MS-C909

Industrial Data Machine

User Guide

Contents

Revision

V1.0, 2024/01

Safety Information

- The components included in this package are prone to damage from electrostatic discharge (ESD). Please adhere to the following instructions to ensure successful computer assembly.
- Ensure that all components are securely connected. Loose connections may cause the computer to not recognize a component or fail to start.
- Hold the motherboard by the edges to avoid touching sensitive components.
- It is recommended to wear an electrostatic discharge (ESD) wrist strap when handling the motherboard to prevent electrostatic damage. If an ESD wrist strap is not available, discharge yourself of static electricity by touching another metal object before handling the motherboard.
- Store the motherboard in an electrostatic shielding container or on an anti-static pad whenever the motherboard is not installed.
- Before turning on the computer, ensure that there are no loose screws or metal components on the motherboard or anywhere within the computer case.
- Do not boot the computer before installation is completed. This could cause permanent damage to the components as well as injury to the user.
- If you need help during any installation step, please consult a certified computer technician.
- Always turn off the power supply and unplug the power cord from the power outlet before installing or removing any computer component.
- Keep this user guide for future reference.
- Keep this motherboard away from humidity.
- Make sure that your electrical outlet provides the same voltage as is indicated on the PSU, before connecting the PSU to the electrical outlet.
- Place the power cord such a way that people can not step on it. Do not place anything over the power cord.
- All cautions and warnings on the motherboard should be noted.
- If any of the following situations arises, get the motherboard checked by service personnel:
  - Liquid has penetrated into the computer.
  - The motherboard has been exposed to moisture.
  - The motherboard does not work well or you can not get it work according to user guide.
  - The motherboard has been dropped and damaged.
  - The motherboard has obvious sign of breakage.
- Do not leave this motherboard in an environment above 60°C (140°F), it may damage the motherboard.

Regulatory Notices

CE Conformity

Hereby, Micro-Star International CO., LTD declares that this device is in compliance with the essential safety requirements and other relevant provisions set out in the European Directive.

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

Under the European Union ("EU") Directive on Waste Electrical and Electronic Equipment, Directive 2012/19/EU, products of "electrical and electronic equipment" cannot be discarded as municipal waste anymore and manufacturers of covered electronic equipment will be obligated to take back such products at the end of their useful life.

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

Green Product Features

- Reduced energy consumption during use and stand-by
- Limited use of substances harmful to the environment and health
- Easily dismantled and recycled
- Reduced use of natural resources by encouraging recycling
- Extended product lifetime through easy upgrades
- Reduced solid waste production through take-back policy

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 and locate a nearby distributor for further recycling information.
- Users may also reach us at gpcontdev@msi.com for information regarding proper disposal, take-back, recycling, and disassembly of MSI products.

Copyright and Trademarks Notice

HIGH-DEFINITION MULTIMEDIA INTERFACE

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.

Specifications

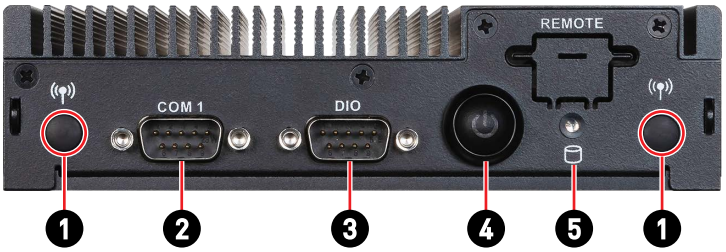
Model	MS-C909
Processor	Intel® Elkhart Lake Celeron® Processor J6412, QC, TDP 10W
Chipset	Within processor
Antenna	• 2 x Openings reserved for antennas - Supports Wi-Fi/ BT
Network	1 x Intel® I226-V 2.5GbE LAN
Graphics	• 2 x HDMI™ 1.4b up to 3840x2160 @30Hz • 2 independent display supported - HDMI™ + HDMI™
Memory	• 1 x DDR4 SO-DIMM slot (260-pin) - Single Channel DDR4, Non-ECC - Up to 3200 MT/s - Up to 16GB
Storage	• 1 x M.2 B Key slot (2242/2280) - Supports B+M Key SATA 3.0 SSD
Expansion Slots	• 1 x M.2 E Key slot (2230) - Supports PCIe x1 & USB 2.0 signal - Supports Intel® AX210 Wi-Fi 6E & BT-5.2
Front Panel I/O	• 2 x Openings reserved for antennas • 1 x RJ-45 2.5 Gbps LAN Jack • 1 x RS232/ 422/ 485 COM port - Mode selection by BIOS control. - 0V/ 5V/ 12V, 0.5A (Power selection by Jumper, default: 5V) • 1 x DIO Port - 8-bit DIO from motherboard • 1 x M.2 SSD Activity LED (M.2 B key SSD) • 1 x Power button/ LED
Rear Panel I/O	• 1 x DC power jack (lockable) • 1 x RJ-45 2.5 Gbps LAN Jack • 2 x HDMI™ connectors • 4 x USB 3.2 Gen 1 Type-A connectors

Continued on next column

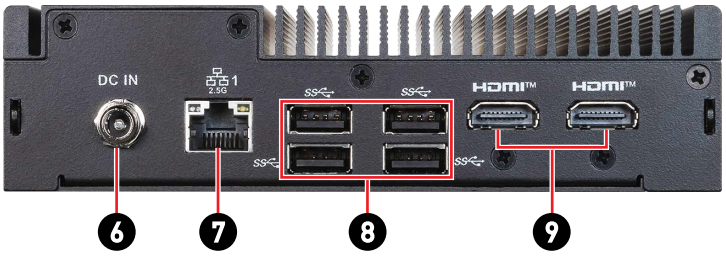
Model	MS-C909
Power Solution	• 19V, 65W Power Adapter (indoor SKU) - Power Input: 100~240Vac, 50/60Hz - Power Output: 19V , 3.42A
Dimension	155mm (W) x 130mm (D) x 40mm (H)
Weight	0.91 kg
Mounting	Wall Mount (Standard)
Accessories	• 1 x 19V, 65W Power Adapter • Wall Mount Set (w/ 4 x #6-32*L9 screws)
OS Support	• Windows 10 IoT Enterprise 2021 LTSC (64-bit, 21H2) • Linux (64-bit, by request)
Regulatory Compliance	FCC Class B / CE / RCM / BSMI / VCCI / UKCA / IC/ IEC 62368: CE(LVD) / UL / C-UL / CB / PSE/ RoHS Compliant
Environment	• Operation Temperature: -20 ~ 60°C • Operation Humidity: 10 ~ 90%, non-condensing • Storage Temperature: -20 ~ 80°C • Storage Humidity: 10 ~ 90%, non-condensing • Vibration: IEC 61373 Category 1 – Class B • Shock: IEC 61373 Category 1 – Class B

System Overview

Front Panel I/O



Rear Panel I/O



1

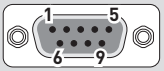
Wi-Fi Antenna Connector (Openings reserved for antennas)

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

2

RS232/422/485 Serial Port: COM1

The serial port is a 16550A high speed communications port that sends/ receives 16 bytes FIFOs. You can attach a serial mouse or other serial devices directly to the connector.



