B13DEE

USER'S MANUAL

Revision 1.0a

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.**
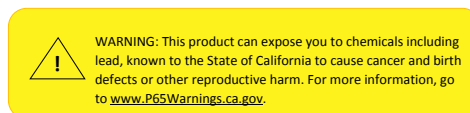
Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/ or its licensors, and is supplied only under a license. Any use or 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 A 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 an industrial environment. 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 1.0a

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 B13DEE motherboard in a Supermicro blade server.

About This Motherboard

The Supermicro B13DEE supports dual 4th/5th Gen Intel® Xeon® Scalable Processors (in Socket E LGA 4677) with three UPIs (20GT/s max.) and a TDP (Thermal Design Power) up to 350W. Built with the Intel C741 chipset, the B13DEE supports 8TB (max.) 3DS RDIMM/ RDIMM DDR5 ECC memory with speeds up to 5600 MT/s in 16 DIMM slots (or up to 4400 MT/s in 32 DIMM slots). (See Note 1 below.) This motherboard features superior I/O expandability and flexibility, including one SIOM PCIe 4.0 x16 connector with SATA 6G/ NVMe/SAS 3.0 support, one Mezzanine riser card connector with PCIe 3.0 support, one Type A USB 3.0 header with two USB connection support, one M.2 with up to PCIe 5.0 x4 support (optional), and four MCIO x8 connectors with dual PCIe 5.0 x16 support (optional). It also offers the most advanced data protection with hardware RoT (Root of Trust) and TPM (Trusted Platform Module) support (See Note 2 below.) The B13DEE is optimized for 6U SuperBlade systems with high density capability and high speed I/O support. It is ideal for High Performance Computing (HPC) used in most innovative technological applications. For processor/memory updates, please refer to our website at https://www.supermicro.com/en/ products/motherboards.

Note 1: Memory speed/capacity support depends on the processors used in the sytem. The 4th Gen Intel Xeon Scalable processors support DDR5 memory with speeds up to 4800MT/s (or up to 4400 MT/s in 32-DIMM configuration). The 5th Gen Intel Xeon Scalable processors support DDR5 memory with speeds up to 5600MT/s (or up to 4400 MT/s in 32-DIMM configuration).

Note 2: For TPM support, an optional part is needed. Please contact Supermicro Technical support for more details.

Conventions Used in the Manual

Special attention should be given to the following symbols for proper installation and for protection against possible component damage or bodily injury:

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

Warning! Important information given to prevent equipment/property damage or personal injury.

Warning! Indicates that high voltage may be encountered when you perform a task

Note: Additional Information given to differentiate between 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 Inquiry: Non-Government)
	Government_Sales-USA@supermicro.com (Sales Inquiry: Government)
	Support@supermicro.com (Technical Support)
	RMA@supermicro.com (RMA Support)
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

Congratulations on purchasing your blade server board from an industry leader. Supermicro products are designed to provide you with the highest standards in quality and performance.

This motherboard is intended to be used in a Supermicro proprietary server as a part of an integrated solution. It will not be shipped as a standard, independent product. There will be no shipping package provided for this motherboard.

1.1 Blade Server Board Overview

This chapter provides detailed information on the components installed on B13DEE Blade Server board as well as specifications and features supported by the blade server.

Important Links

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

- 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=/wdl/utility/Lot9_Secure_Data_Deletion_Utility/

- Firmware-related and AOC user's guides: http://www.supermicro.com/support/manuals/

- If you have any questions, please contact our support team at: support@supermicro.com

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

B13DEE Motherboard Image
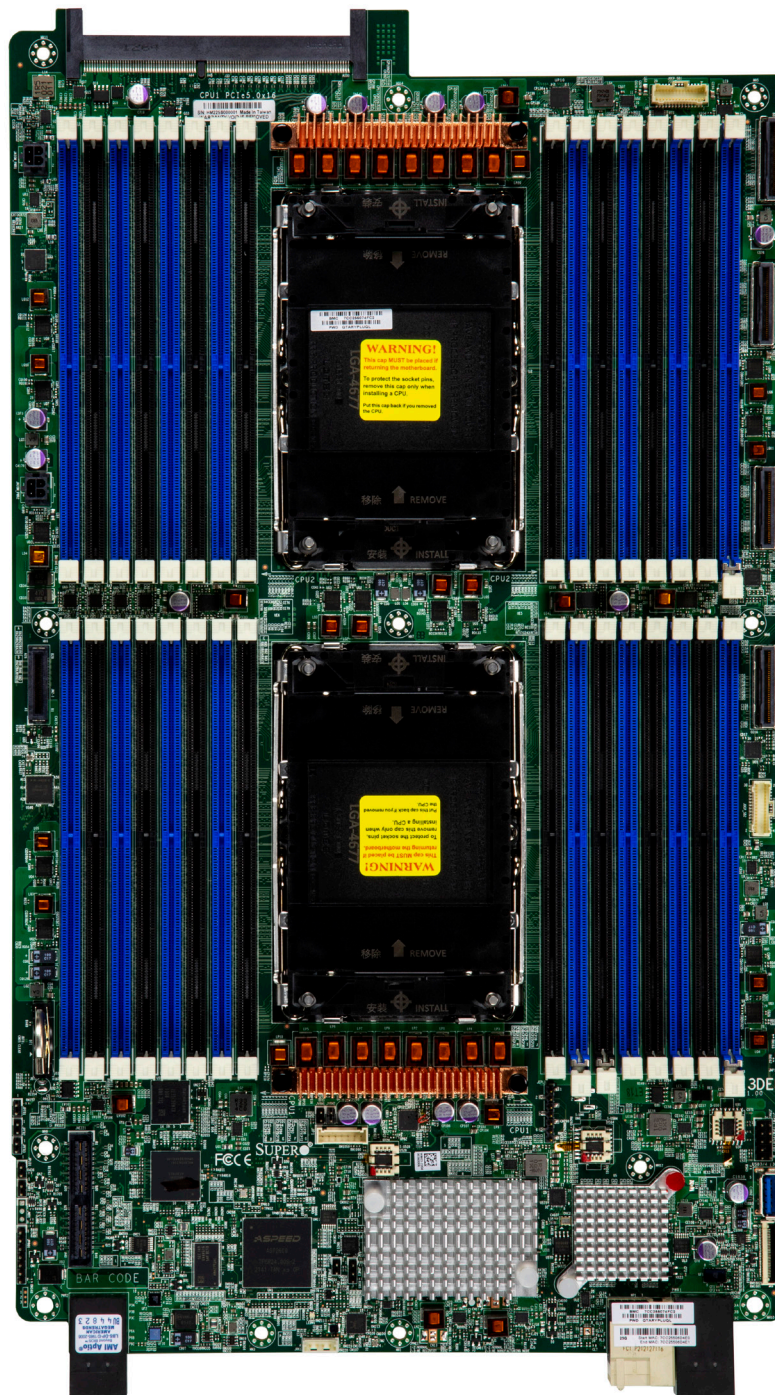
Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publication of this manual. The motherboard you received may or may not look exactly the same as the graphics shown in the manual.

B13DEE Motherboard Layout

(not drawn to scale)
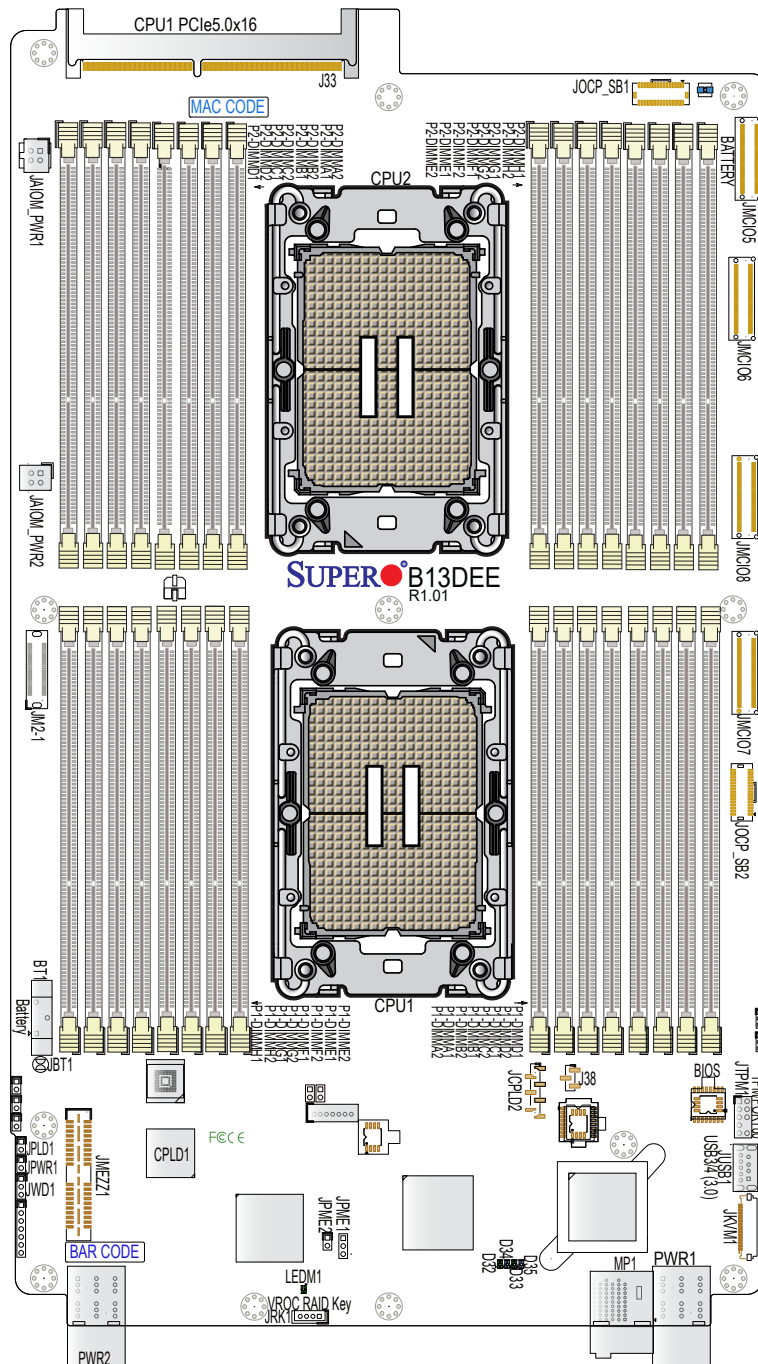
Notes:

- See Chapter 2 for detailed information on jumpers and 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 a possible explosion.

Quick Reference

PCIe 5.0 x 16 (J33)
CPU1 PCIe5.0 x16
J33
MAC CODE

JOCP_SB1
JOCP_SB1

JAIOM_PWR1
JAIOM_PWR1

JMCIO5 (Battery)
JMCIO5

CPU2

P2-D1MMA2
P2-D1MMA1
P2-D1MMB2
P2-D1MMB1
P2-D1MMC2
P2-D1MMC1
P2-D1MMD2
P2-D1MMD1

JMCIO6

P2-D1MME2
P2-D1MME1
P2-D1MMF2
P2-D1MMF1
P2-D1MMG2
P2-D1MMG1
P2-D1MMH2
P2-D1MMH1

JAIOM_PWR2
JAIOM_PWR2

JMCIO8

SUPER● B13DEE
R1.01

JM2-1 (M.2 Slot)
JM2-1

JMCIO7

P1-D1MME2
P1-D1MME1
P1-D1MMF2
P1-D1MMF1
P1-D1MMG2
P1-D1MMG1
P1-D1MMH2
P1-D1MMH1

JOCP_SB2
JOCP_SB2

P1-D1MMA2
P1-D1MMA1
P1-D1MMB2
P1-D1MMB1
P1-D1MMC2
P1-D1MMC1
P1-D1MMD2
P1-D1MMD1

CPU1

Battery (BT1)
BT1 Battery

Clear CMOS (JBT1)
JBT1

JCPLD2
J38
BIOS
TPM/PORT80 JTPM1

TPM/Port80
BIOS
USB 3/4 (3.0)
USB1 USB3/4 (3.0)

JPLD1 JPLD1
JPWR1 JPWR1
JWD1 JWD1
JMEZZ1 JMEZZ1
CPLD1
FCC CE

JKVM1 JKVM1

BAR CODE

JPME2
LEDM1
VROC RAID Key
JRK1
JPME1

D34
D33
D35
JCPLD2

MP1
PWR1

PWR2

PWR2 CPLD1 JPME2 LEDM1 VROC Key JRK1 JPME1 D32 D34 D33 D35 JCPLD2 MP1 PWR1

Note: Components not documented are for internal testing only.

Quick Reference Table

Jumper	Description	Jumper Setting (Bold: Default)
JBT1	CMOS Clear	**Open (Normal)**
JPME1	Manufacture Mode (ME Select)	**Pins 1/2: Manufacture Mode**
JPME2	ME Recovery	**Open: Normal**
JWD1	Watch Dog Timer Enable	**Pins 1/2: Reset**

LED	Description	Status
D32	HDD0 Heartbeat LED	Blinking: HDD device installed on HDD0 functions normally
D33	HDD1 Heartbeat LED	Blinking: HDD device installed on HDD1 functions normally
D34	HDD0 Activity LED	Blinking Green: HDD device installed on HDD0: Active
D35	HDD1 Activity LED	Blinking Green: HDD device installed on HDD1: Active
LEDM1	BMC Heartbeat LED	Blinking Green (working as a BMC LED): BMC Normal (Active) Solid Green: During a BMC Reset or a Cold Reboot

Connector	Description
Battery (BT1)	Onboard CMOS battery
J33	PCIe 5.0 x16 slot supported by CPU1
JAIOM_PWR1/JAIOM_PWR2	4-pin AIOM (Advanced I/O Module) Power Connector 1/ AIOM Power Connector 2
JCPLD2	Complex Programmable Logic Device (CPLD) header
JM2-1	M.2 slot for NVMe only (with support of M-Key 2280)
JMCIO5 ~ JMCIO8	PCIe 5.0 x8 Mini Cool Edge IO (MCIO) Connectors 5/6/7/8
JMEZZ1	Mezzanine card Slot1 (used for daughter card)
JKVM1	Keyboard/video display/mouse connector
JOCP_SB1	Supermicro Advanced Input/Output Module (AIOM) sideband connector used to support PCIe 5.0 x8 MCIO Connectors 5/6 (JMCIO5/JMCIO6)
JOCP_SB2	Supermicro Advanced Input/Output Module (AIOM) sideband connector used to support PCIe 5.0 x8 MCIO Connectors 7/8 (JMCIO7/JMCIO8)
JPLD1	Programmable Logic Device (PLD) header
JPWR1	2-pin power connector for Mezzanine card use
JTPM1	Trusted Platform Module/Port 80 connector (See Note 1 below.)
JUSB1	USB 3.0 header with support of USB 3.0 Port3/Port4
MP1	25G Midplane for 25 GbE Ethernet LAN support
PWR1/PWR2	Main Power Connector1/Connector2
VROC Key (JRK1)	Intel VROC RAID Key Header (See Note 2 below.)

Note 1: For TPM support, an optional part is needed. Contact Supermicro Technical Support for more information.

Note 2: For detailed instructions on how to configure VROC RAID settings, please refer to the VROC RAID Configuration User's Guide posted on the web page under the link: http://www.supermicro.com/support/manuals/.

Motherboard Features

Motherboard Features
CPU
• Supports dual 4th/5th Gen Intel Xeon Scalable Processors (in Socket E LGA 4677) with three UPIs (20 GT/s max.) and a TDP (Thermal Design Power) up to 350W
Memory
• Supports up to 8TB 3DS RDIMM/RDIMM DDR5 (288-pin) ECC memory with speeds up 8TB (max.) 3DS RDIMM/RDIMM DDR5 ECC memory with speeds up to 5600 MT/s in 16 DIMM slots (or up to 4400 MT/s in 32 DIMM slots)   **Note:** Memory speed and capacity support depends on the processors used in the system.
DIMM Size
• Up to 256 GB   **Note:** For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.
Chipset
• Intel PCH C741
Expansion Slots
• One SIOM PCIe 4.0 x16 connector with SATA 6G/NVMe/SAS 3.0 support   • One Mezzanine riser card connector with PCIe 3.0 support   • One midplane with 25GbE Ethernet LAN support (MP1)   • One Type A USB 3.0 header with two USB connections (JUSB1)   • One M.2 connector with PCIe 5.0 x4 support (Optional)   • Four MCIO x8 connectors with dual PCIe 5.0 x16 support (Optional)
Baseboard Management Controller (BMC)/Network
• ASPEED AST2600 BMC
Graphics
• Graphics controller and video support via ASPEED AST2600 BMC
• AMI SPI BIOS   • EFI GUI, SPI dual/quad speed control, riser card auto detection, IPMIView, SMCIPMITOOL, IPMI CFG, Redundant power supply unit detection, SSM and SUM-OOB/InBand support
Power Management
• ACPI power management   • S1 and S5 support   • Power button override mechanism   • Power-on mode for AC power recovery   • Wake-on-LAN   • Power-on mode for AC power recovery

System Health Monitoring

- Onboard voltage monitoring for +12V, +5V, +5V standby, +3.3V, +3.3V standby, Vcore, and Vmem
- Onboard temperature monitoring for CPU, PCH, system, and memory
- CPU thermal trip support
- Platform Environment Control Interface (PECI)/TSI

Fan Control

- Fan status monitoring via BMC connections
- Single cooling zone
- Low-noise fan speed control

System Management

- Chassis intrusion header and detection
- Server platform service

Firmware Integrity/System Security

- TPM (Trusted Platform Module) support (Optional)
- Boot Guard
- BMC recovery, BIOS recovery, CPLD recovery
- RoT (Root of Trust) 2.0 support to protect firmware security by detecting critical data corruption and restoring platform integrity

LED Indicators

- CPU/system overheat LED
- Power LED
- UID/remote UID
- LAN activity LED
- BMC/CPLD firmware LED

Dimensions

- 10.00" (W) x 16.50" (L) Big Twin (254.00 mm x 419.10 mm)

Note 1: The CPU maximum Thermal Design Power (TDP) is subject to motherboard SKU, chassis and heatsink cooling restrictions. For proper thermal management, please check the chassis and heatsink specifications.

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

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 Support

Built upon the functionality and capability of the 4th/5th Gen Intel Xeon Scalable Processors (Socket E) and the Intel C741 PCH, the B13DEE motherboard offers critical, pivotal technological breakthroughs that unleash unprecedented computing capabilities and provides a scalable platform optimized for 6U SuperBlade systems with high density and high speed I/O support. It is ideal for High Performance Computing (HPC) used in most innovative technological applications. The key features supported by the platform include the following:

Processor Features Supported

- Increased, scalable performance with substantial advancements, including UPI speed improvement, memory speed/capacity/utilization enhancement, hardware-based security innovations for virtualization and platform interconnectivity optimization

- Integrated accelerators optimized for workload enhancement including Advanced Matrix Extensions (IntelAMX), In-Memory Analytics Accelerator (IAX), Data Streaming Accelerator (IntelDSA), and QuickAssist Technology (Intel QAT)

- Breakthroughs in memory and I/O support, including DDR5 (5600 MT/s max.), Max Series (HBM) (w/1 TB bandwidth max), PCIe 5.0 (80 lanes max.) and CXL 1.1 (4 devices per CPU)

- Increased operational and performance efficiency with substantial enhancements in virtualization, network security and telemetry and power management

- Integrated AI accelerators with support of 4th Gen Intel® Deep Learning Boost and new Tile Matrix Multiply (AMX/MUL)

- Enhanced Intel® Security Boost Software Guard Extensions with Integrity Platform Firmware Resilience support

- Intel® Ultra Path Interconnect (Intel® UPI) 3 links per processor at 20 GT/s

- New Compute Express Link (CXL) and Intel® Speed Select Technology

- CPU with 52 physical address/57 virtual address support

- Intel® Trusted Domain Extensions (TDX) support (5th Gen Intel Xeon Scalable Processors)

PCH Features Supported

• Flexible I/O at 20 lanes for PCIe 3.0, 1G Ethernet in PCH for manageability, and 8 DMIs at PCIe 3.0

1.3 Special Features

Recovery from AC Power Loss

The Basic I/O System (BIOS) provides a setting that determines how the system will respond when AC power is lost and then restored to the system. You can choose for the system to remain powered off (in which case you must press the power switch to turn it back on), or for it to automatically return to the power-on state. See the Advanced BIOS Setup section for this setting. The default setting is **Last State.**

1.4 System Health Monitoring

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

The system health monitor embedded in the BMC chip can check the RPM status of the cooling fans. The CPU and chassis fans are controlled via BMC.

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the BMC interface. Whenever the temperature of the CPU or the system exceeds Supermicro's pre-defined threshold, the system and CPU cooling fan speed will increase to prevent the CPU or system from overheating.

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

1.5 ACPI Features

ACPI stands for Advanced Configuration and Power Interface. The 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 network cards, hard disk 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, please refer to the Supermicro website.

1.6 Power Supply

As with all computer products, a stable power source is necessary for proper and reliable operation. It is even more important for processors that have high CPU clock rates where noisy power transmission is present.

The B13DEE motherboard supports two main power connectors (PWR1/PWR2), two AOM (add-on module) power connectors (JAIOM_PWR1/2), and one Mezzanine card power connector (JPWR1). Although most power supplies generally meet the specifications required by the system, some are inadequate. All these power connections are also required to ensure adequate power supply to the system.

Warning! To avoid damaging the power supply or the motherboard, be sure to connect the main power connectors (PWR1/PWR2), the AOM power connectors (JAIOM_PWR1/2) and the Mezzanine card power connector (JPWR1) to your power supply. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.

It is strongly recommended that you use a high quality power supply that meets ATX power supply Specification 2.02 or above. It must also be SSI compliant.

Chapter 2

Installation

2.1 Static-Sensitive Devices

Electrostatic Discharge (ESD) can damage electronic components. To avoid damaging your motherboard, 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 motherboard 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 a possible battery 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 assembly will be then attached to the heatsink to form the processor heatsink module (PHM) before being installed into the CPU socket. Before installation, be sure to perform the following steps below:

- Please carefully follow the instructions given on the previous page to avoid ESD-related damages.

- Unplug the AC power cords from all power supplies after shutting down the system.

- 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 CPU 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 and memory support.

- All graphics in this manual are for illustrations only. Your components may look different.

> **Note 1:** The 4th Gen Intel® Xeon® Scalable Processor comes with three CPU SKUs: SP XCC, SP MCC, and Max Series (HBM). However, CPU SKU support is mother-board-specific and not all SKUs are enabled on every B13 motherboard. Please refer to the specifications of your motherboard for CPU SKU support. Also, be sure to use processors of the same SKU on a multi-processor motherboard.
>
> **Note 2:** The 4th Gen Intel® Xeon® Scalable Processor comes with three CPU SKUs, and each SKU supports a distinctive carrier. The SP XCC CPU supports Carrier E1A; Max Series (HBM) CPU supports Carrier E1C, and SP MCC, Carrier E1B.
>
> **Note 3:** This installation section provides instructions on how to install 1U heatsink and 2U heatsink on the motherboard. Please note that heatsink support depends on the chassis used in your system. For heatsink support on the motherboard, please refer to your system specifications.
>
> **Note 4:** The installation process is the same for both 4th and 5th Gen Intel Xeon Scalable processors. Please use the 4th Gen Intel Xeon Scalable processor installation process as a reference.

The 4th/5th Gen Intel Xeon Scalable Processor

1. The 4th/5th Gen Intel Xeon Scalable Processor

SP XCC Series	Max Series (HBM)	SP MCC Series

CPU Key

Pin 1

CPU Key

Pin 1

CPU Key

Pin 1

→ = Cutout   ▲ = Pin 1   ○ = CPU Key

Processor Top View

2. The Processor Carrier

Carrier Top View

Pin 1

Pin 1

Pin 1

SP XCC

Mas Series (HBM)

SP MCC

Carrier E1A
(for SP XCC)

Carrier E1C
(for Mas Series (HBM))

Carrier E1B
(for SP MCC)

CPU Key

CPU Key

CPU Key

CPU Key

= Cutout   = Pin 1   = CPU Key

Carrier Bottom View
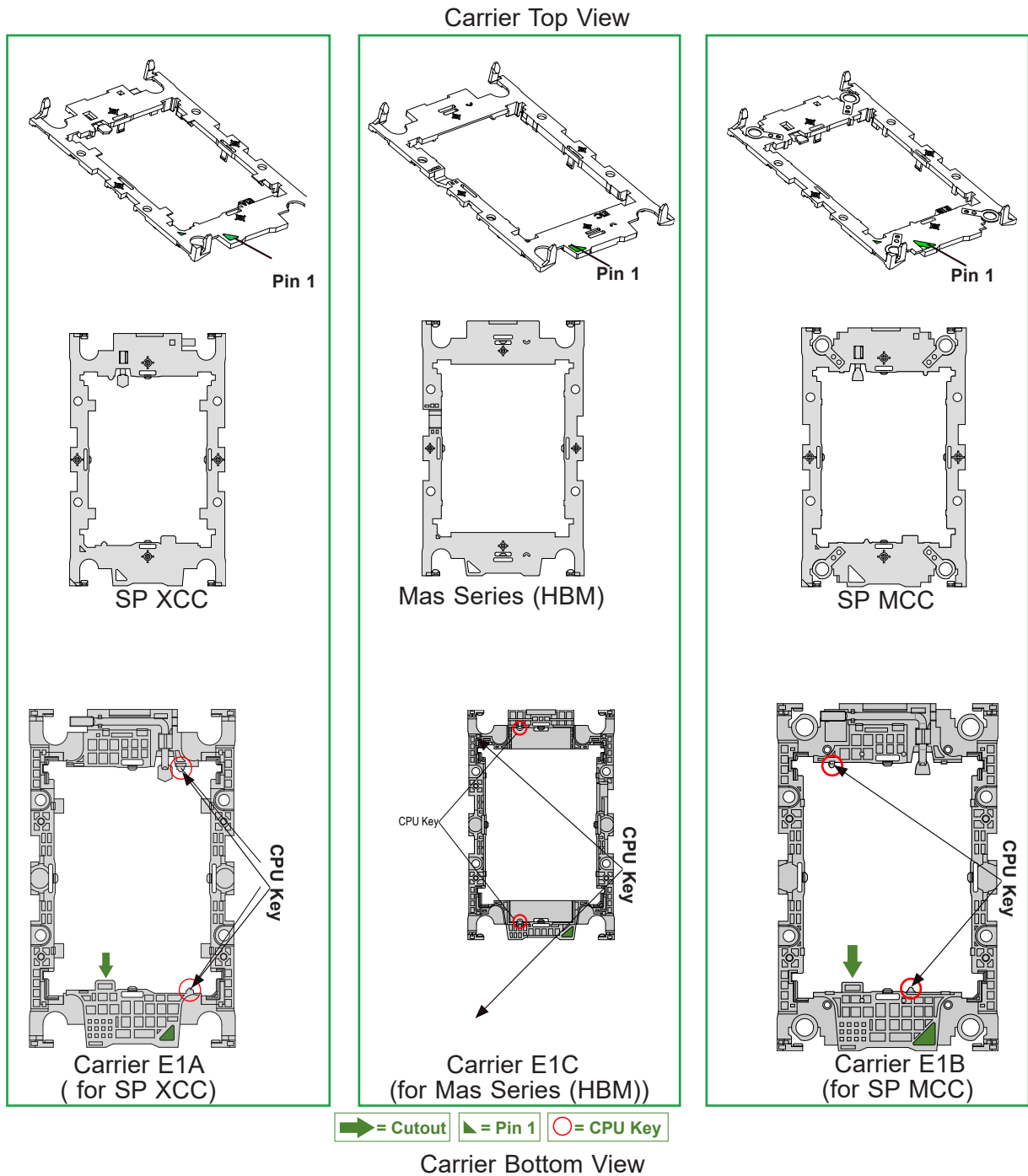
Note 1: The 4th Gen Intel® Xeon® Scalable Processor comes with three CPU SKUs: SP XCC, SP MCC, and (HBM). However, CPU SKU support is motherboard-specific. Please refer to the specifications of your motherboard for CPU SKU support. Also, be sure to use processors of the same SKU on a multi-processor motherboard.
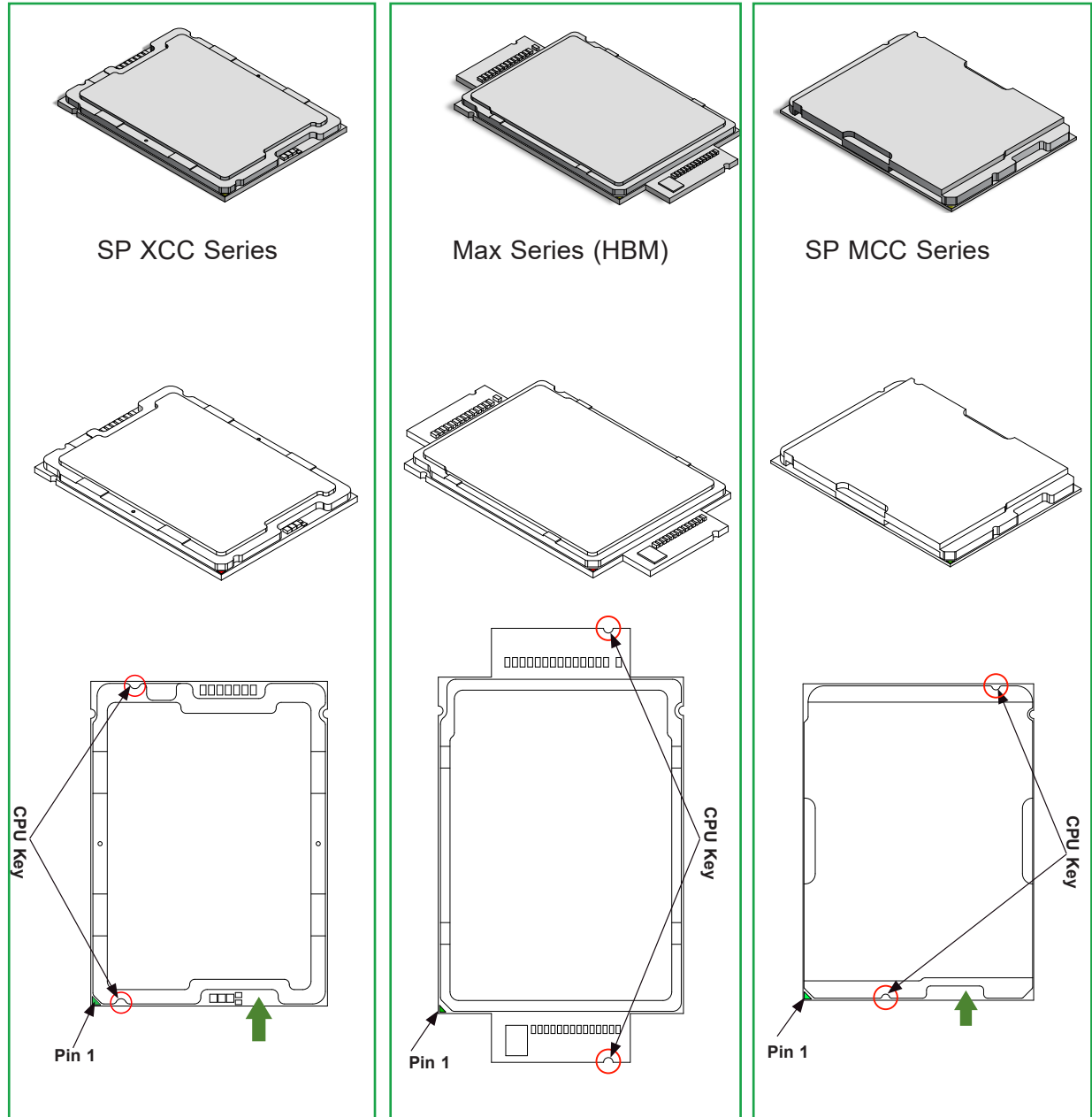
Note 2: The 4th Gen Intel® Xeon® Scalable Processor comes with three CPU SKUs, and each SKU supports a specific carrier. The SP XCC CPU supports Carrier E1A; Max Series (HBM) CPU supports Carrier E1C, and SP MCC, Carrier E1B.

