ROC300-TA45

3U GPGPU short Depth Edge Computing Server

User Manual

- Intel® Xeon Silver Ice Lake 4310 12 Cores 2.1/3.3 GHz, 120W, 18MB cache
- Dual Nvidia MXM RTX A4500 5888 CUDA cores PCIe Gen 4.0 x16
- Two Ethernet LAN ports (LAN1, LAN2) and a dedicated IPMI LAN
- 4x NVMe M.2 (Gen4 x4)
- Equipped with latest tool less design, storage, HDD trays, system fa ns and PCIe riser brackets for easy upgrades and maintenance.
- Size: 450.0 x 450.0 x 131.0 mm.
- 4x 80mm Fan, 11000RPM
- Redundant 2U 1600W 1+1 CRPS

Contents/目錄

1 Chapter1 : General Information..

1.1 Introduction...

ROC300-TA45 is an efficient 3U rackmount workstation designed with the most advanced NVIDIA Quadro RTX (A4500) professional GPU, specifically designed for the most demanding workflows of today. Experience GPU acceleration performance through innovative computers and mobile devices that combine real-time ray tracing, programmable shading technology, and artificial intelligence. ROC300-TA45 adopts the latest industrial design, providing users with high-performance and cutting-edge operating platforms. This machine supports EATX/ATX/MicroATX motherboards, with efficient power switching and easy maintenance of fans. ROC300-TA45 provides 6 SAS/SATA HDD Hot-Swap drive bays and 4 built-in M.2 SSD, providing a flexible solution for data storage. The high-performance series can support up to 1600W power supply and has excellent heat dissipation capacity to support up to two A4500 GPU cards and extra two acceleration cards. In addition, the system fan can increase or decrease speed based on the temperature inside the chassis to effectively reduce noise under low system loads. A wide range of standard computing peripherals can be integrated with these chassis to accommodate robust applications in rugged environments, 24 hours a day, 7 days a week.

1.2 Specifications…

Model Name	ROC300-TA45
Form Factor	EATX/ ATX/ Micro ATX
CPU	Intel Xeon Silver Ice Lake 4310 with Fansink
Chipset	C621A
Memory	DDR4 256GB (4x 64GB)
Display	1x VGA (AST2500)
GPU	2x NVIDIA MXM A4500 with Fansink
Storage	2x M.2 2TB NVMe
Front I/O	
Indicators	1x Power Status; 2x LAN activity, 1x UID, 1x HDD Status; 1x System Alarm
Front Control	1x Power On/Offf; 1x System Reset; 1x UID; 1x USB3.0
Drive Bay	6x SAS/SATA Hot-swap bay
Cooling Fan	4x 80x80 mm, 11000RPM, Hot-swap
Rear I/O	
LAN	1x LAN1 : 1GbE ; 1x LAN2 : 10GbE
Net Work	1x IPMI (AST2500)
Display	1x VGA (AST2500)
Serial	4x USB3.2; 2x USB2.0; 1x Type C (USB3.2)
COM	1x COM
Audio	1x Lin/out; 1x Mic in; 1x Center/LFE out; 1x Surround out
S/PDIF	1x out
PSU Form Factor	2U 1600W 1+1 CRPS
Expansion	
PCIe Slot opening	2x MXM Carrier Card; 2x Opening slot for U55C
Dimension (D x W x H)	450.0 x 450.0 x 131.0 mm

1.3 Power Supply Options...

1.3.1 Features

1.3.1.1 A High Reliability PDB(power distribution board)

1.3.1.2 CRPS Module Compatible

1.3.1.3 2U Narrow Form Factor

1.3.1.4 Meet PMBus 1.2

1.3.1.5 Design for 5,000 Meter above Sea level

1.3.1.6 High Reliability

1.3.1.7 Low Ripple & Noise

1.3.1.8 Over Current Protection

1.3.1.9 Over Temperature Protection

1.3.1.10 Over Voltage Protection

1.3.2 Genernal Specification

GENERNAL SPECIFICATION	
Dimension	210 x 76 x 83.8 mm(Lx W x H)
Hold-up Time at 100%	12V = 11ms
Operating Altitude	5,000 meters above Sea level
Environment	
Working Temperature	0℃to 55℃
Storage Temperature	-40℃ to +70℃
Working Humidity	5% to 90% RH non-condensing
Storage Humidity	5% to 95% RH non-condensing
MTBF	500,000 hours of continuous operation at 55℃, 100% output load.

1.3.3 Table 1.1:Power supply output rating

Output power	Input Voltage	Current Range	DC Outputs				
			+3.3V	+5V	+12V	-12V	+5VSB
1600W	100-240VAC (1000W)	Max. Current	12A	24A	80.5A	0.3A	5A
		Combined Power	972W			3.6W	25W
	200-240VAC (1600W)	Max. Current	12A	24A	130.3A	0.3A	5A
		Combined Power	1572W			3.6W	25W

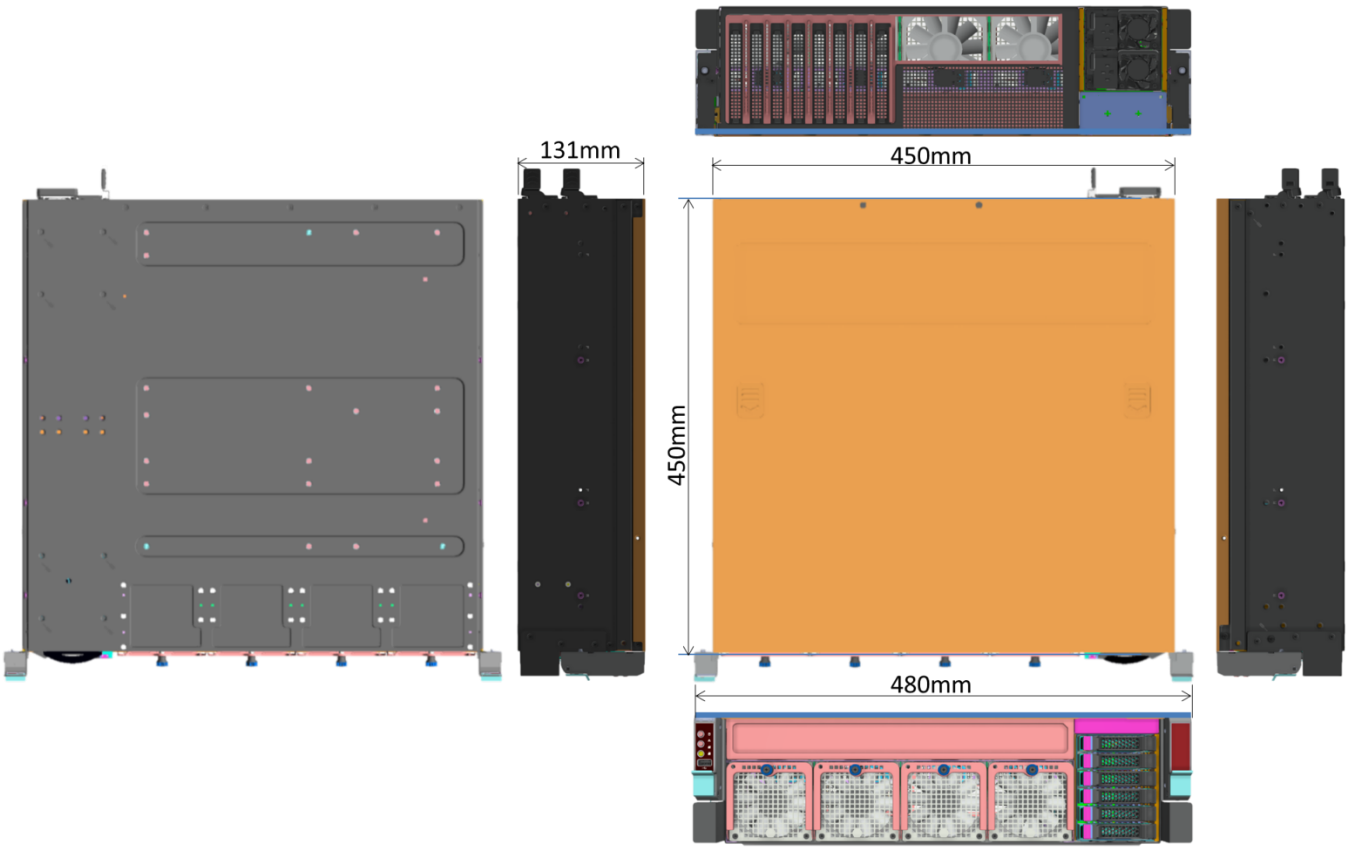
1.4 Environmental Specifications…

1.4.1 Table1.2 list

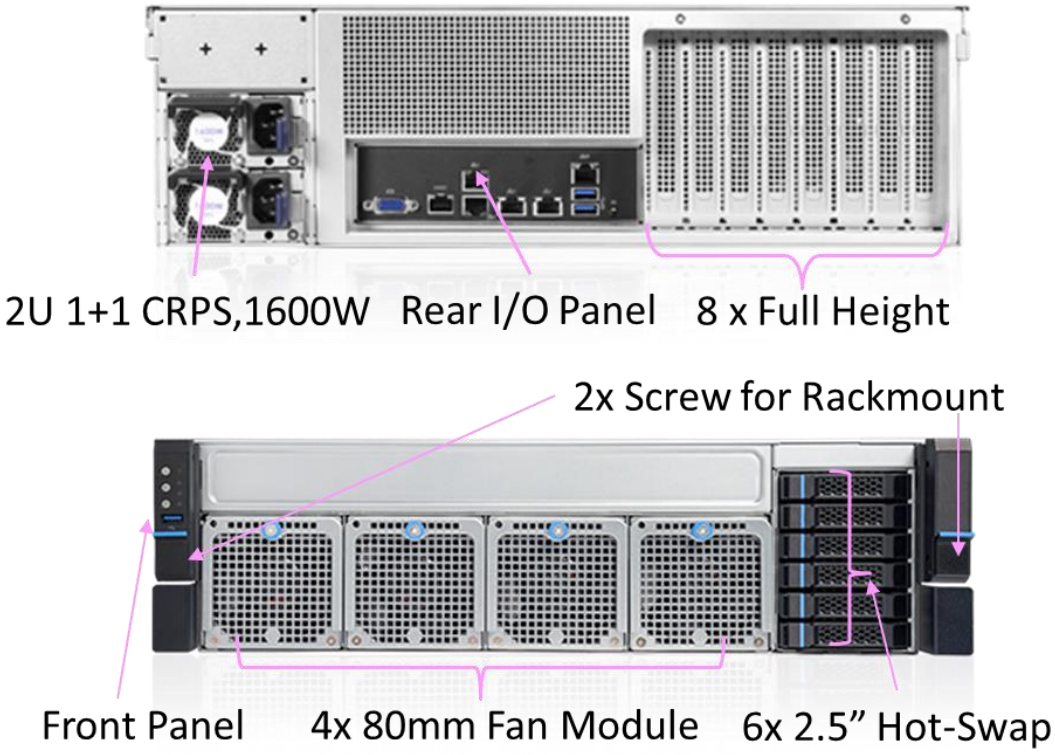
Table 1.2: Environment specifications/ 环境规格 / 環境規格

Environment 环境 環境	Operating 工作	Non-operating 非工作
Temperature 温度 溫度	0 ~ 40° C (32 ~ 104° F)	--40 ~ 70° C (-40 ~ 158° F)
Humidity 湿度 濕度	10 ~ 95% @ 40° C, non-condensing	10 ~ 95% @ 60° C, non-condensing
Vibration (5 ~ 500Hz) 振动 振動	1G rms	2 G
Shock 冲击 衝擊	10 G with 11 ms duration, half sine wave	
Safety 安规认证 安規認證	CE compliant	

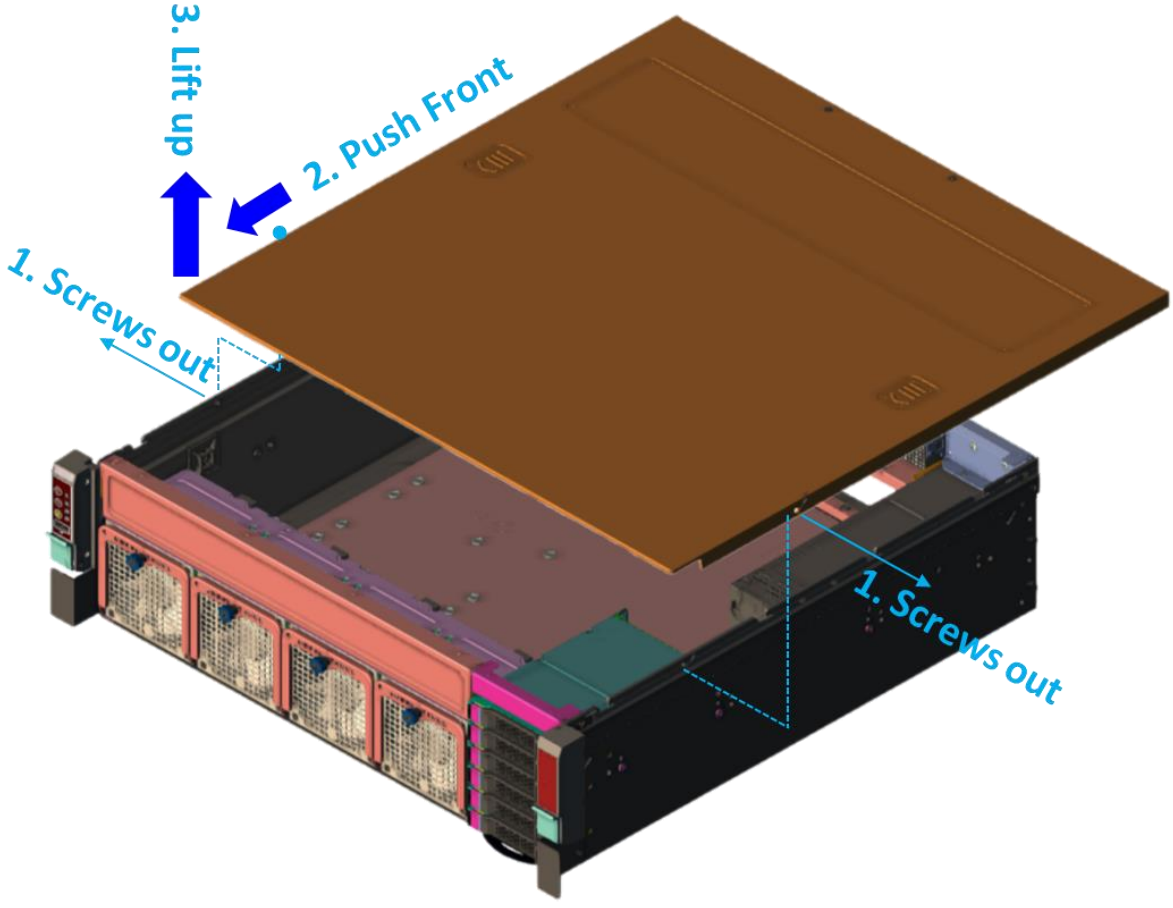
1.4.2 Dimension Diagram



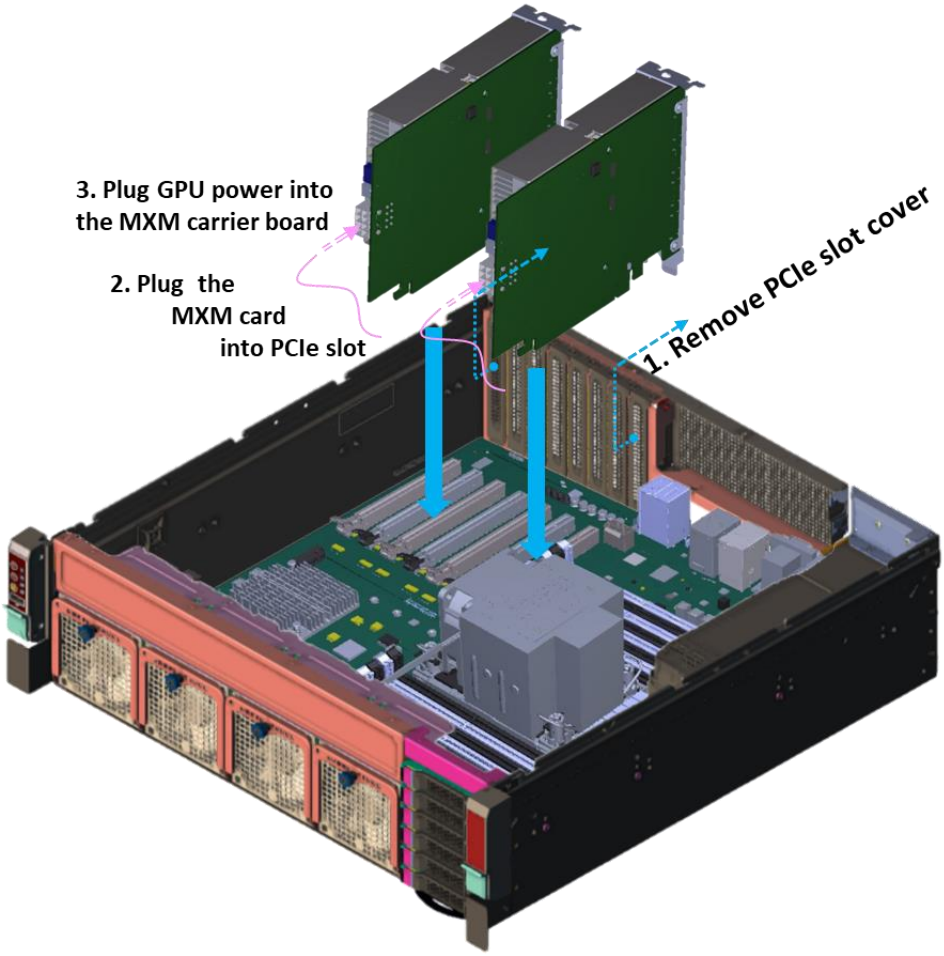
1.4.3 Feature Overview



1.5 Removing the Top Cover...



1.6 Installing the GPU Card…

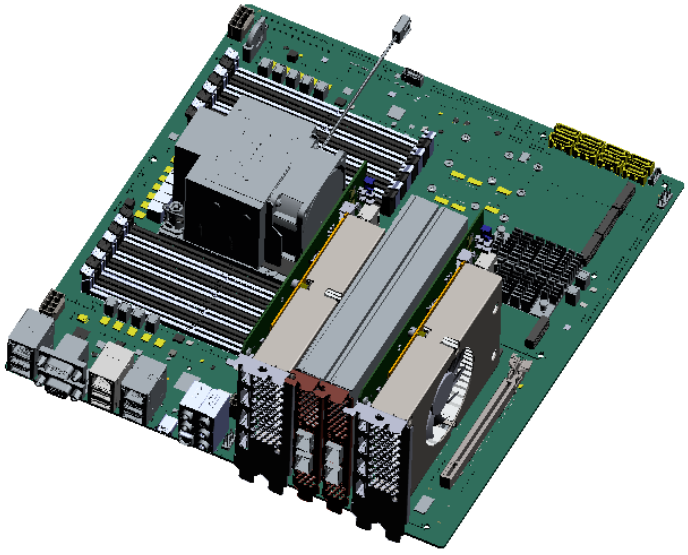


1.6.1 Remove the PCIe slot cover

1.6.2 Plug the MXM carrier card with MXM GPU card into the PCIe slot3 (then 7 for 2nd MXM card)

1.6.3 Plug GPU power into the MXM carrier board

⁎Suggest to install extra accelerated card at Slot 4 &5.



