



# SCH-406

IEC-61850-3, IEEE-1613 1U Computer



**User's Manual**

Revision Date: June.11.2021



## Safety Information

### Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

### Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

### Statement

- All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- All trademarks are the properties of the respective owners.
- All product specifications are subject to change without prior notice



## Revision History

Revision	Date (yyyy/mm/dd)	Changes
V1.0	2021/06/11	First release

## Packing List

Item	Description	Q'ty
1	SCH-406 IEC-61850-3, IEEE-1613 1U Computer	1
2	Driver CD	1

## Ordering Information

### SCH-401

2U 19" Smart Grid Fanless Rackmount Server with Intel® 10th Gen. XEON W-1200 ; Core i Processor up to 35W ,2 x GbE, 6 x USB, 2 x DP, 1 x VGA, 1 x DVI-D, 1 x IPMI, 125V DC-IN, 2 x 200W DC/DC Redundant Power Supply, TPM/FTDI support, Operating Temperature -20~+60°C

### SCH400-AA

2U 19" Smart Grid Fanless Rackmount Server with Intel® 10th Gen. XEON W-1200 ; Core i Processor up to 35W ,2 x GbE, 6 x USB, 2 x DP, 1 x VGA, 1 x DVI-D, 1 x IPMI, 9V~36V DC-IN, 2 x 150W DC/DC Redundant Power Supply, Operating Temperature -20~+60°C

### SCH-406

2U 19" Smart Grid Fanless Rackmount Server with Intel® 10th Gen. XEON W-1200 ; Core i Processor up to 35W ,2 x GbE,2 x 10GbE, 6 x USB, 2 x DP, 1 x VGA, 1 x DVI-D, 1 x IPMI, 100~240V AC-IN, 2 x 200W AC/DC Redundant Power Supply, Operating Temperature -20~+60°C

## Optional Ordering Information

INTEL X710 Dual 10GbE SFP+ LAN card

## RoHS Compliance



### Perfectron RoHS Environmental Policy and Status Update

Perfectron is a global citizen for building the digital infrastructure. We are committed to providing green products and services, which are compliant with

European Union RoHS (Restriction on Use of Hazardous Substance in Electronic Equipment) directive 2011/65/EU, to be your trusted green partner and to protect our environment.

In order to meet the RoHS compliant directives, Perfectron has established an engineering and manufacturing task force to implement the introduction of green products. The task force will ensure that we follow the standard Perfectron development procedure and that all the new RoHS components and new manufacturing processes maintain the highest industry quality levels for which Perfectron are renowned.

The model selection criteria will be based on market demand. Vendors and suppliers will ensure that all designed components will be RoHS compliant



<b>Chapter 1 : Production Introduction</b> .....	5
1.1 Specification .....	5
1.2 Front Panel I/O Placement .....	7
1.3 Rear Panel I/O Placement .....	8
1.4 Mechanical Dimensions .....	9
<b>Chapter 2 : Rear I/O Ports</b> .....	10
2.1 LAN/IPMI port .....	10
2.2 VGA/DVI-D port.....	10
2.3 USB3.2 port .....	10
<b>Chapter 3 : System Setup</b> .....	11
3.1 Removing the Top Cover from the Chassis .....	11
3.2 Installing PCIe Card.....	11
3.3 Install the screws on the upper cover .....	12
3.4 2.5" Easy Swap SSD installation .....	12
<b>Chapter 4: AMI BIOS UTILITY</b> .....	13
4.1 Starting .....	13
4.2 Navigation Keys .....	14
4.3 Main Setup .....	14
4.4 Advanced Setup Configurations .....	17
4.5 Event Logs .....	51
4.6 IPMI .....	53
4.7 Security.....	56
4.8 Boot.....	63
4.9 Save & Exit.....	66
<b>Chapter 5: Appendix A BIOS Codes</b> .....	68
5.1 BIOS Error POST (Beep) Codes .....	68
5.2 Additional BIOS POST Codes .....	69
<b>Chapter 6 : Appendix B Software</b> .....	70
6.1 Microsoft Windows OS Installation.....	70
6.2 Driver Installation.....	72
6.3 SuperDoctor® 5 .....	73
6.4 IPMI .....	74
<b>Chapter 7: Appendix C Standardized Warning Statements</b> .....	75
<b>Chapter 8:Appendix D UEFI BIOS Recovery</b> .....	78
8.1 Overview .....	78
8.2 Recovering the UEFI BIOS Image.....	78



8.3 Recovering the BIOS Block with a USB Device ..... 78

## Chapter 1 : Production Introduction

### 1.1 Specification

#### System

CPU	10th Generation Intel® Core™ i9/i7/i5 Processors Intel® Core™ i9-10900TE(20M Cache, up to 4.60 GHz) Intel® Core™ i7-10700TE(16M Cache, up to 4.50 GHz) Intel® Core™ i5-10500TE(12M Cache, up to 3.70 GHz)
Memory type	4 x DDR4 up to 128GB(Unbuffered ECC/non-ECC UDIMM), 2933MHz
Expansion Slot	1 PCI-E 3.0 x16 2 PCI-E 3.0 x4
Storage Device	2 x 2.5" Easy swap HDD/SSD Tray

#### Rear I/O

Power Button	1 with backlight
Indicator	1 HDD backlight
USB	2 x USB 2.0

#### Front I/O

Power Input	100V~240V AC-IN
LAN	2 x RJ45 GbE LAN ; 2 x RJ45 10GbE LAN (by option) ; 1 x IPMI
USB	4 x USB 3.0
DisplayPort	2 x DP
DVI	1 x DVI-D
VGA	1

#### Optional

Dual 10GbE+ Module	INTEL X710 Dual 10GbE SFP+
--------------------	----------------------------

#### Power

Power Input	100V~240V AC-IN, 2 x 200W AC/DC Redundant Power Supply
-------------	--

#### OS support list

Windows	Windows 10 x64
---------	----------------



---

Linux	Ubuntu, Red Hat
-------	-----------------

---

## **Mechanical and Environmental**

---

Dimension	430 x 396 x 88 mm ( W x D x H )
-----------	---------------------------------

---

Operating Temp.	-20 to 60°C
-----------------	-------------

---

Storage Temp.	-40°C to 85°C
---------------	---------------

---

Relative Humidity	5% to 95%, non-condensing
-------------------	---------------------------

---

Certification	CE, FCC, MIL-STD 810G Compliance
---------------	----------------------------------

---

System Design	Fanless
---------------	---------

---

Mounting	2U Rackmount
----------	--------------

---

MIL-STD-810G	Method 507.5, Procedure II (Temperature & Humidity)
--------------	---

---

Test	Method 516.6 Shock-Procedure V Non-Operating (Mechanical Shock)
------	---

---

Method 516.6 Shock-Procedure I Operating (Mechanical Shock)
---

---

Method 514.6 Vibration Category 24/Non-Operating (Category 20 & 24, Vibration)
--