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	0V/5V/12V	Power Pin

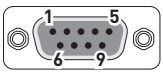
RS422		
PIN	**SIGNAL**	**DESCRIPTION**
1	422 TXD-	Transmit Data, Negative
2	422 RXD+	Receive Data, Positive
3	422 TXD+	Transmit Data, Positive
4	422 RXD-	Receive Data, Negative
5	GND	Signal Ground
6	NC	No Connection
7	NC	No Connection
8	NC	No Connection
9	NC	No Connection

RS485		
PIN	**SIGNAL**	**DESCRIPTION**
1	485 TXD-	Transmit Data, Negative
2	485 TXD+	Transmit 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

3

DIO Port

This port is provided for the Digital Input/Output (DIO) peripheral module.



PIN	SIGNAL	PIN	SIGNAL
1	GPO3	6	GPI2
2	GPO2	7	GPI1
3	GPO1	8	GPI0
4	GPO0	9	VCC5
5	GPI3	Shell	GND

Continued on next column

4 **Power Button/ 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

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

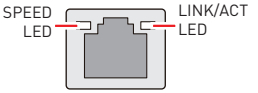
This indicator shows the activity status of the **M.2 B key SSD**. It flashes when the system is accessing data on the SSD and remains off when no disk activity is detected.

6 **DC Power Jack**

Power supplied through this jack supplies power to the system.

7 **2.5 Gbps LAN Jack**

The standard RJ-45 LAN jack is provided for connection to the Local Area Network (LAN). You can connect a network cable to it.



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

8 **USB 3.2 Gen 1 Port**

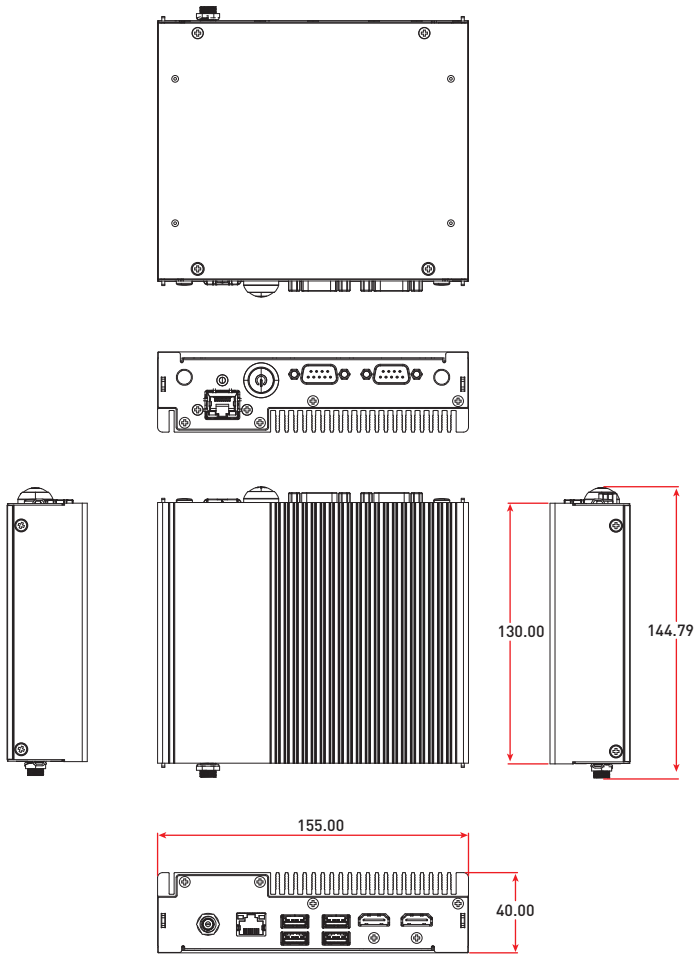
This connector is provided for USB peripheral devices. (Speed up to **5 Gbps**)

9 **HDMI™ Connector**

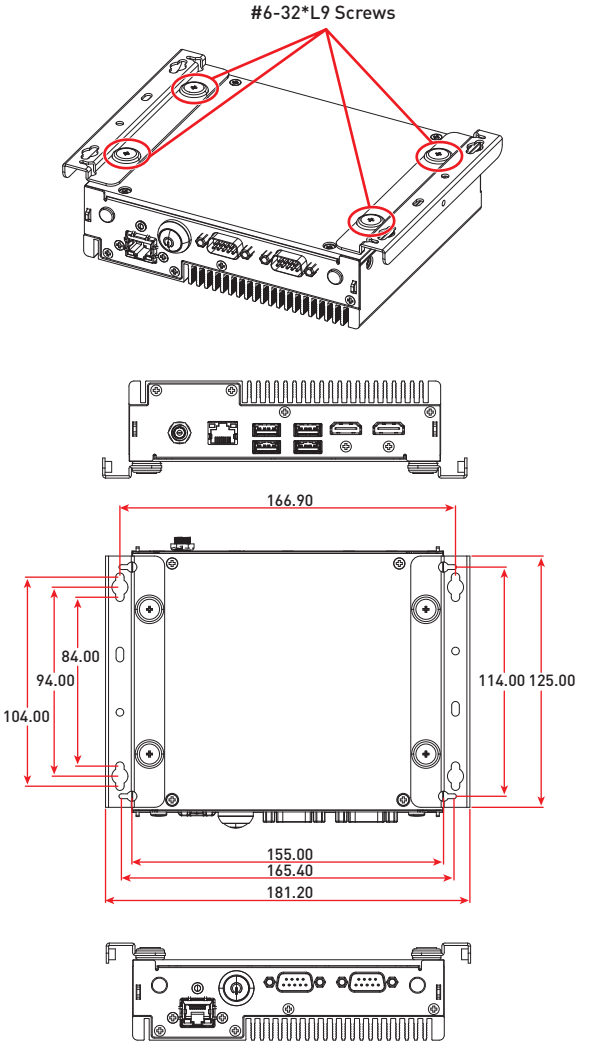
Supports 3840x2160@30Hz as specified in HDMI™ 1.4b.

