THOR200-U8-D

2.5U Half-Rack Data Recording Computer

User's Manual

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
Version 1.0	2025/07/07	Initial release

Packing list

☐ THOR200-U8-D 2.5U Half-Rack Data Recording Computer

☐ CD (Driver + Quick Installation Guide + Intel VROC RAID Configuration Guide + AOC-VROCxxxMOD. VMware ESXi User guide)

> If any of the above items is damaged or missing, please contact your local distributor.

Ordering Information

Model Number	Description
THOR200-U8-D	2.5U Half-Rack Data Recording Computer, Intel® XEON® D-2733NT 8 Cores/16 Threads 2.1 GHz/3.2 GHz, 64GB DDR4-3200 RDIMM ECC, Storage: 8 x Swappable 8 TB 2.5" U.2 NVMe SSD support RAID 0, 1, 5, 2 x 10G, 4 x 1G, 2x 25G SFP28, 2 x USB 3.0, 1 x IPMI, 1 x VGA, 1 x DC-In with D38999, 18~36VDC, Operating Temperature: -40°C to 60°C

Contents

1 CHAPTER 1: PRODUCT INTRODUCTION

1-1. Key Features

SYSTEM

High Performance Processor	Intel® XEON D-2733NT 2.1(3.2) GHz, 15MB, 80W, 8C/16T
Memory type	64GB DDR4-3200MHz RDIMM ECC
Chipset	SoC, integrated with CPU

DISPLAY

Graphics Processor	ASPEED AST2600
Resolution	Up to 1920x1200@60Hz 32bpp

STORAGE

Storage	8 x Swappable 8TB 2.5" NVMe SSD support RAID 0,1,5

ETHERNET

Ethernet Controller	Dual 25GbE SFP28 (SoC) Dual 10GBase-T (Intel X550-AT2) Quad 1GBase-T (Intel i350-AM4) IPMI LAN
TPM2.0	TPM Header & Chip both
RAID Card	Intel VROC Premium

FRONT I/O

IPMI	1x IPMI
USB	2x USB 3.0
LAN 1, 2	2 x 25GbE SFP28
LAN 3, 4	2x 10GbE Base-T
LAN 5, 6, 7, 8	4x 1GbE Base-T
Display	1x VGA
GND	1

REAR I/O

Swap Tray	8 x HDD/SSD Swappable Tray
Power Button	1 x w/Indicator LED
HDD LED	1
DC-IN	1 x D38999 connector

Operating System

Operating System	Windows Server 2022

Physical

Dimension (W x D x H)	220 x 400 x 111 mm (W x D x H)
Weight	11 Kg (24.25lbs)

Environmental

MIL-STD-810	Method 516.7 Shock 20G 11ms
Operating Temperature	-40 to +60°C
Storage Temperature	-40 to 85°C
Relative Humidity	5% to 95%, non-condensing

Specifications are subject to change without notice

1-2. Mechanical Dimensions
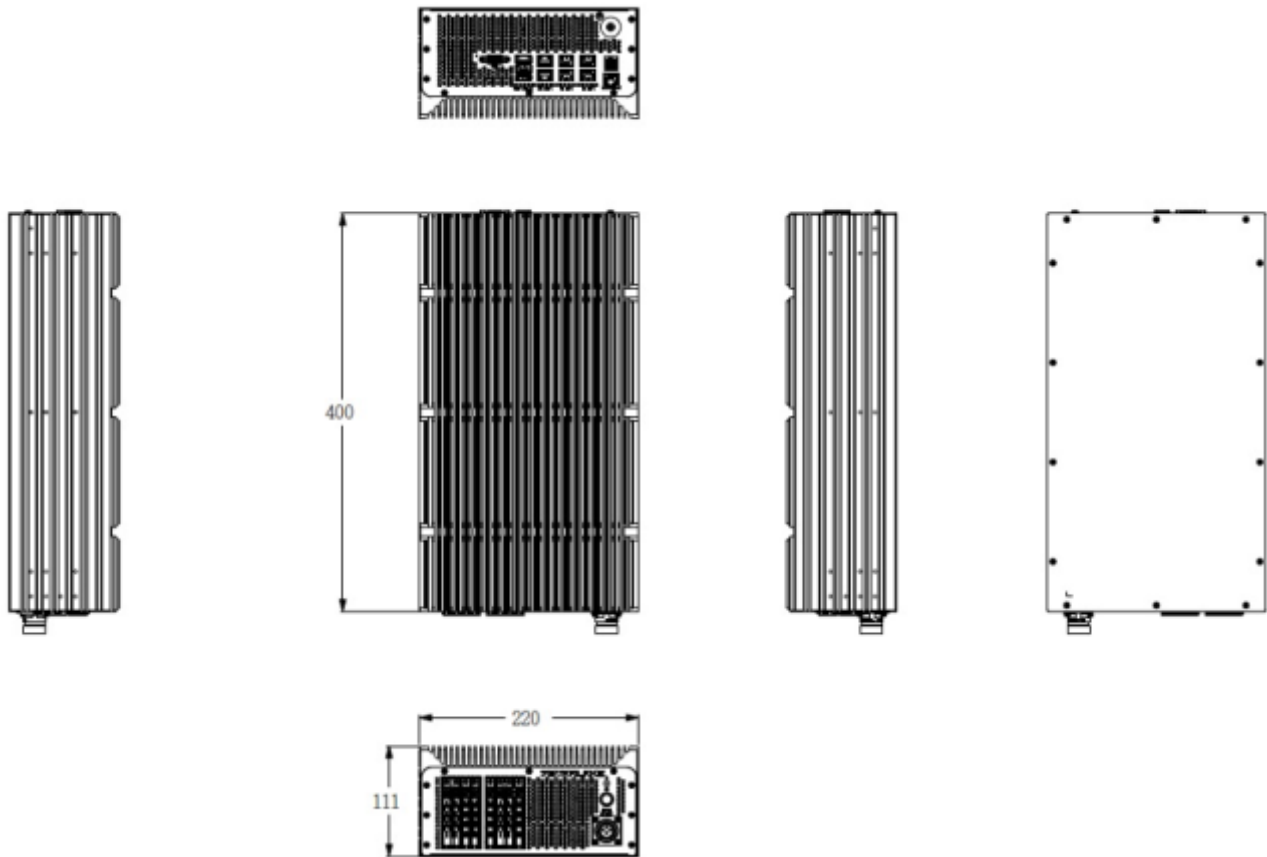
1-3. Front I/O

IPMI	Dedicated IPMI LAN Port
USB 3.0	2 x USB 3.0 Ports
LAN 1G	4 x RJ45 1GbE LAN Ports
LAN 10G	2 x RJ45 10GbE LAN Ports
LAN 25G	2 x SFP28 25GbE LAN Ports
VGA	1 x VGA Port
GND	1

1-4. REAR I/O

DC-IN	1 x D38999 Connector
Power Button	1 w/Indicator LED
HDD LED	1
Swap Tray	8 x HDD/SSD Swappable Tray

2 CHAPTER 2: CONNECTORS LOCATIONS

2.1 Front I/O Connector

IPMI LAN:

Dedicated IPMI LAN Port

2 x USB 3.0:

2xUSB 3.0

4 x 1GbE LAN:

4 x RJ45 1GbE LAN Ports

2 x 10GbE LAN:

2 xRJ45 10GbE LAN Ports

2 x 25GbE SFP28 LAN:

2x SFP28 25GbE LAN Ports

VGA Port:

VGA Port

2.2   REAR I/O Connector

SSD LED indicator:

Power button/DC-In:

Swappable Tray :

3   CHAPTER 3 UEFI BIOS

3-1   Introduction

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

Note: Due to periodic changes to the BIOS, some settings may have been added or deleted and might not yet be recorded in this manual. Please refer to the Manual Download area of our website for any changes to the BIOS that may not be reflected in this manual.

Starting the Setup Utility

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

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

Settings printed in Bold are the default values.

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

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

3-2   Main Setup

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

```
                        Aptio Setup - AMI
  Main  Advanced  BMC  Event Logs  Security  Boot  Save & Exit

  System Date                 [Thu 02/17/2022]       Set the Date. Use Tab to
  System Time                 [11:18:49]             switch between Date
                                                     elements.
  Supermicro X12SDV-4C-SPT8F                          Default Ranges:
  BIOS Version                T20220216101642        Year: 1998-9999
  Build Date                  02/16/2022             Months: 1-12
                                                     Days: Dependent on month
  Memory Information                                 Range of Years may vary.
  Total Memory                8192 MB


                                                     ++: Select Screen
                                                     ↑↓: Select Item
                                                     Enter: Select
                                                     +/-: Change Opt.
                                                     F1: General Help
                                                     F2: Previous Values
                                                     F3: Optimized Defaults
                                                     F4: Save & Exit
                                                     ESC: Exit

                 Version 2.22.1281 Copyright (C) 2022 AMI
```

System Date/System Time

Use this option to change the system date and time. Highlight System Date or System Time using the arrow keys. Enter new values using the keyboard. Press the <Tab> key or the arrow keys to move between fields. The date must be entered in MM/DD/YYYY format. The time is entered in HH:MM: SS format.

Note: The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00. The date's default value is the BIOS build date after RTC reset.

