X12DSC-A6

USER'S MANUAL

Revision 1.0

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

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

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

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

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

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

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

Manual Revision 1.0

Release Date: October 27, 2021

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 © 2021 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 X12DSC-A6 motherboard.

About This Motherboard

The Supermicro X12DSC-A6 supports dual 3rd Generation Intel® Xeon® Scalable Processors (in Socket P+ LGA 4189) with up to 40 CPU cores and a Thermal Design Power (TDP) of up to 270W. Built with the Intel C621A chipset, the X12DSC-A6 supports up to 4 TB of 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 ECC memory with speeds of 3200/2933/2666 MHz in 16 DIMMs, and up to 4 TB of Intel Optane™ Persistent Memory (PMem) 200 Series with speeds of up to 3200 MHz. This motherboard features superior IO expandability, which includes three PCIe 4.0 x16 slots, one PCIe 4.0 x16 in AIOM networking slot, eight PCIe 4.0 NVMe U.2 connections, two PCIe 4.0 x4/S-SATA hybrid M.2 slots (with support of M-key 2280 and 22110), four SATA 3.0 connections (two SATA 3.0 and two SuperDOM ports), two USB 3.0 ports and one vertical Type-A connector. It also offers the most advanced data protection capability that encompasses Trusted Platform Module (TPM, with support of a TPM header) and Root of Trust (RoT) support. The X12DSC-A6 provides superb system performance, effective system cooling, and unparalleled PCIe capability currently available on the market. This motherboard is ideal for high-end, high-performance enterprise storage, database storage, and virtualization server platforms. Please note that this motherboard is intended to be installed and serviced by professional technicians only. For processor/memory updates, please refer to our website at http://www.supermicro.com/products/.

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

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

Conventions Used in the Manual

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

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

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

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

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

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
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@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer 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:	support@supermicro.com.tw
Website:	www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Overview....8
1.2 Processor and Chipset Support....17
1.3 Special Features....17
1.4 System Health Monitoring....18
1.5 ACPI Features....18
1.6 Power Supply....19
1.7 Serial Port....19
1.8 Intel® Optane™ Persistent Memory (PMem) 200 Series Overview....19

Chapter 2 Installation

2.1 Static-Sensitive Devices....20
2.2 Processor and Heatsink Installation....21
2.3 Motherboard Installation....37
2.4 Memory Support and Installation....39
2.5 Rear I/O Ports....43
2.6 Front Control Panel....47
2.7 Connectors....53
2.8 Jumper Settings....64
2.9 LED Indicators....67

Chapter 3 Troubleshooting

3.1 Troubleshooting Procedures....68
3.2 Technical Support Procedures....71
3.3 Frequently Asked Questions....72
3.4 Battery Removal and Installation....74
3.5 Returning Merchandise for Service....75

Chapter 4 UEFI BIOS

4.1 Introduction....76
4.2 Main Setup....77
4.3 Advanced Setup Configurations....79
4.4 Event Logs....143
4.5 IPMI....145

4.6 Security.....148
4.7 Boot.....153
4.8 Save & Exit.....155
Appendix A BIOS POST Codes
A.1 BIOS POST Codes.....157
Appendix B Software
B.1 Microsoft Windows OS Installation.....158
B.2 Driver Installation.....160
B.3 SuperDoctor® 5.....161
B.4 BMC.....162
B.5 Logging into the BMC (Baseboard Management Controller).....162
Appendix C Standardized Warning Statements

Chapter 1

Introduction

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

1.1 Overview

This motherboard was designed to be used with a Supermicro-proprietary chassis as an integrated server platform. It is not to be used as a stand-alone product and will not be shipped independently in a retail box. No motherboard shipping package will be provided in your shipment.

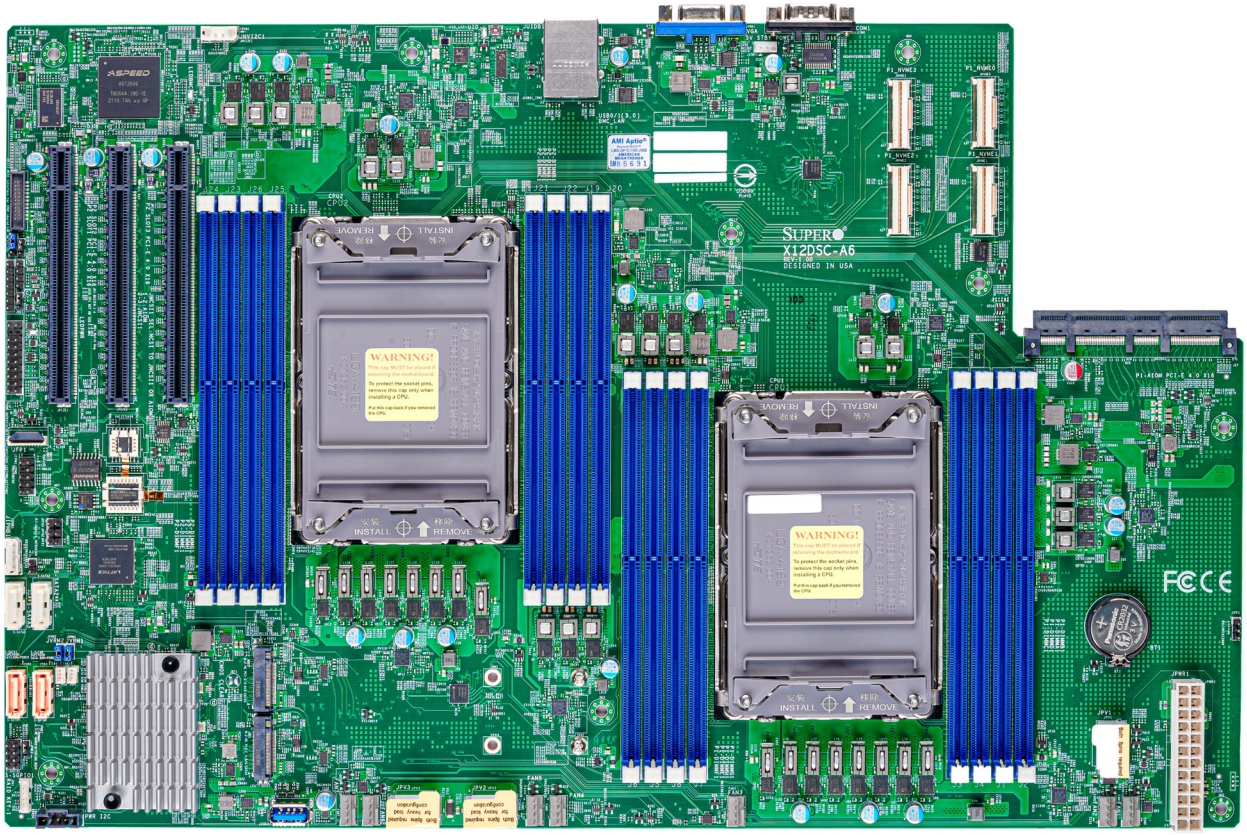
Important Links

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

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

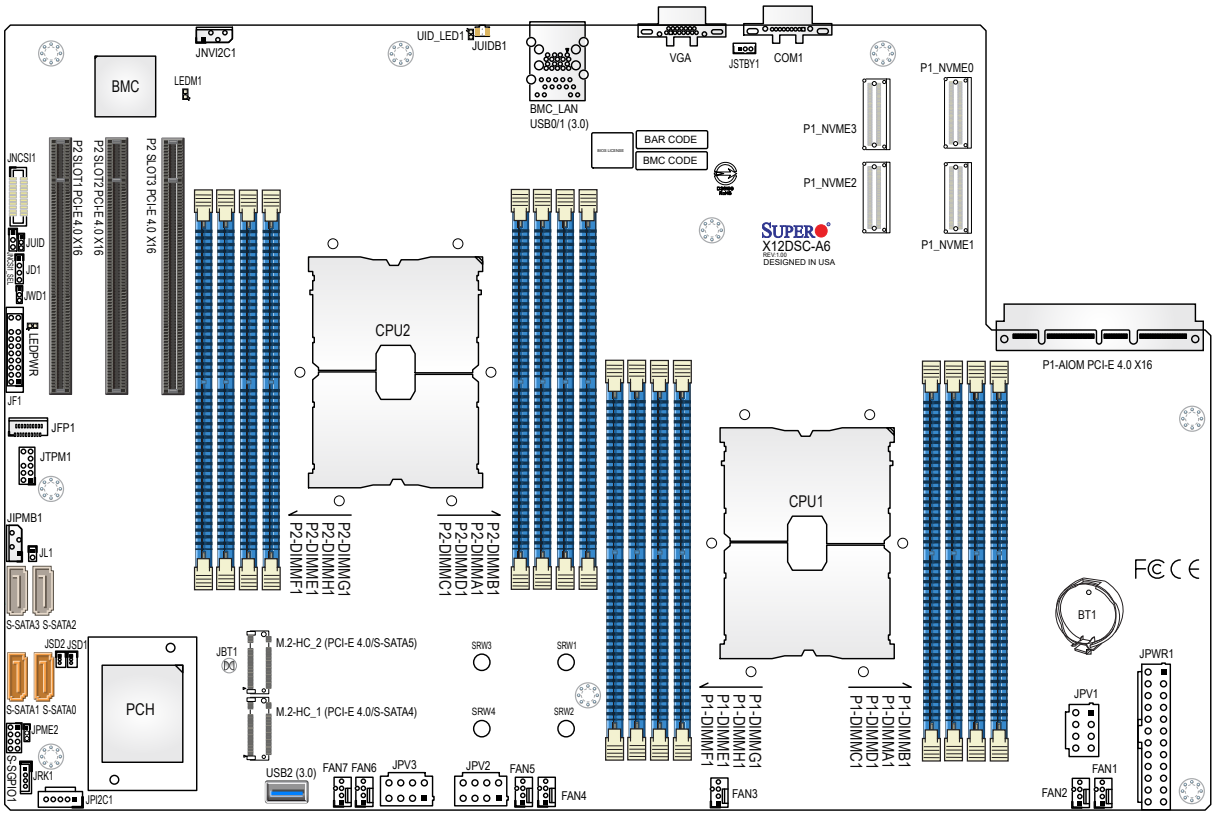
X12DSC-A6 Motherboard Image



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.

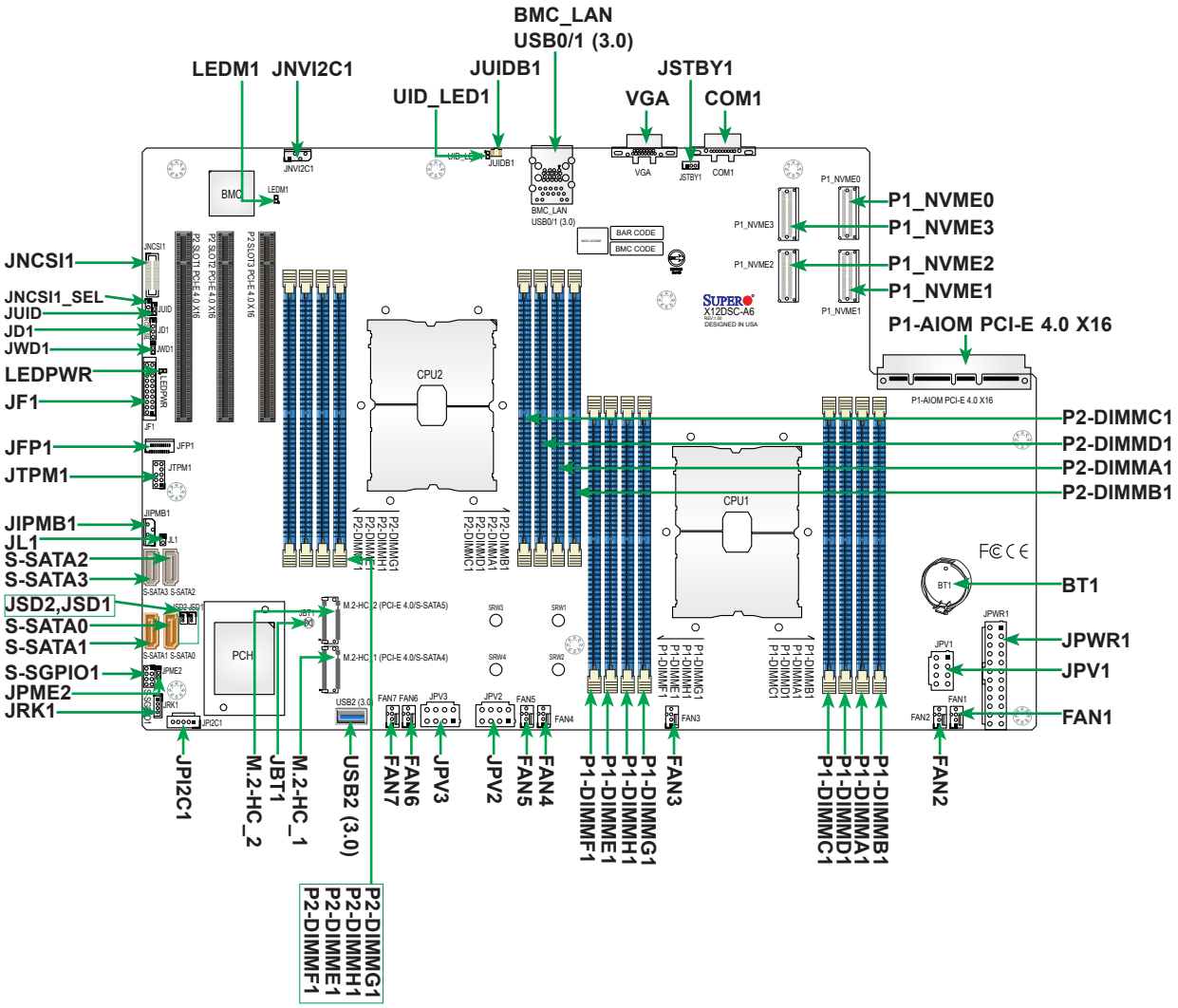
X12DSC-A6 Motherboard Layout

(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
JBT1	CMOS Clear	Open (Normal)
JNCSI1_SEL	NCSI to JNCSI1 or AIOM	Pins 1-2 (AIOM, default) Pins 2-3 (JNCSI1)
JPME2	ME Manufacturing Recovery	Pins 1-2 (Normal)
JUID	UID Switch	Pins 1-2 (UID Enabled) Pins 2-3 (System Reset, default)
JWD1	Watchdog Timer Reset	Pins 1-2 (Reset)

LED	Description	Status
LEDM1	BMC Heartbeat LED	Blinking Green: BMC Normal
LEDPWR	Onboard Power LED	LED On: Onboard Power On
UID_LED1	Unit Identifier (UID) LED	Solid Blue: Unit Identified

Connector	Description
Battery (BT1)	Onboard CMOS Battery
BMC_LAN	Dedicated BMC LAN Port
COM1	Rear I/O COM Port
FAN1 - FAN7	System Cooling Fan Headers
JD1	4-pin Speaker Header (Optional)
JF1	Front Control Panel Header
JFP1	Front Control Panel Header for FFC/FPC cable * FCC: Flexible Flat Cable. FPC: Flexible Printed Circuit
JIPMB1	4-pin BMC External I^2C Header
JL1	Chassis Intrusion Header
JNCSI1	Network Controller Sideband Interface (NC-SI) Connector for BMC shared LAN
JNVI2C1	NVMe I^2C Header
JPI2C1	Power System Management Bus (SMBus) I^2C Header
JPV1, JPV2, JPV3	8-pin Power Connectors (Required)
JPWR1	24-pin ATX Power Connector (Required)
JRK1 (VROC)	Intel VROC Key Header for NVMe RAID support
JSD1, JSD2	SATA DOM Power Connectors
JSTBY1	5V Standby Power Header
JTPM1	Trusted Platform Module (TPM)/Port 80 Header
JUIDB1	Unit Identifier (UID) Switch / BMC Reset Button
M.2-HC_1/S-SATA4, M.2-HC_2/S-SATA5	PCIe 4.0 x4/S-SATA Hybrid M.2 Slots (with support of M-key 2280 and 22110)
P1_NVME0 - P1_NVME3	PCIe 4.0 x8 NVMe SlimSAS Slots
P1-AIOM	CPU1 PCIe 4.0 x16 Slot for SMCI Advanced I/O Module (AIOM) * This slot supports a network adapter card.

Connector	Description
P2 SLOT1 - P2 SLOT3	CPU2 PCIe 4.0 x16 Slots
S-SATA0, S-SATA1	Intel PCH Powered S-SATA 3.0 Ports (with support of SuperDOM devices) * DOM: Disk on Module
S-SATA2, S-SATA3	Intel PCH SATA 3.0 Ports (with support of RAID 0, 1, 5, 10)
S-SGPIO1	Serial General Purpose I/O Connection Header (for S-SATA0/1/2/3)
SRW1 - SRW4	M.2 Device Mounting Holes
USB0, USB1	Rear I/O USB 3.0 Ports
USB2	Internal USB 3.0 Vertical Type-A Connector
VGA	Rear VGA Port (on the I/O back panel)

Motherboard Features

Motherboard Features	
CPU	
• Supports dual 3rd Gen. Intel Xeon Scalable Processors (in Socket P+ LGA 4189) with up to 40 cores per CPU and a Thermal Design Power (TDP) of up to 270W	
Memory	
• Supports up to 4 TB of 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 (288-pin) ECC memory with speeds of 3200/2933/2666 MHz in 16 memory slots and up to 4 TB of Intel Optane PMem 200 Series with speeds of up to 3200 MHz **Note 1:** The Intel Optane Persistent Memory (PMem) 200 Series are supported by the 3rd Gen. Intel Xeon Scalable (83xx/63xx/53xx/4314) processors. **Note 2:** Memory speed and capacity support depends on the processors used in the system.	
DIMM Size	
• Up to 256 GB at 1.2V **Note:** For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.	
Chipset	
• Intel PCH C621A	
Expansion Slots	
• Three PCIe 4.0 x16 slots (P2 SLOT1, P2 SLOT2, P2 SLOT3) • Two PCIe 4.0 x4/S-SATA hybrid M.2 slots (with support of M-key 2280 and 22110) • Four PCIe 4.0 x8 NVMe SlimSAS slots (P1_NVME0, P1_NVME1, P1_NVME2, P1_NVME3)	
Network	
• One Dedicated BMC LAN located on the rear I/O panel (via AST2600 BMC)	
Baseboard Management Controller (BMC)	
• ASPEED AST2600 BMC	
Graphics	
• Graphics controller & VGA support via ASPEED AST2600 BMC	
I/O Devices	
• Serial (COM) Port	• One serial port on the rear I/O panel (COM1)
• SATA 3.0	• Four S-SATA 3.0 ports supported by Intel PCH (S-SATA0 - S-SATA3). Two of them are with support for SuperDOM (Disk on Module) devices (S-SATA0, S-SATA1).
• Video (VGA) Connection	• One VGA port on the rear I/O panel (VGA)
Peripheral Devices	
• Two USB 3.0 ports on the rear I/O panel (USB0, USB1) • One internal USB 3.0 vertical Type-A connector (USB2)	

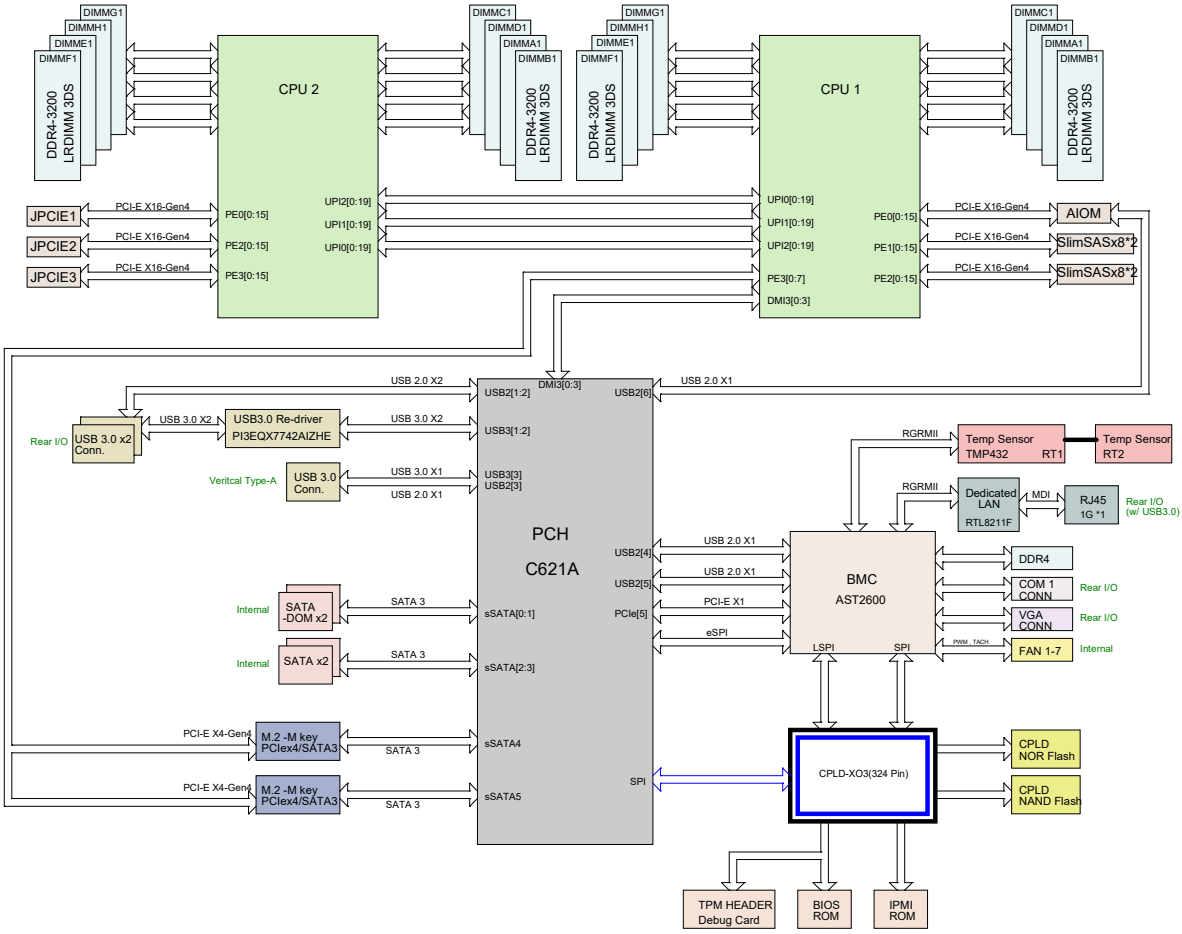
BIOS
• AMI BIOS • ACPI 3.0 or later, PCI firmware 4.0 support, BIOS rescue hot-key, SPI dual/quad speed support, RTC (Real Time Clock) wakeup, and SMBIOS 3.0 or later
Power Management
• ACPI power management • Power button override mechanism • Power-on mode for AC power recovery • Wake-on-LAN • Power supply monitoring
System Health Monitoring
• Onboard voltage monitoring for +/-12V, +5V/+5V standby, +3.3V, and +3.3V standby • Onboard temperature monitoring for CPU, VRM, LAN, PCH, system, and memory • 7+1 CPU switch phase voltage regulator • CPU thermal trip support • Platform Environment Control Interface (PECI)
Fan Control
• Fan status monitoring via BMC connections • Single cooling zone • Low-noise fan speed control • Seven 4-pin fan headers
System Management
• SuperDoctor® 5 • Chassis intrusion header and detection • Server platform service
Firmware Integrity/System Security
• Trusted Platform Module (TPM) support • Root of Trust (RoT) support to protect firmware security by detecting critical data corruption, and restoring platform integrity
LED Indicators
• Power LED • UID/remote UID • LAN activity LED • BMC Heartbeat LED
Dimensions
• 16.9" (W) x 11" (L) ATX (429.3 mm x 279.4 mm)

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

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

System Block Diagram

X12DSC-A6



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

1.2 Processor and Chipset Support

Built upon the functionality and capability of the 3rd Gen. Intel Xeon Scalable Processors (Socket P+) and the Intel C621A chipset, the X12DSC-A6 motherboard increases energy efficiency, and system performance for a multitude of applications such as high-end, high-performance enterprise storage, database storage, and virtualization server platforms.

Features Supported

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

1.3 Special Features

Recovery from AC Power Loss

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

1.4 System Health Monitoring

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the BMC interface. Whenever the temperature of the CPU or the system exceeds the manufacturer-defined threshold, system/CPU cooling fans will increase fan spin to provide better air flow to prevent the CPU or the system from overheating.

Note: To avoid possible system overheating, please be sure to provide adequate air-flow to your system.

System Resource Alert

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

1.5 ACPI Features

ACPI stands for Advanced Configuration and Power Interface. The ACPI specification defines a flexible and abstract hardware interface that provides a standard way to integrate power management features throughout a computer system, including its hardware, operating system and application software. This enables the system to automatically turn on and off peripherals such as network cards, hard disk drives and printers.

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play, and an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures, while providing a processor architecture-independent implementation that is compatible with appropriate Windows operating systems. For detailed information regarding OS support, please refer to the Supermicro website.

1.6 Power Supply

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

The X12DSC-A6 motherboard accommodates proprietary power distribution board (PDB) with two power supply units. Although most power supplies generally meet the specifications required by the CPU, some are inadequate. In addition, three 12V 8-pin power connections are also required to ensure adequate power supply to the system.

Warning! To avoid damaging the power supply on the motherboard, be sure to use a power distribution board (PDB) that contains one 24-pin and three 8-pin power connectors. Be sure to connect the power supplies to the 24-pin power connector (JPWR1) and the 8-pin power connectors (JPV1/JPV2/JPV3) on the motherboard. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.

1.7 Serial Port

The X12DSC-A6 motherboard supports one serial communication connection. COM1 port can be used for input/output. The UART provides legacy speeds with a baud rate of up to 115.2 Kbps as well as an advanced speed with baud rates of 250 K, 500 K, or 1 Mb/s, which support high-speed serial communication devices.

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

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

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

Chapter 2

Installation

2.1 Static-Sensitive Devices

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

Precautions

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

Unpacking

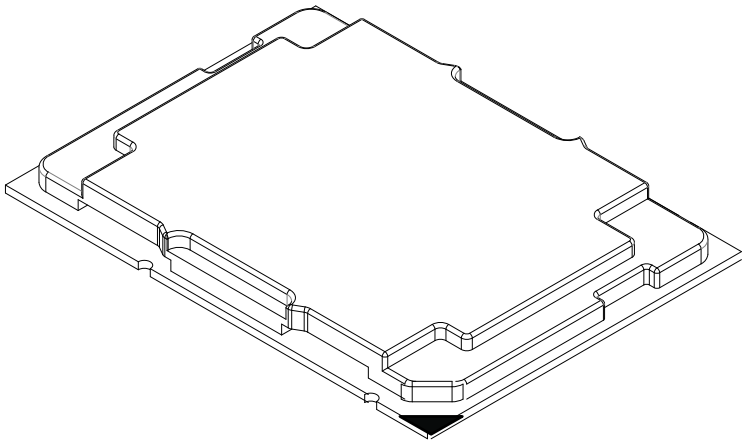
The motherboard is shipped in antistatic packaging to avoid static damage. When unpacking the motherboard, make sure that the person handling it is static protected.