ME Overview

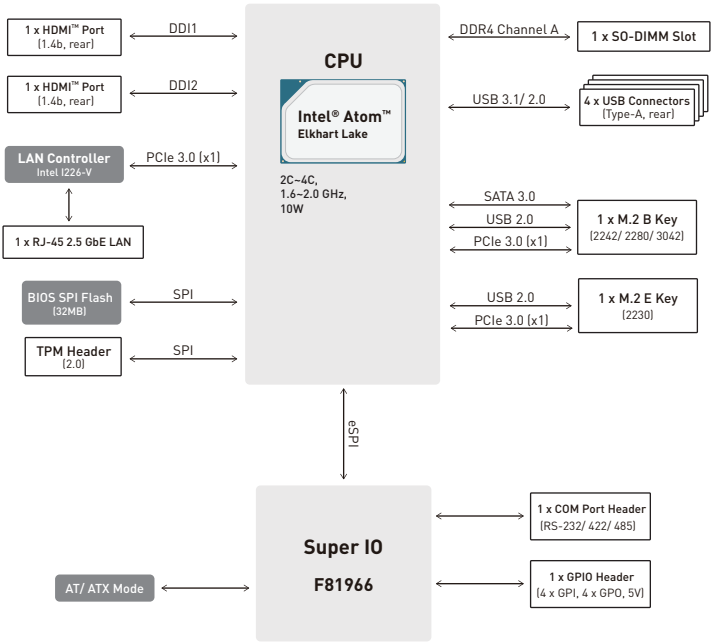
System Dimensions



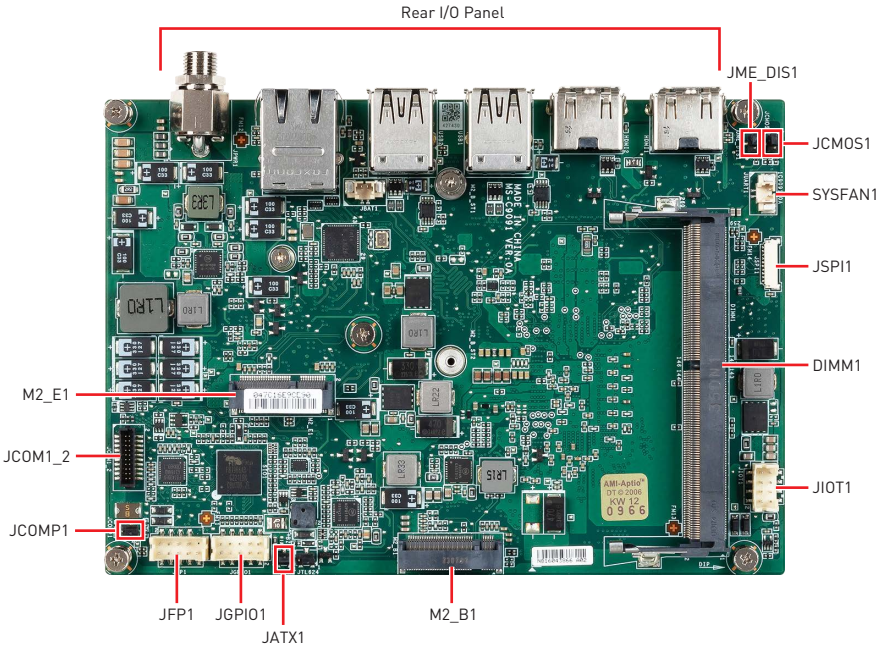
System Dimensions with Wall Mount Bracket



Block Diagram



Motherboard Overview

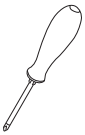


Getting Started

Important

- *All information is subject to change without prior notice.*
- *The system photos are provided for **demonstration of system assembly only**. The components of your system may differ based on the model you have purchased.*

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, HDD, 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.

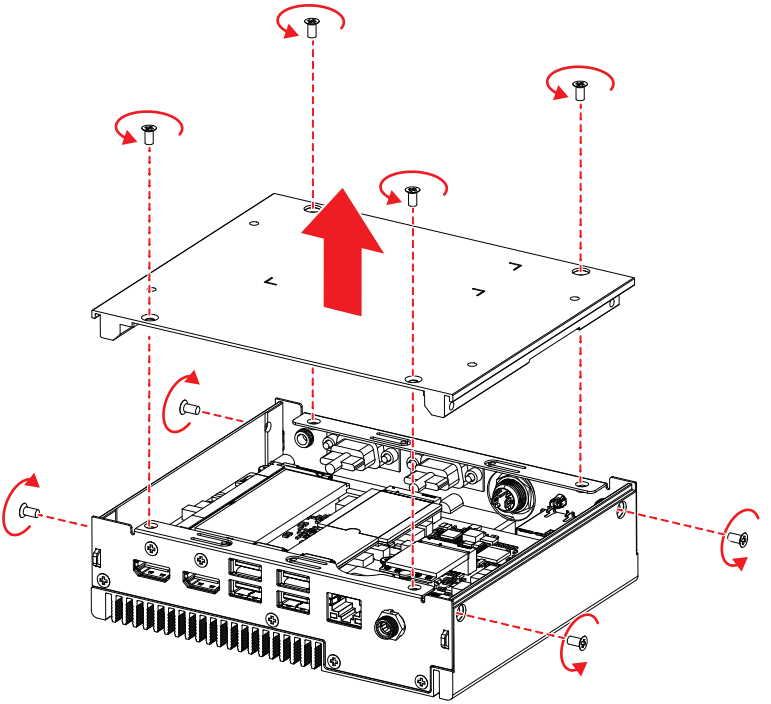
Removing System Cover

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 and remove the screw on the back and both sides of the system.
2. Carefully remove the cover and set the cover and screws aside for later use.

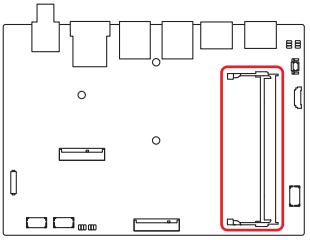
- *Follow the above procedures in reverse order to install the cover.*

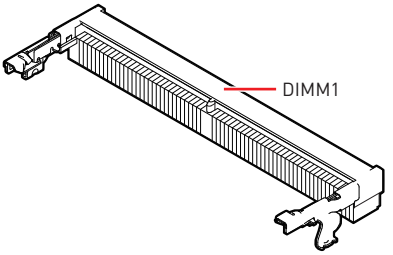


Installing Memory Module

1. Locate the SO-DIMM slot. Align the notch on the DIMM with the key on the slot and insert the DIMM into the slot.
2. Push the DIMM gently downwards until the slot levers click and lock the DIMM in place.
3. To uninstall the DIMM, flip the slot levers outwards and the DIMM will be released instantly.

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

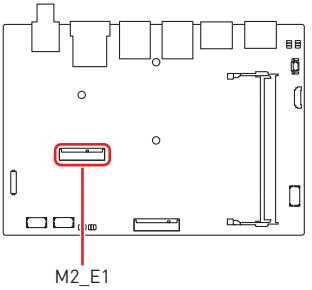




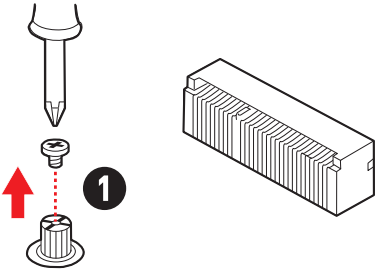
Important

- *You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.*
- *To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.*

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



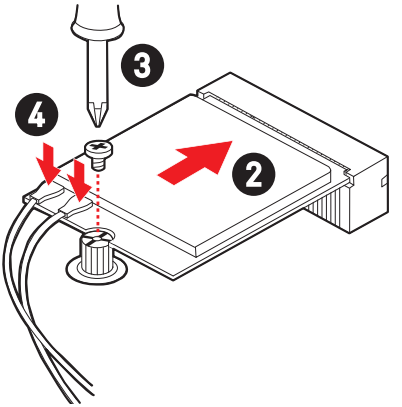
1. Loosen the M.2 screw from the motherboard.