1.7 Installing Disk Drives…

1.7.1 Installing SSD in the Mobile SSD tray

Figure 2.5Removing the mobile SAS / SATA HDD trays

1. Press the tray button and release the lever as shown.
2. Pull the SSD assembly out of the drive bay.

1. With the open latch, insert the SSD assembly into the drive bay until the end of the SSD cage.
2. Push in the lever when it is secured with a click.

1.7.2 Installing the SSD

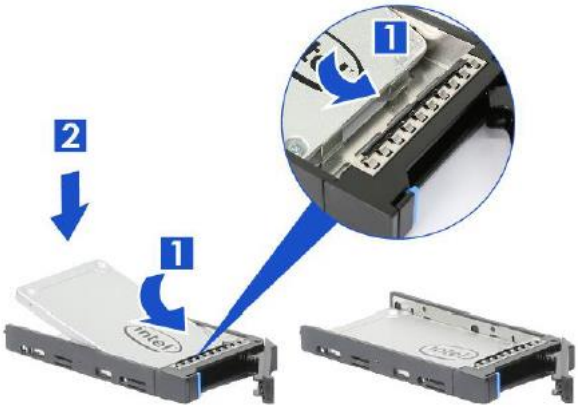


Figure 2.6 2.5”SSD installation (tool-less type)

1. Slide in the SSD until align the anchor points of SSD tray.
2. Push down the SSD when it is secured with a click.

1.8 PSU Installation and Removal…

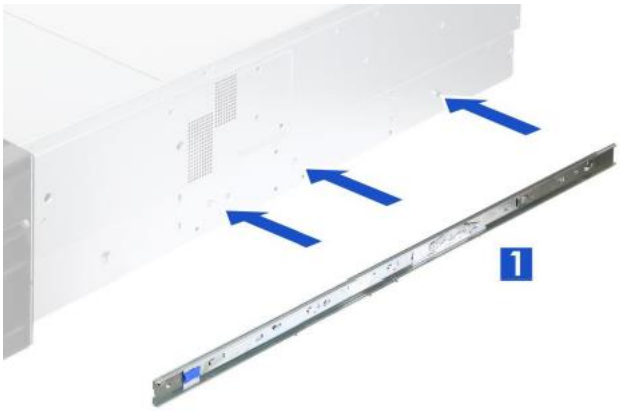
1.8.1 CRPS module installation

1. Insert CRPS module into the PSU cage and push until it is secured into place.

1.8.2 CRPS module removal

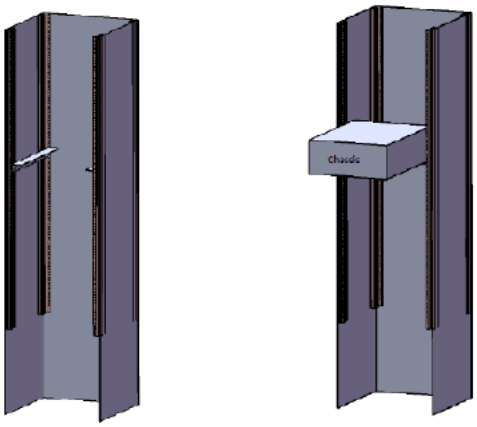
1. Press the latch without release as shown.
2. Pull the module handle to remove it from the PSU cage.

1.9 Slide Rail or Pallet…



1. Attach the inner rail to the chassis base while aligning T-pins on the side of the system with the slots on the inner rail.

2. Engage T-pins with the slots on the inner rail as shown.
3. Secure the inner rail with one screw.



Install the chassis in the cabinet with the slide rail or pallet supplied /

2 Chapter2 : Operation..

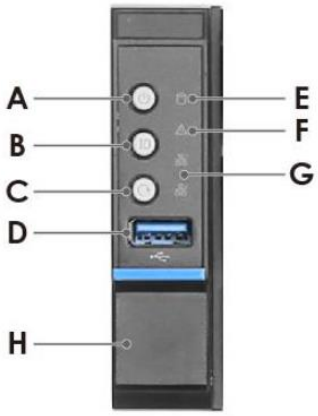
2.1 The Front Panel…

(Overview)

2.1.1 Switch, Buttons and I/O Interfaces.

2.1.2 LED indicators for System Status

2.1.3 LED Indicators for SSD Power & Status

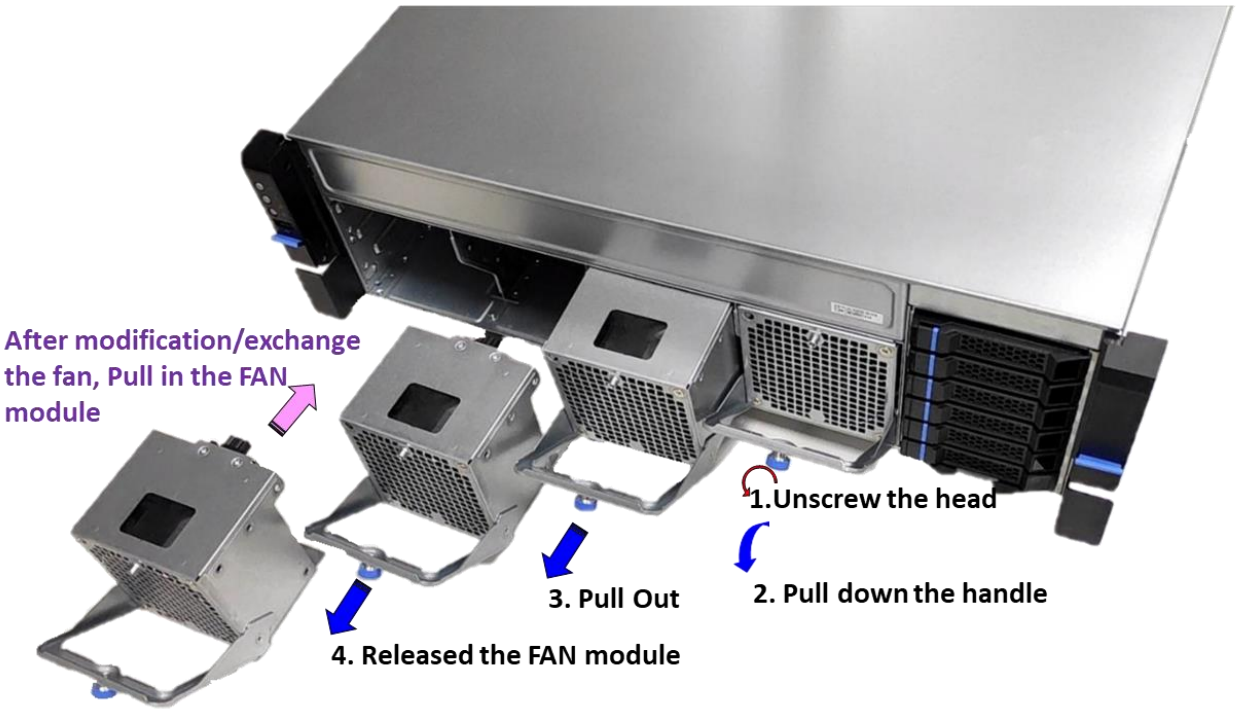


Label	ICON	Indicator, button or connector
A	⏻	Power Button
B	ID	UID Button
C	↻	Reset Button
D	⇐	USB3.0
E	⛁	HDD Activity LED
F	⚠	System Alarm LED
G	品	LAN1, LAN2 Activity LED
H		Rack Handle (Left)
I		Rack Handle (Right)

2.2 The Rear Panel…

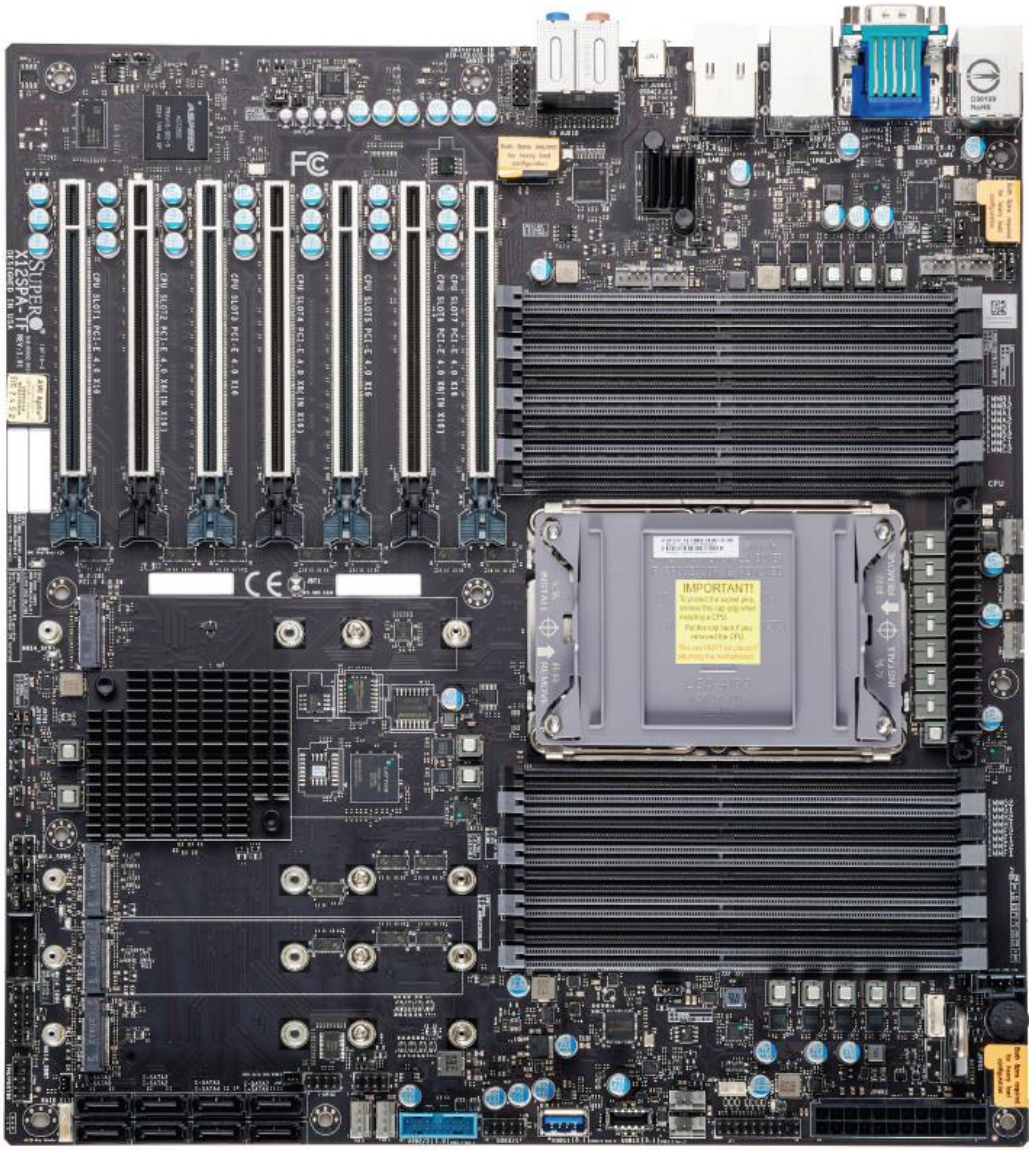
2.2.1 Plug the AC power with standard IEC power cable
2.2.2 Plug the cable into the I/O jack by the Device
2.2.3 Broke the cover to install function card into PCIe slot

2.3 Replacing the system Cooling Fan…

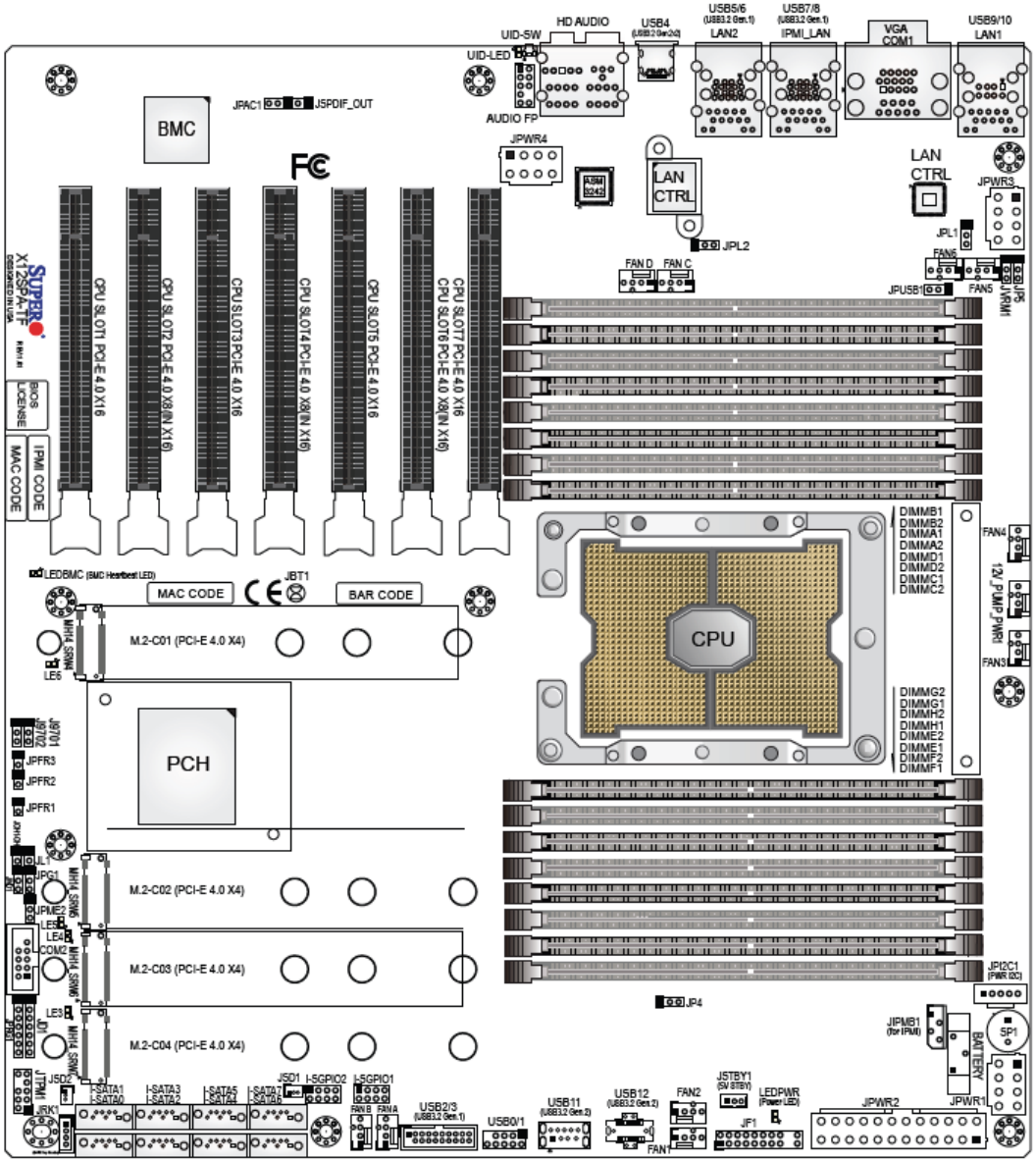


3 Chapter 3 : Motherboard Overview

3.1 Motherboard Image…



3.2 Motherboard Layout…



✳Notes:

