X11SPA-TF
X11SPA-T

USER'S MANUAL

Revision 1.0c

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

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

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

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

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

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

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

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

Manual Revision 1.0c

Release Date: January 18, 2022

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 X11SPA-TF/-T motherboard.

About This Motherboard

The Supermicro X11SPA-TF/-T supports a single Intel® Xeon® Scalable-SP series processor (Socket LGA 3647) with up to 28 cores and a thermal design power (TDP) of up to 205W. Built with the Intel PCH C621 chipset, the X11SPA-TF/-T supports 6-channel, 12-DIMM DDR4 ECC RDIMM/LRDIMM memory with speeds of up to 2933 MHz, four M.2 PCIe 3.0 x4 slots, three RJ45 ports (two RJ45 LAN ports and one IPMI LAN port), and a Trusted Platform Module (TPM) header. The X11SPA-TF/-T is optimized for high-performance and high-end computing platforms that address the needs of next generation server applications. 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. X11SPA-TF supports 2nd Generation Intel Xeon Scalable-SP (82xx/62xx/52xx/42xx/32xx series) processors. X11SPA-T supports 2nd Gen Intel Xeon Scalable-SP (82xx/62xx/52xx/42xx/32xx series) and Intel Xeon W-32xx series processors. **2.** Support for 2933MHz memory is dependent on the CPU SKU.

Conventions Used in the Manual

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

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

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

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

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

Contacting Supermicro

Headquarters

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

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Website:	www.supermicro.com.tw

Table of Contents

Chapter 1

Introduction

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

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

1.1 Checklist

Main Parts List		
Description	**Part Number**	**Quantity**
Supermicro Motherboard	X11SPA-TF/-T	1
I/O Shield	MCP-260-00042-0N	1
SATA Cables	CBL-0044L	6
GPU to CPU Power Cable	CBL-PWEX-0663	1
Quick Reference Guide	MNL-2173-QRG	1
M.2 Heatsinks	SNK-C0121L-1	4

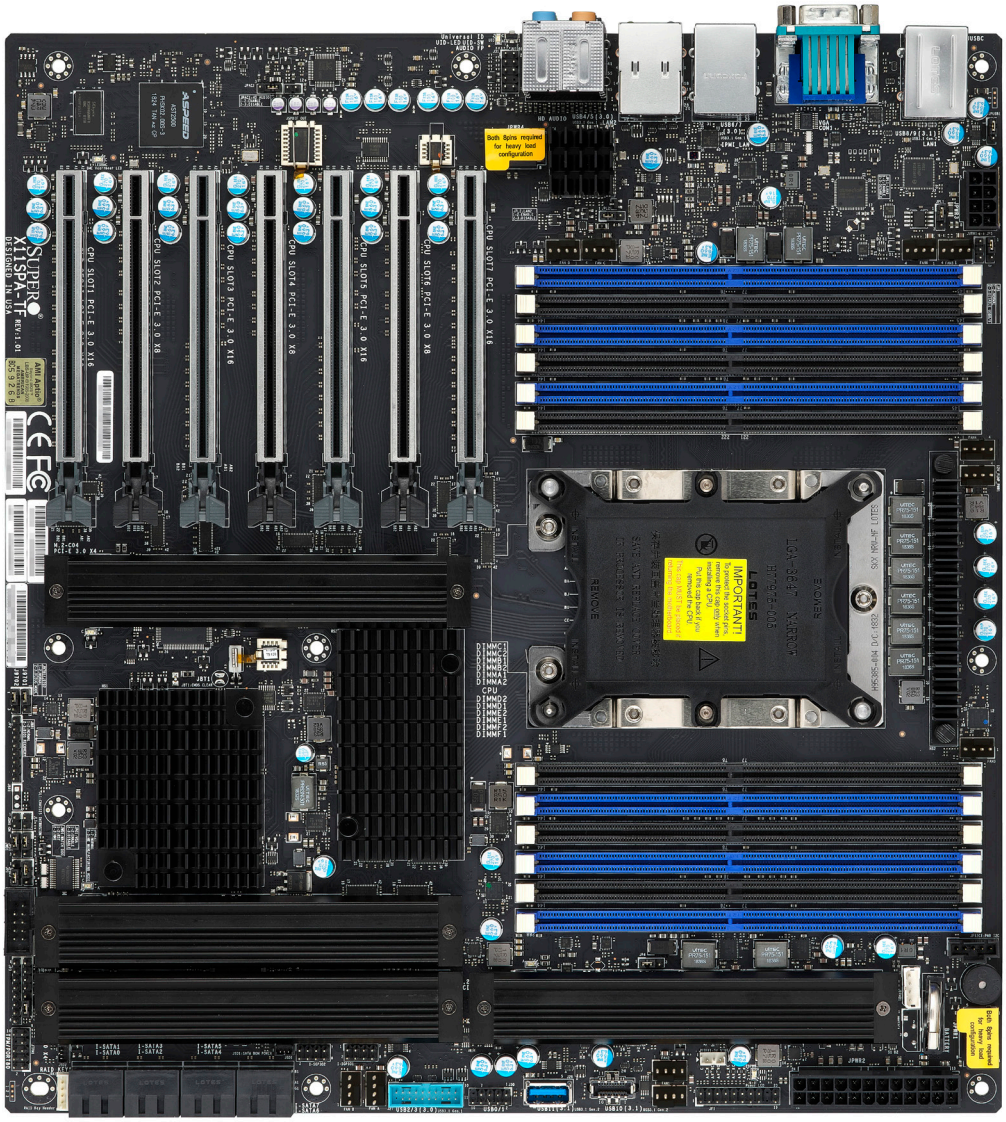
Important Links

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

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

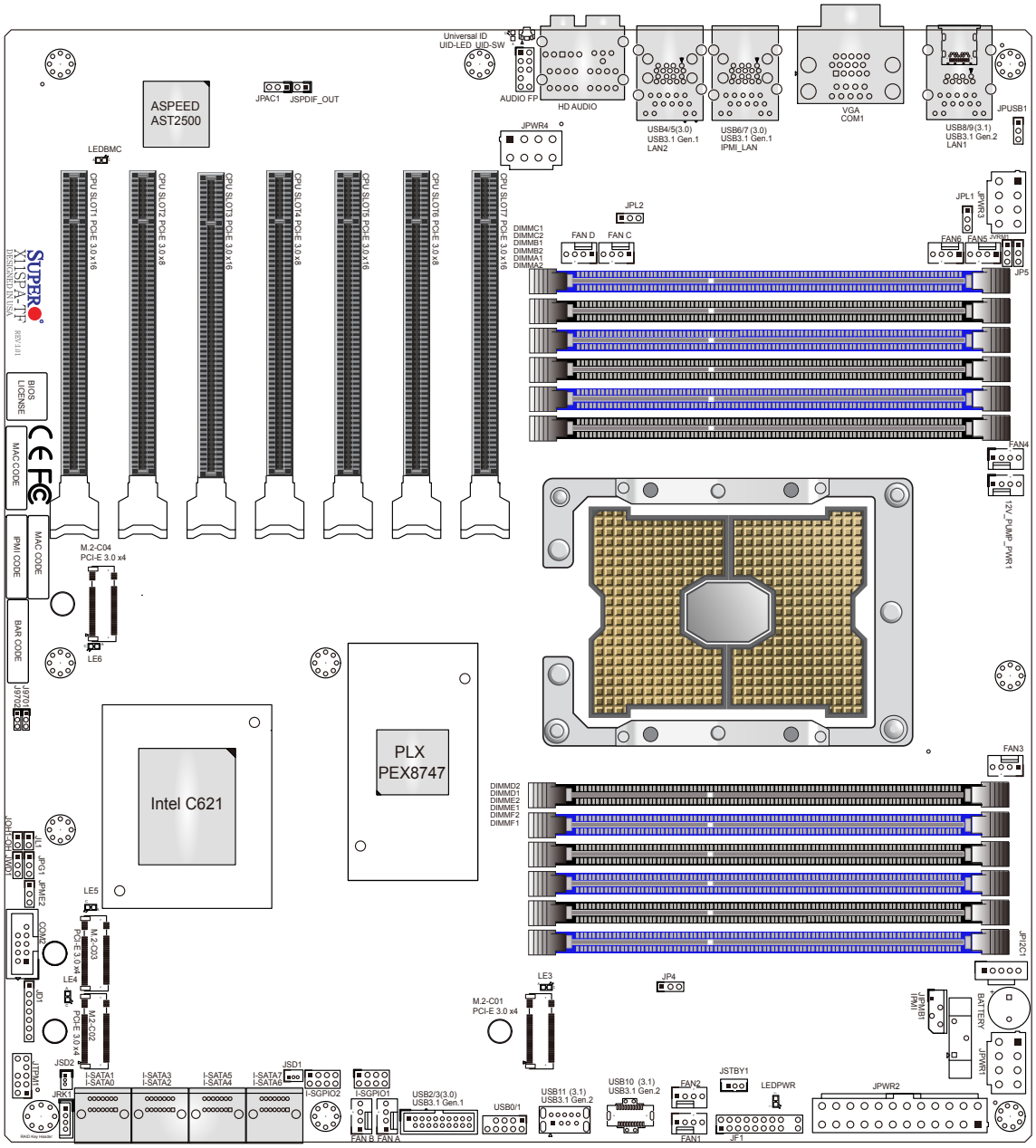
This manual may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

Figure 1-1. X11SPA-TF/-T Motherboard Image



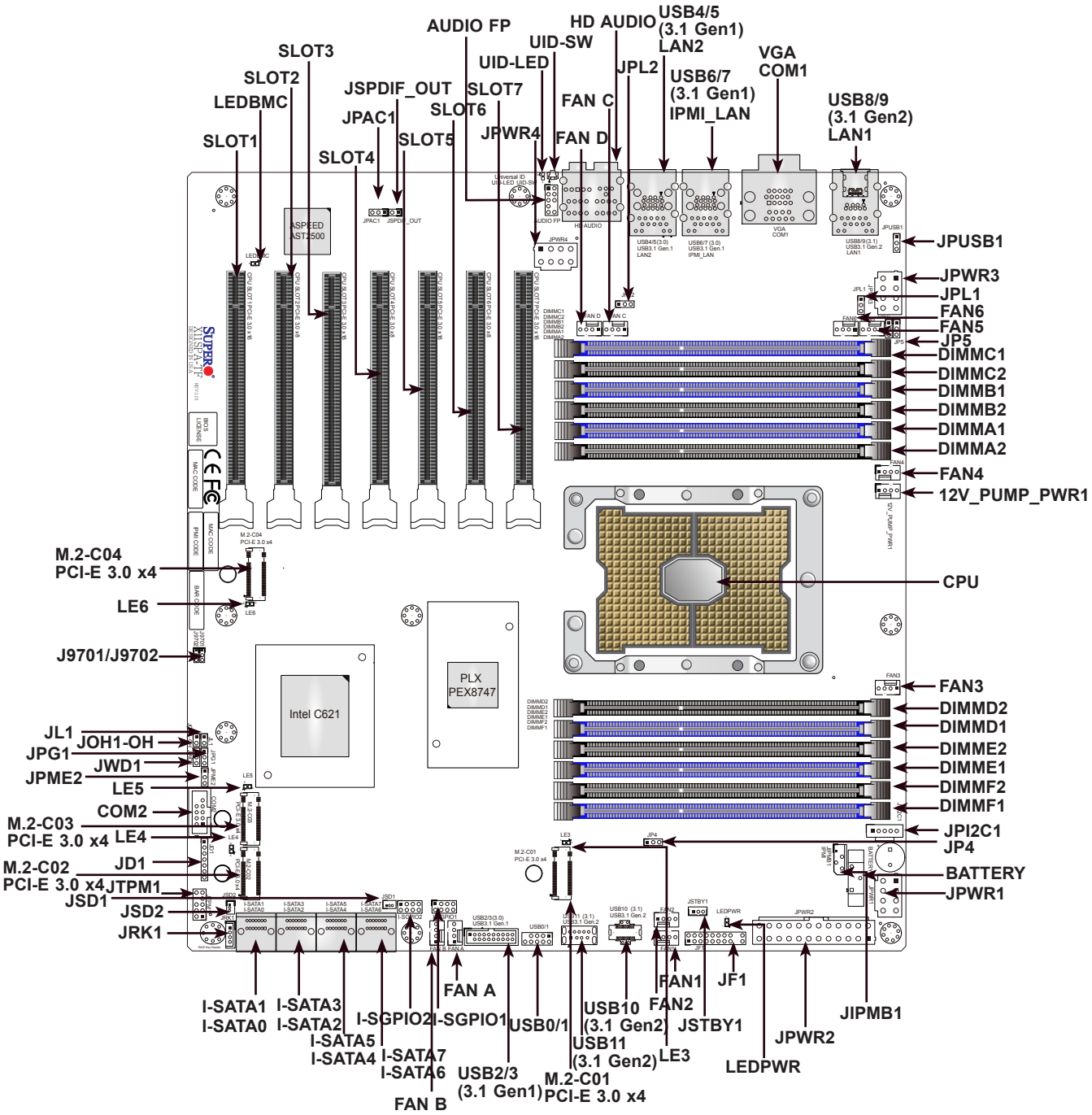
Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publication of the manual. The motherboard you received may or may not look exactly the same as the graphics shown in this manual.

Figure 1-2. X11SPA-TF Motherboard Layout
(not drawn to scale)



Note: Components not documented are for internal testing only.

Quick Reference



Notes:

- See Chapter 2 for detailed information on jumpers, I/O ports, and JF1 front panel connections.
- " ■ " indicates the location of Pin 1.
- Jumpers/LED indicators not indicated are used for testing only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. Do not install the onboard battery upside down to avoid possible explosion.

