



X12SPA-TF

USER'S MANUAL

Revision 1.1a

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

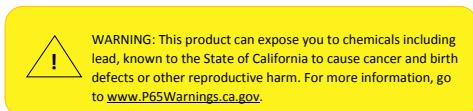
Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or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

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

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

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

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



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

Manual Revision 1.1a

Release Date: September 16, 2022

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 © 2022 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 X12SPA-TF motherboard.

About This Motherboard

The Supermicro X12SPA-TF supports a single 3rd Generation Intel® Xeon® Scalable Series processor (in Socket P+ LGA 4189) with up to 40 CPU cores and a thermal design power (TDP) of up to 270W. Built with the Intel C621A chipset, the X12SPA-TF supports up to 1 TB of ECC RDIMM, 4 TB of 3DS RDIMM, 2 TB of LRDIMM, 4 TB of 3DS LRDIMM, and 4 TB of Intel Optane™ Persistent Memory (PMem) 200 Series with speeds of up to 3200 MHz (2DPC) in 16 DDR4 (288-pin) SMD DIMM slots. This motherboard features superior IO expandability, which includes seven PCIe 4.0 slots, eight SATA 3.0 ports, four M.2 sockets, and 13 USB ports/headers. It also offers the most advanced data protection capability that encompasses Trusted Platform Module (TPM) and Root of Trust (RoT) support. The X12SPA-TF is optimized for high-performance, high-end computing platforms and is ideal for big data, enterprise applications. Please note that this motherboard is intended to be installed and serviced by professional technicians only. For processor/memory updates, please refer to our website at <http://www.supermicro.com/products/>.



Note 1: Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.

Note 2: Memory speed support depends on the processors used in the system.

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 (Sales Inquiries)
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 Inquiries)
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 Checklist	7
1.2 Processor and Chipset Support	17
1.3 Special Features	17
1.4 System Health Monitoring	17
1.5 ACPI Features	18
1.6 Power Supply	19
1.7 Serial Port.....	19
1.8 Intel® Optane™ Persistent Memory (PMem) 200 Series Overview.....	19

Chapter 2 Installation

2.1 Static-Sensitive Devices	20
2.2 Processor and Heatsink Installation	21
2.3 Motherboard Installation.....	37
2.4 Memory Support and Installation	39
2.5 Rear I/O Ports	44
2.6 Front Control Panel	49
2.7 Connectors	55
2.8 Jumper Settings	66
2.9 LED Indicators.....	71

Chapter 3 Troubleshooting

3.1 Troubleshooting Procedures	73
3.2 Technical Support Procedures	76
3.3 Frequently Asked Questions	77
3.4 Battery Removal and Installation	79
3.5 Returning Merchandise for Service.....	80

Chapter 4 UEFI BIOS

4.1 Introduction.....	81
4.2 Main Setup	82
4.3 Advanced Setup Configurations.....	84
4.4 Event Logs	118

4.5 IPMI120

4.6 Security.....124

4.7 Boot.....132

4.8 Save & Exit.....135

Appendix A BIOS POST Codes

A.1 BIOS POST Codes.....137

Appendix B Software

B.1 Microsoft Windows OS Installation.....138

B.2 Driver Installation.....140

B.3 SuperDoctor® 5.....141

B.4 IPMI142

B.5 Logging into the BMC (Baseboard Management Controller).....142

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.

In addition to the motherboard, several important parts that are included in the retail box are listed below. If anything listed is damaged or missing, please contact your retailer.

1.1 Checklist

Main Parts List		
Description	Part Number	Quantity
Supermicro Motherboard	X12SPA-TF	1
I/O Shield	MCP-260-00148-0N	1
SATA Cables	CBL-0044L	6 (single pack)
SATA Cables	CBL-0044L	2 (bulk pack)
GPU to CPU Power Cable	CBL-PWEX-0663	1
CPU Carrier	SKT-1205L-P4IC-FXC	1

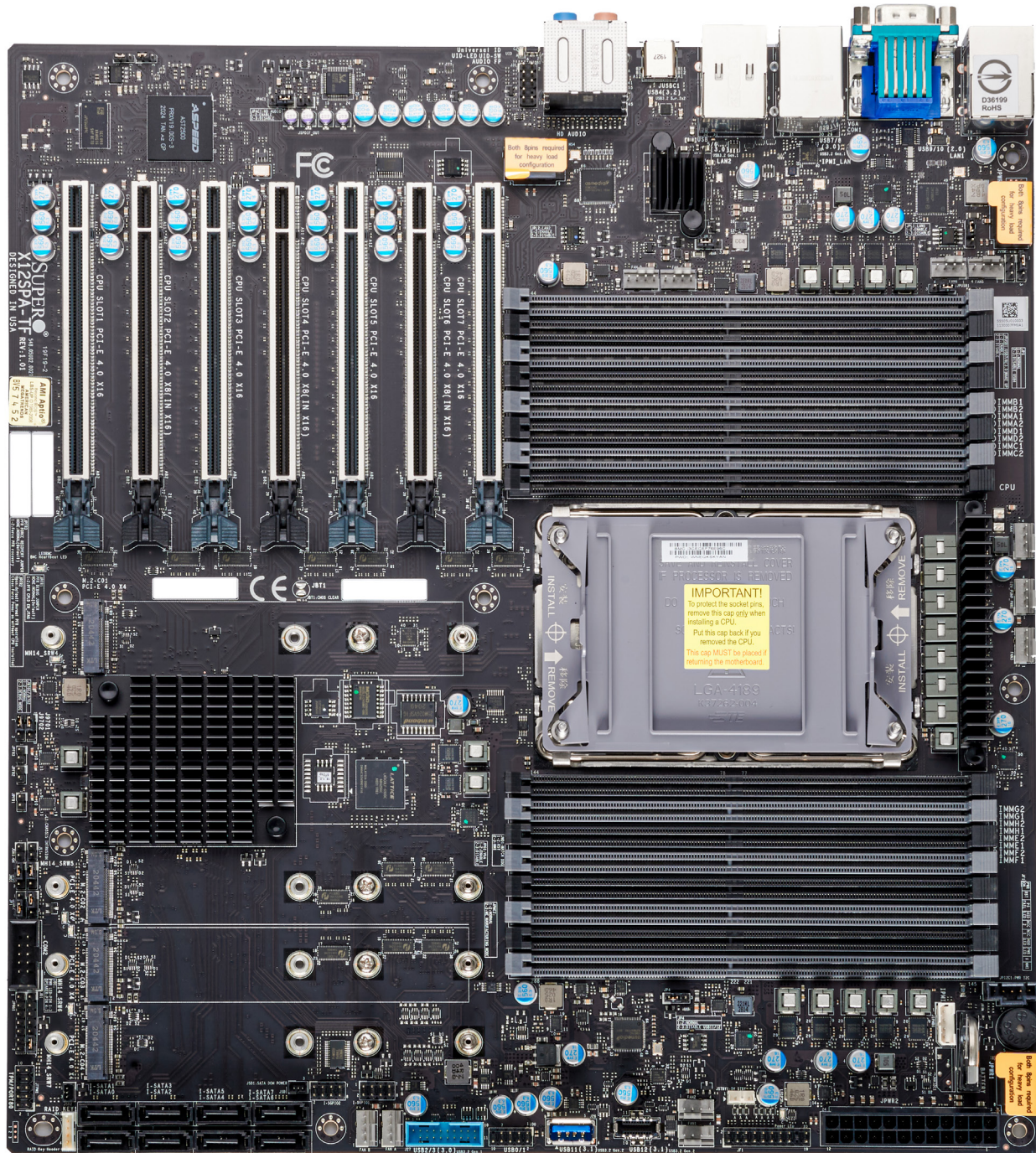
Important Links

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

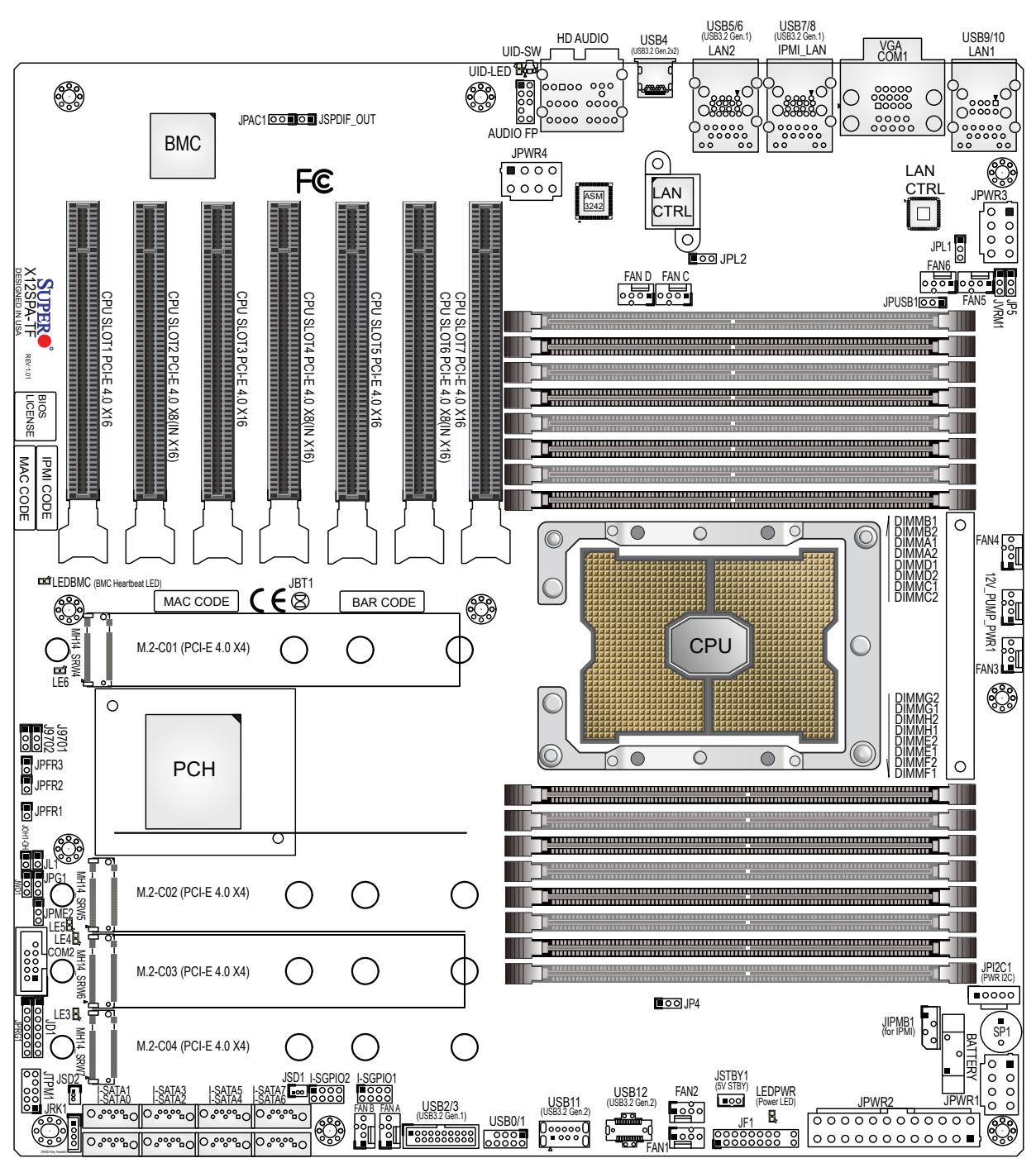
- Supermicro product manuals: <http://www.supermicro.com/support/manuals/>
- Product drivers and utilities: <https://www.supermicro.com/wdl/driver>
- Product safety info: http://www.supermicro.com/about/policies/safety_information.cfm
- A secure data deletion tool designed to fully erase all data from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

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

X12SPA-TF Motherboard Image

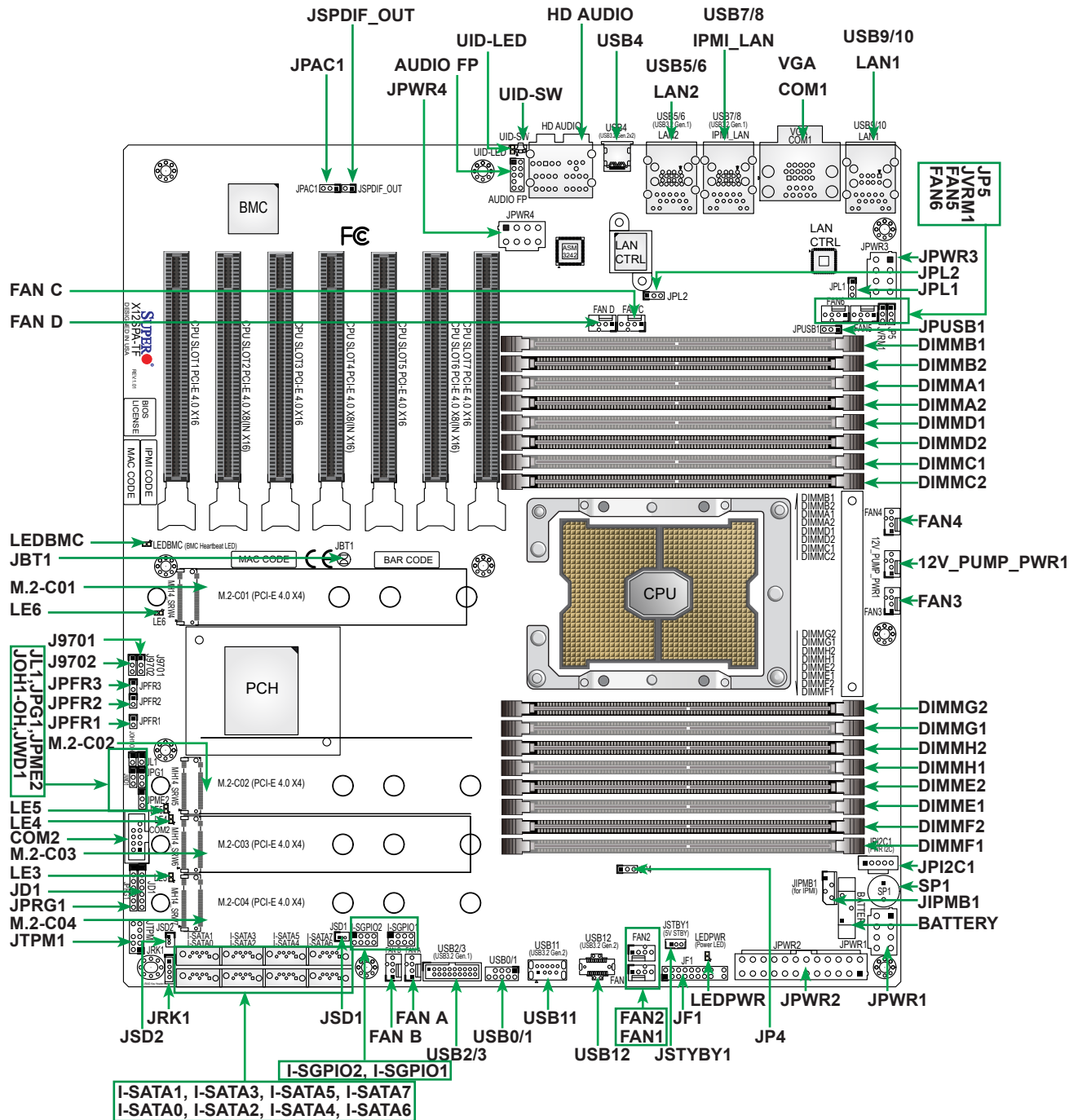


Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publication of the manual. The motherboard you received may or may not look exactly the same as the graphics shown in this manual.



Note: Components not documented are for internal testing only.

Quick Reference



Notes:



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

Quick Reference Table

Jumper	Description	Default Setting
J9701, J9702	Debug Mode	Pins 1-2 (Normal)
JBT1	Clear CMOS (Onboard)	Short Pads to Clear CMOS
JP4	USB11/12 Disable	Pins 1-2 (Normal)
JP5	USB4 Disable	Pins 1-2 (Normal)
JPAC1	HD Audio Enable/Disable	Pins 1-2 (Enabled)
JPFR1	PFR Debug (Pins 1-2: PFR CPLD EN_JTAG)	None (Normal)
JPFR2	PFR Operation (Close: force power on without CPU installed)	Open (Normal PFR Operation)
JPFR3	PFR Force Recovery (Pins 1-2: force PFR recovery)	None (Normal)
JPG1	VGA Enable/Disable	Pins 1-2 (Enabled)
JPL1, JPL2	LAN1/LAN2 Enable/Disable	Pins 1-2 (Enabled)
JPME2	Intel Manufacturing Mode	Pins 1-2 (Normal)
JPUSB1	USB7/8 Wake Up	Pins 1-2 (Enabled)
JVRM1	Debug Mode	None (Normal)
JWD1	Watch Dog Function Enable	Pins 1-2 (Reset)
LED	Description	Status
LE3, LE4, LE5, LE6	M.2 LEDs for M.2-C04/M.2-C03/M.2-C02/M.2-C01	Blinking Green: Device Working
LEDBMC	BMC Heartbeat LED	Blinking Green: BMC Normal
LEDPWR	Onboard Power LED	Solid Green: Power On
UID-LED	Unit Identifier (UID) LED	Blue On: Unit Identified
Connector	Description	
12V_PUMP_PWR1	12V 4-pin Power Connector (for CPU liquid cooling pump)	
AUDIO_FP	Front Panel Audio Header	
BATTERY	Onboard Battery	
COM1, COM2	COM1: COM Port (back panel). COM2: COM Header	
CPU SLOT1/3/5/7	PCIe 4.0 x16 Slots * SLOT1 will change to PCIe x8 link when either M.2-C03 or M.2-C04 is populated with an SSD. Also, SLOT1 will be completely disabled when either M.2-C01 or M.2-C02 is populated with an SSD.	
CPU SLOT2/4/6	PCIe 4.0 x16 Slots (PCIe 4.0 x8 link)	
FAN1 - FAN6	CPU Fan Headers	
FAN A - FAN D	System Fan Headers	
HD AUDIO	Back Panel High Definition Audio Ports	
I-SATA0 - I-SATA7	Intel Serial ATA (SATA 3.0) Ports 0~7 (6 Gb/second)	
I-SGPIO1, I-SGPIO2	Serial General Purpose I/O Headers * I-SGPIO1 is for I-SATA0 - I-SATA3. I-SGPIO2 is for I-SATA4 - I-SATA7.	
IPMI_LAN	Dedicated IPMI LAN Port	
JD1	Power LED / Speaker Header (Pins 1-3: Power LED, Pins 4-7: Speaker)	

Connector	Description
JF1	Front Control Panel Header
JIPMB1	4-pin External I ² C Header (for an IPMI card)
JL1	Chassis Intrusion Header
JOH1-OH	Overheat LED Header
JPI ² C1	Power Supply SMBus I ² C Header
JPRG1	CPLD FW Update (Debug Mode)
JPWR1/3/4	+12V 8-pin CPU Power Connectors (Required)
JPWR2	24-pin ATX Main Power Connector (Required)
JRK1	Intel VROC RAID Key Header (Note: A VROC hardware key is required for RAID support.)
JSD1, JSD2	SATA DOM (Disk-On-Module) Power Connectors
JSPDIF_OUT	Sony/Philips Digital Interface (S/PDIF) Out Header
JSTBY1	Standby Power Header (5V)
JTPM1	Trusted Platform Module (TPM)/Port 80 Header
LAN1, LAN2	LAN1: RJ45 1GbE LAN Port. LAN2: RJ45 10GbE LAN Port
M.2-C01 - M.2-C04	PCIe 4.0 x4 M.2 M-key Sockets (Support RAID 0, 1, 5, and 10) (Small form factor devices and other portable devices for high speed NVMe SSDs)
MH14_SRW4 - MH14_SRW7	M.2 Mounting Holes
SP1	Internal Speaker/Buzzer
UID-SW	Unit Identifier (UID) Switch / BMC Reset Button
USB0/1	Front Accessible USB 2.0 Header
USB2/3	Front Access USB 3.2 Gen. 1 Header
USB4	Back Panel USB 3.2 Gen. 2x2 Port
USB5, USB6, USB7, USB8	Back Panel USB 3.2 Gen. 1 Ports
USB9, USB10	Back Panel USB 2.0 Ports
USB11	Front Access Type-A USB 3.2 Gen. 2 Port
USB12	Front Access USB 3.2 Gen. 2 Header
VGA	VGA Port (Dedicated for IPMI)

Motherboard Features

Motherboard Features	
CPU	
<ul style="list-style-type: none"> Supports a single 3rd Generation Intel Xeon Scalable-SP processor (in Socket P+ LGA 4189) with up to 40 CPU cores and a thermal design power (TDP) of up to 270W 	
Memory	
<ul style="list-style-type: none"> Supports up to 1 TB of ECC RDIMM, 4 TB of 3DS RDIMM, 2 TB of LRDIMM, 4 TB of 3DS LRDIMM, and 4 TB of Intel Optane PMem 200 Series with speeds of up to 3200 MHz (2DPC) in 16 DDR4 (288-pin) SMD DIMM slots <p> Note 1: Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.</p> <p>Note 2: Memory speed and capacity support depends on the processors used in the system.</p>	
DIMM Size	
<ul style="list-style-type: none"> Up to 256 GB at 1.2V <p> Note: For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.</p>	
Chipset	
<ul style="list-style-type: none"> Intel PCH C621A 	
Expansion Slots	
<ul style="list-style-type: none"> Four PCIe 4.0 x16 slots (CPU SLOT1/3/5/7) Three PCIe 4.0 x8 (IN x16) slots (CPU SLOT2/4/6) Four PCIe 4.0 x4 M.2 sockets (support M-Key 2260, 2280, and 22110) 	
Network	
<ul style="list-style-type: none"> Intel i210AT for one 1Gb Ethernet LAN port Aquantia AQC113 for one 10Gb Ethernet LAN port One Dedicated IPMI LAN port located on the rear I/O panel (via AST2500 BMC) 	
Baseboard Management Controller (BMC)	
<ul style="list-style-type: none"> ASPEED AST2500 BMC 	
Graphics	
<ul style="list-style-type: none"> Graphics controller & VGA support via ASPEED AST2500 BMC 	
I/O Devices	
<ul style="list-style-type: none"> Serial (COM) Port 	<ul style="list-style-type: none"> One (serial port on the rear I/O panel (COM1) One front accessible serial port header (COM2)
<ul style="list-style-type: none"> SATA 3.0 	<ul style="list-style-type: none"> Eight I-SATA 3.0 ports at 6 Gb/s (I-SATA0~7)
<ul style="list-style-type: none"> Video (VGA) Connections 	<ul style="list-style-type: none"> One VGA port on the rear I/O panel (VGA)

Peripheral Devices

- One USB 3.2 Gen. 2x2 port (USB4), four USB 3.2 Gen. 1 ports (USB5/USB6/USB7/USB8), two USB 2.0 ports (USB9/USB10) on the rear I/O panel
- One front accessible USB 2.0 header with two USB connections (USB0/1)
- One front accessible USB 3.2 Gen. 1 header with two USB connections (USB2/3)
- One front accessible Type-A USB 3.2 Gen. 2 port (USB11)
- One front accessible USB 3.2 Gen. 2 header (USB12)

BIOS

- AMI BIOS
- ACPI 3.0 or later, PCI firmware 4.0 support, BIOS rescue hot-key, SPI dual/quad speed support, Real Time Clock (RTC) wakeup, 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 +/-12V, +5V/+5V standby, +3.3V, and +3.3V standby
- Onboard temperature monitoring for CPU, VRM, LAN, PCH, system, and memory
- 7+1 CPU switch phase voltage regulator
- CPU thermal trip support
- Platform Environment Control Interface (PECI)

Fan Control

- Fan status monitoring via IPMI connections
- Single cooling zone
- Low-noise fan speed control
- Ten 4-pin fan headers

System Management

- SuperDoctor® 5
- Chassis intrusion header and detection
- Server platform service

Firmware Integrity/System Security

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

LED Indicators

- Power LED
- UID/remote UID
- LAN activity LED

Dimensions

- 13" (L) x 12" (W) E-ATX (330 mm x 305 mm)

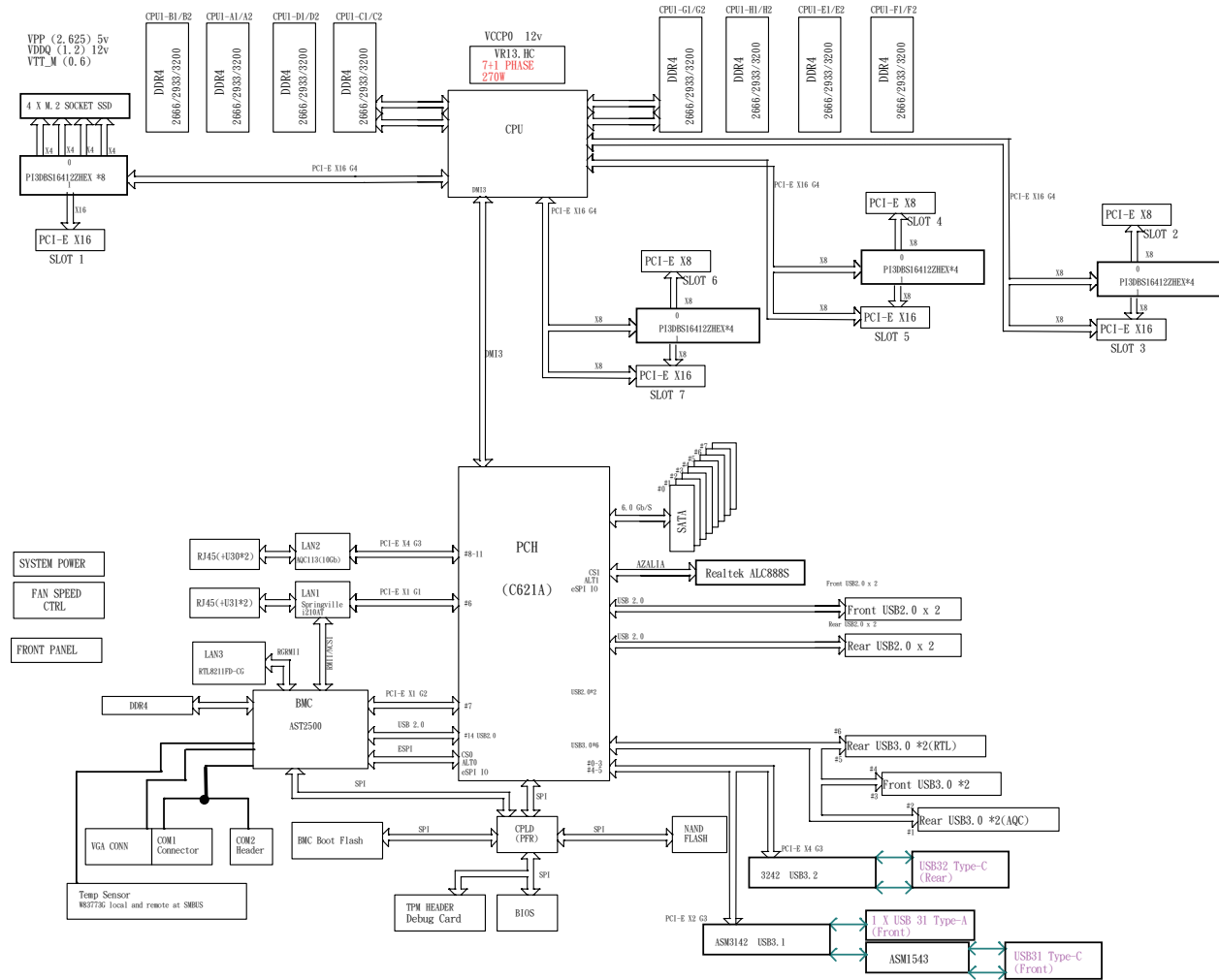


Note 1: The CPU maximum thermal design power (TDP) is subject to chassis and heatsink cooling restrictions. For proper thermal management, please check the chassis and heatsink specifications.

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

Note 3: For proper BMC configuration, please refer to https://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf.

