X11DPU-S

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: April 06, 2020

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 X11DPU-S motherboard.

About This Motherboard

The X11DPU-S motherboard supports dual Intel® Xeon® Scalable-SP and 2nd Generation Intel Xeon Scalable-SP processors (Socket P) with the TDP (Thermal Design Power) of up to 205W and 2 UPIs (Ulta Path Interconnects) of up to 10.4 GT/s (Note 1 below). With the Intel C621 chipset built-in, this motherboard supports RDIMM/LRDIMM/NVDIMM DDR4 ECC 2933*/2666/2400/2133 MHz memory in 24 slots (Note 2 below) with four NVMe slots onboard. It also supports up to 6TB Intel Optane™ DC Persistent Memory in memory mode (2nd Gen Intel Xeon Scalable-SP processors only). The X11DPU-S provides maximum performance, system cooling, and PCI-E capacity, and is ideal for Ultra IO 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/.

Notes: 1. UPI/memory speeds are dependent on the processors installed in your system. **2.** Support for 2933MHz memory is dependent on the CPU SKU.

Manual organization

Chapter 1 describes the features, specifications and performance of the motherboard, and 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 provides BIOS Error Beep Codes.

Appendix B lists software program installation instructions**.**

Appendix C lists standardized warning statements in various languages**.**

Appendix D contains UEFI BIOS Recovery instructions.

Appendix E explains Intel VROC RAID settings**.**

Appendix F describes secure boot 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

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

The X11DPU-S motherboard was designed to be used with a Supermicro-proprietary chassis as an integrated server platform. It is not to be used as a stand-alone product and will not be shipped independently in a retail box. No motherboard shipping package will be provided in your shipment.

1.1 Checklist

Main Parts List		
Description	**Part Number**	**Quantity**
Supermicro Motherboard	11DPU-S	1

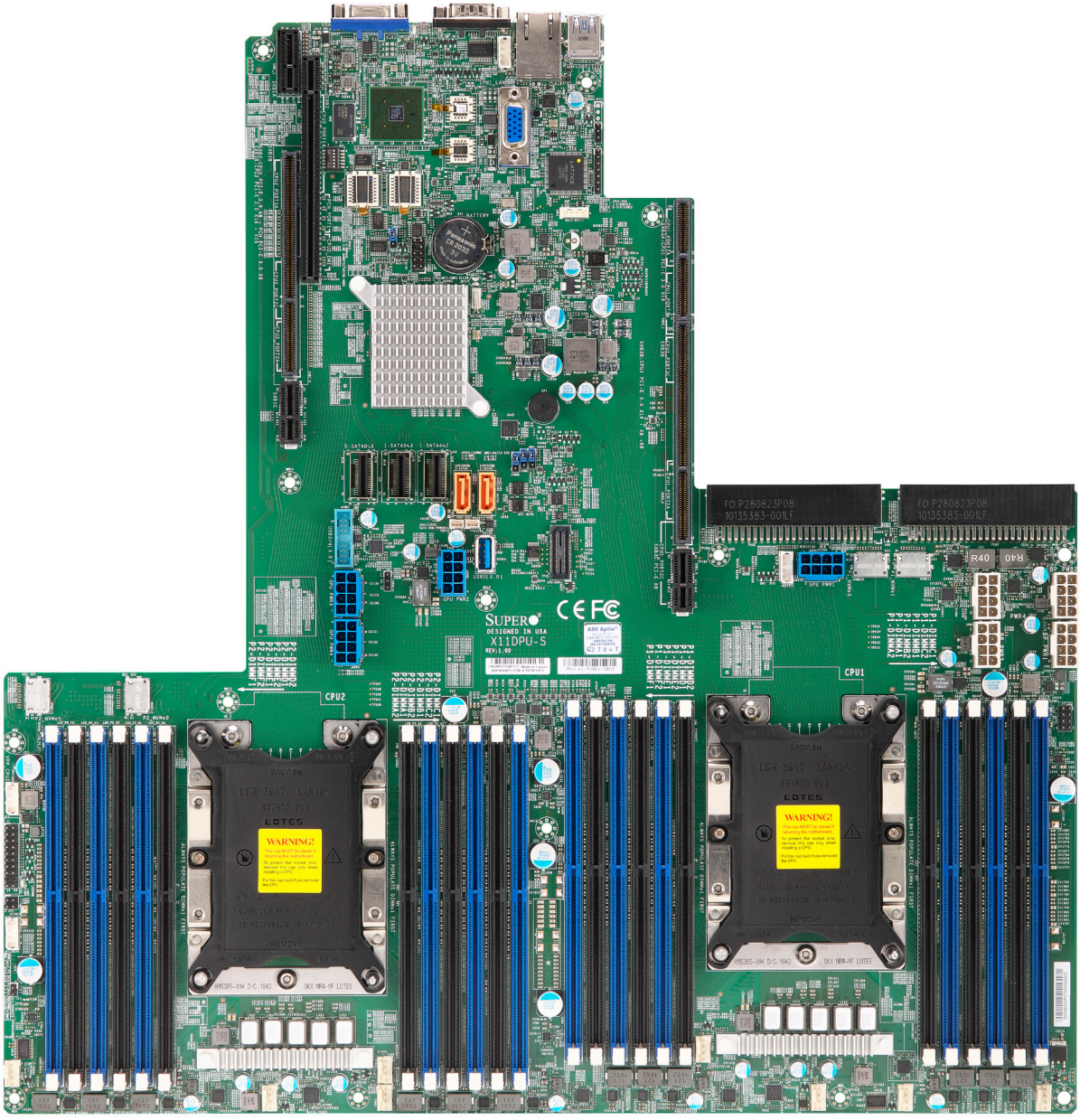
Important Links

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

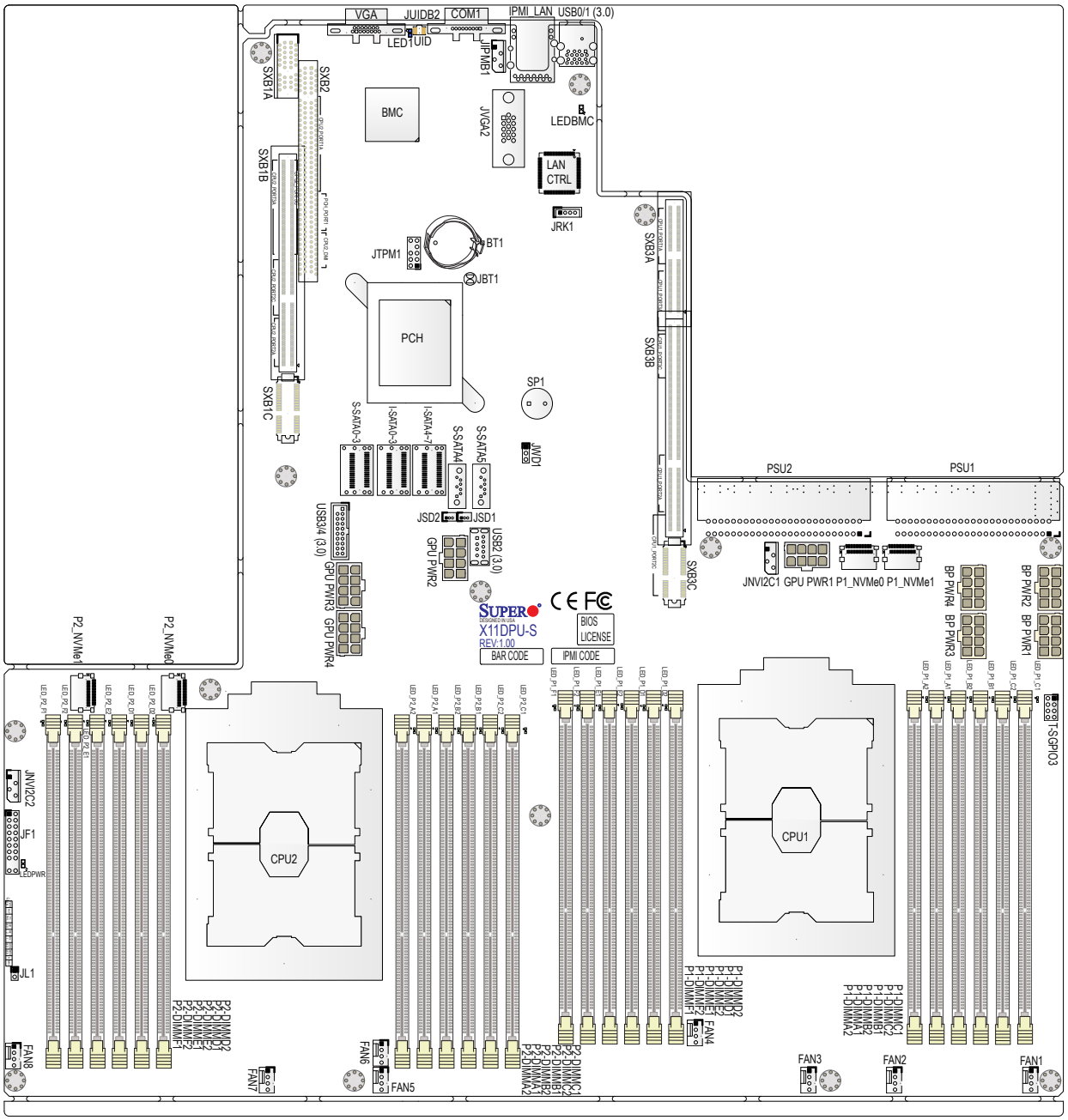
This manual may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

Figure 1-1. X11DPU-S Motherboard Image



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

Figure 1-2. X11DPU-S Motherboard Layout
(not drawn to scale)

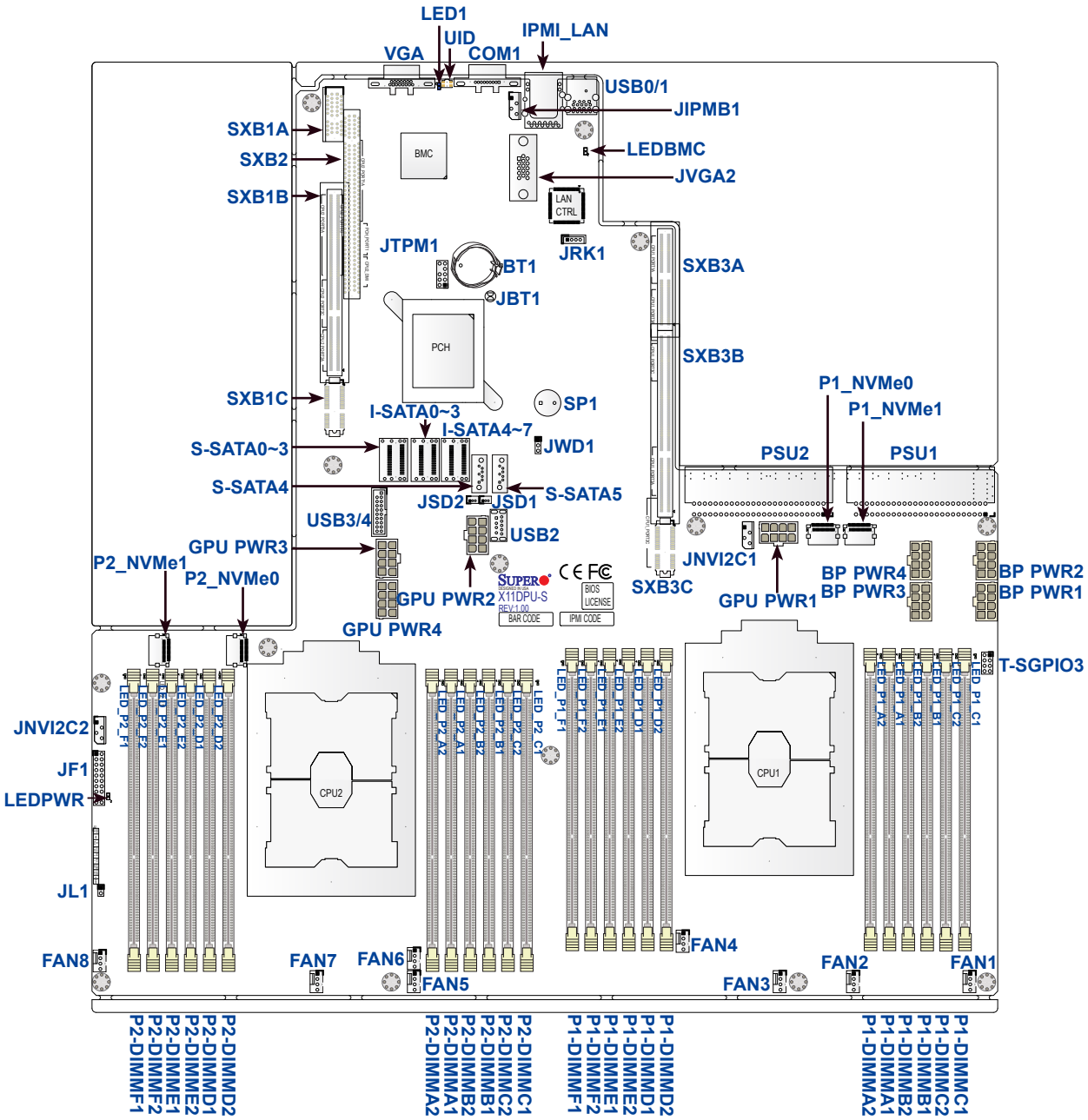


Notes:

1. Components not documented are for internal testing only.

2. Intel VMD is supported by P1_NVMe0, P1_NVMe1, P2_NVMe0, and P2_NVMe1. After you've enabled VMD in the BIOS on a PCI-E slot of your choice, this PCI-E slot will be dedicated for VMD use only, and it will no longer support any PCI-E device. To re-activate this slot for PCI-E use, please disable VMD in the BIOS.

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.
- Components/jumpers/LED indicators not documented are reserved 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.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JWD1	Watch Dog	Pins 1-2 (Reset)

Connector	Description
BP PWR 1/2/3/4	8-pin Power Connectors 1/2/3/4 for Backplane Use
BT1	Onboard Battery
COM1	COM Port (COM1) on the I/O Back Panel
FAN1 ~ FAN8	System/CPU Fan Headers
GPU PWR 1/2/3/4	8-pin Power Connectors 1/2/3/4 Used for GPU Devices
I-SATA0~3, I-SATA4~7	Intel PCH SATA 3.0 Ports (0~3, 4~7)
IPMI_LAN	Dedicated IPMI LAN Port
JF1	Front Control Panel Header
JIPMB1	4-pin BMC External I^2C Header (for an IPMI card)
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.)
JNVI2C1, JNVI2C2	NVMe SMBus (I^2C) headers used for NVMe hot-plug SMBus clock & data connections (an SMCI-proprietary NVMe add-on card and cable are required; available for a Supermicro complete system only)
(VROC) JRK1	Intel VROC RAID Key Header for NVMe SSD
JSD1, JSD2	SATA DOM Power Connectors 1/2
JTPM1	Trusted Platform Module/Port 80 Connector
JUIDB2	UID (Unit Identifier) Switch
P1_NVMe 0/1, P2_NVMe 0/1	Non-Volatile Memory Express (NVMe) 3.0 Devices Ports. Supported by CPU1 (P1_NVMe 0/1) and CPU2 (P2_NVMe 0/1) (**Note:** When installing an NVMe device on a motherboard, please be sure to connect the first NVMe port (P1_NVMe0) first for your system to work properly.)
PSU1, PSU2	Power Supply Unit (PSU) Connector 1/Power Supply Unit Connector 2
S-SATA0~3	SATA 3.0 Ports 0~3 Supported by Intel SCU Chip
S-SATA4, S-SATA5	SATA 3.0 Ports with Power-pin Built-in w/ support of SuperDOM (Device-On Module)
SP1	Internal Speaker/Buzzer
SXB1A, SXB1B, SXB1C	PCI-E 3.0 (x16 + x16) Slot Supported by CPU2 for SMCI- Proprietary Riser Card (w/ left riser card support)
SXB2	PCI-E 3.0 x8 (in x16) Slot Supported by CPU2 for Center Right Riser Card Support
SXB3A, SXB3B, SXB3C	PCI-E 3.0 (x16 + x16 + x8) Slot from CPU1 for Far_right Ultra Riser (SAS3 AOM & LAN options)
T-SGPIO3	Serial_Link General Purpose I/O Header for S-SATA4/S-SATA5

Note 1: Intel VMD is supported by P1_NVMe0, P1_NVMe1, P2_NVMe0, and P2_NVMe1.

Note 2: After you've enabled VMD in the BIOS on a PCI-E slot of your choice, this PCI-E slot will be dedicated for VMD use only, and it will no longer support any PCI-E device. To re-activate this slot for PCI-E use, please disable VMD in the BIOS.

Connector	Description
USB0, USB1	Back Panel Universal Serial Bus (USB) 3.0 Ports 0/1
USB2	USB 3.0 Type A Header
USB 3/4	Front Accessible USB 3.0 Header for USB 3/4 Connections
VGA	VGA Port

LED	Description	Status
LED1	UID (Unit Identifier) LED	Solid Blue: Unit Identified
LEDBMC	BMC Heartbeat LED	Blinking Green: BMC Normal
LEDPWR	Onboard Power LED	Solid Green: Power On

Memory LED	Description	Status
LED_P1_A1/LED_P1_A2	Memory Fault LEDs for Memory Module P1_A1/ Memory Module P1_A2	Solid Red: Memory Error Occurs
LED_P1_B1/LED_P1_B2	Memory Fault LEDs for Memory Module P1_B1/ Memory Module P1_B2	Solid Red: Memory Error Occurs
LED_P1_C1/LED_P1_C2	Memory Fault LEDs for Memory Module P1_C1/ Memory Module P1_C2	Solid Red: Memory Error Occurs
LED_P1_D1/LED_P1_D2	Memory Fault LEDs for Memory Module P1_D1/ Memory Module P1_D2	Solid Red: Memory Error Occurs
LED_P1_E1/LED_P1_E2	Memory Fault LEDs for Memory Module P1_E1/ Memory Module P1_E2	Solid Red: Memory Error Occurs
LED_P1_F1/LED_P1_F2	Memory Fault LEDs for Memory Module P1_F1/ Memory Module P1_F2	Solid Red: Memory Error Occurs
LED_P2_A1/LED_P2_A2	Memory Fault LEDs for Memory Module P2_A1/ Memory Module P2_A2	Solid Red: Memory Error Occurs
LED_P2_B1/LED_P2_B2	Memory Fault LEDs for Memory Module P2_B1/ Memory Module P2_B2	Solid Red: Memory Error Occurs
LED_P2_C1/LED_P2_C2	Memory Fault LEDs for Memory Module P2_C1/ Memory Module P2_C2	Solid Red: Memory Error Occurs
LED_P2_D1/LED_P2_D2	Memory Fault LEDs for Memory Module P2_D1/ Memory Module P2_D2	Solid Red: Memory Error Occurs
LED_P2_E1/LED_P2_E2	Memory Fault LEDs for Memory Module P2_E1/ Memory Module P2_E2	Solid Red: Memory Error Occurs
LED_P2_F1/LED_P2_F2	Memory Fault LEDs for Memory Module P2_F1/ Memory Module P2_F2	Solid Red: Memory Error Occurs

Note: To avoid causing interference with other components, please be sure to use an add-on card that is fully compliant with the PCI-E standard on a PCI-E slot.

Motherboard Features

Motherboard Features
CPU
• 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 GT/s **Note:** For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.
Memory
• Integrated memory controller supports up to 6TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 3TB of Load Reduced DIMM (LRDIMM) with speeds of up to 2933 MHz or 2666 MHz in 24 slots **Notes: 1.** The memory capacity support will differ according to the processor SKUs. **2.** Up to 6TB DCPMM memory is supported (2nd Gen Intel Xeon Scalable-SP processors only). **3.** Support for 2933MHz memory is dependent on the CPU SKU.
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 (1) PCI Express 3.0 (x16 + x16) slot supported by CPU2 for left riser card use (SXB1A/SXB1B/SXB1C) • One (1) PCI Express 3.0 x8 in x16 slot supported by CPU2 (SXB2) for center right hand riser card use • One (1) PCI Express 3.0 (x16 + x16 + x8) slot supported by CPU1 for far_right ultra riser card (used for SAS3 AOC expansion and LAN options via ultra riser) (SXB3A/SXB3B/SXB3C)
Non Volatile Memory Express (NVMe) Slots
• Four (4) NVMe PCI-E slots (P1-NVMe0/P1-NVMe1 supported by CPU1 & P2-NVMe0/P2-NVMe1 supported by CPU2) • RAID 0/1/5/10 using Intel® VROC (option RAID key)
BaseBoard Management Controller (BMC)
• Nuvoton NPCM710S BMC supports IPMI 2.0 • One (1) IPMI_dedicated_LAN located on the I/O back panel
Graphics
• Graphics controller via Nuvoton NPCM710S BMC

Note 1: Please refer to the Memory Configuration for the X11 UP/DP/MP Motherboard User Guide posted on our website for detailed information on memory support for this motherboard.

Note 2: The table above is continued on the next page.

Motherboard Features	
I/O Devices	
• Serial (COM) Port	• One (1) Fast UART 16550 port on the I/O back panel
• SATA 3.0	• Eight (8) SATA 3.0 connections supported by Intel PCH (I-SATA0~3, I-SATA4~7) • Four (4) SATA 3.0 connections supported by Intel SCU (S-SATA0~3) • Two (2) SATA 3.0 ports with power-pin built-in, w/ support of Supermicro SuperDOM (S-SATA4/S-SATA5)
• RAID (PCH)	• RAID 0/1/5/10 (RSTe 5.0)
Peripheral Devices	
• Two (2) USB 3.0 ports on the I/O back panel (USB0/USB1) • One (1) internal USB 3.0 header with two (2) USB connections on the motherboard for front access (USB 3/4) • One (1) Type A USB 3.0 connector (USB2)	
BIOS	
• 64 MB SPI AMI BIOS® SM Flash UEFI BIOS • ACPI 3.0/4.0, USB keyboard, Plug-and-Play (PnP), SPI dual/quad speed support, riser-card auto detection support, and SMBIOS 2.7 or later	
Power Management	
• Main switch override mechanism • Power-on mode for AC power recovery • Intel Intelligent Power Node Manager 4.0 (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 +3.3V, 3.3V standby, +5V, +5V standby, +12V, CPU core, memory, chipset, BMC, and PCH voltages • 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 next page.)	
Fan Control	
• Fan status monitoring via IPMI • Single cooling zone • Multi-speed fan control via onboard BMC • Pulse Width Modulation (PWM) fan control	
System Management	
• Trusted Platform Module (TPM) support • PECI (Platform Environment Control Interface) 2.0 support • UID (Unit Identification)/Remote UID • System resource alert via SuperDoctor® 5 • SuperDoctor 5, Watch Dog, NMI • 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.)	

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

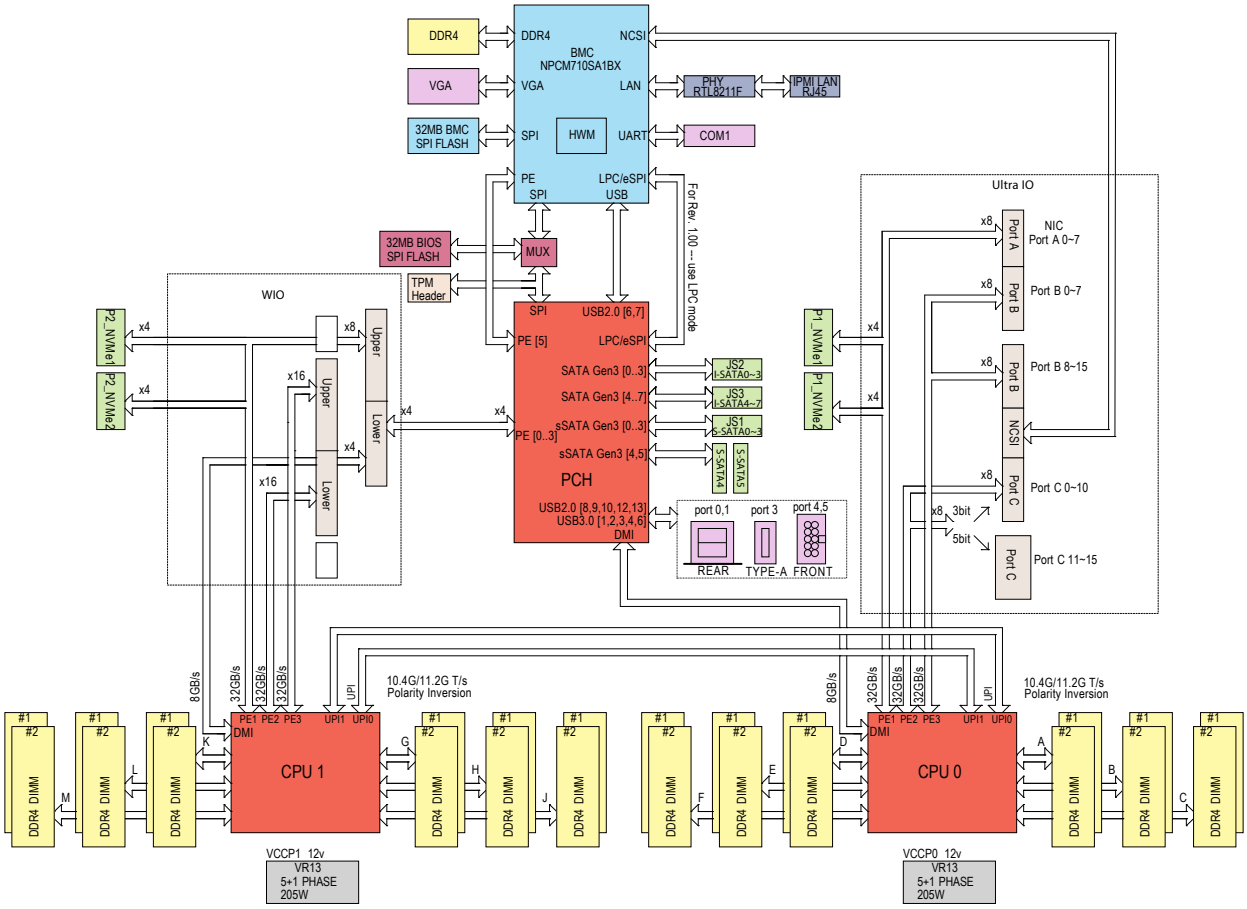
Motherboard Features
LED Indicators
• CPU/Overheating • Fan Failure • UID/remote UID • HDD activity, LAN activity.
Dimensions
• 17.00" (L) x 16.80" (W) (431.80 mm x 426.72 mm)

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 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 Intel Xeon Scalable-SP series and 2nd Gen Intel Xeon Scalable-SP series processors (Socket P) with the Intel C621 chipset, the X11DPU-S motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users. This motherboard is ideal for general purpose, cloud computing, and is optimized for server platforms used in data centers.

The Intel C621 chipset provides Enterprise SMbus support and includes the following features:

- DDR4 288-pin memory support on Socket P
- Support for MCTP Protocol
- Support for Management Engine (ME)
- Support of SMBus speeds of up to 400KHz for BMC connectivity
- Improved I/O capabilities to high-storage-capacity configurations
- SPI enhancements
- Intel Node Manager 4.0 for advanced power monitoring, capping, and management for BMC enhancement
- The BMC supports remote management, virtualization, and the hardware security with silicon root of trust (sROT) for enterprise platforms

Note: Node Manager 4.0 support is dependent on the power supply used in the system.

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 PCI-E lanes (48 lanes)
- Integrated Intel Ethernet Connection X722 with iWARP RDMA

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

Intel 2nd Generation 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 2933 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 X11DPU-S motherboard. The motherboard has an onboard Nuvoton NPCM710S 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 X11DPU-S motherboard. The motherboard has an onboard Baseboard Management Controller (BMC) 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 the manufacturer-defined threshold, system/CPU cooling fans will increase fan spin to provide better air flow to prevent the CPU or the system from overheating.

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

System Resource Alert

This feature is available when used with SuperDoctor 5. 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 Generation Intel Xeon Scalable-SP processors support new DCPMM (Optane™ DC Persistent Memory Modules) technology that offers data persistence with higher capacity than 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

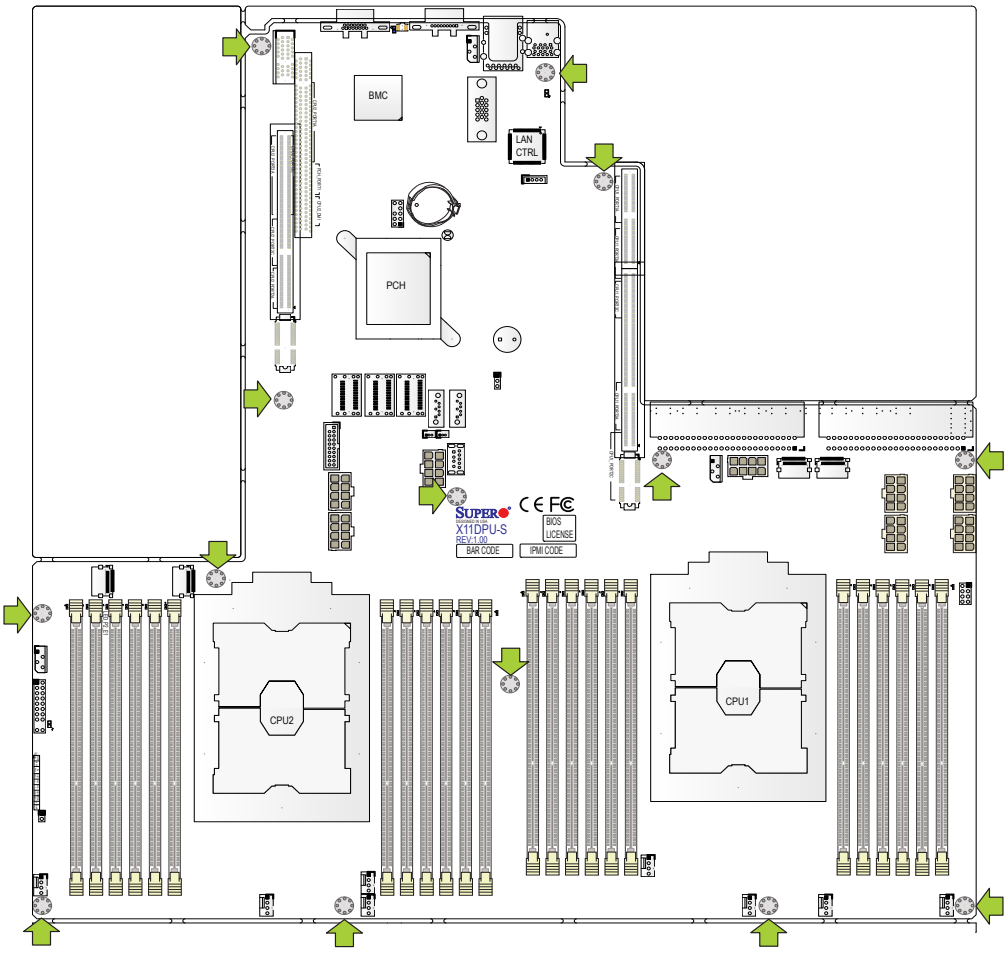
All motherboards have standard mounting holes to fit different types of chassis. Make sure that the locations of all the mounting holes for both the motherboard and the chassis match. Although a chassis may have both plastic and metal mounting fasteners, metal ones are highly recommended because they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

Tools Needed

Philips Screwdriver (1)

Philips Screws (14)

Standoffs (14) Only if Needed



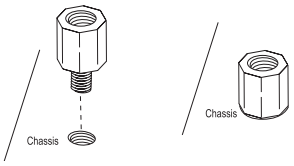
Location of Mounting Holes

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.

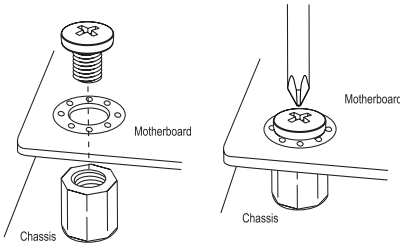
Installing the Motherboard

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

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



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



4. Install standoffs in the chassis as needed.

5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.

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

7. Repeat Step 5 to insert Pan head #6 screws into all mounting holes.

8. 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.

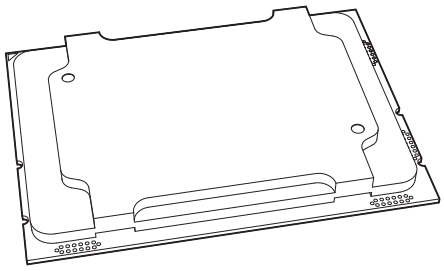
2.3 Processor and Heatsink Installation

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



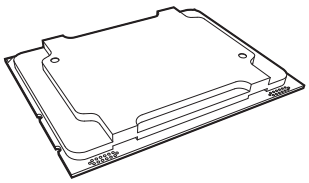
Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processor

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.

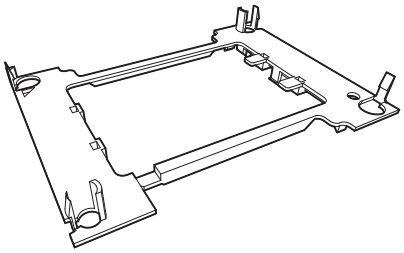
Overview of the Processor Socket Assembly

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

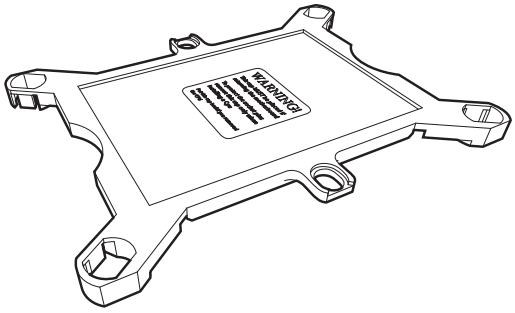
1. Intel Processor



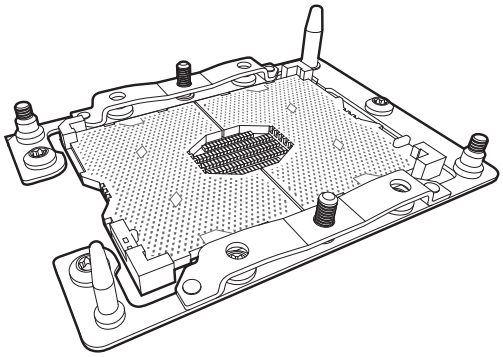
2. Narrow processor clip (the plastic processor package carrier used for the CPU)



3. Dust Cover



4. CPU Socket

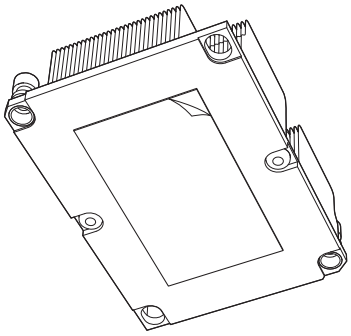


Note: Be sure to cover the CPU socket with the dust cover when the CPU is not installed.

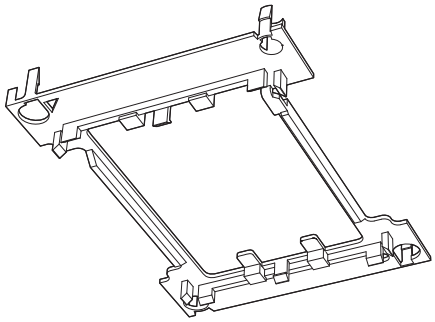
Overview of the Processor Heatsink Module (PHM)

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.

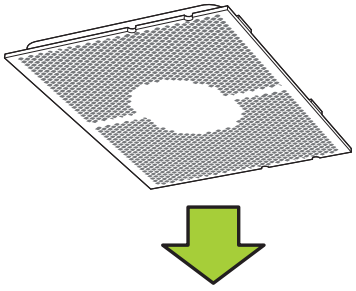
1. Heatsink



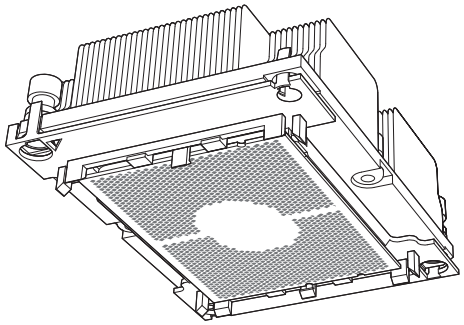
2. Narrow processor clip



3. Intel Processor



Processor Heatsink Module (PHM)



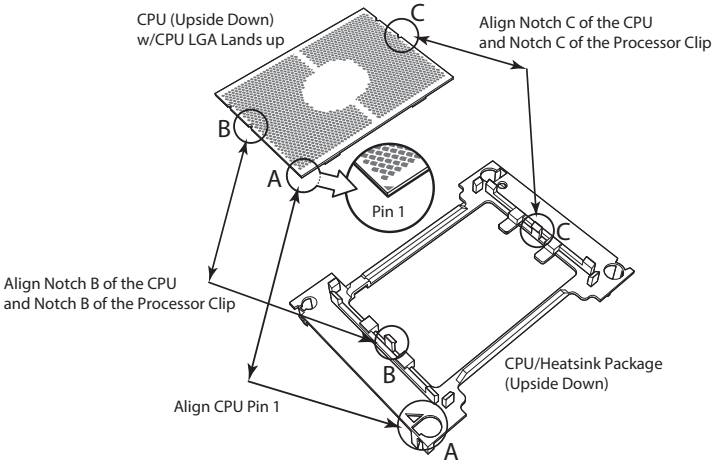
(Bottom View)

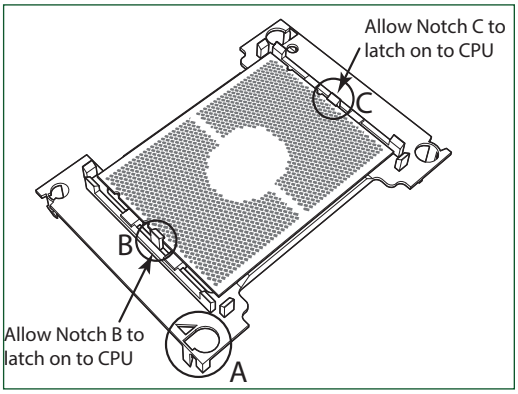
Attaching the Processor to the Narrow Processor Clip to Create the Processor Package Assembly

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).

