

# B14DBT

## USER'S MANUAL

Revision 1.0a (MNL-2699)

The information in this User's Manual has been carefully reviewed and is believed to be accurate. The vendor 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. Note: For the most up-to-date version of this manual, see our website at https://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 or Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in industrial environment for Class A device or in residential environment for Class B device. 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 https://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 https://www.P65Warnings.ca.gov.



AVERTISSEMENT : Ce produit peut vous exposer à des agents chimiques, y compris le plomb, identifié par l'État de Californie comme pouvant causer le cancer, des malformations congénitales ou d'autres troubles de la reproduction. Pour de plus amples informations, prière de consulter https://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: May 08, 2026

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2026 by Super Micro Computer, Inc.
All rights reserved.
**Published in the United States of America**

# Preface

## About This Manual

This manual is written for professional system integrators and PC technicians. It provides information for the installation and use of the B14DBT motherboard. Installation and maintenance should be performed by certified service technicians only.

## Notes

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

- Supermicro product manuals: https://www.supermicro.com/support/manuals
- Product drivers and utilities: https://www.supermicro.com/wdl
- Product safety info: https://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 on our website: https://www.supermicro.com/about/policies/disclaimer.cfm?url=/wdl/utility/Lot9_Secure_Data_Deletion_Utility
- Frequently Asked Questions: https://www.supermicro.com/FAQ/index.php
- If you still have questions after referring to our FAQs, contact our support team. Region-specific Technical Support email addresses can be found at: "Contacting Supermicro" on page 10
- If you have any feedback on Supermicro product manuals, contact our writing team at: Techwriterteam@supermicro.com

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

## Conventions Used in the Manual

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



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



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



**Warning!** Indicates hazardous moving parts may be encountered while handling a fan or components near a fan.

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

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

# Contents

***Contacting Supermicro*** ..... ***10***

***Chapter 1: Introduction*** ..... ***11***

1.1 Quick Reference ..... 12

Motherboard Layout ..... 13

Quick Reference Table ..... 15

Memory Slots ..... 16

Motherboard Features ..... 17

System Block Diagram ..... 21

1.2 Platform Overview ..... 22

Flexible and Scalable Processor Architectural Design ..... 22

New Software Capability and Performance Optimization ..... 22

1.3 Special Features ..... 23

Recovery from AC Power Loss ..... 23

1.4 System Health Monitoring ..... 24

Onboard Voltage Monitors ..... 24

Fan Status Monitor with Firmware Control ..... 24

Environmental Temperature Control ..... 24

1.5 ACPI Features ..... 25

***Chapter 2: Component Installation*** ..... ***26***

2.1 Static-Sensitive Devices ..... 28

Precautions ..... 28

Unpacking ..... 28

2.2 Motherboard Installation ..... 29

Tools Needed ..... 29

Locations of Mounting Holes ..... 30

Installing the Motherboard ..... 30

2.3 Processor and Heatsink Installation ..... 32

LGA 4710 Socket E2 Processors ..... 32

Processor Top View ..... 32

Overview of the Processor Socket ..... 33

Overview of the Processor Carrier ..... 33

Processor Carriers ..... 34
Overview of the Processor Heatsink Module ..... 35
Installing the Processor ..... 38
Assembling the Processor Heatsink Module ..... 40
Preparing the Processor Socket for Installation ..... 47
Preparing to Install the PHM into the Processor Socket ..... 48
Installing the Processor Heatsink Module ..... 51
Removing the Processor Heatsink Module ..... 59
2.4 Memory Support and Installation ..... 69
Memory Support ..... 69
The Intel Xeon 6700-Series Processors with E-Cores ..... 69
The Intel Xeon 6700-Series Processors with P-Cores ..... 72
DIMM Installation ..... 76
DIMM Removal ..... 79
2.5 Battery Removal and Installation ..... 80
Battery Removal ..... 80
Proper Battery Disposal ..... 80
Battery Installation ..... 80
2.6 Connections, Jumpers, and LEDs ..... 81
Power Supply and Power Connections ..... 81
25 G Midplane ..... 81
MEZZ1 Card ..... 81
PCIe 5.0 M.2 Slot and M.2 Standoff (MH-SRW1) ..... 81
MCIO PCIe 5.0 x8 Connectors ..... 81
Power Connectors ..... 81
Power Supply ..... 82
Headers and Connections ..... 82
Complex Programmable Logic Device Header ..... 82
Liquid Cooling Leakage Sensor Header ..... 82
M.2 M-Key PCIe 5.0 x4 Slot ..... 83
Motherboard CPLD Header ..... 83
TPM/Port 80 Header ..... 83
Universal Serial Bus (USB) 3.0/2.0 Port ..... 83
VROC RAID Key Header ..... 84

Front Panel Control Board and Front I/O Connector ..... 85
Front Control Panel ..... 85
Advanced I/O Module (AIOM) for Front I/O Support (JAIOM1) ..... 85
Jumper Settings ..... 85
CMOS Clear ..... 86
LED Indicators ..... 87
BMC Heartbeat LED ..... 87
LAN1/LAN2 Activity LED Indicators (D40/D42) ..... 87
LAN1/LAN2 Link LED Indicators (D39/D41) ..... 87
M.2 LED ..... 88
Onboard Power LED ..... 88
***Chapter 3: Troubleshooting*** ..... ***89***
3.1 Troubleshooting Procedures ..... 90
Before Power On ..... 90
No Power ..... 90
No Video ..... 90
System Boot Failure ..... 90
Memory Errors ..... 91
Losing the System's Setup Configuration ..... 91
If the System Becomes Unstable ..... 91
3.2 Technical Support Procedures ..... 93
3.3 Frequently Asked Questions ..... 94
3.4 Motherboard Battery ..... 95
3.5 Where to Get Replacement Components ..... 96
3.6 Returning Merchandise for Service ..... 97
3.7 Feedback ..... 98
***Chapter 4: UEFI BIOS*** ..... ***99***
4.1 Introduction ..... 100
Updating BIOS ..... 100
Starting the Setup Utility ..... 100
4.2 Main Setup ..... 102
4.3 Advanced Setup Configurations ..... 104
Boot Feature Menu ..... 104
CPU Configuration Menu ..... 105

Advanced Power Management Configuration Menu ..... 108
CPU P State Control Menu ..... 109
Hardware PM State Control Menu ..... 111
CPU C State Control Menu ..... 112
Package C State Control Menu ..... 113
CPU1/CPU2 Core Disable Bitmap Menu ..... 113
Chipset Configuration Menu ..... 114
Uncore Configuration Menu ..... 114
Memory Configuration Menu ..... 116
Memory Topology Menu ..... 116
Memory Map Menu ..... 117
Memory RAS Configuration Menu ..... 117
Security Configuration Menu ..... 118
IIO Configuration Menu ..... 123
CPU1/CPU2 Configuration Menu ..... 124
Intel VT for Directed I/O (VT-d) Menu ..... 126
PCIe Leaky Bucket Configuration Menu ..... 127
Super IO Configuration Menu ..... 127
Serial Port 1 Configuration Menu ..... 128
Serial Port 2 Configuration Menu ..... 128
Serial Port Console Redirection Menu ..... 129
Network Stack Configuration Menu ..... 132
MAC:(MAC address)-IPv6 Network Configuration Menu ..... 133
MAC:(MAC address)-IPv4 Network Configuration Menu ..... 134
PCIe/PCI/PnP Configuration Menu ..... 134
ACPI Settings Menu ..... 137
Trusted Computing Menu ..... 138
Supermicro KMS Server Configuration Menu ..... 140
Super-Guardians Configuration Menu ..... 142
HTTP Boot Configuration Menu ..... 144
Intel(R) Ethernet Controller Menu ..... 145
TLS Authenticate Configuration Menu ..... 147
VLAN Configuration (MAC:(MAC address)) ..... 148
Driver Health Menu ..... 148

4.4 Event Logs ..... 150
4.5 BMC ..... 152
System Event Log Menu ..... 152
BMC Network Configuration Menu ..... 153
4.6 Security ..... 156
Supermicro Security Erase Configuration Menu ..... 157
HDD Security Configuration Menu ..... 158
Secure Boot Menu ..... 159
TCG Storage Security Configuration Menu ..... 162
4.7 Boot ..... 163
4.8 Save & Exit ..... 165
***Appendix A: BIOS Codes*** ..... ***167***
BIOS Error POST (Beep) Codes ..... 167
Additional BIOS POST Codes ..... 167
***Appendix B: Software*** ..... ***168***
Microsoft Windows OS Installation ..... 168
Installing the OS ..... 168
B.1 Driver Installation ..... 171
BMC ..... 171
BMC ADMIN User Password ..... 172
B.2 Logging into the BMC ..... 173
***Appendix C: Standardized Warning Statements*** ..... ***174***
Battery Handling ..... 174
Product Disposal ..... 176

# Contacting Supermicro

**Headquarters**

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.
Tel: +1 (408) 503-8000
Fax: +1 (408) 503-8008
Email: Marketing@supermicro.com (General Information)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
Support@supermicro.com (Technical Support)
RMA@Supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)
Website: https://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 (Sales Inquiries)
Support_Europe@supermicro.com (Technical Support)
RMA_Europe@supermicro.com (RMA Support)
Website: https://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 Inquiries)
Support@supermicro.com.tw (Technical Support)
RMA@supermicro.com.tw (RMA Support)
Website: https://www.supermicro.com.tw

# Chapter 1:

# Introduction

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

**1.1 Quick Reference** ..... **12**
Motherboard Layout ..... 13
Quick Reference Table ..... 15
Memory Slots ..... 16
Motherboard Features ..... 17
System Block Diagram ..... 21
**1.2 Platform Overview** ..... **22**
Flexible and Scalable Processor Architectural Design ..... 22
New Software Capability and Performance Optimization ..... 22
**1.3 Special Features** ..... **23**
Recovery from AC Power Loss ..... 23
**1.4 System Health Monitoring** ..... **24**
Onboard Voltage Monitors ..... 24
Fan Status Monitor with Firmware Control ..... 24
Environmental Temperature Control ..... 24
**1.5 ACPI Features** ..... **25**

## 1.1 Quick Reference

For details on the B14DBT motherboard layout, features, and other quick reference information, refer to the content below.

## Motherboard Layout

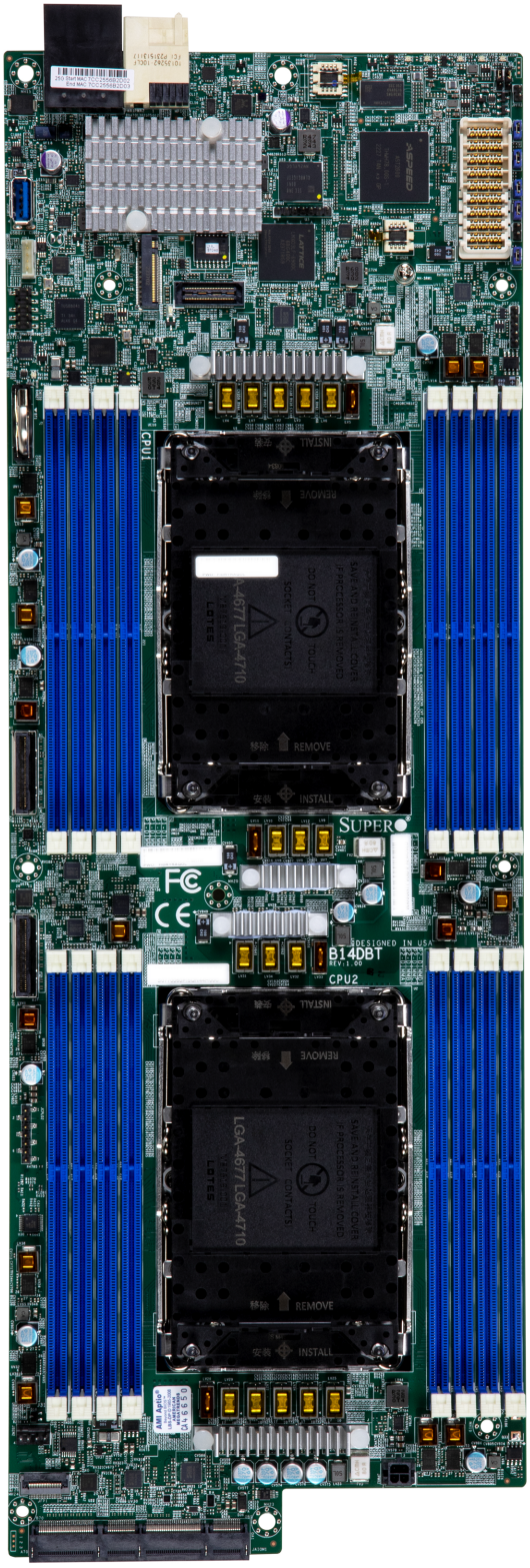



**Figure 1-1. B14DBT Motherboard Image**

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

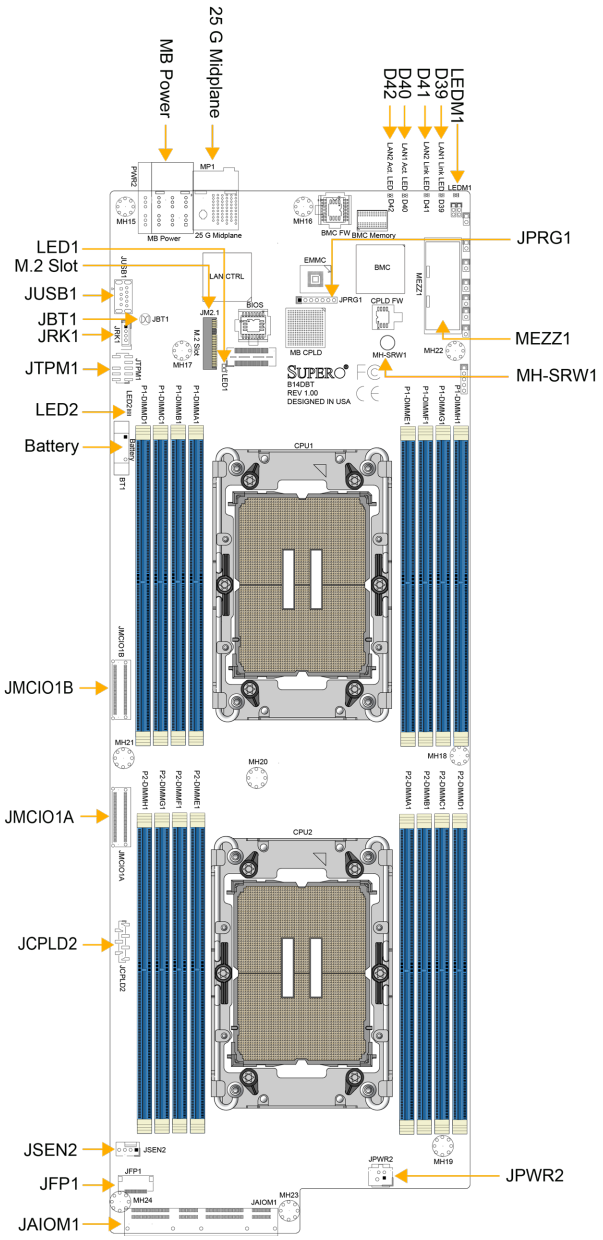



**Figure 1-2. B14DBT Motherboard Layout**

**Notes:**

- For detailed information on jumpers, connectors, and LED indicators, see "Component Installation" on page 26.
- "■" indicates the location of pin 1.
- "MH" indicates the location of a mounting hole.
- Components not documented are for internal testing purposes only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. To avoid possible explosion, do not install the onboard battery upside down.

## Quick Reference Table

| Jumper | Description | Jumper Setting (Default: Bold) |
|---|---|---|
| JBT1 | CMOS Clear | Open (**Normal**) |

| LED | Description | Status |
|---|---|---|
| D39 | LAN1 Link LED | Green: Solid on: 25G<br>Yellow: 10G/1G (Onboard LAN E810) |
| D40 | LAN1 Activity LED | Green: Blinking: Onboard LAN E810 Active |
| D41 | LAN2 Link | Green: Solid on: 25G<br>Yellow: 10G/1G (Onboard LAN E810 Speed) |
| D42 | LAN2 Activity LED | Green: Blinking: Onboard LAN E810 Active |
| LED1 | M.2 Activity LED | Green: Blinking: M.2 Active |
| LED2 | Onboard LAN Power Indicator | Solid Amber: Onboard LAN E810 Power: Normal |
| LEDM1 | BMC Heartbeat LED | Blinking Green: BMC Normal (Active),<br>Solid Green: During BMC Reset or Cold Reboot |

| Connector | Description |
|---|---|
| Battery (BT1) | Onboard Battery |
| JAIOM1 | Supermicro Advanced Input/Output Module (AIOM) PCIe 5.0x16 Connector |
| JPRG1 | Programming Header for Mainboard Complex Programmable Logic Devices |
| JCPLD2 | Complex Programmable Logic Device (CPLD) |

| Connector | Description |
|---|---|
| JFP1 | Front Control Panel |
| JM2_1 | PCIe 5.0x4 M.2 Slot with support for the 2280 form factor |
| JMCIO1A/JMCIO1B | MCIO PCIe 5.0x8 Slots for Backplane EDSFF E1.S Drive Support |
| MP1 | Middle-plane Connectors for Signals and Guides |
| JPWR2 | 4-pin Backplane Power Connector (Pin 1 and 2: Ground, Pin 3 and 4: 12 V) |
| PWR2 | Motherboard Power Supply Connector (12 V) |
| JSEN2 | Coolant Leakage Sensor |
| JTPM1 | Trusted Platform Module/Port 80 Connector |
| MEZZ1 | Mezzanine Card PCIe 5.0x16 Slot |
| MH-SRW1 | M.2 Slot Standoff for M.2 Card Support |
| JUSB1 | Internal USB 3.0/2.0 Type-A USB Port for Two USB Connections |
| VROC RAID Key (JRK1) | Intel VROC RAID Key Header for NVMe RAID Support |

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

## Memory Slots

This motherboard supports up to 64GB of DDR5 memory in 32 slots.

| DIMM Slots Supported by CPU1 | DIMM Slots Supported by CPU2 |
|---|---|
| P1-DIMMA1 | P2-DIMMA1 |
| P1-DIMMB1 | P2-DIMMB1 |
| P1-DIMMC1 | P2-DIMMC1 |
| P1-DIMMD1 | P2-DIMMD1 |
| P1-DIMME1 | P2-DIMME1 |
| P1-DIMMF1 | P2-DIMMF1 |
| P1-DIMMG1 | P2-DIMMG1 |
| P1-DIMMH1 | P2-DIMMH1 |

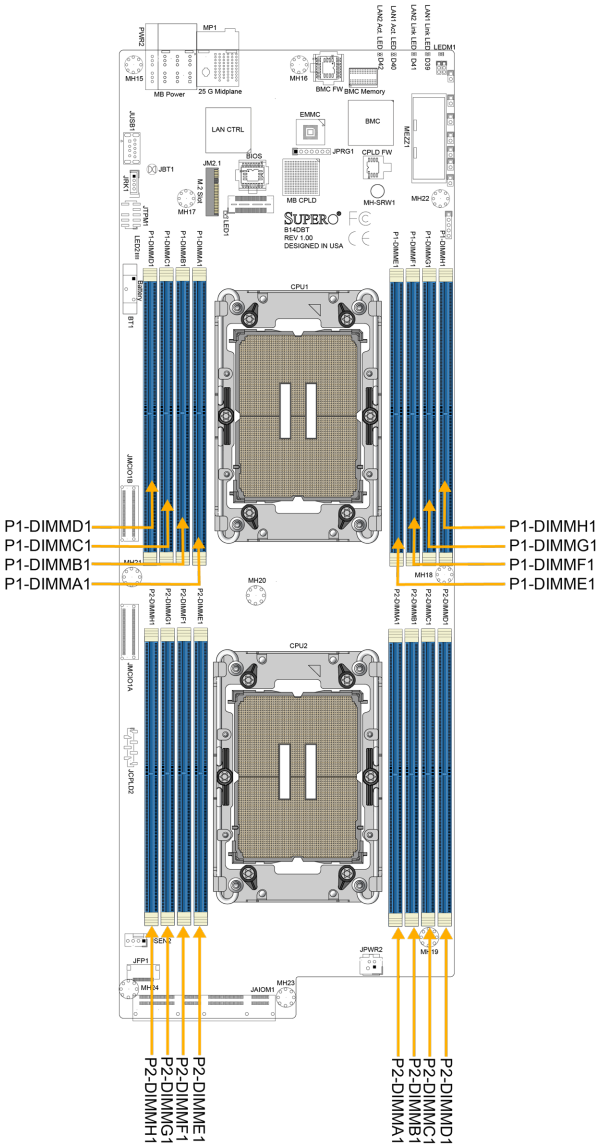



**Figure 1-3. Memory Slots**

## Motherboard Features

| Motherboard Features |
|---|
| **Processor** |
| • Supports dual Intel® Xeon® 6 Processors (in Socket E2 LGA 4710) with four UPIs (24 GT/s max.) and a thermal design power (TDP) up to 350 W.<br>• Supports Intel® Xeon® 6700E Series Processor (XCC, LCC, and HCC) SKUs. |
| **Memory** |

| Motherboard Features |
| --- |
| • Supports ECC DDR5 RDIMM/3DS RDIMM memory with speeds up to 6400 MT/s in 16 slots. (Memory speed/capacity support depends on the processors used in the system.) |
| **DIMM Size** |
| • Up to 256 GB<br><br>**Note:** For the latest processor/memory updates, refer to our website at https://www.supermicro.com/en/products/motherboards. |
| **Expansion Slots** |
| • One AIOM PCIe 5.0x16 connector<br>• One Mezzanine card PCIe 5.0x16 slot<br>• One M.2 M-Key PCIe 5.0x4 slot (2280 Format)<br>• Two MCIO PCIe 5.0x8 connectors for backplane EDSFF E1.S drive support |
| **Baseboard Management Controller (BMC)/Network** |
| • ASPEED AST2600 BMC<br>• One dedicated BMC LAN/VGA |
| **Graphics** |
| • Graphics controller and VGA support from ASPEED AST2600 BMC |
| **I/O Devices** |
| • VGA support from BMC |
| **Peripheral Devices** |
| • Internal USB 3.0/2.0 Type-A port for two USB connections |
| **BIOS** |
| • AMI SPI BIOS<br>• NAND Flash 512 Mb support<br>• SPI dual/quad speed control, Real Time Clock (RTC) wakeup, riser card auto detection support, IPMIView, SMCIPMITOOL, IPMI CFG, Redundant power supply unit detection, SDO, SSM, SPM, EFI GUI |
| **Power Connections** |

| Motherboard Features |
| --- |
| • Motherboard power supply connector (PWR2)<br>• 4-pin backplane power connector (JPWR2) |
| **Power Management** |
| • ACPI power management<br>• S1, S5 support<br>• Power button override mechanism<br>• Power-on mode for AC power recovery<br>• Power supply monitoring |
| **System Health Monitoring** |
| • Onboard voltage monitoring for +3.3 V, +3.3 V Standby, +5 V, +5 V Standby, +12 V, Vcore, Vmem<br>• Onboard temperature monitoring for processor, GPU, VRM, LAN, system, peripheral, memory, NIC, M.2 SSD, AOM, and NVMe devices<br>• Eight processor switch phase voltage regulator<br>• Processor thermal trip support<br>• Platform Environment Control Interface (PECI) and TSI |
| **Fan Control** |
| • Fan status monitoring via BMC connections<br>• Three cooling zones<br>• Low-noise fan speed control<br>• 6-pin proprietary fan support |
| **System Management** |
| • Chassis intrusion header and detection<br>• Server platform service<br>• RoHS |
| **Firmware Integrity/System Security** |

| Motherboard Features |
| --- |
| • Trusted Platform Module (TPM) support (optional part needed)<br>• Root of Trust (RoT) support to protect firmware security by detecting critical data corruption, and restoring platform integrity |
| **LED Indicators** |
| • CPU/system overheat LED<br>• Power/suspend state indicator LED<br>• Fan-Failed LED<br>• UID/remote UID<br>• LAN activity LED<br>• HDD activity LED |
| **Dimensions** |
| 18.23" (L) x 6.3" (W) Proprietary (463.04 mm x 160.02 mm) |

**Notes:**

- The processor maximum Thermal Design Power (TDP) is subject to chassis and heatsink cooling restrictions, and it also depends on server SKUs. For proper thermal management, check the chassis and heatsink specifications.
- For BMC configuration instructions, refer to the Embedded BMC Configuration User's Guide available at https://www.supermicro.com/support/manuals.

## System Block Diagram

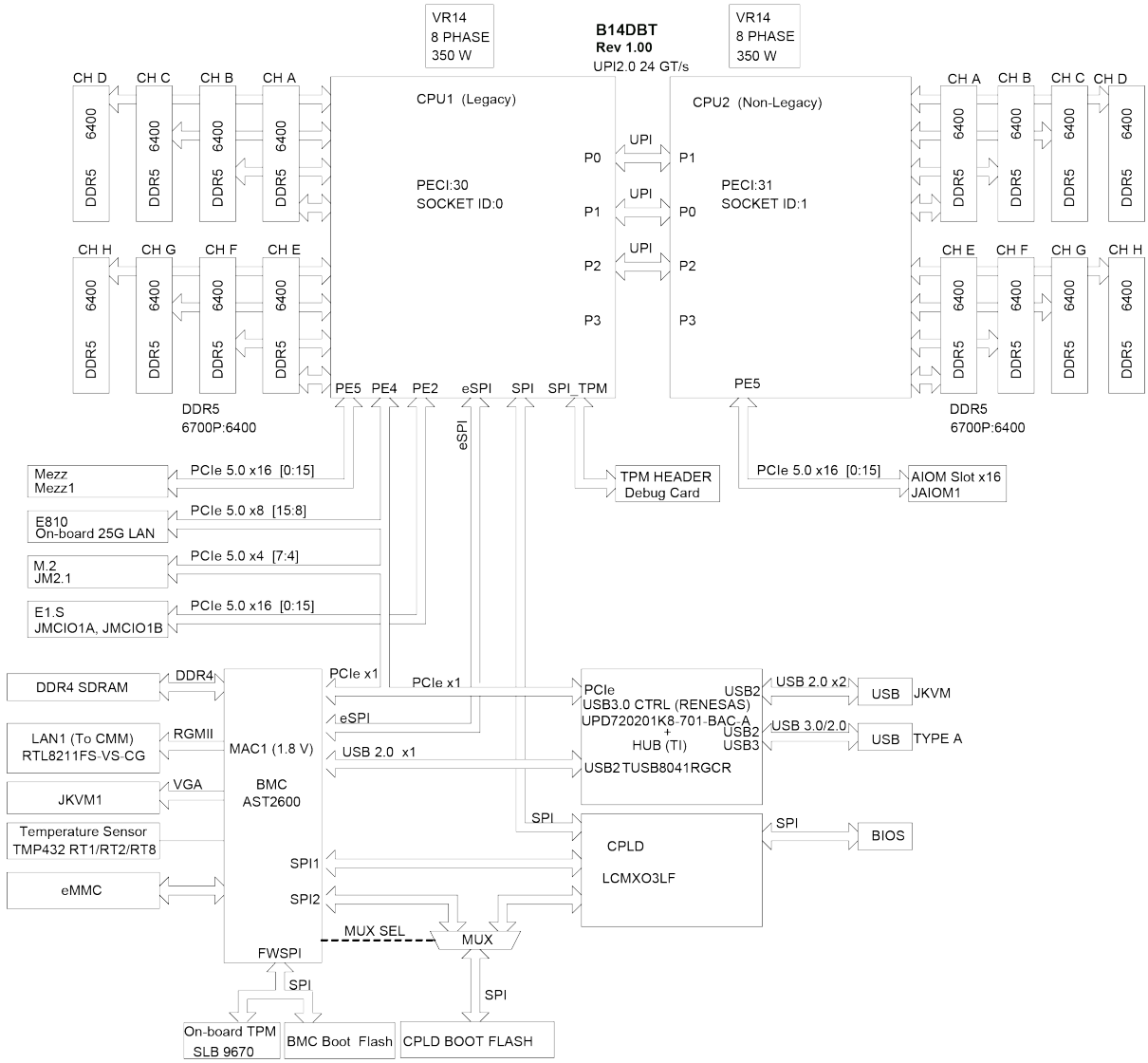



**Figure 1-4. System Block Diagram**

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

## 1.2 Platform Overview

Built upon the capability of the Intel® Xeon® 6 Processors, the B14DBT motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users.

The B14DBT motherboard dramatically increases system performance for a multitude of server applications and supports the following features:

### Flexible and Scalable Processor Architectural Design

The Intel® Xeon® 6 Processors platform is built upon System-on-Chip (SoC) modular design, which offers computer systems with flexible, unrestrictive expansion options.

- Separate Compute and IO silicon chiplets
- Modular die fabric that enables flexible construction
- EmiB packaging with high bandwidth/low latency support
- Common IP, Firmware, OS, and platform ingredients
- Processor scalability: E-core (1S-2S) supported (with E-core for efficiency)
- A wide range of core counts and thermals supported
- Memory: up to 8 channels of DDR
- PCIe 88 lanes including CXL2.0 64 lanes up to 4 UPI 2.0 links supported
- Self-boot capabilities

### New Software Capability and Performance Optimization

- AMX supports FP16 (Floating Point 16-bit format) for AI/ML
- 2 K memory encryption keys with 256-bit strength
- 64 KB, 16-way I-cache with improved branch predictor and miss recovery
- More outstanding memory requests and prefetch capabilities
- New Intel Xeon Architecture optimized for power efficiency throughput performance

## 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 Advanced Setup Configurations under "UEFI BIOS" on page 99 for this setting. The default setting is **Last State**.

# 1.4 System Health Monitoring

## Onboard Voltage Monitors

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

## 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 processor and chassis fans are controlled via IPMI.

## Environmental Temperature Control

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

**Note:** To avoid possible system overheating, 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 drives, and printers.

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play and an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures while providing a processor architecture-independent implementation that is compatible with operating systems such as Microsoft Windows, Red Hat Linux, and Ubuntu Linux. For detailed information about our certified operating systems, refer to OS Compatibility.

# Chapter 2:

# Component Installation

This chapter provides instructions on installing and replacing main system components for the B14DBT motherboard. To prevent compatibility issues, only use components that match the specifications and/or part numbers given.

Installation or replacement of most components require that power first be removed from the system. Follow the procedures given in each section.


**2.1 Static-Sensitive Devices ..... 28**
Precautions ..... 28
Unpacking ..... 28
**2.2 Motherboard Installation ..... 29**
Tools Needed ..... 29
Installing the Motherboard ..... 30
**2.3 Processor and Heatsink Installation ..... 32**
LGA 4710 Socket E2 Processors ..... 32
Overview of the Processor Socket ..... 33
Overview of the Processor Carrier ..... 33
Overview of the Processor Heatsink Module ..... 35
Installing the Processor ..... 38
Assembling the Processor Heatsink Module ..... 40
Preparing the Processor Socket for Installation ..... 47
Preparing to Install the PHM into the Processor Socket ..... 48
Installing the Processor Heatsink Module ..... 51
Removing the Processor Heatsink Module ..... 59
**2.4 Memory Support and Installation ..... 69**
Memory Support ..... 69
DIMM Installation ..... 76
DIMM Removal ..... 79
**2.5 Battery Removal and Installation ..... 80**
Battery Removal ..... 80
Proper Battery Disposal ..... 80

Battery Installation ..... 80
**2.6 Connections, Jumpers, and LEDs ..... 81**
Power Supply and Power Connections ..... 81
Headers and Connections ..... 82
Front Panel Control Board and Front I/O Connector ..... 85
Jumper Settings ..... 85
LED Indicators ..... 87

## 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 board from the antistatic bag.
- Handle the motherboard only by its edges. 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. To avoid possible explosion, do not install the onboard battery upside down.

### Unpacking

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

## 2.2 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.

**Notes:**

- To avoid damaging the motherboard and its components, do not use a force greater than 8 lbf-in on each mounting screw during motherboard installation.
- Some components are very close to the mounting holes. Take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

### Tools Needed

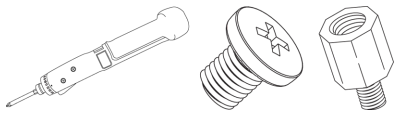


**Figure 2-1. Driver (1) (Right), Phillips Screws (10) (Middle), Standoffs (10 or As Needed) (Left)**

### *Locations of Mounting Holes*

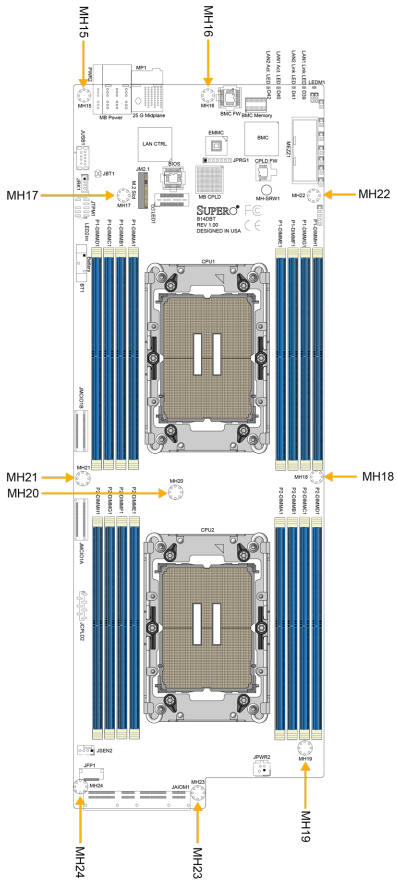



**Figure 2-2. B14DBT Mounting Holes**

## Installing the Motherboard

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

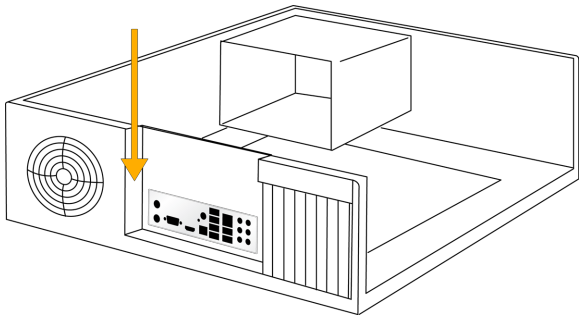


**Figure 2-3. Installing the I/O Shield**

**Note:** Images displayed are for illustration purposes only. The components installed in your system may or may not look exactly the same as the graphics shown in the manual.

