



MS-C906

Industrial Data Machine

User Guide

Contents

Regulatory Notices.....	4
Safety Information	7
Specifications	9
System Overview	12
ME Overview.....	16
System Dimensions	16
Motherboard Overview	17
Motherboard Jumpers	18
Getting Started	20
Safety Precautions.....	20
System Cover.....	21
Removing System Cover.....	21
Applying Thermal Pad on the heatsink (Industrial SKUs only)	22
Memory Module.....	23
Applying DDR5 DIMM Thermal Pad	23
Installing Memory Module.....	23
M.2 SSD	24
Applying Thermal Pad for the M.2 SSD (Industrial SKUs only)	24
Installing M.2 SSD (M-Key).....	25
M.2 Wi-Fi Card.....	26
Installing M.2 Wi-Fi Card (E-Key)	26
M.2 Expansion Card	27
Installing M.2 Expansion Card (B-Key)	27
2.5" HDD/ SSD (Embedded SKUs only)	28
Installing 2.5" HDD/ SSD (9.5mm)	28

Revision

V1.3, 2025/04

Wall Mount Brackets	30
Installing Wall Mount Brackets.....	30
Din Rail	31
Installing Din Rail Clips	31
VESA Mount Plate (Optional)	32
Installing VESA Mount Plate	32
BIOS Setup.....	33
Entering Setup	33
The Menu Bar	35
Main	36
Advanced	37
Boot	44
Security	45
Chipset	59
Power	60
Save & Exit.....	62
GPIO WDT SMBus Programming.....	63
Abstract	63
General Purpose IO	64
Watchdog Timer.....	66
SMBus Access	67

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

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>

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.
- Please visit <https://us.msi.com/page/recycling> for information regarding the recycling of your product in the US.



Copyright and Trademarks Notice

msi MSI 微星 微星科技

MICRO-STAR INTERNATIONAL



Copyright © Micro-Star Int'l Co., Ltd. All rights reserved. The MSI logo used is a registered trademark of Micro-Star Int'l Co., Ltd. All other marks and names mentioned may be trademarks of their respective owners. No warranty as to accuracy or completeness is expressed or implied. MSI reserves the right to make changes to this document without prior notice.

HDMI™

HIGH-DEFINITION MULTIMEDIA INTERFACE

The terms HDMI™, HDMI™ High-Definition Multimedia Interface, HDMI™ Trade dress and the HDMI™ Logos are trademarks or registered trademarks of HDMI™ Licensing Administrator, Inc.

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-C906
Processor	<ul style="list-style-type: none"> • 13th Gen Intel® Core™ Raptor Lake-P, U-Series Mobile Processors (TDP up to 15W) • Embedded SKUs <ul style="list-style-type: none"> - i5-1345UE - i5-1335UE(Non-vPro®) - i3-1315UE (Non-vPro®) • Industrial SKUs <ul style="list-style-type: none"> - i5-1345URE - i3-1315URE (Non-vPro®)
Chipset	Within processor
Antenna	<ul style="list-style-type: none"> • 6 x Openings reserved for antennas - Supports Wi-Fi/ BT/ 4G/ LTE/ 5G
Network	<ul style="list-style-type: none"> • Embedded SKUs <ul style="list-style-type: none"> - 4 x Intel® I226-LM 2.5 Gbps LAN • Industrial SKUs <ul style="list-style-type: none"> - 4 x Intel® I226-IT 2.5 Gbps LAN
Audio	Realtek® ALC897 High Definition Audio codec
Graphics	<ul style="list-style-type: none"> • 4 x HDMI™ 2.0b up to 4096x2304 @60Hz • 4 independent displays supported
Memory	<ul style="list-style-type: none"> • 1 x DDR5 SO-DIMM slot (262-pin) - Single Channel for DDR5, Non-ECC Up to 5200 MT/s, 32 GB
Storage	<ul style="list-style-type: none"> • 1 x SATA 3.0 port (6Gb/s) • 1 x M.2 M Key slot (2280) - Supports PCIe 4.0 x4 signal - Supports NVMe devices
Expansion Slots	<ul style="list-style-type: none"> • 1 x M.2 B Key slot (2242/ 3042) - Supports PCIe x1, USB 2.0 signals - Shared with nano SIM holder • 1 x M.2 E Key slot (2230) - Supports PCIe x1, USB 2.0 signal - Supports CNVi modules • 1 x Nano SIM Holder - Shared with M.2 B key slot

Continued on next column

Model	MS-C906
Front Panel I/O	<ul style="list-style-type: none"> • 2 x Openings reserved for antennas • 1 x Line-Out jack • 1 x Microphone jack • 4 x RS232/ 422/ 485 Serial ports (COM1~4) <ul style="list-style-type: none"> - 0V/ 5V/ 12V, 0.5A each port (Power selection by Jumper, default: 5V) • 4 x USB 2.0 Type-A connectors (5V/0.5A) • 1 x Extend switch header • 1 x Hard disk drive (HDD) LED • 1 x Power button/ LED
Rear Panel I/O	<ul style="list-style-type: none"> • 4 x Openings reserved for antennas • 1 x DC power jack • 1 x Phoenix DC power connector • 4 x RJ-45 2.5 Gbps LAN ports • 4 x HDMI™ connectors (2.0b) • 4 x USB 10Gbps Type-A connectors (5V/0.9A) • DIO Port • 1 x Grounding point
Power Solution	<ul style="list-style-type: none"> • 19V, 90W Power Adapter
Dimension	215mm (W) x 155mm (D) x 65mm (H)
Weight	2.25kg
Mounting	<ul style="list-style-type: none"> • Wall mount • DIN rail mount • VESA mount (Optional)
Accessories	<ul style="list-style-type: none"> • 1 x 19V, 90W Power Adapter (Embedded SKUs only) • 1 x Wall Mount Set • 1 x DIN Rail Mount Set • 1 x VESA Mount Set (Optional) • 2 x Phoenix Contact Plug-in Terminal Blocks • 1 x SATA Power & Signal Cable • 1 x Memory Pad (Embedded SKUs only) • 3 x Memory Pad (Industrial SKUs only) • 3 x M.2 SSD Pad (Industrial SKUs only)

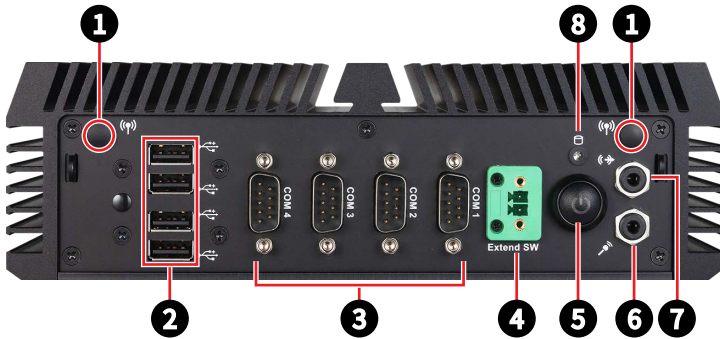
Continued on next column

Model	MS-C906
OS Support	<ul style="list-style-type: none"> • Windows 10 IoT Enterprise LTSC 21H2 (64-bit) • Windows 11 IoT Enterprise LTSC 24H2 (64-Bit) • Linux (supports by request)
Regulatory Compliance	FCC Class B / CE / RCM / BSMI / VCCI / UKCA / IC / RoHS Compliant/ IEC 62368: CE(LVD)
Environment	<ul style="list-style-type: none"> • Operation Temperature: <ul style="list-style-type: none"> - Embedded SKUs: 0 ~ 50°C (w/SSD, thermal test w/ Airflow: 0.7m/s) - Industrial SKUs: -20 ~ 70°C (w/ WT devices, thermal test w/ Airflow: 0.7m/s) • Operation Humidity: 10 ~ 90%, non-condensing • Storage Temperature: -20 ~ 80°C • Storage Humidity: 10 ~ 90%, non-condensing

