X11DPD-L/-M25

USER'S MANUAL

Revision 1.0a

The information in this user's manual has been carefully reviewed and is believed to be accurate. The vendor 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 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".

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

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

Manual Revision 1.0a

Release Date: October 08, 2020

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 © 2020 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 X11DPD-L/-M25 motherboard.

About This Motherboard

The X11DPD-L/-M25 motherboard supports dual Intel® Xeon® Scalable-SP and 2nd Generation Intel Xeon Scalable-SP series processors (Socket P) with a TDP (Thermal Design Power) of up to 205W and two UPI (UltraPath Interconnect) links of up to 10.4 GT/s (**Note 1** below). Built with the Intel C621 built-in, this motherboard supports up to 4TB of 3DS LRDIMM/RDIMM DDR4 ECC 2933*/2666/2400/2133 MHz memory in 16 memory slots (**Note 2** below). It also supports up to 2TB Intel Optane™ DC Persistent Memory in memory mode (2nd Gen Intel Xeon Scalable-SP processors only). The X11DPD-L/-M25 provides maximal system performance, SATA versatility, and PCIe expandability. It is optimized for PCIe expansion with flexible I/O support, and is ideal for general-purpose 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: UPI/memory speeds are dependent on the processors installed in your system.

Note 2: Support for 2933 MHz memory is dependent on the CPU SKU.

Manual organization

Chapter 1 describes the features, specifications, and performance of the motherboard. It also provides detailed information on the Intel C621 chipset.

Chapter 2 provides hardware installation instructions. Read this chapter when installing the processor, memory modules, and other hardware components into the system.

Chapter 3 describes troubleshooting procedures for video, memory, and system setup stored in the CMOS.

Chapter 4 includes an introduction to the BIOS, and provides detailed information on running the CMOS Setup utility.

Appendix A lists software program installation instructions.

Appendix B lists standardized warning statements in various languages.

Appendix C contains UEFI BIOS Recovery instructions.

Appendix D provides information on how to configure VROC RAID settings.

Appendix E provides information on how to configure iSCSI settings.

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 Checklist 8
1.2 Processor and Chipset Overview 19
1.3 Special Features 20
1.4 System Health Monitoring 20
1.5 ACPI Features 21
1.6 Power Supply 21
1.7 Advanced Power Management 21
1.8 Intel Optane DC Persistent Memory Overview 22

Chapter 2 Installation

2.1 Static-Sensitive Devices 23
Precautions 23
Unpacking 23
2.2 Motherboard Installation 24
Tools Needed 24
Location of Mounting Holes 24
Installing the Motherboard 25
2.3 Processor and Heatsink Installation 26
Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processors 26
Overview of the Processor Socket Assembly 27
Overview of the Processor Heatsink Module (PHM) 28
Attaching the Processor to the Narrow Processor Clip to Create the Processor Package Assembly 29
Attaching the Processor Package Assembly to the Heatsink to Form the Processor Heatsink Module (PHM) 30
Preparing the CPU Socket for Installation 31
Removing the Dust Cover from the CPU Socket 31
Installing the Processor Heatsink Module (PHM) 32
Removing the Processor Heatsink Module (PHM) from the Motherboard 33
2.4 Memory Support and Installation 34
Memory Support 34
Memory Installation Sequence 34

General Memory Population Requirements....34
DDR4 Memory Support for Intel Xeon Scalable-SP Processors....35
DDR4 Memory Support for 2nd Gen Intel Xeon Scalable-SP Processors....35
DIMM Population Guidelines for Optimal Performance....36
DIMM Population Table....37
Memory Rank Sparing Tables....38
DIMM Installation....40
DIMM Module Removal....40
2.5 Rear I/O Ports....41
2.6 Front Control Panel....48
2.7 Connectors....53
Power Connector....53
Headers....55
2.8 Jumper Settings....64
How Jumpers Work....64
2.9 LED Indicators....68

Chapter 3 Troubleshooting

3.1 Troubleshooting Procedures....71
3.2 Technical Support Procedures....74
3.3 Battery Removal and Installation....75
3.4 Frequently Asked Questions....76
3.5 Returning Merchandise for Service....78

Chapter 4 UEFI BIOS

4.1 Introduction....79
4.2 Main Setup....80
4.3 Advanced Setup Configurations....82
4.4 Event Logs....130
4.5 IPMI....132
4.6 Security....135
4.7 Boot....138
4.8 Save & Exit....140

Appendix A Software

A.1 Microsoft Windows OS Installation 142

A.2 Driver Installation.....144

A.3 SuperDoctor 5 145

A.4 IPMI 146

A.5 Logging into the BMC (Baseboard Management Controller).....146

Appendix B Standardized Warning Statements

Appendix C UEFI BIOS Recovery

C.1 Overview.....150

C.2 Recovering the UEFI BIOS Image 150

C.3 Recovering the Main BIOS Block with a USB Device 151

Appendix D Configuring VROC RAID Settings

D.1 All Intel VMD Controllers Menu.....155

D.2 Configuring RAID Settings 159

D.3 Use of Journaling Drive.....175

Appendix E Configuring iSCSI Settings

E.1 PCIe/PCI/PnP Features.....179

E.2 Configuring iSCSI Settings.....182

Chapter 1

Introduction

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

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

1.1 Checklist

Main Parts List		
Description	**Part Number**	**Quantity**
Supermicro Motherboard	X11DPD-L/-M25	1

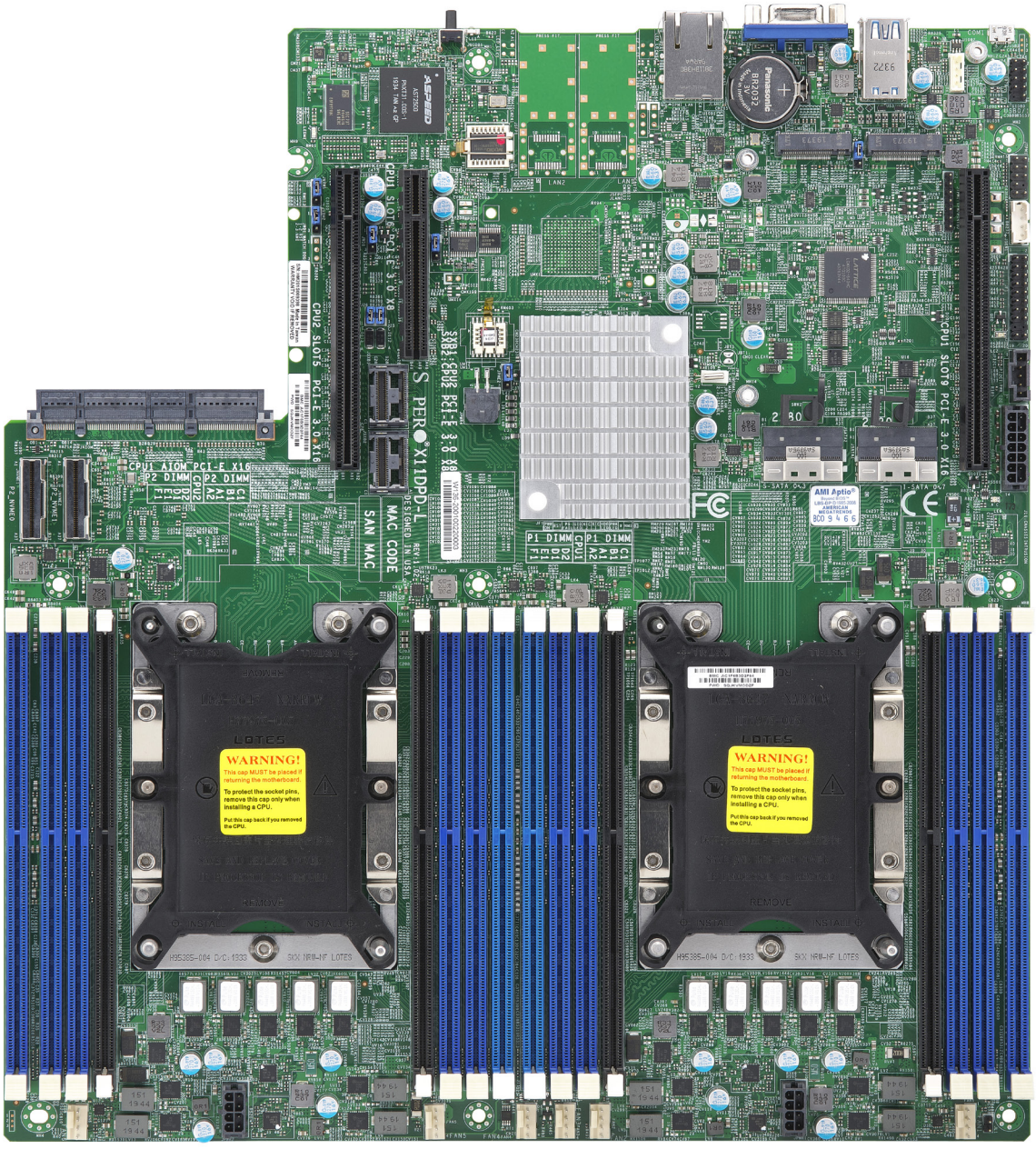
Important Links

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

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

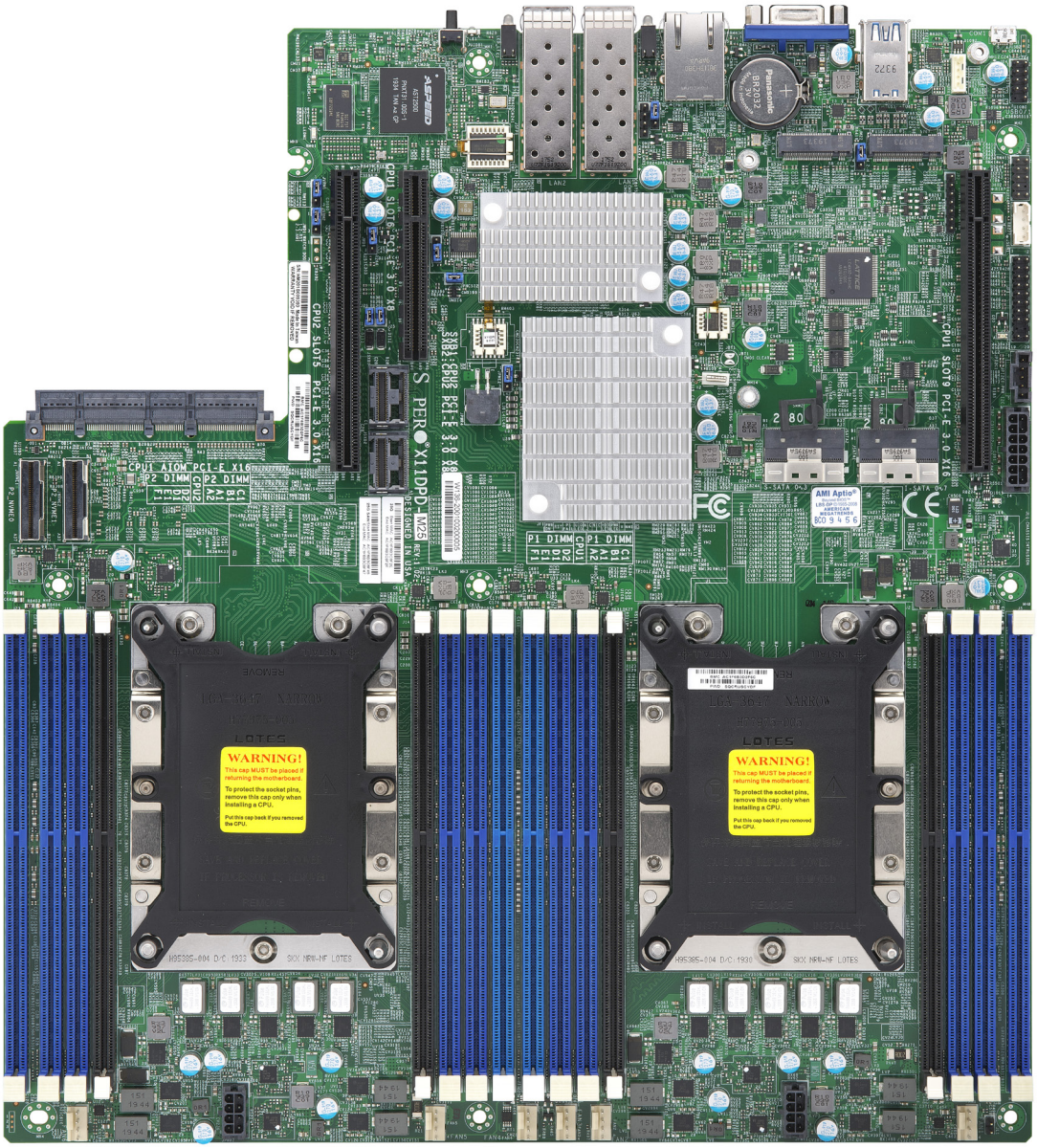
This manual may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

X11DPD-L 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.

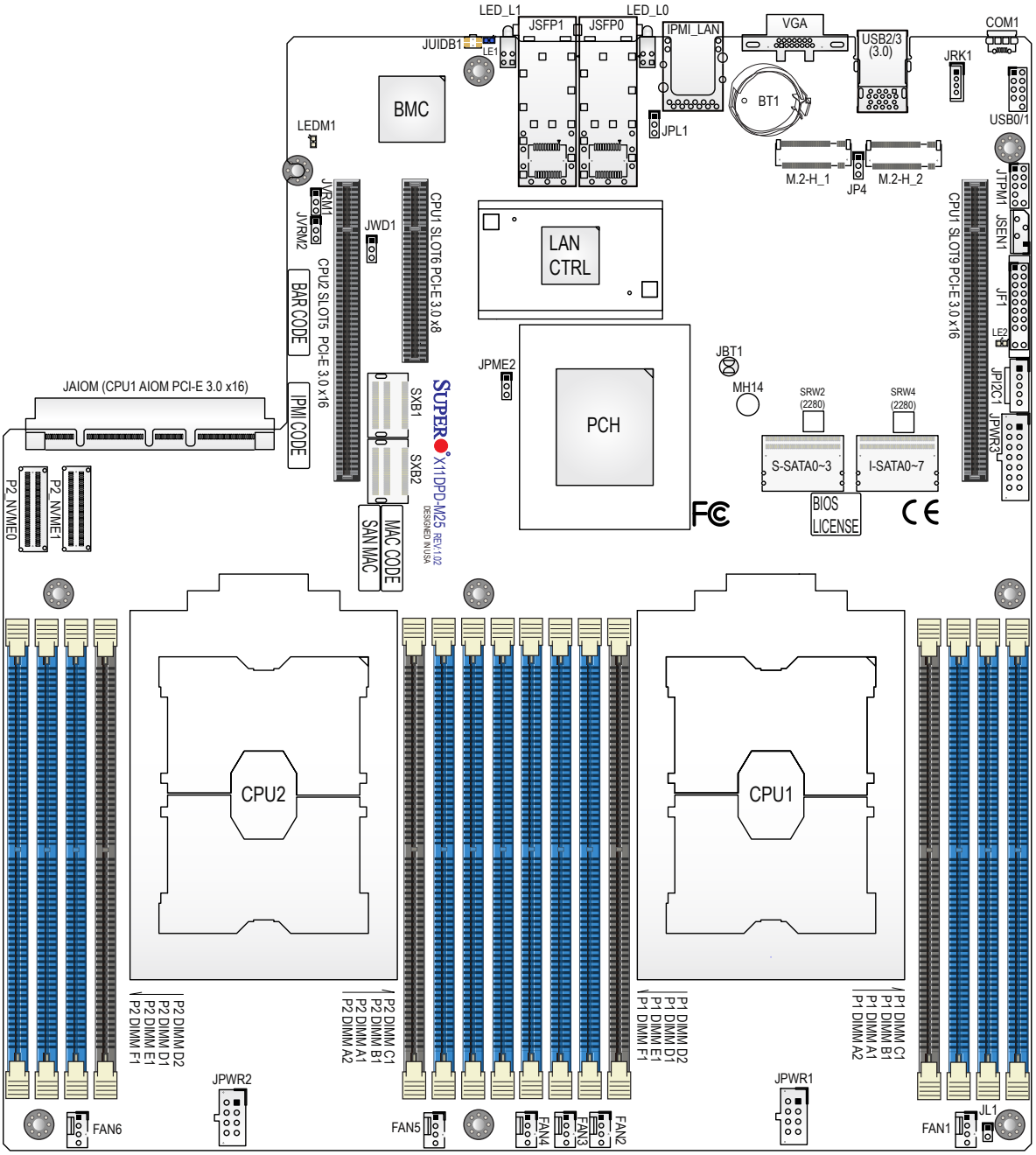
X11DPD-M25 Motherboard Image



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.

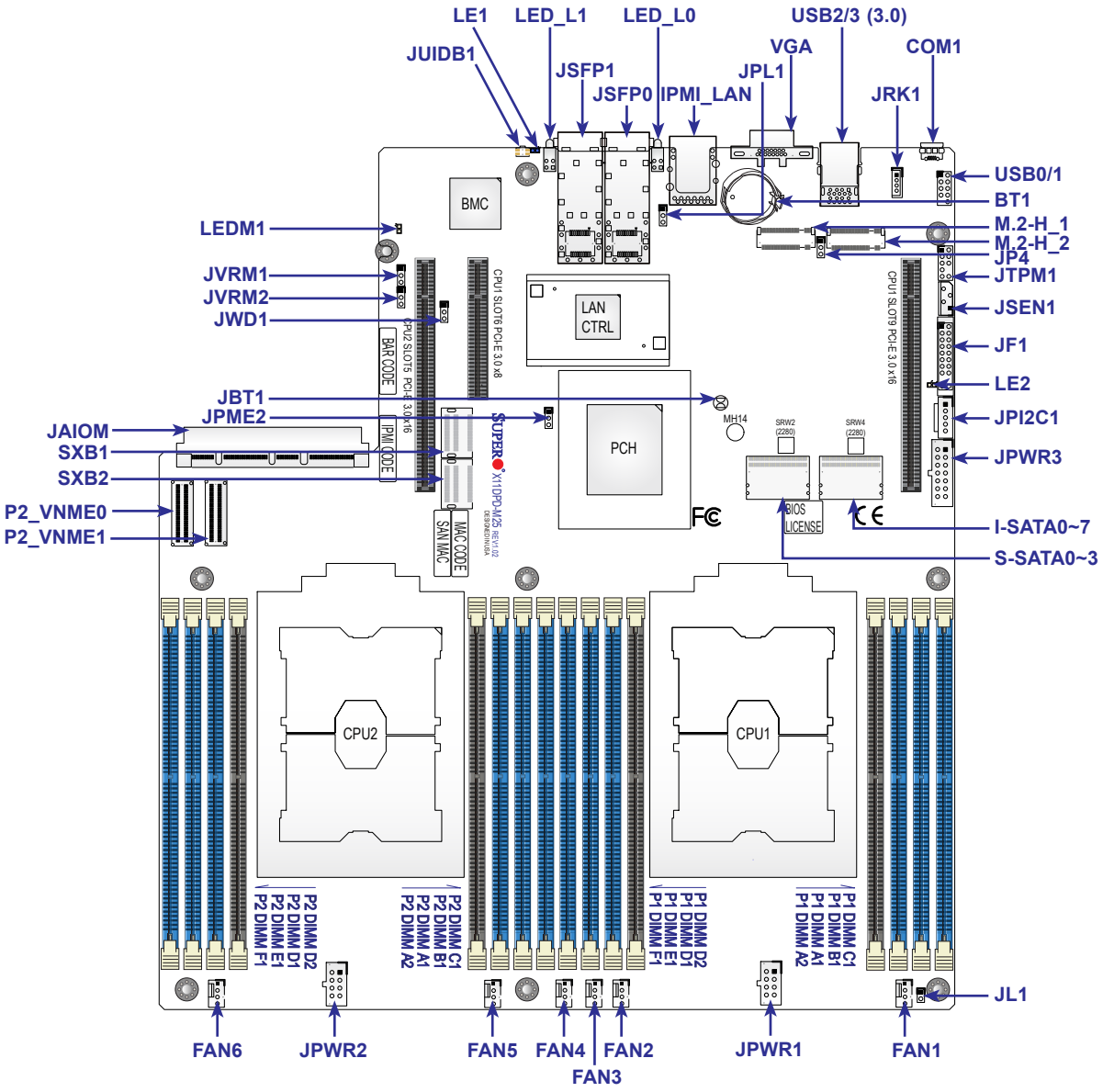
X11DPD-L/-M25 Motherboard Layout

(not drawn to scale)



Differences between X11DPD-L and X11DPD-M25		
	X11DPD-L	**X11DPD-M25**
25GbE SFP28 Ports and LED Indicators	No	Yes
JPL1	No	Yes

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/components/LED indicators not indicated are used for internal 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.
- To avoid causing interference with other components, please be sure to use an add-on card that is fully compliant with the PCIe standard on a PCIe slot.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JP4	JF1 Pin 3 Function Selection	Pins 1-2 (Reset Button)
JPL1	25GbE SFP28 Ports Enable (X11DPD-M25 only)	Pins 1-2 (Enabled)
JPME2	Manufacturing (ME) Mode Select	Pins 1-2 (Normal)
JVRM1	VRM SMB Clock (to BMC or PCH)	Pins 1-2 (BMC)
JVRM2	VRM SMB Data (to BMC or PCH)	Pins 1-2 (BMC)
JWD1	Watch Dog Timer Enable	Pins 1-2 (Reset)

Connector	Description
BT1	Onboard CMOS Battery
COM1	Back Panel Serial Port (Micro USB to COM)
FAN1 ~ FAN6	System Cooling Fan Headers
IPMI_LAN	Dedicated IPMI LAN Port
JAIOM	PCIe 3.0 x16 Supermicro Advanced I/O Module (AIOM) Slot (supported by CPU1)
JF1	Front Control Panel Header
JL1	Chassis Intrusion Header (**Note:** Please connect a cable from the Chassis Intrusion Header at JL1 to the chassis to receive an alert via IPMI.)
JPI^{2}C1	Power Supply SMBus I^{2}C Header
JPWR1, JPWR2	12V 8-pin Power Supply Connectors
JPWR3	14-pin Power Supply Connector
(VROC) JRK1	Intel VROC RAID Key Header for NVMe SSDs
JSEN1	Inlet Sensor Header
JSFP0, JSFP1	25GbE SFP28 Ports (X11DPD-M25 only)
JTPM1	Trusted Platform Module (TPM)/Port 80 Header
JUIDB1	Unit Identifier (UID) Switch
M.2-H_1	PCIe 3.0 x4 / SATA Hybrid M.2 Socket
M.2-H_2	PCIe 3.0 x1 / SATA Hybrid M.2 Socket
P2_NVME0, P2_NVME1	NVM Express PCIe 3.0 x4 Ports with two connections each (supported by CPU2)
(I-)SATA0~7, (S-)SATA0~3	Intel PCH SATA 3.0 Ports
SXB1, SXB2	PCIe 3.0 x8 Riser Card Slots (supported by CPU2)
USB0/1	USB 2.0 Header
USB2/3	Back Panel USB 3.0 Ports
VGA	Back Panel VGA Port

Notes:

1. Components not documented are for internal testing only.

2. When installing an NVMe device on a motherboard, please be sure to connect the first NVMe port (P2_NVME0) first for your system to work properly.

LED	Description	Status
LE1	UID LED	Solid Blue: Unit Identified
LE2	Onboard Power LED	Solid Green: Power On
LED_L0	SFP28 Port 0 (JSFP0) Link/Activity LED (X11DPD-M25 only)	(Activity LED) Blinking Green: SFP28 Port 0 (JSFP0) Active (Link LED) Solid Green: 25G (Link LED) Solid Yellow: 10G/1G
LED_L1	SFP28 Port 1 (JSFP0) Link/Activity LED (X11DPD-M25 only)	(Activity LED) Blinking Green: SFP28 Port 1 (JSFP1) Active (Link LED) Solid Green: 25G (Link LED) Solid Yellow: 10G/1G
LEDM1	BMC Heartbeat LED	Blinking Green: BMC Normal

Notes:

1. Intel VMD is supported by PCIe slots and NVMe ports (P2_NVME0 and P2_NVME1).

2. After you've enabled VMD 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.

Motherboard Features

Motherboard Features	
CPU	
• This motherboard supports dual Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP processors (Socket P) with two Intel UltraPath Interconnect (UPI) links of up to 10.4 G/s **Note:** Both CPUs need to be installed for full access to the PCIe slots, DIMM slots, and onboard controllers. Refer to the block diagram on page 18 to determine which slots or devices may be affected.	
Memory	
• Integrated memory controller supports up to 4TB of 3DS Load Reduced DIMM (3DS LRDIMM), Load Reduced DIMM (LRDIMM), 3DS Registered DIMM (3DS RDIMM), Registered DIMM (RDIMM), Non-Volatile DIMM (NV-DIMM) DDR4 (288-pin) ECC 2933*/2666/2400/2133 MHz memory in 16 memory slots. **Notes: 1.** Support for 2933 MHz memory is dependent on the CPU SKU **2.** Up to 2TB DCPMM memory is supported (2nd Gen Intel Xeon Scalable-SP 82xx/62xx/52xx/4215 series processors only).	
DIMM Size	
• Up to 256GB at 1.2V **Note 1:** Memory speed support depends on the processors used in the system. **Note 2:** For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.	
Chipset	
• Intel C621	
Expansion Slots	
• One PCIe 3.0 x8 slot supported by CPU1 • One PCIe 3.0 x16 slot supported by CPU1 • One PCIe 3.0 x16 AIOM slot supported by CPU1 • One PCIe 3.0 x16 slot supported by CPU2 • Two PCIe 3.0 x8 riser card slots (SXB1/SXB2) supported by CPU2	
BaseBoard Management Controller (BMC)	
• ASPEED AST2500 Baseboard Management Controller (BMC) supports IPMI 2.0 • One dedicated IPMI LAN located on the rear I/O back panel	
Graphics	
• Graphics controller via ASPEED AST2500 BMC (BaseBoard Management Controller)	
I/O Devices	
• SATA 3.0	Twelve SATA ports • I-SATA0~7 • S-SATA0~3
• RAID (PCH)	• RAID 0, 1, 5, 10
Peripheral Devices	
• One COM by Micro USB port • Two USB 3.0 ports on the rear I/O panel (USB2/USB3) • Two USB 2.0 connections via one front accessible header (USB0/USB1)	

Motherboard Features
BIOS
• 256Mb Aten BIOS • ACPI 3.0 or later, SPI dual/quad speed support, and SMBIOS 2.7 or later
Power Management
• ACPI power management • Power button override mechanism • Wake-On-LAN • Power-on mode for AC power recovery • Intel Intelligent Power Node Manager 3.0 (available when the Supermicro Power Manager [SPM] is installed and a special power supply is used) • Management Engine (ME)
System Health Monitoring
• Onboard voltage monitoring for +1.8V, +3.3V, +5V, +/-12V, +3.3V standby, +5V standby, HT, memory, chipset temperature, system temperature, and memory temperature • CPU system LED and control • CPU thermal trip support • Status monitor for on/off control • CPU Thermal Design Power (TDP) support of up to 205W (See Note 1 on the next page.)
Fan Control
• Six 4-pin fan headers • Fan status monitoring via IPMI connections • Multi-speed fan control via onboard BMC
System Management
• Trusted Platform Module (TPM) support • PECI (Platform Environment Control Interface) 2.0 support • Power supply monitoring • SuperDoctor® 5, Watch Dog, Non-maskable interrupt (NMI), RoHS • Chassis intrusion header and detection (**Note:** Please connect a cable from the Chassis Intrusion Header at JL1 to the chassis to receive an alert via IPMI.)
LED Indicators
• CPU/Overheating • Power/Suspend-state indicator • Fan failure • UID/remote UID • HDD activity • LAN activity
Dimensions
• 12" (L) x 13" (W) (30.48 mm x 33.02 mm)

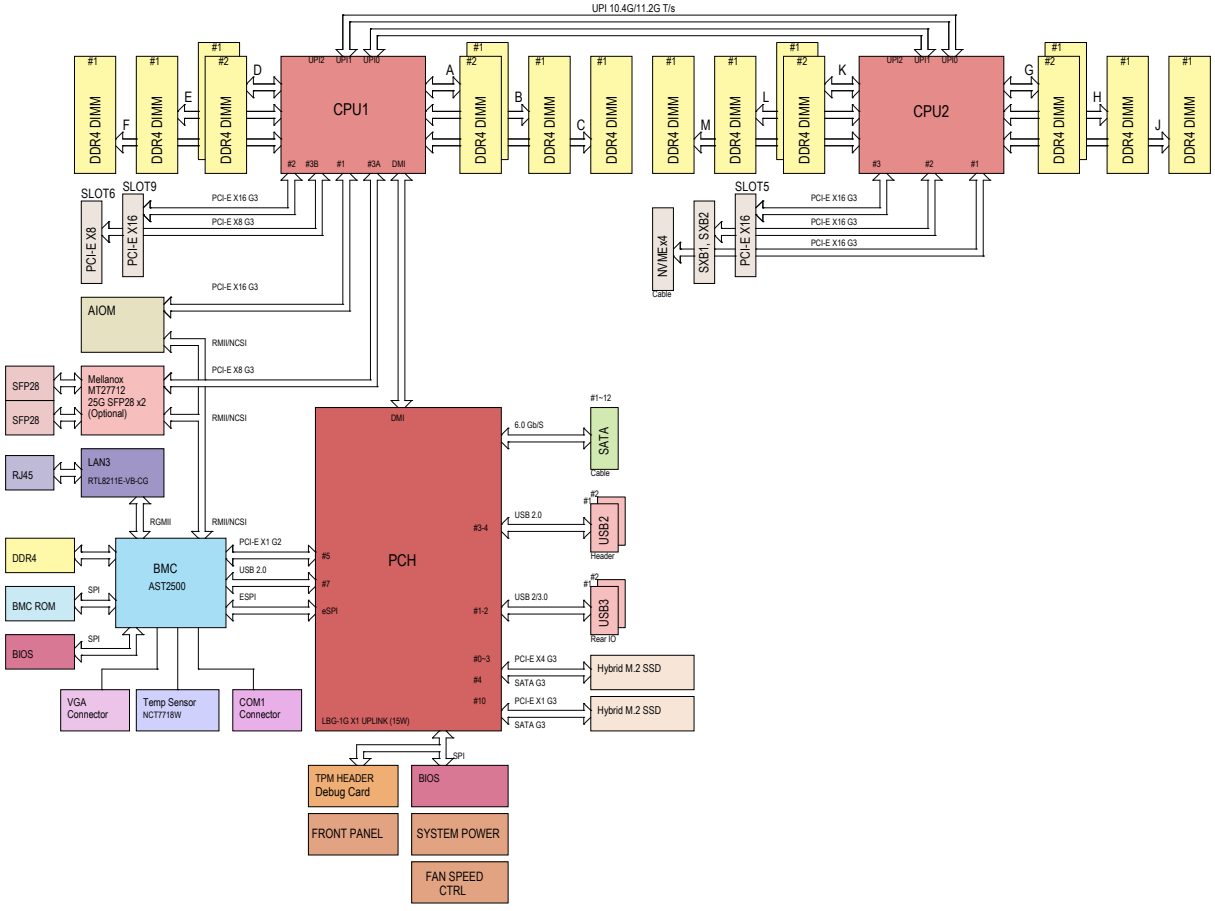
Note 1: The CPU maximum thermal design power (TDP) is subject to chassis and heatsink cooling restrictions. For proper thermal management, please check the chassis and heatsink specifications for proper CPU TDP sizing.

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

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

Note 4: If you purchase a Supermicro Out of Band (OOB) software license key (Supermicro P/N: SFT-OOB-LIC), please DO NOT change the IPMI MAC address.

Figure 1-3.
System Block Diagram



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

1.2 Processor and Chipset Overview

Built upon the functionality and capability of the dual Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP processors (Socket P) with support of Intel C621 chipset, this motherboard provides superb system performance, efficient power management, and a rich feature sets based on cutting-edge technologies to address the needs of next-generation computer users. With support of a 6-channel DDR4 memory controller and up to 28 cores with Hyper-Threading technology, the X11DPD-L/-M25 provides maximal performance, system cooling, and PCIe capacity. This motherboard is optimized for general purpose server platforms.

Features Supported by Intel Xeon Scalable-SP Processors

Intel Xeon Scalable-SP processors support the following features:

- Intel AVX-512 instruction support to handle complex workloads
- 1.5x memory bandwidth increased to 6 channels
- Hot plug and enclosure management with Intel Volume Management Device (Intel VMD)
- Rich set of available IOs with increased PCIe lanes (48 lanes)

New features supported by 2nd Gen Intel Xeon Scalable-SP Processors

2nd Gen Intel Xeon Scalable-SP processors support the following features:

- Higher performance for a wider range of workloads with per-core performance increase
- Support of Optane DC Persistent Memory (DCPMM) with affordable, persistent, and large capacity. Refer to Section 1.8 for details.
- Up to 2993 MHz memory supported
- Vector Neural Network Instruction (VNNI) support for Accelerate Deep Learning & Artificial Intelligence (AI) workloads
- Speed Select Technology provides multiple CPU profiles that can be set in the BIOS. (This feature is available on select CPU SKUs.)
- Seamless hardware security mitigations & performance/frequency flexibility

Note: Support for 2933MHz memory and DCPMM memory is dependent on the CPU SKU.

1.3 Special Features

This section describes the health monitoring features of the X11DPD-L/-M25 motherboard. The motherboard has an onboard ASPEED AST2500 Baseboard Management Controller (BMC) that supports system health monitoring.

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

This section describes the health monitoring features of the X11DPD-L/-M25 motherboard. The motherboard has an onboard Baseboard Management Controller (AST2500) chip that supports system health monitoring.

Onboard Voltage Monitors

The onboard voltage monitor will continuously scan crucial voltage levels. Once a voltage becomes unstable, it will give a warning or send an error message to the IPMI WebGUI and IPMIView. Real time readings of these voltage levels are all displayed in IPMI.

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

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

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

System Resource Alert

This feature is available when used with SuperDoctor 5. SuperDoctor 5 is used to notify the user of certain system events. For example, you can configure SuperDoctor 5 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 on OS support, please refer to our website at www.supermicro.com.

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.

1.7 Advanced Power Management

The following new advanced power management features are supported by the motherboard.

Intel Intelligent Power Node Manager (IPNM)

Intel's Intelligent Power Node Manager (IPNM) provides your system with real-time thermal control and power management for maximum energy efficiency. Although IPNM Specification Version 2.0/3.0 is supported by the BMC (Baseboard Management Controller), your system must also have IPNM-compatible Management Engine (ME) firmware installed to use this feature.

Note: Support for IPNM 2.0/3.0 support is dependent on the power supply used in the system.

Management Engine (ME)

The Management Engine, which is an ARC controller embedded in the IOH (I/O Hub), provides Server Platform Services (SPS) to your system. The services provided by SPS are different from those provided by the ME on client platforms.

1.8 Intel Optane DC Persistent Memory Overview

2nd Gen Intel Xeon Scalable-SP supports new DCPMM (Optane™ DC Persistent Memory Modules) technology that offers data persistence with higher capacity than the existing memory modules and lower latency than NVMe SSDs. DCPMM memory provides hyper-speed storage capability for high performance computing platforms with flexible configuration options.

Chapter 2

Installation

2.1 Static-Sensitive Devices

Electrostatic Discharge (ESD) can damage electronic components. To avoid damaging your motherboard and your system, 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 chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the motherboard.
- Use only the correct type of CMOS onboard battery as specified by the manufacturer. Do not install the CMOS battery upside down, which may result in a 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 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.

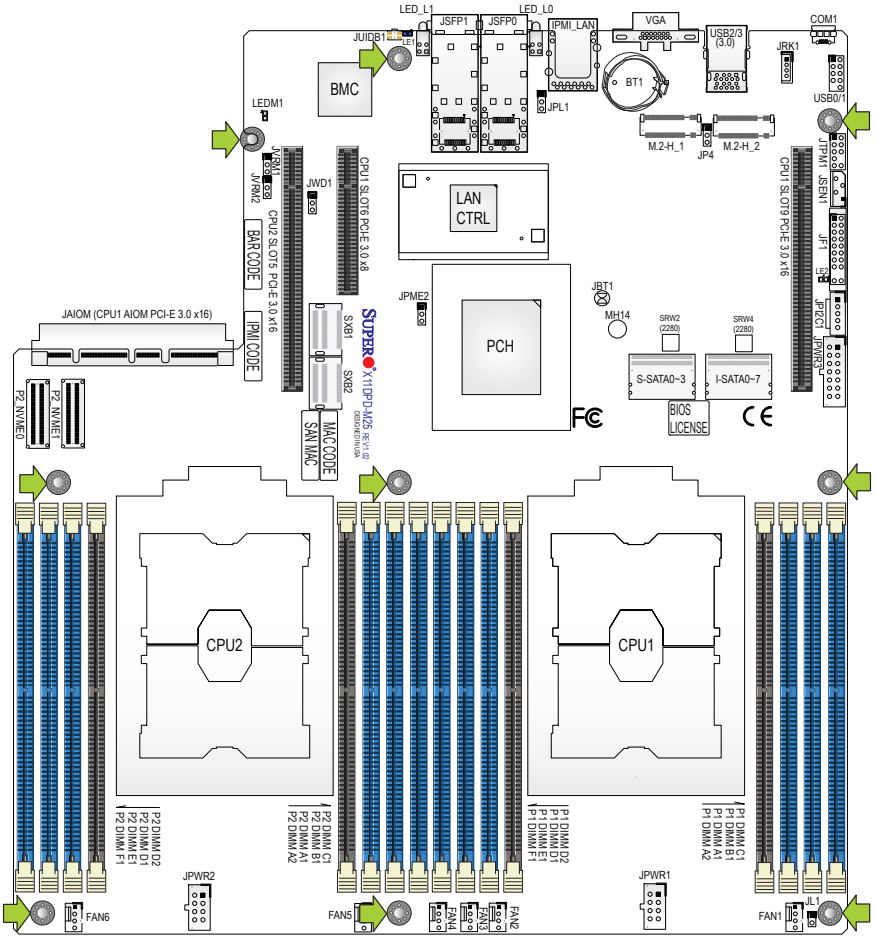
Tools Needed

Phillips Screwdriver (1)

Phillips Screws (9)

Standoffs (9) Only if Needed

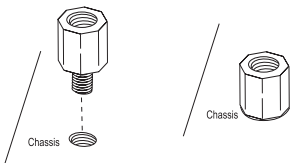
Location of Mounting Holes



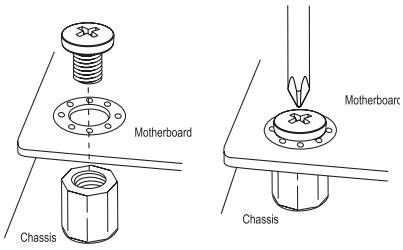
Notes: 1. To avoid damaging the motherboard and its components, please do not use a force greater than 8 lb/inch on each mounting screw during motherboard installation.
2. Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components when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

Installing the Motherboard

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



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



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

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

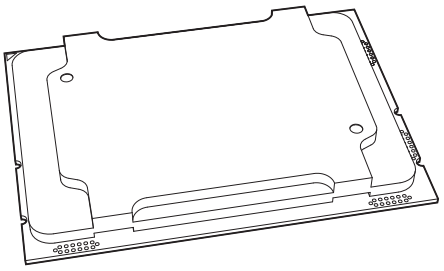
2.3 Processor and Heatsink Installation

Warning: When handling the processor package, avoid placing direct pressure on the label area of the CPU or CPU socket. Also, improper CPU installation or socket misalignment can cause serious damage to the CPU or motherboard which may result in RMA repairs. Please read and follow all instructions thoroughly before installing your CPU and heatsink.

Notes:

- Always connect the power cord last, and always remove it before adding, removing, or changing any hardware components. Please note that the processor and heatsink should be assembled together first to form the Processor Heatsink Module (PHM), and then install the entire PHM into the CPU socket.
- When you receive a motherboard without a processor pre-installed, make sure that the plastic CPU socket cap is in place and that none of the socket pins are bent; otherwise, contact your retailer immediately.
- Refer to the Supermicro website for updates on CPU support.
- Please follow the instructions given in the ESD Warning section on the first page of this chapter before handling, installing, or removing system components.

Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processors



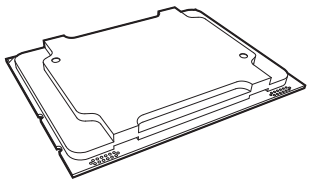
Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processor

Note: All graphics, drawings, and pictures shown in this manual are for illustration only. The components that came with your machine may or may not look exactly the same as those shown in this manual.

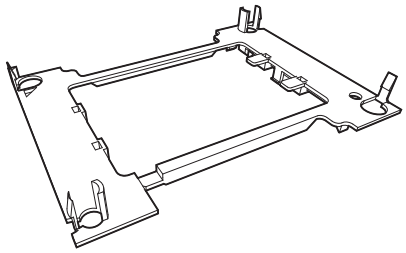
Overview of the Processor Socket Assembly

The processor socket assembly contains 1) Intel Xeon Scalable-SP or 2nd Generation Intel Xeon Scalable-SP processor, 2) the narrow processor clip, 3) the dust cover, and 4) the CPU socket.

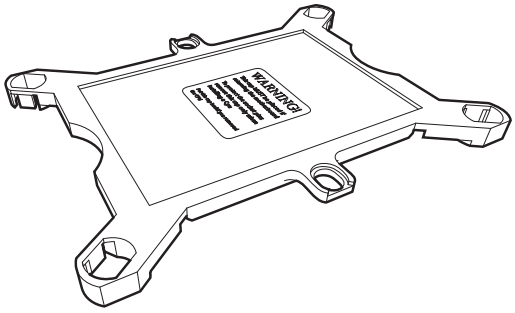
1. Intel Processor



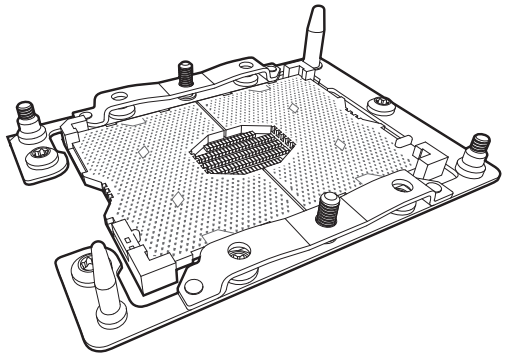
2. Narrow processor clip (the plastic processor package carrier used for the CPU)



3. Dust Cover



4. CPU Socket



Note: Be sure to cover the CPU socket with the dust cover when the CPU is not installed.