2. Locate the mounting holes on the motherboard. See Motherboard Installation for the location.

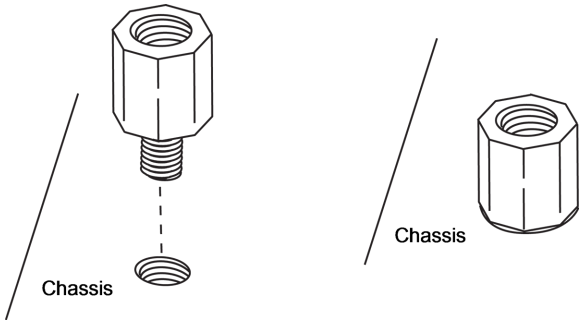



**Figure 2-4. Locating the Mounting Holes**

3. Locate the matching mounting holes on the chassis. Align the mounting holes on the motherboard against the mounting holes on the chassis.

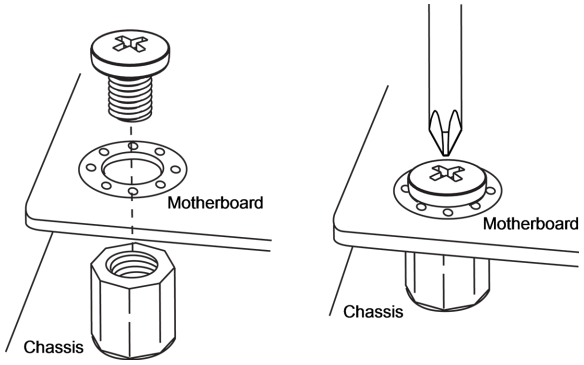



**Figure 2-5. Aligning the Mounting Holes**

4. Install standoffs in the chassis as needed.
5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
6. Insert pan head #6 screws into the mounting holes on the motherboard and the matching mounting holes on the chassis.
7. Make sure that the motherboard is securely placed in the chassis.

## 2.3 Processor and Heatsink Installation

This section provides procedures to install the processor(s) and heatsink(s).

**Notes:**

- Take industry standard precautions to avoid ESD damage. For details, see "Static-Sensitive Devices" on page 28.
- Before starting, make sure that the plastic socket cap is in place and none of the socket pins are bent. If any damage is noted, contact your retailer.
- Do not connect the system power cord before the processor and heatsink installation is complete.
- 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 processor socket.
- Install the processor in the socket and the motherboard into the chassis before installing the heatsink.
- When buying a processor separately, use only a Supermicro certified heatsink.
- Refer to the Supermicro website for the most recent processor support.
- When installing the 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.

### LGA 4710 Socket E2 Processors

#### *Processor Top View*

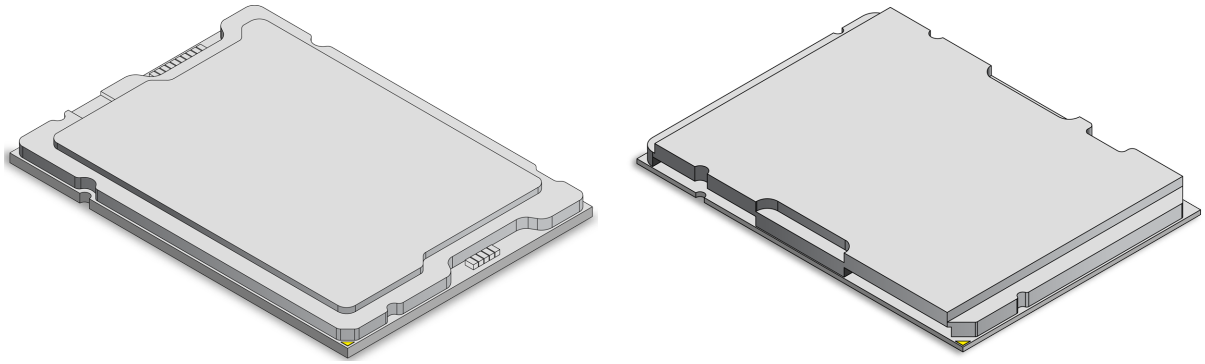


**Figure 2-6. Processor (SP XCC left, SP HCC/LCC right)**

**Note:** The motherboard supports three processor SKUs: SP XCC, SP HCC, and SP LCC. Each SKU supports a specific carrier; the SP XCC processor supports Carrier E2A while SP HCC and SP LCC support Carrier E2B. Make sure the processors of the same SKU are on the motherboard.

## Overview of the Processor Socket

The processor socket is protected by a plastic protective cover.

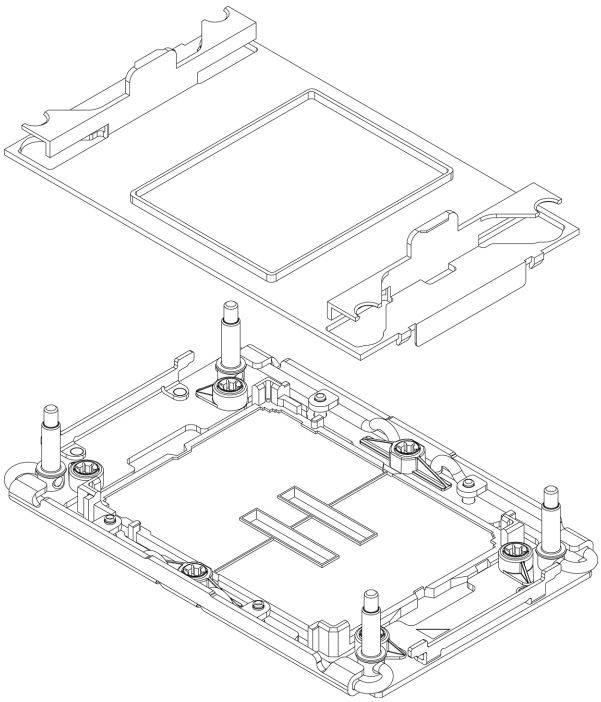


**Figure 2-7. Plastic Protective Cover and Processor Socket**

## Overview of the Processor Carrier

The motherboard supports two types of processors and their associated processor carrier.

## *Processor Carriers*

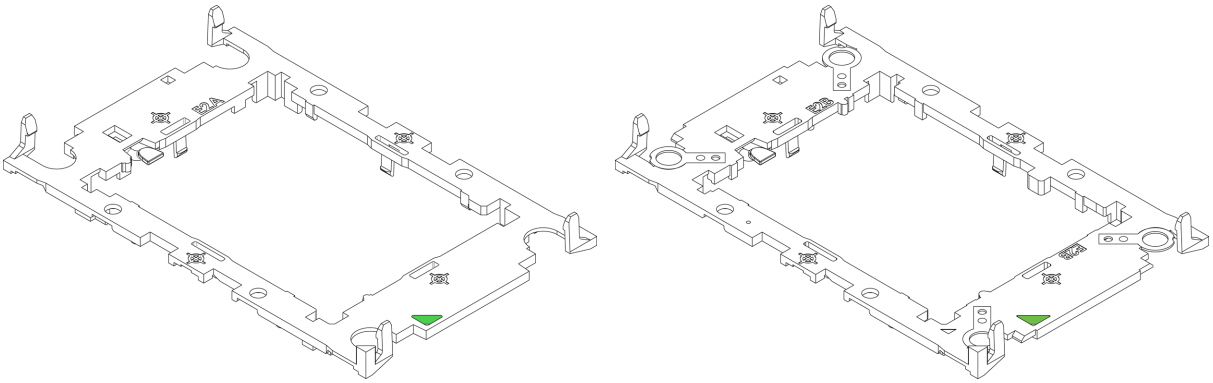


**Figure 2-8. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)**

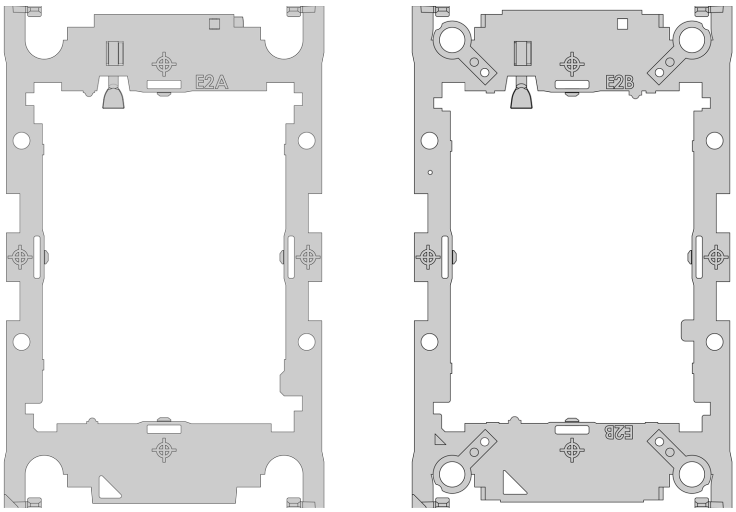



**Figure 2-9. Carrier Top View (SP XCC E2A left, SP HCC/LCC E2B right)**

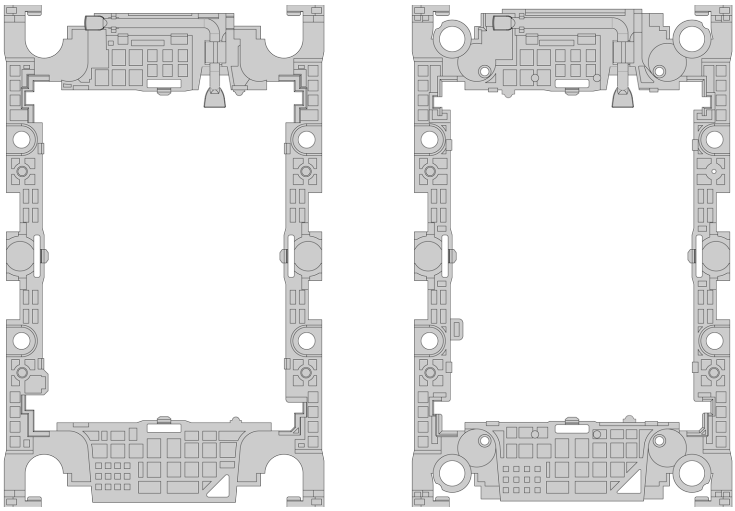


**Figure 2-10. Carrier Bottom View (SP XCC E2A left, SP HCC/LCC E2B right)**

## Overview of the Processor Heatsink Module

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

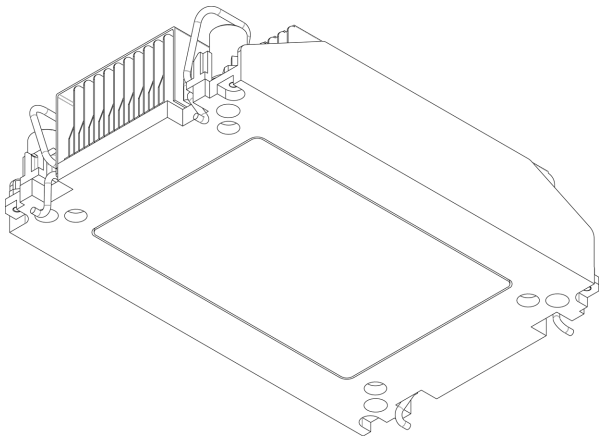


**Figure 2-11. Heatsink (1U)**

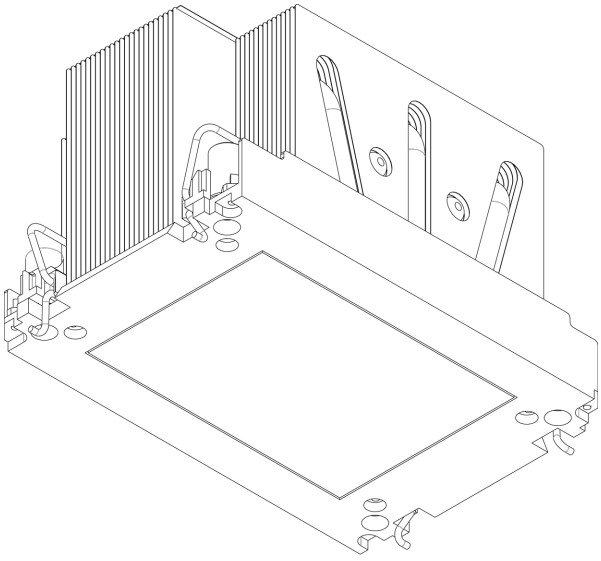


**Figure 2-12. Heatsink (2U)**

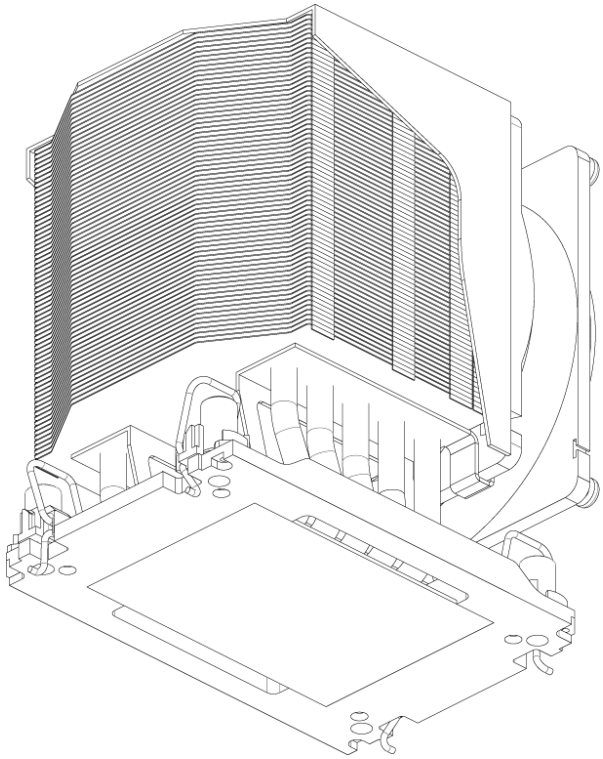


**Figure 2-13. Heatsink (4U)**

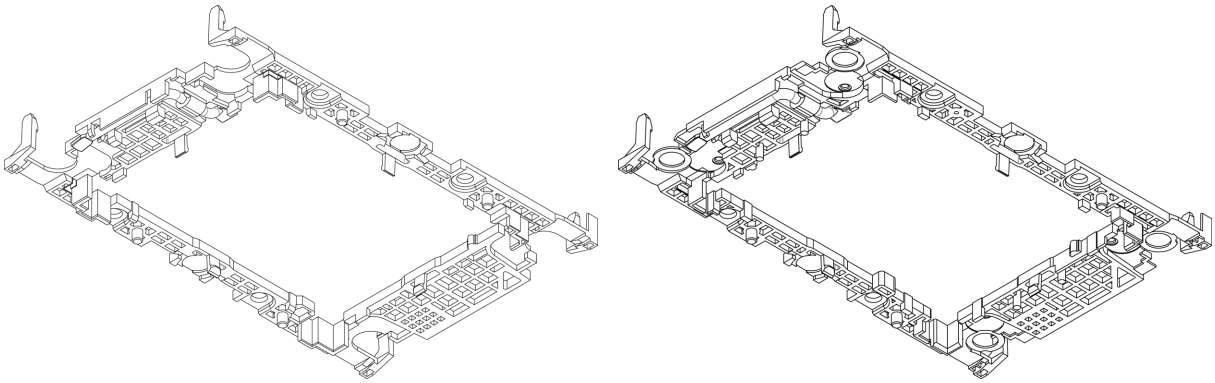


**Figure 2-14. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)**

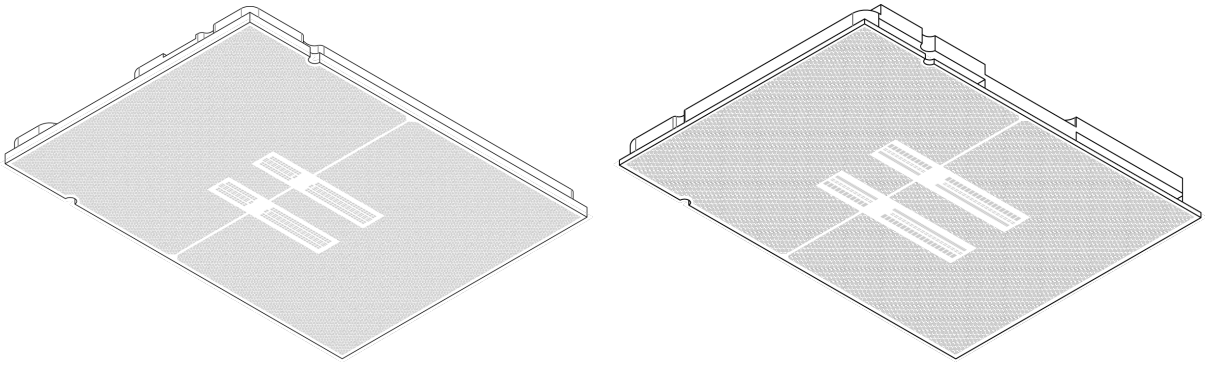


**Figure 2-15. Processor (SP XCC E2A left, SP HCC/LCC E2B right)**

## Installing the Processor

To install the processor, follow the steps below:

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

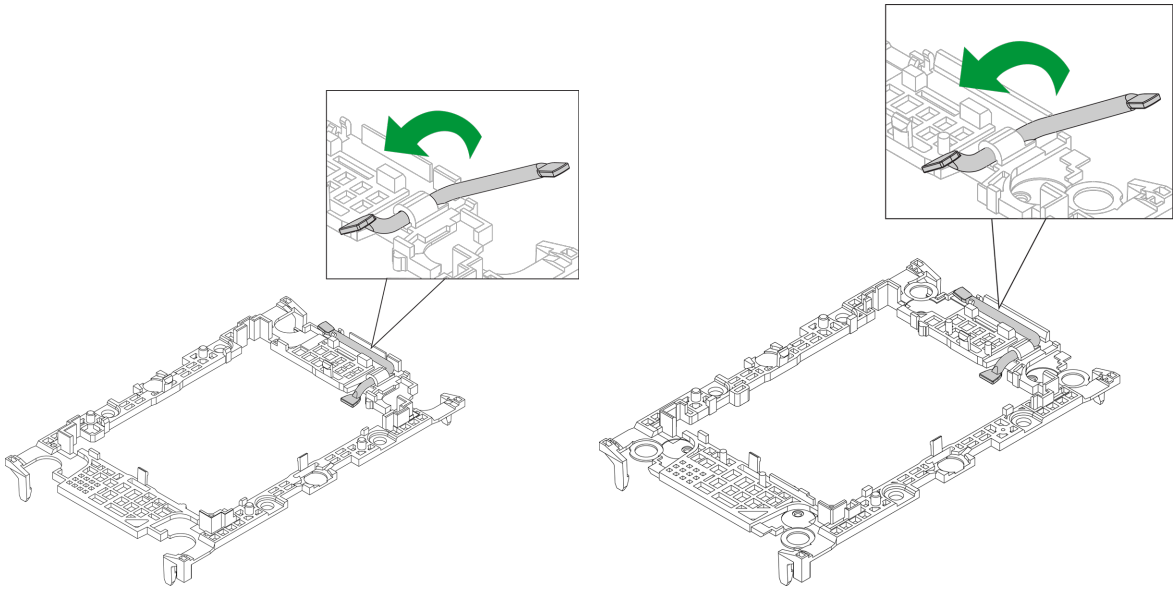


**Figure 2-16. Carrier Lever (SP XCC left, SP HCC/LCC right)**

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

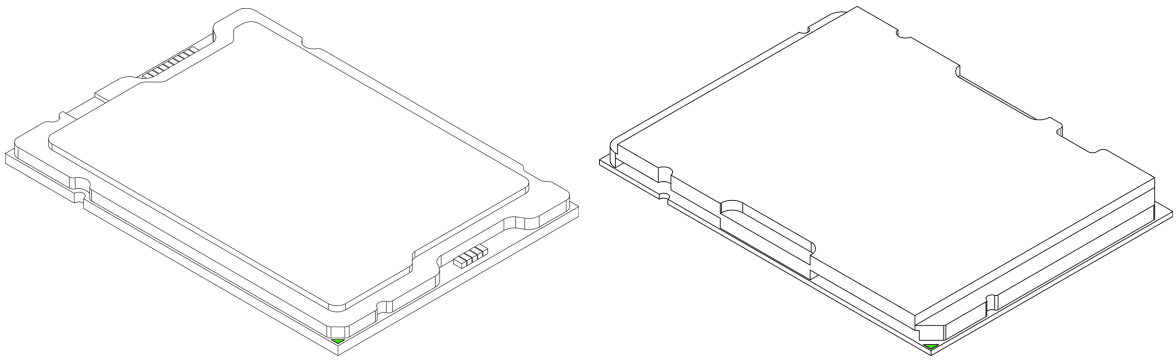


**Figure 2-17. Processor (SP XCC E2A left, SP HCC/LCC E2B right)**

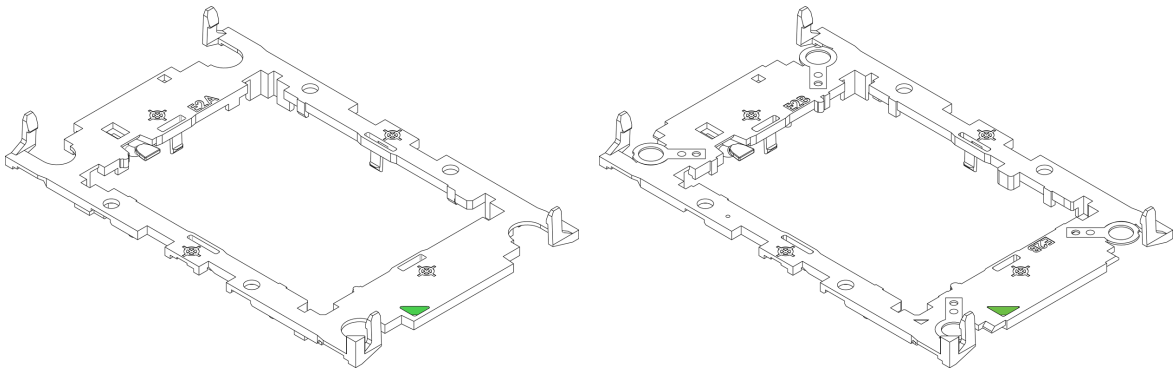


**Figure 2-18. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)**

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

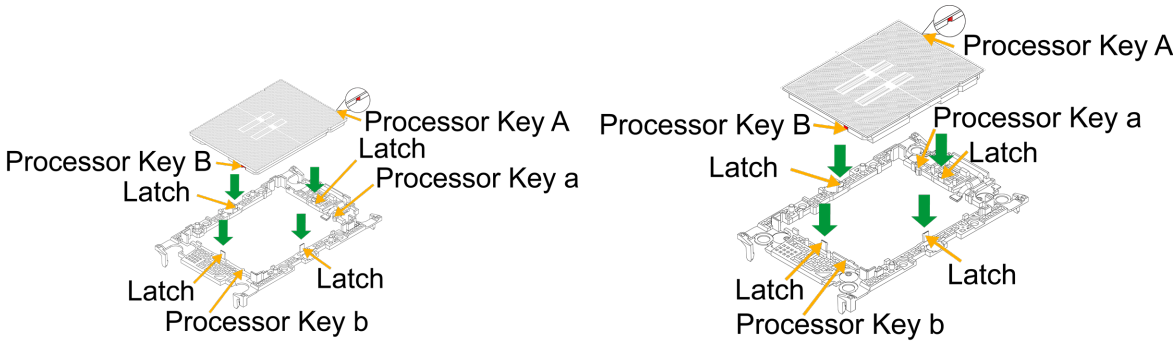



**Figure 2-19. Keys and Latches Locations (SP XCC E2A left, SP HCC/LCC E2B right)**

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

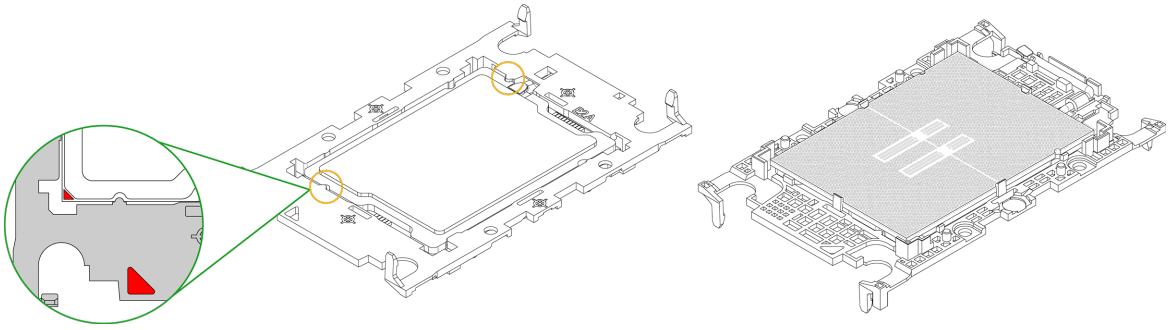


**Figure 2-20. SP XCC E2A Keys and Latches**

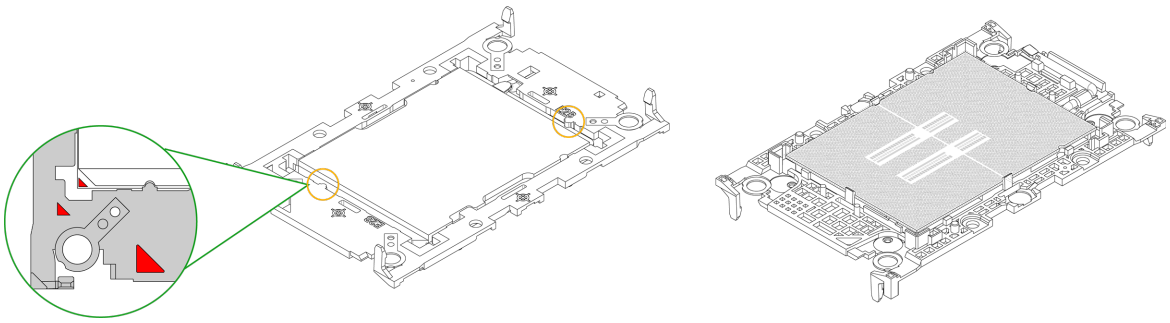


**Figure 2-21. SP HCC/LCC E2B Keys and Latches Together**

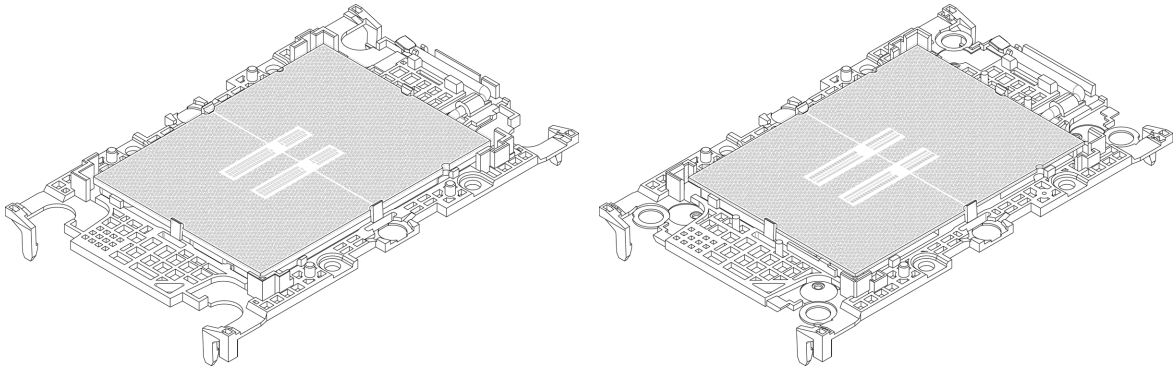


**Figure 2-22. Carrier Assembly Completed (SP XCC E2A left, SP HCC/LCC E2B right)**

## Assembling the Processor Heatsink Module

After installing the processor into the carrier, mount it onto the heatsink to create the processor heatsink module (PHM):

1. Loosen the Torx screw from the heatsink.

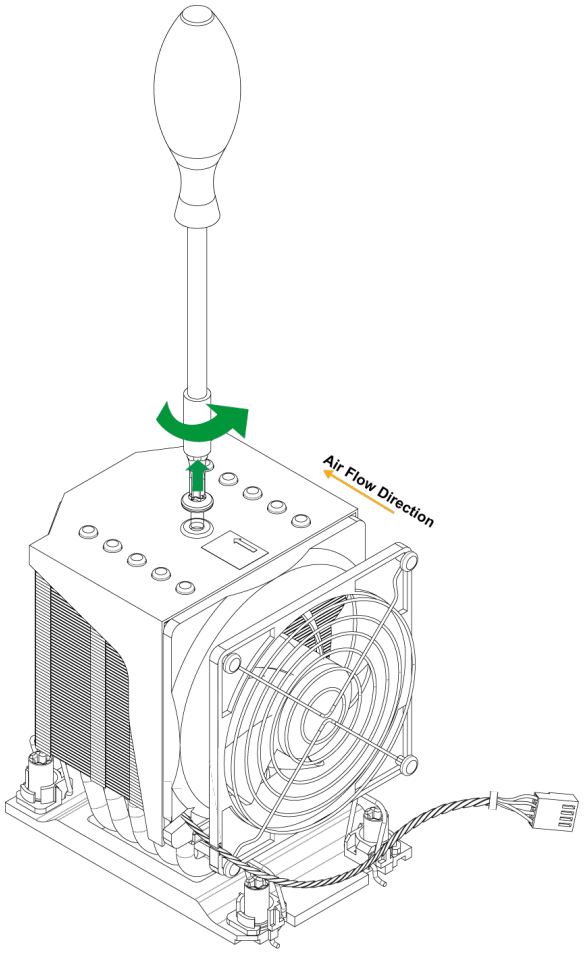



**Figure 2-23. Loosening the Screw**

2. Gently pull the heatsink fan upward to detach it from the heatsink.

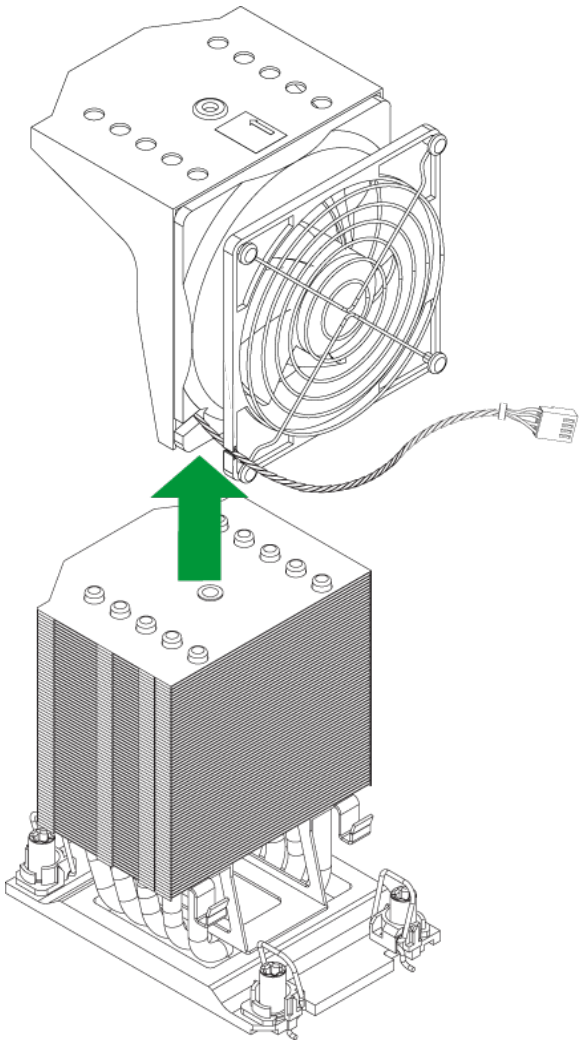


**Figure 2-24. Heatsink Fan Detached**

3. Note the label on top of the heatsink, which marks the airflow direction. Turn the heatsink over and orient the heatsink so the airflow arrow is pointing towards the triangle on the processor.
4. If this is a new heatsink, the thermal grease has been pre-applied. Otherwise, apply the proper amount of thermal grease.
5. Hold the processor carrier so the processor's gold contacts are facing up, then align the holes of the processor carrier with the holes on the heatsink. Press the processor carrier down until it snaps into place. The plastic clips of the processor carrier will lock at the four corners.