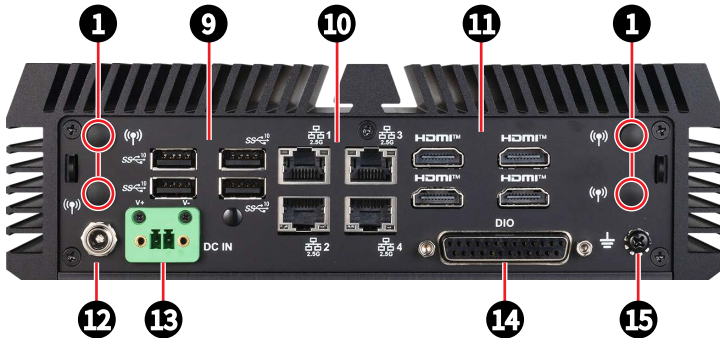
System Overview


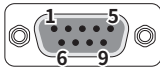


Front Panel I/O
































Rear Panel I/O

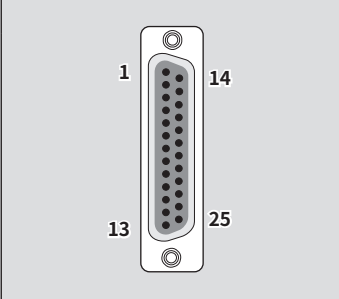


<p>1</p>	<p>Wi-Fi Antenna Connector (Openings reserved for antennas)</p> <p>These connectors allow you to connect an external antenna for wireless communication. User may find two on the front side and 4 on the rear side of the system.</p>																																																																																																			
<p>2</p>	<p>USB 2.0 Port</p> <p>This connector is provided for USB peripheral devices. (Speed up to 480 Mbps)</p> <p> Important</p> <p><i>High-speed devices are recommended for USB 3.2 ports whereas low-speed devices, such as mouse or keyboard, are suggested to be plugged into the USB 2.0 ports.</i></p>																																																																																																			
<p>3</p>	<p>RS232/422/485 Serial Port: COM1~4</p> <p>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.</p> <div style="text-align: center;">  </div> <table border="1" style="margin: 10px auto; width: 60%;"> <thead> <tr> <th colspan="3">RS232</th> </tr> <tr> <th>PIN</th> <th>SIGNAL</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr><td>1</td><td>NDCD</td><td>Data Carrier Detect</td></tr> <tr><td>2</td><td>NSIN</td><td>Signal In</td></tr> <tr><td>3</td><td>NSOUT</td><td>Signal Out</td></tr> <tr><td>4</td><td>NDTR</td><td>Data Terminal Ready</td></tr> <tr><td>5</td><td>GND</td><td>Signal Ground</td></tr> <tr><td>6</td><td>NDSR</td><td>Data Set Ready</td></tr> <tr><td>7</td><td>NRTS</td><td>Request To Send</td></tr> <tr><td>8</td><td>NCTS</td><td>Clear To Send</td></tr> <tr><td>9</td><td>0V/5V/12V</td><td>Power Pin</td></tr> </tbody> </table> <table border="1" style="margin: 10px auto; width: 45%;"> <thead> <tr> <th colspan="3">RS422</th> </tr> <tr> <th>PIN</th> <th>SIGNAL</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr><td>1</td><td>422 TXD-</td><td>Transmit Data, Negative</td></tr> <tr><td>2</td><td>422 RXD+</td><td>Receive Data, Positive</td></tr> <tr><td>3</td><td>422 TXD+</td><td>Transmit Data, Positive</td></tr> <tr><td>4</td><td>422 RXD-</td><td>Receive Data, Negative</td></tr> <tr><td>5</td><td>GND</td><td>Signal Ground</td></tr> <tr><td>6</td><td>NC</td><td>No Connection</td></tr> <tr><td>7</td><td>NC</td><td>No Connection</td></tr> <tr><td>8</td><td>NC</td><td>No Connection</td></tr> <tr><td>9</td><td>NC</td><td>No Connection</td></tr> </tbody> </table> <table border="1" style="margin: 10px auto; width: 45%;"> <thead> <tr> <th colspan="3">RS485</th> </tr> <tr> <th>PIN</th> <th>SIGNAL</th> <th>DESCRIPTION</th> </tr> </thead> <tbody> <tr><td>1</td><td>485 TXD-</td><td>Transmit Data, Negative</td></tr> <tr><td>2</td><td>485 TXD+</td><td>Transmit Data, Positive</td></tr> <tr><td>3</td><td>NC</td><td>No Connection</td></tr> <tr><td>4</td><td>NC</td><td>No Connection</td></tr> <tr><td>5</td><td>GND</td><td>Signal Ground</td></tr> <tr><td>6</td><td>NC</td><td>No Connection</td></tr> <tr><td>7</td><td>NC</td><td>No Connection</td></tr> <tr><td>8</td><td>NC</td><td>No Connection</td></tr> <tr><td>9</td><td>NC</td><td>No Connection</td></tr> </tbody> </table>	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
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																																																																																																		

Continued on next column

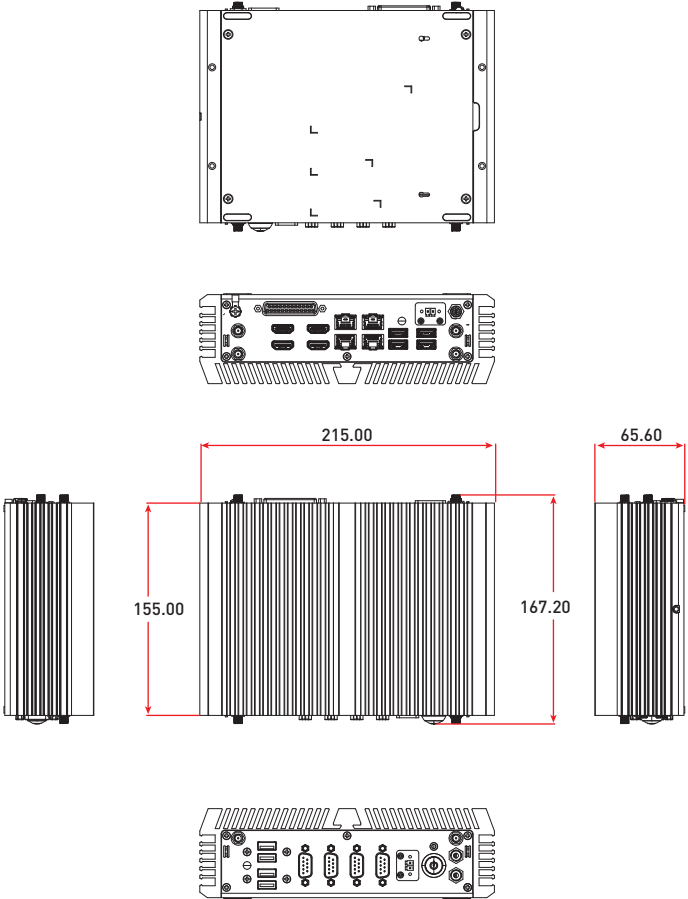
<p>4</p>	<p>Extend Switch Connector This connector is provided for remote power button control.</p>																	
<p>5</p>	<p> Power Button/ LED Press the button to turn the system on or off.</p> <table border="1" data-bbox="207 316 923 451"> <thead> <tr> <th>LED Status</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td> Off</td> <td>ACPI S4/ S5/ Deep S5, Power Off</td> </tr> <tr> <td> Blinking</td> <td>ACPI S3</td> </tr> <tr> <td> Green</td> <td>ACPI S0</td> </tr> </tbody> </table>	LED Status	Description	 Off	ACPI S4/ S5/ Deep S5, Power Off	 Blinking	ACPI S3	 Green	ACPI S0									
LED Status	Description																	
 Off	ACPI S4/ S5/ Deep S5, Power Off																	
 Blinking	ACPI S3																	
 Green	ACPI S0																	
<p>6</p>	<p>Mic-In Jack This connector is provided for microphones.</p>																	
<p>7</p>	<p>Line-Out Jack This connector is provided for headphones or speakers.</p>																	
<p>8</p>	<p> HDD Activity LED This indicator shows the activity status of the HDD. It flashes when the system is accessing data on the HDD and remains off when no disk activity is detected.</p>																	
<p>9</p>	<p>USB 10Gbps Type-A Port This connector is provided for USB peripheral devices. (Speed up to 10 Gbps)</p>																	
<p>10</p>	<p>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.</p> <table border="1" data-bbox="202 1045 927 1273"> <thead> <tr> <th>LED</th> <th>Status</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td rowspan="3">Link/ Activity LED</td> <td> Off</td> <td>No link</td> </tr> <tr> <td> Yellow</td> <td>Linked</td> </tr> <tr> <td> Blinking</td> <td>Data activity</td> </tr> <tr> <td rowspan="3">Speed LED</td> <td> Off</td> <td>10/100 Mbps</td> </tr> <tr> <td> Green</td> <td>1 Gbps</td> </tr> <tr> <td> Orange</td> <td>2.5 Gbps</td> </tr> </tbody> </table>	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
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																

Continued on next column

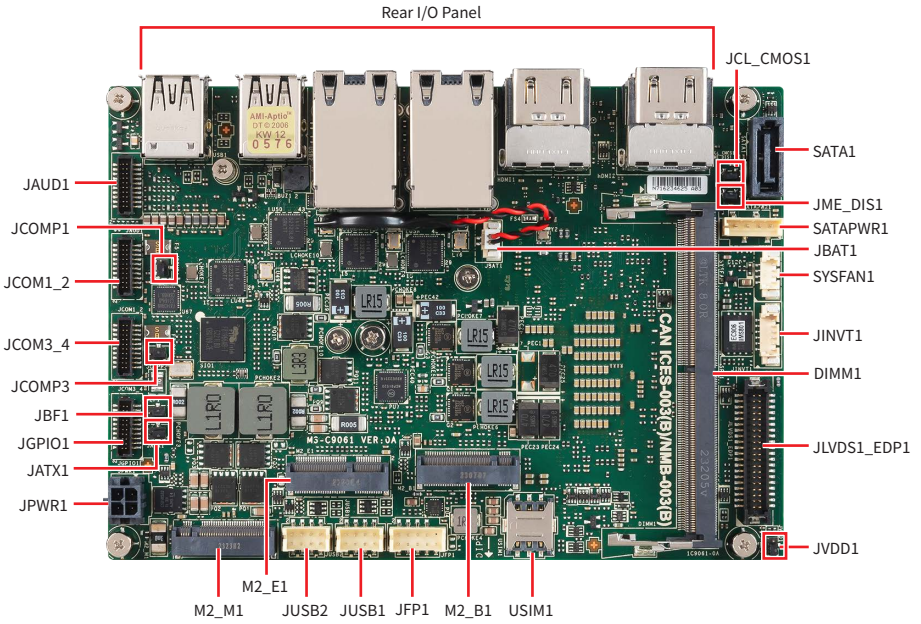
<p>11</p>	<p>HDMI™ Connector HDMI™ HIGH-DEFINITION MULTIMEDIA INTERFACE</p> <p>Supports 4096x2304 @60Hz as specified in HDMI™ 2.0b.</p>																																																								
<p>12</p>	<p>DC Power Jack</p> <p>Power supplied through this jack supplies power to the system.</p>																																																								
<p>13</p>	<p>Phoenix DC Power Connector</p> <p>The system is designed with a Phoenix connector that carries DC input.</p> <p>⚠ Important</p> <p><i>Your power source can either be connected to the Power Jack or the Phoenix DC Power Connector. Avoid connecting to both simultaneously.</i></p>																																																								
<p>14</p>	<p>DIO Port</p> <p>This port is provided for the Digital Input/Output (DIO) peripheral module.</p> <div style="display: flex; align-items: center;">  <table border="1" data-bbox="566 635 902 935" style="margin-left: 20px;"> <thead> <tr> <th>PIN</th> <th>SIGNAL</th> <th>PIN</th> <th>SIGNAL</th> </tr> </thead> <tbody> <tr><td>1</td><td>GND</td><td>14</td><td>GND</td></tr> <tr><td>2</td><td>GP00</td><td>15</td><td>GP10</td></tr> <tr><td>3</td><td>GP01</td><td>16</td><td>GP11</td></tr> <tr><td>4</td><td>GP02</td><td>17</td><td>GP12</td></tr> <tr><td>5</td><td>GP03</td><td>18</td><td>GP13</td></tr> <tr><td>6</td><td>GP04</td><td>19</td><td>GP14</td></tr> <tr><td>7</td><td>GP05</td><td>20</td><td>GP15</td></tr> <tr><td>8</td><td>GP06</td><td>21</td><td>GP16</td></tr> <tr><td>9</td><td>GP07</td><td>22</td><td>GP17</td></tr> <tr><td>10</td><td>VCC5</td><td>23</td><td>VCC5</td></tr> <tr><td>11</td><td>NC</td><td>24</td><td>NC</td></tr> <tr><td>12</td><td>NC</td><td>25</td><td>NC</td></tr> <tr><td>13</td><td>NC</td><td></td><td></td></tr> </tbody> </table> </div>	PIN	SIGNAL	PIN	SIGNAL	1	GND	14	GND	2	GP00	15	GP10	3	GP01	16	GP11	4	GP02	17	GP12	5	GP03	18	GP13	6	GP04	19	GP14	7	GP05	20	GP15	8	GP06	21	GP16	9	GP07	22	GP17	10	VCC5	23	VCC5	11	NC	24	NC	12	NC	25	NC	13	NC		
PIN	SIGNAL	PIN	SIGNAL																																																						
1	GND	14	GND																																																						
2	GP00	15	GP10																																																						
3	GP01	16	GP11																																																						
4	GP02	17	GP12																																																						
5	GP03	18	GP13																																																						
6	GP04	19	GP14																																																						
7	GP05	20	GP15																																																						
8	GP06	21	GP16																																																						
9	GP07	22	GP17																																																						
10	VCC5	23	VCC5																																																						
11	NC	24	NC																																																						
12	NC	25	NC																																																						
13	NC																																																								
<p>15</p>	<p>Grounding Point</p> <p>The Grounding Point is provided to connect a grounding wire.</p>																																																								