---

Method 514.6 Vibration Category 20/Operating (Category 20 & 24, Vibration)
--

---

Method 501.5, Procedure I (Storage/High Temperature)
--

---

Method 501.5, Procedure II (Operation/High Temperature)
---

---

Method 502.5, Procedure I (Storage/Low Temperature)
---

---

Method 502.5, Procedure II (Operation/Low Temperature)
--

---

Method 503.5, Procedure I (Temperature shock)
---

---

EMC	CE, FCC compliant
-----	-------------------

---

Green Product	RoHS, WEEE compliance
---------------	-----------------------

---

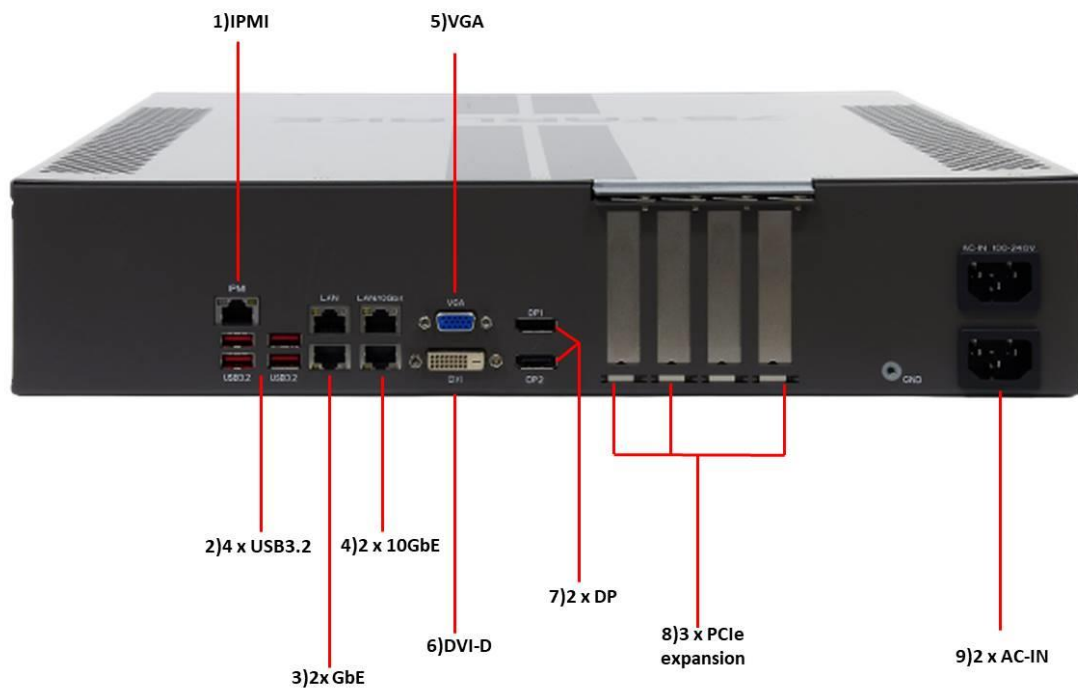
## 1.2 Front Panel I/O Placement



1)	4 x HDD Tray
2)	2 x USB2.0
3)	Power Button

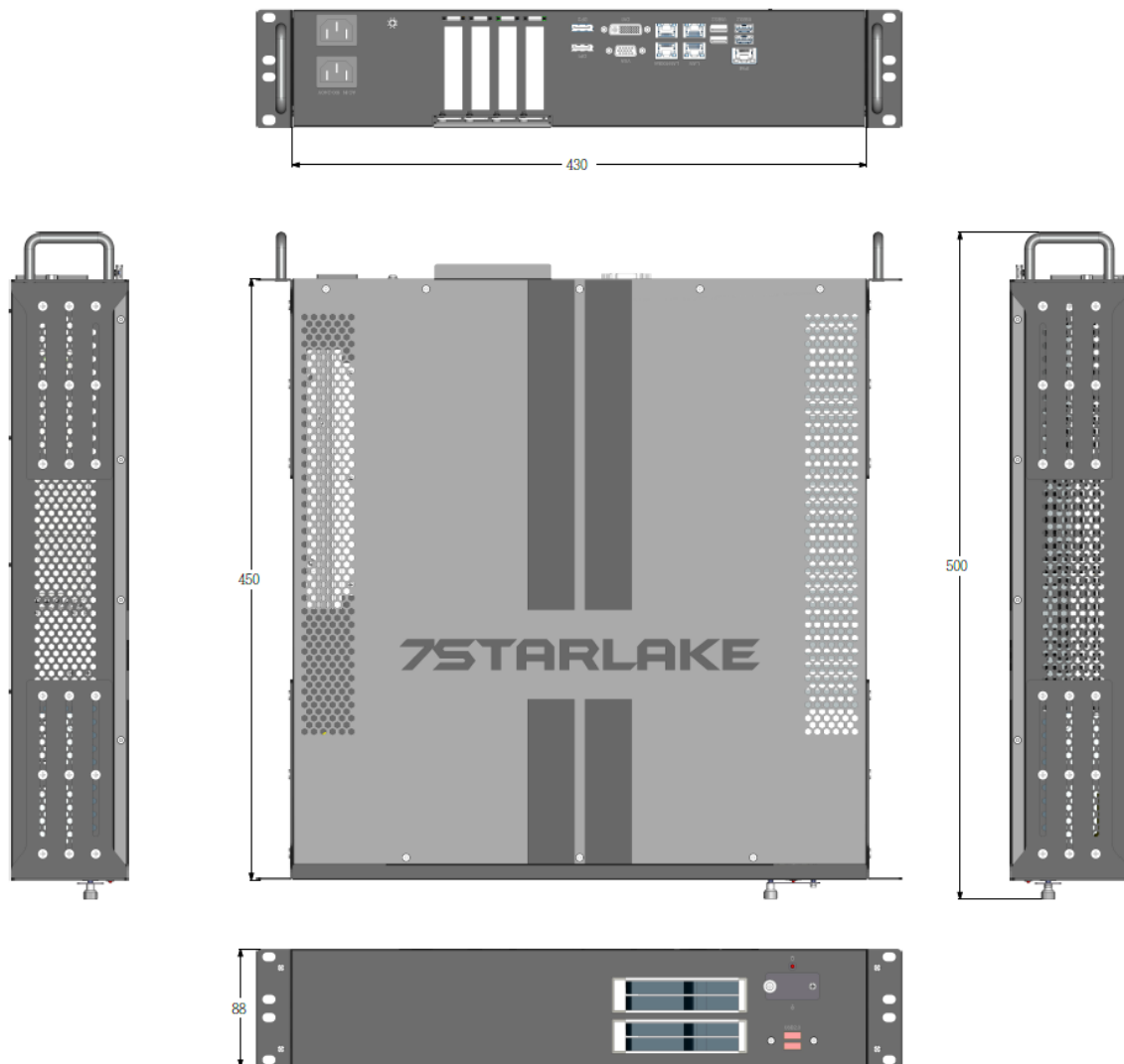


## 1.3 Rear Panel I/O Placement



1)	IPMI
2)	4 x USB3.2
3)	2 x GbE
4)	2 x 10GbE
5)	VGA
6)	DVI-D
7)	2 x DP
8)	3 x PCIe expansion
9)	2 x AC-IN

## 1.4 Mechanical Dimensions



## Chapter 2 : Rear I/O Ports

### 2.1 LAN/IPMI port

LAN Port Pin Definition			
Pin#	Definition	Pin#	Definition
1	TRCT2	13	IETCT
2	TRD2+	14	IET+
3	TRD2-	15	IET-
4	TRD3+	16	
5	TRD3-	17	L1-GRE-
6	TRCT3	18	L1-GRE+
7	TRCT1	19	L2-YEL-
8	TRD1+	20	COMMON
9	TRD1-	21	L2-GRE-
10	TRD4+	22	CG1
11	TRD4-	23	CG2
12	TRCT4		

IPMI LAN Pin Definition			
Pin#	Definition	Pin#	Definition
9	VCC	19	YEL-
10	TX1+	20	YEL+
11	TX1-	21	ORG+/GRN-
12	TX2+	22	ORG-/GRN+
13	TX2-	23	SGND
14	TX3+	24	SGND
15	TX3-	25	SGND
16	TX4+	26	SGND
17	TX4-		
18	GND		

### 2.2 VGA/DVI-D port

A VGA port and a DVI-D port are located next to DisplayPorts 1/2 on the I/O back panel. Use these connections for VGA and DVI displays. The VGA connector is on top and the DVI-D is on the bottom.

DP

There are two DisplayPorts located on the rear I/O back panel. DisplayPort, developed by the VESA consortium, delivers digital display and fast refresh rate. It can connect to virtually any display using a DisplayPort adaptor for devices such as VGA, DVI, or HDMI.

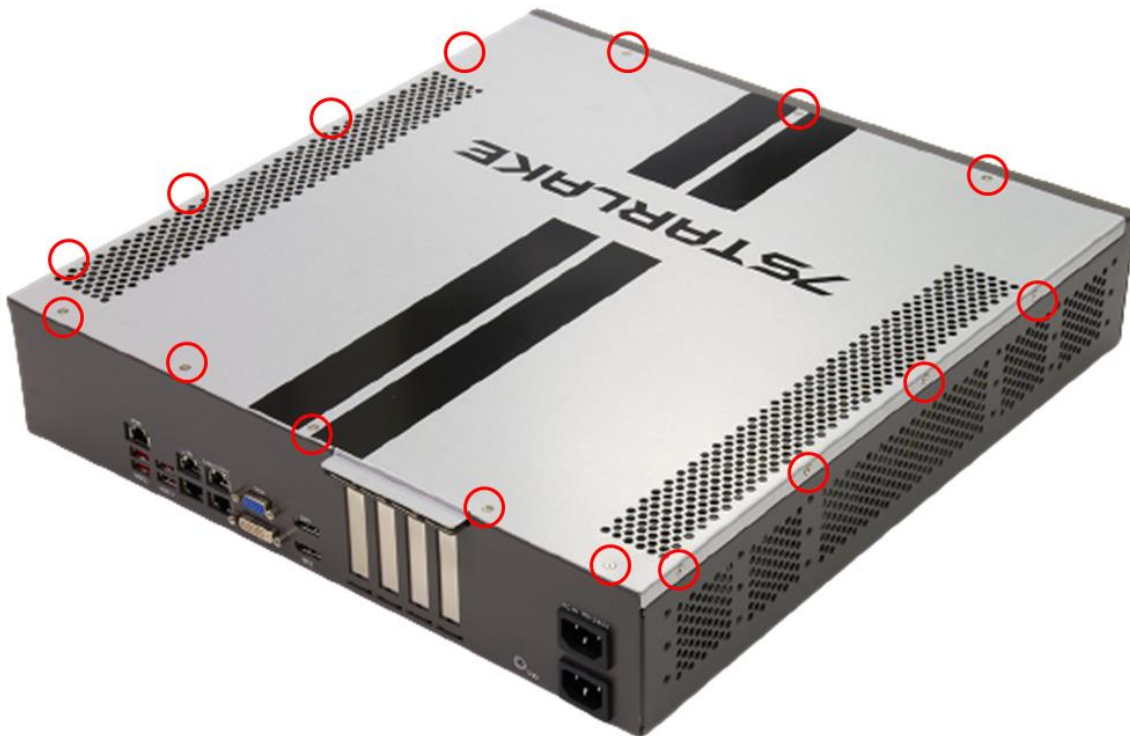
### 2.3 USB3.2 port

Back Panel USB 6/7. 8/9 (3.2) Pin Definitions			
Pin#	Definition	Pin#	Definition
A1	VBUS	B1	Power
A2	USB_N	B2	USB_N
A3	USB_P	B3	USB_P
A4	GND	B4	GND
A5	SS_RX_N3_CON	B5	SS_RX_N4_CON
A6	SS_RX_P3_CON	B6	SS_RX_P4_CON
A7	GND	B7	GND
A8	SS_TX_N3_CON	B8	SS_TX_N4_CON
A9	SS_TX_P3_CON	B9	SS_TX_P4_CON

## Chapter 3 : System Setup

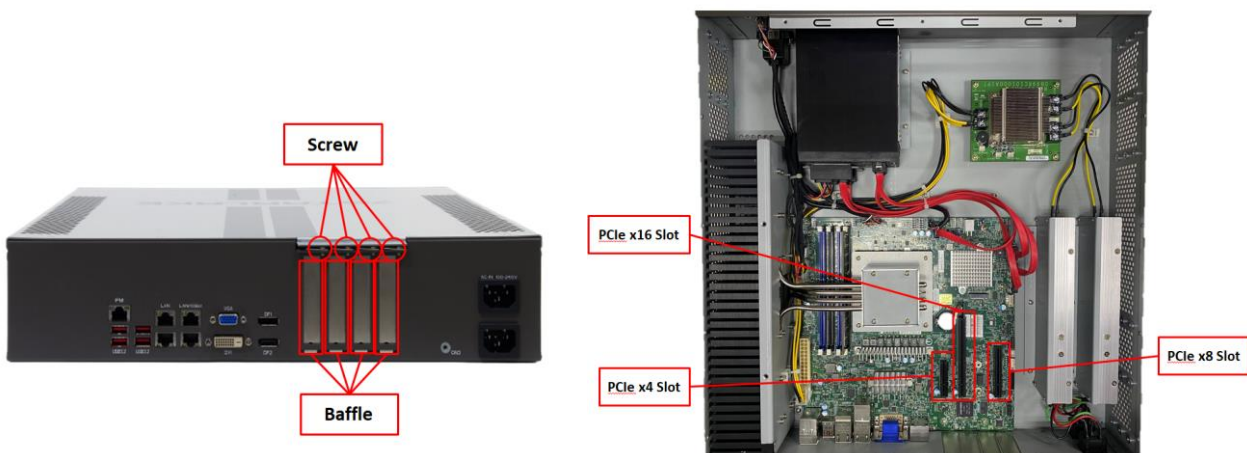
### 3.1 Removing the Top Cover from the Chassis

The sixteen screws on the top and side are used to secure the cover to the chassis. Remove these screws and put them in a safe place for later use



### 3.2 Installing PCIe Card

First, you need to remove the baffle and screws. There is PCIe x4 / 8/16 slot on the motherboard, insert the corresponding PCIe Card and lock the screw



### 3.3 Install the screws on the upper cover

Attach the screws at sixteen locations to complete the installation



### 3.4 2.5" Easy Swap SSD installation

SCH-406 support four 2.5" Easy Swap SSD

- Use Tri-angle security key to open keylock and pull out the 2.5"SSD tray.
- Put 2.5"SSD on the tray and make sure SSD is fixed and push the tray back.
- Use Tri-angle security key to lock tray door.



**Prior to removing the chassis cover, make sure the unit's power is off and disconnected from the power sources to prevent electric shock or system damage.**





## Chapter 4: AMI BIOS UTILITY

This chapter provides users with detailed descriptions on how to set up a basic system configuration through the AMI BIOS setup utility.

### 4.1 Starting

To enter the setup screens, perform the following steps:

- Turn on the computer and press the <Del> key immediately.
- After the <Del> key is pressed, the main BIOS setup menu displays. Other setup screens can be accessed from the main BIOS setup menu, such as the Chipset and Power menus.

## 4.2 Navigation Keys

The BIOS setup/utility uses a key-based navigation system called hot keys. Most of the BIOS setup utility hot keys can be used at any time during the setup navigation process.

Some of the hot keys are <F1>, <F10>, <Enter>, <ESC>, and <Arrow> keys.