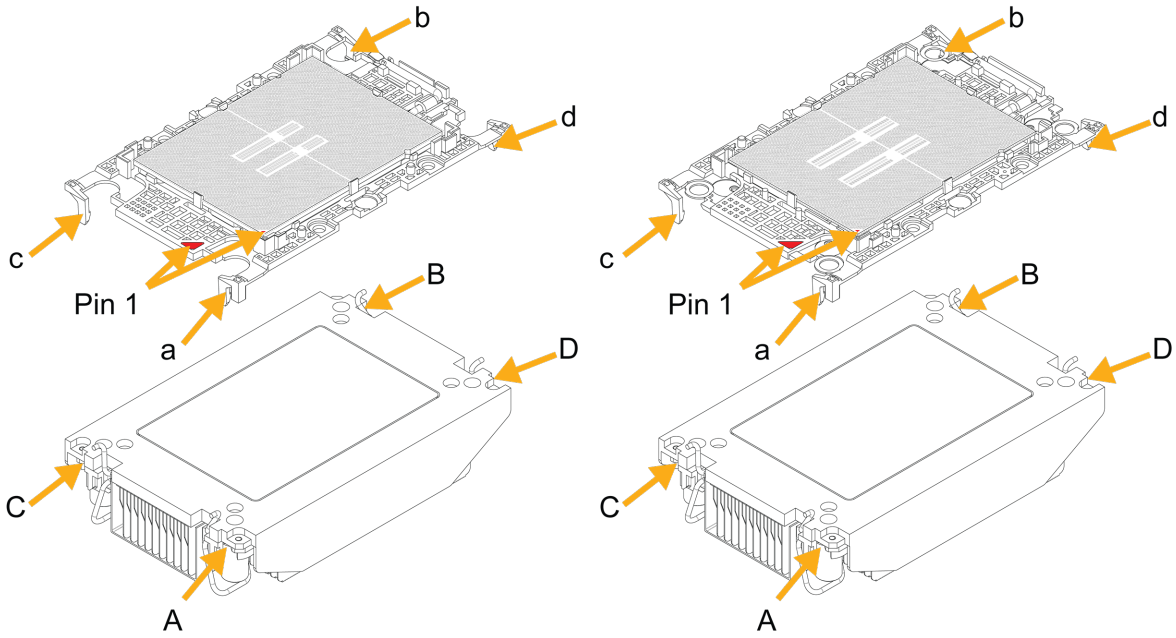



**Figure 2-25. Carrier with 1U Heatsink (SP XCC left, SP HCC/LCC right)**

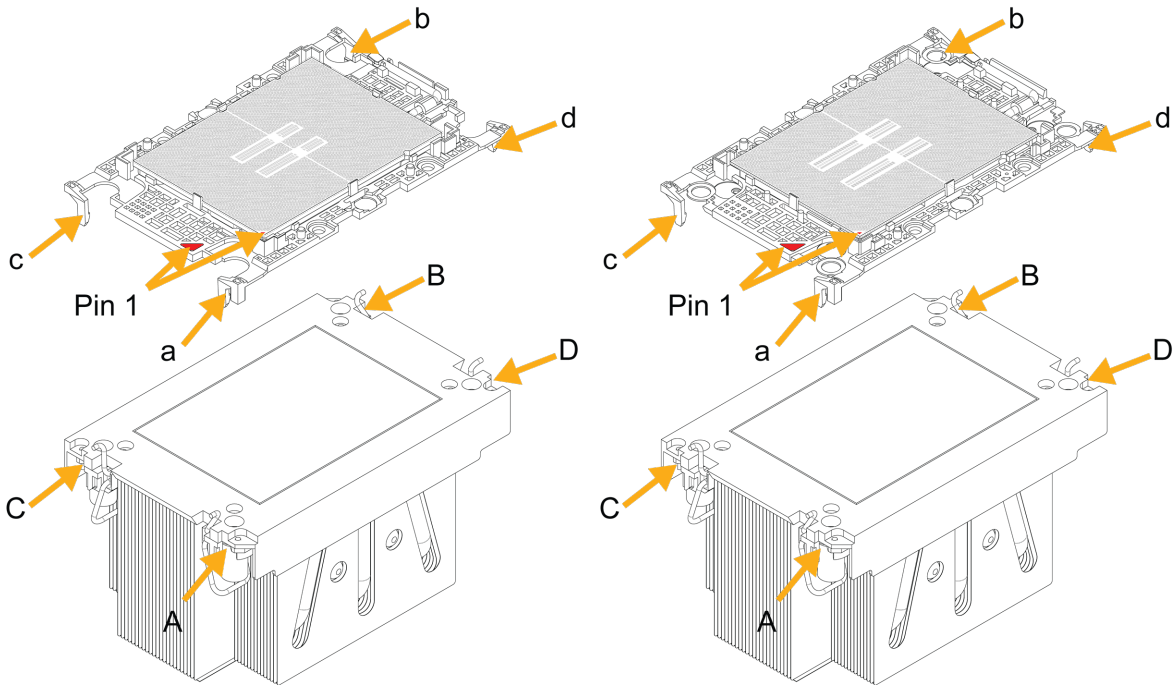



**Figure 2-26. Carrier with 2U Heatsink (SP XCC left, SP HCC/LCC right)**

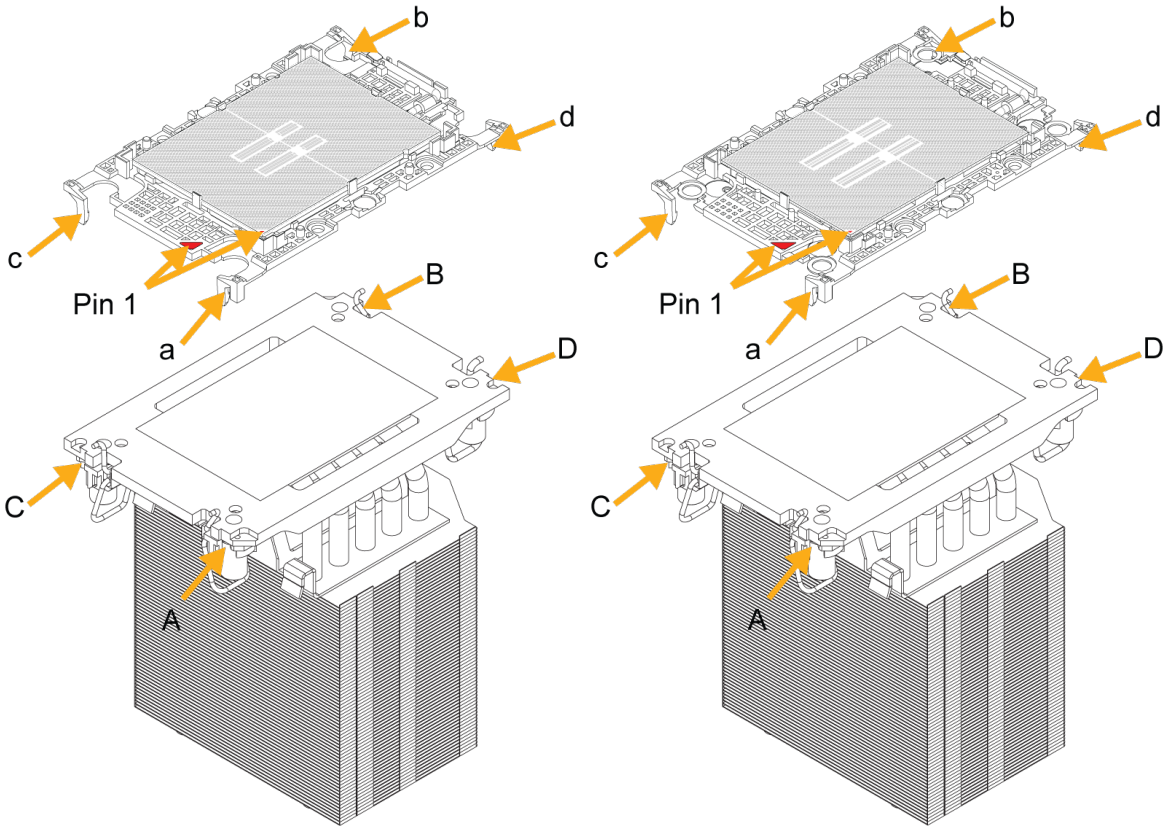



**Figure 2-27. Carrier with 4U Heatsink (SP XCC left, SP HCC/LCC right)**

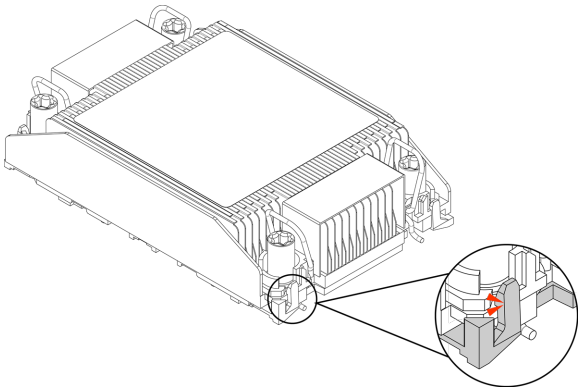


**Figure 2-28. PHM Plastic Clips Locked (1U)**

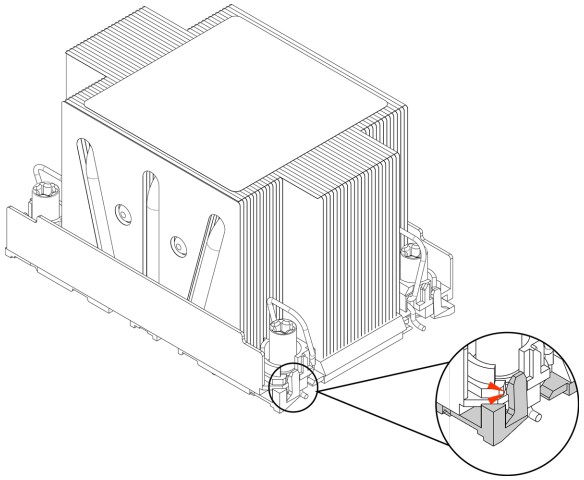


**Figure 2-29. PHM Plastic Clips Locked (2U)**

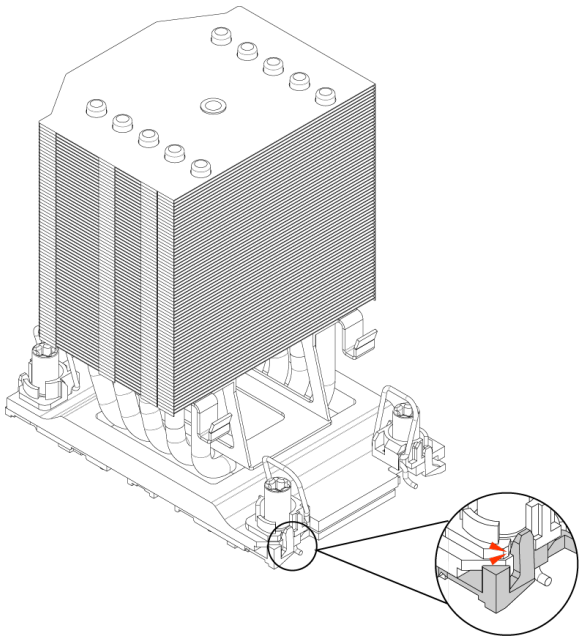


**Figure 2-30. PHM Plastic Clips Locked (4U)**

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

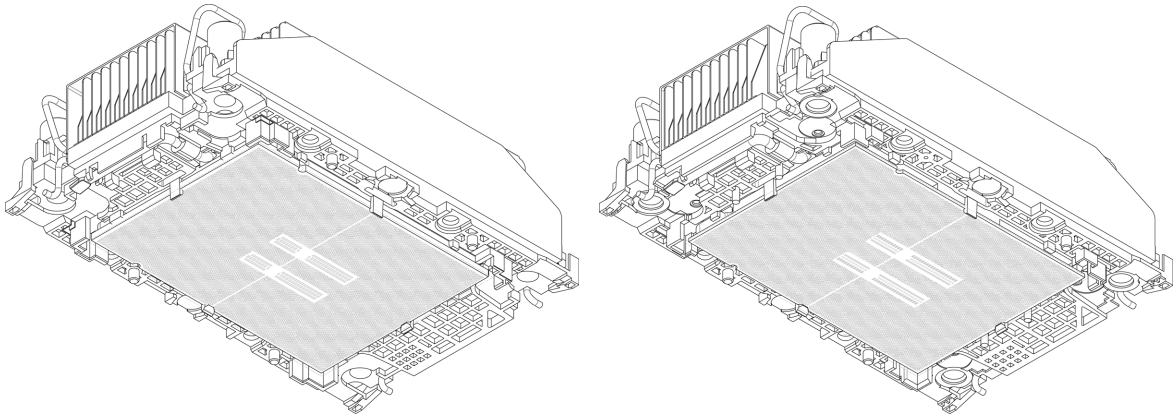


**Figure 2-31. 1U PHM Completed (SP XCC left, SP HCC/LCC right)**

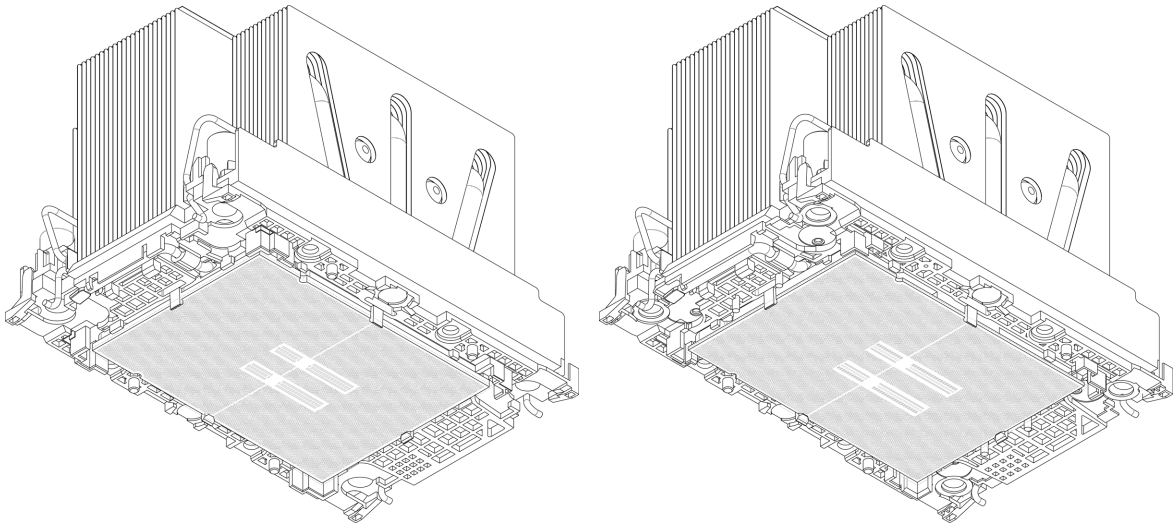


**Figure 2-32. 2U PHM Completed (SP XCC left, SP HCC/LCC right)**

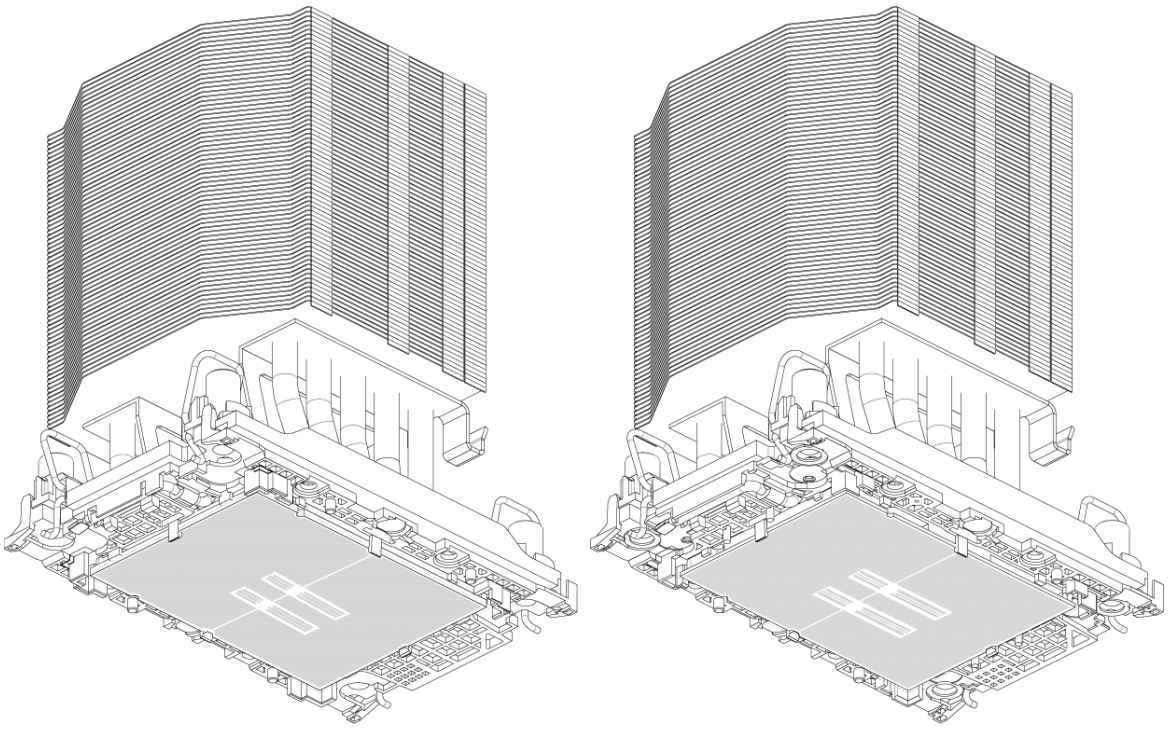


**Figure 2-33. 4U PHM Completed (SP XCC left, SP HCC/LCC right)**

## Preparing the Processor Socket for Installation

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

1. Press the tabs inward.

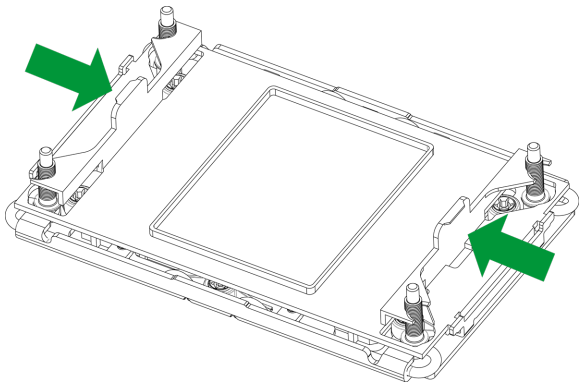


**Figure 2-34. Processor Socket with Plastic Protective Cover**

2. Pull up the protective cover from the socket.

**Note:** Do not touch or bend the socket pins.

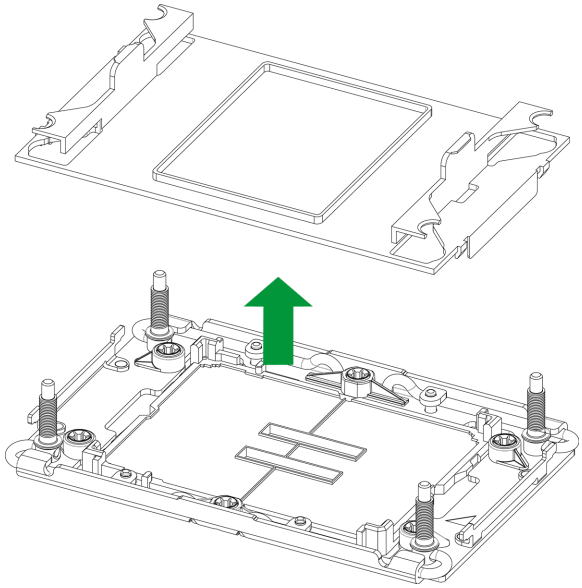
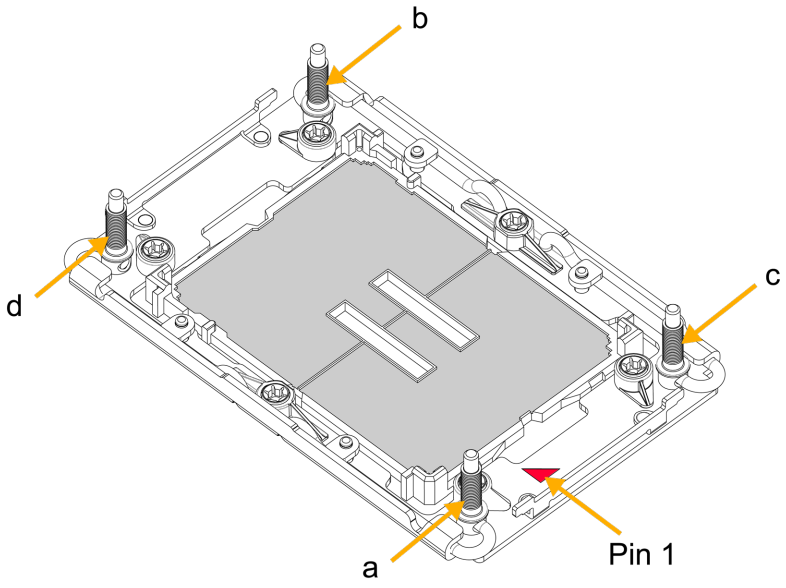


**Figure 2-35. Plastic Protective Cover Removed**

## Preparing to Install the PHM into the Processor Socket

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

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




a, b, c, d: Threaded Fasteners

**Figure 2-36. Threaded Fasteners**

2. Locate four PEEK nuts (marked A, B, C, and D) and four rotating wires (marked 1, 2, 3, and 4) on the heatsink.

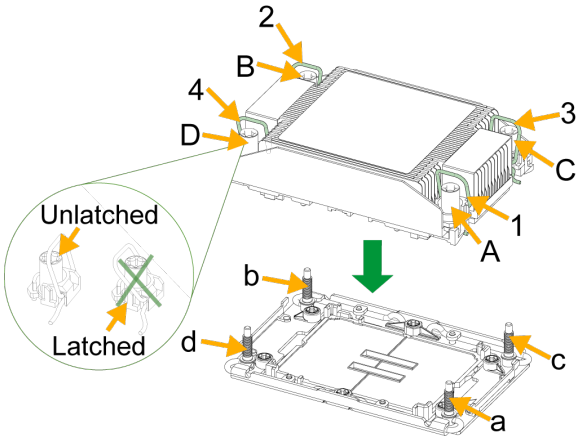



**Figure 2-37. PEEK Nuts and Rotating Wires (1U)**

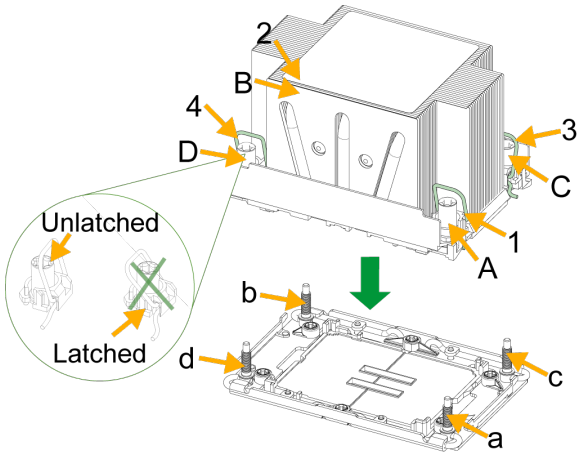



**Figure 2-38. PEEK Nuts and Rotating Wires (2U)**

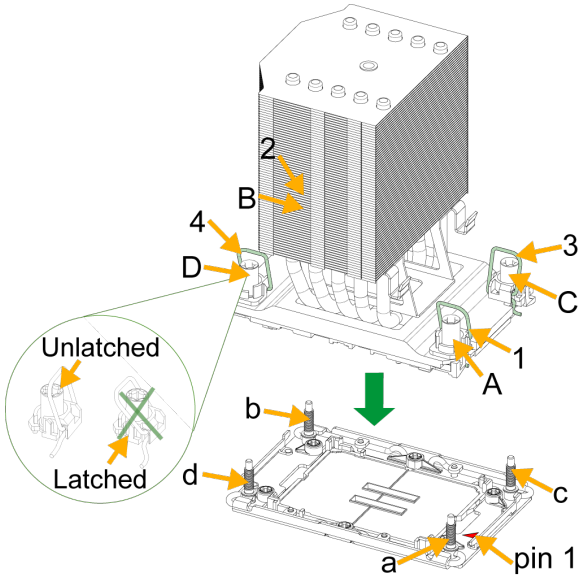



**Figure 2-39. PEEK Nuts and Rotating Wires (4U)**

3. Check the rotating wires (marked 1, 2, 3, and 4) to make sure that they are at unlatched positions before installing the PHM into the processor socket.

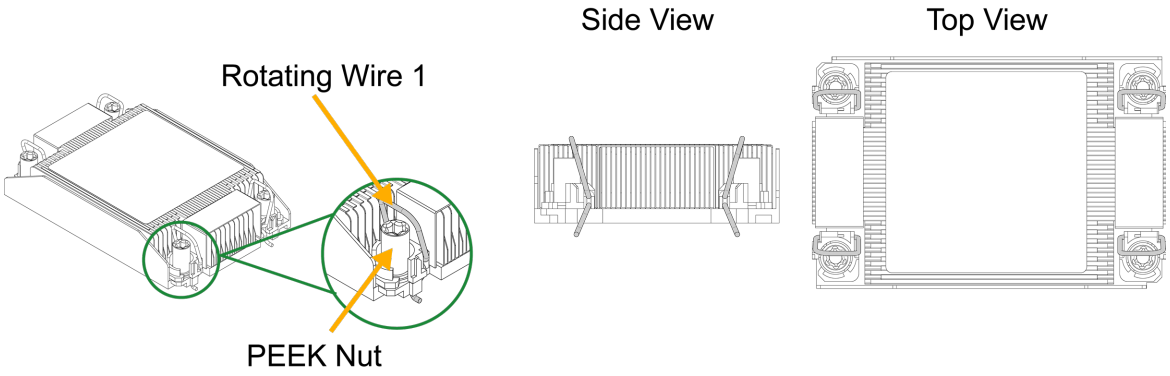



**Figure 2-40. 1U Unlatched Positions**

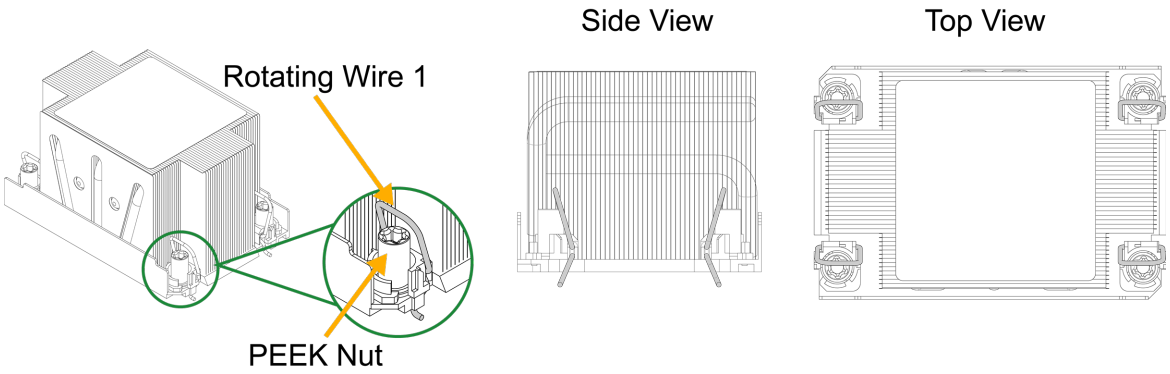



**Figure 2-41. 2U Unlatched Positions**

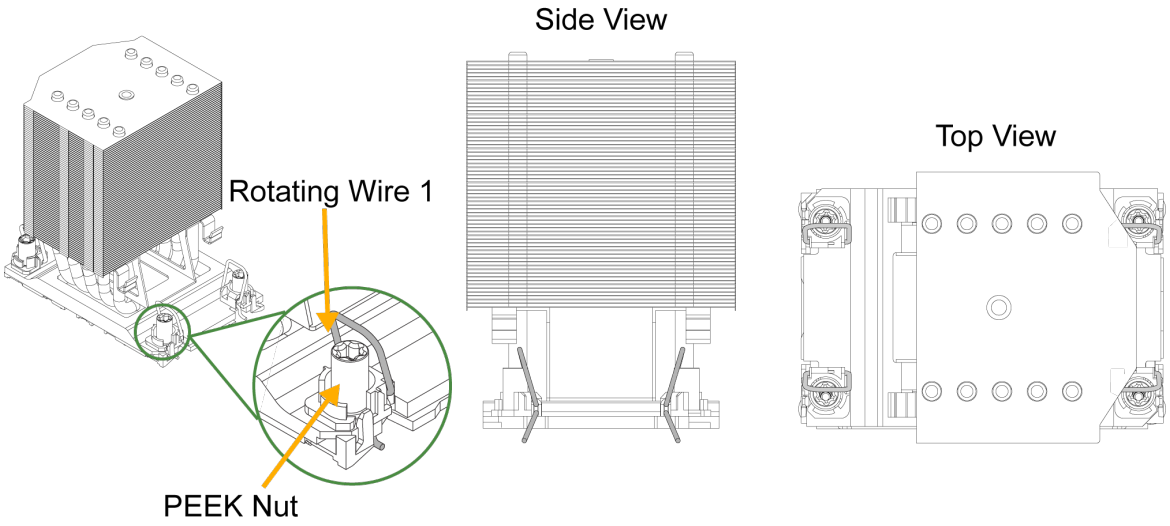



**Figure 2-42. 4U Unlatched Positions**

## Installing the Processor Heatsink Module

1. Align pin 1 of the PHM with the printed triangle on the processor socket.
2. Make sure all four PEEK nuts of the heatsink (marked A, B, C, and D) are aligned with the threaded fasteners (marked a, b, c, and d), then gently place the heatsink on top of the processor socket.