ME Overview

System Dimensions



Motherboard Overview

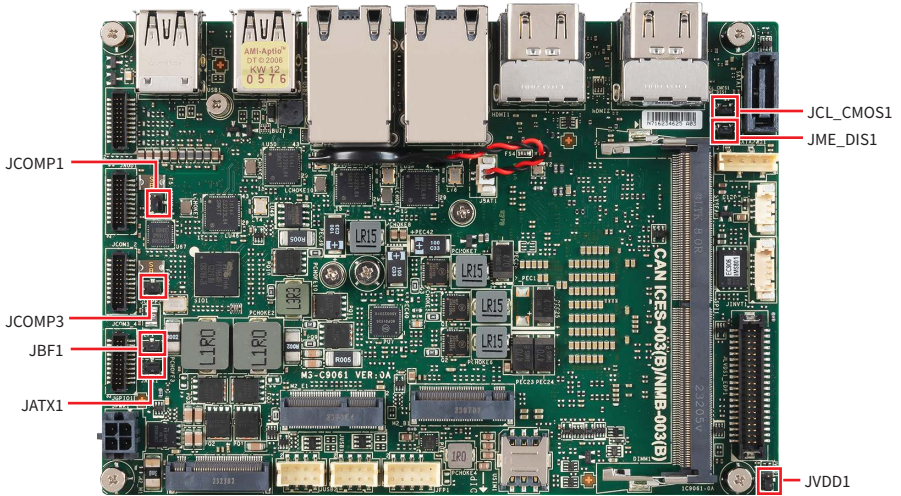


Motherboard Jumpers






Important

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



Jumper Name	Default Setting	Description
JCL_CMOS1	1	CMOS Clear Jumper
		1-2: Normal (Default) 2-3: Clear CMOS
JME_DIS1	1	ME Jumper
		1-2: Normal (Default) 2-3: ME disable
JVDD1	1	LVDS Power Select Jumper
		1-2: VCC3 (Default) 2-3: VCC5
JATX1	1	ATX Mode Select Jumper
		1-2: ATX mode (Default) 2-3: AT mode

Continued on next column

JBF1	 1	SMbus Power Select Jumper
		1-2: Normal (Default) 2-3: Flash
JCOMP1	 1	JCOM1_2 Power Select Jumper
		1-2: VCC5 (Default) 2-3: +12V
JCOMP3	 1	JCOM3_4 Power Select Jumper
		1-2: VCC5 (Default) 2-3: +12V

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.

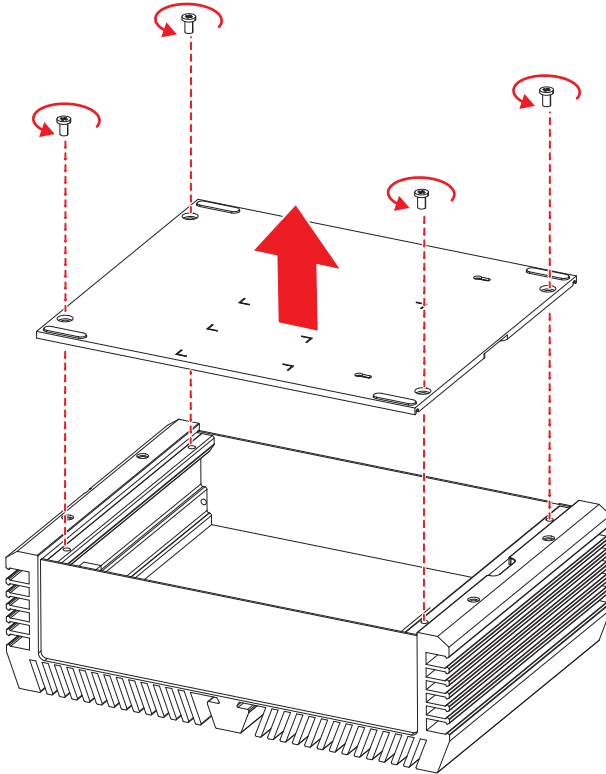
System Cover

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 side.
 2. Carefully remove the cover and set the cover and screw aside for later use.
- *Follow the above procedures in reverse order to install the cover.*



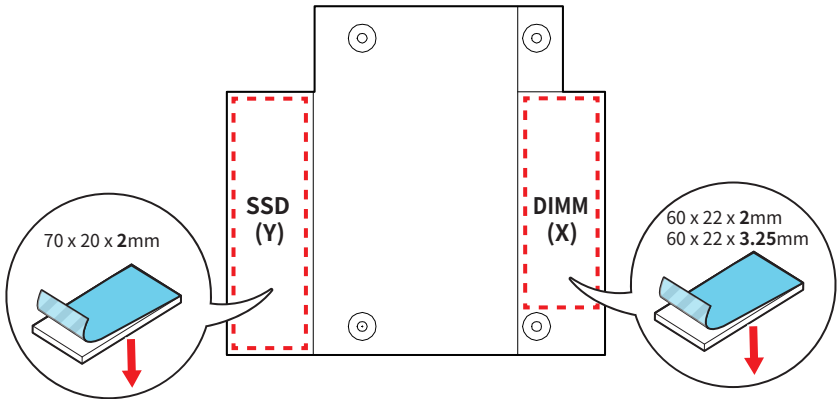
Applying Thermal Pad on the heatsink (Industrial SKUs only)

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

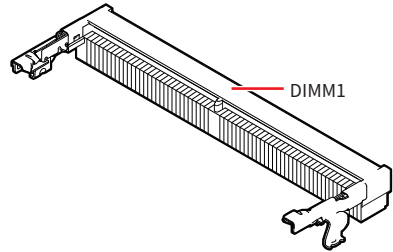
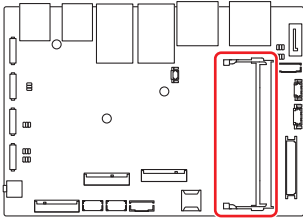
- Locate the heatsink on the backside of the system cover.

Heatsink Thermal Pad Application Table

Component	DIMM Type	Pad Size	How to Apply
DIMM	Single-sided (chips on one side)	60 x 22 x 3.25mm	Place the thermal pad on Location X of the heatsink, ensuring it fully covers the contact area on the DIMM.
	Double-sided (chips on both sides)	60 x 22 x 2mm	
SSD	Single-sided (chips on one side)	70 x 20 x 2mm	Place the thermal pad on Location Y of the heatsink, aligning it with the thermal contact area on the SSD.
	Double-sided (chips on both sides)		



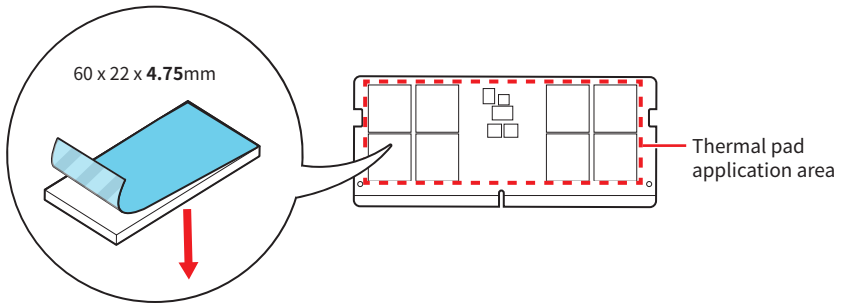
Memory Module



Applying DDR5 DIMM Thermal Pad

Align the **60 x 22 x 4.75mm** thermal pad with the memory chips on the DIMM.

- The thermal pad will be placed **between the DDR5 DIMM and the motherboard**.