2.2 Processor and Heatsink Installation

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

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

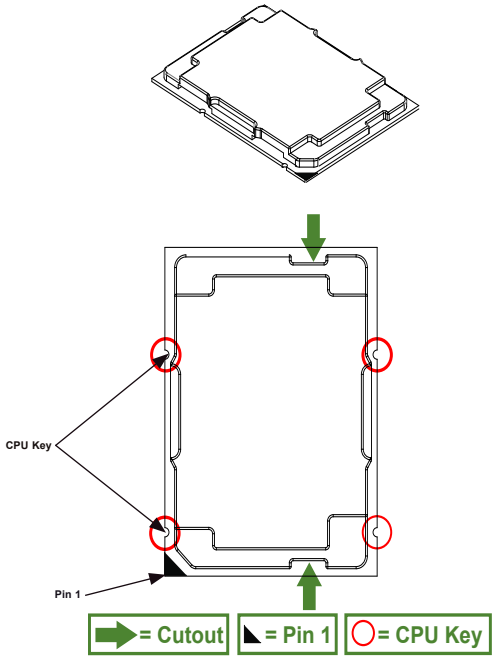
The 3rd Gen. Intel Xeon Scalable Processor



Processor Top View

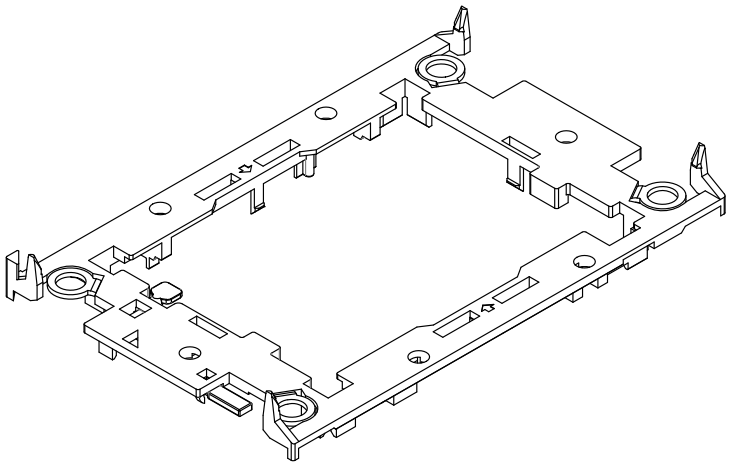
1. The 3rd Gen. Intel Xeon Scalable Processor

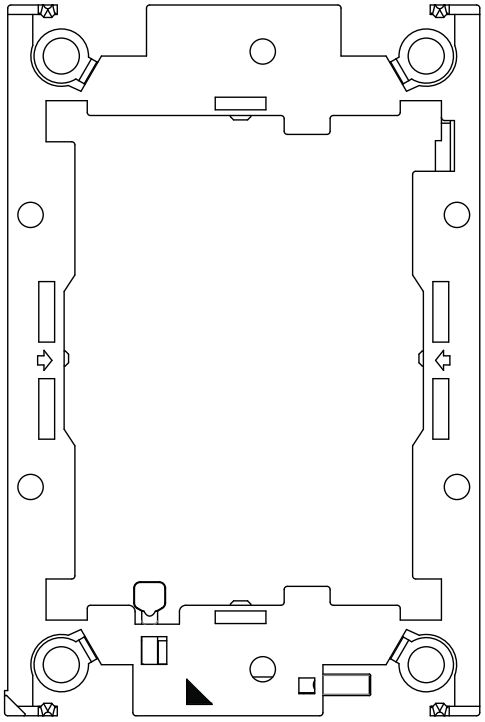
Processor Top View (3D)



Processor Top View

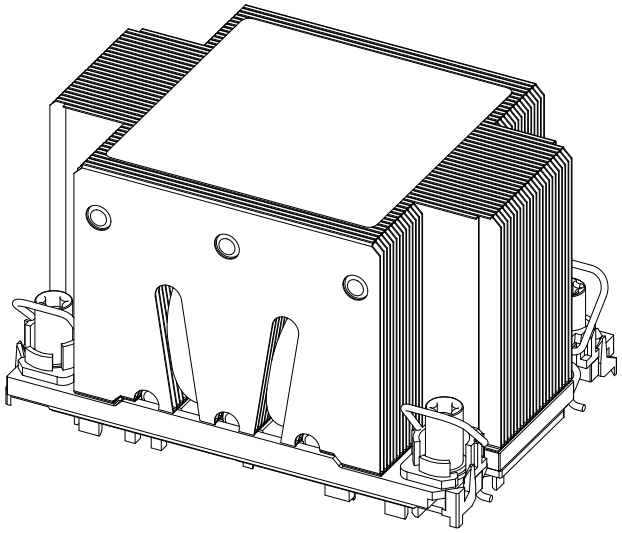
2. The Processor Carrier





Carrier Bottom View

3. Heatsink

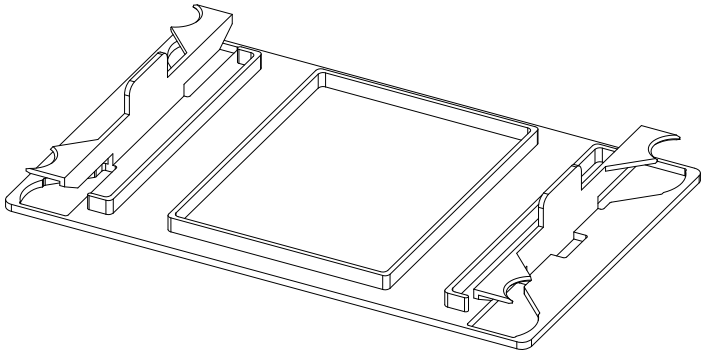


Note: Exercise extreme care when handling the heatsink. Pay attention to the edges of heatsink fins which can be sharp! To avoid damaging the heatsink, please do not apply excessive force on the fins when handling the heatsink.

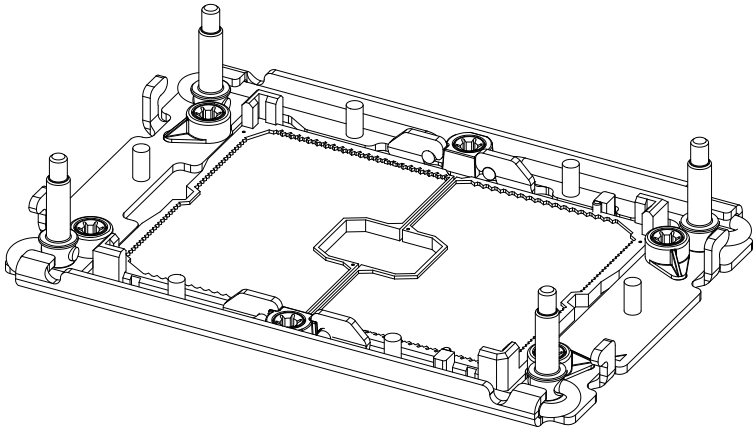
Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

Plastic Protective Cover



CPU Socket

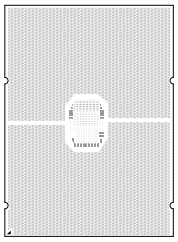


Overview of the Processor Carrier Assembly

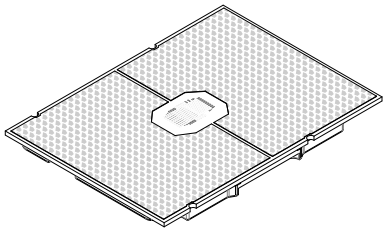
The processor carrier assembly contains a 3rd Gen. Intel Xeon Scalable processor and a processor carrier. Carefully follow the instructions given in the installation section to place a processor into the carrier to create a processor carrier.

1. The 3rd Gen. Intel Xeon Scalable Processor

Intel Processor (Bottom View)



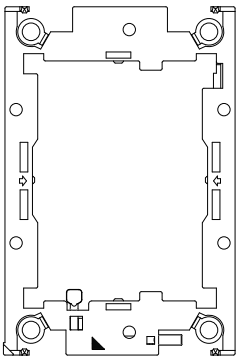
Processor (2D)



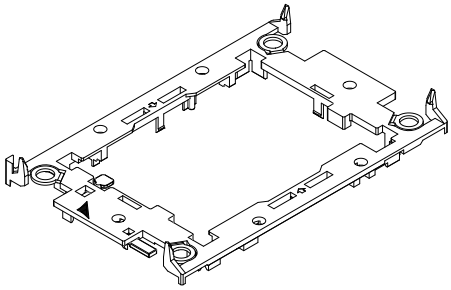
Processor (3D)

2. Processor Carrier

Intel Processor Carrier (Top View)

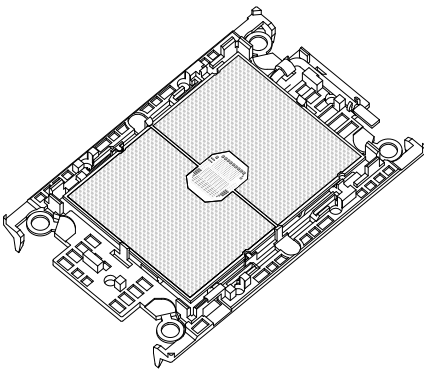


Processor Carrier (2D)



Processor Carrier (3D)

3. Processor Carrier Assembly

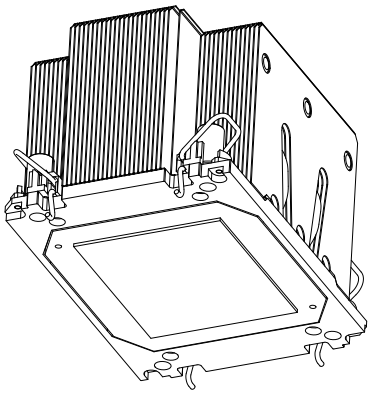


(with Processor Seated inside the Carrier)

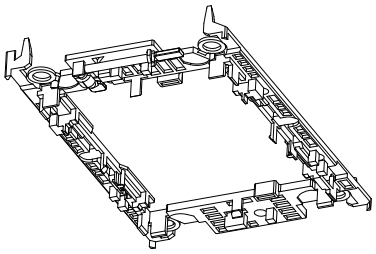
Overview of the Processor Heatsink Module

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

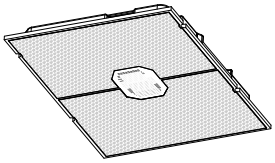
1. Heatsink (with Thermal Grease)



2. Processor Carrier

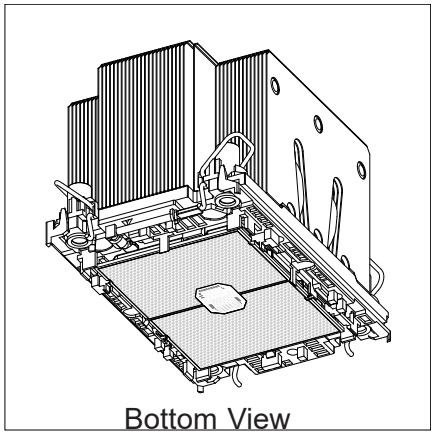


3. The 3rd Gen. Intel Xeon Scalable Processor



Bottom View

4. Processor Heatsink Module (PHM)



Bottom View

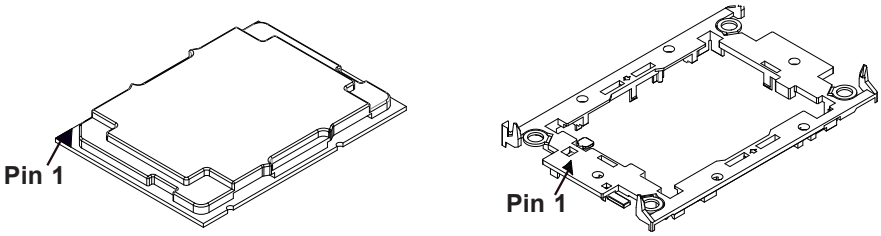
Creating the Processor Carrier Assembly

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

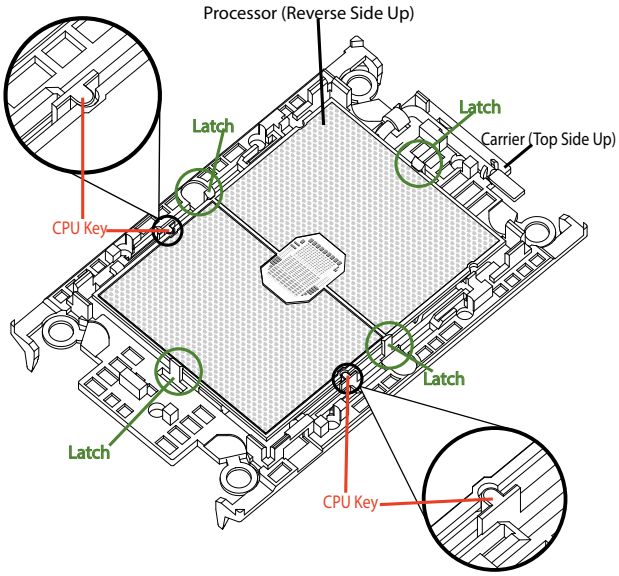
To create the processor carrier assembly, please follow the steps below:

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

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

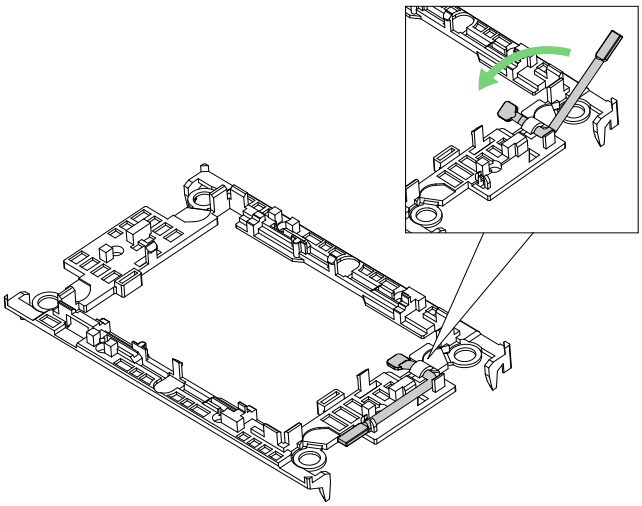


2. First, turn over the processor carrier and locate Pin 1 on the CPU and Pin 1 on the carrier. Then, turn the processor over with the processor reverse side (gold contacts) facing up and locate CPU keys on the processor. Finally, locate the CPU keys and four latches on the carrier as shown below.



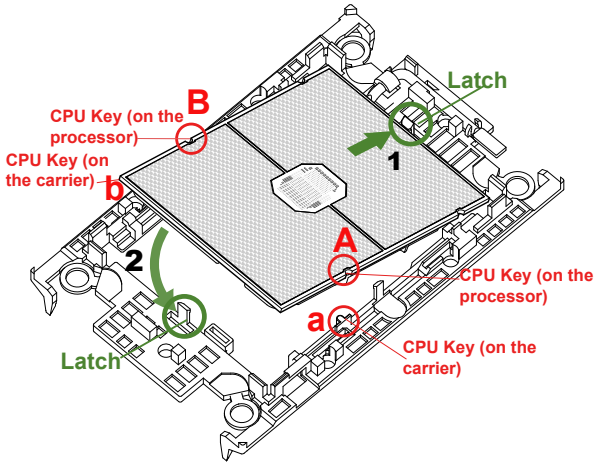
Carrier with the Processor Installed

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



4. Using Pin 1 as a guide, carefully align the CPU keys (A & B) on the processor against the CPU keys on the carrier (a & b) as shown in the drawing below.

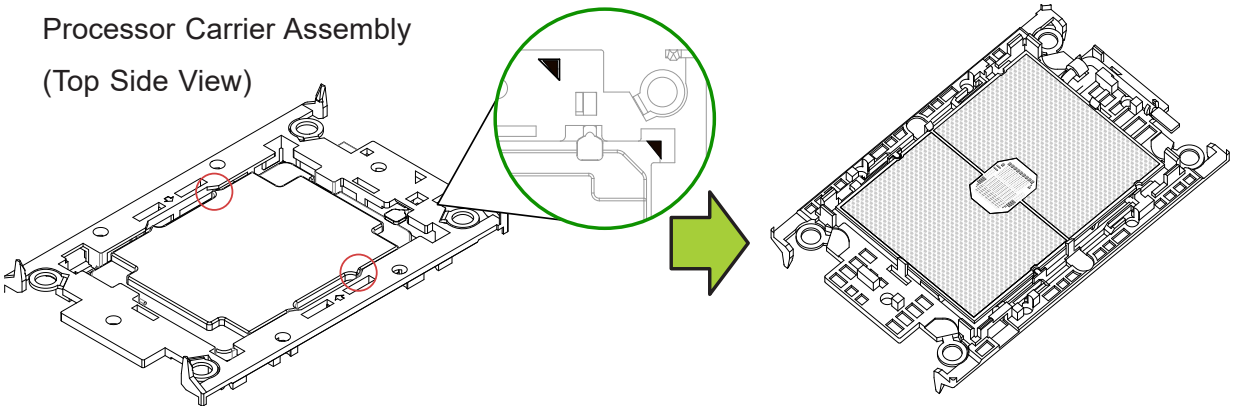
5. Once they are properly aligned, carefully place one end of the processor into the latch marked 1 on the carrier, and place the other end of processor into the latch marked 2.



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

Processor Carrier Assembly

(Top Side View)



Processor Carrier Assembly

Creating the Processor Heatsink Module (PHM)

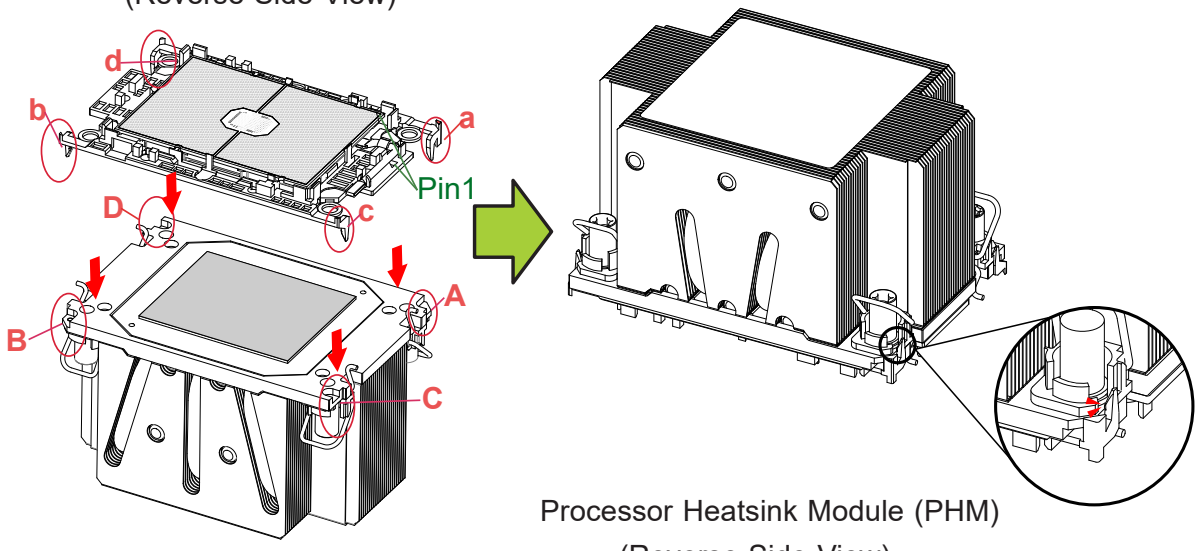
After creating the processor carrier assembly, please follow the instructions below to mount the processor carrier into the heatsink to form the processor heatsink module (PHM).

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

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

Processor Carrier Assembly

(Reverse Side View)



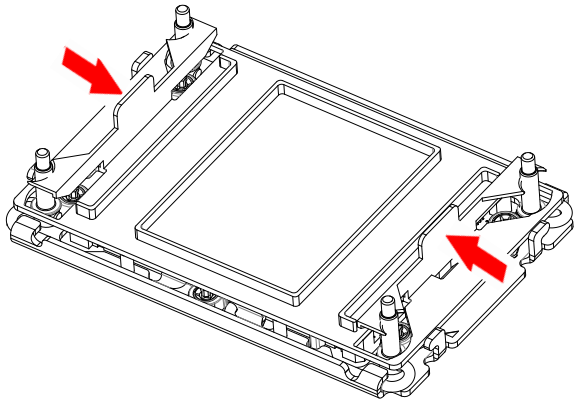
Processor Heatsink Module (PHM)

(Reverse Side View)

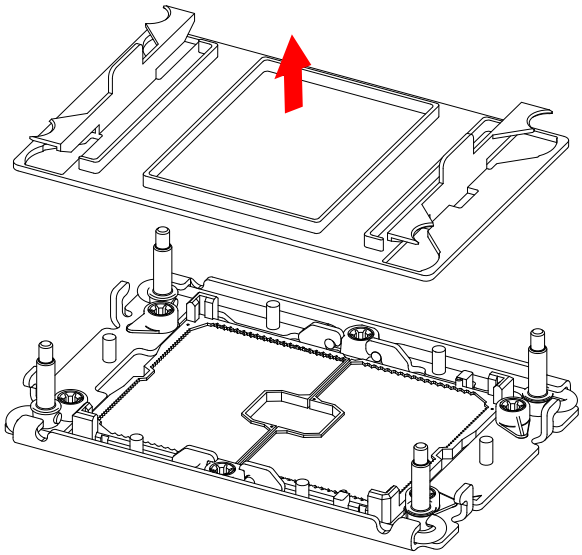
Preparing the CPU Socket for Installation

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

Removing the Plastic Protective Cover from the Socket



1. Press the tabs inward.

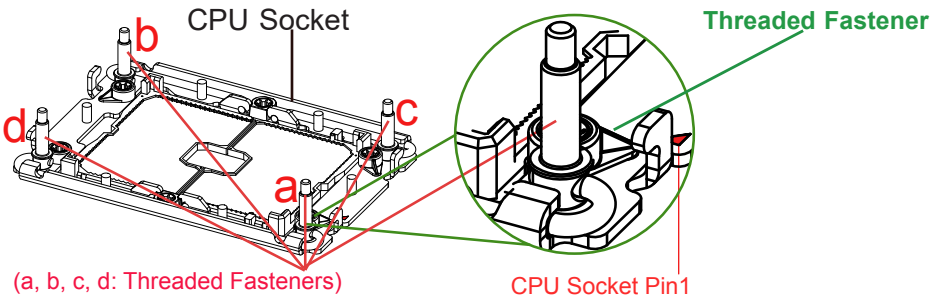


2. Pull up the protective cover from the socket.

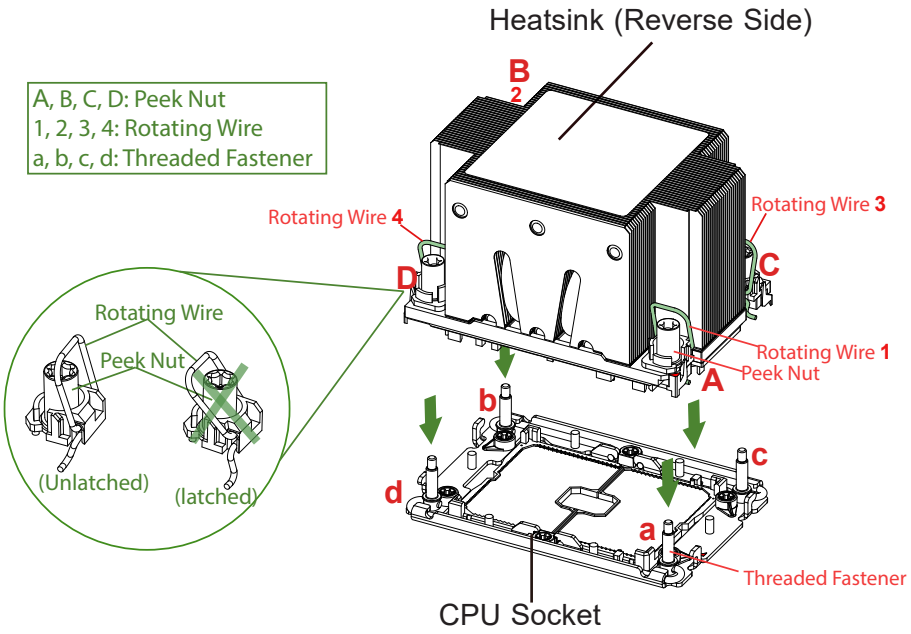
Preparing to Install the Processor Heatsink Module (PHM) into the CPU Socket

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

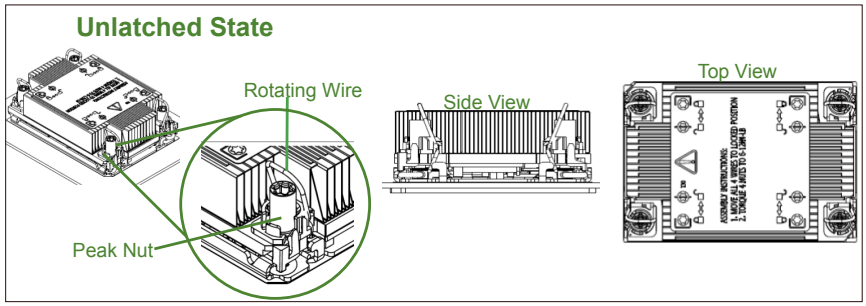
1. Locate four threaded fasteners (a, b, c, d) on the CPU socket.



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



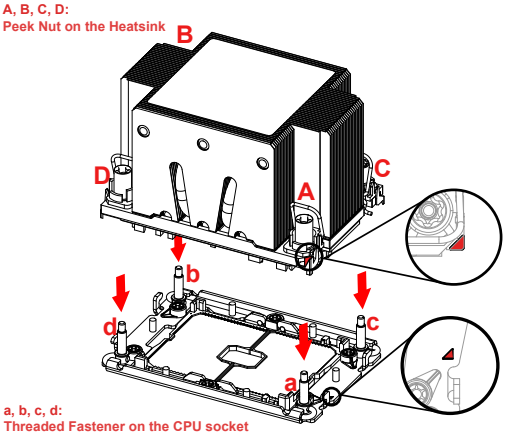
3. Check the rotating wires (1, 2, 3, 4) to make sure that they are at unlatched positions as shown in the drawing below before installing the PHM into the CPU socket.