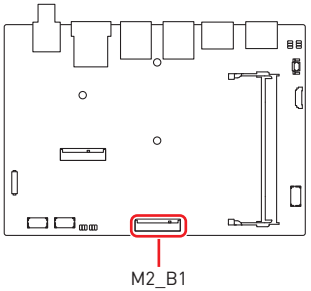
2. Insert your M.2 Wi-Fi card into the M.2 slot at a 30-degree angle.

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

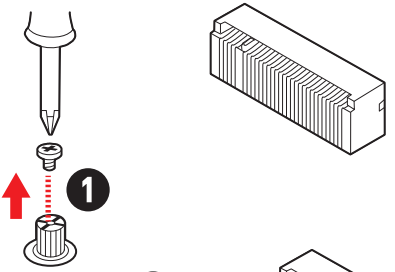
4. Locate the antenna cables and gently connect them to the Wi-Fi card.



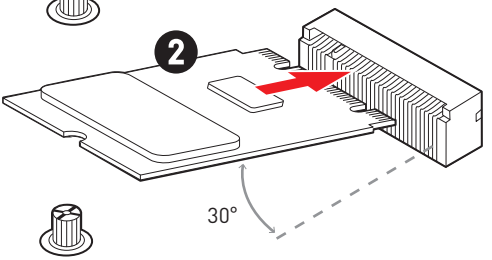
Installing M.2 Expansion Card (B-Key)



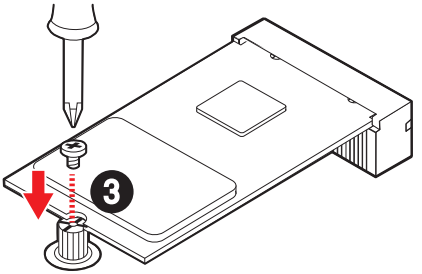
1. Loosen the M.2 screw from the motherboard.



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.

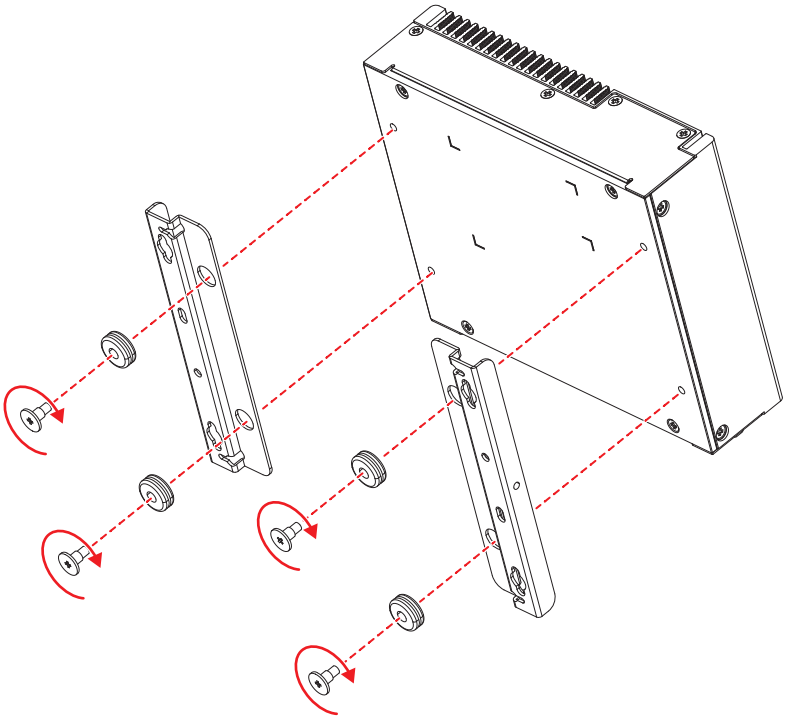


Important

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.

Installing Wall Mount Brackets

1. Flip over the system and locate the bracket screw holes.
2. Place the brackets and rubber pads along the sides with screw holes aligned.
3. Fasten the screws to fix the brackets.



Screws for Wall Mount Brackets

Screw Type: #6-32*L9 screw

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>** key to Boot Menu, **<F12>** key to PXE Boot .

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
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.

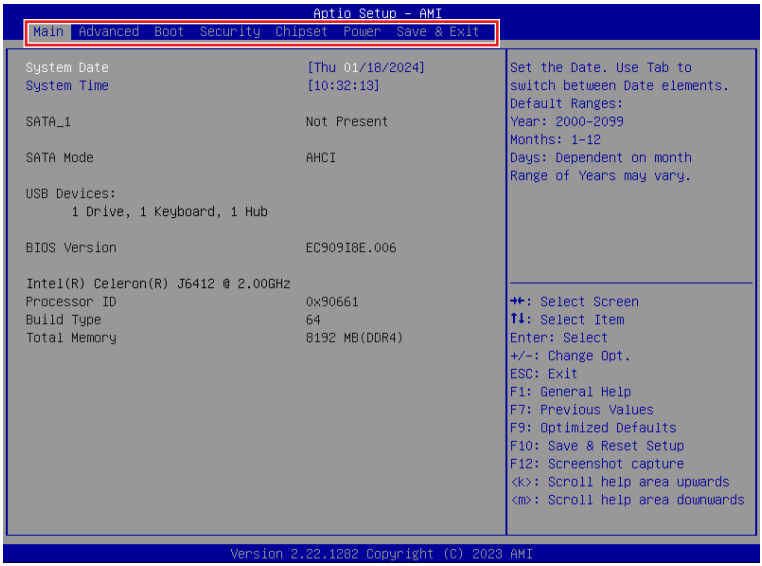
Sub-Menu

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.

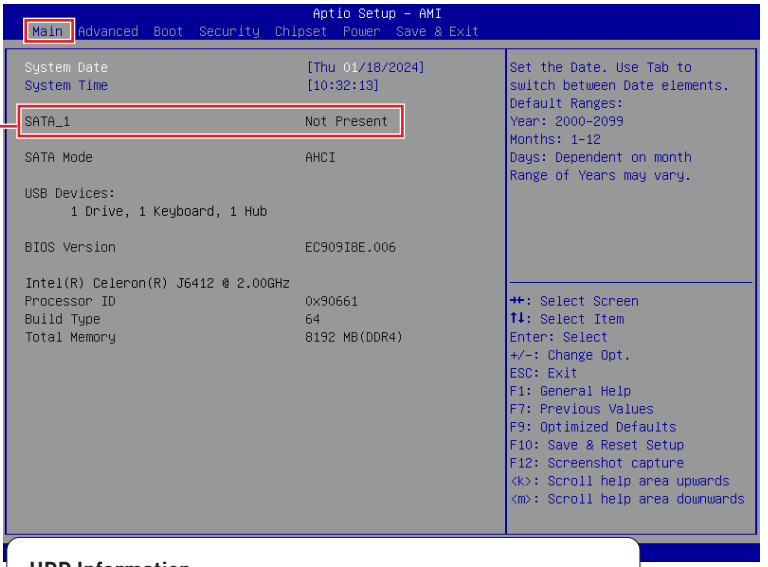
▶ Power

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 "Empty" only.