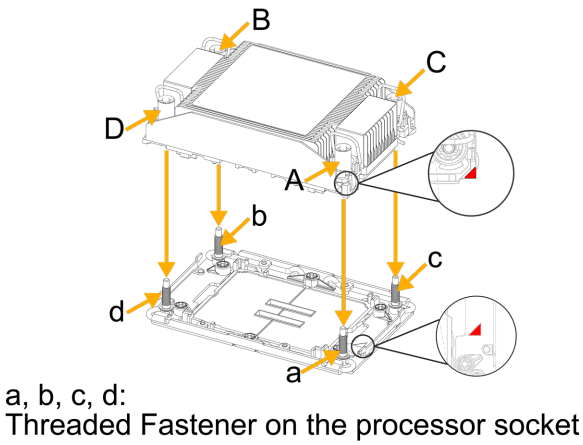



**Figure 2-43. Aligning the Heatsink with the Socket (1U)**

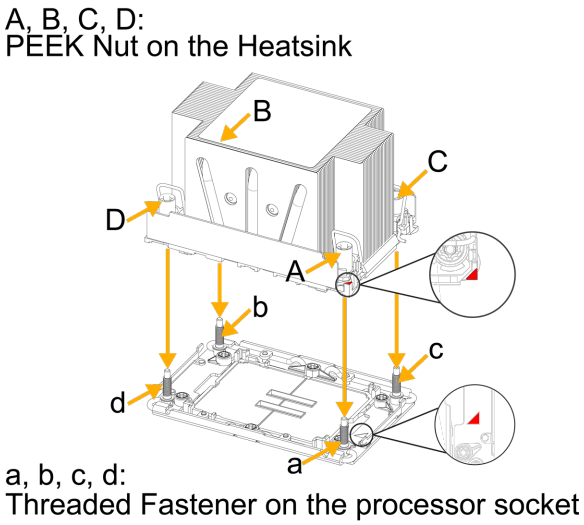



**Figure 2-44. Aligning the Heatsink with the Socket (2U)**

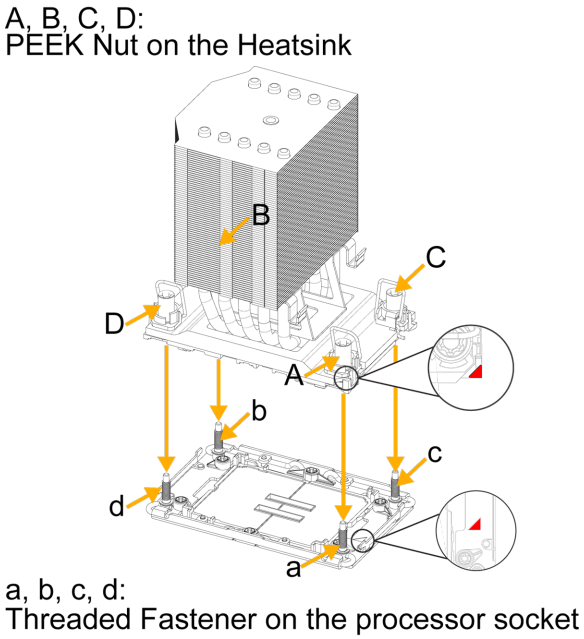



**Figure 2-45. Aligning the Heatsink with the Socket (4U)**

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

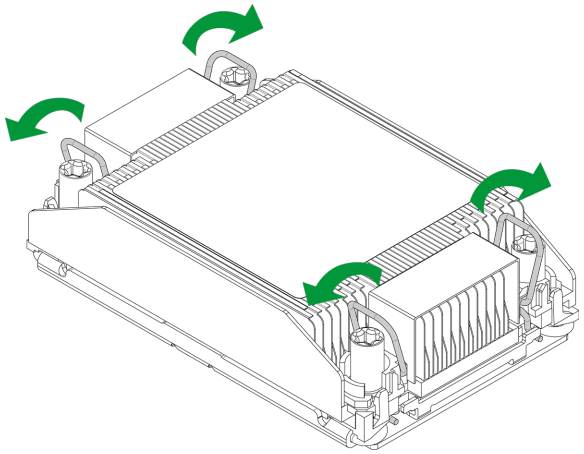


**Figure 2-46. Latching the PHM (1U)**

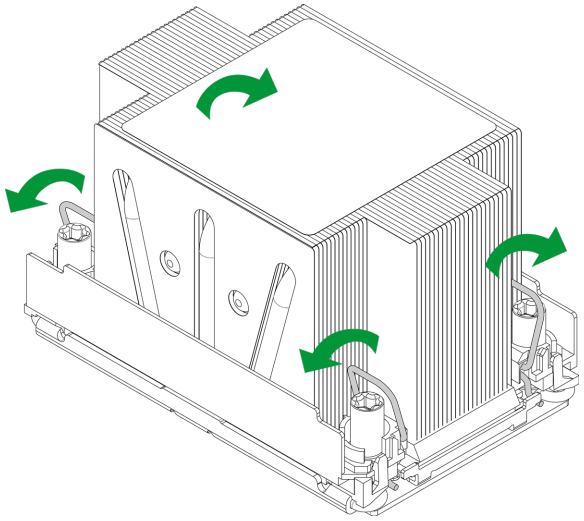


**Figure 2-47. Latching the PHM (2U)**

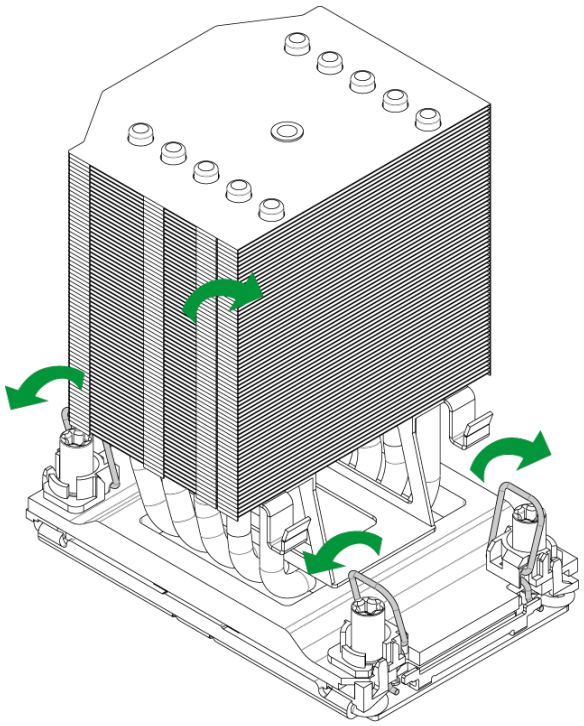


**Figure 2-48. Latching the PHM (4U)**

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

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

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

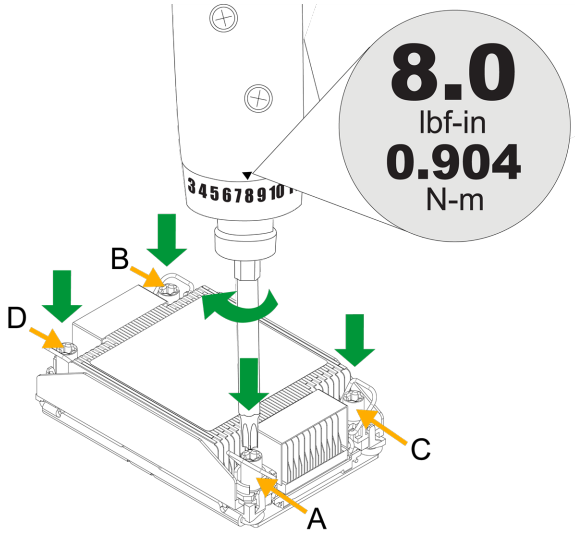



**Figure 2-49. Installing the PHM with a Torque Driver (1U)**

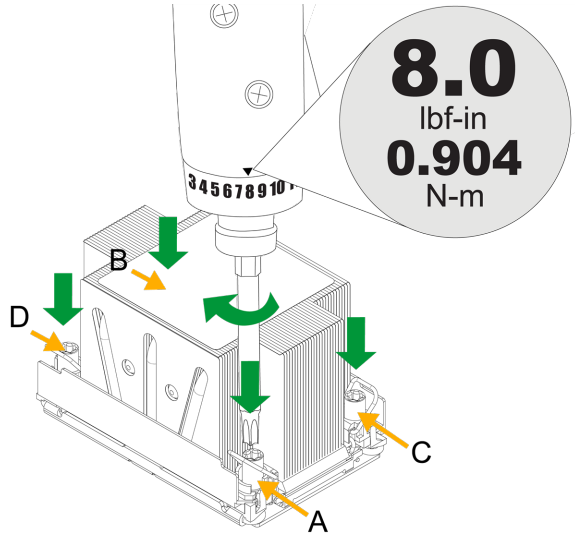



**Figure 2-50. Installing the PHM with a Torque Driver (2U)**

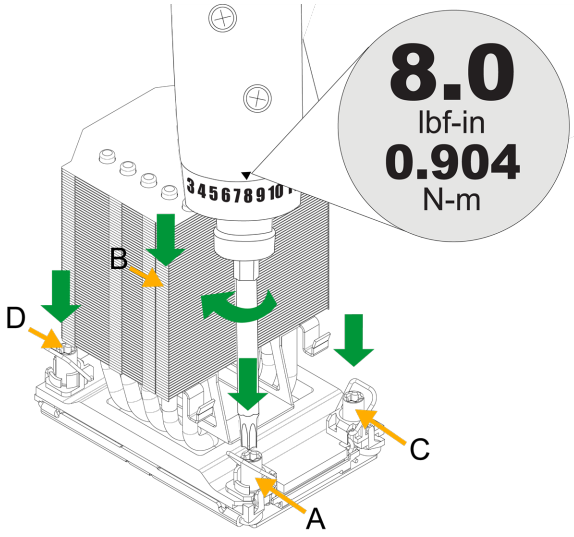



**Figure 2-51. Installing the PHM with a Torque Driver (4U)**

6. Align the aluminum fan shroud against the top of the 4U heatsink. The fan shroud was designed to match perfectly with the top of the heatsink in terms of geometric shape.

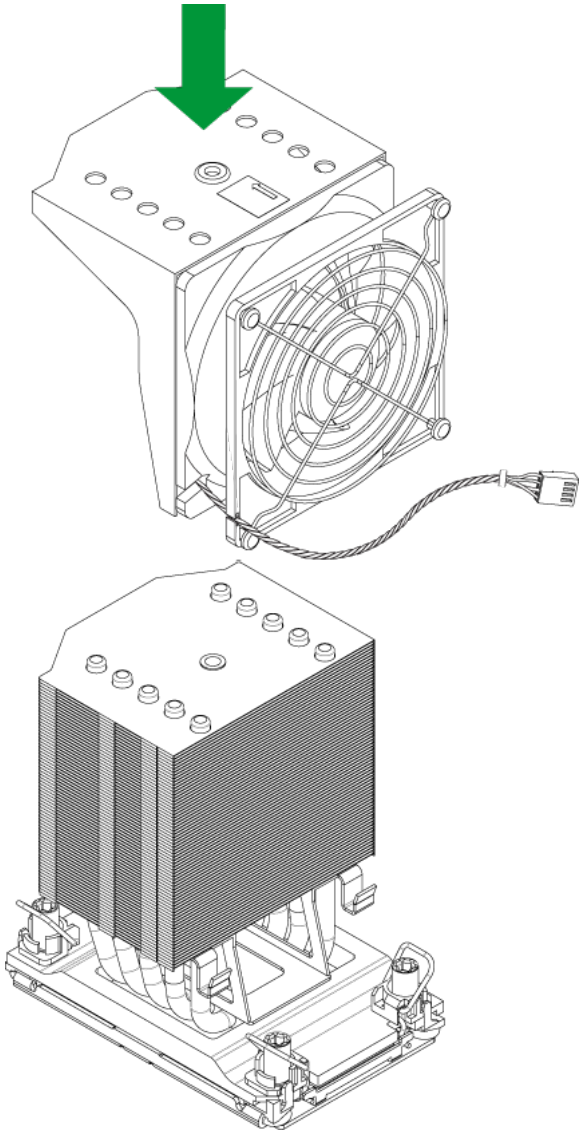


**Figure 2-52. Aligning the Heatsink Fan**

7. When the fan shroud and the top of the heatsink are properly aligned, gently push the fan onto the heatsink until the bottom of the fan properly rests on the two hooks of the heatsink.

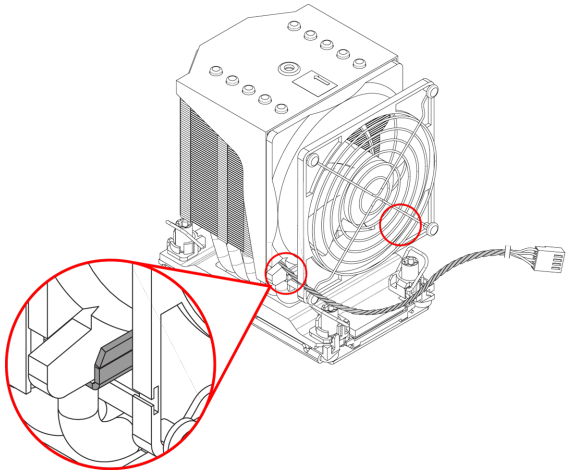


**Figure 2-53. Installing the Heatsink Fan**

8. Insert the Torx screw into the screw hole on top of the heatsink and turn it clockwise to tighten the screw.

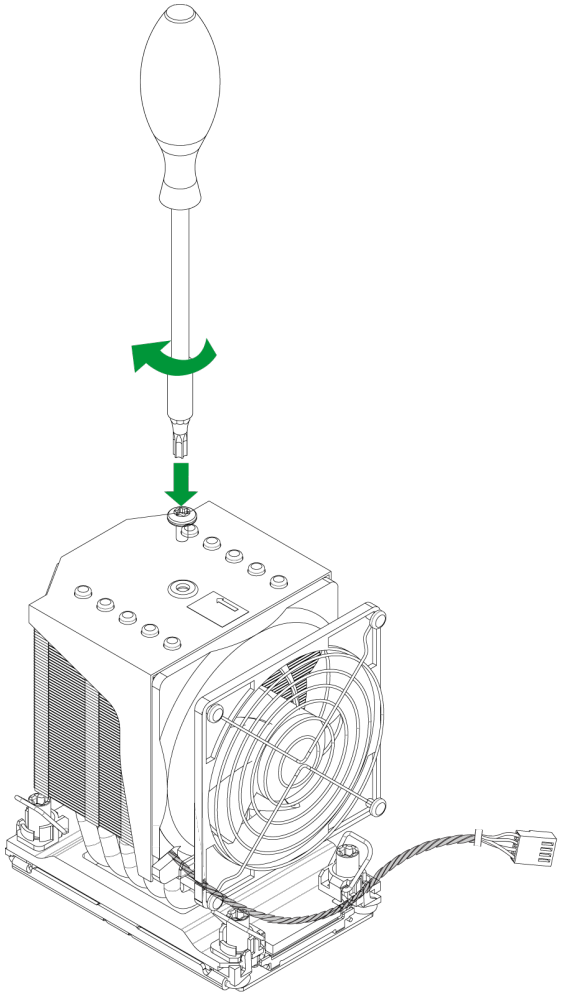


**Figure 2-54. Tightening the Screw**

9. Connect the fan power connector to a 4-pin fan header on the motherboard.

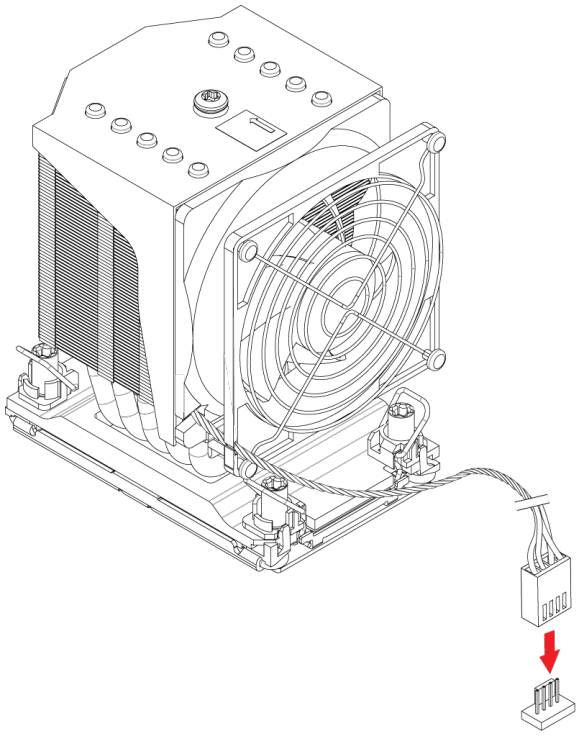


**Figure 2-55. Connecting the Fan Power**

## Removing the Processor Heatsink Module

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

Then follow the steps below:

1. Loosen the Torx screw from the heatsink. Unplug the fan power connector from the fan header.

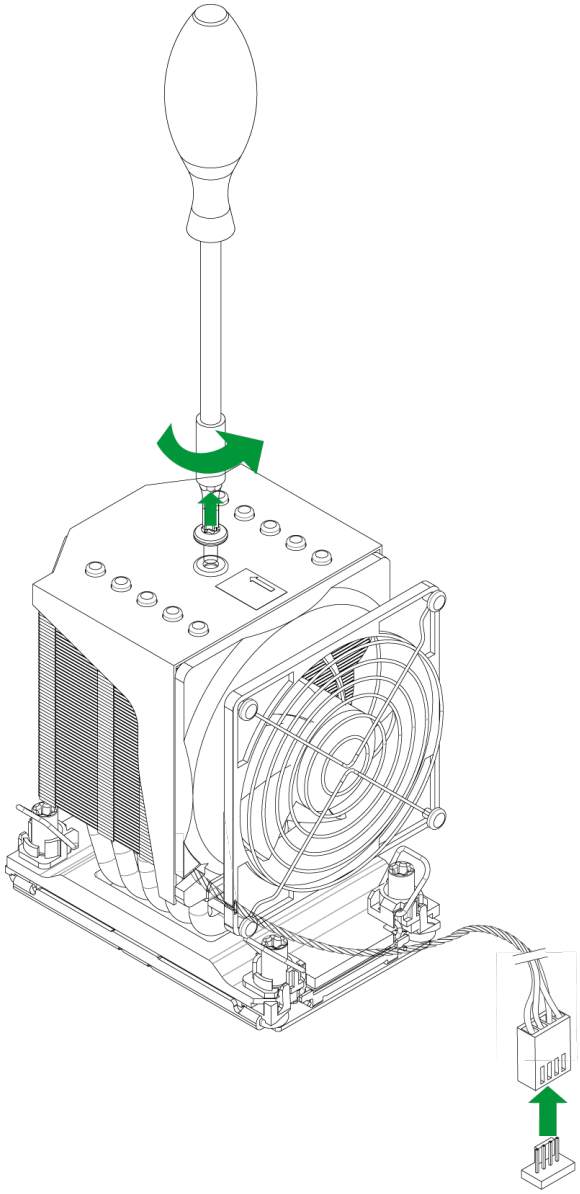


**Figure 2-56. Loosening the Screw and Unplugging the Fan Power Header**

2. Gently pull the heatsink fan upward to detach it from the heatsink.

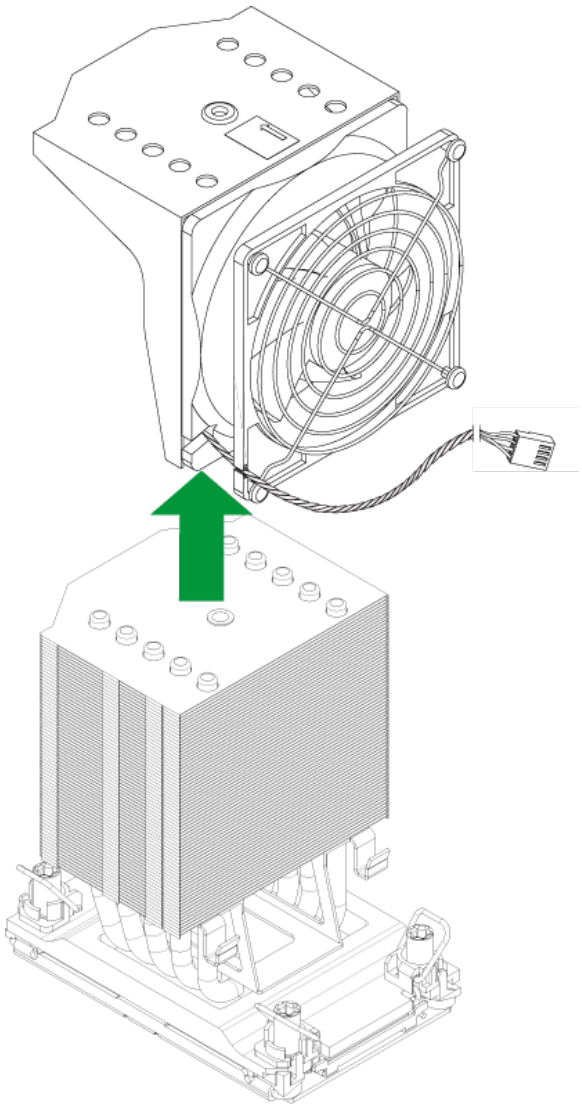


**Figure 2-57. Removing the Fan**

3. Use a screwdriver to loosen the four screws. You can start with any screw, but make sure to loosen the screws in a diagonal pattern.