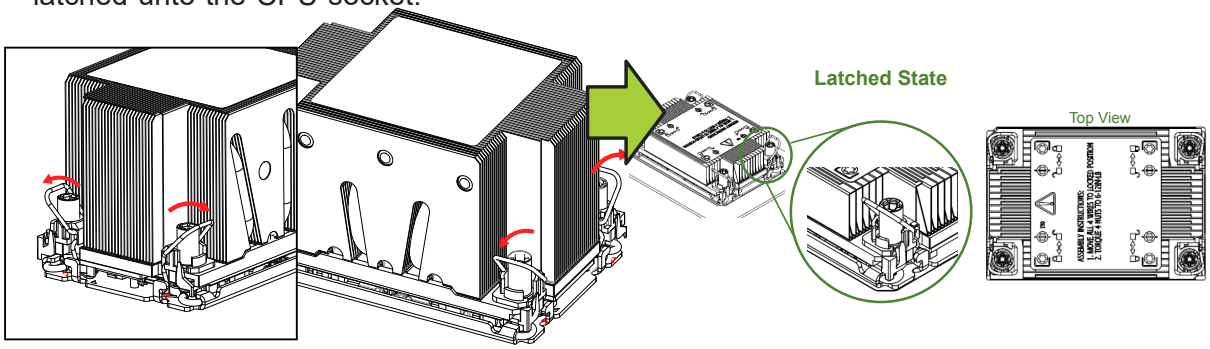
Installing the Processor Heatsink Module (PHM)

1. Align peek nut "A", which is next to the triangle (Pin 1) on the heatsink, against threaded fastener "a" on the CPU socket. Then align peek nuts "B", "C", "D" on the heatsink against threaded fasteners "b", "c", "d" on the CPU socket, making sure that all peek nuts on the heatsink are properly aligned with the correspondent threaded fasteners on the CPU socket.

2. Once they are aligned, gently place the heatsink on top the CPU socket, making sure that each peek nut is properly attached to its corresponding threaded fastener.

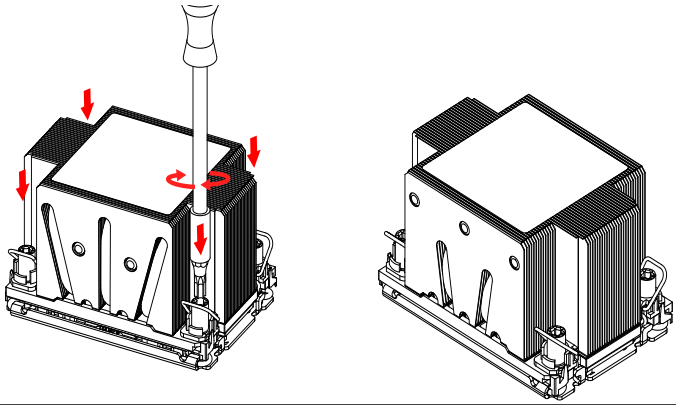


3. Press all four rotating wires outwards and make sure that the heatsink is securely latched unto the CPU socket.



4. With a T30-bit screwdriver, tighten all peek nuts in the sequence of "A", "B", "C", and "D" with even pressure. To avoid damaging the processor or socket, do not use a force greater than 12 lbf-in when tightening the screws.

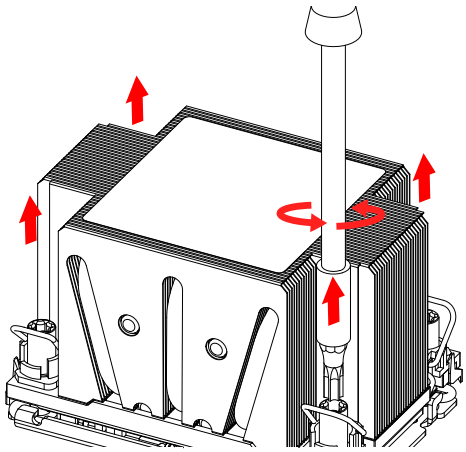
5. Examine all corners heatsink to ensure that the PHM is firmly attached to the CPU socket.



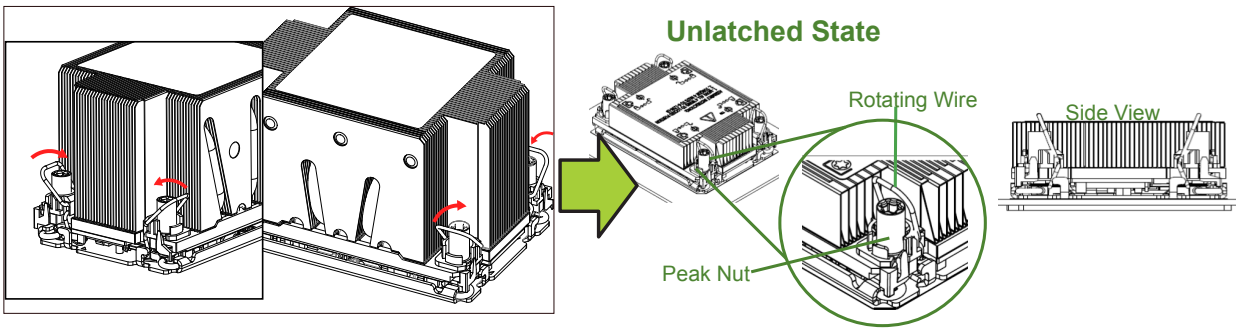
Removing the Processor Heatsink Module from the CPU Socket

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

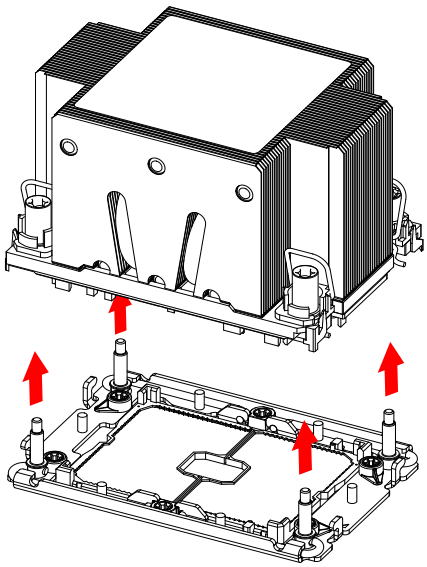
1. Use a T30-bit screwdriver to loosen the four peek nuts on the heatsink in the sequence of #A, #B, #C, and #D.



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



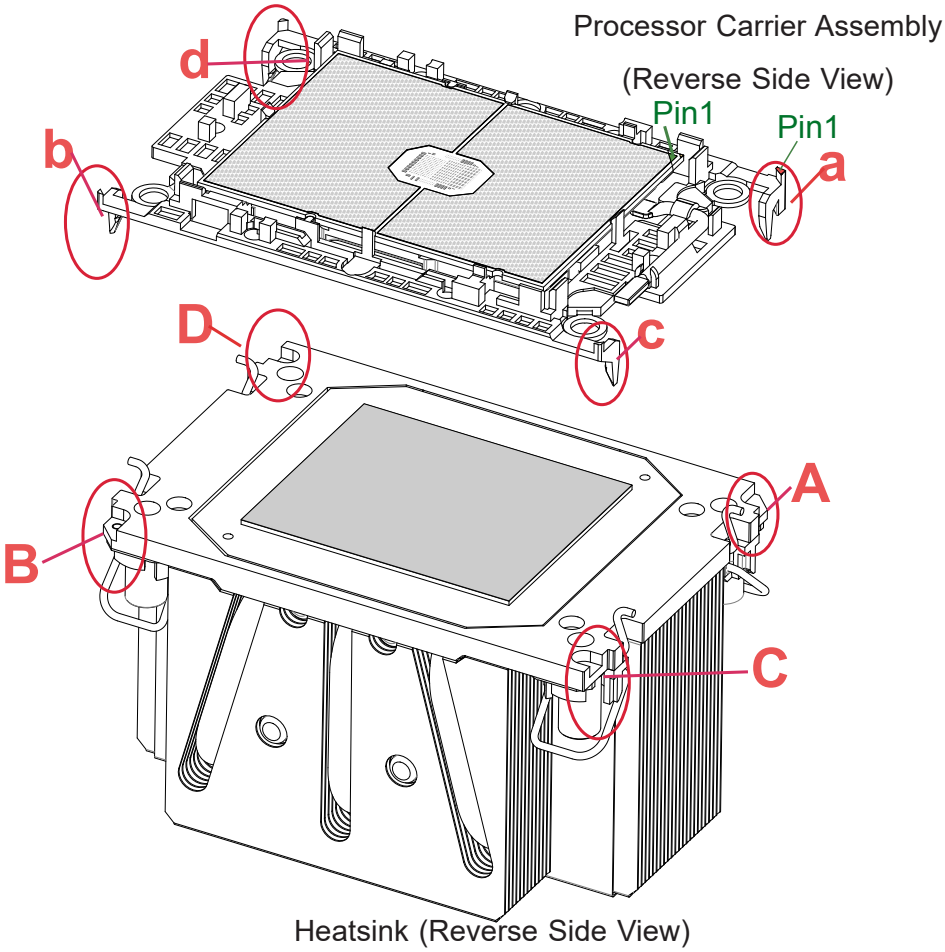
3. Gently lift the PHM upwards to remove it from the CPU socket.



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

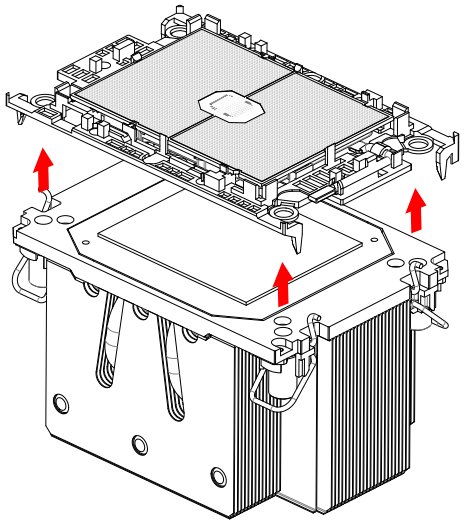
To remove the processor carrier assembly from the PHM, please follow the steps below:

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



Heatsink (Reverse Side View)

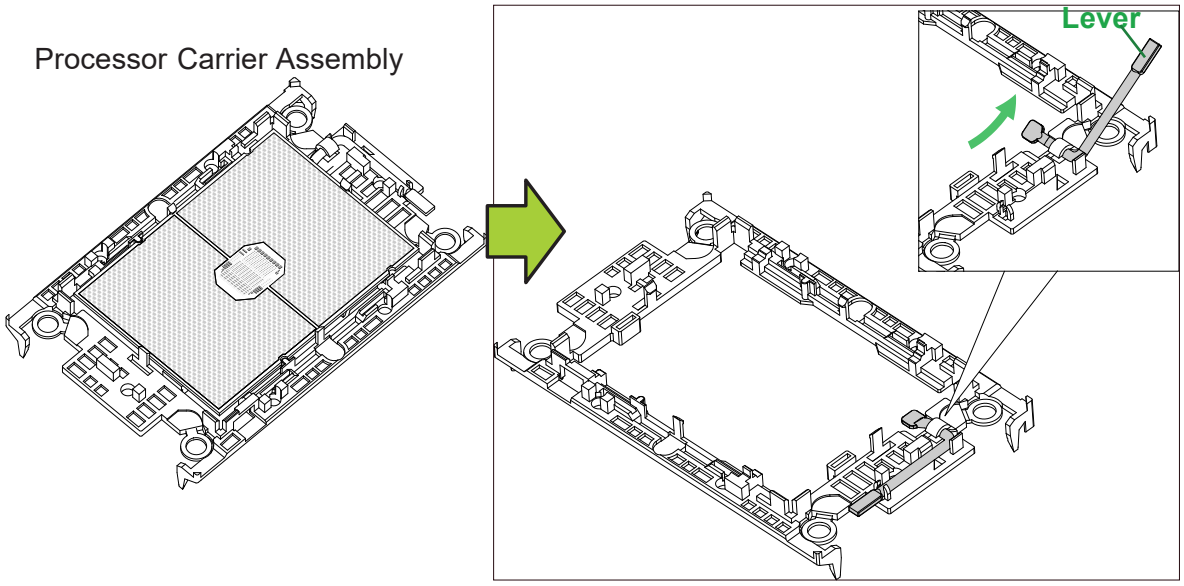
2. When all plastic clips are detached from the heatsink, remove the processor carrier assembly from the heatsink



Removing the Processor from the Processor Carrier Assembly

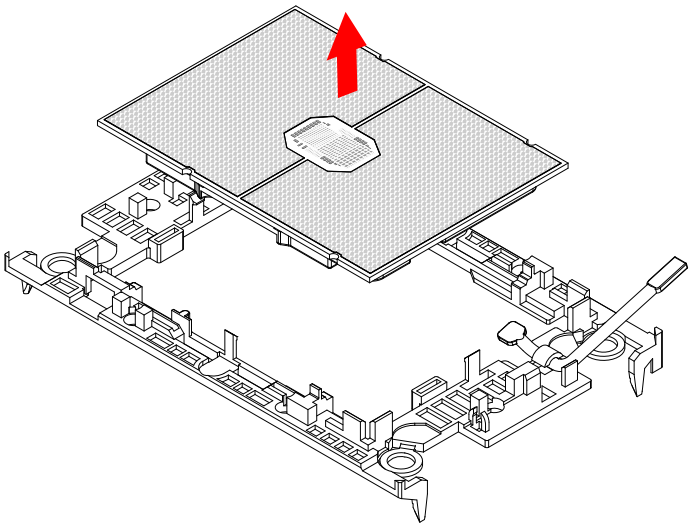
Once you have removed the processor carrier assembly from the PHM, you are ready to remove the processor from the processor carrier by following the steps below.

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



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

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



2.3 Motherboard Installation

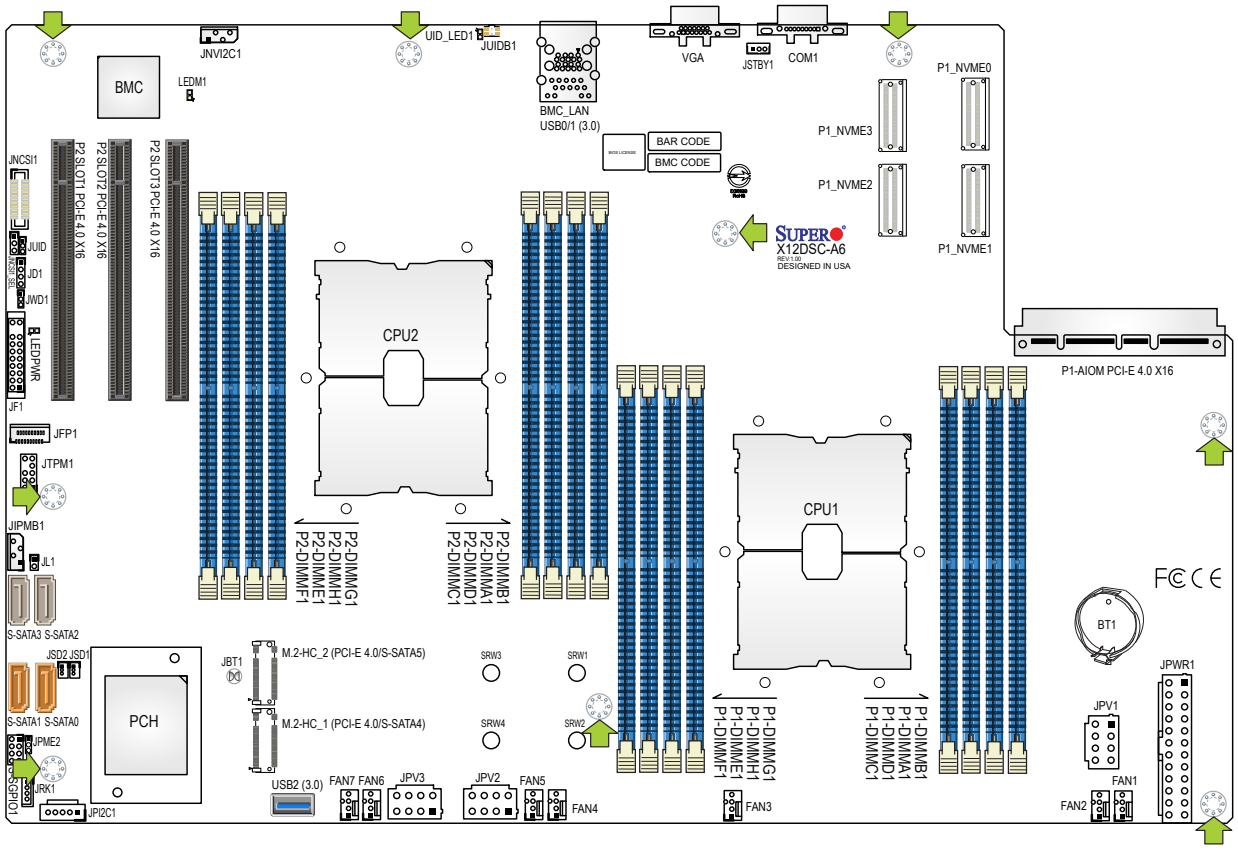
All motherboards have standard mounting holes to fit different types of chassis. Make sure that the locations of all the mounting holes for both the motherboard and the chassis match. Although a chassis may have both plastic and metal mounting fasteners, metal ones are highly recommended because they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

Tools Needed

Phillips Screwdriver (1)

Phillips Screws (9)

Standoffs (9) Only if Needed



Location of Mounting Holes

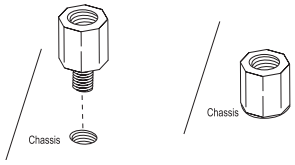
Note 1: To avoid damaging the motherboard and its components, please do not use a force greater than 8 lbf-in on each mounting screw during motherboard installation.

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

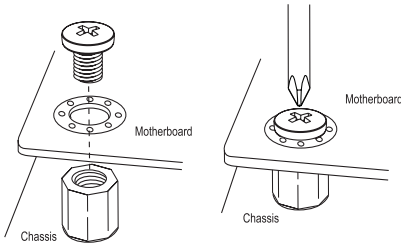
Installing the Motherboard

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

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



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



4. Install standoffs in the chassis as needed.
5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
6. Using the Phillips screwdriver, insert a pan head #6 screw into a mounting hole on the motherboard and its matching mounting hole on the chassis.
7. Repeat Step 6 to insert #6 screws into all mounting holes.
8. Make sure that the motherboard is securely placed in the chassis.

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

2.4 Memory Support and Installation

Note: Check the Supermicro website for recommended memory modules.

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

Memory Support

The X12DSC-A6 supports up to 4 TB of 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 (288-pin) ECC memory with speeds of 3200/2933/2666 MHz in 16 memory slots and up to 4 TB of Intel Optane PMem 200 Series with speeds of up to 3200 MHz.

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

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

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

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

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

Memory Population Table (with 16 Slots)	
When 1 CPU is used:	***Memory Population Sequence***
1 CPU & 1 DIMM	CPU1: P1-DIMMA1
1 CPU & 2 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1
1 CPU & 4 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1
1 CPU & 6 DIMM	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1
1 CPU & 8 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1/P1-DIMMD1/P1-DIMMH1
When 2 CPUs are used:	***Memory Population Sequence***
2 CPUs & 2 DIMMs[Note]	CPU1: P1-DIMMA1 CPU2: P2-DIMMA1
2 CPUs & 4 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1 CPU2: P2-DIMMA1/P2-DIMME1
2 CPUs & 6 DIMMs	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1 CPU2: P2-DIMMA1/P2-DIMME1
2 CPUs & 8 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1 CPU2: P2-DIMMA1/P2-DIMME1/P2-DIMMC1/P2-DIMMG1
2 CPUs & 10 DIMMs	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1 CPU2: P2-DIMMA1/P2-DIMME1/P2-DIMMC1/P2-DIMMG1
2 CPUs & 12 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1 CPU2: P2-DIMMA1/P2-DIMME1/P2-DIMMC1/P2-DIMMG1/P2-DIMMB1/P2-DIMMF1
2 CPUs & 14 DIMMs	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1/P1-DIMMD1/P1-DIMMH1 CPU2: P2-DIMMA1/P2-DIMME1/P2-DIMMC1/P2-DIMMG1/P2-DIMMB1/P2-DIMMF1
2 CPUs & 16 DIMMs[Note]	CPU1: P1-DIMMA1/P1-DIMME1/P1-DIMMC1/P1-DIMMG1/P1-DIMMB1/P1-DIMMF1/P1-DIMMD1/P1-DIMMH1 CPU2: P2-DIMMA1/P2-DIMME1/P2-DIMMC1/P2-DIMMG1/P2-DIMMB1/P2-DIMMF1/P2-DIMMD1/P2-DIMMH1

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

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

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

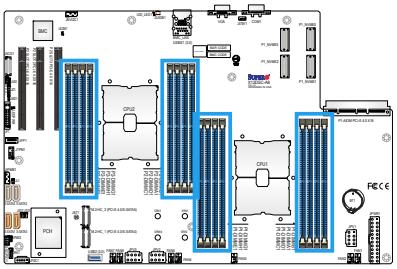
16-DIMM Motherboard PMem Population within 1 CPU socket										
DDR4+PMem	Mode	AD Interleave	P1-DIMMF1	P1-DIMME1	P1-DIMMH1	P1-DIMMG1	P1-DIMMC1	P1-DIMMD1	P1-DIMMA1	P1-DIMMB1
4+4	AD MM	One - x4	***PMem***	DDR4	***PMem***	DDR4	DDR4	***PMem***	DDR4	***PMem***
		One - x4	DDR4	***PMem***	DDR4	***PMem***	***PMem***	DDR4	***PMem***	DDR4
6+1	AD	One - x1	DDR4	DDR4	-	DDR4	DDR4	***PMem***	DDR4	DDR4
			-	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	***PMem***
			DDR4	DDR4	***PMem***	DDR4	DDR4	-	DDR4	DDR4
			PMem	DDR4	DDR4	DDR4	DDR4	DDR4	DDR4	-
			DDR4	DDR4	DDR4	-	***PMem***	DDR4	DDR4	DDR4
			DDR4	-	DDR4	DDR4	DDR4	DDR4	***PMem***	DDR4
			DDR4	DDR4	DDR4	***PMem***	-	DDR4	DDR4	DDR4
			DDR4	***PMem***	DDR4	DDR4	DDR4	DDR4	-	DDR4

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

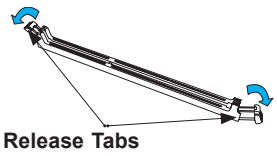
- Mode definitions: AD = App Direct Mode, MM = Memory Mode.
- No mixing of PMem and NVDIMMs within the platform.
- For MM, NM/FM ratio is between 1:4 and 1:16. The capacity not used for FM can be used for AD. (NM = Near Memory (DRAM); FM = Far Memory (PMem)).
- Matrix targets configs for optimized PMem to DRAM cache ratio in MM mode.
- For each individual population, different PMem rearrangements among channels are permitted so long as the configuration doesn't break X12 DP Memory population rules.
- Ensure the same DDR4 DIMM type and capacity are used for each DDR4 + PMem population.
- If the system detects an unvalidated configuration, then the system issues a BIOS warning. The CLI functionality is limited in non-POR configurations, and select commands will not be supported.

Validation Matrix (DDR4 DIMMS with PMem 200 Series)			
DIMM Type	Ranks Per DIMM & Data Width (Stack)	DIMM Capacity (GB)	
		DRAM Density	
		8Gb	16Gb
RDIMM (up to 3200)	1Rx8	N/A	N/A
	1Rx4	16GB	32GB
	1Rx8	16GB	32GB
	1Rx4	32GB	64GB
RDIMM 3DS (up to 3200)	4Rx4 (2H)	N/A	128GB
	8Rx4 (4H)	NA	256GB
LRDIMM (up to 3200)	4Rx4	64GB	128GB
LRDIMM 3DS (up to 3200)	4Rx4 (2H)	N/A	N/A
	8Rx4 (4H)	126GB	256GB

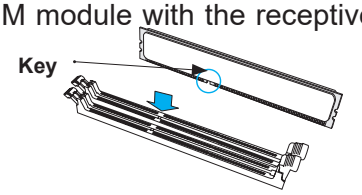
DIMM Installation



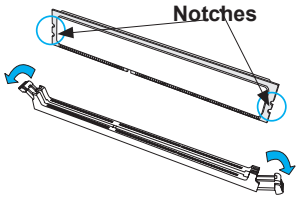
1. Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population tables in the previous section. Locate DIMM memory slots on the motherboard as shown on the right.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.



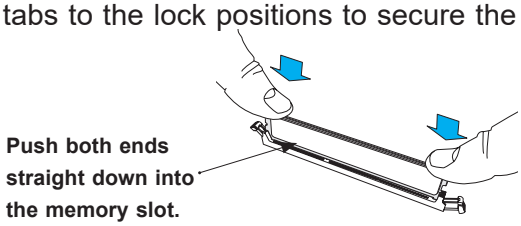
3. Align the key of the DIMM module with the receptive point on the memory slot.



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

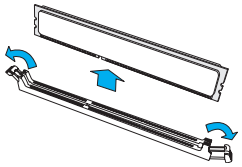


5. Push both ends of the module straight down into the slot until the module snaps into place.
6. Press the release tabs to the lock positions to secure the DIMM module into the slot.