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

Important

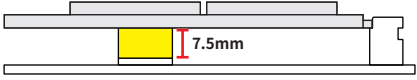
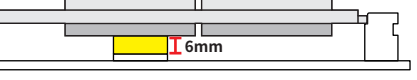
- You can barely see the golden finger if the DIMM is properly inserted in the DIMM slot.
- To ensure system stability for Dual channel mode, memory modules must be of the same type, number and density.

M.2 SSD

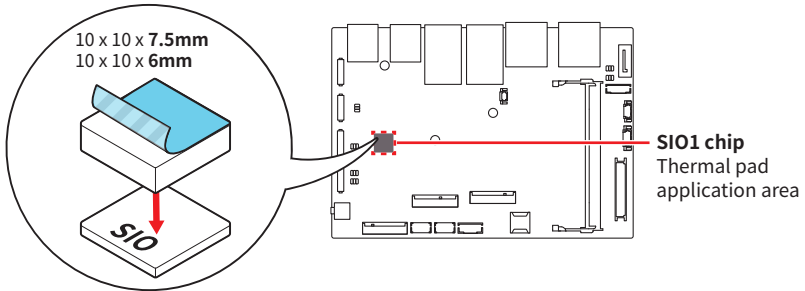
Applying Thermal Pad for the M.2 SSD (Industrial SKUs only)

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.

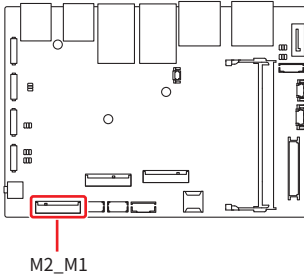
M.2 SSD Thermal Pad Application Table

M.2 SSD Type	Pad Size	M.2 SSD & Thermal Pad Side View
Single-sided (chips on one side)	10 x 10 x 7.5mm	
Double-sided (chips on both sides)	10 x 10 x 6mm	

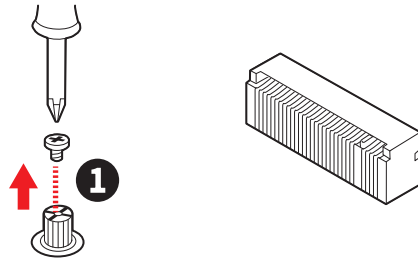
Apply a thermal pad to the S10 chip.



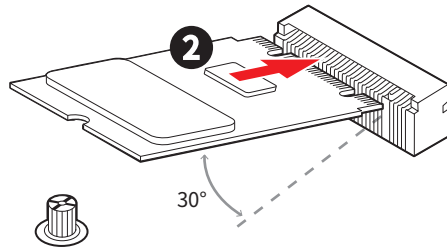
Installing M.2 SSD (M-Key)



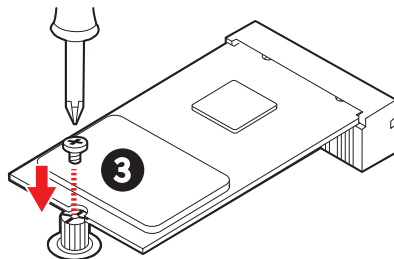
1. Loosen the M.2 screw from the motherboard.



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

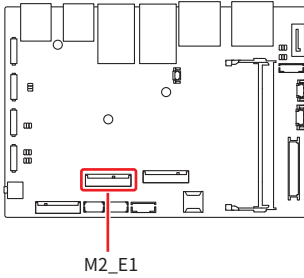


3. Secure the M.2 SSD in place with the supplied M.2 screw.

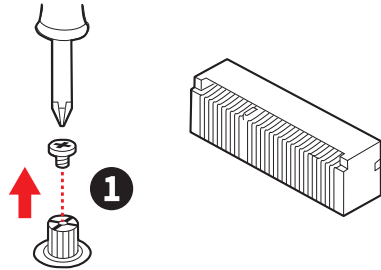


M.2 Wi-Fi Card

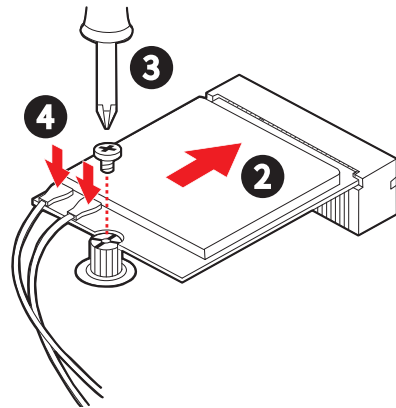
Installing M.2 Wi-Fi Card (E-Key)



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



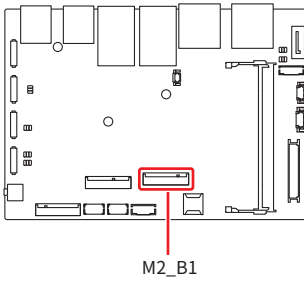
2. Insert your M.2 Wi-Fi card into the M.2 slot at a 30-degree angle.
3. Secure the M.2 Wi-Fi card in place with the supplied M.2 screw.



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

M.2 Expansion Card

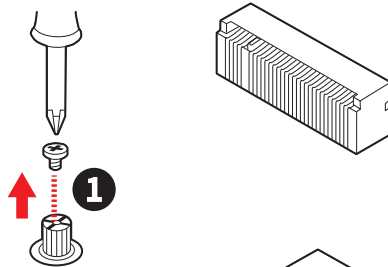
Installing M.2 Expansion Card (B-Key)



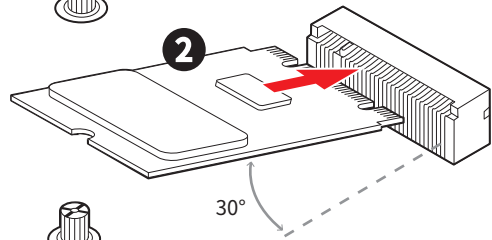
Important

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.

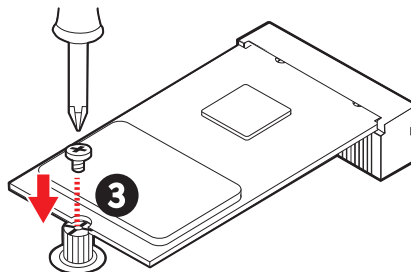
1. Loosen the M.2 screw from the motherboard.



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




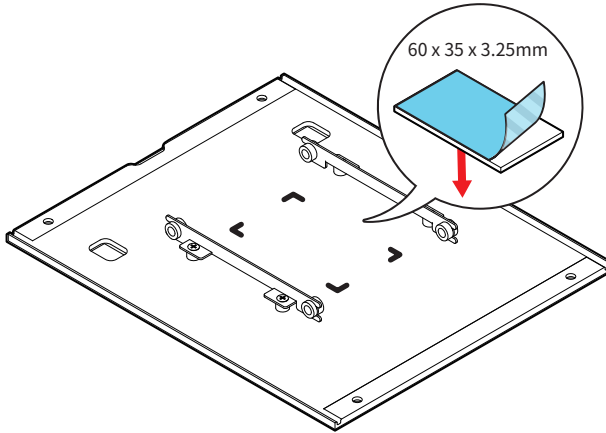
3. Secure the M.2 SSD in place with the supplied M.2 screw.



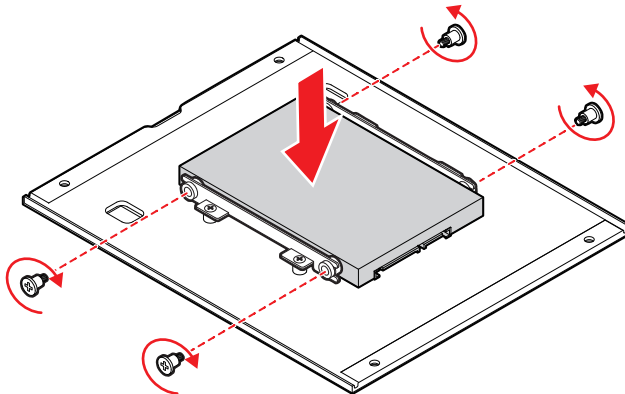
2.5" HDD/ SSD (Embedded SKUs only)

Installing 2.5" HDD/ SSD (9.5mm)

1. Flip over the system cover and locate the HDD/SSD bracket.
2. Apply the provided **thermal pad (60 x 35 x 3.25mm)** to the **rectangular recess**  in the middle of the HDD/SSD bracket.



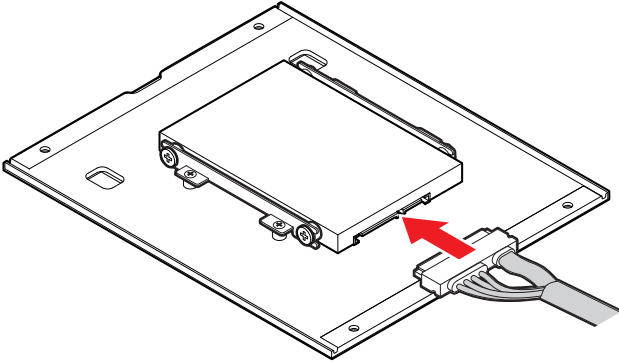
3. Insert the HDD/SSD into the bracket, aligning the screw holes. Secure the drive to the bracket by tightening the screws.



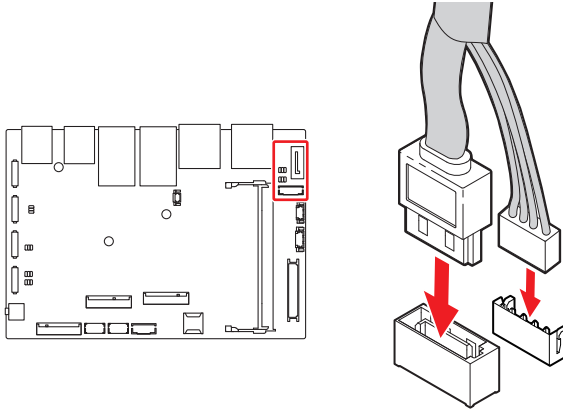
Important

- Before assembly, please make sure the HDD/SSD is compatible with the bracket.
 - Please make sure the HDD is properly and completely fixed to the bracket.
-

-
4. Align the SATA data & power connector and connect to the HDD/SSD.



