



X12SPT-G/-GC

USER'S MANUAL

Revision 1.0b

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 a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

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



WARNING: This product can expose you to chemicals including lead, known to the State of California to cause cancer and birth defects or other reproductive harm. For more information, go to www.P65Warnings.ca.gov.

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

Manual Revision 1.0b

Release Date: April 30, 2025

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

Copyright © 2025 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About This Manual

This manual is written for system integrators, IT technicians and knowledgeable end users. It provides information for the installation and use of the motherboard.

About This Motherboard

The Supermicro X12SPT-G/-GC motherboard supports a 3rd Generation Intel® Xeon Scalable Processor with up to 40 cores and a Thermal Design Power (TDP) of 270 W. Built with the Intel C621A chipset, the X12SPT-G/-GC supports up to 4 TB of ECC RDIMM 3DS and LRDIMM 3DS DDR4 with speeds of up to 3200 MHz in 16 DIMM modules with support for Intel Optane PMem 200 Series memory. (See Note 1 below). This motherboard features superior IO expandability, which includes four PCIe 4.0 x8 MCIO connectors, two SlimSAS ports (can support six SATA via PCH for –G or six SAS3 via onboard SAS3808 for –GC), two Hybrid M.2 in 2280. This motherboard also offers the most advanced data protection capability that encompasses Trusted Platform Module (TPM) and Root of Trust (RoT) support. X12SPT-G/GC is optimized for high-density, high-end computing platforms for big data, virtualization, and enterprise applications. Note that this motherboard is intended to be installed and serviced by professional technicians only. For processor/memory updates, refer to our website at <http://www.supermicro.com/products/>.

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

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

Conventions Used in the Manual

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



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



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



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



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

Contacting Supermicro

Headquarters

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

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: Marketing@supermicro.com (General Information)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
Support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)

Website: www.supermicro.com

Europe

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

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

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

Website: www.supermicro.nl

Asia-Pacific

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

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

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

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

Quick Reference	13
Quick Reference Table	14
Motherboard Features	15
1.2 Processor and Chipset Overview	18
1.3 Special Features	18
Recovery from AC Power Loss	18
1.4 System Health Monitoring	18
Onboard Voltage Monitors	18
Fan Status Monitor with Firmware Control	19
Environmental Temperature Control	19
System Resource Alert	19
1.5 ACPI Features	19
1.6 Power Supply	19
1.7 Serial Port	20
1.8 Intel® Optane™ Persistent Memory (PMem) 200 Series Overview	20

Chapter 2 Installation

2.1 Static-Sensitive Devices	21
Precautions	21
Unpacking	21
2.2 Processor and Heatsink Installation	22
The 3rd Generation Intel Xeon Scalable Processor	22
Overview of the Processor Carrier Assembly	23
Overview of the CPU Socket	23
Overview of the Processor Heatsink Module	24
Creating the 3rd Generation Intel Xeon Scalable Processor Carrier Assembly	25
Assembling the Processor Heatsink Module	26
Preparing the CPU Socket for Installation	27
Installing the Processor Heatsink Module	28
Removing the Processor Heatsink Module	29
2.3 Motherboard Installation	30

Tools Needed	30
Location of Mounting Holes	30
Installing the Motherboard.....	31
2.4 Memory Support and Installation	32
Memory Support.....	32
General Guidelines for Optimizing Memory Performance	35
DIMM Installation	36
DIMM Removal	36
2.5 Rear I/O Ports	37
2.6 Connectors	38
Power Connections	38
Headers.....	39
2.7 Jumper Settings	43
How Jumpers Work.....	43
2.8 LED Indicators.....	45
<i>Chapter 3 Troubleshooting</i>	
3.1 Troubleshooting Procedures	47
Before Power On	47
No Power	47
System Boot Failure	48
Memory Errors	48
Losing the System's Setup Configuration	48
When the System Becomes Unstable	49
3.2 Technical Support Procedures	51
3.3 Frequently Asked Questions	52
3.4 Battery Removal and Installation	53
Battery Removal.....	53
Proper Battery Disposal	53
Battery Installation.....	53
3.5 Returning Merchandise for Service.....	54

Chapter 4 UEFI BIOS

4.1 Introduction	55
Starting the Setup Utility	55
4.2 Main Setup	56
4.3 Advanced Setup Configurations	58
4.4 Event Logs	98
4.5 IPMI	100
4.6 Security	104
4.7 Boot	108
4.8 Save & Exit	110

Appendix A Software**Appendix B Standardized Warning Statements****Appendix C UEFI BIOS Recovery**

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.

 **Note:** This motherboard was designed to be a part of an integrated server solution. No shipping package will be included in the shipment.

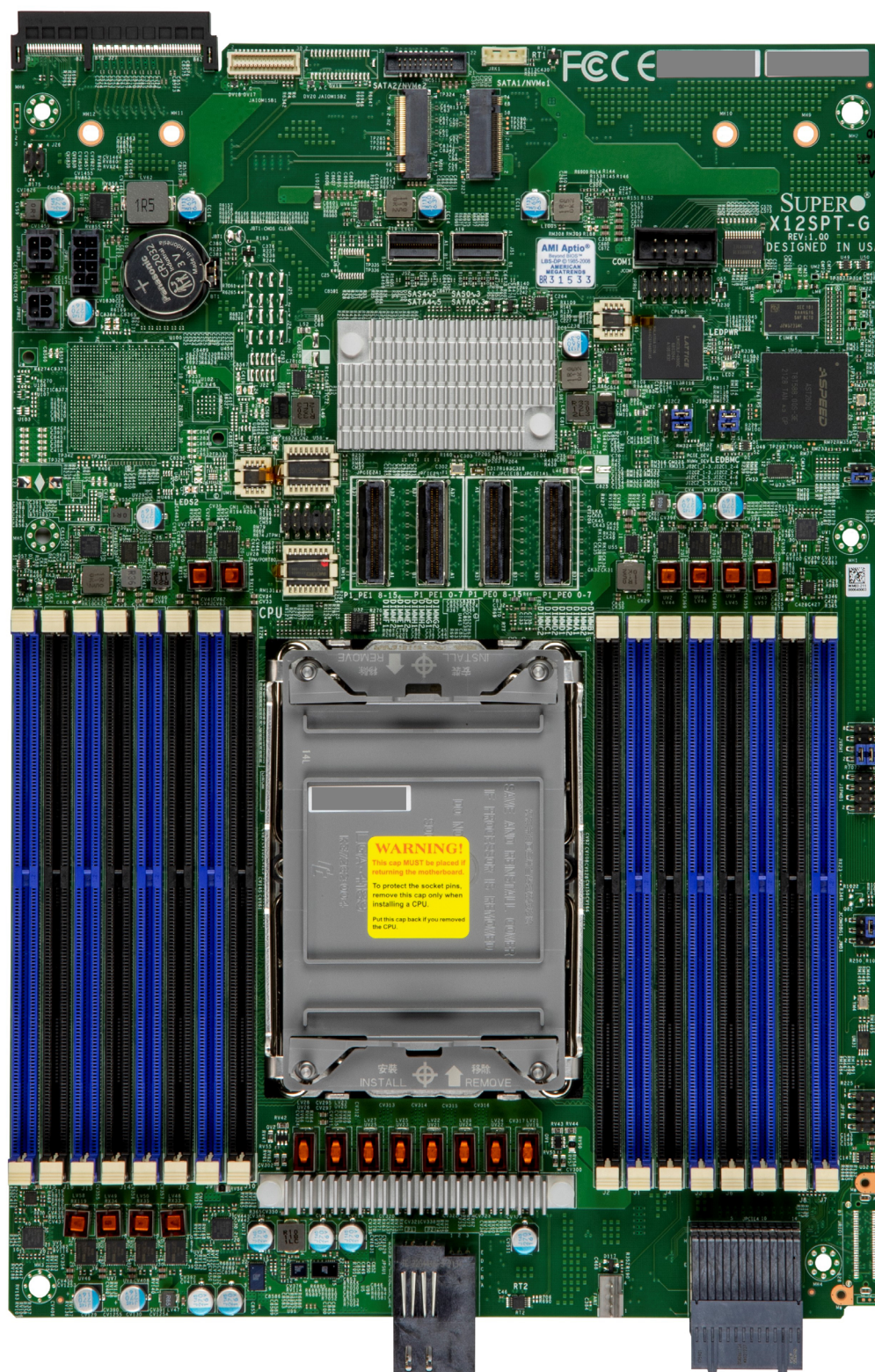
Important Links

For your system 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

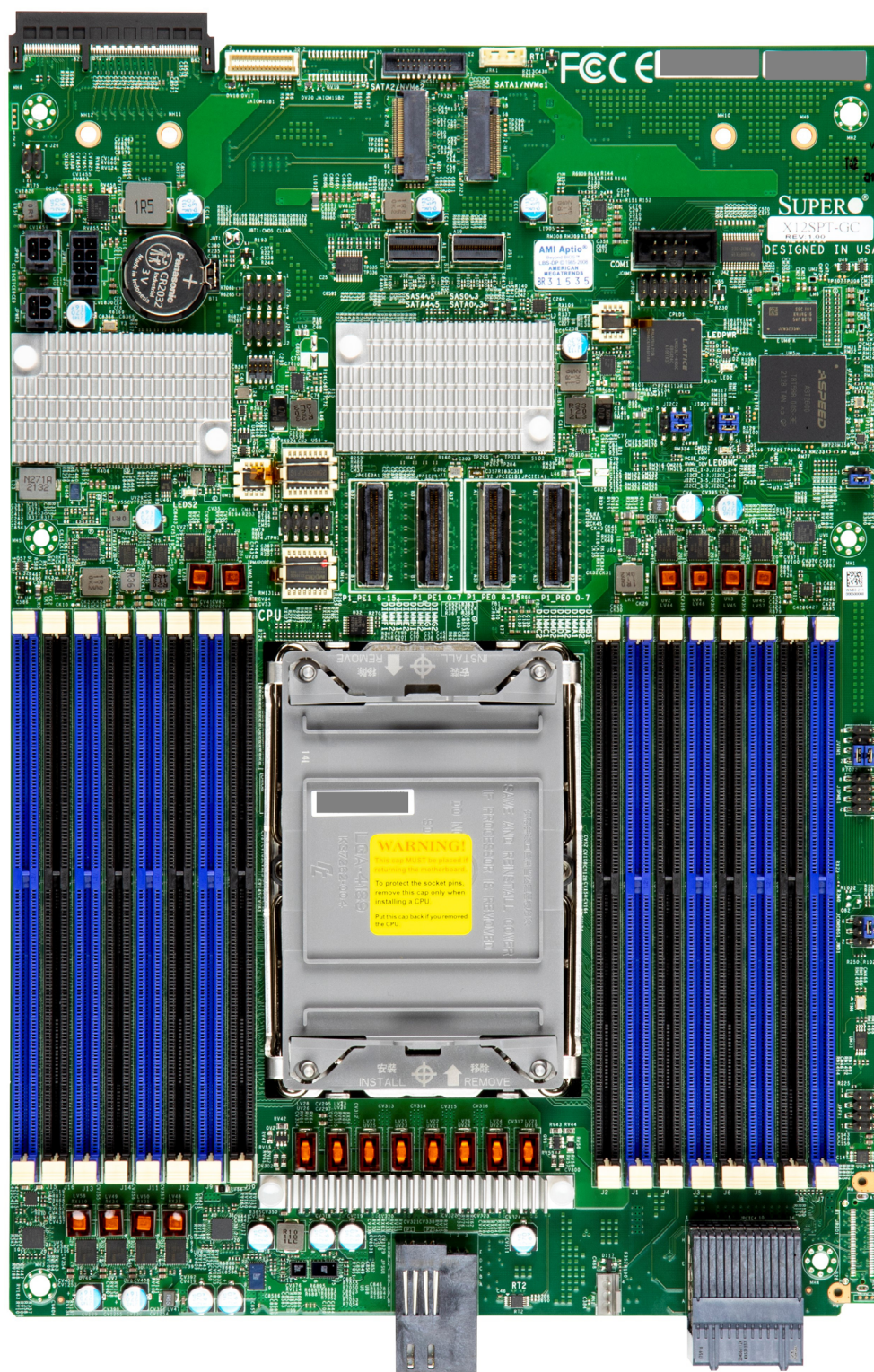
This manual may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

Figure 1-1. X12SPT-G Motherboard Image

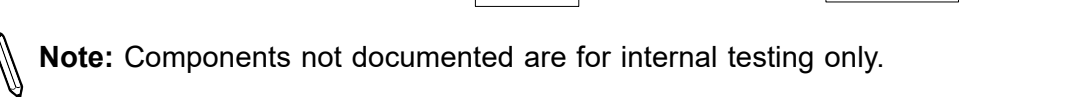


Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publication of the manual. The motherboard you received may or may not look exactly the same as the graphics shown in this manual.

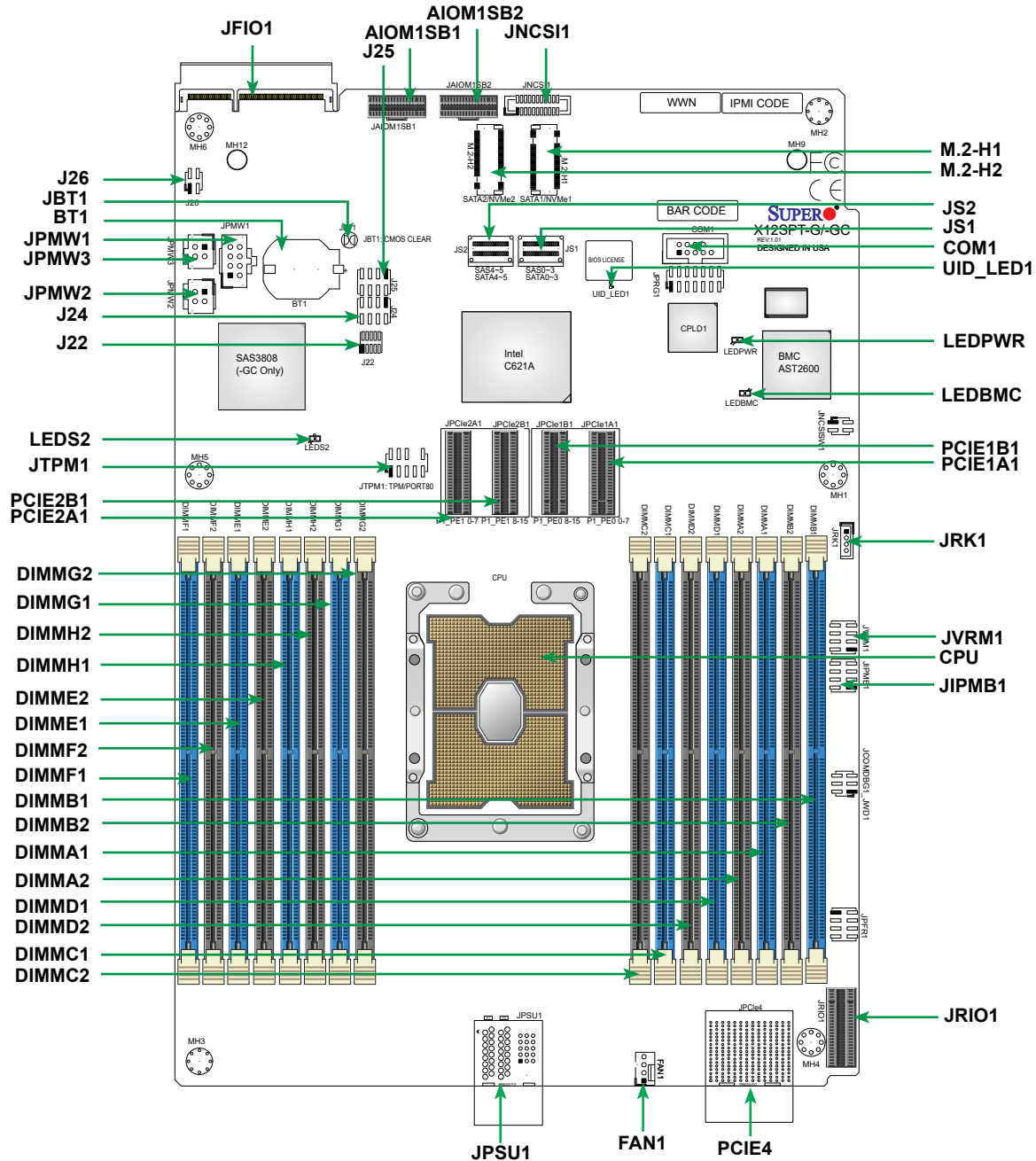
Figure 1-2. X12SPT-GC Motherboard Image



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.



