



X13DDW-A

USER'S MANUAL

Revision 1.1

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

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

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

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

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

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



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 1.1

Release Date: February 06, 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 © 2025 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About This Manual

This manual is written for system integrators, IT technicians, and knowledgeable end users. It provides information for the installation and use of the X13DDW-A motherboard, which is intended for use in a Supermicro proprietary server.

About This Motherboard

The Supermicro X13DDW-A supports dual 4th/5th Gen Intel® Xeon® Scalable Processors (Socket-E LGA 4677) with four UPIs (20 GT/s max.) and a thermal design power (TDP) of up to 350 W. Built with the Intel C741 chipset, the X13DDW-A supports up to 4 TB 3DS RDIMM/ RDIMM DDR5 ECC memory with speeds up to 5600 MT/s in 16 DIMM slots. This motherboard features superior IO flexibility with support for six PCIe 5.0 x16 riser cards, two PCIe 5.0 x16 advanced I/O modules (AIOM) for OCP 3.0-compliant cards, 12 SATA 3.0 ports, four MCIO x8 and eight MCIO x4 connectors for 12 NVMe device support (refer to Note 1), two USB 3.1 rear ports, and a dedicated BMC LAN/VGA connector. It also offers the most advanced data protection features with hardware Root of Trust (RoT) and Trusted Platform Module (TPM) support (refer to Note 2). The X13DDW-A is optimized for use in WI/O servers with High Performance Computing (HPC) and networking support and is ideal for enterprise applications and data center deployments. For processor/memory updates, refer to our website at <http://www.supermicro.com/products/>.



Note 1: This motherboard supports eight 5.0 x4, four 5.0 x8 MCIO NVMe connections, and up to 12 NVMe slots if an S12 (12" x 3.5") backplane is used.

Note 2: Memory speed/capacity support depends on the processors used in the system. The 4th Gen Intel Xeon Scalable processors support DDR5 memory with speeds up to 4800 MT/s (or up to 4400 MT/s in the 32-DIMM configuration). The 5th Gen Intel Xeon Scalable processors support DDR5 memory with speeds up to 5600 MT/s (or up to 4400 MT/s in the 32-DIMM configuration).

Note 3: For TPM support, an optional part is needed. Contact Supermicro Technical Support for more information.

Conventions Used in the Manual

Special attention should be given to the following symbols for proper installation and to avoid damaging the components or causing injuries to yourself.



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



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



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



Note: Additional Information given to provide information for proper system setup.

Contacting Supermicro

Headquarters

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

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: Marketing@supermicro.com (General Information)
Sales-USA@supermicro.com (Sales Inquiry: Non-Government)
Government_Sales-USA@supermicro.com (Sales Inquiry: Government)
Support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)

Website: www.supermicro.com

Europe

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

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

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

Website: www.supermicro.nl

Asia-Pacific

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

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

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

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Overview.....	8
1.2 Processor and Chipset Support.....	18
1.3 Special Features	19
1.4 System Health Monitoring	19
1.5 ACPI Features.....	19
1.6 Power Supply	20
1.7 Serial Port.....	20

Chapter 2 Installation

2.1 Static-Sensitive Devices.....	21
2.2 Processor and Heatsink Installation.....	22
2.3 Motherboard Installation.....	54
2.4 Memory Support and Installation	56
2.5 I/O Panel	62
2.6 Front Control Panels	69
2.7 Connectors and Headers	86
2.8 Jumper Settings	98
2.9 LED Indicators.....	101

Chapter 3 Troubleshooting

3.1 Troubleshooting Procedures	106
3.2 Technical Support Procedures	109
3.3 Frequently Asked Questions	110
3.4 Battery Removal and Installation	111
3.5 Returning Merchandise for Service.....	112

Chapter 4 UEFI BIOS

4.1 Introduction.....	113
4.2 Main Setup	114
4.3 Advanced Setup Configurations.....	116
4.4 Event Logs	185
4.5 BMC.....	187
4.6 Security.....	191
4.7 Boot	201

4.8 Save & Exit.....	204
----------------------	-----

Appendix A BIOS POST Codes

A.1 BIOS POST Codes.....	206
--------------------------	-----

Appendix B Software

B.1 Microsoft Windows OS Installation.....	207
--	-----

B.2 Driver Installation.....	209
------------------------------	-----

B.3 BMC.....	210
--------------	-----

B.4 Logging into the Baseboard Management Controller (BMC).....	210
---	-----

Appendix C Standardized Warning Statements

Chapter 1

Introduction

1.1 Overview

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

This chapter provides detailed information on the components installed on your system board and the features supported by your system.

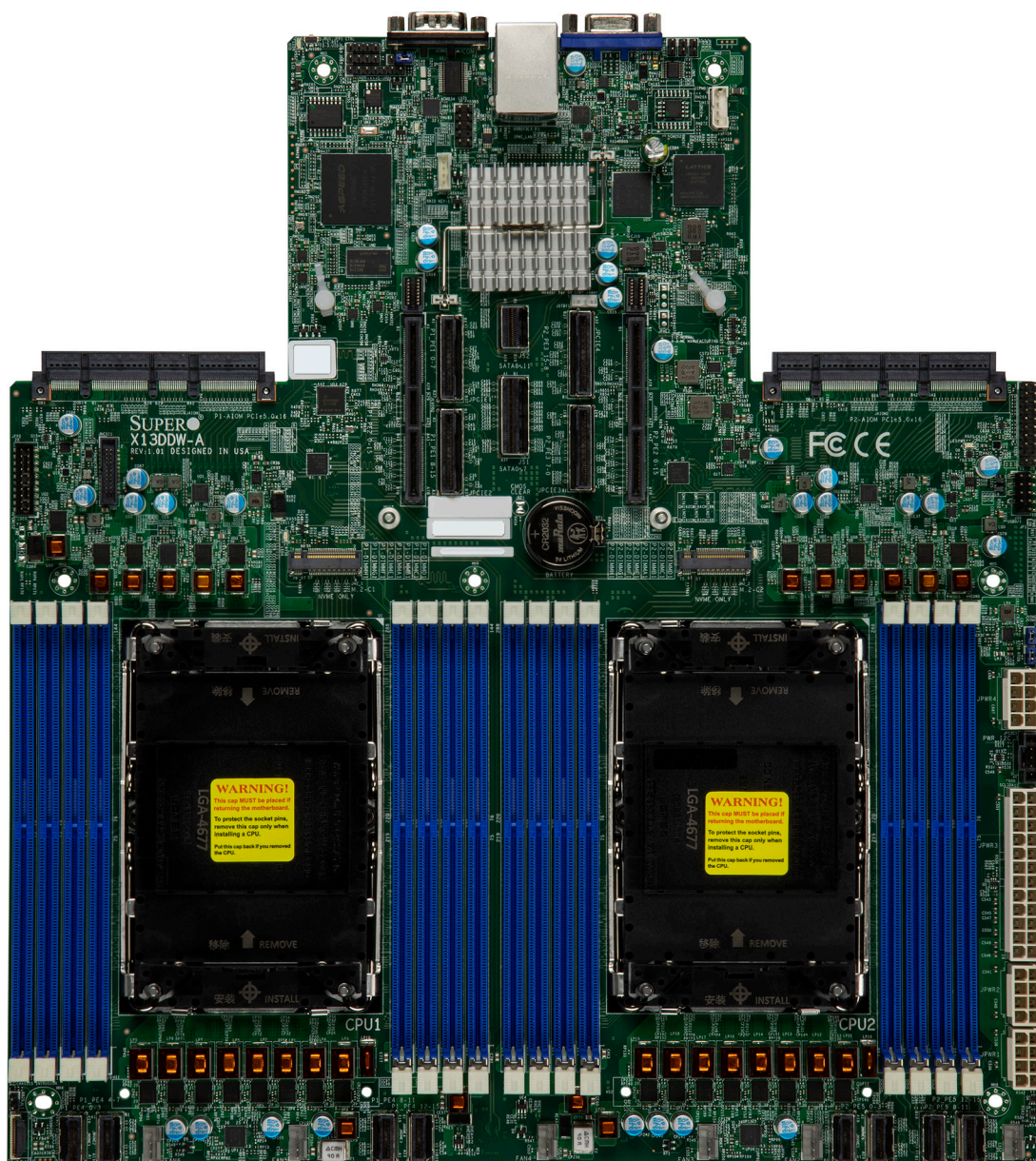
Important Links

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

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

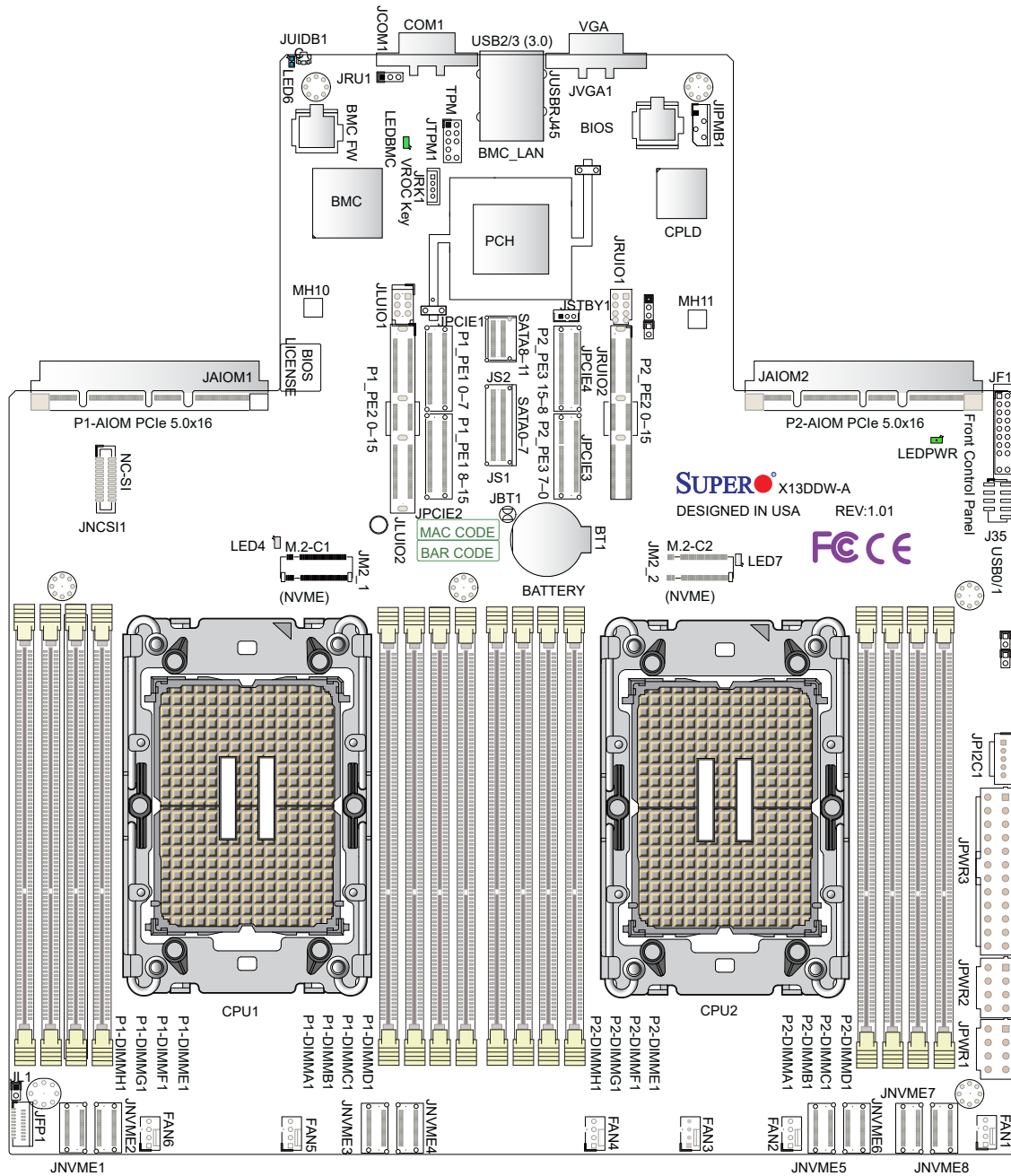
This manual may be periodically updated without notice. Check the Supermicro website for possible updates to the manual revision level.

Figure 1-1: X13DDW-A 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: X13DDW-A Motherboard Layout
(not drawn to scale)



Note: Components not documented are for internal testing only.

Quick Reference

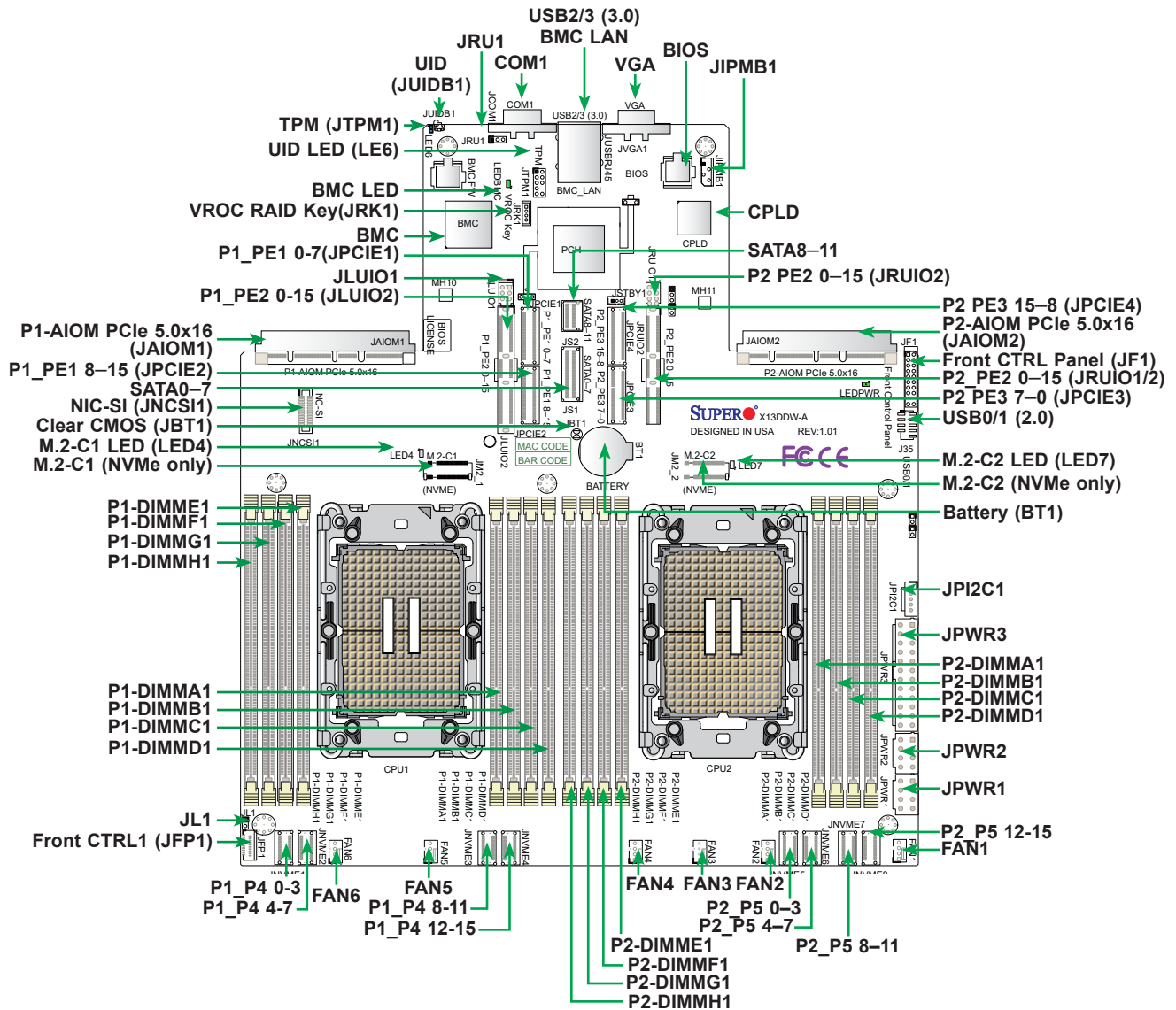


Figure 1-3: Quick Reference Layout

 Notes:

- See [Chapter 2](#) for detailed information on jumpers, I/O ports, and JF1 front panel connections.
- "■" indicates the location of Pin 1.
- Components that are not documented in this manual are for internal testing only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. Do not install the onboard battery upside down to avoid a possible explosion.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JRU1	Front UID Button Select	Pins 2–3 (Reset Pin 2 of JFP1 for Front UID Use)
LED	Description	Status
LED6 (UID-LED)	Unit Identifier (UID) LED	Solid Blue: Unit Identified
LED4	M.2-C1 LED	On: M.2-C1 Active
LED7	M.2-C2 LED	On: M.2-C2 Active
LEDBMC	BMC Heartbeat LED	Blinking Green: BMC Normal (Active) Solid Green: (During BMC Reset or during a Cold Reboot)
LEDPWR	Power LED	LED On: Onboard Power On
Connector	Description	
Battery (BT1)	Onboard Battery	
COM1 (JCOM1)	COM Port 1 on the Rear I/O Panel	
FAN1–6	4-Pin Cooling Fan Headers (FAN1—FAN 6)	
IPMI_LAN (JUSBRJ45)	BMC LAN Connector on the Rear I/O Panel	
JF1	Front Control Panel Header	
JFP1	Front Control Panel Header	
JIPMB1	4-Pin BMC SMBus Header	
JL1	Chassis Intrusion header	
JNCSI1	Network Controller Sideband Interface (NC-SI) Connector	
JPWR1/JPWR2	8-Pin Power Connectors	
JPWR3	24-Pin Power Connector	
JSTBY1	5 V Standby Power Header	
JTPM1	Trusted Platform Module/Port 80 Connector	
JUIDB1	Unit Identifier (UID) Switch/Button	
M.2-C1/M.2-C2 (JM2_1/JM2_2)	M.2 Slots for NVMe Use Only (with Support of M-Key 2280)	
MH10/MH11	Mounting Holes for M.2 Slots (MH10 for M.2-C1, MH11 for M.2-C2)	
P1-AIOM PCIe 5.0 x16 (JAIOM1)	SupermicroAdvanced Input/Output Module (AIOM) PCIe 5.0 x16 Rear I/O Connector Supported by CPU1	
P2-AIOM PCIe 5.0 x16 (JAIOM2)	Supermicro Advanced Input/Output Module (AIOM) PCIe 5.0 x16 Rear I/O Connector Supported by CPU2	



Note 1: For details on how to configure Network Interface Card (NIC) settings, refer to the Network Interface Card Configuration User's Guide posted on our website under the link: <https://www.supermicro.com/support/manuals/>.

Note 2: For TPM support, an optional part is needed. Contact Supermicro Technical Support for more information.

P1_PE2 0–15 (JLUIO1/ JLUIO2)	PCIe 5.0 x16 Left Add-On Card Slot Supported by CPU1
P2_PE2 0–15 (JRUIO1/ JRUIO2)	PCIe 5.0 x16 Right Add-On Card Slot Supported by CPU2
P1_PE1 0–7 (JPCIE1)	PCIe 5.0 x8 MCIO Connector Supported by CPU1
P1_PE1 8–15 (JPCIE2)	PCIe 5.0 x8 MCIO Connector Supported by CPU1
P2_PE3 7–0 (JPCIE3)	PCIe 5.0 x8 MCIO Connector Supported by CPU2
P2_PE3 15–8 (JPCIE4)	PCIe 5.0 x8 MCIO Connector Supported by CPU2
P1_PE4 0–3 (JNVME1)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU1
P1_PE4 4–7 (JNVME2)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU1
P1_PE4 8–11 (JNVME3)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU1
P1_PE4 12–15 (JNVME4)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU1
P2_PE5 0–3 (JNVME5)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU2
P2_PE5 4–7 (JNVME6)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU2
P2_PE5 8–11 (JNVME7)	PCIe 5.0 x4 MCIO Connector Used for NVMe Devices Supported by CPU2
P2_PE5 12–15 (JNVME8)	PCIe 5.0 x4 MCIO Connector used for NVMe Devices Supported by CPU2
PWR I2C (JPI2C1)	Power I ² C System Management Bus (SMBus) Header
SATA 0–7 (JS1)	SATA 0–7 Ports Supported by PCH
SATA 8–11 (JS2)	SATA 8–11 Ports Supported by PCH
USB 0/1 (USB 2.0) (J35)	USB 2.0 Header with Support of USB Port1/USB Port2
USB 2/3 (USB 3.0) (JUSBRJ45)	Rear USB 3.0 Connector with Support for Two USB 3.0 Connections (USB Port2/ USB Port3)
VGA (JVGA1)	Rear VGA Connector
VROC RAID Key (JRK1)	Intel VROC RAID Key Header for NVMe RAID Support



Note 1: This motherboard supports eight 5.0 x4, four 5.0 x8 MCIO NVMe connections, and it also supports up to 12 NVMe devices if an S12 (12" x 3.5") backplane is used.

Note 2: 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 link: <https://www.supermicro.com/support/manuals/>.

Memory Slots

This motherboard supports up to 4 TB of DDR5 memory in 16 DIMM slots. Refer to the layout drawing for the locations of the DIMM slots:

DIMM Slot Locations	
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

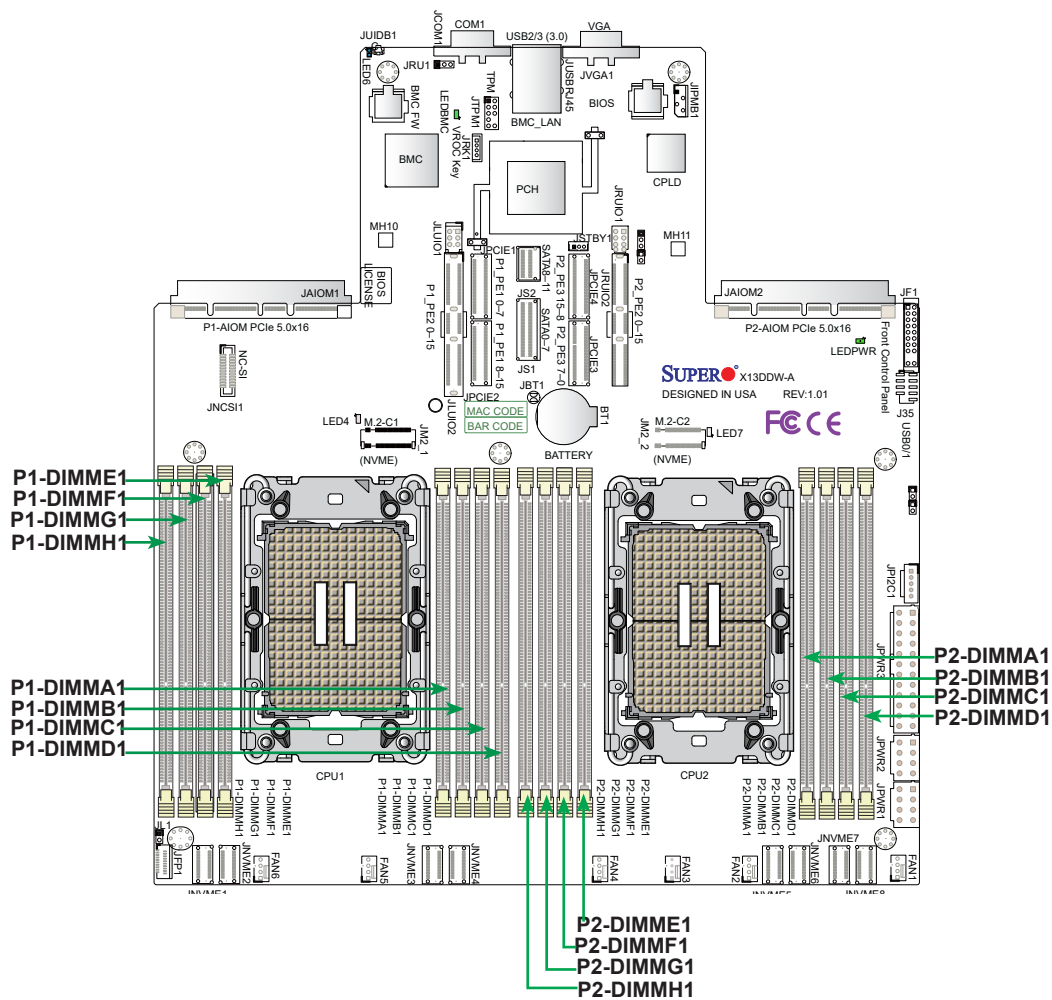


Figure 1-4: Memory Slot Locations

Motherboard Features

Motherboard Features	
CPU	Supports dual 4th/5th Gen Intel Xeon Scalable Processors (Socket-E LGA 4677) with four UPIs (20 GT/s max.) and a Thermal Design Power (TDP) of up to 350W  Note: SP XCC and SP MCC SKUs are supported.
Memory	- Supports up to 4 TB 3DS RDIMM/RDIMM DDR5 (288-pin) ECC memory - Memory speeds of up to 4800 MT/s (DDR5-4400 MT/s when fully populated) in 16 memory slots (4th Generation Intel Xeon) - Memory speeds of up to 5600 MT/s (DDR5-4400 MT/s when fully populated) in 16 memory slots (5th Generation Intel Xeon)  Note: Memory speed and capacity support depend on the processors used in the system.
DIMM Size	Up to 256 GB  Note: For the latest CPU/memory updates, refer to our website at http://www.supermicro.com/products/motherboard.
Chipset	Intel PCH C741
Expansion Slots	- Six PCIe 5.0 x16 riser cards supported - Two NVMe M.2 ports from CPU1 (with M-Key 2280 support) - Flexible Advanced I/O Module (AIOM) for (OCP 3.0 compatible) cards for Ethernet connections - Two AIOM (OCP 3.0 compatible) x16 slots - Two USB 3.0 rear I/O connectors - Four MCIO 5.0 x8 and eight MCIO 5.0 x4 connectors for 12 NVMe device support (*Note below) 12 SATA 3.0 connections supported (RAID 0, 1, 5, 10) - One Trusted Platform Module (TPM) slot  Note: This motherboard supports eight x4, four x8 MCIO NVMe connections, and it also supports up to 12 NVMe slots if an S12 (12" x 3.5") backplane is used.
Baseboard Management Controller (BMC)/Network	- ASPEED AST2600 BMC - One dedicated BMC LAN/VGA (via AST2600)
Graphics	Graphics controller and VGA support via ASPEED AST2600 BMC
I/O Devices	- One VGA connector (JVGA1) for VGA/video display on the rear I/O panel - Flexible AIOM (OCP 3.0 compatible) card for Ethernet connection support
Peripheral Devices	- One dedicated USB 3.0 connector via BMC for two USB 3.0 connections (USB 2/3) on the rear I/O panel - One USB 2.0 header (J35) with support of two USB 2.0 ports (USB 0/1) for front access

BIOS

- AMI SPI BIOS
- Super Flash, EFI GUI, SPI dual/quad speed control, riser card auto detection support, IPMIView, SMCIPMITOOL, IPMI CFG, redundant power supply unit detection, SPM, SUM-OOB/InBand

Power Management

- ACPI power management and power supply monitoring
- S1 and S5 support
- Power button override mechanism
- Power-on mode for AC power recovery
- Wake-on-LAN

System Health Monitoring

- Onboard voltage monitoring for +12 V, +5 V/+5 V standby, +3.3 V, and +3.3 V standby, BMC, PCH, and CPU VRM power
- Onboard temperature monitoring for system, peripheral, CPU, memory, PCH, AOC, AIOM, and M.2
- Eight CPU switch phase voltage regulator
- CPU thermal trip support
- Platform Environment Control Interface (PECI)

Fan Control

- Fan status monitoring via BMC health monitoring
- Low noise fan speed control
- Six 4-pin proprietary fan headers

System Management

- SuperDoctor® 5 and SD3 (for Windows OS)
- Chassis intrusion header and detection
- Server platform service

Firmware Integrity/System Security

- Trusted Platform Module (TPM) support
- Root of Trust (RoT) support to protect firmware security by detecting critical data corruption and restoring platform integrity

LED Indicators

- Power LED
- UID LED
- LAN activity LED
- BMC Heartbeat LED
- M.2 LED indicators

Dimensions

- Supermicro proprietary 13.40" x 12.30" (340.36 mm x 312.42 mm) (L x W)



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

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

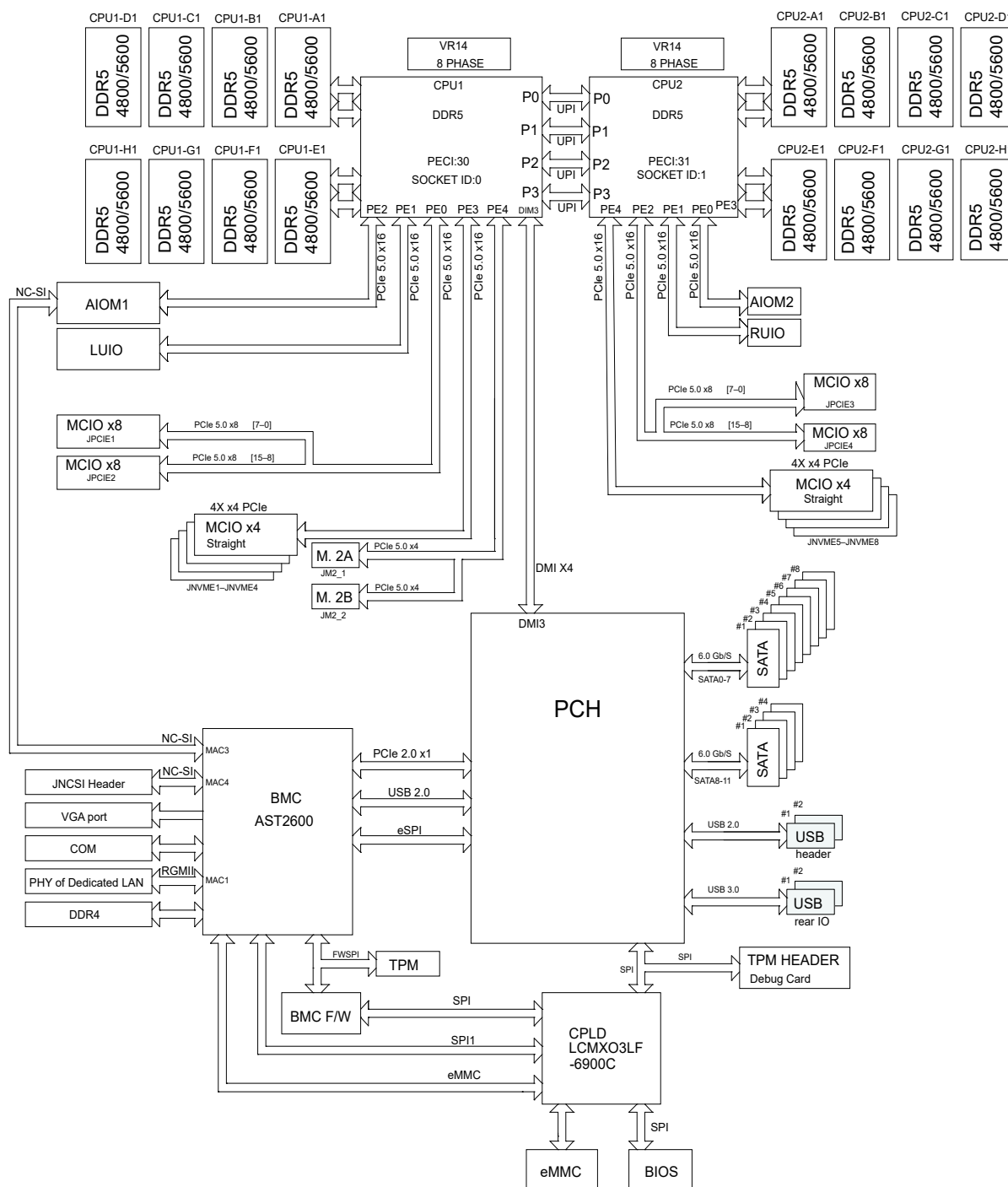


Figure 1-5: System Block Diagram

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

1.2 Processor and Chipset Support

Built upon the functionality and capability of 4th/5th Gen Intel Xeon Scalable Processors (Socket-E) and the Intel C741 chipset, the X13DDW-A motherboard offers critical, pivotal technological breakthroughs that unleash unprecedented computing capabilities. It also provides a scalable platform optimized for applications used in Artificial Intelligence (AI) Acceleration, Deep Learning Boost, Network Interconnectivity, and Platform Manageability technologies. The key features supported by the platform include the following:

Processor Features Supported

- Increased, scalable performance with substantial advancements, including UPI speed improvement, memory speed/capacity/utilization enhancement, hardware-based security innovations for virtualization, and platform interconnectivity optimization
- Integrated accelerators optimized for workload enhancement, including Advanced Matrix Extensions (IntelAMX), In-Memory Analytic Accelerator (IAX), and Data Streaming Accelerator (IntelDSA).
- Breakthroughs in memory and I/O support, including DDR5 (4800 MT/s max.), PCIe 5.0 (80 lanes max.), and CXL 1.1 (four devices per CPU)
- Increased operational and performance efficiency with substantial enhancements in virtualization, network security, and both telemetry and power management
- Integrated AI accelerators with support of 3rd Gen Intel® Deep Learning Boost and new Tile Matrix Multiply (AMX/MUL)
- Enhanced Intel Security Boost Software Guard Extensions with Integrity Platform Firmware Resilience support
- Intel Ultra Path Interconnect (Intel UPI) up to four links per processor at 20 GT/s
- New Computer Express Link (CXL) and Intel Speed Select Technology
- CPU with 52 physical address/57 virtual address support
- Intel Trusted Domain Extensions (TDX) support (5th Gen Xeon Scalable processors only)

PCH Features Supported

- Flexible IO at 20 lanes for PCIe 3.0, 1G Ethernet in PCH for manageability, and four DMIs at PCIe 3.0

1.3 Special Features

Recovery from AC Power Loss

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

1.4 System Health Monitoring

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the BMC interface. Whenever the temperature of the CPU or the system exceeds Supermicro's pre-defined threshold, the system and CPU cooling fan speeds will increase to prevent the CPU or 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 appropriate Windows operating systems. For detailed information regarding OS support, refer to the Supermicro website.

1.6 Power Supply

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

The X13DDW-A motherboard accommodates two 8-pin power connectors (JPWR1/JPWR2) and a 24-pin power connector (JPWR3). Although most power supplies generally meet the specifications required by the CPU, some are inadequate. All these power connections are also required to ensure an adequate power supply to the system.



Warning! To avoid damaging the power supply or the motherboard, be sure to use a power supply that accommodates two 8-pin power connectors (JPWR1/JPWR2) and a 24-pin power connector (JPWR3) for your system. Failure to do so may void the manufacturer's 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. For more information, refer to the website at <http://www.ssiforum.org/>.

1.7 Serial Port

The X13DDW-A motherboard supports one serial port on the rear I/O panel. COM Port 1 can be used for input/output. The UART provides legacy speeds with a baud rate of up to 115.2 Kbps.

Chapter 2

Installation

2.1 Static-Sensitive Devices

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

Precautions

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

Unpacking

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

2.2 Processor and Heatsink Installation

The processor (CPU) and processor carrier should be assembled together first to form the processor carrier assembly. This assembly will then be attached to the heatsink to form the processor heatsink module (PHM) before being installed into the CPU socket. Before installation, be sure to perform the following steps:

- Carefully follow the instructions given on the previous page to avoid ESD-related damages.
- Unplug the AC power cords from all power supplies after shutting down the system.
- Check that the plastic protective cover is on the CPU socket, and none of the socket pins are bent. If they are, contact your retailer.
- When installing the processor and heatsink, ensure a torque driver set to the correct force is used for each screw.
- When handling the processor, avoid touching or placing direct pressure on the LGA lands (gold contacts). Improper installation or socket misalignment can cause serious damage to the processor or CPU socket, which may require manufacturer repairs.
- Thermal grease is pre-applied on a new heatsink. No additional thermal grease is needed.
- Refer to the Supermicro website for updates on processor and memory support.
- All graphics in this manual are for illustrative purposes only. Your components may look different.



Note: The installation process is the same for both 4th/5th Gen Intel Xeon Scalable processors. Use the 4th Gen Intel Xeon Scalable processor installation process as a reference.

The 4th/5th Gen Intel Xeon Scalable Processor (for SP XCC and SP MCC Series only)

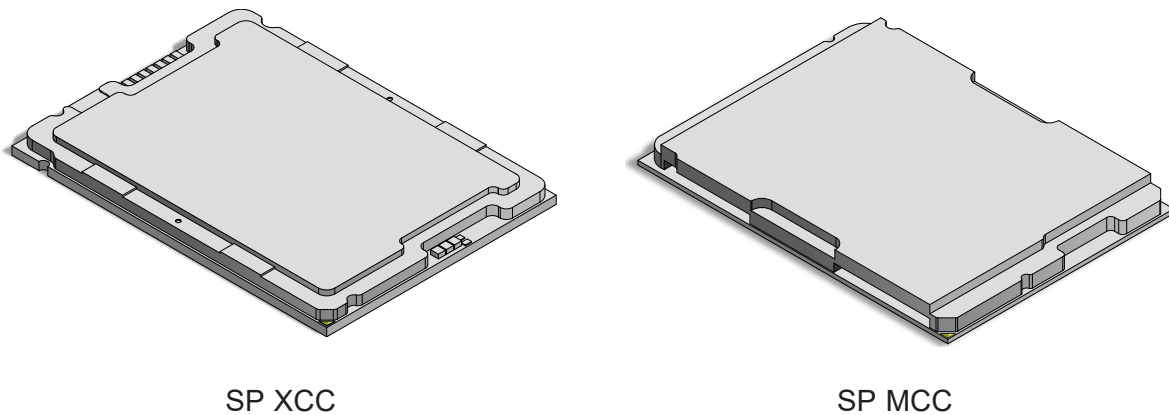


Figure 2-1: Top View of Processors

 **Note:** This motherboard supports two CPU SKUs: SP XCC Series and SP MCC Series. Each CPU SKU supports a specific carrier; the SP XCC CPU supports Carrier E1A, and the SP MCC supports Carrier E1B.

