

X13SET-PT

USER'S MANUAL

Revision 1.0a

The information in this user's manual has been carefully reviewed and is believed to be accurate. The manufacturer assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Note: For the most up-to-date version of this manual, 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 1.0a

Release Date: September 03, 2024

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 © 2024 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 motherboard.

About This Motherboard

The Supermicro X13SET-PT motherboard built with Intel® PCH C741 supports the 4th/5th Generation Intel® Xeon® Scalable Processors (LGA 4677 in Socket E) with up to 52 cores, and a thermal design power (TDP) of 300 W. The X13SET-PT motherboard also supports 2 TB of memory in eight memory slots. The 4th Generation Intel Xeon Scalable Processor memory has speeds of up to 4800 MT/s (4400 MT/s when fully populated), while the 5th Generation Intel Xeon Scalable Processor memory has speeds of up to 5600 MT/s (4400 MT/s when fully populated). This motherboard features superior IO expandability, which includes two PCIe 5.0 x16 slots for riser cards, one PCIe 5.0 x16 slot, one SXB1 slot for six SATA 3.0 ports, and two SATA 3.0 connectors (SuperDOMs). This motherboard also offers the most advanced data protection capability that encompasses Trusted Platform Module (TPM) and Root of Trust (RoT) support. X13SET-PT is optimized for high-density, high-end computing platforms for big data, virtualization,and enterprise applications. Note that this motherboard is intended to be installed and serviced by professional technicians only. For processor/memory updates, refer to our website at http://www.supermicro.com/products/.

Note 1: Supermicro X13 TwinPro system is designed to cap at 600 W per node. When system node power is over 600 W, power capping function will be enabled and cause CPU throttling. When system power is below 600 W, CPU will resume to normal operation automatically.

Note 2: Supported memory data transfer rate is subject to the specification of processor.

Conventions Used in the Manual

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



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



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



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



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

Contacting Supermicro

Headquarters

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

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	Sales_Europe@supermicro.com (General Information) Support_Europe@supermicro.com (Technical Support) RMA_Europe@supermicro.com (RMA Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	Sales-Asia@supermicro.com.tw (Sales Inquiry) Support@supermicro.com.tw (Technical Support) RMA@supermicro.com.tw (RMA Support)
Website:	www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Important Links 9
Quick Reference 12
Quick Reference Table 13
Motherboard Features 15
1.2 Processor and Chipset Support 19
Features Supported 19
1.3 Special Features 19
Recovery from AC Power Loss 19
1.4 System Health Monitoring 19
Onboard Voltage Monitors 19
Fan Status Monitor with Firmware Control 19
Environmental Temperature Control 20
1.5 ACPI Features 20
1.6 Power Supply 20
1.7 Serial Port 20

Chapter 2 Installation

2.1 Static-Sensitive Devices 21
Precautions 21
Unpacking 21
2.2 Processor and Heatsink Installation 22
The 4th/5th Generation Intel Xeon Scalable Processor 22
Installation Overview 23
Removal Overview 23
Create the Processor Carrier Assembly 24
Creating the PHM 28
Preparing the CPU Socket for Installation 30
Installing the PHM into the CPU Socket 31
Removing the PHM from the CPU Socket 32
Removing the Processor Carrier Assembly from the PHM 33
Removing the Processor from the Processor Carrier Assembly 34

2.3 Motherboard Installation 35
Tools Needed 35
Location of Mounting Holes 35
Installing the Motherboard 36
2.4 Memory Support and Installation 37
Memory Support 37
General Guidelines for Optimizing Memory Performance 40
DIMM Installation 41
DIMM Removal 41
2.5 Rear I/O Ports 42
2.6 Connectors 47
Power and Front Control Panel Connector 47
Headers 48
2.7 Jumper Settings 55
How Jumpers Work 55
2.8 LED Indicators 58

Chapter 3 Troubleshooting

3.1 Troubleshooting Procedures 61
Before Power On 61
No Power 61
No Video 62
System Boot Failure 62
Memory Errors 62
Losing the System's Setup Configuration 62
When the System Becomes Unstable 62
3.2 Technical Support Procedures 64
3.3 Frequently Asked Questions 65
3.4 Battery Removal and Installation 67
Battery Removal 67
Proper Battery Disposal 67
Battery Installation 67
3.5 Returning Merchandise for Service 68

Chapter 4 UEFI BIOS

4.1 Introduction....69

4.2 Main Setup....70

4.3 Advanced Setup Configurations....72

4.4 Event Logs....113

4.5 BMC....115

4.6 Security....119

4.7 Boot....125

4.8 Save & Exit....128

Appendix A BIOS POST Codes

A.1 BIOS POST Codes....130

Appendix B Software

B.1 Microsoft Windows OS Installation....131

Installing the OS....131

B.2 Driver Installation....133

B.3 BMC....134

B.4 Logging into the BMC....134

Appendix C Standardized Warning Statements

Chapter 1

Introduction

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

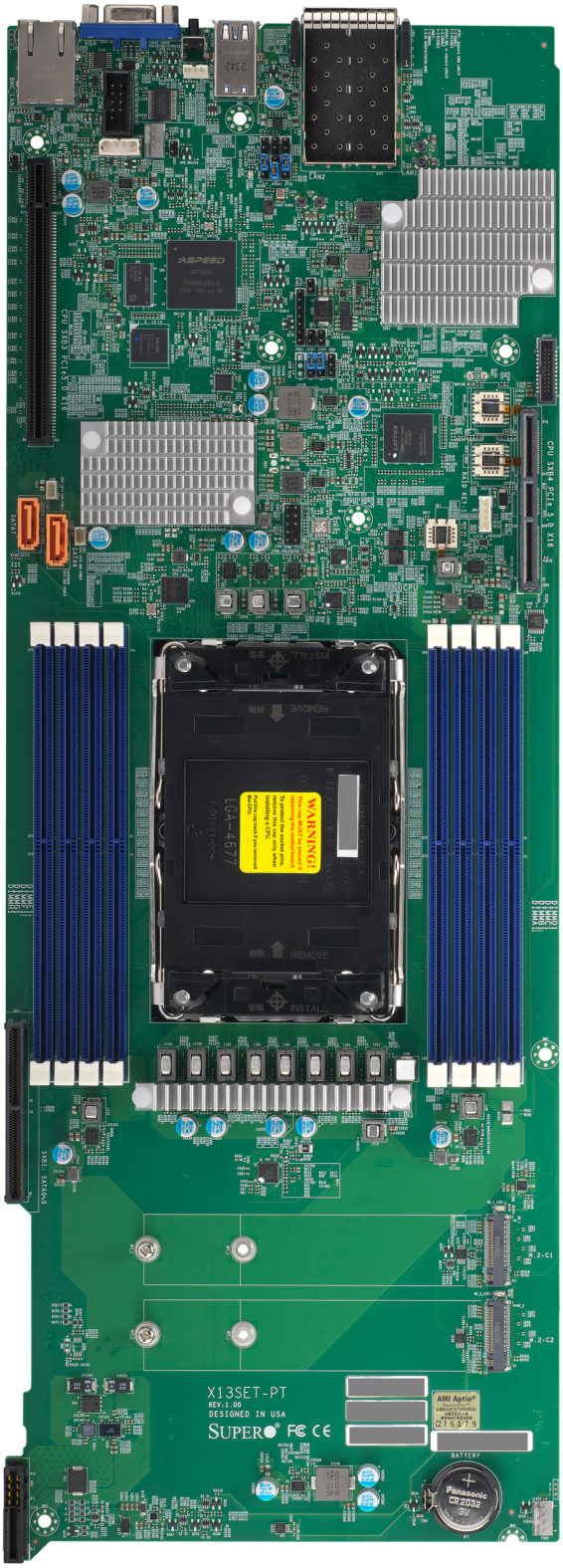
1.1 Important Links

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

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

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

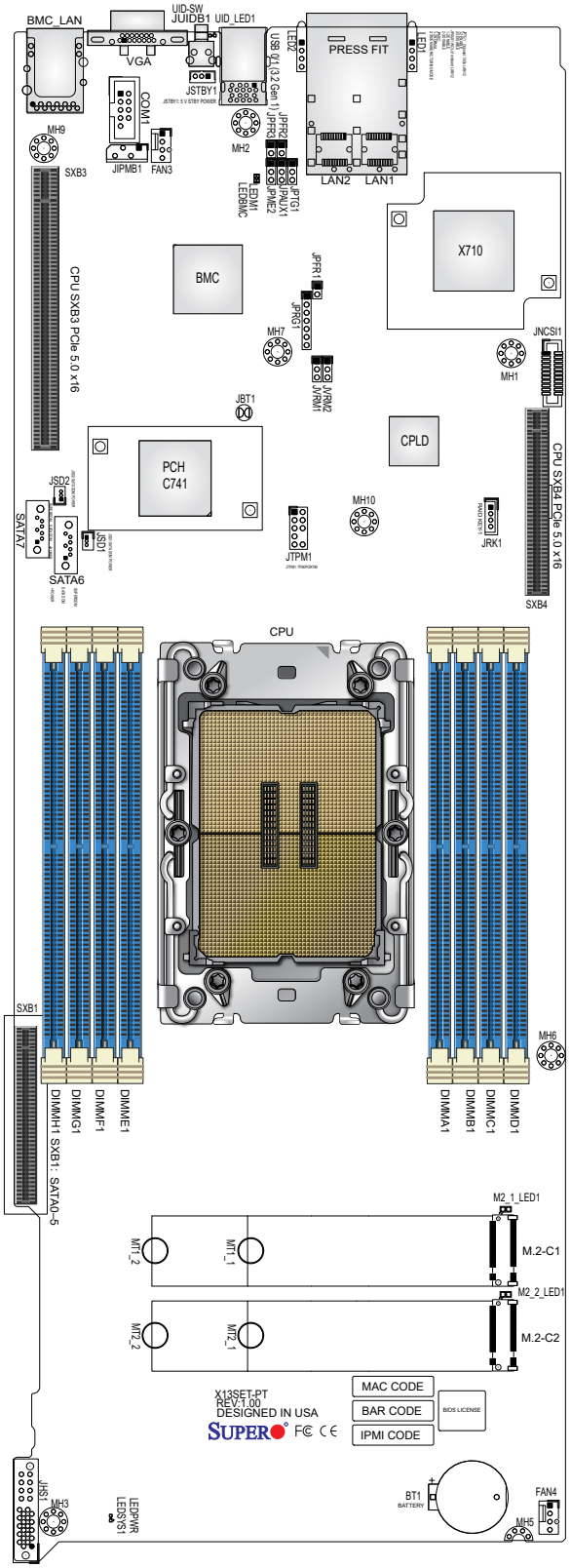
Figure 1-1. X13SET-PT Motherboard Image



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.

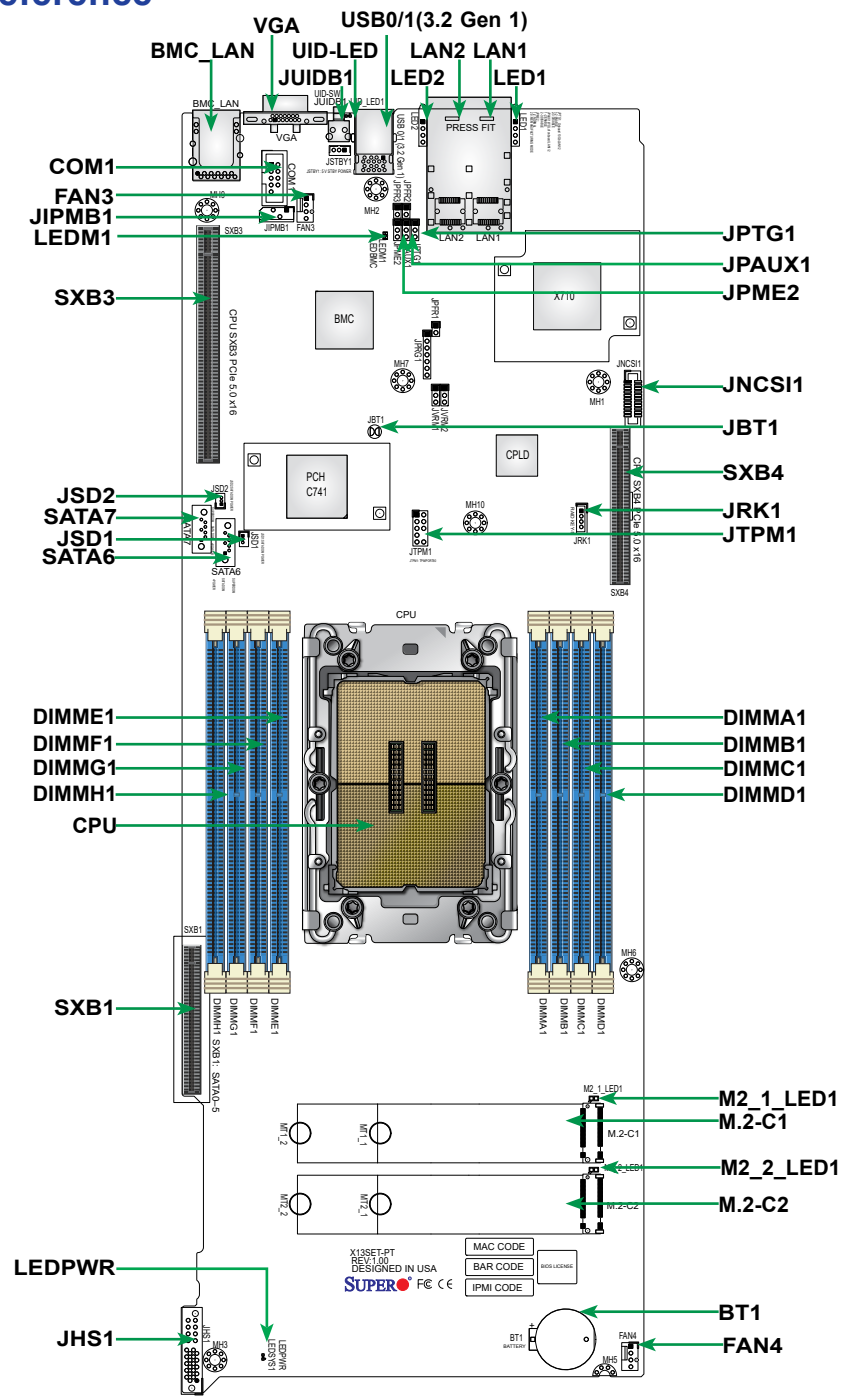
Figure 1-2. X13SET-PT Motherboard Layout

(not drawn to scale)



Note: Components not documented are for internal testing only.

Quick Reference



Notes:

- See Chapter 2 for detailed information on jumpers, I/O ports, and JHS1 front panel connections.
- "▪" indicates the location of Pin 1.
- Jumpers/LED indicators not indicated are used for testing only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. Do not install the onboard battery upside down to avoid possible explosion.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JPAUX1	10 Gb LAN1/LAN2 AUX Power Enable/Disable *Consult Supermicro before enabling this jumper. There must be sufficient airflow to enable JPAUX1 in standby mode (S5 state).	Pins 2-3 (Disabled)
JPME2	ME Manufacturing Mode	Pins 1-2 (Normal)
JPTG1	10 Gb LAN1/LAN2 Enable/Disable	Pins 1-2 (Enabled)

LED	Description	Status
HDD_LED1	HDD Activity LED	Blinking Green: HDD Active
LED1, LED2	SFP+ Port LEDs	Blinking Green (Bottom): Activity Solid Green (Top): 10 Gbps Link Speed Solid Yellow (Top): 1 Gbps Link Speed
LEDM1	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
M.2_1_LED1	M.2 LED for M.2-C1	Blinking Green: M.2 Active
M.2_2_LED1	M.2 LED for M.2-C2	Blinking Green: M.2 Active
UID-LED	Unit Identifier (UID) LED	Solid Blue: Unit Identified

Connector	Description
BMC_LAN	Dedicated BMC LAN Port
BT1	Onboard CMOS Battery
COM1	Front Accessible COM Port Header
FAN3, FAN4	4-pin CPU Fan Headers
JHS1	Supermicro Proprietary Front Control Panel Header
JIPMB1	4-pin BMC External I^2C Header
JNCSI1	NC-SI (Network Controller Sideband Interface) Connector
JSD1, JSD2	SATA DOM (Disk-On-Module) Power Connector
JTPM1	Trusted Platform Module/Port 80 Connector
JRK1	Intel VROC Key Header for NVMe RAID support
JUIDB1	Unit Identifier (UID) Switch / BMC Reset Button
LAN1, LAN2	10 Gb SFP+ Ports
M.2-C1, M.2-C2	M.2 M-Key PCIe 5.0 x4 Slots in the 2280/22110 form factors
SATA6, SATA7	Intel PCH Powered SATA 3.0 Ports with support for SuperDOM (Disk on Module) devices
SXB1	Six SATA connections (SATA0–5) supported by PCH
SXB3	PCIe 5.0 x16 Slot supported by CPU for the Supermicro proprietary riser card
SXB4	PCIe 5.0 x16 Slot supported by CPU for the Supermicro proprietary riser card

Note: The table is continued on the next page.

USB0, USB1	Rear I/O USB Ports (USB 3.2 Gen 1)
VGA	Rear VGA Port on the I/O back panel

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: http://www.supermicro.com/support/manuals/.

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: http://www.supermicro.com/support/manuals/.

Motherboard Features

Motherboard Features	
Processor	
• Supports the 4th/5th Generation Intel Xeon Scalable Processors (LGA 4677 in Socket E) with up to 52 cores and a thermal design power (TDP) of up to 300 W	
Memory	
• Up to 4096GB of 3DS RDIMM ECC DDR5 DDR5 memory • Memory speeds of up to 4800 MT/s (DDR5-4400 MT/s when fully populated) in eight memory slots (4th Generation Intel Xeon) • Memory speeds of up to 5600 MT/s (DDR5-4400 MT/s when fully populated) in eight memory slots (5th Generation Intel Xeon) **Note:** Supported memory data transfer rate is subject to the specification of processor.	
DIMM Size	
• 16 GB, 24 GB, 32 GB, 48 GB, 64 GB, 96 GB, 128 GB, 256 GB at 1.2 V **Note:** For the latest CPU/memory updates, refer to our website at http://www.supermicro.com/products/motherboard.	
Chipset	
• Intel PCH C741	
Expansion Slots	
• One PCIe 5.0 x16 slot (SXB3) supported by CPU for the riser card • One PCIe 5.0 x16 slot (SXB4) supported by CPU for the riser card • Two M.2 PCIe 5.0 x4 slots in 2280 and 22110 form factors	
Network	
• Two rear 10 Gb SFP+ ports via Intel X710 BM2 • One rear dedicated BMC LAN via AST2600	
Baseboard Management Controller (BMC)	
• ASPEED AST2600	
Graphics	
• ASPEED AST2600 Graphics Controller	
I/O Devices	
• Serial (COM) Port	• One front accessible serial port header (COM1)
• SATA 3.0	• Six SATA 3.0 ports at 6 Gb/s (SATA0–5) via SXB1 slot • Two SATA 3.0 ports built-in power-pins for SuperDOM (SATA6, SATA7)
• Video (VGA) Connections	• One rear VGA port

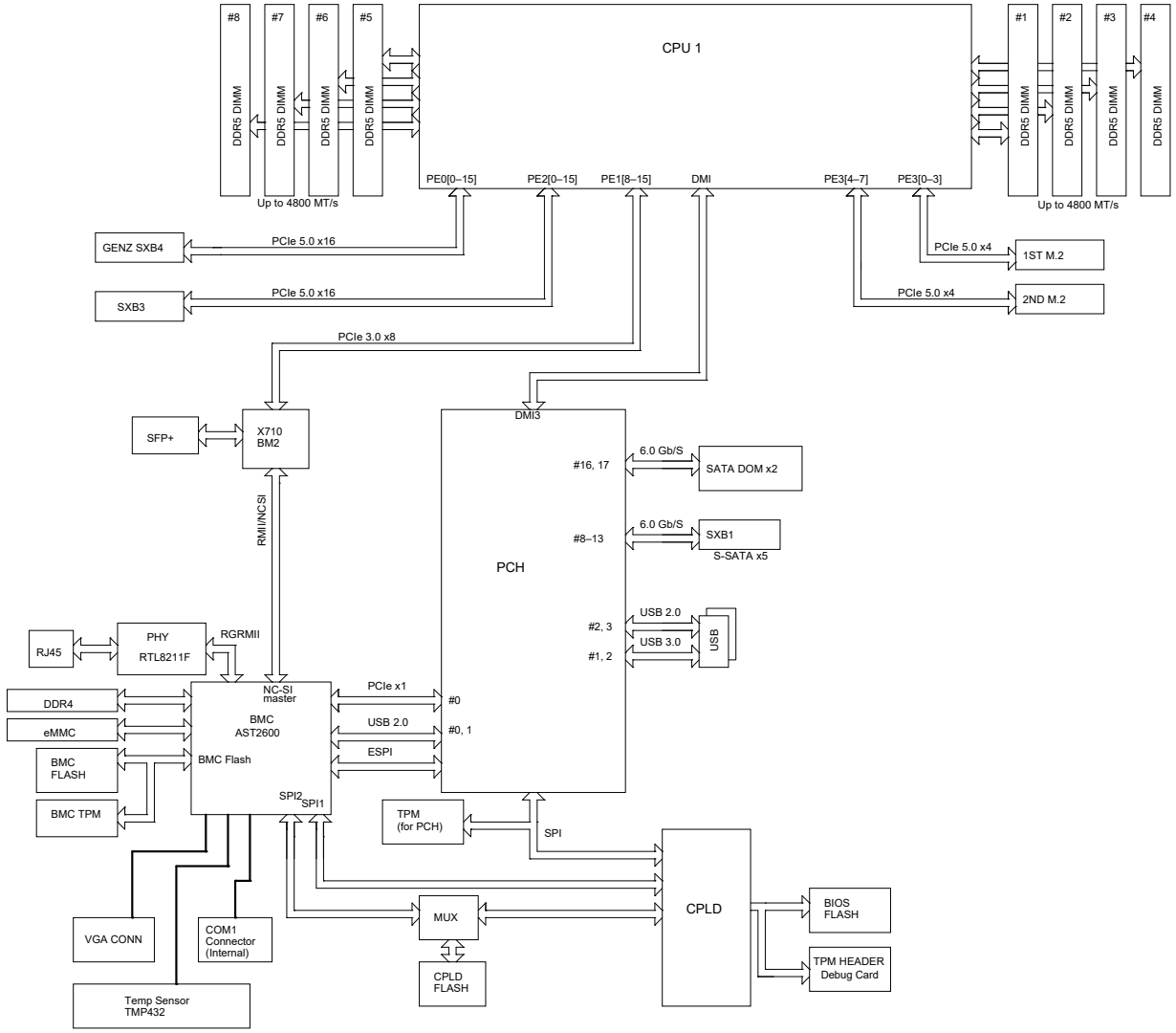
Note: The table is continued on the next page.