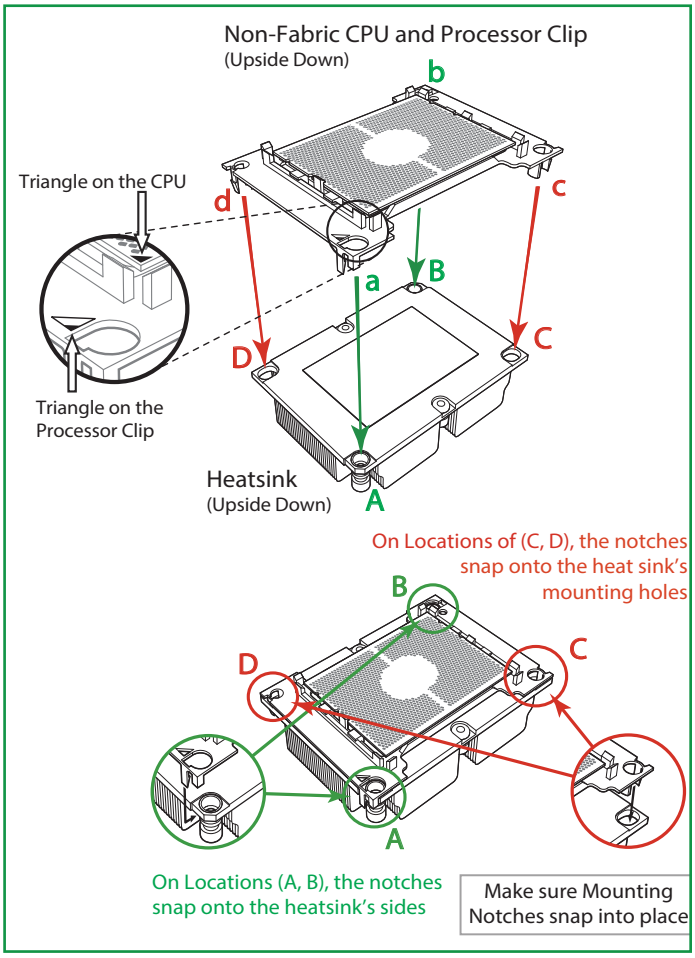
1. Locate "1" on the heatsink label and the triangular corner next to it on the heatsink. With your index finger pressing against the screw at this triangular corner, carefully hold and turn the heatsink upside down with the thermal-grease side facing up. Remove the protective thermal film if present, 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.

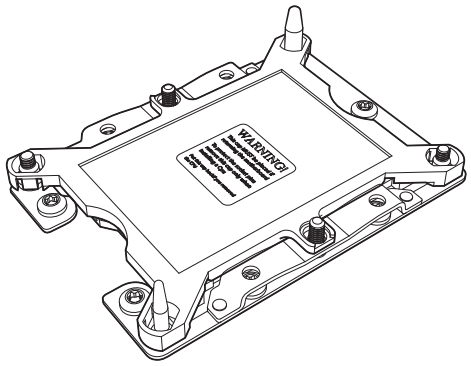
4. Also align the triangular corner ("B") at the diagonal side of the heatsink with the corresponding clips on the processor package assembly ("b").

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 socket, and 4) a back plate. These components are pre-installed on the motherboard before shipping.

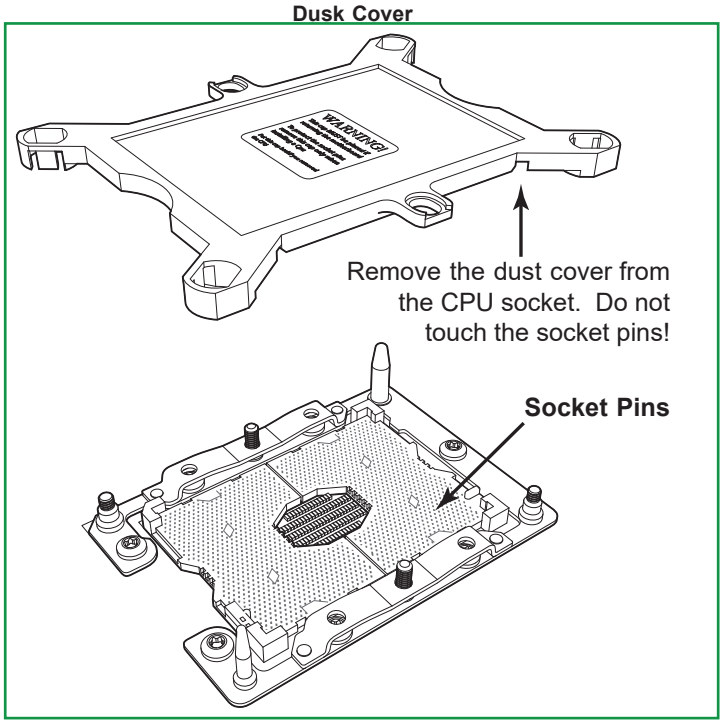


CPU Socket w/Dust Cover On

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 page 29 or page 30, 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.

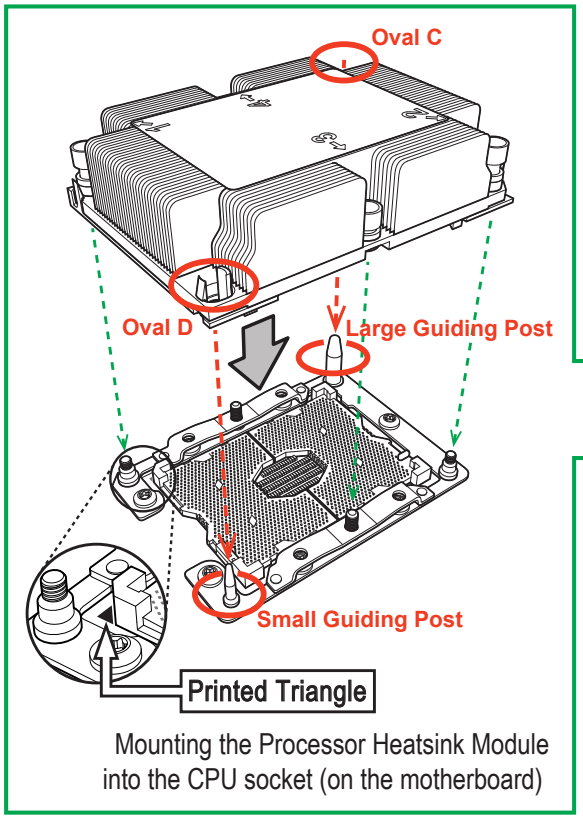
2. Locate the triangle (pin 1) on the CPU socket, and locate the triangle (pin 1) at the corner of the PHM that is closest to "1." (If you have difficulty locating pin 1 of the PHM, turn the PHM upside down. With the LGA-lands side facing up, you will note the hollow triangle located next to a screw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

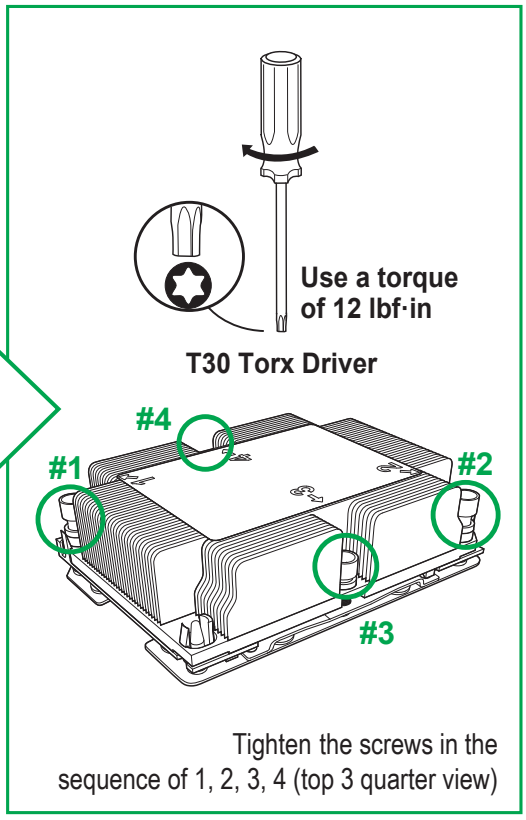
4. Once they are properly aligned, insert the two diagonal oval holes on the heatsink into the guiding posts.

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)



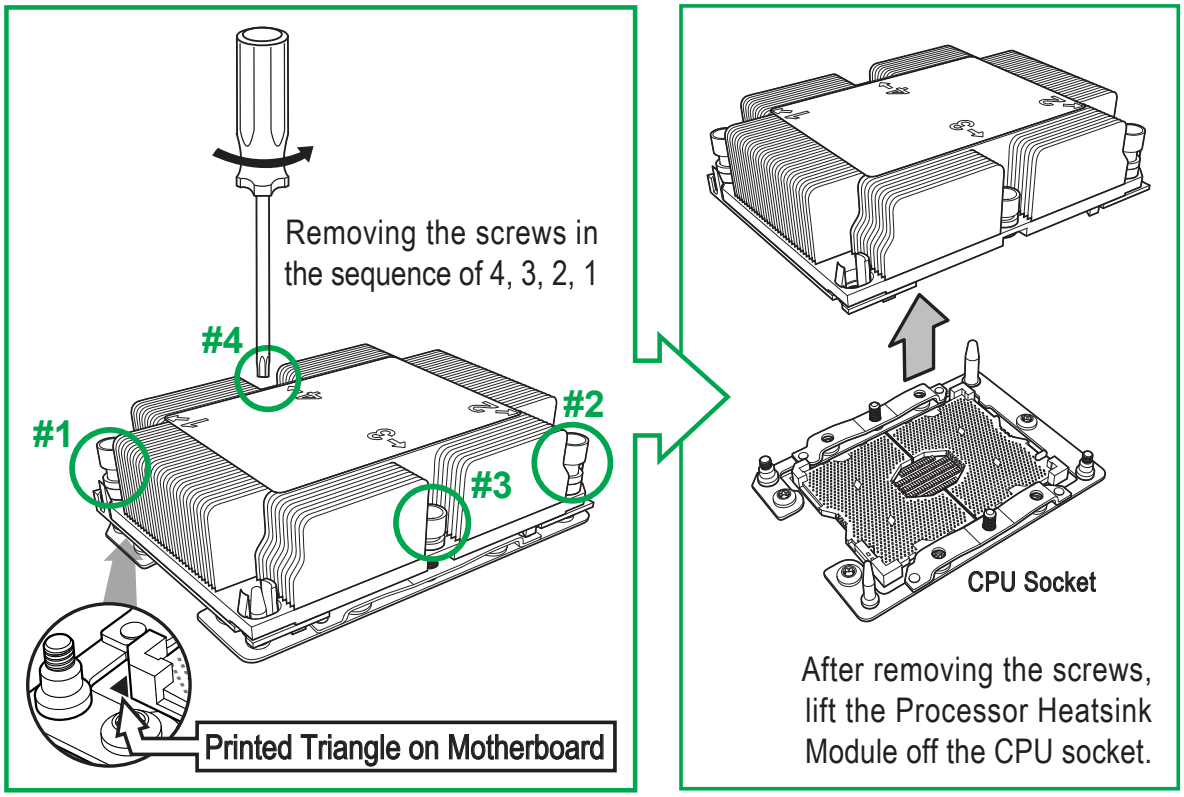
Tighten the screws in the sequence of 1, 2, 3, 4 (top 3 quarter view)

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

Memory Support

The X11DPU-S supports up to 6TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 3TB of Load Registered DIMM (LRDIMM), with speeds of 2933*/2666/2400/2133/1866/1600/1333 MHz modules in 24 memory slots (***Notes** below). Populating these DIMM modules with a pair of memory modules of the same type and size will result in interleaved memory, which will improve memory performance.

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.** 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. **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.

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.
3. Populating memory slots with a pair of DIMM modules of the same type and size will result in interleaved memory, which will improve 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/24 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-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/P1-DIMMD1/P1-DIMME1/P1-DIMMF1
1 CPU & 8 DIMMs	CPU1: P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1
1 CPU & 9 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD1/P1-DIMME1/P1-DIMMF1
1 CPU & 10 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF1
1 CPU & 11 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF1
1 CPU & 12 DIMMs	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF2/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	CPU1: P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1 CPU2: P2-DIMMC1/P2-DIMMB1/P2-DIMMA1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1
2 CPUs & 16 DIMMs	CPU1: P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1 CPU2: P2-DIMMB1/P2-DIMMB2/P2-DIMMA1/P2-DIMMA2/P2-DIMMD2/P2-DIMMD1/P2-DIMME2/P2-DIMME1
2 CPUs & 18 DIMMs	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF2/P1-DIMMF1 CPU2: P2-DIMMC1/P2-DIMMB1/P2-DIMMA1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1
2 CPUs & 20 DIMMs	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF2/P1-DIMMF1 CPU2: P2-DIMMB1/P2-DIMMB2/P2-DIMMA1/P2-DIMMA2/P2-DIMMD2/P2-DIMMD1/P2-DIMME2/P2-DIMME1
2 CPUs & 22 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF1 CPU2: P2-DIMMC1/P2-DIMMC2/P2-DIMMB1/P2-DIMMB2/P2-DIMMA1/P2-DIMMA2/ P2-DIMMD2/P2-DIMMD1/P2-DIMME2/P2-DIMME1/P2-DIMMF1
2 CPUs & 24 DIMMs	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF2/P1-DIMMF1 CPU2: P2-DIMMC1/P2-DIMMC2/P2-DIMMB1/P2-DIMMB2/P2-DIMMA1/P2-DIMMA2/ P2-DIMMD2/P2-DIMMD1/P2-DIMME2/P2-DIMME1/P2-DIMMF2/P2-DIMMF1

Note: Please refer to the Memory Configuration User 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	24GB	16GB
A1+A2+B1+B2	48GB	32GB
A1+A2+B1+B2+C1+C2	72GB	48GB
A1+A2+B1+B2+C1+C2+D1+D2	96GB	64GB
A1+A2+B1+B2+C1+C2+D1+D2+E1+E2	120GB	80GB
A1+A2+B1+B2+C1+C2+D1+D2+E1+E2+F1+F2	144GB	96GB

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	112GB	96GB
A1+A2+B1+B2	224GB	192GB
A1+A2+B1+B2+C1+C2	336GB	288GB
A1+A2+B1+B2+C1+C2+D1+D2	448GB	384GB
A1+A2+B1+B2+C1+C2+D1+D2+E1+E2	560GB	480GB
A1+A2+B1+B2+C1+C2+D1+D2+E1+E2+F1+F2	672GB	576GB

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-DIMMF2**	**P1-DIMME1**	**P1-DIMME2**	**P1-DIMMD1**	**P1-DIMMD2**	**P1-DIMMA2**	**P1-DIMMA1**	**P1-DIMMB2**	**P1-DIMMB1**	**P1-DIMMC2**	**P1-DIMMC1**	**Channel Config.**
AD	DRAM1	***DCPMM***	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	***DCPMM***	DRAM1	**2-2-2**
MM	DRAM1	***DCPMM***	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	***DCPMM***	DRAM1	**2-2-2**
AD + MM	DRAM3	***DCPMM***	DRAM3	***DCPMM***	DRAM3	***DCPMM***	***DCPMM***	DRAM3	***DCPMM***	DRAM3	***DCPMM***	DRAM3	**2-2-2**
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	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	**2-2-1**
MM	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	**2-2-1**
AD + MM	DRAM3	-	DRAM3	***DCPMM***	DRAM3	***DCPMM***	***DCPMM***	DRAM3	***DCPMM***	DRAM3	-	DRAM3	**2-2-1**
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**
AD	***DCPMM***	-	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	-	***DCPMM***	**2-2-1**

Asymmetric Population within 1 CPU Socket													
Modes	**P1-DIMMF1**	**P1-DIMMF2**	**P1-DIMME1**	**P1-DIMME2**	**P1-DIMMD1**	**P1-DIMMD2**	**P1-DIMMA2**	**P1-DIMMA1**	**P1-DIMMB2**	**P1-DIMMB1**	**P1-DIMMC2**	**P1-DIMMC1**	**Channel Config.**
AD	DRAM1	-	DRAM1	-	DRAM1	-	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1	**2/1-1-1**
AD*	DRAM1	-	DRAM1	-	DRAM1	-	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1	**2/1-1-1**

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.

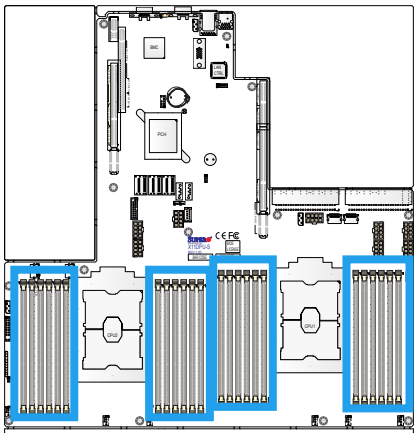
Legend (for the first two tables above)	
Capacity	
DCPMM	Any Capacity (Uniformly for all channels for a given configuration)

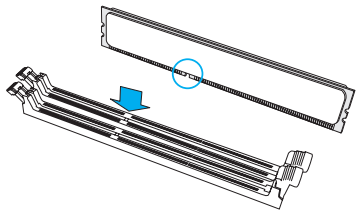
- * 2nd socket has no DCPMM DIMM
- Mode definitions: AD=App Direct Mode, MM=Memory Mode, AD+MM=Mixed Mode
- For MM, general DDR4+DCPMM ratio is between 1:4 and 1:16. Excessive capacity for DCPMM can be used for AD.
- For each individual population, rearrangements between channels are allowed as long 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

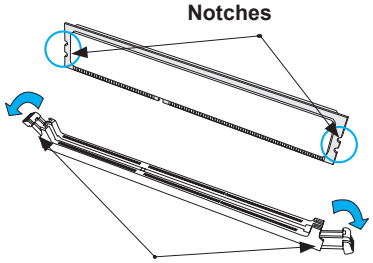
DIMM Installation

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.



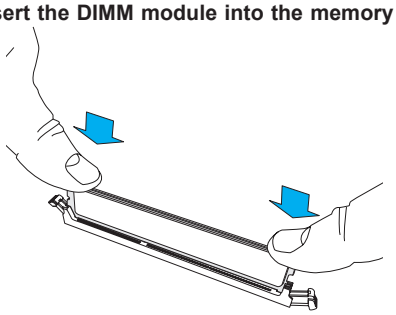


Notches



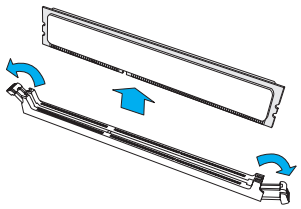
Release Tabs

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 Page 1 of this chapter to prevent ESD-related damages to your memory modules or components.

2.5 Rear I/O Ports

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

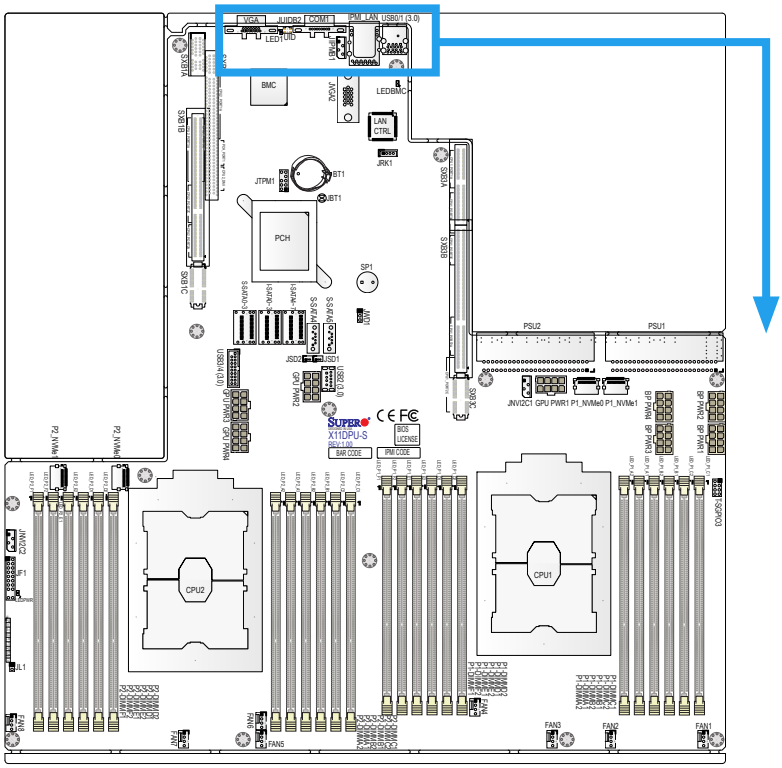
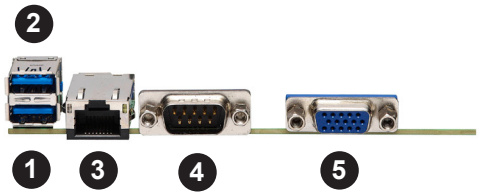


Figure 2-2. I/O Port Locations and Definitions



Rear I/O Ports	
#	**Description**
1.	USB0 (3.0)
2.	USB1 (3.0)
3.	IPMI Dedicated LAN
4.	COM Port 1
5.	VGA

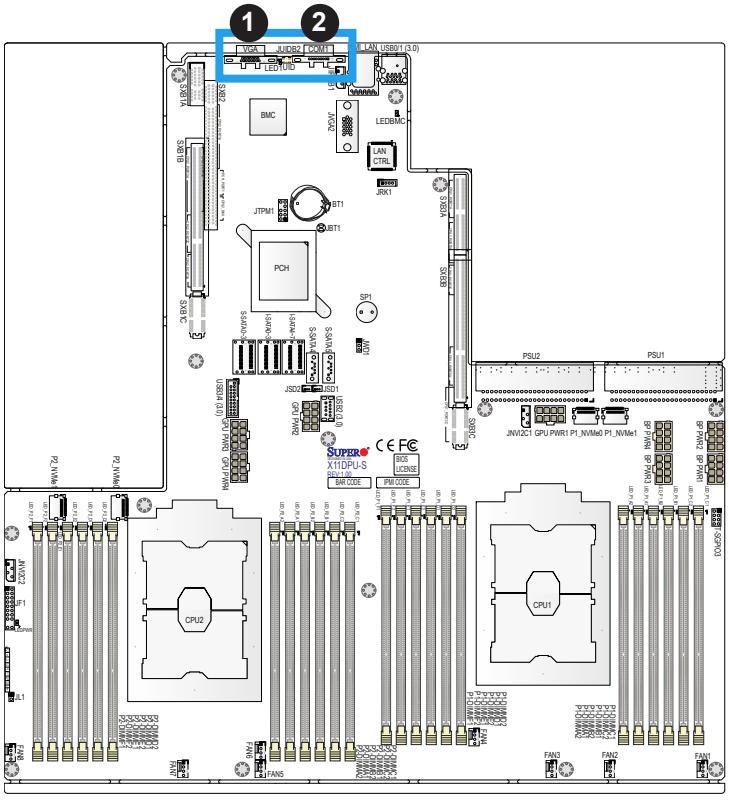
VGA Port

One VGA port is located next to COM Port 1 on the I/O back panel. Use this connection for VGA display.

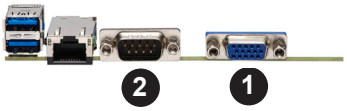
Serial Port

There is one COM port (COM1) on the I/O back panel on the motherboard. This COM port provides serial communication support. See the table below for pin definitions.

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



1. VGA Port
2. COM Port 1



Universal Serial Bus (USB) Ports

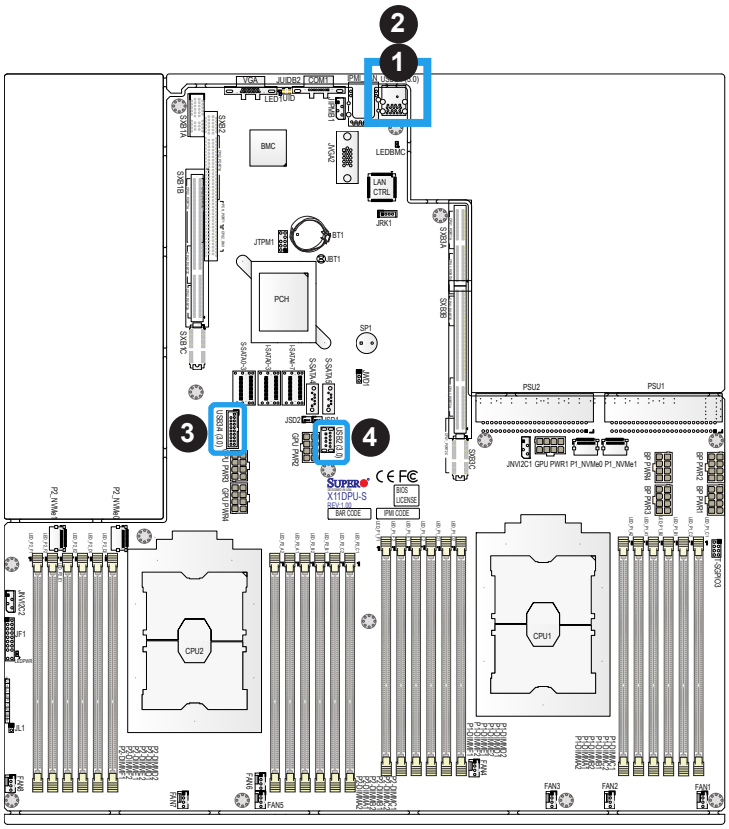
There are two USB 3.0 ports (USB0/USB1) located on the I/O back panel. The motherboard also has a front access USB 3.0 header that supports two USB connections (USB3/USB4). A USB Type A header (USB2), located next to GPU PWR2, provides also USB 3.0 support. The onboard headers can be used to provide front side USB access with a cable (not included).

Back Panel USB (3.0) Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	10	Power
2	D-	11	USB 2.0 Differential Pair
3	D+	12	
4	Ground	13	Ground of PWR Return
5	StdA_SSRX-	14	SuperSpeed Receiver
6	StdA_SSRX+	15	Differential Pair
7	GND_DRAIN	16	Ground for Signal Return
8	StdA_SSTX-	17	SuperSpeed Transmitter
9	StdA_SSTX+	18	Differential Pair

Front Panel USB (3.0) Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	19	Power
2	Stda_SSRX-	18	USB3_RN
3	Stda_SSRX+	17	USB3_RP
4	Ground	16	Ground
5	Stda_SSTX-	15	USB3_TN
6	Stda_SSTX+	14	USB3_TP
7	Ground	13	Ground
8	D-	12	USB_N
9	D+	11	USB_P
10		x	



1. USB0 (3.0)
2. USB1 (3.0)
3. USB3/4 (USB 3.0)
4. Type A USB2 (USB 3.0)

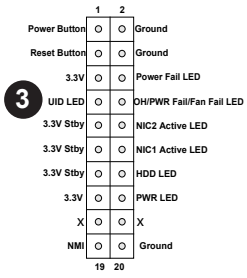
Unit Identifier Switch/UID LED Indicator

A rear Unit Identifier (UID) switch (JUIDB2) and an rear LED Indicator (LED1) are located on the rear side of the system. 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

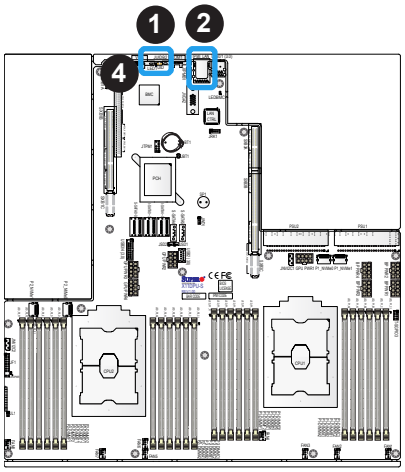
UID LED Pin Definitions	
Color	**Status**
Blue: On	Unit Identified



IPMI LAN Port

An IPMI_Dedicated LAN that supports Gigabit LAN is located next to USB0/USB1 ports on the back panel. This LAN port is supported by the onboard Nuvoton NPCM710S BMC and accepts an RJ45 type cable. Refer to the LED Indicator Section for LAN LED information.

Note: For additional LAN connections, please install an appropriate Ultra riser card on Slot SXB3A/3B/3C. Please refer to the AOC list posted at http://www.supermicro.com/support/resources/aoc/aoc_compatibility_ultra.cfm for more information.

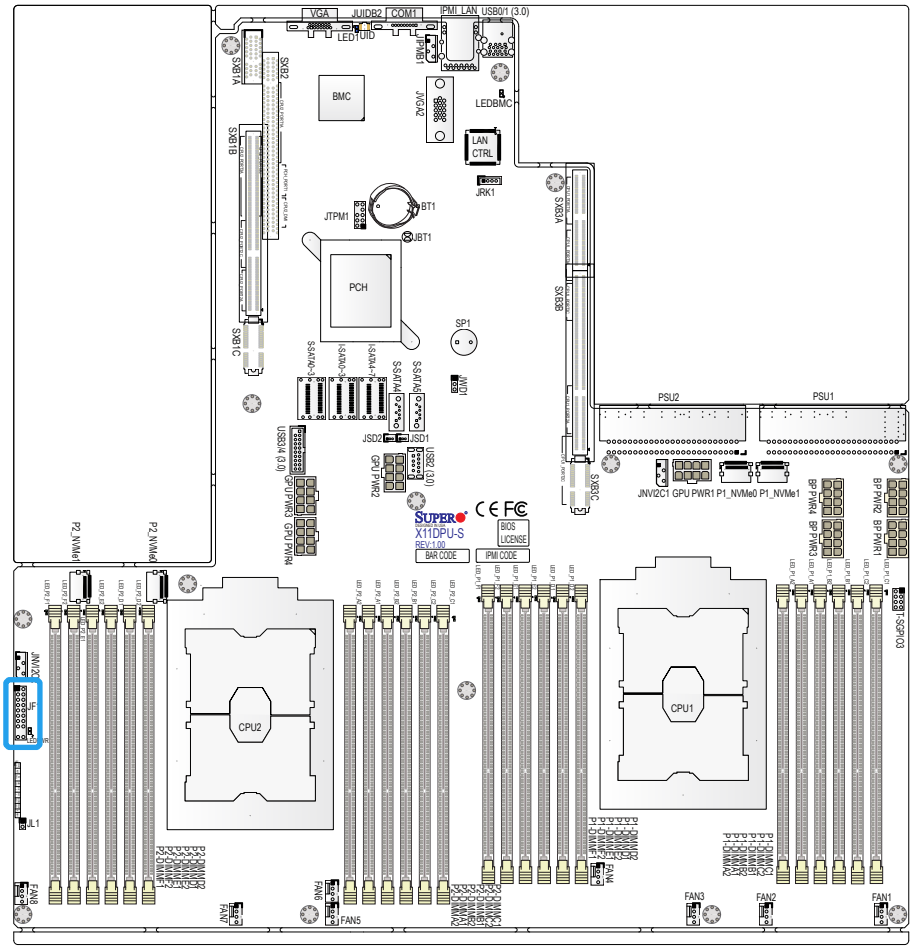


1. UID
2. IPMI_LAN
3. Front UID LED
4. LED1

LAN Ports Pin Definitions			
Pin#	**Definition**	**Pin#**	**Definition**
1	P2V5SB	10	SGND
2	TD0+	11	Act LED
3	TD0-	12	P3V3SB
4	TD1+	13	Link 100 LED (Yellow, +3V3SB)
5	TD1-	14	Link 1000 LED (Yellow, +3V3SB)
6	TD2+	15	Ground
7	TD2-	16	Ground
8	TD3+	17	Ground
9	TD3-	18	Ground

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	○	○	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	○	○	HDD LED
3.3V	○	○	PWR LED
X	○	○	X
NMI	○	○	Ground
	19	20	

Figure 2-3. JF1 Header Pins

NMI Button

The non-maskable interrupt 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

Power LED

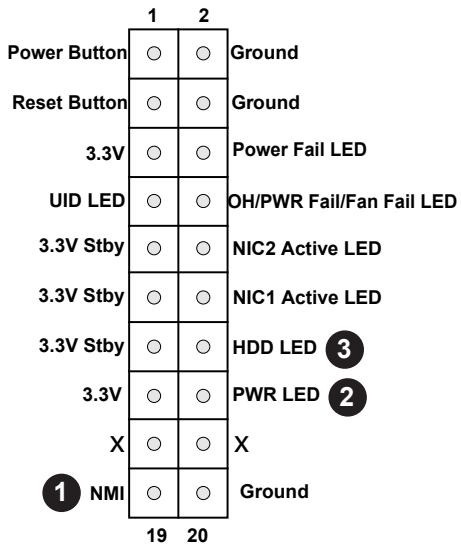
The Power LED connection is located on pins 15 and 16 of JF1. Refer to the table below for pin definitions.

Power LED Pin Definitions (JF1)	
Pin#	Definition
15	Vcc
16	FP PWR 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	Vcc
14	HDD LED



1. NMI
2. FP PWR LED
3. HDD LED

NIC1/NIC2 (LAN1/LAN2) LED

The NIC (Network Interface Controller) LED connection for LAN port 1 is located on pin 12 of JF1, and LAN port 2 is on pin 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

UID/OH/Fan Fail/PWR Fail LED

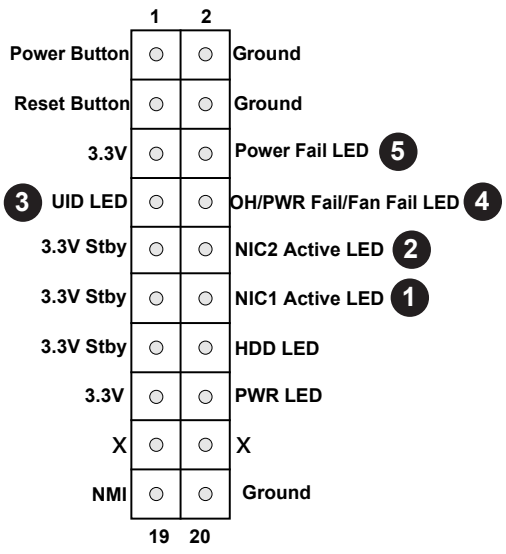
Connect an LED cable to pins 7 and 8 of the Front Control Panel (JF1) to use UID/Overheat/ Fan Fail/Power Fail LED connections. The LED on pin 8 provides warnings of overheat, power failure or fan failure. Refer to the tables below for details.

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.

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



1. NIC1 LED
2. NIC2 LED
3. Front UID LED
4. OH/PWR Fail/Fan Fail LED
5. PWR Fail LED

Reset Button

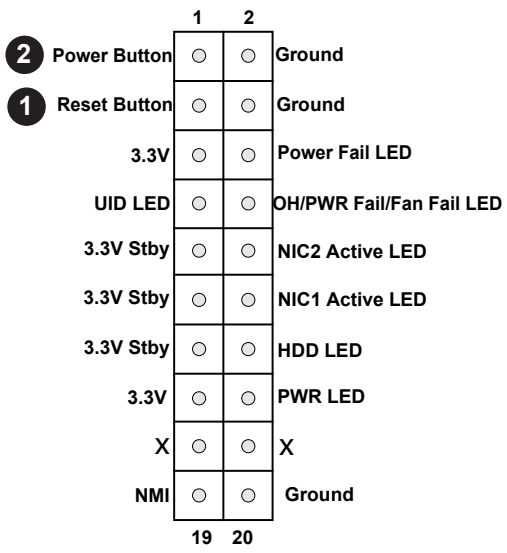
The Reset Button connection is located on pins 3 and 4 of JF1. Attach it to a hardware reset switch on the computer case to reset the system. Refer to the table below for pin definitions.

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

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. To turn off the power in the suspend mode, press the button for at least four seconds. Refer to the table below for pin definitions.

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



1. Reset Button
2. Power Button

2.7 Connectors

Power Connections

SMCI-Propietary Main Power Supply Units

Two SMCI-proprietary main power supply units are located at PSU1 and PSU2. Connect appropriate power supply units to these two headers to provide adequate power to your system.