DIMM Removal

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



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

2.5 Rear I/O Ports

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

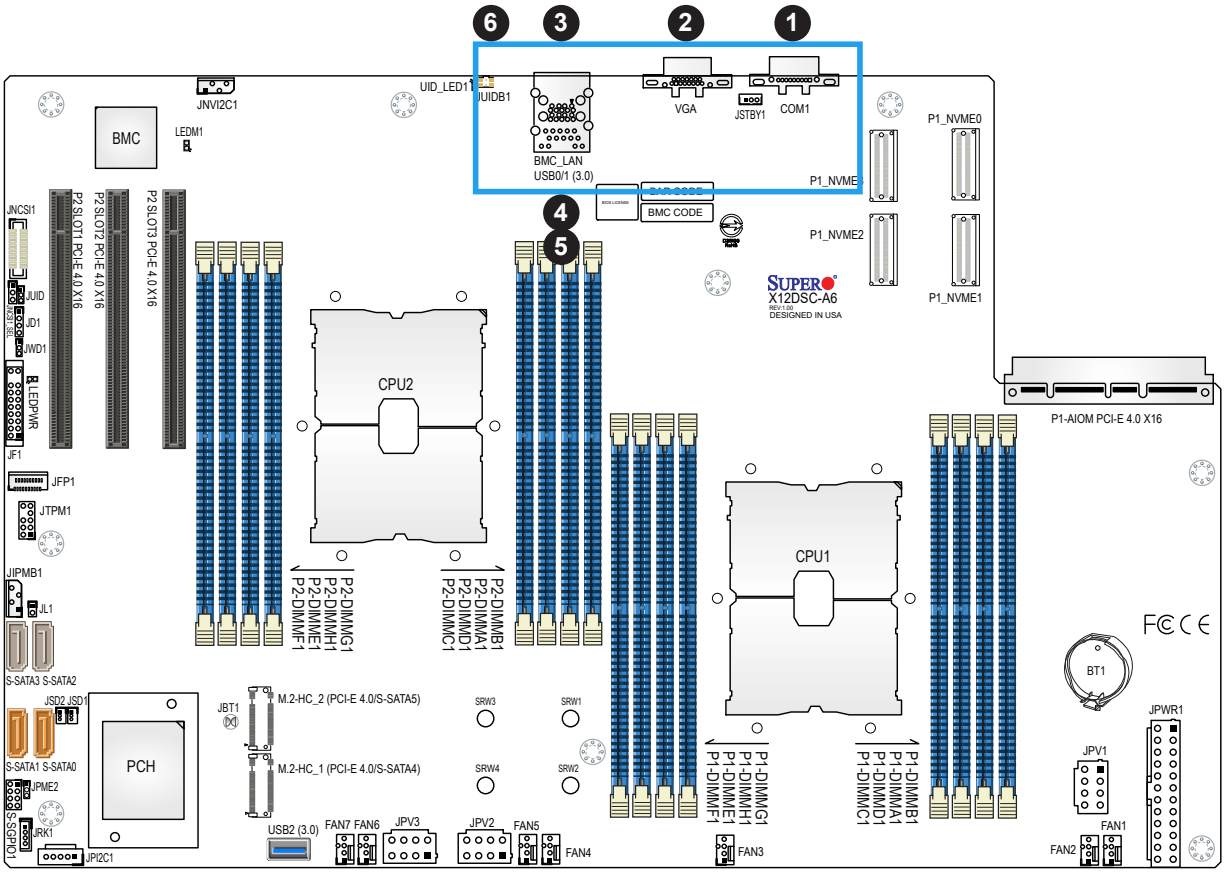
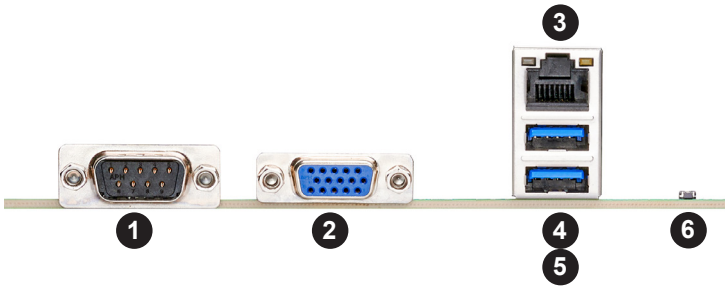


Figure 2-1. I/O Port Locations and Definitions



Rear I/O Ports			
#	Description	#	Description
1	COM Port 1	4	USB0 (3.0)
2	VGA Port	5	USB1 (3.0)
3	Dedicated BMC LAN Port	6	UID Switch / BMC Reset

COM Port

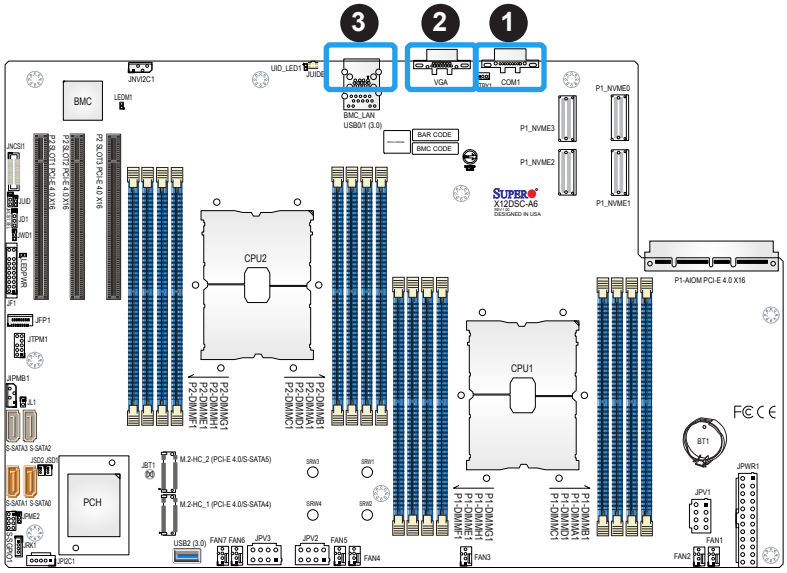
One COM port hat supports serial link interface is on the motherboard. COM1 is located on the rear I/O panel of the motherboard. Refer to the layout below for the location of COM1.

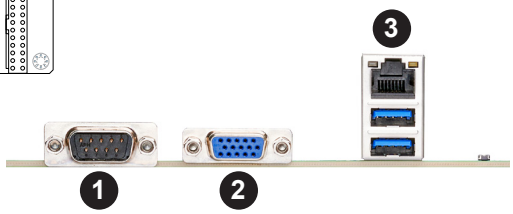
VGA Connections

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

Dedicated BMC LAN Port

One dedicated BMC LAN port (BMC_LAN) is located on the rear I/O panel of the motherboard. The dedicated BMC LAN port, located above the USB0/USB1 ports, provides LAN support for the Baseboard Management Controller (BMC) and accepts RJ45 cables. Refer to Section 2.9 for LAN LED information.





1. COM1 Port
2. VGA Port
3. BMC LAN Port

Universal Serial Bus (USB) Ports and Connector

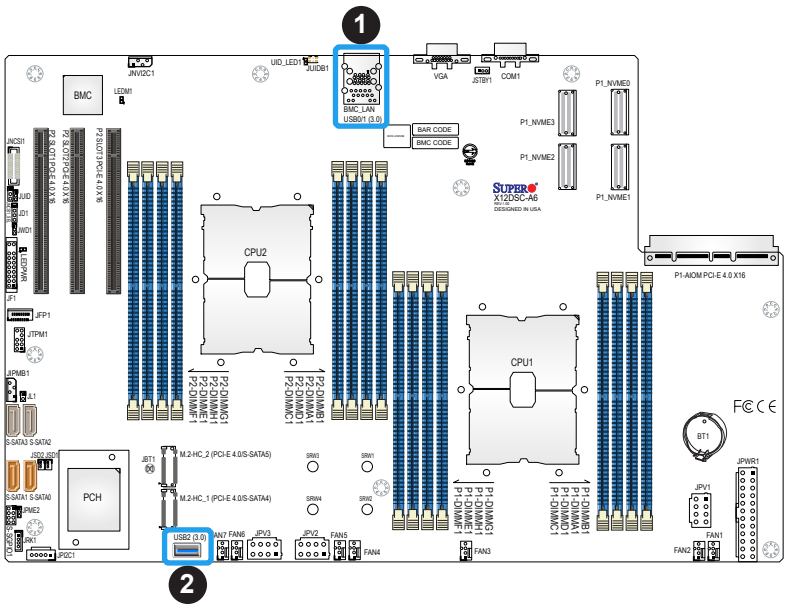
There are two USB 3.0 ports (USB0, USB1) located on the rear I/O panel of the motherboard. One internal USB 3.0 vertical Type-A connector is located at USB2. These USB ports and connector can be used for USB support via USB cables (not included).

Rear I/O Panel USB 3.0 Ports (USB0/USB1) Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS1	10	VBUS2
2	USB2_N_1	11	USB2_N_2
3	USB2_P_1	12	USB2_P_2
4	GND	13	GND
5	USB3_RN_1	14	USB3_RN_2
6	USB3_RP_1	15	USB3_RP_2
7	GND	16	GND
8	USB3_TN_1	17	USB3_TN_2
9	USB3_TP_1	18	USB3_TP_2

Internal Type-A USB 3.0 (USB2) Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	5	SSRX-
2	USB_N	6	SSRX+
3	USB_P	7	GND
4	Ground	8	SSTX-
		9	SSTX+



1. (Rear) USB0/USB1 (3.0)
2. (Internal Type-A) USB2 (3.0)

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

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

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

When functioning as a UID LED switch, JUIDB1 will turn both rear UID LED (UID_LED1) and front UID LED (Pin 7/Pin 8 of JF1) on and off when the user presses the switch on/off.

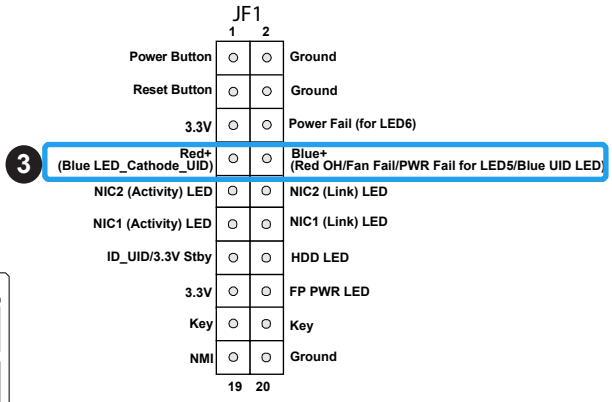
To achieve these dual purposes, the UID LED/BMC Reset switch works in conjunction with the BMC Heartbeat LED (LEDM1) and front/rear UID LEDs. Please note that UID can also be triggered via BMC on the motherboard. For more details on the UID LEDs and BMC LEDs, refer to the tables below. Also, refer to the BMC User's Guide posted on our website at http://www.supermicro.com for more information on BMC.

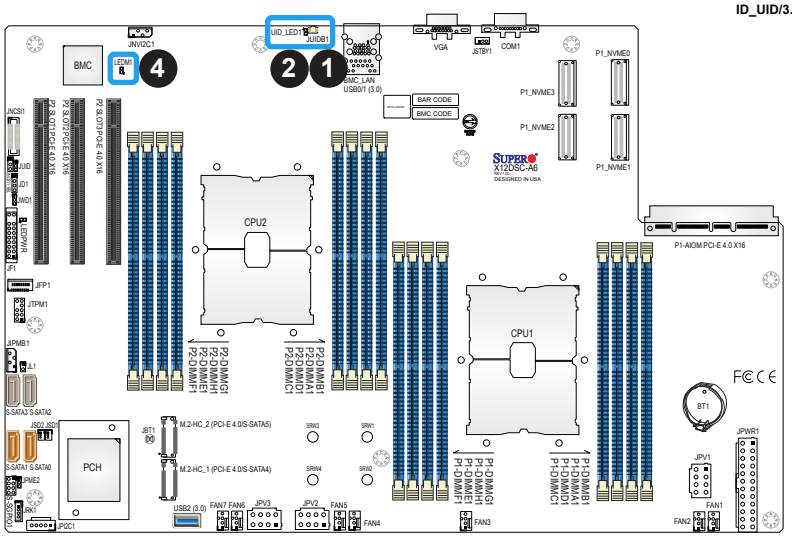
UID/BMC Reset Switch (JUIDB1) Features & Settings

When Used as a UID LED Switch			When Used as a BMC Reset Switch		
Work w/ Rear UID LED (UID_LED1) & Front UID LED (JF1: Pins 7 & 8)			**Work with BMC Heartbeat LED (LEDM1)**		
Rear UID LED	UID_LED1	Blue: Unit identified	BMC Heartbeat LED	LEDM1	Blinking Green: BMC Normal
Front UID LED	Pins 7 & 8 (JF1)	Blue: Unit identified	BMC Reset: Press and hold the switch (JUIDB1) 6 seconds		LEDM1: Solid Green: during reboot
Press the switch (JUIDB1) to turn on and off both rear and front UID LED indicators.					Triggering a cold reboot; LED: solid green on during cold reboot
			BMC Reset: Press and hold the switch (JUIDB1) 12 seconds		LEDM1: Solid Green: during BMC reset
					BMC: Reset to the manufacturer's default; LED solid on during BMC Reset

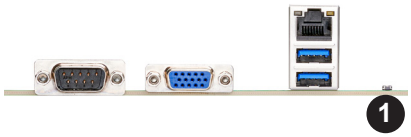
UID/BMC Reset Switch (JUIDB1) Pin Definitions

Pin#	Definition
1	Ground
2	Ground
3	Button In
4	Button In



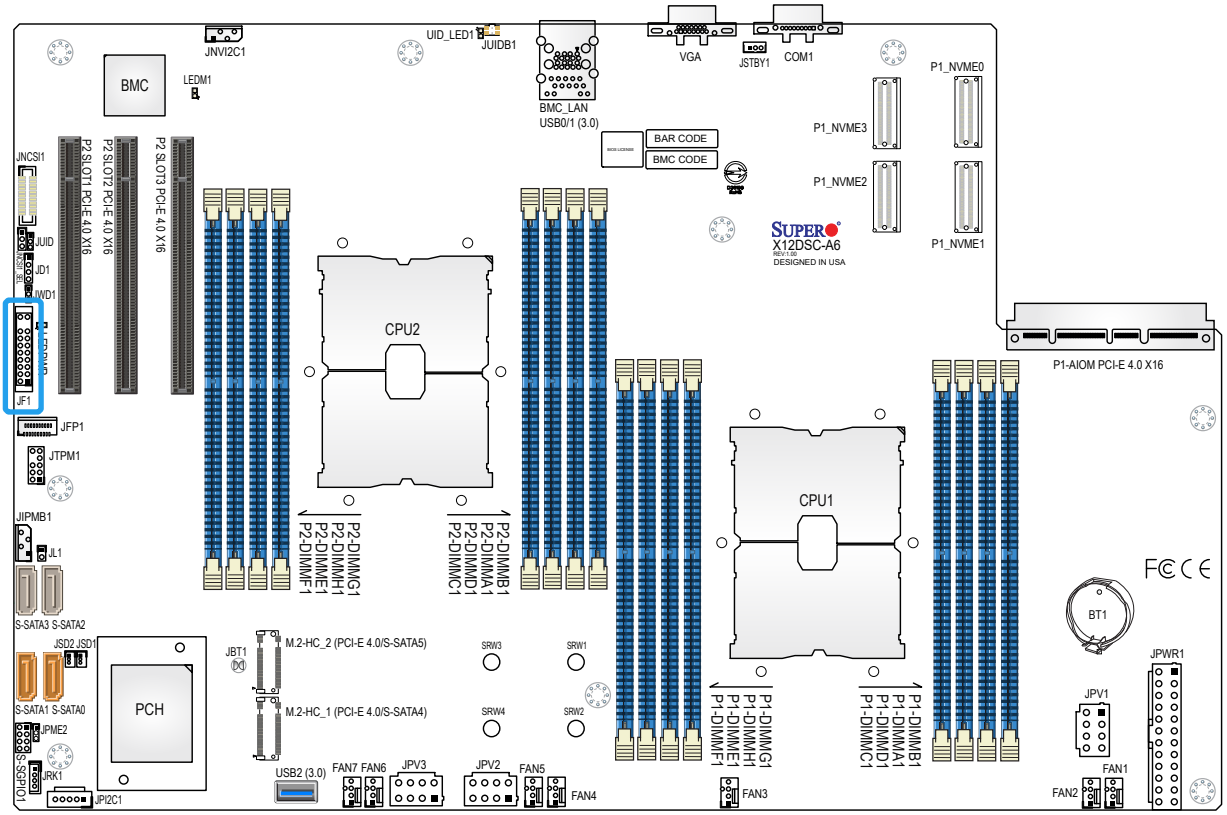


1. UID Switch / BMC Reset
2. Rear UID LED (UID_LED1)
3. Front UID LED
4. BMC Heartbeat LED (LEDM1)



2.6 Front Control Panel

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

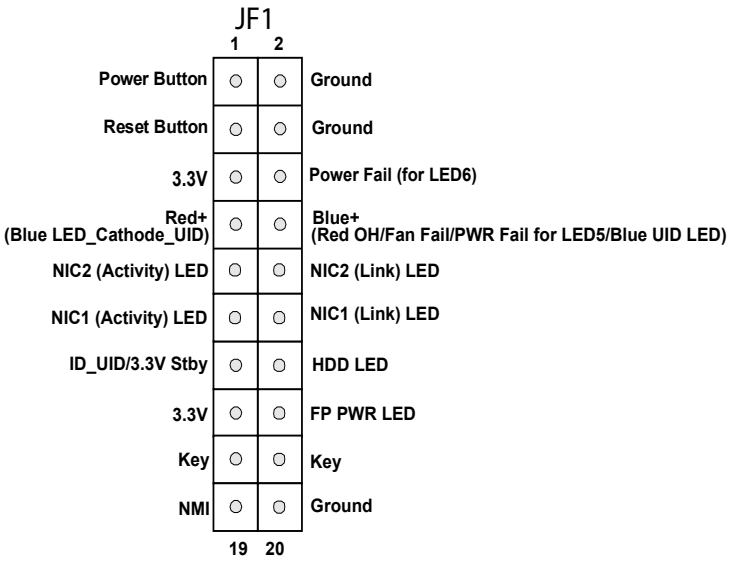


JF1

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

Figure 2-2. JF1 Header Pins

Front Control Panel LEDs



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

Power On & BMC/BIOS Status LED Button

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

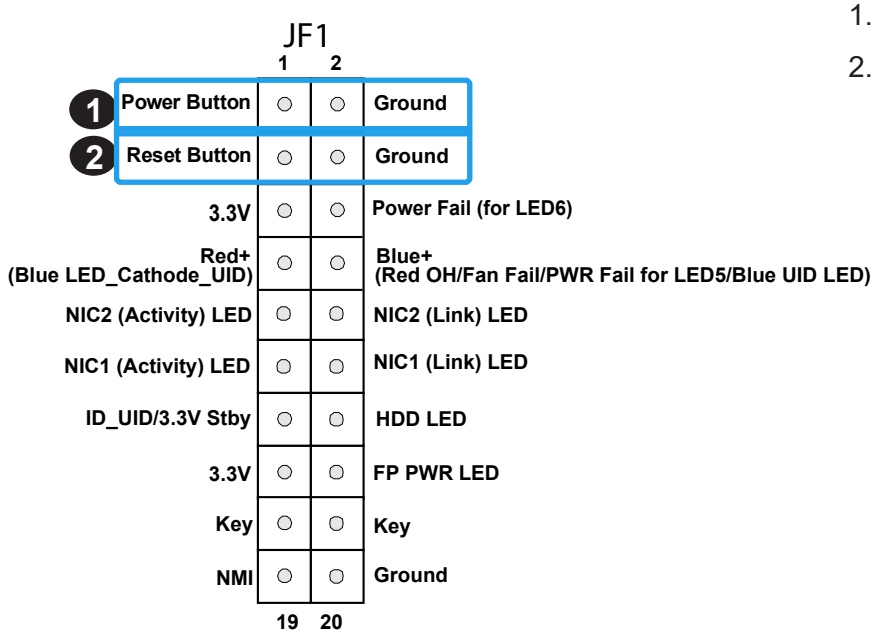
Power Button & BIOS/BMC Status LED Indicator Pin Definitions (JF1)	
Pin#	**Definition**
1	Signal
2	Ground

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

Reset Button

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

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



1. PWR Button
2. Reset Button

Power Fail LED

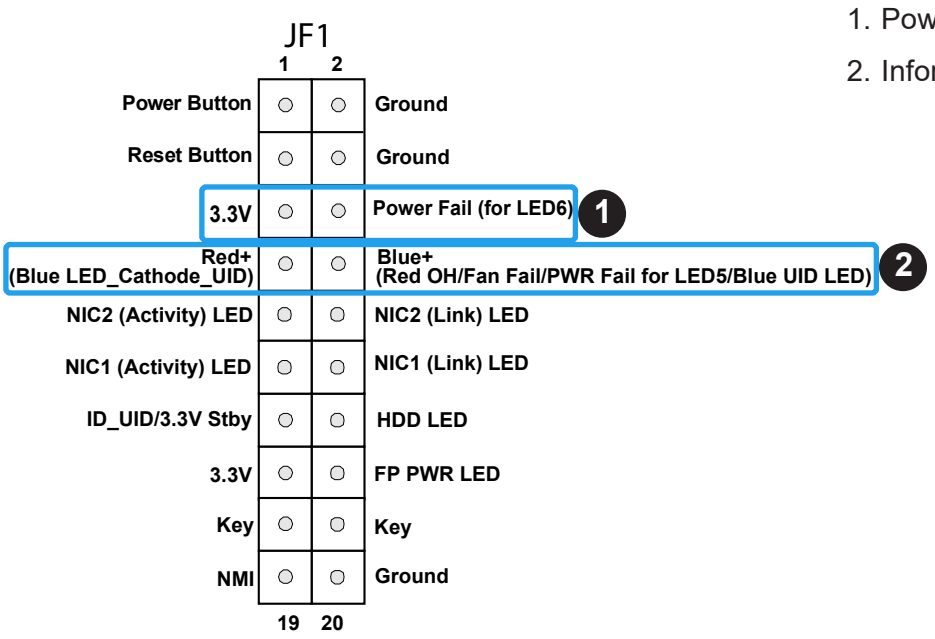
The Power Fail LED connection is located on pins 5 and 6 of JF1. When this LED turns solid red, it indicates a power failure. Refer to the table below for pin definitions.

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

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

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

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



1. Power Fail LED
2. Information LED

NIC1/NIC2 (LAN1/LAN2)

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

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

LAN1/LAN2 LED Pin Definitions (JF1)	
Color	State
NIC 2: Blinking green	LAN 2: Active
NIC 1: Blinking green	LAN 1: Active

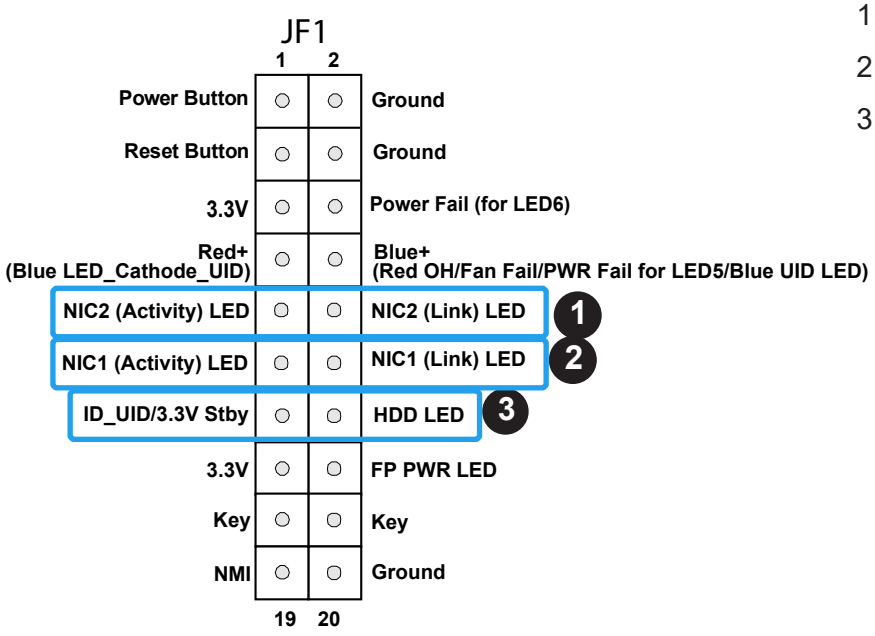
ID_UID Switch/HDD LED

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

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

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

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



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

FP Power LED

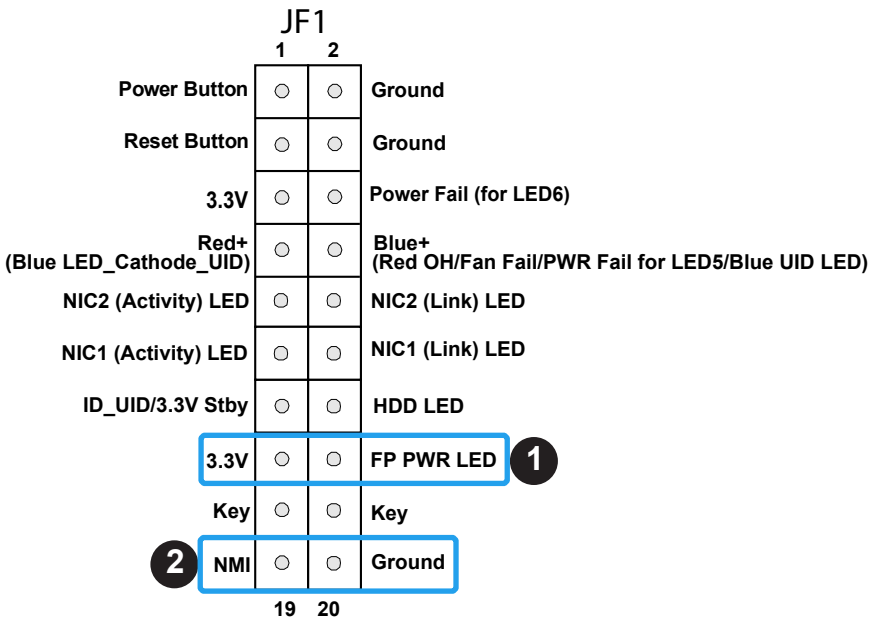
The Front Panel Power LED connection is located on pins 15 and 16 of JF1. Refer to the table below for pin definitions.

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

NMI Button

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

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



1. FP PWR LED
2. NMI

2.7 Connectors

Power Connections

ATX Power Supply Connector

The 24-pin power supply connector (JPWR1) meets the ATX SSI EPS 12V specification. You must also connect the 8-pin 12V DC power connectors (JPV1/JPV2/JPV3) to the power distribution board (PDB) to provide adequate power to your system.

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

ATX Power 24-pin Connector Pin Definitions

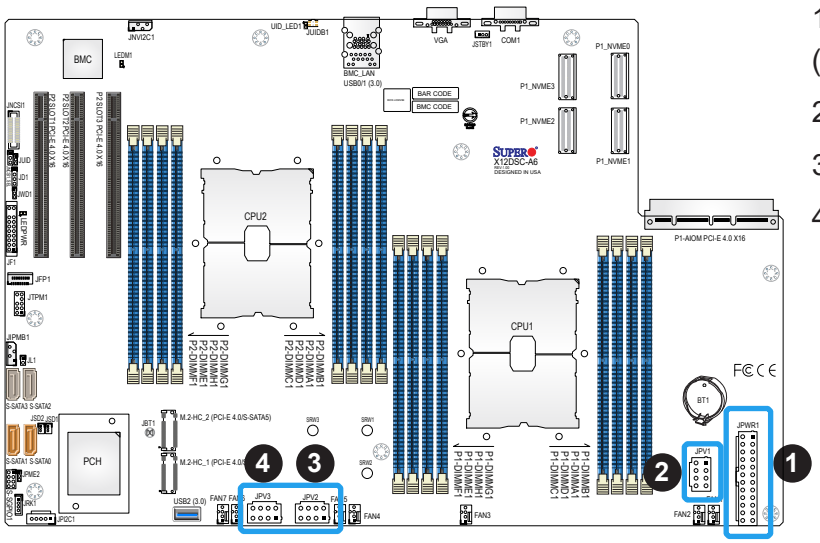
Pin#	Definition	Pin#	Definition
13	+3.3V	1	+3.3V
14	NC	2	+3.3V
15	Ground	3	Ground
16	PS_ON	4	+5V
17	Ground	5	Ground
18	Ground	6	+5V
19	Ground	7	Ground
20	Res (NC)	8	PWR_OK
21	+5V	9	5VSB
22	+5V	10	+12V
23	+5V	11	+12V
24	Ground	12	+3.3V

Required Connection

12V 8-pin Power Pin Definitions

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

Required Connection



1. 24-pin ATX Power Connector (JPWR1)
2. 8-pin Power Connector (JPV1)
3. 8-pin Power Connector (JPV2)
4. 8-pin Power Connector (JPV3)

Headers

Fan Headers

There are seven 4-pin fan headers (FAN1 - FAN7) on the motherboard. All these 4-pin fan headers are backwards compatible with the traditional 3-pin fans. However, fan speed control is available for 4-pin fans only by Thermal Management via the BMC interface. Refer to the table below for pin definitions.