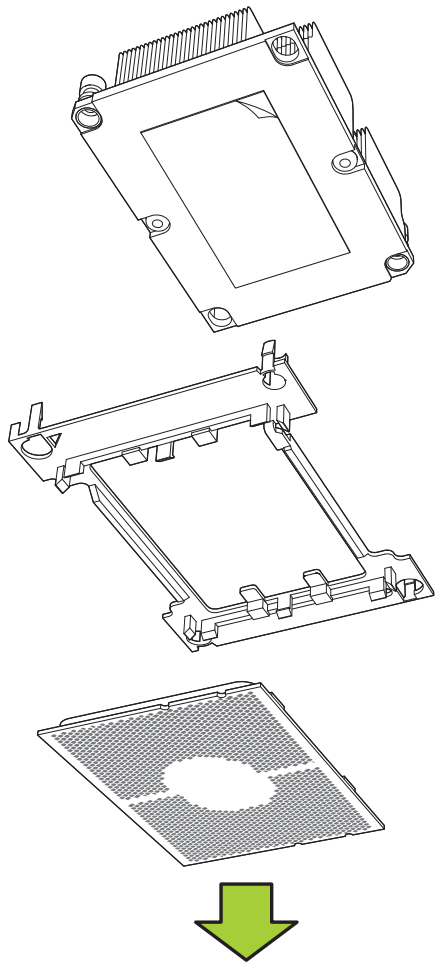
Overview of the Processor Heatsink Module (PHM)

The Processor Heatsink Module (PHM) contains 1) a heatsink, 2) a narrow processor clip, and 3) Intel Xeon Scalable-SP or 2nd Generation Intel Xeon Scalable-SP processor.

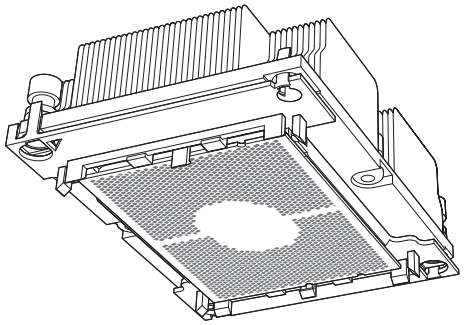
1. Heatsink

2. Narrow processor clip

3. Intel Processor



Processor Heatsink Module (PHM)



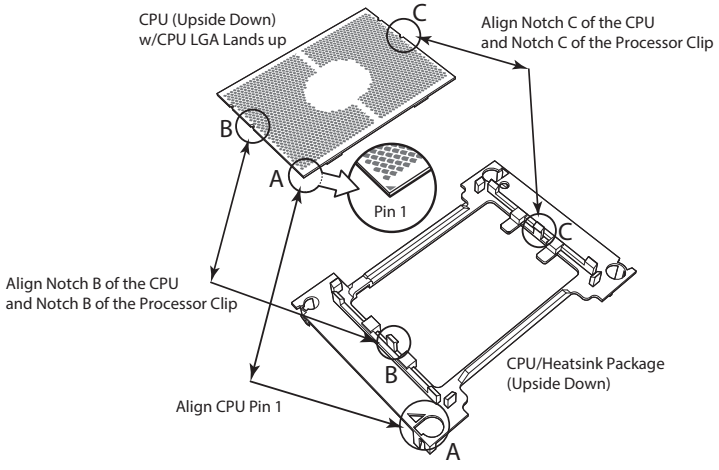
(Bottom View)

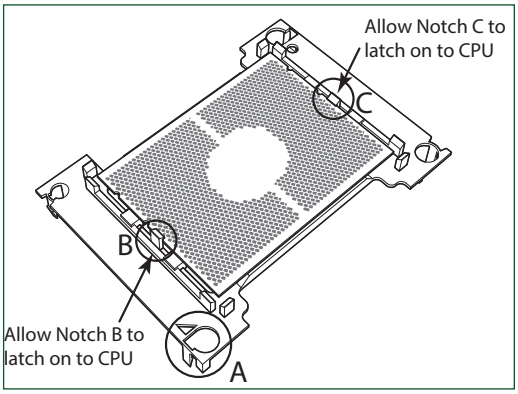
Attaching the Processor to the Narrow Processor Clip to Create the Processor Package Assembly

To properly install the CPU into the narrow processor clip, please follow the steps below.

1. Locate pin 1 (notch A), which is the triangle located on the top of the narrow processor clip. Also locate notch B and notch C on the processor clip.
2. Locate pin 1 (notch A), which is the triangle on the substrate of the CPU. Also, locate notch B and notch C on the CPU as shown below.
3. Align pin 1 (the triangle on the substrate) of the CPU with pin 1 (the triangle) of the narrow processor clip. Once they are aligned, carefully insert the CPU into the processor clip by sliding notch B of the CPU into notch B of the processor clip, and sliding notch C of the CPU into notch C of the processor clip.
4. Examine all corners of the CPU to ensure that it is properly seated on the processor clip. Once the CPU is securely attached to the processor clip, the processor package assembly is created.

Note: Please exercise extreme caution when handling the CPU. Do not touch the CPU LGA-lands to avoid damaging the LGA-lands or the CPU. Be sure to wear ESD gloves when handling components.





Processor Package Carrier (w/CPU mounted on the Processor Clip)

Attaching the Processor Package Assembly to the Heatsink to Form the Processor Heatsink Module (PHM)

After you have made a processor package assembly by following the instructions on the previous page, please follow the steps below to mount the processor package assembly onto the heatsink to create the Processor Heatsink Module (PHM).

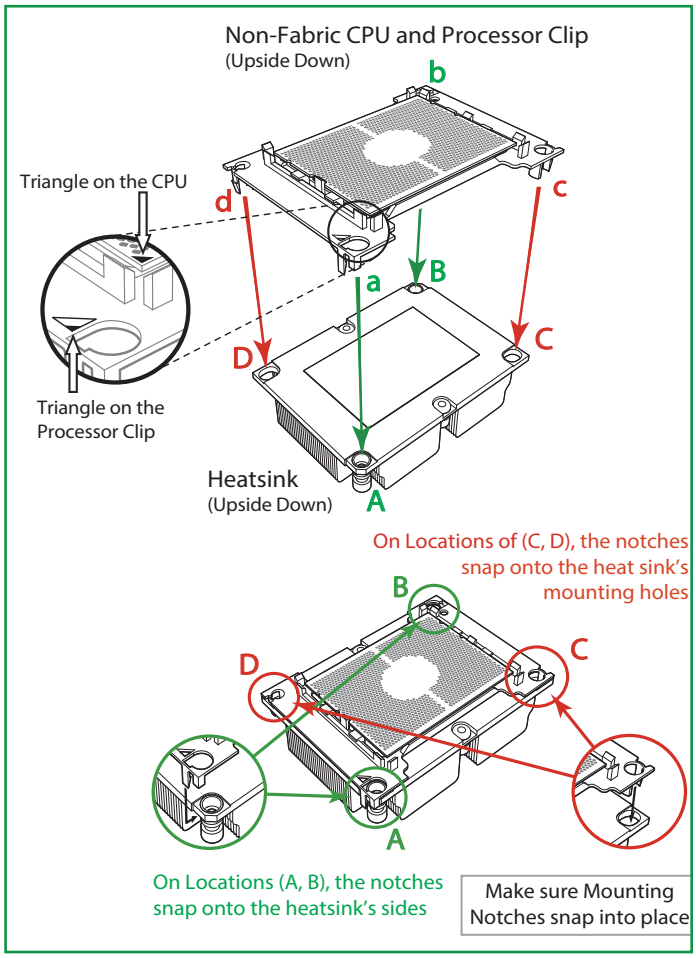
1. Locate "1" on the heatsink label and the triangular corner next to it on the heatsink. With your index finger pressing against the screw at this triangular corner, carefully hold and turn the heatsink upside down with the thermal-grease side facing up. Remove the protective thermal film if present, and apply the proper amount of the thermal grease as needed. (Skip this step if you have a new heatsink because the necessary thermal grease is pre-applied in the factory.)

2. Holding the processor package assembly at the center edge, turn it upside down. With the thermal-grease side facing up, locate the hollow triangle located at the corner of the processor carrier assembly ("a" in the graphic). Note a larger hole and plastic mounting clicks located next to the hollow triangle. Also locate another set of mounting clicks and a larger hole at the diagonal corner of the same (reverse) side of the processor carrier assembly ("b" in the graphic).

3. With the back of heatsink and the reverse side of the processor package assembly facing up, align the triangular corner on the heatsink ("A" in the graphic) against the mounting clips next to the hollow triangle ("a") on the processor package assembly.

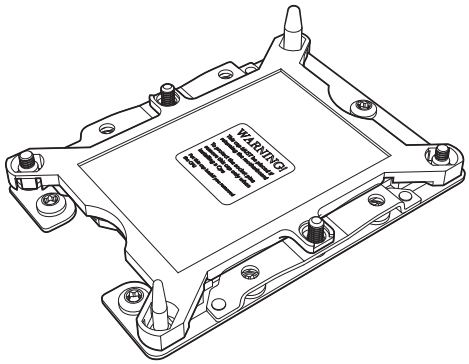
4. Also align the triangular corner ("B") at the diagonal side of the heatsink with the corresponding clips on the processor package assembly ("b").

5. Once the mounting clips on the processor package assembly are properly aligned with the corresponding holes on the back of heatsink, securely attach the heatsink to the processor package assembly by snapping the mounting clips at the proper places on the heatsink to create the processor heatsink module (PHM).



Preparing the CPU Socket for Installation

This motherboard comes with the CPU socket pre-assembled in the factory. The CPU socket contains 1) a dust cover, 2) a socket bracket, 3) the CPU (P) socket, and 4) a back plate. These components are pre-installed on the motherboard before shipping.

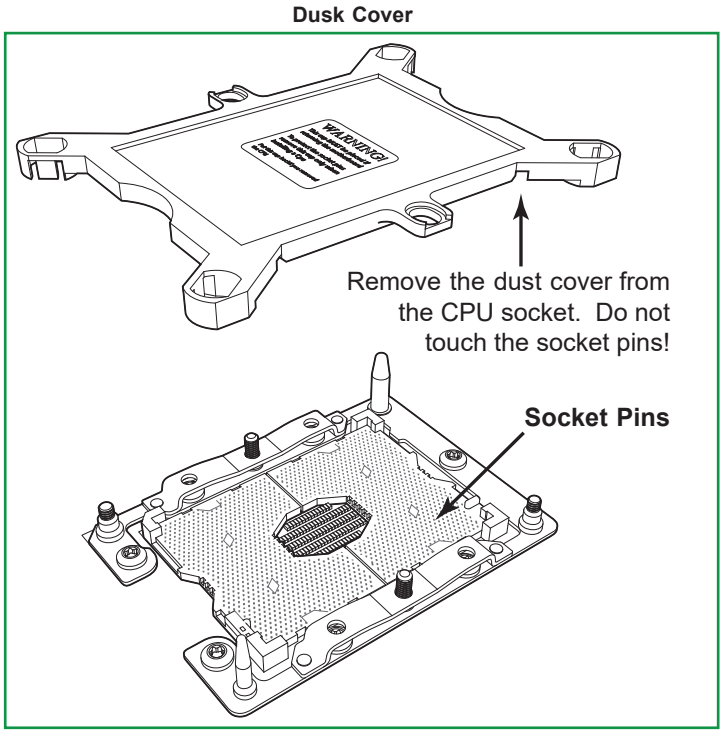


CPU Socket w/Dust Cover On

Removing the Dust Cover from the CPU Socket

Remove the dust cover from the CPU socket, exposing the CPU socket and socket pins as shown on the illustration below.

Note: Do not touch the socket pins to avoid damaging them, causing the CPU to malfunction.



CPU Socket

Installing the Processor Heatsink Module (PHM)

1. Once you have assembled the processor heatsink module (PHM) by following the instructions listed on previsou pages, you are ready to install the processor heatsink module (PHM) into the CPU socket on the motherboard. To install the PHM into the CPU socket, follow the instructions below.

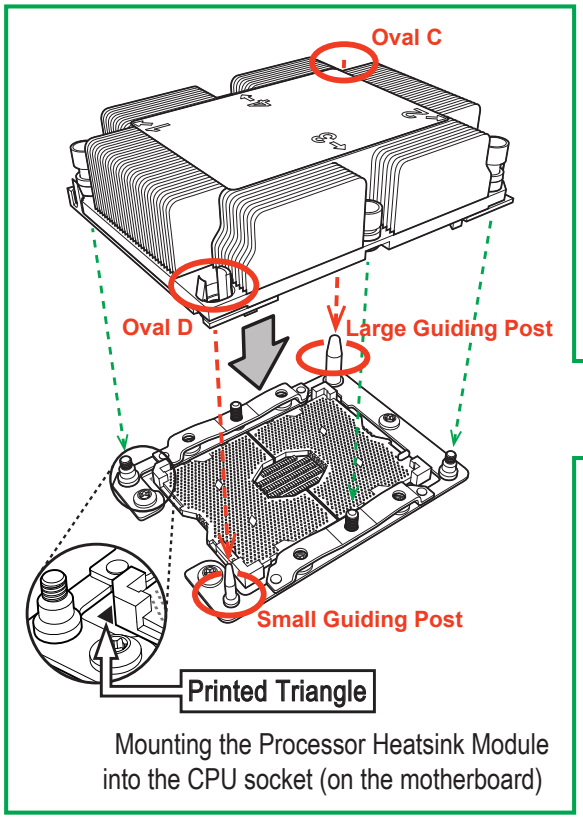
2. Locate the triangle (pin 1) on the CPU socket, and locate the triangle (pin 1) at the corner of the PHM that is closest to "1". (If you have difficulty locating pin 1 of the PHM, turn the PHM upside down. With the LGA-lands side facing up, you will note the hollow triangle located next to a screw at the corner. Turn the PHM right side up, and you will see a triangle marked on the processor clip at the same corner of hollow triangle.)

3. Carefully align pin 1 (the triangle) on the PHM against pin 1 (the triangle) on the CPU socket.

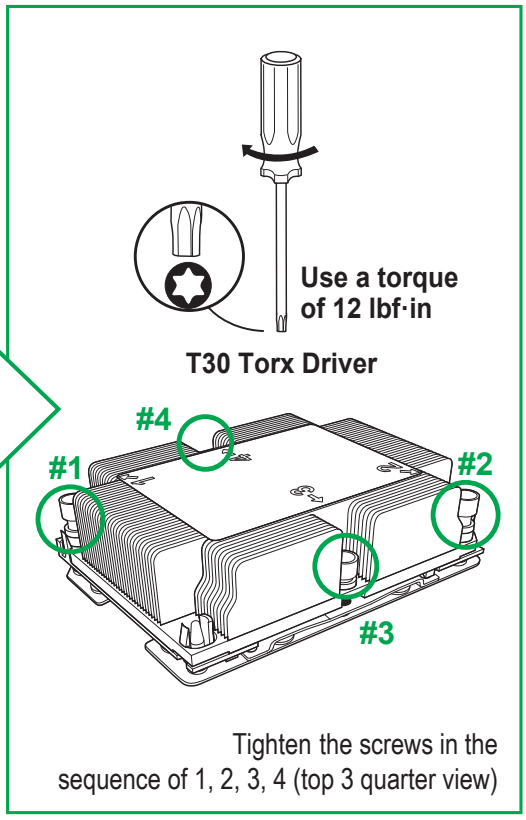
4. Once they are properly aligned, insert the two diagonal oval holes on the heatsink into the guiding posts.

5. Using a T30 Torx-bit screwdriver, install four screws into the mounting holes on the socket to securely attach the PHM onto the motherboard starting with the screw marked "1" (in the sequence of 1, 2, 3, and 4).

Note: Do not use excessive force when tightening the screws to avoid damaging the LGA-lands and the processor.



Mounting the Processor Heatsink Module into the CPU socket (on the motherboard)



Tighten the screws in the sequence of 1, 2, 3, 4 (top 3 quarter view)

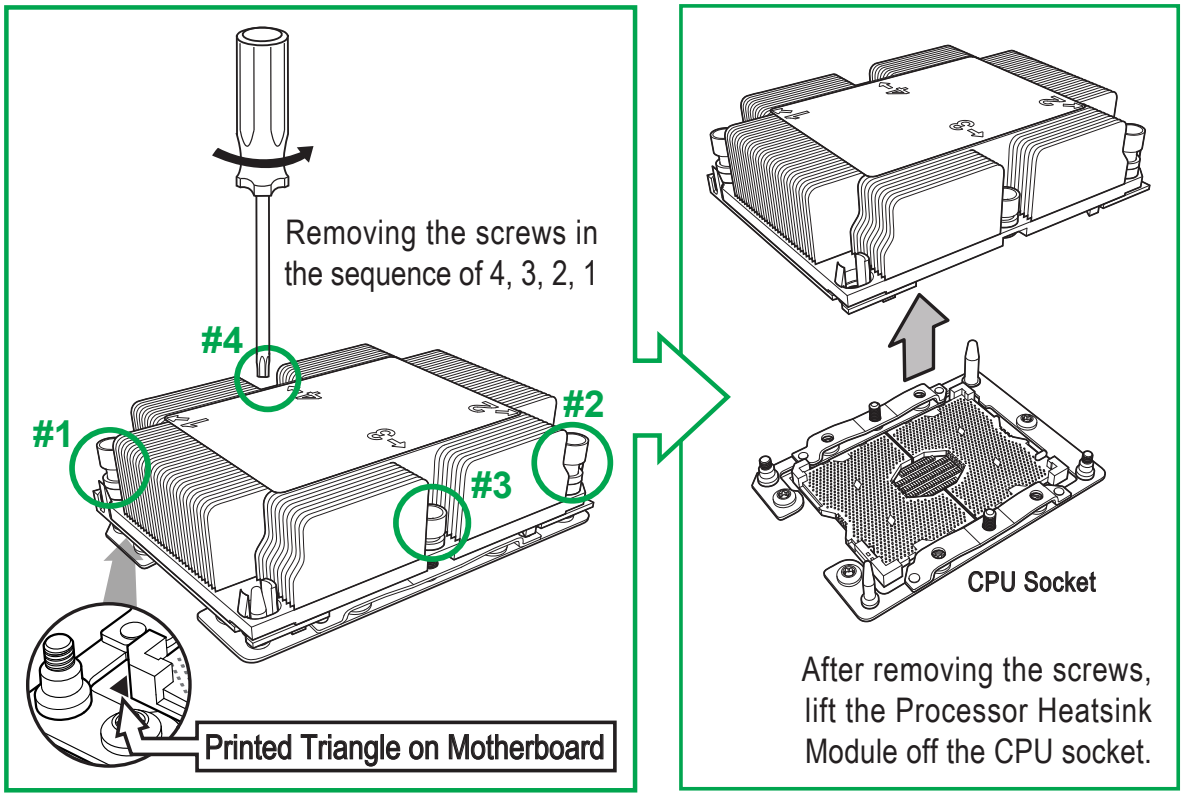
Removing the Processor Heatsink Module (PHM) from the Motherboard

Before removing the processor heatsink module (PHM), unplug power cord from the power outlet.

1. Using a T30 Torx-bit screwdriver, turn the screws on the PHM counterclockwise to loosen them from the socket, starting with screw marked #4 (in the sequence of 4, 3, 2, 1).

2. After all four screws are removed, wiggle the PHM gently and pull it up to remove it from the socket.

Note: To properly remove the processor heatsink module, be sure to loosen and remove the screws on the PHM in the sequence of 4, 3, 2, 1 as shown below.



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 damage.

Memory Support

The X11DPD-L/-M25 supports up to 4TB of 3DS Load Reduced DIMM (3DS LRDIMM), Load Reduced DIMM (LRDIMM), 3DS Registered DIMM (3DS RDIMM), Registered DIMM (RDIMM), Non-Volatile DIMM (NV-DIMM) DDR4(288-pin) ECC 2933*/2666/2400/2133 MHz memory in 16 memory slots. This motherboard also supports up to 2TB memory with DCPMM modules installed based on the DCPMM population table on page 39.

Notes: 1. Be sure to use the memory modules of the same type and speed on the motherboard. Mixing of memory modules of different types and speeds is not allowed. **2.** When installing memory modules, be sure to populate the first DIMM module on the blue memory slot, which is the first memory slot of a memory channel, and then populate the second DIMM in the black slot if 2DPC memory configuration is used. **3.** Memory speed is dependent on the type of processors used in your system. **4.** Populating DDR4 memory modules in a two-DIMMs per-channel (2DPC) configuration on this motherboard will affect memory bandwidth and performance. **5.** Unbalanced memory configuration is not recommended. **6.** Support for 2933MHz memory is dependent on the CPU SKU. **7.** 16Gb-based memory modules are supported by 2nd Gen Intel Xeon Scalable-SP processors only.

Memory Installation Sequence

Memory modules for this motherboard are populated using the "Fill First" method. The blue memory slot of each channel is considered the "first DIMM module" of the channel, and the black slot, the second module of the channel. When installing memory modules, be sure to populate the blue memory slots first and then populate the black slots. To maximize memory capacity and performance, please populate all DIMM slots on the motherboard, including all blue slots and black slots.

General Memory Population Requirements

1. Be sure to use the memory modules of the same type and speed on the motherboard. Mixing of memory modules of different types and speeds is not allowed.

2. Using unbalanced memory topology such as populating two DIMMs in one channel while populating one DIMM in another channel on the same motherboard will result in reduced memory performance.

DDR4 Memory Support for Intel Xeon Scalable-SP Processors

DDR4 Memory Support						
Type	Ranks Per DIMM & Data Width	DIMM Capacity (GB)		Speed (MT/s); Voltage (V); Slots Per Channel (SPC) and DIMMs Per Channel (DPC)		
				1 Slot Per Channel	2 Slots Per Channel	
		DRAM Density		1DPC (1-DIMM Per Channel)	1DPC (1-DIMM Per Channel)	2DPC (2-DIMM Per Channel)
		4Gb*	8Gb	1.2 V	1.2 V	1.2 V
RDIMM	SRx4	4GB	8GB	2666	2666	2666
RDIMM	SRx8	8GB	16GB	2666	2666	2666
RDIMM	DRx8	8GB	16GB	2666	2666	2666
RDIMM	DRx4	16GB	32GB	2666	2666	2666
RDIMM 3Ds	QRX4	N/A	2H-64GB	2666	2666	2666
RDIMM 3Ds	8RX4	N/A	4H-128GB	2666	2666	2666
LRDIMM	QRx4	32GB	64GB	2666	2666	2666
LRDIMM 3Ds	QRX4	N/A	2H-64GB	2666	2666	2666
LRDIMM 3Ds	8Rx4	N/A	4H-128GB	2666	2666	2666

DDR4 Memory Support for 2nd Gen Intel Xeon Scalable-SP Processors

DDR4 Memory Support							
Type	Ranks Per DIMM & Data Width	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); Slots Per Channel (SPC) and DIMMs Per Channel (DPC)		
					1 Slot Per Channel	2 Slots Per Channel	
		DRAM Density			1DPC (1-DIMM Per Channel)	1DPC (1-DIMM Per Channel)	2DPC (2-DIMM Per Channel)
		4Gb*	8Gb	16Gb	1.2 V	1.2 V	1.2 V
RDIMM	SRx4	4GB	8GB	16GB	2933	2933	2933
RDIMM	SRx8	8GB	16GB	32GB	2933	2933	2933
RDIMM	DRx8	8GB	16GB	32GB	2933	2933	2933
RDIMM	DRx4	16GB	32GB	64GB	2933	2933	2933
RDIMM 3Ds	QRX4	N/A	2H-64GB	2H-128GB	2933	2933	2933
RDIMM 3Ds	8RX4	N/A	4H-128GB	4H-256GB	2933	2933	2933
LRDIMM	QRx4	32GB	64GB	128GB	2933	2933	2933
LRDIMM 3Ds	QRX4	N/A	2H-64GB	2H-128GB	2933	2933	2933
LRDIMM 3Ds	8Rx4	N/A	4H-128GB	4H-256GB	2933	2933	2933

Notes: 1. 2933 MHz memory support in two-DIMMs per-channel (2DPC) configuration can be achieved by using memory purchased from Supermicro. **2.** Support for 2933 MHz memory is dependent on the CPU SKU. **3.** 16Gb-based memory modules are supported by 2nd Gen Intel Xeon Scalable-SP processors only.

DIMM Population Guidelines for Optimal Performance

For optimal memory performance, follow the instructions listed in the tables below when populating memory modules.

Key Parameters for DIMM Configuration

Key Parameters for DIMM Configurations	
Parameters	**Possible Values**
Number of Channels	1, 2, 3, 4, 5, or 6
Number of DIMMs per Channel	1DPC (1 DIMM Per Channel) or 2DPC (2 DIMMs Per Channel)
DIMM Type	RDIMM (w/ECC), 3DS RDIMM, LRDIMM, 3DS LRDIMM
DIMM Construction	non-3DS RDIMM Raw Cards: A/B (2Rx4), C (1Rx4), D (1Rx8), E (2Rx8) 3DS RDIMM Raw Cards: A/B (4Rx4) non-3DS LRDIMM Raw Cards: D/E (4Rx4) 3DS LRDIMM Raw Cards: A/B (8Rx4)

DIMM Mixing Guidelines

General DIMM Mixing Guidelines
DIMM Mixing Rules
• All DIMMs must be all DDR4 DIMMs. • x4 and x8 DIMMs can be mixed in the same channel. • Mixing of LRDIMMs and RDIMMs is not allowed in the same channel, across different channels, and across different sockets. • Mixing of non-3DS and 3DS LRDIMM is not allowed in the same channel, across different channels, and across different sockets.

Mixing of DIMM Types within a Channel			
DIMM Types	**RDIMM**	**LRDIMM**	**3DS LRDIMM**
RDIMM	Allowed	Not Allowed	Not Allowed
LRDIMM	Not Allowed	Allowed	Not Allowed
3DS LRDIMM	Not Allowed	Not Allowed	Allowed

DIMM Population Table

Note: Unbalanced memory configuration decreases memory performance and is not recommended for Supermicro motherboards.

Memory Population Table for the Motherboard Using Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processors

Memory Population Table for the X11DP Motherboard w/16 DIMM Slots Onboard	
When 1 CPU is used:	**Memory Population Sequence**
1 CPU & 1 DIMM	CPU1: P1-DIMMA1
1 CPU & 2 DIMMs	CPU1: P1-DIMMA1/P1-DIMMD1
1 CPU & 3 DIMMs	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1
1 CPU & 4 DIMMs	CPU1: P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1
1 CPU & 5 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1
1 CPU & 6 DIMM	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1
1 CPU & 7 DIMMs (Unbalanced: not recommended)	CPU1:P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMA2/P1-DIMMD1/P1-DIMME1/P1-DIMMF1
1 CPU & 8 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME1/P1-DIMMF1
When 2 CPUs are used:	**Memory Population Sequence**
2 CPUs & 2 DIMMs	CPU1: P1-DIMMA1 CPU2: P2-DIMMA1
2 CPUs & 4 DIMMs	CPU1: P1-DIMMA1/P1-DIMMD1 CPU2: P2-DIMMA1/P2-DIMMD1
2 CPUs & 6 DIMMs	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1 CPU2: P2-DIMMC1/P2-DIMMB1/P2-DIMMA1
2 CPUs & 8 DIMMs	CPU1: P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1 CPU2: P2-DIMMB1/P2-DIMMA1/P2-DIMMD1/P2-DIMME1
2 CPUs & 10 DIMMs	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1 CPU2: P2-DIMMB1/P2-DIMMA1/P2-DIMMD1/P2-DIMME1
2 CPUs & 12 DIMMs	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1 CPU2: P2-DIMMC1/P2-DIMMB1/P2-DIMMA1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1
2 CPUs & 14 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMA2/P1-DIMMD1/P1-DIMME1/P1-DIMMF1 CPU2: P2-DIMMC1/P2-DIMMB1/P2-DIMMA1/P2-DIMMA2/P2-DIMMD1/P2-DIMME1/P2-DIMMF1
2 CPUs & 16 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME1/P1-DIMMF1 CPU2: P2-DIMMC1/P2-DIMMB1/P2-DIMMA1/P2-DIMMA2/P2-DIMMD2/P2-DIMMD1/P2-DIMME1/P2-DIMMF1

Note: Please refer to the Memory Configuration User's Guide for the X11 UP/DP/MP motherboards that is posted on our website for detailed information on memory support for this motherboard.

Memory Rank Sparing Tables

Dual Rank Memory Rank Sparing (16GB DIMM)		
Memory Population	**Total RAM Detected**	
	One Rank Configuration	Two Rank Configuration
A1	8GB	8GB
A1+B1	16GB	16GB
A1+B1+C1	24GB	24GB
A1+B1+C1+D1	32GB	32GB
A1+B1+C1+D1+E1	40GB	40GB
A1+B1+C1+D1+E1+F1	49GB	49GB
A1+A2+B1+C1+D1+D2+E1+F1	80GB	64GB

Quad Rank Memory Rank Sparing (64GB DIMM)		
Memory Population	**Total RAM Detected**	
	One Rank Configuration	Two Rank Configuration
A1	48GB	32GB
A1+B1	96GB	64GB
A1+B1+C1	144GB	96GB
A1+B1+C1+D1	192GB	128GB
A1+B1+C1+D1+E1	240GB	160GB
A1+B1+C1+D1+E1+F1	288GB	192GB
A1+A2+B1+C1+D1+D2+E1+F1	416GB	320GB

DCPMM Memory Population Tables for 2nd Gen Intel Xeon Scalable-SP Processors

Note: Only 2nd Gen Intel Xeon Scalable-SP (82xx/62xx/52xx/4215 series) processors support DCPMM memory.

Symmetric Population within 1 CPU Socket									
Modes	**P1-DIMMF1**	**P1-DIMME1**	**P1-DIMMD1**	**P1-DIMMD2**	**P1-DIMMA2**	**P1-DIMMA1**	**P1-DIMMB1**	**P1-DIMMC1**	**Channel Config.**
AD	DRAM1	DRAM1	DRAM1	***DCPMM***	***DCPMM***	DRAM1	DRAM1	DRAM1	**2-1-1**
MM	DRAM2	DRAM2	DRAM2	***DCPMM***	***DCPMM***	DRAM2	DRAM2	DRAM2	**2-1-1**
AD + MM	DRAM3	DRAM3	DRAM3	***DCPMM***	***DCPMM***	DRAM3	DRAM3	DRAM3	**2-1-1**
AD	***DCPMM***	DRAM1	DRAM1	-	-	DRAM1	DRAM1	***DCPMM***	**1-1-1**
MM	***DCPMM***	DRAM1	DRAM1	-	-	DRAM1	DRAM1	***DCPMM***	**1-1-1**
AD + MM	***DCPMM***	DRAM3	DRAM3	-	-	DRAM3	DRAM3	***DCPMM***	**1-1-1**

Asymmetric Population within 1 CPU Socket									
Modes	**P1-DIMMF1**	**P1-DIMME1**	**P1-DIMMD1**	**P1-DIMMD2**	**P1-DIMMA2**	**P1-DIMMA1**	**P1-DIMMB1**	**P1-DIMMC1**	**Channel Config.**
AD	DRAM1	DRAM1	DRAM1	-	***DCPMM***	DRAM1	DRAM1	DRAM1	2-1-1
AD*	DRAM1	DRAM1	DRAM1	-	***DCPMM***	DRAM1	DRAM1	DRAM1	2-1-1

Legend (for the two tables above)					
	DDR4 Type				**Capacity**
DRAM1	RDIMM	3DS RDIMM	LRDIMM	3DS LRDIMM	Refer to Validation Matrix (DDR4 DIMMs validated with DCPMM) below.
DRAM2	RDIMM	-	-	-	
DRAM3	RDIMM	3DS RDIMM	LRDIMM	-	

Note: DDR4 single rank x8 is not available for DCPMM Memory Mode or App-Direct Mode.

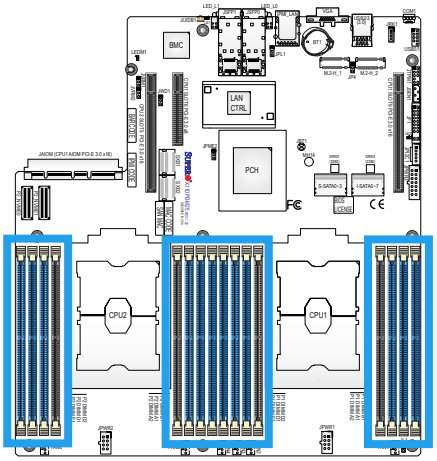
Legend (for the first two tables above)	
Capacity	
DCPMM	Any Capacity (Uniformly for all channels for a given configuration)

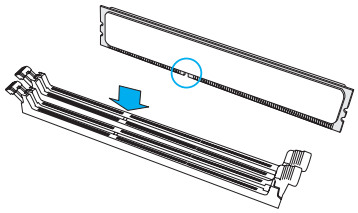
- * 2nd socket has no DCPMM DIMM
- Mode definitions: AD=App Direct Mode, MM=Memory Mode, AD+MM=Mixed Mode
- For MM, general DDR4+DCPMM ratio is between 1:4 and 1:16. Excessive capacity for DCPMM can be used for AD.
- For each individual population, rearrangements between channels are allowed as long as the resulting population is compliant with the X11 memory population rules for the 2nd Gen Intel Xeon Scalable-SP processors.
- For each individual population, please use the same DDR4 DIMM in all slots.
- For each individual population, sockets are normally symmetric with exceptions for 1 DCPMM per socket and 1 DCPMM per node case. Currently, DCPMM modules operate at 2666 MHz.
- No mixing of DCPMM and NVMDIMMs within the same platform is allowed.
- This DCPMM population guide targets a balanced DCPMM-to-DRAM-cache ratio in MM and MM + AD modes.

Validation Matrix (DDR4 DIMMs Validated w/DCPMM)			
DIMM Type	**Ranks Per DIMM & Data Width (Stack)**	**DIMM Capacity (GB)**	
		DRAM Density	
		4Gb	**8Gb**
RDIMM	1Rx4	8GB	16GB
	2Rx8	8GB	16GB
	2Rx4	16GB	32GB
LRDIMM	4Rx4	N/A	64GB
LRDIMM 3DS	8Rx4 (4H)	N/A	128GB

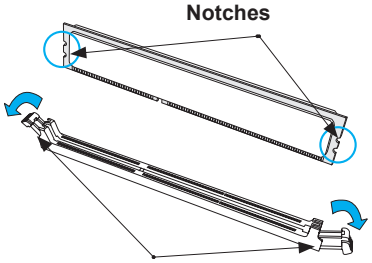
DIMM Installation

1. Insert the desired number of DIMMs into the memory slots, starting with P1 DIMM A1. For the system to work properly, please use memory modules of the same type and speed on the motherboard.
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. Use two thumbs together to press the notches on 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.



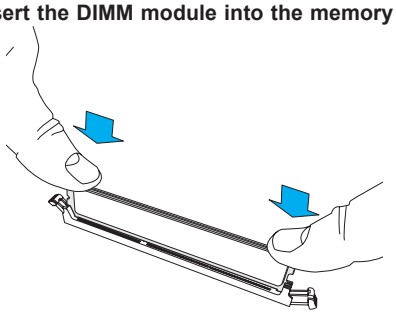


Notches



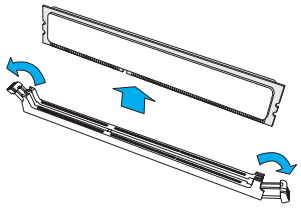
Release Tabs

Insert the DIMM module into the memory slot.



DIMM Module Removal

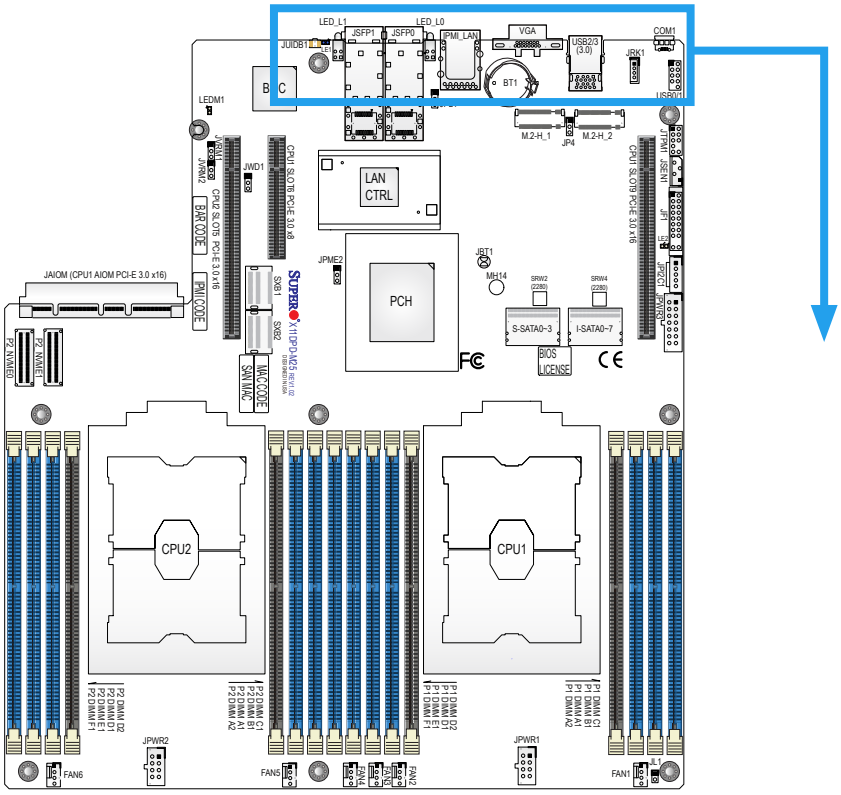
Press the release tabs on both ends of the DIMM socket to release the DIMM module from the socket as shown in the drawing below.



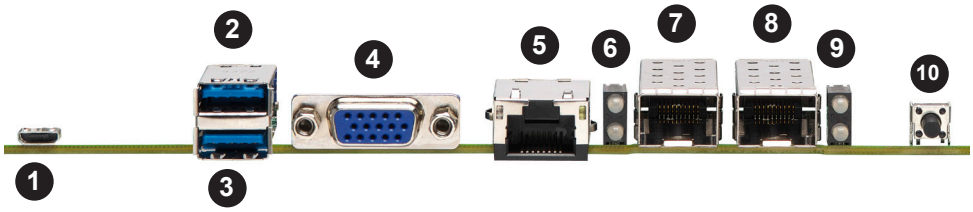
Warnings: 1. Please do not use excessive force when pressing the release tabs on the ends of the DIMM socket to avoid causing any damage to the DIMM module or the DIMM socket. **2.** Please handle DIMM modules with care. Carefully follow all the instructions given on the first page of this chapter to prevent ESD-related damages to your memory modules or components. **3.** Please be sure to remove fan header cable(s) before installing or removing memory module(s).

2.5 Rear I/O Ports

See the figure below for the locations and descriptions of the various I/O ports on the rear of the motherboard.



Rear I/O Port Locations and Definitions



Rear I/O Ports					
#	**Description**	**#**	**Description**	**#**	**Description**
1.	COM1 Port	5.	Dedicated IPMI LAN Port	9.	SFP28 Port 1 Link/Activity LED (LED_L1)
2.	USB2 (3.0)	6.	SFP28 Port 0 Link/Activity LED (LED_L0)	10.	UID Switch (JUIDB1)
3.	USB3 (3.0)	7.	SFP28 Port 0 (JSFP0)		
4.	VGA Port	8.	SFP28 Port 1 (JSFP1)		

Differences between X11DPD-L and X11DPD-M25		
	X11DPD-L	**X11DPD-M25**
25GbE SFP28 Ports and LED Indicators	No	Yes
JPL1	No	Yes

Serial Port

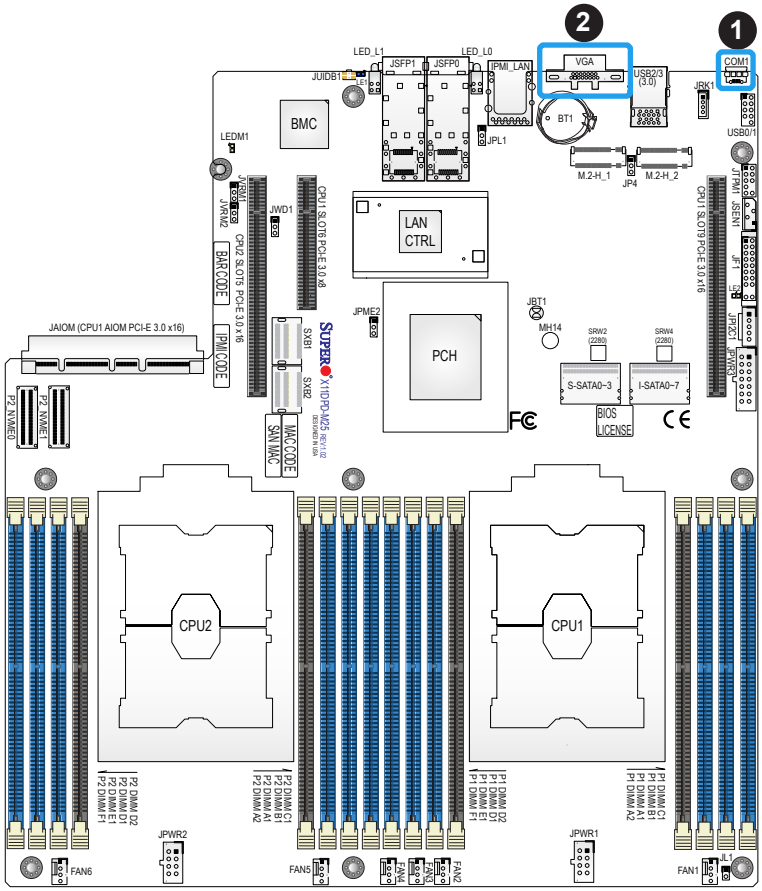
There is one COM port (COM1) on the I/O back panel. The COM port provides serial communication support (micro USB to COM). Refer to the table below for pin definitions.

COM Port Pin Definitions

Pin#	Definition
1	Ground
2	NC
3	USB_P
4	USB_N
5	+5V

VGA Port

One VGA port is located next to IPMI LAN port on the I/O back panel. Use this connection for VGA display.