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

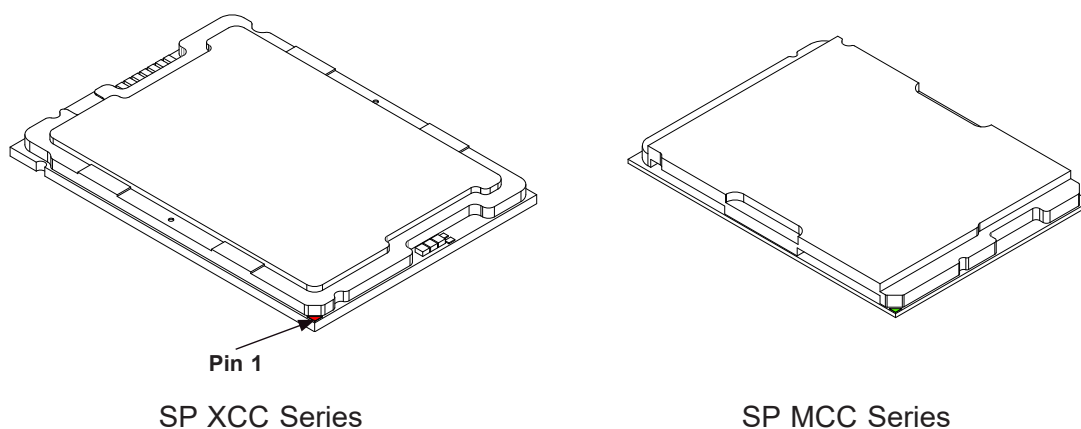


Figure 2-2: Top View of Processors

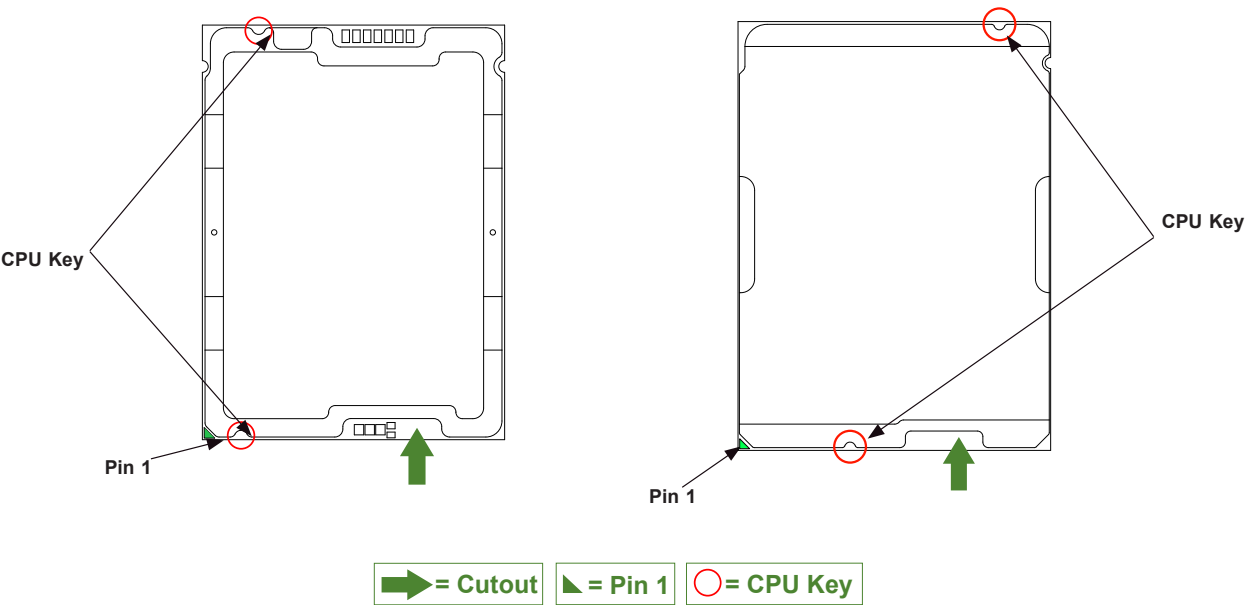


Figure 2-3: Top View of Processors

2. The Processor Carrier

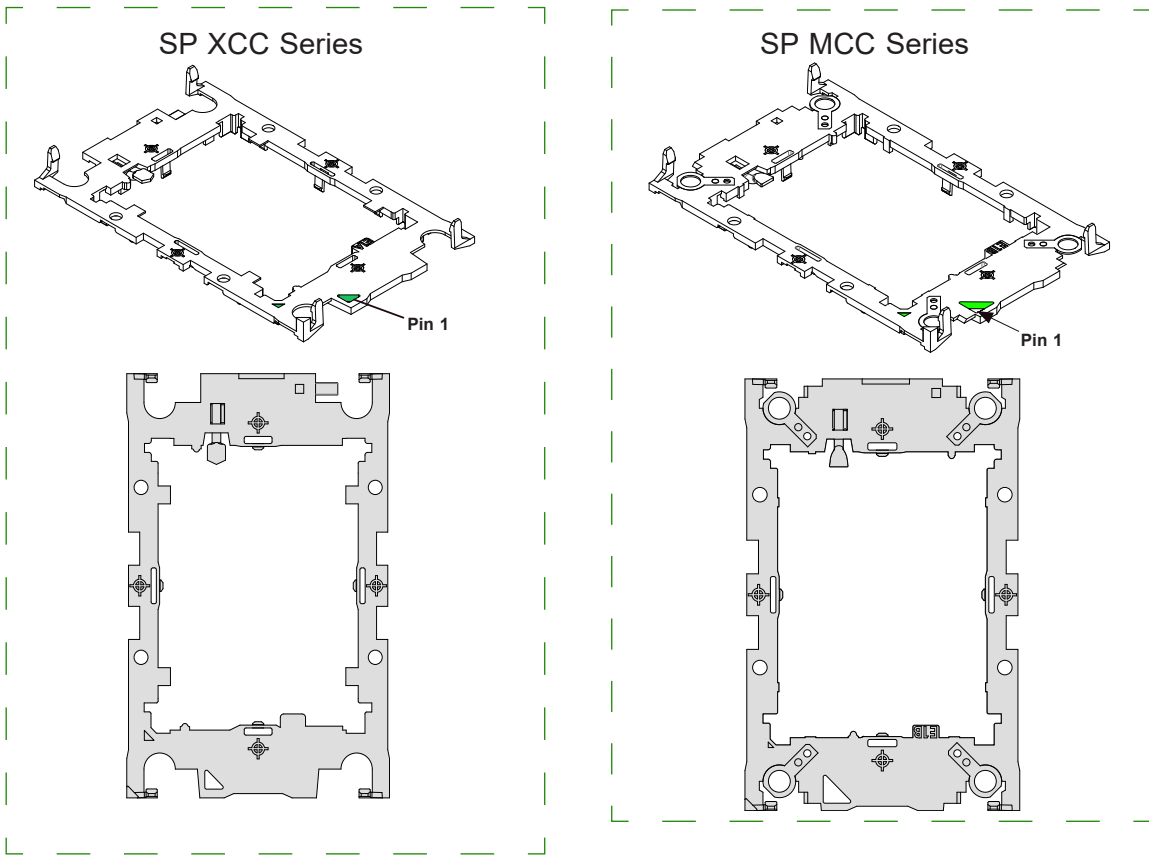


Figure 2-4: Top View of Carriers

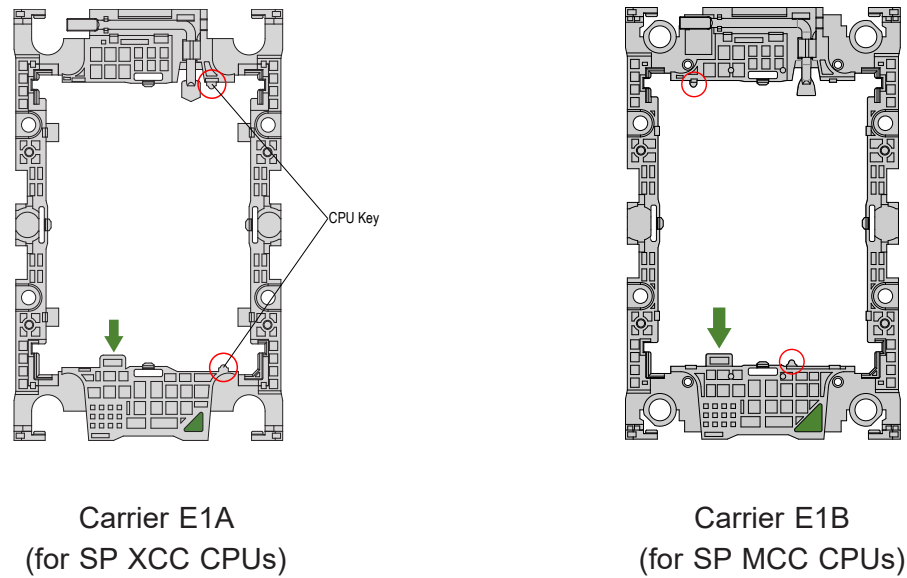


Figure 2-5: Bottom View of Carriers

Note 1: The 4th/5th Gen Intel Xeon Scalable Processor comes with three CPU SKUs: SP XCC, Max Series (HBM), and SP MCC. Each CPU SKU supports a specific carrier. The SP XCC CPU supports Carrier E1A, Max Series (HBM) CPU supports Carrier E1C, and the SP MCC supports Carrier E1B.

Note 2: Be sure to use processors of the same SKU on this motherboard.

3. Heatsink

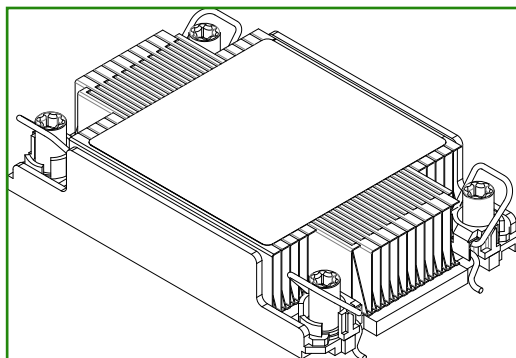


Figure 2-6: 1U Heatsink

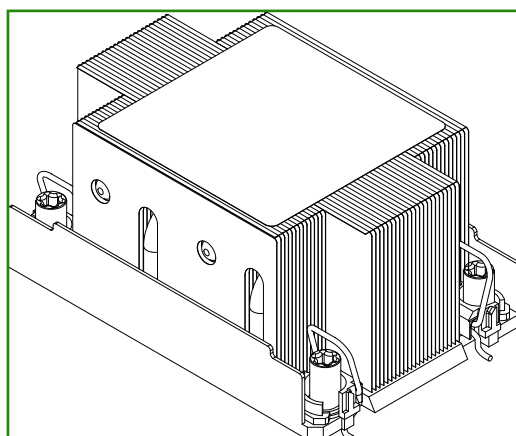


Figure 2-7: 2U Heatsink

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

Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

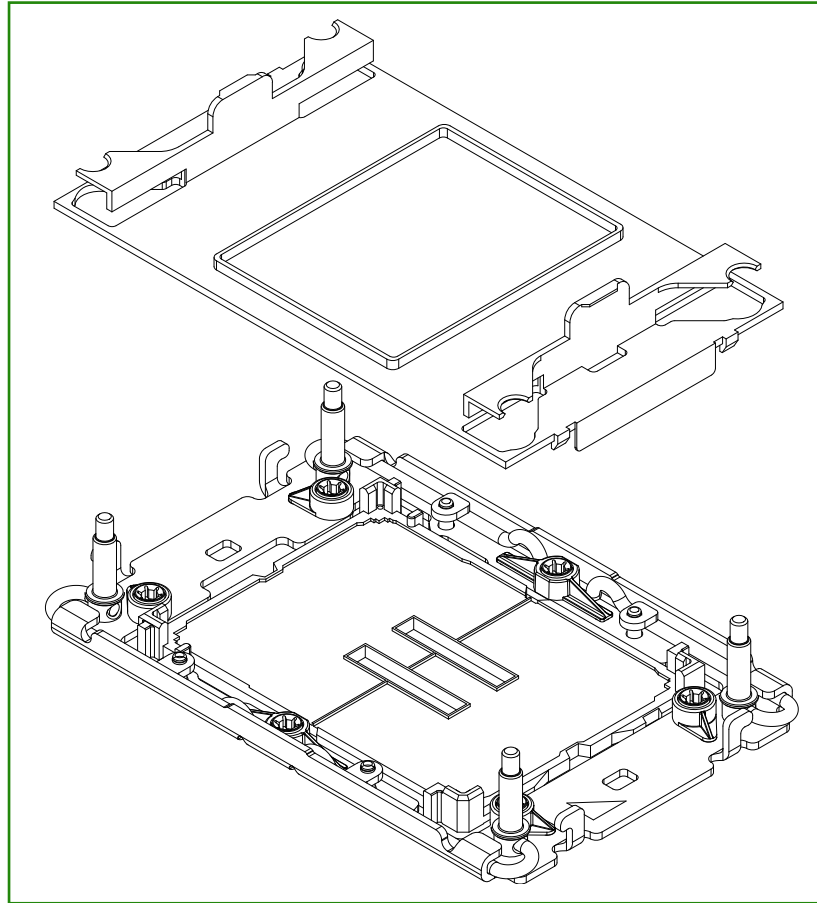


Figure 2-8: CPU Socket and Plastic Protective Cover

Overview of the Processor Carrier Assembly

The processor carrier assembly contains a 4th/5th Gen Intel Xeon Scalable processor and a processor carrier. Carefully follow the instructions given in the installation section to place a processor into the carrier to create a processor carrier. The processor carrier assembly includes a processor and a carrier, as shown:

1. The 4th/5th Gen Intel Xeon Scalable Processor (SP XCC and MCC Series only)

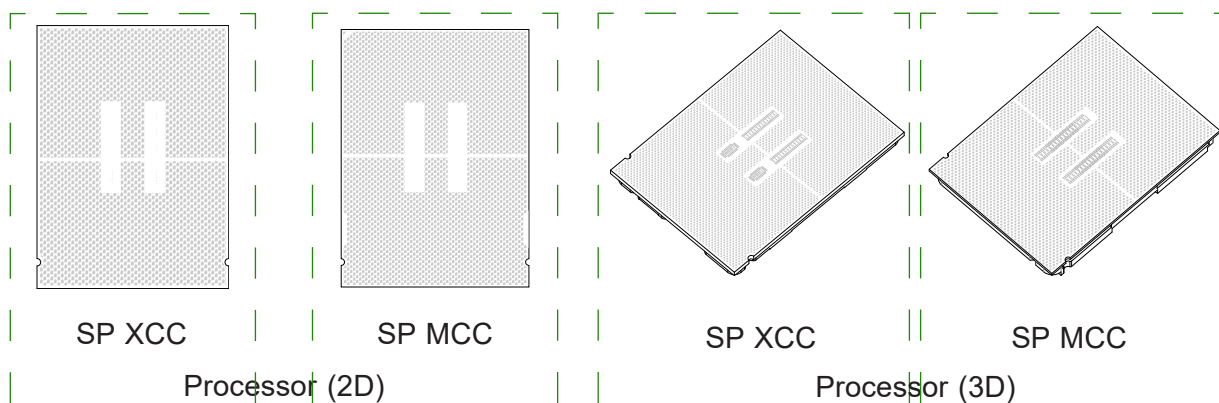


Figure 2-9: Intel Processor Component Side

2. Processor Carrier

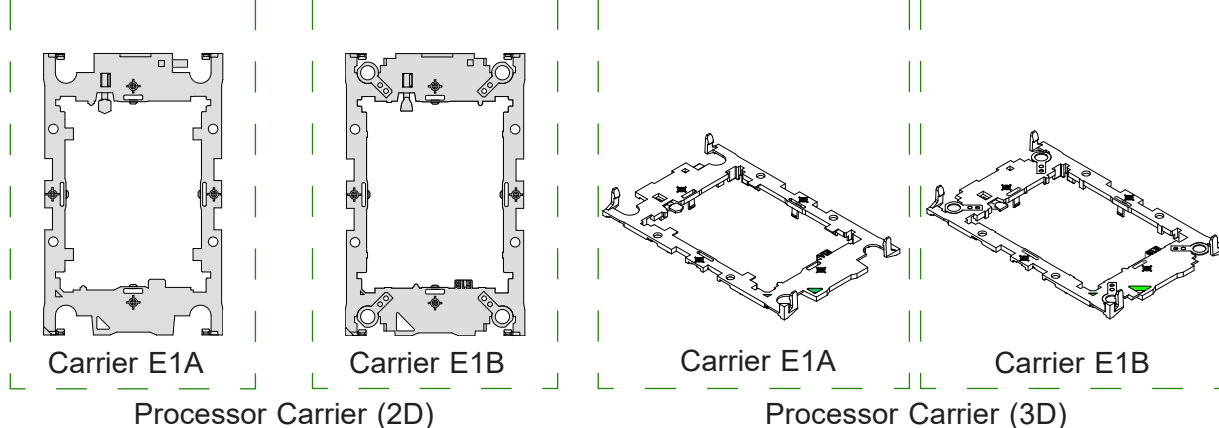


Figure 2-10: Intel Processor Carrier Top View



3. Processor Carrier Assembly

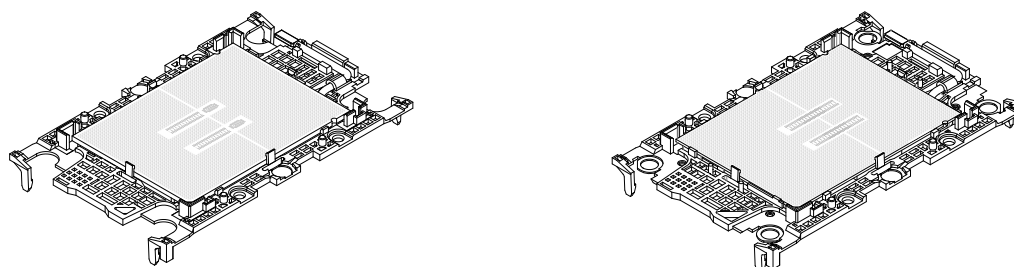


Figure 2-11: Processor Seated inside the Carrier

Overview of the Processor Heatsink Module (PHM)

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

1. Illustrations of 1U Heatsink and 2U Heatsink for SP XCC CPU

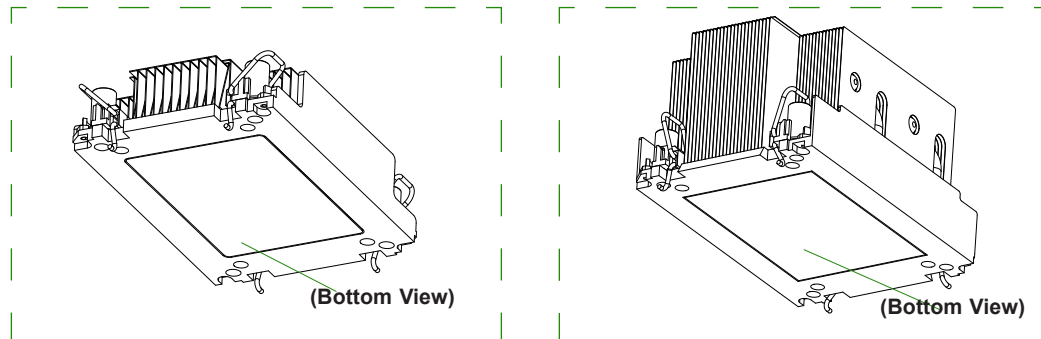


Figure 2-12: Heatsinks' Bottom View

2. Processor Carrier E1A

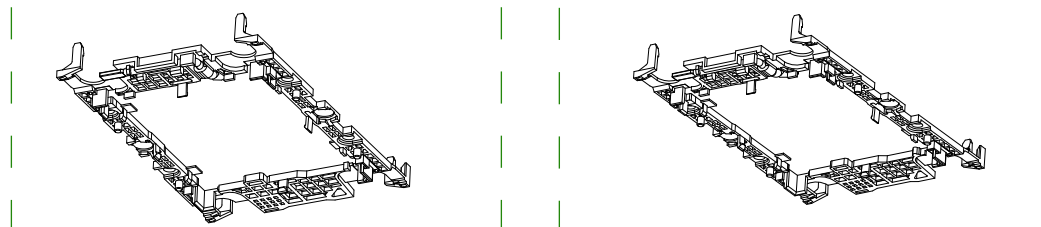
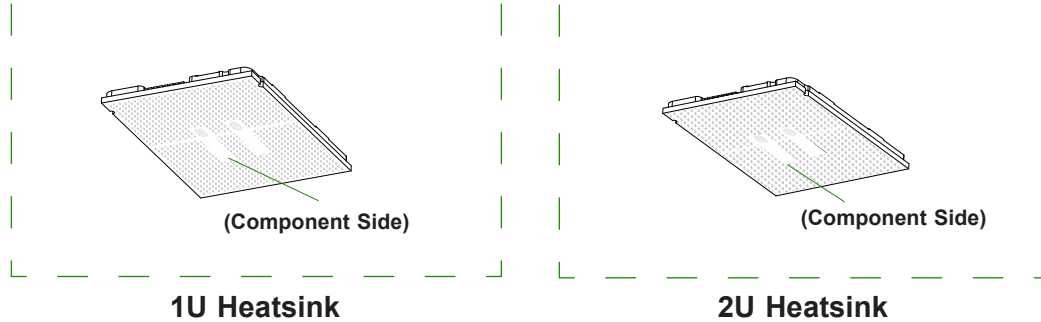


Figure 2-13: Processor Carrier View

3. The 4th/5th Gen Intel Xeon Scalable Processor (SP XCC Series)



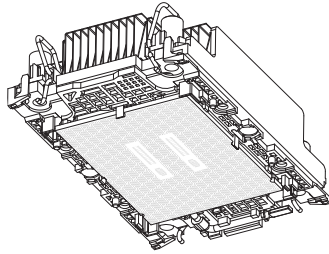
1U Heatsink

2U Heatsink

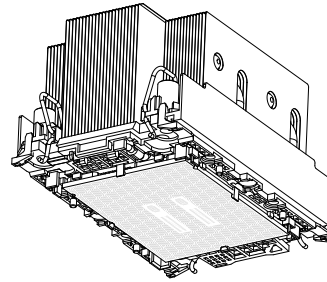
Figure 2-14: Processor Component View



4. Processor Heatsink Module (PHM)



1U Heatsink



2U Heatsink

Figure 2-15: Bottom View

1. Heatsink (1U Heatsink and 2U Heatsink for SP MCC CPU Illustration)

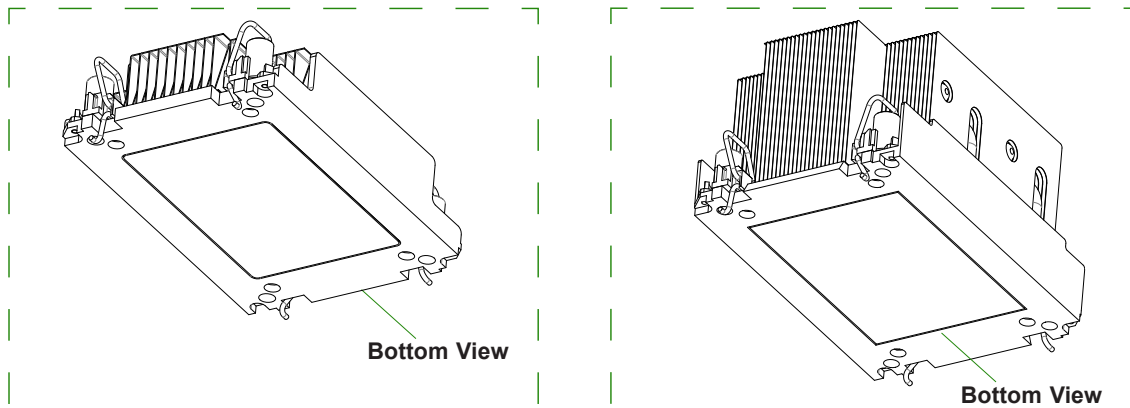
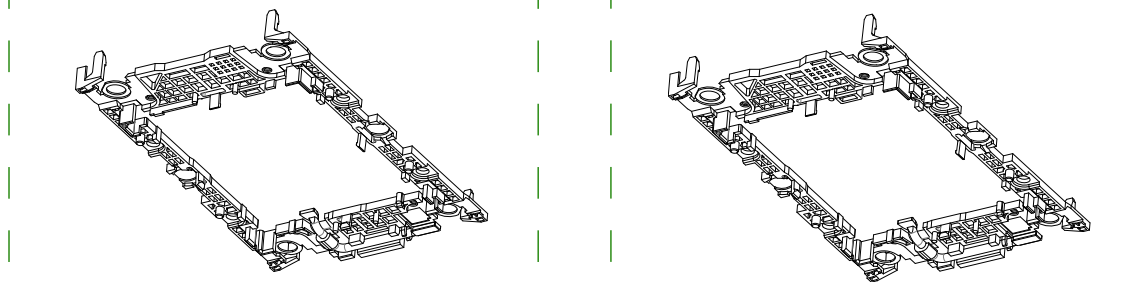


Figure 2-16: Bottom View of Heatsinks

2. Processor Carrier E1B



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

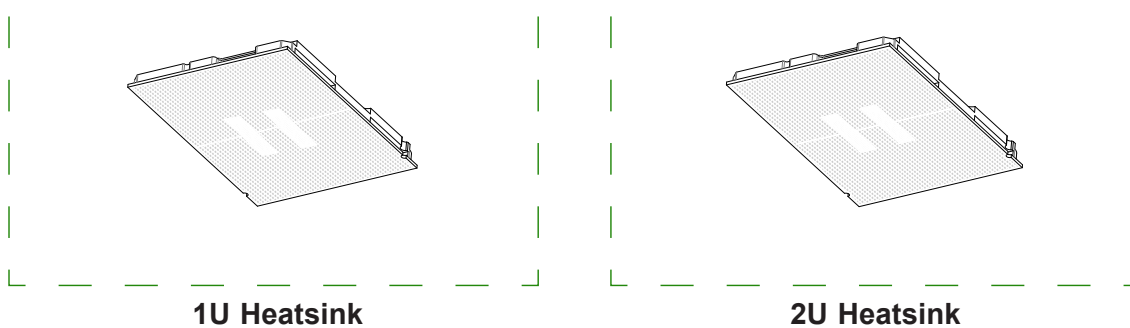
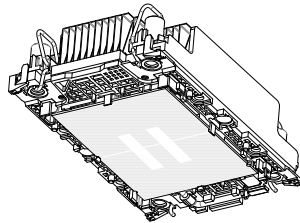


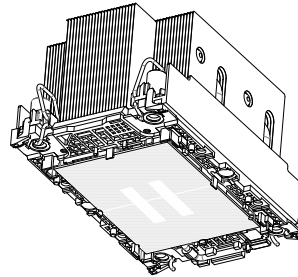
Figure 2-18: Processors Component Side View



4. Processor Heatsink Module (PHM)



1U Heatsink



2U Heatsink

Figure 2-19: View of Processor Heatsink Modules

Creating the Processor Carrier Assembly

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

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

To create the processor carrier assembly, follow the steps:

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

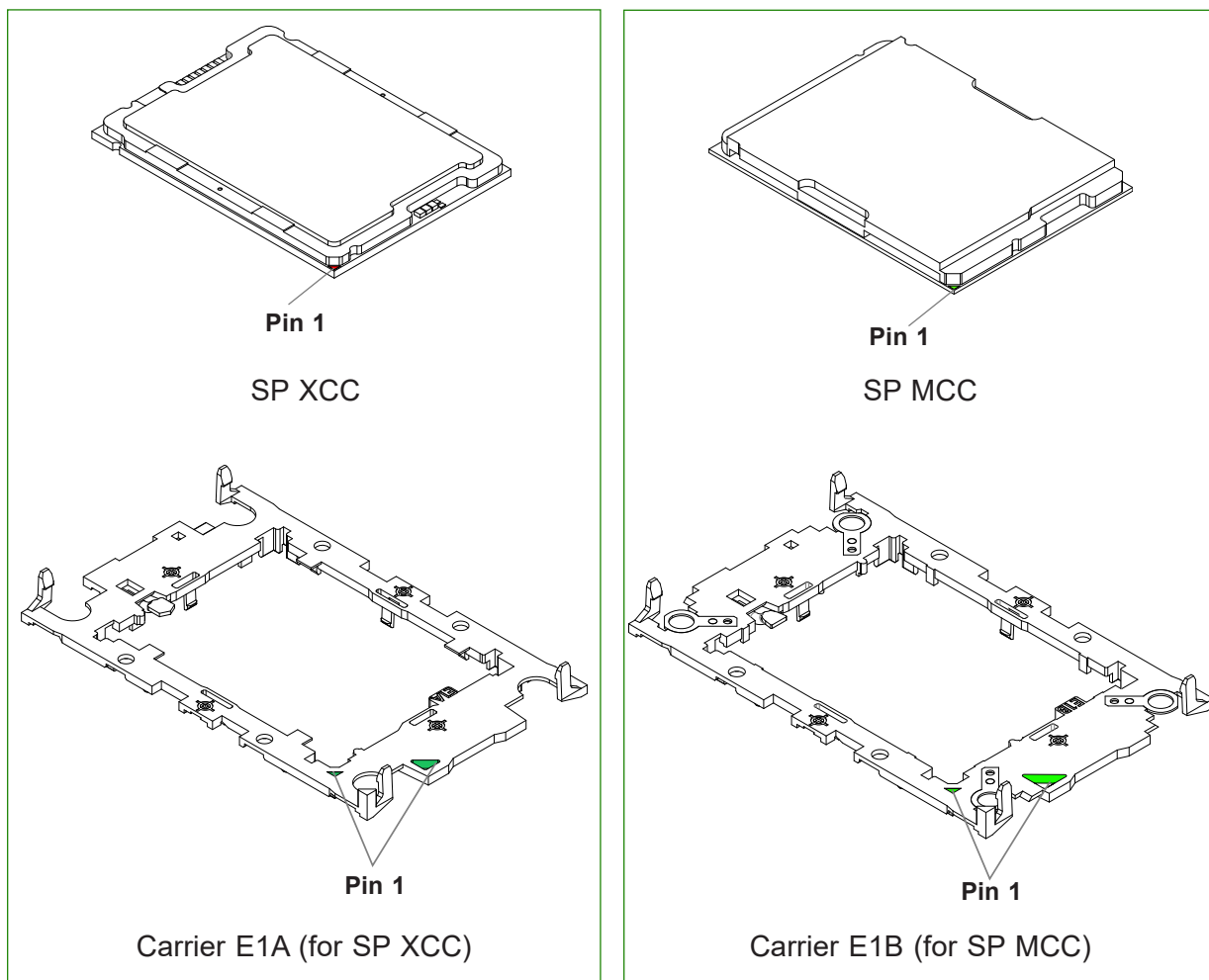


Figure 2-20: Processors with Marching Carrier

3. Turn over the processor carrier and locate pin 1 on the CPU and pin 1 on the carrier.
4. Turn the processor over with the component side (including the gold contacts) facing up and locate the CPU keys on the processor.
5. Locate the CPU keys and four latches on the carrier as shown:

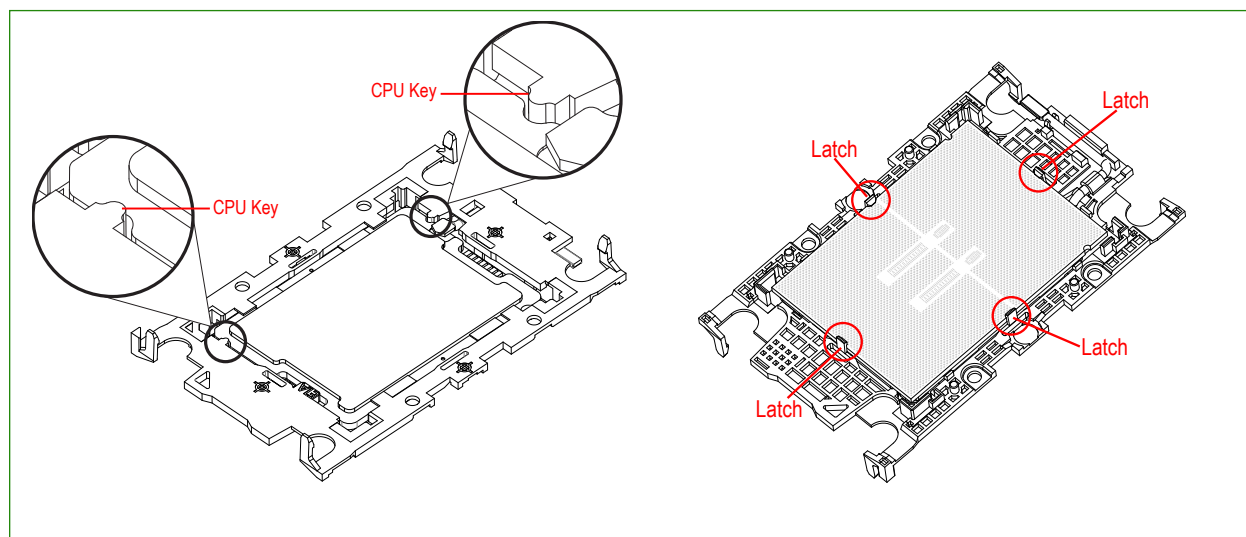


Figure 2-21: SP XCC Series

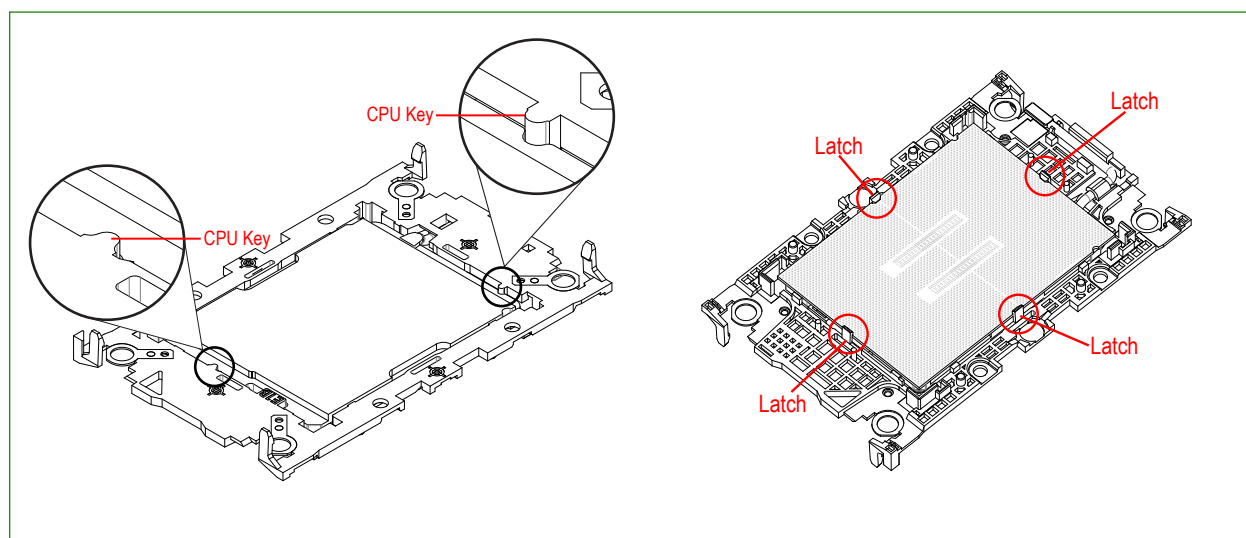


Figure 2-22: SP MCC Series

6. Locate the lever on the CPU socket and press it down as shown:

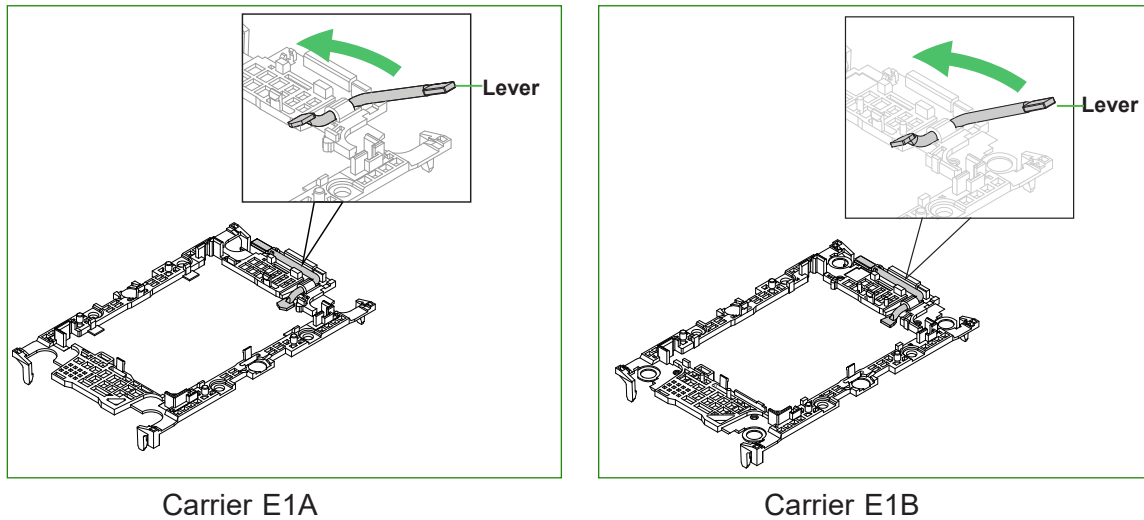


Figure 2-23: Pressing the Lever on the CPU Socket

7. Using pin 1 as a guide, carefully align the CPU keys (A and B) on the processor against the CPU keys on the carrier (a and b) as shown in the drawing.
8. Once they are properly aligned, carefully insert the CPU into the carrier. Make sure that the CPU is properly secured by latches 1, 2, 3, and 4.

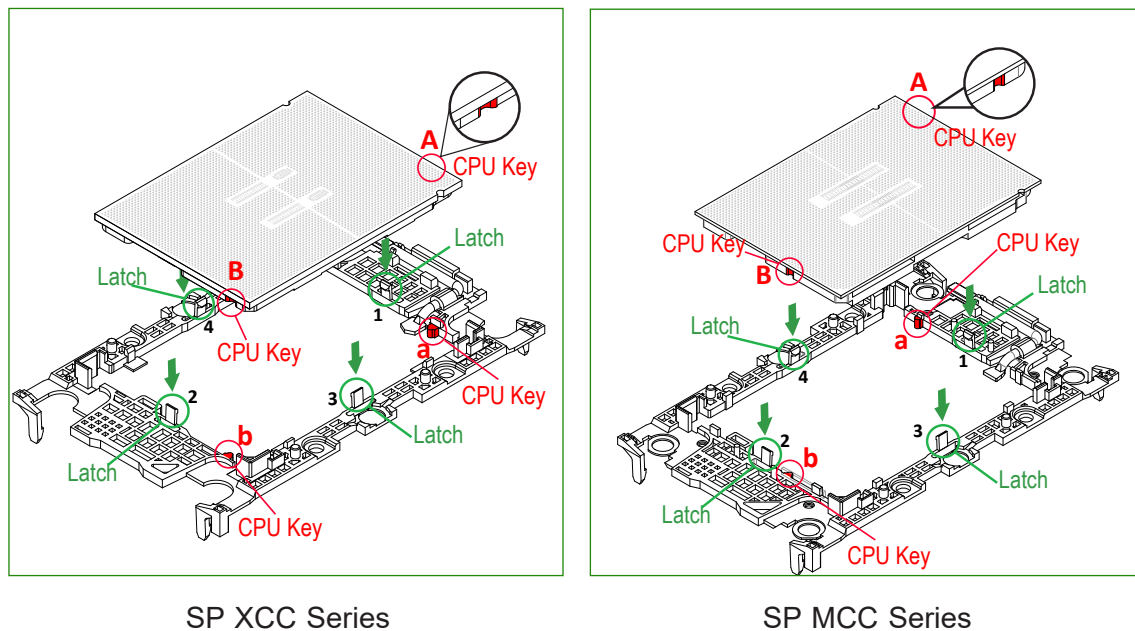


Figure 2-24: Insert the CPU Into the Carrier

9. After the processor is placed inside the carrier, examine the four sides of the processor, making sure that the processor is properly seated on the carrier.