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
JBT1	CMOS Clear	Open (Normal)
JVRM1	Jumper for switching VRM SMBus Controllers	Pins 1-3/2-4 (BMC)
LED	Description	Status
LEDBMC	BMC Heartbeat	Blinking Green: BMC Normal
LEDPWR	Power LED	Solid Green: Power On
LEDS2	SAS Error LED	Solid RED: SAS Error
UID_LED1	UID LED	Solid Blue: Unit Identified
Connector	Description	
AIOM1SB1	AIOM1 Sideband Signals Header	
AIOM1SB2	AIOM2 Sideband Signals Header	
BT1	Onboard Battery	
COM1	COM Header	
FAN1	CPU/System Fan Header (FAN1: CPU Fan)	
J22	SAS PSOC FW Update Header	
J24	SAS3808 PSOC UART Header	
J25	SAS3808 RMC and SDB UART Header	
J26	SAS3808 SBL Disable	
JFIO1	Grand Twin Front IPMI and Onboard NIC Module Connector	
JIPMB1	8-pin External I ² C Header (For an IPMI card)	
JNCSI1	Network Controller Sideband Interface (NC-SI) Connector	
JPMW1	8-pin GPU and NVMe power connector	
JPMW2 - JPMW3	4-pin GPU and NVMe power connectors	
JPSU1	Grand Twin Power Supply Connector	
JRIO1	Grand Twin Rear IPMI Module Connector	
JRK1	Intel RAID Key Header	
JS1	SAS0-3/SATA0-3	
JS2	SAS4-5/SATA4-5	
JTPM1	Trusted Platform Module/Port 80 Connector	
MH9-MH12	M.2 Mounting Holes	
M.2-H1, M.2.-H2	M.2 PCIe 3.0x4/SATA3 Slot (supports M-Key 2280)	
PCIE1A1	PE0 0-7 PCIe Connector	
PCIE1B1	PE0 8-15 PCIe Connector	
PCIE2A1	PE1 0-7 PCIe Connector	
PCIE2B1	PE1 8-15 PCIe Connector	

Motherboard Features

Motherboard Features	
CPU	
Supports a 3rd Generation Intel Xeon Scalable Processor (Socket P+) with up to 40 cores and a thermal design power (TDP) of 270W	
Memory	
Supports up to 4 TB of ECC RDIMM 3DS and LRDIMM 3DS DDR4 memory with speeds of up to 3200 MHz in 16 memory including the support for Intel Optane Persistent Memory (PMem) 200 Series with speeds of up to 3200 MHz	
	Note 1: Supported memory data transfer rate is subject to the specification of processor. Note 2: Intel Optane PMem 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) series processors.
DIMM Size	
Up to 256 GB at 1.2 V for the DDR4 memory module, up to 512 GB for the Intel Optane PMem 200 series module.	
	Note: For the latest CPU/memory updates, refer to our website at http://www.supermicro.com/products/motherboard.
Chipset	
Intel C621A	
Expansion Slots	
- One PCIe 4.0 x8 4C customized 124-pin SLIM COOL EDGE connector (for front I/O module) - One PCIe 4.0 x16 Molex Impelplus connector - Four PCIe 4.0 x8 MCIO connectors - Two M.2 in 2280 (PCIe3.0 x4 and SATA)	
Baseboard Management Controller	
Aspeed AST2600 BMC with RoT support	
Network	
- Intel i350 Ethernet Controller - Intel BMC57414 25G Ethernet Controller	
Graphics	
Aspeed AST2600	
I/O Devices	
- SATA 3.0: Two SlimSASx4 ports for six SATA via PCH for -G - SAS 3.0: Two SlimSASx4 ports for six SAS3 via onboard SAS3808 for -GC (one PCIe 4.0 x8) - One front accessible serial port header (COM1) - One TPM header	



Note: The table above is continued on the next page.

Motherboard Features

BIOS

- 256 Mb SPI AMI® BIOS
- ACPI 6.0, Plug and Play (PnP), BIOS rescue hot-key, riser card auto detection support, and SMBIOS 3.0 or later
- Super Flash
- SPI dual/quad speed support
- Riser Card auto detection support
- Real Time Clock (RTC) wakeup

Power Management

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

System Health Monitoring

- Onboard voltage monitoring for +3.3 V, +5 V, +12 V, +3.3 VStb, +5 Stb, Vcore, Vmem, CPU temperature, PCH temperature, system temperature, memory temperature, and peripheral temperature
- 7+1 CPU switch phase voltage regulator
- CPU thermal trip support
- Platform Environment Control Interface (PECI)/TSI

Fan Control

- Low-noise fan speed control
- One 4-pin fan header (spare)

System Management

- Trusted Platform Module (TPM) support
- SuperDoctor® 5
- Server Platform Service
- IPMI View, SMCIPMITOOL, IPMICFG, SSM, SUM-OOB

LED Indicators

- CPU/System Overheat
- Power/Suspend State Indicator LED
- Fan Fail LED
- UID LED

Dimensions

- 12.42" (W) x 8.52" (L) ATX (315.47 mm x 216.41 mm), proprietary FF

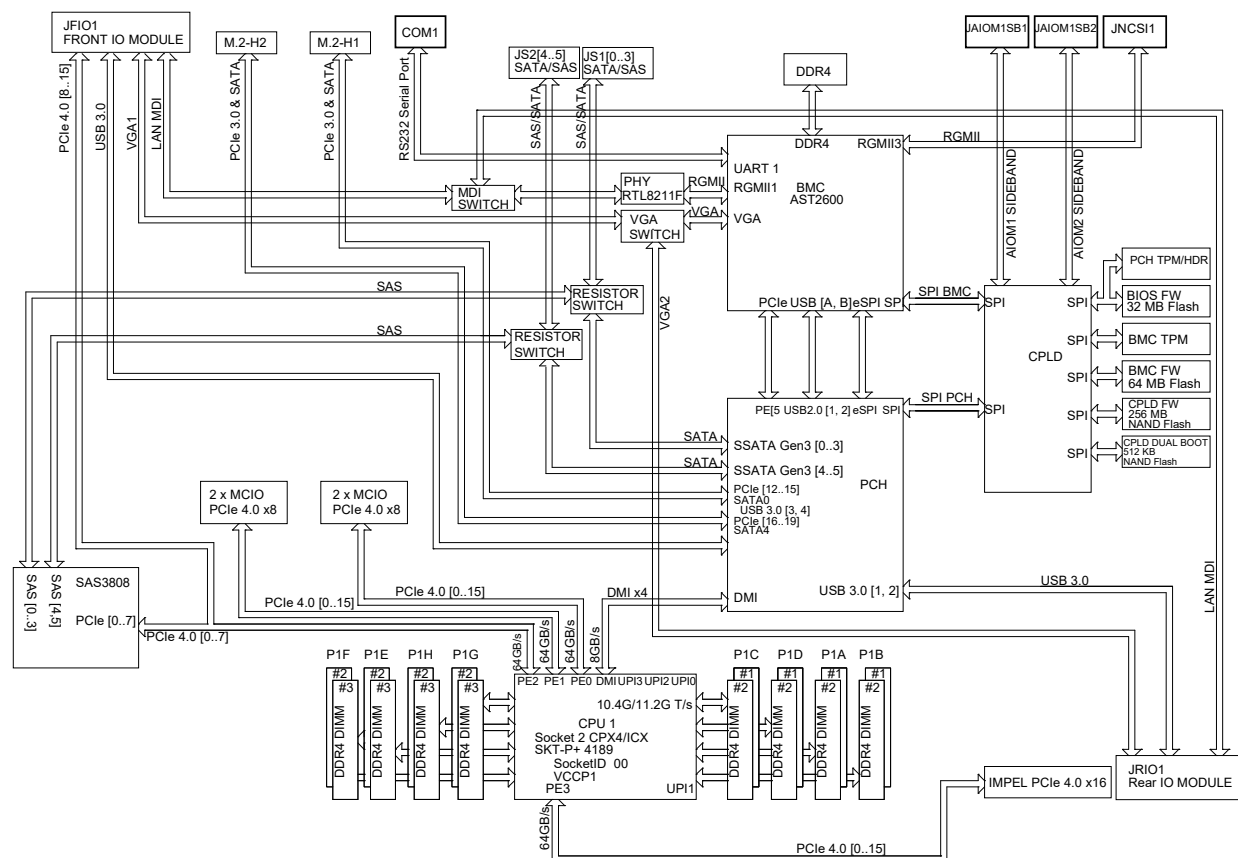


Note 1: The CPU maximum thermal design power (TDP) is subject to chassis and heatsink cooling restrictions. For proper thermal management, please check the chassis and heatsink specifications for proper CPU TDP sizing.



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

Figure 1-3.
System Block Diagram



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

1.2 Processor and Chipset Overview

Built upon the functionality and capability of the 3rd Generation Intel Xeon Scalable Processor and the Intel C621A chipset, the X12SPT-G/-GC motherboard provides system performance, power efficiency, and feature sets optimized for high-performance computing, artificial intelligence (AI), and HPC. The X12SPT-G/-GC dramatically increases system performance for a multitude of server applications and supports:

- 4 TB ECC RDIMM 3DS and LRDIMM 3DS DDR4 memory with speeds of up to 3200 MHz
- Support of SMBus speeds of up to 400 KHz for BMC connectivity
- SPI Enhancements
- Intel Node Manager for advanced power monitoring, capping and management for BMC enhancement (see note below)
- BMC supports remote management, virtualization, and the security package for enterprise platforms



Note: Node Manager support depends on the power supply used in your system.

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, CPU, and battery continuously. Once a voltage becomes unstable, a warning is given, or an error message is sent to the screen. The user can adjust the voltage thresholds to define the sensitivity of the voltage monitor.

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the IPMI interface. Whenever the temperature of the CPU or the system exceeds a user-defined threshold, system/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

The Advanced Configuration and Power Interface (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 CD-ROMs, 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.

1.7 Serial Port

The X12SPT-G/-GC motherboard supports one serial communication connection. COM1 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 Generation Intel Xeon Scalable Processor supports the new Intel® Optane™ Persistent Memory (PMem) 200 Series technology. PMem offers data persistence with higher capacity at similar latencies to the existing memory modules and provides hyper-speed storage capability for high performance computing platforms with flexible configuration options.

 **Note:** The Intel® Optane™ Persistent Memory (PMem) 200 Series are supported by the 3rd Generation 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 system board, it is important to handle it very carefully. The following measures are generally sufficient to protect your equipment from ESD.

Precautions

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

Unpacking

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

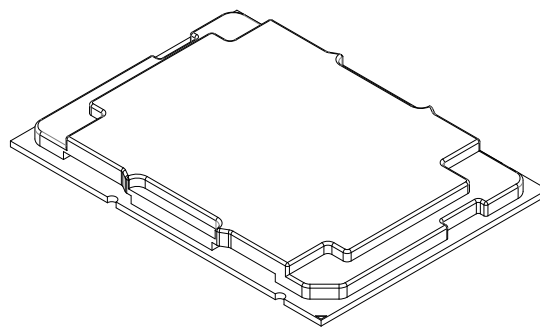
2.2 Processor and Heatsink Installation

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

Notes:

- Use ESD protection.
- Unplug the AC power cord 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 support.
- All graphics in this manual are for illustration purposes only. Your components may look different.

The 3rd Generation Intel Xeon Scalable Processor

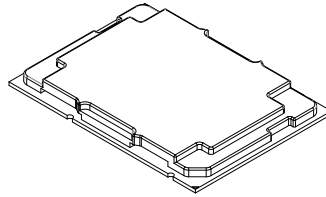


3rd Generation Intel Xeon Scalable Processor

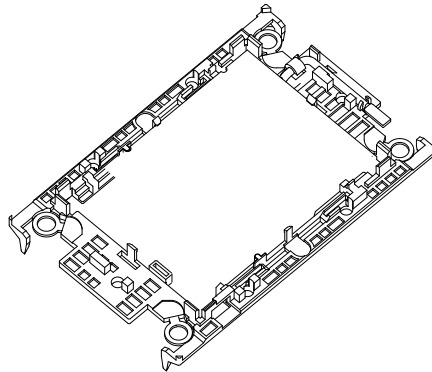
Overview of the Processor Carrier Assembly

The processor carrier assembly contains the 3rd Generation Intel Xeon Scalable Processor and a processor carrier.

1. Processor



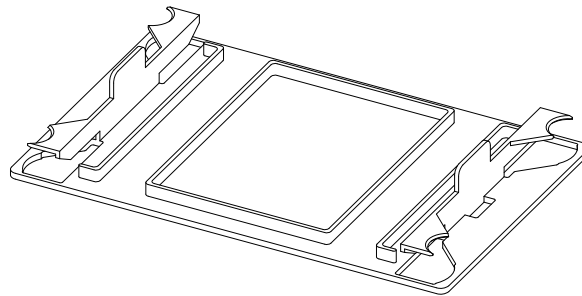
2. Processor Carrier



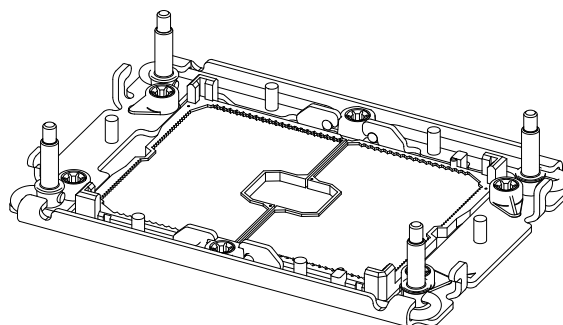
Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

1. Plastic Protective Cover



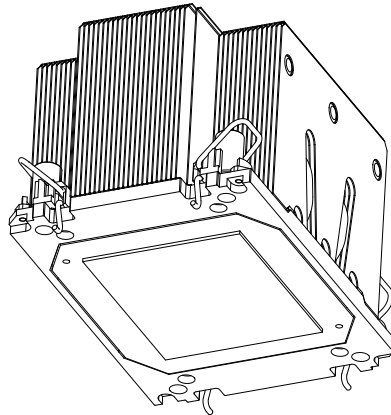
2. CPU Socket



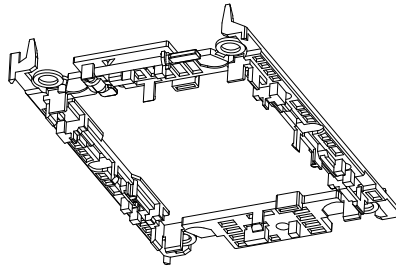
Overview of the Processor Heatsink Module

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

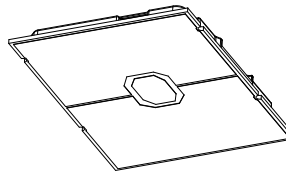
1. Heatsink with Thermal Grease



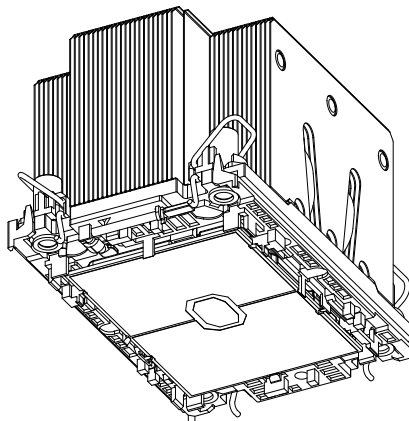
2. Processor Carrier



3. Processor



Processor Heatsink Module



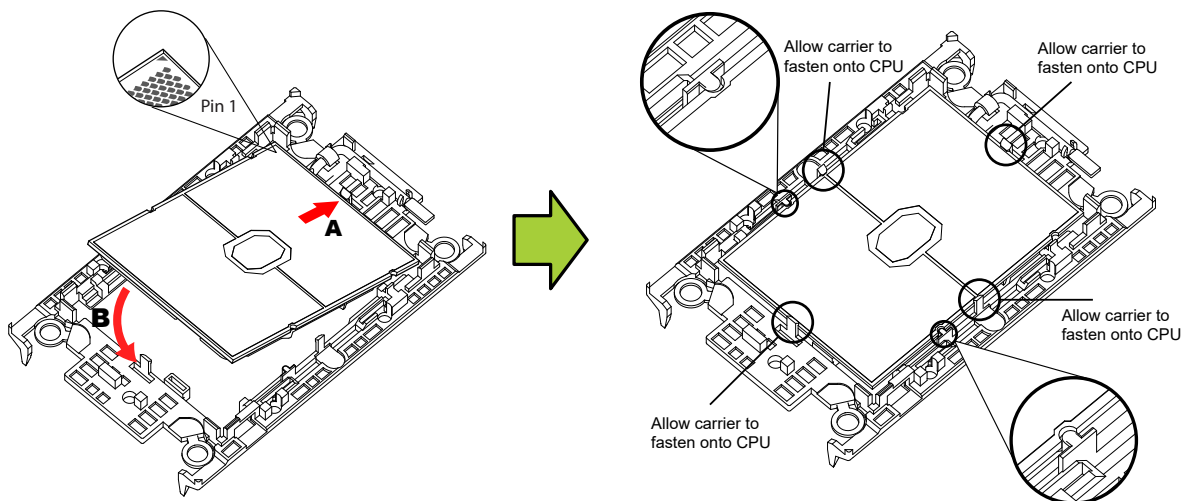
Creating the 3rd Generation Intel Xeon Scalable Processor Carrier Assembly

To install the processor into the processor carrier, follow the steps below:

1. Hold the processor with the LGA lands (gold contacts) facing up. Locate the small, gold triangle in the corner of the processor and the corresponding hollowed triangle on the processor carrier. These triangles indicate pin 1. The triangles can be found on the top and bottom of the processor. See the images below.
2. Using the triangles as a guide, carefully align and place Point A of the processor into the carrier. Then gently snap in the other side of the carrier for the processor to fasten into Point B.

 **Note:** The 3rd Generation Intel Xeon Scalable Processor carrier contains four metal rings on each corner.

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



Processor Carrier Assembly

 **Note:** The following CPU carriers have been successfully tested in our labs and are available from Supermicro. Please order the CPU carriers with the CPU heatsink.

