



B12SPE-CPU-25G

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 B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a consumer environment or residential installation. 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: November 27, 2023

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 © 2023 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 B12SPE-CPU-25G motherboard.

About This Motherboard

The B12SPE-CPU-25G motherboard supports a 3rd Generation Intel® Xeon® Scalable Processor in an LGA4189 socket. This motherboard provides maximum performance, supports up to 4 TB of DDR4 ECC RDIMM/LRDIMM/3DSLRDIMM memory with speeds of up to 3200 MT/s in 16 slots, one hybrid M.2 M-Key PCIe 3.0 x4 or SATA 3.0 slot, one PCIe 4.0 x8 Mezzanine Card connector for AOM, and is optimized for data centers and cloud computing. Please note that this motherboard is intended to be installed and serviced by professional technicians only. For processor and memory updates, please refer to our website at <http://www.supernmicro.com/products/>.

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

1.1 Checklist	8
Quick Reference	11
Quick Reference Table	12
Motherboard Features	13
1.2 Processor and Chipset Overview	16
1.3 Special Features	16
Recovery from AC Power Loss	16
1.4 System Health Monitoring	16
Onboard Voltage Monitors	16
Fan Status Monitor with Firmware Control	16
Environmental Temperature Control	17
System Resource Alert	17
1.5 ACPI Features	17

Chapter 2 Installation

2.1 Static-Sensitive Devices	18
Precautions	18
Unpacking	18
2.2 Processor and Heatsink Installation	19
The 3rd Generation Intel Xeon Scalable Processor Series	19
Overview of the Processor Carrier Assembly	20
Overview of the CPU Socket	20
Overview of the Processor Heatsink Module	21
Creating the Non-F Model Processor Carrier Assembly	22
Assembling the Processor Heatsink Module	23
Preparing the CPU Socket for Installation	24
Installing the Processor Heatsink Module	25
Removing the Processor Heatsink Module	26
2.3 Motherboard Installation	27
Tools Needed	27
Location of Mounting Holes	27

Installing the Motherboard.....	28
Installing the Motherboard into the Superblade Chassis.....	29
2.4 Memory Support and Installation	30
Memory Support.....	30
General Guidelines for Optimizing Memory Performance	31
DIMM Installation	32
DIMM Removal	32
2.5 Connectors	33
2.8 Jumper Settings	39
How Jumpers Work.....	39
2.9 LED Indicators.....	44
<i>Chapter 3 Troubleshooting</i>	
3.1 Troubleshooting Procedures	45
Before Power On	45
No Power	45
No Video	46
System Boot Failure	46
Memory Errors	46
Losing the System's Setup Configuration.....	47
When the System Becomes Unstable	47
3.2 Technical Support Procedures	49
3.3 Frequently Asked Questions	50
3.4 Battery Removal and Installation	51
Battery Removal.....	51
Proper Battery Disposal	51
Battery Installation.....	51
3.5 Returning Merchandise for Service.....	52
<i>Chapter 4 UEFI BIOS</i>	
4.1 Introduction.....	53
4.2 Main Setup	54
4.3 Advanced.....	56
4.4 Event Logs	119
4.5 IPMI	121

4.6 Security.....	124
4.7 Boot.....	128
4.8 Save & Exit.....	130

Appendix A BIOS Codes

A.1 BIOS Error POST (Beep) Codes	132
A.2 Additional BIOS POST Codes.....	133

Appendix B Software

B.1 Microsoft Windows OS Installation.....	134
B.2 Driver Installation.....	136
B.3 SuperDoctor® 5.....	137
B.4 IPMI	138

Appendix C Standardized Warning Statements

Appendix D UEFI BIOS Recovery

D.1 Overview.....	142
D.2 Recovering the UEFI BIOS Image.....	142
D.3 Recovering the BIOS Block with a USB Device	142

Chapter 1

Introduction

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

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

1.1 Checklist

Main Parts List		
Description	Part Number	Quantity
Supermicro Motherboard	B12SPE-CPU-25G	1
Quick Reference Guide	MNL-2272-QRG	1

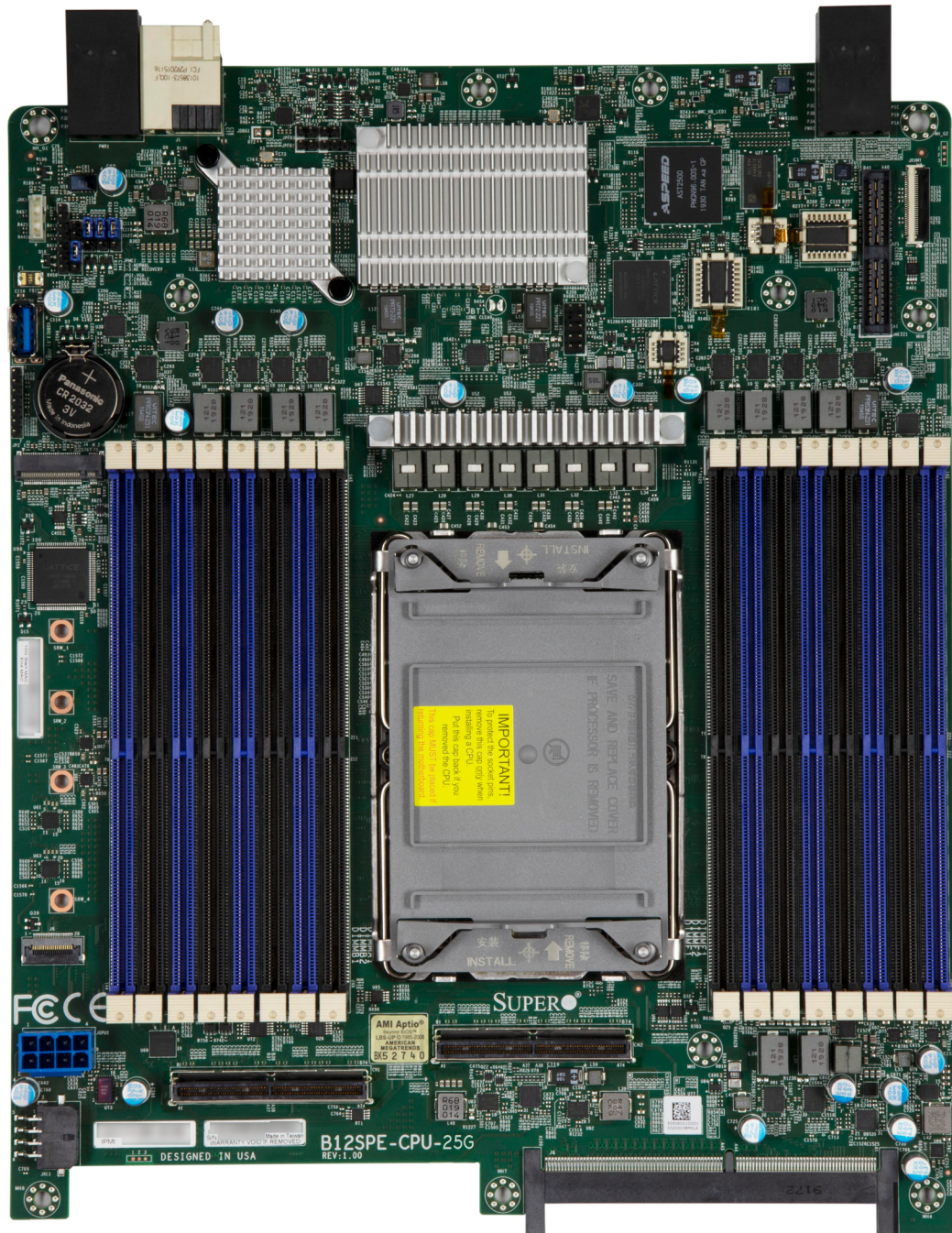
Important Links

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.

- Frequently Asked Questions: <https://www.supermicro.com/FAQ/index.php>
- 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=/wftp/utility/Lot9_Secure_Data_Deletion_Utility/
- If you have any questions, please contact our support team at: support@supermicro.com

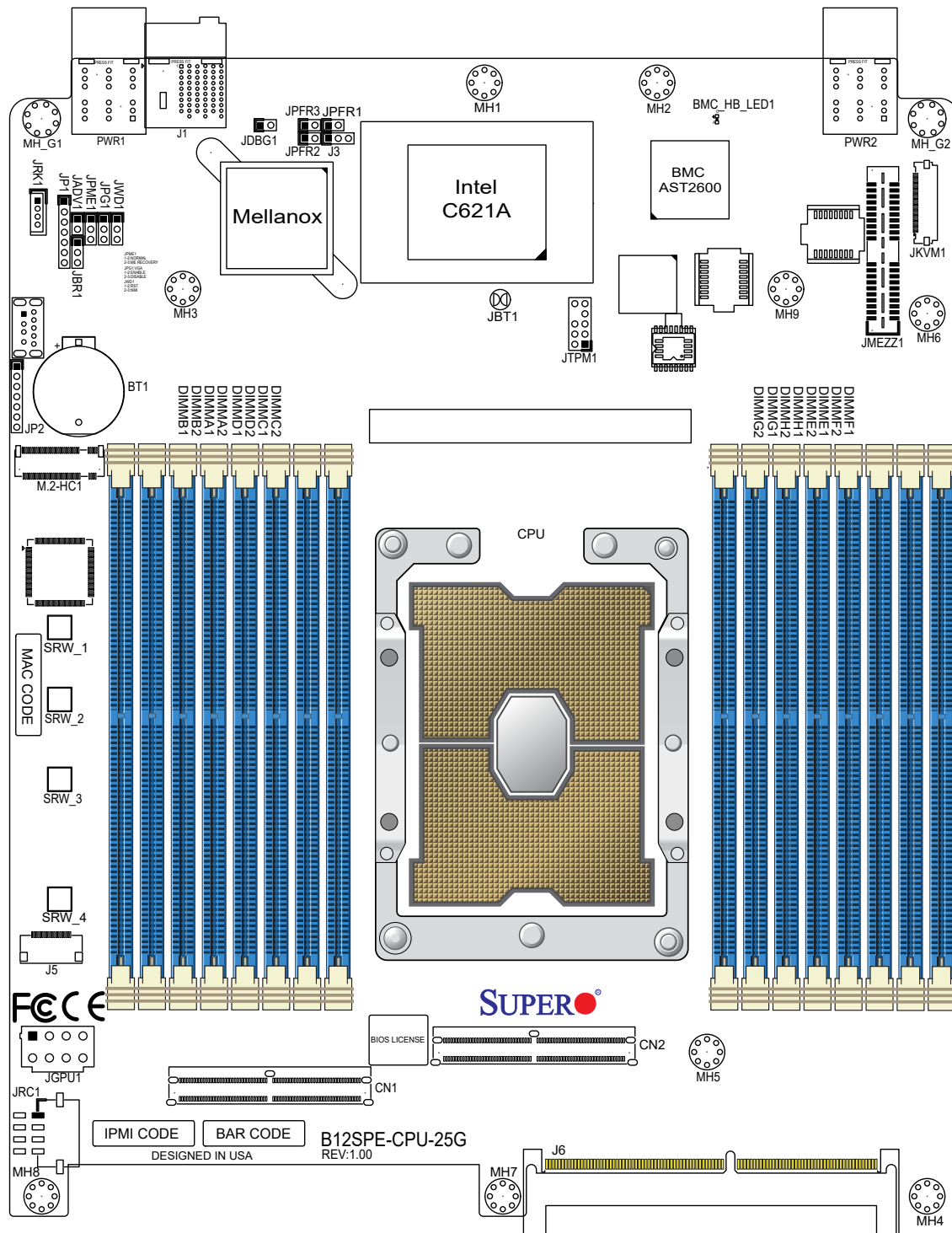
This manual may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

Figure 1-1. B12SPE-CPU-25G Motherboard Image



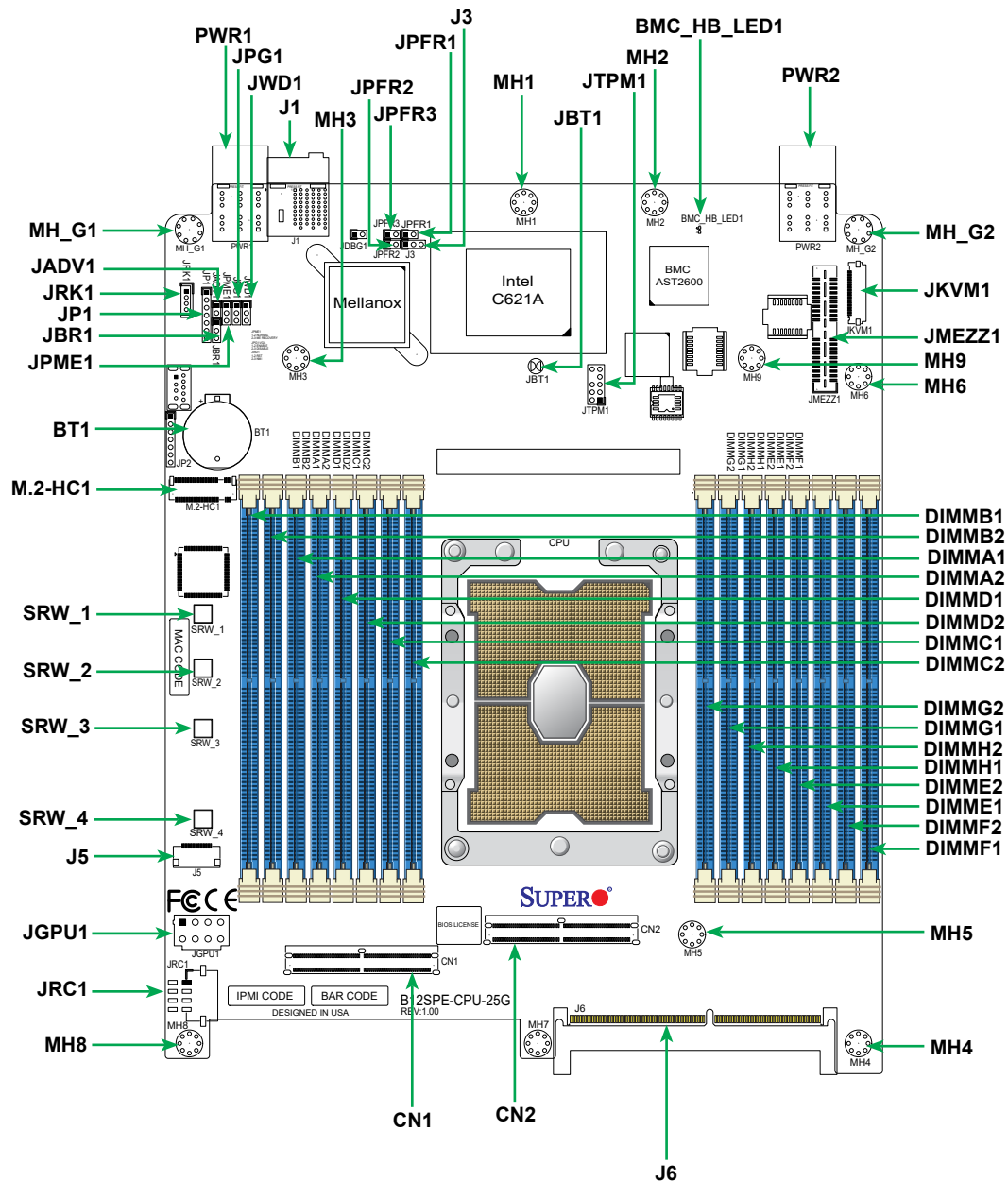
Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publication of the manual. The motherboard you received may or may not look exactly the same as the graphics shown in this manual.

Figure 1-2. Motherboard Layout
(not drawn to scale)



Note: Components not documented are for internal testing only.

Quick Reference



Notes:

- See [Chapter 2](#) for detailed information on jumpers, I/O ports, and 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
JBR1	BIOS Recovery	Pins 1-2 (Enable)
JBT1	CMOS Clear	Open (Normal)
JPG1	VGA Enable/Disable	Pins 1-2 (Enabled)
JPME1	ME Recovery	Pins 1-2 (Normal)
JWD1	Watch Dog Timer	Pins 1-2 (Reset)

Connector	Description
BT1	Onboard Battery
CN1, CN2	MCIO PCIe 4.0 x16 Connectors
J1	Chassis Backplane Connector
J3	VRM Debug Jumper (Manufacturing Use Only)
J5	Front Panel Connector
J6	PCIe 3.0 x16 SIOM Connector
JGPU1	12 V GPU Power Connector (ATX 8-pin)
JKVM1	VGA/USB Module Connector
JMEZZ1	PCIe 4.0 x8 Mezzanine Card Connector for AOM
JP1, JP2	PLD Header (Manufacturing Use Only)
JRC1	Proprietary Riser Power Connector
JRK1	Intel RAID Key Header
JTPM1	Trusted Platform Module (TPM)/Port 80 Header
MH1 - MH9	Mounting Holes
MH_G1 - MH_G2	Mounting Holes
M.2-HC1	Hybrid M.2 M-Key PCIe 3.0 x4 or SATA 3.0 Slot
PWR1	Power Receptacle to Chassis Backplane
PWR2	Power Receptacle to Chassis Backplane
SRW_1 - SRW_4	M.2 Mounting Holes

LED	Description	Status
BMC_HB_LED1	BMC Heartbeat LED	Blinking Green: BMC Normal

Motherboard Features

Motherboard Features	
CPU	Supports a 3rd Generation Intel Xeon Scalable Processor in an LGA4189 socket.
Memory	Supports up to 4 TB of DDR4 ECC RDIMM/LRDIMM/LRDIMM 3DS memory with speeds of up to 3200 MT/s in 16 slots.
DIMM Size	Up to 256 GB at 1.2 V
Chipset	Intel PCH C621A
I/O Devices	- One PCIe 3.0 x16 SIOM Connector - One PCIe 4.0 x8 Mezzanine Card Connector for AOM - One Hybrid M.2 M-Key PCIe 3.0 x4 or SATA 3.0 Slot - Two USB 2.0 ports via JKVM1 header
Network	Mellanox MT27712
Baseboard Management Controller (BMC)	ASpeed AST2600 BMC
Graphics	Graphics controller via ASpeed AST2600 BMC
BIOS	256 Mb MX25L2567 BIOS - ACPI 6.2, SMBIOS 2.8/3.2, UEFI 2.7 specification, PCI F/W 3.1, Plug and Play (PnP), SPI dual/quad speed support, RTC wake up
Power Management	- Power button override mechanism - Management Engine (ME) - Power-on mode for AC recovery



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

Motherboard Features	
System Health Monitoring	
- Onboard voltage monitoring for +3.3 V, +3.3 V Stdb, +5 V, +5 V Stdb, +Vcore, Vmem - Temperature monitoring for CPU, PCH, System, DIMM, Peripheral, GPU, NVMe, SAS HDD 6+2 CPU switching phase voltage regulator - CPU Thermal Trip support	
System Management	
- Trusted Platform Module (TPM) support - Platform Environment Control Interface (PECI) 2.0 support - IPMI 2.0 - Watch Dog, NMI	
LED Indicators	
BMC Heartbeat LED	
Dimensions	
Proprietary Form Factor, 9.358" x 11.408" (23.77 cm x 28.98 cm)	

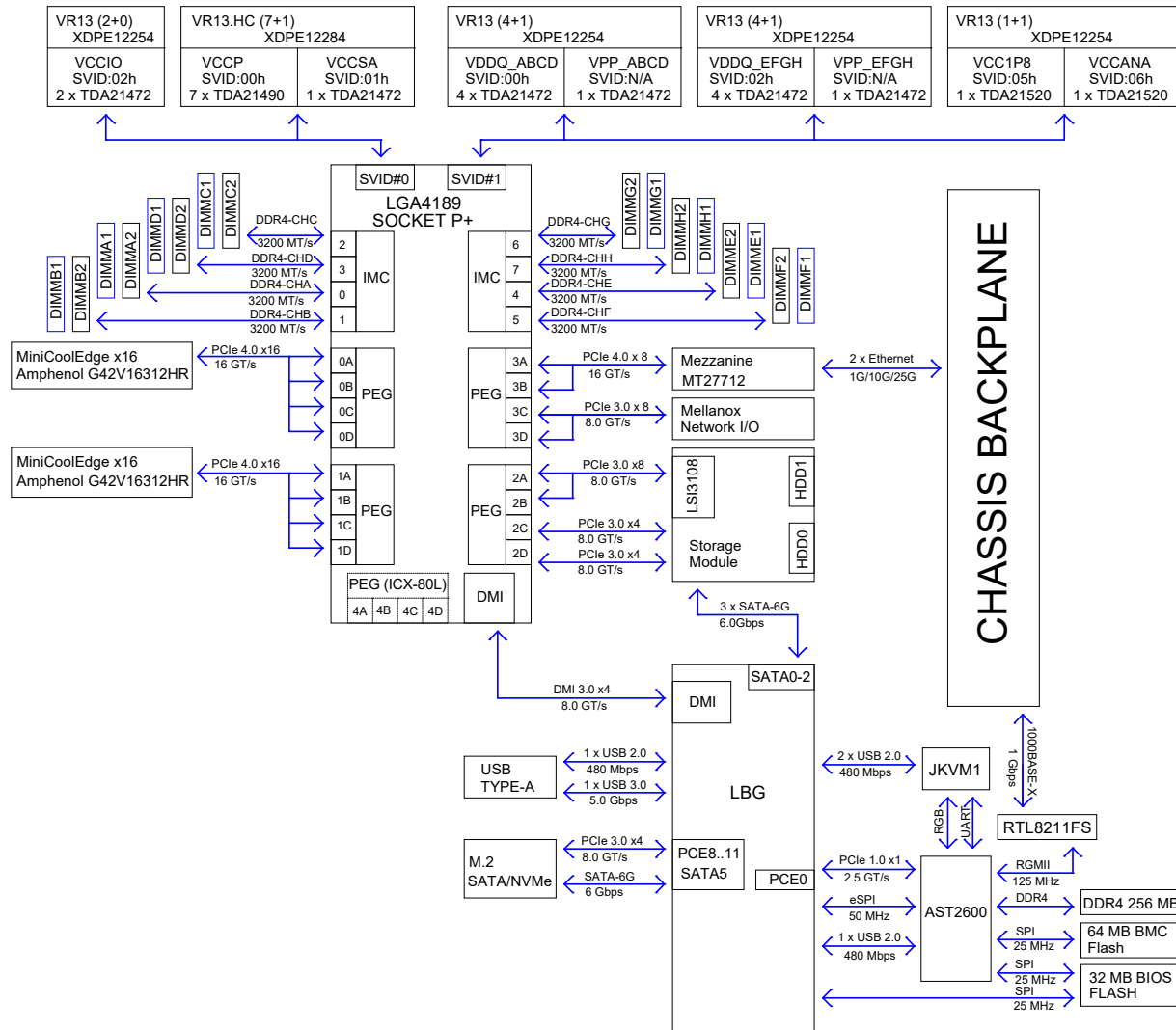
 **Note 1:** The CPU maximum thermal design power (TDP) is subject to chassis and heatsink cooling restrictions. For proper thermal management, check the chassis and heatsink specifications for proper CPU TDP sizing.