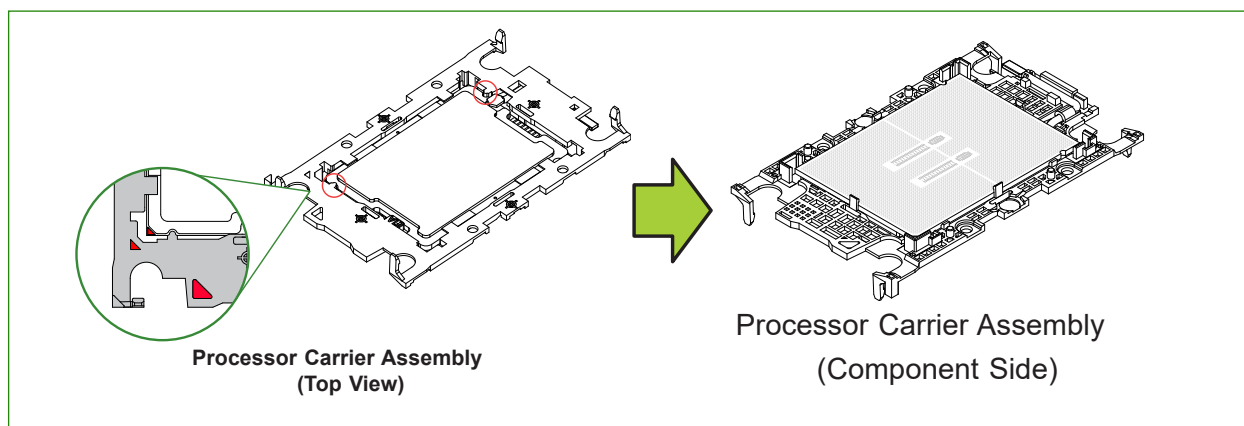


Figure 2-25: SP XCC Series

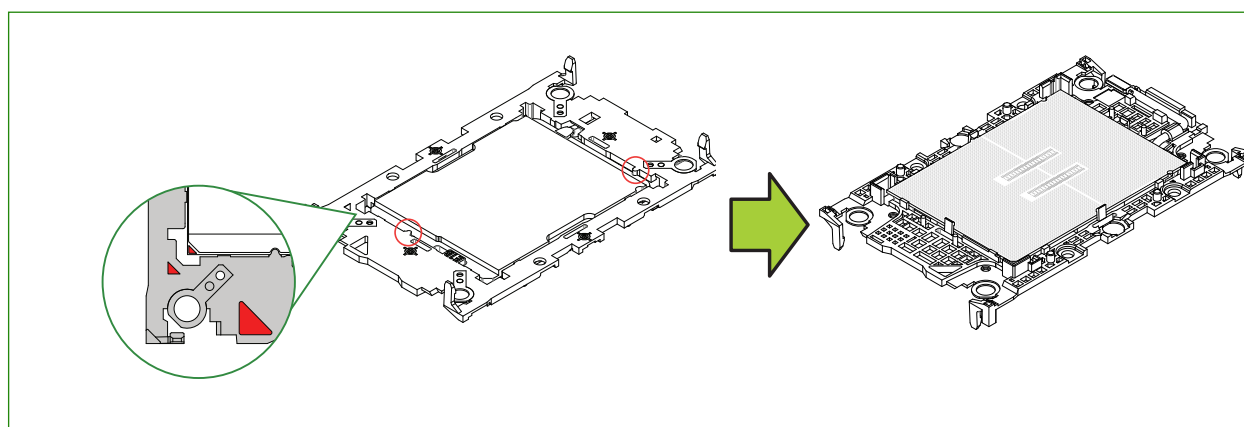


Figure 2-26: SP MCC Series

Creating the PHM

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



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

1. Turn the heatsink over with the thermal grease, which is on the reverse side of the heatsink, facing up. Pay attention to the two triangle cutouts (A, B) located at the diagonal corners of the heatsink, as shown in the following drawing.
2. Hold the processor carrier component side facing up.
3. Locate the triangle on the CPU and the triangle on the carrier. (Triangle indicates pin 1.)
4. Using pin 1 as a guide, turn the processor carrier assembly over with the gold contacts facing up.
5. Locate pin 1 (A) on the processor and pin 1 (a) on the processor carrier assembly.
6. Align the corner marked a on the processor carrier assembly against the triangle cutout A on the heatsink. Do the same for the corners marked b, c, and d on the processor assembly against the corners marked B, C, and D on the heatsinks.
7. Once they are properly aligned, place the corners marked a, b, c, and d on the processor carrier assembly into the corners of the heatsink marked A, B, C, and D. Make sure that all plastic clips are properly attached to the heatsink.

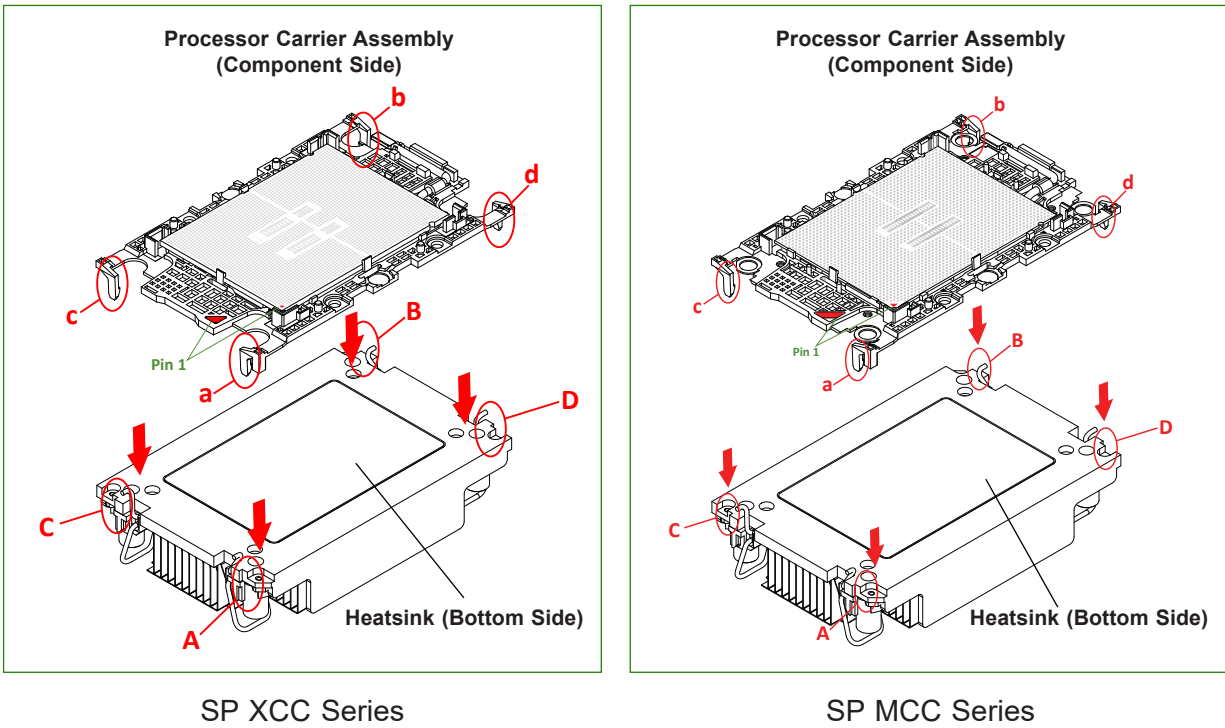


Figure 2-27: Processor Carrier Assembly (1U Heatsink)



(Top View)

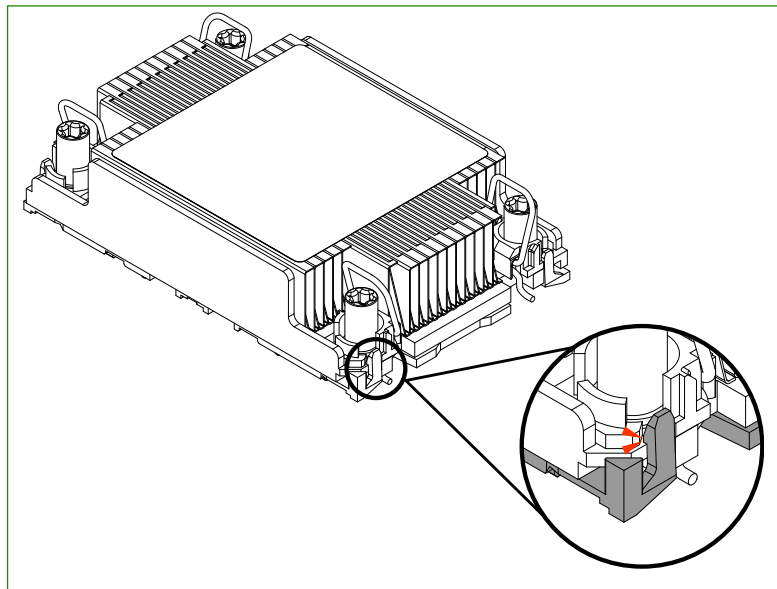


Figure 2-28: Processor Heatsink Module (PHM) 1U Heatsink

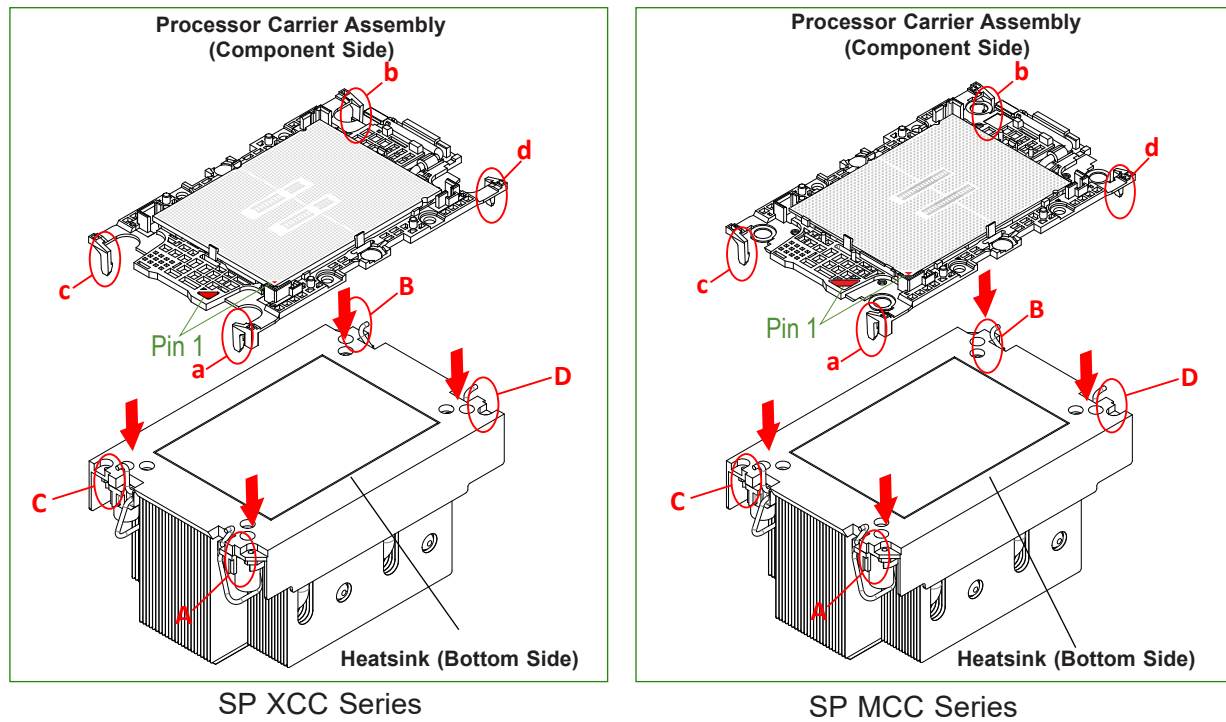


Figure 2-29: Processor Carrier Assembly (2U Heatsink)



(Top View)

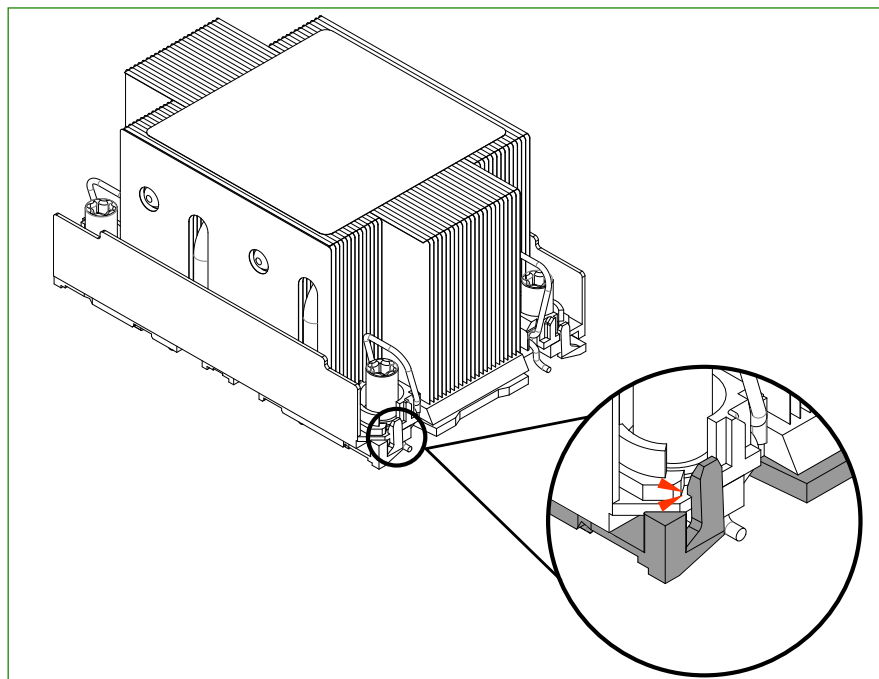


Figure 2-30: Processor Heatsink Module (PHM) 2U Heatsink

Preparing the CPU Socket for Installation

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

1. Press the tabs inward.

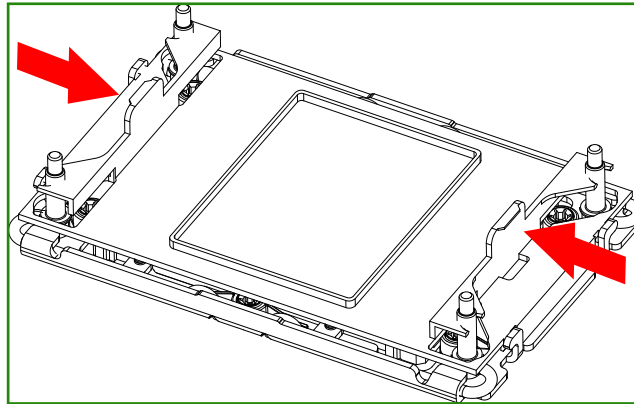


Figure 2-31: Pressing the Tabs Inward

2. Pull up the protective cover from the socket.

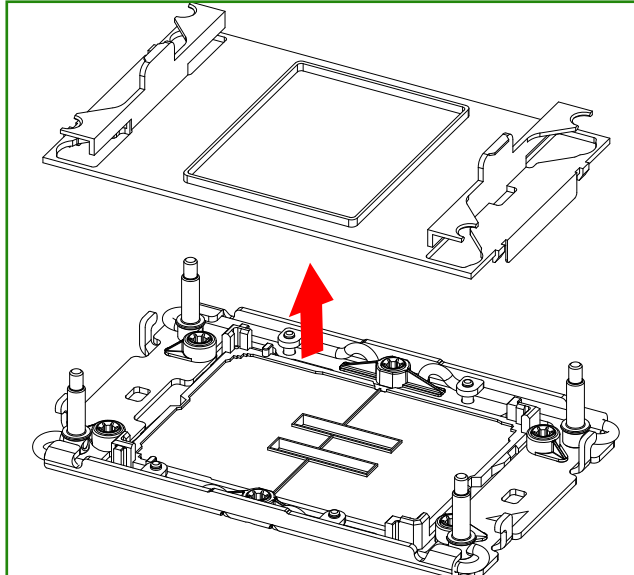


Figure 2-32: Pull Off the Protective Cover

Preparing to Install the PHM into the CPU Socket

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

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

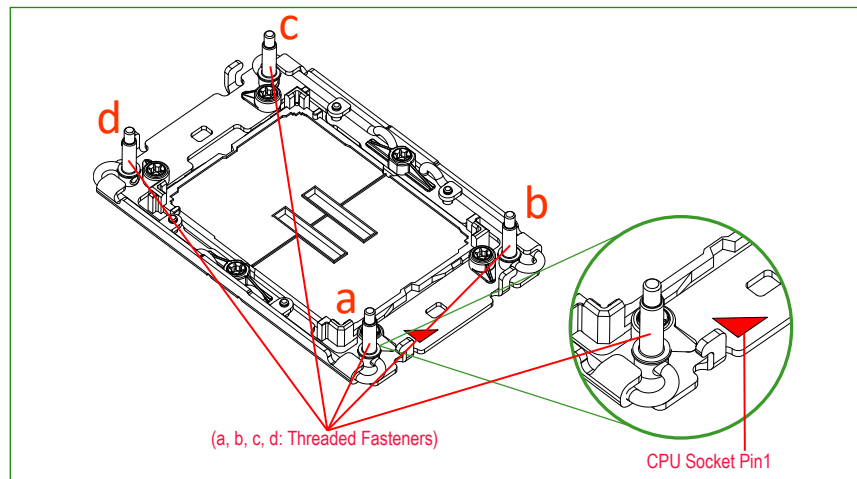


Figure 2-33: Fasteners on CPU Socket

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

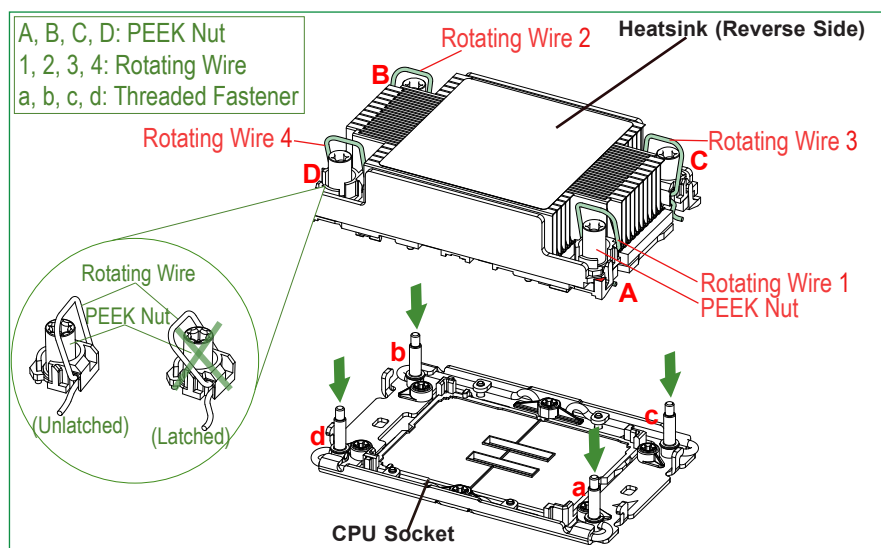


Figure 2-34: 1U Heatsink PEEK Nuts Assembly

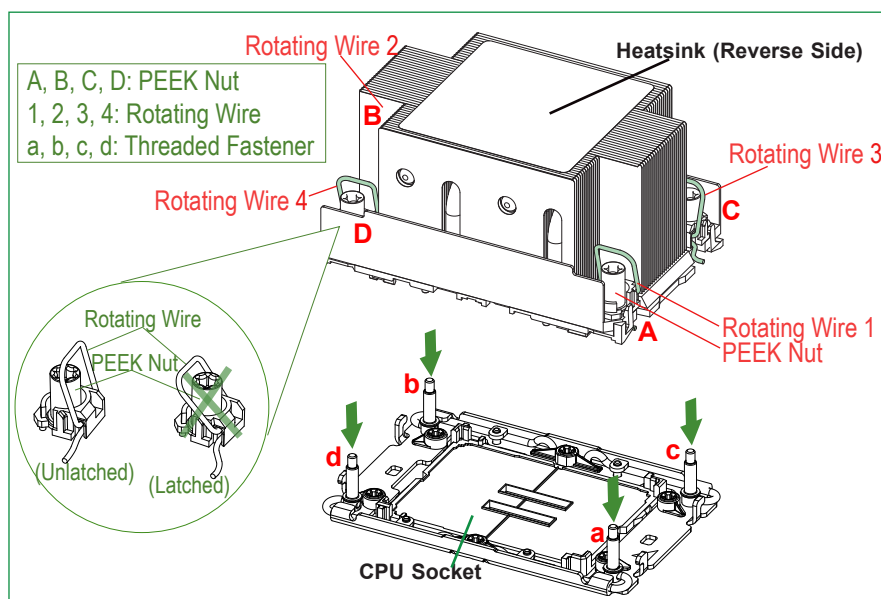


Figure 2-35: 2U Heatsink PEEK Nuts Assembly

3. Check the rotating wires (1, 2, 3, 4) to make sure that they are in the unlatched positions as shown in the drawing before installing the PHM into the CPU socket.

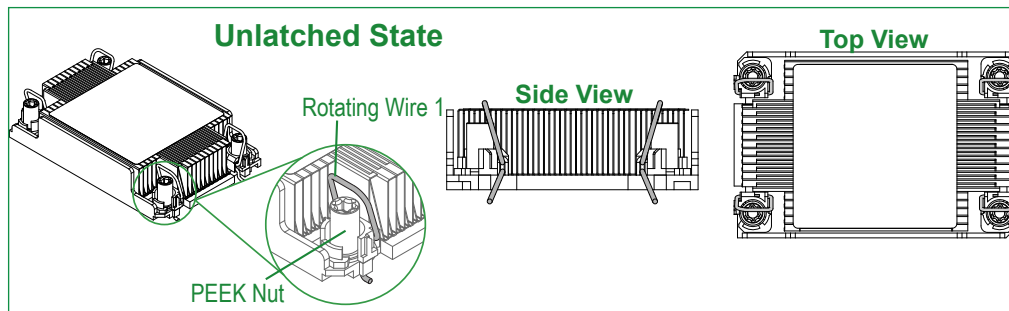


Figure 2-36: 1U Heatsink Rotating Wires

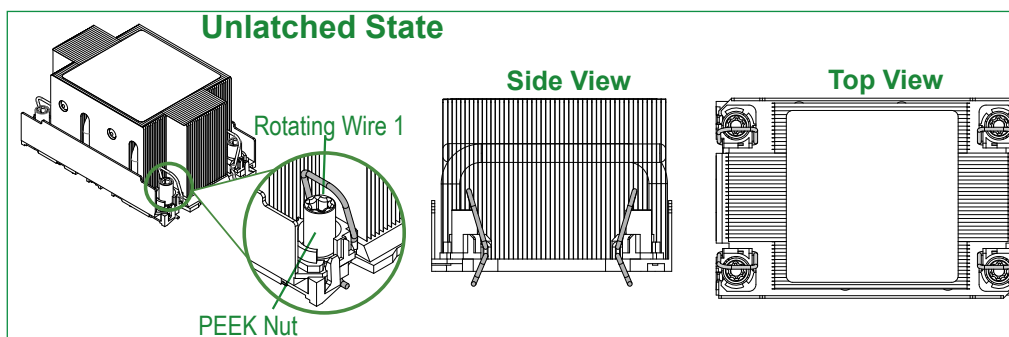


Figure 2-37: 2U Heatsink Rotating Wires

Installing the PHM into the CPU Socket

1. Align PEEK nut A, which is next to the triangle (pin 1) on the heatsink, against threaded fastener a on the CPU socket. Do the same in aligning PEEK nuts B, C, and D on the heatsink against threaded fasteners b, c, and d on the CPU socket. Make sure that all PEEK nuts on the heatsink are properly aligned with the corresponding threaded fasteners on the CPU socket.
2. Once they are aligned, gently place the heatsink on top of the CPU socket. Make sure that each PEEK nut is properly attached to its corresponding threaded fastener.

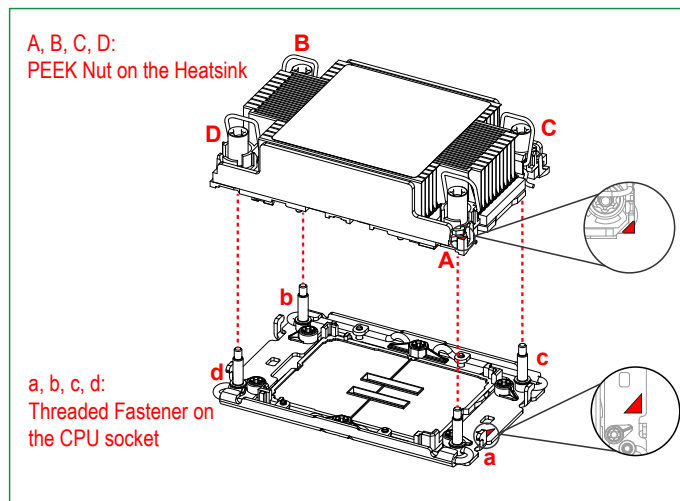


Figure 2-38: Align 1U Heatsink PEEK Nuts

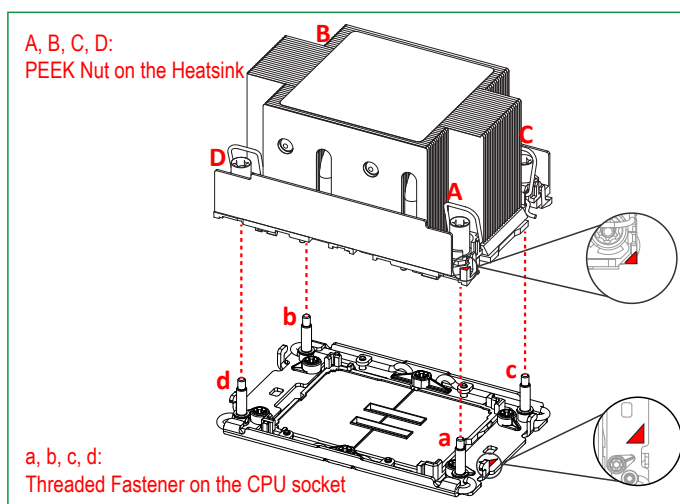


Figure 2-39: Align 2U Heatsink PEEK Nuts

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

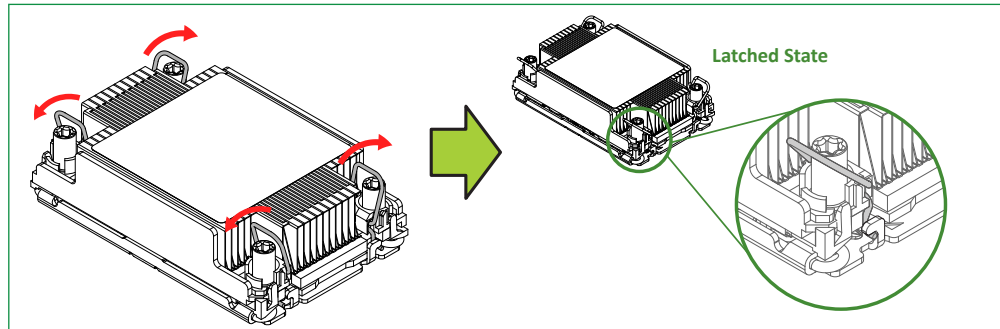


Figure 2-40: 1U Heatsink Rotating Wires

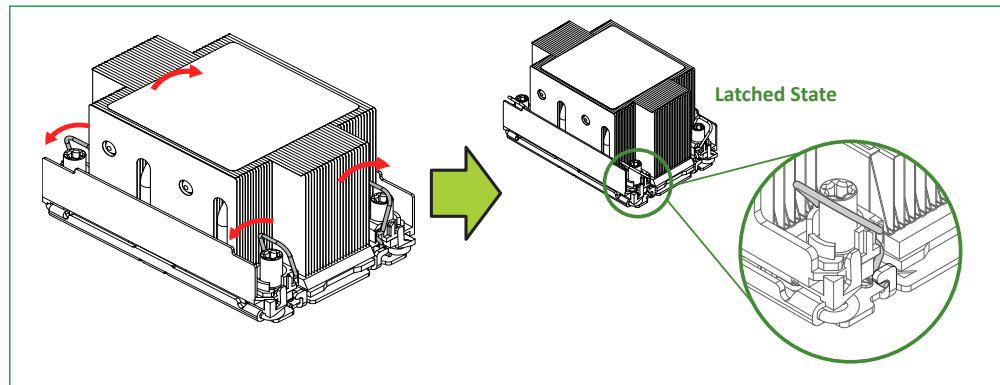


Figure 2-41: 2U Heatsink Rotating Wires

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

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

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

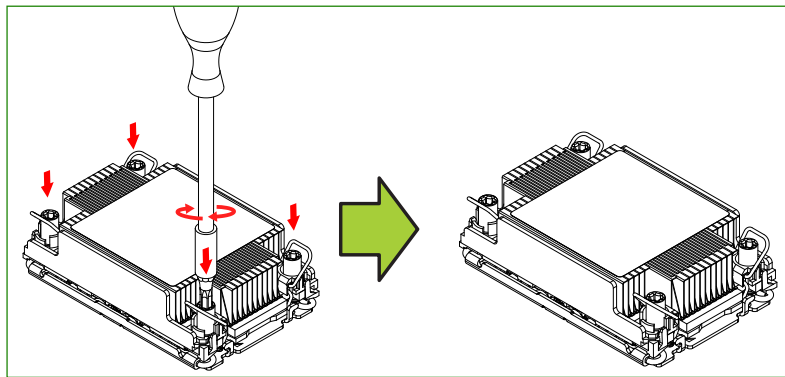


Figure 2-42: 1U Heatsink Securing PHM to the CPU Socket

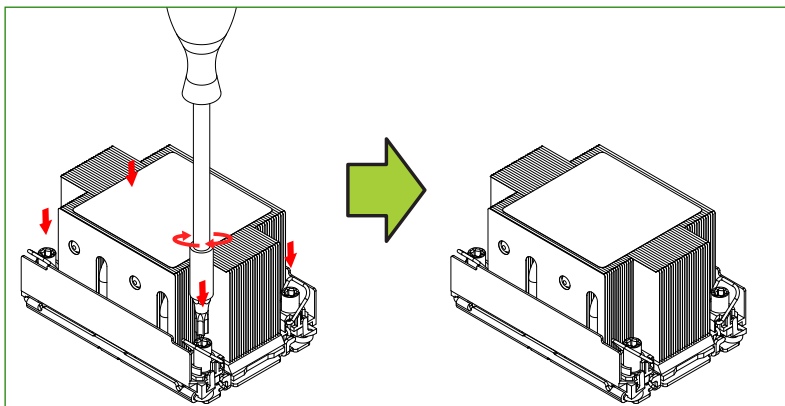


Figure 2-43: 2U Heatsink Securing PHM to the CPU Socket

Removing the PHM from the CPU Socket

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

1. Use a T30 driver to loosen the four PEEK nuts on the heatsink in the sequence of A, B, C, and D.

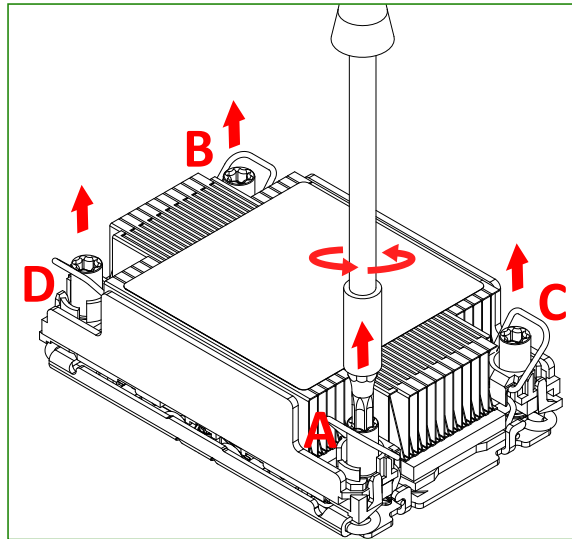


Figure 2-44: Using a T30 Drive to Loosen PEEK Nuts on 1U Heatsink

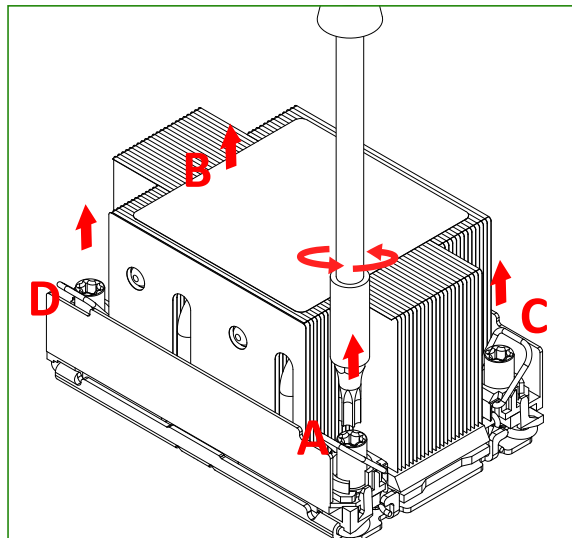


Figure 2-45: Using a T30 Drive to Loosen PEEK Nuts on 2U Heatsink

2. Once the PEEK nuts are loosened from the CPU socket, press the rotating wires inwards to unlatch the PHM from the socket, as shown in the drawings.