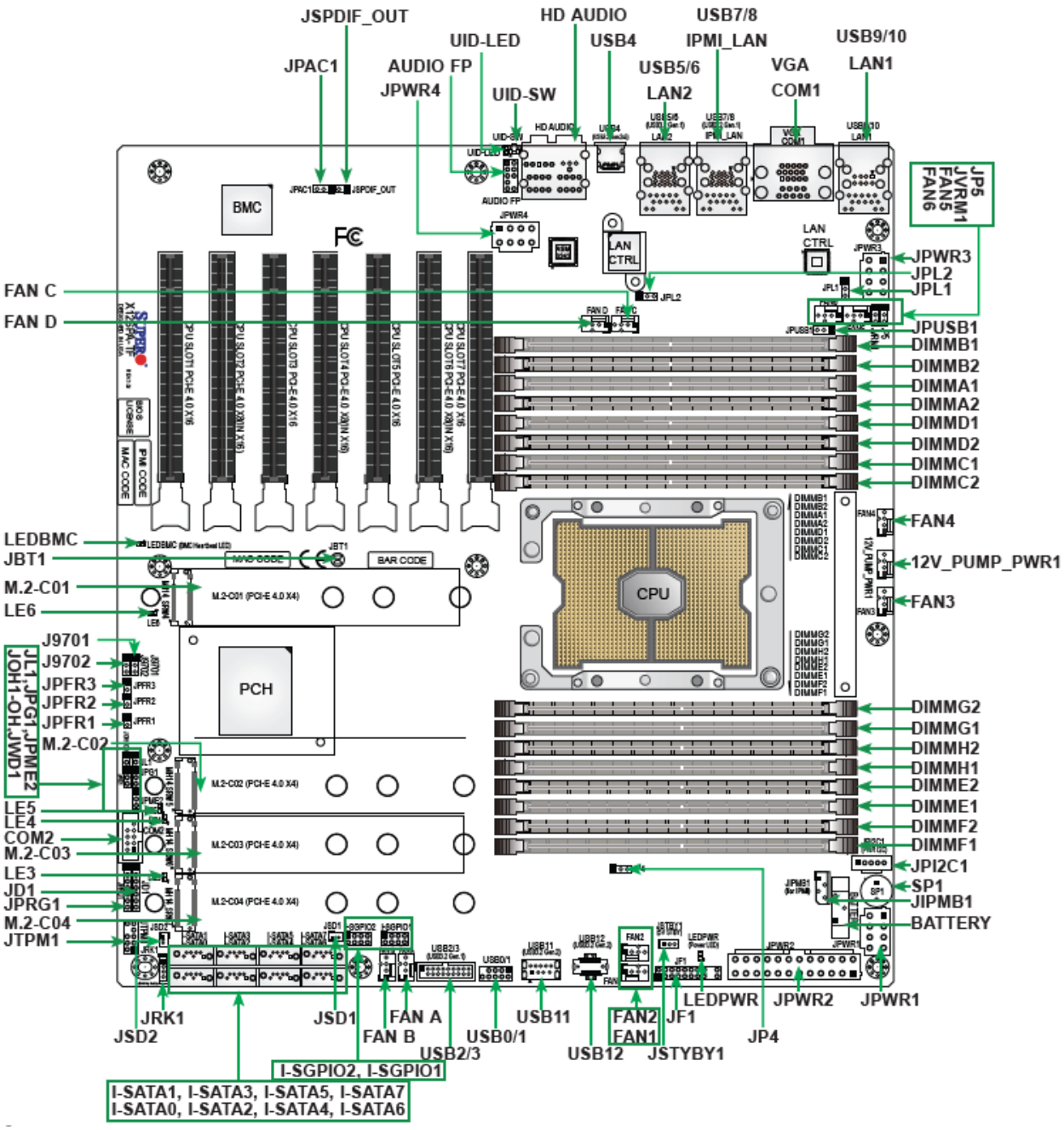
CPU SLOT1/3/5/7 : PCIe 4.0 x16 Slots

** SLOT1 will be disabled when either M.2-C01 or M.2-C02 is in use.*

** SLOT1 will change to PCIe x8 when M.2-C03 or/and M.2-C04 are in use.*

** SLOT3/5/7 will change to PCIe x8 when SLOT2/4/6 is in use respectively.*

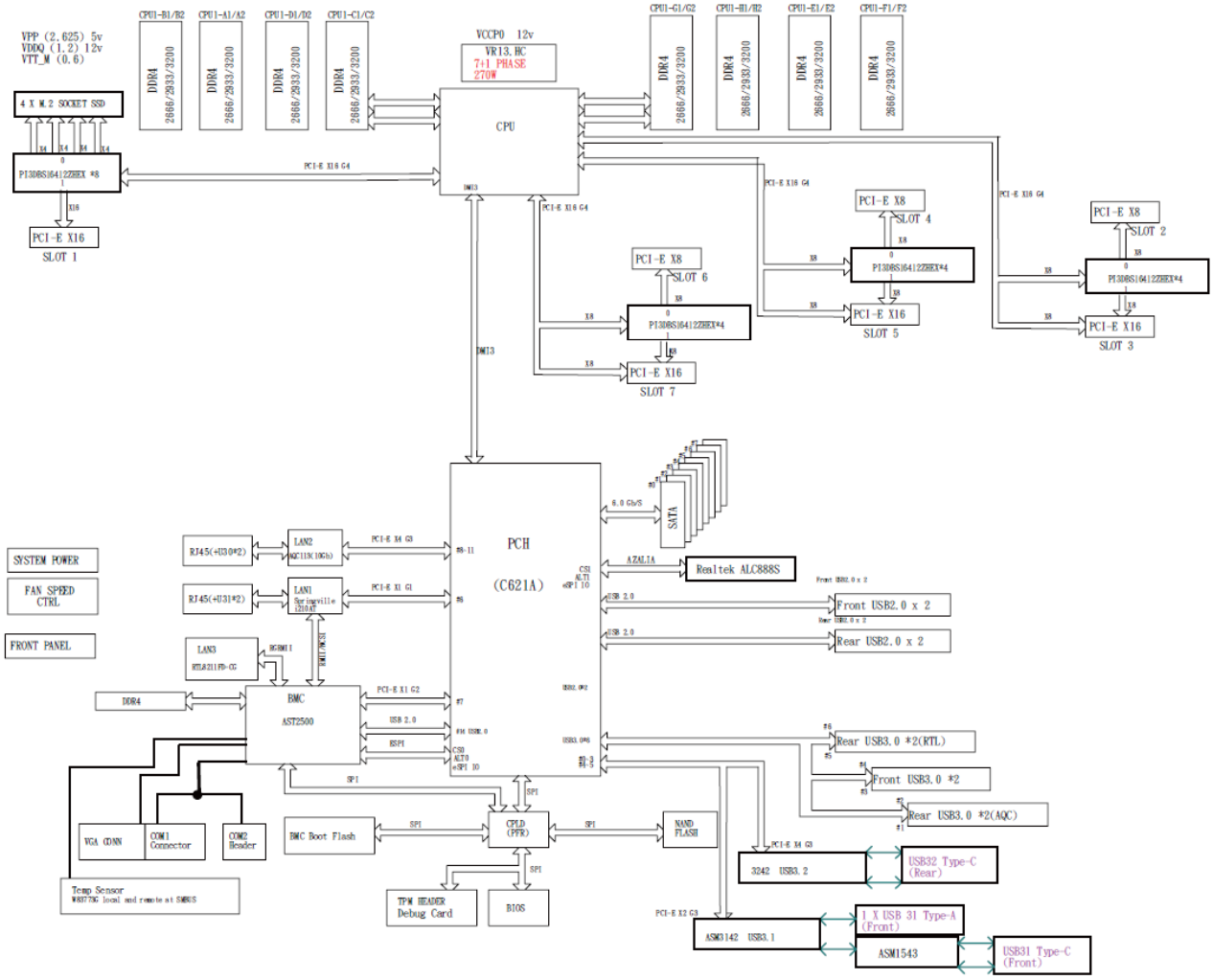
CPU SLOT2/4/6 : PCIe 4.0 x16 Slots (PCIe 4.0 x8 link)



Notes:

- See Chapter 2 for detailed information on jumpers, I/O ports, and JF1 front panel connections.
- " " indicates the location of Pin 1.
- Jumpers/LED indicators not indicated are used for testing only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. Do not install the onboard battery upside down to avoid possible explosion.

3.3 System Diagram…



3.4 Memory Support and Installation…

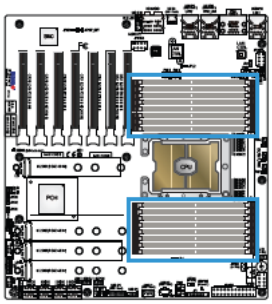
Memory supports up to 1 TB of ECC RDIMM, 4 TB of 3DS RDIMM, 2 TB of LRDIMM, 4 TB of 3DS LRDIMM, and 4 TB of Intel Optane Persistent Memory (PMem) 200 Series with speeds of up to 3200 MHz (2DPC) in 16 DDR4 (288-pin) SMD DIMM slots.

Note 1: Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.

Note 2: Memory speed support depends on the processors used in the system.

DDR4 Memory Support

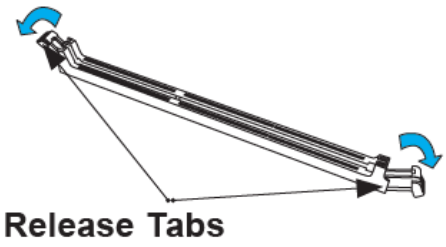
DDR4 Memory Support					
Type	Ranks Per DIMM & Data Width	DIMM Capacity (GB)		Speed (MT/s); Voltage (V); Slots Per Channel (SPC) and DIMMs Per Channel (DPC)	
				1DPC (1-DIMM Per Channel)	2DPC (2-DIMM Per Channel)
		8Gb	16Gb	1.2 V	1.2 V
RDIMM	SRx8	8GB	16GB	3200	3200
	SRx4	16GB	32GB		
	DRx8	16GB	32GB		
	DRx4	32GB	64GB		
RDIMM 3Ds	(4R/8R) X4	2H- 64 GB 4H-128 GB	2H- 128 GB 4H-256 GB		
LRDIMM	QRx4	64GB	128GB	3200	3200
LRDIMM - 3Ds	(4R/8R) X4	4H-128 GB	2H- 128 GB 4H-256 GB	3200	3200



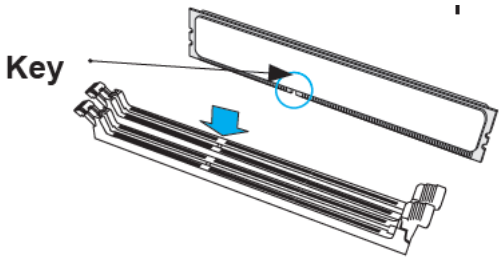
3.4.1 DIMM Installation

- Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population tables in the previous section. Locate DIMM memory slots on the motherboard as shown on the right.

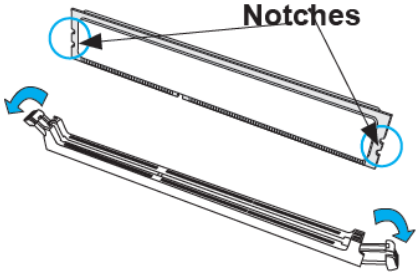
- Push the release tabs outwards on both ends of the DIMM slot to unlock it.



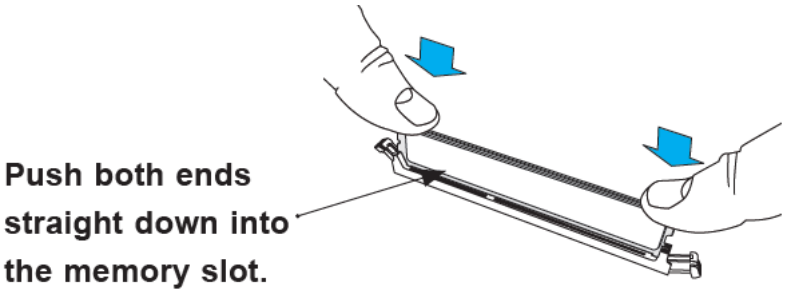
- Align the key of the DIMM module with the receptive point on the memory slot.



- Align the notches on both ends of the module against the receptive points on the ends of the slot.

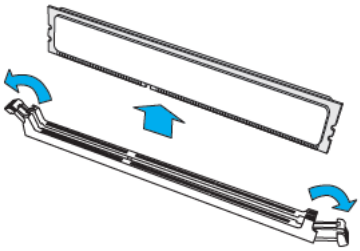


- Push both ends of the module straight down into the slot until the module snaps into place.
- Press the release tabs to the lock positions to secure the DIMM module into the slot.



3.4.2 DIMM Removal

- Press both release tabs on the ends of the DIMM module to unlock it. Once the DIMM module is loosened, remove it from the memory slot.



Warning! Please do not use excessive force when pressing the release tabs on the ends of the DIMM socket to avoid causing any damage to the DIMM module or the DIMM socket. Please handle DIMM modules with care. Carefully follow all the instructions given on Page 1 of this chapter to avoid ESD-related damages done to your memory modules or components.

3.4.3 Rear I/O Ports

Rear I/O Ports							
#	Description	#	Description	#	Description	#	Description
1	LAN1 (1Gb)	6	Dedicated IPMI LAN	11	USB6 (3.2 Gen. 1)	16	Line In
2	USB9 (2.0)	7	USB7 (3.2 Gen. 1)	12	USB4 (3.2 Gen. 2x2)	17	Line Out
3	USB10 (2.0)	8	USB8 (3.2 Gen. 1)	13	Center/LFE Out	18	Mic In
4	COM1 Port	9	LAN2 (10Gb)	14	Surround Out	19	UID Switch / BMC Reset Button
5	VGA Port	10	USB5 (3.2 Gen. 1)	15	S/PDIF Out		

3.4.4 Universal Serial Bus (USB) Ports and Headers

There are four USB 3.2 Gen. 1 ports (USB5, USB6, USB7, USB8) located on the rear I/O panel, and one USB 3.2 Gen. 1 header (USB2/3) located on the motherboard to provide front USB access. One USB 3.2 Gen. 2x2 port (USB4) is located on the rear I/O panel. The 10- pin black USB header supports two USB 2.0 connections (USB0/1), and two USB 2.0 ports (USB9, USB10) are located on the rear I/O panel. The motherboard also provides one front accessible Type-A USB 3.2 Gen. 2 port (USB11) and one USB 3.2 Gen. 2 header (USB12). These USB ports and headers can be used for USB support via USB cables (not included).

Front Panel USB 2.0 Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	+5V	2	+5V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	Ground	8	Ground
9	Key	10	NC

Front Panel USB 3.2 Gen. 1 Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	19	Power
2	Stda_SSRX-	18	USB3_RN
3	Stda_SSRX+	17	USB3_RP
4	GND	16	GND
5	Stda_SSTX-	15	USB3_TN
6	Stda_SSTX+	14	USB3_TP
7	GND	13	GND
8	D-	12	USB_N
9	D+	11	USB_P
10		x	

Type-A USB 3.2 Gen. 2 (USB11) Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	5	SSRX-
2	USB_N	6	SSRX+
3	USB_P	7	GND
4	Ground	8	SSTX-
		9	SSTX+

Front Panel USB 3.2 Gen. 2 (USB12) Pin Definitions

Pin#	Definition	Pin#	Definition	Pin#	Definition	Pin#	Definition	Pin#	Definition
1	VBUS	5	RX1+	9	NC	13	TX2-	17	GND
2	TX1+	6	RX1-	10	NC	14	GND	18	D-
3	TX1-	7	VBUS	11	VBUS	15	RX2+	19	D+
4	GND	8	CC1	12	TX2+	16	RX2-	20	CC2

3.5 Troubleshooting Procedures…

Use the following procedures to troubleshoot your system. If you have followed all of the procedures below and still need assistance, refer to the 'Technical Support Procedures' and/or 'Returning Merchandise for Service' section(s) in this chapter. Always disconnect the AC power cord before adding, changing or installing any non hot-swap hardware components.

3.5.1 Before Power On

1. Make sure that there are no short circuits between the motherboard and chassis.
2. Disconnect all ribbon/wire cables from the motherboard, including those for the keyboard and mouse.

3. Remove all add-on cards.

4. Install the CPU (making sure it is fully seated) and connect the front panel connectors to the motherboard.

3.5.2 No Power

1. Make sure that there are no short circuits between the motherboard and the chassis.

2. Make sure that the ATX power connectors are properly connected.

3. Check that the 115V/230V switch, if available, on the power supply is properly set.

4. Turn the power switch on and off to test the system, if applicable.

5. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3VDC. If it does not, replace it with a new one.

3.5.3 No Video

1.If the power is on, but you do not have video, remove all add-on cards and cables.

2.Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory, or try a different one).

3.5.4 System Boot Failure

If the system does not display POST (Power-On-Self-Test) or does not respond after the power is turned on, check the following:

1. Check for any error beep from the motherboard speaker.

• If there is no error beep, try to turn on the system without DIMM modules installed. If there is still no error beep, replace the motherboard.

• If there are error beeps, clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper (JBT1). Refer to Section 2.8.

2. Remove all components from the motherboard, especially the DIMM modules. Make sure that system power is on and that memory error beeps are activated.

3. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this chapter.

3.5.5 Memory Errors

When a no-memory beep code is issued by the system, check the following:

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)

2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMM modules in the system.

3. Make sure that you are using the correct type of ECC DDR4 modules recommended by the manufacturer.

4. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.

3.5.6 Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to Chapter 1 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3VDC. If it does not, replace it with a new one.

3.6 Battery Removal and Installation…

3.6.1 Battery Removal

To remove the onboard battery, follow the steps below:

1. Power off your system and unplug your power cable.
2. Locate the onboard battery as shown below.
3. Using a tool such as a pen or a small screwdriver, push the battery lock outwards to unlock it. Once unlocked, the battery will pop out from the holder.
4. Remove the battery.

3.6.2 Proper Battery Disposal

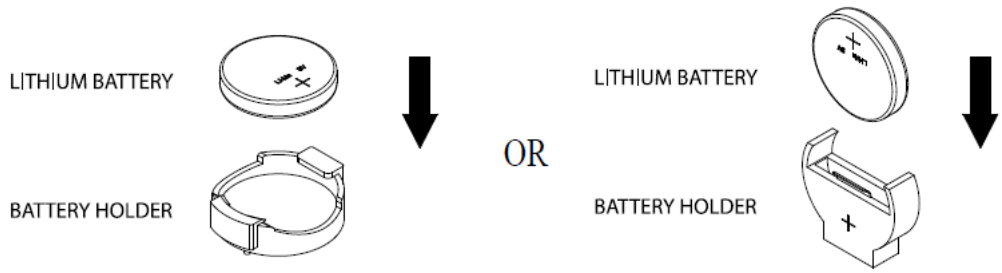
Warning: Please handle used batteries carefully. Do not damage the battery in anyway; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency to dispose of your used battery properly.

3.6.3 Battery Installation

To install an onboard battery, follow the steps below:

1. Power off your system and unplug your power cable.
2. Locate the onboard battery as shown below
3. Identify the battery's polarity. The positive (+) side should be facing up.
4. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.

Warning: When replacing a battery, be sure to only replace it with the same type.



4 Chapter 4 : UEFI BIOS

4.1 Introduction

This chapter describes the AMIBIOS™ Setup utility for the motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.

Starting the Setup Utility

To enter the BIOS Setup Utility, hit the <Delete> key while the system is booting-up. (In most cases, the <Delete> key is used to invoke the BIOS setup screen. There are a few cases when other keys are used, such as <F1>, <F2>, etc.) Each main BIOS menu option is described in this manual.

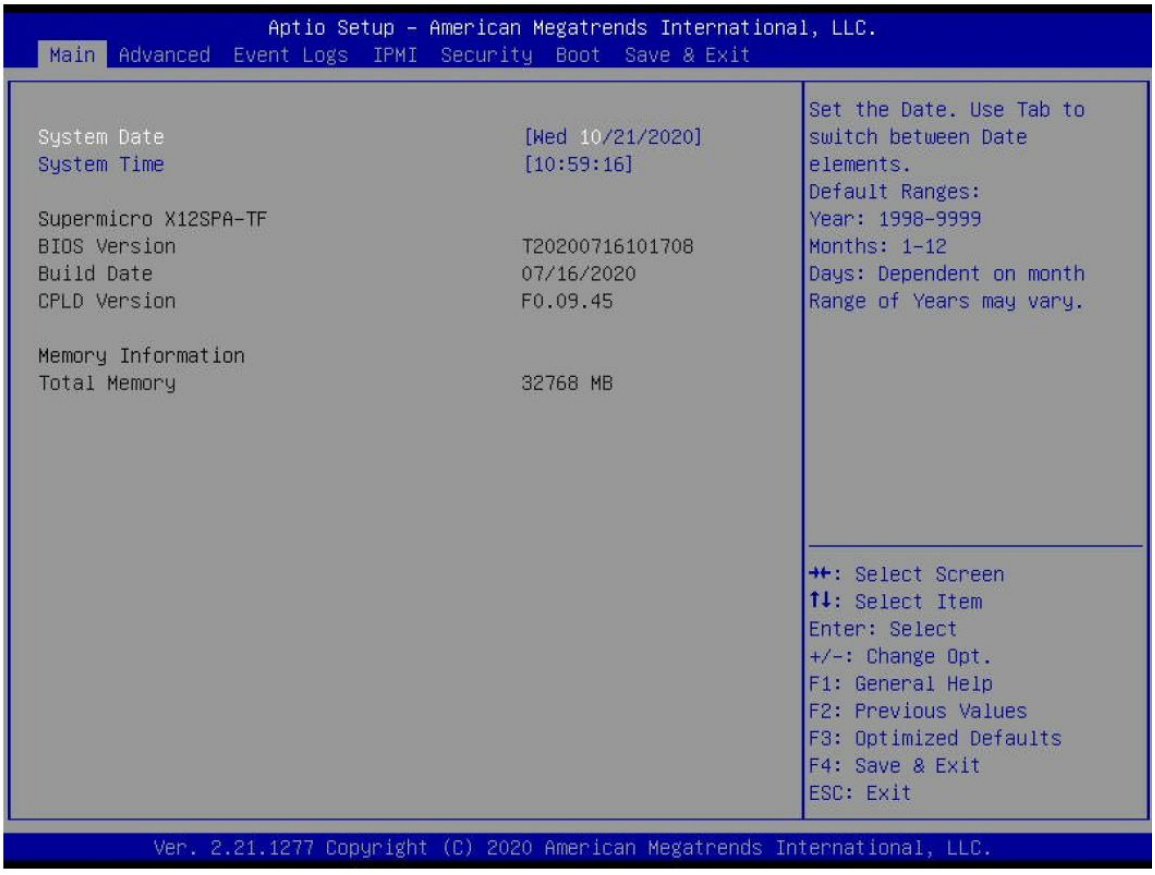
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. "Grayed-out" options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it. (Note that the BIOS has default text messages built in. We retain the option to include, omit, or change any of these text messages.) Settings printed in Bold are the default values.

A " ► " indicates a submenu. Highlighting such an item and pressing the <Enter> key will open the list of settings within that submenu.