Quick Reference Table

Jumper	Description	Default Setting
J9701, J9702	Manufacturing Mode	Pins 1-2 (Normal)
JPAC1	Audio Enable/Disable	Pins 1-2 (Enabled)
JPG1	VGA Enable/Disable	Pins 1-2 (Enabled)
JPL1, JPL2	LAN1/LAN2 Enable/Disable	Pins 1-2 (Enabled)
JPME2	Intel Manufacturing Mode	Pins 1-2 (Normal)
JWD1	Watch Dog Function Enable	Pins 1-2 (Reset)

LED	Description	Status
LE3, LE4, LE5, LE6	M.2 LED	Blinking Green: Device Working
LEDBMC	BMC Heartbeat LED	Blinking Green: BMC Normal
LEDPWR	Onboard Power LED	Solid Green: Power On
UID-LED	Unit Identifier (UID) LED	Blue on: Unit Identified

Connector	Description
12V_PUMP_PWR1	12V 4-pin Power Connector for CPU Liquid Cooling Pump
AUDIO FP	Front Panel Audio Header
BATTERY	Onboard Battery
COM1, COM2	COM1: COM Port (Back Panel), COM2: COM Header
CPU SLOT1/3/5/7 PCI-E 3.0 x16	PCIe x16 Slots *PCIe SLOT1 will change to PCIe x8 link when either M.2-C03 or M.2-C04 is populated with an SSD. PCIe SLOT1 will be completely disabled when either M.2-C01 or M.2-C02 is populated with an SSD.
CPU SLOT2/4/6 PCI-E 3.0 x8 (in x16)	PCIe x16 Slots (PCIe x8 link)
FAN1 ~ FAN6	CPU Fan Headers
FAN A ~ FAN D	System Fan Headers *The initial system fan speed must not be lower than 600 RPM.
HD AUDIO	Back Panel High Definition Audio Ports
IPMI_LAN	Dedicated IPMI LAN Port *For IPMI support, X11SPA-TF is via SPS, whereas X11SPA-T is via ME.
I-SATA0 ~ 7	Intel Serial ATA (SATA 3.0) Ports 0~7 (6Gb/sec)
I-SGPIO1, I-SGPIO2	Serial General Purpose I/O Headers
JD1	Speaker/Power LED Indicator
JF1	Front Control Panel Header
JIPMB1	4-pin External I2C Header (for an IPMI card)
JL1	Chassis Intrusion Header
JOH1-OH	Overheat LED Indicator
JP4, JP5	JP4: Enable/Disable USB10/11, JP5: Enable/Disable USB8/9
JPI2C1	Power Supply SMBus I2C Header
JPUSB1	Enable/Disable USB6/7 WakeUp
JPWR1/3/4	+12V 8-pin CPU Power Connectors (Required)
JPWR2	24-pin ATX Main Power Connector (Required)

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

Connector	Description
JRK1 (VROC)	Intel RAID Key Header *A VROC hardware key is required to enable an M.2 RAID card.
JSD1, JSD2	SATA DOM (Disk-On-Module) Power Connectors
JSPDIF_OUT	Sony/Philips Digital Interface (S/PDIF) Out Header
JSTBY1	Standby Power Header (5V)
JTPM1	Trusted Platform Module (TPM)
LAN1, LAN2	RJ45 1GbE/10GbE LAN Ports
PCI-E M.2-C01/C02/C03/C04 PCI-E 3.0 x4	PCIe M.2 Sockets (Small Form Factor Devices and Other Portable Devices for High Speed NVMe SSDs)
UID-SW	Unit Identifier (UID) Switch
USB0/1	Front Access USB 2.0 Header
USB2/3	Front Access USB 3.1 Gen1 Header
USB4/5, USB6/7	Back Panel USB 3.1 Gen1 Ports *X11SPA-TF/-T does not support S3 or S4. *Either USB4/5 or USB6/7 support standby power.
USB8/9	Back Panel USB 3.1 Gen2 Ports
USB10	Front Access USB 3.1 Gen2 20-pin Connector
USB11	Front Access USB 3.1 Gen2 Port (Type A)
VGA	VGA Port

Motherboard Features

Motherboard Features
CPU
• Supports a single Intel Xeon Scalable-SP series processor with up to 28 cores and a thermal design power (TDP) of up to 205W **Notes: 1.** The X11SPA-TF/-T does not support FPGA or Fabric processors. **2.** X11SPA-TF supports 2nd Gen Intel Xeon Scalable-SP (82xx/62xx/52xx/42xx/32xx series) processors. X11SPA-T supports 2nd Gen Intel Xeon Scalable-SP (82xx/62xx/52xx/42xx/32xx series) and Intel Xeon W-32xx series processors.
Memory
• Up to 768GB of RDIMM, 3TB of 3DS RDIMM, 1.5TB of LRDIMM, and 3TB of 3DS LRDIMM DDR4 (288-pin) ECC memory with speeds of up to 2933 MHz (2DPC) in twelve memory slots. (1DPC and 2DPC are recommended for memory installation. Only selected 2nd Gen Intel Xeon Scalable-SP processors support Intel Optane™ DC Persistent memory modules.) **Note:** Support for 2933MHz memory is dependent on the CPU SKU.
DIMM Size
• Up to 128GB at 1.2V **Note:** For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.
Chipset
• Intel PCH C621
Expansion Slots
• Four PCIe 3.0 x16 Slots (CPU SLOT1, 3, 5, 7) • Three PCIe 3.0 x8 Slots (IN x16) (CPU SLOT2, 4, 6) • Four M.2 PCIe 3.0 x4 Sockets (Supports M-Key 2260, 2280, and 22110)
Network
• One Intel Ethernet Controller I210-AT • One Aquantia® AQC107 10G Ethernet Controller • One Realtek RTL8211E PHY (dedicated IPMI)
Baseboard Management Controller (BMC)
• ASPEED AST2500 BMC
Graphics
• Graphics controller via ASPEED AST2500 BMC

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

Motherboard Features	
I/O Devices	
• Serial (COM) Port	• One serial port on the rear I/O panel (COM1) • One front accessible serial port header (COM2)
• SATA 3.0	• Eight SATA 3.0 ports at 6 Gb/s (I-SATA0~7 with RAID 0, 1, 5, 10)
• Video (VGA) Port	• One VGA connection on the rear I/O panel
Peripheral Devices	
• Two front accessible USB 2.0 connections via one header (USB0/1) • Two front accessible USB 3.1 Gen1 connections via one header (USB2/3) • Four USB 3.1 Gen1 ports on the rear I/O panel (USB4/5, USB6/7) • Two USB 3.1 Gen2 ports on the rear I/O panel (USB8/9) • One front accessible USB 3.1 Gen2 header (USB10) • One front accessible USB 3.1 Gen2 port (USB11: Type A)	
BIOS	
• 256Mb AMI BIOS® SPI Flash BIOS • ACPI 6.0, Plug and Play (PnP), BIOS rescue hot-key, riser card auto detection support, and SMBIOS 3.0 or later	
Power Management	
• ACPI power management • Power button override mechanism • Power-on mode for AC power recovery • Wake-on-LAN • Power supply monitoring	
System Health Monitoring	
• Onboard voltage monitoring for +12V, +5V, +3.3V, CPU, Memory, VBAT, +5V stdby, +3.3V stdby, +1.8V PCH, +1.05V PCH, +1.0V PCH, CPU temperature, VRM temperature, LAN temperature, PCH temperature, system temperature, and memory temperature • 6 CPU switch phase voltage regulator • CPU thermal trip support • Platform Environment Control Interface (PECI)/TSI	
Fan Control	
• Fan status monitoring via IPMI connections • Single cooling zone • Multi-speed fan control via onboard BMC • Ten 4-pin fan headers and one 12V pump connector	
System Management	
• Trusted Platform Module (TPM) support • SuperDoctor® 5 • Chassis Intrusion header and detection • Server Platform Service	

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

Motherboard Features
LED Indicators
• Onboard Power LED • UID LED • BMC Heartbeat LED • M.2 LED
Dimensions
• 13" (W) x 12" (L) EATX

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

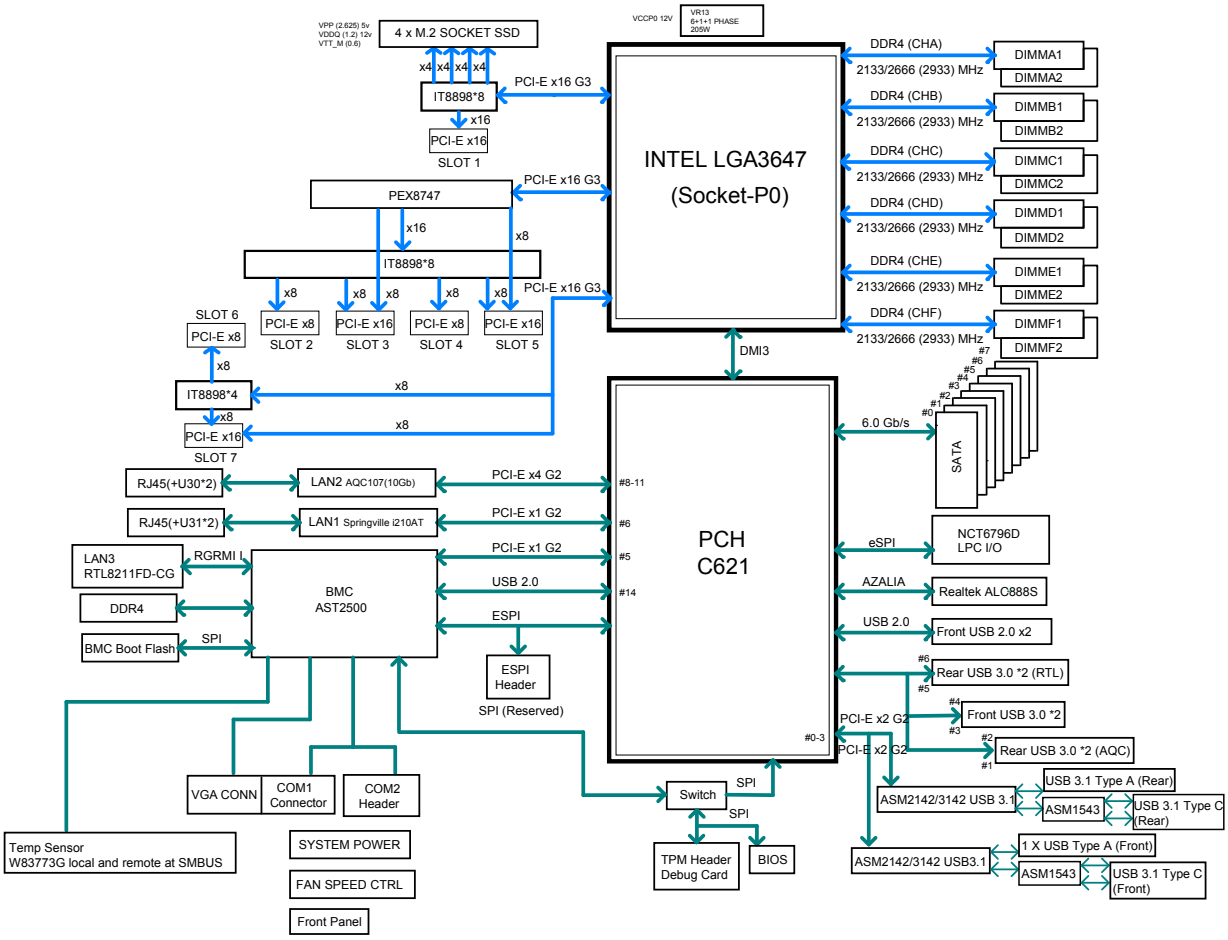
Note 2: For IPMI configuration instructions, please refer to the Embedded IPMI Configuration User's Guide available at http://www.supermicro.com/support/manuals/.

Note 3: 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.

Note 4: X11SPA-T does not support Out of Band (OOB) flash BIOS.

Note 5: For proper BMC configuration, please refer to https://www.supermicro.com/products/nfo/files/IPMI/Best_Practices_BMC_Security.pdf.

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 SP series (Socket P0-LGA3647) processor and the Intel PCH C621 chipset, the X11SPA-TF/-T motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users.

With the support of the new Intel Microarchitecture 14nm Process Technology, the X11SPA-TF/-T dramatically increases system performance for a multitude of server applications.

The Intel PCH C621 chipset provides Enterprise SMBus support, including the following features:

- DDR4 288-pin memory support
- 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 3.0 for advanced power monitoring, capping, and management for BMC enhancement (see note below).
- BMC supports remote management, virtualization, and the security package for enterprise platforms

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

Features Supported by Intel Xeon Scalable-SP Processors

Intel Xeon Scalable-SP processors support the following features:

- Intel AVX-512 instructions support to handle complex workloads
- 1.5x memory bandwidth increased to 6 channels
- Hot plug and enclosure management with Intel Volume Management Device (Intel VMD)
- Rich set of available IOs with increased PCIe lanes (48 lanes)
- Integrated Intel Ethernet Connection X722 with iWARP RDMA

New Features Supported by the 2nd Gen Intel Xeon Scalable-SP Processors

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

- Higher performance for a wider range of workloads with per-core performance increase
- Support of Optane™ DC Persistent Memory (DCPMM) with affordable, persistent, and large capacity (Refer to Section 1.8 for more details.)
- Up to 2933 MHz memory supported
- Vector Neutral 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 selected 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

Recovery from AC Power Loss

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

1.4 System Health Monitoring

Onboard Voltage Monitors

An onboard voltage monitor will scan the voltages of the onboard chipset, memory, CPU, and battery continuously. If a voltage becomes unstable, a warning will be given, or an error message will be sent to the screen. The user can adjust the voltage thresholds to define the sensitivity of the voltage monitor.