-
5. Connect the **SATA signal & power connector** to the motherboard to complete the installation.

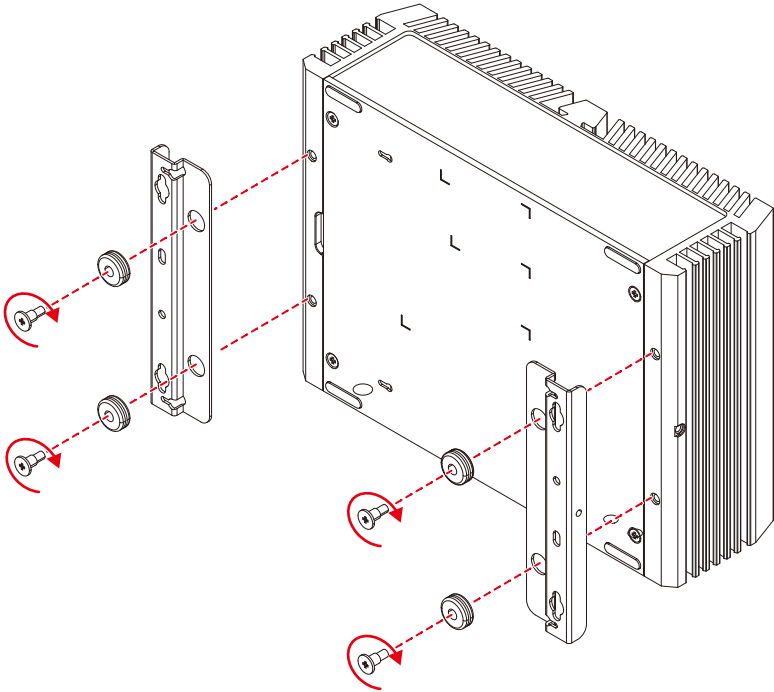


- *Follow the above procedures in reverse order to replace the HDD/SSD if needed.*
-

Wall Mount Brackets

Installing Wall Mount Brackets

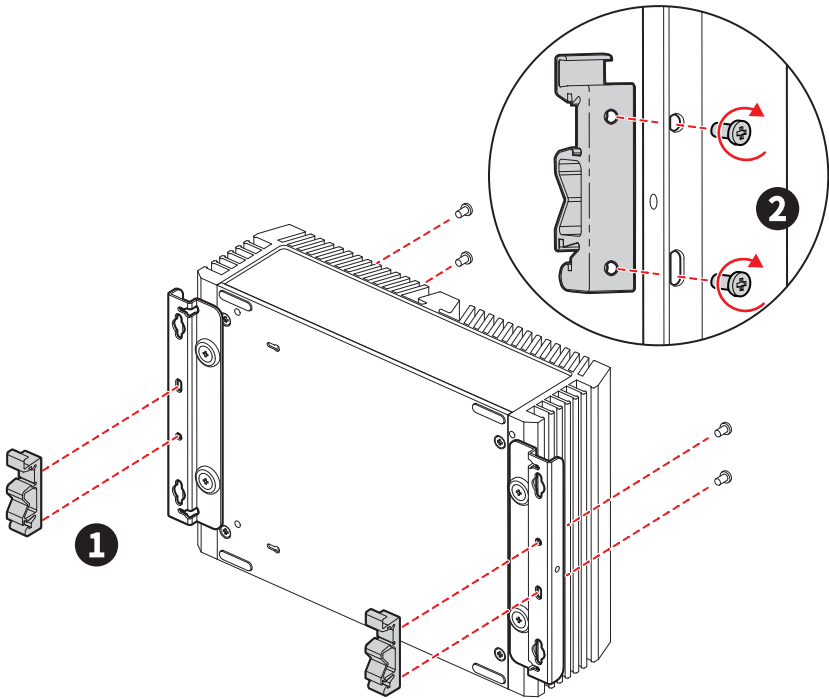
1. Flip over the system and locate the bracket screw holes.
2. Place the brackets and rubber pads along the sides with screw holes aligned.
3. Fasten the screws to fix the brackets.



Din Rail

Installing Din Rail Clips

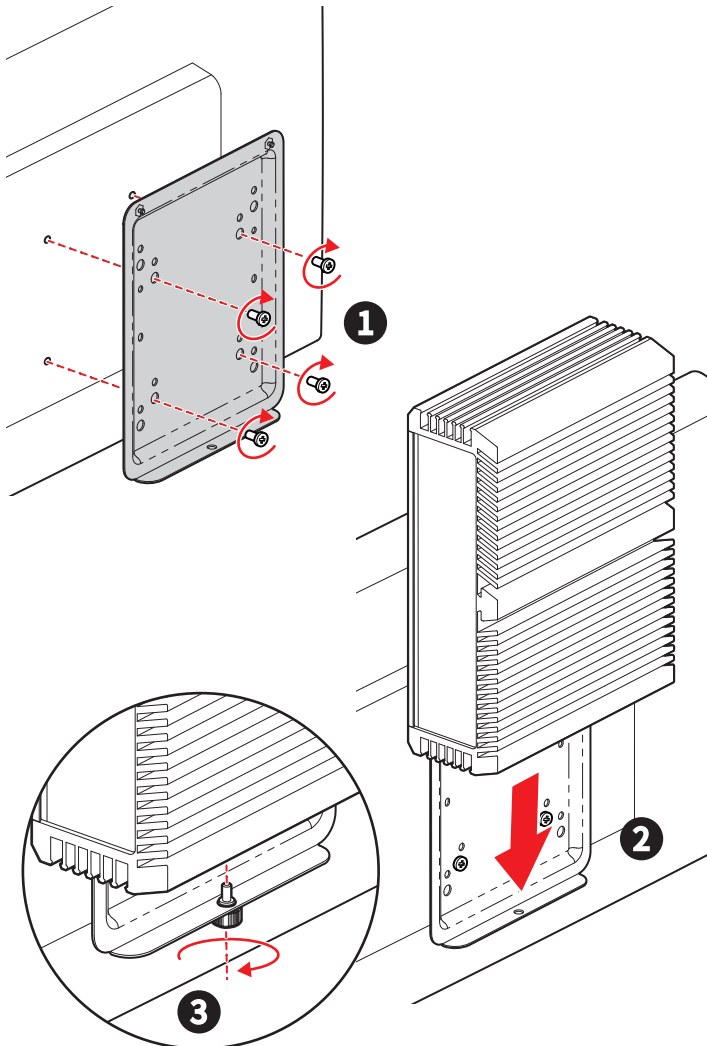
1. Attach the **DIN rail clips** to the wall mount brackets with the hooks aligned.
2. Insert screws through the wall mount brackets into the DIN rail clips and tighten until secure.



VESA Mount Plate (Optional)

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 or <F2> key to enter Setup, <F11> key to Boot Menu, <F12> key to PXE Boot .

Press 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.

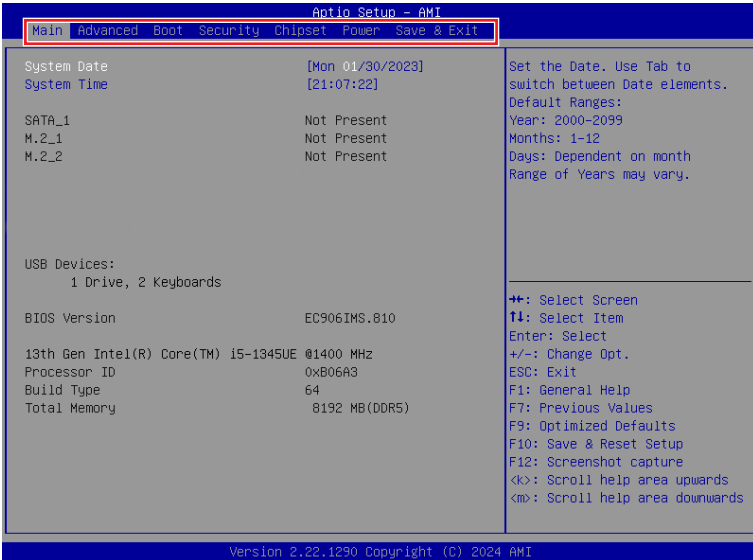
Sub-Menu

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.