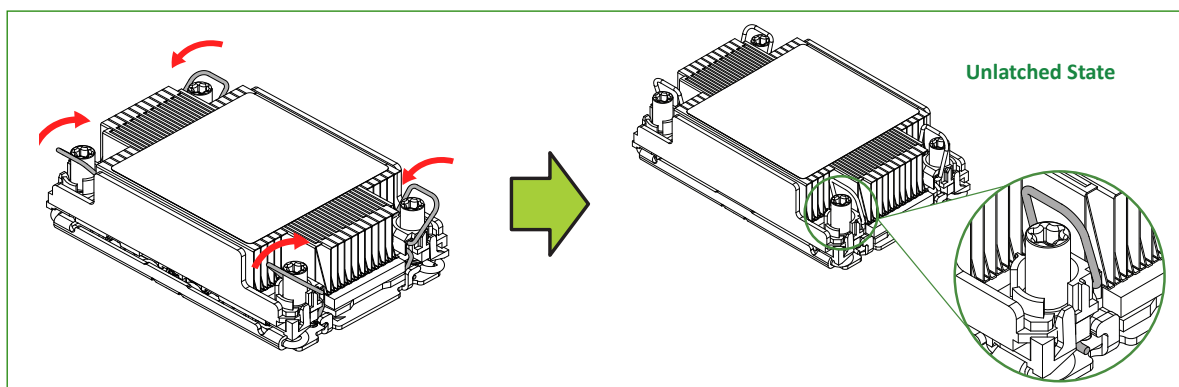


Figure 2-46: Press Rotating Wires Inwards for 1U Heatsink

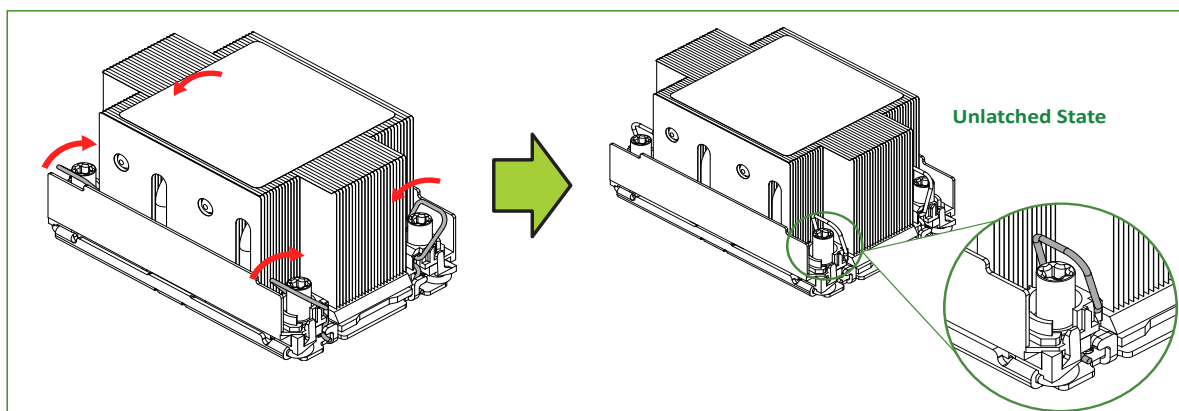


Figure 2-47: Press Rotating Wires Inwards for 2U Heatsink

3. Gently pull the PHM upwards to remove it from the CPU socket.

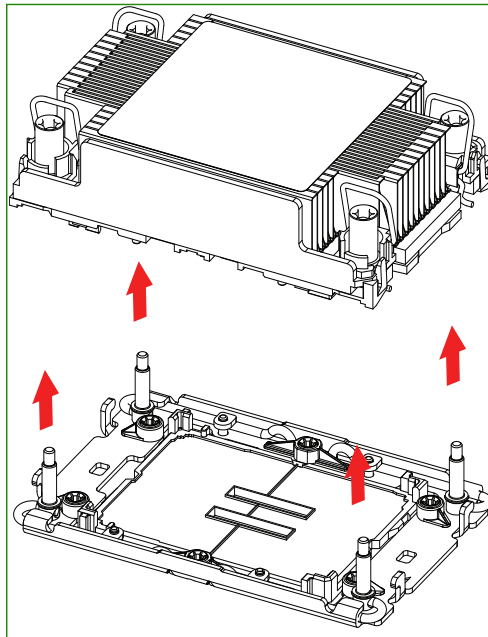


Figure 2-48: Removing PHM for 1U Heatsink

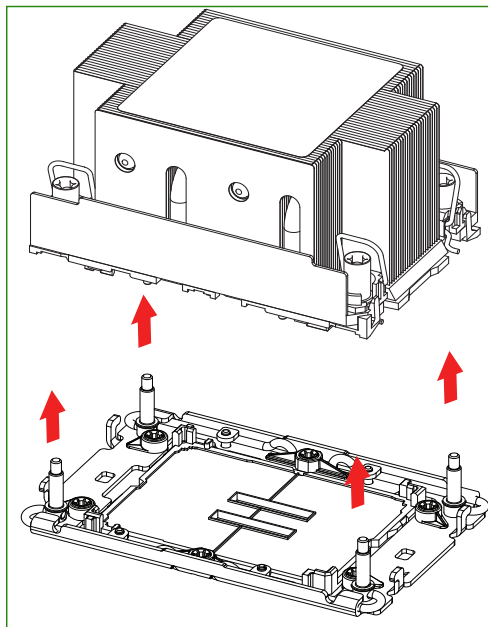
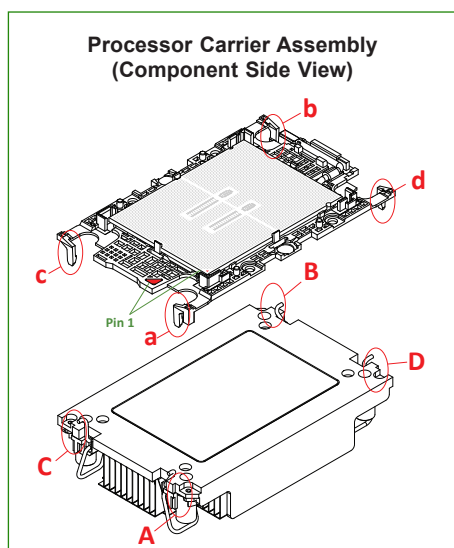


Figure 2-49: Removing PHM for 2U Heatsink

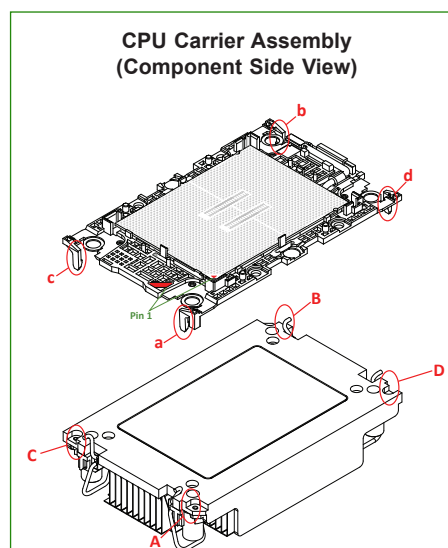
Removing the Processor Carrier Assembly from the PHM

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

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

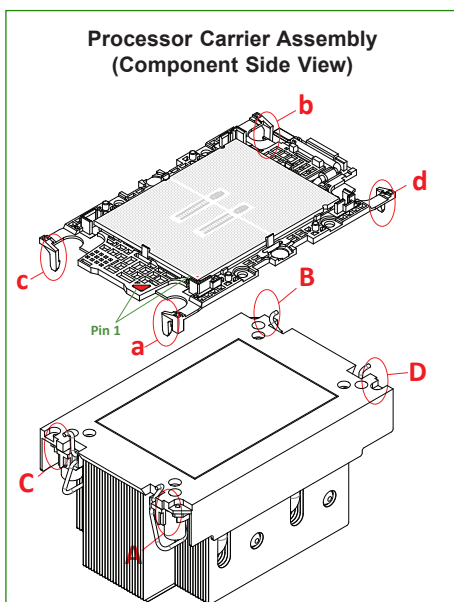


SP XCC Series

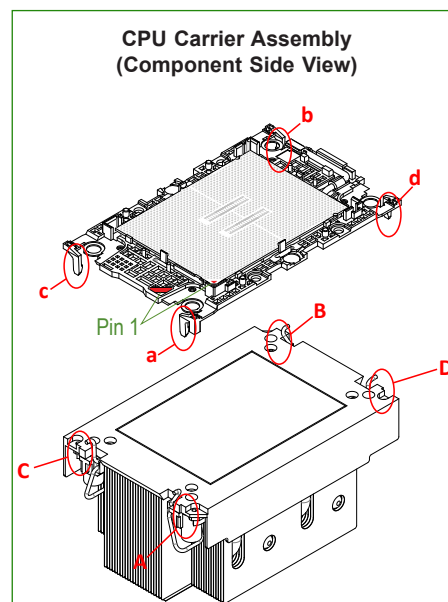


SP MCC Series

Figure 2-50: 1U Heatsink Processor Carrier Assembly



SP XCC Series

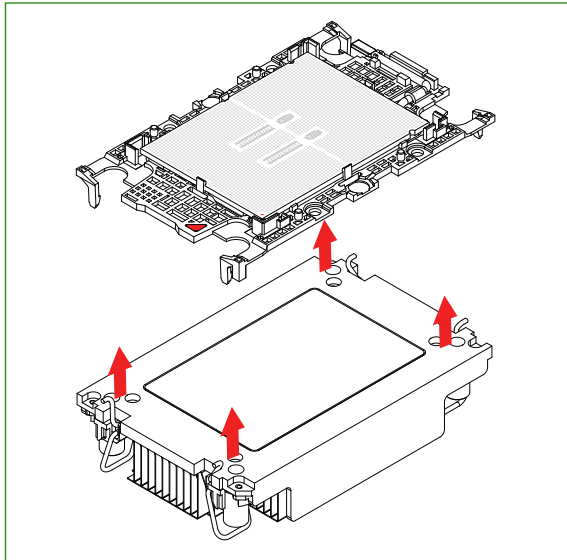


SP MCC Series

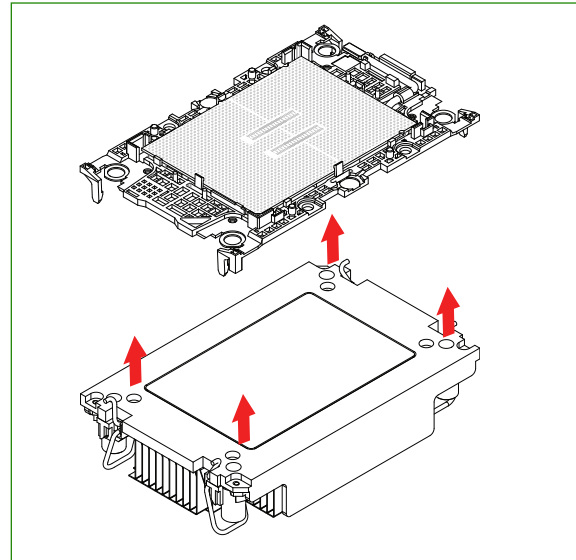
Heatsink (Bottom View)

Figure 2-51: 2U Heatsink Processor Carrier Assembly

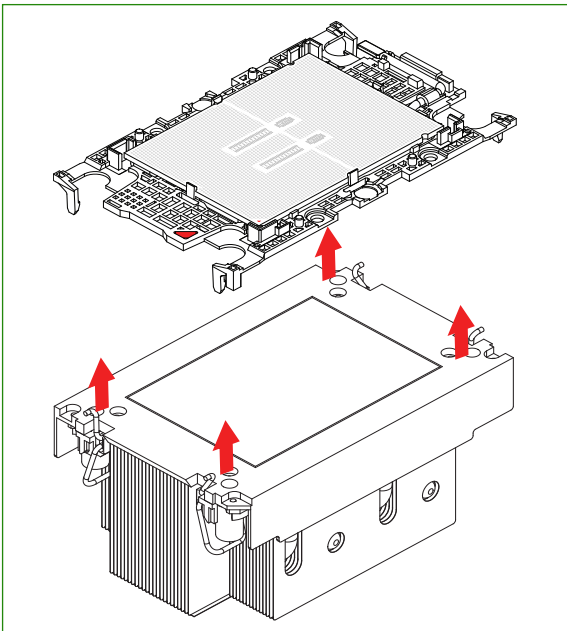
2. When all plastic clips are detached from the heatsink, remove the processor carrier assembly from the heatsink.



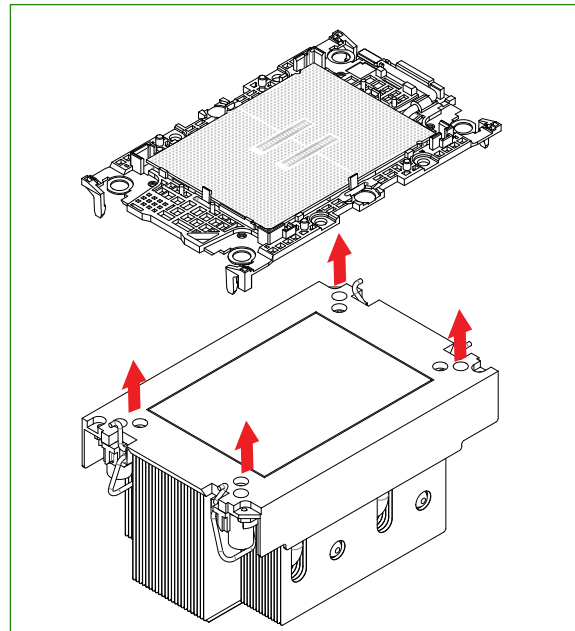
SP XCC Series



SP MCC Series

Figure 2-52: Removing the Processor Carrier Assembly From the 1U Heatsink

SP XCC Series



SP MCC Series

Figure 2-53: Removing the Processor Carrier Assembly From the 2U Heatsink

Removing the Processor from the Processor Carrier Assembly

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

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

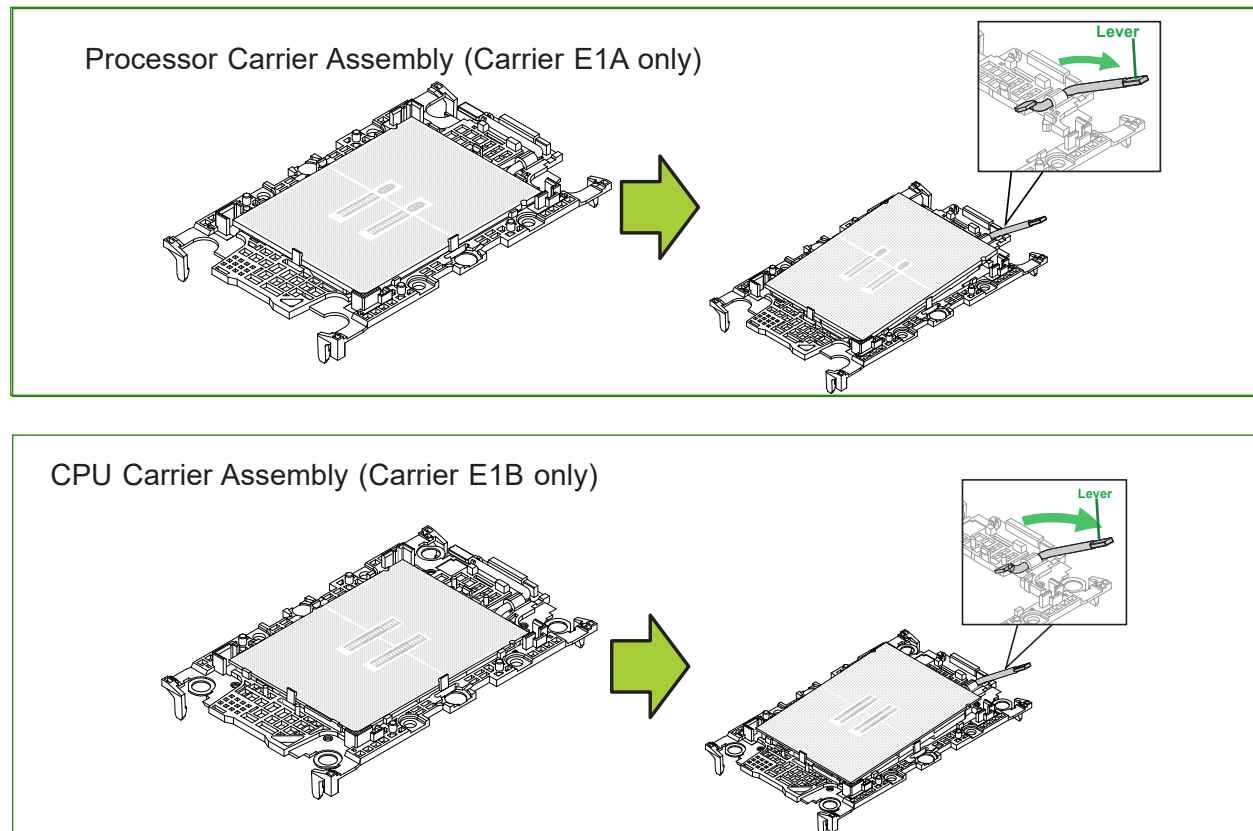
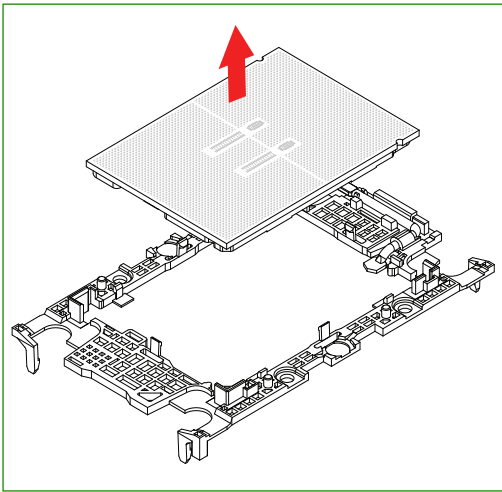


Figure 2-54: Disengaging the Process From the Carrier

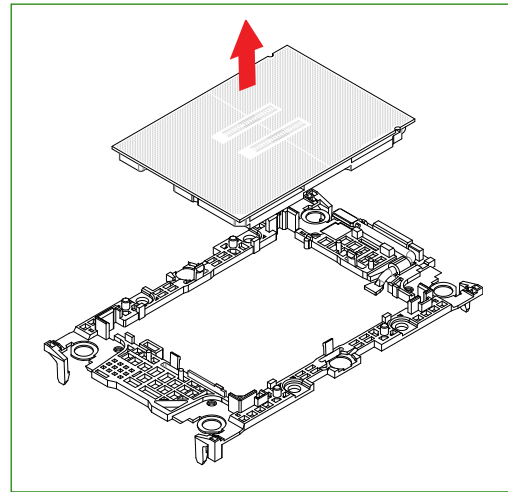
2. Once the processor is loosened from the carrier, carefully remove the processor from the processor carrier.



Note: Handle the processor with care to avoid damaging the processor and its pins.



SP XCC Series



SP MCC Series

Figure 2-55: Removing Processor From the Carrier

2.3 Motherboard Installation

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

Tools Needed

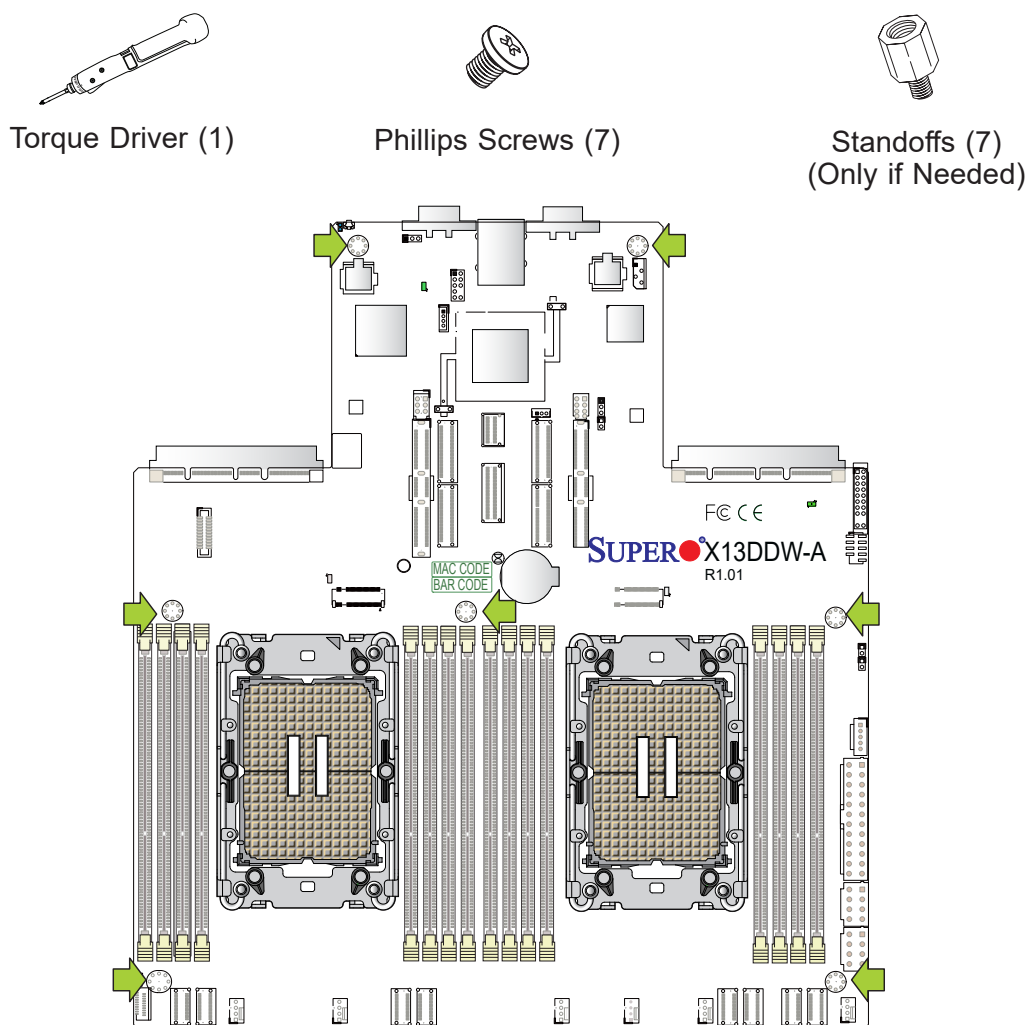


Figure 2-56: Tools Needed and the Locations of Mounting Holes

Do not use a force greater than 8 in-lbf (0.904 N-m) on each mounting screw during motherboard installation. Exceeding this force may over-torque the screw, causing damage to the motherboard and screw. Additionally, some components are very close to the mounting holes. Take precautionary measures to avoid damaging these components when installing the motherboard into the chassis.

Installing the Motherboard

1. Install the I/O shield into the back of the chassis, if applicable.
2. Locate the mounting holes on the motherboard. See the previous page for the location.
3. Locate the matching mounting holes on the chassis. Align the mounting holes on the motherboard with the mounting holes on the chassis.
4. Install standoffs in the chassis as needed.

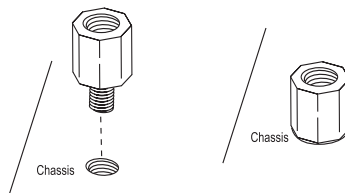


Figure 2-57: Installing Standoffs

5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
6. Using the Phillips screwdriver, insert a pan head #6 screw into a mounting hole on the motherboard and its matching mounting hole on the chassis.

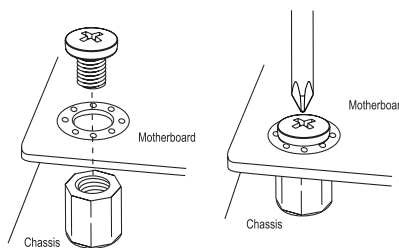


Figure 2-58: Securing Chassis to Standoffs with #6 Screws

7. Repeat Step 5 to insert #6 screws into all mounting holes.
8. Make sure that the motherboard is securely placed in the chassis.

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

2.4 Memory Support and Installation



Note: Check the Supermicro website for recommended memory modules.



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

Memory Support

This motherboard supports up to 4 TB 3DS RDIMM/RDIMM DDR5 (288-pin) ECC memory with speeds up to 5600 MT/s in 16 DIMM slots. To enhance memory performance, do not mix memory modules of different speeds and sizes. Follow all the memory installation instructions.



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

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

For your system memory to work properly, follow the memory population tables to install the memory modules on your motherboard. These memory population tables were created based on the general memory population guidelines provided by Intel to support Supermicro X13DP motherboards.

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

 **Note 1:** 1 DPC applies to 1 SPC or 2 SPC implementation (SPC — Sockets Per Channel).

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

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

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

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

 **Note:** 1 DPC applies to 1 SPC or 2 SPC implementation (SPC — Sockets Per Channel).

Memory Population Table for 4th/5th Gen Intel Xeon Scalable Processors

DDR5 Memory Population Table for X13DP Motherboards (with 16 DIMMs installed)	
1 CPU:	Memory Population Sequence
1 CPU and 1 DIMM	P1-DIMMA1 P1-DIMME1 P1-DIMMB1 P1-DIMMF1
1 CPU and 2 DIMMs	P1-DIMMA1 / P1-DIMMG1 P1-DIMMC1 / P1-DIMME1
1 CPU and 4 DIMMs	P1-DIMMA1 / P1-DIMMC1 / P1-DIMME1 / P1-DIMMG1
1 CPU and 6 DIMM	P1-DIMMA1 / P1-DIMMC1 / P1-DIMMD1 / P1-DIMME1 / P1-DIMMF1 / P1-DIMMG1 P1-DIMMA1 / P1-DIMMB1 / P1-DIMMC1 / P1-DIMME1 / P1-DIMMG1 / P1-DIMMH1 P1-DIMMB1 / P1-DIMMC1 / P1-DIMMD1 / P1-DIMME1 / P1-DIMMF1 / P1-DIMMH1 P1-DIMMA1 / P1-DIMMB1 / P1-DIMMD1 / P1-DIMMF1 / P1-DIMMG1 / P1-DIMMH1
1 CPU and 8 DIMMs	P1-DIMMA1 / P1-DIMMB1 / P1-DIMMC1 / P1-DIMMD1 / P1-DIMME1 / P1-DIMMF1 / P1-DIMMG1 / P1-DIMMH1
2 CPUs: (Recommended)	Memory Population Sequence
2 CPUs and 2 DIMMs	CPU1: P1-DIMMA1, CPU2: P2-DIMMA1 CPU1: P1-DIMME1, CPU2: P2-DIMME1 CPU1: P1-DIMMB1, CPU2: P2-DIMMB1 CPU1: P1-DIMMF1, CPU2: P2-DIMMF1
2 CPUs and 4 DIMMs	CPU1: P1-DIMMA1 / P1-DIMMG1, CPU2: P2-DIMMA1 / P2-DIMMG1 CPU1: P1-DIMMC1 / P1-DIMME1, CPU2: P2-DIMMC1 / P2-DIMME1
2 CPUs and 8 DIMMs	CPU1: P1-DIMMA1 / P1-DIMMC1 / P1-DIMME1 / P1-DIMMG1 CPU2: P2-DIMMA1 / P2-DIMMC1 / P2-DIMME1 / P2-DIMMG1
2 CPUs and 12 DIMMs	CPU1: P1-DIMMA1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1 CPU2: P2-DIMMA1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1 CPU1: P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMME1/P1-DIMMG1/P1-DIMMH1 CPU2: P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMME1/P2-DIMMG1/P2-DIMMH1 CPU1: P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMH1 CPU2: P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMH1 CPU1: P1-DIMMA1/P1-DIMMB1/P1-DIMMD1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1 CPU2: P2-DIMMA1/P2-DIMMB1/P2-DIMMD1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1
2 CPUs and 16 DIMMs	CPU1: P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1 CPU2: P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1



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

DIMM Installation

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

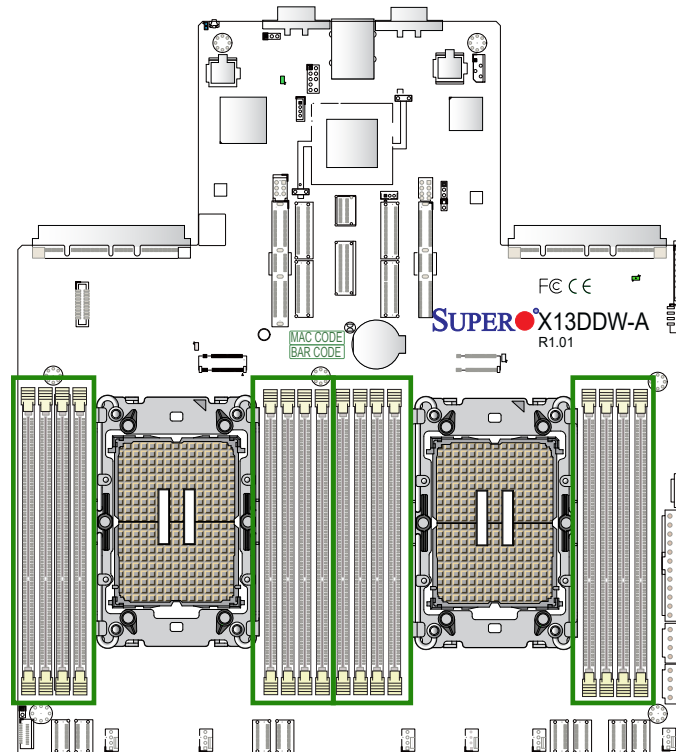
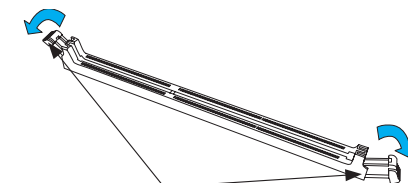


Figure 2-59: Locations of DIMM Memory Slots

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



Release Tabs

Figure 2-60: Unlocking Release Tabs

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

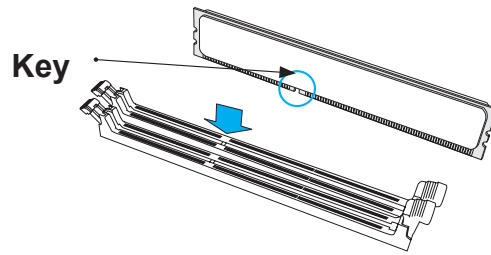


Figure 2-61: Aligning Key

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

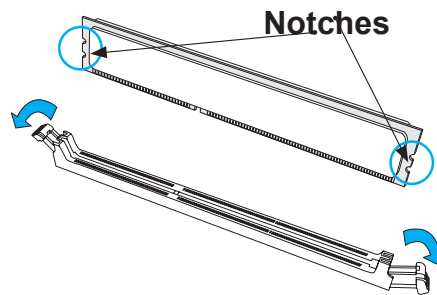


Figure 2-62: Aligning Notches

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

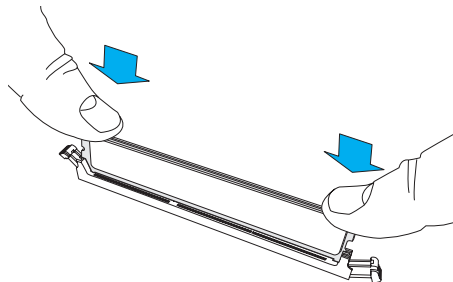


Figure 2-63: Pushing Both Ends Straight Down Into the Memory Slot

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

DIMM Removal

Press both release tabs on the ends of the memory module to unlock it. Once the memory module has been loosened, remove it from the memory slot.

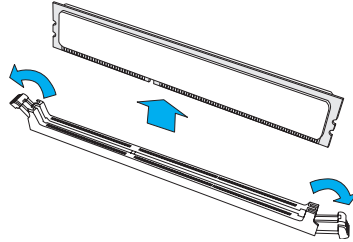


Figure 2-64: Unlock and Remove Memory Module



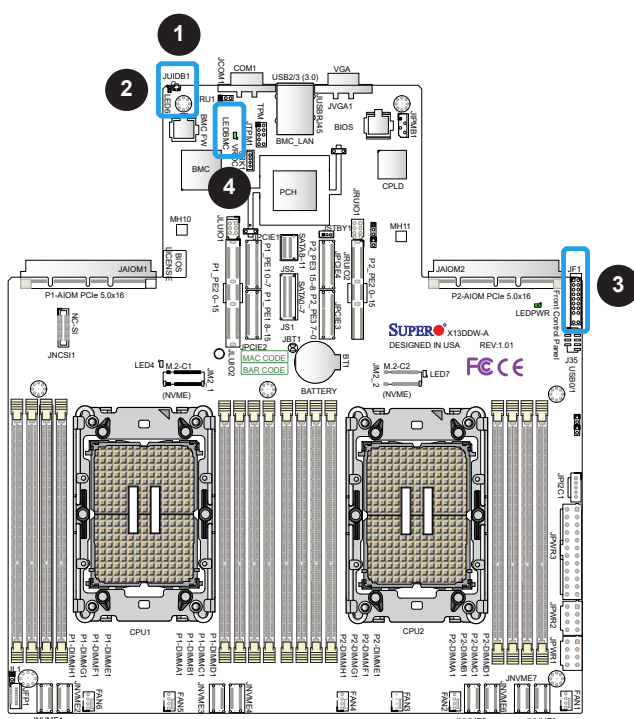
Warning! Do not use excessive force when pressing the release tabs on the ends of the DIMM socket to avoid causing any damage to the memory module or the DIMM socket. Handle memory modules with care. Carefully follow all the instructions given on page 1 of this chapter to avoid causing ESD-related damage to your memory modules or components.

2.5 I/O Panel

Unit Identification (UID)/BMC Reset Switch and UID/BMC Reset LED Indicators

A UID LED/BMC Reset switch (JUIDB1) is located on the I/O port. This switch has dual functions. It can be used to identify a system unit that is in need of service, and it can also be used to reset the BMC settings.

When functioning as a BMC reset switch, JUIDB1 will trigger a cold reboot when the user presses and holds the switch for six seconds. It will also restore the BMC to the manufacturer's default when the user presses and holds the switch for 12 seconds.



1. UID LED/BMC Reset Switch
2. Rear UID LED (LED6)
3. Front UID LED (Pins 7–8 of JF1)
4. BMC Heartbeat LED (LEDBMC)

When functioning as a UID LED switch, JUIDB1 will turn both rear UID LED (LED6) and front UID LED (Pin 7/Pin 8 of JF1) on and off when the user presses the switch on/off.

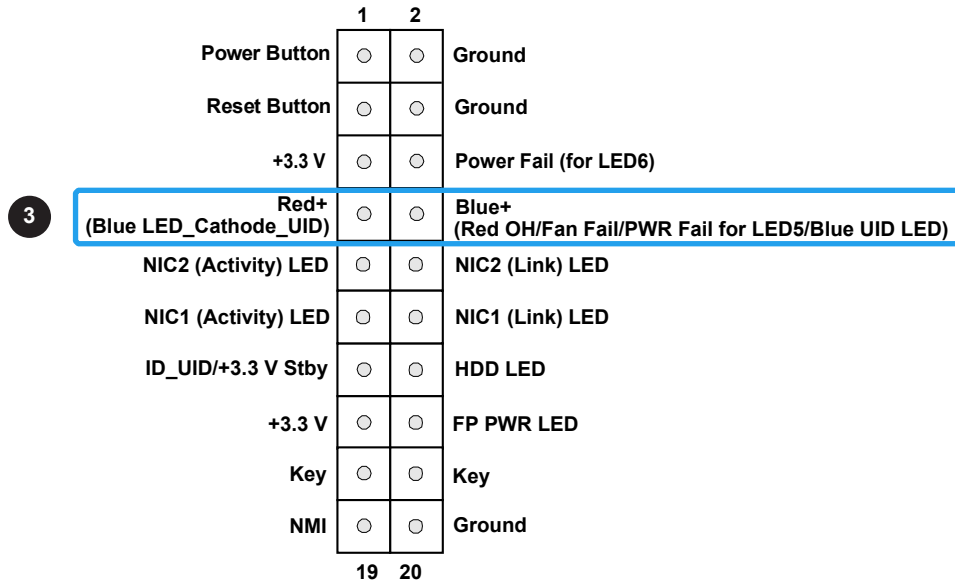


Figure 2-66: UID LED Pins

To achieve these dual purposes, the UID LED/BMC Reset switch works in conjunction with the BMC Heartbeat LED (LEDBMC) and front/rear UID LEDs. Note that UID can also be triggered via BMC on the motherboard. For more details on the UID LEDs and BMC LEDs, refer to the tables. Also, refer to the BMC User's Guide posted on our website at <http://www.supermicro.com> for more information on BMC.

UID/BMC Reset Switch (JUIDB1) Pin Definitions	
Pin#	Definition
1	GND
2	GND
3	Button In
4	Button In

UID/BMC Reset Switch (JUIDB1) as a BMC Reset Switch Features and Settings		
Work with BMC Heartbeat LED (LEDBMC)		
BMC Heartbeat LED	LEDBMC	Green Blinking: BMC Normal
BMC Reset: Press and Hold the Switch (JUIDB1) Six Seconds	LEDBMC	Solid Green: During Reboot
		Triggering a Cold Reboot Solid Green: On During Cold Reboot
BMC Reset: Press and Hold the Switch (JUIDB1) 12 Seconds	LEDBMC	Solid Green: During BMC Reset
		BMC: Reset to the manufacturer's default; LED solid on during BMC Reset

UID/BMC Reset Switch (JUIDB1) as a UID LED Switch Features and Settings		
Work with Rear UID LED (LED6) and Front UID LED (JF1: Pins 7/8)		
Rear UID LED	LED6	Blue: Unit Identified
Front UID LED	Pin 7/Pin 8 (JF1)	Blue: Unit Identified
Press the switch (JUIDB1) to turn on and off both rear and front UID LED indicators;		

VGA Connector

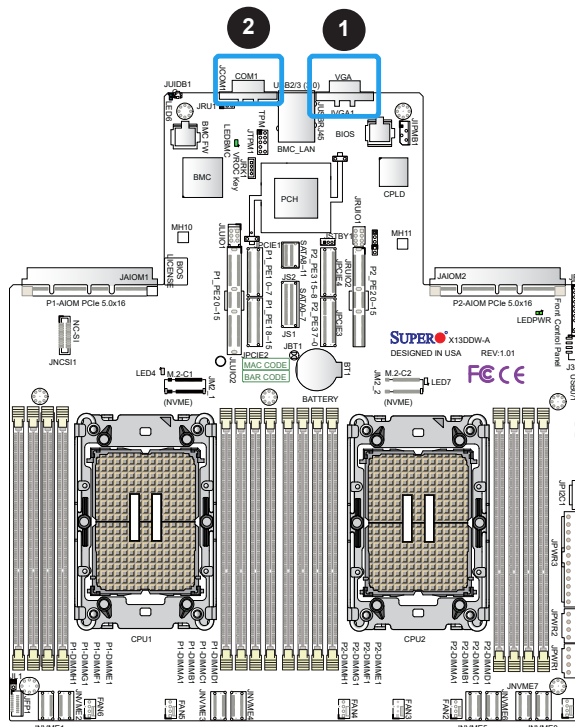
A rear VGA connector is located at JVGA1 on the I/O panel of your system. This VGA connection provides analog interface support between the computer and the video displays. Refer to the layout for the location of the rear VGA connector.

COM Port

A communication (COM) port that supports a serial link interface is on the motherboard. COM1 (JCOM1) is located on the I/O panel. Refer to the board layout for the location of COM1.



Figure 2-67: VGA Connector and COM Port



1. (Rear) VGA
2. COM1 on I/O Panel

Universal Serial Bus (USB) Ports and Headers

There are two USB 3.0 ports (USB2/USB3) located on the I/O panel for USB rear side support. The USB 2.0 header, located at J35, supports two USB connections (USB0/USB1) for front access. Connect these USB ports and the header for USB support via USB cables (not included).

USB 0/1 (USB 2.0) (J35) Pin Definitions			
Pin#	Definition	Pin#	Definition
1	+5 V	2	+5 V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	GND	8	GND
9	Key	10	NC

I/O Panel USB 2/3 (USB 3.0) Pin Definitions			
Pin#	Definition	Pin#	Definition
A1	VBUS	B1	Power
A2	D-	B2	USB_N
A3	D+	B3	USB_P
A4	GND	B4	GND
A5	Std_a_SSRX-	B5	USB3_RN
A6	Std_a_SSRX+	B6	USB3_RP
A7	GND	B7	GND
A8	Std_a_SSTX-	B8	USB3_TN
A9	Std_a_SSTX+	B9	USB3_TP

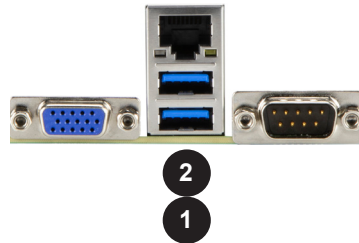
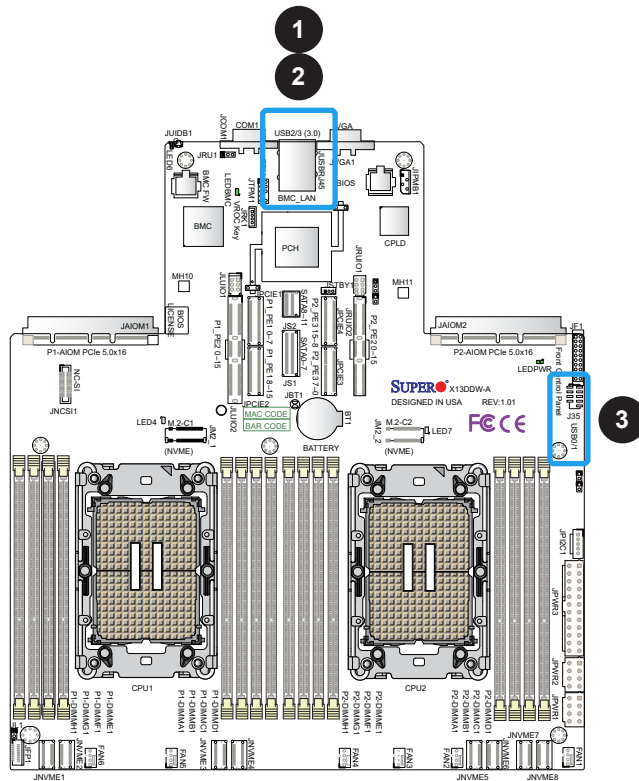


Figure 2-69: USBs on the I/O Panel



1. USB2 (USB 3.0) on I/O Panel
2. USB3 (USB 3.0) on I/O Panel
3. USB0/1 (USB 2.0) for Front Access (J35)

BMC LAN

A dedicated BMC LAN (BMC LAN) port is located on the I/O panel. The dedicated BMC LAN, located above the USB2/3 ports on the I/O panel, provides LAN support for the Baseboard Management Controller (BMC). Connect an RJ45 cable to JUSB RJ45 on the I/O panel for BMC LAN support. Refer to the LED Indicator section for LAN LED information.

