B13SEE-CPU-25G

USER'S MANUAL

Revision 1.0b

The information in this user's manual has been carefully reviewed and is believed to be accurate. The manufacturer assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our website at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL Super Micro Computer, Inc. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a consumer environment or residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate".

⚠ WARNING: This product can expose you to chemicals including lead, known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to www.P65Warnings.ca.gov.

The products sold by Supermicro are not intended for and will not be used in life support systems, medical equipment, nuclear facilities or systems, aircraft, aircraft devices, aircraft/emergency communication devices or other critical systems whose failure to perform be reasonably expected to result in significant injury or loss of life or catastrophic property damage. Accordingly, Supermicro disclaims any and all liability, and should buyer use or sell such products for use in such ultra-hazardous applications, it does so entirely at its own risk. Furthermore, buyer agrees to fully indemnify, defend and hold Supermicro harmless for and against any and all claims, demands, actions, litigation, and proceedings of any kind arising out of or related to such ultra-hazardous use or sale.

Manual Revision 1.0b

Release Date: December 15, 2023

Preface

About This Manual

This manual is written for system integrators, IT technicians and knowledgeable end users. It provides information for the installation and use of the B13SEE-CPU-25G motherboard.

About This Motherboard

The Supermicro B13SEE-CPU-25G motherboard supports a 4th and 5th Generation Intel® Xeon® Scalable Processor in an LGA4677 socket with a thermal design power (TDP) of up to 350 W. Built with the Intel C741 chipset, this motherboard features up to 4 TB of DDR5 ECC RDIMM/3DSRDIMM memory with speeds of up to 5600 MT/s in eight DIMM slots or 4400 MT/s in 16 DIMM slots, one M.2 M-Key PCIe 3.0 or SATA 3.0 connector (2280/22110), one PCIe 4.0 x16 mezzanine card connector, four PCIe 5.0 x8 MCIO connectors for GPU/E1.S/AIOM riser cards, and one PCIe 4.0 x16 SIOM connector for one SAS Card/two M.2 x4/two PCIe 4.0 NVMe. The B13SEE-CPU-25G is optimized for data centers and cloud computing. Note that this motherboard is intended to be installed and serviced by professional technicians only. For processor and memory updates, refer to our website at http://www.supermicro.com/products/.

Conventions Used in the Manual

Special attention should be given to the following symbols for proper installation and to prevent damage done to the components or injury to yourself:

⚠ **Warning!** Indicates important information given to prevent equipment/property damage or personal injury.

⚡ **Warning!** Indicates high voltage may be encountered while performing a procedure.

☝ **Important:** Important information given to ensure proper system installation or to relay safety precautions.

✎ **Note:** Additional Information given to differentiate various models or to provide information for proper system setup.

Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: Marketing@supermicro.com (General Information)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
Support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)

Website: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: Sales_Europe@supermicro.com (General Information)
Support_Europe@supermicro.com (Technical Support)
RMA_Europe@supermicro.com (RMA Support)

Website: www.supermicro.nl

Asia-Pacific

Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 235
Taiwan (R.O.C)

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

Email: Sales-Asia@supermicro.com.tw (Sales Inquiry)
Support@supermicro.com.tw (Technical Support)
RMA@supermicro.com.tw (RMA Support)

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

Chapter 2 Installation

Chapter 3 Troubleshooting

Chapter 4 UEFI BIOS

Appendix A BIOS Codes

Appendix B Software

Appendix C Standardized Warning Statements

Appendix D UEFI BIOS Recovery

Chapter 1

Introduction

Congratulations on purchasing your computer motherboard from an industry leader. Supermicro motherboards are designed to provide you with the highest standards in quality and performance.

1.1 Checklist

Main Parts List		
Description	**Part Number**	**Quantity**
Supermicro Motherboard	B13SEE-CPU-25G	1
Quick Reference Guide	MNL-2505-QRG	1

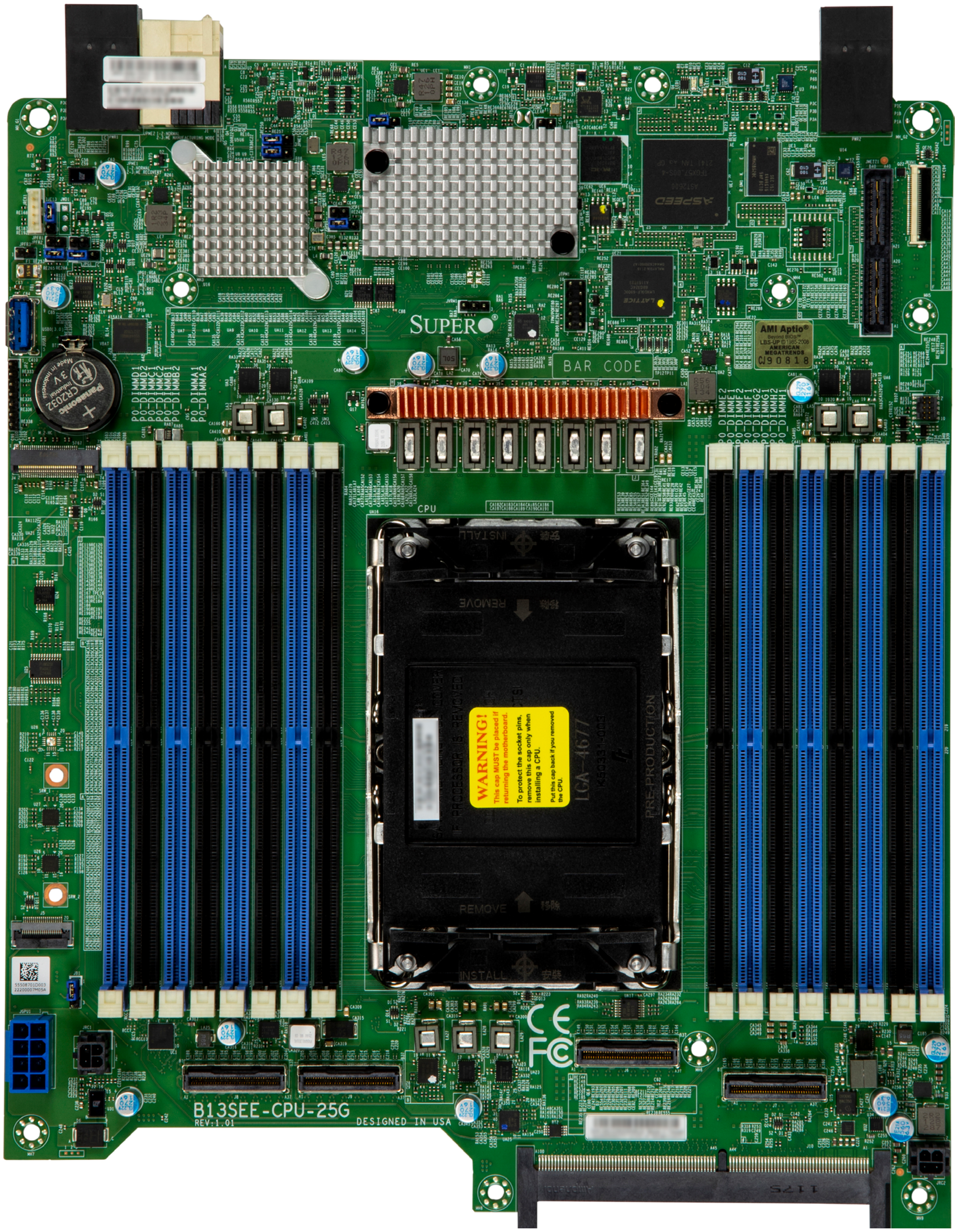
Important Links

For your system to work properly, follow the links below to download all necessary drivers/ utilities and the user's manual for your server.

- Frequently Asked Questions: https://www.supermicro.com/FAQ/index.php
- Supermicro product manuals: http://www.supermicro.com/support/manuals/
- Product drivers and utilities: https://www.supermicro.com/wdl/driver/
- Product safety info: http://www.supermicro.com/about/policies/safety_information.cfm
- A secure data deletion tool designed to fully erase all data from storage devices can be found at our website: https://www.supermicro.com/about/policies/disclaimer.cfm?url=/wftp/utility/Lot9_Secure_Data_Deletion_Utility/
- If you have any questions, contact our support team at: support@supermicro.com

This manual may be periodically updated without notice. Check the Supermicro website for possible updates to the manual revision level.

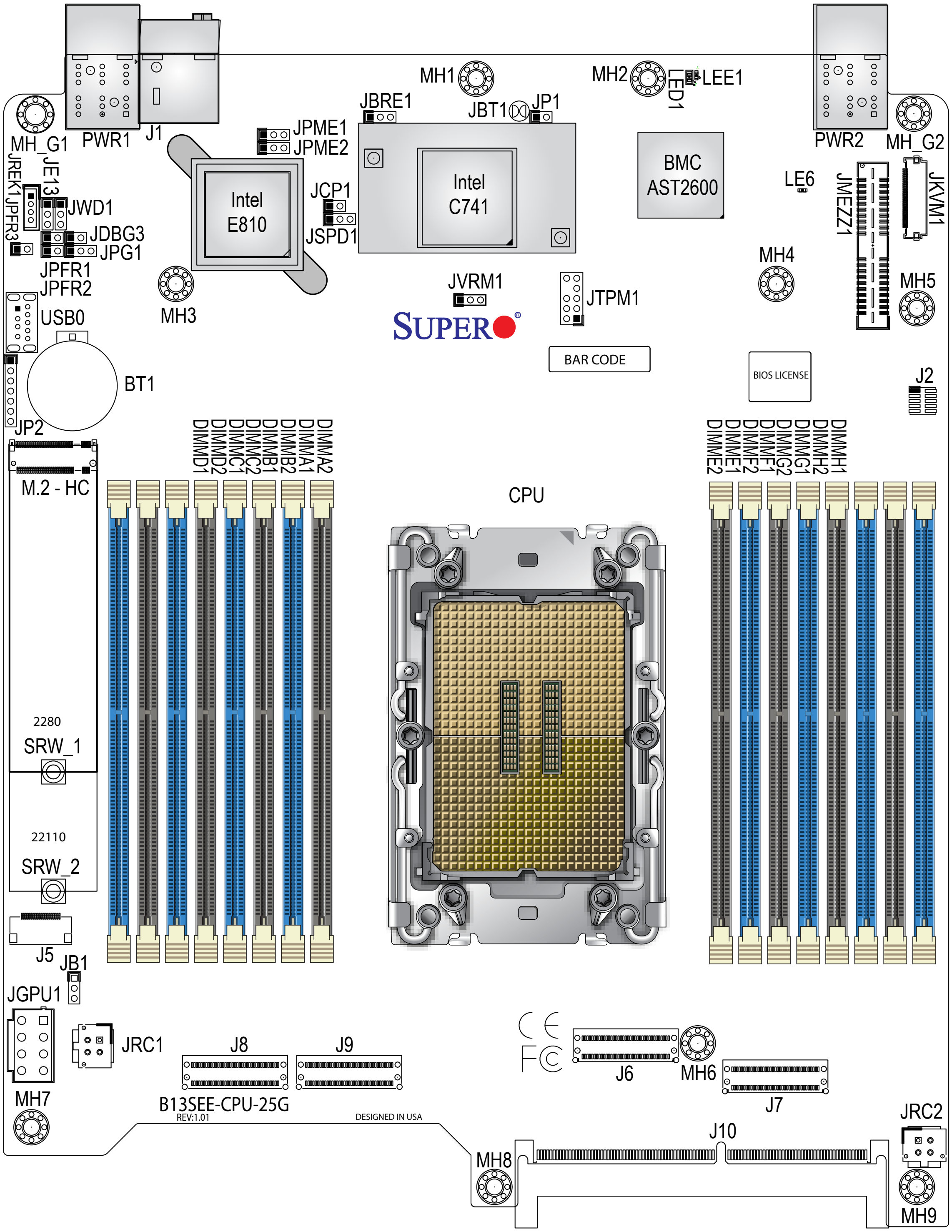
Figure 1-1. B13SEE-CPU-25G Motherboard Image



Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publication of the manual. The motherboard you received may or may not look exactly the same as the graphics shown in this manual.

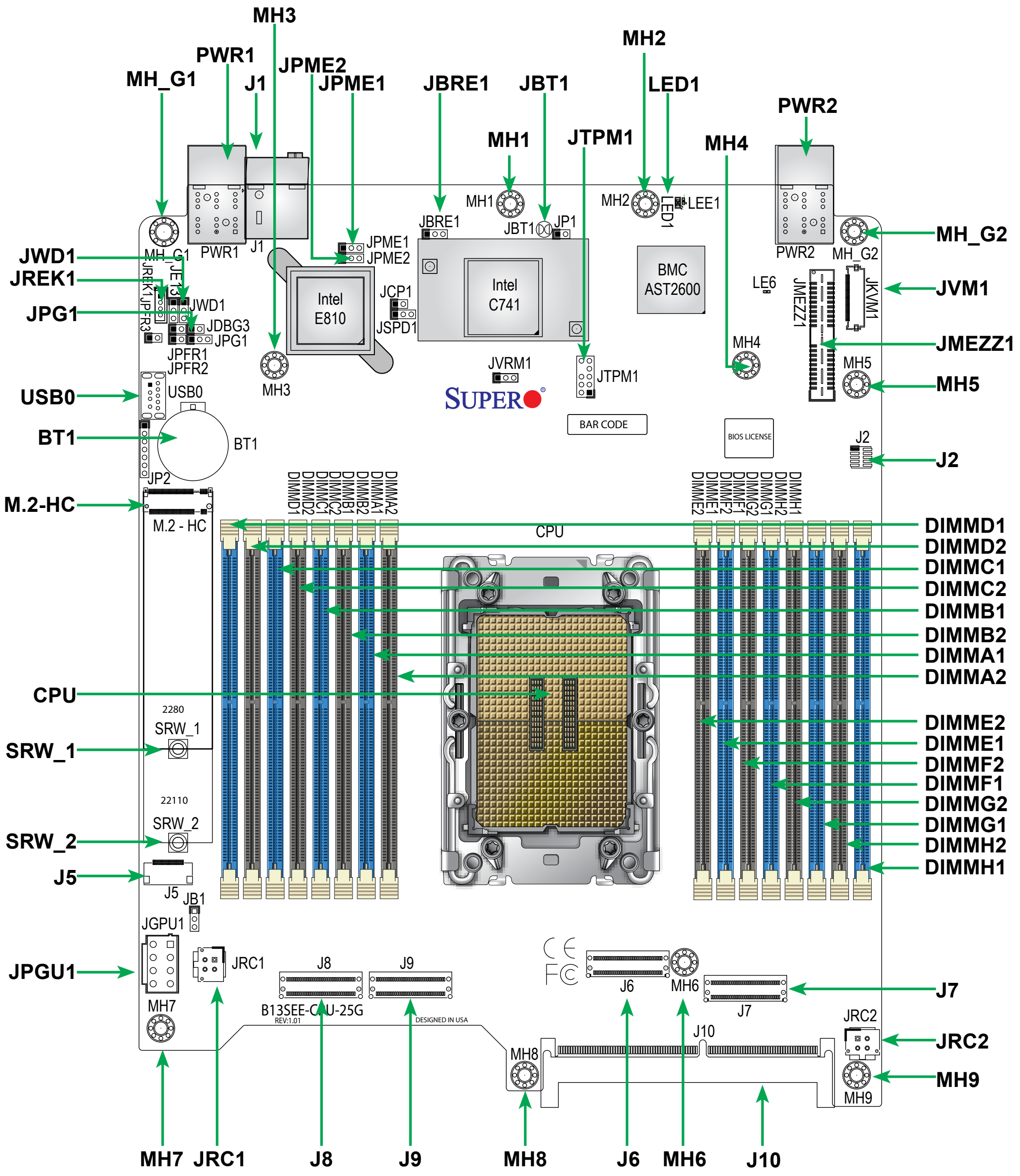
Figure 1-2. B13SEE-CPU-25G Motherboard Layout

(not drawn to scale)



Note: Components not documented are for internal testing only.

Quick Reference



Notes:

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

Quick Reference Table

Jumper	Description	Default Setting
JBRE1	BIOS Recovery	Pins 1-2 (Normal)
JPG1	VGA Enable/Disable	Pins 1-2 (Enable)
JPME1	ME Recovery Mode	Pins 1-2 (Normal)
JPME2	Manufacturing Mode	Pins 1-2 (Normal)
JWD1	Watchdog Timer	Pins 1-2 (Reset)

Connector	Description
BT1	Onboard CMOS Battery
J1	Chassis Backplane Connector
J5	Front Panel Connector
J6, J7, J8, J9	PCIe 5.0 x8 MCIO Connector
J10	PCIe 4.0 x16 SIOM Connector for one SAS card or two M.2 x4 or two PCIe 4.0 NVMe
JKVM1	VGA/USB Module Connector
JGPU1	12 V GPU Power Connector (ATX 8-pin)
JRC1	Proprietary Riser Power Connector
JRC2	Proprietary Riser Power Connector
JREK1	Intel RAID Key Header
JMEZZ1	PCIe 4.0 x16 Mezzanine Card Connector for AOM
JTPM1	Trusted Platform Module (TPM)/Port 80 Connector
M.2-HC	M.2 M-Key PCIe 3.0 or SATA 3.0 Connector (2280/22110)
PWR1	Power Receptacle to Chassis Backplane
PWR2	Power Receptacle to Chassis Backplane
USB0	Internal USB 2.0/3.0 Type-A Connector
MH_G1, MH_G2	Mounting Holes
MH1–MH9	Mounting Holes

LED	Description	Status
LED1	BMC Heartbeat LED	Blinking Green: BMC Normal

Motherboard Features

Motherboard Features
CPU
• Supports a 4th and 5th Generation Intel Xeon Scalable Processor in an LGA4677 socket with up to 64 cores and 350 W TDP
Memory
• Supports up to 4 TB of DDR5 ECC RDIMM/3DSRDIMM memory with speeds of up to 5600 MT/s in eight DIMM slots or 4400 MT/s in 16 DIMM slots
DIMM Size
• Up to 256 GB
Chipset
• Intel PCH C741
Expansion Slots
• One PCIe 4.0 x16 Mezzanine card connector • One PCIe 4.0 x16 SIOM connector for one SAS card or two M.2 x4 or two PCIe 4.0 NVMe • Four PCIe 5.0 x8 MCIO connectors for GPU/E1.S/AIOM riser cards • One M.2 M-Key PCIe 3.0 or SATA 3.0 connector (2280/22110)
Baseboard Management Controller (BMC)
• Aspeed AST2600
Network
• Intel E810 for dual 25G LAN ports
Super I/O
• Aspeed AST2600
Graphics
• Aspeed AST2600
I/O Devices
• Two internal SATA 3.0 ports
Peripheral Devices
• One internal USB 2.0/3.0 Type-A port

Note: The table above is continued on the next page.

Motherboard Features

BIOS

- 256 Mb AMI BIOS® SPI Flash BIOS
- APCI, Plug and Play (PnP), Real Time Clock (RTC) Wakeup

Power Management

- ACPI power management (supports S5)
- Power-on mode for AC power recovery

System Health Monitoring

- Onboard voltage monitoring for +3.3 V, +5 V, +12 V, +3.3 VStb, +5 VStb, Vcore, and Vmem
- Temperature of CPU, PCH, System, DIMM, and peripheral
- Temperature of GPU, NVMe, and SAS
- CPU thermal trip support
- Platform Environment Control Interface (PECI)/TSI

System Management

- Trusted Platform Module (TPM) 2.0 header onboard
- SuperDoctor® 5
- IPMIView, SMCIPMITOOL, IPMICFG, SDO, SSM, Supermicro Update Manager (SUM) InBand, SUM-OOB
- Redundant power supply unit detection sensor

LED Indicators

- BMC Heartbeat LED

Dimensions

- 11.605" (L) x 9.358" (W)

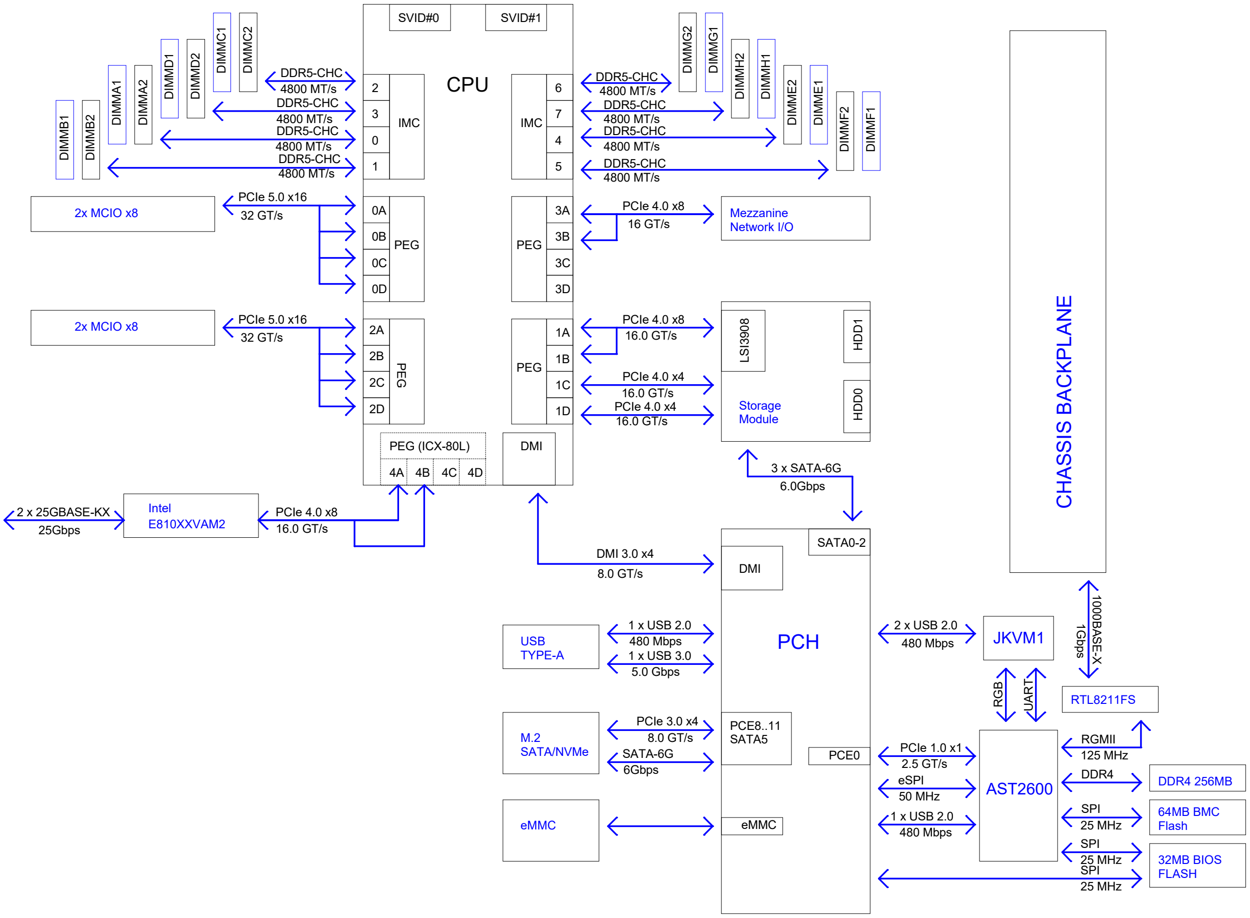
Note 1: The CPU maximum thermal design power (TDP) is subject to chassis and heatsink cooling restrictions. For proper thermal management, check the chassis and heatsink specifications for proper CPU TDP sizing.

Note 2: For IPMI configuration instructions, refer to the Embedded IPMI Configuration User's Guide available at http://www.supermicro.com/support/manuals/.

Note 3: If you purchase a Supermicro Out of Band (OOB) software license key (Supermicro P/N: SFT-OOB-LIC), DO NOT change the IPMI MAC address. Once the Mac address has been changed, the OOB license key will be invalid.

Note 4: Supermicro ships standard products with a unique password for the BMC ADMIN user. This password can be found on a label on the motherboard.

Figure 1-3. System Block Diagram



Note: This is a general block diagram and may not exactly represent the features on your motherboard. See the previous pages for the actual specifications of your motherboard.

1.2 Processor and Chipset Overview

The Supermicro B13SEE-CPU-25G motherboard, with the C741 chipset, supports a 4th and 5th Generation Intel Xeon Scalable Processor and provides superb performance, efficient power management while providing a rich feature set based on cutting edge technology to address today's needs in advanced computing, engineering simulation, and automation.

The processor and the chipset support the following features:

- Intel Hyper-Threading, Intel VT-D, VT-x, TDX
- Intel Turbo Boost Technology
- Intel Rapid Storage Technology
- 4 TB of DDR5 ECC RDIMM/3DSRDIMM memory with speeds of up to 5600 MT/s in eight DIMM slots or 4400 MT/s in 16 DIMM slots
- ACPI Power Management

1.3 System Health Monitoring

Onboard Voltage Monitors

An onboard voltage monitor will scan the voltages of the onboard chipset, memory, CPU, and battery continuously. Once a voltage becomes unstable, a warning is given, or an error message is sent to the screen. You can adjust the voltage thresholds to define the sensitivity of the voltage monitor.

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the IPMI interface. Whenever the temperature of the CPU or the system exceeds a user-defined threshold, system/CPU cooling fans will be turned on to prevent the CPU or the system from overheating.

Note: To avoid possible system overheating, be sure to provide adequate airflow to your system.

System Resource Alert

This feature is available when used with SuperDoctor 5® in the Windows OS or in the Linux environment. SuperDoctor is used to notify you of certain system events. For example, you can configure SuperDoctor to provide you with warnings when the system temperature, CPU temperatures, voltages and fan speeds go beyond a predefined range.

1.4 ACPI Features

The Advanced Configuration and Power Interface (ACPI) specification defines a flexible and abstract hardware interface that provides a standard way to integrate power management features throughout a computer system, including its hardware, operating system and application software. This enables the system to automatically turn on and off peripherals such as CD-ROMs, network cards, solid state drives, and printers.

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play, and an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures, while providing a processor architecture-independent implementation that is compatible with appropriate Windows operating systems. For detailed information regarding OS support, refer to the Supermicro website.

1.5 Power Supply

As with all computer products, a stable power source is necessary for proper and reliable operation. This is even more important for processors that have high CPU clock rates. In areas where noisy power transmission is present, you may choose to install a line filter to shield the computer from noise. It is recommended that you also install a power surge protector to help avoid problems caused by power surges.

Chapter 2

Installation

2.1 Static-Sensitive Devices

Electrostatic Discharge (ESD) can damage electronic components. To avoid damaging your system board, it is important to handle it very carefully. The following measures are generally sufficient to protect your equipment from ESD.

Precautions

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the motherboard by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules, avoid touching their pins.
- Put the motherboard and peripherals back into their antistatic bags when not in use.
- For grounding purposes, make sure that your computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the motherboard.
- Use only the correct type of onboard CMOS battery. Do not install the onboard battery upside down to avoid possible explosion.

Unpacking

The motherboard is shipped in antistatic packaging to avoid static damage. When unpacking the motherboard, make sure that the person handling it is static protected.

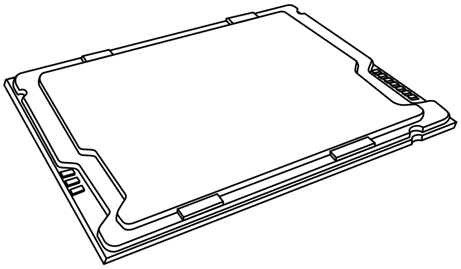
2.2 Processor and Heatsink Installation

The processor (CPU) and processor carrier should be assembled together first to form the processor carrier assembly. This will be attached to the heatsink to form the processor heatsink module (PHM) before being installed onto the CPU socket.

Notes:

- Use ESD protection.
- Shut down the system and then unplug the AC power cord from all power supplies.
- Check that the plastic protective cover is on the CPU socket and none of the socket pins are bent. If they are, contact your retailer.
- When handling the processor, avoid touching or placing direct pressure on the LGA lands (gold contacts). Improper installation or socket misalignment can cause serious damage to the processor or socket, which may require manufacturer repairs.
- When installing the processor and heatsink, ensure a torque driver set to the correct force is used for each screw.
- Thermal grease is pre-applied on a new heatsink. No additional thermal grease is needed.
- Refer to the Supermicro website for updates on processor support.
- All graphics in this manual are for illustrations only. Your components may look different.
- The following CPU carrier has been successfully tested in our labs and is available from Supermicro. Order the CPU carrier with the CPU heatsink.

