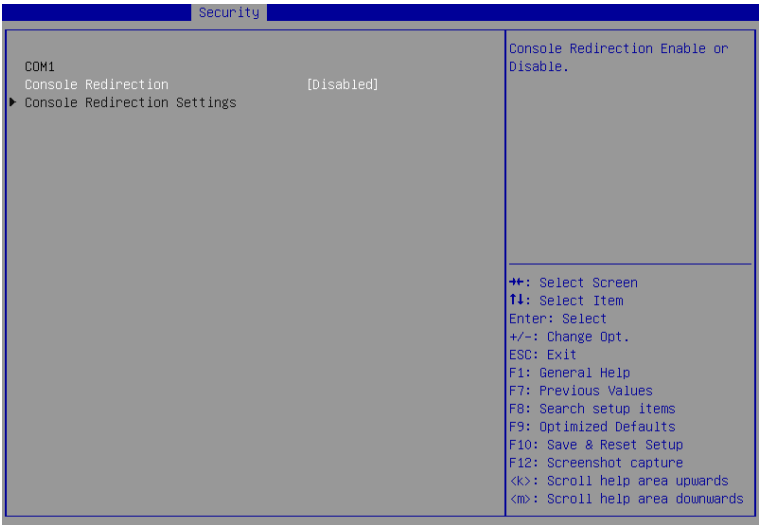
▸ TPM 2.0 Interface Type

This setting shows the TPM 2.0 Interface Type.

▸ Device Select

Select your TPM device through this setting.

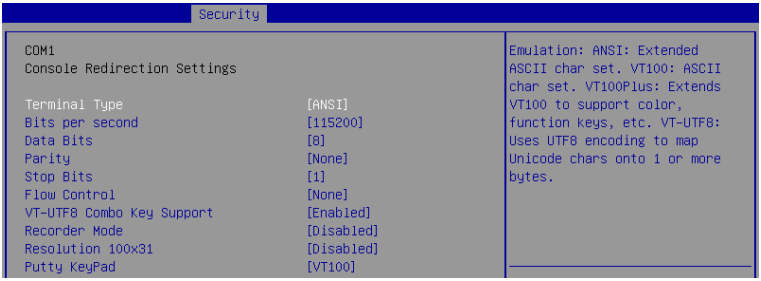
▸ Serial Port Console Redirection



▸ Console Redirection

Console Redirection operates in host systems that do not have a monitor and keyboard attached. This setting enables or disables the operation of console redirection. When set to [Enabled], BIOS redirects and sends all contents that should be displayed on the screen to the serial COM port for display on the terminal screen. Besides, all data received from the serial port is interpreted as keystrokes from a local keyboard.

▸ **Console Redirection Settings (COM1)**



» **Terminal Type**

To operate the system' s console redirection, you need a terminal supporting ANSI terminal protocol and a RS-232 null modem cable connected between the host system and terminal(s). You can select emulation for the terminal from this setting.

[ANSI] Extended ASCII character set.

[VT100] ASCII character set.

[VT100Plus] Extends VT100 to support color, function keys, etc.

[VT-UTF8] Uses UTF8 encoding to map Unicode characters onto one or more bytes.

» **Bits per second, Data Bits, Parity, Stop Bits**

These setting specifies the transfer rate (bits per second, data bits, parity, stop bits) of Console Redirection.

» **Flow Control**

Flow control is the process of managing the rate of data transmission between two nodes. It' s the process of adjusting the flow of data from one device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it.

» **VT-UTF8 Combo Key Support**

This setting enables or disables the VT-UTF8 combination key support for ANSI/ VT100 terminals.

» **Recorder Mode**

These settings enables or disables the recorder mode.

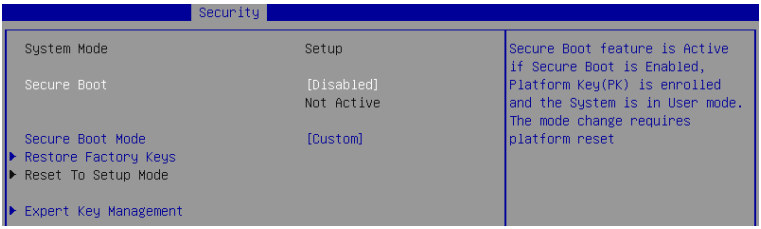
» **Resolution 100x31**

These settings enables or disables the resolution 100x31.