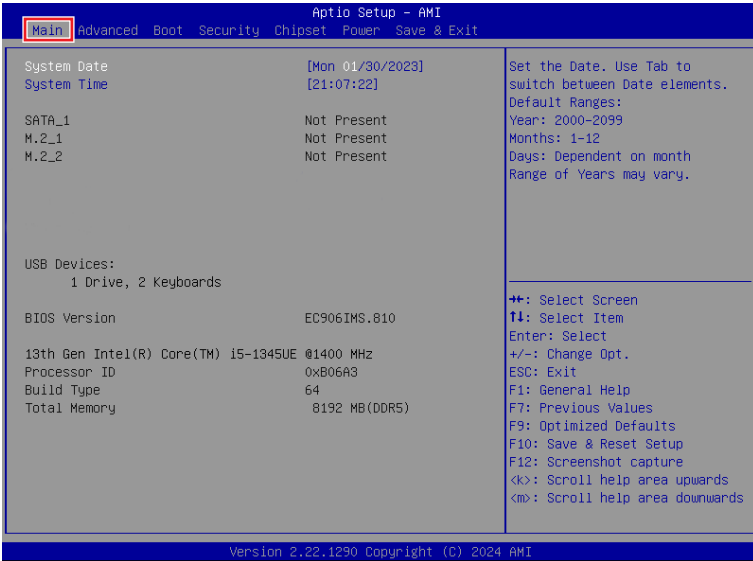
► Power

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



► System Date

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

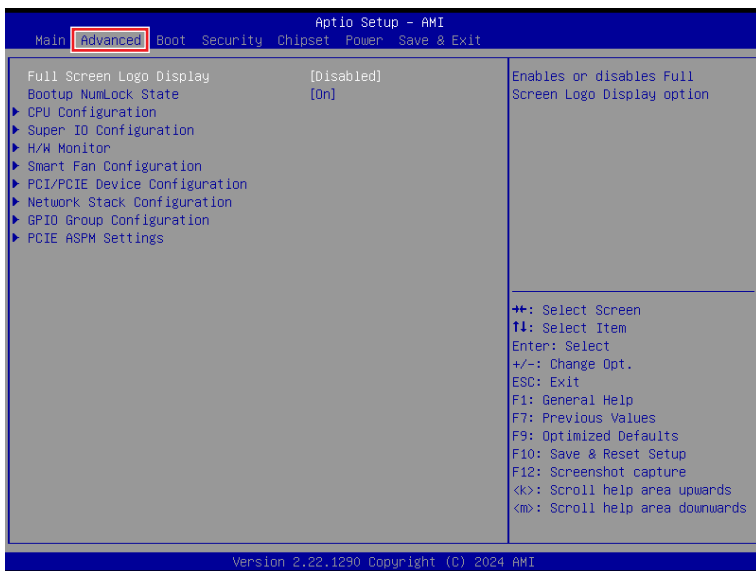
Format: <Day> <Month> <Date> <Year>.

► 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

Advanced	
CPU Configuration	
13th Gen Intel(R) Core(TM) i5-1345UE	
Processor ID	0xB06A3
Processor Speed	1400 MHz
P-core Information	
L1 Data Cache	48 KB x 2
L1 Instruction Cache	32 KB x 2
L2 Cache	1280 KB x 2
L3 Cache	12 MB
E-core Information	
L1 Data Cache	32 KB x 8
L1 Instruction Cache	64 KB x 8
L2 Cache	2048 KB x 2
L3 Cache	12 MB
Intel Virtualization Technology	[Enabled]
Hyper-Threading	[Enabled]
Active Performance-cores	[All]
Active Efficient-cores	[All]
Intel(R) SpeedStep(tm)	[Enabled]
Intel(R) Speed Shift Technology	[Enabled]
C states	[Enabled]
When enabled, a VMM can utilize the additional hardware capabilities provided by Vanderpool Technology.	
+/: Select Screen T1: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <K>: Scroll help area upwards <M>: Scroll help area downwards	

► 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.

► 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

Advanced	
Super IO Configuration	
Serial Port 1	[Enabled]
Device Settings	IO=3F8h; IRQ=4;
Change Settings	[Auto]
Mode Select	[RS232]
Serial Port 2	[Enabled]
Device Settings	IO=2F8h; IRQ=3;
Change Settings	[Auto]
Mode Select	[RS232]
Serial Port 3	[Enabled]
Device Settings	IO=3E8h; IRQ=7;
Change Settings	[Auto]
Mode Select	[RS232]
Serial Port 4	[Enabled]
Device Settings	IO=2E8h; IRQ=7;
Change Settings	[Auto]
Mode Select	[RS232]
FIFO Mode	[128-byte]
Watch Dog Timer	[Disabled]
Enable or Disable Serial Port (COM)	
++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards	

► Serial Port 1/ 2/ 3/ 4

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/ 3/ 4.

► 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.

Advanced	
Pc Health Status	Thermal Shutdown
Thermal Shutdown	[Disabled]
System temperature	: +31 °C
CPU temperature	: +30 °C
SYSFAN	: N/A
VCC_CORE	: +0.712 V
VCC3	: +3.312 V
VCC5	: +5.129 V
+12V	: +12.144 V
VSBS3V	: +3.328 V
VSBS5V	: +5.016 V
VBAT	: +3.088 V
⚡: Select Screen ⚡: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture <k>: Scroll help area upwards <m>: Scroll help area downwards	

► 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.

► Smart Fan Configuration

Advanced	
Configuration Smart FAN	Disabled/Enabled Smart FAN Function
SYSFAN	[Disabled]

► SYSFAN

This setting enables or disables the Smart Fan function. Smart Fan is an excellent feature which will adjust the CPU/system fan speed automatically depending on the current CPU/system temperature, avoiding the overheating to damage your system. The following item will display when **SYSFAN1** is enabled.

» Min. Speed (%)

The beginning speed of the System fan.

► PCI/PCIE Device Configuration

Advanced		
Audio Controller	[Enabled]	Control Detection of the Audio Controller. Disabled = Audio Controller will be unconditionally disabled. Enabled = Audio Controller will be unconditionally Enabled.

► 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.

Advanced		
Network Stack	[Disabled]	Enable/Disable UEFI Network Stack

► Network Stack

This menu provides Network Stack settings for users to enable network boot (PXE) from BIOS. The following items will display when **Network Stack** 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

Advanced		
GP00	[Low]	Set GP00 to output High/Low
GP01	[Low]	
GP02	[Low]	
GP03	[Low]	
GP04	[Low]	
GP05	[Low]	
GP06	[Low]	
GP07	[Low]	

► GPO0 ~ GPO7

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.

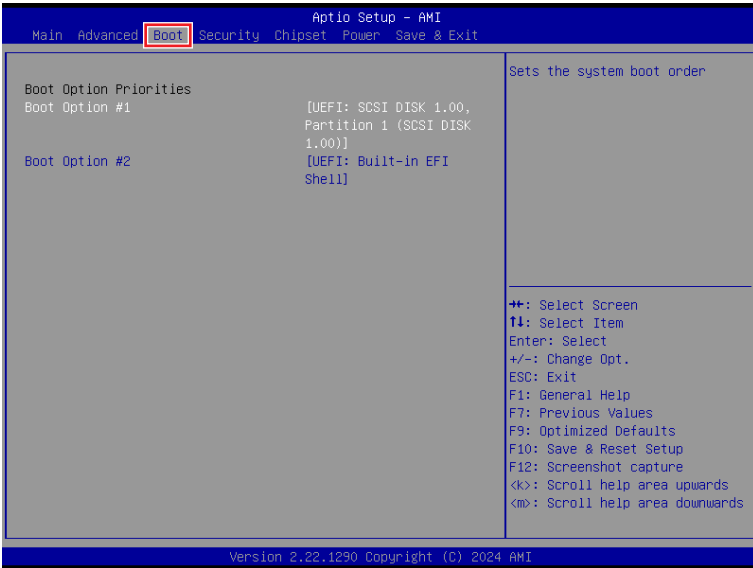
Advanced		
M2_B1	[Disabled]	PCI Express Active State Power Management settings.
M2_E1	[Disabled]	
M2_M1	[Disabled]	

► M2_B1/ M2_E1/ M2_M1

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.

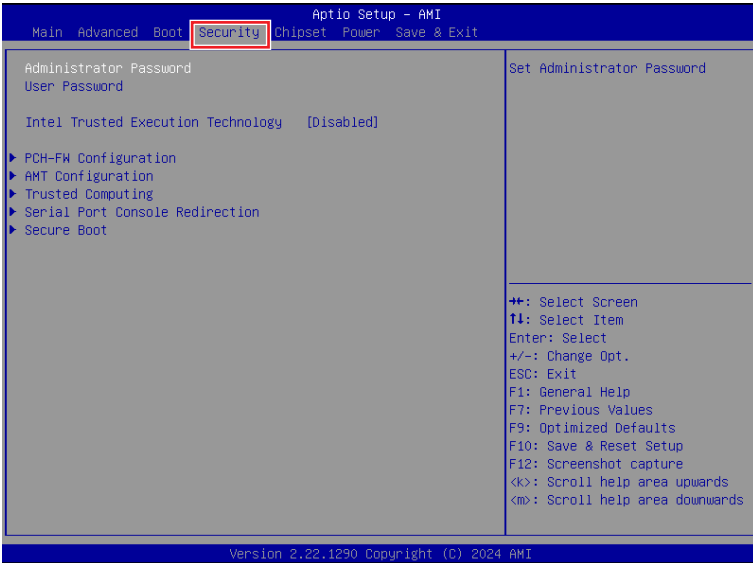
Boot



► Boot Option #1-2

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

Security



▶ Administrator Password

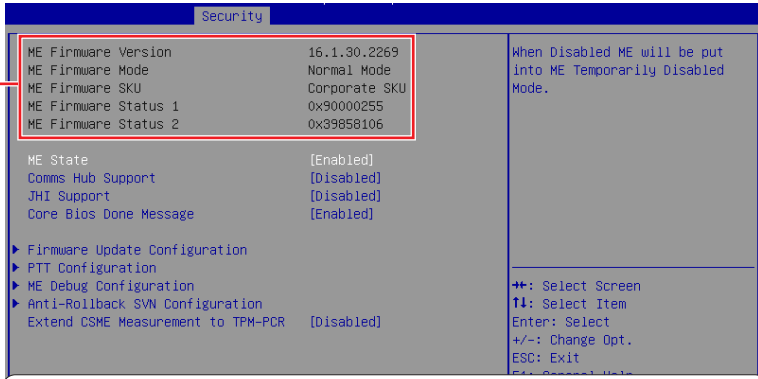
Administrator Password controls access to the BIOS Setup utility.

▶ 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.



The screenshot shows the BIOS Security menu with the following settings:

ME Firmware Version	16.1.30.2269	When Disabled ME will be put into ME Temporarily Disabled Mode.
ME Firmware Mode	Normal Mode	
ME Firmware SKU	Corporate SKU	
ME Firmware Status 1	0x9000255	
ME Firmware Status 2	0x39858106	
ME State	[Enabled]	++: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: Screen Help
Comms Hub Support	[Disabled]	
JHI Support	[Disabled]	
Core Bios Done Message	[Enabled]	
► Firmware Update Configuration		
► PTT Configuration		
► ME Debug Configuration		
► Anti-Rollback SVN Configuration		
Extend CSME Measurement to TPM-PCR	[Disabled]	
Firmware Information		

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.