The 4th and 5th Generation Intel Xeon Scalable Processor

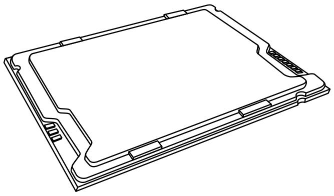


Intel Xeon Processor

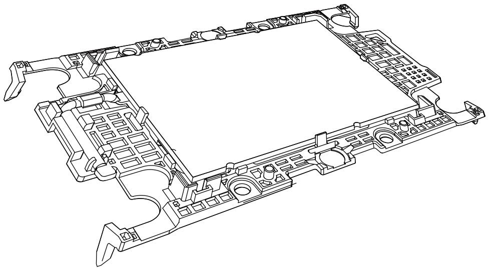
Overview of the Processor Carrier Assembly

The processor carrier assembly contains the Intel Xeon processor and a processor carrier.

1. Intel Xeon Scalable Processor



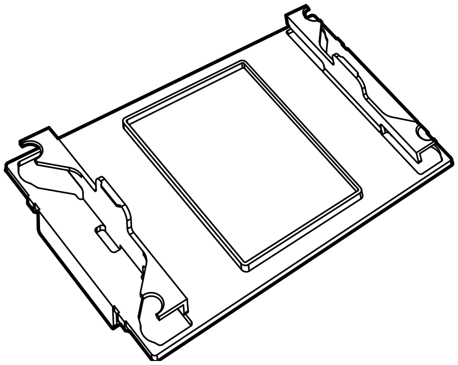
2. Processor Carrier



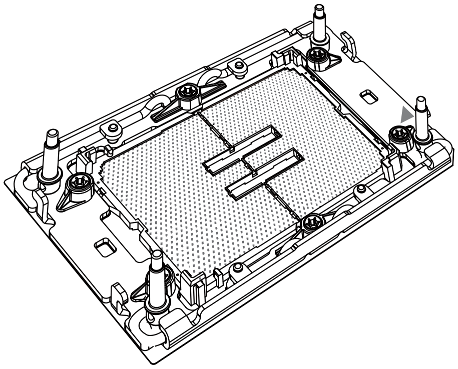
Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

1. Plastic Protective Cover



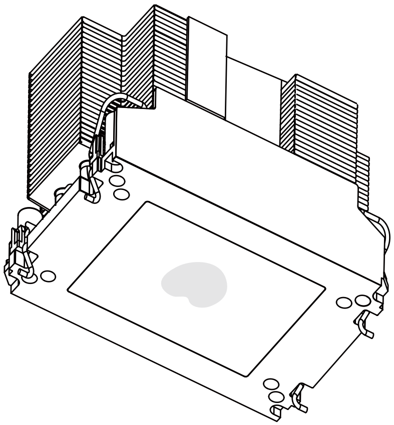
2. CPU Socket



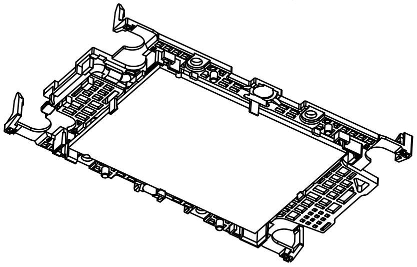
Overview of the Processor Heatsink Module

The Processor Heatsink Module (PHM) contains a heatsink, a processor carrier, and the Intel Xeon processor.

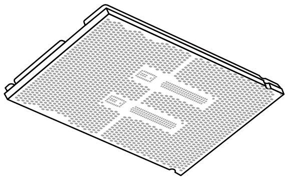
1. Heatsink with Thermal Grease



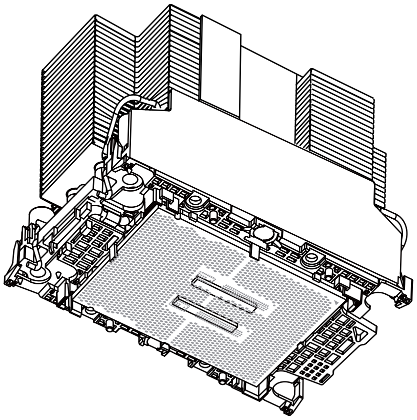
2. Processor Carrier



3. Intel Xeon Scalable Processor



Processor Heatsink Module (PHM)



Bottom View

Creating the Processor Carrier Assembly

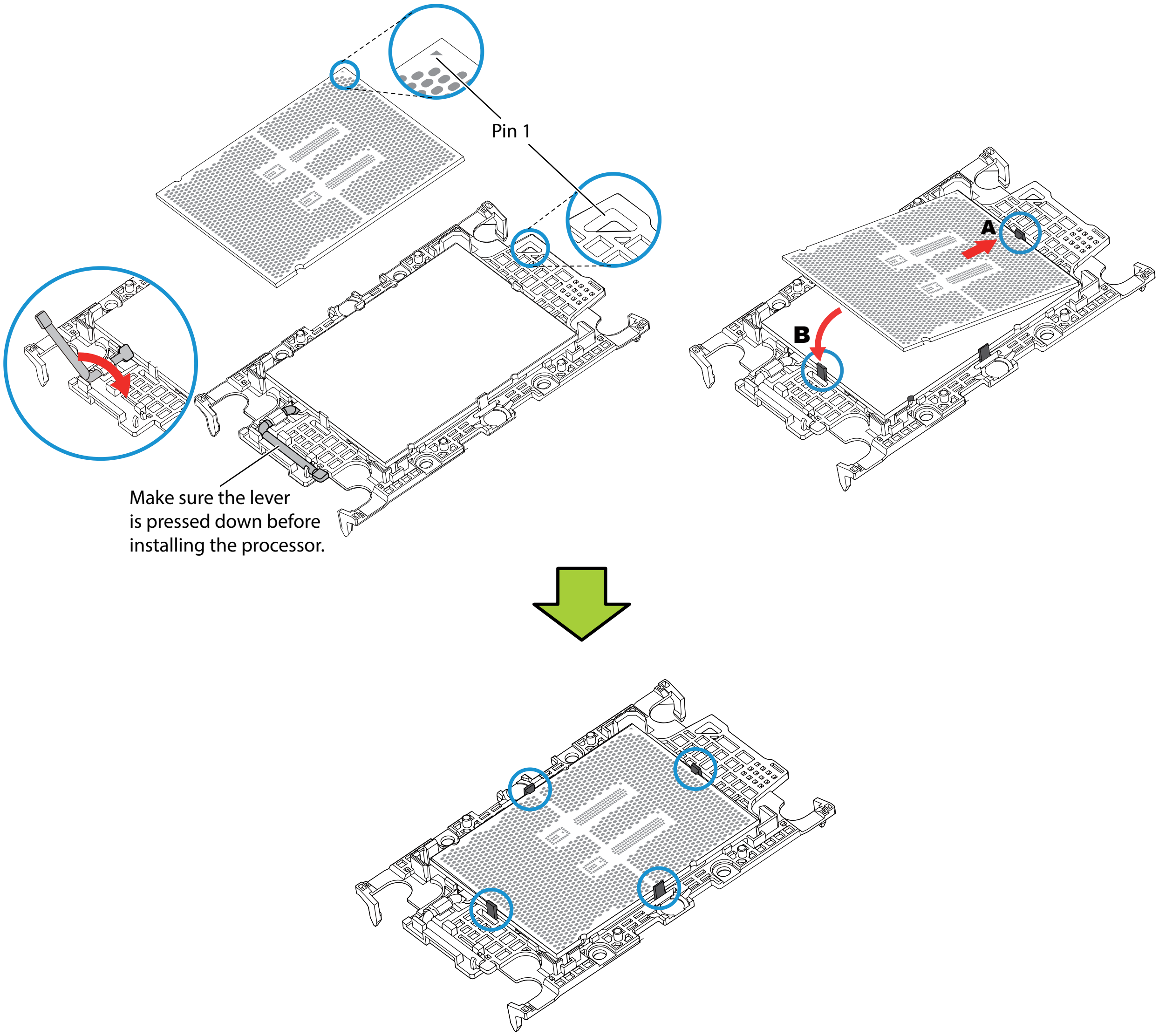
To install a processor into the processor carrier, follow the steps below:

1. Before installation, make sure the lever on the processor carrier is pressed down as shown below.

2. Hold the processor with the LGA lands (gold contacts) facing up. Locate the small, gold triangle in the corner of the processor and the corresponding hollowed triangle on the processor carrier. These triangles indicate pin 1. See the images below.

3. Use the triangles as a guide to carefully align and place one end of the processor into the latch marked A, and place the other end of processor into the latch marked B as shown below.

4. Examine all corners to ensure that the processor is firmly attached to the carrier.


Pin 1
A
B
Make sure the lever is pressed down before installing the processor.

Processor Carrier Assembly

Assembling the Processor Heatsink Module

After creating the processor carrier assembly for the processor, mount it onto the heatsink to create the processor heatsink module (PHM):

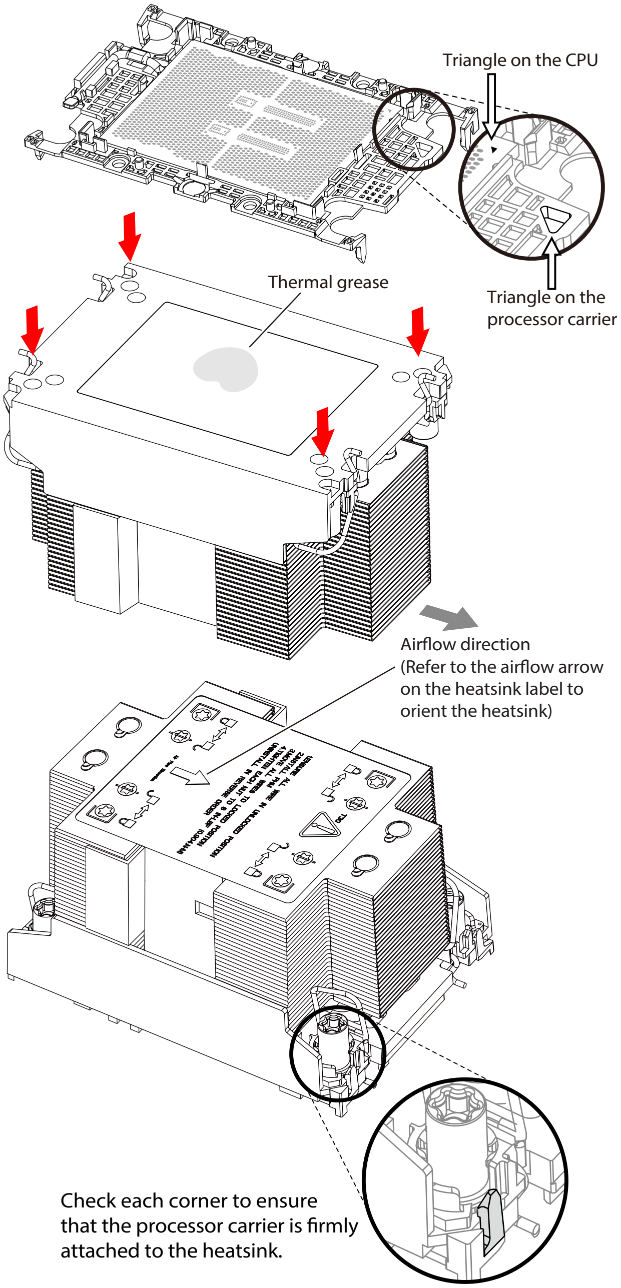
1. Note the label on top of the heatsink, which marks the airflow direction. Turn the heatsink over and orient the heatsink so the airflow arrow points towards the triangle on the processor.

2. If this is a new heatsink, the thermal grease has been pre-applied. Otherwise, apply the proper amount of thermal grease.

3. Hold the processor carrier assembly so the processor's gold contacts are facing up, then align the holes of the processor carrier assembly with the holes on the heatsink. Press the processor carrier assembly down until it snaps into place. The plastic clips of the processor carrier assembly will lock at the four corners.

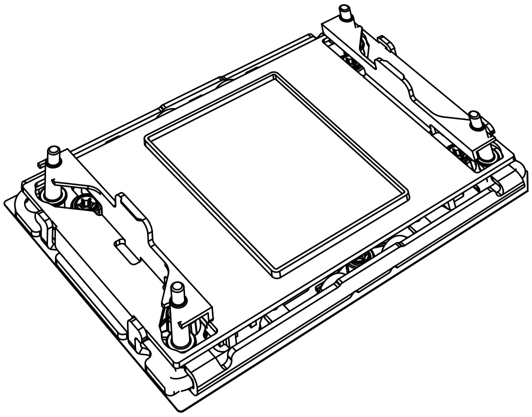
4. Examine all corners to ensure that the plastic clips on the processor carrier assembly are firmly attached to the heatsink.

Processor Carrier Assembly (Upside Down)

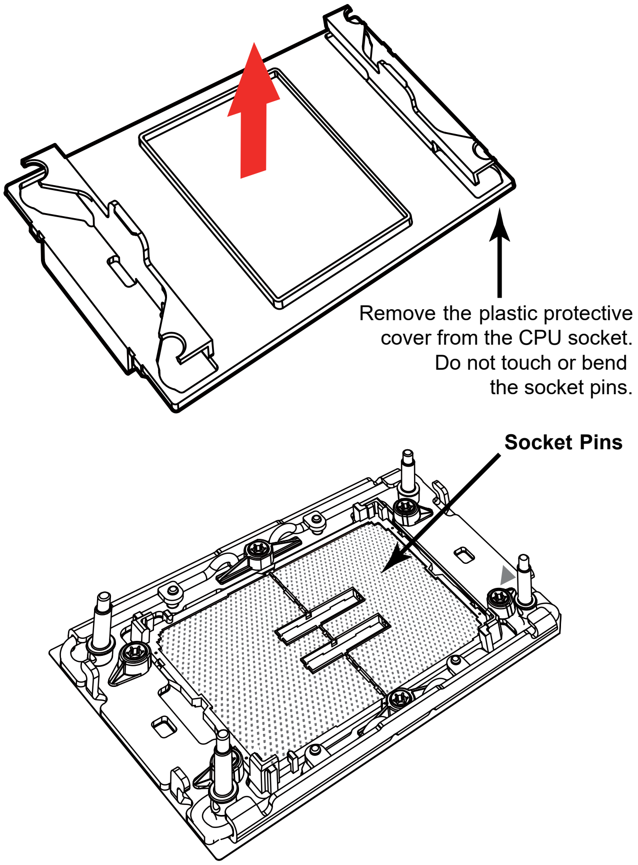

Triangle on the CPU
Triangle on the processor carrier
Thermal grease
Airflow direction (Refer to the airflow arrow on the heatsink label to orient the heatsink)
Check each corner to ensure that the processor carrier is firmly attached to the heatsink.

Preparing the CPU Socket for Installation

This motherboard comes with a plastic protective cover installed on the CPU socket. Remove it from the socket to install the Processor Heatsink Module (PHM). Gently pull up one corner of the plastic protective cover to remove it.



CPU Socket with Plastic Protective Cover



Remove the plastic protective cover from the CPU socket. Do not touch or bend the socket pins.

Installing the Processor Heatsink Module

After assembling the Processor Heatsink Module (PHM), install it onto the CPU socket:

1. Align pin 1 of the PHM with the printed triangle on the CPU socket. See the left image below.

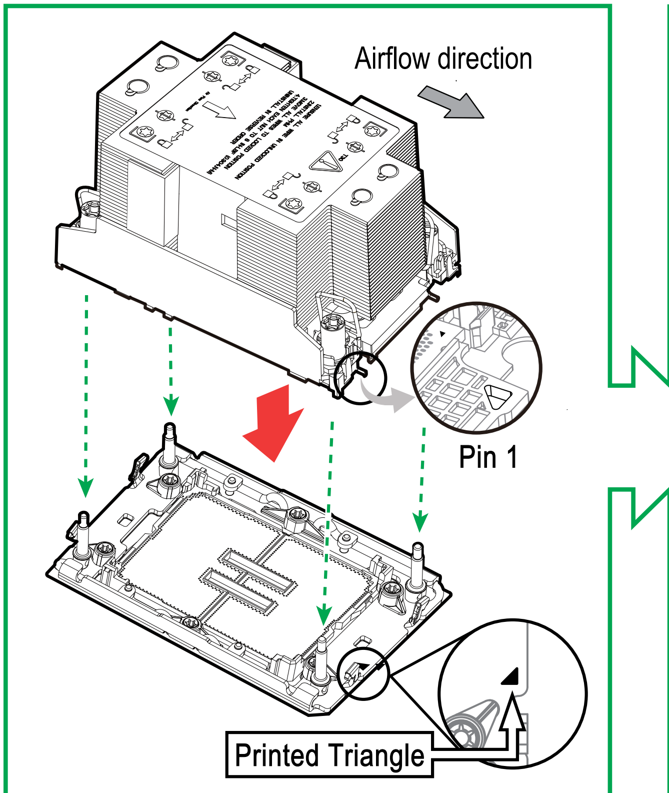
2. Make sure all four holes of the heatsink are aligned with the socket, then gently place the heatsink on top of the CPU socket.

3. Press all four rotating wires outwards and make sure that the heatsink is securely latched into the CPU socket.

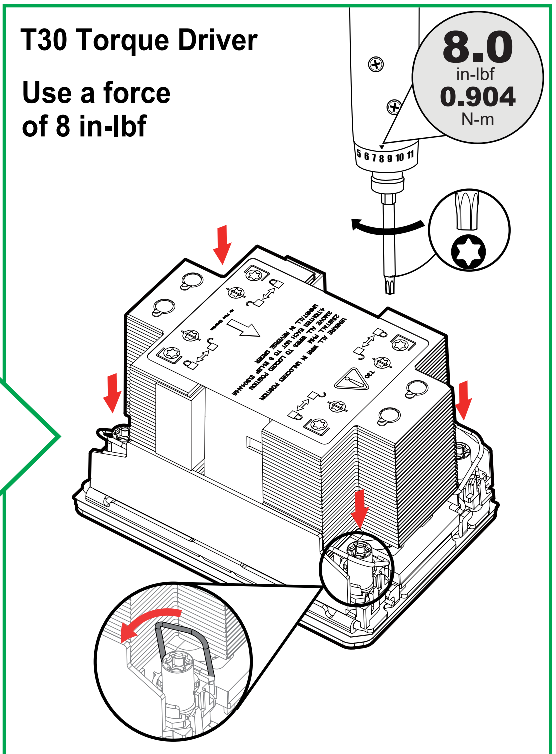
4. With a T30 bit torque driver set to a force of 8.0 in-lbf (0.904 N-m), gradually tighten the four screws to ensure even pressure. You can start with any screw, but make sure to tighten the screws in a diagonal pattern.

Important: Do not use a force greater than 8.0 in-lbf (0.904 N-m). Exceeding this force may over-torque the screw, causing damage to the processor, heatsink, and screw.

5. Examine all corners to ensure that the PHM is firmly attached to the socket.



Mount the Processor Heatsink Module onto the CPU socket (on the motherboard).



Press the rotating wires outwards to latch the PHM and then tighten the four screws.

Removing the Processor Heatsink Module

Before removing the processor heatsink module (PHM) from the motherboard, shut down the system and then unplug the AC power cord from all power supplies.

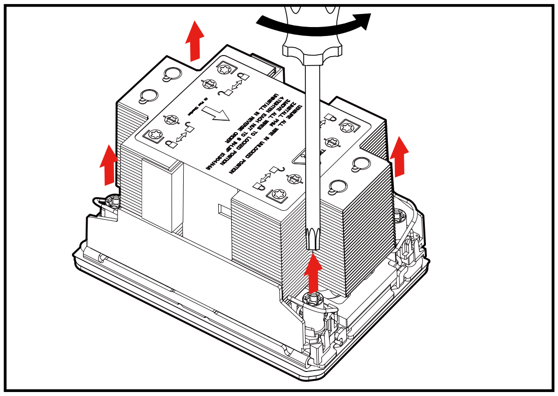
Then follow the steps below:

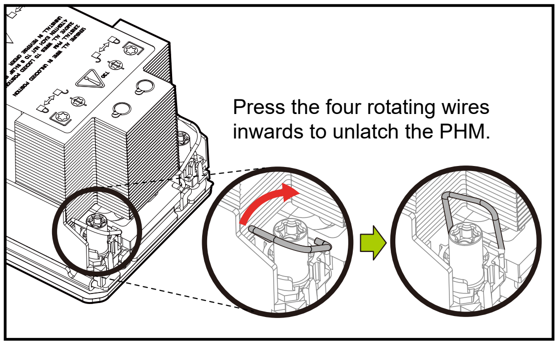
1. Use a T30 bit driver to loosen the four screws. You can start with any screw, but make sure to tighten the screws in a diagonal pattern.

2. Press the four rotating wires inwards to unlatch the PHM from the socket.

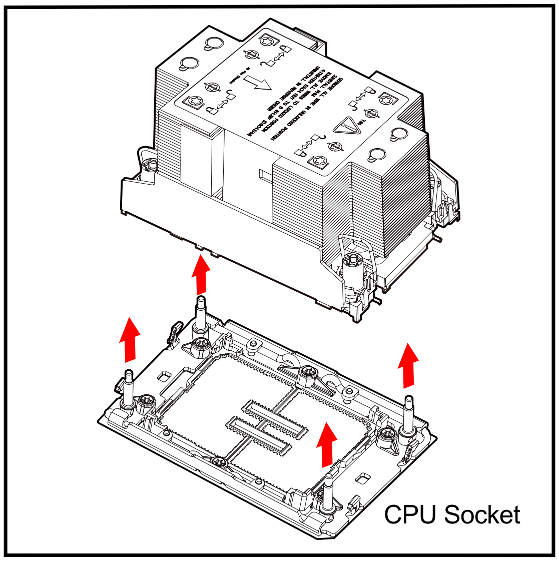
3. Gently lift the PHM upwards to remove it from the socket.

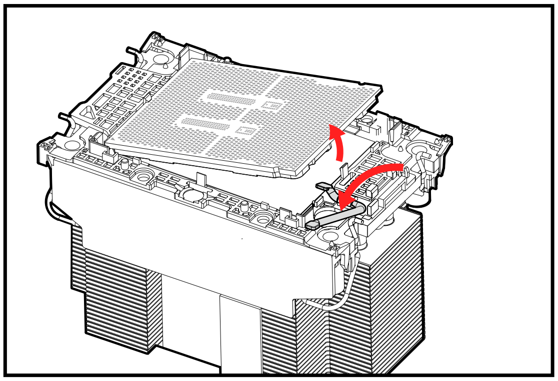
4. To remove the CPU, move the lever to its unlocked position and gently remove the CPU.





Press the four rotating wires inwards to unlatch the PHM.

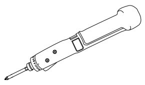




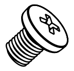
2.3 Motherboard Installation

All motherboards have standard mounting holes to fit different types of chassis. Make sure that the locations of all the mounting holes for both the motherboard and the chassis match. Although a chassis may have both plastic and metal mounting fasteners, metal ones are highly recommended because they ground the motherboard to the chassis. Make sure that the metal standoffs click in or are screwed in tightly.

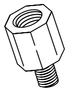
Tools Needed



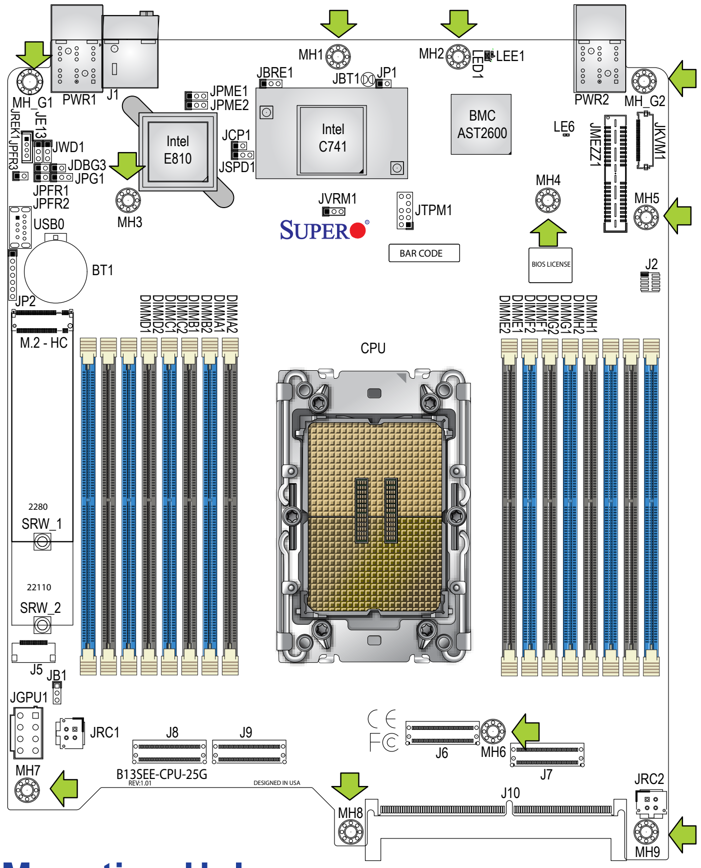
Torque Driver (1)



Phillips Screws (11)



Standoffs (11) Only if Needed



Location of Mounting Holes

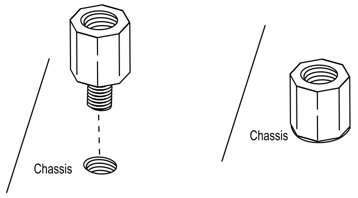
Note 1: Do not use a force greater than 8 in-lbf (0.904 N-m) on each mounting screw during motherboard installation. Exceeding this force may over-torque the screw, causing damage to the motherboard and screw.

Note 2: Some components are very close to the mounting holes. Take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

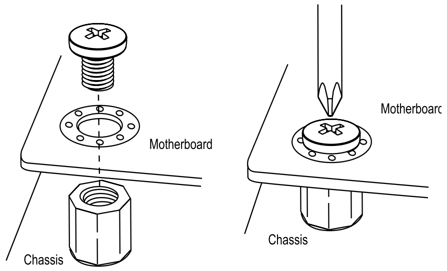
Installing the Motherboard

1. Locate the mounting holes on the motherboard and the mounting tray. See the previous page for the location.

2. Install the standoffs on the mounting tray. Align the mounting holes on the motherboard against the mounting holes on the tray.



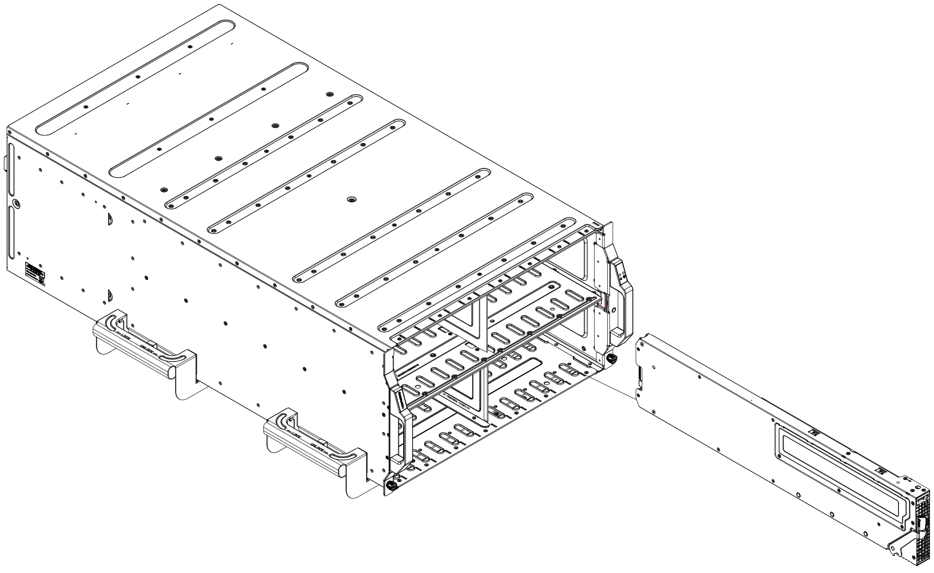
3. Using the torque driver, insert a pan head #6 screw into the mounting hole on the motherboard and its matching hole on the tray.



4. Repeat step 3 to insert #6 screws to all mounting holes located on the motherboard and the tray and securely install the motherboard onto the tray.