Peripheral Devices
• Two rear accessible USB 3.2 Gen 1 ports (USB0/1)
BIOS
• AMI BIOS • ACPI 6.0 or later, PCI firmware 4.0 support, SPI dual/quad speed support, Real Time Clock (RTC) wake up, riser card auto detection support, and SMBIOS 3.0 or later
Power Management
• ACPI power management • Power button override mechanism • Power-on mode for AC power recovery • Wake-on-LAN • Power supply monitoring
System Health Monitoring
• Onboard voltage monitoring for +3.3 V, +5 V, +12 V, +3.3 Vstb, +5 Vstb, Vcore, Vmem • Onboard temperature monitoring for CPU, PCH, system, memory, and peripheral • CPU thermal trip support • Platform Environment Control Interface (PECI)/TSI
Fan Control
• Fan status monitoring via BMC connections • Single cooling zone • Low-noise fan speed control • Two 4-pin fan headers
System Management
• Server platform service • IPMIView, SMCIPMITOOL, IPMICFG • Redundant power supply unit detection sensor • Plug-in tools through Redfish
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
• CPU / System overheat LED • Power / suspend-state indicator LED • Fan failed LED • UID / remote UID • LAN activity LED
Dimensions
• Proprietary 6.8" x 18.86" (172.72 mm x 479.04 mm) (W x L)

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

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

Figure 1-3.
System Block Diagram



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

1.2 Processor and Chipset Support

Built upon the functionality and capability of the 4th and 5th Generation Intel Xeon Processor (Socket E) with the Intel C741 chipset, the X13SET-PT motherboard increases energy efficiency, and system performance for a multitude of applications such as high performance computing, Hyper-Converged Infrastructure, big data, and enterprise applications.

Features Supported

- Vector Neural Network Instructions (VNNI) support to accelerate training
- New hardware-enhanced security features help protect platform and data without compromising performance
- High PCIe performance (PCIe 5.0) with double the bandwidth of PCIe 4.0

1.3 Special Features

Recovery from AC Power Loss

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

1.4 System Health Monitoring

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

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

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

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.

1.7 Serial Port

The X13SET-PT motherboard supports one serial communication connection (COM1). COM1 port header can be used for input/output. The UART provides legacy speeds with a baud rate of up to 115.2 Kbps as well as an advanced speed with baud rates of 250 K, 500 K, or 1 Mb/s, which support high-speed serial communication devices.

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 possible explosion.

Unpacking

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

2.2 Processor and Heatsink Installation

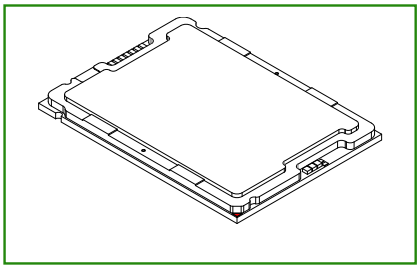
The processor (CPU) and processor carrier should be assembled together first to form the processor carrier assembly. This will be attached to the heatsink to form the processor heatsink module (PHM) before being installed onto the CPU socket.

Notes:

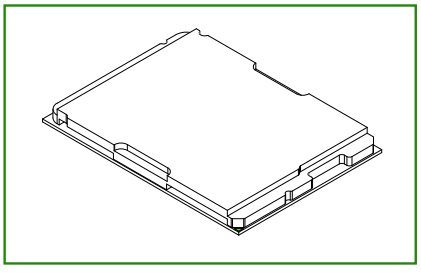
- Use ESD protection.
- Shut down the system and then unplug the AC power cord from all power supplies.
- Check that the plastic protective cover is on the CPU socket and none of the socket pins are bent. If they are, contact your retailer.
- When handling the processor, avoid touching or placing direct pressure on the LGA lands (gold contacts). Improper installation or socket misalignment can cause serious damage to the processor or socket, which may require manufacturer repairs.
- When installing the processor and heatsink, ensure a torque driver set to the correct force is used for each screw.
- Thermal grease is pre-applied on a new heatsink. No additional thermal grease is needed.
- Installing the PHM to the motherboard socket requires a Torx T30 screwdriver.
- Refer to the Supermicro website for updates on processor support.
- All graphics in this manual are for illustration purposes only. Your components may look different.
- Please order the CPU carrier to pair with the CPU.

CPU carrier for 4th/5th Generation Intel Xeon Scalable Processors (XCC)	SKT-1333L-0000-FXC
CPU carrier for 4th/5th Generation Intel Xeon Scalable Processors (MCC)	SKT-1424L-001B-FXC

The 4th/5th Generation Intel Xeon Scalable Processor



SP XCC



SP MCC

Installation Overview

There are four steps to installing the processor and heatsink onto the motherboard.

1. Attach the processor to a plastic carrier to create the processor carrier assembly.
2. Attach the processor carrier assembly to the heatsink to create the processor heatsink module (PHM).
3. Prepare the socket for PHM installation.
4. Install the PHM.

Removal Overview

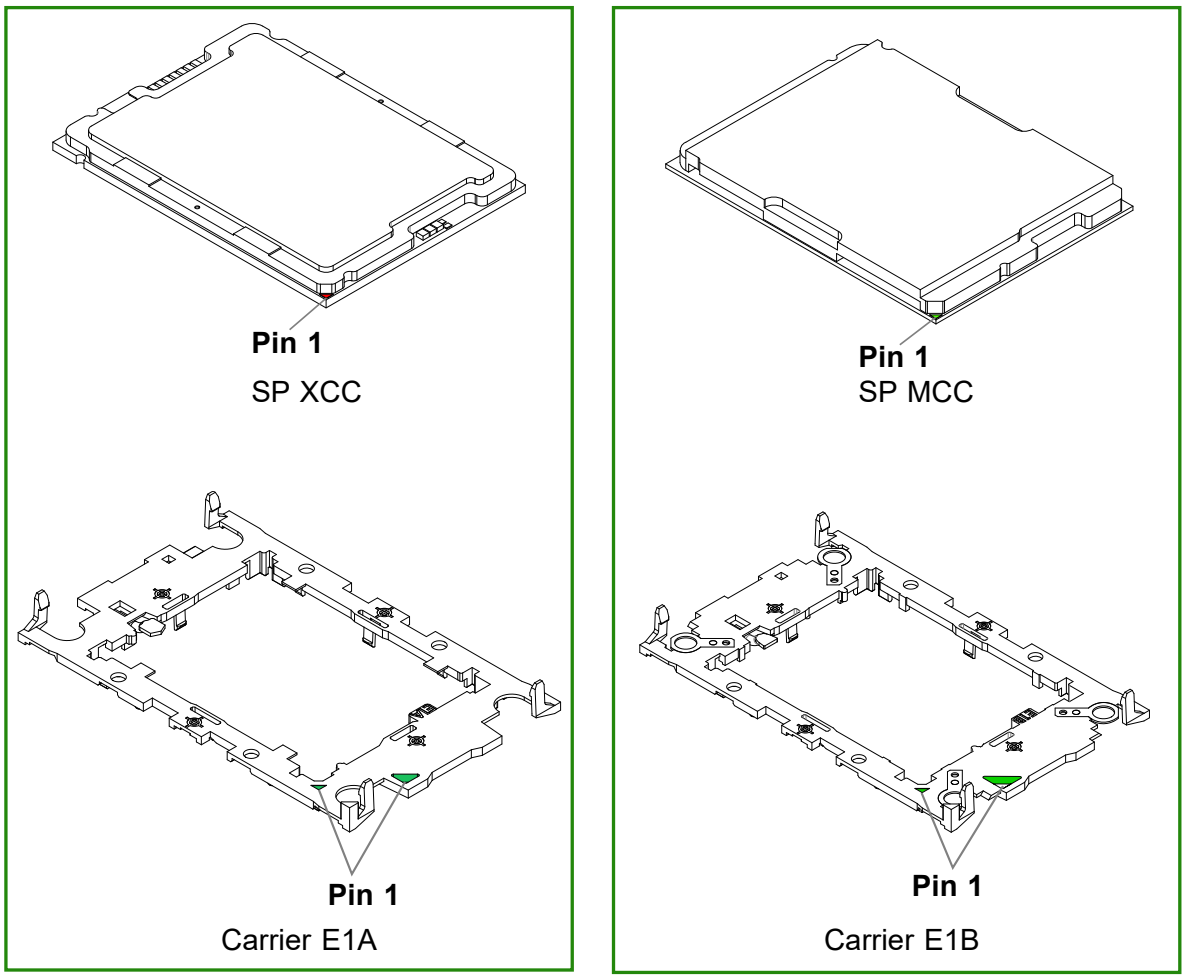
There are three steps to removing the processor and heatsink from the motherboard.

1. Remove the PHM from the motherboard.
2. Remove the processor carrier assembly from the heatsink.
3. Remove the processor from the carrier.

Create the Processor Carrier Assembly

Processor Carrier Assembly

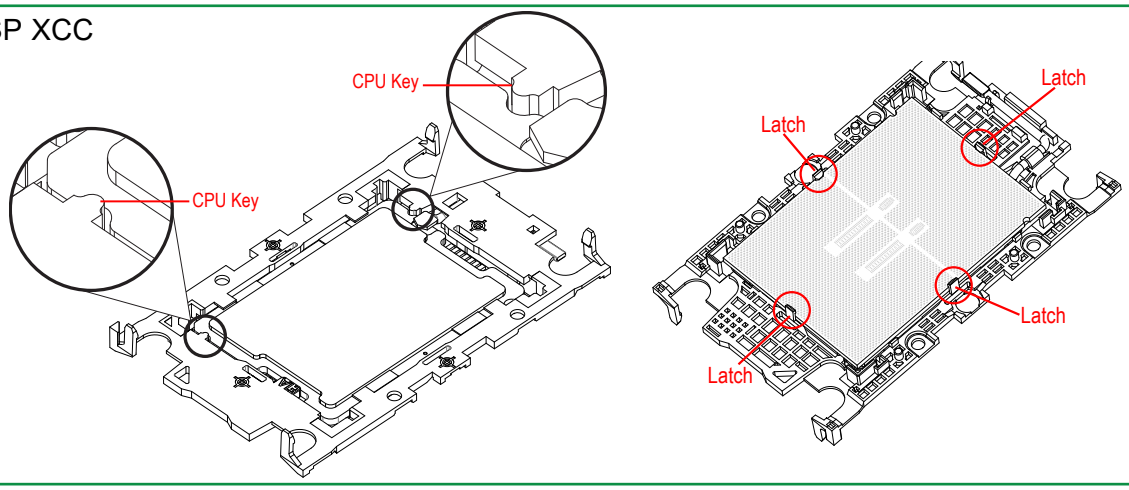
1. Hold the processor with the gold pins (LGA lands) facing down. Locate the gold triangle at the corner of the processor and the corresponding hollowed triangle on the processor carrier as shown below. These triangles indicate the location of pin 1.



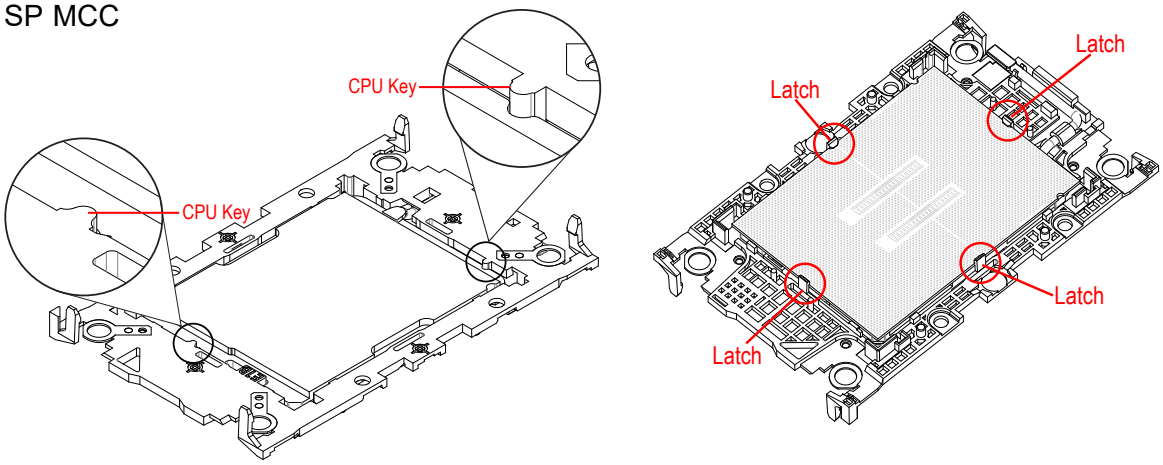
The Processor with its Matching Carrier

2. Turn the processor over with the gold pins up. Locate the CPU keys on the processor and the four latches on the carrier as shown below.

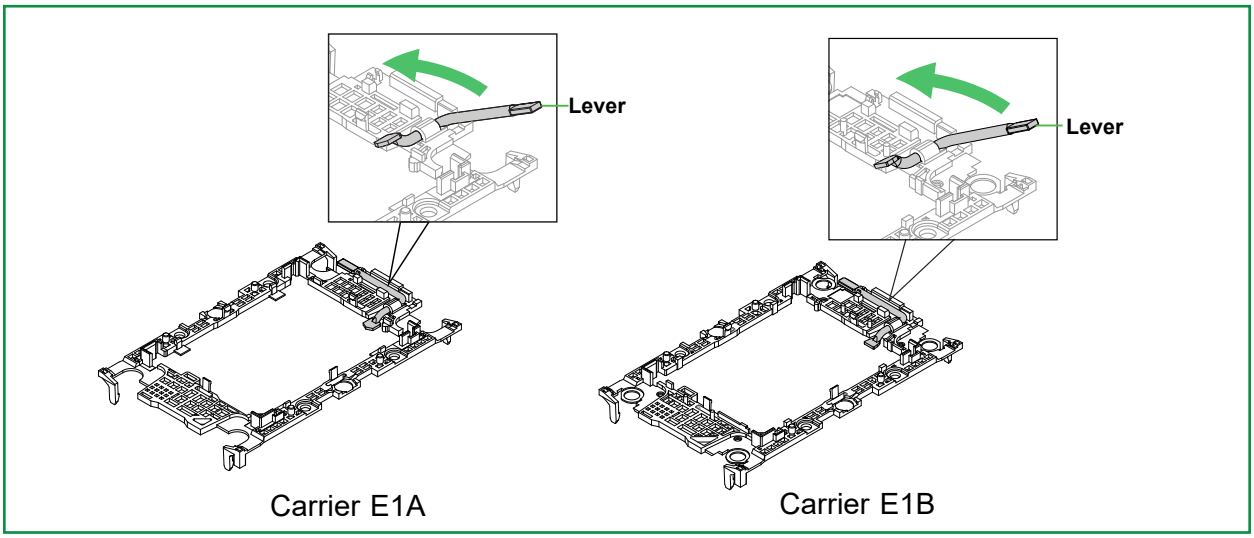
SP XCC



SP MCC

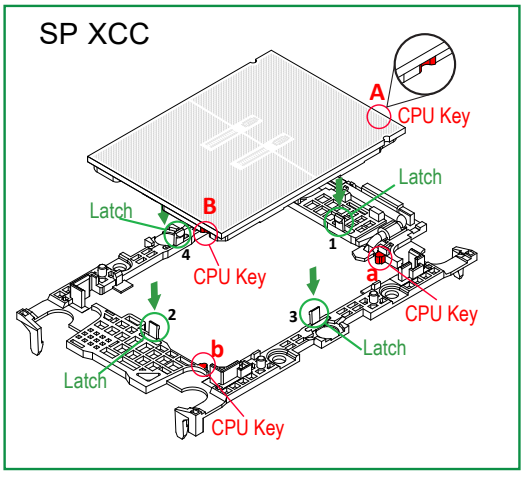


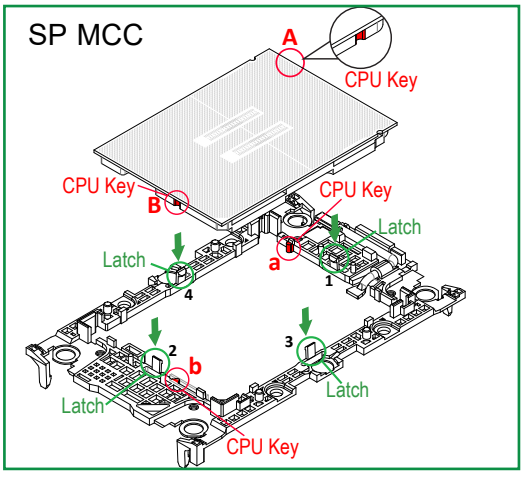
3. Locate the lever on the CPU socket and press it down as shown below.



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

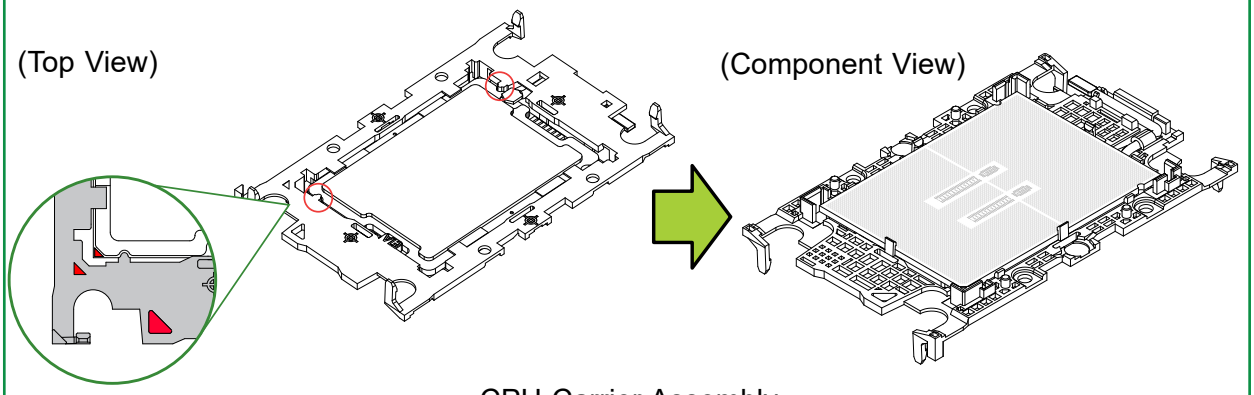
5. Once they are properly aligned, carefully insert the CPU into the carrier, making sure that the CPU is properly secured by latches 1, 2, 3, and 4. After the processor is placed inside the carrier, examine the four sides of the processor, making sure that the processor is properly seated on the carrier.