Backplane Power Connectors & GPU Power Connectors

In addition to the two SMCI-proprietary main power supply units located at PSU1/PSU2, eight 8-pin power connectors are also located on the motherboard to supply power to onboard devices. GPU Power Connectors 1~4 are used for GPU devices, while BP PWR 1~4 are used for backplane devices. Connect these connectors to your power supply to provide adequate power to your onboard devices.

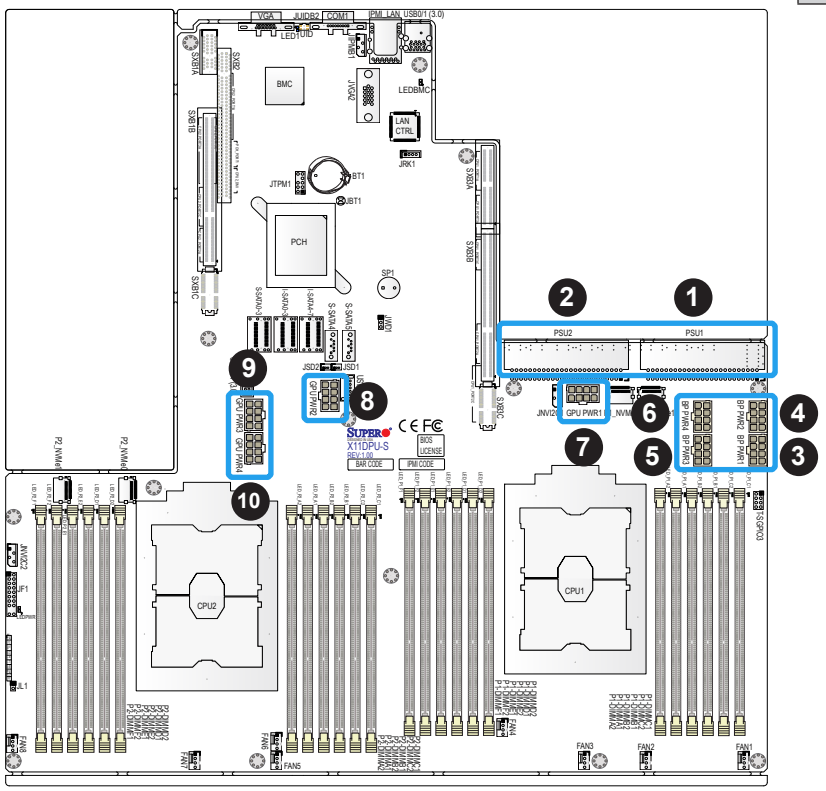
Warning: To provide adequate power to your system and to avoid damaging the power supply or the motherboard, be sure to connect all power connectors mentioned above to the power supply. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.

8-pin GPU Power Pin Definitions

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

8-pin Backplane Power Pin Definitions

Pin#	Definition
1 - 4	Ground
5 - 6	+12V
7 - 8	+5V



1. PSU1 (Required)
2. PSU2 (Required)
3. BP PWR1 (Required)
4. BP PWR2 (Required)
5. BP PWR3 (Required)
6. BP PWR4 (Required)
7. GPU PWR1 (Required)
8. GPU PWR2 (Required)
9. GPU PWR3 (Required)
10. GPU PWR4 (Required)

Headers

Fan Headers

There are eight 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 monitored and controlled by BMC. Use 4-pin fan headers for fan speed control support.

Fan Header Pin Definitions

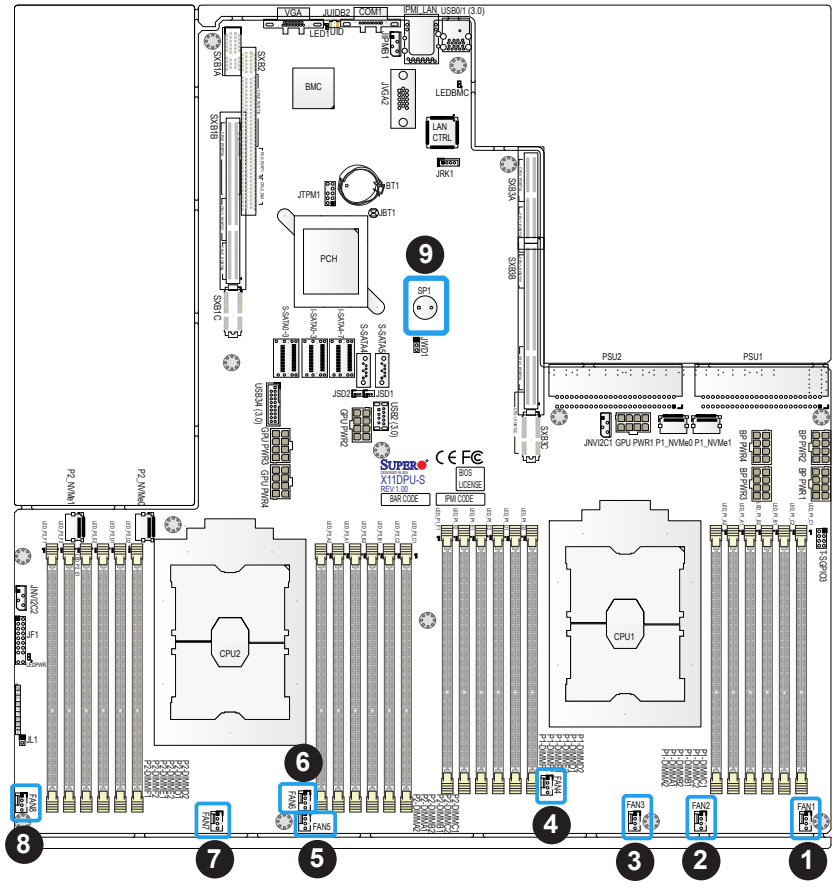
Pin#	Definition
1	Ground (Black)
2	+12V (Red)
3	Tachometer
4	PWM Control

Internal Speaker/Buzzer

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

Internal Buzzer Pin Definitions

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



1. FAN1
2. FAN2
3. FAN3
4. FAN4
5. FAN5
6. FAN6
7. FAN7
8. FAN8
9. Internal Speaker

T-SGPIO3 Header

A Serial General Purpose Input/Output header (T-SGPIO3) is located on the motherboard. This header is used to communicate with the enclosure management chip on the backplane. See the table below for pin definitions.

SGPIO Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	NC	2	NC
3	Ground	4	DATA Out
5	Load	6	Ground
7	Clock	8	NC

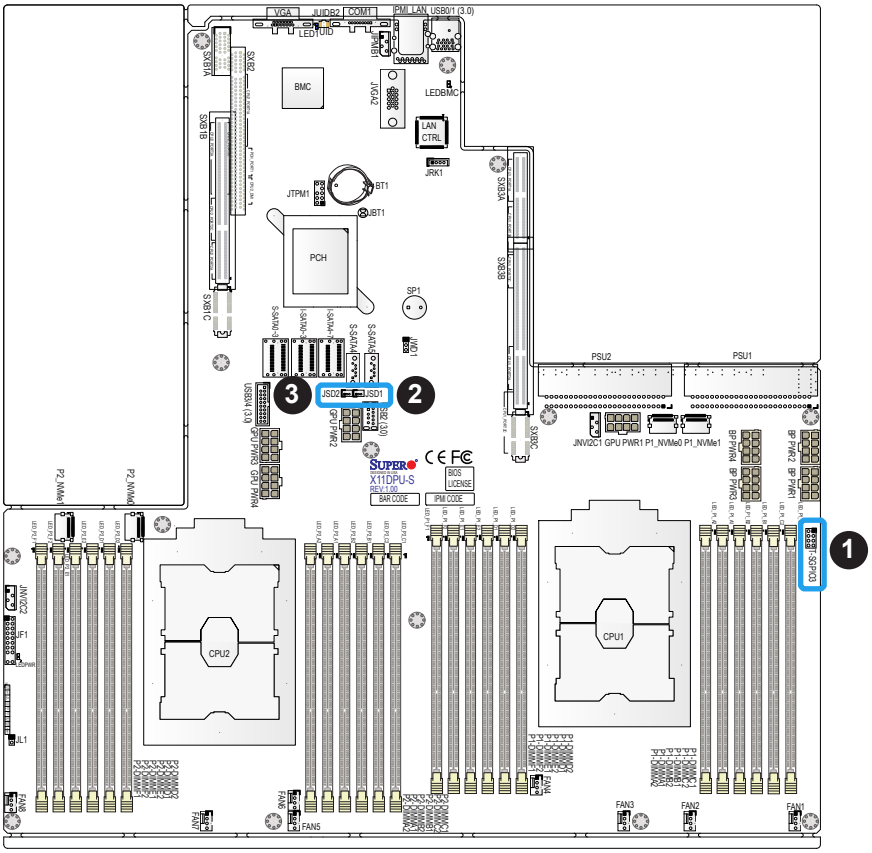
NC = No Connection

Disk-On-Module Power Connectors

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

DOM Power Pin Definitions

Pin#	Definition
1	5V
2	Ground
3	Ground

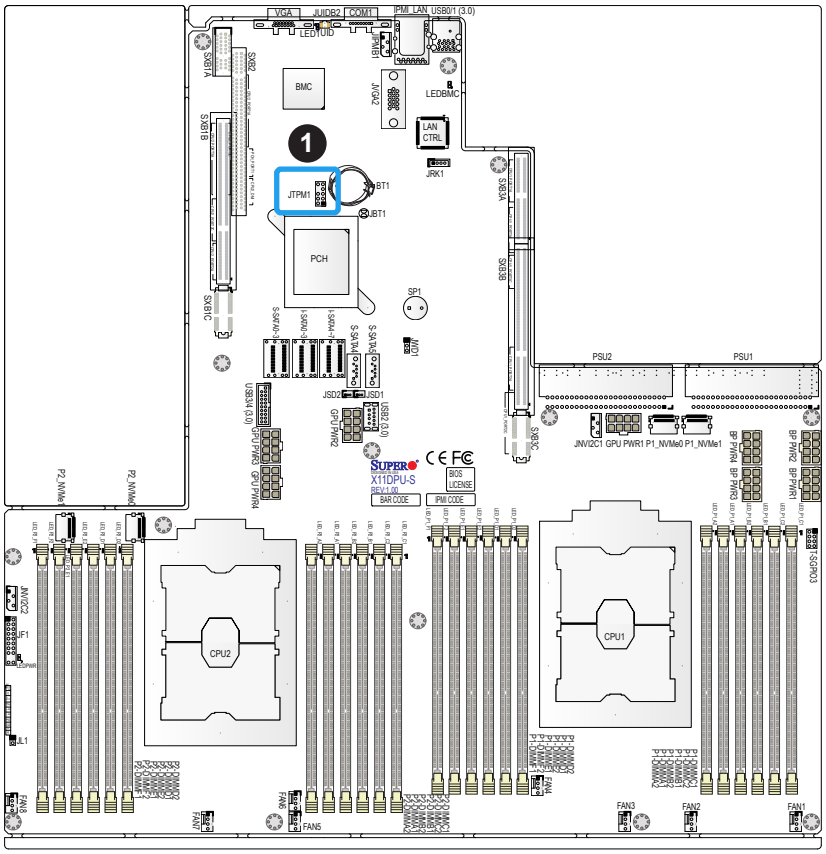


1. T-SGPIO3
2. JSD1
3. JSD2

TPM Header

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

Trusted Platform Module/Port 80 Header Pin Definitions			
Pin#	**Definition**	**Pin#**	**Definition**
1	P3V3	2	SPI_TPM_CS_N
3	PCIE_RESET_N#	4	SPI_PCH_MISO
5	SPI_PCH_CLK#	6	Ground
7	SPI_PCH_MOSI	8	N/A
9	JTPM1_P3V3A	10	IRQ_TPM_SPIN_N



1. TPM/Port 80 Header

4-pin BMC External I2C Header

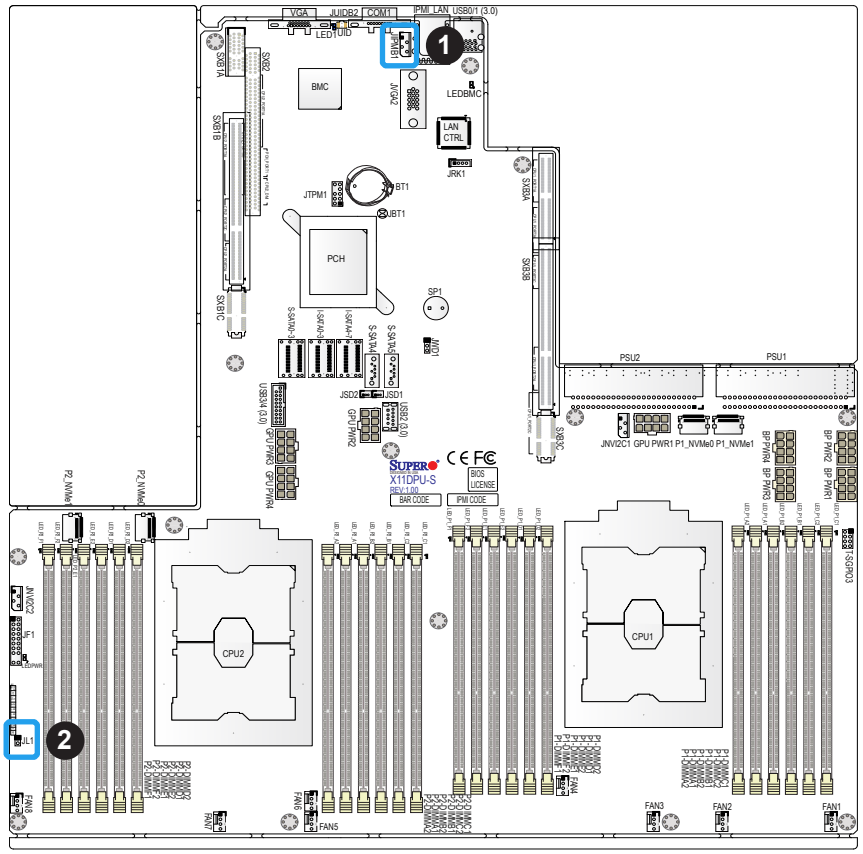
A System Management Bus header for IPMI 2.0 is located at JIPMB1. Connect a cable to this header to use the IPMB I²C connection on your system. See the table below for pin definitions.

External I²C Header Pin Definitions	
Pin#	**Definition**
1	Data
2	Ground
3	Clock
4	No Connection

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



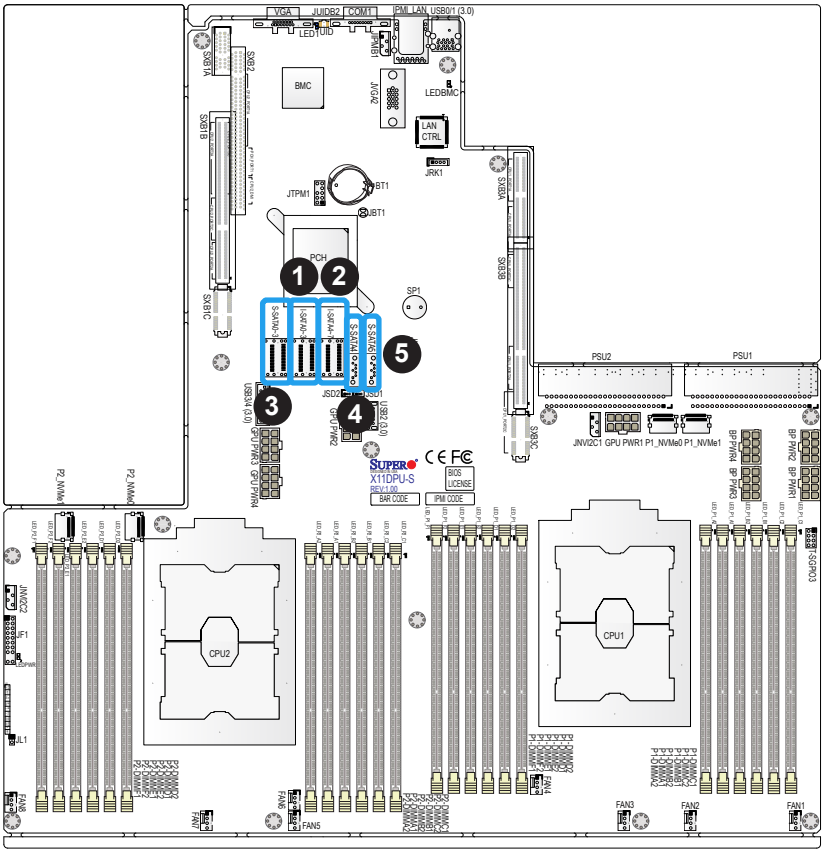
1. BMC External I²C Header
2. Chassis Intrusion

I-SATA 3.0 and S-SATA 3.0 Ports

The X11DPU-S has eight I-SATA 3.0 ports (I-SATA0~3, I-SATA4~7) which are supported by the Intel C621 chipset. In addition, it also has six S-SATA 3.0 ports (S-SATA0~3, S-SATA4/S-SATA5) that are supported by the Intel SCU. S-SATA4/S-SATA5 can be used with Supermicro SuperDOMs which are yellow SATA DOM connectors with power pins built in, and do not require external power cables. Supermicro SuperDOMs are backward-compatible with regular SATA HDDs or SATA DOMs that need external power cables. All these SATA ports provide serial-link signal connections, which are faster than the connections of Parallel ATA.

SATA 3.0 Port Pin Definitions

Pin#	Signal
1	Ground
2	SATA_TXP
3	SATA_TXN
4	Ground
5	SATA_RXN
6	SATA_RXP
7	Ground

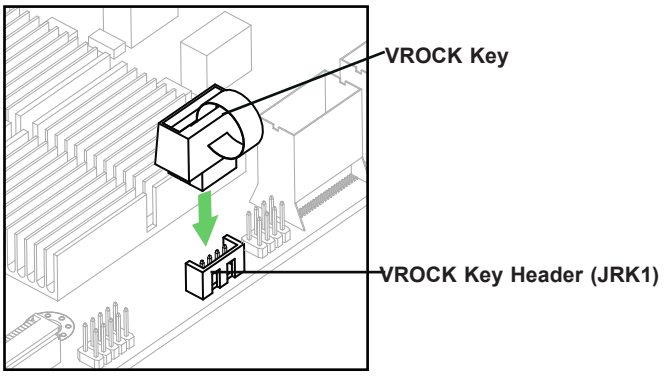


1. I-SATA0~3
2. I-SATA4~7
3. S-SATA0~3
4. S-SATA4
5. S-SATA5

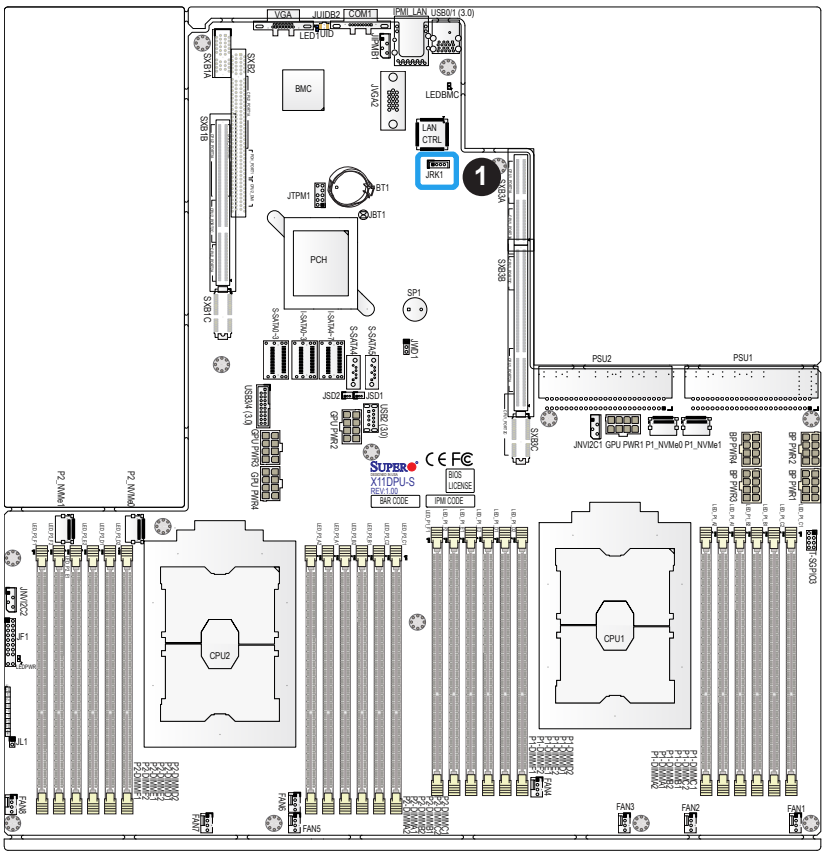
VROC RAID Key Header

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. Please refer to the layout below for the location of JRK1.

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



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

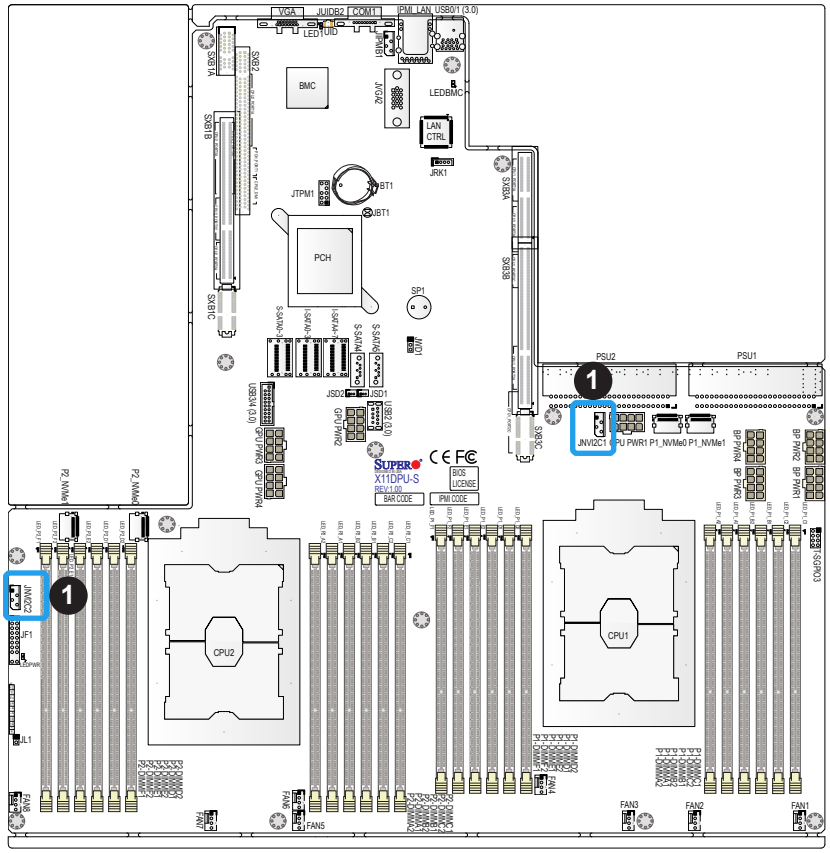


1. VROC RAID Key Header

NVMe SMBus Headers

NVMe SMBus (I^2C) headers (JNVI^{2}C1/JNVI^{2}C2), used for PCI-E SMBus clock and data connections, provide hot-plug support via a dedicated SMBus interface. This feature is only available for a Supermicro complete system with an SMCI-proprietary NVMe add-on card and cable installed. See the table below for pin definitions.

NVMe SMBus Header Pin Definitions	
Pin#	**Definition**
1	Data
2	Ground
3	Clock
4	VCCIO



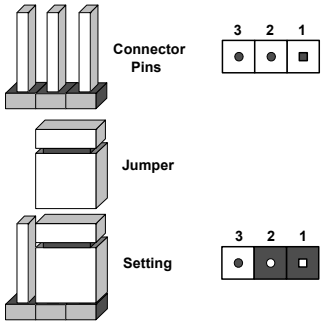
1. NVMe I^{2}C Headers

2.8 Jumper Settings

How Jumpers Work

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

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



CMOS Clear

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

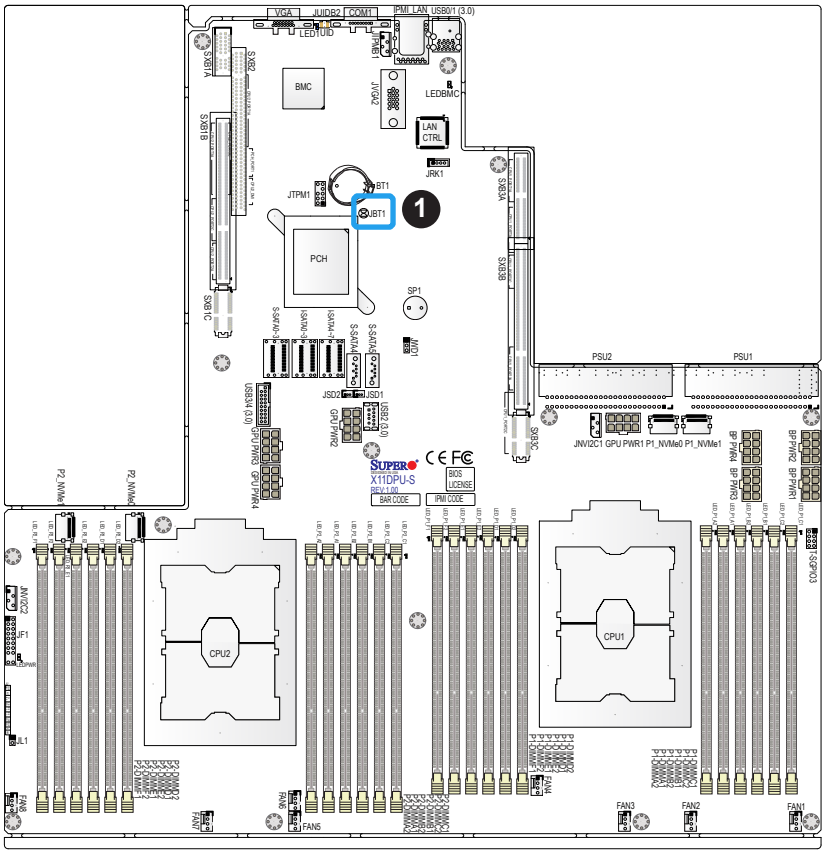
To Clear CMOS

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

Note: Clearing CMOS will also clear all passwords.

Do not use the PW_ON connector to clear CMOS.

JBT1 contact pads



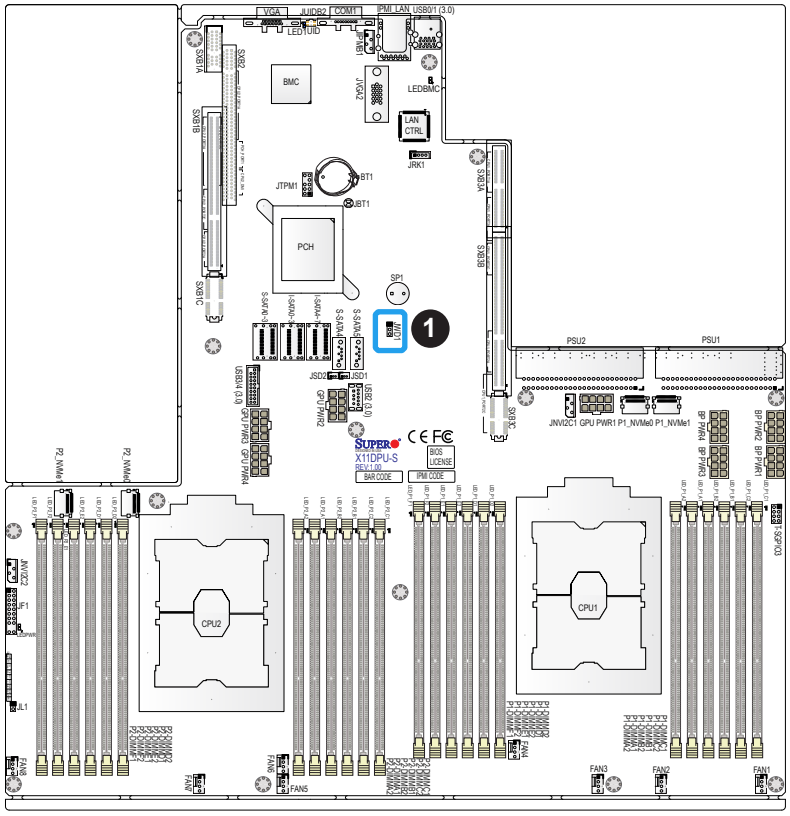
1. CMOS Clear

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

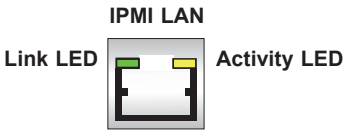


1. Watch Dog

2.9 LED Indicators

IPMI-Dedicated LAN LEDs

A dedicated IPMI LAN 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. See the table below for more information.

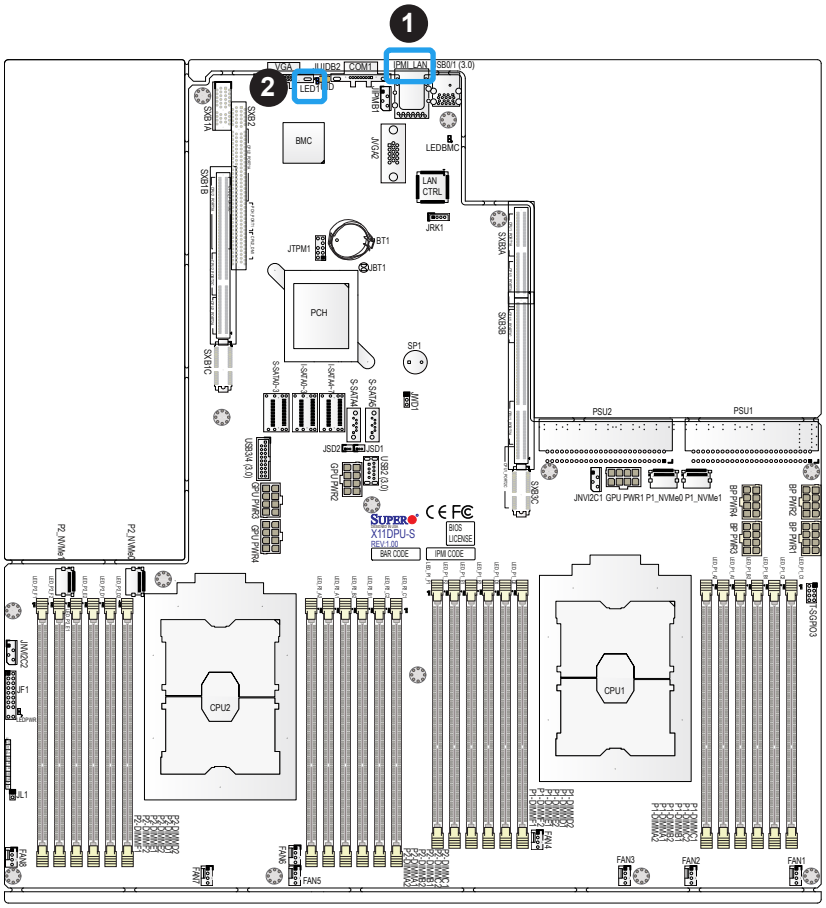


IPMI LAN LEDs		
Color	**Status**	**Definition**
Off	Off	No Connection
Green: Solid	Link/Speed (Left)	100 Mb/s
Amber Blinking	Activity (Right)	Active

Unit ID LED

A rear UID LED indicator at LED1 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. IPMI-Dedicated LAN LEDs
2. UID LED

Onboard Power LED

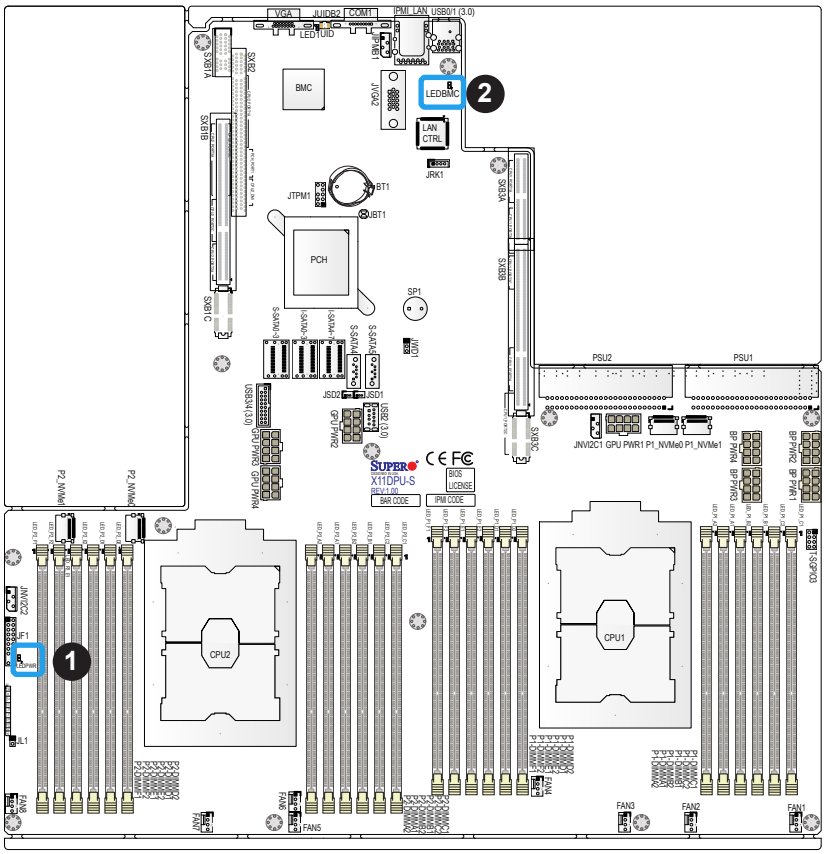
LEDPWR is an Onboard Power LED. When this LED is lit, it means that power is present on the motherboard. Be sure to turn off the system and unplug the power cord(s) before removing or installing components.

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

BMC Heartbeat LED

LEDBMC is the BMC heartbeat LED. When the LED is blinking green, BMC is functioning normally. See the table below for the LED status.

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

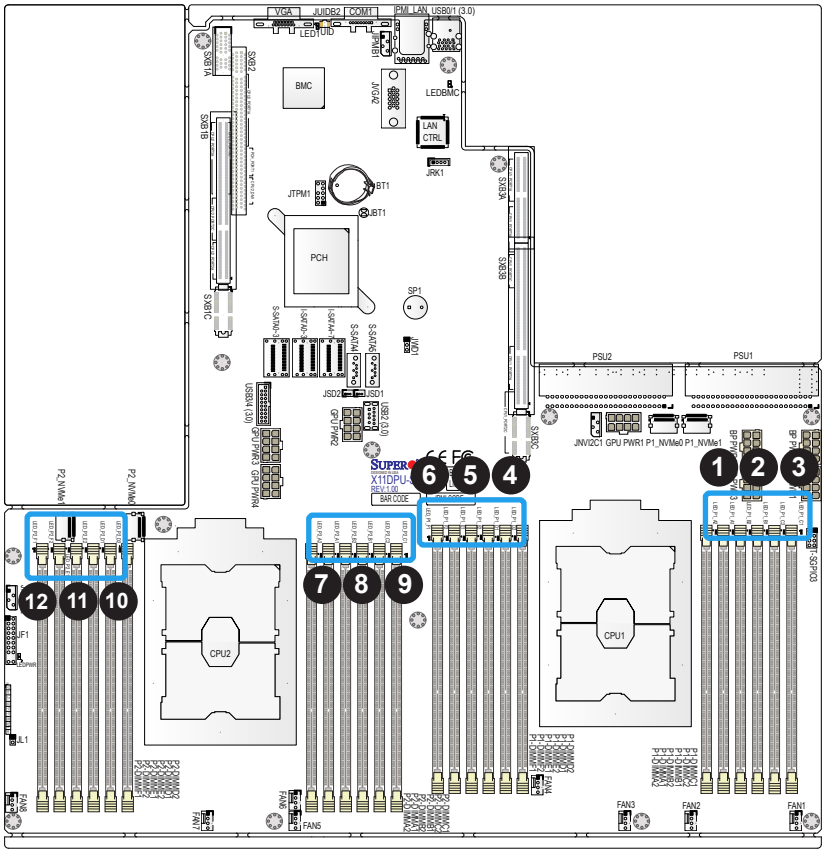


1. Onboard Power LED
2. BMC Heartbeat LED

Memory Fault Indication LEDs

The memory fault LEDs provide visual notification to a service technician which memory DIMM slot(s) are at fault due to un-correctable memory errors during POST (Power-On Self-Test). A memory fault LED will remain "on" even after system reboots (or repeated "power cycling") until it is reset manually by the technician using the BIOS setup menu to turn it off. This feature allows the technician to easily identify and replace any bad DIMMs that may be at fault in the system.