Fan Header Pin Definitions

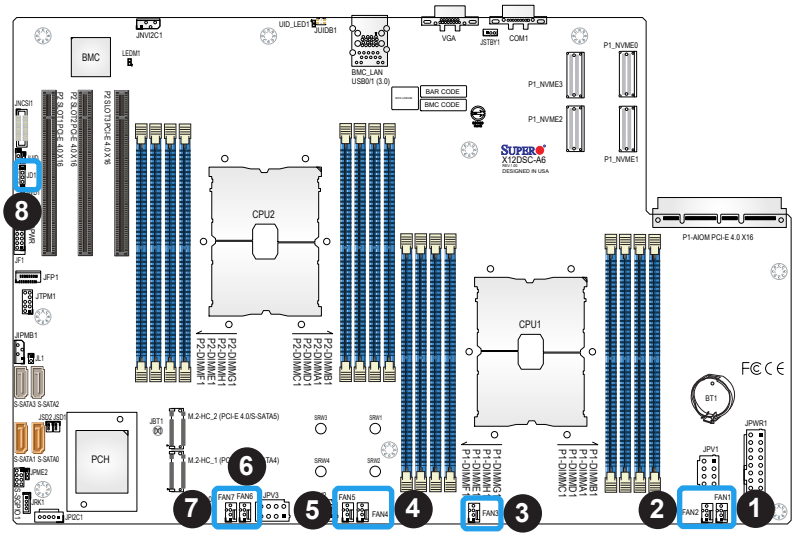
Pin#	Definition
1	Ground
2	2.5A/+12V
3	Tachometer
4	PWM_Control

Speaker Header

A speaker header, located at JD1, can be used in conjunction with an external speaker (optional). Use an appropriate cable to connect this header to an external speaker or buzzer for support of BIOS beep codes and system alarms. Refer to the table below for pin definitions.

Speaker Header Pin Definitions

Pin#	Definition
1	5V
2	No Connection
3	No Connection
4	Speaker

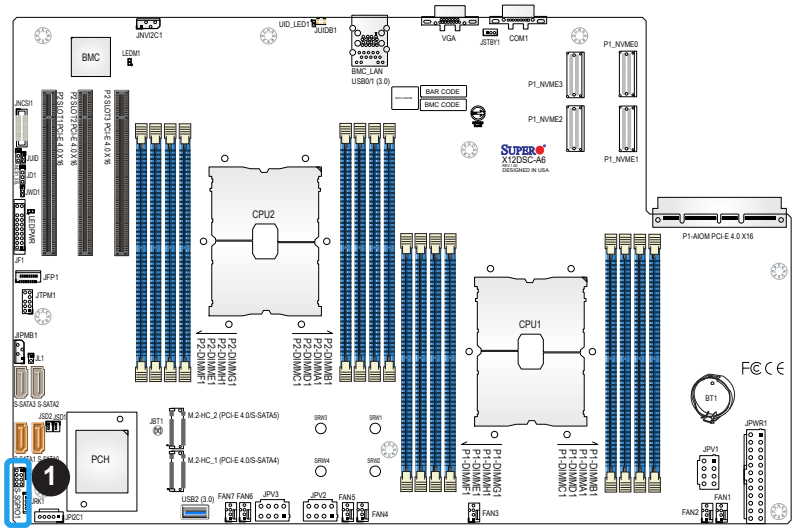


1. FAN1
2. FAN2
3. FAN3
4. FAN4
5. FAN5
6. FAN6
7. FAN7
8. Speaker Header (JD1)

S-SGPIO Header

The S-SGPIO (Serial General Purpose Input/Output) header (S-SGPIO1) is used to communicate with the enclosure management chip on the backplane. Refer to the table below for pin definitions.

S-SGPIO Header Pin Definitions			
Pin#	**Definition**	**Pin#**	**Definition**
1	No Connection	2	No Connection
3	Ground	4	Data
5	Load	6	Ground
7	Clock	8	No Connection



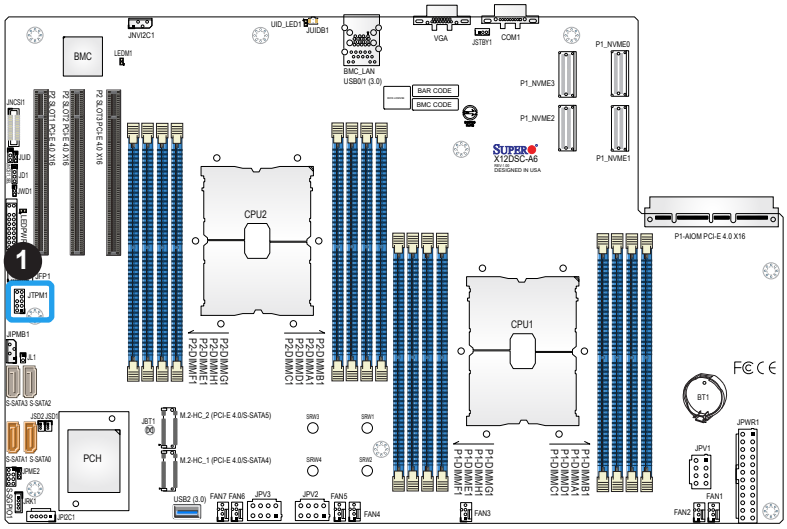
1. S-SGPIO Header (S-SGPIO1)

TPM/Port 80 Header

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

Trusted Platform Module Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	+3.3V	2	SPI_CS#
3	RESET#	4	SPI_MISO
5	SPI_CLK	6	GND
7	SPI_MOSI	8	No Connection
9	+3.3V Stdby	10	SPI_IRQ#

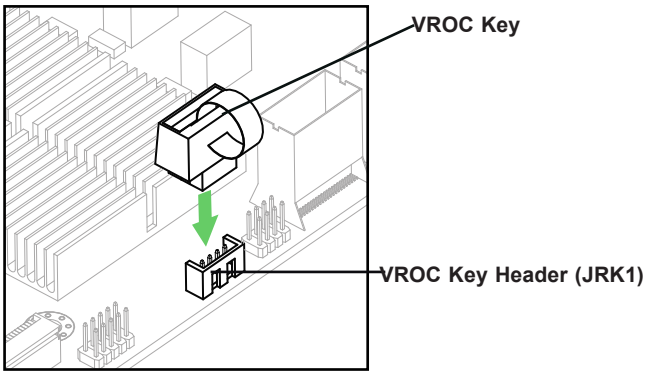


1. TPM/Port 80 Header (JTPM1)

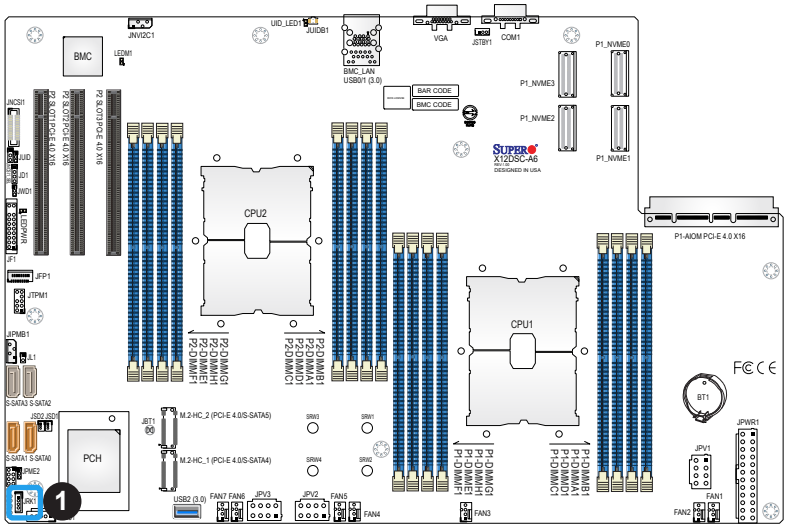
VROC RAID Key Header

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

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



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



1. VROC RAID Key Header (JRK1)

Standby Power

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

Standby Power Pin Definitions

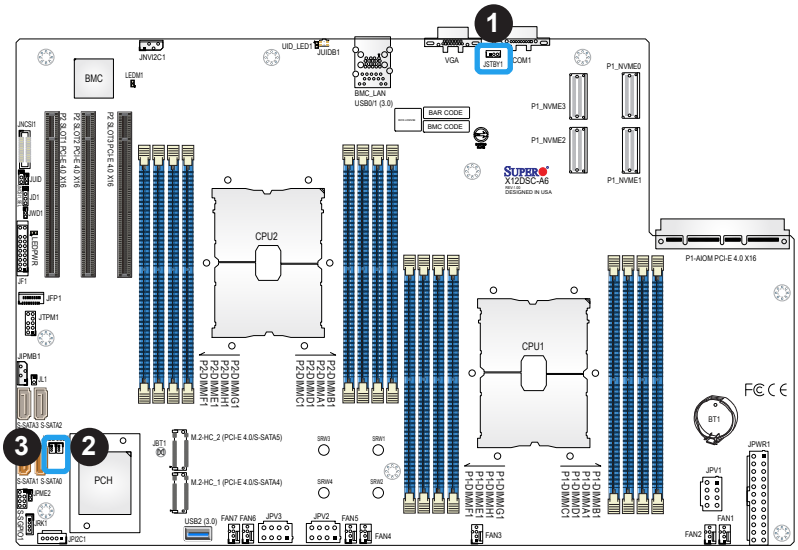
Pin#	Definition
1	+5V Standby
2	Ground
3	No Connection

Disk-On-Module Power Connector

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

DOM Power Pin Definitions

Pin#	Definition
1	5V
2	Ground
3	Ground



1. Standby Power Header (JSTBY1)
2. Disk-On-Module (DOM) Power Connector (JSD1)
3. Disk-On-Module (DOM) Power Connector (JSD2)

Power SMB (I²C) Header

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

Power SMB Header Pin Definitions

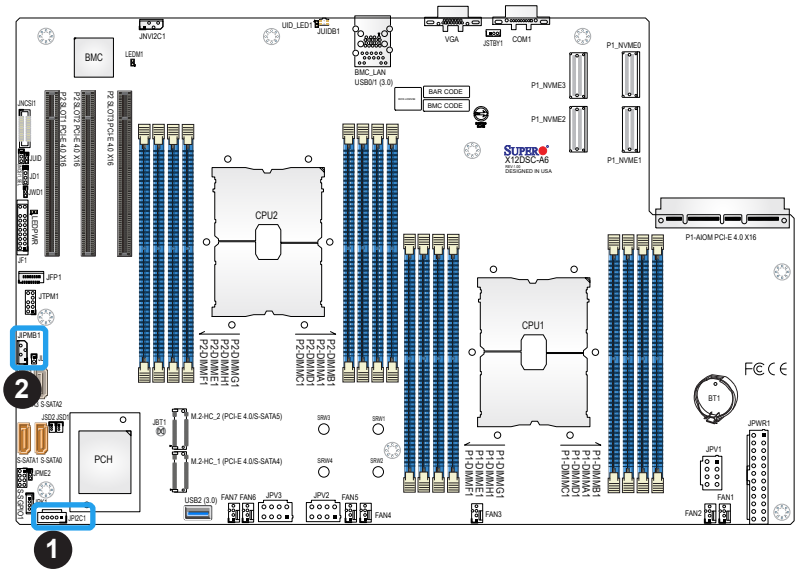
Pin#	Definition
1	Clock
2	Data
3	PMBUS_Alert
4	Ground
5	+3.3V

4-pin BMC External I²C Header

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

External I²C Header Pin Definitions

Pin#	Definition
1	Data
2	Ground
3	Clock
4	No Connection



1. Power SMB Header (JPI2C1)
2. BMC External Header (JIPMB1)

Chassis Intrusion

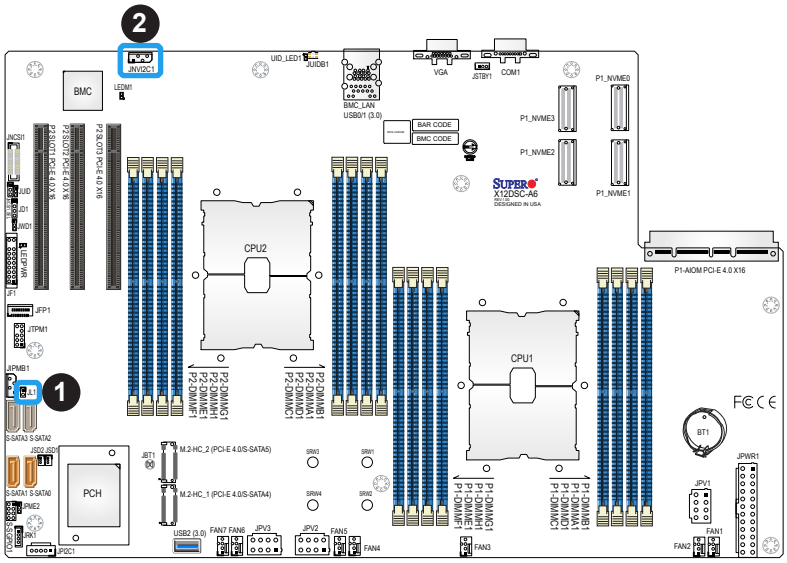
A Chassis Intrusion header is located at JL1 on the motherboard. Attach the appropriate cable from the chassis to inform you when the chassis is opened. Refer to the table below for pin definitions.

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

NVMe SMBus Headers

NVMe SMBus (I²C) header (JNVI2C1), used for PCIe SMBus clock and data connections, provides hot-plug support via a dedicated SMBus interface. This feature is only available for a Supermicro complete system with an SMCI-proprietary NVMe add-on card and a proper cable installed. Refer to the table below for pin definitions.

NVMe SMBus Header Pin Definitions	
Pin#	**Definition**
1	Data
2	Ground
3	Clock
4	+3.3V



1. Chassis Intrusion Header (JL1)
2. NVMe I²C Header (JNVI2C1)

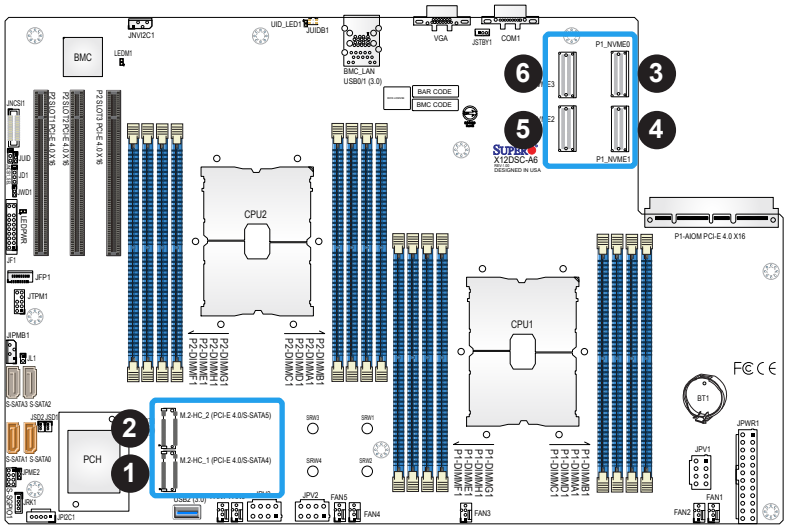
PCI-E 4.0/S-SATA Hybrid M.2 Slots

The X12DSC-A6 motherboard has two PCIe 4.0/S-SATA hybrid M.2 slots (M.2-HC_1/S-SATA4, M.2-HC_2/S-SATA5). M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. The M.2 slots on the motherboard support PCIe 4.0 x4 M.2 NVMe SSDs or SATA 3.0 SSDs in the 2280 and 22110 form factors.

SlimSAS NVMe Connectors

Four SlimSAS NVMe connectors (P1_NVME0 - P1_NVME3) provide eight NVMe U.2 connections. Use these NVMe connections to attach high-speed PCIe storage devices.

Note: When installing an NVMe device on a motherboard, please be sure to connect the first NVMe port (P1_NVME0) first for your system to work properly.



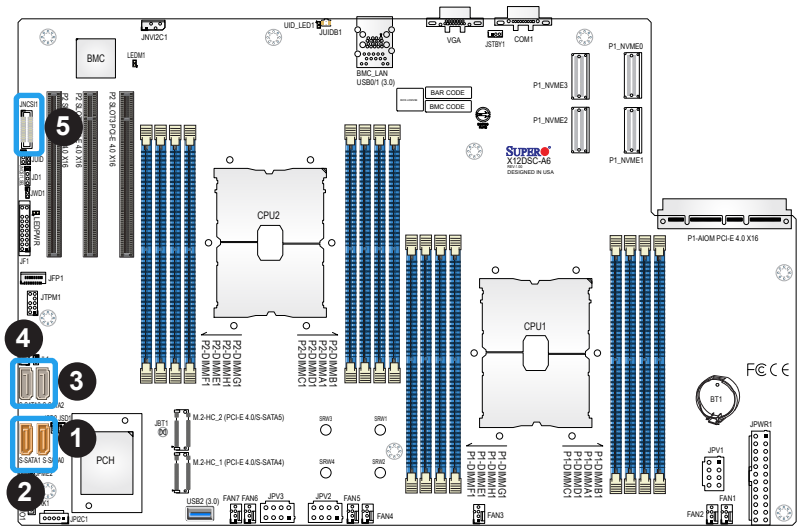
1. M.2 Slot (M.2-HC_1 PCI-E 4.0/S-SATA4)
2. M.2 Slot (M.2-HC_2 PCI-E 4.0/S-SATA5)
3. P1_NVME0
4. P1_NVME1
5. P1_NVME2
6. P1_NVME3

S-SATA 3.0 Ports

The X12DSC-A6 has four S-SATA 3.0 ports (S-SATA0 - S-SATA3) on the motherboard. These SATA ports are supported by the C621A chipset. S-SATA0 and S-SATA1 can be used with Supermicro SuperDOMs, which are orange SATA DOM connectors with power pins built in and do not require external power cables. S-SATA0 and S-SATA-1 are compatible with regular SATA HDDs or SATA DOMs that need external power cables.

NCSI Connector

The NCSI connector (JNCSI1) is used to connect a Network Interface Card (NIC) to the motherboard which allows the onboard BMC (Baseboard Management Controller) to communicate with a network.



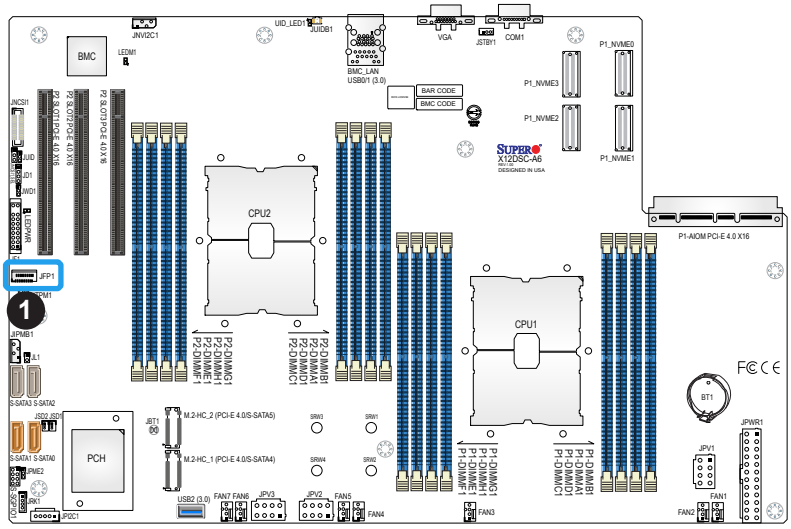
1. S-SATA0
2. S-SATA1
3. S-SATA2
4. S-SATA3
5. NCSI Connector (JNCSI1)

Front Control Panel Header for FFC/FPC Cable

JFP1 contains header pins for various buttons and indicators that are normally located on a control panel at the front of the chassis. These connectors are designed specifically for use with Supermicro chassis. Refer to the table below for pin definitions of JFP1. Regarding the pin functions, refer to Section 2.6. (JFP1 and JF1 have the same pin functions although the pin numbers might differ.)

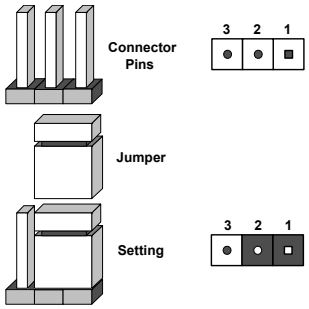
Front Control Panel Header for FFC/FPC Cable Pin Definitions

Pin#	Definition
20	Ground
19	Power Fail
18	+5V
17	+5V
16	+5V
15	+3.3 Pull Up
14	Ground
13	FP Sensor Clock
12	FP Sensor DATA
11	Ground
10	+3.3VSB
9	FP PWR LED
8	STBY LED
7	HDD LED
6	NIC1 (Link) LED
5	No Connection
4	Blue+(Red OH/Fan Fail/PWR Fail for LED5/Blue UID LED)
3	Red+(Blue LED_Cathode_UID)
2	Reset or UID Button
1	Power Button



1. Front Control Panel Header for FFC/FPC Cable (JFP1)

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 on the right 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.

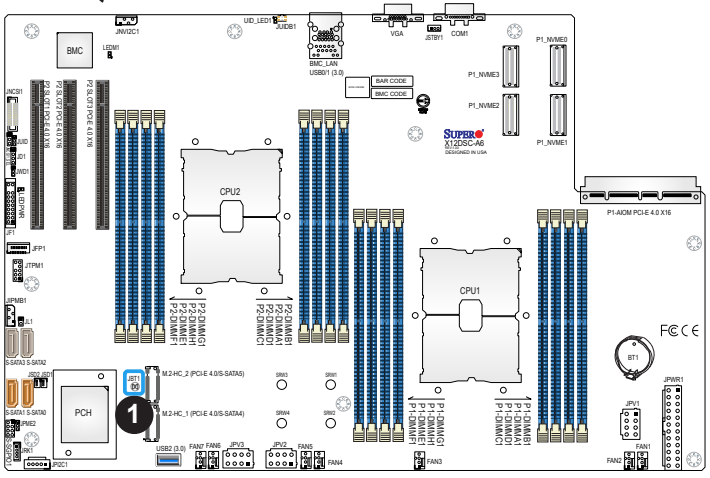
CMOS Clear

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

Note: Clearing CMOS will also clear all passwords.



1. JBT1

BMC NC-SI Connection

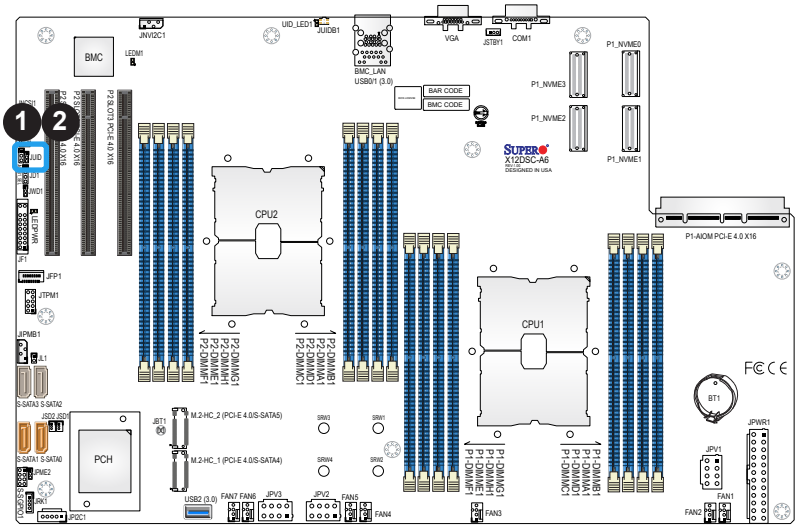
This jumper (JNCSI1_SEL) allows you to set the BMC NC-SI connection. Close pins 1 and 2 of JNCSI1_SEL to set the BMC NC-SI connection to the AIOM slot (P1-AIOM). Close pins 2 and 3 of JNCSI1_SEL to set the BMC NC-SI connection to the NC-SI connector (JNCSI1) for BMC shared LAN. Refer to the table below for jumper settings.

BMC NC-SI Connection Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	AIOM (Default)
Pins 2-3	JNCSI1

UID Enable/System Reset

This jumper (JUID) is used to select one of JFP1 pin 2 functions (refer to page 63 for pin definitions of JFP1). Close pins 1 and 2 of JUID to enable onboard UID support. Close pins 2 and 3 of JUID to reset your system. Refer to the table below for jumper settings.

UID Enable/System Reset Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	UID Enabled
Pins 2-3	System Reset (Default)



1. BMC NC-SI Connection (JNCSI1_SEL)
2. UID Enable/System Reset (JUID)

ME Recovery

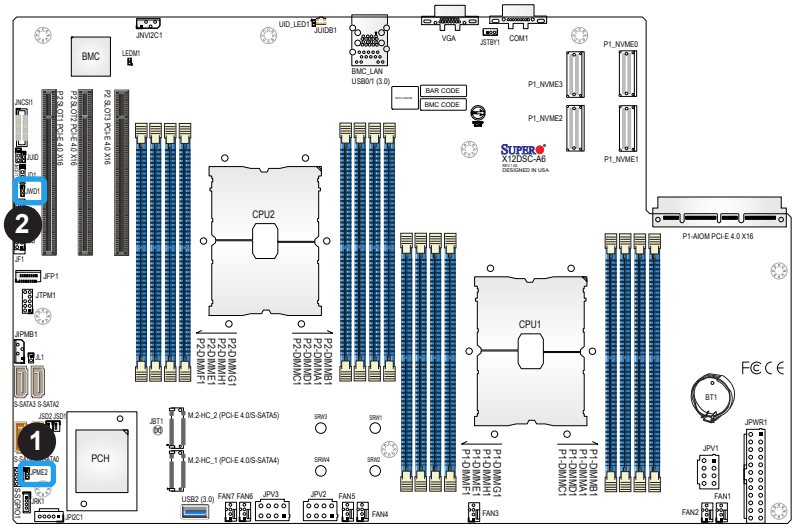
JPME2 is used for ME Firmware Recovery mode, which will limit system resource for essential function use only without putting restrictions on power use. In the single operation mode, online upgrade will be available via Recovery mode. Refer to the table below for jumper settings.