» **Putty KeyPad**

PuTTY is a terminal emulator for Windows. This setting controls the numeric keypad for use in PuTTY.

Secure Boot



Secure Boot

Secure Boot function can be enabled only when the **Platform Key(PK)** is enrolled and running accordingly.

Secure Boot Mode

Selects the secure boot mode. This item is to select how the secure boot keys be loaded. This item appears when "**Secure Boot**" is enabled.

[Standard]	The system will automatically load the secure keys from BIOS.
[Custom]	Allows user to configure the secure boot settings and manually load the secure keys.

Restore Factory Keys

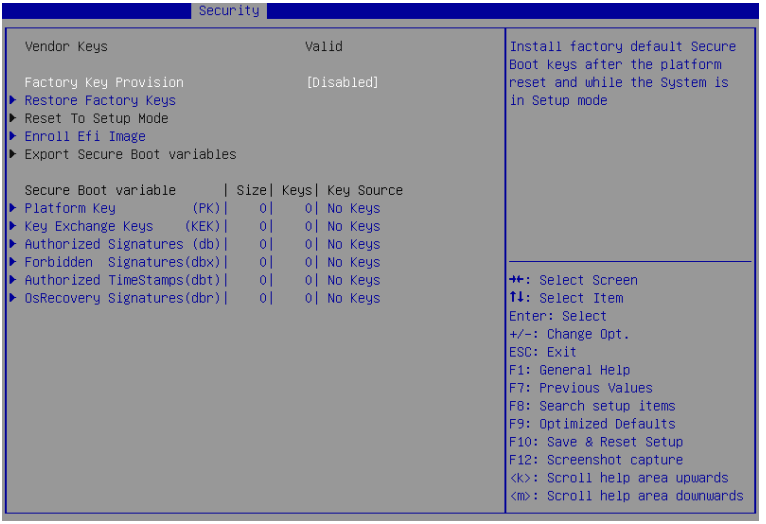
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

Reset to setup Mode

Allows you to delete all the Secure Boot keys (PK,KEK,db,dbt,dbx). The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

▸ **Expert Key Management**

Press **Enter** key to enter the sub-menu. Manage the secure boot keys. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.



» **Platform Key (PK):**

The Platform Key (PK) can protect the firmware from any un-authenticated changes. The system will verify the PK before your system enters the OS. Platform Key (PK) is used for updating KEK.

» **Set New Key**

Sets a new PK to your system.

» **Delete Key**

Deletes the PK from your system.

» **Key Exchange Keys (KEK):**

Key Exchange Key (KEK) is used for updating DB or DBX.

» **Set New Key**

Sets a new KEK to your system.

» **Append Key**

Loads an additional KEK from storage devices to your system.

» **Delete Key**

Deletes the KEK from your system.

» **Authorized Signatures (db) :**

Authorized Signatures (db) lists the signatures that can be loaded.

» **Set New Key**

Sets a new db to your system.

» **Append Key**

Loads an additional db from storage devices to your system.

» **Delete Key**

Deletes the db from your system.

» **Forbidden Signatures (dbx):**

Forbidden Signatures (dbx) lists the forbidden signatures that are not trusted and cannot be loaded.

» **Set New Key**

Sets a new dbx to your system.

» **Append Key**

Loads an additional dbx from storage devices to your system.

» **Delete Key**

Deletes the dbx from your system.

» **Authorized TimeStamps (dbt):**

Authorized TimeStamps (dbt) lists the authentication signatures with authorization time stamps.

» **Set New Key**

Sets a new DBT to your system.