*__SATA_1__ is for M.2 B key (SATA signal)

▶System Date

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

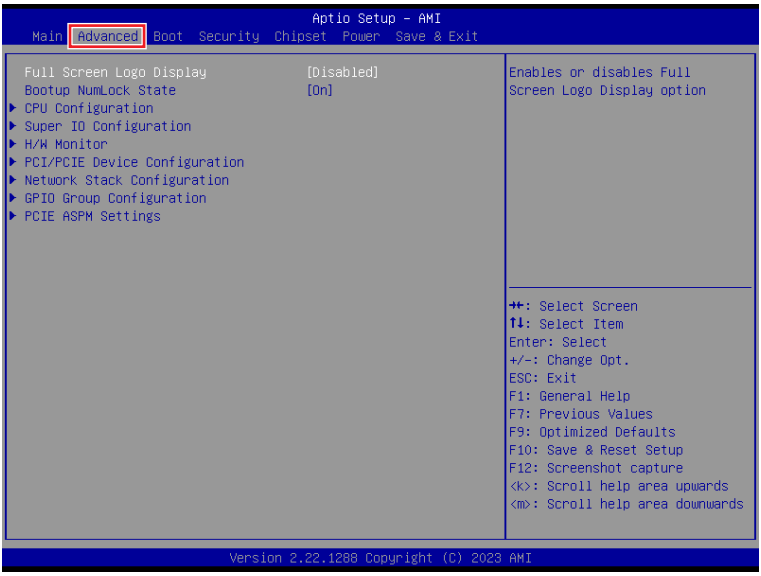
Format: <Day> <Month> <Date> <Year>.

▶System Time

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

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

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.**

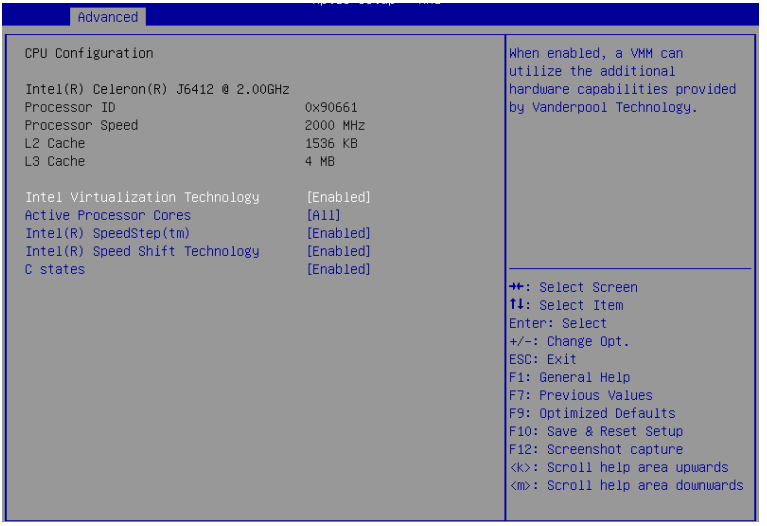
▶ Bootup NumLock State

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



▸ **Intel Virtualization Technology**

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.

▸ **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**

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.

▸ **FIFO Mode**

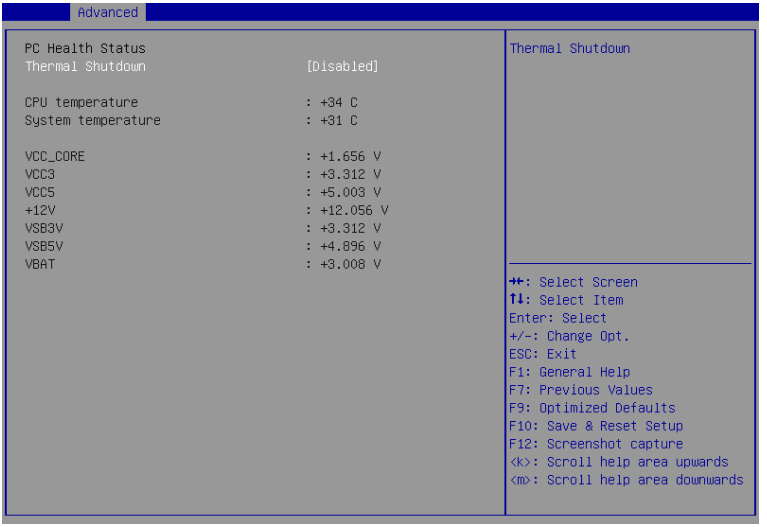
This setting controls the FIFO (First In First Out) data transfer mode.

▸ **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.



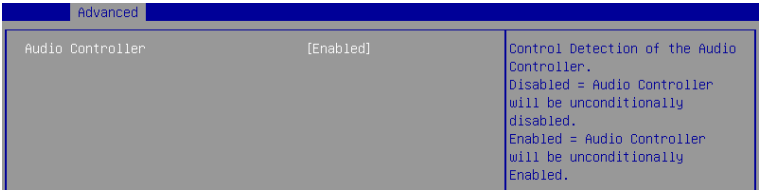
▸ Thermal Shutdown

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

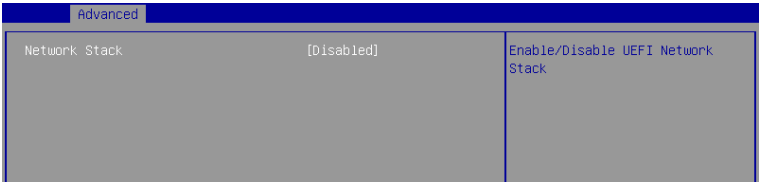


▸ Audio Controller

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 network boot (PXE) from BIOS. The following items will display when **Network Stak** is enabled.

» **IPV4 PXE Support**

Enables or disables IPv4 PXE boot support.

» **IPV4 HTTP Support**

Enables or disables Ipv4 HTTP Support.

» **IPV6 PXE Support**

Enables or disables Ipv6 PXE Support.

» **IPV6 HTTP Support**

Enables or disables Ipv6 HTTP Support.

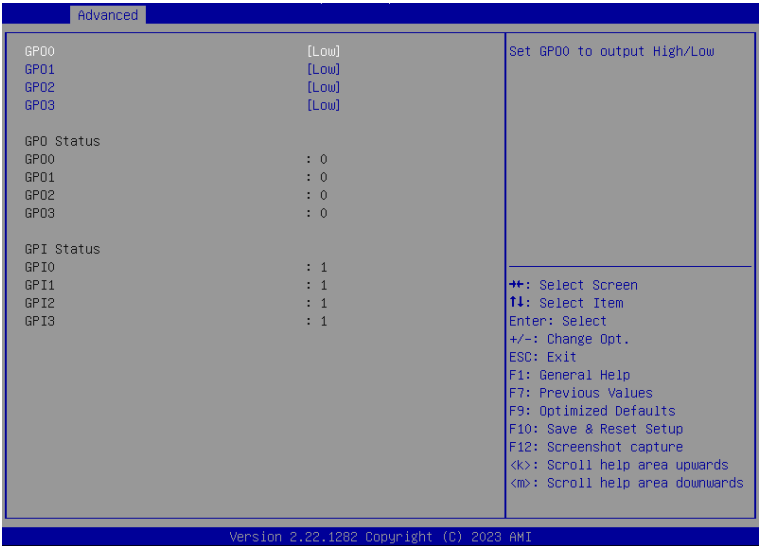
» **PXE boot wait time**

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.