1. Serial Port
2. VGA Port

Universal Serial Bus (USB) Ports and Headers

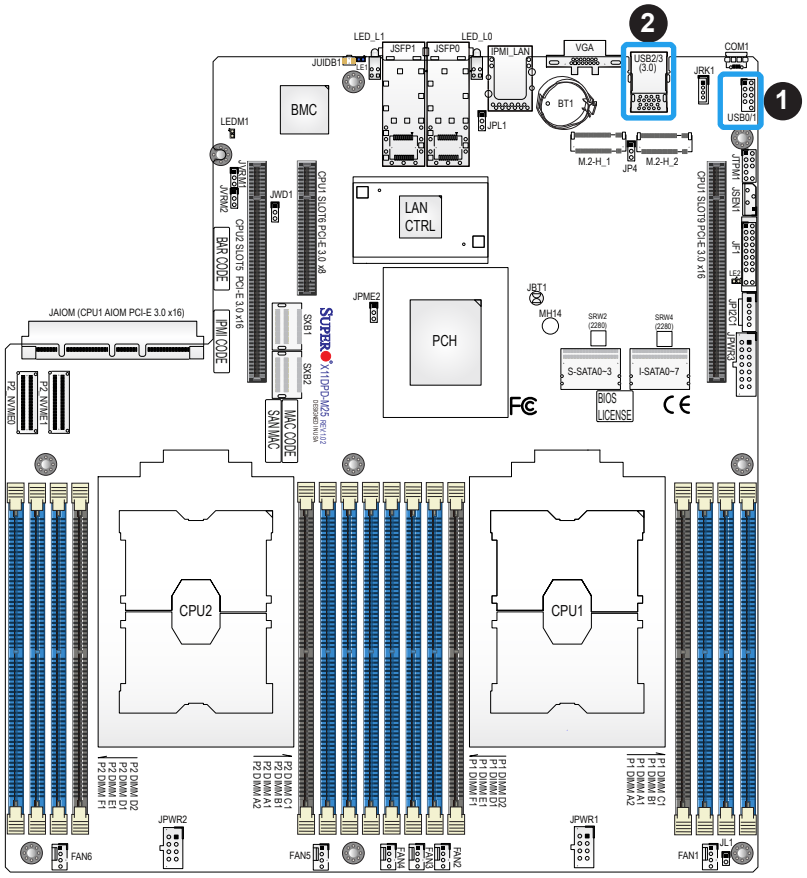
There are two USB 3.0 ports (USB2/3) located on the I/O back panel. The motherboard also has a front access USB 2.0 header that supports two USB connections (USB0/1). The onboard header can be used to provide front side USB access with a cable (not included).

Front Panel USB0/1 (2.0) Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	+5V	2	+5V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	Ground	8	Ground
		10	USB_OC

Back Panel USB2/3 (3.0/2.0) Port Pin Definitions

Pin#	Definition	Pin#	Definition
A1	+5V	B1	+5V
A2	USB_N	B2	USB_N
A3	USB_P	B3	USB_P
A4	Ground	B4	Ground
A5	USB3_RX_N	B5	USB3_RX_N
A6	USB3_RX_P	B6	USB3_RX_P
A7	Ground	B7	Ground
A8	USB3_TX_N	B8	USB3_TX_N
A9	USB3_TX_P	B9	USB3_TX_P



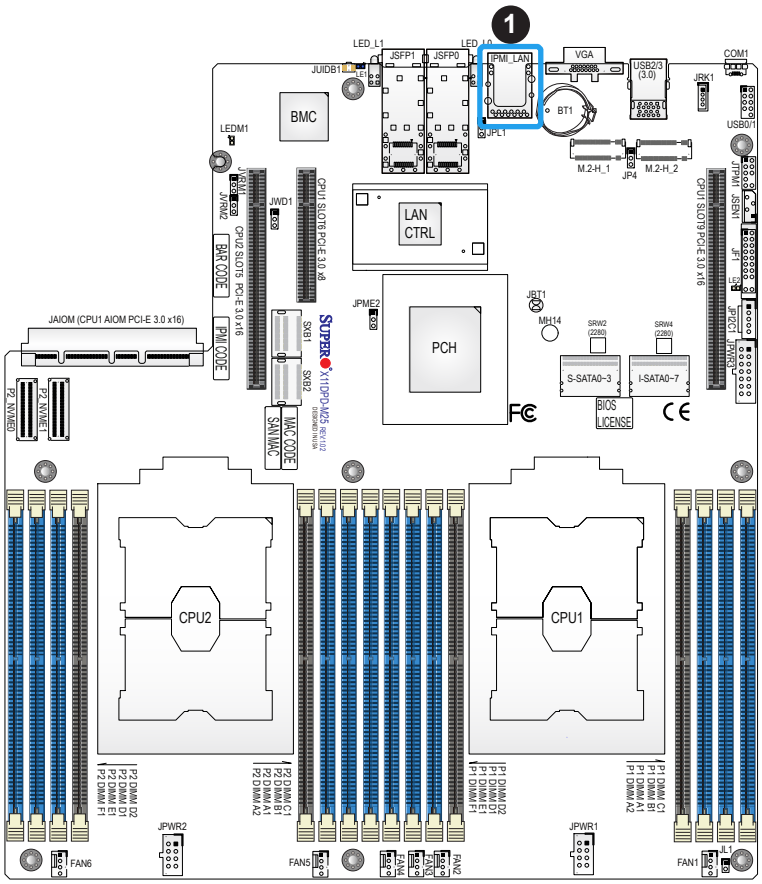
1. USB Header (USB0/1)
2. USB Ports (USB2/3)

IPMI LAN Port

A dedicated IPMI LAN port that supports Gigabit LAN is located next to the VGA port on the back panel. This LAN port is supported by the onboard AST2500 BMC and accepts an RJ45 type cable. Refer to Section 2.9 LED Indicators for LAN LED information.

IPMI LAN Port Pin Definitions

Pin#	Definition	Pin#	Definition
1	D1+	11	D4-
2	D1-	12	CT4
3	CT1	13	ACTIVE LED
4	D2+	14	+3.3V_LAN
5	D2-	15	LINK 1000M LED
6	CT2	16	LINK 100M LED
7	D3+	17	Ground
8	D3-	18	Ground
9	CT3	19	Ground
10	D4+	20	Ground

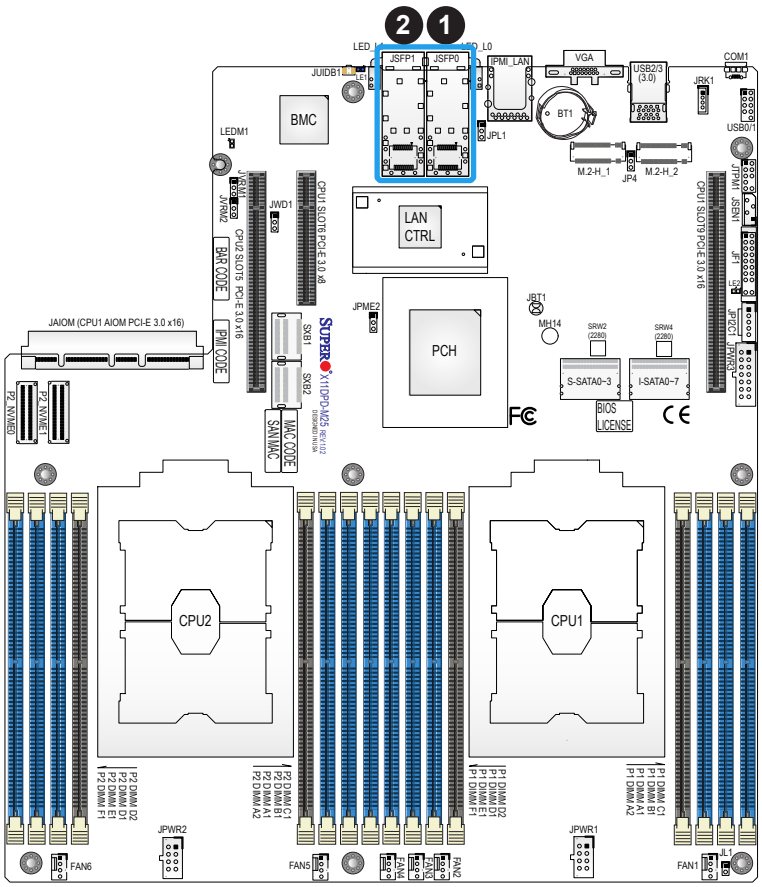


1. IPMI LAN Port

SFP28 Ports (JSFP0/JSFP1)

The motherboard supports two small form factor pluggable (SFP28) optical transceiver ports (JSFP0/JSFP1). These SFP28 ports provide up to 25GbE Ethernet network connections.

SFP28 Port Pin Definitions			
Pin#	**Definition**	**Pin#**	**Definition**
1	Ground	11	Ground
2	TX_Fault	12	SFP+_RX_P
3	TX_Disable	13	SFP+_RX_N
4	I2C_SDA	14	Ground
5	I2C_SCL	15	+3.3V_RX
6	MOD_DEF	16	+3.3V_TX
7	RS0	17	Ground
8	NC	18	SFP+_TX_P
9	RS1	19	SFP+_TX_N
10	Ground	20	Ground



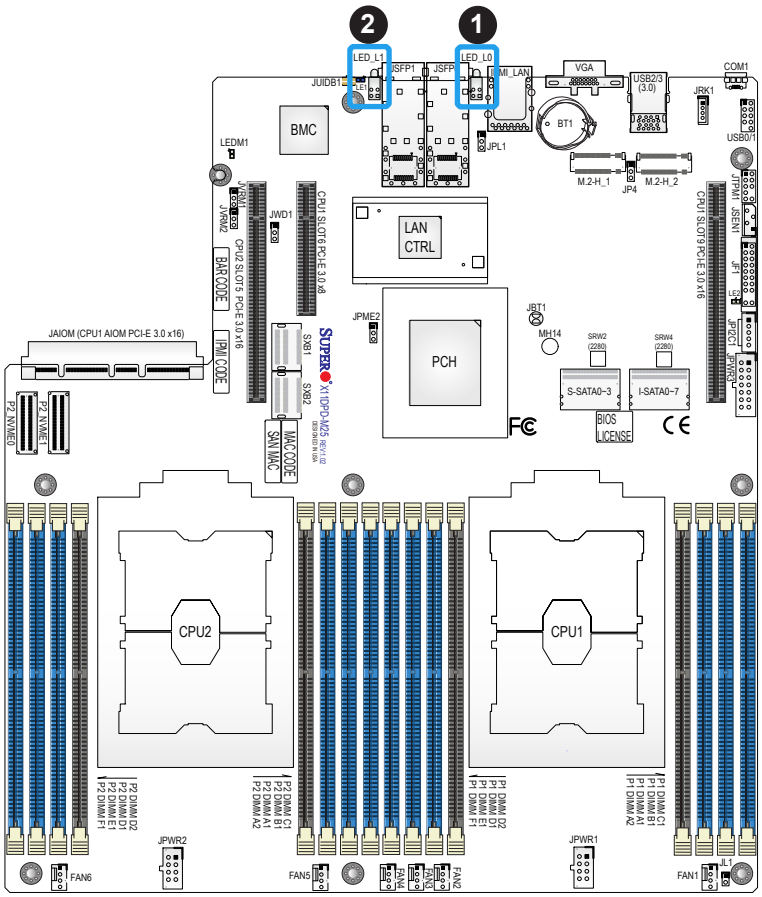
1. SFP28 Port 0 (JSFP0)
2. SFP28 Port 1 (JSFP1)

SFP28 Port Link/Activity LED Indicators (LED_L0/LED_L1)

Two LAN Link/Activity LED indicators are located at LED_L0 and LED_L1. LED_L0 indicates the SFP28 port 0 connection. LED_L1 indicates the SFP28 port 1 connection. Refer to the tables below for more information.

SFP28 Port Activity LED Indicator Assignment/State	
LED	**LAN Port Assigned**
LED_L0	SFP28 Port 0 Active
LED_L1	SFP28 Port 1 Active
Blinking Green	SFP28 LAN Port Active

SFP28 Port Link LED Indicator LED State	
LED Color	**Definition**
Solid Yellow	10 Gbps/ 1 Gbps
Solid Green	25 Gbps



1. SFP28 Port 0 Link/Activity LEDs (LED_L0)
2. SFP28 Port 1 Link/Activity LEDs (LED_L1)

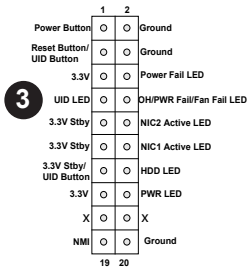
Unit Identifier Switch/ UID LED Indicator

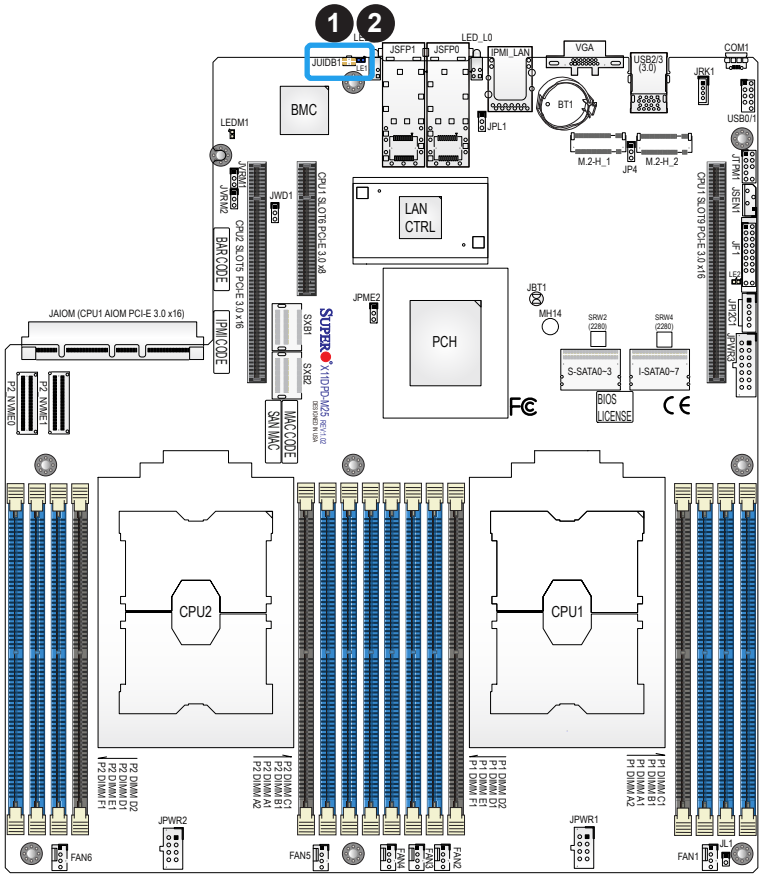
A rear Unit Identifier (UID) switch (JUIDB1) and an rear UID LED indicator (LE1) are located on the rear side of the motherboard. The front UID LED is located on Pin 7 of the Front Control Panel (JF1). When you press the UID switch, both front and rear UID LED indicators will be turned on. Press the UID switch again to turn off the LEDs. The UID Indicators provide easy identification of a system unit that may be in need of service.

Note: UID can also be triggered via IPMI on the motherboard. For more information on IPMI, please refer to the IPMI User's Guide posted on our website at http://www.supermicro.com.

UID Switch Pin Definitions	
Pin#	**Definition**
1	Ground
2	Ground
3	Button In
4	Button In

UID LED Indicator	
LED Color	**Definition**
Blue: On	Unit Identified

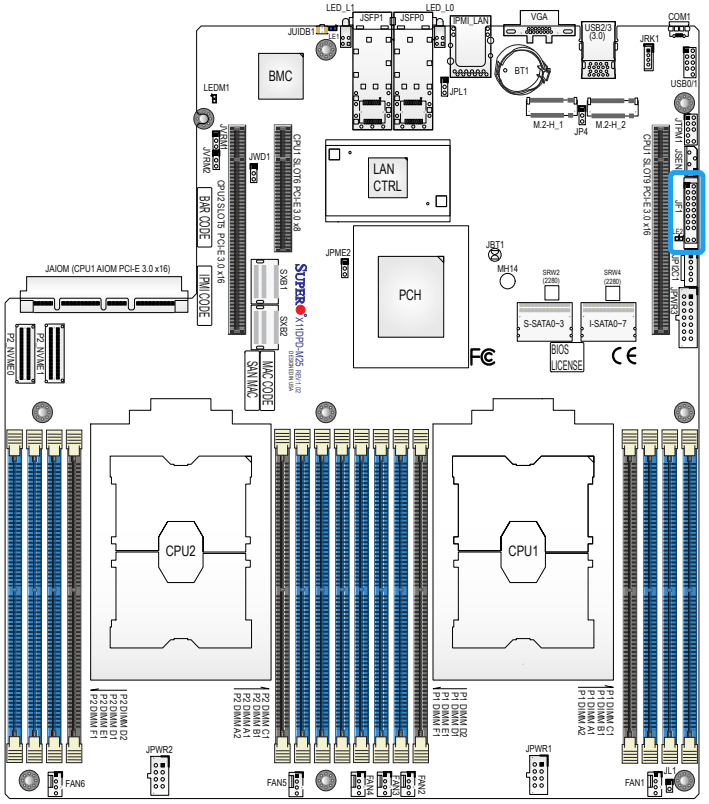




1. UID Switch
2. Rear UID LED
3. Front UID LED

2.6 Front Control Panel

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. See the figure below for the descriptions of the front control panel buttons and LED indicators.



	1	2	
Power Button	○	○	Ground
Reset Button/ UID Button	○	○	Ground
3.3V	○	○	Power Fail LED
UID LED	○	○	OH/PWR Fail/Fan Fail LED
3.3V Stby	○	○	NIC2 Active LED
3.3V Stby	○	○	NIC1 Active LED
3.3V Stby/ UID Button	○	○	HDD LED
3.3V	○	○	PWR LED
X	○	○	X
NMI	○	○	Ground
	19	20	

JF1 Header Pins

Power Button

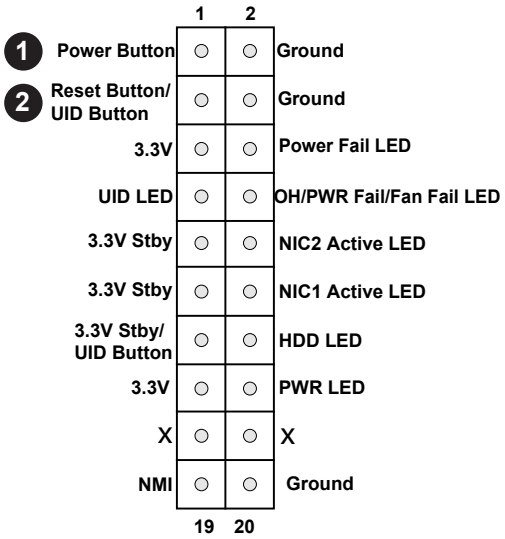
The Power Button connection is located on pins 1 and 2 of JF1. Momentarily contacting both pins will power on/off the system. This button can also be configured to function as a suspend button (with a setting in the BIOS - see Chapter 4). To turn off the power in the suspend mode, press the button for four seconds or longer. Refer to the table below for pin definitions.

Power Button Pin Definitions (JF1)	
Pin#	**Definition**
1	Signal
2	Ground

Reset Button/UID Button

The Reset Button/UID Button connection is located on pins 3 and 4 of JF1. Attach it to a hardware reset switch on the computer case to reset the system or use JP4 to set the function of pin 3 of JF1. Refer to JF1 Pin 3 Function Selection on page 65 for more information on JP4.

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



1. PWR Button
2. Reset Button/UID Button

Power Fail LED

The Power Fail LED connection is located on pins 5 and 6 of JF1. Refer to the table below for pin definitions.

Power Fail LED Pin Definitions (JF1)	
Pin#	**Definition**
5	3.3V
6	PWR Supply Fail

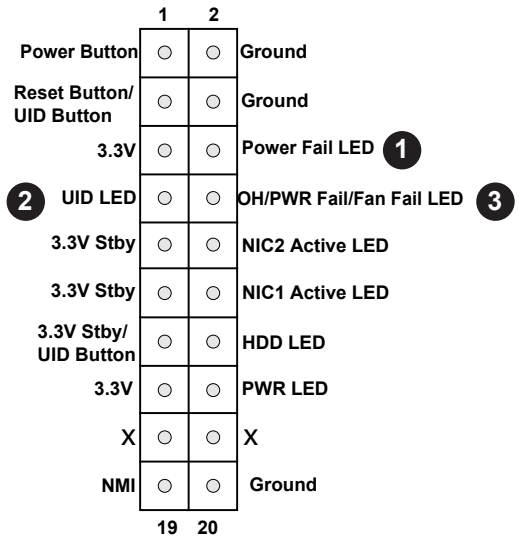
UID/Overheat(OH)/Fan Fail/PWR Fail LED

Connect an LED cable to pins 7 and 8 of the Front Control Panel(JF1) to use UID/Overheat/ Fan Fail/Power Fail LED connections. The LED on pin 8 provides warnings of overheat, power failure or fan failure. Refer to the tables below for more information.

Information LED (UID/OH/PWR Fail/Fan Fail LED) Pin Definitions (Pin 7 & Pin 8 of JF1)	
Pin#	**Definition**
7	Blue UID LED
8	OH/Fan Fail/PWR Fail LED

Information LED (UID/OH/PWR Fail/Fan Fail LED) State Definitions (Pin 7 & Pin 8 of JF1)	
State	**Definition**
Off	Normal
On	Overheat
Flashing	Fan Fail

Information LED (UID/OH/PWR Fail/Fan Fail LED) Pin Definitions (Pin 7 & Pin 8 of JF1)	
Status	**Description**
Solid red	An overheat condition has occurred. (This may be caused by cable congestion).
Blinking red (1Hz)	Fan failure: check for an inoperative fan.
Blinking red (0.25Hz)	Power failure: check for a non-operational power supply
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 (300 msec)	Remote UID is on. Use this function to identify a unit from a remote location that might be in need of service.



1. Power Fail LED
2. UID LED
3. OH/PWR Fail/Fan Fail LED

NIC1/NIC2 (LAN1/LAN2)

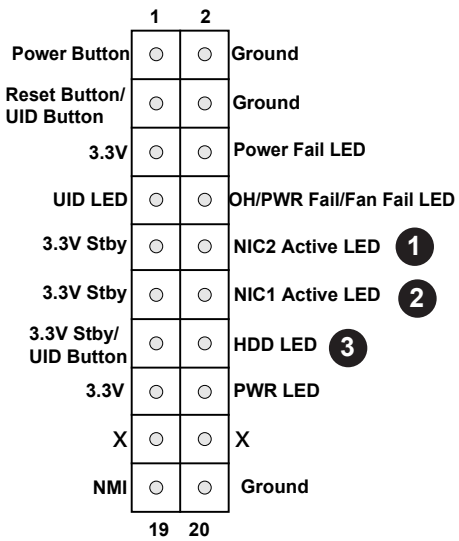
The NIC (Network Interface Controller) LED connection for LAN port 1 is located on pins 11 and 12 of JF1, and LAN port 2 is on pins 9 and 10. Attach the NIC LED cables here to display network activity. Refer to the table below for pin definitions.

LAN1/LAN2 LED Pin Definitions (JF1)	
Pin#	**Definition**
10	NIC2 Activity LED
12	NIC1 Activity LED

HDD LED

The HDD LED connection is located on pins 13 and 14 of JF1. Attach a cable here to indicate the status of HDD-related activities, including IDE, SATA activities. Refer to the table below for pin definitions.

HDD LED Pin Definitions (JF1)	
Pin#	**Definition**
13	3.3V Stby/UID Button
14	HDD Active



1. NIC2 Activity LED
2. NIC1 Activity LED
3. HDD LED

Power LED

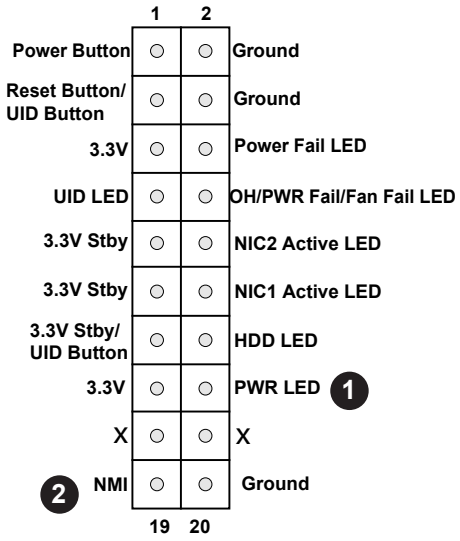
The Power LED connection is located on pins 15 and 16 of JF1. Refer to the table below for pin definitions.

Power LED Pin Definitions (JF1)	
Pin#	**Definition**
15	3.3V
16	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)	
Pin#	**Definition**
19	NMI
20	Ground



1. Power LED
2. NMI

2.7 Connectors

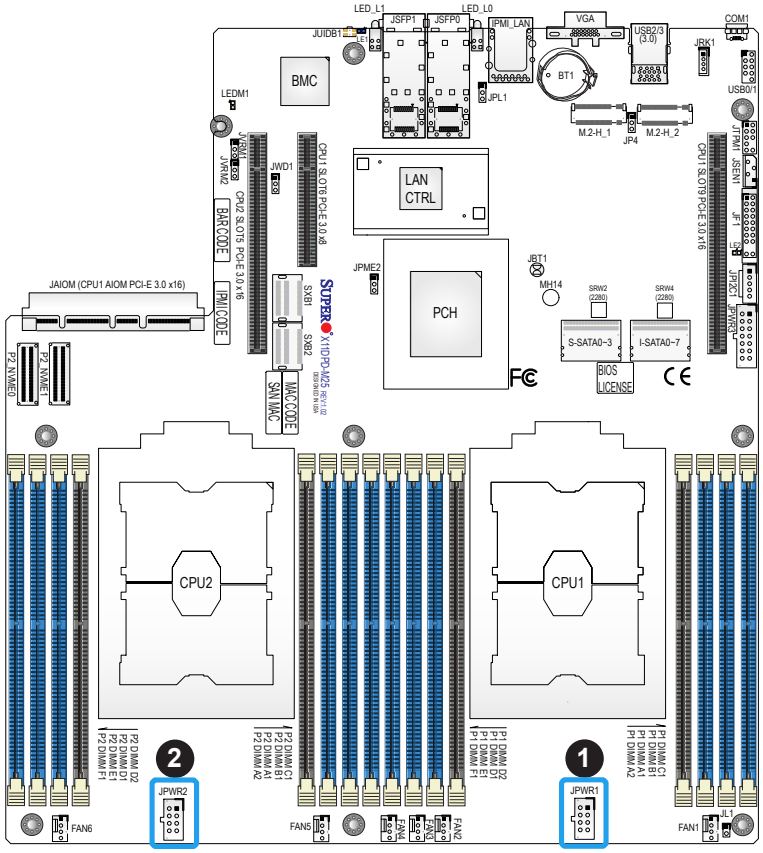
Power Connector

12V 8-pin CPU Power Connectors

JPWR1 and JPWR2 are the 8-pin 12V DC power input for the CPU or alternative single power source for a special enclosure when the 14-pin ATX power is not in use. Refer to the table below for pin definitions.

12V 8-pin Power Connector Pin Definitions

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



1. 8-pin Power Connector (JPWR1) (Required)
2. 8-pin Power Connector (JPWR2) (Required)

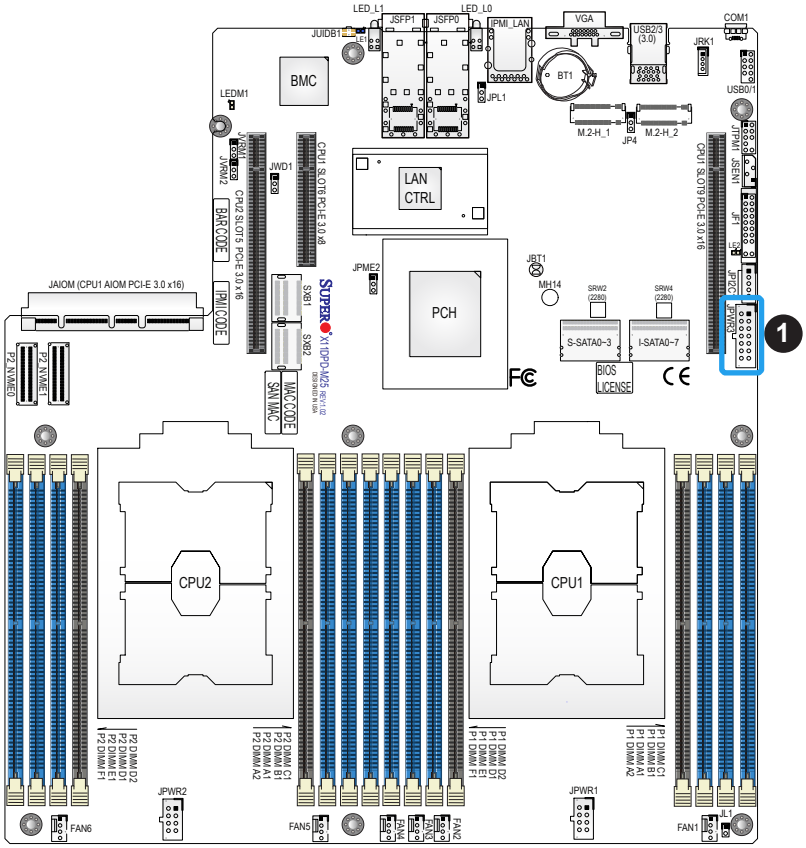
Main ATX Power Supply Connector

The primary power supply connector (JPWR3) used on the motherboard is via 14-pin ATX power connection. It is also required to connect 8-pin power connectors (JPWR1/JPWR2) to the power supply.

Warning: To provide adequate power to your system and to avoid damaging the power supply or the motherboard, be sure to connect all power connectors mentioned above to the power supply. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.

14-pin Power Connector (JPWR3)
Pin Definitions

Pin#	Definition	Pin#	Definition
1	Ground	8	+12V
2	Ground	9	+12V
3	Ground	10	+12V
4	Ground	11	+12V
5	Ground	12	+12V
6	Ground	13	+12V_STBY
7	PWROK (Input, open drain pull high to 3.3V)	14	PS_ON (Output, open drain pull down to Ground)



1. 14-pin ATX Power Connector (Required)

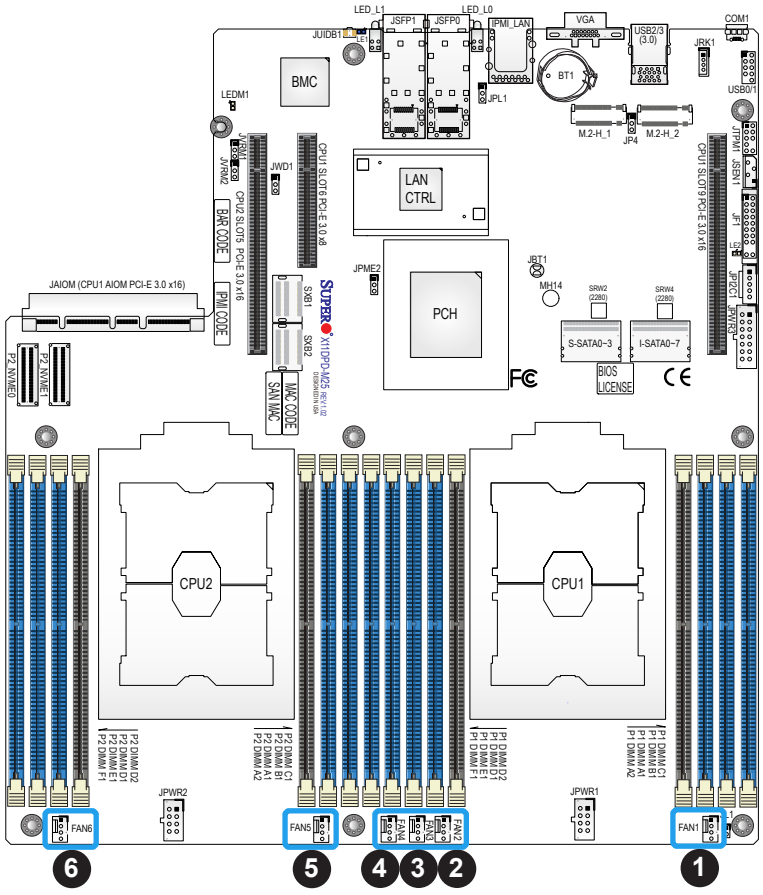
Headers

Fan Headers

There are six fan headers on the motherboard. These are 4-pin fan headers; pins 1-3 are backward compatible with traditional 3-pin fans. The onboard fan speeds are controlled by Thermal Management via the BMC (or by IPMI). When using Thermal Management setting, please use all 3-pin fans or all 4-pin fans.

Fan Header Pin Definitions

Pin#	Definition
1	Ground (Black)
2	+12V (Red)
3	Tachometer
4	PWM Control



1. FAN Header 1
2. FAN Header 2
3. FAN Header 3
4. FAN Header 4
5. FAN Header 5
6. FAN Header 6

AIOM Slot

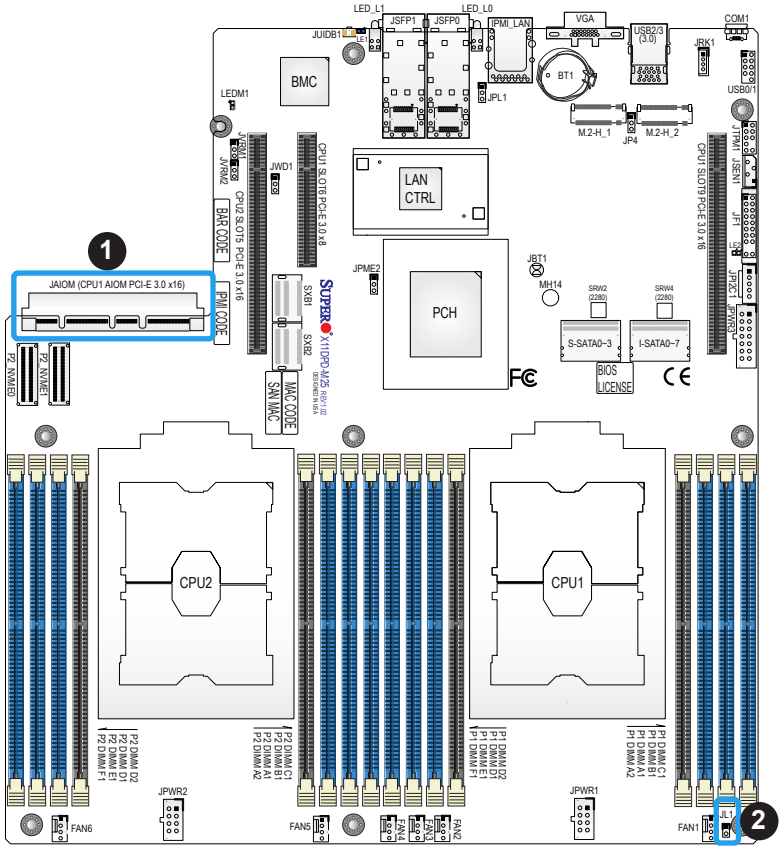
The Supermicro Advanced I/O Module (AIOM) PCIe 3.0 x16 slot (JAIOM) can be utilized to offer additional LAN ports, VPU, storage devices, etc. on the motherboard. Please visit the Supermicro website for all available module options. Also, please note that it is mandatory to unplug power cords prior to removing or installing an AIOM module card.

Chassis Intrusion

A Chassis Intrusion header is located at JL1 on the motherboard. Connect an appropriate cable from JL1 to the chassis so that you can be informed of a chassis intrusion (via IPMI) when the system case is opened. Refer to the table below for pin definitions.

Chassis Intrusion Pin Definitions

Pins	Definition
1	Intrusion Input
2	Ground



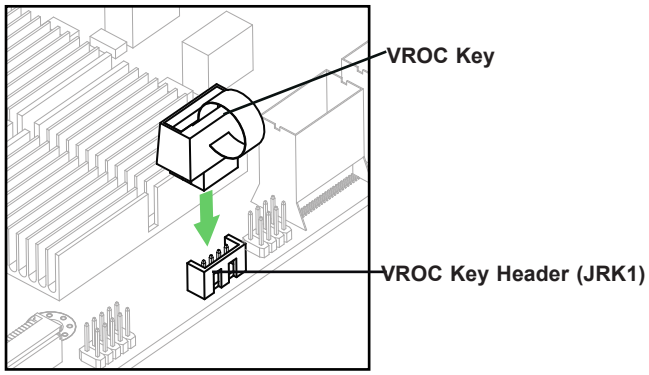
1. AIOM Slot (JAIOM)
2. Chassis Intrusion Header

VROC RAID Key Header

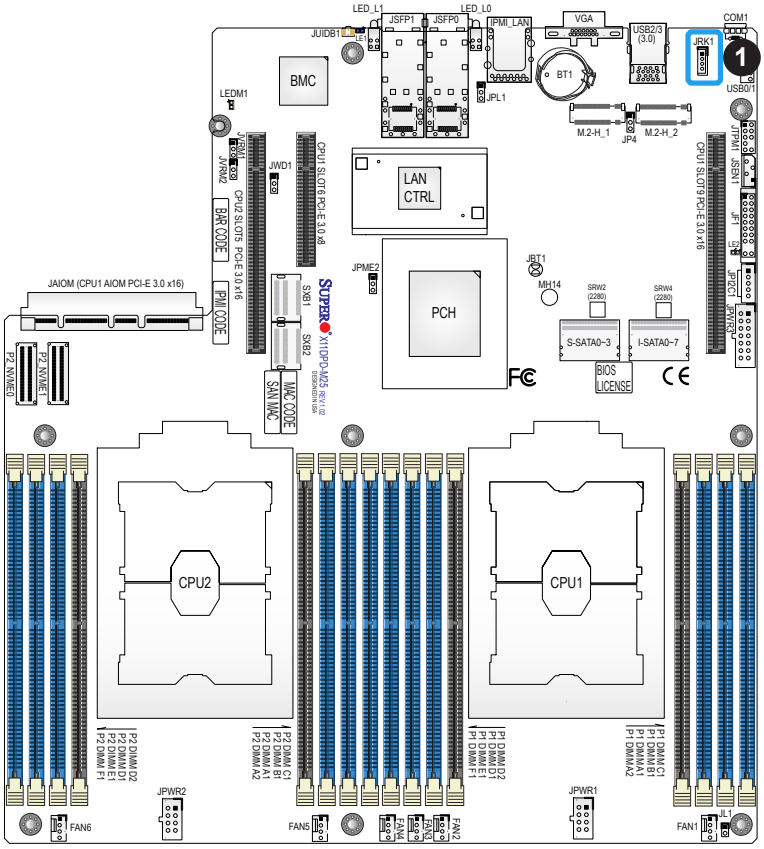
A VROC RAID Key header is located at JRK1 on the motherboard. Install a VROC RAID Key on JRK1 for NVMe RAID support as shown in the illustration below. Refer to the layout below for the location of JRK1.

Note: Enable the VROC Key is required when using the RAID function.

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

Inlet Sensor Header

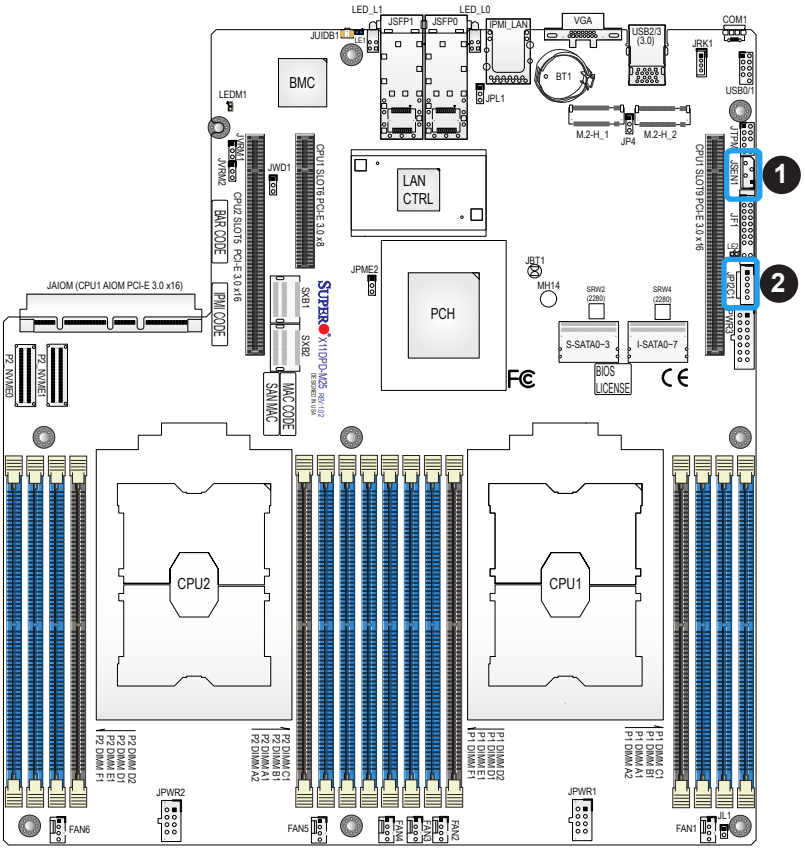
This header (JSEN1) allows BMC to monitor thermal inlet temperature. A special module is required. Please contact Supermicro at www.supermicro.com to purchase the module for this header. Refer to the table below for pin definitions.

Inlet Sensor Header Pin Definitions	
Pin#	**Definition**
1	SMBDAT
2	Ground
3	SMBCLK
4	3.3V STBY

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



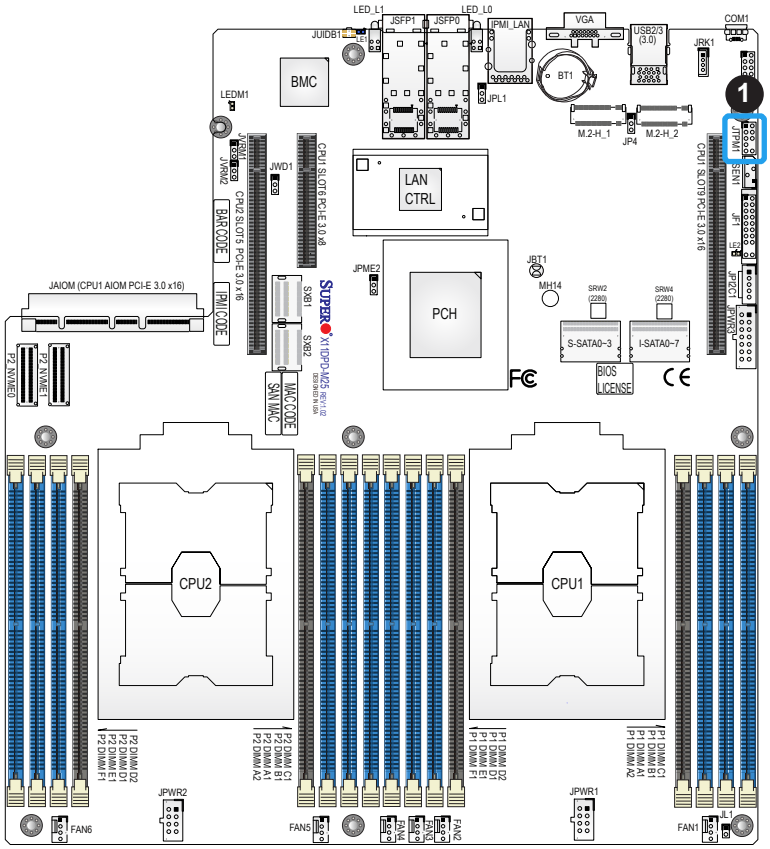
1. Inlet Sensor Header (JSEN1)
2. Power SMB Header

TPM/Port 80 Header

The JTPM1 header is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from Supermicro (optional). A TPM/Port 80 header is a security device that supports encryption and authentication in hard drives. It allows the motherboard to deny access if the TPM associated with the hard drive is not installed in the system. Refer to the table below for pin definitions.