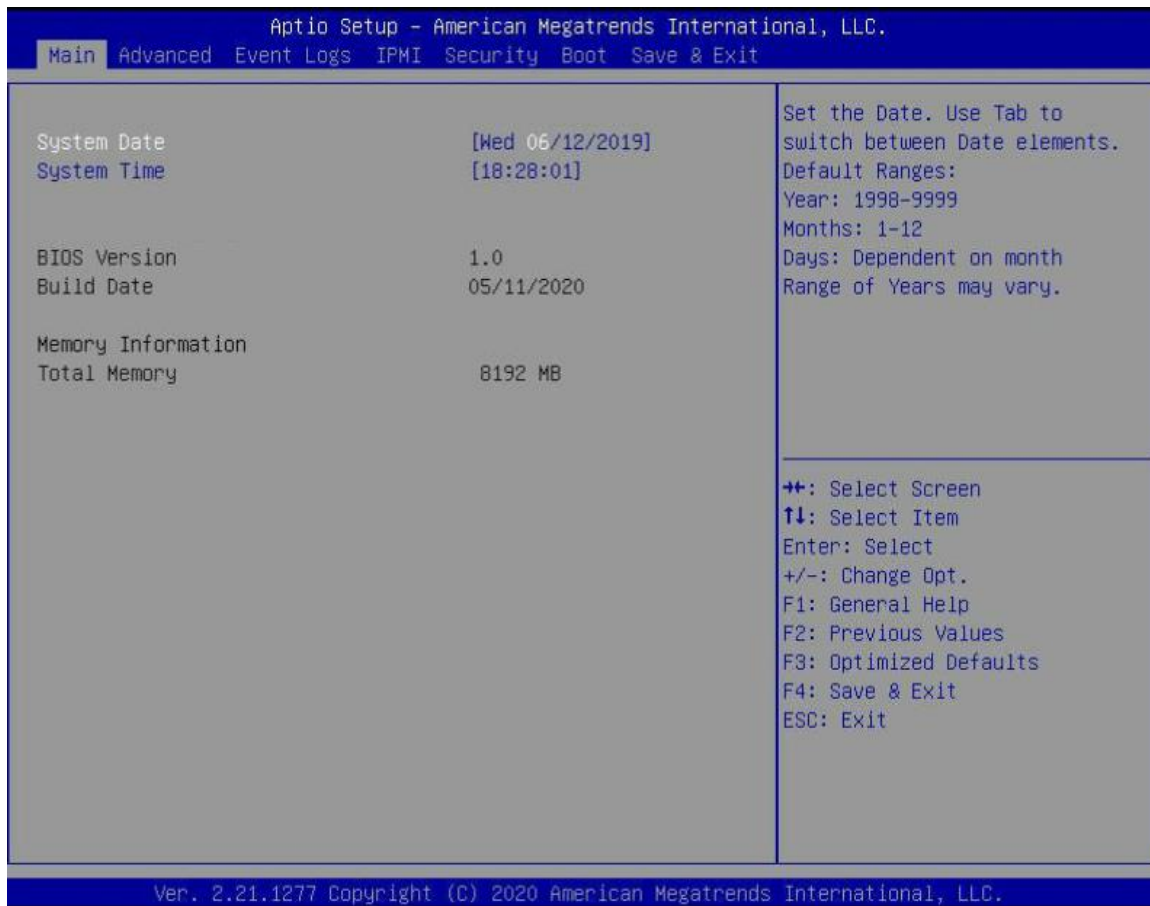


Some of the navigation keys may differ from one screen to another.

Left/Right	The Left and Right <Arrow> keys moves the cursor to select a menu.
Up/Down	The Up and Down <Arrow> keys moves the cursor to select a setup screen or sub-screen.
+– Plus/Minus	The Plus and Minus <Arrow> keys changes the field value of a particular setup setting.
Tab	The <Tab> key selects the setup fields.
F1	The <F1> key displays the General Help screen.
F10	The <F10> key saves any changes made and exits the BIOS setup utility.
Esc	The <Esc> key discards any changes made and exits the BIOS setup utility.
Enter	The <Enter> key displays a sub-screen or changes a selected or highlighted option in each menu.

## 4.3 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:



The Main BIOS setup screen has two main frames. The left frame displays all the options that can be configured. Grayed-out options cannot be configured; options in blue can. 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.

- **System Date**

Use this function to change the system date.

Select System Date using the Up and Down <Arrow> keys. Enter the new values through the keyboard. Press the Left and Right <Arrow> keys to move between fields.

The date setting must be entered in MM/DD/YY format.

- **System Time**

Use this function to change the system time.

Select System Time using the Up and Down <Arrow> keys. Enter the new values through the keyboard. Press the Left and Right <Arrow> keys to move between fields.

The time setting is entered in HH:MM:SS format.

**Note:** The time is in 24-hour format. For example, 5:30 A.M. appears as 05:30:00, and 5:30 P.M. as





17:30:00.

- **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.

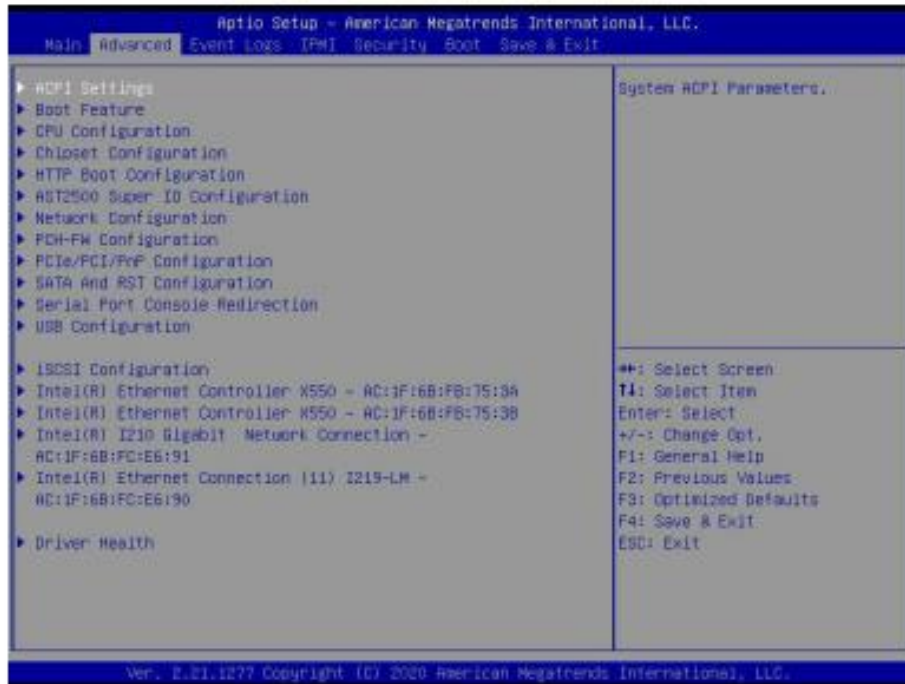
- **Memory Information**

- **Total Memory**

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

## 4.4 Advanced Setup Configurations

Use the arrow keys to select the Advanced menu and press <Enter> to access the menu 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.

### ▶ ACPI Settings

#### ACPI Sleep State

Use this feature to select the ACPI Sleep State that the system will enter into when the suspend button is activated. The options are Suspend Disabled and **S3 (Suspend to RAM)**.

#### 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**.

## Native PCIE Enable

Enable this feature to grant control of PCI Express Native hot plug, PCI Express Power Management Events, and PCI Express Capability Structure Control. The options are Disabled and **Enabled**.

## Native ASPM

Select Enabled for the operating system to control the ASPM, or Disabled for the BIOS to control the ASPM. The options are Auto, Enabled, and **Disabled**.

## ► Boot Feature

### Fast Boot

Enable this feature to reduce the time the computer takes to boot up. The computer will boot with a minimal set of required devices. This feature does not have an effect on BBS boot options in the Boot tab. The options are **Disabled** and Enabled.

### 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**.



## 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.

## ►Connectivity Configuration

This submenu becomes configurable when a CNVi device is plugged into the motherboard.

### CNVi present

This feature displays the status of wireless connections.

### CNVi Configuration

#### CNVi WiFi&BT

Use this feature to enable CNVi WiFi and Bluetooth support. The options are Disabled and **Enabled**.

## ►CPU Configuration

The following CPU information will display:

- CPU Signature
- Microcode Patch



- Max CPU Speed
- Min CPU Speed
- CPU Speed
- Processor Cores
- Hyper Threading Technology
- VMX
- SMX/TXT
- 64-bit
- EIST Technology
- CPU C3 state
- CPU C6 state
- CPU C7 state
- CPU C8 state
- CPU C9 state
- CPU C10 state
- L1 Data Cache
- L1 Instruction Cache
- L2 Cache
- L3 Cache
- L4 Cache

### **C6DRAM (Available when supported by the CPU)**

This feature enables moving DRAM contents to PRM memory when the CPU is in a C6 state. The options are Disabled and **Enabled**.

### **Hardware Prefetcher**

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

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.

## Intel (VMX) Virtualization Technology (Available when supported by the CPU)

Use this feature to enable the Vanderpool Technology. This technology allows the system to run several operating systems simultaneously. The options are Disabled and **Enabled**.

## Active Processor Cores

This feature determines how many CPU cores will be activated for each CPU. When all is selected, all cores in the CPU will be activated. The options are **All** and 1, 2, 3, 4, and 5.

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

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

## AES (Available when supported by the CPU)

Select Enabled for Intel CPU Advanced Encryption Standard (AES) instructions support to enhance data integrity. The options are Disabled and **Enabled**.

## Boot Performance Mode

This feature allows the user to select the performance state that the BIOS will set before the operating system handoff. The options are Power Saving, **Max Non-Turbo Performance**, and Turbo Performance.

## Intel® SpeedStep™ C (Available when supported by the CPU)

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

## Intel® Speed Shift Technology

Use this feature to enable or disable Intel Speed Shift Technology support. When this feature is enabled, the Collaborative Processor Performance Control (CPPC) version 2 interface will be available to control CPU P-States. The options are Disabled and **Enabled**.

## Turbo Mode (Available when supported by the CPU)

Select Enable for processor cores to run faster than the frequency specified by the manufacturer. The options are Disable and **Enable**.

## Power Limit 1 Override (Available when supported by the CPU)

Use this feature to enable or disable Power Limit 1 override. The options are **Disabled** and Enabled.



## **Power Limit 1**

Use this feature to set the power limit 1, in milliwatts. When the limit is exceeded, the CPU ratio is lowered after a period of time (see Power Limit 1 Time Window below). A lower limit can save power and protect the CPU, while a higher limit improves performance. This value must be between Min Power Limit TDP limit. Use the number keys on your keyboard to enter the value. The default setting is **0**.

## **Power Limit 1 Time Window**

This feature determines how long the time window over which the TDP value is maintained. Use the number keys on your keyboard to enter the value. The default setting is **0**. This value may vary between 0 and 128.

## **Power Limit 2 Override (Available when supported by the CPU)**

Use this feature to enable or disable Power Limit 2 override. The options are **Disabled** and **Enabled**.

## **Power Limit 2**

Use this feature to set the power limit 2. Use the number keys on your keyboard to enter the value. The default setting is **0**.

## **C-States**

Use this feature to enable the C-State of the CPU. The options are **Disabled** and **Enabled**.

## **Enhanced C-states**

Use this feature to enable the enhanced C-State of the CPU. The options are **Disabled** and **Enabled**.

## **C-State Auto Demotion**

Use this feature to prevent unnecessary excursions into the C-states to improve latency. The options are **Disabled**, **C1**, **C3**, and **C1 and C3**.

## **C-State Un-Demotion**

This feature allows the user to enable or disable the un-demotion of C-State. The options are **Disabled**, **C1**, **C3**, and **C1 and C3**

## **Package C-State Demotion**

Use this feature to enable or disable the Package C-State demotion. The options are **Disabled** and **Enabled**.

## **Package C-State Un-Demotion**

Use this feature to enable or disable the Package C-State un-demotion. The options are **Disabled** and **Enabled**.



## CState Pre-Wake

This feature allows the user to enable or disable the C-State Pre-Wake. The options are Disabled and **Enabled**.

## Package C State Limit

Use this feature to set the Package C-State limit. The options are C0/C1, C2, C3, C6, C7, C7s, C8, C9, Cpu Default, and **Auto**.

## ► Chipset Configuration

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

### ► System Agent (SA) Configuration

The following information will display:

- SA PCIe Code Version: 7.0.53.66
- VT-d: Supported

### ► Memory Configuration

#### Memory Configuration

- Memory RC Version
- Memory Frequency
- Memory Timing (tCL-tRCD-tRP-tRAS)
- DIMMA1
- DIMMA2
- DIMMB1
- DIMMB2

#### Maximum Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 1067, 1200, 1333, 1400, 1600, 1800, 1867, 2000, 2133, 2200, 2400, 2600, 2667, 2800, 2933.