System Block Diagram X12SPA-TF



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 3rd Gen. Intel Xeon Scalable Processors (Socket P+) and the Intel C621A chipset, the X12SPA-TF motherboard increases energy efficiency, and system performance for a multitude of applications such as high performance computing, artificial intelligence (AI), deep learning (DL), big data, and enterprise applications.

Features Supported

- Performance improvements with higher core counts, up to 3 UPIs/socket at 11.2 GT/s
- Vector Neural Network Instructions (VNNI) support to accelerate training
- New hardware-enhanced security features help protect platform & data without compromising performance
- High PCIe performance (PCIe 4.0) with double the bandwidth of PCIe 3.0

1.3 Special Features

Recovery from AC Power Loss

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

1.4 System Health Monitoring

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the IPMI interface. Whenever the temperature of the CPU or the system exceeds a user-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, please be sure to provide adequate air-flow to your system.

System Resource Alert

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

1.5 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, please refer to the Supermicro website.

1.6 Power Supply

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

The X12SPA-TF motherboard accommodates a 24-pin ATX power supply. Although most power supplies generally meet the specifications required by the CPU, some are inadequate. In addition, three 12V 8-pin and one 4-pin power connections are also required to ensure adequate power supply to the system.

Warning! To avoid damaging the power supply on the motherboard, be sure to use a power supply that contains one 24-pin and three 8-pin power connectors. Be sure to connect the power supplies to the 24-pin power connector (JPWR2) and 8-pin power connectors (JPWR1/JPWR3/JPWR4) on the motherboard. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.


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

1.7 Serial Port

The X12SPA-TF motherboard supports two serial communication connections. COM1 port and COM2 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.

1.8 Intel® Optane™ Persistent Memory (PMem) 200 Series Overview

The 3rd Gen. Intel Xeon Scalable Processors support the new Intel Optane PMem 200 Series memory. Intel Optane PMem offers higher capacities than the traditional DDR4 modules. It also provides increased storage capabilities due to data persistence in a DDR4 form factor for higher performance computing platforms with flexible configuration options.

 **Note:** Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.

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

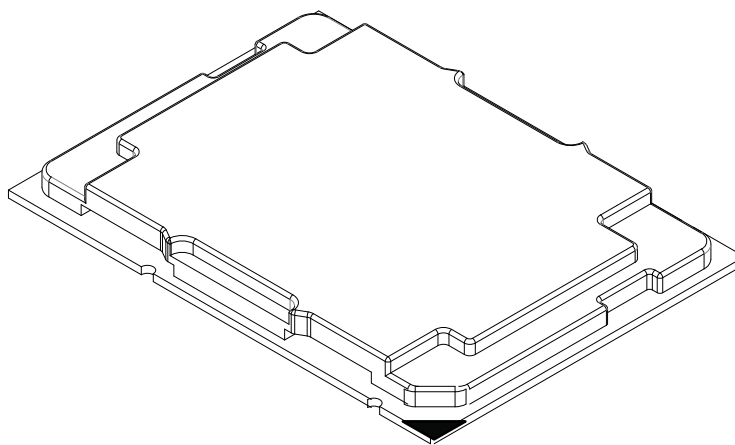
The motherboard is shipped in antistatic packaging to avoid static damage. When unpacking the motherboard, make sure that the person handling it is static protected.

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 into the CPU socket. Before installation, be sure to perform the following steps below:

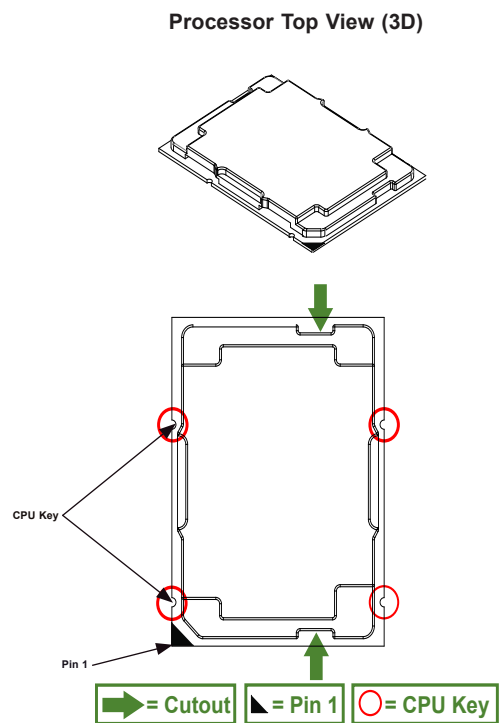
- Please carefully follow the instructions given on the previous page to avoid ESD-related damages.
- Unplug the AC power cords from all power supplies after shutting down the system.
- Check that the plastic protective cover is on the CPU socket and none of the socket pins are bent. If they are, contact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

The 3rd Gen. Intel Xeon Scalable Processor



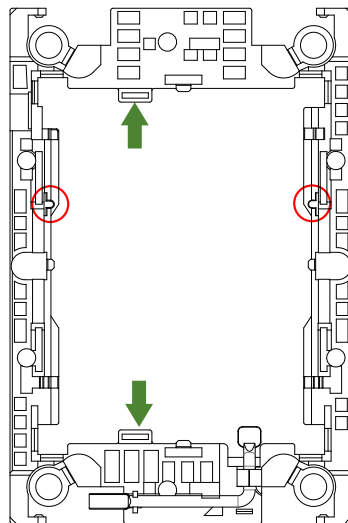
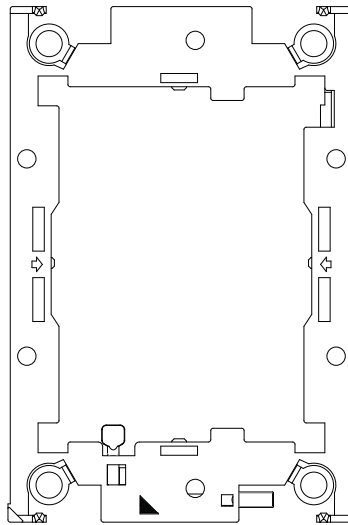
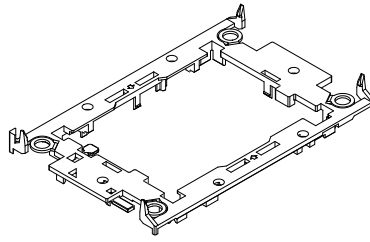
Processor Top View

1. The 3rd Gen. Intel Xeon Scalable Processor



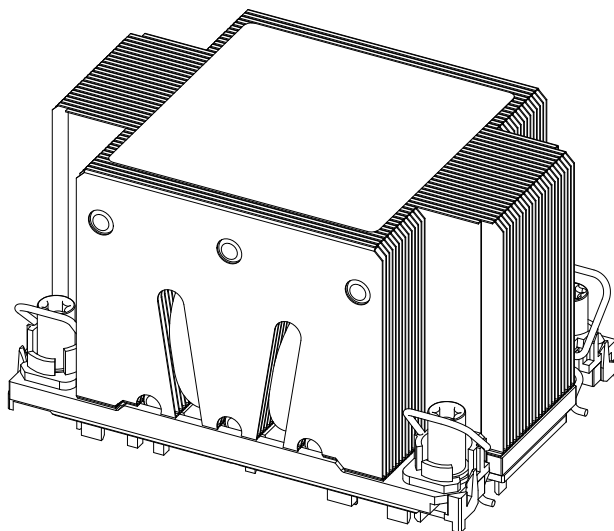
Processor Top View


2. The Processor Carrier



Carrier Bottom View

3. Heatsink

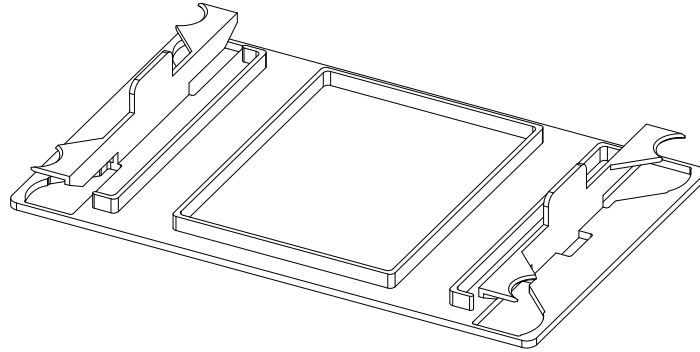


 **Note:** Exercise extreme care when handling the heatsink. Pay attention to the edges of heatsink fins which can be sharp! To avoid damaging the heatsink, please do not apply excessive force on the fins when handling the heatsink.

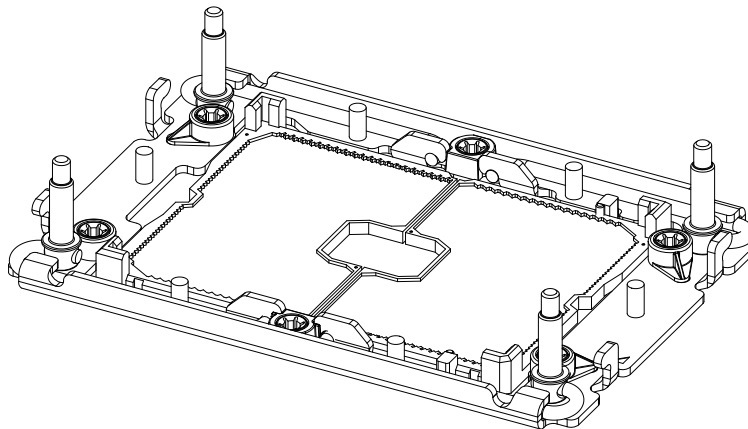
Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

Plastic Protective Cover



CPU Socket

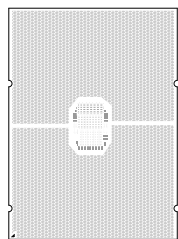


Overview of the Processor Carrier Assembly

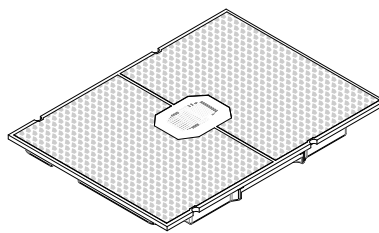
The processor carrier assembly contains a 3rd Gen. Intel Xeon Scalable processor and a processor carrier. Carefully follow the instructions given in the installation section to place a processor into the carrier to create a processor carrier.

1. The 3rd Gen. Intel Xeon Scalable Processor

Intel Processor (Bottom View)



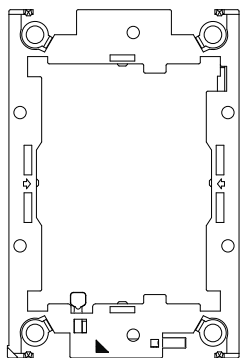
Processor (2D)



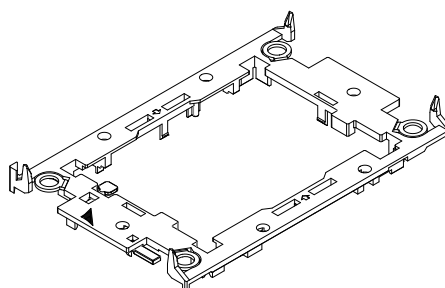
Processor (3D)

2. Processor Carrier

Intel Processor Carrier (Top View)

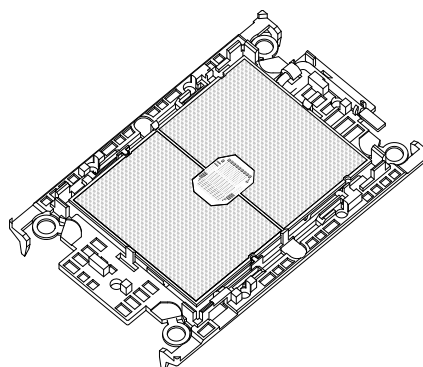


Processor Carrier (2D)



Processor Carrier (3D)

3. Processor Carrier Assembly

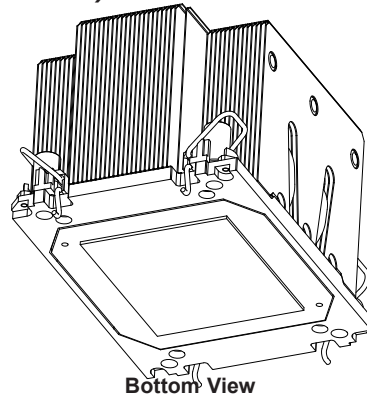


(with Processor Seated inside the Carrier)

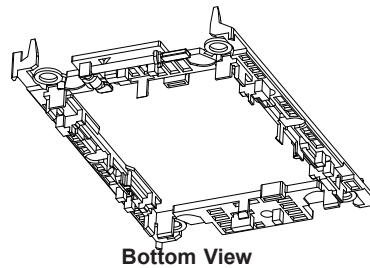
Overview of the Processor Heatsink Module

The Processor Heatsink Module (PHM) contains a heatsink, a processor carrier, and a 3rd Gen. Intel Xeon Scalable processor.

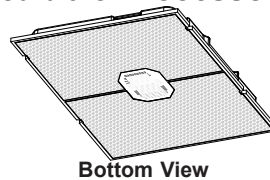
1. Heatsink (with Thermal Grease)



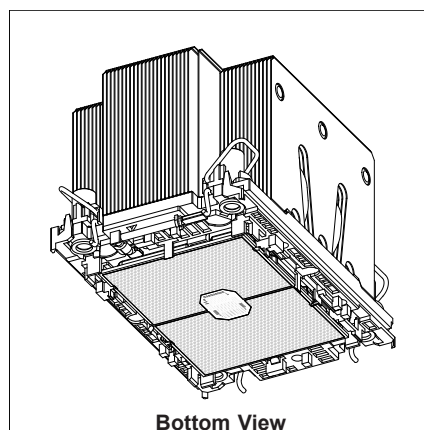
2. Processor Carrier



3. The 3rd Gen. Intel Xeon Scalable Processor




4. Processor Heatsink Module (PHM)



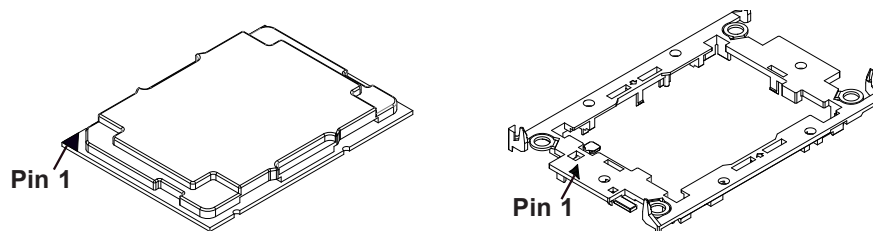
Creating the Processor Carrier Assembly

The processor carrier assembly contains a 3rd Gen. Intel Xeon Scalable processor and a processor carrier.

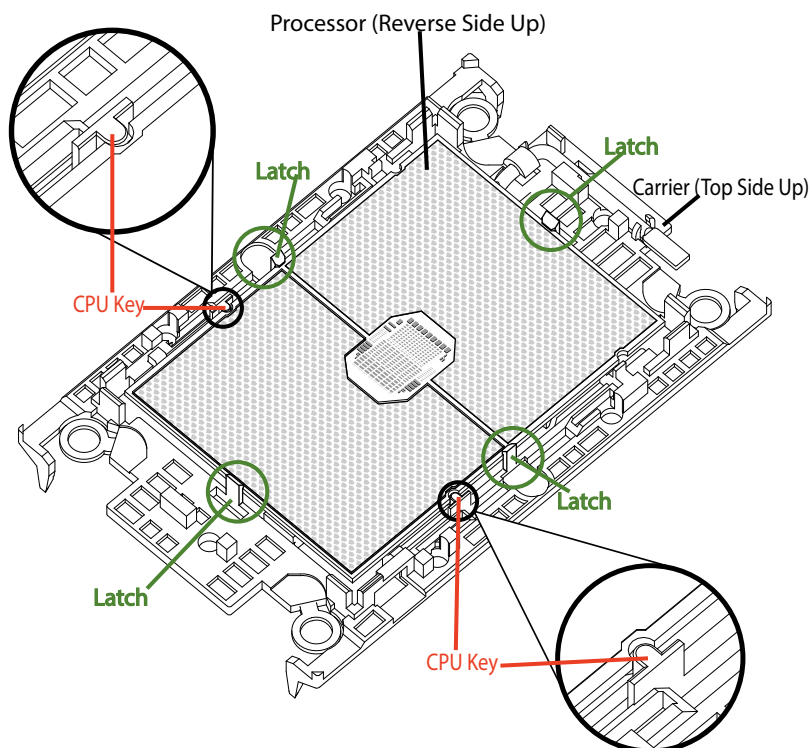
To create the processor carrier assembly, please follow the steps below:

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

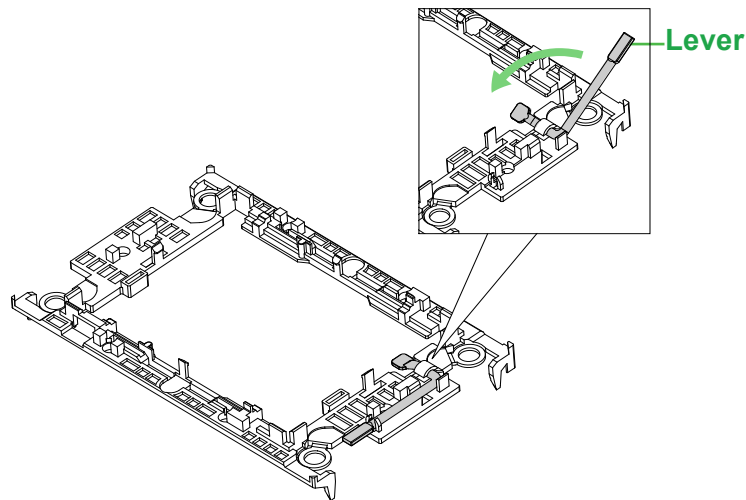
1. Hold the processor with the LGA lands (with Gold CPU contacts) facing down. Locate the small, gold triangle at the corner of the processor and the corresponding hollowed triangle on the processor carrier as shown in the graphics below. Please note that the triangle indicates Pin 1 location.



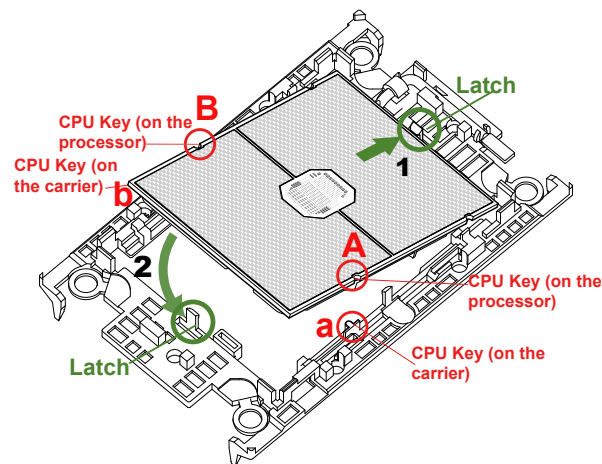
2. First, turn over the processor carrier and locate Pin 1 on the CPU and Pin 1 on the carrier. Then, turn the processor over with the processor reverse side (gold contacts) facing up and locate CPU keys on the processor. Finally, locate the CPU keys and four latches on the carrier as shown below.



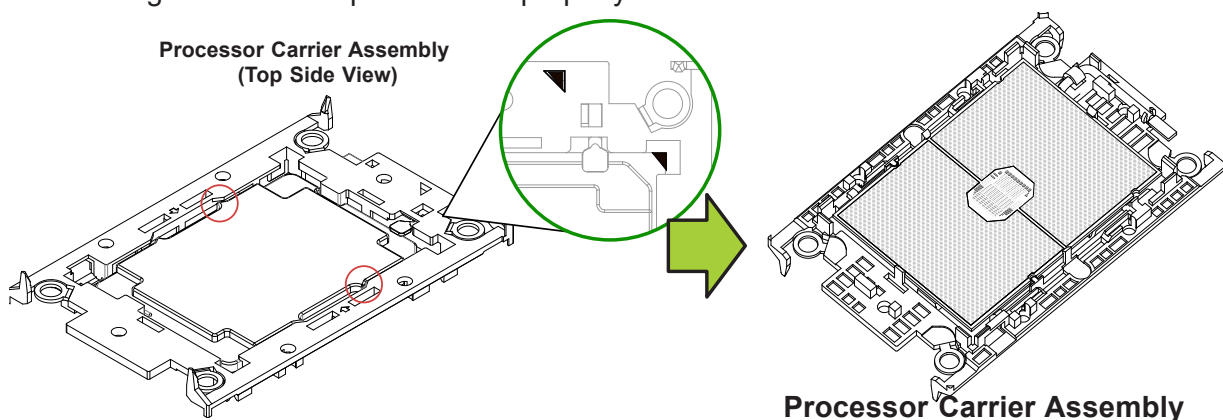
3. Locate the lever on the CPU socket and press the lever down as shown below.



4. Using Pin 1 as a guide, carefully align the CPU keys (A & B) on the processor against the CPU keys on the carrier (a & b) as shown in the drawing below.
5. Once they are properly aligned, carefully place one end of the processor into the latch marked 1 on the carrier, and place the other end of processor into the latch marked 2.




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.

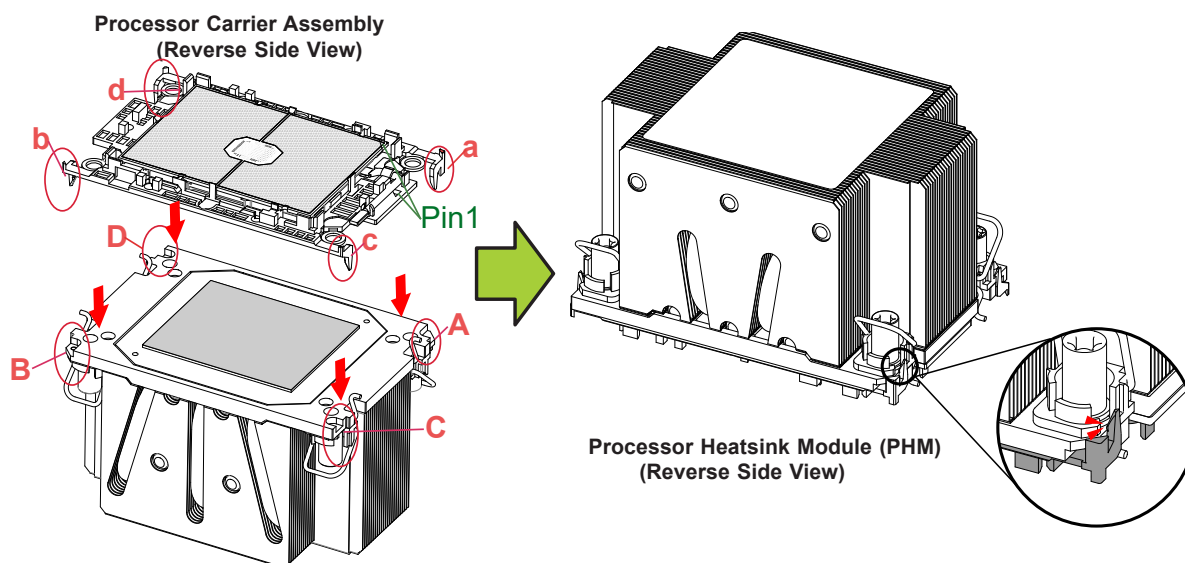


Creating the Processor Heatsink Module (PHM)

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

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

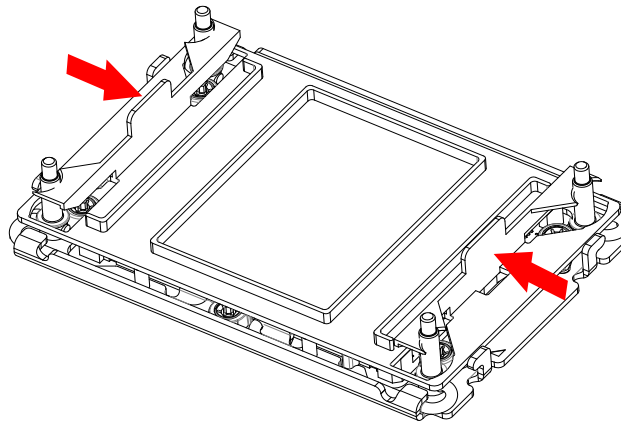
1. Turn the heatsink over with the thermal grease, which is on the reverse side of the heatsink, facing up. Pay attention to the two triangle cutouts (A, B) located at the diagonal corners of the heatsink as shown in the drawing below.
2. Hold the processor carrier assembly top side (with thermal grease)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



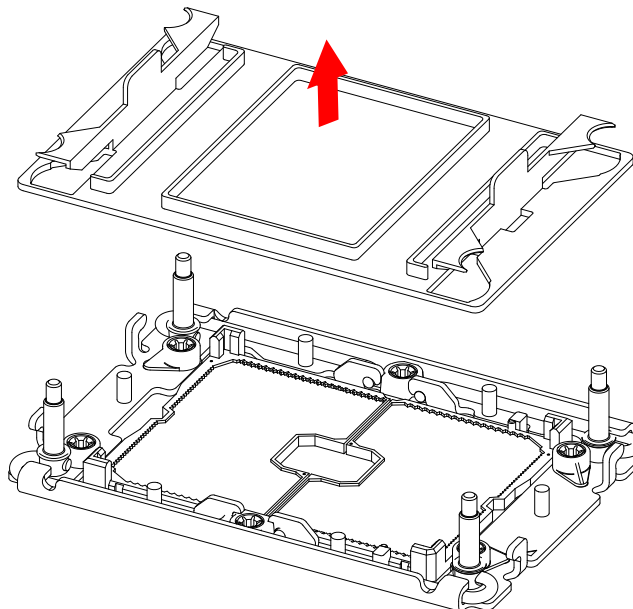
Preparing the CPU Socket for Installation

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

Removing the Plastic Protective Cover from the socket



1. Press the tabs inward.

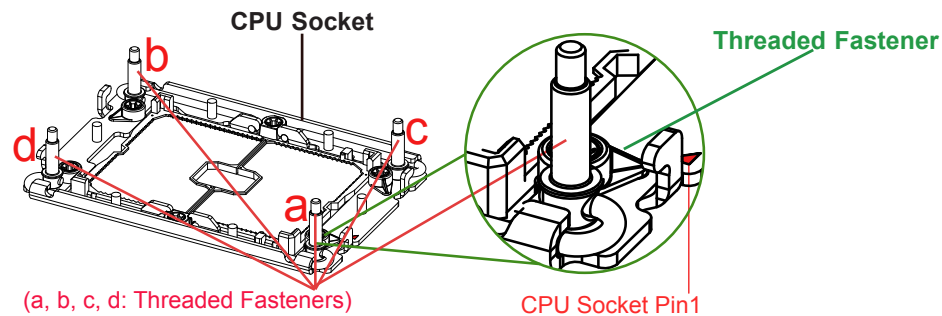


2. Pull up the protective cover from the socket.

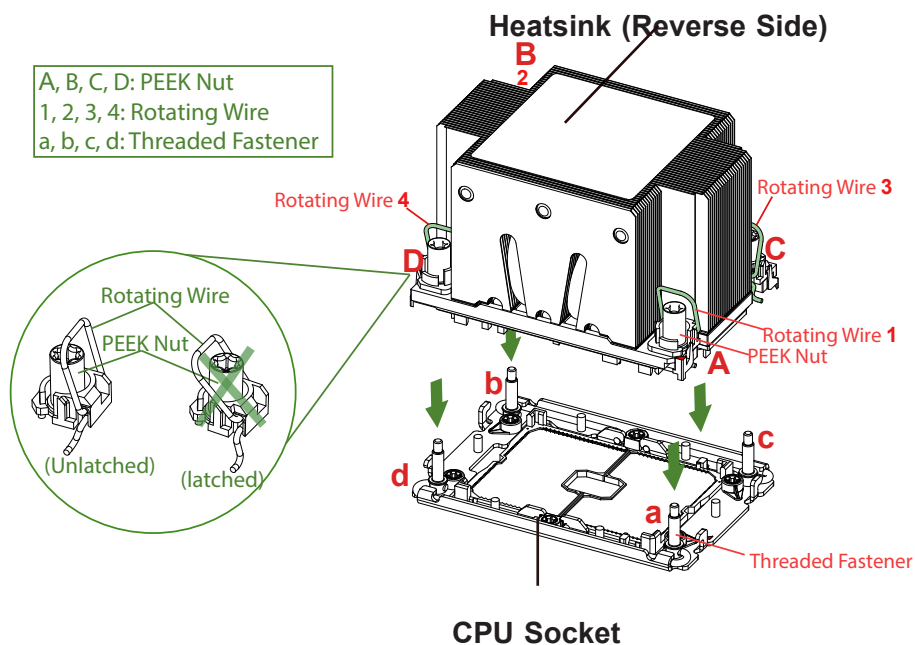
Preparing to Install the Processor Heatsink Module (PHM) into the CPU Socket

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

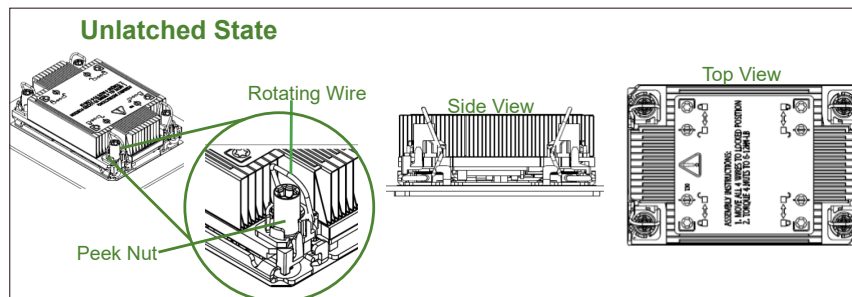
1. Locate four threaded fasteners (a, b, c, d) on the CPU socket.