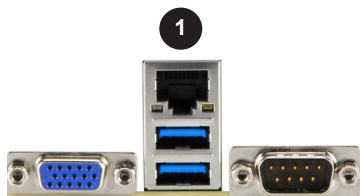
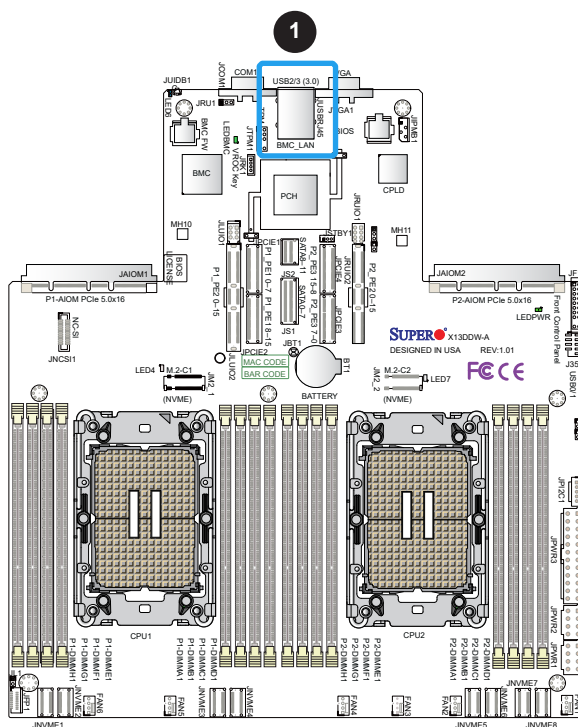


Figure 2-71: BMC LAN Port

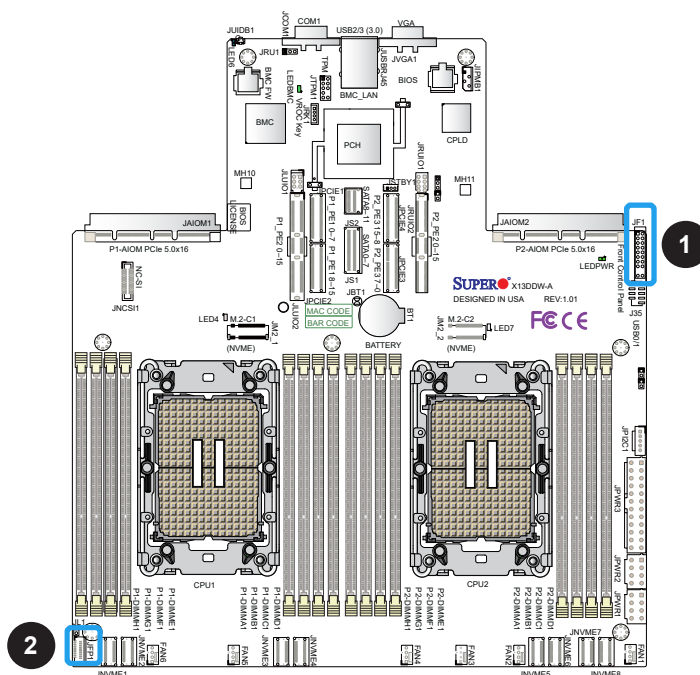


1. BMC LAN (IPMI LAN)

2.6 Front Control Panels

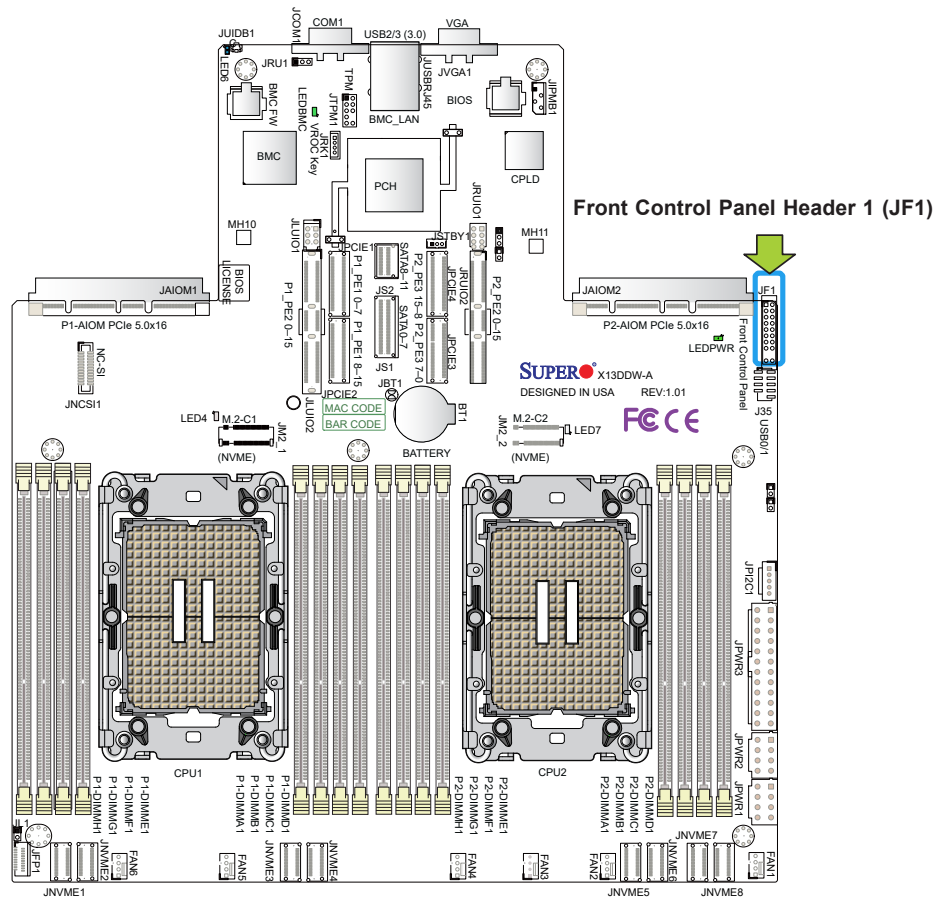
Front Control Panels

There are two front control panel headers on the motherboard. These front control panel headers, located at JF1 and JFP1, contain header pins for various buttons and LED indications with I²C support for front access. The front control panels are designed specifically for use with Supermicro chassis. See the layout for the locations of JF1 and JFP1.



1. JF1
2. JFP1

1. Front Control Panel Header (JF1)



	1	2	
Power Button	○	○	Ground
Reset Button	○	○	Ground
+3.3 V	○	○	Power Fail (for LED6)
Red+ (Blue LED_Cathode_UID)	○	○	Blue+ (Red OH/Fan Fail/PWR Fail for LED5/Blue UID LED)
NIC2 (Activity) LED	○	○	NIC2 (Link) LED
NIC1 (Activity) LED	○	○	NIC1 (Link) LED
ID_UID/+3.3 V Stby	○	○	HDD LED
+3.3 V	○	○	FP PWR LED
Key	○	○	Key
NMI	○	○	Ground
	19	20	

Figure 2-75: JF1 Header Pins

Power On and BMC/BIOS Status LED Button

The Power On and BMC/BIOS Status LED button is located on pins 1–2 of JF1. Momentarily contacting both pins will power on/off the system or display BMC/BIOS status. Refer to the tables for more information.

Power Button and BIOS/BMC Status LED Indicator Pin Definitions (JF1)	
Pin#	Definition
1	Signal
2	GND

Power Button LED Indicator Status	
Status	Event
Green: Solid On	System Power On
BMC/BIOS Blinking Green at 4 Hz	BMC/BIOS Checking
BIOS Blinking Green at 4 Hz	BIOS Recovery/Update in Progress
BMC Blinking Red x2 (Two Blinks Red) at 4 Hz, One Pause at 2 Hz (On-On-Off-Off)	BMC Recovery/Update in Progress
BMC/BIOS Blinking Green at 1 Hz	Flash of detected or golden image checking failure

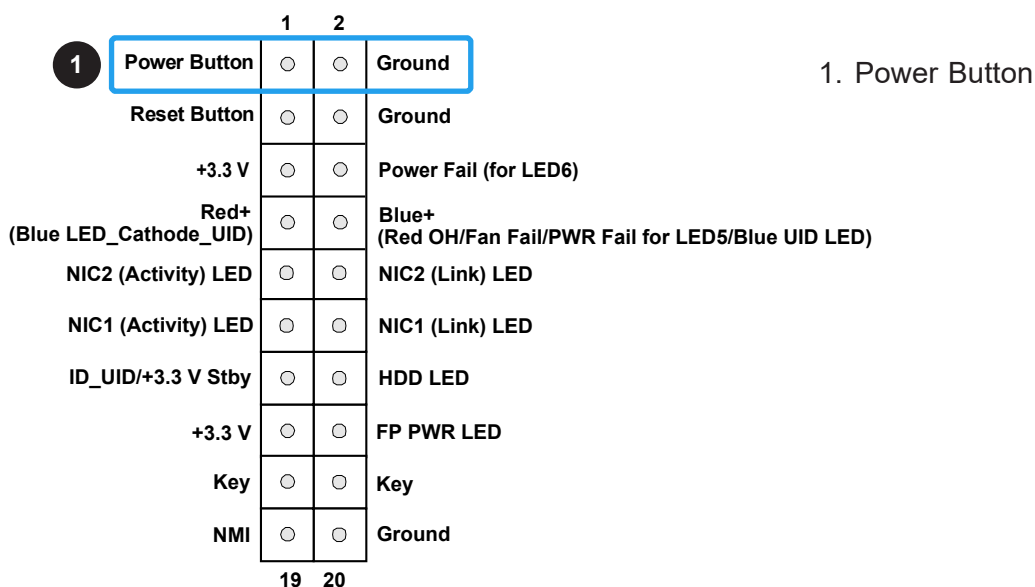


Figure 2-76: Power Button Pins

Reset Button

The Reset Button connection is located on pins 3–4 of JF1. Momentarily contacting both pins will reset the system. Refer to the table for pin definitions.

Reset Button Pin Definitions (JF1)	
Pin#	Definition
3	Reset
4	GND

1. Reset Button

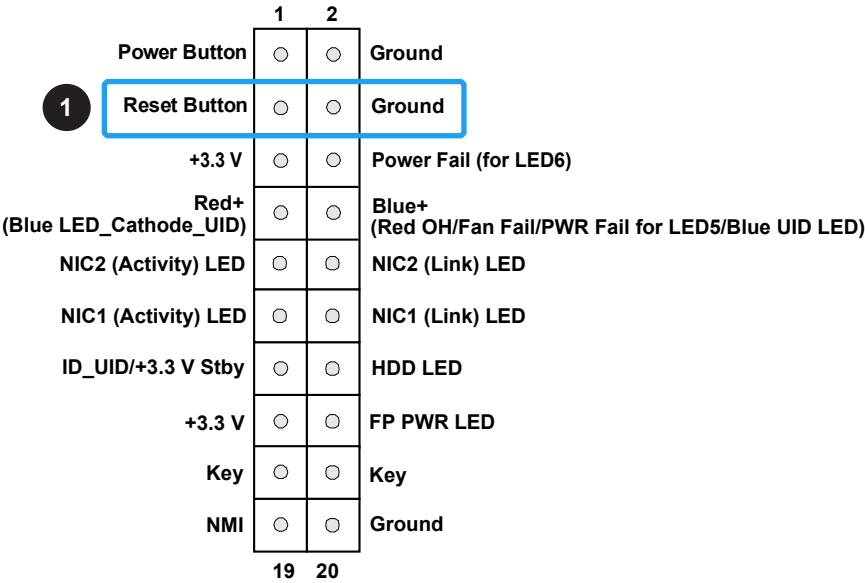


Figure 2-77: Reset Button Pins

Power Fail LED

The Power Fail LED connection is located on pins 5–6 of JF1. When this LED turns solid red, it indicates a power failure. Refer to the table for pin definitions.

Power Fail LED Pin Definitions (JF1)	
Pin#	Definition
5	+3.3 V
6	PWR Fail for LEDPWR (Solid Red On: PWR Failure)

1. Power Fail LED

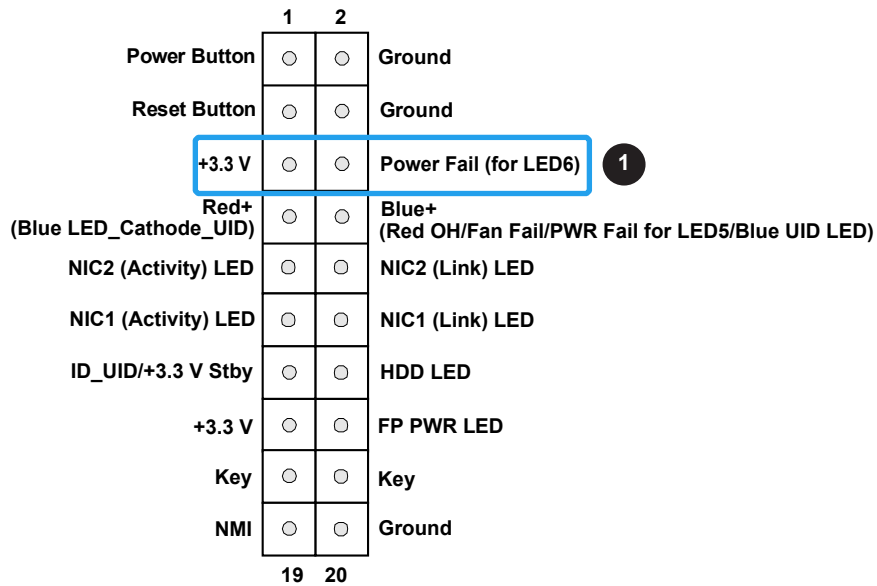


Figure 2-78: Power Fail LED Pins

Information LED (OH/Fan Fail/PWR Fail/UID LED)

The Information LED (OH/Fan Fail/PWR Fail/UID LED) connection is located on pins 7–8 of JF1. The LED on pin 7 is active when the UID button (JUIDB1) on the I/O panel is pressed. The LED on pin 8 provides warnings of overheating, power failure, or fan failure. Refer to the table for more information.

Information LED-Blue+ (OH/Fan Fail/PWR Fail LED/Blue UID LED) (Pins 7–8 of JF1) LED Indicator Status	
Status	Description
Solid Red (On)	An overheating has occurred.
Blinking Red (1 Hz)	Fan failure: Check for an inoperative fan.
Blinking Red (0.25 Hz)	Power failure: Check for a non-operational power supply.
Blinking Red (10 Hz) (FP Red LED)	CPLD recovery mode error(s).
Solid Blue	Local UID is activated. Use this function to locate a unit in a rack mount environment that might be in need of service.
Blinking Blue (1 Hz)	Remote UID is on. Use this function to identify a unit from a remote location that might be in need of service.
BIOS/BMC Blinking Blue (10 Hz)	BIOS/BMC: Recovery and/or update in progress.
Red Info LED Blinking (10 Hz) and MB UID LED Blue Blinking (10 Hz)	CPLD: Recovery and/or update in progress.

1. Information LED

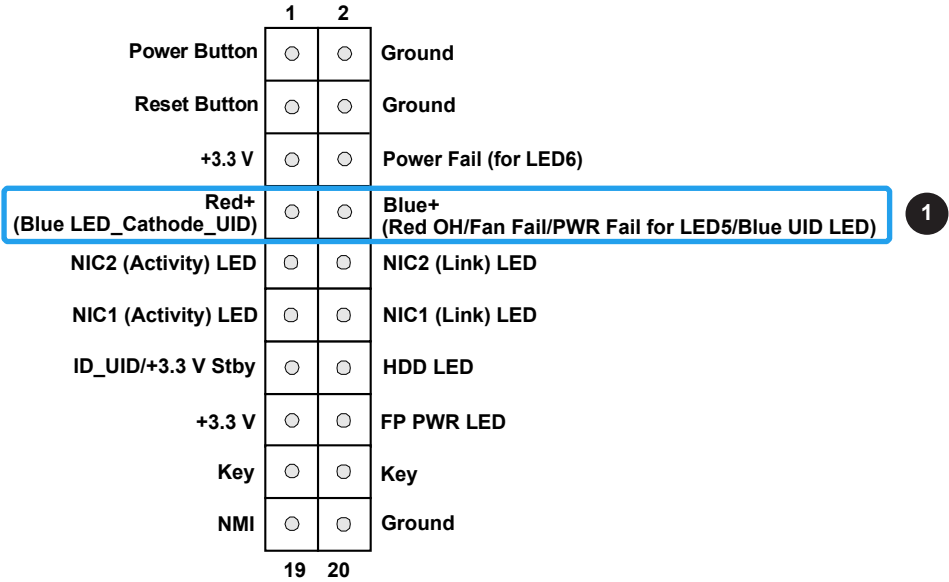


Figure 2-79: Information LED Pins

NIC1/NIC2 (LAN1/LAN2)

The Network Interface Controller (NIC) LED connection for LAN port 1 is located on pins 11–12 of JF1, and LAN port 2 is on pins 9–10. Refer to the tables for pin definitions.

LAN1/LAN2 LED Pin Definitions (JF1)			
Pin#	Definition	Pin#	Definition
9	NIC 2 Activity LED	10	NIC 2 Link LED
11	NIC 1 Activity LED	12	NIC 1 Link LED

LAN1/LAN2 LED LED Indicator Status	
Color	State
NIC 2: Blinking Green	LAN 2: Active
NIC 1: Blinking Green	LAN 1: Active

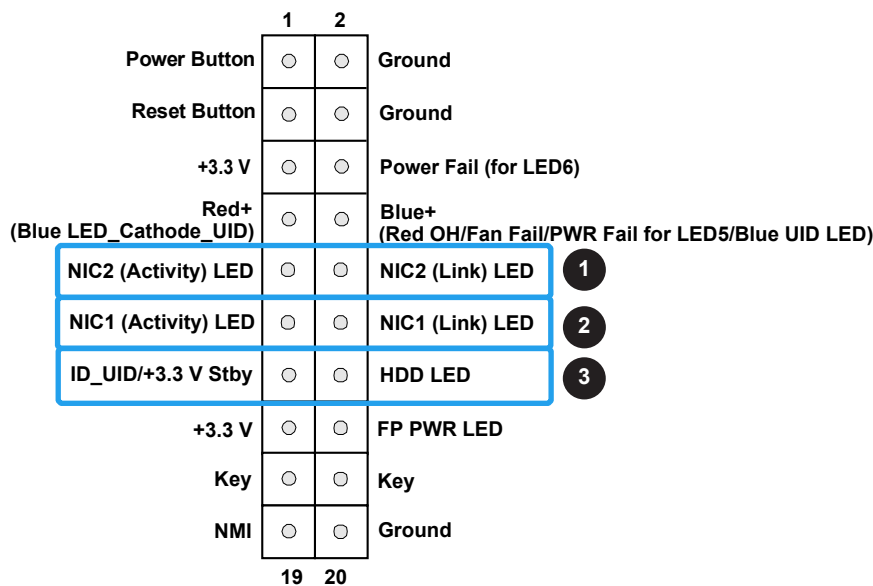
ID_UID Button/HDD LED

The UID Button/HDD LED connection is located on pins 13–14 of JF1. The UID Button is used for a chassis that supports a front UID Button. The front UID Button functions in the same way as the rear UID Button; both are for input only and cannot be used for output.

When this LED is blinking green, it indicates HDD is active. Attach a cable to pins 13–14 to show ID_UID status and hard drive activity. Refer to the tables for pin definitions.

ID_UID/HDD LED Pin Definitions (JF1)	
Pins	Definition
13	ID_UID/+3.3 V Stdby
14	HDD Activity

ID_UID/HDD LED Pin Definitions (JF1)	
Color	State
Blinking Green	HDD Active



1. NIC2 (LAN 2) LED

2. NIC1 (LAN 1) LED

3. ID_UID/HDD LED

Figure 2-80: NIC2, NIC1, and HDD LED Pins

Front Panel Power LED

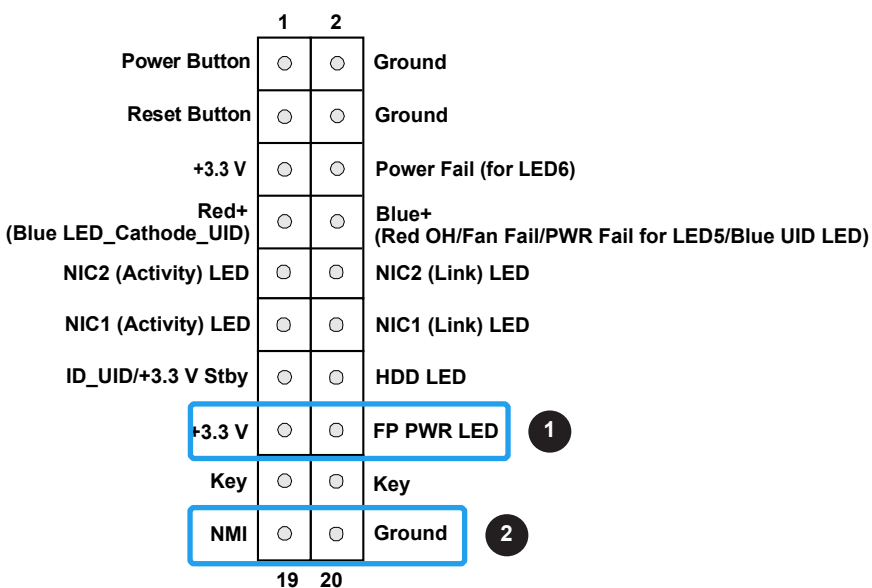
The Front Panel Power LED connection is located on pins 15–16 of JF1. Refer to the table for pin definitions.

FP Power LED Pin Definitions (JF1)	
Pins	Definition
15	+3.3 V
16	FP PWR LED

NMI Button

The non-maskable interrupt (NMI) button header is located on pins 19–20 of JF1. Refer to the table for pin definitions.

NMI Button Pin Definitions (JF1)	
Pins	Definition
19	NMI
20	GND

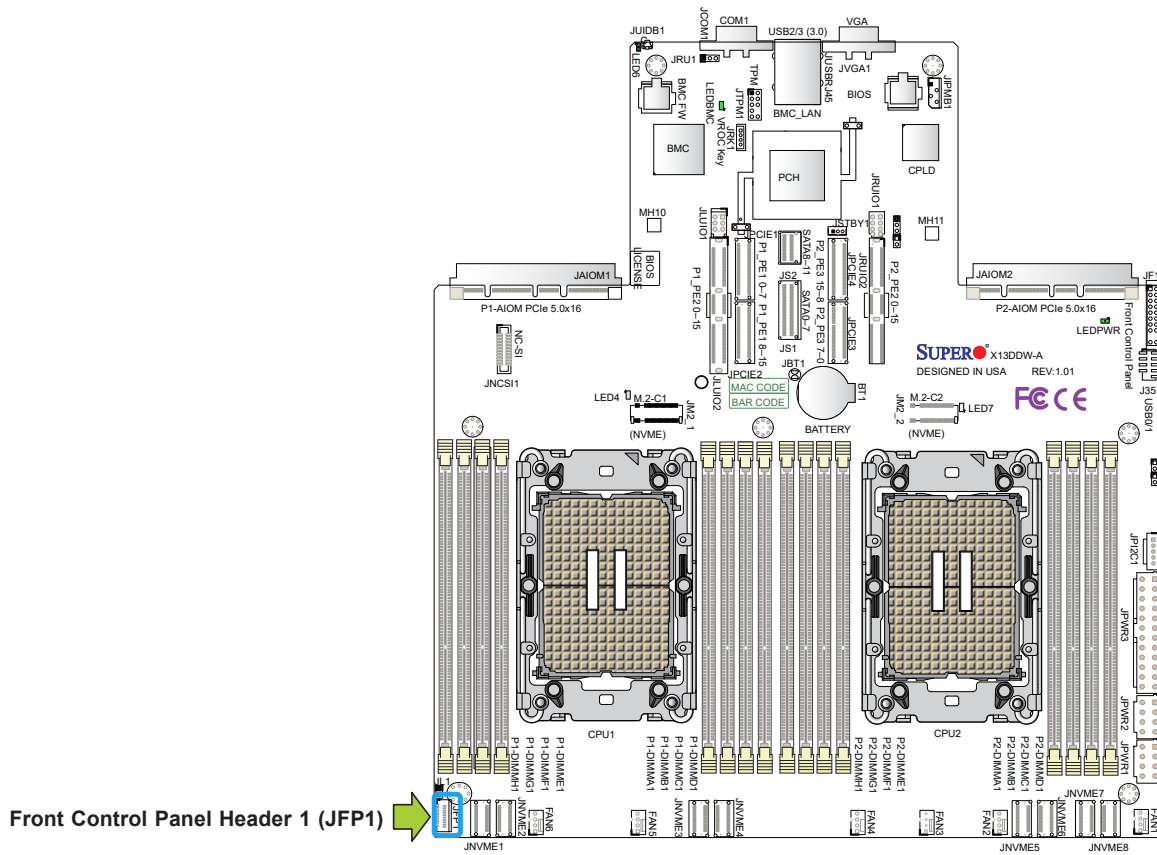


1. FP PWR LED

2. NMI

Figure 2-81: FP PWR LED and NMI Pins

2. Front Control Panel Header (JFP1)



1	○	Power Button
2	○	UID Button
3	○	UID LED_N
4	○	Fail LED_N (OH/FF/PF)
5	○	LAN-2 Activity LED
6	○	LAN-1 Activity LED (Aggregate All LAN)
7	○	HDD Activity LED
8	○	Standby LED_N
9	○	Power/RoT LED_N
10	○	P3V3_STBY
11	○	GND
12	○	I2C Data
13	○	I2C Clock
14	○	GND
15	○	Power Fail LED_P
16	○	P5V_USB
17	○	P5V_USB
18	○	P5V_USB
19	○	Power Fail LED_N
20	○	GND

Figure 2-83: JFP1 Header Pins

Power On and BMC/BIOS Status LED Button

The Power On and BMC/BIOS Status LED button is located on pin 1 of the front control panel header located at JFP1. Momentarily contacting pin 1 of JFP1 will power on/off the system or display BMC/BIOS status. Refer to the table for more information.

Power Button BMC/BIOS Status LED Indicator	
Status	Event
Green: Solid On	System Power On
BMC/BIOS Blinking Green at 4 Hz	BMC/BIOS Checking
BIOS Blinking Green at 4 Hz	BIOS Recovery/Update in Progress
BMC Blinking Red x2 (Two Blinks Red) at 4 Hz, One Pause at 2 Hz (On-On-Off-Off)	BMC Recovery/Update in Progress
BMC/BIOS Blinking Green at 1 Hz	Flash not detected or golden image checking failure

1. Power On Button

1	○	Power Button	1
2	○	UID Button	
3	○	UID LED_N	
4	○	Fail LED_N (OH/FF/PF)	
5	○	LAN-2 Activity LED	
6	○	LAN-1 Activity LED (Aggregate All LAN)	
7	○	HDD Activity LED	
8	○	Standby LED_N	
9	○	Power/RoT LED_N	
10	○	P3V3_STBY	
11	○	GND	
12	○	I2C Data	
13	○	I2C Clock	
14	○	GND	
15	○	Power Fail LED_P	
16	○	P5V_USB	
17	○	P5V_USB	
18	○	P5V_USB	
19	○	Power Fail LED_N	
20	○	GND	

Figure 2-84: Power On Button Pin

Front UID Button

The Front UID button is located on pin 2 of JFP1, which is used in conjunction with the Front UID Button Select jumper located at JRU1. To set Pin 2 of JFP1 for use as the Front UID button, close pins 2–3 of Jumper JRU1. This will be the default setting. Refer to the jumper section for more information and the layout for the location of JRU1.

Power and Front UID Button Select Jumper (JRU1) Jumper Settings	
State	Description
Close pins 2–3 of JRU1	Pin 2 of JFP1: Used as a Front UID (Default)

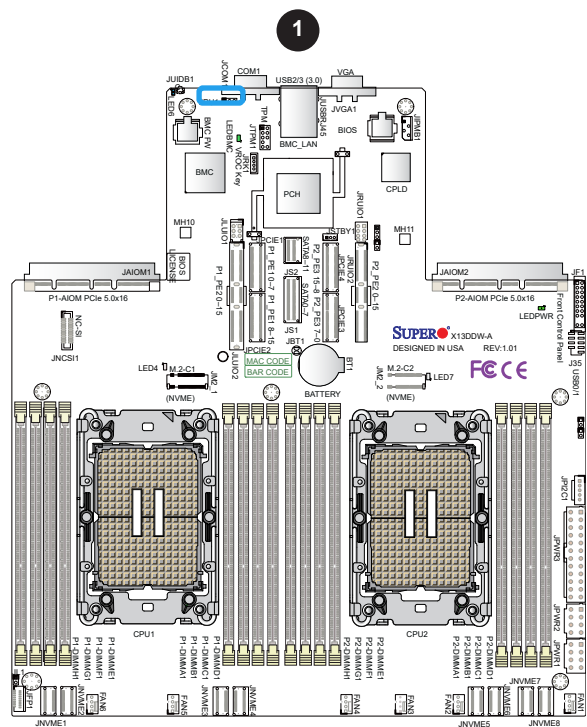
1	○	Power Button
2	○	UID Button
3	○	UID LED_N
4	○	Fail LED_N (OH/FF/PF)
5	○	LAN-2 Activity LED
6	○	LAN-1 Activity LED (Aggregate All LAN)
7	○	HDD Activity LED
8	○	Standby LED_N
9	○	Power/RoT LED_N
10	○	P3V3_STBY
11	○	GND
12	○	I2C Data
13	○	I2C Clock
14	○	GND
15	○	Power Fail LED_P
16	○	P5V_USB
17	○	P5V_USB
18	○	P5V_USB
19	○	Power Fail LED_N
20	○	GND

1
2

1. Power On Button

2. UID Button Connection

Figure 2-85: JFP1 Header Pins



1. JRU1

Figure 2-86: JRU1 Location

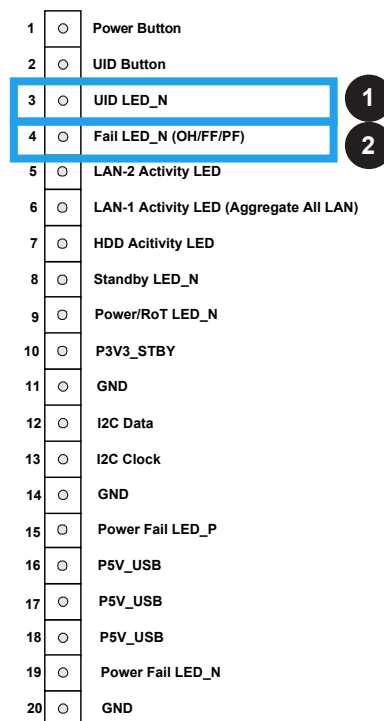
UID LED

The unit identifier LED connection is located on Pin 3 of JFP1. See the following figure for more information on JFP1.

Fail LED (Information LED for OH/FF/PF)

The Fail LED (Information LED for OH/Fan Fail/PWR Fail) connection is located on Pin 4 of JFP1. The LED provides warnings of overheating, power failure, or fan failure. Refer to the following figure for more information.

Fail LED (Information LED) (OH/Fan Fail/PWR Fail) LED States	
Status	Description
Solid Red (On)	An overheating condition has occurred.
Blinking Red (1 Hz)	Fan failure: Check for an inoperative fan.
Blinking Red (0.25 Hz)	Power failure: Check for a non-operational power supply.
Blinking Red (10 Hz) (FP Red LED)	CPLD recovery mode error(s).
Solid Blue	UID has been activated locally. Use this function to locate a unit in a rack mount environment that might be in need of service.
Blinking Blue (1 Hz)	Local UID has been activated locally on. Use this function to identify a unit that might be in need of service.
BIOS/BMC Blinking Blue (10 Hz)	BIOS/BMC: Recovery and/or update in progress.
Red Info LED Blinking (10 Hz) and MB UID LED Blue Blinking (10 Hz)	CPLD: Recovery and/or update in progress.



1. UID LED Indicator
2. Fail LED (Information LED for OH/FF/PF)

Figure 2-87: UID LED Indicator and Fail LED Pins

LAN1/LAN2 (NIC1/NIC2)

The switch LED connection for LAN Port 1 is located on Pin 6 of JFP1, and LAN Port 2 is on Pin 5. Refer to the table.

LAN1/LAN2 LED LED States	
Color	State
NIC 2: Blinking green	LAN 2: Active
NIC 1: Blinking green	LAN 1: Active

HDD Activity LED

The HDD activity LED connection is located on Pin 7 of JFP1. When this LED is blinking green, it indicates HDD activity. Refer to the table.

HDD LED LED State	
Color	State
Blinking Green	HDD Active

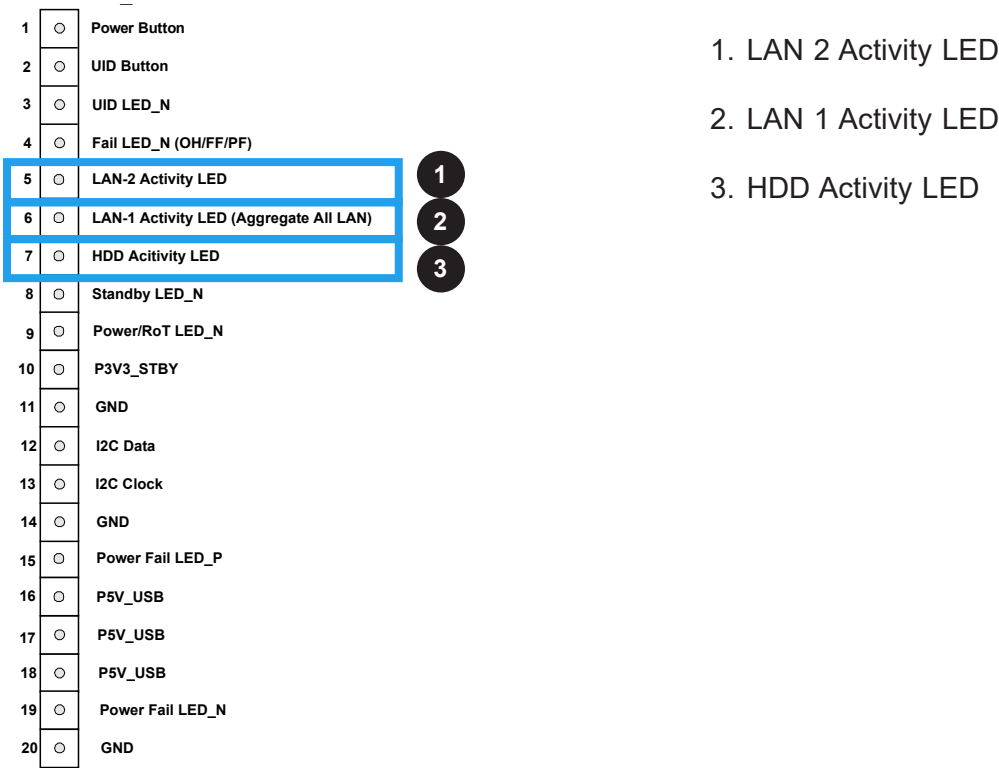


Figure 2-88: LAN2 Activity LED, LAN1 Activity LED, and HDD Activity LED Pins

Standby Power LED

The LED indicator for standby power is located on Pin 8 of JFP1. If this LED is on, standby power is on.

Root of Trust (RoT) Power LED

The Power LED for Root of Trust (RoT) connection is located on Pin 9 of JFP1. If this LED is on, power for the RoT chip is on.

1	○	Power Button
2	○	UID Button
3	○	UID LED_N
4	○	Fail LED_N (OH/FF/PF)
5	○	LAN-2 Activity LED
6	○	LAN-1 Activity LED (Aggregate All LAN)
7	○	HDD Activity LED
8	○	Standby LED_N
9	○	Power/RoT LED_N
10	○	P3V3_STBY
11	○	GND
12	○	I2C Data
13	○	I2C Clock
14	○	GND
15	○	Power Fail LED_P
16	○	P5V_USB
17	○	P5V_USB
18	○	P5V_USB
19	○	Power Fail LED_N
20	○	GND

1. Standby Power LED

2. RoT Power LED

Figure 2-89: Standby Power LED and RoT Power LED Pins

Standby Power

A Standby Power (I²C) connection is located on pins 10–14 of JFP1 to provide power to the system when it is in standby mode. Refer to the table for pin definitions.

+3.3 V Standby PWR Pin Definitions	
Pin#	Definition
10	P3V3 Standby
11	GND
12	I ² C Data
13	I ² C Clock
14	GND

Power Fail LED Indicators

Power Failure LED Indicators are located on pins 15–19 of JFP1. Refer to the table for pin definitions.

FP Power LED Pin Definitions (JFP1)	
Pin#	Definition
15	PWR Failure LED-Positive
19	PWR Failure LED-Negative

1	○	Power Button
2	○	UID Button
3	○	UID LED_N
4	○	Fail LED_N (OH/FF/PF)
5	○	LAN-2 Activity LED
6	○	LAN-1 Activity LED (Aggregate All LAN)
7	○	HDD Activity LED
8	○	Standby LED_N
9	○	Power/RoT LED_N
10	○	P3V3_STBY
11	○	GND
12	○	I2C Data
13	○	I2C Clock
14	○	GND
15	○	Power Fail LED_P
16	○	P5V_USB
17	○	P5V_USB
18	○	P5V_USB
19	○	Power Fail LED_N
20	○	GND

1. (+3.3 V) Standby Power
2. PWR Fail LED (Positive)
3. PWR Fail LED (Negative)

Figure 2-90: Standby Power, PWR Fail LED, and PWR Fail LED Pins

FP USB Power

Front Panel USB power connections are located on pins 16–18 of JFP1 to provide power to front USB devices. Refer to the table for definitions.

FP USB PWR Pin Definitions	
Pin#	Definition
16	+5 V USB PWR
17	
18	

1	○	Power Button
2	○	UID Button
3	○	UID LED_N
4	○	Fail LED_N (OH/FF/PF)
5	○	LAN-2 Activity LED
6	○	LAN-1 Activity LED (Aggregate All LAN)
7	○	HDD Activity LED
8	○	Standby LED_N
9	○	Power/RoT LED_N
10	○	P3V3_STBY
11	○	GND
12	○	I2C Data
13	○	I2C Clock
14	○	GND
15	○	Power Fail LED_P
16	○	P5V_USB
17	○	P5V_USB
18	○	P5V_USB
19	○	Power Fail LED_N
20	○	GND

1. FP USB Power

Figure 2-91: FP USB Power Pins

2.7 Connectors and Headers

Power Connections

ATX Power Supply Connector

The 24-pin power supply connector (JPWR3) meets the ATX SSI EPS +12 V specification. You must also connect the 8-pin +12 V DC power connectors (JPWR1/JPWR2) to the power supply to provide adequate power to your system.



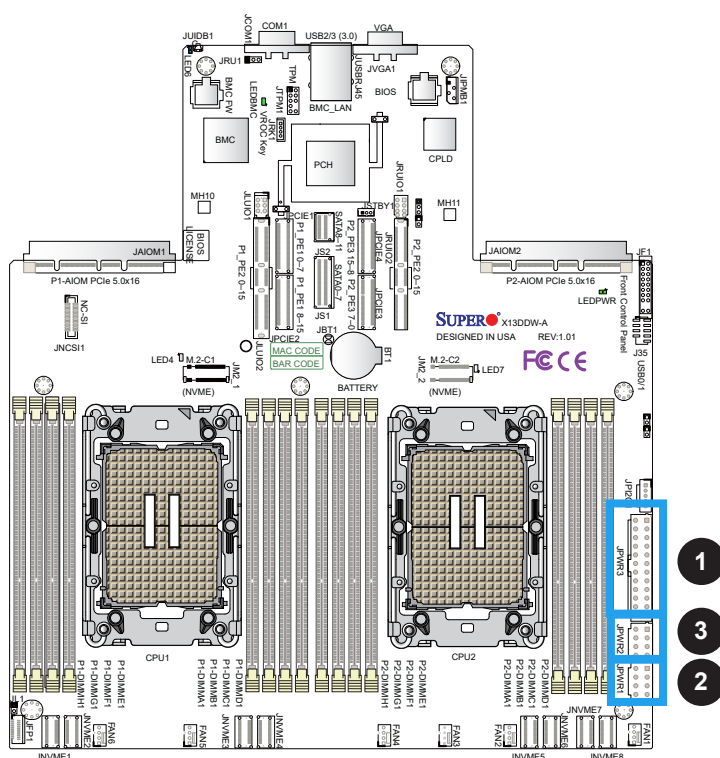
Important: To provide an adequate power supply to the motherboard, be sure to connect the 24-pin ATX PWR and the 8-pin PWR connectors to the power supply. Failure to do so may void the manufacturer's warranty on your power supply and motherboard.