## Max TOLUD

This feature sets the maximum TOLUD value, which specifies the "Top of Low Usable DRAM" memory space to be used by internal graphics devices, GTT Stolen Memory, and TSEG, respectively, if these devices are enabled. The options are **Dynamic**, 1 GB, 1.25 GB, 1.5 GB, 1.75 GB, 2 GB, 2.25 GB, 2.5 GB, 2.75 GB, 3 GB, 3.25 GB, and 3.5 GB.

## Memory Scrambler

Use this feature to enable or disable memory scrambler support. The options are **Disabled** and **Enabled**.

## Force ColdReset

Use this feature to enable or disable a cold boot during a MRC execution. The options are **Enabled** and **Disabled**.

## Force Single Rank

Select enabled to use only Rank 0 in each DIMM. The options are **Disabled** and **Enabled**.

## Memory Remap

Use this feature to enable or disable memory remap above 4GB. The options are **Enabled** and **Disabled**.

## MRC Fast Boot

Use this feature to enable or disable fast path through the memory reference code. The options are **Disabled** and **Enabled**.

## ►Graphics Configuration

### Graphics Configuration

- IGFX VBIOS Version
- IGFX GOP Version

### Graphics Turbo IMON Current

Use this feature to set the graphics turbo IMON value. The default is **31**.

### Skip Scanning of External Gfx Card

If set to enabled, the system will not scan for an external graphics card on PEG and PCIE slots. The options are **Disabled** and **Enabled**.



## Primary Display

Use this feature to select the primary video display. The options are **Auto**, IGFX, PEG, and PCI.

## Internal Graphics

Select Auto to keep an internal graphics device installed on an expansion slot supported by the CPU to be automatically enabled. The options are **Auto**, Disable, and Enable.

## GTT Size

Use this feature to set the memory size to be used by the graphics translation table (GTT). The options are 2MB, 4MB, and **8MB**.

## Aperture Size

Use this feature to set the Aperture size, which is the size of system memory reserved by the BIOS for graphics device use. The options are 128MB, **256MB**, 512MB, 1024MB, and 2048MB.

## DVMT Pre-Allocated

Dynamic Video Memory Technology (DVMT) allows dynamic allocation of system memory to be used for video devices to ensure best use of available system memory based on the DVMT 5.0 platform. The options are 0M, **32M**, 64M, 4M, 8M, 12M, 16M, 20M, 24M, 28M, 32M/F7, 36M, 40M, 44M, 48M, 52M, 56M, and 60M.

## DVMT Total Gfx Mem

Use this feature to set the total memory size to be used by internal graphics devices based on the DVMT 5.0 platform. The options are 128MB, **256MB**, and MAX.

## PM Support

Enable this feature to activate Power Management BIOS support. The options are **Enable** and Disable.

## PAVP Enable

Protected Audio Video Path (PAVP) decodes Intel integrated graphics encrypted video. The options are Disable and **Enable**.

## Cdynmax Clamping Enable

Enable this feature to activate Cdynmax Clamping. The options are **Enable** and Disable.

## Graphics Clock Frequency

Use this feature to set the internal graphics clock frequency. The options are 337.5 Mhz, 450 Mhz, 540 Mhz, and **675 Mhz**.



## Skip CD Clock Init in S3 resume

Use this feature to enable skipping of the full CD initialization. If set to Disabled, the full CD clock will initialize. The options are Enabled and **Disabled**.

## ► DMI/OPI Configuration

The following DMI information will display:

DMI: X4 Gen3

### DMI Link ASPM Control

Use this feature to set the ASPM (Active State Power Management) state on the SA (System Agent) side of the DMI Link. The options are Disable, L0s, L1, and **L0sL1**.

### DMI Extended Sync Control

Use this feature to enable or disable the DMI extended synchronization. The options are Enable and **Disable**.

## ► PEG Configuration

### CPU SLOT6 PCI-E 3.0 X16

#### Enable Root Port

Use this feature to enable or disable the PCI Express Graphics (PEG) device in the port specified by the user. The options are Disable, Enable, and **Auto**.

#### Max Link Speed

Use this feature to select PCIe support for the device installed on SLOT7. The options are **Auto**, Gen 1, Gen 2, and Gen 3.

## ► GT - Power Management Control

### RC6 (Render Standby)

Use this feature to enable render standby support. The options are Disabled and **Enabled**.

### Maximum GT frequency

Use this feature to define the Maximum GT frequency. Choose between 33MHz (RPN) and 1200MHz (RP0). Any value beyond this range will be clipped to its min/max supported by the CPU. The options are **Default Max Frequency**, 100Mhz, 150Mhz, 200Mhz, 250Mhz, 300Mhz, 350Mhz, 400Mhz, 450Mhz, 500Mhz, 550Mhz, 600Mhz, 650Mhz, 700Mhz, 750Mhz, 800Mhz, 8520Mhz, 900Mhz, 950Mhz, 1000Mhz, 1050Mhz, 1100Mhz, 1150Mhz, and 1200Mhz.



## Disable Turbo GT frequency

Use this feature to disable Turbo GT frequency. If set to Enabled, Turbo GT frequency becomes disabled. If set to Disabled, GT frequency limiters will be removed. The options are Enabled and **Disabled**.

## VT-d

Select Enabled to activate Intel Virtualization Technology support for Direct I/O VT-d by reporting the I/O device assignments to VMM through the DMAR ACPI Tables. This feature offers fully-protected I/O resource-sharing across the Intel platforms, providing the user with greater reliability, security and availability in networking and data-sharing. The options are Disabled and **Enabled**.

## SW Guard Extensions (SGX)

Select Enabled to activate the Software Guard Extensions (SGX). The options are Disabled, Enabled, and **Software Controlled**.

## GNA Device (B0:D8:F0)

Use this feature to enable SA GNA device. The options are **Enabled** and Disabled.

***\*If the feature SGX is set to Enabled, the following features below will be available for configuration:***

## Select Owner EPOCH Input Type

There are three Owner EPOCH modes (each EPOCH is 64 bit). The options are **No Change in Owner EPOCHs**, Change to New Random Owner EPOCH, and Manual User Defined Owner EPOCHs.

***\*If the feature Select Owner EPOCH Input Type is set to Manual User Defined Owner EPOCHs, the following features below will be available for configuration:***

## Software Guard Extensions Epoch 0

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

## Software Guard Extensions Epoch 1

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

## PRMRR Size

The BIOS must reserve a contiguous region of Processor Reserved Memory (PRM) in the Processor Reserved Memory Range Register (PRMRR). The options are 32MB, 64MB, and **128MB**.



## ► PCH-IO Configuration

### PCH-IO Configuration

- PCH SKU Name
- Stepping

## ► PCI Express Configuration

### DMI Link ASPM Control

Use this feature to set the ASPM (Active State Power Management) state on the SA (System Agent) side of the DMI Link. The options are Disabled, L0s, L1, L0sL1, and **Auto**.

### Peer Memory Write Enable

Use this feature to enable or disable peer memory write. The options are **Disabled** and **Enabled**.

- PCH SLOT4 PCI-E 3.0 X4 (IN X8)
- PCI-E M.2-E1
- PCH SLOT7 PCI-E 3.0 X4
- PCI-E M.2-M1

### ASPM

Use this feature to activate the Active State Power Management (ASPM) level for a PCIe device. Select Auto for the system BIOS to automatically set the ASPM level based on the system configuration. Select Disabled to disable ASPM support. The options are Disabled, L0s, L1, L0sL1, and **Auto**.

### L1 Substates

Use this feature to set the PCI Express L1 Substates. The options are Disabled, L1.1, and **L1.1 & L1.2**.

### PCIe Speed

Use this feature to select the PCI Express port speed. The options are **Auto**, Gen1, Gen2, and Gen3.

### PCIe PLL SSC

Use this feature to enable or disable PCIe PLL SSC. The options are **Disabled** and **Enabled**.

## ▶HDD Security Configuration

### HDD Security Configuration

The following HDD information will display:

**P0**

**Security Supported**

**Security Enabled**

**Security Locked**

**Security Frozen**

**HDD User Pwd Status**

**HDD Master Pwd Status**

**Set User Password**

Press Enter to create a new, or change an existing HDD password.

## ▶HTTP Boot Configuration

### HTTP BOOT Configuration

#### HTTP Boot One Time

Use this feature to create the HTTP boot option. The options are **Disabled** and **Enabled**.

#### Input The Description

Highlight the feature and press enter to create a description.

#### Boot URI

Highlight the feature and press enter to create a boot URI.

## ▶AST2500 Super IO Configuration

The following Super IO information will display:

- Super IO Chip AST2500

## ▶Serial Port 1 Configuration

### Serial Port 1

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



## Device Settings

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

## Change Settings

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;).

## ► Serial Port 2 Configuration

### Serial Port 2

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

### Device Settings

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

### Change Settings

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.

## ► Network Configuration

### ► MAC:XXXXXXXXXXXX-IPv4 Network Configuration

#### Configured

This feature indicates whether a network address is configured successfully or not. The default is **Unchecked**.

*\*If the feature above is set to Checked, the following features below will be available for configuration:*

#### Enable DHCP

Use this feature to set the DHCP. The default is **Unchecked**.



*\*If the feature above is set to Unchecked, the following features below will be available for configuration:*

#### **Local IP Address**

Enter an IP address in dotted decimal notation.

#### **Local Netmask**

Enter a NetMask address in dotted decimal notation.

#### **Local Gateway**

Enter a Gateway in dotted decimal notation.

#### **Local DNS Servers**

Enter a DNS server in dotted decimal notation.

#### **Save Changes and Exit**

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

### **►MAC:XXXXXXXXXX-HTTP Boot Configuration**

This submenu is available for configuration when IPv4 HTTP Support and IPv6 HTTP Support are set to Enabled.

#### **Input the description**

This feature is an input field that, when the HTTP boot option is created, can be used to enter text to describe or identify the HTTP connection.

#### **Internet Protocol**

Select the version of Internet Protocol. The options are subject to change depending on the features you enabled in IPv4 HTTP Support and IPv6 HTTP Support.

#### **Boot URI**

This feature is an input field used to enter a web or network address to point to the HTTP boot files. This supports the HTTP or HTTPS protocols only.

### **►MAC:XXXXXXXXXX-IPv6 Network Configuration**

The following information is displayed:

#### **Interface Name**

#### **Interface Type**

#### **MAC Address**





## Host Addresses

### Route Table

### Gateway addresses

### DNS addresses

### Interface ID

Enter an ID for the device.

### DAD Transmit Count

Enter a value for DAD (Duplicate Address Detection) Transmit Count. A value of zero indicates the DAD is not performed. The default is 1.

### Policy

Use this feature to set the Policy. The options are **Automatic** and **Manual**.

***\*If the feature above is set to Manual, the following features below will be available for configuration:***

### Advanced Configuration

#### New IPv6 Addresses

Enter a new IPv6 Gateway address.

#### New DNS Addresses

Enter a new DNS address.

### Commit Changes and Exit

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

### Saves Changes and Exit

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

## ▶ Enter Configuration Menu

### Interface Name

### Interface Type

### MAC address

### Host addresses



## Route Table

### Gateway addresses

### DNS addresses

### Interface ID

This feature shows the interface ID for the specified network device.

### DAD Transmit Count

This feature sends Neighbor Solicitation messages while performing a Duplicate Address Detection (DAD) to make sure there is no IP address duplication. A value of zero means a DAD has not been performed.

### Policy

Use this feature to select an automatic or manual policy. The options are **Automatic** and **Manual**.

### Save Changes And Exit

When you have completed the changes for this section, select this option to save all changes made and exit.