The BIOS setup utility uses a key-based navigation system called hot keys. Most of these hot keys (<F1>, <F2>, <F3>, <Enter>, <ESC>, <Arrow> keys, etc.) can be used at any time during the setup navigation process.

4.2 Main Setup

When you first enter the AMI BIOS setup utility, you will enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS setup screen is shown below and the following items will be displayed:



System Date/System Time

Use this option to change the system date and time. Highlight System Date or System Time using the arrow keys. Enter new values using the keyboard. Press the <Tab> key or the arrow keys to move between fields. The date must be entered in MM/DD/YYYY format. The time is entered in HH:MM:SS format. Note: The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00. The date's default value is the BIOS build date after RTC reset.

Supermicro X12SPA-TF

BIOS Version

This item displays the version of the BIOS ROM used in the system.

Build Date

This item displays the date when the version of the BIOS ROM used in the system was built.

CPLD Version

This item displays the Complex Programmable Logic Device version.

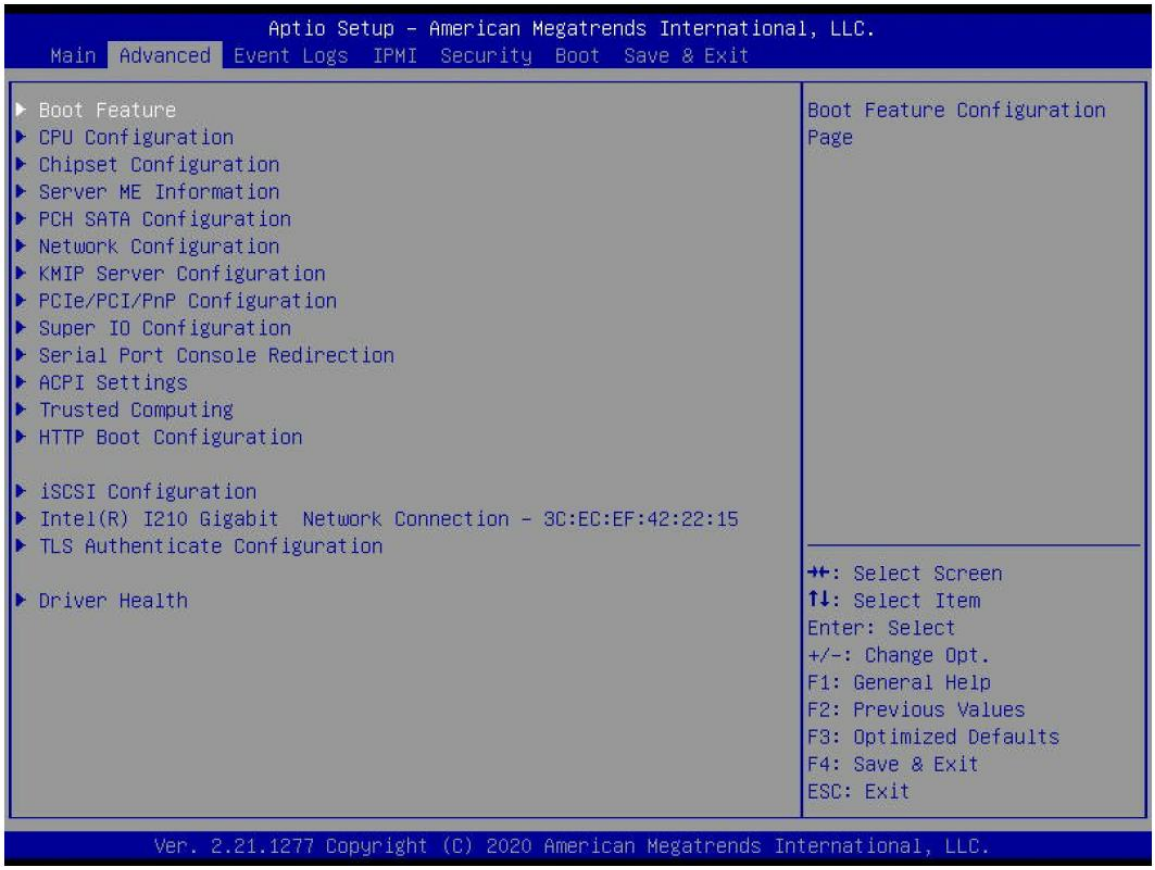
Memory Information

Total Memory

This item displays the total size of memory available in the system.

4.2.1 Advanced Setup Configurations

Use the arrow keys to select the Advanced menu and press <Enter> to access the submenu items:



Warning: Take caution when changing the Advanced settings. An incorrect value, a very high DRAM frequency, or an incorrect DRAM timing setting may make the system unstable. When this occurs, revert to default manufacturer settings.

4.2.2 Boot Feature

Quiet Boot

Use this feature to select the screen display between the POST messages and the OEM logo upon bootup. Select Disabled to display the POST messages. Select Enabled to display the OEM logo instead of the normal POST messages. The options are Disabled and Enabled.

Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to display the current AddOn ROM setting. Select Force BIOS to use the Option ROM display set by the system BIOS. The options are Force BIOS and Keep Current.

Bootup NumLock State

Use this feature to set the Power-on state for the <Numlock> key. The options are On and Off.

Wait For "F1" If Error

Use this feature to force the system to wait until the "F1" key is pressed if an error occurs.

The options are Disabled and Enabled.

INT19 (Interrupt 19) Trap Response

Interrupt 19 is the software interrupt that handles the boot disk function. When this feature is set to Immediate, the ROM BIOS of the host adapters will "capture" Interrupt 19 at Bootup immediately and allow the drives that are attached to these host adapters to function as bootable disks. If this feature is set to Postponed, the ROM BIOS of the host adapters will not capture Interrupt 19 immediately and allow the drives attached to these adapters to function as bootable devices at bootup. The options are Immediate and Postponed.

Re-try Boot

If this feature is enabled, the BIOS will automatically reboot the system from a specified boot device after its initial boot failure. The options are Disabled, Legacy Boot, and EFI Boot.

Power Configuration

Watch Dog Function

If enabled, the Watch Dog timer will allow the system to reset or generate NMI based on jumper settings when it is expired for more than five minutes. The options are Disabled and Enabled.

Restore on AC Power Loss

Use this feature to set the power state after a power outage. Select Stay Off for the system power to remain off after a power loss. Select Power On for the system power to be turned on after a power loss. Select Last State to allow the system to resume its last power state before a power loss. The options are Stay Off, Power On, and Last State.

Power Button Function

This feature controls how the system shuts down when the power button is pressed. Select 4 Seconds Override for the user to power off the system after pressing and holding the power button for four seconds or longer. Select Instant Off to instantly power off the system as soon as the user presses the power button. The options are Instant Off and 4 Seconds Override.

4.2.3 CPU Configuration

The following CPU information will display:

Processor BSP Revision

Processor Socket

Processor ID

Processor Frequency

Processor Max Ratio

Processor Min Ratio

Microcode Revision

L1 Cache RAM (Per Core)

L2 Cache RAM (Per Core)

L3 Cache RAM (Per Package)

Processor 0 Version

4.2.4 CPU1 Core Disable Bitmap

CPU1 Core Diable Bitmap

Available Bitmap:

This feature displays the available bitmap.

Core Disable Bitmap(Hex)

Enter a value to enable or disable the cores for the CPU in socket 0.

Hyper-Threading (ALL) (Available when supported by the CPU)

Select Enable to support Intel Hyper-threading Technology to enhance CPU performance. The options are Disable and Enable.

Hardware Prefetcher (Available when supported by the CPU)

If set to Enable, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the L2 cache to improve CPU performance. The options are Disable and Enable.

Adjacent Cache Prefetch (Available when supported by the CPU)

The CPU prefetches the cache line for 64 bytes if this feature is set to Disabled. The CPU prefetches both cache lines for 128 bytes as comprised if this feature is set to Enable. The options are Enable and Disable.

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enable to enable the DCU (Data Cache Unit) Streamer Prefetcher which will stream and prefetch data and send it to the Level 1 data cache to improve data processing and system performance. The options are Enable and Disable.

DCU IP Prefetcher (Available when supported by the CPU)

Select Enable for DCU (Data Cache Unit) IP Prefetcher support, which will prefetch IP addresses to improve network connectivity and system performance. The options are Enable and Disable.

LLC Prefetch

If set to Enable, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the L3 cache to improve CPU performance. The options are Disable and Enable.

Extended APIC

Select Enable to activate APIC (Advanced Programmable Interrupt Controller) support. The options are Disable and Enable.

Enable Intel(R) TXT

Intel Trusted Execution Technology (TXT) helps protect against software-based attacks and ensures protection, confidentiality, and integrity of data stored or created on the system. The options are Disable and Enable.

VMX

Use this feature to enable the Vanderpool Technology support. The options are Disable and Enable.

Note: If a change is made to this setting, you will need to reboot the system for the change to take effect.

Enable SMX

Use this feature to enable the Safer Mode Extensions support. The options are Disable and Enable.

PPIN Control

Select Unlock/Enable to use the Protected-Processor Inventory Number (PPIN) in the system. The options are Lock/Disable and Unlock/Enable.

AES-NI

Select Enable to use the Intel Advanced Encryption Standard (AES) New Instructions (NI) to ensure data security. The options are Disable and Enable.

Total Memory Encryption (TME) (Available when CPU supports TME capability)

Use this feature to enable the Total Memory Encryption (TME) function for physical memory protection. The options are Disabled and Enabled.

Total Memory Encryption Multi-Tenant (TME-MT) (Available when "Total Memory Encryption (TME)" is set to Enabled and "Limit CPU PA to 46 bits" is set to Disabled)

Use this feature to support tenant-provided (SW-provided) keys. The options are Disabled and Enabled.

MAX TME-MT Keys (Available when "Total Memory Encryption Multi-Tenant (TME-MT)" is set to Enabled)

This feature displays the maximum TME-MT keys.

The following Software Guard Extension (SGX) features are available when "Total Memory Encryption (TME)" is set to Enabled and CPU supports Intel Software Guard Extensions (SGX).

Note: Each memory channel must have at least one DIMM populated on the motherboard to support the Intel SGX feature.

SGX Factory Reset

Use this feature to perform an SGX factory reset to delete all registration data and force an Initial Platform Establishment flow. Reboot the system for the change to take effect. The options are Disabled and Enabled.

SW Guard Extensions (SGX)

Use this feature to enable Intel Software Guard Extensions (SGX) support. Intel SGX is a set of extensions that increases the security of application code and data by using enclaves in memory to protect sensitive information. The options are Disabled and Enabled.

SGX Package Info In-Band Access

Setting this feature to Enabled is required before BIOS provides software with the key blobs, which are generated for each CPU package. The options are Disabled and Enabled.

PRMRR Size

Use this feature to set the Processor Reserved Memory Range Register (PRMRR) size. The options are No vaild PRMRR size, 1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, and 512G.

SGX QoS

Use this feature to enable Intel SGX Quality of Service (QoS) support. QoS can make better network performance by prioritizing network traffic. The options are Disabled and Enabled.

Select Owner EPOCH input type

Owner EPOCH is used as a parameter to allow the owner to add entropy to the keys during the derivation. Use this feature to select the two Owner EPOCH modes. One is New Random

Owner EPOCH , the other is manually entered by the user. Each EPOCH is 64-bit. The options are Change to New Random Owner EPOCHs and Manual User Defined Owner EPOCHs.

Note: Changing the Owner EPOCH value will lose the data in enclaves.

Software Guard Extensions Epoch 0 (Available when "Select Owner EPOCH input type" is set to Manual User Defined Owner EPOCHs)

Enter a numeric value for this feature. The default is 0.

Software Guard Extensions Epoch 1 (Available when "Select Owner EPOCH input type" is set to Manual User Defined Owner EPOCHs)

Enter a numeric value for this feature. The default is 0.

SGXLEPUBKEYHASHx Write Enable

Use this feature to write SGX LE Public Key Hash 0-3 from OS/SW. The options are Disabled and Enabled.

SGXLEPUBKEYHASH0 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 0-7 of SGX Launch Enclave Public Key Hash. The default is 0.

SGXLEPUBKEYHASH1 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 8-15 of SGX Launch Enclave Public Key Hash. The default is 0.

SGXLEPUBKEYHASH2 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 16-23 of SGX Launch Enclave Public Key Hash. The default is 0.

SGXLEPUBKEYHASH3 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 24-31 of SGX Launch Enclave Public Key Hash. The default is 0.

Enable/Disable SGX Auto MP Registration Agent

Use this feature to enable/disable SGX Auto Multi-Package Registration Agent (MPA) running automatically at boot time. The options are Disabled and Enabled.

Limit CPU PA to 46 Bits

Select Enable to limit the CPU physical address to 46 bits to support older Hyper-v The options are Disable and Enable.

4.2.5 Advanced Power Management Configuration

Power Technology

Select Energy Efficient to support power-saving mode. Select Custom to customize system power settings. Select Disable to disable power-saving settings. The options are Disable, Energy Efficient, and Custom.

Power Performance Tuning (Available when the Power Technology is set to Custom)

This feature allows you to select whether the BIOS or Operating System chooses energy performance bias tuning. The options are OS Controls EPB and BIOS Controls EPB.

ENERGY_PERF_BIAS CFG Mode (Available when the Power Performance Tuning is set to BIOS Controls EPB)

The Energy Performance BIAS (EPB) feature allows you to configure CPU power and performance settings. Select Maximum Performance to set the highest performance. Select Performance to optimize performance over energy efficiency. Select Balanced Performance to prioritize performance optimization while conserving energy. Select Balanced Power to prioritize energy conservation while maintaining good

performance. Select Power to optimize energy efficiency over performance. The options are Maximum Performance, Performance, Balanced Performance, Balanced Power, and Power.

4.2.5.1 CPU P State Control

This feature allows you to configure the following CPU power settings:

SpeedStep (P-States)

Intel SpeedStep Technology allows the system to automatically adjust processor voltage and core frequency to reduce power consumption and heat dissipation. The options are Disable and Enable.

Dynamic SST-PP

Use this feature to enable the Dynamic SST-PP support. The options are Disable and Enable.

Intel SST-PP (Available when the Dynamic SST-PP is set to Disable)

Use this feature to select from up to two additional base frequency conditions. The options are Base, Config 1, and Config 2.

The following information displays.

Intel SST-PP (Core Count, Current P1 Ration [0], Package TDP (W), Tjmax) / Base / Config 1 / Config 2

Activate SST-BF

Use this feature to enable the SST-BF support. The options are Disable and Enable.

Configure SST-BF (Available when the Activate SST-BF is set to Enable)

This feature allows the BIOS to configure SST-BF High Priority Cores so that SW does not have to configure. The options are Disable and Enable.

EIST PSD Funtion (Available when the SpeedStep (P-States) is set to Enable)

This feature reduces the latency that occurs when one P-state changes to another, thus allowing the transitions of P-state changing to occur more frequently. This will allow for more demand-based P-state changing or switching that is based on real-time energy needs of applications so that the power-to-performance balance can be optimized for energy efficiency. The options are HW_ALL and SW_ALL.

Turbo Mode (Available when the SpeedStep (P-States) is set to Enable)

This feature will enable dynamic control of the processor, allowing it to run above stock frequency. The options are Disable and Enable.

CPU Flex Ratio Override (Available when the SpeedStep (P-States) is set to Enable)

Select Enable to activate CPU Flex Ratio programming. The options are Disable and Enable.

CPU Core Flex Ratio (Available when the CPU Flex Ratio Override is set to Enable)

Use this feature to set a value of the CPU Flex Ratio. The default is 23.

4.2.5.2 Hardware PM State Control

Hardware P-States

This feature allows you to select between OS and hardware-controlled P-states. Selecting

Native Mode allows the OS to choose a P-state. Selecting Out of Band Mode allows the hardware to autonomously choose a P-state without OS guidance. Selecting Native Mode with No Legacy Support functions as Native Mode with no support for older hardware. The options are Disable, Native Mode, Out of Band Mode, and Native Mode with No Legacy Support.

4.2.5.3 CPU C State Control

Enable Monitor MWAIT

Select Enable to support Monitor and Mwait, which are two instructions in Streaming SIMD Extension 3 (SSE3), to improve synchronization between multiple threads for CPU performance enhancement. The options are Disable and Enable.

CPU C6 Report

Select Enable to allow the BIOS to report the CPU C6 State (ACPI C3) to the operating system. During the CPU C6 State, the power to all cache is turned off. The options are Disable, Enable, and Auto.

Enhanced Halt State (C1E)

Select Enable to use Enhanced Halt State technology, which will significantly reduce the CPU's power consumption by reducing its clock cycle and voltage during a Halt-state. The options are Disable and Enable.

4.2.5.4 Package C State Control

Package C State

This feature allows you to set the limit on the C State package register. The options are C0/C1 state, C2 state, C6 (non Retention) state, and Auto.

4.2.5.5 CPU T State Control

Software Controlled T-States

Use this feature to enable Software Controlled T-States. The options are Disable and Enable.

T-State Throttle Level (Available when the Software Controlled T-States is set to Enable)

Use this feature to select the On-Die thermal throttling. The options are Disable, 6.25%, 12.5%, 18.75%, 25.0%, 37.5%, 43.75%, 50.0%, 56.25%, 62.5%, 75.0%, 81.25%, 87.5%, and 93.75%.

4.2.6 Chipset Configuration

Warning: Setting the wrong values in the following features may cause the system to malfunction.

4.2.6.1 North Bridge

This feature allows you to configure the following North Bridge settings.

4.2.6.2 Uncore Configuration

The following information will display:

- Number of CPU
- Number of IIO
- Current UPI Link Speed
- Current UPI Link Frequency

- Global MMIO Low Base / Limit
- Global MMIO High Base / Limit
- Pci-e Configuration Base / Size

Degrade Precedence

Use this feature to set degrade precedence when system settings are in conflict. Select Topology Precedence to degrade Features. Select Feature Precedence to degrade Topology.

The options are Topology Precedence and Feature Precedence.

Link L0p Enable

Select Enable for the QPI to enter the L0p state for power saving. The options are Disable, Enable, and Auto.

Link L1 Enable

Select Enable for the QPI to enter the L1 state for power saving. The options are Disable, Enable, and Auto.

XPT Remote Prefetch

Select Enable to support XPT (Extended Prediction Table) Remote Prefetch which will allow an LLC request to be duplicated and sent to an appropriate memory controller in a remote machine based on the recent LLC history to reduce latency. The options are Disable, Enable, and Auto.

KTI Prefetch

KTI Prefetch enables memory read to start early on a DDR bus. The options are Disable, Enable, and Auto.

Local/Remote Threshold

This feature allows you to set the threshold for the Interrupt Request (IRQ) signal. The options are Disable, Auto, Low, Medium, and High.

IO Directory Cache (IODC)

IO Directory Cache is an 8-entry cache that stores the directory state of remote IIO writes and memory lookups, and saves directory updates. Use this feature to lower cache to cache (C2C) transfer latencies. The options are Disable, Auto, Enable for Remote InvItoM Hybrid Push, InvItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, and Enable for Remote InvItoM and Remote WViLF.

SNC (Sub NUMA)

Sub NUMA Clustering (SNC) is a feature that breaks up the Last Level Cache (LLC) into clusters based on address range. Each cluster is connected to a subset of the memory controller. Enable this feature to improve average latency and reduce memory access congestion for higher performance. The options are Disable, Enable SNC2 (2-clusters), and Enable SNC4 (4-clusters).

XPT Prefetch

This feature makes a copy to the memory controller of a read request being sent to LLC. The options are Disable, Enable, and Auto.