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

 **Note 3:** If you purchase a Supermicro Out of Band (OOB) software license key (Supermicro P/N: SFT-OOB-LIC), please DO NOT change the IPMI MAC address. Once the Mac address has been changed, the OOB license key will be invalid.

 **Note 4:** Supermicro ships standard products with a unique password for the BMC ADMIN user. This password can be found on a label on the motherboard.

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

The Supermicro B12SPE-CPU-25G motherboard, with the C621A chipset, supports an Intel Xeon SP processor and provides superb performance, efficient power management, all the while providing a rich feature set based on cutting edge technology to address today's needs in advanced computing, engineering simulation, and automation.

The processor and the chipset support the following features:

- Intel Hyper-Threading, Intel VT-D, VT-x
- Intel Turbo Boost Technology
- Intel Rapid Storage Technology
- 4 TB memory support with speeds of up to 3200 MT/s
- ACPI Power Management

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 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 IPMI.

Environmental Temperature Control

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

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.

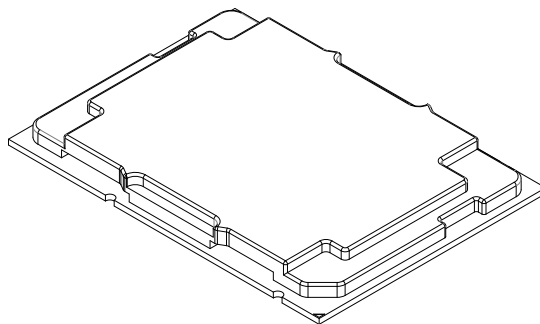
2.2 Processor and Heatsink Installation

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 illustrations only. Your components may look different.

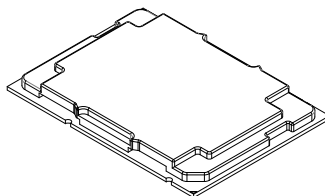
The 3rd Generation Intel Xeon Scalable Processor Series



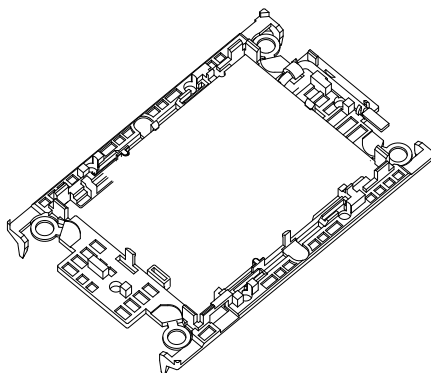
Overview of the Processor Carrier Assembly

The processor carrier assembly contains the processor and a processor carrier.

1. Processor



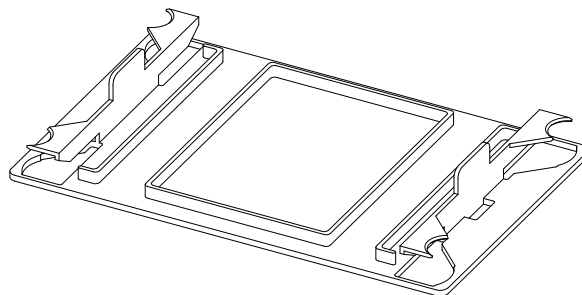
2. Processor Carrier



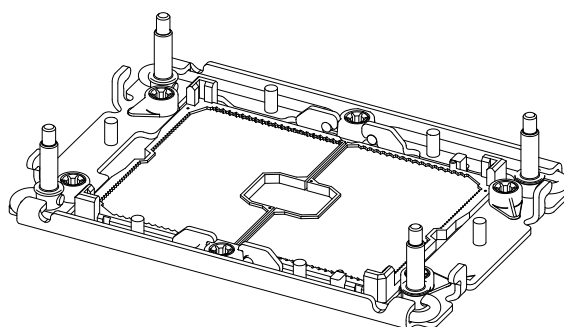
Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

1. Plastic Protective Cover



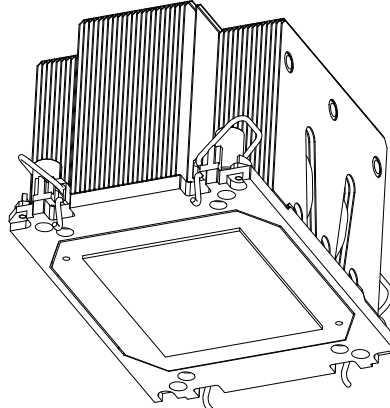
2. CPU Socket



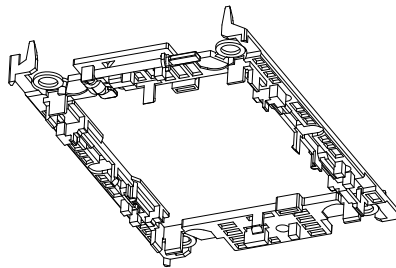
Overview of the Processor Heatsink Module

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

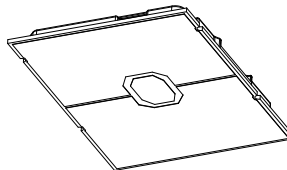
1. Heatsink with Thermal Grease



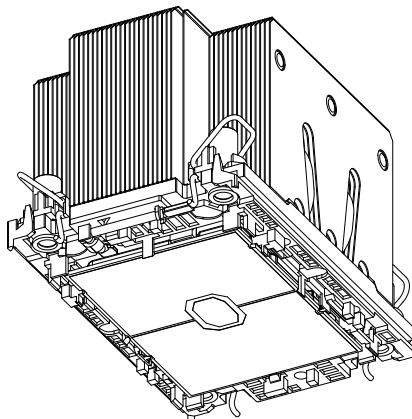
2. Processor Carrier



3. Processor



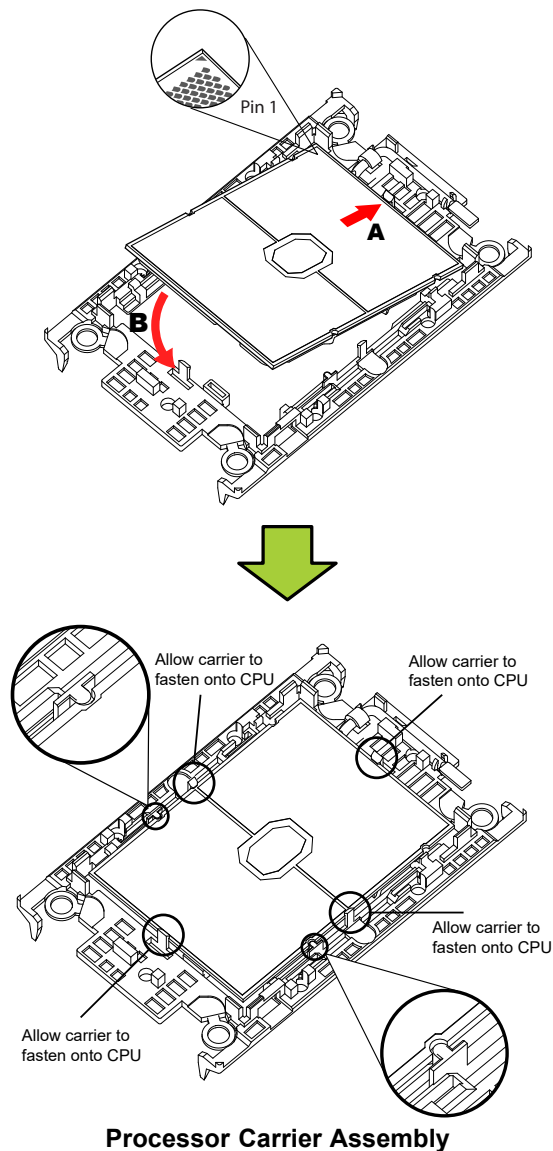
Processor Heatsink Module



Creating the Non-F Model Processor Carrier Assembly

To install a Non-F model 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.
3. Examine all corners to ensure that the processor is firmly attached to the carrier.

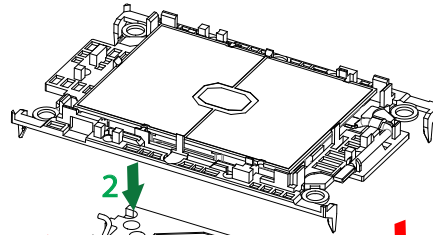


Assembling the Processor Heatsink Module

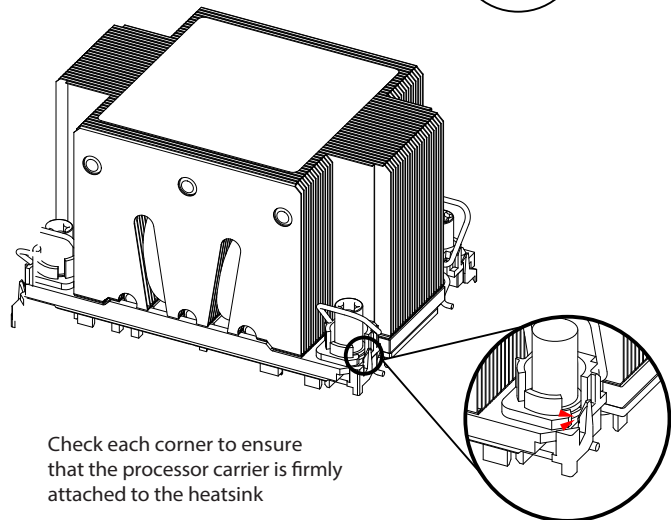
After creating the processor carrier assembly for the processor, mount it onto the heatsink to create the processor heatsink module (PHM):

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)



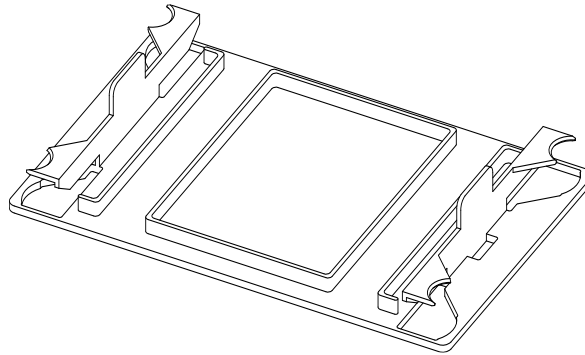
Heatsink
(Upside Down)



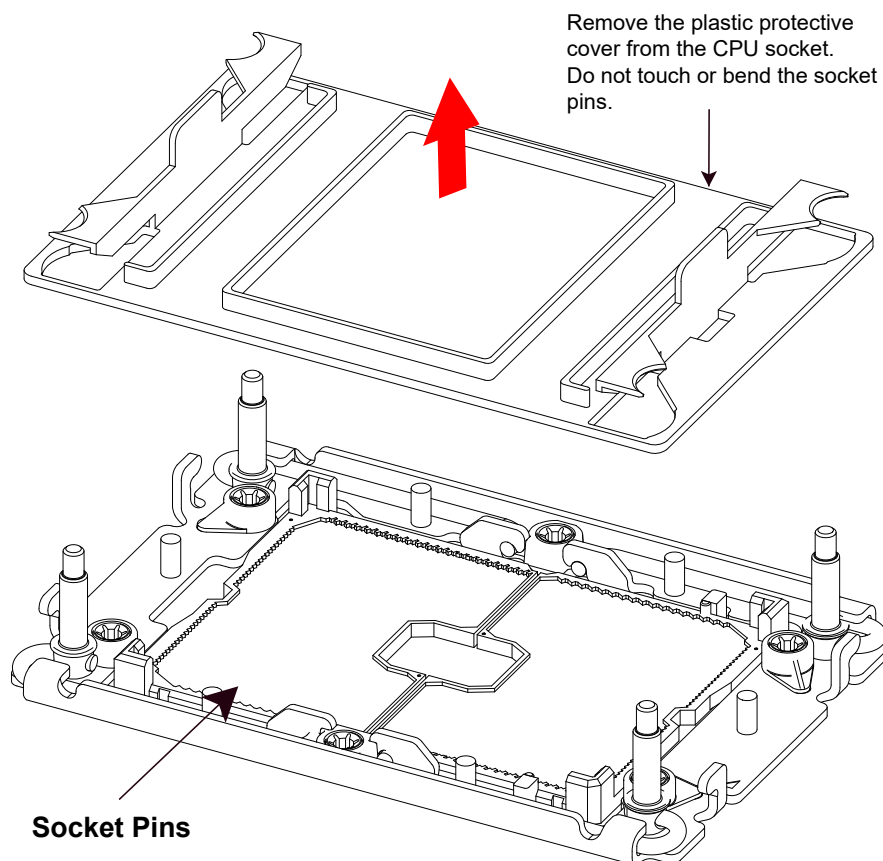
Check each corner to ensure that the processor carrier is firmly attached to the heatsink

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.



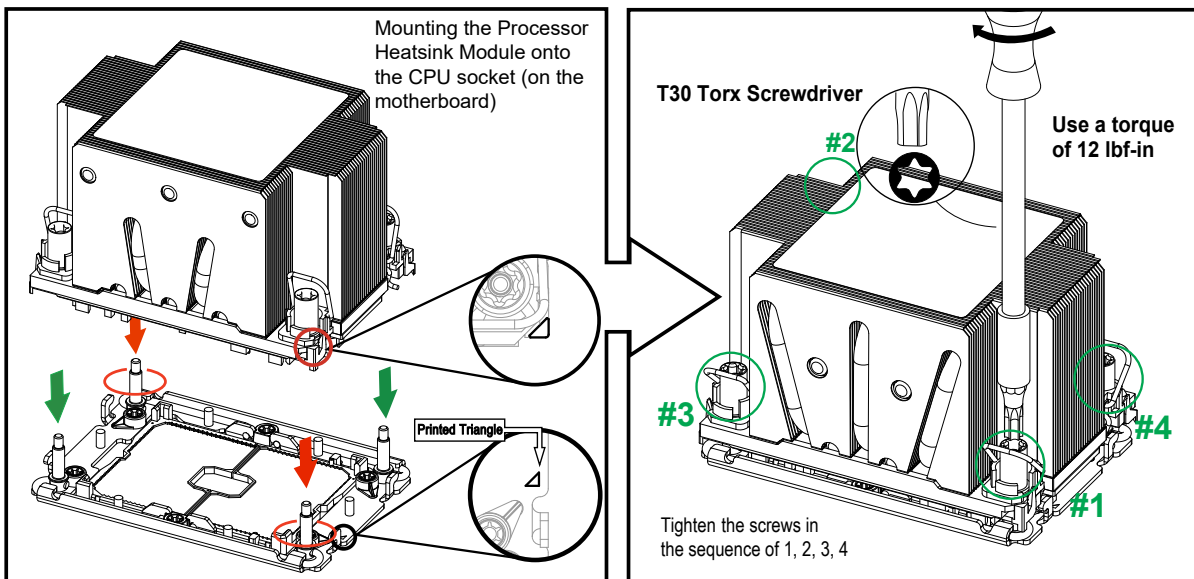
CPU Socket with Plastic Protective Cover



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.

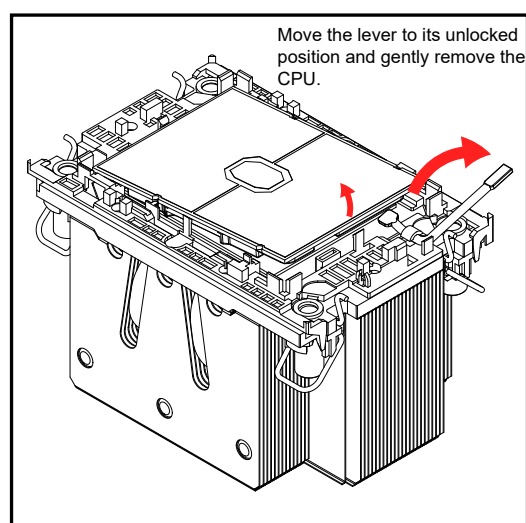
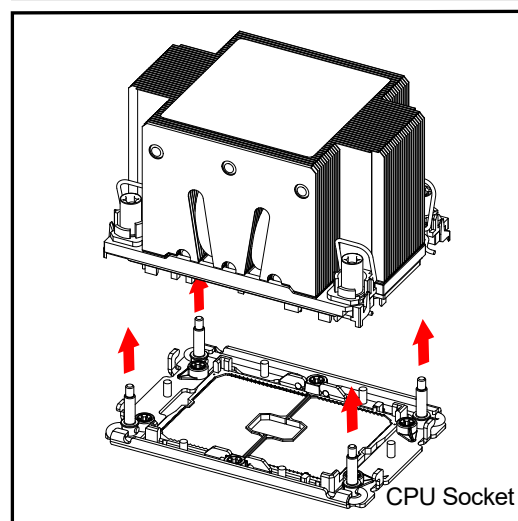
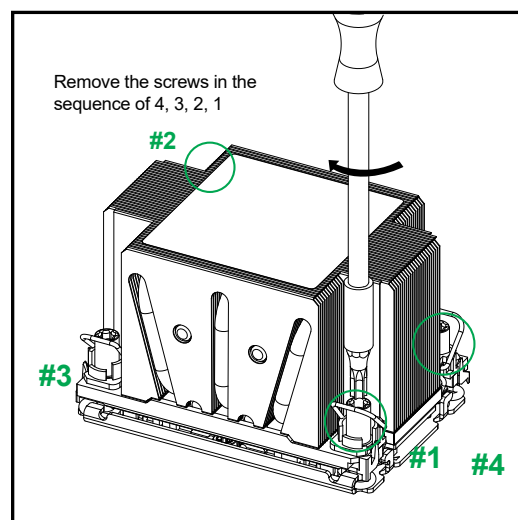


Removing the Processor Heatsink Module

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:

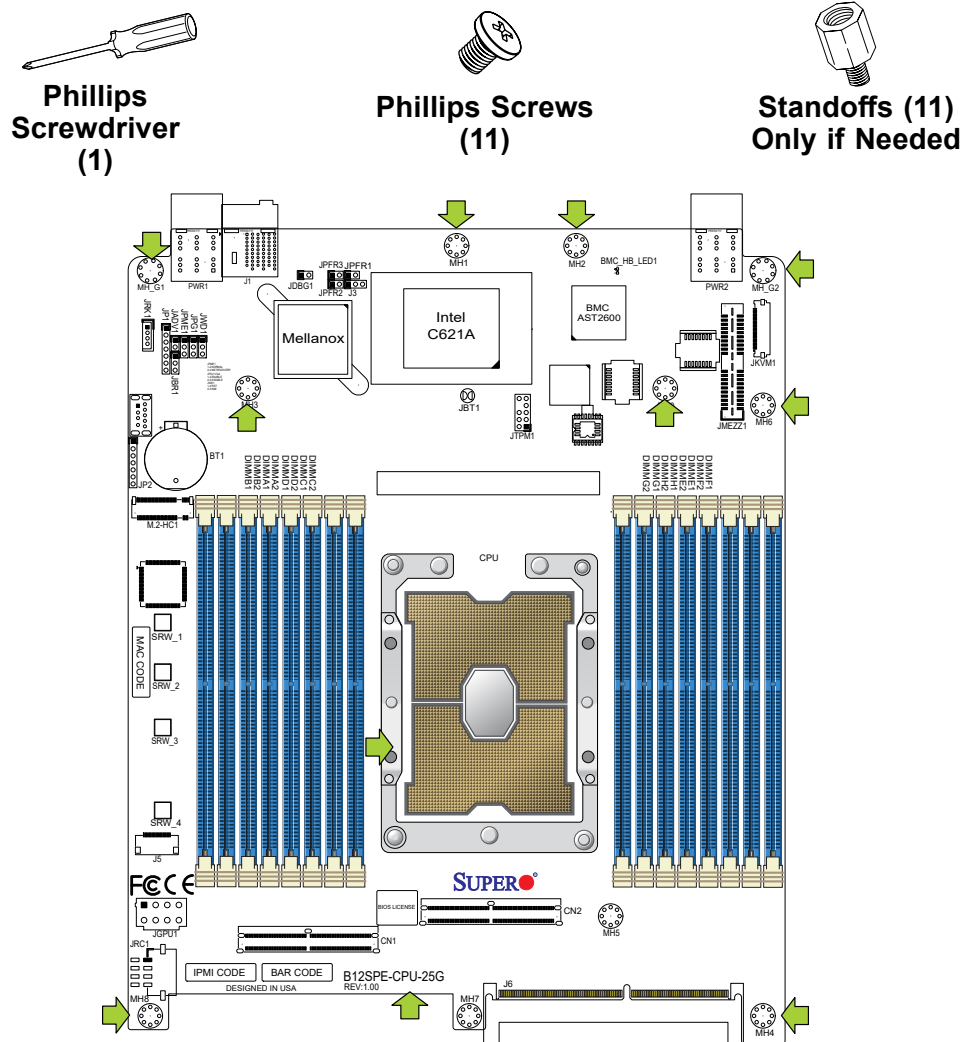
1. Use a T30 Torx-bit screwdriver to loosen the four screws in reverse sequence of #4, #3, #2, and #1.
2. Gently lift the PHM upwards to remove it from the socket.
3. Move the lever to its unlocked position and gently remove the CPU.