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

Watchdog

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

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



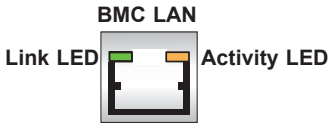
1. ME Manufacturing Recovery (JPME2)
2. Watchdog (JWD1)

2.9 LED Indicators

BMC LAN LEDs

The BMC LAN port is located on the rear I/O panel. The LED on the right indicates activity, while the LED on the left indicates the speed of the connection. Refer to the table below for more information.

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

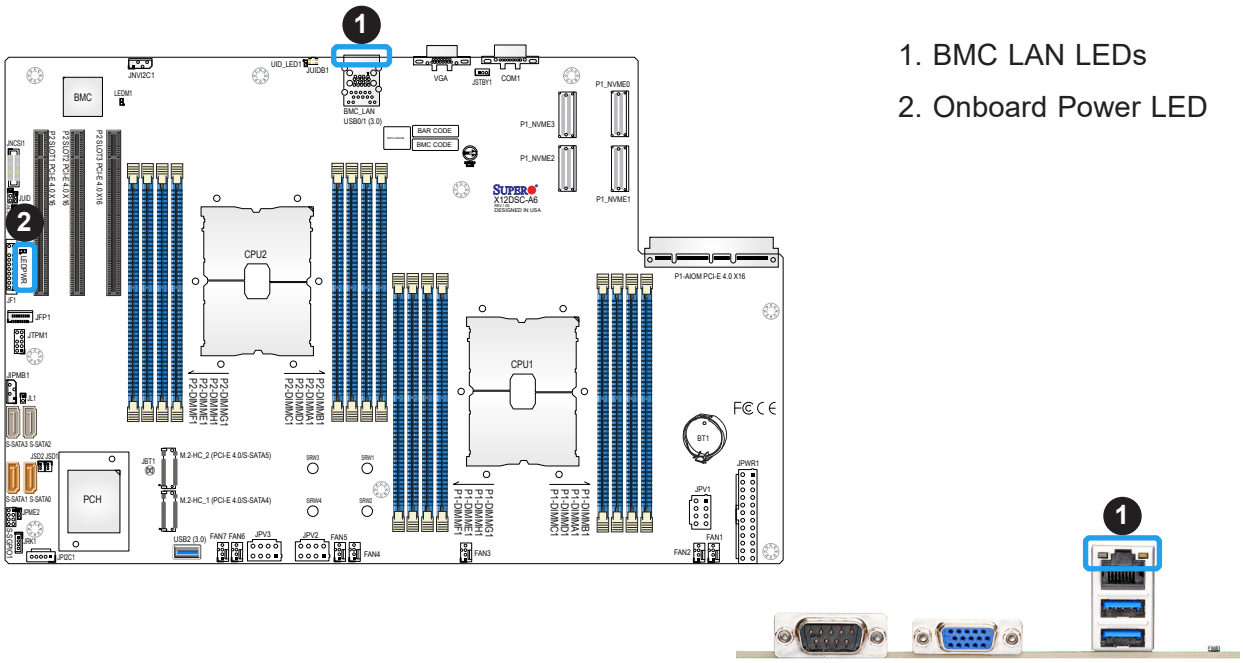


Onboard Power LED

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

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

Note: For information on UID LED Indicators (UID_LED1) and BMC Heartbeat LED Indicator (LEDM1), please refer to page 46.



1. BMC LAN LEDs
2. Onboard Power 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 power connectors are properly connected to the power distribution board (PDB).
3. Check that the 115V/230V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. The battery on your motherboard may be old. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.

No Video

1. Make sure that your peripherals or devices function normally.
2. If you see no any video in power on mode, please turn off the system, then remove all add-on cards and cables. Check if the system can be powered on.

System Boot Failure

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

1. Remove all components from the motherboard, especially the DIMM modules.
2. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this chapter.

Memory Errors

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)
2. Check if all memory modules are populated with same type and speed.
3. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.

Losing the System's Setup Configuration

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

When the System Becomes Unstable

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

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

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

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

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

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

5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Please refer to our website for more information on the minimum power requirements.

6. Proper software support: Make sure that the correct drivers are used.

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

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as USB flash drives, USB HDD, USB CD/DVD.

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

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

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

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

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

3.2 Technical Support Procedures

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

1. Please go through the Troubleshooting Procedures and Frequently Asked Questions (FAQ) sections in this chapter or see the FAQs on our website (http://www.supermicro.com/FAQ/index.php) before contacting Technical Support.
2. BIOS upgrades can be downloaded from our website (http://www.supermicro.com/ResourceApps/BIOS_BMC_Intel.html).
3. If you still cannot resolve the problem, include the following information when contacting Supermicro for technical support:

- Motherboard model, motherboard serial number, and PCB revision number
- BIOS release date/version (This can be seen on the initial display when your system first boots up.)
- System configuration

4. An example of a Technical Support form is on our website at http://www.supermicro.com/RmaForm/.
5. Distributors: For immediate assistance, please have your account number ready when placing a call to our Technical Support department. We can be reached by email at support@supermicro.com.

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: This motherboard supports up to 4 TB of 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 (288-pin) ECC memory with speeds of 3200/2933/2666 MHz in 16 slots and up to 4 TB of Intel Optane PMem 200 Series with speeds of up to 3200 MHz. To enhance memory performance, do not mix memory modules of different speeds and sizes. Please follow all memory installation instructions given in Section 2.4.

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

Question: How do I update my BIOS?

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

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

To update your BIOS under UEFI Shell

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

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

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

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

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

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

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

a. If a different FDT is found

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

b. If the FDT is the same

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

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

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

3.4 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

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

Proper Battery Disposal

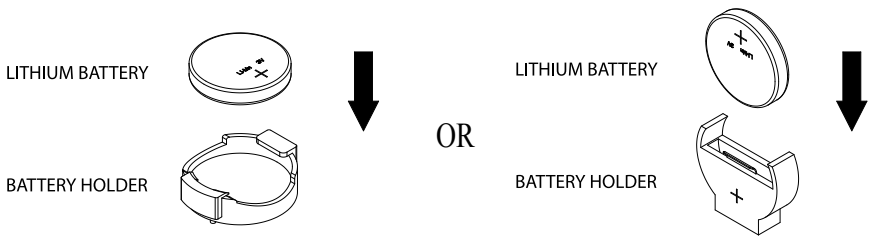
Warning: Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management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

Battery Installation

To install an onboard battery, follow the steps below:

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

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



3.5 Returning Merchandise for Service

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

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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

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

Starting the Setup Utility

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

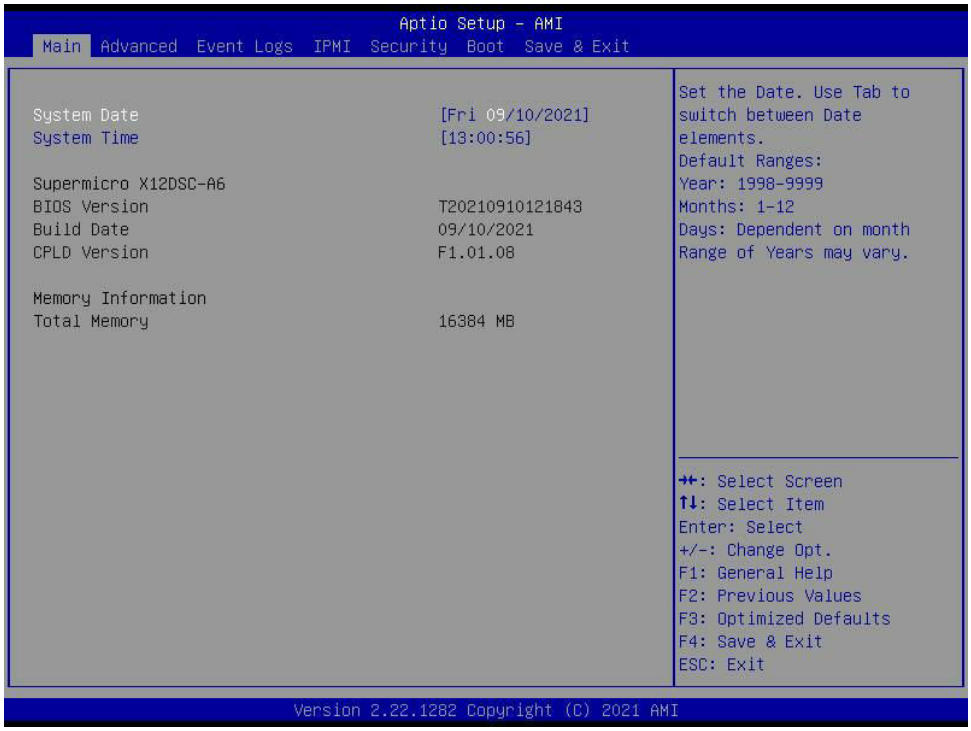
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

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

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

4.2 Main Setup

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



System Date/System Time

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

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

Supermicro X12DSC-A6

BIOS Version

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

Build Date

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

CPLD Version

This feature displays the Complex Programmable Logic Device version.

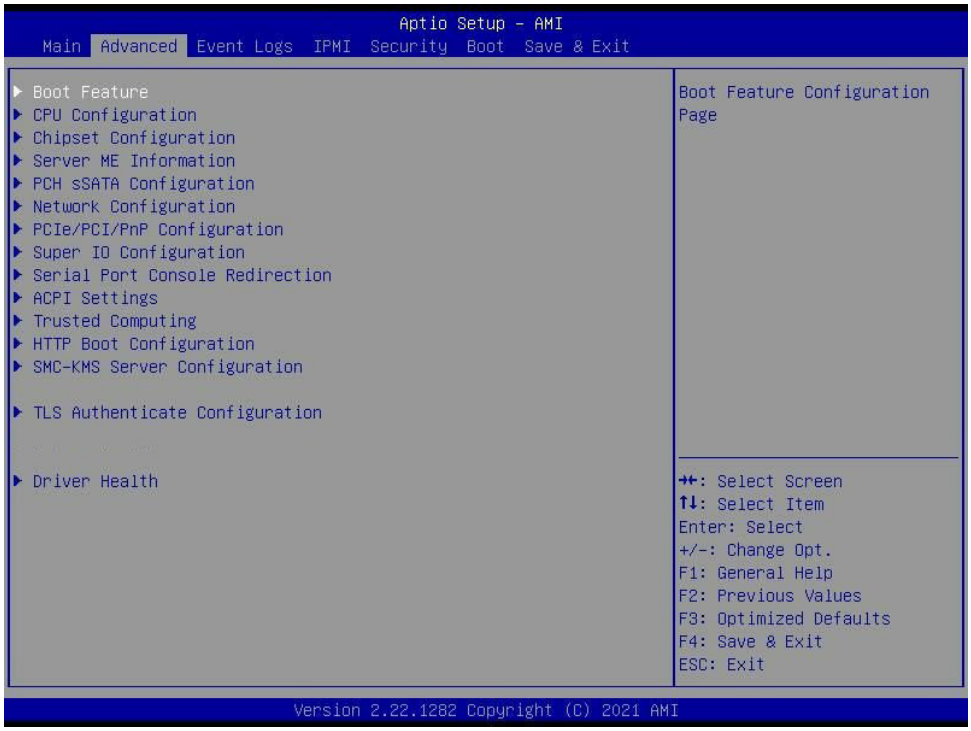
Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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



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

▶Boot Feature

Quiet Boot

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

Option ROM Messages

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

Bootup NumLock State

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

Wait For "F1" If Error

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

INT19 (Interrupt 19) Trap Response

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

Re-try Boot

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

Power Configuration

Watch Dog Function

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

Restore on AC Power Loss

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

Power Button Function

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

▶CPU Configuration

The following CPU information will display:

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

▶CPU1 Core Disable Bitmap

CPU1 Core Disable Bitmap

Available Bitmap:

This feature displays the available bitmap.

Core Disable Bitmap(Hex)

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

CPU2 Core Disable Bitmap

Available Bitmap:

This feature displays the available bitmap.

Core Disable Bitmap(Hex)

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

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

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

Hardware Prefetcher (Available when supported by the CPU)

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

Adjacent Cache Prefetch (Available when supported by the CPU)

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

DCU Streamer Prefetcher (Available when supported by the CPU)

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

DCU IP Prefetcher (Available when supported by the CPU)

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

LLC Prefetch

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

Extended APIC (Extended Advanced Programmable Interrupt Controller)

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

VMX

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

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

Enable SMX

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

PPIN Control

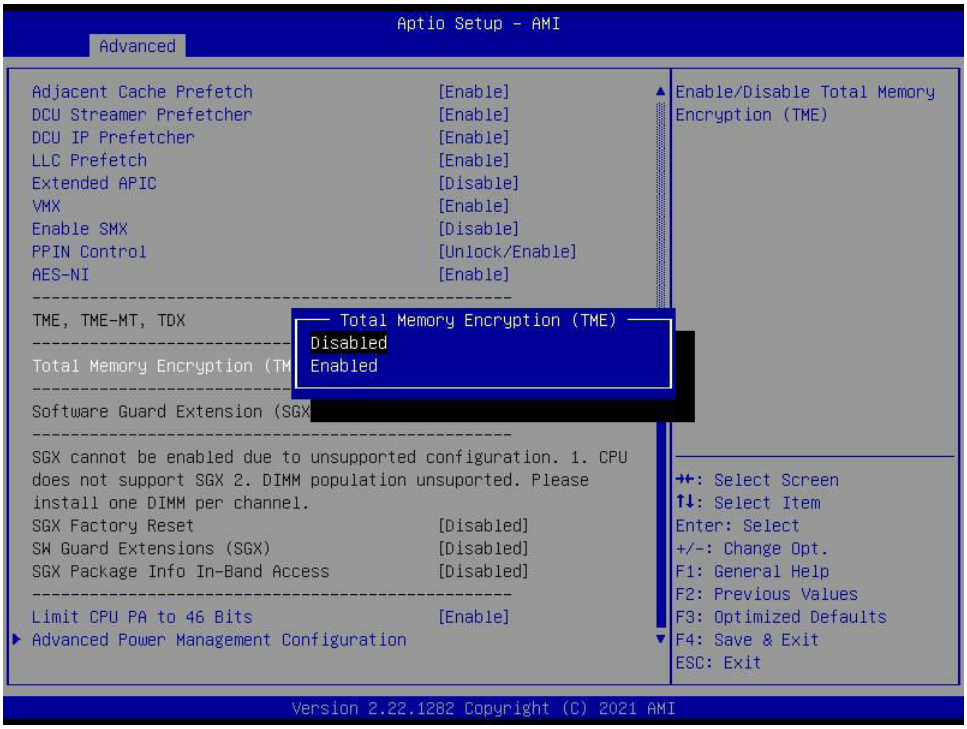
Select Unlock/Enable to use the Protected-Processor Inventory Number (PPIN) in the system. The options are Lock/Disable and **Unlock/Enable**.

AES-NI

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

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

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



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

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

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

This feature displays the maximum TME-MT keys.

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

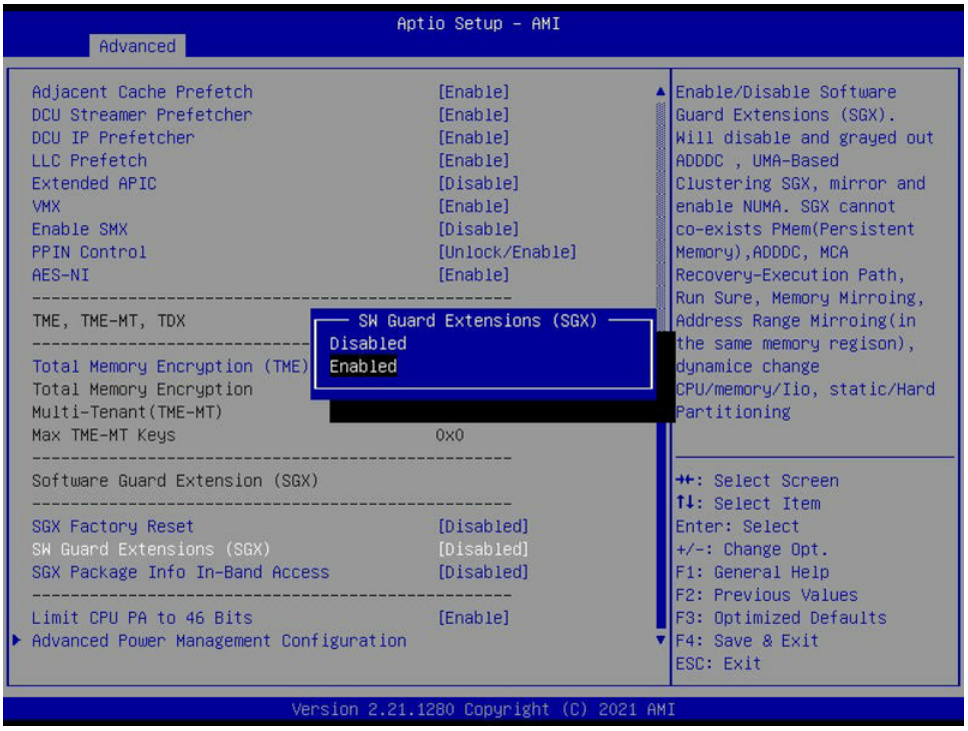
Note: Each memory channel must have at least one DIMM populated on the motherboard to support the Intel SGX feature.

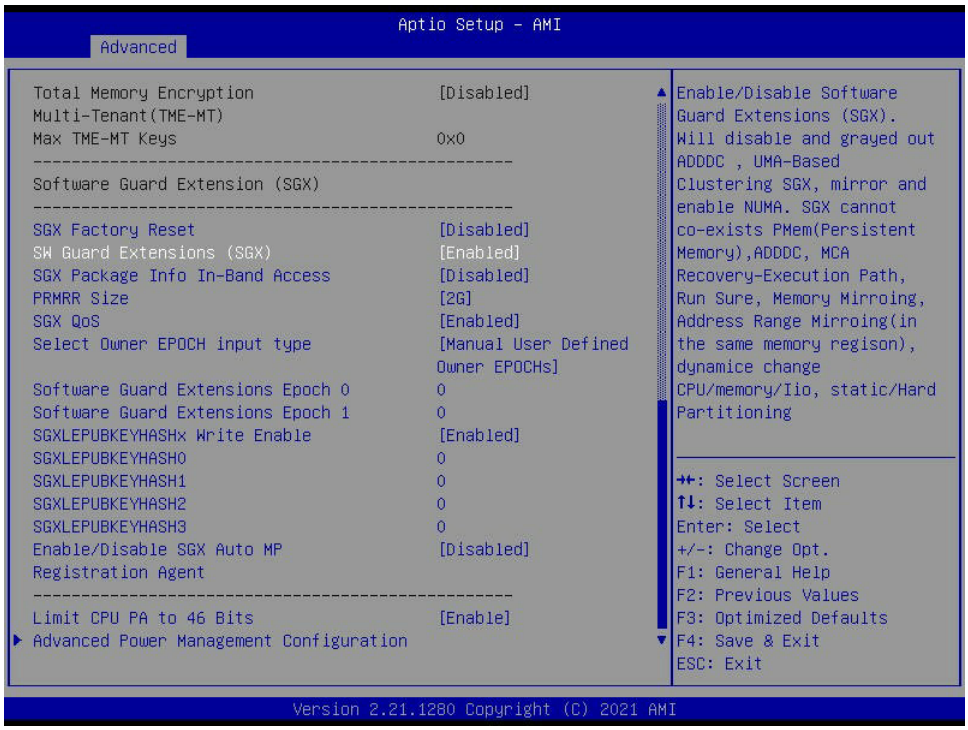
SGX Factory Reset

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

SW Guard Extensions (SGX)

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





SGX Package Info In-Band Access

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

PRMRR Size

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

SGX QoS

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

Select Owner EPOCH input type

Owner EPOCH is used as a parameter to allow the owner to add entropy to the keys during the derivation. Use this feature to select the two Owner EPOCH modes. One is New Random Owner EPOCH , the other is manually entered by the user. Each EPOCH is 64-bit. The options are Change to New Random Owner EPOCHs and **Manual User Defined Owner EPOCHs**.

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

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

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

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

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

SGXLEPUBKEYHASHx Write Enable

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

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

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

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

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

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

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

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

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

Enable/Disable SGX Auto MP Registration Agent

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

Limit CPU PA to 46 bits

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

▶Advanced Power Management Configuration

Power Technology

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

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

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

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

Use this feature to configure the proper operation setting for your machine to achieve the desired system performance level and energy saving (efficiency) level at the same time. Selecting Performance can enhance system performance but may consume more power as energy is needed to fuel the processors for operation. The options are Maximum Performance, Performance, **Balanced Performance,** Balanced Power, and Power.

▶CPU P State Control

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

SpeedStep (P-States)

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

AVX P1

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

Dynamic SST-PP (Speed Select Technology-Performance Profile)

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

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

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

Activate SST-BF (Speed Select Technology-Base Frequency)

Select Enable for Intel Speed Select Technology-Base Frequency support. The options are **Disable** and Enable.

Configure SST-BF (Speed Select Technology-Base Frequency)

When this feature is set to Enable, the system BIOS will configure SST-BF High Priority Core settings so that system software does not have to configure these settings. The options are **Enable** and Disable.

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

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

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

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

CPU Flex Ratio Override (Available when supported by the CPU installed on the motherboard)

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

CPU Core Flex Ratio (Available when supported by the CPU installed on the motherboard and when "CPU Flex Ratio Override" is set to Enable)

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

▶Hardware PM State Control

Hardware P-States

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

▶Frequency Prioritization

RAPL (Running Average Power Limit) Prioritization

Select Enable to prioritize RAPL (Running Average Power Limit) which sets the power consumption limit for a processor to save energy. The options are Enable and **Disable**.

▶CPU C State Control

Enable Monitor MWAIT

Select Enable to support Monitor and Mwait, which are two instructions in Streaming SIMD Extension 3 (SSE3), to improve synchronization between multiple threads for CPU performance enhancement. The options are Disable 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 enable "Enhanced Halt State" support, which will significantly reduce the CPU's power consumption by minimizing CPU's clock cycles and reduce voltage during a "Halt State". The options are Disable and **Enable**.

▶Package C State Control

Package C State

Use this feature to optimize and reduce CPU package power consumption in the idle mode. Please note that the changes you've made in this setting will affect all CPU cores or the circuits of the entire system. The options are C0/C1 state, C2 state, C6 (non Retention) state, and **Auto**.

▶CPU T State Control (Available when "Power Technology" is set to Custom)

Software Controlled T-States

If this feature is set to Enable, CPU throttling will be controlled by the OS, which will reduce the speed of CPU. The options are **Disable** and Enable.

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

Select any percentage (%) from the option list to configure the on-die thermal throttling setting. 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

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

▶Uncore Configuration

The following information will display:

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

Degrade Precedence

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

Link L0p Enable

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

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

Link L1 Enable

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

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

XPT Remote Prefetch

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

KTI Prefetch

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

Local/Remote Threshold

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

IO Directory Cache (IODC)

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

SNC (Sub NUMA)

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

XPT Prefetch

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

Snoop Throttle Configuration

Use this feature to set the level of snoop throttle for the PCH, which will determine how much speed to decrease in operation when the system is in the snoop state. The options are Disabled, Low, Medium, High, and **Auto**.

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

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

Stale AtoS (A to S)

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

LLC Dead Line Alloc

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

▶Memory Configuration

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

Enhanced PPR

Use this feature to enable or disable Enhanced PPR function. The options are **Disable** and Enable.

Operation Mode (Available when "Enhanced PPR" is set to Enable)

Use this feature to set Operation Mode. The options are Test Only and **Test and Repair**.

Enforce POR (Plan of Record)

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

PPR Type

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

Memory Frequency

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

Data Scrambling for DDR4

Select Enable to enable data scrambling for Intel Optane Persistent Memory (PMem) modules to enhance memory data security. Select Auto to use the Memory Reference Code (MRC) defaulting setting for PMem memory data scrambling. The options are Disable and **Enable**.

2x Refresh Enable

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

▶Memory Topology

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

▶Memory RAS Configuration

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

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

Pcode, a register transfer language designed for reverse engineering, translates individual processor instructions into a sequence of Pcode operations in order to facilitate

the construction of data-flow graphs and dissembling of processor instructions for machine application. Select Enabled to allow Pcode to work around the SAI group policy to achieve a solution with a next-step instruction. The options are **Disabled** and Enabled.

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

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

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

Select Enabled to mimic behavior of UEFI-based ARM (Address Range Mirror) with setup options to increase memory security, but it will reduce the memory capacity into half. 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 **512**.

Partial Cache Line Sparing PCLS

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

ADDDC Sparing

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

Patrol Scrub

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

▶IIO Configuration

▶CPU1 Configuration

IOU0 (II0 PCIe Port 1)

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

IOU1 (II0 PCIe Port 2)

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

IOU3 (II0 PCIe Port 4)

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

IOU4 (II0 PCIe Port 5)

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

▶P1_AIOM PCI-E 4.0 X16 / P1_NVME0 / P1_NVME1 / P1_NVME2 / P1_NVME3 / P1_NVME4 / P1_NVME5 / P1_NVME6 / P1_NVME7 / M.2-HC_1 / M.2-HC_2

Link Speed

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

The following information will also display:

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

PCI-E Port Max (Maximum) Payload Size

Use this feature to set the maximum payload size support in the PCIe Device Capabilities Register for the device installed in the PCIe port. The options are 128B, 256B, 512B, and **Auto.**

▶CPU2 Configuration

IOU0 (II0 PCIe Port 1)

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

IOU1 (II0 PCIe Port 2)

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

IOU3 (II0 PCIe Port 4)

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

IOU4 (II0 PCIe Port 5)

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

▶P2 SLOT1 PCI-E 4.0 X16 / P2 SLOT2 PCI-E 4.0 X16 / P2 SLOT3 PCI-E 4.0 X16

Link Speed

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

The following information will also be displayed:

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

PCI-E Port Max Payload Size

Use this feature to set the maximum payload size support in the PCIe Device Capabilities Register for the device installed in the DMI port. The options are 128B, 256B, 512B, and **Auto.**

▶IOAT Configuration

Disable TPH

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

Prioritize TPH

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

Relaxed Ordering

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

▶Intel® VT for Directed I/O (VT-d)

Intel® VT for Directed I/O (VT-d)

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

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

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

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

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

▶Intel® VMD Technology

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

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

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

NVMe Mode Switch

When this feature is set to Auto, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are Manual, VMD, and **Auto**.