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

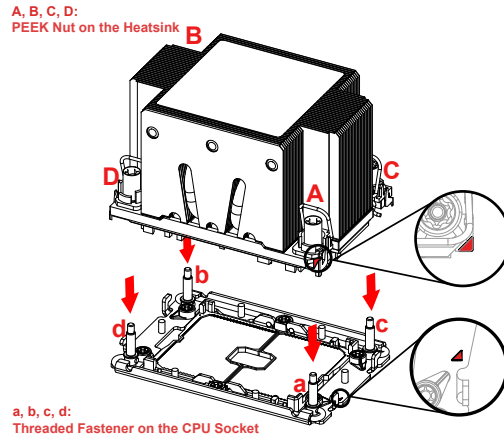


3. Check the rotating wires (1, 2, 3, 4) to make sure that they are at unlatched positions as shown in the drawing below before installing the PHM into the CPU socket.

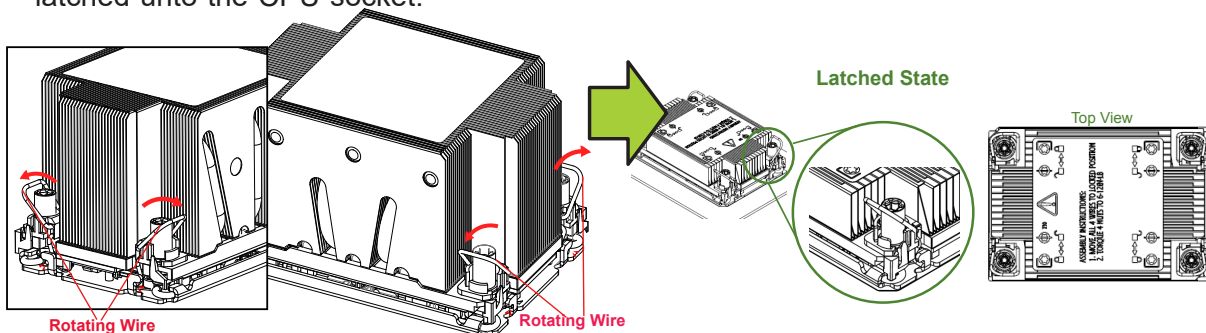


Installing the Processor Heatsink Module (PHM)

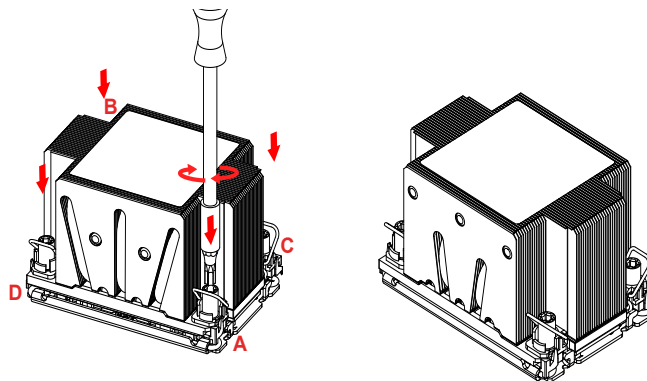
1. Align PEEK nut "A", which is next to the triangle (Pin 1) on the heatsink, against threaded fastener "a" on the CPU socket. Then align PEEK nuts "B", "C", "D" on the heatsink against threaded fasteners "b", "c", "d" on the CPU socket, making sure that all PEEK nuts on the heatsink are properly aligned with the correspondent threaded fasteners on the CPU socket.
2. Once they are aligned, gently place the Processor Heatsink Module (PHM) on top the CPU socket, making sure that each PEEK nut is properly attached to its corresponding threaded fastener.



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



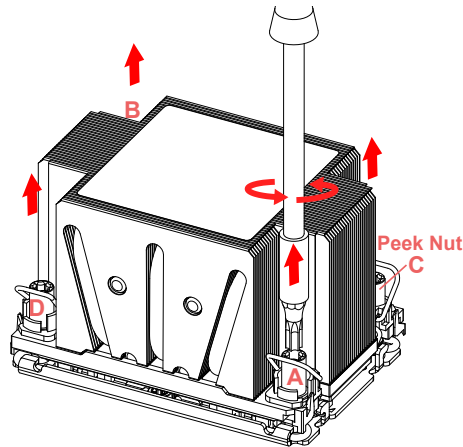
4. With a T30-bit screwdriver, tighten all PEEK nuts in the sequence of "A", "B", "C", and "D" with even pressure. To avoid damaging the processor or socket, do not use a force greater than 12 lbf-in when tightening the screws.
5. Examine all corners heatsink to ensure that the PHM is firmly attached to the CPU socket.



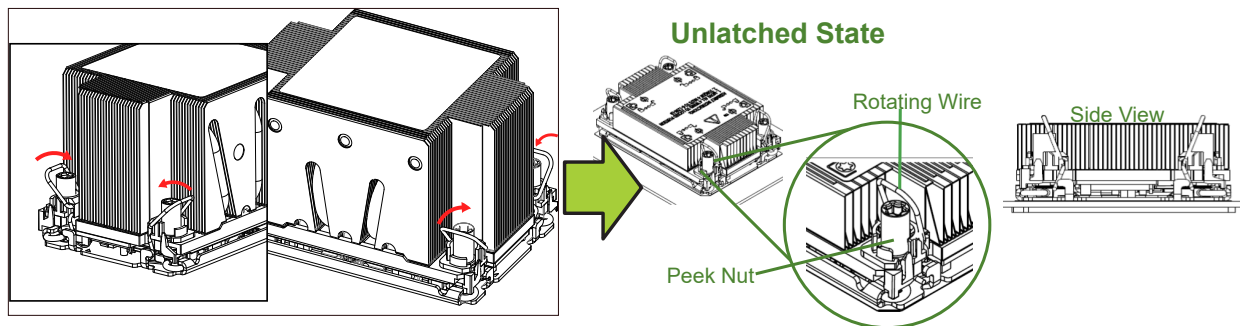
Removing the Processor Heatsink Module from the CPU Socket

Before removing the processor heatsink module (PHM) from the motherboard, unplug the AC power cord from all power supplies after shutting down the system. Then follow the steps below:

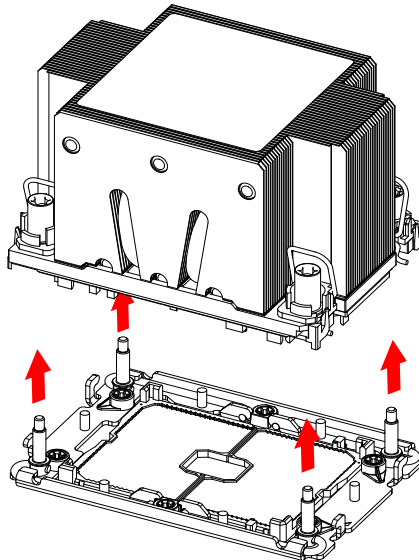
1. Use a T30-bit screwdriver to loosen the four peek nuts on the heatsink in the sequence of #A, #B, #C, and #D.



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.



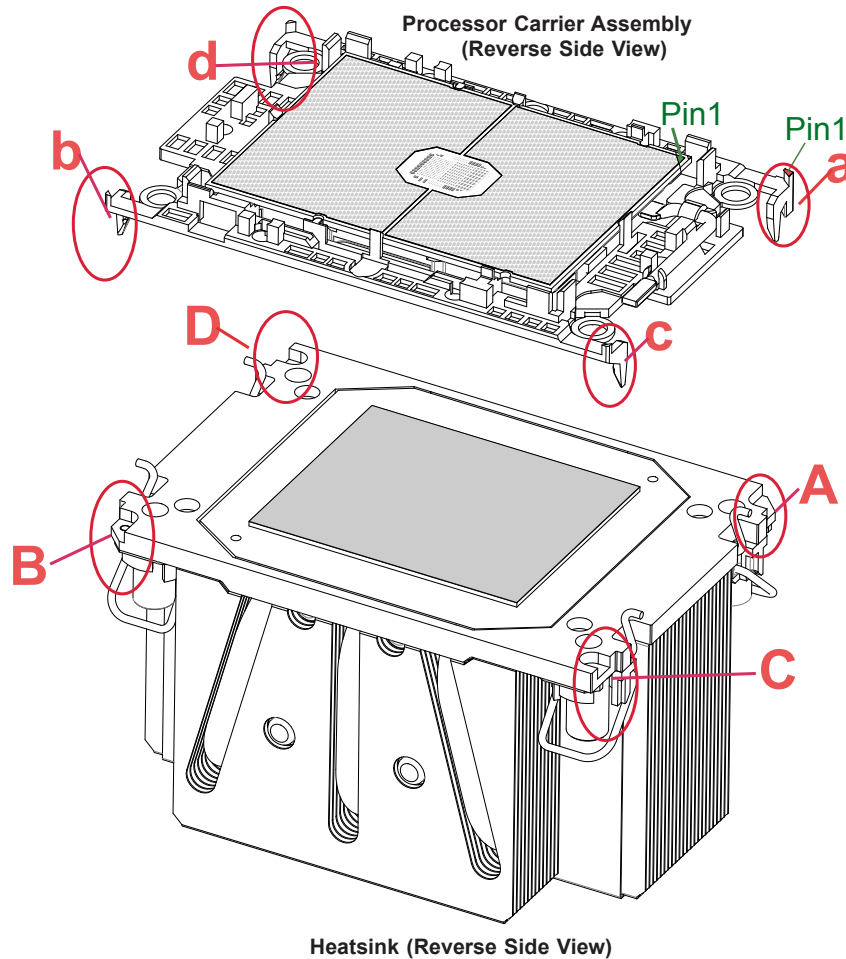
3. Gently lift the PHM upwards to remove it from the CPU socket.



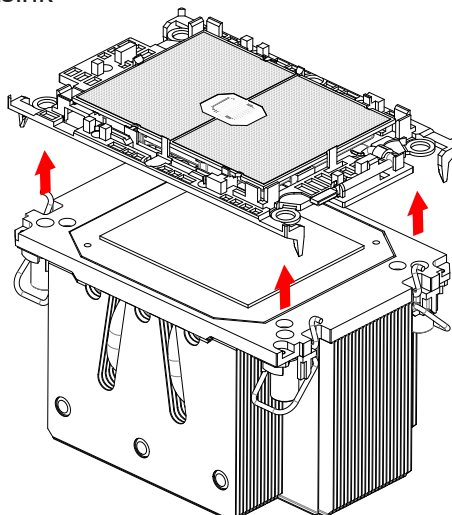
Removing the Processor Carrier Assembly from the Processor Heatsink Module (PHM)

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

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



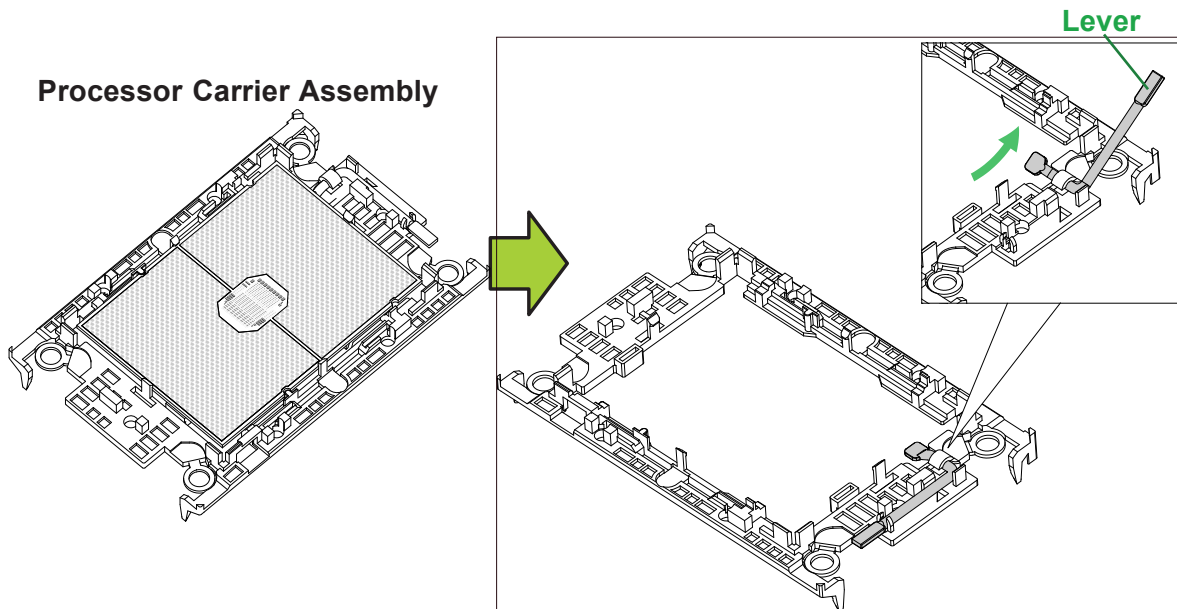
2. When all plastic clips are detached from the heatsink, remove the processor carrier assembly from the heatsink




Removing the Processor from the Processor Carrier Assembly

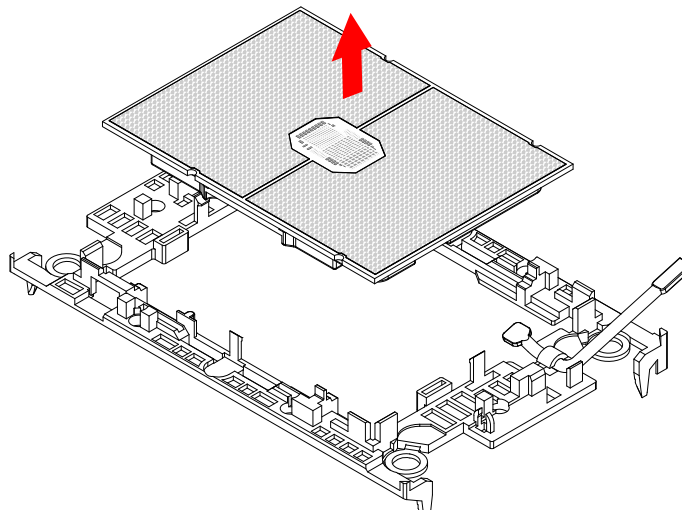
Once you have removed the processor carrier assembly from the PHM, you are ready to remove the processor from the processor carrier by following the steps below.

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



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

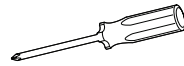
 **Note:** To avoid damaging the processor and its pins, please handle the processor with care.



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



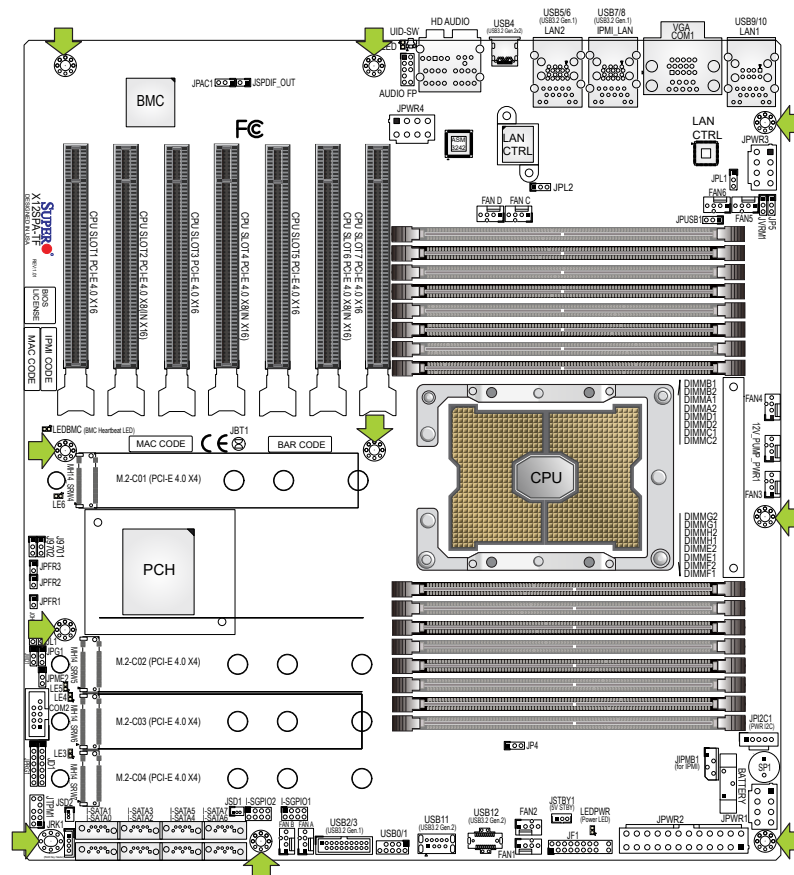
**Phillips
Screwdriver
(1)**



**Phillips Screws
(10)**



**Standoffs (10)
Only if Needed**



Location of Mounting Holes

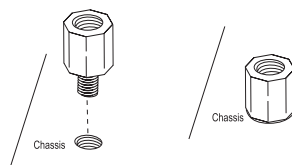
Note 1: To avoid damaging the motherboard and its components, please do not use a force greater than 8 lbf-in on each mounting screw during motherboard installation.

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

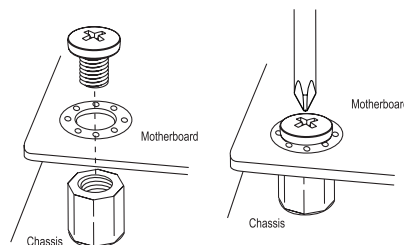
Installing the Motherboard

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


2. Locate the mounting holes on the motherboard. See the previous page for the location.



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



4. Install standoffs in the chassis as needed.
5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
6. Using the Phillips screwdriver, 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 X12SPA-TF supports up to 1 TB of ECC RDIMM, 4 TB of 3DS RDIMM, 2 TB of LRDIMM, 4 TB of 3DS LRDIMM, and 4 TB of Intel Optane Persistent Memory (PMem) 200 Series with speeds of up to 3200 MHz (2DPC) in 16 DDR4 (288-pin) SMD DIMM slots.



Note 1: Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.

Note 2: Memory speed support depends on the processors used in the system.


DDR4 Memory Support for the 3rd Gen. Intel Xeon Scalable Processors

DDR4 Memory Support for the 3rd Gen. Intel Xeon Scalable Processors					
Type	Ranks Per DIMM & Data Width	DIMM Capacity (GB)		Speed (MT/s); Voltage (V); Slots Per Channel (SPC) and DIMMs Per Channel (DPC)	
				1DPC (1-DIMM Per Channel)	2DPC (2-DIMM Per Channel)
		8Gb	16Gb	1.2 V	1.2 V
RDIMM	SRx8	8GB	16GB	3200	3200
	SRx4	16GB	32GB		
	DRx8	16GB	32GB		
	DRx4	32GB	64GB		
RDIMM 3Ds	(4R/8R) X4	2H- 64 GB 4H-128 GB	2H- 128 GB 4H-256 GB		
LRDIMM	QRx4	64GB	128GB	3200	3200
LRDIMM - 3Ds	(4R/8R) X4	4H-128 GB	2H- 128 GB 4H-256 GB	3200	3200

Memory Population Table for the 3rd Gen. Intel Xeon Scalable Processors

Memory Population Table (with 16 Slots)	
<i>When 1 CPU is used:</i>	<i>Memory Population Sequence</i>
1 CPU & 1 DIMM	CPU1: P1-DIMMA1
1 CPU & 2 DIMMs	CPU1: P1-DIMMA1/P1-DIMME1
1 CPU & 4 DIMMs	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1
1 CPU & 6 DIMMs	CPU1: P1-DIMMA1/P1-DIMMB1/P1-DIMME1/P1-DIMMF1/P1-DIMMC1/P1-DIMMG1
1 CPU & 8 DIMMs	CPU1: P1-DIMMA1/P1-DIMMB1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMC1/P1-DIMMG1/P1-DIMMH1
1 CPU & 12 DIMMs	CPU1: P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMME1/P1-DIMME2/ P1-DIMMF1/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1
1 CPU & 16 DIMMs	CPU1: P1-DIMMA1/P1-DIMMA2/P1-DIMMB1/P1-DIMMB2/P1-DIMMC1/P1-DIMMC2/P1-DIMMD1/P1-DIMMD2/ P1-DIMME1/P1-DIMME2/P1-DIMMF1/P1-DIMMF2/P1-DIMMG1/P1-DIMMG2/P1-DIMMH1/P1-DIMMH2

Intel Optane PMem 200 Series Memory Population Table (with 16 Slots)

 **Note:** The Intel Optane PMem 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.

Intel Optane PMem 200 Series Population Table (16-DIMM, within 1 CPU Socket)																		
DDR4+ Pmem	Mode	AD Interleave	P1-DIMMF1	P1-DIMMF2	P1-DIMME1	P1-DIMME2	P1-DIMMH1	P1-DIMMH2	P1-DIMMG1	P1-DIMMG2	P1-DIMMC2	P1-DIMMC1	P1-DIMMD2	P1-DIMMD1	P1-DIMMA2	P1-DIMMA1	P1-DIMMB2	P1-DIMMB1
4+4	AD MM	One - x4	PMem	-	DDR4	-	PMem	-	DDR4	-	-	DDR4	-	PMem	-	DDR4	-	PMem
		One - x4	DDR4	-	PMem	-	DDR4	-	PMem	-	-	PMem	-	DDR4	-	PMem	-	DDR4
6+1	AD	One - x1	DDR4	-	DDR4	-	-	-	DDR4	-	-	DDR4	-	DDR4	-	PMem	-	DDR4
			-	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	DDR4	-	PMem
			DDR4	-	DDR4	-	PMem	-	DDR4	-	-	DDR4	-	-	-	DDR4	-	DDR4
			PMem	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	DDR4	-	-
			DDR4	-	DDR4	-	DDR4	-	-	-	-	PMem	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	-	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	PMem	-	DDR4
			DDR4	-	DDR4	-	DDR4	-	PMem	-	-	-	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	PMem	-	DDR4	-	DDR4	-	-	-	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	PMem	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	-	-	DDR4
8+1	AD	One - x1	DDR4	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	PMem	DDR4	-	DDR4
			DDR4	-	DDR4	-	DDR4	-	DDR4	-	PMem	DDR4	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	DDR4	PMem	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	DDR4	-	DDR4	-	DDR4	PMem	-	DDR4	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	PMem	DDR4	-	DDR4	-	DDR4
			DDR4	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	DDR4	PMem	DDR4
			DDR4	PMem	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	DDR4	-	DDR4
			DDR4	-	DDR4	-	DDR4	PMem	DDR4	-	-	DDR4	-	DDR4	-	DDR4	-	DDR4
8+4	AD MM	One - x4	DDR4	-	DDR4	PMem	DDR4	-	DDR4	PMem	PMem	DDR4	-	DDR4	PMem	DDR4	-	DDR4
		Two - x2	DDR4	-	DDR4	PMem	DDR4	PMem	DDR4	-	-	DDR4	PMem	DDR4	PMem	DDR4	-	DDR4
		Two - x2	DDR4	PMem	DDR4	-	DDR4	-	DDR4	PMem	PMem	DDR4	-	DDR4	-	DDR4	PMem	DDR4
		One - x4	DDR4	PMem	DDR4	-	DDR4	PMem	DDR4	-	-	DDR4	PMem	DDR4	-	DDR4	PMem	DDR4
8+8	AD, MM,	One - x8	DDR4	PMem	DDR4	PMem	DDR4	PMem	DDR4	PMem	PMem	DDR4	PMem	DDR4	PMem	DDR4	PMem	DDR4
12+2	AD	One - x2	DDR4	-	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	-	PMem	
			DDR4	DDR4	DDR4	DDR4	PMem	-	DDR4	DDR4	DDR4	DDR4	-	PMem	DDR4	DDR4	DDR4	DDR4
			DDR4	DDR4	PMem	-	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	-	PMem	DDR4	DDR4	DDR4

Legend (for the table above)	
DDR4 Type and Capacity	
DDR4	See Validation Matrix (DDR4 DIMMs validated with PMem)
Capacity	
PMem	Any Capacity (Uniformly for all channels for a given configuration)

- Mode definitions: AD = App Direct Mode, MM = Memory Mode.
- No mixing of PMem and NVDIMMs within the platform.
- For MM, NM/FM ratio is between 1:4 and 1:16. (NM = Near Memory (DRAM); FM = Far Memory (PMem)).
- Matrix targets configs for optimized PMem to DRAM cache ratio in MM mode.
- For each individual population, different PMem rearrangements among channels are permitted so long as the configuration doesn't break X12DP Memory population rules.
- Ensure the same DDR4 DIMM type and capacity are used for each DDR4 + PMem population.
- If the system detects an unvalidated configuration, then the system issues a BIOS warning. The CLI functionality is limited in non-POR configurations, and select commands will not be supported.

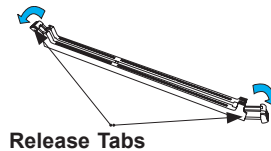
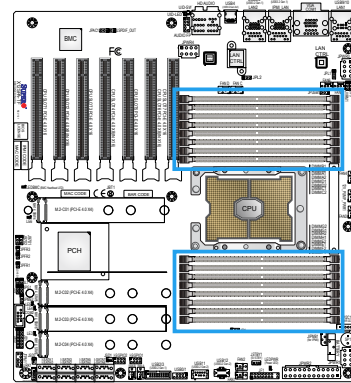
(Continued to next page)

(Continued from previous page)

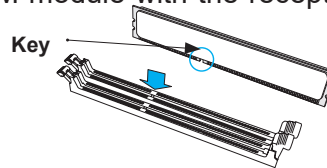
Validation Matrix (DDR4 DIMMS with PMem 200 Series)			
DIMM Type	Ranks Per DIMM & Data Width (Stack)	DIMM Capacity (GB)	
		DRAM Density	
		8Gb	16Gb
RDIMM (up to 3200)	1Rx8	N/A	N/A
	1Rx4	16GB	32GB
	1Rx8	16GB	32GB
	1Rx4	32GB	64GB
RDIMM 3DS (up to 3200)	4Rx4 (2H)	N/A	128GB
	8Rx4 (4H)	NA	256GB
LRDIMM (up to 3200)	4Rx4	64GB	128GB
LRDIMM 3DS (up to 3200)	4Rx4 (2H)	N/A	N/A
	8Rx4 (4H)	128GB	256GB

DIMM Installation

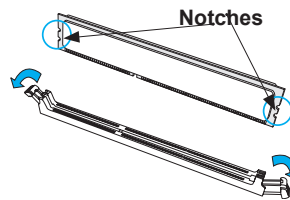
1. Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population tables in the previous section. Locate DIMM memory slots on the motherboard as shown on the right.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.