Installing the Motherboard into the Superblade Chassis

1. When the motherboard is securely installed on the mounting tray, push the tray into the Superblade chassis shown below.



2. Once the mounting tray is pushed into the chassis, the connectors on the motherboard's edge will make contact with the chassis' backplane, which provides the connections to the chassis power, network, and other I/O devices.

Note: Images displayed are for illustration only. Your chassis or components may look different from those shown in this manual.

2.4 Memory Support and Installation

Note: Check the Supermicro website for recommended memory modules.

Important: Exercise extreme care when installing or removing DIMM modules to prevent any possible damage.

Memory Support

The B13SEE-CPU-25G supports up to 4 TB of DDR5 ECC RDIMM/3DSRDIMM memory with speeds of up to 5600 MT/s in eight DIMM slots or 4400 MT/s in 16 DIMM slots.

1 CPU, 16 DIMM Slots

Number of DIMMs	Memory Population Sequence
1	DIMMA1 DIMME1 DIMMB1 DIMMF1
2	DIMMA1 / DIMMG1 DIMMC1 / DIMME1
4	DIMMA1 / DIMMG1 / DIMMC1 / DIMME1
6	DIMMA1 / DIMMG1 / DIMMC1 / DIMME1 / DIMMD1 / DIMMF1 DIMMA1 / DIMMG1 / DIMMC1 / DIMME1 / DIMMB1 / DIMMH1 DIMMC1 / DIMME1 / DIMMB1 / DIMMH1 / DIMMD1 / DIMMF1 DIMMA1 / DIMMG1 / DIMMB1 / DIMMH1 / DIMMD1 / DIMMF1
8	DIMMA1 / DIMMG1 / DIMMB1 / DIMMH1 / DIMMD1 / DIMMF1 / DIMMC1 / DIMME1
12	DIMMA1 / DIMMA2 / DIMMB1 / DIMMC1 / DIMMC2 / DIMMD1 / DIMME1 / DIMME2 / DIMMF1 / DIMMG1 / DIMMG2 / DIMMH1 DIMMA1 / DIMMB1 / DIMMB2 / DIMMC1 / DIMMD1 / DIMMD2 / DIMME1 / DIMMF1 / DIMMF2 / DIMMG1 / DIMMH1 / DIMMH2
16	DIMMA1 / DIMMA2 / DIMMB1 / DIMMB2 / DIMMC1 / DIMMC2 / DIMMD1 / DIMMD2 / DIMME1 / DIMME2 / DIMMF1 / DIMMF2 / DIMMH1 / DIMMH2 / DIMMG1 / DIMMG2

1 HBM CPU, 16 DIMM Slots

Number of DIMMs	Memory Population Sequence
1	DIMMA1 DIMME1
2	DIMMA1 / DIMMG1 DIMMC1 / DIMME1
4	DIMMA1 / DIMMG1 / DIMMC1 / DIMME1
8	DIMMA1 / DIMMG1 / DIMMC1 / DIMME1 / DIMMD1 / DIMMF1 / DIMMB1 / DIMMH1
16	DIMMA1 / DIMMA2 / DIMMB1 / DIMMB2 / DIMMC1 / DIMMC2 / DIMMD1 / DIMMD2 / DIMME1 / DIMME2 / DIMMF1 / DIMMF2 / DIMMH1 / DIMMH2 / DIMMG1 / DIMMG2

1 CPU, 16 DIMM Slots and Intel® Optane™ Persistent Memory 300 Series DIMM Slots
Supported only with a 4th Generation Intel Xeon Scalable Processor

DDR5 + PMem	Mode	DIMMH1	DIMMH2	DIMMG1	DIMMG2	DIMMF1	DIMMF2	DIMME1	DIMME2	CPU	DIMMA2	DIMMA1	DIMMB2	DIMMB1	DIMMC2	DIMMC1	DIMMD2	DIMMD1
4+4	1LM+AD, MM, MM+AD	DDR5		PMem		DDR5		PMem				PMem		DDR5		PMem		DDR5
6+1	1LM+AD			DDR5		DDR5		DDR5				DDR5		PMem		DDR5		DDR5
8+1	1LM+AD	DDR5		DDR5		DDR5		DDR5				DDR5		DDR5		DDR5	PMem	DDR5
8+4	1LM+AD, MM, MM+AD	DDR5		DDR5	PMem	DDR5		DDR5	PMem		PMem	DDR5		DDR5	PMem	DDR5		DDR5
	1LM+AD, MM, MM+AD	DDR5	PMem	DDR5		DDR5	PMem	DDR5				DDR5	PMem	DDR5		DDR5	PMem	DDR5
8+8	1LM+AD, MM, MM+AD	DDR5	PMem	DDR5	PMem	DDR5	PMem	DDR5	PMem		PMem	DDR5	PMem	DDR5	PMem	DDR5	PMem	DDR5

Compatible and Incompatible DIMM Types in a Channel and a System

DIMM Type	RDIMM	RDIMM 3DS	9x4 RDIMM	Intel PMem 300 Series DIMM (Supported only with an Intel 4th Generation Intel Xeon Scalable Processor)
RDIMM	Compatible	Incompatible	Incompatible	Compatible
RDIMM 3DS	Incompatible	Compatible	Incompatible	Compatible
9x4 RDIMM	Incompatible	Incompatible	Compatible	Incompatible
Intel PMem 300 Series DIMM	Compatible	Compatible	Incompatible	Incompatible

DDR5 Memory Support for the 4th Generation Intel Xeon Scalable Processor Processors-SP

Type	Ranks Per DIMM and Data Width (Stack)	DIMM Capacity (GB)		Speed (MT/s)	
				One DIMM per Channel [1]	Two DIMMs per Channel
		Memory Density 16 Gb	Memory Density 24 Gb[2]	1.1 Volts	
RDIMM	SRx8 (RC D)	16 GB	24 GB	4800*	4400*
	SRx4 (RC C)	32 GB	48 GB		
	SRx4 (RC F) 9x4	32 GB	NA		
	DRx8 (RC E)	32 GB	48 GB		
	DRx4 (RC A)	64 GB	96 GB		
	DRx4 (RC B) 9x4	64 GB	NA		
RDIMM 3DS	(4R/8R) x4 (RC A)	2H-128 GB 4H-256 GB	NA		

*Memory speed and capacity support depends on the processors used in the system.

Note 1: 1 DPC applies to 1 SPC or 2 SPC implementations (SPC – sockets per channel).

Note 2: 24 Gb XCC only with limited configs: 1 DPC all DIMM types, 2 DPC 96 GB only. Only eight and sixteen DIMM configs, no failbacks. 25 at PLR1 4S/8S later in 2023.

DDR5 Memory Support for the 5th Generation Intel Xeon Scalable Processor Processors-SP

Type	Ranks Per DIMM and Data Width	DIMM Capacity (GB)		Speed (MT/s)	
				One DIMM per Channel (DPC)[1]	Two DIMMs per Channel (DPC)
		Memory Density 16 Gb	Memory Density 24 Gb	1.1 Volts	
RDIMM	SRx8 (RC D)	16 GB	24 GB[2]	5600[3]	4400[3]
	SRx4 (RC C)	32 GB	48 GB[2]		
	SRx4 (RC F) 9x4	NA	NA		
	DRx8 (RC E)	32 GB	48 GB[2]		
	DRx4 (RC A)	64 GB	96 GB		
	DRx4 (RC B) 9x4	NA	NA		
RDIMM 3DS	(4R/8R) x4 (RC A)	2H-128 GB 4H-256 GB	NA		

*Memory speed and capacity support depends on the processors used in the system.

Note 1: 1 DPC applies to 1 SPC or 2 SPC implementations (SPC – sockets per channel).

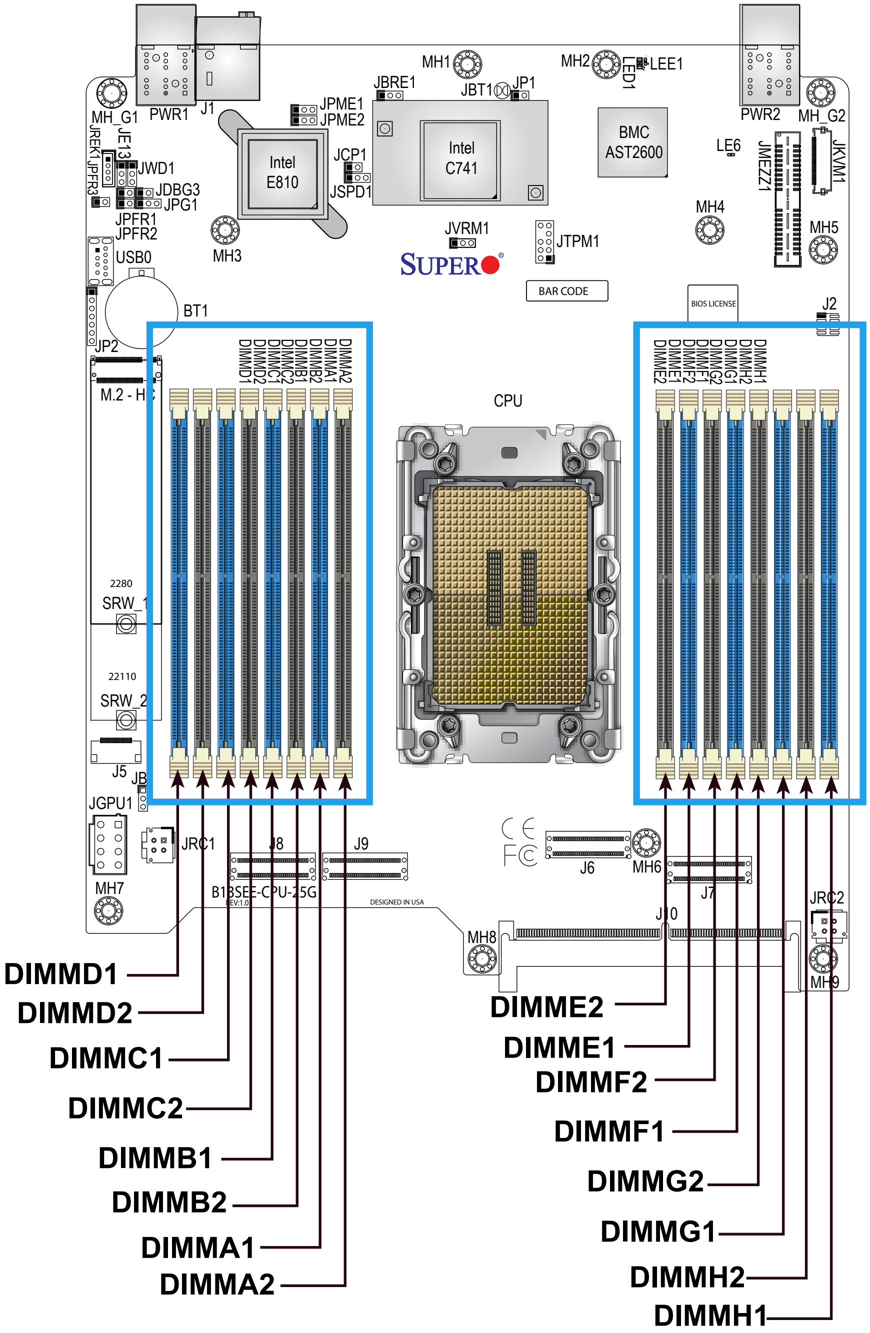
Note 2: 24 Gb 2 DPC is not POR with 24 GB and 48 GB DIMMs.

Note 3: DDR5-5600 DIMMs will be limited to 5600 MT/s 1 DPC and 4400 MT/s 2 DPC. DDR5-4800 DIMMs will be limited to 4800 MT/s 1 DPC and 4400 MT/s 2 DPC.

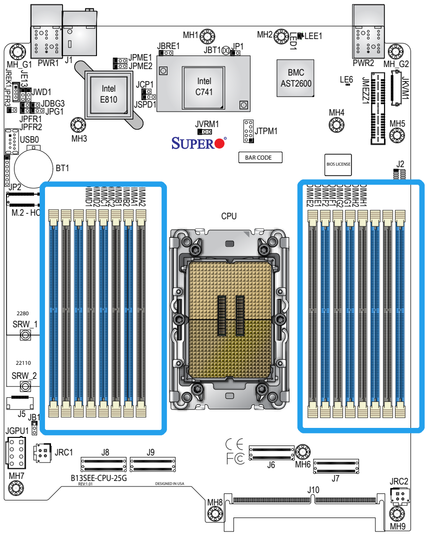
Note 4: DDR5-5600 DIMMs are requires for 5600 MT/s and 5200 MT/s 1 DPC speeds.

General Guidelines for Optimizing Memory Performance

- It is recommended to use DDR5 ECC memory of the same type, size and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- The motherboard will not support an odd-numbered amount of DIMM modules except for a single DIMM module necessary for board operation.



DIMM Installation



1. For the system to work properly, use memory modules of the same type and speed. Refer to the table in Chapter 2.4 for the memory population sequence.

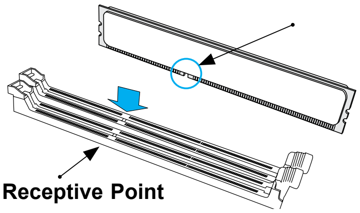
2. Align the DIMM module key with the receptive point on the single-latch DIMM slot.

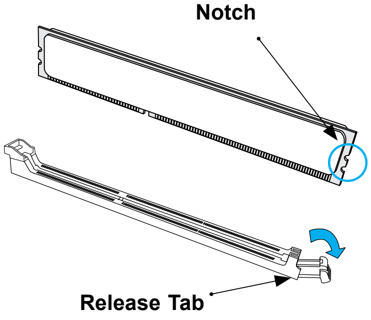
3. Push the release tab outwards to unlock the slot.

4. Align the notch on the end of the module against the receptive point on the end of the slot.

5. Press both ends of the module straight down into the slot until the module snaps into place.

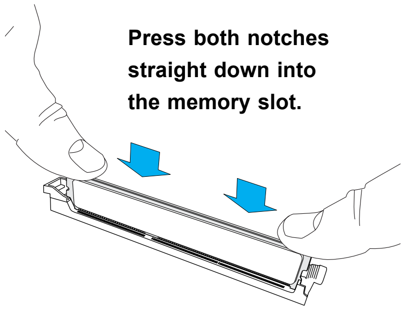
6. Push the release tab to the lock position to secure the module into the slot.

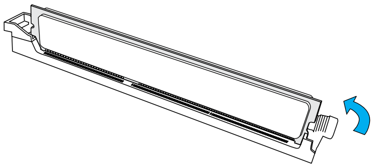




DIMM Removal

Press the release tab on one end of the DIMM module to unlock it. Once the DIMM module is loosened, remove it from the memory slot.





2.5 Connectors & Headers

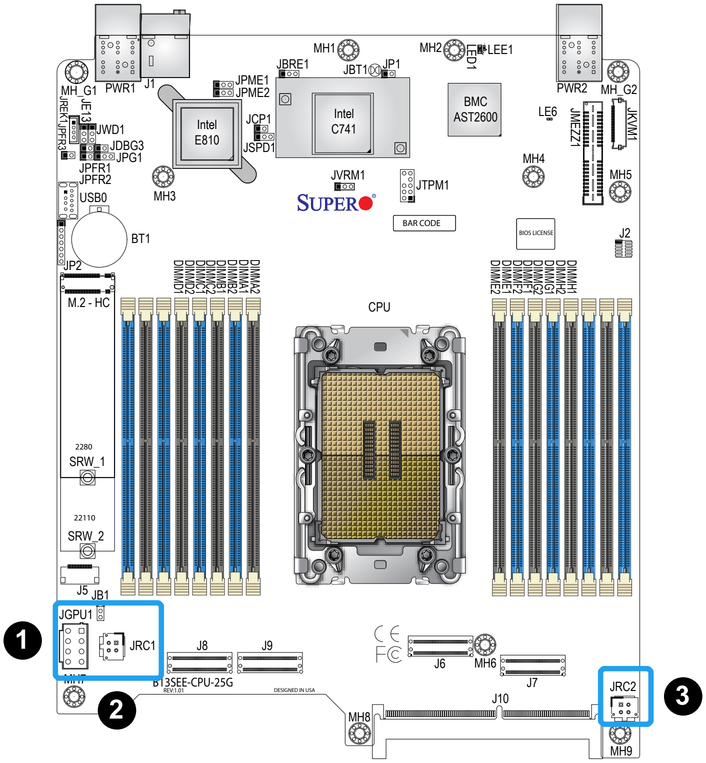
Power Connections

12 V GPU Power Connector

JGPU1 is the EATX 12 V 8-pin power connector.

Proprietary Riser Power Connector

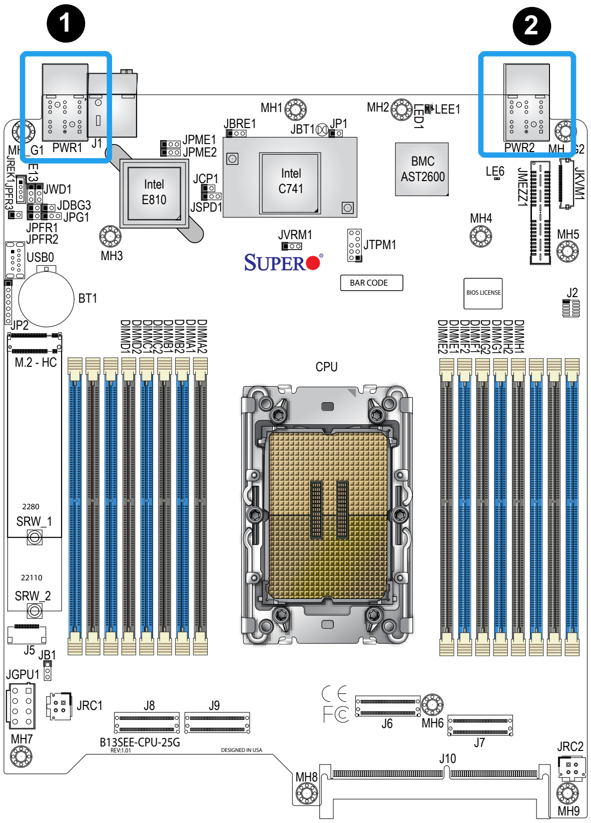
JRC1 and JRC2 are proprietary riser power connectors with a rated 150 W, two 75 W CEM specification.



1. 12 V GPU Power Connector
2. Riser Power Connector
3. Riser Power Connector

Power Receptables to Chassis Backplane

PWR1 and PWR2 are primary power supply connectors that provide power to the motherboard via the chassis backplane.



1. Chassis Backplane Connector (PWR1)
2. Chassis Backplane Connector (PWR2)

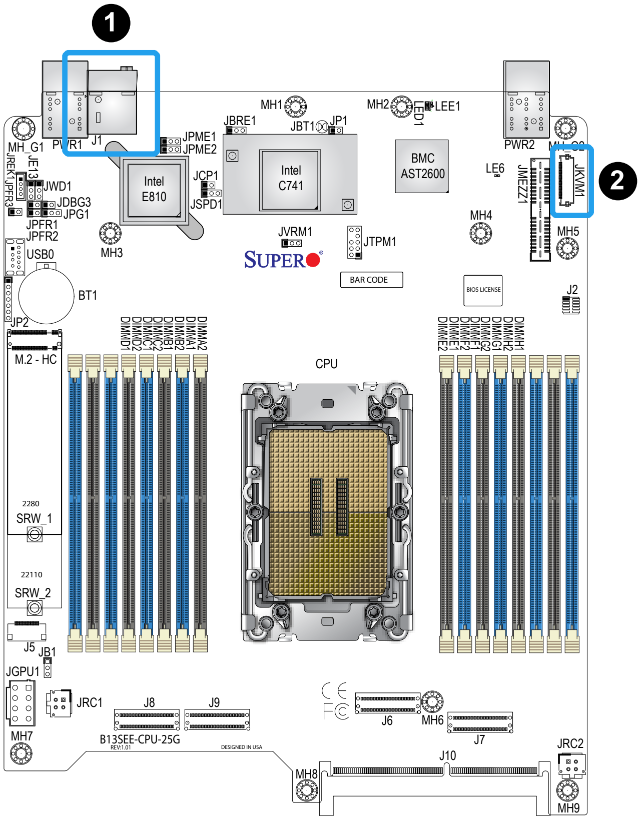
Headers

Chassis Backplane Connector

Use J1 to connect to the system backplane. This connection provides Ethernet to the system and CMM management.

VGA/USB Module Connector

Use JKVM1 to connect to a VGA/USB module.



1. Chassis Backplane Connector
2. VGA/USB Module Connector

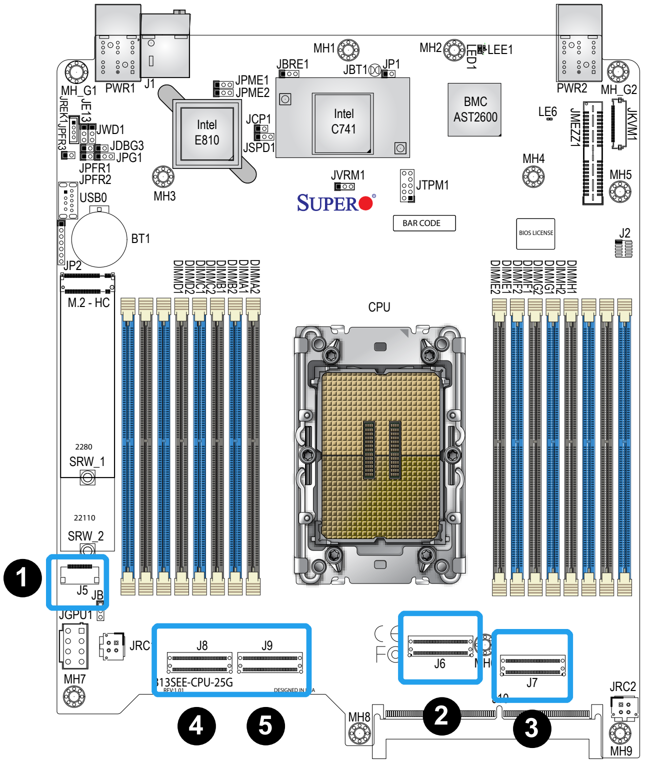
Front Panel Connector

Connect an FPC cable from J5 to the front panel module for power on/off, KVM, and other system LED notifications. Refer to the table below for LEDs and their functions.

Function	State	Description
Power Button	N/A	Turns the blade module on and off
Power LED	Green Solid Orange Flashing Orange	Indicates power status "On" Indicates power status "Off" (with power cables plugged in) Indicates the node is not ready or not enough power to turn on
KVM/UID LED	Blue Flashing Blue	Indicates KVM is being utilized by the blade unit Indicates UID activated on the blade module
Network/IB LED	Flashing Green Flashing Orange	Indicates network activity over LAN Indicates network activity over the Infiniband module
System Fault LED	Red	Indicates a memory error, overheat, VGA error, or any error that prevents booting

PCIe 5.0 x8 MCIO Connectors

J6, J7, J8, J9 are Mini Cool Edge IO PCIe x8 connectors. Use these connectors for GPU/ E1.S/AIOM riser cards.



1. Front Panel Connector
2. MCIO Connector (J6)
3. MCIO Connector (J7)
4. MCIO Connector (J8)
5. MCIO Connector (J9)

PCIe 4.0 x16 SIOM Connector

J10 is the SIOM connector for one SAS card or two M.2 x4 or two PCIe 4.0 NVMe.

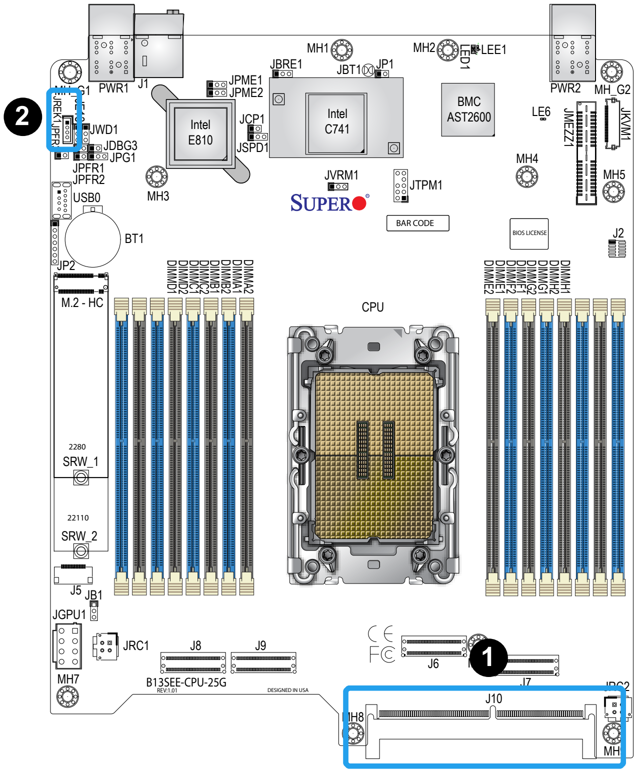
Intel RAID Key Header

An Intel RAID Key header is located at JREK1 on the motherboard. Install a VROC RAID key on JREK1 for NVMe RAID support.

Note: For detailed instructions on how to configure VROC RAID settings, refer to the VROC RAID Configuration User's Guide posted on the Supermicro website at http:\\www.supermicro.com/support/manuals.

Intel RAID Key
Pin Definitions

Pin#	Definition
1	GND
2	PU 3.3 V Stdby
3	GND
4	PCH RAID KEY



1. SIOM Connector
2. Intel RAID Key Header

PCIE 4.0 x16 Mezzanine Card Connector

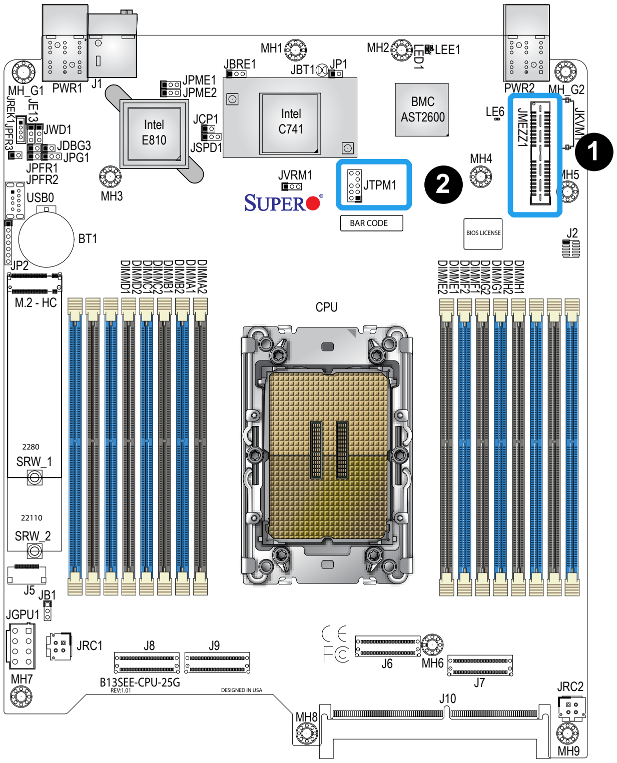
JMEZZ1 connects to a backplane Ethernet add-on card expansion slot.

Trusted Platform Module(TPM)/Port 80 Header

A Trusted Platform Module (TPM)/Port 80 header is located at JTPM1 to provide TPM support and Port 80 connection. Use this header to enhance system performance and data security. Refer to the table below for pin definitions. Go to the following link for more information on the TPM: http://www.supermicro.com/manuals/other/TPM.pdf.