Snoop Throttle Configuration

Use this feature to select the level of snoop throttle setting for CHA. The options are Disabled, Low, Medium, High, and Auto.

PCIe Remote P2P (Peer-to-Peer) Relaxed Ordering

Select Disable to support PCIe remote peer-to-peer relaxed writing ordering, which will allow hardware to enforce peer-to-peer write ordering. The options are Disable and Enable.

Stale AtoS

Use this feature to optimize the A to S directory. The options are Disable, Enable, and Auto.

LLC Dead Line Alloc

Select Enable to optimally fill dead lines in LLC. The options are Disable, Enable, and Auto.

4.2.6.3 Memory Configuration

Enforce POR

Select POR (Plan of Record) to enforce POR restrictions on DDR4 frequency and voltage programming. The options are POR and Disable.

PPR Type

Use this feature to set the Post Package Repair type. The options are PPR Disabled, Hard PPR, and Soft PPR.

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are Auto, 2133, 2200, 2400, 2600, 2666, 2800, 2933, 3000 and 3200.

Data Scrambling for DDR4

Use this feature to enable or disable data scrambling for DDR4 memory. The options are Disable and Enable.

2x Refresh Enable

Select Enable for memory 2X refresh support to enhance memory performance. The options are Auto, Disable, and Enable.

4.2.6.4 Memory Topology

This feature displays the information of onboard memory modules as detected by the BIOS.

4.2.6.5 Memory RAS Reliability_Availability_Serviceability Configuration

Enable Pcode WA (Workaround) for SAI (Security Attribute of the Initiator) PG (Policy Group)

Pcode, a register transfer language designed for reverse engineering, translates individual processor instructions into a sequence of Pcode operations in order to facilitate the construction of data-flow graphs and dissembling of processor instructions for machine application. Select Enabled to allow Pcode to work around the SAI group policy to achieve a solution with a next-step instruction. The options are Disabled and Enabled.

Mirror Mode (Available when the UEFI ARM Mirror is set to Disable)

This feature allows memory to be mirrored between two channels, providing 100% redundancy. The options are Disabled, Full Mirror Mode, and Partial Mirror Mode.

UEFI ARM Mirror

Select Enable to support the UEFI-based address range mirroring with setup option. The options are Disable and Enable.

ARM Mirror Percentage (Available when the UEFI ARM Mirror is set to Enable)

Use this feature to set the percentage of memory space to be used for UEFI ARM mirroring for memory security enhancement.

Correctable Error Threshold

Use this feature to specify the threshold value for correctable memory-error logging, which sets a limit on the maximum number of events that can be logged in the memory error log at a given time. The default setting is 512.

Partial Cache Line Sparing PCLS

Use this feature to enable/disable PCLS sparing. The options are Disabled and Enabled.

ADDDC Sparing

Adaptive Double Device Data Correction (ADDDC) Sparing detects when the predetermined threshold for correctable errors is reached, copying the contents of the failing DIMM to spare memory. The failing DIMM or memory rank will then be disabled. The options are Disabled and Enabled.

Patrol Scrub

Patrol Scrubbing is a process that allows the CPU to correct correctable memory errors detected on a memory module and send the correction to the requestor (the original source). When this feature is set to Enable, the IO hub will read and write back one cache line every 16K cycles if there is no delay caused by internal processing. By using this method, roughly 64 GB of memory behind the IO hub will be scrubbed every day. The options are Disabled, Enable, and Enable at End of POST.

4.2.7 I/O Configuration

4.2.7.1 CPU1 Configuration

IOU0 (II0 PCIe Port 1) / IOU1 (II0 PCIe Port 2) / IOU2 (II0 PCIe Port 3) / IOU3 (II0 PCIe Port 4)/ IOU4 (II0 PCIe Port 5)

This feature configures the PCIe port Bifurcation setting for a PCIe port specified by the user. The options are Auto, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

PCI-E Port MPSS

Selecting Auto for this feature will enable the motherboard to automatically detect the maximum Transaction Layer Packet (TLP) size for the connected PCIe device, allowing for maximum I/O efficiency. Selecting 128B or 256B will designate maximum packet size of 128 or 256. The options are 128B, 256B, and Auto.

4.2.7.2 IOAT Configuration

Disable TPH

Transparent Huge Pages (TPH) is a Linux memory management system that enables communication in larger blocks (pages). Enabling this feature will increase performance.

The options are No and Yes.

Prioritize TPH (Available when the Disable TPH is set to No)

Use this feature to enable Prioritize TPH support. The options are Enable and Disable.

Relaxed Ordering

Select Enable to enable Relaxed Ordering support, which will allow certain transactions to violate the

strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been enqueued. The options are No and Yes.

4.2.7.3 Intel® VT for Directed I/O(VT-d)

Intel® VT for Directed I/O (VT-d)

Select Enable to use Intel Virtualization Technology for Direct I/O VT-d support by reporting the I/O device assignments to the VMM (Virtual Machine Monitor) through the DMAR ACPI tables. This feature offers fully-protected I/O resource sharing across Intel platforms, providing greater reliability, security and availability in networking and data-sharing. The options are Yes and No.

ACS Control (Available when Intel VT for Directed I/O (VT-d) is set to Yes)

Use this feature to program Access Control Services (ACS) to the PCI-e Root Port Bridges. The options are Enable and Disable.

Interrupt Remapping (Available when Intel VT for Directed I/O (VT-d) is set to Yes)

Use this feature to enable Interrupt Remapping support, which detects and controls external interrupt requests. The options are Auto, Yes, and No.

4.2.7.4 Intel®VMD (Volume Management Device) Technology

This section describes the configuration settings for the Intel VMD Technology.

Note 1: After you've enabled VMD in the BIOS on a PCIe slot, this PCIe slot will be dedicated for VMD use only, and it will no longer support any PCIe device. To re-activate this slot for PCIe use, please disable VMD in the BIOS.

Note 2: PCIe slots and naming can differ depending on the PCIe devices installed on your motherboard.

4.2.7.5 Intel® VMD for Volume Management Device on CPU1

VMD Config for PCH ports / VMD Config for IOU 0 / VMD Config for IOU 1 / VMD Config for IOU 3 / VMD Config for IOU 4

Enable/Disable VMD

Select Enable to enable Intel Volume Management Device Technology support for the root port specified by the user. The options are Disable and Enable.

*If the feature above is set to Enable, the following features will become available for configuration:

VMD Port A/B/C/D (Available when the device is detected by the system)

Select Enable to use the Intel Volume Management Device Technology for this specific root port. The options are Disable and Enable.

Hot Plug Capable (Available when the device is detected by the system)

Select Enable to enable Hot Plug support for the root ports specified by the user, which will allow you to change the devices on those root ports without shutting down the system. The options are Disable and Enable.

CfgBar Size

Use this feature to set the VMD Config Bar size (in bits. Minimum is 20 bits and maximum is 27 bits.) The

default setting is 25 (in bits).

CfgBar Attribute

Use this feature to set the VMD Configuration Bar attribute (e.g. 64-bit or Prefetchable.) The options are 32-bit non-prefetchable, 64-bit non-prefetchable, and 64-bit prefetchable.

MemBar1 Size

Use this feature to set the VMD Memory Bar1 size (in bits. Minimum is 20 bits.) The default setting is 25 (in bits).

MemBar1 Attribute

Use this feature to set the VMD Memory Bar1 attribute (e.g. 64-bit or Prefetchable.) The options are 32-bit non-prefetchable, 64-bit non-prefetchable, and 64-bit prefetchable.

MemBar2 Size

Use this feature to set the VMD Memory Bar2 size (in bits. Minimum is 20 bits.) The default setting is 20 (in bits).

MemBar2 Attribute

Use this feature to set the VMD Memory Bar2 attribute (e.g. 64-bit or Prefetchable.) The options are 32-bit non-prefetchable, 64-bit non-prefetchable, and 64-bit prefetchable.

4.2.8 South Bridge

The following USB information will display:

- USB Module Version
- USB Devices

Legacy USB Support

This feature enables support for USB 2.0 and older. The options are Enabled, Disabled, and Auto.

XHCI Hand-off

When this feature is disabled, the motherboard will not support USB 3.0. The options are **Enabled** and Disabled.

Port 60/64 Emulation

This feature allows legacy I/O support for USB devices like mice and keyboards. The options are Disabled and Enabled.

PCIe PLL SCC

Select Enable for PCH PCI-E Spread Spectrum Clocking support, which will allow the BIOS to monitor and attempt to reduce the level of Electromagnetic interface caused by the components whenever needed. The options are Disabled and Enabled.

Port 61h Bit-4 Emulation

Select Enabled for I/O Port 61h-Bit 4 emulation support to enhance system performance.
The options are Disabled and Enabled.

4.2.9 Server ME Configuration

The following General ME Configuration will display:

- General ME Configuration
- Oper. Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1
- ME Firmware Status #2
- Current State
- Error Code

4.2.10 PCH SATA Configuration

When this submenu is selected, the AMI BIOS automatically detects the presence of the SATA devices that are supported by the Intel PCH chip and displays the following features:

SATA Controller

This feature enables or disables the onboard SATA controller supported by the Intel PCH chip. The options are Disable and Enable.

Configure SATA as (Available when the SATA Controller is set to Enable)

Select AHCI to configure a SATA drive specified by the user as an AHCI drive. Select RAID to configure a SATA drive specified by the user as a RAID drive. The options are AHCI and RAID.

SATA RSTe Boot Info (Available when the Configure SATA as is set to RAID)

Select Enable to provide full int13h support for the devices attached to SATA controller. The options are Disable and Enable.

Support Aggressive Link Power Management

When this feature is set to Enable, the SATA AHCI controller manages the power usage of the SATA link. The controller will put the link in a low power mode during extended periods of I/O inactivity, and will return the link to an active state when I/O activity resumes. The options are Disable and Enable.

SATA Port 0 - Port 7

These features display the information detected on the installed SATA drive on the particular SATA port.

- Model number of drive and capacity
- Software Preserve Support

Hot Plug

Select Enable to support Hot-plugging for the device installed on a selected SATA port which will allow you to replace the device installed in the slot without shutting down the system. The options are Disable and Enable.

Spin Up Device

Select Enable for Staggered Spin Up support which will allow the SATA devices specified by the user to spin up one at a time at boot up in an effort to prevent all hard drive disks from spinning up at the same time, causing a power surge. The options are Disable and Enable.

SATA Device Type

Use this feature to specify if the device installed on the SATA port specified by the user should be

connected to a Solid State drive or a Hard Disk Drive. The options are Hard Disk Drive and Solid State Drive.

4.2.11 Network Configuration

Network Stack

Select Enabled to enable PXE (Preboot Execution Environment) or UEFI (Unified Extensible Firmware Interface) for network stack support. The options are Disabled and Enabled.

*If the feature above is set to Enable, the following features will become available for configuration:

IPv4 PXE Support

Select Enabled to enable IPv4 PXE boot support. The options are Disabled and Enabled.

IPv4 HTTP Support

Select Enabled to enable IPv4 HTTP boot support. The options are Disabled and Enabled.

IPv6 PXE Support

Select Enabled to enable IPv6 PXE boot support. The options are Disabled and Enabled.

IPv6 HTTP Support

Select Enabled to enable IPv6 HTTP boot support. The options are Disabled and Enabled.

PXE Boot Wait Time

Use this feature 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.

***Use the following features to configure network parameters:**

4.2.11.1 MAC: (MAC address)-IPv4 Netwrok Configuration

Configured

Use this feature to indicate whether the above MAC address has been configured successfully. The options are Disabled and Enabled.

Enable DHCP (Available when the Configured is set to Enable)

Use this feature to set the DHCP. The options are Disabled and Enabled.

*If this feature is set to Disabled, the following features will become available for configuration:

Local IP Address - Enter an IP address in dotted-decimal notation

Local NetMask - Enter a NetMask in dotted-decimal notation

Local Gateway - Enter a Gateway in dotted-decimal notation

Local DNS Servers - Enter a DNS Servers in dotted-decimal notation

Save Changes and Exit

Press <Enter> to save changes and exit. The options are Yes and No.

4.2.11.2 MAC: (MAC address)-IPv6 Netwrok Configuration

4.2.11.3 Enter Configuration Menu

The following information will display:

Interface Name / Interface Type / MAC address / Host addresses / Route Table / Gateway addresses / DNS addresses

Interface ID

Use this feature to change/enter the 64 bit alternative interface ID for the device. The string format is colon separated. The default setting is the above MAC address.

DAD Transmit Count

This feature displays the number of consecutive neighbor solicitation messages have been sent while performing duplicate address detection on a tentative address.

Policy

Use this feature to set the Policy. The options are automatic and manual.

4.2.11.4 Advanced Configuration

New IPv6 Address - Enter a new IPv6 address

New Gateway Addresses - Enter a Gateway address

New DNS Addresses - Enter a new DNS address

Commit Changes and Exit

Select this feature to save the changes you've made and return to the upper configuration page.

Discard Changes and Exit

Select this feature to discard all the changes and return to the upper configuration page.

Save Changes and Exit

Press <Enter> to save changes and exit. The options are Yes and No**.**

4.2.12 KMIP Server Configuration

KMIP Server IP address

Use this feature to enter the KMIP server IP4 address in dotted-decimal notation.

KMIP TCP Port number

Use this feature to enter the KMIP TCP port number. The valid range is 100 - 9999. The default setting is 5696.

TimeZone

Use this feature to enter the correct time zone. The default setting is 8 (GT+8 Taiwan time).

Client UserName

Press <Enter> to set the client user name. The name length is 0 - 63 characters.

Client Password

Press <Enter> to set the client password. The password length is 0 - 31 characters.

KMS TLS Certificate / Size

4.2.12.1 CA Certificate

For the CA certificate, use this feature to enroll factory defaults or load the KMS TLS certificates from the file. The options are Update, Delete, and Export.

4.2.12.2 Client Certificate

For the client certificate, use this feature to enroll factory defaults or load the KMS TLS certificates from the file. The options are Update, Delete, and Export.

4.2.12.3 Client Private Key

For the client private key, use this feature to enroll factory defaults or load the KMS TLS certificates from the file. The options are Update, Delete, and Export.

4.2.13 PCIe/PCI/PnP Configuration

The following information will display:

- PCI Bus Driver Version
- PCI Devices Common Settings:

Above 4G Decoding (Available if the system supports 64-bit PCI decoding)

Select Enabled to decode a PCI device that supports 64-bit in the space above 4G Address. The options are Disabled and Enabled.

SR-IOV Support

Use this feature to enable or disable Single Root IO Virtualization Support. The options are Disabled and Enabled.

ARI Support

Select Enable for Alternative Routing-ID Interpretation (ARI) support. The options are Disabled and Enabled.

Bus Master Enable

Select Enabled to enable the Bus Driver Master bit. The options are Disabled and Enabled.

MMIO High Base

Use this feature to select the base memory size according to memory-address mapping for the IO hub. The options are 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, and 512 G.

MMIO High Granularity Size

Use this feature to select the high memory size according to memory-address mapping for the IO hub. The options are 1G, 4G, 16G, 64G, 256G, and 1024G.

Maximum Read Request

Use this feature to select the Maximum Read Request size of the PCIe device, or select Auto to allow the System BIOS to determine the value. The options are Auto, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.

MMCFG Base

Use this feature to select the low base address for PCIe adapters to increase base memory. The options are

1G, 1.5G, 1.75G, 2G, 2.25G, 3G, and Auto.

NVMe Firmware Source

The feature determines which type of NVMe firmware should be used in your system. The options are Vendor Defined Firmware and AMI Native Support.

VGA Priority

Use this feature to select VGA priority when multiple VGA devices are detected. Select Onboard to give priority to your onboard video device. Select Offboard to give priority to your graphics card. The options are Onboard and Offboard.

Onboard Video Option ROM

Use this feature to select the Onboard Video Option ROM type. The options are Disabled and EFI.

CPU SLOT1 PCI-E 4.0 X16 OPROM

CPU SLOT2 PCI-E 4.0 X8 OPROM

CPU SLOT3 PCI-E 4.0 X16 OPROM

CPU SLOT4 PCI-E 4.0 X8 OPROM

CPU SLOT5 PCI-E 4.0 X16 OPROM

CPU SLOT6 PCI-E 4.0 X8 OPROM

CPU SLOT7 PCI-E 4.0 X16 OPROM

M.2-C01 PCI-E 4.0 x4 OPROM

M.2-C02 PCI-E 4.0 x4 OPROM

M.2-C03 PCI-E 4.0 x4 OPROM

M.2-C04 PCI-E 4.0 x4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled and EFI.

Onboard SAS Option ROM

Use this feature to select the Option ROM type for the SAS device specified by the user for system boot. The options are Disabled and EFI.

Onboard LAN Device

Use this feature to enable the Onbaord LAN device. The options are Disabled and Enabled.

Onboard LAN1 Option ROM (Available when the Onboard LAN Device is set to Enable)

Use this feature to select which firmware function to be loaded for LAN port 1 used for system boot. The options are Disabled and EFI.

Onboard LAN2 Option ROM (Available when the Onboard LAN Device is set to Enable)

Use this feature to select which firmware function to be loaded for LAN port 2 used for system boot. The options are Disabled and EFI.

4.2.14 Super IO Configuration

The following Super IO information will display:

- Super IO Chip AST2500

4.2.14.1 Serial Port 1 Configuration

This submenu allows you to configure the settings of Serial Port 1.

Serial Port 1

Select Enabled to enable the selected onboard serial port. The options are Disabled and Enabled.

Device Settings (Available when the Serial Port 1 is set to Enabled)

This feature displays the status of a serial port specified by the user.

Change Settings (Available when the Serial Port 1 is set to Enabled)

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options are Auto, (IO=3F8h; IRQ=4;), (IO=2F8h; IRQ=4;), (IO=3E8h; IRQ=4;), and (IO=2E8h; IRQ=4;).

4.2.14.2 Serial Port 2 Configuration

This submenu allows you to configure the settings of Serial Port 2.

Serial Port 2

Select Enabled to enable the selected onboard serial port. The options are Disabled and Enabled.

Device Settings (Available when the Serial Port 2 is set to Enabled)

This item displays the status of a serial port specified by the user.

Change Settings (Available when the Serial Port 2 is set to Enabled)

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options are Auto, (IO=3F8h; IRQ=3;), (IO=2F8h; IRQ=3;), (IO=3E8h; IRQ=3;), and (IO=2E8h; IRQ=3;).

Serial Port 2 Attribute (Available for Serial Port 2 only)

Select SOL to use COM Port 2 as a Serial Over LAN (SOL) port for console redirection.

The options are SOL and COM.

4.2.14.3 Serial Port Console Redirection

COM1

Console Redirection

Select Enabled to enable console redirection support for a serial port specified by the user. The options are Disabled and Enabled.

4.2.14.3.1 Console Redirection Settings (Available when the Console Redirection is set to Enabled)

Use this feature to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Terminal Type

This feature allows you to select the target terminal emulation type for Console Redirection.

Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF8 encoding to map Unicode

characters into one or more bytes. The options are VT100, VT100+, VT-UTF8, and ANSI.

Bits Per Second

Use this feature to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 38400, 57600, and 115200 (bits per second).

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 and 8 (bits).