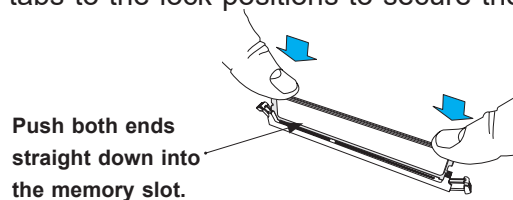
3. Align the key of the DIMM module with the receptive point on the memory slot.



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

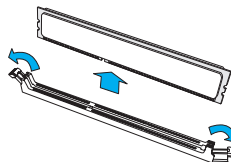


5. Push both ends of the module straight down into the slot until the module snaps into place.
6. Press the release tabs to the lock positions to secure the DIMM module into the slot.



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.



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

2.5 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.

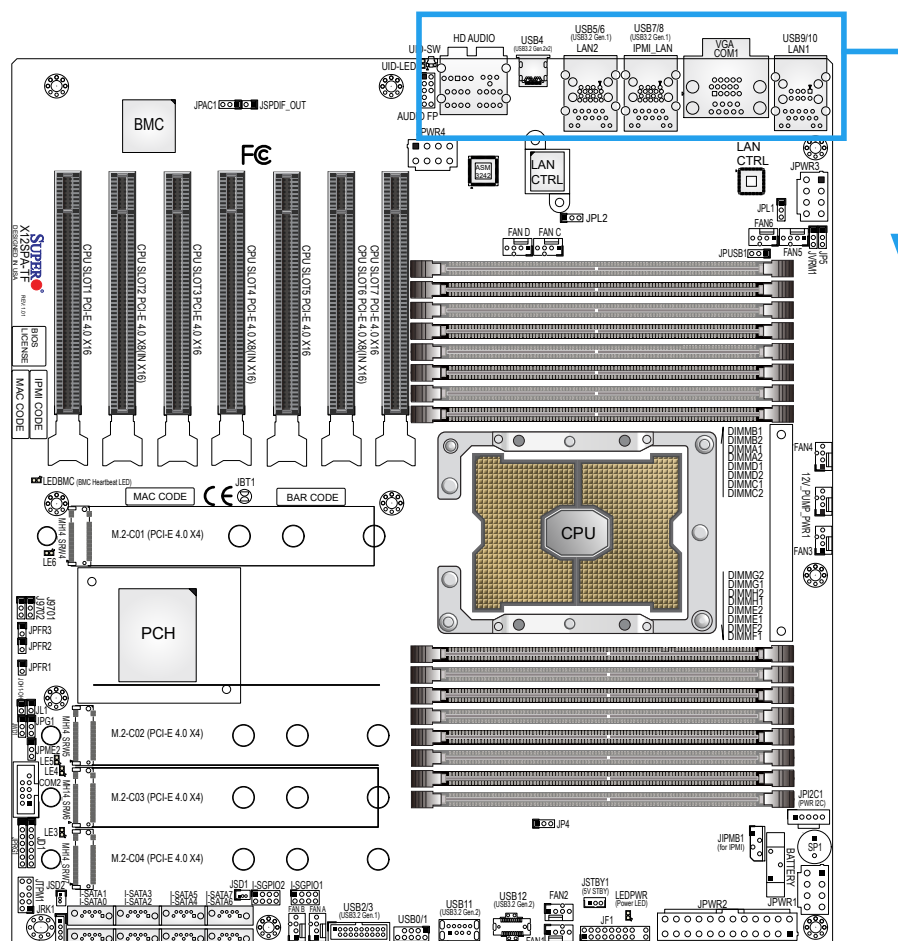
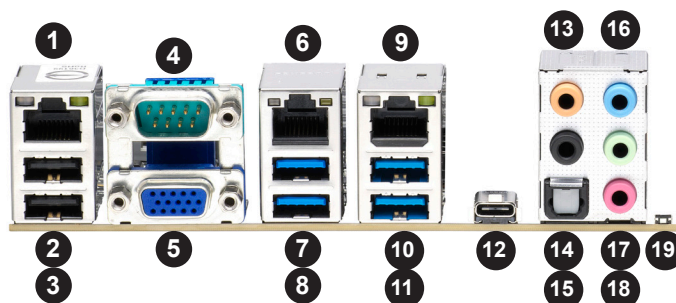


Figure 2-1. I/O Port Locations and Definitions



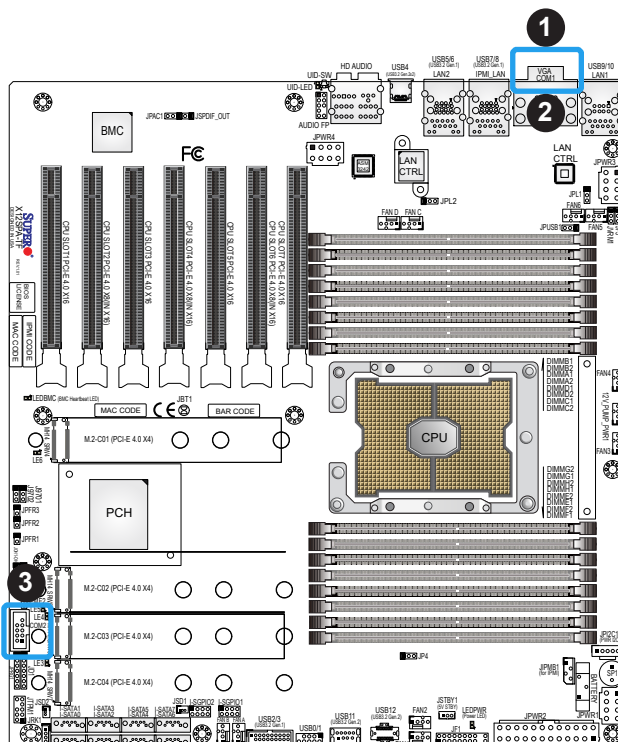
Rear I/O Ports							
#	Description	#	Description	#	Description	#	Description
1	LAN1 (1Gb)	6	Dedicated IPMI LAN	11	USB6 (3.2 Gen. 1)	16	Line In
2	USB9 (2.0)	7	USB7 (3.2 Gen. 1)	12	USB4 (3.2 Gen. 2x2)	17	Line Out
3	USB10 (2.0)	8	USB8 (3.2 Gen. 1)	13	Center/LFE Out	18	Mic In
4	COM1 Port	9	LAN2 (10Gb)	14	Surround Out	19	UID Switch / BMC
5	VGA Port	10	USB5 (3.2 Gen. 1)	15	S/PDIF Out		Reset Button

VGA Connection

One VGA port (VGA) is located on the rear I/O panel. The VGA connection provide analog interface support between the computer and the video displays. Refer to the layout below for the location of VGA port.

COM Port/Header

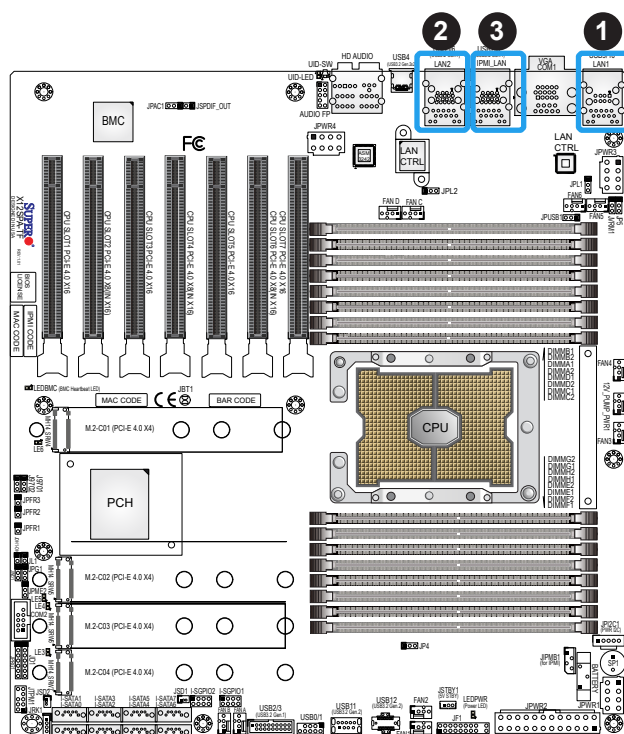
One COM port (COM1) and one COM header (COM2) that support serial link interface are on the motherboard. COM1 is located on the rear I/O panel. COM2 is located next to JD1. Refer to the layout below for the locations of COM1 and COM2.



1. VGA
2. COM1
3. COM2

LAN Ports (LAN1/LAN2 and IPMI LAN)

Two Ethernet LAN ports (LAN1, LAN2) and a dedicated IPMI LAN port (IPMI_LAN) are located on the rear I/O panel. LAN1 supports 1 GbE LAN connections (via the Intel i210AT LAN controller). LAN2 supports 10 GbE LAN connections (via the Aquantia AQC113 LAN controller). The dedicated IPMI LAN port, located above the USB7/8 ports on the rear I/O panel, provides LAN support for the BMC (Baseboard Management Controller). All of these LAN ports accept RJ45 cables. Please refer to the LED Indicator section ([Section 2.9](#)) for LAN LED information.



1. LAN1
2. LAN2
3. IPMI LAN



Universal Serial Bus (USB) Ports and Headers

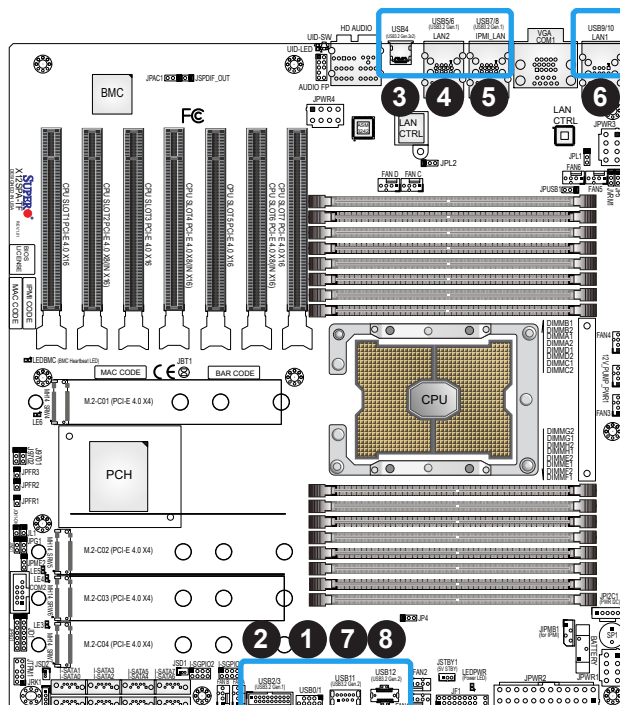
There are four USB 3.2 Gen. 1 ports (USB5, USB6, USB7, USB8) located on the rear I/O panel, and one USB 3.2 Gen. 1 header (USB2/3) located on the motherboard to provide front USB access. One USB 3.2 Gen. 2x2 port (USB4) is located on the rear I/O panel. The 10-pin black USB header supports two USB 2.0 connections (USB0/1), and two USB 2.0 ports (USB9, USB10) are located on the rear I/O panel. The motherboard also provides one front accessible Type-A USB 3.2 Gen. 2 port (USB11) and one USB 3.2 Gen. 2 header (USB12). These USB ports and headers can be used for USB support via USB cables (not included).

Front Panel USB 2.0 Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	+5V	2	+5V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	Ground	8	Ground
9	Key	10	NC

Type-A USB 3.2 Gen. 2 (USB11) Pin Definitions			
Pin#	Definition	Pin#	Definition
1	VBUS	5	SSRX-
2	USB_N	6	SSRX+
3	USB_P	7	GND
4	Ground	8	SSTX-
		9	SSTX+

Front Panel USB 3.2 Gen. 1 Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	VBUS	19	Power
2	StdA_SSRX-	18	USB3_RN
3	StdA_SSRX+	17	USB3_RP
4	GND	16	GND
5	StdA_SSTX-	15	USB3_TN
6	StdA_SSTX+	14	USB3_TP
7	GND	13	GND
8	D-	12	USB_N
9	D+	11	USB_P
10		x	

Front Panel USB 3.2 Gen. 2 (USB12) Pin Definitions							
Pin#	Definition	Pin#	Definition	Pin#	Definition	Pin#	Definition
1	VBUS	5	RX1+	9	NC	13	TX2-
2	TX1+	6	RX1-	10	NC	14	GND
3	TX1-	7	VBUS	11	VBUS	15	RX2+
4	GND	8	CC1	12	TX2+	16	RX2-
						17	GND
						18	D-
						19	D+
						20	CC2



1. Front Access USB0/1 (2.0)
2. Front Access USB2/3 (3.2 Gen. 1)
3. Rear I/O Panel USB4 (3.2 Gen. 2x2)
4. Rear I/O Panel USB5/6 (3.2 Gen. 1)
5. Rear I/O Panel USB7/8 (3.2 Gen. 1)
6. Rear I/O Panel USB9/10 (2.0)
7. Front Access Type-A USB11 Port (3.2 Gen. 2)
8. Front Access USB12 (3.2 Gen. 2)

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

A UID / BMC Reset switch (UID-SW) 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, UID-SW will trigger a cold reboot when the user presses and holds the switch for six seconds. It will also restore the BMC to the manufacturer's default when the user presses and holds the switch for 12 seconds.

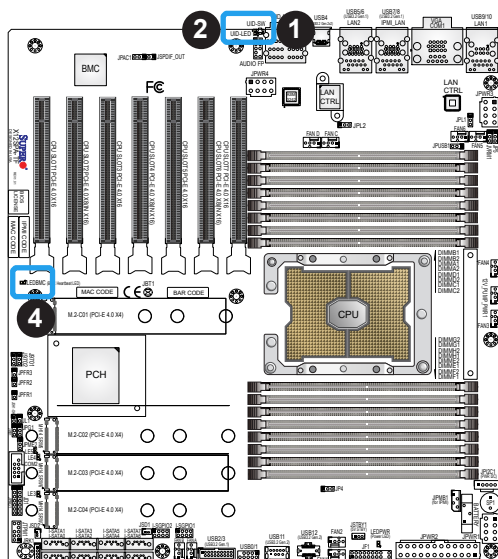
When functioning as a UID LED switch, UID-SW will turn both rear UID LED (UID-LED) and front UID LED (Pin 7/Pin 8 of JF1) on and off when the user presses the switch on/off.

To achieve these dual purposes, the UID LED/BMC Reset switch works in conjunction with the BMC Heartbeat LED (LEDBMC) and front/rear UID LEDs. Please 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 <http://www.supermicro.com> for more information on BMC.

UID/BMC Reset Switch (UID-SW) Features & Settings					
When Used as a UID LED Switch			When Used as a BMC Reset Switch		
Work w/Rear UID LED (UID-LED) & Front UID LED (JF1: Pins 7 & 8)			Work with BMC Heartbeat LED (LEDBMC)		
Rear UID LED	UID-LED	Blue: Unit identified	BMC Heartbeat LED	LEDBMC	Green Blinking: BMC Normal
Front UID LED	Pins 7 & 8 (JF1)	Blue: Unit identified	BMC Reset: Press & hold the switch (UID-SW) 6 seconds	LEDBMC: Solid green: during reboot	Triggering a cold reboot; LED: solid green on during cold reboot
Press the switch (UID-SW) to turn on and off both rear and front UID LED indicators.			BMC Reset: Press & hold the switch (UID-SW) 12 seconds	LEDBMC: Solid green: during BMC reset	BMC: Reset to the manufacturer's default; LED solid on during BMC Reset

UID/BMC Reset Switch (UID-SW) Pin Definitions	
Pin#	Definition
1	Ground
2	Ground
3	Button In
4	Button In

JF1		
1	2	
Power Button	Ground	
Reset Button	Ground	
3.3V	Power Fail (for LED6)	
3 (Blue LED_Cathode_UID)	Red+ (Blue LED_Cathode_UID)	Blue+ (Red OH/Fan Fail/PWR Fail for LED5/Blue UID LED)
P3V3_STBY	NIC2 Active LED	
P3V3_STBY	NIC1 Active LED	
ID_UID/3.3V Stby	HDD LED	
3.3V	FP PWR LED	
Key	Key	
NMI	Ground	
19	20	

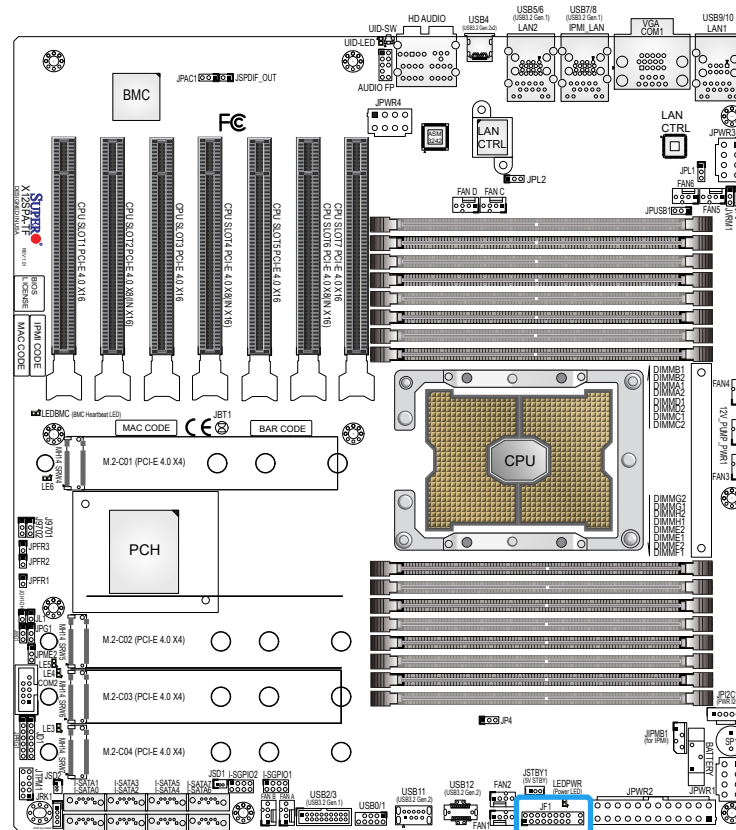


1. UID Switch / BMC Reset
2. Rear UID LED (UID-LED)
3. Front UID LED
4. BMC Heartbeat LED (LEDBMC)



2.6 Front Control Panel

The front control panel header (JF1) contains header pins for various buttons and indicators that are normally located on a control panel at the front of the chassis. These connectors are designed specifically for use with Supermicro chassis. Refer to the figure below for the descriptions of the front control panel buttons and LED indicators.























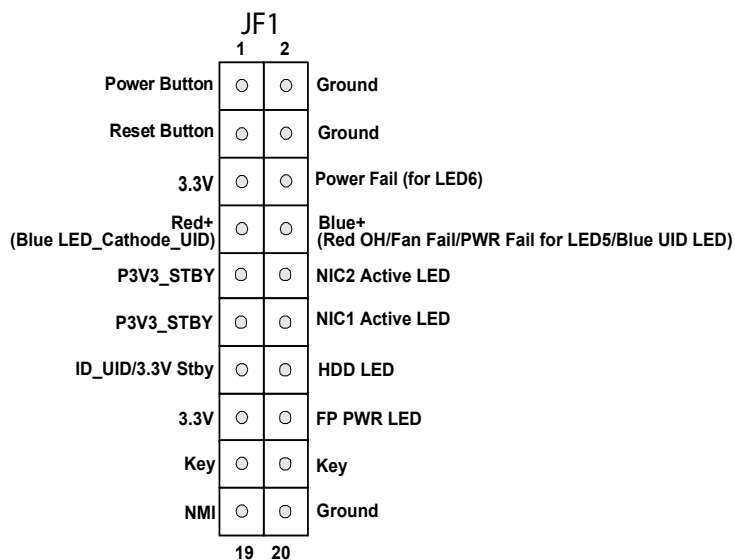
JF1		1	2
Power Button			Ground
Reset Button			Ground
3.3V			Power Fail (for LED6)
Red+ (Blue LED_Cathode_UID)			Blue+ (Red OH/Fan Fail/PWR Fail for LED5/Blue UID LED)
P3V3_STBY			NIC2 Active LED
P3V3_STBY			NIC1 Active LED
ID_UID/3.3V Stby			HDD LED
3.3V			FP PWR LED
Key			Key
NMI			Ground
		19	20

Figure 2-2. JF1 Header Pins

Front Control Panel LEDs



Front Control Panel (JF1) LED Indicators						
Event	Power (LED1)	HDD (LED2)	LAN (LED3/4)	UID (LED5)	Information (LED5)	Power Fail (LED6)
Power On	Solid On					
HDD Activity		Blinking				
NIC Activity			Blinking			
Overheat					Solid On	
Fan Fail					Blinking @1Hz	
Power Fail					Blinking @1/4Hz	Solid On
Local UID On				Solid On		
Remote UID On				Blinking 1Hz		
Checking	BMC/BIOS Blinking @4HZ					
Recovering/Updating	BMC Blinking @4HZ BMC 2 Blinks @4Hz, 1 Pause @2Hz (on-on-off-off)			BIOS/BMC Blinking @10Hz		
Flash Not Detected or Golden Image Check Failed	BMC/BIOS Blinking @1HZ					
CPLD Recovery Mode				Blinking @10Hz (MB UID LED)	Blinking @10Hz (FP Red LED)	

Power On & BMC/BIOS Status LED Button

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

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

Power Button Pin Definitions (Pin 1 & Pin 2 of JF1)	
Status	Event
Green: solid on	System power on
BMC/BIOS blinking green @ 4Hz	BMC/BIOS checking
BIOS blinking green @ 4Hz	BIOS recovery/update in progress
BMC blinking red x2 (2 blinks red) @ 4Hz, 1 pause @ 2Hz (on-on-off-off)	BMC recovery/update in progress
BMC/BIOS blinking green @ 1Hz	Flash not detected or golden image checking failure

Reset Button

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

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

JF1			
	1	2	
1 Power Button	○	○	Ground
2 Reset Button	○	○	Ground
3.3V	○	○	Power Fail (for LED6)
Red+ (Blue LED_Cathode_UID)	○	○	Blue+ (Red OH/Fan Fail/PWR Fail for LED5/Blue UID LED)
P3V3_STBY	○	○	NIC2 Active LED
P3V3_STBY	○	○	NIC1 Active LED
ID_UID/3.3V Stby	○	○	HDD LED
3.3V	○	○	FP PWR LED
Key	○	○	Key
NMI	○	○	Ground
	19	20	

1. PWR Button
2. Reset Button

Power Fail LED

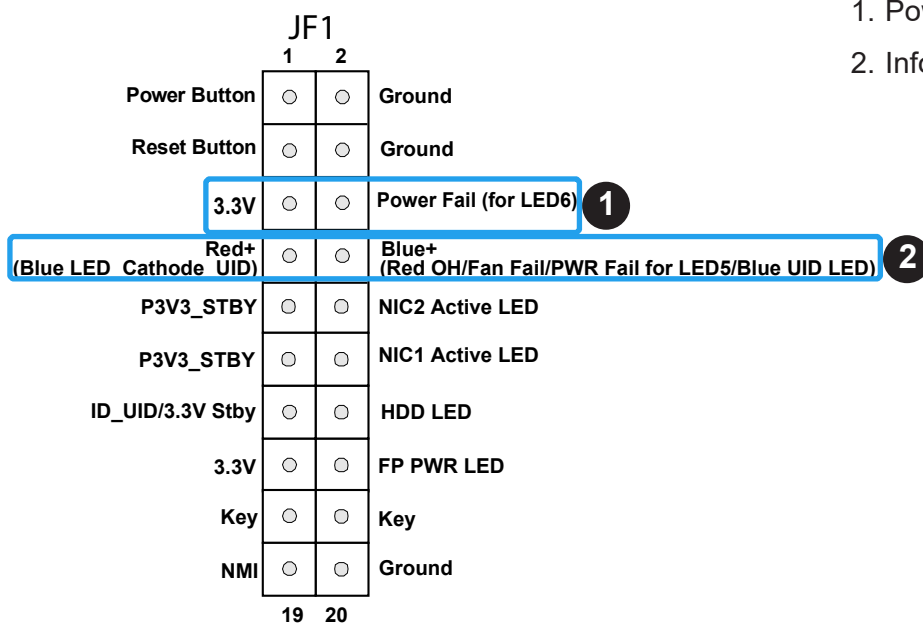
The Power Fail LED connection is located on pins 5 and 6 of JF1. When this LED turns solid red, it indicates a power failure. Refer to the table below for pin definitions.

Power Fail LED Pin Definitions (JF1)	
Pin#	Definition
5	3.3V
6	PWR Fail for LED6 (Solid red on: PWR failure)

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

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

Information LED-Blue+ (OH/Fan Fail/PWR Fail LED for LED5/blue UID LED) Pin Definitions (Pin 7 & Pin 8 of JF1)	
Status	Description
Solid red (on)	An overheat condition has occurred.
Blinking red (1Hz)	Fan failure: check for an inoperative fan.
Blinking red (0.25Hz)	Power failure: check for a non-operational power supply
Blinking red (10Hz) (FP red LED)	CPLD recovery mode error(s)
Solid blue	Local UID is activated. Use this function to locate a unit in a rack mount environment that might be in need of service.
Blinking blue (1Hz)	Remote UID is on. Use this function to identify a unit from a remote location that might be in need of service.
BIOS/BMC blinking blue (10Hz)	BIOS/BMC: recovery and/or update in progress
Red Info LED blinking (10Hz) and MB UID LED blue blinking (10Hz)	CPLD: recovery and/or update in progress



1. Power Fail LED
2. Information LED

NIC1/NIC2 (LAN1/LAN2)

The NIC (Network Interface Controller) LED connection for LAN port 1 is located on pins 11 and 12 of JF1, and LAN port 2 is on pins 9 and 10. Attach the NIC LED cables here to display network activity. Refer to the table below for pin definitions.

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

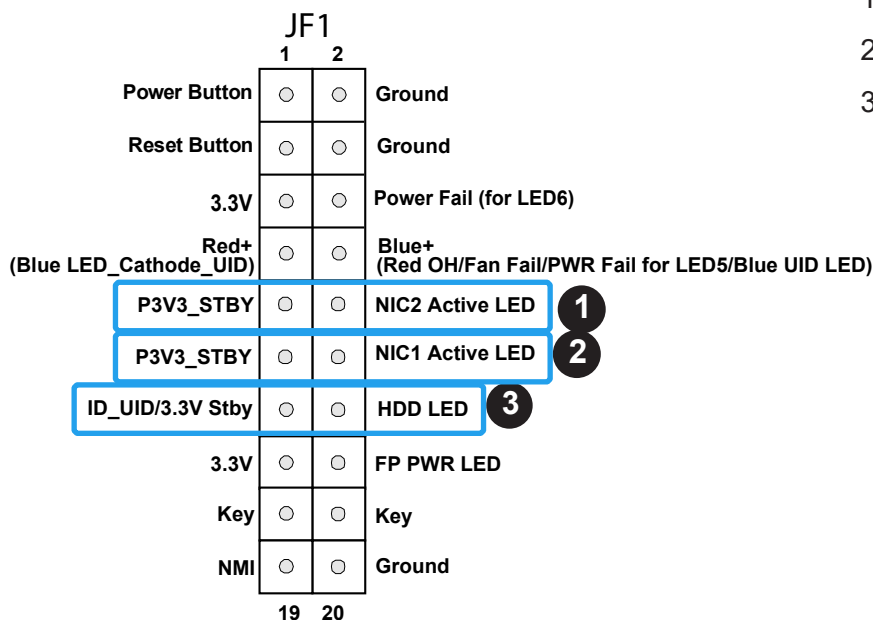
ID_UID Switch/HDD LED

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

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

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

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



1. NIC2 (LAN 2) LED
2. NIC1 (LAN 1) LED
3. ID_UID/HDD LED

FP Power LED

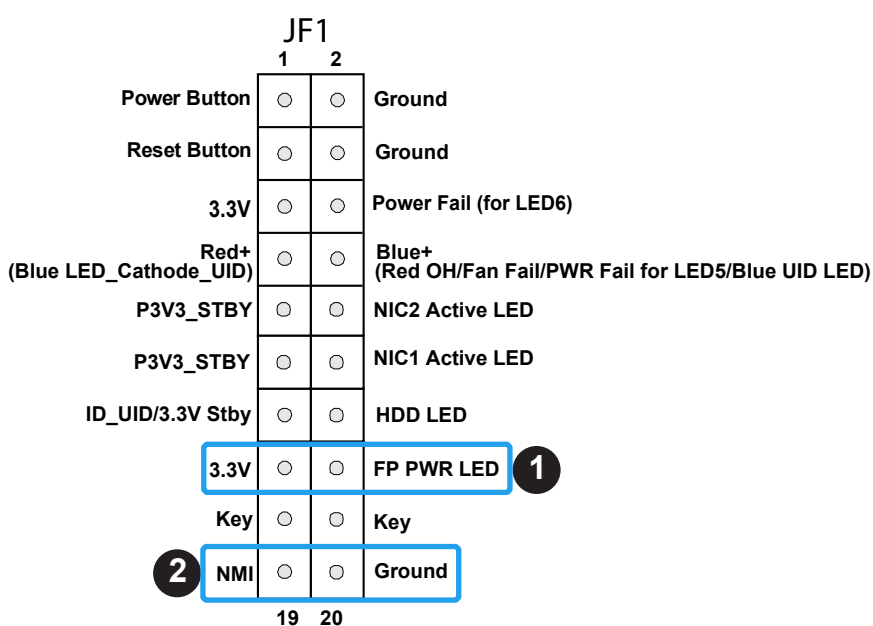
The Front Panel Power LED connection is located on pins 15 and 16 of JF1. Refer to the table below for pin definitions.