Memory Fault LED Indicators		
LED	**Description**	**Status**
LED_P1_A1~A2	Memory Fault LEDs for Memory Module P1_A1~A2	Red: on (memory errors)
LED_P1_B1~B2	Memory Fault LEDs for Memory Module P1_B1~B2	Red: on (memory errors)
LED_P1_C1~C2	Memory Fault LEDs for Memory Module P1_C1~C2	Red: on (memory errors)
LED_P1_D1~D2	Memory Fault LEDs for Memory Module P1_D1~D2	Red: on (memory errors)
LED_P1_E1~E2	Memory Fault LEDs for Memory Module P1_E1~E2	Red: on (memory errors)
LED_P1_F1~F2	Memory Fault LEDs for Memory Module P1_F1~F2	Red: on (memory errors)
LED_P2_A1~A2	Memory Fault LEDs for Memory Module P2_A1~A2	Red: on (memory errors)
LED_P2_B1~B2	Memory Fault LEDs for Memory Module P2_B1~B2	Red: on (memory errors)
LED_P2_C1~C2	Memory Fault LEDs for Memory Module P2_C1~C2	Red: on (memory errors)
LED_P2_D1~D2	Memory Fault LEDs for Memory Module P2_D1~D2	Red: on (memory errors)
LED_P2_E1~E2	Memory Fault LEDs for Memory Module P2_E1~E2	Red: on (memory errors)
LED_P2_F1~F2	Memory Fault LEDs for Memory Module P2_F1~F2	Red: on (memory errors)



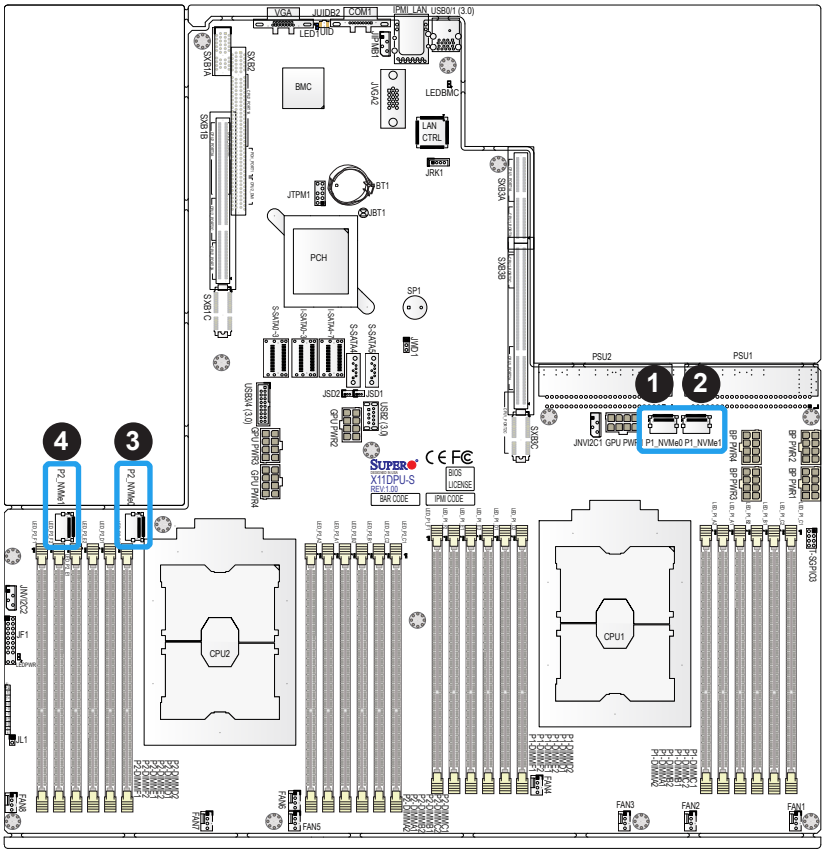
1. LED_P1_A1~A2
2. LED_P1_B1~B2
3. LED_P1_C1~C2
4. LED_P1_D1~D2
5. LED_P1_E1~E2
6. LED_P1_F1~F2
7. LED_P2_A1~A2
8. LED_P2_B1~B2
9. LED_P2_C1~C2
10. LED_P2_D1~D2
11. LED_P2_E1~E2
12. LED_P2_F1~F2

2.10 NVM Express Connections

NVM Express Connections

Four NVM Express ports are located on the motherboard. These NVM ports provide PCI-E 3.0 x4 connections. P1_NVMe0 and P1_NVMe1 are supported by CPU1. P2_NVMe0 and P1_NVMe1 are supported by CPU2. The NVM Express ports 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 PCI-E latency by simplifying driver/software requirements resulting from direct PCI-E interface from the CPU to the NVMe SSD drives.

Note: When installing an NVMe device on a motherboard, please be sure to connect the first NVMe port (P1_NVMe0) first for your system to work properly.



1. P1_NVMe0
2. P1_NVMe1
3. P2_NVMe0
4. P2_NVMe1

Chapter 3

Troubleshooting

3.1 Troubleshooting Procedures

Use the following procedures to troubleshoot your system. If you have followed all of the procedures below and still need assistance, refer to the 'Technical Support Procedures' and/or 'Returning Merchandise for Service' section(s) in this chapter. Always disconnect the AC power cord before adding, changing or installing any non hot-swap hardware components.

Before Power On

1. 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 internal speaker and 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 (CR2032) 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. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.

No Video

1. If the power is on but you have no video, remove all the add-on cards and cables.
2. Use the speaker to determine if any beep codes exist. Refer to Appendix A for details on beep codes.

System Boot Failure

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

1. Check for any error beep from the motherboard speaker.

- If there is no error beep, try to turn on the system without DIMM modules installed. If there is still no error beep, replace the motherboard.
- If there are error beeps, clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS Clear Jumper (JBT1). Refer to chapter 2.

2. Remove all components from the motherboard, especially the DIMM modules. Make sure that system power is on and that memory error beeps are activated.
3. Turn on the system with only one DIMM module installed. If the system boots, check for bad DIMM modules or slots by following the Memory Errors Troubleshooting procedure in this Chapter.

Memory Errors

1. Make sure that the DIMM modules are properly and fully installed.
2. Confirm 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. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.

3. If the above steps do not fix the setup configuration problem, contact your vendor for repairs.

When the System Becomes Unstable

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

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

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

   Note: 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 make sure that the CPU and system temperatures are within the normal range. Also check the front panel Overheat LED and make sure that it is not on.

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

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

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

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

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 depending 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

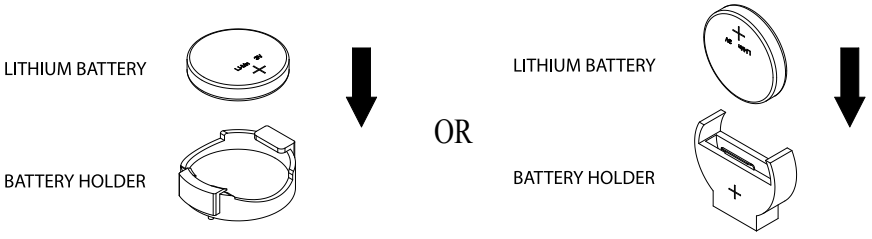
Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency 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: The X11DPU-S motherboard supports up to 6TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 3TB of Load Registered DIMM (LRDIMM), with speeds of 2933*/2666/2400/2133/1866/1600/1333 MHz modules in 24 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 X11DPU-S motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.

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

Starting the Setup Utility

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

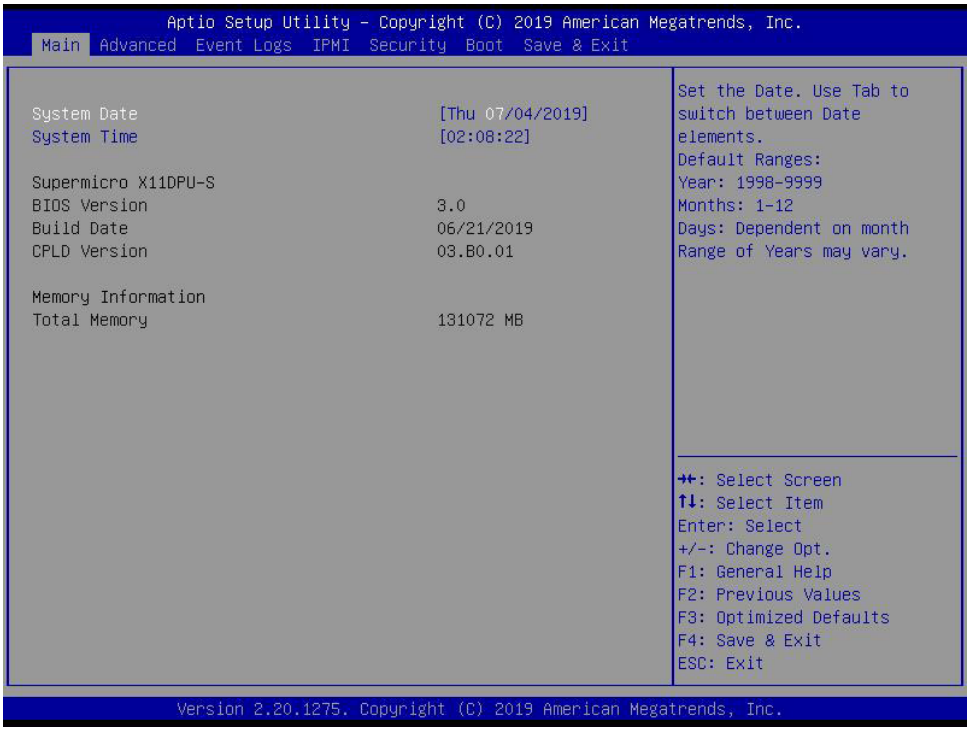
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it. (Note that the AMI 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 AMI BIOS Setup utility, you will enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS setup screen is shown below. The following Main menu items will be displayed:



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 after RTC reset.

Supermicro X11DPU-S

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.

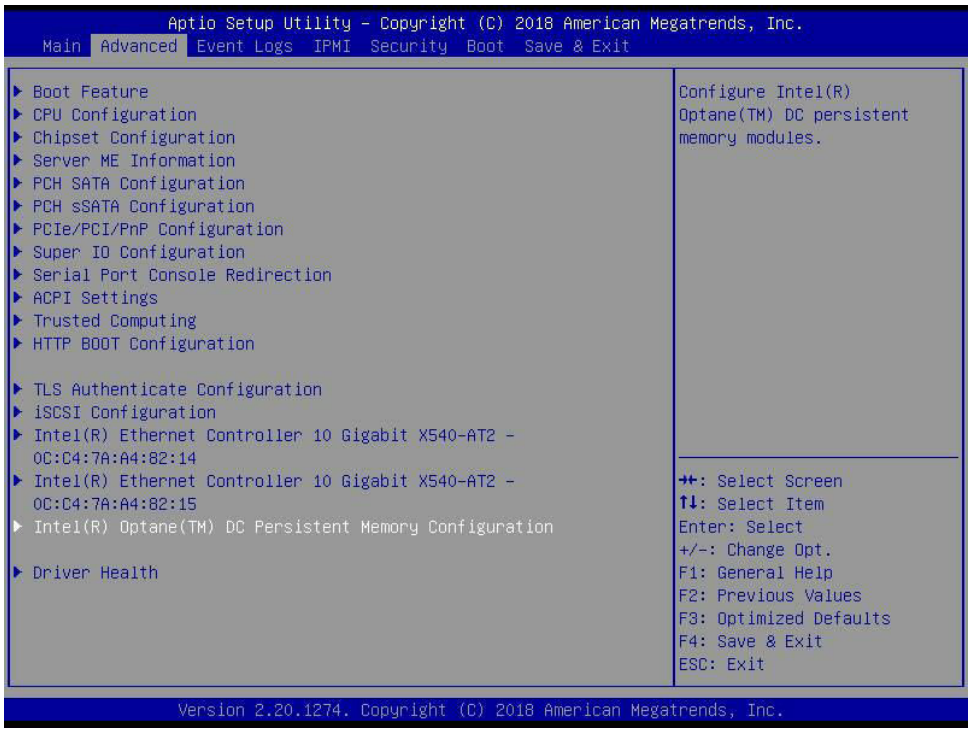
Memory Information

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 Boot Setup and press <Enter> to access the submenu items.



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

▶Boot Feature

Quiet Boot

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

Option ROM Messages

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

Bootup NumLock State

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

Wait For "F1" If Error

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

INT19 (Interrupt 19) Trap Response

Interrupt 19 is the software interrupt that handles the boot disk function. When this feature is set to Immediate, the ROM BIOS of the host 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 and 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 (Expansible 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

Enable this feature to use the USB keyboard and mouse during the Windows 7 installation, since the native XHCI driver support is unavailable. Use a SATA optical drive as a USB drive. USB CD/DVD drives are not supported. Disable this feature after the XHCI driver has been installed in Windows. The options are **Disabled** and Enabled.

Port 61h Bit-4 Emulation

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

Power Configuration

Watch Dog Function

If enabled, the Watch Dog Timer will allow the system to reset or generate NMI based on jumper settings when it is expired for more than 5 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.

Throttle on Power Fail

Throttling improves reliability and reduces power consumption in the processor via automatic voltage control during processor idle states. Select Enabled to decrease the system power by throttling CPU frequency when one power supply is failed. The options are **Disabled** and Enabled.

▶CPU Configuration

This submenu displays the information of the CPU as detected by the BIOS. It also allows the user to configuration CPU settings:

- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ration
- Processor Min Ration
- 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 support Intel® Hyper-threading Technology to enhance CPU performance. The options are Disable and **Enable**.

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

Select Enable to enable the Execute-Disable Bit 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 or damage the system during an attack. (Please refer to Intel's website for more information.) The options are Disable and **Enable**.

Intel Virtualization Technology (Available when supported by the CPU)

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's website for detailed information.

PPIN Control

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

Hardware Prefetcher (Available when supported by the CPU)

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

Adjacent Cache Prefetch (Available when supported by the CPU)

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

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enabled to enable Intel® CPU Advanced Encryption Standard (AES) Instructions for CPU to enhance data integrity. The options are **Enable** and Disable.

DCU IP Prefetcher (Available when supported by the CPU)

If this feature is set to Enable, the DCU (Data Cache Unit) IP prefetcher will prefetch IP addresses in advance to improve network connectivity and system performance. The options are **Enable** and Disable.

LLC Prefetch

Select Enable to support the LLC prefetch on all threads. The options are **Disable** and Enable.

Extended APIC (Extended Advanced Programmable Interrupt Controller)

Select Enable to use the extended APIC (Advanced Programmable Interrupt Control) support to enhance power management. 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

▶CPU P State Control

SpeedStep (Pstates)

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

Activate PBF (Available when SpeedStep is set to Enable)

Select Enable to enable Prioritized Base Frequency (PBF) feature support which will enhance 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. The options are **Enable** and Disable.

EIST PSD Function

This feature allows the user to change the P-State (Power-Performance State) coordination type. P-State is also known as "SpeedStep" for Intel® processors. Select HW_ALL to change the P-State coordination type for all hardware components only. Select SW_ALL to change the P-State coordination type for all software installed in the system. Select SW_ANY to change the P-State coordination type for a particular software program specified by the user in the system. The options are **HW_ALL**, SW_ALL, and SW_ANY.

Turbo Mode (Available when Intel® EIST Technology is enabled)

Select Enable to use the Turbo Mode to boost system performance. The options are Disable and **Enable**.

▶Hardware PM State Control

Hardware P-States

This feature enables the hardware P-States support. The options are **Disable**, Native Mode, Out of Band Mode, and Native Mode with No Legacy Support.

▶CPU C State Control

Autonomous Core C-State

Use this feature to enable the autonomous core C-State control. The options are **Disable** and Enable.

CPU C6 report

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

Enhanced Halt State (C1E)

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

▶Package C State Control

Package C State

This feature allows the user to set the limit on the C-State package register. The options are C0/C1 state, C2 state, C6 (non Retention) state, C6 (Retention) state, No Limit, and **Auto**.

▶CPU T State Control

Software Controlled T-States

This feature enables the software controlled T-States support. 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 following North Bridge settings.

▶UPI Configuration

UPI Configuration

The following information will be displayed:

- Number of CPU

- Number of IIO
- 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

Select **Topology Precedence** to degrade features if system options are in conflict. Select Feature Precedence to degrade topology if system options are in conflict. The options are **Topology Precedence** and Feature Precedence.

Link L0p Enable

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

Link L1 Enable

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

IO Directory Cache (IODC)

Use this feature to enable the IO Directory Cache (IODC) support. 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.

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 Enable to enforce POR restrictions on DDR4 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 permanent repair on a raw element. The options are **Auto**, Hard PPR, Soft PPR, and PPR Disabled.

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:** 2933 MHz memory is supported by 2nd Gen Intel Xeon Scalable-SP (82xx/62xx series) processors only.)

Data Scrambling for NVMDIMM

Select Enable to enable data scrambling to enhance system performance and data integrity. The options are **Auto**, Disable, and Enable.

Data Scrambling for DDR4

Use this feature to enable data scrambling for DDR4. The options are **Auto**, Disable, and Enable.

Enable ADR

Select Enable for ADR (Automatic Diagnostic Repository) support to enhance memory performance. The options are **Disable** and Enable.

Refresh Options

Use this feature to select the self refresh mode. The options are Accelerated Self Refresh and **2x Refresh**.

▶Memory Topology

The following information will be displayed: P1 DIMMA1/P1 DIMMB1/P1 DIMMC1/P1 DIMMD1/P1 DIMME1/P1 DIMMF1

▶Memory RAS (Reliability_Availability_Serviceability) Configuration

Memory RAS Configuration Setup

Use this submenu to configure the following Memory RAS settings.

Static Virtual Lockstep Mode

Select Enable to support the static virtual lockstep mode. The options are **Disable** and Enable.

Mirror Mode

Use this feature to select the mirror mode. The options are **Disable**, Mirror Mode 1LM, and Mirror Mode 2LM. If this feature is set to Mirror Mode 1LM or Mirror Mode 2LM, the available memory capacity will be reduced by 50 percent.

UEFI ARM Mirror

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

Memory Rank Sparing

Select Enable to enable memory-sparing support for memory ranks to improve memory performance. The options are **Disable** and Enable.

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

Multi Rank Sparing

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 feature to enter the threshold value for correctable memory errors. The default setting is **10**.

SDDC Plus One

Single Device Data Correction (SDDC) allows data to be reconstructed when one of the memory devices fails on a DIMM. Use this feature to enable the SDDC support. The options are **Disable** and Enable.

ADDDC Sparing

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

Patrol Scrub

Patrol Scrubbing is a process that allows the CPU to correct correctable memory errors detected on a memory module and send the correction to the requestor (the original source). When this feature is set to Enable, read-and-write will be performed every 16K cycles per cache line if there is no delay caused by internal processing. The options are Disable and **Enable**.

Patrol Scrub Interval

This feature allows you to decide how many hours the system should wait before the next complete patrol scrub is performed. Use the keyboard to enter a value from 0-24. The Default setting is **24**.

▶IIO Configuration

IIO Configuration

EV DFX Features

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

▶CPU1 Configuration

IOU0 (IIO PCIe Br1)

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

IOU1 (IIO PCIe Br2)

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

IOU2 (IIO PCIe Br3)

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

MCP0 (IIO PCIe Br4)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x16 and **Auto**.

MCP1 (IIO PCIe Br5)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x16 and **Auto**.

▶P1_NVMe0

Link Speed

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

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶P1_NVMe1

Link Speed

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

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶AOC-URN6-i2XT NVME2 (Available when the device is detected by the system)

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s).

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶AOC-URN6-i2XT NVME3 (Available when the device is detected by the system)

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s).

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶AOC-URN6-i2XT NVME4 (Available when the device is detected by the system)

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s).

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶AOC-URN6-i2XT NVME5 (Available when the device is detected by the system)

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s).

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶AOC-URN6-i2XT NVME6 (Available when the device is detected by the system)

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s).

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶CPU2 Configuration

IOU0 (IIO PCIe Br1)

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

IOU1 (IIO PCIe Br2)

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

IOU2 (IIO PCIe Br3)

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

MCP0 (IIO PCIe Br4)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x16 and **Auto**.

MCP1 (IIO PCIe Br5)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x16 and **Auto**.

▶RSC-UMR-8 SLOT1

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s)..

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶P2_NVMe0

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s)..

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size -

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶P2_NVMe1

Link Speed

This feature allows the user to select PCI-E support for the device installed in the system. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s)..

PCI-E Port Link Status

PCI-E Port Link Max

PCI-E Port Link Speed

PCI-E Port Max Payload Size -

Select Auto for the system BIOS to automatically set the maximum payload value for a PCI-E device to enhance system performance. The options are 128B, 256B, and **Auto**.

▶IOAT (Intel® IO Acceleration) Configuration

Disable TPH

Select Yes to deactivate TLP Processing Hint support. The options are **No** and Yes.

Prioritize TPH

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

Relaxed Ordering

Select Enable to enable Relaxed Ordering support which will allow certain transactions to violate the strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been enqueued. The options are **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 support by reporting the I/O device assignments to the VMM (Virtual Machine Monitor) through the DMAR ACPI Tables. This feature offers fully-protected I/O resource sharing across Intel® platforms, providing greater reliability, security and availability in networking and data-sharing. The options are **Enable** and Disable.

Interrupt Remapping

Select Enable for Interrupt Remapping support to enhance system performance. The options are **Enable** and Disable.

PassThrough DMA

Select Enable to use the Non-Isoch VT_D engine pass through DMA support. The options are **Enable** and Disable.

ATS

Select Enable to use the Non-Isoch VT_D engine ATS support. The options are **Enable** and Disable.

Posted Interrupt

Use this feature to enable VT_D posted interrupt. The options are **Enable** and Disable.

Coherency Support (Non-Isoch)

Select Enable for the Non-Iscoh 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 PCI-E slot of your choice, this PCI-E slot will be dedicated for VMD use only, and it will no longer support any PCI-E device. To re-activate this slot for PCI-E use, please disable VMD.

▶Intel® VMD for Volume Management Device on CPU1

VMD Config for PStack0

Intel® VMD for Volume Management Device

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

P1_NVMe0 VMD (Available when the device is detected by the system)

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

P1_NVMe1 VMD (Available when the device is detected by the system)

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

Hot Plug Capable (Available when the device is detected by the system)
Use this feature to enable the hot plug support for PCIe root ports 1A~1D. The options are **Disable** and Enable.

VMD Config for PStack1

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

AOC-URN6-i2XT NVME2 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

Hot Plug Capable (Available when the device is detected by the system)
Use this feature to enable the hot plug support for PCIe root ports 2A~2D. The options are Disable and **Enable**.

VMD Config for PStack2

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

AOC-URN6-i2XT NVME3 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

AOC-URN6-i2XT NVME4 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

AOC-URN6-i2XT NVME5 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

AOC-URN6-i2XT NVME6 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

Hot Plug Capable (Available when the device is detected by the system)
Use this feature to enable the hot plug support for PCIe root ports 3A~3D. The options are Disable and **Enable**.

▶Intel® VMD for Volume Management Device on CPU2

VMD Config for PStack0

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

RSC-UMR-8 SLOT1 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

P2_NVMe0 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

P2_NVMe1 VMD (Available when the device is detected by the system)
Select Enable to use the Intel® Volume Management Device Technology for this device. The options are Disable and **Enable**.

Hot Plug Capable (Available when the device is detected by the system)
Use this feature to enable the hot plug support for PCIe root ports 1A~1D. The options are Disable and **Enable**.

VMD Config for PStack1

Intel® VMD for Volume Management Device
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, 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)

Use this feature to enable the hot plug support for PCIe root ports 2A~2D. The options are **Disable** and Enable.

VMD Config for PStack2

Intel® VMD for Volume Management Device

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, 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)

Use this feature to enable the hot plug support for PCIe root ports 3A~3D. The options are **Disable** and Enable.

IIO-PCIE Express Global Options

PCI-E Completion Timeout Disable

Use this feature for PCI-E Completion Timeout support for electric tuning. The options are Yes, **No**, and Per-Port.

▶South Bridge

The following South Bridge information will be 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 will provide complete legacy USB keyboard support for the operating systems that do not support legacy USB devices. The options are Disabled and **Enabled**..

▶Server ME Configuration

This feature displays the following system ME configuration settings.

- Operational Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1
- ME Firmware Status #2
  - Current State
  - Error Code

▶PCH SATA Configuration

SATA Controller

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

Configure SATA as

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

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

Aggressive Link Power Management

When this feature is set to Enable, the SATA AHCI controller manages the power usage of the SATA link. The controller will put the link to a low power state when the I/O is inactive for an extended period of time, and the power state will return to normal when the I/O becomes active. The options are **Disable** and Enable.

If the feature, Configure SATA as, is set to AHCI, the following features will become available for user's configuration:

SATA Port 0~ Port 7

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

- Model number of drive and capacity
- Software Preserve Support

Hot Plug (SATA Port 0~ Port 7)

Select Enabled to enable a SATA port specified by the user. The options are **Disable** and Enable.

Spin Up Device (SATA Port 0~ Port 7)

On an edge detect from 0 to 1, set this feature to allow the PCH to initialize the device. The options are **Disable** and Enable.

SATA Device Type (SATA Port 0~ Port 7)

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

If the feature, Configure SATA as, is set to RAID, the following features will become available for user's configuration:

SATA RSTe Boot Info

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

Aggressive Link Power Management

When this feature is set to Enable, the SATA AHCI controller manages the power usage of the SATA link. The controller will put the link to a low power state when the I/O is inactive for an extended period of time, and the power state will return to normal when the I/O becomes active. The options are **Disable** and Enable.

SATA RAID Option ROM/UEFI Driver

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~ Port 7

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

- Model number of drive and capacity
- Software Preserve Support

Hot Plug (SATA Port 0~ Port 7)

Select Enabled to enable a SATA port specified by the user. The options are **Disable** and Enable.

Spin Up Device (SATA Port 0~ Port 7)

On an edge detect from 0 to 1, set this feature to allow the PCH to initialize the device. The options are **Disable** and Enable.

SATA Device Type (SATA Port 0~ Port 7)

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

▶PCH sSATA Configuration

sSATA Controller

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

Configure sSATA as

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

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

Aggressive Link Power Management

When this feature is set to Enable, the SATA AHCI controller manages the power usage of the SATA link. The controller will put the link to a low power state when the I/O is inactive for an extended period of time, and the power state will return to normal when the I/O becomes active. The options are **Disable** and Enable.

If the feature, Configure sSATA as, is set to AHCI, the following features will become available for user's configuration:

sSATA Port 0~ Port 5

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

- Model number of drive and capacity
- Software Preserve Support

Hot Plug (sSATA Port 0~ Port 5)

Select Enabled to enable a SATA port specified by the user. The options are **Disable** and Enable.

Spin Up Device (sSATA Port 0~ Port 5)

On an edge detect from 0 to 1, set this feature to allow the PCH to initialize the device. The options are **Disable** and Enable.

sSATA Device Type (sSATA Port 0~ Port 5)

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

If the feature, Configure SATA as, is set to RAID, the following features will become available for user's configuration:

sSATA RSTe Boot Info

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

sSATA RAID Option ROM/UEFI Driver

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~ Port 5

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

- Model number of drive and capacity
- Software Preserve Support

Hot Plug (sSATA Port 0~ Port 5)

Select Enabled to enable a SATA port specified by the user. The options are **Disable** and Enable.

Spin Up Device (sSATA Port 0~ Port 5)

On an edge detect from 0 to 1, set this feature to allow the PCH to initialize the device. The options are **Disable** and Enable.

sSATA Device Type (sSATA Port 0~ Port 5)

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

▶PCIe/PCI/PnP Configuration

The following information will be displayed:

- PCI Bus Driver Version

PCI Devices Common Settings:

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

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

SR-IOV Support

Use this feature to enable or disable Single Root IO Virtualization 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 base memory size must be between 4032G to 4078G. The options are **56T**, 40T, 24T, 16T, 4T, 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.

PCI PERR/SERR Support

Select Enabled to activate PCI Error and System Error report handling. The options are Disabled and **Enabled**.

Maximum Read Request

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

MMCFG Base

Use this feature to select the default value for the PCI MMIO (Memory-Mapped IO) base address. The options are 1G, 1.5G, 1.75G, **2G**, 2.25G, and 3G.

NVMe Firmware Source

Use this feature to select the NVMe firmware to support booting. The options are **Vendor Defined Firmware** and AMI Native Support. The default option, **Vendor Defined Firmware**, is pre-installed on the drive and may resolve errata or enable innovative functions for the drive. The other option, AMI Native Support, is offered by the BIOS with a generic method.

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.

RSC-UMR-8 SLOT1 PCI-E x8 OPROM
RSC-UMR-8 M.2_PCIe OPROM

Select Disabled to deactivate the selected slot, Legacy to activate the slot in legacy mode, and EFI to activate the slot in EFI mode. The options are Disabled, **Legacy**, and EFI.

Onboard LAN Option ROM Type

Select an option to enable Option ROM support to boot the computer using a device specified by the user. The options are **Legacy** and EFI.

Onboard LAN1 Option ROM
Onboard LAN2 Option ROM

Use the above two features to select the type of device installed in a LAN port specified by the user for system boot. The default setting for Onboard LAN1 Option ROM is **PXE**, and the default setting for Onboard LAN2 Option ROM is **Disabled**.

Onboard NVMe1 Option ROM
Onboard NVMe2 Option ROM
Onboard NVMe3 Option ROM
Onboard NVMe4 Option ROM

Use the above four features to select the type of the device installed on an NVMe port specified by the user for system boot. The options are Disabled, Legacy, and **EFI**.

Onboard Video Option ROM

Select Legacy to boot the system using a legacy video device installed on the motherboard. The options are Disabled, **Legacy**, and EFI.

▶Network Stack Configuration

Network Stack

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

Ipv4 HTTP Support

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

Ipv6 PXE Support

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

Ipv6 HTTP Support

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

PXE boot wait time

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

Media detect count

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

▶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 the configure settings of Serial Port 1.

Serial Port 1

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

Device Settings

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

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options are **Auto**, (IO=3F8h; IRQ=4;), (IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), and (IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;).

▶Serial Port 2 Configuration

Serial Port 2 Configuration

This submenu allows the user the configure settings of Serial Port 2.

Serial Port 2

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

Device Settings

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

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), and (IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;).

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

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

▶Serial Port Console Redirection

COM1

Console Redirection

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

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

This feature allows the user 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.

SOL

Console Redirection

Select Enabled to enable console redirection support for a serial port specified by the user. 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

This feature allows the user 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 the 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 submenu 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 Management 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

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)

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 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 be displayed:

- **Active PCR banks**
- **Available PCR banks**

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending operation

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

Platform Hierarchy

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

Storage Hierarchy

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

Endorsement Hierarchy

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

PH Randomization

Use this feature to disable or enable Platform Hierarchy Randomization. The options are **Disabled** and Enabled.

TXT Support

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

▶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

If this feature is set to Enable, the certificate enrolled in the system will be deleted. The options are Enable and **Disable**.

▶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® Virtual RAID on CPU

This submenu displays the information of the Intel® VMD controllers as detected by the BIOS.

▶Intel® Optane(TM) DC Persistent Memory Configuration (Available when Apache Pass device plug-in)

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

Version: 1.0.0.3380

Select an action below.

Detected DIMMs:

This feature displays the number of DIMMs as detected by the system.

All DIMMs are healthy.

▶DIMMs

This feature configures and displays the information of a selected DCPMM.

Select a specific DIMM to view more information.

DIMMs on socket 0x0000:

▶DIMM ID 0x0001

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-0000115D**
DIMM handle	**0x0001**
DIMM physical ID	**0x0019**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x0000115D**
Part number	**NMA1XBD256GQS**
Socket	**0x0**
Memory controller ID	**0x0**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**
Subsystem device ID	**0x97A**
Device locator	**P1-DIMMA2**

Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P0_Node0_Channel0_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0000**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**
Package sparing capable	**1**
Package sparing enabled	**1**

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM ADR Command Received, DDRT Power Fail Command Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x0101

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-00000B35**
DIMM handle	**0x0101**
DIMM physical ID	**0x0021**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x00000B35**
Part number	**NMA1XBD256GQS**
Socket	**0x0**
Memory controller ID	**0x1**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID 0x97A

Device locator P1-DIMMD2

Subsystem revision ID 0x18

Interface format code 0x0301 (Non-Energy Backed Byte Addressable)

Manufacturing info valid 1

Manufacturing date 18-37

Manufacturing location 0xA2

Memory type Logical Non-Volatile Device

Memory bank label P0_Node1_Channel0_Dimm1

Data width label [b] 64

Total width [b] 72

Speed [MHz] 2666

Channel ID 0x0000

Channel position 1

Revision ID 0x0

Form factor [DIMM]

Manufacturer ID 0x8089

Controller revision ID B0 (0x0020)

Is new 0

Memory capacity 252.0 GiB

App Direct capacity 0 B

Unconfigured capacity 0 B

Inaccessible capacity 0 B

Reserved capacity 465.2 MiB

Peak power budget [mW] 20000

Avg power budget [mW] 15000

Max average power budget [mW] 10000

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x0011

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID **8089-A2-1837-00000B34**

DIMM handle **0x0011**

DIMM physical ID **0x001B**

Manageability state **[Manageable]**

Health state **[Healthy]**

Health state reason **None**

Capacity **252.4 GiB**

Firmware version **01.00.00.5127**

Firmware API Version **01.11**

Lock state **[Disabled]**

Staged firmware version **N/A**

Firmware update status **Update loaded successfully**

Manufacturer **Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number **0x00000B34**

Part number **NMA1XBD256GQS**

Socket **0x0**

Memory controller ID **0x0**

Vendor ID **0x8089**

Device ID **0x5141**

Subsystem vendor ID **0x8089**

Subsystem device ID 0x97A

Device locator P1-DIMMB2

Subsystem revision ID 0x18

Interface format code 0x0301 (Non-Energy Backed Byte Addressable)

Manufacturing info valid 1

Manufacturing date 18-37

Manufacturing location 0xA2

Memory type Logical Non-Volatile Device

Memory bank label P0_Node0_Channel1_Dimm1

Data width label [b] 64

Total width [b] 72

Speed [MHz] 2666

Channel ID 0x0001

Channel position 1

Revision ID 0x0

Form factor [DIMM]

Manufacturer ID 0x8089

Controller revision ID B0 (0x0020)

Is new 0

Memory capacity 252.0 GiB

App Direct capacity 0 B

Unconfigured capacity 0 B

Inaccessible capacity 0 B

Reserved capacity 465.2 MiB

Peak power budget [mW] 20000

Avg power budget [mW] 15000

Max average power budget [mW] 10000

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x0111

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-0000110C**
DIMM handle	**0x0111**
DIMM physical ID	**0x0023**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x000011C**
Part number	**NMA1XBD256GQS**
Socket	**0x0**
Memory controller ID	**0x1**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID	**0x97A**
Device locator	**P1-DIMME2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P0_Node1_Channel1_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0001**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x0021

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-00000B2E**
DIMM handle	**0x0021**
DIMM physical ID	**0x001D**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

If the feature, Show more details +, is set to Enable, the following will be displayed:

Serial number	**0x00000B2E**
Part number	**NMA1XBD256GQS**
Socket	**0x0**
Memory controller ID	**0x0**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID	**0x97A**
Device locator	**P1-DIMMC2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P0_Node0_Channel2_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0002**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x0121

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-000010AE**
DIMM handle	**0x0121**
DIMM physical ID	**0x0025**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

If the feature, Show more details +, is set to Enable, the following will be displayed:

Serial number	**0x000010AE**
Part number	**NMA1XBD256GQS**
Socket	**0x0**
Memory controller ID	**0x0**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID 0x97A

Device locator P1-DIMMF2

Subsystem revision ID 0x18

Interface format code 0x0301 (Non-Energy Backed Byte Addressable)

Manufacturing info valid 1

Manufacturing date 18-37

Manufacturing location 0xA2

Memory type Logical Non-Volatile Device

Memory bank label P0_Node1_Channel2_Dimm1

Data width label [b] 64

Total width [b] 72

Speed [MHz] 2666

Channel ID 0x0002

Channel position 1

Revision ID 0x0

Form factor [DIMM]

Manufacturer ID 0x8089

Controller revision ID B0 (0x0020)

Is new 0

Memory capacity 252.0 GiB

App Direct capacity 0 B

Unconfigured capacity 0 B

Inaccessible capacity 0 B

Reserved capacity 465.2 MiB

Peak power budget [mW] 20000

Avg power budget [mW] 15000

Max average power budget [mW] 10000

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

DIMMs on socket 0x0001:

▶DIMM ID 0x1001

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-0000111C**
DIMM handle	**0x1001**
DIMM physical ID	**0x0029**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x0000111C**
Part number	**NMA1XBD256GQS**
Socket	**0x1**
Memory controller ID	**0x0**
Vendor ID	**0x8089**
Device ID	**0x5141**

Subsystem vendor ID	**0x8089**
Subsystem device ID	**0x97A**
Device locator	**P2-DIMMA2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P1_Node0_Channel0_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0000**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**

Max average power budget [mW] 10000

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x1101

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-00001038**
DIMM handle	**0x1101**
DIMM physical ID	**0x0031**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x00001038**
Part number	**NMA1XBD256GQS**
Socket	**0x1**
Memory controller ID	**0x1**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID	**0x97A**
Device locator	**P2-DIMMD2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P1_Node1_Channel0_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0000**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x1011

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-00000AA5**
DIMM handle	**0x1011**
DIMM physical ID	**0x002B**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x00000AA5**
Part number	**NMA1XBD256GQS**
Socket	**0x1**
Memory controller ID	**0x0**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID	**0x97A**
Device locator	**P2-DIMMB2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P1_Node0_Channel1_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0001**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x1111

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-000000E3A**
DIMM handle	**0x1111**
DIMM physical ID	**0x0033**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x00000E3A**
Part number	**NMA1XBD256GQS**
Socket	**0x1**
Memory controller ID	**0x1**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID 0x97A

Device locator P2-DIMME2

Subsystem revision ID 0x18

Interface format code 0x0301 (Non-Energy Backed Byte Addressable)

Manufacturing info valid 1

Manufacturing date 18-37

Manufacturing location 0xA2

Memory type Logical Non-Volatile Device

Memory bank label P1_Node1_Channel1_Dimm1

Data width label [b] 64

Total width [b] 72

Speed [MHz] 2666

Channel ID 0x0001

Channel position 1

Revision ID 0x0

Form factor [DIMM]

Manufacturer ID 0x8089

Controller revision ID B0 (0x0020)

Is new 0

Memory capacity 252.0 GiB

App Direct capacity 0 B

Unconfigured capacity 0 B

Inaccessible capacity 0 B

Reserved capacity 465.2 MiB

Peak power budget [mW] 20000

Avg power budget [mW] 15000

Max average power budget [mW] 10000

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x1021

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-0000118C**
DIMM handle	**0x1021**
DIMM physical ID	**0x002D**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x0000118C**
Part number	**NMA1XBD256GQS**
Socket	**0x1**
Memory controller ID	**0x0**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID	**0x97A**
Device locator	**P2-DIMMC2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory bank label	**P1_Node1_Channel2_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0002**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶DIMM ID 0x1121

Press <Enter> and the following information regarding this DIMM will be displayed.