Supermicro X12SDV-8C-SPT8F

BIOS Version

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

Build Date

This feature displays the date when the version of the BIOS ROM used in the system was built.
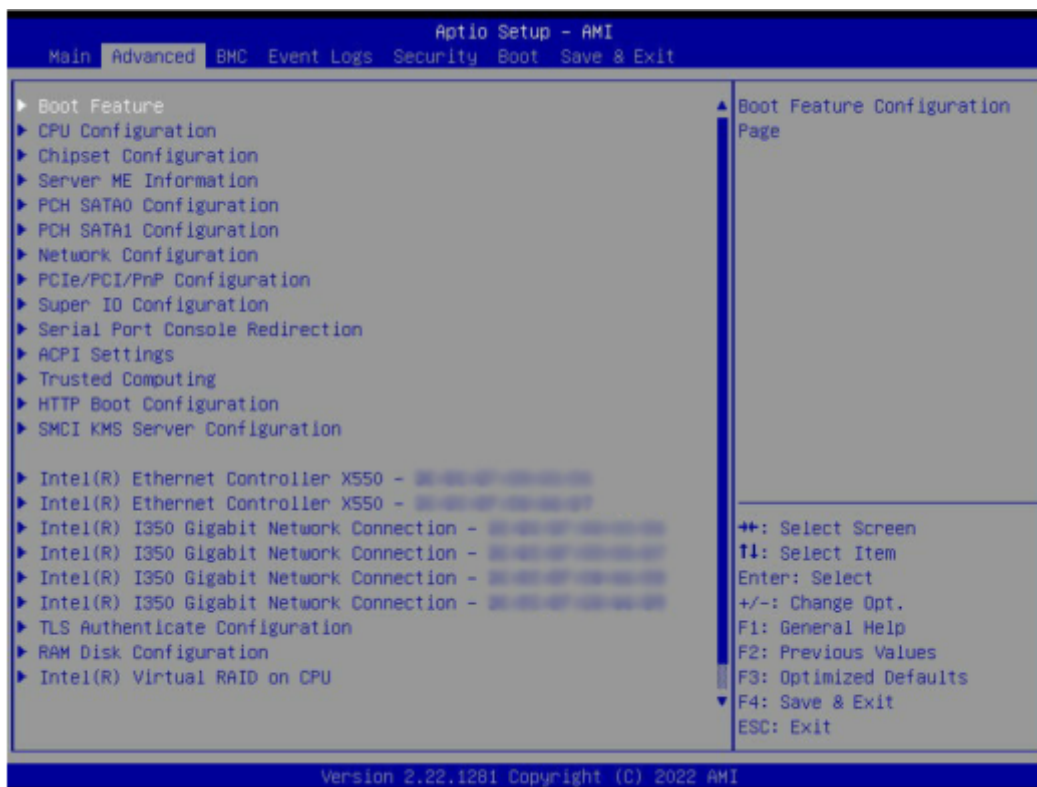
Memory Information

Total Memory

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

3-3   Advanced

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

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.

▶   Boot Feature

Quiet Boot

Use this feature to select the screen display between the POST messages and the OEM logo upon boot up. 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.

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 automatically reboots 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 allows 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.

Front USB Port(s) (Available when DCMS key is activated)

Select Enabled to allow the specific type of USB devices to be used in the front USB ports. Select Enabled (Dynamic) to allow or disallow this particular type of USB devices to be used in the front USB ports without rebooting the system. The options are Enabled, Disabled, and Enabled (Dynamic).

Rear USB Port(s) (Available when DCMS key is activated)

▶ Select Enabled to allow the specific type of USB devices to be used in the rear USB ports. Select Enabled (Dynamic) to allow or disallow this particular type of USB devices to be used in the rear USB ports without rebooting the system. The options are Enabled, Disabled, and Enabled (**Dynamic**).

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 you 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 you press the power button. The options are Instant Off and 4 Seconds Override.

▶ **CPU Configuration**

Processor Configuration

The following CPU information is displayed:
- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM (Per Core)
- L2 Cache RAM (Per Core)
- L3 Cache RAM (Per Package)
- Processor 0 Version

■ **CPU1 Core Disable Bitmap**

CPU1 Core Disable Bitmap

Available Bitmap

CPU Core Count

CPU1 Cores Enable

Select 0 to enable all cores or 17592186044415 (maximum) to disable all cores. One core must be enabled.

Hyper-Threading (ALL)

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

Hardware Prefetcher

If set to Enable, the hardware prefetcher prefetches 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.

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enable to enable the Data Cache Unit (DCU) Streamer Prefetcher, which streams and prefetches data and sends it to the Level 1 data cache to improve data processing and system performance. The options are Disable and Enable.

DCU IP Prefetcher (Available when supported by the CPU)

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

LLC Prefetch

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

Extended APIC

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

Enable Intel(R) TXT

Use this feature to enable or disable Intel Trusted Execution Technology support. The options are Disable and Enable.

VMX

Use this feature to enable or disable Vanderpool Technology. The options are Disable and

Enable.

Enable SMX

Use this feature to enable or disable Safer Mode Extensions. The options are Disable and Enable.

PPIN Control

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

AES-NI

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

TME, TME-MT, TDX

Total Memory Encryption (TME)

Use this feature to enable or disable total memory encryption. The options are Disabled and Enabled.

Software Guard Extension (SGX)

Limit CPU PA to 46 Bits

Use this feature to limit the CPU physical address to 46 bits to support older hyper-v. The options are Disable and Enable.

■ **Advanced Power Management Configuration**

Advanced Power Management Configuration

Power Performance Tuning

Use this feature to select whether the BIOS or the operating system chooses energy performance tuning. The options are OS Controls EPB, BIOS Controls EPB, and PECI Controls EPB.

*If the feature above is set to BIOS Controls EPB, the next feature is available for configuration:

ENERGY_PERF_BIAS CFG Mode

Use this feature to set the energy performance bias. The options are Maximum Performance,
Performance, Balanced Performance, Balanced Power, and Power.

■ **CPU P State Control**

CPU P State Control

SpeedStep (P-States)

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

AVX-P1

Use this feature to select the AVX-P1 level. The options are Normal, Level 1, and Level 2.

EIST PSD Function

This feature allows you to choose between Hardware and Software to control the processor's

frequency and performance (P-state). In HW_ALL mode, the processor hardware is responsible for coordinating the P-state, and the OS is responsible for keeping the P-state request up to date on all Logical Processors. In SW_ALL mode, the OS Power Manager is responsible for coordinating the P-state, and must initiate the transition on all Logical Processors. The options are HW_ALL and SW_ALL.

Turbo Mode

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

■ **Hardware PM State Control**

Hardware PM State Control

Hardware P-States

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

■ **Frequency Prioritization**

Frequency Prioritization

RAPL Prioritization

Use this feature to enable the RAPL balancer. The options are Enable and Disable.

■ **CPU C State Control**

CPU C State Control

Enable Monitor MWAIT

Select Enabled to enable the Monitor/Mwait instructions. The Monitor instructions monitors a region of memory for writes, and MWait instructions instruct the CPU to stop until the monitored region begins to write. The options are Disable and Enable.

CPU C6 Report

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

Enhanced Halt State (C1E)

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

■ **Package C State Control**

Package C State Control

Package C State

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

■ **CPU T State Control**

CPU T State Control

Software Controlled T-States

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

If the feature above is set to Enable, the next feature is available for configuration:

T-State Throttle Level

Use this feature to enable or disable CPU throttling, which reduces power consumption. The options are Disable, 6.25%, 12.5%, 18.75%, 25.0%, 31.25%, 37.5%, 43.75%, 50.0%, 56.25%, 62.5%, 68.75%, 75.0%, 81.25%, 87.5%, 93.75%.

▶ **Chipset Configuration**

Warning: Setting the wrong values in below sections may cause system to malfunction.

■ **North Bridge**

◆ **Uncore Configuration**

Uncore Configuration

- Number of CPU
- Number of IIO
- Current UPI Link Speed
- Current UPI Link Frequency
- Global MMIO Low Base / Limit
- Global MMIO High Base / Limit
- PCIe Configuration Base / Size

XPT Prefetch

Use this feature to enable or disable XPT Prefetch support, which allows an LLC request
to be duplicated and sent to an appropriate memory controller based on the recent LLC
history to reduce latency. The options are Disable, Enable, and Auto.

PCIe Remote P2P Relaxed Ordering

Enable peer-to-peer relaxed ordering to optimize system performance. The options are Disable and Enable.

Stale AtoS

Use this feature to enable or disable Stale A to S optimization. There are three states

in the in-memory directory: invalid (I), snoop All (A), and shared (S). Data in the I state is clean and does not exist in other sockets. Data in the A state may exist in another exclusive or modified socket. Data in the S state is clean and may be shared across one or more sockets. The options are Disable, Enable, and Auto.

LLC Dead Line Alloc

Select Enable to opportunistically fill dead lines in the LLC. Select Disable to never fill dead lines in LLC. The options are Disable, Enable, and Auto.

◆ **Memory Configuration**

Integrated Memory Controller (iMC)

Enforce POR

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

PPR Type

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

Memory Frequency

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

Data Scrambling for DDR4/5

Use this feature to enable or disable data scrambling for DDR4/5 memory. The options are Disable and Enable.

2x Refresh Enable

Use this feature to enable 2x memory refresh support to enhance memory performance. The options are Auto, Disable, and Enable.

◆ **Memory Topology**

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

◆ **Memory RAS Configuration Setup**

Memory RAS Configuration Setup

Enable Pcode WA for SAI PG

Use this feature to enable Pcode Work Around for SAI Policy group for A Step. The options are Disabled and Enabled.

Mirror Mode

Correctable Error Threshold

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

Partial Cache Line Sparing PCLS

Use this feature to enable or disable Partial Cache Line Sparing (PCLS). The options

are Disabled and Enabled.

ADDDC Sparing

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

Patrol Scrub

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

- **IIO Configuration**

IIO Configuration

- ◆ **CPU1 Configuration**

CPU Slot6 PCIe 4.0 x16 Bifurcation

Use this feature to configure the bifurcation setting for the PCIe port. The options are Auto, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

- ◆ **CPU SLOT6 PCIe 4.0 x16**

CPU SLOT6 PCIe 4.0 x16

Link Speed

Use this feature to select the link speed for the PCIe port. The options are Auto, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), Gen 3 (8 GT/s), and Gen 4 (16 GT/s).

The following information is displayed:

- ・PCIe Port Link Status
- ・PCIe Port Link Max
- ・PCIe Port Link Speed

PCIe Port Max Payload Size

Selecting Auto for this feature enables the motherboard to automatically detect the maximum Transaction Layer Packet (TLP) size for the connected PCIe device, allowing for maximum I/O efficiency. Selecting 128B or 256B designates maximum packet size of 128 or 256. The options are 128B, 256B, 512B, and Auto.

- ◆ **IOAT Configuration**

Disable TPH

Transparent Huge Pages (TPH) is a Linux memory management system that enables communication in larger blocks (pages). Enabling this feature increases performance. The options are No and Yes.

Prioritize TPH

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

Relaxed Ordering

Select Enable to enable Relaxed Ordering support, which allows certain transactions to violate the strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been enqueued. The options are Yes and No.

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

Intel® VT for Directed I/O (VT-d)

Intel® VT for Directed I/O (VT-d)

Select Yes to use Intel Virtualization Technology for Direct I/O VT-d support by reporting the I/O device assignments to the Virtual Machine Monitor (VMM) through the DMAR ACPI tables. This feature offers fully-protected I/O resource sharing across Intel platforms, providing greater reliability, security and availability in networking and data-sharing. The options are Enable and Disable.