Trusted Platform Module Header
Pin Definitions

Pin#	Definition	Pin#	Definition
1	+3.3 V	2	SPI_CS#
3	RESET#	4	SPI_MISO
5	SPI_CLK	6	GND
7	SPI_MOSI	8	
9	+3.3 V Stby	10	SPI_IRQ#



1. Mezzanine Card Connector
2. TPM/Port 80

M.2-HC Slot

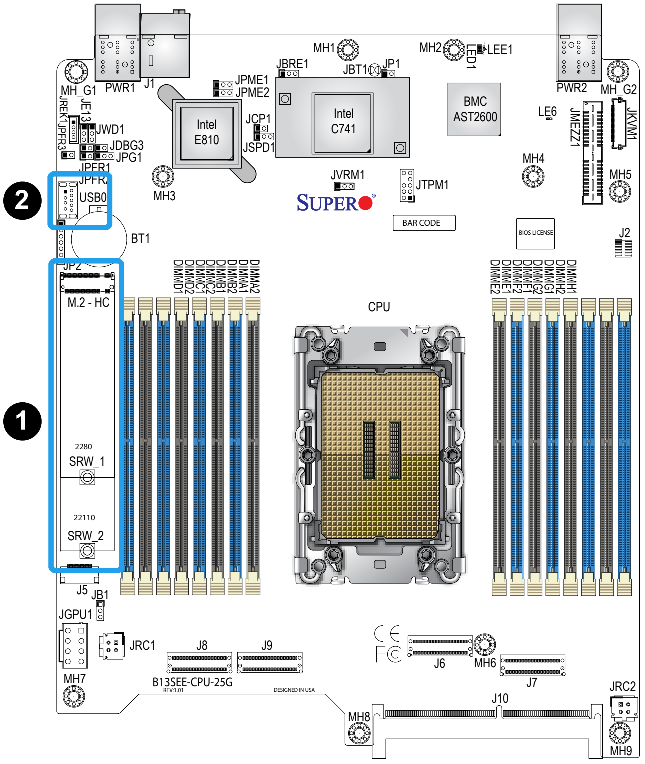
This motherboard has one hybrid M.2 slot at M.2-HC. M.2 was formerly known as Next Generation Form Factor (NGFF) and serves to replace mini PCIe. M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. M.2-HC supports an M-Key PCIe 3.0 x4 or SATA 3.0 device in the 2280 and 22110 form factors.

Internal USB 2.0/3.0 Type-A Connector

There is one internal USB 2.0/3.0 port (USB0) on the motherboard.

Internal USB0
Pin Definitions

Pin#	Definition	Pin#	Definition
A1	VBUS	B1	VBUS
A2	D-	B2	D-
A3	D+	B3	D+
A4	GND	B4	GND
A5	Stda_SSRX-	B5	Stda_SSRX-
A6	Stda_SSRX+	B6	Stda_SSRX+
A7	GND	B7	GND
A8	Stda_SSTX-	B8	Stda_SSTX-
A9	Stda_SSTX+	B9	Stda_SSTX+



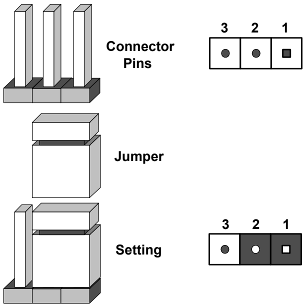
1. M.C-HC Slot
2. Internal USB2.0/3.0 Type-A Connector

2.6 Jumper Settings

How Jumpers Work

To modify the operation of the motherboard, jumpers can be used to choose between optional settings. Jumpers create shorts between two pins to change the function of the connector. Pin 1 is identified with a square solder pad on the printed circuit board. See the diagram below for an example of jumping pins 1 and 2. Refer to the motherboard layout page for jumper locations.

Note: On two-pin jumpers, Closed means the jumper is on and Open means the jumper is off the pins.



CMOS Clear

JBT1 is used to clear CMOS, which will also clear any passwords. Instead of pins, this jumper consists of contact pads to prevent accidentally clearing the contents of CMOS.

To Clear CMOS

1. First power down the system and unplug the power cord(s).

2. Remove the cover of the chassis to access the motherboard.

3. Remove the onboard battery from the motherboard.

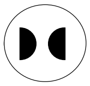
4. Short the CMOS pads with a metal object such as a small screwdriver for at least four seconds.

5. Remove the screwdriver or shorting device.

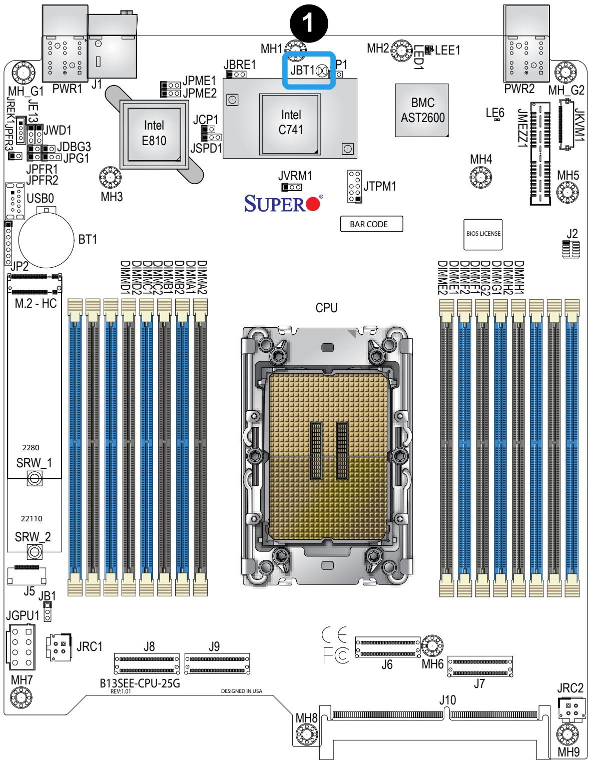
6. Replace the cover, reconnect the power cord(s), and power on the system.

Note: Clearing CMOS will also clear all passwords.

Do not use the PW_ON connector to clear CMOS.



JBT1 contact pads



1. Clear CMOS

BIOS Recovery

Close pins 2-3 of JBRE1 for BIOS recovery. The default setting is on pins 1 and 2 for normal operation. Refer to the table below for jumper settings. The default setting is Normal.

BIOS Recovery Jumper Settings

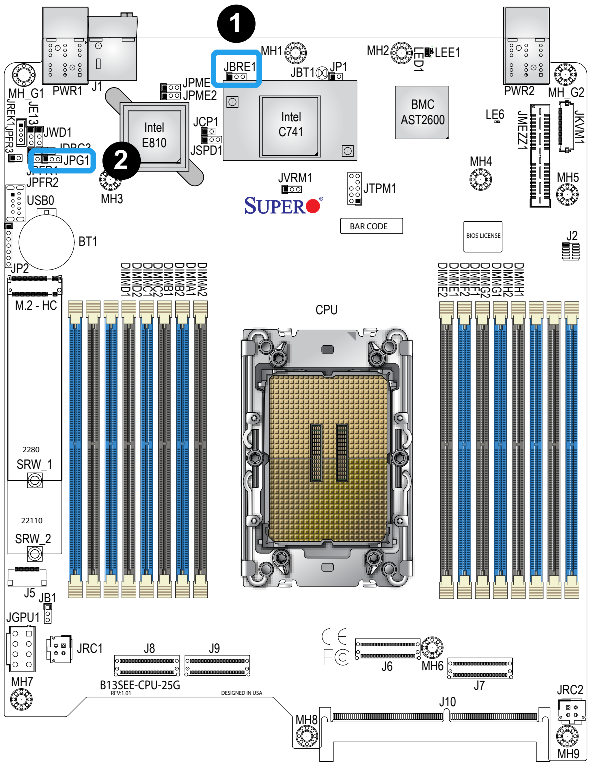
Jumper Setting	Definition
Pins 1-2	Normal
Pins 2-3	BIOS Recovery

VGA Enable/Disable

Use JPG1 to enable or disable the VGA port using the onboard graphics controller. The default setting is Enabled.

VGA Enable/Disable Jumper Settings

Jumper Setting	Definition
Pins 1-2	Enabled
Pins 2-3	Disabled



1. BIOS Recovery
2. VGA Enable/Disable

Management Engine (ME) Recovery Mode

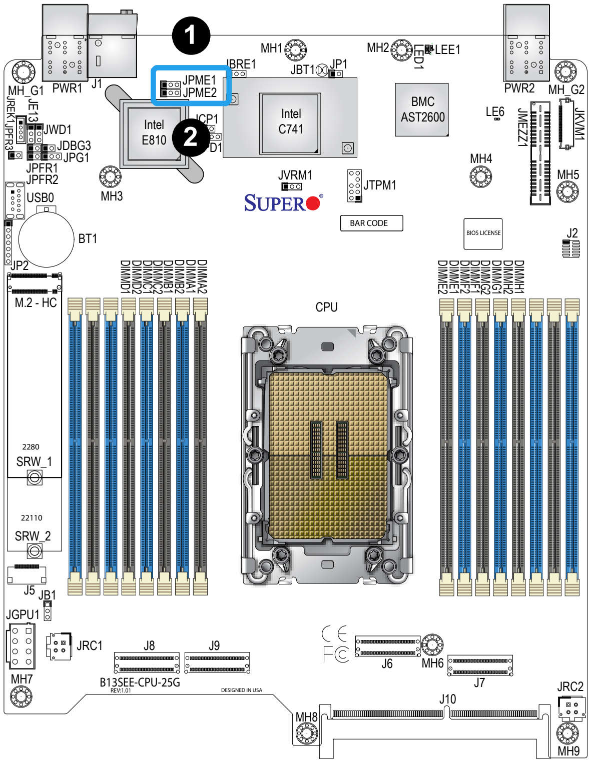
Use JPME1 to select ME Firmware Recovery mode, which will limit resource allocation for essential system operation only in order to maintain normal power operation and management. In the single operation mode, online upgrade will be available via Recovery mode. Refer to the table below for jumper settings.

ME Recovery Mode Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Normal
Pins 2-3	ME Recovery

Manufacturing Mode Select

Close pins 2-3 of JPME2 to bypass SPI flash security and force the system to operate in the manufacturing mode, which will allow you to flash the system firmware from a host server for system setting modifications. Refer to the table below for jumper settings.

Manufacturing Mode Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Normal (Default)
Pins 2-3	Manufacturing Mode



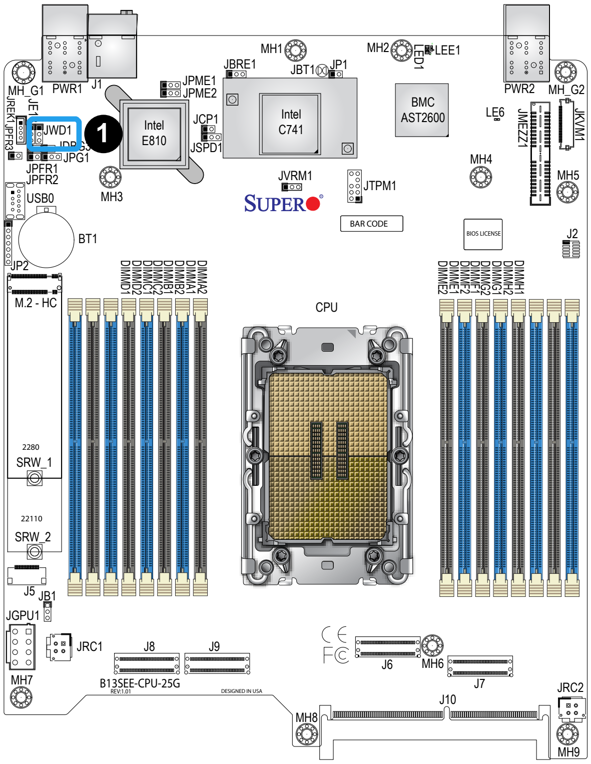
1. ME Recovery
2. Manufacturing Mode Select

Watchdog

JWD1 controls the Watchdog function. Watchdog is a monitor that can reboot the system when a software application hangs. Jumping pins 1-2 will cause Watchdog to reset the system if an application hangs. Jumping pins 2-3 will generate a non-maskable interrupt signal for the application that hangs. Watchdog must also be enabled in BIOS.

Note: When Watchdog is enabled, users need to write their own application software to disable it.

Watchdog Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Reset (Default)
Pins 2-3	NMI
Open	Disabled



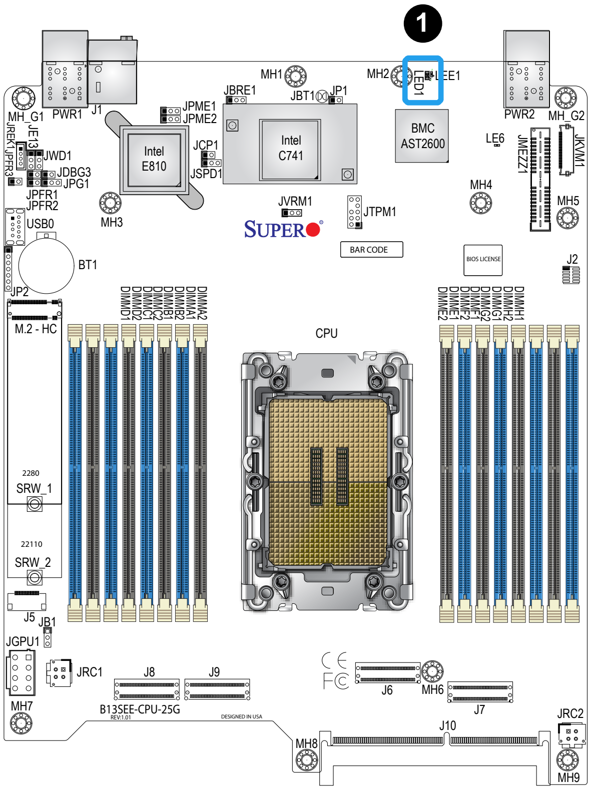
1. Watchdog Timer

2.7 LED Indicators

BMC Heartbeat LED

LED1 is the BMC Heartbeat LED. When the LED is blinking green, the BMC is working. Refer to the table below for the LED status.

BMC Heartbeat LED	
LED Color	**Definition**
Green: Blinking	BMC Normal



1. BMC Heartbeat LED

Chapter 3

Troubleshooting

3.1 Troubleshooting Procedures

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

Before Power On

1. Make sure that there are no short circuits between the motherboard and chassis.
2. Disconnect all ribbon/wire cables from the motherboard, including those for the keyboard and mouse.
3. Remove all add-on cards.
4. Install the CPU (making sure it is fully seated) and connect the front panel connectors to the motherboard.

No Power

1. Make sure that there are no short circuits between the motherboard and the chassis.
2. Make sure that the ATX power connectors are properly connected.
3. Check that the 115 V/230 V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.

No Video

1. If the power is on but you have no video, remove all add-on cards and cables.
2. Use the speaker to determine if any beep codes are present. Refer to Appendix A for details on beep codes.
3. Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory or try a different one).

System Boot Failure

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

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

- If there is no error beep, try to turn on the system without DIMM modules installed. If there is still no error beep, replace the motherboard.
- If there are error beeps, clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper (JBT1). Refer to Chapter 2.6 for instructions on how to clear CMOS.

2. Remove all components from the motherboard, especially the DIMM modules. Make sure that system power is on and that memory error beeps are activated.
3. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors troubleshooting procedure in this chapter.

Memory Errors

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

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

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

3. Make sure that you are using the correct type of DDR5 ECC RDIMM/3DSRDIMM modules recommended by the manufacturer.

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

Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to Chapter 2 for details on recommended power supplies.

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

3. If the above steps do not fix the setup configuration problem, contact your vendor for repairs.

When the System Becomes Unstable

A. If the system becomes unstable during or after OS installation, check the following:

1. CPU/BIOS support: Make sure that your CPU is supported and that you have the latest BIOS installed in your system.

2. Memory support: Make sure that the memory modules are supported by testing the modules using memtest86 or a similar utility.

   Note: Click on the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.

3. SSD support: Make sure that all solid state drives (SSDs) work properly. Replace the bad SSDs with good ones.

4. System cooling: Check the system cooling to make sure that all heatsink fans and CPU/system fans, etc., work properly. Check the hardware monitoring settings in the IPMI to make sure that the CPU and system temperatures are within the normal range. Also check the front panel Overheat LED and make sure that it is not on.

5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Refer to our website for more information on the minimum power requirements.

6. Proper software support: Make sure that the correct drivers are used.

B. If the system becomes unstable before or during OS installation, check the following:

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as a USB flash or media drive.

2. Cable connection: Check to make sure that all cables are connected and working properly.

3. Use the minimum configuration for troubleshooting: Remove all unnecessary components (starting with add-on cards first), and use the minimum configuration (but with the CPU and a memory module installed) to identify the trouble areas. Refer to the steps listed in Section A above for proper troubleshooting procedures.

4. Identify bad components by isolating them: If necessary, remove a component in question from the chassis, and test it in isolation to make sure that it works properly. Replace a bad component with a good one.

5. Check and change one component at a time instead of changing several items at the same time. This will help isolate and identify the problem.

6. To find out if a component is good, swap this component with a new one to see if the system will work properly. If so, then the old component is bad. You can also install the component in question in another system. If the new system works, the component is good and the old system has problems.

3.2 Technical Support Procedures

Before contacting Technical Support, take the following steps. Also, note that as a motherboard manufacturer, Supermicro also sells motherboards through its channels, so it is best to first check with your distributor or reseller for troubleshooting services. They should know of any possible problems with the specific system configuration that was sold to you.

1. Go through the Troubleshooting Procedures and Frequently Asked Questions (FAQ) sections in this chapter or see the FAQs on our website (http://www.supermicro.com/FAQ/index.php) before contacting Technical Support.

2. BIOS upgrades can be downloaded from our website (http://www.supermicro.com/ResourceApps/BIOS_IPMI_Intel.html).

3. If you still cannot resolve the problem, include the following information when contacting Supermicro for technical support:

- Motherboard model and PCB revision number

- BIOS release date/version (This can be seen on the initial display when your system first boots up.)

- System configuration

4. An example of a Technical Support form is on our website at https://webpr3.supermicro.com/SupportPortal/.

- Distributors: For immediate assistance, have your account number ready when placing a call to our Technical Support department. We can be reached by email at support@supermicro.com.

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: The supports up to 4 TB of DDR5 ECC RDIMM/3DSRDIMM memory with speeds of up to 5600 MT/s in eight DIMM slots or 4400 MT/s in 16 DIMM slots.

Question: How do I update my BIOS?

Answer: It is recommended that you do not upgrade your BIOS if you are not experiencing any problems with your system. Updated BIOS files are located on our website at http://www.supermicro.com/ResourceApps/BIOS_IPMI_Intel.html. Check our BIOS warning message and the information on how to update your BIOS on our website. Select your motherboard model and download the BIOS file to your computer. Also, check the current BIOS revision to make sure that it is newer than your BIOS before downloading. Unzip the BIOS file onto a bootable USB device. Run the batch file using the format FLASH.BAT filename.rom from your bootable USB device to flash the BIOS. Then, your system will automatically reboot.

Warning: Do not shut down or reset the system while updating the BIOS to prevent possible system boot failure!

Note: The SPI BIOS chip used on this motherboard cannot be removed. Send your motherboard back to our RMA Department at Supermicro for repair. For BIOS Recovery instructions, refer to the AMI BIOS Recovery Instructions posted at http://www.supermicro.com/support/manuals/.

3.4 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

1. Power off your system and unplug your power cable.

2. Locate the onboard battery as shown below.

3. Using a tool such as a pen or a small screwdriver, push the battery lock outwards to unlock it. Once unlocked, the battery will pop out from the holder.

4. Remove the battery.

Proper Battery Disposal

Warning: Handle a used battery carefully. Do not discard it in the garbage or a public landfill. Comply with the regulations set up by your local hazardous waste management agency to dispose a used battery properly.

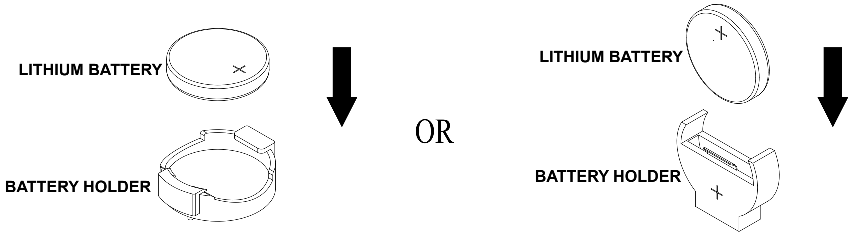
Battery Installation

1. To install an onboard battery, follow steps 1 and 2 above and continue below:

2. Identify the battery's polarity. The positive (+) side should be facing up.

3. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.

Warning: When replacing a battery, replace it with the same type.



3.5 Returning Merchandise for Service

A receipt or copy of your invoice marked with the date of purchase is required before any warranty service will be rendered. You can obtain service by calling your vendor for a Returned Merchandise Authorization (RMA) number. When returning the motherboard to the manufacturer, the RMA number should be prominently displayed on the outside of the shipping carton, and the shipping package is mailed prepaid or hand-carried. Shipping and handling charges will be applied for all orders that must be mailed when service is complete. For faster service, you can also request a RMA authorization online (http://www.supermicro.com/RmaForm/).

This warranty only covers normal consumer use and does not cover damages incurred in shipping or from failure due to the alternation, misuse, abuse or improper maintenance of products.

During the warranty period, contact your distributor first for any product problems.

Chapter 4

UEFI BIOS

4.1 Introduction

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

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. Refer to the Manual Download area of our website for any changes to 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.

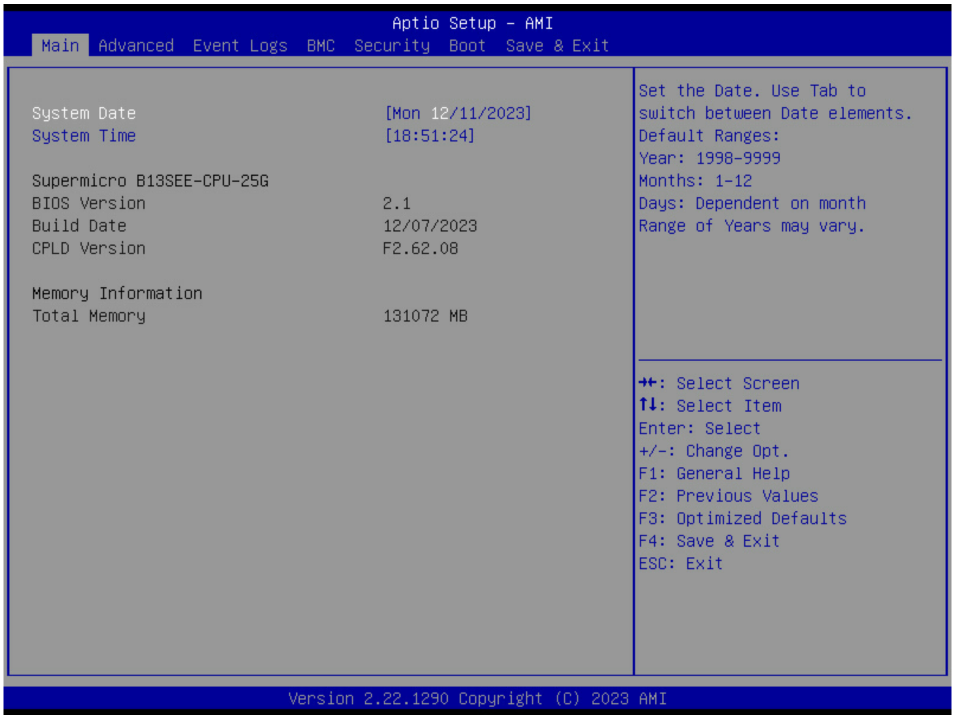
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message accompany it. (Note that 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 open the list of settings within that submenu.

The BIOS setup utility uses a key-based navigation system called hot keys. Most of these hot keys (<F1>, <F10>, <Enter>, <ESC>, Arrow keys, etc.) can be used at any time during the setup navigation process.

4.2 Main Setup

When you first enter the AMI BIOS setup utility, you 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. The following Main menu items be displayed:



```
System Date                                  [Mon 12/11/2023]
System Time                                  [18:51:24]

Supermicro B13SEE-CPU-25G
BIOS Version                                 2.1
Build Date                                   12/07/2023
CPLD Version                                 F2.62.08

Memory Information
Total Memory                                 131072 MB
```

```
Set the Date. Use Tab to
switch between Date elements.
Default Ranges:
Year: 1998-9999
Months: 1-12
Days: Dependent on month
Range of Years may vary.

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

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 B13SEE-CPU-25G

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.

CPLD Version

This feature displays the version of the CPLD.

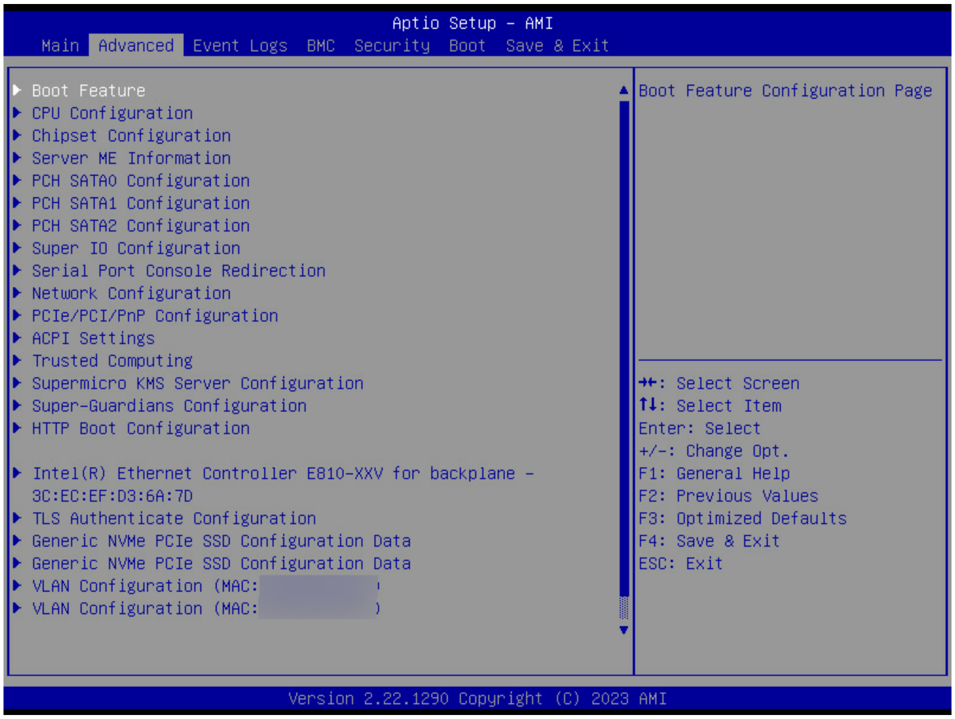
Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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



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

▶ Boot Feature                                              Boot Feature Configuration Page
▶ CPU Configuration
▶ Chipset Configuration
▶ Server ME Information
▶ PCH SATA0 Configuration
▶ PCH SATA1 Configuration
▶ PCH SATA2 Configuration
▶ Super IO Configuration
▶ Serial Port Console Redirection
▶ Network Configuration
▶ PCIe/PCI/PnP Configuration
▶ ACPI Settings
▶ Trusted Computing
▶ Supermicro KMS Server Configuration                       →←: Select Screen
▶ Super-Guardians Configuration                             ↑↓: Select Item
▶ HTTP Boot Configuration                                   Enter: Select
                                                            +/-: Change Opt.
▶ Intel(R) Ethernet Controller E810-XXV for backplane -     F1: General Help
  3C:EC:EF:D3:6A:7D                                         F2: Previous Values
▶ TLS Authenticate Configuration                            F3: Optimized Defaults
▶ Generic NVMe PCIe SSD Configuration Data                  F4: Save & Exit
▶ Generic NVMe PCIe SSD Configuration Data                  ESC: Exit
▶ VLAN Configuration (MAC:[redacted])
▶ VLAN Configuration (MAC:[redacted])

              Version 2.22.1290 Copyright (C) 2023 AMI
```

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 between displaying the Power-on Self Test (POST) messages or the OEM logo at 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**.

Note: BIOS Power-on Self Test (POST) messages are always displayed regardless of the setting of this feature.

Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to use the current AddOn ROM display settings. Select Force BIOS to use the Option ROM display mode 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

Select Enabled to force the system to wait until the <F1> key is pressed if an error occurs. The options are **Disabled** and Enabled.

INT19 Trap Response

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

Re-try Boot

When Extensible Firmware Interface (EFI) Boot is selected, the system BIOS will automatically reboot the system from an EFI boot device after an initial boot failure. Select Legacy Boot to allow the BIOS to automatically reboot the system from a Legacy boot device after an initial boot failure. The options are **Disabled**, Legacy Boot, and EFI Boot.

▶Power Configuration

Watch Dog Function

Select Enabled to allow the Watch Dog timer to reboot the system when it is inactive for more than 5 minutes. The options are **Disabled** and Enabled.

Watch Dog Action (Available when "Watch Dog Function" is set to Enabled)

Use this feature to configure the Watch Dog Time_out setting. The options are **Reset** and NMI.

Front USB Port(s) (Available when "Lockdown Mode" is set to Enabled with the DCMS key)

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 device to be used in the front USB ports without booting the system. The options are **Enabled**, Disabled, and Enabled (Dynamic).