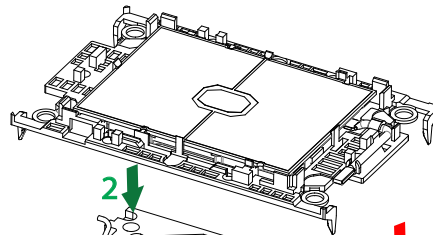
Intel 3rd Generation Xeon Scalable Processors	SKT-1205L-P4IC-FXC
	SKT-1205L-P4IC-TYC

Assembling the Processor Heatsink Module

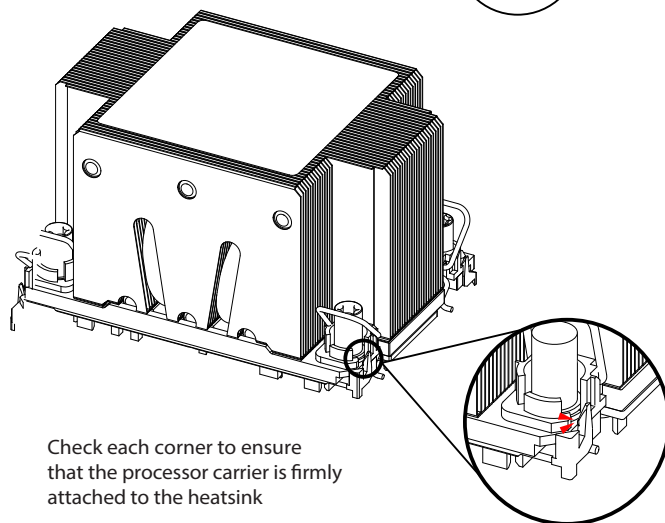
After creating the processor carrier assembly for the processor, mount it onto the heatsink to create the processor heatsink module (PHM):

1. Note the label on top of the heatsink, which marks the heatsink mounting holes as 1, 2, 3, and 4. If this is a new heatsink, the thermal grease has been pre-applied on the underside. Otherwise, apply the proper amount of thermal grease.
2. Turn the heatsink over with the thermal grease facing up. Hold the processor carrier assembly so the processor's gold contacts are facing up, then align the triangle on the assembly with hole 1 of the heatsink. Press the processor carrier assembly down. The plastic clips of the assembly will lock outside of holes 1 and 2, while the remaining clips will snap into their corresponding holes.
3. Examine all corners to ensure that the plastic clips on the processor carrier assembly are firmly attached to the heatsink.

Processor Carrier Assembly
(Upside Down)



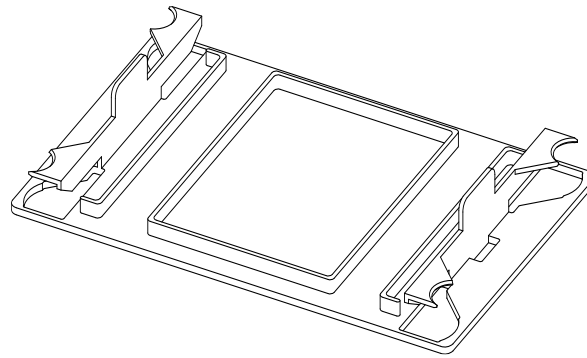
Heatsink
(Upside Down)



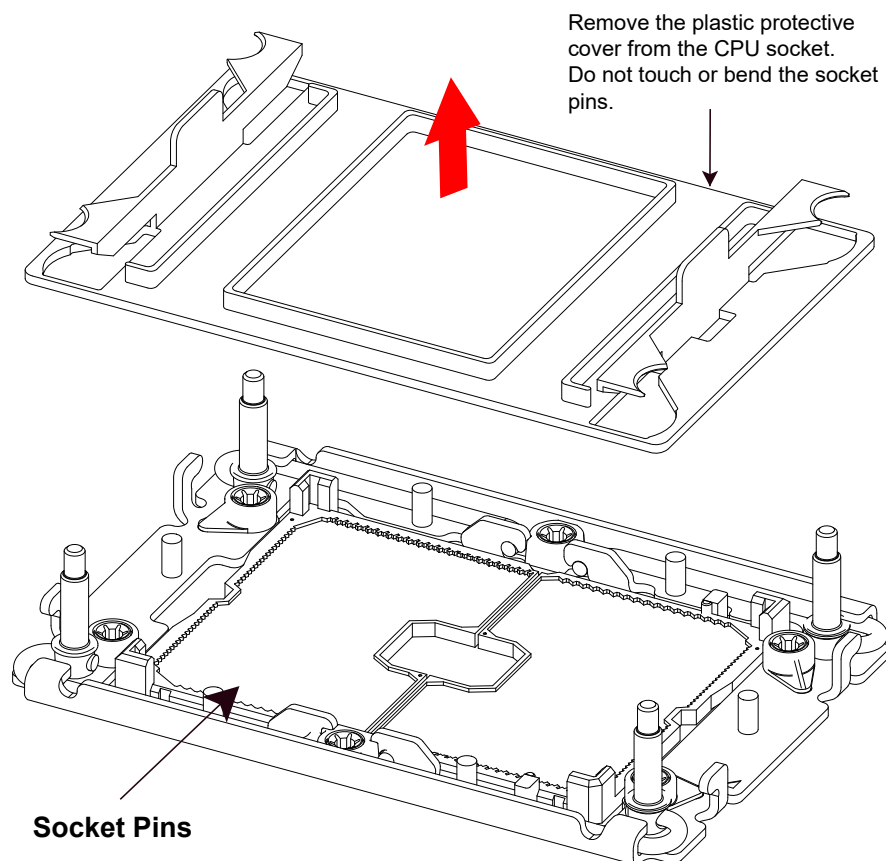
Check each corner to ensure that the processor carrier is firmly attached to the heatsink

Preparing the CPU Socket for Installation

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



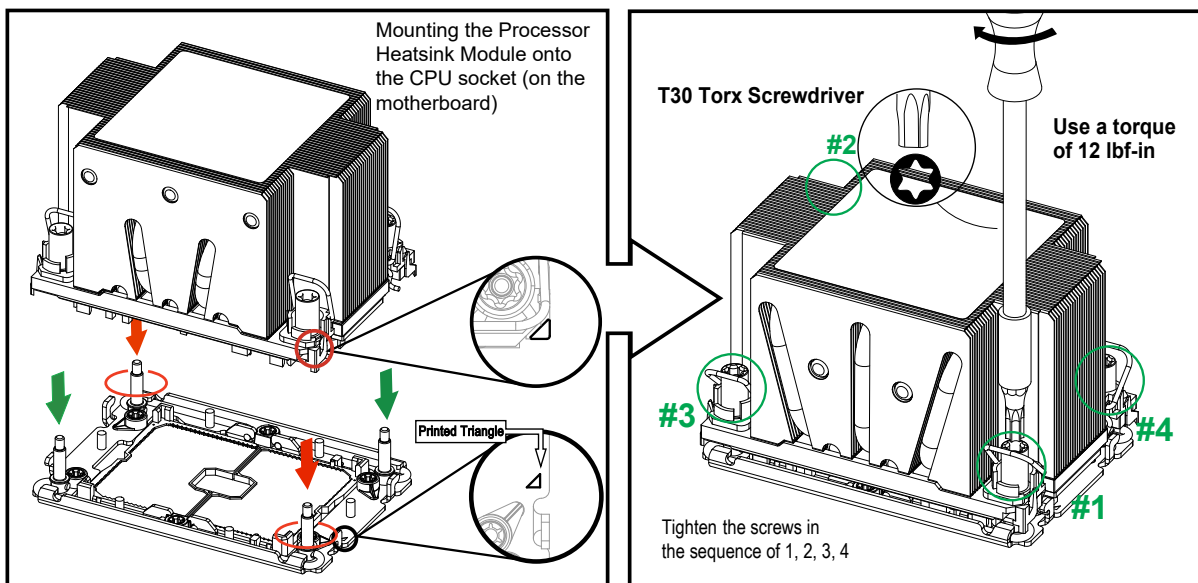
CPU Socket with Plastic Protective Cover



Installing the Processor Heatsink Module

After assembling the Processor Heatsink Module (PHM), install it onto the CPU socket:

1. Align hole 1 of the heatsink with the printed triangle on the CPU socket. See the left image below.
2. Make sure all four holes of the heatsink are aligned with the socket before gently placing the heatsink on top.
3. With a T30 Torx-bit screwdriver, gradually tighten screws #1 - #4 to ensure even pressure. The order of the screws is shown on the label on top of the heatsink. To avoid damaging the processor or socket, do not use a force greater than 12 lbf-in when tightening the screws.
4. Examine all corners to ensure that the PHM is firmly attached to the socket.

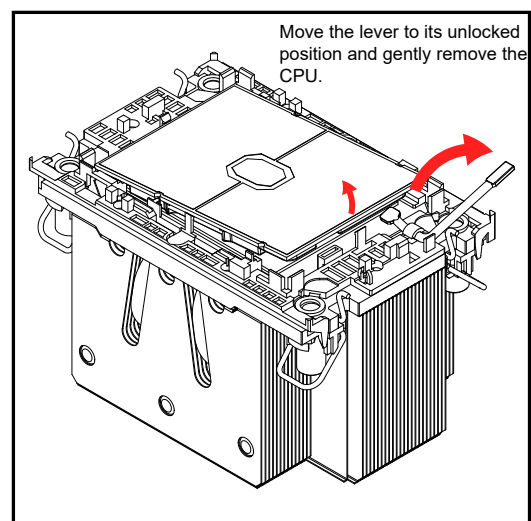
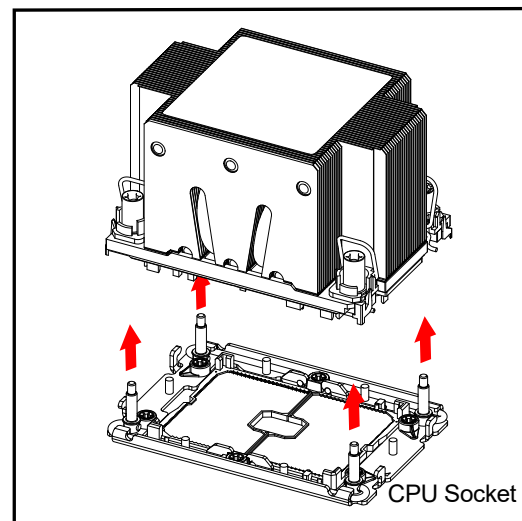
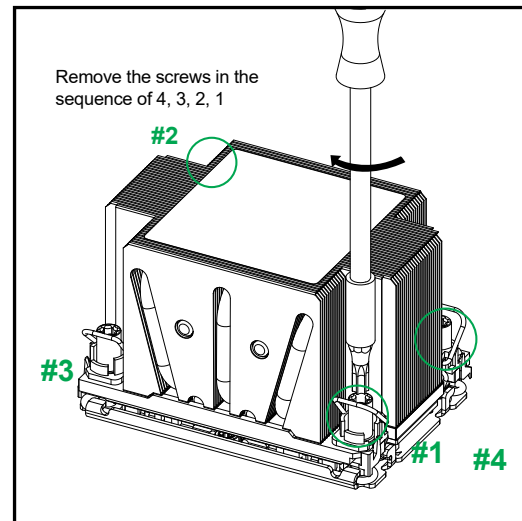


Removing the Processor Heatsink Module

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

Then follow the steps below:

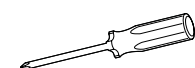
1. Use a T30 Torx-bit screwdriver to loosen the four screws in a backwards sequence of #4, #3, #2, and #1.
2. Gently lift the PHM upwards to remove it from the socket.
3. Move the lever to its unlocked position and gently remove the CPU.



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



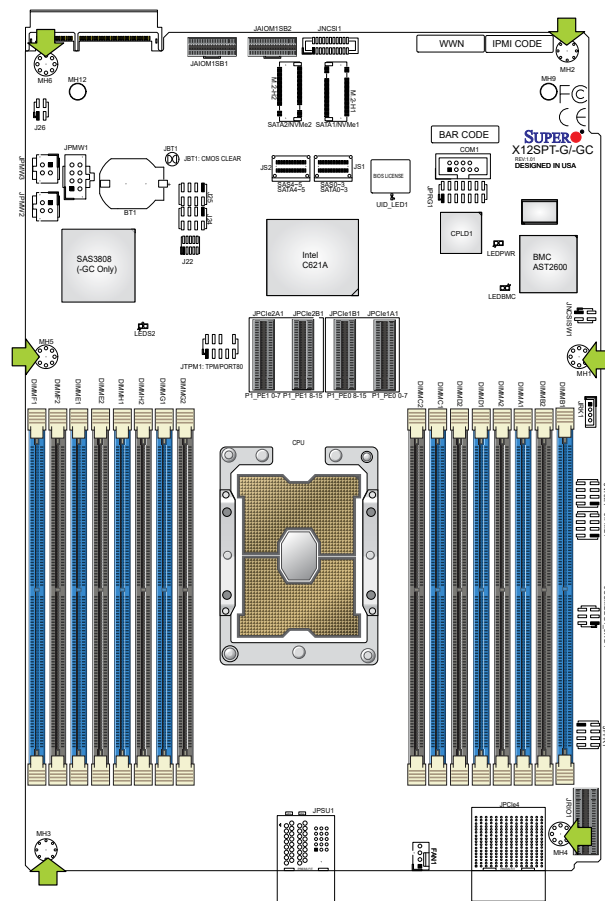
**Phillips
Screwdriver
(1)**



**Phillips Screws
(6)**



**Standoffs (6)
Only if Needed**



Location of Mounting Holes



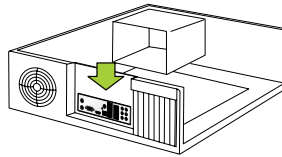
Note 1: To avoid damaging the motherboard and its components, please do not use a force greater than 8 lbf-in on each mounting screw during motherboard installation.



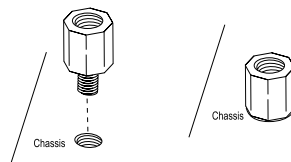
Note 2: Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

Installing the Motherboard

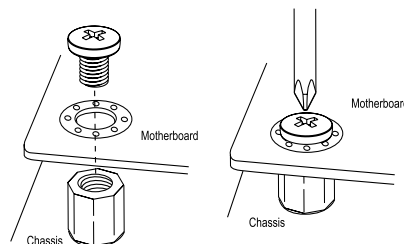
1. Install the I/O shield into the back of the chassis, if applicable.



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 X12SPT-G/-GC supports 4 TB of ECC RDIMM 3DS and LRDIMM 3DS DDR4 memory with speeds of 3200/2933/2666 MHz in 16 memory slots and up to 2 TB Intel Optane PMem 200 Series with speeds up to 3200 MHz (see the notes below).



Note 1: Intel® Optane™ Persistent Memory (PMem) 200 Series is supported by the 3rd Gen Intel Xeon Scalable (83xx/63xx/53xx/4314 Series) 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	8 GB	16 GB	3200	3200
	SRx4	16 GB	32 GB		
	DRx8	16 GB	32 GB		
	DRx4	32 GB	64 GB		
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

Key Parameters for DIMM Configurations	
Parameters	Possible Values
Number of Channels	8
Number of DIMMs per Channel	1DPC (1 DIMM Per Channel) or 2DPC (2 DIMMs Per Channel)
DIMM Type	RDIMM (w/ECC), 3DS RDIMM, LRDIMM, 3DS LRDIMM
DIMM Construction	non-3DS RDIMM Raw Cards: A/B (2Rx4), C (1Rx4), D (1Rx8), E (2Rx8) 3DS RDIMM Raw Cards: A/B (4Rx4) non-3DS LRDIMM Raw Cards: D/E (4Rx4) 3DS LRDIMM Raw Cards: A/B (8Rx4)

Memory Population Table (w/16 Slots)

DDR4 Memory Population Table for X12SP 16-DIMM Motherboards	
Number of DIMMs	Memory Population Sequence
1	P1-DIMMA1
2 (Note)	P1-DIMMA1/P1-DIMME1
4 (Note)	P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1
6 (Note)	P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1
8 (Note)	P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1/P1-DIMMD1/P1-DIMMH1
12 (Note)	P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1/P1-DIMMA2/P1-DIMME2/P1-DIMMC2/P1-DIMMG2/P1-DIMMB2/P1-DIMMF2
16 (Note)	P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1/P1-DIMMD1/P1-DIMMH1/P1-DIMMA2/P1-DIMME2/P1-DIMMC2/P1-DIMMG2/P1-DIMMB2/P1-DIMMF2/P1-DIMMD2/P1-DIMMH2



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

PMem 200 Series Population table for X12SPT-G/-GC Motherboards (w/16 Slots)



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

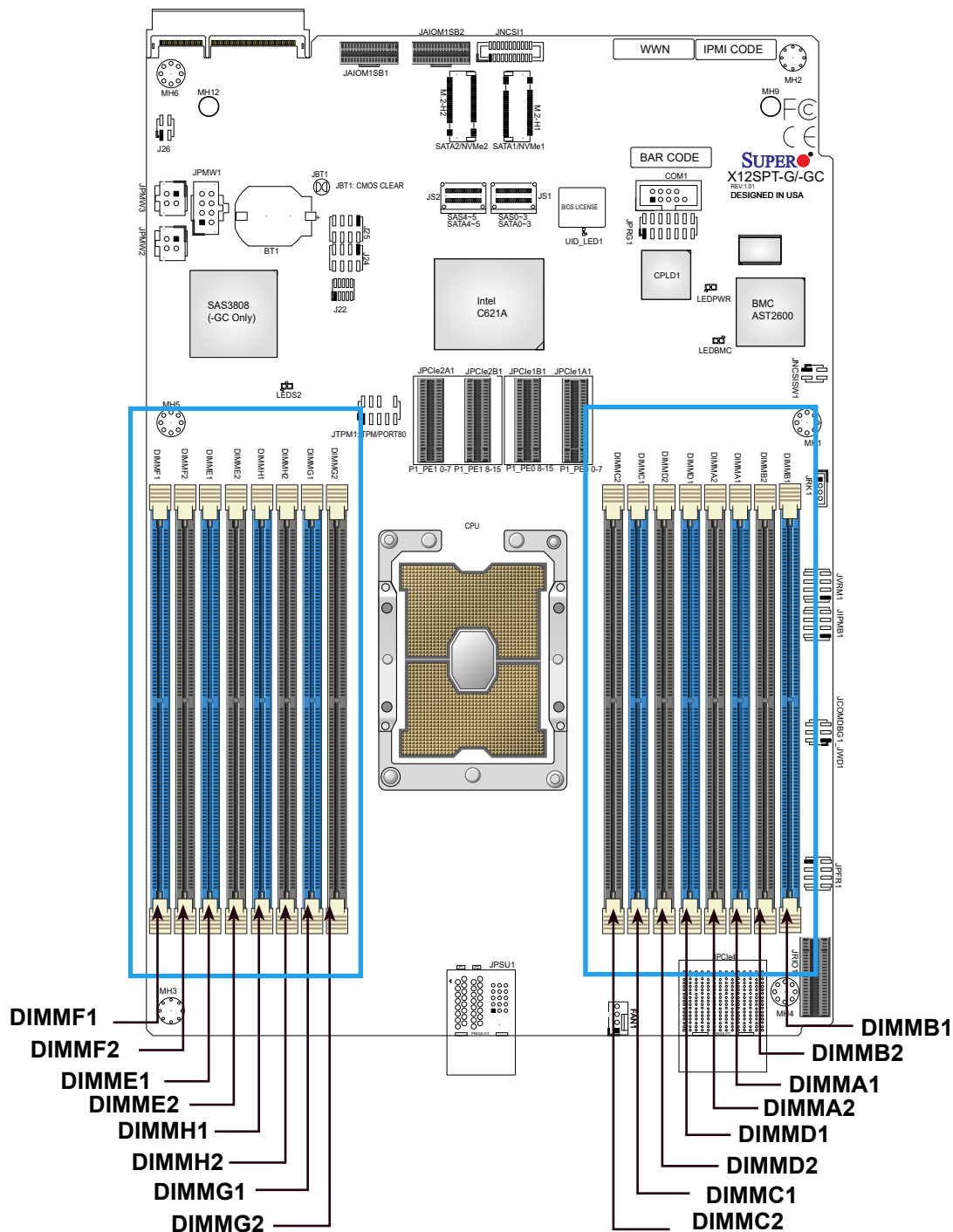
PMem 200 Series Population Table for X12SPT 16-DIMM Motherboards (within 1 CPU socket)																		
DDR4+ PMem	Mode	AD Interleave	P1-DIMMF1	P1-DIMMF2	P1-DIMME1	P1-DIMME2	P1-DIMMH1	P1-DIMMH2	P1-DIMMG1	P1-DIMMG2	P1-DIMMC2	P1-DIMMC1	P1-DIMMD2	P1-DIMMD1	P1-DIMMA2	P1-DIMMA1	P1-DIMMB2	P1-DIMMB1
4+4	AD 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	-	PMem	-	DDR4	-	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	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	PMem	DDR4	-	DDR4
			DDR4	-	DDR4	-	DDR4	-	DDR4	-	PMem	DDR4	-	DDR4	-	DDR4	-	DDR4
8+1	AD	One - x1	DDR4	-	DDR4	-	DDR4	-	DDR4	-	-	DDR4	-	DDR4	-	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	PMem	-	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	-	-	PMem	DDR4	DDR4	DDR4
			DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	PMem	-	-	PMem	DDR4	DDR4	DDR4	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.