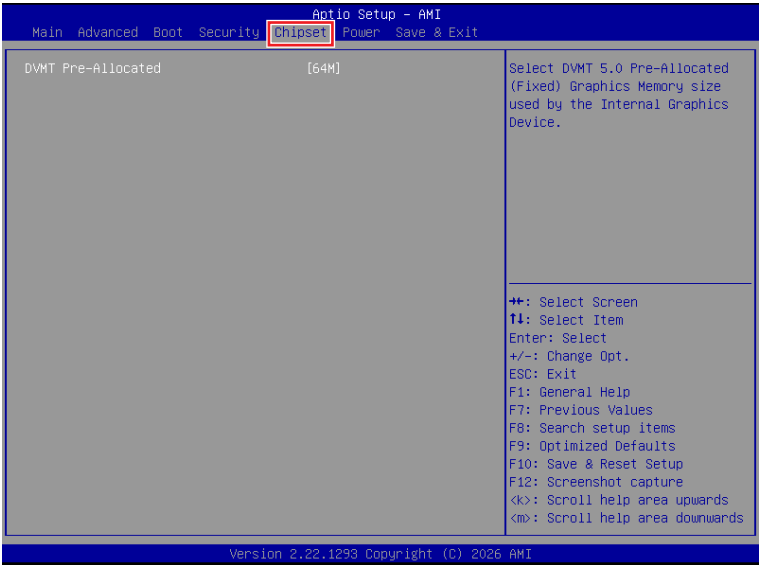
» **Append Key**

Loads an additional DBT from storage devices to your system.

» **OsRecovery Singnatures (dbr):**

Lists the available signatures for OS recovery.

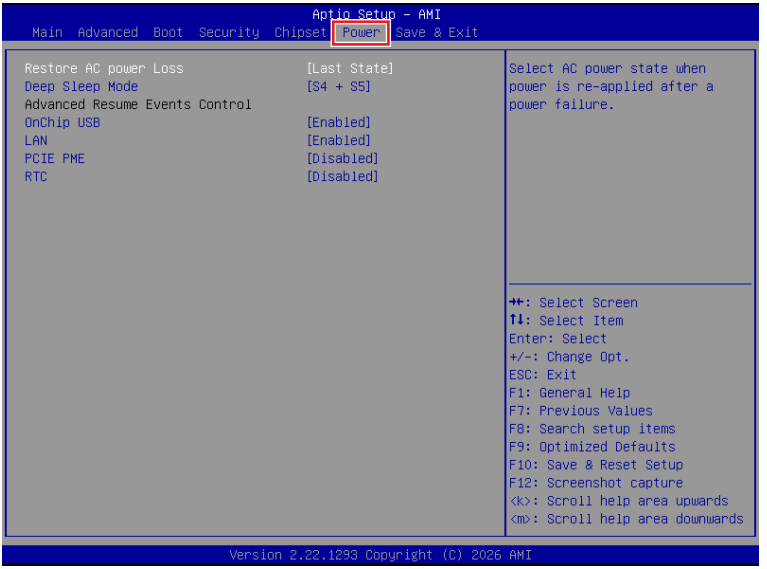
Chipset



- **DVMT Pre-Allocated**

  Select the Dynamic Video Memory Technology (DVMT) Pre-Allocated graphics memory size used by the internal graphics device.

Power



▸ Restore AC Power Loss

This setting specifies whether your system will reboot after a power failure or interrupt occurs. Available settings are:

[Power Off]	Leaves the computer in the power off state.
[Power On]	Leaves the computer in the power on state.
[Last State]	Restores the system to the previous status before power failure or interrupt occurred.

▸ Deep Sleep Mode

This setting provides two options: [S4+S5] and [Disabled]. It enables a power saving mode that reduces energy consumption when the system is off or in a low-power state. Some components remain powered to allow wake-up via the power button or RTC.

▸ OnChip USB

The item allows the activity of the OnChip USB device to wake up the system from S4/ S5 sleep state.