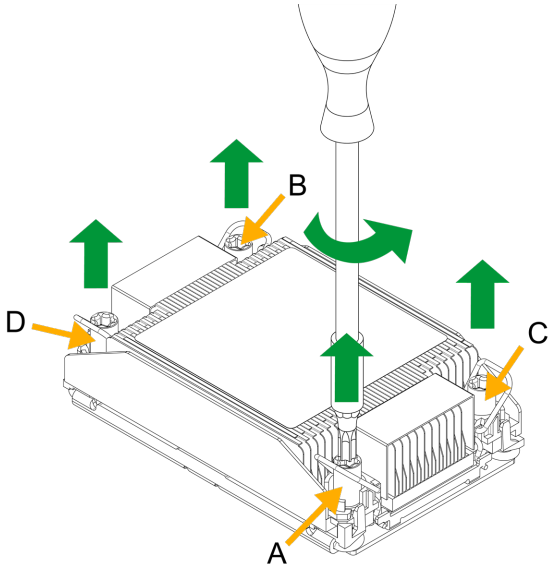



**Figure 2-58. Loosening the Screws (1U)**

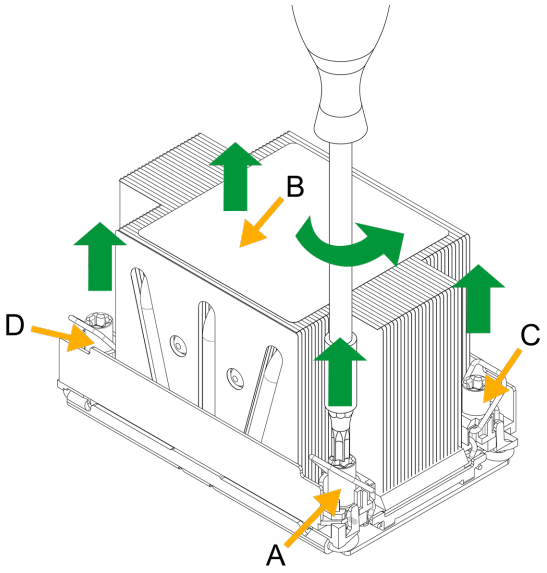



**Figure 2-59. Loosening the Screws (2U)**

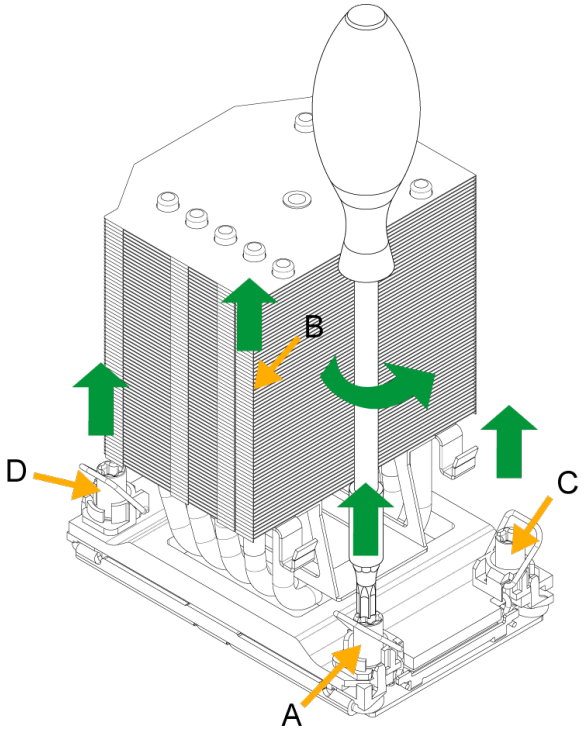



**Figure 2-60. Loosening the Screws (4U)**

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

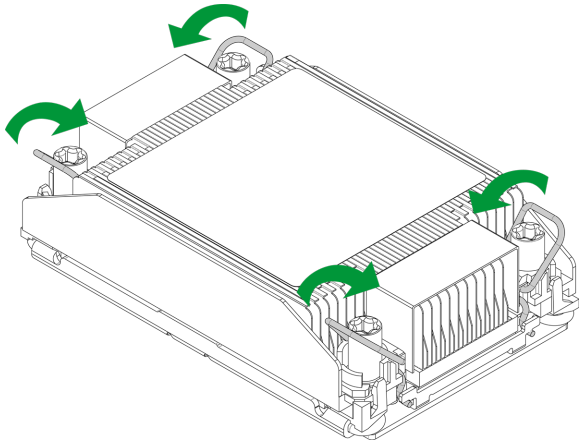


**Figure 2-61. Unlatching the PHM (1U)**

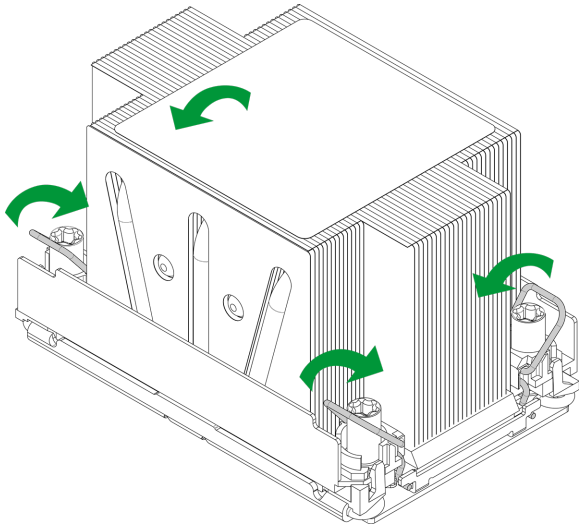


**Figure 2-62. Unlatching the PHM (2U)**

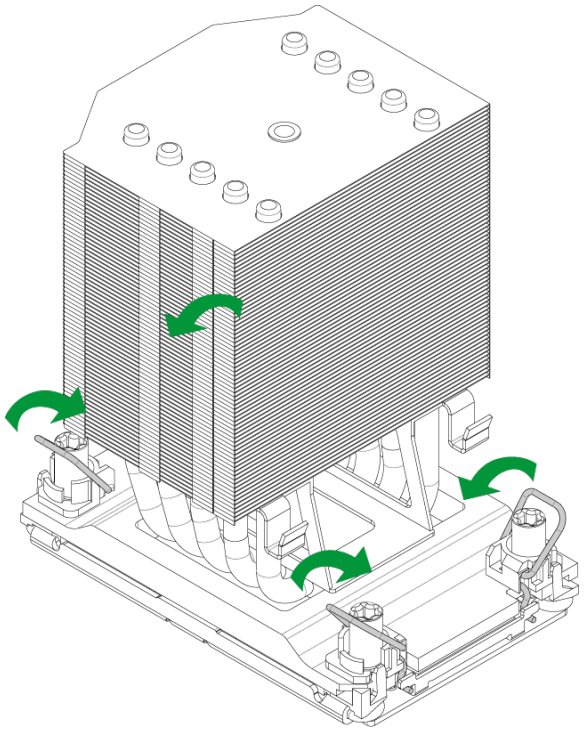


**Figure 2-63. Unlatching the PHM (4U)**

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

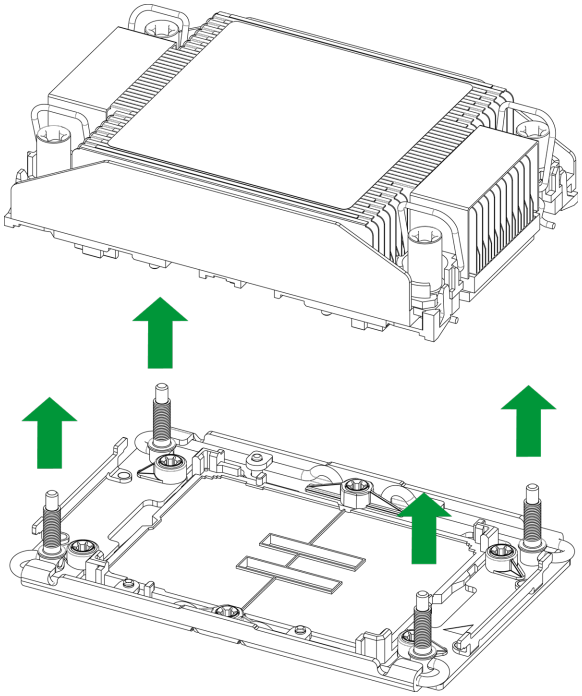


**Figure 2-64. Removing the PHM from the Socket (1U)**

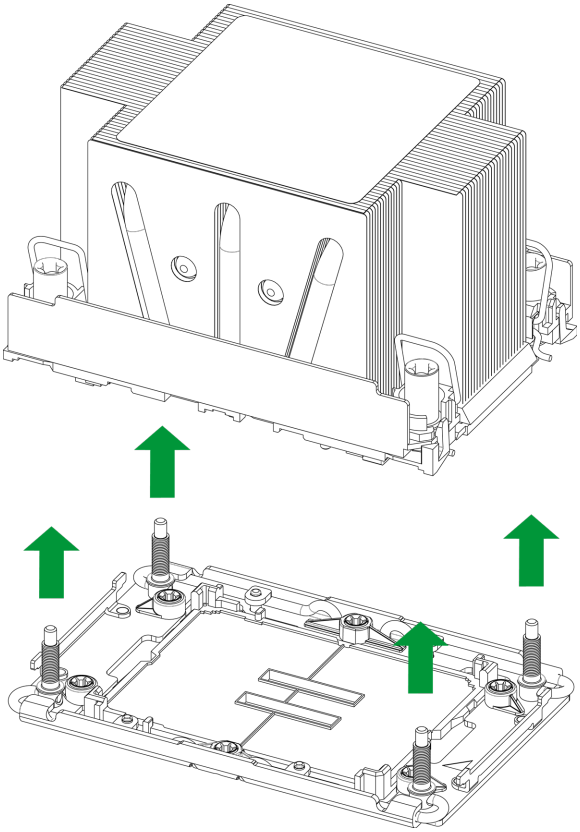


**Figure 2-65. Removing the PHM from the Socket (2U)**

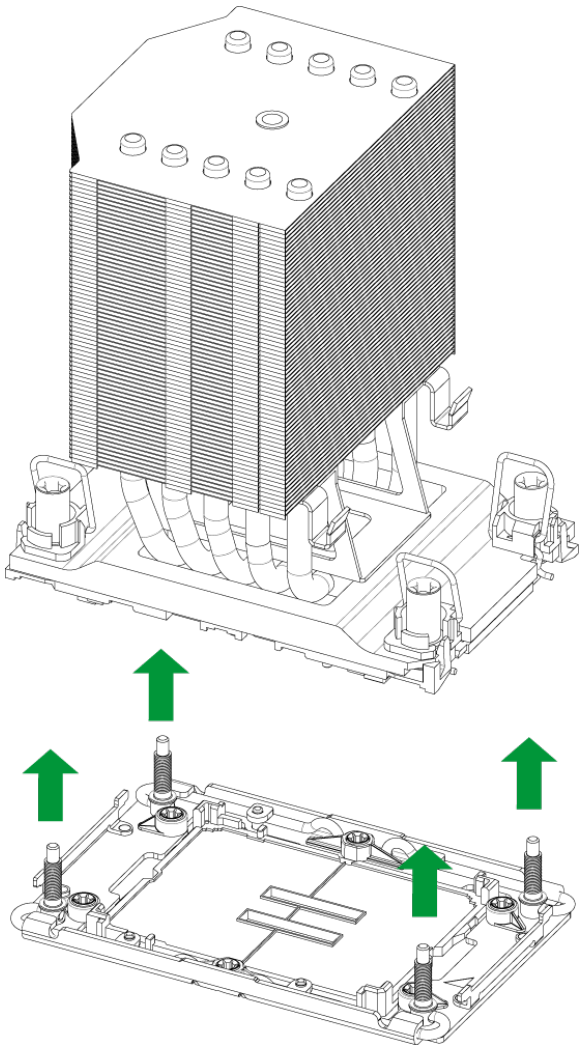


**Figure 2-66. Removing the PHM from the Socket (4U)**

6. To remove the processor from the heatsink, gently lift the lever from the processor carrier.

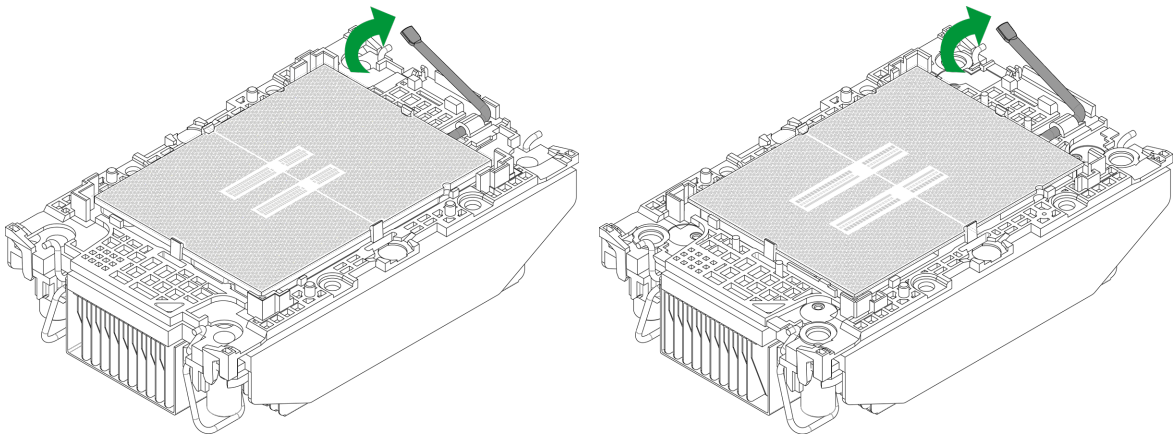


**Figure 2-67. Carrier with 1U Heatsink (SP XCC left, SP HCC/LCC right)**

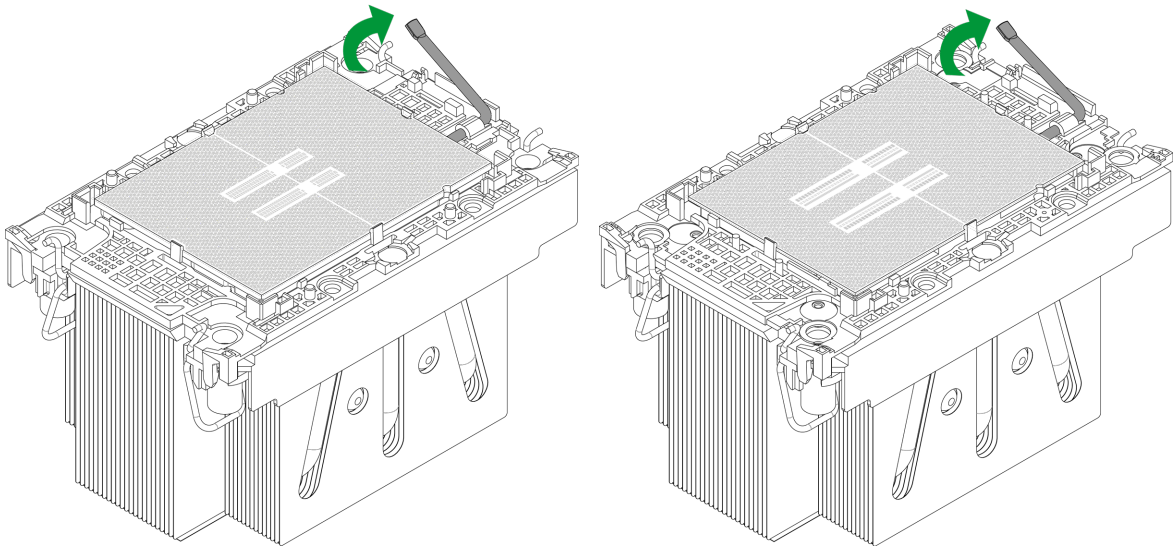


**Figure 2-68. Carrier with 2U Heatsink (SP XCC left, SP HCC/LCC right)**

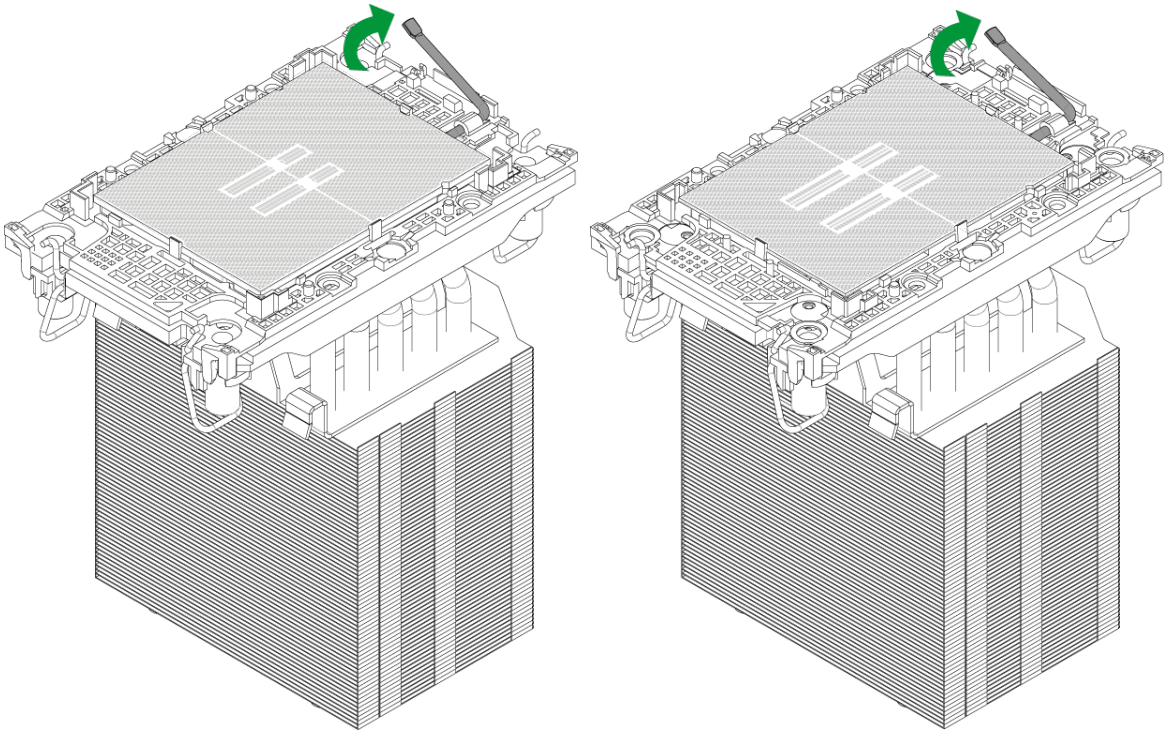


**Figure 2-69. Carrier with 4U Heatsink (SP XCC left, SP HCC/LCC right)**

7. To remove the processor, move the lever to its unlocked position and gently remove the processor.

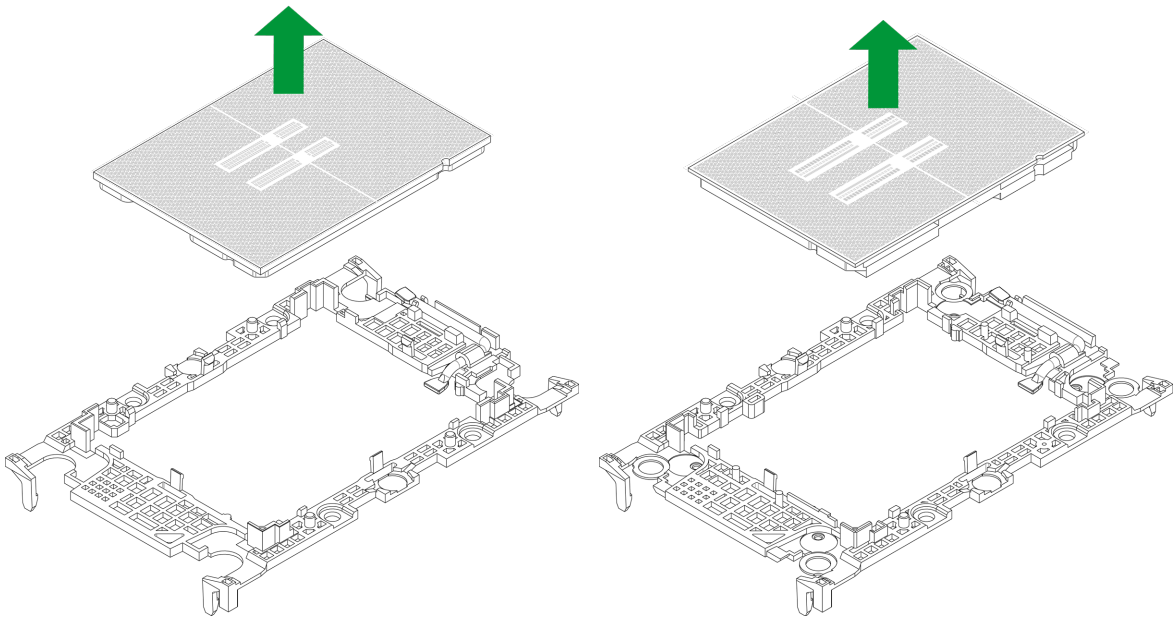


**Figure 2-70. Removing the Processor (SP XCC left, SP HCC/LCC right)**

## 2.4 Memory Support and Installation

**Important:** To prevent any damage, exercise extreme care when installing or removing memory modules.

**Note:** Check the Supermicro website for recommended memory modules.

### Memory Support

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

This motherboard supports ECC DDR5 RDIMM/3DS RDIMM with speeds up to 6400 MT/s in 16 memory slots.

To enhance memory performance and ensure system stability, do not mix memory modules of different speeds, different sizes, and different types in your server.

**Note:** Memory speed/capacity support depends on the processors used in the system.

#### *The Intel Xeon 6700-Series Processors with E-Cores*

| DDR5-6400 Memory Support for Intel® Xeon® 6700-Series Processors with E-Cores | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Type | Ranks Per DIMM, Data Width (Stack) | DIMM Capacity (GB) | | | | | | Speed (MT/s); Voltage (V); Slots per Channel (SPC) and DIMMs per Channel (DPC) | |
| | | DRAM Density | | | | | | | |
| | | 16 Gb | | 24 Gb | | 32 Gb | | 1DPC/2SPC | 2DPC/2SPC |
| | | 1DPC | 2DPC | 1DPC | 2DPC | 1DPC | 2DPC | +1.1 V | |
| RDIMM | 1Rx4 | 32 GB | - | - | - | - | - | 6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMs only) | N/A |
| | 2Rx8 | 32 GB | - | - | - | - | - | | N/A |
| | 2Rx4 | 64 GB | 64 GB | 96 GB | 96 GB | - | - | | 5200, 4800 (DDR5-6400 rated RDIMMs only) |
| | 2Rx4 | - | - | - | - | 128 GB | 128 GB | | |
| 3DS RDIMM | 4Rx4 | | | | | 256 GB | 256 GB | | |

| CXL Memory Configuration Support for Intel® Xeon® 6700-Series Processors with E-Cores | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Native DDR5 Memory Per Socket | | | | CXL Memory Per Socket | | | | |
| Slot 0 DIMM Ranks | Slot 0 DIMM Capacity (GB) | DIMM Type | DRAM Density (Gb) | CXL Memory Channels | CXL Memory Type | CXL Capacity Per Device/ Module | CXL Interleave | CXL Mode |
| 2Rx4 | 64 | 10x4 | 16 | 2+2 | DDR5 x8 | 64 GB | 1x4*, 2x2, 4x1 | 1LM+Vol |
| 2Rx4 | 64 | 10x4 | 16 | 1+1 | DDR5 x16 | 128 GB | 1x2*, 2x1 | 1LM+Vol |
| 1Rx4 | 32 | 10x4 | 16 | 2 | DDR5 x8 | 128 GB | 1x2* | Intel Flat Memory Mode |

**Notes:**

- The items with an asterisk (*) are the default settings in the BIOS.
- The Intel® Xeon® 6700-series processors with E-cores CXL memory configurations are 1DPC ('Slot 0') only for native DDR5.
- CXL Memory Channel: number of devices per root port, with root ports separated by "+," e.g. 2+2+2+2 = four root ports populated with two devices per root port.
- CXL Interleave: sets x ways, e.g. 2x4 = One set of two modules, interleaved four-way.
- CXL Modes:
  - 1LM + Vol = DDR5 ('1LM') and (volatile) CXL memory visible to SW as separate tiers, separately interleaved.
  - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW.

| Intel® Xeon® 6700-Series Processors with E-Cores DDR5 Memory Population Table<br>(2 Processors and 16 DIMMs Installed, 2DPC) | |
|---|---|
| ***1 Processor DIMM Count*** | ***Memory Population Sequence (2DPC)*** |
| **1 Processor and 1 DIMM** | P1-DIMMA1 |
| **1 Processor and 4 DIMMs** | P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1<br>P1-DIMMB1/P1-DIMMD1/P1-DIMMH1/P1-DIMMF1 |

| Intel® Xeon® 6700-Series Processors with E-Cores DDR5 Memory Population Table<br>(2 Processors and 16 DIMMs Installed, 2DPC) | |
|---|---|
| **1 Processor and 8 DIMMs** | P1-DIMMA1/P1-DIMMA2/P1-DIMMC1/P1-DIMMC2/P1-DIMME1/P1-DIMME2/P1-DIMMG1/P1-DIMMG2<br>P1-DIMMB1/P1-DIMMB2/P1-DIMMD1/P1-DIMMD2/P1-DIMMF1/P1-DIMMF2/P1-DIMMH1/P1-DIMMH2<br>P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1 |
| ***2 Processor DIMM Counts (Recommended)*** | ***Memory Population Sequence (2DPC)*** |
| **2 Processors and 2 DIMMs** | P1-DIMMA1<br>P2-DIMMA1 |
| **2 Processors and 8 DIMMs** | P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1<br>P2-DIMMA1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1 |
| **2 Processors and 8 DIMMs** | P1-DIMMB1/P1-DIMMD1/P1-DIMMF1/P1-DIMMH1<br>P2-DIMMB1/P2-DIMMD1/P2-DIMMF1/P2-DIMMH1 |
| **2 Processors and 16 DIMMs** | P1-DIMMA1/P1-DIMMA2/P1-DIMMC1/P1-DIMMC2/P1-DIMME1/P1-DIMME2/P1-DIMMG1/P1-DIMMG2<br>P2-DIMMA1/P2-DIMMA2/P2-DIMMC1/P2-DIMMC2/P2-DIMME1/P2-DIMME2/P2-DIMMG1/P2-DIMMG2 |
| **2 Processors and 16 DIMMs** | P1-DIMMB1/P1-DIMMB2/P1-DIMMD1/P1-DIMMD2/P1-DIMMF1/P1-DIMMF2/P1-DIMMH1/P1-DIMMH2<br>P2-DIMMB1/P2-DIMMB2/P2-DIMMD1/P2-DIMMD2/P2-DIMMF1/P2-DIMMF2/P2-DIMMH1/P2-DIMMH2 |
| **2 Processors and 16 DIMMs** | P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1<br>P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1 |

**Notes:**

- The memory configurations with an asterisk (*) are recommended by Supermicro for optimal memory performance.
- DIMMs must be all DDR5-6400 rated RDIMMs.
- All DIMMs in a channel must have the same number of ranks (unless explicitly specified otherwise).
- x8 DIMMs and x4 DIMMs cannot be mixed in the same channel or same processor socket (see the memory support table above).
- Rank mixing is not allowed.
- Vendor mixing is not allowed.

### *The Intel Xeon 6700-Series Processors with P-Cores*

| DDR5-6400 Memory Support for Intel® Xeon® 6700-Series Processors with P-Cores | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| Type | Ranks Per DIMM, Data Width (Stack) | DIMM Capacity (GB) | | | | | Speed (MT/s); Voltage (V); Slots per Channel (SPC) and DIMMs per Channel (DPC) | |
| | | DRAM Density | | | | | | |
| | | 16 Gb | | 24 Gb | | 32 Gb | 1DPC/2SPC | 2DPC/2SPC |
| | | 1DPC | 2DPC | 1DPC | 2DPC | 2DPC | +1.1 V | |
| RDIMM | 1Rx8 | 16 GB | - | 24 GB | - | - | 6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMs only) | 5200, 4800 (DDR5-6400 rated RDIMMs only) |
| | 1Rx4 | 32 GB | - | 48 GB | - | - | | |
| | 2Rx8 | 32 GB | 32 GB | 48 GB | - | - | | |
| | 2Rx4 | 64 GB | 64 GB* | 96 GB | 96 GB* | 128 GB* | | |
| 3DS RDIMM | 4Rx4 | - | 128 GB | - | - | - | | |
| | 8Rx4 | - | 256 GB | - | - | - | | |
| MRDIMM | 2Rx8 | 32 GB | - | - | - | - | 8000, 7200 (MRDIMM-8800 only) | N/A |
| | 2Rx4 | 64 GB | - | - | - | - | | N/A |

**Note:** The items marked with an asterisk (*) are supported in 1S/2S/4S/8S systems. All others support 1S/2S only.

| CXL Memory Configuration Support for Intel® Xeon® 6700-Series Processors with P-Cores | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Native DDR5 Memory Per Socket | | | | CXL Memory Per Socket | | | | | |
| Slot 0 DIMM Ranks | Slot 0 DIMM Capacity (GB) | DIMM Type | DRAM Density (Gb) | CXL Memory Channels | CXL Memory Type | CXL Capacity Per Device/ Module | CXL Inter leave | CXL Mode | 4S and 8S support |
| 2Rx4 | 96 | 10x4 | 24 | 2+2 | DDR5 x8 | 96 GB | 1x4*, 2x2, 4x1 | 1LM+Vol | Yes |
| 2H 3DS | 128 | 10x4 | 16 | 2+2 | DDR5 x8, DDR x8 | 128 GB | 1x4*, 2x2, 4x1 | 1LM+Vol | Yes |
| 2Rx4 | 64 | 10x4 | 16 | 2+2 | DDR5 x8 | 64 GB | hetero x12 | Hetero | Yes |
| 2Rx4 | 64 | 10x4 | 16 | 1+1 | DDR5 x16 | 2ch 64 GB | hetero x12 | Hetero | Yes |
| 2Rx4 | 64 | 10x4 | 16 | 2+2+2+2 | DDR5 x8 | 64 GB | 1x8*, 2x4, 4x2 | 1LM+Vol | No |
| 2Rx4 | 64 | 10x4 | 16 | 2 | DDR5 x8 | 256 GB | 1x2* | 1LM+Vol | No |
| 2Rx4 | 64 | 10x4 | 16 | 1+1 | DDR4 x16, DDR5 x16 | 2ch 128 GB | 1x2* | Intel Flat Memory Mode | No |

**Notes:**

- The items with an asterisk (*) are the default settings in the BIOS.
- The Intel® Xeon® 6700-series processors with P-cores CXL memory configurations are 1DPC ('Slot 0') only for native DDR5.
- CXL Memory Channel: number of devices per root port, with root ports separated by "+," e.g. 2+2+2+2 = four root ports populated with two devices per root port.
- CXL Interleave: sets x ways, e.g. 2x4 = One set of two modules, interleaved four-way.
- CXL Modes:
  - 1LM + Vol = DDR5 ('1LM') and (volatile) CXL memory visible to SW as separate tiers, separately interleaved.
  - Hetero x12 = DDR5 and (volatile) CXL memory interleaved together in one 12-way set.
  - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW.

| **Intel® Xeon® 6700-Series Processors with P-Cores DDR5 Memory Population Table**<br>**(2 Processors and 16 DIMMs Installed, 2DPC)** | |
|---|---|
| ***1 Processor DIMM Counts*** | ***Memory Population Sequence (2DPC)*** |
| **1 Processor and 1 DIMM** | P1-DIMMA1 |
| **1 Processor and 4 DIMMs** | P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1<br>P1-DIMMB1/P1-DIMMD1/P1-DIMMF1/P1-DIMMH1 |
| **1 Processor and 8 DIMMs** | P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1<br>P1-DIMMA1/P1-DIMMA2/P1-DIMMC1/P1-DIMMC2/P1-DIMME1/P1-DIMME2/P1-DIMMG1/P1-DIMMG2<br>P1-DIMMB1/P1-DIMMB2/P1-DIMMD1/P1-DIMMD2/P1-DIMMF1/P1-DIMMF2/P1-DIMMH1/P1-DIMMH2 |
| ***2 Processor DIMM Counts (Recommended)*** | ***Memory Population Sequence (2DPC)*** |
| **2 Processors and 2 DIMMs** | P1-DIMMA1<br>P2-DIMMA1 |
| **2 Processors and 8 DIMMs** | P1-DIMMA1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1<br>P2-DIMMA1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1 |

| Intel® Xeon® 6700-Series Processors with P-Cores DDR5 Memory Population Table<br>(2 Processors and 16 DIMMs Installed, 2DPC) | |
|---|---|
| **2 Processors and 8 DIMMs** | P1-DIMMB1/P1-DIMMD1/P1-DIMMF1/P1-DIMMH1<br>P2-DIMMB1/P2-DIMMD1/P2-DIMMF1/P2-DIMMH1 |
| **2 Processors and 16 DIMMs** | P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1<br>P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1 |
| **2 Processors and 16 DIMMs** | P1-DIMMA1/P1-DIMMA2/P1-DIMMC1/P1-DIMMC2/P1-DIMME1/P1-DIMME2/P1-DIMMG1/P1-DIMMG2<br>P2-DIMMA1/P2-DIMMA2/P2-DIMMC1/P2-DIMMC2/P2-DIMME1/P1-DIMME2/P2-DIMMG1/P2-DIMMG2 |
| **2 Processors and 16 DIMMs** | P1-DIMMB1/P1-DIMMB2/P1-DIMMD1/P1-DIMMD2/P1-DIMMF1/P1-DIMMF2/P1-DIMMH1/P1-DIMMH2<br>P2-DIMMB1/P2-DIMMB2/P2-DIMMD1/P2-DIMMD2/P2-DIMMF1/P2-DIMMF2/P2-DIMMH1/P2-DIMMH2 |

**Notes:**

- DIMMs must be all DDR5 RDIMM or all MRDIMMs.
- All DIMMs in a channel must have the same number of ranks (unless explicitly specified otherwise).
- x8 DIMMs and x4 DIMMs cannot be mixed in the same channel or same processor socket (see the memory support table above).
- Mixing of non-3DS and 3DS RDIMMs is not allowed in the same channel, across different channels, and across different sockets.
- 9x4 RDIMMs cannot be mixed with other DIMMs.
- All DDR5 DIMM must be in the same speed per processor socket.
- Rank mixing is not allowed.
- Mixing of DDR5 operating frequencies is not validated within a socket or across sockets by Intel. When DIMMs with different maximum frequencies are mixed in the same channel or across different channels across processor sockets, BIOS determines and sets the DIMM speed to the highest common frequency across all channels on the platform. For example, if a 6000 MT/s max frequency DIMM is installed in one channel and a 6400 MT/s max frequency DIMM in another, BIOS sets the platform speed to 6000 MT/s.
- Mixing memory made by different vendors is allowed for both RDIMM and 3DS RDIMM.
- The 1-DIMM per processor configuration supports only 16 GB 1Rx8 and 32 GB 2Rx8 modules.

## DIMM Installation

**Important:** To avoid causing any damage to the memory module or the DIMM socket, do not use excessive force when pressing the release tabs on the ends of the DIMM socket. Handle memory modules with care. To avoid ESD-related damage to your memory modules or components, carefully follow all the instructions given in "Static-Sensitive Devices" on page 28.

1. Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population table earlier in this section.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.

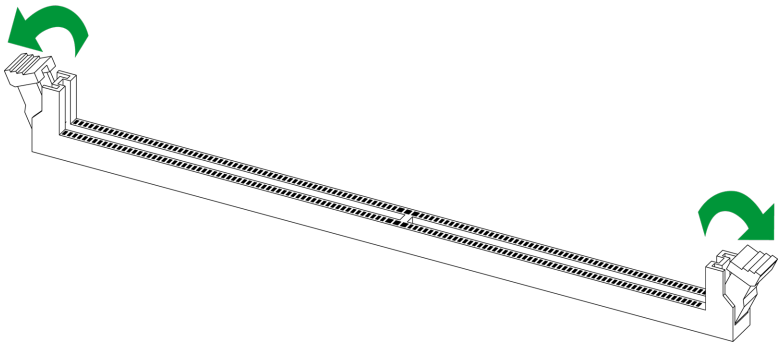


**Figure 2-71. Unlocking the DIMM Slot**

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

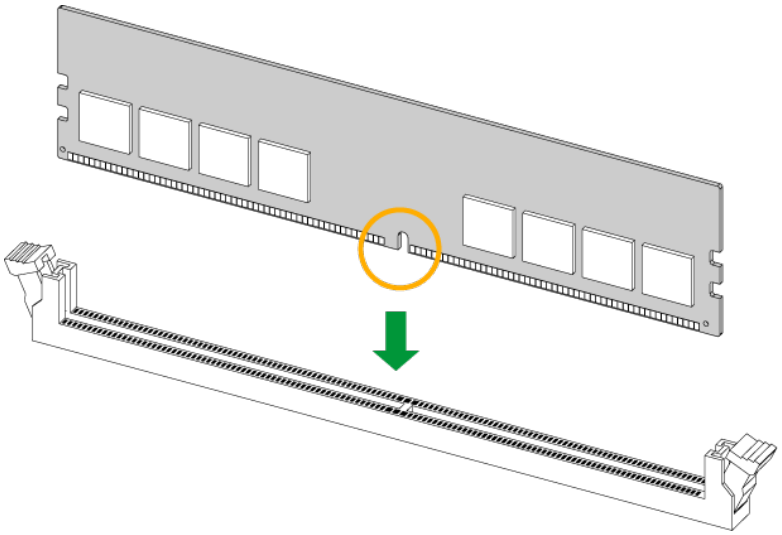


**Figure 2-72. Aligning the DIMM Slot with the Receptive Point**

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

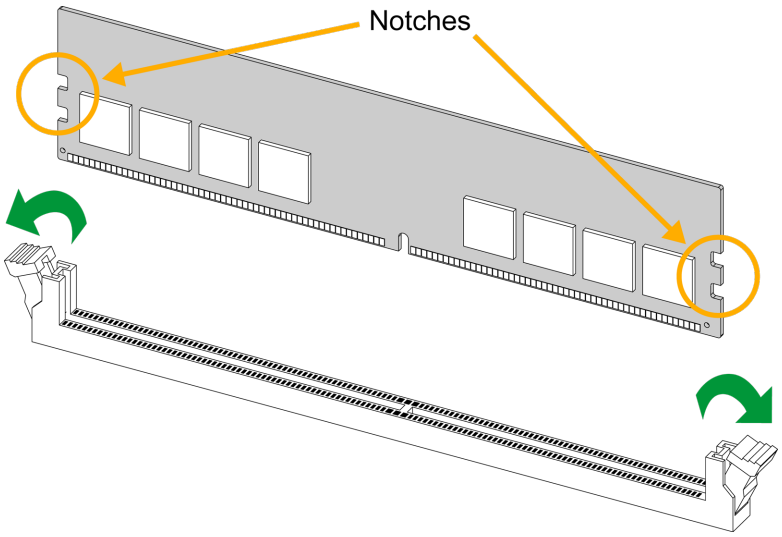



**Figure 2-73. Aligning the Notches**

5. Press 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 DIMM into the slot.

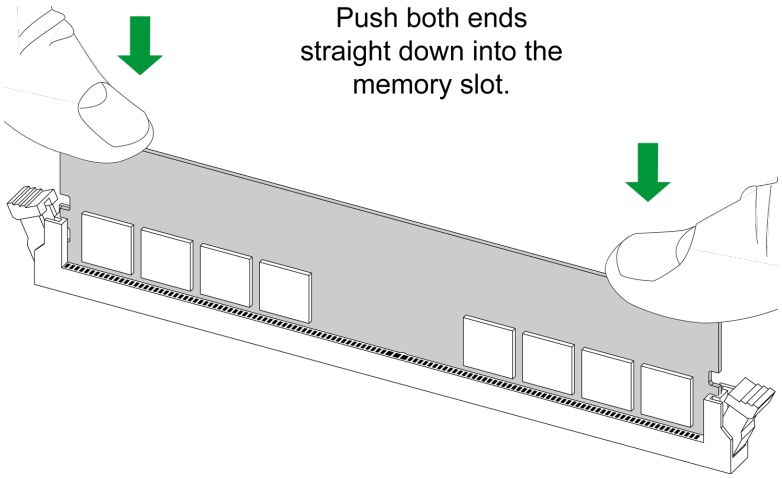



**Figure 2-74. Securing the DIMM**

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

## DIMM Removal

**Important:** To avoid causing any damage to the memory module or the DIMM socket, do not use excessive force when pressing the release tabs on the ends of the DIMM socket. Handle memory modules with care. To avoid ESD-related damage to your memory modules or components, carefully follow all the instructions given in "Static-Sensitive Devices" on page 28.

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

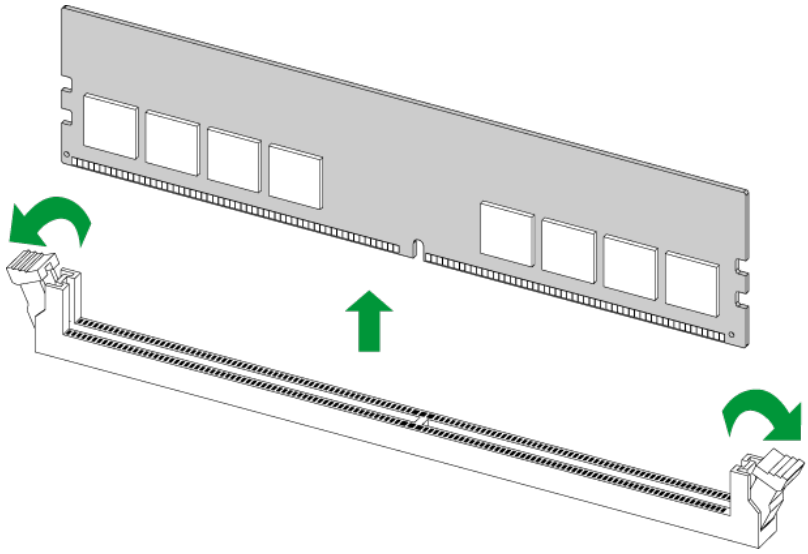


**Figure 2-75. Unlocking the DIMM Slot**

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

# 2.5 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. Place the system on a workbench.
3. Remove the top cover from the system.
4. Locate the onboard battery as shown below.
5. 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.
6. Remove the battery.

## Proper Battery Disposal

**Important:** 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. 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 steps 1 and 2 above and continue below:

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

1. Identify the battery's polarity. The positive (+) side should be facing up.
2. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.

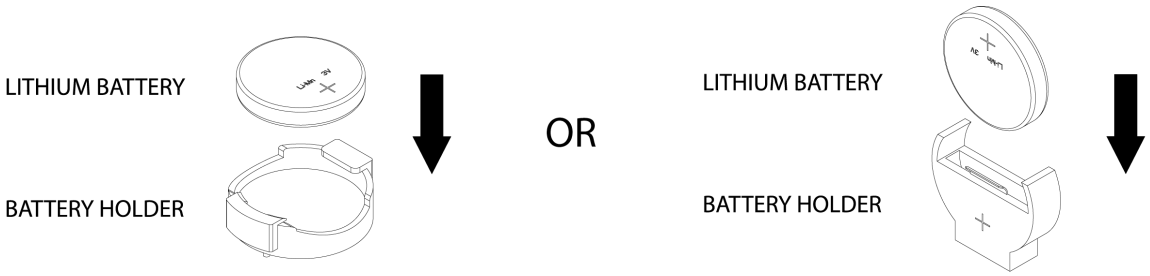



**Figure 2-76. Installing a Battery**

# 2.6 Connections, Jumpers, and LEDs

Refer to the following sections for information about connections, jumpers, and LEDs for the B14DBT motherboard.

## Power Supply and Power Connections

For information about the power supply and power connections of the B14DBT motherboard, refer to the following content.

### *25 G Midplane*

A 25 G midplane is located at MP1 on the rear side of the system. This midplane supports 25 GbE Ethernet connection and functions as a guide-post for your system components.

Please refer to the LED Indicator section for LAN LED information.

### *MEZZ1 Card*

The mezzanine card connector, located at MEZZ1, supports a PCIe 5.0 x16 riser card.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *PCIe 5.0 M.2 Slot and M.2 Standoff (MH-SRW1)*

This motherboard has one M.2 M-Key PCIe 5.0 x4 slot, which is located at JM2-1. The M.2 slot on the motherboard supports PCIe 5.0 x4 M.2 in the 2280 form factor. The M.2 standoff mounting hole located at MH-SRW1 on the motherboard supports the 2280 form factor.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *MCIO PCIe 5.0 x8 Connectors*

Mini Cool Edge IO (MCIO) PCIe 5.0 x8 connectors are located at JMCIO1A and JMCIO1B on the B14DBT motherboard. These connectors can be used for backplane EDSFF E1.S drives and other high-speed storage devices, and are supported by CPU1.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *Power Connectors*

Two power connectors are located on the motherboard. The motherboard power supply connector (PWR2) provides main power to your system. The 4-pin backplane power connector, located at JPWR2, provides power to your backplane devices (via power cables).

| 4-pin Backplane Power<br>Pin Definitions: Four Total | |
|---|---|
| **Pin#** | **Definition** |
| 1–2 | GND |
| 3–4 | P12 V (12 V Power) |

### *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 B14DBT hyper server board accommodates two power connectors: 12 V motherboard power supply connector (PWR2) and 4-pin backplane power connector (JPWR2). Although most power supplies generally meet the specifications required by the processors, 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 also connect the power supplies to the motherboard power connectors (PWR2) and the 4-pin backplane connector (JPWR2) on the motherboard. Failure to do 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.

## Headers and Connections

For information about the headers on the B14DBT motherboard, refer to the following content.

### *Complex Programmable Logic Device Header*

A Complex Programmable Logic Device header (JCPLD2), located on the front side of the motherboard, provides firmware support for your system.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *Liquid Cooling Leakage Sensor Header*

A liquid cooling leakage sensor header is located at JSEN2 on the B14DBT motherboard. This header is reserved for liquid cooling support in systems. Liquid cooling leakage sensor headers are used to detect leakage of the coolant used in your liquid cooling system.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *M.2 M-Key PCIe 5.0 x4 Slot*

The M.2 M-key slot on the motherboard supports PCIe 5.0 x4 devices in a 2280 form factor.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *Motherboard CPLD Header*

A Motherboard Complex Programmable Logic Device header, located at JPRG1 on the rear side of the motherboard, allows for engineering programming for firmware/software performance.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *TPM/Port 80 Header*

The JTPM1 header on the B14DBT motherboard 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 storage drives. It allows the motherboard to deny access if the TPM associated with the storage drive is not installed in the system. Information on the TPM is available at the following page:

https://www.supermicro.com/manuals/other/AOM-TPM-9670V_9670H__X12_H12.pdf

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

| **Trusted Platform Module Header**<br><br>**Pin Definitions: 10 Total** | | | |
|---|---|---|---|
| **Pin#** | **Definition** | **Pin#** | **Definition** |
| 1 | +3.3 V | 2 | SPI_CS# |
| 3 | RESET# | 4 | SPI_MISO |
| 5 | SPI_CLK | 6 | GND |
| 7 | SPI_MOSI | 8 | No Connection |
| 9 | +1.8 V Standby | 10 | SPI_IRQ# |

### *Universal Serial Bus (USB) 3.0/2.0 Port*

A USB 3.0/2.0 Type-A port that supports two USB 3.0/2.0 connections is located at JUSB1 on the motherboard. This USB port can be used for USB support with USB cables (not included).

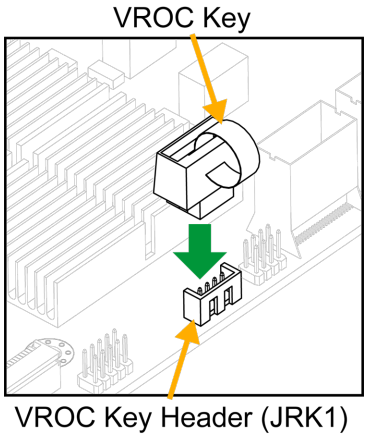
For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

| USB 3.0/2.0 (JUSB1) Pin Definitions | | | |
|---|---|---|---|
| **Pin#** | **Definitions** | **Pin#** | **Definitions** |
| A1 | VBUS | B1 | Power |
| A2 | D- | B2 | USB_N |
| A3 | D+ | B3 | USB_P |
| A4 | GND | B4 | GND |
| A5 | STDA_SSRX- | B5 | USB3_RN |
| A6 | STDA_SSRX+ | B6 | USB3_RP |
| A7 | GND | B7 | GND |
| A8 | STDA_SSTX- | B8 | USB3_TN |
| A9 | STDA_SSTX+ | B9 | USB3_TP |

## *VROC RAID Key Header*

A VROC RAID Key header is located at JRK1 on the B14DBT motherboard. Install a VROC RAID key on JRK1 for NVMe RAID support as shown in the illustration below.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.




| Intel VROC Key Pin Definitions: Four Total | |
|---|---|
| **Pin#** | **Definition** |
| 1 | GND |
| 2 | +3.3 V Standby |
| 3 | GND |
| 4 | CPU RAID Key |

**Note:** Images displayed are for illustrative purposes only. The components installed in your system may or may not look exactly the same as the graphics shown in the manual.