General Guidelines for Optimizing Memory Performance

- It is recommended to use DDR4 memory of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- To achieve the best memory performance, a balanced memory population is recommended.

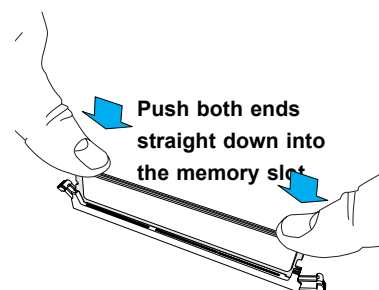
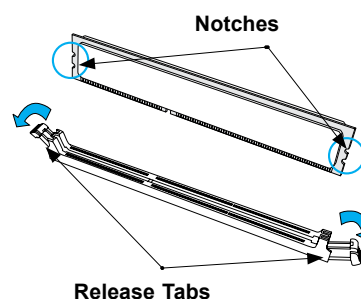
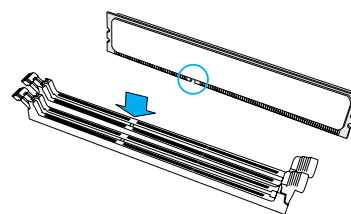
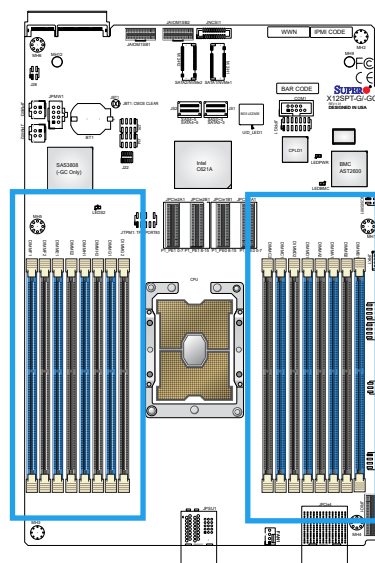


DIMM Installation

1. Insert DIMM modules in the following order: DIMMC1, DIMMD1, DIMMA1, DIMMB1, DIMMG1, DIMMH1, DIMME1, DIMMF1, and insert the desired number of DIMMs into the memory slots based on the Recommended Memory Population Guide table on page 30.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.
3. Align the key of the DIMM module with the receptive point on the memory slot.
4. Align the notches on both ends of the module against the receptive points on the ends of the slot.
5. Push both ends of the module straight down into the slot until the module snaps into place.
6. Press the release tabs to the lock positions to secure the DIMM module into the slot.

DIMM Removal

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



2.5 Rear I/O Ports

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

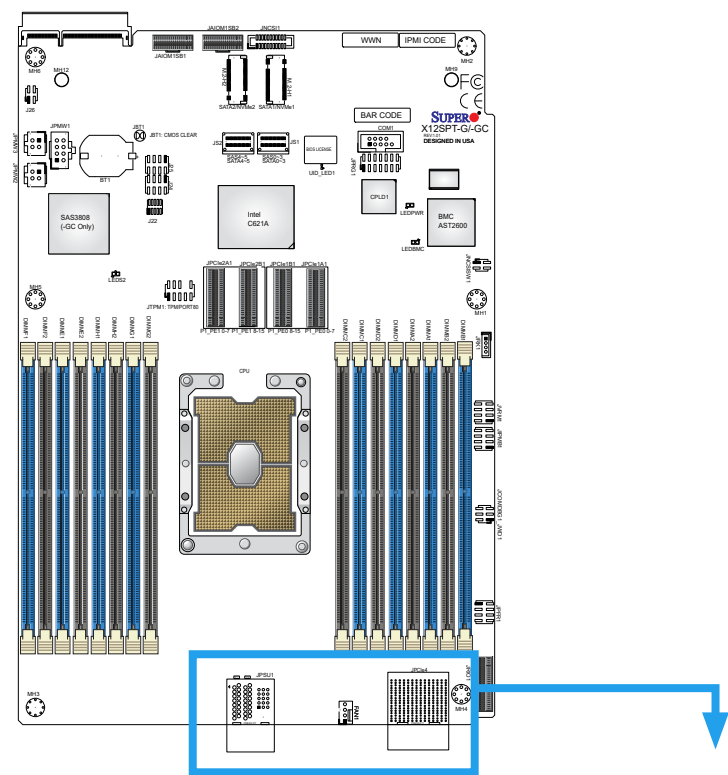
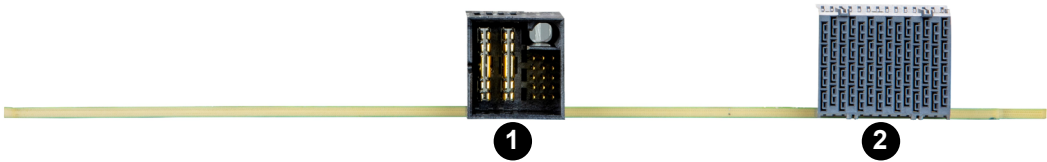


Figure 2-1. I/O Port Locations and Definitions



Rear I/O Ports	
#	Description
1	JPSU1
2	JPCIE4

2.6 Connectors

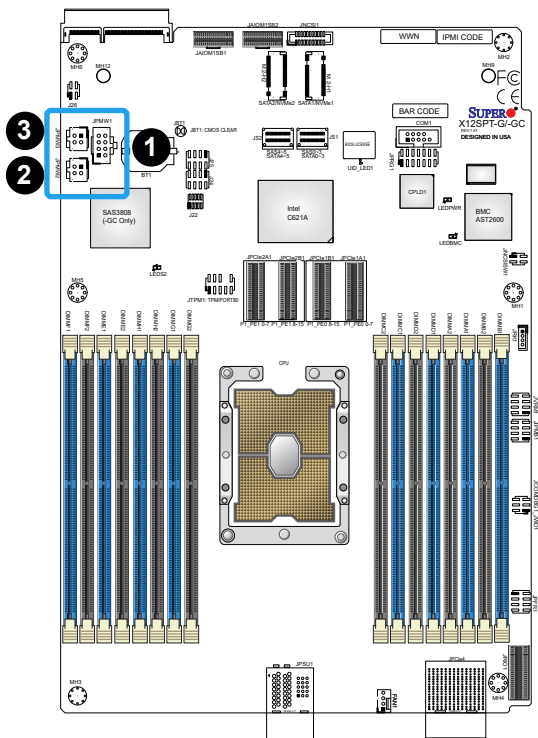
Power Connections

Power Connectors

JPMW1 is the 8-pin power connector for GPU and NVMe power. JPMW2 and JPMW3 are the 4-pin 12 V DC power connectors on the motherboard that provide adequate power supply to your system.

8-pin GPU Power Pin Definitions	
Pin#	Definition
1-4	GND
5-6	12 V
7-8	5 V

4-pin Power Pin Definitions	
Pin#	Definition
1-2	GND
3-4	12 V



- 1. 8-Pin GPU Power
- 2. 4-Pin Power
- 3. 4-Pin Power

Headers

COM Header

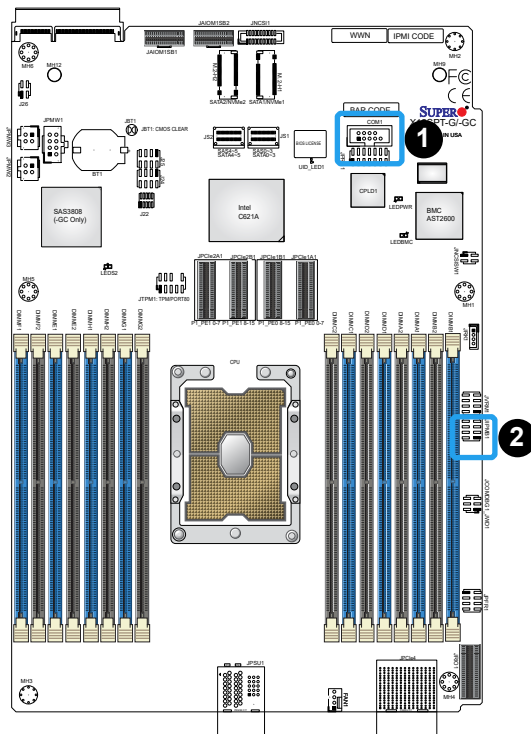
The motherboard has one COM header (COM1) that provides a serial connection.

COM Header (COM1) Pin Definitions			
Pin#	Definition	Pin#	Definition
1	DCD	2	DSR
3	RXD	4	RTS
5	TXD	6	CTS
7	DTR	8	RI
9	Ground	10	N/A

4-pin External BMC I²C Header

A System Management Bus header for IPMI 2.0 is located at JIPMB1. Connect a cable to this header 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. COM Header
2. External BMC I²C Header

Fan Header

There is one 4-pin fan header (FAN1) on the motherboard. The 4-pin fan header is 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.

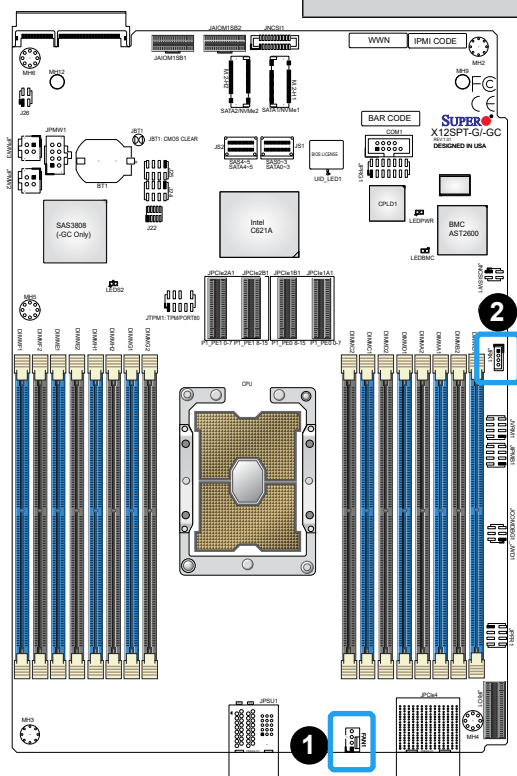
Fan Header Pin Definitions	
Pin#	Definition
1	Ground (Black)
2	2.5 A/+12 V (Red)
3	Tachometer
4	PWM_Control

Intel RAID Key Header

The JRK1 header allows you to enable RAID functions for NVMe connections. Refer to the table below for pin definitions and supported VROC key model.

Intel RAID Key Header Pin Definitions	
Pin#	Definition
1	GND
2	PU 3.3 V Stdby
3	GND
4	PCH RAID KEY

Intel RAID Key		
VROC Type	Key	RAID Levels
VROC Intel SSD Only	AOC-VROCINTMOD	Intel VROC, RAID 0, 1, 5, 10 (Intel SSD Only)
VROC Premium	AOC-VROCINTMOD	Intel VROC Premium, RAID 0, 1, 5, 10
VROC Standard	AOC-VROCINTMOD	Intel VROC Standard, RAID 0, 1, 10



1. FAN1
2. Intel RAID Key Header

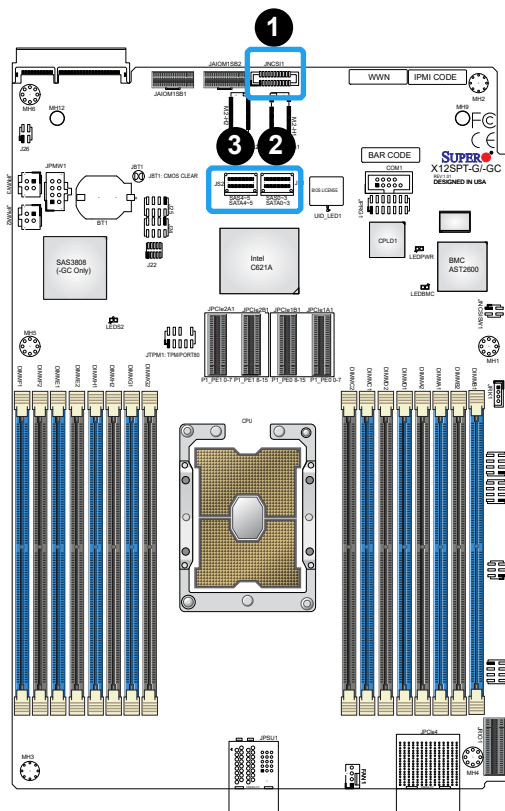
NC-SI Connector

A Network-Controller Sideband Interface (NC-SI) header is located at JNCSI1 on the motherboard. The NCSI header is used to connect a Network Interface Card (NIC) to the motherboard so that the BMC is able to poll the temperature reading from it.

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

SAS and SATA Ports

This motherboard has two slimSAS connectors located at JS1 and JS2. They can support either six SAS (SAS0-5) for X12SPT-GC or six SATA (SATA0-SATA5) for X12SPT-G. X12SPT-GC will provide SAS3808 controller on board to support SAS.

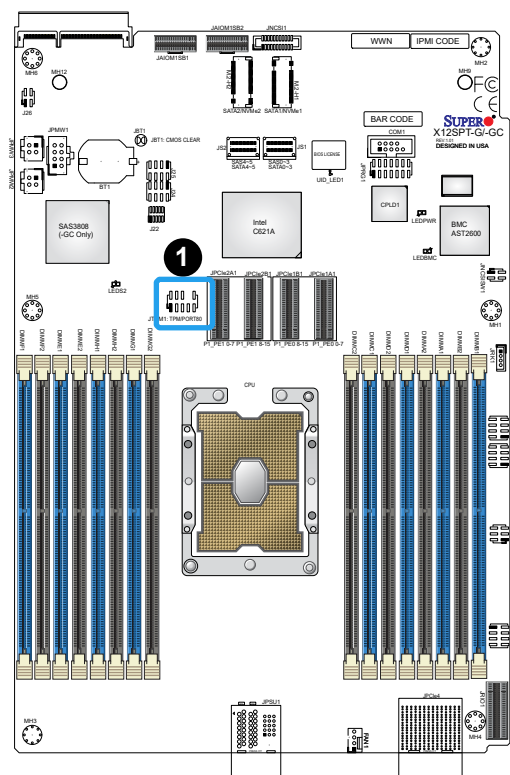


1. JNCSI1
2. JS1
3. JS2

TPM/Port 80 Header

A Trusted Platform Module (TPM)/Port 80 header is located at JTPM1 to provide TPM support and Port 80 connection. Use this header to enhance system performance and data security. Refer to the table below for pin definitions. Please go to the following link for more information on the TPM: <http://www.supermicro.com/manuals/other/TPM.pdf>.

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



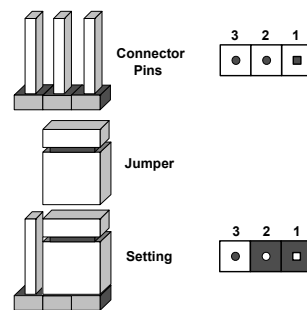
1. TPM Module

2.7 Jumper Settings

How Jumpers Work

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

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



CMOS Clear

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

To Clear CMOS

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

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

Do not use the PW_ON connector to clear CMOS.