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

NMI Button

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

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



1. FP PWR LED

2. NMI

2.7 Connectors

Power Connections

ATX Power Supply Connector

The 24-pin power supply connector (JPWR2) meets the ATX SSI EPS 12V specification. You must also connect the 8-pin 12V DC power connectors (JPWR1/JPWR3/JPWR4) to the power supply to provide adequate power to your system.



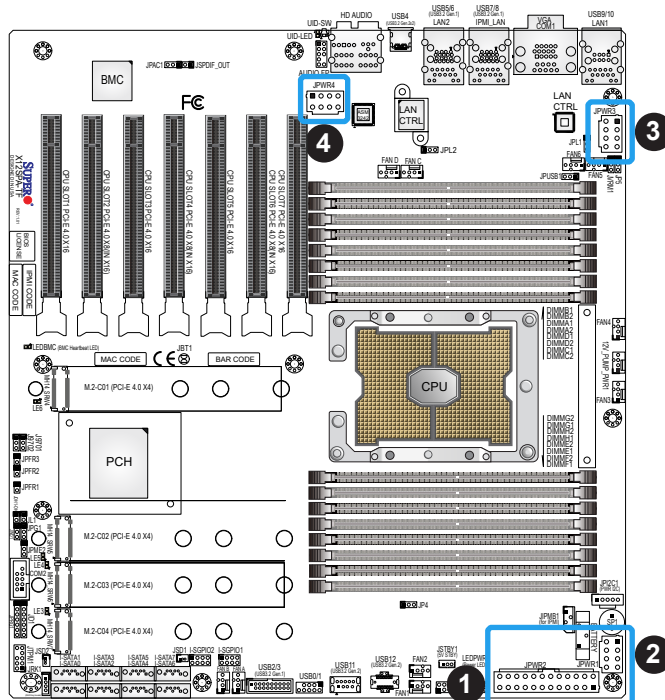
Important: To provide adequate power supply to the motherboard, be sure to connect the 24-pin ATX PWR, 8-pin PWR, and 4-pin PWR connectors to the power supply. Failure to do so may void the manufacturer warranty on your power supply and motherboard.

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

Required Connection

12V 8-pin Power Pin Definitions	
Pin#	Definition
1 - 4	Ground
5 - 8	+12V

Required Connection



1. JPWR2: 24-pin ATX PWR
2. JPWR1: 8-pin PWR
3. JPWR3: 8-pin PWR
4. JPWR4: 8-pin PWR

Headers

Fan Headers

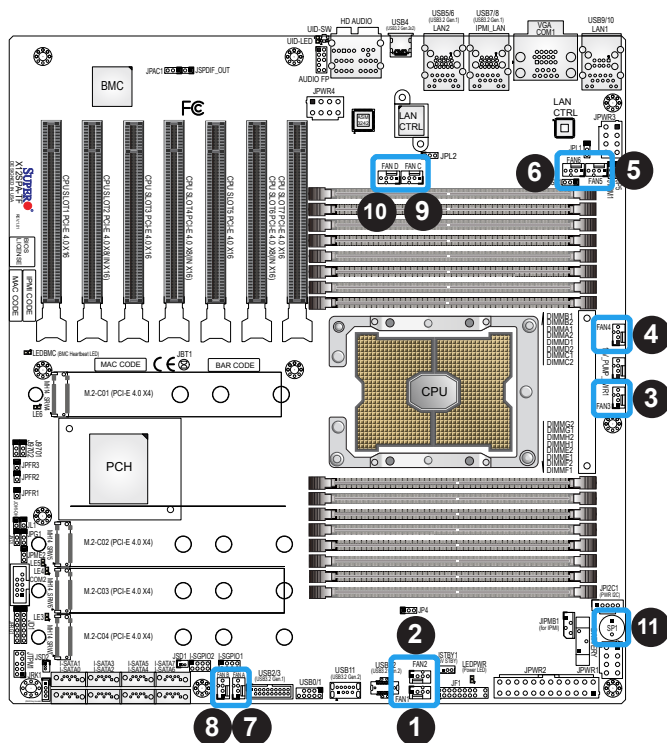
There are 10 4-pin fan headers (FAN1 - FAN6, FAN A - FAN D) on the motherboard. All these 4-pin fan headers are backwards compatible with the traditional 3-pin fans. However, fan speed control is available for 4-pin fans only by Thermal Management via the IPMI 2.0 interface. Refer to the table below for pin definitions.

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

Internal Speaker/Buzzer

The Internal Speaker/Buzzer (SP1) is used to provide audible indications for various beep codes. Refer to the table below for pin definitions.

Internal Buzzer Pin Definitions		
Pin#	Definition	
1	Pos (+)	Beep In
2	Neg (-)	Alarm Speaker



1. FAN1 (CPU Fan Header)
2. FAN2 (CPU Fan Header)
3. FAN3 (CPU Fan Header)
4. FAN4 (CPU Fan Header)
5. FAN5 (CPU Fan Header)
6. FAN6 (CPU Fan Header)
7. FAN A (System Fan Header)
8. FAN B (System Fan Header)
9. FAN C (System Fan Header)
10. FAN D (System Fan Header)
11. Internal Speaker/Buzzer

S-SGPIO Headers

The SGPIO (Serial General Purpose Input/Output) headers (I-SGPIO1, I-SGPIO2) are used to communicate with the enclosure management chip on the backplane, and to support the onboard I-SATA 3.0 ports. Refer to the table below for pin definitions.

I-SGPIO1/I-SGPIO2 Headers	
Header	Corresponded Ports
I-SGPIO1	I-SATA0 - I-SATA3
I-SGPIO2	I-SATA4 - I-SATA7

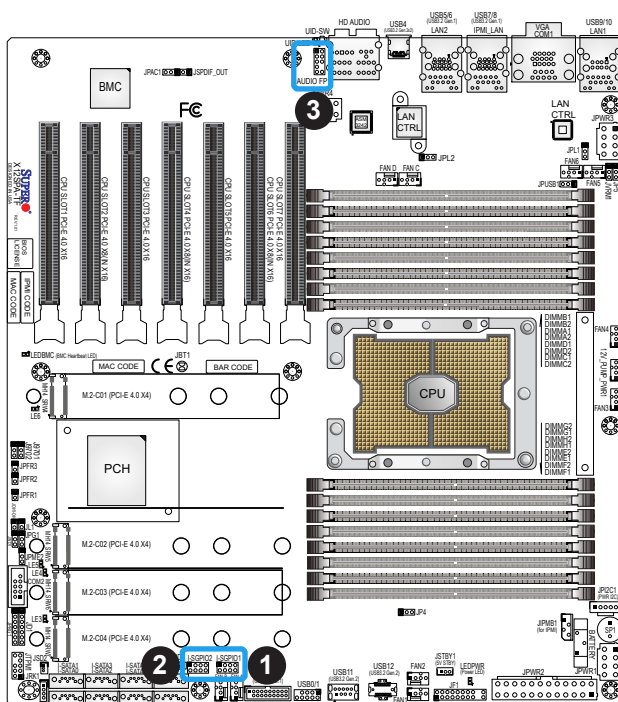
S-SGPIO Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	NC	2	NC
3	Ground	4	Data
5	Load	6	Ground
7	Clock	8	NC

NC = No Connection

Audio Front Panel Header

A 10-pin audio header (AUDIO FP) located on the motherboard allows you to use the onboard sound chip (ALC888S) for audio function. Connect an audio cable to this header to use this feature. Refer to the table below for pin definitions.

Audio Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	Microphone_Left	2	Audio_Ground
3	Microphone_Right	4	Audio_Detect
5	Line_2_Right	6	Ground
7	Jack_Detect	8	Key
9	Line_2_Left	10	Ground



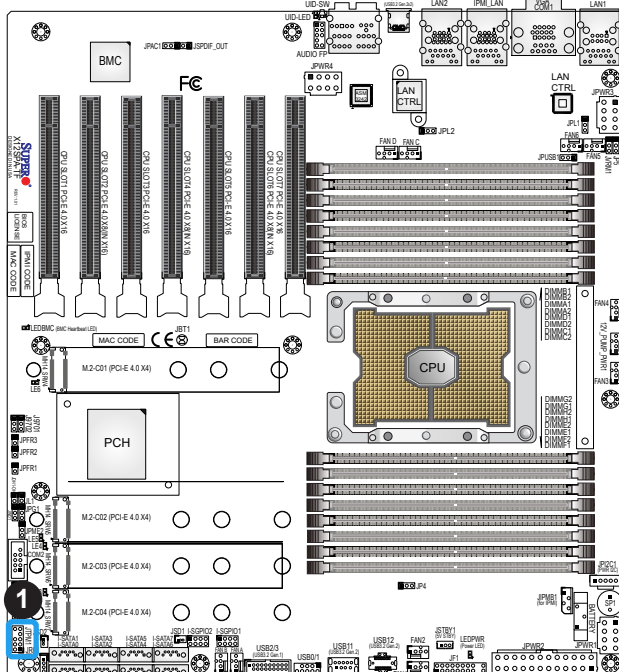
1. I-SGPIO1 Header
2. I-SGPIO2 Header
3. Audio Front Panel Header

TPM/Port 80 Header

The JTPM1 header is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from Supermicro (optional). A TPM/Port 80 header 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 header. Please go to the following link for more information on the TPM: https://www.supermicro.com/manuals/other/AOM-TPM-9670V_9670H.pdf.

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

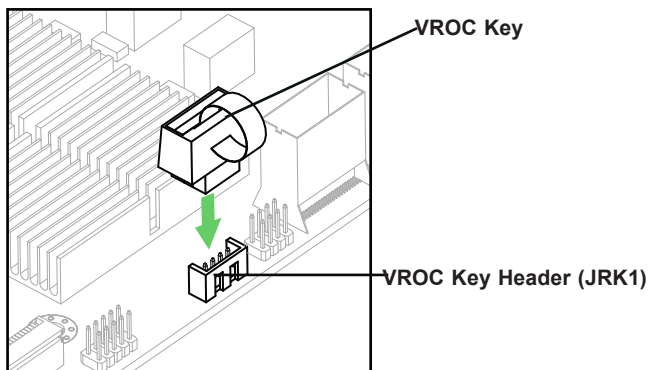
1. TPM/Port 80 Header



VROC RAID Key Header

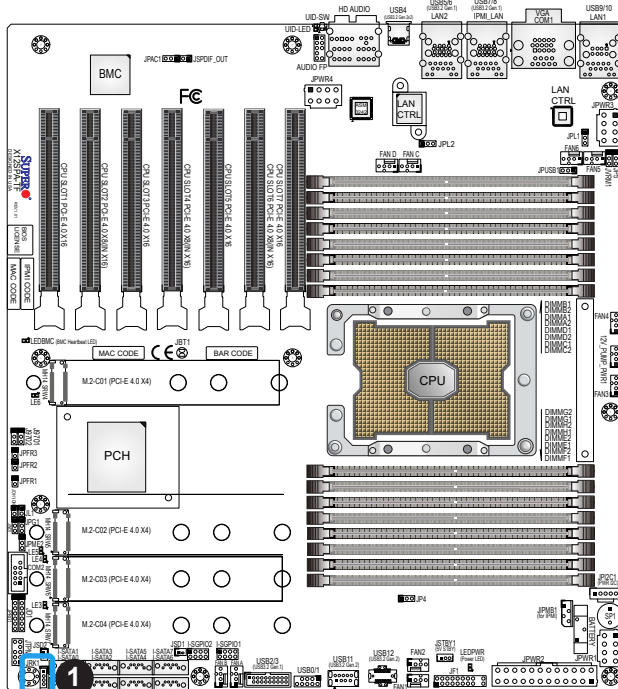
A VROC RAID Key header is located at JRK1 on the motherboard. Install a VROC RAID Key on JRK1 for NVMe RAID support as shown in the illustration below. Refer to the layout below for the location of JRK1.

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



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

1. VROC RAID Key Header (JRK1)



Standby Power

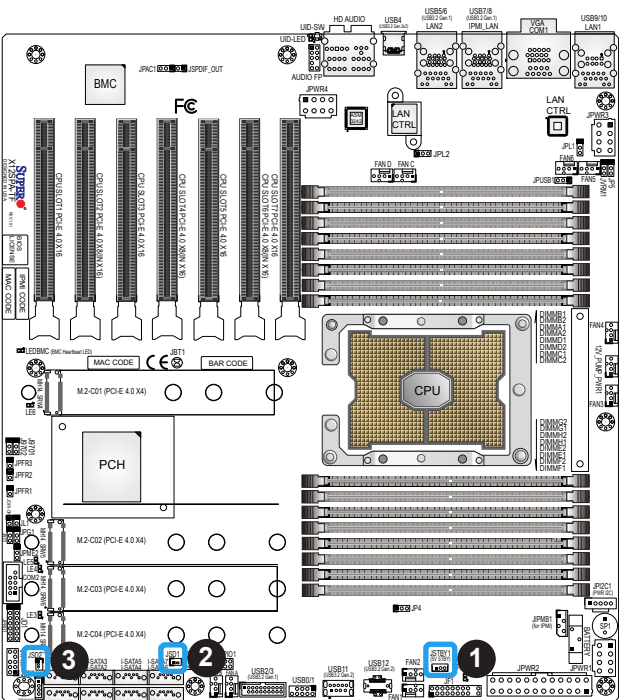
The Standby Power header is located at JSTBY1 on the motherboard. You must have a card with a Standby Power connector and a cable to use this feature. Refer to the table below for pin definitions.

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

Disk-On-Module Power Connector

The Disk-On-Module (DOM) power connectors at JSD1 and JSD2 provide 5V 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	5V
2	Ground
3	Ground



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

Power SMB (I²C) Header

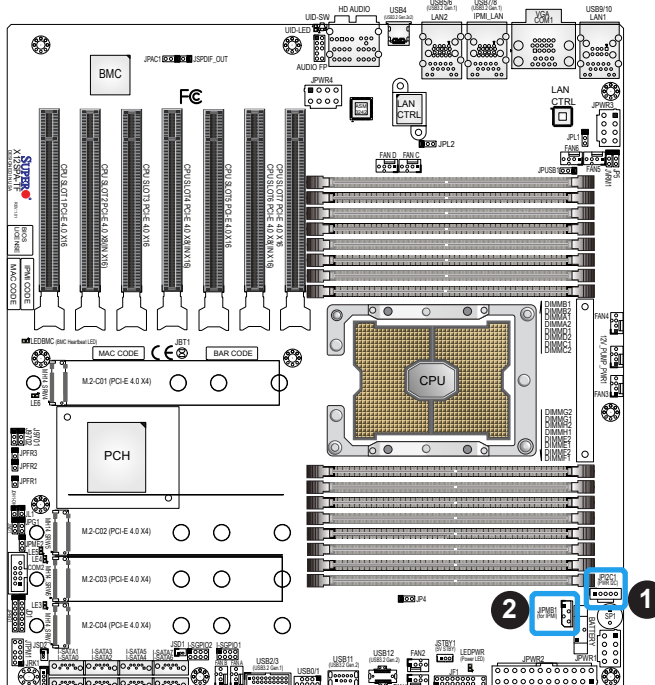
The Power System Management Bus (I²C) connector (JPI²C1) monitors the power supply, fan, and system temperatures. Refer to the table below for pin definitions.

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

4-pin BMC External I²C Header

A System Management Bus header for IPMI 2.0 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 I ² C Header Pin Definitions	
Pin#	Definition
1	Data
2	Ground
3	Clock
4	No Connection



1. Power SMB Header
2. BMC External Header

Chassis Intrusion

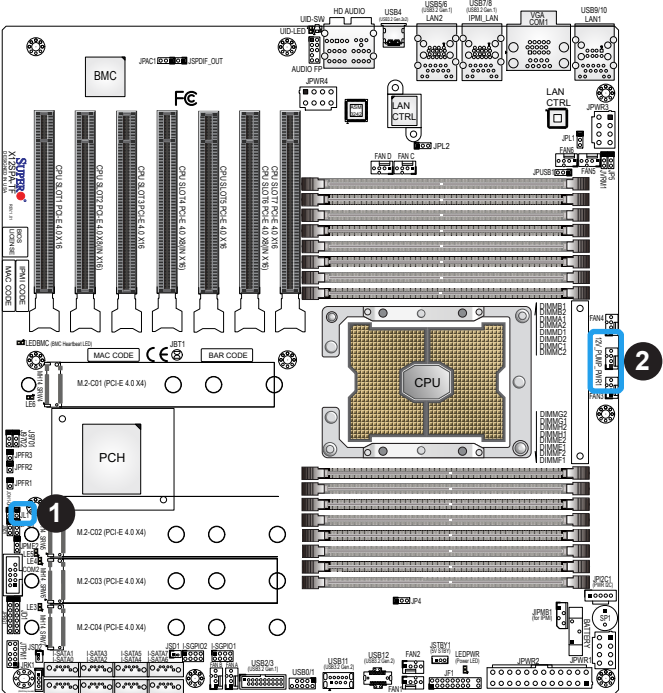
A Chassis Intrusion header is located at JL1 on the motherboard. Attach the appropriate cable from the chassis to inform you when the chassis is opened. Refer to the table below for pin definitions.

Chassis Intrusion Pin Definitions	
Pin#	Definition
1	Intrusion Input
2	Ground

Pump Power Header

The motherboard has one +12V 4-pin header for optional CPU liquid cooling systems. When using a liquid cooling system, attach the pump power cable to the 12V_PUMP_PWR1 header.

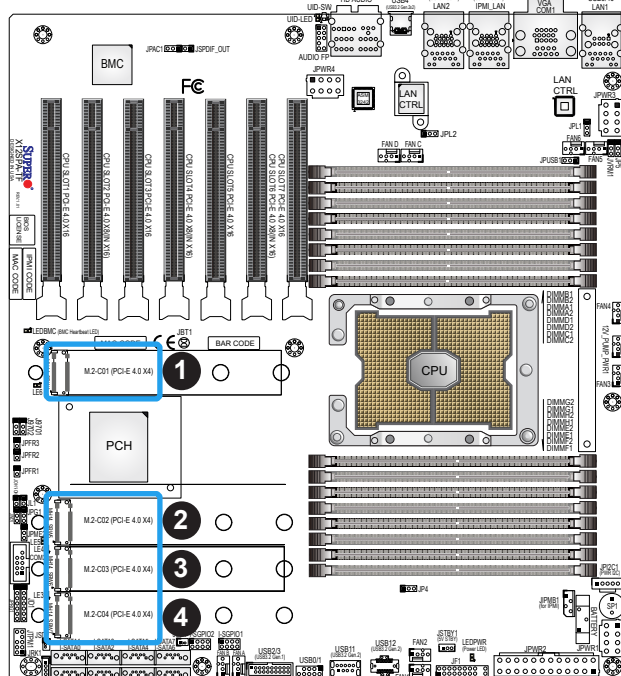
Pump Power Header Pin Definitions	
Pin#	Definition
1	Ground (Black)
2	2A/+12V (Red)
3	N/A
4	N/A



- 1. Chassis Intrusion Header
- 2. Pump Power Header (12V_PUMP_PWR1)

PCIe 4.0 M.2 Sockets

The motherboard has four PCIe 4.0 M.2 sockets (M.2-C01 - M.2-C04). M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. The M.2 slots on the motherboard support PCIe 4.0 x4 M.2 NVMe SSDs in the 2260, 2280, and 22110 form factors.



1. M.2 Socket (M.2-C01)
2. M.2 Socket (M.2-C02)
3. M.2 Socket (M.2-C03)
4. M.2 Socket (M.2-C04)

Power LED/Speaker Header

Pins 1-3 of JD1 are used for power LED indication, and pins 4-7 are for the speaker. Please note that the speaker connector pins (4-7) are used with an external speaker. If you wish to use the onboard speaker, you should close pins 6-7 with a cap. Refer to the tables below for pin definitions.

PWR LED Connector Pin Definitions	
Pin#	Signal
1	JD1_PIN1
2	FP_PWR_LED
3	FP_PWR_LED

Speaker Connector Pin Definitions	
Pin#	Signal
4	P5V
5	Key
6	R_SPKPIN_N
7	R_SPKPIN

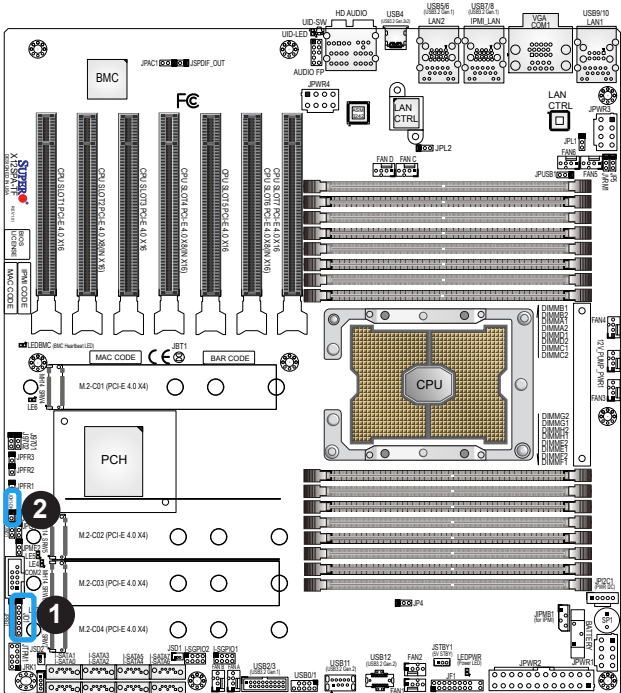
Overheat/Fan Fail LED Header

Header JOH1-OH is used to connect to an LED indicator to provide warnings of chassis overheating and fan failure. This LED will blink when a fan failure occurs. Refer to the tables below for pin definitions.

Overheat LED Header Status	
State	Definition
Solid	Overheat
Blinking	Fan Fail

Overheat LED Header Pin Definitions	
Pin#	Signal
1	Pull high to +3.3V power through 330-ohm resistor
2	OH Active

1. Power LED/Speaker Header
2. Overheat/Fan Fail LED Header



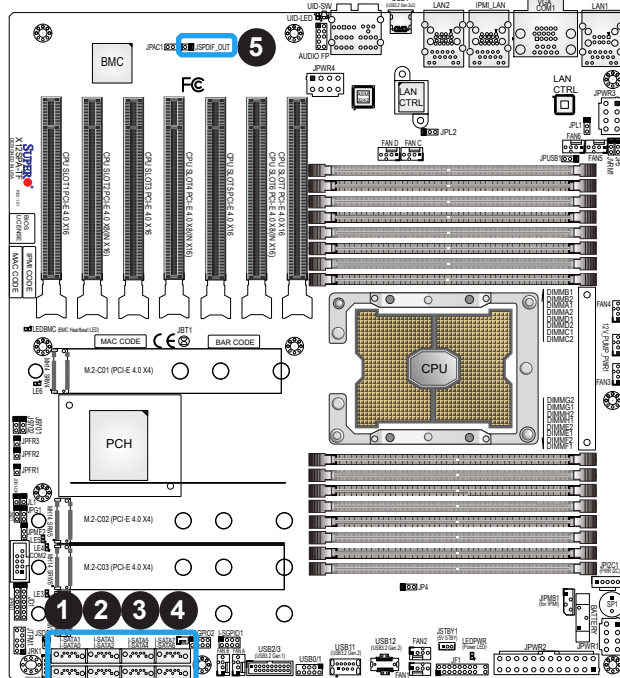
I-SATA Ports

Eight SATA 3.0 ports (I-SATA0 - I-SATA7) are located on the motherboard, which are supported by the C621 chipset. These SATA ports support RAID 0, 1, 5, and 10. SATA ports provide serial-link signal connections, which are faster than the connections of Parallel ATA.

SPDIF_IN Header

The Sony/Philips Digital Interface (JSPDIF_OUT) header is used for digital audio. Place a cap on each header for audio support. A cable is needed to use the connection.

SPDIF_In Pin Definitions	
Pin#	Definition
1	S/PDIF_In
2	Ground

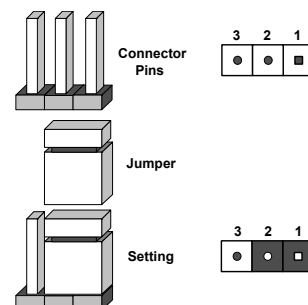


1. I-SATA0/I-SATA1
2. I-SATA2/I-SATA3
3. I-SATA4/I-SATA5
4. I-SATA6/I-SATA7
5. JSPDIF_OUT

2.8 Jumper Settings

How Jumpers Work

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



Note 1: Unplug the power cord from the power supply before adjust jumper setting.

Note 2: 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.

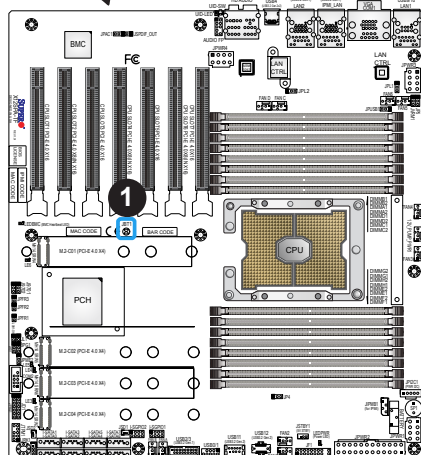
To Clear CMOS



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



Note: Clearing CMOS will also clear all passwords.



1. JBT1

LAN Port Enable/Disable

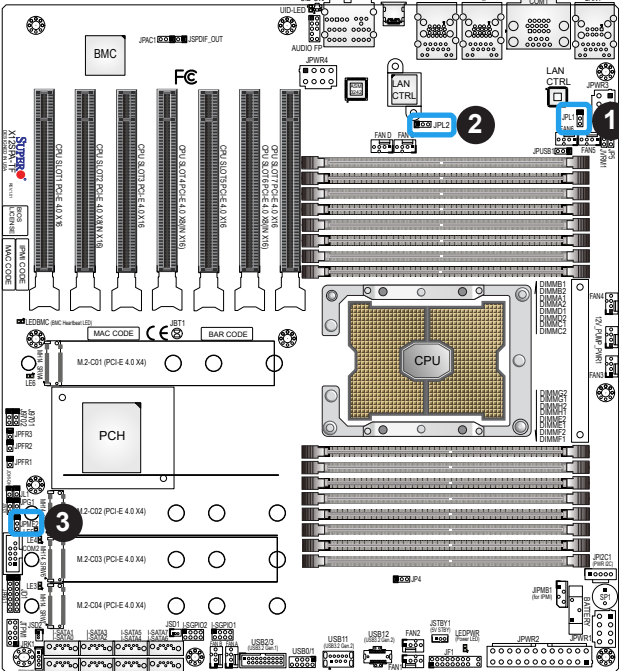
JPL1 and JPL2 allow you to enable the onboard LAN ports (LAN1 and LAN2). The default setting is pins 1-2 to enable the connections. Refer to the table below for jumper settings.