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

## Front Panel Control Board and Front I/O Connector

Refer to the following content for information about the front control board and the front I/O connector on the B14DBT motherboard.

### *Front Control Panel*

The header for the Front Panel Control board, located at JFP1, contains various header pins and LED indications for front access via an appropriate cable.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

### *Advanced I/O Module (AIOM) for Front I/O Support (JAIOM1)*

A Supermicro proprietary Advanced I/O Module (AIOM) connector used for a PCIe 5.0x16 add-on module is located at JAIOM1. This AIOM connector, supported by CPU1, provides input/output connections on the front side of your system.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

## Jumper Settings

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

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

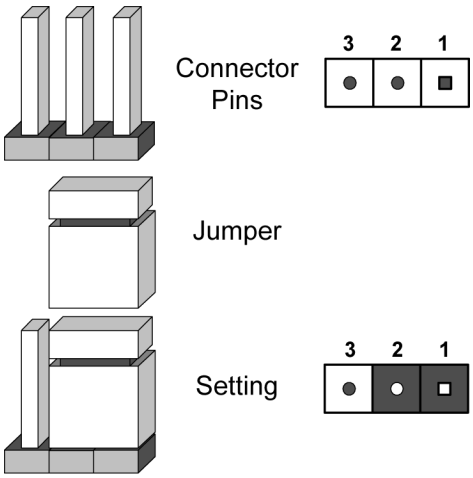



**Figure 2-77. Jumping Connector Pins**

### *CMOS Clear*

JBT1 on the B14DBT motherboard 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.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.




1. Power down the system.
2. Unplug the power cord(s).
3. Remove the cover of the chassis to access the motherboard.
4. Remove the onboard battery from the motherboard.
5. Short the CMOS pads, JBT1, with a metal object such as a small screwdriver for at least four seconds.

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

6. Remove the screwdriver or shorting device.
7. Reinsert the battery.
8. Replace the cover.
9. Reconnect the power cord(s).
10. Power on the system.

## LED Indicators

For information about the LED indicators on the B14DBT motherboard, refer to the following content.

### *BMC Heartbeat LED*

A BMC Heartbeat LED is located at LEDM1 on the B14DBT motherboard. When this LED is blinking, the BMC is functioning normally. During a BMC Reset or a Cold Boot, LEDM1 will turn solid green.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

| BMC Heartbeat LED Indicator | |
|---|---|
| **LED Color** | **Definition** |
| Blinking Green | BMC Normal |
| Solid Green | During BMC Reset or Cold Boot |

### *LAN1/LAN2 Activity LED Indicators (D40/D42)*

LAN1/LAN2 Activity LED indicators are located at D40 and D42 on the rear side of the motherboard. When these LEDs are blinking green, LAN connections are active.

| LAN Activity LED Indicators (D40/D42) | | |
|---|---|---|
| **LED#** | **LED Color** | **State** |
| D40 | Green: Blinking | LAN1: Active |
| D42 | Green: Blinking | LAN2: Active |

### *LAN1/LAN2 Link LED Indicators (D39/D41)*

LAN1/LAN2 Link LED indicators are located at D39 and D41 on the rear side of the motherboard. These LEDs indicate the speed of the LAN connections.

| LAN Link LED Indicators (D39/D41) | | |
|---|---|---|
| **LED#** | **LED Color** | **State** |
| D39 | Green On | LAN1 Link: 25G |
| | Yellow On | LAN1 Link: 10G/1G |
| D41 | Green On | LAN2 Link: 25G |
| | Yellow On | LAN2 Link: 10G/1G |

### *M.2 LED*

One M.2 LED is located at LED1 on the B14DBT motherboard. When this LED is blinking, the M.2 device is functioning normally.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

| M.2 LED State | |
|---|---|
| **LED Color** | **Definition** |
| Blinking Green | Device Working |

### *Onboard Power LED*

The Onboard Power LED is located at LED2 on the B14DBT motherboard. When this LED is on, the system E810 LAN Controller is on. Be sure to turn off the system and unplug the power cord before removing or installing components.

For a detailed diagram of the B14DBT motherboard, see the layout under "Quick Reference" on page 12.

| Onboard Power LED Indicator | |
|---|---|
| **LED Color** | **Definition** |
| Off | System Power Off (power cable not connected) |
| Solid Green | System Power On |

# Chapter 3:

# Troubleshooting

The following content contains information on common issues and how to resolve them.

**3.1 Troubleshooting Procedures** ..... **90**
Before Power On ..... 90
No Power ..... 90
No Video ..... 90
System Boot Failure ..... 90
Memory Errors ..... 91
Losing the System's Setup Configuration ..... 91
If the System Becomes Unstable ..... 91
**3.2 Technical Support Procedures** ..... **93**
**3.3 Frequently Asked Questions** ..... **94**
**3.4 Motherboard Battery** ..... **95**
**3.5 Where to Get Replacement Components** ..... **96**
**3.6 Returning Merchandise for Service** ..... **97**
**3.7 Feedback** ..... **98**

# 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" on page 93 or "Returning Merchandise for Service" on page 97 section(s) in this chapter. Always disconnect the AC power cord before adding, changing or installing any non hot-swappable hardware components. If the below steps do not fix the setup configuration problem, contact your vendor for repairs.

## 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 processor (making sure it is fully seated) and connect the front panel connectors to the motherboard.

## No Power

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

## No Video

1. If the power is on, but you 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 Power-On-Self-Test (POST) or does not respond after the power is turned on, do the following:

1. Check the screen for an error message.
2. Clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper. Restart the system. Refer to "CMOS Clear" on page 86.
3. Remove all components from the motherboard and turn on the system with only one DIMM installed. If the system boots, turn off the system and repopulate the components back into the system to retest. Add one component at a time to isolate which one may have caused the system boot issue.

## Memory Errors

When suspecting faulty memory is causing the system issue, check the following:

1. Make sure that the memory modules are compatible with the system and are properly installed. See "Component Installation" on page 26 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMMs in the system.
3. Make sure that you are using the correct type of DIMMs recommended by the manufacturer.
4. Check for bad DIMMs 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 "Introduction" on page 11 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.

## If the System Becomes Unstable

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

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

2. Memory support: Make sure that the memory modules are supported. Refer to the product page on our website at https://www.supermicro.com. Test 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. Storage Drive support: Make sure that all storage drives work properly. Replace the failed storage drives with good ones.
4. System cooling: Check the system cooling to make sure that all heatsink fans and processor/system fans, etc., work properly. Check the hardware monitoring settings in the IPMI to make sure that the processor and system temperatures are within the normal range. Also, check the front panel Overheat LED and make sure that it is not on.
5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Refer to our website for more information on the minimum power requirements.
6. Proper software support: Make sure that the correct drivers are used.

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

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as a USB flash or media device.
2. Cable connection: Check to make sure that all cables are connected and working properly.
3. Use the minimum configuration for troubleshooting: Remove all unnecessary components (starting with add-on cards first), and use the minimum configuration (but with the processor and a memory module installed) to identify the trouble areas. Refer to the steps listed above in this section for proper troubleshooting procedures.
4. Identify bad components by isolating them: If necessary, remove a component in question from the chassis, and test it in isolation to make sure that it works properly. Replace a bad component with a good one.
5. Check and change one component at a time instead of changing several items at the same time. This will help isolate and identify the problem.
6. To find out if a component is good, swap this component with a new one to see if the system will work properly. If so, then the old component is bad. You can also install the component in question in another system. If the new system works, the component is good and the old system has problems.

## 3.2 Technical Support Procedures

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

1. Refer to "Troubleshooting Procedures" on page 90 or see the FAQs on our website (https://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 https://webpr3.supermicro.com/SupportPortal.
5. Distributors: For immediate assistance, have your account number ready when placing a call to our Technical Support department. For Supermicro contact information, refer to "Contacting Supermicro" on page 10.

## 3.3 Frequently Asked Questions

**Question: What type of memory does my motherboard support?**

**Answer:** This motherboard supports This motherboard supports ECC DDR5 RDIMM/3DS RDIMM with speeds up to 6400 MT/s in 16 memory slots. To enhance memory performance and ensure system stability, do not mix memory modules of different speeds, different sizes, and different types in your server. Please follow all memory installation instructions given in the Memory Support and Installation section.

**Note:** 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:**

- The SPI BIOS chip used on this motherboard cannot be removed. Send your motherboard back to our RMA Department at Supermicro for repair.
- For BIOS Update and Recovery instructions, please refer to the Firmware Update and Recovery Instructions for Supermicro's X14 Motherboards User's Guide posted at https://www.supermicro.com/support/manuals.
- When BIOS update is in progress, do not reset the BMC firmware.

## 3.4 Motherboard Battery

For information on removing, disposing of, and replacing the motherboard battery of your system, refer to "Battery Removal and Installation" on page 80.

## 3.5 Where to Get Replacement Components

If you need replacement parts for your B14DBT motherboard, to ensure the highest level of professional service and technical support, purchase exclusively from our Supermicro Authorized Distributors/System Integrators/Resellers. A list can be found on the Supermicro website:

https://www.supermicro.com

Under the "Buy" menu, click the "Where to Buy" link.

## 3.6 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, RMA authorizations can be requested online at the following page:

https://www.supermicro.com/RmaForm

Whenever possible, repack the motherboard in the original Supermicro carton, using the original packaging material. If these are no longer available, be sure to pack the motherboard securely, using packaging material to surround the motherboard so that it does not shift within the carton and become damaged during shipping.

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

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

## 3.7 Feedback

Supermicro values your feedback as we strive to improve our customer experience in all facets of our business. Email us at Techwriterteam@supermicro.com to provide feedback on our manuals.

# Chapter 4:

# UEFI BIOS

The following content contains information on BIOS configuration with the B14DBT motherboard.

**4.1 Introduction** ..... **100**
**4.2 Main Setup** ..... **102**
**4.3 Advanced Setup Configurations** ..... **104**
**4.4 Event Logs** ..... **150**
**4.5 BMC** ..... **152**
**4.6 Security** ..... **156**
**4.7 Boot** ..... **163**
**4.8 Save & Exit** ..... **165**

# 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 UEFI script (flash.nsh), the BMC WebUI, or the SuperServer Automation Assistant (SAA) 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. Refer to the Manual Download area of our website for any changes to BIOS that may not be reflected in this manual.

## Updating BIOS

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 the following page:

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

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.

**Important:** Do not shut down or reset the system while updating the BIOS to prevent possible system boot failure! Read the motherboard README file carefully before you perform the BIOS update.

To update the BIOS under the UEFI Shell, unzip the BIOS file onto a bootable USB device and then boot into the built-in UEFI Shell. For motherboards with BMC support, type "flash.nsh <BIOS filename> <BMC Username> <BMC Password>" to start the BIOS update. The flash.nsh script will invoke the SAA (EFI) tool automatically to perform the BIOS update, beginning with uploading the BIOS image to BMC. After uploading the BIOS image, the system will reboot to continue the process. The BMC will take over and continue the BIOS update in the background. The process will take 3– 5 minutes. Refer to the README file for more information.

## 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. There are a few cases when other hot keys are used, such as <F1>, <F2>, etc. Each main BIOS menu option is described in this manual.

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

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

The BIOS Setup utility uses a key-based navigation system called hot keys. Most of these hot keys (<F1>, <F2>, <F3>, <F4>, <F5>, <F6>, <Enter>, <ESC>, the arrow keys, etc.) can be used at any time during the setup navigation process.

## 4.2 Main Setup

The Main setup screen appears when the AMI BIOS Setup utility is first entered. To return to the Main setup screen, select the Main tab at the top of the screen. The Main BIOS setup screen is shown below.

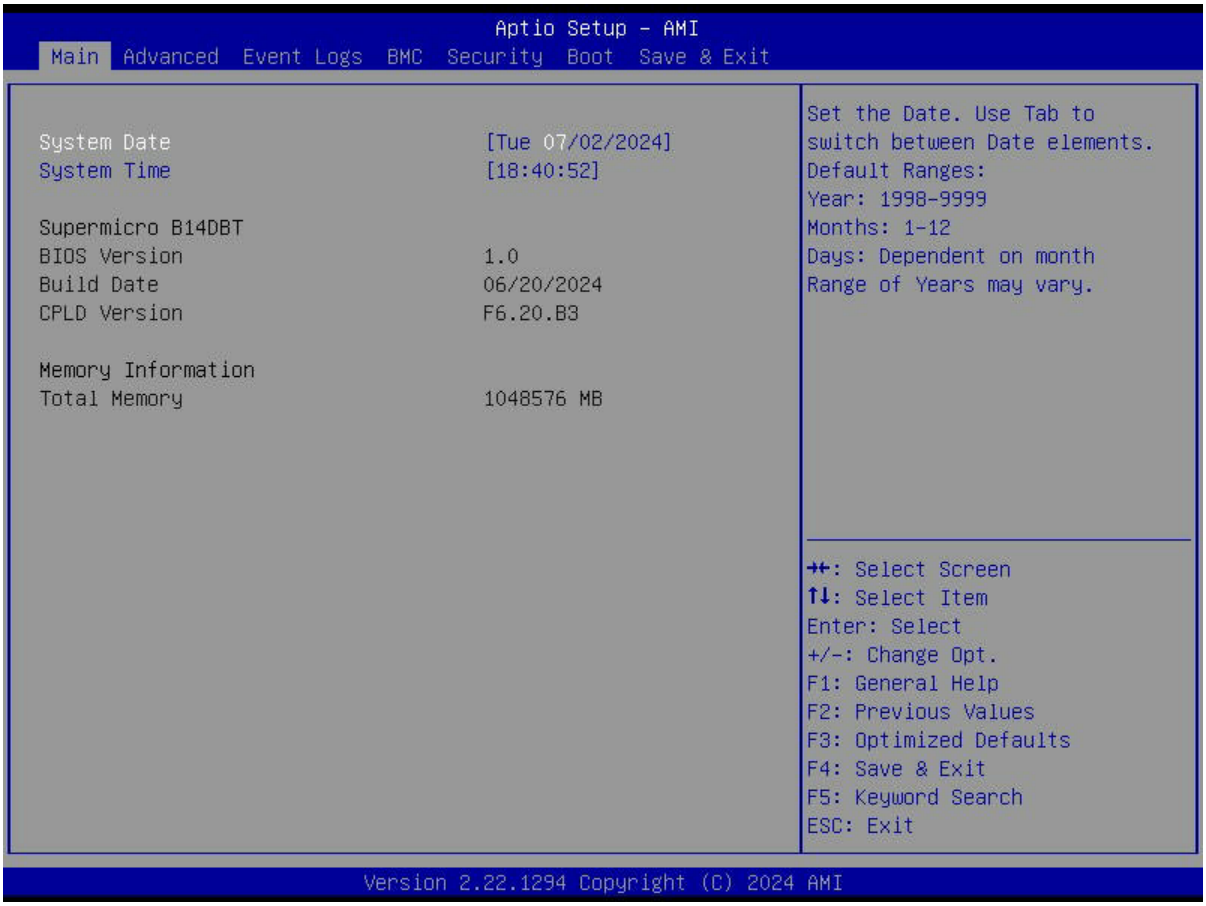



**Figure 4-1. Main Setup**

### System Date/System Time

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

**Note:** The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00.

### Supermicro B14DBT

### 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.

**Important:** Use 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, revert the settings to the default manufacturing settings.

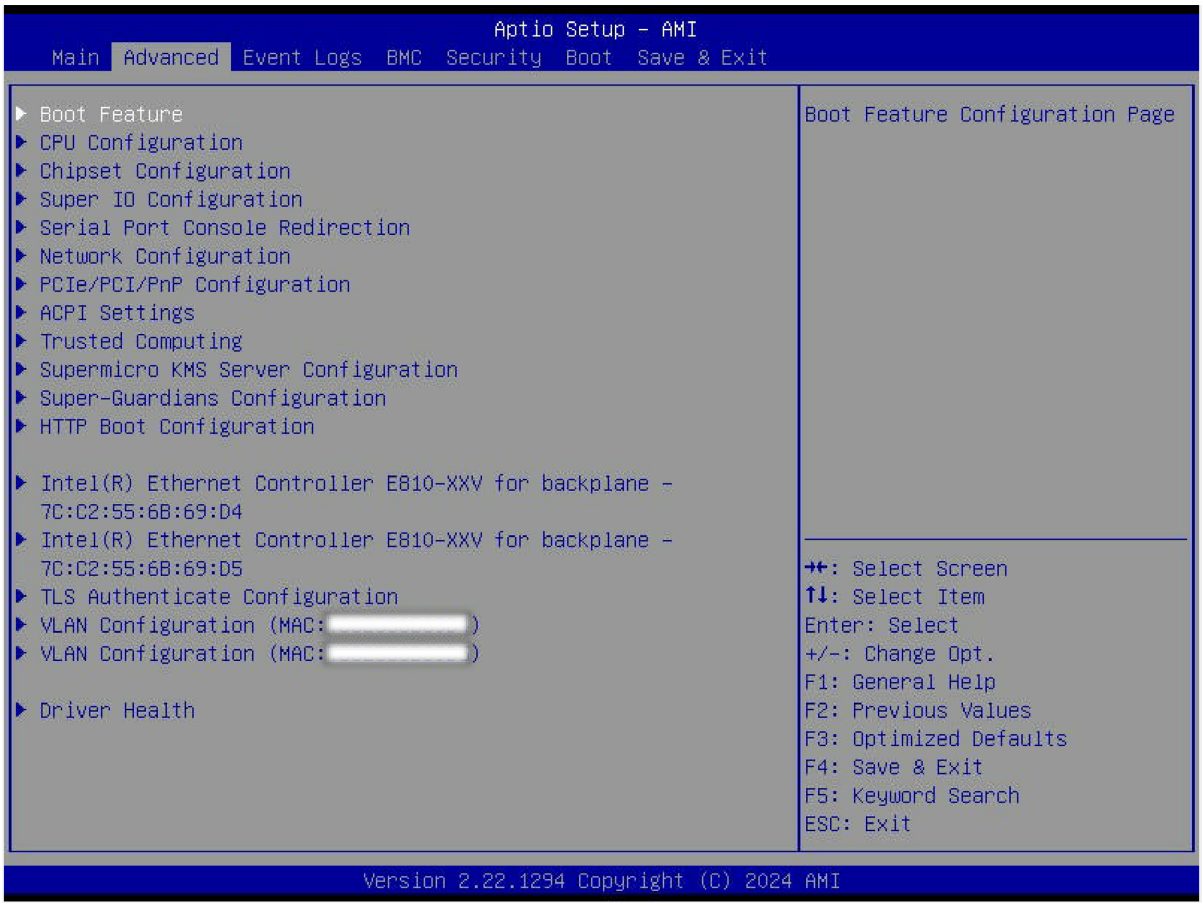



**Figure 4-2. Advanced BIOS Screen**

### Boot Feature Menu

#### ►Boot Feature

**Quiet Boot**

Use this feature to select the screen between displaying the Power On Self Test (POST) messages or the OEM logo upon bootup. Select Disabled to display the POST messages. Select Enabled to display the OEM logo instead of the normal POST messages. The options

are Disabled and **Enabled**.

**Note:** BIOS POST messages are always displayed regardless of the setting of this feature.

**Bootup NumLock State**

Use this feature to set the power on state for the <Num Lock> 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.

**Re-try Boot**

If this feature is set to Enabled, the system BIOS will automatically reboot the system from an Extensible Firmware Interface (EFI) 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 Watchdog timer to reboot the system when it is inactive for more than five minutes. The options are **Disabled** and Enabled.

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

Use this feature to configure the Watchdog timeout setting. The options are **Reset** and NMI.

**Restore on AC Power Loss**

Use this feature to set the power state after a power outage. Select Stay Off for the system power to remain off after a power loss. Select Power On for the system power to be turned on after a power loss. Select Last State to allow the system to resume its last power state before a power loss. The options are Power On, **Stay Off**, 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 you press the power button. The options are **Instant Off** and 4 Seconds Override.

## CPU Configuration Menu

### ►CPU Configuration

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

The following processor 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

**Hardware Prefetcher**

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

**Note:** This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

**Adjacent Cache Prefetch**

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

**Note:** This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

**DCU Streamer Prefetcher**

If this feature is set to Enabled, 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 Enabled, Disabled, and **Auto**.

**Note:** This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

### 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 **Enabled** and Disabled.

**Note:** This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

### APIC Physical Mode

Use this feature to enable the APIC physical destination mode. The options are **Disabled** and Enabled. (APIC is the abbreviation for Advanced Programmable Interrupt Controller.)

### 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. This feature is CPU-dependent.

**Note:** 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.

### Intel Virtualization Technology

Select Enabled to enable the Intel Vanderpool Technology for Virtualization platform support, which allows multiple operating systems to run simultaneously on the same computer to maximize system resources for performance enhancement. The options are Disabled and **Enabled**. Changes take effect after you save settings and reboot the system.

**Notes:**

- This feature is NOT available when "TXT Support" is set to Enabled.
- This feature is NOT available when "Workload Profile" is set to Virtualization.

### Enable SMX

Select Enabled 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 **Disabled** and Enabled.

**Note:** This feature is available when "TXT Support" is set to Disabled.

**PPIN Control**

Select Unlock/Enabled 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/Disabled and **Unlock/Enabled**.

**AES-NI**

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

## *Advanced Power Management Configuration Menu*

### ►Advanced Power Management Configuration

**Workload Profile**

Use this feature to select a preconfigured workload profile, which is used to tune the resources in your server system. The options are **Disabled**, HPC, I/O, Virtualization, Telco NFVI, Telco NFVI-FP, and Telco FlexRAN.

**Power Performance Tuning**

This feature allows either operating system (OS) or BIOS to control the EPB. The options are **OS Controls EPB** and BIOS Controls EPB. (PECI is the abbreviation for Platform Environment Control Interface. EPB is the abbreviation for Intel Performance and Energy Bias Hint.)

**Note:** This feature is available when "Workload Profile" is set to Disabled.

**ENERGY_PERF_BIAS_CFG Mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode)**

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

**Notes:**

- This feature is available when "Power Performance Tuning" is set to BIOS Controls EPB.
- This feature is available when "Workload Profile" is set to Disabled.

### *CPU P State Control Menu*

**►CPU P State Control**

**Note:** This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.

**AVX P1**

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

**Notes:**

- This feature is available when "SpeedStep (P-States)" is set to Enabled.
- This feature is NOT available when "Workload Profile" is set to Telco FlexRAN.

**Intel SST-PP**

Use this feature to choose from two additional Base-Frequency conditions maximum for CPU P State Control. The options are **Auto**, Level 0, Level 1, Level 2, Level 3, and Level 4. The options regarding SST-PP levels are CPU-dependent. (SST-PP is the abbreviation for Speed Select Technology-Performance Profile.)

**Notes:**

- This feature is available when "SpeedStep (P-States)" is set to Enabled and when the number of SST-PP levels supported by your CPU is no less than two.
- This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

**Dynamic SST-PP**

Use this feature to disable or enable the dynamic SST-PP. The options are **Disabled** and Enabled.

**Notes:**

- This feature is available when "SpeedStep (P-States)" is set to Enabled and when your CPU supports the Intel Speed Select function.
- This feature is available when "AVX P1" is set to Nominal.
- This feature is NOT available when "Hardware P-States" is set to Disabled or Out of Band Mode.
- This feature is NOT available when "Workload Profile" is set to HPC or Virtualization.

When "SpeedStep (P-States)" is set to Enabled, the information about SST-PP levels supported by your CPU is displayed.

- SST-PP Level
- Capable
- Core Count
- P1 Ratio
- Package TDP (W)
- DTS_Max

**SpeedStep (P-States)**

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

**Note:** This feature is available when "Workload Profile" is set to Disabled.

**EIST PSD Function**

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.

**Notes:**

- This feature is available when "SpeedStep (P-States)" is set to Enabled.
- This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

**Turbo Mode**

Select Enabled 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 Disabled and **Enabled**.

**Notes:**

- This feature is available when "SpeedStep (P-States)" is set to Enabled.
- This feature is available when "Workload Profile" is set to Disabled.

### *Hardware PM State Control Menu*

**►Hardware PM State Control**

**Notes:**

- This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.
- This submenu is NOT available when “Workload Profile” is set to HPC or Virtualization.

**Hardware P-States**

If this feature is set to Disabled, system hardware will choose a P-state setting for the system based on an OS request. If this feature is set to Native Mode, system 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 the OS guidance. The options are Disabled, **Native Mode**, Out of Band Mode, and Native Mode with No Legacy Support.

## *CPU C State Control Menu*

### ►CPU C State Control

**Note:** This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.

**Monitor MWAIT**

Select Enabled 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 Disabled and **Enabled**.

**Note:** This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

**C1 to C1e Promotion**

If this feature is set to Enabled, CPU will run at its minimum frequency for lower power consumption in the C1 state. The options are Disabled and **Enabled**. This feature is CPU-dependent.

**Note:** This feature is available when "Workload Profile" is set to Disabled.

**ACPI C1 Enumeration**

Use this feature to select the ACPI C1 state or the ACPI C1e state. The options are C1 and **C1e**. This feature is CPU-dependent. (ACPI is the abbreviation for Advanced Configuration and Power Interface.)

**Note:** This feature is available when "Workload Profile" is set to Disabled.

**ACPI C6x Enumeration**

Use this feature to configure C6 state or C6 P-state as ACPI C2 or ACPI C3 state. The options are Disabled, C6 as ACPI C2, C6 as ACPI C3, C6-P as ACPI C2, C6-P as ACPI C3, and **Auto**.

**Note:** This feature is available when "Workload Profile" is set to Disabled.

### *Package C State Control Menu*

**►Package C State Control**

**Note:** This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.

**Package C State**

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

**Note:** This feature is NOT available when "Workload Profile" is set to I/O.

**LTR IIO Input**

Use this feature to set the MSR 1FCh Bit[29]. The options are Take IIO LTR input and **Ignore IIO LTR input**.

### *CPU1/CPU2 Core Disable Bitmap Menu*

**►CPU1/CPU2 Core Disable Bitmap**

**Note:** The submenu of CPU2 Core Disable Bitmap is available when your motherboard supports dual processors.

**Available Bitmap[0]:**

This feature displays the available Bitmap[0]. This feature is CPU-dependent.

**Available Bitmap[1]:**

This feature displays the available Bitmap[1]. This feature is CPU-dependent.

**CPU Core Count:**

This feature displays the number of CPU cores that can be enabled.

**CPU1/CPU2 Cores Enable**

Use this feature to set the number of CPU cores to be enabled. Enter 0 to enable all CPU cores. Note that it is required to enable at least one core per CPU. The default setting is **0**.

## Chipset Configuration Menu

### ►Chipset Configuration

**Important:** Setting the wrong values in this section may cause the system to malfunction.

### *Uncore Configuration Menu*

### ►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 Precedence to degrade UPI features if system options are in conflict. Select Feature Precedence to degrade UPI topology if system options are in conflict. The options are **Topology Precedence** and Feature Precedence.

**Link L0p Enable**

Select Enabled for the system BIOS to enable Link L0p support, which allows 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 **Disabled**, Enabled, and Auto.

**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.

**Link L1 Enable**

Select Enabled 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 **Disabled**, Enabled, 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**

Keizer Technology Interconnect (KTI) is also known as the Intel Ultra Path Interconnect (UPI) technology. Select Enabled for the KTI prefetcher to preload the L1 cache with data deemed relevant, which allows 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 it is needed. The options are Disabled, Enabled, and **Auto**.

**IO Directory Cache (IODC)**

This feature allows 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 Disabled, **Auto**, Enable for Remote InvItoM Hybrid Push, Enable for Remote InvItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, and Enable for Remote InvItoM and Remote WCiLF.

**SNC**

Sub NUMA Clustering (SNC) is a feature that breaks up the 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 Disabled, Enabled, and **Auto**. This feature is CPU-dependent.

**Note:** This feature is NOT available when "Workload Profile" is set to I/O, Virtualization, or Telco FlexRAN.

**XPT Prefetch**

XPT Prefetch is a feature that speculatively makes a copy to the memory controller of a read request being sent to the LLC. If the read request maps to the local memory address and the recent memory reads are likely to miss the LLC, a speculative read is sent to the local memory controller. The options are Disabled, Enabled, and **Auto**.

**Stale AtoS**

The in-memory directory has three states: I, A, and S states. The I (-invalid) state indicates that the data is clean and does not exist in the cache of any other sockets. The A (-snoop All) state indicates that the data may exist in another socket in an exclusive or modified state. The S state (-Shared) indicates that the data is clean and may be shared in the caches across one or more sockets. When the system is performing "read" on the memory and if the directory line is in A state, we must snoop all other sockets because another socket may have the line in a modified state. If this is the case, a "snoop" will return the modified data. However, it may be the case that a line "reads" in an A state, and all the snoops come back with a "miss." This can happen if

another socket reads the line earlier and then has silently dropped it from its cache without modifying it. If "Stale AtoS" is enabled, a line will transition to the S state when the line in the A state returns only snoop misses. That way, subsequent reads to the line will encounter it in the S state and will not have to snoop, saving the latency and snoop bandwidth. Stale "AtoS" may be beneficial in a workload where there are many cross-socket reads. The options are Disabled, Enabled, and **Auto**.

**LLC Dead Line Alloc**

Select Enabled to optimally fill the dead lines in the LLC. The options are Disabled, **Enabled**, and Auto.

## *Memory Configuration Menu*

### ►Memory Configuration

This submenu is used to configure the Integrated Memory Controller (IMC) settings.

**Enforce DDR Memory Frequency POR**

Select Enforce POR to enforce Plan of Record (POR) restrictions for DDR memory frequency and voltage programming. The options are **Enforce POR**, Enforce Stretch Goals, and Disabled.

**Host Memory Frequency**

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 4800, 5200, 5600, 6000, 6400, and 7200. Note that the available options are CPU-dependent.

**Global Scrambling**

Select Enabled to enable data scrambling to enhance system performance and data integrity. The options are Disabled and **Enabled**.

## *Memory Topology Menu*

### ►Memory Topology

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

P1-DIMMA1: 5600MT/s Hynix SRx8 16GB RDIMM

## *Memory Map Menu*

### ►Memory Map

**Intel(R) Flat Memory Mode Support**

Enable this feature to allow hardware-managed data movement between DDR5 and CXL memory, making total memory capacity visible to your system. The options are **Disabled** and Enabled.

**DDR CXL Heterogeneous Interleave Support**

Select Enabled to support heterogeneous interleaving for physical DDR5 and CXL memory. The options are **Disabled** and Enabled.

## *Memory RAS Configuration Menu*

### ►Memory RAS Configuration

Use this submenu to configure the memory mirroring, Reliability Availability Serviceability (RAS) settings.

**Mirror Mode**

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

**Note:** This feature is available when "UEFI ARM Mirror" is set to Disabled.

**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**.

**Note:** This feature is available when "Memory PFA Support" is set to Disabled.

**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 **12**.

**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 **13**.

**ADDDC Sparing (Available when populating 1Rx4, 2Rx4, and 4Rx4 DIMMs and when "Memory PFA Support" is set to Disabled)**

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. 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**.

**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.

**Note:** This feature is available when "Memory PFA Support" is set to Disabled.

**Enhanced PPR**

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

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

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

## *Security Configuration Menu*

### ►Security Configuration

---

Memory Encryption (TME) [Outputs]

---

The following information is displayed.

- MSE activation state
- MK-TME activation state
- CI activation state
- Cryptographic Algorithm configured

---

Memory Encryption (TME) [Inputs]

---

**Memory Encryption (TME)**

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

**Total Memory Encryption Multi-Tenant (TME-MT)**

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

**Memory Integrity**

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

The following information is displayed.

- KEY stock amount
- TME-MT key ID bits

**TME Encryption Algorithm**

Use this feature to set the TME encryption algorithm. The options are AES-XTS-128 and **AES-XTS-256**.

---

Trust Domain Extensions (TDX) [Outputs]

---

The following information is displayed.

- TDX activation state

---

Trust Domain Extensions (TDX) [Inputs]

---

**Trust Domain Extensions (TDX) (Available when your motherboard supports Intel TDX)**

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

**Note:** To support TDX features, DIMM population must be symmetric across integrated Memory Controllers (IMCs) and at least DIMMs per socket. For each memory controller, populating the first slots (Px-DIMMX1 or DIMMX1 depending on the motherboard design) in all channels is required. Refer to memory population below for your motherboard.

**TDX Secure Arbitration Mode Loader (SEAM Loader) (Available when your motherboard supports Intel TDX and when "Trust Domain Extensions (TDX)" is set to Enabled)**

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.

**TME-MT/TDX Key Split (Available when "Trust Domain Extensions (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**.

The following information is displayed when "Trust Domain Extensions (TDX)" is set to Enabled.

- TME-MT Keys:
- TDX Keys:

---

Processor Reserved Memory [Capabilities]

---

The following information is displayed.

- PRMRR Min Size per domain
- PRMRR Max Size per domain

---

Processor Reserved Memory [Outputs]

---

The following information is displayed.

- PRMRR Size per domain
- PRM Size per socket
- PRM Size per system

---

Software Guard Extensions (SGX) [Outputs]

---

The following information is displayed when your motherboard supports SGX.

- SGX activation state
- SGX error code [HEX]

---

Software Guard Extensions (SGX) [Inputs]

---

The following features are available when your motherboard supports SGX.

**Note:** To support SGX features, DIMM population must be symmetric across Integrated Memory Controllers (IMCs) and at least DIMMs per socket. For each memory controller, populating the first slots (Px-DIMMX1 or DIMMX1 depending on the motherboard design) in all channels is required. Refer to memory population below for your motherboard.