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

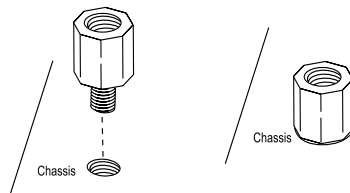


Location of Mounting Holes

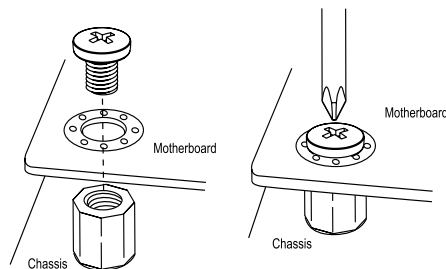
-  **Note 1:** To avoid damaging the motherboard and its components, please do not use a force greater than 8 lbf-in on each mounting screw during motherboard installation.
-  **Note 2:** Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

Installing the Motherboard

1. Locate the mounting holes on the motherboard and the mounting tray. See the previous page for the location.
2. Install the standoffs on the mounting tray. Align the mounting holes on the motherboard against the mounting holes on the tray.



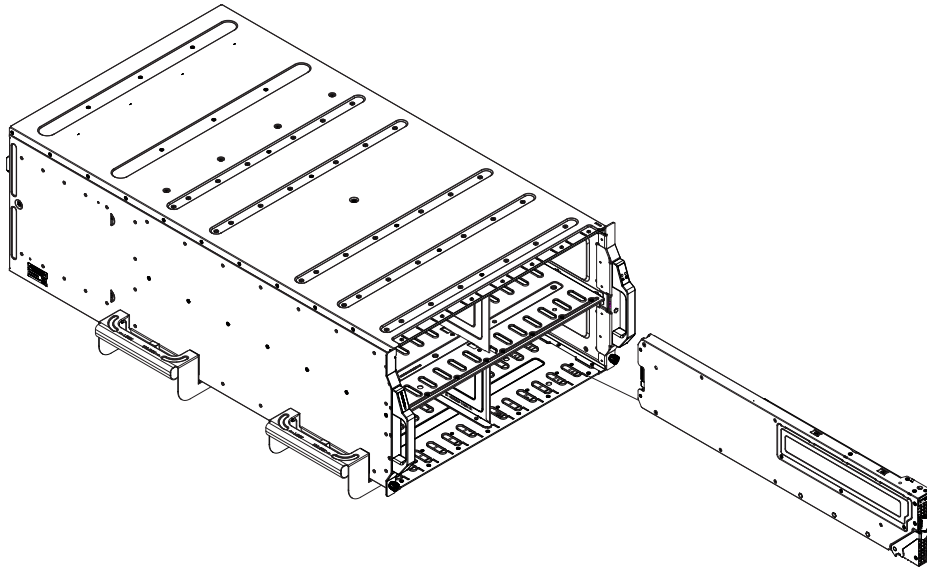
3. Using the Phillips screwdriver, insert a Phillips head #6 screw into the mounting hole on the motherboard and its matching hole on the tray.



4. Repeat step 3 to insert #6 screws to all mounting holes located on the motherboard and the tray and securely install the motherboard onto the tray.

Installing the Motherboard into the Superblade Chassis

1. When the motherboard is securely installed on the mounting tray, push the tray into the Superblade chassis shown below.



2. Once the mounting tray is pushed into the chassis, the connectors on the motherboard's edge will make contact with the chassis' backplane, which provides the connections to the chassis power, network, and other I/O devices.

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

2.4 Memory Support and Installation



Note: Check the Supermicro website for recommended memory modules.



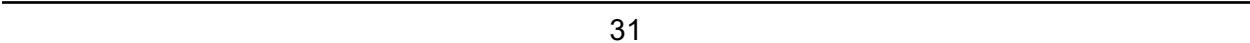
Important: Exercise extreme care when installing or removing DIMM modules to prevent any possible damage.

Memory Support

The B12SPE-CPU-25G supports up to 4 TB of DDR4 ECC RDIMM/LRDIMM/3DSLRDIMM memory with speeds of up to 3200 MT/s in 16 slots.

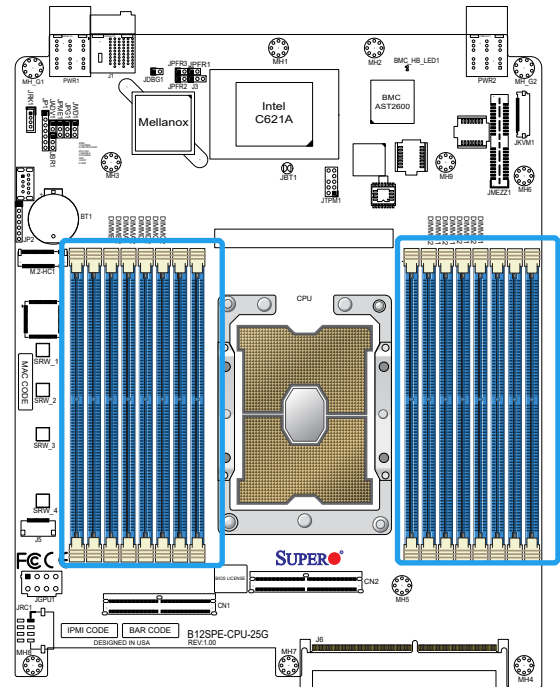
The following memory population sequence table was created on guidelines provided by Intel to support Supermicro motherboards.

Memory Population for the B12/X12 UP Motherboard, 16 DIMM Slots		
DIMMs	Memory Slots	Alternate Slots
1 DIMM	A1	
2 DIMMs	A1, E1,	C1, E1
4 DIMMs	A1, C1, E1, G1	B1, D1, F1, H1
6 DIMMs	A1, B1, C1, E1, F1, G1	A1, C1, D1, E1, G1, H1
8 DIMMs	A1, B1, C1, D1, E1, F1, G1, H1	
12 DIMMs	A1, A2, B1, B2, C1, D1, E1, E2, F1, F2, G1, H1	A1, A2, C1, C2, D1, D2, E1, E2, G1, G2, H1, H2 or A1, A2, B1, C1, C2, D1, E1, E2, F1, G1, G2, H1
16 DIMMs	all	



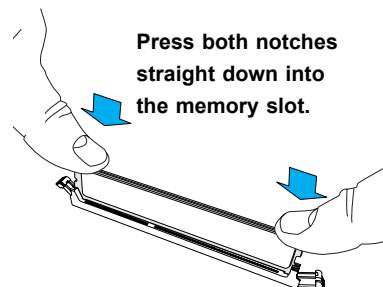
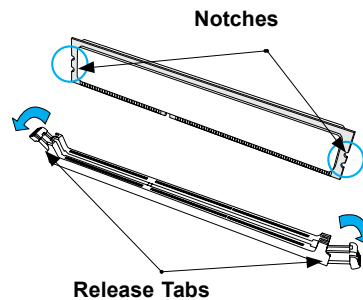
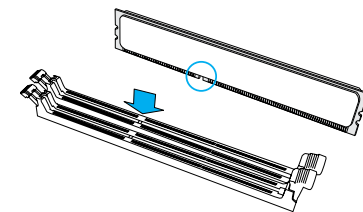
DIMM Installation

1. Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population 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.

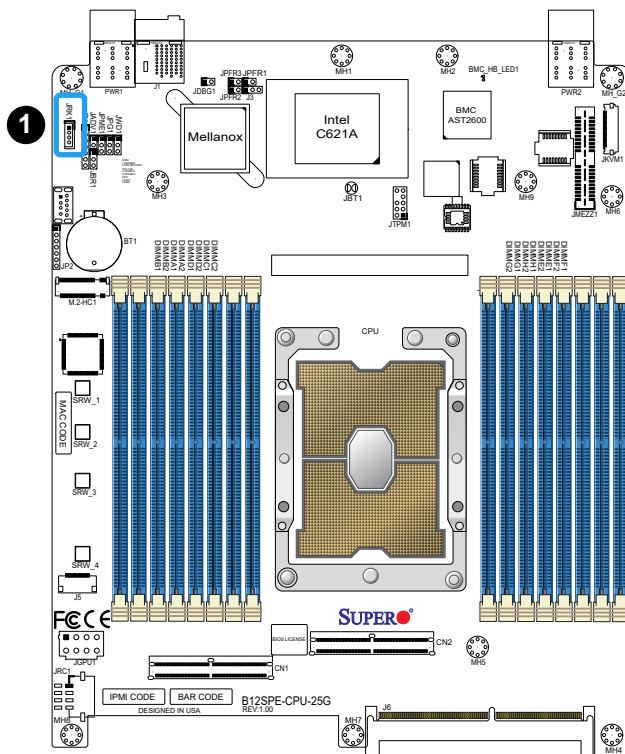


2.5 Connectors

Intel RAID Key Header

The JRK1 header allows you to enable RAID functions. Refer to the table below for pin definitions.

Intel RAID Key Pin Definitions	
Pins	Definition
1	GND
2	PU 3.3 V Stdbby
3	GND
4	PCH RAID KEY



1. Intel RAID Key Header

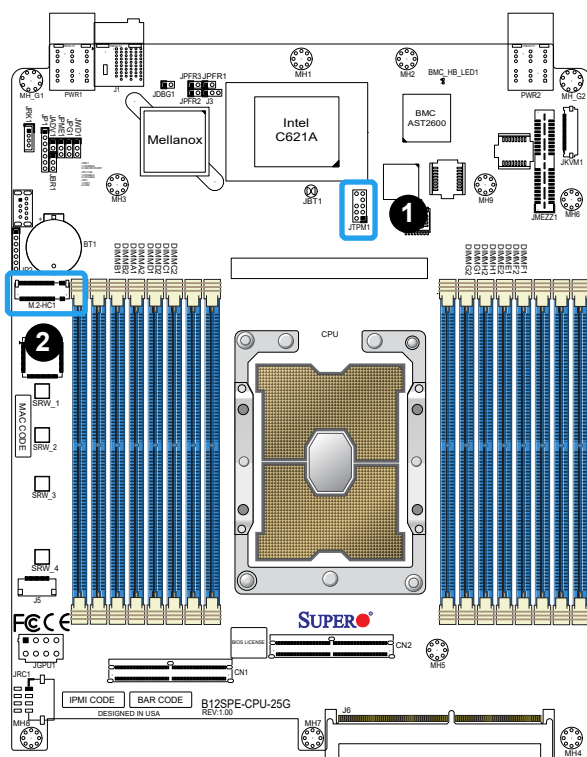
TPM Header

The JTPM1 header is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from a third-party vendor. A TPM/Port 80 connector is a security device that supports encryption and authentication in hard drives. It allows the motherboard to deny access if the TPM associated with the hard drive is not installed in the system.

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	
9	+3.3 V Stby	10	SPI_IRQ#

Hybrid M.2 M-Key PCIe 3.0 x4 or SATA 3.0 Slot

There is one hybrid M.2 M-Key PCIe 3.0 x4 or SATA 3.0 slot that supports M Key. M.2 is formerly known as Next Generation Form Factor (NGFF) and designed for internal mounting devices.



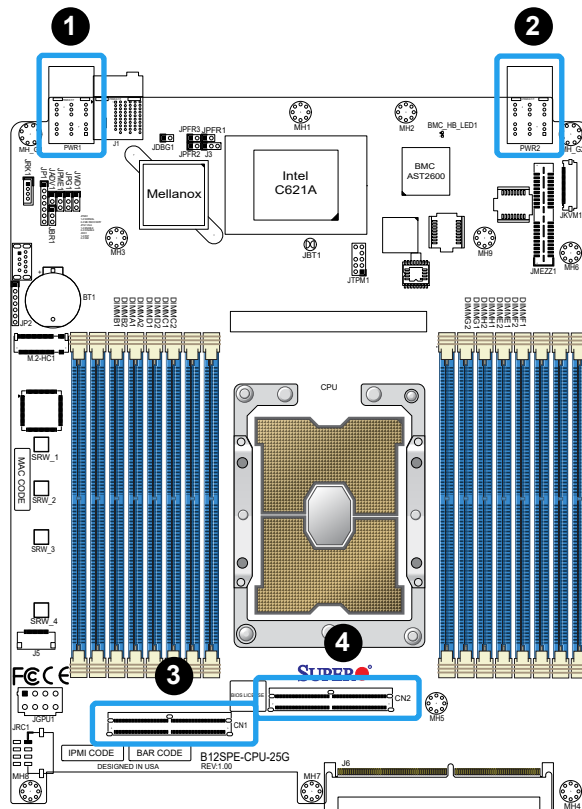
1. TPM Header
2. Hybrid M.2 M-Key PCIe 3.0 x4 or SATA 3.0 Slot

Main Power Connector

PWR1 and PWR2 are primary power supply connectors that provide power to the motherboard via the chassis backplane.

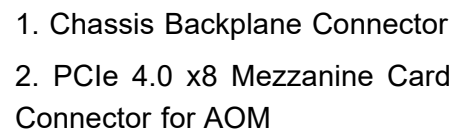
MCIO PCIe 4.0 x16 Connectors

CN1 and CN2 are Mini Cool Edge IO (MCIO) PCIe 4.0 x16 connectors.



Use J1 to connect to the system backplane. This connection provides Ethernet to the system and CMM management.

JMEZZ1 connects to a backplane Ethernet add-on card expansion slot.



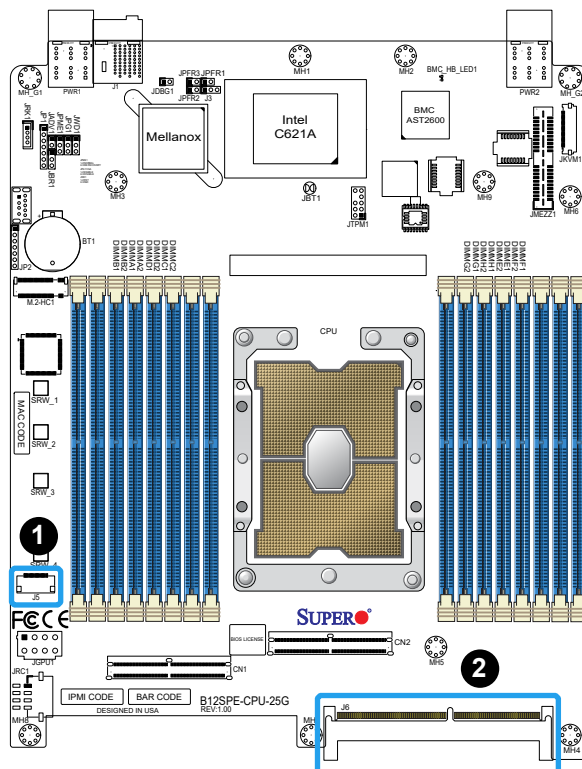
Front Panel Connector

Connect an FPC cable from J5 to the front panel module for power on/off, KVM, and other system LED notifications. Refer to the table below for LEDs and their functions.

	Function	State	Description
	Power Button	N/A	Turns the blade the module on and off
	Power LED	Green	Indicates power status "On"
		Solid Orange	Indicates power status "Off" (with power cables plugged in)
		Flashing Orange	Indicates the node is not ready or not enough power to turn on
	KVM/UID LED	Blue	Indicates KVM is being utilized by the blade unit
		Flashing Blue	Indicates UID activated on the blade module
	Network/IB LED	Flashing Green	Indicates network activity over LAN
		Flashing Orange	Indicates network activity over the Infiniband module
	System Fault LED	Red	Indicates a memory error, overheat, VGA error or any error that prevents booting

PCIe 3.0 x16 SIOM Connector

J6 is the PCIe 3.0 x16 SIOM connector that connects to a SAS HBA/RAID, NVMe, or M.2 device.



1. Front Panel Connector

2. PCIe 3.0 x16 SIOM Connector

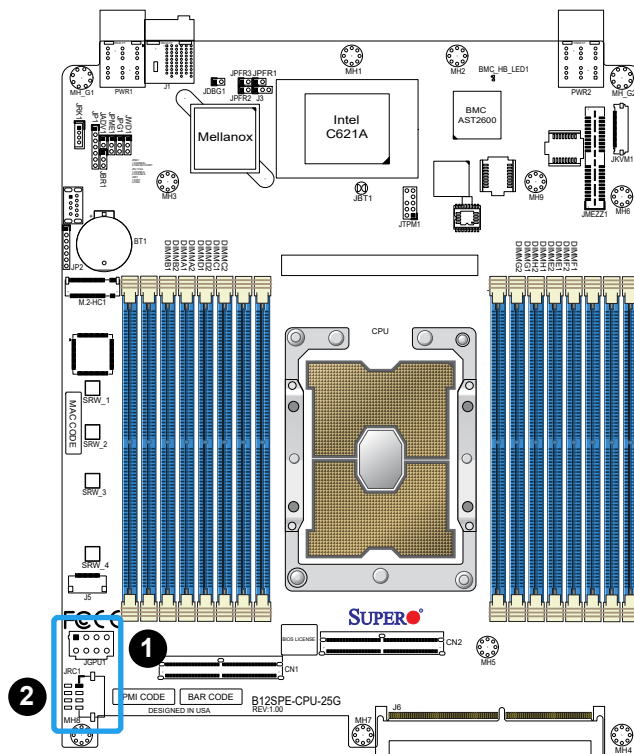
12 V GPU Power Connector

JGPU1 is the EATX 12 V 8-pin power connector.

Proprietary Riser Power Connector

JRC1 is the proprietary riser power connector with a rated 150 W, two 75 W CEM specification.