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

VMD Config for PCH ports

Enable/Disable VMD

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

VMD Config for IOU 0

Enable/Disable VMD

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

P1_AIOM PCI-E 4.0 X16 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 1

Enable/Disable VMD

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

P1_NVME0 VMD / P1_NVME1 VMD / P1_NVME2 VMD / P1_NVME3 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 3

Enable/Disable VMD

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

P1_NVME4 VMD / P1_NVME5 VMD / P1_NVME6 VMD / P1_NVME7 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 4

Enable/Disable VMD

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

M.2-HC_1 VMD / M.2-HC_2 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

▶Intel® VMD for Volume Management Device on CPU2 (Available when "NVMe Mode Switch" is set to Manual)

VMD Config for IOU 0

Enable/Disable VMD

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

P2 SLOT1 PCI-E 4.0 X16 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 1

Enable/Disable VMD

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 3

Enable/Disable VMD

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

P2 SLOT2 PCI-E 4.0 X16 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

VMD Config for IOU 4

Enable/Disable VMD

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

P2 SLOT3 PCI-E 4.0 X16 VMD (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

Hot Plug Capable (Available when the device is detected by the system and "Enable/Disable VMD" above is set to Enable)

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

PCI-E ASPM Support (Global)

Select Enabled to enable Active State Power Management (ASPM) support for all downstream devices of the drive installed on a PCI-E slot. The options are **Disable** and Auto.

IIO eDPC (Enhanced Downstream Port Containment) Support

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

Select On Fatal and Non-Fatal Error to enable IIO eDPC support when an error, fatal or non-fatal, has occurred. The options are **Disable**, On Fatal Error, and On Fatal and Non-Fatal Errors.

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

Select Enable to enable IIO eDPC Interrupt support. The options are Disable and **Enable**.

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

If this feature is set to Enable, an IIO eDPC error correction message will be displayed. The options are Disable and **Enable**.

▶South Bridge

The following information is displayed:

- USB Module Version
- USB Devices

Legacy USB Support

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

XHCI Hand-off

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

Port 60/64 Emulation

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

PCIe PLL SCC

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

Port 61h Bit-4 Emulation

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

▶Server ME Information

The following information is displayed:

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

▶PCH sSATA Configuration

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

Select AHCI to configure an sSATA drive specified by the user 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.

Support Aggressive Link Power Management

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

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

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

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

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

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

sSATA Port 0 - sSATA Port 3 / M.2-HC_1 / M.2-HC_2

Hot Plug

Select Enable to support Hot-plugging for the device installed on an sSATA port specified by the user which will allow the user to replace the device installed in the slot without shutting down the system. The options are Disable and **Enable**.

Spin Up Device

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

sSATA Device Type

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

▶Network Configuration

Network Stack

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

IPv4 PXE Support

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

IPv4 HTTP Support

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

IPv6 PXE Support

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

IPv6 HTTP Support

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

PXE Boot Wait Time

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

Media Detect Count

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

Use the following features to configure network parameters:

▶MAC:(MAC address)-IPv4 Network Configuration

Configured

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

Save Changes and Exit

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

▶MAC:(MAC address)-IPv6 Network Configuration

▶Enter Configuration Menu

The following information will display:

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

Interface ID

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

DAD Transmit Count

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

Policy

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

Save Changes and Exit

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

▶MAC:(MAC address)-IPv4 Network Configuration

Configured

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

Save Changes and Exit

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

▶MAC:(MAC address)-IPv6 Network Configuration

▶Enter Configuration Menu

The following information will display:

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

Interface ID

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

DAD Transmit Count

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

Policy

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

Save Changes and Exit

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

▶MAC:(MAC address)-IPv4 Network Configuration

Configured

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

Save Changes and Exit

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

▶PCIe/PCI/PnP Configuration

The following information is displayed:

- PCI Bus Driver Version
- PCI Devices Common Settings:

Above 4G Decoding (Available 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

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

ARI Support

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

Bus Master Enable

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

Consistent Device Name Support

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

MMIO High Base

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

MMIO High Granularity Size

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

Maximum Read Request

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

MMCFG Base

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

NVMe Firmware Source

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

VGA Priority

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

Onboard Video Option ROM

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

CPU2 SLOT1 PCI-E 4.0 X16 OPROM / CPU2 SLOT2 PCI-E 4.0 X16 OPROM / CPU2 SLOT3 PCI-E 4.0 X16 OPROM

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

M.2-HC_1 OPROM / M.2-HC_2 OPROM

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

CPU1 AIOM PCI-E 4.0 X16 OPROM

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

Onboard NVME0 Option ROM / Onboard NVME1 Option ROM / Onboard NVME2 Option ROM / Onboard NVME3 Option ROM / Onboard NVME4 Option ROM / Onboard NVME5 Option ROM / Onboard NVME6 Option ROM / Onboard NVME7 Option ROM

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

▶Super IO Configuration

Super IO Chip AST2600

▶Serial Port 1 Configuration

Serial Port 1

Select Enabled to enable serial port 1. The options are Disabled and **Enabled**.

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

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

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

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

▶Serial Port 2 Configuration

Serial Port 2

Select Enabled to enable serial port 2. The options are Disabled and **Enabled**.

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

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

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

This feature specifies the base I/O port address and the Interrupt Request address of serial port 2. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 2. The options 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 serial port 2 as a Serial Over LAN (SOL) port for console redirection. The options are **SOL** and COM.

▶Serial Port Console Redirection

COM1

Console Redirection

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

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

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

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

SOL (Serial-Over-LAN)

Console Redirection

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

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

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

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

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

Legacy Console Redirection

Legacy Serial Redirection Port

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

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

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

Console Redirection EMS

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

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

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 EMS

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

Flow Control EMS

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

The following information is displayed:

Data Bits EMS / Parity EMS / Stop Bits EMS

▶ACPI Settings

NUMA

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

UMA (Uniform Memory Access)-Based Clustering

When the option is set to Hemisphere, UMA-based clustering will support 2-cluster configuration for system performance enhancement. The options are Disable (All2All) and **Hemisphere (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**.

High Precision Event Timer

Select Enabled to activate the High Precision Event Timer (HPET) that produces periodic interrupts at a much higher frequency than a Real-time Clock (RTC) does in synchronizing

multimedia streams, providing smooth playback and reducing the dependency on other timestamp calculation devices, such as an x86 RDTSC Instruction embedded in the CPU. The High Performance Event Timer is used to replace the 8254 Programmable Interval Timer. The options are Disabled and **Enabled**.

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

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

- TPM 2.0 Device Found:
- Firmware Version:
- Vendor:

Security Device Support

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

*If this option is set to Enable, the following information will display:

- Active PCR Banks
- Available PCR Banks

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending Operation

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

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

Platform Hierarchy (for TPM Version 2.0 and above)

Select Enabled for TPM Platform Hierarchy support which will allow the manufacturer to utilize the cryptographic algorithm to define a constant key or a fixed set of keys to be

used for initial system boot. These early boot codes are shipped with the platform and are included in the list of "public keys". During system boot, the platform firmware uses the trusted public keys to verify a digital signature in an attempt to manage and control the security of the platform firmware used in a host system via a TPM device. The options are **Enabled** and Disabled.

Storage Hierarchy

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

Endorsement Hierarchy

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

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

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

Disable Block Sid

Select Enabled to allow SID authentication be performed in TCG Storage devices. The options are Enabled and **Disabled**.

SMCI BIOS-Based TPM Provision Support

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

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

TXT Support

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

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

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

▶HTTP Boot Configuration

HTTP BOOT Configuration

HTTP Boot Policy

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

HTTPS Boot Checks Hostname

Select Enabled to have HTTPS Boot to check if the hostname of TLS certificates matches the hostname provided by the remote server. The options are **Enabled** and Disabled (WARNING: Security Risk!!).

Priority of HTTP Boot

Instance of Priority 1:

This feature sets the rank target port. The default setting is **1**.

Select IPv4 or IPv6

This feature specifies which connection the target LAN port should boot from. The options are **IPv4** and IPv6.

Boot Description

Use this feature to enter a boot description, which cannot be longer than 75 characters. Please be suer to enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI (Uniform Research Identifier)

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

Instance of Priority 2

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

▶SMC-KMS Server Configuration

SMC-KMS Server IP address

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

Second SMC-KMS Server IP address

Use this feature to enter the second SMC-KMS server IP4 address in dotted-decimal notation.

SMC-KMS TCP Port number

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

KMS Time Out

Use this feature to enter the KMS server connecting time-out (in seconds). The default setting is **3** (seconds).

TimeZone

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

TCG Nvme KMS Policy

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

TCG Nvme KMS Retry Count

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

Client UserName

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

Client Password

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

KMS TLS Certificate / Size

▶CA Certificate

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

▶Client Certificate

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

▶Client Private Key

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

▶TLS Authenticate Configuration

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

▶Server CA Configuration

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

▶Enroll Certification

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

▶Enroll Certification Using File

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

Certification GUID (Global Unique Identifier)

Press <Enter> and input the certification GUID.

▶Commit Changes and Exit

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

▶Discard Changes and Exit

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

▶Delete Certification

This feature is used to delete the certificate if a certificate has been enrolled in the system.

▶Client Certification Configuration

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

▶Enroll Certification

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

▶Enroll Certification Using File

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

Certification GUID (Global Unique Identifier)

Press <Enter> and input the certification GUID.

▶Commit Changes and Exit

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

▶Discard Changes and Exit

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

▶Delete Certification

This feature is used to delete the certificate if a certificate has been enrolled in the system.

▶SMC PMem Configuration

▶SMCI PMem Information

Select this submenu and press <Enter>, the following will display:

- PMem UEFI Drive Version
- All Initialized DIMMs
- Total Initialized Intel PMem Count
- All DIMMs Security State

Note: The information provided in the following section is for illustration only. The number of PMem DIMM displays depends on the number of PMem populated in the system.

- DIMM [1] Handle: 10
- DIMM [1] DimmID (DIMMID)
- DIMM [1] Health State
- DIMM [1] Security State
- DIMM [1] Master PassEn: The default setting is Disabled.
- DIMM [1] UID (Unit ID)
- DIMM [1] Serial Number
- DIMM [1] FW (Firmware) Version
- DIMM [1] Capacity
- DIMM [1] APP Direct Capacity
- DIMM [1] Unconfigured Capacity
- DIMM [1] Reserved Capacity
- DIMM [1] Inaccessible Capacity
- DIMM [2] Handle
- DIMM [2] DimmID (DIMMID)
- DIMM [2] Health State

- DIMM [2] Security State
- DIMM [2] Master PassEn: the default setting is Disabled.
- DIMM [2] UID (Unit ID)
- DIMM [2] Serial Number
- DIMM [2] FW (Firmware) Version
- DIMM [2] Capacity
- DIMM [2] APP Direct Capacity
- DIMM [2] Unconfigured Capacity
- DIMM [2] Reserved Capacity
- DIMM [2] Inaccessible Capacity
- DIMM [3] Handle
- DIMM [3] DimmID (DIMMID)
- DIMM [3] Health State
- DIMM [3] Security State
- DIMM 3] Master PassEn: the default setting is Disabled.
- DIMM [3] UID (Unit ID)
- DIMM [3] Serial Number
- DIMM [3] FW (Firmware) Version
- DIMM [3] Capacity
- DIMM [3] APP Direct Capacity
- DIMM [3] Unconfigured Capacity
- DIMM [3] Reserved Capacity
- DIMM [3] Inaccessible Capacity
- DIMM [4] Handle
- DIMM [4] DimmID (DIMMID)

- DIMM [4] Health State
- DIMM [4] Security State
- DIMM [4] Master PassEn: the default setting is Disabled.
- DIMM [4] UID (Unit ID)
- DIMM [4] Serial Number
- DIMM [4] FW (Firmware) Version
- DIMM [4] Capacity
- DIMM [4] APP Direct Capacity
- DIMM [4] Unconfigured Capacity
- DIMM [4] Reserved Capacity
- DIMM [4] Inaccessible Capacity
- Total Intel PMem Regions Count

▶SMCI PMem Settings

Select this submenu and press <Enter>, the following items will display:

Create Goal Config (Configuration): Persistent: The default setting is [Do Nothing].

Memory Type

Reserved [%]

All PMem DIMMs have (the) same security state

User Security Policy

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

User DIMMs Current PassPhrase

User DIMMs New PassPhrase

All PMem DIMMs Master Security Policy

Master Security Policy

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

All PMem DIMMs FW (Firmware) Settings

Updated PMem DIMMs FW (Firmware) Version:

Update PMem DIMMs FW (Firmware) from BIOS

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

▶Intel® Optane™ Persistent Memory Configuration

Version:

This feature displays the version of PMem used in the system.

Select an action below.

Detected PMem Modules

All PMem modules are healthy.

▶PMem Modules

This submenu allows the user to view and configure the following settings for the PMem memory modules installed in the system:

Select a specific DIMM that you want to view.

Note: The following section, which describes the status of PMem memory, is for illustration only. The number or the status of PMem memory displayed on your BIOS screen will vary, depending on the PMem memory installed on your motherboard.

DIMMs on Socket 0x0000:

▶DIMM IO 0x0010 / ▶DIMM IO 0x0110 / ▶DIMM IO 0x0210 / ▶DIMM IO 0x0310

DIMMs on Socket 0x0001:

▶DIMM IO 0x1010 / ▶DIMM IO 0x1110 / ▶DIMM IO 0x1210 / ▶DIMM IO 0x1310

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

- DIMM UID: This feature displays the unique ID of the PMem module.
- DIMM Handle: This feature displays the unique handle assigned to the PMem module.

- DIMM Physical ID: This feature displays the physical ID of the PMem module.
- Manageability State: This feature indicates the manageability state of the PMem module.
- Health State: This feature indicates the health state of the PMem module.
- Health State Reason: This feature indicates the reason that effectuates the health state of the PMem module.
- Capacity: This feature indicates the capacity of the PMem module.
- Firmware Version: This feature indicates the firmware version of the PMem module.
- Firmware API Version: This feature indicates the firmware API version of the PMem module.
- Firmware Active API Version: This feature indicates the firmware API version of the PMem module.
- Lock State: This feature indicates the lock state of the PMem module.
- SVN Downgrade: This feature indicates the status of SVN Downgrade of the PMem module.
- Secure Erase Policy: This feature indicates the status of the Secure Erase Policy of the PMem module.
- S3 Resume Opt-in: This feature indicates the status of the S3 Resume Opt-in support for the PMem module.
- Firmware Activate Opt-in: This feature indicates the status of the Firmware Activate Opt-in support for the PMem module.
- Staged Firmware Version: This feature indicates the status of the staged firmware version of the PMem module.
- Staged Firmware Activate: This feature indicates the status of the staged firmware activate support of the PMem module.
- Firmware Update Status: This feature indicates the firmware update status of the PMem module.
- Firmware Activation Quiece Required: This feature indicates whether Firmware Activation Quiesce is required for the PMem module.
- Firmware Activation Quiece Required: This feature indicates whether Firmware Activation Quiesce is required for the PMem module.

- Firmware Activation Time: This feature indicates the time needed to activate the firmware.
- Manufacturer: This feature indicates the manufacturer of the PMem module.

Show More Details

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

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

- Serial Number
- Part Number
- Socket
- Memory Controller ID
- Vendor ID
- Device ID
- System Vendor ID
- Subsystem Vendor ID
- Subsystem Device ID
- Device Locator
- Subsystem Revision ID
- Interface Format Code
- Manufacturing Information Valid
- Manufacturing Date
- Manufacturing Location
- Memory Type
- Memory Bank Label
- Data Width Label [b]
- Total Width [b]
- Speed [MHz]

- Channel ID
- Channel Position
- Revision ID
- Form Factor
- Manufacturer ID
- Controller Revision ID
- IS New
- Memory Capacity
- APP Direct Capacity
- Unconfigured Capacity
- Inaccessible Capacity
- Reserved Capacity
- Avg (Average) Power Limit [mW]
- Memory Bandwidth Boost Feature
- Memory Bandwidth Boost Max Power Limit [mW]
- Memory Bandwidth Boost Average Power Time Constant [ms]
- Max Average Power Limit [mW]
- Max Memory Bandwidth Boost Max Power Limit [mW]
- Max Memory Bandwidth Boost Average Power Time Constant [ms]
- Memory Bandwidth Boost Average Power Time Constant Step [ms]
- Max Average Power Reporting Time Constant [ms]
- Average Power Reporting Time Constant Step [ms]
- Package Sparing Capable
- Package Sparing Enabled

- Package Spares Available
- Configuration Status
- SKU Violation
- Population Violation
- ARS Status
- Overwrite PMem Module Status
- Last Shutdown Time
- Average Power Reporting Time Constant [ms]
- Viral Policy Enable
- Viral State
- Thermal Throttle Loss %
- Latched Last Shutdown Status
- Unlatched Shutdown Status
- Security Capabilities
- Modes Supported
- Boot Status
- AIT DRAM Enabled
- Error Injection Enabled
- Max Controller Temperature [C]
- Software Triggers Enabled [0]
- Software Triggers Enabled Details
- Poison Error Injection Counter
- Poison Error Clear Counter
- Media Temperature Injections Counter

- Software Triggers Counter
- Max Media Temperature [C]
- Media Temperature Injection Enabled
- Master Passphrase Enabled
- Average Power
- Average Power 12V
- Average Power 1.2V
- eADR Enable
- Previous Power Cycle eADR Enabled
- Latch System Shutdown State
- Previous Power Cycle Latch System Showdown State
- Speed [MHz]
- Channel ID
- Channel Position
- Revision ID
- Form Factor
- Manufacturer ID
- Controller Revision ID
- IS New
- Memory Capacity
- APP Direct Capacity
- Unconfigured Capacity
- Inaccessible Capacity
- Reserved Capacity

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

- Unlatched Shutdown Status
- Security Capabilities
- Modes Supported
- Boot Status
- AIT DRAM Enabled
- Error Injection Enabled
- Max Controller Temperature [C]
- Software Triggers Enabled [0]
- Software Triggers Enabled Details
- Poison Error Injection Counter
- Poison Error Clear Counter
- Media Temperature Injections Counter
- Software Triggers Counter
- Max Media Temperature [C]
- Media Temperature Injection Enabled
- Master Passphrase Enabled
- Average Power
- Average Power 12V
- Average Power 1.2V
- eADR Enable
- Previous Power Cycle eADR Enabled
- Latch System Shutdown State
- Previous Power Cycle Latch System Showdown State

▶Monitor Health

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

- Current Alarm Threshold Status Controller Temperature: (within the alarm threshold on all PM modules)
- Controller Temperature: (within the alarm threshold on all PM modules).
- Media Temperature: (within the alarm threshold on all PM modules).
- Percentage Remaining: (within the alarm threshold on all PM modules).

Modify Alarm Thresholds Control Temperature [C]

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

Controller Temperature [C]

This feature indicates the media temperature of the PMem memory.

Media Temperature [C]

This feature indicates the media temperature of the PMem memory.

Percentage Remaining [%]

This feature displays the remaining percentage of the PMem memory.

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Update Firmware

Use this feature to select the firmware image to be loaded on the PMem module. After loading the firmware image, please reboot the system and select Update for the firmware to take effect. The following items will display:

Current Firmware Version

This feature displays the current firmware version.

Selected Firmware Version

Use this feature to select a new firmware version to use.

File

Use this feature to specify the file path in the root directory that contains the new firmware for firmware update.

Staged Firmware Version:

This feature indicates the staged firmware version of the PMem module specified by the user.

▶Update

Select this feature to update the firmware settings.

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Configure Security

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

State

Select Enabled to configure the security settings for the PMem modules installed in the system. The options are **Disabled** and Enabled.

Enable Security

This feature enables the security settings for the onboard PMem modules.

Secure Erase with User Password

Use this feature to erase all the persistent data saved in the PMem modules by entering user password.

Freeze Lock

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

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Configure Data Policy

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

Average Power Reporting Time Constant [ms]

This feature specified the constant average power reporting time.

Modify Average Power Reporting Time Constant

Use this feature to modify the constant average power reporting time.

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Regions

Current Configuration

▶Region ID 1

When this submenu is selected, the following items will display:

- Region ID: This feature displays the Region ID of the PMem module.
- DIMM ID: This feature displays the DIMM ID of the PMem module.
- ISet ID: This feature displays the ISet ID of the PMem module.
- Persistent Memory Type: This feature indicates the memory type of the PMem module.
- Capacity: This feature indicates the capacity of the PMem module.
- Free Capacity: This feature indicates the capacity of the PMem module that is available for use.
- Health: This feature indicates the health state of the PMem module.
- Socket ID: This feature displays the Socket ID of the PMem module.

▶Back to Regions Menu

▶Back to Provisioning Menu

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Provisioning

This submenu configures the memory allocation goal for the onboard PMem memory modules.

▶Create Goal Configuration

When this submenu is selected, the following items will display:

Create Goal Configuration for

- Use this feature to select the target to create goal configuration for the PMem modules. The options are Platform and Socket.
- Reserved [%]: This feature reserves a percentage of the PMem capacity for a particular purpose and keep this portion of memory space from being mapped into the physical address of system for system use.
- Memory Mode [%]: This feature reserves a percentage of the PMem capacity for special use in a specific Memory Mode. (This value can be automatically set by the system.)

Persistent Memory Type

This feature specifies the type of PMem memory capacity to be created. The options are **App Direct** and App Direct Not Interleave.

Namespace Label Version

Use this feature to view and modify the namespace label version to initialize when creating goals. The options are **1.2** and 1.1.

▶Create Goal Configuration

▶DIMM ID

- MemorySize
- AppDirect1Size
- AppDirect2Size

▶Delete Goal Configuration

▶Back to Previous Menu

Select this feature and press <Enter> to go back to the previous menu.

▶Back to Main Menu

Select this feature and press <Enter> to go back to the Intel® Optane™ Persistent Memory Configuration menu.

▶Namespaces

This subsection allows the user to select a namespace to view the following information on the selected namespace

Namespace ID/Name/Heath Status

▶0x00000201

Select this feature and press <Enter>, the following items will display:

- UUID
- ID
- Name
- Region
- Health
- Mode
- Block Size
- Units: Use this feature to change the namespace capacity (in the unit of B, MB, MiB, GB, **GiB**, TB, and TiB.)
- Capacity
- Label Version

▶**Delete** After configuring the settings for the namespace above, click on <delete> to delete the changes you've made on the namespace. Please note that all data contained in the namespace will be deleted as well when you press <delete>.

▶Back to Namespaces

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Create Namespace

Use this submenu to create a namespace. The following information will display:

Name

Region ID

This feature displays the Region ID of the PMem module. The options are **0x0001** and 0x0001.

Mode

Use this feature to set the Namespace mode. The options are **None** and Sector.

Capacity Input

Select Remaining to use the maximum memory capacity currently available as system memory capacity. Select Manual to enter the system memory capacity manually. The options are **Remaining** and Manual.

Units

Use this feature to select the type of unit to use when inputting namespace capacity in the system.

The options are B, MB, MiB, GB, **GiB**, TB, and TiB.

- **Capacity**: This feature displays the namespace capacity.

▶Create Namespace

▶Back to Namespaces

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Total Capacity

This feature allows the user to set the total PMem resource capacity allocated across all segments in the host server.

PMem Module Capacities

This section displays the following information:

- Volatile: This feature specifies Volatile information of the PMem module.
- AppDirect: This feature specifies the App. direct capacity of the PMem module.
- Inaccessible: This feature specifies the capacity of the PMem module that is not accessible to the user.
- Raw: This feature specifies the raw capacity of the PMem module.

DDR Capacities

- Volatile: This feature specifies Volatile information of the PMem module.
- Cache: This feature specifies the capacity of the cache memory.
- Inaccessible: This feature specifies the capacity of the PMem module that is not accessible to the user.
- Raw: This feature specifies the raw capacity of the PMem module.

Total Memory Capacities

- Volatile: This feature specifies Volatile information of the PMem module.
- AppDirect: This feature specifies the App. direct capacity of the PMem module.
- Cache: This feature specifies the capacity of the cache memory.
- Inaccessible: This feature specifies the capacity of the PMem module that is not accessible to the user.
- Raw: This feature specifies the raw capacity of the PMem module.

▶Back to Main Menu

Select this feature and press <Enter> to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Diagnostics

Perform Diagnostic Tests on DIMMs

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

Choose Diagnostics Type:

Use this feature to choose the type of diagnostics test to be performed on the PMem module installed in the system

Quick Diagnostics

Select Enabled for the quick diagnostics test to be performed on the PMem module installed in the system when needed. The options are **Enabled** and Disabled.

DIMM ID

Select Enabled to display the DIMM ID of a PMem module upon which the diagnostic test will be performed. The options are **Enabled** and Disabled. Please note that more DIMM IDs will appear If more PMem modules are installed on the motherboard.

Config (Configure) Diagnostics

Select Enabled for the platform configuration diagnostics test to be performed on the PMem module. The options are **Enabled** and Disabled.

FW (Firmware) Diagnostics

Select Enabled for the firmware diagnostics test to be performed on the PMem module. The options are **Enabled** and Disabled.

Security Diagnostics

Select Enabled for the security diagnostics test to be performed on the PMem module. The options are **Enabled** and Disabled.

▶Execute Tests

Select this feature and press <Enter> to execute the selected diagnostic tests. The following items will be displayed:

▶Back to Diagnostics

▶Back to Main Menu

Use this feature to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Preferences

View and/or modify user preferences

Default DIMM ID

This feature allows the user to view and to modify the default DIMM ID as displayed on the screen. The options are **Handle** and UID.

Capacity Units

This feature allows the user to view and to set the default capacity unit of the selected PMem to be displayed on the screen. The options are **Auto**, Auto_10, B, MB, MiB, GB, GiB, TB, and TiB.

App Direct Settings

This feature displays the Application Direct Settings. The default setting is **4KB_4KB (Recommended)**.