► 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.

► **Firmware Update Configuration**

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

Security		
Me FW Image Re-Flash	[Disabled]	Enable/Disable Me FW Image
Local FW Update	[Enabled]	Re-Flash function.

» **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.

Security		
PTT Capability / State	1 / 0	Selects TPM device: PTT or dTPM. PTT - Enables PTT in SkuMgr dTPM 1.2 - Disables PTT in SkuMgr Warning ! PTT/dTPM will be disabled and all data saved on it will be lost.
TPM Device Selection	[dTPM]	

» **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.

Security		
HECI Timeouts	[Enabled]	Enable/Disable HECI Send/Receive Timeouts.
Force ME DID Init Status	[Disabled]	
CPU Replaced Polling Disable	[Disabled]	
HECI Message check Disable	[Disabled]	
MBP HOB Skip	[Disabled]	
HECI2 Interface Communication	[Disabled]	
KT Device	[Enabled]	
End Of Post Message	[Send in DXE]	
DOI3 Setting for HECI Disable	[Disabled]	
MCTP Broadcast Cycle	[Disabled]	

» **HECI Timeouts**

This setting enables/ 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**

Enables or disables End of Post Message sent to ME.

» **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**

Security		
Minimal Allowed Anti-Rollback SVN	0	When enabled,
Executing Anti-Rollback SVN	1	hardware-enforced
Automatic HW-Enforced	[Disabled]	Anti-Rollback mechanism is
Anti-Rollback SVN		automatically activated: once
Set HW-Enforced Anti-Rollback for	[Disabled]	ME FW was successfully run on
Current SVN		a platform, FW with lower
		ARB-SVN will be blocked from
		execution

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

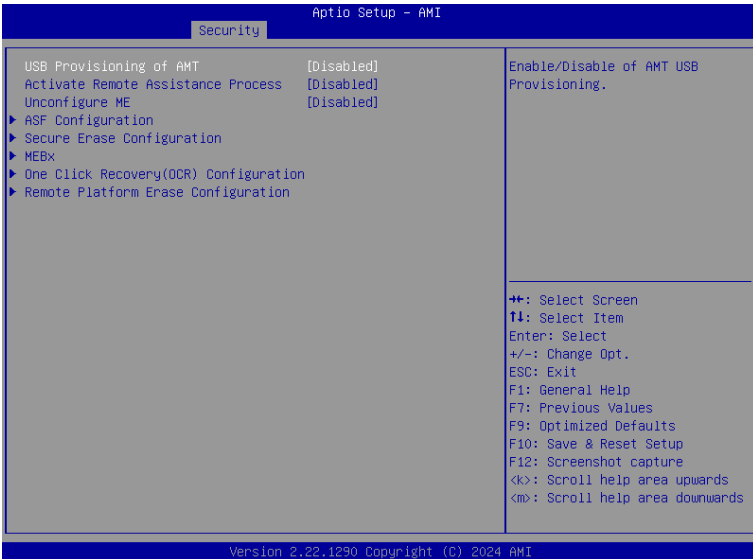
Setting this item enables will automatically activate the hardware-enforced anti-rollback protection based on the Secure Version Number (SVN). Once enabled, the hardware will enforce that only firmware updates with an SVN equal to or higher than the current SVN can be installed.

» **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**

Security		
PET Progress	[Enabled]	Enable/Disable PET Events Progress to receive PET Events.
WatchDog	[Disabled]	
OS Timer	0	
BIOS Timer	0	
ASF Sensors Table	[Disabled]	

» **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**

Security		
Secure Erase mode	[Simulated]	Change Secure Erase module behavior: Simulated: Performs SE flow without erasing SSD Real: Erase SSD. *** If SATA device is used, DEM could use SECURE_ERASE_HOOK_PROTOCOL to remove SATA power to skip G3 cycle. ***
Force Secure Erase	[Disabled]	

» **Secure Erase Mode**

This setting change Secure Erase module behavior.

[Simulated] Performs SE flow without erasing SSD.

[Real] Erase SSD.

» **Force Secure Erase**

Enables or disables to force Secure Erase on next boot.

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

Security	
Intel(R) ME Password	MEBx Login

► One Click Recovery (OCR) Configuration

Security		
OCR Https Boot	[Enabled]	Enable/Disable One Click Recovery Https Boot
OCR PBA Boot	[Enabled]	
OCR Windows Recovery Boot	[Enabled]	
OCR Disable Secure Boot	[Enabled]	

» 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.

Security		
Enable Remote Platform Erase Feature	[Enabled]	Enable/Disable Remote Platform Erase Feature
SSD Erase Mode	[Simulated]	

» 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		
TPM 2.0 Device Found		Enables or Disables BIOS support for security device. O.S. will not show Security Device, TCG EFI protocol and INT1A interface will not be available.
Firmware Version:	15.23	
Vendor:	IFX	
Security Device Support	[Enable]	
Active PCR banks	SHA256	
Available PCR banks	SHA256,SHA384	
SHA256 PCR Bank	[Enabled]	
SHA384 PCR Bank	[Disabled]	
Pending operation	[None]	
Platform Hierarchy	[Enabled]	
Storage Hierarchy	[Enabled]	
Endorsement Hierarchy	[Enabled]	
Physical Presence Spec Version	[1.3]	
TPM 2.0 InterfaceType	[TIS]	
PH Randomization	[Enabled]	
Device Select	[TPM 2.0]	
		++: Select Screen T4: Select Item Enter: Select +/-: Change Opt. ESC: Exit F1: General Help F7: Previous Values F9: Optimized Defaults F10: Save & Reset Setup F12: Screenshot capture < >: Scroll help area upwards < m >: Scroll help area downwards

► 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.

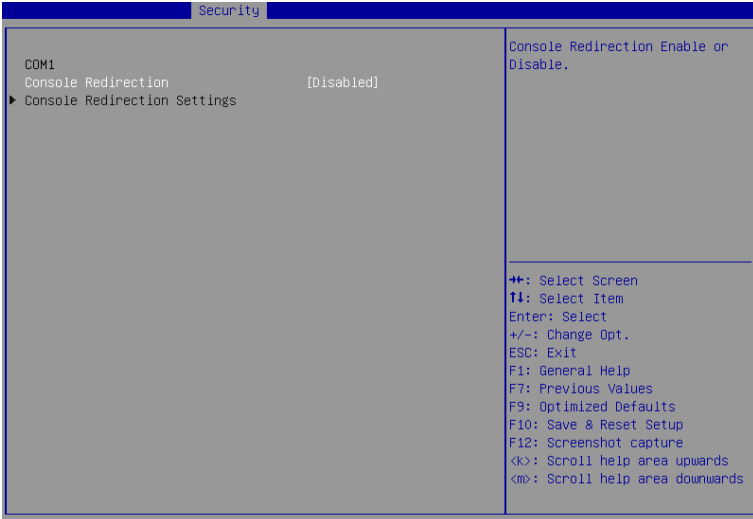
► PH Randomization

Enables or disables Platform Hierarchy (PH) Randomization.

► Device Select

Select your TPM device through this setting.

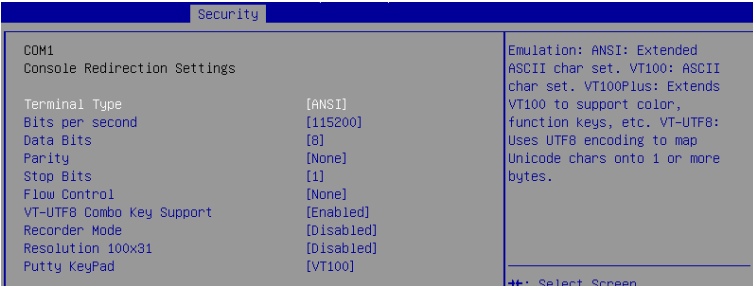
► Serial Port Console Redirection



► 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.

[VT100+] 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.

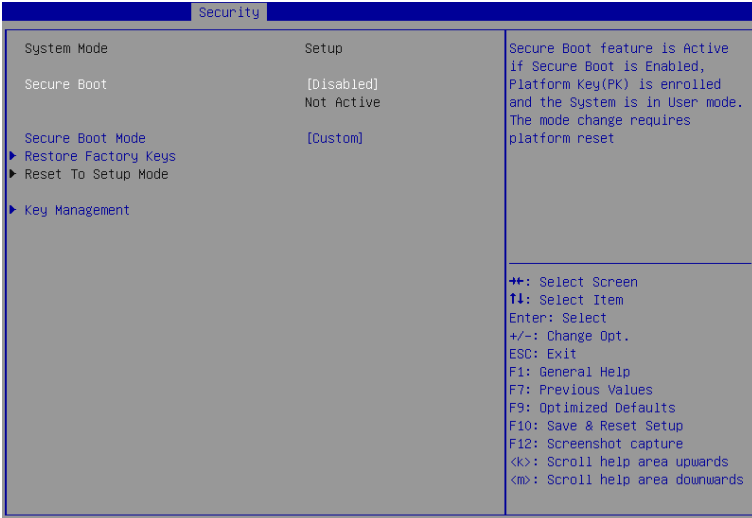
» **Recorder Mode, Resolution 100x31**

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

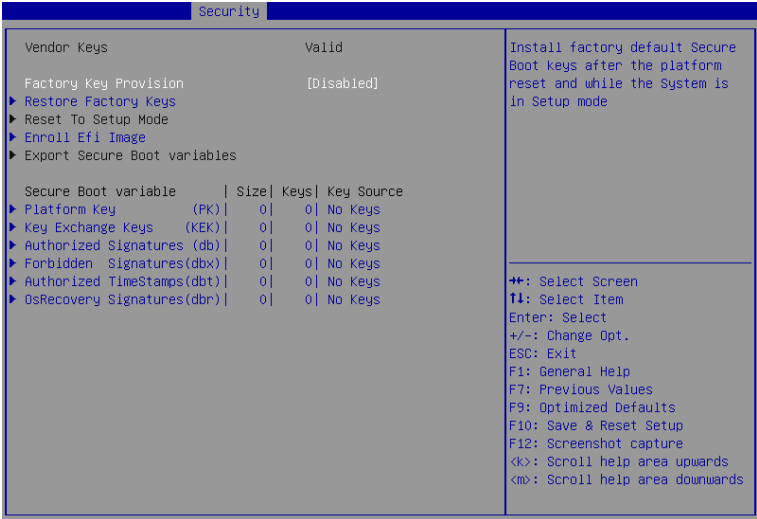
Allows you to restore all factory default keys. The settings will be applied after reboot or at the next reboot. This item appears when "**Secure Boot Mode**" sets to [Custom].