Trusted Platform Module/Port 80 Header Pin Definitions

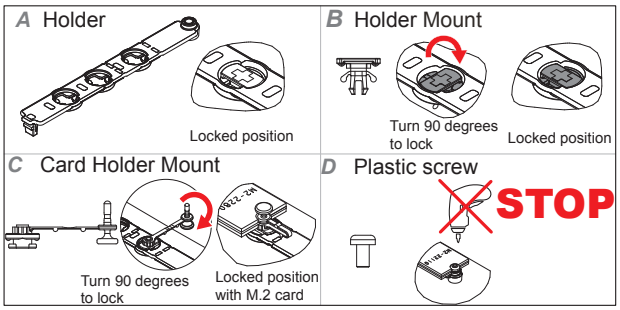
Pin#	Definition	Pin#	Definition
1	+3.3V	2	SPI_CS#
3	RESET#	4	SPI_MISO
5	SPI_CLK	6	GND
7	SPI_MOSI	8	
9	+3.3V Stdby	10	SPI_IRQ#

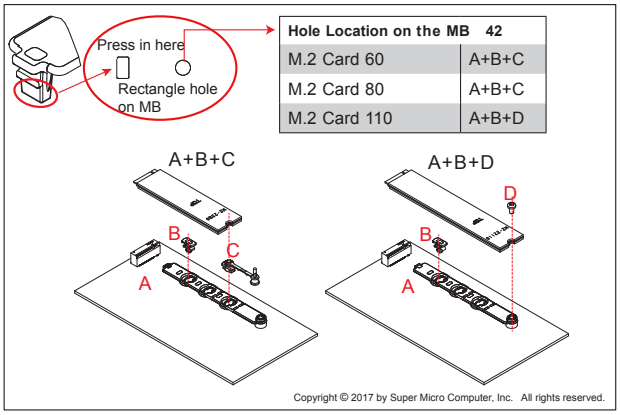


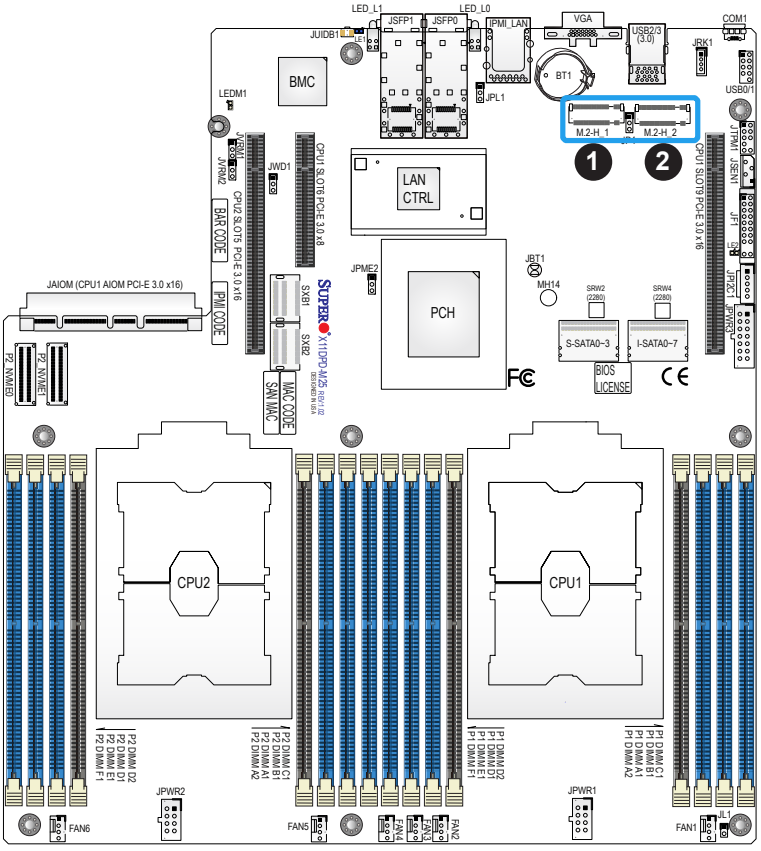
1. TPM/Port 80 Header

PCIe/SATA Hybrid M.2 Sockets

This motherboard has two PCIe/SATA hybrid M.2 sockets (M.2-H_1, M.2-H_2). M.2 was formerly known as Next Generation Form Factor (NGFF) and serves to replace mini PCIe. M.2 socket 1 (M.2-H_1) supports PCIe 3.0 x4 (32 Gb/s) SSD cards in the 2280 form factor only. M.2 socket 2 (M.2-H_2) supports PCIe 3.0 x1 (8 Gb/s) SSD cards in the 2280 form factor only.





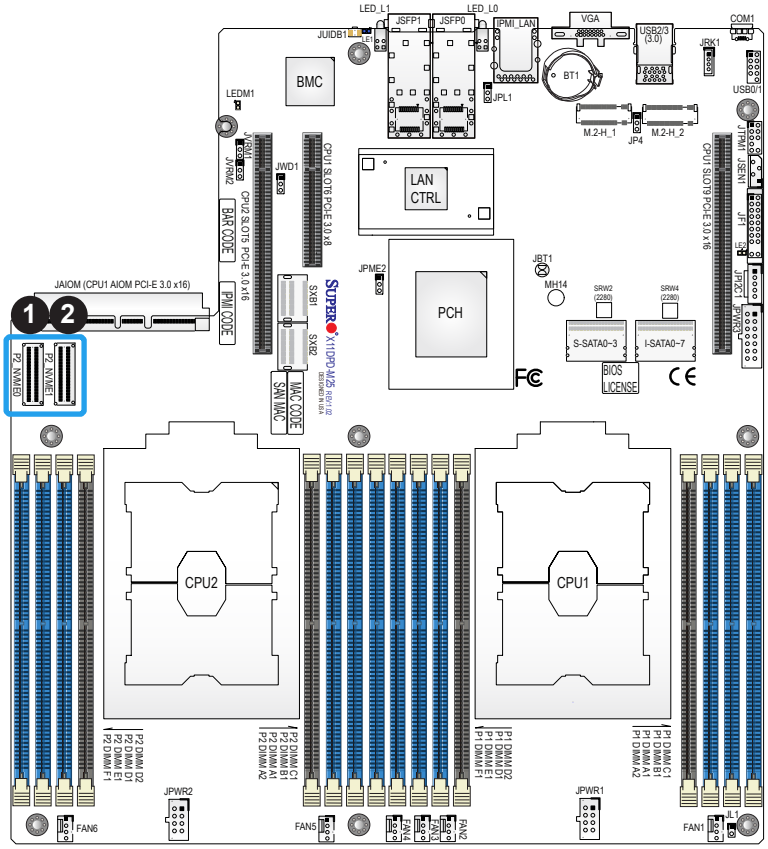


1. PCIe/SATA Hybrid M.2 Socket 1 (M.2-H_1)
2. PCIe/SATA Hybrid M.2 Socket 2 (M.2-H_2)

NVM Express Connections

Two NVMe connectors are located on the motherboard. These NVMe connectors provide PCIe 3.0 x4 connections. P2_NVME0 and P2_NVME1 are supported by CPU2. The NVMe connectors provide high-speed low-latency connections directly from the CPU to NVMe Solid State (SSD) drives. This greatly increases SSD data-throughput performance and significantly reduces PCIe latency by simplifying driver/software requirements resulting from direct PCIe interface from the CPU to the NVMe SSD drives.

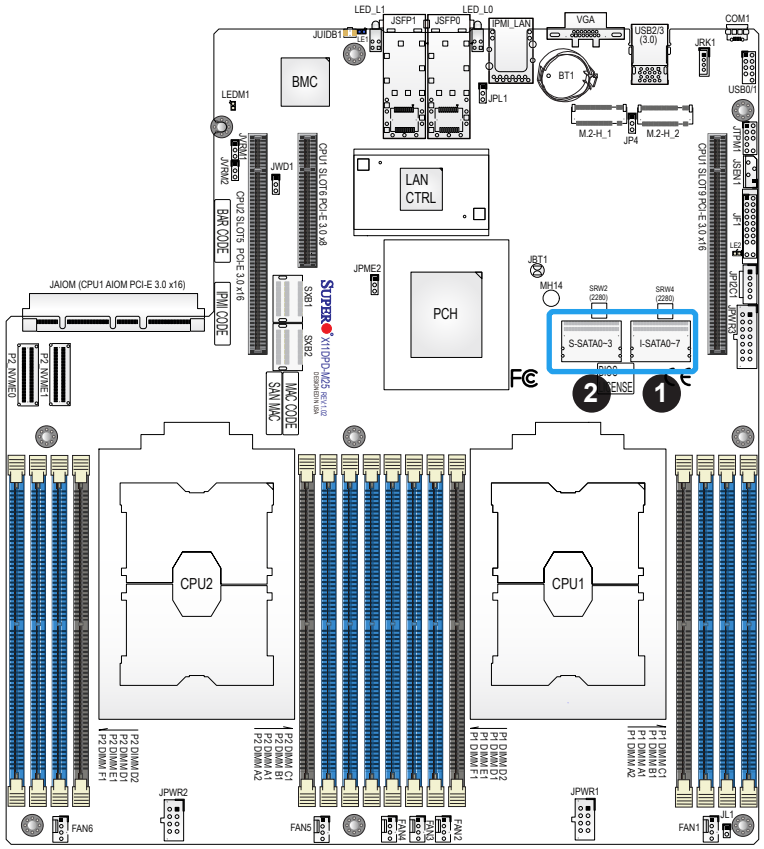
Note: When installing an NVMe device on the motherboard, please be sure to connect the first NVMe connector (P2_NVME0) first for your system to work properly.



1. NVMe Connector 0 (P2_NVME0)
2. NVMe Connector 1 (P2_NVME1)

SATA Ports

This motherboard has eight I-SATA 3.0 ports (I-SATA0~7) and four S-SATA 3.0 ports (S-SATA0~3). These SATA ports are supported by the Intel C621 chipset. All these SATA ports provide serial-link signal connections, which are faster than the connections of Parallel ATA. Refer to the tables on the next page for pin definitions.



1. I-SATA0~7
2. S-SATA0~3

I-SATA 3.0 Port Pin Definitions			
Pin#	Definition	Pin#	Definition
A1	Ground	B1	Ground#
A2	SATA_RX0_P	B2	SATA_TX0_P
A3	SATA_RX0_N	B3	SATA_TX0_N
A4	Ground	B4	Ground
A5	SATA_RX1_P	B5	SATA_TX1_P
A6	SATA_RX1_N	B6	SATA_TX1_N
A7	Ground	B7	Ground
A8	Ground	B8	SATA_SCLK
A9	SDATAOUT0	B9	SATA_SLOAD
A10	Ground	B10	Ground
A11	NC	B11	NC
A12	NC	B12	NC
A13	Ground	B13	Ground
A14	SATA_RX2_P	B14	SATA_TX2_P
A15	SATA_RX2_N	B15	SATA_TX2_N
A16	Ground	B16	Ground
A17	SATA_RX3_P	B17	SATA_TX3_P
A18	SATA_RX3_N	B18	SATA_TX3_N
A19	Ground	B19	Ground
A20	SATA_RX4_P	B20	SATA_TX4_P
A21	SATA_RX4_N	B21	SATA_TX4_N
A22	Ground	B22	Ground
A23	SATA_RX5_P	B23	SATA_TX5_P
A24	SATA_RX5_N	B24	SATA_TX5_N
A25	Ground	B25	Ground
A26	Ground	B26	SATA_SCLK
A27	SDATAOUT1	B27	SATA_SLOAD
A28	Ground	B28	Ground
A29	NC	B29	NC
A30	NC	B30	NC
A31	Ground	B31	Ground
A32	SATA_RX6_P	B32	SATA_TX6_P
A33	SATA_RX6_N	B33	SATA_TX6_N
A34	Ground	B34	Ground
A35	SATA_RX7_P	B35	SATA_TX7_P
A36	SATA_RX7_N	B36	SATA_TX7_N
A37	Ground	B37	Ground

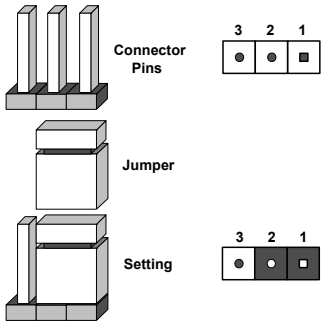
S-SATA 3.0 Port Pin Definitions			
Pin#	Definition	Pin#	Definition
A1	Ground	B1	Ground#
A2	SATAX_RX0_P	B2	SATAX_TX0_P
A3	SATAX_RX0_N	B3	SATAX_TX0_N
A4	Ground	B4	Ground
A5	SATAX_RX1_P	B5	SATAX_TX1_P
A6	SATAX_RX1_N	B6	SATAX_TX1_N
A7	Ground	B7	Ground
A8	Ground	B8	SATAX_SCLK
A9	SDATAXOUT0	B9	SATAX_SLOAD
A10	Ground	B10	Ground
A11	NC	B11	NC
A12	NC	B12	NC
A13	Ground	B13	Ground
A14	SATAX_RX2_P	B14	SATAX_TX2_P
A15	SATAX_RX2_N	B15	SATAX_TX2_N
A16	Ground	B16	Ground
A17	SATAX_RX3_P	B17	SATAX_TX3_P
A18	SATAX_RX3_N	B18	SATAX_TX3_N
A19	Ground	B19	Ground
A20	NC	B20	NC
A21	NC	B21	NC
A22	Ground	B22	Ground
A23	NC	B23	NC
A24	NC	B24	NC
A25	Ground	B25	Ground
A26	NC	B26	NC
A27	NC	B27	NC
A28	Ground	B28	Ground
A29	NC	B29	NC
A30	NC	B30	NC
A31	Ground	B31	Ground
A32	NC	B32	NC
A33	NC	B33	NC
A34	Ground	B34	Ground
A35	NC	B35	NC
A36	NC	B36	NC
A37	Ground	B37	Ground

2.8 Jumper Settings

How Jumpers Work

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

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



CMOS Clear

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

To Clear CMOS

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

Note: Clearing CMOS will also clear all passwords.

JBT1 contact pads

Do not use the PW_ON connector to clear CMOS.

JF1 Pin 3 Function Selection

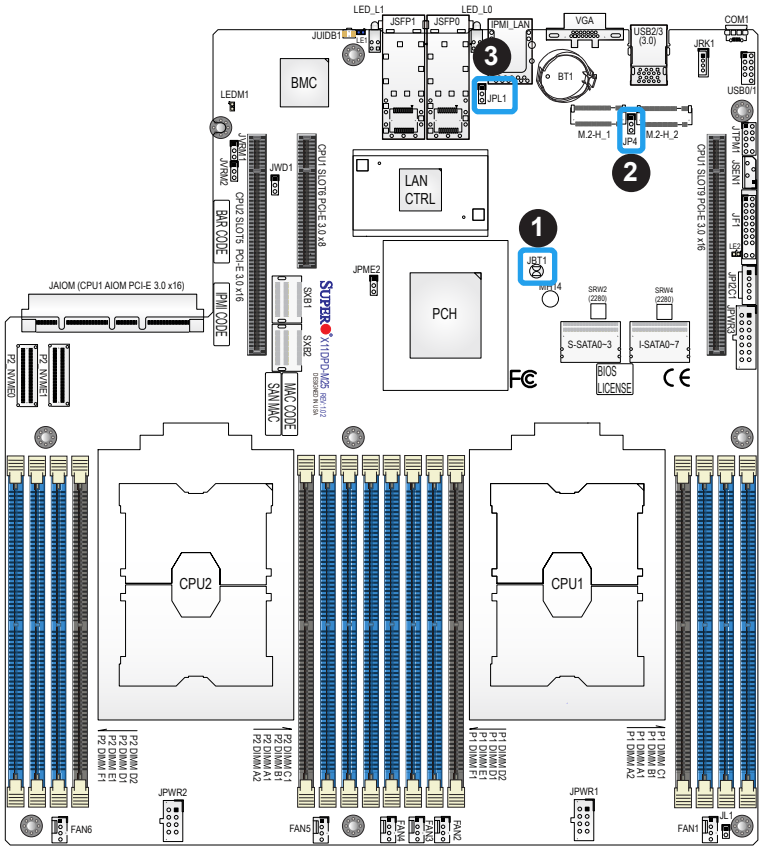
Use JP4 to set the function of pin 3 of JF1. Set JP4 with pins 1 and 2 jumped to the Reset Button. Set JP4 with pins 2 and 3 jumped to the UID Button (for SC802 front panel board). Refer to the table below for jumper settings.

JF1 Pin 3 Function Selection Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Reset Button (Default)
Pins 2-3	UID Button (for SC802 Front Panel Board)

LAN Port Enable/Disable (X11DPD-M25 only)

Change the setting of JPL1 to enable or disable SFP28 LAN ports (JSFP0 and JSFP1). The default setting is Enable.

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



1. CMOS Clear
2. JF1 Pin 3 Function Selection (JP4)
3. SFP28 LAN Ports (JSFP0/JSFP1) Enable/ Disable (X11DPD-M25 only)

Manufacturing Mode

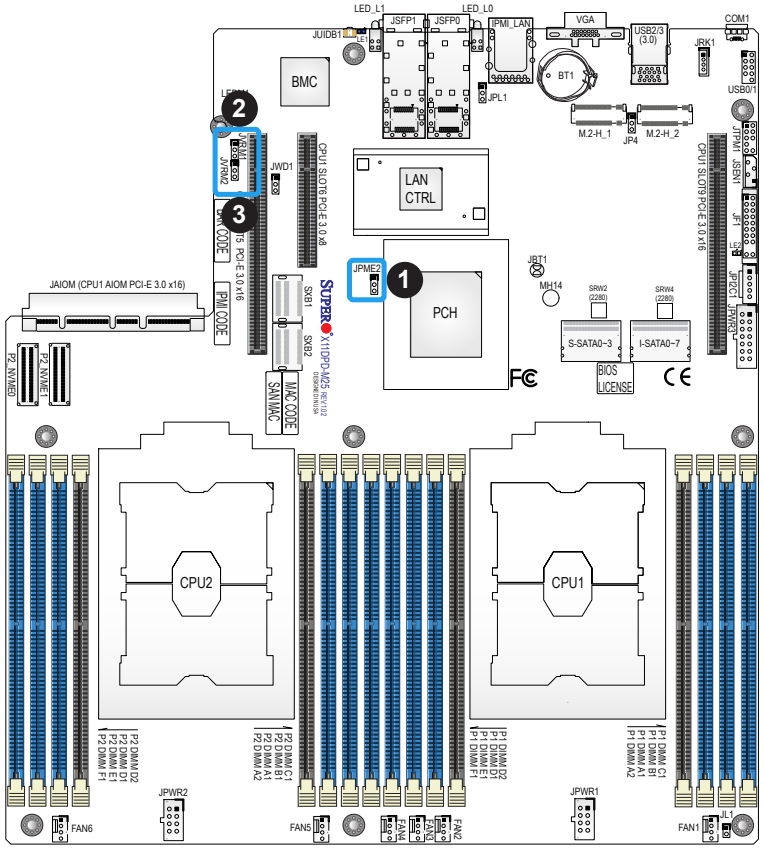
Close JPME2 to bypass SPI flash security and force the system to use the Manufacturing Mode, which will allow you to flash the system firmware from a host server to modify system settings. Refer to the table below for jumper settings.

Manufacturing Mode Select Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Normal (Default)
Pins 2-3	Manufacturing Mode

I²C Bus for VRM

JVRM1 and JVRM2 allow the BMC or the PCH to access CPU and memory VRM controllers. Refer to the table below for jumper settings.

VRM Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	BMC (Default)
Pins 2-3	PCH



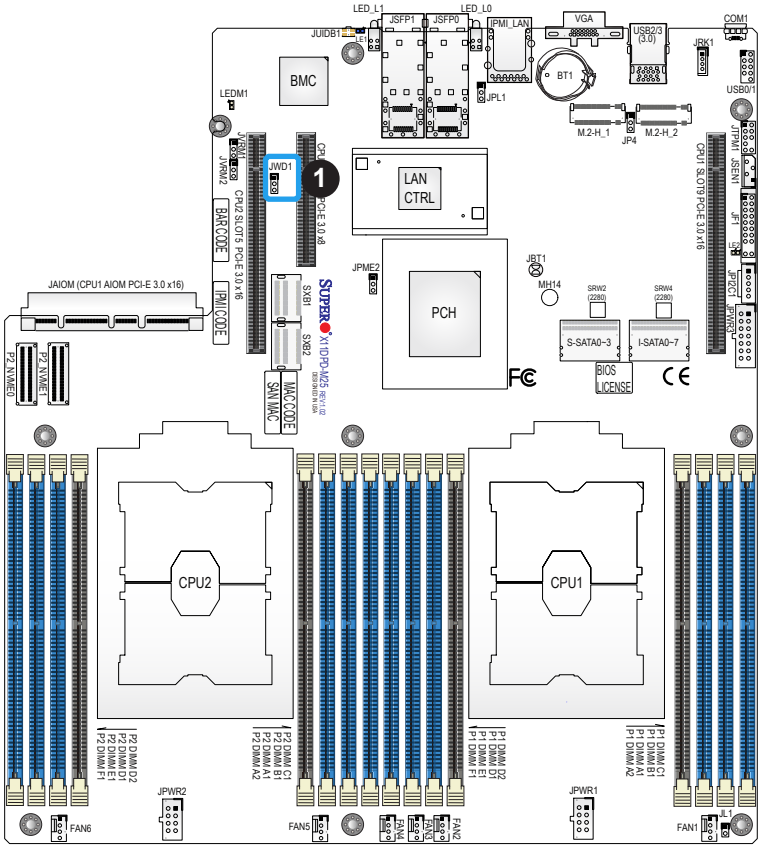
1. Manufacturing Mode
2. I²C Bus for VRM Jumper (JVRM1)
3. I²C Bus for VRM Jumper (JVRM2)

Watch Dog

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

Note: When Watch Dog is enabled, the user needs to write their own application software to disable it.

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



1. Watch Dog

2.9 LED Indicators

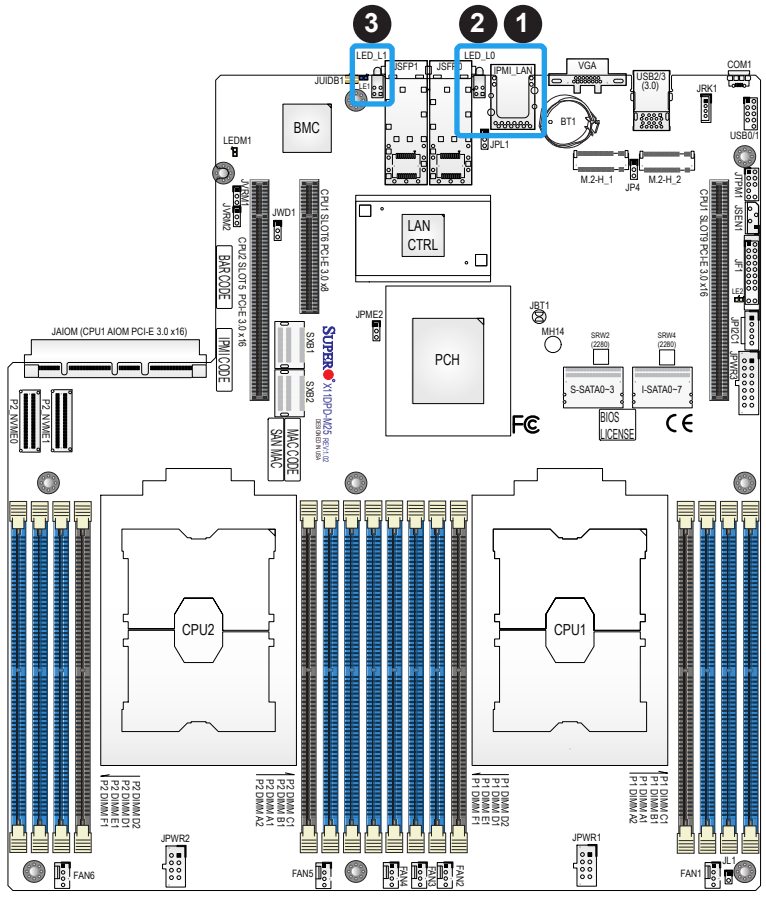
IPMI-Dedicated LAN LEDs

A dedicated IPMI LAN port is also included on the motherboard. The amber LED on the right of the IPMI LAN port indicates activity, while the green LED on the left indicates the speed of the connection. Refer to the table below for more information.

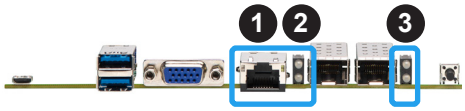
IPMI LAN LEDs		
	Color/State	**Definition**
Link (left)	Green: Solid Amber: Solid	100 Mbps 1 Gbps
Activity (Right)	Amber: Blinking	Active

SFP28 Port Link/Activity LED Indicators (LED_L0/LED_L1)

Please refer to page 46 for more information.



1. IPMI LAN LEDs
2. SFP28 Port 0 Link/Activity LEDs (LED_L0)
3. SFP28 Port 1 Link/Activity LEDs (LED_L1)



BMC Heartbeat LED

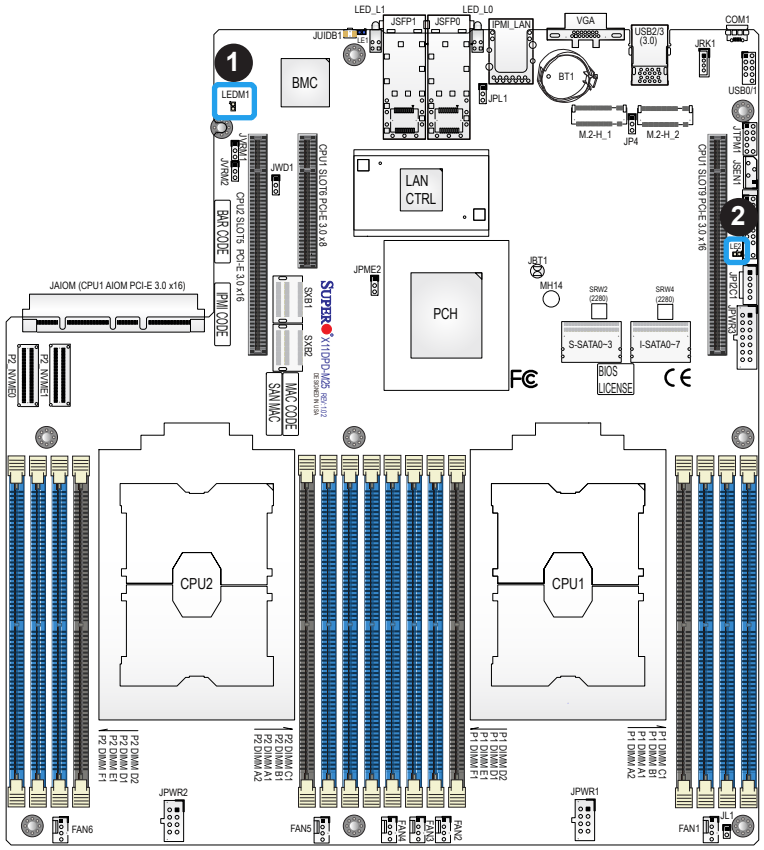
LEDM1 is the BMC heartbeat LED. When the LED is blinking green, BMC is functioning normally. Refer to the table below for the LED status.

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

Onboard Power LED

The Onboard Power LED is located at LE2 on the motherboard. When this LED is lit, it means that power is present on the motherboard. In suspend mode, this LED will blink on and off. Be sure to turn off the system and unplug the power cord(s) before removing or installing components.

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

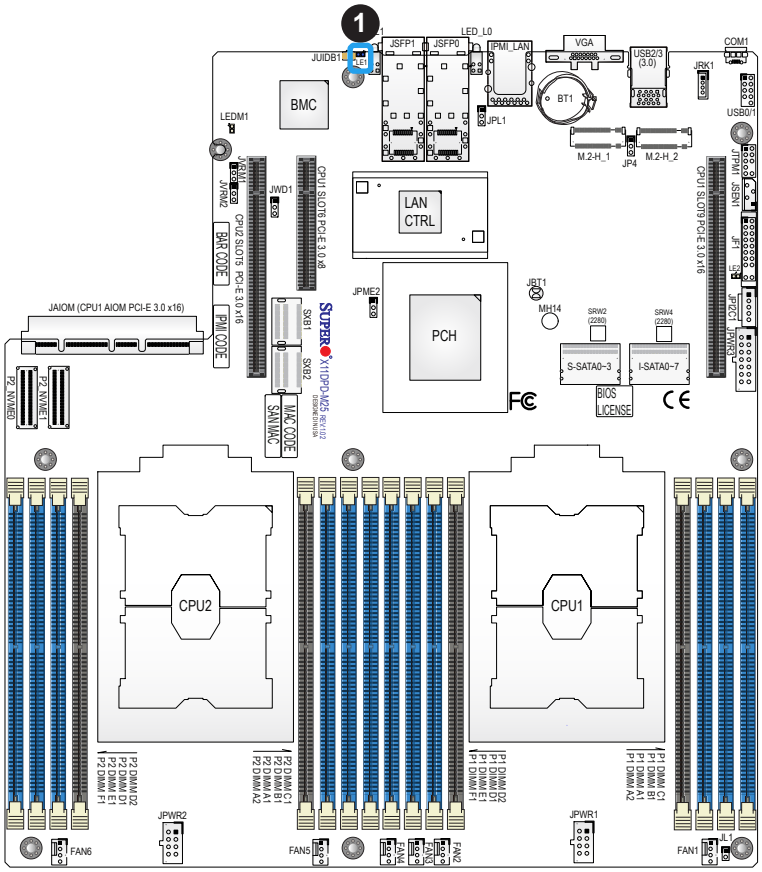


1. BMC Heartbeat LED
2. Onboard Power LED

Unit ID LED

A rear UID LED indicator at LE1 is located near the UID switch on the I/O back panel. This UID indicator provides easy identification of a system unit that may need service.

UID LED Indicator	
LED Color	**Definition**
Blue: On	Unit Identified



1. UID 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.

Note: Always disconnect the AC power cord before adding, changing or installing any non hot-swap hardware components.

Before Power On

1. Check that the power LED on the motherboard is on.
2. Make sure that the power connector is connected to your power supply.
3. Make sure that no short circuits exist between the motherboard and chassis.
4. Disconnect all cables from the motherboard, including those for the keyboard and mouse.
5. Remove all add-on cards.
6. Install a CPU, a heatsink, and connect the power LED to the motherboard. Check all jumper settings as well. (Make sure that the heatsink is fully seated.)
7. Use the correct type of onboard CMOS battery as recommended by the manufacturer. To avoid possible explosion, do not install the CMOS battery upside down.

No Power

1. Make sure that no short circuits exist between the motherboard and the chassis.
2. Verify that all jumpers are set to their default positions.
3. Check that the 115V/230V switch on the power supply is properly set.
4. Turn the power switch on and off to test the system.
5. The battery on your motherboard may be old. If it is too old, replace it with a new one.

No Video

If the power is on but you have no video, remove all the add-on cards and cables, then clear CMOS.

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. Clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS Clear Jumper (JBT1). Refer to Chapter 2.
2. Remove all components from the motherboard, especially the DIMM modules.
3. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this Chapter.

Memory Errors

1. Make sure that the DIMM modules are properly and fully installed.
2. Check to ensure that you are using the correct memory. Also, it is recommended that you use the same memory type and speed for all DIMMs in the system. See Section 2.4 for memory details.
3. Check for bad DIMM modules or slots by swapping modules between slots and noting the results.
4. Check the power supply voltage 115V/230V switch.

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 Section 1.6 for details on recommended power supplies.
2. The battery on your motherboard may be old. If it is too old, replace it with a new one.
3. If the above steps do not fix the setup configuration problem, contact your vendor for repairs.

When the System Becomes Unstable

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

1. CPU/BIOS support: Make sure that your CPU is supported by the motherboard 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: Refer to the product page on our website at http://www.supermicro.com for memory and CPU support and updates.

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

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

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

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

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

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as CD.

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

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

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

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

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

3.2 Technical Support Procedures

Before contacting Technical Support, please take the following steps. Also, note that as a motherboard manufacturer, we do not sell directly to end-users, so it is best to first check with your distributor or reseller for troubleshooting services. They should know of any possible problem(s) with the specific system configuration that was sold to you.

1. Please review the 'Troubleshooting Procedures' and 'Frequently Asked Questions' (FAQs) sections in this chapter or see the FAQs on our website before contacting Technical Support.
2. BIOS upgrades can be downloaded from our website. **Note:** Not all BIOS can be flashed; it depends on the modifications to the boot block code.
3. If you still cannot resolve the problem, include the following information when contacting us for technical support:

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

An example of a Technical Support form is posted on our website.

Distributors: For immediate assistance, please have your account number ready when contacting our technical support department by e-mail.

3.3 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

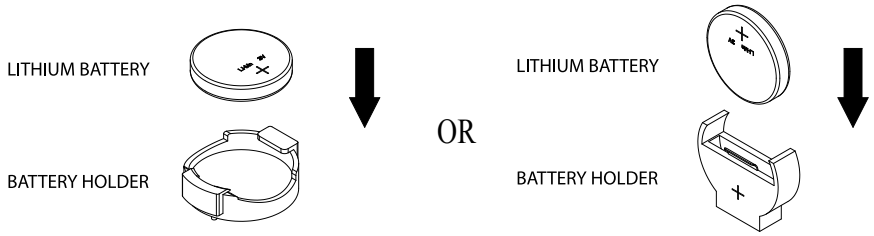
Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency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

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



3.4 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: This motherboard supports up to 4TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 2TB of Load Registered DIMM (LRDIMM), with speeds of 2933*/2666/2400/2133/1866/1600/1333 MHz modules in 16 memory slots. See Section 2.4 for details on Memory Support and Installation.

Note: Support for 2933MHz memory is dependent on the CPU SKU.

Question: Why can't I turn off the power using the momentary power on/off switch?

Answer: The instant power off function is controlled in BIOS by the Power Button Mode setting. When the On/Off feature is enabled, the motherboard will have instant off capabilities as long as the BIOS is in control of the system. When the Standby or Suspend feature is enabled or when the BIOS is not in control such as during memory count (the first screen that appears when the system is turned on), the momentary on/off switch must be held for more than four seconds to shut down the system. This feature is required to implement the ACPI features on the motherboard.

Question: How do I update my BIOS?

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

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/.

Question: How do I update my 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 stick.

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

3. Insert the USB stick into a USB port, boot to the UEFI Built-In 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 system 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.

3.5 Returning Merchandise for Service

A receipt or copy of your invoice marked with the date of purchase is required before any warranty service is rendered. You can obtain service by calling your vendor for a Returned Merchandise Authorization (RMA) number. When returning to the manufacturer, the RMA number should be prominently displayed on the outside of the shipping carton and 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, RMA authorizations may be requested online (http://www.supermicro.com/support/rma/).

This warranty only covers normal consumer use and does not cover damages incurred in shipping or from failure due to the alteration, 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 X11DPD-L/-M25 motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.

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

Starting the Setup Utility

To enter the BIOS Setup utility, press 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.

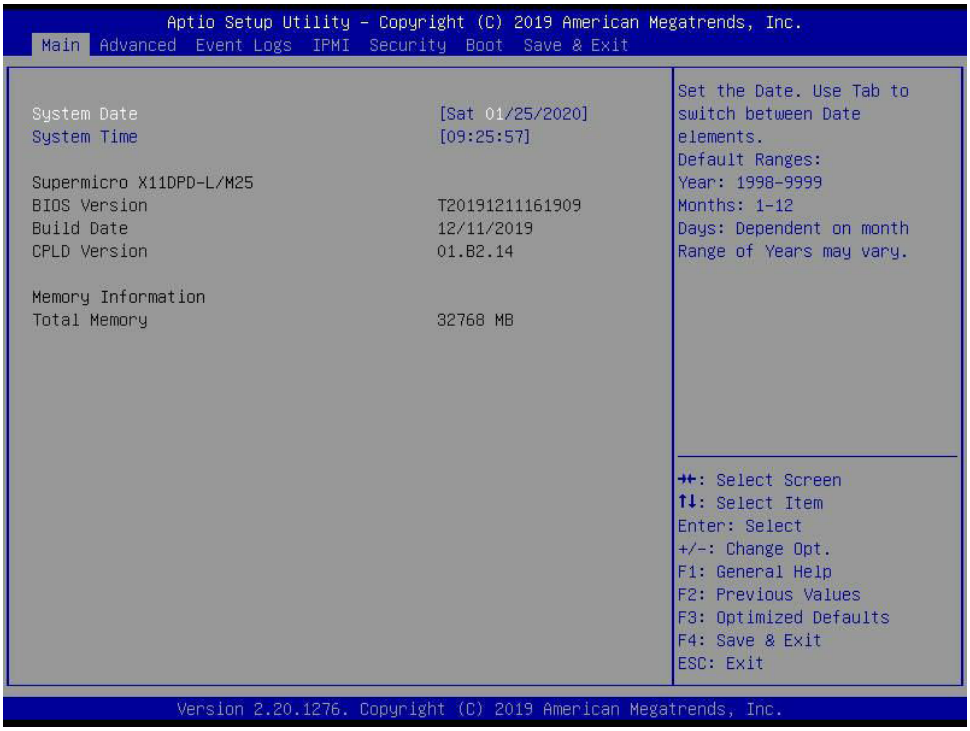
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is 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>, <F4>, <Enter>, <ESC>, <Arrow> keys, etc.) can be used at any time during the setup navigation process.

4.2 Main Setup

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



System Date/System Time

Use this feature to change the system date and time. 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 the RTC (Read Time Clock) reset.

Supermicro X11DPD-L/M25

BIOS Version

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

Build Date

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

CPLD Version

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

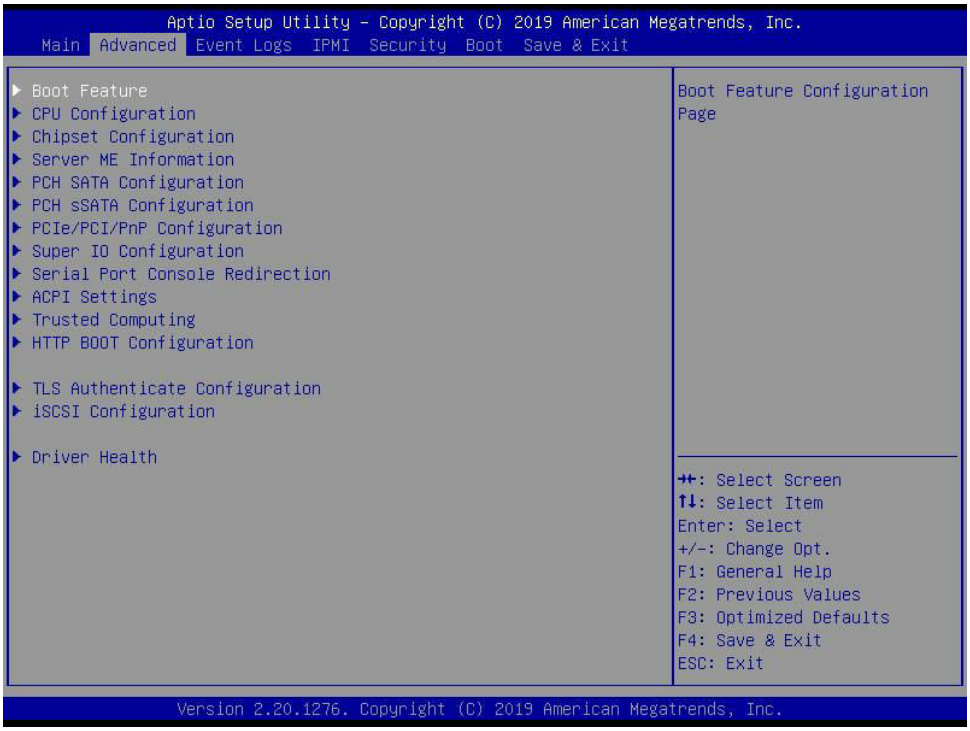
Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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



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

▶Boot Feature

Quiet Boot

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

Note: POST message is always displayed regardless of the item setting.

Option ROM Messages

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

Bootup NumLock State

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

Wait For "F1" If Error

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

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

Re-try Boot

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

Install Windows 7 USB Support

Select Enabled to install the Windows 7 USB utility to support legacy USB devices for Windows 7 systems. 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.

Power Configuration

Watch Dog Function

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

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

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

Processor 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
- L2 Cache RAM
- L3 Cache RAM
- Processor 0 Version
- Processor 1 Version

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

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

Cores Enabled

Use this feature to enable or disable CPU cores in the processor specified by the user. Use the <+> key and the <-> key on the keyboard to set the desired number of CPU cores you want to enable in a processor. Please note that the maximum of 24 CPU cores are currently available in each CPU package. The default setting is **0**.

Monitor/Mwait

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

Execute Disable Bit (Available if supported by the OS and the CPU)

Select Enable for Execute Disable Bit support which will allow the processor to designate areas in the system memory where an application code can execute and where it cannot, thus preventing a worm or a virus from flooding illegal codes to overwhelm the processor, damaging the system during a virus attack. The options are Disable and **Enable**. (Refer to Intel and Microsoft websites for more information.)

Intel Virtualization Technology (Available when two processors are installed on the motherboard)

Select Enable to use Intel Virtualization Technology which will allow multiple workloads to share the same set of common resources. On shared virtualized hardware, various workloads (or tasks) can co-exist, sharing the same resources, while functioning in full independence from each other, and migrating freely across multi-level infrastructures and scale as needed. 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. Refer to Intel website for detailed information.

PPIN Control

Select Unlock/Enable to use the Protected-Processor Inventory Number (PPIN) in the system. The options are Lock/Disable and **Unlock/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 (L2) cache to help expedite data transaction for memory performance enhancement. 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: Please power off and reboot the system for the changes you've made to take effect. Please refer to Intel 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.

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**.

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

ENERGY_PERF_BIAS_CFG mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode) (Available when Power Performance Tuning is set to BIOS Controls EPB)

Use this feature to set the processor power use policy to achieve the desired operation settings for your machine by prioritizing system performance or energy savings. Select Maximum Performance to maximize system performance (to its highest potential); however, this may result in maximum power consumption as energy is needed to fuel the processor frequency. The higher the performance is, the higher the power consumption will be.

Select Max Power Efficient to maximize power saving; however, system performance may be substantially impacted because limited power use decreases the processor frequency. The options are Maximum Performance, Performance, **Balanced Performance**, Balanced Power, and Power.

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

SpeedStep (P-States)

EIST (Enhanced Intel SpeedStep Technology) 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 website for detailed information. The options are Disable and **Enable**.