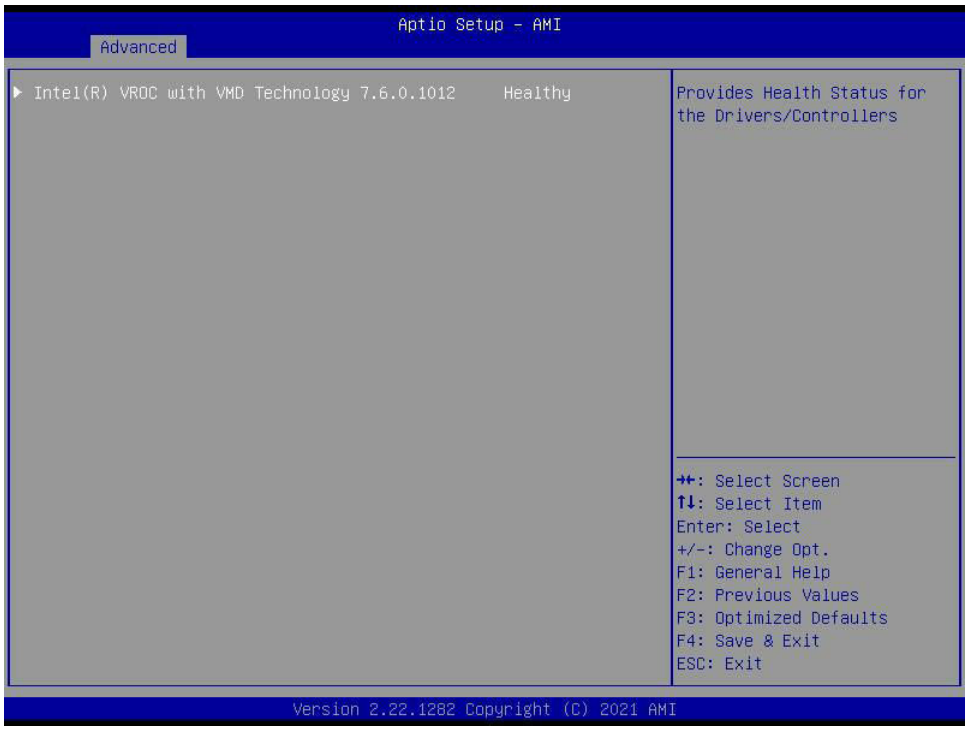
▶Back to Main Menu

Use this feature to go back to the **Intel® Optane™ Persistent Memory Configuration** menu.

▶Driver Health

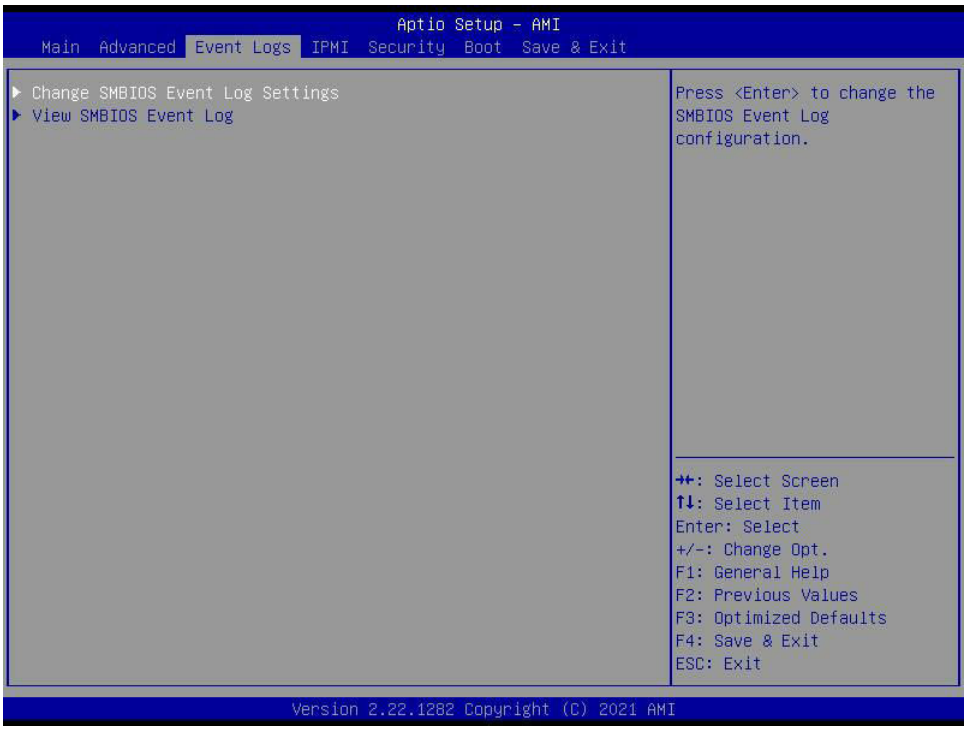
This feature displays the health information of the drivers installed in your system, including LAN controllers, as detected by the BIOS. Select one and press <Enter> to see the details.

Note: This section is provided for reference only, for the driver health status will differ depending on the drivers installed in your system. It's also based on your system configuration and the environment that your system is operating in.



4.4 Event Logs

Use this feature to configure Event Log settings.



▶Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

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

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

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

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

SMBIOS Event Log Standard Settings

Log System Boot Event

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

MECI (Multiple Event Count Increment)

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

METW (Multiple Event Time Window)

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

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

▶View SMBIOS Event Log

This feature allows you to view the event in the system event log. Select this feature and press <Enter> to view the status of an event in the log. The following categories will be displayed:

DATE / TIME / ERROR CODE / SEVERITY.

4.5 IPMI

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

BMC Firmware Revision

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

IPMI STATUS

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

▶System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

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

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

▶BMC Network Configuration

BMC Network Configuration

Update IPMI LAN Configuration

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

****

Configure IPv4 Support

****

IPMI LAN Selection

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

IPMI Network Link Status

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

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

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

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

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

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

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

Station MAC Address

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

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

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

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

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

****

Configure IPv6 Support

****

IPv6 Address Status

This feature displays the status of IPv6 addresses.

IPv6 Support

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

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

Use this feature to select the source of the IPv6 connection. If Static is selected, you will need to know the IP address of IPv6 connection and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server in the network that is attached to and request the next available IP address for this computer. The options are Static and **DHCP**.

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

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

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

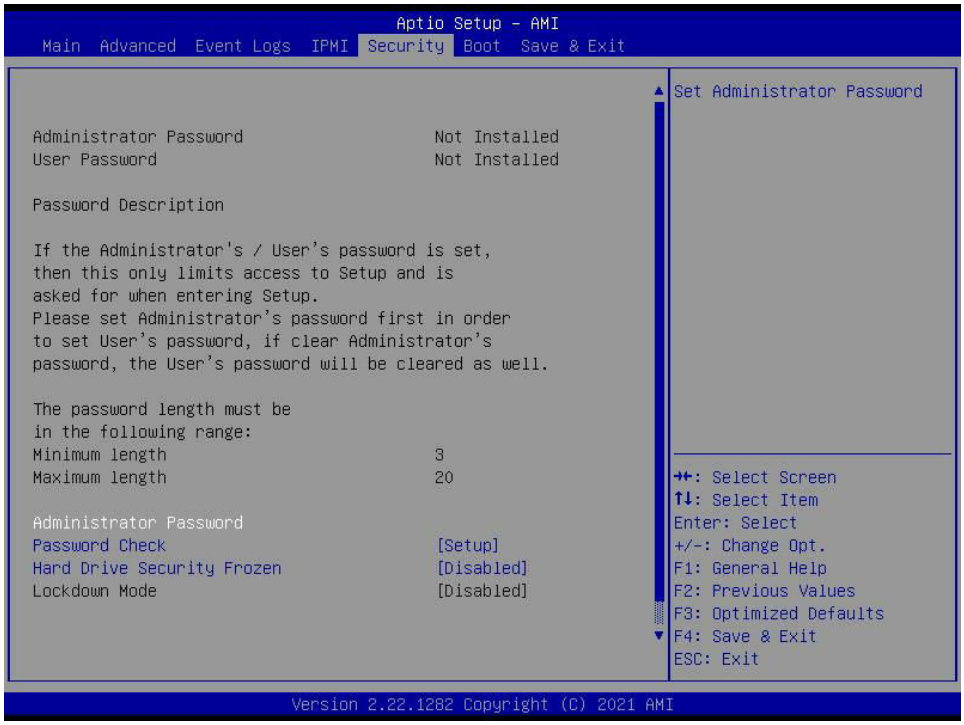
This feature displays the prefix length. Press <Enter> to change the setting.

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

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

4.6 Security

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



Administrator Password

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

Password Check

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

Hard Drive Security Frozen

Select Enabled to freeze and lock hard drive security settings to protect important data stored in the HDDs from being altered. The options are Enabled and **Disabled**.

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

Lockdown Mode

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

▶Secure Boot

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

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

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

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

Secure Boot Mode

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

CSM Support

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

▶Enter Audit Mode

This feature allows you to set the Audit Mode.

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

The following information is displayed.

- Vendor Keys

Provision Factory Defaults

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

▶Restore Factory Keys

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

▶Reset to Setup Mode

This feature resets the system to the Setup Mode. The options are **Yes** and No.

▶Export Secure Boot variables

This feature exports the NVRAM contents of secure boot variables to a storage device. The options are **Yes** and No.

▶Enroll Efi Image

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

Device Guard Ready

▶Remove 'UEFI CA' from DB

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

▶Restore DB defaults

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

Secure Boot Variable / Size / Keys / Key Source

▶Platform Key(PK)

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

▶Key Exchange Keys

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

▶Authorized Signatures

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

▶Forbidden Signatures

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

▶Authorized TimeStamps

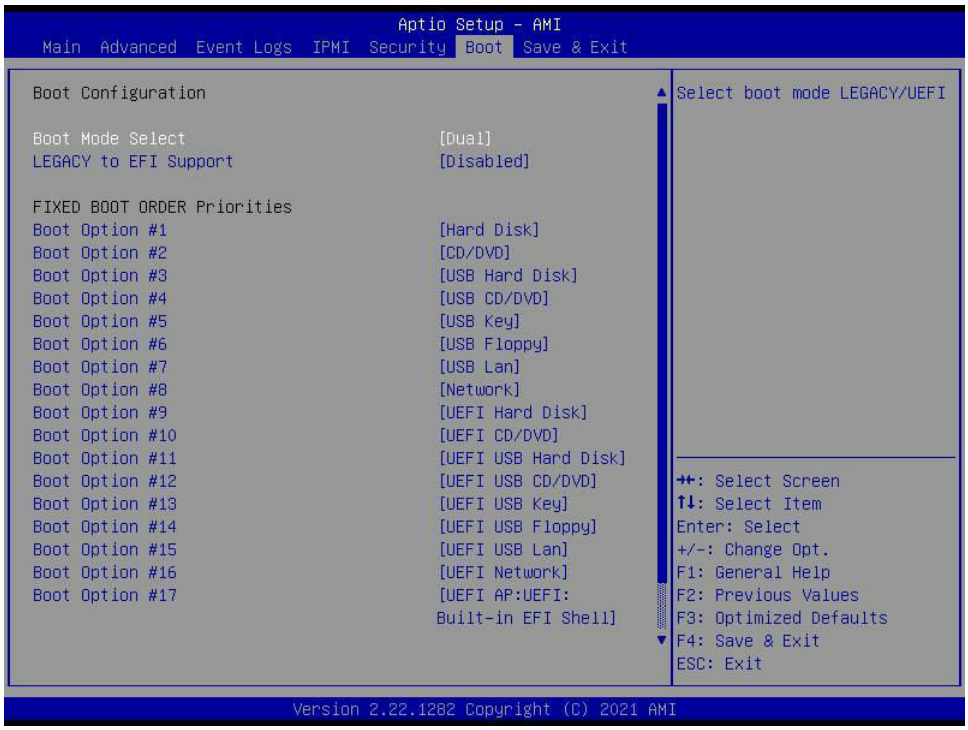
This feature allows you to set and save the timestamps for the authorized signatures which will indicate the time when these signatures are entered into the system. These values also indicate sizes, keys, and key sources of the authorized timestamps. Select Update to update your "Authorized TimeStamps".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

▶OsRecovery Signature

This feature allows you to set and save the authorized signatures used for OS recovery. Select Update to update your "OS Recovery Signatures". These values also indicate sizes, keys, and key sources of the OsRecovery signatures. Select Append to append your "OS Recovery Signatures". The options are **Details**, Export, Update, Append, and Delete.

4.7 Boot

Use this feature to configure Boot settings.



Boot Mode Select

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

Note: When the feature "Boot Mode Select" above is set to Dual, be sure to set all OPROM-related settings to Legacy.

Legacy to EFI Support

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

Fixed Boot Order Priorities

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

If the feature "Boot Mode Select" above is set to Dual (default), the following features will be displayed for the user to configure the boot settings:

- Boot Option #1 - Boot Option #17

If the feature "Boot Mode Select" above is set to Legacy, the following features will be displayed for the user to configure the boot settings:

- Boot Option #1 - Boot Option #8

If the feature "Boot Mode Select" above is set to UEFI, the following features will be displayed for the user to configure the boot settings:

- Boot Option #1 - Boot Option #9

▶Delete Boot Option

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

Delete Boot Option

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

▶UEFI Application Boot Priorities

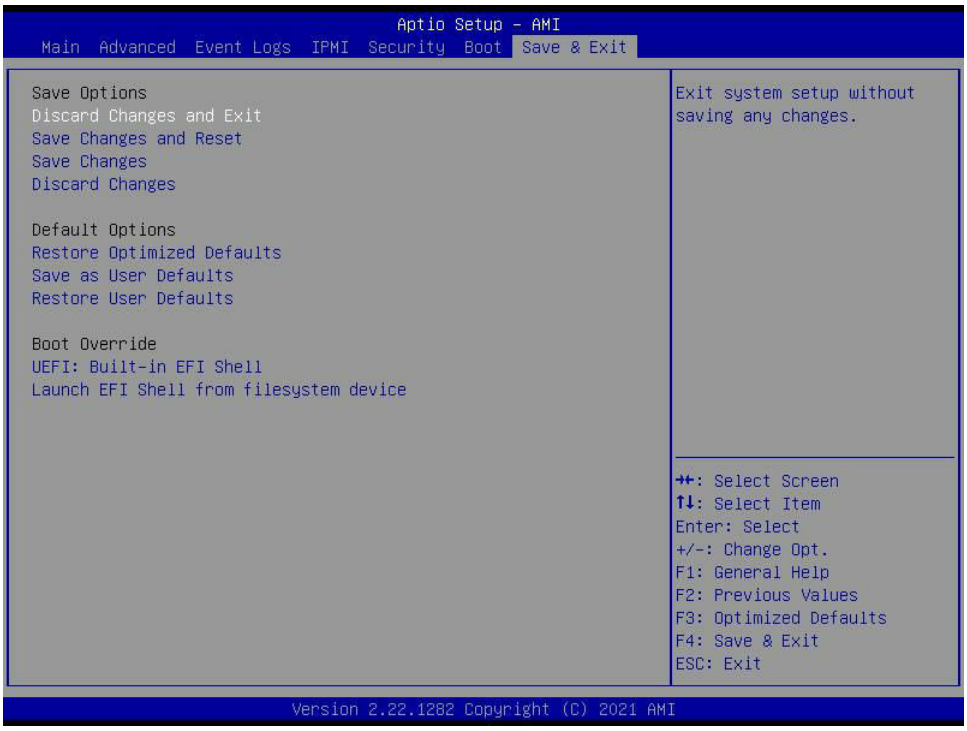
This feature allows you to change the UEFI network drive priority boot list.

▶UEFI NETWORK Drive BBS Priorities

This feature allows you to change the UEFI network drive priority boot list.

4.8 Save & Exit

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



Save Options

Discard Changes and Exit

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

Save Changes and Reset

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

Save Changes

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

Discard Changes

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

Default Options

Restore Optimized Defaults

Select this feature and press <Enter> to load manufacturer optimized default settings which are intended for maximum system performance but not for maximum stability.

Save as User Defaults

Select this feature and press <Enter> to save all changes on the default values specified to the BIOS Setup utility for future use.

Restore User Defaults

Select this feature and press <Enter>. Use this feature to retrieve user-defined default settings that have been saved previously.

Boot Override

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

Appendix A

BIOS POST Codes

A.1 BIOS POST Codes

The AMI BIOS supplies additional checkpoint codes, which are documented online at http://www.supermicro.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 (Supermicro p/n AOM-SPI80-V).

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

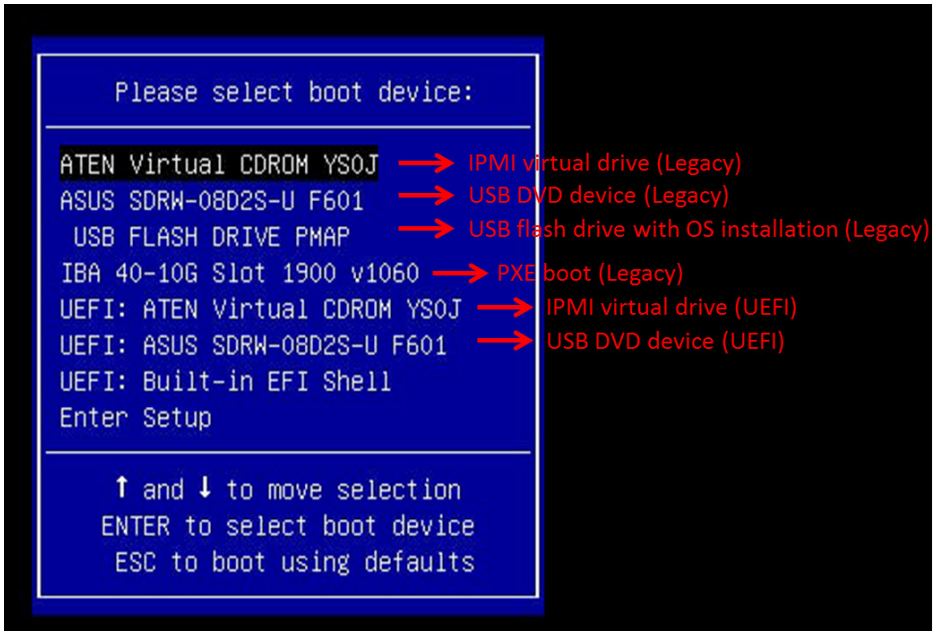
If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at www.supermicro.com/support/manuals.

Installing the OS

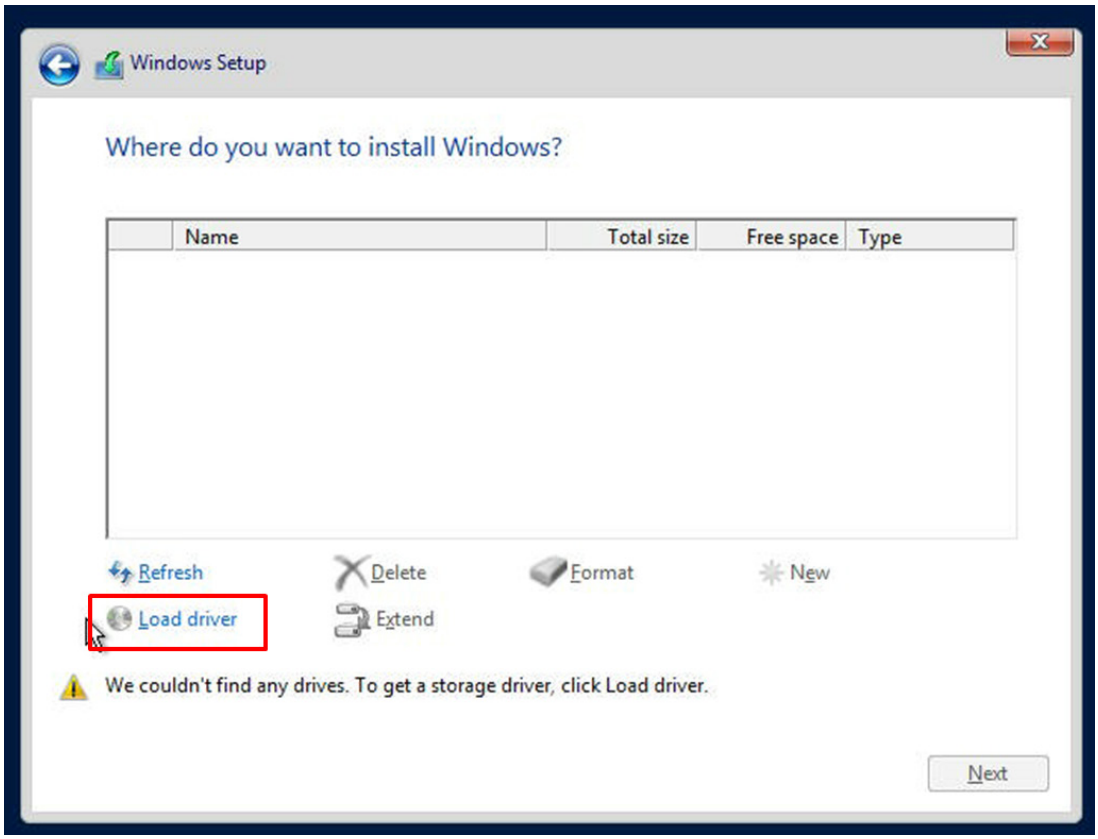
1. Create a method to access the MS Windows installation ISO file. That might be a DVD, perhaps using an external USB/SATA DVD drive, or a USB flash drive, or the BMC KVM console.

2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.

3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing **F11** during the system startup.



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



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

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

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

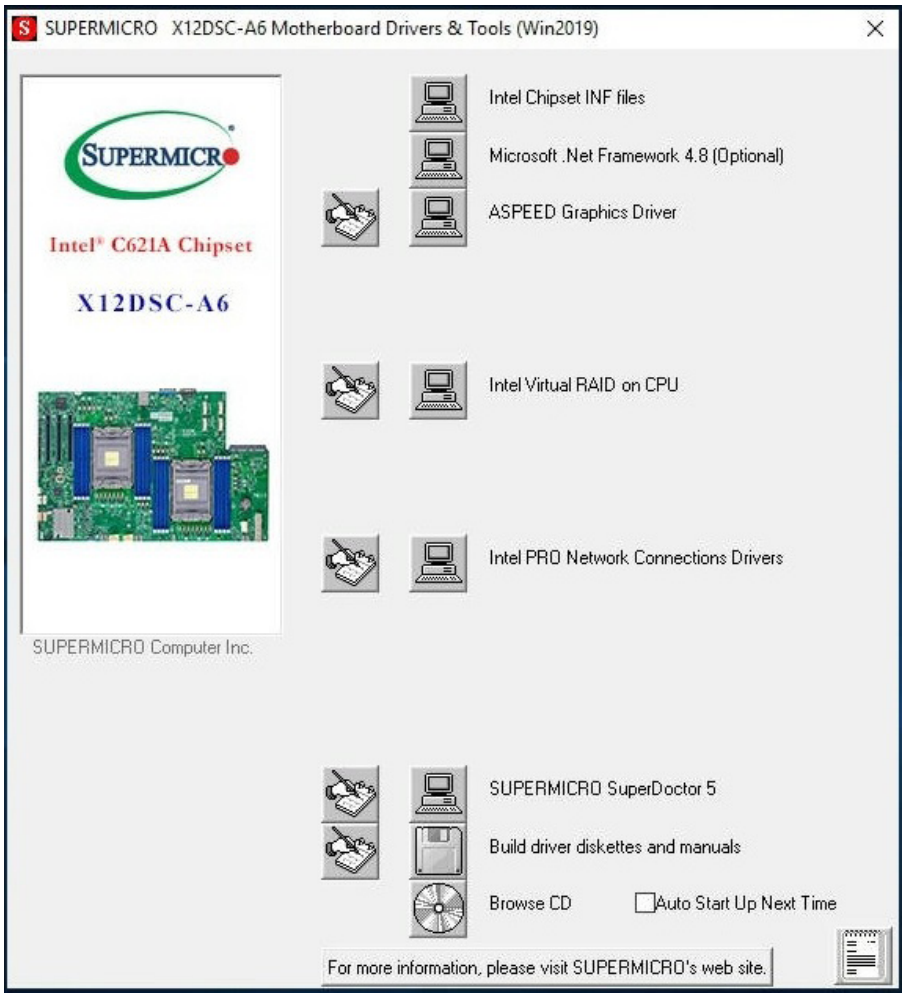
B.2 Driver Installation

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

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

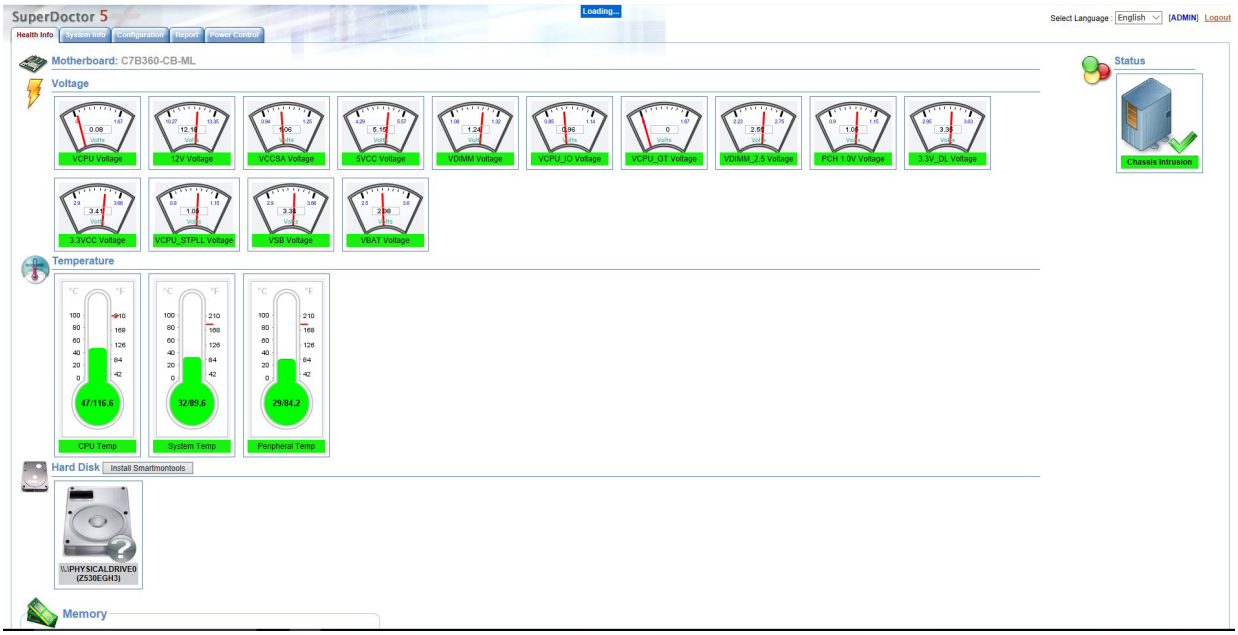


Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to bottom) one at a time. **After installing each item, you must re-boot the system before moving on to the next item on the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

B.3 SuperDoctor® 5

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

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



B.4 BMC

The X12DSC-A6 supports the Baseboard Management Controller (BMC). BMC is used to provide remote access, monitoring and management. There are several BIOS settings that are related to BMC.

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

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

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

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

For more information regarding BMC passwords, please visit our website at http://www.supermicro.com/bmcpassword.

Appendix C

Standardized Warning Statements

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

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

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

Battery Handling

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

電池の取り扱い

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

警告

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

警告

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

Warnung

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

Attention

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

¡Advertencia!

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

אזהרה!

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

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

경고!

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

Waarschuwing

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

Product Disposal

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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

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

경고!

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

Waarschuwing

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