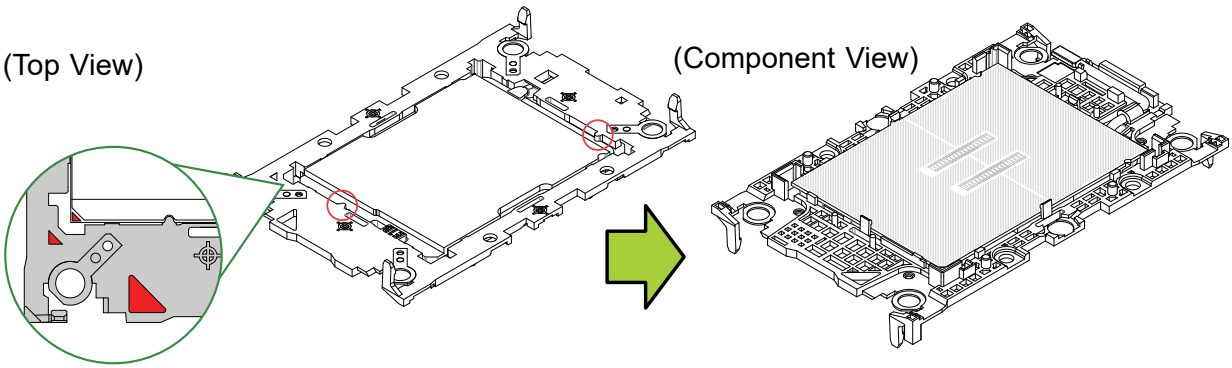
6. After the processor is placed inside the carrier, examine the four sides of the processor, making sure that the processor is properly seated on the carrier.

SP XCC



CPU Carrier Assembly

SP MCC



CPU Carrier Assembly

Creating the PHM

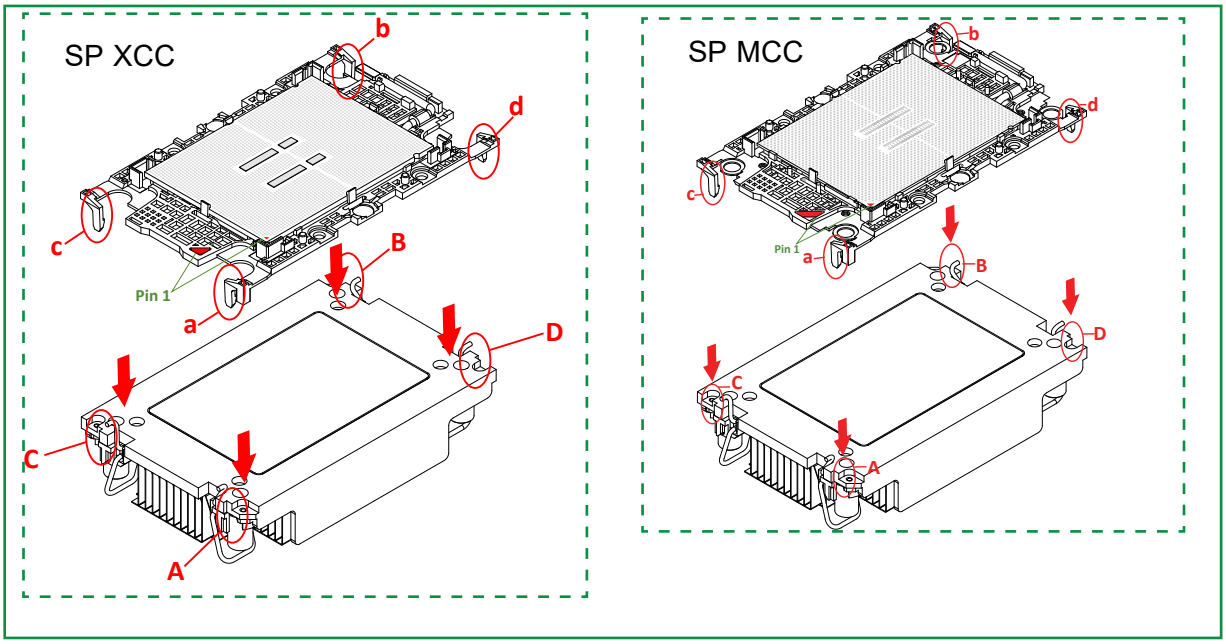
After creating the processor carrier assembly, follow the instructions below to mount the processor carrier into the heatsink to form the PHM.

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

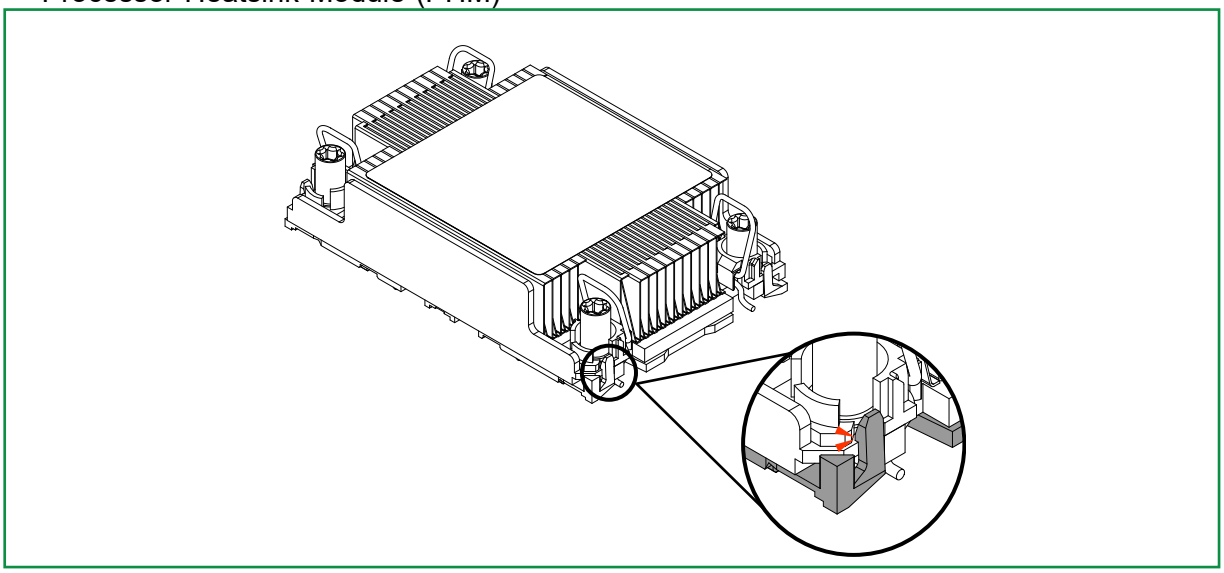
1. Turn the heatsink over with the thermal grease, which is on the reverse side of the heatsink, facing up.
2. With the processor gold contacts facing up, locate the triangle on the CPU and the triangle on the carrier. (Triangle indicates Pin 1.)
3. Follow the illustration to align corners A, B, C, and D of the heatsink with corners a, b, c, and d of the processor carrier assembly.
4. 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. Ensure that all plastic clips are properly attached to the heatsink.

CPU Carrier Assembly

(CPU Component Side and Heatsink Bottom Side)



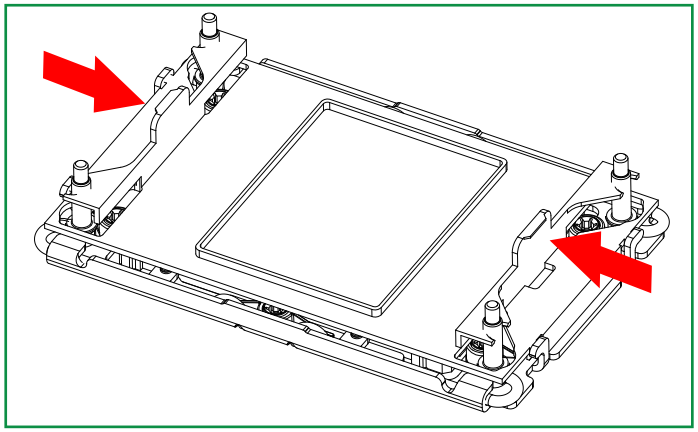
Processor Heatsink Module (PHM)



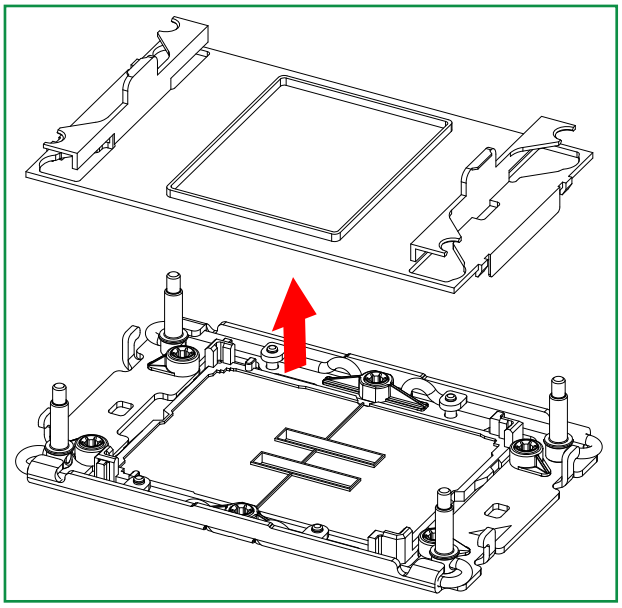
Preparing the CPU Socket for Installation

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

1. Press the tabs inward.



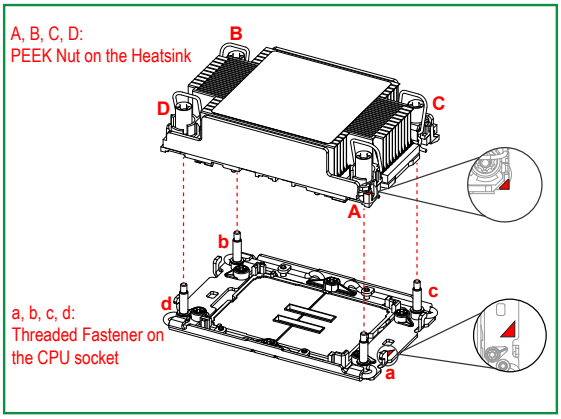
2. Pull up the protective cover from the socket.



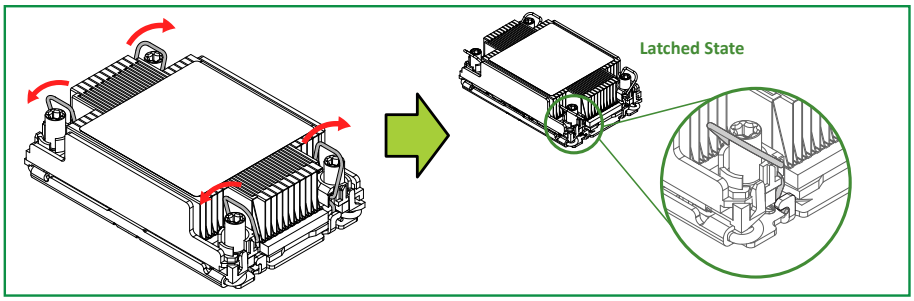
Installing the PHM into the CPU Socket

1. Locate four threaded fasteners on the CPU socket.

2. Follow the illustration to align PEEK nuts A, B, C, and D of the heatsink with threaded fasteners a, b, c, and d on the CPU socket.



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

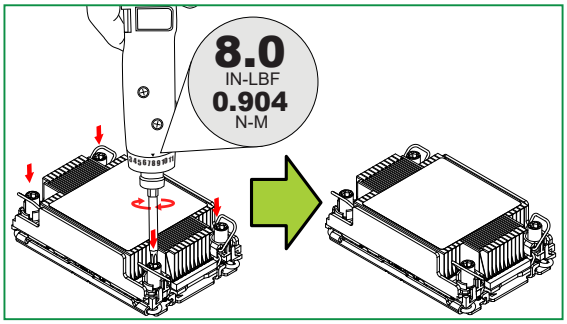


4. Press all four rotating wires outwards to ensure that the heatsink is securely latched onto the CPU socket.

5. Starting with two screws on opposite corners, use a T30 bit torque driver set to a force of 8.0 in-lbf (0.904 N-m) to tighten the PEEK nuts on the heatsink.

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.

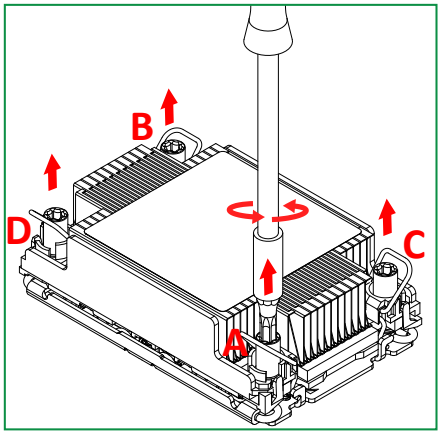
6. Examine all corners of the heatsink to ensure that the PHM is firmly attached to the CPU socket.



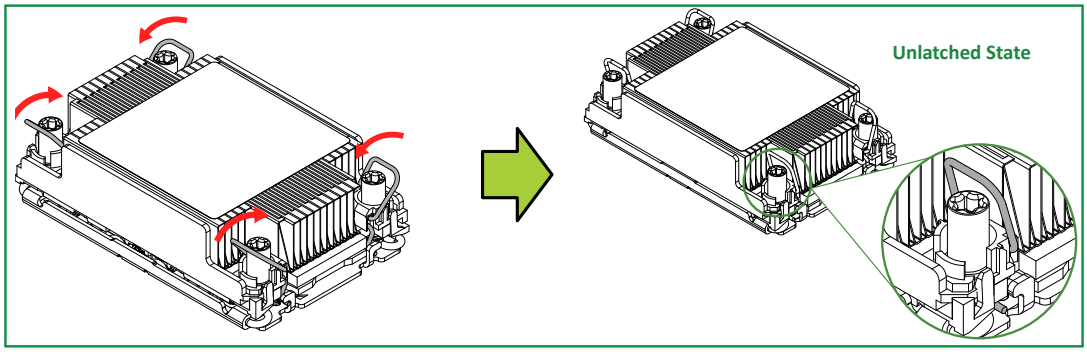
Removing the PHM from the CPU Socket

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 below:

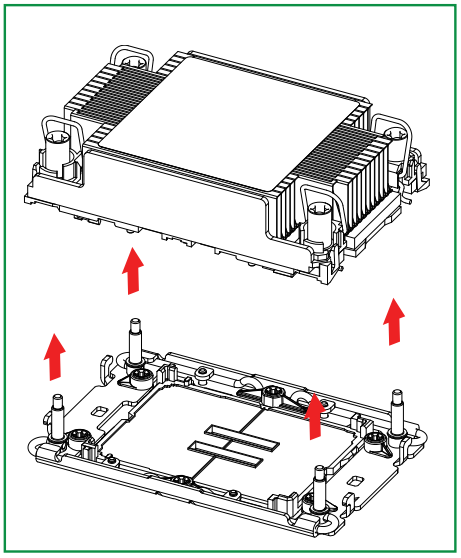
1. Starting with two screws on opposite corners, use a T30 torx-bit screwdriver to loosen the PEEK nuts on the heatsink.



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



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

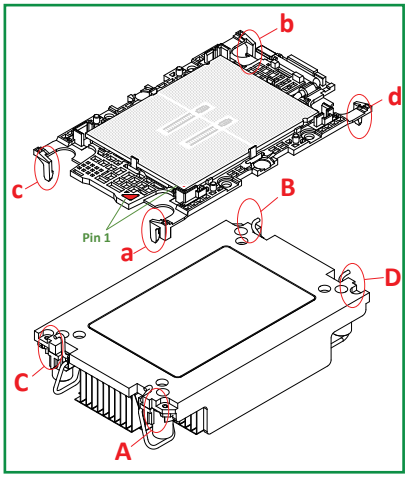


Removing the Processor Carrier Assembly from the PHM

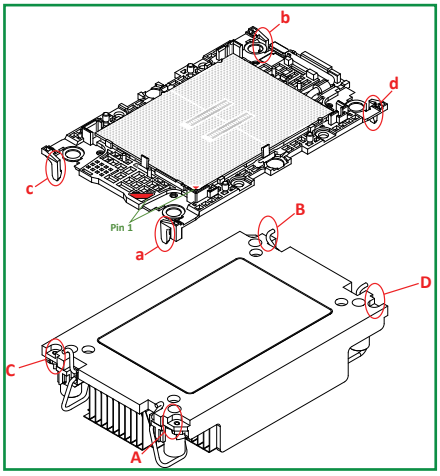
To remove the processor carrier assembly from the PHM, please follow the steps below:

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

1U Heatsink (View of Gold Contacts Facing Up and Heatsink Bottom Side)



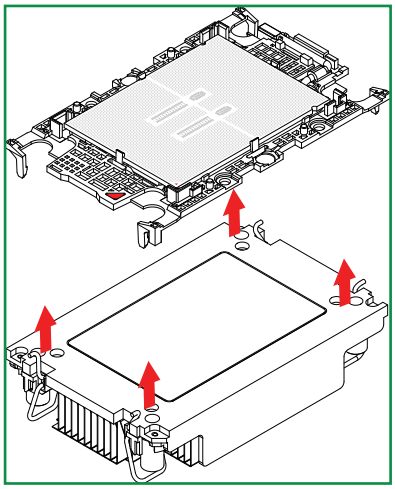
SP XCC



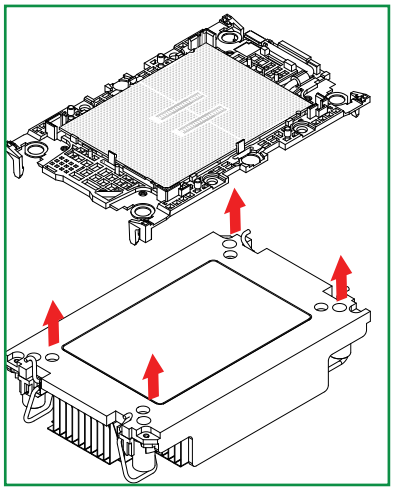
SP MCC

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

1U Heatsink (View of Gold Contacts Facing Up and Heatsink Bottom Side)