Proprietary Riser Power Pin Definitions	
Pin#	Definition
1	GND
2	GND
3	GND
4	GND
5	12 V ATX
6	12 V ATX
7	3.3 V ATX
10	3.3 V AUX



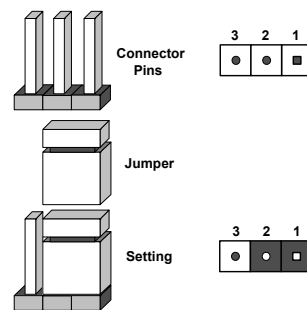
1. 12 V GPU Power
2. Proprietary Rise Power

2.8 Jumper Settings

How Jumpers Work

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

 **Note:** 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.



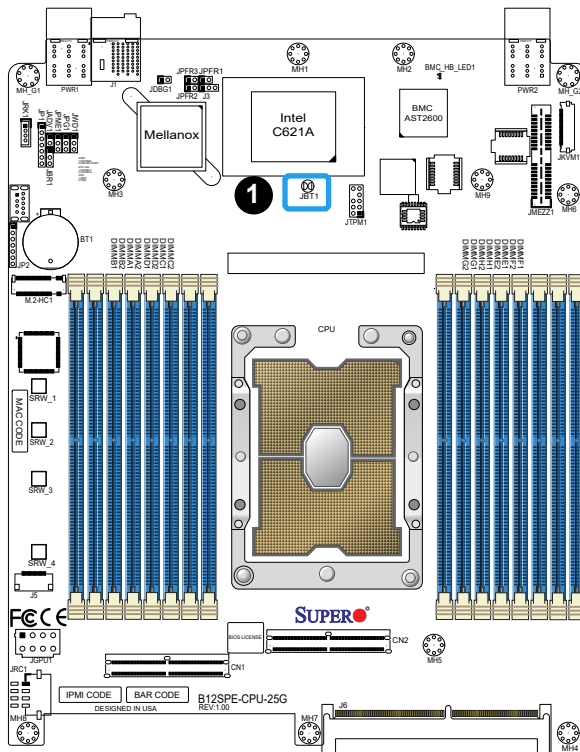
Note: Clearing CMOS will also clear all passwords.

Do not use the PW_ON connector to clear CMOS.



JBT1 contact pads

1. Clear CMOS

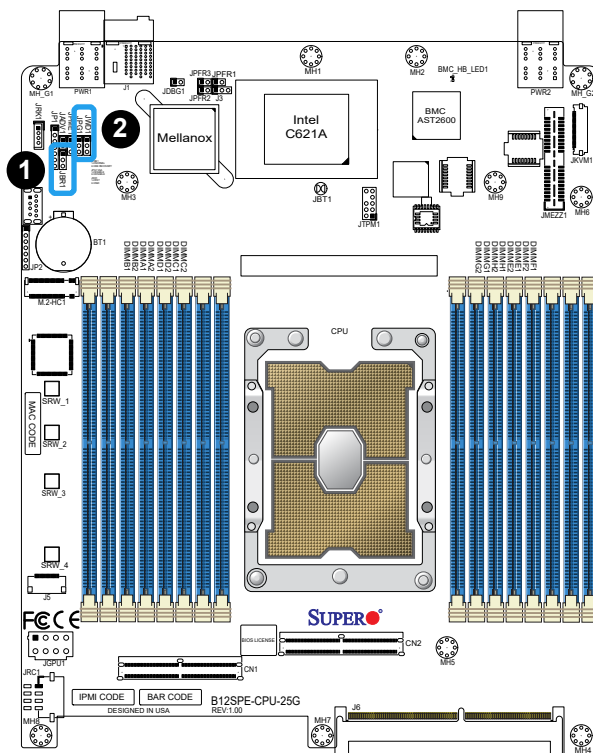


Close pins 2-3 of jumper JBR1 for BIOS recovery. The default setting is on pins 1 and 2 for normal operation. Refer to the table below for jumper settings. The default setting is Normal.

BIOS Recovery Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Normal
Pins 2-3	BIOS Recovery

Use jumper JPG1 to enable or disable the VGA port using the onboard graphics controller. The default setting is Enabled.

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

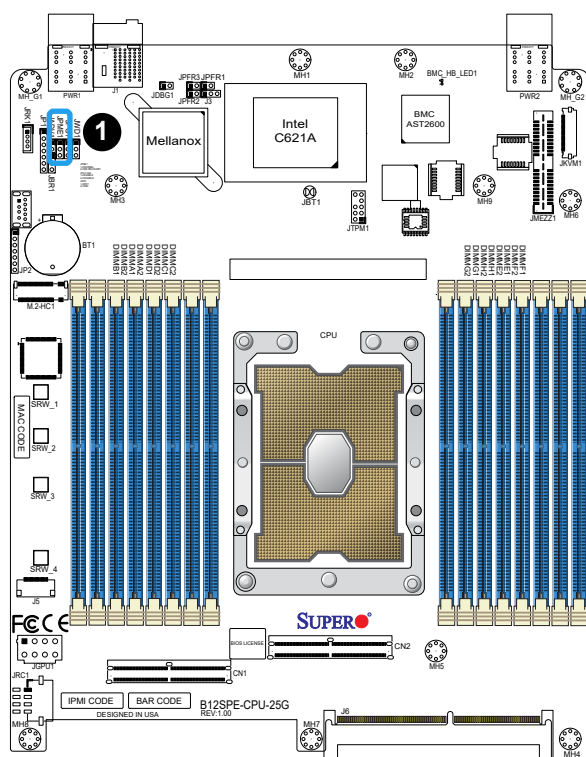


1. BIOS Recovery
2. VGA Enable/Disable

Management Engine (ME) Recovery

Use jumper JPME1 to select ME Firmware Recovery mode, which will limit resource allocation for essential system operation only in order to maintain normal power operation and management. In the single operation mode, online upgrade will be available via Recovery mode. Refer to the table below for jumper settings.

ME Recovery Mode Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Normal
Pins 2-3	ME Recovery



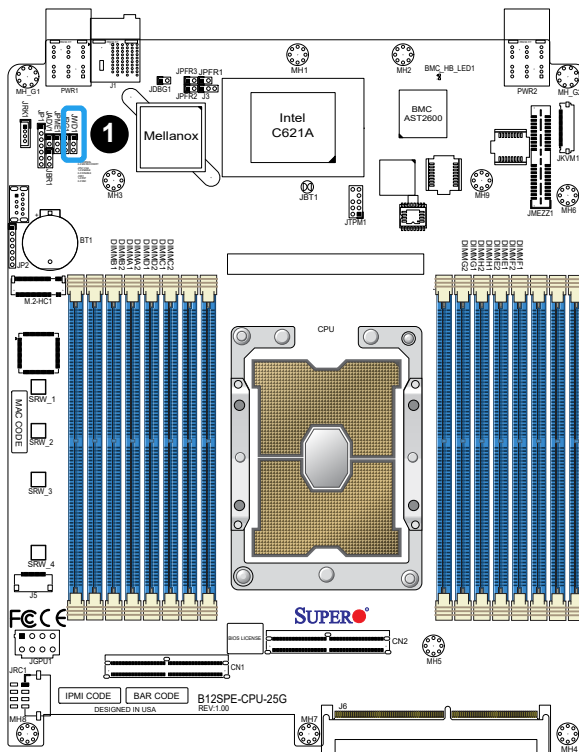
1. ME Recovery

Watch Dog

JWD1 controls the Watch Dog function. Watch Dog is a monitor that can reboot the system when a software application hangs. Jumping pins 1-2 will cause Watch Dog to reset the system if an application hangs. Jumping pins 2-3 will generate a non-maskable interrupt signal for the application that hangs. Watch Dog must also be enabled in BIOS.

 **Note:** When Watch Dog is enabled, users need to write their own application software to disable it.

Watch Dog Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Reset (Default)
Pins 2-3	NMI
Open	Disabled



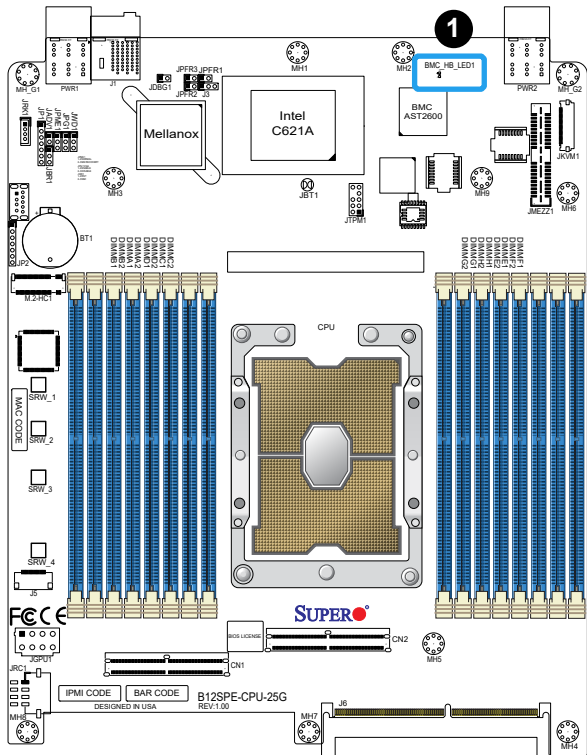
1. Watch Dog Timer

2.9 LED Indicators

BMC Heartbeat LED

BMC_HB_LED1 is the BMC heartbeat LED. When the LED is blinking green, BMC is functioning normally.

BMC LED Indicator	
LED Color	Definition
Blinking Green	BMC Normal



1. BMC LED

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. The battery on your motherboard may be old. Check to verify that it still supplies about 3 VDC. If it does not, replace it with a new one.

No Video

1. If the power is on, but you have no video, remove all add-on cards and cables.
2. Use the speaker to determine if any beep codes are present. Refer to Appendix A for details on beep codes.
3. Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory or try a different one).

System Boot Failure

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

1. Check for any error beep from the motherboard speaker.
 - If there is no error beep, try to turn on the system without DIMM modules installed. If there is still no error beep, replace the motherboard.
 - If there are error beeps, clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper (JBT1). Refer to Chapter 2.8 in Chapter 2.
2. Remove all components from the motherboard, especially the DIMM modules. Make sure that system power is on and that memory error beeps are activated.
3. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this chapter.

Memory Errors

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

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all 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 about 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 CD/DVD.
2. Cable connection: Check to make sure that all cables are connected and working properly.

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

3.2 Technical Support Procedures

Before contacting Technical Support, 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 B12SPE-CPU-25G supports up to 4 TB of DDR4 ECC RDIMM/LRDIMM/LRDIMM 3DS memory with speeds of up to 3200 MT/s in 16 slots.

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. Please unzip the BIOS file onto a bootable USB device. Run the batch file using the format FLASH.BAT filename.rom from your bootable USB device to flash the BIOS. Then, your system will automatically reboot.

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



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

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.

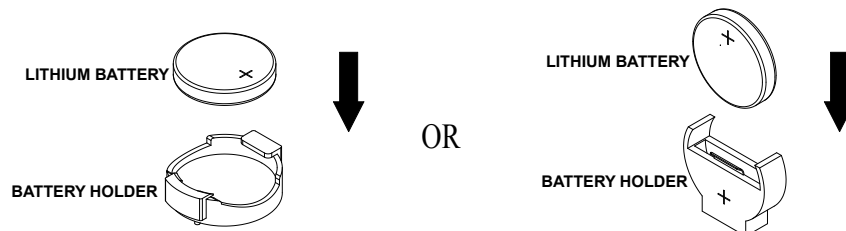
Proper Battery Disposal

Warning: Please handle a used battery carefully. Do not discard it in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency to dispose a 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, replace it with the same type.



3.5 Returning Merchandise for Service

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

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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



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

Starting the Setup Utility

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

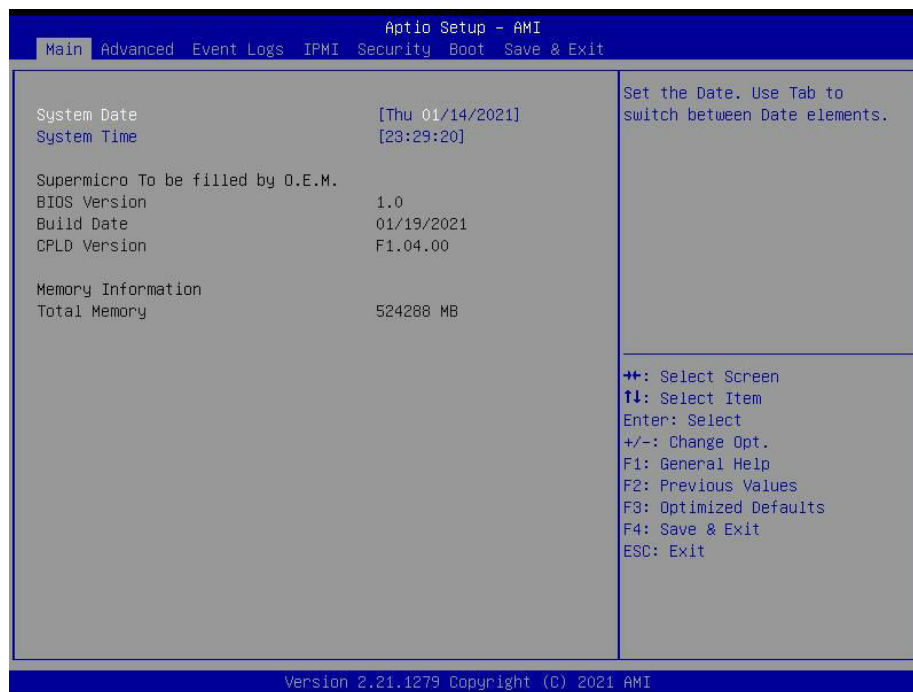
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. "Grayed-out" options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

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

The BIOS setup utility uses a key-based navigation system called hot keys. Most of these hot keys (<F1>, <F10>, <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 enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS setup screen is shown below. The following Main menu items be displayed:



System Date/System Time

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



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

Supermicro B12SPE-CPU-25G

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

Memory Information

Total Memory

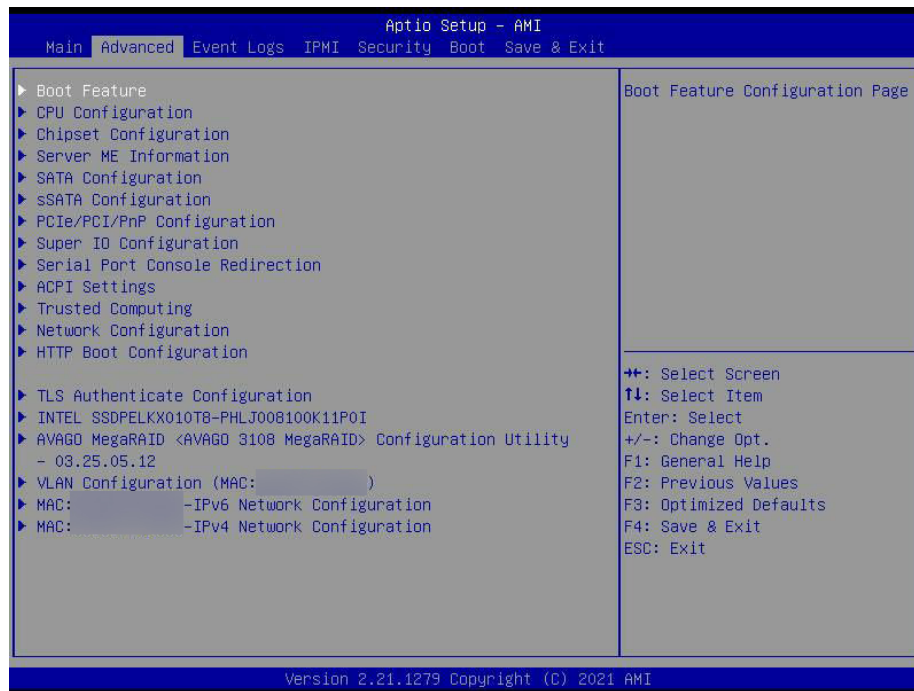
This feature displays the total size of memory available in the system.

Memory Speed

This item displays the memory speed.

4.3 Advanced

Use the arrow keys to select Boot Setup and press <Enter> to access the submenu items.



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

► Boot Feature

Quiet Boot

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

Option ROM Messages

Use this feature to set the display mode for the Option ROM. The options are **Force BIOS** and Keep Current.

Bootup NumLock State

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

Wait For "F1" If Error

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

Interrupt 19 Capture

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 capture Interrupt 19 at boot up 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 and allow the drives attached to these adaptors to function as bootable devices at boot up. The options are **Immediate** and Postponed.

Re-try Boot

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

►Power Configuration**Watch Dog Function**

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

****If the feature above is set to Enabled, Watch Dog Action is available for configuration:***

Watch Dog Action

Use this feature to reset the system or generate NMI. The options are **Reset** and NMI.

Front USB Port(s)

Use this feature to enable or disable front USB ports. If this feature is set to Enabled (Dynamic), then front USB ports can be enabled or disabled with resetting the system. The options are **Enabled**, Disabled, and Enabled (Dynamic).

Power Button Function

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

► CPU Configuration

The following CPU information is displayed:

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

► CPU1 Core Disable Bitmap

Core Disable Bitmap (Hex)

Use this feature to enable all CPU cores. Enter a value to select a core. Enter 0 to disable all cores.

Hyper-threading (ALL)

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

Hardware Prefetcher (Available when supported by the CPU)

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

Adjacent Cache Prefetch (Available when supported by the CPU)

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

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enable to enable the Data Cache Unit (DCU) Streamer Prefetcher, which streams and prefetches data and sends it to the Level 1 data cache to improve data processing and system performance. The options are **Enable** and Disable.

DCU IP Prefetcher

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

LLC Prefetch

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

Extended APIC

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

Enable Intel® TXT

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

VMX

Use this feature to enable the Vanderpool Technology. This technology allows the system to run several operating systems simultaneously. The options are Disable and **Enable**.

Enable SMX

Use this feature to enable safer mode extensions. 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)**

Use this feature to enable or disable total memory encryption. The options are Disabled and **Enabled**.

****If the feature above is set to Enabled, the next five features are displayed:***

Total Memory Encryption Multi-Tenant (TME-MT)**Max TME-MT Keys****Software Guard Extension (SGX)****SGX Factory Reset****SW Guard Extensions (SGX)****SGX Package Into In-Band Access****Limit CPU PA to 46 Bits**

Use this feature to limit the CPU physical address to 46 bits to support older hyper-v. The options are Disable and **Enable**.

► Advanced Power Management Configuration**Power Technology**

Use this feature to enable or disable processor power management features. The options are Disable, Energy Efficient, and **Custom**.

Power Performance Tuning

Use this feature to select whether the BIOS or the operating system chooses energy performance tuning. The options are **OS Controls EPB** and BIOS Controls EPB.

****If the feature above is set to BIOS Controls EPB, the next feature is available for configuration:***

ENERGY_PERF_BIAS CFG Mode

Use this feature to set the energy performance bias. The options are Maximum Performance, Performance, Balanced Performance, **Balanced Power**, and Power.

► CPU P State Control

SpeedStep (Pstates)

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

Dynamic SST-PP

Use this feature to enable or disable Intel Speed Select Technology Performance Profile (SST-PP). The options are **Disable** and Enable.

Intel SST-PP

Use this feature to select the base frequency conditions for SST-PP. The options are **Base**, Config 3, and Config 4.

Activate SST-BF

Use this feature to enable or disable Intel Speed Select Technology Base Frequency. The options are **Disable** and Enable.

****If the feature above is set to Enable, the next feature is available for configuration:***

Configure SST-BF

Enable this feature for the BIOS to configure the SST-BF High Priority Cores so the software does not configure it. The options are Disable and **Enable**.

EIST PSD Funtion

This feature allows you to choose between Hardware and Software to control the processor's frequency and performance (P-state). In HW_ALL mode, the processor hardware is responsible for coordinating the P-state, and the OS is responsible for keeping the P-state request up to date on all Logical Processors. In SW_ALL mode, the OS Power Manager is responsible for coordinating the P-state, and must initiate the transition on all Logical Processors. In SW_ANY mode, the OS Power Manager is responsible for coordinating the P-state and may initiate the transition on any Logical Processors. The options are **HW_ALL** and SW_ALL.

Turbo Mode

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

CPU Flex Ratio Override

Use this feature to enable or disable CPU Flex Ratio Prgramming. The options are **Disable** and **Enable**.

*If the feature above is set to **Enable**, the next feature is available for configuration:*

CPU Core Flex Ratio

Use this feature to set the non-turbo mode processor core ratio multiplier. The default value is **23**.

►Hardware PM State Control

Hardware P-States

This setting allows you to select between OS and hardware-controlled P-states. Selecting Native Mode allows the OS to choose a P-state. Selecting Out of Band Mode allows the hardware to autonomously choose a P-state without OS guidance. Selecting Native Mode with No Legacy Support functions as Native Mode with no support for older hardware. The options are **Disable**, Native Mode, Out of Band Mode, and Native Mode with No Legacy Support.

►Frequency Prioritization

RAPL Prioritization

Use this feature to enable the RAPL balancer. The options are **Enable** and **Disable**.

►CPU C State Control

Enable Monitor MWAIT

Select **Enabled** to enable the Monitor/Mwait instructions. The Monitor instructions monitors a region of memory for writes, and MWait instructions instruct the CPU to stop until the monitored region begins to write. The options are **Disable** and **Enable**.