Parity

A parity bit can be sent along with regular data bits to detect data transmission errors. Select Even if the parity bit is set to 0, and the number of 1's in data bits is even. Select Odd if the parity bit is set to 0, and the number of 1's in data bits is odd. Select None if you do not want to send a parity bit with your data bits in transmission. Select Mark to add a mark as a parity bit to be sent along with the data bits. Select Space to add a Space as a parity bit to be sent with your data bits. The options are None, Even, Odd, Mark, and Space.

Stop Bits

A stop bit indicates the end of a serial data packet. Select 1 Stop Bit for standard serial data communication. Select 2 Stop Bits if slower devices are used. The options are 1 and 2.

Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None and Hardware RTS/CTS.

VT-UTF8 Combo Key Support

Select Enabled to enable VT-UTF8 Combination Key support for ANSI/VT100 terminals. The options are Disabled and Enabled.

Recorder Mode

Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote server. The options are Disabled and Enabled.

Resolution 100x31

Select Enabled for extended-terminal resolution support. The options are Disabled and Enabled.

Legacy OS Redirection Resolution

Use this feature to select the number of rows and columns used in Console Redirection for legacy OS support. The options are 80x24 and 80x25.

Putty KeyPad

This feature selects the settings for Function Keys and KeyPad used for Putty, which is a terminal emulator designed for the Windows OS. The options are VT100, LINUX, XTERMR6, SC0, ESCN, and VT400.

Redirection After BIOS POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When set to Bootloader,

legacy console redirection is disabled before booting the OS. When set to Always Enable, legacy console redirection remains enabled when booting the OS. The options are Always Enable and BootLoader.

SOL/COM2

Console Redirection

Select Enabled to use the SOL port for Console Redirection. The options are Disabled and Enabled.

4.2.14.3.2 Console Redirection Settings (Available when the Console Redirection is set to Enabled)

Use this feature to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Terminal Type

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, VT-UTF8, and ANSI.

Bits Per Second

Use this feature to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 38400, 57600 and 115200 (bits per second).

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 and 8 (bits).

Parity

A parity bit can be sent along with regular data bits to detect data transmission errors. Select Even if the parity bit is set to 0, and the number of 1's in data bits is even. Select Odd if the parity bit is set to 0, and the number of 1's in data bits is odd. Select None if you do not want to send a parity bit with your data bits in transmission. Select Mark to add a mark as a parity bit to be sent along with the data bits. Select Space to add a Space as a parity bit to be sent with your data bits. The options are None, Even, Odd, Mark, and Space.

Stop Bits

A stop bit indicates the end of a serial data packet. Select 1 Stop Bit for standard serial data communication. Select 2 Stop Bits if slower devices are used. The options are 1 and 2.

Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None and Hardware RTS/CTS.

VT-UTF8 Combo Key Support

Select Enabled to enable VT-UTF8 Combination Key support for ANSI/VT100 terminals. The options are Disabled and Enabled.

Recorder Mode

Select Enabled to capture the data displayed on a terminal and send it as text messages to a remote server.

The options are Disabled and Enabled.

Resolution 100x31

Select Enabled for extended-terminal resolution support. The options are Disabled and Enabled.

Legacy OS Redirection Resolution

Use this feature to select the number of rows and columns used in Console Redirection for legacy OS support. The options are 80x24 and 80x25.

Putty KeyPad

This feature selects Function Keys and KeyPad settings for Putty, which is a terminal emulator designed for the Windows OS. The options are VT100, LINUX, XTERMR6, SC0, ESCN, and VT400.

Redirection After BIOS POST

Use this feature to enable or disable legacy Console Redirection after BIOS POST. When set to Bootloader, legacy Console Redirection is disabled before booting the OS. When set to Always Enable, legacy Console Redirection remains enabled when booting the OS. The options are Always Enable and BootLoader.

Legacy Console Redirection

Legacy Serial Redirection Port

Use this feature to select a COM port to display redirection of Legacy OS and Legacy OPROM messages. The options are COM1 and SOL/COM2.

Serial Port for Out-of-Band Management/Windows Emergency Management Services (EMS)

Console Redirection EMS

Select Enabled to use a COM port selected by the user for EMS Console Redirection. The options are Disabled and Enabled.

4.2.14.3.3 Console Rediredtion Settings (Available when the Console Redirection EMS is set to Enable)

This feature allows you to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Out-of-Band Mgmt Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are COM1 and SOL/COM2.

Terminal Type

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII character set. Select VT100+ to add color and function key support. Select ANSI to use the extended ASCII character set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, VT-UTF8, and, ANSI.

Bits Per Second EMS

This feature sets the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 57600, and 115200 (bits per second).

Flow Control EMS

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options are None, Hardware RTS/CTS, and Software Xon/Xoff.

The following information displays:

Data Bits EMS, Parity EMS, Stop Bits EMS

4.2.15 ACPI Settings

WHEA Support

Select Enabled to support the Windows Hardware Error Architecture (WHEA) platform and provide a common infrastructure for the system to handle hardware errors within the Windows OS environment to reduce system crashes and to enhance system recovery and health monitoring. The options are Disabled and Enabled.

High Precision Event Timer

Select Enabled to activate the High Precision Event Timer (HPET) that produces periodic interrupts at a much higher frequency than a Real-time Clock (RTC) does in synchronizing multimedia streams, providing smooth playback and reducing the dependency on other timestamp calculation devices, such as an x86 RDTSC Instruction embedded in the CPU. The High Performance Event Timer is used to replace the 8254 Programmable Interval Timer. The options are Disabled and Enabled.

4.2.16 Trusted Computing (Available when a TPM device is installed and detected by the BIOS)

This motherboard supports TPM 1.2 and 2.0. The following Trusted Platform Module (TPM) information will display if a TPM 2.0 module is detected:

- Vendor Name
- Firmware Version

Security Device Support

If this feature and the TPM jumper on the motherboard are both set to Enabled, onboard security devices will be enabled for TPM (Trusted Platform Module) support to enhance data integrity and network security. Please reboot the system for a change on this setting to take effect. The options are Disable and Enable.

- Active PCR Bank
- Available PCR banks
- SHA256 PCR Bank

If the feature above is set to Enable, SHA-1 PCR Bank and SHA256 PCR Bank will become available for configuration:

SHA-1 PCR Bank

Use this feature to disable or enable the SHA-1 Platform Configuration Register (PCR) bank for the installed TPM device. The options are Disabled and Enabled.

SHA256 PCR Bank

Use this feature to disable or enable the SHA256 Platform Configuration Register (PCR) bank for the installed TPM device. The options are Disabled and Enabled.

Pending Operation

Use this feature to schedule a TPM-related operation to be performed by a security device for system data integrity. Your system will reboot to carry out a pending TPM operation. The options are None and TPM Clear.

Note: Your system will reboot to carry out a pending TPM operation.

Platform Hierarchy (for TPM Version 2.0 and above)

Select Enabled for TPM Platform Hierarchy support which will allow the manufacturer to utilize the cryptographic algorithm to define a constant key or a fixed set of keys to be used for initial system boot. These early boot codes are shipped with the platform and are included in the list of "public keys". During system boot, the platform firmware uses the trusted public keys to verify a digital signature in an attempt to manage and control the security of the platform firmware used in a host system via a TPM device. The options are Disabled and Enabled.

Storage Hierarchy

Select Enabled for TPM Storage Hierarchy support that is intended to be used for non-privacysensitive operations by a platform owner such as an IT professional or the end user. Storage Hierarchy has an owner policy and an authorization value, both of which can be set and are held constant (rarely changed) through reboots. This hierarchy can be cleared or changed independently of the other hierarchies. The options are Disabled and Enabled.

Endorsement Hierarchy

Select Enabled for Endorsement Hierarchy support, which contains separate controls to address the user's privacy concerns because the primary keys in the hierarchy are certified by the TPM key or by a manufacturer with restrictions on how an authentic TPM device that is attached to an authentic platform can be accessed and used. A primary key can be encrypted and certified with a certificate created by using TPM2_ ActivateCredential, which allows you to independently enable "flag, policy, and authorization values" without involving other hierarchies. A user with privacy concerns can disable the endorsement hierarchy while still using the storage hierarchy for TPM applications, permitting the platform software to use the TPM. The options are Disabled and Enabled.

PH (Platform Hierarchy) Randomization (for TPM Version 2.0 and above)

Select Enabled for Platform Hierarchy Randomization support, which is used only during the platform developmental stage. This feature cannot be enabled in the production platforms. The options are Disabled and Enabled.

SMCI BIOS-Based TPM Provision Support

Use feature to enable the Supermicro TPM Provision support. The options are Disabled and Enabled.

TXT Support

Intel Trusted Execution Technology (TXT) helps protect against software-based attacks and ensures

protection, confidentiality, and integrity of data stored or created on the system. Use this feature to enable or disable TXT Suppport. The options are Disabled and Enabled.

Note 1: If the option for this feature (TXT Support) is set to Enabled, be sure to dis-able EV DFX (Device Function On-Hide support when it is present in the BIOS for the system to work properly.

Note 2: For more information on TPM, please refer to the TPM manual at http://www.supermicro.com/manuals/other.

4.2.17 HTTP Boot Configuration

HTTP BOOT Configuration

HTTP Boot Policy

Use this feature to set the HTTP boot policy. The options are Apply to all LANs, Apply to each LAN, and Boot Priority #1 instantly.

Priority of HTTP Boot

Instance of Priority 1:

The priority sequence of HTTP Boot. The default setting is 1.

Select IPv4 or IPv6

Use this feature to select which internet protocol the targeted LAN port is boot from IPv4 or IPv6. The options are IPv4 and IPv6.

Boot Description

Press <Enter> and enter a boot description. The maximal length is 20.

Boot URI

This feature allows you to boot the system from a network connection. The maximal length is 128.

Instance of Priority 2: (Available when the HTTP Boot Policy is set to Apply to each LAN or Boot Priority #1 instantly)

The priority sequence of HTTP Boot. The default setting is 0.

4.2.18 iSCSI Configuration

4.2.18.1 Attempt Priority

Attempt Priority

Use this feature to change the priority of iSCSI attempt using the + or - keys. The options are Host Attempt, Redfish Attempt, and Rst Attempt.

Commit Changes and Exit

Use this feature to save all changes and exit the above settings.

4.2.18.2 Host iSCSI Configuration

iSCSI Initiator Name

This feature allows you to enter the unique name of the iSCSI Initiator in IQN format. Once the name of the iSCSI Initiator is entered into the system, configure the proper settings for the following items.

4.2.18.3 Add an Attempt
4.2.18.4 Delete Attempts
4.2.18.5 Change Attempt Order

4.2.19 Intel® i210 Gigabit Netwrok Connection – (MAC address)

4.2.19.1 Firmware Image Properties

The following information will display:

- Option ROM version
- Unique NVM/EEPROM ID
- NVM Version

4.2.19.2 NIC Configuration

Link Speed

This feature allows you to specify the port speed used for the selected boot protocol. The options are Auto Negotiated, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, and 100 Mbps Full.

Wake On LAN

Select Enabled for the Wake_On_LAN support, which will allow the system to "wake up" when an onboard device receives an incoming signal. The options are Disabled and Enabled.

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. Use the keyboard to select a value. The maximal value is 15 (seconds).

UEFI Driver

This feature displays the UEFI driver version.

Adapter PBA

This feature displays the Processor Bus Adapter (PBA) model number. The PBA number is a nine digit number (i.e., 010B00-000) located near the serial number.

Device Name

This feature displays the adapter device name.

Chip Type

This feature displays the network adapter chipset name.

PCI Device ID

This feature displays the device ID number.

PCI Address

This feature displays the PCI address for this computer. PCI addresses are three two-digit hexadecimal numbers.

Link Status

This feature displays the connection status.

MAC Address

This feature displays the MAC address for this computer. Mac addresses are six two-digit hexadecimal numbers.

Virtual MAC Address

This feature displays the Virtual MAC address for this computer. Mac addresses are six two-digit hexadecimal numbers.

4.2.20 TLS Authenticate Configuration

This submenu allows you to configure Transport Layer Security (TLS) settings.

4.2.20.1 Server CA Configuration / Client Certification Configuration

4.2.20.2 Enroll Certification

4.2.20.3 Enroll Certification Using File

Use this feature to enroll certification from a file.

Certification GUID (Global Unique Identifier)

Press <Enter> and input the certification GUID

4.2.20.4 Commit Changes and Exit

Use this feature to save all changes and exit TLS settings.

4.2.20.5 Discard Changes and Exit

Use this feature to discard all changes and exit TLS settings.

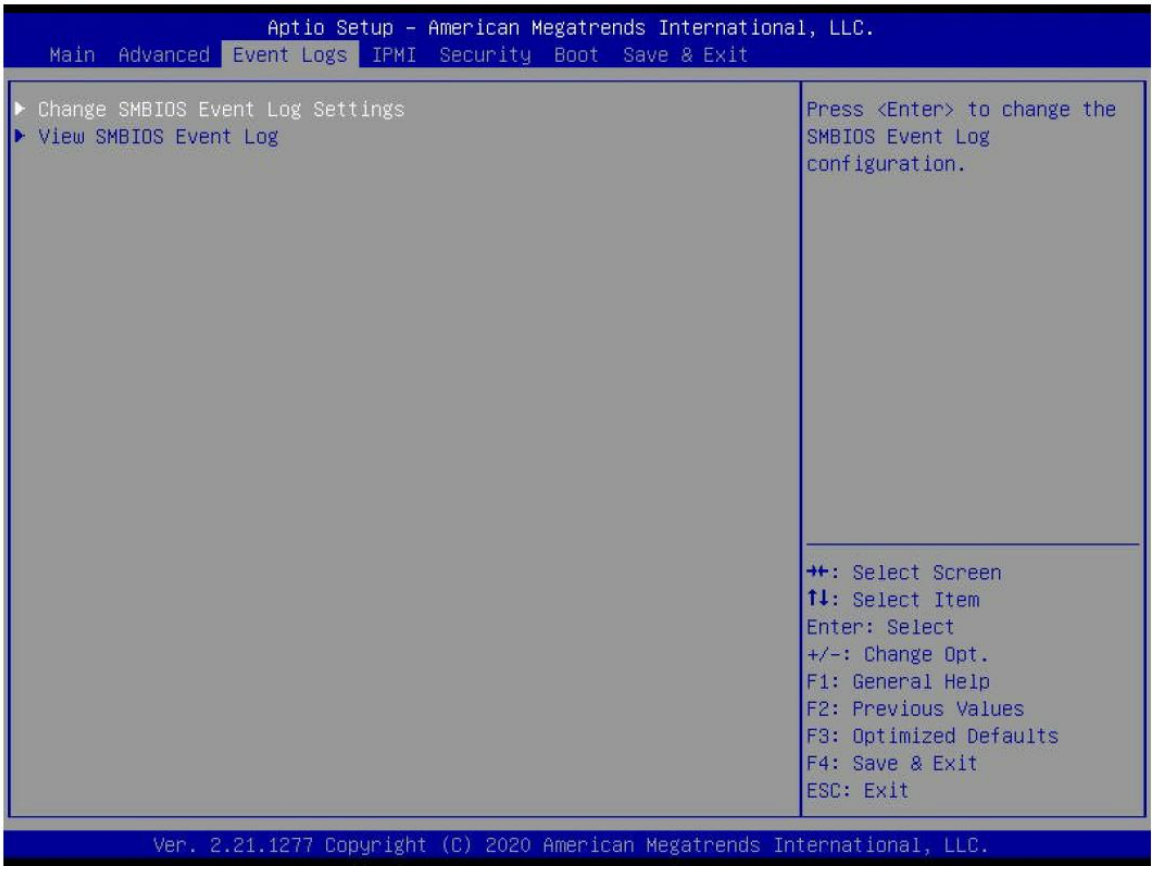
4.2.20.6 Delete Certification

4.2.21 Driver Health

This feature provides health status for the drivers and controllers.

4.3 Event Logs

Use this feature to configure Event Log settings.



4.3.1 Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

Change this feature to enable or disable all features of the SMBIOS Event Logging during system boot. The options are Disabled and Enabled.

*If this feature is set to Enable, the following features will become available for configuration:

Erasing Settings

Erase Event Log

If No is selected, data stored in the event log will not be erased. Select Yes, Next Reset, data in the event log will be erased upon next system reboot. Select Yes, Every Reset, data in the event log will be erased upon every system reboot. The options are No, (Yes, Next reset), and (Yes, Every reset).

When Log is Full

Select Erase Immediately for all messages to be automatically erased from the event log when the event log memory is full. The options are Do Nothing and Erase Immediately.

SMBIOS Event Log Standard Settings

Log System Boot Event

This option toggles the System Boot Event logging to enabled or disabled. The options are Enabled and Disabled.

MECI

The Multiple Event Count Increment (MECI) counter counts the number of occurences that a duplicate event must happen before the MECI counter is incremented. This is a numeric value. The default value is 1.

METW

The Multiple Event Time Window (METW) defines the number of minutes that must pass between duplicate log events before MECI is incremented. This is in minutes, from 0 to 99. The default value is 60.

Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

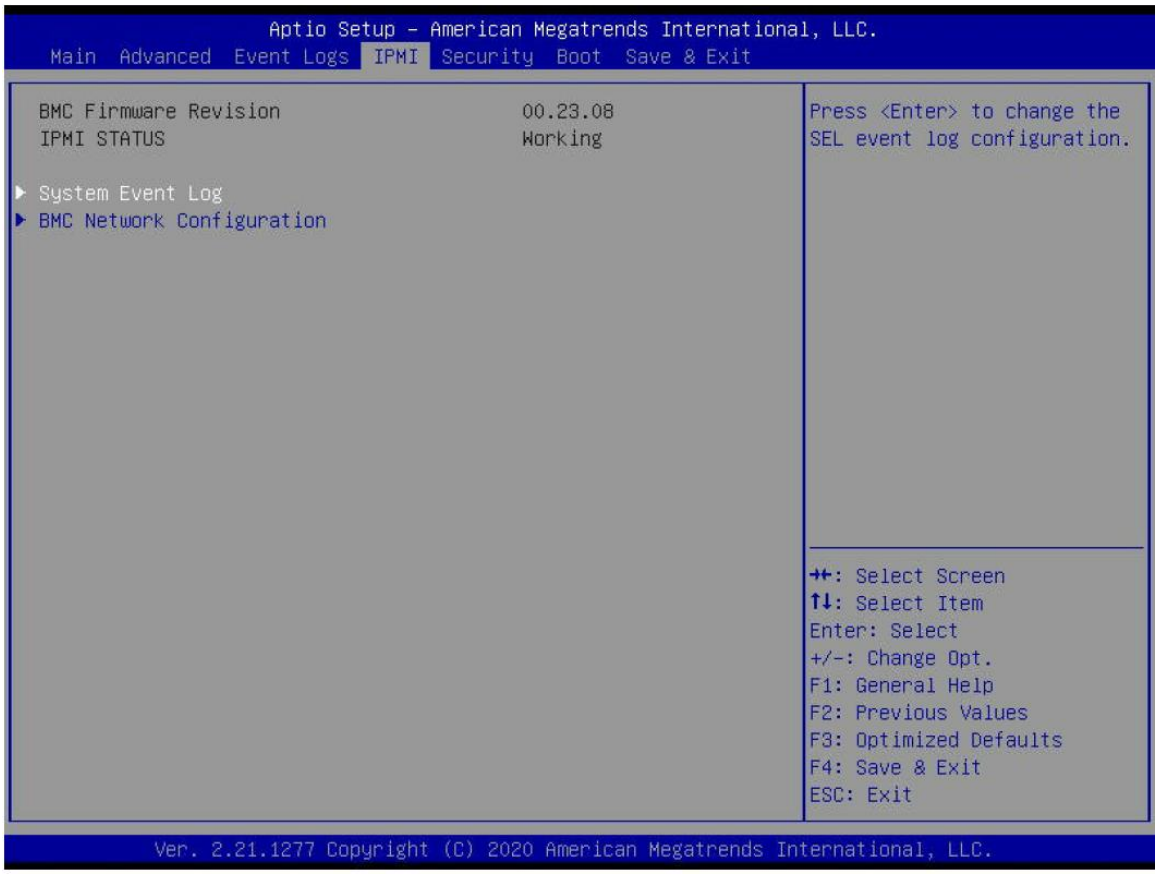
4.3.2 View SEMBIOS Event Log

Select this submenu and press enter to see the contents of the SMBIOS event log. The following categories will be displayed:

DATE / TIME / ERROR CODE / SEVERITY

4.4 IPMI

Use this feature to configure Intelligent Platform Management Interface (IPMI) settings



BMC Firmware Revision

This feature indicates the IPMI firmware revision used in your system.