View settings or select an action below.

DIMM UID	**8089-A2-1837-00000BB2**
DIMM handle	**0x1211**
DIMM physical ID	**0x0035**
Manageability state	**[Manageable]**
Health state	**[Healthy]**
Health state reason	**None**
Capacity	**252.4 GiB**
Firmware version	**01.00.00.5127**
Firmware API Version	**01.11**
Lock state	**[Disabled]**
Staged firmware version	**N/A**
Firmware update status	**Update loaded successfully**
Manufacturer	**Intel**

Show more details +

Use this feature to display or hide additional information about this DIMM. The options are **Disabled** and Enabled.

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

Serial number	**0x00000B82**
Part number	**NMA1XBD256GQS**
Socket	**0x1**
Memory controller ID	**0x1**
Vendor ID	**0x8089**
Device ID	**0x5141**
Subsystem vendor ID	**0x8089**

Subsystem device ID	**0x97A**
Device locator	**P2-DIMMF2**
Subsystem revision ID	**0x18**
Interface format code	**0x0301 (Non-Energy Backed Byte Addressable)**
Manufacturing info valid	**1**
Manufacturing date	**18-37**
Manufacturing location	**0xA2**
Memory type	**Logical Non-Volatile Device**
Memory back label	**P1_Node1_Channel2_Dimm1**
Data width label [b]	**64**
Total width [b]	**72**
Speed [MHz]	**2666**
Channel ID	**0x0002**
Channel position	**1**
Revision ID	**0x0**
Form factor	**[DIMM]**
Manufacturer ID	**0x8089**
Controller revision ID	**B0 (0x0020)**
Is new	**0**
Memory capacity	**252.0 GiB**
App Direct capacity	**0 B**
Unconfigured capacity	**0 B**
Inaccessible capacity	**0 B**
Reserved capacity	**465.2 MiB**
Peak power budget [mW]	**20000**
Avg power budget [mW]	**15000**
Max average power budget [mW]	**10000**

Package sparing capable 1

Package sparing enabled 1

Package spares available 1

Configuration status [Valid]

SKU violation 0

ARS status [Completed]

Overwrite DIMM status [Not started]

Last shutdown time Fri Dec 21 17:29:23 UTC 2018

First fast refresh 0

Viral policy enable 0

Viral state 0

Latched Last shutdown status PM S5 Received, PMIC 12V/DDRT 1.2V Power Loss (PLI), Controller's FW State Flush Complete, Write Data Flush Complete, PM Idle Received

(**Note:** All DCPMM items and strings displayed on the BIOS screen are provided by Intel and will depend on the driver version.)

Unlatched last shutdown status Unknown

Security capabilities Encryption, Erase

Modes supported Memory Mode, App Direct

Boot status Success

AIT DRAM enabled [1]

Error injection enabled [0]

Media temperature injection enabled [0]

Software triggers enabled [0]

Software triggers enabled details None

Poison error injection counter 0

Poison error clear counter 0

Media temperature injection counter 0

Software triggers counter 0

Master Passphrase Enabled 0

▶Monitor health

Current non-critical threshold status

Controller temperature: within the non-critical threshold on all DIMMs.

Media temperature: within the non-critical threshold on all DIMMs.

Percentage remaining: within the non-critical threshold on all DIMMs.

Modify non-critical thresholds

Controller temperature [C]
Use this feature to set controller temperature in Celsius. (Min. = 20°C, Max. = 105°C)

Media temperature [C]
Use this feature to set media temperature in Celsius. (Min = 20°C, Max = 85°C)

Percentage remaining [%]
Use this feature to set spare capacity as a percentage. (Min = 1%, Max = 99%)

▶Apply changes

▶Back to main menu

▶Update firmware

Specify the firmware image to load on the DIMMs on the next system restart and select Update.

Current firmware version: 01.00.00.5127

Selected firmware version: None

File:
Press <Enter> and type in the file path relative to the root directory of the device containing the new firmware image file, such as "\firmware\newFirmware.bin".

Staged firmware version: N/A

▶Update

▶Back to main menu

▶Configure security

Specify the security settings on ALL the DIMMs.

State: [Disabled]
[Disabled, Frozen] will be displayed after pressing the following feature, Frozen lock.

Enable security
Use this feature to enable security by entering a new passphrase. Press <Enter> to type in a new passphrase with at least one character.

Secure erase
Use this feature to erase all persistent data. The options are Yes and No

Frozen lock
Use this feature to prevent further lock state changes until the next reboot.

▶Back to main menu

▶Configure data policy

Specify the data policy settings on ALL the DIMMs.

First fast refresh state: [Disabled] (or [Enabled])
Depending on the settings of the following feature, Enable/Disable first fast refresh, [Disabled] or [Enabled] will be displayed.

▶Enable/Disable first fast refresh

Use this feature to enable/disable the feature above, First fast refresh state.

▶Back to main menu

▶Back to main menu

▶Regions

Use this submenu to configure and display regions.

Current configuration

There are no regions defined in the system.

Memory allocation goal configuration

No goal configuration specified.

▶Create goal config

Use this submenu to create goal configuration of DIMM regions.

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

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

Reserved [%]:
Enter a value (0-100) to reserve a percentage of the requested DIMM capacity that will not be mapped into the system physical address space.

Memory Mode [%]:
Enter a value (0-100) to set the percentage of the total capacity to use in Memory Mode.

Persistent memory type:
Use this feature to select the type of the persistent memory capacity to create. The options are **App Direct** and App Direct Not interleaved.

Namespace Label version:
While creating goals, use this feature to display and modify the namespace label version to initialize. The options are 1.2 and 1.1.

▶Create goal config

Use this feature to create goal configuration on the selected target.

▶Back to Regions menu

▶Back to main menu

▶Back to main menu

▶Namespaces

Use this submenu to display, create, modify, and delete namespaces.

Select a namespace to view more information.

NamespaceID Name Health Status.

▶0x00000101 Healthy

Use this feature to display details for or modify selected namespace.

View details for or modify selected namespace.

UUID 66B9E696-0E38-47B3-81

5E-99FFAFC26A23

ID 0x00000101

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

Region 1

Health [Healthy]

Mode [None]

Block size [4096 B]

Units
Use this feature to change the units of the input namespace capacity. The options are B, MB, MiB, GB, GiB, TB, and TiB.

Capacity 125.0

Label version 1.2

▶Save

Use this feature to save current namespace.

▶Delete

Use this feature to delete current namespace.

▶Back to Namespaces

▶Back to main menu

▶Create namespace

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

Region ID

This feature displays the region ID on which to create namespace.

Mode

Use this feature to set namespace mode. The options are **None** and Sector. The option, None, is for raw access only. Set this feature to Sector to guarantee powerfail write automicity via a block translation table (BTT)

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 change the units of the input namespace capacity. The options are B, MB, MiB, GB, **GiB**, TB, and TiB.

Capacity

This feature displays the capacity of namespace.

▶Create namespace

Press <Enter> to create a namespace with the above configuration.

▶Back to Namespace

▶Back to main menu

▶Back to main menu (return to the main menu.)

▶Total capacity

The following information is displayed.

Total DCPMM resource allocation across the host server.

Raw capacity: 2.9 TiB

App Direct capacity: 0 B

Memory capacity: 2.9 TiB

Unconfigured capacity: 0 TiB

Inaccessible capacity: 0 TiB

Reserved capacity: 5.4 GiB

▶Back to main menu

▶Diagnostics

Perform diagnostic tests on DIMMS.

Choose diagnostics type:

Quick diagnostics

Select Enabled to perform quick diagnostics test. The options are Disabled and **Enabled**.

DIMM ID 0x0001

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x0101

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x1001

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x1101

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x0011

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x0111

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x1011

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x1111

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x0021

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x0121

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x1021

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

DIMM ID 0x1121

Select Enabled to enable the diagnostics procedure for this DIMM. The options are Disabled and **Enabled**.

Config diagnostics

Select Enabled to enable the platform configuration diagnostics test. The options are Disabled and **Enabled**.

FW diagnostics

Select Enabled to enable the firmware diagnostics test. The options are Disabled and **Enabled**.

Security diagnostics

Select Enabled to enable the security diagnostics test. The options are Disabled and **Enabled**.

▶Execute tests (execute selected diagnostic tests)

Press <Enter> to perform the selected diagnostic tests. The following information is displayed.

▶Back to Diagnostics

▶Back to main menu

TestName: Quick

State: Ok

Message:

The quick health check succeeded.

TestName: Config

State: Ok

Message:

The platform configuration check succeeded.

TestName: Security

State: Ok

Message:

The security check succeeded.

TestName: FW

State: Ok

Message:

The firmware consistency and settings check succeeded.

▶Back to main menu

▶Preferences

Use this submenu to display and/or modify user preferences.

View and/or modify user preferences.

Default DIMM ID:

Use this feature to view and/or modify the default display of DIMM identifiers. The options are **Handle** and UID.

Capacity units:

This feature is to view and/or modify the default units for displaying capacities. Use auto (x1024) or Auto_10 (x1000) to automatically select the best format. The options are **Auto**, Auto_10, B, MB, MiB, GB, GiB, TB, and TiB .

App Direct settings:

This feature is to view and/or modify the interleaving settings for creating App Direct capacity. The default setting is 4KB_4KB (Recommended).

App Direct granularity:

This feature is to view and/or modify the minimum App Direct granularity per DIMM. The options are **Recommended** and 1.

▶Back to main menu

▶Driver Health

This submenu displays the health status of the drivers and controllers as detected by the system. The following information is displayed.

▶Intel(R) DCPMM 1.0.0.3380 Driver Healthy

Intel(R) DCPMM Controller Healthy

Intel Persistent Memory DIMM 25 Controller Healthy

Intel Persistent Memory DIMM 33 Controller Healthy

Intel Persistent Memory DIMM 41 Controller Healthy

Intel Persistent Memory DIMM 49 Controller Healthy

Intel Persistent Memory DIMM 27 Controller Healthy

Intel Persistent Memory DIMM 35 Controller Healthy

Intel Persistent Memory DIMM 43 Controller Healthy

Intel Persistent Memory DIMM 51 Controller Healthy

Intel Persistent Memory DIMM 29 Controller Healthy

Intel Persistent Memory DIMM 37 Controller Healthy

Intel Persistent Memory DIMM 45 Controller Healthy

Intel Persistent Memory DIMM 53 Controller Healthy

▶Intel(R) DCPMM 1.0.0.3380 HII Driver Healthy

Controller 665c5c98 Child 0 Healthy

▶Intel(R) 10GbE Driver 7.0.19 x64 Healthy

Controller 63f38f18 Child 0 Healthy

Intel(R) Ethernet Controller 10 Gigabit X540-AT2 Healthy

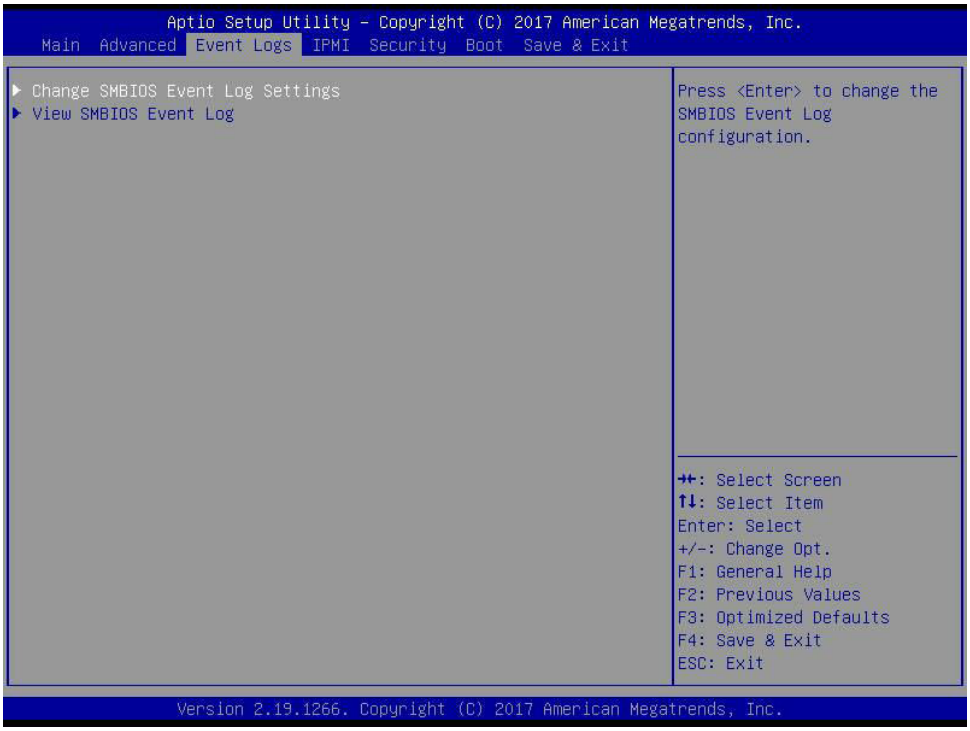
Controller 63f37398 Child 0 Healthy

Intel(R) Ethernet Controller 10 Gigabit X540-AT2 Healthy

▶Intel(R) PRO/1000 8.5.21 PCI-E Healthy

4.4 Event Logs

Use this feature to configure the Event Log settings.



▶Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

Erase Event Log

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

When Log is Full

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

SMBIOS Event Log Standard Settings

Log System Boot Event

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

MECI

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

METW

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

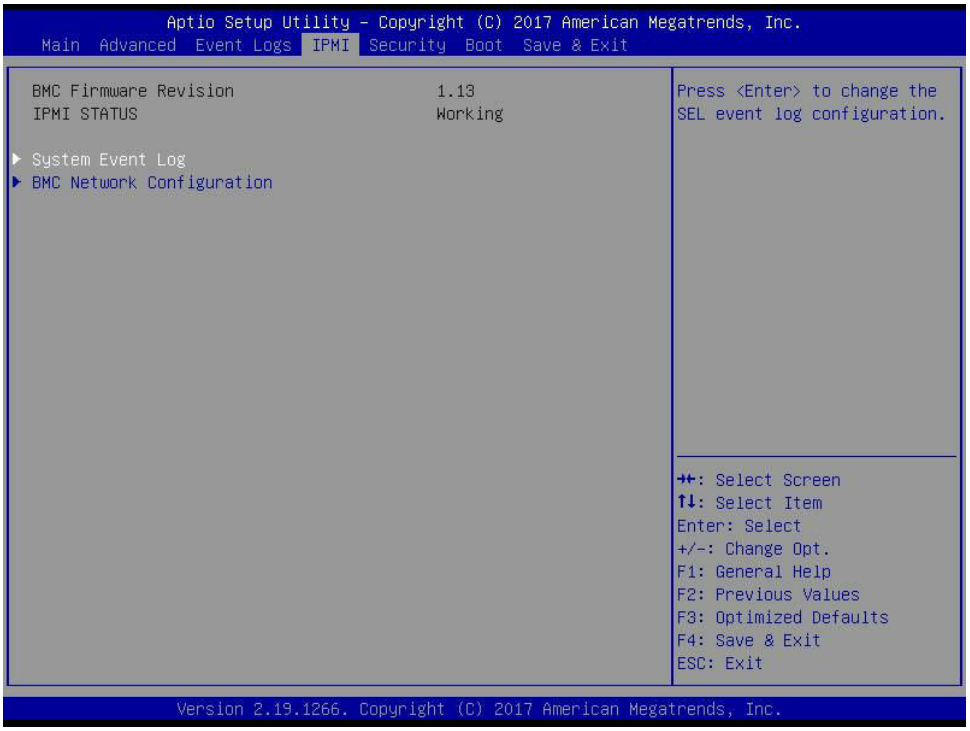
Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

▶View SMBIOS Event Log

This section displays the contents of the SMBIOS Event Log.

4.5 IPMI

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



BMC Firmware Revision

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

IPMI STATUS (Baseboard Management Controller)

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

▶System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

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

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

▶BMC Network Configuration

BMC Network Configuration

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 **Shared LAN**.

Update IPMI LAN Configuration

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

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

Configuration Address Source

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

This feature displays the current configuration address for this computer.

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., 172.31.0.1).

VLAN

Use this feature to enable or disable the IPMI VLAN function. The options are **Disable** and Enable.

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

VLAN ID

Use this feature to enter the VLAN ID. The default setting is **0**.

Configure IPV6 support

Lan channel 1

IPV6 Support

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

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

Configuration Address Source

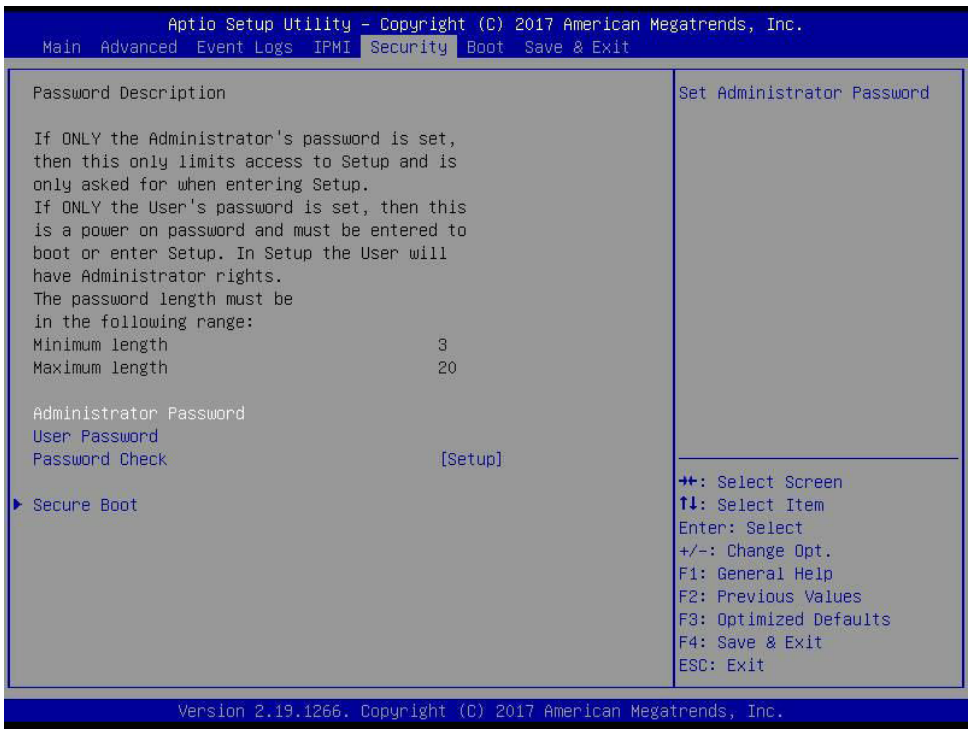
This feature allows the user to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol)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

The following information is displayed:

- Current Configuration Address source
- Station IPV6 address
- Prefix Length
- IPV6 Router1 IP Address
- IPV6 address status
- IPV6 DHCP Algorithm

4.6 Security

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



Administrator Password

Press Enter 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.

User Password

Press Enter 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 bootup or upon entering the BIOS Setup utility. The options are **Setup** and Always.

▶Secure Boot

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

- System Mode
- Secure Boot
- Vendor Keys

Secure Boot

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

Secure Boot Mode

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

CSM Support

Select Enabled to support the EFI Compatibility Support Module (CSM), which provides compatibility support for traditional legacy BIOS for system boot. 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.

Provision Factory Defaults

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

▶Enroll all Factory Default Keys

Select Yes to install all default secure keys set by the manufacturer. The options are **Yes** and No.

▶Enroll Efi Image

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

▶Save all Secure Boot variables

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

Secure Boot variable: Size/Key#/Key Source

▶Platform Key (PK)

This feature allows the user to configure the settings of the platform keys. Select Update to load the new platform keys (PK) from the manufacturer's defaults. The options are **Details**, Export, Update, and Delete.

▶Key Exchange Keys (KEK)

Select Update to load the KEK from the manufacturer's defaults. Select Append to add the KEK from the manufacturer's defaults list to the existing KEK. The options are **Details**, Export, Update, Append, and Delete.

▶Authorized Signatures

Authorized Signature Database (DB) contains authorized signing certificates and digital signatures. Select Update to load the DB from the manufacturer's defaults. Select Append to add the database from the manufacturer's defaults to the existing DB. The options are **Details**, Export, Update, Append, and Delete.

▶Forbidden Signatures

Forbidden Signature Database (DBX) contains forbidden certificates and digital signatures. Select Update to load the DBX from the manufacturer's defaults. Select Append to add the DBX from the manufacturer's defaults to the existing DBX. The options are **Details**, Export, Update, Append, and Delete.

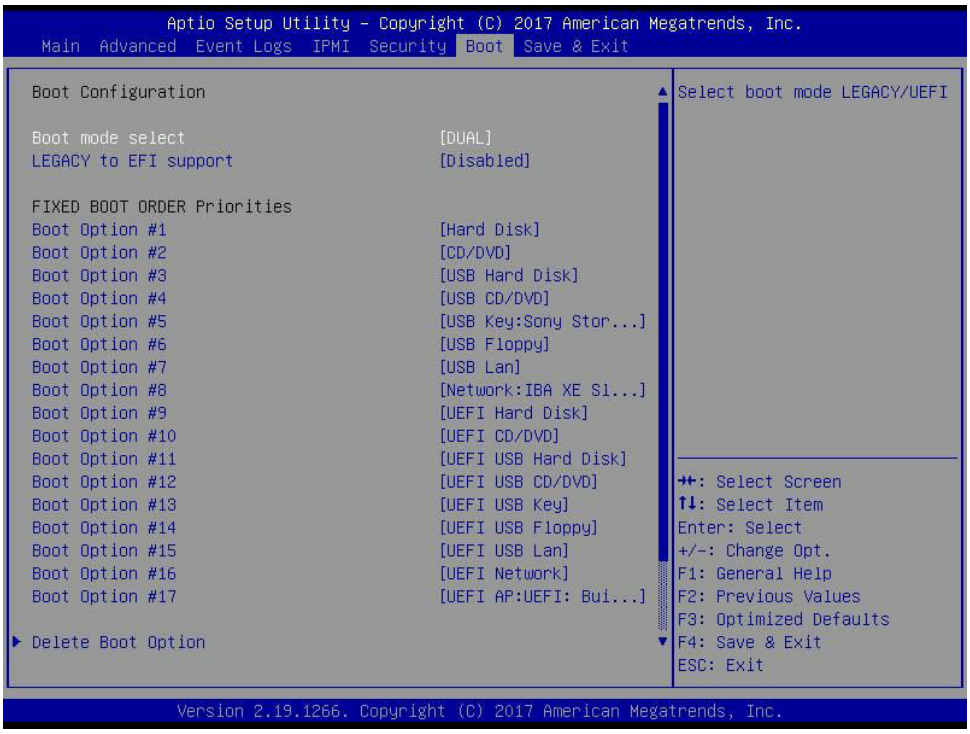
▶Authorized TimeStamps

Select Update to load the Authorized Timestamp Database (DBT) from the manufacturer's defaults. Select Append to add the DBT from the manufacturer's defaults list to the existing DBT. The options are **Details**, Export, Update, Append, and Delete.

▶OsRecovery Signatures

Select Update to load the OsRecovery Signatures Database (DBR) from the manufacturer's defaults. Select Append to add the DBR from the manufacturer's defaults list to the existing DBR. The options are **Details**, Export, Update, Append, and Delete.

4.7 Boot



Use this feature to configure Boot Settings:

Boot mode select

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

LEGACY to EFI support

Use this feature to enable the EFI boot support. The options are **Disabled** and Enabled.

FIXED BOOT ORDER Priorities

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

If the feature above is set to Legacy/UEFI/Dual, the following will be displayed:

- Legacy/UEFI/Dual Boot Order #1
- Legacy/UEFI/Dual Boot Order #2
- Legacy/UEFI/Dual Boot Order #3
- Legacy/UEFI/Dual Boot Order #4
- Legacy/UEFI/Dual Boot Order #5

- Legacy/UEFI/Dual Boot Order #6
- Legacy/UEFI/Dual Boot Order #7
- Legacy/UEFI/Dual Boot Order #8
- UEFI/Dual Boot Order #9
- Dual Boot Order #10
- Dual Boot Order #11
- Dual Boot Order #12
- Dual Boot Order #13
- Dual Boot Order #14
- Dual Boot Order #15
- Dual Boot Order #16
- Dual Boot Order #17

▶Delete Boot Option

Use this feature to remove a pre-defined boot device from which the system will boot during startup. The options are **Select one to Delete** and UEFI: Built-in EFI Shell.

▶UEFI Application Boot Priorities

This feature allows the user to specify which UEFI devices are boot devices.

Boot Option #1

The options are **UEFI: Built-in EFI Shell** and Disabled.

▶Network Drive BBS Priorities

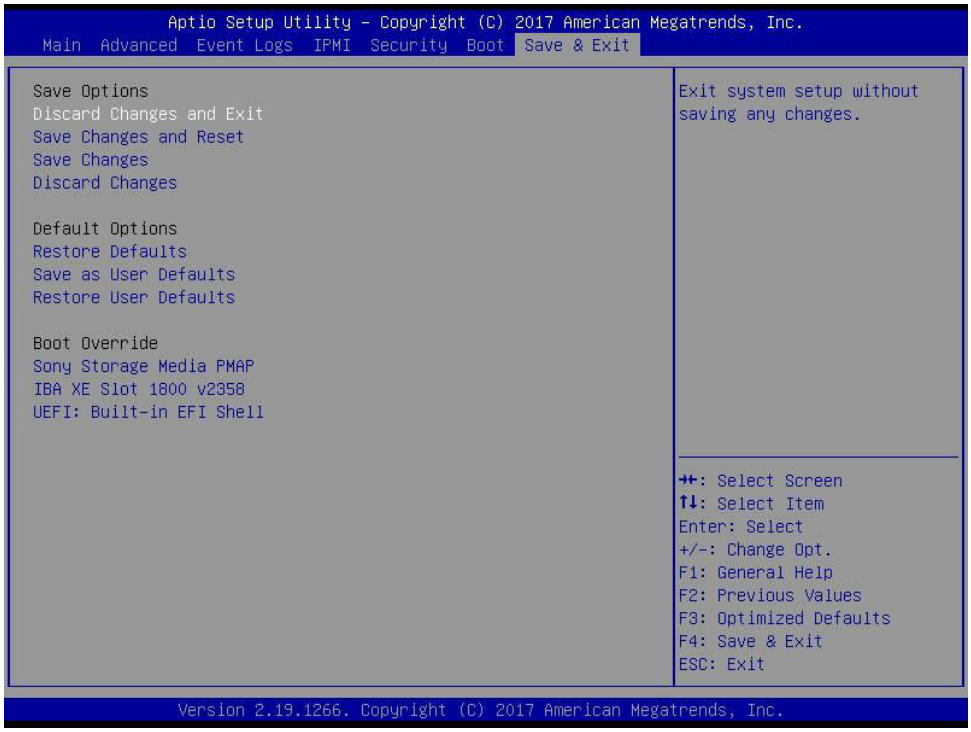
This feature allows the user to specify which available network drives are boot devices.

Boot Option #1

The options are **IBA XE Slot 1800 v2358** 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 quit the BIOS Setup without making any permanent changes to the system configuration, and reboot the computer. Select Discard Changes and Exit from the Exit menu and press <Enter>.

Save Changes and Reset

After completing the system configuration changes, select this option to save the changes you have made. This will reset (reboot) the system.

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 and return to the AMI BIOS utility Program.

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

Default Options

Restore Defaults

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

Save As User Defaults

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

Restore User Defaults

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

Boot Override

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

Appendix A

BIOS Codes

A.1 BIOS Error POST (Beep) Codes

During the POST (Power-On Self-Test) process, which is performed each time the system is powered on, system errors may be detected.

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

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

The fatal errors are usually communicated through repeated patterns of audible beeps. Each pattern of audible beeps listed below corresponds to its respective error.

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

A.2 Additional BIOS POST Codes

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

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

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

Appendix B

Software

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

B.1 Microsoft Windows OS Installation

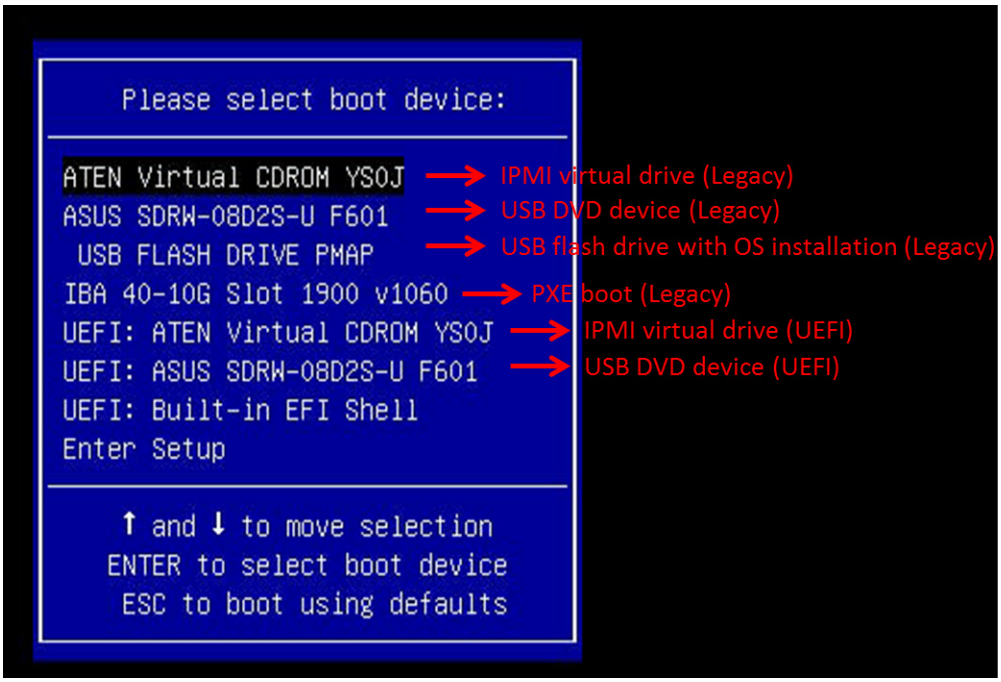
If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at www.supermicro.com/support/manuals.

Installing the OS

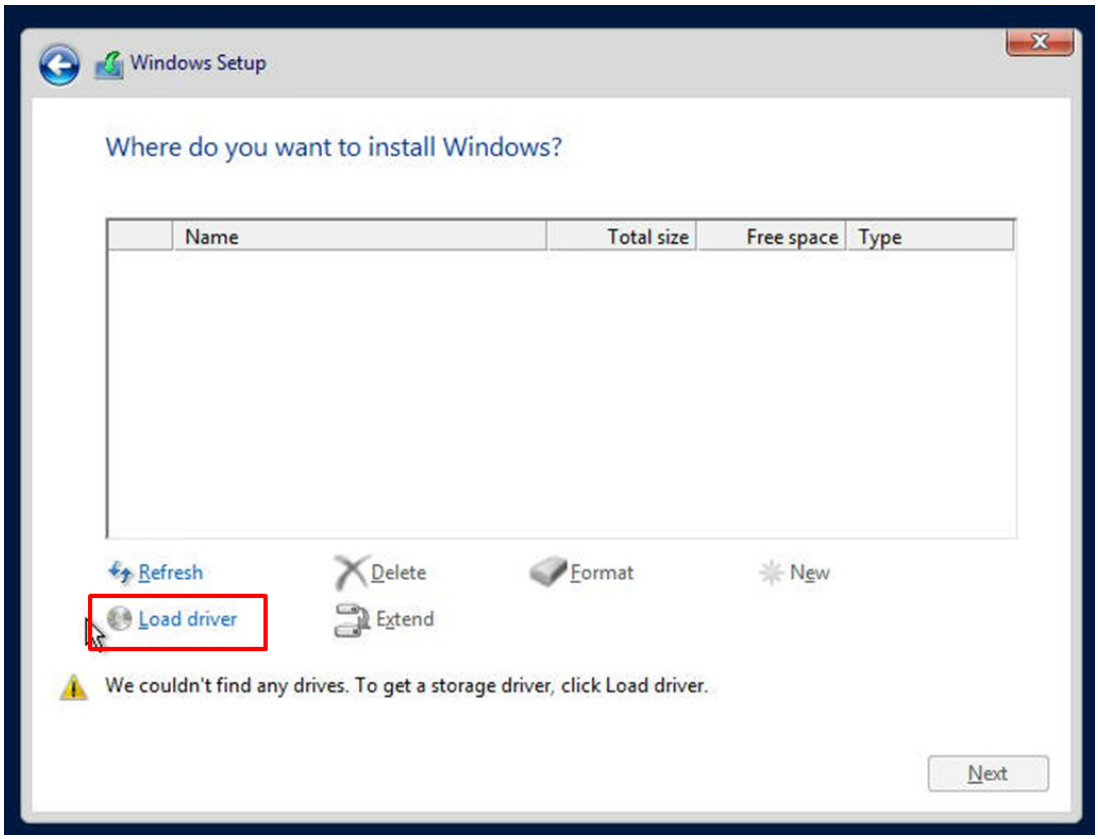
1. Create a method to access the MS Windows installation ISO file. That might be a DVD, perhaps using an external USB/SATA DVD drive, or a USB flash drive, or the IPMI KVM console.

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

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



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



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

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

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

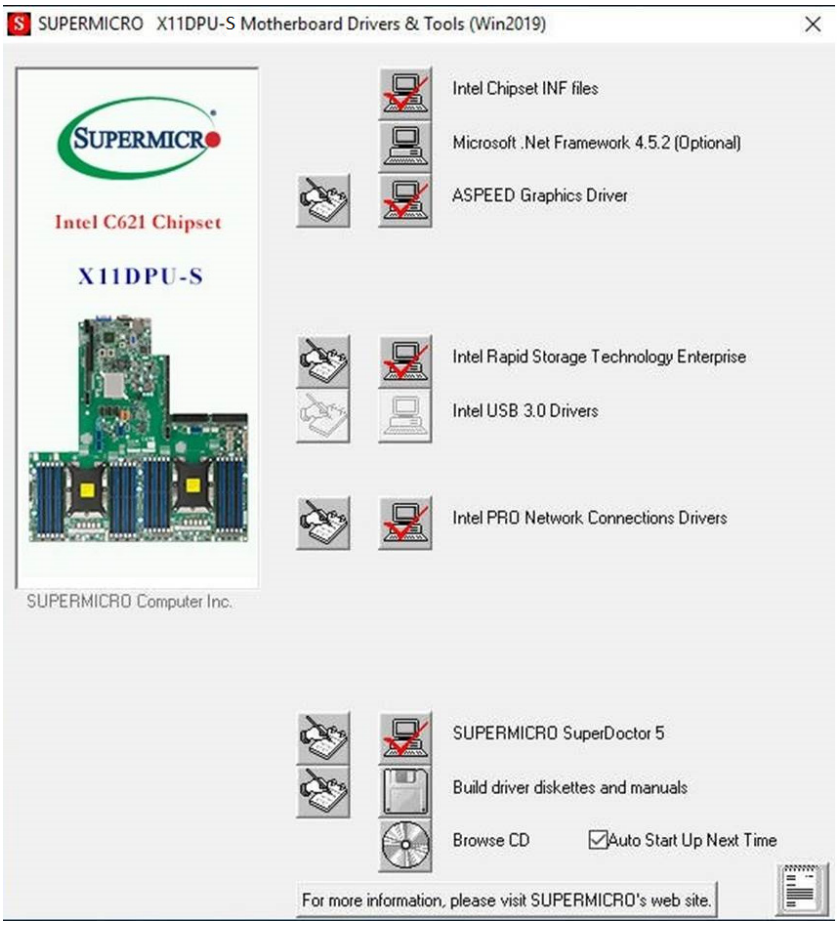
B.2 Driver Installation

The Supermicro website that contains drivers and utilities for your system is at https://www.supermicro.com/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.