CPU C6 Report

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

Enhanced Halt State (C1E)

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

► Package C State Control

Package C State

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

► CPU T State Control

Software Controlled T-States

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

If the feature above is set to Enable, the next feature is available for configuration:

T-State Throttle Level

Use this feature to enable or disable CPU throttling, which reduces power consumption. 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 the wrong values in the following features may cause the system to malfunction.

► North Bridge

► Uncore Configuration

The following Uncore information is displayed:

- Number of CPU
- Number of IIO
- Current UPI Link Speed

- Current UPI Link Frequency
- Global MMIO Low Base / Limit
- Global MMIO High Base / Limit
- PCI-e Configuration Base / Size

Degrade Precedence

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

Link L0p Enable

When this feature is enabled, the CPU reduces 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 the UPI technology support. The options are Disable, Enable, and **Auto**.

Link L1 Enable

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

XPT Remote Prefetch

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

KTI Prefetch

If this feature is set to enabled, the KTI prefetch preloads the L1 cache with data deemed relevant to allow the memory read to start earlier on a DDR bus in an effort to reduce latency. The options are Disable, Enable, and **Auto**.

Local/Remote Threshold

Use this feature to set the threshold for the IRQ signal, which handles hardware interrupts. The options are Disable, **Auto**, Low, Medium, and High.

IO Directory Cache (IODC)

IO directory cache generates snoops instead of memory lookups for remote Invltom. IODC is supported only in four socket configurations and not in eight. The options are Disable, **Auto**, Enable for Remote Invltom Hybrid Push, Invltom AllocFlow, Enable for Remote Inv.

SNC (Sub NUMA)

Sub NUMA clustering (SNC) creates two localized domains from the memory controller, then the processor maps addresses from the controllers to lower LLC and memory latency. The options are **Disable**, Enable SNC2 (2-clusters), and Enable SNC4 (4-clusters).

XPT Prefetch

This prefetcher performs memory read requests to improve memory latency. The options are Disable, Enable, and **Auto**.

Snoop Throttle Configuration

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

PCIe Remote P2P Relaxed Ordering

The default for this feature is disable, so the hardware enforces P2P write ordering. The options are **Disable** and Enable.

Stale AtoS

In the in-memory directory, the A state is snoop All and the S state is Shared. Data in the A state may be in one socket exclusively or in a modified state, whereas the data in the S state may be shared with multiple sockets. If this feature is enabled, A state returns snoop misses and transitions them to S state. The options are Disable, Enable, and **Auto**.

LLC dead line alloc

If this feature is enabled, the LLC can opportunistically fill dead lines. If this feature is disabled, deadlines are never filled in the LLC. The options are Disable, **Enable**, and Auto.

►Memory Configuration

Integrated Memory Controller (iMC)

Enforce POR

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

PPR Type

Post Package Repair (PPR) provides additional spare capacity within a DDR4 memory module that is used to replace faulty cell areas detected during the system boot. PPR offers a hard and soft repair. The soft repair provides a quick and temporary fix, while the hard repair provides permanent fix. The options are PPR Disable, 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 for data scrambling of DDR4 memory. The options are Disable and **Enable**.

Legacy ADR Mode

Use this setting to enable or disable Legacy Asynchronous DRAM Refresh (ADR), a feature that allows the device to store pending write data into NVDIMMs in the event of a power failure or system crash. The options are Enable and **Disable**.

Erase-Arm NVDIMMs

Use this feature to enable or disable erase and arm NVDIMMs. The options are Disable and **Enable**.

Restore NVDIMMs

Use this feature to enable or disable automatic restoring of NVDIMMs. The options are Disable and **Enable**.

Interleave NVDIMMs

Use this feature to enable or disable interleaving for NVDIMMs. The options are **Disable** and Enable.

2x Refresh Enable

Use this feature to enable or disable a 2x refresh rate. The options are **Auto**, **Disable**, and **Enable**.

► Memory Topology

This submenu displays memory detected by the system.

► Memory RAS Configuration

Enable Pcode WA for SAI PG

Use this feature to enable Pcode work around for SAI policy group for A step. The options are **Disabled** and **Enabled**.

Mirror Mode

Single device data correction +1 (SDDC Plus One) organizes data in a single bundle (x4/x8 DRAM). If any or all the bits become corrupted, corrections occur. The x4 condition is corrected on all cases. The x8 condition is corrected only if the system is in Lockstep Mode. The options are **Disabled**, **Full Mirror Mode**, and **Partial Mirror Mode**.

UEFI ARM Mirror

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

Correctable Error Threshold

Use this feature to specify the threshold value for correctable memory-error logging, which sets a limit on the maximum number of events that can be logged in the memory error log at a given time. The default setting is **7fff**.

Partial Cache Line Sparing PCLS

Use this feature to enable or disable Partial Cache Line Sparing. The options are **Disabled** and **Enabled**.

ADDDC Sparing

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

Patrol Scrub

Patrol Scrubbing is a process that allows the CPU to correct correctable memory errors detected on a memory module and sends the correction to the requestor (the original source). When this feature is set to Enable, the IO hub 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 is scrubbed every day. The options are **Disabled**, Enabled, and Enable at End of POST.

► IIO Configuration

► CPU1 Configuration

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

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

- Port 1A
- Port 2A
- Port 4A
- Port 4C
- Port 4D
- Port 5A
- Port 5C

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:

- PCI-E Port Link Status
- PCI-E Port Link Max
- PCI-E Port Link Speed

PCI-E 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

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

****If the feature above is set to No, the feature below is available for configuration:***

Prioritize TPH

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

Relaxed Ordering

Select Yes to enable Relaxed Ordering support, which allows certain transactions to violate the strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been enqueued. The options are **No** and Yes.

► Intel VT® for Directed I/O (VT-D)

Intel® VT for Directed I/O

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

ACS Control

Select Enable to program Access Control Services (ACS) to the chipset PCIe root port bridge. Select No to program ACS to all PCIe root port bridges. The options are **Enable** and Disable.

Interrupt Remapping

Select Enable for Interrupt Remapping support to enhance system performance. The options are **Yes** and No.

X2APIC Opt Out

Use this feature to enable or disable X2APIC_OPT_OUT bit. The options are Enable and **Disable**.

Pre-boot DMA Protection

Use this feature to enable or disable pre-boot DMA protection. The options are **Disable** and **Enable**.

► Intel® VMD technology

► Intel® VMD for Volume Management Device on CPU1

VMD Config for IOU3

Disable/Enable VMD

Use this feature to enable or disable VMD in this socket. The options are **Disable** and **Enable**.

****If the feature above is set to Enable, the five features below are available for configuration:***

VMD port 4A/4B/4C/4D

Use this feature to enable or disable VMD technology for this port. The options are **Disable** and **Enable**.

Hot Plug Capable

Use this feature to enable or disable hot plug for this port. The options are **Disable** and **Enable**.

PCI-E ASPM Support (Global)

Use this feature to enable or disable ASPM support for all downstream devices. The options are **No**, **Per-Port**, and **L1 Only**.

► South Bridge

The following USB information display:

- USB Module Version
- USB Devices

Legacy USB Support

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

XHCI Hand-off

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

Port 60/64 Emulation

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

PCIe PLL SSC

Use this feature to enable or disable PCIe PLL SSC. The options are **Disabled** and Enabled.

Port 61h Bit-4 Emulation

Select Enabled to enable the emulation of Port 61h bit-4 toggling in System Management Mode (SMM). The options are **Disabled** and Enabled.

► Server ME Information

The following Unocore information display:

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

► SATA Configuration

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

SATA Controller

Use this feature to enable or disable the onboard SATA controller supported by the Intel PCH chip. The options are Disable and **Enable**.

Configure SATA as

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

****If the feature above is set to RAID, the SATA RSTe Boot Info and SATA RAID Option ROM/UEFI Driver are available for configuration:***

SATA RSTe Boot Info

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

Support Aggressive Link Power Management

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

SATA RAID Option ROM/UEFI Driver

Select UEFI 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 - Port 7

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

Port 0 - Port 7

Use this feature to enable or disable the specified SATA port. The options are Disable and **Enable**.

Port 0 - Port 7 Hot Plug

Set this feature to Enable for hot plug support, which allows you to replace a SATA drive without shutting down the system. The options are **Disable** and Enable.

Port 0 - Port 7 Spin Up Device

Set this feature to enable or disable the PCH to initialize the device. The options are **Disable** and Enable.

Port 0 - Port 7 SATA Device Type

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

► sSATA Configuration

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

sSATA Controller

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

Configure sSATA as

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

****If the feature above is set to RAID, the sSATA RSTe Boot Info and sSATA RAID Option ROM/UEFI Driver are available for configuration:***

sSATA RSTe Boot Info

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

Support Aggressive Link Power Management

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

sSATA RAID Option ROM/UEFI Driver

Select UEFI 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 - Port 5

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

Port 0 - Port 5

Use this feature to enable or disable the specified SATA port. The options are Disable and **Enable**.

Port 0 - Port 5 Hot Plug

Set this feature to Enable for hot plug support, which allows you to replace a SATA drive without shutting down the system. The options are **Disable** and Enable.

Port 0 - Port 5 Spin Up Device

Set this feature to enable or disable the PCH to initialize the device. The options are **Disable** and **Enable**.

Port 0 - Port 5 SATA Device Type

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

►PCIe/PCI/PnP Configuration**PCI Bus Driver Version****PCI Devices Common Settings:****Above 4G Decoding (Available if the system supports 64-bit PCI decoding)**

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

SR-IOV Support

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

ARI Support

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

Bus Master Enable

Use this feature to enable the Bus Master, which enables the Bus Master Attribute for DMA transaction. The options are **Disabled** and **Enabled**.

MMIO High Base

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

MMIO High Granularity Size

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

Maximum Read Request

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

MMCFG Base

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

NVMe Firmware Source

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

VGA Priority

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

Onboard Video Option ROM

Use this feature to select which firmware function to be loaded for LAN1 used for system boot. The options are Disabled and **Legacy** (if the Boot Mode Select feature under the Boot tab is set to Legacy), Disabled and **EFI** (if the Boot Mode Select feature under the Boot tab is set to UEFI), and Disabled, Legacy, and **EFI** (if the Boot Mode Select feature under the Boot tab is set to Dual).

Slot 1 PCI-E x16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled and **Legacy** (if the Boot Mode Select feature under the Boot tab is set to Legacy), Disabled and **EFI** (if the Boot Mode Select feature under the Boot tab is set to UEFI), and Disabled, Legacy, and **EFI** (if the Boot Mode Select feature under the Boot tab is set to Dual).

Slot 2 PCI-E x16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled and **Legacy** (if the Boot Mode Select feature under the Boot tab is set to Legacy), Disabled and **EFI** (if the Boot Mode Select feature under the Boot tab is set to UEFI), and Disabled, Legacy, and **EFI** (if the Boot Mode Select feature under the Boot tab is set to Dual).

CPU1 Slot 3 PCI-E x8 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled and **Legacy** (if the Boot Mode Select feature under the Boot tab is set to Legacy), Disabled and **EFI** (if the Boot Mode Select feature under the Boot tab is set to UEFI), and Disabled, Legacy, and **EFI** (if the Boot Mode Select feature under the Boot tab is set to Dual).

Onboard LAN1 - LAN2 Option ROM

Use this feature to select a desired firmware function to be loaded for onboard LAN2 - LAN6. The options are Disabled and **Legacy** (if the Boot Mode Select feature under the Boot tab is set to Legacy), Disabled and **EFI** (if the Boot Mode Select feature under the Boot tab is set to UEFI), and Disabled, Legacy, and **EFI** (if the Boot Mode Select feature under the Boot tab is set to Dual).

Onboard NVMe1 Option ROM

Use this feature to select a desired firmware function to be loaded for the specified NVMe slot. The options are Disabled and **Legacy** (if the Boot Mode Select feature under the Boot tab is set to Legacy), Disabled and **EFI** (if the Boot Mode Select feature under the Boot tab is set to UEFI), and Disabled, Legacy, and **EFI** (if the Boot Mode Select feature under the Boot tab is set to Dual).

► Super IO Configuration

The following Super IO information is 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 the selected onboard serial port. The options are Disabled and **Enabled**.

Device Settings

This feature displays the status of the serial port.

Change Settings

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

► Serial Port 2 Configuration

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

Serial Port 2

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

Device Settings

This feature displays the status of the serial port.

Change Settings

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

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

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

► Serial Port Console Configuration

COM1 Console Redirection

Select Enabled to enable console redirection support for the serial port. The options are Enabled and **Disabled**.

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

► COM1 Console Redirection Settings

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

Terminal Type

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

Bits Per Second

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

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 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 the settings for Function Keys and KeyPad used for Putty, which is a terminal emulator designed for the Windows OS. The options are **VT100**, LINUX, XTERMR6, SC0, ESCN, and VT400.

Redirection After BIOS POST

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

► Legacy Console Redirection Settings

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

Legacy Serial Redirection Port

Use this feature to select the COM port to display the redirection of Legacy OS and Legacy OPRM messages. The default is **COM1**.

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.

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.

EMS (Emergency Management Services) Console Redirection

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

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

► Console Redirection Settings

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

Out-of-Band Mgmt Port

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

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

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

Flow Control

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

Data Bits, Parity, Stop Bits

► ACPI Settings

Numa

Use this feature to enable or disable Non-Uniform Memory Access (NUMA), a feature that improves memory-to-processor communication and performance. The options are Disabled and **Enabled**.

UMA-Based Clustering

Use this feature to enable or disable Uniform Memory Access (UMA) clustering. The options are Disable (All2All) and **Hemishpere (2-clusters)**.

WHEA Support

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

►Trusted Computing

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

- Vendor Name
- Firmware Version

Security Device Support

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

- Active PCR Bank
- SHA256 PCR Bank

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

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending Operation

Use this feature to schedule a TPM-related operation to be performed by a security device for system data integrity. Your system reboots to carry out a pending TPM operation. The options are **None** and TPM Clear.

Platform Hierarchy

Use this feature to disable or enable platform hierarchy for platform protection. The options are Disabled and **Enabled**.

Storage Hierarchy

Use this feature to disable or enable storage hierarchy for cryptographic protection. The options are Disabled and **Enabled**.

Endorsement Hierarchy

Use this feature to disable or enable endorsement hierarchy for privacy control. The options are Disabled and **Enabled**.

PH Randomization

Use this item to disable or enable Platform Hierarchy (PH) Randomization. The options are **Disabled** and Enabled.

TXT Support

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

► Network Stack Configuration

Network Stack

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

****If the feature above is set to Enabled, the next six features are available for configuration:***

Ipv4 PXE Support

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

Ipv4 HTTP Support

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

Ipv6 PXE Support

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

Ipv6 HTTP Support

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

PXE boot wait time

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

Media detect count

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

► HTTP Boot Configuration**HTTP Boot Configuration****HTTP Boot Policy**

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

Priority of HTTP Boot:**Instance of Priority 1:**

Use this feature to set the rank target port. The default value is **1**.

Select IPv4 or IPv6

Use this feature to select which LAN port to boot from. The options are **IPv4** and IPv6.

Boot Description

Highlight the feature and press enter to create a boot description. The description cannot be more than 75 characters.

Boot URI

Highlight the feature and press enter to create a boot URI.

Instance of Priority 2:

Use this feature to set the rank target port. The default value is **0**.

► TLS Auth Configuration

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

► Server CA Configuration**► Enroll Certification****Enroll Certification Using File**

Use this feature to enroll certification from a file.

Cert GUID

Use this feature to 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

Use this feature to delete certification.

►INTEL SSDPELKX010T8-PHLJ008100K11P0I

- PCI Generic Information
- Bus Protocol:
- PCI Vendor/Device ID:
- PCI Vendor subsystem id:
- PCI subsystem id:
- Model Number:
- Serial Number:
- IEEE Organization Unique Id:
- PCIe Maximum Link Width:
- PCIe Maximum Speed:
- PCIe Negotiated Link Width:
- PCIe Negotiated Link Speed:
- NVMe Drive Information
- Drive Health:
- Firmware Revision:
- Option ROM Revision:
- Total Drive Capacity:

- Number of Namespaces:
- Namespace Id:
- Device Capacity
- Device Size

▶ **AVAGO MegaRaid <AVAGO 3108 MegaRAID> Configuration Utility - 03.25.05.12**

▶ **Main Menu**

▶ **Configuration Management**

▶ **Create Virtual Drive**

Select RAID Level

Use this feature to select the RAID level. The options are **RAID0**, RAID1, RAID00.

Select Drives From

Use this feature to select the physical drive option. The options are **Unconfigured Capacity** and Free Capacity.

▶ **Select Drives**

▶ **Apply Changes**

Apply the changes made regarding the drive selection.

Select Media Type

Use this feature to select the media type. The options are SSD, HDD, and **Both**.

Select Interface From

Use this feature to select the technology of the drive. The options are SAS, SATA, and **Both**.

Select Drives From

Use this feature to select the physical drive option. The options are **Unconfigured Capacity** and Free Capacity.

Logical Sector Size

Use this feature to select the sector size of the drive. The options are 512 B, 4 KB, and **Both**.

CHOOSE UNCONFIGURED DDRIVES:

Drive Port 0 (Drive information may vary depending on detection)

Use this feature to select the physical drive option. The options are Disabled and **Enabled**.

Check All

Check all drives.

Uncheck All

Uncheck all drives.

►Apply Changes

Apply the changes made regarding the drive selection.

CONFIGURE VIRTUAL DRIVE PARAMETERS:

Virtual Drive Name

Assign a name for the virtual drive.

Virtual Drive Size

Assign the amount of the storage space for the virtual drive.

Strip Size

Use this feature to select the strip element size for the virtual drive. The options are 64 KB, 128 KB, **256 KB**, 512 KB, 1 MB.

Read Policy

Use this feature to select the read cache policy for the virtual drive. The options are No Read Ahead and **Read Ahead**.

Write Policy

Use this feature to select the write cache policy for the virtual drive. The options are Write Through, **Write Back**, and Always Write Back.

I/O Policy

Use this feature to select the I/O policy for the virtual drive. The options are Direct and **Cached**.

Access Policy

Use this feature to select the access policy for the virtual drive. The options are **Read/Write**, Read Only, and Blocked.

Drive Cache

Use this feature to select the virtual drive cache setting. The options are **Unchanged**, Enable, and Disabled.

Disable Background Initialization

Use this feature to enable or disable the background initialization status. Select No to leave it enabled. The options are **No** and Yes.

Default Initialization

Select No to disable the initialization of the virtual drive, Fast to initialize the first 100MB of the virtual drive, and Full to initialize the entire drive. The options are **No**, Fast, and Full.

Emulation Type

Use this feature to select the emulation type. The options are **Default**, Disable, and Force.

► Create Profile Based Virtual Drive**► Generic RAID 0****► Generic RAID 1****Drive Selection Criteria**

The information displayed here is dependent on what the system detects.

PROFILE PARAMETERS:**Virtual Drive Name**

Displays the amount of the virtual drive storage space.

Power Save Mode

The setting is Controller Defined.

Strip Size

Displays the strip element size of the virtual drive.

Read Policy

Displays the read policy of the virtual drive.

Write Policy

Displays the write cache policy of the virtual drive.

I/O Policy

Displays the Input and Output policy of the virtual drive.

Drive Cache

Use this feature to select the virtual drive cache setting. The options are Unchanged, **Enable**, and Disable.

Default Initialization

Displays the virtual drive initialization setting.

► Save Configuration

Save the configuration that the wizard created. The options are Yes and **No**.

► Clear Configuration

Use this feature to delete all existing configurations on the RAID controller.

► Controller Management

Product Name

Displays the name of the controller.

Serial Number

Displays the serial number of the controller.

Controller Status

Displays the current status of the controller.

Select Boot Device

Use this feature to select the primary bootable device.

PCI ID

Displays the manufacturer-assigned ID.

PCI Slot Number

Displays the PCI slot number that the controller is plugged in.

Package Version

Displays the version of the controller package.

Firmware Version

Displays the controller firmware version.

NVDATA Version

Displays the NVDATA version.

Connector Count

Displays the number of host data ports present on the controller.

Drive Count

Displays the number of drives currently attached to the controller.

Virtual Drive Count

Displays the number of virtual drives present on the controller.

► Advanced Controller Management**► Clear Controller Events**

Use this feature to delete all of the existing controller events.

► Save Controller Events**Select File System**

Choose the file system to save the controller logs.

Select Directory

Choose the directory to save the controller logs. The options are **Current Dir** and **EFI**.

Enter Filename

Enter a filename for the event log.

► Save TTY Log**Select File System**

Choose the file system to save the controller logs.

Select Directory

Choose the directory to save the controller logs. The options are **Current Dir** and **EFI**.

Enter Filename

Enter a filename for the event log.

Entries to Save

Enter the number of entries to be saved. The options are 2 KB, 4 KB, 8 KB, 16 KB, and **All**.

► **Save Log**

Save the logs to the specified file system and directory.