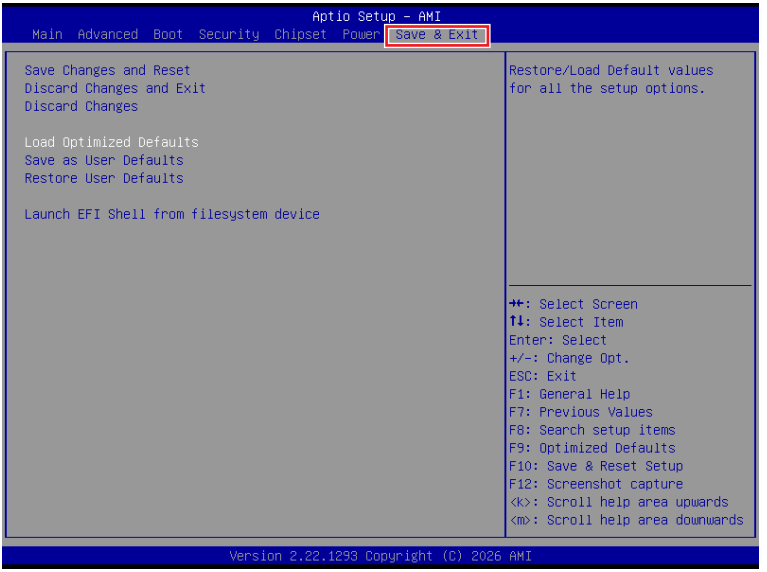
- **LAN/ PCIE PME**

  Enables or disables the system to be awakened from the power saving modes when activity or input signal of Intel LAN device and onboard PCIE PME is detected.

- **RTC**

  When [Enabled], your can set the date and time at which the RTC (real-time clock) alarm awakens the system from suspend mode.

Save & Exit



- **Save Changes and Reset**

  Save changes to CMOS and reset the system.

- **Discard Changes and Exit**

  Abandon all changes and exit the Setup Utility.

- **Discard Changes**

  Abandon all changes.

- **Load Optimized Defaults**

  Use this menu to load the default values set by the motherboard manufacturer specifically for optimal performance of the motherboard.

- **Save as User Defaults**

  Save changes as the user’ s default profile.

- **Restore User Defaults**

  Restore the user’ s default profile.

- **Launch EFI Shell from filesystem device**

  This setting helps to launch the EFI Shell application from one of the available file system devices.

WDT Programming

This chapter provides WDT (Watch Dog Timer) programming guide.

Abstract

In this section, code examples based on C programming language provided for customer interest. **Inportb, Outportb, Inportl** and **Outportl** are basic functions used for access IO ports and defined as following.

Inportb: Read a single 8-bit I/O port.

Outportb: Write a single byte to an 8-bit port.

Inportl: Reads a single 32-bit I/O port.

Outportl: Write a single long to a 32-bit port.

Watchdog Timer -- WDT

The base address (WDT_BASE) of WDT configuration registers is 0xA10.

1.1 Set WDT Time Unit

```
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting
val = val | 0x08;                       // minute mode. val = val & 0xF7 if second mode
Outportb (WDT_BASE + 0x05, val);        // Write back WDT setting
```

1.2 Set WDT Time

```
Outportb (WDT_BASE + 0x06, Time);       // Write WDT time, value 1 to 255.
```

1.3 Enable WDT

```
val = Inportb (WDT_BASE + 0x0A);        // Read current WDT_PME setting
val = val | 0x01;                       // Enable WDT OUT: WDOUT_EN (bit 0) set to 1.
Outportb (WDT_BASE + 0x0A, val);        // Write back WDT setting.
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting
val = val | 0x20;                       // Enable WDT by set WD_EN (bit 5) to 1.
Outportb (WDT_BASE + 0x05, val);        // Write back WDT setting.
```

1.4 Disable WDT

```
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting
val = val & 0xDF;                       // Disable WDT by set WD_EN (bit 5) to 0.
Outportb (WDT_BASE + 0x05, val);        // Write back WDT setting.
```

1.5 Check WDT Reset Flag

If the system has been reset by WDT function, this flag will set to 1.

```
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting.
val = val & 0x40;                       // Check WDTMOUT_STS (bit 6).
if (val)    printf ("timeout event occurred");
else        printf ("timeout event not occurred");
```

1.6 Clear WDT Reset Flag

```
val = Inportb (WDT_BASE + 0x05);        // Read current WDT setting
val = val | 0x40;                       // Set 1 to WDTMOUT_STS (bit 6);
Outportb (WDT_BASE + 0x05, val);        // Write back WDT setting
```