▶GPIO Group Configuration

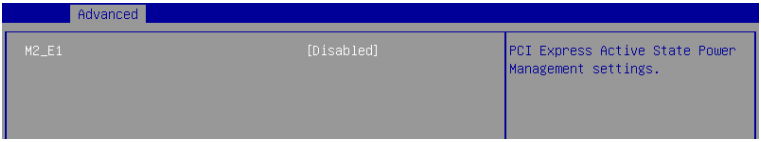


▸ GPO0 ~ GPO3

These settings control the operation mode of the specified GPIO.

▶PCIE ASPM settings

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

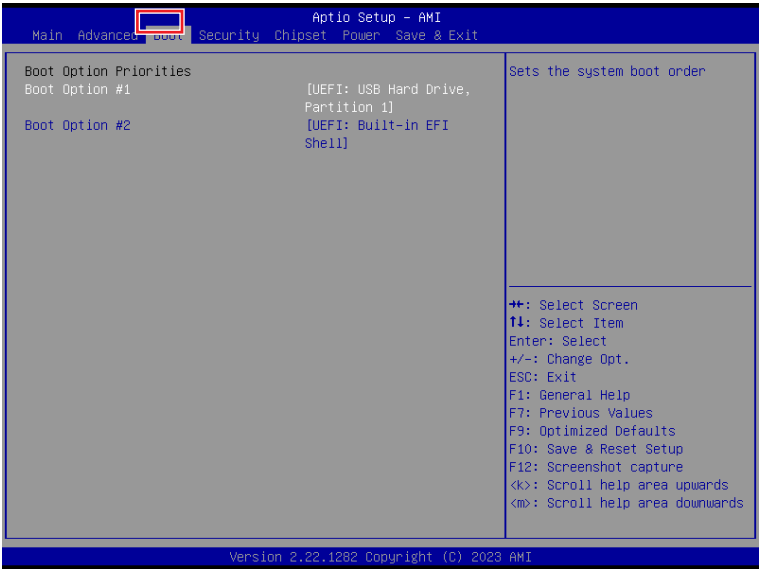


▸ M2_E1

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

[Disabled]	Disable this function.
[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.
[Auto]	Set the best state supported by the system.

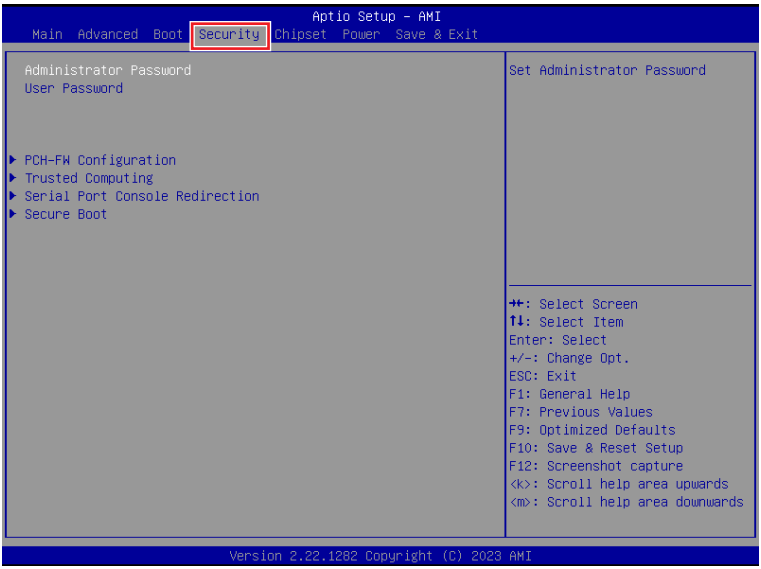
Boot



▶ Boot Option #1-2

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

Security



▶Administrator Password

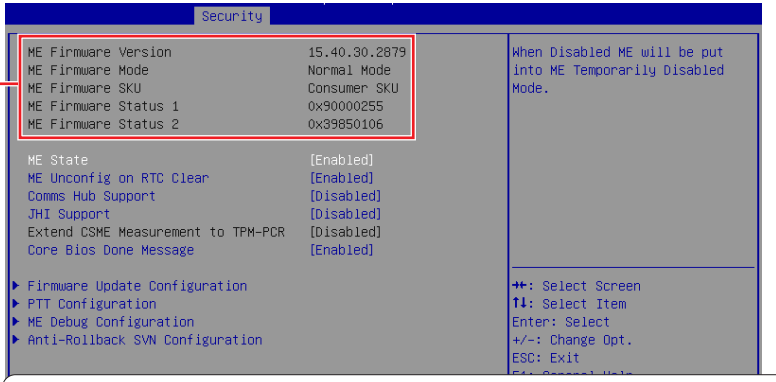
Administrator Password controls access to the BIOS Setup utility.

▶User Password

User Password controls access to the system at boot and to the BIOS Setup utility.

▶ PCH-FW Configuration

This menu allows you to configure settings related to the PCH firmware.



Firmware Information

ME Firmware Version	System Integrity Value	These settings show the firmware information of the **Intel ME (Management Engine).**
ME Firmware Mode	ME Firmware Status 1-2	
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.

▸ ME Unconfig on RTC Clear

Enables or disables the resetting of the ME configuration when the Real-Time Clock(RTC) is cleared.

▸ 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.

▸ **Firmware Update Configuration**

This menu will display when **ME State** is enabled.

» **ME FW Image Re-Flash**

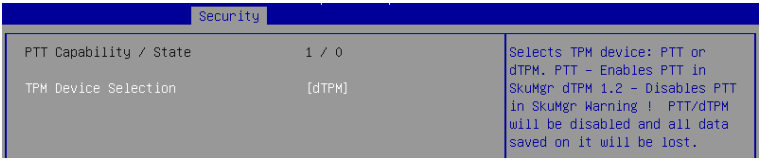
Enables or disables the ME Firmware Image Re-flashing**.**

» **FW Update**

Enables or disables the capability to perform a firmware update.

▸ **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.



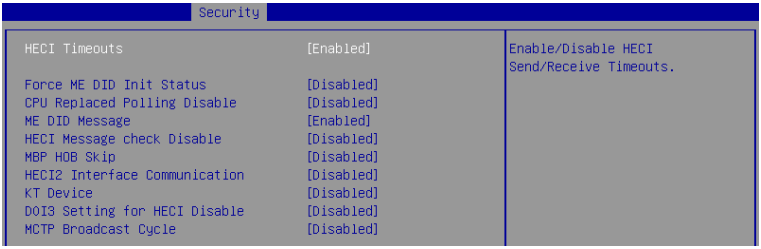
» **TPM Device Selection**

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). This menu will display when **ME State** is enabled.



» **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.

» **ME DID Message**

Enables or disables sending ME DID messages.

» **HECI Message Check Disable**

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

» **MBP H0B Skip**

Setting this option will skip ME's Memory-Based Protection (MBP) H0B region.

» **HECI2 Interface Communication**

This setting Adds/ Removes HECI2 device from PCI space.

» **KT Device**

Enables or disables Key Transfer (KT) Device.