► **Manage Link Speed**

VIEW THE PHY SETTINGS FOR THE CONTROLLER AND CHANGE THEM IF NEEDED.

Phy #0 (0x5000C500C9EAF29D)

Phy #2 (0x5000C500C9EAF0C1)

Phy #3 - #7 (0x0000000000000000)

Choose a link speed for the physical port. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

► **OK**

Select OK to save the changes.

► **Cancel**

Select Cancel to cancel the changes.

► **Manage MegaRAID Advanced Software Options**

SAFE ID

Displays the 40-digit ID number generated by the controller.

Serial Number

Displays the 10-digit serial number generated by the controller.

► **Activate**

Displays the summary and allows you to activate advanced software options. Then select OK to activate.

► **Schedule Consistency Frequency**

Consistency Check Frequency

The feature checks the frequency of the consistency check runs. The options are Disable, Hourly, Daily, **Weekly**, and Monthly.

Consistency Check Start Date

Assign the start date for the consistency check operation.

Consistency Check Start Time

Assign the start time for the consistency check operation.

Consistency Check Mode

Use this feature to select the consistency check mode. The options are **Concurrent** and Sequential.

SELECT VIRTUAL DRIVES TO CHECK:**► Apply Changes**

Saves changes made to the entire form.

► Set Factory Defaults

Restores factory defaults for all the controller properties.

► Switch to JBOD mode

Use this feature to switch to JBOD or RAID mode.

► Advanced Controller Properties**► Cache And Memory****Cache:****Cache Flush Interval**

This feature displays and allows you to modify the interval (in seconds) the contents of the onboard data cache are flushed. The default value is **4**.

Preserved Cache

This feature displays if the controller cache is preserved because of missing or offline virtual drives. The options are **Concurrent** and Sequential.

CACHECADE:**CacheCADE - SSD CACHING**

This feature determines if SSD disk cache is supported or not by the controller. The options are **Disabled** and Enabled.

CacheCade 2.0 Capable

This feature determines whether or not the controller can write to the SSD cache. The options are **No** and Yes.

Configured Cache Size (GB)

Displays the total configured cache size.

Maximum Cache Size (GB)

Displays the maximum configurable cache size.

MEMORY:

Meomry Size (MB)

Displays the size of the controller's cache memory.

NVRAM (KB)

Displays the size of the NVRAM.

► Patrol Read

► Start

Starts patrol read for the seclected controller.

State

Displays the current state of the patrol read operation.

Iterations

Displays the number of patrol read iterations.

Mode

Displays the changes the patrol read mode for the controller. Patrol read scans and resolves potential problems on configured drives. The options are **Auto**, Manual, and Disable.

Rate

Displays the percentage of system resources dedicated to perform a Partol Read operation on configured drives.

Setting for Unconfigured Space

Displays the Patrol Read settings for the unconfigured space.

► Apply Changes

Submits the changes made to the entire form.

►Power Save Settings**►Apply Changes**

Submits the changes made to the entire form.

Spin Down Unconfigured Good

Use this feature to enable or disable spin down of unconfigured good drives. The options are **Enabled** and Disabled.

Spin Down Hot Spare Drives

Use this feature to enable or disable spin down of hot spare drives. The options are **Enabled** and Disabled.

Drive Standby Time

Use this feature to specify the drive's idle time. The options are **30 Mins**, 1 Hour, 1.50 Hour, 2 Hours, 3 Hours, 4 Hours, 5 Hours, 6 Hours, 7 Hours, 8 Hours, 9 Hours, 10 Hours, 11 Hours, 12 Hours, 13 Hours, 14 Hours, 15 Hours, 16 Hours, 17 Hours, 18 Hours, 19 Hours, 20 Hours, 21 Hours, 22 Hours, 23 Hours, and 24 Hours.

Spinup Drive Count

Use this feature to specify the maximum number of drives that can spin up at one time. The default is **2**.

Spinup Delay

Use this feature to control the interval (in seconds) between spin up of drives. The default is **12**.

►Apply Changes

Submits the changes made to the entire form.

►Spare**►Apply Changes**

Submits the changes made to the entire form.

Emergency Spare

Use this feature to indicate whether it is acceptable to commission incompatible global hot spare drives and unconfigured good drives as emergency hot spare drives. The options are None, **Unconfigured Good**, Global Hotspare, and Unconfigured Good and Global Hotspare.

Emergency for SMARTer

Use this feature to indicate whether it is acceptable to commission Emergency Hot Spare drives for PFA events. The options are Enabled and **Disabled**.

Persistent Hot Spare

Use this feature to enable or disable the ability to have the system backplane or storage enclosure drive slots dedicated as hot spare slots. The options are Enabled and **Disabled**.

Replace Drive

Use this feature to enable or disable the option to copy data back from a hot spare drive to a drive. The options are **Enabled** and Disabled.

Replace Hard Disk Drive on SMART Error

Use this feature to enable or disable the option to start a replace operation if a Self-monitoring Analysis and Report Technology (SMART) error is detected on a hard drive. The options are **Disabled** and Enabled.

Replace Solid State Drive on SMART Error

Use this feature to enable or disable the option to start a replace operation if a Self-monitoring Analysis and Report Technology (SMART) error is detected on a solid state drive. The options are **Disabled** and Enabled.

► Apply Changes

Submits the changes made to the entire form

► Task Rates

► Apply Changes

Submits the changes made to the entire form.

Background Initialization (BGI) Rate

This feature displays or changes the percentage of system resources dedicated to perform a background initialization on a redundant virtual drive. The default rate is **30**.

Consistency Check Rate

This feature displays or changes the percentage of system resources dedicated to perform a consistency check operation on a redundant virtual drive. The default rate is **30**.

Patrol Read Rate

This feature displays the percentage of system resources dedicated to perform a Patrol Read operation on configured drives. The default rate is **30**.

Rebuild Rate

This feature displays or changes the percentage of system resources dedicated to rebuild the data on a new drive after a storage configuration drive has failed. The default rate is **30**.

Reconstruction Rate

This feature displays or changes the percentage of system resources dedicated to perform a RAID level Migration (RLM) or Online Capacity Expansion (OCE) on a virtual drive. The default rate is **30**.

►Apply Changes

Submits the changes made to the entire form.

CONTROLLER PROPERTIES:**►Apply Changes**

Submits the changes made to the entire form.

Alarm Control

Use this feature to enable or disable the controller alarm. The options are Disabled and **Enabled**.

Auto Import Foreign Configuration

Use this feature to enable or disable the automatic import of foreign configurations without any user intervention. The options are **Disabled** and Enabled.

Coercion Mode

Coercion forces the drives of varying capacities to the same size so they can be used in a drive group. The coercion mode options are **None**, 128 MB, and 1 GB.

Boot Mode

Use this feature to specify the option to handle errors, if they occur, during boot time. The options are **Stop on errors**, Pause on errors, Ignore errors, and Safe mode on errors.

Controller BIOS

Use this feature to enable or disable the controller BIOS. The options are **Enabled** and Disabled.

ROC Controller (C)

This feature displays the temperature of the ROC.

Shield State Supported

This feature indicates whether shield state is supported in the controller or not.

Drive Security

This feature indicates the status of the drive security feature on the controller.

T10-PI

This feature indicates the status of the data protection feature on the controller.

Extended Virtual Drive Support

Use this feature to enable or disable the controller's max virtual drive limit. The options are **No** and Yes. Reboot the system for the change to take effect.

Maintain Drive Fail History

Use this feature to track the bad physical drives. The options are Disabled and **Enabled**.

Shield State Supported

This feature determines how frequently the controller polls for drives reporting a Predictive Drive Failure. The default is **300** seconds.

Stop Consistency Check on Error

Use this feature to enable or disable the option to stop the consistency check operation on a redundant virtual drive if there is an inconsistency found in the data. The options are **Disabled** and Enabled.

JBOD Mode

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

Write Verify

Use this feature to enable or disable the write verify during cache flush. The options are **Disabled** and Enabled.

Large IO Support

Use this feature to enable or disable large IO support. Reboot the system for changes to take effect. The options are **Disabled** and Enabled.

►Apply Changes

Submits the changes made to the entire form.

►Virtual Drive Management

Use this submenu to view the basic virtual drive properties and perform operations such as background initialization and consistency check.

►Drive Management

►Drive Port 0/Drive Port 0 - (Displays the detected drive)

Displays the name of the controller.

Operation

Lists the operations that can be performed on a drive. The options are **Select operation**, Start Locate, Stop Locate, Initialize Drive, Drive Erase, Make Unconfigured Bad, Assign Global Hot Spare Drive, and Prepare For Removal.

BASIC PROPERTIES:

Drive ID

Displays the ID of the drive.

Status

Displays the status of the drive.

Size

Displays the size of the drive.

Type

Displays the type of the drive.

Model

Displays the model number of the drive.

Hardware Vendor

Displays the manufacturer of the drive.

► **Advanced...**

Certified

This feature indicates where the selected drive is vendor certified.

Logical Sector Size

Displays the logical vector size of this drive. The options are 4 KB or 512 B.

Physical Sector Size

Displays the physical vector size of this drive. The options are 4 KB or 512 B.

SMART Status

Displays the SMART status of the drive.

Revision

Displays the firmware revision of the drive.

Media Errors

Displays the physical errors that have been detected on the disk media.

Predicted Fail Count

Displays the errors that have been detected on the disk media.

SAS Address

Displays the World Wide Name (WWN) of the drive.

Drive Power State

Displays the power condition of the drive.

Cache Setting

Displays the disk cache setting of the drive.

Available Size

Displays the available size of the drive.

Used Space

Displays the configured space of the drive.

Disk Protocol

Displays the type of hard disk drive used.

Device Speed

Displays the speed of the drive.

Negotiated Link Speed

Displays the negotiated link speed of the drive.

Number of Connections

Displays the number of connections of the drive.

FDE Capable

Indicates whether the drive is encryption capable or not.

Protection Capable

Indicates whether the drive is capable of protection or not.

Temperature (C)

Displays the temperature of the drive.

► Hardware Components**Temperature Sensors**

Displays the status of temperature sensors present in an enclosure.

Fans

Displays the status of fans present in an enclosure.

Power Supplies

Displays the status of power supplies present in an enclosure.

► Enclosure Management**Select Enclosure**

Displays all attached enclosures.

Vendor ID

Displays the vendor ID of the enclosure.

Enclosure ID

Displays the ID of the enclosure.

Enclosure Model

Displays the model of the enclosure.

Enclosure Location

Displays the location of the enclosure.

Attached Drives

Displays the list of drives attached to the selected enclosure.

► Help

Contains help instructions to create virtual drives.

PROPERTIES:

Status

Displays the status of the controller.

Current Personality

Displays the current personality.

Backplane

Displays the number of backplanes connected to the controller.

BBU

Indicates if the battery backup unit is present or not.

Enclosure

Displays the number of enclosures connected to the controller.

Drives

Displays the number of drives connected to the controller.

Drive Groups

Displays the number of drive groups on the controller.

Virtual Drives

Displays the number of virtual drives on the controller.

► View Server Profile

SERVER

UEFI Spec Version

Displays the version of the UEFI Spec this system supports.

CONTROLLER COMPONENTS

► Controller Management

BASIC PROPERTIES:

Product Name

Displays the marketing name of the controller.

Serial Number

Displays the serial number of the controller.

Controller Status

Displays the status of the controller.

Select Boot Device

Use this feature to select the primary boot device.

PCI ID

Displays the manufacturer-assigned ID.

PCI Slot Number

Displays the PCI Slot ID number that contains the controller.

Package Version

Displays the package version of the controller package.

Firmware Version

Displays the firmware version of the controller.

NVDATA Version

Displays the version of the NVDATA.

Connector Count

Displays the number of host data ports and connectors present on the controller.

Drive Count

Displays the number of drives attached to the controller.

Virtual Drive Count

Displays the number of virtual drives present on the controller.

► Advanced Controller Management

► Clear Controller Events

Deletes all of the existing controller events.

► Save Controller Events

Select File System

Use this feature to choose the appropriate file system to save the controller logs.

Select Directory

Use this feature to choose the appropriate directory to save the controller logs. The options are **Current Dir** and **EFI**.

Enter Filename

Assign a filename to identify the event log.

► Save Events

Saves the log to the specified file system and directory.

► Save TTY Log

Select File System

Use this feature to choose the appropriate file system to save the controller logs.

Select Directory

Use this feature to choose the appropriate directory to save the controller logs. The options are **Current Dir** and **EFI**.

Enter Filename

Assign a filename to identify the event log.

Entries to Save

Displays the number of entries to be saved. The options are 2 KB, 4 KB, 8 KB, 16 KB, and **All**.

► Save Log

Saves the log to the specified file system and directory.

► Manage Link Speed**Phy #0 (0x50000C500C9EAF29D)****Phy #1 (0x50000C500C9EAF0C1)****Phy #3 - Phy #7 (0x0000000000000000)**

Use this feature to select a speed for the specified port. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

► OK

Commit to the changes.

► Cancel

Cancel the changes.

► Manage MegaRAID Advanced Software Options**Safe ID**

The SAFE ID is a 40 alpha-numeric character value generated by the controller.

Serial Number

The SAFE ID is a 10 alpha-numeric character value generated by the controller.

Activation Key

Use this feature to enter a 40 alpha-numeric character value.

► Activate

Displays a summary and allows you to activate the advanced software options.

► Schedule Consistency Check**Consistency Check Frequency**

Use this feature to select the frequency of the consistency check runs. The options are Disable, Hourly, Daily, **Weekly**, and Monthly.

Consistency Check Start Date

Use this feature to assign the start date for the consistency check operation.

Consistency Check Start Time

Use this feature to assign the start time for the consistency check operation.

Consistency Check Start Date

Use this feature to select the consistency check mode. The options are **Concurrent** and Sequential.

SELECT VIRTUAL DRIVES TO CHECK:

Consistency Check Start Date

Use this feature to assign the start date for the consistency check operation.

► Apply Changes

Submits the changes made to the entire form.

► Set Factory Defaults

Restores factory default values for all the controller properties.

► Switch to JBOD mode

Use this feature to select JBOD or RAID mode.

► Advanced Controller Properties

► Cache And Memory

Cache:

Cache Flush Interval

This feature displays and allows you to modify the interval (in seconds) the contents of the onboard data cache are flushed. The default value is **4**.

Preserved Cache

This feature displays if the controller cache is preserved because of missing or offline virtual drives. The options are **Concurrent** and Sequential.

CACHECADE:

CacheCADE - SSD CACHING

This feature determines if SSD disk cache is supported or not by the controller. The options are **Disabled** and Enabled.

CacheCade 2.0 Capable

This feature determines whether or not the controller can write to the SSD cache. The options are **No** and Yes.

Configured Cache Size (GB)

Displays the total configured cache size.

Maximum Cache Size (GB)

Displays the maximum configurable cache size.

MEMORY:**Meomry Size (MB)**

Displays the size of the controller's cache memory.

NVRAM (KB)

Displays the size of the NVRAM.

► Patrol Read**► Start**

Starts patrol read for the selected controller.

State

Displays the current state of the patrol read operation.

Iterations

Displays the number of patrol read iterations.

Mode

Displays the changes the patrol read mode for the controller. Patrol read scans and resolves potential problems on configured drives. The options are **Auto**, Manual, and Disable.

Rate

Displays the percentage of system resources dedicated to perform a Partol Read operation on configured drives.

Setting for Unconfigured Space

Displays the Patrol Read settings for the unconfigured space.

► Apply Changes

Submits the changes made to the entire form.

► Power Save Settings**► Apply Changes**

Submits the changes made to the entire form.

Spin Down Unconfigured Good

Use this feature to enable or disable spin down of unconfigured good drives. The options are **Enabled** and Disabled.

Spin Down Hot Spare Drives

Use this feature to enable or disable spin down of hot spare drives. The options are **Enabled** and Disabled.

Drive Standby Time

Use this feature to specify the drive's idle time. The options are **30 Mins**, 1 Hour, 1.50 Hour, 2 Hours, 3 Hours, 4 Hours, 5 Hours, 6 Hours, 7 Hours, 8 Hours, 9 Hours, 10 Hours, 11 Hours, 12 Hours, 13 Hours, 14 Hours, 15 Hours, 16 Hours, 17 Hours, 18 Hours, 19 Hours, 20 Hours, 21 Hours, 22 Hours, 23 Hours, and 24 Hours.

Spinup Drive Count

Use this feature to specify the maximum number of drives that can spin up at one time. The default is **2**.

Spinup Delay

Use this feature to control the interval (in seconds) between spin up of drives. The default is **12**.

► Apply Changes

Submits the changes made to the entire form.

► Spare

► Apply Changes

Submits the changes made to the entire form.

Emergency Spare

Use this feature to indicate whether it is acceptable to commission incompatible global hot spare drives and unconfigured good drives as emergency hot spare drives. The options are None, **Unconfigured Good**, Global Hotspare, and Unconfigured Good and Global Hotspare.

Emergency for SMARTer

Use this feature to indicate whether it is acceptable to commission Emergency Hot Spare drives for PFA events. The options are Enabled and **Disabled**.

Persistent Hot Spare

Use this feature to enable or disable the ability to have the system backplane or storage enclosure drive slots dedicated as hot spare slots. The options are Enabled and **Disabled**.

Replace Drive

Use this feature to enable or disable the option to copy data back from a hot spare drive to a drive. The options are **Enabled** and Disabled.

Replace Hard Disk Drive on SMART Error

Use this feature to enable or disable the option to start a replace operation if a Self-monitoring Analysis and Report Technology (SMART) error is detected on a hard drive. The options are **Disabled** and Enabled.

Replace Solid State Drive on SMART Error

Use this feature to enable or disable the option to start a replace operation if a Self-monitoring Analysis and Report Technology (SMART) error is detected on a solid state drive. The options are **Disabled** and Enabled.

► Apply Changes

Submits the changes made to the entire form

► Task Rates**► Apply Changes**

Submits the changes made to the entire form.

Background Initialization (BGI) Rate

This feature displays or changes the percentage of system resources dedicated to perform a background initialization on a redundant virtual drive. The default rate is **30**.

Consistency Check Rate

This feature displays or changes the percentage of system resources dedicated to perform a consistency check operation on a redundant virtual drive. The default rate is **30**.

Patrol Read Rate

This feature displays the percentage of system resources dedicated to perform a Patrol Read operation on configured drives. The default rate is **30**.

Rebuild Rate

This feature displays or changes the percentage of system resources dedicated to rebuild the data on a new drive after a storage configuration drive has failed. The default rate is **30**.

Reconstruction Rate

This feature displays or changes the percentage of system resources dedicated to perform a RAID level Migration (RLM) or Online Capacity Expansion (OCE) on a virtual drive. The default rate is **30**.

►Apply Changes

Submits the changes made to the entire form.

CONTROLLER PROPERTIES:

►Apply Changes

Submits the changes made to the entire form.

Alarm Control

Use this feature to enable or disable the controller alarm. The options are Disabled and **Enabled**.

Auto Import Foreign Configuration

Use this feature to enable or disable the automatic import of foreign configurations without any user intervention. The options are **Disabled** and Enabled.

Coercion Mode

Coercion forces the drives of varying capacities to the same size so they can be used in a drive group. The coercion mode options are **None**, 128 MB, and 1 GB.

Boot Mode

Use this feature to specify the option to handle errors, if they occur, during boot time. The options are **Stop on errors**, Pause on errors, Ignore errors, and Safe mode on errors.

Controller BIOS

Use this feature to enable or disable the controller BIOS. The options are **Enabled** and Disabled.

ROC Controller (C)

This feature displays the temperature of the ROC.

Shield State Supported

This feature indicates whether shield state is supported in the controller or not.

Drive Security

This feature indicates the status of the drive security feature on the controller.

T10-PI

This feature indicates the status of the data protection feature on the controller.

Extended Virtual Drive Support

Use this feature to enable or disable the controller's max virtual drive limit. The options are **No** and Yes. Reboot the system for the change to take effect.

Maintain Drive Fail History

Use this feature to track the bad physical drives. The options are Disabled and **Enabled**.

Shield State Supported

This feature determines how frequently the controller polls for drives reporting a Predictive Drive Failure. The default is **300** seconds.

Stop Consistency Check on Error

Use this feature to enable or disable the option to stop the consistency check operation on a redundant virtual drive if there is an inconsistency found in the data. The options are **Disabled** and Enabled.

JBOD Mode

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

Write Verify

Use this feature to enable or disable the write verify during cache flush. The options are **Disabled** and Enabled.

Large IO Support

Use this feature to enable or disable large IO support. Reboot the system for changes to take effect. The options are **Disabled** and Enabled.

►Apply Changes

Submits the changes made to the entire form.

► Hardware Components

Temperature Sensors

Displays the status of temperature sensors present in an enclosure.

Fans

Displays the status of fans present in an enclosure.