ACS Control

Select Yes to program Access Control Services (ACS) to the chipset PCIe root port bridge. Select No to program ACS to all PCIe root port bridges. The options are Enable and Disable.

Interrupt Remapping

Use this feature to enable Interrupt Remapping support, which detects and controls external interrupt requests. The options are Enable, Disable, and Auto.

◆ **Intel® VMD Technology**

◆ **Intel® VMD for Volume Management Device on CPU1**

VMD Config for PCH ports

Enable/Disable VMD

Use this feature to enable or disable the volume management device for this stack. The options are Disable and Enable.

If the feature above is set to Enable, the following features are available for configuration:

JMD1:M.2-H PCIe 3.0 X4/S-SATA 3.0 VMD

Enable this feature to allow the VMD to control this root port. The options are Disable and Enable.

VMD Config for IOU 0

Enable/Disable VMD

Use this feature to enable or disable the volume management device for this stack. The options are Disable and Enable.

If the feature above is set to Enable, the following features are available for configuration:

CPU SLOT6 PCIe 4.0 X16 VMD Port 0 / CPU SLOT6 PCIe 4.0 X16 VMD Port 1 / CPU SLOT6 PCIe 4.0 X16 VMD Port 2 / CPU SLOT6 PCIe 4.0 X16 VMD Port 3

Use this feature to enable or disable the volume management device for this expansion slot. The options are Disable and Enable.

Hot Plug Capable

Use this feature to enable or disable hot plug for this port. The options are Disable and Enable.

VMD Config for IOU 4

Enable/Disable VMD

Use this feature to enable or disable the volume management device for this stack. The options are Disable and Enable.

If the feature above is set to Enable, the following features are available for configuration:
JSLIM1 PCIe 4.0 X8 VMD Port0 / JSLIM1 PCIe 4.0 X8 VMD Port1 / JSLIM2 PCIe 4.0 X8 VMD Port0 / JSLIM2 PCIe 4.0 X8 VMD Port1

Use this feature to enable or disable the volume management device for this expansion slot. The options are Disable and Enable.

Hot Plug Capable

Use this feature to enable or disable hot plug for this port. The options are Disable and Enable.

IIO eDPC Support

Use this feature to enable or disable IIO enhanced DPC support. The options are Disable, On Fatal Error, and On Fatal and Non-Fatal Errors.

PCIe ASPM Support (Global)

Use this feature to enable or disable ASPM support for all downstream devices. The options are Disable and Auto.

■ **South Bridge**

The following USB information is displayed:

・USB Module Version

・USB Devices

XHCI Hand-off

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

PCIe PLL SSC

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

▶ Server ME Information

The following General ME Configuration is displayed:

・ Oper. Firmware Version

・ Backup Firmware Version

・ Recovery Firmware Version

・ ME Firmware Status #1

・ ME Firmware Status #2

・ Current State

・ Error Code

▶ PCH SATA0 Configuration

PCH SATA Configuration

SATA Controller 0

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

SATA Mode Selection

Select AHCI to configure an sSATA drive specified as an AHCI drive. Select RAID to configure an sSATA drive specified as a RAID drive. The options are AHCI and RAID.

Support Aggressive Link Power Management

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

SATA 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 allows you 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 should be connected to a Solid State Drive or a Hard Disk Drive. The options are Hard Disk Drive and Solid State Drive.

▶ PCH SATA1 Configuration

PCH SATA1 Configuration

SATA Controller 1

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

SATA Mode Selection

Select AHCI to configure an sSATA drive specified as an AHCI drive. Select RAID to configure an sSATA drive specified as a RAID drive. The options are AHCI and RAID.

Support Aggressive Link Power Management

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

SATA Port 0/1/4/5/6/7

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

・ Software Preserve Support

SATA Port 0/1/4/5/6/7 Hot Plug

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

SATA Port 0/1/4/5/6/7 Spin Up Device

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

SATA Port 0/1/4/5/6/7 SATA Device Type

Use this feature to specify if the SATA port specified should be connected to a Solid State Drive or a Hard Disk Drive. The options are Hard Disk Drive and Solid State Drive.

▶ **Network Configuration**

Network Stack

Select Enabled to enable Preboot Execution Environment (PXE) or Unified Extensible Firmware Interface (UEFI) 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 is checked. Press "+" or "-" on your keyboard to change the value. The default setting is 1.

    MAC:XXXXXXXXXXXX-IPv6 Network Configuration
    MAC:XXXXXXXXXXXX-IPv4 Network Configuration
    MAC:XXXXXXXXXXXX-IPv6 Network Configuration
    MAC:XXXXXXXXXXXX-IPv4 Network Configuration
    MAC:XXXXXXXXXXXX-IPv6 Network Configuration
    MAC:XXXXXXXXXXXX-IPv4 Network Configuration
    MAC:XXXXXXXXXXXX-IPv6 Network Configuration
    MAC:XXXXXXXXXXXX-IPv4 Network Configuration
    MAC:XXXXXXXXXXXX-IPv6 Network Configuration
    MAC:XXXXXXXXXXXX-IPv4 Network Configuration
    MAC:XXXXXXXXXXXX-IPv6 Network Configuration
    MAC:XXXXXXXXXXXX-IPv4 Network Configuration

▶ **Enter Configuration Menu**

    Interface Name
    Interface Type
    MAC Address
    Host addresses
    Route Table
    Gateway addresses

DNS addresses

Interface ID

Use this feature to set the 64-bit alternative interface ID for the device.

DAD Transmit Count

If this set feature is set to 0, the Duplication Address Detection is not performed. Set the value to a preferred selection.

Policy

Use this feature to set the policy to automatic or manual. The options or automatic and manual.

Save Changes and Exit

Select this feature to save the changes for the features above and exit.

▶ PCIe/PCI/PnP Configuration

PCI Bus Driver Version

PCI Devices Common Settings:

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

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

SR-IOV Support

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

ARI Support

Use this feature to enable or disable ARI support. The options are Disabled and Enabled.

Bus Master Enable

Use this feature to enable the Bus Master, which enables the Bus Master Attribute for DMA transaction. The options are Disabled and Enabled.

Consistent Device Name Support

Use this feature to enable ACPI_DSM device name support for onboard devices and slots. The options are Disabled and Enabled.

MMIO High Base

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

MMIO High Granularity Size

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

Maximum Read Request

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

MMCFG Base

Use this feature to select the low base address for PCIe adapters to increase base memory. The options are 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, and Auto.

NVMe Firmware Source

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

VGA Priority

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

CPU SLOT6 PCIe 4.0 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 and EFI.

JMD1:M.2-H PCIe 3.0 X4/S-SATA 3.0 OPROM

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

Intel X550 LAN5/6 Support

Use this feature to enable or disable the Intel X550 LAN5/6 device. The options are Disabled and Enabled.

Intel I350 LAN1/2/3/4 Support

Use this feature to enable or disable the Intel X550 LAN1/2/3/4/5 devices. The options are Disabled and Enabled.

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 and EFI.

▶ **Super IO Configuration**

Super IO Configuration

The following Super IO information is display:

・Super IO Chip AST2600

■ **Serial Port 1 Configuration**

Serial Port 1 Configuration

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

Serial Port

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

Device Settings

This feature displays the status of the serial port.

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of the serial port. 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 Configuration

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

Serial Port

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

Device Settings

This feature displays the status of the serial port.

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of the serial port. 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 Console Redirection

COM1

Console Redirection

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

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

■ **COM1 Console Redirection Settings**

COM1

Console Redirection Settings

Terminal Type

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

Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, VT-UTF8, and ANSI.

Bits Per Second

Use this feature to set the transmission speed for a serial port used in Console Redirection.

Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 38400, 57600 and 115200 (bits per second).

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

Redirection After BIOS POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When set to Bootloader, legacy console redirection is disabled before booting the OS. When set to Always Enable, legacy console redirection remains enabled when booting the OS. The

options are Always Enable and Bootloader.

SOL 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 are available for configuration:**

■ **SOL Console Redirection Settings**

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 ANSI, VT100, VT100+, and VT-UTF8.

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

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

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

Console Redirection EMS

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

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

■ **EMS Console Redirection Settings**

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

Out-of-Band Mgmt Port

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

Terminal Type

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

Bits Per Second EMS

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

Flow Control EMS

Use this item 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 EMS

Parity EMS

Stop Bits EMS

▶ **ACPI Settings**

ACPI Settings

WHEA Support

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

Headless Support

This feature is used to enable the system to function without a keyboard, monitor or mouse attached. 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.

RTC Wake Systm From S4/S5

Use this feature to enable or disable the system wake on alarm event.. The options are Disabled and Enabled.

▶ Trusted Computing

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

・Firmware Version

・Vendor

Security Device Support

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

Active PCR Bank

Available PCR banks

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.

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 to be performed in TCG Storage devices. The options are Enabled and Disabled.

TXT Support

Intel Trusted Execution Technology (TXT) helps protect against software-based attacks and ensures protection, confidentiality, and integrity of data stored or created on the system. Use this feature to enable or disable TXT Support. The options are Disabled and Enabled.

▶ **HTTP Boot Configuration**

HTTP Boot Configuration

HTTP Boot Policy

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

HTTPS Boot Checks Hostname

Use this feature to select whether HTTPS Boot checks the hostname of TLS certificates matches the hostname provided by the remote server. The options are Enabled and Disabled (WARNING: Security Risk!).

Priority of HTTP Boot:

Instance of Priority 1:

Use this feature to set the rank target port. The default value is 1.

Select IPv4 or IPv6

Use this feature to select which LAN port to boot from. The options are IPv4 and IPv6.

Boot Description

Highlight the feature and press enter to create a boot description. The description cannot be more than 75 characters.

Boot URI

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

Instance of Priority 2 - Priority 4:

Use this feature to set the rank target port. The default value is 0.

▶ **SMCI KMS Server Configuration**

SMCI KMS Server IP address

Enter the IP4 address in dotted-decimal notation (e.g., 255.255.255.255).

Second SMCI KMS Server IP address

Enter the IP4 address in dotted-decimal notation (e.g., 255.255.255.255).

SMCI KMS TCP Port number

Enter the KMIP TCP port number (from 100 to 9999) The default is 5696.