Note 1: Supermicro DataCenter Management Suite per Node License Key (SFT-DC-MS-SINGLE) is Supermicro's Data Center Management Suite license that enables server nodes to take full advantage of Supermicro Management Software and Utilities features.

Note 2: Refer to the submenu of Security > Supermicro Security Erase COnfiguration to set "Lockdown Mode."

Rear USB Port(s) (Available when "Lockdown Mode" is set to Enabled with the DCMS key)

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 device to be used in the rear USB ports without booting the system. The options are **Enabled**, Disabled, and Enabled (Dynamic).

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 presses the power button. The options are **Instant Off** and 4 Seconds Override.

▶CPU Configuration

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

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

▶Advanced Power Management Configuration

Power Technology

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

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

Set this feature to allow either the operating system (OS) or the BIOS to control the Intel Performance and Energy Bias Hint (EFB). The options are OS Controls EFB and BIOS Controls EFB.

ENERGY_PERF_BIAS_CFG Mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode) (Available when "Power Performance Tuning" is set to BIOS Controls EFB)

Use this feature to configure the proper operation setting for your machine by achieving the desired system performance level and energy saving (efficiency) level at the same time. Select Maximum Performance to maximize system performance to its highest potential; however, this may consume maximal amount of power as energy is needed to fuel processor operation. Select Performance to enhance system performance; however, this may consume more power as energy is needed to fuel the processors for operation. The options are Extreme Performance, Maximum Performance, Performance, **Balanced Performance**, Balanced Power, Power, and Max Power Efficient. .

Optimized Power Mode

Set this feature to Enable to reduce overall power consumption. The options are **Disable** and Enable. When this feature to set to Enable, the features below will automatically be set by the BIOS:

- "Power Performance Tuning" – BIOS Controls EFB
- "ENERGY_PERF_BIAS_CFG Mode" – Balanced Performance
- "Enhanced Halt State (C1E) – Enable

▶CPU P State Control

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

AVX P1 (Available when "SpeedStep (P-States)" is set to Enable)

Use this feature to set the appropriate TDP level for the system. The Intel Advanced Vector Extensions (Intel AVX) P1 feature allows you to set the base P1 ratio for Streaming SIMD Extensions (SSE) and AVX workloads. Each P1 ratio has the corresponding AVX Impressed Current Cathodic Protection (ICCP) pre-grant license level, which refers to the selection between different AVX ICCP transition levels. The options are **Nominal**, Level 1, and Level 2.

Intel SST-PP (Available when "SpeedStep (P-States)" is set to Enable and "Dynamic SST-PP" is set to Disable)

Use this feature to configure the Intel Speed Select Technology-Performance Profile. This feature allows you to choose from two additional Base-Frequency conditions maximum for CPU P State Control. The options are **Auto**, Level 0, Level 3, and Level 4.

Dynamic SST-PP (Available when "SpeedStep (P-States)" is set to Enable and when your CPU supports the Intel Speed Select function)

If this feature is set to Enable, it allows you to configure Intel SST-PP features, including Base, Configuration 3, and Configuration 4 settings under various processor working conditions. The options are **Disable** and Enable.

The following information is displayed when "SpeedStep (P-States)" is set to Enable:

- SST-PP Level
- Capable
- Core Count
- P1 Ration

- Package TDP (W)
- DTS_Max

Activate SST-BF (Available when your CPU supports the Intel Speed Select function)

Select Enable for Intel Speed Select Technology-Base Frequency (SST-BF) support. The options are **Disable** and Enable.

Configure SST-BF (Available when your CPU supports the Intel Speed Select function and when "Activate SST-BF" is set to Enable)

When this feature is set to Enable, the system BIOS will configure SST-BF High Priority Core settings so that system software does not have to configure these settings. The options are Disable and **Enable**.

SpeedStep (P-States)

Enhanced Intel SpeedStep Technology (EIST) allows the system to automatically adjust processor voltage and core frequency in an effort to reduce power consumption and heat dissipation. Refer to Intel's website for detailed information. The options are Disable and **Enable**.

EIST PSD Function (Available when "SpeedStep (P-States)" is set to Enable)

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

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

Select Enable to allow the CPU to operate at the manufacturer-defined turbo speed by increasing CPU clock frequency. This feature is available when it is supported by the processors used in the system. The options are Disable and **Enable**.

▶Hardware PM State Control

Hardware P-States

If this feature is set to Disable, system hardware will choose a P-state setting for the system based on an OS request. If this feature is set to Native Mode, hardware will choose a P-state setting based on the OS guidance. If this feature is set to Native Mode with No Legacy Support, system hardware will choose a P-state setting independently without OS guidance. The options are **Disable**, Native Mode, Out of Band Mode, and Native Mode with No Legacy Support.

▶Frequency Prioritization (Available when "Power Technology" is set to Custom, "Hardware P-states" is set to Native Mode or "Native Mode with No Legacy Support," and when your processor supports Intel SST-CP)

SST-CP

With Intel Speed Select Technology (Intel SST-CP), surplus frequency is allocated based on the cores' weights. The weight for each core is assigned by the OS or the Virtual Machine Manager (VMM). The options are Enable and **Disable**.

▶CPU C State Control

Enabled Monitor MWAIT

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

CPU C1 Auto Demotion

Select Enable to allow the CPU to automatically demote to the CPU C1 state. The options are Disable, Enable, and **Auto**.

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 enable "Enhanced Halt State" support, which will significantly reduce the CPU's power consumption by minimizing CPU's clock cycles and reduce voltage during a "Halt State." The options are Disable and **Enable**.

▶Package C State Control

Package C State

Use this feature to optimize and reduce CPU package power consumption in the idle mode. Note that the changes you've made in this setting will affect all CPU cores or the circuits of the entire system. The options are C0/C1 state, C2 state, C6 (non Retention) state, C6 (Retention) state, No Limit, and **Auto**.

▶CPU1 Core Disable Bitmap

Available Bitmap:

This feature displays the available bitmap.

Disable Bitmap

Enter 0 to enable this feature for all CPU cores. Enter FFFFFFFFFFF to disable this feature for all CPU cores. Note that at least one core per CPU must be enabled. Disabling all cores is not allowed. The default setting is 0.

Hyper-Threading [ALL]

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

Hardware Prefetcher

If this feature is set to Enable, the hardware prefetcher will prefetch data from the main system memory to Level 2 cache to help expedite data transaction to enhance memory performance. The options are **Enable** and Disable.

Adjacent Cache Prefetch

Select Enable for the CPU to prefetch both cache lines for 128 bytes as comprised. Select Disable for the CPU to prefetch both cache lines for 64 bytes. The options are **Enable** and Disable.

DCU Streamer Prefetcher

If this feature is set to Enable, the Data Cache Unit (DCU) streamer prefetcher will prefetch data streams from the cache memory to the DCU to speed up data accessing and processing to enhance CPU performance. The options are **Enable** and Disable.

DCU IP Prefetcher

This feature allows the system to use the sequential load history, which is based on the instruction pointer of previous loads, to determine whether the system will prefetch additional lines. The options are **Enable** and Disable.

LLC Prefetch

If this feature is set to Enable, LLC (hardware cache) prefetching on all threads will be supported. The options are **Disable** and Enable.

Extended APIC

Use this feature to set the Extended Extended Advanced Programmable Interrupt Controller (APIC) feature. Based on the Intel Hyper-Threading technology, each logical processor (thread) is assigned 256 APIC IDs (APIDs) in 8-bit bandwidth. When this feature is set to Enable, the APIC ID will be expanded from 8 bits to 16 bits to provide 512 APIDs to each thread to enhance CPU performance. The options are Disable and **Enable**.

Intel Virtualization Technology

Select Enable to enable the Intel Vanderpool Technology for Virtualization platform support, which will allow multiple operating systems to run simultaneously on the same computer to maximize system resources for performance enhancement. The options are Disable and **Enable**.

Note: Reboot the system for any change of the setting to take effect.

Enable SMX

Select Enable to support Safer Mode Extensions (SMX) which provides a programming interface for system software to establish a controlled environment to support the trusted

platform configured by the end user and to verify a virtual machine monitor before it is allowed to run. The options are **Disable** and Enable.

PPIN Control

Select Unlock/Enable to use the Protected Processor Inventory Number (PPIN) in the system. The PPIN is a unique number set for tracking a given Intel Xeon server processor. 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**.

Limit CPU PA to 46 Bits

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

TME, TME-MT, TDX

Memory Encryption (TME) (Available when your CPU supports Intel TME)

Select Enabled for Intel Total Memory Encryption (TME) support to enhance memory data security. The options are **Disabled** and Enabled.

Total Memory Encryption (TME) Bypass (Available when "Memory Encryption (TME)" is set to Enabled)

Use this feature to disable/enable the TME function for physical memory protection. The options are **Auto**, Disabled, and Enabled.

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

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

Memory Integrity (Available when both "Memory Encryption (TME)" and "Total Memory Encryption Multi-Tenant (TME-MT)" are set to Enabled and when "Limit CPU PA to 46 Bits" is set to Disable)

Use this feature to enable TME-MT memory integrity protection for memory transactions. The options are **Disabled** and Enabled.

Key Stock Amount (Available when "Memory Encryption (TME)" is set to Enabled and when your system supports this feature)

Use this feature to set the number of unique keys per system (the number of tenants per platform). The default setting is **0**.

TME-MT Key ID Bits (Available when "Memory Encryption (TME)" is set to Enabled)

Use this feature to set the number of bits for each key ID. The default setting is **0**.

Trust Domain Extension (TDX) (Available when your CPU supports Intel TDX)

Use this feature to enable Intel Trust Domain Extension (TDX) technology support to enhance control of data security. The options are **Disabled** and Enabled.

TDX Secure Arbitration Mode Loader (SEAM Loader) (Available when your CPU supports Intel TDX)

The SEAM Loader (SEAMLDR) is used to load and update Intel TDX modules into the SEAM memory range by verifying the digital signature. The options are **Disabled** and Enabled.

Disable Excluding Mem Below 1MB In CMR (Available when "Memory Encryption (TME)" is set to Enabled and when "Trust Domain Extension (TDX)" is set to Enabled)

Use this feature to enable/disable TDX Excluding CMR below 1 MB. The options are Disabled, Enabled, and **Auto**.

TME-MT/TDX Key Split (Available when "Memory Encryption (TME)" is set to Enabled and when "Trust Domain Extension (TDX)" is set to Enabled)

Use this feature to set the number of bits for TDX. The other bits will be used by TME-MT. The default setting is **1**.

TME-MT Keys: (Available when "Memory Encryption (TME)" is set to Enabled and when "Trust Domain Extension (TDX)" is set to Enabled)

This feature displays the number of keys designated for TME-MT.

TDX Keys: (Available when "Memory Encryption (TME)" is set to Enabled and when "Trust Domain Extension (TDX)" is set to Enabled)

This feature displays the number of keys designated for TDX.

Software Guard Extension (SGX)

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

SGX Factory Reset (Available when "Memory Encryption (TME)" is set to Enabled and when your CPU supports Intel SGX).

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

SW Guard Extensions (SGX)

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

SGX Package Info In-Band Access

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

PRM Size for SGX (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Use this feature to set the Processor Reserved Memory Range Register (PRMRR) size. The options are Auto, 128M, **256M**, 512M, 1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, and 512G. Please note that the available options are based on your motherboard features, memory size, and memory map.

SGX QoS (Available when "SW Guard Extensions (SGX)" is set to Enabled)

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

Select Owner EPOCH Input Type (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Owner EPOCH is used as a parameter to allow you to add personal entropy into the key derivation process. A correct Owner EPOCH is required to have access to personal data previously sealed by other platform users. There are two Owner EPOCH modes. One is New Random Owner EPOCH, and the other is manually entered by the user. Each EPOCH is 64-bit. The options are Change to New Random Owner EPOCHs and **Manual User Defined Owner EPOCHs**.

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

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

Use this feature to enter the EPOCH value. The default is **0**.

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

Use this feature to enter the EPOCH value. The default is **0**.

SGXLEPUBKEYHASHx Write Enable (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Use this feature to enable writes to SGXLEPUBKEYHASH[3..0] from OS/SW. The options are Disabled and **Enabled**. Only those CPUs that support Intel SGX Flexible Launch Control (FLC) feature have SGXLEPUBKEYHASH, which contains the hash of the public key for the SGX Launch Enclave (LE) to be signed with.

SGXLEPUBKEYHASH0 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 0–7 of SGX Launch Enclave Public Key Hash.

SGXLEPUBKEYHASH1 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 8–15 of SGX Launch Enclave Public Key Hash.

SGXLEPUBKEYHASH2 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 16–23 of SGX Launch Enclave Public Key Hash.

SGXLEPUBKEYHASH3 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 24–31 of SGX Launch Enclave Public Key Hash.

SGX Auto MP Registration (Available when "SW Guard Extensions (SGX)" is set to Enabled)

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

▶Chipset Configuration

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

▶North Bridge

▶Uncore Configuration

The following Uncore information is displayed:

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

Degrade Precedence

Use this feature to select the degrading precedence option for Ultra Path Interconnect (UPI) connections. Select Topology Precedent to degrade UPI features if system options are in conflict. Select Feature Precedent to degrade UPI topology if system options are in conflict. The options are **Topology Precedence** and Feature Precedence.

Link L0p Enable

Select Enable for the system BIOS to enable Link L0p support, which will allow the CPU to attempt to save power by reducing the UPI links from full width to half width when the CPU's workload is low. This feature is available for systems that use Intel processors with UPI technology support. The options are Disable, Enable, **Auto**, and Full L0p Enable.

Note 1: You can change the performance settings for non-standard applications by using this parameter. It is recommended that the default settings be used for standard applications.

Note 2: The "Full L0P Enable" option is available when a 5th Generation Intel Xeon Scalable Processor is installed.

Link L1 Enable

Select Enable for the BIOS to activate Link L1 support, which will power down the UPI links to save power when the system is idle. This feature is available for the system that uses Intel processors with UPI technology support. The options are Disable, Enable, and **Auto**.

Note: Linked L1 is an excellent feature for an idle system. L1 is used during Package C-States when its latency is hidden by other components during a wakeup.

KTI Prefetch

Keizer Technology Interconnect (KTI) is also known as the Intel Ultra Path Interconnect (UPI) technology. Select Enable for the KTI prefetcher to preload the L1 cache with data deemed relevant, which will allow the memory read to start earlier on a DDR bus in an effort to reduce latency. Select Auto for the KTI prefetcher to automatically preload the L1 cache with relevant data whenever is needed. The options are Disable, Enable, and **Auto**.

IO Directory Cache (IODC)

Select Enable for the IODC to generate snoops instead of generating memory lockups for remote IIO (InvIToM) and/or WCiLF (Cores). Select Auto for the IODC to generate snoops (instead of memory lockups) for WCiLF (Cores). The options are Disable, **Auto**, Enable for Remote InvItoM Hybrid Push, InvItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, and Enable for Remote InvItoM and Remote WViLF.

SNC

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

Note: The "Enable SNC4 (4-clusters)" is available depending based on your system configuration and processor.

Stale AtoS

The in-memory directory has three states: I, A, and S states. The I (-invalid) state indicates that the data is clean and does not exist in the cache of any other sockets. The A (-snoop All) state indicates that the data may exist in another socket in an exclusive or modified state. The S state (-Shared) indicates that the data is clean and may be shared in the caches across one or more sockets. When the system is performing "read" on the memory and if the directory line is in A state, we must snoop all other sockets because another socket may have the line in a modified state. If this is the case, a "snoop" will return the modified data. However, it may be the case that a line "reads" in an A state, and all the snoops come back with a "miss". This can happen if another socket reads the line earlier and then has silently dropped it from its cache without modifying it. If "Stale AtoS" is enabled, a line will transition to the S state when the line in the A state returns only snoop misses. That way, subsequent reads to the line will encounter it in the S state and will not have to snoop, saving the latency and snoop bandwidth. Stale "AtoS" may be beneficial in a workload where there are many cross-socket reads. The options are Disable, Enable, and **Auto**.

LLC Dead Line Alloc

Select Enable to opportunistically fill the deadlines in the LLC. The options are Disable, **Enable**, and Auto.

▶Memory Configuration

This feature allows you to configure Integrated Memory Controller (iMC) settings.

Enforce DDR Memory Frequency POR

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

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 3200, 3600, 4000, 4400, 4800, 5200, and 5600. Note that the options displayed are CPU-dependent.

Data Scrambling for PMem

Select Enable to enable data scrambling for PMem modules to enhance memory data security. Select Auto to use the Memory Reference Code (MRC) default setting for PMem data scrambling. The options are Disable, Enable, and **Auto**. This feature depends on support for the Intel Optane PMem 300 Series.

Data Scrambling for DDR5

Select Enable to enable data scrambling for DDR5 modules to enhance memory data security. The options are Disable and **Enable**.

Enable fADR

Select Enable to have Fast Asynchronous DRAM Refresh (fADR) support to enhance memory performance on Intel PMem 300 series DIMMs. With the support of fADR feature, the ADR safe domain (flush domain) includes CPU caches, IIO caches, and Write Pending Queue (WPQ). The implementation of fADR can lower flush time and reduce flush times. The support of fADR is based on your motherboard hardware features. The options are **Disable** and Enable. This feature depends on support for the Intel Optane PMem 300 Series.

Enable ADR (Available when "Enable fADR" is set to Disable)

Select Enable for Asynchronous DRAM Refresh (ADR) support to enhance memory performance. The options are Disable and **Enable**.

Legacy ADR Mode (Available when "Enable fADR" is set to Disable and "Enable ADR" is set to Enable)

Use this feature to support the Legacy ADR mode to enhance memory performance. In Legacy ADR mode, the ADR safe domain (flush domain) includes the WPQ in memory controllers. The options are Disable, Enable, and **Auto**

▶fADR Configuration (Available when "Enable fADR" is set to Enable)

Note: This submenu depends on support for the Intel Optane PMem 300 series.

Number of Cores

Use this feature to set the number of CPU cores to be involved in the fADR event. The options are 1 Core, 4 Cores, and **All Cores**.

Core Ratio

Use this feature to set the CPU core ratio to be involved in the fADR event. The options are **Auto** and Manual.

Core Ratio Value (Available when "Core Ratio" is set to Manual)

Use this feature to enter the core ratio value. The default value is **FF**.

Mesh Ratio

Use this feature to set the mesh ratio to be involved in the fADR event. The mesh ratio determines the frequency of data access between CPU cores and caches. The options are **Auto** and Manual.

Mesh Ratio Value (Available when "Mesh Ratio" is set to Manual)

Use this feature to enter the mesh ratio value. The default value is **FF**.

Flush Timeout

Use this feature to set the timeout setting when the data in the CPU cache memory will be flushed by the applications to persistent memory in the absence of system power. The options are **Auto** and Manual.

Flush Timeout Value (Available when "Flush Timeout" is set to Manual)

Use this feature to enter the flush timeout value. The default value is **FFF**.

DDR 2x Refresh Enable

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

CXL Type 3 Legacy

Select Enable to use the CXL Type 3 memory device, which can be supported by the CXL Type 2 flows, for memory bandwidth and capacity expansion. The options are **Disable** and Enable.

Note: This feature depends on the CXL Type 2 flow and the memory device used.

CXL Type 3 Legacy

Select Enable to use the CXL Type 3 memory device, which can be supported by the CXL Type 2 flows, for memory bandwidth and capacity expansion. The options are **Disable** and Enable.

Note 1: This feature depends on support for the Intel Optane PMem 300 Series

Note 2: This feature is available when your motherboard has a high bandwidth memory (HBM) CPU installed and when "NUMA" in ACPI Settings is set to Enabled.

▶Memory Topology

This feature displays the information of onboard memory modules as detected by the BIOS, for example:

P1-DIMMA1: 4800 MT/s Hynix DRx8 32 GB RDIMM

▶Page Policy

Page Policy

Use this feature to set your memory page policy. The options are **Closed** and Adaptive. The Closed Page Policy is good for random memory access patterns. The Adaptive Page Policy can reduce average memory latency.

▶Memory RAS Configuration

Use this submenu to configure the following Memory Reliability_Availability_Serviceability (RAS) settings.

Mirror Mode (Available when "ADDDC Sparing" is set to Disabled and "UEFI ARM Mirror" is set to Disabled)

Use this feature to configure the mirror mode settings for all 1LM/2LM memory modules in the system, which will create a duplicate copy of data stored in the memory to increase memory security and also reduce the memory capacity into half. The options are **Disabled**, Full Mirror Mode, and Partial Mirror Mode.

UEFI ARM Mirror (Available when "ADDDC Sparing" is set to Disabled and "Mirror Mode" is set to Disabled)

If this feature is set to Enable, mirror mode configuration settings for UEFI-based Address Range memory will be enabled upon system boot. This will create a duplicate copy of data stored in the memory to increase memory security, but it will reduce the memory capacity into half. The options are **Disabled** and Enabled.

ARM Mirror Percentage (Available when "UEFI ARM Mirror" is set to Enabled)

Use this feature to set the percentage of memory space to be used for UEFI ARM mirroring for memory security enhancement. The default setting is **0**.

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**.

Leaky Bucket Low Bit

Use this feature to set the Low Bit value for the Leaky Bucket algorithm, which is used to check the data transmissions between CPU sockets and the memory controller. The default setting is **11**.

Leaky Bucket High Bit

Use this feature to set the High Bit value for the Leaky Bucket algorithm, which is used to check the data transmissions between CPU sockets and the memory controller. The default setting is **14**.

ADDDC Sparing (Available when populating 1Rx4, 2Rx4, and 4Rx4 DIMM)

Select Enabled for Adaptive Double Device Data Correction (ADDDC) support, which will not only provide memory error checking and correction but will also prevent the system from issuing a performance penalty before a device fails. Please note that virtual lockstep mode will only start to work for ADDDC after a faulty DRAM module is spared. The options are Disabled and **Enabled**.

Patrol Scrub

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

DDR PPR Type

Post Package Repair (PPR) is a new feature available for the DDR4/DDR5 technology. PPR provides additional spare capacity within a DDR4/DDR5 DRAM module that is used to replace faulty cell areas detected during system boot. PPR offers two types of memory repairs. Soft Post Package Repair (sPPR) provides a quick, temporary fix on a raw element in a bank group of a DDR4/DDR5 DRAM device, while hard Post Package Repair (hPPR) will take a longer time to provide a permanent repair on a raw element. The options are PPR Disabled, **Hard PPR**, and Soft PPR.

Enhanced PPR

Use this feature to set advanced memory test. Select Enabled to always execute for every boot. Select Once to execute only one time. The options are **Disabled**, Enabled, and Persistent.

Memory PFA Support (Available when the DCMS key is activated)

Select Enabled to enable memory Predictive Failure Analysis (PFA) support. PFA can be used to avoid uncorrectable faults in the same memory page. The options are **Disabled** and Enabled.

▶PMem Configuration (Available when any PMem device is detected by the BIOS)

PMem QoS

Use this feature to set the PMem Quality of Service (QoS) mode.The options are **Disabled** and Profile 1.

PMem Performance Setting

This feature configures the baseline (default) performance setting for the onboard PMem memory, which largely depends on workload requirements. Select BW (Bandwidth) Optimized to optimize PMem performance. The options are **BW Optimized** and Balanced Profile.

Seamless: Opt-in DIMMs

This feature allows you to update PMem firmware if the DIMM firmware is available. The options are **Keep**, Disabled, and Enabled.

▶IIO Configuration

▶CPU1 Configuration

IOU0 (IIO PCIe Port 1)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU1 (IIO PCIe Port 2)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU2 (IIO PCIe Port 3)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU3 (IIO PCIe Port 4)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU4 (IIO PCIe Port 5)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

▶Socket0 Port DMI

Link Speed

Use this feature to select or view the link speeds 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

Data Link Feature Exchange

Use this feature to enable/disable the PCIe port to enter PCIe 4.0 DL_Feature negotiation state. The options are Disable and **Enable.**

DMI/PCIe Port MPSS

This feature allows you to configure the Max Payload Size Supported in DMI Device Capabilities register. 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, and **Auto**.

Note: If Auto is not used, make sure MPSS in PCH root ports is updated to the same or smaller value.

Equalization Bypass to Highest Rate

Enable this feature to bypass the equalization of intermediate data rates. This will reduce the time for link training in PCIe 5.0 devices. The options are Disable and **Enable**.

▶CPU2 Configuration / ▶CPU3 Configuration/ ▶CPU4 Configuration

IOU0 (IIO PCIe Port 1)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU1 (IIO PCIe Port 2)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU2 (IIO PCIe Port 3)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU3 (IIO PCIe Port 4)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

IOU4 (IIO PCIe Port 5)

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for a PCIe port. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

▶IOAT Configuration

Relaxed Ordering

Select Yes to allow certain transactions to be processed and completed before other transactions that have already been enqueued. The options are **No** and Yes.

▶Intel VT for Directed I/O (VT-D)

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

Select Enable to use Intel Virtualization Technology for Direct I/O VT-d support by reporting the I/O device assignments to the Virtual Machine Monitor (VMM) through the Direct Memory Access Remap Reporting (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.

Opt-Out Illegal MSI Mitigation (Available when "Intel VT for Directed I/O (VT-d)" is set to Enable)

If this feature is set to Enable, "Illegal OxzFEE Platform Mitigation" will be opted out. The options are Enable and **Disable**.

Pre-boot DMA Protection (Available when "Intel VT for Directed I/O (VT-d)" is set to Enable)

Select Enable to establish DMA protection during pre-boot processing by setting DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR ACPI table. The options are Enable and **Disable**.

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

Select Enable to support I/O DMA transfer remapping and device-generated interrupts. The options are **Auto**, Enable, and Disable.

PCIe ACSCTL (Available when "Intel VT for Directed I/O (VT-d)" is set to Enable)

Select Enable to program ACS control to Chipset PCIe Root Port bridges. Select Disable to program ACS control to all PCIe Root Port bridges. The options are Enable and **Disable**.

▶Intel VMD Technology

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

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

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

NVMe Mode Switch

When this feature is set to Auto, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are Manual, VMD, and **Auto**.

▶Intel VMD for Volume Management Device on CPU1 (Available when "NVMe Mode Switch" is set to Manual)

VMD Config for PCH ports

Enable/Disable VMD

Select Enable to enable Intel Volume Management Device (VMD) technology support for the stack specified. The options are **Disable** and Enable.

PCH Root Port 4/12/13 (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

Select Enable to enable Intel Volume Management Device (VMD) technology support for the stack specified. The options are **Disable** and Enable.

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 0/1/2/3/4/5/6

Enable/Disable VMD

Select Enable to enable Intel Volume Management Device (VMD) technology support for the stack specified. The options are **Disable** and Enable.

Socket0 IOU0 VMD port A/C/E/G (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

Select Enable to enable Intel Volume Management Device (VMD) technology support for the stack specified. The options are **Disable** and Enable.

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

▶Intel VMD for Volume Management Device on CPU2 / CPU3 / CPU4 (Available when "NVMe Mode Switch" is set to Manual)

VMD Config for IOU 0/1/2/3/4/5/6

Enable/Disable VMD

Select Enable to enable Intel Volume Management Device (VMD) technology support for the stack specified. The options are **Disable** and Enable.

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

▶PCIe Leaky Bucket Configuration

Gen2 / Gen3 / Gen4 / Gen5 Link Degradation

Use this feature to enable or disable link degradation for the selected PCIe link. When a link degradation even is triggered, the PCIe link (5 GT/s, 8 GT/s, 16 GT/s, 32 GT/s) and higher modes are disabled. The options are Disable and **Enable**.

IIO-PCIe Express Global Options

==

PCIe ASPM Support (Global)

Use this feature to disable the Active State Power Management (ASPM) support for all PCIe root ports. The options are Disable and Auto.

PCIe Max Read Request Size

Use this feature to set the maximum read request size in PCI hierarchy. The options are **Auto**, 128B, 256B, 512B, 1024B, 2048B, and 4096B.

Equalization Bypass To Highest Rate

Set this feature to Enable to reduce the link training time for PCIe 5.0 device by skipping equalization of intermediate data rates. The options are Disable and **Enable**.

IIO eDPC Support (Available when your system supports this feature)

Use this feature to configure the setting for IIO Enhanced Downstream Port Containment (eDPC) support for your system in an effort to improve the error containment capacity within the PCIe subsystem when an uncorrected error is detected either at the root port or at the switch downstream port. Select Disable to disable IIO eDPC support. Select On Fatal Error to enable IIO eDPC support in your system when a fatal error occurs. Select On Fatal and Non-Fatal Error to enable IIO eDPC support when an error, fatal or non-fatal, has occurred. The options are **Disable**, On Fatal Error, and On Fatal and Non-Fatal Errors.