## ► PCH-FW Configuration

**ME Firmware Version: 14.**

**ME Firmware Mode: Normal Mode**

**ME Firmware SKU: Corporate SKU**

### ME FW Image Re-Flash

Use this feature to update the Management Engine firmware. The options are **Disabled** and **Enabled**.

## ► AMT Configuration

### USB Provisioning of AMT

Use this feature to enable or disable USB provisioning. The options are **Disabled** and **Enabled**.



## ► CIRCA Configuration

### Activate Remote Assistance Process

Use this feature to activate Remote Assistance. Enabling this feature will also trigger the CIRCA boot. The options are **Disabled** and **Enabled**.

*\*If the feature above is set to Enabled, the feature below will be available for configuration:*

### CIRCA Timeout

Use this feature to set the timeout value for MPS connection. Use 0 for the default timeout value of 60 seconds.

## ► ASF Configuration

### PET Progress

Use this feature to enable or disable PET Events Progress to receive PET Events alerts. The options are **Disabled** and **Enabled**.

### WatchDog

Select **Enabled** to allow AMT to reset or power down the system if the operating system or BIOS hangs or crashes. The options are **Disabled** and **Enabled**.

### OS Timer / BIOS Timer

These options appear if Watch Dog (above) is enabled. This is a timed delay in seconds, before a system power down or reset after a BIOS or operating system failure is detected. Enter the value in seconds.

### ASF Sensors Table

Enable this feature for the ASF Sensor Table to be added into the ASF! ACPI table. The options are **Disabled** and **Enabled**.

## ► Secure Erase Configuration

### Secure Erase mode

Select **Real** to securely erase a solid state drive. The options are **Simulated** and **Real**.

### Force Secure Erase

Select **Enabled** to force a secure erase of the solid state drive on the next boot. The options are **Disabled** and **Enabled**.



## ►OEM Flags Settings

### **MEBx hotkey Pressed**

Use this feature to specify whether the MEBx hotkey should be enabled during the system boot. The options are **Disabled** and **Enabled**.

### **MEBx Selection Screen**

Use this feature to select the type of MEBx selection screen. Press 1 to enter the ME Configuration screen and 2 to initiate a remote connection. Network access must be activated for a remote connection. The options are **Disabled** and **Enabled**.

### **Hide Unconfigure ME Confirmation Prompt**

Use this feature to hide the unconfigure ME confirmation prompt. The options are **Disabled** and **Enabled**.

### **MEBx OEM Debug Menu Enable**

Use this feature to enable or disable the OEM debug menu in MEBx. The options are **Disabled** and **Enabled**.

### **Unconfigure ME**

Use this feature to reset the MEBx password to default. The options are **Disabled** and **Enabled**.

## ►MEBx Resolution Settings

### **Non-UI Mode Resolution**

Use this feature to specify the resolution for the non-UI text mode. The options are **Auto**, **80x25**, and **100x31**.

### **UI Mode Resolution**

Use this feature to specify the resolution for the UI text mode. The options are **Auto**, **80x25**, and **100x31**.

### **Graphics Mode Resolution**

Use this feature to specify the resolution for the graphics mode. The options are **Auto**, **640x480**, **800x600**, and **1024x768**.



## ► PCIe/PCI/PnP Configuration

### Option ROM execution

#### Video

Use this feature to select the execution of the video OpROM. The options are Do not launch and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

#### PCI PERR/SERR Support

Use this feature to enable or disable the runtime event for PCI errors. The options are **Disabled** and Enabled.

#### Above 4GB MMIO BIOS Assignment

Select Enable for remapping of BIOS above 4GB. The options are Enabled and **Disabled**.

#### SR-IOV Support

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

#### BME DMA Mitigation

Enable this feature to help block DMA attacks. The options are Enabled and **Disabled**.

#### Onboard Video Option ROM

Use this feature to select which firmware function to be loaded for LAN1 used for system boot. The options are Disabled, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

#### 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.

#### Consistent Device Name Support

This feature controls the device naming for network devices and slots. The options are **Disabled** and Enabled.

#### PCIe/PCI/PnP Configuration

#### PCH SLOT4 PCI-E 3.0 X4 (IN X8) OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.



## **CPU SLOT6 PCI-E 3.0 X16 OPROM**

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

## **PCH SLOT7 PCI-E 3.0 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, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

## **PCI-E M.2-M1 OPROM**

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

## **PCI-E M.2-E1 OPROM**

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

## **Onboard LAN1 Option ROM**

Use this feature to select which firmware function to be loaded for LAN1 used for system boot. The options are Disabled, Legacy and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

*\*These options are subject to change depending on the feature of Boot Mode Select.*

## **Onboard LAN2 Option ROM**

Use this feature to select a desired firmware function to be loaded for onboard LAN1. The options are Disabled, Legacy, and **EFI**. The Legacy option is hidden when the Boot mode is EFI. The EFI option is hidden when the Boot mode is Legacy.

## **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**.

## **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 option to specify the wait time to press the ESC key to abort the PXE boot. Press "+" or "-" on your keyboard to change the value. The default setting is **0**.

## Media Detect Count

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

## ► SATA And RST Configuration

### SATA Controller(s)

This feature enables or disables the onboard SATA controller supported by the Intel PCH chip. The options are **Enabled** and Disabled.

### SATA Mode Selection

Use this feature to select the SATA mode. The options are **AHCI** and Intel RST Premium With Intel Optane System Acceleration.

*\*If the feature above is set to Intel RST Premium With Intel Optane System Acceleration, the next four features will be available for configuration:*

### SATA Interrupt Selection

Use this feature to select the SATA interrupt. The options are Msix, **Msi**, and Legacy.

### PCI-E M.2-M1

The feature shown here is dependent on the M.2 device plugged into the motherboard. This feature appears if an M.2 device is plugged in and RAID is selected in the SATA Mode Selection feature. Use this feature to enable or disable RST PCIe storage remapping. The options are RST Controlled and **Not RST Controlled**.

### RAID Device ID

Use this feature to select the RAID device ID. The options are **iRST Mode** and Alternate.

### Storage Option ROM/UEFI Driver

Select UEFI to load the EFI driver for system boot. Select Legacy to load a legacy driver for system boot. The options are Do not Launch, **EFI**, and Legacy.

### Teton Glacier Mode

Use this feature to enable or disable Intel Optane memory with solid state storage. The options are Dynamic Configuration for Hybrid Storage Device Enable and **Disabled**.



## Aggressive LPM Support

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 Disabled and **Enabled**.

## Serial ATA Port 0-3

This feature displays the information detected on the installed SATA drive on the particular SATA port.

- Software Preserve Support

### SATA Port 0-3 Hot Plug

Set this feature to Enable for hot plug support, which will allow the user to replace a SATA drive without shutting down the system. The options are Disabled and **Enabled**.

### SATA Port 0-3 Spin Up Device

Set this feature to enable or disable the PCH to initialize the device. The options are **Disabled** and Enabled.

### SATA Port 0-3 SATA Device Type

Use this feature to specify if 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.

## ► 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 Enabled and **Disabled**.

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

### ► COM1 Console Redirection Settings

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.

### COM1 Terminal Type

This feature allows the user 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.





## COM1 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).

## COM1 Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 Bits and **8 Bits**.

## COM1 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.

## COM1 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.

## COM1 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.

## COM1 VT-UTF8 Combo Key Support

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

## COM1 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.

## COM1 Resolution 100x31

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

## COM1 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.



## COM1 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**.

## COM1 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**.

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

### ► SOL/COM2 Console Redirection Settings

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.

### 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.

### SOL/COM2 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).

### SOL/COM2 Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 Bits and **8 Bits**.



## SOL/COM2 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.

## SOL/COM2 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.

## SOL/COM2 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.

## SOL/COM2 VT-UTF8 Combo Key Support

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

## SOL/COM2 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.

## SOL/COM2 Resolution 100x31

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

## SOL/COM2 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**.

## SOL/COM2 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, SCO, ESCN, and VT400.

## SOL/COM2 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.



## ▶ AMT SOL Console Redirection Settings

### AMT SOL 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.

### AMT SOL 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).

### AMT SOL Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 Bits and **8 Bits**.

### AMT SOL 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.

### AMT SOL 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.

### AMT SOL 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.

### AMT SOL VT-UTF8 Combo Key Support

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



## AMT SOL 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**.

## AMT SOL Resolution 100x31

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

## AMT SOL 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**, **SCO**, **ESCN**, and **VT400**.

## AMT SOL 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**.

## AMT SOL 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 Settings

### Redirection COM Port

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

## EMS (Emergency Management Services) Console Redirection

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

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

## ► EMS Console Redirection Settings

This feature allows the user 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**, **SOL/COM2**, and **AMT SOL**.

## 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

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

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**.

## Data Bits, Parity, Stop Bits

### ► Trusted Computing

The motherboard supports TPM 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.

### **Platform Hierarchy**

Use this feature to disable or enable platform hierarchy for platform protection. The options are Disabled and **Enabled**.

### **Storage Hierarchy**

Use this feature to disable or enable storage hierarchy for cryptographic protection. The options are Disabled and **Enabled**.

### **Endorsement Hierarchy**

Use this feature to disable or enable endorsement hierarchy for privacy control. The options are Disabled and **Enabled**.

### **TPM 20 Interface Type**

### **PH Randomization**

Use this feature to disable or enable Platform Hierarchy (PH) Randomization. The options are **Disabled** and Enabled.

### **Disable Block sid**

Select Enabled to allow SID authentication be performed in TCG Storage devices. The options are **Enabled** and Disabled.



## Intel Trusted Execution 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 Support. The options are **Disabled** and **Enabled**.

### Current Status Information

The following information will be displayed:

**TPM Enabled Status**

**TPM Active Status**

**TPM Owner Status**

## ► USB Configuration

### USB Configuration

**USB Module Version: 21**

**USB Controllers: 2 XHCIs**

**USB Devices:**

### Legacy USB Support

Select **Enabled** to support onboard legacy USB devices. Select **Auto** to disable legacy support if there are no legacy USB devices present. Select **Disable** to have all USB devices available for EFI applications only. The options are **Enabled**, **Disabled**, and **Auto**.

### XHCI Hand-off

This is a work-around solution for operating systems that do not support XHCI (Extensible Host Controller Interface) hand-off. The XHCI ownership change should be claimed by the XHCI driver. The settings are **Enabled** and **Disabled**.

### USB Mass Storage Driver Support

Select **Enabled** for USB mass storage device support. The options are **Disabled** and **Enabled**.

## ► iSCSI Configuration

### ► Attempt Priority

#### Attempt Priority

Use this feature to set the attempt priorities. The options are **Host Attempt**, **Redfish Attempt**, and **Rsd Attempt**.





## Commit Changes and Exit

Select this item to save the changes and exit.

## ► Host iSCSI Configuration

### iSCSI Initiator Name

This feature allows the user 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.

#### ► Add an Attempt

#### ► Delete Attempts

#### ► Change Attempt Order

- Intel(R) Ethernet Controller X550 - AC:1F:6B:FB:75:3A
- Intel(R) Ethernet Controller X550 - AC:1F:6B:FB:75:3B
- Intel(R) I210 Gigabit Network Connection - AC:1F:6B:FC:E6:91
- NIC Configuration

### Link Speed

Use this feature 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 wake on LAN support, which will allow the system to wake up when an onboard LAN 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.

### UEFI Driver

### Adapter PBA

### Device Name

### Chip Type

### PCI Device ID

### PCI Address

### Link Status



## MAC Address

### Virtual MAC Address

#### ▶ Intel(R) Ethernet Connection (11) I219-LM - AC:1F:6B:FC:E6:90

## PORT CONFIGURATION INFORMATION

### UEFI Driver

### Adapter PBA

### PCI Device ID

### PCI Address

### MAC Address

#### ▶ Intel(R) Rapid Storage Technology

This submenu will only appear if the following requirements are met when entering the BIOS: Set the Boot Mode Select to **DUAL** or **UEFI**. Set the SATA Mode Selection to **Intel RST Premium With Intel Optane System Acceleration**. Set the Storage Option ROM/UEFI Driver to **EFI**.