KMS Time Out

Use this feature to determine when the server connection times out. The range is 5 - 30 seconds. The default is 5.

SMCI KMS Server Retry Count

Use this feature to test the connection to the Key Manage Server. The range is 0 - 10. 0 means retrying infinitely. The default option is 2.

TimeZone

Use this feature to select the current time zone.

TCG Nvme KMS Policy

Use this feature to select the Trusted Computing Group (TCG) NVMe KMS policy. The options are Normal Unlock, Do Nothing, Reset All Devices Deleted Key Id List.

Client UserName

Press Enter to create a client username.

Client Password

Press Enter to create a client username password.

KMS TLS Certificate

- **CA Certificate**

  Use this feature to enroll factory defaults or load the CA certificates from a file. The options are Update, Delete, and Export.

- **Client Certificate**

  Use this feature to enroll factory defaults or load the client certificates from a file. The options are Update, Delete, and Export.

- **Client Private Key**

  Use this feature to enroll factory defaults or load the client private key from a file. The options are Update, Delete, and Export.

▶ **Intel(R) Ethernet Controller X550 - XX:XX:XX:XX:XX:XX**

▶ **Intel(R) Ethernet Controller X550 - XX:XX:XX:XX:XX:XX**

▶ **Intel(R) I350 Gigabit Network Connection - XX:XX:XX:XX:XX:XX**

- **Firmware Image Properties**

  This submenu displays NVM firmware detected by the system.

- **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 allows 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) I350 Gigabit Network Connection - XX:XX:XX:XX:XX:XX**

▶ **Intel(R) I350 Gigabit Network Connection - XX:XX:XX:XX:XX:XX**

▶ **Intel(R) I350 Gigabit Network Connection - XX:XX:XX:XX:XX:XX**

■ **Firmware Image Properties**

This submenu displays NVM firmware detected by the system.

■ **NIC Configuration**

Legacy Boot Protocol

Use this feature to select a non-UEFI boot protocol. The options are None, PXE, iSCSI Primary, and iSCSI Secondary.

Link Speed

Wake On LAN

Select Enabled for wake on LAN support, which allows the system to wake up when an onboard LAN device receives an incoming signal. The options are Disabled and Enabled.

Legacy Virtual LAN ID

Use this feature to specify the VLAN ID used for PXE VLAN Mode. The VLAN ID range is 0 - 4094. This setting is only applicable when the System ROM boots in Legacy BIOS mode.

PCI Virtual Functions Advertised

■ **Device Level Configuration Menu**

Virtualization Mode

Active Physical Functions

Use this feature to specify which physical functions are enabled. Disabled functions will not be exposed and their associated ports will be completely shut down. The options are PF0 only, PF0 and PF1, PF0, PF1 and PF2, PF0, PF1, PF2 and PF3, PF0, PF1, PF2, PF3 and PF4, PF0, PF1, PF2, PF3, PF4 and PF5, PF0, PF1, PF2, PF3, PF4, PF5 and PF6, and All.

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

▶ TLS Authentication Configuration

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

■ **Server CA Configuration**

■ **Enroll Certification**

Enroll Certification Using File

Use this feature to enroll certification from a file.

Certification GUID

Use this feature to input the certification GUID.

Commit Changes and Exit

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

Discard Changes and Exit

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

■ **Delete Certification**

Use this feature to delete certification.

◆ **Client Certification Configuration**

▶ RAM Disk Configuration

This submenu allows you to configure the settings for the RAM disks installed in the system.

Disk Memory Type

This feature specifies the type of memory that is available for you to create a RAM disk. The options are Boot Service Data and Reserved.

■ **Create raw**

This feature allows you to create a raw RAM disk from all available memory modules in the system.

Size (Hex)

Use this feature to set the size of the raw RAM disk. The default setting is 1.

Create & Exit

Select this feature when you want to exit from this submenu after you've created a raw RAM disk.

Discard & Exit

Select this feature when you want to abandon the changes you've made and to exit from this submenu.

- **Create from file**

This feature allows the user to create a RAM disk from a file specified by the user..

Created RAM disk list

Remove selected RAM disk(s).

Use this feature to delete the RAM disk(s) specified by the user.

- **Intel(R) VROC SATA Controller**

Note 1: This feature is based on your system and related device(s) installed.

Note 2: This feature is available when "SATA Mode Selection" is set to RAID.

Note 3: Refer to PCH SATA0 Configuration, PCH SATA1 Configuration, and PCH SATA2 Configuration submenus in BIOS Setup main menu to set "SATA Mode Selection".

The following information is displayed.

- Intel VROC SATA driver version

- ◆ **Create RAID Volume**

  Use this feature to create and configure the settings of the RAID volume(s).

  Non-RAID Physical Disks:

  This feature displays the information of non-RAID physical disk(s).

  RAID Volumes:

  This feature displays the information of RAID volumes have been created earlier.

- **Intel(R) VROC sSATA Controller**

Note 1: This feature is based on your system and related device(s) installed.

Note 2: This feature is available when "SATA Mode Selection" is set to RAID.

Note 3: Refer to PCH SATA0 Configuration, PCH SATA1 Configuration, and PCH SATA2 Configuration submenus in BIOS Setup main menu to set "SATA Mode Selection".

The following information is displayed.

- Intel VROC sSATA driver version

▶ Intel(R) Virtual RAID on CPU

RAID volumes and Intel VMD Controllers information will be displayed if they are detected by the system.

- Intel VROC Managed Volumes:

- **Volume0, RAID0(Stripe), 1768.89GB, Normal**

  RAID VOLUME INFO

  Volume Actions

- ◆ Delete

  Name

  RAID Level

Stip Size

Size

Status

Bootable

Block size

Raid Member Disks

◆ **INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB**

INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB

Disk Actions:

Reset to non-RAID

This feature removes RAID data from the disk.

Locate LED

This feature sends locate LED command to a drive. The options are Off and On.

Controller

Model Number

Serial Number

Size

Status

Block Size

Root Port Number

Root Port Offset

Slot Number

Socket Number

VMD Controller Number

PCI Bus:Device.Function

VMD Bus:Device.Function

Port 4:2, Slot 0, CPU0, VMD4, BDF 03:00.0

◆ **INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB**

INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB

Disk Actions:

Reset to non-RAID

This feature removes RAID data from the disk.

Locate LED

This feature sends locate LED command to a drive. The options are Off and On.

Controller

Model Number

Serial Number

Size

Status

Block Size

Root Port Number

Root Port Offset

Slot Number

Socket Number

VMD Controller Number

PCI Bus:Device.Function

VMD Bus:Device.Function

Port 4:3, Slot 0, CPU0, VMD4, BDF 04:00.0

Intel VROC Managed Controllers:

- **All Intel VMD Controllers**
  - ◆ **Create RAID Volume**

    Create RAID Volume

    Name

    Enter a unique volume name that does not contain a space at the beginning or backslash. The name must be 16 characters or less.

    RAID Level

    Use this feature to select the RAID Level. The default option is RAID0(Stripe).

    Enable RAID Spanned over VMD Controllers

    Use this feature to enable RAID Spanned over VMD controllers.

    Select Disks:

    INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB Port 4:2 CPU0 VMD4

    Select X to select the disk.

    INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB Port 4:3 CPU0 VMD4

    Select X to select the disk.

    *If the feature above is selected, the following features are available for configuration:

    Strip Size

    Use this feature to select the size of the strip. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and 128KB.

    Capacity (GB)

    Use this feature to enter the desired volume size in gigabytes. The default capacity is approximately 95% of the maximum size. 0 will be treated as the maximum size.

  - ◆ **Create Volume**

    This submenu will allow you to create a volume with the settings you specified above.

    RAID Volumes:

  - ◆ **Volume0, RAID0(Stripe), 2831, 78GB, Normal**

    RAID VOLUME INFO

Volume Actions

◆ **Delete**

Name

RAID Level

Stip Size

Size

Status

Bootable

Block size

Raid Member Disks

◆ **INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB**

Disk Actions:

Reset to non-RAID

This feature removes RAID data from the disk.

Locate LED

This feature sends locate LED command to a drive. The options are Off and On.

Controller

Model Number

Serial Number

Size

Status

Block Size

Root Port Number

Root Port Offset

Slot Number

Socket Number

VMD Controller Number

PCI Bus:Device.Function

VMD Bus:Device.Function

Port 4:2, Slot 0, CPU0, VMD4, BDF 03:00.0

◆ **INTEL SSDPE2KE016T8 SN:PHLN928100J11P6AGN, 1490, 42GB**

Disk Actions:

Reset to non-RAID

This feature removes RAID data from the disk.

Locate LED

This feature sends locate LED command to a drive. The options are Off and On.

Controller

Model Number

Serial Number

Size

Status

Block Size

Root Port Number

Root Port Offset

Slot Number

Socket Number

VMD Controller Number

PCI Bus:Device.Function

VMD Bus:Device.Function

■ **Driver Health**

This submenu provides the health status for the network drivers and controllers, and all UEFI drivers detected by the system.