IIO eDPC Interrupt (Available when your system supports this feature and when "IIO eDPC Support" is set to On Fatal Error or "On Fatal and Non-Fatal Errors")

Select Enable to enable IIO eDPC Interrupt support. The options are **Enable** and Disable.

IIO eDPC ERR_COR Message (Available when your system supports this feature and when "IIO eDPC Support" is set to On Fatal Error or "On Fatal and Non-Fatal Errors")

If this feature is set to Enable, an IIO eDPC error correction message will be displayed. The options are **Enable** and Disable.

CXL Security Level

By defining security protocols, CXL standards provide protection against the data security threats. Use this feature to set the CXL security level for data transiting the CXL link. The options are Fully Trusted, Partially Trusted, Untrusted, and **Auto**.

- Fully Trusted: This option allows the CXL device to access CXL.$ for both host attached and device-attached memory ranges in the write-back (WB) address space.
- Partially Trusted: This option allows the CXL device to access CXL.$ for device attached memory ranges only.
- Untrusted: If this option is selected, the host (your system) will abort all requests on CXL.$.
- Auto: This option is based on Si Compatibility.

CXL Header Bypass

Set this feature to enable or disable the CXL header bypass. The options are Disable and Enable.

▶South Bridge

The following information is displayed:

- 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 Disabled 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 Extensible Host Controller Interface (XHCI) hand-off. The XHCI ownership change should be claimed by the XHCI driver. The options are **Enabled** and Disabled.

Port 60/64 Emulation

Select Enabled for I/O port 60h/64h emulation support, which in turn, provides complete legacy USB keyboard support for the operating systems that do not support legacy USB devices. The options are **Disabled** and Enabled.

PCIe PLL SSC

Select Enabled for PCH PCIe Spread Spectrum Clocking (SSC) support, which allows the BIOS to monitor and attempt to reduce the level of electromagnetic interference caused by the components whenever needed. The options are **Disabled** and Enabled.

▶Server ME Information

The following information is displayed:

- General ME Configuration
- Oper. Firmware Version
  - Current State
  - Error Code

▶PCH SATA0 Configuration / ▶PCH SATA1 Configuration / ▶PCH SATA2 Configuration

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

SATA Controller(s)

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

SATA Mode Selection (Available when "SATA Controller" is set to Enabled)

Use this feature to select the mode of installed SATA drives. The options are **AHCI** and RAID.

Note 1: The RAID option is unavailable when "Boot Mode Select" is set to Legacy.

Note 2: Refer to Boot submenu in the UEFI BIOS Setup main menu to set "Boot Mode Select."

Support Aggressive Link Power Management (Available when "SATA Controller" is set to Enabled)

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

SATA SGPIO Mode

Use this feature to enable serial GPIO for the SATA controller to ensure which storage driver can monitor and auxiliary service in a drive enclosure. This feature is only valid in AHCI/RAID mode. When you select SGPIO, it supports multiple-activity LEDs to show the per drive status information from the Front Panel. When you select LED, the SGPIO signals are off to deliver the LED messages from the Front Panel. The options are LED and **SGPIO**.

Note: The signals are not related to SATALED.

SATA Port 0 - SATA Port 7 (Available when "SATA Controller" is set to Enabled)

Hot Plug

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

Spin Up Device

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

SATA Device Type

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

▶Super IO Configuration

The following Super IO information is displayed:

- Super IO Chip AST2600

▶Serial Port 1 Configuration

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

Serial Port 1

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

Device Settings

This feature displays the base I/O port address and the Interrupt Request address of serial port 1.

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

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

Serial Port 2

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

Device Settings

This feature displays the status of a 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=2F8h; IRQ=3;), (IO=3F8h; 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 serial port 2 as a Serial Over LAN (SOL) port for console redirection. The options are **SOL** and COM.

▶Serial Port Console Redirection

COM1

Console Redirection

Select Enabled to enable the COM port for Console Redirection, which will allow a client machine to be connected to a host machine at a remote site for networking. The options are **Disabled** and Enabled.

SOL/COM2

Console Redirection

Select Enabled to enable the COM or SOL port for Console Redirection, which will allow a client machine to be connected to a host machine at a remote site for networking. The options are Disabled and **Enabled**.

▶Console Redirection Settings (Available when "Console Redirection" is set to Enabled)

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

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.

▶Legacy Console Redirection Settings

Legacy Redirection COM Port

Use this feature to select a COM port to display redirection of Legacy OS and Legacy OPROM messages. The options are **COM1** and SOL. Note that the options displayed are based on your motherboard.

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**.

Redirection After POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When BootLoader is selected, legacy console redirection is disabled before booting the OS. When Always Enable is selected, legacy console redirection remains enabled upon OS bootup. The options are **Always Enable** and BootLoader.

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

The feature allows you to configure Console Redirection settings to support Out-of-Band Serial Port management.

Console Redirection EMS

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

▶Console Redirection Settings (Available when "Console Redirection EMS" above is set to Enabled)

Out-of-Band Mgmt Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2. Note that the SOL option is unavailable if there is no BMC support.

Terminal Type EMS

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII character set. Select VT100Plus to add color and function key support. Select ANSI to use the extended ASCII character set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, **VT-UTF8**, and, ANSI.

Bits Per Second EMS

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

Flow Control EMS

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

The following information is displayed:

- Data Bits EMS
- Parity EMS
- Stop Bits EMS

▶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 (Available when "Network Stack" is set to Enabled)

Select Enabled to enable IPv4 PXE boot support. If this feature is disabled, it will not create the IPv4 PXE boot option. The options are Disabled and **Enabled**.

IPv4 HTTP Support (Available when "Network Stack" is set to Enabled)

Select Enabled to enable IPv4 HTTP boot support. If this feature is disabled, it will not create the IPv4 HTTP boot option. The options are **Disabled** and Enabled.

IPv6 PXE Support (Available when "Network Stack" is set to Enabled)

Select Enabled to enable IPv6 PXE boot support. If this feature is disabled, it will not create the IPv6 PXE boot option. The options are **Disabled** and Enabled.

IPv6 HTTP Support (Available when "Network Stack" is set to Enabled)

Select Enabled to enable IPv6 HTTP boot support. If this feature is disabled, it will not create the IPv6 HTTP boot option. The options are **Disabled** and Enabled.

PXE Boot Wait Time (Available when "Network Stack" is set to Enabled)

Use this feature to set the wait time (in seconds) that the system BIOS will wait for you to press the <ESC> key to abort PXE boot instead of proceeding with PXE boot by connecting to a network server immediately. Press <+> or <-> on your keyboard to change the value. The default setting is **0**.

Media Detect Count

Use this feature to select the wait time (in seconds) for the BIOS ROM to detect the presence of a LAN media either via the Internet connection or via a LAN port. Press <+> or <-> on your keyboard to change the value. The default setting is **1**.

▶MAC:XX:XX:XX:XX:XX:XX-IPv6 Network Configuration

▶Enter Configuration Menu

The following information is displayed:

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

Interface ID

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

DAD Transmit Count

This feature displays the number of consecutive neighbor solicitation messages to be sent while performing duplicate address detection on a tentative address. When this feature is set to 0, duplicate address detection will not be performed. The default setting is **1**.

Policy

Use this feature to select how the policy is to be configured. The options are **automatic** and manual.

▶Advanced Configuration (Available when "Policy" is set to manual)

New IPv6 address

Use this feature to enter the IPv6 address for the local machine.

New Gateway address

Use this feature to set the gateway address for the local machine.

New DNS address

Use this feature to set the DNS server address for the local machine.

Commit Changes and Exit

Press <Enter> to save changes and exit.

Discard Changes and Exit

Press <Enter> to discard changes and exit.

Save Changes and Exit

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

▶MAC:XX:XX:XX:XX:XX:XX-IPv4 Network Configuration

Configured

Select Enabled to show whether the network address has been successfully configured. The options are **Disabled** and Enabled.

Enable DHCP (Available when "Configured" is set to Enabled)

Select Enabled to support Dynamic Host Configuration Protocol (DHCP) which allows the BIOS to search for a DHCP server attached to the network and request the next available IP address for this computer. The options are **Disabled** and Enabled.

Local IP Address (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to enter an IP address for the local machine.

Local NetMask (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to set the netmask for the local machine.

Local Gateway (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to set the gateway address for the local machine.

Local DNS Servers (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to set the Domain Name System (DNS) server address for the local machine.

Save Changes and Exit

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

▶PCIe/PCI/PnP Configuration

The following information is displayed:

- PCI Bus Driver Version

PCI Devices Common Settings:

Above 4G Decoding (Available when 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**.

Re-Size BAR Support

Use this feature to enable the Resizable BAR support. Resizable BAR is a PCIe interface technology that allows the CPU to access to the entire frame buffer. With this technology, your system will be able to handle multiple CPU to GPU transfers simultaneously rather than queuing, which can improve the frame rate performance. The options are **Disabled** and Enabled.

MMCFG Base

This feature determines how the lowest Memory Mapped Configuration (MMCFG) base is assigned to onboard PCI devices. The options are 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, and **Auto**.

MMCFG Size

Use this feature to set the MMCFG size. The options are 64M, 128M, 256M, 512M, 1G, 2G, and **Auto**. Note that the MMCFG size is based on the memory populated.

Note: The options shown here depend on your memory size.

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.

SR-IOV Support

Select Enabled for Single-Root IO Virtualization support. The options are Disabled and **Enabled**.

ARI Support

Use this feature to enable or disable Alternate Routing-ID Interpretation (ARI) support. The options are Disabled and **Enabled**.

Bus Master Enable

If this setting is set to Enabled, the PCI Bus Driver will enable the Bus Master Attribute for DMA transactions. If this setting is set to Disabled, the PCI Bus Driver will disable the Bus Master Attribute for Pre-Boot DMA protection. The options are Disabled and **Enabled**.

Consistent Device Name Support

Select Enabled to ACPI_DSM (DSM: Device Specific Method) device name support for onboard devices and slots. The options are **Disabled** and Enabled.

NVMe Firmware Source

Use this feature to select the NVMe firmware to support booting. The options are **Vendor Defined Firmware** and AMI Native Support. The default option, Vendor Defined Firmware, is pre-installed on the drive and may resolve errata or enable innovative functions for the drive. The other option, AMI Native Support, is offered by the BIOS with a generic method.

VGA Priority

Use this feature to select the graphics device to be used as the primary video display for system boot. The options are **Onboard** and Offboard.

For the following features, note that:

Note 1: The number of slots and slot naming vary based on your motherboard.

Note 2: The Legacy option is available when "Boot Mode Select" is set to Dual or Legacy.

Note 3: Refer to Boot submenu in BIOS Setup main menu to set "Boot Mode Select."

Onboard Video Option ROM

Select EFI to allow you to boot the computer using the Extensible Firmware Interface (EFI) device installed on the onboard video port. The options are Disabled, **EFI**, and Legacy.

AOM / M.C-C1 / M.2-C2

Select EFI to allow you to boot the computer using the EFI device installed on the PCIe slot specified. The options are Disabled, Legacy, and **EFI**.

Onboard LAN1 Option ROM

Use this feature to select the type of device installed in LAN1 used for system boot. The options are Disabled, Legacy, and **EFI**.

Onboard LAN2 Option ROM

Use this feature to select the type of device installed in LAN2 used for system boot. The options are **Disabled**, Legacy, and EFI.

▶ACPI Settings

NUMA

Use this feature to enable Non-Uniform Memory Access (NUMA) to enhance system performance. The options are Disabled and **Enabled**.

UMA-Based Clustering

When this feature is set to Hemisphere, Uniform Memory Access (UMA)-based clustering will support 2-cluster configuration for system performance enhancement. The options are Disabled (All2All), Hemisphere (2-clusters), and **Quadrant (4-clusters)**.

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 HPET is used to replace the 8254 Programmable Interval Timer. The options are Disabled and **Enabled**.

▶Trusted Computing

When a Trusted-Platform Module (TPM) device is detected in your machine, the following information will display:

- TPM 2.0 Device Found
- Firmware Version:
- Vendor:

Security Device Support

Select Enable to enable BIOS support for onboard security devices, which are not displayed in the OS. If this feature is set to Enable, TCG EFI protocol and INT1A interface will not be available. The options are Disable and **Enable**.

- Active PCR banks (Available when "Security Device Support" is set to Enable)
- Available PCR banks (Available when "Security Device Support" is set to Enable)

SHA256 PCR Bank (Available when "Security Device Support" is set to Enable)

Select Enabled to enable SHA256 PCR Bank support to enhance system integrity and data security. The options are **Enabled** and Disabled.

Pending Operation (Available when "Security Device Support" is set to Enable)

Use this feature to schedule a TPM-related operation to be performed by a security (TPM) device at the next system boot to enhance system data integrity. Your system will reboot to carry out a pending TPM operation. The options are **None** and TPM Clear.

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

Platform Hierarchy (Available when "Security Device Support" is set to Enable)

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

Storage Hierarchy (Available when "Security Device Support" is set to Enable)

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

Endorsement Hierarchy (Available when "Security Device Support" is set to Enable)

Select Enabled for Endorsement Hierarchy support, which contains separate controls to address privacy concerns because the primary keys in the hierarchy are certified by the TPM key or by a manufacturer with restrictions on how an authentic TPM device that is attached to an authentic platform can be accessed and used. A primary key can be encrypted and certified with a certificate created by using TPM2_ActivateCredential, which allows you to independently enable "flag, policy, and authorization values" without involving other hierarchies. A user with privacy concerns can disable the endorsement hierarchy while still using the storage hierarchy for TPM applications, permitting the platform software to use the TPM. The options are Disabled and **Enabled**.

PH Randomization

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

Supermicro BIOS-Based TPM Provision Support

If this feature is set to Enabled, Supermicro BIOS-based TPM provision will be supported. The options are **Disabled** and Enabled.

Note: Enabling this feature will lock your TPM on the production platform, and you will not be able to delete the NV indexes.

TXT Support

Select Enabled to enable Intel Trusted Execution Technology (TXT) support to enhance system integrity and data security. The options are **Disabled** and Enabled.

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

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

▶Supermicro KMS Server Configuration

Supermicro KMS Server IP address

Use this feature to enter the Supermicro Key Management Service (KMS) server IPv4 address in dotted-decimal notation.

Second Supermicro KMS Server IP address

Use this feature to enter the second Supermicro KMS server IPv4 address in dotted-decimal notation.

Supermicro KMS TCP Port number

Use this feature to enter the Supermicro KMS TCP port number. The valid range is 100–9999. The default setting is **5696**. Do not change the default setting unless a different TCP port number was specified and used in the Supermicro KMS Server.

KMS Time Out

Use this feature to enter the KMS server connecting time-out in seconds. The default setting is **5** seconds.

TimeZone

Use this feature to enter the correct time zone. The default setting is **0** (not specified).

Client UserName

Press <Enter> to set the client identity (UserName). The maximum length is 63 characters.

Client Password

Press <Enter> to set the client identity (Password). The maximum length is 31 characters.

KMS TLS Certificate | Size

Use the "CA Certificate," "Client Certificate," and "Client Private Key" features to enroll factory defaults or load the KMS Transport Layer Security (TLS) certificates, which are generated by the KMS Server, from a file stored in a USB flash drive.

▶CA Certificate

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

▶Client Certificate

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

▶Client Private Key

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

Private Key Password (Available when "Client Private Key" has been set)

Use this feature to change the private key password.

▶Super-Guardians Configuration

Super Guardians is a unified security solution to facilitate KMS, TPM, or USB-based authentication controls for Supermicro X13 motherboards. Use this submenu to configure the authentication policy, method, and KMS server settings.

Super-Guardians Protection Policy

Use this feature to enable the Super-Guardians Protection Policy. The options are **Storage**, System, and "System and Storage." Set this feature to Storage to protect and have secure access to Trusted Computing Group (TCG) NVMe devices with the Authentication-Key (AK). Set this feature to System to protect and have secure access to your system/motherboard with the AK. Set this feature to "System and Storage" to protect and have secure access to your TCG NVMe devices/system/motherboard with the AK.

KMS Security Policy

Set this feature to Enabled to enable the Key Management Service (KMS) Security Policy. When this feature has not previously been set to Enabled, the options are **Disabled** and Enabled. Changes take effect after you save settings and reboot the system.

Note 1: Be sure that the KMS server is ready before configuring this feature.

Note 2: Use the professional KMS server solutions (e.g., Thales Server) or the Supermicro PyKMIP Software Package to establish the KMS server.

When this feature has previously been set to Enabled, the options are **Enabled**, Reset, and Key Rotation. Set this feature to Key Rotation to obtain an existing Authentication-Key from the KMS server and create a new Authentication-Key. To disable the KMS Security Policy, set this feature to Reset. When this feature is set to reset, the system and TCG NVMe devices chosen in "Super-Guardians Protection Policy" will be in the unprotected mode.

KMS Server Retry Count

Use this feature to specify how many times the system will attempt reconnecting to the KMS server. Press <+> or <-> on your keyboard to change the value. The default setting is **5**. If the value is 0, the system will retry infinitely. The valid range is 0 to 10.

TPM Security Policy

Use this feature to enable or disable the TPM Security Policy. When this feature has not previously been set to Enabled, the options are **Disabled** and Enabled. Changes take effect after you save settings and reboot the system.

Note: Install a Trusted Platform Module 2.0 device to your system before configuring this feature.

When this feature has previously been set to Enabled, the options are **Enabled** and Reset. To disable the TPM Security Policy, set this feature to Reset. When this feature is set to reset, the system and TCG NVMe devices chosen in "Super-Guardians Protection Policy" will be in the unprotected mode.

Load Authentication-Key

Use this feature to toggle whether the BIOS should automatically load an Authentication-Key named TPMAuth.bin from a USB flash drive. The options are **Disabled** and Enabled. Set this feature to Enabled to load the Authentication-Key. After an Authentication Key is loaded, this option will be reset to Disabled. Changes take effect after you save settings and reboot the system.

Note 1: Connect a USB flash drive with the Authentication-Key (TPMAuth.bin) to your system before configuring this feature.

Note 2: Load the Authentication-Key after installing a TPM device. The TPM function will not work properly without an Authentication-Key.

Save Authentication-Key

Use this feature to toggle whether the BIOS should automatically save an Authentication-Key with the name TPMAuth.bin to a USB flash drive. The options are **Disabled** and Enabled. After an Authentication Key is saved, this option will be reset to Disabled. Changes take effect after you save settings and reboot the system.

Note 1: Connect a USB flash drive to your system before configuring this feature. Save the Authentication-Key and keep a backup.

Note 2: Load the Authentication-Key after installing a TPM device. The TPM function will not work properly without an Authentication-Key.

USB Security Policy

Use this feature to configure USB Security Policy settings. When this feature has not previously been set to Enabled, this feature will toggle whether the BIOS should automatically save a USB Authentication-Key named "USBAuth.bin" to a USB flash drive and begin the USB Security Policy. The options are **Disabled** and Enabled. Changes take effect after you save settings and reboot the system.

Note: Connect a USB flash drive to your system before configuring this feature. Save the USB Authentication-Key and keep a backup.

When this feature has been previously set to Enabled, the options are **Enabled** and Reset. To disable the USB Security Policy, set this feature to Reset. When this feature is set to reset, the system and TCG NVMe devices chosen in "Super-Guardians Protection Policy" will be in the unprotected mode.

▶HTTP Boot Configuration

HTTP Boot Policy

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

HTTPS Boot Checks Hostname

Use this feature to allow HTTPS Boot to check if the hostname of the TLS certificate matches the hostname provided by the remote server. Selecting Disabled is a violation of RFC6125. The options are **Enabled** and Disabled (WARNING: Security Risk!!).

Priority of HTTP Boot

Instance of Priority 1

This feature sets the rank target port. The default setting is **1**.

Select IPv4 or IPv6

This feature specifies which connection the target LAN port should boot from. The options are **IPv4** and IPv6.

Boot Description

Use this feature to enter a boot description. The boot description cannot be longer than 75 characters. Be sure to enter a boot description, otherwise the boot option for the URI cannot be created.

Boot URI

Enter a Boot Uniform Research Identifier (URI). The boot URI cannot be longer than 128 characters. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created. This feature is only supported on Dual or EFI Boot Mode.

▶Intel(R) Ethernet Controller E810-XXV for backplane - XX:XX:XX:XX:XX:XX

Note 1: This feature is available when "Onboard LAN Option ROM Type" is set to EFI.

Note 2: The Ethernet controller and MAC addresses shown above are based on you system.

▶Firmware Image Properties

The following information is displayed:

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

▶NIC Configuration

Link Speed

Use this feature to specify a port speed for the selected boot protocol. The default option is **Auto Negotiated**.

Wake On LAN

If this feature is set to Enabled, the LAN port will be enabled when the system is powered on. The options are Disabled and **Enabled**.

LLDP Agent

Select Enabled to persistently enable the Linked Layer Discovery Protocol Agent. The options are **Disabled** and Enabled.

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. The default setting is **0** (up to 15 seconds).

The following information is displayed:

- UEFI Driver
- Adapter PBA
- Device Name
- Chip Type
- PCI Device ID
- PCI Address
- Link Status
- MAC Address
- Virtual MAC Address

▶TLS Authenticate Configuration

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

▶Server CA Configuration

This feature allows you to configure the client certificate that is to be used by the server.

▶Enroll Certification

This feature allows you to enroll the certificate in the system.

▶Enroll Certification Using File

This feature allows you to enroll the security certificate in the system by using a file.

Certification GUID

Press <Enter> and input the certification Global Unique Identifier (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

This feature is used to delete the certificate if a certificate has been enrolled in the system. The options are **Disabled** and Enabled.

▶Client Certification Configuration

This feature allows you to configure the client certificate to be used by the server.

▶Enroll Certification

This feature allows you to enroll the certificate in the system.

▶Enroll Certification Using File

This feature allows you to enroll the security certificate in the system by using a file.

Certification GUID

Press <Enter> and input the certification Global Unique Identifier (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

This feature is used to delete the certificate if a certificate has been enrolled in the system.

▶Supermicro PMem Configuration (Available when any PMem device is detected by the BIOS)

▶Supermicro PMem Information

Note: The information provided in the following section is for illustration only. The number of PMem DIMMs displayed depends on the number of PMem populated in the system.

The following information is displayed:

- PMem UEFI Drive Version
- All Initialized DIMMs:
- Total Initialized INTEL PMem Count
- All DIMMs Security State
- DIMM [1] Handle
- DIMM [1] DimmID
- DIMM [1] Health State
- DIMM [1] Security State
- DIMM [1] Master PassEn
- DIMM [1] UID
- DIMM [1] Serial Number
- DIMM [1] FW Version
- DIMM [1] Capacity
- DIMM [1] APP Direct Capacity
- DIMM [1] UnConfigured Capacity
- DIMM [1] Reserved Capacity
- DIMM [1] InAccessible Capacity
- Total INTEL PMem REGIONS Count

▶Supermicro PMem Settings

Create Goal Config:: Persistent Memory Type

Use this feature to set the preferred PMem type. The options are **Do Nothing**, App Direct, App Direct Not Interleaved, and Back to Memory Mode.

- If this feature is set to App Direct, the memory can be byte-addressable. Also, applications can directly access the memory (non-volatile access).
- If this feature is set to App Direct Not Interleaved, each Pmem is seen as a separate logic storage device (non-volatile access)
- If this feature is set to Back to Memory Mode, PMem can be used as the volatile system memory. Meanwhile, the DRAM is used as a cache for data access.

Reversed [%]

This feature reverses a percentage of the PMem capacity for a particular purpose and keeps this portion of memory space from being mapped into the physical address of the system for system use. The default setting is **0**.

All PMem DIMMs have same security state! (This information is displayed based on PMem modules detected by the system)

User Security Policy

Use this feature to set the User Security Policy. The options are **Do Nothing**, Set User PassPhrase, and User Secure Erase DIMMs.

User DIMMs Current PassPhrase

User DIMMs New PassPhrase

All PMem DIMMs Master Security Policy

Master Security Policy

Use this feature to set the User Master Policy. The options are **Do Nothing** and Enable Master Secure Policy.

All PMem DIMMs FW Settings

Updated PMem DIMMs FW version:

The updated PMem DIMMs firmware (FW) version is displayed.

Update PMem DIMMs FW from BIOS

Select Enabled to update PMem DIMM Firmware from the BIOS. The options are **Disabled** and Enabled.

▶Intel(R) Optane(TM) Persistent Memory Configuration (Available when any PMem device is detected by the BIOS)

The following information is displayed:

- Version: This feature displays the version of PMem used in the system.
- Detected PMem modules: This feature displays the number of PMem modules detected by the system.

Note: The following sections, which describe the status of PMem modules, are for illustration only. The number and status of PMem modules displayed on your UEFI BIOS screen will vary depending on the PMem modules connected to the system.

▶PMem Modules

This feature allows you to view information for PMem modules installed in the system. The following information is displayed:

PMem modules on socket:

▶DIMM ID

Note: The Socket ID and DIMM IDs displayed above are based on your system configuration.

Use this feature to view general information for the PMem module with the listed ID.

The following settings are displayed:

- DIMM UID: This feature displays the unique ID of the PMem module.
- DIMM handle: This feature displays the unique handle assigned to the PMem module.
- DIMM physical ID: This feature displays the physical ID of the PMem module.
- Manageability state: This feature displays the manageability state of the PMem module.
- Health state: This feature displays the health state of the PMem module.
- Health state reason: This feature displays the reason for the health state of the PMem module.
- Capacity: This feature displays the capacity of the PMem module.

- Firmware version: This feature displays the firmware version of the PMem module.
- Firmware API version: This feature displays the firmware API version of the PMem module.
- Firmware Active API version: This feature displays the active firmware API version of the PMem module.
- Lock state: This feature displays the lock state of the PMem module.
- SVN downgrade: This feature displays the status of SVN Downgrade of the PMem module.
- Secure erase policy: This feature displays the status of the Secure Erase Policy of the PMem module.
- S3 resume opt-in: This feature displays the status of the S3 Resume Opt-in support of the PMem module.
- Firmware activate opt-in: This feature displays the status of the Firmware Activate Opt-in of the PMem module.
- Staged firmware version: This feature displays the status of the staged firmware version of the PMem module.
- Staged firmware activatable: This feature displays the status of the staged firmware activate support of the PMem module.
- Firmware update status: This feature displays the firmware update status of the PMem module.
- Firmware activation quiesce required: This feature displays whether Firmware Activation Quiesce is required for the PMem module.
- Firmware activation time [ms]: This feature displays the time needed to activate the firmware of the PMem module.
- Manufacturer: This feature displays the manufacturer of the PMem module.
- Show more details

Note: The below PMem information is displayed when "Show more details" is set to Enabled. The settings are **Disabled** and Enabled.

- Serial number

- Part number
- Socket
- Memory controller Id
- Vendor ID
- Device ID
- Subsystem vendor ID
- Subsystem device ID
- Device locator
- Subsystem revision ID
- Interface format code
- Manufacturing info valid
- Manufacturing date
- Manufacturing location
- Memory type
- Memory bank label
- Data width label [b]
- Total width [b]
- Speed [MT/s]
- Channel ID
- Channel position
- Revision ID
- Form factor
- Manufacturer ID

- Controller revision ID
- Is new
- Memory capacity
- App Direct capacity
- Unconfigured capacity
- Inaccessible capacity
- Reserved capacity
- Avg power limit [mW]
- Avg power reporting time constant
- Memory Bandwidth Boost Feature
- Memory Bandwidth Boost Max Power Limit [mW]
- Memory Bandwidth Boost Average Power Time Constant [ms]
- Max average power limit [mW]
- Max Memory Bandwidth Boost Max Power Limit [mW]
- Max Memory Bandwidth Boost Average Power Time Constant [ms]
- Max Memory Bandwidth Boost Average Power Time Constant Step [ms]
- Average Power Reporting Time Constant [ms]
- Average Power Reporting Time Constant Step [ms]
- Package sparing capable
- Package sparing enabled
- Package spares available
- Configuration status
- SKU violation

- Population violation
- ARS status
- Overwrite PMem module status
- Last shutdown time
- Average power reporting time constant [ms]
- Viral policy enable
- Viral state
- Thermal throttle loss %
- Latched Last shutdown status
- Unlatched last shutdown status
- Security capabilities
- Modes supported
- Boot status
- AIT DRAM enabled
- Error injection enabled
- Max Controller temperature [C]
- Software triggers enabled
- Software triggers enabled details
- Poison error injections counter
- Poison error clear counter
- Media temperature injections counter
- Software triggers counter
- Max Media temperature [C]
- Media temperature injection enabled

- Master Passphrase Enabled
- Average Power [mW]
- eADR enabled
- Previous Pwr Cycle eADR enabled
- Latch System Shutdown State
- Previous Power Cycle Latch System
- Shutdown State
- FIPS Mode Status

▶Monitor health

Use this feature to view PMem module health status and alarm thresholds for the selected DIMM. For each sensor on the PMem module, the following information is displayed

- Sensor Type
- Value
- Alarm threshold
- Throttling stop threshold
- Throttling start threshold
- Shutdown threshold
- Max temperature [C]
- Alarm enabled state

Modify alarm thresholds

Use the following features to view or change the default alarm thresholds. These settings are independent of the sensor information displayed above.