3. Heatsink

1U Heatsink (SNK-P1046V)

1U Heatsink (SNK-P1046VM)
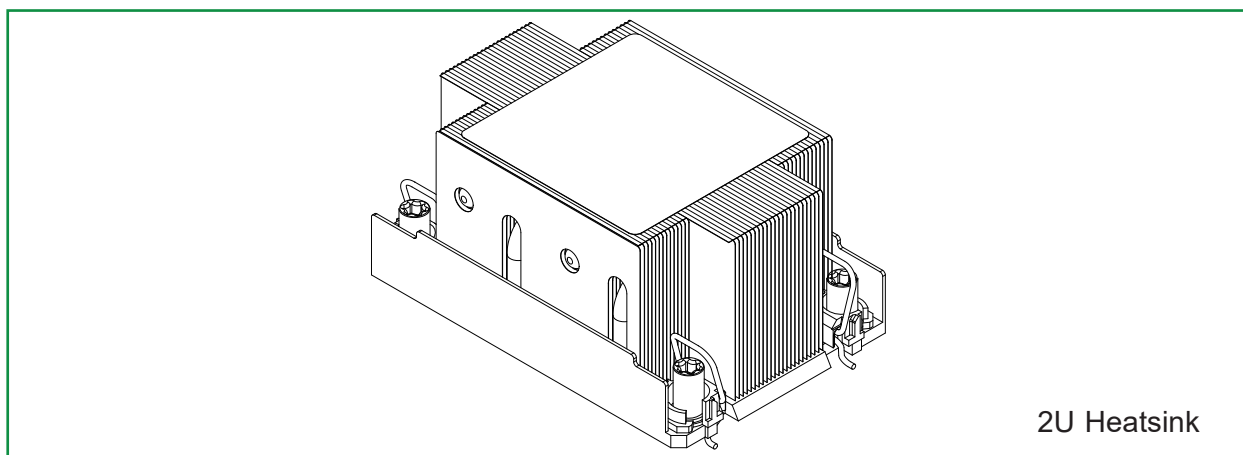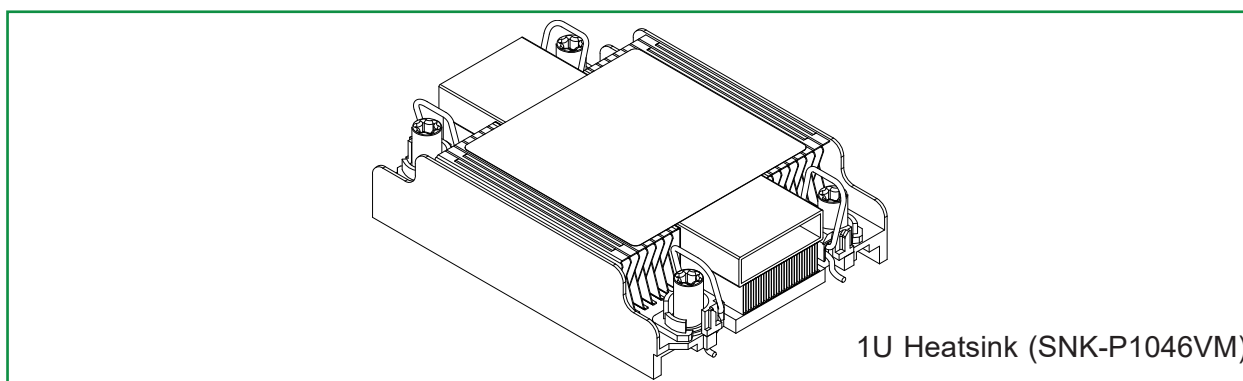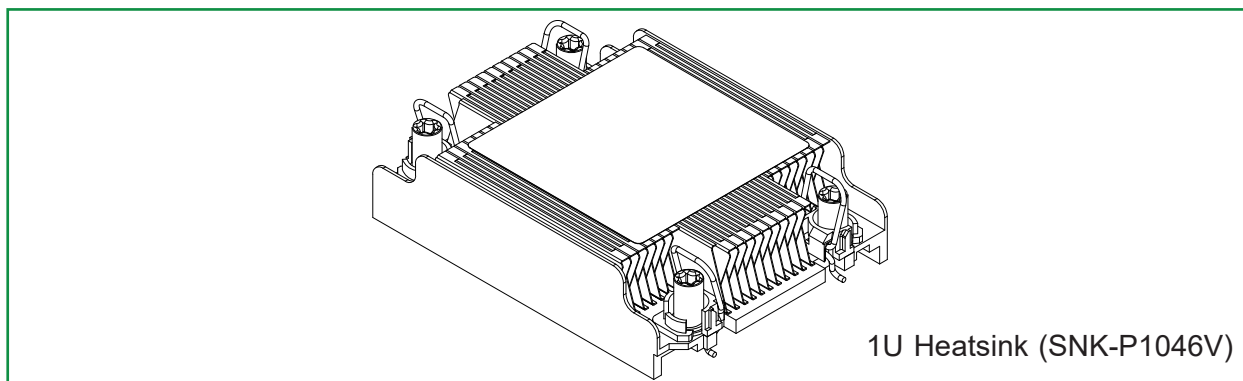
2U Heatsink

Note 1: Exercise extreme care when handling the heatsink. Pay attention to the edges of heatsink fins, which can be sharp! To avoid damaging the heatsink, please do not apply excessive force on the fins.

Note 2: This installation guide provides instructions on how to install 1U heatsink and 2U heatsink on the motherboard. Please note that heatsink support depends on the chassis used in your system. For heatsink support on your motherboard or in your system, please refer to your system specifications.

Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

Plastic Protective Cover
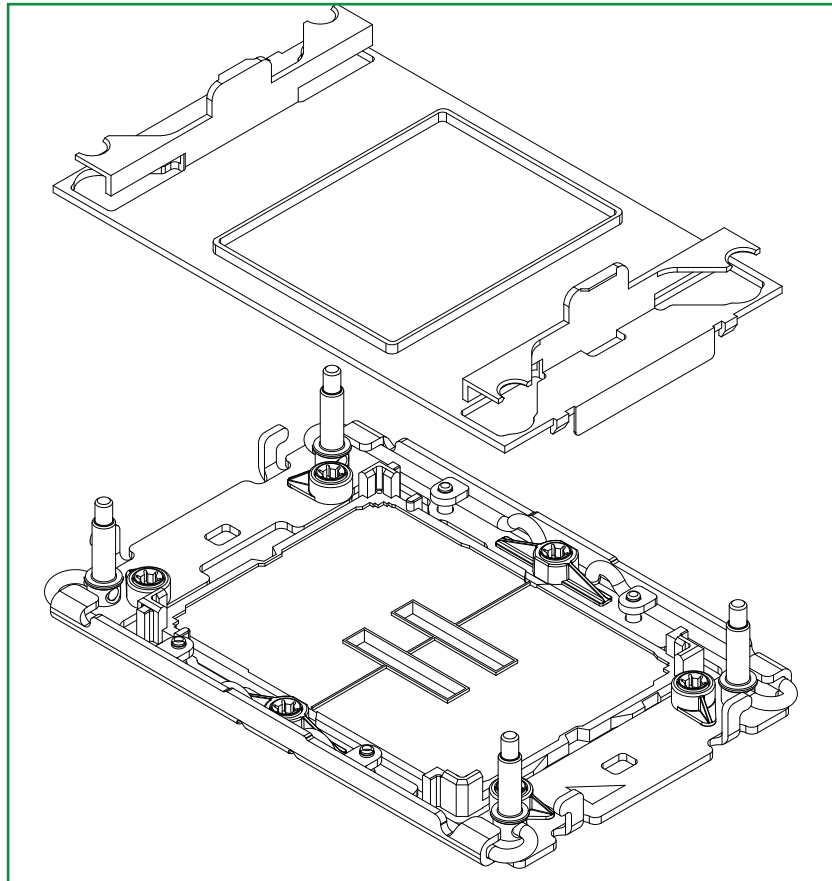
CPU Socket

Overview of the Processor Carrier Assembly

The processor carrier assembly contains a 4th/5th Gen Intel Xeon Scalable processor and a processor carrier. Carefully follow the instructions given in the installation section to place a processor into the carrier to create a processor carrier assembly. Please note that SP XCC CPU supports Carrier E1A, Max Series (HBM) CPU supports Carrier E1C, and SP MCC, Carrier E1B.

The processor carrier assembly includes a processor and a carrier as shown below.

1. The 4th/5th Gen Intel Xeon Scalable Processor (Component Side)

Processor (2D)			Processor (3D)		
SP XCC	Max Series (HBM)	SP MCC	SP XCC	Max Series(HBM)	SP MCC

2. CPU Carrier (Top View)

CPU Carrier (2D)			CPU Carrier (3D)		
Carrier E1A	Carrier E1C	Carrier E1B	Carrier E1A	Carrier E1C	Carrier E1B

3. CPU Carrier Assembly

SP XCC CPU	Max Series (HBM) CPU	SP MCC CPU
in Carrier E1A	in Carrier E1C	in Carrier E1B
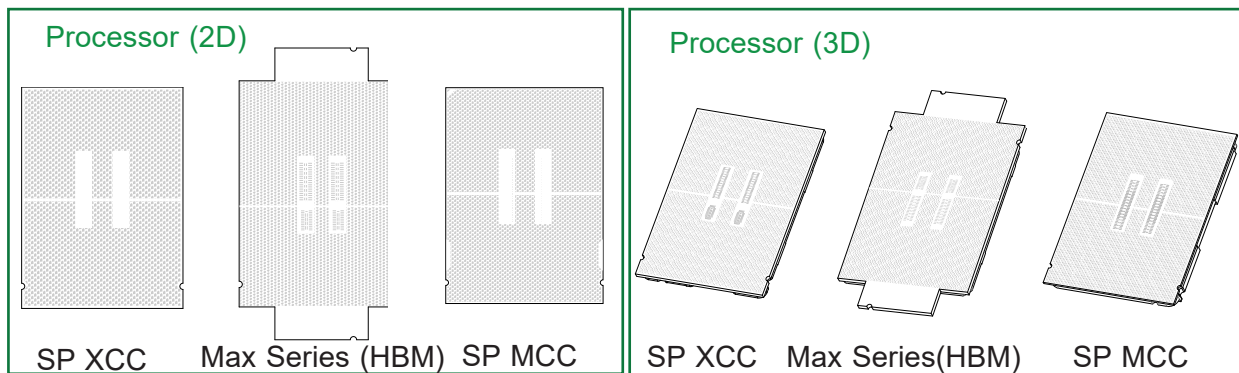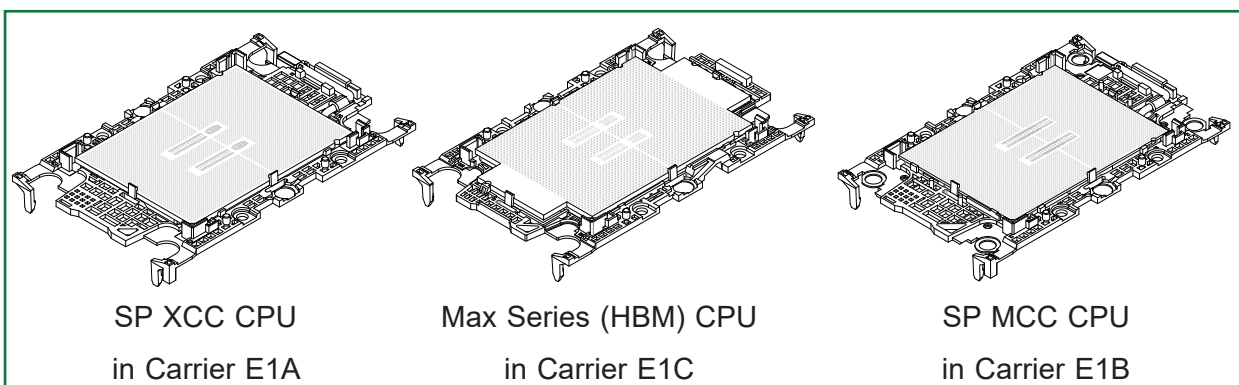
(with Processor Seated inside the Carrier)

Overview of the Processor Heatsink Module (PHM)

The Processor Heatsink Module (PHM) contains a heatsink, a processor carrier, and a 4th/5th Gen Intel Xeon Scalable processor.

1. Heatsink: for SP XCC CPU Illustration (Bottom View Shown Below)

1U Heatsink   2U Heatsink

SNK-P1046VM   SNK-P1046V
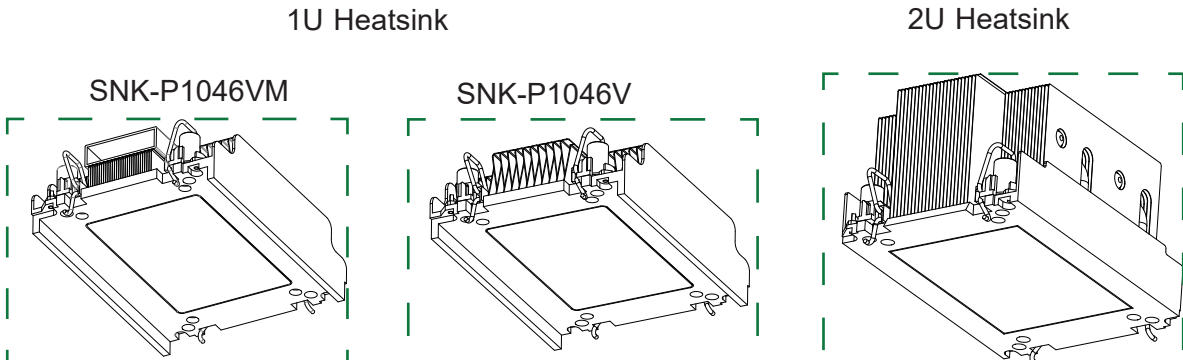
2. Processor Carrier E1A (for SP XCC CPU)
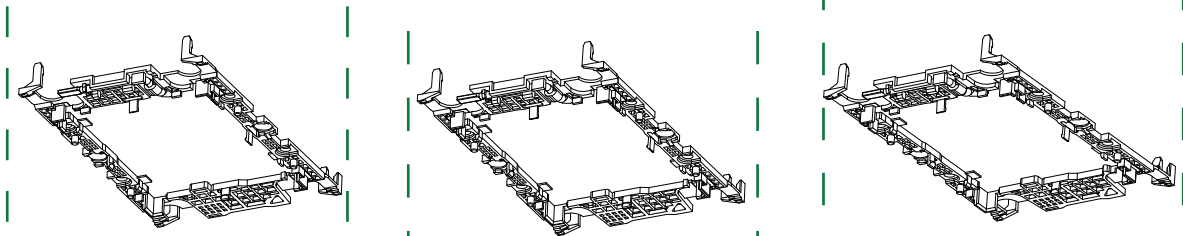
3. The 4th/5th Gen Intel Xeon Scalable Processor (SP XCC) (Component Side)

4. Processor Heatsink Module (PHM) (Bottom View Shown Below)
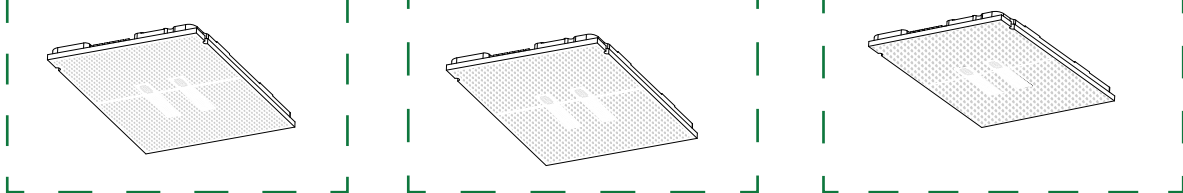
1U Heatsink   2U Heatsink
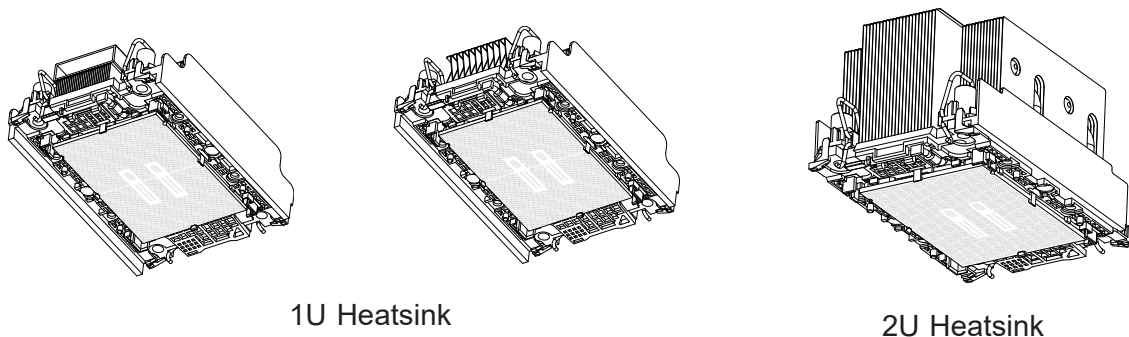
1. Heatsink: for Max Series (HBM) CPU Illustration (Bottom View Shown Below)

1U Heatsink   2U Heatsink

SNK-P1046VM   SNK-P1046V
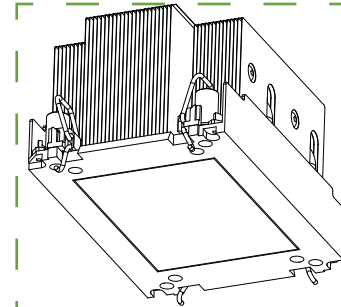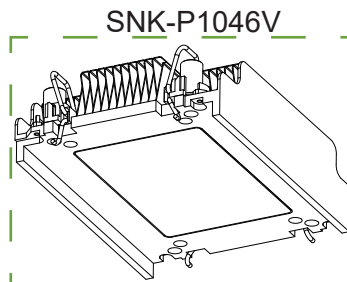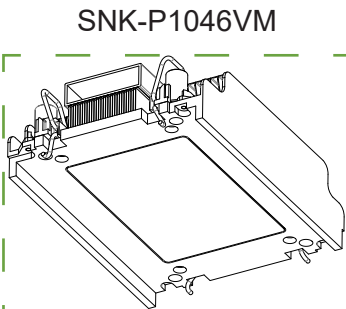
2. Processor Carrier E1C (Max Series ((HBM))
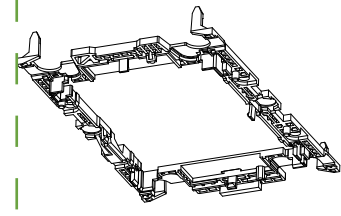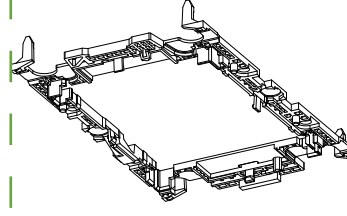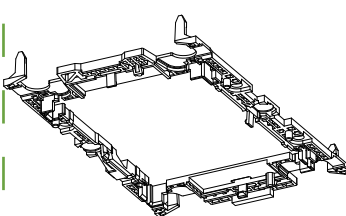
3. The 4th/5th Gen Intel Xeon Scalable Processor (Max Series ((HBM)) (Component Side)
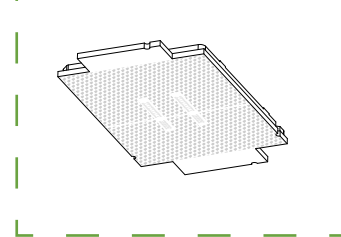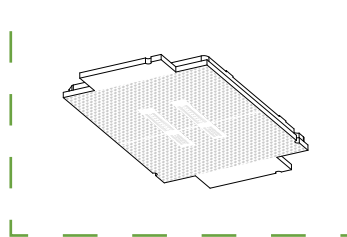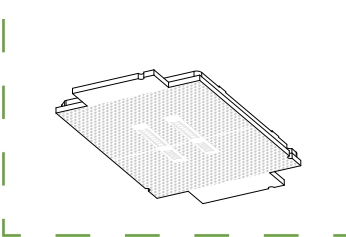
4. Processor Heatsink Module (PHM) (Bottom View Shown Below)
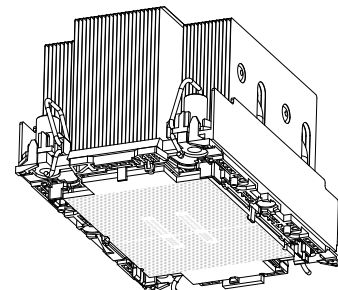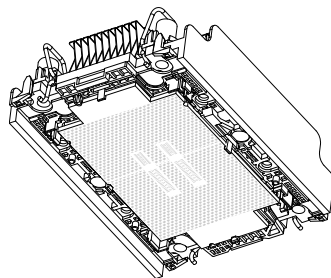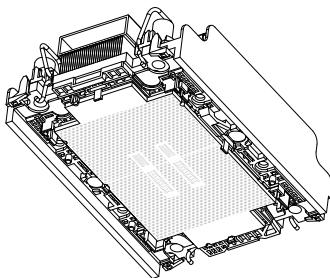
1U Heatsink   2U Heatsink

1. Heatsink: for SP MCC CPU Illustration (Bottom View Shown Below)
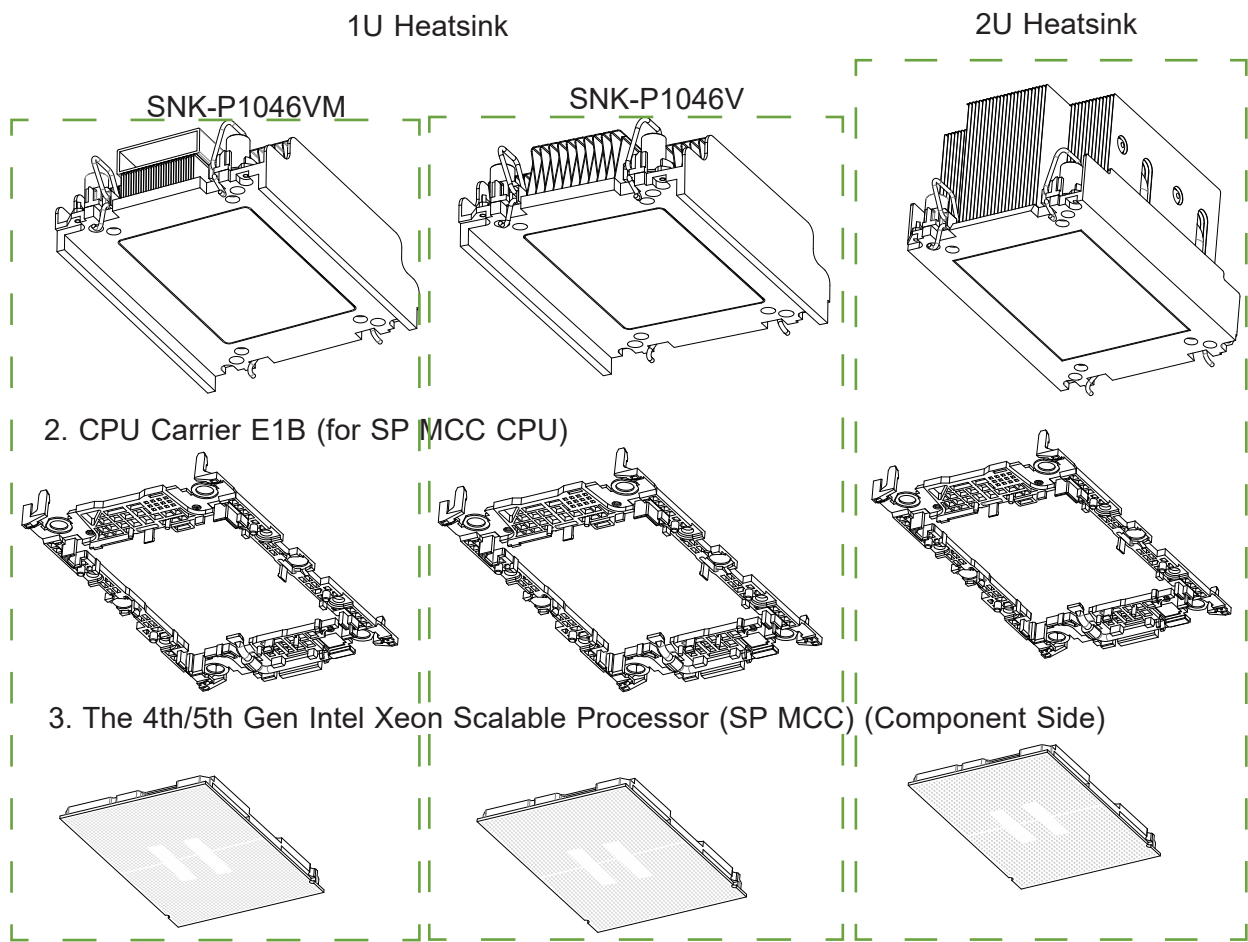
1U Heatsink

2U Heatsink

SNK-P1046VM

SNK-P1046V

2. CPU Carrier E1B (for SP MCC CPU)

3. The 4th/5th Gen Intel Xeon Scalable Processor (SP MCC) (Component Side)

4. Processor Heatsink Module (PHM) (Bottom View Shown Below)
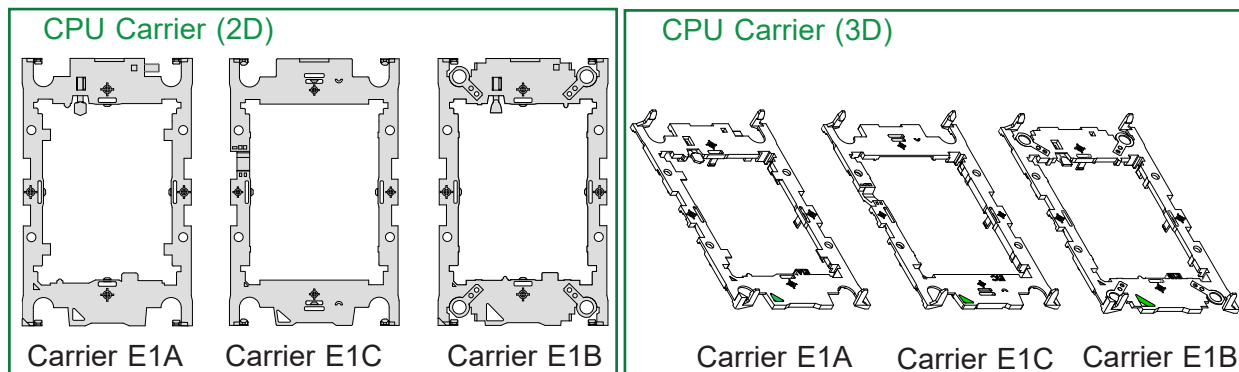
1U Heatsink

2U Heatsink
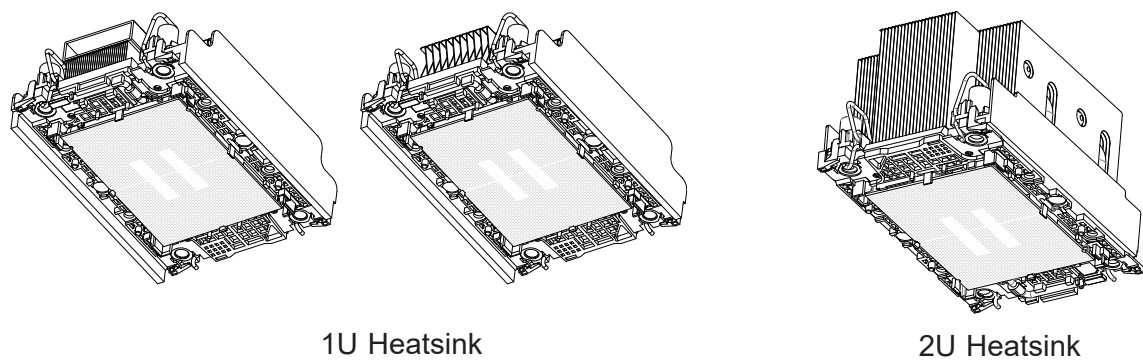
Creating the Processor Carrier Assembly

The processor carrier assembly contains a 4th/5th Gen Intel Xeon Scalable processor and a processor carrier.

To create the processor carrier assembly, please follow the steps below:

> **Note**: Before installation, be sure to follow the instructions given on pages 1 and 2 of this chapter to properly prepare for installation.

1. Hold the processor with the component side (including the gold contacts) facing down. Locate the small, gold triangle at the corner of the processor and the corresponding hollowed triangle on the processor carrier as shown in the graphics below. Please note that the triangle indicates the Pin 1 location.

Pin 1
SP XCC

Pin 1
Max Series (HBM)

Pin 1
SP MCC

Pin 1
Carrier E1A

Pin 1
Carrier E1C
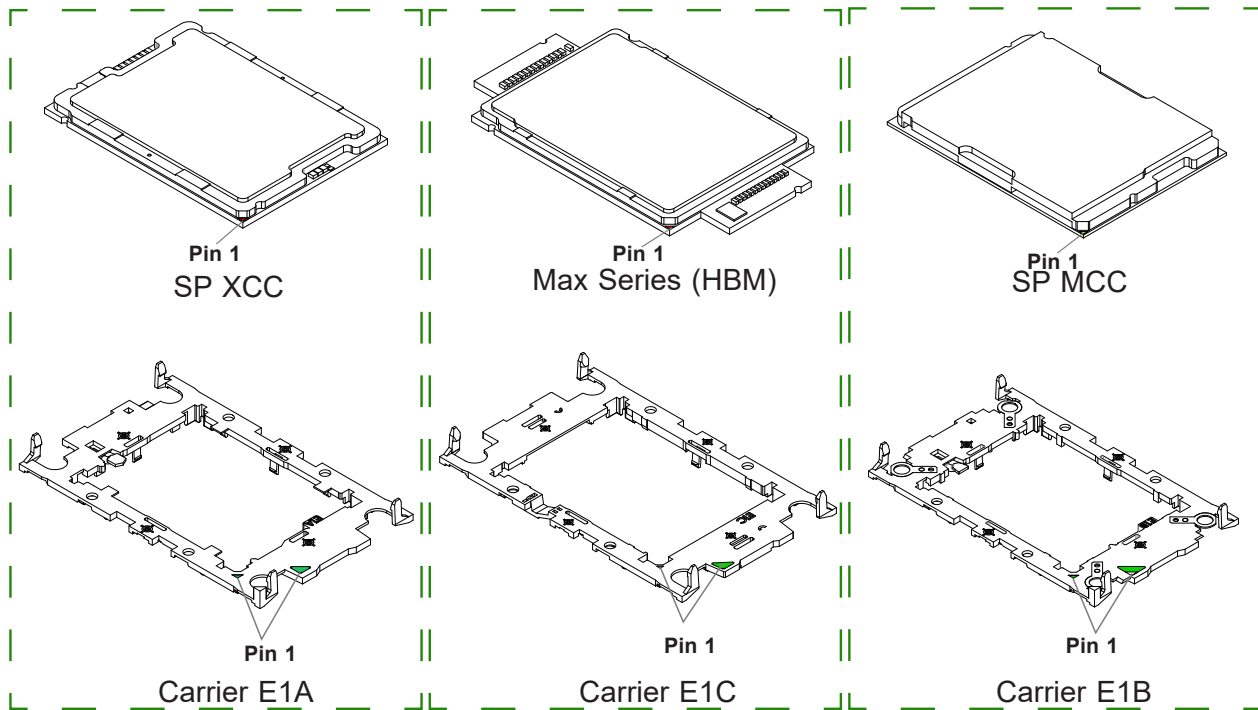
Pin 1
Carrier E1B

The Processor with its Matching Carrier

2. First, turn over the processor carrier and locate Pin 1 on the CPU and Pin 1 on the carrier. Then, turn the processor over with the component side (including the gold contacts) facing up and locate CPU keys on the processor. Finally, locate the CPU keys and four latches on the carrier as shown below.