Config (Configuring) TDP (Available when SpeedStep is set to Enable and when the 2nd Gen Intel Xeon Scalable-SP 8260Y/6240Y/4214Y processor is used)

This Feature allows the user to configure the maximum CPU TDP (Thermal Design Power) level for the system. The TDP level is subject to chassis and heatsink cooling restrictions. For proper thermal management, please check the chassis and heatsink specifications for proper CPU TDP sizing. The options are **Normal**, Level 1, and Level 2.

Intel Speed Select (Available when SpeedStep is set to Enable and when the 2nd Gen Intel Xeon Scalable-SP 8260Y/6240Y/4214Y processor is used)

This feature allows the user to configure up to two additional base frequency settings for the processors used in your system as shown in the display below. The options are **Base**, Config 1, and Config 2.

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

Use this item to configure the processor's P-State coordination settings. During a P-State, the voltage and frequency of the processor will be reduced when it is in operation. This makes the processor more energy efficient, resulting in further energy gains. The options are **HW_ALL**, SW_ALL, and SW-ANY.

Turbo Mode (Available when SpeedStep is set to Enable)

Select Enable for processor cores to run faster than the frequency specified by the manufacturer. The options are Disable and **Enable**.

Activate PBF (Available when SpeedStep is set to Enable and when the 2nd Gen Intel Xeon Scalable-SP 6252N/6230N/5218N processor is used)

Select Enable to support Prioritized Base Frequency (PBF), which will increase the base frequency on high-priority cores and decrease the base frequency on low-priority cores to improve CPU performance. The options are **Disable** and Enable.

Configure PBF (Available when Activate PBF is set to Enable)

Select Enable to allow the BIOS to configure high priority CPU cores as Prioritized Base Frequency (PBF) so that software programs do not have to configure the PBF settings. This feature is available when it is supported by the CPUs used in the system. The options are Disable and **Enable**.

▶Hardware PM (Power Management) State Control (Available when Power Technology is set to Custom)

Hardware P-States

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

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

Autonomous Core C-State

Select Enable to support Autonomous Core C-State control which will allow the processor core to control its C-State setting automatically and independently. The options are **Disable** and Enable.

CPU C6 report (Available when Autonomous Core C-State is set to Disable)

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

Enhanced Halt State (C1E) (Available when Autonomous Core C-State is set to Disable)

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 (Available when Power Technology is set to Custom)

Package C State

This feature is used to optimize and reduce CPU package power consumption in 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, C6 (Retention) state, No Limit, 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 settings will be supported by the software of the system. The options are Disable and **Enable**

▶Chipset Configuration

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

▶North Bridge

This feature allows the user to configure the settings for the Intel North Bridge.

▶UPI (Ultra Path Interconnect) Configuration

UPI Configuration

The following information will be displayed:

- Number of CPU
- Number of Active UPI Link
- Current UPI Link Speed
- Current UPI Link Frequency
- UPI Global MMIO Low Base/Limit
- UPI Global MMIO High Base/Limit
- UPI 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.

IO Directory Cache (IODC)

Select Enable for the IODC (I/O Directory Cache) 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

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**, Enable, and Auto.

XPT Prefetch

Select Enable for XPT (Extended Prediction Table) Prefetch support 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** and Enable.

KTI Prefetch

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

Local/Remote Threshold

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

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 the "Stale AtoS" feature 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.

Isoc Mode

Select Enable to enable Isochronous support to meet QoS (Quality of Service) requirements. This feature is especially important for Virtualization Technology. The options are Disable, Enable, and **Auto**.

▶Memory Configuration

Integrated Memory Controller (iMC)

Enforce POR

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 Auto, **Hard PPR**, Soft PPR, and PPR Disabled.

Enhanced PPR

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

Operation Mode

Use this feature to set Test Only or Test/Repair from the Enhanced PPR. The options are **Test and Repair** and Test Only.

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 1866, 2000, 2133, 2400, 2666, and 2933. (**Note:** Support for 2933 MHz memory is dependent on the CPU SKU.)

Data Scrambling for DDR4

Select Enable to enable data scrambling for DDR4 memory to enhance system performance and security. Select Auto for the default setting of the Memory Reference Code (MRC) to set configure data scrambling for DDR4 setting. The options are **Auto**, Disable, and Enable.

tCCD_L Relaxation

If this feature is set to Enable, SPD (Serial Presence Detect) will override tCCD_L ("Column to Column Delay-Long", or “Command to Command Delay-Long” on the column side.) If this feature is set to Disable, tCCD_L will be enforced based on the memory frequency. The options are Disable and **Auto**.

tRWSR (Read to Write turnaround time for Same Rank) Relaxation

Select Enable to use the same tRWSR DDR timing setting among all memory channels, and in which case, the worst case value among all channels will be used. Select Disable to use different values for the tRWSR DDR timing settings for different channels as trained. The options are **Disable** and Enable.

tRFC Optimization for 16Gb Based DIMM

Use this feature to select the 16Gb Based DIMM Refresh Cycle time The options are **Auto**, Force 350ns, and Force 550ns.

Enable ADR (Available when any NVDIMM is installed)

Select Enable for ADR (Async DIMM Self-Refresh) support to enhance memory performance. The options are Disable and **Enable**.

Data Scrambling for NVDIMM (Available when any NVDIMM is installed)

Select Enable to enable data scrambling support for onboard NVDIMM memory to improve system performance and security. The options are **Auto**, Disable, and Enable.

Erase-Arm NVDIMMs (Available when any NVDIMM is installed)

If this feature is set to Enable, the function that arms the NVDIMMs for safe operations in the event of a power loss will be removed. The options are **Disable** and Enable.

Restore NVDIMMs (Available when any NVDIMM is installed)

Select Enable to restore the functionality and the features of NVDIMMs. The options are Disable and **Enable**.

Interleave NVDIMMs (Available when any NVDIMM is installed)

If this feature is set to Enable, all onboard NVDIMM modules will be configured together as a group for the interleave mode. If this item is set to Disable, individual NVDIMM modules will be configured separately for the interleave mode. The options are **Disable** and Enable.

Reset Trigger ADR (Async DIMM Self-Refresh) (Available when any NVDIMM is installed)

Upon system power loss, an ADR sequence will be triggered to allow ADR to flush the write-protected data buffers in the memory controller and place the DRAM memory in self-refresh mode. When this process is complete, the NVDIMM will then take control of the DRAM memory and transfer the contents to the onboard Flash memory. After the transfer is complete, the NVDIMM goes into a zero power state. The data transferred will be retained for the duration specified by the flash memory. The options are **Disable** and Enable.

S5 Trigger ADR (Available when any NVDIMM is installed)

Select Enabled to support S5-Triggered ADR to enhance system performance and data integrity. The options are **Disabled** and Enabled.

2X Refresh

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

Page Policy

Use this feature to set the page policy for onboard memory support. The options are **Auto**, Closed, and Adaptive.

IMC Interleaving

Use this feature to configure interleaving settings for the IMC (Integrated Memory Controller), which will improve memory performance. The options are **Auto**, 1-way Interleave, and 2-way Interleave.

DCPMM Average Power Budget (in mW) (Available when any DCPMM is installed)

This feature sets the power management policy for average power use (in an increment of 250 mW). The default setting is **15000**.

DCPMM QoS (Available when any DCPMM is installed)

Use this feature to enable QoS tuning recipes for Intel DCPMM. The options are Enable and **Disable**.

DCPMM Performance Setting (Available when any DCPMM is installed)

This feature sets the DCPMM baseline performance, which is based on the workload behavior. Select BW Optimized for a optimized DDR and DDR-T bandwidth. Select Latency Optimized for a better DDR latency. The options are **BW Optimized** and Latency Optimized.

▶Memory Topology

This feature displays the information of onboard memory modules as detected by the BIOS, such as P1 DIMMA1 and P1 DIMM01.

▶Memory RAS (Reliability_Availability_Serviceability) Configuration

Use this submenu to configure the following Memory RAS settings.

Memory RAS Configuration Setup

Static Virtual Lockstep Mode

Select Enable to support Static Virtual Lockstep mode to enhance memory performance. The options are **Disable** and Enable.

Mirror Mode

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 **Disable**, Mirror Mode 1LM, and Mirror Mode 2LM.

Memory Rank Sparing

Select Enable to support memory-rank sparing to optimize memory performance. The options are **Disable** and Enable.

Note: This feature will not be available when memory mirror mode is set to Mirror Mode 1LM or an AEP device is plugged in.

Multi Rank Sparing (Available when Memory Rank Sparing is set to Enable)

Use this feature to set the multiple rank sparing number. The default setting and the maximum is two ranks per channel. The options are One Rank and **Two Rank**.

Correctable Error Threshold

Use this item to enter the threshold value for correctable memory errors. The default setting is **512**.

Intel Run Sure

Select Enable to use Intel Run Sure Technology which will enhance critical data protection and increase system uptime and resiliency. The options are **Disable** and Enable.

SDDC Plus One

SDDC (Single Device Data Correction) checks and corrects single-bit or multiple-bit (4-bit max.) memory faults that affect an entire single x4 DRAM device. SDDC Plus One, an enhanced feature to SDDC, copies data stored in a faulty DRAM device to a spare device when an SDDC event has occurred. After the event, the SDDC+1 ECC mode is activated to protect against any additional memory failure caused by a 'single-bit' error in the same memory rank. The options are **Disable** and Enable. (**Note:** SDDC or SDDC Plus One is available when it is supported by the processors installed on the motherboard.)

ADDDC Sparing (Adaptive Double Device Data Correction) Sparing

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

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 Disable and **Enable**.

Patrol Scrub Interval

Use this item to specify the number of hours (between 0 to 24) required for the system to complete a full patrol scrubbing. Enter 0 for patrol scrubbing to be performed automatically. The default setting is **24**.

Note: This feature is hidden when Patrol Scrub is set to Disable.

▶IIO Configuration

IIO Configuration

EV DFX (Device Function On-Hide) Features

When this feature is set to Enable, the EV_DFX Lock Bits that are located in a processor will always remain clear during electric tuning. The options are **Disable** and Enable.

▶CPU1 Configuration

IOU0 (IIO PCIe Br1)

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

IOU1 (IIO PCIe Br2)

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

IOU2 (IIO PCIe Br3)

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

▶CPU1 AIOM PCI-E X16 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

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

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶CPU1 SLOT9 PCI-E 3.0 X16 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

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

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶CPU1 SLOT6 PCI-E 3.0 X8 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

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

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶CPU2 Configuration

IOU0 (IIO PCIe Br1)

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

IOU1 (IIO PCIe Br2)

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

IOU2 (IIO PCIe Br3)

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

▶P2_NVMe1 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

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

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶P2_NVMe2 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

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

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶P2_NVMe3 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

• PCI-E Port Link Status

• PCI-E Port Link Max

• PCI-E Port Link Speed

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶P2_NVMe4 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

• PCI-E Port Link Status

• PCI-E Port Link Max

• PCI-E Port Link Speed

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶CPU2 SLOT5 PCI-E 3.0 X16 (Available when the device is detected by the system)

Link Speed

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

The following information is displayed:

• PCI-E Port Link Status

• PCI-E Port Link Max

• PCI-E Port Link Speed

PCI-E Port Max (Maximum) Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCIe device specified by to user for system performance enhancement. The options are 128B, 256B, and **Auto**.

▶IOAT (Intel IO Acceleration Technology) 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 in this item 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 (TLP Processing Hint)

Select Yes 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 Enable to allow certain transactions to be processed and completed before other transactions that have already been enqueued. The options are **Disable** and Enable.

▶Intel® VT for Directed I/O (VT-d)

Intel® VT for Directed I/O (VT-d)

Select Enable to use Intel Virtualization Technology support for Direct I/O VT-d 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 (Access Control Services) Control

Select Enable to program Access Control Services to Chipset PCIe Root Port Bridges. Select Disable to program Access Control Services to all PCIe Root Port Bridges. The options are **Enable** and Disable.

Interrupt Remapping

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

PassThrough DMA

Select Enable for the Non-Isoch VT-d engine to pass through DMA (Direct Memory Access) to enhance system performance. The options are **Enable** and Disable.

ATS

Select Enable to enable ATS (Address Translation Services) support for the Non-Isoch VT-d engine to enhance system performance. The options are **Enable** and Disable.

Posted Interrupt

Select Enable to support VT_D Posted Interrupt which will allow external interrupts to be sent directly from a direct-assigned device to a client machine in non-root mode

to improve virtualization efficiency by simplifying interrupt migration and lessening the need of physical interrupts. The options are **Enable** and Disable.

Coherency Support (Non-Isoch)

Select Enable for the Non-Isoch VT-d engine to pass through DMA (Direct Memory Access) to enhance system performance. The options are **Enable** and Disable.

▶Intel® VMD technology

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

Note: After you've enabled VMD on a PCIe slot of your choice, 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.

▶Intel® VMD for Volume Management Device on CPU1

VMD Config for PStack1

Intel® VMD for Volume Management Device for PStack1

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

If the feature, Intel® VMD for Volume Management Device for PStack1, is set to Enable, the following features will become available for user's configuration:

CPU1 SLOT9 PCI-E 3.0 X16 VMD (Available when the device is detected by the system)

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

Note: After you've enabled VMD support on a NMVe port, this port will be dedicated for VMD use only. To reactivate this port for NMVe use, please disable VMD support on the port.

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

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

VMD Config for PStack2

Intel® VMD for Volume Management Device for PStack2

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

If the feature, Intel® VMD for Volume Management Device for PStack2, is set to Enable, the following features will become available for user's configuration:

CPU1 SLOT6 PCI-E 3.0 X8 VMD (Available when the device is detected by the system)
Select Enable to enable Intel Volume Management Device Technology support for the root port specified by the user. The options are **Disable** and Enable.

Note: After you've enabled VMD support on a NMVe port, this port will be dedicated for VMD use only. To reactivate this port for NMVe use, please disable VMD support on the port.

Hot Plug Capable (Available when the device is detected by the system)
Select Enable to enable Hot Plug support for the root ports specified by the user, which will allow 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

VMD Config for PStack0

Intel® VMD for Volume Management Device for PStack0
Select Enable to use the Intel Volume Management Device Technology for this stack. The options are **Disable** and Enable.

If the feature, Intel® VMD for Volume Management Device for PStack0, is set to Enable, the following features will become available for user's configuration:

P2_NVMe1 VMD (Available when the device is detected by the system)
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_NVMe2 VMD (Available when the device is detected by the system)
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_NVMe3 VMD (Available when the device is detected by the system)
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_NVMe4 VMD (Available when the device is detected by the system)
Select Enable to enable Intel Volume Management Device Technology support for the root port specified by the user. The options are **Disable** and Enable.

Note: After you've enabled VMD support on a NMVe port, this port will be dedicated for VMD use only. To reactivate this port for NMVe use, please disable VMD support on the port.

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

VMD Config for PStack1

Intel® VMD for Volume Management Device for PStack1
Select Enable to use the Intel Volume Management Device Technology for this stack. The options are **Disable** and Enable.

If the feature, Intel® VMD for Volume Management Device for PStack1, is set to Enable, the following features will become available for user's configuration:

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

VMD Config for PStack2

Intel® VMD for Volume Management Device for PStack2
Select Enable to use the Intel Volume Management Device Technology for this stack. The options are **Disable** and Enable.

If the feature, Intel® VMD for Volume Management Device for PStack2, is set to Enable, the following features will become available for user's configuration:

CPU2 SLOT5 PCI-E 3.0 X16 VMD (Available when the device is detected by the system)
Select Enable to enable Intel Volume Management Device Technology support for the root port specified by the user. The options are **Disable** and Enable.

Note: After you've enabled VMD support on a NMVe port, this port will be dedicated for VMD use only. To reactivate this port for NMVe use, please disable VMD support on the port.

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

IIO-PCIE Express Global Options

PCI-E Completion Timeout Disable

Use this feature to select the PCIe Completion Time-out settings. The options are Yes, **No**, and Per-Port.

▶South Bridge

The following South Bridge 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 Disable to have all USB devices available for EFI applications only. The options are **Enabled,** Disabled, and Auto.

XHCI Hand-off

This is a work-around solution for operating systems that do not support 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 SSC

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 **Disable** and Enable.

▶Server ME (Management Engine) Information

This feature displays the following general ME configuration settings.

- Oper. (Operational) Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1

- ME Firmware Status #2
  - Current State
  - Error Code

▶PCH SATA Configuration

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

SATA Controller

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

Configure SATA as (Available when SATA Controller is set to Enable)

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

SATA HDD Unlock (Available when SATA Controller is set to Enable)

Select Enable to unlock SATA HDD password in the OS. The options are Disable and **Enable**.

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

When this feature is set to Enable, the SATA Controller provides full int 13h support for SATA controller attached devices. CSM storage OPROM policy should be set to legacy to make this selection effective. The options are Disable and **Enable**.

Aggressive Link Power Management

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

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

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

SATA Port 0 ~ SATA Port 7

Hot Plug

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

Spin Up Device

When this feature is set to Enable, the SATA device installed on the SATA port specified by the user will start a COMRESET initialization when an edge is detected from 0 to 1. The options are **Disable** and Enable.

SATA Device Type

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

▶PCH sSATA Configuration

When this submenu is selected, the AMI BIOS automatically detects the presence of the sSATA devices that are supported by the sSATA controller and displays the following items:

sSATA Controller

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

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

Select AHCI to configure an sSATA drive 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.

SATA HDD Unlock (Available when sSATA Controller is set to Enable)

Select Enable to unlock sSATA HDD password in the OS. The options are Disable and **Enable**.

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

When this feature is set to Enable, the SATA Controller provides full int 13h support for SATA controller attached devices. CSM storage OPROM policy should be set to legacy to make this selection effective. The defualt options are Disable and **Enable**.

Aggressive Link Power Management

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

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

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

sSATA Port 0 ~ sSATA Port 5

Hot Plug

Select Enable to support Hot-plugging for the device installed on an sSATA port 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 Disabled and **Enable**.

Spin Up Device

This setting allows the SATA device installed on the SATA port specified by the user to start a COMRESET initialization when an edge is detected from 0 to 1. 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.

▶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 (Available if the system supports Single-Root Virtualization)

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

ARI Support

Select Enabled for the Alternative Routing ID Interpretation support 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, 24T, 16T, 4T, 2T, and 1T.

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, and 3G.

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.

CPU1 AIOM PCI-E X16 OPROM/ CPU1 SLOT9 PCI-E 3.0 X16 OPROM/ CPU1 SLOT6 PCI-E 3.0 X8 OPROM/ CPU2 SLOT5 PCI-E 3.0 X16 OPROM/ M.2-H_1 OPROM/ M.2-H_2 OPROM

Select EFI to allow the user to boot the computer using an EFI (Extensible Firmware Interface) device installed on the PCIe slot specified by the user. Select Legacy to allow the user to boot the computer using a legacy device installed on the PCIe slot specified by the user. The options are Disabled, **Legacy,** and EFI. (**Note:** Riser card names may differ in each system.).

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 **Enabled** and Disabled.

Onboard LAN1 Option ROM (for X11DPD-M25 only)

Use this feature to select the onboard Ethernet controller port 1 option ROM execution. The options are Disabled, **Legacy**, and EFI.

Onboard LAN2 Option ROM (for X11DPD-M25 only)

Use this feature to select the onboard Ethernet controller port 2 option ROM execution. The options are **Disabled**, Legacy, and EFI.

Onboard NVMe#1 Option ROM ~ Onboard NVMe#4 Option ROM

Select EFI to allow the user to boot the computer using an EFI (Extensible Firmware Interface) device installed on the NVME connector specified by the user. Select Legacy to allow the user to boot the computer using a legacy device installed on the NVME connector specified by the user. The options are Disabled, Legacy, and **EFI**.

Onboard Video Option ROM

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

▶Network Stack Configuration

Network Stack

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

If the feature "Network Stack" is set to Enabled, the following features will become available for user's configuration:

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 select the wait time to press the <ESC> key to abort the PXE boot. The default is **0**.

Media detect count

Use this feature to select the wait time in seconds for the BIOS ROM to detect the LAN media (Internet connection or LAN port). The default is **1**.

SATA Driving Is Set As

This feature displays the current SATA driving value. Otherwise, it displays [Common].

Backplane Selection

Select Auto for the BIOS to automatically select the backplane to be used for network support. The default setting is **Auto**.

▶Super IO Configuration

Super IO Configuration

The following Super IO information will be displayed:

- Super IO Chip AST2500

▶Serial Port 1 Configuration

Serial Port 1 Configuration

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

Serial Port 1

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

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

This feature displays the base I/O port address and the Interrupt Request address of a serial port specified by the user.

Change Settings

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 a serial port specified. The options are **Auto**, (IO=3F8h; IRQ=4;), (IO=2F8h; IRQ=4;), (IO=3E8h; IRQ=4;), and (IO=2E8h; IRQ=4;).

▶SOL Configuration

SOL Configuration

This submenu allows the user to configure settings of SOL (Serial Over LAN).

SOL

Select Enabled to enable SOL. The options are Disabled and **Enabled**.

Device Settings (Available when SOL is set to Enabled)

This feature displays the base I/O port address and the Interrupt Request address of a serial port specified by the user.

Change Settings

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

▶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.

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

▶Console Redirection Settings

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

COM1

Console Redirection Settings

Terminal Type

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

Bits Per second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

Use this feature to enable or disable Legacy Console Redirection after BIOS POST. When the BootLoader is selected, Legacy Console Redirection is disabled before booting the OS. When the Always Enable is selected, Legacy Console Redirection remains enabled upon OS boot up. The options are **Always Enable** and BootLoader.

SOL

Console Redirection

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

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

▶Console Redirection Settings

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

SOL

Console Redirection Settings

Terminal Type

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

Bits Per second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

Use this feature to enable or disable legacy console redirection after BIOS POST. When this feature is set to BootLoader, legacy console redirection is disabled before booting the OS. When this feature is 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 the 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 the user to configure Console Redirection settings to support Out-of-Band Serial Port management.

Console Redirection

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

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

▶Console Redirection Settings

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

Out-of-Band Mgmt Port

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

Terminal Type

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

Bits Per second

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

Flow Control

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

The settings below are displayed:

Data Bits, Parity, Stop Bits

▶ACPI Settings

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

NUMA (Available when the OS supports this feature)

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

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 be displayed.

- TPM2.0 Device Found
- Firmware Version
- Vendor

Security Device Support

If a Trusted Platform Module (TPM) device is connected to the TPM header (JTPM1) on the motherboard and this feature is set to Enable, onboard security devices will be available for the TPM support to enhance data integrity and network security. Please note that the OS will not show the security device. Neither TCG EFI protocol nor INT1A interaction will be made available for use. Please reboot the system for a change on this setting to take effect. The options are Disable and **Enable**.

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

The following Platform Configuration Register information will display:

- Active PCR banks
- Available PCR banks

SHA256 PCR Bank

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

Pending operation

Use this feature to schedule a TPM-related operation to be performed by a security (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 or later)

Select Enabled for TPM Platform Hierarchy support which will allow the manufacturer to utilize the cryptographic algorithm to define a constant key or a fixed set of keys to be used for initial system boot. These early boot codes are shipped with the platform and are included in the list of "public keys". During system boot, the platform firmware uses the trusted public keys to verify a digital signature in an attempt to manage and control the security of the platform firmware used in a host system via a TPM device. The options are Disabled and **Enabled**.

Storage Hierarchy

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

Endorsement Hierarchy

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

PH (Platform Hierarchy) Randomization (for TPM Version 2.0 or later)

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

SMCI BIOS-Based TPM Provision Support (Please confirm the description.)

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

TXT Support

Select Enabled to enable Intel Trusted Execution Technology (TXT) support to enhance system security and data integrity. 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 for the system to work properly. (EV DFX is under "IIO Configuration" in the "Chipset/North Bridge" submenu.)

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

▶HTTP BOOT Configuration

Use this feature to configure HTTP Boot settings for your system.

HTTP Boot One Time

If this feature is set to Enabled, the system will automatically boot into the HttpBoot setting that has been previously configured when it is powered up the first time. The options are **Disabled** and Enabled.

Input the description

This feature allows the user to input the description of the boot.

Boot URI

This feature allows the user to boot the system from a network connection.

▶TLS Authenticate Configuration

When this submenu is selected, the following features will be displayed:

▶Server CA Configuration

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

▶Enroll Certification

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

▶Enroll Cert (Certification) Using File

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

Cert (Certification) GUID (Global Unique Identifier)

This feature displays the GUID for this system.

▶Commit Changes and Exit

Select this feature to keep the changes you have made and exit from the system.

▶Discard Changes and Exit

Select this feature to discard the changes you have made and exit from the system.

▶Delete Certification

This feature displays and sets the certificate enrolled in the system. If the certificate is set to Enable, it will be deleted. The options are **Disabled** and Enabled.

▶iSCSI Configuration

iSCSI Initiator Name

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

▶Add an Attempt

▶Delete Attempts

▶Change Attempt Order

▶Intel(R) Optane(TM) DC Persistent Memory Configuration (Available when Apache Pass device is installed)

This submenu configures AEP (Apache Pass) device parameters and displays driver version.

- **Version**: This feature displays the version of DCPMM used in the system.
- **Select an action below**
- **Detected DIMMs**: This feature displays the number of DCPMM memory modules detected by the BIOS.
- **All DIMMs are healthy** (The health status of the DCPMM is displayed.)

▶DIMMs

This submenu allows the user to view and configure the settings of the DCPMM memory modules installed in the system. Select this submenu and press <Enter>, the following items will display:

- Select a specific DIMM that you want to view.
- DIMMs on Socket 0x0000:
- DIMMs on Socket 0x0001:

▶DIMM ID

This submenu allows the user to view and to perform an action on a DCPMM module specified by the user. When this submenu is selected, the following items will display:

- **DIMM UID:** This feature displays the unique ID of the DCPMM module.
- **DIMM handle:** This feature displays the unique handle that the CPU assigns to the DCPMM module.
- **DIMM physical ID:** This feature displays the physical ID of the DCPMM module.
- **Manageability state:** This feature indicates the manageability state of the DCPMM module.
- **Health state:** This feature indicates the health state of the DCPMM module.
- **Health state reason:** This feature indicates the reason that effectuates the health state of the DCPMM module.
- **Capacity:** This feature indicates the capacity of the DCPMM module.
- **Firmware version:** This feature indicates the firmware version of the DCPMM module.
- **Firmware API version:** This feature indicates the firmware API version of the DCPMM module.
- **Lock state:** This feature indicates the lock state of the DCPMM module.
- **Staged firmware version:** This feature indicates the staged firmware version of the DCPMM module.
- **Firmware update status:** This feature indicates the firmware update status of the DCPMM module.
- **Manufacturer:** This feature indicates the manufacturer of the DCPMM module.

Show more details +

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

If the feature, Show more details +, is set to Enabled, the following will display:

- Serial number
- Part number
- Socket
- Memory controller ID
- Vendor ID
- Device ID

- Subsystem vendor ID
- Subsystem device ID
- Device locator
- Subsystem revision ID
- Interface format code
- Manufacturing Info 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

- Peak power budget [mW]
- Avg (Average) power budget [mW]
- Max average power budget [mW]
- Package sparing capable
- Package sparing enabled
- Package spares available
- Configuration status
- SKU violation
- ARS status
- Overwrite DIMM status
- Last shutdown time
- Viral policy enable
- Viral state
- Latched Last shutdown status
- Unlatched Last shutdown status
- Security capabilities
- Modes supported
- Boot status
- AIT DRAM enabled
- Error injection enabled
- Media temperature injection enabled
- Software triggers enabled
- Software triggers enabled details
- Poison error injections counter
- Poison error clear counter

- Media temperature injections counter
- Software triggers counter
- Master passphrase enabled

▶Monitor health

Select this submenu to view the health status and thresholds of the DCPMM module specified by the user.

- **Sensor Type:** This feature displays the type of health items that are being monitored.
- **Value:** This feature displays the value of the monitor sensor mentioned above.
- **Non-critical thresholds:** This feature displays the normal threshold value for the DCPMM module to maintain normal operations.
- **Critical lower threshold:** This feature displays the lowest threshold value for the DCPMM module to maintain normal operations.
- **Critical upper threshold:** This feature displays the higher threshold value for the DCPMM module to maintain normal operations.
- **Fatal threshold:** This feature indicates the highest value allowed for the DCPMM module to remain functional. Beyond this value, the DCPMM selected will become non-operational.
- **State:** This feature indicates the health state of the DCPMM module.
- **Alarm enabled state:** This feature indicates the status of the non-critical threshold alarm for the DCPMM module specified by the user.
- **Modify non-critical thresholds:** Use this feature to modify non-critical thresholds.
- **Controller temperature:** This feature displays the controller temperature in Celsius.
- **Media temperature:** This feature displays the media temperature in Celsius.
- **Percentage remaining [%]:** Use this feature to set spare capacity as a percentage. (Min. = 1%, Max. = 99%)

▶Apply changes

Use this feature to apply changes that you've made on the DCPMM modules to the system.

▶Back to main menu

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

▶Update firmware

Use this feature to select the firmware image to be loaded on the DCPMM module. Once it is loaded to the system, 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:** This feature allows the user to select a new firmware version to use.
- **File:** This feature allows the user 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 DCPMM 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(R) Optane(TM) DC Persistent Memory Configuration** menu.

▶Configure security

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

State:

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

- **Enable security:** Use this feature to enable security settings for the onboard DCPMM modules.
- **Secure erase:** Use this feature to erase all the persistent data saved in the DCPMM modules.
- **Freeze lock:** Use this feature to enable the security lock for the onboard DCPMM modules.

▶Back to main menu

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

▶Back to main menu

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

▶Regions

Current configuration

▶Region ID

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

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

The following information is displayed:

- Persistent memory type
- Capacity
- Free capacity

▶Create Goal Configuration

Use this submenu to create goal configuration of DIMM regions.

Select the scope of the new region then set the desired sizes.

Create goal configuration for:
Use this feature to select the target to create goal configuration for the DCPMM modules. The options are **Platform** and Socket.

Reserved [%]:
Enter a value (0-100) to reserve a percentage of the DCPMM 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 [%]:
Enter a value (0-100) to reserve a percentage of the DCPMM capacity for special use in a specific Memory Mode. Please note that this value can be automatically set by the system.

Persistent memory type:

This feature allows the user to specify the type of DCPMM memory capacity to be created. The options are **App Direct** and App Direct Not interleaved.

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.

▶Back to Regions menu

Select this feature and press <Enter> to go back to the Regions submenu.

▶Back to main menu

Select this feature and press <Enter> to go back to the **Intel(R) Optane(TM) DC 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

▶0x00000101

Select this feature and press <Enter>, the following information 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

▶Save

After configuring the settings for the namespace above, click on <Save> to save changes.

▶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

▶Create namespace

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

Name
Press <Enter> to type in a name of namespace.

Region ID
This feature displays the region ID of the DCPMM module. The options are **0x0001** and 0x0002.

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

Capacity input
The options are **Remaining** and Manual. Set this feature to Remaining to use the maximum available capacity. Set this feature to Manual to enter the capacity manually.

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 capacity of namespace.

▶Create namespace

Use this submenu to create a namespace.

▶Back to Namespaces

Select this feature and press <Enter> to go back to the **Namespaces** submenu.

▶Back to main menu

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

▶Total capacity

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

- **Raw capacity**: This feature specifies the raw capacity of the DCPMM module.
- **App. Direct capacity**: This feature specifies the App. direct capacity of the DCPMM module.
- **Memory capacity**: This feature specifies the memory capacity of the DCPMM module.
- **Unconfigured capacity**: This feature specifies the capacity of the DCPMM module that has not been configured.
- **Inaccessible capacity**: This feature specifies the capacity of the DCPMM memory that is not accessible to the user.
- **Reserved capacity**: This feature specifies the capacity of the DCPMM memory that is reserved for a particular use.

▶Back to main menu

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

▶Diagnostics

Perform diagnostic tests on DIMMs.

Choose diagnostics type:

Quick diagnostics

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

DIMM ID

Select Enabled for the quick diagnostics test to be performed on the DCPMM module. The options are **Enabled** and Disabled. (**Note**: More DIMM IDs will appear If more DCPMM modules are installed on the motherboard.)

Config (Configure) diagnostics

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

FW (Firmware) diagnostics

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

Security diagnostics

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

▶Execute tests (execute selected diagnostic tests)

Select this feature and press <Enter> to execute the selected diagnostic tests.

▶Back to main menu

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

▶Preferences

Use this submenu to display and/or modify user 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 DCPMM 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)**.

App Direct granularity:

This feature allows the user to view and modify the minimum App Direct Granularity for each DIMM installed on the motherboard. The options are **Recommended** and 1.

▶Back to main menu

Use this feature to go back to the **Intel(R) Optane(TM) DC Persistent Memory Configuration menu**.

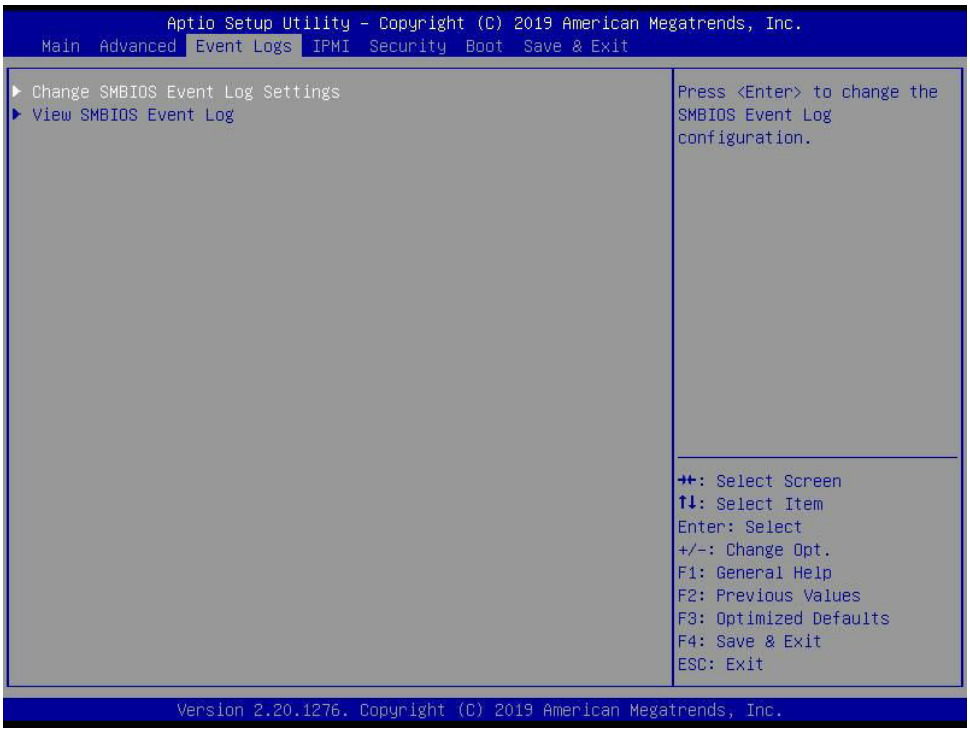
▶Driver Health

This submenu displays the health status of the drivers and controllers as detected by the system.

4.4 Event Logs

Use this feature to configure Event Log settings.

Note: After you've made a change on a setting below, please be sure to reboot the system for the change to take effect.



▶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

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

When Log is Full

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

SMBIOS Event Log Standard Settings

Log System Boot Event

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

MECI (Multiple Event Count Increment)

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

METW (Multiple Event Count 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**.

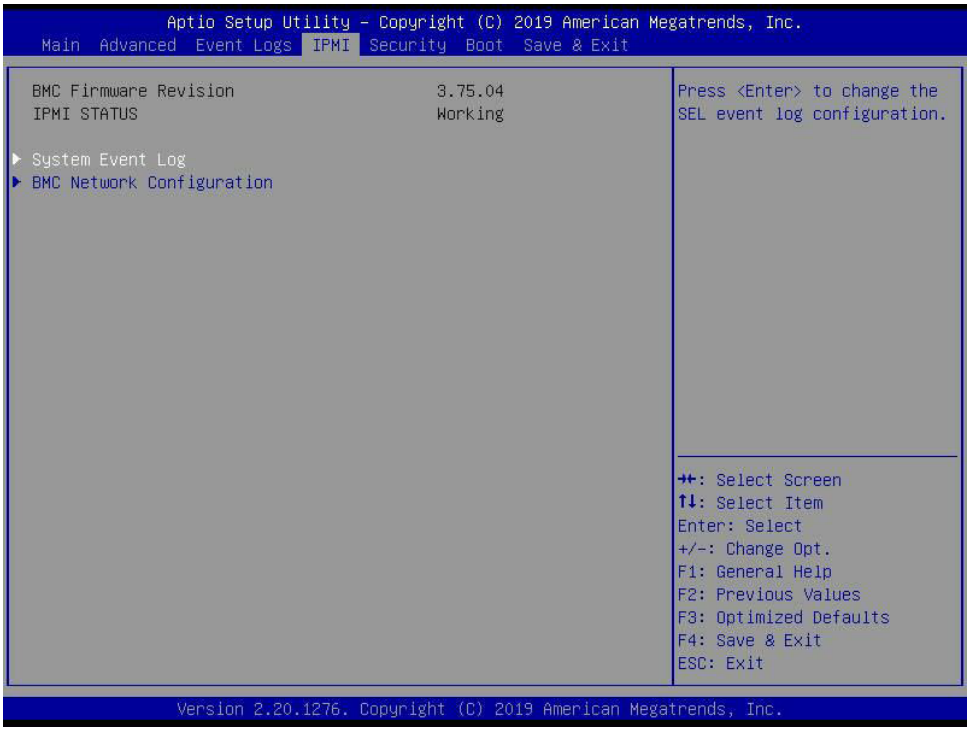
Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

▶View SMBIOS Event Log

This feature allows the user to view the event in the system event log. Select this item and press <Enter> to view the status of an event in the log. The following categories are displayed: **DATE/TIME/ERROR CODE/SEVERITY**

4.5 IPMI

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



BMC Firmware Revision

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

IPMI STATUS (Baseboard Management Controller)

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

▶System Event Log

Enabling/Disabling Options

SEL Components

Select Enabled 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

This feature displays the IPMI LAN setting. The default setting is **Failover**.

IPMI Network Link Status:

This feature displays the IPMI Network Link status. The default setting is **Dedicated LAN**.

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

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

Station IP Address

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

Subnet Mask

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

Station MAC Address

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

Gateway IP Address

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

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

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

VLAN ID (Available when VLAN is set to Enable)

Use this feature to enter the VLAN ID. The default setting is **1**.

Configure IPv6 support

IPv6 address status

This feature displays the IPMI LAN IPv6 status. The options could be SLAAC, DHCPv6, and Unknown(-).

IPv6 Support (Available when Update IPMI LAN Configuration is set to Yes)

This feature displays the IPMI LAN setting. The options are Enabled and **Disabled**.

Configuration Address Source (Available when Update IPMI LAN Configuration is set to Yes and IPv6 Support is set to Enabled)

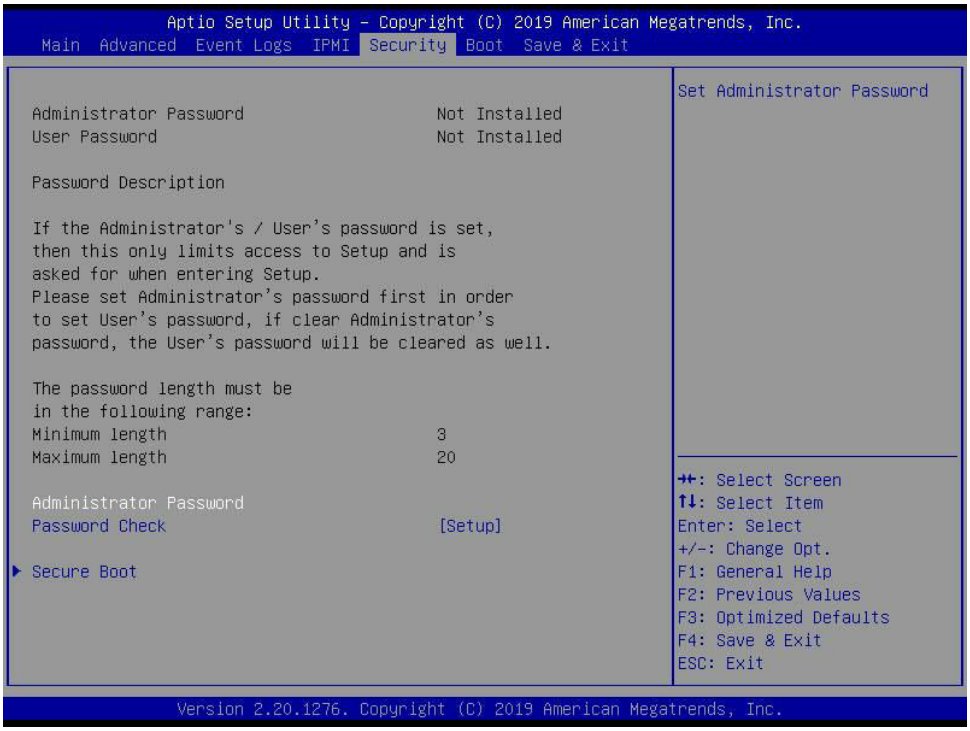
Use this feature to select the IP address source for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, AMI BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server attached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

The following information is displayed:

- Station IPv6 address: This feature displays the station IPv6 address.
- Prefix Length: This item displays the prefix length.
- IPv6 Router1 IP Address: This feature displays the IPv6 router IP address.

4.6 Security

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



Administrator Password

Use this feature 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.

User Password

Use this feature to set the user 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 at system boot and upon entering the BIOS Setup utility. The options are **Setup** and Always.

▶Secure Boot

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

- 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**.

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

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

Vendor Keys

Provision Factory Defaults

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

▶Restore Factory Keys

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

▶Reset To Setup Mode

Select Yes to reset the system to the Setup Mode. The options are **Yes** and No.

▶Export Secure Boot variables

This feature is used to copy the NVRAM content of Secure Boot variables to a storage device.

▶Enroll Efi Image

Select this feature and press <Enter> to specify an EFI (Extensible Firmware Interface) image for the system to use when it operates in the Secure Boot mode.

Device Guard Ready

▸Remove 'UEFI CA' from DB

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

▸Restore DB defaults

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

Secure Boot variable: Size/Key#s/Key Source

▶Platform Key (PK)

This feature allows the user to enter and configure a set of values to be used as platform firmware keys for the system. The sizes, keys numbers, and key sources of the platform keys will be indicated as well. Select Update to update the platform key.

▶Key Exchange Keys

This feature allows the user to enter and configure a set of values to be used as Key-Exchange-Keys for the system. The sizes, keys numbers, and key sources of the Key-Exchange-Keys will be indicated as well. Select Update to update your "Key Exchange Keys". Select Append to append your "Key Exchange Keys".

▶Authorized Signatures

This feature allows the user 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".