Information for installed storage drives will be viewable in this submenu when the settings above are completed

#### ▶ Driver Health

This feature provides the health status for the network drivers and controllers.

##### ▶ Intel(R) PRO/1000 6.7.05 PCI-E

Controller 97d46818 Child 0

Intel(R) I210 Gigabit Network Connection

##### ▶ Intel(R) Gigabit 0.0.29

Controller 97d44b18 Child 0

##### ▶ Intel(R) 10GbE Driver 6.9.04 x64

Controller 97d47718 Child 0

Intel(R) Ethernet Controller X550



▶ Intel(R) 10GbE Driver 6.9.04 x64

Controller 97d46a18 Child 0

Intel(R) Ethernet Controller X550

## 4.5 Event Logs

Use this menu to configure Event Log settings.



### ► 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**.

#### 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 **Disabled** and **Enabled**.

### MECI

The Multiple Event Count Increment (MECI) counter counts the number of occurrences 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**.

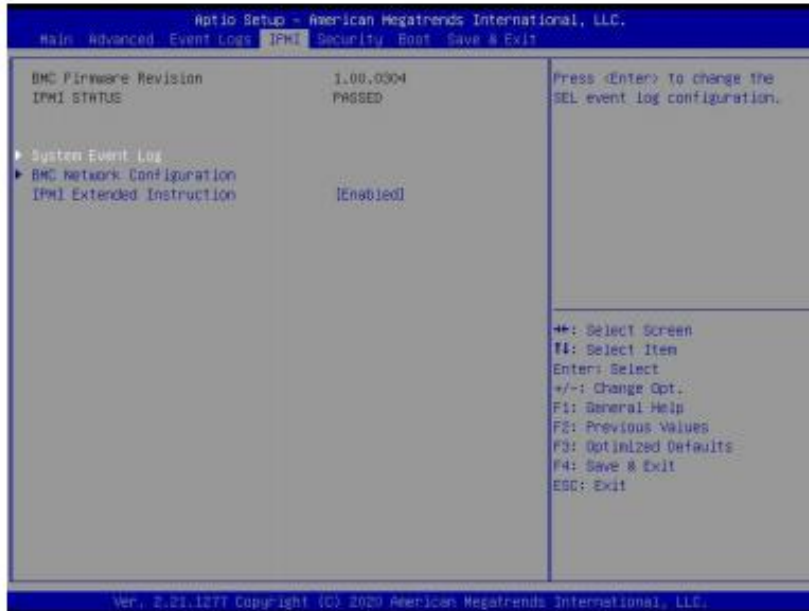
 **Note:** After making changes on a setting, be sure to reboot the system for the changes to take effect.

## ► View SMBIOS 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 Codes/Severity.

## 4.6 IPMI

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



### BMC Firmware Revision

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

### IPMI STATUS (Baseboard Management Controller)

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

## ► System Event Log

### Enabling/Disabling Options

#### SEL Components

Select Enabled for all system event logging at bootup. The options are **Enabled** and Disabled.


#### 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 the user 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.

## ► 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, Configuration Address Source, VLAN, and IPv6 Support available for configuration:*

#### Configure IPv4 Support

#### IPMI LAN Selection

#### IPMI Network Link Status

#### Configuration Address Source

This feature allows the user 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 **DHCP** and Static.

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

#### Station IP Address

This features displays the Station IP address for this computer. The address can be manually entered. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).

#### Subnet Mask

This feature displays the sub-network that this computer belongs to. The address can be manually entered. The value of each three-digit number separated by dots should not exceed 255.

#### Station MAC Address



## Gateway IP Address

This feature displays the Gateway IP address for this computer. The address can be manually entered. This should be in decimal and in dotted quad form (i.e., 172.31.0.1).

## VLAN

This feature displays the virtual LAN settings. The options are Disabled and Enabled.

## VLAN ID

This feature is enabled if VLAN is enabled.

## Configure IPv6 Support

### IPv6 Address Status

### IPv6 Support

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

### Configuration Address Source

### Station IPv6 Address

### Prefix Length

### IPv6 Router1 IP Address

## IPMI Extended Instruction

Use this feature to enable IPMI support. The options are **Enabled** and Disabled. When Disabled, the system powers on quickly by removing BIOS support for extended IPMI features. The Disable option is for applications that require faster power on time without using Supermicro Update Manager (SUM) or extended IPMI features. The BMC network configuration in the BIOS setup is also invalid when IPMI Function Support is disabled. The general BMC function and motherboard health monitor such as fan control are still functioning even when this option is disabled.



## 4.7 Security

Use this menu to configure the following security settings for the system.



### Administrator Password

Press Enter to create a new, or change an existing, Administrator password.

### ▶ SMC Security Erase Configuration

This submenu becomes configurable when a storage device has been plugged into the motherboard. The options are Enabled and **Disabled**.

### HDD Name

### HDD Serial Number

### Security Erase Mode

### Estimated Time

### HDD PserPwd Status

### Security Function

Use this feature to set Security Function. The options are **Disabled**, Security Erase, and Set Password.

### Password

Enter a numeric value to set the password.



## Hard Drive Security Frozen

Use this feature to enable or disable the BIOS security frozen command for 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.

## Lockdown Mode

This feature is grayed out when the DCMS Key is not installed.

### ► Secure Boot

This section displays the contents of the following secure boot features:

- System Mode
- Secure Boo

## Secure Boot

Use this feature to enable secure boot. The options are **Disabled** and Enabled.

## Secure Boot Mode

Use this item to configure Secure Boot variables without authentication. The options are Standard and **Custom**.

## CSM Support

This feature is for manufacturing debugging purposes.

## Enter Audit Mode

This submenu can only be used if current System Mode is set to User (refer to Exit Deployed Mode). The PK variable will be erased on transition to Audit Mode.

## Enter Deployed Mode

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

## Exit Deployed Mode

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

### ► Key Management

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



## ▶ Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot key databases.

## ▶ Reset to Setup Mode

This feature deletes all Secure Boot key databases from NVRAM.

## ▶ Export Secure Boot variables

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

## ▶ Enroll EFI Image

This feature allows the image to run in Secure Boot Mode. Enroll SHA256 Hash Certificate of the image into the Authorized Signature Database.

## Device Guard Ready

### ▶ Remove 'UEFI CA' from DB

This feature allows the user to decide if all secure boot variables should be saved.

### ▶ Restore DB defaults

Select Yes to restore the DB defaults.

## Secure Boot Variable

### ▶ Platform Key (PK)

#### Details

Review details on current settings of the platform keys.

#### Export

This feature allows the user to export Platform Keys to an available file system.

#### Update

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

#### Delete

Select OK to confirm deletion of the Platform Key from NVRAM.

## ▶ Key Exchange Key

### Details

Review details on current settings of the Key Exchange Keys.

### Export

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

### Update

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

### Append

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

### Delete

Select Yes delete the Key.

## ▶ Authorized Signatures

### Details

Review details on current settings of the Authorized Signatures.

### Export

This feature allows the user to export Authorized Signatures to an available file system.

### Update

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

### Append

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

### Delete

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



## ► Forbidden Signatures

### Details

Review details on current settings of the Forbidden Signatures.

### Export

This feature allows the user to export Forbidden Signatures to an available file system.

### Update

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

### Append

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

### Delete

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

## ► Authorized TimeStamps

### Details

Review details on current settings of the Authorized TimeStamps.

### Export

This feature allows the user to export Authorized TimeStamps 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 Authorized TimeStamps key database. Select No to delete only a certificate from the key database.

## ► OsRecovery Signature

### Details

Review details on current settings of the OsRecovery Signatures.

### Export

This feature allows the user to export OsRecovery Signatures 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 OsRecovery Signatures key database. Select No to delete only a certificate from the key database.

## ► TCG Storage Device Security Configuration

### Storage Device

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

### Password Configuration:

The following information is displayed:

#### Password

#### Security Subsystem Class

#### Security Supported

#### Security Enabled

#### Security Locked

#### Security Frozen

#### User Pwd Status

#### Admin Pwd Status



## **Set Admin Password**

Press <Enter> to create a new admin password.

## **Set User Password**

Press <Enter> to create a new user password.

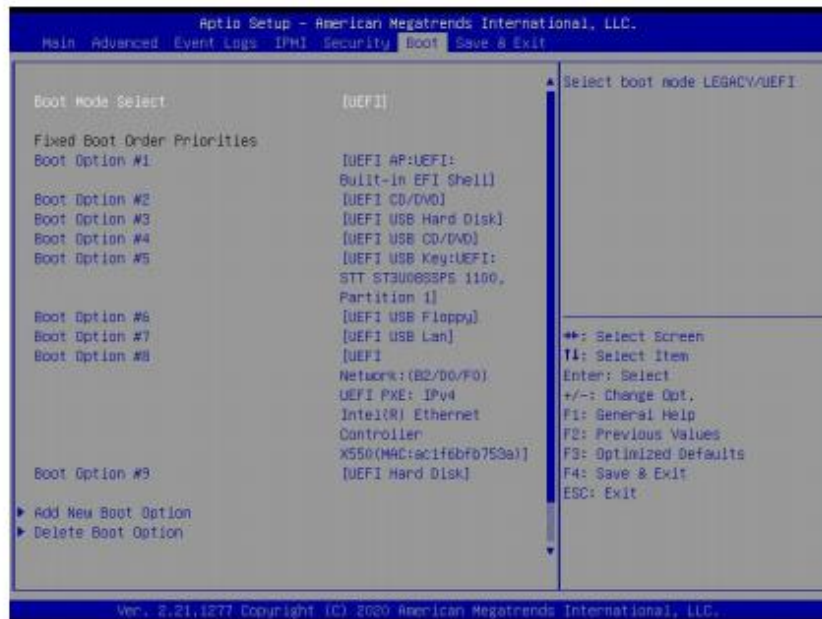
***\*The next feature is available when the Admin Password has been activated.***

## **Device Reset**

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

## 4.8 Boot

Use this menu 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.