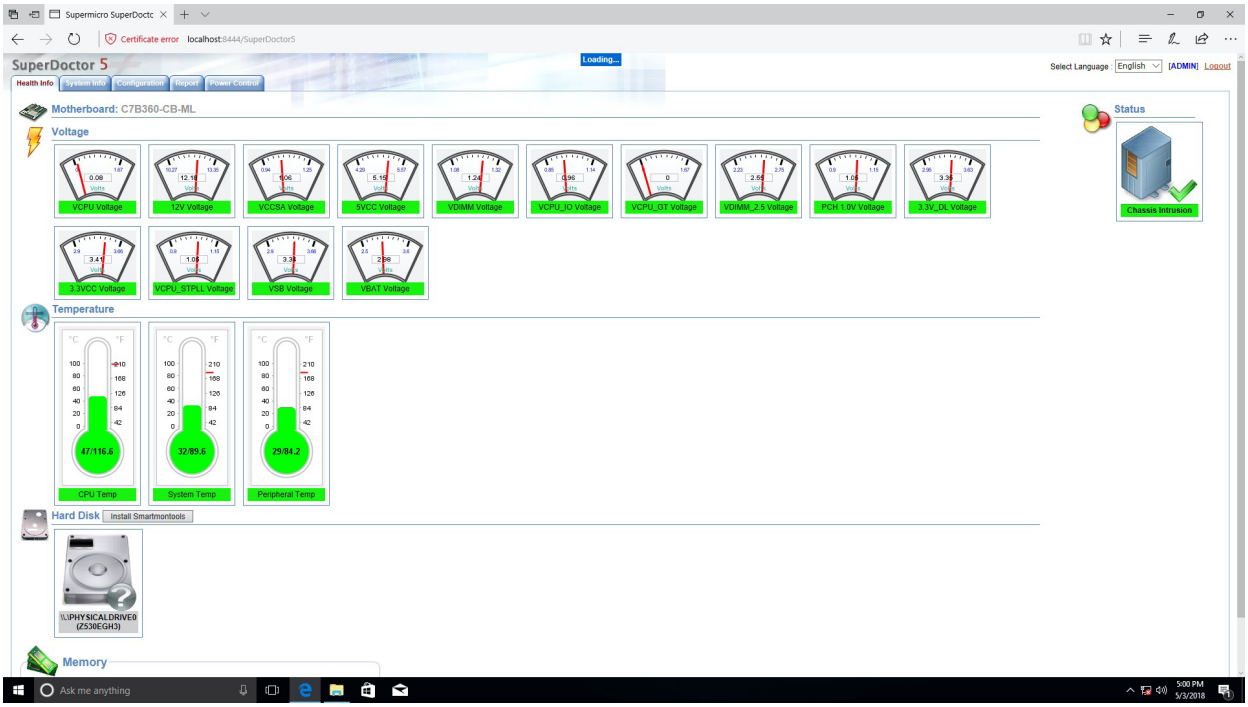
Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to the bottom) one at a time. **After installing each item, you must re-boot the system before moving on to the next item on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

B.3 SuperDoctor® 5

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

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

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



B.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.

B.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 C

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 استبدال البطارية بطريقة غير صحيحة فعليك استبدال البطارية
فقط بنفس النوع أو ما يعادلها كما أوصت به الشركة المصنعة
تخلص من البطاريات المستعملة وفقا لتعليمات الشركة الصانعة

경고!

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

Waarschuwing

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

Product Disposal

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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

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

يجب فصل النظام من جميع مصادر الطاقة وإزالة سلك الكهرباء من وحدة امداد

경고!

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

Waarschuwing

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

Appendix D

UEFI BIOS Recovery

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

D.1 Overview

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

D.2 Recovering the UEFI BIOS Image

A UEFI BIOS flash chip consists of a recovery BIOS block and a main BIOS block (a main BIOS image). The recovery block contains critical BIOS codes, including memory detection and recovery codes for the user to flash a healthy BIOS image if the original main BIOS image is corrupted. When the system power is 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 D.3 for BIOS recovery when the main BIOS block crashes.

Note 2: If the recovery instructions in Section D.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.

D.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.

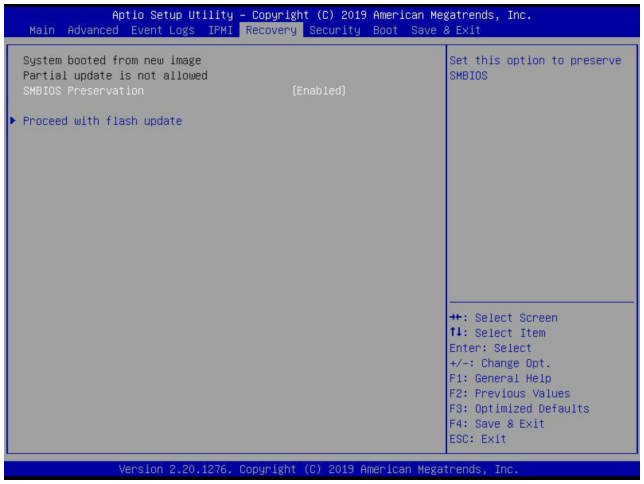
To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below.

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.

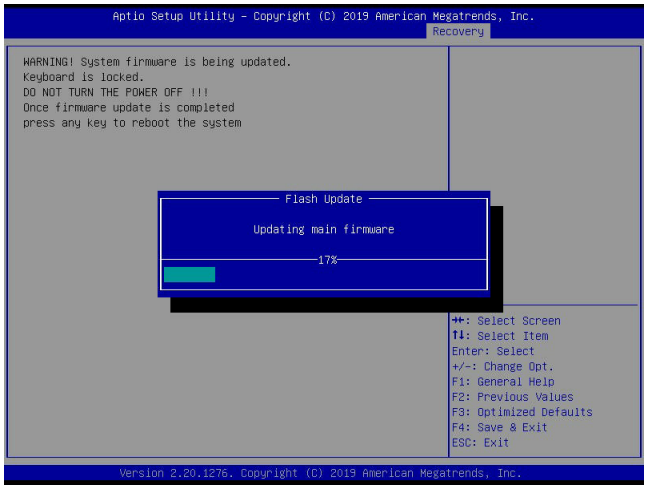
5. After locating the SUPER.ROM file, the system will enter the BIOS Recovery menu as shown below.



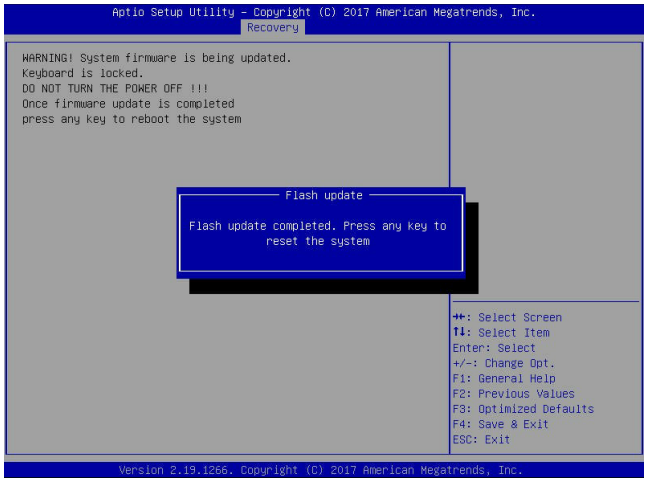
Note: At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

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*.

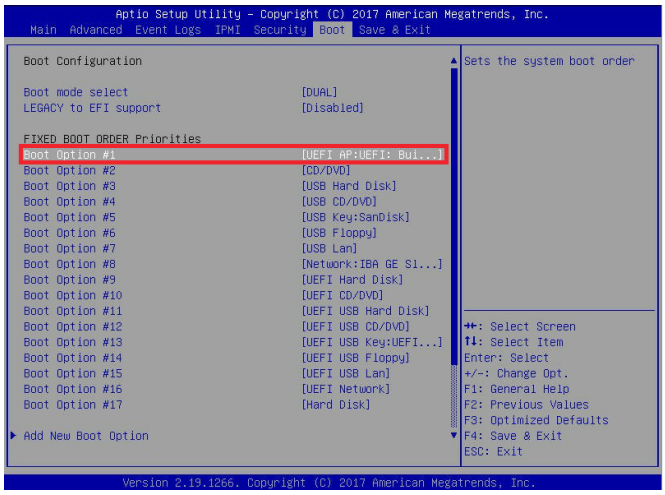


7. After the BIOS recovery process is complete, press any key to reboot the system.

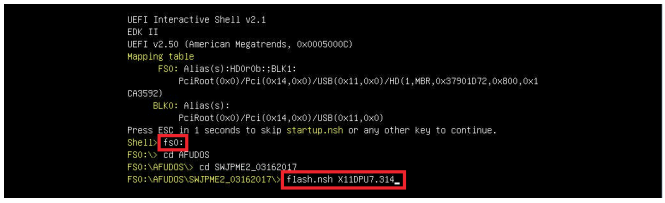


Note: It is recommended that you update your BIOS after BIOS recovery. Please refer to Chapter 3 for BIOS update instructions.

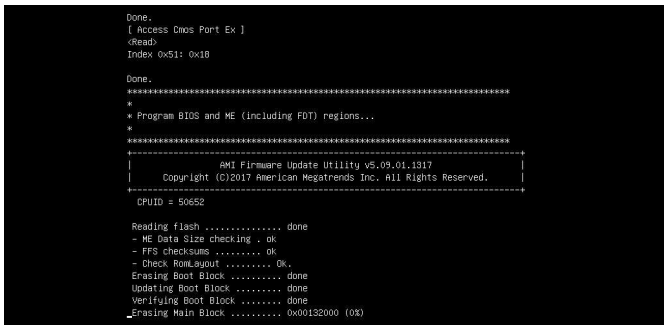
8. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the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



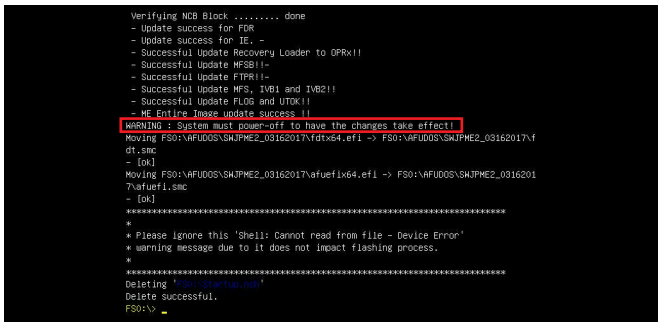
9. When the UEFI Shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier in Step 2. Enter flash.nsh BIOSname#.### at the prompt to start the BIOS update process.



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 E

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 E.1 section provides instructions on how to access the All Intel VMD Controller menu. The E.2 section provides instructions on how to configure RAID settings. The E.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.

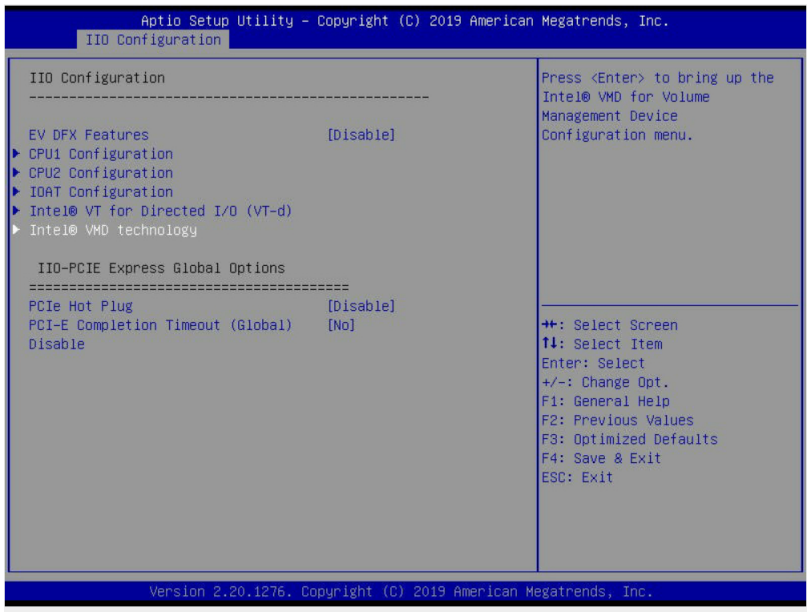
E.1 All Intel VMD Controllers Menu

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.

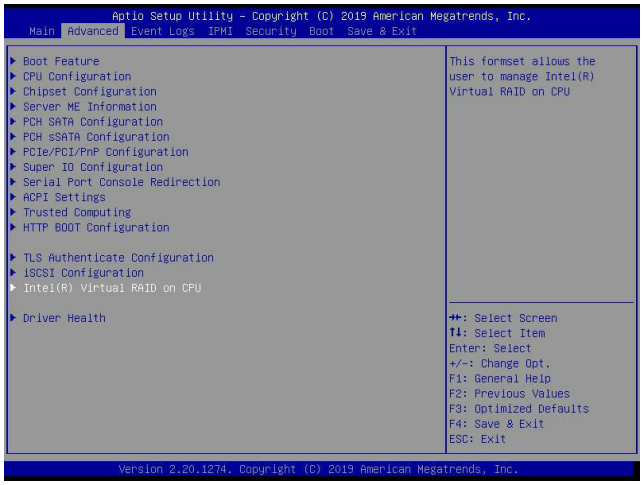
10. Repeat Step 8 ~ Step 9 to select and enable all the PCI slots of your choice for VMD support.

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,

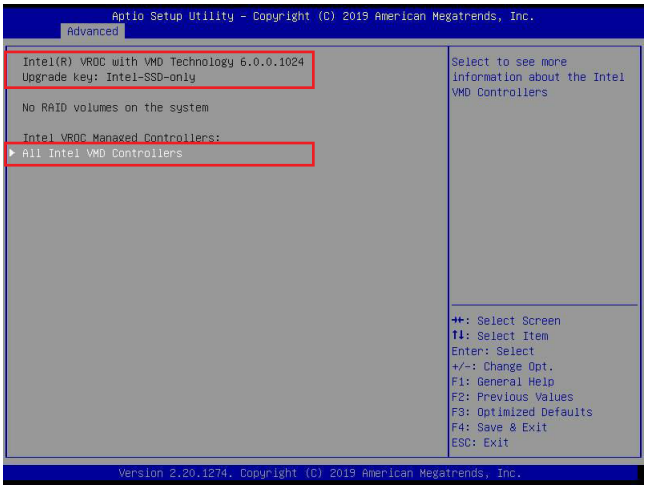
12. Press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility.

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

13. Navigate to the Advanced tab.



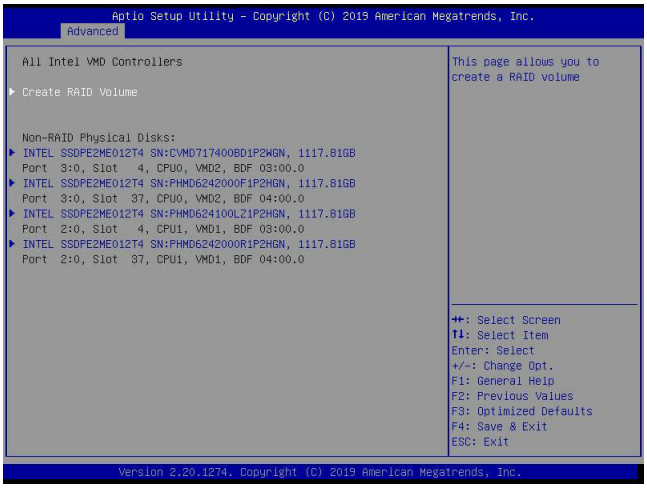
14. Use the arrow keys to select Intel(R) Virtual RAID on CPU and press <Enter> to access the menu items. The following screen will appear showing that the feature "**All Intel VMD Controllers**" has become available.



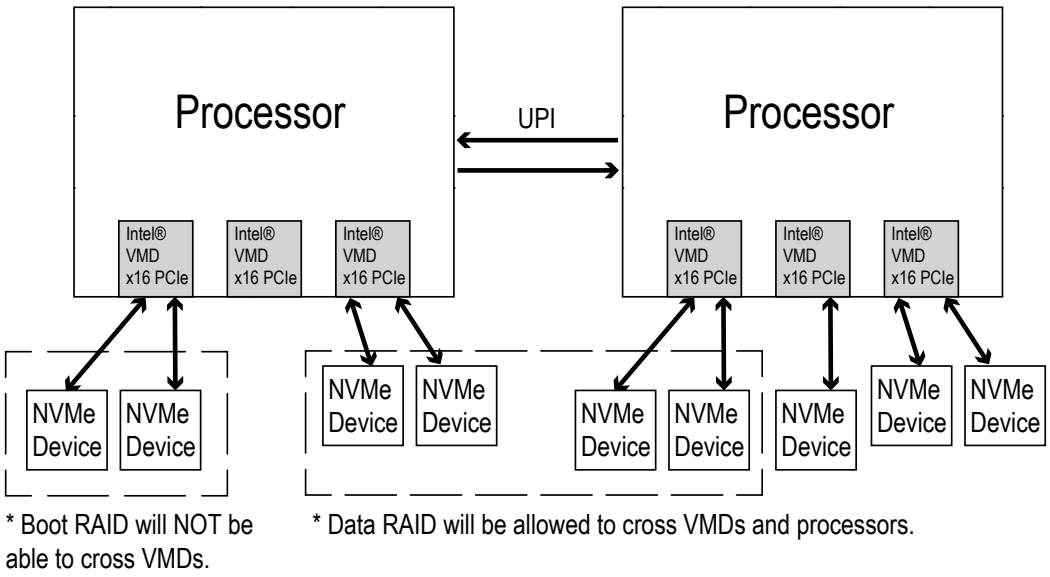
Note 1: The license and header (on the motherboard) for Intel® VROC hardware key are required. Also, be sure the version of Intel® Rapid Storage Technology enterprise (Intel® RSTe) VROC utility is 5 or above (look for Intel(R) VROC with VMD Technology x.x.x.xxxx shown on the screen).

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.

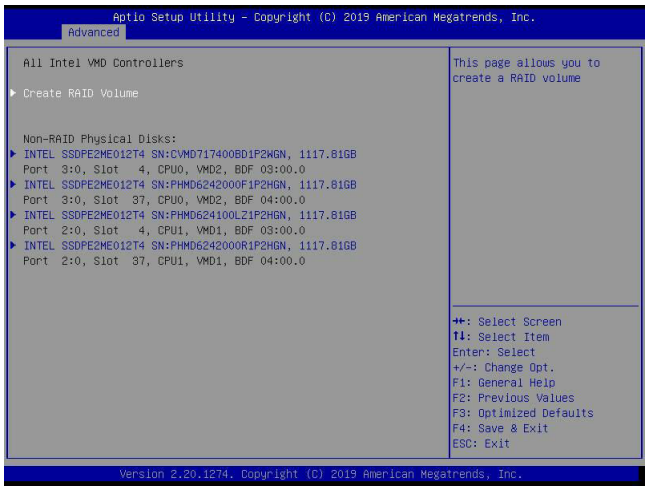


Note : A single Intel® VMD supported processor supplies 48 PCIe lanes and contains three Intel® VMD controllers (domains). Refer to the following illustration for more information.



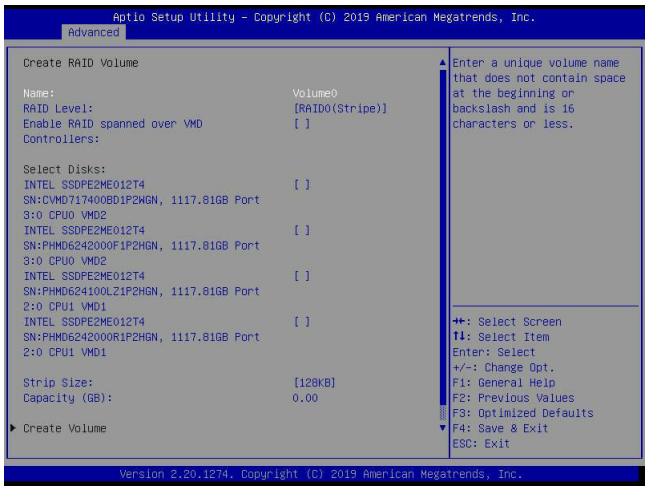
E.2 Configuring RAID Settings

Follow the instructions stated in the E.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.



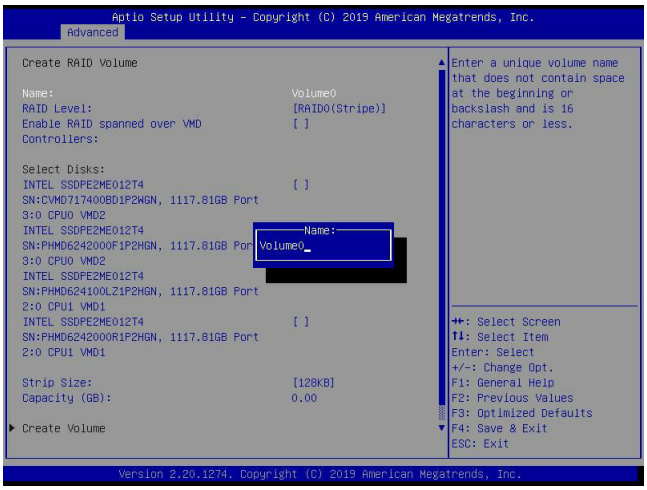
To Create a RAID Volume

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

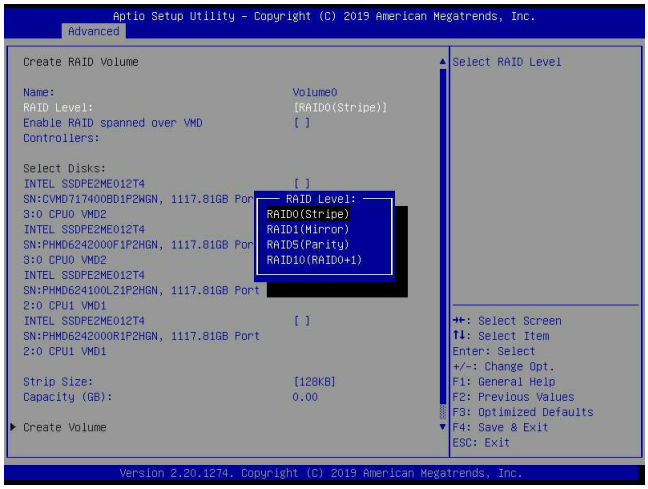
From the **Create RAID Volume** submenu as shown on the previous screen, use the arrow keys to select **Name** and press <Enter>, and the following screen will display.



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).

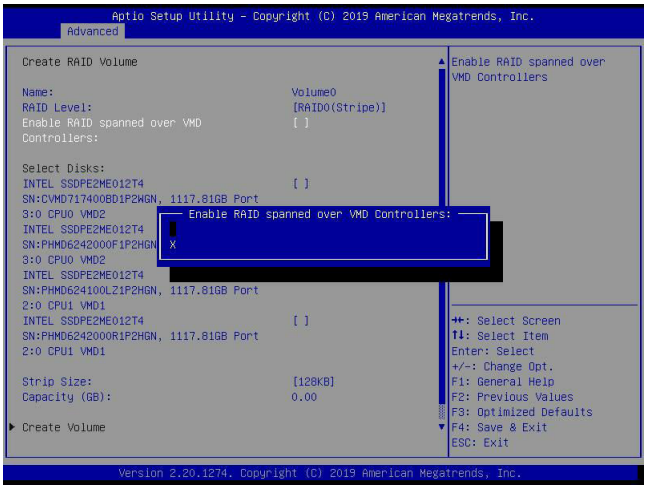
Note 1: The RAID level(s) displayed is(are) based on the number of NVMe devices connected to the system.

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.

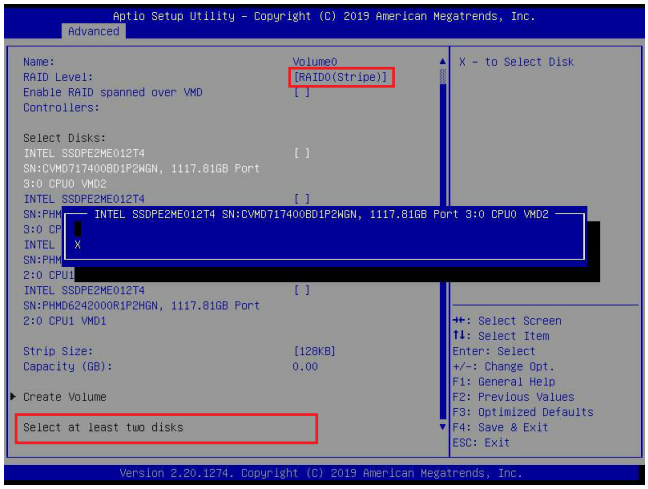


Enter a desired setting for your RAID volume in the pop-up menu. The options are **(not selected)** and X (selected). Please set this feature to X if the RAID level you selected earlier from Step 3 will cross VMD domains.

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

To Select Disks for the RAID Volumes

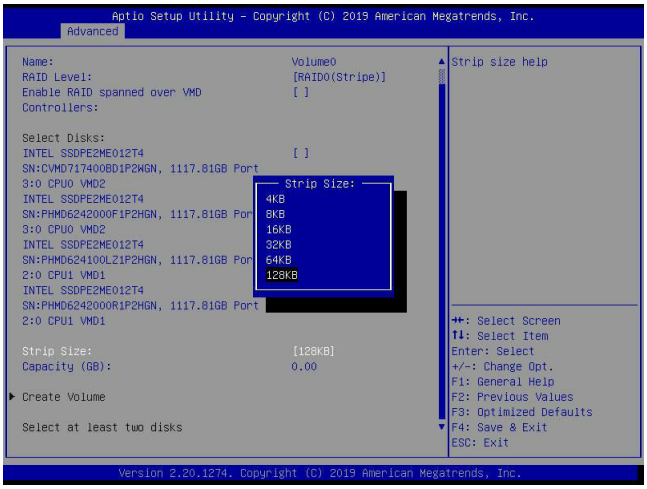
From the **Create RAID Volume** submenu, use the arrow keys to highlight **Select Disk:** and press <Enter>. The following screen will display.



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.

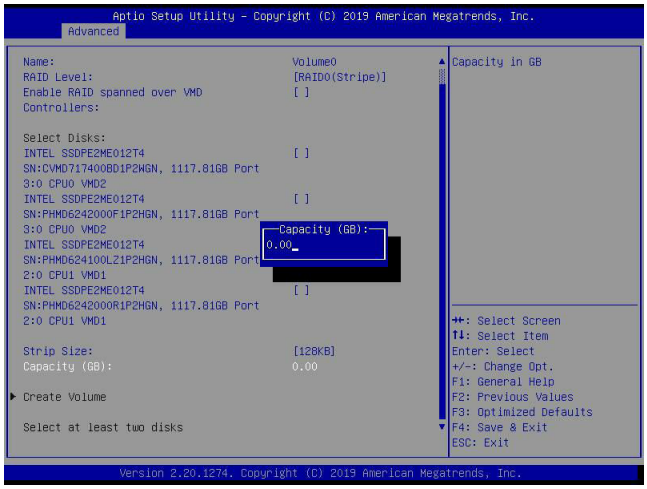


From the pop-up menu as shown above, select the desired RAID strip size for your RAID volume and press <Enter>. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**.

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

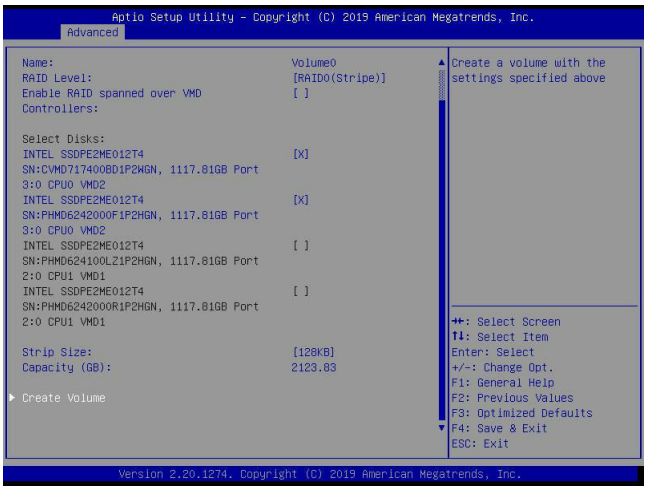
From the **Create RAID Volume** submenu, use the arrow keys to select **Capacity (GB):** and press <Enter>. The following screen will display.



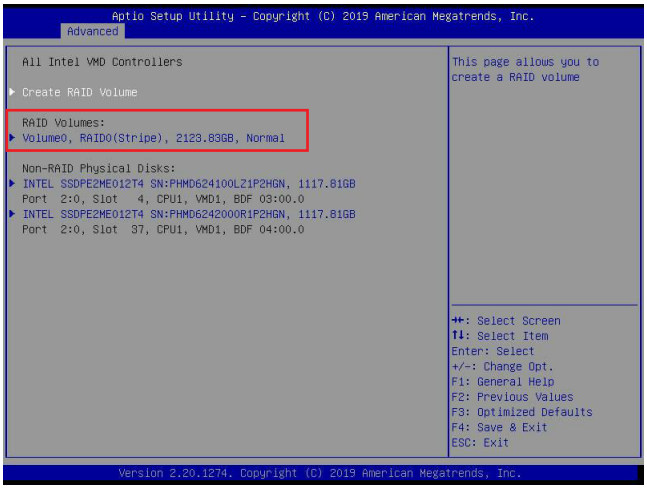
Enter the desired RAID capacity (in GB) in the pop-up menu to set the capacity for your RAID volume.

To Create Volumes

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

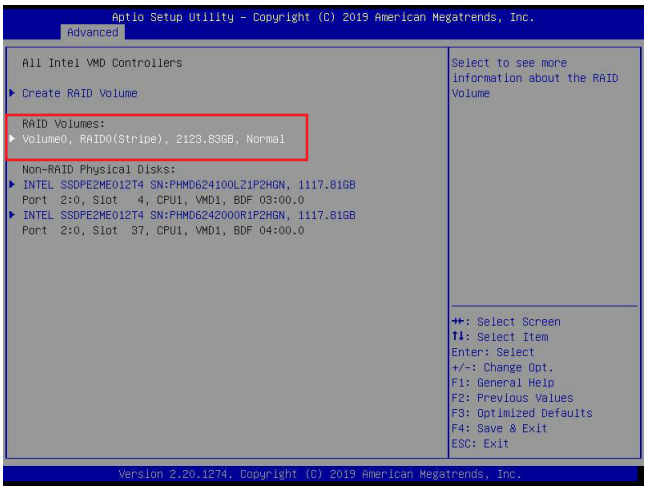


After selecting **Create Volume**, press <Enter>. The following screen will appear and display RAID volumes as shown below.



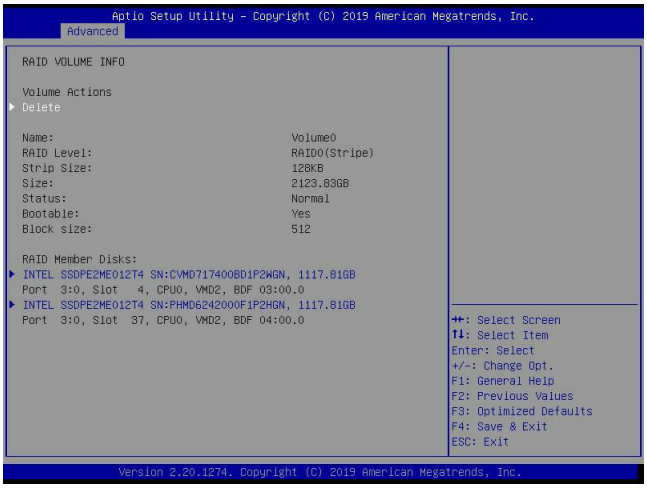
To Display RAID Volumes

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



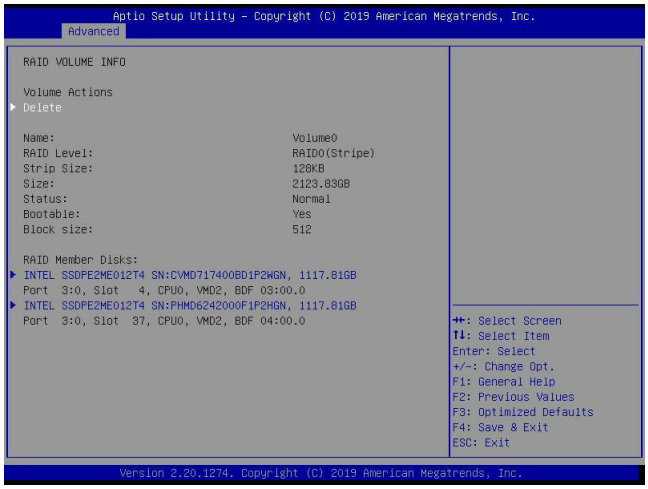
To Display RAID VOLUME Information

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

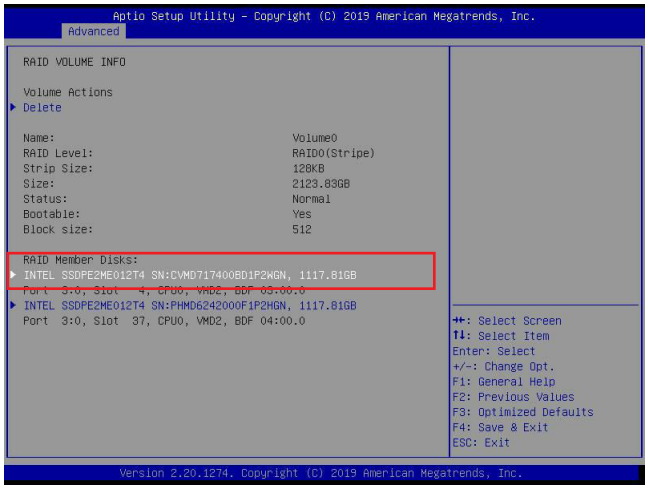
On the **RAID VOLUME INFO** menu, use the arrow keys to select Delete and press <Enter> to delete the RAID volume you have selected.



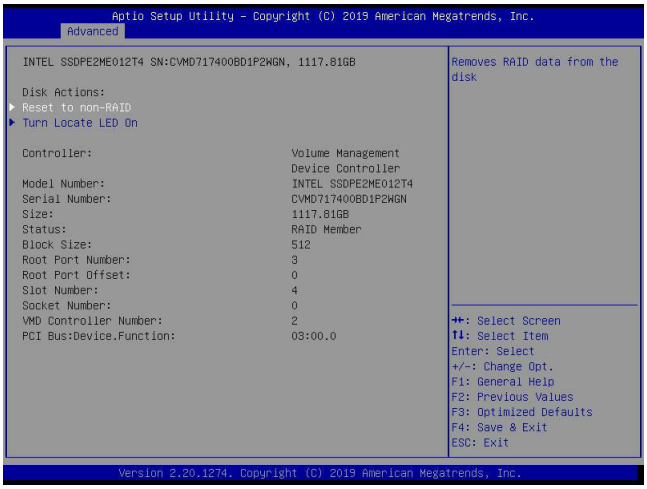
The following screen will appear to confirm if you want to delete the RAID Volume. Select Yes to delete the RAID Volume. The options are **Yes** and No.

To Reset the RAID Volume to non-RAID

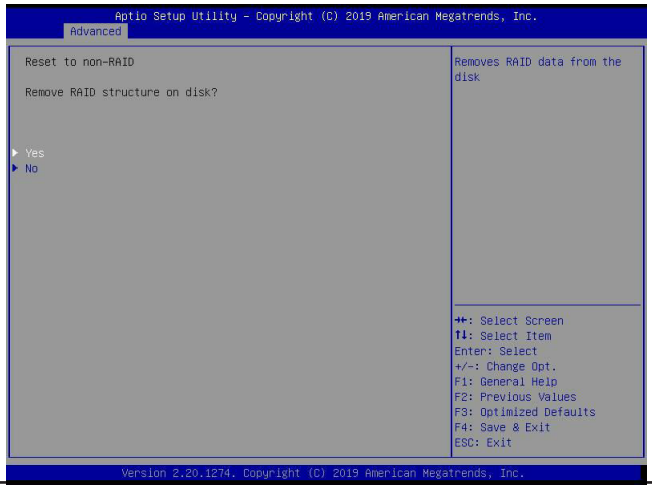
On the **RAID VOLUME INFO** submenu shown on the bottom screen of page 194, select the desired NVMe device from the list of RAID Member Disks and press <Enter> as shown below.



Select **Reset to Non-RAID** from the screen below and press <Enter> to remove RAID data from the selected NVMe device.