**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 PRMRR Size Requested (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. Note that the available options are based on your motherboard features, memory size, and memory map.

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

Owner EPOCH is used as a parameter 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 **SGX Owner EPOCH deactivated**, 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**

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

**Note:** This feature is available when "SW Guard Extensions (SGX)" is set to Enabled. This feature is NOT available when "Select Owner EPOCH Input Type" is set to SGX Owner EPOCH deactivated.

**Software Guard Extensions Epoch 1**

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

**Note:** This feature is available when "SW Guard Extensions (SGX)" is set to Enabled. This feature is NOT available when "Select Owner EPOCH Input Type" is set to SGX Owner EPOCH deactivated.

**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 the 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.

## *IIO Configuration Menu*

### ►IIO Configuration

**PCIe Completion Timeout**

Use this feature to set the PCIe completion timeout. The options are 50us to 50ms, 50us to 100us, 1ms to 10ms, 16ms to 55ms, 65ms to 210ms, **260ms to 900ms**, 1s to 3.5s, and Disabled.

**PCIe ASPM Support (Global)**

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

**PRM Feature Control**

Use this feature to enable the Platform Runtime Mechanism (PRM). The PRM is a mechanism to reduce the System Management Mode (SMM) usages and to provide an alternate means to invoke native code through the Advanced Configuration and Power Interface (ACPI) context of runtime events. The options are **Disabled** and Enabled.

**Equalization Bypass To Highest Rate**

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

**NVMe Mode Switch**

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

**PCIe PLL SSC**

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

**Snoop Response Hold Off for PCIe Stack**

Use this feature to set the IIO snoop response hold-off value to improve throughput and reduce latency. The default setting is **9**. The valid range is 0 to F. Set this feature to 0 to disable the hold-off time.

**Snoop Response Hold Off for IOAT Stack**

Use this feature to set the snoop response time of the I/O subsystem for data movements that is handled by the Intel IOAT DMA engine. The default setting is **A**. The valid range is 0 to F. Set this feature to 0 to disable the hold-off time. (DMA is the abbreviation for Direct Memory Access. IOAT is the abbreviation for I/O Acceleration Technology.)

**CXL Security Level**

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

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

**CXL Header Bypass**

Use this feature to enable the CXL header bypass. The options are **Disabled** and Enabled.

### *CPU1/CPU2 Configuration Menu*

**►CPU1/CPU2 Configuration**

**Note:** The submenu of CPU2 Configuration is motherboard-dependent.

### ►PCI Express 0 / PCI Express 1 / PCI Express 2 / PCI Express 3 / PCI Express 4 / PCI Express 5

**Note:** The number of PCIe slots and the slot naming can differ depending on the PCIe devices connected to your motherboard.

**Intel VMD Technology**

When this feature is set to Enabled, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are **Disabled** and Enabled. This feature is available for configuration when the system supports a VROC key.

**Notes:**

- This feature is available when "NVMe Mode Switch" is set to Manual.
- After you've enabled VMD in the BIOS on a PCIe slot, this PCIe slot will be dedicated for VMD use only, and it will no longer support any PCIe device. To re-activate this slot for PCIe use, disable VMD in the BIOS.

**Bifurcation**

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

### ►PCI Express 5 Port A/Port C/Port E/Port G

**Note:** The number of PCIe slots and the slot naming can differ depending on the PCIe devices connected to your motherboard.

**Requested Link Speed**

Use this feature to configure the link speed of the PCIe port you specified. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), Gen 3 (8 GT/s), Gen 4 (16 GT/s), and Gen 5 (32 GT/s).

The following information is displayed.

- Max Link Width
- Current Link Width
- Current Link Speed

**Data Link Feature Exchange**

Use this feature to enable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register. The options are Disabled and **Enabled**.

**PCIe Port Max Payload Size**

Use this feature to configure the maximum payload size supported in PCIe device capabilities register for the device installed in the PCIe port. The options are 128B, 256B, 512B, and **Auto**.

**MCTP**

Enable this feature, Management Component Transport Protocol (MCTP), to support communications between devices in a platform management subsystem. MCTP's underlying device buses include SMBus/$I^2C$, serial links, PCIe, and USB. The options are Disabled and **Enabled**.

**Equalization Bypass To Highest Rate**

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

**Intel VMD Technology**

When this feature is set to Enabled, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are **Disabled** and Enabled. This feature is available for configuration when the system supports a VROC key.

## *Intel VT for Directed I/O (VT-d) Menu*

### ►Intel VT for Directed I/O (VT-d)

**Note:** This submenu is NOT available when "Workload Profile" is set to Virtualization.

**Kernel DMA Protection**

Select Enabled to notify OS to enable DMA protection after the system has booted by setting DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR ACPI table. The options are Enabled and **Disabled**. (DMAR is the abbreviation for DMA Remapping Reporting.)

**Pre-boot DMA Protection**

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

**PCIe ACSCTL**

Select Enabled to program ACS control to Chipset PCIe Root Port Bridges. The options are Enabled and **Disabled**. (ACS is the abbreviation for Access Control Services.)

### *PCIe Leaky Bucket Configuration Menu*

#### ►PCIe Leaky Bucket Configuration

**Gen2 Link Degradation**

Use this feature to enable PCIe Gen2 link degradation. The options are Disabled and **Enabled**.

**Note:** The default setting is Enabled when your motherboard supports PCIe Gen2 link. Otherwise, the default setting is Disabled.

**Gen3 Link Degradation**

Use this feature to enable PCIe Gen3 link degradation. The options are Disabled and **Enabled**.

**Note:** The default setting is Enabled when your motherboard supports PCIe Gen3 link. Otherwise, the default setting is Disabled.

**Gen4 Link Degradation**

Use this feature to enable PCIe Gen4 link degradation. The options are Disabled and **Enabled**.

**Note:** The default setting is Enabled when your motherboard supports PCIe Gen4 link. Otherwise, the default setting is Disabled.

**Gen5 Link Degradation**

Use this feature to enable PCIe Gen5 link degradation. The options are Disabled and **Enabled**.

**Note:** The default setting is Enabled when your motherboard supports PCIe Gen5 link. Otherwise, the default setting is Disabled.

## Super IO Configuration Menu

#### ►Super IO Configuration

The following information is displayed.

- Super IO Chip

**Note:** This submenu is available when your system supports this feature.

## *Serial Port 1 Configuration Menu*

### ►Serial Port 1 Configuration

**Serial Port 1**

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

**Device Settings (Available when "Serial Port 1" above 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" above is set to Enabled)**

Use this feature to specify 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=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

## *Serial Port 2 Configuration Menu*

### ►Serial Port 2 Configuration

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

**Serial Port 2/SOL ("Serial Port 2" or "SOL" based on your system support)**

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

**Device Settings (Available when "Serial Port 2/SOL" above 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" above is set to Enabled)**

Use this feature to specify 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 (or SOL).

The options are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

**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 Menu

### ►Serial Port Console Redirection

**COM1 (Available when your system supports the 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.

**SOL/COM2**

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

**Console Redirection**

Select Enabled to use the SOL/COM2 port for Console Redirection. The options are Disabled and **Enabled**.

#### ►Console Redirection Settings

**Note:** This submenu is available when "Console Redirection" for COM1 or SOL/COM2 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 1s in data bits is even. Select Odd if the parity bit is set to 0 and the number of 1s 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**

Use this feature to select the function key and keypad settings on Putty, which is a terminal emulator designed for the Windows OS. The options are **VT100**, LINUX, XTERMR6, SCO, ESCN, and VT400.

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

Use the features below 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**

**Note:** This submenu is available when "Console Redirection EMS" is set to Enabled.

**Out-of-Band Mgmt Port**

Use this feature to select a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2. Note that the option of SOL/COM2 indicates a shared serial port. SOL 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 Stack Configuration Menu

### ►Network Stack 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 you to press the <ESC> key to abort PXE boot instead of proceeding with PXE boot by connecting to a network server immediately. Press the <+> or <-> key on your keyboard to change the value. The default setting is **0**.

**Media Detect Count (Available when "Network Stack" is set to Enabled)**

Use this feature to set 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 the <+> or <-> key on your keyboard to change the value. The default setting is **1**.

## *MAC:(MAC address)-IPv6 Network Configuration Menu*

### ►MAC:(MAC address)-IPv6 Network Configuration

#### ►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**

Use this feature to set the number of consecutive neighbor solicitation messages that have been sent while performing duplicate address detection on a tentative address. 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

**Note:** This submenu is available when "Policy" is set to manual.

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

**New Gateway addresses**: Use this feature to set the gateway address for the local machine.

**New DNS addresses**: Use this feature to set the DNS server address for the local machine.

**Commit Changes and Exit**: Press <Enter> to save changes and exit.

**Discard Changes and Exit**: Press <Enter> to discard changes and exit.

**Save Changes and Exit**

Press <Enter> to save changes and exit.

## *MAC:(MAC address)-IPv4 Network Configuration Menu*

### ►MAC:(MAC address)-IPv4 Network Configuration

**Configured**

Enable this feature to configure network addresses for DHCP, local IP address, local netmask, local gateway, and local DNS server. 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 "Enable 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 "Enable 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 "Enable 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 "Enable 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.

## PCIe/PCI/PnP Configuration Menu

### ►PCIe/PCI/PnP Configuration

The following information is displayed.

- PCI Bus Driver Version

**PCI Devices Common Settings:**

**Above 4G Decoding**

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

**Re-Size BAR Support**

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

**MMCFG Base**

This feature determines how the lowest Memory Mapped Configuration (MMCFG) base is assigned to onboard PCI devices. The options are 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, and **Auto**. The options of 2G and 2.25G are not available when the MMCFG size is 2G. The option of 3G is not available when the MMCFG size is 1G or 2G.

**MMCFG Size**

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

**MMIO High Base**

Use this feature to select the base memory size according to memory-address mapping for the I/O hub. The options are 248T, 120T, 88T, 60T, 30T, 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T, and **Auto**. The options of 248T, 120T, 88T, 60T, 30T, and 3584T are CPU-dependent.

**MMIO High Granularity Size**

Use this feature to select the high memory size according to memory-address mapping for the I/O hub. The options are 1G, 4G, 16G, 32G, 64G, 256G, and **1024G**. This feature is motherboard-dependent.

**SR-IOV Support (Unavailable when "Workload Profile" is set to Virtualization)**

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

**Bus Master Enable**

If this feature is set to Enabled, the PCI Bus Driver will enable the Bus Master Attribute for DMA transactions. If this feature 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 option of Vendor Defined Firmware is pre-installed on the drive and may resolve errata or enable innovative functions for the drive. The option of AMI Native Support is offered by the BIOS with a generic method. The default option is motherboard-dependent.

**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.

**PCI Devices Option Rom Setting**

**M.2 PCIe Option OPROM / Onboard SAS Option ROM / Onboard LAN1 Option ROM / Onboard NVMe1 Option ROM – Onboard NVMe24 Option ROM**

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

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

**Onboard LAN1 Option ROM**

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

**Note:** This feature is available when your motherboard supports onboard LAN ports.

**Onboard LAN2 Option ROM**

Use this feature to boot the computer using the EFI device installed on LAN port 2. Select Disabled to disable this feature. The default setting is **Disabled**.

**Note:** This feature is available when your motherboard supports onboard LAN ports and when "Onboard LAN1 Option ROM" is set to Disabled.

# ACPI Settings Menu

## ►ACPI Settings

**NUMA**

Use this feature to enable Non-Uniform Memory Access (NUMA) support to minimize memory access latencies. The options are Disabled and **Enabled**. This feature is CPU-dependent.

**Virtual NUMA**

Enable this feature to optimize the memory-access performance for VMware virtual machines. The options are **Disabled** and Enabled.

**Note:** This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

**Number of Virtual NUMA Nodes (Available when "Virtual NUMA" is set to Enabled)**

This feature displays the number of virtual NUMA nodes. A NUMA architecture divides hardware resources (including processors, memory, and I/O buses) into groups, called NUMA nodes. This feature indicates the available number of virtual NUMA nodes that can be assigned to the virtual machine. By default, this setting is automatically adjusted to match the physical NUMA topology.

**UMA-Based Clustering (Available when SNC is set to Disabled)**

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)** and Hemisphere (2-clusters).

**WHEA Support**

Select Enabled to support the Windows Hardware Error Architecture (WHEA) platform. WHEA provides a common infrastructure for the system to handle hardware errors within the Windows OS environment, reducing system crashes and enhancing 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 Menu

### ►Trusted Computing

When the TPM 2.0 (either onboard or external) is detected by your system, the following information is displayed.

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

**Note:** This submenu is available when the TPM 2.0 (either onboard or external) is detected by the BIOS.

**Security Device Support**

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

When "Security Device Support" is set to Enabled and the TPM 2.0 (either onboard or external) is detected by the BIOS, the following information is displayed.

- Active PCR banks
- Available PCR banks

**Note:** The following features are available when the TPM 2.0 (either onboard or external) is detected by the BIOS.

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

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

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

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

**SHA384 PCR Bank (Available when "Security Device Support" is set to Enabled)**

Select Enabled to enable SHA384 PCR Bank support to enhance system integrity and data security. The options are **Disabled** and Enabled.

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

Use this feature to schedule a TPM-related operation to be performed by the security TPM (either onboard or external) at the next system boot to enhance system data integrity. The options are **None** and TPM Clear.

**Note:** If this feature is used, your system will reboot to carry out a pending TPM operation.

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

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 the TPM (either onboard or external). The options are Disabled and **Enabled**.

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

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 Enabled)**

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 (either onboard or external) 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**

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

Set this feature to Enabled to unlock the TPM. Save settings and exit the BIOS Setup utility. The Non-volatile (NV) indexes can be deleted after the system reboot. The options are **Disabled** and Enabled.

## Supermicro KMS Server Configuration Menu

### ►Supermicro KMS Server Configuration

**Note:** Be sure to configure all the features in the submenu of Supermicro KMS Server Configuration and the feature of "KMS Security Policy" in the submenu of Super-Guardians Configuration so that your system can communicate with the KMS server.

### TPM-KMS Support

This feature combines the capabilities of a hardware-based security module (TPM) with the Key Management Service (KMS) to enhance security by managing cryptographic keys and ensuring secure access to sensitive data. The options are **Disabled** and Enabled.

### Supermicro KMS Server IP address

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

### Second Supermicro KMS Server IP address

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

### Supermicro KMS TCP Port number

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

### KMS Time Out

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

### TimeZone

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

### Client UserName

Press <Enter> to set the client identity (UserName). The length is 0–63 characters.

### Client Password

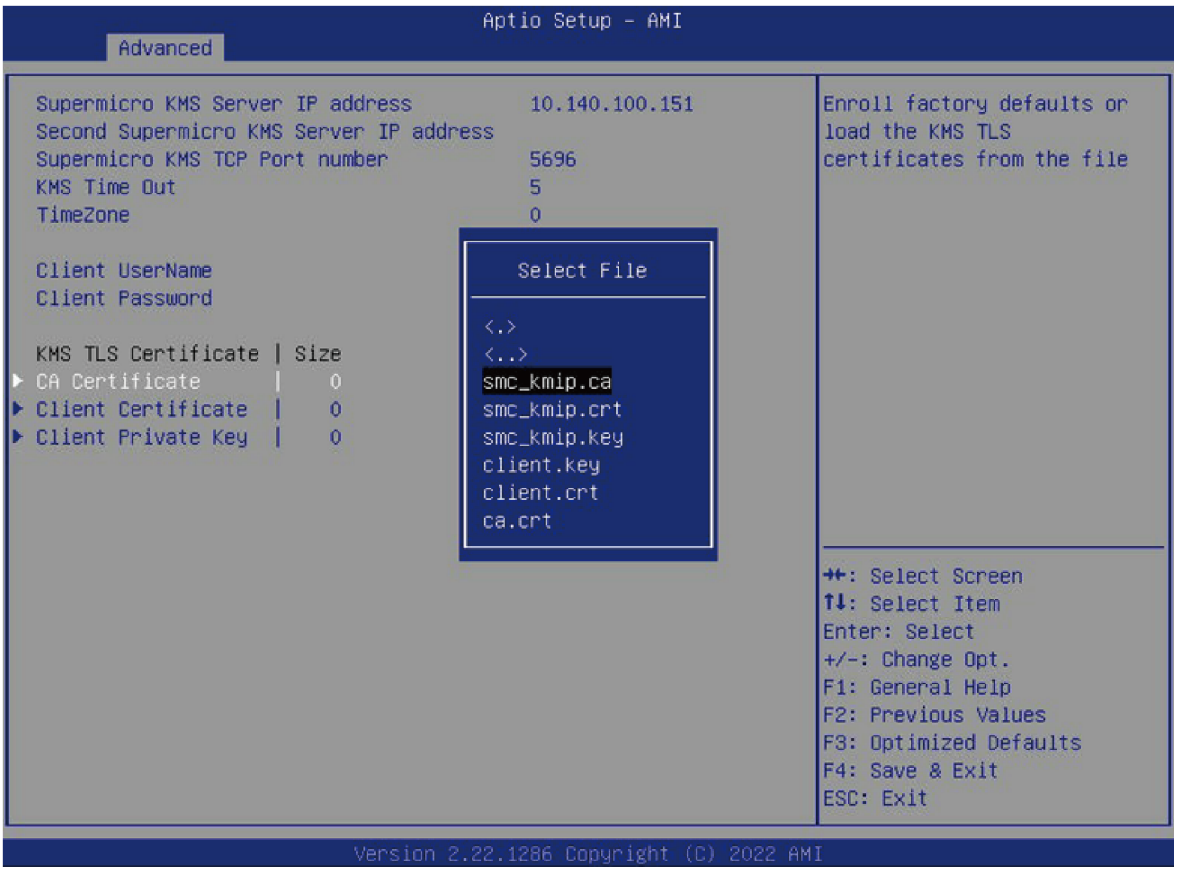
Press <Enter> to set the client identity (Password). The length is 0–31 characters.

### ►CA Certificate

### ►Client Certificate

### ►Client Private Key

Use the three features above to enroll factory defaults or load the KMS Transport Layer Security (TLS) certificates, which are generated by the KMS server, from the file stored in the USB flash drive as shown below.




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

Use this feature to change the private key password.

## Super-Guardians Configuration Menu

### ►Super-Guardians Configuration

**Super-Guardians Protection Policy**

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

**KMS Security Policy (Available when "TPM Security Policy" and "USB Security Policy" are set to Disabled)**

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

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

**Notes:**

- Be sure that the KMS server is ready before configuring this feature.
- Use the professional KMS server solutions (e.g., Thales Server) or the Supermicro PyKMIP Software Package to establish the KMS server.

**KMS Server Retry Count (Available when "TPM Security Policy" and "USB Security Policy" are set to Disabled)**

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

**TPM Security Policy (Available when "KMS Security Policy" and "USB Security Policy" are set to Disabled)**

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

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

**Note:** The TPM 2.0 (either onboard or external) is required to configure this feature.

**Load Authentication-Key (Available when "KMS Security Policy," "TPM Security Policy," and "USB Security Policy" are set to Disabled)**

Use this feature to load the Authentication-Key. The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save settings and reboot the system. While booting, the BIOS will automatically load the Authentication-Key (filename: TPMAuth.bin) from the USB flash drive. Afterwards, the default setting will be set to Disabled by the BIOS.

**Notes:**

- Be sure to connect a USB flash drive with the Authentication-Key (filename: TPMAuth.bin) to your system before the system reboot.
- Be sure to save the Authentication-Key (filename: TPMAuth.bin) to the USB flash drive and keep a backup. Load the Authentication-Key (filename: TPMAuth.bin) after the TPM (either onboard or external) is detected by your system. Otherwise, the TPM function can not work properly.

**Save Authentication-Key (Available when "TPM Security Policy" is set to Enabled)**

Use this feature to save the Authentication-Key. The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save settings and reboot the system. While booting, the BIOS will automatically save the Authentication-Key (filename: TPMAuth.bin) to the USB flash drive. Afterwards, the default setting will be set to Disabled by the BIOS.

**Note:** Be sure to connect a USB flash drive to your system before the system reboot.

**USB Security Policy (Available when "KMS Security Policy" and "TPM Security Policy" are set to Disabled)**

Use this feature to enable the USB Security Policy. The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save settings and reboot the system. Connect a USB flash drive to your system before the system reboot. While booting, the BIOS will automatically create the USB Authentication-Key (filename: USBAuth.bin) and save it to the USB flash drive.

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

**Note:** Be sure to connect a USB flash drive to your system before configuring this feature. Save the USB Authentication-Key (filename: USBAuth.bin) to the USB flash drive and keep a backup.

## HTTP Boot Configuration Menu

### ►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**

**Important:** Disabling "HTTPS Boot Checks Hostname" is a violation of RFC 6125 and may expose you to Man-in-the-Middle Attacks. Supermicro is not responsible for any and all security risks incurred by you disabling this feature.

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. Be sure to enter a boot description; otherwise, the boot option for the URI cannot be created.

**Boot URI**

Enter a Boot Uniform Research Identifier (URI) with 128 characters or shorter. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created.

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

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

**Select IPv4 or IPv6 (Unavailable when "Instance of Priority 2:" above is set to 0)**

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

**Boot Description (Unavailable when "Instance of Priority 2:" above is set to 0)**

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

**Boot URI (Unavailable when "Instance of Priority 2:" above is set to 0)**

Enter a Boot URI with 128 characters or shorter. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created.

## Intel(R) Ethernet Controller Menu

### ►Intel(R) Ethernet Controller (Ethernet controller) - (MAC address)

**Notes:**

- The Ethernet controller and MAC address shown above are based on your system features.
- This submenu is available when the LAN Option ROM type is EFI.

#### ►Firmware Image Properties

Use this feature to review device firmware version information.

The following information is displayed.

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

#### ►NIC Configuration

**Link Speed**

Use this feature to set the connection speed of a selected LAN port. The options are **Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, and 100 Mbps Full.

**Wake On LAN**

Set this feature to support system wake-up via the selected LAN port. If this feature is set to Enabled, the LAN port selected will be enabled when the system is powered on. The options are Disabled and **Enabled**.

**LLDP Agent**

Use this feature to enable or disable Link Layer Discovery Protocol (LLDP) agent support on a long-term basis. The LLDP, a vendor-neutral link layer protocol, is used by a network device to identify itself and announce its capability to the neighboring devices in a network environment for networking. When disabling the LLDP agent in the firmware, the function of Data Center Bridging (DCB) will also be disabled. The options are Disabled and **Enabled**.

**Link Speed Method**

Set a port's link parameters automatically or manually. The options are Manual and **Auto**.

### ►Device Level Configuration

**Transmit Balancing**

For environments with highly scaled workloads and uneven performance between threads, enable to provide a consistent transmit fairness across queues, PFs, and VFs. The options are **Disabled** and Enabled.

**Virtualization Mode**

Sets the virtualization mode setting of the controller. The options are **None**, SR-IOV, Scalable IOV.

### ►Port Option Configuration

**Port Option**

Configure the port option of the device. The options are Option 0: 2x25G and **Option 1: 1x50G**.

**Port option outlines**

#### ►Option 0: 2x25G

#### ►Option 1: 1x50G

**Blink LEDs**

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

The following information is displayed.

- UEFI Driver
- Adapter PBA
- Device Name
- Chip Type
- PCI Device ID
- PCI Address
- Link Status
- MAC Address
- Virtual MAC Address
- Media Detection
  - The options are Enabled and **Disabled**.
- Forward Error Correction
- No-FEC in FEC Auto
  - The options are Enabled and **Disabled**.

## TLS Authenticate Configuration Menu

### ►TLS Authenticate Configuration

Use this submenu to configure Transport Layer Security (TLS) settings.

#### ►Server CA Configuration

Use this feature to configure the server Certificate Authority (CA).

#### ►Enroll Certification

Use this feature to enroll the certificate in the system.

#### ►Enroll Certification Using File

Use this feature to enroll the security certificate in the system by using a file.

#### ►Commit Changes and Exit

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

#### ►Discard Changes and Exit

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

### ►Delete Certification

Use this feature to delete the certificate if a certificate has been enrolled in the system.

### ►Client Certification Configuration

## VLAN Configuration (MAC:(MAC address))

### ►VLAN Configuration (MAC:(MAC address))

### ►Enter Configuration Menu

**Create new VLAN**

**VLAN ID**

Use this feature to create a new VLAN ID. The valid range is 1–4094. The default setting is **1**.

**Priority**

Press <Enter> to set the priority of this VLAN. The valid range is 0–7.

**Add VLAN**

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

**Configured VLAN List**

The following information is displayed about currently configured VLANs.

- VLAN ID
- Priority

**Remove VLAN**

Press <Enter> to remove selected VLANs.

## Driver Health Menu

### ►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. The driver health status will differ depending on the drivers installed in your system. It's also based on your system configuration and the environment that your system is operating in.

## 4.4 Event Logs

Use this menu to configure Event Logs settings.

**Note:** After making any changes in this section, be sure to reboot the system for the changes to take effect.

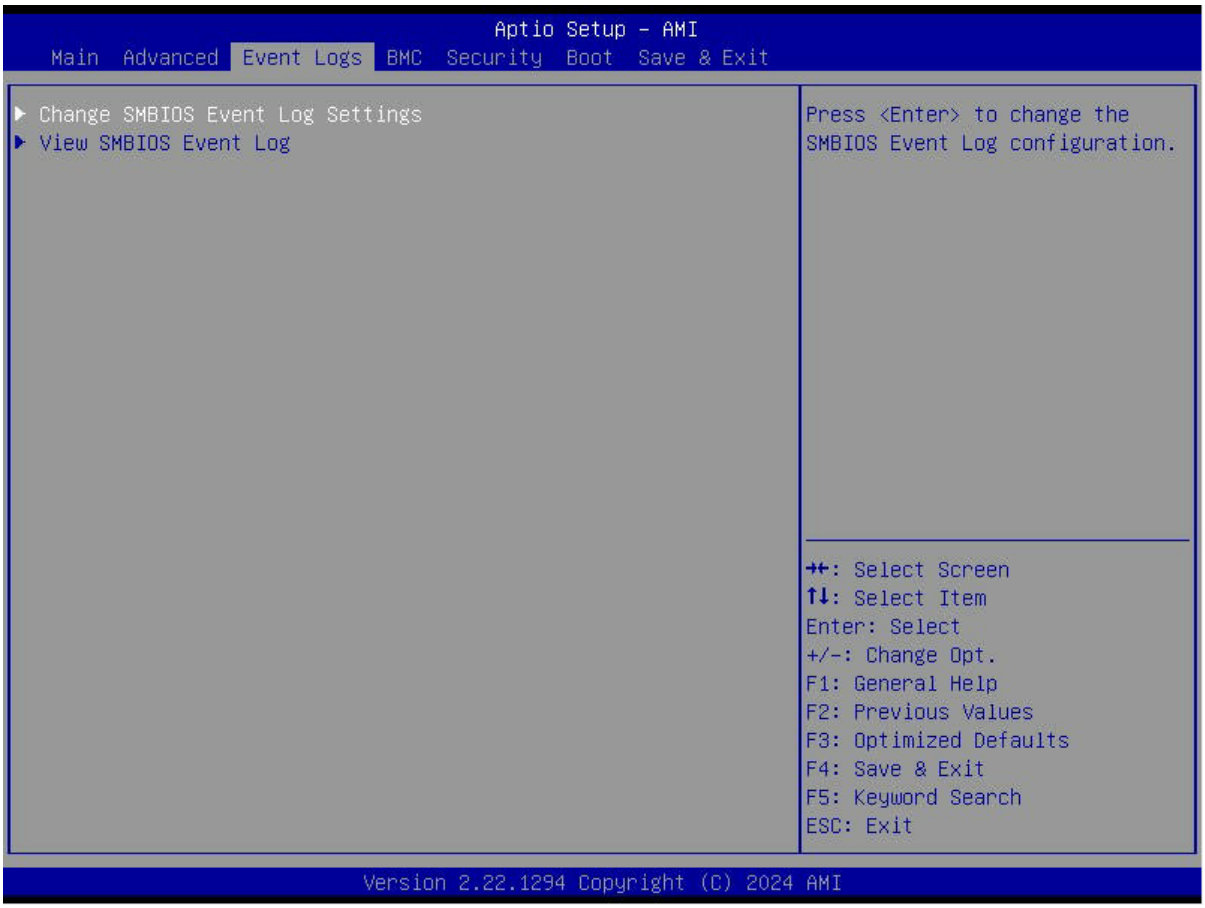



**Figure 4-3. Event Logs**

### ►Change SMBIOS Event Log Settings

**Note:** Reboot the system for the changes in this section to take effect.

**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 and 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)**

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

### ►View SMBIOS Event Log

Use this feature to view the events in the system event log. Select this feature and press <Enter> to view the status of an event in the log. The following information is displayed: DATE / TIME / ERROR CODE / SEVERITY.

# 4.5 BMC

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

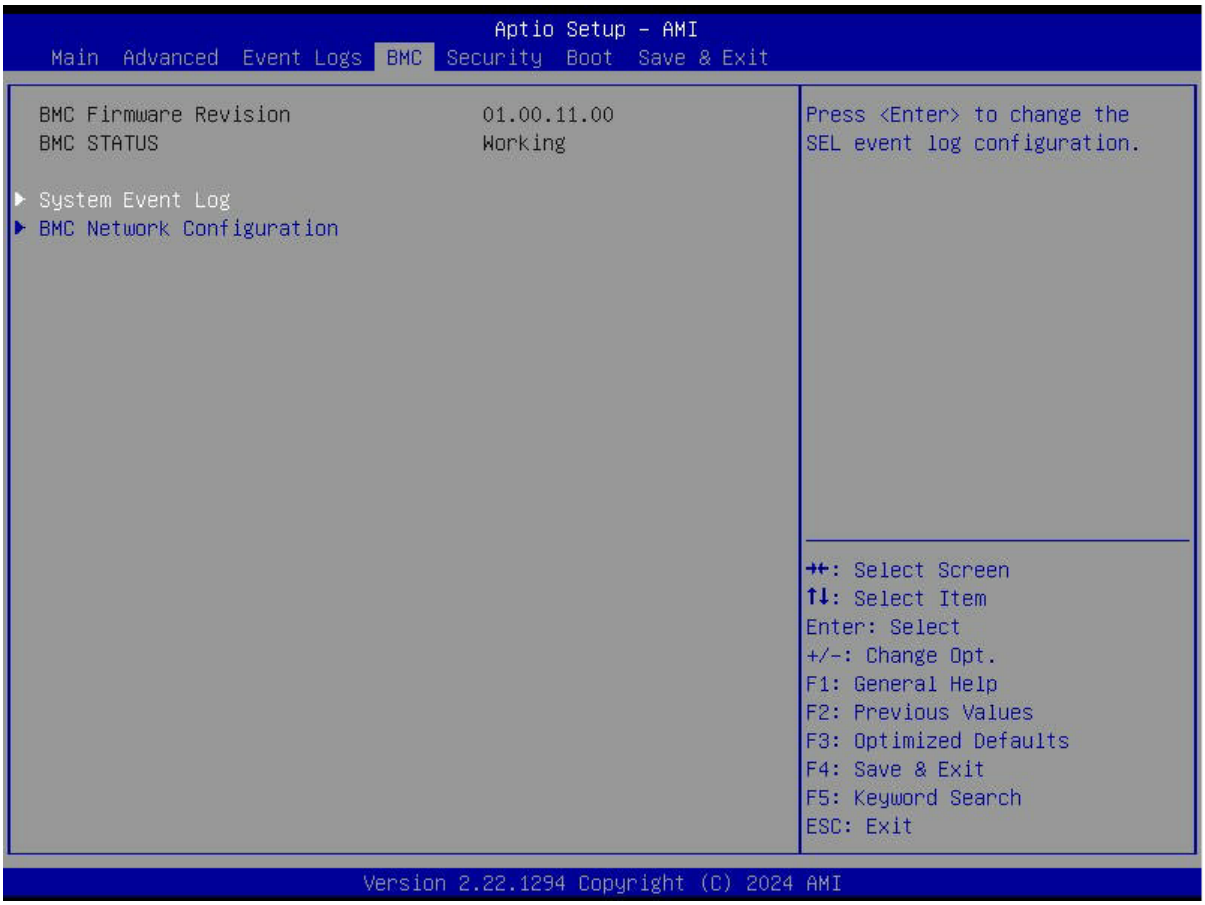



**Figure 4-4. BMC**

### BMC Firmware Revision

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

### BMC STATUS

This feature indicates the status of the BMC firmware installed in this system.

## System Event Log Menu

### ►System Event Log

**Note:** All values changed in this submenu do not take effect until computer is restarted.

**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 (Available when "SEL Components" is set to Enabled)**

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 (Available when "SEL Components" is set to Enabled)**

This feature defines 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.

## BMC Network Configuration Menu

### ►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**

This feature displays the type of the BMC LAN.

**BMC Network Link Status:**

This feature displays the status of the BMC network link for this system.

**Configuration Address Source**

Use this feature to select the source of the IPv4 connection. If Static is selected, note the IP address of the 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**. It is available for configuration when "Update BMC LAN Configuration" is set to Yes.

**Station IP Address**

This feature displays the Station IP address in decimal and in dotted quad form (i.e., 172.29.176.131). It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static.

**Subnet Mask**

This feature displays the sub- network that this computer belongs to. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static.

**Station MAC Address**

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

**Gateway IP Address**

This feature displays the IPv4 gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1). It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static.

**VLAN (Available when "Update BMC LAN Configuration" is set to Yes)**

This feature displays the status of VLAN supprt. The options are **Disable** and Enable.