### 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.

***\*If the feature "Boot Mode Select" is set to Legacy, UEFI, or Dual, the following items will be displayed:***

- Boot Option #1
- Boot Option #2
- Boot Option #3
- Boot Option #4
- Boot Option #5
- Boot Option #6
- Boot Option #7
- Boot Option #8





- Boot Option #9
- Boot Option #10
- Boot Option #11
- Boot Option #12
- Boot Option #13
- Boot Option #14
- Boot Option #15

## ► Add New Boot Option

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

### Add Boot Option

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

### Path for Boot Option

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

### Boot Option File Path

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

### Create

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

## ► Delete Boot Option

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

### Delete Boot Option

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

- UEFI Hard Disk Drive BBS Priorities
- UEFI CD/DVD Drive BBS Priorities
- UEFI Application Boot Priorities
- UEFI USB Hard Disk Drive BBS Priorities
- UEFI USB CD/DVD Drive BBS Priorities
- UEFI USB Key Drive BBS Priorities
- UEFI USB Floppy Drive BBS Priorities
- UEFI USB LAN Drive BBS Priorities



- ▶ UEFI NETWORK Drive BBS Priorities
- ▶ Hard Disk Drive BBS Priorities
- ▶ CD/DVD Drive BBS Priorities
- ▶ USB Hard Disk Drive BBS Priorities
- ▶ USB CD/DVD Drive BBS Priorities
- ▶ USB Key Drive BBS Priorities
- ▶ USB Floppy Drive BBS Priorities
- ▶ USB LAN Drive BBS Priorities
- ▶ NETWORK Drive BBS Priorities

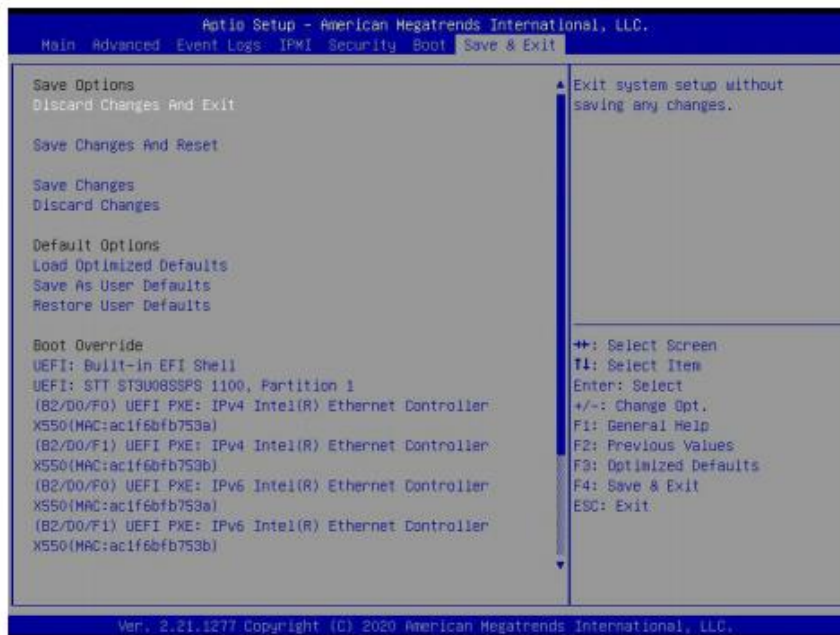
These submenus are subject to change depending on the feature of Boot Mode Select and the devices installed on this motherboard.

### **Boot Option #1 - X**

Use this feature to set the system boot order. The number of X is depending on the devices installed on the motherboard.

## 4.9 Save & Exit

Use this menu to save settings and exit from the BIOS.



### Save Options

#### Discard Changes and Exit

Select this option to quit the BIOS Setup without making any permanent changes to the system configuration, and reboot the computer. Select Discard Changes and Exit from the Save & Exit menu and press <Enter>.

#### Save Changes and Reset

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

#### Save Changes

When you have completed the system configuration changes, select this option to leave the BIOS setup utility and reboot the computer for the new system configuration parameters to take effect. Select Save Changes from the Save & Exit menu and press <Enter>.

#### Discard Changes

Select this option and press <Enter> to discard all the changes and return to the AMI BIOS utility program.



## **Default Options**

### **Load Optimized Defaults**

To set this feature, select Restore Defaults from the Save & Exit menu and press <Enter>. These are factory settings designed for maximum system stability, but not for maximum performance.

### **Save As User Defaults**

To set this feature, select Save as User Defaults from the Save & Exit menu and press <Enter>. This enables the user to save any changes to the BIOS setup for future use.

### **Restore User Defaults**

To set this feature, select Restore User Defaults from the Save & Exit menu and press <Enter>. Use this feature to retrieve user-defined settings that were saved previously.

### **Boot Override**

This feature allows the user to override the Boot priorities sequence in the Boot menu, and immediately boot the system with a device specified by the user instead of the one specified in the boot list. This is an one-time override.

### **UEFI: Built-in EFI Shell**

#### **Intel(R) Ethernet Controller X550**



## Chapter 5: Appendix A BIOS Codes

### 5.1 BIOS Error POST (Beep) Codes

During the POST (Power-On Self-Test) routines, which are performed each time the system is powered on, errors may occur.

Non-fatal errors are those which, in most cases, allow the system to continue the boot-up process. The error messages normally appear on the screen.

**Fatal errors** are those which will not allow the system to continue the boot-up procedure. If a fatal error occurs, you should consult with your system manufacturer for possible repairs.

These fatal errors are usually communicated through a series of audible beeps. The table shown below lists some common errors and their corresponding beep codes encountered by users.

BIOS Beep (POST) Codes		
Beep Code	Error Message	Description
1 beep	Refresh	Circuits have been reset (Ready to power up)
5 short, 1 long	Memory error	No memory detected in system
5 long, 2 short	Display memory read/write error	Video adapter missing or with faulty memory
1 long continuous	System OH	System overheat condition



## 5.2 Additional BIOS POST Codes

The AMI BIOS supplies additional checkpoint codes, which are documented online at [http://](http://www.supermicro.com/support/manuals/)

[www.supermicro.com/support/manuals/](http://www.supermicro.com/support/manuals/)

("AMI BIOS POST Codes User's Guide"). When BIOS performs the Power On Self Test, it writes checkpoint codes to I/O port 0080h. If the computer cannot complete the boot process, a diagnostic card can be attached to the computer to read I/O port 0080h (Supermicro p/n AOC-LPC80-20). For information on AMI updates, please refer to <http://www.ami.com/products/>.

## Chapter 6 : Appendix B Software

After the hardware has been installed, you can install the Operating System (OS), configure RAID settings and install the drivers.

### 6.1 Microsoft Windows OS Installation

If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at [www.supermicro.com/support/manuals](http://www.supermicro.com/support/manuals).

Installing the OS 1. Create a method to access the MS Windows installation ISO file. That might be a DVD, perhaps using an external USB/SATA DVD drive, or a USB flash drive, or the IPMI KVM console. 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.

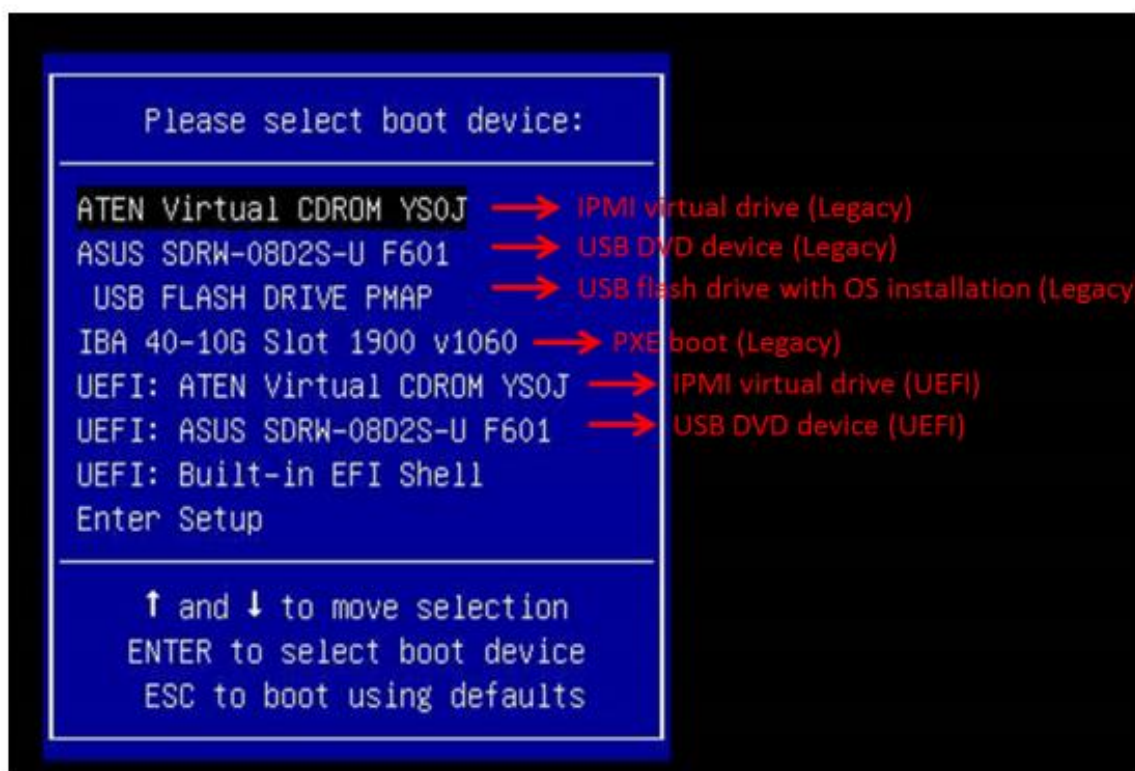
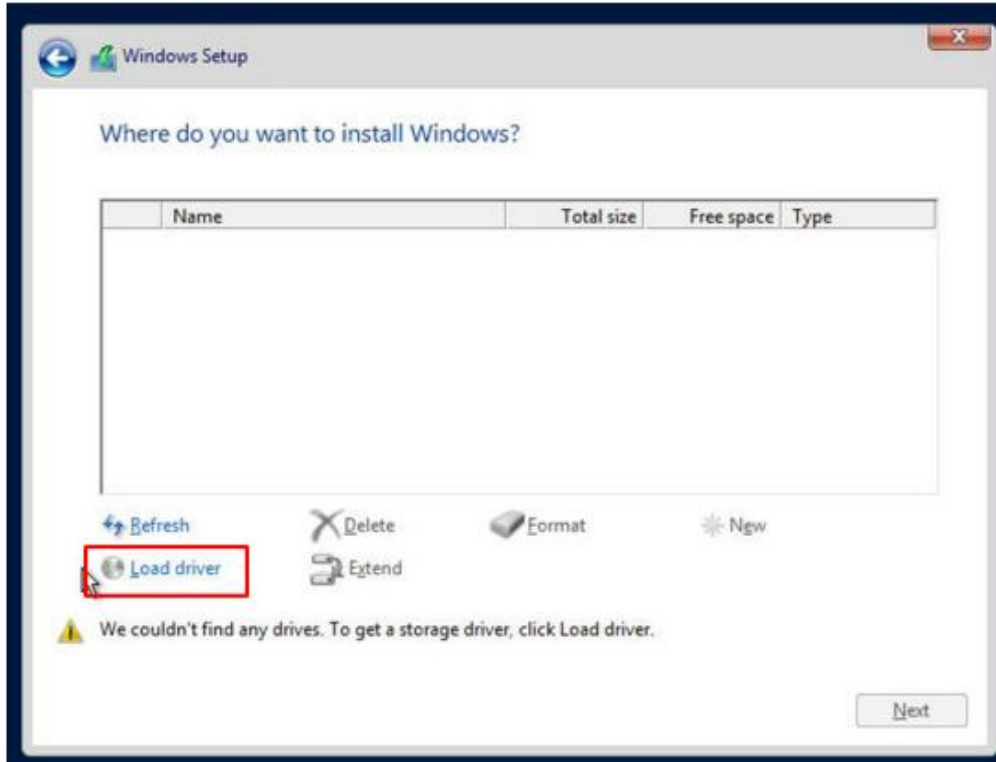


Figure 6-1. Select Boot Device

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.



## 6-2 Load Driver Link

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 contains drivers and utilities for your system at <https://www.supermicro.com/wftp/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 drive or a DVD. (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.