SP XCC

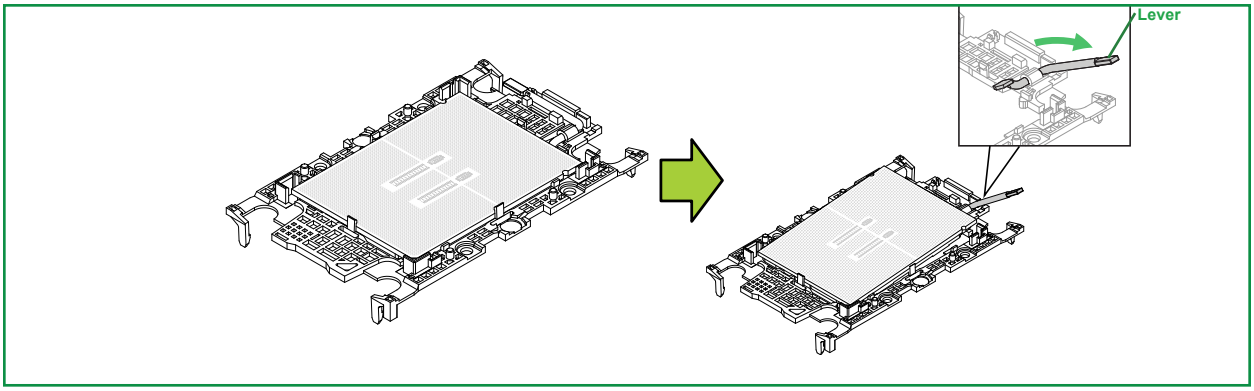


SP MCC

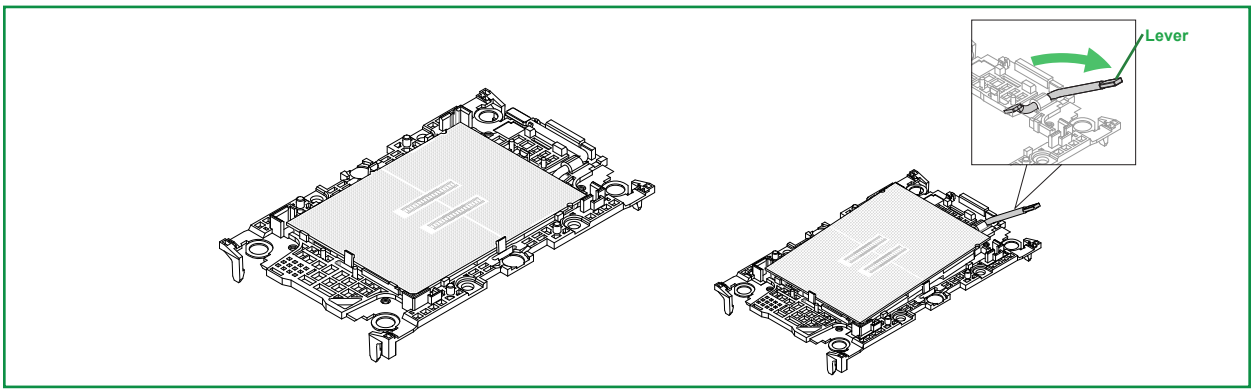
Removing the Processor from the Processor Carrier Assembly

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

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



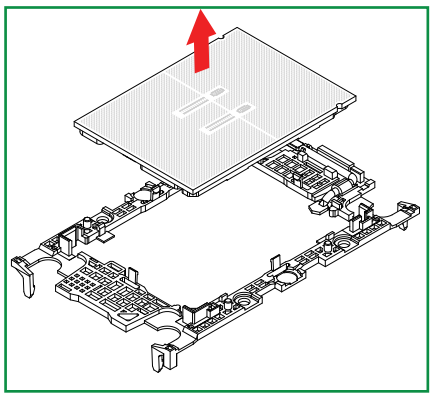
CPU Carrier Assembly (carrier E1A)



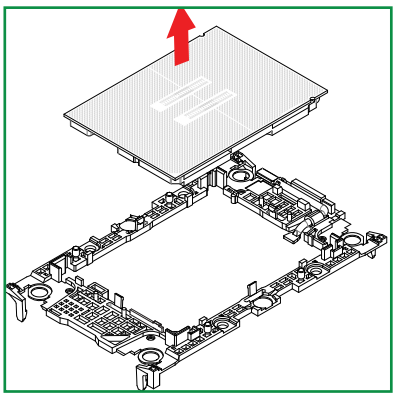
CPU Carrier Assembly (carrier E1B)

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

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



SP XCC

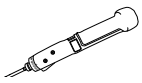


SP MCC

2.3 Motherboard Installation

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

Tools Needed



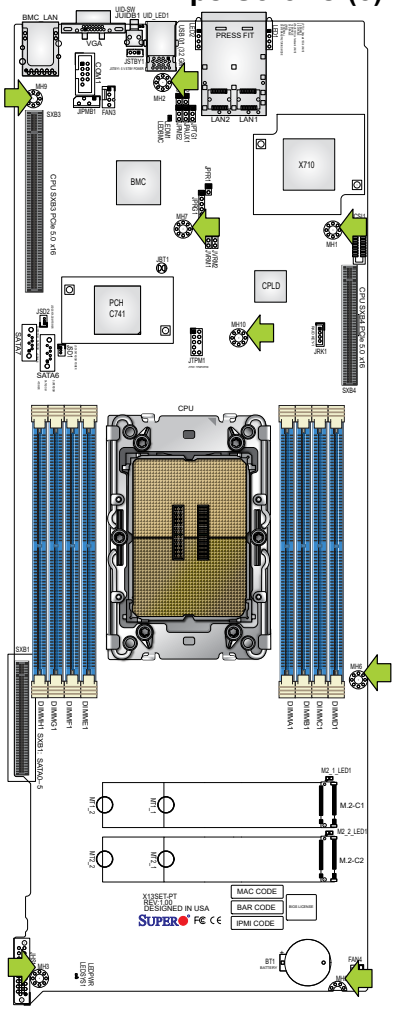
Torque Driver (1)



Phillips Screws (8)



Standoffs (8)
(Only if Needed)



Location of Mounting Holes

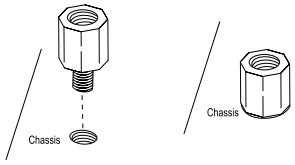
Note 1: Do not use a force greater than 8 in-lbf (0.904 N-m) on each mounting screw during motherboard installation. Exceeding this force may over-torque the screw, causing damage to the motherboard and screw.

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

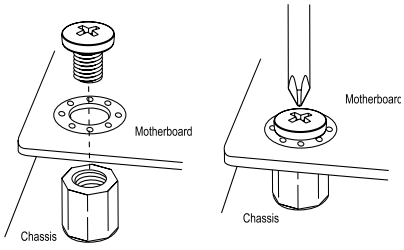
Installing the Motherboard

1. 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 locations.



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



4. Install standoffs in the chassis as needed.

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

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

7. Repeat Step 6 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 DIMM modules to prevent any possible damage.

Memory Support

The X13SET-PT motherboard supports 2 TB of 3DS RDIMM ECC DDR5 memory in eight memory slots. The 4th Generation Intel Xeon Scalable Processor memory has speeds of up to 4800 MT/s (4400 MT/s when fully populated), while the 5th Generation Intel Xeon Scalable Processor memory has speeds of up to 5600 MT/s (4400 MT/s when fully populated).

Note: Use one DIMM per channel when populating the channels.

1 CPU, 8 DIMM Slots	
Number of DIMMs	**Memory Population Sequence**
1	DIMMA1 DIMME1
2	DIMMA1 / DIMMG1 DIMMC1 / DIMME1
4	DIMMA1 / DIMMG1 / DIMMC1 / DIMME1
6	DIMMA1 / DIMMG1 / DIMMC1 / DIMME1 / DIMMD1 / DIMMF1 DIMMA1 / DIMMG1 / DIMMC1 / DIMME1 / DIMMB1 / DIMMH1 DIMMC1 / DIMME1 / DIMMB1 / DIMMH1 / DIMMD1 / DIMMF1 DIMMA1 / DIMMG1 / DIMMB1 / DIMMH1 / DIMMD1 / DIMMF1
8	DIMMA1 / DIMMG1 / DIMMB1 / DIMMH1 / DIMMD1 / DIMMF1 / DIMMC1 /DIMME1

Compatible and Incompatible DIMM Types in a Channel and a System			
DIMM Type	**RDIMM**	**RDIMM 3DS**	**9x4 RDIMM**
RDIMM	Compatible	Incompatible	Incompatible
RDIMM 3DS	Incompatible	Compatible	Incompatible
9x4 RDIMM	Incompatible	Incompatible	Compatible

DDR5 Memory Support for the 4th Generation Intel® Xeon® Scalable Processors-SP					
Type	**Ranks Per DIMM and Data Width (Stack)**	**DIMM Capacity (GB)**		**Speed (MT/s)**	
				One DIMM per Channel [1]	**Two DIMMs per Channel**
		Memory Density 16 Gb	**Memory Density 24 Gb[2]**	**1.1 Volts**	
RDIMM	SRx8 (RC D)	16 GB	24 GB	4800*	4400*
	SRx4 (RC C)	32 GB	48 GB		
	SRx4 (RC F) 9x4	32 GB	NA		
	DRx8 (RC E)	32 GB	48 GB		
	DRx4 (RC A)	64 GB	96 GB		
	DRx4 (RC B) 9x4	64 GB	NA		
RDIMM 3DS	(4R/8R) x4 (RC A)	2H-128 GB 4H-256 GB	NA		

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

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

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

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

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

DDR5 Memory Support for the 5th Generation Intel® Xeon® Scalable Processors-SP					
Type	**Ranks Per DIMM and Data Width (Stack)**	**DIMM Capacity (GB)**		**Speed (MT/s)**	
				One DIMM per Channel [1]	**Two DIMMs per Channel**
		Memory Density 16 Gb	**Memory Density 24 Gb**	**1.1 Volts**	
RDIMM	SRx8 (RC D)	16 GB	24 GB[2]	5600*	4400*
	SRx4 (RC C)	32 GB	48 GB[2]		
	SRx4 (RC F) 9x4	NA	NA		
	DRx8 (RC E)	32 GB	48 GB[2]		
	DRx4 (RC A)	64 GB	96 GB		
	DRx4 (RC B) 9x4	NA	NA		
RDIMM 3DS	(4R/8R) x4 (RC A)	2H-128 GB 4H-256 GB	NA		

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

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

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

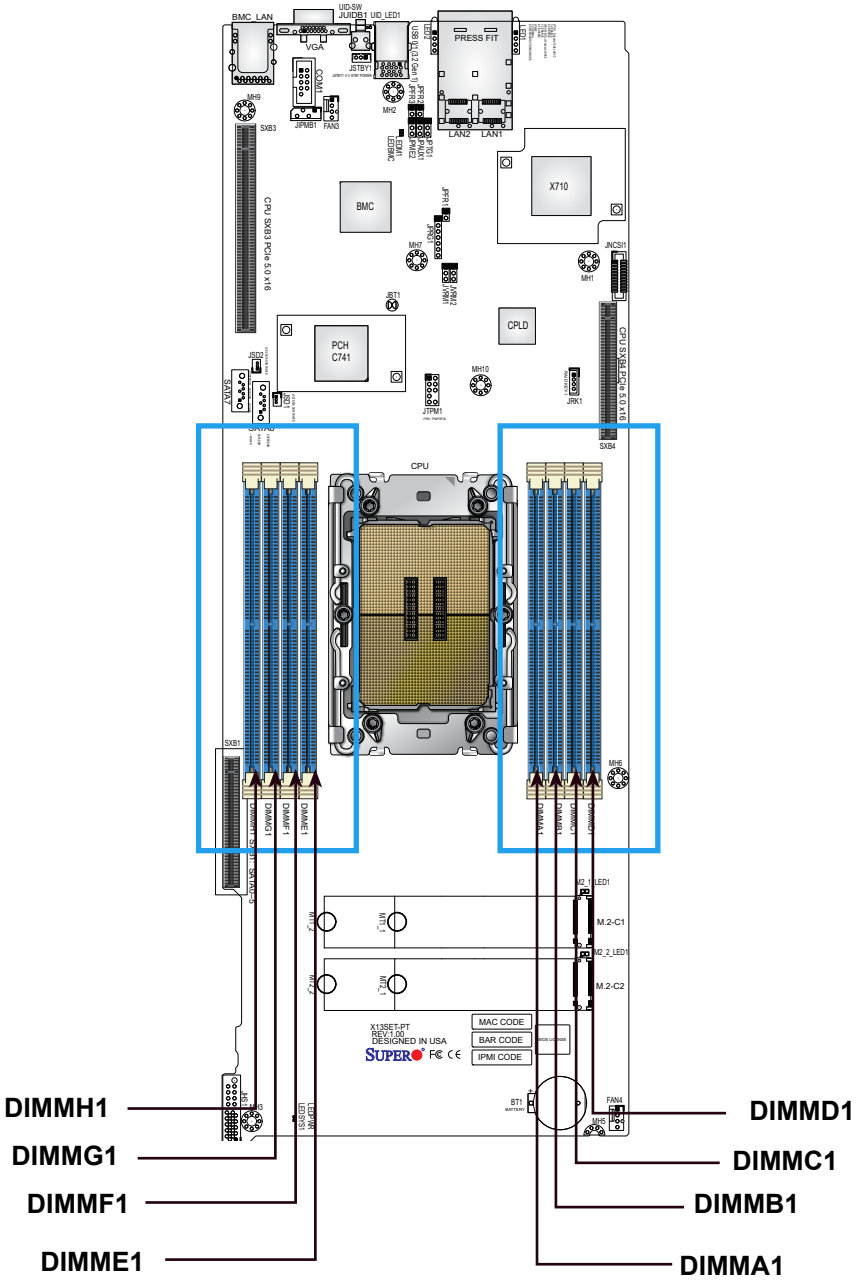
Note 3: Memory speed will be 5600 MT/s 1DPC and 4400 MT/s 2DPC.

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

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

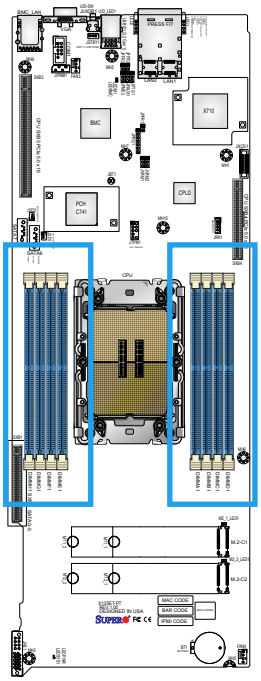
General Guidelines for Optimizing Memory Performance

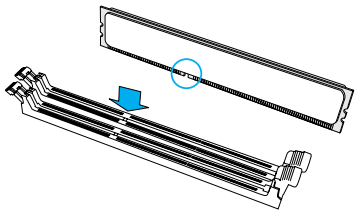
- It is recommended to use DDR5 memory of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- Some DIMM types are not compatible with each other. Refer to Compatible and Incompatible DIMM Types in a Channel and a System on page 32.
- The motherboard will not support an odd number amount of modules except for a single DIMM module necessary for board operation. However, to achieve the best memory performance, a balanced (even number) memory population is recommended.

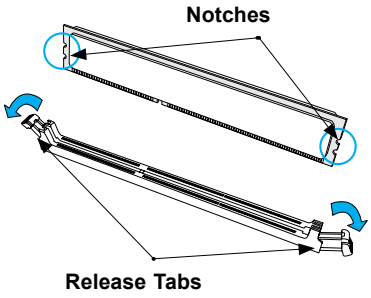


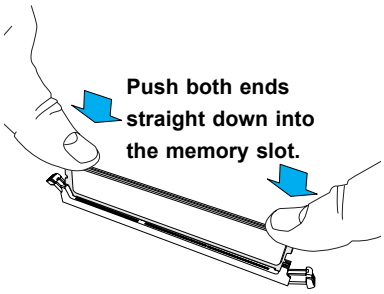
DIMM Installation

1. Insert the desired number of DIMMs into the memory slots based on the Recommended Memory Population Guide tables on page 32.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.
3. Align the key of the DIMM module with the receptive point on the memory slot.
4. Align the notches on both ends of the module against the receptive points on the ends of the slot.
5. Push both ends of the module straight down into the slot until the module snaps into place.
6. Press the release tabs to the lock positions to secure the DIMM module into the slot.









DIMM Removal

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

2.5 Rear I/O Ports

See Figure 2-1 below for the locations and descriptions of the various I/O ports on the rear of the motherboard.

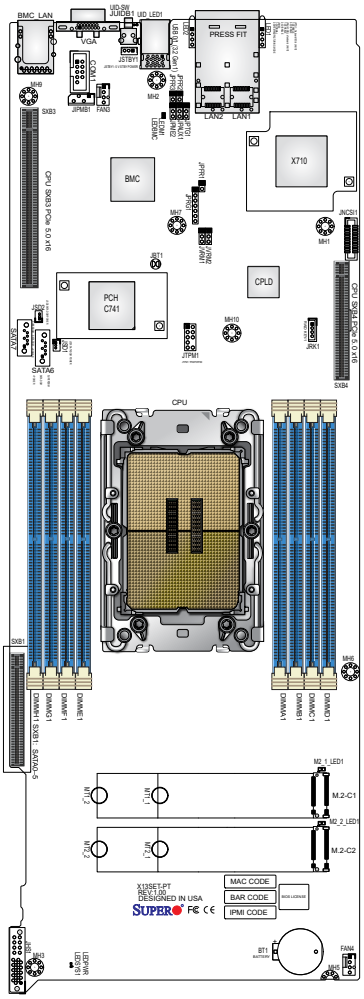
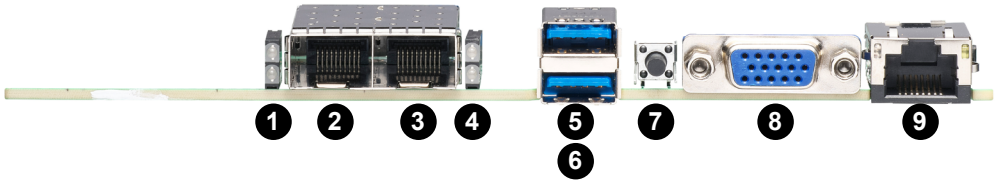


Figure 2-1. I/O Port Locations and Definitions



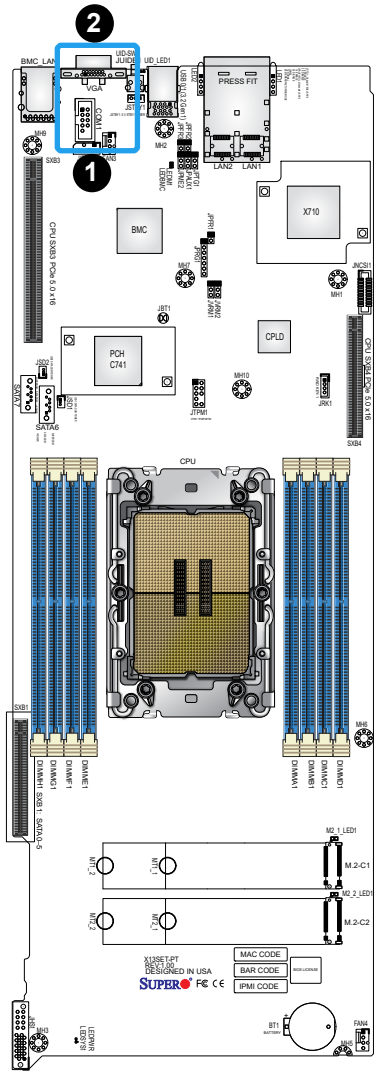
Rear I/O Ports					
#	Description	#	Description	#	Description
1	LED1	5	USB0 (3.2 Gen 1)	9	Dedicated BMC LAN
2	LAN1	6	USB1 (3.2 Gen 1)		
3	LAN2	7	UID Switch / BMC Reset Button		
4	LED2	8	VGA Port		

COM Port Header

One COM (communication) port header (COM1) that supports serial link interface is on this motherboard. COM1 is located next to VGA port. Refer to the layout below for the location of COM1.

VGA Connection

There is one VGA connection in your system. The VGA port is located on the rear I/O panel. The VGA connection provides analog interface support between the computer and the video displays. Refer to the layout below for the location of VGA port.



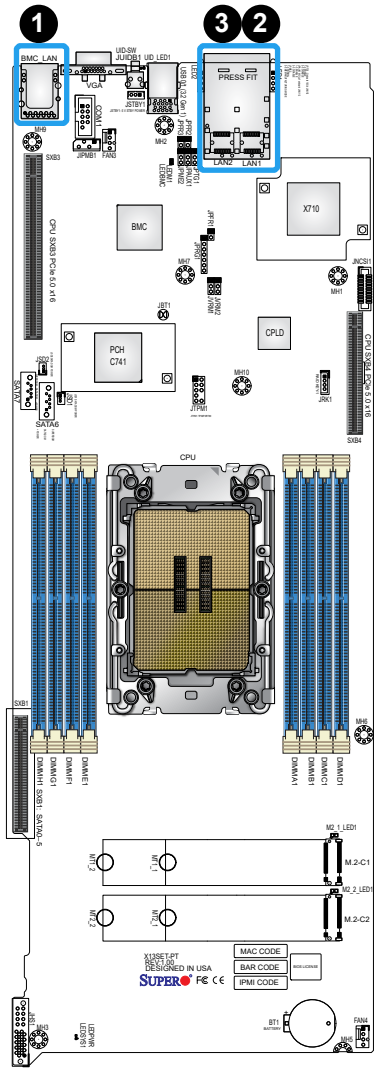
1. COM1
2. VGA

LAN Port (Dedicated BMC LAN)

A dedicated BMC LAN port (BMC_LAN) is located on the rear I/O panel. The dedicated BMC LAN port, located on the rear I/O panel, provides LAN support for the Baseboard Management Controller (BMC). Refer to the LED Indicator section (Section 2.8) for LAN LED information.