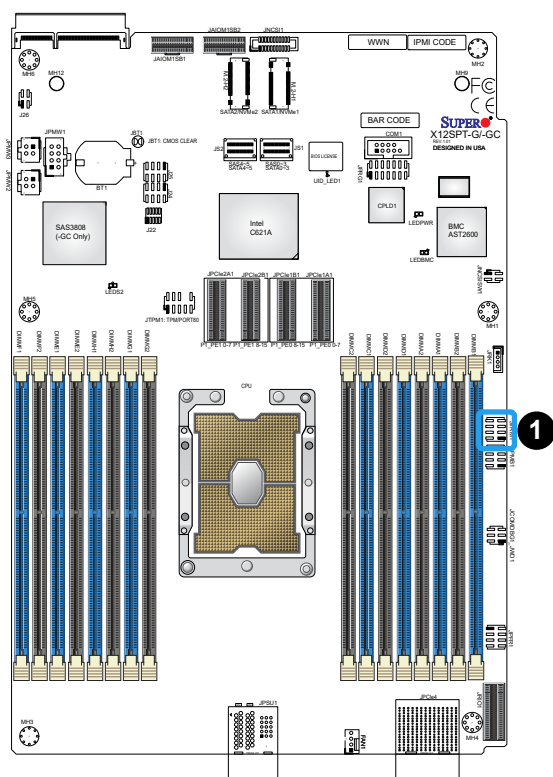


JBT1 contact pads

VRM SMBus Jumper

JVRM1 is a voltage regulator module (VRM) SMBus jumper. Use this jumper to configure the CPU and memory VRM controllers. Setting JVRM1 to pins 1-3 and 2-4 will configure the BMC as the VRM controller. Setting JVRM1 to pins 3-5 and 4-6 will configure the PCH as the VRM controller. Refer to the table below for pin definitions.

VRM SMBus Jumper Pin Definitions			
Pin#	Definition	Pin#	Definition
1	SMBDAT_VRM	2	SMBCLK_VRM
3	SDA_VRM	4	SCL_VRM
5	PCH_SMBDAT	6	PCH_SMBCLK
7	Ground	8	Ground



1. JVRM1

2.8 LED Indicators

BMC Heartbeat LED

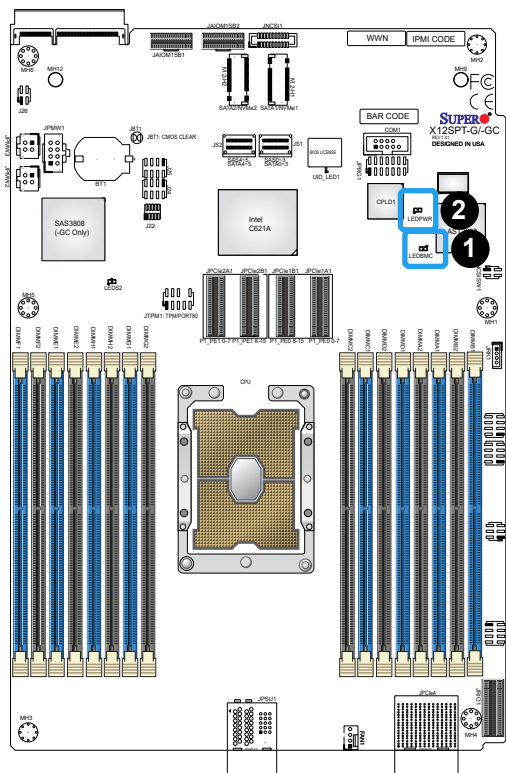
LEDBMC is the BMC Heartbeat LED. When the LED is blinking green, BMC is working. Refer to the table below for the LED status.

BMC Heartbeat LED	
LED Color	Definition
Green: Blinking	BMC Normal

Onboard Power LED

LEDPWR is the onboard Power LED. When this LED is on, the system is on. Turn off the system and unplug the power cord before removing or installing components. Refer to the table below for more information.

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



1. Onboard Power LED
2. BMC Heartbeat LED

LEDS2 is the SAS Error LED. When the LED is solid red, there is an error with the SAS. Refer to the table below for the LED status.

A Unit Identifier (UID) LED indicator is located on the motherboard. The UID Indicator provides easy identification of a system unit that may be in need of service.

--	--



1. SAS Error LED
2. UID_LED1

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 115 V/230 V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. Check the CPU socket for bent pins and make sure the CPU is fully seated.
6. 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.

System Boot Failure

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

1. Check the screen for an error message.
2. Clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper (JBT1). Restart the system. Refer to Section 2-8 in Chapter 2.
3. Remove all components from the motherboard and turn on the system with only one DIMM module installed. If the system boots, turn off the system and repopulate the components back into the system to retest. Add one component at a time to isolate which one may have caused the system boot issue.

Memory Errors

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

1. Make sure that the memory modules are compatible with the system and are properly installed. See 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 DIMMs 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 2 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.
3. If the above steps do not fix the setup configuration problem, contact your vendor for repairs.

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 a USB flash or media drive.
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: The motherboard supports up to 4 TB of ECC RDIMM 3DS and LRDIMM 3DS DDR4 memory with speeds of up to 3200 MHz in 16 memory slots. To enhance memory performance, do not mix memory modules of different speeds and sizes. Please follow all memory installation instructions given on Section 2-4 in Chapter 2.

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.

Unzip the BIOS file onto a bootable USB device and then boot into the built-in UEFI Shell and type "flash.nsh <BIOS filename><BMC Username><BMC Password>" to start the BIOS update. The flash script will invoke the SUM (EFI) tool automatically to perform the BIOS update, beginning with uploading the BIOS image to BMC. After uploading the firmware, the system will reboot to continue the process. The BMC will take over and continue the BIOS update in the background. The process will take 3-5 minutes.

Warning: Do not shut down or reset the system while updating the BIOS to prevent possible system boot failure! Please read the X12_AMI_BIOS_Upgrade_README file carefully before you perform the BIOS update.

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.

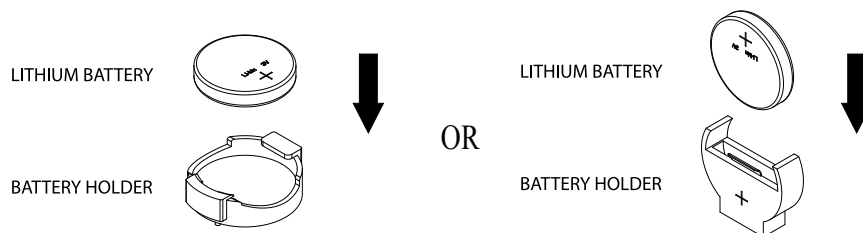
Proper Battery Disposal

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

1. To install an onboard battery, follow steps 1 and 2 above and continue below:
2. Identify the battery's polarity. The positive (+) side should be facing up.
3. 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 X12SPT-G/-GC motherboard. The BIOS is stored on a chip and can be easily upgraded using the BMC WebUI or the SUM utility.



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

Starting the Setup Utility

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

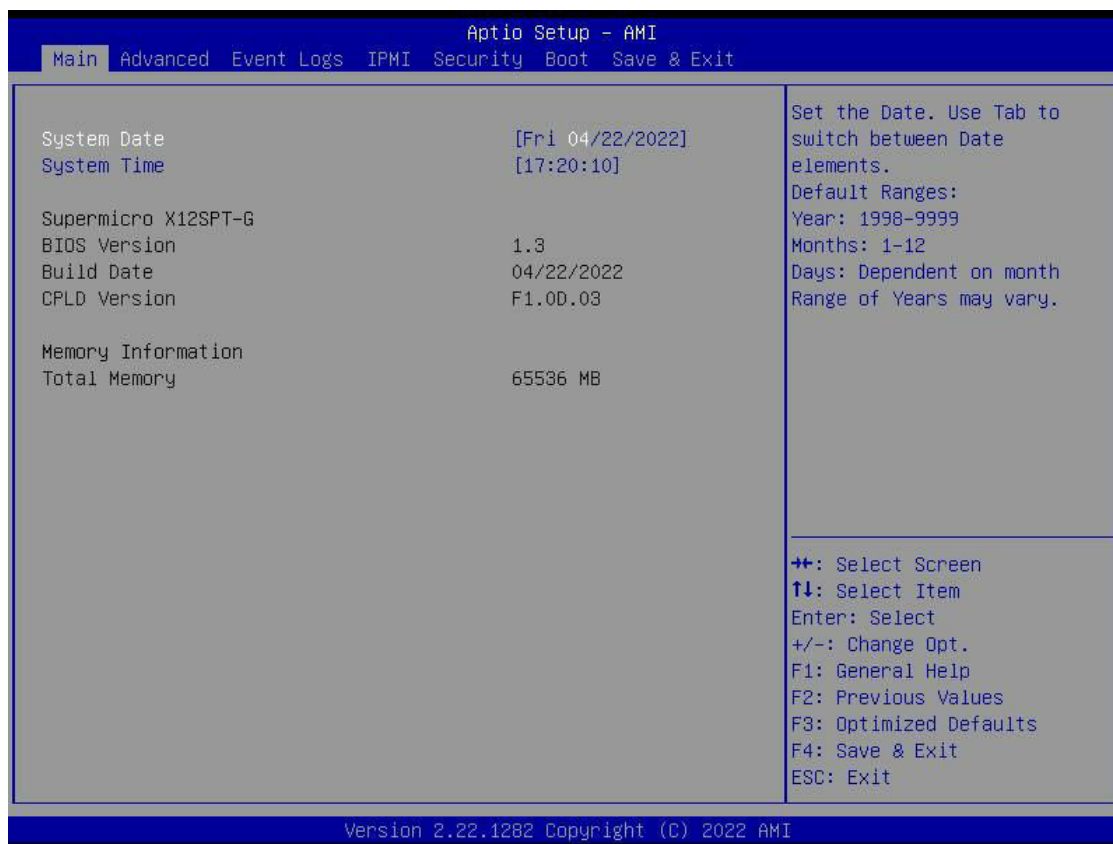
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

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

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

4.2 Main Setup

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



System Date/System Time

Use this feature to change the system date and time. To change system date and time settings, highlight System Date or System Time using the arrow keys and enter new values using the keyboard. Press the <Tab> key or the arrow keys to move between fields. The date must be entered in Day 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 the Real Time Clock (RTC) reset.

Supermicro X12SPT-G/GC

BIOS Version

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

Build Date

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

CPLD Version

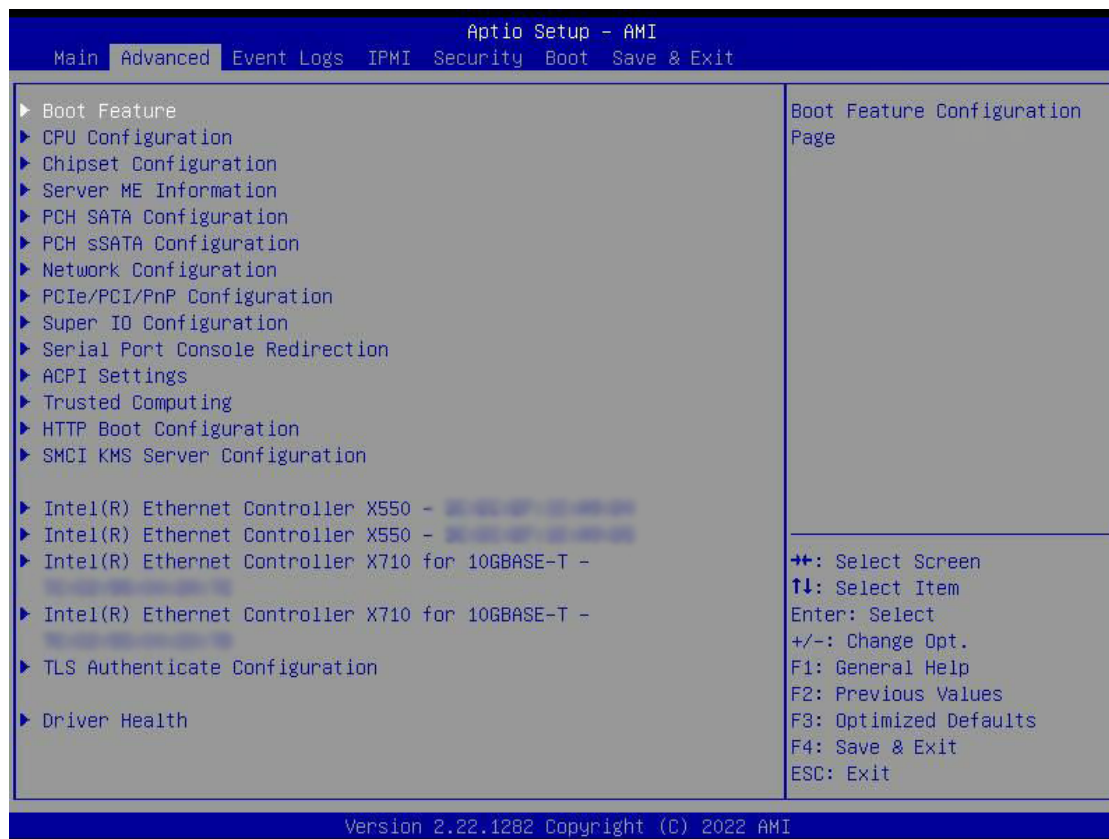
This feature displays the version of the Complex-Programmable Logical Device (CPLD) used in the system.

Memory Information**Total Memory**

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

4.3 Advanced Setup Configurations

Use the arrow keys to select the Advanced menu and press <Enter> to access the menu features.



Warning: Take Caution when changing the Advanced settings. An incorrect value may cause the system to malfunction. When this occurs, restore the setting to the manufacturer default setting.

► Boot Feature

Quiet Boot

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



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

Option ROM Messages

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

Bootup NumLock State

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

Wait For "F1" If Error

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

INT19 Trap Response

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

Re-try Boot

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

Power Configuration**Watch Dog Function**

Select Enabled to allow the Watch Dog timer to reboot the system when it is inactive for more than 5 minutes. The options are **Disabled** and Enabled.

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

This feature allows you to determine how the watch dog function can be triggered. The options are **Reset** and NMI.

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

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

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

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

Restore on AC Power Loss

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

Power Button Function

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

►CPU Configuration

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

Processor Configuration

The following CPU information will be displayed:

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

►CPU1 Core Disable Bitmap

Available Bitmap: The available Bitmap will be displayed.

Core Disable Bitmap(Hex)

Enter 0 to enable all CPU cores. Enter FFFFFFFFFF to disable all CPU cores. Note that at least one core per CPU must be enabled. Disabling all cores is not allowed. The default option is **0**.

Hyper-Threading [ALL]

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

Hardware Prefetcher

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

Adjacent Cache Prefetch

Select Enable for the CPU to prefetch both cache lines for 128 bytes as comprised. Select Disable for the CPU to prefetch both cache lines for 64 bytes. The options are **Enable** and Disable. (**Note:** Refer to Intel's website for detailed information.)

DCU Streamer Prefetcher

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

DCU IP Prefetcher

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

LLC Prefetch

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

Extended APIC (Extended Advanced Programmable Interrupt Controller)

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



Note: This will enable VT-d automatically if x2APIC is enabled.

Intel Virtualization Technology

Select Enable to use Intel Virtualization Technology to allow one platform to run multiple operating systems and applications in independent partitions, creating multiple virtual systems in one physical computer. The options are Disable and **Enable**.

Enable SMX

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

PPIN Control

Select Unlock/Enable to use the Protected-Processor Inventory Number (PPIN) in the system. The options are Lock/Disable and **Unlock/Enable**.

AES-NI

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

TME, TME-MT, TDX

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 (TME)" is set to Enabled)

This feature displays the maximum TME-MT keys.

Software Guard Extension (SGX)

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 the BIOS provides software with the key blobs, which are generated for each CPU package. The options are **Disabled** and **Enabled**.

Limit CPU PA to 46 bits

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

►Advanced Power Management Configuration

Power Technology

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

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

SpeedStep (P-States)

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

AVX P1

Use this feature to set the appropriate TDP level for the system. The Intel Advanced Vector Extensions (Intel AVX) P1 feature allows you to specify the base P1 ratio for Streaming SIMD Extensions (SSE) and AVX workloads and to pre-grant a license level. The options are **Normal**, Level 1, and Level 2.

Dynamic SST-PP (Speed Select Technology-Performance Profile) (Available when "SpeedStep (P-States)" is set to Enable and when CPU supports this feature)

If this feature is set to Enable, it allows you to configure Intel SST-PP features, including Base, Configuration 3, and Configuration 4 settings under various processor working conditions. The options are **Disable** and Enable.

Intel SST-PP (Speed Select Technology-Performance Profile) (Available when "SpeedStep (P-States)" is set to Enable and "Dynamic SST-PP" is set to Disable)

This feature allows you to choose from two additional Base-Frequency conditions maximum for CPU P State Control. The options are **Base**, Config 3, and Config 4.

The following information is displayed when "SpeedStep (P-States)" is set to Enable:

- Intel SST-PP / Base / Config 3 / Config 4
- Core Count
- Current P1 Ratio [0]
- Package TDP (W)
- Tjmax

Activate SST-BF

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

Configure SST-BF (Available when "Activate SST-BF" is set to Enable)

Enabling this feature allows the BIOS to configure SST-BF High Priority Cores. The options are Disable and **Enable**.

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

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

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

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

CPU Flex Ratio Override (Available when "SpeedStep (P-States)" is set to Enable and when CPU supports this feature)

Select Enable to override the CPU Flex-Ratio setting, which is the minimum multiplier that allows the computer to clock. The options are **Disable** and Enable.

CPU Core Flex Ratio (Available when "CPU Flex Ratio Override" is set to Enable and when CPU supports this feature)

Use this feature to configure the Core Ratio Multiplier settings for non-Turbo mode processors. The default setting is **23**.

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

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

►Frequency Prioritization**RAPL (Running Average Power Limit) Prioritization**

This feature allows to prioritize running average power limit. The options are **Disable** and Enable.

►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, power to all caches is turned off. The options are Disable, Enable, and **Auto**.