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

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

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

System Resource Alert

This feature is available when used with SuperDoctor 5 in the Windows® OS or in the Linux® environment. SuperDoctor is used to notify the user of certain system events. For example, you can configure SuperDoctor to provide you with warnings when system temperatures, CPU temperatures, voltages, or 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 CD-ROMs, network cards, hard disk drives, and printers.

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

1.6 Power Supply

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

The X11SPA-TF/-T motherboard accommodates a 24-pin ATX power supply. Although most power supplies generally meet the specifications required by the CPU, some are inadequate. In addition, three 12V 8-pin power connections (JPWR1/JPWR3/JPWR4) are also required to ensure adequate power supply to the system.

> **Warning:** To prevent damage to the power supply and the motherboard, please use power supplies that contain 24-pin and 8-pin power connectors. Be sure to connect the power supply to the 24-pin power connector (JPWR2) and all the 8-pin power connectors (JPWR1/JPWR3/JPWR4) when more than four of the PCIe slots are populated. The connections of these 8-pin connectors should be JPWR1, JPWR3, and JPWR4 in sequence. Note that the power connectors provided by power supply may vary. You may connect the 8-pin connector using the bundled GPU to CPU power cable to the power supply. This cable is an adapter converting the connector on the power supply to the 8-pin power connector on the motherboard. Failure in doing so may void the manufacturer warranty on your power supply and motherboard. Refer to the checklist table on page 7 and contact Supermicro for more detailed cable information.

It is strongly recommended that you use a high quality power supply that meets ATX power supply Specification 2.02 or above. It must also be SSI compliant. For more information, please refer to the website at http://www.ssiforum.org/.

1.7 Serial Port

The X11SPA-TF/-T motherboard supports two serial communication connections. COM port (COM1) and header (COM2) can be used for input/output. The UART provides legacy speeds with a baud rate of up to 115.2 Kbps as well as an advanced speed with baud rates of 250 K, 500 K, or 1 Mb/s, which support high-speed serial communication devices.

1.8 Intel Optane 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 capacity for high performance computing platform with flexible configuration options.

Chapter 2

Installation

2.1 Static-Sensitive Devices

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

Precautions

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

Unpacking

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

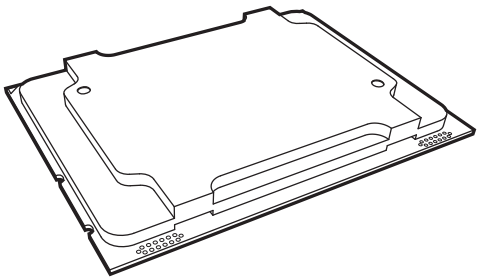
2.2 Processor and Heatsink Installation

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

Notes:

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

The Intel Xeon SP Series Processor

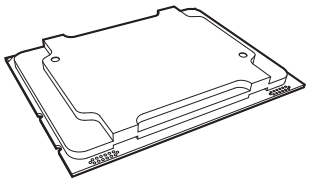


Non-Fabric Model

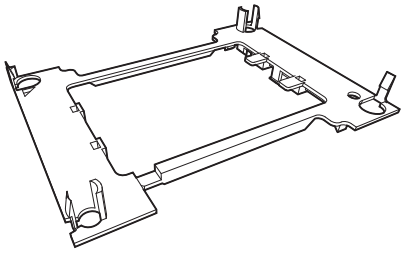
Overview of the Processor Carrier Assembly

The processor carrier assembly contains the Intel Xeon Non-Fabric (Non-F) processor and a processor carrier.

1. Non-F Processor



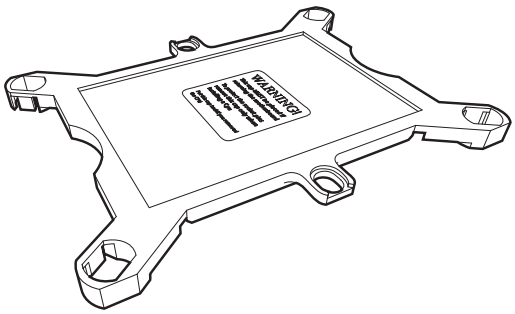
2. Processor Carrier



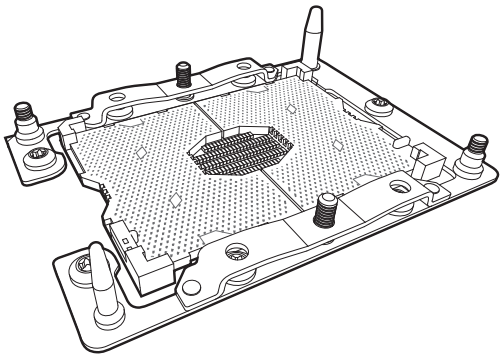
Overview of the CPU Socket

The CPU socket is protected by a plastic protective cover.

1. Plastic Protective Cover



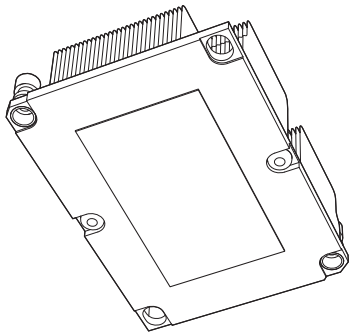
2. CPU Socket



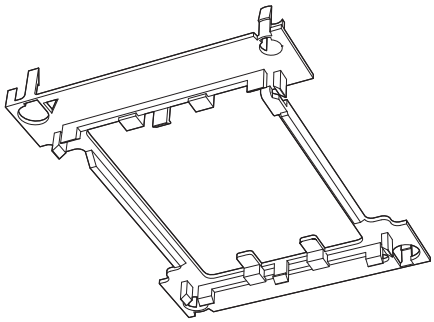
Overview of the Processor Heatsink Module

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

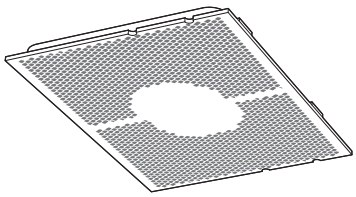
1. Heatsink with Thermal Grease



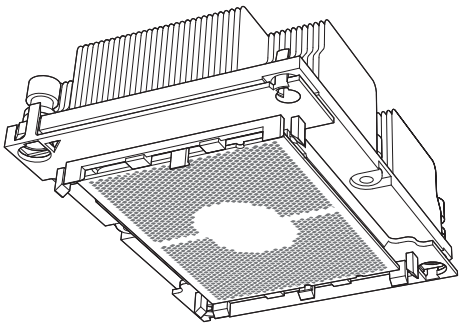
2. Processor Carrier



3. Non-F Processor



Processor Heatsink Module



Bottom View

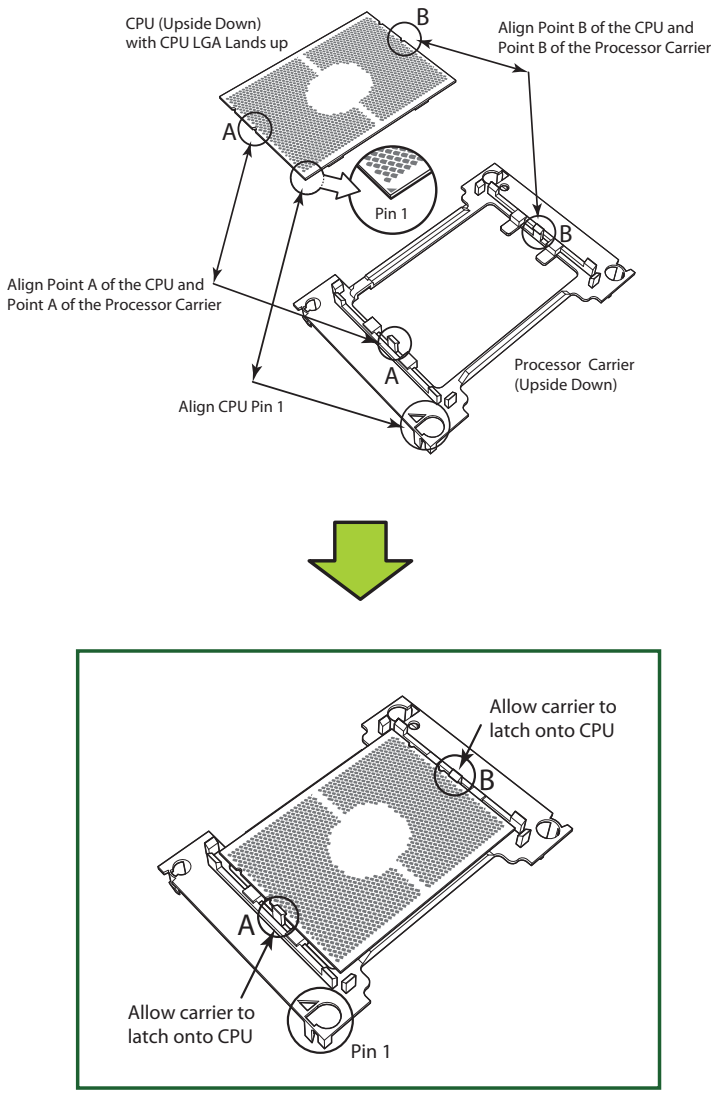
Creating the Non-F Model Processor Carrier Assembly

To install a Non-F model processor into the processor carrier, follow the steps below:

1. Hold the processor with the LGA lands (gold contacts) facing up. Locate the small, gold triangle in the corner of the processor and the corresponding hollowed triangle on the processor carrier. These triangles indicate pin 1. See the images below.

2. Using the triangles as a guide, carefully align and place Point A of the processor into Point A of the carrier. Then gently flex the other side of the carrier for the processor to fit into Point B.

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



Processor Carrier Assembly (Non-F Model)

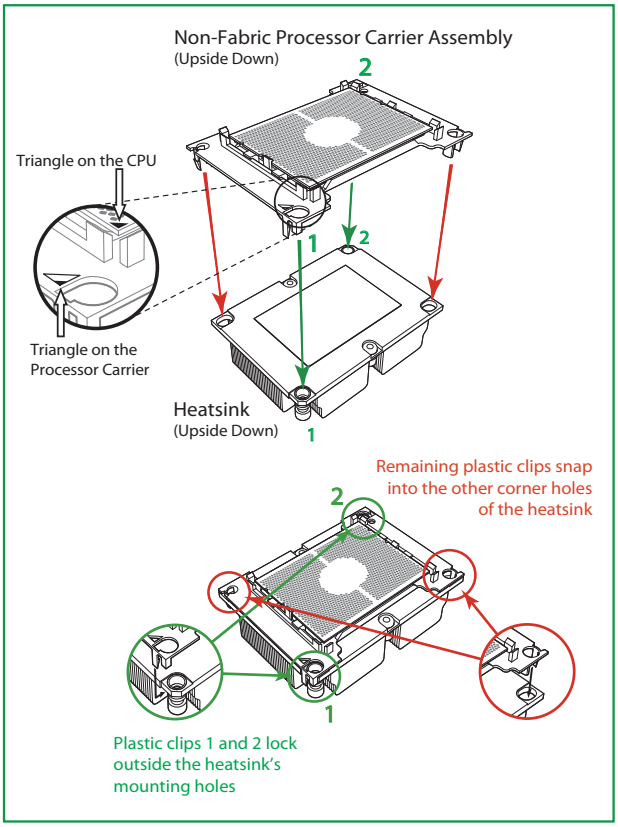
Assembling the Processor Heatsink Module

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

1. Note the label on top of the heatsink, which marks the heatsink mounting holes as 1, 2, 3, and 4. If this is a new heatsink, the thermal grease has been pre-applied on the underside. Otherwise, apply the proper amount of thermal grease.

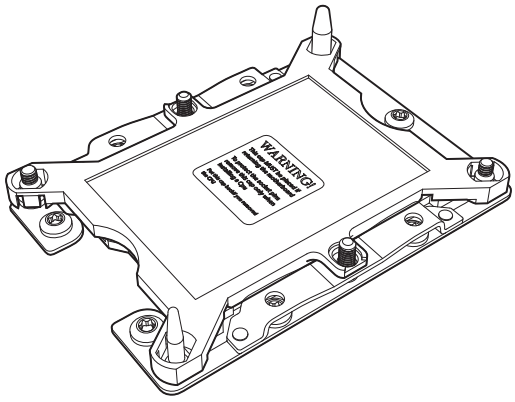
2. Turn the heatsink over with the thermal grease facing up. Hold the processor carrier assembly so the processor's gold contacts are facing up, then align the triangle on the assembly with hole 1 of the heatsink. Press the processor carrier assembly down. The plastic clips of the assembly will lock outside of holes 1 and 2, while the remaining clips will snap into their corresponding holes.

3. Examine all corners to ensure that the plastic clips on the processor carrier assembly are firmly attached to the heatsink.