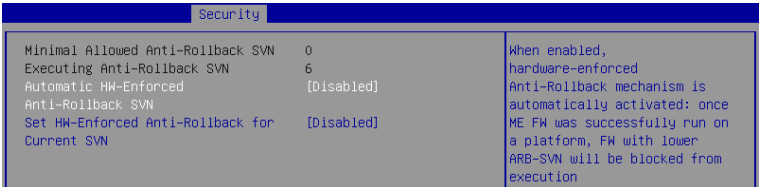
» **DOI3 Setting for HECI Disable**

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**



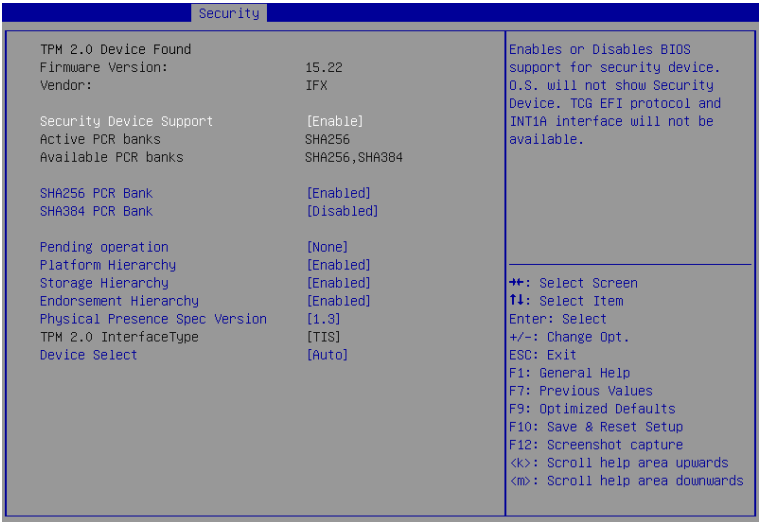
» **Automatic HW-Enforced Anti-Rollback SVN**

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.

▶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.

- **SHA256/ SHA384 PCR Bank**

  These settings enables or disables the SHA256 PCR Bank and SHA384 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 selection.

- **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.

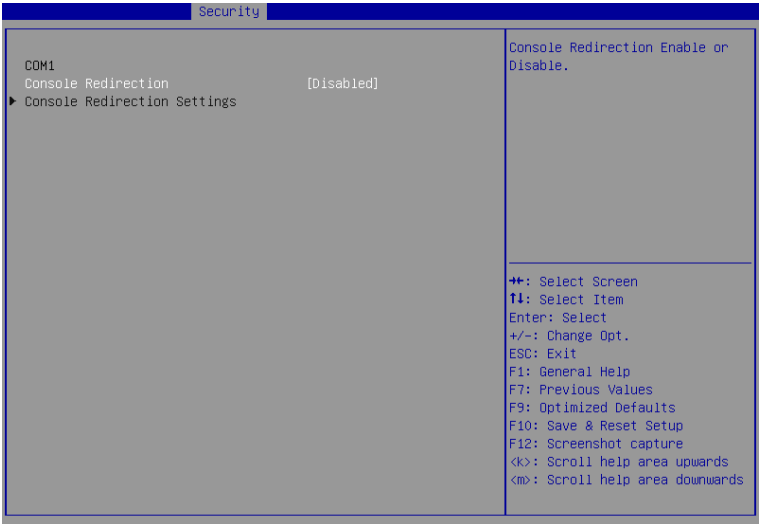
- **TPM 2.0 Interface Type**

  This setting shows the TPM 2.0 Interface Type.

- **Device Select**

  Select your TPM device through this setting.

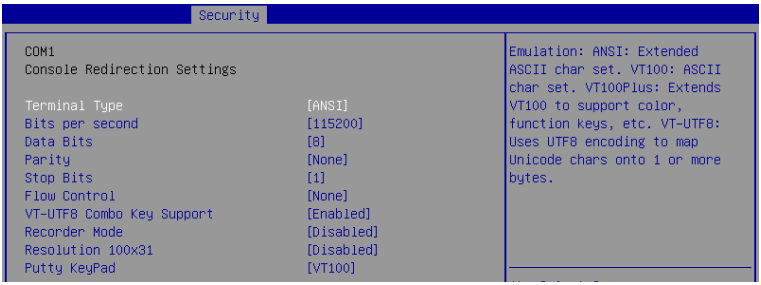
▶Serial Port Console Redirection



▸ 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.

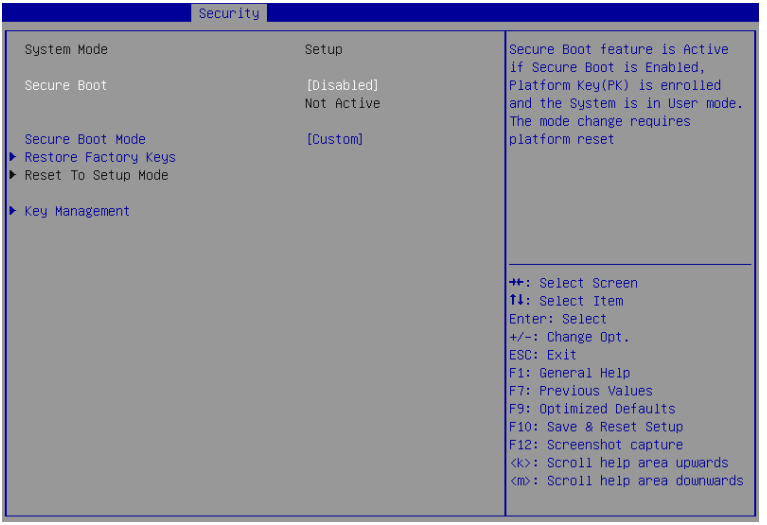
» **Recorder Mode, Resolution 100x31**

These settings enables or disables the recorder mode and 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 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**

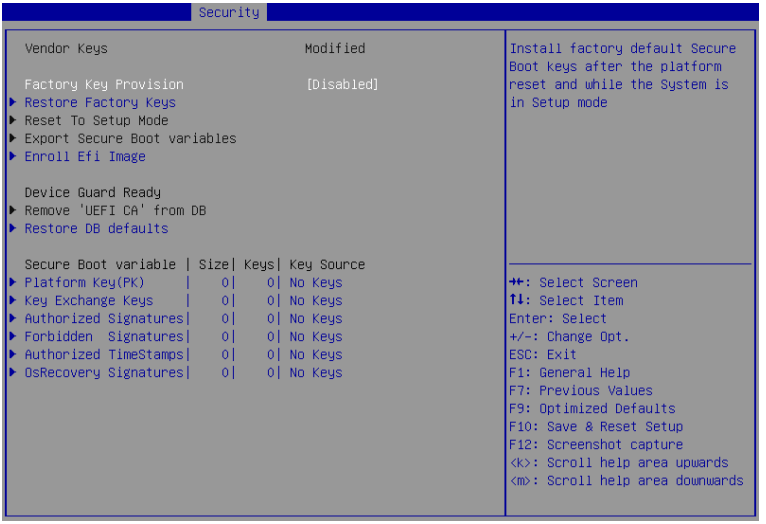
  Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when **"Secure Boot Mode"** sets to **[Custom]**.