SP XCC

Max Series (HBM)

SP MCC
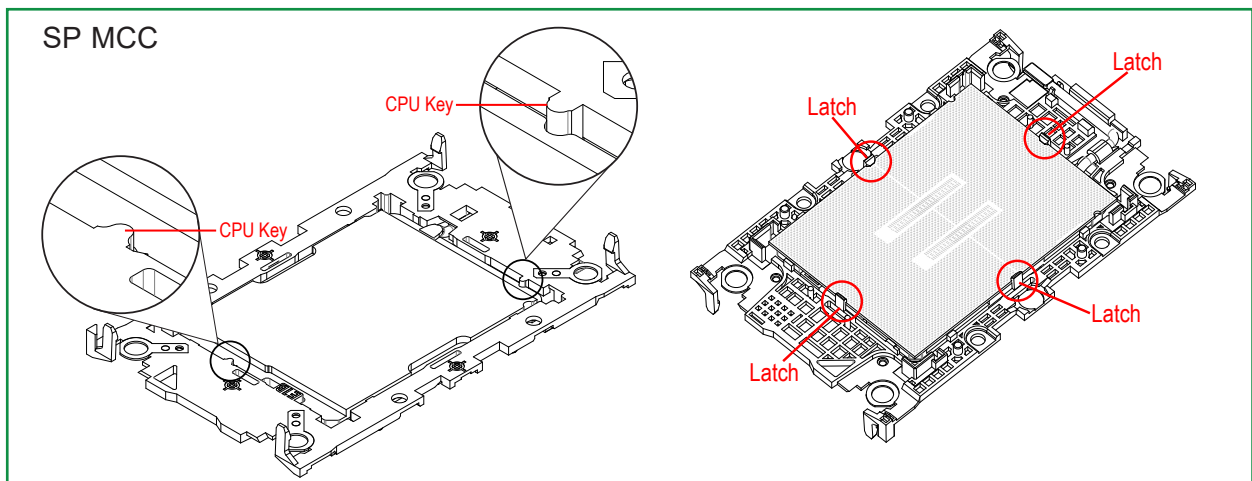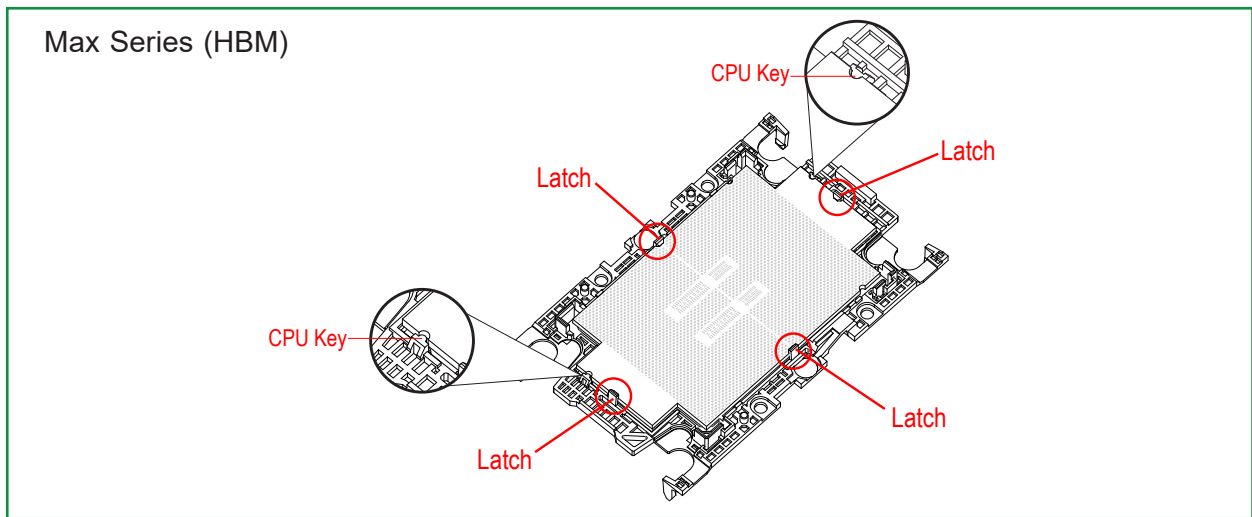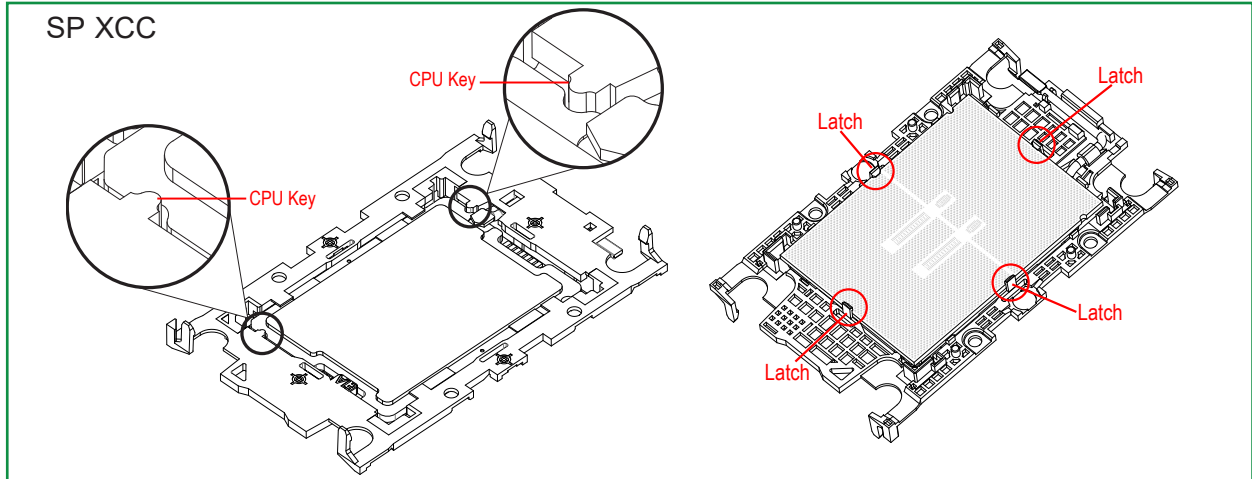
3. Locate the lever on the CPU socket and press it down as shown below.

Carrier E1A

Lever

Carrier E1B

Lever
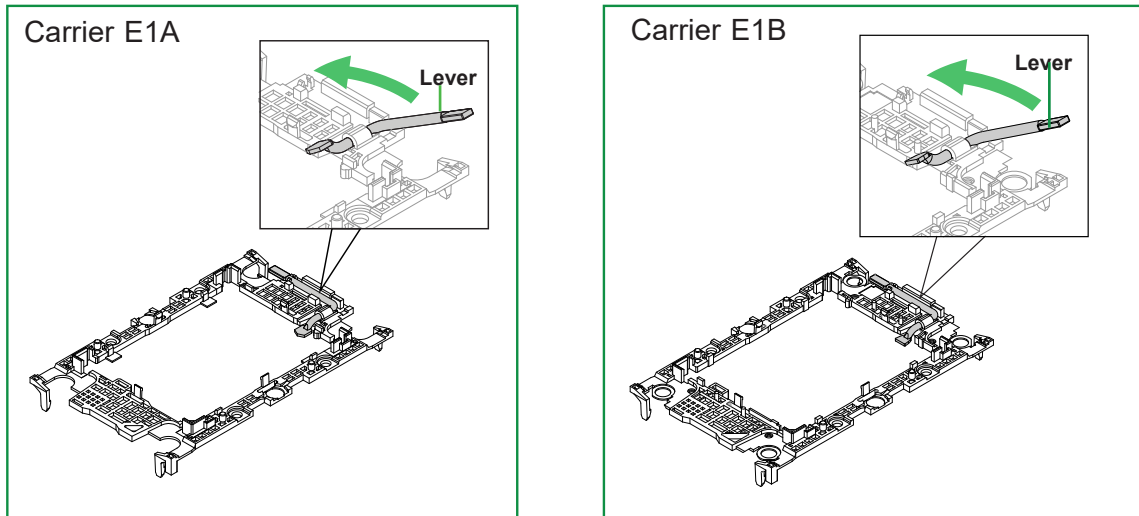
4. Using Pin 1 as a guide, carefully align the CPU keys (A and B) on the processor against the CPU keys on the carrier (a and b) as shown in the drawing below.

5. Once they are properly aligned, carefully insert the CPU into the carrier, making sure that the CPU is properly seated and secured by latches 1, 2, 3, and 4.

SP XCC

SP MCC

Max Series (HBM)
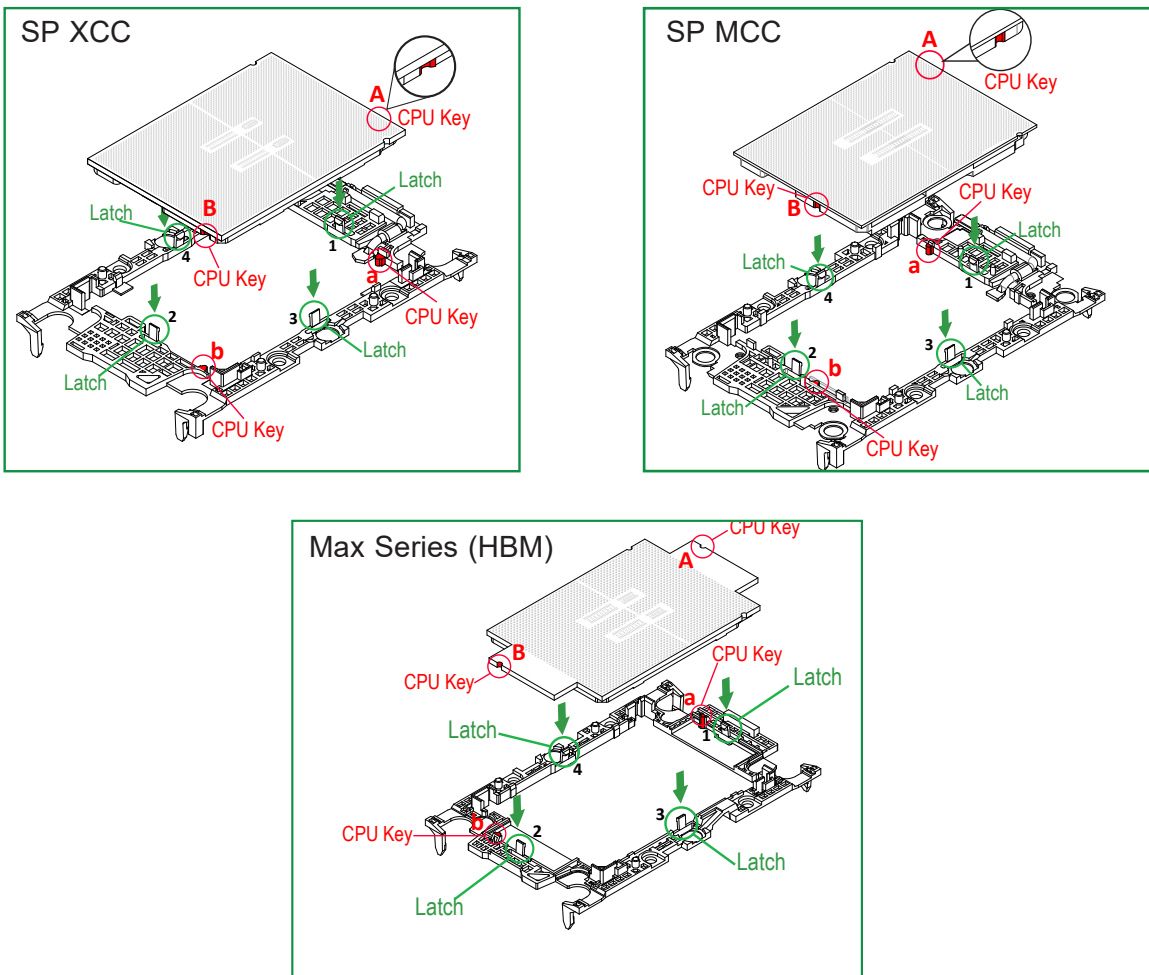
6. After the processor is placed inside the carrier, examine the four sides of the processor, making sure that the processor is properly seated on the carrier.

SP XCC

(Top View) (Component View)

CPU Carrier Assembly

Max Series (HBM)

(Top View) (Component View)

CPU Carrier Assembly

SP MCC

(Top View) (Component View)

CPU Carrier Assembly
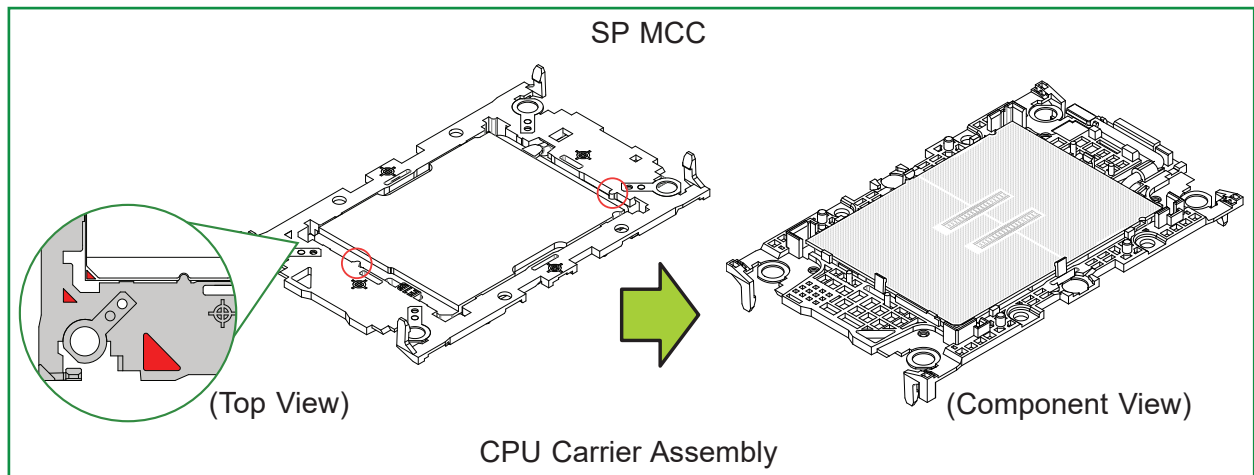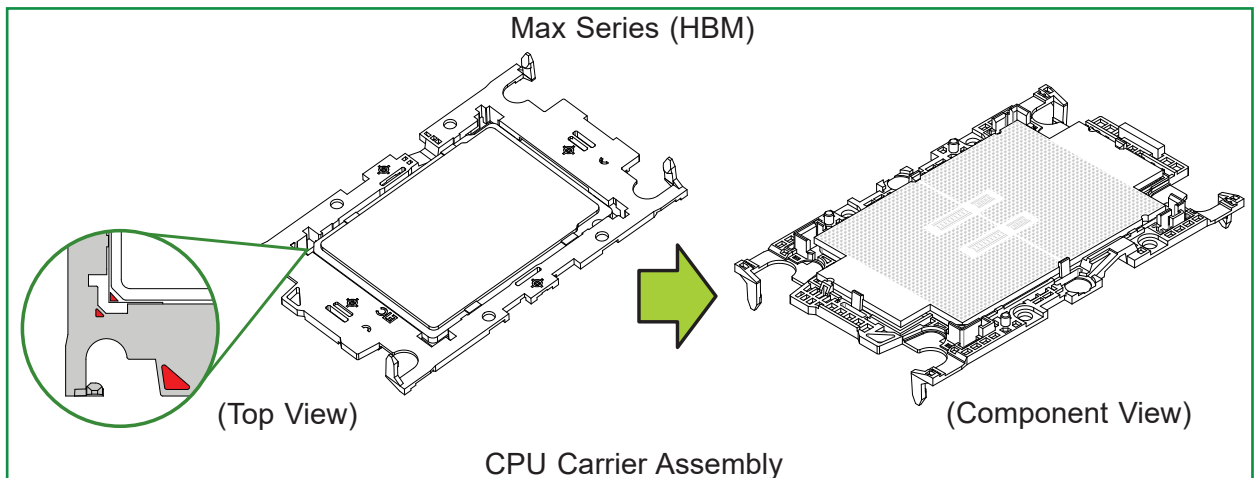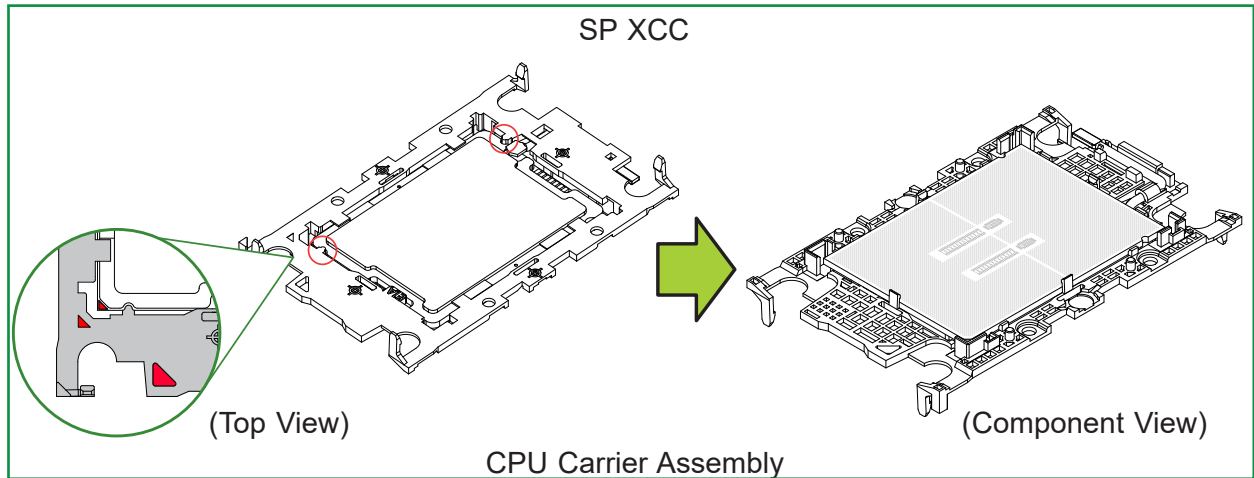
Creating the PHM

After creating the processor carrier assembly, please follow the instructions below to mount the processor carrier into the heatsink to form the PHM.

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

1. Turn the heatsink over with the thermal grease, which is on the reverse side of the heatsink, facing up. Pay attention to the two triangle cutouts (A, B) located at the diagonal corners of the heatsink as shown in the following drawings.

2. Hold the processor carrier component side facing up, and locate the triangle on the CPU and the triangle on the carrier. (Triangle indicates Pin 1.)

3. Using Pin 1 as a guide, turn the processor carrier assembly over with the gold contacts facing up. Locate Pin 1 (A) on the processor and Pin 1 (a) on the processor carrier assembly.

4. Align the corner marked a on the processor carrier assembly against the triangle cutout A on the heatsink, and align the corners marked b, c, and d on the processor assembly against the corners marked B, C, and D on the heatsinks.

5. Once they are properly aligned, place the corners marked a, b, c, and d on the processor carrier assembly into the corners of the heatsink marked A, B, C, and D making sure that all plastic clips are properly attached to the heatsink.

CPU Carrier Assembly (for 1U Heatsink SNK-P1046V)

(CPU Component Side and Heatsink Bottom Side)
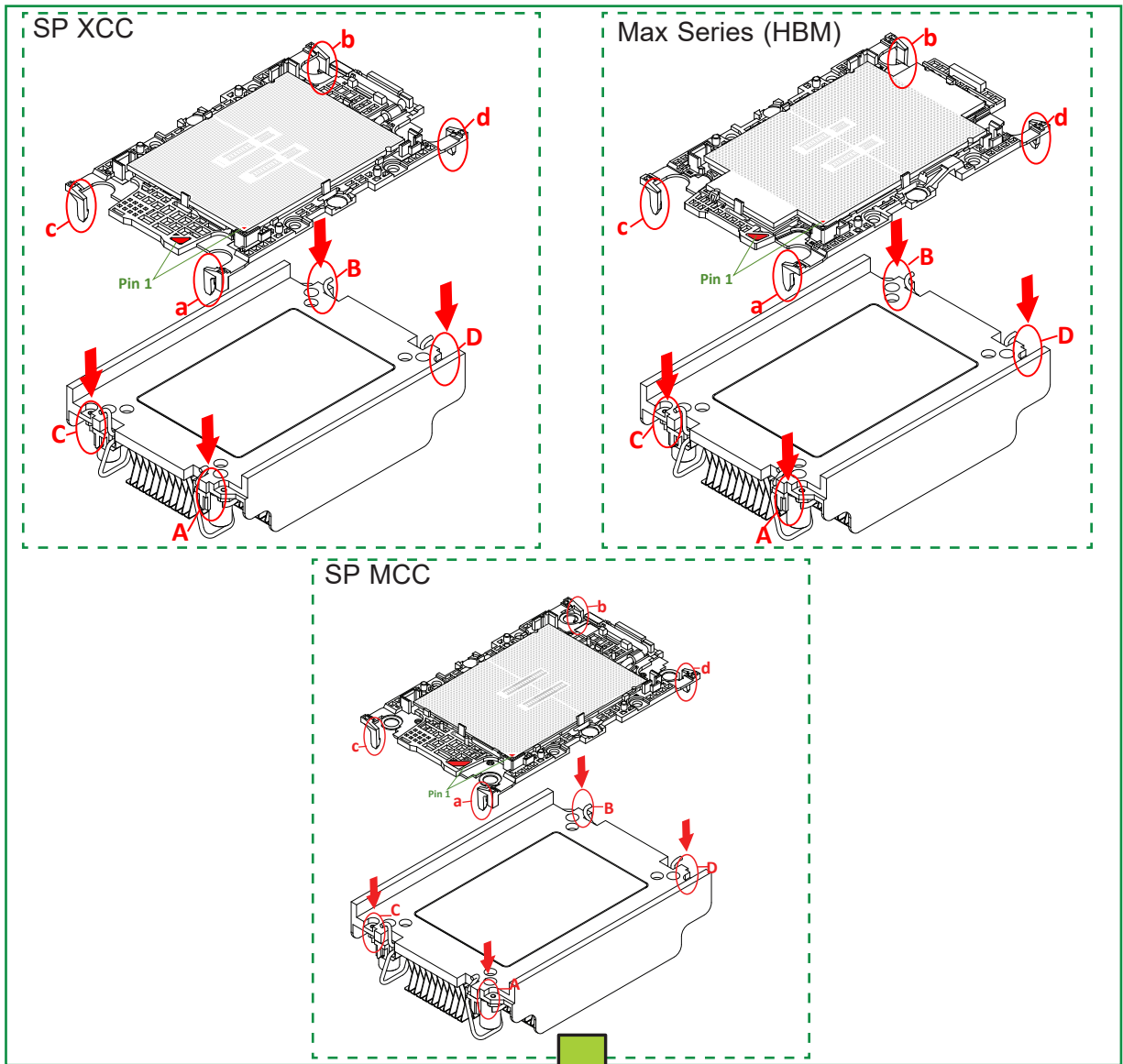
SP XCC

Max Series (HBM)

SP MCC

Processor Heatsink Module (PHM)
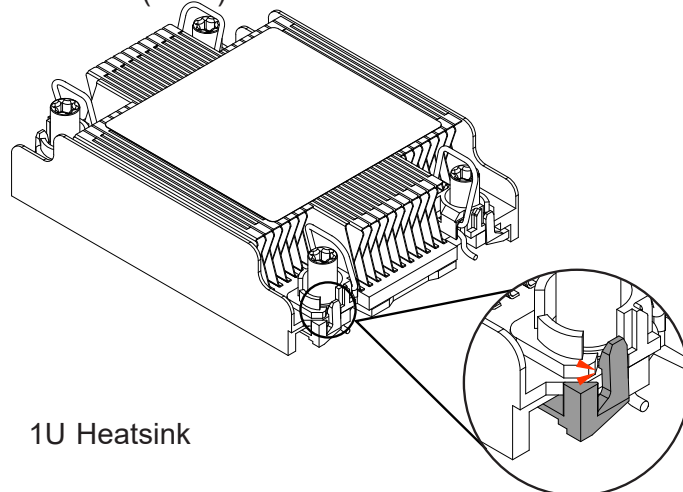
1U Heatsink

CPU Carrier Assembly (for 1U Heatsink SNK-P1046VM)

(CPU Component Side and Heatsink Bottom Side)

SP XCC

Max Series (HBM)

SP MCC

Processor Heatsink Module (PHM)
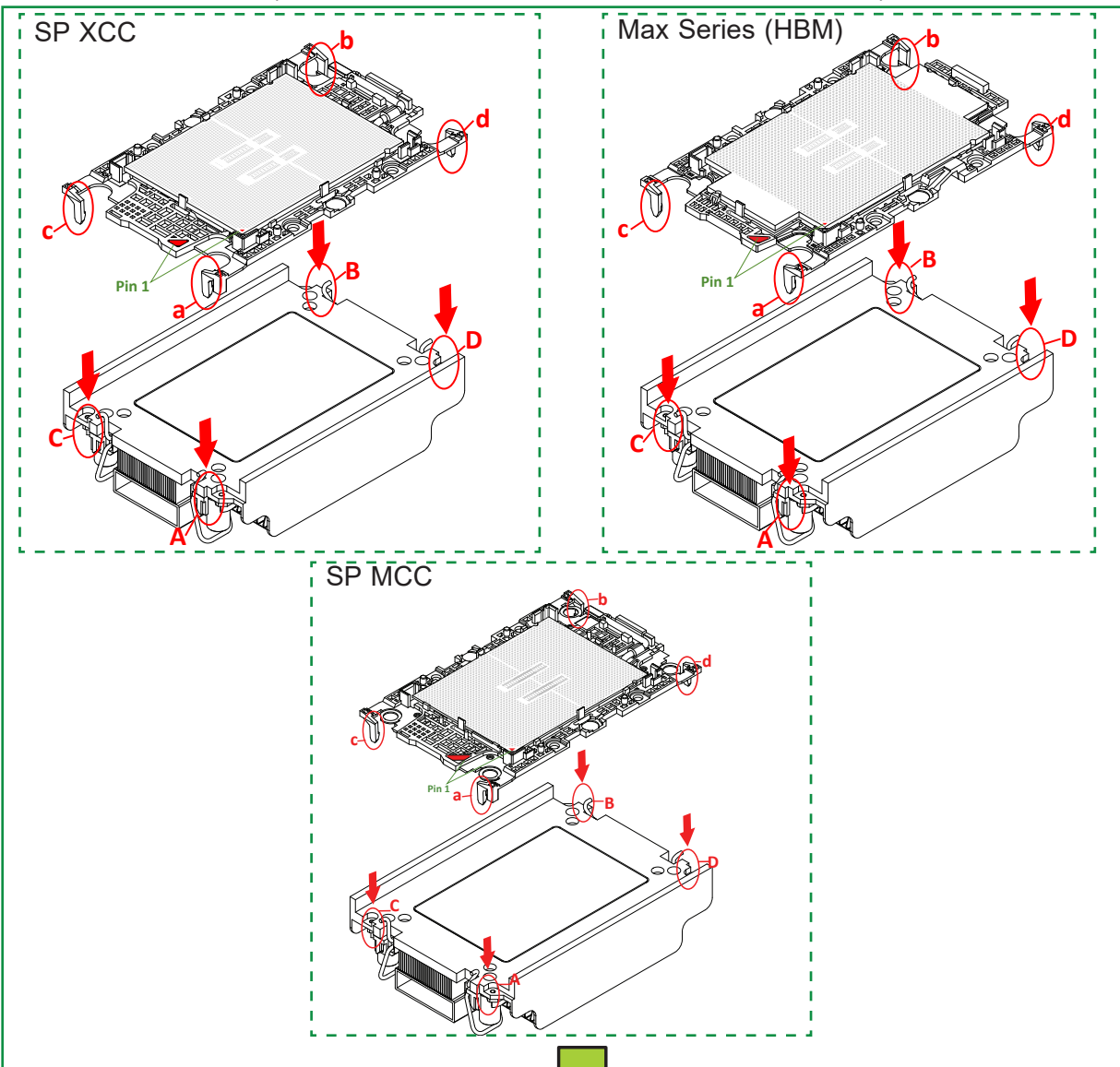
1U Heatsink

CPU Carrier Assembly (for 2U Heatsink)

(CPU Component Side and Heatsink Bottom Side)

SP XCC

b

d

c

Pin 1

a

B

D

C

A

Max Series (HBM)

b

d

c

Pin 1

a

B

D

C

A

SP MCC

b

d

c

Pin 1

a

B

D

C

A

Processor Heatsink Module (PHM)