◆ **Intel(R) VROC with VMD Technology 7.7.0.1052**

Controller 5F9F2F98 Child 0

◆ **Intel(R) VROC 7.7.0.1054 SATA Driver**

◆ **Intel(R) PRO/1000 9.3.10 PCIe**

Controller 5ED9D898 Child 0

Intel(R) I350 Gigabit Network Connection

◆ **Intel(R) 10GbE Driver 7.9.05 x64**

Controller 5EDD7398 Child 0

Intel(R) Ethernet Controller X550

◆ **Intel(R) 10GbE Driver 7.9.05 x64**

Controller 5ED9D018 Child 0

Intel(R) Ethernet Controller X550

◆ **Intel(R) 100GbE 3.1.18**

3-4 BMC

Use this menu to configure BMC settings.
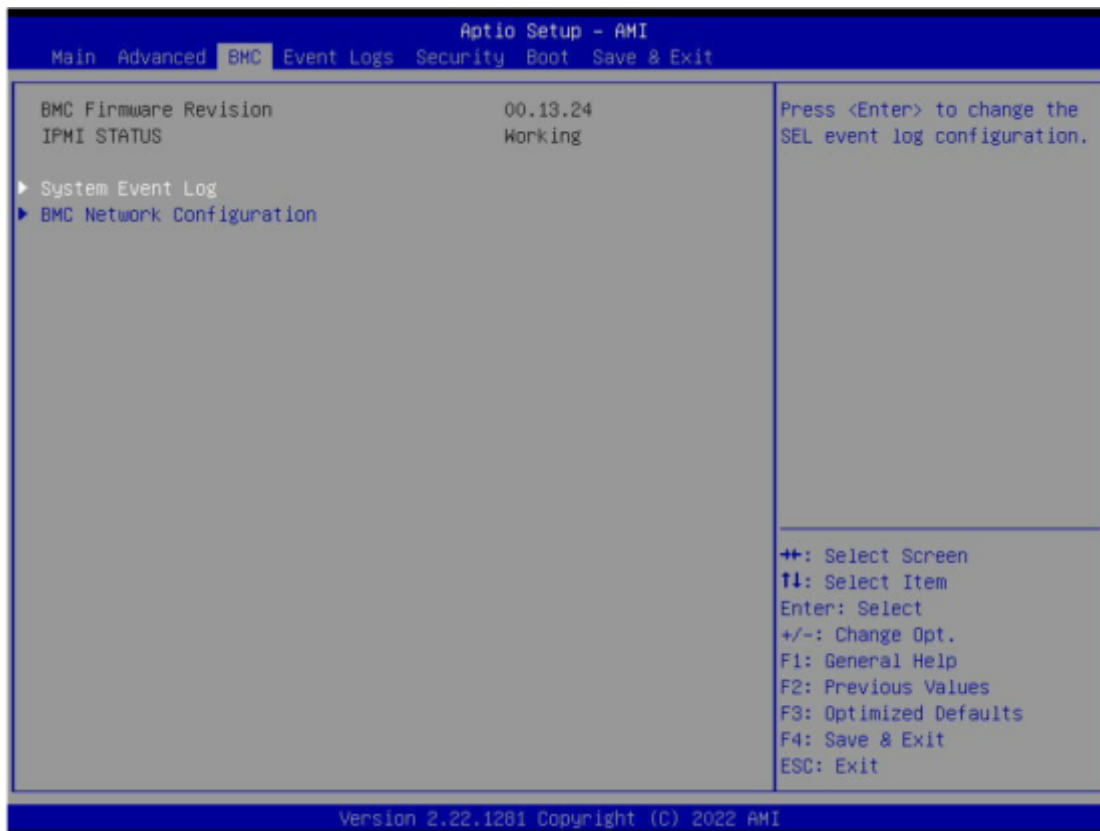
BMC Firmware Revision

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

IPMI STATUS (Baseboard Management Controller)

This feature displays 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 boot up. The options are Disabled and Enabled.

Erasing Settings

Erase SEL

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

When SEL is Full

This feature allows you to decide what the BIOS should do when the system event log is full.

Select Erase Immediately to erase all events in the log when the system event log is full. The options are Do Nothing and Erase Immediately.

Note: All values changed here do not take effect until computer is restarted.

▶ 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 are available for configuration:

Configure IPv4 Support

IPMI LAN Selection

IPMI Network Link Status

Configuration Address Source

This feature allows you to select the source of the IP address for this computer. If Static is selected, you 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 searches for a Dynamic Host Configuration Protocol (DHCP) 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 feature 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.

Configure IPv6 Support

IPv6 Address Status

IPv6 Support

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

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

Configuration Address Source

This feature allows you to select the source of the IP address for this computer. If Static is selected, you 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 searches for a Dynamic Host Configuration Protocol (DHCP) 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 IPv6 Address

This feature displays the Station IPv6 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).

Prefix Length

Use this feature to set the IPv6 prefix length from the BMC.

IPv6 Router1 IP Address

This feature displays the IPv6 Router1 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).

3-5 Event Logs

Use this menu to configure the following security settings for the system.
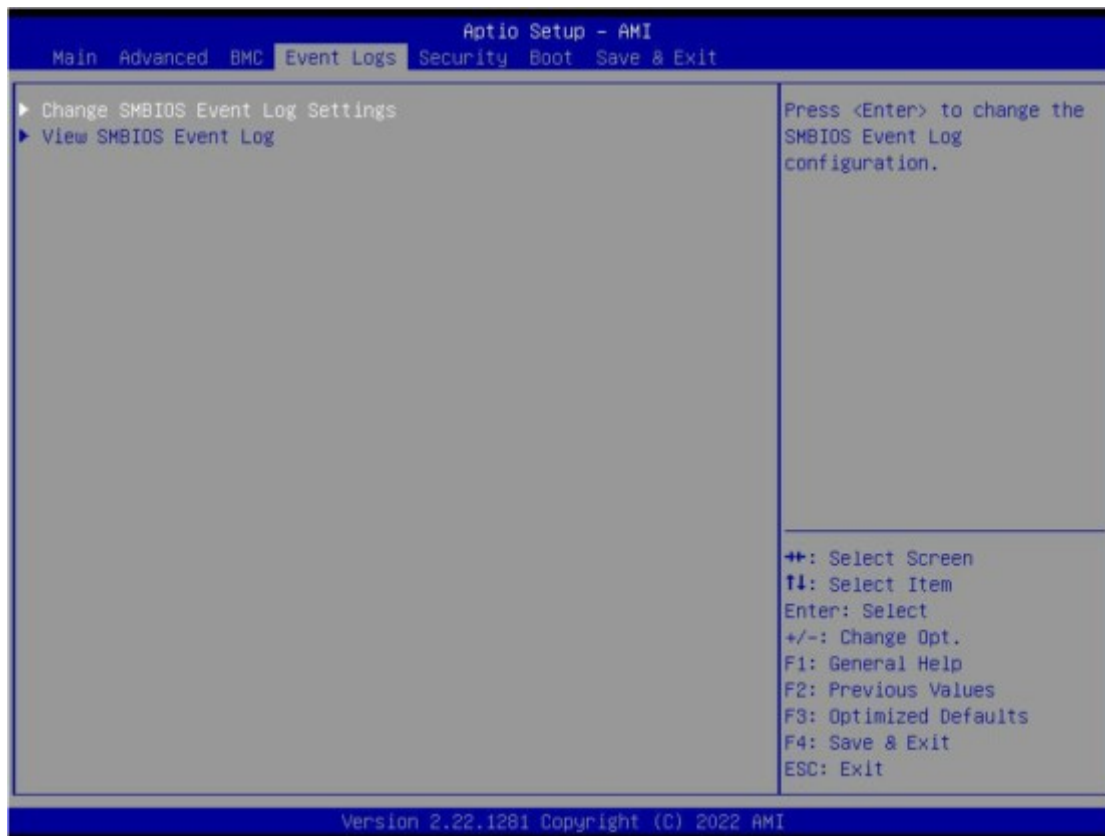
▶ **Change SMBIOS Event Log Settings**

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: All values changed here do not take effect until computer is restarted.

▶ **View SMBIOS Event Log**

Select this submenu and press enter to see the contents of the SMBIOS event log. The following categories is displayed: Date/Time/Error Codes/Severity.

3-6 Security

Use this menu to configure Security settings.
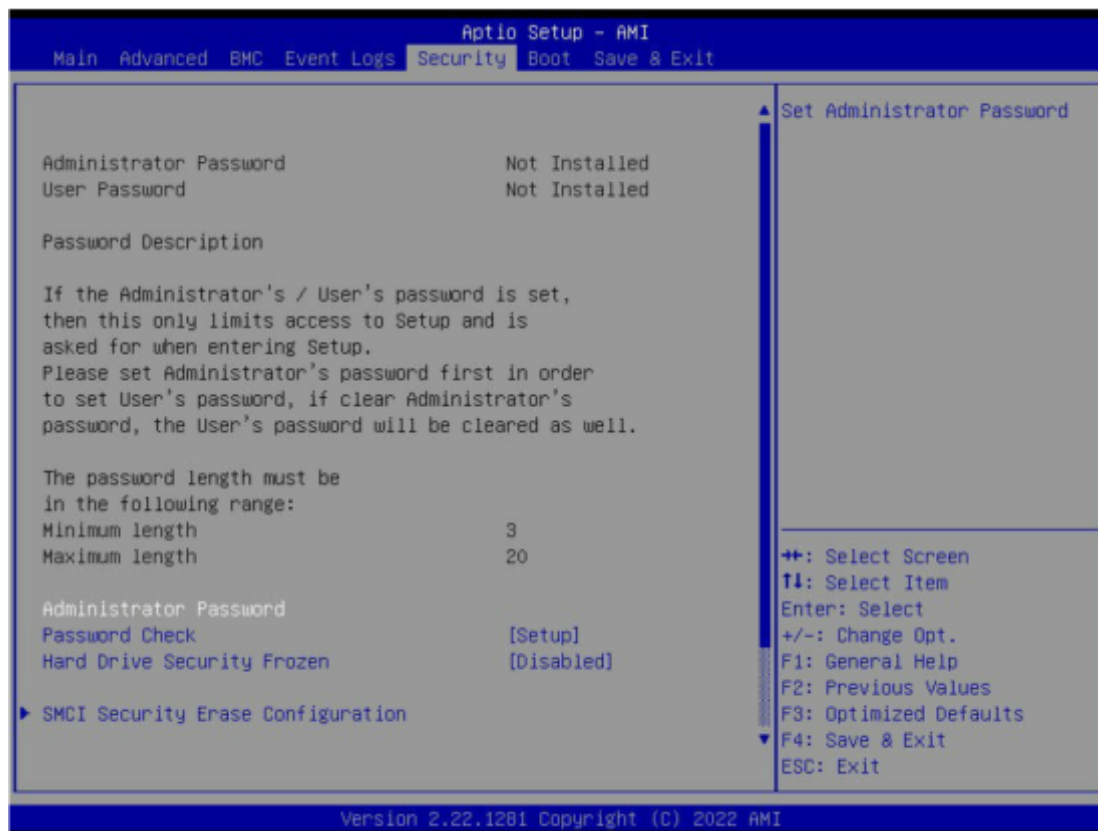
Administrator Password

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

Password Check

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

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.

▶ SMCI Security Erase Configuration

Select this submenu and press enter to see the information to delete the SMCI security

configuration.

HDD Name

HDD Serial Number

Security Mode

Security Function

Enable or Disable this feature to erase the device without a password. The options are Disable

and Security Erase - Without Password.

HDD Name

HDD Serial Number

Security Mode

Security Function

Enable or Disable this feature to erase the device without a password. The options are Disable and Security Erase - Without Password.

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
- ・Vendor Keys
- ・Secure Boot

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.
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.