SFP+ LAN Ports

Two SFP+ LAN ports (LAN1 and LAN2) are located on the rear I/O panel. The SFP+ LAN ports provide Ethernet 10Gb network connections. Refer to the LED Indicator section (Section 2.8) for LAN LED information.



1. BMC LAN Port
2. LAN1 (SFP+)
3. LAN2 (SFP+)

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

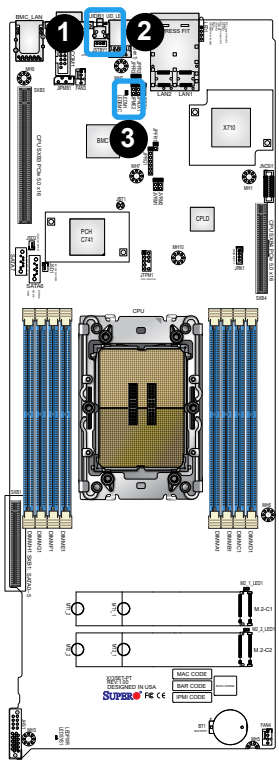
A UID/BMC Reset switch (JUIDB1) is located on the rear side of the motherboard. This switch has dual functions. It can be used to identify a system unit that is in need of service, and it can also be used to reset the BMC settings.

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

When functioning as a UID LED switch, JUIDB1 will turn the rear UID LED (UID-LED) on and off when you press the switch on/off.

To achieve these dual purposes, the UID LED/BMC Reset switch works in conjunction with the BMC Heartbeat LED (LEDM1) and rear UID LED (UID-LED). 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 below. Also, refer to the BMC User's Guide posted on our website at www.supermicro.com for more information on BMC.

UID/BMC Reset Switch (JUIDB1) Features and Settings					
When Used as a UID LED Switch			**When Used as a BMC Reset Switch**		
Work w/Rear UID LED (UID-LED)			**Work with BMC Heartbeat LED (LEDM1)**		
Rear UID LED	UID-LED	Blue: Unit identified	BMC Heartbeat LED	LEDM1	Green Blinking: BMC Normal
Press the switch (JUIDB1) to turn on and off rear UID LED indicator.			BMC Reset: Press & hold the switch (JUIDB1) 6 seconds		LEDM1: Solid green: during reboot
					Triggering a cold reboot; LED: solid green on during cold reboot
			BMC Reset: Press & hold the switch (JUIDB1) 12 seconds		LEDM1: Solid green: during BMC reset
					BMC: Reset to the manufacturer's default; LED solid on during BMC Reset



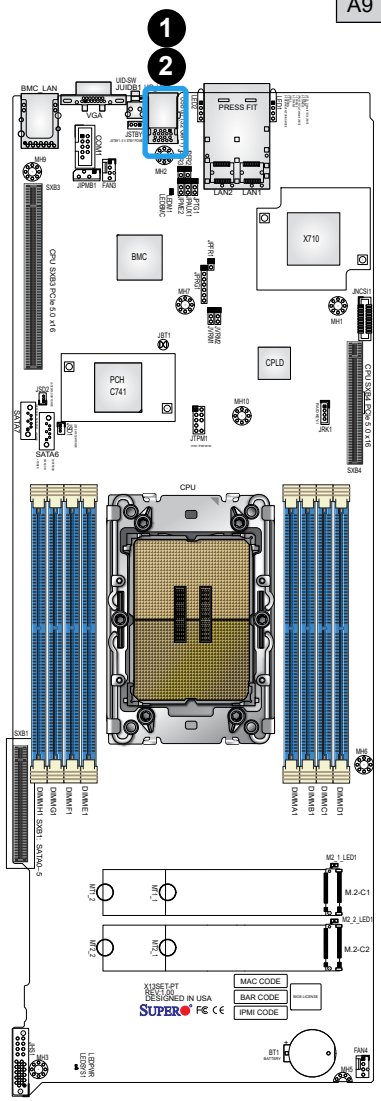
UID/BMC Reset Switch (JUIDB1) Pin Definitions	
Pin#	**Definition**
1	GND
2	GND
3	Button In
4	Button In

1. UID Switch / BMC Reset
2. Rear UID LED (UID-LED)
3. BMC Heartbeat LED (LEDM1)

Universal Serial Bus (USB) Ports

There are two USB ports (USB0/1, USB 3.2 Gen 1) located on the rear I/O panel. The USB ports can be used for USB support via USB cables (not included).

Back Panel USB0/1 (USB 3.2 Gen 1) Pin Definitions			
Pin#	**Definition**	**Pin#**	**Definition**
A1	VBUS	B1	VBUS
A2	USB_N	B2	USB_N
A3	USB_P	B3	USB_P
A4	GND	B4	GND
A5	Stda_SSRX-	B5	Stda_SSRX-
A6	Stda_SSRX+	B6	Stda_SSRX+
A7	GND	B7	GND
A8	Stda_SSTX-	B8	Stda_SSTX-
A9	Stda_SSTX+	B9	Stda_SSTX+



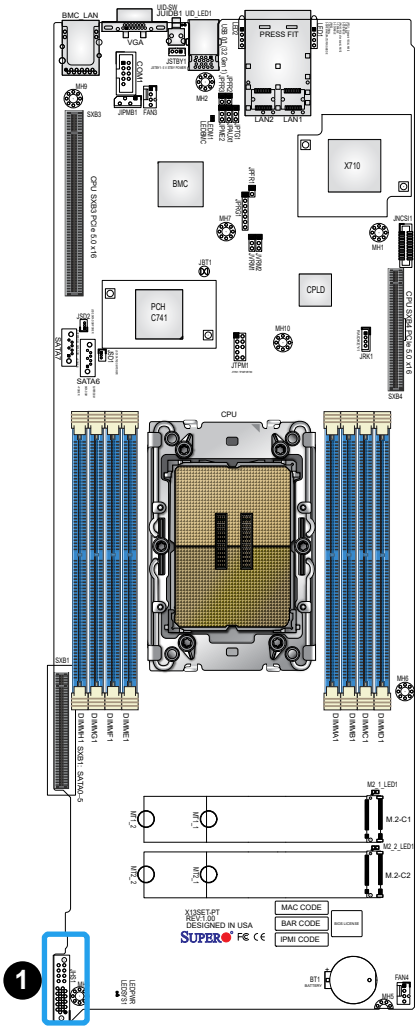
1. Rear I/O Panel USB0 (3.2 Gen 1)
2. Rear I/O Panel USB1 (3.2 Gen 1)

2.6 Connectors

Power and Front Control Panel Connector

SMCI-Proprietary Power Connector

An SMCI proprietary power and front control panel connector is located at JHS1 on the motherboard. This connector is reserved for an SMCI proprietary server use only.



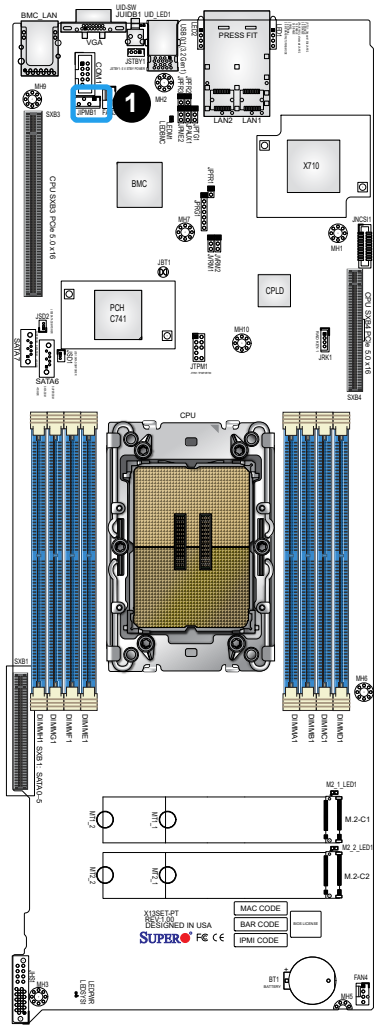
1. SMCI-Proprietary PWR

Headers

4-pin BMC External I²C Header

A System Management Bus header for BMC is located at JIPMB1. Connect the appropriate cable here to use the IPMB I²C connection on your system. Refer to the table below for pin definitions.

External I²C Header Pin Definitions	
Pin#	**Definition**
1	Data
2	GND
3	Clock
4	NC
NC = No Connection	



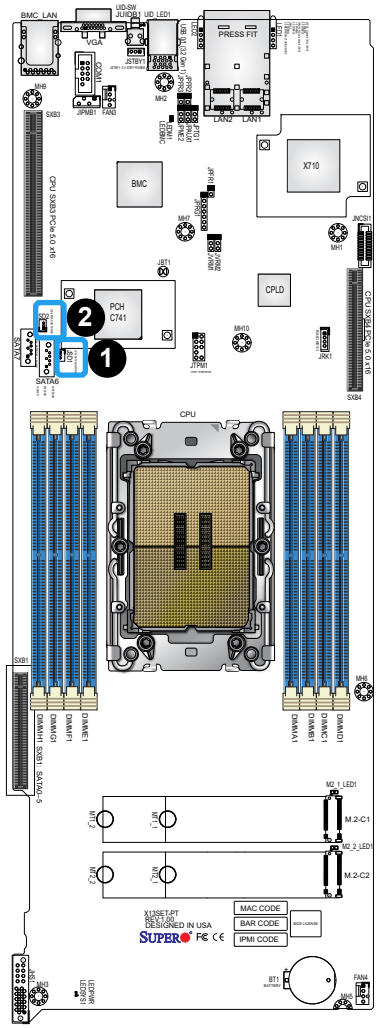
1. BMC External Header

Disk-On-Module Power Connector

The Disk-On-Module (DOM) power connectors at JSD1 and JSD2 provide 5 V power to a solid-state DOM storage devices connected to one of the SATA ports. Refer to the table below for pin definitions.

DOM Power Pin Definitions

Pin#	Definition
1	5 V
2	GND
3	GND

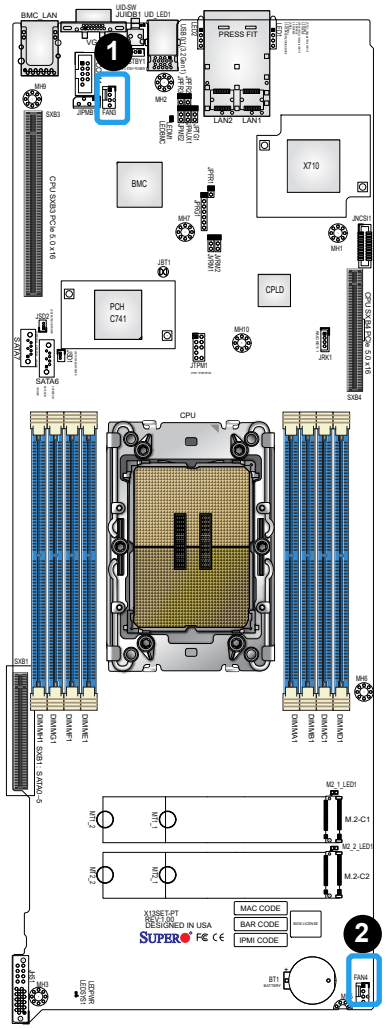


1. Disk-On-Module (DOM) Power Connector (JSD1)
2. Disk-On-Module (DOM) Power Connector (JSD2)

Fan Headers

There are two 4-pin CPU fan headers (FAN3, FAN4) on the motherboard. All the 4-pin fan headers are backwards compatible with the traditional 3-pin fans. Refer to the table below for pin definitions.

Fan Header Pin Definitions	
Pin#	**Definition**
1	GND
2	2.5 A/+12 V
3	Tachometer
4	PWM_Control



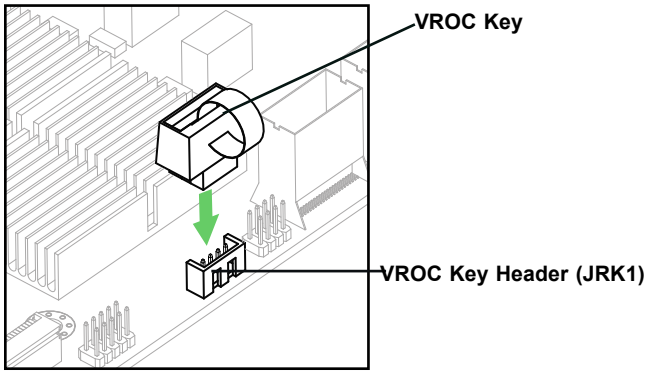
1. FAN3 (CPU Fan Header)
2. FAN4 (CPU Fan Header)

Intel VROC RAID Key Header

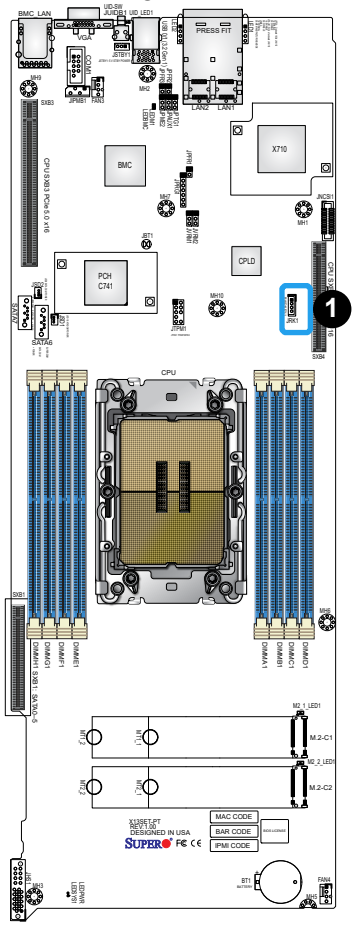
A VROC RAID Key header is located at JRK1 on the motherboard. Install a VROC RAID Key on JRK1 for NVMe RAID support as shown in the illustration below. Refer to the layout below for the location of JRK1.

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: http://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



Note: The graphics contained in this user's manual are for illustrational purposes only. The components installed in your system may or may not look exactly the same as the graphics shown in the manual.



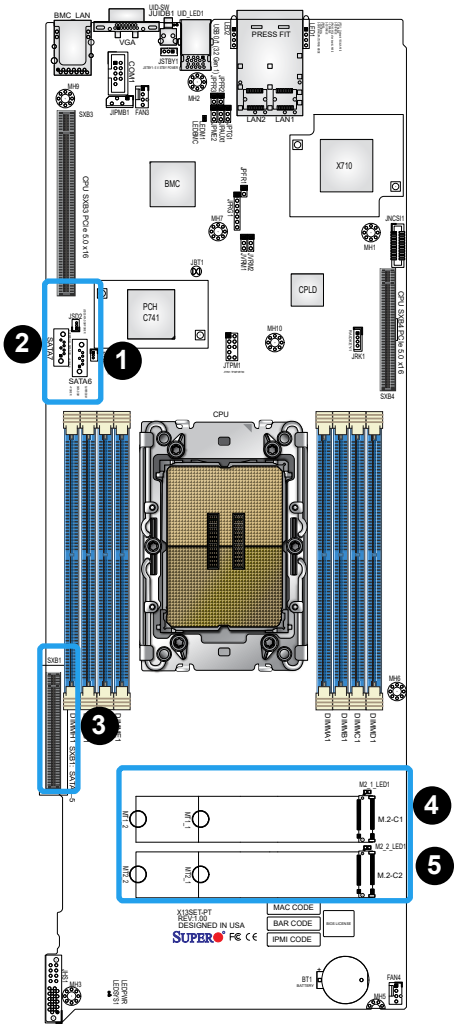
1. VROC RAID Key (JRK1)

SATA 3.0 Ports

There are two SATA 3.0 ports (SATA6, SATA7) and six SATA ports (SATA0-5) on the motherboard. These SATA ports are supported by the C741 chipset. SATA6 and SATA7 can be used with Supermicro SuperDOMs, which are orange SATA DOM connectors with power pins built in and do not require external power cables. SATA0–5 are supported by PCH and are connected to Supermicro storage backplane.

M.2 Slot

M.2 is formerly known as Next Generation Form Factor (NGFF). The M.2 slot is designed for internal mounting devices and provides M Key 22110/2280 support dedicated for SSD devices with the ultimate performance capability in a PCI Express 5.0 interface for native PCIe SSD support.



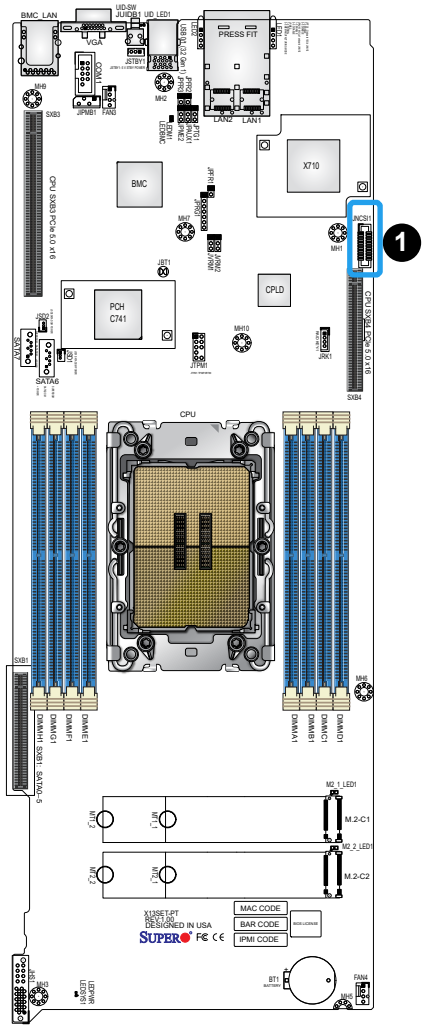
1. SATA6 (SuperDOM)
2. SATA7 (SuperDOM)
3. SATA0–5
4. M.2-C1
5. M.2-C2

NC-SI Connector

The NC-SI connector (JNSCI1) is used to connect a Network Interface Card (NIC) to the motherboard which will allow the onboard Baseboard Controller (BMC) to communicate with a network.

Note 1: 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: http://www.supermicro.com/support/manuals/.

Note 2: LAN1 is the default shared LAN port.



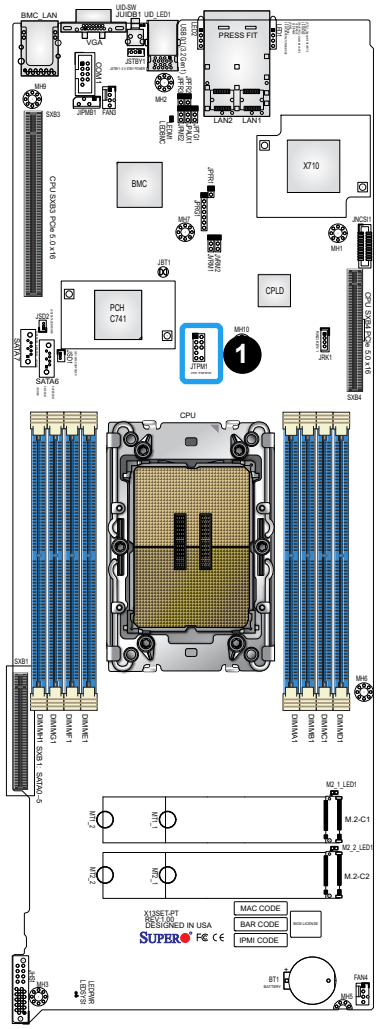
1. NC-SI Connector

TPM/Port 80 Connector

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

Trusted Platform Module Header Pin Definitions

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



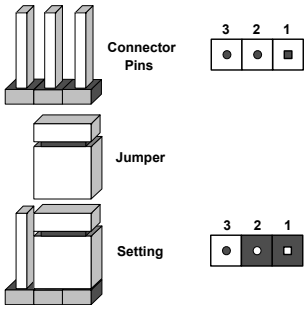
1. TPM/Port 80 Header

2.7 Jumper Settings

How Jumpers Work

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

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



CMOS Clear

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

To Clear CMOS

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

Note: Clearing CMOS will also clear all passwords.

Do not use the PW_ON connector to clear CMOS.