Controller temperature [C]

The default setting is **98**.

Media temperature [C]

The default setting is **82**.

Percentage remaining [%]

The default setting is **50**.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Update firmware

Use this feature to enter the firmware update menu for the selected PMem module.

Current firmware version:

This feature displays the current firmware version on the selected PMem module.

Selected firmware version:

This feature displays the firmware version of the file selected with the "File:" feature.

File:

Use this feature to select a firmware image. Press <Enter> and enter a valid file path to load a firmware image.

Staged firmware version:

This feature displayed the staged firmware version.

▶Update

This feature initiates the firmware update process if a valid firmware image is selected.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Configure security

Use this feature to view security settings for the selected PMem module.

Note: Warning! Modifying the settings of a single PMem module may result in an unusable configuration.

State

This feature displays the status of the security feature for this PMem module.

Enable security

Use this feature to enable security. A new password will be requested when this feature is entered.

Secure erase with user password

Use this feature to secure erase the selected PMem module.

Freeze lock

Use this feature to freeze lock the selected PMem module.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Configure data policy

Use this feature to view or specify the data policy settings of the selected PMem module.

Average power reporting time constant [ms]

This feature displays the average power reporting time constant.

Freeze lock

Use this feature to modify the average power reporting time constant. The value must be a multiple of 100.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Monitor health

Use this feature to view PMem module alarm thresholds and alarm threshold status for all DIMMs. For each sensor on the PMem modules, the following information is displayed:

- Controller temperature status
- Media temperature status
- Percent remaining

Modify alarm thresholds

Use the following features to view or change the default alarm thresholds. These settings are independent of the sensor information displayed above.

Controller temperature [C]

The default setting is 98.

Media temperature [C]

The default setting is 82.

Percentage remaining [%]

The default setting is 50.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Update firmware

Use this feature to enter the firmware update menu for all PMem modules.

Current firmware version:

This feature displays the current firmware version for all PMem modules.

Selected firmware version:

This feature displays the firmware version of the file selected with the "File:" feature.

File:

Use this feature to select a firmware image. Press <Enter> and enter a valid file path to load a firmware image.

Staged firmware version:

This feature displayed the staged firmware version.

▶Update

This feature initiates the firmware update process if a valid firmware image is selected.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Configure security

Use this feature to view security settings for all PMem modules.

State

This feature displays the status of the security feature for all modules.

Change master password

Use this feature to change master password. The current password will be requested when this feature is entered. The default password is two double quotation marks: **""**.

Secure erase with user password

Use this feature to secure erase all PMem modules.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Configure data policy

Use this feature to view or specify the data policy settings of all PMem modules.

Average power reporting time constant [ms]

This feature displays the average power reporting time constant.

Freeze lock

Use this feature to modify the average power reporting time constant. The value must be a multiple of 100.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Regions

This feature allows you to configure PMem regions. A region is a set of PMem modules. Interleaving PMem across processors is not allowed.

Note: The following information is an example of what may appear when a PMem region exists.

▶Region ID 1

- Region ID
- DIMM ID
- ISet ID
- Persistent memory type
- Capacity
- Free Capacity
- Health
- Socket ID

▶Back to Regions menu

Highlight this feature and press <Enter> to return to the Regions menu.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Provisioning

This feature allows you to configure configuration goals for new regions with the installed PMem modules.

Create goal config for:

Use this feature to select whether the new region should use the PMem modules of the platform, sockets, or partially-configured sockets. The options are **Platform**, Socket, and Partially-configured sockets.

Socket (Available when "Create goal config for:" is set to "Socket" or "Partially-configured sockets")

Use this feature to select if this socket should be used for the new region.

Reversed [%]:

Use this feature to select the percent of the PMem module that should NOT be used in the system physical address space. The default setting is **0.**

Memory Mode [%]

Use this feature to select the percent of the Pmem module that should be used in Memory Mode. The value entered in this feature will be aligned automatically to platform memory alignment requirements. The default setting is **0**.

Persistent memory type:

Use this feature to select if the persistent memory capacity should be interleaved. The options are **App Direct** and App Direct Not Interleaved.

Namespace Label version:

Use this feature to view or change the namespace label version.

▶Create goal config

Use this feature to create a configuration goal for a region determined by the above settings. This feature is disabled when "Create goal config for:" or "Socket" do not have a valid scope.

▶Back to Provisioning menu

Highlight this feature and press <Enter> to return to the Provisioning menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Delete goal config

Use this feature to delete configuration goals.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Namespaces

This feature allows you to create namespaces or view information of existing namespaces.

▶Create namespace

Use this feature to create a namespace. This feature is available only when a valid AppDirect region is available.

Name

Use this feature to enter the name for the namespace.

Region ID

This feature displays the region ID of this namespace.

Mode

Use this feature to set the namespace mode. The options are **None** and Sector. The option of None is for raw access only. Set this feature to Sector to guarantee powerfail write atomicity via a block translation table (BTT) l

Capacity Input

Set this feature to Remaining to use the maximum available capacity. Set this feature to Manual to enter the capacity manually. The options are **Remaining** and Manual.

Units

Use this feature to select how the namespace capacity units should be displayed. The options are B, MB, MiB, GB, **GiB**, TB, and TiB.

Capacity

This feature displays the capacity of the namespace.

▶Create namespace

Use this feature to create a namespace determined by the above settings.

▶Back to Namespaces menu

Highlight this feature and press <Enter> to return to the Namespaces menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

✎ **Note:** The following information is an example of what may appear when a namespace exists.

▶0x00000101 Health

The following information is displayed about the selected namespace:

- UUID
- ID
- Name
- Region
- Health
- Mode
- Block Size
- Units
- Capacity
- Label version

▶Delete

Use this feature to delete the selected namespace. The options are **Yes** and No.

▶Back to Namespace

Highlight this feature and press <Enter> to return to the Namespaces menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Total capacity

This feature allows you to view the memory resource allocation of memory modules on the system.

For each type of memory module, the following capacities are displayed:

- Volatile:
- AppDirect:
- Cache:
- Inaccessible:
- Raw:

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Diagnostics

This feature allows you to view and perform detailed checks of the PMem modules.

Quick diagnostics

Use this feature to toggle if a quick diagnostic test should be performed. The options are **Enabled** and Disabled.

DIMM ID (available when "Quick diagnostics" is set to "Enabled")

Use this feature to toggle which PMem modules should be included in the quick diagnostic test.

Config diagnostics

Use this feature to toggle the platform configuration diagnostics test. The options are **Enabled** and Disabled.

FW diagnostics

Use this feature to toggle the firmware diagnostics test. The options are **Enabled** and Disabled.

Security diagnostics

Use this feature to toggle the security diagnostics test. The options are **Enabled** and Disabled.

▶Execute tests

This feature executes toggled tests. A report is presented when tests are executed.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶Preferences

This feature allows you to view and modify user preferences of the PMem modules.

Default DIMM ID:

Use this feature to select how PMem module identifiers should be displayed. The options are **Handle** and UID.

Capacity units:

Use this feature to select how PMem module capacity units should be displayed. Auto is in units of x1024 and Auto_10 is in units of x1000. The options are **Auto,** Auto_10, B, MB, MiB, GB, GiB, TB, and TiB.

App Direct settings:

Use this feature to view or modify the AppDirect interleaving setting. The default setting is **236B_256B**.

▶Back to main menu

Highlight this feature and press <Enter> to return to the main menu of Intel(R) Optane(TM) Persistent Memory Configuration.

▶VLAN Configuration (MAC:XXXXXXXXXXXX)

▶VLAN Configuration (MAC:XXXXXXXXXXXX)

▶Main Menu

Create new VLAN

VLAN ID

Use this feature to enter a value between 0 and 4094 for the VLAN ID.

Priority

Use this feature to enter a value between 0 and 7 for the VLAN priority.

Add VLAN

Use this feature to create a new VLAN based on the information in "VLAN ID" and "Priority."

Configured VLAN List

This feature displays VLANs that were created with the "Add VLAN" feature.

Remove VLAN

Use this feature to remove selected VLANs from the Configured VLAN List.

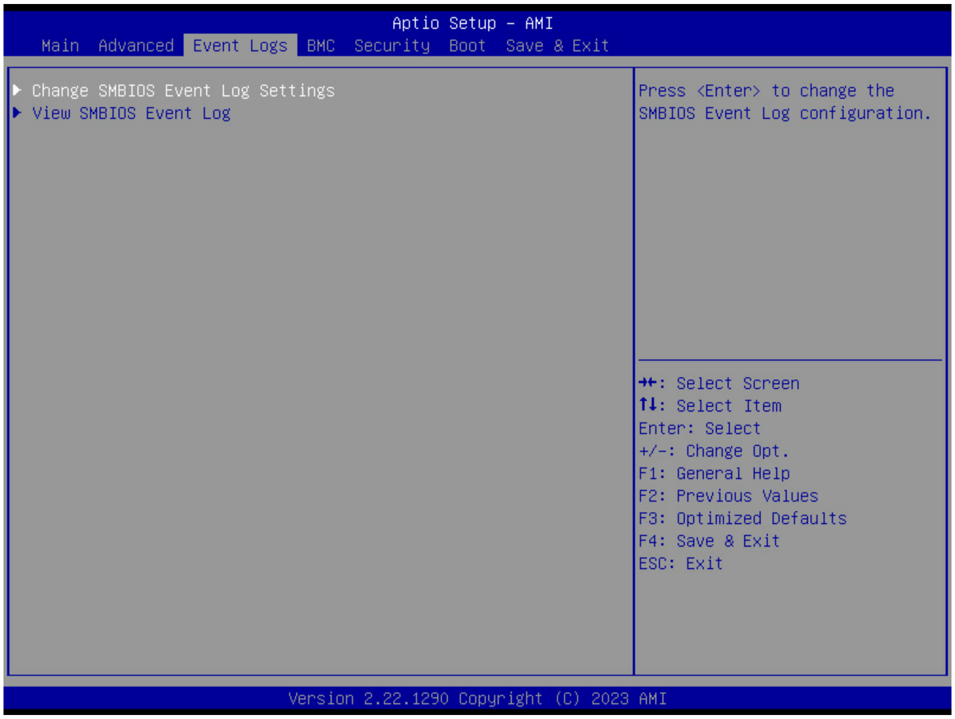
▶Driver Health

This feature displays the health information of the drivers installed in your system, including LAN controllers, as detected by the BIOS. Select one and press <Enter> to see the details.

Note: This section is provided for reference only, for the driver health status will differ depending on the drivers installed in your system. It's also based on your system configuration and the environment that your system is operating in.

4.4 Event Logs

Use this menu to configure Event Log settings.



```
▶ Change SMBIOS Event Log Settings
▶ View SMBIOS Event Log
```

```
Press <Enter> to change the
SMBIOS Event Log configuration.

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

Version 2.22.1290 Copyright (C) 2023 AMI

▶Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

Select Enabled to enable System Management BIOS (SMBIOS) Event Logging during system boot. The options are Disabled and **Enabled**.

Erasing Settings

Erase Event Log (Available when "SMBIOS Event Log" is set to Enabled)

Select No to keep the event log without erasing it upon next system bootup. Select Yes, Next reset to erase the event log upon next system reboot. The options are **No**, (Yes, Next reset), and (Yes, Every reset).

When Log is Full (Available when "SMBIOS Event Log" is set to Enabled)

Select Erase Immediately to immediately erase all errors in the SMBIOS event log when the event log is full. Select Do Nothing for the system to do nothing when the SMBIOS event log is full. The options are **Do Nothing** and Erase Immediately.

SMBIOS Event Log Standard Settings

Log System Boot Event (Available when "SMBIOS Event Log" is set to Enabled)

Select Enabled to log system boot events. The options are Enabled and **Disabled**.

MECI (Available when "SMBIOS Event Log" is set to Enabled)

Use this feature to set the Multiple Event Count Increment (MECI) value for the multiple event counter. Enter a number between 1 to 255. The default setting is **1**.

METW (Available when "SMBIOS Event Log" is set to Enabled)

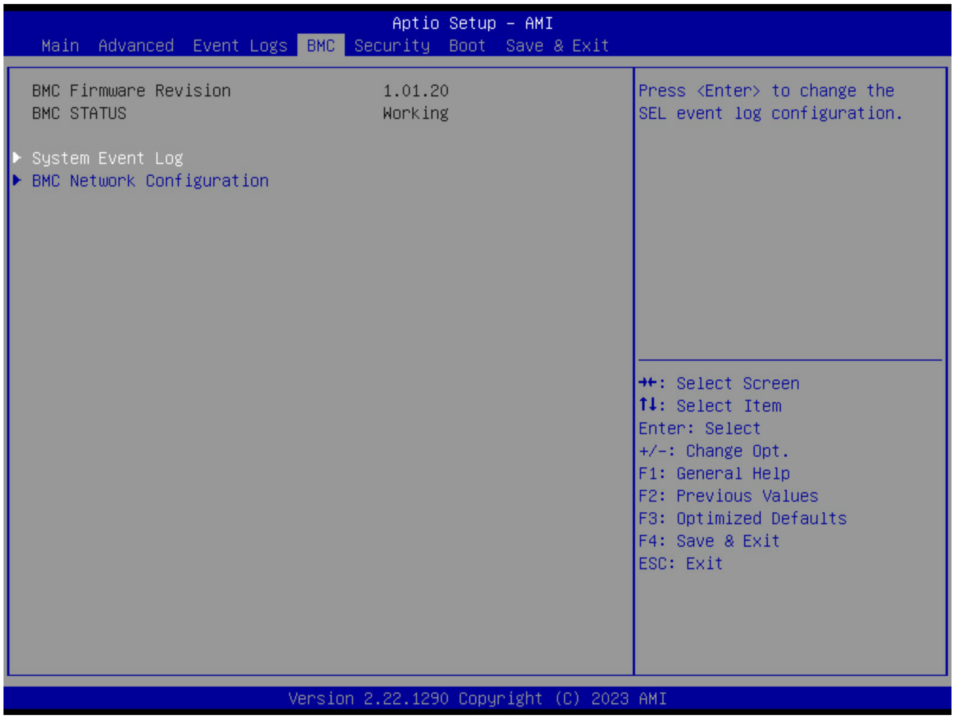
Use this feature to set how long the Multiple Event Count Time Window (METW) should the wait in minutes before generating a new event log. Enter a number between 0 to 99. The default setting is **60**.

▶View SMBIOS Event Log

This feature allows you to view the events in the 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.

4.5 BMC

Use this feature to configure Baseboard Management Console (BMC) settings.



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

  BMC Firmware Revision                 1.01.20         Press <Enter> to change the
  BMC STATUS                            Working         SEL event log configuration.

▶ System Event Log
▶ BMC Network Configuration


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

               Version 2.22.1290 Copyright (C) 2023 AMI
```

BMC Firmware Revision

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

BMC STATUS

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

▶System Event Log

Enabling/Disabling Options

SEL Components

Select Enabled to enable all system event logging upon system boot. The options are Disabled and **Enabled**.

Erasing Settings

Erase SEL

Select (Yes, On next reset) to erase all system event logs upon next system boot. 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 determine 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

Update BMC LAN Configuration

Select Yes for the BIOS to implement all IP/MAC address changes upon next system boot. The options are **No** and Yes.

****

Configure IPv4 Support

****

BMC LAN Selection

Use this feature to select the type of the IPMI LAN. The default setting is **Failover (Auto Mode)**.

BMC Network Link Status:

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

Configuration Address Source (Available when "Update BMC LAN Configuration" is set to Yes)

Use this feature to select the source of the IPv4 connection. If Static is selected, you will need to know the IP address of IPv4 connection and enter it to the system manually in the field. If DHCP is selected, the BIOS will search 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 Static and **DHCP**.

Station IP Address (Available when "Configuration Address Source" is set to Static)

This feature displays the Station IP address in decimal and in dotted quad form (i.e., 172.29.176.131).

Subnet Mask (Available when "Configuration Address Source" is set to Static)

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

Station MAC Address (Available when "Configuration Address Source" is set to Static)

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

Gateway IP Address (Available when "Configuration Address Source" is set to Static)

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1).

VLAN (Available when "Update BMC LAN Configuration" is set to Yes)

This feature displays the status of virtual LAN (VLAN) support. The options are **Disable** and Enable.

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

Use this feature to create a new VLAN ID by using an existing VLAN or creating a new VLAN ID. Enter a valid value between 1–4094. The default setting is 1.

****

Configure IPv6 Support

****

IPv6 Address Status

This feature displays the status of the IPv6 address.

IPv6 Support

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

Configuration Address Source (Available when "IPv6 Support" is set to Enabled)

Use this feature to select the source of the IPv6 connection. If Static Configuration is selected, you will need to know the IP address of IPv6 connection and enter it to the system manually in the field. If the other two options are selected, the BIOS will search for a DHCP server in the network that is attached to and request the next available IP address for this computer. The options are Static Configuration, **DHCPv6 Stateless**, and DHCPv6 Stateful.

IPv6 Address ("Static", "DHCPv6 Stateless", or "DHCPv6 Stateful", depending on the option you selected for "Configuration Address Source" above)

This feature displays the station IPv6 address. Press <Enter> to change the setting.

Prefix Length (Available when "Configuration Address Source" is set to Static Configuration)

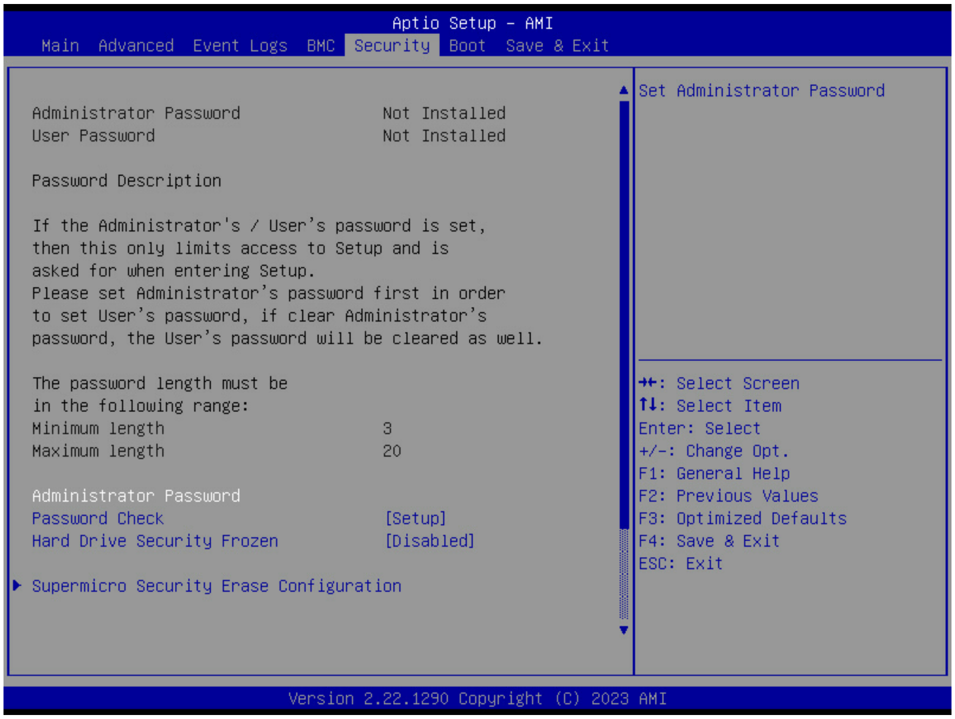
This feature displays the prefix length. Press <Enter> to change the setting.

Gateway IP (Available when "Configuration Address Source" is set to Static Configuration)

Use this feature to enter the IPv6 gateway IP address. Press <Enter> to change the setting.

4.6 Security

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



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

  Administrator Password              Not Installed      Set Administrator Password
  User Password                       Not Installed

  Password Description

  If the Administrator's / User's password is set,
  then this only limits access to Setup and is
  asked for when entering Setup.
  Please set Administrator's password first in order
  to set User's password, if clear Administrator's
  password, the User's password will be cleared as well.

  The password length must be                            →←: Select Screen
  in the following range:                                ↑↓: Select Item
  Minimum length                      3                  Enter: Select
  Maximum length                      20                 +/-: Change Opt.
                                                         F1: General Help
  Administrator Password                                 F2: Previous Values
  Password Check                      [Setup]            F3: Optimized Defaults
  Hard Drive Security Frozen          [Disabled]         F4: Save & Exit
                                                         ESC: Exit
▶ Supermicro Security Erase Configuration

               Version 2.22.1290 Copyright (C) 2023 AMI
```

Administrator Password

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

Password Check

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

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**.

Lockdown mode

Use this feature to switch lockdown mode. The options are **Disabled** and Enabled.

▶Supermicro Security Erase Configuration

This section displays the following information if a storage device is detected by the system:

- HDD Name
- HDD Serial Number
- Security Mode
- Estimated Time
- HDD User Pwd Status

Security Function

Select Password to set an HDD/SATA password, which will allow you to configure the security settings of the HDD/SATA device. Select Security Erase-Password to enter a SATA user password to erase the password and the contents previously stored in the HDD/SATA device. Select Security Erase-Without Password to use the manufacturer default password "111111111" as the SATA user password and to erase the contents of the HDD/SATA device by using this default password. The options are **Disable**, Set Password, Security Erase-Password, Security Erase-PSID, and Security Erase-Without Password.

Note: Security Erase-PSID is only supported by the M.2 TCG function.

Password

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

HDD Security Configuration

This section is available for configuration if a storage device is detected by the system.

HDD Password Description:

Use this feature to set, modify, and clear both HDD User Password and HDD Master Password. An installed HDD User Password is required to enable HDD security features. HDD Master Password can be modified only when successfully unlocked in POST. If the "Set HDD Password" option is grayed out, do a power cycle to enable it.

HDD PASSWORD CONFIGURATION:

Set User Password

Use this option to set up the HDD User Password. Power cycle the system after setting the HDD User Password.

▶Secure Boot

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

- System Mode
- 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**.

CSM Support

Use this feature to enable or disable CSM Support. This feature is for manufacturing debugging purposes. The options are Disabled and **Enabled**.

▶Enter Audit mode

This submenu can only be used if the 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

Provision Factory Defaults

Use this feature to install the factory default secure boot keys after the platform 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

This feature deletes all Secure Boot key databases from NVRAM.

▶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.

▶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.

Secure Boot Variable

▶Platform Key (PK)

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.

▶Key Exchange Key

Update

Select Yes to load the Key Exchange Key (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.

▶Authorized Signatures

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.

▶Forbidden Signatures

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.

▶Authorized TimeStamps

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.

▶OsRecovery Signature

Update

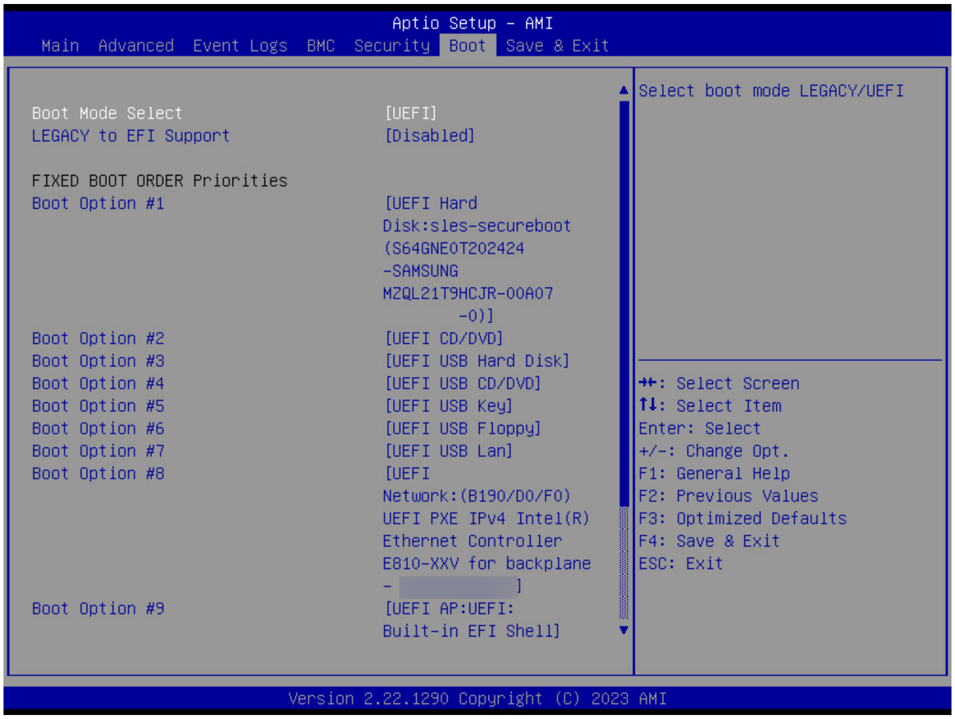
Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file.

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.

4.7 Boot

Use this feature to configure Boot Settings:



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

  Boot Mode Select                      [UEFI]             Select boot mode LEGACY/UEFI
  LEGACY to EFI Support                 [Disabled]

  FIXED BOOT ORDER Priorities
  Boot Option #1                        [UEFI Hard
                                        Disk:sles-secureboot
                                        (S64GNE0T202424
                                        -SAMSUNG
                                        MZQL21T9HCJR-00A07
                                                -0)]
  Boot Option #2                        [UEFI CD/DVD]
  Boot Option #3                        [UEFI USB Hard Disk]
  Boot Option #4                        [UEFI USB CD/DVD]  →←: Select Screen
  Boot Option #5                        [UEFI USB Key]     ↑↓: Select Item
  Boot Option #6                        [UEFI USB Floppy]  Enter: Select
  Boot Option #7                        [UEFI USB Lan]     +/-: Change Opt.
  Boot Option #8                        [UEFI              F1: General Help
                                        Network:(B190/D0/F0) F2: Previous Values
                                        UEFI PXE IPv4 Intel(R) F3: Optimized Defaults
                                        Ethernet Controller F4: Save & Exit
                                        E810-XXV for backplane ESC: Exit
                                        - [redacted]]
  Boot Option #9                        [UEFI AP:UEFI:
                                        Built-in EFI Shell]

                  Version 2.22.1290 Copyright (C) 2023 AMI
```

Setup Prompt Timeout

Use this feature to set timeout (in seconds) for setup activation key. The default setting is 1.

Boot Mode Select

Use this feature to select the type of devices from which the system will boot. The options are Legacy, **UEFI**, and Dual.

Note: When "Boot Mode Select" is set to Dual, all OPROM-related features will be set to Legacy.

Fixed Boot Order Priorities

This feature prioritizes the order of a bootable device from which the system will boot. Press <Enter> on each item sequentially to select devices.

When "Boot Mode Select" is set to **Dual** (default), the following features will be displayed for configuration:

- Boot Option #1 - Boot Option #17

When "Boot Mode Select" is set to Legacy, the following features will be displayed for configuration:

- Boot Option #1 - Boot Option #8

When "Boot Mode Select" is set to UEFI, the following features will be displayed for configuration:

- Boot Option #1 - Boot Option #9

▶Add New Boot Option (Available when any storage device is detected by the BIOS)

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

Add boot option

This feature allows you 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

This feature allows you to specify the file path for the new boot option.

Create

After the name and the file path for the boot option are set, press <Enter> to create the new boot option in the boot priority list.

▶Delete Boot Option

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

Delete Boot Option

This feature allows you to remove an EFI boot option from the boot priority list.

▶UEFI Hard Disk Drive BBS Priorities

This feature allow you to set the system boot order of detected devices.