▶ Key Management

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

Vendor Keys

Provision Factory Defaults

Use this feature to install the factory default secure boot keys after the platform has reset and while the system is in Setup mode. The options are Disabled and Enabled.

- ■ **Restore Factory Keys**

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

- ■ **Reset to Setup Mode**

- ■ **Export Secure Boot variables**

  This feature allows you 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**

◆ **Restore DB defaults**

Select Yes to restore the DB defaults.

Secure Boot Variable

■ **Platform Key (PK)**
Update
Select Yes to load a factory default PK or No to load from a file on an external media.

■ **Key Exchange Key**
Update
Select Yes to load a factory default KEK or No to load from a file on an external media.
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. The options are Yes and No.

■ **Authorized Signatures**
Update
Select Yes to load a factory default DB or No to load from a file on an external media.
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. The options are Yes and No.

■ **Forbidden Signatures**
Update
Select Yes to load a factory default DBX or No to load from a file on an external media.
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. The options are Yes and No.

■ **Authorized TimeStamps**
Update
Select Yes to load a factory default DBT or No to load from a file on an external media.
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. The options are Yes and No.

■ **OsRecovery Signature**
Update
Select Yes to load a factory default DBR or No to load from a file on an external media.
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. The options are Yes and No.

3-7 Boot

Use this menu to configure Boot settings.
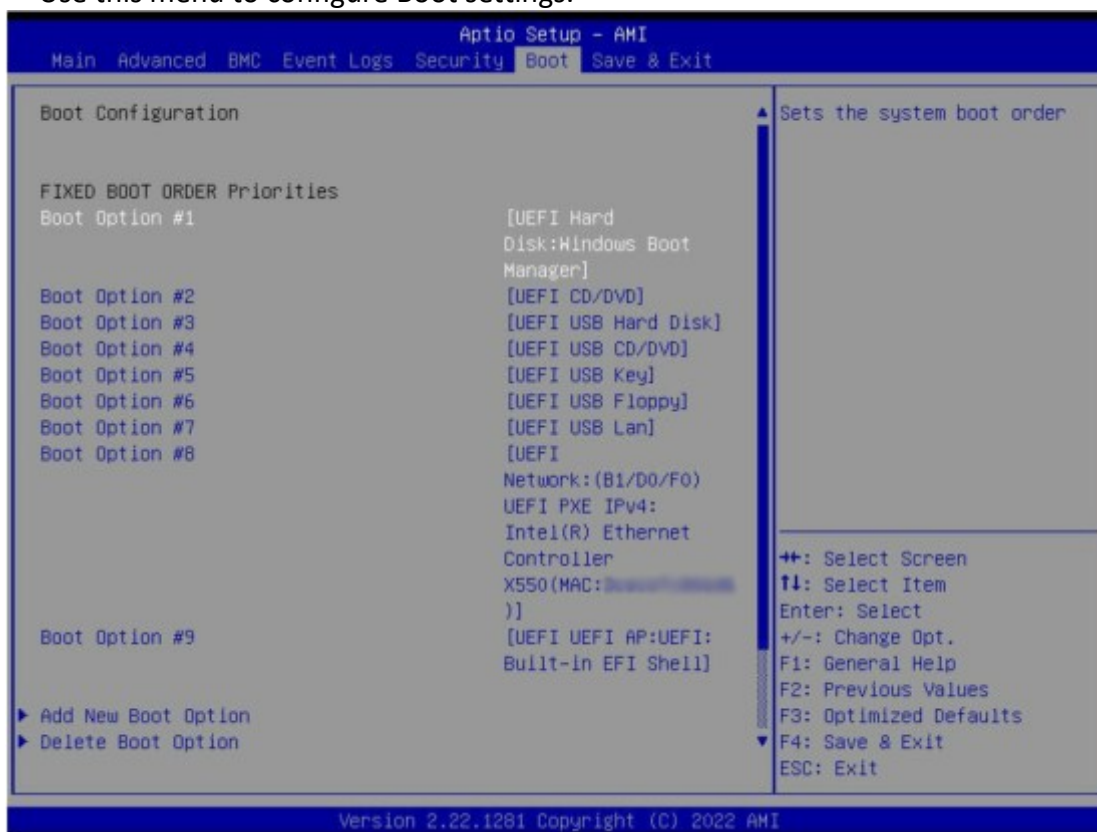
Boot Configuration
FIXED BOOT ORDER Priorities
・ Boot Option #1
・ Boot Option #2
・ Boot Option #3
・ Boot Option #4
・ Boot Option #5
・ Boot Option #6
・ Boot Option #7
・ Boot Option #8
・ Boot Option #9

■ **Add New Boot Option**
This feature allows you to add a boot option to the boot priority list.
Add New Boot Option
Add boot option
Use this feature to specify the name for a new boot option to add to the boot priority list.
Path for boot option
Use this feature to enter the path to the boot option.
Boot option File Path
Create

Use this feature to create the newly formed boot option.

■ **Delete Boot Option**

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

Delete Boot Option

Delete Boot Option

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

■ **UEFI Hard Disk Drive BBS Priorities**

This feature sets the system boot order of Hard Disk Drives.

・Boot Option #1

■ **UEFI NETWORK Drive BBS Priorities**

This feature sets the system boot order of detected devices.

・Boot Option #1 - #6

■ **UEFI Application Boot Priorities**

This feature sets the system boot order of detected devices.

・Boot Option #1

3-8 Save & Exit

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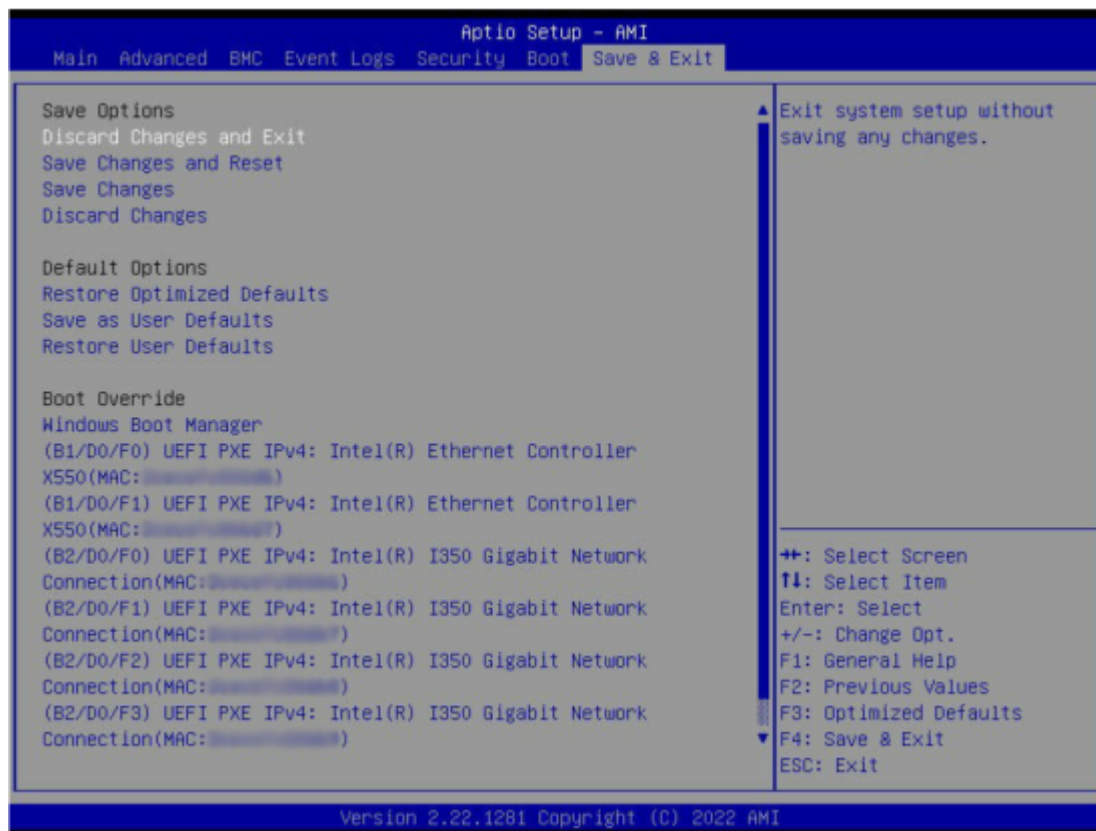
Save Options

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 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

Restore 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 you 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

Windows Boot Manager

(B1/D0/F0) UEFI PXE IPv4: Intel(R) Ethernet Controller X550 (MAC:xxxxxxxxxxxx)

(B1/D0/F0) UEFI PXE IPv4: Intel(R) Ethernet Controller X550 (MAC:xxxxxxxxxxxx)

(B2/D0/F0) UEFI PXE IPv4: Intel(R) I350 Gigabit Network Connection (MAC:xxxxxxxxxxxx)

(B2/D0/F3) UEFI PXE IPv4: Intel(R) I350 Gigabit Network Connection (MAC:xxxxxxxxxxxx)

(B2/D0/F0) UEFI PXE IPv4: Intel(R) I350 Gigabit Network Connection (MAC:xxxxxxxxxxxx)

(B2/D0/F0) UEFI PXE IPv4: Intel(R) I350 Gigabit Network Connection (MAC:xxxxxxxxxxxx)

UEFI: Built-in EFI Shell

Launch EFI Shell from filesystem device

This feature attempts to launch EFI Shell application from one of the available filesystem devices.

Appendix A

BIOS Codes

A.1 BIOS Error POST (Beep) Codes

During the Power-On Self-Test (POST) 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 process. 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 that can be heard on an external buzzer connected to JD1. 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

A.2 Additional BIOS POST Codes

The AMI BIOS supplies additional checkpoint codes, which are documented online at http://www.supermicro.com/support/manuals/ ("AMI BIOS POST Codes User's Guide").
When BIOS performs the Power On Self Test, it writes checkpoint codes to I/O port 0080h. For information on AMI updates, refer to http://www.ami.com/products/.

Appendix B

Software

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

B.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.