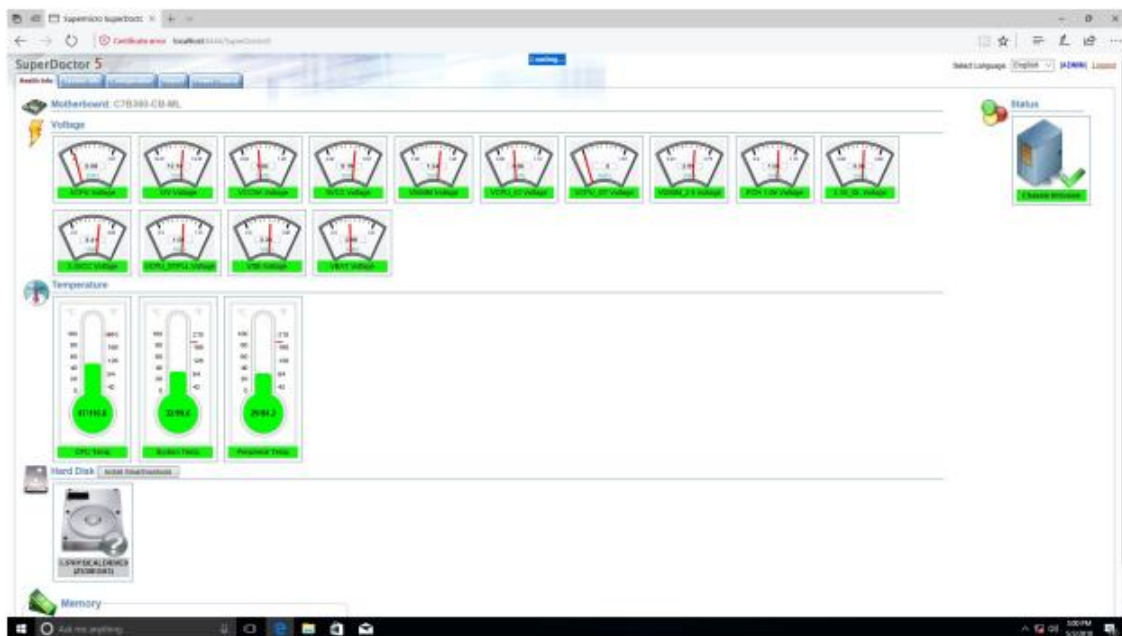


6-3 Driver & Tool Installation Screen

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 the 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, FTP, and SMTP services to optimize the efficiency of your operation. Note: The default User Name and Password for SuperDoctor 5 is ADMIN / ADMIN.



6-4 SuperDoctor 5 Interface Display Screen (Health Information)



## 6.4 IPMI

The X12SCZ-TLN4F/QF/F 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. Supermicro ships standard products with a unique password for the BMC ADMIN user. This password can be found on a label on the motherboard.

## Chapter 7: Appendix C Standardized Warning Statements

The following statements are industry standard warnings, provided to warn the user of situations which have the potential for bodily injury. Should you have questions or experience difficulty, contact Supermicro's Technical Support department for assistance. Only certified technicians should attempt to install or configure components. Read this section in its entirety before installing or configuring components. These warnings may also be found on our website at [http://www.supermicro.com/about/policies/safety\\_information.cfm](http://www.supermicro.com/about/policies/safety_information.cfm).

### Battery Handling



**Warning!** There is the danger of explosion if the battery is replaced incorrectly. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions

#### 電池の取り扱い

電池交換が正しく行われなかった場合、破裂の危険性があります。交換する電池はメーカーが推奨する型、または同等のものを使用下さい。使用済電池は製造元の指示に従って処分して下さい。

#### 警告

電池更換不當會有爆炸危險。請只使用同類電池或制造商推薦的功能相當的電池更換原有電池。請按製造商的說明處理廢舊電池。

#### 警告

電池更換不當會有爆炸危險。請使用製造商建議之相同或功能相當的電池更換原有電池。請按照製造商的說明指示處理廢棄舊電池。

#### Warnung

Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

## Attention

Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

## ¡Advertencia!

Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

## אזהרה!

קיימת סכנת פיצוץ של הסוללה במידה והוחלפה בדרך לא תקינה. יש להחליף את הסוללה בסוג התואם מחברת יצרן מומלצת. סילוק הסוללות המשומשות יש לבצע לפי הוראות היצרן.

هناك خطر من انفجار في حالة اسبدال البطارية بطريقة غير صحيحة فعلي

اسبدال البطارية

فقط بنفس النوع أو ما يعادلها مما أوصت به الشركة المصنعة

جخلص من البطاريات المسعملة وفقا لعمليات الشركة الصانعة

## 경고!

배터리가 올바르게 교체되지 않으면 폭발의 위험이 있습니다. 기존 배터리와 동일하거나 제조사에서 권장하는 동등한 종류의 배터리로만 교체해야 합니다. 제조사의 안내에 따라 사용된 배터리를 처리하여 주십시오.

## Waarschuwing

Er is ontploffingsgevaar indien de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type die door de fabrikant aanbevolen wordt. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften afgevoerd te worden.

## Product Disposal



**Warning!** Ultimate disposal of this product should be handled according to all national laws and regulations.

### 製品の廃棄

この製品を廃棄処分する場合、国の関係する全ての法律・条例に従い処理する必要があります。

### 警告

本产品的废弃处理应根据所有国家的法律和规章进行。

### 警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

### Warnung

Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.

### ¡Advertencia!

Al deshacerse por completo de este producto debe seguir todas las leyes y reglamentos nacionales.

### Attention

La mise au rebut ou le recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environnement. Renseignez-vous auprès de l'organisme compétent.

סילוק המוצר

אזהרה!

סילוק סופי של מוצר זה חייב להיות בהתאם להנחיות וחוקי המדינה.

عند التخلص النهائي من هذا المنتج ينبغي التعامل معه وفقا لجميع القوانين واللوائح الوطنية

### 경고!

이 제품은 해당 국가의 관련 법규 및 규정에 따라 폐기되어야 합니다.

### Waarschuwing

De uiteindelijke verwijdering van dit product dient te geschieden in overeenstemming met alle nationale wetten en reglementen.

## Chapter 8:Appendix D UEFI BIOS Recovery

Warning: Do not upgrade the BIOS unless your system has a BIOS-related issue. Flashing the wrong BIOS can cause irreparable damage to the system. In no event shall Supermicro be liable for direct, indirect, special, incidental, or consequential damages arising from a BIOS update. If you need to update the BIOS, do not shut down or reset the system while the BIOS is updating to avoid possible boot failure.

### 8.1 Overview

The Unified Extensible Firmware Interface (UEFI) provides a software-based interface between the operating system and the platform firmware in the pre-boot environment. The UEFI specification supports an architecture-independent mechanism that will allow the UEFI OS loader stored in an add-on card to boot the system. The UEFI offers clean, hands-off management to a computer during system boot.

### 8.2 Recovering the UEFI BIOS Image

A UEFI BIOS flash chip consists of a recovery BIOS block and a main BIOS block (a main BIOS image). The recovery block contains critical BIOS codes, including memory detection and recovery codes for the user to flash a healthy BIOS image if the original main BIOS image is corrupted. When the system power is first turned on, the boot block codes execute first. Once this process is completed, the main BIOS code will continue with system initialization and the remaining POST (Power-On Self-Test) routines. Note 1: Follow the BIOS recovery instructions below for BIOS recovery when the main BIOS block crashes. Note 2: When the BIOS recovery block crashes, you will need to follow the procedures to make a Returned Merchandise Authorization (RMA) request. (For a RMA request, please see section 3.5 for more information). Also, you may use the Supermicro Update Manager (SUM) Out-of-Band (OOB) ([https://www.supermicro.com.tw/products/nfo/SMS\\_SUM.cfm](https://www.supermicro.com.tw/products/nfo/SMS_SUM.cfm)) to reflash the BIOS.

### 8.3 Recovering the BIOS Block with a USB Device

This feature allows the user to recover the main BIOS image using a USB-attached device without additional utilities used. A USB flash device such as a USB Flash Drive, or a USB CD/DVD ROM/RW device can be used for this purpose. However, a USB Hard Disk drive cannot be used for BIOS recovery at this time

The file system supported by the recovery block is FAT (including FAT12, FAT16, and FAT32), which is installed on a bootable or non-bootable USB-attached device. However, the BIOS might need several minutes to locate the SUPER.ROM file if the media size becomes too large due to the huge volumes of folders and files stored in the device. To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below: 1. Using a different machine, copy the "Super.ROM" binary image file into the disc Root "\\" directory of a USB device or a writable CD/DVD.

Note 1: If you cannot locate the "Super.ROM" file in your driver disk, visit our website at [www.supermicro.com](http://www.supermicro.com) to download the BIOS package. Extract the BIOS binary image into a USB flash device and rename it "Super.ROM" for the BIOS recovery use.

Note 2: Before recovering the main BIOS image, confirm that the "Super.ROM" binary image file you download is the same version or a close version meant for your motherboard.


2. Insert the USB device that contains the new BIOS image ("Super.ROM") into your USB port and reset the system until the following screen appears:





3. After locating the new BIOS binary image, the system will enter the BIOS Recovery menu as shown below:



 **Note:** At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

4. When the screen as shown above displays, use the arrow keys to select the item "Proceed with flash update" and press the <Enter> key. You will see the BIOS recovery progress as shown in the screen below:

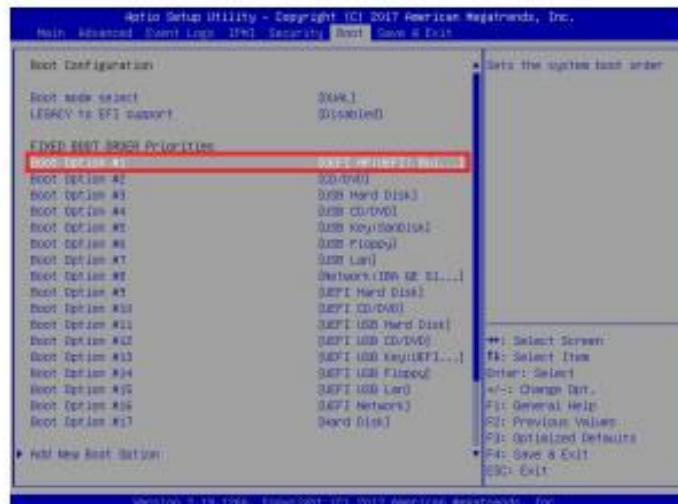
 **Note:** Do not interrupt the BIOS flashing process until it has completed.



5. After the BIOS recovery process is completed, press any key to reboot the system.
6. Using a different system, extract the BIOS package into a USB flash drive.



7. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the BIOS Setup utility.





- When the UEFI Shell prompt appears, type `fs#` to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 6. Enter `flash.nsh BIOSName.###` at the prompt to start the BIOS update process.

```

UEFI Interactive Shell v2.1
FS: FS:
UEFI v2.50 (American Megatrends, 8000000)
Flash: flash
FS# cd "\EFI\BOOT\" >
FS# fs#
FS# cd "\\P:\0001\F:\0004\BIOS\UEFI\MAIN\ASPM\UEFI.MBR" >
FS# flash.nsh BIOSName.###
[Redacted]
=====
UEFI Firmware Update Utility v2.31.0.1027
Copyright (C)2021 American Megatrends Inc. All Rights Reserved.
=====
Options = 0x000
Reading flash ..... Done
- MC Data Size checking ..... OK
- FF2 verification ..... OK
- Check checksum ..... OK
Erasing boot block ..... Done
Updating boot block ..... Done
Verifying boot block ..... Done
Flashing main block ..... 100% (2000000)

Verifying MB block ..... Done
- Update success for F0C
- Successful update Recovery Loader to SPI01
- Successful update SPI01
- Successful update SPI02
- Successful update SPI3 and SPI4
- MC Firmware Image update success !!
WARNING : System must power-off to have the changes take effect!
Please use "/FS#\EFI\BOOT\ASPM\UEFI.MBR" or "/FS#\0001\F:\0004\BIOS\UEFI\MAIN\ASPM\UEFI.MBR"
=====
+ Please ignore this 'Shell: Cannot read from file - device error'
+ warning message due to it does not impact flashing process.
=====
Retrieving '
Retrieval successful.
=====

```

**Note:** Do not interrupt this process until the BIOS flashing is complete.

- The screen above indicates that the BIOS update process is complete. When you see the screen above, unplug the AC power cable from the power supply, clear CMOS, and plug the AC power cable in the power supply again to power on the system.
- Press `<Del>` to enter the BIOS Setup utility.
- Press `<F3>` to load the default settings.
- After loading the default settings, press `<F4>` to save the settings and exit the BIOS Setup utility.