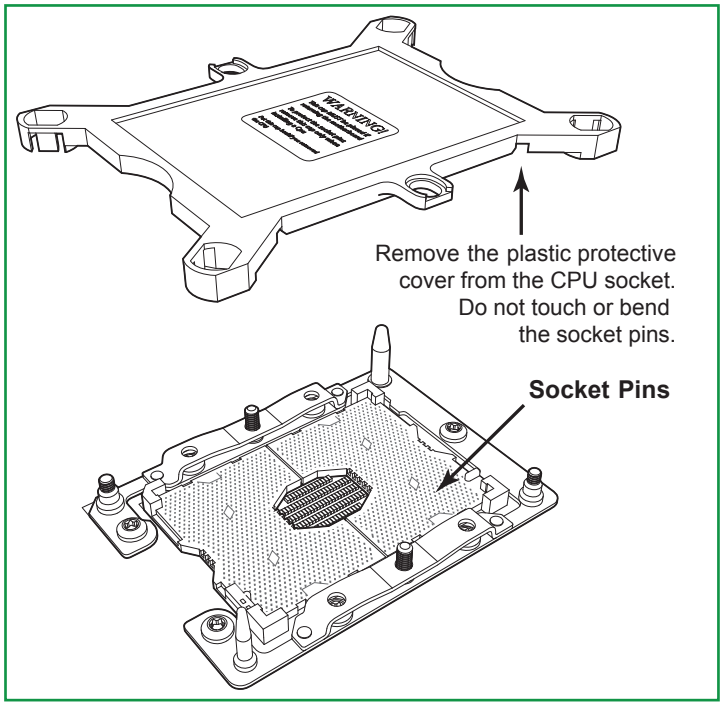


Preparing the CPU Socket for Installation

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



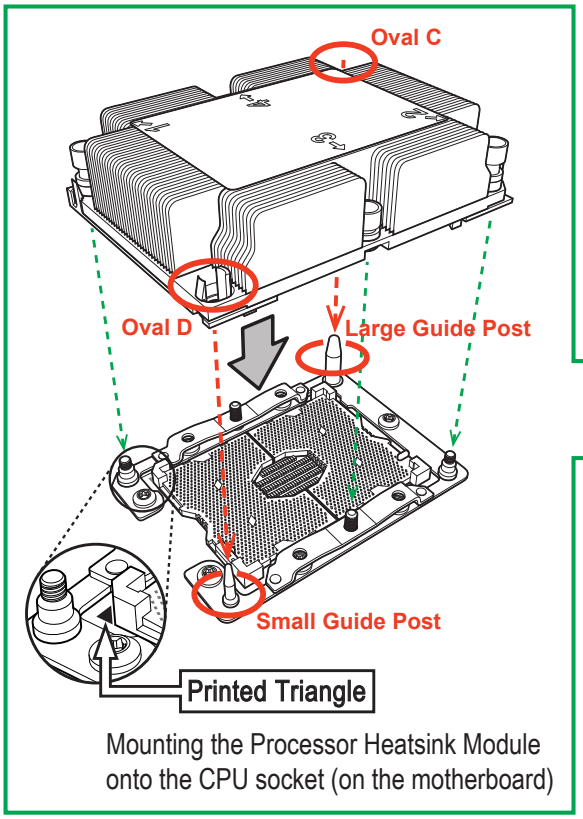
CPU Socket with Plastic Protective Cover



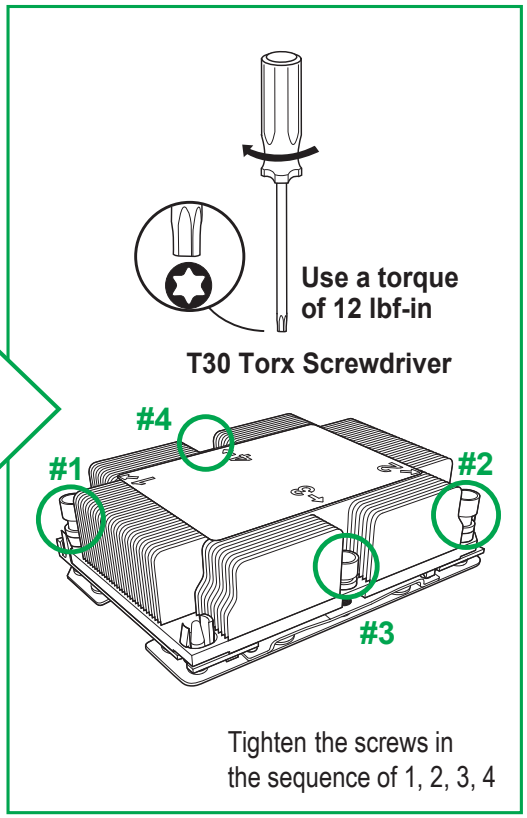
Installing the Processor Heatsink Module

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

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



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



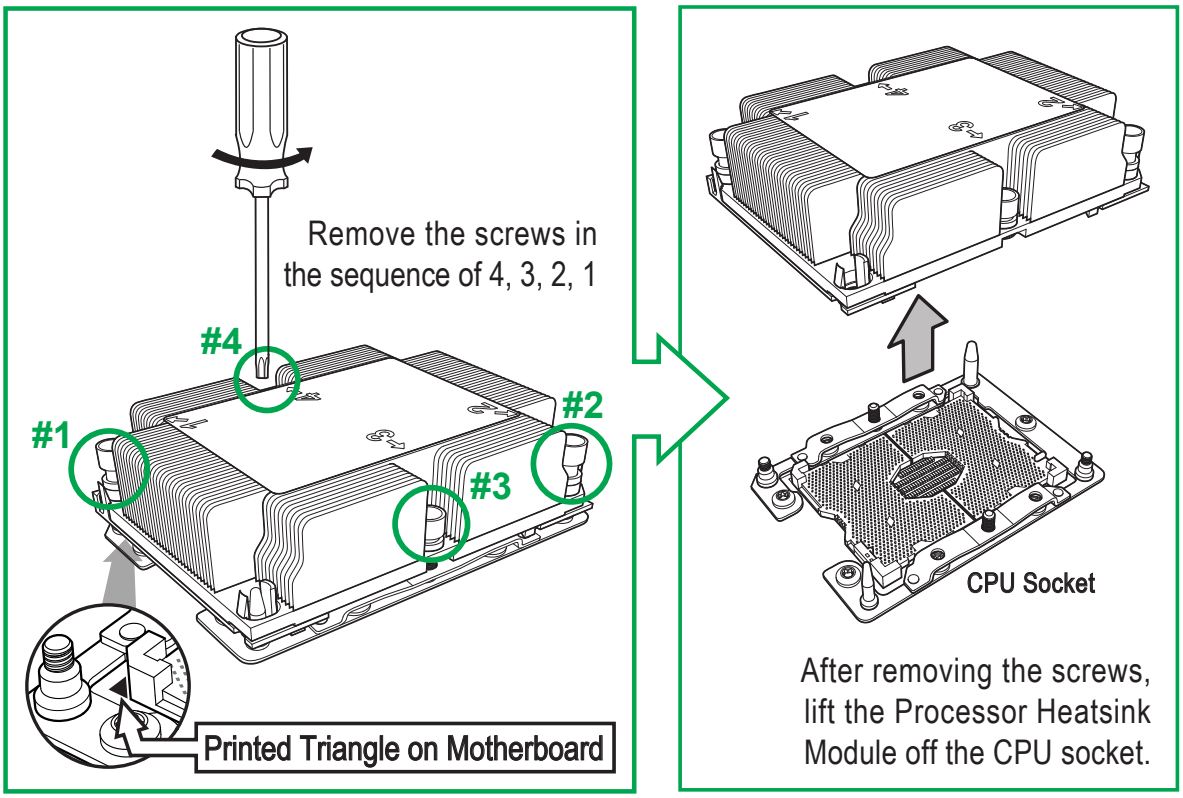
Tighten the screws in the sequence of 1, 2, 3, 4

Removing the Processor Heatsink Module

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

1. Use a T30 Torx-bit screwdriver to loosen the four screws in a backwards sequence of #4, #3, #2, and #1.

2. Gently lift the PHM upwards to remove it from the socket.



2.3 Motherboard Installation

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

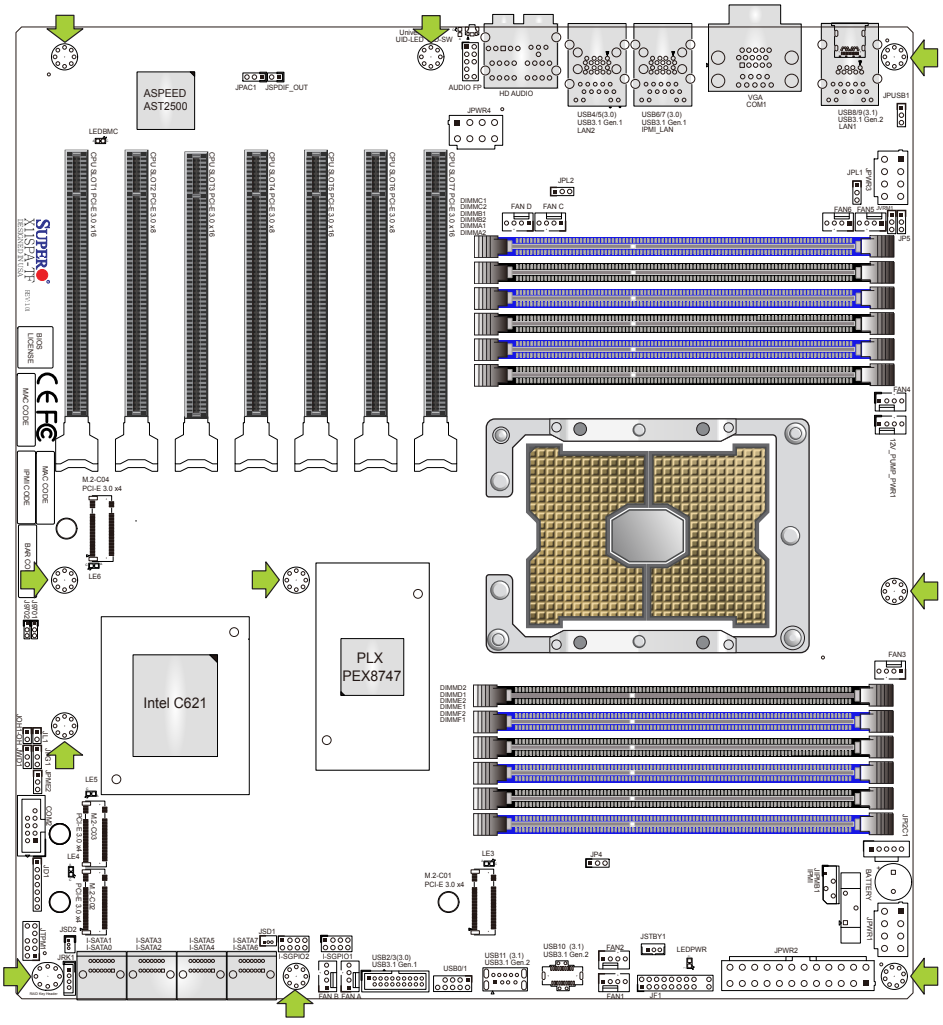
Tools Needed

Phillips Screwdriver (1)

Phillips Screws (10)

Standoffs (10) Only if Needed

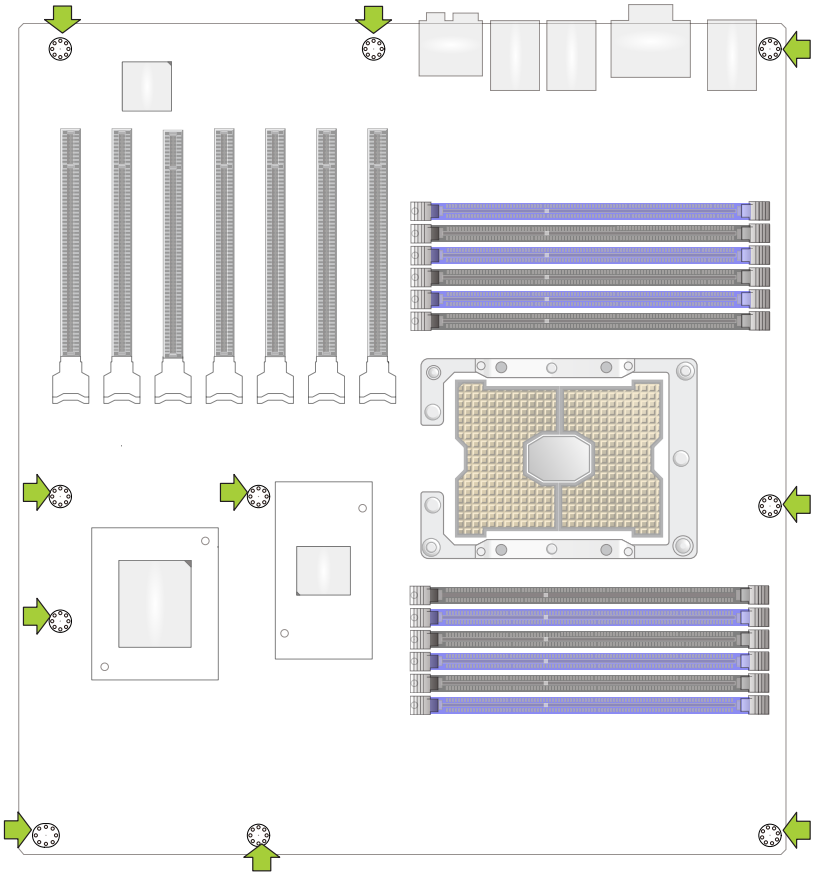
Location of Mounting Holes



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

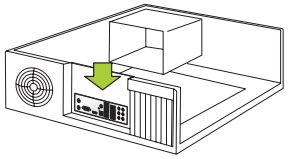
Note 2: Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

Note 3: Before assembling the motherboard, pay attention to the location of mounting holes. Please select the chassis which fits the mounting hole locations of this motherboard. Refer to the illustration below for the location details.

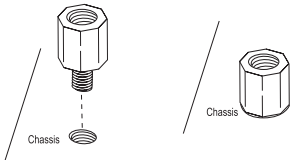


Installing the Motherboard

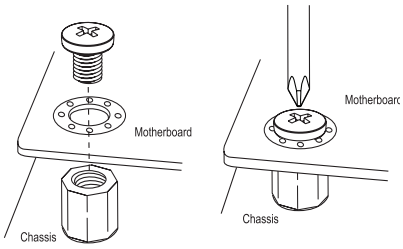
1. Install the I/O shield into the back of the chassis, if applicable.