▶Forbidden Signatures

This feature allows the user to enter and configure a set of values to be used as Forbidden Signatures for the system. These values also indicate sizes, keys numbers, and key sources of the forbidden signatures. Select Update to update your "Forbidden Signatures". Select Append to append your "Forbidden Signatures".

▶Authorized TimeStamps

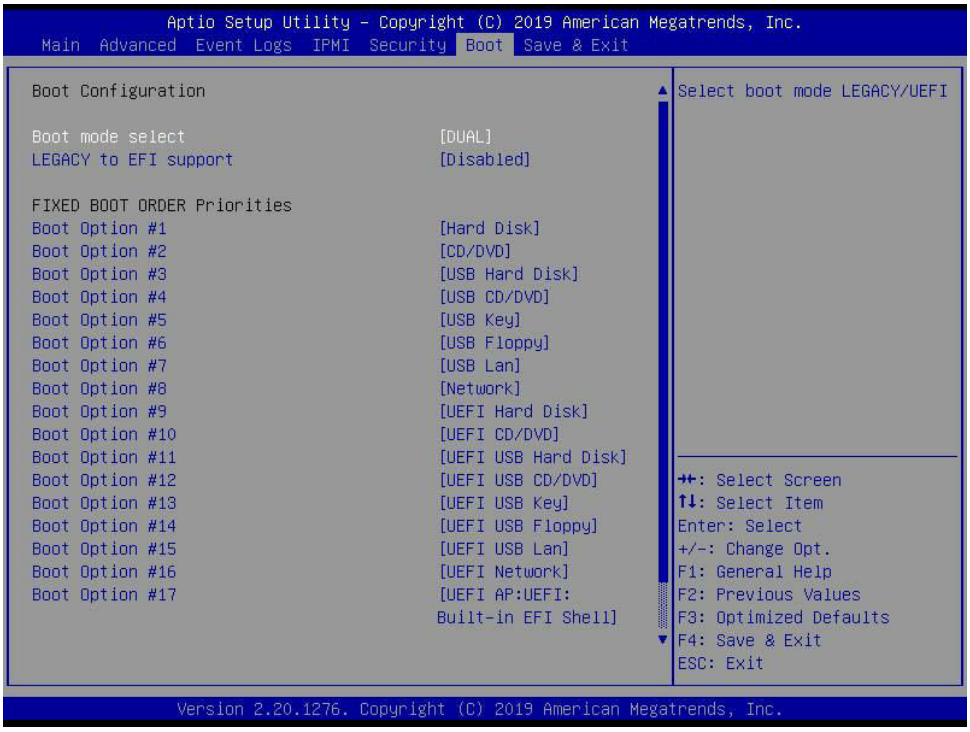
This feature allows the user to set and save the timestamps for the authorized signatures which will indicate the time when these signatures are entered into the system. Select Update to update your "Authorized TimeStamps". Select Append to append your "Authorized TimeStamps".

▶OsRecovery Signatures

This feature allows the user to set and save the authorized signatures used for OS recovery. Select Update to update your "OS Recovery Signatures". Select Append to append your "OS Recovery Signatures".

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.** The default setting is **DUAL**.

LEGACY to EFI support

Select Enabled for the system to boot from an EFI OS when the Legacy OS fails. The options are **Disabled** and Enabled.

FIXED BOOT ORDER Priorities

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

When the feature above -"Boot Mode Select" is set to **Dual** (default), the following items will be displayed for user's configuration:

- Boot Option #1 - Boot Option #17

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

- Boot Option #1 - Boot Option #8

When the feature above -"Boot Mode Select" is set to UEFI, the following items will be displayed for configuration:

- Boot Option #1 - Boot Option #9

▶Add New Boot Option

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

Add Boot Option

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

Path for Boot Option

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

Boot Option File Path

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

Create

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

▶Delete Boot Option

Use this feature to select a boot device to delete from the boot priority list.

Delete Boot Option

Use this feature to remove an EFI boot option from the boot priority list. The options are **Select one to Delete** and UEFI: Built-in EFI Shell.

▶UEFI Application Boot Priorities (Available when any USB/HDD/ Network device is attached)

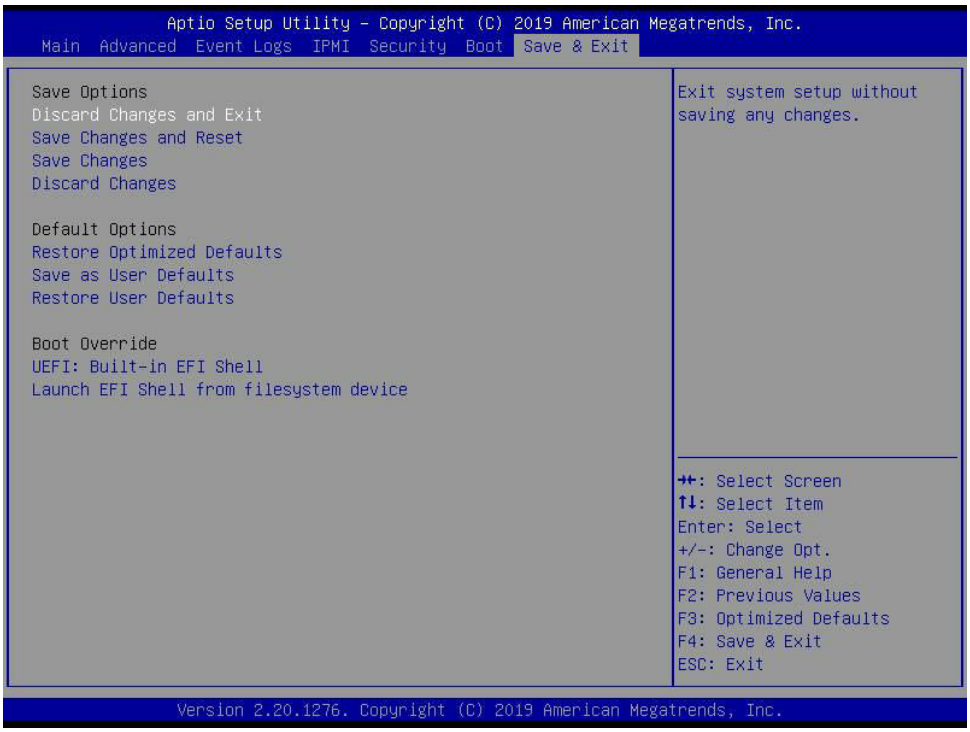
Use this feature to specify a boot device priority sequence from available UEFI application.

Boot Option #1

Use this feature to set the system boot order. The options are **UEFI: Built-in EFI Shell** and Disabled.

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

Save Changes and Reset

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

Save Changes

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

Discard Changes

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

Restore Optimized Defaults

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

Save as User Defaults

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

Restore User Defaults

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

Boot Override

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

UEFI: Built-in EFI Shell

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

Launch EFI Shell from filesystem device

This feature allows the user to launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

Appendix A

Software

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

A.1 Microsoft Windows OS Installation

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

Installing the OS

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

2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.

3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing **F11** during the system startup.

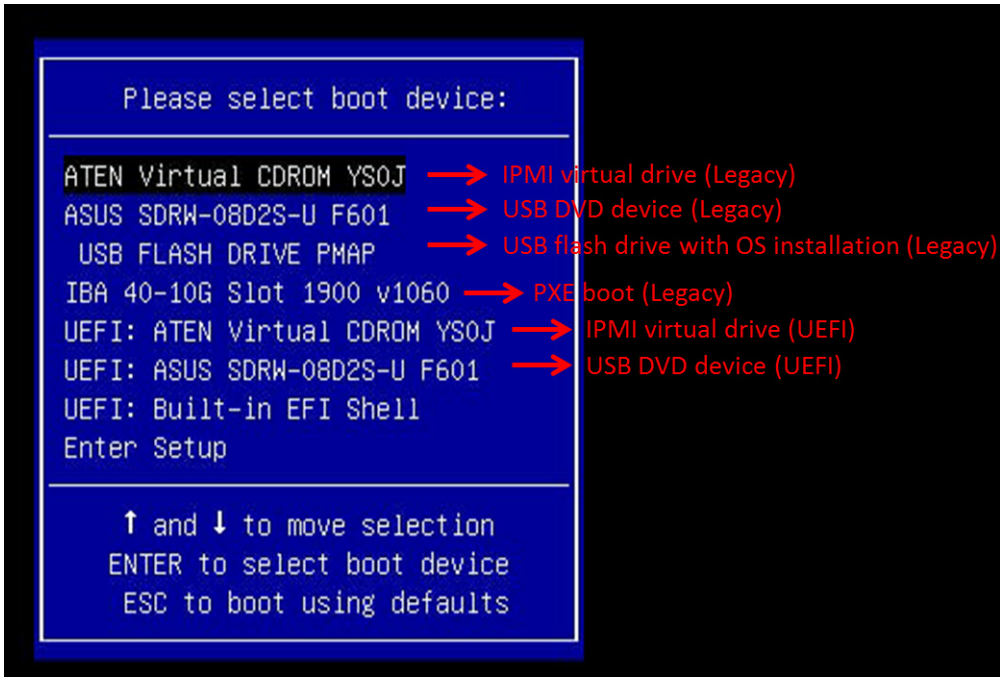


Figure A-1. Select Boot Device

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

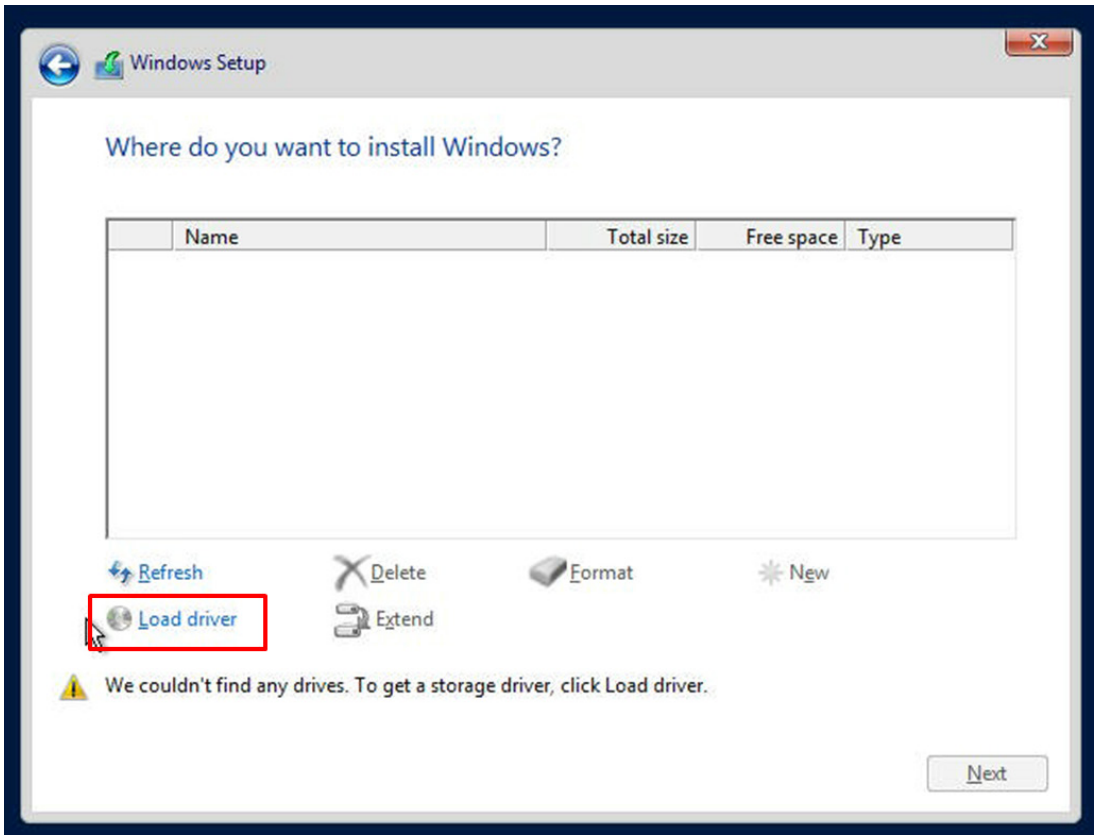


Figure A-2. Load Driver Link

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

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

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

A.2 Driver Installation

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

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

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

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

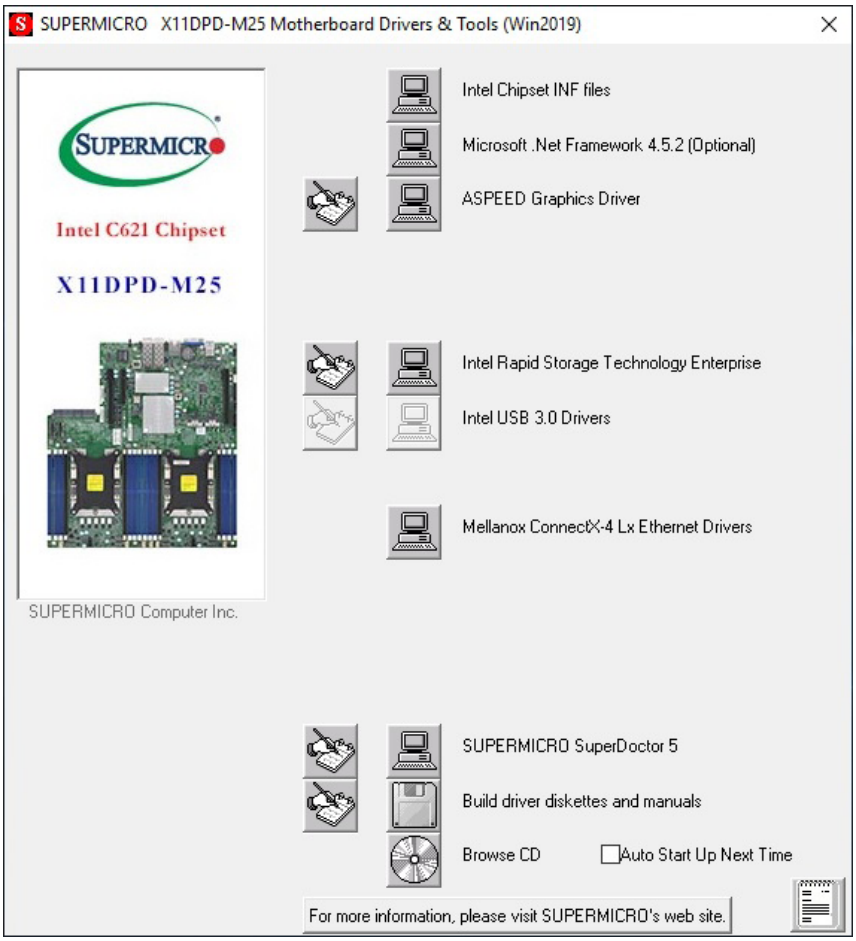


Figure A-3. Driver & Tool Installation Screen

Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to the bottom) one at a time. **After installing each item, you must 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.

A.3 SuperDoctor 5

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

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

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

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

A.4 IPMI

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

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

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

Supermicro ships standard products with a unique password for the BMC 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 B

Standardized Warning Statements

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

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

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

Battery Handling

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

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

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

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

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

Attention

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

¡Advertencia!

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

אזהרה!

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

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

경고!

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

Waarschuwing

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

Product Disposal

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

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

警告
本产品的废弃处理应根据所有国家的法律和规章进行。

警告
本產品的廢棄處理應根據所有國家的法律和規章進行。

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

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

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

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

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

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

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

Appendix C

UEFI BIOS Recovery

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

C.1 Overview

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

C.2 Recovering the UEFI BIOS Image

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

Note 1: Follow the BIOS recovery instructions in Section C.3 for BIOS recovery when the main BIOS block crashes.

Note 2: If the recovery instructions in Section C.3 for BIOS recovery fail, you may use the Supermicro Update Manager (SUM) Out-of-Band (OOB) (https://www.supermicro.com.tw/products/nfo/SMS_SUM.cfm) to reflash the BIOS.

Note 3: If the recovery block processes stated in Note 1 and Note 2 above fail, you will need to follow the procedures to make a Returned Merchandise Authorization (RMA) request. Refer to Section 3.5 for more information about the RMA request.

C.3 Recovering the Main BIOS Block with a USB Device

This feature allows the user to recover the main BIOS image using a USB-attached device without additional utilities used. A USB flash device such as a USB Flash Drive, or a USB CD/DVD ROM/RW device can be used for this purpose. However, a USB hard disk drive cannot be used for BIOS recovery at this time. The file system supported by the recovery block is FAT (including FAT12, FAT16, and FAT32) which is installed on a bootable or non-bootable USB-attached device.

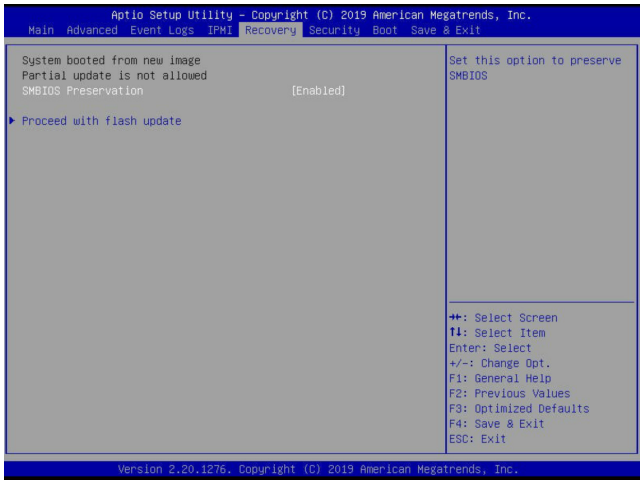
To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below.

1. Please use a different machine to download the BIOS package for your motherboard or your system from the product page available on our website at www.supermicro.com.
2. Extract the BIOS package to a USB device and rename the BIOS ROM file [BIOSname#.###] that is included in the BIOS package to SUPER.ROM for BIOS recovery use.
3. Copy the SUPER.ROM file into the Root "\" directory of the USB device.

Note: Before recovering the main BIOS image, confirm that the SUPER.ROM file you have is the same version or a close version meant for your motherboard.

4. Insert the USB device that contains the SUPER.ROM file into the system before you power on the system or when the following screen appears.

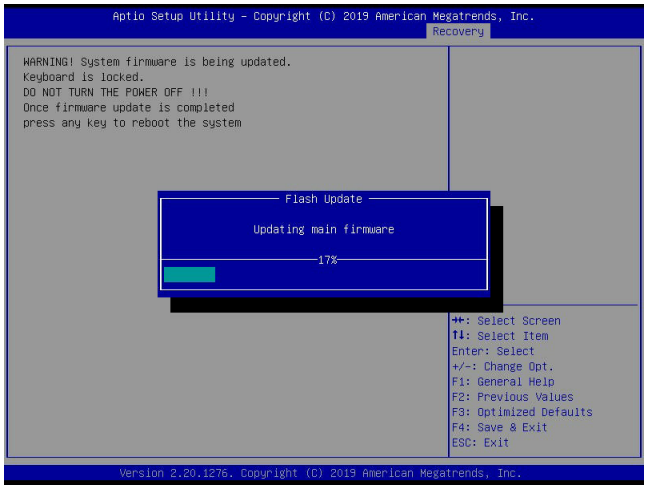
5. After locating the SUPER.ROM file, the system will enter the BIOS Recovery menu as shown below.



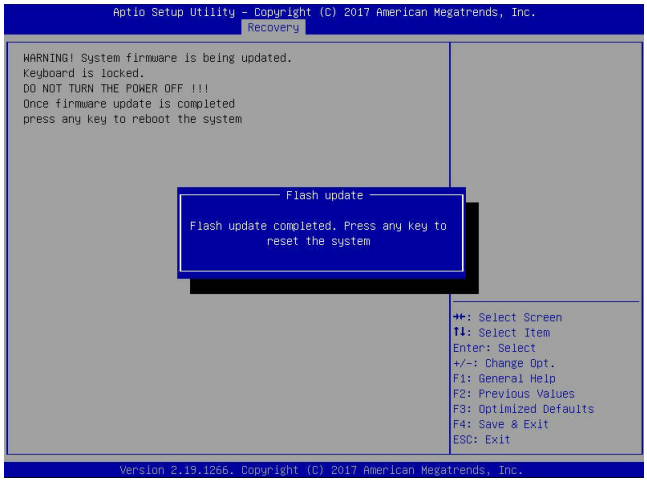
Note: At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

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

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

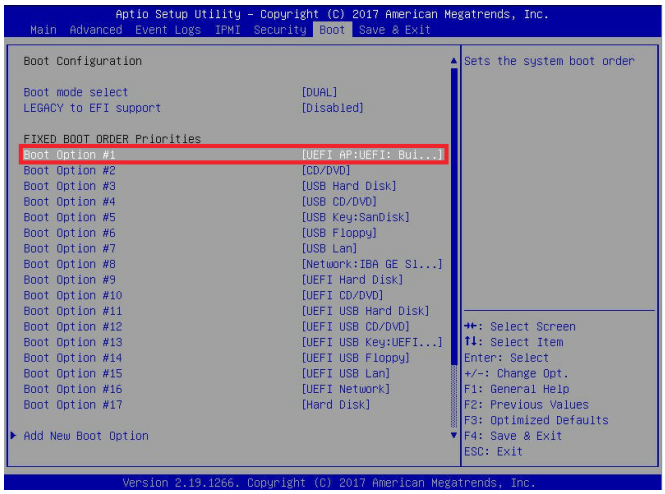


7. After the BIOS recovery process is complete, press any key to reboot the system.

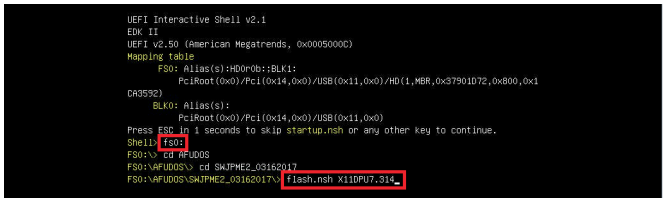


Note: It is recommended that you update your BIOS after BIOS recovery. Please refer to Chapter 3 for BIOS update instructions.

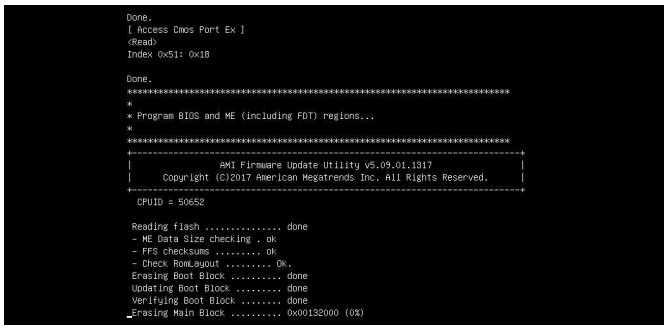
8. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the BIOS Setup utility.



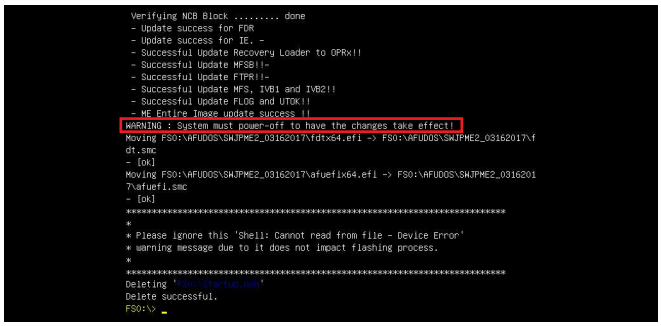
9. When the UEFI Shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier in Step 2. Enter flash.nsh BIOSname#.### at the prompt to start the BIOS update process.



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



10. The screen above indicates that the BIOS update process has completed. Reboot the system when you see the screen below.



Appendix D

Configuring VROC RAID Settings

Intel Virtual RAID on CPU (Intel VROC) is a RAID (Redundant Array of Independent Disks) solution that integrates with Intel Volume Management Device (Intel VMD) for Non-Volatile Memory Express (NVMe) solid-state drives (SSDs). The D.1 section provides instructions on how to access the All Intel VMD Controller menu. The D.2 section provides instructions on how to configure RAID settings. The D.3 section describes the use of journaling drive for the RAID5 volume (parity based RAID).

Note 1: Only use NVMe devices that have been validated by Supermicro. For the latest updates, please contact us or refer to our website at https://www.supermicro.com.

Note 2: Depending on the version of driver/utility/package, it may or may not have exactly the same as the BIOS settings/features shown in the appendix.

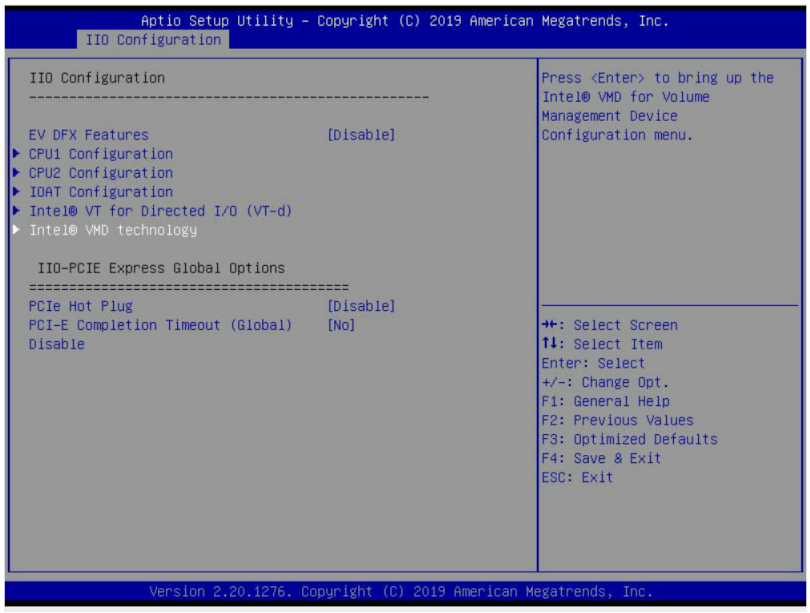
D.1 All Intel VMD Controllers Menu

The following section provide you with instructions on how to access the **All Intel VMD Controllers menu** which will allow you to enable a selected PCI slot for VMD support.

Enabling a PCI Slot for VMD Support in the BIOS Setup Utility

1. Press <Del> during system boot to enter the BIOS Setup utility.
2. Use the arrow key to select **Advanced** on top of the BIOS menu bar.
3. Use the down arrow key to select **Chip Configuration** and press <Enter>.
4. Select **North Bridge** and press <Enter>.
5. Use the down arrow key to select **IIO Configuration** and press <Enter>.

6. When the following screen displays, use the down arrow key to select **Intel® VMD Technology** and press <Enter> to enter the Intel VMD Technology submenu.



7. When the Intel VMD Technology submenu appears, it will display all the PCI slots that can be configured for VMD support on the screen.

8. From the available PCI slots displayed on the screen, select a PCI slot you want to use for a VMD device by highlighting it.

9. Select the option [Enable] and press <Enter> to enable the selected slot for VMD support.

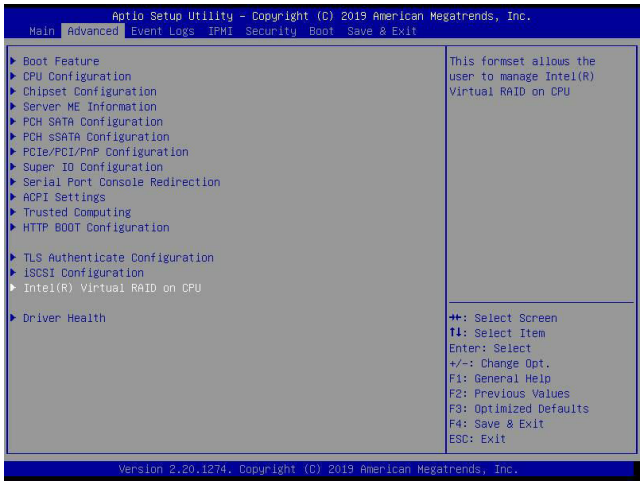
10. Repeat Step 8 ~ Step 9 to select and enable all the PCI slots of your choice for VMD support.

11. After enabling all PCI slots for VMD support on the BIOS Setup utility, install the VMD devices (such as add-on cards) on the slots that you've configured for VMD support on the motherboard. For the changes to take effect,

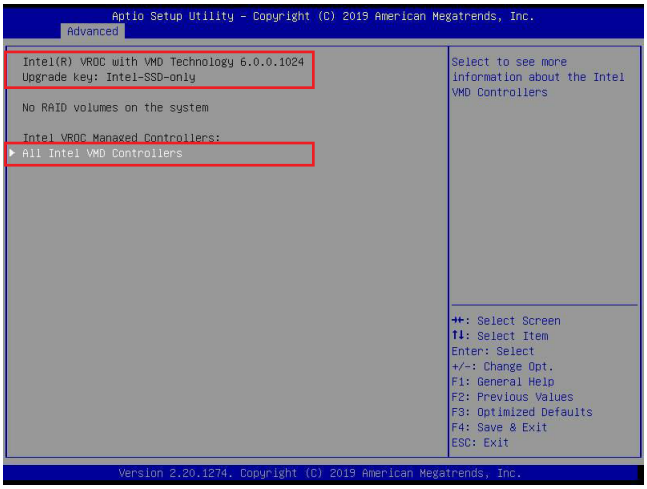
12. Press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility.

Note: After you've enabled VMD in the BIOS on a PCIe slot of your choice, 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.

13. Navigate to the Advanced tab.



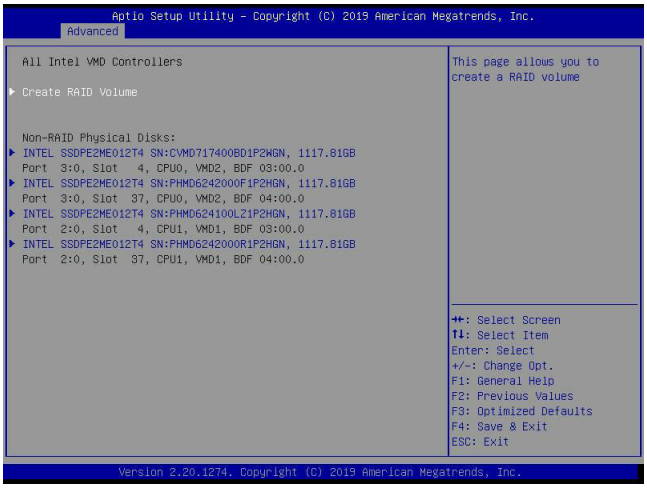
14. Use the arrow keys to select Intel(R) Virtual RAID on CPU and press <Enter> to access the menu items. The following screen will appear showing that the feature "**All Intel VMD Controllers**" has become available.



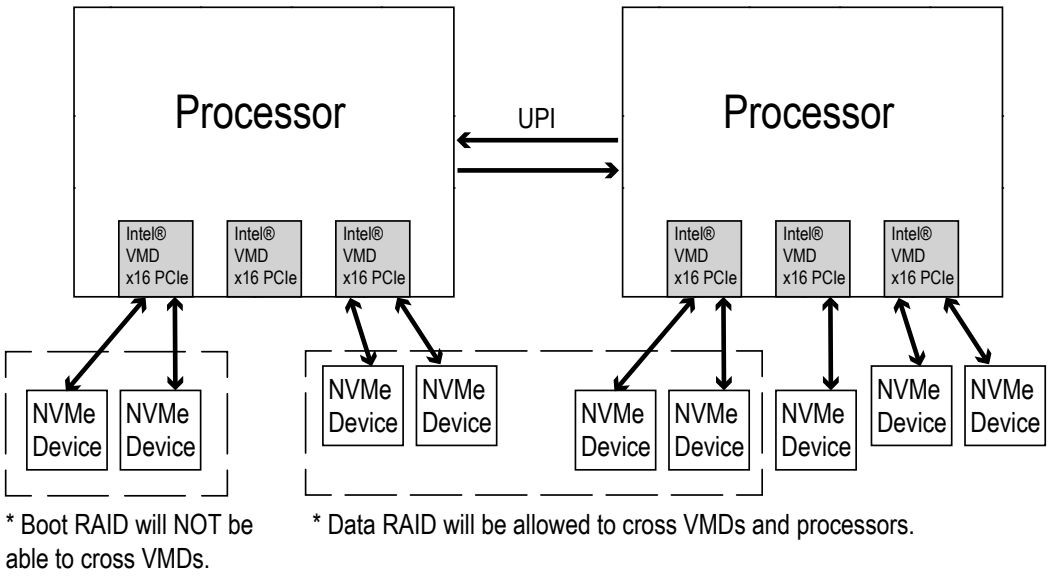
Note 1: The license and header (on the motherboard) for Intel VROC hardware key are required. Also, be sure the version of Intel Rapid Storage Technology enterprise (Intel RSTe) VROC utility is 5 or above (look for Intel(R) VROC with VMD Technology x.x.x.xxxx shown on the screen).

Note 2: Intel VROC Premium hardware key is used in the appendix to demonstrate RAID settings.

15. Use the arrow keys to select **All Intel VMD Controllers** and press <Enter> to access the menu items. The following screen will appear. It allows the user to create RAID volumes and configure settings of NVMe devices as detected by the system.

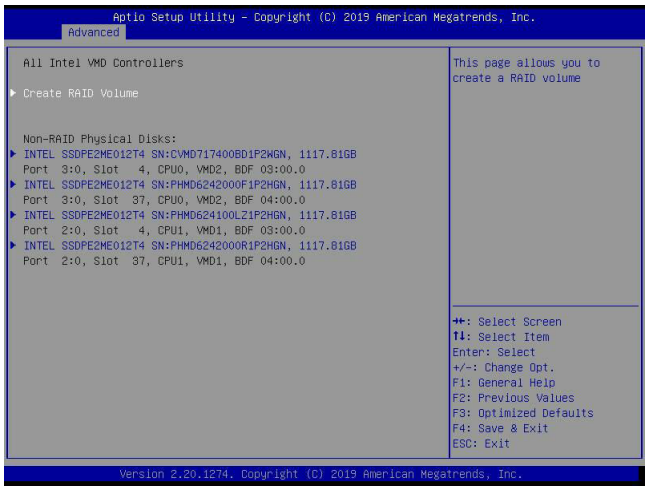


Note : A single Intel VMD supported processor supplies 48 PCIe lanes and contains three Intel VMD controllers (domains). Refer to the following illustration for more information.



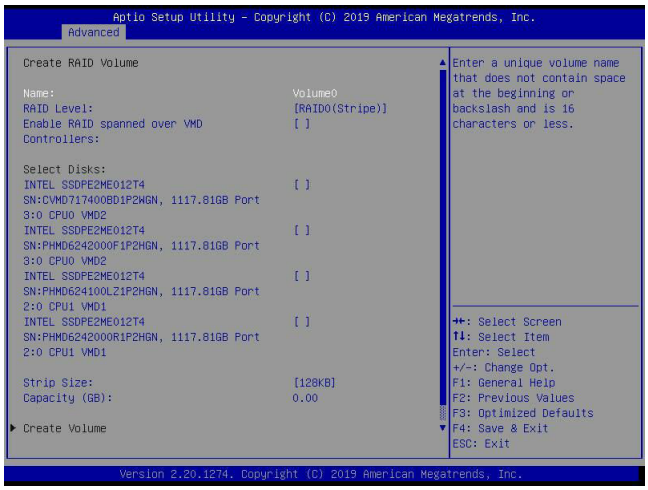
D.2 Configuring RAID Settings

Follow the instructions stated in the D.1 section to access the **All Intel VMD Controllers** menu items, the following screen will appear. Please carefully follow the instructions listed in this section to configure RAID settings for your devices as desired.



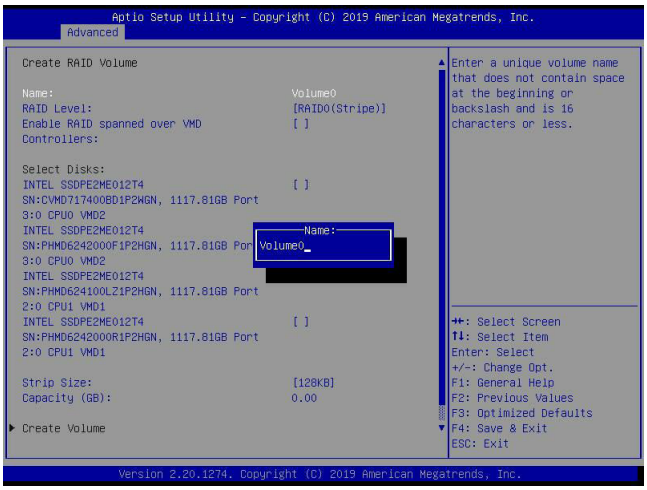
To Create a RAID Volume

Use the arrow keys to select **Create RAID Volume** from the screen above and press <Enter> to create a RAID Volume. The Create RAID Volume submenu, which allows you to configure the settings of the RAID volume you've created, will appear as shown below.



To Enter a Name for the RAID Volume

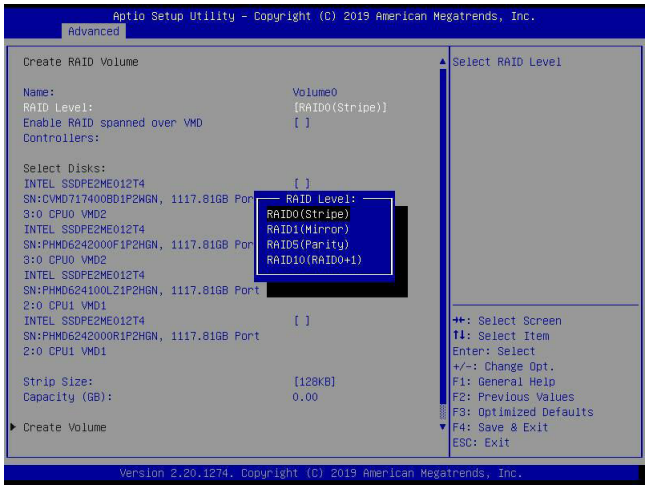
From the **Create RAID Volume** submenu as shown on the previous screen, use the arrow keys to select **Name** and press <Enter>, and the following screen will display.



When the screen above displays, enter a unique name for the RAID volume.

To Set the RAID Level for the RAID Volume

From the **Create RAID Volume** submenu, select **RAID Level** and press <Enter>. The following screen will display.



Use the arrow keys to select the desired RAID level for the RAID volume that you've created. The options are **RAID0(Stripe)**, RAID1(Mirror), RAID5(Parity), and RAID10(RAID0+1).

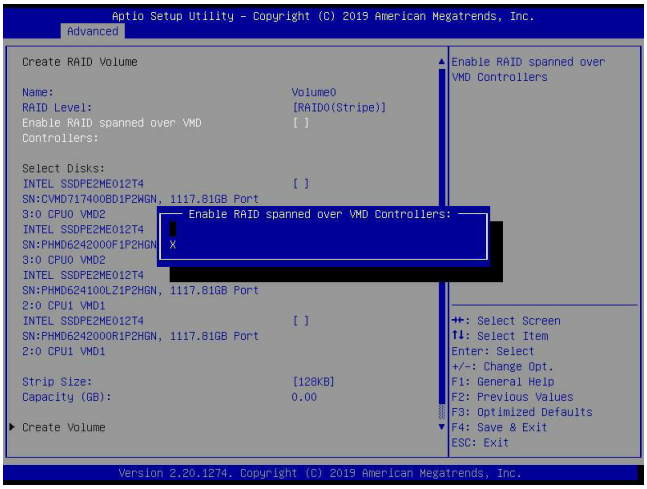
Note 1: The RAID level(s) displayed is(are) based on the number of NVMe devices connected to the system.

Note 2: For RAID0/RAID1/RAID5/RAID10, the minimum number of NVMe devices required is two/two/three/four respectively.

Note 3: Use Intel VROC Standard hardware key to support RAID 0/1/10. Use Intel VROC Premium hardware key (or Intel SSD Only hardware key) to support RAID 0/1/5/10.

Enabling RAID Spanned over VMD Controllers

From the **Create RAID Volume** submenu, use the arrow keys to select **Enter RAID spanned over VMD Controllers** and press <Enter>. The following screen will display.

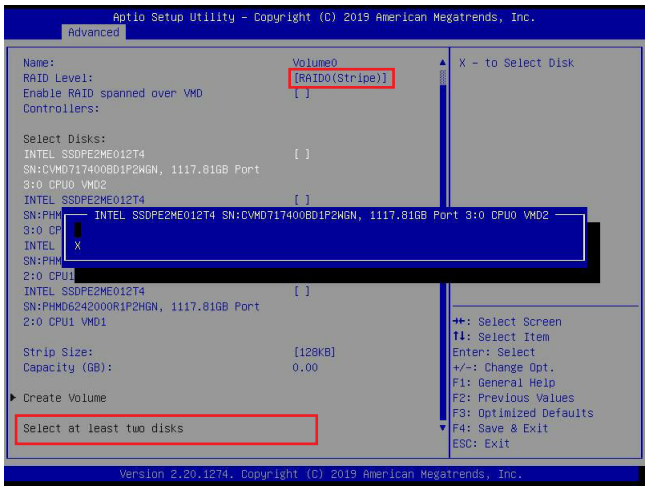


Enter a desired setting for your RAID volume in the pop-up menu. The options are **(not selected)** and X (selected). Please set this feature to X if the RAID level you selected earlier from Step 3 will cross VMD domains.

Note: For a bootable RAID volume, do not cross VMD domains.

To Select Disks for the RAID Volumes

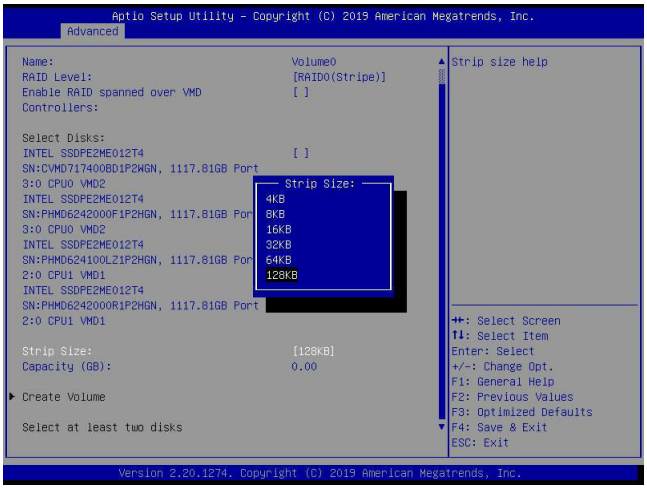
From the **Create RAID Volume** submenu, use the arrow keys to highlight **Select Disk:** and press <Enter>. The following screen will display.



The options are **(not selected)** and X (selected). Set the features one by one to X to select the desired RAID disks for your RAID volumes.

To Set Strip Size for the RAID Volume

From the **Create RAID Volume** submenu, use the arrow keys to select **Strip Size:** and press <Enter>. The following screen will display.