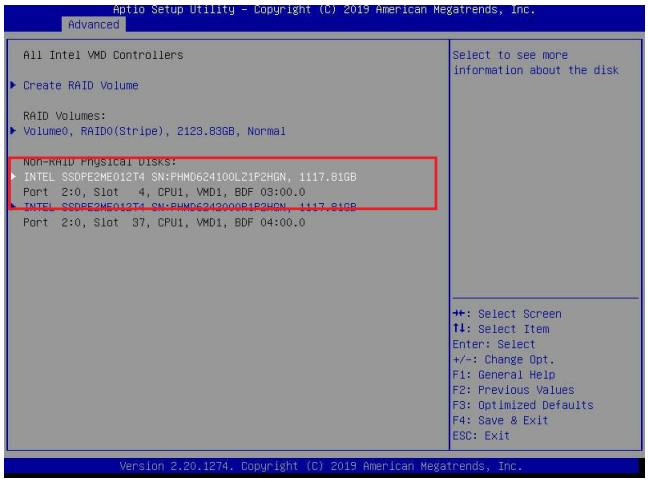


When the following screen appears, select Yes to confirm that you want to set the selected NVMe device to non-RAID. The options are **Yes** and No.

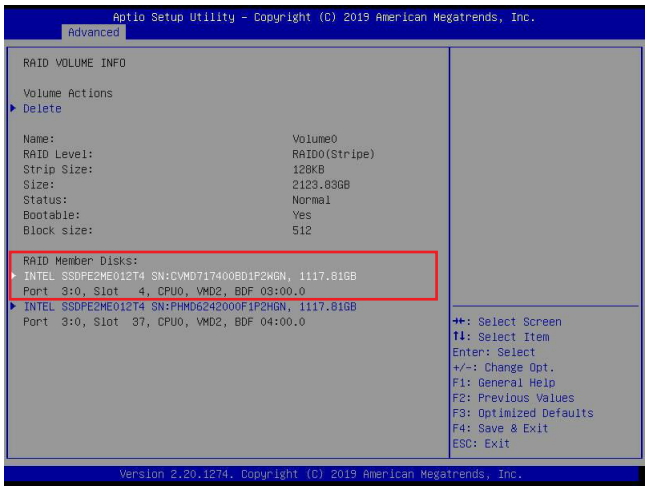


To Turn on the Disk Locator LED

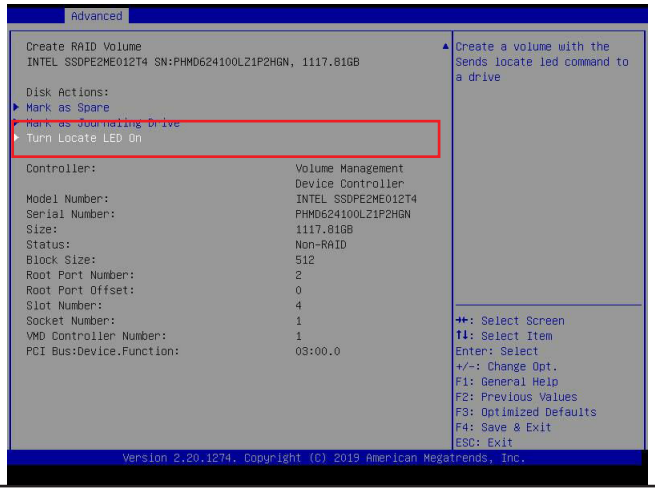
Follow the instructions stated in the E.1 section to access the **All Intel VMD Controllers** menu. When the following screen displays, select a non-RAID physical disk to turn on the disk locator LED to locate a selected device.



You can also select a RAID member disk to locate the selected device.

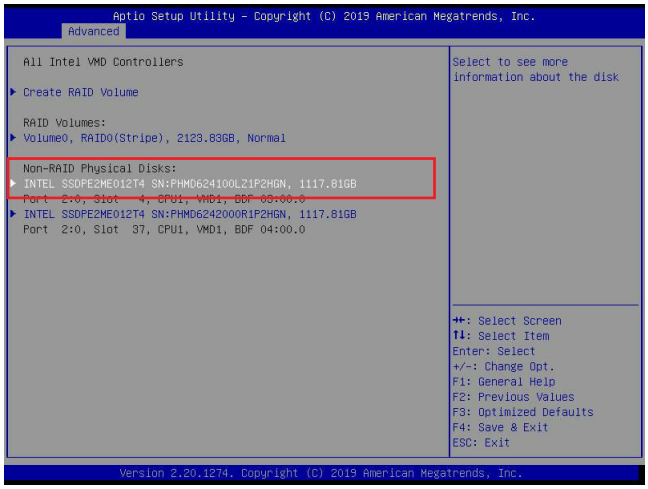


When the following screen appears, use the arrow keys to select **Turn Locate LED On**. Press <Enter> to turn on the locator LED to show the location of the selected device.

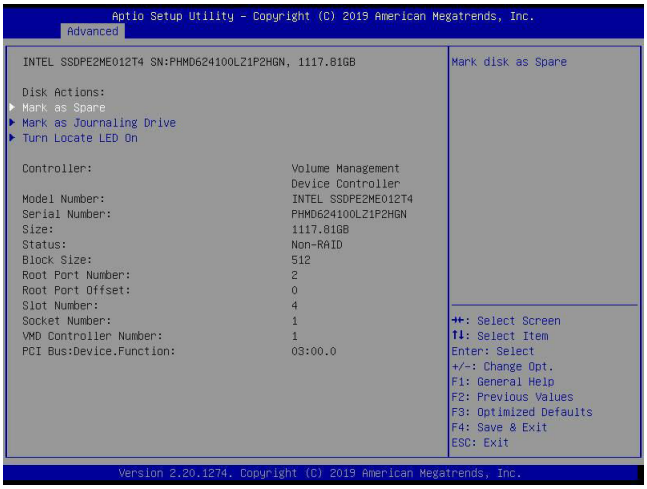


To Mark a RAID Volume as Spare

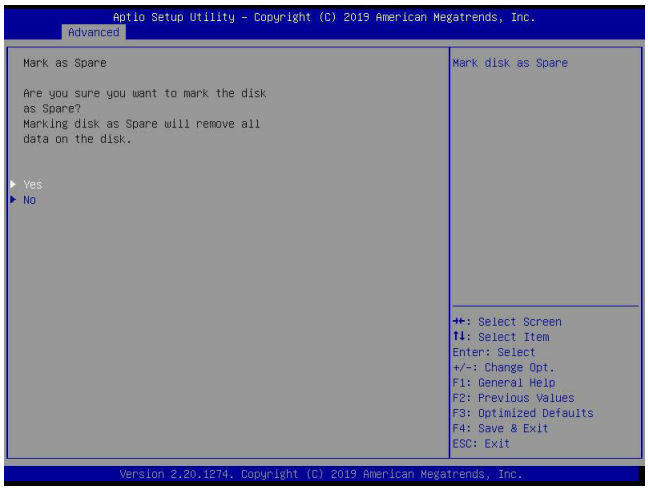
Follow the instructions stated in the E.1 section to access the **All Intel VMD Controllers** menu. When the following screen appears, select a desired NVMe device from the list of Non-RAID Physical Disks.



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.



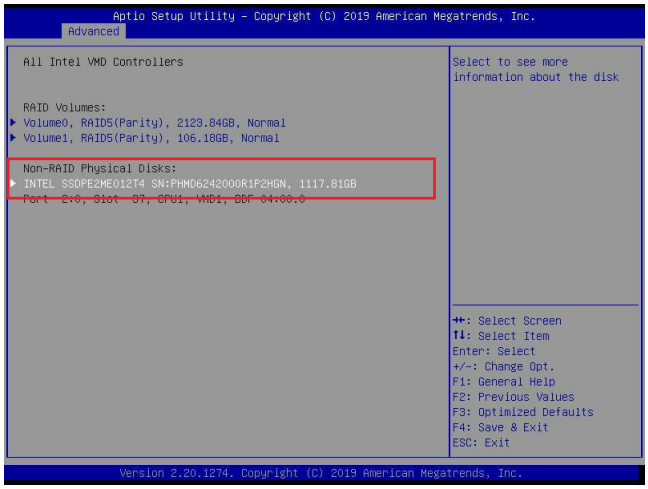
When the following screen appears, select Yes to confirm that you want the selected device to be used as a spare device. The options are **Yes** and No.



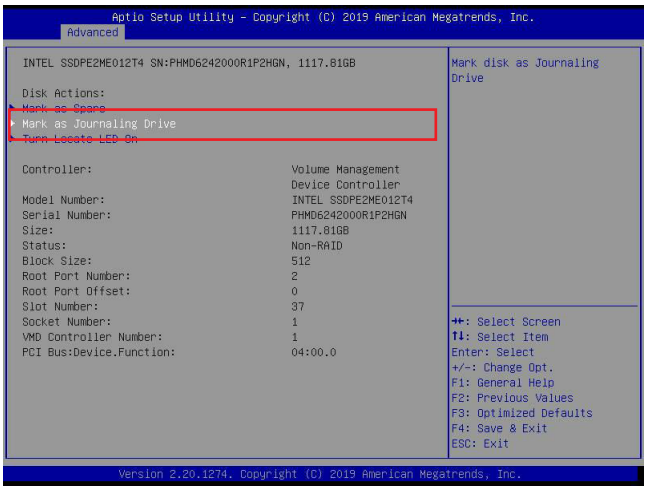
Note: A spare disk is used for automatic RAID volume rebuilds when status of failed, missing, or at risk is detected on the array disk. For a RAID0 volume, only status of at risk will trigger automatic RAID volume rebuilds.

To Mark a RAID Volume as a Journaling Drive

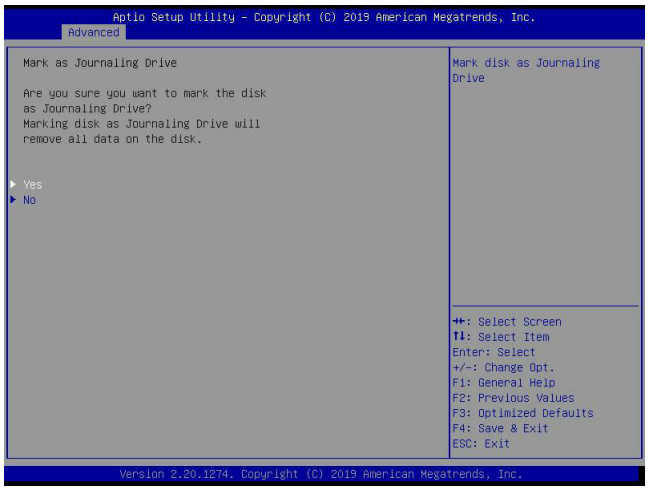
Refer to the instructions stated in the E.1 section to access the All Intel VMD Controllers menu. When the following screen appears, select a desired NVMe device from the list of Non-RAID Physical Disks for use as a journaling drive.



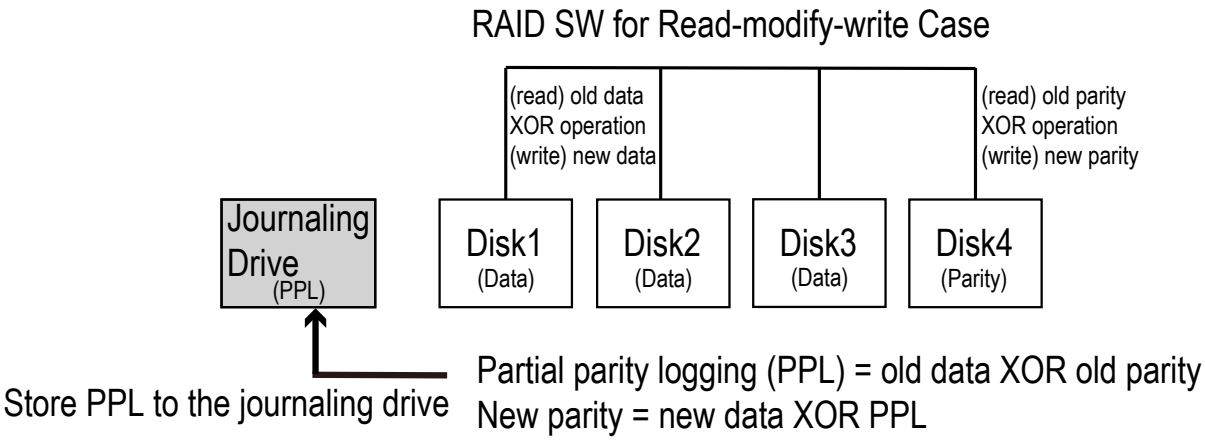
After selecting a NVMe device, press <Enter> and the following screen will appear. Select **Mark as Journaling Drive** and press <Enter>.



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.



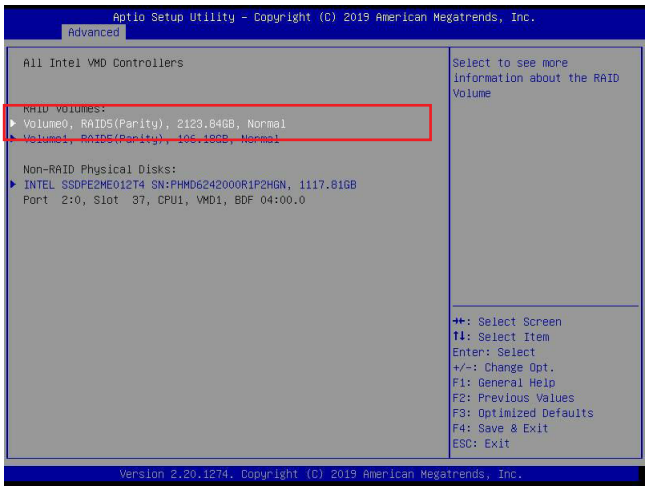
Note: RAID Write Hole (RWH) is a condition associated with a power/drive-failure/crash while writing to a RAID5 volume. The use of journaling drive that contains partial parity logging (PPL) can reduce the potential data loss. Refer to the following illustration for the use of journaling drive.



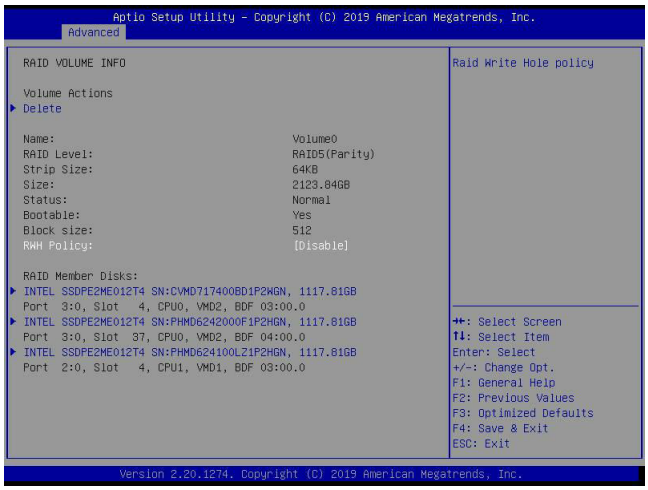
E.3 Use of Journaling Drive

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 E.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.



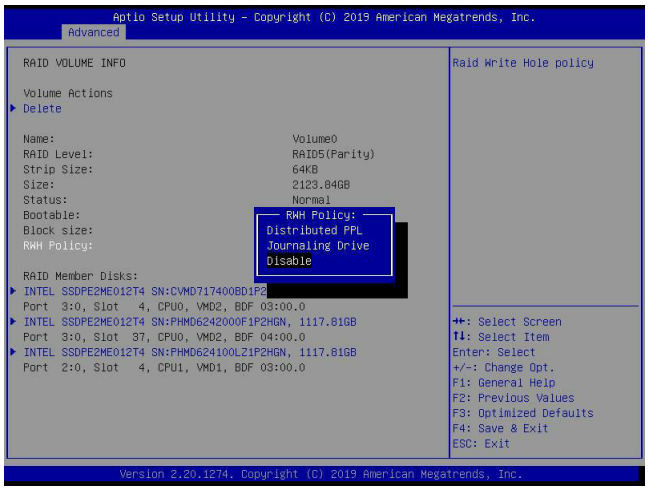
Press <Enter> and the following screen will appear.



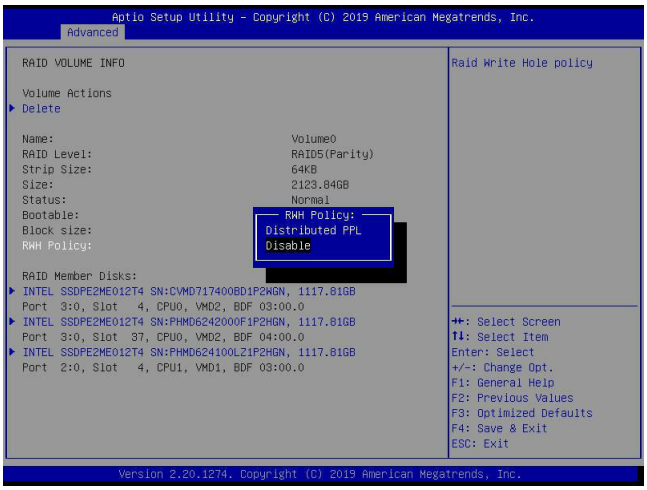
Step 2. Use the arrow keys to select RWH Policy. RWH is a scenario related to a power/drive-failure/crash.

RWH Policy

Press <Enter> and the following screen will appear. If any device has been set as a journaling drive (see pages 200 and 201), the options are Distributed PPL, Journaling Drive, and **Disable**.



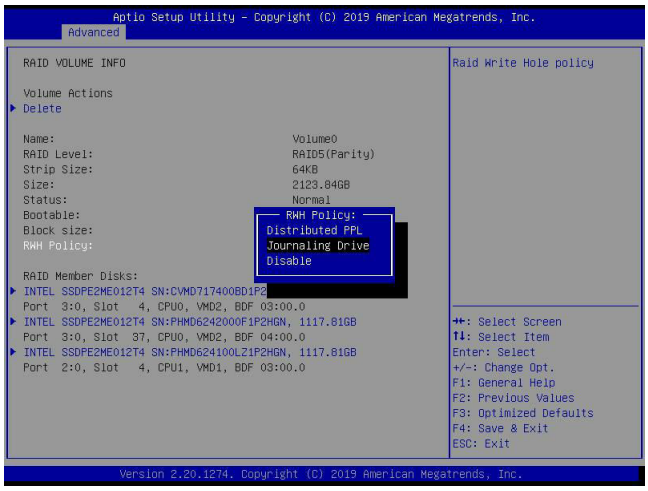
If no device has been set as a journaling drive, the options are Distributed PPL and **Disable**.



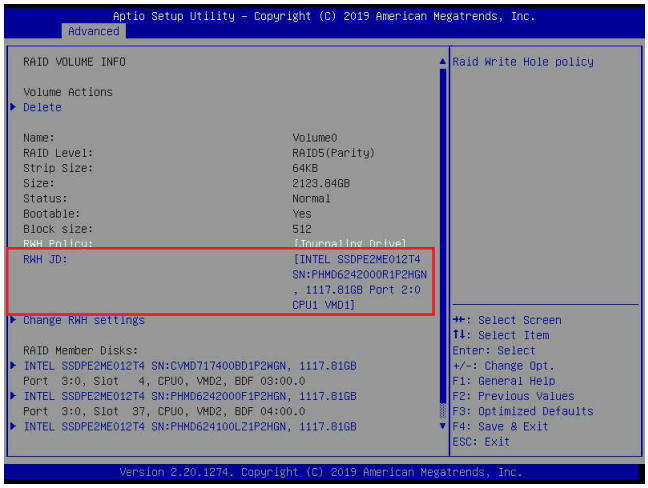
Note 1: Partial parity logging (PPL) can be defined as the result of XOR calculation of old data and old parity. PPL is a feature available for RAID5 volumes. While a power/drive-failure/crash occurring, PPL information helps rebuild the RAID volume and reduce the potential data loss.

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**.

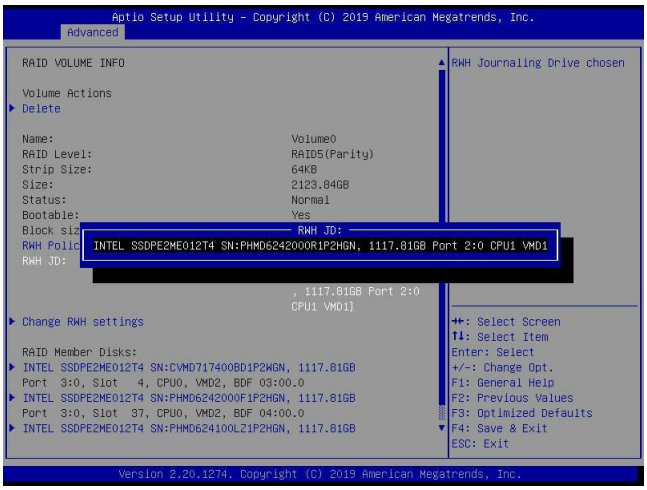


Press <Enter> and the RWH JD feature will become available as shown below.



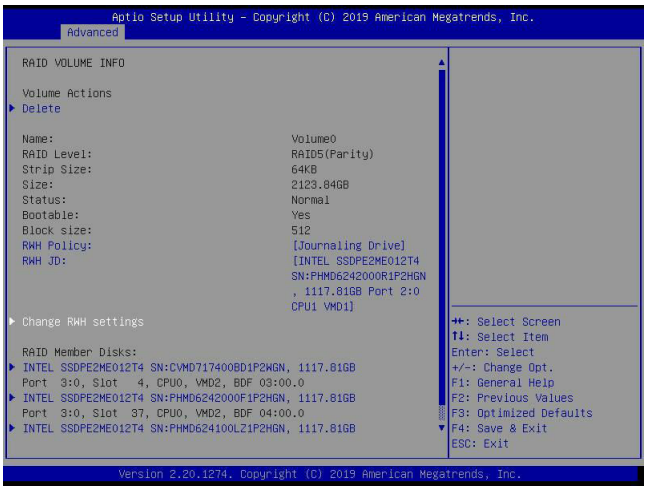
RWH JD

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).

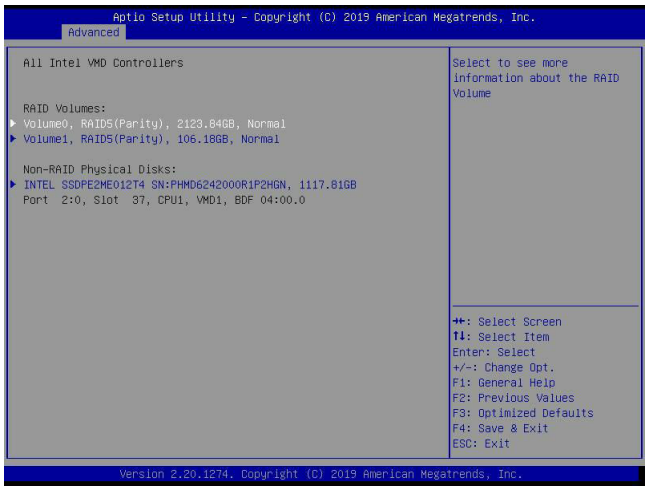


Step 4. Use the arrow keys and press <Enter> to select the desired journaling drive from the option list of RWH JD.

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.



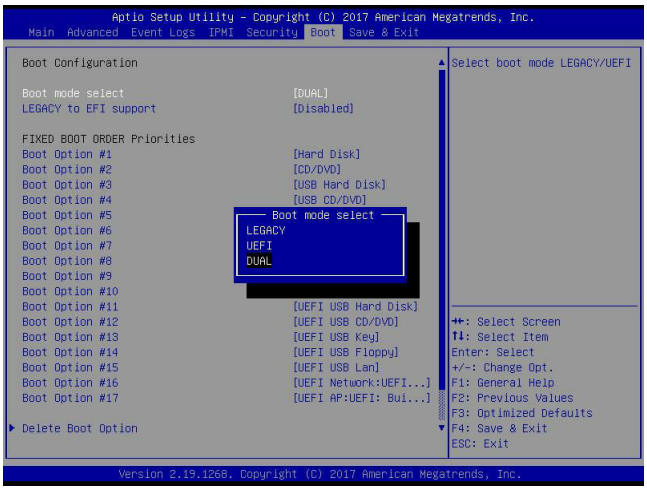
Appendix F

Secure Boot Settings

Secure boot is a feature of UEFI (Unified Extensible Firmware Interface) that ensures boot loaders are digitally signed and validated. The F.1, F.2, and F.3 sections provide instructions on how to enable the secure boot features. The F.4 section states Key Management settings.

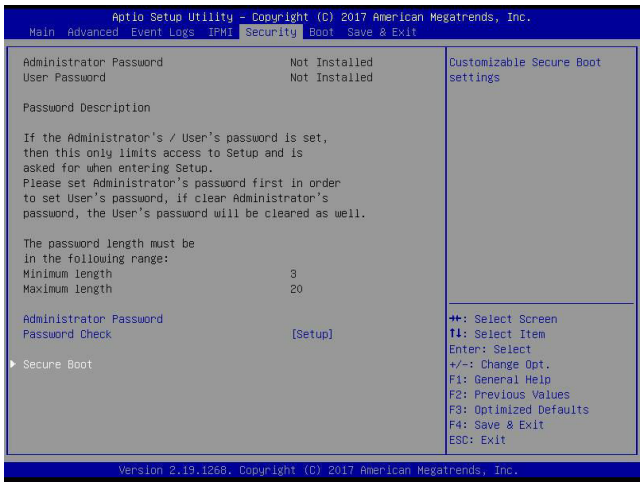
F.1 Boot mode select Feature

Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Boot tab. Use the arrow keys to select Boot mode select and press <Enter>. The options are LEGACY, UEFI, and **DUAL**. Set Boot mode select to UEFI. For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

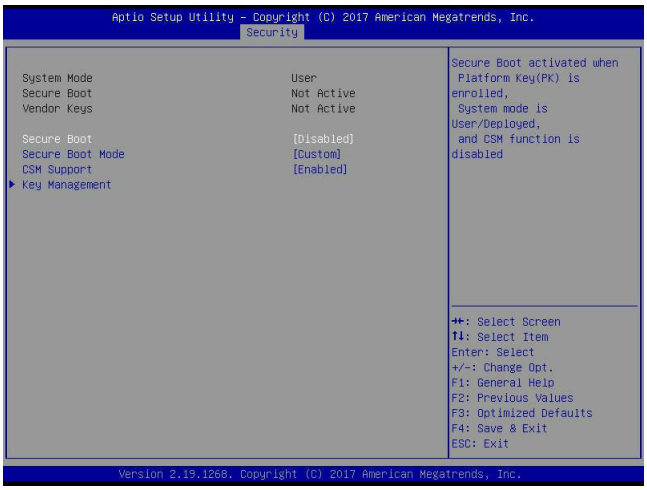


F.2 Secure Boot/ Secure Boot Mode/ CSM Support Features

Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab as shown below.



Use the arrow keys to select Secure Boot and press <Enter> to access the menu items. The following screen will appear.



Secure Boot

This feature is available when the platform key (PK) is pre-registered where the platform operates in the User mode and compatibility support module (CSM) support is disabled in the BIOS Setup utility. Select Enabled for secure boot flow control. The options are **Disabled** and Enabled.

Secure Boot Mode

Use this feature to set the secure boot mode. The options are Standard and **Custom**. Select Standard to load manufacturer's default secure variables. Select Custom to change the image execution policy and to manage secure boot keys.

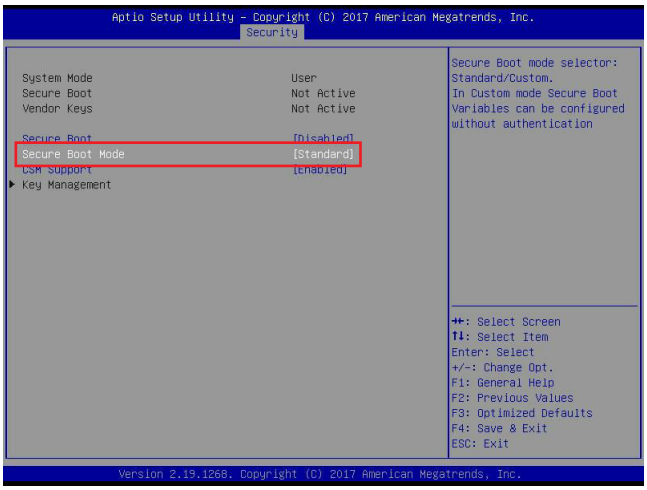
CSM Support

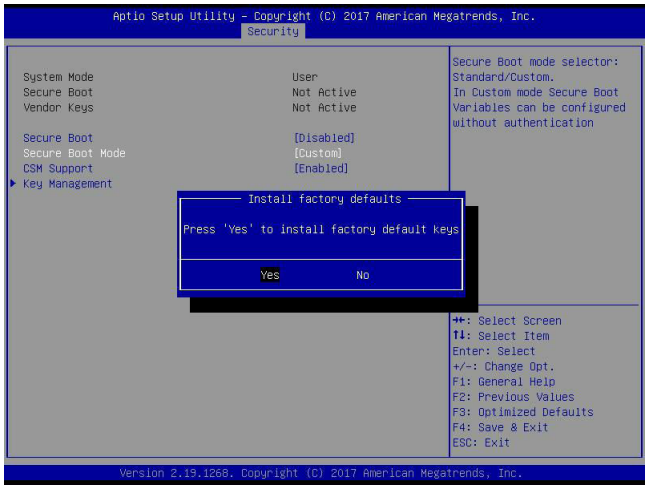
Select Enabled to support the legacy CSM, which provides compatibility support for traditional legacy BIOS for system boot. The options are Disabled and **Enabled**.

F.3 Secure Boot Settings

To have the secure boot support, be sure to follow the steps below (Step 1 ~ Step 4).

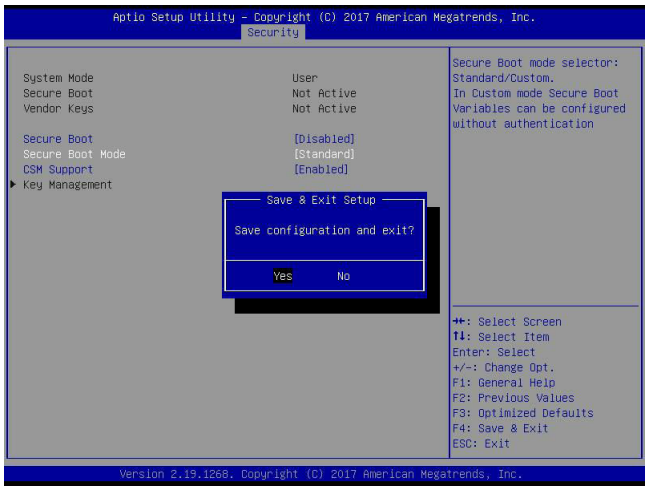
Step 1. Set Secure Boot Mode to Standard. Press Yes to install factory default keys as needed.



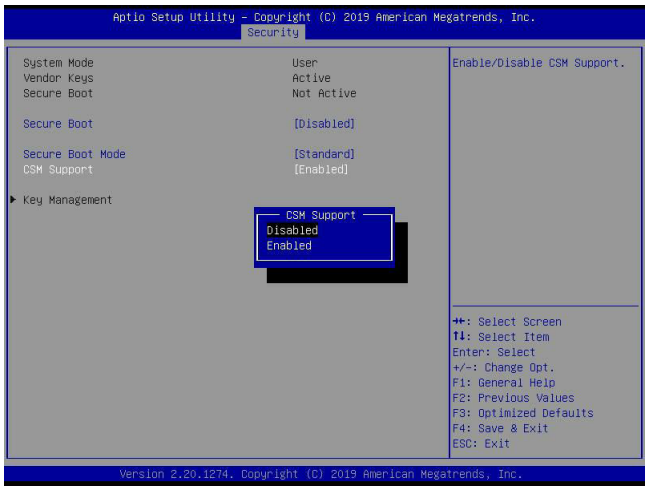


Note: The Key Management menu will become unavailable when Secure Boot Mode is set to Standard.

Step 2. For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

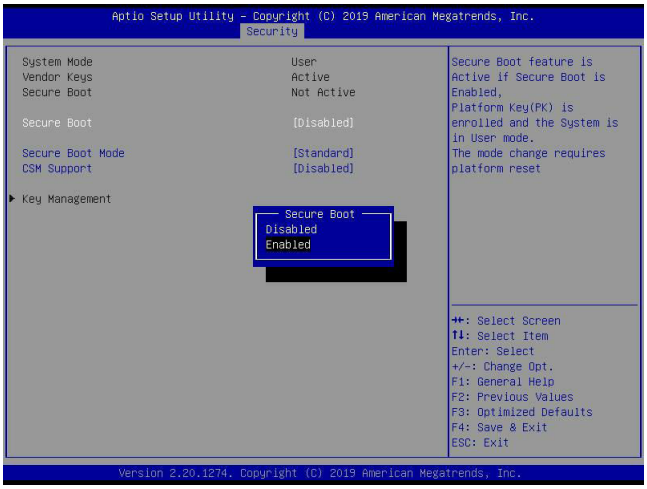


Step 3. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. Set CSM Support to Disabled.

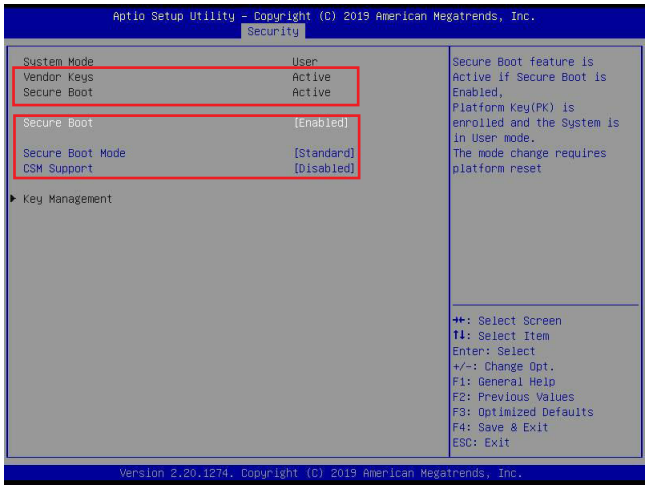


For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

Step 4. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. Set Secure Boot to Enabled.



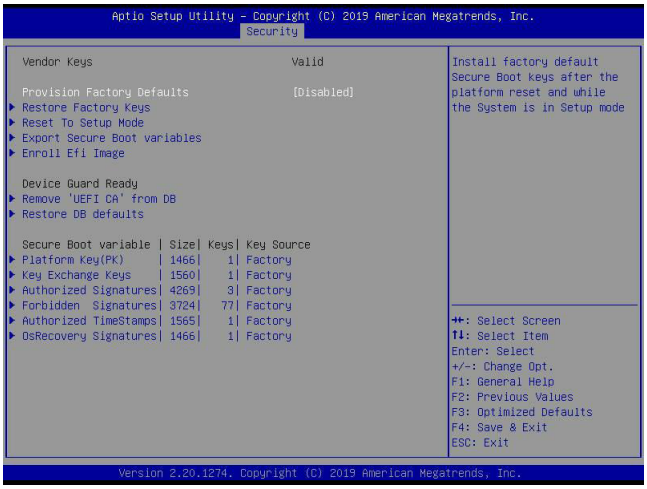
For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. The following screen will appear.



Note: Once Secure Boot is enabled, CSM Support will become disabled and the legacy environment is no longer valid. The authorized UEFI support such as UEFI OS, AOC UEFI FW, and UEFI PXE server are allowed.

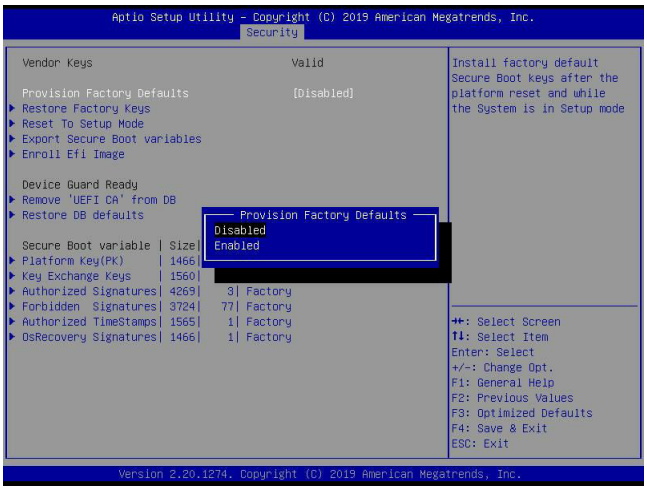
F.4 Key Management Settings

The Key Management menu as shown below, which is available when Secure Boot Mode is set to Custom, allows the secure boot keys to be installed via the external device and be involved in the secure boot process.



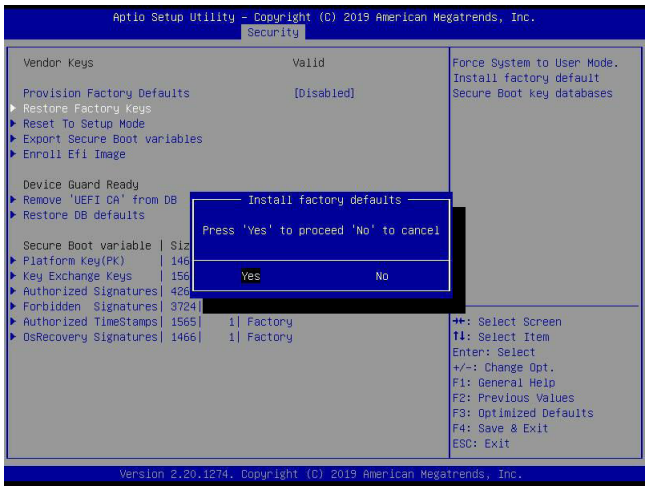
Provision Factory Defaults

This feature is to provision the default secure boot keys set by the manufacturer when system is in the Setup mode. The options are **Disabled** and Enabled.