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That can be a USB flash or media 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.
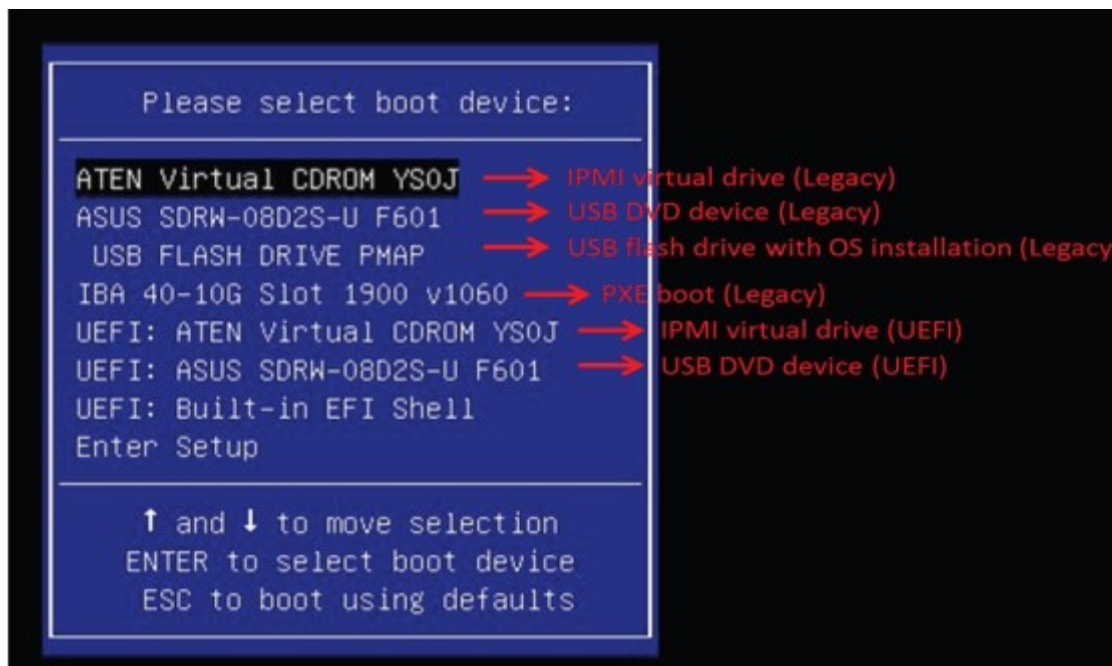
Figure B-1. Select Boot Device

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.
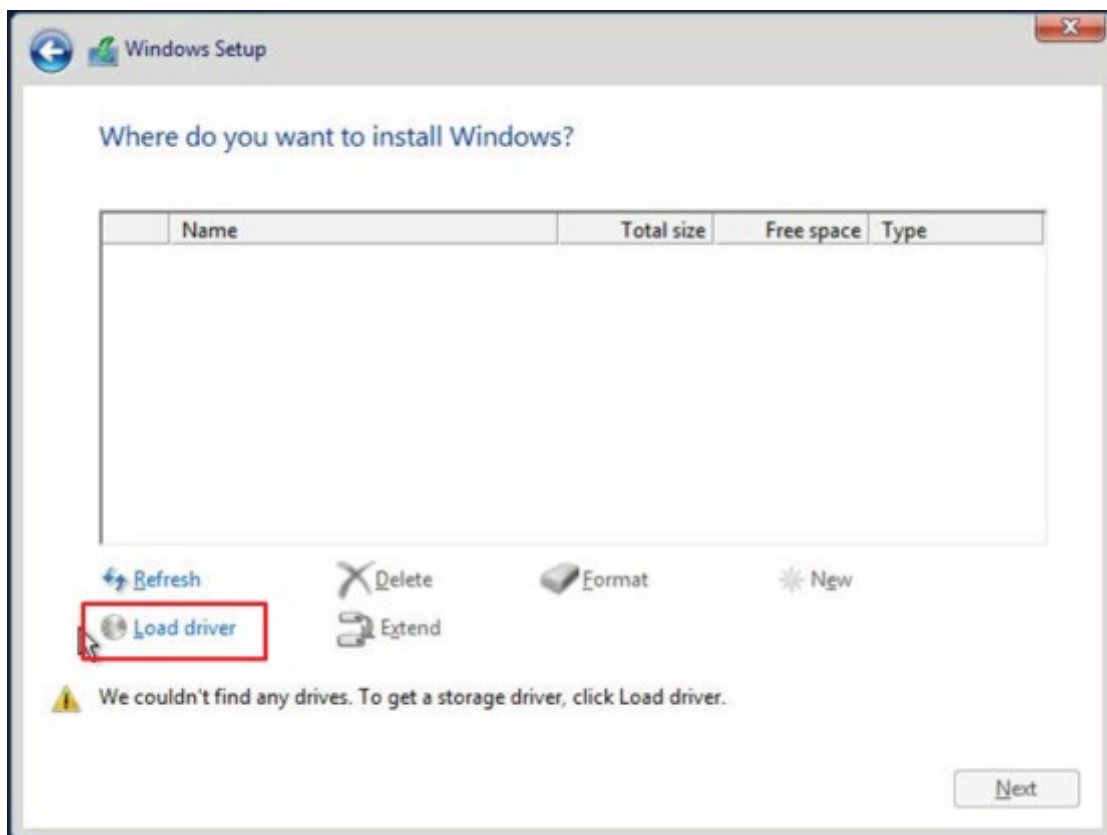
Figure B-2. Load Driver Link

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.

B.2 Driver Installation

The Supermicro website that contains drivers and utilities for your system is at https://www.supermicro.com/wdl/driver/. Some of these must be installed, such as the chipset driver. After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash drive or a USB flash or media drive. (You may also use a utility to extract the ISO file if preferred.) Another option is to go to the Supermicro website at http://www.supermicro.com/products/. Find the product page for your motherboard and download the latest drivers and utilities. Insert the flash drive or disk and the screenshot shown below should appear.
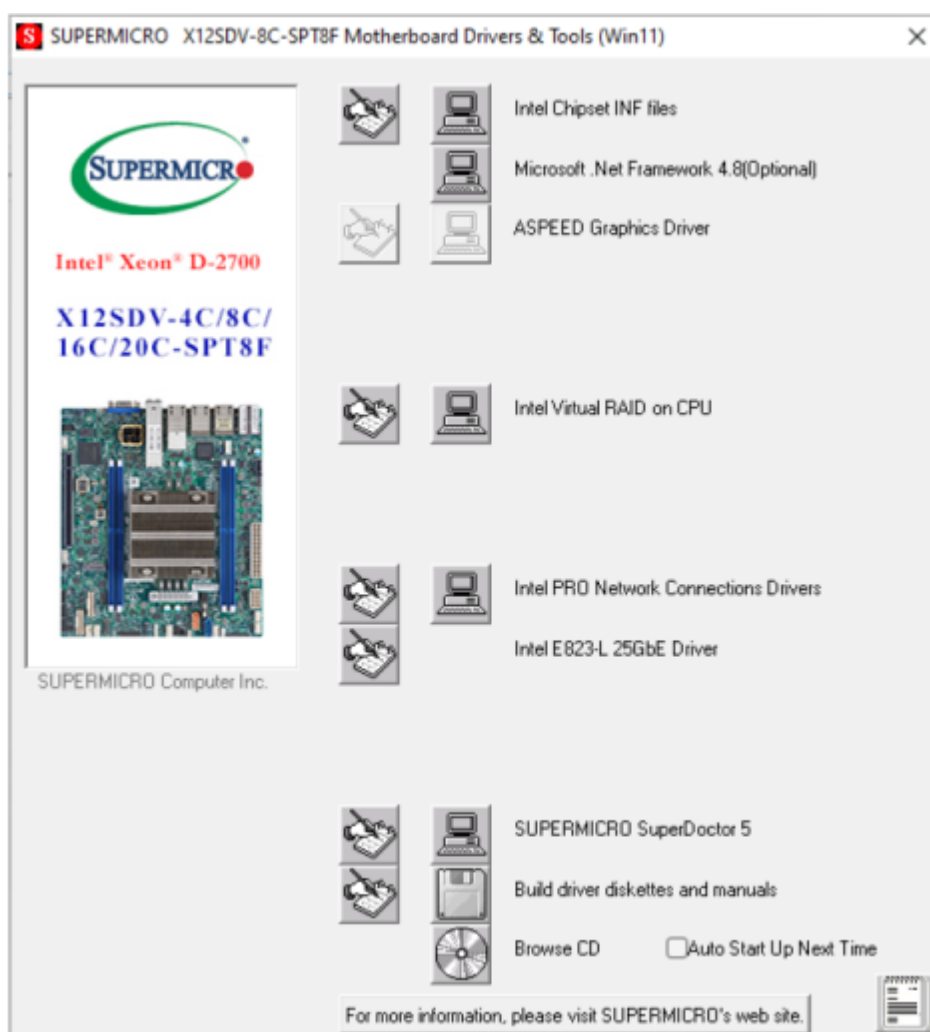
Figure B-3. Driver & Tool Installation Screen

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 bottom) one at a time. After installing each item, you must reboot 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.