Enhanced Halt State (C1E)

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

►Package C State Control

Package C State

Use this feature to optimize and reduce CPU package power consumption in idle mode. Note that the changes you've made in this setting will affect all CPU cores or the circuits of the entire system. The options are C0/C1 state, C2 state, C6 (non Retention) state, 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%, 31.25%, 37.5%, 43.75%, 50.0%, 56.25%, 62.5%, 68.75%, 75.0%, 81.25%, 87.5%, and 93.75%.

►Chipset Configuration

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

►North Bridge

This submenu contains features that allows you to configure Intel North Bridge parameters.

►Uncore Configuration

This section allows you to configure the following Uncore settings:

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

Degrade Precedence

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

Link L0p Enable

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

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

Link L1 Enable

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

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

XPT Remote Prefetch

Select Enable to support Extended Prediction Table (XPT) 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

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

Local/Remote Threshold

Use this feature to set the threshold for the Interrupt Request (IRQ) signals which handle hardware interruptions. The options are Disable, **Auto**, Low, Medium, and High.

IO Directory Cache (IODC)

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

SNC (Sub NUMA)

Select Enable to use "Sub NUMA Clustering" (SNC) which supports full SNC (2-cluster) interleave and 1-way IMC interleave. Select Auto for 1-cluster or 2-cluster support depending on the status of Integrated Memory Controller (iMC) Interleaving. The options are **Disable** and Enable SNC2 (2-clusters).

XPT Prefetch

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

Snoop Throttle Configuration

Use this feature to set the level of snoop throttle for the PCH which will determine how much speed to decrease in operation when the system is in the snoop state. 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 (A to S)

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

LLC Dead Line Alloc

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

►Memory Configuration

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

Enhanced PPR

Use this feature to enable or disable DRAM Test and Postpackage Repair function during POST. The options are **Disable** and Enable.

Enforce POR (Plan of Record)

Select POR to enforce POR restrictions for DDR4 memory frequency and voltage programming. The options are **POR** and Disable.

PPR Type

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

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

Select Enable to enable data scrambling for Intel Optane Persistent Memory (PMem) modules to enhance memory data security. Select Auto to use the Memory Reference Code (MRC) defaulting setting for PMem memory data scrambling. 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 Configuration

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

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 "ADDDC Sparing" below is set to Disabled)

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

UEFI ARM Mirror (Available when ADDDC Sparing is set to Enabled)

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

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

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

Correctable Error Threshold

This feature allows you to enter the threshold value for correctable memory errors. The default setting is **512**.

The following information is displayed:

- Leaky Bucket Low Bit
- Leaky Bucket High Bit

Partial Cache Line Sparing PCLS

Select Enabled to support partial cache line sparing which will allow partial of data contained in a cache line to be copied in the cache memory for safe-keeping/data security. The options are Disabled and **Enabled**.

ADDDC (Adaptive Double Device Data Correction) Sparing

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

Patrol Scrub

Patrol Scrubbing is a process that allows the CPU to correct correctable memory errors detected in a memory module and send the corrections to the 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, Enabled, and **Enable at End of POST** (Power_On Self Test).

► IIO Configuration

► CPU1 Configuration

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

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

► Port 1A / AIOM SLOT1 PCIe 4.0 x16 / Port 1C / Port 1D / Port 2A / AOC-GTG-i2T / Port 4C / Port 5A

Link Speed

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

The following information is displayed:

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

Data Link Feature Exchange

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

PCIe Port Max Payload Size

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

► IOAT Configuration

Disable TPH

The TLP Processing Hint (TPH) is used for data-tagging with a destination ID and a few important attributes. It can send critical data to a particular cache without writing through to memory. Select No for TLP Processing Hint support which will allow a "TLP request" to provide "hints" to help optimize the processing of each transaction occurred in the target memory space. The options are **No** and Yes.

Prioritize TPH (TLP Processing Hint) (Available when "Disable TPH" is set to No)

Select Enable to prioritize the TPL requests that will allow the "hints" to be sent to help facilitate and optimize the processing of certain transactions in the system memory. The options are Enable and **Disable**.

Relaxed Ordering

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

►Intel® VT for Directed I/O (VT-d)**Intel® VT for Directed I/O (VT-d)**

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

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

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

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

If this feature is set to Yes, I/O DMA transfer remapping and device-generated interrupts will be supported. The options are **Auto**, Enable, and Disable.

►Intel® VMD Technology

This section describes the configuration settings for the Intel Volume Management Device (VMD) Technology.

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

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

NVMe Mode Switch

Select Auto to enable the VMD support for NVMe devices in the system when a VROC RAID Key is installed. Select Manual to change the NVMe mode for each port. Select VMD to enable the VMD support for each port. The options are Manual, VMD, and **Auto**.

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

VMD Config for PCH ports

Enable/Disable VMD

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

PCH Root Port 12 / PCH Root Port 16 (Available when "Enable/Disable VMD" is set to Enable)

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

VMD Config for IOU 0

Enable/Disable VMD

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

VMD port 1A / VMD port 1B / VMD port 1C / VMD port 1D (Available when "Enable/Disable VMD" is set to Enable)

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

Hot Plug Capable (Available when "Enable/Disable VMD" is set to Enable)

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

VMD Config for IOU 1

Enable/Disable VMD

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

VMD port 2A / VMD port 2B / VMD port 2C / VMD port 2D (Available when "Enable/Disable VMD" is set to Enable)

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

Hot Plug Capable (Available when "Enable/Disable VMD" is set to Enable)

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

VMD Config for IOU 3**Enable/Disable VMD**

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

VMD port 4A / VMD port 4B / VMD port 4C / VMD port 4D (Available when "Enable/Disable VMD" is set to Enable)

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

Hot Plug Capable (Available when "Enable/Disable VMD" is set to Enable)

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

VMD Config for IOU 4**Enable/Disable VMD**

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

Hot Plug Capable (Available when "Enable/Disable VMD" is set to Enable)

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

PCIe ASPM Support (Global)

Active-state power management (ASPM) is a power management mechanism for PCI Express devices to garner power savings while otherwise in a fully active state. The options are **Disable** and Enable.

IIO eDPC (Enhanced Downstream Port Containment) Support

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

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

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

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

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

► South Bridge

Select this submenu and press <Enter>. The following South Bridge information will display:

- USB Module Version
- USB Devices

Legacy USB Support

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

XHCI Hand-Off

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

Port 60/64 Emulation

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

PCIe PLL SSC

Select Enabled for PCH PCIe Spread Spectrum Clocking support. This feature 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 (Management Engine) Configuration

This submenu displays the following general ME configuration settings:

- Oper. (Operation) Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1
- ME Firmware Status #2
- Current State
- Error Code

►PCH SATA Configuration

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 "SATA Controller" is set to Enable)

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

SATA RSTe Boot Info (Available when "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**.



Note: For this feature to work properly, set the CSM Storage OPRM policy to Legacy.

Support Aggressive Link Power Management

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

SATA RAID Option ROM/UEFI Driver (Available when "Configure SATA as" is set to RAID)

Select EFI to load the EFI driver for system boot. Select Legacy to load a legacy driver for system boot. The options are Disable, **EFI**, and Legacy.

SATA Port 0 - SATA Port 7

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 you specified to spin up one at a time at boot 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 you specified should be connected to a Solid State drive or a Hard Disk Drive. The options are **Hard Disk Drive** and Solid State Drive.

►PCH sSATA Configuration

sSATA Controller

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

Configure sSATA as (Available when "sSATA Controller" is set to Enable)

Select AHCI to configure an sSATA drive you specified as an AHCI drive. Select RAID to configure an sSATA drive you specified as a RAID drive. The options are **AHCI** and RAID.

sSATA RSTe Boot Info (Available when "Configure sSATA as" is set to RAID)

Select Enable for full int13h support which will allow the system to boot using a device attached to the SATA controller. The options are Disable and **Enable**.



Note: For this feature to work properly, set the CSM Storage OPRM policy to Legacy.

Support Aggressive Link Power Management

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

sSATA RAID Option ROM/UEFI Driver (Available when "Configure sSATA as" is set to RAID)

Select EFI to load the EFI driver for system boot. Select Legacy to load a legacy driver for system boot. The options are Disable, **EFI**, and Legacy.

sSATA Port 0 - sSATA Port 5

Hot Plug

Select Enable to support Hot-plugging for the device installed on an sSATA port you specified 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 you specified to spin up one at a time at bootup preventing all hard drive disks from spinning up at the same time, causing a power surge. The options are Enable and **Disable**. The options are **Disable** and Enable.

sSATA Device Type

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

► Network Configuration

Network Stack

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

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

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

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

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

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

Select Enabled to enable IPv4 PXE boot support. If this feature is disabled, it will not create the IPv6 PXE boot option. The options are Disabled and **Enabled**.

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

Select Enabled to enable IPv4 HTTP boot support. If this feature is disabled, it will not create the IPv6 HTTP boot option. The options are **Disabled** and Enabled.

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

Use this feature to set the wait time (in seconds) upon which the system BIOS will wait for you to press the <ESC> key to abort PXE boot instead of proceeding with PXE boot by connecting to a network server immediately. The default is **0**.

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

Use this option to specify the number of times for the BIOS ROM to detect the presence of a LAN media either via the Internet connection or via a LAN port. The default setting is **1**.

▶ **MAC:xxxxxxxxxxx-IPv4 Network Configuration**
▶ **MAC:xxxxxxxxxxx-IPv4 Network Configuration**
▶ **MAC:xxxxxxxxxxx-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 "Configured" is set to Enabled)

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

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

Enter the IP address in dotted-decimal notation (i.e., 192.168.10.12).

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

Enter the NetMask in dotted-decimal notation (i.e., 255.255.255.0).

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

Enter the Gateway in dotted-decimal notation (i.e., 192.168.10.1).

Local DNS Servers (Available when "Configured" is set to Enabled and "Enable DHCP" is set to Disabled)

Enter the DNS Servers in dotted-decimal notation (i.e., 192.168.10.8).

Save Changes and Exit

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

▶ **MAC:xxxxxxxxxxx-IPv6 Network Configuration**
▶ **MAC:xxxxxxxxxxx-IPv6 Network Configuration**
▶ **MAC:xxxxxxxxxxx-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 select how the policy is to be configured. The options are **automatic** and manual.

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

New IPv6 address

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

New Gateway address

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

New DNS address

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

Commit Changes and Exit

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

Discard Changes and Exit

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

Save Changes and Exit

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

►PCIe/PCI/PnP Configuration

The following PCI information will be displayed:

- PCI Bus Driver Version
- PCI Devices Common Settings

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

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

SR-IOV Support (Available if the system supports Single-Root Virtualization)

Select Enabled for 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**.

Consistent Device Name Support

Use this feature to enable ACPI_DSM (DSM: Device Specific Method) device name support for onboard devices and slots. 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

Select Auto for the system BIOS to automatically set the maximum size for a read request for a PCIe device to enhance system performance. The options are **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.

MMCFG Base

This feature determines how the lowest Memory-Mapped Configuration (MMCFG) base is assigned to onboard PCI devices. The options are 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 the graphics device to be used as the primary video display for system boot. The options are **Onboard** and Offboard.

Onboard Video Option ROM

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

AOC-GTG-i2T Option ROM

Use this feature to select which firmware function to be loaded for CPU IO Module PCIe 4.0 x8 OPRM. The options are Disabled and **EFI**.

AIOM SLOT1 PCIe 4.0 x16 OPRM / PCH M.2A PCIe 3.0 x4 OPRM / PCH M.2B PCIe 3.0 x4 OPRM

Use this feature to select which firmware function to be loaded for the specified PCIe. The options are Disabled and **EFI**.

Onboard NVMe1 Option ROM / Onboard NVMe2 Option ROM / Onboard NVMe3 Option ROM / Onboard NVMe4 Option ROM / Onboard NVMe5 Option ROM / Onboard NVMe6 Option ROM

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



Note: OPRM control will be hidden if you install six port NVMe on the back plane.

►Super IO Configuration

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

- Super IO Chip AST2600

► Serial Port 1 Configuration

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

Serial Port 1

Select Enabled to enable Serial Port 1. The options are Disabled and **Enabled**.

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

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

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

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

► Serial Port 2 Configuration

Serial Port 2

Select Enabled to enable Serial Port 2. The options are Disabled and **Enabled**.

Device Settings (Available when "Serial Port 2" is set to Enabled)

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

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

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

Serial Port 2 Attribute

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

► Serial Port Console Redirection

COM 1

Console Redirection

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

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

Terminal Type

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

Bits Per Second

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

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 (Bits) 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, SCO, 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

Console Redirection

Select Enabled to enable SOL for Console Redirection which will allow a client machine to be connected to a host machine at a remote site for networking. The options are Disabled and **Enabled**.

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

Terminal Type

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

Bits Per second

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

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 (Bits) 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, SCO, 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 enable or disable Legacy Console Redirection after BIOS POST. When the option - Bootloader is selected, Legacy Console Redirection is disabled before booting the OS. When the option - Always Enable is selected, Legacy Console Redirection remains enabled upon OS bootup. The options are **COM1** and SOL.

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

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

Console Redirection EMS

Select Enabled to use a COM port you specified for EMS Console Redirection. The options are **Disabled** and Enabled.

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

Out-of-Band Management Port

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

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 both 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 data-sending when the receiving buffer is full. Send a "Start" signal to start data-sending when the receiving buffer is empty. The options are **None**, Hardware RTS/CTS, and Software Xon/Xoff.

The following information will also be displayed:

- Data Bits EMS
- Parity EMS
- Stop Bits EMS

►ACPI Settings

Use submenu to configure Advanced Configuration and Power Interface (ACPI) power management settings for your system.

NUMA

Select Enabled to enable Non-Uniform Memory Access support to enhance system performance. The options are Disabled and **Enabled**.

UMA-Based Clustering

The options for this feature are Disable (All2All) and **Hemisphere (2-clusters)**. The options are only available when SNC is disabled.

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)

When a Trusted-Platform Module (TPM) device is detected in your machine, the following information will display:

TPM 2.0 Device Found:

- Firmware Version:
- Vendor:

Security Device Support

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

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

- Active PCR banks
- Available PCR banks

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending Operation

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



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

Platform Hierarchy (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 **Enabled** and Disabled.

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 **Enabled** and Disabled.

Endorsement Hierarchy

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

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

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



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

TXT Support

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



Note 1: If 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, refer to the TPM manual at <http://www.supermicro.com/manuals/other/TPM.pdf>.

► HTTP Boot Configuration

HTTP Boot Policy

The options are Apply to all LANs, **Apply to each LAN**, and Boot Priority #1 instantly.

HTTPS Boot Checks Hostname

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

Priority of HTTP Boot

Instance of Priority 1

This configures the order that your computer searches the physical devices for the boot sequence. The default setting for this rank targeted port is **1**.

Select IPv4 or IPv6

You can choose either one Internet Protocol version. The options are **IPv4** and IPv6.

Boot Description

The Boot Description must be filled out; otherwise the boot option for URI would not be created. (Length of description shouldn't be more than 75 characters.)

Boot URI

Highlight the feature and press <Enter> to create a boot URI. A new IPv4/IPv6 Boot option will be created according to this Boot URI. This feature is only supported on Dual or EFI Boot mode. (Length of URI shouldn't be more than 128 characters.)

► SMCI KMS Server Configuration

This submenu displays the configuration settings for the SMCI KMS server which will allow the clients to ask a server to encrypt or decrypt data without a direct access key.

SMCI KMS Server IP address

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

Second SMCI KMS Server IP address

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

SMCI KMS TCP Port number

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

KMS Time Out

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

SMCI KMS Server Retry Count

Use this feature to specify how many times of the connection retry to the KMS server. The valid range is 0 - 10. Press "+" or "-" on your keyboard to change the value. The default setting is **2** (retrying twice).

TimeZone

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

TCG Nvme KMS Policy

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

Client UserName

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

Client Password

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

KMS TLS Certificate / Size**►CA Certificate**

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

►Client Certificate

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

► Client Private Key

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

► Intel(R) Ethernet Controller X710 for 10GBASE-T xx:xx:xx:xx:xx:xx

► Intel(R) Ethernet Controller X710 for 10GBASE-T xx:xx:xx:xx:xx:xx

► Firmware Image Properties

Press <Enter> to display the following device firmware version information.

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

► NIC Configuration

Link Speed

This feature displays the connection speed of a LAN port you specified.

Wake On LAN

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

LLDP Agent

The Link Layer Discovery Protocol (LLDP) runs over the data-link layer. An LLDP agent can transmit information of the local system and/or receive information of the remote system. Three modes are available: Transmit-only mode, Receive-only mode, Transmit and receive mode. 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).

The following information will display as well:

- UEFI Driver
- Adapter PBA
- Device Name

- Chip Type
- PCI Device ID
- PCI Address
- Link Status
- MAC Address
- Virtual MAC Address

► TLS Authenticate Configuration

► Server CA Configuration

This submenu allows you to configure the client certificate to be used by the server.

► Enroll Certification

► Enroll Certification Using File

Use this feature to enroll certification from a file.

Certification GUID

Press <Enter> and input the certification GUID.

► Commit Changes and Exit

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

► Discard Changes and Exit

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

► Delete Certification

Press <Enter> to delete certification.

► Client Certification Configuration

► SAS3808 (PCISlot=0x4) Configuration

Enter this submenu to configure SAS3808.



Note: This submenu will only appear for X12SPT-GC.

► Controller Properties

The following information is displayed:

- Controller Name
- Chip Name
- PCI Revision ID
- PCI Bus:Dev:Func
- PCI Slot
- PCI Ven:Dev
- PCI SSVen:SSDev
- SAS address
- Package Version
- Firmware Version
- UEFI BSD HII Version
- Legacy BIOS Version
- Default NVData Version
- Persistent NVData Version

► Controller Properties

Use this feature to execute Refresh Topology which will allow you to discover devices.



Note: Refresh Topology must be executed at least once to enable Device Properties.