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

ME Manufacturing Mode

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 jumper settings.

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



- 1. LAN1 Enable/Disable (JPL1)
- 2. LAN2 Enable/Disable (JPL2)
- 3. ME Manufacturing Mode (JPME2)

HD Audio Enable

JPAC1 allows you to enable or disable the onboard high definition audio support. The default position is on pins 1-2 to enable onboard audio connections. Refer to the table below for jumper settings.

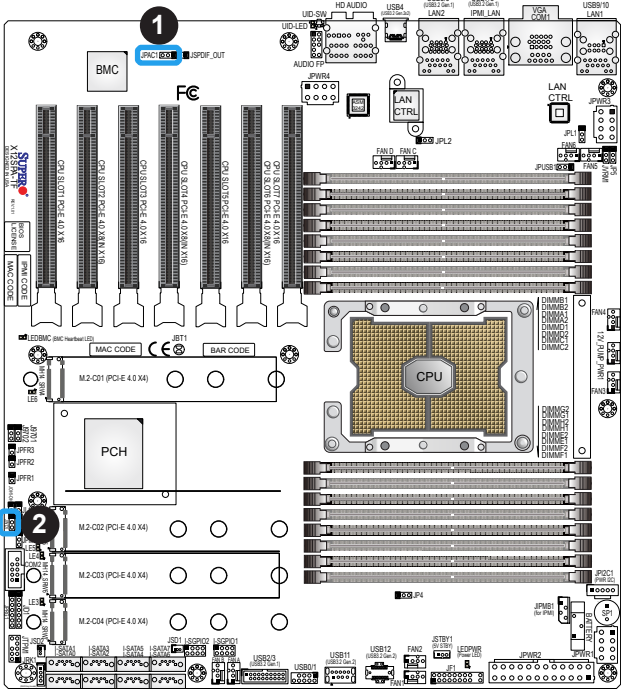
Audio Enable/Disable Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Enabled (Default)
Pins 2-3	Disabled

Watchdog

Watchdog (JWD1) is a system monitor that can reboot the system when a software application hangs. Close pins 1-2 to reset the system if an application hangs. Close pins 2-3 to generate a non-maskable interrupt (NMI) signal for the application that hangs. Refer to the table below for jumper settings. For this function to work properly, please also enable the Watchdog setting in the BIOS.

Watchdog Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Reset
Pins 2-3	NMI
Open	Disabled

- 1. HD Audio Enable/Disable
- 2. Watchdog




VGA Enable/Disable

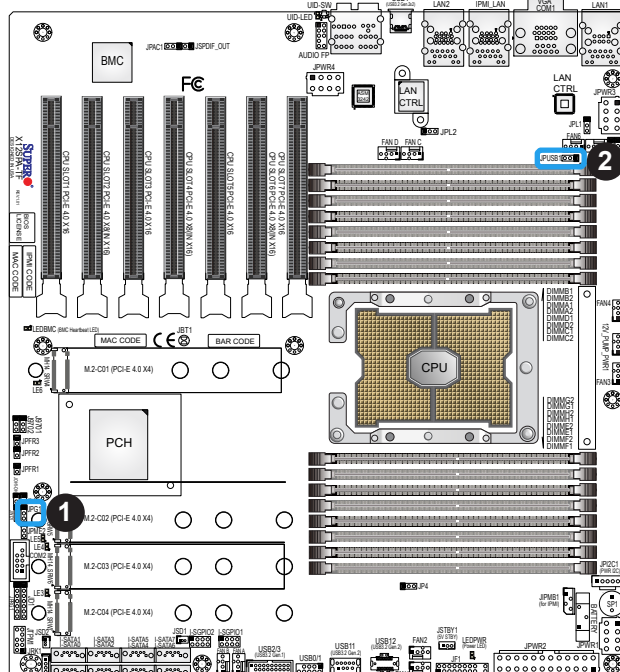
JPG1 allows you to enable the onboard VGA connector. The default setting is pins 1-2 to enable the connection. Refer to the table below for jumper settings.

VGA Enable/Disable Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Enabled (Default)
Pins 2-3	Disabled

USB (USB7/8) Wake-Up

This jumper allows you to "wake up" the system by pressing a key on the USB keyboard or by clicking the USB mouse of your system. JPUSEB1 is used together with the USB Wake-Up feature in BIOS. Both JPUSEB1 and the BIOS setting must be enabled to use this feature. The default setting is Enabled (Pins 1-2).

 **Note:** Please be sure to remove all other USB devices from the USB ports whose jumpers are set to disabled before the system goes into standby mode.



1. VGA Enable/Disable
2. USB7/8 Wake Up (JPUSEB1)

USB11/USB12 Disable (JP4)

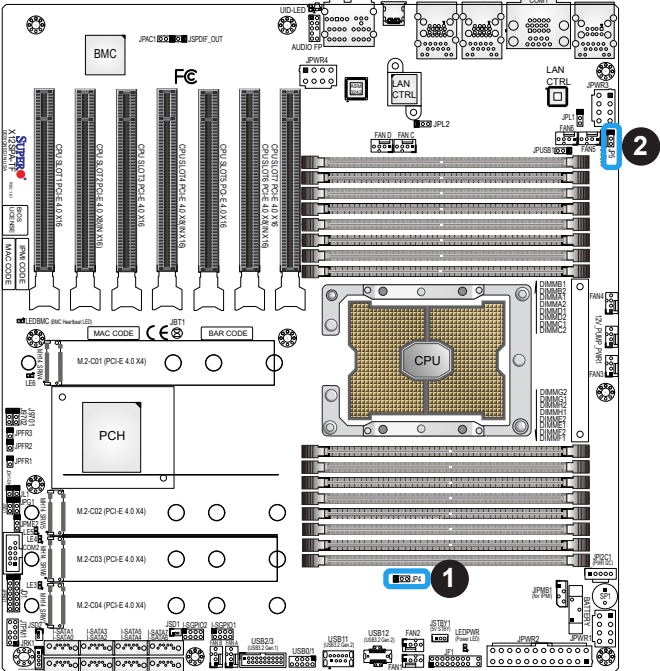
JP4 allows you to disable the USB connections for USB11 and USB12. The default setting is pins 1-2 to enable the connections. Refer to the table below for jumper settings.

USB11/USB12 Disable Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Normal
Pins 2-3	Disable USB11/12

USB4 Disable (JP5)

JP5 allows you to disable the USB connection for USB4. The default setting is pins 1-2 to enable the connection. Refer to the table below for jumper settings.

USB4 Disable Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Normal
Pins 2-3	Disable USB4



- 1. USB11/USB12 Disable (JP4)
- 2. USB4 Disable (JP5)

2.9 LED Indicators

LAN LEDs

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

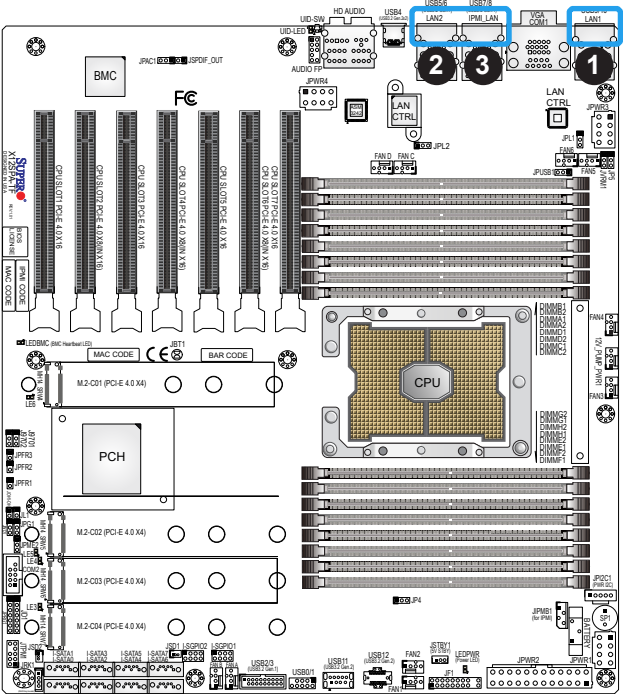
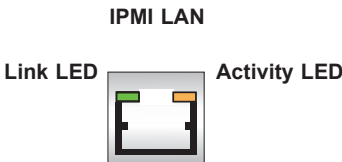
LAN1/2 Activity LED (Right) LED State		
Color	Status	Definition
Green	Flashing	Active

LAN1/2 Link LED (Left) LED State	
LED Color	Definition
Green	10Gbps
Yellow/Amber	1Gbps

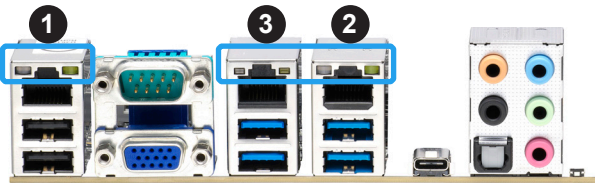
IPMI LAN LEDs

In addition to LAN1 and LAN2, an IPMI LAN is also located on the rear I/O panel. The LED on the right indicates activity, while the LED on the left indicates the speed of the connection. Refer to the table below for more information.

IPMI LAN LEDs		
	Color/State	Definition
Link (left)	Green: Solid Amber: Solid	100 Mbps 1Gbps
Activity (Right)	Amber: Blinking	Active



1. LAN1 LEDs
2. LAN2 LEDs
3. IPMI LAN LEDs



Onboard Power LED

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

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

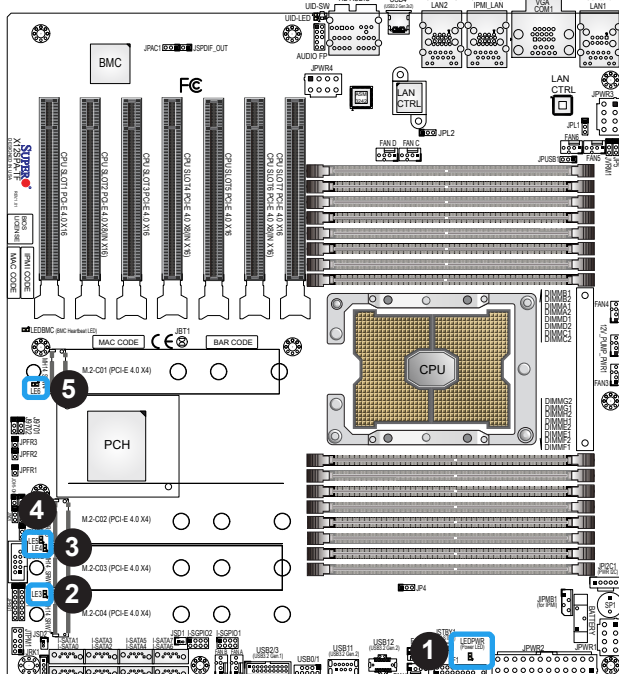
M.2 LEDs

Four M.2 LEDs are located at LE3, LE4, LE5, and LE6 on the motherboard. When the M.2 LED is blinking, M.2 functions normally. Refer to the table below for more information.

M.2 LED State	
LED Color	Definition
Green: Blinking	Device Working



Note: For information on UID LED Indicators and BMC Heartbeat LED Indicator, please refer to the section on UID LED/BMC Reset Switch and LED Indicator on page 48.



1. Onboard Power LED
2. LE3 (for M.2-C04)
3. LE4 (for M.2-C03)
4. LE5 (for M.2-C02)
5. LE6 (for M.2-C01)

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 ATX power connectors are properly connected.
3. Check that the 115V/230V 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 3VDC. If it does not, replace it with a new one.

No Video

1. If the power is on, but you do not have video, remove all add-on cards and cables.
2. Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory, or try a different one).

System Boot Failure

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

1. Check for any error beep from the motherboard speaker.
 - If there is no error beep, try to turn on the system without DIMM modules installed. If there is still no error beep, replace the motherboard.
 - If there are error beeps, clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper (JBT1). Refer to Section 2-8.
2. Remove all components from the motherboard, especially the DIMM modules. Make sure that system power is on and that memory error beeps are activated.
3. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this chapter.

Memory Errors

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

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMM modules in the system.
3. Make sure that you are using the correct type of ECC DDR4 modules recommended by the manufacturer.
4. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.

Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to Chapter 1 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies 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 IPMI to make sure that the CPU and system temperatures are within the normal range. Also check the front panel Overheat LED and make sure that it is not on.
5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Please refer to our website for more information on the minimum power requirements.
6. Proper software support: Make sure that the correct drivers are used.

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

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as USB flash or media drives.
2. Cable connection: Check to make sure that all cables are connected and working properly.
3. Use the minimum configuration for troubleshooting: Remove all unnecessary components (starting with add-on cards first), and use the minimum configuration (but with the CPU and a memory module installed) to identify the trouble areas. Refer to the steps listed in Section A above for proper troubleshooting procedures.

4. Identify bad components by isolating them: If necessary, remove a component in question from the chassis, and test it in isolation to make sure that it works properly. Replace a bad component with a good one.
5. Check and change one component at a time instead of changing several items at the same time. This will help isolate and identify the problem.
6. To find out if a component is good, swap this component with a new one to see if the system will work properly. If so, then the old component is bad. You can also install the component in question in another system. If the new system works, the component is good and the old system has problems.

3.2 Technical Support Procedures

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

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

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: This motherboard supports up to 1 TB of ECC RDIMM, 4 TB of 3DS RDIMM, 2 TB of LRDIMM, 4 TB of 3DS LRDIMM, and 4 TB of Intel Optane Persistent Memory (PMem) 200 Series with speeds of up to 3200 MHz (2DPC) in 16 DDR4 (288-pin) SMD DIMM slots. To enhance memory performance, do not mix memory modules of different speeds and sizes. Please follow all memory installation instructions given in Section 2.4.



Note: Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors.

Question: How do I update my BIOS?

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



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

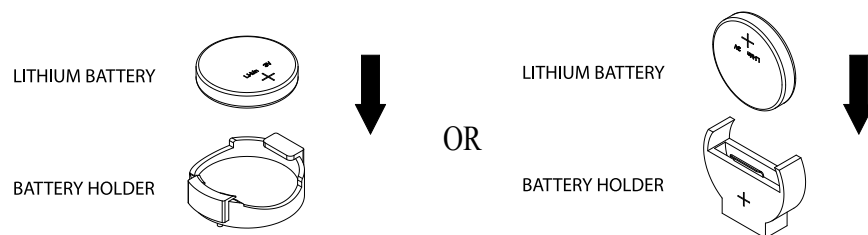
Warning: Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management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

Battery Installation

To install an onboard battery, follow the steps below:

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

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



3.5 Returning Merchandise for Service

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

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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



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

Starting the Setup Utility

To enter the BIOS Setup Utility, hit the <Delete> key while the system is booting-up. (In most cases, the <Delete> key is used to invoke the BIOS setup screen. There are a few cases when other keys are used, such as <F1>, <F2>, etc.) Each main BIOS menu option is described in this manual.

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

A " ►" indicates a submenu. Highlighting such an item and pressing the <Enter> key 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>, <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 enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS setup screen is shown below and the following items will be displayed:



System Date/System Time

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



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

Supermicro X12SPA-TF

BIOS Version

This item displays the version of the BIOS ROM used in the system.

Build Date

This item displays the date when the version of the BIOS ROM used in the system was built.

CPLD Version

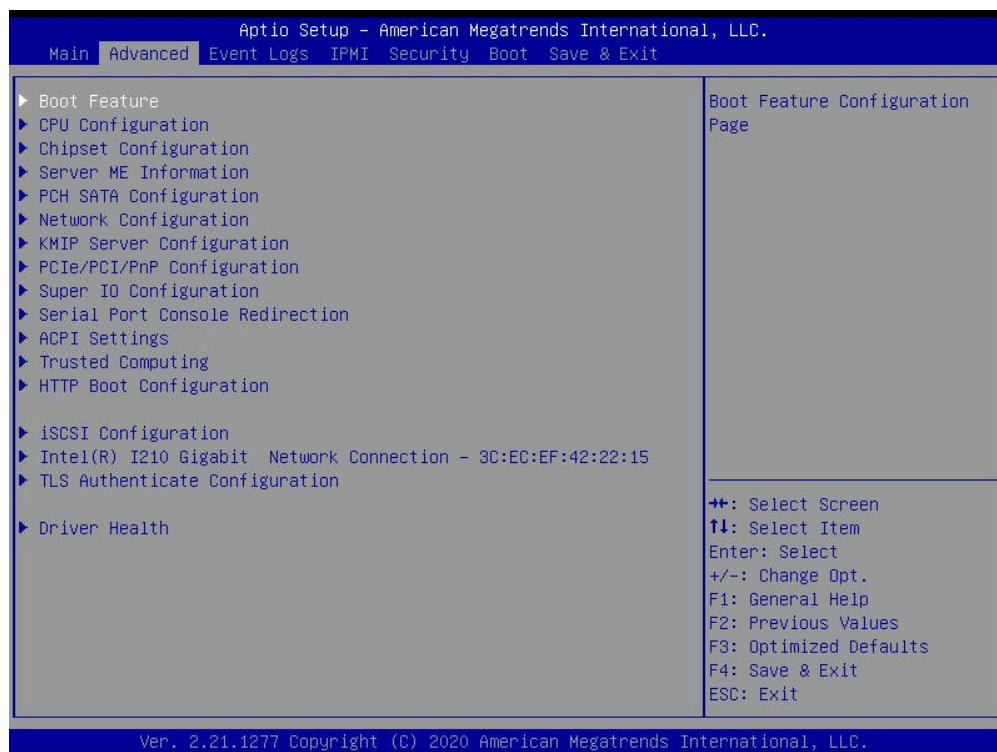
This item displays the Complex Programmable Logic Device version.

Memory Information**Total Memory**

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

4.3 Advanced Setup Configurations

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



Warning: Take caution when changing the Advanced settings. An incorrect value, a very high DRAM frequency, or an incorrect DRAM timing setting may make the system unstable. When this occurs, revert to default manufacturer settings.

► Boot Feature

Quiet Boot

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

Option ROM Messages

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

Use this feature to force the system to wait until the "F1" key is pressed if an error occurs. The options are Disabled and **Enabled**.

INT19 (Interrupt 19) 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 adapters will "capture" Interrupt 19 at bootup immediately and allow the drives that are attached to these host adapters to function as bootable disks. If this feature is set to Postponed, the ROM BIOS of the host adapters will not capture Interrupt 19 immediately and allow the drives attached to these adapters to function as bootable devices at bootup. The options are **Immediate** and Postponed.

Re-try Boot

If this feature is enabled, the BIOS will automatically reboot the system from a specified boot device after its initial boot failure. The options are **Disabled**, Legacy Boot, and EFI Boot.

Power Configuration**Watch Dog Function**

If enabled, the Watch Dog timer will allow the system to reset or generate NMI based on jumper settings when it is expired for more than five minutes. The options are **Disabled** and Enabled.

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 for the user to power off the system after pressing and holding the power button for four seconds or longer. Select Instant Off to instantly power off the system as soon as the user presses the power button. The options are **Instant Off** and 4 Seconds Override.

►CPU Configuration

The following CPU information will display:

- 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

►CPU1 Core Disable Bitmap

CPU1 Core Diabile Bitmap

Available Bitmap:

This feature displays the available bitmap.

Core Disable Bitmap(Hex)

Enter a value to enable or disable the cores for the CPU in socket 0.

Hyper-Threading (ALL) (Available when supported by the CPU)

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

Hardware Prefetcher (Available when supported by the CPU)

If set to Enable, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the L2 cache to improve CPU performance. The options are Disable and **Enable**.

Adjacent Cache Prefetch (Available when supported by the CPU)

The CPU prefetches the cache line for 64 bytes if this feature is set to Disabled. The CPU prefetches both cache lines for 128 bytes as comprised if this feature is set to Enable. The options are **Enable** and Disable.

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enable to enable the DCU (Data Cache Unit) Streamer Prefetcher which will stream and prefetch data and send it to the Level 1 data cache to improve data processing and system performance. The options are **Enable** and Disable.

DCU IP Prefetcher (Available when supported by the CPU)

Select Enable for DCU (Data Cache Unit) IP Prefetcher support, which will prefetch IP addresses to improve network connectivity and system performance. The options are **Enable** and Disable.

LLC Prefetch

If set to Enable, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the L3 cache to improve CPU performance. The options are Disable and **Enable**.

Extended APIC

Select Enable to activate APIC (Advanced Programmable Interrupt Controller) support. The options are **Disable** and Enable.

Enable Intel(R) TXT

Intel Trusted Execution Technology (TXT) helps protect against software-based attacks and ensures protection, confidentiality, and integrity of data stored or created on the system. The options are **Disable** and Enable.

VMX

Use this feature to enable the Vanderpool Technology support. The options are Disable and **Enable**.



Note: If a change is made to this setting, you will need to reboot the system for the change to take effect.

Enable SMX

Use this feature to enable the Safer Mode Extensions support. 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**.

Total Memory Encryption (TME) (Available when CPU supports TME capability)

Use this feature to enable the Total Memory Encryption (TME) function for physical memory protection. The options are **Disabled** and Enabled.

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

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

MAX TME-MT Keys (Available when "Total Memory Encryption Multi-Tenant (TME-MT)" is set to Enabled)

This feature displays the maximum TME-MT keys.

**The following Software Guard Extension (SGX) features are available when "Total Memory Encryption (TME)" is set to Enabled and CPU supports Intel Software Guard Extensions (SGX).*



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

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.

PRMRR Size

Use this feature to set the Processor Reserved Memory Range Register (PRMRR) size. The options are No valid PRMRR size, 1G, **2G**, 4G, 8G, 16G, 32G, 64G, 128G, 256G, and 512G.

SGX QoS

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

Select Owner EPOCH input type

Owner EPOCH is used as a parameter to allow the owner to add entropy to the keys during the derivation. Use this feature to select the two Owner EPOCH modes. One is New Random Owner EPOCH, 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 "Select Owner EPOCH input type" is set to Manual User Defined Owner EPOCHs)

Enter a numeric value for this feature. The default is **0**.

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

Enter a numeric value for this feature. The default is **0**.

SGXLEPUBKEYHASHx Write Enable

Use this feature to write SGX LE Public Key Hash 0-3 from OS/SW. The options are Disabled and **Enabled**.

SGXLEPUBKEYHASH0 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 0-7 of SGX Launch Enclave Public Key Hash. The default is **0**.

SGXLEPUBKEYHASH1 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 8-15 of SGX Launch Enclave Public Key Hash. The default is **0**.

SGXLEPUBKEYHASH2 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 16-23 of SGX Launch Enclave Public Key Hash. The default is **0**.

SGXLEPUBKEYHASH3 (Available when "SGXLEPUBKEYHASHx Write Enable" is set to Enabled)

Use this feature to enter the bytes 24-31 of SGX Launch Enclave Public Key Hash. The default is **0**.

Enable/Disable SGX Auto MP Registration Agent

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

Limit CPU PA to 46 Bits

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

►Advanced Power Management Configuration**Power Technology**

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

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

This feature allows you to select whether the BIOS or Operating System chooses energy performance bias tuning. The options are **OS Controls EPB** and **BIOS Controls EPB**.

ENERGY_PERF_BIAS CFG Mode (Available when the **Power Performance Tuning is set to **BIOS Controls EPB**)**

The Energy Performance BIAS (EPB) feature allows you to configure CPU power and performance settings. Select Maximum Performance to set the highest performance. Select Performance to optimize performance over energy efficiency. Select Balanced Performance to prioritize performance optimization while conserving energy. Select Balanced Power to prioritize energy conservation while maintaining good performance. Select Power to optimize energy efficiency over performance. The options are **Maximum Performance**, **Performance**, **Balanced Performance**, **Balanced Power**, and **Power**.

►CPU P State Control

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

SpeedStep (P-States)

Intel SpeedStep Technology allows the system to automatically adjust processor voltage and core frequency to reduce power consumption and heat dissipation. The options are **Disable** and **Enable**.

Dynamic SST-PP

Use this feature to enable the Dynamic SST-PP support. The options are **Disable** and **Enable**.

Intel SST-PP (Available when the [Dynamic SST-PP](#) is set to Disable)

Use this feature to select from up to two additional base frequency conditions. The options are **Base**, Config 1, and Config 2.

The following information displays.

Intel SST-PP (Core Count, Current P1 Ration [0], Package TDP (W), Tjmax) / Base / Config 1 / Config 2

Activate SST-BF

Use this feature to enable the SST-BF support. The options are **Disable** and **Enable**.

Configure SST-BF (Available when the [Activate SST-BF](#) is set to Enable)

This feature allows the BIOS to configure SST-BF High Priority Cores so that SW does not have to configure. The options are **Disable** and **Enable**.

EIST PSD Funtion (Available when the [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 of P-state changing to occur more frequently. This will allow for more demand-based P-state changing or switching that is based on real-time energy needs of applications so that the power-to-performance balance can be optimized for energy efficiency. The options are **HW_ALL** and **SW_ALL**.

Turbo Mode (Available when the [SpeedStep \(P-States\)](#) is set to Enable)

This feature will enable dynamic control of the processor, allowing it to run above stock frequency. The options are **Disable** and **Enable**.

CPU Flex Ratio Override (Available when the [SpeedStep \(P-States\)](#) is set to Enable)

Select **Enable** to activate CPU Flex Ratio programming. The options are **Disable** and **Enable**.

CPU Core Flex Ratio (Available when the [CPU Flex Ratio Override](#) is set to Enable)

Use this feature to set a value of the CPU Flex Ratio. The default is 23.

► [Hardware PM State Control](#)**Hardware P-States**

This feature allows you to select between OS and hardware-controlled P-states. Selecting **Native Mode** allows the OS to choose a P-state. Selecting **Out of Band Mode** allows the hardware to autonomously choose a P-state without OS guidance. Selecting **Native**

Mode with No Legacy Support functions as Native Mode with no support for older hardware. 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 and **Enable**.

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 use Enhanced Halt State technology, which will significantly reduce the CPU's power consumption by reducing its clock cycle and voltage during a Halt-state. The options are Disable and **Enable**.

►Package C State Control

Package C State

This feature allows you to set the limit on the C State package register. The options are C0/C1 state, C2 state, C6 (non Retention) state, and **Auto**.

►CPU T State Control

Software Controlled T-States

Use this feature to enable Software Controlled T-States. The options are **Disable** and Enable.

T-State Throttle Level (Available when the **Software Controlled T-States** is set to Enable)

Use this feature to select the On-Die thermal throttling. The options are **Disable**, 6.25%, 12.5%, 18.75%, 25.0%, 37.5%, 43.75%, 50.0%, 56.25%, 62.5%, 75.0%, 81.25%, 87.5%, and 93.75%.

► Chipset Configuration

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

► North Bridge

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

► Uncore Configuration

The following information will display:

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

Degrade Precedence

Use this feature to set degrade precedence when system settings are in conflict. Select Topology Precedence to degrade Features. Select Feature Precedence to degrade Topology. The options are **Topology Precedence** and Feature Precedence.

Link L0p Enable

Select Enable for the QPI to enter the L0p state for power saving. The options are **Disable**, Enable, and Auto.

Link L1 Enable

Select Enable for the QPI to enter the L1 state for power saving. The options are **Disable**, Enable, and Auto.

XPT Remote Prefetch

Select Enable to support XPT (Extended Prediction Table) Remote Prefetch which will allow an LLC request to be duplicated and sent to an appropriate memory controller in a remote machine based on the recent LLC history to reduce latency. The options are Disable, Enable, and **Auto**.

KTI Prefetch

KTI Prefetch enables memory read to start early on a DDR bus. The options are Disable, Enable, and **Auto**.