IPMI STATUS (Baseboard Management Controller)

This feature indicates the status of the IPMI firmware installed in your system.

4.4.1 System Event Log

Enabling/Disabling Options

SEL Components

Select Enabled for all system event logging at boot up. The options are Disabled and Enabled.

Erasing Settings

Erase SEL

Select Yes, On next reset to erase all system event logs upon next system reboot. Select Yes, On every reset to erase all system event logs upon each system reboot. Select No to keep all system event logs after each system reboot. The options are No, (Yes, On next reset), and (Yes, On every reset).

When SEL is Full

This feature allows you to decide what the BIOS should do when the system event log is full. Select Erase Immediately to erase all events in the log when the system event log is full. The options are Do Nothing and Erase Immediately.

Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

4.4.2 BMC Network Configuration

BMC Network Configuration

Update IPMI LAN Configuration

Select Yes for the BIOS to implement all IP/MAC address changes at the next system boot.

The options are No and Yes.

*If the feature above is set to Yes, the following features will become available for configuration:

Configure IPv4 Support

This section displays configuration features for IPV4 support.

IPMI LAN Selection

This feature allows you to select the type of the IPMI LAN. The default setting is Failover.

IPMI Network Link Status

This feature displays the status of the IPMI network link for this system. The default setting is Shared LAN.

Configuration Address Source

This feature allows you to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server in the network that is attached to and request the next available IP address for this computer. The options are Static and DHCP.

**If the feature above is set to Static, the following features will become available for configuration:*

Station IP Address

This feature displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253). Press <Enter> to change the setting.

Subnet Mask

This feature displays the sub-network that this computer belongs to. The value of each three-digit number separated by dots should not exceed 255. Press <Enter> to change the setting.

Station MAC Address

This feature displays the Station MAC address for this computer. Mac addresses are six two-digit hexadecimal numbers.

Gateway IP Address

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.31.0.1). Press <Enter> to change the setting.

VLAN

This feature displays the virtual LAN settings. The options are Disable and Enable.

VLAN ID (Available when the VLAN is set to Enable)

Use this feature to create a new LAN ID by using an existing VLAN or creating a new VLAN ID. Enter a valid value between 0 - 4094.

Configure IPv6 Support

This section displays configuration features for IPV6 support.

IPv6 Address Status

This feature displays the IPv6 address status.

IPv6 Support

Use this feature to enable IPv6 support. The options are Enabled and Disabled.

**If the feature above is set to Enabled, the following features will become available for configuration:*

Configuration Address Source

This feature allows you to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server in the network that is attached to and request the next available IP address for this computer. The options are Static and DHCP.

**If the feature above is set to Static, the following features will become available for configuration:*

Station IPv6 Address

This feature displays the station IPv6 address.

Prefix Length

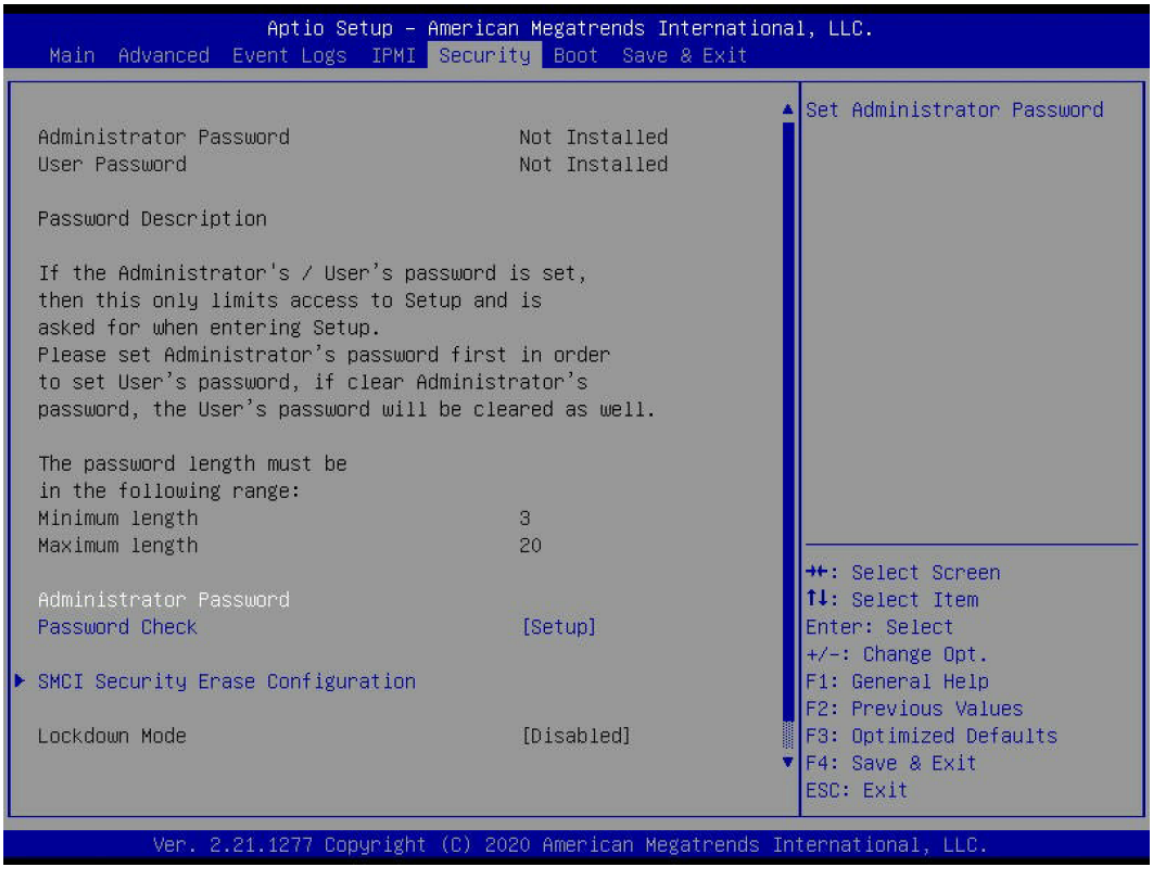
This feature displays the prefix length.

IPv6 Router IP Address

This feature displays the IP address of the IPv6 router.

4.5 Security

This submenu allows you to configure the following security settings for the system.



Administrator Password

Press <Enter> to create a new or change an existing administrator password.

Password Check

Select Setup for the system to check for a password at Setup. Select Always for the system to check for a password at bootup or upon entering the BIOS Setup utility. The options are Setup and Always.

4.5.1 SMCI Securuty Erase Configuration

Note: This submenu becomes configurable when a storage device has been plugged into the motherboard. This section allows you to configure the SMCI-proprietary Security Erase settings. When this section is selected, the following features will display:

- **HDD Name:** This feature displays the name of the HDD/SATA drive that is connected to the SMCI Security Erase Configuration submenu.
- **HDD Serial Number:** This feature displays the serial number of the HDD/SATA device that is connected to the SMCI Security Erase Configuration submenu.
- **Security Erase Mode:** This feature displays the security erase mode used in the system.
- **Estimated Time:** This feature displays the estimate time needed to perform the selected Security Erase features.
- **Admin Pwd (Administrator Password) Status:** This feature displays the status of the administrator password.

Security Function

Use this feature to configure the security settings for the HDD/SATA device. Select Security Erase to enter a SATA user password to allow you to erase the password and the contents previously stored in the HDD/SATA device. Select Security Erase - Without Password to use the manufacturer default password "111111111" as the SATA user password and allow you to erase the contents of the HDD/SATA device by using this default password. The options are Disabled, Security Erase, and Set Password.

- **HDD User Pwd (Password) Status:** This feature indicates if a password has been set as a SATA user password which will allow you to configure SMCI Security Erase settings on the HDD (SATA) device by using this SATA user password.

Password

Use this feature to set the SATA user password which will allow you to configure the SMCI Security Erase settings by using the SATA user password.

Hard Drive Security Frozen

Use this feature to disable or enable the BIOS security frozen command to SATA and NVMe devices. The options are Enabled and Disabled.

Password Check

Select Setup for the system to check for a password at Setup. Select Always for the system to check for a password at bootup or upon entering the BIOS Setup utility. The options are Setup and Always.

4.5.2 Secure Boot

Note: For detailed instructions on how to configure Security Boot settings, please refer to the Security Boot Configuration User's Guide posted on the web page under the link: http://www.supermicro.com/support/manuals/.

When you select this submenu and press the <Enter> key, the following items will display:

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

Select Enabled for Secure Boot flow control. This feature is available when the platform key (PK) is pre-registered, the platform operates in the user mode, and CSM is disabled in the Setup utility. The options are Disabled and Enabled.

Secure Boot Mode

This feature allows selection of the Secure Boot Mode between Standard and Custom. Selecting Custom enables users to change the Image Execution Policy and manage Secure Boot Keys. The options are Custom and Standard.

CSM Support

Select enabled to support the Compatibility Support Module (CSM), which provides compatibility support for traditional legacy BIOS for system boot. The options are Disabled and Enabled.

Note: It is recommended to disable this feature. If this feature is set to Enabled, the Intel Trusted Execution Technology (TXT) will be invalid.

**If the feature of Secure Boot Mode is set to Custom, the following features will become available for configuration:*

4.5.2.1 Enter Audit Mode

Press <Enter> to enter the audit mode workflow. It will result in erasing of Platform Key (PK) variables and reset system to the Setup/Audit mode.

4.5.2.2 Enter Deployed Mode / Exit Deployed Mode

Press <Enter> button to switch between Deployment and User Mode.

4.5.3 Key Management (Available when Secure Boot Mode is set to Custom)

This submenu allows you to configure the following Key Management settings.

Vendor Keys

This feature displays the Vendor Keys. The default is Modified.

Provision Factory Default Keys

Select Enabled to install the default Secure Boot keys set by the manufacturer. The options are Disabled and Enabled.

4.5.3.1 Restore Factory Keys

Use this feature to Install factory default secure boot key databases. The options are Yes and No. Select Yes will reset system to the User mode.

4.5.3.2 Reset to Setup Mode

Use this feature to delete all secure boot key databases from NVRAM. Select Yes will reset system to the Setup mode.

4.5.3.3 Export Secure Boot variable

This feature allows you to copy NVRAM content of secure boot variables to files in a root folder on a file system device.

4.5.3.4 Enroll EFI Image

This feature allows the image to run in the secure boot mode. Enroll SHA256 Hash certificate of a PE image into the Authorized Signature Database (DB).

Device Guard Ready

4.5.3.5 Remove 'UEFI CA' from DB

Use this feature to remove the Microsoft UEFI CA certificate from the database.

4.5.3.6 Restore DB defaults

Select Yes to restore DB variables to factory defaults.

Secure Boot Variable / Size / Keys / Key Source

4.5.3.7 Platform Key(PK)

This feature allows you to configure the settings of the Platform Key (PK).

Details

Review details on current settings of the PK.

Export

This feature allows you to export the PK to an available file system.

Update

Select Yes to load the new PK from the manufacturer's defaults. Select No to load the PK from a file.

Delete

Select Yes to confirm deletion of the PK from NVRAM.

4.5.3.8 Key Exchange Keys

Details

Review details on current settings of the Key Exchange Keys.

Export

This feature allows you to export Key Exchange Keys to an available file system.

Update

Select Yes to load the Key Exchange Keys from the manufacturer's defaults. Select No to load thenKey Exchange Keys from a file.

Append

Select Yes to add the Key Exchange Keys from the manufacturer's defaults list to the existing Key Exchange Keys. Select No to load the Key Exchange Keys from a file.

Delete

Select Yes to delete the Key Exchange Keys. Select No to delete only a certificate from the key database.

4.5.3.9 Authorized Signatures

Details

Review details on current settings of the Authorized Signatures (DB).

Export

This feature allows you to export authorized signatures to an available file system.

Update

Select Yes to load the factory default DB. Select No to load the DB from a external file.

Append

Select Yes to add the database from the manufacturer's defaults to the existing DB. Select No to load the DB from a file.

Delete

Select Yes to delete the DB. Select No to delete only a certificate from the DB.

4.5.3.10 Forbidden Signatures

Details

Review details on current settings of the Forbidden Signatures (DBX).

Export

This feature allows you to export the DBX to an available file system.

Update

Select Yes to load the DBX factory defaults. Select No to load it from an external file.

Append

Select Yes to add the DBX from the manufacturer's defaults to the existing DBX. Select No to load the DBX from a file.

Delete

Select Yes to delete the DBX. Select No to delete only a certificate from the DBX.

4.5.3.11 Authorized TimeStamps

Details

Review details on current settings of the Authorized TimeStamps (DBT).

Export

This feature allows you to export the DBT to an available file system.

Update

Select Yes to load the DBT from the manufacturer's defaults. Select No to load the DBT from a file.

Append

Select Yes to add the DBT from the manufacturer's defaults list to the existing DBT. Select No to load the DBT from a file.

Delete

Select Yes to delete the DBT. Select No to delete only a certificate from the key database.

4.5.3.12 OsRecovery Signature

This feature uploads and installs an OsRecovery Signature (DBR). You may insert a factory default key or load from a file. The file formats accepted are:

1) Public Key Certificate
   a. EFI_SIGNATURE_LIST
   b. EFI_CERT_X509 (DER Encoded)
   c. EFI_CERT_RSA2048 (bin)
   d. EFI_CERT_SHAXXX
2) Authenticated UEFI Variable
3) EFI PE/COEF Image (SHA256)

When prompted, select Yes to load Factory Defaults or No to load from a file.

Details

Review details on current settings of the DBR.

Export

This feature allows you to export the DBR to an available file system.

Update

Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file.

Append

Select Yes to add the DBR from the manufacturer's defaults list to the existing DBR. Select No to load the DBR from a file.

Delete

Select Yes to delete the DBR. Select No to delete only a certificate from the key database.

4.5.4 TCG Storage Device Security Configuration

4.5.5 Storage Device

Note: The feature shown here is dependent on the storage device plugged into the motherboard.

4.5.6 Password Configuration

Information for the following is displayed:

- **Security Subsystem Class**
- **Security Supported**
- **Security Enabled**
- **Security Locked**
- **Security Frozen**
- **User Pwd Status**
- **Admin Pwd Status**

4.5.7 Set Admin Passwrod

Press <Enter> to create a new admin password.

4.5.8 Set User Passwrod

Press <Enter> to create a new user password.

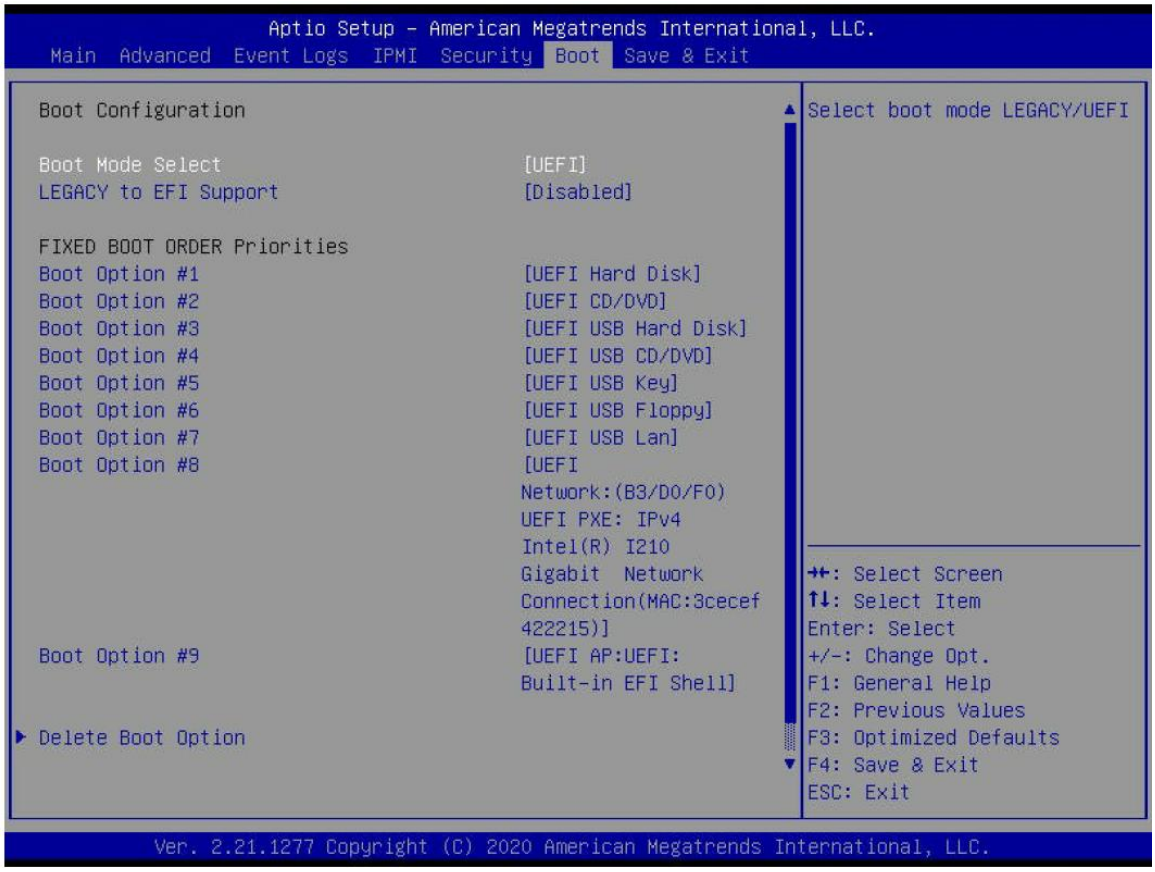
Note: This feature is available when the Admin Password has been activated.

Device Reset

Reset the device using 32 byte PSID (Physical Security Identification) value of the device.

4.6 Boot

Use this feature to configure Boot settings.



Boot Mode Select

Use this item to select the type of device that the system is going to boot from. The options are Legacy, UEFI, and Dual.

Legacy to EFI Support

Select Enabled to boot EFI OS support after Legacy boot order has failed. The options are Disabled and Enabled.

Fixed Boot Order Priorities

This option prioritizes the order of bootable devices that the system boots from. Press <Enter> on each entry from top to bottom to select devices.

Legacy Boot Option #1-#8

These features display when Boot mode select is set to Legacy. The options are Hard Disk, CD/DVD, USB Hard Disk, USB CD/DVD, USB Key, USB Floppy, USB LAN, and Network.