+12 V 8-Pin Power Pin Definitions	
Pin#	Definition
1–4	GND
5–8	+12 V

Required Connection

ATX Power 24-Pin Connector Pin Definitions			
Pin#	Definition	Pin#	Definition
13	++3.3 V	1	++3.3 V
14	NC	2	++3.3 V
15	GND	3	GND
16	PS_ON	4	+5 V
17	GND	5	GND
18	GND	6	+5 V
19	GND	7	GND
20	Res (NC)	8	PWR_OK
21	+5 V	9	5VSB
22	+5 V	10	+12 V
23	+5 V	11	+12 V
24	GND	12	++3.3 V

Required Connection

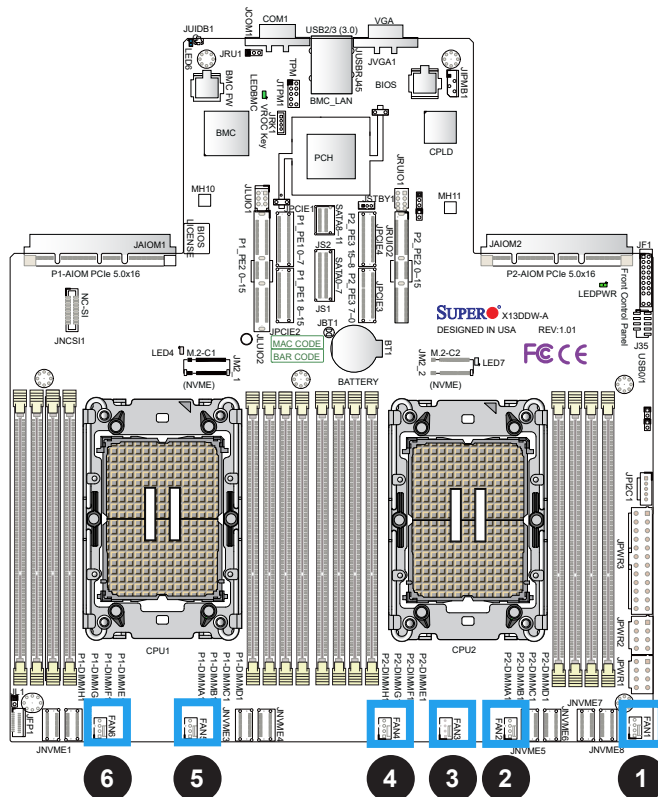


1. JPWR3: 24-Pin ATX PWR
2. JPWR1: 8-Pin PWR
3. JPWR2: 8-Pin PWR

Headers

Fan Headers

There are six 4-pin fan headers (FAN1–FAN6) used for your system cooling fans. Fan speed control for these fans is supported by Thermal Management via BMC 2.0 interface. Refer to the layout for the locations of the fan headers.



1. FAN1
2. FAN2
3. FAN3
4. FAN4
5. FAN5
6. FAN6

TPM/Port 80 Header

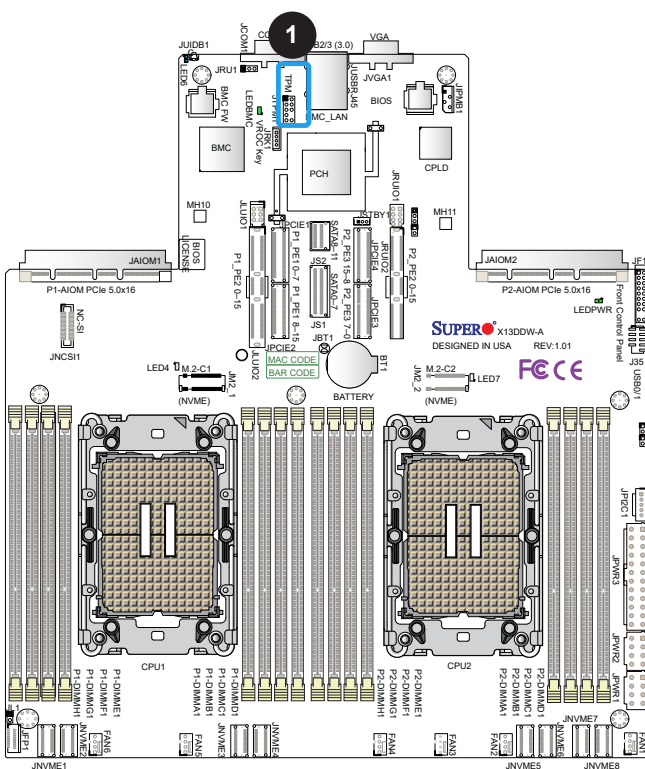
The JTPM1 header is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from Supermicro (optional). A TPM/Port 80 connector is a security device that supports encryption and authentication in hard drives. It allows the motherboard to deny access if the TPM, which is associated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



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

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

1. TPM Header



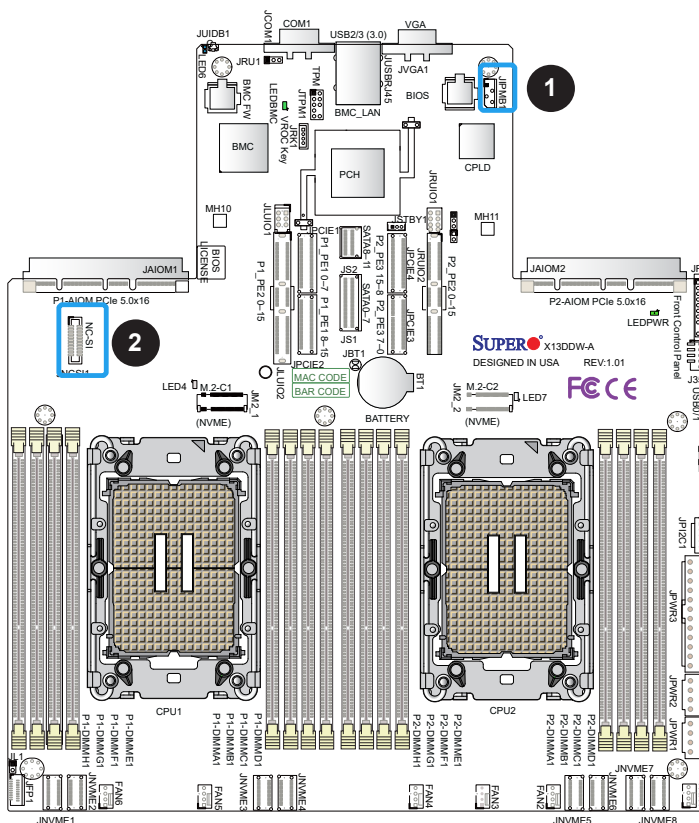
Four-Pin BMC External I²C Header

A System Management Bus header for the BMC is located at JIPMB1. Connect the appropriate cable here to use the IPMB I²C connection on your system. Refer to the layout for the location of JIPMB1.

NC-SI Connector

The Network Controller Sideband Interface (NC-SI) connector is located at (JNC SI1). This connector is used to connect a Network Interface Card (NIC) to the motherboard to allow the onboard BMC to communicate with a network.

Note: For detailed instructions on how to configure Network Interface Card (NIC) settings, refer to the Network Interface Card Configuration User's Guide posted on the web page under the link: <https://www.supermicro.com/support/manuals/>.



1. BMC External Header

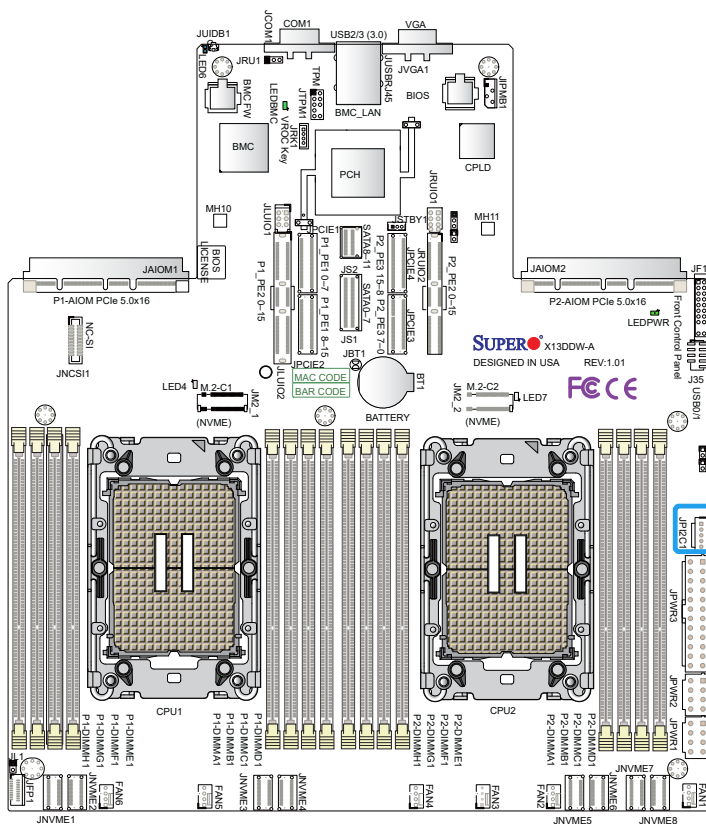
2. NC-SI Connector (JNC SI1)

Power SMB (I²C) Header

The Power System Management Bus (I²C) connector (JPI²C1) monitors the power supply, fan, and system temperatures. Refer to the table for pin definitions.

Power SMB Header Pin Definitions	
Pin#	Definition
1	Clock
2	Data
3	PMBUS_Alert
4	GND
5	++3.3 V

1. Power I²C1 Header (JPI²C1)



A Chassis Intrusion header is located at JL1 on the motherboard. Attach the appropriate cable from the chassis to inform you when the chassis is opened. Refer to the table for pin definitions.

- 1

VROC RAID Key Header

An Intel VROC RAID Key header is located at JRK1 on the motherboard. Install a VROC RAID Key on JRK1 for NVMe RAID support as shown in the illustration. Refer to the layout for the location of JRK1.

 **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 link: <https://www.supermicro.com/support/manuals/>.

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

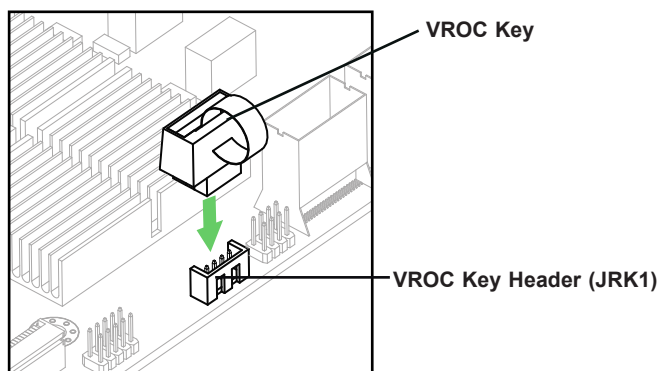
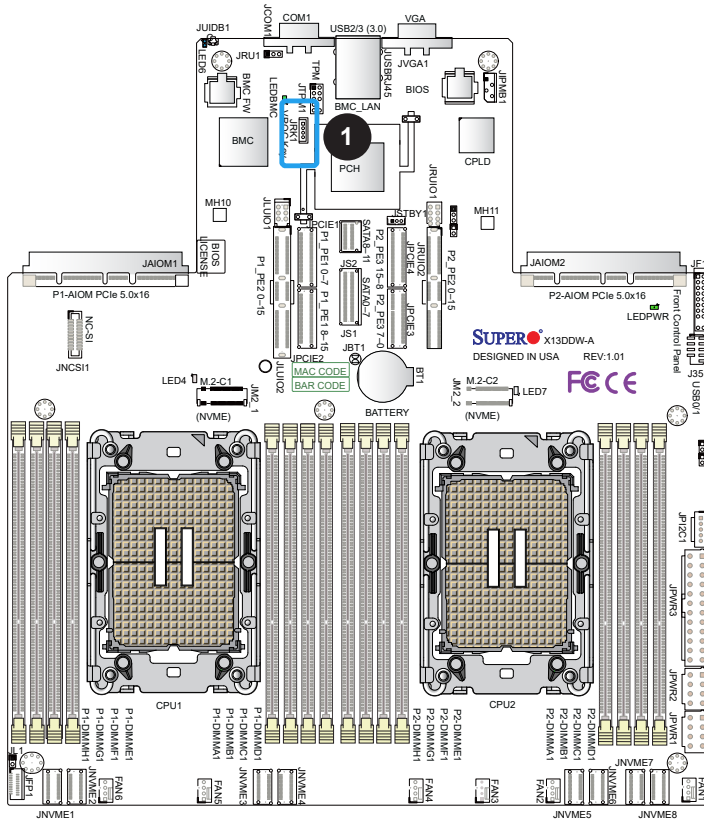


Figure 2-98: VROC RAID Key and Key Header

1. VROC RAID Key (JRK1)

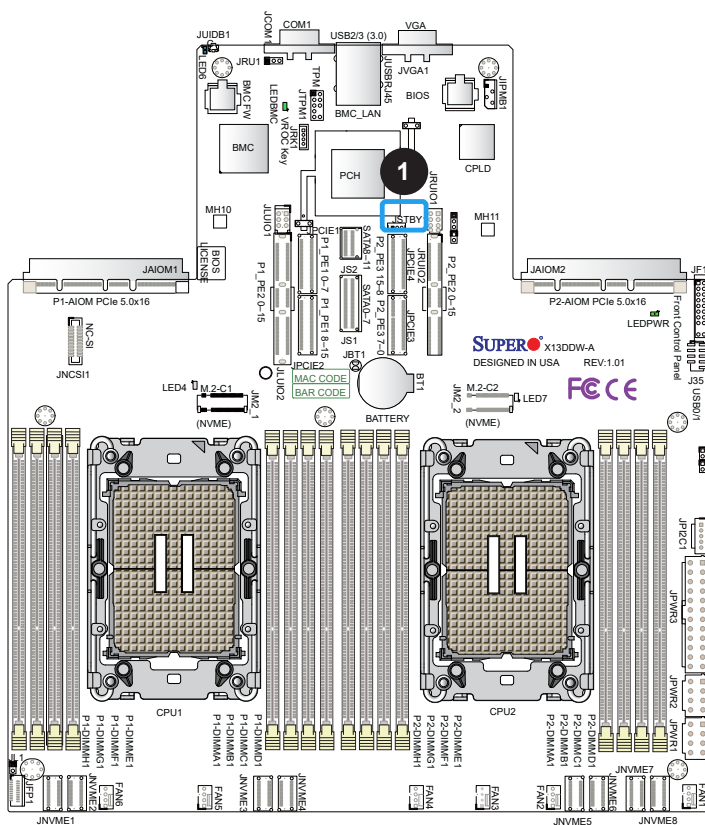


Standby Power

The Standby Power header is located at JSTBY1 on the motherboard. You must have a card with a Standby Power connector and a cable to use this feature. Refer to the table for pin definitions.

Standby Power Pin Definitions	
Pin#	Definition
1	+5 V Standby
2	GND
3	No Connection

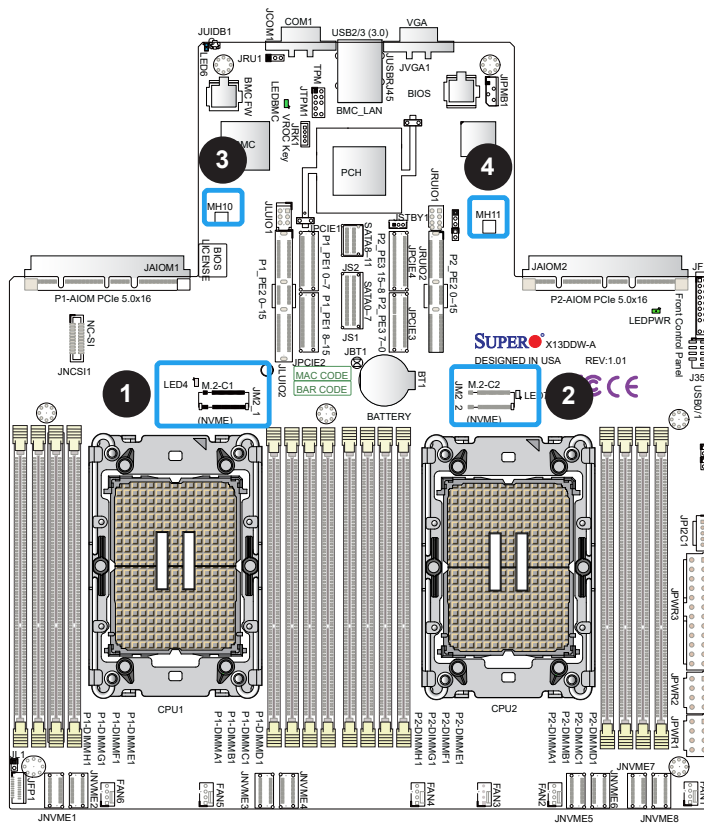
1. Standby Power



M.2-C1/M.2-C2 M-Key Slots (for NVMe Only)

Two M.2 slots are located at M.2-C1 and M.2-C2 on the motherboard. These M.2 slots support PCIe 5.0 x4 M.2 NVMe devices in the 2280 form factor. M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. Note that two M.2 mounting holes, located at MH10/MH11, are provided for proper M.2 device installation. Refer to the layout for the locations of the M.2-C1/M.2-C2 and the mounting holes located at MH10/MH11.

1. M.2-C1 Slot
2. M.2-C2 Slot
3. MH10: (M.2-C1 Mounting Hole)
4. MH11: (M.2-C2 Mounting Hole)

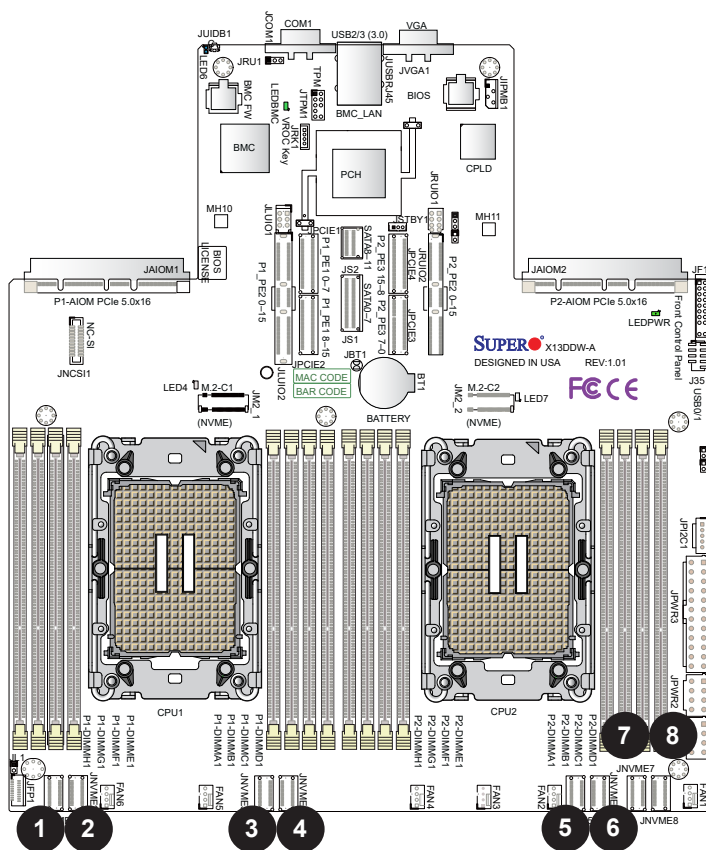


MCIO NVMe Connectors

MCIO NVMe connectors, located at JNVME1 through JNVME4 and JNVME5 through JNVME8, provide eight PCIe 5.0 x4 or four PCIe 5.0 x8 MCIO NVMe connections on the motherboard. JNVME1–4 connections are supported by CPU1, and JNVME5 to JNVME8 connections, CPU2. Use these MCIO connectors to support high-speed PCIe NVMe storage devices.

Note 1: When installing an NVMe device on a motherboard, be sure to connect the first NVMe port (JNVME1) first for your system to work properly.

Note 2: This motherboard supports eight 5.0 x4, four 5.0 x8 MCIO NVMe connections, and up to 12 NVMe connectors if an S12 (12" x 3.5") backplane is used.

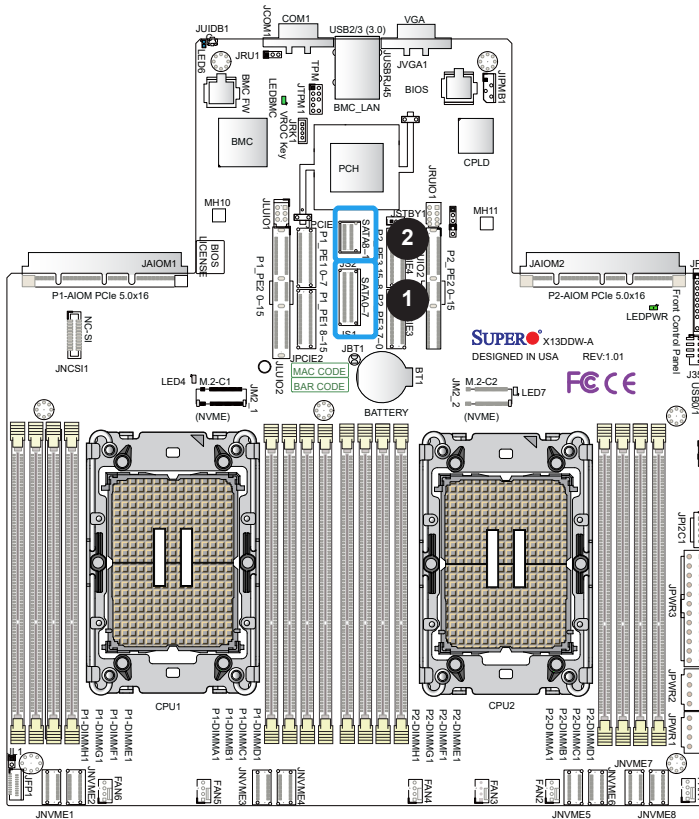


1. P1_PE4 0–3 (JNVME1)
2. P1_PE4 4–7 (JNVME2)
3. P1_PE4 8–11 (JNVME3)
4. P1_PE4 12–15 (JNVME4)
5. P2_PE5 0–3 (JNVME5)
6. P2_PE5 4–7 (JNVME6)
7. P2_PE5 8–11 (JNVME7)
8. P2_PE5 12–15 (JNVME8)

SATA 0–7/SATA 8–11 Ports

Two SATA 3.0 headers, located at JS1 and JS2, support 12 SATA connections (SATA0–7/SATA8–11) on the motherboard. These SATA 3.0 ports are supported by the Intel PCH chip. Connecting proper SATA cables to JS1 and JS2 to use SATA 3.0 connections.

1. SATA0–7 (JS1)
2. SATA8–11 (JS2)



2.8 Jumper Settings

How Jumpers Work

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

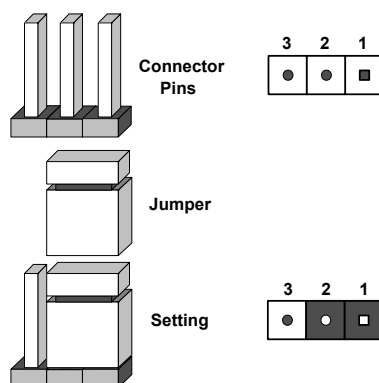


Figure 2-104: Three-Pin Jumpers

CMOS Clear

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

To Clear CMOS

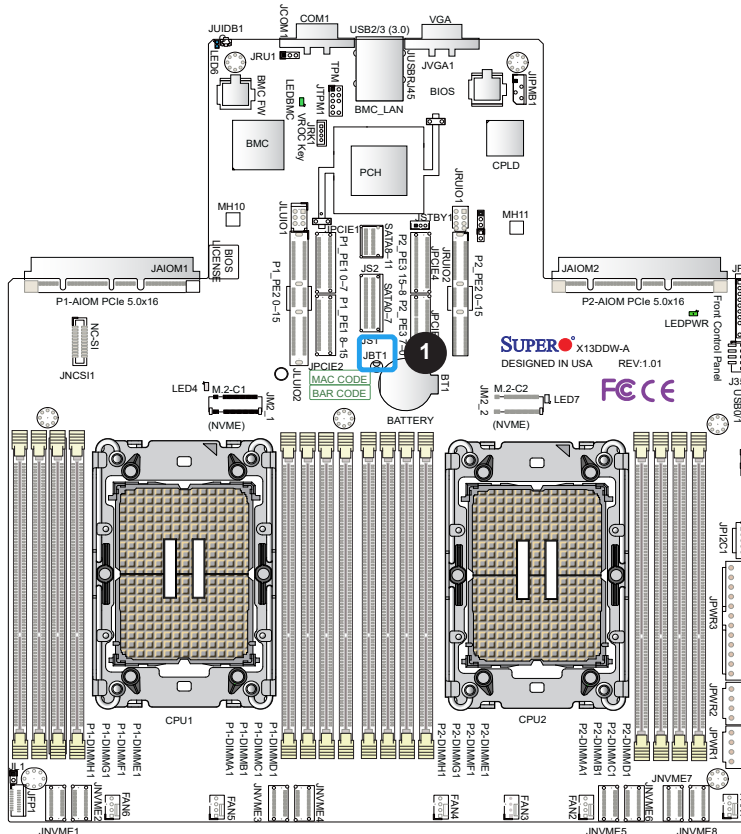
1. Power down the system and unplug the power cord(s).
2. Remove the cover of the chassis to access the motherboard.
3. Remove the battery from the motherboard.
4. Short the CMOS pad (JBT1) with a metal object such as a small screwdriver for at least four seconds.
5. Remove the screwdriver (or shorting device).
6. Replace the cover, reconnect the power cord(s), and power on the system.



Note 1: Clearing CMOS will also clear all passwords.

Note 2: Do not use the PW_ON connector to clear CMOS.

1. JBT1 (Clear CMOS)



Front UID Button Select

Jumper JRU1 can be used to set pin 2 of the Front Control Panel header 1 (JFP1) to function as the Front UID button. Close pins 2–3 of Jumper JRU1 to configure pin 2 of JFP1 for the Front UID button use in a chassis that supports the front UID connection. Refer to the figure for JFP1 pin definitions, and refer to the table for JRU1 settings.

Front UID Button Select Jumper (JRU1) Jumper Settings	
State	Description
Close pins 2–3 of JRU1	Pin 2 of JFP1: Used as a front UID button (Default)

1. JRU1

2. UID Button

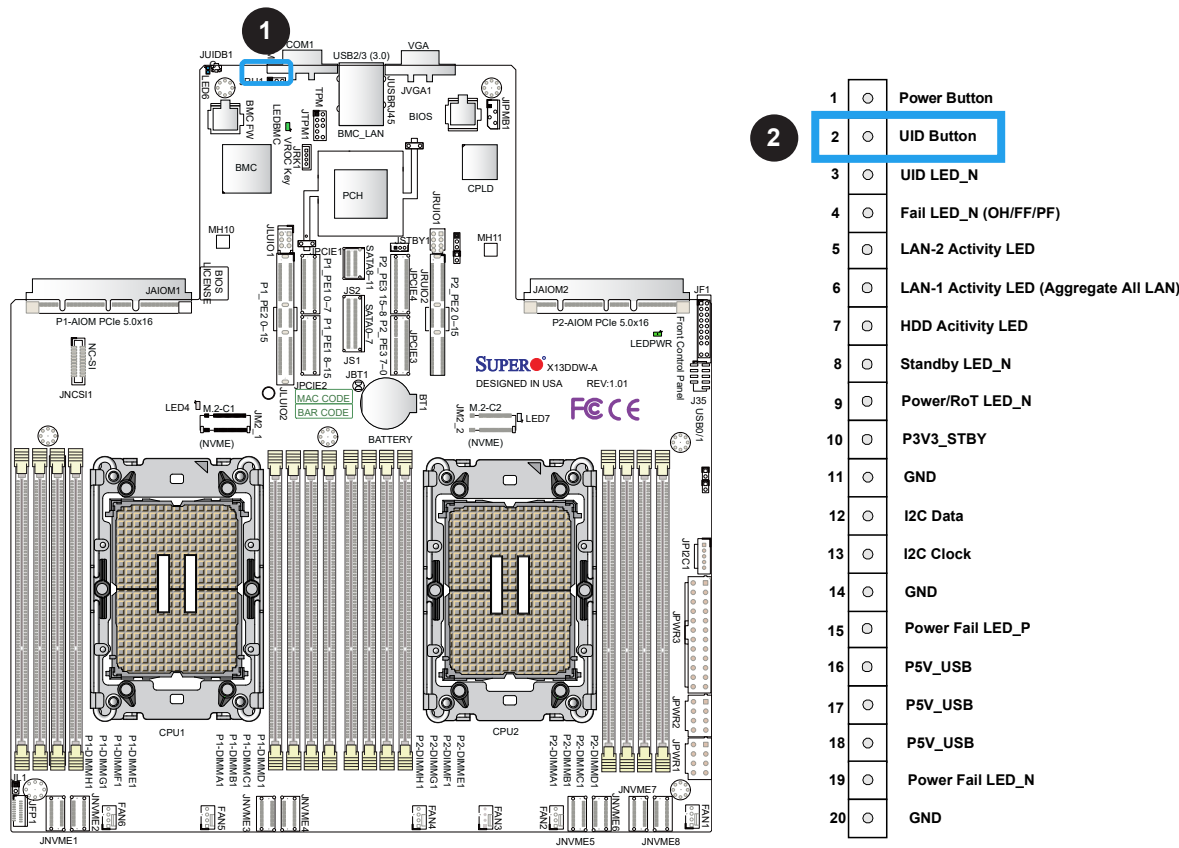


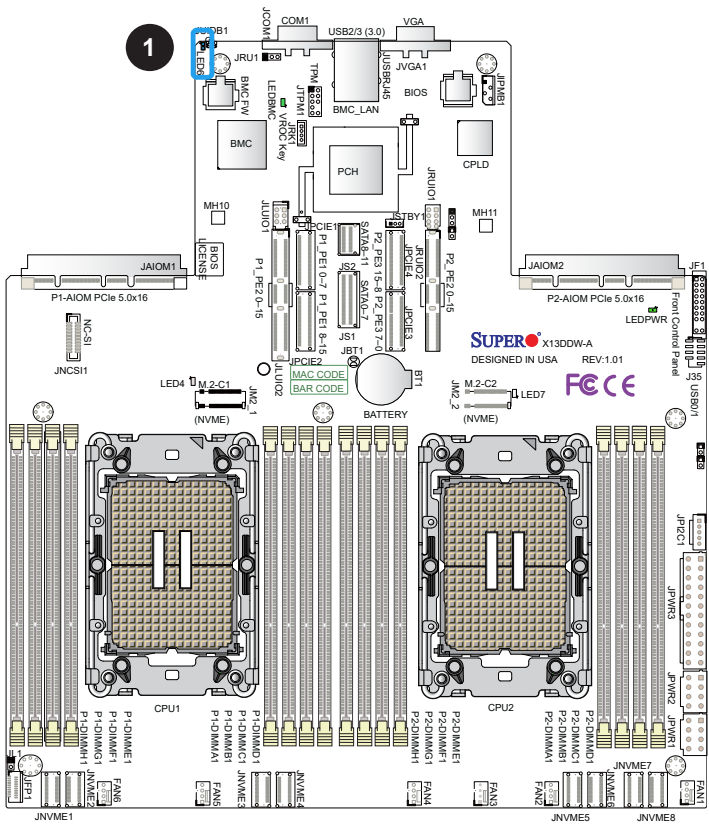
Figure 2-107: UID Button

Unit ID LED (UID LED)

The front UID LED indicator is located at LED6. This UID indicator provides easy identification of a system that may need service.

UID LED LED Indicator	
LED Color	Definition
Blue: On	System Identified

1. UID LED (LED6)

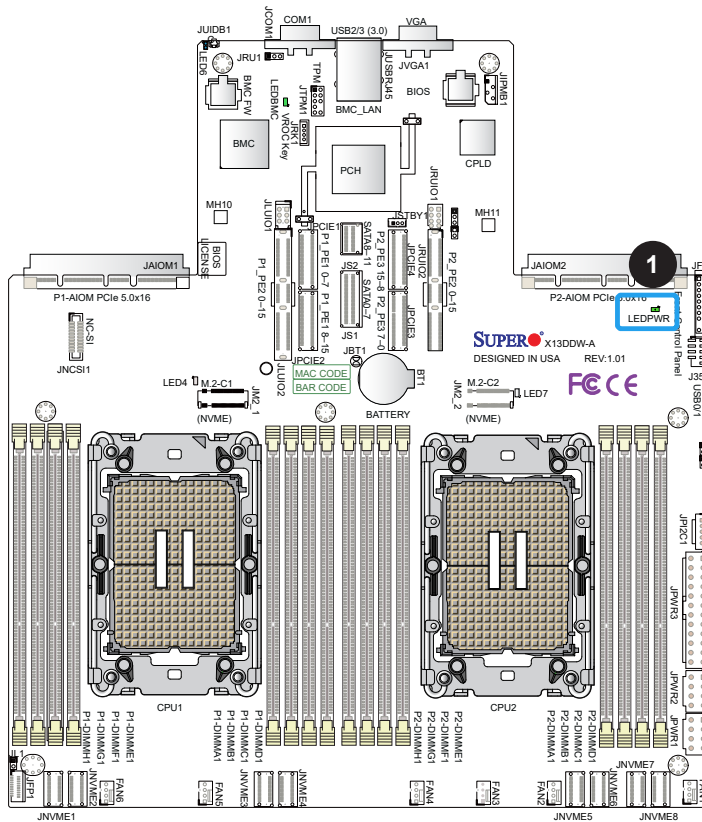


Onboard Power LED

The Onboard Power LED is located at LEDPWR on the motherboard. When this LED is on, the system power is on. Be sure to turn off the system power and unplug the power cords before removing or installing components. Refer to the table for more information.

Onboard Power LED Indicator	
LED Color	Definition
Off	System Power Off: Power Cable Not Connected
Green	System Power On

1. Power LED (LEDPWR)

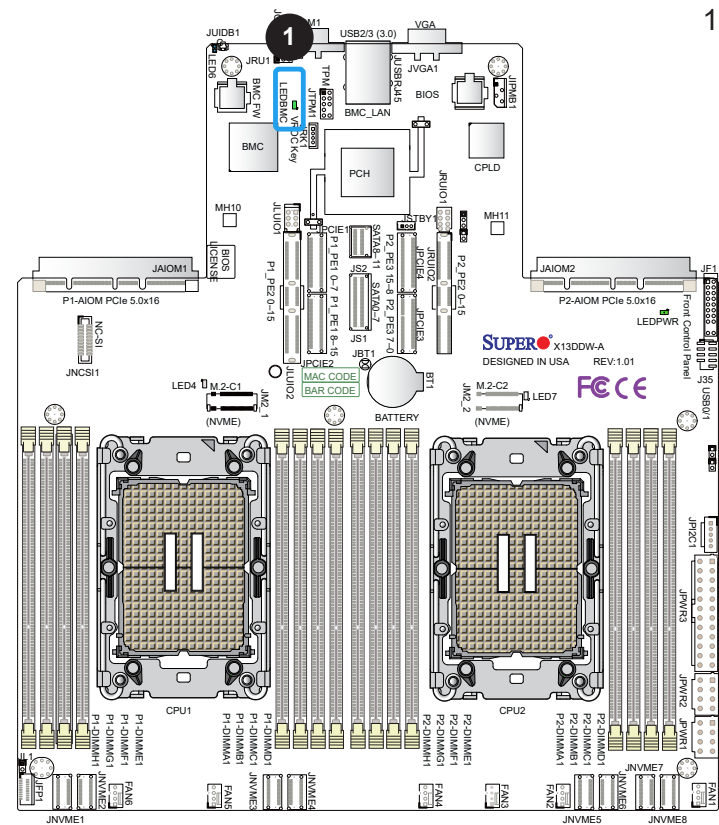


BMC Heartbeat LED

A BMC Heartbeat LED is located at LEDBMC on the motherboard. When LEDBMC is blinking green, the BMC is functioning normally. Refer to the layout for the location of LEDBMC.

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

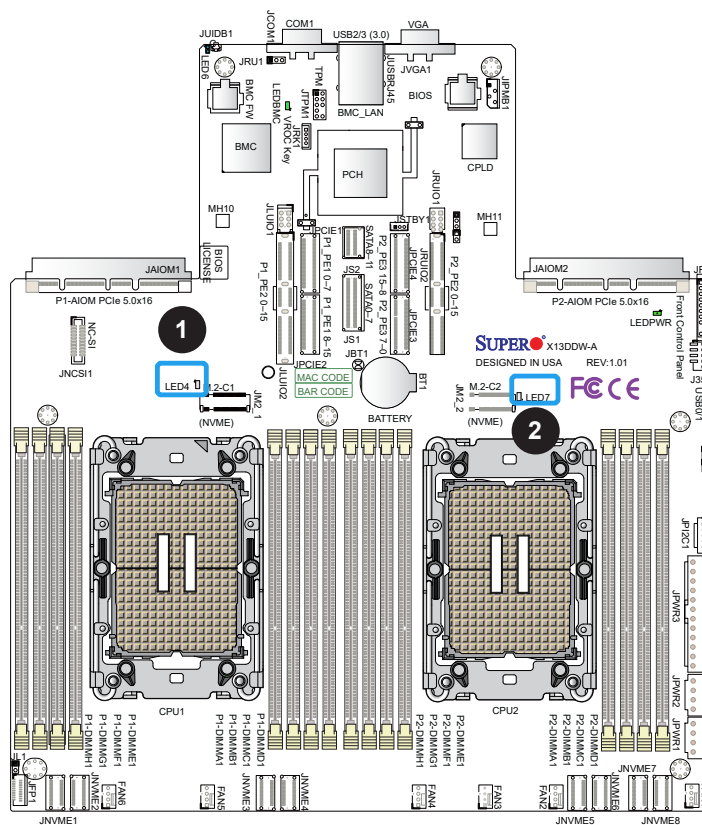
1. BMC Heartbeat LED (LEDBMC)



M.2 LED Indicators

Two M.2 LED indicators are located at LED4 and LED7 on the motherboard. When LED4 is blinking, M.2-C1 functions normally. While LED7 is blinking, M.2-C2 functions properly. Refer to the layout for LED4 and LED7 locations.