Local/Remote Threshold

This feature allows you to set the threshold for the Interrupt Request (IRQ) signal. The options are Disable, **Auto**, Low, Medium, and High.

IO Directory Cache (IODC)

IO Directory Cache is an 8-entry cache that stores the directory state of remote IIO writes and memory lookups, and saves directory updates. Use this feature to lower cache to cache (C2C) transfer latencies. The options are Disable, **Auto**, Enable for Remote Invltom Hybrid Push, Invltom AllocFlow, Enable for Remote Invltom Hybrid AllocNonAlloc, and Enable for Remote Invltom and Remote WvILF.

SNC (Sub NUMA)

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 **Disable**, Enable SNC2 (2-clusters), and Enable SNC4 (4-clusters).

XPT Prefetch

This feature makes a copy to the memory controller of a read request being sent to LLC. The options are Disable, Enable, and **Auto**.

Snoop Throttle Configuration

Use this feature to select the level of snoop throttle setting for CHA. The options are Disabled, Low, Medium, High, and **Auto**.

PCIe Remote P2P (Peer-to-Peer) Relaxed Ordering

Select Disable to support PCIe remote peer-to-peer relaxed writing ordering, which will allow hardware to enforce peer-to-peer write ordering. The options are **Disable** and Enable.

Stale AtoS

Use this feature to optimize the A to S directory. The options are Disable, Enable, and **Auto**.

LLC Dead Line Alloc

Select Enable to optimally fill dead lines in LLC. The options are Disable, **Enable**, and Auto.

► Memory Configuration

Enforce POR

Select POR (Plan of Record) to enforce POR restrictions on DDR4 frequency and voltage programming. The options are **POR** and Disable.

PPR Type

Use this feature to set the Post Package Repair type. The options are PPR Disabled, **Hard PPR**, and Soft PPR.

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 2133, 2200, 2400, 2600, 2666, 2800, 2933, 3000 and 3200.

Data Scrambling for DDR4

Use this feature to enable or disable data scrambling for DDR4 memory. The options are Disable and **Enable**.

2x Refresh Enable

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

► Memory Topology

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

► Memory RAS Reliability_Availability_Serviceability) Configuration

Enable Pcode WA (Workaround) for SAI (Security Attribute of the Initiator) PG (Policy Group)

Pcode, a register transfer language designed for reverse engineering, translates individual processor instructions into a sequence of Pcode operations in order to facilitate the construction of data-flow graphs and disassembling of processor instructions for machine application. Select Enabled to allow Pcode to work around the SAI group policy to achieve a solution with a next-step instruction. The options are **Disabled** and Enabled.

Mirror Mode (Available when the **UEFI ARM Mirror** is set to Disable)

This feature allows memory to be mirrored between two channels, providing 100% redundancy. The options are **Disabled**, Full Mirror Mode, and Partial Mirror Mode.

UEFI ARM Mirror

Select Enable to support the UEFI-based address range mirroring with setup option. The options are **Disable** and Enable.

ARM Mirror Percentage (Available when the [UEFI ARM Mirror](#) is set to Enable)

Use this feature to set the percentage of memory space to be used for UEFI ARM mirroring for memory security enhancement.

Correctable Error Threshold

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

Partial Cache Line Sparing PCLS

Use this feature to enable/disable PCLS sparing. The options are **Disabled** and Enabled.

ADDDC Sparing

Adaptive Double Device Data Correction (ADDDC) Sparing detects when the predetermined threshold for correctable errors is reached, copying the contents of the failing DIMM to spare memory. The failing DIMM or memory rank will then be disabled. The options are **Disabled** and Enabled.

Patrol Scrub

Patrol Scrubbing is a process that allows the CPU to correct correctable memory errors detected on a memory module and send the correction 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, **Enable**, and Enable at End of POST.

► IIO Configuration**► CPU1 Configuration**

IOU0 (IIO PCIe Port 1) / IOU1 (IIO PCIe Port 2) / IOU2 (IIO PCIe Port 3) / IOU3 (IIO PCIe Port 4) / IOU4 (IIO PCIe Port 5) /

This feature configures the PCIe port Bifurcation setting for a PCIe port specified by the user. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

PCI-E Port MPSS

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

►IOAT Configuration

Disable TPH

Transparent Huge Pages (TPH) is a Linux memory management system that enables communication in larger blocks (pages). Enabling this feature will increase performance. The options are **No** and Yes.

Prioritize TPH (Available when the **Disable TPH** is set to No)

Use this feature to enable Prioritize TPH support. The options are Enable and **Disable**.

Relaxed Ordering

Select Enable to enable Relaxed Ordering support, which will allow 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 VMM (Virtual Machine Monitor) 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 **Yes** and No.

ACS Control (Available when **Intel VT for Directed I/O (VT-d)** is set to Yes)

Use this feature to program Access Control Services (ACS) to the PCI-e Root Port Bridges. The options are **Enable** and Disable.

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

Use this feature to enable Interrupt Remapping support, which detects and controls external interrupt requests. The options are **Auto**, Yes, and No.

► Intel® VMD (Volume Management Device) Technology

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



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

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

► Intel® VMD for Volume Management Device on CPU1

VMD Config for PCH ports / VMD Config for IOU 0 / VMD Config for IOU 1 / VMD Config for IOU 3 / VMD Config for IOU 4

Enable/Disable VMD

Select Enable to enable Intel Volume Management Device Technology support for the root port specified by the user. The options are **Disable** and Enable.

****If the feature above is set to Enable, the following features will become available for configuration:***

VMD Port A/B/C/D (Available when the device is detected by the system)

Select Enable to use the Intel Volume Management Device Technology for this specific root port. The options are **Disable** and Enable.

Hot Plug Capable (Available when the device is detected by the system)

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

CfgBar Size

Use this feature to set the VMD Config Bar size (in bits. Minimum is 20 bits and maximum is 27 bits.) The default setting is **25** (in bits).

CfgBar Attribute

Use this feature to set the VMD Configuration Bar attribute (e.g. 64-bit or Prefetchable.) The options are 32-bit non-prefetchable, 64-bit non-prefetchable, and **64-bit prefetchable**.

MemBar1 Size

Use this feature to set the VMD Memory Bar1 size (in bits. Minimum is 20 bits.) The default setting is **25** (in bits).

MemBar1 Attribute

Use this feature to set the VMD Memory Bar1 attribute (e.g. 64-bit or Prefetchable.) The options are **32-bit non-prefetchable**, 64-bit non-prefetchable, and 64-bit prefetchable.

MemBar2 Size

Use this feature to set the VMD Memory Bar2 size (in bits. Minimum is 20 bits.) The default setting is **20** (in bits).

MemBar2 Attribute

Use this feature to set the VMD Memory Bar2 attribute (e.g. 64-bit or Prefetchable.) The options are 32-bit non-prefetchable, **64-bit non-prefetchable**, and 64-bit prefetchable.

► South Bridge

The following USB information will display:

- USB Module Version
- USB Devices

Legacy USB Support

This feature enables support for USB 2.0 and older. The options are **Enabled**, Disabled, and Auto.

XHCI Hand-off

When this feature is disabled, the motherboard will not support USB 3.0. The options are **Enabled** and Disabled.

Port 60/64 Emulation

This feature allows legacy I/O support for USB devices like mice and keyboards. The options are Disabled and **Enabled**.

PCIe PLL SCC

Select Enable for PCH PCI-E Spread Spectrum Clocking support, which will allow 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.

Port 61h Bit-4 Emulation

Select Enabled for I/O Port 61h-Bit 4 emulation support to enhance system performance. The options are **Disabled** and Enabled.

►Server ME Configuration

The following General ME Configuration will display:

- General ME Configuration
- Oper. Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1
- ME Firmware Status #2
- Current State
- Error Code

►PCH SATA Configuration

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

SATA Controller

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

Configure SATA as (Available when the [SATA Controller](#) is set to Enable)

Select AHCI to configure a SATA drive specified by the user as an AHCI drive. Select RAID to configure a SATA drive specified by the user as a RAID drive. The options are **AHCI** and RAID.

SATA RSTe Boot Info (Available when the [Configure SATA as](#) is set to RAID)

Select Enable to provide full int13h support for the devices attached to SATA controller. The options are Disable and **Enable**.

Support Aggressive Link Power Management

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

SATA Port 0 ~ Port 7

These features display the information detected on the installed SATA drive on the particular SATA port.

- Model number of drive and capacity
- Software Preserve Support

Hot Plug

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

Spin Up Device

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

SATA Device Type

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

► Network Configuration

Network Stack

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

****If the feature above is set to Enable, the following features will become available for configuration:***

IPv4 PXE Support

Select Enabled to enable IPv4 PXE boot support. The options are Disabled and **Enabled**.

IPv4 HTTP Support

Select Enabled to enable IPv4 HTTP boot support. The options are **Disabled** and Enabled.

IPv6 PXE Support

Select Enabled to enable IPv6 PXE boot support. The options are Disabled and **Enabled**.

IPv6 HTTP Support

Select Enabled to enable IPv6 HTTP boot support. The options are **Disabled** and Enabled.

PXE Boot Wait Time

Use this feature to specify the wait time to press the ESC key to abort the PXE boot. Press "+" or "-" on your keyboard to change the value. The default setting is **0**.

Media Detect Count

Use this option to specify the number of times media will be checked. Press "+" or "-" on your keyboard to change the value. The default setting is **1**.

**Use the following features to configure network parameters:*

►MAC:(MAC address)-IPv4 Network Configuration

Configured

Use this feature to indicate whether the above MAC address has been configured successfully. The options are **Disabled** and **Enabled**.

Enable DHCP (Available when the **Configured** is set to **Enable**)

Use this feature to set the DHCP. The options are **Disabled** and **Enabled**.

If **this feature is set to **Disabled**, the following features will become available for configuration:*

Local IP Address - Enter an IP address in dotted-decimal notation

Local NetMask - Enter a NetMask in dotted-decimal notation

Local Gateway - Enter a Gateway in dotted-decimal notation

Local DNS Servers - Enter a DNS Servers in dotted-decimal notation

Save Changes and Exit

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

►MAC:(MAC address)-IPv6 Network Configuration

►Enter Configuration Menu

The following information will display:

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

Interface ID

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

DAD Transmit Count

This feature displays the number of consecutive neighbor solicitation messages have been sent while performing duplicate address detection on a tentative address.

Policy

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

►Advanced Configuration

New IPv6 Address - Enter a new IPv6 address

New Gateway Addresses - Enter a Gateway address

New DNS Addresses - Enter a new DNS address

Commit Changes and Exit

Select this feature to save the changes you've made and return to the upper configuration page.

Discard Changes and Exit

Select this feature to discard all the changes and return to the upper configuration page.

Save Changes and Exit

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

►KMIP Server Configuration**KMIP Server IP address**

Use this feature to enter the KMIP server IP4 address in dotted-decimal notation.

KMIP TCP Port number

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

TimeZone

Use this feature to enter the correct time zone. The default setting is **8** (GT+8 Taiwan time).

Client UserName

Press <Enter> to set the client user name. The name length is 0 ~ 63 characters.

Client Password

Press <Enter> to set the client password. The password 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.

►PCIe/PCI/PnP Configuration

The following information will display:

- 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**.

SR-IOV Support

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

ARI Support

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

Bus Master Enable

Select Enabled to enable the Bus Driver Master bit. The options are Disabled and **Enabled**.

MMIO High Base

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

MMIO High Granularity Size

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

Maximum Read Request

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.

MMCFG Base

Use this feature to select the low base address for PCIe adapters to increase base memory. The options are 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, and **Auto**.

NVMe Firmware Source

The feature determines which type of NVMe firmware should be used in your system. The options are **Vendor Defined Firmware** and AMI Native Support.

VGA Priority

Use this feature to select VGA priority when multiple VGA devices are detected. Select Onboard to give priority to your onboard video device. Select Offboard to give priority to your graphics card. The options are **Onboard** and Offboard.

Onboard Video Option ROM

Use this feature to select the Onboard Video Option ROM type. The options are Disabled and **EFI**.

CPU SLOT1 PCI-E 4.0 X16 OPROM**CPU SLOT2 PCI-E 4.0 X8 OPROM****CPU SLOT3 PCI-E 4.0 X16 OPROM****CPU SLOT4 PCI-E 4.0 X8 OPROM****CPU SLOT5 PCI-E 4.0 X16 OPROM****CPU SLOT6 PCI-E 4.0 X8 OPROM****CPU SLOT7 PCI-E 4.0 X16 OPROM****M.2-C01 PCI-E 4.0 x4 OPROM****M.2-C02 PCI-E 4.0 x4 OPROM****M.2-C03 PCI-E 4.0 x4 OPROM****M.2-C04 PCI-E 4.0 x4 OPROM**

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled and **EFI**.

Onboard SAS Option ROM

Use this feature to select the Option ROM type for the SAS device specified by the user for system boot. The options are Disabled and **EFI**.

Onboard LAN Device

Use this feature to enable the Onboard LAN device. The options are Disabled and **Enabled**.

Onboard LAN1 Option ROM (Available when the [Onboard LAN Device](#) is set to Enable)

Use this feature to select which firmware function to be loaded for LAN port 1 used for system boot. The options are Disabled and **EFI**.

Onboard LAN2 Option ROM (Available when the [Onboard LAN Device](#) is set to Enable)

Use this feature to select which firmware function to be loaded for LAN port 2 used for system boot. The options are Disabled and **EFI**.

► Super IO Configuration

The following Super IO information will display:

- Super IO Chip AST2500

► 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 (Available when the [Serial Port 1](#) is set to Enabled)

This feature displays the status of a serial port specified by the user.

Change Settings (Available when the [Serial Port 1](#) is set to Enabled)

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. 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 (Available when the **Serial Port 2** is set to Enabled)

This item displays the status of a serial port specified by the user.

Change Settings (Available when the **Serial Port 2** is set to Enabled)

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options are **Auto**, (IO=3F8h; IRQ=3;), (IO=2F8h; 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 COM 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 console redirection support for a serial port specified by the user. The options are **Disabled** and Enabled.

►Console Redirection Settings (Available when the **Console Redirection** is set to Enabled)

Use this feature to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection 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**.

Putty KeyPad

This feature selects the settings for Function Keys and KeyPad used for Putty, which is a terminal emulator designed for the Windows OS. The options are **VT100**, LINUX, XTERMR6, SC0, ESCN, and VT400.

Redirection After BIOS POST

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

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 the Console Redirection is set to Enabled)

Use this feature to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection 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**.

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, SC0, ESCN, and VT400.

Redirection After BIOS POST

Use this feature to enable or disable legacy Console Redirection after BIOS POST. When set to Bootloader, legacy Console Redirection is disabled before booting the OS. When set to Always Enable, legacy Console Redirection remains enabled when booting the OS. The options are **Always Enable** and BootLoader.

Legacy Console Redirection

Legacy Serial Redirection Port

Use this feature to select a COM port to display redirection of Legacy OS and Legacy OPR0M messages. The options are **COM1** and SOL/COM2.

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

Console Redirection EMS

Select Enabled to use a COM port selected by the user for EMS Console Redirection. The options are **Disabled** and Enabled.

► Console Redirection Settings (Available when the Console Redirection EMS is set to Enabled)

This feature allows you to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Out-of-Band Mgmt Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2.

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 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 displays:

Data Bits EMS, Parity EMS, Stop Bits EMS

►ACPI Settings

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**.

►Trusted Computing (Available when a TPM device is installed and detected by the BIOS)

This motherboard supports TPM 1.2 and 2.0. The following Trusted Platform Module (TPM) information will display if a TPM 2.0 module is detected:

- Vendor Name
- Firmware Version

Security Device Support

If this feature and the TPM jumper on the motherboard are both set to Enabled, onboard security devices will be enabled for TPM (Trusted Platform Module) support to enhance data integrity and network security. Please reboot the system for a change on this setting to take effect. The options are Disable and **Enable**.

- Active PCR Bank
- Available PCR banks
- SHA256 PCR Bank

****If the feature above is set to Enable, **SHA-1 PCR Bank** and **SHA256 PCR Bank** will become available for configuration:***

SHA-1 PCR Bank

Use this feature to disable or enable the SHA-1 Platform Configuration Register (PCR) bank for the installed TPM device. The options are Disabled and **Enabled**.

SHA256 PCR Bank

Use this feature to disable or enable the SHA256 Platform Configuration Register (PCR) bank for the installed TPM device. The options are Disabled and **Enabled**.

Pending Operation

Use this feature to schedule a TPM-related operation to be performed by a security device for 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 (for TPM Version 2.0 and above)

Select Enabled for TPM Platform Hierarchy support which will allow 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

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

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

PH (Platform Hierarchy) Randomization (for TPM Version 2.0 and above)

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

SMCI BIOS-Based TPM Provision Support

Use feature to enable the Supermicro TPM Provision support. The options are **Disabled** and **Enabled**.

TXT Support

Intel Trusted Execution Technology (TXT) helps protect against software-based attacks and ensures protection, confidentiality, and integrity of data stored or created on the system. Use this feature to enable or disable TXT Support. The options are **Disabled** and **Enabled**.



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

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

► HTTP Boot Configuration

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**.

Priority of HTTP Boot

Instance of Priority 1:

The priority sequence of HTTP Boot. The default setting is **1**.

Select IPv4 or IPv6

Use this feature to select which internet protocol the targeted LAN port is boot from IPv4 or IPv6. The options are **IPv4** and **IPv6**.

Boot Description

Press <Enter> and enter a boot description. The maximal length is 20.

Boot URI

This feature allows you to boot the system from a network connection. The maximal length is 128.

Instance of Priority 2: (Available when the **HTTP Boot Policy** is set to **Apply to each LAN or Boot Priority #1 instantly**)

The priority sequence of HTTP Boot. The default setting is **0**.

► iSCSI Configuration

► Attempt Priority

Attempt Priority

Use this feature to change the priority of iSCSI attempt using the + or - keys. The options are Host Attempt, Redfish Attempt, and Rst Attempt.

Commit Changes and Exit

Use this feature to save all changes and exit the above settings.

► Host iSCSI Configuration

iSCSI Initiator Name

This feature allows you to enter the unique name of the iSCSI Initiator in IQN format. Once the name of the iSCSI Initiator is entered into the system, configure the proper settings for the following items.

► Add an Attempt

► Delete Attempts

► Change Attempt Order

► Intel(R) I210 Gigabit Network Connection - (MAC address)

► Firmware Image Properties

The following information will display:

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

► NIC Configuration

Link Speed

This feature allows you to specify the port speed used for the selected boot protocol. The options are **Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, and 100 Mbps Full.

Wake On LAN

Select Enabled for the Wake_On_LAN support, which will allow the system to "wake up" when an onboard device receives an incoming signal. The options are Disabled and **Enabled**.

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. Use the keyboard to select a value. The maximal value is 15 (seconds).

UEFI Driver

This feature displays the UEFI driver version.

Adapter PBA

This feature displays the Processor Bus Adapter (PBA) model number. The PBA number is a nine digit number (i.e., 010B00-000) located near the serial number.

Device Name

This feature displays the adapter device name.

Chip Type

This feature displays the network adapter chipset name.

PCI Device ID

This feature displays the device ID number.

PCI Address

This feature displays the PCI address for this computer. PCI addresses are three two-digit hexadecimal numbers.

Link Status

This feature displays the connection status.

MAC Address

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

Virtual MAC Address

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

► TLS Authenticate Configuration

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

► Server CA Configuration / Client Certification Configuration

► Enroll Certification

► Enroll Certification Using File

Use this feature to enroll certification from a file.

Certification GUID (Global Unique Identifier)

Press <Enter> and input the certification GUID.

► Commit Changes and Exit

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

► Discard Changes and Exit

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

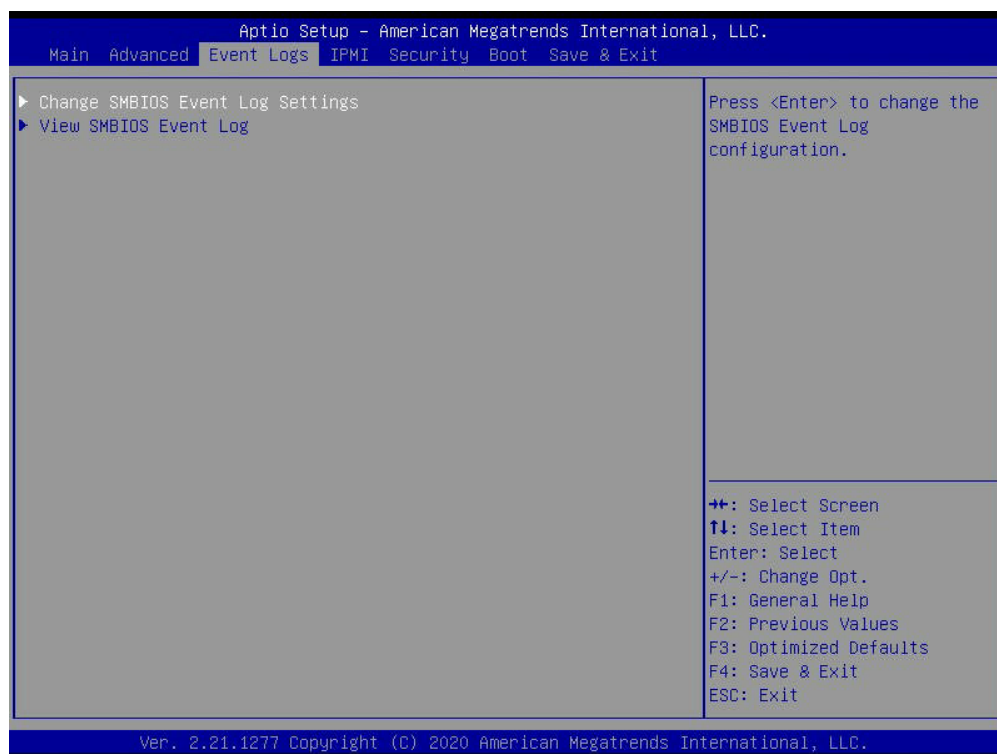
► Delete Certification

► Driver Health

This feature provides health status for the drivers and controllers.

4.4 Event Logs

Use this feature to configure Event Log settings.



► Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

Change this feature to enable or disable all features of the SMBIOS Event Logging during system boot. The options are Disabled and **Enabled**.

****If **this feature** is set to **Enable**, the following features will become available for configuration:***

Erasing Settings

Erase Event Log

If No is selected, data stored in the event log will not be erased. Select Yes, Next Reset, data in the event log will be erased upon next system reboot. Select Yes, Every Reset, data in the event log will be erased upon every system reboot. The options are **No**, (Yes, Next reset), and (Yes, Every reset).

When Log is Full

Select Erase Immediately for all messages to be automatically erased from the event log when the event log memory is full. The options are **Do Nothing** and Erase Immediately.

SMBIOS Event Log Standard Settings

Log System Boot Event

This option toggles the System Boot Event logging to enabled or disabled. The options are Enabled and **Disabled**.

MECI

The Multiple Event Count Increment (MECI) counter counts the number of occurrences that a duplicate event must happen before the MECI counter is incremented. This is a numeric value. The default value is **1**.

METW

The Multiple Event Time Window (METW) defines the number of minutes that must pass between duplicate log events before MECI is incremented. This is in minutes, from 0 to 99. The default value is **60**.



Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

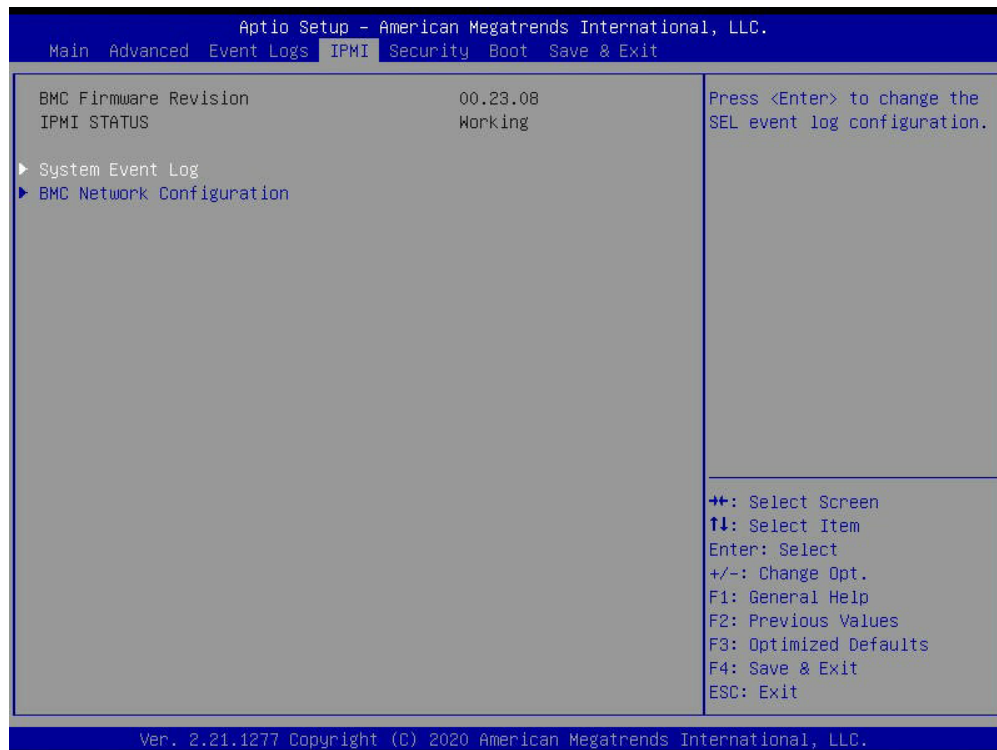
►View SMBIOS Event Log

Select this submenu and press enter to see the contents of the SMBIOS event log. The following categories will be displayed:

DATE / TIME / ERROR CODE / SEVERITY.

4.5 IPMI

Use this feature to configure Intelligent Platform Management Interface (IPMI) settings.



BMC Firmware Revision

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

IPMI STATUS (Baseboard Management Controller)

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

▶ System Event Log

Enabling/Disabling Options

SEL Components

Select Enabled for all system event logging at boot up. The options are Disabled and **Enabled**.

Erasing Settings

Erase SEL

Select Yes, On next reset to erase all system event logs upon next system reboot. 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 decide what the BIOS should do when the system event log is full. Select Erase Immediately to erase all events in the log when the system event log is full. The options are **Do Nothing** and Erase Immediately.



Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

►BMC Network Configuration

BMC Network Configuration

Update IPMI LAN Configuration

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

****If the feature above is set to Yes, the following features will become available for configuration:***

Configure IPv4 Support

This section displays configuration features for IPV4 support.

IPMI LAN Selection

This feature allows you to select the type of the IPMI LAN. The default setting is **Failover**.

IPMI Network Link Status

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

Configuration Address Source

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

****If the feature above is set to Static, the following features will become available for configuration:***

Station IP Address

This feature displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253). Press <Enter> to change the setting.

Subnet Mask

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. Press <Enter> to change the setting.

Station MAC Address

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

Gateway IP Address

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.31.0.1). Press <Enter> to change the setting.

VLAN

This feature displays the virtual LAN settings. The options are **Disable** and **Enable**.

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

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

Configure IPv6 Support

This section displays configuration features for IPV6 support.

IPv6 Address Status

This feature displays the IPv6 address status.

IPv6 Support

Use this feature to enable IPv6 support. The options are **Enabled** and **Disabled**.

****If the feature above is set to Enabled, the following features will become available for configuration:***

Configuration Address Source

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

If the **feature above is set to Static, the following features will become available for configuration:*

Station IPv6 Address

This feature displays the station IPv6 address.