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



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



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

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

2.4 Memory Support and Installation

Note: Check the Supermicro website for recommended memory modules.

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

Memory Support

The X11SPA-TF/-T supports up to 768GB of ECC RDIMM, 3TB of 3DS RDIMM, 1.5TB of LRDIMM, and 3TB of 3DS LRDIMM DDR4 (288-pin) ECC memory with speeds of up to 2933MHz in 12 memory slots. Refer to the tables below for the recommended DIMM population order and additional memory information. (1DPC and 2DPC are recommended for memory installation. Only selected 2nd Gen Intel Xeon Scalable-SP processors support Intel DC Persistent memory.)

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

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 the black slots. To maximize memory capacity and performance, please populate all DIMM slots on the motherboard, including all blue and black slots.

General Memory Population Requirements

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

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

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 the 81xx/61xx/51xx/41xx/31xx Platform

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 the 82xx/62xx/52xx/42xx/32xx Platform (W-32xx is supported by X11SPA-T only)

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

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 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, or across different sockets. • Mixing of non-3DS and 3DS LRDIMM is not allowed in the same channel, across different channels, or 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

Memory Population

Memory Population Table for the X11SPA-T/-TF (w/12 Slots) based on the 81xx/61xx/51xx/41xx/31xx and 82xx/62xx/52xx/42xx/32xx Platforms (W-32xx is supported by X11SPA-T only)

Memory Population Table for the X11SPA-T/-TF (w/12 Slots)	
	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

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

DCPMM (Intel Optane™ DC Persistent Memory Modules) Population Table for the X11SPA-T/-TF Motherboards (w/12 Slots) based on the 82xx/62xx/52xx/42xx Platform

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.

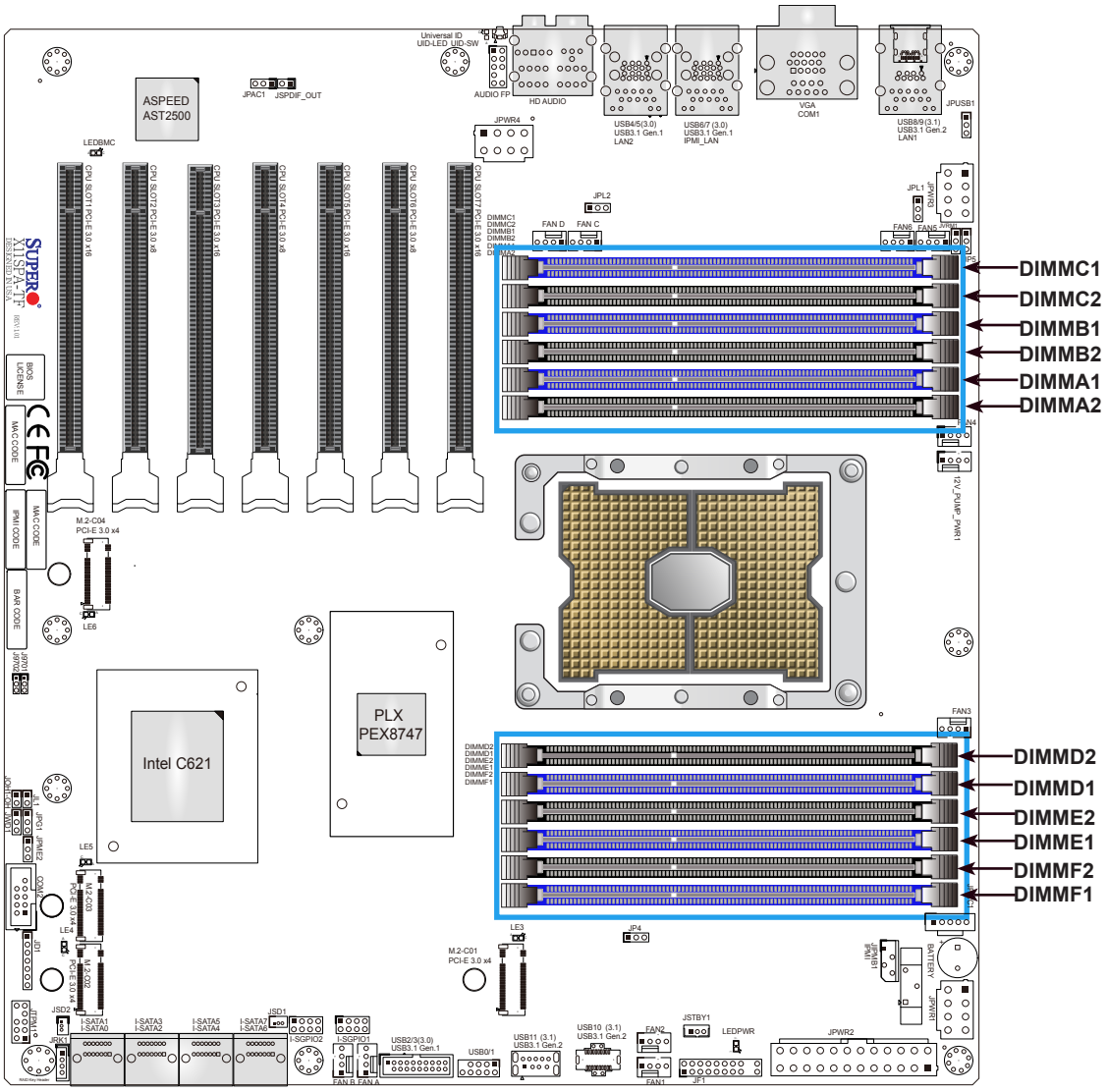
Legend (for the first two tables above)	
	Capacity
DCPMM	Any Capacity (Uniformly for all channels for a given configuration)

- 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

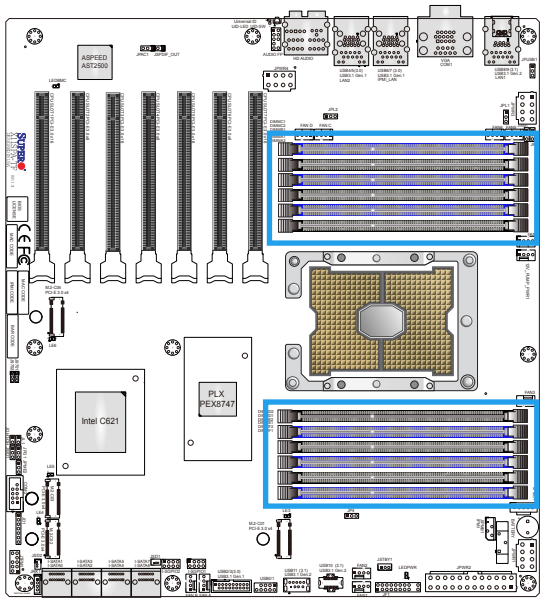
General Guidelines for Optimizing Memory Performance

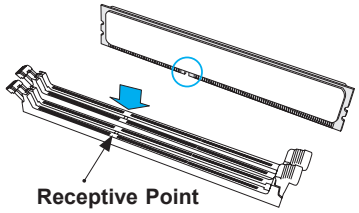
- The blue slots must be populated first.
- Only populate DIMMA2 and DIMMD2 if the extra memory support is needed.
- Always use DDR4 memory of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- The motherboard will support odd-numbered modules (one or three modules installed). However, to achieve the best memory performance, a balanced memory population is recommended.



DIMM Installation

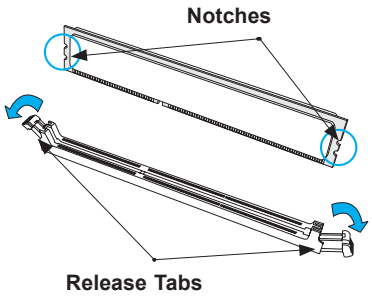
1. Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population tables on pages 33, 34, 35, 36, and 37.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.
3. Align the key of the DIMM module with the receptive point on the memory slot.
4. Press the notches on both ends of the module straight down into the slot until the module snaps into place.
5. Press the release tabs to the lock positions to secure the DIMM module into the slot.

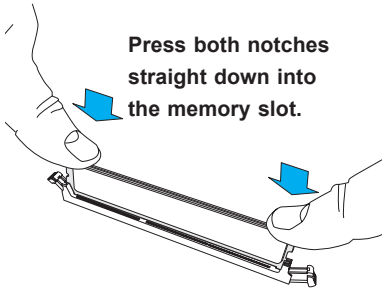




DIMM Removal

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

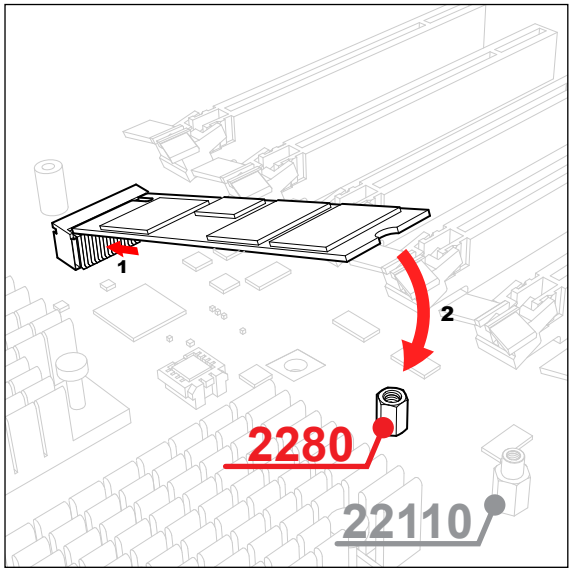




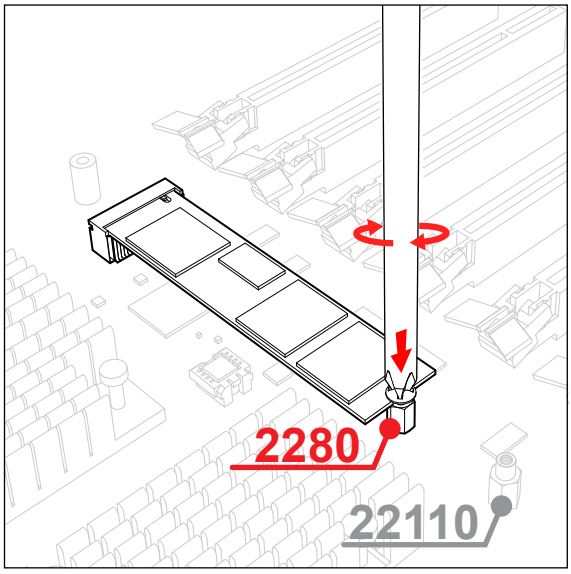
2.5 M.2 SSD Installation

The X11SPA-TF/T motherboard has four M.2 PCIe 3.0 sockets that support 2260, 2280, and 22110 SSD modules. By default, two standoffs are pre-installed into the positions of 2280 and 22110 mounting holes. Follow the steps below to install the M.2 SSD module according to the length specification of the M.2 module.

2280 SSD Module Installation

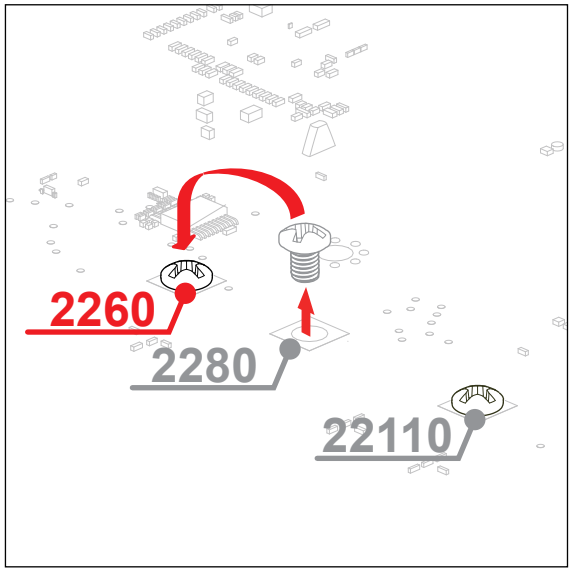


1. To install a 2280 SSD module, insert it into the slot at a 30 degree angle and press down.

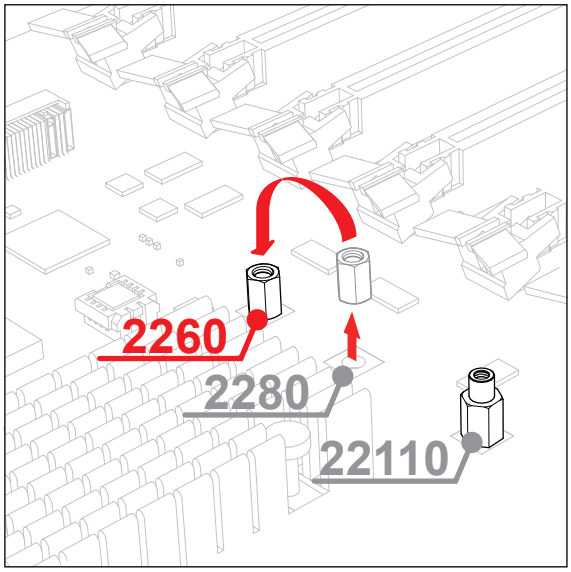


2. With the cutoff circle at the end of the module aligned with the standoff, tighten the screw to secure the module. Go to the section of heatsink installation to complete the installation.