M.2 LED Indicators (LED4/LED7)		
LED#	LED Color	State
LED4	Green: Blinking	M.2-C1: M.2 Device Working Properly
LED7	Green: Blinking	M.2-C2: M.2 Device Working Properly



1. LED4 (M.2-C1 LED)

2. LED7 (M.2-C2 LED)

Chapter 3

Troubleshooting

3.1 Troubleshooting Procedures

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

Before Power On

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

No Power

1. Make sure that there are no short circuits between the motherboard and the chassis.
2. The battery on your motherboard may be old. Check to verify that it still supplies 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, check the following:

1. Remove all components from the motherboard, especially the DIMM modules. Power on the system and check if the Power LED (LEDPWR) and the BMC Heartbeat LED (LEDBMC) are on, and the system fans are spinning.
2. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this chapter.

Memory Errors

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMM modules in the system.
3. Make sure that you are using the correct type of ECC DDR5 modules recommended by the manufacturer.
4. Check for bad DIMM modules or slots by swapping a single module among all memory slots and checking the results.

Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to Chapter 1 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.

When the System Becomes Unstable

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

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

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



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

3. HDD Support — Make sure that all hard disk drives (HDDs) work properly. Replace the bad HDDs with good ones.
4. System Cooling — Check the system cooling to make sure that all heatsink fans and CPU/system fans, etc., work properly. Check the hardware monitoring settings in the BMC to make sure that the CPU and system temperatures are within the normal range. Also, check the front panel Overheat LED and make sure that it is not on.
5. Adequate Power Supply — Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Refer to our website for more information on the minimum power requirements.
6. Proper Software Support — Make sure that the correct drivers are used.

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

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

3.2 Technical Support Procedures

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

1. Go through the Troubleshooting Procedures and Frequently Asked Questions (FAQ) sections in this chapter or see the FAQs on our website (<http://www.supermicro.com/FAQ/index.php>) before contacting Technical Support.
2. BIOS upgrades can be downloaded from our website (http://www.supermicro.com/ResourceApps/BIOS_BMC_Intel.html).
3. If you still cannot resolve the problem, include the following information when contacting Supermicro for technical support:
 - Motherboard model and PCB revision number
 - BIOS release date/version (This can be seen on the initial display when your system first boots up.)
 - System configuration
4. An example of a Technical Support form is on our website at <http://www.supermicro.com/RmaForm/>.
5. Distributors: For immediate assistance, have your account number ready when placing a call to our Technical Support department. We can be reached by email at support@supermicro.com.

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: This motherboard supports up to 4 TB 3DS RDIMM/RDIMM DDR5 (288-pin) DDR5 memory with speeds up to 5600 MT/s in 16 DIMM slots. To enhance memory performance, do not mix memory modules of different speeds and sizes. Follow all memory installation instructions given in [Section 2-4](#) in Chapter 2.



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

Question: How do I update my BIOS?

Answer: It is recommended that you do not upgrade your BIOS if you are not experiencing any problems with your system. Updated BIOS files are located on our website at http://www.supermicro.com/ResourceApps/BIOS_BMC_Intel.html. Check our BIOS warning message and the information on how to update your BIOS on our website. Select your motherboard model and download the BIOS file to your computer. Also, check the current BIOS revision to make sure that it is newer than your BIOS before downloading.



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

Note 2: For BIOS Update and Recovery instructions, refer to the Firmware Update and Recovery Instructions for Supermicro's X13 Motherboards User's Guide posted at <https://www.supermicro.com/support/manuals/>.

Note 3: When the BIOS update is in progress, do not reset the BMC firmware.

3.4 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps:

1. Power off your system and unplug your power cable.
2. Locate the onboard battery as shown in the image at the bottom of this page..
3. Using a tool such as a pen or a small screwdriver, push the battery lock outwards to unlock it. Once unlocked, the battery will pop out from the holder.
4. Remove the battery.

Proper Battery Disposal



Warning: Handle 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 the steps:

1. Power off your system and unplug your power cable.
2. Locate the onboard battery as shown in the image at the bottom of this page..
3. Identify the battery's polarity. The positive (+) side should be facing up.
4. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.



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

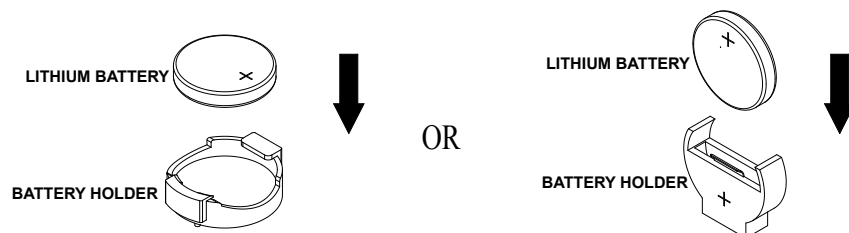


Figure 3-1: Onboard Battery

3.5 Returning Merchandise for Service

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

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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



Note 1: 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 the BIOS that may not be reflected in this manual.

Note 2: When the BIOS update is in progress, do not reset the BMC firmware.

Starting the Setup Utility

To enter the BIOS Setup utility, press the <Delete> key while the system is booting up. In most cases, the <Delete> key is used to invoke the BIOS Setup screen; however, in other cases, other hot keys, such as <F1>, <F2>, may be used for this purpose. Each main BIOS menu option is described in this manual.

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

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

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

4.2 Main Setup

When you first enter the AMI BIOS Setup utility, you will see the Main setup screen. You can always return to the Main setup screen by selecting the Main tab at the top of the screen. The Main BIOS Setup screen will appear as follows:

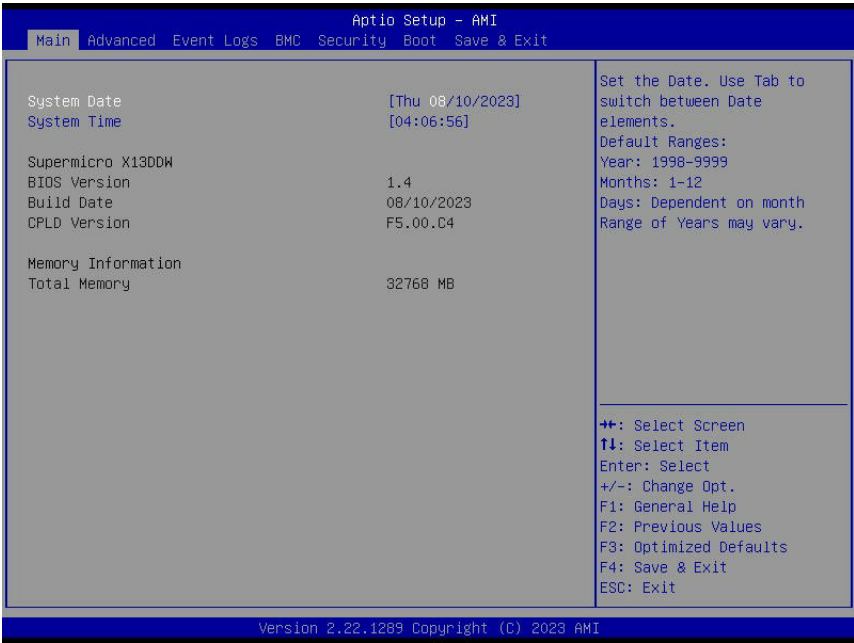


Figure 4-1: Main Page Settings and Options

System Date

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

System Time

This feature displays the current time of the system in operation, which is based on the Real Time Clock (RTC) of the system. The system time is displayed in "HH:MM:SS" format.



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

Supermicro X13DDW

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:

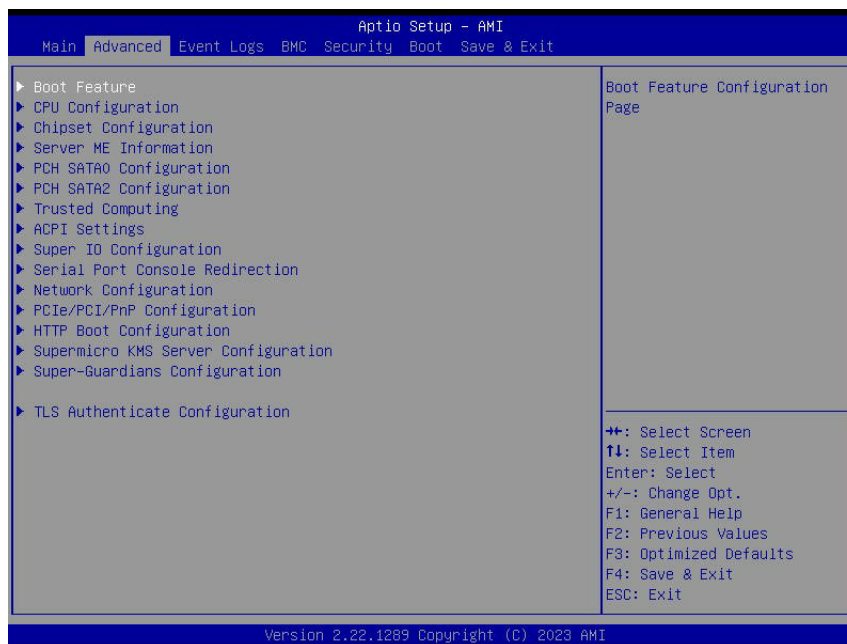


Figure 4-2: Processor Configuration Window

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

► Boot Feature

Quiet Boot

Use this feature to select the screen between displaying Power-on Self Test (POST) messages or the OEM logo at bootup. Select Disabled to display the POST messages. Select Enabled to display the OEM logo instead of the normal POST messages. The options are **Enabled** and Disabled.

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

Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to use the current AddOn ROM display settings. Select Force BIOS to use the Option ROM display mode set by the system BIOS. The options are **Force BIOS** and Keep Current.

Bootup NumLock State

Use this feature to set the Power-on state for the Numlock key. The options are **On** and Off.

Wait For "F1" If Error

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

INT19 Trap Response

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

Re-try Boot

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

Power Configuration

Watch Dog Function

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

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

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

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

Restore on AC Power Loss

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

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

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

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

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

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

Restore on AC Power Loss

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

Power Button Function

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

► CPU Configuration



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

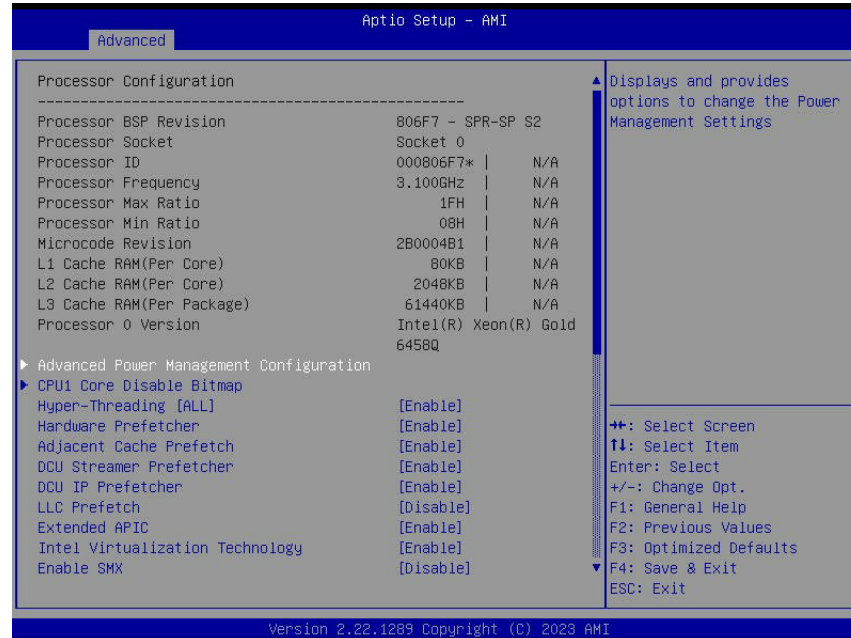


Figure 4-3: Processor Configuration Window

Processor Configuration

The following CPU information is displayed:

- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM (Per Core) / L2 Cache RAM (Per Core)
- L3 Cache RAM (Per Package)
- Processor 0 Version / Processor 1 Version

►Advanced Power Management Configuration

Power Technology

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

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

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

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

Use this feature to configure the proper operation settings 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 Maximum Performance, Performance, **Balanced Performance**, Balanced Power, and Power.



Note: The options of "Extreme Performance" and "Max Power Efficient" will be supported when supported by the motherboard.

Optimized Power Mode

Select Enable to use Optimized Power Mode for optimal power performance. The options are Enable and **Disable**.

► CPU P State Control

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

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

Use this feature to set the appropriate 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. Select Normal for the Intel® AVX feature to operate normally, which will provide a set of instructions to allow Single-Instruction Multiple-Data (SIMD) operations to be performed in Intel processors by adding MMX and SSE support. The options are **Nominal**, Level 1, and Level 2.

Intel Speed Select Technology-Power Profile (SST-PP)

Use this feature to set the appropriate level for Intel SST-PP to operate on. Select Auto to use the lowest level that is supported by the system hardware. The options are **Auto**, Level 0, Level 3, and Level 4.

The following sub-items will display:

- Intel SST-PP
- Capable
- Core Count
- P1 Ration
- 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 **Disable** and **Enable**.

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

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

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

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

► Hardware PM State Control**Hardware P-States**

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

► Frequency Prioritization (Available when the previous item "Hardware P-States" is set to "Native Mode with Legacy Support" or using the Native Mode with No Legacy support)**SST-CP**

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

► CPU C State Control**Enable Monitor MWAIT**

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

CPU C1 Auto Demotion

Select Auto to allow the BIOS to automatically demote the CPU to C1 State. The options are Disable, Enable, and **Auto**. (Be sure to save your settings and reboot the system for the change you've made to take effect.)

CPU C6 Report

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

Enhanced Halt State (C1E)

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

►Package C State Control

Package C State

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

►CPU1 Core Disable Bitmap / CPU2 Core Disable Bitmap

Available Bitmap:

This feature displays the available bitmap.

Disable Bitmap

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

Hyper-Threading [ALL]

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

Hardware Prefetcher

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

Adjacent Cache Prefetch

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

DCU Streamer Prefetcher

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

DCU IP Prefetcher

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

LLC Prefetch

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

Extended Advanced Programmable Interrupt Controller (Extended APIC)

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

Intel Virtualization Technology

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



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

Enable SMX

Select Enable to support Safer Mode Extensions (SMX), which provides a programming interface for system software to establish a controlled environment to support the trusted platform configured by the end user and to verify a virtual machine monitor before it is allowed to run. The options are **Disable** and Enable.

PPIN Control

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

AES-NI

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

Limit CPU PA to 46 Bits

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

TME, TME-MT, TDX

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

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

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

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

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

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

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

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

Key Stock Amount (Available when "Memory Encryption (TME)" is set to Enabled)

Use this feature to set the number of unique keys per system, which also indicates the number of tenants per platform. The default setting is **63**.

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

Use this feature to set the number of bits for each key ID. The default setting is **6**.

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

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

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

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

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

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

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

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

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

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

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

This feature displays the number of keys designated for TDX.

Software Guard Extension (SGX)

***The following SGX features are available when "Memory Encryption (TME)" is Set to Enabled and When Your CPU Supports Intel SGX.**



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

SGX Factory Reset

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

SW Guard Extensions (SGX)

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

SGX Package Info In-Band Access

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

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

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

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

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

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

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

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

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

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

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

SGXLEPUBKEYHASHx Write Enable (Available When "SW Guard Extensions (SGX)" is Set to Enabled)

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

SGXLEPUBKEYHASH0 (Available When Both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are Set to Enabled)

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

SGXLEPUBKEYHASH1 (Available When Both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are Set to Enabled)

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

SGXLEPUBKEYHASH2 (Available When Both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are Set to Enabled)

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

SGXLEPUBKEYHASH3 (Available When Both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are Set to Enabled)

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

SGX Auto MP Registration (Available When "SW Guard Extensions (SGX)" is Set to Enabled)

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

► Chipset Configuration



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

► North Bridge

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

► Uncore Configuration

The following information will be displayed:

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

Degrade Precedence

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

Link L0p Enable

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



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

Note 2: The option of Full L0p Enable is available when the 5th Gen. Intel Xeon Scalable Series processor is used.

Link L1 Enable

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

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

KTI Prefetch

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

IO Directory Cache (IODC)

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

SNC

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

 **Note:** The option of Enable SNC4 (4-clusters) depends on your system configuration and the processor.

Stale AtoS (A to S)

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

LLC Dead Line Alloc

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

UPI3

Use this feature to enable/disable the 4th Intel Ultra Path Interconnect (UPI) link. The default setting is Enable if your motherboard supports UPI3. The options are Disable and **Enable**. This feature depends on your system configuration.

► Memory Configuration

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

Enforce DDR Memory Frequency POR

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

Memory Frequency

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



Note: The options available are CPU-dependent.

Data Scrambling for PMem (Available when any PMem device is detected by the BIOS)

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

Data Scrambling for DDR5

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

Enable ADR (Available When "Enable fADR" is Set to Disable)

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

Legacy ADR Mode (Available When "Enable fADR" is Set to Disable and "Enable ADR" is Set to Enable)

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

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

Number of Cores

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

Core Ratio

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

Core Ratio Value (Available When "Core Ratio" is Set to Manual)

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

Mesh Ratio

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

Mesh Ratio Value (Available When "Mesh Ratio" is Set to Manual)

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

Flush Timeout

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

Flush Timeout Value (Available When "Flush Timeout" is Set to Manual)

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

DDR 2X Refresh Enable

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

CXL Type 3 Legacy

Select Enable to allow CXL Type 3 devices to use CXL Type 2 flow in operation. The options are **Disable** and Enable.



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

Volatile Memory Mode

Use this feature to select 1LM mode or 2LM mode for Volatile Memory. If 2LM is not configurable, Volatile Memory will revert back to 1LM mode. The default setting is **1LM** (Mode). Note that this feature depends on the support of the Intel Optane PMem 300 series.

 **Note:** This feature is available when your motherboard has the high bandwidth memory (HBM) CPU installed and when "NUMA" (Advanced > ACPI Settings > NUMA) is set to Enabled.

►Memory Topology

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

P1-DIMMA1: 4800 MT/s Hynix DRx8 32 GB RDIMM — P2-DIMMH1: 4800 MT/s Hynix DRx8 32 GB RDIMM

►Page Policy

Page Policy

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

►Memory RAS Configuration

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

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

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

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

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

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

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

Correctable Error Threshold

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

Leaky Bucket Low Bit

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

Leaky Bucket High Bit

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

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

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

Patrol Scrub

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

The options are Disabled and **Enable at End of POST**. POST is the abbreviation for Power-On Self-Test.

DDR PPR Type

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

Enhanced PPR

Use this feature to set an advanced memory test for PPR enhancement. Select Persistent to always execute PPR 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 in the same memory page. The options are **Disabled** and Enabled.

► PMem Configuration (Available When Any PMem Device is Detected by the BIOS)



Note: This submenu depends on the support of Intel Optane PMem 300 Series.

PMem QoS

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

PMem Performance Setting

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

Seamless: Opt-In DIMMs

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

► IIO Configuration

► CPU1 Configuration / CPU2 Configuration

IOU0 (IIO PCIe Port 1)

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

IOU1 (IIO PCIe Port 2)

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

IOU2 (IIO PCIe Port 3)

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

IOU3 (IIO PCIe Port 4)

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

IOU4 (IIO PCIe Port 5)

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

► Socket0 Port DMI



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

PCIe Port

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

Link Speed

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

The following information is displayed:

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

Data Link Feature Exchange

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

DMI Port MPSS

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

Equalization Support to Highest Rate (Available When Supported By the PCIe Port)

When this feature is set to Enable, the Equalization Bypass mode will be supported at the highest rate for fast link initialization by negotiation through link training, helping avoid burst errors, and looping back by mimicking crosstalk behaviors. The options are **Enable** and Disable.

►IOAT Configuration

Relaxed Ordering

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

► Intel VT for Directed I/O (VT-d)

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

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

Opt-Out Illegal MSI Mitigation

If this feature is set to Enable, "Illegal 0xFEE Platform Mitigation" will be supported by the system. The options are Enable and **Disable**.

Pre-boot Direct Memory Access (DMA) Protection

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

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

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

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

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

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

If this feature is set to Enable, "Illegal 0xFEE Platform Mitigation" will be opted out. The options are Enable and **Disable**.

► Intel VMD Technology

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

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

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

NVMe Mode Switch

When this feature is set to Auto, VMD support will be automatically enabled when a VROC key is detected by the BIOS. When this feature is set to Manual, all PCIe ports will be in legacy mode, but you can manually switch each port to VMD mode in the submenu. When this feature is set to VMD, all detected NVMe ports will be in VMD mode while other PCIe ports will still be in legacy mode. The options are Manual, VMD, and **Auto**.

► Intel VMD for Volume Management Device on Socket 0 (CPU1) (Available When "NVMe Mode Switch" is Set to Manual)

VMD Config for PCH Ports

Enable/Disable VMD

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

PCH Root Port 0 – Port 11 (Available When the Device is Detected by the System and "Enable/Disable VMD" Above is Set to Enable)

Select Enable to enable the Intel VMD technology support for the root port specified. The options are **Disable** and Enable.

Hot Plug Capable (Available When the Device is Detected by the System and "Enable/Disable VMD" Above is Set to Enable)

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

VMD Config for IOU 0 / VMD Config for IOU 1 / VMD Config for IOU 2 / VMD Config for IOU 3 / VMD Config for IOU 4 / VMD Config for IOU 5 / VMD Config for IOU 6 (Available When the Device is Detected by the System and "Enable/

Disable VMD" Above is Set to Enable)**Enable/Disable VMD**

Select Enable to enable the Intel VMD technology support for the root port specified. The options are **Disable** and Enable.

Socket0 IOU0 VMD Port A / Socket0 IOU0 VMD Port C / Socket0 IOU0 VMD Port E / Socket0 IOU0 VMD Port G — Socket0 IOU6 VMD Port A / Socket0 IOU6 VMD Port C / Socket0 IOU6 VMD Port E / Socket0 IOU6 VMD Port G (Available When the Device is Detected by the System and "Enable/Disable VMD" Above is Set to Enable and When the Devices Installed on the Port Specified is Detected by the BIOS)

Select Enable to enable the Intel VMD technology support for the root port specified. The options are **Disable** and Enable.

Hot Plug Capable (Available When the Device is Detected by the System and "Enable/Disable VMD" Above is Set to Enable)

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

►Intel VMD for Volume Management Device on Socket 1 (CPU2) CPU2 (Available When "NVMe Mode Switch" is Set to Manual)

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

Enable/Disable VMD

Select Enable to enable the Intel VMD technology support for the root port specified. The options are **Disable** and Enable.

Socket1 IOU0 VMD Port A / Socket1 IOU0 VMD Port C / Socket1 IOU0 VMD Port E / Socket0 IOU1 VMD Port G — Socket1 IOU6 VMD Port A / Socket1 IOU6 VMD

Port C / Socket1 IOU6 VMD Port E / Socket1 IOU6 VMD Port G (Available When the Device is Detected by the System and "Enable/Disable VMD" Above is Set to Enable)

Select Enable to enable the Intel VMD technology support for the root port specified. The options are **Disable** and Enable.

Hot Plug Capable (Available When the Device is Detected by the System and "Enable/Disable VMD" Above is Set to Enable)

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

► PCIe Leaky Bucket Configuration**Gen2 Link Degradation**

Use this feature to enable PCIe Gen. 2 link degradation. The options are Disable and **Enable**.

Gen3 Link Degradation

Use this feature to enable PCIe Gen. 3 link degradation. The options are Disable and **Enable**.

Gen4 Link Degradation

Use this feature to enable PCIe Gen. 4 link degradation. The options are Disable and **Enable**.

Gen5 Link Degradation

Use this feature to enable PCIe Gen. 5 link degradation. The options are Disable and **Enable**.

IIO-PCIe Express Global Options
-----**PCIe ASPM Support (Global)**

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

PCIe Max Read Request Size

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

Equalization Support to Highest Rate

When this feature is set to Enable, the Equalization Bypass mode will be supported at the highest rate for fast link initialization by negotiation through link training, helping avoid burst errors, and looping back by mimicking crosstalk behaviors. The options are **Enable** and Disable.

IIO eDPC Support (Available When Your System Supports This Feature)

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

CXL Security Level

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

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

CXL Header Bypass

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

► South Bridge

The following information is displayed:

- USB Devices:

Legacy USB Support

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

XHCI Hand-off

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

Port 60/64 Emulation

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

PCIe PLL SSC

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

► Server ME Information

The following information is displayed:

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

►PCH SATA0 Configuration / ►PCH SATA2 Configuration (Available When Related Devices are Detected)

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

SATA Controller(s)

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

SATA Mode Selection (Available When "SATA Controller(s)" is Set to Enabled)

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



Note: The option of RAID is unavailable when "Boot Mode Select" is set to Legacy. Also, refer to the Boot submenu in the BIOS Setup main menu to set "Boot Mode Select".

Support Aggressive Link Power Management (Available When "SATA Controller(s)" is Set to Enabled)

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

SATA SGPIO Mode (Available When "SATA Controller(s)" is Set to Enabled)

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

SATA Port 0 — SATA Port 7 (Available When "SATA Controller(s)" is Set to Enabled)



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

Hot Plug

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

Spin Up Device

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

SATA Device Type

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

► Trusted Computing (Available When a TPM Device is Installed and Detected by the BIOS)

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

- TPM 2.0 Device Found
- Firmware Version:
- Vendor

Security Device Support

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

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

- Active PCR banks
- Available PCR banks

SHA-1 PCR Bank (Available When "Security Device Support" is Det to Enable)

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

SHA256 PCR Bank (Available When "Security Device Support" is Set to Enable)

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

Pending Operation (Available When "Security Device Support" is Set to Enable)

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



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

Platform Hierarchy (Available When "Security Device Support" is Set to Enable) (For TPM Version 2.0 and Above)

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

Storage Hierarchy (Available When "Security Device Support" is Set to Enable)

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

Endorsement Hierarchy (Available When "Security Device Support" is Set to Enable)

Select Enabled for Endorsement Hierarchy support, which contains separate controls to address the user's privacy concerns because the primary keys in the hierarchy are certified by the TPM key or by a manufacturer with restrictions on how an authentic TPM device that is attached to an authentic platform can be accessed and used. A primary key can be encrypted and certified with a certificate created by using TPM2_ ActivateCredential, which allows the user to independently enable "flag, policy, and authorization values" without involving other hierarchies. A user with privacy concerns can disable the endorsement hierarchy while still using the storage hierarchy for TPM applications, permitting the platform software to use the TPM. The options are Disabled and **Enabled**.

PH Randomization (For TPM Version 2.0 and Above)

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

Supermicro BIOS-Based TPM Provision Support

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



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

TXT Support

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



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

Note 2: For more information on TPM, refer to the TPM manual at <http://www.super-micro.com/manuals/other/TPM.pdf>.

►ACPI Settings

NUMA

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

UMA-Based Clustering

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

WHEA Support

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

High Precision Event Timer

Select Enabled to activate the High Precision Event Timer (HPET) that produces periodic interrupts at a much higher frequency than a Real-time Clock (RTC) does in synchronizing multimedia streams, providing smooth playback and reducing the dependency on other timestamp calculation devices, such as an x86 RDTSC Instruction embedded in the CPU. The HPET is used to replace the 8254 Programmable Interval Timer. The options are Disabled and **Enabled**.

►Super IO Configuration (Available When Your System Supports This Feature)

The following information is displayed:

- Super IO Chip

►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)

This feature specifies the base I/O port address and the Interrupt Request address of serial port 1. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 1. The options are **Auto**, (IO=3F8h; IRQ=4;), (IO=2F8h; IRQ=4;), (IO=3E8h; IRQ=4;), and (IO=2E8h; IRQ=4;).

► Serial Port 2 Configuration

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

Serial Port 2 ("SOL" or "Serial Port 2" Based on Your System Support)

Select Enabled to enable SOL or Serial port 2. The options are Disabled and **Enabled**.

Device Settings (Available When "SOL/Serial Port 2" is Set to Enabled)

This feature displays the base I/O port address and the Interrupt Request address of Serial Port 2 or the SOL port.

Change Settings (Available When "SOL/Serial Port 2 is Set to Enabled)

This feature specifies the base I/O port address and the Interrupt Request address of serial port 2. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 2. The options are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3;), (IO=3E8h; IRQ=3;), and (IO=2E8h; IRQ=3;).

Serial Port 2 Attribute (Available for Serial Port 2 Only)

Select SOL to use serial port 2 as a Serial Over LAN (SOL) port for console redirection. The options are **SOL** and COM.

► Serial Port Console Redirection**COM1 (Available When Your System Supports 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.

► Console Redirection Settings (Available When "Console Redirection" Above is Set to Enabled)

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

SOL/COM2



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

Console Redirection

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

► Console Redirection Settings (Available When "Console Redirection" Above is Set to Enabled)

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

Legacy Console Redirection:

► Legacy Console Redirection Settings

Legacy Serial Redirection Port

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

Resolution

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

Redirect After BIOS POST

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

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

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

Console Redirection EMS

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

► Console Redirection Settings (Available When "Console Redirection EMS" Above is Set to Enabled)

Out-of-Band Management (Mgmt) Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2. Note that the option of SOL/COM2 indicates a shared serial port. SOL/COM2 is available with BMC support.

Terminal Type EMS

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII character set. Select VT100+ to add color and function

key support. Select ANSI to use the extended ASCII character set. Select VT-UTF8 to use UTF8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, **VT-UTF8**, and ANSI.

Bits Per Second EMS

This feature sets the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 57600, **115200**, 230400, 460800, and 921600 (bits per second).

Flow Control EMS

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

The following items will be displayed:

Data Bits EMS

Parity EMS

Stop Bits EMS

► Network Configuration

Network Stack

Select Enabled to enable Preboot Execution Environment (PXE) or Unified Extensible Firmware Interface (UEFI) for network stack support. The options are Disabled and **Enabled**.

IPv4 PXE Support (Available When "Network Stack" is Set to Enabled)

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

IPv4 HTTP Support (Available When "Network Stack" is Set to Enabled)

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

IPv6 PXE Support (Available When "Network Stack" is Set to Enabled)

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

IPv6 HTTP Support (Available When "Network Stack" is Set to Enabled)

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

PXE Boot Wait Time (Available When "Network Stack" is Set to Enabled)

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

Media Detect Count

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

►MAC:(MAC Address)-IPv6 Network Configuration



Note: The display for this section will differ, depending on your system 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

This feature displays the number of times that Duplicate Address Detection (DAD) has been performed. DAD is a procedure used to verify whether an IPv6 address is unique on the LAN before it is assigned for physical interface; only a unique IP address will be used for real-time interface. The default setting is **1**.

Policy

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

► Advanced Configuration (Available When "Policy" is Set to Manual)**New IPv6 Address**

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

New Gateway Addresses

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

New DNS Address

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

Commit Changes and Exit

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

Discard Changes and Exit

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

Save Changes and Exit

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

► MAC:(MAC Address)-IPv4 Network Configuration

Note: The display for this section will differ, depending on your system configuration.

Configured

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

Enable DHCP (Available When "Configured" is Set to Enabled)

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

Local IP Address (Available When "Configured" is Set to Enabled and "Enabled DHCP" is Set to Disabled)

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

Local NetMask (Available When "Configured" is Set to Enabled and "Enabled DHCP" is Set to Disabled)

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

Local Gateway (Available When "Configured" is Set to Enabled and "Enabled DHCP" is Set to Disabled)

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

Local DNS Servers (Available When "Configured" is Set to Enabled and "Enabled DHCP" is Set to Disabled)

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

Save Changes and Exit

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

► PCIe/PCI/PnP Configuration

The following information is displayed:

- PCI Bus Driver Version

PCI Devices Common Settings:**Above 4G Decoding (Available When the System Supports 64-bit PCI Decoding)**

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

MMCFG Base

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

MMCFG Size

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



Note 1: The options shown here depend on your memory size.

Note 2: The option of 64 MB is not available on motherboards with dual processors.

MMIO High Base

Use this feature to select the base memory size according to memory-address mapping for the IO hub. The options are 56T, 40T, **32T**, 24T, 16T, 4T, 2T, 1T, 512G, and 3584T.

MMIO High Granularity Size

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

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 to improve the frame rate performance. The options are **Disabled** and Enabled.

SR-IOV Support

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

ARI Support

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

Bus Master Enable

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

Consistent Device Name Support

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

NVMe Firmware Source

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

VGA Priority

Use this feature to select the graphics device to be used as the primary video display for system boot. The options are **Onboard** and Offboard. For the following features, note that:



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

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

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

Onboard Video Option ROM

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

RSC-D-6G5 PCIe 5.0 X16 OPROM / RSC-DR-6G5 PCIe 5.0 X16 OPROM / P1-AIOM OPROM / P2-AIOM OPROM / M.2-C1 OPROM / M.2-C2 OPROM

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

Onboard NVMe1 Option ROM — Onboard NVMe2 Option ROM (Available When NVMe Devices are Detected by the BIOS)

Use this feature to select which firmware function to be loaded for the NVMe device in this slot. The options are Disabled and **EFI**.

► HTTP Boot Configuration

HTTP Boot Policy

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

HTTPS Boot Checks Hostname

Enable this feature for HTTPS boot to check the hostname of the TLS certificates to see if it matches the hostname 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 fewer. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created. This feature is only supported on Dual or EFI Boot Mode.

► Supermicro KMS Server IP Configuration

Supermicro KMS Server IP Address

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

Second Supermicro KMS Server IP Address

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

Supermicro KMS TCP Port Number

Use this feature to enter the Supermicro KMS TCP port number. The valid range is 100 to 9999. The default setting is **5696**.

KMS Time Out

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

Supermicro KMS Server Retry Count

Use this feature to specify how many times the connection will retry to connect to the KMS server. The valid range is zero to 10. Press "+" or "-" on your keyboard to change the value. The default setting is **2** (retrying twice).

TimeZone

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

TCG NVMe KMS Policy

Use this feature to select the TCG NVMe KMS policy. The options are Normal Unlock, **Do Nothing**, Reset All Devices, and Delete Key ID List.

Client UserName

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

Client Password

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

KMS TLS Certificate / Size

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

► CA Certificate

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

► Client Certificate

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

► Client Private Key

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

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

Use this feature to change the private key password. The options are **Update**, Delete, and Export.

► Super-Guardians Configuration

Super-Guardians Protection Policy

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

KMS Security Policy

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

KMS Server Retry Count

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

TPM Security Policy

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

Load Authentication-Key

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

USB Security Policy

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

► Intel(R) Ethernet Controller (Ethernet Controller) — (MAC Address)



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

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

Note 3: This submenu depends on the support of the Intel Optane PMem 300 series.

► Firmware Image Properties

The following information is displayed:

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

► NIC Configuration

Link Speed

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

Wake On LAN

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

Link Layer Discovery Protocol (LLDP) Agent

Use this feature to enable or disable 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**.

Blink LEDs

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

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

► Mellanox Network Adapter — (MAC Address)



Note 1: This feature is available when a Mellanox network adapter is installed.

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

► Firmware Image Properties

The following information is displayed:

- Family Firmware Version
- EFI Version

► NIC Configuration

Banner Message Time Out

Use this feature to specify how long the OptionROM banner message should be displayed during Power-On Self-Testing (POST). The default setting is **4** (seconds).

Legacy Boot Protocol

Use this feature to select a Legacy network boot protocol, which will allow the BIOS to automatically reboot the system from a Legacy boot device after an initial boot failure. The options are None, **PXE**, iSCSI, PXE without failover, and iSCSI without failover.

IPv4/IPv6 Support

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

Virtual LAN Mode

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

Virtual LAN ID

This feature displays the VLAN ID. The default setting is **1**.

Boot Retry Count

Use this feature to specify how many times a system should try to reboot in case of a boot failure. The options are No Retry, 1 Retry, 2 Retries, 3 Retries, 4 Retries, 5 Retries, 6 Retries, and Indefinite Retries.

Boot Strap Type

Use this feature to set the Boot Strap type (method) for the BIOS to boot to the OS. The default setting is **Int 19h**.

Wake On LAN

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

Wake On LAN Speed

Use this feature to set the LAN port speed to be used for Wake On Lan Mode. The default setting is **1 Gbps**.

► Supermicro PMem Configuration (Available When Any PMem Module is Detected by the BIOS)



Note: This submenu depends on the support of Intel Optane PMem 300 Series.

► Supermicro PMem Information



Note: The information provided in the following section depends on the PMem modules populated in your system.

The following information is displayed:

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

- Region [1] RegionId
- Region [1] RegionType
- Region [1] Capacity
- Region [1] FreeCapacity
- Region [1] Health
- Region [1] DimmIdCount
- Region [1] DimmId

► Supermicro PMem Settings

Create Goal Config:: Persistent Memory Type

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

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

Reserved [%]

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

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

User Security Policy

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

User DIMMs Current PassPhrase

User DIMMs New PassPhrase

All PMem DIMMs Master Security Policy

Master Security Policy

Use this feature to set the User Master Policy. The options are **Do Nothing** and Master Security Erase DIMMs.

All PMem DIMMs FW Settings

Updated PMem DIMMs FW Version::

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

Update PMem DIMMs FW from BIOS

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

Last Status :: (Update Fw) (Success) Code

This feature displays the active PMem Last status.

► Intel(R) Optane(TM) Persistent Memory Configuration (Available When Any PMem Module is Detected by the BIOS)



Note: This submenu depends on the support of Intel Optane PMem 300 Series.

The following information is displayed:

- Version: This feature displays the version of PMem used in the system.
- Select an action.
- Detected PMem modules: This feature displays the number of PMem modules detected by the system.
- All PMem modules are healthy.



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

► PMem Modules

This feature allows you to view and configure the following settings for the PMem modules installed in the system.

PMem Modules on Socket 0x000:

► DIMM ID 0x0000 / ► DIMM ID 0x0100 / ► DIMM ID 0x0200 / ► DIMM ID 0x300



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

When you select the DIMM ID above and press <Enter>, the following information will display:

- DIMM UID: This feature displays the unique ID of the PMem module.
- DIMM handle: This feature displays the unique handle assigned to the PMem module.
- DIMM Physical ID: This feature displays the physical ID of the PMem module.
- Manageability State: This feature indicates the manageability state of the PMem module.
- Health state: This feature indicates the health state of the PMem module.
- Health state reason: This feature indicates the reason that effectuates the health state of the PMem module.
- Capacity: This feature indicates the capacity of the PMem module.
- Firmware version: This feature indicates the firmware version of the PMem module.
- Firmware API version: This feature indicates the firmware API version of the PMem module.
- Firmware Active API version: This feature indicates the firmware API version of the PMem module.
- Lock state: This feature indicates the lock state of the PMem module.
- SVN downgrade: This feature indicates the status of SVN Downgrade of the PMem module.
- Secure erase policy: This feature indicates the status of the Secure Erase Policy of the PMem module.