▶UEFI NETWORK Drive BBS Priorities

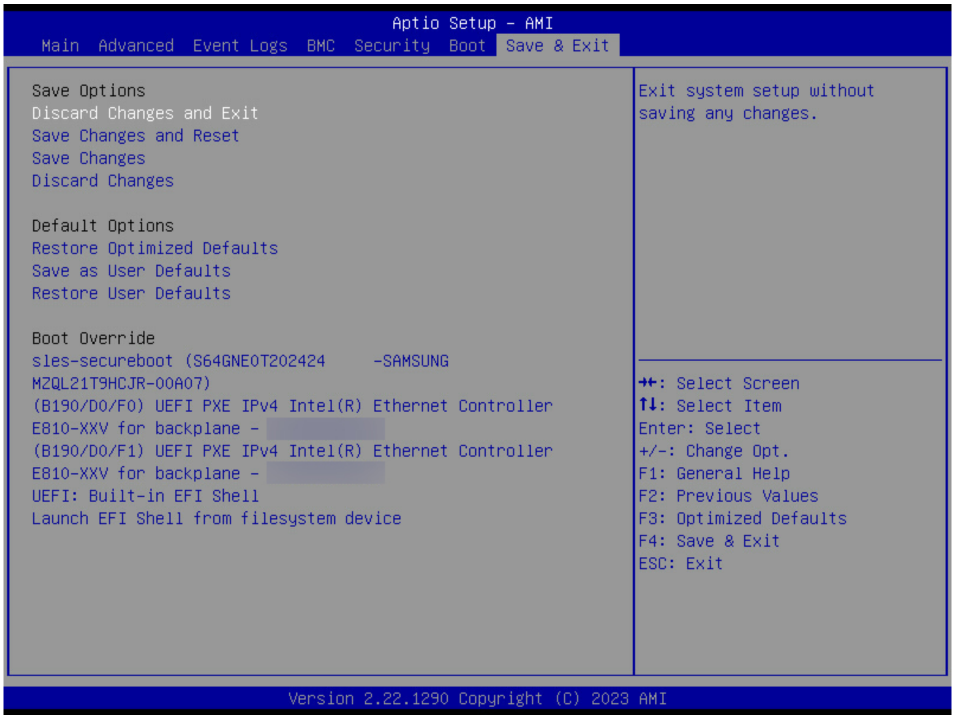
This feature allow you to set the system boot order of detected devices.

▶UEFI Application Boot Priorities

This feature allow you to set the system boot order of detected devices.

4.8 Save & Exit

Select Save & Exit from the BIOS Setup screen to configure the settings below.



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

 Save Options                                      Exit system setup without
 Discard Changes and Exit                          saving any changes.
 Save Changes and Reset
 Save Changes
 Discard Changes

 Default Options
 Restore Optimized Defaults
 Save as User Defaults
 Restore User Defaults

 Boot Override
 sles-secureboot (S64GNE0T202424     -SAMSUNG
 MZQL21T9HCJR-00A07)                               ++: Select Screen
 (B190/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller   ↑↓: Select Item
 E810-XXV for backplane - [redacted]               Enter: Select
 (B190/D0/F1) UEFI PXE IPv4 Intel(R) Ethernet Controller   +/-: Change Opt.
 E810-XXV for backplane - [redacted]               F1: General Help
 UEFI: Built-in EFI Shell                          F2: Previous Values
 Launch EFI Shell from filesystem device           F3: Optimized Defaults
                                                   F4: Save & Exit
                                                   ESC: Exit

             Version 2.22.1290 Copyright (C) 2023 AMI
```

Save Options

Discard Changes and Exit

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

Save Changes and Reset

When you have completed the system configuration changes, use this feature to leave the BIOS Setup utility and reboot the computer for the new system configuration parameters to become effective.

Save Changes

When you have completed the system configuration changes, use this feature to save all changes you've made. This will not reset (reboot) the system.

Discard Changes

Select this feature and press <Enter> to discard all the changes you've made and return to the BIOS Setup utility.

Default Options

Restore Optimized Defaults

Select this feature and press <Enter> to load manufacturer optimized default settings which are intended for maximum system performance but not for maximum stability.

Save as User Defaults

Select this feature and press <Enter> to save all changes on the default values specified to the BIOS Setup utility for future use.

Restore User Defaults

Select this feature and press <Enter> to retrieve user-defined default settings that have been saved previously.

Boot Override

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

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 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

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").

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

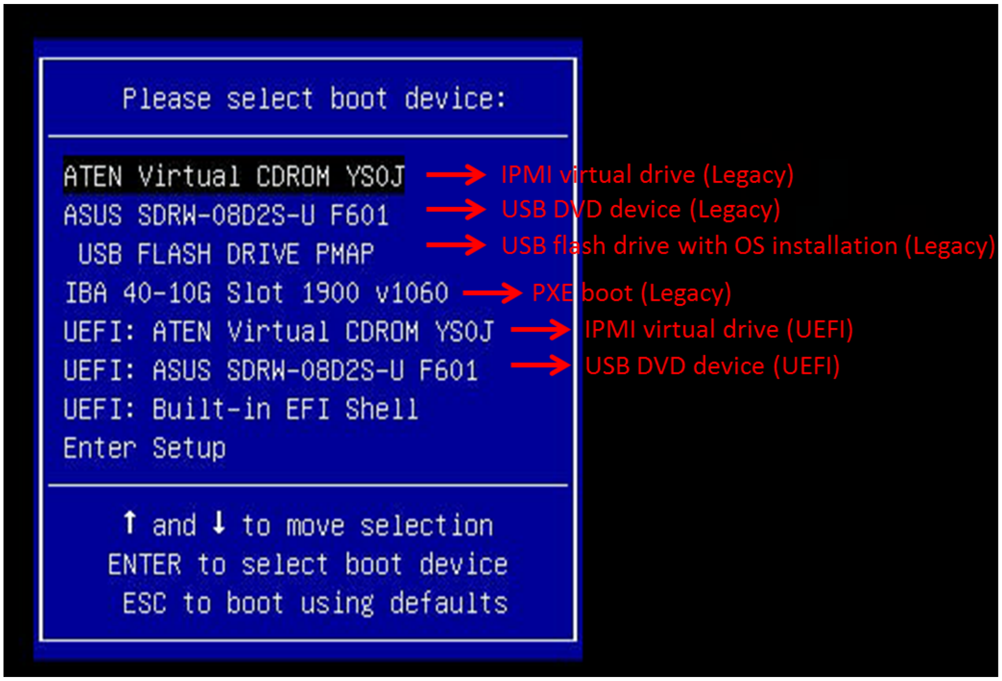
If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at www.supermicro.com/support/manuals.

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That might be a USB flash or media drive.

2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.

3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing <F11> during the system startup.

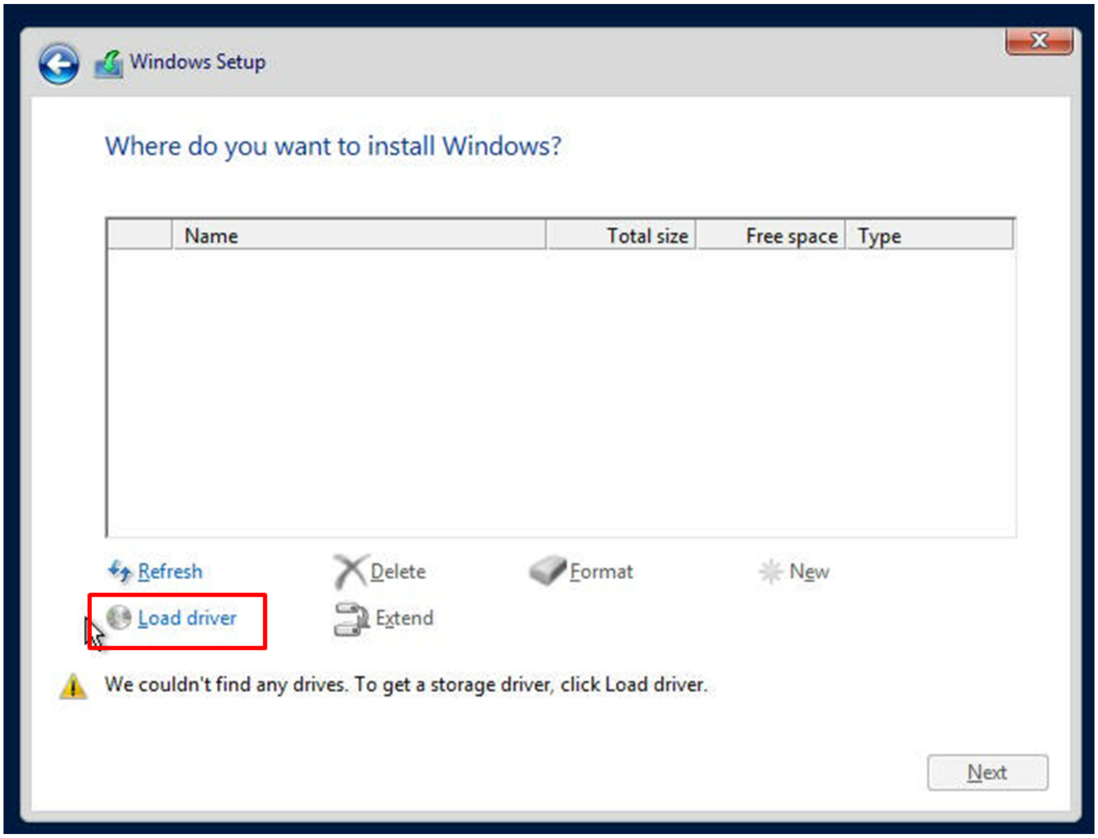


```
   Please select boot device:

ATEN Virtual CDROM YSOJ
ASUS SDRW-08D2S-U F601
 USB FLASH DRIVE PMAP
IBA 40-10G Slot 1900 v1060
UEFI: ATEN Virtual CDROM YSOJ
UEFI: ASUS SDRW-08D2S-U F601
UEFI: Built-in EFI Shell
Enter Setup

   ↑ and ↓ to move selection
  ENTER to select boot device
   ESC to boot using defaults
```

IPMI virtual drive (Legacy)
USB DVD device (Legacy)
USB flash drive with OS installation (Legacy)
PXE boot (Legacy)
IPMI virtual drive (UEFI)
USB DVD device (UEFI)

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.



We couldn't find any drives. To get a storage driver, click Load driver.

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 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.

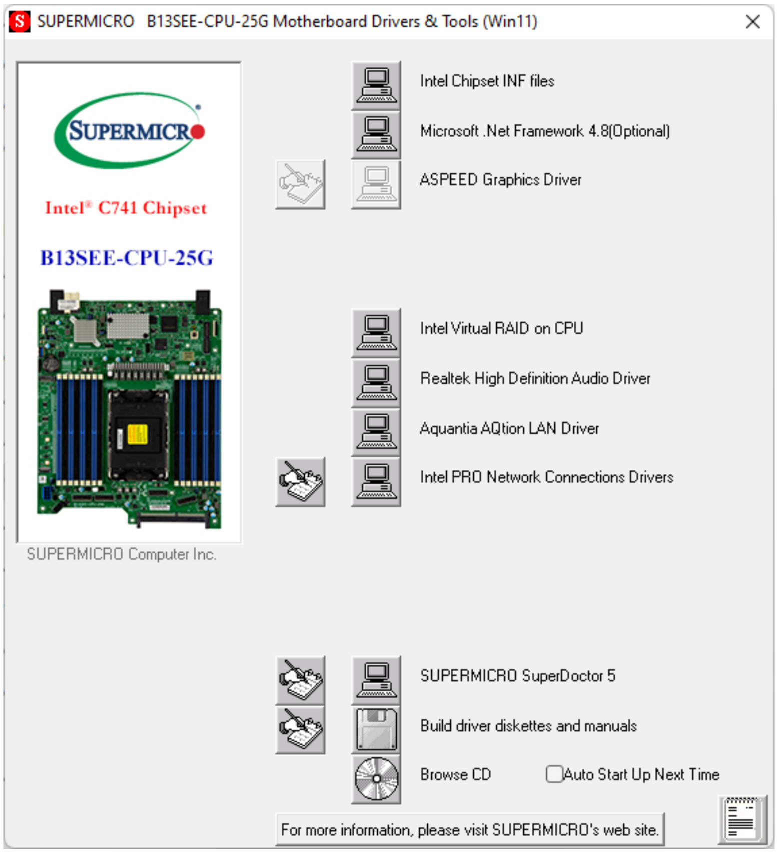

SUPERMICRO B13SEE-CPU-25G Motherboard Drivers & Tools (Win11)
SUPERMICRO
Intel® C741 Chipset
B13SEE-CPU-25G
SUPERMICRO Computer Inc.
Intel Chipset INF files
Microsoft .Net Framework 4.8(Optional)
ASPEED Graphics Driver
Intel Virtual RAID on CPU
Realtek High Definition Audio Driver
Aquantia AQtion LAN Driver
Intel PRO Network Connections Drivers
SUPERMICRO SuperDoctor 5
Build driver diskettes and manuals
Browse CD
□Auto Start Up Next Time
For more information, please visit SUPERMICRO's web site.

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.

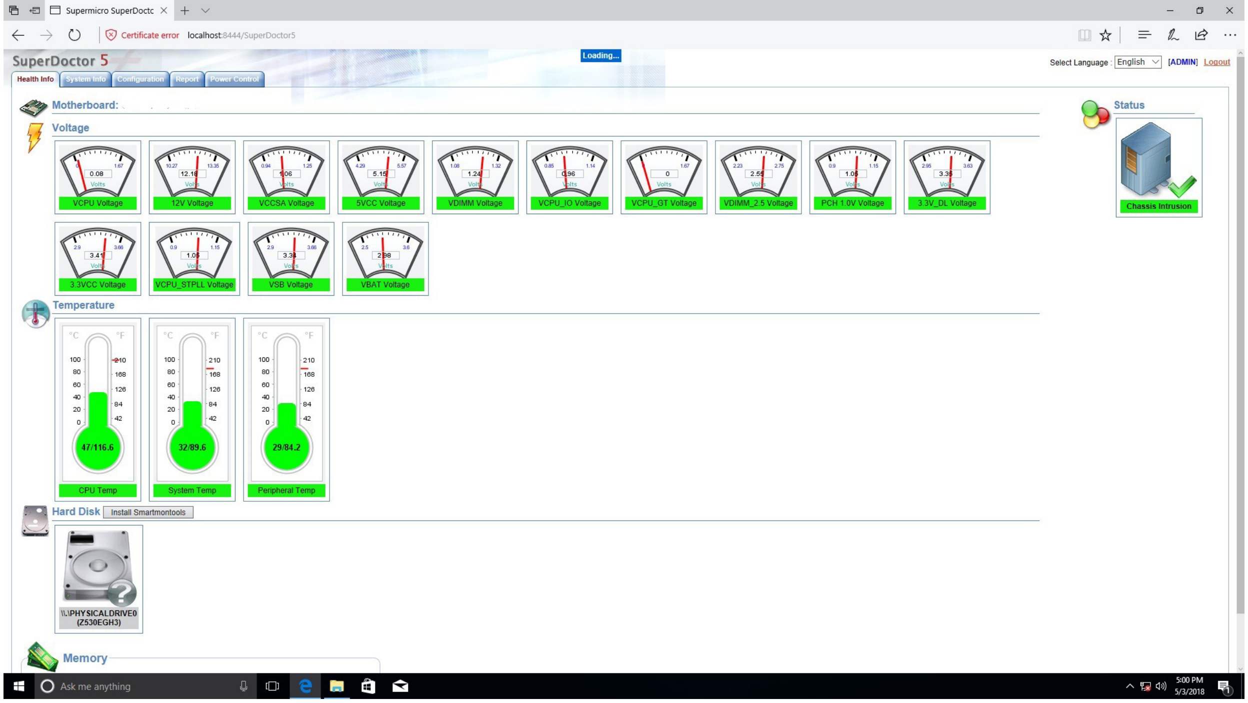


Figure B-4. SuperDoctor 5 Interface Display Screen (Health Information)

B.4 IPMI

The 4th and 5th Generation Intel Xeon Scalable Processor 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 http://www.supermicro.com/products/nfo/IPMI.cfm.

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。

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 اسحبذال البطارية بطريقة غير صحيحة فعليل
اسحبذال البطارية
فقط بنفس النع أو ما يعادلها مما أوصث به الشرمة المصنعة
جخلص من البطاريات المسحعملة وفقا لحعليمات الشرمة 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 القانين واللائح الطنية

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.

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 you 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 Power-On Self-Test (POST) 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 you to recover the main BIOS image using a USB-attached device without additional utilities used. A USB flash or media device can be used for this purpose. However, a USB Solid State 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.

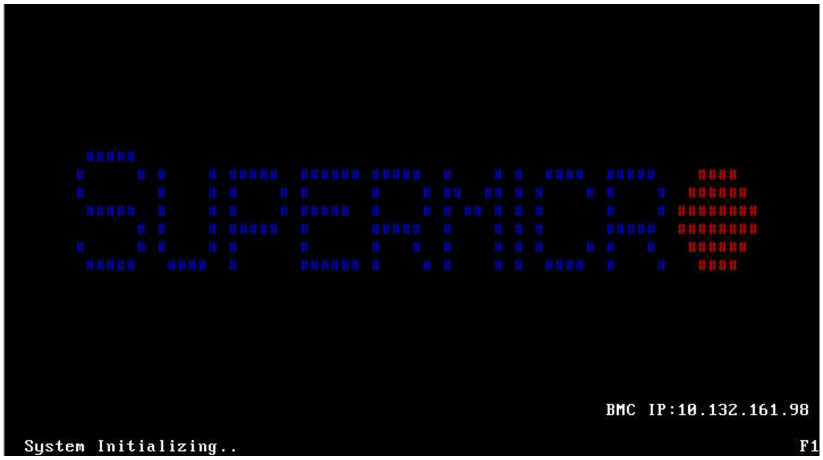
To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below:

1. Using a different machine, copy the "Super.ROM" binary image file into the disc Root "\" directory of a USB flash or media device.

   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.

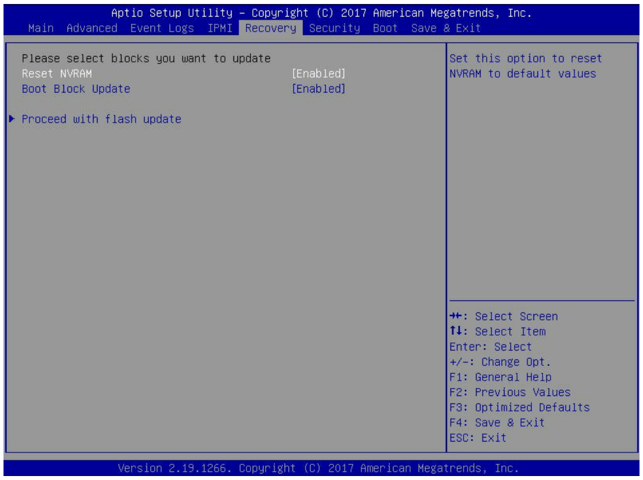
2. Insert the USB device that contains the new BIOS image ("Super.ROM") into your USB port and reset the system until the following screen appears:



```
BMC IP:10.132.161.98
System Initializing..                                    F1
```

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.

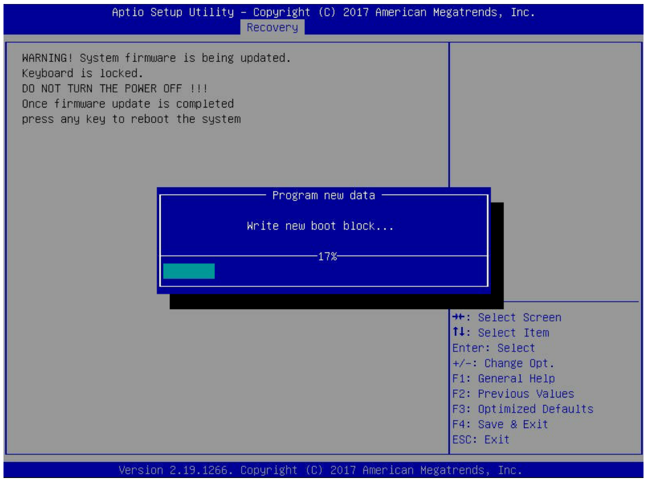

Aptio Setup Utility – Copyright (C) 2017 American Megatrends, Inc.
Main Advanced Event Logs IPMI Recovery Security Boot Save & Exit
→←: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
Version 2.19.1266. Copyright (C) 2017 American Megatrends, Inc.

```
Please select blocks you want to update
Reset NVRAM                                  [Enabled]
Boot Block Update                            [Enabled]

▶ Proceed with flash update
```

Set this option to reset NVRAM to default values

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:

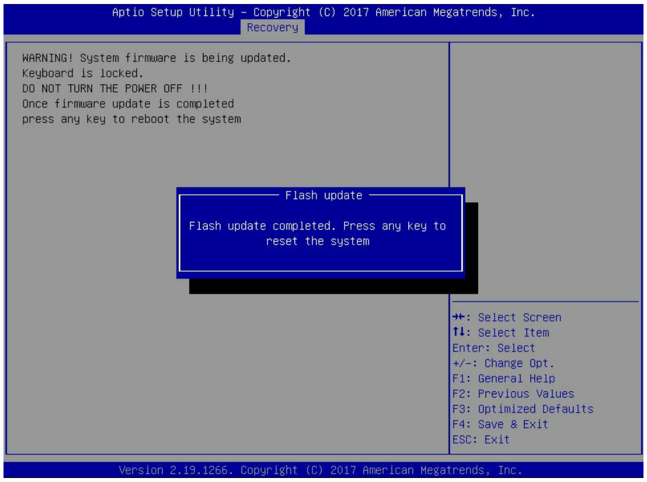
Note: *Do not interrupt the BIOS flashing process until it has completed*.



```
WARNING! System firmware is being updated.
Keyboard is locked.
DO NOT TURN THE POWER OFF !!!
Once firmware update is completed
press any key to reboot the system
```

```
Program new data
Write new boot block...
17%
```

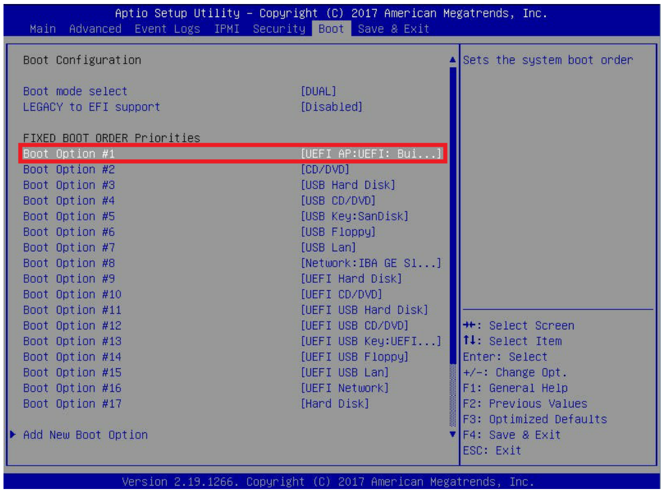
5. After the BIOS recovery process is completed, press any key to reboot the system.



```
WARNING! System firmware is being updated.
Keyboard is locked.
DO NOT TURN THE POWER OFF !!!
Once firmware update is completed
press any key to reboot the system

Flash update completed. Press any key to
reset the system
```

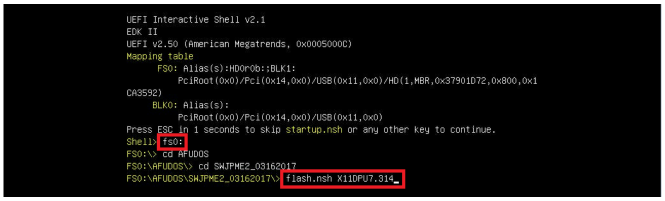
6. Using a different system, extract the BIOS package into a USB flash drive.

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.



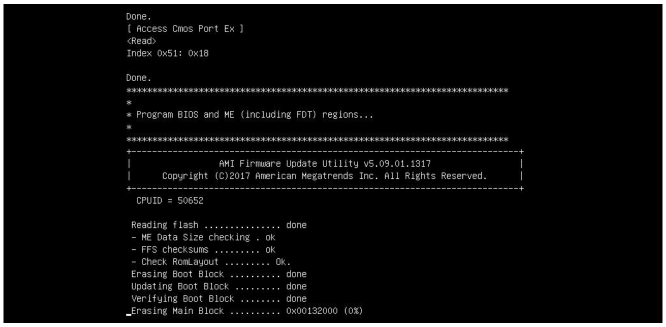
```
Boot Configuration                                 Sets the system boot order

Boot mode select              [DUAL]
LEGACY to EFI support         [Disabled]

FIXED BOOT ORDER Priorities
Boot Option #1                [UEFI AP:UEFI: Bui...]
Boot Option #2                [CD/DVD]
Boot Option #3                [USB Hard Disk]
Boot Option #4                [USB CD/DVD]
Boot Option #5                [USB Key:SanDisk]
Boot Option #6                [USB Floppy]
Boot Option #7                [USB Lan]
Boot Option #8                [Network:IBA GE Sl...]
Boot Option #9                [UEFI Hard Disk]
Boot Option #10               [UEFI CD/DVD]
Boot Option #11               [UEFI USB Hard Disk]
Boot Option #12               [UEFI USB CD/DVD]
Boot Option #13               [UEFI USB Key:UEFI...]
Boot Option #14               [UEFI USB Floppy]
Boot Option #15               [UEFI USB Lan]
Boot Option #16               [UEFI Network]
Boot Option #17               [Hard Disk]

▶ Add New Boot Option
```

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.

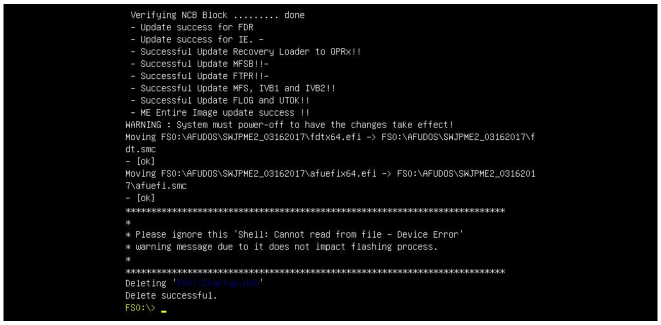


```
UEFI Interactive Shell v2.1
EDK II
UEFI v2.50 (American Megatrends, 0x0005000C)
Mapping table
      FS0: Alias(s):HD0r0b:;BLK1:
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)/HD(1,MBR,0x37901D72,0x800,0x1
CA3592)
     BLK0: Alias(s):
          PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> cd AFUDOS
FS0:\AFUDOS\> cd SWJPME2_03162017
FS0:\AFUDOS\SWJPME2_03162017\> flash.nsh X11DPU7.314_
```

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



```
Done.
[ Access Cmos Port Ex ]
<Read>
Index 0x51: 0x18

Done.
***************************************************************************
*
* Program BIOS and ME (including FDT) regions...
*
***************************************************************************
+-----------------------------------------------------------------------------+
|                 AMI Firmware Update Utility v5.09.01.1317                  |
|      Copyright (C)2017 American Megatrends Inc. All Rights Reserved.      |
+-----------------------------------------------------------------------------+
  CPUID = 50652

 Reading flash ............... done
 - ME Data Size checking . ok
 - FFS checksums ......... ok
 - Check RomLayout ......... Ok.
 Erasing Boot Block .......... done
 Updating Boot Block ......... done
 Verifying Boot Block ........ done
_Erasing Main Block .......... 0x00132000 (0%)
```



```
 Verifying NCB Block ......... done
 - Update success for FDR
 - Update success for IE. -
 - Successful Update Recovery Loader to OPRx!!
 - Successful Update MFSB!!-
 - Successful Update FTPR!!-
 - Successful Update MFS, IVB1 and IVB2!!
 - Successful Update FLOG and UTOK!!
 - ME Entire Image update success !!
WARNING : System must power-off to have the changes take effect!
Moving FS0:\AFUDOS\SWJPME2_03162017\fdtx64.efi -> FS0:\AFUDOS\SWJPME2_03162017\f
dt.smc
- [ok]
Moving FS0:\AFUDOS\SWJPME2_03162017\afuefix64.efi -> FS0:\AFUDOS\SWJPME2_0316201
7\afuefi.smc
- [ok]
***************************************************************************
*
* Please ignore this 'Shell: Cannot read from file - Device Error'
* warning message due to it does not impact flashing process.
*
***************************************************************************
Deleting 'FS0:\Startup.nsh'
Delete successful.
FS0:\> _
```

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.