JBT1 contact pads

LAN Port Enable/Disable

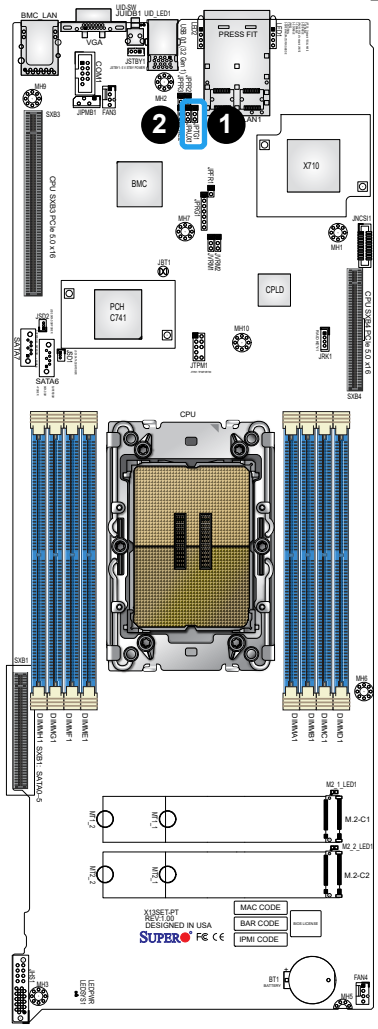
JPTG1 allows you to enable/disable the onboard LAN ports. The default setting is pins 1-2 to enable the connection. Refer to the table below for jumper settings.

LAN Enable/Disable Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Enabled
Pins 2-3	Disabled

LAN Port AUX Power Enable/Disable

JPAUX1 allows you to enable/disable the LAN port AUX power to enable/disable onboard LAN ports when the system is in power off status. The default setting is to short pins 2-3 to disable onboard LAN ports when the system is in power off status. Refer to the table below for jumper settings.

LAN Port AUX Power Enable/Disable Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Enabled
Pins 2-3	Disabled



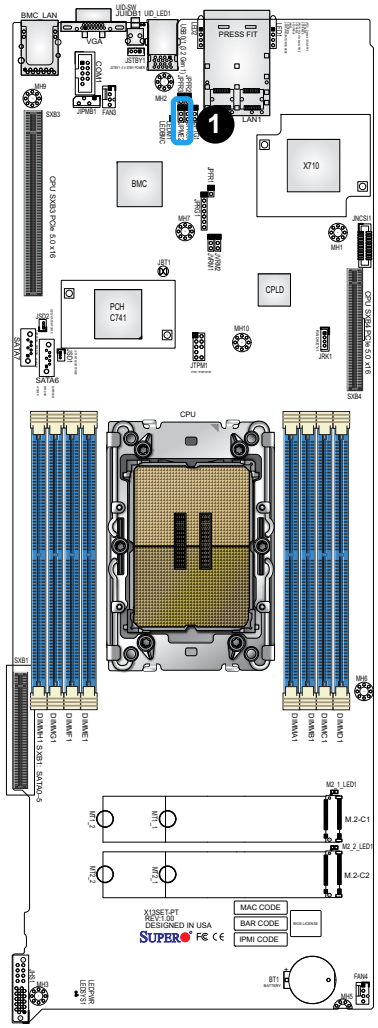
1. LAN Controller Enable/Disable (JPTG1)
2. LAN Port AUX Power Enable/Disable

Note: Consult Supermicro before enabling JPAUX1. There must be sufficient airflow to enable JPAUX1 in standby mode (S5 state).

ME Recovery

JPME2 is used for ME Firmware Recovery mode, which will limit system resource for essential function use only without putting restrictions on power use. In the single operation mode, online upgrade will be available via Recovery mode. Refer to the table below for pin definitions.

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



1. JPME2

2.8 LED Indicators

BMC Heartbeat LED

LEDM1 is the BMC heartbeat LED. When the LED is blinking green, BMC is functioning normally. Refer to the table below for the LED status.

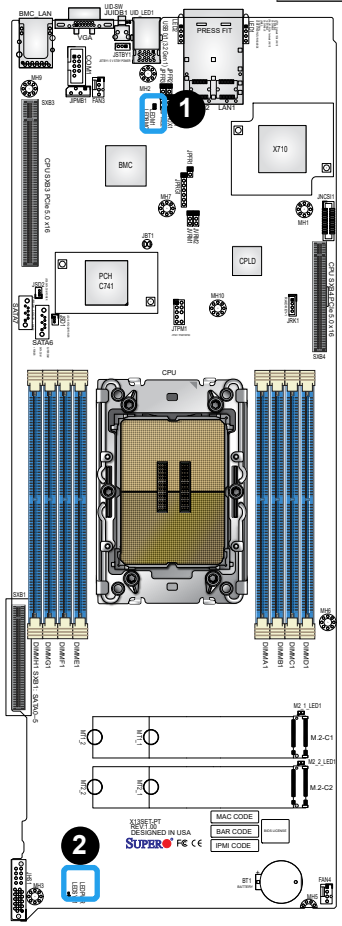
BMC Heartbeat LED Indicator	
LED Color	**Definition**
Blinking Green	BMC Normal

Note: For information on UID LED Indicators and BMC Heartbeat LED Indicator, refer to the section on UID LED/BMC Reset Switch and LED Indicator on page 45.

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 cord before removing or installing components. Refer to the table below for more information.

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

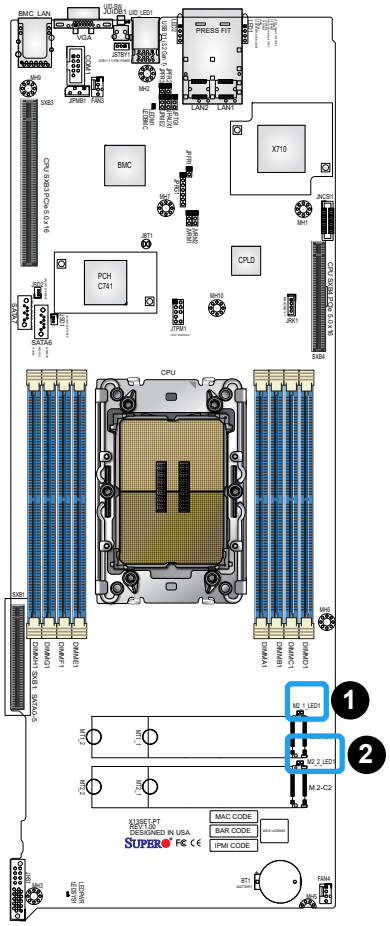


1. BMC LAN LEDs
2. Onboard Power LED

M.2 LED

The M.2 LEDs are located at M2_1_LED1 and M2_2_LED1 on the motherboard. M2_1_LED1 is for M.2-C1 and M2_2_LED1 is for M.2-C2. When they are blinking, the M.2 devices are working. Refer to the table below for more information

M.2 LED State	
LED Color	**Definition**
Green: Blinking	Device is working



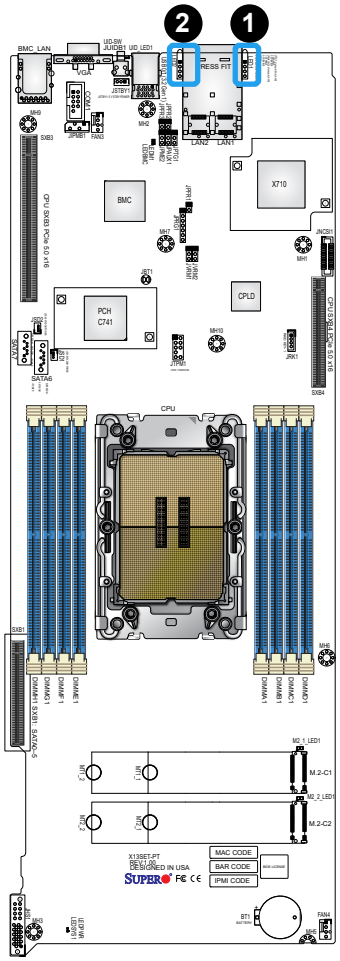
1. M.2 LED
2. M.2 LED

SFP+ LAN Link/Activity LEDs

Two SFP+ LAN Link/Activity LED indicators (LED1 for LAN1, LED2 for LAN2) are located on the rear I/O panel of the motherboard. Each SFP+ LAN port has two LEDs. The green LED indicates activity, while the other Link LED may be green, yellow, or off to indicate the speed of the connection. Refer to the tables below for more information.

SFP+ LAN Port LEDs LED1/LED2 Assignment	
LED	**LAN Port Assignment**
LED1	SFP+ LAN Port (LAN1)
LED2	SFP+ LAN Port (LAN2)

SFP+ LAN Port Activity/Link LEDs (LED1/LED2) LED State		
LED	**LED Color**	**Definition**
Activity (Bottom)	Blinking Green	Activity
Link (Top)	Solid Green	10 Gbps Link Speed
	Solid Yellow	1 Gbps Link Speed



1. LED1 (SFP+ LEDs, for LAN1)
2. LED2 (SFP+ LEDs, for LAN2)

Chapter 3

Troubleshooting

3.1 Troubleshooting Procedures

Use the following procedures to troubleshoot your system. If you have followed all of the procedures below and still need assistance, refer to the 'Technical Support Procedures' and/or 'Returning Merchandise for Service' section(s) in this chapter. 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. Make sure that the power connectors are properly connected.
3. Check that the 115 V/230 V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. 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. Make sure that your peripherals or devices function normally.
2. If you see no any video in power on mode, turn off the system, then remove all add-on cards and cables. Check if the system can be powered on.

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.
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 all memory modules are populated with same type and speed.
3. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.

Losing the System's Setup Configuration

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

When the System Becomes Unstable

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

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

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

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

3. HDD support: Make sure that all hard disk drives (HDDs) work properly. Replace the bad HDDs with good ones.

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

5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. 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 USB flash or media drives.

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

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

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

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

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

3.2 Technical Support Procedures

Before contacting Technical Support, 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: The X13SET-PT motherboard supports 2 TB of 3DS RDIMM ECC DDR5 memory in eight memory slots. The 4th Generation Intel Xeon Scalable Processor memory has speeds of up to 4800 MT/s (4400 MT/s when fully populated), while the 5th Generation Intel Xeon Scalable Processor memory has speeds of up to 5600 MT/s (4400 MT/s when fully populated). 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.

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

To update your BIOS under UEFI Shell

Note: We do not recommend that you update your BIOS if you are not experiencing a BIOS-related problem. If you need to update your BIOS, follow the steps below to properly update your BIOS under UEFI Shell.

1. Download and save the BIOS update package to your computer.

2. Extract the files from the UEFI folder of the BIOS package to a USB flash drive.

Note: The USB flash drive doesn't have to be bootable; however, it has to be formatted with the FAT/FAT32 file system.

3. Insert the USB flash drive into a USB port, boot to the Build-In UEFI Shell, and enter the following commands to start the BIOS update:

```
Shell> fs0:
fs0:\> cd UEFI
fs0:\UEFI> flash.nsh BIOSname#.###
```

4. The FLASH.NSH script will compare the Flash Descriptor Table (FDT) code in the new BIOS with the existing one in the motherboard:

a. If a different FDT is found

- A new file, STARTUP.NSH, will be created, and the system will automatically reboot in 10 seconds without you pressing any key. BIOS will be updated after the system reboots.
- You can also press <Y> to force an immediate system reboot to shorten the process. During system reboot, press the <F11> key to invoke the boot menu and boot into the build-in UEFI Shell. Your BIOS will be updated automatically.

b. If the FDT is the same

- BIOS update will be immediately performed without a system reboot initiated.

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

5. Perform an A/C power cycle after the message indicating the BIOS update has completed.
6. Go to the BIOS setup utility, and restore the BIOS settings.

3.4 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

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

Proper Battery Disposal

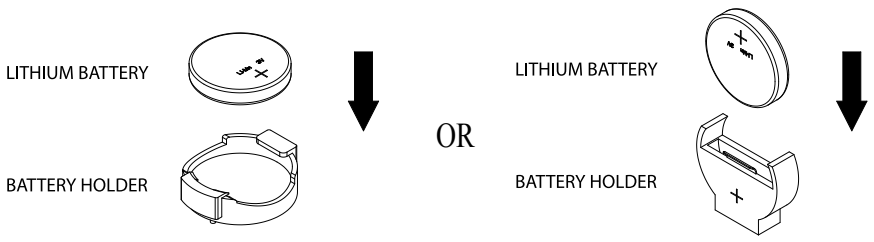
Warning: Handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Comply with the regulations set up by your local hazardous waste management agency to dispose of your used battery properly.

Battery Installation

To install an onboard battery, follow the steps below:

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

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



3.5 Returning Merchandise for Service

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

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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

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

Starting the Setup Utility

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

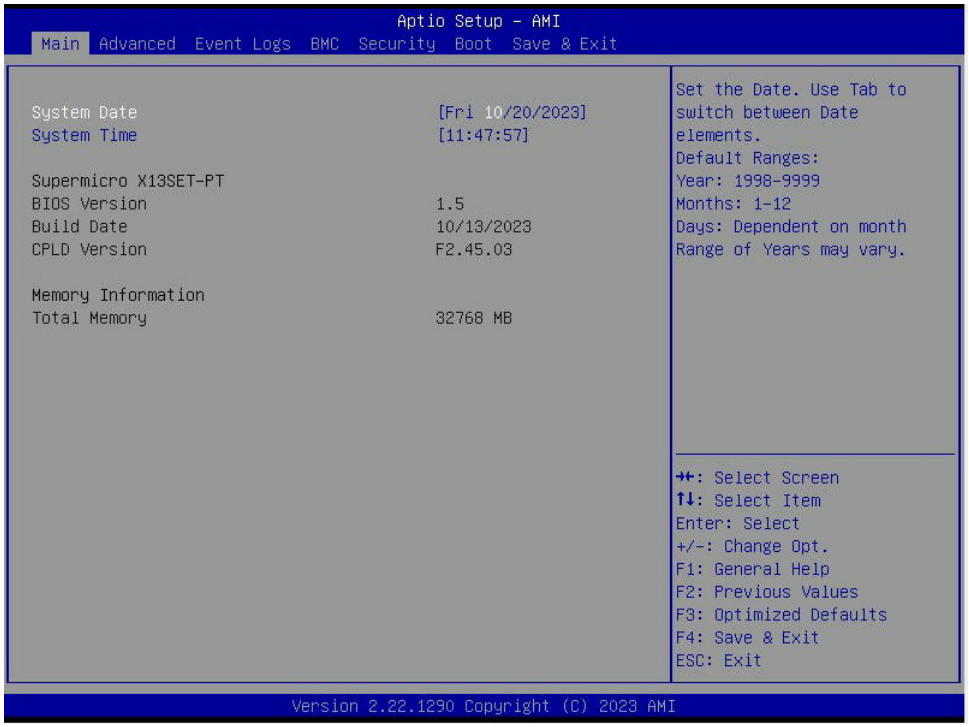
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

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

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

4.2 Main Setup

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



System Date / System Time

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

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

Supermicro X13SET-PT

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 Logic Device (CPLD) used in the system.

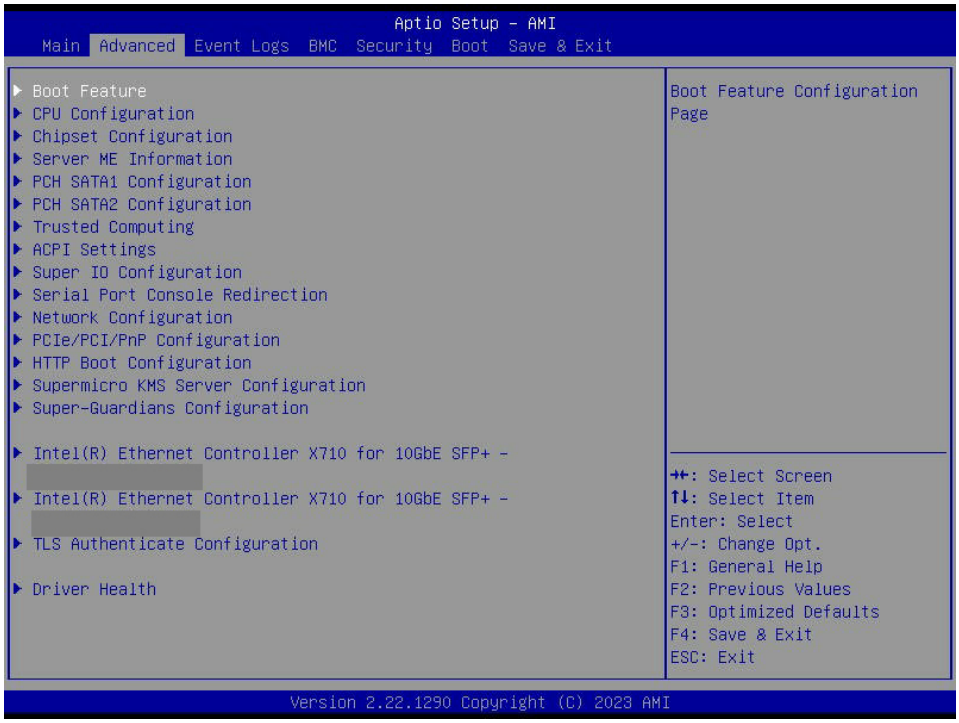
Memory Information

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.



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

▶Boot Feature

Quiet Boot

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

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

Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to display 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 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.

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

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

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

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

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

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

Restore on AC Power Loss

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

Power Button Function

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

▶CPU Configuration

The following processor configuration information is displayed:

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

▶Advanced Power Management Configuration

Power Technology

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

Power Performance Tuning

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

Optimized Power Mode

Use this feature to enable or disable Optimized Power Mode. The options are **Disable** and Enable.

▶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 specify the base P1 ratio for Streaming SIMD Extensions (SSE) and AVX workloads and to pre-grant a license level. The options are **Nominal**, Level 1, and Level 2.

SpeedStep (P-States)

Enhanced Intel SpeedStep Technology (EIST) allows the system to automatically adjust processor voltage and core frequency in an effort to reduce power consumption and heat dissipation. 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 feature allows for more demand-based P-state switching based on real-time energy needs of applications and optimize the power-to-performance balance for energy efficiency. The options are **HW_ALL** and SW_ALL.

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

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

▶Hardware PM State Control

Hardware P-States

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

▶CPU C State Control

Enable Monitor MWAIT

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

CPU C1 Auto Demotion

Select Enable to allow the CPU to demote C3, C6, or C7 requests to C1 based on un-core auto-demote information. The options are Disable, Enable, and **Auto**.

CPU C6 Report

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

Enhanced Halt State (C1E)

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

▶Package C State Control

Package C State

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

▶CPU1 Core Disable Bitmap

Available Bitmap:

This feature displays the available bitmap.

Disable Bitmap(Hex)

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 prefectch data from the main system memory to Level 2 cache to help expedite data transaction to enhance memory performance. The options are **Enable** and Disable.

Adjacent Cache Prefetch

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

DCU Streamer Prefetcher

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

DCU IP Prefetcher

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

LLC Prefetch

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

Extended APIC

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

Note: When enabled, VT-d and Interrupt Remapping will be automatically enabled.

Intel Virtualization Technology

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

Note: The changes take effect after you press Save Changes and Exit, Save Changes and Reset, or Save Changes in the Save and Exit submenu.

Enable SMX

Select Enable to support Safer Mode Extensions (SMX). This feature 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 options are Lock/Disable and **Unlock/Enable**.

AES-NI

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

Limit CPU PA to 46 Bits

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

TME, TME-MT, TDX

Memory Encryption (TME)

Select Enabled for total memory encryption 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 Total Memory Encryption (TME) function for physical memory protection. The options are **Auto**, Disabled, and Enabled.

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

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

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

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

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

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

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

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

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

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

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

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

Software Guard Extension (SGX)

The following SGX features are available when "Memory Encryption (TME)" is set to Enabled and 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 change 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 BIOS provides software with the key blobs, which are generated for each CPU package. The options are **Disabled** and Enabled.

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

Use this feature to set the Processor Reserved Memory Range Register (PRMRR) size. The options are **256 M**, 512 M, 1 G, 2 G, 4 G, 8 G, 16 G and 32 G.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

▶Chipset Configuration

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

▶North Bridge

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

▶Uncore Configuration

The following Uncore General Configuration information is displayed.