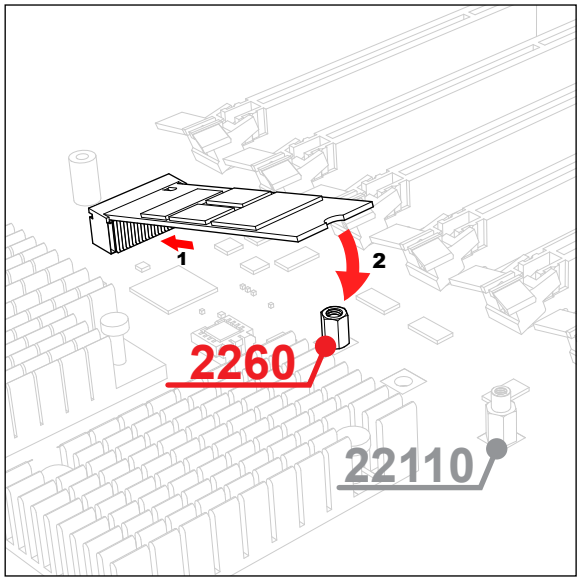
2260 SSD Module Installation



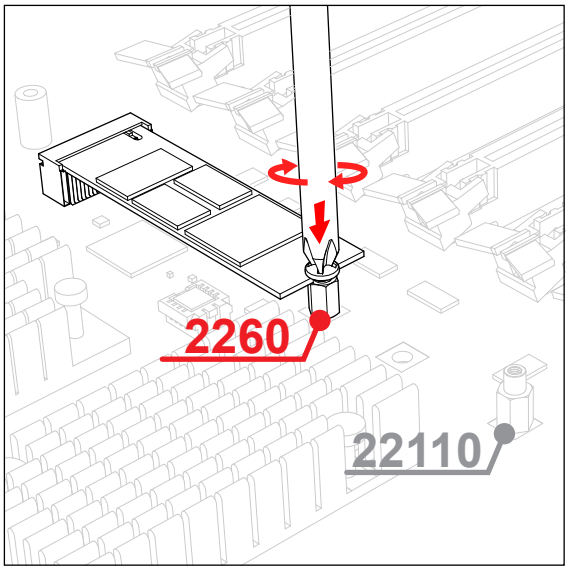
1. Loose and relocate the screw from the position of 2280 to 2260 mounting hole on the bottom of the motherboard.



2. Re-install the standoff to the screw located at the position of 2260 mounting hole on the motherboard.

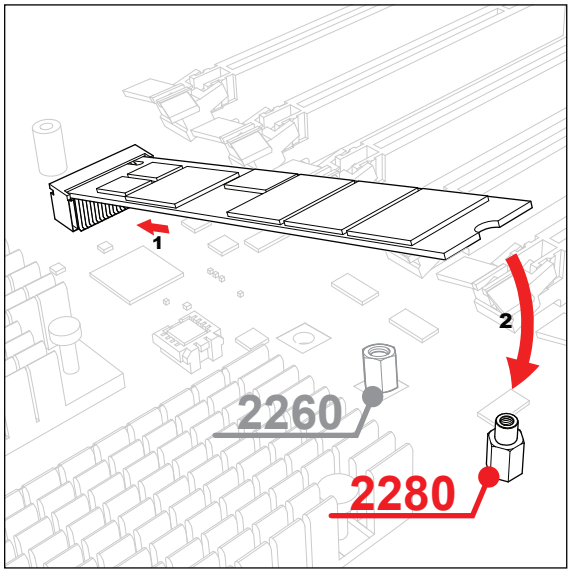


3. To install a 2260 SSD module, insert it into the slot at a 30 degree angle and press down.

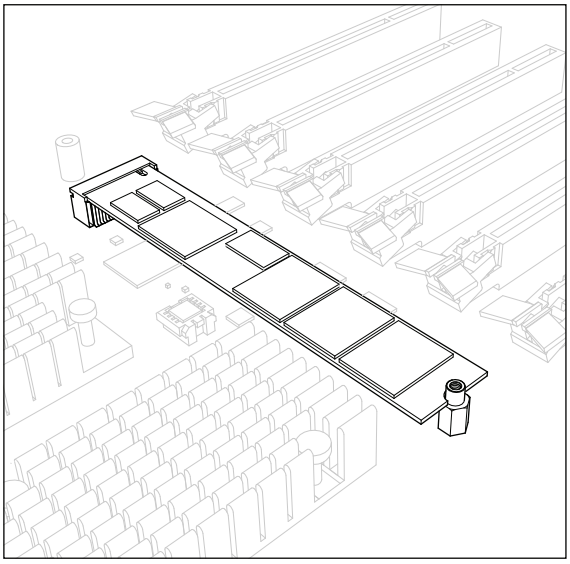


4. With the cutoff circle at the end of the module aligned with the standoff, tighten the screw to secure the module. Go to the section of heatsink installation to complete the installation.

22110 SSD Module Installation

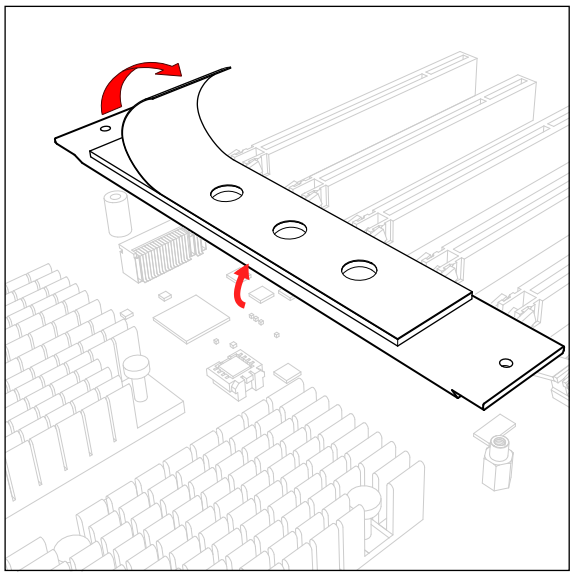


1. To install a 22110 SSD module, insert it into the M.2 socket at a 30 degree angle and align the cutoff circle at the end with the standoff.

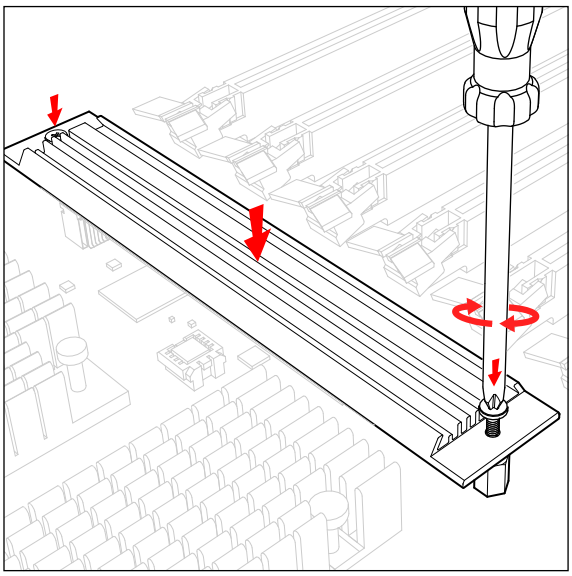


2. Go to the section of heatsink installation to complete the installation.

Heatsink Installation



1. Remove the plastic liner from the heatsink's thermal pad.



2. With the thermal pad faced down, secure the heatsink on top of the module.

2.6 Rear I/O Ports

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

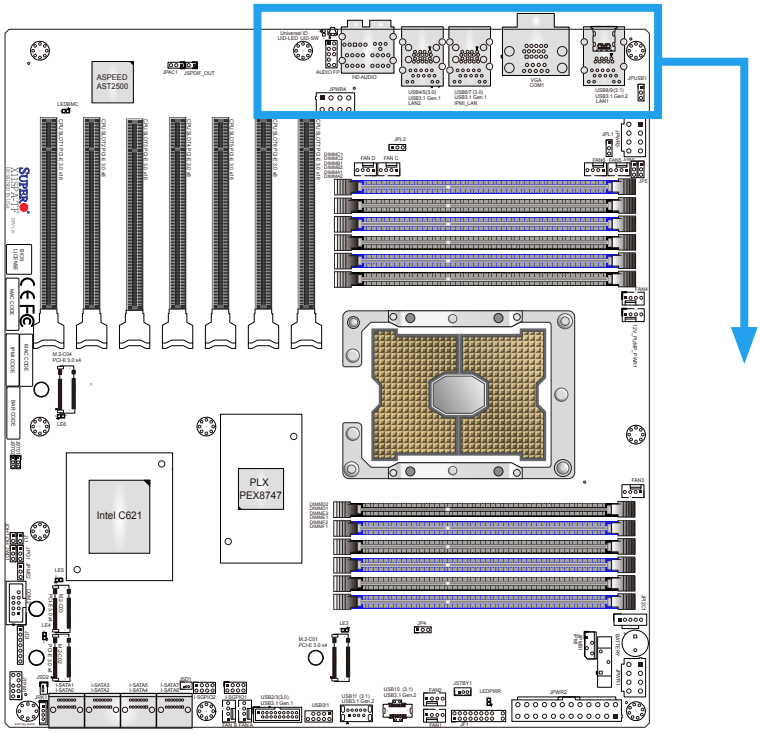
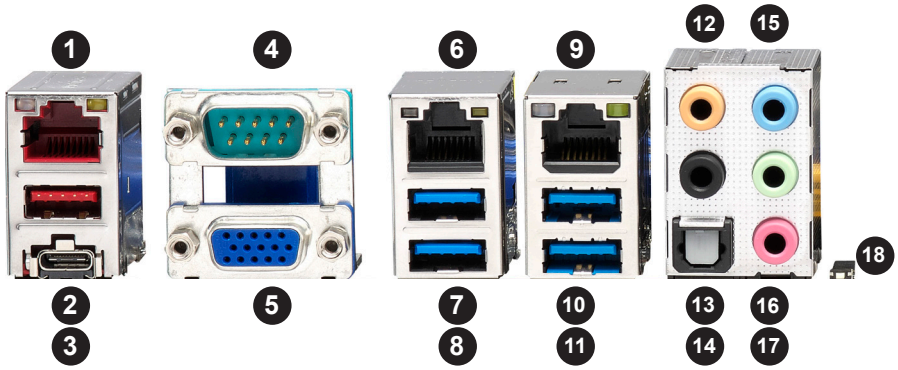


Figure 2-1. I/O Port Locations and Definitions



#	Description	#	Description	#	Description
1	1Gb RJ45 Port 1	7	USB 3.1 Gen1 Port 7	13	Surround Out
2	USB 3.1 Gen2 Port 9	8	USB 3.1 Gen1 Port 6	14	S/PDIF Out
3	USB 3.1 Gen2 Port 8 (Type C)	9	10Gb RJ45 Port2	15	Line In
4	COM1 Port	10	USB 3.1 Gen1 Port 5	16	Line Out
5	VGA Port	11	USB 3.1 Gen1 Port 4	17	Mic In
6	Dedicated IPMI LAN Port	12	Center/LFE Out	18	UID Switch

VGA Port

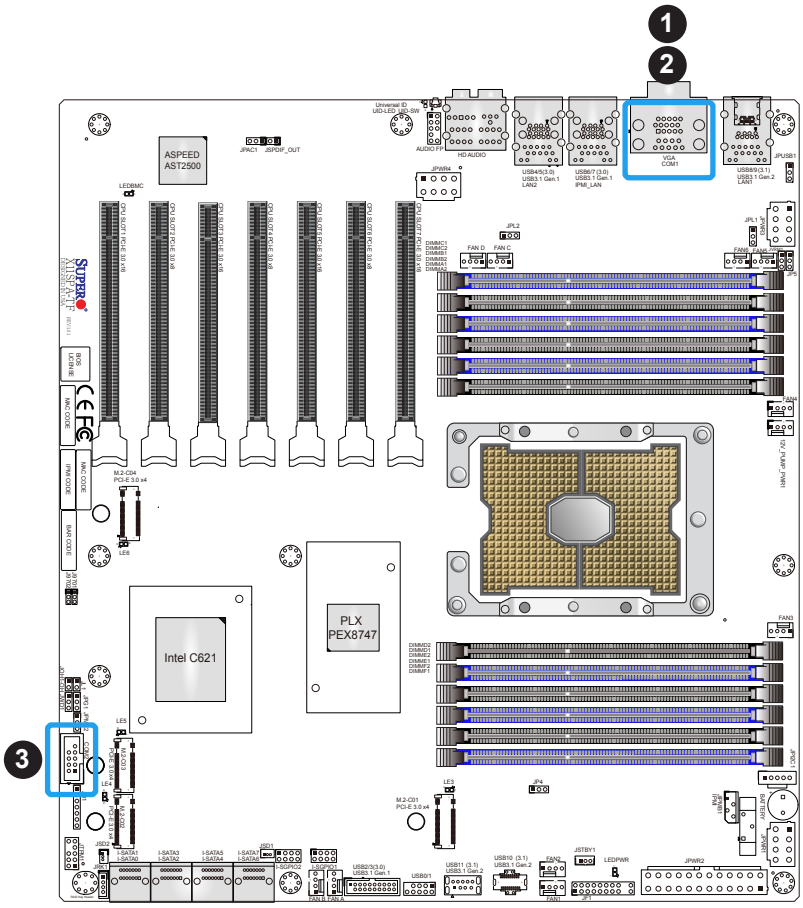
A video (VGA) port is located next to USB 3.1 Gen2 Port 8 (Type C) on the I/O back panel. Refer to the motherboard layout below for the location.

COM Connections

Two COM connections (COM1/COM2) are located on the motherboard. COM1 is located on the I/O back panel. COM2 is located next to M.2-C03 PCIe 3.0 x4.