Power Supplies

Displays the status of power supplies present in an enclosure.

► Enclosure Management

Select Enclosure

Displays all attached enclosures.

Vendor ID

Displays the vendor ID of the enclosure.

Enclosure ID

Displays the ID of the enclosure.

Enclosure Model

Displays the model of the enclosure.

Enclosure Location

Displays the location of the enclosure.

Attached Drives

Displays the list of drives attached to the selected enclosure.

► Drive Management

► Drive Port 0 - (Displays the detected drive)

Displays the name of the controller.

Operation

Lists the operations that can be performed on a drive. The options are **Select operation**, Start Locate, Stop Locate, Initialize Drive, Drive Erase, Make Unconfigured Bad, Assign Global Hot Spare Drive, and Prepare For Removal.

BASIC PROPERTIES:**Drive ID**

Displays the ID of the drive.

Status

Displays the status of the drive.

Size

Displays the size of the drive.

Type

Displays the type of the drive.

Model

Displays the model number of the drive.

Hardware Vendor

Displays the manufacturer of the drive.

►Advanced...**Certified**

This feature indicates where the selected drive is vendor certified.

Logical Sector Size

Displays the logical vector size of this drive. The options are 4 KB or 512 B.

Physical Sector Size

Displays the physical vector size of this drive. The options are 4 KB or 512 B.

SMART Status

Displays the SMART status of the drive.

Revision

Displays the firmware revision of the drive.

Media Errors

Displays the physical errors that have been detected on the disk media.

Predicted Fail Count

Displays the errors that have been detected on the disk media.

SAS Address

Displays the World Wide Name (WWN) of the drive.

Drive Power State

Displays the power condition of the drive.

Cache Setting

Displays the disk cache setting of the drive.

Available Size

Displays the available size of the drive.

Used Space

Displays the configured space of the drive.

Disk Protocol

Displays the type of hard disk drive used.

Device Speed

Displays the speed of the drive.

Negotiated Link Speed

Displays the negotiated link speed of the drive.

Number of Connections

Displays the number of connections of the drive.

FDE Capable

Indicates whether the drive is encryption capable or not.

Protection Capable

Indicates whether the drive is capable of protection or not.

Temperature (C)

Displays the temperature of the drive.

► **Virtual Drive Management**

Use this submenu to view the basic virtual drive properties and perform operations such as background initialization and consistency check.

ACTIONS

► Configure

► Create Virtual Drive

Select RAID Level

Use this feature to select the RAID level. The options are **RAID0**, RAID1, RAID00.

Select Drives From

Use this feature to select the physical drive option. The options are **Unconfigured Capacity** and Free Capacity.

► Select Drives

► Apply Changes

Apply the changes made regarding the drive selection.

Select Media Type

Use this feature to select the media type. The options are SSD, HDD, and **Both**.

Select Interface From

Use this feature to select the technology of the drive. The options are SAS, SATA, and **Both**.

Select Drives From

Use this feature to select the physical drive option. The options are **Unconfigured Capacity** and Free Capacity.

Local Sector Size

Use this feature to select the sector size of the drive. The options are 512 B, 4 KB, and **Both**.

CHOOSE UNCONFIGURED DDIVES:

Drive Port 0 (Drive information may vary depending on detection)

Use this feature to select the physical drive option. The options are Disabled and **Enabled**.

Check All

Check all drives.

Uncheck All

Uncheck all drives.

► Apply Changes

Apply the changes made regarding the drive selection.

CONFIGURE VIRTUAL DRIVE PARAMETERS:

Virtual Drive Name

Assign a name for the virtual drive.

Virtual Drive Size

Assign the amount of the storage space for the virtual drive.

Strip Size

Use this feature to select the strip element size for the virtual drive. The options are 64 KB, 128 KB, **256 KB**, 512 KB, 1 MB.

Read Policy

Use this feature to select the read cache policy for the virtual drive. The options are No Read Ahead and **Read Ahead**.

Write Policy

Use this feature to select the write cache policy for the virtual drive. The options are Write Through, **Write Back**, and Always Write Back.

I/O Policy

Use this feature to select the I/O policy for the virtual drive. The options are Direct and **Cached**.

Access Policy

Use this feature to select the access policy for the virtual drive. The options are **Read/Write**, Read Only, and Blocked.

Drive Cache

Use this feature to select the virtual drive cache setting. The options are **Unchanged**, Enable, and Disabled.

Disable Background Initialization

Use this feature to enable or disable the background initialization status. Select no to leave it enabled. The options are **No** and Yes.

Default Initialization

Select No to disable the initialization of the virtual drive, Fast to initialize the first 100MB of the virtual drive, and Full to initialize the entire drive. The options are **No**, Fast, and Full.

Emulation Type

Use this feature to select the emulation type. The options are **Default**, Disable, and Force.

► Create Profile Based Virtual Drive**► Generic RAID 0****► Generic RAID 1****Drive Selection Criteria**

The information displayed here is dependent on what the system detects.

PROFILE PARAMETERS:**Virtual Drive Name**

Displays the amount of the virtual drive storage space.

Power Save Mode

Displays the power save mode. The setting is Controller Defined.

Strip Size

Displays the strip element size of the virtual drive.

Read Policy

Displays the read policy of the virtual drive.

Write Policy

Displays the write cache policy of the virtual drive.

I/O Policy

Displays the Input and Output policy of the virtual drive.

Drive Cache

Use this feature to select the virtual drive cache setting. The options are Unchanged, **Enable**, and Disable.

Default Initialization

Displays the virtual drive initialization setting.

► Save Configuration

Save the configuration that the wizard created. The options are Yes and **No**.

► Clear Configuration

Use this feature to delete all existing configurations on the RAID controller.

► Set Factory Defaults

Restores factory default values for all the controller properties.

► Update Firmware

Use this feature to update to a new firmware version.

Silence Alarm

Use this feature to silence the controller alarm.

BACKGROUND OPERATIONS

Virtual Drive Operations in Progress

Displays the operation of a virtual drive that is in progress.

Drive Operations in Progress

Displays the drive operation that is in progress.

MegaRAID ADVANCED SOFTWARE OPTIONS

MegaRAID RAID6

Displays the status of RAID6.

MegaRAID RAID5

Displays the status of RAID5.

MegaRAID FastPath

Displays the status of FastPath.

► Manage MegaRAID Advanced Software Options

SAFE ID

Displays the 40 alpha-numeric character value generated by the controller.

Serial Number

Displays the 10 alpha-numeric character value generated by the controller.

Activation Key

Use this feature to enter a 40 alpha-numeric character value

► Activate

Displays a summary of the advanced software options that can be activated.

► VLAN Configuration (MAC:3CECEF71D356)**► Enter Configuration Menu****Create New VLAN****VLAN ID**

Enter a value between 0 and 4094 for the VLAN ID.

Priority

Enter a Priority value between 0 and 7.

Add VLAN

Use this feature to create a new VLAN or update an existing one.

Configured VLAN List**Remove VLAN**

Use this feature to remove the selected VLANs.

► MAC:3CECEF71D356-IPv6 Network Configuration**► Enter Configuration Menu****Interface Name****Interface Type****MAC Address****Host Address****Route Table****Gateway addresses**

DNS addresses

Interface ID

Displays the 64-bit interface ID for the device.

DAD Transmit Count

Displays the number of consecutive Neighbor Solicitation messages sent while performing the Duplicate Address Detection on a tentative address. The value 0 means the DAD is not performed.

Policy

Use this feature to set to automatic or manual mode.

Save Changes and Exit.

Save changes for interface ID, DAD, and policy settings and then exit.

► MAC:3CECEF6C751C-IPv4 Network Configuration

Configured

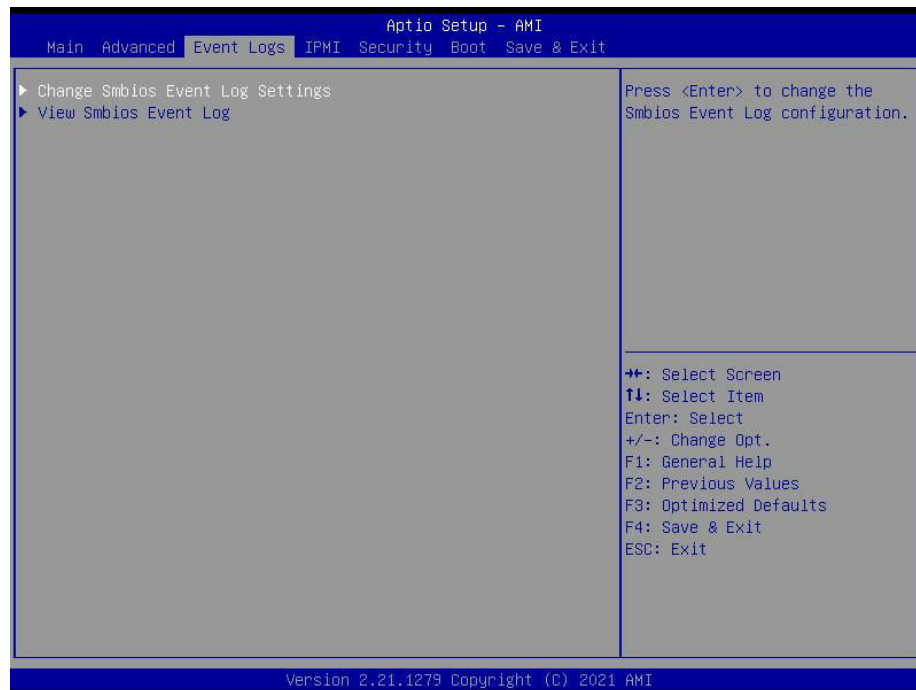
Use this feature to indicate whether the network address is configured successfully or not. The options are **Disabled** and Enabled.

Save Changes and Exit.

Save changes and exit.

4.4 Event Logs

Use this menu to configure Event Log settings.



► Change Smbios Event Log Settings

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase Event Log

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

When Log is Full

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

SMBIOS Event Long Standard Settings

Log System Boot Event

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

MECI

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

METW

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



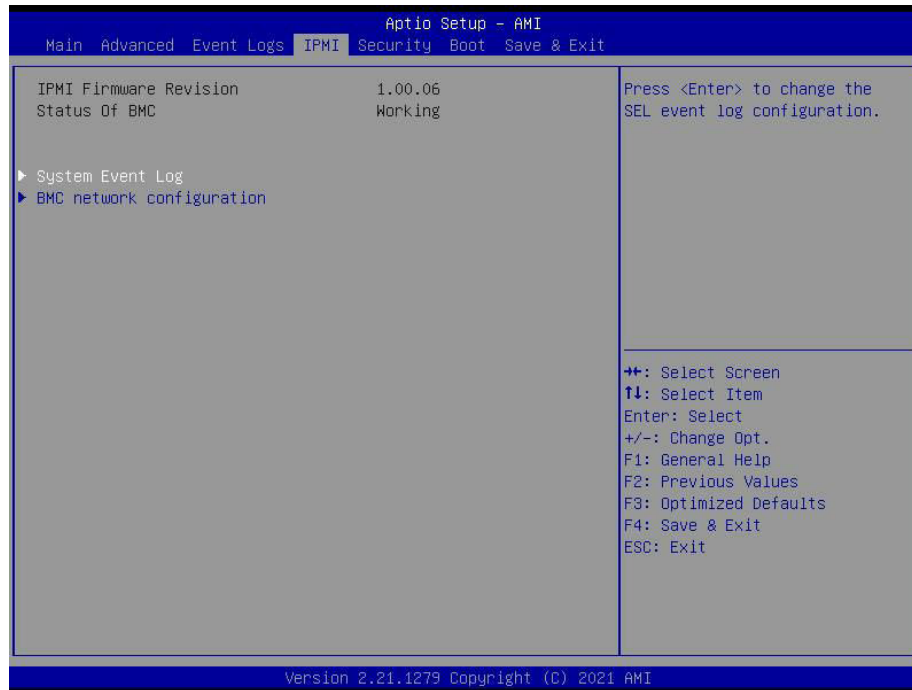
Note: After making changes to a setting, reboot the system for the changes to take effect.

►View Smbios Event Log

This section displays the contents of the SMBIOS Event Log.

4.5 IPMI

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



IPMI Firmware Revision

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

Status of BMC

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

► System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

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



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

► BMC Network Configuration

BMC Network Configuration

Update IPMI LAN Configuration

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

****If the feature above is set to Yes, Configuration Address Source, VLAN, and IPv6 Support are available for configuration:***

Configure IPv4 Support

IPMI LAN Selection

IPMI Network Link Status

Configuration Address Source

This feature allows you to select the source of the IP address for this computer. If Static is selected, you 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 searches for a Dynamic Host Configuration Protocol (DHCP) server in the network that is attached to and request the next available IP address for this computer. The options are **DHCP** and Static.

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

Station IP Address

This feature displays the Station IP address for this computer. The address can be manually entered. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).

Subnet Mask

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

Station MAC Address**Gateway IP Address**

This feature displays the Gateway IP address for this computer. The address can be manually entered. This should be in decimal and in dotted quad form (i.e., 172.31.0.1).

VLAN

This feature displays the virtual LAN settings. The options are **Disabled** and Enabled.

VLAN ID

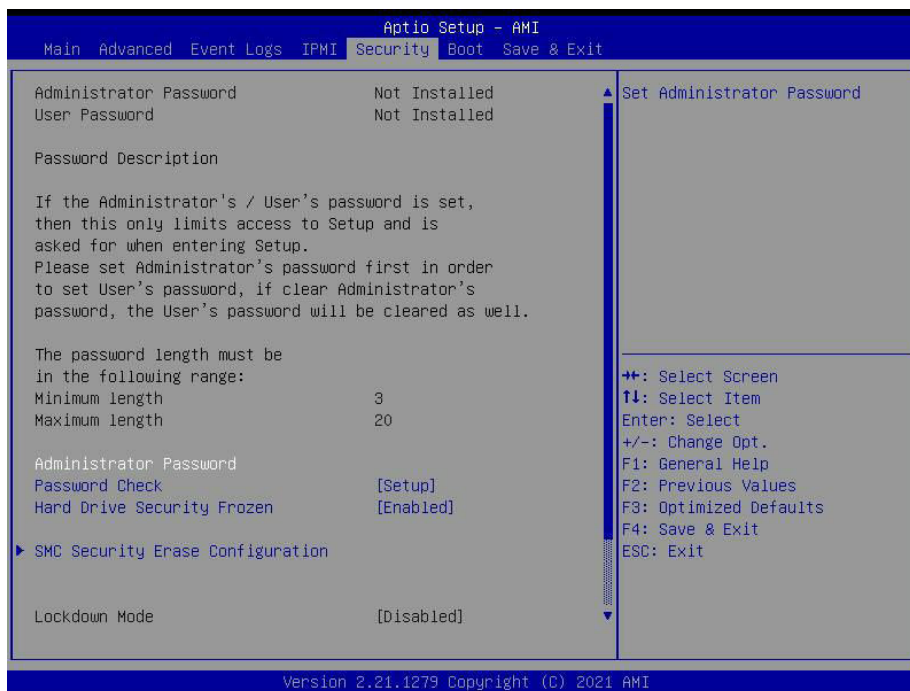
This feature is enabled if VLAN is enabled.

Configure IPv6 Support**IPv6 Address Status****IPv6 Support**

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

4.6 Security

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



Administrator Password

Press Enter to create a new, or change an existing, Administrator password.

Password Check

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

Hard Drive Security Frozen

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

▶ Secure Boot

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

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

Use this feature to enable secure boot. The options are **Disabled** and Enabled.

Secure Boot Mode

Use this feature to configure Secure Boot variables without authentication. The options are Standard and **Custom**.

CSM Support

This feature is for manufacturing debugging purposes.

Enter Audit Mode

This submenu can only be used if current System Mode is set to User (refer to Exit Deployed Mode). The PK variable will be erased on transition to Audit Mode.

▶ Key Management

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

Factory Key Provision

Use this feature to install secure boot keys after the platform reset and while the system is in setup mode. The options are **Disabled** and Enabled.

▶ Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot key databases.

▶ Reset to Setup Mode

This feature deletes all Secure Boot key databases from NVRAM.

▶ Export Secure Boot variables

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

▶ Enroll EFI Image

This feature allows the image to run in Secure Boot Mode. Enroll SHA256 Hash Certificate of the image into the Authorized Signature Database.

Device Guard Ready

► Remove 'UEFI CA' from DB

This feature allows you to decide if all secure boot variables should be saved.

► Restore DB defaults

Select Yes to restore the DB defaults.

Secure Boot Variable

► Platform Key (PK)

Update

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

► Key Exchange Key

Update

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

Append

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

► Authorized Signatures

Update

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

Append

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

►Forbidden Signatures

Update

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

Append

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

►Authorized TimeStamps

Update

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

Append

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

►OsRecovery Signature

Update

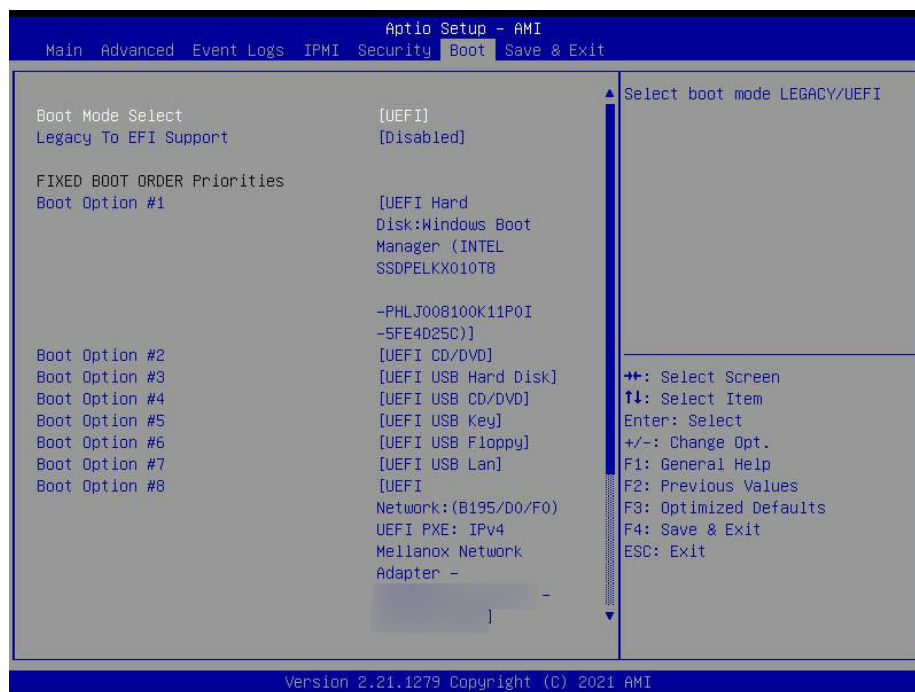
Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file.

Append

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

4.7 Boot

Use this submenu to configure Boot Settings:



Boot Mode Select

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

FIXED BOOT ORDER Priorities

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

****If the feature above is set to Legacy, UEFI/Dual, the following features are displayed:***

- Legacy/UEFI/Dual/Boot Option #1
- Legacy/UEFI/Dual/Boot Option #2
- Legacy/UEFI/Dual/Boot Option #3
- Legacy/UEFI/Dual/Boot Option #4
- Legacy/UEFI/Dual/Boot Option #5
- Legacy/UEFI/Dual/Boot Option #6
- Legacy/UEFI/Dual/Boot Option #7

- Legacy/UEFI/Dual/Boot Option #8
- Legacy/UEFI/Dual/Boot Option #9

►Add New Boot Option

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

Add boot option label

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

Path for boot option

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

Boot option File Path

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

Save

Use this feature to save the newly formed boot option.

►Delete Boot Option

Use this feature to remove a pre-defined boot device from which the system will boot during startup.

The settings are [any pre-defined boot device].

►UEFI Hard Disk Drive BBS Priorities

- Boot Order #1 - This feature sets the system boot order of detected devices. The options are **[the list of detected boot device(s)]** and Disabled.