Prefix Length

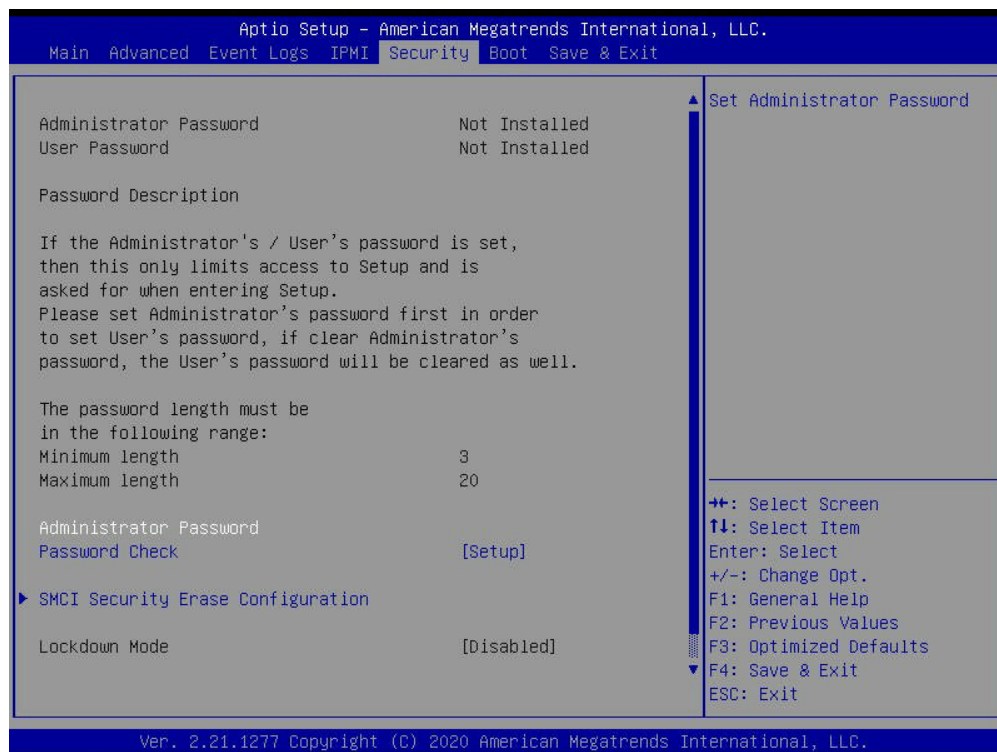
This feature displays the prefix length.

IPv6 Router IP Address

This feature displays the IP address of the IPv6 router.

4.6 Security

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



Administrator Password

Press <Enter> to create a new or change an existing administrator password.

Password Check

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

► SMCI Security Erase Configuration



Note: This submenu becomes configurable when a storage device has been plugged into the motherboard.

This section allows you to configure the SMCI-proprietary Security Erase settings. When this section is selected, the following features will display:

- **HDD Name:** This feature displays the name of the HDD/SATA drive that is connected to the SMCI Security Erase Configuration submenu.
- **HDD Serial Number:** This feature displays the serial number of the HDD/SATA device that is connected to the SMCI Security Erase Configuration submenu.
- **Security Erase Mode:** This feature displays the security erase mode used in the system.
- **Estimated Time:** This feature displays the estimate time needed to perform the selected Security Erase features.
- **Admin Pwd (Administrator Password) Status:** This feature displays the status of the administrator password.

Security Function

Use this feature to configure the security settings for the HDD/SATA device. Select Security Erase 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 - Without Password to use the manufacturer default password "11111111" 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**, Security Erase, and Set Password.

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

Password

Use this feature to set the SATA user password which will allow you to configure the SMCI Security Erase settings by using the SATA user password.

Hard Drive Security Frozen

Use this feature to disable or enable the BIOS security frozen command to SATA and NVMe devices. The options are Enabled and **Disabled**.

Password Check

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

► Secure Boot



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

When you select this submenu and press the <Enter> key, the following items will display:

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

Select Enabled for Secure Boot flow control. This feature is available when the platform key (PK) is pre-registered, the platform operates in the user mode, and CSM is disabled in the Setup utility. The options are **Disabled** and Enabled.

Secure Boot Mode

This feature allows selection of the Secure Boot Mode between Standard and Custom. Selecting Custom enables users to change the Image Execution Policy and manage Secure Boot Keys. The options are **Custom** and Standard.

CSM Support

Select enabled to support the Compatibility Support Module (CSM), which provides compatibility support for traditional legacy BIOS for system boot. The options are **Disabled** and Enabled.



Note: It is recommended to disable this feature. If this feature is set to Enabled, the Intel Trusted Execution Technology (TXT) will be invalid.

****If the feature of **Secure Boot Mode** is set to Custom, the following features will become available for configuration:***

► Enter Audit Mode

Press <Enter> to enter the audit mode workflow. It will result in erasing of Platform Key (PK) variables and reset system to the Setup/Audit mode.

► Enter Deployed Mode / Exit Deployed Mode

Press <Enter> button to switch between Deployment and User Mode.

► Key Management (Available when **Secure Boot Mode** is set to Custom)

This submenu allows you to configure the following Key Management settings.

Vendor Keys

This feature displays the Vendor Keys. The default is Modified.

Provision Factory Default Keys

Select Enabled to install the default Secure Boot keys set by the manufacturer. The options are **Disabled** and Enabled.

▶ Restore Factory Keys

Use this feature to Install factory default secure boot key databases. The options are **Yes** and No. Select Yes will reset system to the User mode.

▶ Reset to Setup Mode

Use this feature to delete all secure boot key databases from NVRAM. Select Yes will reset system to the Setup mode.

▶ Export Secure Boot variables

This feature allows you to copy NVRAM content of secure boot variables to files in a root folder on a file system device.

▶ 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).

Device Guard Ready

▶ Remove 'UEFI CA' from DB

Use this feature to remove the Microsoft UEFI CA certificate from the database.

▶ Restore DB defaults

Select **Yes** to restore DB variables to factory defaults.

Secure Boot Variable / Size / Keys / Key Source

▶ Platform Key(PK)

This feature allows you to configure the settings of the Platform Key (PK).

Details

Review details on current settings of the PK.

Export

This feature allows you to export the PK to an available file system.

Update

Select Yes to load the new PK from the manufacturer's defaults. Select No to load the PK from a file.

Delete

Select Yes to confirm deletion of the PK from NVRAM.

► Key Exchange Keys

Details

Review details on current settings of the Key Exchange Keys.

Export

This feature allows you to export Key Exchange Keys to an available file system.

Update

Select Yes to load the Key Exchange Keys from the manufacturer's defaults. Select No to load the Key Exchange Keys from a file.

Append

Select Yes to add the Key Exchange Keys from the manufacturer's defaults list to the existing Key Exchange Keys. Select No to load the Key Exchange Keys from a file.

Delete

Select Yes to delete the Key Exchange Keys. Select No to delete only a certificate from the key database.

► Authorized Signatures

Details

Review details on current settings of the Authorized Signatures (DB).

Export

This feature allows you to export authorized signatures to an available file system.

Update

Select Yes to load the factory default DB. Select No to load the DB from an external file.

Append

Select Yes to add the database from the manufacturer's defaults to the existing DB. Select No to load the DB from a file.

Delete

Select Yes to delete the DB. Select No to delete only a certificate from the DB.

►Forbidden Signatures**Details**

Review details on current settings of the Forbidden Signatures (DBX).

Export

This feature allows you to export the DBX to an available file system.

Update

Select Yes to load the DBX factory defaults. Select No to load it from an external file.

Append

Select Yes to add the DBX from the manufacturer's defaults to the existing DBX. Select No to load the DBX from a file.

Delete

Select Yes to delete the DBX. Select No to delete only a certificate from the DBX.

►Authorized TimeStamps**Details**

Review details on current settings of the Authorized TimeStamps (DBT).

Export

This feature allows you to export the DBT to an available file system.

Update

Select Yes to load the DBT from the manufacturer's defaults. Select No to load the DBT from a file.

Append

Select Yes to add the DBT from the manufacturer's defaults list to the existing DBT. Select No to load the DBT from a file.

Delete

Select Yes to delete the DBT. Select No to delete only a certificate from the key database.

► OsRecovery Signature

This feature uploads and installs an OsRecovery Signature (DBR). You may insert a factory default key or load from a file. The file formats accepted are:

- 1) Public Key Certificate
 - a. EFI_SIGNATURE_LIST
 - b. EFI_CERT_X509 (DER Encoded)
 - c. EFI_CERT_RSA2048 (bin)
 - d. EFI_CERT_SHAXXX

2) Authenticated UEFI Variable

3) EFI PE/COEF Image (SHA256)

When prompted, select Yes to load Factory Defaults or No to load from a file.

Details

Review details on current settings of the DBR.

Export

This feature allows you to export the DBR to an available file system.

Update

Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file.

Append

Select Yes to add the DBR from the manufacturer's defaults list to the existing DBR. Select No to load the DBR from a file.

Delete

Select Yes to delete the DBR. Select No to delete only a certificate from the key database.

► TCG Storage Device Security Configuration

► Storage Device



Note: The feature shown here is dependent on the storage device plugged into the motherboard.

► Password Configuration:

Information for the following is displayed:

- **Security Subsystem Class**
- **Security Supported**
- **Security Enabled**
- **Security Locked**
- **Security Frozen**
- **User Pwd Status**
- **Admin Pwd Status**

► Set Admin Password

Press <Enter> to create a new admin password.

► Set User Password

Press <Enter> to create a new user password.



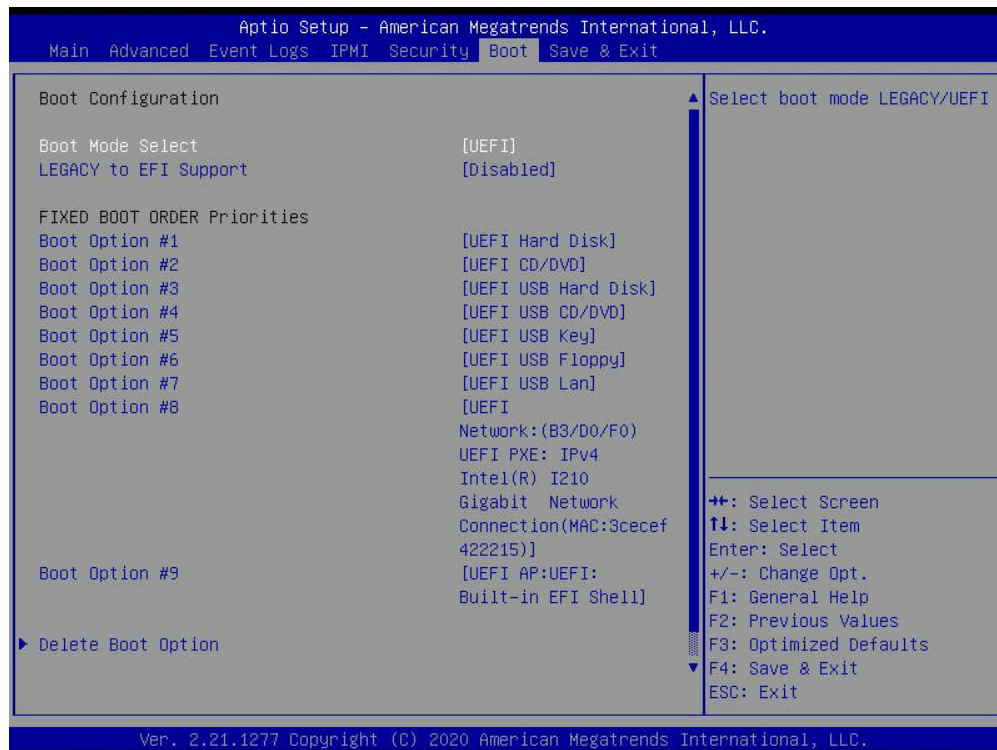
Note: This feature is available when the [Admin Password](#) has been activated.

Device Reset

Reset the device using 32 byte PSID (Physical Security Identification) value of the device.

4.7 Boot

Use this feature to configure Boot settings.



Boot Mode Select

Use this item to select the type of device that the system is going to boot from. The options are Legacy, **UEFI**, and Dual.

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 option prioritizes the order of bootable devices that the system boots from. Press <Enter> on each entry from top to bottom to select devices.

Legacy Boot Option #1~#8

These features display when [Boot mode select](#) is set to Legacy. The options are Hard Disk, CD/DVD, USB Hard Disk, USB CD/DVD, USB Key, USB Floppy, USB LAN, and Network.

UEFI Boot Option #1~#9

These features display when [Boot mode select](#) is set to UEFI. The options are UEFI Hard Disk, UEFI CD/DVD, UEFI USB Hard Disk, UEFI USB CD/DVD, UEFI USB Key, UEFI USB Floppy, UEFI USB Lan, UEFI Network, and UEFI AP.

DUAL Boot Option #1~#17

These features display when [Boot mode select](#) is set to DUAL. The options contain all options from UEFI and Legacy boot modes.

►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 priority list.

►UEFI Network Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1 ~ Boot Option #4

►UEFI Application Boot Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

****If any storage media is detected, the following features will become available for configuration:***

►Add New Boot Option

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

Add Boot Option

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

Path for Boot Option

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

Boot Option File Path

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

Create

Use this item to set the name and the file path of the new boot option.

►UEFI USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

►USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

►UEFI Hard Disk Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

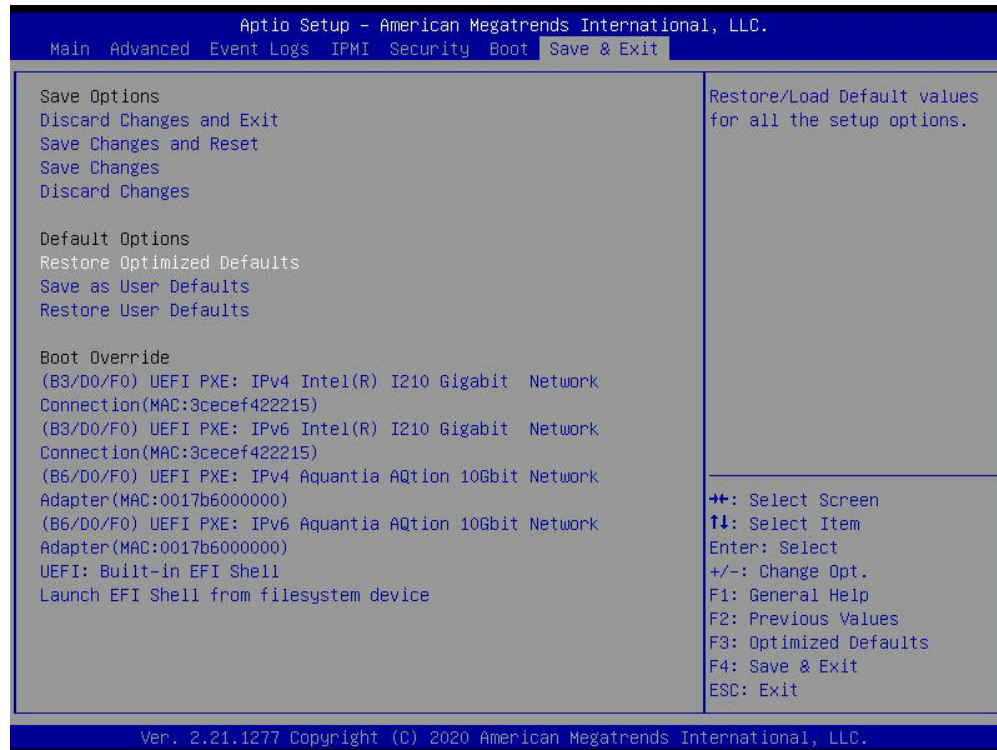
►Hard Disk Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

4.8 Save & Exit

Select the Save & Exit tab from the BIOS setup screen to configure the settings below:



Save Options

Discard Changes and Exit

Use this feature to quit the BIOS Setup 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 take effect.

Save Changes

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

Discard Changes

Press <Enter> to discard all the changes and return to the AMI BIOS utility Program.

Default Options

Restore Optimized Defaults

Use this feature to restore/load default values. These are factory settings designed for maximum system stability, but not for maximum performance.

Save as User Defaults

This feature enables the user to save any changes to the BIOS setup for future use.

Restore User Defaults

Use this feature to retrieve user-defined settings that were saved previously.

Boot Override

Listed in this section are other boot options for the system (i.e., Built-in EFI shell). Select an option and press <Enter>. Your system will boot to the selected boot option.

Appendix A

BIOS POST Codes

A.1 BIOS POST Codes

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

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

Appendix B

Software

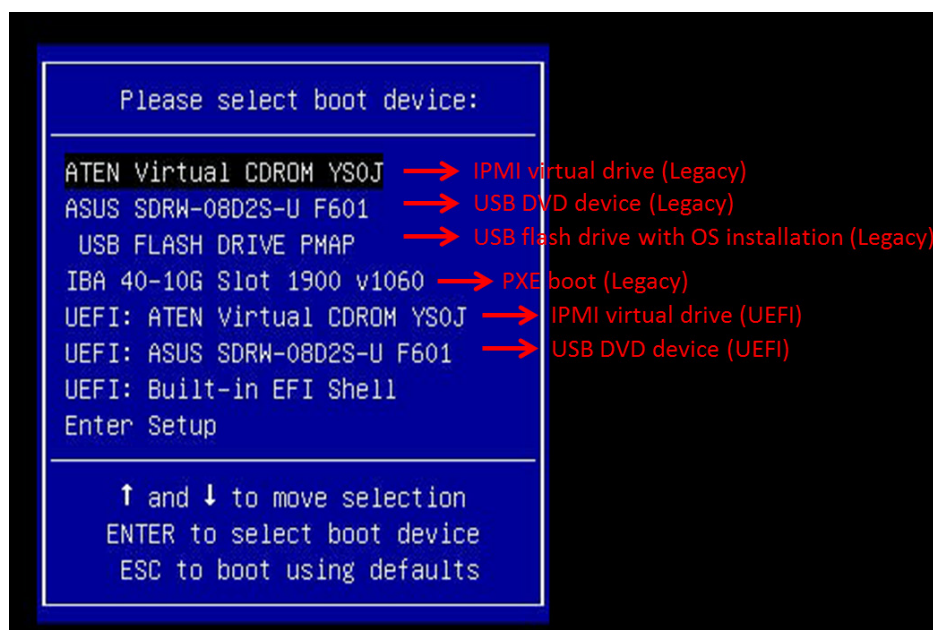
After the hardware has been installed, you can install the Operating System (OS), configure RAID settings, and install the drivers.

B.1 Microsoft Windows OS Installation

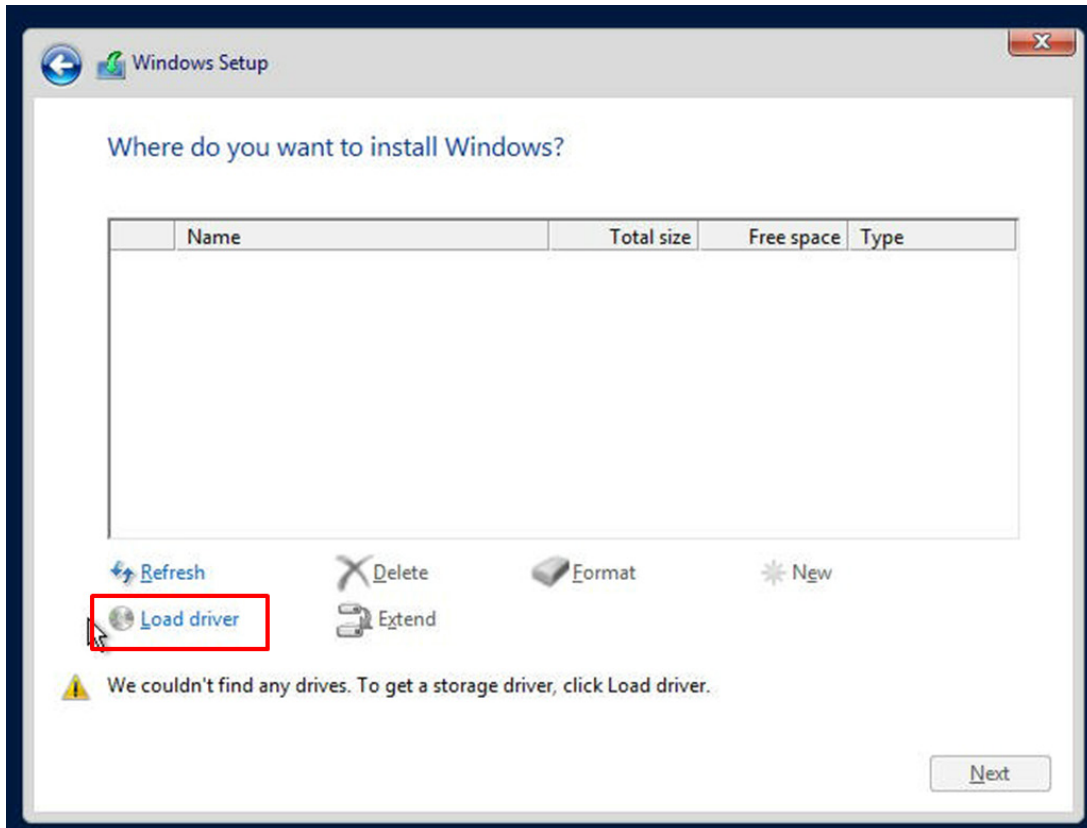
If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at www.supermicro.com/support/manuals.

Installing the OS

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



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.

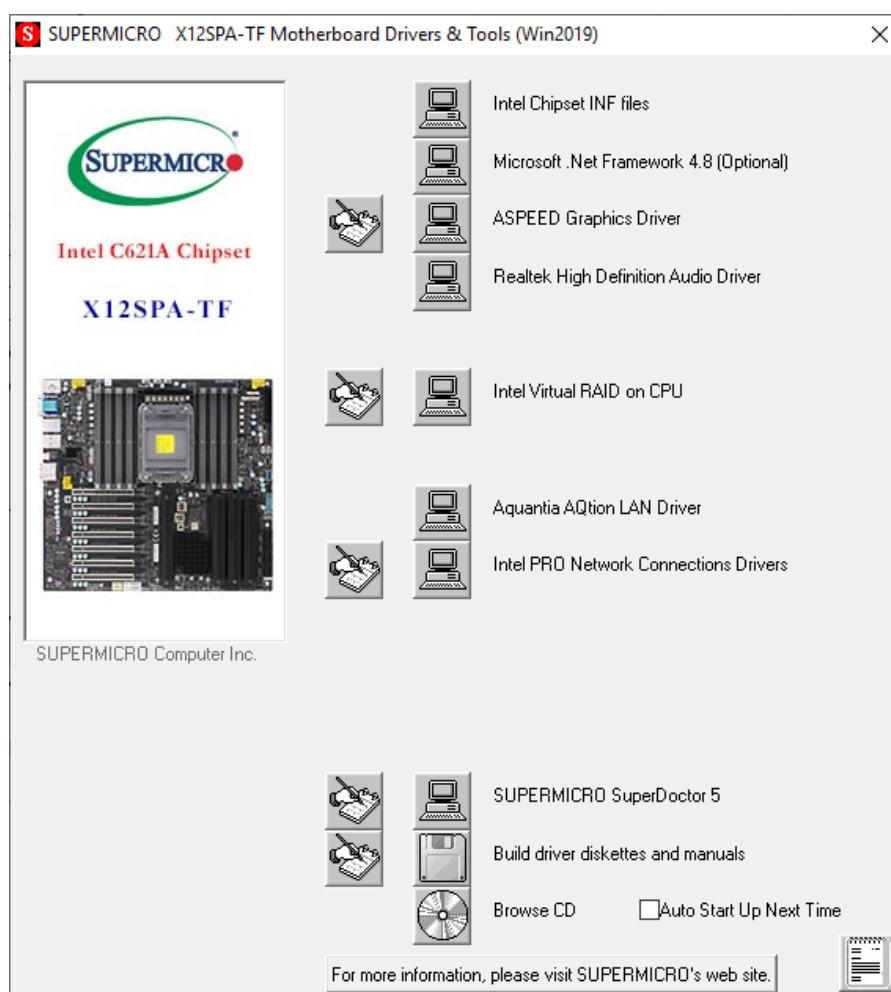
B.2 Driver Installation

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.

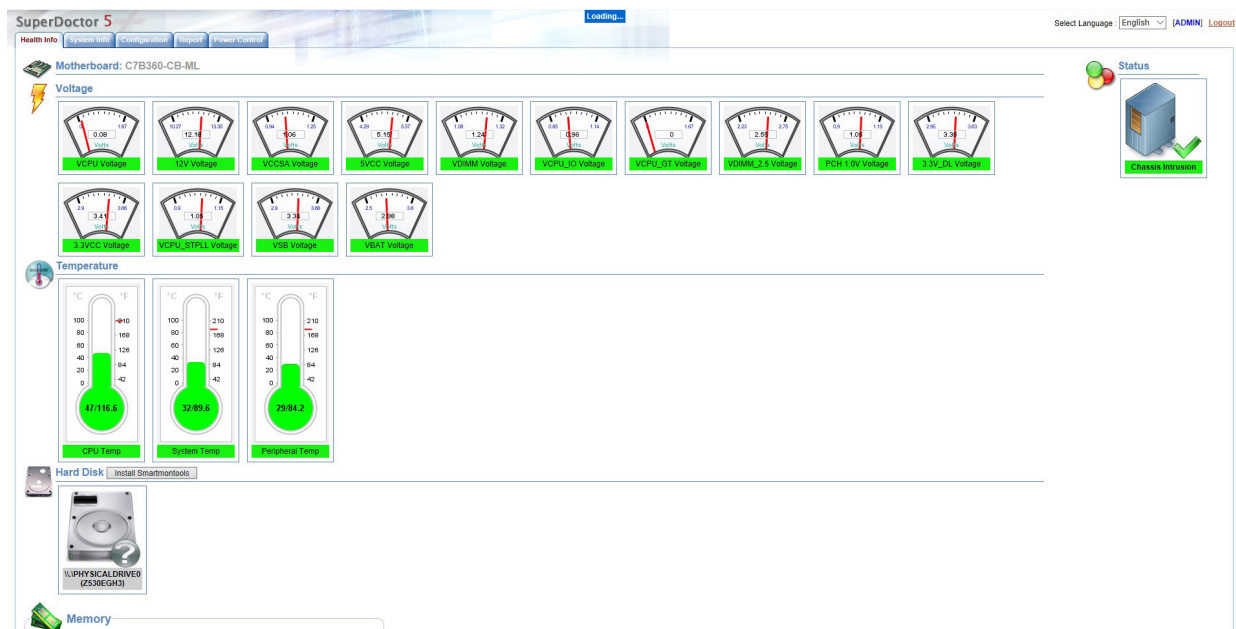


Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to bottom) one at a time. **After installing each item, you must re-boot the system before moving on to the next item on the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

B.3 SuperDoctor® 5

The Supermicro SuperDoctor 5 is a program that functions in a command-line or web-based interface for Windows and Linux operating systems. The program monitors such system health information as CPU temperature, system voltages, system power consumption, fan speed, and provides alerts via email or Simple Network Management Protocol (SNMP).

SuperDoctor 5 comes in local and remote management versions and can be used with Nagios to maximize your system monitoring needs. With SuperDoctor 5 Management Server (SSM Server), you can remotely control power on/off and reset chassis intrusion for multiple systems with SuperDoctor 5 or IPMI. SuperDoctor 5 Management Server monitors HTTP and SMTP services to optimize the efficiency of your operation.



B.4 IPMI

The X12SPA-TF supports the Intelligent Platform Management Interface (IPMI). IPMI is used to provide remote access, monitoring and management. There are several BIOS settings that are related to IPMI.

For general documentation and information on IPMI, please visit our website at: <http://www.supermicro.com/products/nfo/IPMI.cfm>.

B.5 Logging into the BMC (Baseboard Management Controller)

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

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

For more information regarding BMC passwords, please visit our website at <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

電池更換不當會有爆炸危險。請只使用同類電池或制造商推薦的功能相當的電池更換原有電池。請按製造商的說明處理廢舊電池。

警告

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

Warnung

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

Attention

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

¡Advertencia!

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

אזהרה!

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

هناك خطر من انفجار في حالة اسبدال البطارية بطريقة غير صحيحة فاعلil

اسبدال البطارية

فقط بنفس النوع أو ما يعادلها مما أوصت به الشركة المصنعة

جخلص من البطاريات المسحمة وفقا لعليمات الشركة الصانعة

경고!

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

Waarschuwing

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

Product Disposal



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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

عند التخلص النهائي من هذا المنتج ينبغي التعامل معه وفقا لجميع القوانين واللوائح الوطنية

경고!

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

Waarschuwing

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