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

Degrade Precedence

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

Link L0p Enable

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

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

Link L1 Enable

Select Enable for the BIOS to activate Link L1 support. This feature 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

Select Enable for the KTI prefetcher to preload the L1 cache with data deemed relevant. This allows the memory read to start earlier on a DDR bus in an effort to reduce latency. Select Auto for the KTI prefetcher to automatically preload the L1 cache with relevant data whenever is needed. The options are Disable, Enable, and **Auto**.

IO Directory Cache (IODC)

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

SNC

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

Stale AtoS (A to S)

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

LLC Dead Line Alloc

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

▶Memory Configuration

This feature allows 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.

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

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

Legacy ADR Mode

Use this feature to support the Legacy ADR mode to enhance memory performance. The options are Disable, Enable, and **Auto**.

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

Use this feature to enable or disable legacy support for CXL Type 3 devices. The options are Enable and **Disable**.

Volatile Memory Mode

Select 1LM or 2LM mode for volatile memory. The options are **1LM** and 2LM (available when using HBM CPU and the "NUMA" feature is set to Enabled).

▶Memory Topology

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

▶Page Policy

Page Policy

Use this feature to select DRAM page policy. The options are **Close** and Adaptive.

▶Memory RAS Configuration Setup

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

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

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

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

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

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

Use this feature to set the percentage of memory space to be used for UEFI ARM mirroring for memory security enhancement. Enter the percentage to be mirrored in basis points, such as 1275 (12.75%). The default setting is **0**.

Correctable Error Threshold

Use this feature to specify the threshold value for correctable memory-error logging. This 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**.

The following information is displayed:

- Leaky Bucket Low Bit
- Leaky Bucket High Bit

ADDDC Sparing

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

Patrol Scrub

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

DDR PPR Type

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

Enhanced PPR

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

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

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

▶IIO Configuration

▶CPU1 Configuration

IOU0/1/2/3/4 (IIO PCIe Port 1/2/3/4/5)

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

For detailed slot bifurcation mapping, refer to the system block diagram in Chapter 1.

▶M.2-C1 / ▶M.2-C2 / ▶RSC-PR-6G5 SLOT1 / ▶RSC-P-6G5 SLOT1

Note: The name of the riser cards depend on the riser card installed on the system. These riser cards only show when the system detects them.

Link Speed

Use this feature to select the link speed for the PCIe port. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), Gen 3 (8 GT/s), Gen 4 (16 GT/s), and Gen 5 (32 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 or disable the data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register. The options are Disable and **Enable**.

PCIe Port Max Payload Size

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

Equalization Bypass to Highest Rate

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

▶IOAT Configuration

Relaxed Ordering

Select Yes to enable Relaxed Ordering support. This feature allows certain transactions to violate the strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been enqueued. The options are **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

Use this feature to enable or disable Opt-Out Illegal 0xFEE Platform Mitigation Select Enable to Opt-Out. Illegal Message Signaled Interrupt (MSI) mitigation prevents non-maskable interrupts generated by improper MSI from causing software panic. The options are **Disable** and Enable.

Pre-boot DMA Protection

Enable this feature to help block DMA attacks. The options are Enable and **Disable**.

Interrupt Remapping

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

PCIe ACSCTL

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

▶Intel® VMD Technology

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

Note: 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.

NVMe Mode Switch

If this feature is set to Auto, VMD mode will be automatically enabled for all NVMe slots when a VROC key is plugged in. The options are Manual, VMD, and **Auto**.

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

VMD Config for IOU 0 / VMD Config for IOU 2 / VMD Config for IOU 4

Enable/Disable VMD

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

Hot Plug Capable

Select Enable to enable Hot Plug support for the root ports specified. This feature 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 / Gen3 Link Degradation / Gen4 Link Degradation / Gen 5 Degradation

Use this feature to enable or disable link degradation. The options are **Enable** and Disable.

IIO-PCIe Express Global Options

PCIe ASPM Support (Global)

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

PCIe Max Read Request Size

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

Equalization Bypass to Highest Rate

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

IIO eDPC Support

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

IIO eDPC Interrupt (Available if "IIO eDPC Support" is set to On Fatal Error or On Fatal and Non-Fatal Errors)

Use this feature to enable or disable IIO enhanced DPC (eDPC) interrupt. The options are Disable and **Enable**.

IIO eDPC ERR_COR Message (Available if "IIO eDPC Support" is set to On Fatal Error or On Fatal and Non-Fatal Errors)

Use this feature to enable or disable IIO enhanced DPC (eDPC) error correction message. The options are Disable and **Enable**.

CXL Security Level

Use this feature to select the level of security for the CXL devices. The options are Fully Trusted, Partially Trusted, Untrusted, and **Auto**.

CXL Header Bypass

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

▶South Bridge

The following USB information is displayed:

- USB Devices

Legacy USB Support

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

XHCI Hand-off

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

Port 60/64 Emulation

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

PCIe PLL SSC

Select Enabled for PCH PCIe Spread Spectrum Clocking support. This feature 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 General ME Configuration is displayed:

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

▶PCH SATA1 Configuration

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

SATA Controller(s)

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

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

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

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

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

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

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

SATA SGPIO Mode

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

Note: The signals are not related to SATALED.

SATA Port 0–SATA Port 5

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

Hot Plug

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

Spin Up Device

Select Enable for Staggered Spin Up support. This feature allows the SATA devices you specified 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 you specified should be connected to a Solid State drive or a Hard Disk Drive. The options are **Hard Disk Drive** and Solid State Drive.

▶PCH SATA2 Configuration

When the 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

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

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

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

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

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

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

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

SATA SGPIO Mode

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

Note: The signals are not related to SATALED.

SATA Port 0 / SATA Port 1

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

Hot Plug

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

Spin Up Device

Select Enable for Staggered Spin Up support. This feature allows the SATA devices you specified 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 you specified 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

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

- TPM 2.0 Device Found
- Firmware Version
- Vendor

Security Device Support

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

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

- Active PCR banks
- Available PCR banks

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

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



Note: Exposed when TPM module supports. (Ex: Nuvoton TPM module)

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 Disabled and **Enabled**.

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

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

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

Platform Hierarchy (Available when "Security Device Support" is set to Enable) (for TPM Version 2.0 and above)

Select Enabled for TPM Platform Hierarchy support. This feature 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. This feature contains separate controls to address your privacy concerns because the primary keys in the hierarchy are certified by the TPM key or by a manufacturer with restrictions on how an authentic TPM device that is attached to an authentic platform can be accessed and used. A primary key can be encrypted and certified with a certificate created by using TPM2_ ActivateCredential, which allows you to independently enable "flag, policy, and authorization values" without involving other hierarchies. You 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. This feature is used only during the platform developmental stage. This feature cannot be enabled in the production platforms. The options are **Disabled** and Enabled.

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.

Supermicro BIOS-Based TPM Provision Support

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

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

TXT Support

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

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

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

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

WHEA Support

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

High Precision Event Timer

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

▶Super IO Configuration

The following Super IO information is displayed:

- Super IO Chip AST2600

▶Serial Port 1 Configuration

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

Serial Port 1

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

Device Settings

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

Change Settings

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

▶Serial Port 2 Configuration

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

Serial Port 2

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

Device Settings

This feature displays the status of a serial port.

Change Settings

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

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

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

▶Serial Port Console Redirection

COM1

Console Redirection

Select Enabled to enable COM port 1 for Console Redirection. This feature 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**.

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

SOL/COM2

Console Redirection

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

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

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

Terminal Type

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

Legacy Console Redirection

▶Legacy Console Redirection Settings

Legacy Serial Redirection Port

Use this feature to select a COM port to display redirection of Legacy OS and Legacy OPROM messages. The options are **COM1** and SOL.

Resolution

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

Redirection After POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When 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)

Console Redirection EMS

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

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

This feature allows you to specify how the host computer exchanges data with the client computer. The client computer is the remote computer you use.

Out-of-Band Mgmt Port

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

Terminal Type EMS

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII character set. Select 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, and **115200** (bits per second).

Flow Control EMS

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

The following information is displayed:

Data Bits EMS / Parity EMS / Stop Bits EMS

▶Network Configuration

Network Stack

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

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

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

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

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

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

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

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

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

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

Use this feature to set the wait time (in seconds) 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:xxxxxxxxxxxx-IPv6 Network Configuration
▶MAC:xxxxxxxxxxxx-IPv6 Network Configuration

▶Enter Configuration Menu

The following information is displayed:

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

Interface ID

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

DAD Transmit Count

If this set feature is set to 0, the Duplication Address Detection is not performed. Set the value to a preferred selection. The default value is **1**.

Policy

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

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

New IPv6 address

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

New Gateway address

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

New DNS address

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

Commit Changes and Exit

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

Discard Changes and Exit

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

Save Changes and Exit

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

▶MAC:xxxxxxxxxxxx-IPv4 Network Configuration
▶MAC:xxxxxxxxxxxx-IPv4 Network Configuration

Configured

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

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

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

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

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

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

Use this feature to set the network 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

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

▶PCIe/PCI/PnP Configuration

The following information is displayed:

- PCI Bus Driver Version

PCI Devices Common Settings:

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

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

MMCFG Base

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

MMCFG Size

Use this feature to set the MMCFG size. The options are 64 M, 128 M, 256 M, 512 M, 1 G, 2 G, and **Auto**.

MMIO High Base

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

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 1 G, 4 G, 16 G, 64 G, **256 G**, and 1024 G.

SR-IOV Support

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

ARI Support

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

Bus Master Enable

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

Consistent Device Name Support

Use this feature to enable or disable ACPI_DSM 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 booting. 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. The options are **Vendor Defined Firmware** and AMI Native Support.

VGA Priority

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

For the following features, note that:

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

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

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

Onboard Video Option ROM

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

M.2-C1 OPROM / M.2-C2 OPROM / RSC-PR-6G5 SLOT1 OPROM / RSC-P-6G5 SLOT1 OPROM

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

Onboard LAN1 Option ROM

Use this feature to select which firmware function to be loaded for LAN Port 1 used for system boot. The options are Disabled, Legacy, 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

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

Priority of HTTP Boot

Instance of Priority 1:

This feature sets the rank target port. The default value 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 that cannot be longer than 75 characters. Enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI

Enter a Boot Uniform Research Identifier (URI) with 128 characters or shorter. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created. This feature is only supported on Dual or EFI Boot Mode.

▶Supermicro KMS Server Configuration

Supermicro KMS Server IP address

Use this feature to enter the Supermicro Key Management Service (KMS) server IPv4 address in dotted-decimal notation (e.g., 255.255.255.255).

Second Supermicro KMS Server IP address

Use this feature to enter the second Supermicro KMS server IPv4 address in dotted-decimal notation (e.g., 255.255.255.255).

Supermicro KMS TCP Port number

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

KMS Time Out

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

TimeZone

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

Client UserName

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

Client Password

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

KMS TLS Certificate / Size

▶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.

▶Super-Guardians Configuration

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

Super-Guardians Protection Policy

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

KMS Security Policy

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

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

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

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

KMS Server Retry Count

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

TPM Security Policy

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

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

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

Load Authentication-Key

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

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

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

Save Authentication-Key

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

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

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

USB Security Policy

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

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

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

▶Intel(R) Ethernet Controller X710 - XX:XX:XX:XX:XX:XX
▶Intel(R) Ethernet Controller X710 - XX:XX:XX:XX:XX:XX

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

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

▶Firmware Image Properties

The following information is displayed:

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

▶NIC Configuration

Link Speed

Wake On LAN

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

LLDP Agent

Select Enabled to enable the Link Layer Discovery Protocol (LLDP) agent which will provide the basic device information of a device to other devices on the same Local Area Network periodically (about 30 seconds). The options are **Enabled** and Disabled.

Blink LEDs

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

The following information is displayed:

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

▶TLS Authenticate Configuration

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

▶Server CA Configuration

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

▶Enroll Certification

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

▶Enroll Certification Using File

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

Certification GUID

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

Commit Changes and Exit

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

Discard Changes and Exit

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

▶Delete Certification

Use this feature to discard all changes and exit TLS settings. The options are **Disabled** and Enabled.

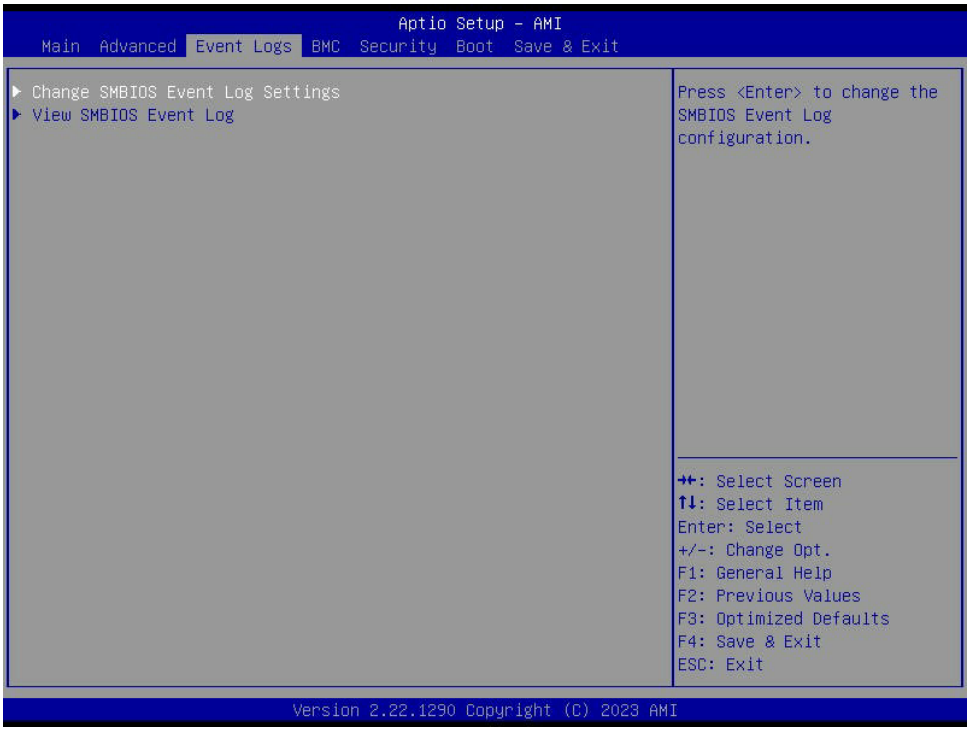
▶Client Certification Configuration

▶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.

4.4 Event Logs

Use this menu to configure Event Log settings.



Note: The changes take effect after you press Save Changes and Exit, Save Changes and Reset, or Save Changes in the Save and Exit submenu.

▶Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

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

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

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

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

SMBIOS Event Log Standard Settings

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

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

MECI (Multiple Event Count Increment) (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**.

METW (Multiple Event Count Time Window) (Available when "SMBIOS Event Log" is set to Enabled)

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



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

▶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 will be displayed:

DATE / TIME / ERROR CODE / SEVERITY.

4.5 BMC

Use this menu to configure BMC settings.



BMC Firmware Revision

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

BMC STATUS (Baseboard Management Controller)

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

▶BMC Network Configuration

BMC Network Configuration

Update BMC LAN Configuration

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

****

Configure IPv4 Support

****

BMC LAN Selection

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

BMC Network Link Status

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

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

Use this feature to select the source of the IPv4 connection. If Static is selected, you will need to know the IP address of IPv4 connection and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a Dynamic Host Configuration Protocol (DHCP) server in the network that is attached to and request the next available IP address for this computer. The options are **DHCP** and Static.

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

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

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

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

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

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

Gateway IP Address

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 1–4094.

****

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 IPv6 connection and enter it to the system manually in the field. If the Dynamic Host Configuration Protocol (DHCP) related option is selected, the BIOS will search for a DHCP server in the network that is attached to and request the next available IP address for this computer. The options are Static Configuration, **DHCPv6 Stateless**, and DHCPv6 Stateful.

IPv6 Address (DHCPv6 Static) (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

This feature allows you to automatically obtain the DNS server IP or manually obtain the DNS server IP. The options are **Auto obtain DNS server IP** and Manually obtain DNS server IP.

Preferred DNS server IP

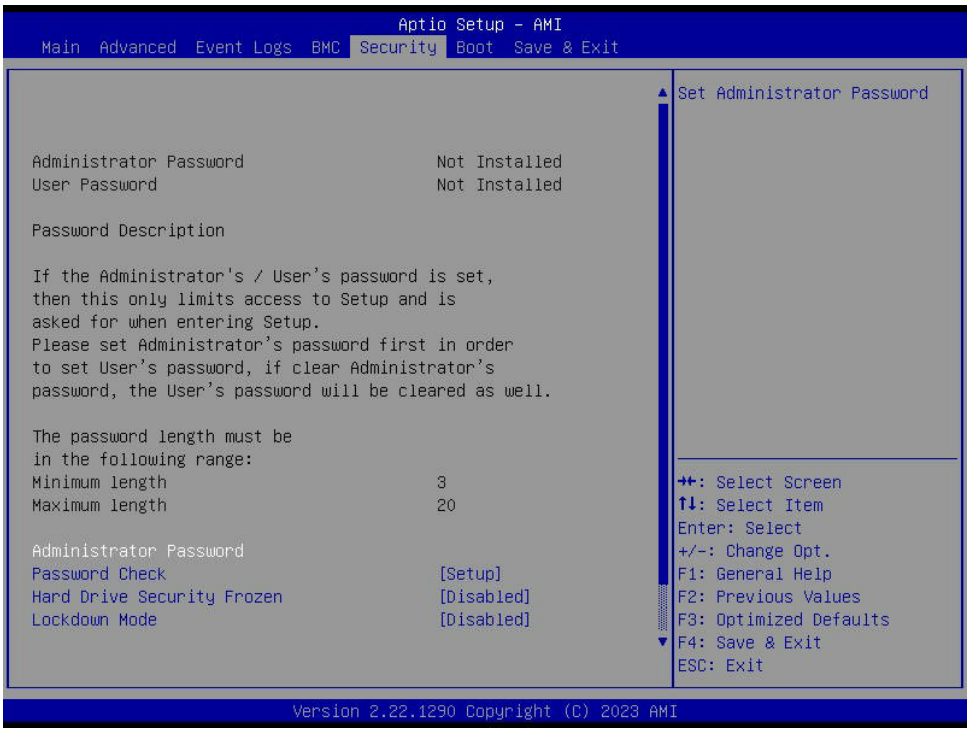
Use this feature to enter the preferred DNS server IP address in dotted-decimal notation (e.g., 255.255.255.255).

Alternative DNS server IP

Use this feature to enter the alternative DNS server IP address in dotted-decimal notation (e.g., 255.255.255.255).

4.6 Security

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



The following information is displayed:

- Administrator Password
- User Password
- Password Description

Administrator Password

This feature indicates if an administrator password has been set. 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 characters to 20 characters long.

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

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

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: http://www.supermicro.com/support/manuals/.

Password Check

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

Hard Drive Security Frozen

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

Lockdown Mode (Available when the DCMS key is activated)

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

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

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

- HDD Name: This feature displays the name of the HDD/SATA drive that is detected by the BIOS.
- HDD Serial Number: This feature displays the serial number of the HDD/SATA device that is detected by the BIOS.
- Security Mode: This feature displays the security mode of the HDD/SATA device that is detected by the BIOS.
- Estimated Time: This feature displays the estimate time needed to perform the selected Security Erase features.
- HDD User Pwd Status: This feature indicates if a password has been set as a SATA user password which allows you to configure Supermicro Security Erase settings on the HDD (SATA) device by using this SATA user password.
- Admin Pwd Status: This feature indicates if a password has been set as a SATA administrator password which allows you to configure Supermicro Security Erase settings on the HDD (SATA) device by using this SATA administrator password.

Security Function

Select Set Password to set an HDD/SATA password which allows you to configure the security settings of the HDD/SATA device. Select Security Erase - Password to enter a SATA user password to allow you to erase the password and the contents previously stored in the HDD/SATA device. Select Security Erase - Password to use the manufacturer default password "111111111" as the SATA user password and allow you to erase the contents of the HDD/SATA device by using this default password. The options are **Disabled**, Set Password, Security Erase - Password, Security Erase - PSID, and Security Erase - Without Password.

Note: The option, Security Erase - PSID, is based on the storage device support.

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.

Lockdown Mode (Available when the DCMS key is activated)

Select Enabled to support Lockdown Mode that will prevent 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.

▶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: http://www.supermicro.com/support/manuals/.