►UEFI Network Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

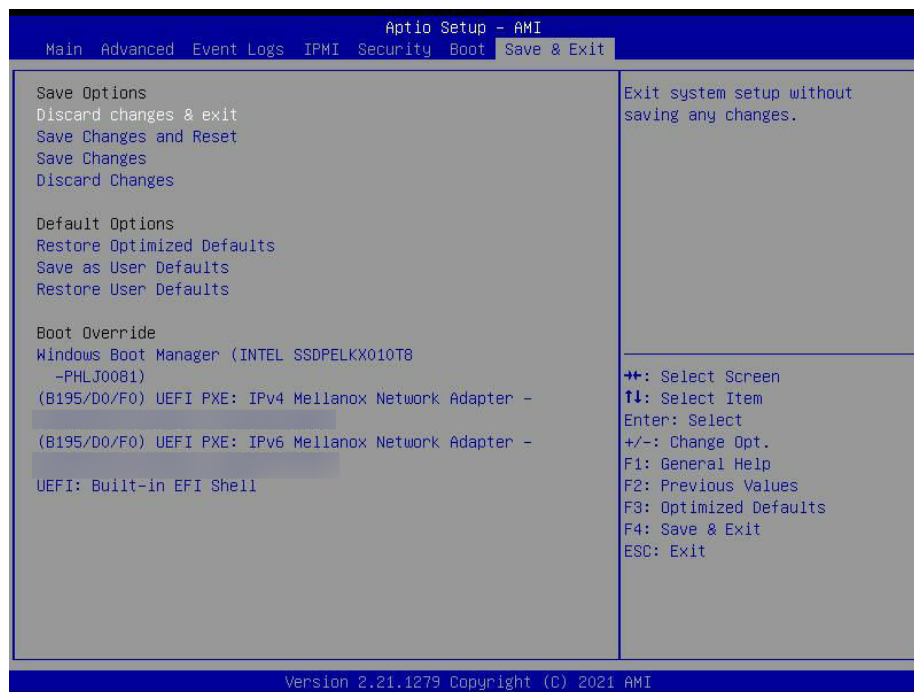
►UEFI Application Boot Priorities

This feature allows you to specify which UEFI devices are boot devices.

- UEFI Boot Order #1

4.8 Save & Exit

Select the Save & Exit tab from the BIOS setup utility screen to enter the Exit BIOS Setup screen.



Discard Changes and Exit

Select this option to quit the BIOS Setup without making any permanent changes to the system configuration, and reboot the computer. Select Discard Changes and Exit from the Exit menu and press <Enter>.

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, so the new system configuration parameters can take effect. Select Save Changes and Exit from the Exit menu and press <Enter>.

Save Changes

After completing the system configuration changes, select this option to save the changes you have made. This does not reset (reboot) the system.

Discard Changes

Select this option and press <Enter> to discard all the changes and return to the AMI BIOS utility Program.

Default Options

Restore Optimized Defaults

To set this feature, select Restore Optimized Defaults from the Save & Exit menu and press <Enter>. These are factory settings designed for maximum system stability, but not for maximum performance.

Save as User Defaults

To set this feature, select Save as User Defaults from the Exit menu and press <Enter>. This enables the user to save any changes to the BIOS setup for future use.

Restore User Defaults

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

Boot Override

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

Windows Boot Manager

UEFI: Built-in EFI Shell

**(B195/D0/F0) UEFI PXE: IPv4 Mellanox Network Adapter - 3C:EC:EF:71:D3:56
3CECEF71D356**

**(B195/D0/F0) UEFI PXE: IPv6 Mellanox Network Adapter - 3C:EC:EF:71:D3:56
3CECEF71D356**

Launch EFI Shell from filesystem device

Appendix A

BIOS Codes

A.1 BIOS Error POST (Beep) Codes

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

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

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

These fatal errors are usually communicated through a series of audible beeps. The table shown below lists some common errors and their corresponding beep codes encountered by users.

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

A.2 Additional BIOS POST Codes

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

When BIOS performs the Power On Self Test, it writes checkpoint codes to I/O port 0080h. If the computer cannot complete the boot process, a diagnostic card can be attached to the computer to read I/O port 0080h (Supernmicro p/n AOC-LPC80-20).

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

Appendix B

Software

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

B.1 Microsoft Windows OS Installation

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

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That might be a DVD, perhaps using an external USB/SATA DVD drive, or a USB flash 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.

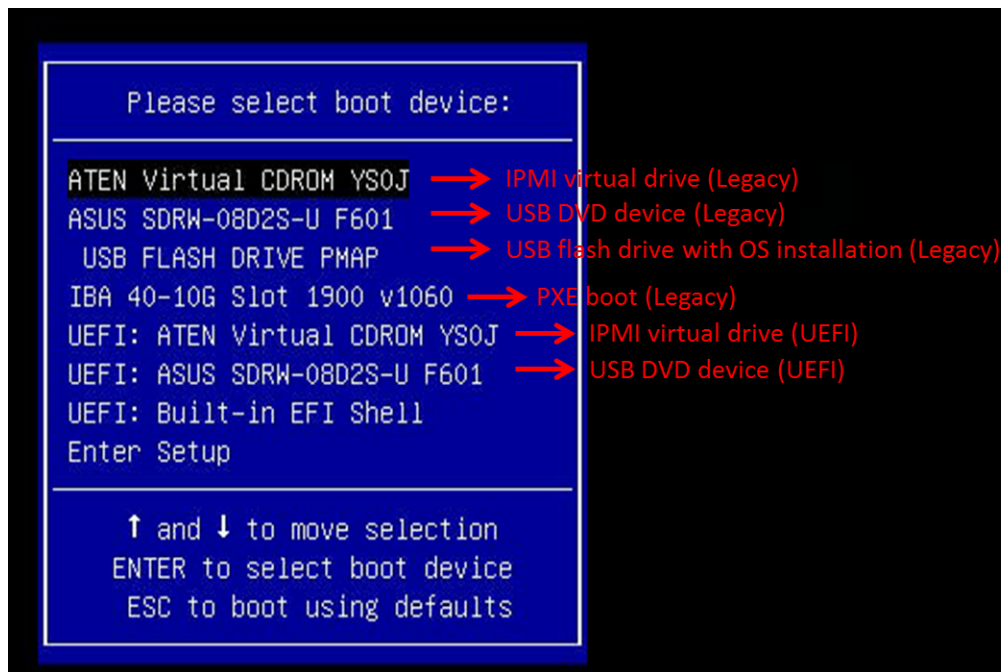


Figure B-1. Select Boot Device

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.

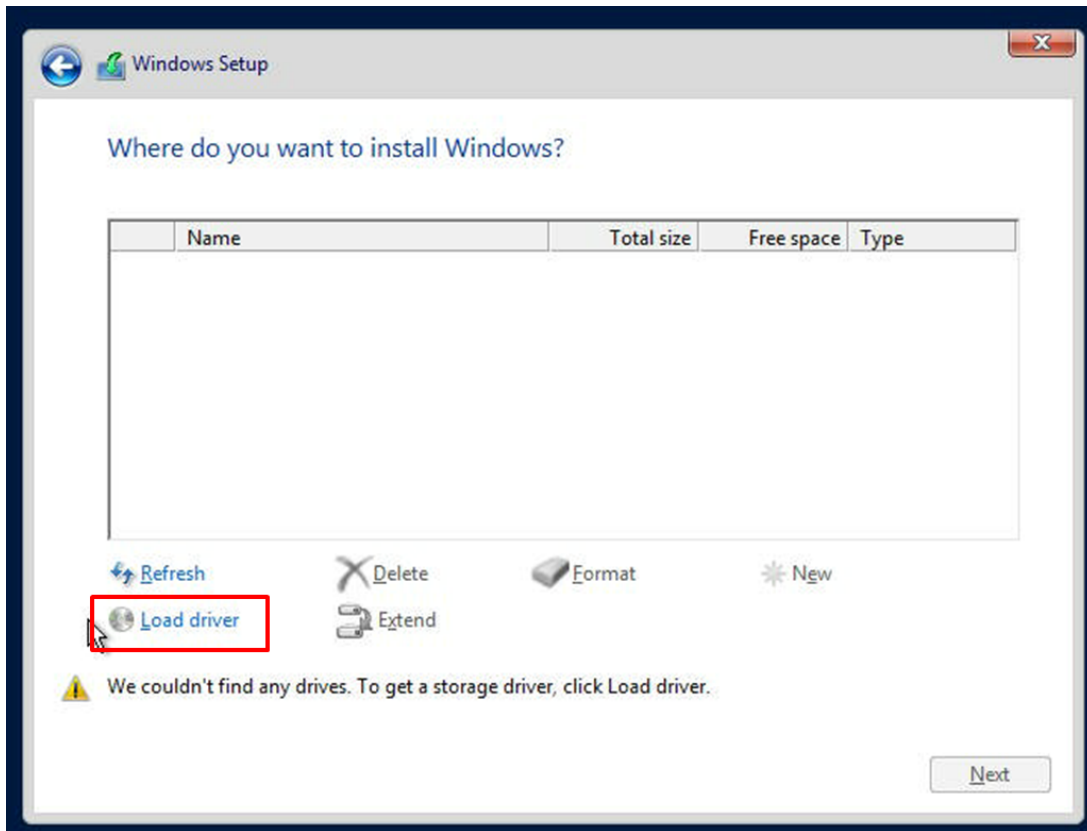


Figure B-2. Load Driver Link

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.

B.2 Driver Installation

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

After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash drive or a DVD. 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.

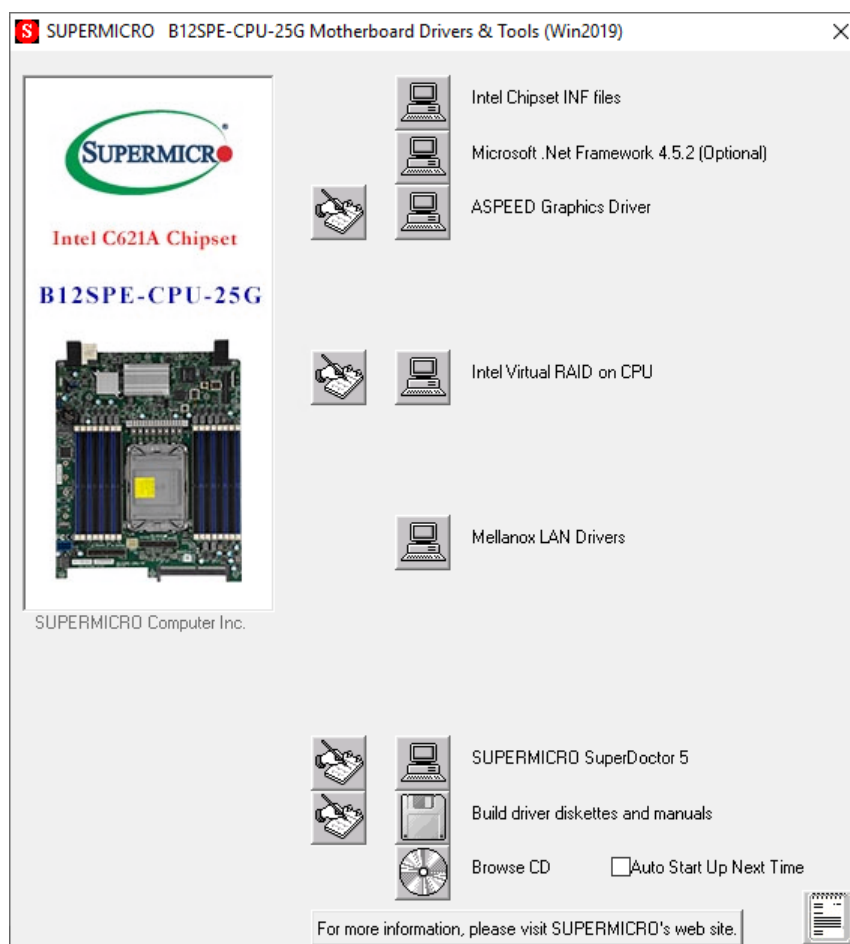


Figure B-3. Driver & Tool Installation Screen

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.

B.3 SuperDoctor® 5

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

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



Note: The default User Name and Password for SuperDoctor 5 is ADMIN / ADMIN.

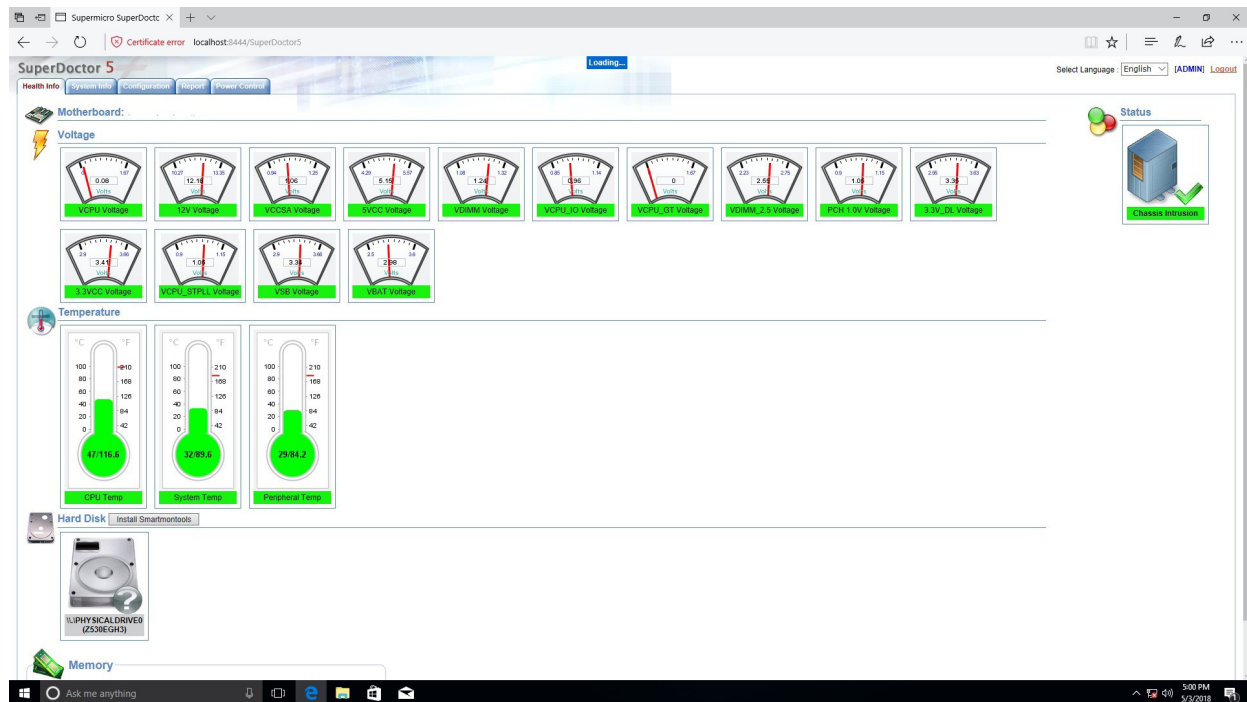


Figure B-4. SuperDoctor 5 Interface Display Screen (Health Information)

B.4 IPMI

The B12SPE-CPU-25G 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 <http://www.supermicro.com/products/nfo/IPMI.cfm>.

Appendix C

Standardized Warning Statements

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

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

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。請按制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 لعمليات 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 D

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.

D.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.

D.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 Power-On Self-Test (POST) 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.

D.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 Drive, or a USB CD/DVD ROM/RW device 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 device or a writable CD/DVD.

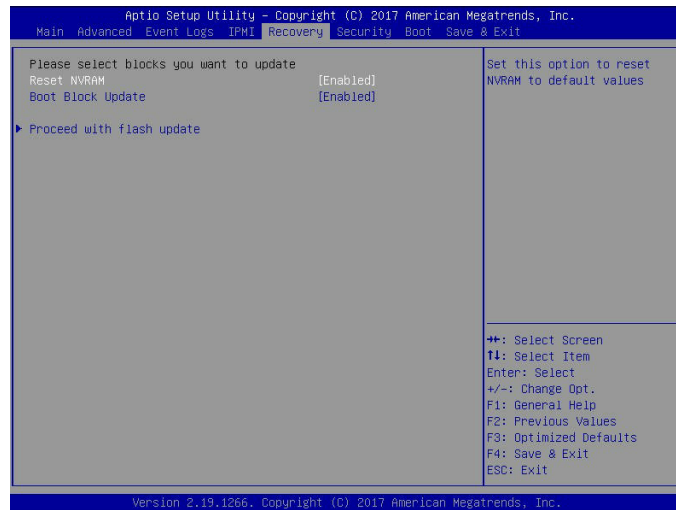
 **Note 1:** If you cannot locate the "Super.ROM" file in your driver disk, visit our website at www.supermicro.com to download the BIOS package. Extract the BIOS binary image into a USB flash device and rename it "Super.ROM" for the BIOS recovery use.

 **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:



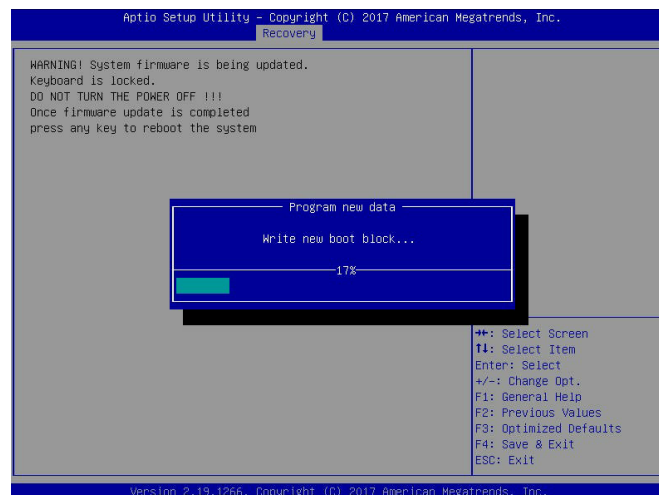
3. After locating the new BIOS binary image, the system will enter the BIOS Recovery menu as shown below:



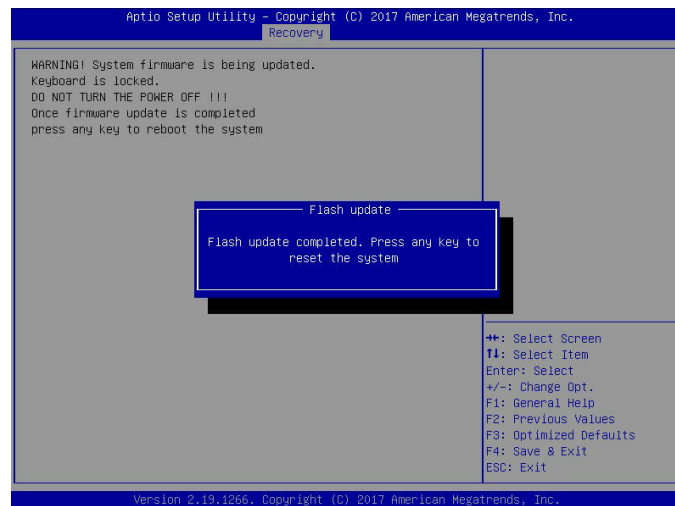
Note: At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

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:

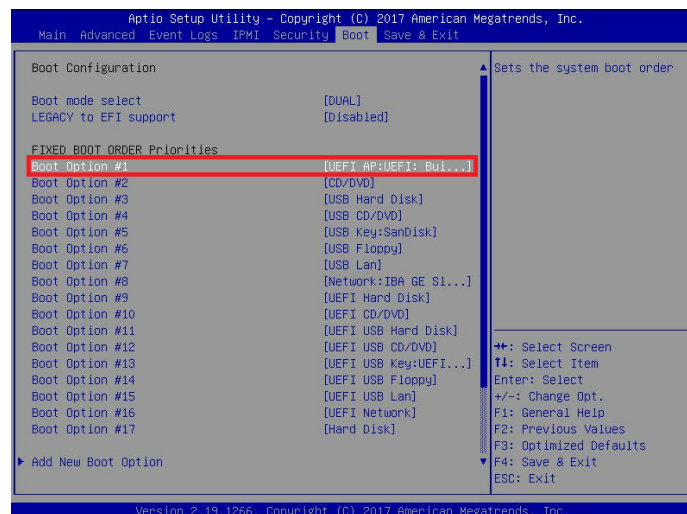
Note: Do not interrupt the BIOS flashing process until it has completed.



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
CR3992)
  BLK0: Alias(s):
    PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)
Press F8C in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> cd AFUDOS
FS0:\AFUDOS> cd SNJPME2_03162017
FS0:\AFUDOS\SNJPME2_03162017> flash.nsh X10PU7.314

```



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...
*****
| AMT Firmware Update Utility v5.09.01.1317 |
| 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 NCB Block ..... done
- Update success for FBR
- Update success for IE
- Successful Update Recovery Loader to OPRx!!
- Successful Update MFSB!!
- Successful Update FPPRI!!
- Successful Update MFS, IVB1 and IVB2!!
- Successful Update FLOG and UTOK!!
- ME Entire Image update success !!
WARNING: System must power-off to have the changes take effect!
Moving FS0:\AFUDOS\SNJPME2_03162017\dtx64.efi -> FS0:\AFUDOS\SNJPME2_03162017\
dt.smc
- [ok]
Moving FS0:\AFUDOS\SNJPME2_03162017\afueflx64.efi -> FS0:\AFUDOS\SNJPME2_0316201
7\afuefl.smc
- [ok]
*****
* Please ignore this 'Shell: Cannot read from file - Device Error'
* warning message due to it does not impact flashing process.
*****
Deleting " "
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.