**VLAN ID**

Use this feature to create a new VLAN ID. The valid range is 1–4094. The default setting is **1**.

**********

**Configure IPv6 Support**

**********

**IPv6 Address Status**

This feature displays the status of the IPv6 address.

**IPv6 Support**

Use this feature to enable IPv6 support. The options are **Enabled** and Disabled. It is available for configuration when "Update BMC LAN Configuration" is set to Yes.

**Configuration Address Source**

Use this feature to select the source of the IPv6 connection. If Static Configuration is selected, note 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. It is available for configuration when "Update BMC LAN Configuration" is set to Yes.

**IPv6 Address ("Static," "DHCPv6 Stateless," or "DHCPv6 Stateful," depending on the option you selected for "Configuration Address Source" above)**

This feature displays the station IPv6 address. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static Configuration.

**Prefix Length**

This feature displays the prefix length. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static Configuration.

**Gateway IP**

This feature displays the IPv6 gateway IP address. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static Configuration.

**Advanced Settings**

Use this feature to set the DNS server IP. The default setting allows this system to obtain the DNS server IP automatically. The options are **Auto obtain DNS server IP** and Manually obtain DNS server IP. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to DHCPv6 Stateless.

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

This feature displays 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 displays the alternative DNS server IP. It can be configured via Redfish.

## 4.6 Security

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

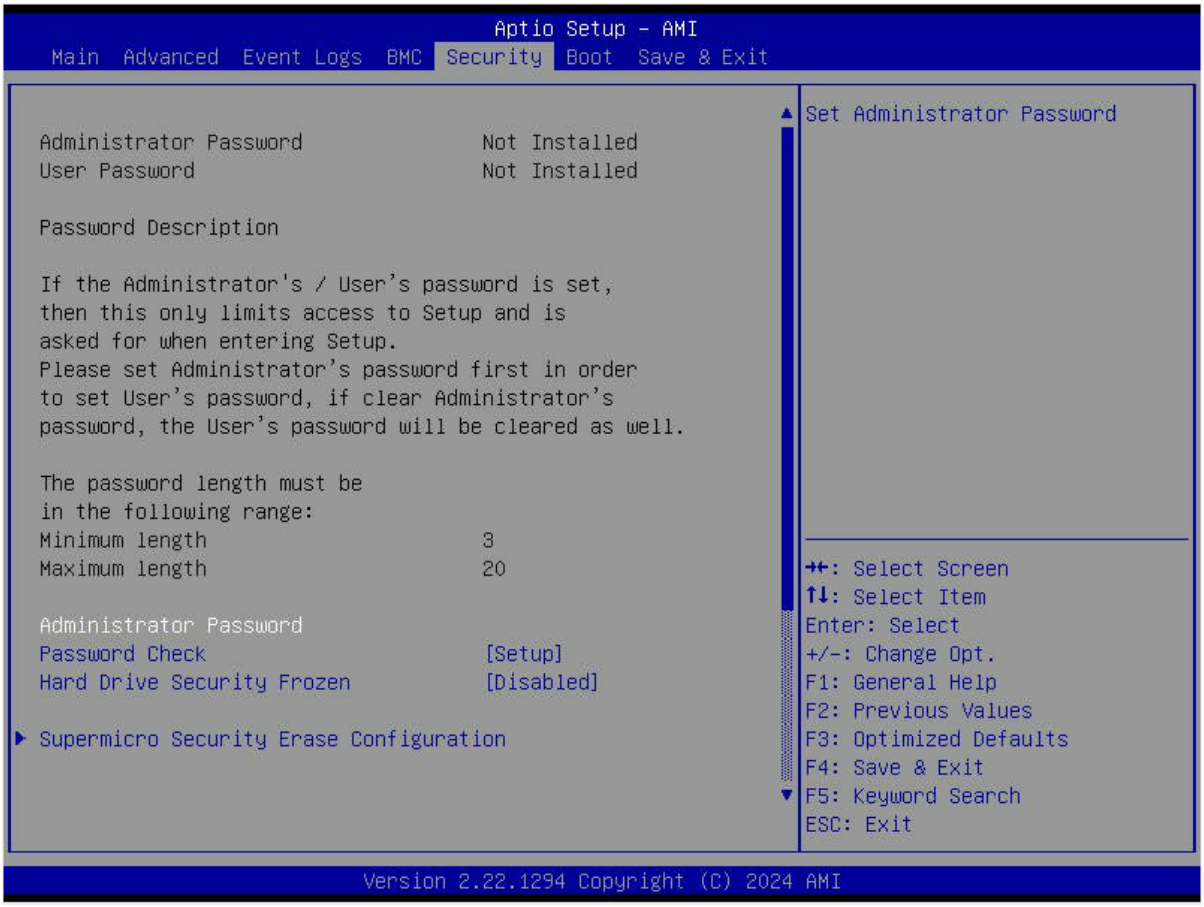



**Figure 4-5. Security**

**Disable Block Sid and Freeze Lock (Available when your storage devices support TCG)**

Select Enabled to allow SID authentication to be performed in TCG storage devices. The options are **Disabled** and Enabled. (SID is the abbreviation for Storage ID Authority.)

The following information is displayed:

- Administrator Password
- User Password
- Password Description

**Administrator Password**

This feature indicates if an administrator password has been installed. Use this feature to set the administrator password, which is required to enter the BIOS Setup utility. The length of the password can be between three and 20 characters long.

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

This feature indicates if a user password has been installed. Use this feature to set the user password which is required to enter the BIOS Setup utility. The length of the password can be between three and 20 characters long.

**Password Check**

Select Setup for the system to check for a password upon entering the BIOS Setup utility. Select Always for the system to check for the passwords needed 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 altered. The options are **Disabled** and Enabled.

**Lockdown Mode (Available when the DCMS key is activated)**

Select Enabled to support the Lockdown Mode, which prevents the existing data or keys stored in the system from being altered or changed in an effort to preserve system integrity and security. The options are **Disabled** and Enabled.

## Supermicro Security Erase Configuration Menu

### ►Supermicro Security Erase Configuration

Use this submenu to configure the Supermicro-proprietary Security Erase settings. When this submenu is selected, the following information is displayed. Note that the order of the following information may differ based on the storage devices being detected.

- HDD Name: This feature displays the model name of the storage device that is detected by the BIOS.
- HDD Serial Number: This feature displays the serial number of the storage device that is detected by the BIOS.
- Security Mode: This feature displays the security mode of the storage device that is detected by the BIOS.
- Estimated Time: This feature displays the estimate time needed to perform the selected Security Erase features.
- HDD User Pwd Status: This feature indicates if a password has been set as a storage device user password, which enables configuring Supermicro Security Erase settings on this storage device.
- TCG Device Type: This feature displays the TCG device type detected by the system.

- Admin Pwd Status: This feature indicates if a password has been set as a storage device administrator password, which enables configuring Supermicro Security Erase settings on this storage device.

**Note:** This submenu is available when any storage device is detected by the BIOS. For more information about this feature, refer to our website.

**Security Function**

Select Set Password to set a storage device user password to enable configuring the security settings on the storage device. Select Security Erase - Password to enter a storage device user password to enable erasing the password and the contents previously stored in the storage device. Select Security Erase - Without Password to use the manufacturer default password "111111111" as the storage device user password and enable erasing the contents of the storage device by using this default password. The options are **Disabled**, Set Password, Change Password, Clear Password, Security Erase - Password, Security Erase - PSID, and Security Erase - Without Password.

**Notes:**

- The option of Security Erase - PSID is based on the storage device support. PSID is the abbreviation for Physical Security Identification.
- The options of Change Password and Clear Password are available when "Password" below has been set.
- The option of Set Password is NOT available when "Password" below has been set.

**Password**

Use this feature to set the storage device user password, which enables configuring the Supermicro Security Erase settings by using this user password.

**New Password (Available when "Password" above has been set)**

Use this feature to set the new user password for the storage device, which enables configuring the Supermicro Security Erase settings by using this new user password.

## HDD Security Configuration Menu

### ►P4: (Storage device model name)

This submenu 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)**

Press <Enter> to set the HDD user password.

## Secure Boot Menu

### ►Secure Boot

The following information is displayed:

- System Mode
- Secure Boot

**Note:** For detailed instructions on configuring Security Boot settings, refer to the Security Boot Configuration User's Guide at https://www.supermicro.com/support/manuals.

**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**.

#### ►Enter Audit Mode

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

**Note:** This submenu is available when "Secure Boot Mode" is set to Custom.

### ►Enter Deployed Mode / Exit Deployed Mode

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

**Note:** This submenu is available when "Secure Boot Mode" is set to Custom.

### ►Key Management

The following information is displayed:

- Vendor Keys

**Note:** This submenu is available when "Secure Boot Mode" is set to Custom.

**Provision Factory Defaults**

Select Enabled to install the default secure boot keys when the system is in the Setup Mode. Changes take effect after you save settings and reboot the system. The options are **Disabled** and Enabled.

#### ►Restore Factory Keys

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

**Note:** This submenu is available when any secure keys have been installed.

#### ►Reset To Setup Mode

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

**Note:** This submenu is available when any secure keys have been installed.

#### ►Enroll Efi Image

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

#### ►Export Secure Boot Variables

This feature exports the NVRAM contents of secure boot variables to a storage device. The options are **Yes** and No.

**Note:** This submenu is available when any secure keys have been installed.

**Secure Boot variable / Size / Keys / 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, key numbers, and the sources of the authorized signatures. Select Update to update the platform key.

### ►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, key numbers, and the sources of the authorized signatures. Select Update to update the Key Exchange Keys. Select Append to append the Key Exchange Keys.

### ►Authorized Signatures (db)

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, key numbers, and sources of the authorized signatures. Select Update to update the Authorized Signatures. Select Append to append the new Authorized Signatures.

### ►Forbidden Signatures (dbx)

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 Signature.

### ►Authorized TimeStamps (dbt)

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.

### ►OsRecovery Signatures (dbr)

Use this feature to set and save the Authorized Signatures used for OS recovery. Select Update to update the OsRecovery Signatures. These values also indicate sizes, keys, and key sources of the OsRecovery Signatures. Select Append to append the OsRecovery Signatures.

## TCG Storage Security Configuration Menu

### ►(Storage device model name)

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:
- User Pwd Status:
- Admin Pwd Status:

**Note:** This submenu is available when the storage device is compliant with TCG specifications.

**Set Admin Password**

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

**Set User Password (Available when "Set Admin Password" has been set)**

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

**Device Reset**

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

## 4.7 Boot

Use this menu to configure Boot settings.

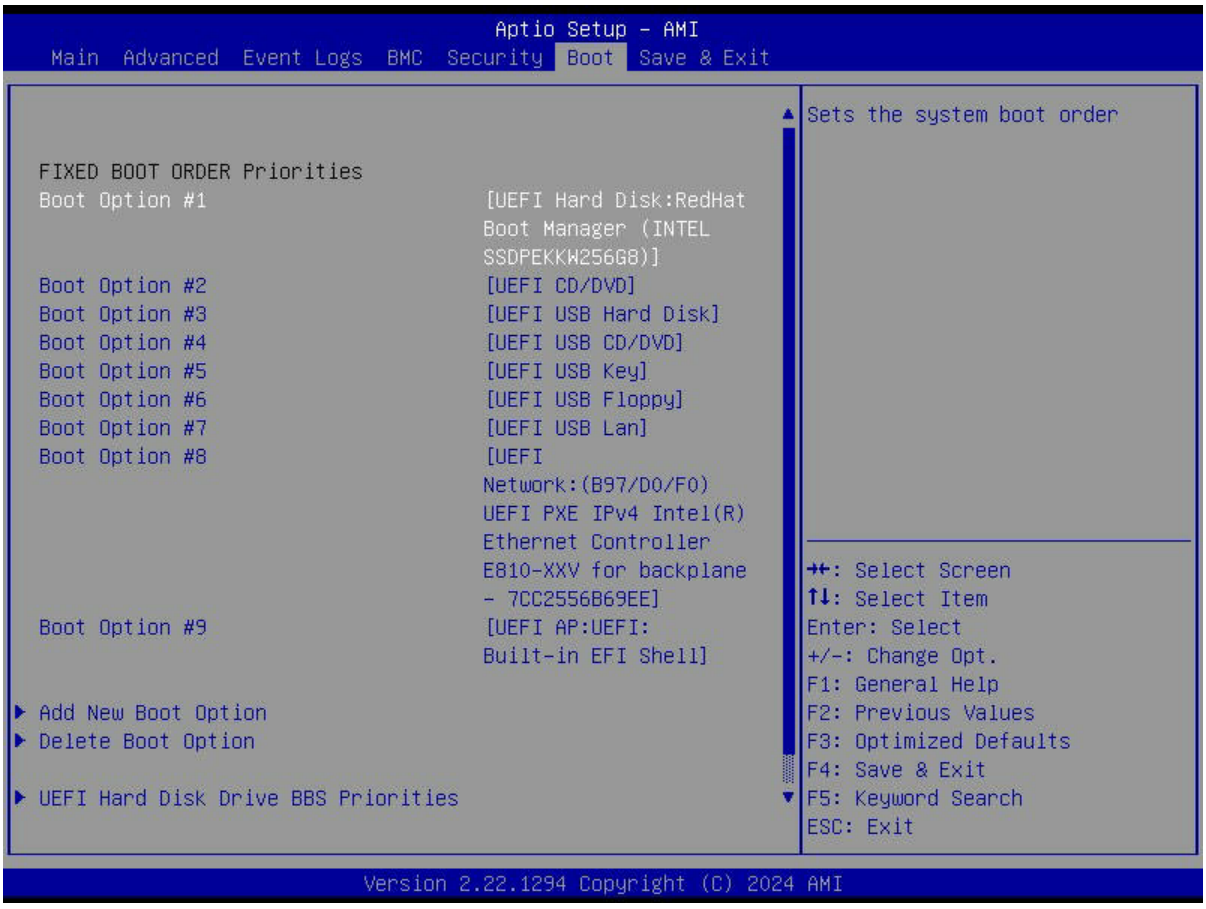



**Figure 4-6. Boot**

### FIXED BOOT ORDER Priorities

Use this feature to prioritize the order of bootable devices from which the system will boot. Press <Enter> on each item sequentially to select the device.

- Boot Option #1 – Boot Option #9

### ▶Add New Boot Option

Use this feature to add a new boot option to the boot priority features for system boot.

**Note:** This submenu is available when any storage device is detected by the BIOS.

#### 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 setting the name and the file path for the boot option, press <Enter> to create the new boot option in the boot priority list.

### ►Delete Boot Option

Use this feature 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

Use this feature to set the system boot order of detected devices.

### ►UEFI NETWORK Drive BBS Priorities

Use this feature to set the system boot order of detected devices.

### ►UEFI Application Boot Priorities

Use this feature to set the system boot order of detected devices.

## 4.8 Save & Exit

Select Save & Exit from the BIOS Setup screen to configure the settings below.

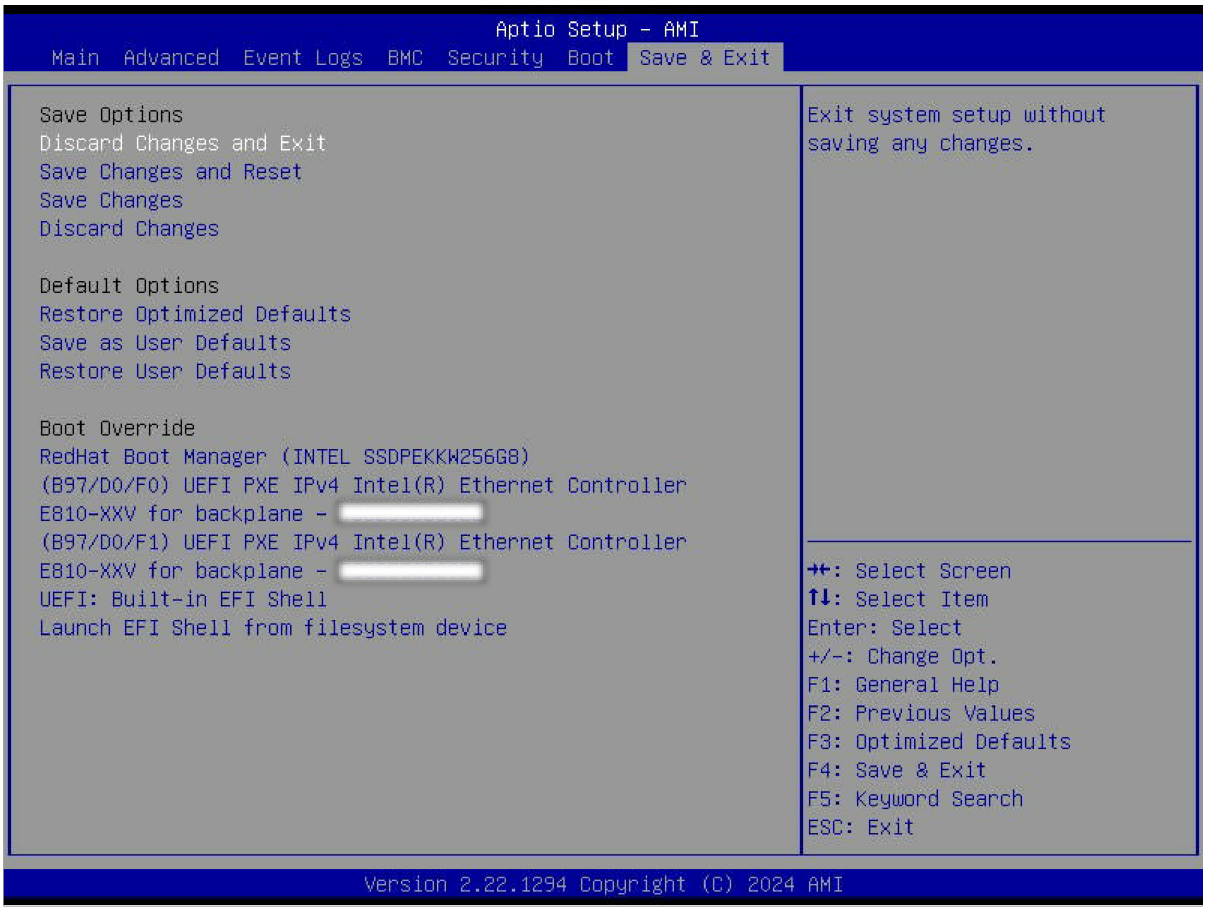



**Figure 4-7. Save and Exit**

### 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 system.

#### Save Changes and Reset

On completing the system configuration changes, use this feature to exit the BIOS Setup utility and reboot the system for the new system configuration parameters to take effect.

#### Save Changes

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

### Discard Changes

Select this feature and press <Enter> to discard all changes 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.

**Note:** Reboot the system for the changes to take effect to ensure that the system has the optimized default settings.

### Save as User Defaults

Select this feature and press <Enter> to save all changes as the default values specified to the BIOS Setup utility for future use.

### Restore User Defaults

Select this feature and press <Enter> to restore user-defined default settings that have been saved previously.

### Boot Override

**Note:** Use this section to override the Boot priorities sequence in the Boot menu, and immediately boot the system with a device specified here instead of the one specified in the boot list. This is a one-time boot override.

### Launch EFI Shell from filesystem device

Use this feature to launch the EFI shell application (Shell.efi) from one of the available filesystem devices. A filesystem is a virtual, logical, or physical system for organizing, managing, and accessing the files and directories on devices such as SSDs, HDDs, or other storage devices.

# Appendix A:

# BIOS Codes

For information about BIOS codes for the B14DBT motherboard, refer to the following content.

## BIOS Error POST (Beep) Codes

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

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

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

These fatal errors are usually communicated through a series of audible beeps that can be heard on an external buzzer connected to JD1. The table shown below lists some common errors and their corresponding beep codes encountered by users.

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

## Additional BIOS POST Codes

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

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

# Appendix B:

# Software

After the B14DBT motherboard has been installed, you can install the Operating System (OS), configure RAID settings, and install the drivers.

## 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 https://www.supermicro.com/support/manuals.

### Installing the OS

1. Create a method to access the Microsoft Windows installation ISO file. That can be a USB flash or media drive, or the BMC KVM console.
2. Retrieve the proper drivers. 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 bootup.

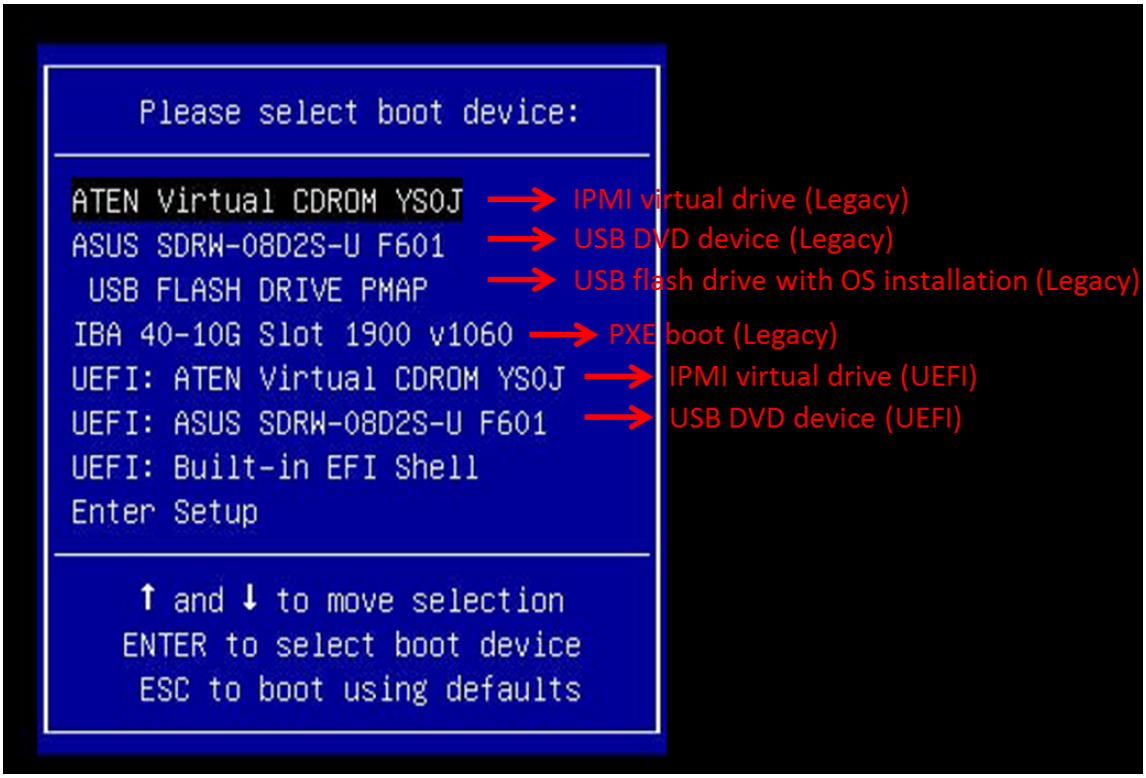



**Figure B-1. Selecting the Boot Device**

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

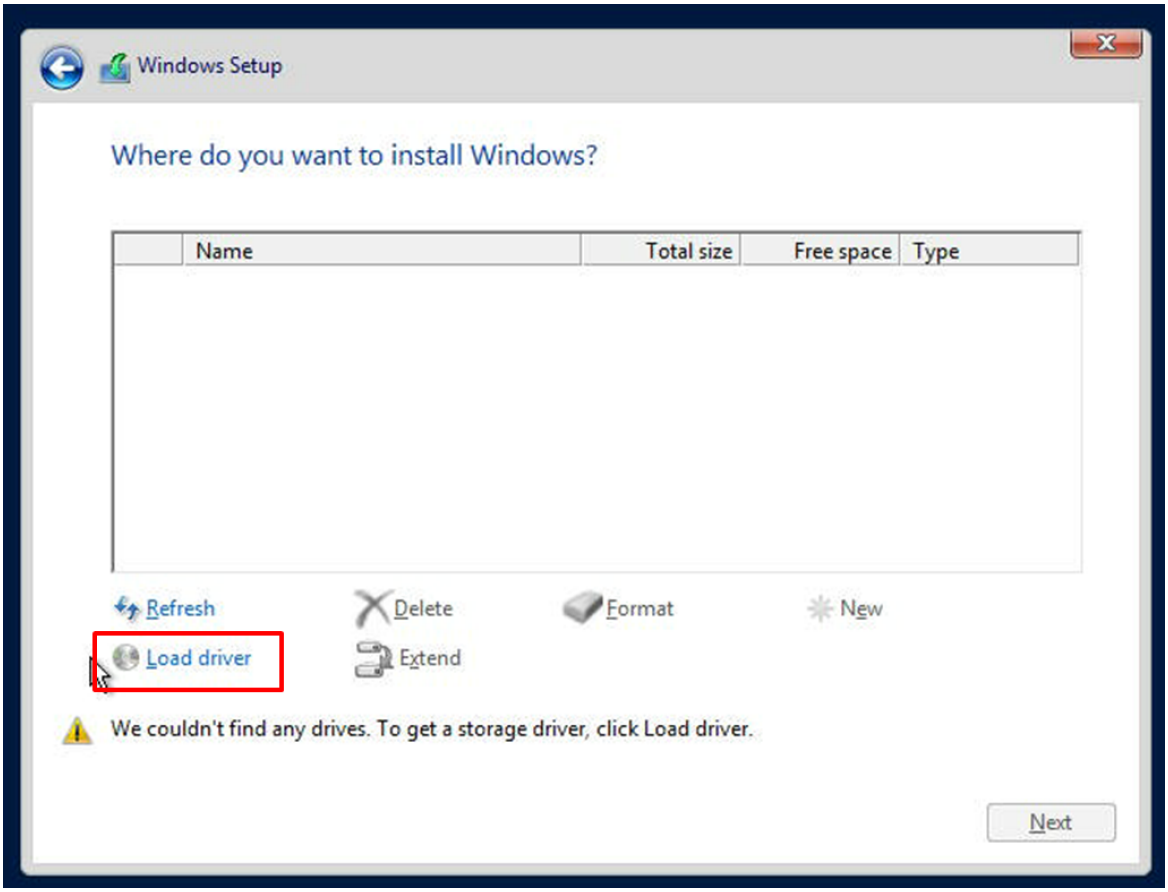



**Figure B-2. Loading the Driver Link**

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

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

# B.1 Driver Installation

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

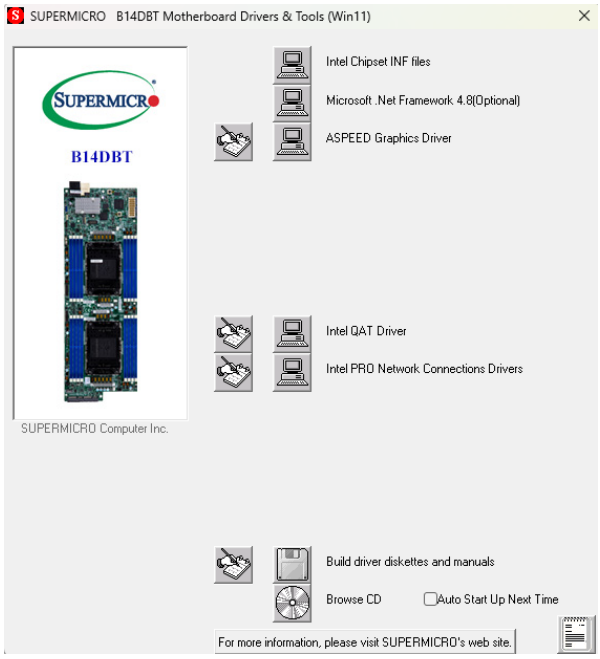



**Figure B-3. Driver Installation**

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

# BMC

The B14DBT motherboard provides remote access, monitoring, and management through the baseboard management controller (BMC) and other management controllers distributed among different system modules. There are several BIOS settings that are related to BMC. For general documentation and information on BMC, visit our website at the following page:

https://www.supermicro.com/en/solutions/management-software/bmc-resources

## BMC ADMIN User Password

For security, each system is assigned a unique default BMC password for the ADMIN user. The password can be found on a sticker on the motherboard and a sticker on the chassis, for Supermicro chassis. The sticker also displays the BMC MAC address. If necessary, the password can be reset using the Supermicro IPMICFG tool.




**Figure B-4. BMC Password Label**

## B.2 Logging into the BMC

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 which have the potential for bodily injury. Should you have questions or experience difficulty, contact Supermicro's Technical Support department for assistance. Only certified technicians should attempt to install or configure components.

Read this section in its entirety before installing or configuring components in the Supermicro B14DBT motherboard.

These warnings may also be found on our website at the following page:

https://www.supermicro.com/about/policies/safety_information.cfm

## Battery Handling



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

تحذير! يوجد خطر حدوث انفجار إذا تم استبدال البطارية بنوع غير صحيح. استبدل البطارية بنفس النوع أو نوع مكافئ موصى به من قبل الشركة المصنعة فقط. يجب التخلص من البطاريات المستخدمة وفقًا لإرشادات الجهة المصنعة.

警告！ 如果更换的电池类型不正确，有爆炸危险。更换电池时，请使用制造商推荐的相同或同等型号的电池。请按制造商的说明处理废旧电池。

警告！ 如果更換的電池類型不正確，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。

Advarsel! Der er risiko for eksplosion, hvis batteriet skiftes med et batteri af den forkerte type. Batteriet må kun skiftes med et batteri af samme eller tilsvarende type, der anbefales af producenten. Opbrugte batterier skal bortskaffes i henhold til vejledningerne fra producenten.

Waarschuwing! Er bestaat een explosiegevaar als de batterij wordt vervangen door een onjuist type. Vervang de batterij alleen door hetzelfde type of een soortgelijk type aanbevolen door de fabrikant. Verwijder gebruikte batterijen overeenkomstig de instructies van de fabrikant.

Varoitus! Väärän tyyppisen akun käyttö voi aiheuttaa räjähdysvaaran. Vaihda akku vain valmistajan suosittelemaan samaan tai vastaavaan tyyppiseen akkuun. Hävitä käytetyt paristot valmistajan ohjeiden mukaisesti.

Attention! Il y a un risque d'explosion si la batterie est remplacée par une d'un type incorrect. Remplacez la batterie uniquement par une d'un type identique ou équivalent recommandé par le fabricant. Éliminez les batteries usagées conformément aux instructions du fabricant.

Warnung! Es besteht Explosionsgefahr, wenn die Batterie durch einen falschen Typ ersetzt wird. Ersetzen Sie die Batterie ausschließlich durch denselben oder einen vom Hersteller empfohlenen gleichwertigen Typ. Entsorgen Sie gebrauchte Batterien gemäß den Anweisungen des Herstellers.

אזהרה! קיימת סכנת פיצוץ אם הסוללה תוחלף בסוללה מסוג שגוי. החלף את הסוללה רק בסוללה מאותו סוג או בסוללה מקבילה המומלצת על ידי היצרן. השלך סוללות משומשות בהתאם להוראות היצרן.

चेतावनी! यदि बैटरी को गलत प्रकार से बदला जाता है तो विस्फोट का जोखिम है। बैटरी को केवल निर्माता द्वारा अनुशंसित समान या समकक्ष प्रकार से ही बदलें। इस्तेमाल की गई बैटरियों का निपटान निर्माता के निर्देशों के अनुसार करें।

警告！ 電池を間違ったタイプに交換すると爆発する危険があります。交換する電池はメーカーが推奨するタイプ、または同等のものを使用してください。使用済み電池は、メーカーの指示に従って廃棄してください。

경고! 배터리를 잘못된 종류로 교체하면 폭발의 위험이 있습니다. 기존 배터리와 동일하거나 제조사에서 권장하는 동등한 종류의 배터리로만 교체해야 합니다. 제조사의 안내에 따라 사용된 배터리를 처리하여 주십시오.

Advarsel! Det er fare for eksplosjon hvis batteriet byttes ut med et av feil type. Batterier skal kun byttes ut med et av lik eller tilsvarende type, som anbefalt av produsenten. Kast brukte batterier i henhold til produsentens instruksjoner.

¡Advertencia! Existe riesgo de explosión si se sustituye la batería por una de tipo incorrecto. Reemplace la batería únicamente con el mismo tipo o uno equivalente recomendado por el fabricante. Deseche las baterías usadas de acuerdo con las instrucciones del fabricante.

Varning! Det finns risk för explosion om batteriet byts ut mot en felaktig typ. Byt endast ut batteriet mot ett batteri av samma eller likvärdig typ som rekommenderas av tillverkaren. Kassera förbrukade batterier i enlighet med tillverkarens anvisningar.

## Product Disposal



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

تحذير! يجب التخلص النهائي من هذا المنتج وفقًا لجميع القوانين واللوائح الوطنية.

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。

Advarsel! Dette produkt skal bortskaffes i henhold til alle nationale love og regler.

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

Varoitus! Tämän tuotteen lopullinen hävittäminen on suoritettava kaikkien kansallisten lakien ja määräysten mukaisesti.

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.

Warnung! Die endgültige Entsorgung dieses Produkts muss gemäß allen nationalen Gesetzen und Vorschriften erfolgen.

אזהרה! סילוק סופי של מוצר זה חייב להתבצע בהתאם לכל החוקים והתקנות הלאומיים.

चेतावनी! इस उत्पाद का अंतिम निपटान सभी राष्ट्रीय कानूनों और नियमों के अनुसार किया जाना चाहिए।

警告！ 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。

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

Advarsel! Når produktet til slutt skal kasseres, må det håndteres i henhold til alle nasjonale lover og forskrifter.

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

Varning! Slutgiltigt bortskaffande av denna produkt ska ske i enlighet med alla nationella lagar och förordningar.