2U Heatsink
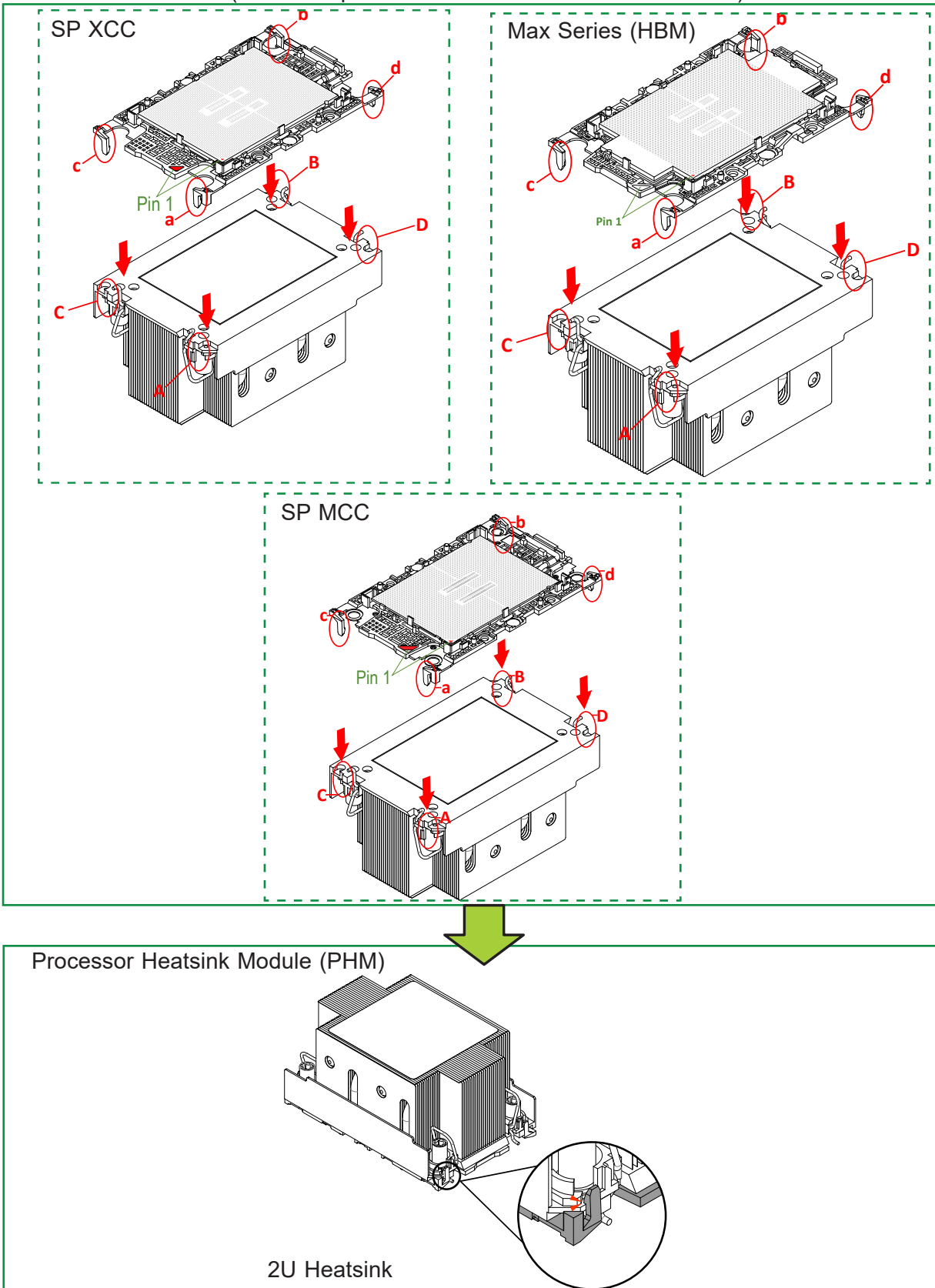
Preparing the CPU Socket for Installation

This motherboard comes with a plastic protective cover installed on the CPU socket. Remove it from the socket by following the instructions below:

1. Press the tabs inward.
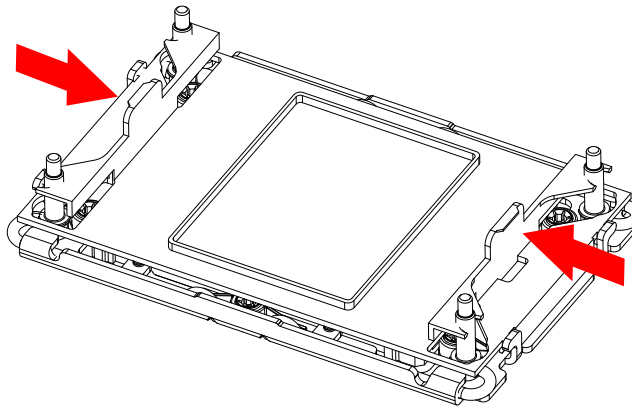
2. Pull up the protective cover from the socket.
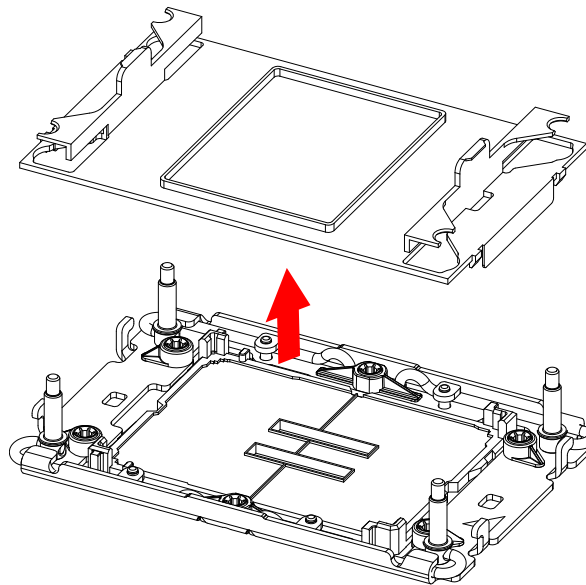
Preparing to Install the PHM into the CPU Socket

After assembling the Processor Heatsink Module, you are ready to install it into the CPU socket. To ensure the proper installation, please follow the procedures below:

1. Locate four threaded fasteners (a, b, c, d) on the CPU socket.

CPU Socket

(a, b, c, d: Threaded Fasteners)

CPU Socket Pin1
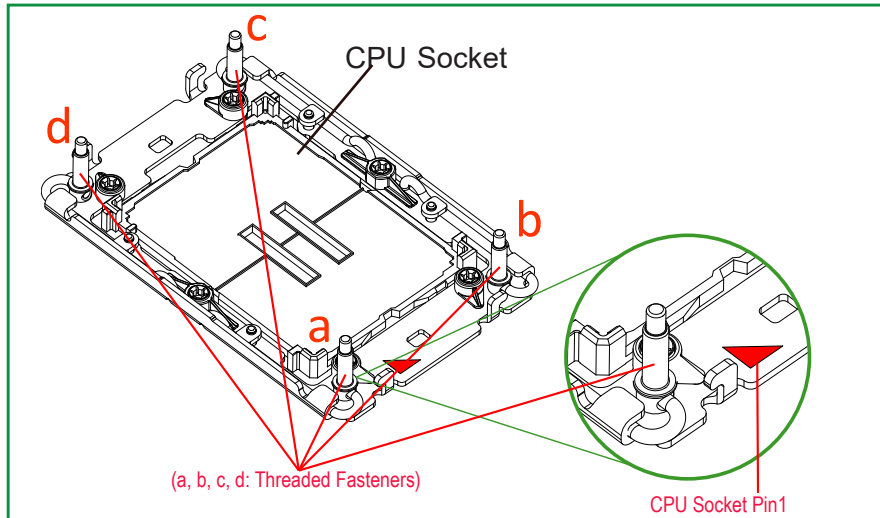
2. Locate four PEEK nuts (A, B, C, D) and four rotating wires (1, 2, 3, 4) on the heatsink as shown in the graphics below.

1U Heatsink (SNK-P1046V)

1U Heatsink (SNK-P1046VM)

Heatsink (Reverse Side)

Rotating Wire 2

A, B, C, D: Peek Nut
1, 2, 3, 4: Rotating Wire
a, b, c, d: Threaded Fastener

B

Rotating Wire 3

Rotating Wire 4

C

D

Rotating Wire
Peek Nut

A

Rotating Wire 1
Peek Nut

(Unlatched) (Latched)

b

d

c

a
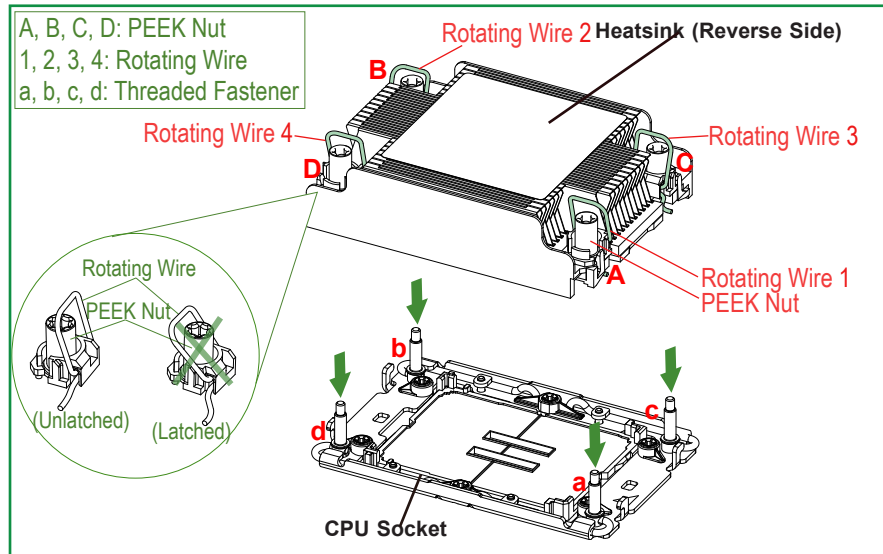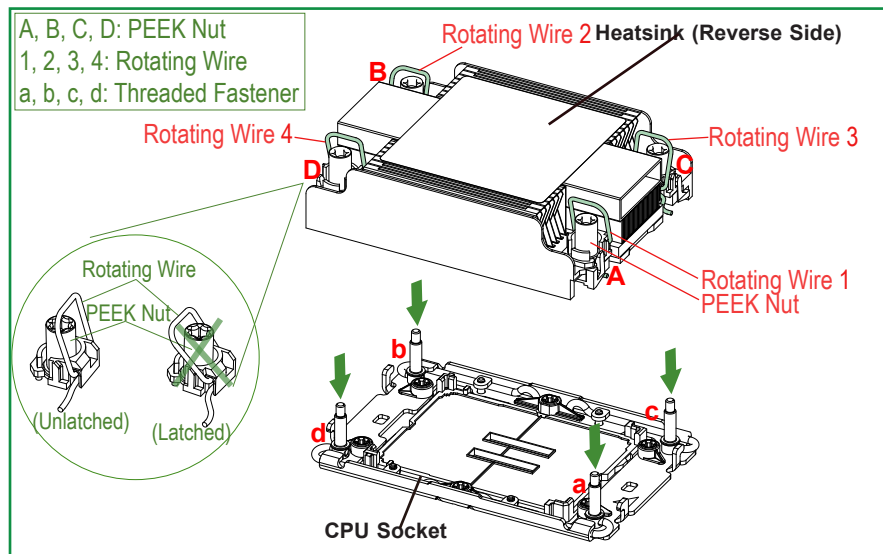
CPU Socket
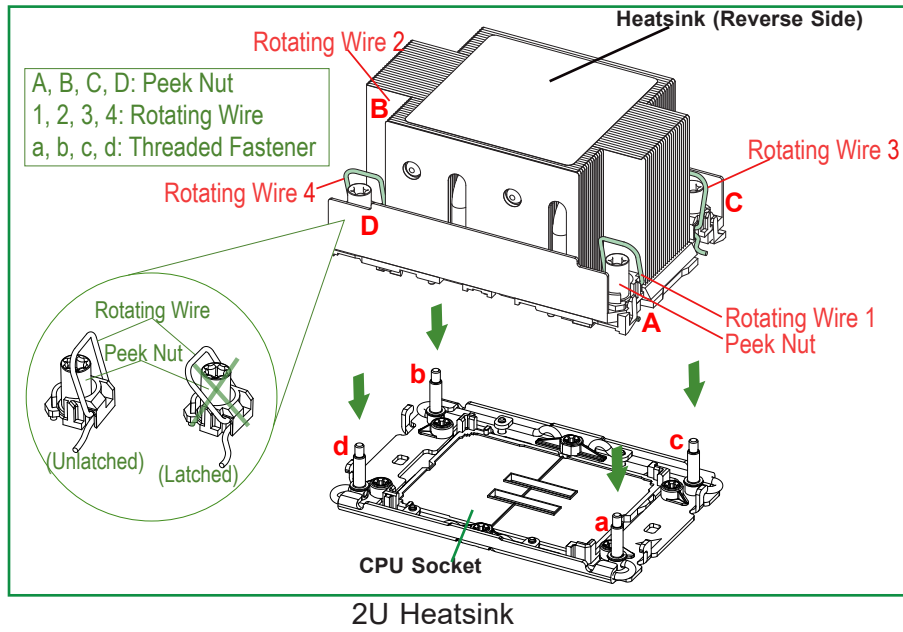
2U Heatsink

3. Check the rotating wires (1, 2, 3, 4) to make sure that they are at unlatched positions as shown in the drawing below before installing the PHM into the CPU socket.
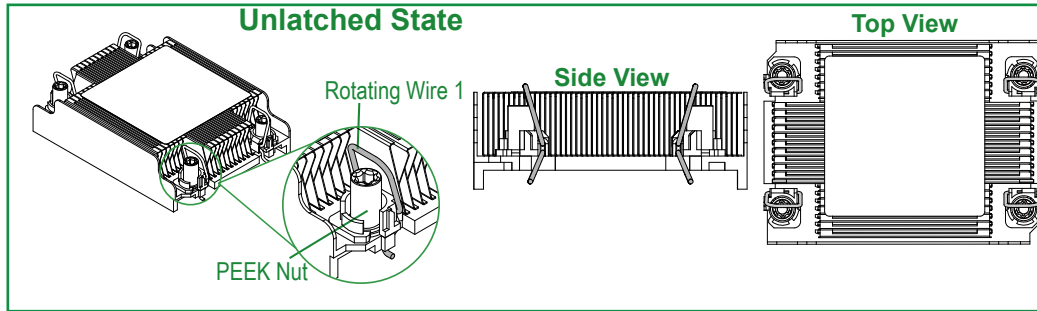
1U Heatsink (SNK-P1046V)
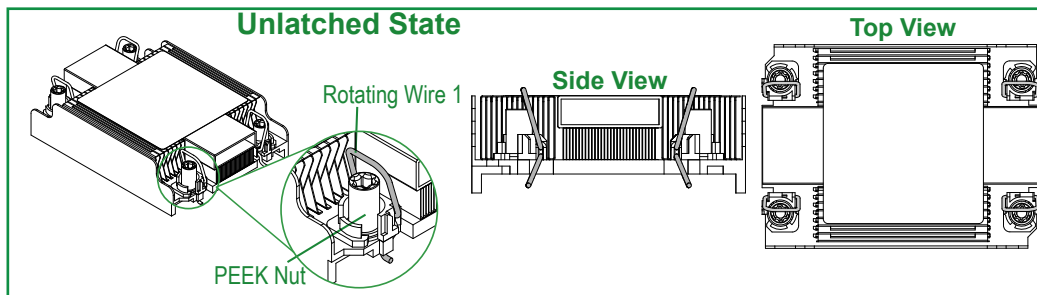
1U Heatsink (SNK-P1046VM)
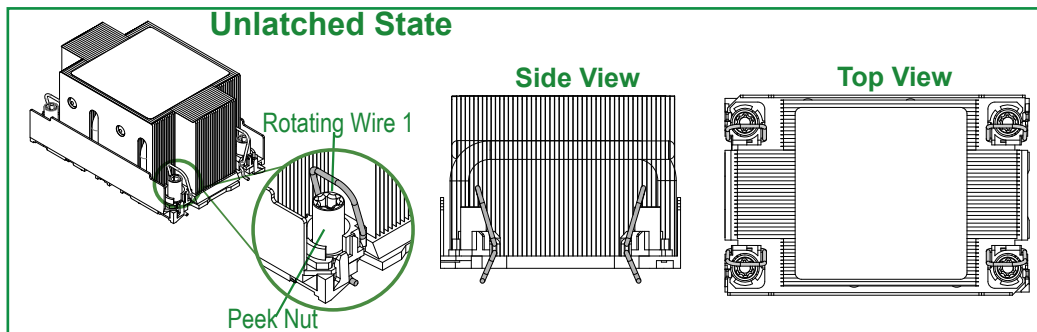
2U Heatsink

Installing the PHM into the CPU Socket

1. Align PEEK nut A, which is next to the triangle (Pin 1) on the heatsink, against threaded fastener a on the CPU socket. Then align PEEK nuts B, C, and D on the heatsink against threaded fasteners b, c, and d on the CPU socket, making sure that all PEEK nuts on the heatsink are properly aligned with the correspondent threaded fasteners on the CPU socket.

2. Once they are aligned, gently place the heatsink on top of the CPU socket, making sure that each PEEK nut is properly attached to its corresponding threaded fastener.

A, B, C, D:
PEEK Nut on the Heatsink

a, b, c, d:
Threaded Fastener on the CPU socket

1U Heatsink

A, B, C, D:
PEEK Nut on the Heatsink

a, b, c, d:
Threaded Fastener on the CPU socket

1U Heatsink

A, B, C, D:
Peek Nut on the Heatsink

B

C

D

A

b

d

c

a

a, b, c, d:
Threaded Fastener on the CPU socket
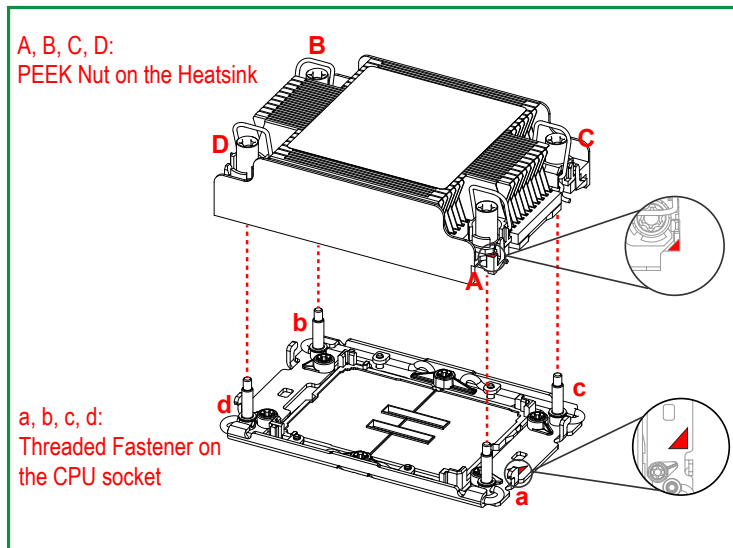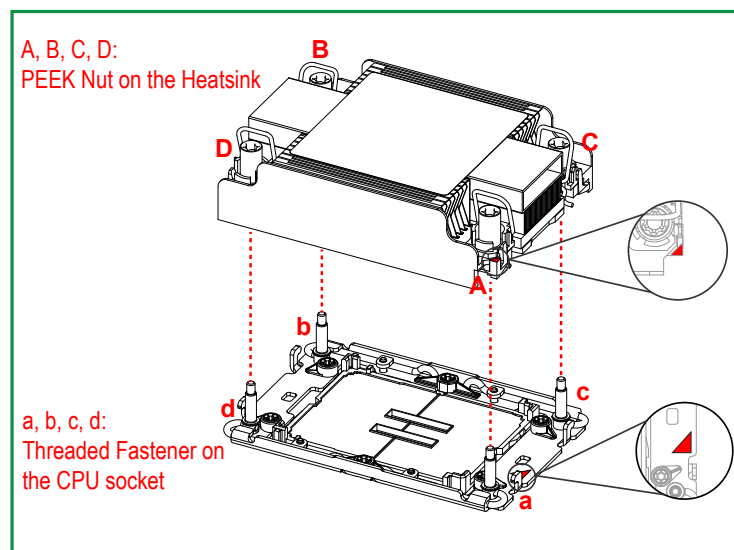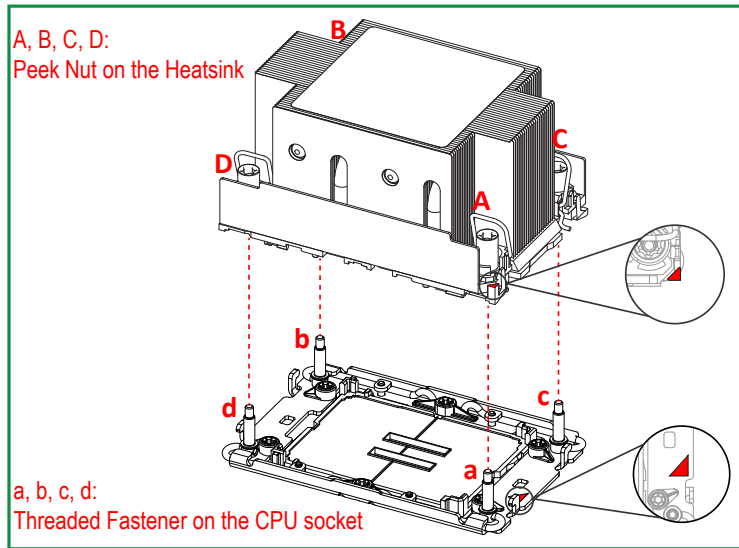
2U Heatsink

3. Press all four rotating wires outwards and make sure that the heatsink is securely latched onto the CPU socket.
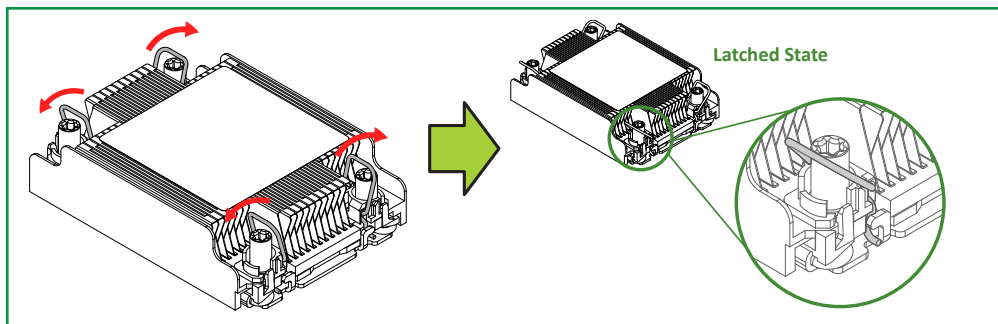
1U Heatsink (SNK-P1046V)
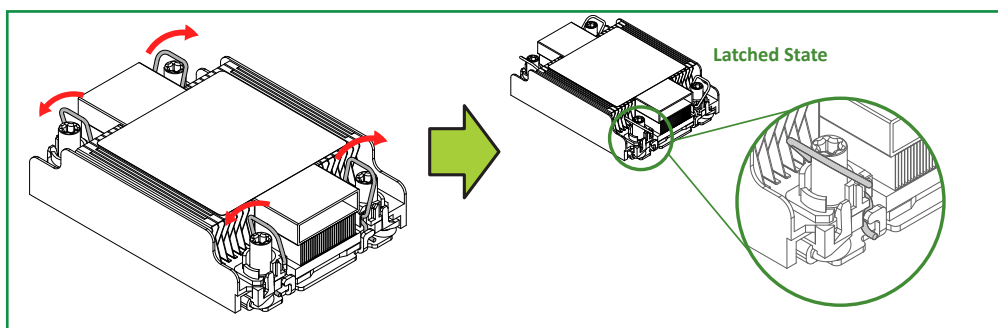
1U Heatsink (SNK-P1046VM)
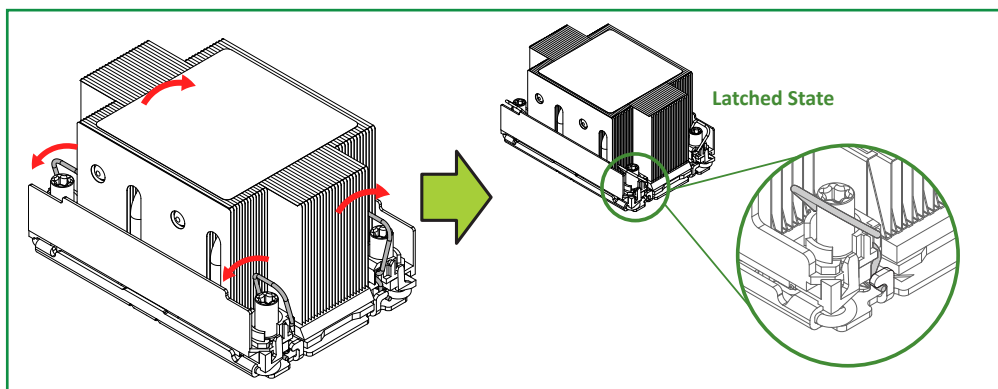
2U Heatsink

4. With a T30 bit torque driver set to a force of 8.0 in-lbf (0.904 N-m), tighten all PEEK nuts in the sequence of A, B, C, and D with even pressure. To avoid damaging the processor or socket, do not use excessive force when tightening the PEEK nuts. (For best durability, 8in-lbf torque is recommended.)

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 of the heatsink to ensure that the PHM is firmly attached to the CPU socket.
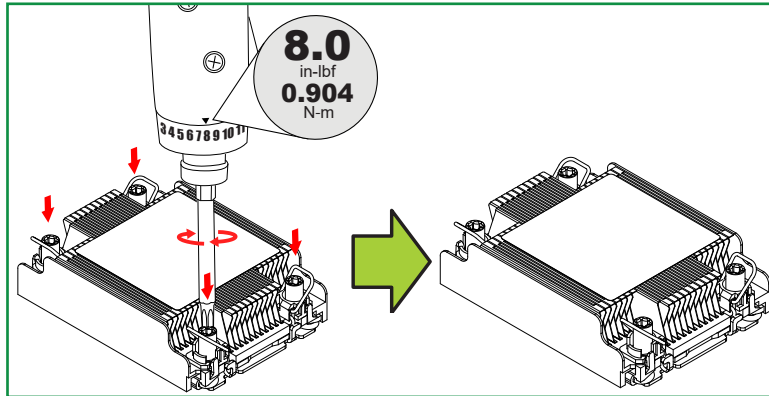
1U Heatsink (SNK-P1046V)
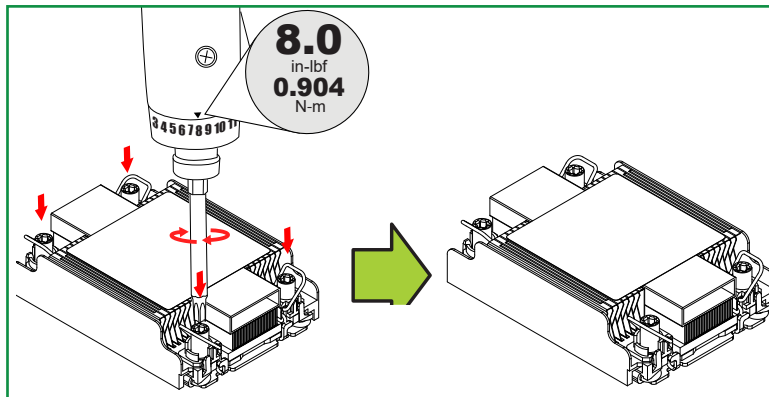
1U Heatsink (SNK-P1046VM)
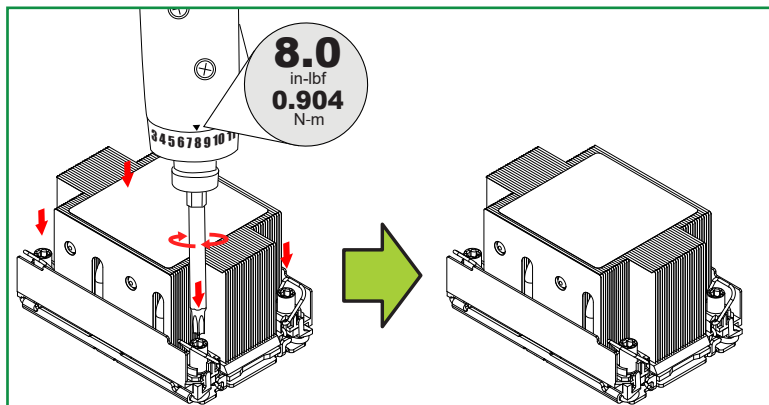
2U Heatsink

Removing the PHM from the CPU Socket

Before removing the PHM from the motherboard, be sure to shut down the system and unplug the power cables from the power supply. Then follow the steps below:

1. Use a T30 bit driver to loosen the four peek nuts on the heatsink in the sequence of A, B, C, and D.
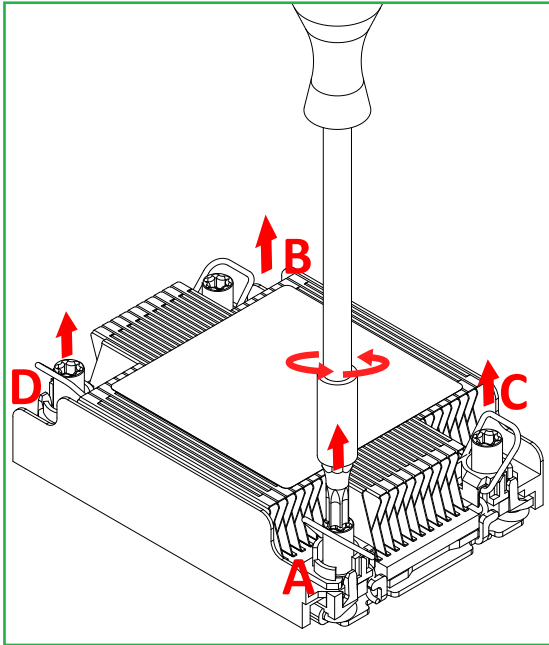
1U Heatsink (SNK-P1046V)
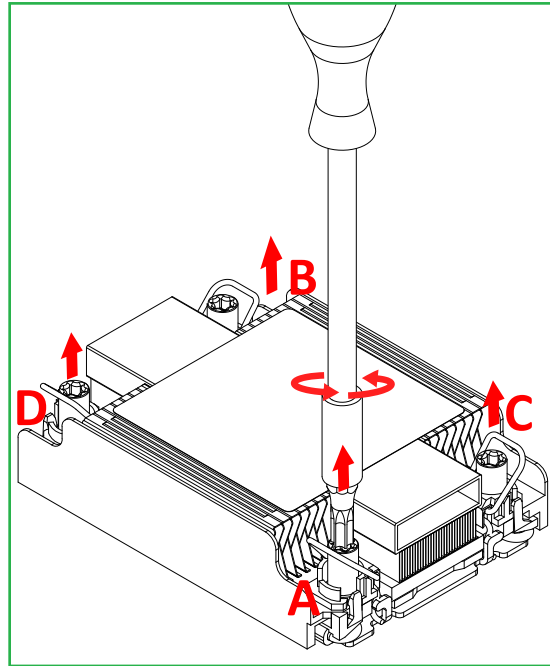
1U Heatsink (SNK-P1046VM)
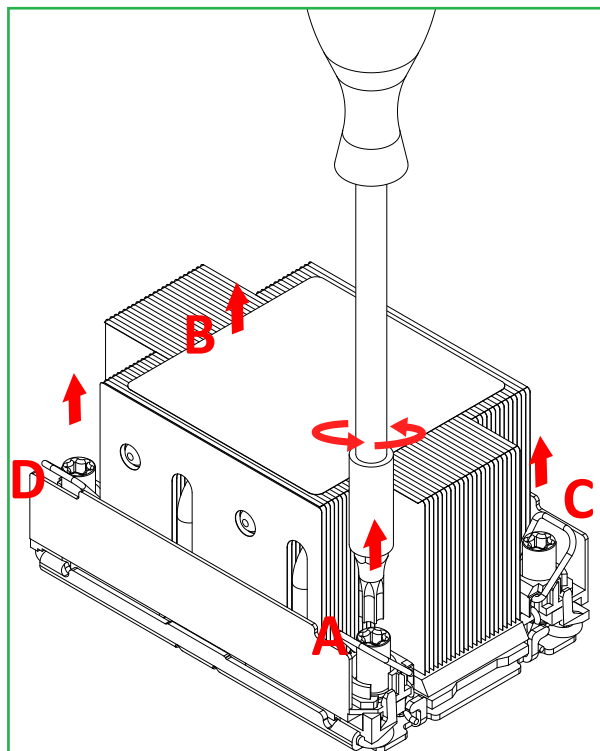
2U Heatsink