► Device Properties

► **Controller Non Fatal Exceptions**

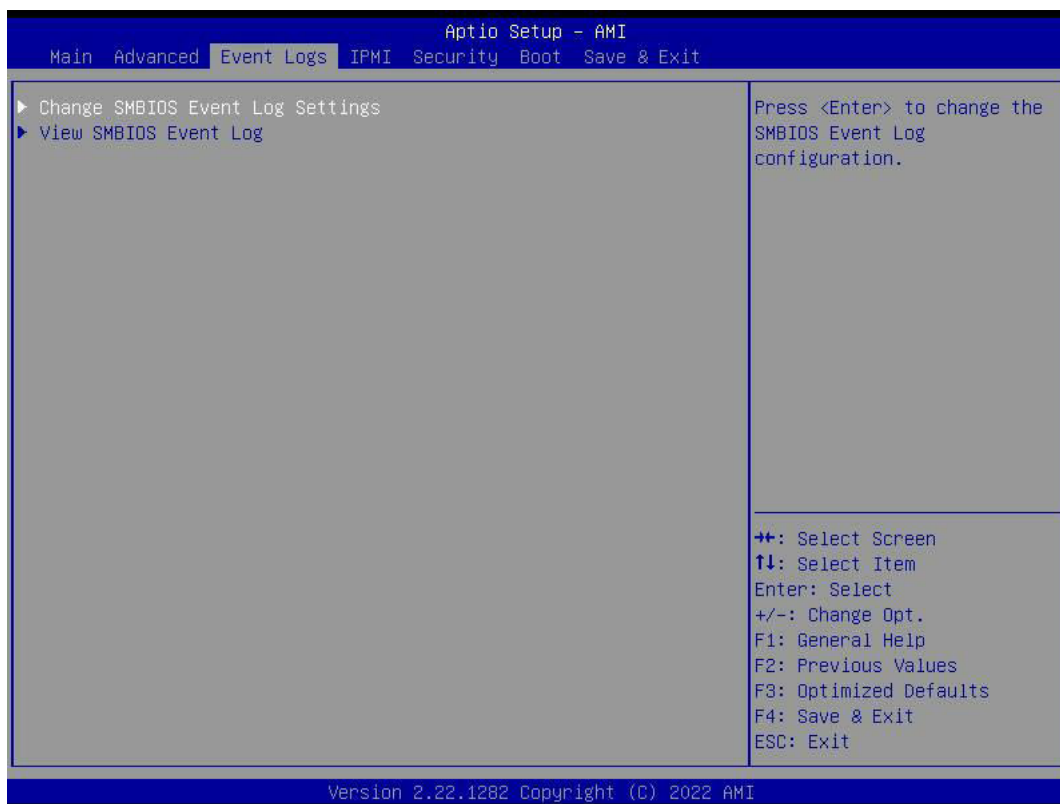
Use this feature to view Controller Exceptions.

► **Driver Health**

This feature displays the driver health information. You can select each one and press <Enter> to see the details.

4.4 Event Logs

Use this feature to configure the Event Log settings.



► Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

Erase Event Log

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

When Log is Full

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

SMBIOS Event Log Standard Settings

Log System Boot Event

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

MECI (Multiple Event Count Increment)

Enter the increment value for the multiple event counter. Enter a number between 1 to 255. The default setting is **1**.

METW (Multiple Event Count Time Window)

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



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

► View System Event Log

This feature allows you to view the event in the system event log. Select this feature and press <Enter> to view the status of an event in the log.

DATE / TIME / ERROR CODE / SEVERITY

4.5 IPMI

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



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

- **BMC Firmware Revision:** This feature indicates the firmware revision of Baseboard Management Controller (BMC) used in your system.
- **IPMI Status:** This feature indicates the status of BMC used in your system.

► System Event Log

Enabling/Disabling Options

SEL Components

Select Enabled to enable all system event logging upon system boot. The options are Disabled and **Enabled**.

Erasing Settings

Erase SEL

Select "Yes, On next reset" to erase all system event logs upon next system boot. Select "Yes, On every reset" to erase all system event logs upon each system reboot. Select "No" to keep all system event logs after each system reboot. The options are "**No**", "Yes, On next reset", and "Yes, On every reset."

When SEL is Full

This feature allows you to determine what the BIOS should do when the system event log is full. Select Erase Immediately to erase all events in the log when the system event log is full. The options are **Do Nothing** and Erase Immediately.

► BMC Network Configuration

Update IPMI LAN Configuration

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

Configure IPv4 Support

IPMI LAN Selection

Use this feature 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 **Dedicated LAN**.

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

Use this feature to select the IP address source 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, AMI BIOS will search for a Dynamic Host Configuration Protocol (DHCP) server attached to the network and request the next available IP address for this computer. The options are Static and **DHCP**.

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

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

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

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

Station MAC Address

This feature displays the Station MAC address for this computer. Mac addresses are 6 two-digit hexadecimal numbers.

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

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1).

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

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

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

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

Configure IPv6 Support

IPv6 Address Status

This feature displays the status of IPv6 addresses.

IPv6 Support

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

Configuration Address Source (Available when "IPv6 Support" is set to Enabled)

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 Dynamic Host Configuration Protocol (DHCP) server in the network that is attached to and request the next available IP address for this computer. The options are **Static** and **DHCP**.

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

This feature displays the station IPv6 address. Press <Enter> to change the setting.

Prefix Length (Available when "Configuration Address Source" is set to Static)

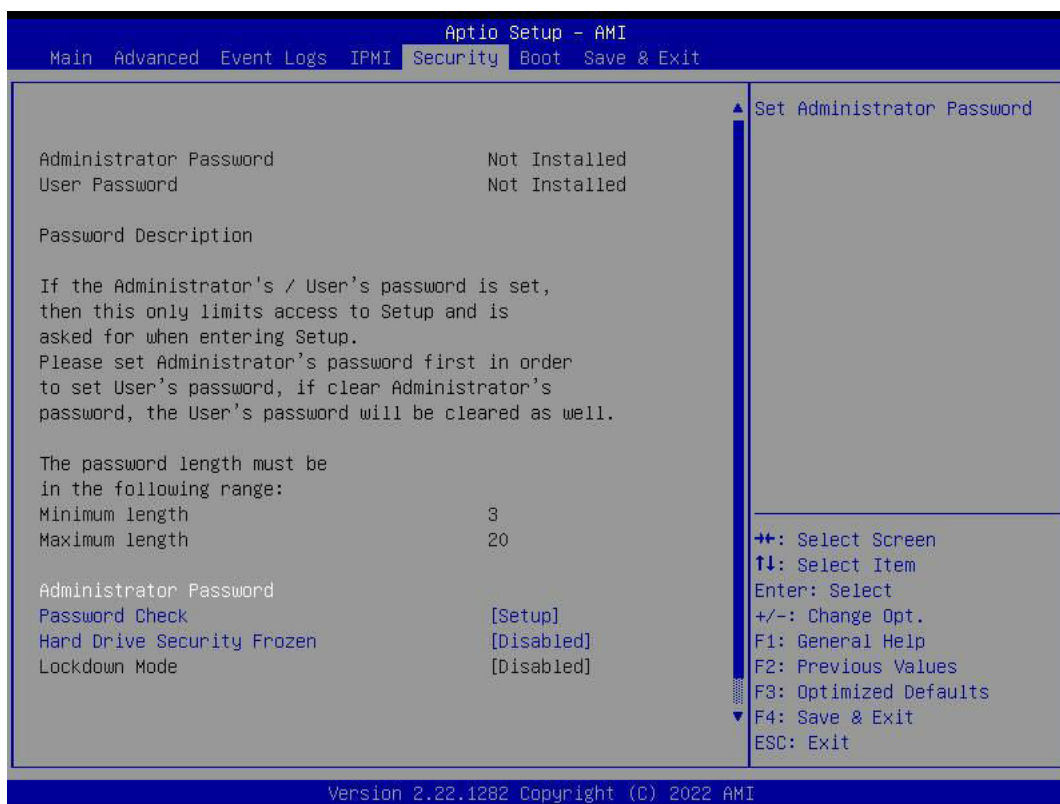
This feature displays the prefix length from BMC. Press <Enter> to change the setting.

IPv6 Router1 IP Address (Available when "Configuration Address Source" is set to Static)

Use this feature to enter the IPv6 Router1 IP address from BMC. Press <Enter> to change the setting.

4.6 Security

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



Administrator Password

This feature indicates if an administrator password has been installed. It also allows you to set the administrator password which is required to enter the BIOS setup utility. The length of the password should be 3 to 20 characters.

User Password (Available when an Administrator Password is entered)

This feature indicates if a user's password has been installed. It also allows you to set the password which is required to enter the BIOS setup utility. This feature provides the description of the password. The length of the password should be 3 to 20 characters.

Password Check

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

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

Hard Drive Security Frozen

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

Lockdown Mode (Available when the DCMS key is activated)

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

► Secure Boot



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

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

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

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

Secure Boot Mode

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

CSM Support

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

► Enter Audit Mode

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

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

Vendor Keys

Provision Factory Defaults

Select Enabled to install factory default Secure Boot keys after the platform reset while the system is in the Setup mode. The options are **Disabled** and Enabled.

► Restore Factory Keys

Select Yes to restore manufacturer default keys used to ensure system security. The options are **Yes** and No.

► Reset to Setup Mode

This feature resets the system to Setup Mode.

► Export Secure Boot Variables

This feature exports the NVRAM contents of Secure Boot variables to a storage device.

► Enroll EFI Image

This feature specifies which Extensible Firmware Interface (EFI) image should be used for the system when it operates in the Secure Boot mode.

Device Guard Ready

► Remove 'UEFI CA' from DB

Select Yes to remove UEFI CA from the database. The options are **Yes** and No.

► Restore DB defaults

Select Yes to restore database variables to the manufacturer default settings. The options are **Yes** and No.

Secure Boot Variable / Size / Keys / Key Source

► Platform Key (PK)

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

►Key Exchange Keys

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

►Authorized Signatures

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

►Forbidden Signatures

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

►Authorized TimeStamps

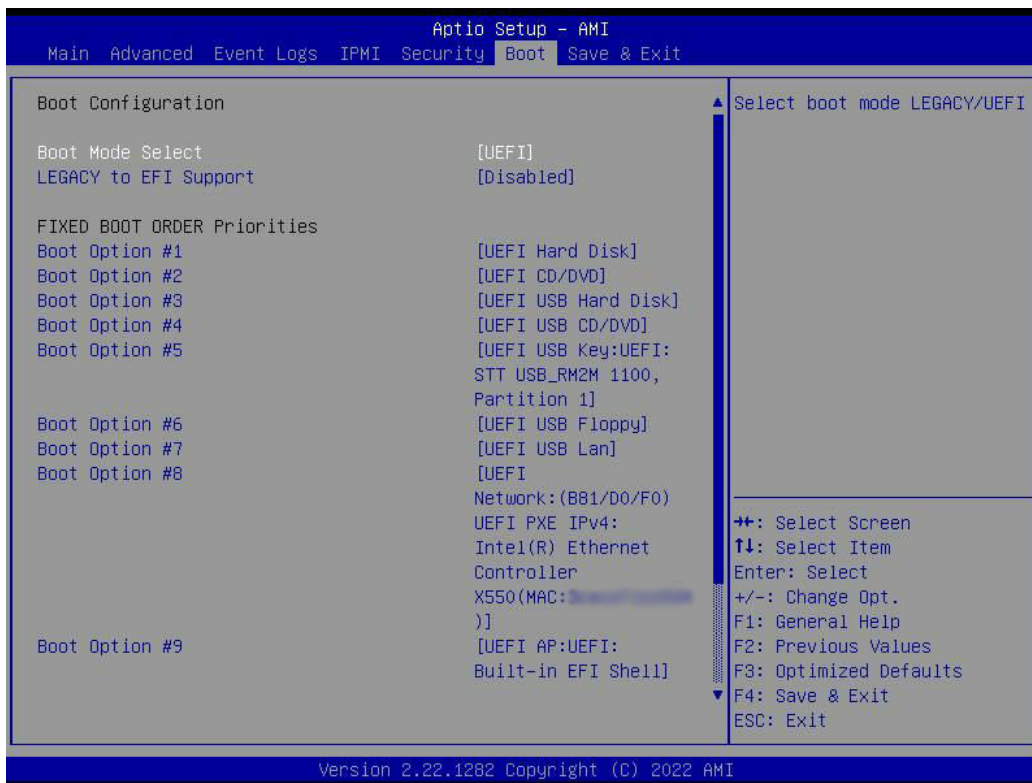
This feature allows you to set and save the timestamps for the authorized signatures which will indicate the time when these signatures are entered into the system. Select Update to update your "Authorized TimeStamps." Select Append to append your "Authorized TimeStamps." The options are **Details**, Export, Update, Append, and Delete.

►OsRecovery (OS Recovery) Signatures

This feature allows you to set and save the authorized signatures used for OS recovery. Select Update to update your "OS Recovery Signatures." Select Append to append your "OS Recovery Signatures." The options are **Details**, Export, Update, Append, and Delete.

4.7 Boot

Use this feature to configure Boot Settings:



Boot Mode Select

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

Legacy to EFI Support

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

FIXED BOOT ORDER Priorities

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

When the feature "**Boot Mode Select**" is set to **UEFI** (default), the following items will be displayed for you to configure the boot settings:

- Boot Option #1 - Boot Option #9

When the feature "**Boot Mode Select**" is set to **Legacy**, the following items will be displayed for configuration:

- Boot Option #1 - Boot Option #8

When the feature "**Boot Mode Select**" is set to **Dual**, the following items will be displayed for configuration:

- Boot Option #1 - Boot Option #17

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

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

Add boot option

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

Path for boot option

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

Boot option File Path

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

Create

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

► **Delete Boot Option**

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

Delete Boot Option

This feature allows you to remove an EFI boot option from the boot priority list.

► **UEFI USB Key Drive BBS Priorities**

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

► **UEFI NETWORK Drive BBS Priorities**

This feature sets the system boot order of detected devices.

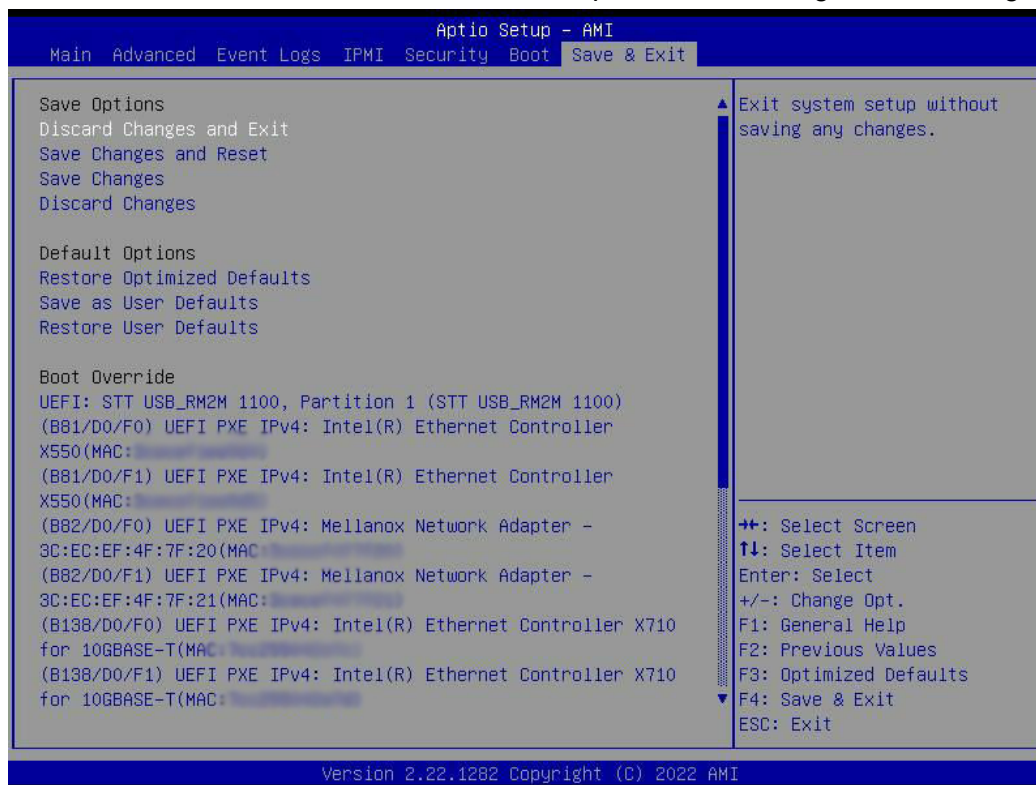
- Boot Option #1 ~ Boot Option #4

► **UEFI Application Boot Priorities**

- Boot Option #1

4.8 Save & Exit

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



Save Options

Discard Changes and Exit

Select this option to exit from the BIOS setup utility without making any permanent changes to the system configuration and reboot the computer.

Save Changes and Reset

When you have completed the system configuration changes, select this option to leave the BIOS setup utility and reboot the computer for the new system configuration parameters to become effective.

Save Changes

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

Discard Changes

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

Default Options

Restore Optimized Defaults

To set this feature, select Restore Default Values from the Exit menu and press <Enter> to load manufacturer default settings which are intended for maximum system performance but not for maximum stability.

Save as User Defaults

To set this feature, select this feature and press <Enter> to save all changes on the default values you entered to the BIOS setup utility for future use.

Restore User Defaults

To set this feature, select Restore the User Default Values from the Exit menu and press <Enter>. Use this feature to retrieve user-defined default settings that have been saved previously.

Boot Override

This feature allows you to override the Boot priorities sequence in the Boot menu, and immediately boot the system with a device you specified instead of the one specified in the boot list. This is a one-time override.