B.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.
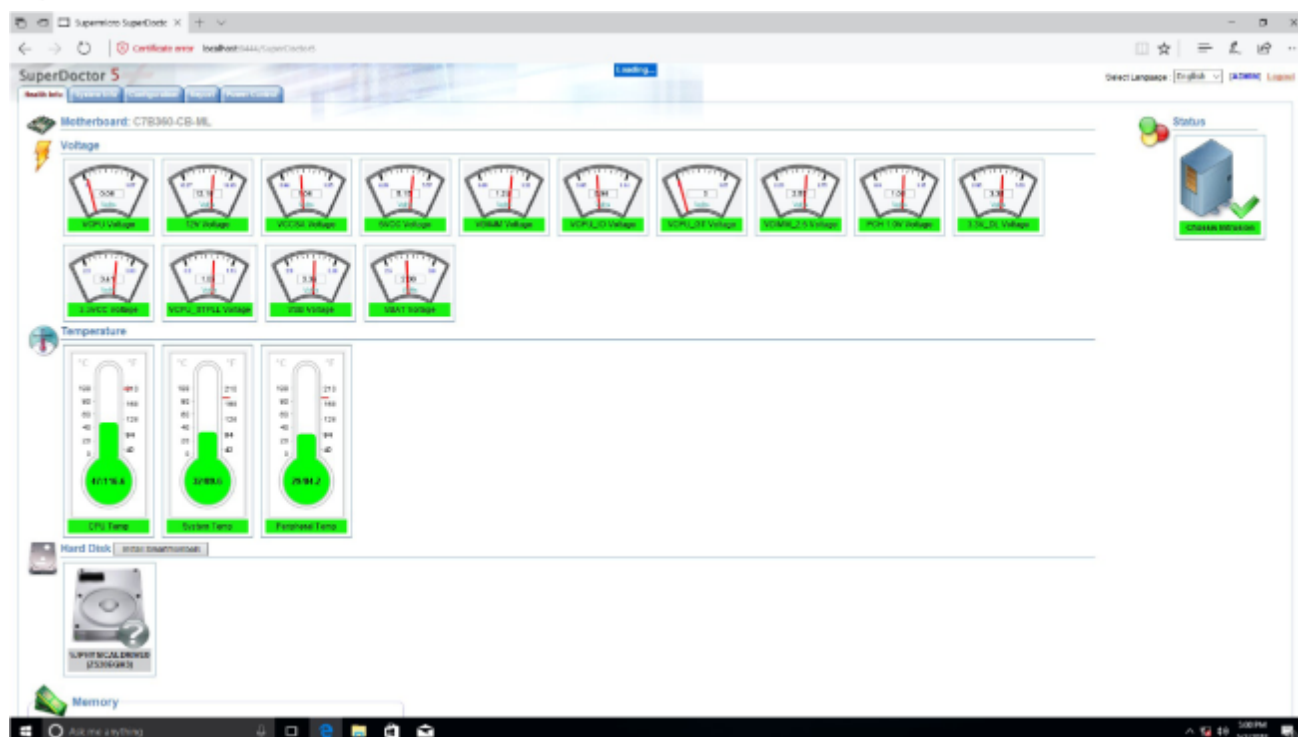
Figure B-4. SuperDoctor 5 Interface Display Screen (Health Information)

B.4 IPMI

The 10th Generation Intel Xeon, Core™ i3, Pentium, Celeron 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. For general documentation and information on IPMI, visit our website at https://www.supermicro.com/en/support/BMC_ Unique_Password.

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.

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

电池更换不当会有爆炸危险。请只使用同类电池或制造商推荐的功能相当的电池更换原有电池。请按制造商的说明处理废旧电池。

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。

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.

D.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.

D.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, 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) to reflash the BIOS.

D.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 or media drive 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 flash or media drive.

Note 1: If you cannot locate the "Super.ROM" file in your driver disk, visit our website at 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.
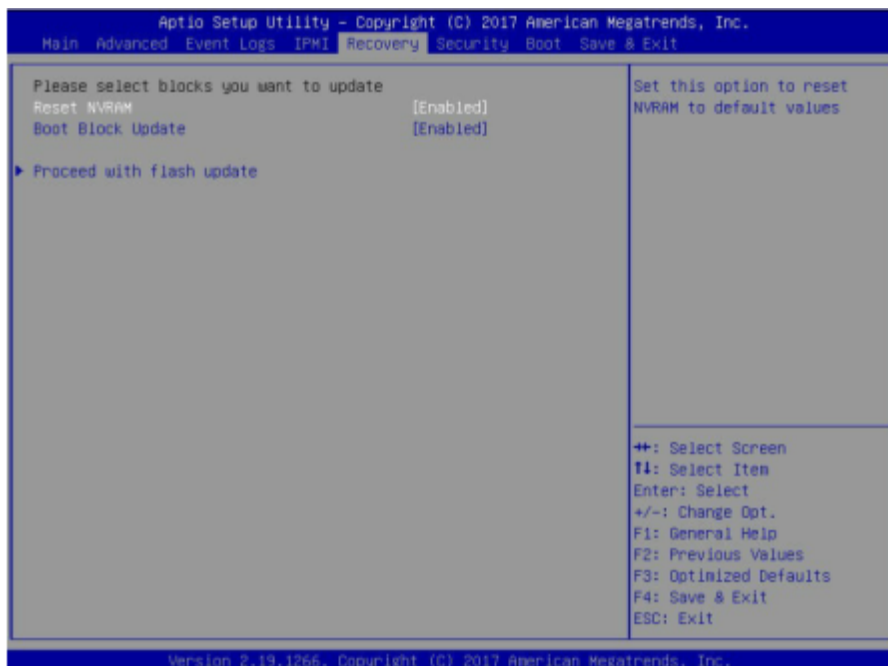
2. Insert the USB device that contains the new BIOS image ("Super.ROM") into your USB port and reset the system until the following screen appears:

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.
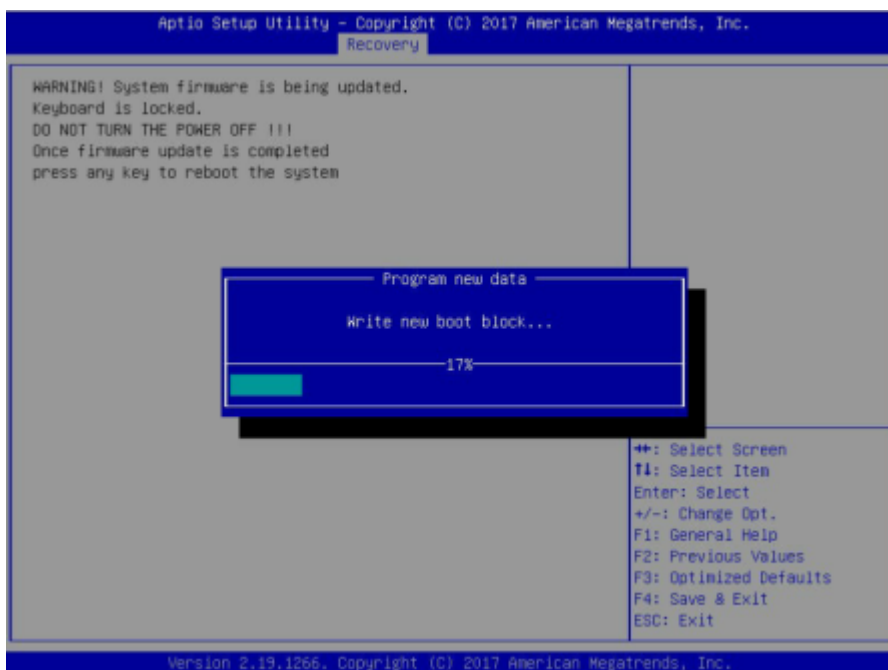
4.When the screen as shown above displays, use the arrow keys to select the item "Proceed with flash update" and press the <Enter> key. You will see the BIOS recovery progress as shown in the screen below:
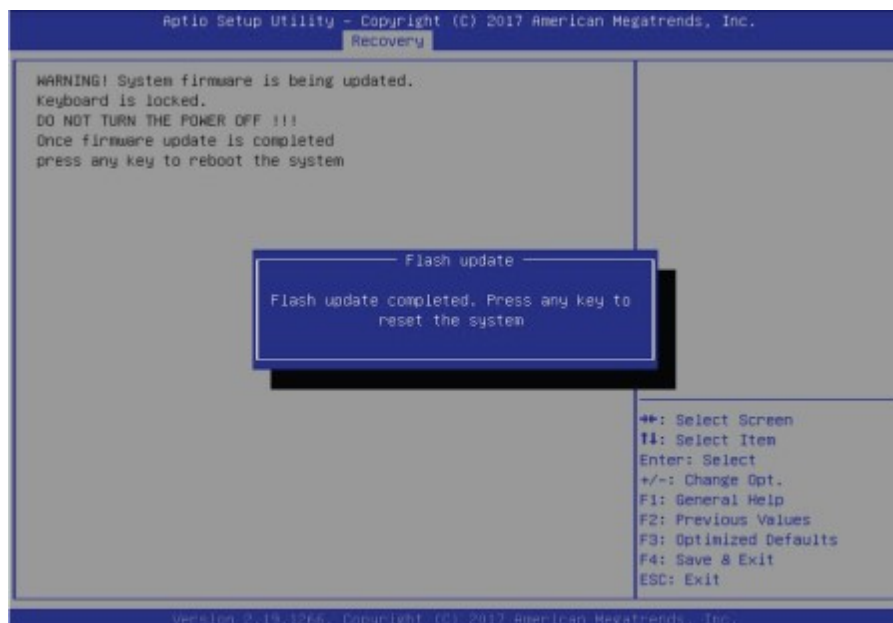
Note: Do not interrupt the BIOS flashing process until it has completed.

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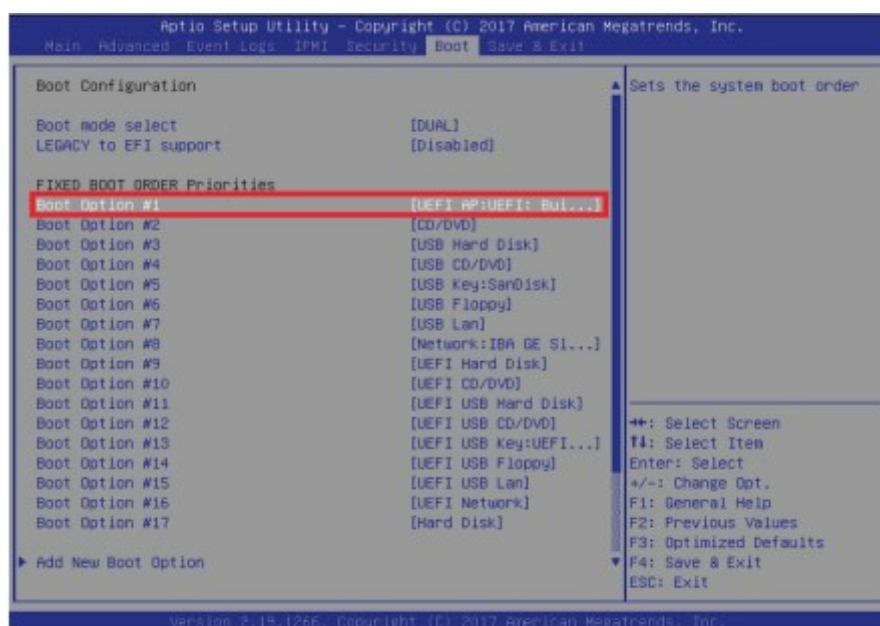
8. When the UEFI Shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 6. Enter flash.nsh BIOSname.### at the prompt to start the BIOS update process.

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

9. 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.

10. Press <Del> to enter the BIOS Setup utility.

11. Press <F3> to load the default settings.

12. After loading the default settings, press <F4> to save the settings and exit the BIOS Setup utility.