2. Once the peek nuts are loosened from the CPU socket, press the rotating wires inwards to unlatch the PHM from the socket as shown in the drawings below.
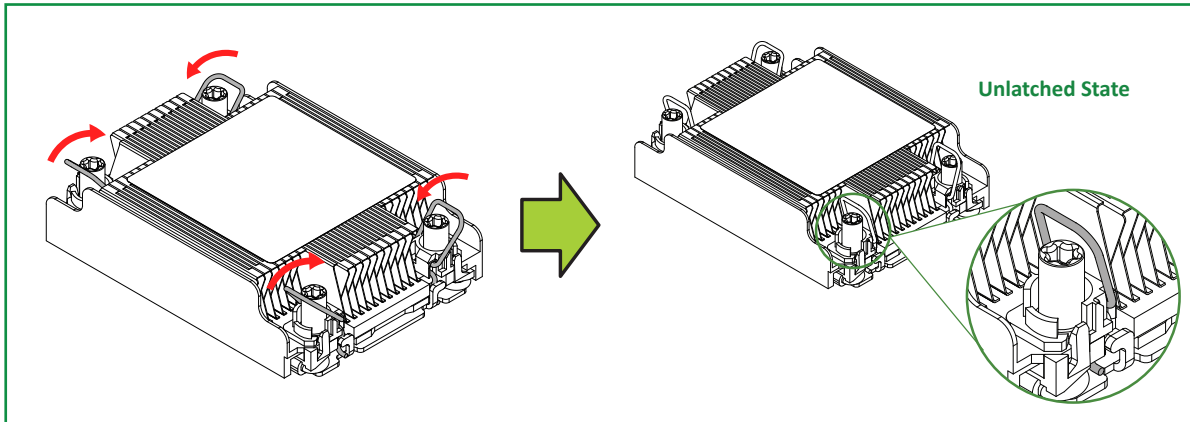
1U Heatsink (SNK-P1046V)
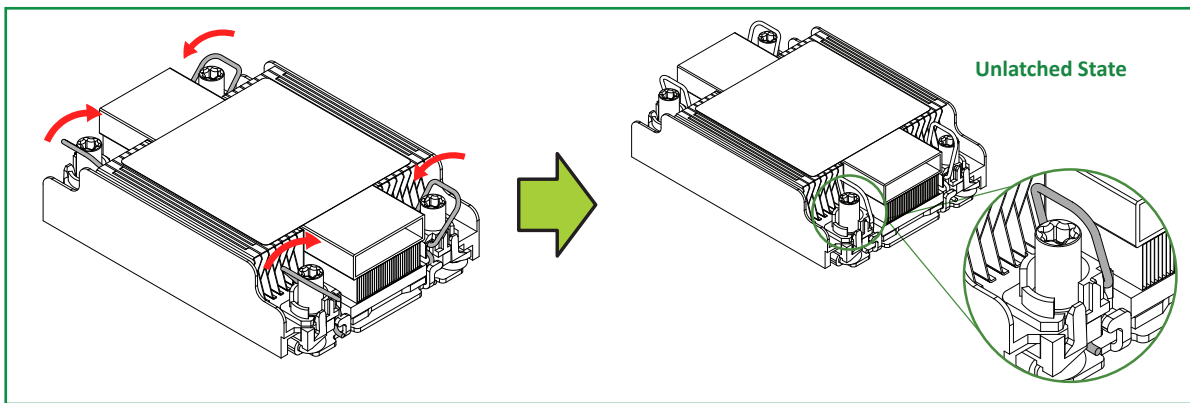
1U Heatsink (SNK-P1046VM)
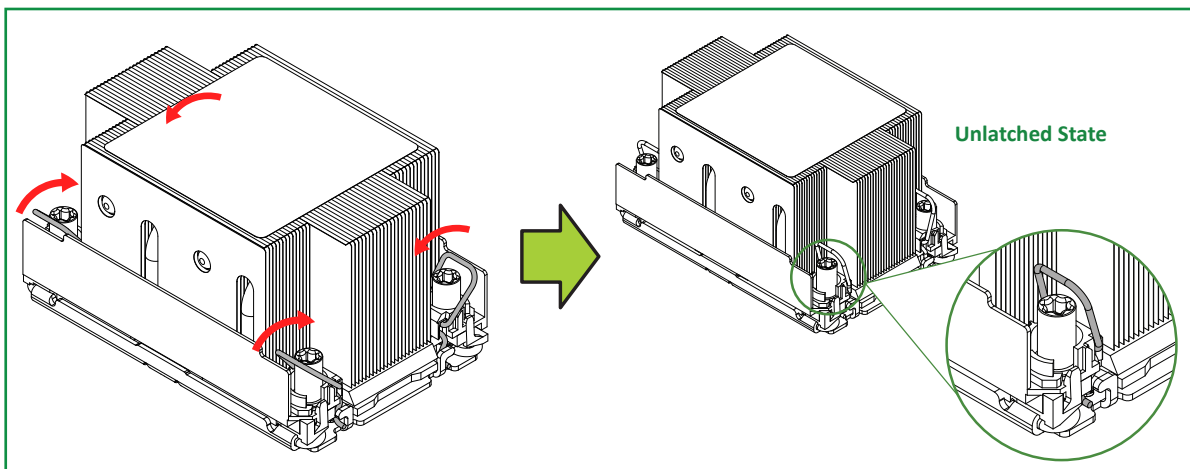
2U Heatsink

3. Gently pull the PHM upwards to remove it from the CPU socket.
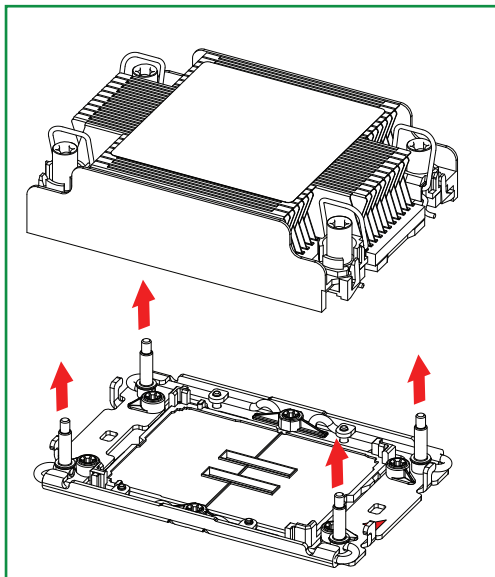
1U Heatsink (SNK-P1046V)
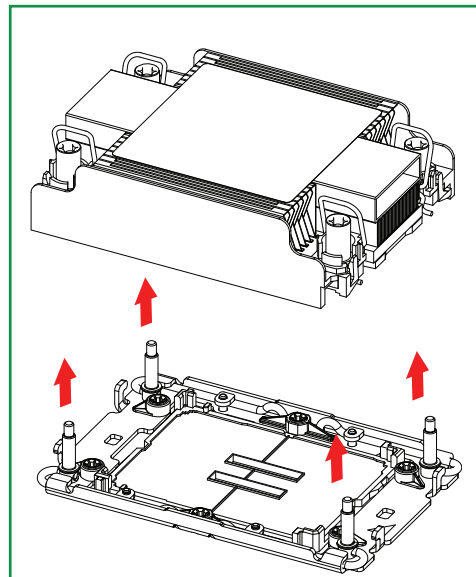
1U Heatsink (SNK-P1046VM)
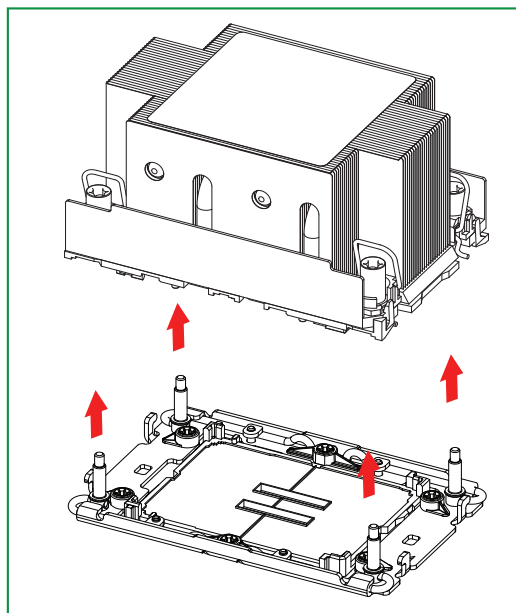
2U Heatsink

Removing the Processor Carrier Assembly from the PHM

To remove the processor carrier assembly from the PHM, please follow the steps below:

1. Detach the four plastic clips (marked a, b, c, d) on the processor carrier assembly from the four corners of the heatsink (marked A, B, C, D) as shown in the drawings below.

1U Heatsink SNK-P1046V(View of Component Side and Heatsink Bottom Side)

| SP XCC Series | Max Series (HBM) | SP MCC Series |

1U Heatsink SNK-P1046VM (View of Component Side and Heatsink Bottom Side)
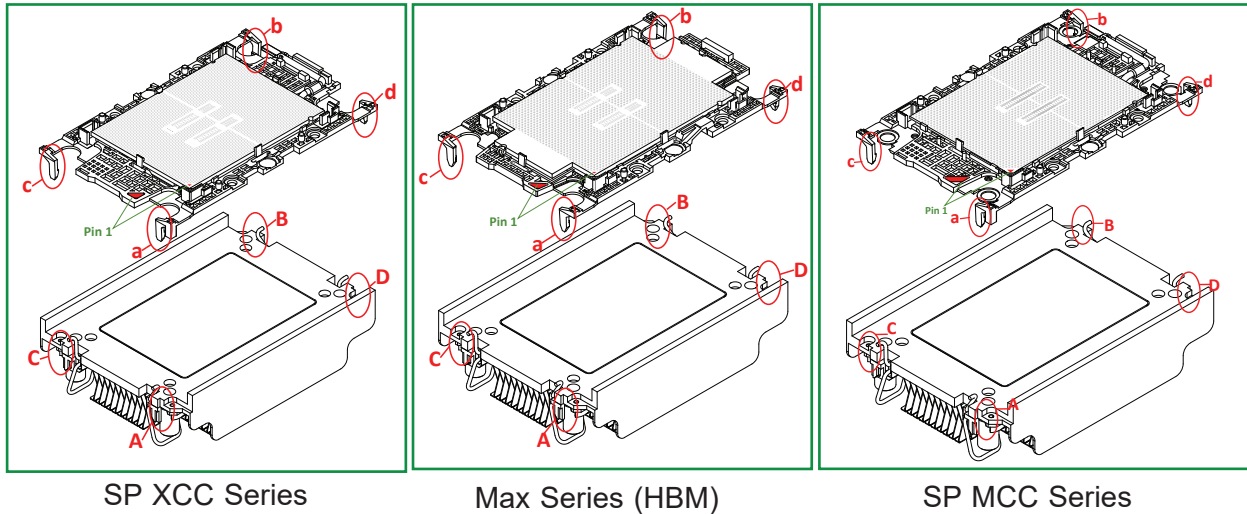
| SP XCC Series | Max Series (HBM) | SP MCC Series |
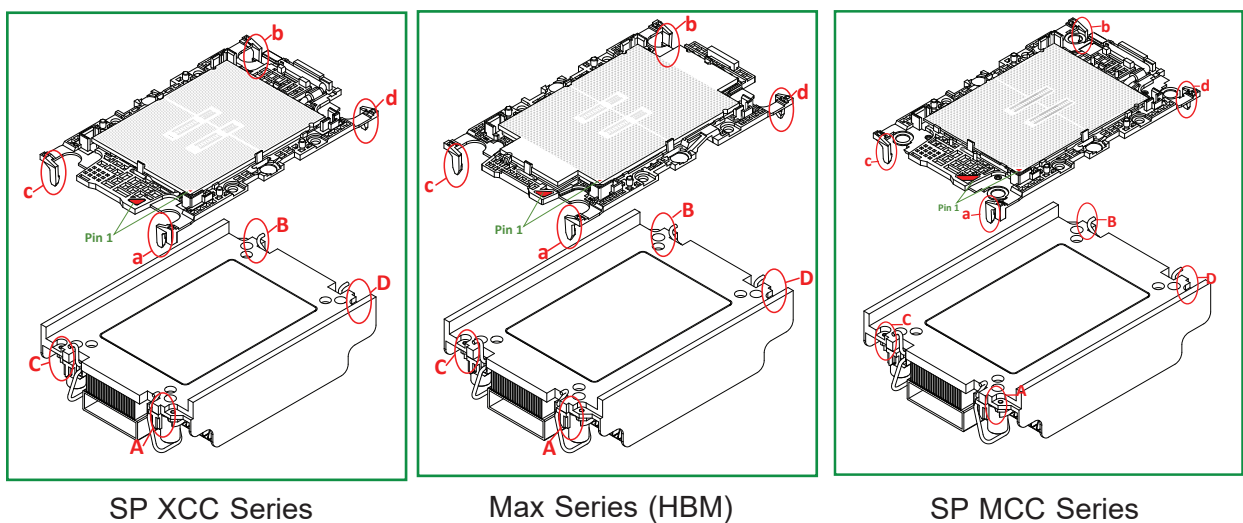
2U Heatsink (View of Component Side and Heatsink Bottom Side)
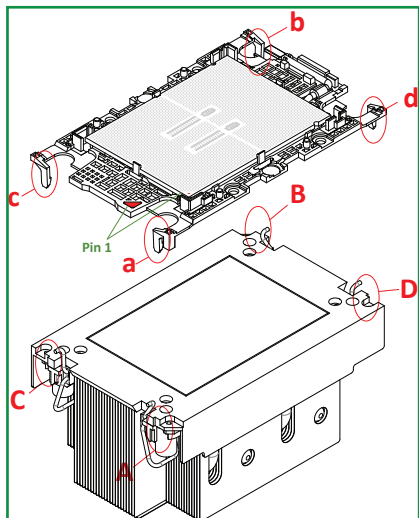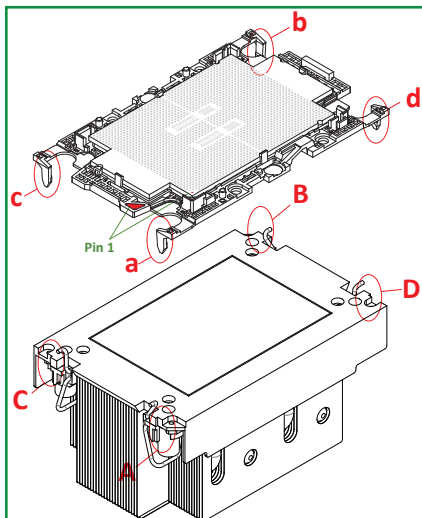
SP XCC Series   Max Series (HBM)   SP MCC Series
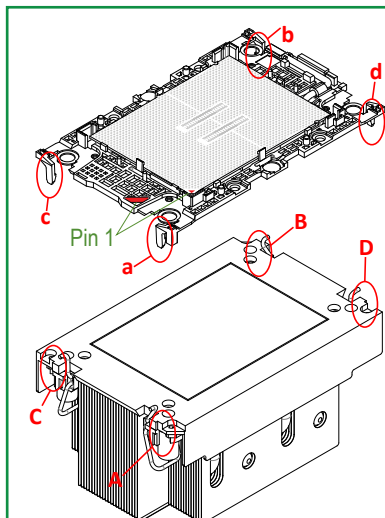
2. When all plastic clips are detached from the heatsink, remove the processor carrier assembly from the heatsink.

1U Heatsink SNK-P1046V(View of Component Side and Heatsink Bottom Side)
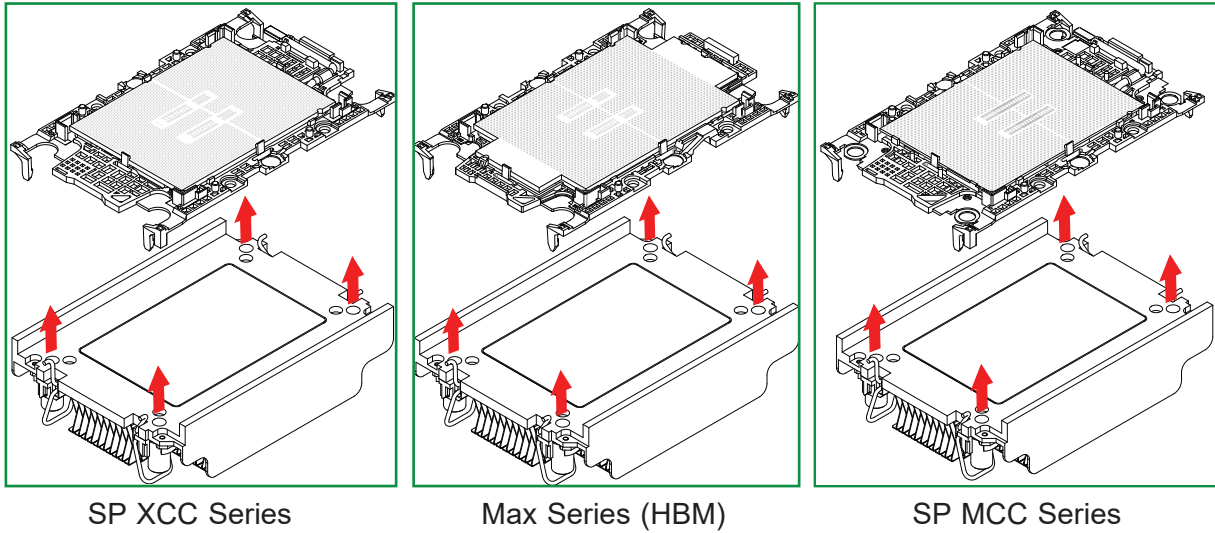
| SP XCC Series | Max Series (HBM) | SP MCC Series |

1U Heatsink SNK-P1046VM (View of Component Side and Heatsink Bottom Side)

| SP XCC Series | Max Series (HBM) | SP MCC Series |
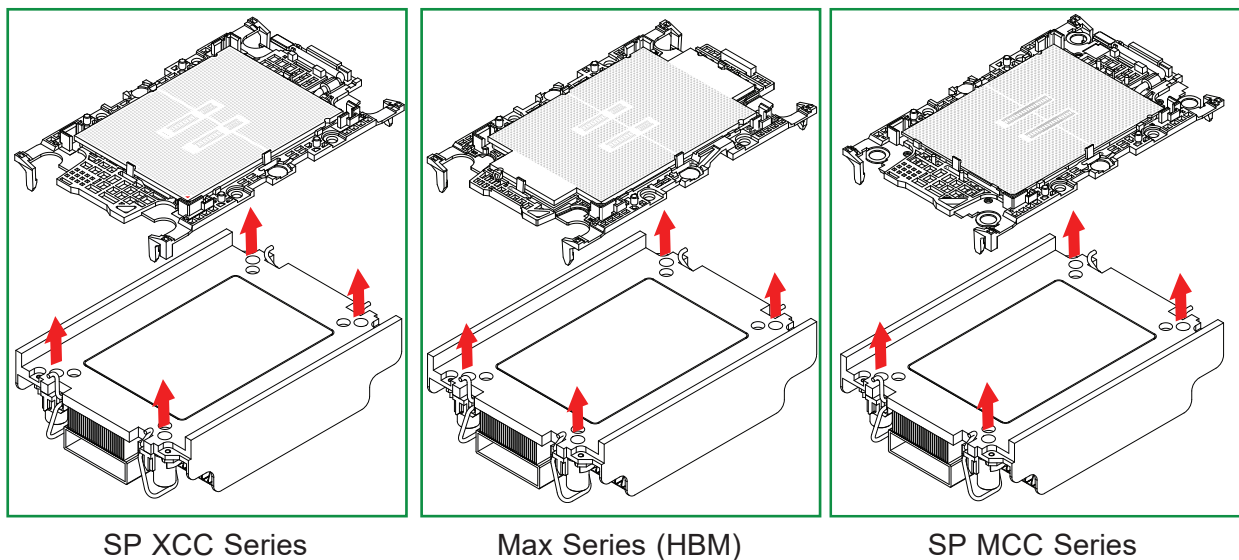
2U Heatsink (View of Component Side and Heatsink Bottom Side)
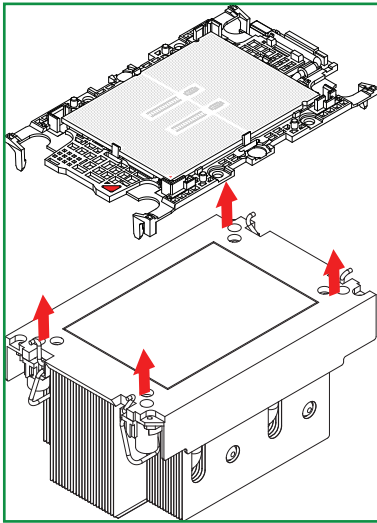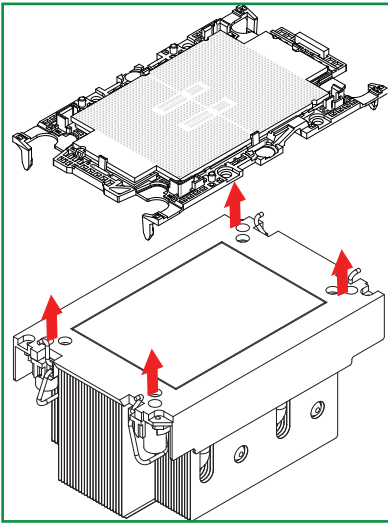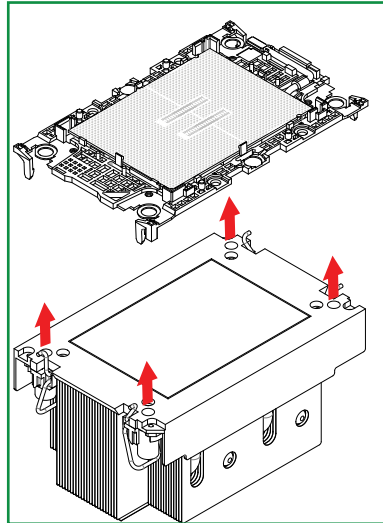
SP XCC Series   Max Series (HBM)   SP MCC Series

Removing the Processor from the Processor Carrier Assembly

Once you have removed the processor carrier assembly from the PHM, you are ready to remove the processor from the processor carrier by following the steps below.

1. Unlock the lever from its locked position and push the lever upwards to disengage the processor from the processor carrier as shown in the drawing on the right below.

CPU Carrier Assembly (carrier E1A)

CPU Carrier Assembly (carrier E1B)
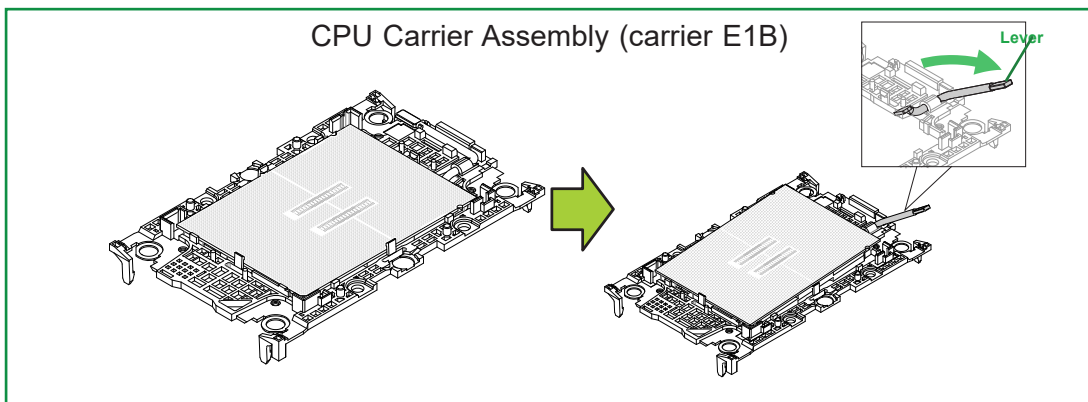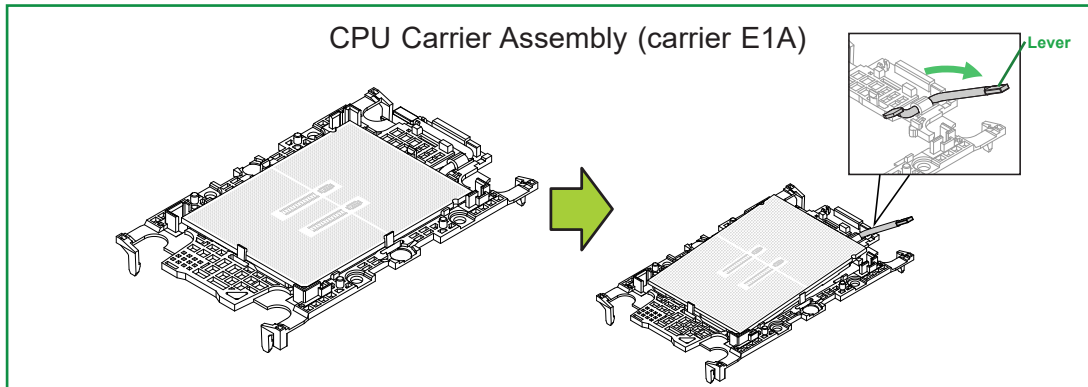
2. Once the processor is loosened from the carrier, carefully remove the processor from the processor carrier.

   Note: Please handle the processor with care to avoid damaging the processor and its pins.
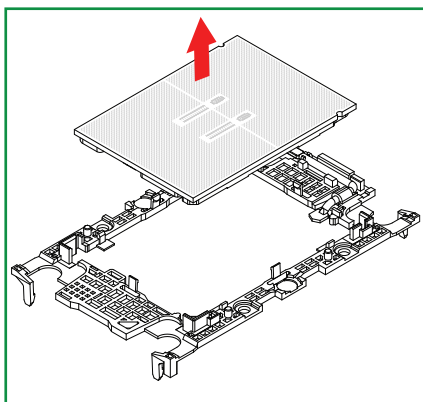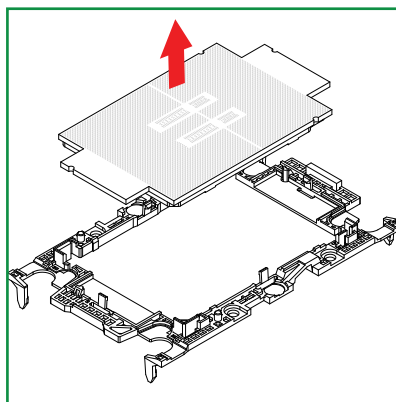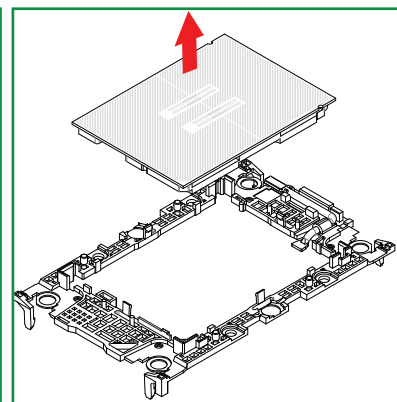
SP XCC Series   Max Series (HBM)   SP MCC Series

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
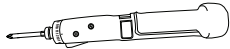
Torque Driver (1)

Phillips Screws (10)

Standoffs (10) (Only As Needed!)
(See below)
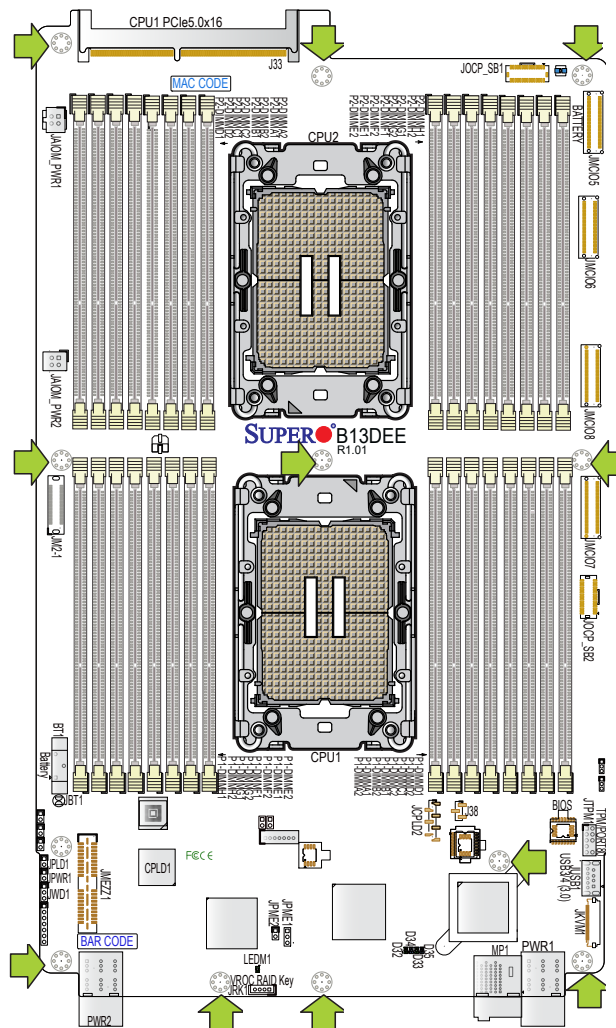
Location of Mounting Holes

Note 1: To avoid damaging the motherboard and its components, do not use a force greater than 8 lbf-in (0.904 N-m) on each mounting screw during motherboard installation.

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

Installing the Motherboard

1. Install the I/O shield into the back of the chassis, if applicable.

2. Locate the mounting holes on the motherboard. See the previous page for the location.
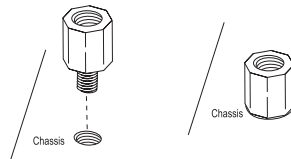
3. Locate the matching mounting holes on the chassis. Align the mounting holes on the motherboard against the mounting holes on the chassis.
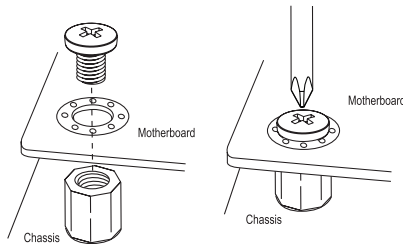
4. Install standoffs in the chassis as needed.

5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.

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

7. Repeat Step 5 to insert #6 screws into all mounting holes.

8. Make sure that the motherboard is securely placed in the chassis.

   Note: Images displayed are for illustration only. Your chassis or components might 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 memory modules to avoid any possible damage.

Memory Support

This motherboard supports 8TB (max.) 3DS RDIMM/RDIMM DDR5 ECC memory with speeds up to 5600 MT/s in 16 DIMM slots (or up to 4400 MT/s in 32 DIMM slots)

Note: Memory speed and capacity support depends on the processors used in the system. The 4th Gen Intel Xeon Scalable processors support DDR5 memory with speeds up to 4800MT/s (or up to 4400 MT/s in 32-DIMM configuration). The 5th Gen Intel Xeon Scalable processors support DDR5 memory with speeds up to 5600MT/s (or up to 4400 MT/s in 32-DIMM configuration).

DDR5 Memory Support for 4th/5th Gen Intel Xeon Scalable Processors

DDR5 Memory Support for the 4th Gen. Intel Xeon Scalable Processors					
Type	Ranks Per DIMM & Data Width (Stack)	DIMM Density and DIMM Capacity (GB)		Speed (MT/s); Voltage (V); DIMM Per Channel (DPC)	
				1DPC (Note)	2DPC
		16Gb (DRAM Density)	24Gb	1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB	4800	4400
	SRx4 (RC C)	32GB	48GB		
	SRx4 (RC F) 9x4	32GB	N/A		
	DRx8 (RC E)	32GB	48GB		
	DRx4 (RC A)	64GB	96GB		
	DRx4 (RC B) 9x4	64GB	N/A		
RDIMM 3DS	(4R/8R) x4 (RC A)	2H-128GB 4H-256GB	N/A		
LRDIMM/LRDIMM-3DS	N/A	N/A	N/A	Not Supported	Not Supported

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

Note 2: 24 GB XCC only with limited configs: 1DPC all DIMM types, 2DPC 96 GB only. Only 8 and 16 DIMM configs, no fallbacks.