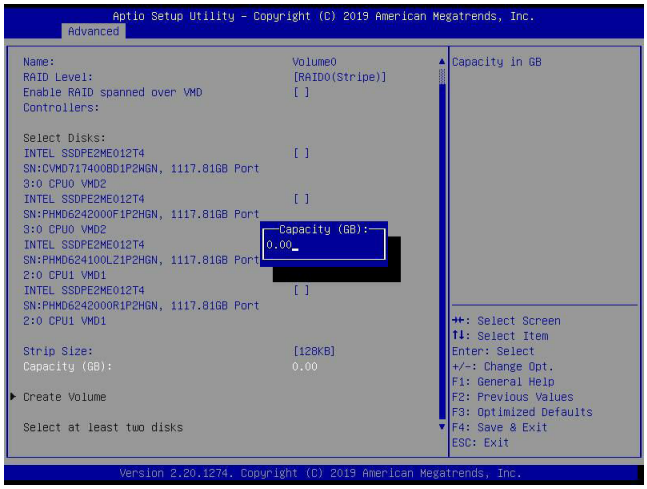


From the pop-up menu as shown above, select the desired RAID strip size for your RAID volume and press <Enter>. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**.

Note: For RAID5, the options are 4KB, 8KB, 16KB, 32KB, **64KB**, and 128KB. For RAID10, the options are 4KB, 8KB, 16KB, 32KB, and **64KB**.

To Set the Capacity (GB) for the RAID Volume

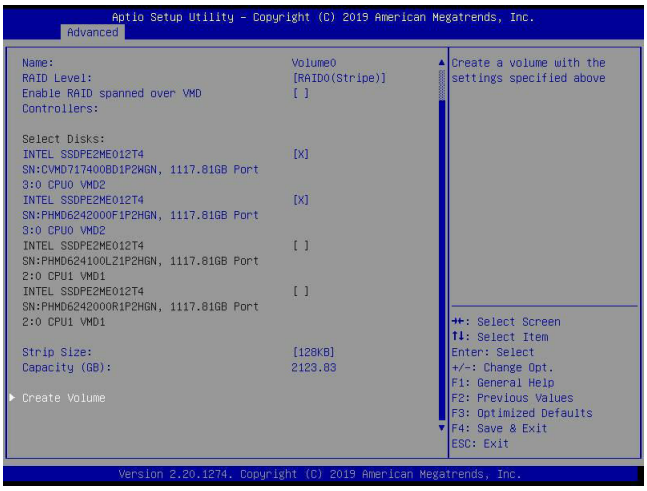
From the **Create RAID Volume** submenu, use the arrow keys to select **Capacity (GB):** and press <Enter>. The following screen will display.



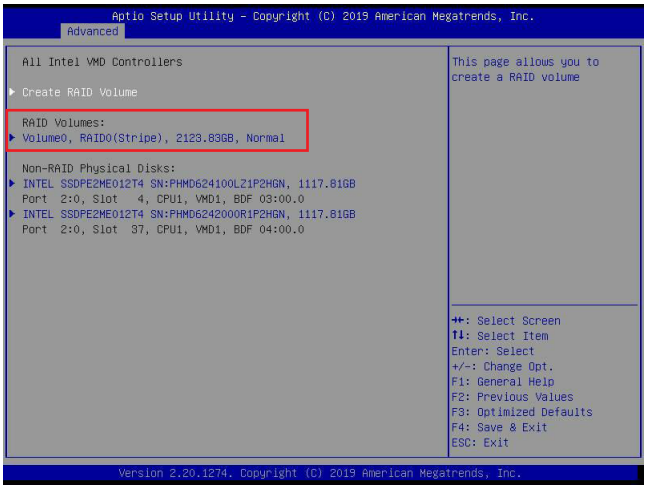
Enter the desired RAID capacity (in GB) in the pop-up menu to set the capacity for your RAID volume.

To Create Volumes

To finalize your RAID volume configuration, select **Create Volume** from the **Create RAID Volume** submenu as shown on the screen below.

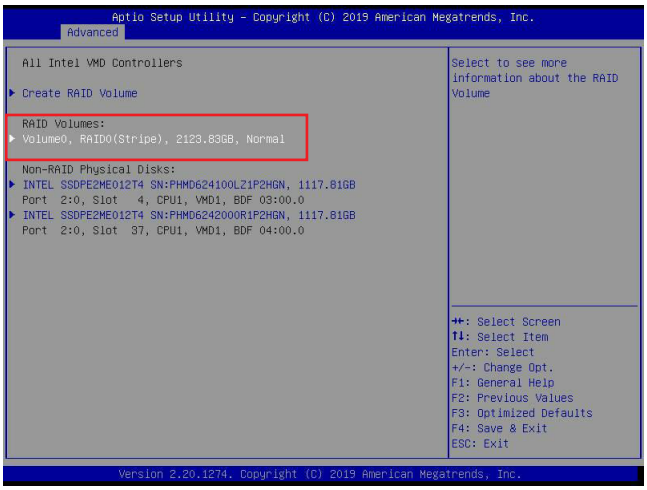


After selecting **Create Volume**, press <Enter>. The following screen will appear and display RAID volumes as shown below.



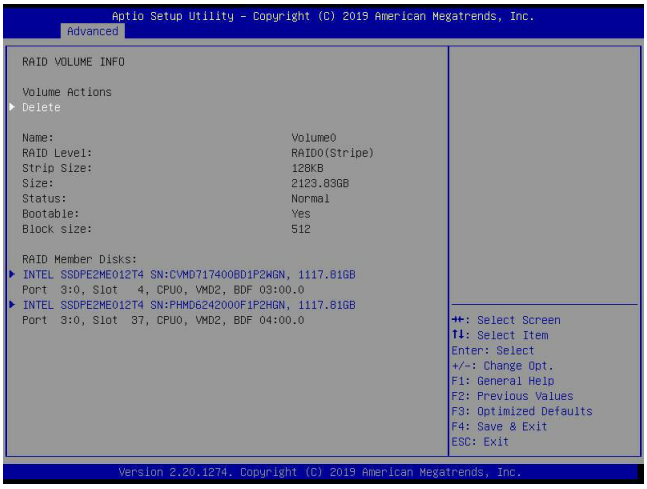
To Display RAID Volumes

For detailed RAID volume information, use the arrow keys to select the desired RAID volume as shown below.



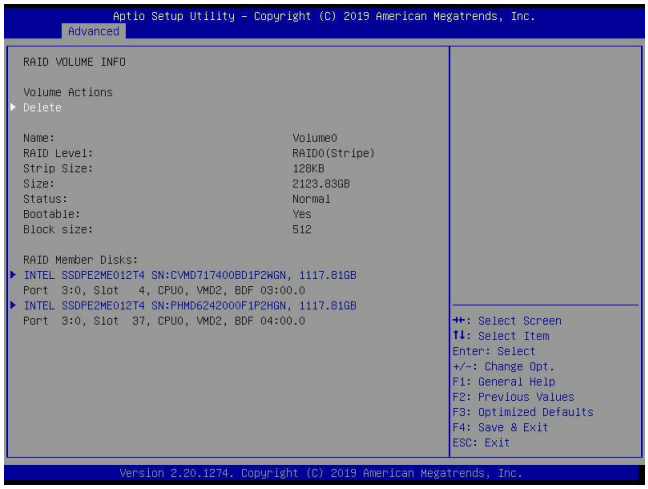
To Display RAID VOLUME Information

When the screen above appears, press <Enter>. The **RAID VOLUME INFO** menu will appear and display the detailed information about the RAID volume you've selected as shown below.



To Delete a RAID Volume

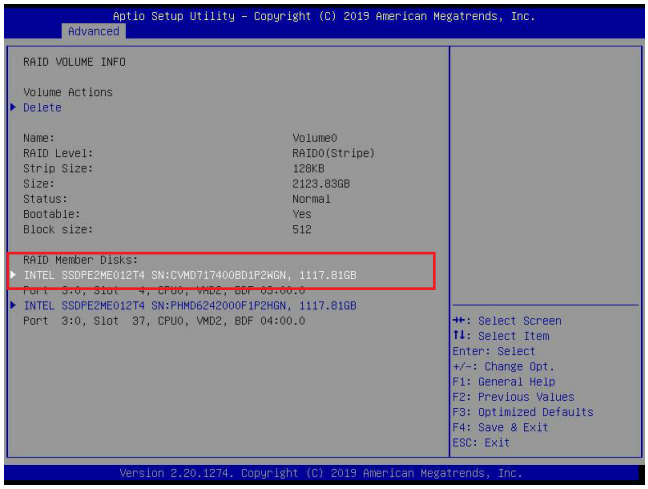
On the **RAID VOLUME INFO** menu, use the arrow keys to select Delete and press <Enter> to delete the RAID volume you have selected.



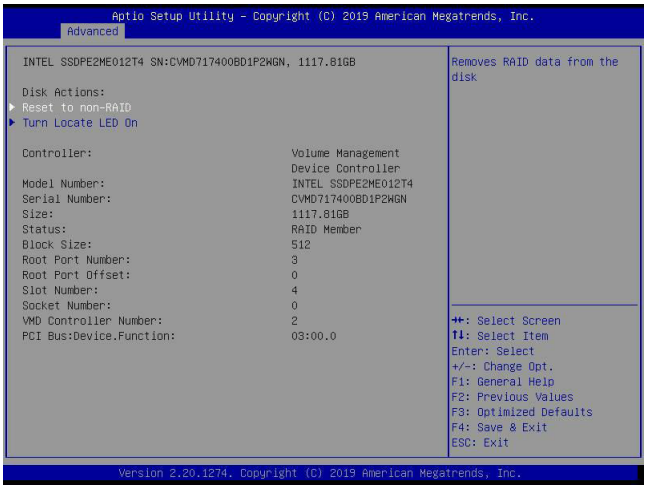
The following screen will appear to confirm if you want to delete the RAID Volume. Select Yes to delete the RAID Volume. The options are **Yes** and No.

To Reset the RAID Volume to non-RAID

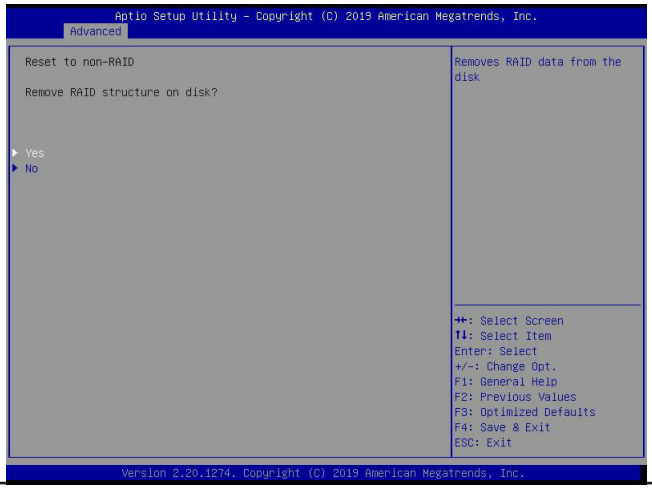
On the **RAID VOLUME INFO** submenu shown on the bottom screen of page 167, select the desired NVMe device from the list of RAID Member Disks and press <Enter> as shown below.



Select **Reset to Non-RAID** from the screen below and press <Enter> to remove RAID data from the selected NVMe device.

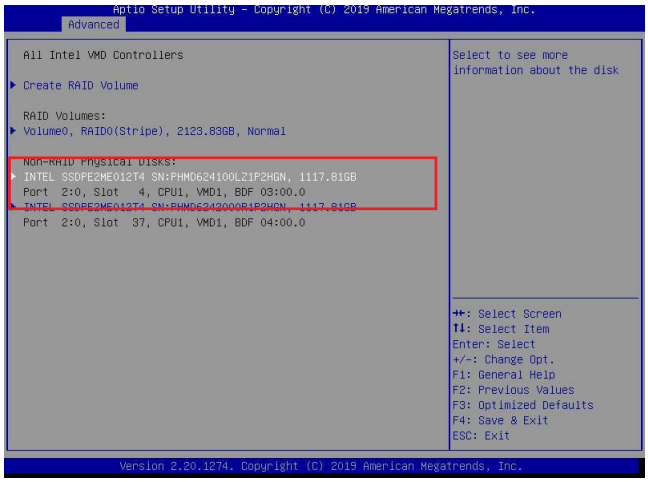


When the following screen appears, select Yes to confirm that you want to set the selected NVMe device to non-RAID. The options are **Yes** and No.

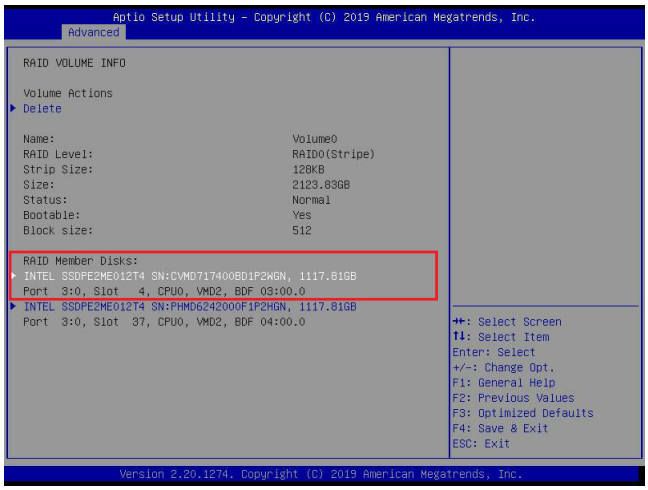


To Turn on the Disk Locator LED

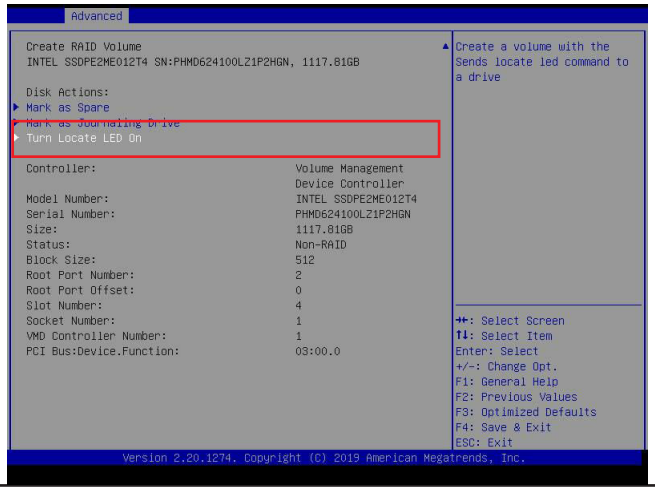
Follow the instructions stated in the D.1 section to access the **All Intel VMD Controllers** menu. When the following screen displays, select a non-RAID physical disk to turn on the disk locator LED to locate a selected device.



You can also select a RAID member disk to locate the selected device.

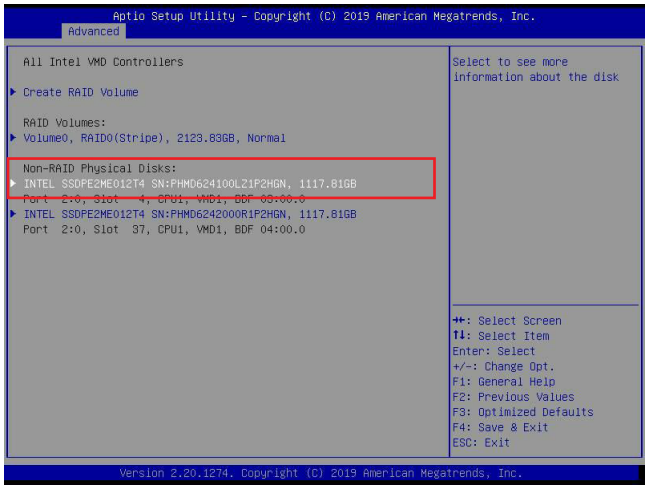


When the following screen appears, use the arrow keys to select **Turn Locate LED On**. Press <Enter> to turn on the locator LED to show the location of the selected device.

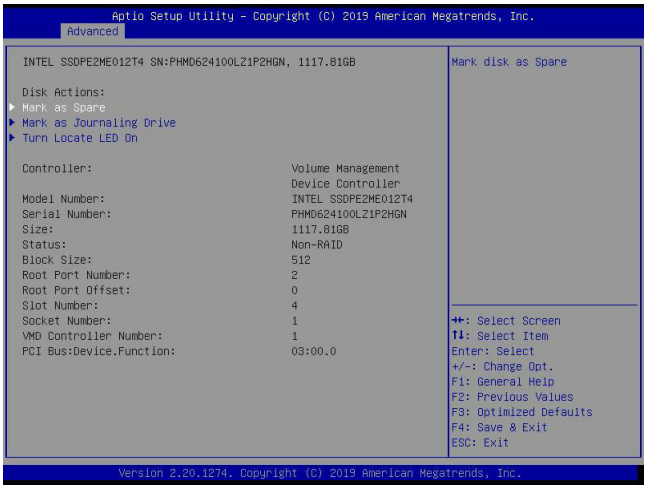


To Mark a RAID Volume as Spare

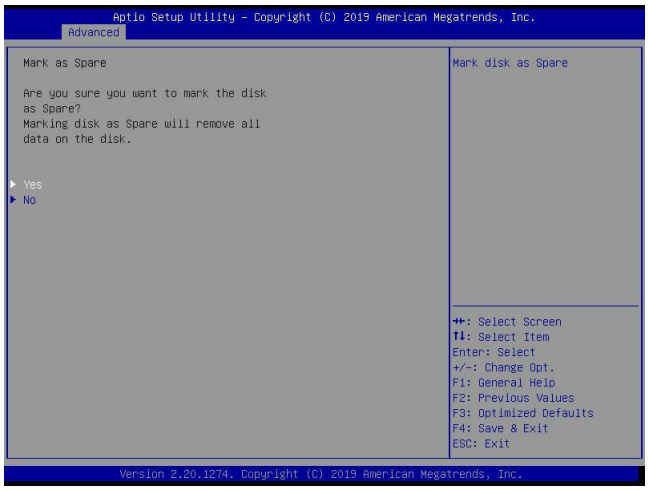
Follow the instructions stated in the D.1 section to access the **All Intel VMD Controllers** menu. When the following screen appears, select a desired NVMe device from the list of Non-RAID Physical Disks.



After a NVMe device is selected, press <Enter> and the following screen will appear. Select **Mark as Spare** and press <Enter> to mark the selected device as a spare device.



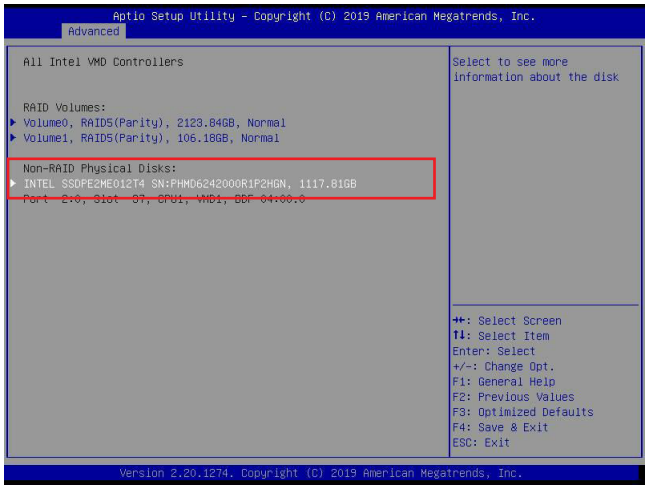
When the following screen appears, select Yes to confirm that you want the selected device to be used as a spare device. The options are **Yes** and No.



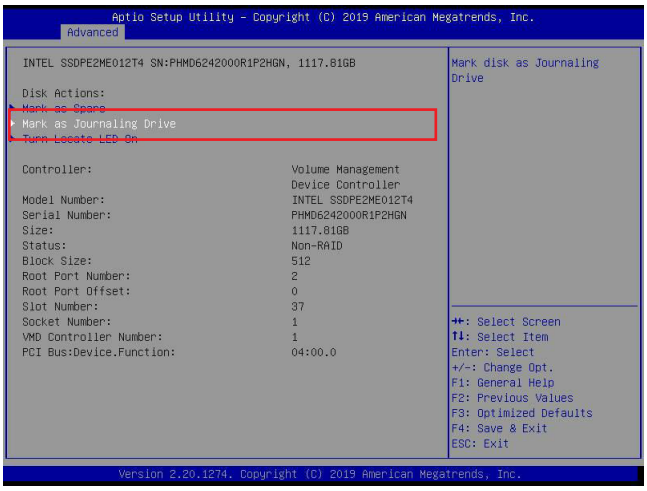
Note: A spare disk is used for automatic RAID volume rebuilds when status of failed, missing, or at risk is detected on the array disk. For a RAID0 volume, only status of at risk will trigger automatic RAID volume rebuilds.

To Mark a RAID Volume as a Journaling Drive

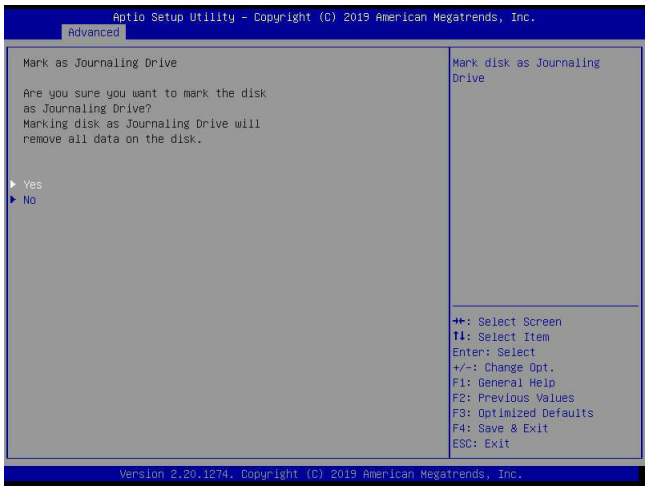
Refer to the instructions stated in the D.1 section to access the All Intel VMD Controllers menu. When the following screen appears, select a desired NVMe device from the list of Non-RAID Physical Disks for use as a journaling drive.



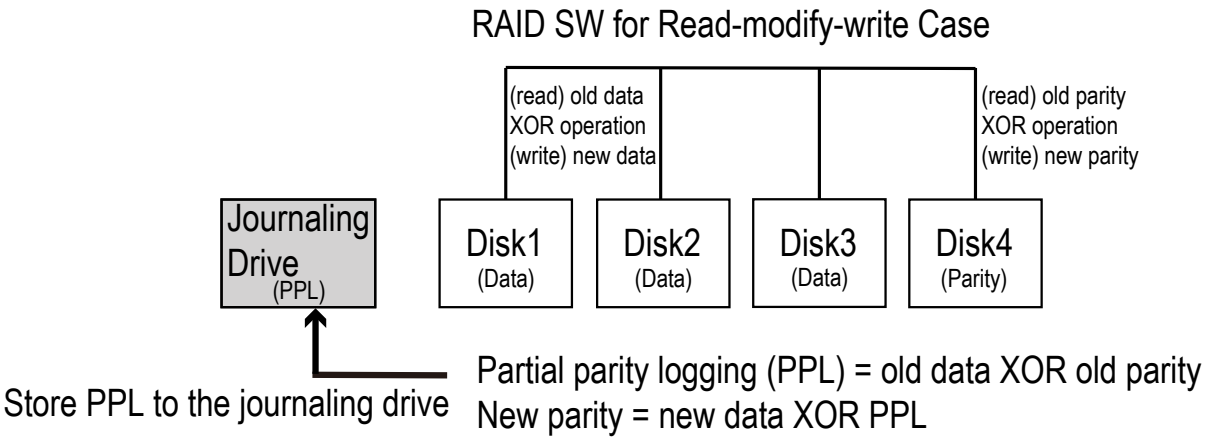
After selecting a NVMe device, press <Enter> and the following screen will appear. Select **Mark as Journaling Drive** and press <Enter>.



When the following screen appears, select Yes to confirm that the selected device is to be used as a journaling drive. The options are **Yes** and No.



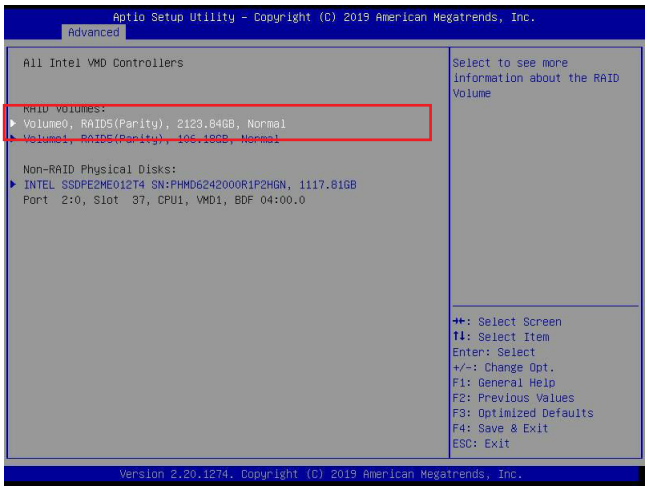
Note: RAID Write Hole (RWH) is a condition associated with a power/drive-failure/crash while writing to a RAID5 volume. The use of journaling drive that contains partial parity logging (PPL) can reduce the potential data loss. Refer to the following illustration for the use of journaling drive.



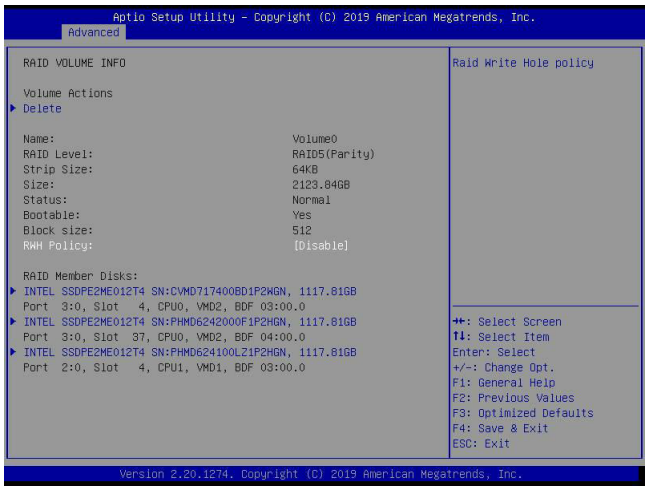
D.3 Use of Journaling Drive

The following section describes the use of a journaling drive for the RAID5 volume, which is a parity-based RAID.

Step 1. Refer to the instructions stated in the D.1 section to access All Intel VMD Controllers menu items. When the following screen appears, use the arrow keys to select the desired RAID5 volume.



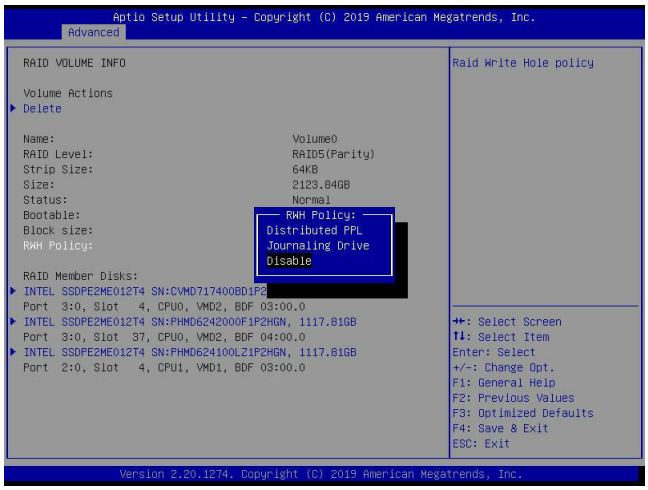
Press <Enter> and the following screen will appear.



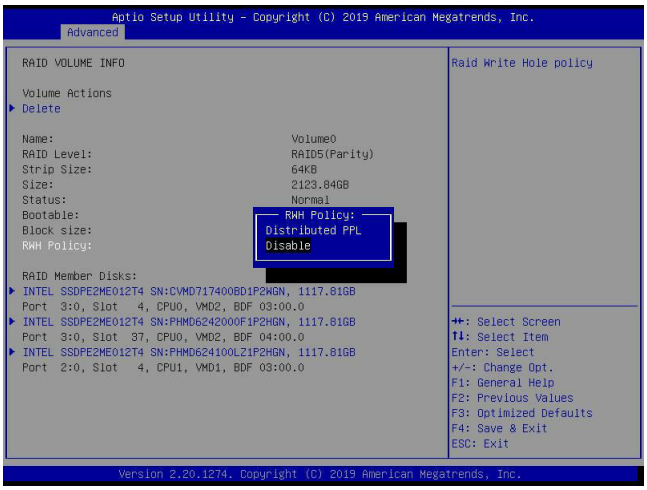
Step 2. Use the arrow keys to select RWH Policy. RWH is a scenario related to a power/drive-failure/crash.

RWH Policy

Press <Enter> and the following screen will appear. If any device has been set as a journaling drive (see pages 173 and 174), the options are Distributed PPL, Journaling Drive, and **Disable**.



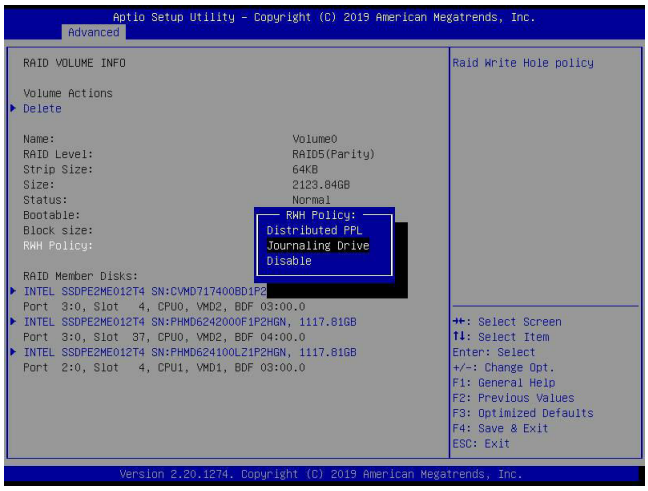
If no device has been set as a journaling drive, the options are Distributed PPL and **Disable**.



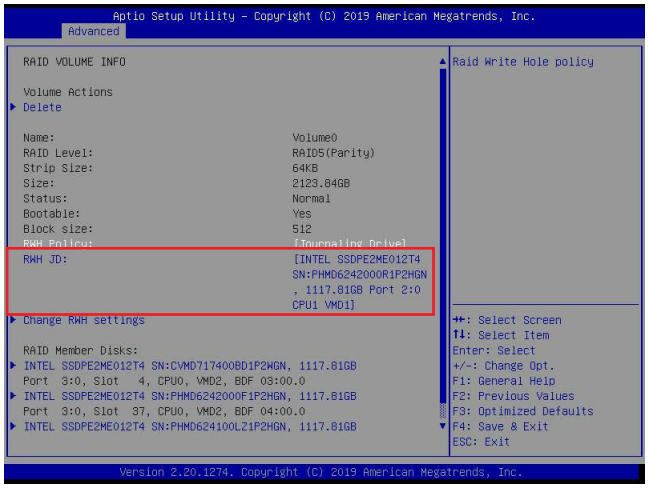
Note 1: Partial parity logging (PPL) can be defined as the result of XOR calculation of old data and old parity. PPL is a feature available for RAID5 volumes. While a power/drive-failure/crash occurring, PPL information helps rebuild the RAID volume and reduce the potential data loss.

Note 2: For the RWH condition, the Intel RSTe 5.X or above RWH closure algorithm provides the option of use of an additional NVMe device for RAID volume rebuilds (Journaling Drive RWH closure mode). Without the use of an additional NVMe device, PPL distributed RWH closure mode can be utilized to close the RWH by using the parity drive for example.

Step 3. Set the feature, RWH Policy, to **Journaling Drive**.

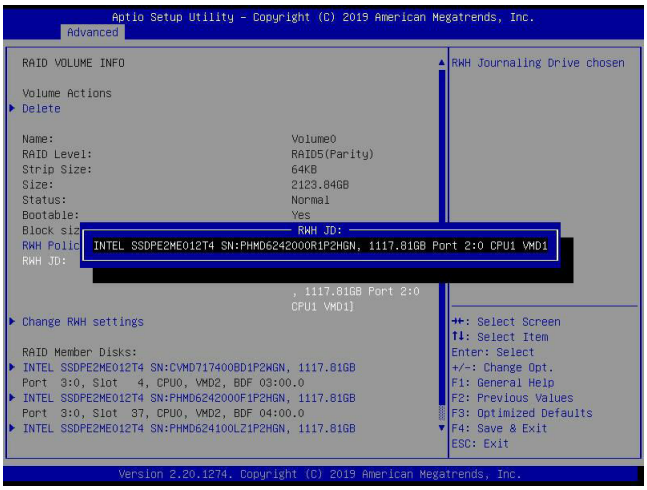


Press <Enter> and the RWH JD feature will become available as shown below.



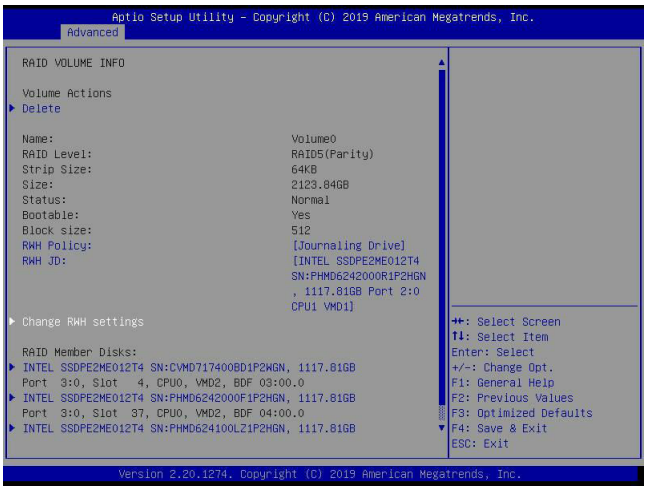
RWH JD

Use the arrow keys to select RWH JD. Press <Enter> and the following screen will appear. The feature displays the information of journaling drive(s).

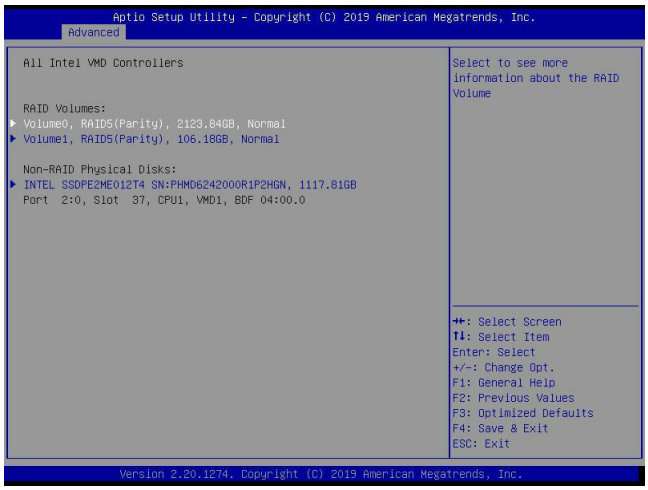


Step 4. Use the arrow keys and press <Enter> to select the desired journaling drive from the option list of RWH JD.

Step 5. For the changes to take effect, use the arrow keys to select Change RWH settings and press <Enter>.



Your computer will return to the main screen of All Intel VMD Controllers as shown below.



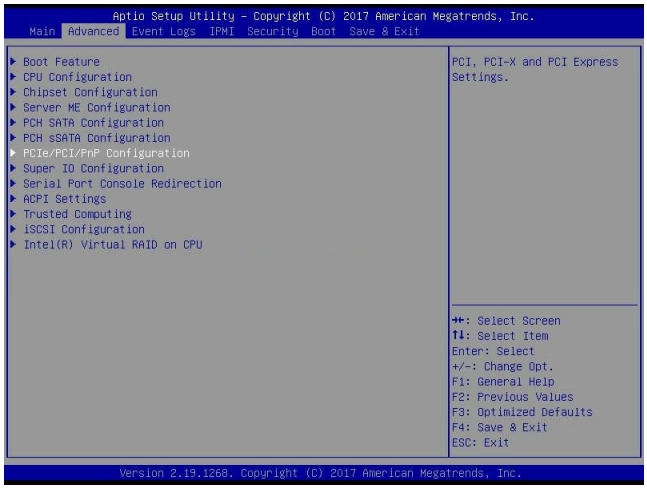
Appendix E

Configuring iSCSI Settings

Internet small computer system interface (iSCSI) is a protocol that defines how block-level data transports between the iSCSI initiator and iSCSI target over an Internet protocol (IP) network. The iSCSI initiator (client/host) enables a connection to the iSCSI target and initiates I/O requests. The iSCSI target can be a group of storage devices or an intermediate device attached to storage devices. The iSCSI initiator and iSCSI target must connect to an IP network. To have iSCSI settings available, refer to instructions stated in the E.1 section. The E.2 section explains iSCSI settings.

E.1 PCIe/PCI/PnP Features

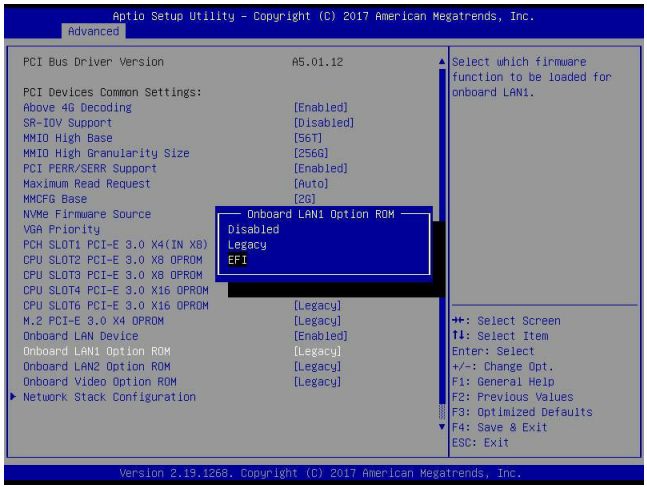
Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Advanced tab. Use the arrow keys to select PCIe/PCI/PnP Configuration and press <Enter> to access the menu items.



Note: Be sure to have configuration information for the iSCSI initiator and iSCSI target before starting iSCSI settings.

Onboard LAN1 Option ROM

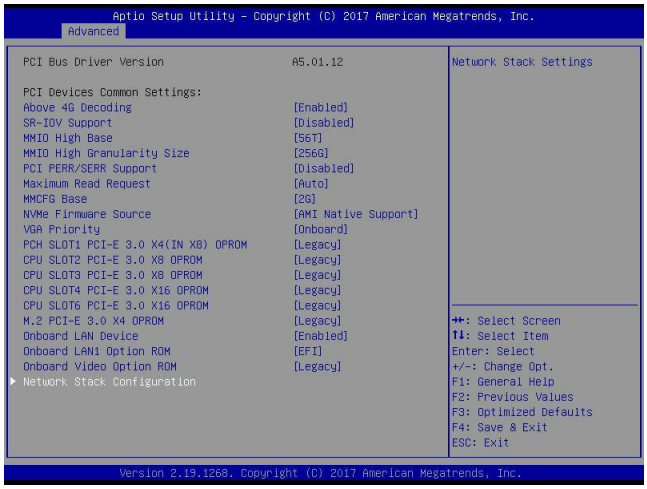
Use the arrow keys to select Onboard LAN1 Option ROM and press <Enter>. The options are Disabled, **Legacy**, and EFI. Set this feature to EFI.



Note: If Onboard LAN1 Option ROM is set to EFI, all features for onboard LAN option ROM will be set to EFI by the EFI driver. Additionally, these features will become unavailable except Onboard LAN1 Option ROM.

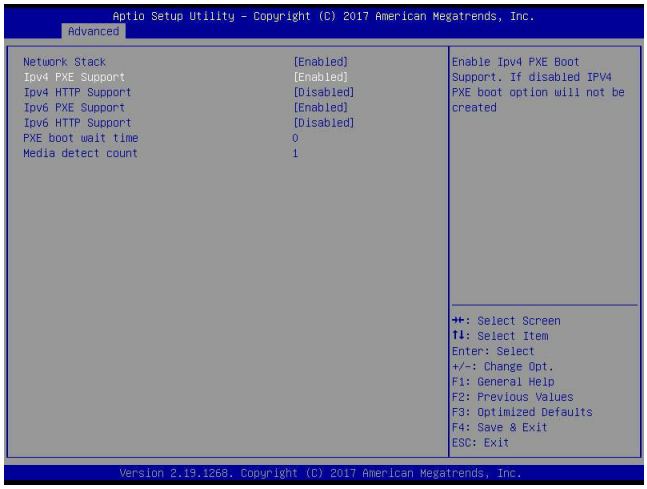
Network Stack Configuration

Use the arrow keys to select Network Stack Configuration and press <Enter> to access the menu items.



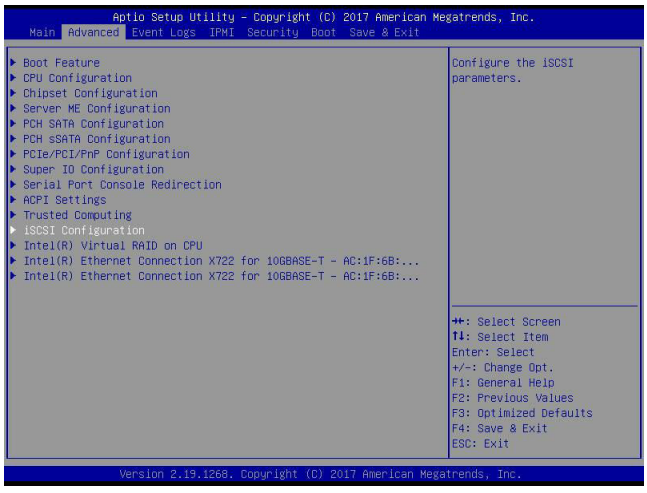
Ipv4 PXE Support/Ipv6 PXE Support

To enable Ipv4/Ipv6 PXE boot support, use the arrow keys to select and set Ipv4 PXE Support/ Ipv6 PXE Support to Enabled.



Note: Enable both Ipv4 PXE Support and Ipv6 PXE Support to have iSCSI settings available. In some cases, enabling either one feature may also have iSCSI settings available depending on the configuration of iSCSI initiator and iSCSI target.