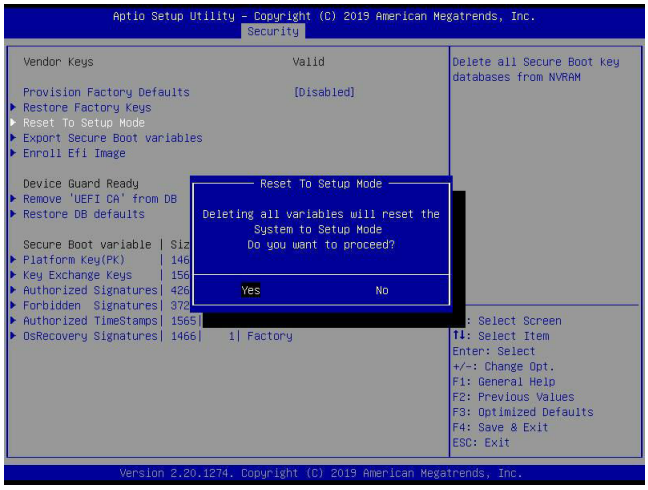
▶Restore Factory Keys

Select and press Yes to restore factory default secure boot keys and key variables. Also, it will reset the system to the User mode. The options are **Yes** and No.



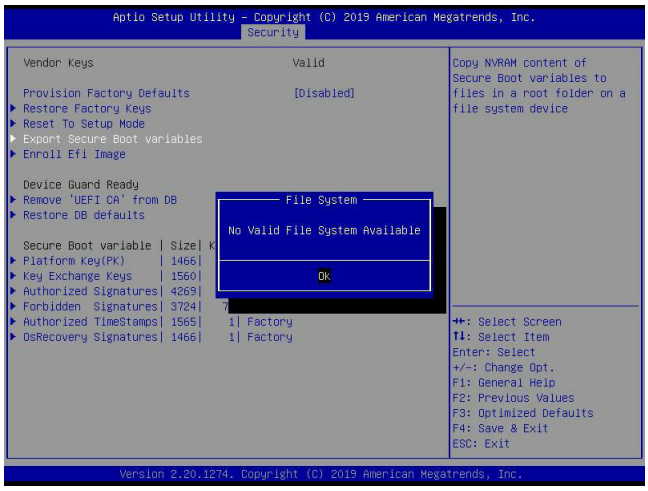
▶Reset To Setup Mode (available when the System Mode is in User mode)

Select and press Yes to clear all secure boot variables and reset the system to the Setup mode. The options are **Yes** and No.



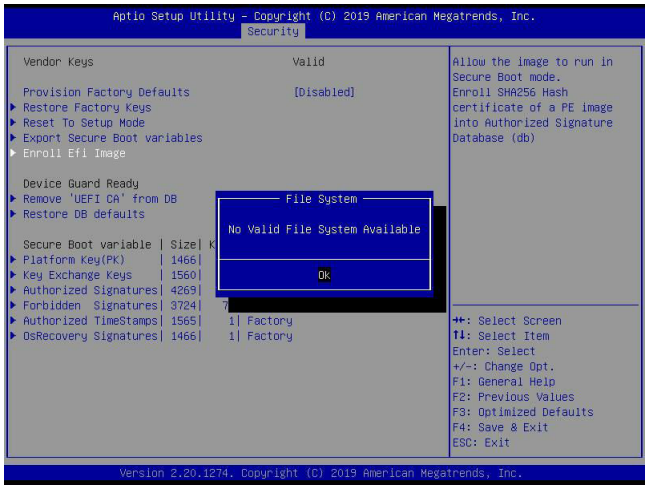
▶Export Secure Boot variables

Use this feature to export NVRAM content of secure boot variables to files in a root folder on a file system device.



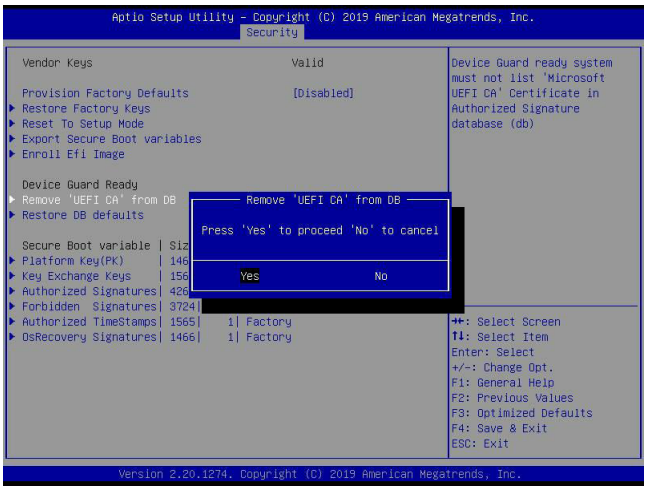
▶Enroll Efi Image

This feature is to enroll SHA256 hash of the binary into the Authorized Signature Database (DB) and to allow the image to run in the secure boot mode.



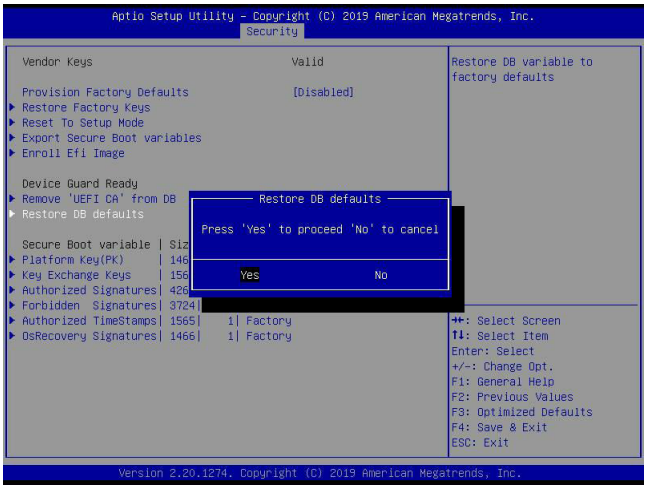
▶Remove 'UEFI CA' from DB (available when the system is not in Device Guard Ready)

Select and press Yes to remove Microsoft UEFI CA certificate from the DB. The options are **Yes** and No.



▶Restore DB defaults

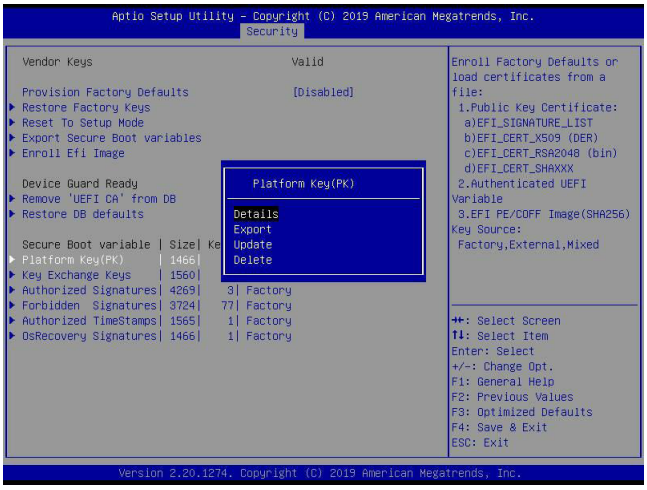
Select and press Yes to restore the DB variables to factory defaults. The options are **Yes** and No.



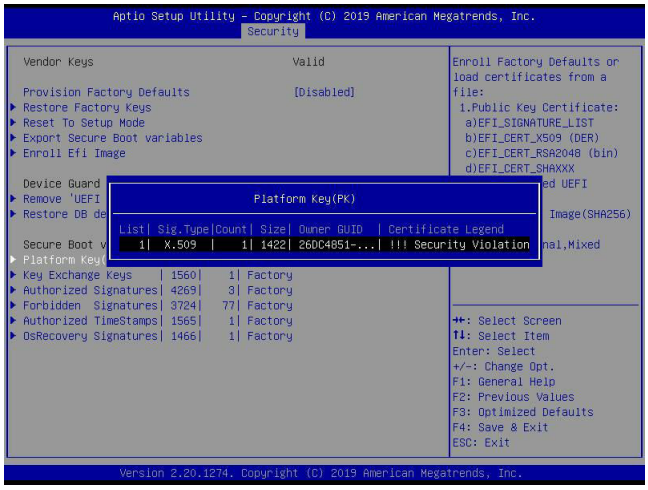
Refer to the following settings for keys and signatures related to secure boot.

▶Platform Key (PK)

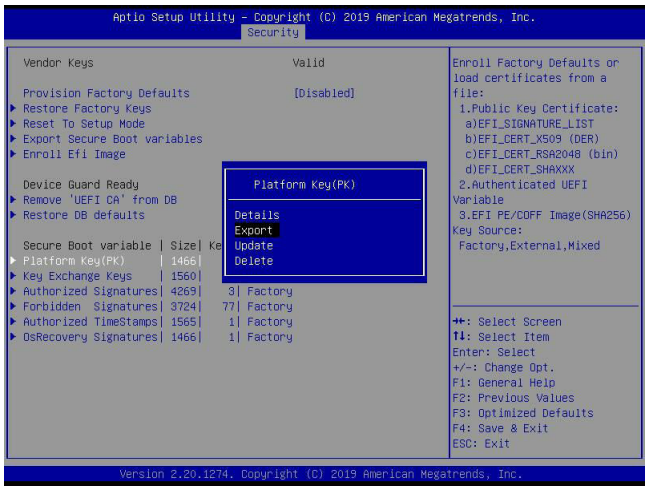
The Platform Key (PK), which is pre-installed in firmware during manufacturing, provides full control of the secure boot key hierarchy. The options are **Details**, Export, Update, and Delete. Select Details to display detailed information of PK. Select Export to save the current PKs to a FAT formatted USB flash drive. Select Update to load the factory defaults or load PKs from a file on the external device. Select Delete to clear the current PKs and reset the system to the Setup mode. See the following for more information of each option.



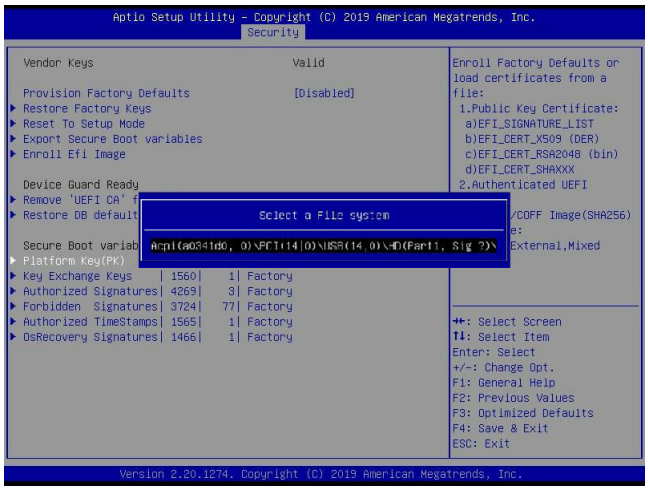
Details: Use the arrow keys to select Details and press <Enter>. It displays detailed information of PK as shown below.



Export: Use the arrow keys to select Export. It is to save the current PKs to a FAT formatted USB flash drive.

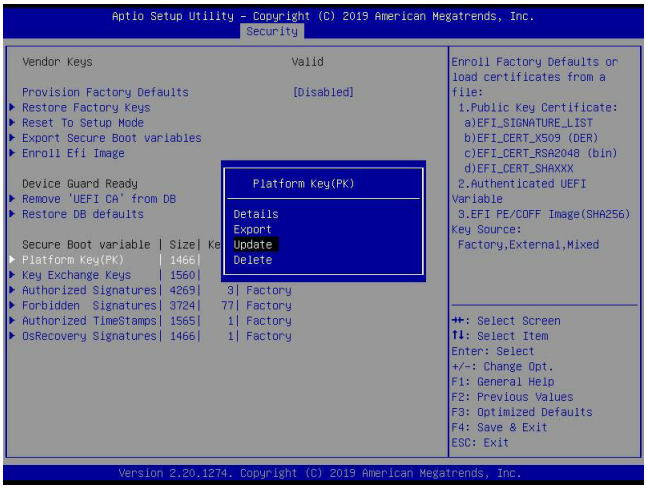


Press <Enter> and the following screen will appear.

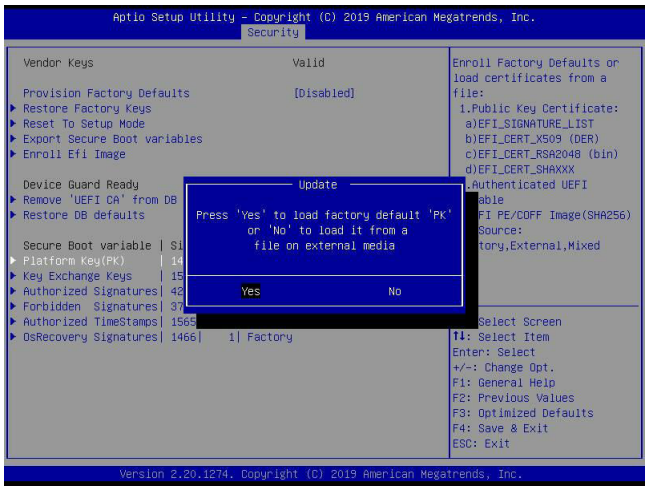


Note: Refer to the right panel of the screen for the file formats accepted.

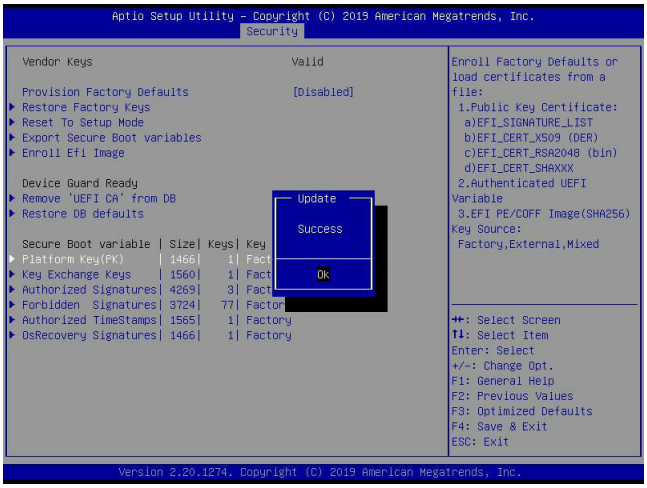
Update: Use the arrow keys to select Update. It is to load the factory defaults or load PKs from a file on the external device.



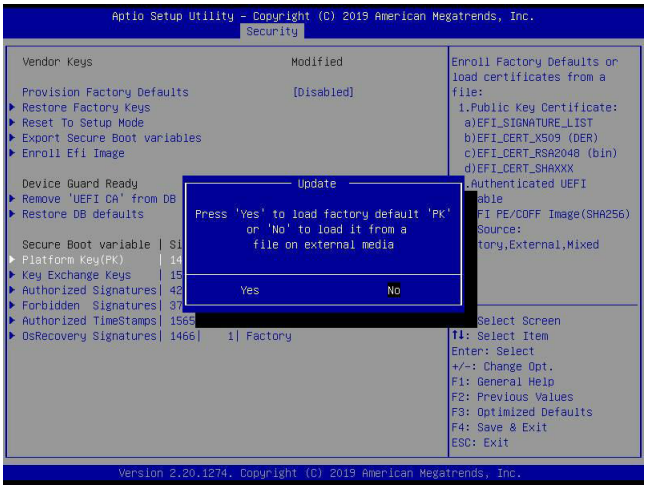
Press <Enter> and the following screen will appear.



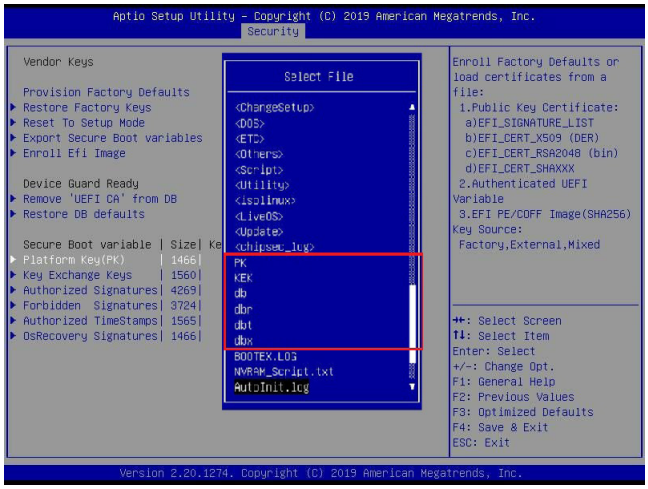
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.

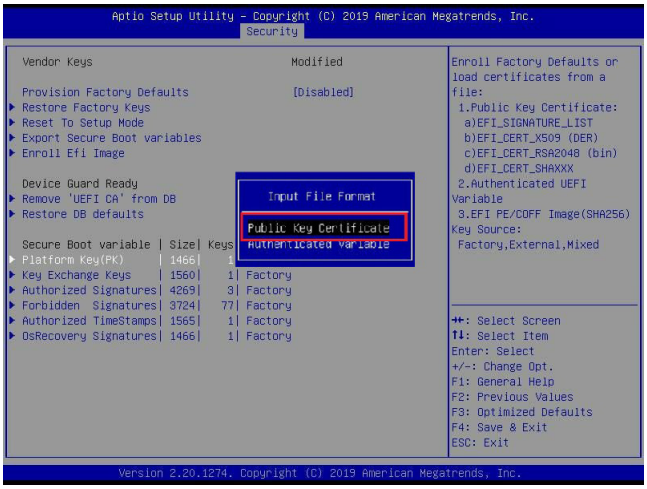


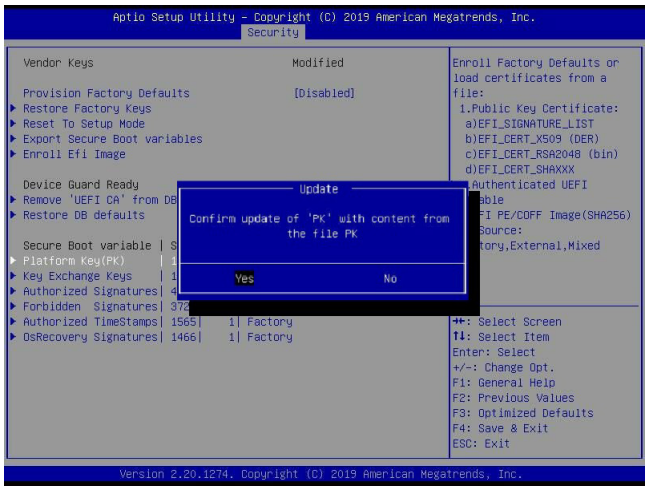
To load PKs from a file on the external device, navigate to No and press <Enter>.



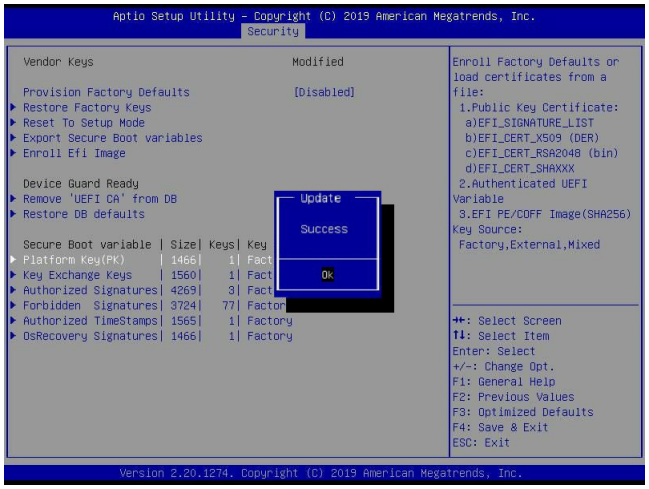
When the following screen appears, select the USB flash drive that contains the desired file.



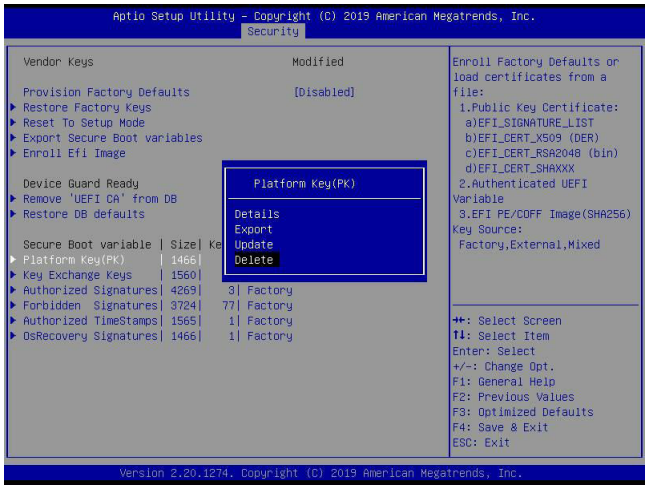


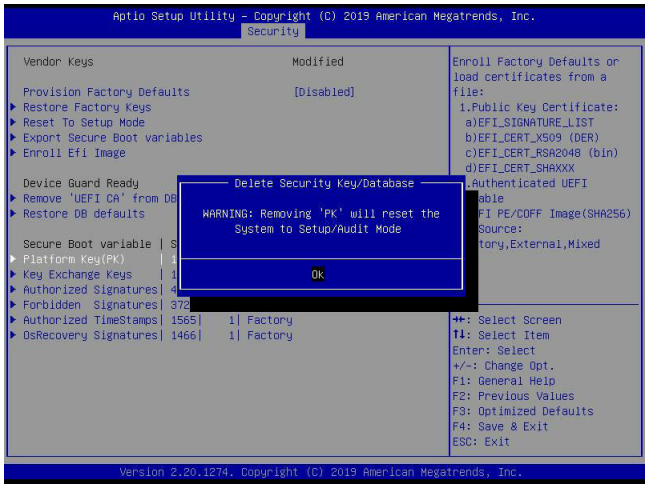


Press <Enter> and the following screen will appear.



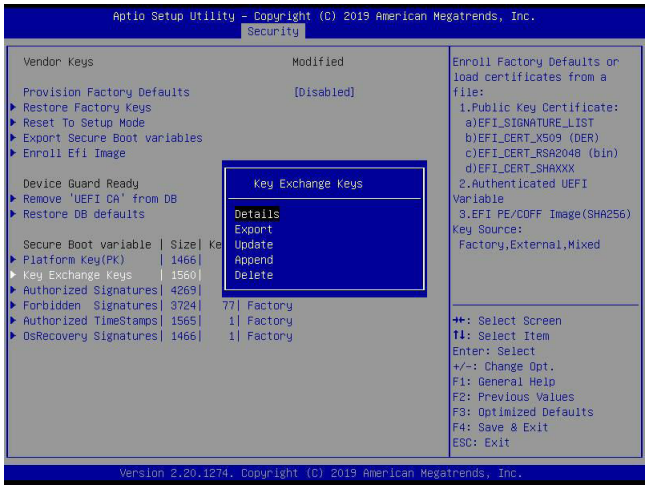
Delete: Use the arrow keys to select Delete and press <Enter> to clear the current PKs and reset the system to the Setup mode.



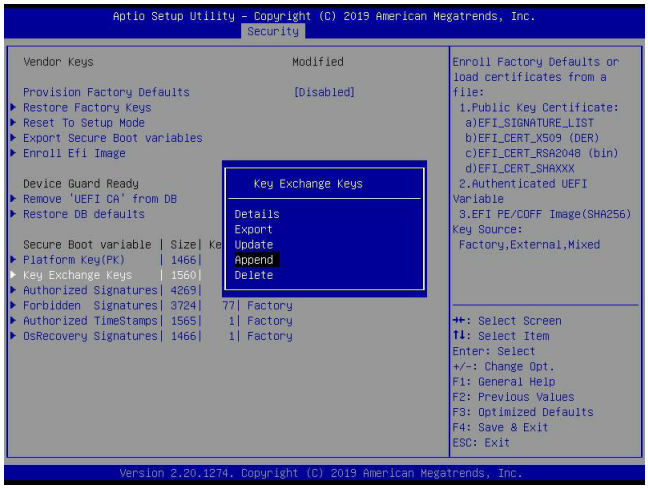


▶Key Exchange Key

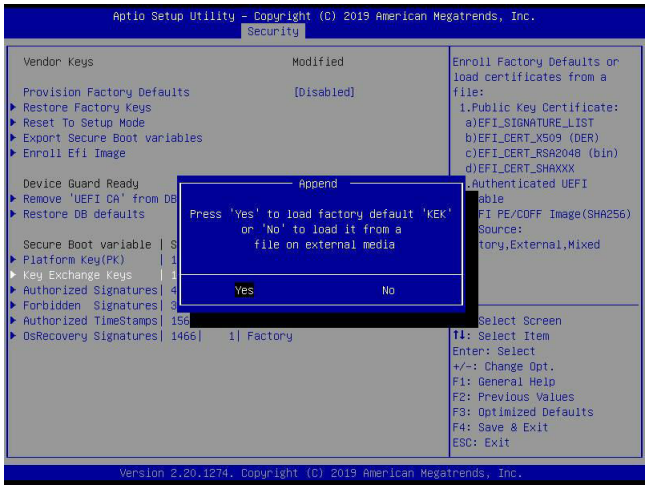
The Key Exchange Key (KEK), which is held by the operating system vendor, can be updated by the holder of the PK and be used by secure boot to protect access to signatures databases. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of KEKs. Select Export to save the current KEKs to a FAT formatted USB flash drive. Select Update to load the factory defaults or load KEKs from a file on the external device. Select Append to load the factory defaults or load KEKs from a file on the external device. Select Delete to clear the current KEKs or to delete only one certificate from the key database. (Refer to page 216 for the Export process. Refer to pages 217, 218, 219, and 220 for the Update process.)



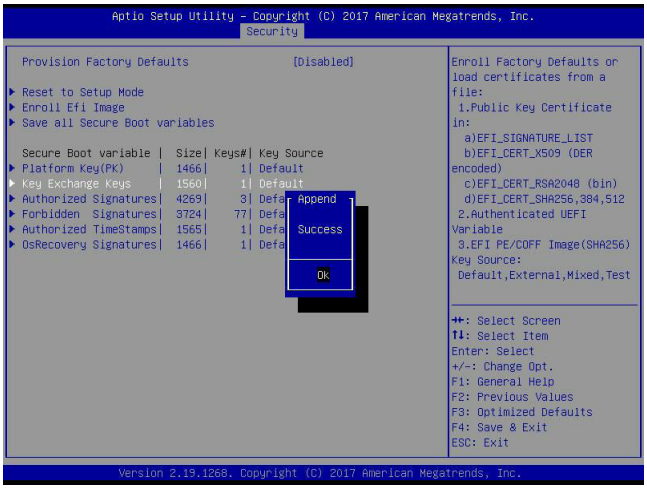
Append: Use the arrow keys to select Append.



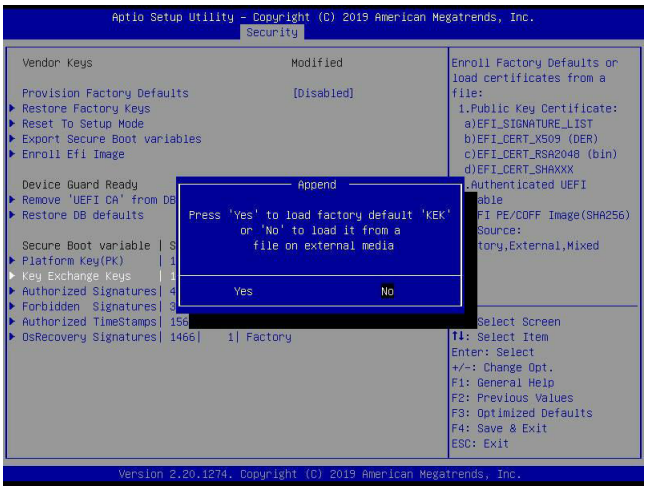
Press <Enter> and the following screen will appear.



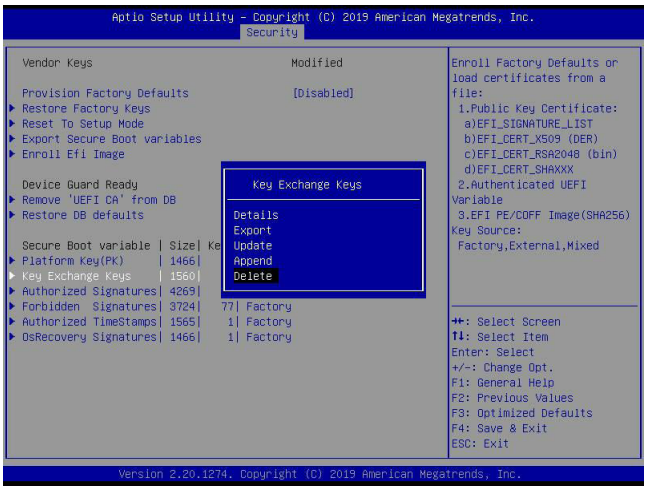
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.

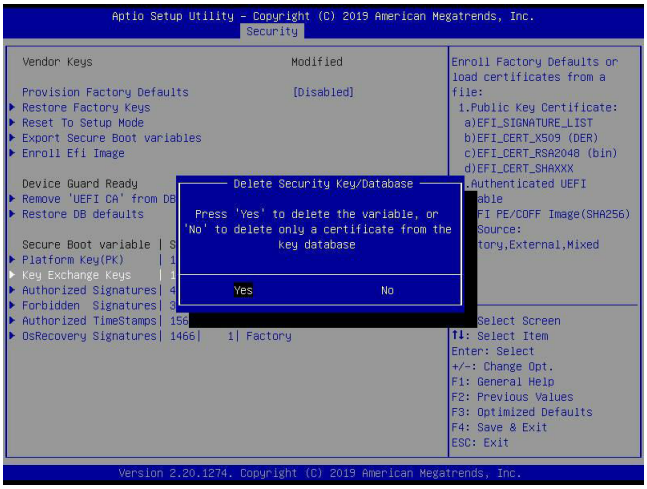


To load KEKs from a file on the external device, navigate to No and press <Enter>. Refer to pages 219 and 220 on how to load KEKs from a file on the external device.

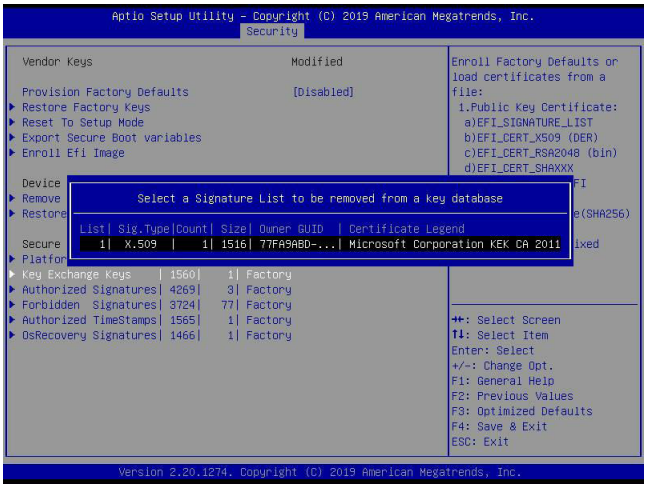


Delete: Use the arrow keys to select Delete and press <Enter>. Navigate to Yes and press <Enter> to clear the current KEKs.



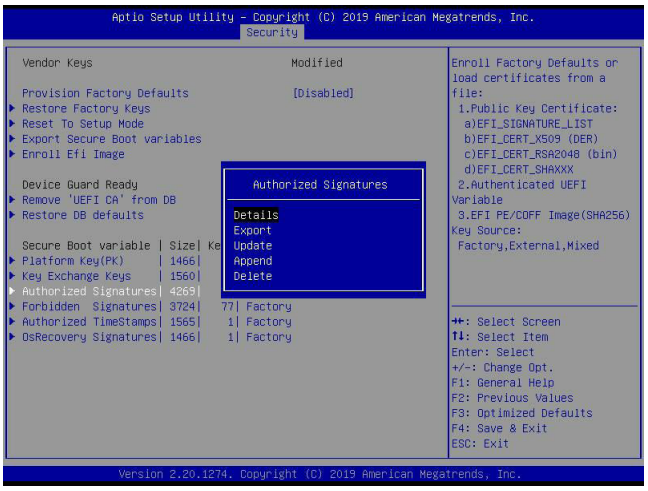


Navigate to No and press <Enter> to delete only one certificate from the key database.



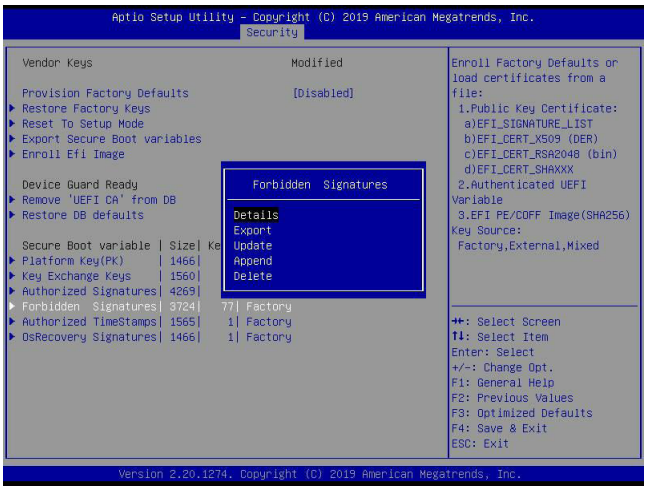
▶Authorized Signatures

Authorized Signature Database (DB) contains authorized signing certificates and digital signatures. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of Authorized Signatures. Select Export to save the current DB to a FAT formatted USB flash drive. Select Update to load the factory defaults or load DB from a file on the external device. Select Append to add variables to the existing DB. Select Delete to clear the current DB or to delete only one certificate from the key database. (Refer to page 216 for the Export process. Refer to pages 217, 218, 219, and 220 for the Update process. Refer to pages 221 and 222 for the Append process. Refer to page 223 for the Delete process.)



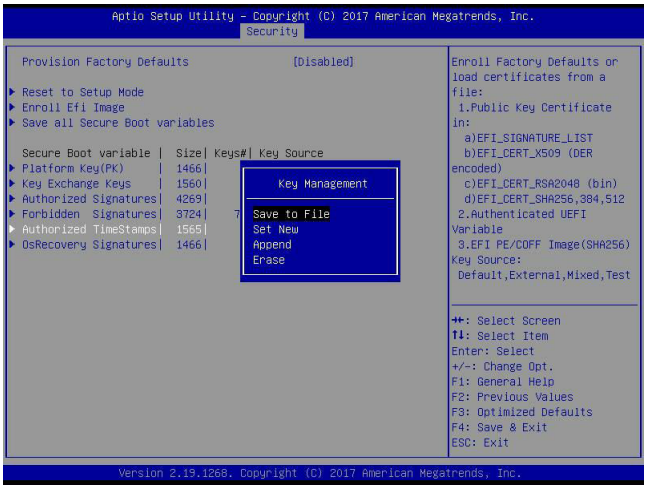
▶Forbidden Signatures

Forbidden Signature Database (DBX), which is the inverse of DB, contains forbidden certificates and digital signatures. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of Forbidden Signatures. Select Export to save the current DBX to a FAT formatted USB flash drive. Select Update to load the factory defaults or load DBX from a file on the external device. Select Append to add variables to the existing DBX. Select Delete to clear the current DBX or to delete only one certificate from the key database. (Refer to page 216 for the Export process. Refer to pages 217, 218, 219, and 220 for the Update process. Refer to pages 221 and 222 for the Append process. Refer to page 223 for the Delete process.)



▶Authorized TimeStamps

Authorized Timestamp Database (DBT) is used to issue and check signed time stamp certificates. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of Authorized Timestamps. Select Export to save the current DBT to a FAT formatted USB flash drive. Select Update to load the factory defaults or load DBT from a file on the external device. Select Append to add variables to the existing DBT. Select Delete to clear the current DBT or to delete only one certificate from the key database. (Refer to page 216 for the Export process. Refer to pages 217, 218, 219, and 220 for the Update process. Refer to pages 221 and 222 for the Append process. Refer to page 223 for the Delete process.)



▶OsRecovery Signatures

OsRecovery Signatures Database (DBR) contains secure boot authorized recovery variables. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of OsRecovery Signatures. Select Export to save the current DBR to a FAT formatted USB flash drive. Select Update to load the factory defaults or load DBR from a file on the external device. Select Append to add variables to the existing DBR. Select Delete to clear the current DBR or to delete only one certificate from the key database. (Refer to page 216 for the Export process. Refer to pages 217, 218, 219, and 220 for the Update process. Refer to pages 221 and 222 for the Append process. Refer to page 223 for the Delete process.)