Note 3: Memory speed will be 4800 MT/s 1DPC and 4400 MT/s 2DPC.

Note 4: Mixing DRAM Density (16 Gb/24 Gb) and/or Frequency is not allowed.

DDR5 Memory Support for the 5th Gen. Intel Xeon Scalable Processors				
Type	Ranks Per DIMM & Data Width (Stack)	DIMM Density and DIMM Capacity (GB)		Speed (MT/s); Voltage (V); DIMM Per Channel (DPC)
				1DPC (Note)	2DPC
		16Gb (DRAM Density)	24Gb	1.1V	
RDIMM	SRx8 (RC D)	16GB	24GB	5600	4400
	SRx4 (RC C)	32GB	48GB		
	SRx4 (RC F) 9x4	N/A	N/A		
	DRx8 (RC E)	32GB	48GB		
	DRx4 (RC A)	64GB	96GB		
	DRx4 (RC B) 9x4	N/A	N/A		
RDIMM 3DS	(4R/8R) x4 (RC A)	2H-128GB 4H-256GB	N/A	5600	
LRDIMM/LRDIMM-3DS	N/A	N/A	N/A	Not Supported	Not Supported

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

Note 2: 24 Gb, 24 GB, and 48 GB DRAM density is not supported in 2DPC.

Note 3: Memory speed will be 5600 MT/s 1DPC and 4400 MT/s 2DPC.

Note 4: For 1DPC 5600 speed, DDR5-5600 DIMMs are required.

Note 5: Mixing DRAM Density (16 Gb/24 Gb) and/or Frequency is not allowed.

Memory Population Table for 4th Gen Intel Xeon Scalable Processors

DDR5 Memory Population Table for X13DP Motherboards (with 32 DIMMs Installed)	
1 CPU:	**Memory Population Sequence**
1 CPU & 1 DIMM	P1-DIMMA1 P1-DIMME1 P1-DIMMB1 P1-DIMMF1
1 CPU & 2 DIMMs	P1-DIMMA1/P1-DIMMG1 P1-DIMMC1/P1-DIMME1
1 CPU & 4 DIMMs	P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1
1 CPU & 6 DIMM	P1-DIMMA1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1 P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1/P1-DIMMH1 P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMH1 P1-DIMMA1/P1-DIMMB1/P1-DIMMD1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1
1 CPU & 8 DIMMs	P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1
1 CPU & 12 DIMMs	P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1 P1-DIMMA1/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMH1/P1-DIMMH2
1 CPU & 16 DIMMs	P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1/P1-DIMMH2
2 CPUs: (Recommended)	**Memory Population Sequence**
2 CPUs & 2 DIMMs	**CPU1:** P1-DIMMA1, **CPU2:** P2-DIMMA1 **CPU1:** P1-DIMME1, **CPU2:** P2-DIMME1 **CPU1**: P1-DIMMB1, **CPU2:** P2-DIMMB1 **CPU1:** P1-DIMMF1, **CPU2:** P2-DIMMF1
2 CPUs & 4 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMG1, **CPU2:** P2-DIMMA1/P2-DIMMG1 **CPU1:** P1-DIMMC1/P1-DIMME1, **CPU2:** P2-DIMMC1/P2-DIMME1
2 CPUs & 8 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1 **CPU2:** P2-DIMMA1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1
2 CPUs & 10 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1 **CPU2:** P2-DIMMA1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1
2 CPUs & 12 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1 **CPU2:** P2-DIMMA1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1 **CPU1:** P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1/P1-DIMMH1 **CPU2:** P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1/P2-DIMMH1 **CPU1:** P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMH1 **CPU2:** P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMH1 **CPU1:** P1-DIMMA1/P1-DIMMB1/P1-DIMMD1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1 **CPU2:** P2-DIMMA1/P2-DIMMB1/P2-DIMMD1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1
2 CPUs & 16 DIMMs	**CPU1**: P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1 **CPU2**: P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1
2 CPUs & 22 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1/P1-DIMMH2 **CPU2:** P2-DIMMA1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1
2 CPUs & 24 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMH1/P1-DIMMH2 **CPU2:** P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1
2 CPUs & 32 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1/P1-DIMMH2 **CPU2:** P2-DIMMA1/P2-DIMMA2/P2-DIMMB1/P2-DIMMB2/P2-DIMMC1/P2-DIMMC2/P2-DIMMD1/P2-DIMMD2/P2-DIMME1/P2-DIMME2/P2-DIMMF1/P2-DIMMF2/P2-DIMMG1/P2-DIMMG2/P2-DIMMH1/P2-DIMMH2

Note: This memory configuration is recommended by Supermicro for optimal memory performance. Please use this configuration to maximize your memory performance.

DDR5 Memory Population Table for the B13DEE Motherboard (based on Max series ((HBM)) CPUs with 32 DIMMs Installed)	
1 CPU:	*Memory Population Sequence*
1 CPU & 1 DIMM	P1-DIMMA1 P1-DIMME1
1 CPU & 2 DIMMs	P1-DIMMA1/P1-DIMMG1 P1-DIMMC1/P1-DIMME1
1 CPU & 4 DIMMs	P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1
1 CPU & 8 DIMMs	P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1
1 CPU & 16 DIMMs	P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1/P1-DIMMH2
2 CPUs: *(Recommended)*	*Memory Population Sequence*
2 CPUs & 2 DIMMs	**CPU1:** P1-DIMMA1, **CPU2:** P2-DIMMA1 **CPU1:** P1-DIMME1, **CPU2:** P2-DIMME1
2 CPUs & 4 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMG1, **CPU2:** P2-DIMMA1/P2-DIMMG1 **CPU1:** P1-DIMMC1/P1-DIMME1, **CPU2:** P2-DIMMC1/P2-DIMME1
2 CPUs & 8 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1 **CPU2:** P2-DIMMA1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1
2 CPUs & 16 DIMMs	**CPU1**: P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1 **CPU2**: P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1
2 CPUs & 32 DIMMs	**CPU1:** P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1/P1-DIMMH2 **CPU2:** P2-DIMMA1/P2-DIMMA2/P2-DIMMB1/P2-DIMMB2/P2-DIMMC1/P2-DIMMC2/P2-DIMMD1/P2-DIMMD2/P2-DIMME1/P2-DIMME2/P2-DIMMF1/P2-DIMMF2/P2-DIMMG1/P2-DIMMG2/P2-DIMMH1/P2-DIMMH2

Notes:

1. Max series (HBM) processors support 1DPC (4800MT/s) / 2DPC (4400MT/s) to optimize the memory bandwidth. Max series (HBM) processors support 1, 2, 4, 8, or 16 DIMMs in Flat Mode and Cache Mode, and 0 DIMMs in HBM-Only mode. HBM-Only mode runs exclusively using HBM memory.

2. For the best memory performance in Flat mode and Cache mode, please use 4, 8, or 16 DIMM configurations. (At least one DIMM per memory controller for balanced configuration)

   4 DIMMs -> populate 1 DIMM/iMC* (*Integrated Memory Controller)

   8 DIMMs -> populate 1 DIMM/Channel, 2 DIMM/iMC

   16 DIMMs -> populate 2 DIMM/Channel, 4 DIMM/iMC

3. All other configurations not listed above are not supported.

4. For 2-Socket design, each socket has to be populated identically.

DIMM Installation

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

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

Release Tabs
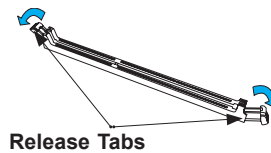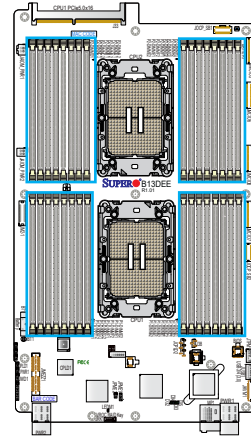
3. Align the key of the memory module with the receptive point on the memory slot.

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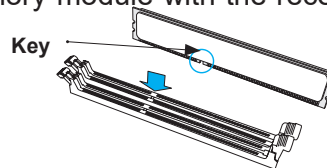
4. Align the notches on both ends of the module against the receptive points on the ends of the slot.

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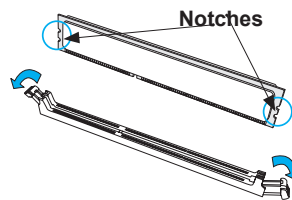
5. Push both ends of the module straight down into the slot until the module snaps into place.

6. Press the release tabs to the lock positions to secure the memory module into the slot.

Push both ends straight down into the memory slot.
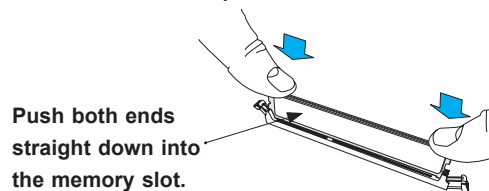
DIMM Removal

Press both release tabs on the ends of the memory module to unlock it. Once the memory module has been loosened, remove it from the memory slot.
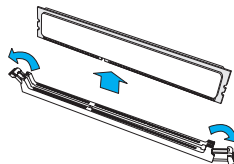
Warning! Please do not use excessive force when pressing the release tabs on the ends of the DIMM socket to avoid causing any damage to the memory module or the DIMM socket. Please handle memory modules with care. Carefully follow all the instructions given on page 1 of this chapter to avoid ESD-related damages done to your memory modules or components.

2.5 Connectors and Headers

Power Connectors

This motherboard supports two main power connectors (PWR1/PWR2) that provide power to your system, two 4-pin AIOM power connectors (JAIOM_PWR1/JAIOM_PWR2) that are used for the devices on advanced IO modules, and a 2-pin power connector (JPWR1) used for the Mezzanine card. Be sure to use appropriate power cables to connect these power connectors to your power supply to ensure adequate power to your system. It is also strongly recommended that you use a high quality power supply with SSI compliance.

> **Important:** To avoid damaging the power supply or the motherboard, be sure to provide adequate power to your system by using proper power cables to connect the power connectors mentioned above to your power supply. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.

1. PWR1: Main System Power Connector (#1)

2. PWR2: Main System Power Connector (#2)

3. JAIOM_PWR1: AIOM PWR Connector (#1)

4. JAIOM_PWR2: AIOM PWR Connector (#2)

5. JPWR1: Mezzanine card PWR Connector

MEZZ1 Card Connector

The Mezzanine card connector, located at MEZZ1, supports a PCIe Gen 5 riser card. Install a PCIe 5.0 x16 riser card on MEZZ1 connector for Mezzanine card support. Refer to the layout below for the location of MEZZ1 slot.

1. MEZZ1: Mezzanine Card Slot

25G Midplane

A 25G Midplane is located at MP1 on the rear side of the system. This Midplane supports 25GbE Ethernet connection for your motherboard. Please refer to the LED Indicator section for LAN LED information.

1. Midplane (MP1)
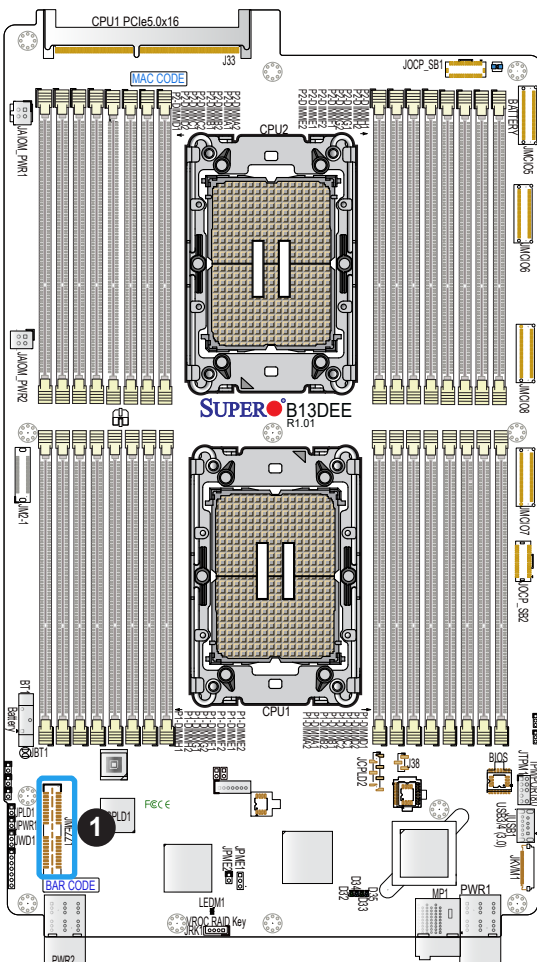
TPM/Port 80 Header

The JTPM1 header is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from Supermicro (optional). A TPM/Port 80 connector is a security device that supports encryption and authentication in hard drives. It allows the motherboard to deny access if the TPM associated with the hard drive is not installed in the system. See the layout below for the location of the TPM header. Please go to the following link for more information on the TPM: http://www.supermicro.com/manuals/other/TPM.pdf.

✎ **Note**: For TPM support, an optional part is needed. Contact Supermicro Technical Support for more information.

Trusted Platform Module Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	+3.3V	2	SPI_CS#
3	RESET#	4	SPI_MISO
5	SPI_CLK	6	GND
7	SPI_MOSI	8	NC
9	+3.3V Stdby	10	SPI_IRQ#
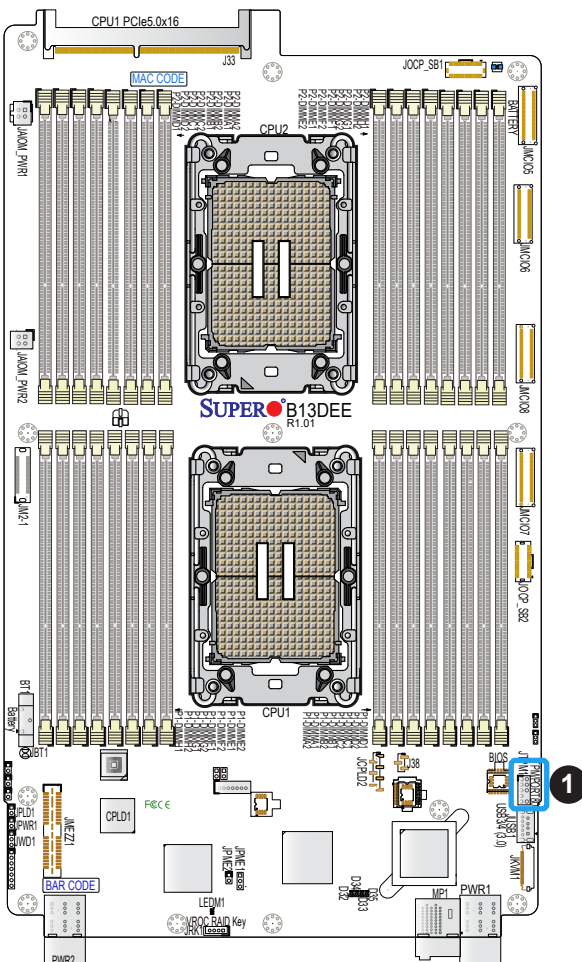
1. TPM/Port80 Header

VROC RAID Key Header

A VROC RAID Key header is located at JRK1 on the motherboard. Install a VROC RAID Key on JRK1 for NVMe RAID support as shown in the illustration below. Please refer to the layout below for the location of JRK1.

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

Intel VROC Key Pin Definitions	
Pin#	Definition
1	Ground
2	3.3V Standby
3	Ground
4	PCH RAID Key

VROC Key

VROC Key Header (JRK1)
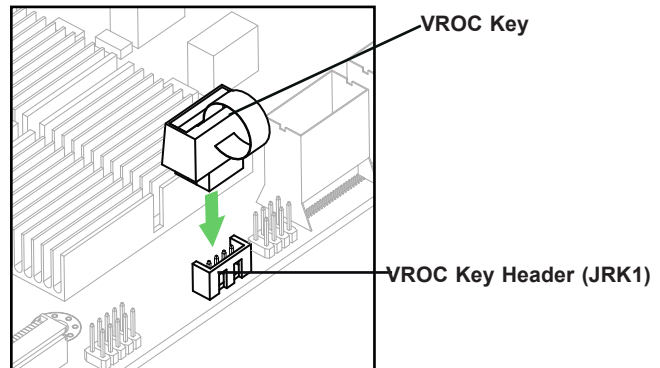
Note: The graphics contained in this user's manual are for illustration only. The components installed in your system may or may not look exactly the same as the graphics shown in the manual.
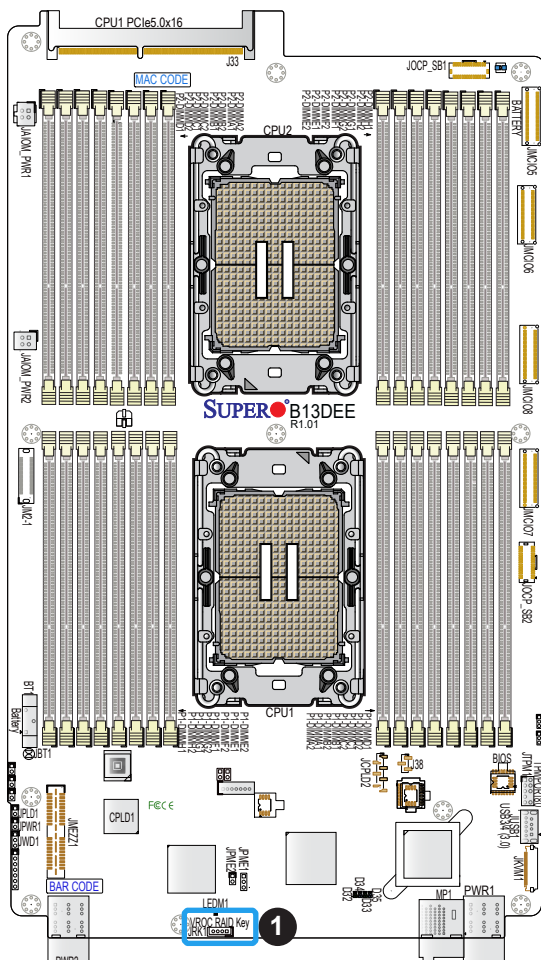
1. VROC RAID Key Header (JRK1)

PCIe 5.0 M.2 Slot (for NVMe Only)

The B13DEE motherboard has one PCIe 5.0 M.2 slot, which is located at JM2-1. M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. The M.2 slot on this motherboard supports PCIe 5.0 x4 M.2 NVMe SSDs in the 2280 form factor. Refer to the layout below the location of the M.2 slot.

1. M.2 Slot (JM2-1)

KVM Support

A KVM support connector is located at JKVM1. This connector provides Keyboard, video display, and mouse connections. Refer to the layout below the location of JKVM1.

1. KVM Connector (JKVM1)

PCIe 5.0 x8 MCIO Connectors

Four PCIe 5.0 x8 Mini Cool Edge IO (MCIO) Connectors 5/6/7/8 are located at JMCIO5 ~ JMCIO8. These connectors can be used for GPU/AIOM (Advanced IO Module) riser cards.

Refer to the layout below for the locations of JMCIO5 ~ JMCIO8.
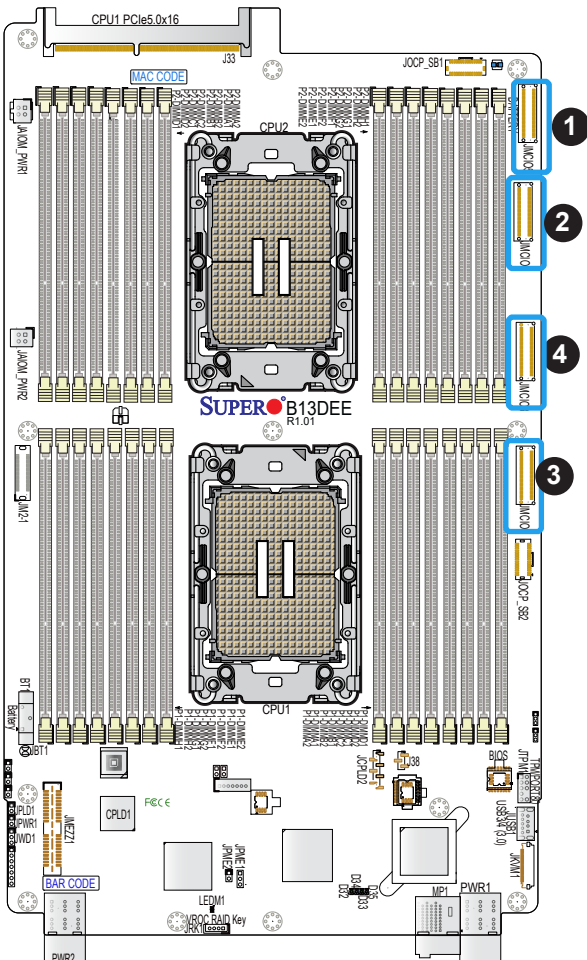
1. JMCIO5
2. JMCIO6
3. JMCIO7
4. JMCIO8

Universal Serial Bus (USB) 3.0 Header

A USB connector that supports two USB 3.0 ports (Port 3/Port 4) is located at JUSB1. These USB ports can be used for USB support via USB cables (not included). Refer to the layout below for the location of JUSB1.

1. USB 3.0 Port3/Port4 (JUSB1)

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 Pin 1 and Pin 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.
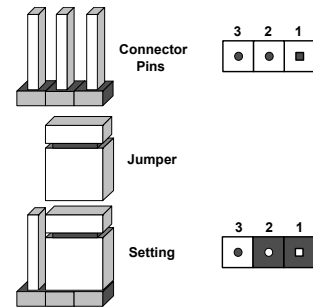
Watch Dog Timer Jumper

JWD1 controls the function of the Watch Dog timer. Close pins 1-2 of JWD1 for the Watch Dog timer to reset the system if an application hangs. Close pins 2-3 for Watch Dog to generate a non-maskable interrupt signal for the application that hangs. Watch Dog must also be enabled in BIOS. The default setting is Reset.

Note: When Watch Dog is enabled, the user needs to write their own application software to disable it.

Watch Dog Jumper (JWD1) Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Reset
Pins 2-3	NMI
Open	Disabled

1. Watch Dog Timer Enable (JWD1)
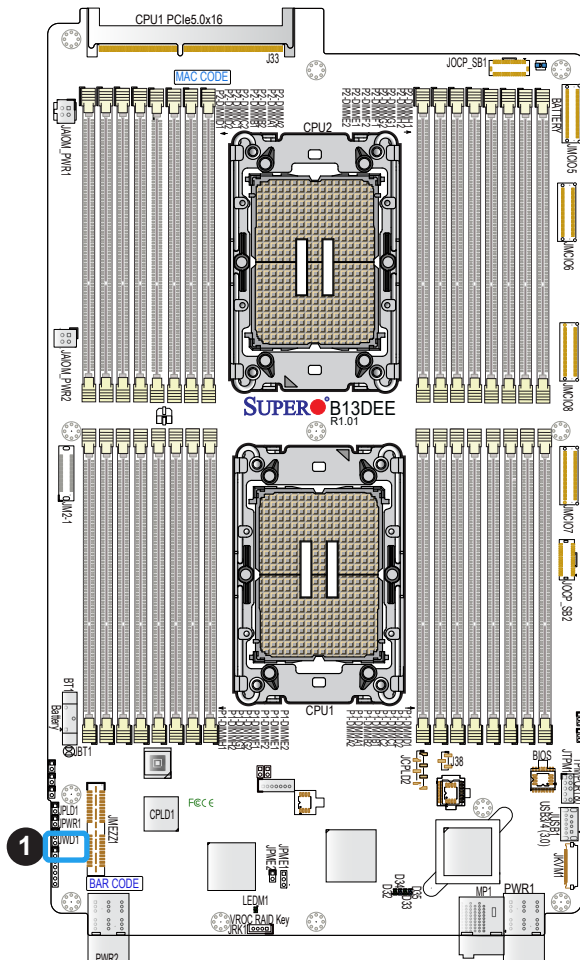
CMOS Clear

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 and remove the battery from the motherboard.

3. Short the CMOS pads, JBT1, with a metal object such as a small screwdriver for at least four seconds.

4. Remove the screwdriver (or shorting device).

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

> **Note**: Clearing CMOS will also clear all passwords.

1. Clear CMOS (JBT1)
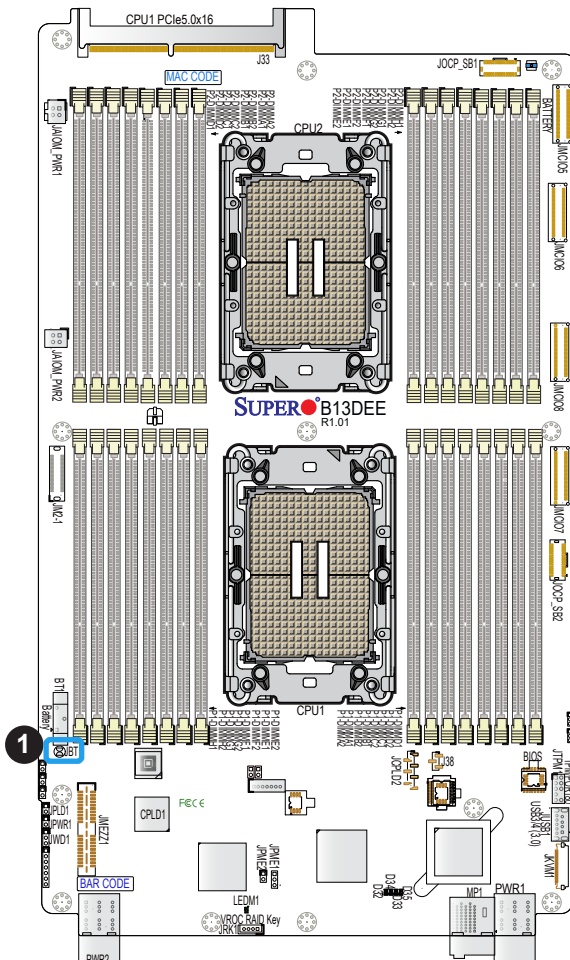
ME Recovery

JPME1 is used for ME Firmware Recovery mode, which will limit system resource for essential function use only without putting restrictions on power use. In the single operation mode, online upgrade will be available via Recovery mode.

ME Recovery (JPME1) Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Normal **(Default)**
Pins 2-3	ME Recovery

1. ME Recovery (JPME1)

Manufacturing Mode Select

Close JPME2 to bypass SPI flash security and force the system to use Manufacturing Mode, which will allow the user to flash the system firmware from a host server to modify system settings. See the table below for jumper settings.

Manufacturing Mode Select (JPME2) Jumper Settings	
Jumper Setting	Definition
Off	Normal **(Default)**
On	Manufacturing Mode

1. Manufacturing Mode Select (JPME2)

2.7 LED Indicators

BMC Heartbeat LED Indicator

A BMC (Baseboard Management Controller) Heartbeat LED is located at LEDM1. When this LED blinks green, the BMC is active. During a BMC reset or a cold reboot, the LED turns solid green. Refer to the table below for details.

BMC Heartbeat LED Status		
Color/State		**Definition**
LEDM1	Green: Blinking	BMC: Active (Normal)
	Green: Solid On	During a BMC reset or a cold system reboot

1. BMC Heartbeat LED

HDD32/HDD33 Heartbeat LED Indicators

Two HDD Heartbeat LED indicators are located at D32 and D33 on the motherboard. D32 is used for HDD0, and D33 is for HDD1. These LEDs are used to indicate if it is safe for the user to remove HDD devices from the system. Refer to the table below for more information.

HDD0 (D32)/HDD1(D33) Heartbeat LED Indicators	
LED Color	Definition
Green: Solid On	Safe to remove HDD devices
Green: Blinking	HDD installed on the slot functions normally; Not ready for HDD device removal

HDD0/HDD1 Activity LED Indicators

Two HDD Activity LED indicators are located at D34 and D35 on the motherboard. D34 is used for HDD0, and D35, for HDD1. Refer to the table below for more information.

HDD0 (D34)/HDD1(D35) Activity LED Indicators	
LED Color	Definition
Blue: Blinking	HDD Active
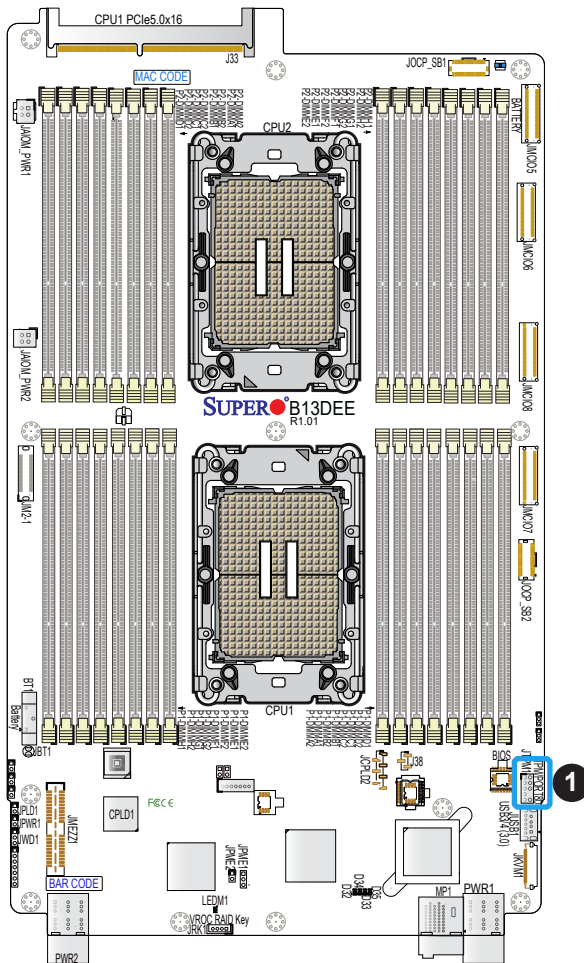
1. DA4: Heartbeat LED for HDD device installed on HDD0

2. D34: Activity LED for HDD device installed on HDD0

3. DA5: Heartbeat LED for HDD device installed on HDD1

4. D35: Activity LED for HDD device installed on HDD1

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

No Video

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

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

System Boot Failure

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

1. Remove all components from the motherboard, especially the DIMM modules. Power on the system and check if the power-on LED and the BMC Heartbeat LED (LEDM1) are on, and system fans are spinning.

2. 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

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

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

3. Make sure that you are using the correct type of ECC DDR5 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 1 for details on recommended power supplies.

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

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. HDD support: Make sure that all hard disk drives (HDDs) work properly. Replace the bad HDDs 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 BMC 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. Please 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 CD/USB flash drive.

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

3. Using 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. Identifying 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, please take the following steps. Also, please 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. Please 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 (https://www.supermicro.com/ support/resources/bios_ipmi.php).

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 http://www.supermicro.com/ RmaForm/.

5. Distributors: For immediate assistance, please 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: This motherboard supports up to 8TB 3DS RDIMM/RDIMM DDR5 (288-pin) memory with speeds up to 5600 MT/s in 16 DIMM slots (or up to 4400 MT/s in 32 DIMM slots). To enhance memory performance, do not mix memory modules of different speeds and sizes. Please follow all memory installation instructions given on Section 2-4 in Chapter 2.

> **Note 1:** The 4th Gen Intel Xeon Scalable processor supports DDR5 memory up to 4800 MT/s (supports up to 4400 MT/s in 32-DIMM configuration). The 5th Gen Intel Xeon Scalable processor supports DDR5 memory up to 5600 MT/s (supports up to 4400 MT/s in 32-DIMM configuration).