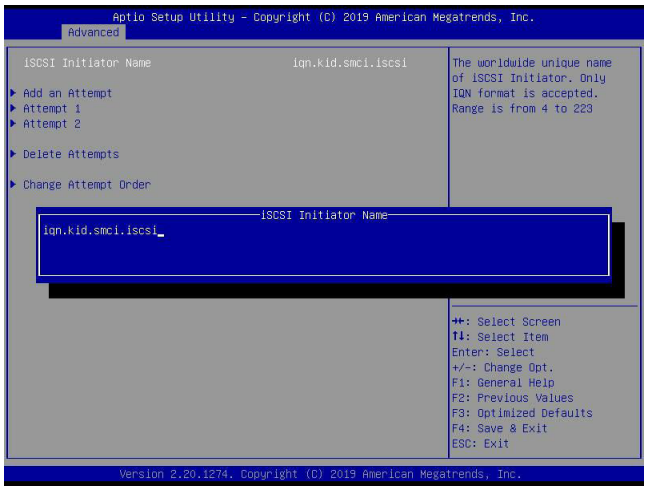
For the changes to take effect, save settings and restart the system. Press <Del> during system boot to enter the BIOS Setup utility. When the BIOS main screen appears, navigate to the Advanced tab. Use the arrow keys to select iSCSI Configuration and press <Enter> to access the menu items.



E.2 Configuring iSCSI Settings

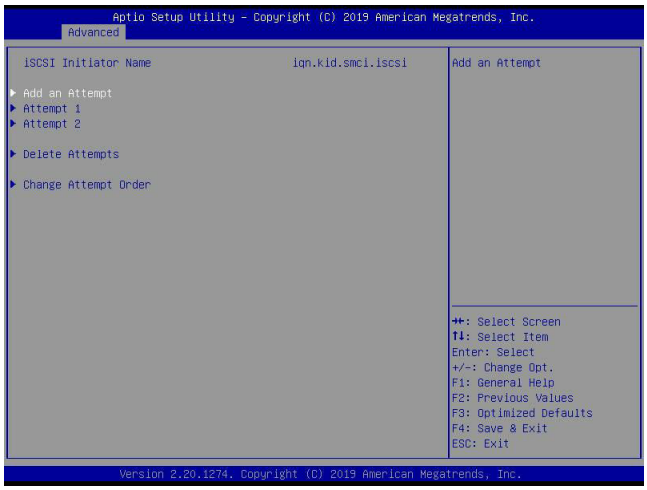
iSCSI Initiator Name

Use this feature to enter the unique initiator name in iSCSI qualified name (IQN) format.

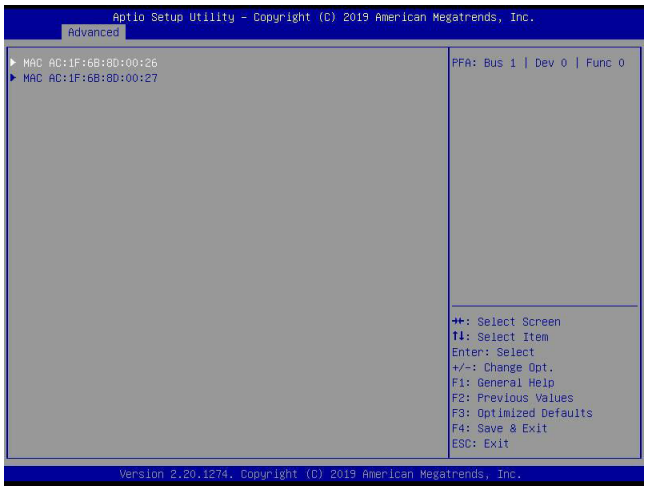


Add an Attempt

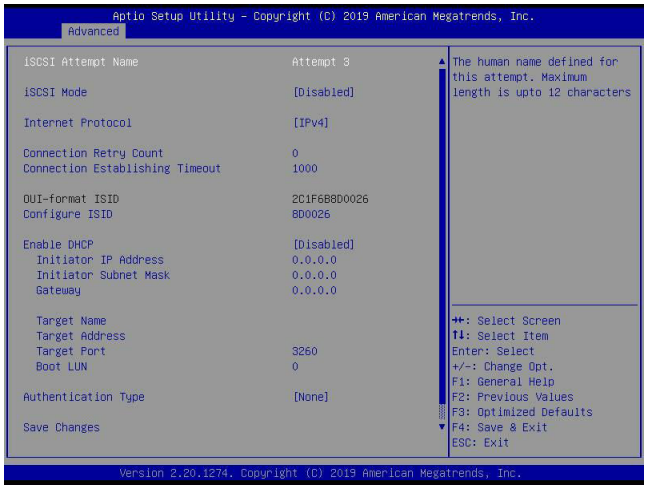
Use the arrow keys to select Add an Attempt.



Press <Enter> and the following screen will appear. Use the arrow keys to select the desired media access control address (MAC address), network interface card (NIC) port.

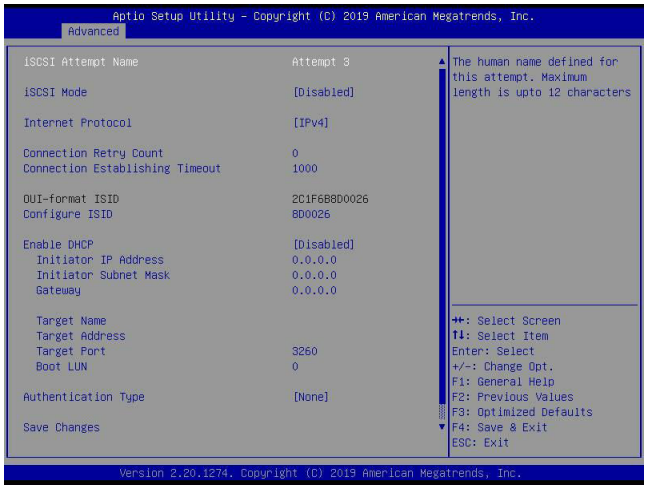


Press <Enter> and the following screen will appear.



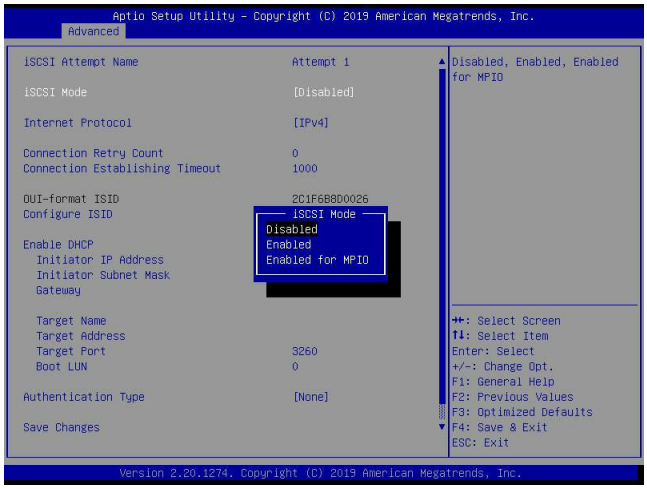
iSCSI Attempt Name

This feature displays the iSCSI attempt name.



iSCSI Mode

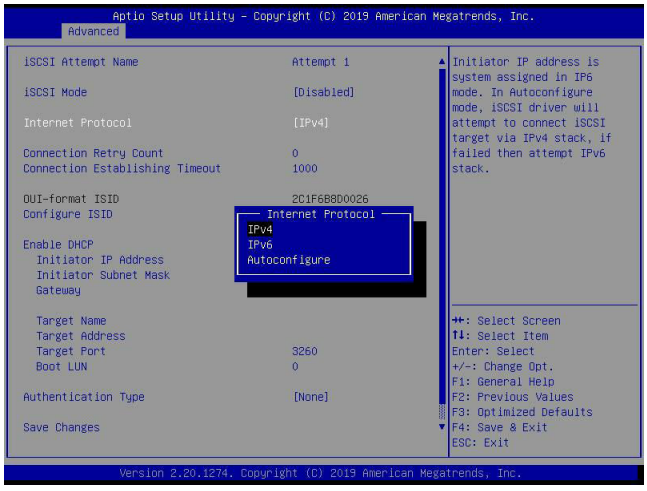
Use this feature to set the iSCSI mode. The options are **Disabled**, Enabled, and Enabled for MPIO. Multipath I/O (MPIO) is a feature that allows the system to route I/O through the available paths if the active path fails (be sure to have more than one physical path connected to the system).



Note: Enabling the feature, iSCSI Mode, is required for iSCSI configuration.

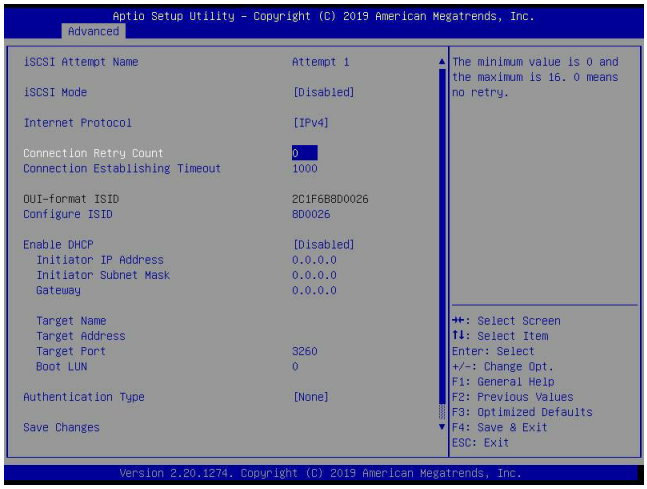
Internet Protocol

Use this feature to set the Internet protocol. The options are **IPv4**, IPv6, and Autoconfigure.



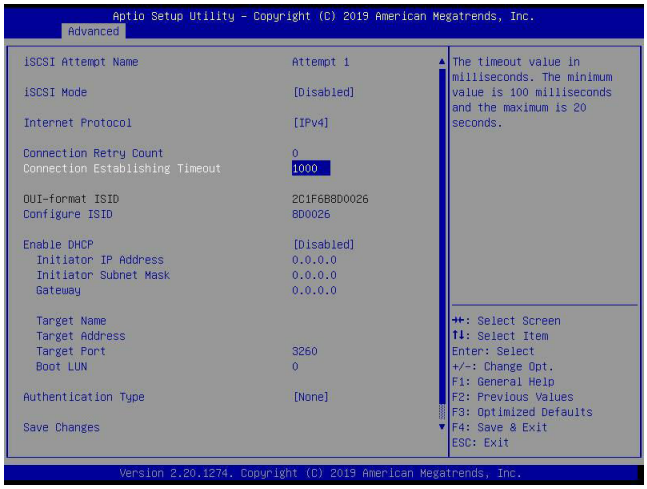
Connection Retry Count

The valid range is 0~16. Use this feature to enter the number of logon sessions allowed for the iSCSI initiator to restart with the iSCSI target if the first logon connection fails.



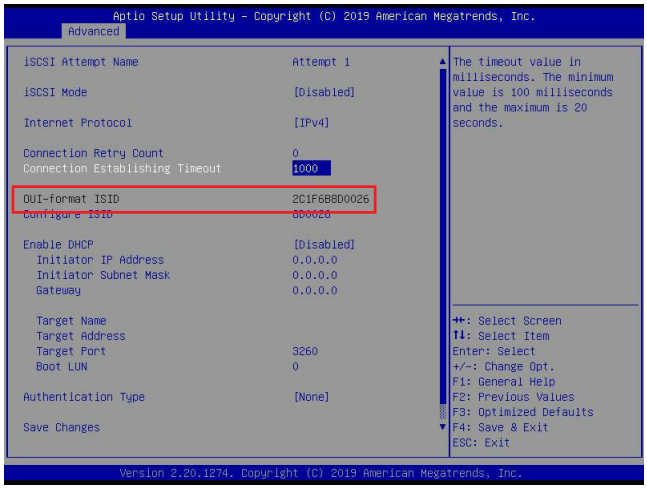
Connection Establishing Timeout

Use this feature to set the logon connection establishing timeout (in milliseconds). The valid range is from 100 milliseconds to 20 seconds.



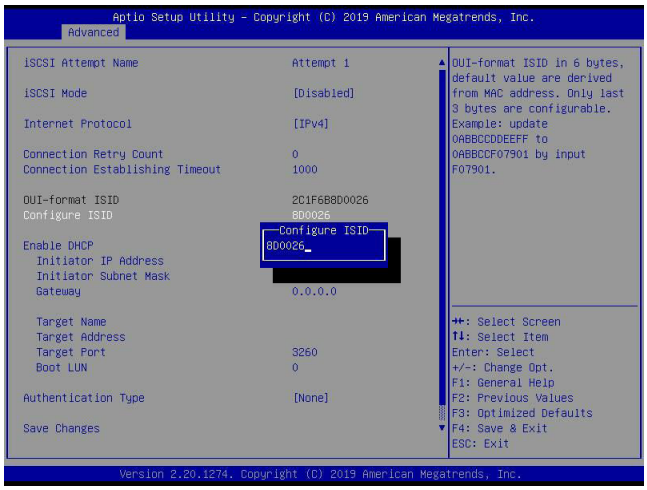
OUI-format ISID

This feature displays the default ISID in OUI format. The value (in six bytes) is derived from the MAC address of the NIC port that you selected earlier.



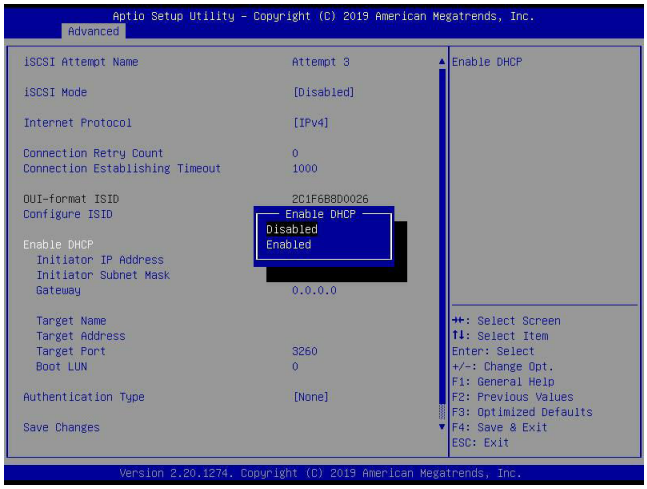
Configure ISID

Press <Enter> to configure the ISID. The default value is derived from the last three bytes of the OUI-format ISID. Also, only the last three bytes of the ISID are configurable.



Enable DHCP

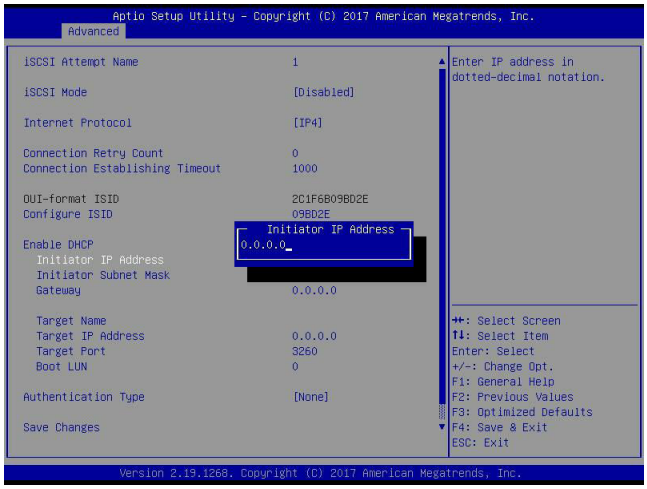
Use this feature to disable/enable dynamic host configuration protocol (DHCP) server service for the iSCSI initiator. The options are **Disabled** and Enabled.



Note: Set the feature, Enable DHCP, to Disabled if you would like to specify the iSCSI initiator IP address/subnet mask/gateway.

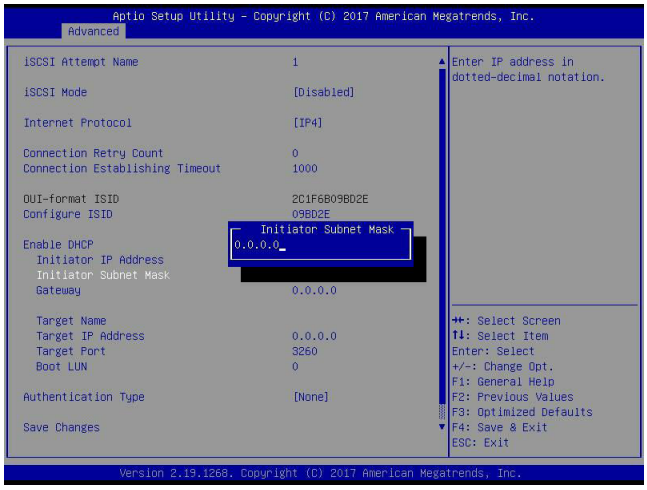
Initiator IP Address (available when Enable DHCP is set to Disabled)

Use this feature to enter the desired iSCSI initiator IP address.



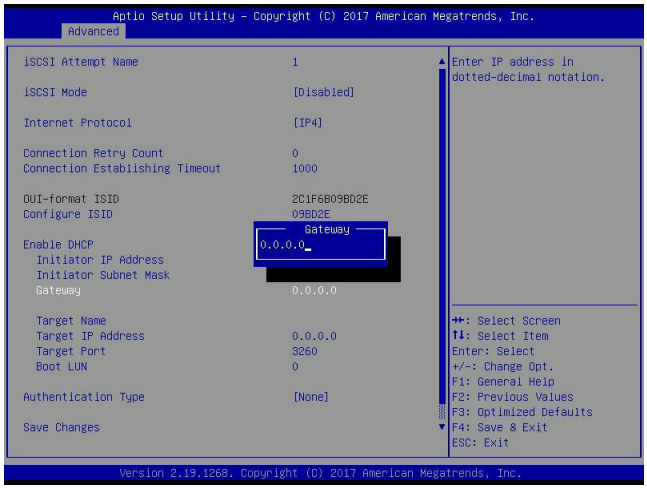
Initiator Subnet Mask (available when Enable DHCP is set to Disabled)

Use this feature to enter the desired iSCSI initiator subnet mask.



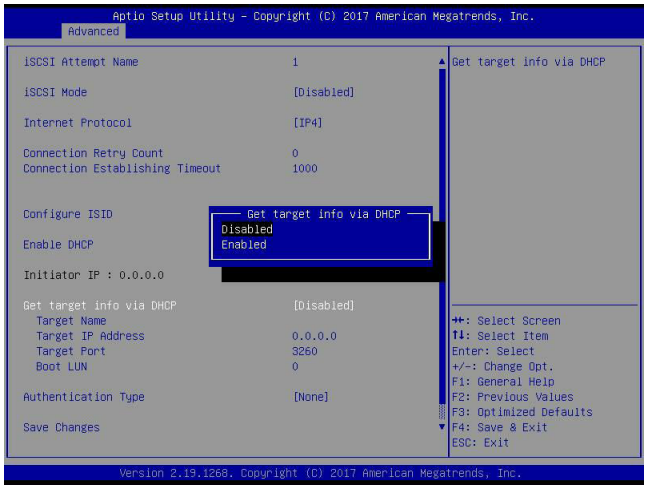
Gateway (available when Enable DHCP is set to Disabled)

Use this feature to enter the desired iSCSI initiator gateway.



Get target info via DHCP (available when Enable DHCP is set to Enabled)

Use this feature to disable/enable dynamic host configuration protocol (DHCP) server service for the iSCSI target. The options are **Disabled** and Enabled.

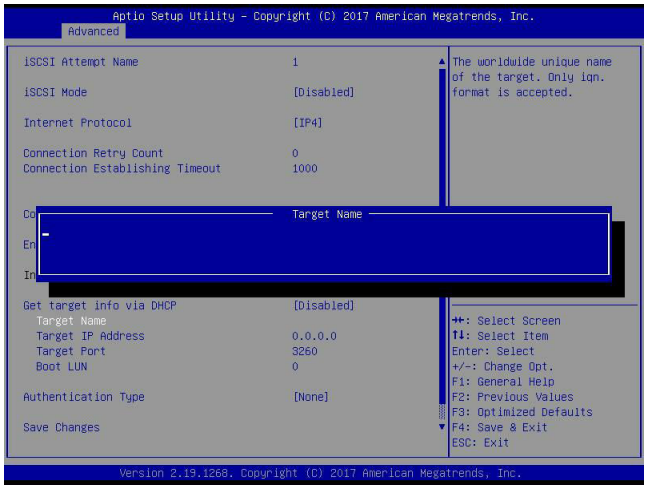


Note 1: Set the feature, Get target info via DHCP, to Disabled if you would like to specify the iSCSI target name/IP address/boot LUN.

Note 2: LUN stands for logical unit number, which is used to identify a logical/physical disk.

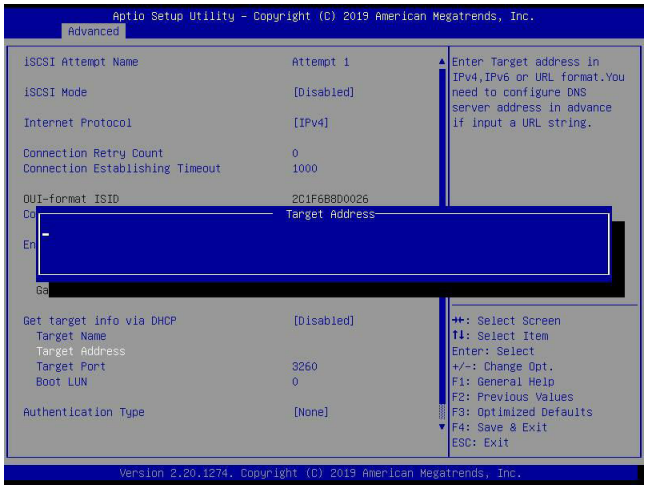
Target Name

Use this feature to enter the desired iSCSI target name in IQN format.



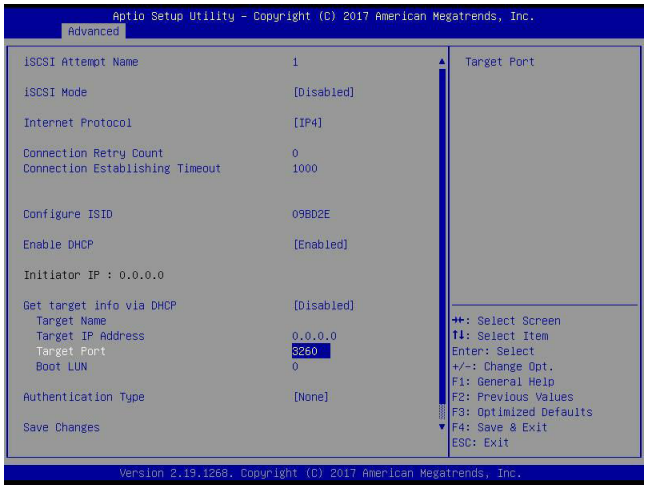
Target Address

Use this feature to enter the desired iSCSI target IP address.



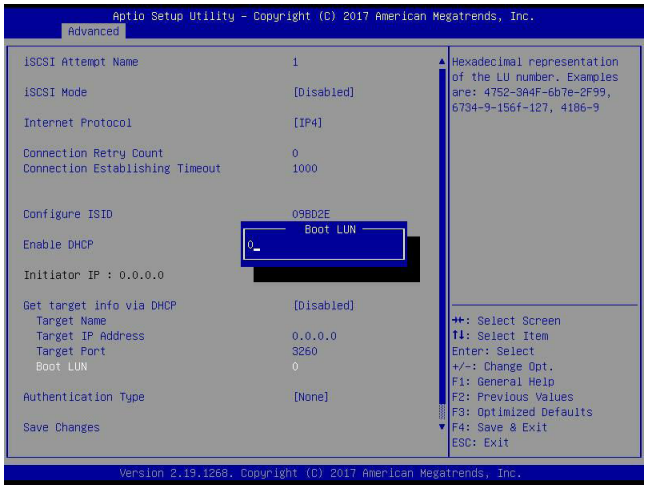
Target Port

This feature displays the iSCSI target port.



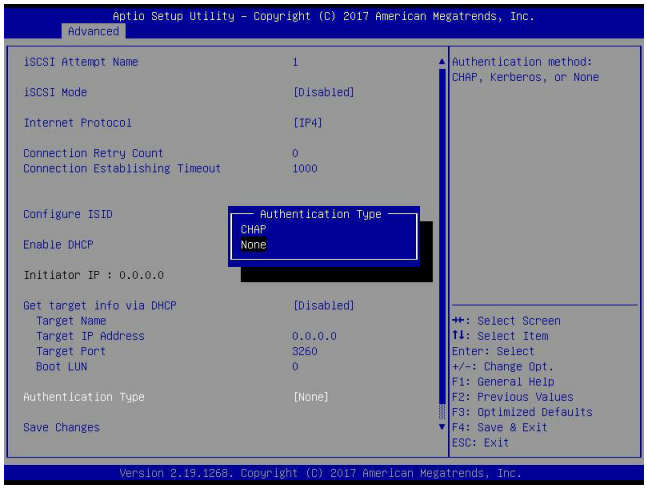
Boot LUN

Use this feature to enter the LUN ID of boot LUN.



Authentication Type

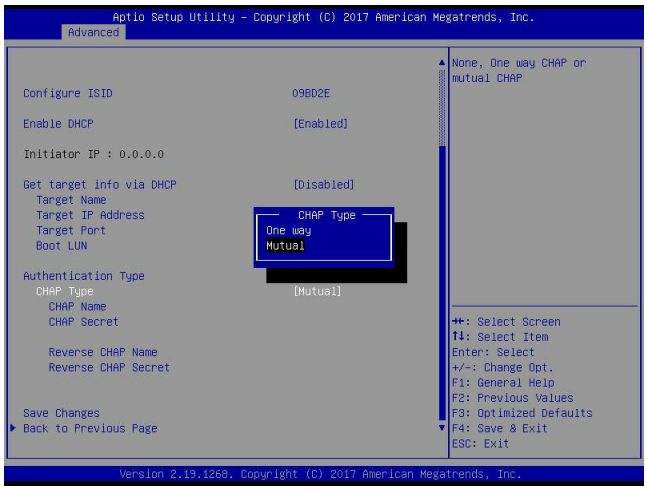
Use this feature to set the authentication method. The options are CHAP and **None**.



Note: Challenge handshake authentication protocol (CHAP) is a protocol used to verify the identity of the peer of a connection.

CHAP Type (available when Authentication Type is set to CHAP)

Use this feature to set the CHAP type. The options are One way and **Mutual**.

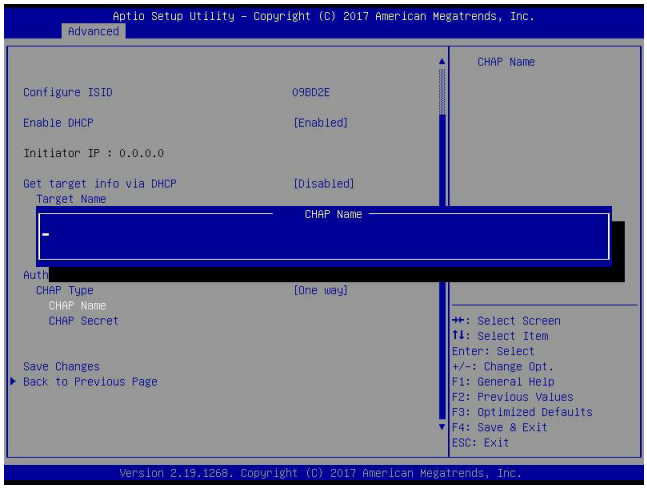


Note 1: If one way (unidirectional) CHAP authentication is performed, the iSCSI target authenticates the iSCSI initiator.

Note 2: If mutual (bidirectional) CHAP authentication is performed, the iSCSI target and iSCSI initiator authenticate each other.

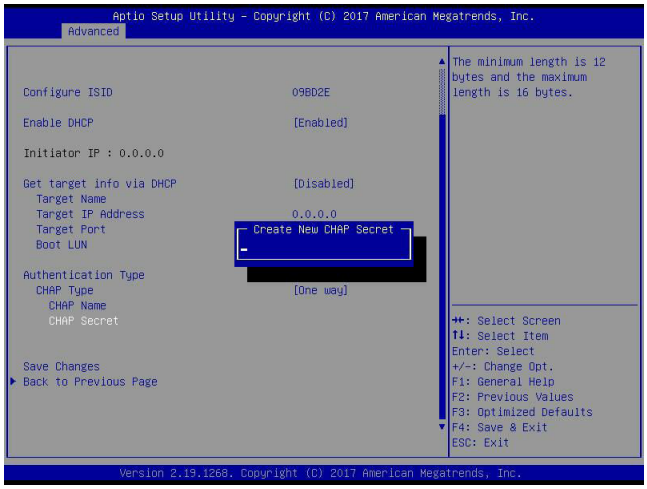
CHAP Name (available when Authentication Type is set to CHAP)

Use this feature to enter the CHAP name authenticated by the iSCSI target.



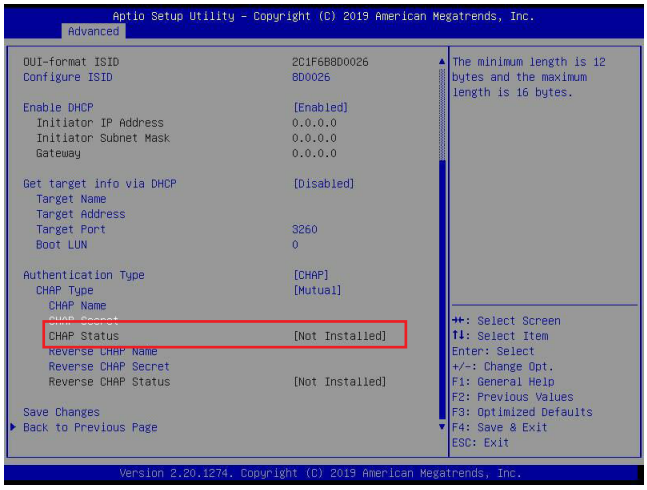
CHAP Secret (available when Authentication Type is set to CHAP)

Use this feature to enter the CHAP secret (12~16 characters) authenticated by the iSCSI target.



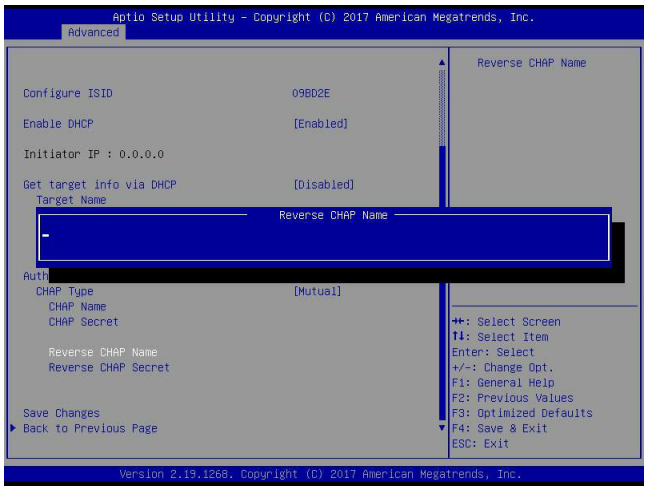
CHAP Status

This feature displays the CHAP status.



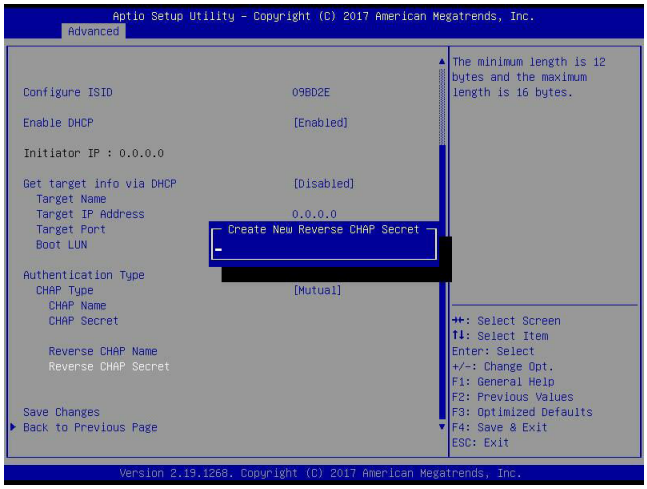
Reverse CHAP Name (available when CHAP Type is set to Mutual)

Use this feature to enter the CHAP name authenticated by the iSCSI initiator.



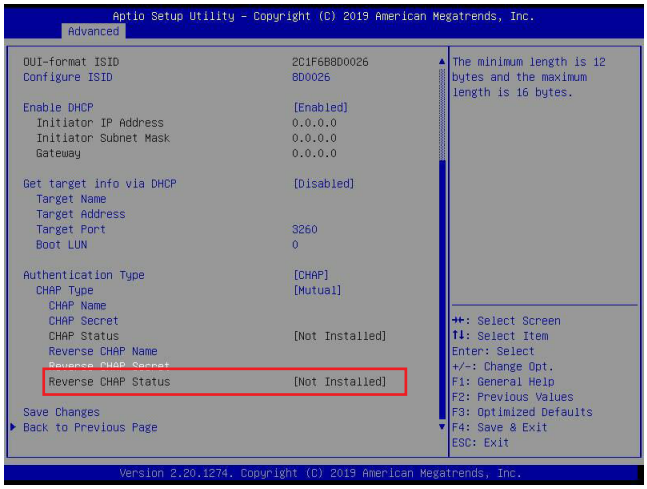
Reverse CHAP Secret (available when CHAP Type is set to Mutual)

Use this feature to enter the CHAP secret (12~16 characters) authenticated by the iSCSI initiator.



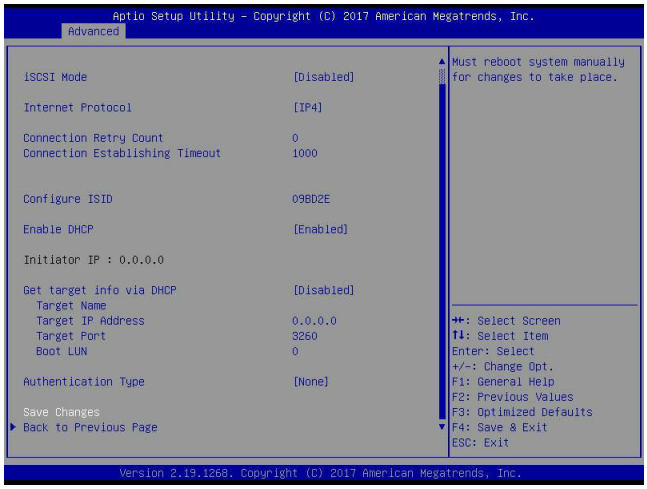
Reverse CHAP Status (available when CHAP Type is set to Mutual)

This feature displays the reverse CHAP status.



Save Changes

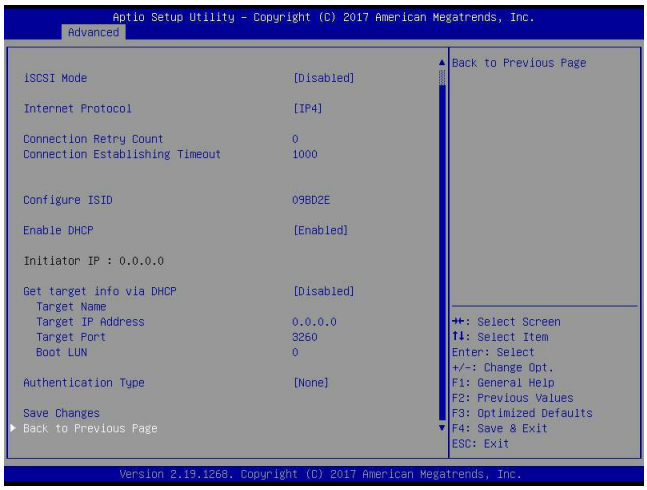
Use the arrow keys to select Save Changes and press <Enter> to save settings shown on the screen.



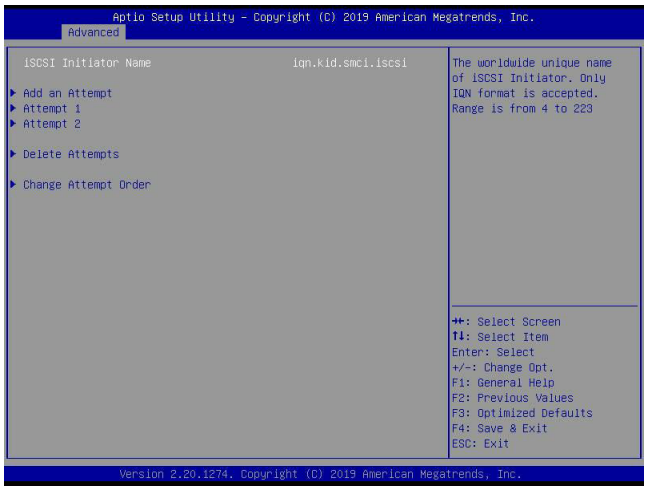
Note: For the changes to take effect, save settings and restart the system.

Back to Previous Page

Use the arrow keys to select Back to Previous Page and press <Enter>.

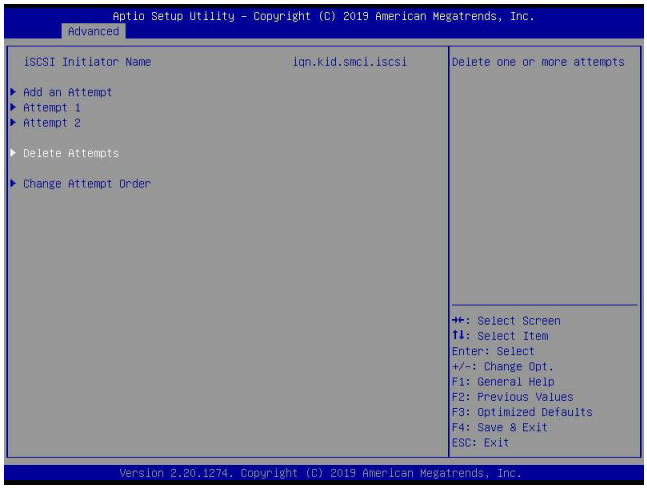


The user will be returned to the main screen of iSCSI Configuration as shown below.



Delete Attempts

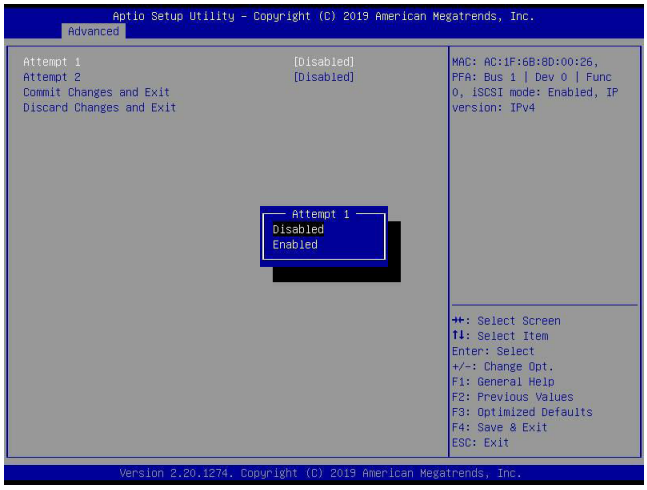
Use the arrow keys to select Delete Attempts.



Press <Enter> and the following screen will appear.

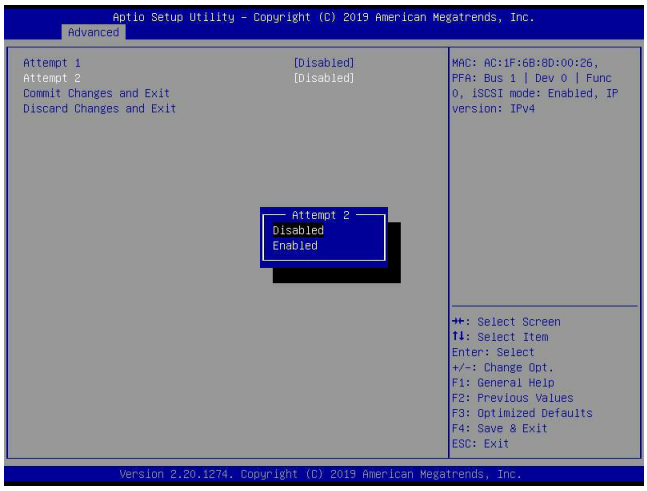
Attempt 1

Use the feature to disable/enable Attempt 1. The options are **Disabled** and Enabled.



Attempt 2

Use the feature to disable/enable Attempt 2. The options are **Disabled** and Enabled.

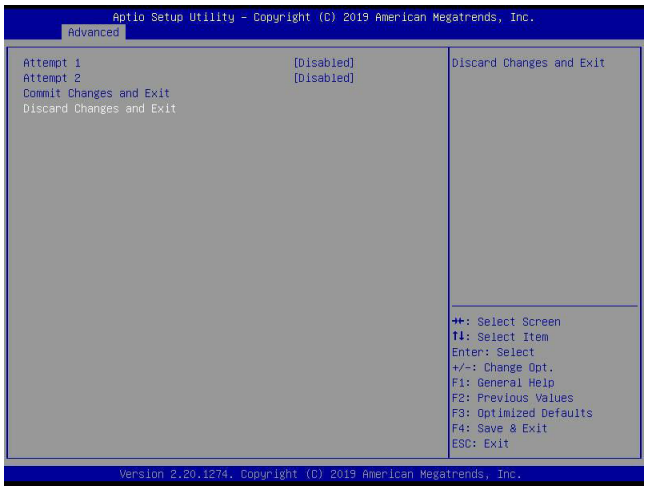


Commit Changes and Exit

Press <Enter> to save changes and return to the main screen of iSCSI Configuration.

Discard Changes and Exit

Press <Enter> to return to the main screen of iSCSI Configuration without any change.



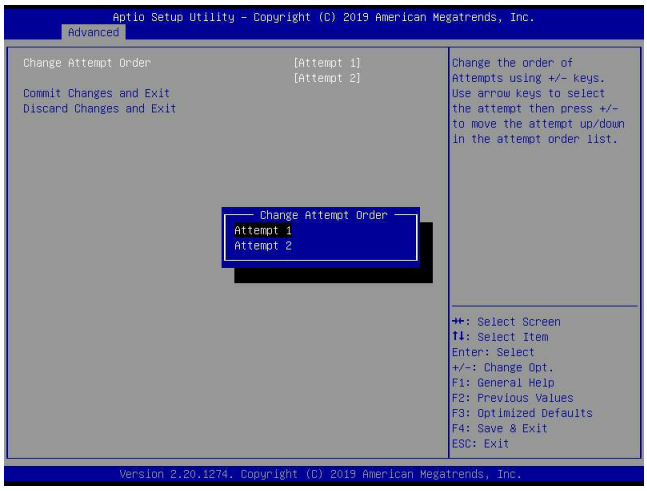
Change Attempt Order

Use the arrow keys to select Change Attempt Order.

Press <Enter> and the following screen will appear.

Change Attempt Order

This feature is to change the Attempt order. Use arrow keys to select the desired Attempt, then <+/-> keys to move up/down the selected Attempt. For instance, move up the selected Attempt by using <+> key. Move down the selected Attempt by using <-> key.



Commit Changes and Exit

Press <Enter> to save changes and return to the main screen of iSCSI Configuration.

Discard Changes and Exit

Press <Enter> to return to the main screen of iSCSI Configuration without any change.