- **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]**.

▸ **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.

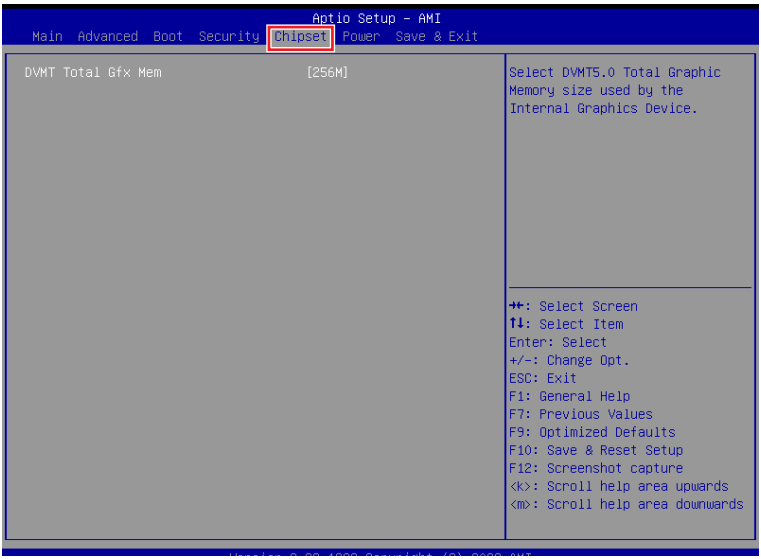
» **Append Key**

Loads an additional DBT from storage devices to your system.

» **OsRecovery Singnatures (dbr):**

Lists the available signatures for OS recovery.

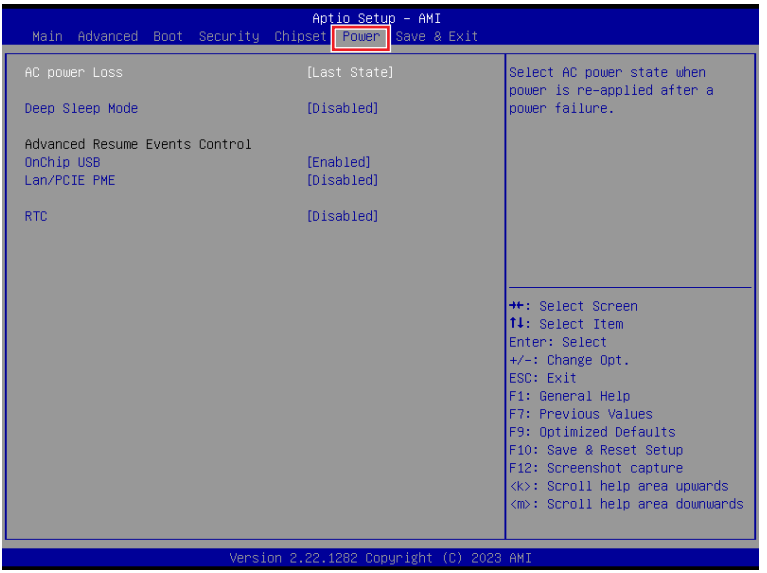
Chipset



▶ DVMT Total Gfx Mem

This setting specifies the total graphics memory size for Dynamic Video Memory Technology (DVMT).

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

The setting enables or disables the Deep S5 power saving mode. S5 is almost the same as G3 Mechanical Off, except that the PSU still supplies power, at a minimum, to the power button to allow return to S0. A full reboot is required. No previous content is retained. Other components may remain powered so the computer can "wake" on input from the keyboard, clock, modem, LAN, or USB device.

▶ OnChip USB

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

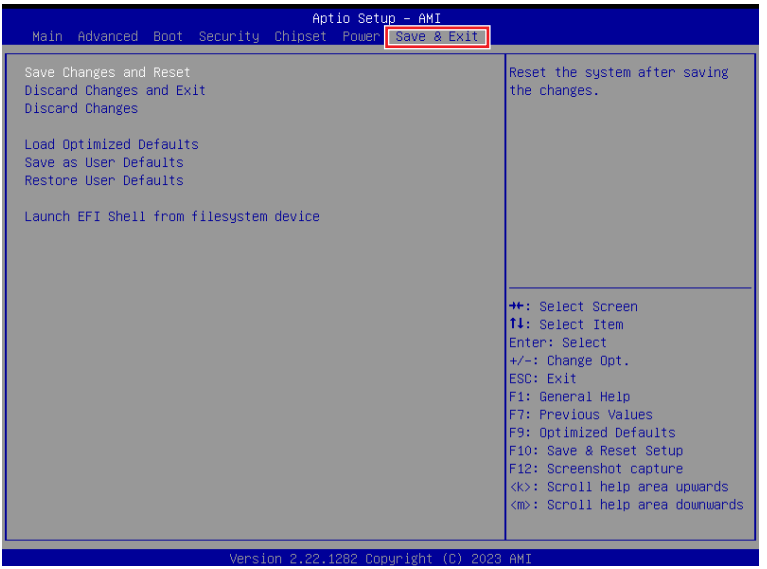
▶ LAN/ PCIE PME

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.

GPIO WDT Programming

This chapter provides GPIO (General Purpose Input/ Output), 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.

General Purpose IO

1. General Purposed IO – GPIO/DIO

The GPIO port configuration addresses are listed in the following table:

Name	IO Port	IO address	Name	IO Port	IO address
N_GPI0	0xA05	Bit 3	**N_GPO0**	0xA05	Bit 0
N_GPI1	0xA05	Bit 4	**N_GPO1**	0xA05	Bit 7
N_GPI2	0xA05	Bit 5	**N_GPO2**	0xA05	Bit 2
N_GPI3	0xA05	Bit 6	**N_GPO3**	0xA05	Bit 1

1.1 Set output value of GPO

1. Read the value from GPO port.
2. Set the value of GPO address.
3. Write the value back to GPO port.

Example: Set **N_GPO0** output “high”

```
val = Inportb (0xA05);          // Read value from N_GPO0 port.
val = val | (1<<0);             // Set N_GPO0 address (bit 0) to 1 (output “high”).
Outportb (0xA05, val);          // Write back to N_GPO0 port.
```

Example: Set **N_GPO1** output “low”

```
val = Inportb (0xA05);          // Read value from N_GPO1 port.
val = val & (~(1<<7));          // Set N_GPO1 address (bit 7) to 0 (output “low”).
Outportb (0xA05, val);          // Write back to N_GPO1 port.
```

1.2 Read input value from GPI

1. Read the value from GPI port.
2. Get the value of GPI address.

Example: Get **N_GPI2** input value.

```
val = Inportb (0xA05);                  // Read value from N_GPI2 port.
val = val & (1<<5);                     // Read N_GPI2 address (bit 5).
if (val)    printf (“Input of  N_GPI2  is High”);
else        printf (“Input of  N_GPI2  is Low”);
```

Watchdog Timer

2. Watchdog Timer – WDT

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

2.1 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
```

2.2 Set WDT Time

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

2.3 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.
```

2.4 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.
```

2.5 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");
```

2.6 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
```