UEFI Boot Option #1-#9

These features display when Boot mode select is set to UEFI. The options are UEFI Hard Disk, UEFI CD/DVD, UEFI USB Hard Disk, UEFI USB CD/DVD, UEFI USB Key, UEFI USB Floppy, UEFI USB Lan, UEFI Network, and UEFI AP.

DUAL Boot Option #1-#17

These features display when Boot mode select is set to DUAL. The options contain all options from UEFI and Legacy boot modes.

4.6.1 Delete Boot Option

This feature allows you to select a boot device to delete from the boot priority list.

Delete Boot Option

Use this feature to remove an EFI boot option from the boot priority list.

4.6.2 UEFI Network Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1 - Boot Option #4

4.6.3 UEFI Application Boot Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

**If any storage media is detected, the following features will become available for configuration:*

4.6.4 Add New Boot Option

This feature allows you to add a new boot option to the boot priority features for your system.

Add Boot Option

Use this item to specify the name for the new boot option.

Path for Boot Option

Use this item to enter the path for the new boot option in the format fsx:\path\filename.efi.

Boot Option File Path

Use this item to specify the file path for the new boot option.

Create

Use this item to set the name and the file path of the new boot option.

4.6.5 UEFI USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

4.6.6 USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

4.6.7 UEFI Hard Disk BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

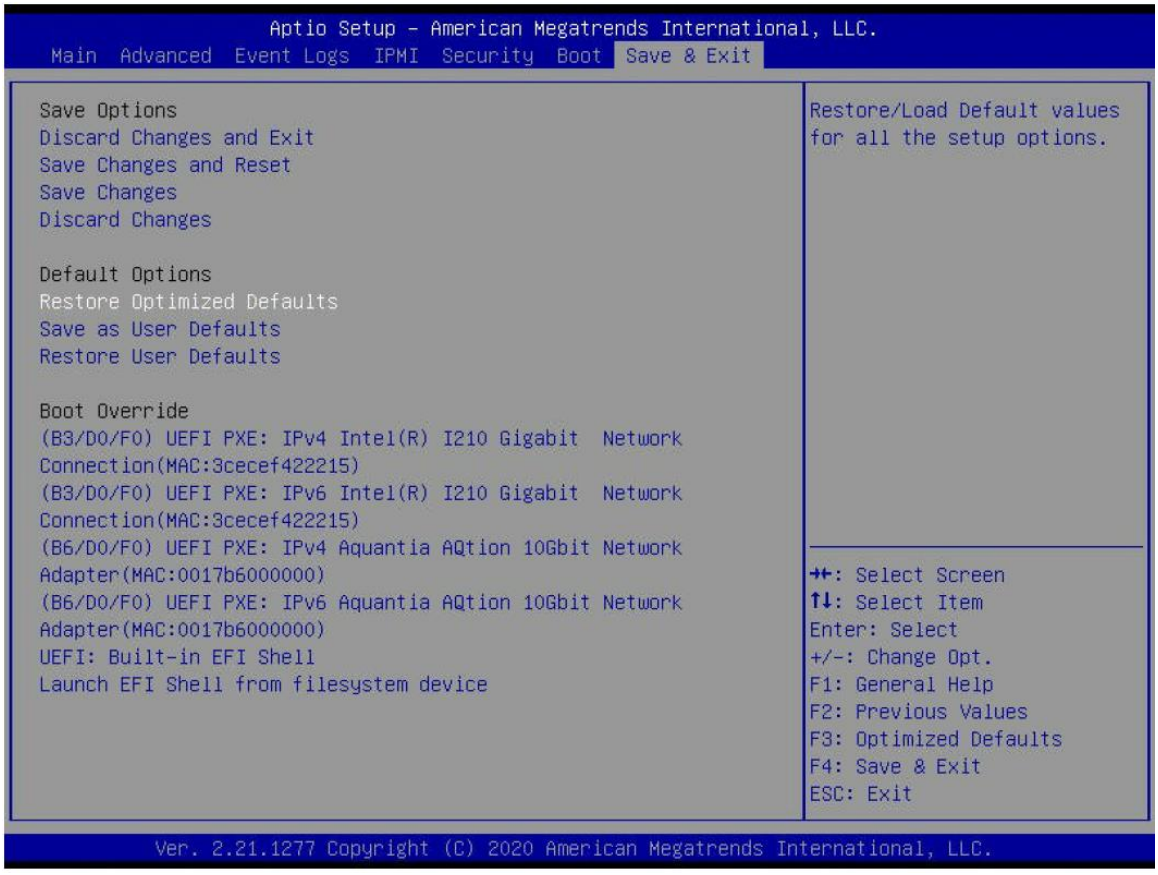
4.6.8 Hard Disk Drive BBS Prioritues

This feature sets the system boot order of detected devices.

- Boot Option #1

4.7 Save & Exit

Select the Save & Exit tab from the BIOS setup screen to configure the settings below:



Save Options

Discard Changes and Exit

Use this feature to quit the BIOS Setup without making any permanent changes to the system configuration and reboot the computer.

Save Changes and Reset

When you have completed the system configuration changes, use this feature to leave the BIOS setup utility and reboot the computer for the new system configuration parameters to take effect.

Save Changes

After completing the system configuration changes, use this feature to save the changes you have made. This will not reset (reboot) the system.

Discard Changes

Press <Enter> to discard all the changes and return to the AMI BIOS utility Program.

Default Options

Restore Optimized Defaults

Use this feature to restore/load default values. These are factory settings designed for maximum system stability, but not for maximum performance.

Save as User Defaults

This feature enables the user to save any changes to the BIOS setup for future use.

Restore User Defaults

Use this feature to retrieve user-defined settings that were saved previously.

Boot Override

Listed in this section are other boot options for the system (i.e., Built-in EFI shell). Select an option and press <Enter>. Your system will boot to the selected boot option.

5 Appendix A BIOS POST Codes...

5.1 BIOS POST Codes

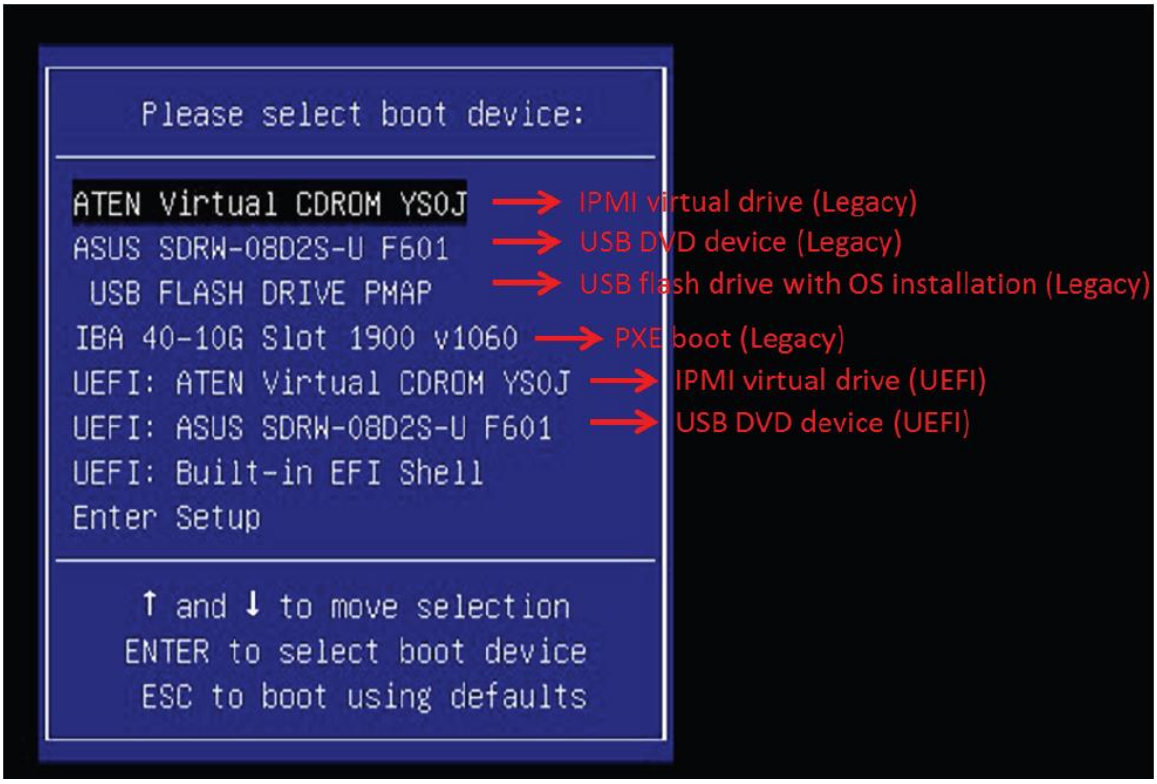
The AMI BIOS supplies additional checkpoint codes, which are documented online at http://www.supermicro.com/support/manuals/ ("AMI BIOS POST Codes User's Guide").
For information on AMI updates, please refer to http://www.ami.com/products/.

6 Appendix B SoftWare

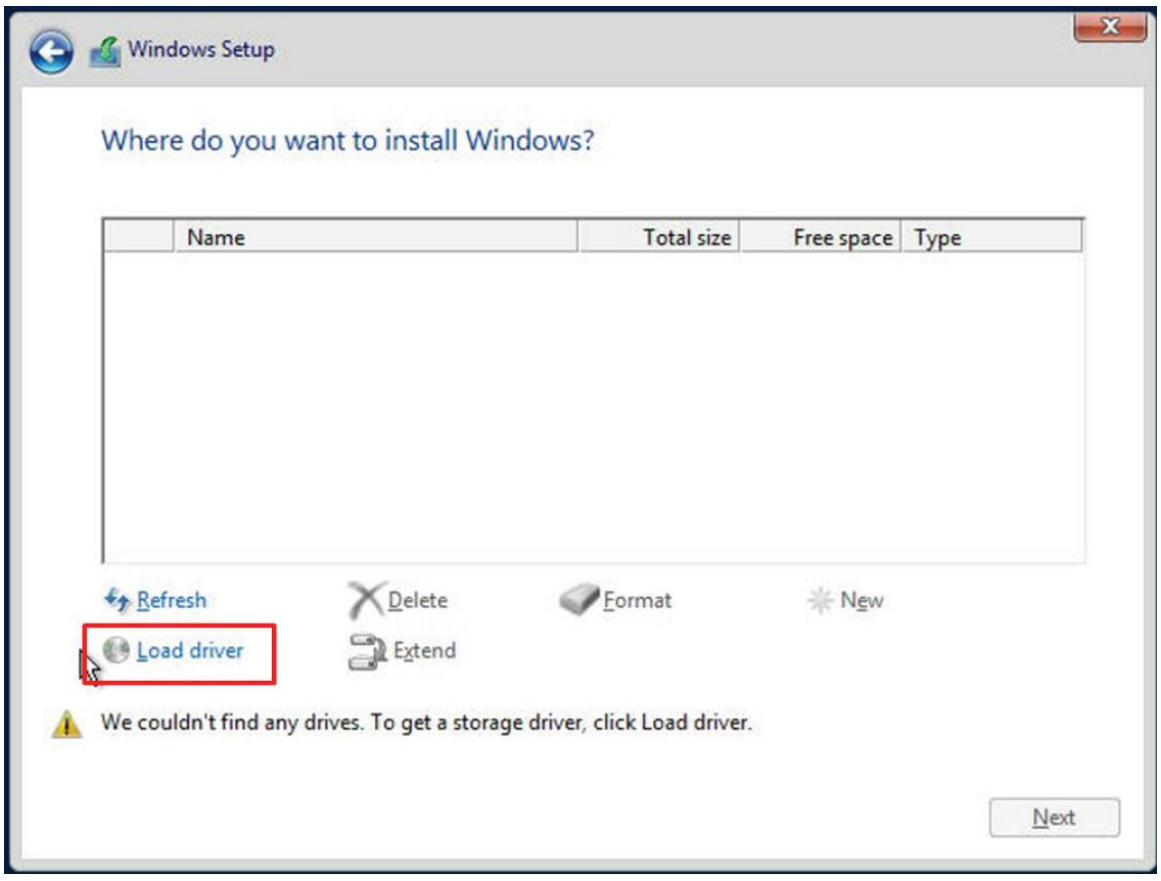
6.1 Microsoft Windows OS Installation

Installing the OS

1. Create a method to access the Microsoft Windows installation ISO file. That can be a USB flash or media drive.
2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.
3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing F11 during the system startup.



4. During Windows Setup, continue to the dialog where you select the drives on which to install Windows. If the disk you want to use is not listed, click on “Load driver” link at the bottom left corner.



To load the driver, browse the USB flash drive for the proper driver files.

• For RAID, choose the SATA/sSATA RAID driver indicated then choose the storage drive on which you want to install it.

• For non-RAID, choose the SATA/sSATA AHCI driver indicated then choose the storage drive on which you want to install it.

5. Once all devices are specified, continue with the installation.
6. After the Windows OS installation has completed, the system will automatically reboot multiple times.

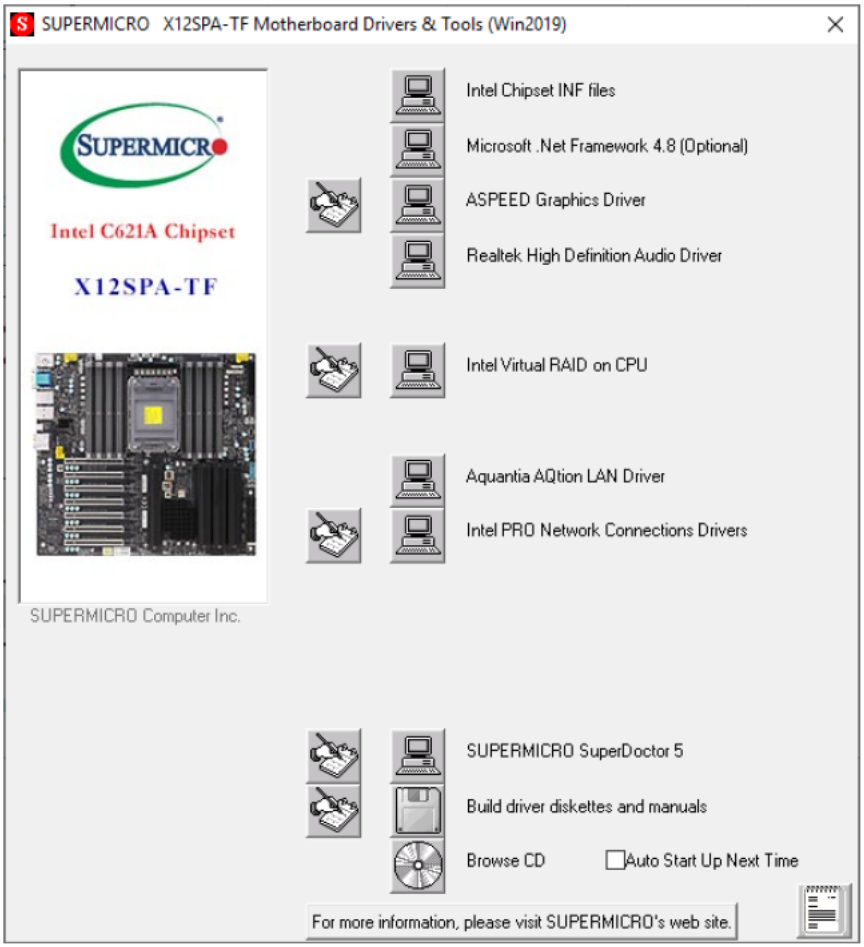
6.2 Driver Installation

The Supermicro website that contains drivers and utilities for your system is at https://www.supermicro.com/wdl/driver. Some of these must be installed, such as the chipset driver.

After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash or media drive. (You may also use a utility to extract the ISO file if preferred.)

Another option is to go to the Supermicro website at http://www.supermicro.com/products/. Find the product page for your motherboard, and "Download the Latest Drivers and Utilities".

Insert the flash drive or disk and the screenshot shown below should appear.

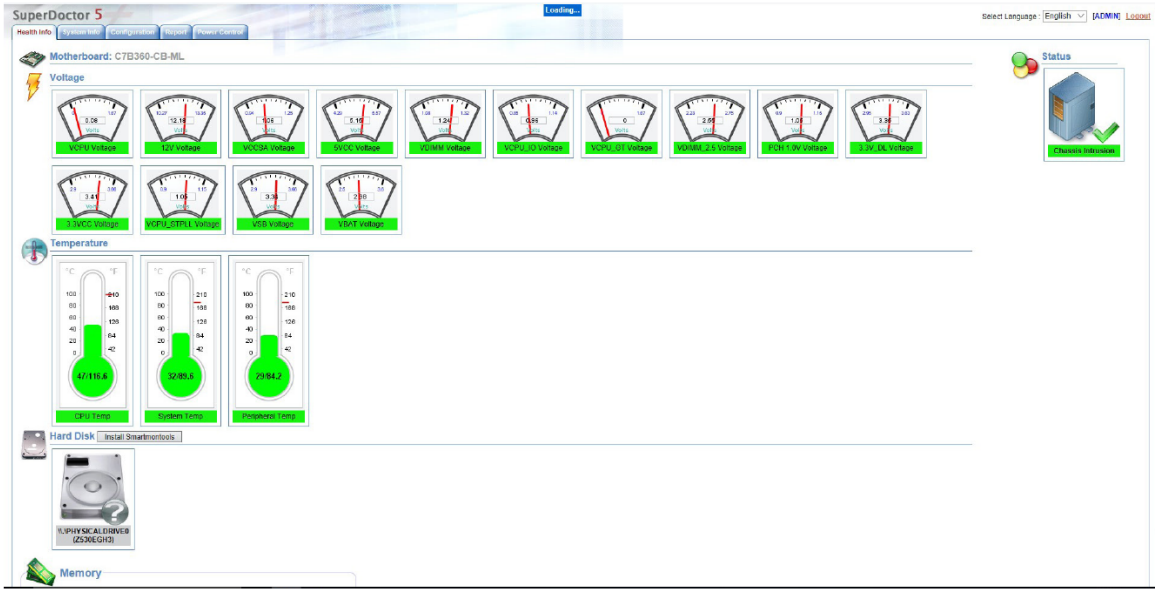


Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to bottom) one at a time. After installing each item, you must re-boot the system before moving on to the next item on the list. The bottom icon with a CD on it allows you to view the entire contents.

6.3 SuperDoctor® 5

The Supermicro SuperDoctor 5 is a program that functions in a command-line or web-based interface for Windows and Linux operating systems. The program monitors such system health information as CPU temperature, system voltages, system power consumption, fan speed, and provides alerts via email or Simple Network Management Protocol (SNMP).

SuperDoctor 5 comes in local and remote management versions and can be used with Nagios to maximize your system monitoring needs. With SuperDoctor 5 Management Server (SSM Server), you can remotely control power on/off and reset chassis intrusion for multiple systems with SuperDoctor 5 or IPMI. SuperDoctor 5 Management Server monitors HTTP and SMTP services to optimize the efficiency of your operation.



6.4 IPMI

The X12SPA-TF supports the Intelligent Platform Management Interface (IPMI). IPMI is used to provide remote access, monitoring and management. There are several BIOS settings that are related to IPMI. For general documentation and information on IPMI, please visit our website at: http://www.supermicro.com/products/nfo/IPMI.cfm.

6.5 Logging into the BMC(Baseboard Management Controller)

Supermicro ships standard products with a unique password for the BMC ADMIN user. This password can be found on a label on the moth