> **Note 2:** Memory speed and capacity support depend on the processors used in the system.

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 https://www.supermicro.com/support/resources/bios_ipmi.php. Please 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.

> **Note 1**: The SPI BIOS chip used on this motherboard cannot be removed. Send your motherboard back to our RMA Department at Supermicro for repair.

> **Note 2**: For BIOS Update and Recovery instructions, please refer to the Firmware Update and Recovery Instructions for Supermicro's X13 MotherboardS User's Guide 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: Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency to dispose of your used battery properly.

Battery Installation

To install an onboard battery, follow the steps below:

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

2. Locate the onboard battery as shown below

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

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

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

LITHIUM BATTERY

BATTERY HOLDER

OR

LITHIUM BATTERY

BATTERY HOLDER
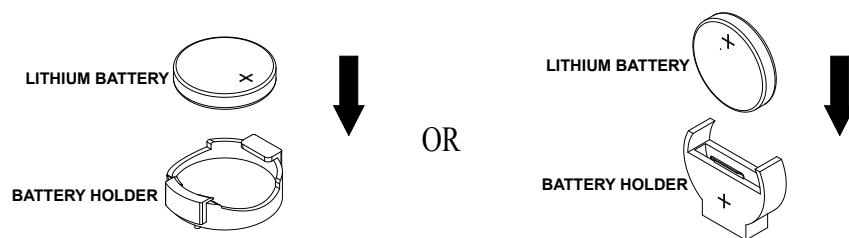
3.5 Returning Merchandise for Service

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 the BMC WebUI or the SUM utility.

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

Starting the Setup Utility

To enter the BIOS Setup utility, press the <Delete> key while the system is booting up. In most cases, the <Delete> key is used to invoke the BIOS Setup screen; however, in other cases, other hot keys, such as <F1>, <F2>, may be used for this purpose. 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, and often a text message will accompany it. Please note that BIOS has default text messages built in, and we retain the option to include, omit, or change any of these text messages. Settings printed in **Bold** are the default values.

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

The BIOS Setup utility uses a key-based navigation system called hot keys. Most of these hot keys (<F1>, <F2>, <F3>, <F4>, <Enter>, <ESC>, <Arrow> keys, etc.) can be used at any time during the setup navigation process.

4.2 Main Setup

When you first enter the AMI BIOS Setup utility, you will see 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.

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

                                                  Set the Date. Use Tab to
    System Date               [Fri 02/17/2023]    switch between Date elements.
    System Time               [20:12:26]          Default Ranges:
                                                  Year: 1998-9999
    Supermicro B13DEE                             Months: 1-12
    BIOS Version              1.0                  Days: Dependent on month
    Build Date               02/01/2023           Range of Years may vary.
    CPLD Version             F4.28.00

    Memory Information
    Total Memory             524288 MB

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



              Version 2.22.1287 Copyright (C) 2023 AMI
```

System Date

This feature displays the current date of the system in operation. The system date is displayed in "Day MM/DD/YYYY" format, which includes the day of the week (Day), the month of the year (in two digits: "MM"), the day of the month (in two digits: "DD"), and the year (in four digits: "YYYY").

System Time

This feature displays the current time of the system in operation, which is based on the RTC (Real Time Clock) of the system. The system time is displayed 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 the RTC (Real Time Clock) reset.

Supermicro B13DEE

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 Complex-Programmable Logical Device (CPLD) used in the system.

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
   ▶ Super IO Configuration
   ▶ Serial Port Console Redirection
   ▶ Network Configuration
   ▶ PCIe/PCI/PnP Configuration
   ▶ ACPI Settings
   ▶ Trusted Computing
   ▶ Supermicro KMS Server Configuration
   ▶ Super-Guardians Configuration
   ▶ HTTP Boot Configuration                         →←: Select Screen
                                                     ↑↓: Select Item
   ▶ Intel(R) Ethernet Controller E810-XXV for backplane -   Enter: Select
     7C:C2:55:7F:46:EC                                +/-: Change Opt.
   ▶ Intel(R) Ethernet Controller E810-XXV for backplane -   F1: General Help
     7C:C2:55:7F:46:ED                                F2: Previous Values
   ▶ TLS Authenticate Configuration                  F3: Optimized Defaults
   ▶ VLAN Configuration (MAC:7CC2557F46EC)           F4: Save & Exit
   ▶ VLAN Configuration (MAC:7CC2557F46ED)           ESC: Exit
   ▶ VLAN Configuration (MAC:AC1F6B55E744)
   ▶ VLAN Configuration (MAC:AC1F6B55E745)
   ▶ INTEL SSDPE2KX020T7-PHLF7013001U2P0HGN        ▼

                         Version 2.22.1287 Copyright (C) 2023 AMI
```

Warning: Take caution when changing the Advanced settings. An incorrect value, an improper DRAM frequency, or a wrong BIOS timing setting may cause the system to malfunction. When this occurs, restore the setting to the manufacturer default setting.

▶Boot Feature

Quiet Boot

Use this feature to select the screen display between Power-on Self Test (POST) messages and 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 **Enabled** and Disabled.

> **Note:** BIOS 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 bootup. The options are **Immediate** and Postponed.

Re-try Boot

When EFI (Extensible Firmware Interface) 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 five minutes. The options are **Disabled** and Enabled.

If this feature is set to Enabled, the following feature will display:

Watch Dog Action (Available when the feature "Watch Dog Function" is enabled)

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

Front USB Port(s) (This feature will display only when DCMS key is activated)

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

> **Note:** To fully utilize the functionality and features supported by Supermicro Management software and utilities, please use the Supermicro DataCenter Management Suite per Node License Key (SFT-DCMS-SINGLE), which is the license to the Supermicro's Data Center Management Suite. For more information, please contact us at www.supermicro.com.

Rear USB Port(s) (This feature will display only when the DCMS key is activated)

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

Restore on AC Power Loss

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

Power Button Function

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

▶CPU Configuration

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

```
                              Aptio Setup - AMI
            Advanced

   Processor Configuration                         Displays and provides options
   --------------------------------------------    to change the Power Management
   Processor BSP Revision        806F6 - SPR-SP E3 Settings
   Processor Socket              CPU1      CPU2
   Processor ID                  000806F6* | 000806F6
   Processor Frequency           2.400GHz  | 2.400GHz
   Processor Max Ratio               18H   |     18H
   Processor Min Ratio               08H   |     08H
   Microcode Revision            2B000161  | 2B000161
   L1 Cache RAM(Per Core)            80KB  |    80KB
   L2 Cache RAM(Per Core)          2048KB  |  2048KB
   L3 Cache RAM(Per Package)      99840KB  | 99840KB
   Processor 0 Version           Intel(R) Xeon(R) Platin
                                 um 8468V
                                                    ➔←: Select Screen
   Processor 1 Version           Intel(R) Xeon(R) Platin  ↑↓: Select Item
                                 um 8468V               Enter: Select
 ▶ Advanced Power Management Configuration           +/-: Change Opt.
 ▶ CPU1 Core Disable Bitmap                          F1: General Help
 ▶ CPU2 Core Disable Bitmap                          F2: Previous Values
   Hyper-Threading [ALL]          [Enable]           F3: Optimized Defaults
   Hardware Prefetcher            [Enable]           F4: Save & Exit
   Adjacent Cache Prefetch        [Enable]           ESC: Exit
   DCU Streamer Prefetcher        [Enable]
   DCU IP Prefetcher              [Enable]
   LLC Prefetch                   [Disable]

              Version 2.22.1287 Copyright (C) 2023 AMI
```

Processor Configuration

The following CPU information is displayed:

- Processor BSP Revision

- Processor Socket

- Processor ID

- Processor Frequency

- Processor Max Ratio

- Processor Min Ratio

- Microcode Revision

- L1 Cache RAM (Per Core)

- L2 Cache RAM (Per Core)

- L3 Cache RAM (Per Package)

- Processor 0 Version

- Processor 1 Version

▶Advanced Power Management Configuration

Power Technology

Use this feature to manage power management settings. 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)

Select BIOS to allow the system BIOS to configure Power-Performance Tuning Bias settings. The options are **OS Controls EPB** and BIOS Controls EPB.

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

Use this feature to configure the proper operation setting for your computer by achieving the desired system performance level and energy saving (efficiency) level at the same time. 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 Performance, **Balanced Performance**, Balanced Power, and Power.

Optimized Power Mode

Select enable to enable Optimized Power Mode. Select Disable to disable Optimized Power Mode. The options are Disable and Enable.

▶CPU P State Control

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

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

Use this feature to set the appropriate Thermal Design Power (TDP) level for the system. The Intel Advanced Vector Extensions (Intel AVX) P1 feature allows the user to set the base P1 ratio for Streaming SIMD Extensions (SSE) and AVX workloads. Each P1 ratio has a corresponding AVX Impressed Current Cathodic Protection (ICCP) pre-grant license level, which refers to the selection between different AVX ICCP transition levels. Select Nominal to provide the base set of instructions to allow Single-Instruction Multiple-Data (SIMD) operations to be performed in an Intel processor by adding MMX and SSE support. The options are **Nominal**, Level 1, and Level 2.

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. Please 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 to occur based on the real-time energy needs of applications so that the power-to-performance balance can be optimized for energy efficiency. The options are **HW_ALL** and SW_ALL.

Turbo Mode (Available when "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 the previous item - "Hardware P-States" is set to "Native Mode with Legacy Support" or using the Native Mode with No Legacy support)

SST-CP

With Intel Speed Select Technology (Intel SST-CP), surplus frequency is allocated based on the weight of the CPU core. 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

Enable Monitor MWAIT

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

CPU C1 Auto Demotion

Select Enable to allow the CPU to automatically demote to C1 State. The options are Disable, Enable, and **Auto**. Please reboot the system for the change(s) you've made to take effect.

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 idle mode. Please 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 / CPU2 Core Disable Bitmap**

Available Bitmap:

This feature displays the available bitmap.

Disable Bitmap

Enter 0 to enable this feature for all CPU cores. Enter FFFFFFFFFFFF to disable this feature for all CPU cores. Please 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 prefectch data from the main system memory to Level 2 cache to help expedite data transaction to enhance memory performance. The options are Disable and **Enable**.

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 Disable and **Enable**.

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 Disable and **Enable**.

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 (Extended Advanced Programmable Interrupt Controller)

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 for CPU performance enhancement. 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:** Please 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)

Use this feature to set the number of unique keys per system, which also indicates 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 1MB. 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)

----

*The following SGX features are available when "Memory Encryption (TME)" is set to Enabled and when your CPU supports Intel SGX.

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

SGX Factory Reset

Use this feature to perform an SGX factory reset to delete all registration data and force an Initial Platform Establishment flow. Reboot the system for the 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.

SGX PRM Size (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.

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 the user 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

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

▶Uncore Configuration

The following 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 reduce the UPI links from full width to half width in the event when the CPU's workload is low in an attempt to save power. This feature is available for the system that uses Intel processors with UPI technology support. The options are Disable, Enable, **Auto,** and Full L0p Enable.

Note: 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 option of Full L0p Enable is available when th 5th Gen Intel Xeon Scalable Series processor is used.

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: Link 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

Use this feature to configure the Prefetch setting supported by Keizer Technology Interconnect (KTI), also known as 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 option of Enable SNC4 (4-clusters) depends on your system configuratio and the processor.

Stale AtoS (A to S)

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 the user to configure the Integrated Memory Controller (iMC) settings.

Enforce DDR Memory Frequency POR

Select POR to enforce Plan of Record (POR) restrictions 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. (Please note that the available options are CPU-dependent.)

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 support Fast Asynchronous DRAM Refresh (fADR) for memory performance enhancement 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 frequency. The support of fADR is based on your motherboard hardware features. The options are **Disable** and Enable.

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 the 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)

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.

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 options are **Auto** and Manual.

Flush Timeout

Use this feature to set the timeout setting when the data in the CPU cache memory should be flushed by the applications to persistent memory during power-off. 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.

▶Memory Topology

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

P1-DIMMA1: 4800MT/s Hynix SRx8 16GB RDIMM ~ P2-DIMMH2: 4800MT/s Hynix SRx8 16GB RDIMM

▶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)

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, but it will 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 16K cycles if there is no delay caused by internal processing. By using this method, roughly 64 GB of memory behind the IO hub will be scrubbed every day. The options are Disabled and **Enable at End of POST**. (POST is the abbreviation for Power_On Self Test.)

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 for PPR enhancement. Select Enabled to always execute for every boot. Select Once to execute only one time. The options are **Disabled**, Enabled, and Once.

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.

▶IIO Configuration

▶CPU1 Configuration / CPU2 Configuration

IOU0 (IIO PCIe Port 1)

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

▶Socket0 Port DMI

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

PCIe Port

Use this feature to set the PCIe Root Port. The options are Auto, No, and Yes. If this feature is set to Auto, the PCIe device will be automatically detected by the BIOS. Select No/Yes to disable/enable the PCIe Root Port manually. Please note that this feature depends on your motherboard specifications.

Link Speed

Use this feature to select the link speed for the PCIe port specified by the user. 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 Port MPSS

Use this feature to set the maximum payload size supported in Direct Media Interface (DMI) Device Capability Register for the device installed in the PCIe port. The options are 128B, 256B, and **Auto.**

Equalization Bypass To Highest Rate

When this feature is set to Enable, the Equalization Bypass will be supported at the highest rate. The options are **Enable** and Disable.

▶**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 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.

Pre-boot DMA (Direct Memory Access) Protection

Select Enable to enable DMA protection support in the pre-boot environment, which is available when the DMAR table is installed in the DXE (Driver Execution Environment), and the VID_INF0_PPI is installed in PEI. 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**.

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.

IIO-PCIE Express Global Options

PCIe ASPM Support (Global)

Select Enabled to enable ASPM (Active State Power Management) support for a device installed in a PCIe drive specified by the user. The options are **Disable** and Auto.

PCIe Max Read Request Size

Use this feature to set the requested Max Read Request Size in the PCI hierarchy. Select Auto to use the default settings of hardware components. The options are **Auto**, 128B, 256B, 512B, 1024B, 2048B, and 4096B.

Equalization Bypass To Highest Rate

When this feature is set to Enable, the Equalization Bypass will be supported at the highest rate. The options are **Enable** and Disable.

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.

CXL (Compute Express Link) Security Level

Use this feature to configure the CXL (Compute Express Link) security level upon which a CXL device gets access on the CXL connection for data transmission and processing. CXL is an open Industry standard that provides the high-speed, high capacity, low latency, CPU-to-device and CPU-to-memory CXL interconnection used for high-performance computers. Select Fully Trusted for a CXL device to get access to host-attached and device-attached memory from another device via CXL. Select Partially Trusted for a CXL device to get access to device-attached memory from another device via CXL. If this feature is set Untrusted: All requests on CXL interconnections will be aborted by the system. The options are Fully Trusted, Partially Trusted, Untrusted, and **Auto**.

CXL (Compute Express Link) Header Bypass

In the CXL technology, a 2-bit (sync) header is inserted before every 128 bits per lane is transmitted in a data block when 128b/130b encoding is used. Enabling Sync Header Bypass support will disable this 2-bit CXL header and improve memory link performance. The options are Enable and **Disable**.

▶South Bridge

The following information is displayed:

- USB Module Version

- 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, 0.3%, 0.5%, and **Auto**.

▶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(s) supported by the Intel PCH chip. The options are Disabled and **Enabled**.

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

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

> **Note 1:** The option of RAID is unavailable when "Boot Mode Select" is set to Legacy.
>
> **Note 2:** Refer to Boot submenu in the BIOS Setup main menu to set "Boot Mode Select".

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

When this feature is set to Enabled, 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 (Available when "SATA Controller(s)" is set to Enabled)

Select Enabled for Serial_Link General Purpose I/O (SGPIO) Mode support. The options are **LED** and SGPIO.

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

> **Note:** The SATA port naming may vary based on the related configuration.

Hot Plug

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

Spin Up Device

Select Enabled for Staggered Spin Up support to allow the SATA devices specified by the user to spin up one at a time at bootup 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 specified by the user should be connected to a Solid State drive or a Hard Disk Drive. The options are **Hard Disk Drive** and Solid State Drive.

▶Super IO Configuration (Available when your system supports this feature)

The following information is displayed.

- Super IO Chip

▶Serial Port 1 Configuration

Serial Port

Select Enabled to enable serial port 1. The options are Disabled and **Enabled**.

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

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

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

This feature specifies the base I/O port address and the Interrupt Request address of serial port 1. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 1. 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

> **Note:** It can be "Serial Port 2 Configuration" or "SOL Configuration" based on your system support.

Serial Port

Select Enabled to enable serial port 2 (or SOL). The options are Disabled and **Enabled**.

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

This feature displays the base I/O port address and the Interrupt Request address of serial port 2 (or SOL).

Change Settings (Available when "Serial Port 2/SOL" is set to Enabled)

This feature specifies the base I/O port address and the Interrupt Request address of serial port 2 (or SOL). Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 2. 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 (Available when your system supports serial port of COM1)

Console Redirection

Select Enabled to enable COM port 1 for Console Redirection, which allows a client machine to be connected to a host machine at a remote site for networking. The options are **Disabled** and Enabled.

> **Note:** This feature will be set to Enabled if there is no BMC support.

▶Console Redirection Settings (Available when "Console Redirection" above 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.

SOL/COM2

> **Note:** This feature is available when your system supports serial port of COM2 and/or SOL. The "SOL" here indicates a shared serial port, and SOL is used as the default.

Console Redirection

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

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

Use this feature to specify how the host computer will exchange data with the client computer.

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

►Legacy Console Redirection Settings

Legacy Serial Redirection Port

Use this feature to select a serial port to display redirection of Legacy OS and Legacy OPROM messages. The options are **COM1** and SOL/COM2. Please note that the available options are based on your motherboard features.

Resolution

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

Redirect After BIOS POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When the option - BootLoader is selected, legacy console redirection is disabled before booting the OS. When the option - 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 the user 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 (Management) 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. Please note that the option of SOL/COM2 indicates a shared serial port. SOL/COM2 is available with 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 VT100+ to add color and function key support. Select ANSI to use the extended ASCII character set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, **VT-UTF8**, and, ANSI.

Bits Per Second EMS

This feature sets the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 57600, **115200,** 230400, 460800, and 921600 (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) upon which the system BIOS will wait for the user 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 the 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 the keyboard to change the value. The default setting is **1**.

▶ **MAC:(MAC address)-IPv6 Network Configuration**

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 configurations.

▶ **Enter Configuration Menu**

The following information is displayed:

- Interface Name

- Interface Type

- MAC address

- Host address

- 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 times that Duplicate Address Detection (DAD) has been performed. DAD is a procedure used to verify whether an IPv6 address is unique on the LAN before it is assigned for physical interface; only a unique IP address will be used for real-time interface. 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. The options are Yes and No.

Discard Changes and Exit

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

Save Changes and Exit

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

▶**MAC:(MAC address)-IPv4 Network Configuration**

> **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 configurations.

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**.

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 128M, 256M, 512M, 1G, 2G, and **Auto**. Please note that the MMCFG size is based on the memory populated.

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 512G.

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**.

Bus Master Enable

If it is set to Enabled, the PCI Bus Driver will enable the Bus Master Attribute for DMA transactions. If it 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**.

ARI Support

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

NVMe Firmware Source

Use this feature to select the NVMe firmware to support system boot. The options are **Vendor Defined Firmware** and AMI Native Support. The default option, **Vendor Defined Firmware**, is pre-installed on the drive by the manufacturer and may resolve errata or enable innovative functions for the drive. The other option, AMI Native Support, is offered by the AMI BIOS with a generic method. (Please use the AMI Native Support option for Supermicro Security Erase Configuration support available in the Security menu.)

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 proper configurations of Option ROM settings, please pay attention to the notes below.

> **Note 1:** The number of slots and slot naming vary based on your motherboard features.
>
> **Note 2:** The option of Legacy is available when "Boot Mode Select" is set to Dual or Legacy.
>
> **Note 3:** Refer to Boot submenu in the 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.

PCI Devices Option ROM Setting

CPU1 SLOT1 PCIe 5.0 x16 OPROM/CPU2 SLOT2 PCIe 5.0 x16 OPROM

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

Onboard LAN1 Option ROM

Select EFI to allow the user to boot the computer using the EFI device installed on LAN Port 1. The options are Disabled and **EFI**.

Onboard LAN2 Option ROM

Select EFI to boot the computer using the EFI device installed on LAN Port 2. The options are **Disabled** and EFI.

▶ACPI Settings

NUMA

Select Enabled 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 (Available when a TPM device is installed and detected by the BIOS)

When a Trusted-Platform Module (TPM) device is detected by your system, the following information is displayed:

• 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**.

*When "Security Device Support" is set to Enable, the following information is displayed:

• Active PCR banks

• Available PCR banks

SHA-1 PCR Bank (Available when "Security Device Support" is set to Enable)

Select Enabled to enable SHA-1 PCR Bank support to enhance system integrity and data security. The options are **Enabled** and Disabled.

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 next system boot to enhance system data integrity. 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) (for TPM version 2.0 and above)

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

Storage Hierarchy (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 the user's privacy concerns because the primary keys in the hierarchy are certified by the TPM key or by a manufacturer with restrictions on how an authentic TPM device that is attached to an authentic platform can be accessed and used. A primary key can be encrypted and certified with a certificate created by using TPM2_ ActivateCredential, which allows the user 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 (for TPM version 2.0 and above)

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, please 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**.

KMS Time Out

Use this feature to enter the KMS server connecting timeout (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

This feature displays the Transport Layer Security (TLS) certificate and its size for CA Certificate, Client Certificate, and Client Private Key.

▶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 "Private Key Password" has been set)

Use this feature to change the private key password.

▶Super-Guardians Configuration

Super-Guardians Protection Policy

Use this feature to select the devices that you want to protect by using the Super-Guardians Policy. The options are: **Storage**, System, and System and Storage.

KMS Security Policy

When this feature is set to Enabled, passwords will be installed to protect the system and storage devices as specified, and these passwords will be required to unlock the system or devices. When this feature is set to Disabled, there will be no passwords used to protect the system and storage devices. The options are **Disabled** and Enabled.

KMS Server Retry Count

Use this feature to specify how many times of the connection retry should the KMS server attempt before quitting. The valid range is 0 - 10. Press "+" or "-" on your keyboard to change the value. The default setting is **5** (retrying five times).

TPM Security Policy

When this feature is set to Enabled, passwords will be installed to protect the system and storage devices as specified, and these passwords will be required to unlock the system or devices. When this feature is set to Disabled, there will be no passwords used to protect the system and storage devices. The options are **Disabled** and Enabled.

Load Authentication-Key

Select Enabled to allow the BIOS to load the Authentication-Key (File name: TPMAuth.bin) from USB storage devices at next system boot. The options are **Disabled** and Enabled.

USB Security Policy

When this feature is set to Enabled, passwords will be installed to protect the system and storage devices as specified, and these passwords will be required to unlock the system or devices. When this feature is set to Disabled, there will be no passwords used to protect the system and storage devices. The options are **Disabled** and Enabled.

▶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

Enable this feature for HTTPS boot to check the hostname of the TLS certificates to see if it matches the host name provided by the remote server. The options are **Enabled** and Disabled (WARNING: Security Risk!!).

Priority of HTTP Boot

Instance of Priority 1 (Available when your motherboard supports this feature)

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, which cannot be longer than 75 characters. Please be suer to enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI

Enter a Boot Uniform Research Identifier (URI) with 128 characters or shorter. 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.

Instance of Priority 2 (Available when your motherboard supports this feature)

This feature sets the rank target port. The default setting is **0**.

▶Mellanox Network Adapter -(MAC address)

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 configurations.

▶Firmware Image Properties

The following information is displayed:

- Family Firmware Version

- EFI Version

▶NIC Configuration

Banner Message Timeout

Use this feature to specify the number of seconds that the OptionROM banner will be displayed during POST (Power On Self-Test). The default setting is 4.

Legacy Boot Protocol

Use this feature to set a non-UEFI network boot protocol. The options are None, **PXE**, iSCSI, PXE without fail-over, and iSCSI without fail-over.

IPv4/IPv6 support

Use this feature to select whether the IPv4 or IPv6 network address will be used for iSCSI initiator and targets. The options are **IPv4**, IPv6, and IPv4/IPv6.

Virtual LAN Mode

Select Enabled to enable Virtual LAN mode, which will allow a VLAN tag to be used by PXE. The options are **Disabled** and Enabled.

Virtual LAN ID (availeble when "Virtual LAN Mode" is set to "Enabled")

Use this feature to set the VLAN ID used in PXE VLAN mode by entering a value ranging from 0 to 4094. When the VLAN ID is set to **0**, PXE VLAN will be disabled.

Boot Retry Count

Use this feature to indicate the number of retries a system should attempt to boot in case of a boot failure. The options are **No Retry**, 1 Retry, 2 Retries, 3 Retries, 4 Retries, 5 Retries, 6 Retries, and Indefinite Retries.

Boot Strap Type

Use this feature to specify the boot strap method to be used by the BIOS to boot to the operating system. The default option is **Int 19h**.

Wake On LAN

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

Wake On LAN Link Speed

Use this feature to set the connection speed of a LAN port specified by the user for Wake on LAN mode. The default option is **1 Gbps**.

▶iSCSI Configuration

iSCSI General Parameters

Boot to Target

Select Enabled to specify whether the iSCSI initiator will boot to the iSCSI target specified by the user at bootup. Select One Time Disabled to disable iSCSI boot upon next system boot after this feature is enabled. The options are Disabled, **Enabled**, and One Time Disabled.

TCP/IP Parameters via DHCP

Use this feature to manage the sources of the IPv4 IP addresses of the initiator, DHCP or a static assignment. The options are Disabled and **Enabled**.

iSCSI Parameters via DHCP

Select Enabled to enable the acquisition of iSCSI target parameters from DHCP. The options are Disabled and **Enabled**.

CHAP Authentication

Use this feature to enable the initiator to use CHAP authentication when connecting to the iSCSI target. The options are **Disabled** and Enabled.

CHAP Mutual Authentication (available when "CHAP Authentication" is set to Enabled)

To use mutual CHAP authentication, specify an initiator secret on the Initiator Parameters page and configure that secret on the target. The options are **Disabled** and Enabled.

IP Version

Use this feature to indicate whether the IPv4 or the IPv6 network address will be used for iSCSI initiator and targets.

iSCSI Initiator Parameters

The following information will be displayed:

- IP Address
- Subnet Mask
- Default Gateway
- Primary DNS
- CHAP ID
- CHAP Secret
- IPv6 Address
- IPv6 Primary DNS

- IPv6 Prefix Length

iSCSI Name

Use this feature to specify the iSCSI Qualified Name (IQN) for the initiator.

iSCSI First Target Parameters

The following information is displayed:

- Connect

- IP Address

- IPv6 Address

- TCP Port

- Boot LUN

- iSCSI Name

- CHAP ID

- CHAP Secret

Device Level Configuration

Virtualization Mode

Use this feature to specify the type of Virtualization used by the controller on all ports. The options are None and **SR-IOV**.

PCI Virtual Functions Advertised

Use this feature to specify the number of Virtual Functions to be supported on this device. The default option is **8.**

Blink LEDs

Use this feature to specify the number of seconds the LEDs on physical network port should blink to assist with port identification. The default option is **0.**

Device Name

This feature displays the official product name of the device**.**

Chip Type

This feature displays the Chip Type**.**

PCI Device ID

This feature displays the PCI Device ID of the controller.

PCI Address

This feature displays the PCI Address of the card.

Link Status

This feature displays the status of the physical link of the network port as reported by the controller.

Link Speed

This feature displays the speed of the physical link of the network port as reported by the controller.

MAC Address

This feature displays the permanent MAC address assigned during manufacturing.

Virtual MAC Address

This feature displays the virtual MAC address of the controller.

Socket Direct Operation

This feature indicates whether Socket Direct support is enabled.

▶TLS Authenticate Configuration

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

▶Server CA Configuration

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

▶Enroll Certification

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

▶Enroll Certification Using File

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

▶**Enroll Certification**

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

▶**Enroll Certification Using File**

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

Certification GUID
Press <Enter> and input the certification GUID.

▶**Commit Changes and Exit**

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

▶**Discard Changes and Exit**

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

▶**Delete Certification**

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

▶VLAN Configuration (MAC: address)

Note : The Ethernet controller and MAC addresses shown above are based on configurations.

▶Enter Configuration Menu

Create New VLAN

VLAN ID

This feature allows the user to enter the VLAN ID of the new VLAN or the existing VLAN. The valid value is 0~4094. The default value is **0**.

Priority

This feature allows the user to enter the 802.1Q Priority. The valid value is 0~7. The default value is **0**.

Remove VLAN

Use feature to remove selected VLANs.

▶Intel(R) VROC SATA Controller

> **Note 1:** This section is based on your system configurations and related device(s) installed in your system.
>
> **Note 2:** This section is available when "SATA Mode Selection" is set to RAID.
>
> **Note 3:** Refer to PCH SATA0 Configuration, PCH SATA1 Configuration, and PCH SATA2 Configuration submenus in the BIOS Setup main menu to set "SATA Mode Selection".

The following information is displayed.

- Intel VROC SATA driver version

▶Create RAID Volume

Name:

This feature allows the user to enter the unique name of RAID volume.

RAID Level:

This feature allows the user to select the RAID level. The options are **RAID0(Stripe)**, RAID1(Mirror), RAID5(Parity), and RAID10(RAID0+1).

Select Disks:

Select the desired RAID disks one by one by setting them to **X**. The options are (not selected) and **X (selected)**.

Strip Size:

Use this feature to select the RAID strip size. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**. The available options are based on the setting of "RAID Level:" above.

Capacity (GB):

This feature allows the user to enter the desired RAID capacity (in GB).

▶Create RAID Volume

Use this feature to create a RAID volume with the settings above. The options are **Yes** and No.

Non-RAID Physical Disks:

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

RAID Volumes:

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

▶Intel(R) VROC sSATA Controller

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

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

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

The following information is displayed.

• Intel VROC sSATA driver version

▶Create RAID Volume

Name:

This feature allows the user to enter the unique name of RAID volume.

RAID Level:

This feature allows the user to select the RAID level. The options are **RAID0(Stripe)**, RAID1(Mirror), RAID5(Parity), and RAID10(RAID0+1).

Select Disks:

Select the desired RAID disks one by one by setting them to **X**. The options are (not selected) and **X (selected)**.

Strip Size:

Use this feature to select the RAID strip size. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**. The available options are based on the setting of "RAID Level:" above.

Capacity (GB):

This feature allows the user to enter the desired RAID capacity (in GB).

▶Create RAID Volume

Use this feature to create a RAID volume with the settings above. The options are **Yes** and No.

Non-RAID Physical Disks:

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

RAID Volumes:

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

▶Intel(R) VROC tSATA Controller

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

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

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

The following information is displayed.

• Intel VROC tSATA driver version

▶Create RAID Volume

Name:

This feature allows the user to enter the unique name of RAID volume.

RAID Level:

This feature allows the user to select the RAID level. The options are **RAID0(Stripe)**, RAID1(Mirror), RAID5(Parity), and RAID10(RAID0+1).

Select Disks:

Select the desired RAID disks one by one by setting them to **X**. The options are (not selected) and **X (selected)**.

Strip Size:

Use this feature to select the RAID strip size. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**. The available options are based on the setting of "RAID Level:" above.

Capacity (GB):

This feature allows the user to enter the desired RAID capacity (in GB).