COM Connection 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. COM1 Port
3. COM2 Header

LAN Ports

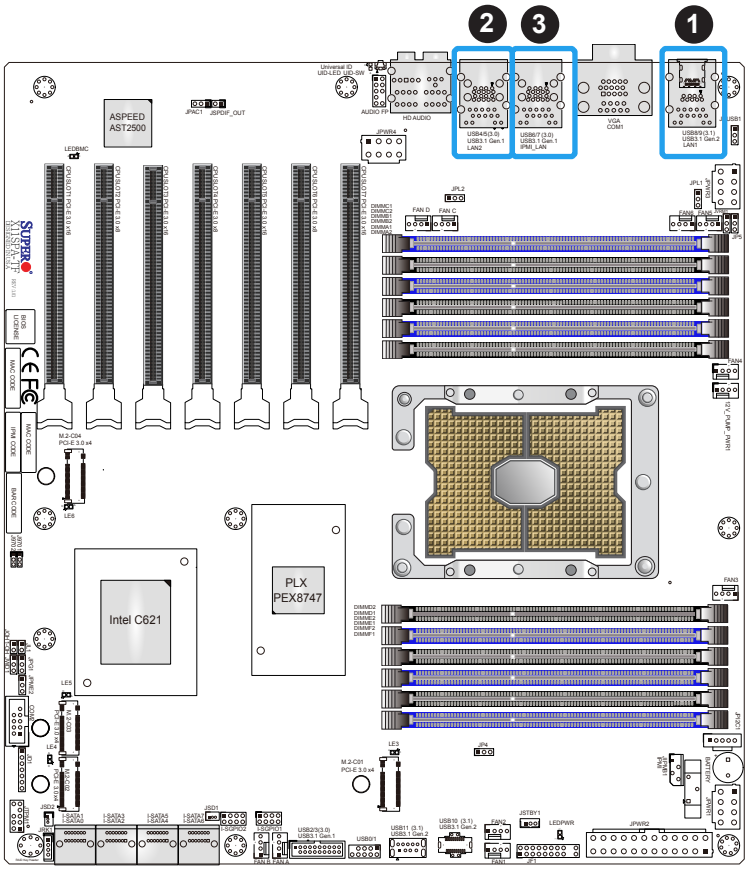
Two RJ45 Ethernet LAN ports (LAN1/LAN2) are located on the I/O back panel. In addition, a Dedicated IPMI LAN port is located above the USB6/7 ports on the I/O back panel. All of these ports accept RJ45 cables. Please refer to Section 2.10 for LAN LED information.

LAN Port Pin Definitions

Pin#	Definition	Pin#	Definition
1	TD0-	11	P3V3_Dual
2	TD0+	12	Act LED (Yellow)
3	TD1-	13	Link 1000 (Amber)
4	TD1+	14	Link 100 LED (Green)
5	TD2-	15	GND
6	TD2+	16	GND
7	TD3-	17	GND
8	TD3+	18	GND
9	COMMCT		
10	GND		

IPMI LAN Port Pin Definitions

Pin#	Definition	Pin#	Definition
9		19	GND
10	TD0+	20	Act LED (Yellow)
11	TD0-	21	Link 100 LED (Green)
12	TD1+	22	Link 1000 LED (Amber)
13	TD1-	23	SGND
14	TD2+	24	SGND
15	TD2-	25	SGND
16	TD3+	26	SGND
17	TD3-		
18	GND		



1. LAN1
2. LAN2
3. IPMI LAN Port

Universal Serial Bus (USB) Ports

There are four USB 3.1 Gen1 ports (USB4/5, USB6/7) and two USB 3.1 Gen2 ports (USB8/9) located on the I/O back panel. The motherboard also has one front access USB 3.1 Gen2 header (USB10), one front access USB 3.1 Gen2 port (USB11, Type A), one front access USB 3.1 Gen1 header (USB2/3), and one front access USB 2.0 header (USB0/1). The onboard headers and port can be used to provide front side USB access with a cable (not included). Refer to the tables below for pin definitions.

USB0/1 (2.0) Header Pin Definitions

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

USB2/3 (3.1 Gen1) Header Pin Definitions

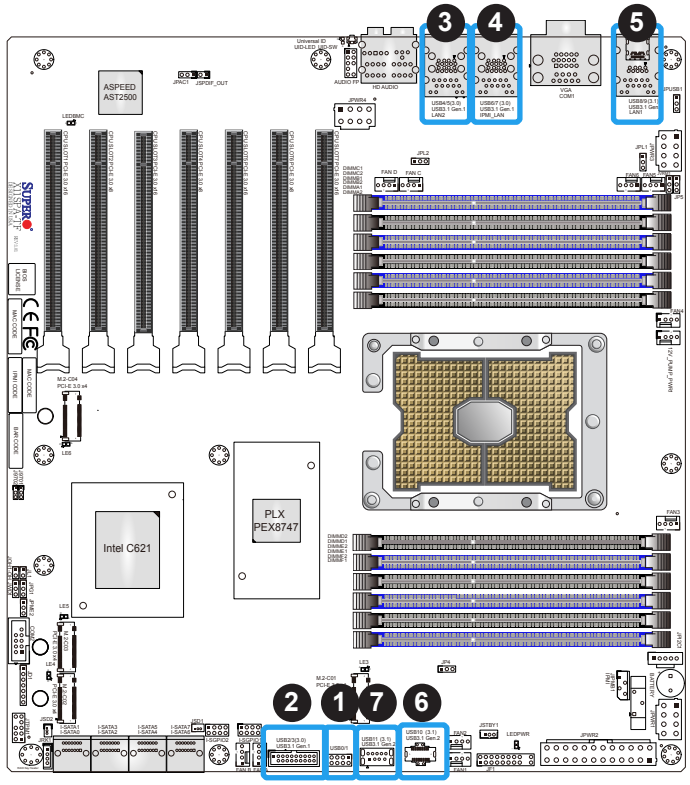
Pin#	Definition	Pin#	Definition
1	+5V	2	+5V
3	USB_N	4	USB_N
5	USB_P	6	USB_P
7	Ground	8	Ground
9	Key	10	NC

USB10 (3.1 Gen2) Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	11	VBUS
2	TX1+	12	TX2+
3	TX1-	13	TX2-
4	GND	14	GND-
5	RX1+	15	RX2+
6	RX1-	16	RX2-
7	VBUS	17	GND
8	CC1	18	D-
9	SBU1	19	D+
10	SBU2	20	CC2

USB11 (3.1 Gen1) Port Pin Definitions

Pin#	Definition	Pin#	Definition
1	VBUS	5	Stda_SSTX-
2	Stda_SSRX-	6	Stda_SSTX+
3	Stda_SSRX+	7	GND
4	GND	8	D-
		9	D+



1. USB0/1
2. USB2/3
3. USB4/5
4. USB6/7
5. USB8/9
6. USB10
7. USB11

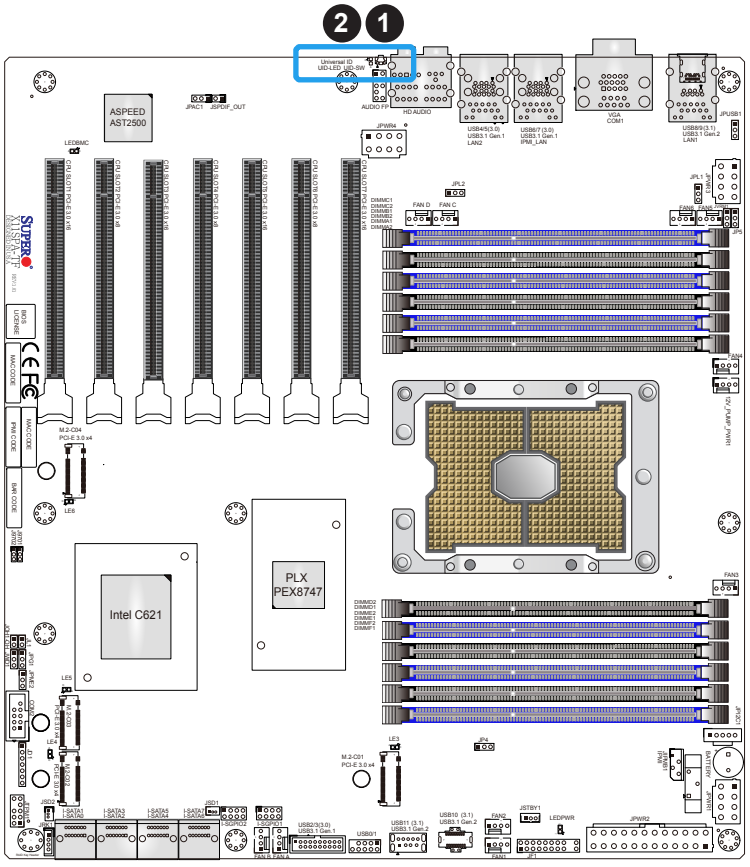
Unit Identifier Switch/UID LED Indicator

A Unit Identifier (UID) switch and an LED indicator are located on the motherboard. The UID switch is located at UID-SW, which is next to the HD AUDIO ports on the back panel. The UID-LED is located next to the switch. When you press the UID switch, the UID LED will be turned on. Press the UID switch again to turn off the LED indicator. The UID indicator provides 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 LED Indicator	
Color	**Status**
Blue: On	Unit Identified



1. UID Switch
2. UID LED

2.7 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.

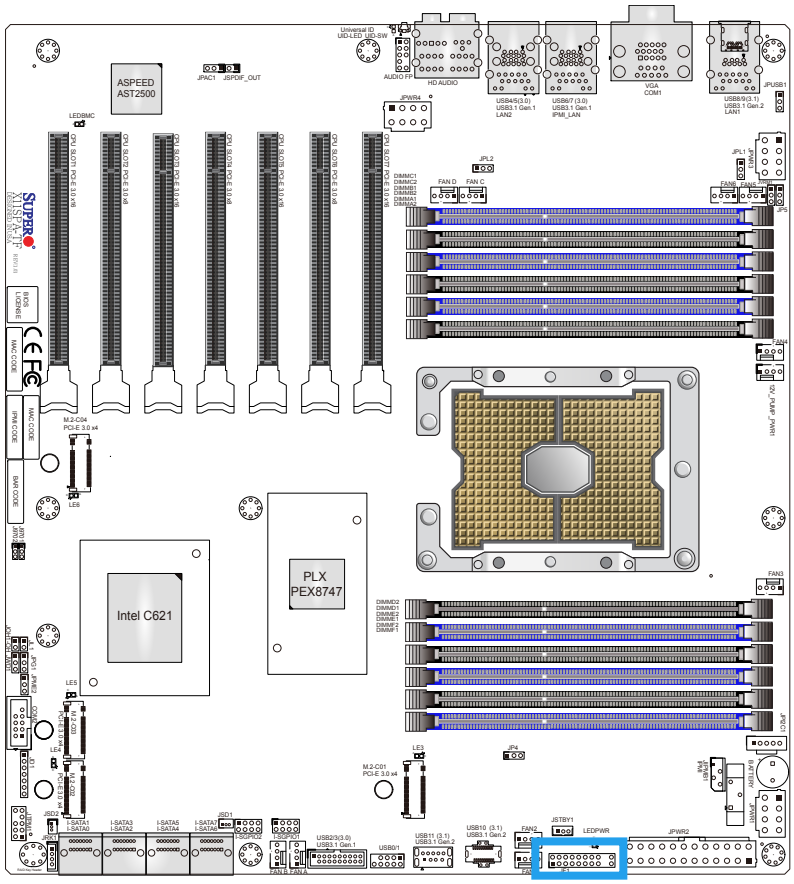
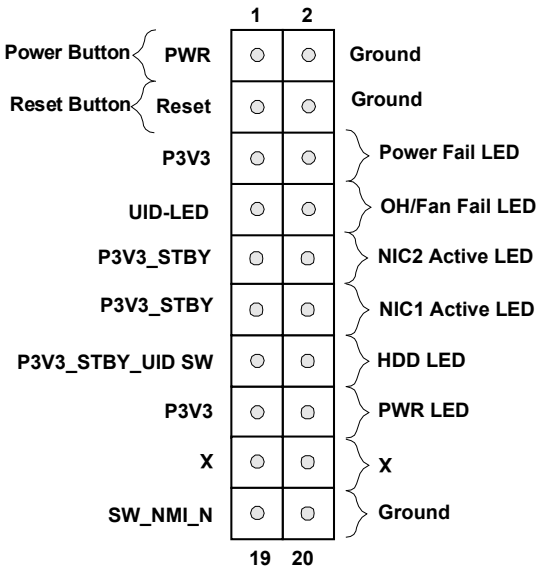


Figure 2-2. JF1 Header Pins



Power Button

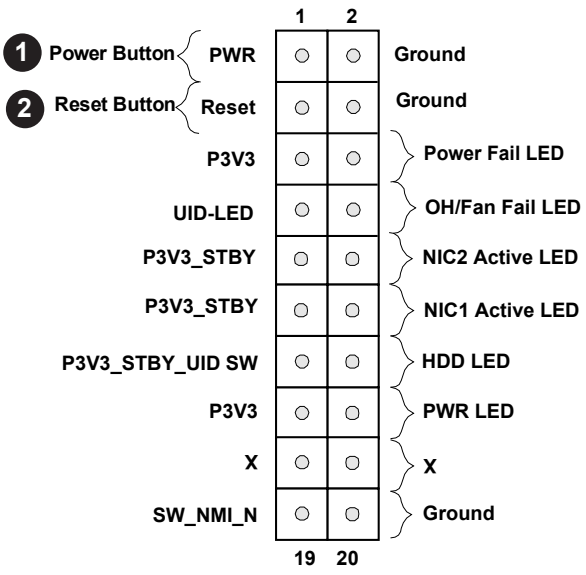
The Power Button connection is located on pins 1 and 2 of JF1. Momentarily contacting both pins will power on/off the system. This button can also be configured to function as a suspend button (with a setting in the BIOS - see Chapter 4). To turn off the power when the system is in suspend mode, press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

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

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)	
Pins	Definition
3	Reset
4	Ground



1. PWR Button
2. Reset Button

Power Fail LED

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

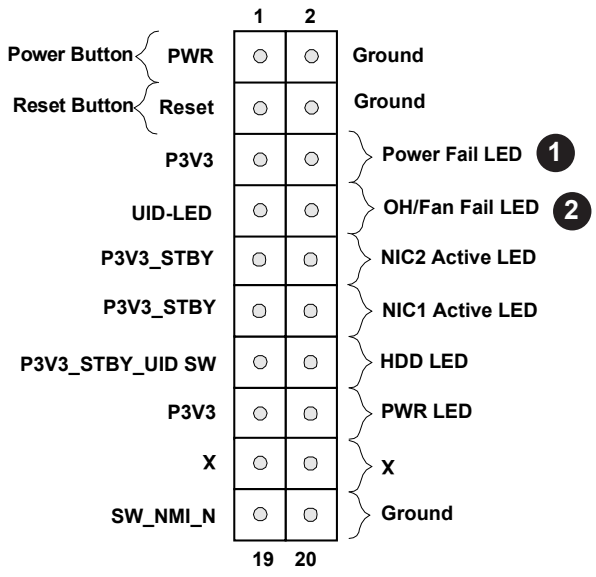
Power Fail LED Pin Definitions (JF1)	
Pin#	**Definition**
5	3.3V
6	PWR Supply Fail

Overheat (OH)/Fan Fail LED

Connect an LED cable to pins 7 and 8 of the Front Control Panel to use the Overheat/Fan Fail LED connections. The LED on pin 8 provides warnings of overheating or fan failure. Refer to the tables below for pin definitions.