► 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) :**

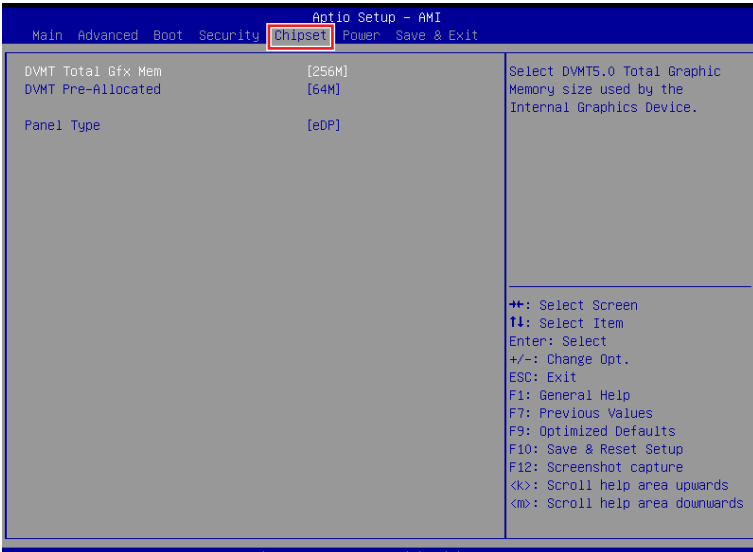
Authorized Signatures (db) lists the signatures that can be loaded.

» **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.

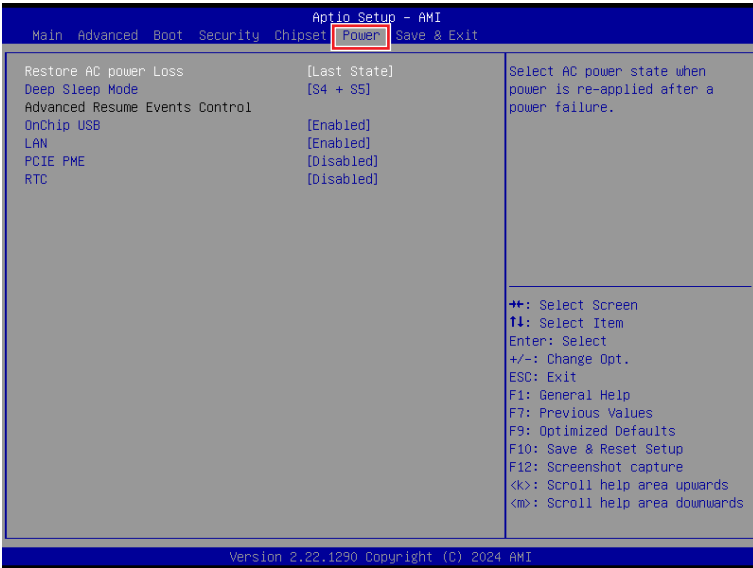
Chipset



► 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.

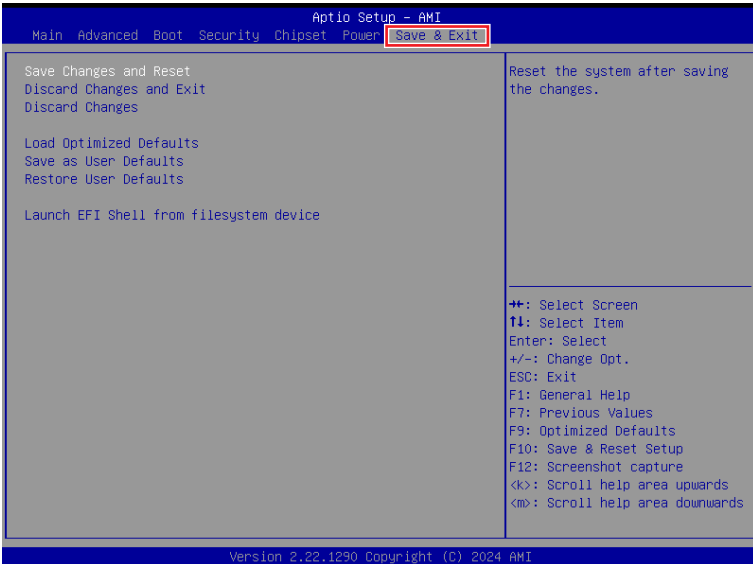
► **LAN/ PCIE PME**

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], you 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 SMBus Programming

This chapter provides WDT (Watch Dog Timer), GPIO (General Purpose Input/ Output) and SMBus Access 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_GPIO0	0x22	Bit 4	N_GPO0	0x11	Bit 4
N_GPIO1	0x22	Bit 5	N_GPO1	0x11	Bit 5
N_GPIO2	0x22	Bit 6	N_GPO2	0x11	Bit 6
N_GPIO3	0x22	Bit7	N_GPO3	0x11	Bit 7
N_GPIO4	0x42	Bit 0	N_GPO4	0x21	Bit 0
N_GPIO5	0x42	Bit 1	N_GPO5	0x21	Bit 1
N_GPIO6	0x42	Bit 2	N_GPO6	0x21	Bit 2
N_GPIO7	0x42	Bit 3	N_GPO7	0x21	Bit 3

Note: GPIO should be accessed through controller device **0x6E** on SMBus. The associated access method in examples (**SMBus_ReadByte**, **SMBus_WriteByte**) are provided in part 3.

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 =SMBus_ReadByte (0x6E, 0x11); // Read value from N_GPO0 port through SMBus.  
val = val | (1<<4); // Set N_GPO0address (bit 4) to 1 (output “high”).  
SMBus_WriteByte (0x6E, 0x11, val); // Write back to N_GPO0 port through SMBus.
```

Example: Set **N_GPO1** output “low”

```
val = SMBus_ReadByte (0x6E, 0x11); // Read value from N_GPO1 port through SMBus..  
val = val & ~(1<<5); // Set N_GPO1 address (bit 5) to 0 (output “low”).  
SMBus_WriteByte (0x6E, 0x11, val); // Write back to N_GPO1 port through SMBus.
```


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 = SMBus_ReadByte (0x6E, 0x22); // Read value from N_GPI2 port through SMBus.  
val = val & (1<<6);                // Read N_GPI2 address (bit 6).  
if (val) printf ("Input of N_GPI2 is High");  
else     printf ("Input of N_GPI2 is Low");
```

Example: Get **N_GPI3** input value.

```
val = SMBus_ReadByte (0x6E, 0x22); // Read value from N_GPI3 port through SMBus.  
val = val & (1<<7);                // Read N_GPI3 address (bit 7).  
if (val) printf ("Input of N_GPI3 is High");  
else     printf ("Input of N_GPI3 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
```

SMBus Access

3. SMBus Access

The base address of SMBus must know before access. The relevant bus and device information are as following.

```
#define IO_SC          0xCF8
#define IO_DA          0xCFC
#define PCIBASEADDRESS 0x80000000
#define PCI_BUS_NUM    0
#define PCI_DEV_NUM    31
#define PCI_FUN_NUM    4
```

3.1 Get SMBus Base Address

```
int SMBUS_BASE;
int DATA_ADDR = PCIBASEADDRESS + (PCI_BUS_NUM<<16) +
                (PCI_DEV_NUM<<11) +
                (PCI_FUN_NUM<<8);

Outputl (DATA_ADDR + 0x20, IO_SC);
SMBUS_BASE = Inportl (IO_DA) & 0xfffff0;
```

3.2 SMBus_ReadByte (char DEVID, char offset)

Read the value of OFFSET from SMBus device DEVID.

```
Outputb (LOWORD (SMBUS_BASE), 0xFE);
Outputb (LOWORD (SMBUS_BASE) + 0x04, DEVID + 1); //out Base + 04, (DEVID + 1)
Outputb (LOWORD (SMBUS_BASE) + 0x03, OFFSET); //out Base + 03, OFFSET
Outputb (LOWORD (SMBUS_BASE) + 0x02, 0x48); //out Base + 02, 48H
mdelay (20); //delay 20ms to let data ready
while ((Inportl (SMBUS_BASE) & 0x01) != 0); //wait SMBus ready
SMB_DATA = Inportb (LOWORD (SMBUS_BASE) + 0x05); //input Base + 05
```

3.3 SMBus_WriteByte (char DEVID, char offset, char DATA)

Write DATA to OFFSET on SMBus device DEVID.

```
Outputb (LOWORD (SMBUS_BASE), 0xFE);
Outputb (LOWORD (SMBUS_BASE) + 0x04, DEVID); //out Base + 04, (DEVID)
Outputb (LOWORD (SMBUS_BASE) + 0x03, OFFSET); //out Base + 03, OFFSET
Outputb (LOWORD (SMBUS_BASE) + 0x05, DATA); //out Base + 05, DATA
Outputb (LOWORD (SMBUS_BASE) + 0x02, 0x48); //out Base + 02, 48H
mdelay (20); //wait 20ms
```