This section displays the contents of the following secure boot features:

- System Mode
- Secure Boot

Secure Boot

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

Secure Boot Mode

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

CSM Support

If this feature is set to Enabled, legacy devices will be supported by the system. The options are Disabled and **Enabled**.

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

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

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

The following information is displayed.

- Vendor Keys

Provision Factory Defaults

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

▶Restore Factory Keys

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

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

▶Enroll Efi Image

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

▶Export Secure Boot Variables (Available when any secure keys have been installed)

Secure Boot variable / Size / Keys / Key Source

▶Platform Key (PK)

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

▶Key Exchange Key (KEK)

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

▶Authorized Signatures (db)

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

▶Forbidden Signatures (dbx)

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

▶Authorized TimeStamps (dbt)

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 (dbr)

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.

▶(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:
  - User Pwd Status:
  - Admin Pwd Status:

Set Admin Password

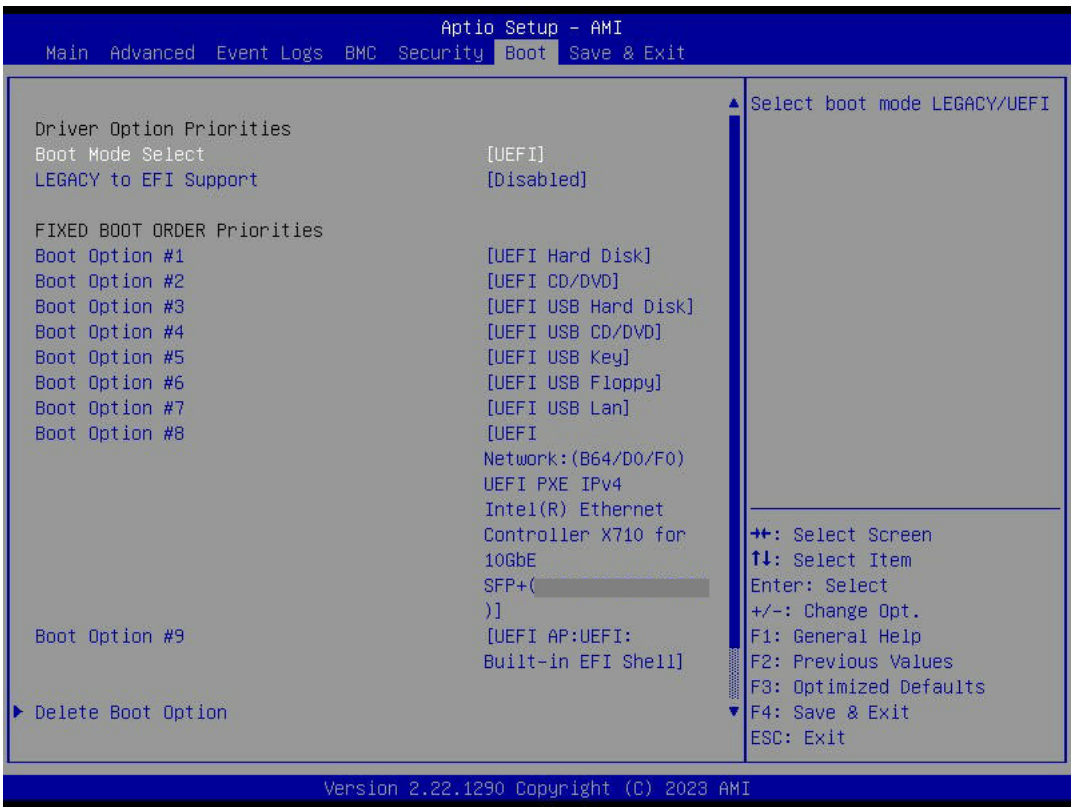
Use this feature to set the administrator password for this storage device.

Device Reset

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

4.7 Boot

Use this menu to configure Boot settings.



Driver Option Priorities

Boot Mode Select

Use this feature to select the type of devices from which the system will boot. The options are Legacy, **UEFI**, and Dual.

Note: When "Boot Mode Select" is set to Dual, all OPROM-related features will be set to Legacy.

LEGACY to EFI Support

Select Enabled to boot EFI OS support after Legacy boot order has failed. The options are **Disabled** and Enabled.

FIXED BOOT ORDER Priorities

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

When "Boot Mode Select" is set to 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

When "Boot Mode Select" is set to **Dual** (default), the following features will be displayed for configuration:

- Boot Option #1–Boot Option #17

▶Delete Boot Option

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

Delete Boot Option

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

▶UEFI NETWORK Drive BBS Priorities

This feature allows you to set the system boot order of detected devices.

▶UEFI Application Boot Priorities

This feature allows you to set the system boot order of detected devices.

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

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

Add boot option

This feature allows you to specify the name for the new boot option.

Path for boot option

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

Boot option File Path

This feature allows you to specify the file path for the new boot option.

Create

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

▶UEFI Hard Disk Drive BBS Priorities

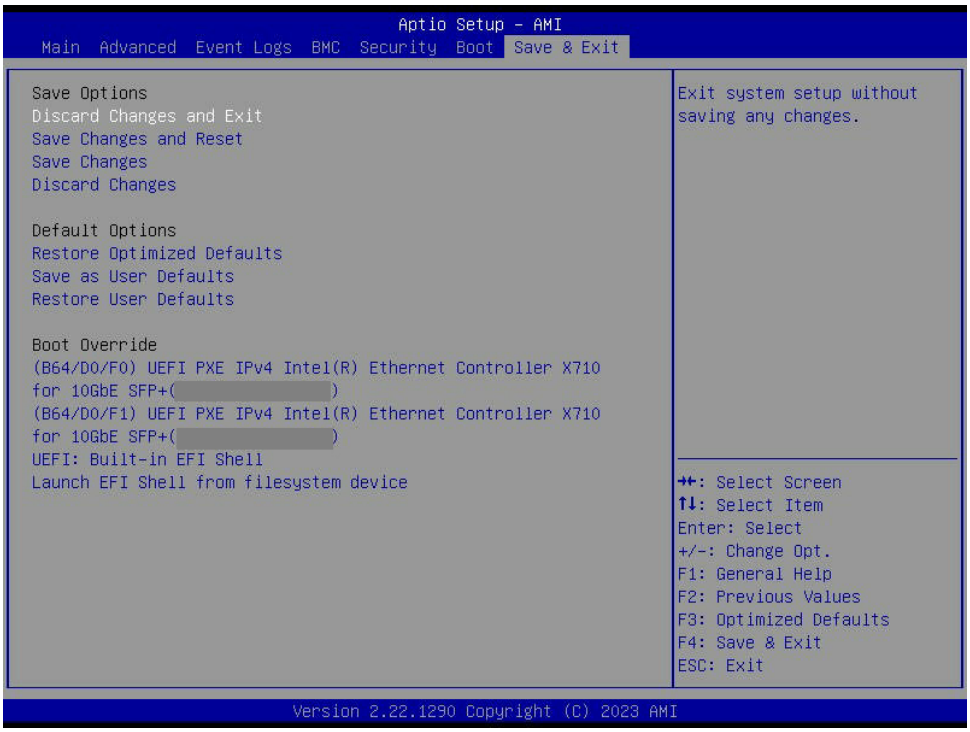
This feature allow you to set the system boot order of detected devices.

▶UEFI USB Key Drive BBS Priorities

This feature allow you to set the system boot order of detected devices.

4.8 Save & Exit

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



Save Options

Discard Changes and Exit

Use this feature to exit from the BIOS Setup utility without making any permanent changes to the system configuration and reboot the computer.

Save Changes and Reset

When you have completed the system configuration changes, use this feature to leave the BIOS Setup utility and reboot the computer for the new system configuration parameters to become effective.

Save Changes

When you have completed the system configuration changes, use this feature to save all changes you've made. This will not reset (reboot) the system.

Discard Changes

Select this feature and press <Enter> to discard all the changes you've made and return to the BIOS Setup utility.

Default Options

Restore Optimized Defaults

Select this feature and press <Enter> to load manufacturer optimized default settings. The default settings 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>. Use this feature 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 an one-time override.

(B106/D0/F0) UEFI PXE IPv4 Intel(R) Ethernet Controller X710 for 10GBASE-T (MAC:xxxxxxxxxxxx)

(B106/D0/F1) UEFI PXE IPv4 Intel(R) Ethernet Controller X710 for 10GBASE-T (MAC: xxxxxxxxxxxx)

UEFI: Built-in EFI Shell

Launch EFI Shell from filesystem device

Appendix A

BIOS POST Codes

A.1 BIOS POST Codes

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

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

Appendix B

Software

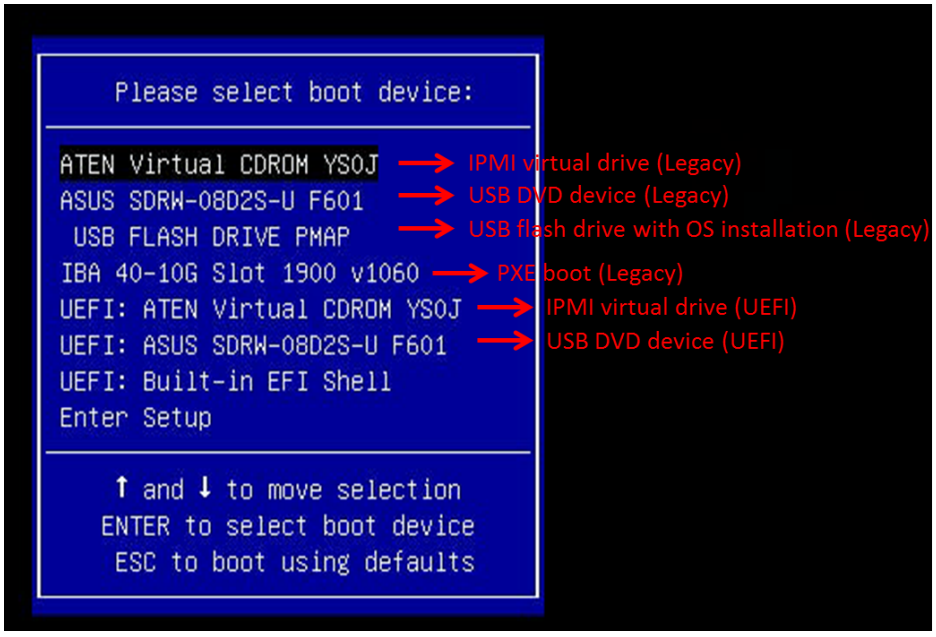
After the hardware has been installed, you can install the Operating System (OS), configure RAID settings, and install the drivers.

B.1 Microsoft Windows OS Installation

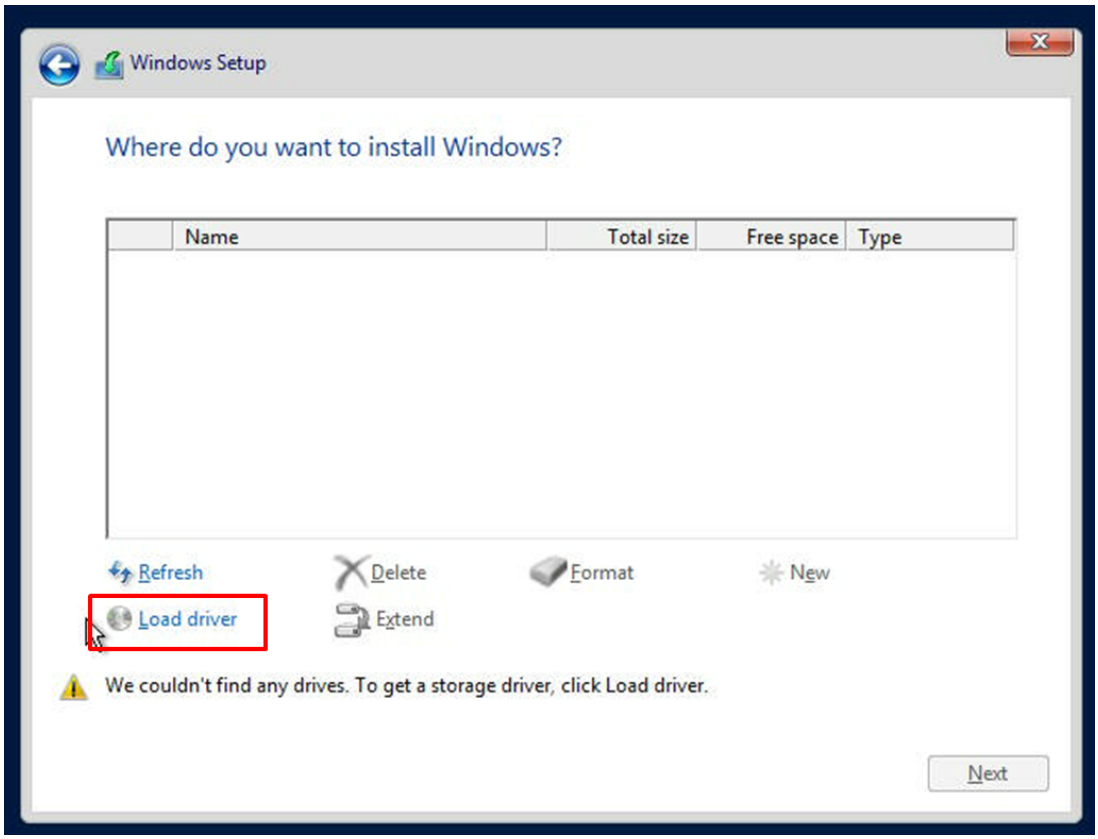
If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at www.supermicro.com/support/manuals.

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That can be a USB flash or media drive, or the BMC KVM console.
2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.
3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing <F11> during the system startup.



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



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

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

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

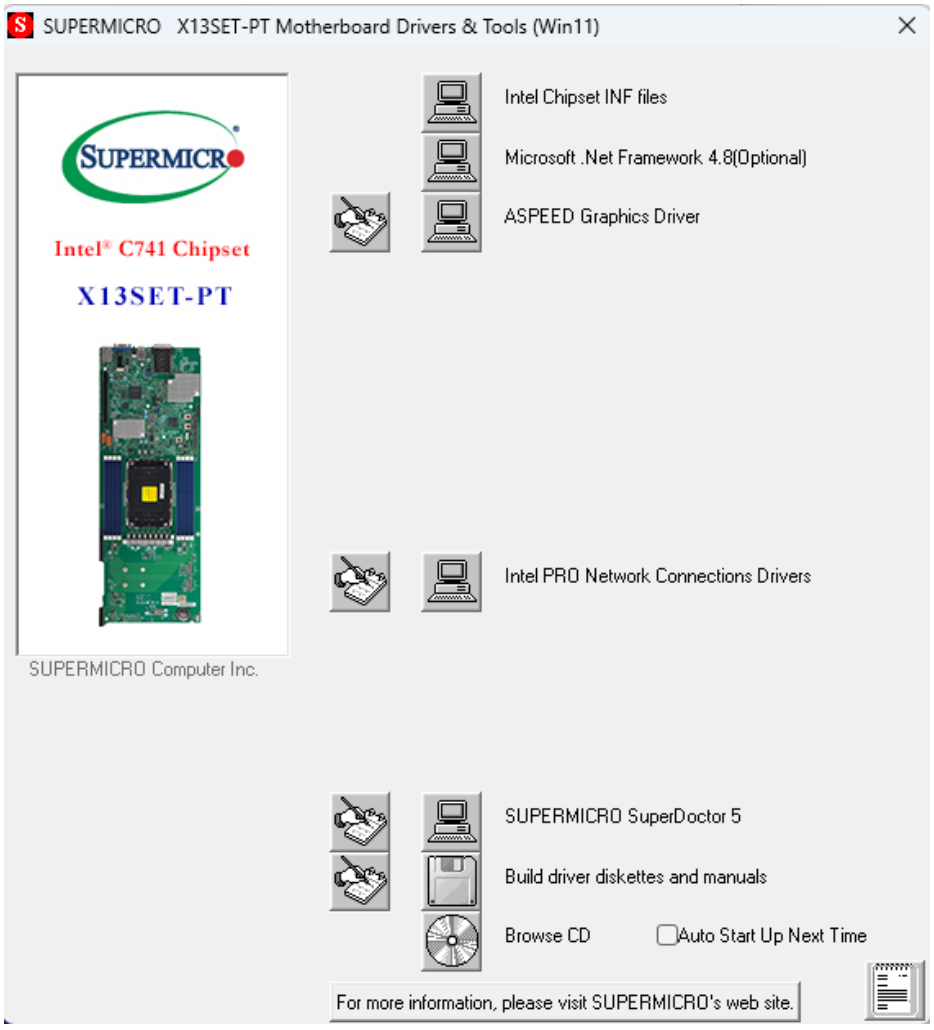
B.2 Driver Installation

The Supermicro website that contains drivers and utilities for your system is at https://www.supermicro.com/wdl/driver. Some of these must be installed, such as the chipset driver.

After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash or media drive. (You may also use a utility to extract the ISO file if preferred.)

Another option is to go to the Supermicro website at http://www.supermicro.com/products/. Find the product page for your motherboard, and "Download the Latest Drivers and Utilities".

Insert the flash drive or disk and the screenshot shown below should appear.



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 re-boot the system before moving on to the next item on the list.** The bottom icon with a CD on it allows you to view the entire contents.

B.3 BMC

The X13SET-PT motherboard 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 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 user name 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 a potential bodily injury may occur. Should you have questions or experience difficulty, contact Supermicro's Technical Support department for assistance. Only certified technicians should attempt to install or configure components.

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

These warnings may also be found on our website at http://www.supermicro.com/about/policies/safety_information.cfm.

Battery Handling



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

電池の取り扱い

電池交換が正しく行われなかった場合、破裂の危険性があります。交換する電池はメーカーが推奨する型、または同等のものを使用下さい。使用済電池は製造元の指示に従って処分して下さい。

警告

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

警告

電池更換不當會有爆炸危險。請使用製造商建議之相同或功能相當的電池更換原有電池。請按照製造商的說明指示處理廢棄舊電池。

Warnung

Bei Einsetzen einer falschen Batterie besteht Explosionsgefahr. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

Attention

Danger d'explosion si la pile n'est pas remplacée correctement. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

¡Advertencia!

Existe peligro de explosión si la batería se reemplaza de manera incorrecta. Reemplazar la batería exclusivamente con el mismo tipo o el equivalente recomendado por el fabricante. Desechar las baterías gastadas según las instrucciones del fabricante.

אזהרה!

קיימת סכנת פיצוץ של הסוללה במידה והוחלפה בדרך לא תקינה. יש להחליף
את הסוללה בסוג התואם מחברת יצרן מומלצת.
סילוק הסוללות המשומשות יש לבצע לפי הוראות היצרן.

هناك خطر من انفجار في حالة اسحبذال البطارية بطريقة غير صحيحة فعليل
اسحبذال البطارية
فقط بنفس النبع أو ما يعادلها مما أوصث به الشرمة المصنعة
جخلص من البطاريات المسحعملة وفقا لحعليمات الشرمة الصانعة

경고!

배터리가 올바르게 교체되지 않으면 폭발의 위험이 있습니다. 기존 배터리와 동일하거나 제조사에서 권장하는 동등한 종류의 배터리로만 교체해야 합니다. 제조사의 안내에 따라 사용된 배터리를 처리하여 주십시오.

Waarschuwing

Er is ontploffingsgevaar indien de batterij verkeerd vervangen wordt. Vervang de batterij slechts met hetzelfde of een equivalent type die door de fabrikant aanbevolen wordt. Gebruikte batterijen dienen overeenkomstig fabrieksvoorschriften afgevoerd te worden.

Product Disposal



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

製品の廃棄

この製品を廃棄処分する場合、国の関係する全ての法律・条例に従い処理する必要があります。

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

Die Entsorgung dieses Produkts sollte gemäß allen Bestimmungen und Gesetzen des Landes erfolgen.

¡Advertencia!

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

Attention

La mise au rebut ou le recyclage de ce produit sont généralement soumis à des lois et/ou directives de respect de l'environnement. Renseignez-vous auprès de l'organisme compétent.

סילוק המוצר

אזהרה!

סילוק סופי של מוצר זה חייב להיות בהתאם להנחיות וחוקי המדינה.

عند التخلص النهائي من هذا المنتج ينبغي التعامل معه وفقا لجميع القانين واللائح البطنية

경고!

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

Waarschuwing

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