▶Create RAID Volume

Use this feature to create a RAID volume with the settings above. The options are **Yes** and No.

Non-RAID Physical Disks:

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

RAID Volumes:

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

▶Intel(R) Virtual RAID on CPU

Note: It is available when your system supports this feature and when "Enable/Disable VMD" is set to Enable.

The following information is displayed:

- Intel(R) VROC with VMD Technology x.x.x.xxxx

- Upgrade key:

- Intel VROC Managed Controllers:

▶INTEL SSDPE2KX020T7-PHLF013001U2P0HGN (Available when the device is detected by the BIOS)

Note : The device displayed and the MAC address shown above are based on configurations.

The following information will be displayed:

- Bus Protocol

- PCI Vendor/Device ID

- PCI Vendor Subsystem

- Model Number

- Serial Number

- Firmware Revision

- IEEE Organization Unique ID

- PCIe Maximum Link Width

- PCIe Maximum Speed

- PCIe Negotiated Link Width

- PCIe Negotiated Speed

- Drive Health

- Total Drive Capacity

- Number of Namespaces

- Namespace ID

  - Device Capacity

  - Device Size

▶Supermicro HTTP BOOT FORM

Enroll HTTPS Boot TLS Certificate

Use this feature to register the HTTPS Boot TLS certificate information with Supermicro.

Delete HTTPS Boot TLS Certificate

Use this feature to remove the HTTPS Boot TLS certificate from Supermicro's record.

▶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. Driver health status differs depending on the drivers installed in your system. It's also based on your system configurations and the environment that your system is operating in.

4.4 Event Logs

Use this feature to configure Event Logs settings.

> **Note:** After you've made any changes in this section, please be sure to reboot the system for the changes to take effect.

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

   ▶ Change SMBIOS Event Log Settings                   Press <Enter> to change the
   ▶ View SMBIOS Event Log                              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 2.22.1287 Copyright (C) 2023 AMI
```
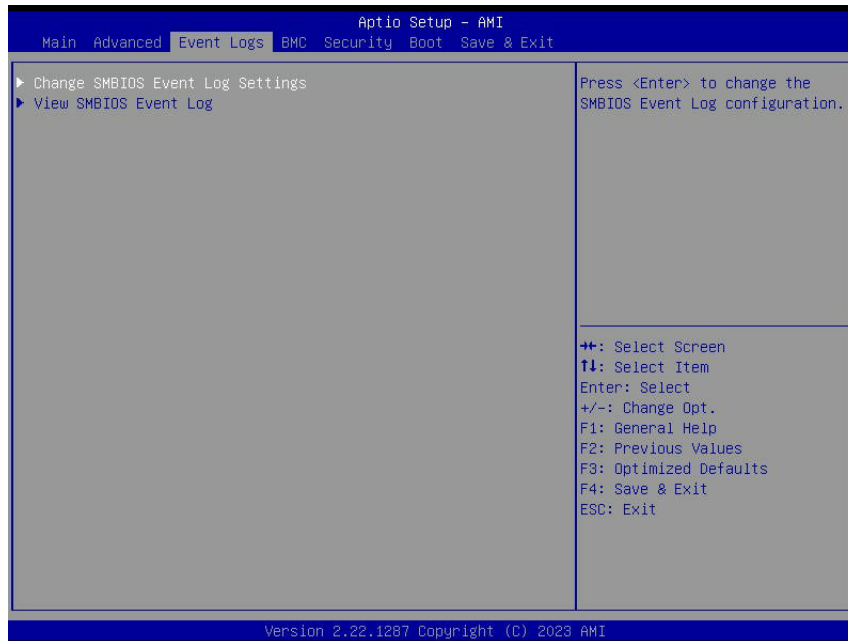
▶Change SMBIOS Event Log Settings

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)

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

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

This feature is used to determine how long (in minutes) should the multiple event counter wait before generating a new event log. Enter a number between 0 to 99. The default setting is **60**. (METW is the abbreviation for Multiple Event Count Time Window.)

▶**View SMBIOS Event Log**

This feature allows the user to view the event in the system event log. Select this feature and press <Enter> to view the status of an event in the log. The following categories is displayed:

DATE / TIME / ERROR CODE / SEVERITY.

4.5 BMC

Use this feature to configure BMC settings.

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

    BMC Firmware Revision            1.00.29          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 2.22.1287 Copyright (C) 2023 AMI
```

BMC Firmware Revision

This feature indicates the BMC firmware revision used in the system.

BMC STATUS

This feature indicates the status of the BMC firmware installed in the 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 the user 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 BMC LAN. The default setting is **Failover**.

BMC Network Link Status:

This feature displays the status of the BMC 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, the user 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 VLAN support. The options are **Disable** and Enable.

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

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

****

Configure IPv6 Support

****

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, the user 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.

Station IPv6 Address (DHCPv6 Stateless) (Available when "Configuration Address Source" is set to Static Configuration)

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.

Advanced Settings (Available when "Configuration Address Source" is set to Static Configuration)

Use this feature to set the DNS server IP. The options are **Auto obtain DNS server IP** and Manually obtain DNS server IP. This default setting allows your system to obtain the DNS server IP automatically.

Preferred DNS server IP (Available when "Advanced Settings" above is set to Manually obtain DNS server IP)

This feature allows the user to set the preferred DNS server IP. It can be configured via Redfish.

Alternative DNS server IP (Available when "Advanced Settings" above is set to Manually obtain DNS server IP)

This feature allows the user to set the alternative DNS server IP. It can be configured via Redfish.

Chapter 4: UEFI BIOS

4.6 Security

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

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

                                             ▲ Set Administrator Password
     Administrator Password      Not Installed
     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 2.22.1287 Copyright (C) 2023 AMI
```

Disable Block Sid (Available when your motherboard supports NVMe)

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

The following information is displayed:

- Administrator Password

- User Password

- Password Description

Administrator Password

This feature indicates if an administrator password has been installed. It also allows the user to set the administrator password which is required to enter the BIOS Setup utility. The length of the password should be from three characters to 20 characters long.

User Password (Available when "Administrator Password" has been set)

This feature indicates if a user password has been installed. It also allows you to set the user password which is required to enter the BIOS Setup utility. The length of the password should be from three characters to 20 characters long.

Note: For more information on Security Boot configuration and Secure Erase instructions, please refer to Secure Erase User's Guide posted on the web page under the link: http://www.supermicro.com/support/manuals/.

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 and upon entering the BIOS Setup utility. The options are **Setup** and Always.

Hard Drive Security Frozen

Select Enabled to freeze the Lock Security feature for HDD to protect key data in hard drives from being accessed and altered. The options are **Disabled** and Enabled.

▶Supermicro Security Erase Configuration (Available when a storage device is detected by the BIOS)

> **Note:** To configure Supermicro Security Erase settings, please follow the instructions below to enable Security Erase feature support in the BIOS.

How to Activate Security Erase Configuration submenu for Secure Erase Support for NVMe SSD Devices

1. From the Advanced menu, select PCIe/PCI/PnP and press <Enter> to invoke the PCI Devices Common Settings page.

2. When the PCI Devices Common Settings screen displays, select NVMe Firmware Sources and press <Enter>. The NVMe Firmware Sources pop-up dialogue box will display.

3. From the pop-up box, select AMI Native Support and press <Enter>. Be sure to save the changes you've made and reboot the system for the new settings to take effect by pressing <F4>.

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

  Administrator Password                Not Installed
  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 2.22.1287 Copyright (C) 2023 AMI
```

4. Press <Del> at bootup to return to the AMI BIOS Setup Utility.

5. When AMI BIOS screen displays, using arrow keys, select Security from the BIOS menu bar on the top of the screen. The Supermicro Security Erase Configuration submenu will display on the Security menu as shown below.

6. Select Supermicro Security Erase Configuration and press <Enter> to enter the Secure Erase configuration page, which will allow you to configure Security Erase settings.

Configuring the settings included in the Supermicro Security Erase Submenu

This section provides information and instructions on how to configure the Supermicro-proprietary Security Erase settings included in the Security Erase submenu. When this submenu is selected, the following information will display as shown in the previous screen. Please note that the device information displayed on your screen may vary, depending on the storage devices installed in your system.

- HDD Name: This feature displays the vendor and model name of the HDD/SSD device detected by the BIOS.

- HDD Serial Number: This feature displays the serial number of the HDD/SSD device detected by the BIOS.

- Security Mode: This feature displays the security mode of the HDD/SSD device detected by the BIOS.

- Estimated Time: This feature displays the estimate time needed to configure the selected Security Erase features.

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

- TCG Device Type: This feature displays the TCG device type detected in the system.

- Admin Pwd Status: This feature indicates if a password has been set as a SATA administrator password which will allow the user to configure Supermicro Security Erase settings on the selected HDD (SATA) device by using this SATA administrator password.

Security Function

Select *Set Password* to set an HDD/SSD password which allows the user to configure the security settings of the HDD/SSD device as follows:

- Select *Security Erase - Password* to enter a user password which will allow the user to erase the password and all data stored in the HDD/SSD device.

- Select *Security Erase - PSID (Physical Security ID)* to enter an SED SSD PSID which will allow the user to erase all data stored in this device.

- Select *Security Erase - Without Password* to use the manufacturer default password "111111111" as the user password which will allow the user to erase all data stored in the HDD/SSD device by using this default password.

The options are **Disable**, Set Password, Change Password, Security Erase - Password, Security Erase - PSID, and Security Erase - Without Password.

> **Note 1:** The option of Security Erase - PSID is based on the storage device support. The section below provides instructions on how to configure the Security Function options.
>
> **Note 2:** The option of Change Password and Clear Password are available when "Password" below has been set.
>
> **Note 3:** The option of Set Password is not available when "Password" below has been set.

Password

Use this feature to set the user password which allows you to configure the Supermicro Security Erase settings by using user password.

Lockdown Mode (Available when the DCMS key is activated)

Select Enabled to support Lockdown Mode that will prevent the existing data or keys stored in the system from being accessed or altered in an effort to preserve system integrity and data security. The options are **Disabled** and Enabled.

> **Note** For more information on Secure Erase instructions, please refer to the Secure Erase User's Guide posted on the web page under the link: http://www.supermicro.com/support/manuals/.

HDD Security Configuration:

▶P1: (Storage Device Name)/▶P2: (Storage Device Name)

This section is available when the storage device is detected by the BIOS. Select this device. Press <Enter> and the following information is displayed:

- HDD Password Description:

- HDD PASSWORD CONFIGURATION:

  - Security Supported:

  - Security Enabled:

  - Security Locked:

- Security Frozen:

- HDD User Pwd Status:

- HDD Master Pwd Status:

Set User Password (Available when "Security Frozen:" above is No)

Select Enabled to support Lockdown Mode that will prevent existing data or keys stored in the system from being accessed and altered in an effort to preserve system integrity and security. The options are **Disabled** and Enabled.

> **Note** For more information on Secure Erase instructions, please refer to the Secure Erase User's Guide posted on the web page under the link: http://www.supermicro. com/support/manuals/.

▶Secure Boot

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

The following information is displayed:

- System Mode

- Secure Boot

Secure Boot

Select Enabled to configure Secure Boot settings. The options are **Disabled** and Enabled.

Secure Boot Mode

Use this feature to select the desired secure boot mode for the system. The options are Standard and **Custom**.

CSM (Compatibility Support Module) Support

Select Enabled for CSM support, which will allow for system boot from a legacy device. Please make sure that your device is compatible with legacy boot before disabling CSM support. The options are Disabled and **Enabled**.

▶Enter Audit Mode (Available when "Secure Boot Mode" is set to Custom)

Select Ok to enter the Audit Mode workflow. It will result in erasing of Platform Key (PK) variables and reset system to the Setup/Audit Mode.

▶Enter Deployed Mode / Exit Deployed Mode (Available when "Secure Boot Mode" is set to Custom)

Select Ok to reset system to the User Mode or to the Deployed Mode.

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

The following information is displayed.

- Vendor Keys

Provision Factory Defaults

Select Enabled to install provision factory default settings after a platform reset while the system is in the Setup Mode. The options are **Disabled** and Enabled.

▶Restore Factory Keys (Available when any secure keys have been installed)

Select Yes to restore manufacturer default keys to ensure system security. The options are **Yes** and No. Selecting Yes will reset system to the Deployed mode.

▶Reset To Setup Mode (Available when any secure keys have been installed)

This feature resets the system to the Setup Mode. The options are **Yes** and No.

▶Export Secure Boot Variables (Available when a secure key has been installed)

Select Yes to export the NVRAM contents of secure boot variables to a storage device. The options are **Yes** and No.

▶Enroll Efi Image

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

▶Export Secure Boot Variables

The following information is displayed:

Secure Boot variable / Size / Key# / Key Source

▶Platform Key(PK)

Use this feature to enter and configure a set of values to be used as platform firmware keys for the system. These values also indicate the sizes, keys numbers, and the sources of the authorized signatures. Select Update to update the platform key. The options are **Details**, Export, Update, and Delete.

▶Key Exchange Keys (KEK)

Use this feature to enter and configure a set of values to be used as Key-Exchange-Keys for the system. These values also indicate the sizes, keys numbers, and the sources of the authorized signatures. Select Update to update your "Key Exchange Keys". Select Append to append your "Key Exchange Keys". The options are **Details**, Export, Update, Append, and Delete.

▶Authorized Signatures

Use this feature to enter and configure a set of values to be used as Authorized Signatures for the system. These values also indicate the sizes, keys numbers, and the sources of the authorized signatures. Select Update to update your "Authorized Signatures". Select Append to append your "Authorized Signatures". The options are **Details**, Export, Update, Append, and Delete.

▶Forbidden Signatures

Use this feature to enter and configure a set of values to be used as Forbidden Signatures for the system. These values also indicate sizes, key numbers, and key sources of the forbidden signatures. Select Update to update the "Forbidden Signatures". Select Append to append the "Forbidden Signatures". The options are **Details**, Export, Update, Append, and Delete.

▶Authorized TimeStamps

Use this feature to set and save the timestamps for the authorized signatures which will indicate the time when these signatures are entered into the system. These values also indicate sizes, keys, and key sources of the authorized timestamps. Select Update to update the "Authorized TimeStamps". Select Append to append the "Authorized TimeStamps". The options are **Details**, Export, Update, Append, and Delete.

▶OsRecovery Signature

This feature allows the user to set and save the authorized signatures used for OS recovery. Select Update to update the "OS Recovery Signatures". These values also indicate sizes,

keys, and key sources of the OsRecovery signatures. Select Append to append the "OS Recovery Signatures". The options are **Details**, Export, Update, Append, and Delete.

TCG Storage Security Configuration:

▶(Storage Device Name) (Available when the storage device is compliant with TCG specifications)

Select this device. Press <Enter> and the following information is displayed:

* TCG Storage Security Password Description:

* PASSWORD CONFIGURATION:

  * Security Subsystem Class:

  * Security Supported:

  * Security Enabled:

  * Security Locked:

  * Security Frozen:

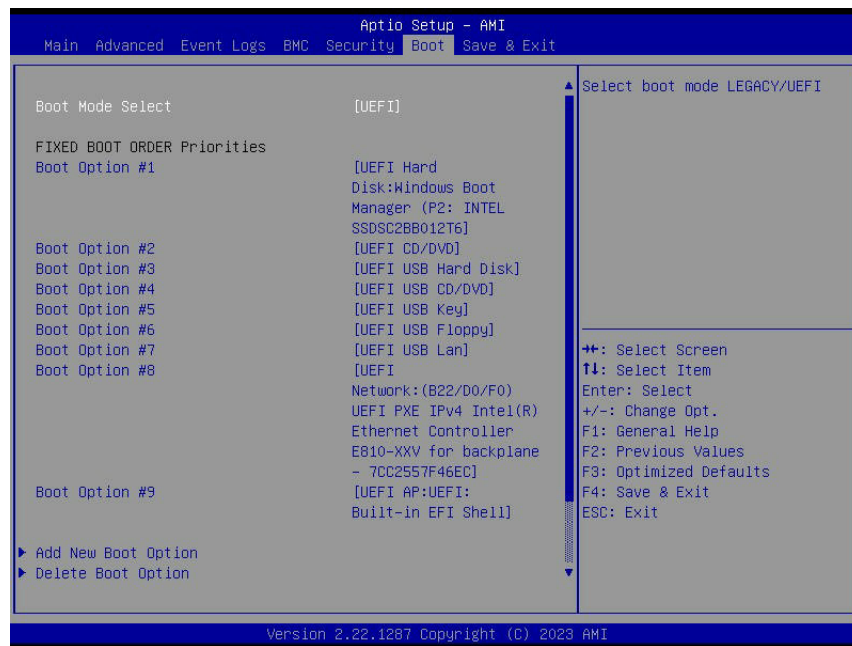 * Admin Pwd Status:

Set Admin Password

Use this feature to set the administrator password for this storage device.

Device Reset

Use this feature to reset the password configuration for this storage device.

4.7 Boot

Use this feature to configure Boot settings:

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

                                         ▲ Select boot mode LEGACY/UEFI
  Boot Mode Select              [UEFI]

  FIXED BOOT ORDER Priorities
  Boot Option #1                [UEFI Hard
                                Disk:Windows Boot
                                Manager (P2: INTEL
                                SSDSC2BB012T6]
  Boot Option #2                [UEFI CD/DVD]
  Boot Option #3                [UEFI USB Hard Disk]
  Boot Option #4                [UEFI USB CD/DVD]
  Boot Option #5                [UEFI USB Key]
  Boot Option #6                [UEFI USB Floppy]
  Boot Option #7                [UEFI USB Lan]        ↔: Select Screen
  Boot Option #8                [UEFI                 ↑↓: Select Item
                                Network:(B22/D0/F0)   Enter: Select
                                UEFI PXE IPv4 Intel(R) +/-: Change Opt.
                                Ethernet Controller   F1: General Help
                                E810-XXV for backplane F2: Previous Values
                                - 7CC2557F46EC]       F3: Optimized Defaults
  Boot Option #9                [UEFI AP:UEFI:        F4: Save & Exit
                                Built-in EFI Shell]   ESC: Exit

  ▶ Add New Boot Option
  ▶ Delete Boot Option                             ▼

                     Version 2.22.1287 Copyright (C) 2023 AMI
```

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 Option Priorities

This feature prioritizes the order of bootable devices from which the system will boot. Press <Enter> on each item sequentially to select devices.

When "Boot Mode Select" is set to Dual, 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 #9 ~ Boot Option #17

▶Add New Boot Option (Available when any storage device is detected by the BIOS)

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

Add boot option

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

Path for boot option

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

Boot option File Path

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

Create

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

Delete Boot Option

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

▶UEFI Hard Disk Drive BBS Priorities

This feature allows the user to set the system boot order of the UEFI HDD devices detected by the BIOS.
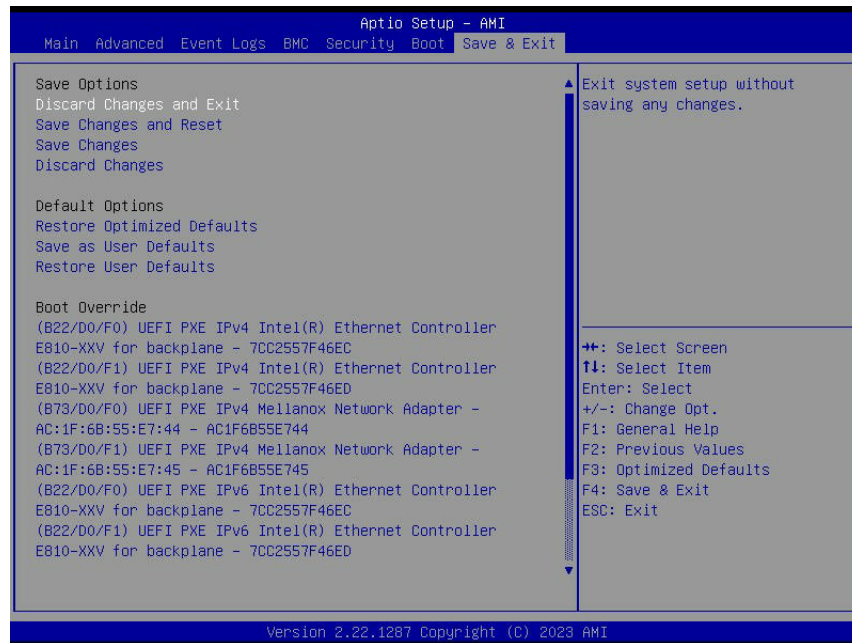
▶UEFI NETWORK Drive BBS Priorities

This feature allows the user to set the system boot order of the UEFI Network devices detected by the BIOS.

▶UEFI Application Boot Priorities

This feature allows the user to set the system boot order of the UEFI Application devices detected by the BIOS.

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
 (B22/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller
 E810-XXV for backplane - 7CC2557F46EC
 (B22/D0/F1) UEFI PXE IPv4 Intel(R) Ethernet Controller
 E810-XXV for backplane - 7CC2557F46ED
 (B73/D0/F0) UEFI PXE IPv4 Mellanox Network Adapter -   →←: Select Screen
 AC:1F:6B:55:E7:44 - AC1F6B55E744                       ↑↓: Select Item
 (B73/D0/F1) UEFI PXE IPv4 Mellanox Network Adapter -   Enter: Select
 AC:1F:6B:55:E7:45 - AC1F6B55E745                       +/-: Change Opt.
 (B22/D0/F0) UEFI PXE IPv6 Intel(R) Ethernet Controller F1: General Help
 E810-XXV for backplane - 7CC2557F46EC                  F2: Previous Values
 (B22/D0/F1) UEFI PXE IPv6 Intel(R) Ethernet Controller F3: Optimized Defaults
 E810-XXV for backplane - 7CC2557F46ED                  F4: Save & Exit
                                           ▼             ESC: Exit

                  Version 2.22.1287 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 exit 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 as "User Default" values in 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 by the user instead of the one specified in the boot list. This is a one-time override.

Appendix A

BIOS POST Codes

A.1 BIOS POST Codes

The AMI BIOS supplies additional checkpoint codes, which are documented online at http://www.supermicro.com/support/manuals/ ("AMI BIOS POST Codes User's Guide").

For information on AMI updates, please refer to http://www.ami.com/products/.

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 drive, an external USB/SATA media drive, or the BMC KVM console.

2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.

3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing **F11** during the system startup.
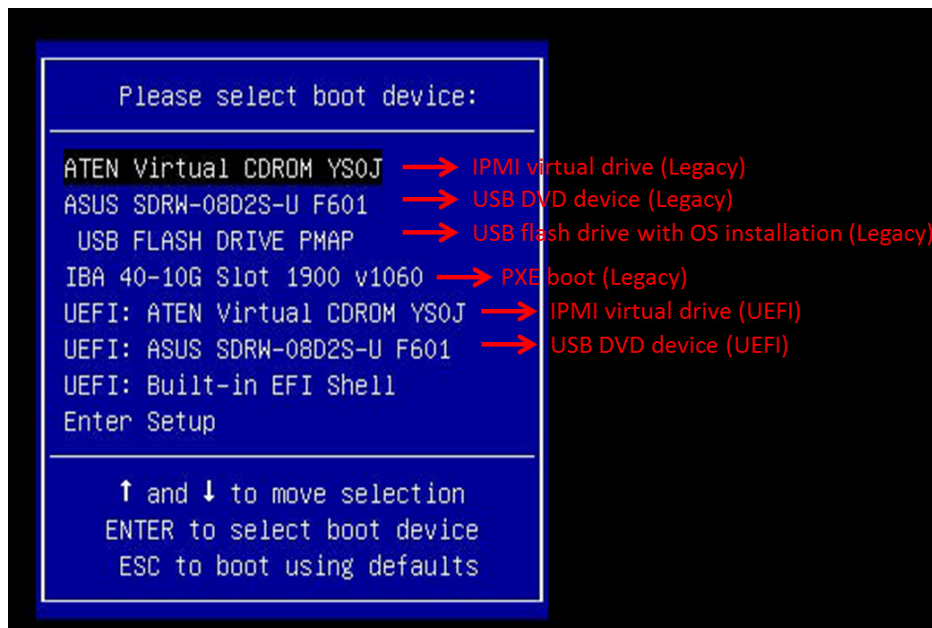
4. During Windows Setup, continue to the dialogue box where you select the drives on which to install Windows. If the disk you want to use is not listed, click on "Load driver" link at the bottom left corner.
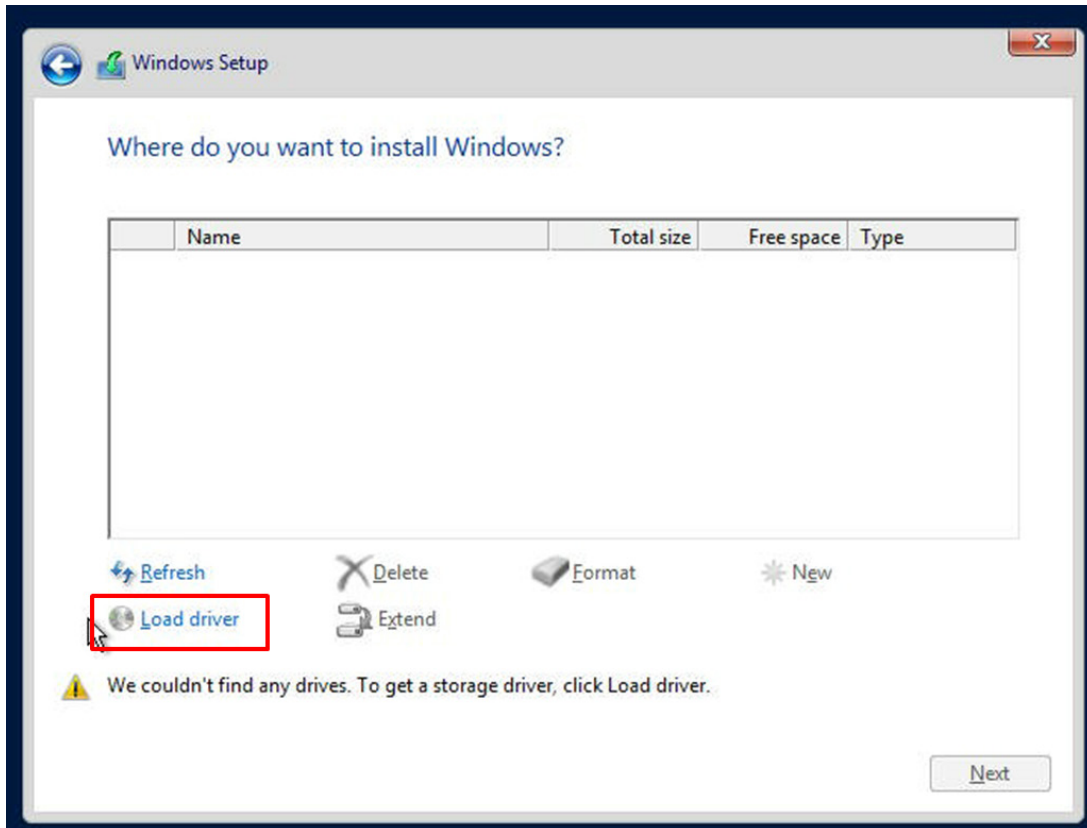
To load the driver, browse the USB flash drive for the proper driver files.

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

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

5. Once all devices are specified, please 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 contains drivers and utilities for your system at https://www.supermicro.com/wdl/driver. Some of these must be installed, such as the chipset driver.

After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash drive or a 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 https://www.supermicro.com/en/products/motherboards. Find the product page for your motherboard, and "Download the Latest Drivers and Utilities".

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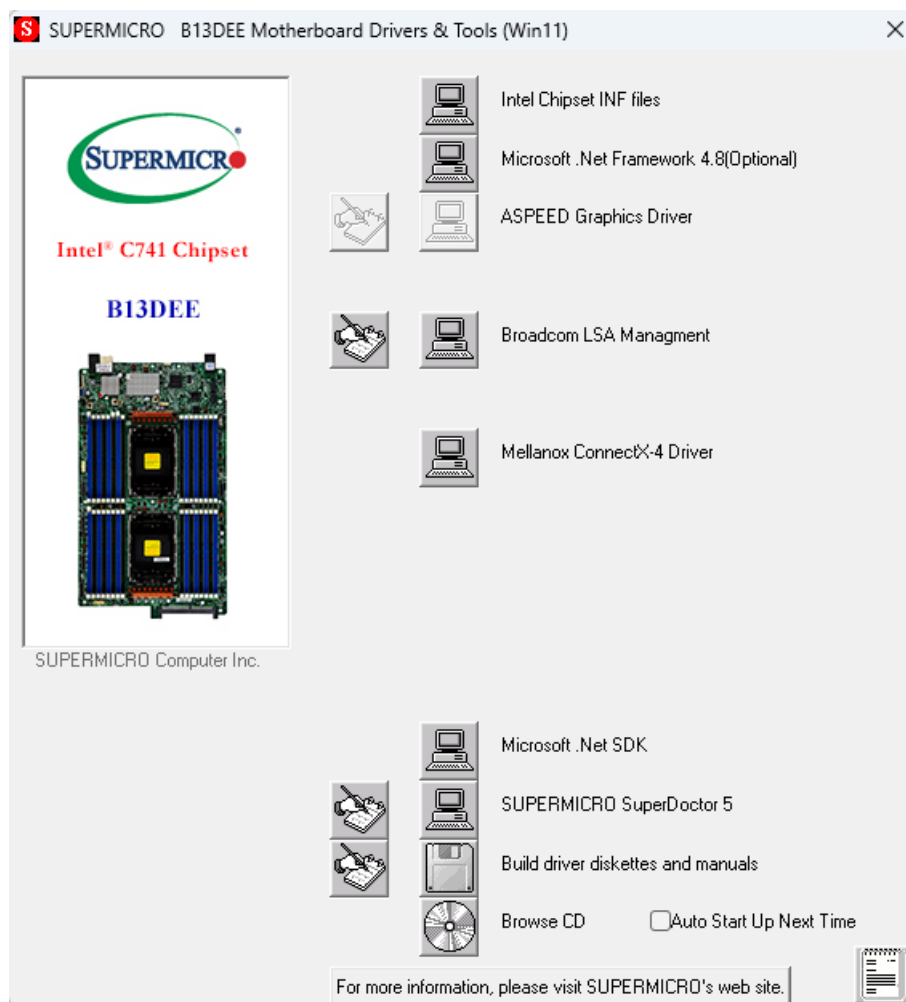
Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to the bottom) one at a time. **After installing each item, you must re-boot the system before moving on to the next item on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

B.3 BMC

The B13DEE supports the Baseboard Management Controller (BMC). BMC is used to provide remote access, monitoring and management. There are several BIOS settings that are related to BMC.

For general documentation and information on BMC, please visit our website at: https://www.supermicro.com/support/resources/bios_ipmi.php.

B.4 Logging into the BMC (Baseboard Management Controller)

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

When logging in to the BMC for the first time, please use the unique password provided by Supermicro to log in. You can change the unique password to a user name and password of your choice for subsequent logins.

For more information regarding BMC passwords, please visit our website at https://www.supermicro.com/en/support/BMC_Unique_Password.

Appendix C

Standardized Warning Statements

The following statements are industry standard warnings, provided to warn the user of situations where a potential bodily injury may occur. Should you have questions or experience difficulty, contact Supermicro's Technical Support department for assistance. Only certified technicians should attempt to install components or configure system settings.

Read this section in its entirety before installing or configuring components.

These warnings may also be found on our website at https://www.supermicro.com/en/about/policies/safety-information.

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 البطنية

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.