Appendix A

Software

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

A.1 Microsoft Windows OS Installation

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

Installing the OS

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

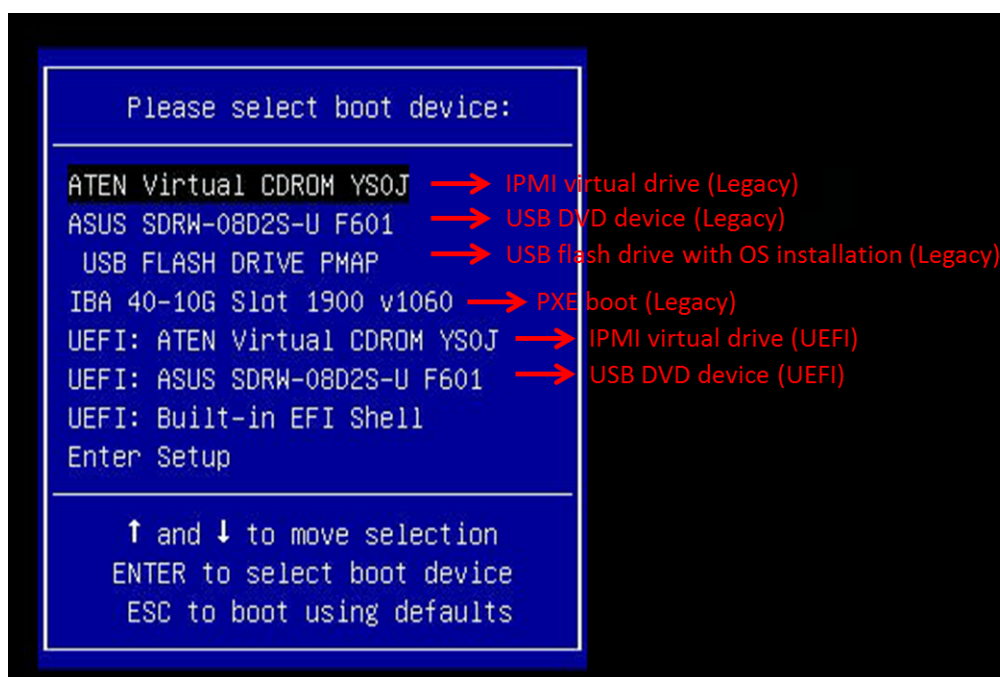


Figure A-1. Select Boot Device

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.

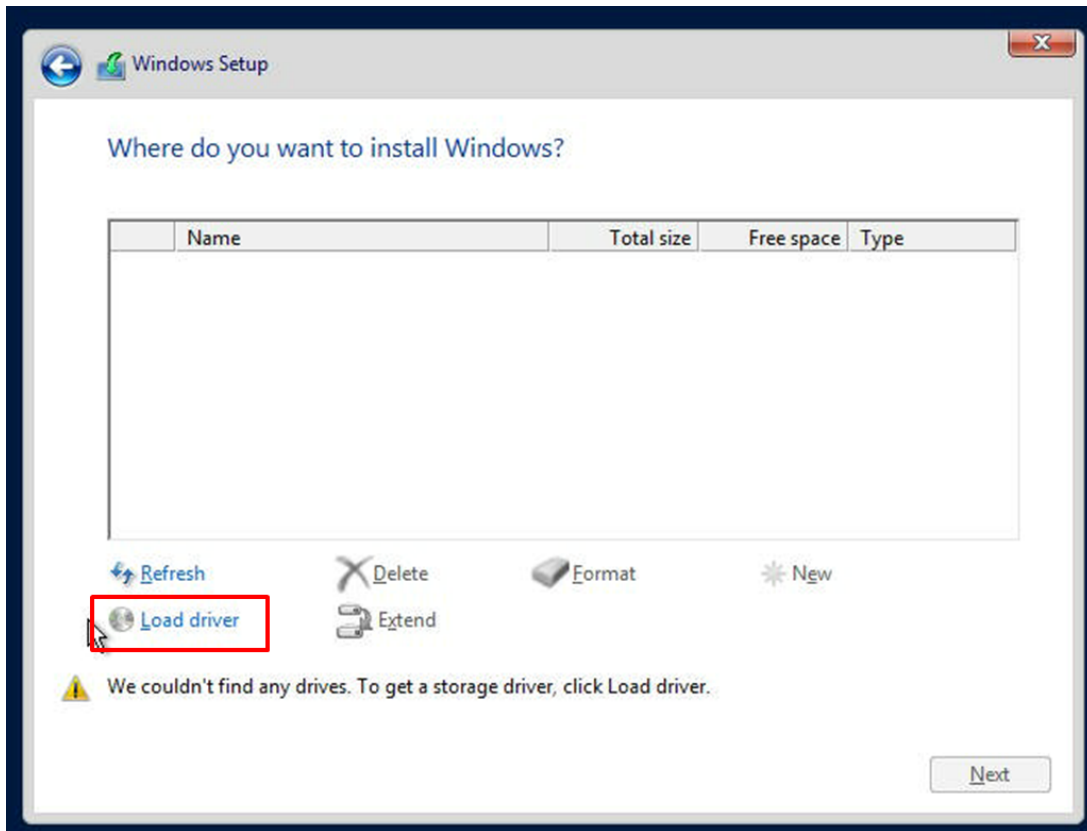


Figure A-2. Load Driver Link

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.

A.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.

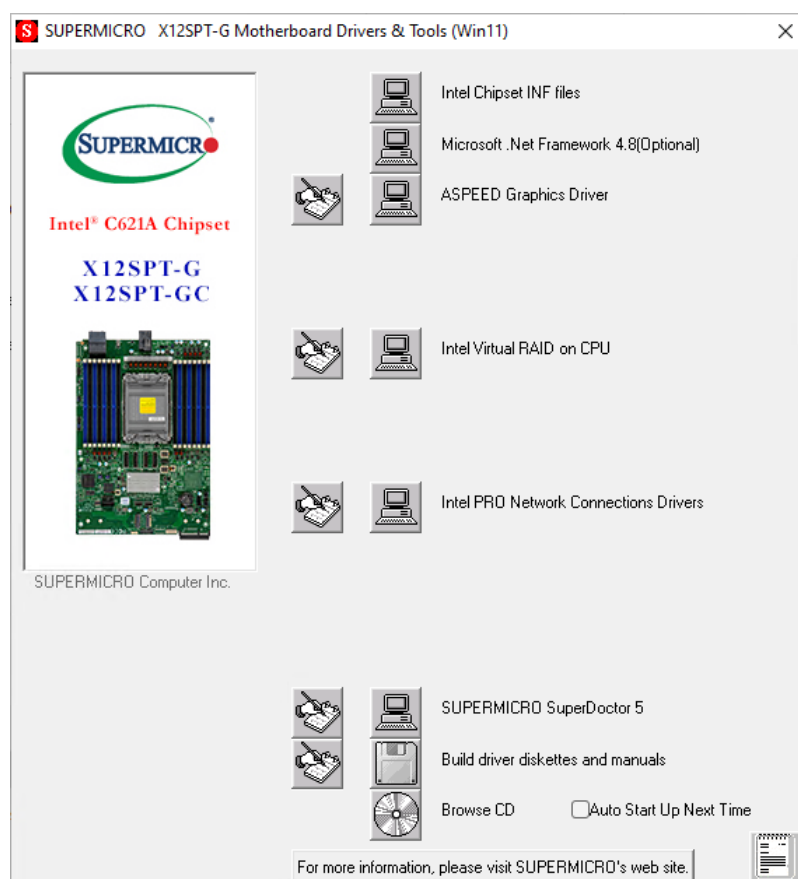


Figure A-3. Driver & Tool Installation Screen

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

A.4 IPMI

The 10th Generation Intel Xeon, Core™ i3, Pentium, Celeron 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.

Supermicro ships standard products with a unique password for the BMC ADMIN user. This password can be found on a label on the motherboard. For general documentation and information on IPMI, please visit our website at https://www.supermicro.com/en/support/BMC_Unique_Password.

Appendix B

Standardized Warning Statements

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

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

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 لعلللمات الشركة الصانعة

경고!

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

Waarschuwing

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

Product Disposal



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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

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

경고!

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

Waarschuwing

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

Appendix C

UEFI BIOS Recovery

Warning: Do not upgrade the BIOS unless your system has a BIOS-related issue. Flashing the wrong BIOS can cause irreparable damage to the system. In no event shall Supermicro be liable for direct, indirect, special, incidental, or consequential damages arising from a BIOS update. If you need to update the BIOS, do not shut down or reset the system while the BIOS is updating to avoid possible boot failure.

C.1 Overview

The Unified Extensible Firmware Interface (UEFI) provides a software-based interface between the operating system and the platform firmware in the pre-boot environment. The UEFI specification supports an architecture-independent mechanism that will allow the UEFI OS loader stored in an add-on card to boot the system. The UEFI offers clean, hands-off management to a computer during system boot.

C.2 Recovering the UEFI BIOS Image

A UEFI BIOS flash chip consists of a recovery BIOS block and a main BIOS block (a main BIOS image). The recovery block contains critical BIOS codes, including memory detection and recovery codes for the user to flash a healthy BIOS image if the original main BIOS image is corrupted. When the system power is first turned on, the boot block codes execute first. Once this process is completed, the main BIOS code will continue with system initialization and the remaining POST (Power-On Self-Test) routines.

 **Note 1:** Follow the BIOS recovery instructions below for BIOS recovery when the main BIOS block crashes.

 **Note 2:** When the BIOS recovery block crashes, you will need to follow the procedures to make a Returned Merchandise Authorization (RMA) request. (For a RMA request, please see section 3.5 for more information). Also, you may use the Supermicro Update Manager (SUM) Out-of-Band (OOB) (https://www.supermicro.com.tw/products/nfo/SMS_SUM.cfm) to reflash the BIOS.

C.3 Recovering the BIOS Block with a USB Device

This feature allows the user to recover the main BIOS image using a USB-attached device without additional utilities used. A USB flash device such as a USB Flash or media drive can be used for this purpose. However, a USB Hard Disk drive cannot be used for BIOS recovery at this time.

The file system supported by the recovery block is FAT (including FAT12, FAT16, and FAT32), which is installed on a bootable or non-bootable USB-attached device. However, the BIOS might need several minutes to locate the SUPER.ROM file if the media size becomes too large due to the huge volumes of folders and files stored in the device.

To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below:

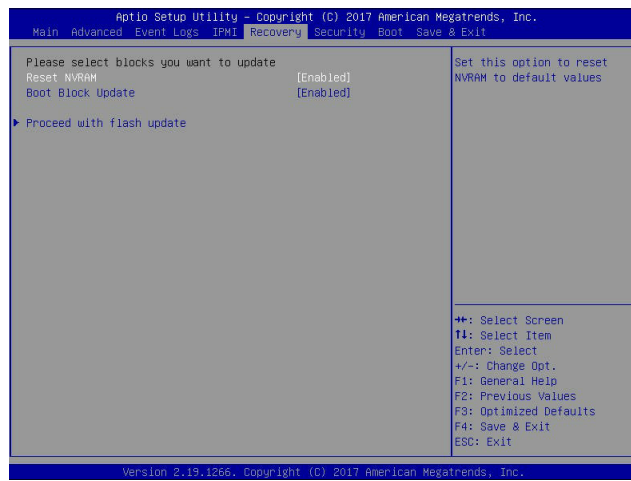
1. Using a different machine, copy the "Super.ROM" binary image file into the disc Root "\" directory of a USB flash or media drive.



Note 1: If you cannot locate the "Super.ROM" file in your driver disk, visit our website at www.supermicro.com to download the BIOS package. Extract the BIOS binary image into a USB flash device and rename it "Super.ROM" for the BIOS recovery use.

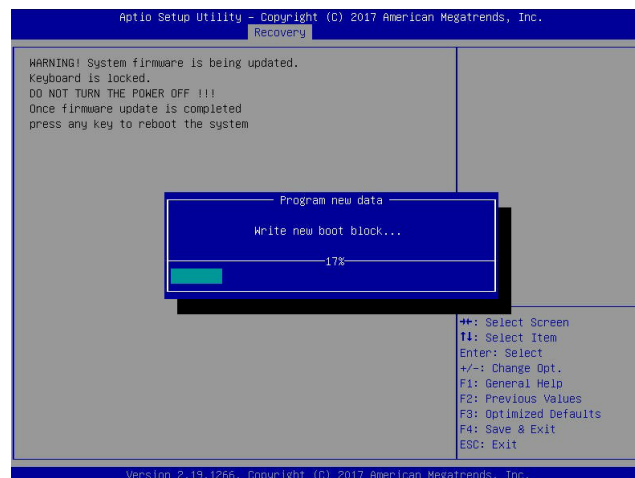


 **Note 2:** Before recovering the main BIOS image, confirm that the "Super.ROM" binary image file you download is the same version or a close version meant for your motherboard.

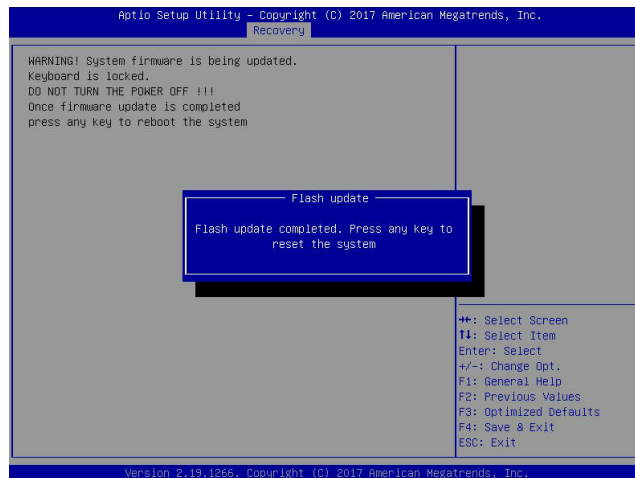


2. Insert the USB device that contains the new BIOS image ("Super.ROM") into your USB port and reset the system until the following screen appears:
3. After locating the new BIOS binary image, the system will enter the BIOS Recovery menu as shown below:

 **Note:** At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

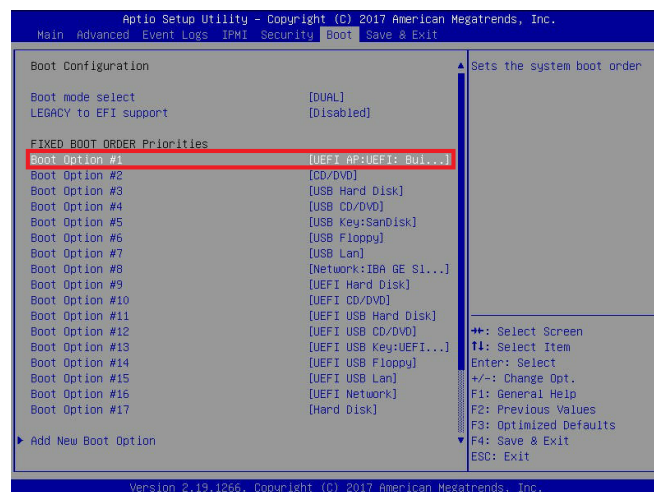


4. When the screen as shown above displays, use the arrow keys to select the item "Proceed with flash update" and press the <Enter> key. You will see the BIOS recovery progress as shown in the screen below:



Note: Do not interrupt the BIOS flashing process until it has completed.

5. After the BIOS recovery process is completed, press any key to reboot the system.
6. Using a different system, extract the BIOS package into a USB flash drive.
7. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the BIOS Setup utility.



8. When the UEFI Shell prompt appears, type `fs#` to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 6. Enter `flash.nsh BIOSname.###` at the prompt to start the BIOS update process.

```

UEFI Interactive Shell v2.1
EDK II
UEFI v2.50 (American Megatrends, 0x0005000C)
Mapping table
  FS0: Alias(s):HD(0)MB:BLK1:
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)/HD(1,MBR,0x37901072,0x800,0x1
CR392)
  BLK0: Alias(s):
      PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)
Press F8 in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> cd AFUDOS
FS0:\AFUDOS> cd SKJPM2_03162017
FS0:\AFUDOS\SKJPM2_03162017> flash.nsh X12PU7.314

```



Note: Do not interrupt this process until the BIOS flashing is complete.

```

Done.
[ Access Cmos Port Ex ]
<Read>
Index 0x51: 0x10

Done.
*****
*
* Program BIOS and ME (including FDT) regions...
*
*****
| AMI Firmware Update Utility v6.09.01.1317 |
| Copyright (C)2017 American Megatrends Inc. All Rights Reserved. |
*****
CPUID = 50652

Reading flash ..... done
- ME Data Size checking - ok
- FFS checksums ..... ok
- Check RomLayout ..... OK
Erasing Boot Block ..... done
Updating Boot Block ..... done
Verifying Boot Block ..... done
Erasing Main Block ..... 0x00132000 (0%)

Verifying NDB Block ..... done
- Update success for FDR
- Update success for IE
- Successful Update Recovery Loader to OPRx!!
- Successful Update MFSB!!
- Successful Update FIPR!!
- Successful Update MFS, IVB1 and IVB2!!
- Successful Update FLOS and UTX!!
- ME Entire Image update success !!

WARNING : System must power-off to have the changes take effect!
Moving FS0:\AFUDOS\SKJPM2_03162017\Fdtx64.efi -> FS0:\AFUDOS\SKJPM2_03162017\F
dt.smc
- [ok]
Moving FS0:\AFUDOS\SKJPM2_03162017\Fuef1x64.efi -> FS0:\AFUDOS\SKJPM2_0316201
7\Fuef1.smc
- [ok]
*****
* Please ignore this 'Shell: Cannot read from file - Device Error'
* warning message due to it does not impact flashing process.
*
*****
Deleting 'FS0:\AFUDOS\SKJPM2_03162017\Fdtx64.efi'
Delete successful.
FS0:\>

```

9. The screen above indicates that the BIOS update process is complete. When you see the screen above, unplug the AC power cable from the power supply, clear CMOS, and plug the AC power cable in the power supply again to power on the system.
10. Press `<Del>` to enter the BIOS Setup utility.
11. Press `<F3>` to load the default settings.
12. After loading the default settings, press `<F4>` to save the settings and exit the BIOS Setup utility.