- S3 resume opt-in: This feature indicates the status of the S3 Resume Opt-In support for the PMem module.
- Firmware Activate opt-in: This feature indicates the status of the Firmware Activate Opt-In support for the PMem module.
- Staged firmware version: This feature indicates the status of the staged firmware version of the PMem module.
- Staged firmware activatable: This feature indicates the status of the staged firmware activation support of the PMem module.
- Firmware update status: This feature indicates the firmware update status of the PMem module.
- Firmware activation quiesce required: This feature indicates whether Firmware Activation Quiesce is required for the PMem module.
- Firmware activation time [ms]: This feature indicates the time needed to activate the firmware.
- Manufacturer: This feature indicates the manufacturer of the PMem module.

Show More Details

Select Enabled to view more detailed information on the PMem module. The options are Disabled and Enabled.

**If "Show More Details" is set to Enabled, the following information will display:*

- Serial Number
- Part Number
- Socket
- Memory Controller ID
- Vendor ID
- Device ID
- System Vendor ID
- Subsystem Device ID
- Device Locator

- Subsystem Revision ID
- Interface Format Code
- Manufacturing Info Valid
- Manufacturing Date
- Manufacturing Location
- Memory Type
- Memory Bank Label
- Data Width Label [b]
- Total Width [b]
- Speed [MT/s]
- Channel ID
- Channel Position
- Revision ID
- Form Factor
- Manufacturer ID
- Controller Revision ID
- Is new
- Memory Capacity
- APP Direct Capacity
- Unconfigured Capacity
- Inaccessible Capacity
- Reserved Capacity
- Avg Power Limit [mW]
- Avg Power Reporting Time Constant
- Memory Bandwidth Boost Feature

- Memory Bandwidth Boost Max Power Limit [mW]
- Memory Bandwidth Boost Average Power Time Constant [ms]
- Max Average Power Limit [mW]
- Max Memory Bandwidth Boost Max Power Limit [mW]
- Max Memory Bandwidth Boost Average Power Time Constant [ms]
- Memory Bandwidth Boost Average Power Time Constant Step [ms]
- Max Average Power Reporting Time Constant [ms]
- Average Power Reporting Time Constant Step [ms]
- Package Sparing Capable
- Package Sparing Enabled
- Package Spares Available
- Configuration Status
- 147
- SKU Violation
- Population Violation
- ARS Status
- Overwrite PMem Module Status
- Last Shutdown Time
- Average Power Reporting Time Constant [ms]
- Viral Policy Enable
- Viral State
- Thermal Throttle Loss %
- Latched Last Shutdown Status
- Unlatched Last Shutdown Status
- Security Capabilities

- Modes Supported
- Boot Status
- AIT DRAM Enabled
- Error Injection Enabled
- Max Controller temperature [C]
- Software Triggers Enabled [0]
- Software Triggers Enabled Details
- Poison Error Injection Counter
- Poison Error Clear Counter
- Media Temperature Injections Counter
- Software Triggers Counter
- Max Media Temperature [C]
- Media Temperature Injection Enabled
- Master Passphrase Enabled
- Average Power [mW]
- eADR Enable
- Previous Pwr Cycle eADR Enabled
- Latch System Shutdown State
- Previous Power Cycle Latch System
- Shutdown State
- FIPS Mode Status

► **Monitor Health**

This submenu displays the following health information on a memory module being monitored:

- Current alarm threshold status Controller temperature: within the alarm threshold on all PMem modules.
- Media temperature: within the alarm threshold on all PMem modules.
- Percentage remaining: within the alarm threshold on all PMem modules.

Modify Alarm Thresholds Control Temperature [C]

This feature indicates the temperature threshold upon which the alarm will be triggered.

Media Temperature [C]

This feature indicates the media temperature of the PMem module.

Percentage Remaining [%]

This feature displays the remaining percentage of the PMem module.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Update Firmware

Use this feature to select the firmware image to be loaded on the PMem module. After loading the firmware image, reboot the system and select Update for the firmware to take effect. The following information is displayed.

- Current firmware version: This feature displays the current firmware version.
- Selected firmware version: Use this feature to select a new firmware version.
- File: Use this feature to specify the file path in the root directory that contains the new firmware for firmware update.
- Staged firmware version: This feature indicates the staged firmware version of the PMem module specified by the user.

►Update

Select this feature to update the firmware settings.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Configure Security

Use this feature to configure the security settings for all onboard PMem modules.



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

State:

Use this feature to enable the security settings for the PMem modules installed in the system. The options are Disabled and Enabled.

Enable Security

Press <Enter> and set the user password for the onboard PMem modules.

Secure Erase with User Password

Use this feature to erase all the persistent data saved in the PMem modules by entering the user password. The options are Yes and No.

Freeze Lock

Use this feature to enable the security lock for the onboard PMem modules.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Configure Data Policy

Use this feature to configure the data policy settings for all onboard PMem modules.

Average Power Reporting Time Constant [ms]

This feature specifies the constant average power reporting time.

Modify Average Power Reporting Time Constant

Use this feature to modify the constant average power reporting time.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Regions

This feature allows you to configure PMem regions. A region is a set of PMem modules. The system supports x1 (no interleave) and AD interleaves of x4 and x8. Interleaving PMem across processors is not allowed.

Current Configuration

►Region ID 1

When this submenu is selected, the following information is displayed:

- Region ID: This feature displays the Region ID of the PMem module.
- DIMM ID: This feature displays the DIMM ID of the PMem module.
- ISet ID: This feature displays the ISet ID of the PMem module.
- Persistent memory type: This feature indicates the memory type of the PMem module.
- Capacity: This feature indicates the capacity of the PMem module.
- Free capacity: This feature indicates the capacity of the PMem module that is available for use.
- Health: This feature indicates the health state of the PMem module.
- Socket ID: This feature displays the Socket ID of the PMem module.

►Back to Regions Menu

Press <Enter> to go back to the main screen of **Regions**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Provisioning

This feature allows you to configure the memory allocation goal for the PMem modules.

►DIMM ID 0x0000 / ►DIMM ID 0x0100 / ►DIMM ID 0x0200 / ►DIMM ID 0x300



Note: The DIMM IDs above are based on your system configuration.

Select the desired DIMM ID. Press <Enter> and the following information is displayed.

- Socket ID:
- DIMM ID:
- Memory Mode size:
- App Direct #1 size:
- App Direct #1 index:
- App Direct #1 settings:
- App Direct #2 size:
- App Direct #2 index:
- App Direct #2 settings:

The following information is displayed without pressing <Enter>.

- MemorySize:
- AppDirect1Size:
- AppDirect2Size:

►Back to Provisioning Menu

Press <Enter> to go back to the main screen of **Provisioning**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Create Goal Config

Create Goal Config For:

Use this feature to select the target to create the goal configuration for PMem modules. The options are **Platform** and **Socket**.

Reserved [%]:

This feature reserves a percentage of the PMem capacity for a particular purpose and keep this portion of memory space from being mapped into the physical address of system for system use.

Memory Mode [%]:

This feature reserves a percentage of the PMem capacity for special use in a specific Memory Mode. (This value can be automatically set by the system.)

Persistent Memory Type

This feature specifies the type of PMem memory capacity to be created. The options are **App Direct** and **App Direct Not Interleave**.

Namespace Label Version

Use this feature to view and modify the namespace label version to initialize when creating goals. The options are **1.2** and **1.1**.

►Create Goal Config

Use this feature to create a memory allocation goal with the above settings.

►Back to Provisioning Menu

Press <Enter> to go back to the main screen of **Provisioning**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Delete Goal Config

Delete goal config for:

Use this feature to select the target to delete the goal configuration for PMem modules. The options are **Platform** and **Socket**.

►Delete Goal Config

Use this feature to delete the goal configuration on the selected target.

►Back to Provisioning menu

Press <Enter> to go back to the main screen of **Provisioning**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Namespaces

Use this feature to view, create, modify, and delete namespaces. The list of namespaces that have been created is displayed. The health status of namespace is also displayed. Select a namespace and press <Enter> to view detailed information.

►0x00000101 Healthy

Select this namespace, which has been created earlier. Press <Enter> and the following information is displayed.

- UUID
- ID

- Name
- Region
- Health
- Mode
- Block Size
- Units: Use this feature to change the namespace capacity (in the unit of B, MB, MiB, GB, GiB, TB, and TiB).
- Capacity
- Label version

►Delete

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

►Delete

Press <Enter> to go back to the main screen of **Namespaces**.

►Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

►Create Namespace

Name

Use this feature to enter the name for a namespace.

Region ID

This feature displays the region ID of this namespace.

Mode

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

Capacity Input

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

Units

Use this feature to change the units of the input namespace capacity. The options are B, MB, MiB, GB, GiB, TB, and TiB.

Capacity

This feature displays the capacity of this namespace.

► Create Namespace

Use this feature to create a namespace with the above settings.

► Back to Namespaces

Press <Enter> to go back to the main screen of **Namespaces**.

► Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

► Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

► Total Capacity

This feature allows you to set the total PMem resource capacity allocated across all segments in the host server.

PMem Module Capacities

This section displays the following information.

- Volatile: This feature specifies Volatile information of the PMem module.
- AppDirect: This feature specifies the App. direct capacity of the PMem module.
- Inaccessible: This feature specifies the capacity of the PMem module that is not accessible to the user.
- Raw: This feature specifies the raw capacity of the PMem module.

DDR Capacities

This section displays the following information.

- Volatile: This feature specifies Volatile information of the PMem module.
- Cache: This feature specifies the capacity of the cache memory.
- Inaccessible: This feature specifies the capacity of the PMem module that is not accessible to the user.
- Raw: This feature specifies the raw capacity of the PMem module.

Total Memory Capacities

This section displays the following information.

- Volatile: This feature specifies Volatile information of the PMem module.
- AppDirect: This feature specifies the App. direct capacity of the PMem module.
- Cache: This feature specifies the capacity of the cache memory.
- Inaccessible: This feature specifies the capacity of the PMem module that is not accessible to the user.
- Raw: This feature specifies the raw capacity of the PMem module.

► Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

► Diagnostics

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

Quick Diagnostics

Select Enabled for the quick diagnostics test to be performed on the PMem modules installed in the system when needed. The options are Disabled and Enabled.

DIMM ID 0x0010

Select Enabled to display the DIMM ID of a PMem module upon which the diagnostic test will be performed. The options are Disabled and Enabled. Note that more DIMM IDs will appear if more PMem modules are installed on the motherboard.

Config Diagnostics

Select Enabled for the platform configuration diagnostics test to be performed on the PMem module. The options are Disabled and Enabled.

FW Diagnostics

Select Enabled for the firmware diagnostics test to be performed on the PMem module. The options are Disabled and Enabled.

Security Diagnostics

Select Enabled for the security diagnostics test to be performed on the PMem module. The options are Disabled and Enabled.

► Execute Tests

Press <Enter> to execute the selected diagnostic tests and view the results.

► Back to Diagnostics

Press <Enter> to go back to the main screen of **Diagnostics**.

► Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

► Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

► Preferences

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

Default DIMM ID:

This feature allows you to view and modify the default DIMM ID as displayed on the screen. The options are Handle and UID.

Capacity Units:

This feature allows you to view and set the default capacity unit of the selected PMem to be displayed on the screen. The options are Auto, Auto_10, B, MB, MiB, GB, GiB, TB, and TiB.

App Direct Settings:

Press <Enter> to view and modify the interleaving setting for creating App Direct capacity.

► Back to Main Menu

Press <Enter> to go back to the main screen of **Intel(R) Optane(TM) Persistent Memory Configuration**.

► 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, as 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 feature to configure Event Logs settings.



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



Figure 4-4: Event Logs Options

► Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

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

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

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

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

SMBIOS Event Log Standard Settings

Log System Boot Event (Available When "SMBIOS Event Log" is Set to Enabled)

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

MECI (Available When "SMBIOS Event Log" is Set to Enabled)

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

METW (Available When "SMBIOS Event Log" is Set to Enabled)

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

►View SMBIOS Event Log

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

- Date
- Time
- Error Code
- Severity

4.5 BMC

Use this feature to configure BMC settings.



Figure 4-5: BMC Options

BMC Firmware Revision

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

BMC STATUS

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

► System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

This feature allows you to determine what the BIOS should do when the system event log is full. Select Erase Immediately to erase all events in the log when the system event log is full. The options are **Do Nothing** and Erase Immediately.



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

►BMC Network Configuration

Update BMC LAN Configuration

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

Configure IPv4 Support

BMC LAN Selection

Use this feature to select the type of BMC LAN. The default setting is **Failover**.

BMC Network Link Status:

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

Configuration Address Source (Available When "Update BMC LAN Configuration" is Set to Yes)

Use this feature to select the source of the IPv4 connection. If Static is selected, you will need to know the IP address of the IPv4 connection and enter it into the system manually in the field. If DHCP is selected, the BIOS will search for a Dynamic Host Configuration Protocol (DHCP) server in the network that is attached to and request the next available IP address for this computer. The options are Static and **DHCP**.

Station IP Address (Available When "Configuration Address Source" is Set to Static)

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

Subnet Mask (Available When "Configuration Address Source" is Set to Static)

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

Station MAC Address (Available When "Configuration Address Source" is Set to Static)

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

Gateway IP Address (Available When "Configuration Address Source" is Set to Static)

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

VLAN (Available When "Update BMC LAN Configuration" is Set to Yes)

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

VLAN ID (Available When "VLAN" is Set to Enable)

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

Configure IPv6 Support

IPv6 Address Status

This feature displays the status of the IPv6 address.

IPv6 Support

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

Configuration Address Source (Available When "IPv6 Support" is Set to Enabled)

Use this feature to select the source of the IPv6 connection. If Static Configuration is selected, you will need to know the IP address of the IPv6 connection and enter it into the system manually in the field. If the other two options are selected, the BIOS will search for a DHCP server in the attached network and request the next available IP address for your computer. The options are Static Configuration, **DHCPv6 Stateless**, and DHCPv6 Stateful.

IPv6 Address (DHCPv6 Stateless) (Available When "Configuration Address Source" is Set to Static Configuration)

This feature displays the station IPv6 address. Press <Enter> to change the setting.

Prefix Length (Available When "Configuration Address Source" is Set to Static Configuration)

This feature displays the prefix length. Press <Enter> to change the setting.

Gateway IP (Available When "Configuration Address Source" is Set to Static Configuration)

Use this feature to enter the IPv6 gateway IP address. Press <Enter> to change the setting.

Advanced Settings

The default is **Auto obtain DNS server IP**, which allows your system to obtain the DNS server IP automatically.

Preferred DNS Server IP

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

Alternative DNS Server IP

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

4.6 Security

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

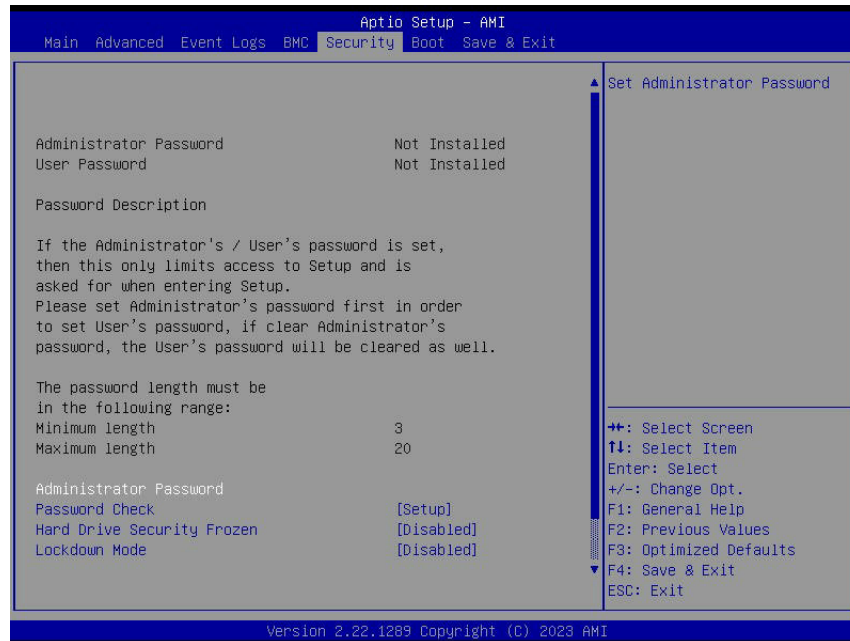


Figure 4-6: Security Options

The following information is displayed:

- Administrator Password
- User Password
- Password Description

Disable Block Sid (Available When Your Motherboard Supports NVMe)

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

Administrator Password

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

User Password (Available When "Administrator Password" has Been Set)

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

Password Check

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

Hard Drive Security Frozen

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



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

► Supermicro Security Erase Configuration (Available When a Storage Device is Detected By the BIOS)

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

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

1. From the Advanced menu, select PCIe/PCI/PnP and press <Enter> to invoke the PCI Devices Common Settings page.
2. When the PCI Devices Common Settings screen displays, select NVMe Firmware Sources and press <Enter>. The NVMe Firmware Sources pop-up dialogue box will display.
3. From the pop-up box, select AMI Native Support and press <Enter>. Be sure to save the changes you've made and reboot the system for the new settings to take effect by pressing <F4>.

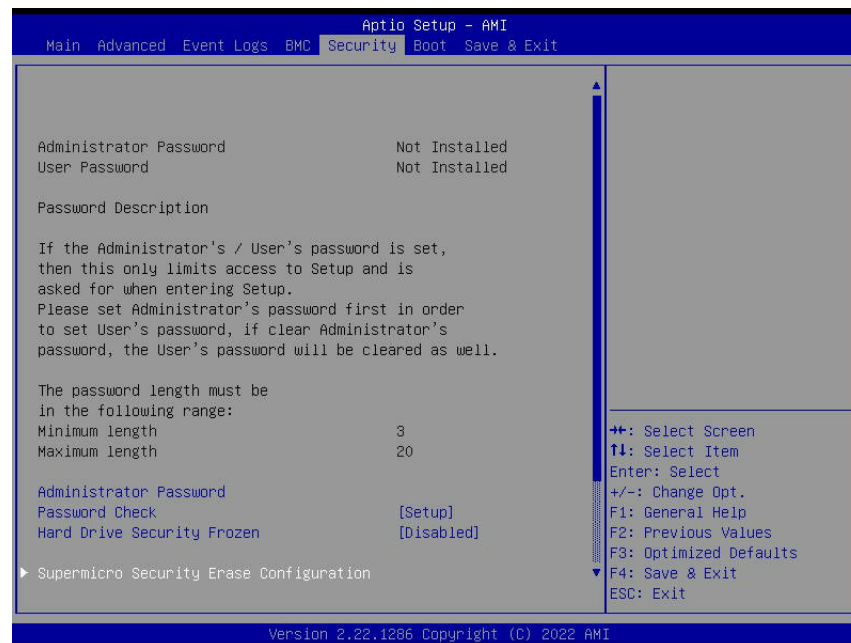


Figure 4-7: Security Options

4. Press <Del> at bootup to return to the AMI BIOS Setup Utility.
5. When the AMI BIOS screen displays, use the arrow keys to select Security from the BIOS menu bar on the top of the screen. The Supermicro Security Erase Configuration submenu will display on the Security menu as shown.
6. Select Supermicro Security Erase Configuration and press **<Enter>** to enter the Secure Erase configuration page, which will allow you to configure Security Erase settings.

Configuring the settings included in the Supermicro Security Erase Submenu

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

- **HDD Name:** This feature displays the vendor and model name of the HDD/SSD device detected by the BIOS.
- **HDD Serial Number:** This feature displays the serial number of the HDD/SSD device detected by the BIOS.
- **Security Mode:** This feature displays the security mode of the HDD/SSD device detected by the BIOS.
- **Estimated Time:** This feature displays the estimated time needed to configure the selected Security Erase features.
- **HDD User Pwd Status:** This feature indicates if a password has been set as a SATA user password, which will allow the user to configure Supermicro Security Erase settings on the selected HDD (SATA) device by using this SATA user password.
- **TCG Device Type:** This feature displays the TCG device type detected in the system.
- **Admin Pwd Status:** This feature indicates if a password has been set as a SATA administrator password, which will allow the user to configure Supermicro Security Erase settings on the selected HDD (SATA) device by using this SATA administrator password.

Security Function

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

- Select *Security Erase - Password* to enter a user password, which will allow the user to erase the password and all data stored in the HDD/SSD device.
- Select *Security Erase - PSID (Physical Security ID)* to enter an SED SSD PSID, which will allow the user to erase all data stored in this device.
- Select *Security Erase - Without Password* to use the manufacturer's default password "11111111" as the user password, which will allow you to erase all data stored in the HDD/SSD device by using this default password.

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



Note 1: The availability of the Security Erase — PSID option depends on the storage device support. PSID is the abbreviation for Physical Security Identification.

Note 2: For more information on Secure Erase instructions, refer to the Secure Erase User's Guide posted at: <https://www.supermicro.com/support/manuals/>.

Note 3: The options of Change Password and Clear Password are available when "Password" has been set.

Note 4: The option of Set Password is not available when "Password" has been set.

Password

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

New Password (Available for the Device with a Password Previously Installed)

Use this feature to set a new SATA user password for the device that previously had a password installed. This new password will allow you to configure the Supermicro Security Erase settings on this device after a "Changing Password" or a "Clear Password" command has been issued.

Lockdown Mode (Available When the DCMS key is Activated)

Select Enabled to support Lockdown Mode, which will prevent 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.

HDD Security Configuration

►P4: (Storage Device Name)

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

- HDD Password Description:
- HDD PASSWORD CONFIGURATION:
 - Security Supported:
 - Security Enabled:
 - Security Locked:
 - Security Frozen:
 - HDD User Pwd Status:
 - HDD Master Pwd Status:

Set User Password (Available When "Security Frozen:" Above is No)

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



Warning!! Be sure to enter the correct password for a device. If an incorrect password is entered, this device will be locked. If this happens, reboot the system and re-enter the correct password. A locked HDD will remain locked until the correct password for the device is entered!! Be sure to keep all your passwords in a safe and secure place.

►Secure Boot



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

The following information is displayed:

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

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

Secure Boot Mode

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

CSM (Compatibility Support Module) Support

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

► Key Management (Available When "Secure Boot Mode" is Set to Custom)

The following information is displayed.

- Vendor Keys

Provision Factory Defaults

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

► Enroll EFI Image

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

► Export Secure Boot Variables (Available When a Secure Key is Installed)

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

► Export Secure Boot Variables

The following information is displayed:

- Secure Boot Variable
- Size
- Key#
- Key Source

► Platform Key (PK)

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

► Key Exchange Keys

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 your "Key Exchange Keys". Select Append to append your "Key Exchange Keys". The options are **Details**, Export, Update, Append, and Delete.

► Authorized Signatures

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

► Forbidden Signatures

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

► Authorized TimeStamps

This feature allows you 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 your "Authorized TimeStamps". Select Append to append your "Authorized TimeStamps". The options are **Details**, Export, Update, Append, and Delete.

► **OsRecovery Signature**

This feature allows you to set and save the authorized signatures used for OS recovery. Select Update to update your "OS Recovery Signatures". These values also indicate sizes, keys, and key sources of the OsRecovery signatures. Select Append to append your "OS Recovery Signatures". The options are **Details**, Export, Update, Append, and Delete.

TCG Storage Security Configuration

► **(Storage Device Name) (Available When the Storage Device is Compliant with TCG Specifications)**

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

- TCG Storage Security Password Description:
- PASSWORD CONFIGURATION:
 - Security Subsystem Class:
 - Security Supported:
 - Security Enabled:
 - Security Locked:
 - Security Frozen:
 - Admin Pwd Status:

Set Admin Password

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

Set User Password

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 feature to configure Boot settings:

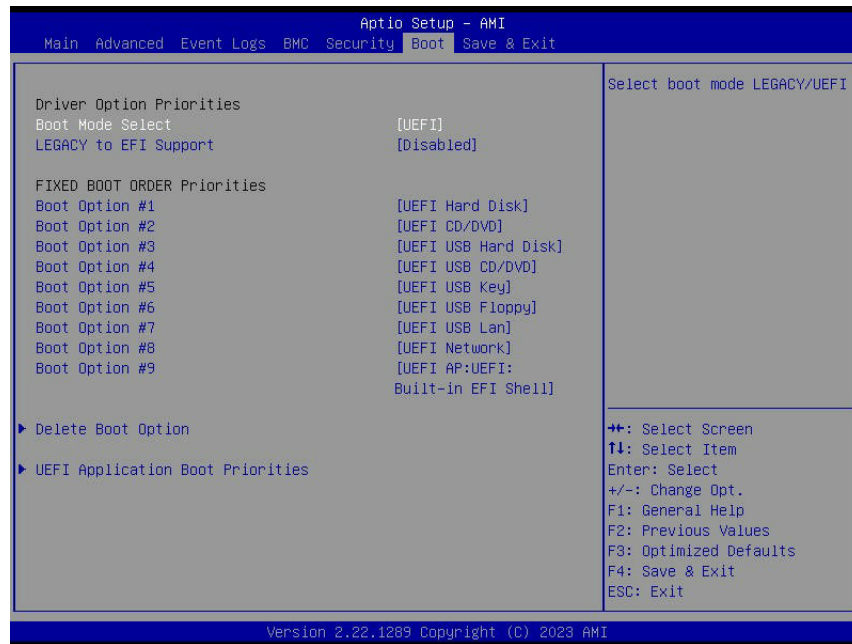


Figure 4-8: Security Options

Boot Mode Select

Use this feature to select the type of devices from which the system will boot. The options are Legacy, **UEFI**, and Dual.



Note: When "Boot Mode Select" is set to Dual, all OPRM-related features will be set to Legacy.

LEGACY to EFI Support

Select Enabled to boot EFI OS support after the Legacy boot order has failed. The options are **Disabled** and Enabled.

FIXED BOOT Option Priorities

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

When "Boot Mode Select" is set to Dual, the following features will be displayed for configuration:

- Boot Option #1 — Boot Option #17

When "Boot Mode Select" is set to Legacy, the following features will be displayed for configuration:

- Boot Option #1 — Boot Option #8

When "Boot Mode Select" is set to UEFI, the following features will be displayed for configuration:

- Boot Option #1 — Boot Option #9

► **Add New Boot Option (Available When Any Storage Device is Detected by the BIOS)**

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

Add Boot option

This feature allows you to specify the name of a new device to be used for the boot option.

Path for Boot option

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

Boot Option File Path

This feature allows you to specify the file path for the new boot option.

Create

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

► **Delete Boot Option**

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

Delete Boot Option

This feature allows you to remove an EFI boot option from the boot priority list.

► **UEFI NETWORK Drive BBS Priorities**

This feature allows you to set the system boot order for detected UEFI network devices.

► **UEFI Application Boot Priorities**

This feature allows you to set the system boot order for detected UEFI application devices.

►UEFI USB Key Drive BBS Priorities

This feature allows you to set the system boot order for detected UEFI USB key drive devices.

►UEFI Hard Disk Drive BBS Priorities

This feature allows you to set the system boot order for detected UEFI HDD devices.

►Hard Disk Drive BBS Priorities

This feature allows you to set the system boot order for detected HDD devices.

►USB Key Drive BBS Priorities

This feature allows you to set the system boot order for detected USB key devices.

►NETWORK Drive BBS Priorities

This feature allows you to set the system boot order for detected network devices.

4.8 Save & Exit

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

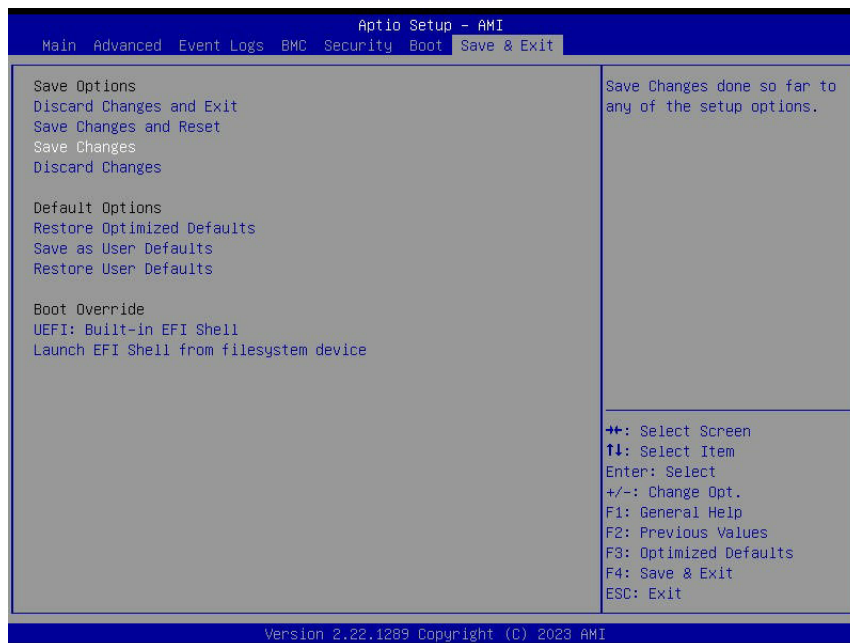


Figure 4-9: Save & Exit Options

Save Options

Discard Changes and Exit

Use this feature to exit from the BIOS Setup utility without making any permanent changes to the system configuration and reboot the computer.

Save Changes and Reset

When you have completed the system configuration changes, use this feature to exit the BIOS Setup utility and reboot the computer for the new system configuration parameters to become effective.

Save Changes

When you have completed the system configuration changes, use this feature to save all changes you've made. This will not reset (reboot) the system.

Discard Changes

Select this feature and press <Enter> to discard all the changes you've made and return to the BIOS Setup utility.

Default Options

Restore Optimized Defaults

Select this feature and press <Enter> to load manufacturer-optimized default settings, which are intended for maximum system performance but not for maximum stability.

Save as User Defaults

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

Restore User Defaults

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

Boot Override

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

Appendix A

BIOS POST Codes

A.1 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 <http://www.ami.com/products/>.

Appendix B

Software

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

B.1 Microsoft Windows OS Installation

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

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That might be a media, perhaps using an external USB/SATA Media drive, a USB flash drive, or the BMC KVM console.
2. Retrieve the proper RST/RSTe driver. Go to the Supermicro website for your motherboard information 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 a Windows OS installation. You can see a bootable device list by pressing **F11** during the system startup.

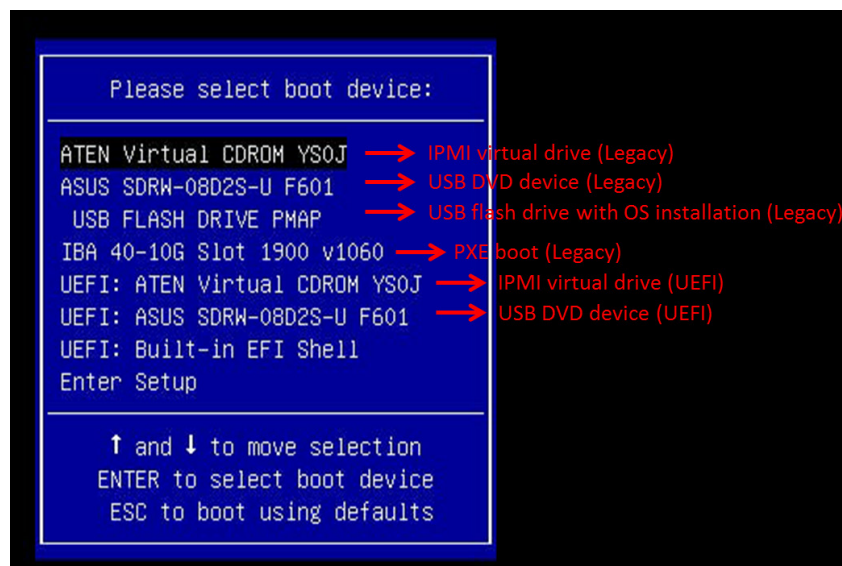


Figure B-1: Bootable Device List

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.

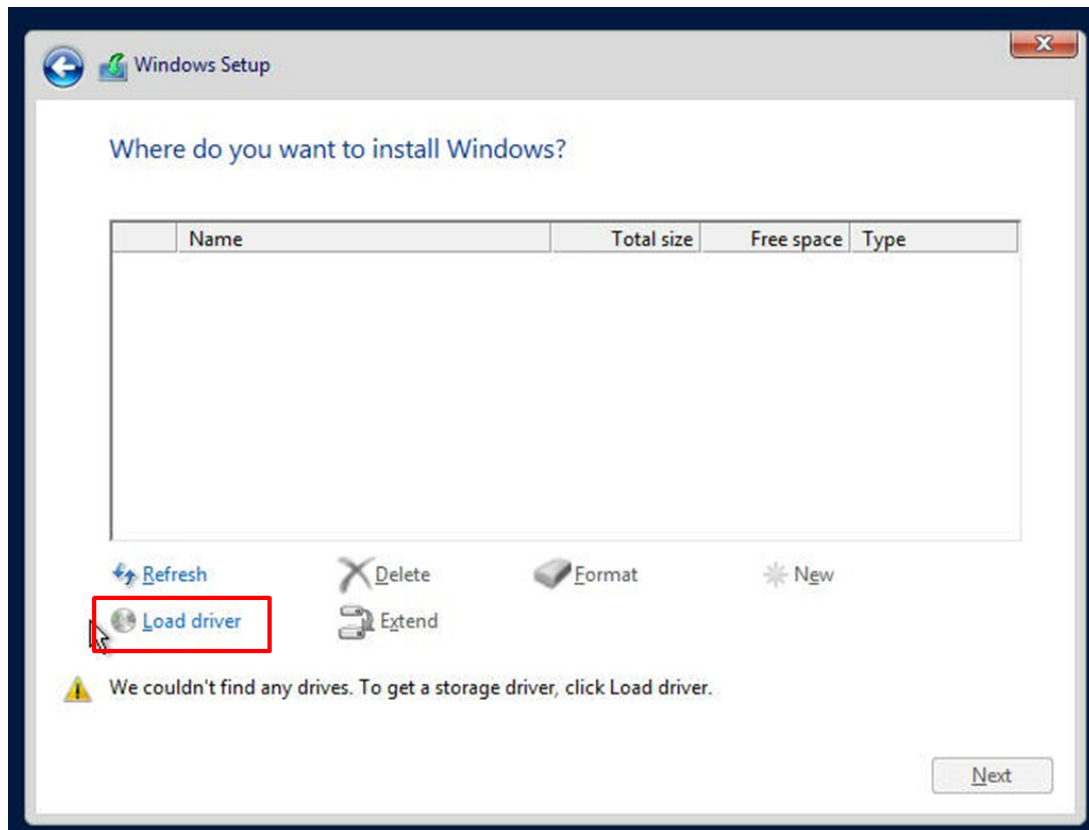


Figure B-2: Windows Setup

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

- For RAID, choose the SATA/sSATA RAID driver indicated and then choose the storage drive on which you want to install it.
 - For non-RAID, choose the SATA/sSATA AHCI driver indicated and choose the storage drive on which you want to install it.
5. Once all devices are specified, continue with the installation.
 6. After the Windows OS installation has completed, the system will automatically reboot multiple times.

B.2 Driver Installation

The Supermicro website contains drivers and utilities for your system at <https://www.supermicro.com/wdl/driver>. Some of these must be installed, such as the chipset driver.

After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash drive or a media drive. You may also use a utility to extract the ISO file if preferred.

Another option is to go to the Supermicro website at <http://www.supermicro.com/products/>. Find the product page for your motherboard, and "Download the Latest Drivers and Utilities". Insert the flash drive or disk, and the screenshot shown should appear.

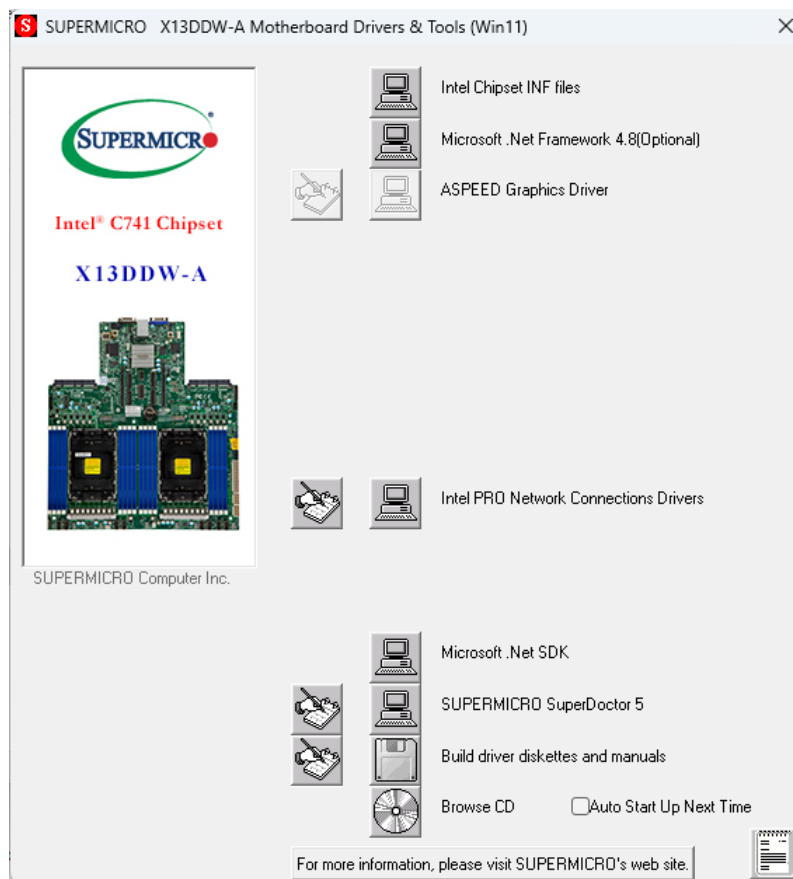


Figure B-3: Drivers & Tools



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

B.3 BMC

The X13DDW-A supports the Baseboard Management Controller (BMC). BMC is used to provide remote access, monitoring, and management. There are several BIOS settings that are related to BMC.

For general documentation and information on BMC, visit our website at: <http://www.supermicro.com/products/nfo/BMC.cfm>.

B.4 Logging into the Baseboard Management Controller (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, use the unique password provided by Supermicro to log in. You can change the unique password to a username and password of your choice for subsequent logins.

For more information regarding BMC passwords, visit our website at <http://www.supermicro.com/bmcpassword>.

Appendix C

Standardized Warning Statements

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

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

These warnings may also be found on our website at http://www.supermicro.com/about/policies/safety_information.cfm.

Battery Handling



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

電池の取り扱い

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

警告

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

警告

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

Warnung

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

Attention

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

¡Advertencia!

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

אזהרה!

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

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

اسبدال البطارية

فقط بنفس النوع أو ما يعادلها مما أوصت به الشركة المصنعة

جخلص من البطاريات المسحمة وفقا لعليمات الشركة الصانعة

경고!

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

Waarschuwing

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

Product Disposal



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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

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

경고!

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

Waarschuwing

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