OH/Fan Fail Indicator Status	
State	**Definition**
Off	Normal
On	Overheat
Flashing	Fan Fail

OH/Fan Fail LED Pin Definitions (JF1)	
Pin#	**Definition**
7	Blue LED
8	OH/Fan Fail LED



1. Power Fail LED
2. OH/Fan Fail LED

NIC1/NIC2 (LAN1/LAN2) LED

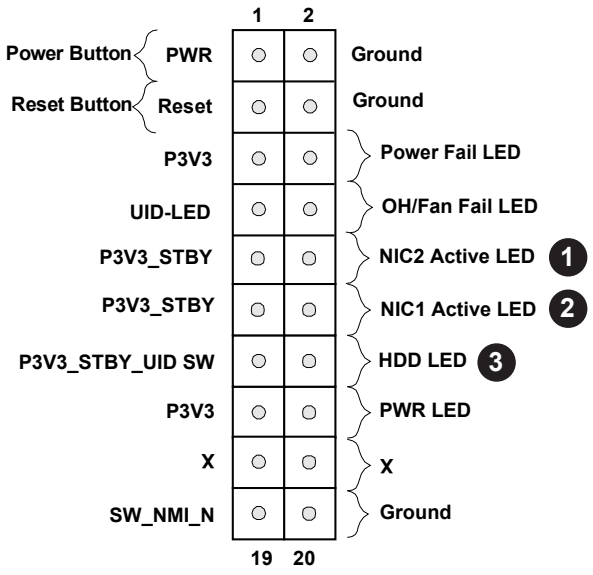
The NIC (Network Interface Controller) LED connection for LAN port 1 is located on pins 11 and 12 of JF1, and LAN port 2 is on pins 9 and 10. Attach the NIC LED cables here to display network activity. Refer to the table below for pin definitions.

LAN1/LAN2 LED Pin Definitions (JF1)	
Pin#	**Definition**
9	NIC 2 Activity LED
11	NIC 1 Activity LED

HDD LED

The HDD LED connection is located on pins 13 and 14 of JF1. Attach a cable to pin 14 to show hard drive activity status. Refer to the table below for pin definitions.

HDD LED Pin Definitions (JF1)	
Pins	**Definition**
13	3.3V Stdby
14	HDD Active



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

Power LED

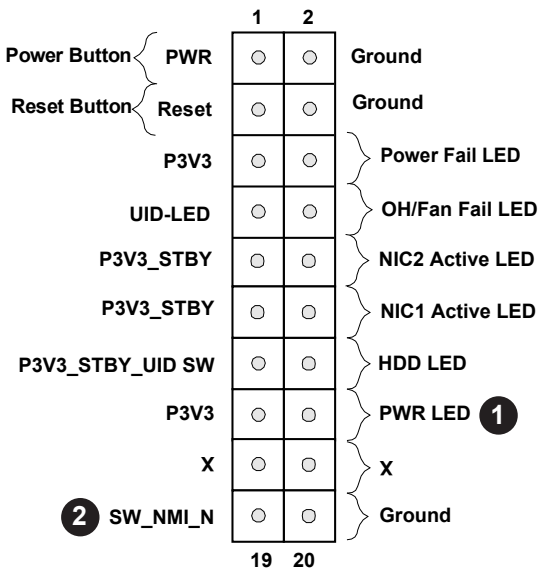
The Power LED connection is located on pins 15 and 16 of JF1. Refer to the table below for pin definitions.

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

NMI Button

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

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



1. Power LED
2. NMI Button

2.8 Connectors

Power Connections

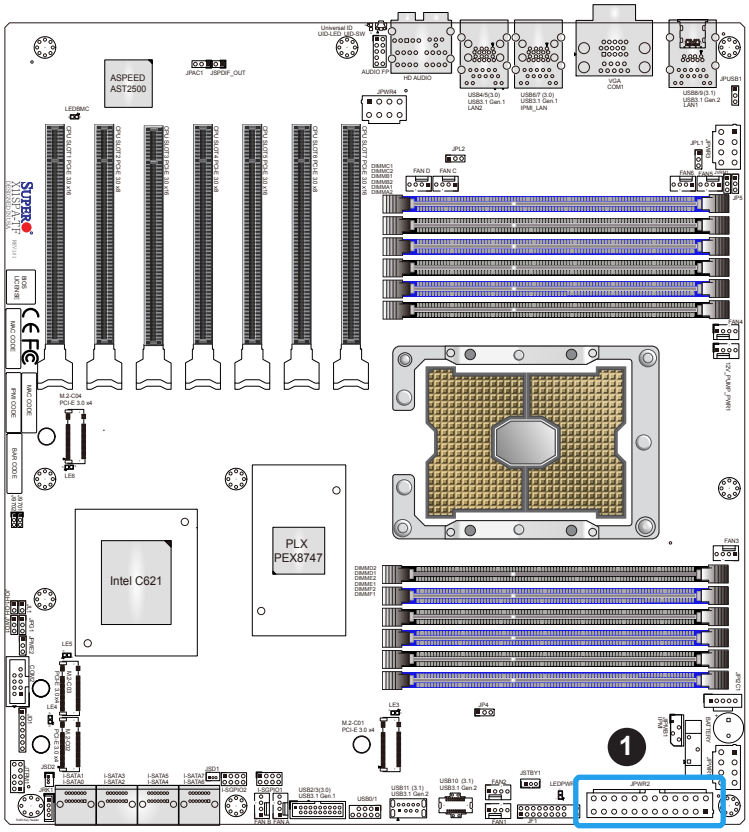
ATX Power Supply Connector

The 24-pin power supply connector (JPWR2) meets the ATX SSI EPS 12V specification. You must also connect the 8-pin processor power connectors to the power supply.

ATX Power 24-pin Connector Pin Definitions

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

Required Connection



1. JPWR2

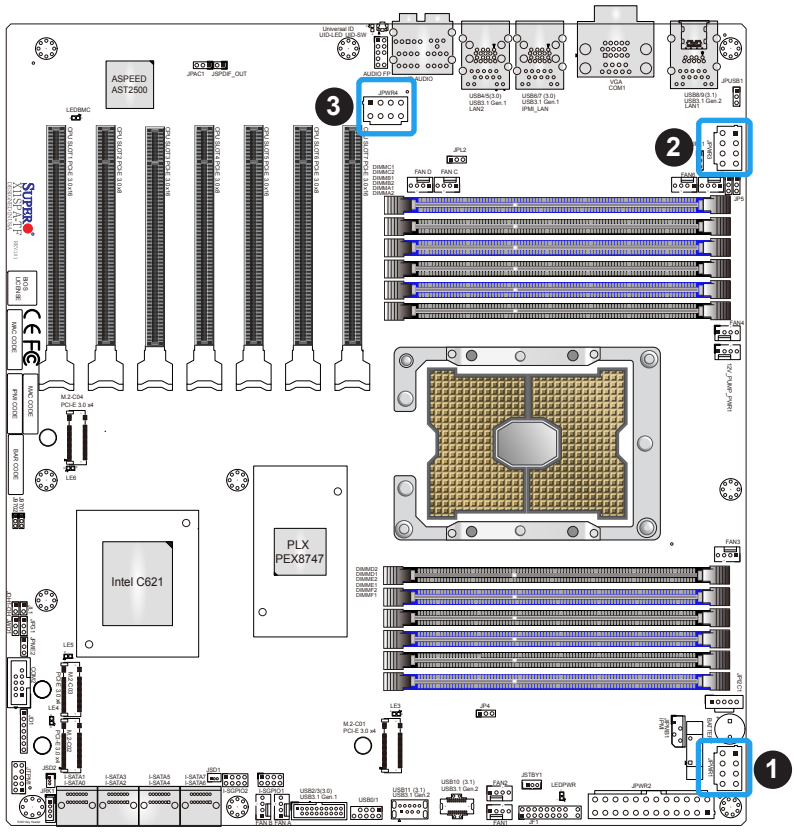
8-Pin Power Connectors

JPWR1/JPWR3/JPWR4 are 8-pin 12V DC power inputs for the CPU on the X11SPA-TF/-T motherboard. Besides the 24-pin ATX PWR (JPWR2), the three 12V 8-pin power connections (JPWR1/JPWR3/JPWR4) are required to ensure adequate power supply to the system. The connections of these 8-pin connectors should be JPWR1, JPWR3, and JPWR4 in sequence. Refer to the table below for pin definitions.

8-pin Power Connector Pin Definitions	
Pin#	**Definition**
1 - 4	Ground
5 - 8	P12V (12V Power)

Required Connection

Important: Please connect the power supplies to the 24-pin power connector (JPWR2) and the 8-pin power connectors (JPWR1/JPWR3/JPWR4) on the motherboard when more than four of the PCIe slots are populated. Note that the power connectors provided by power supply may vary. You may connect the 8-pin connector using the bundled GPU to CPU power cable to the power supply. This cable is an adapter converting the connector on the power supply to the 8-pin power connector on the motherboard. Failure in doing so may void the manufacturer warranty on your power supply and motherboard. Refer to the checklist table on page 7 and contact Supermicro for more detailed cable information.



1. JPWR1
2. JPWR3
3. JPWR4

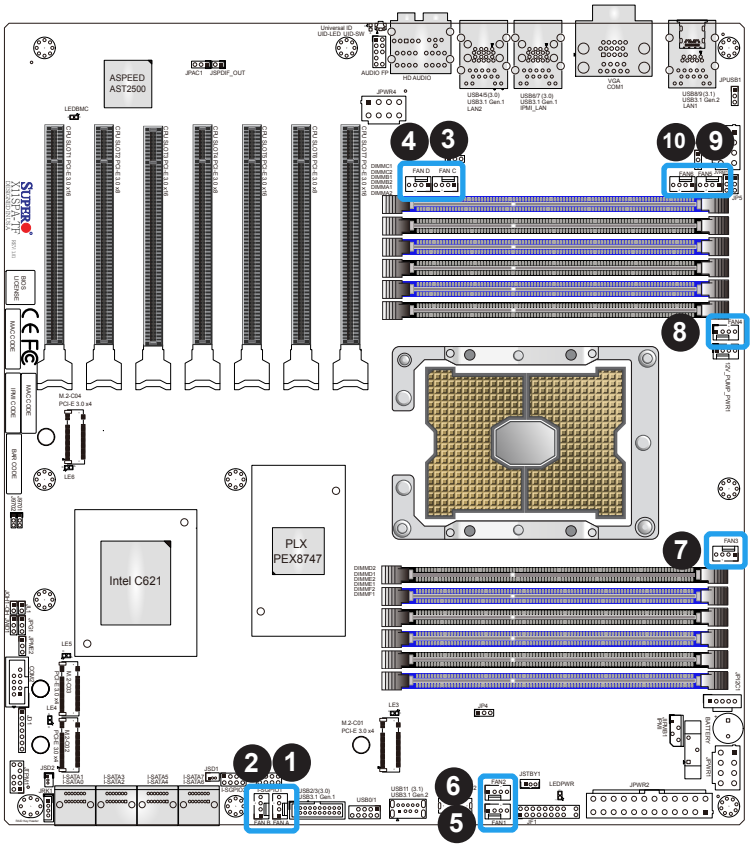
Headers

Fan Headers

There are ten 4-pin fan headers (FAN1 ~ FAN6, FAN A ~ FAN D) on the motherboard. All these 4-pin fan headers are backwards compatible with the traditional 3-pin fan headers. However, fan speed control is available for 4-pin fan headers only by Thermal Management via the IPMI 2.0 interface. Refer to the table below for pin definitions.

Fan Header Pin Definitions

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



1. FAN A
2. FAN B
3. FAN C
4. FAN D
5. FAN1
6. FAN2
7. FAN3
8. FAN4
9. FAN5
10. FAN6

SGPIO Headers

There are two Serial Link General Purpose Input/Output (I-SGPIO1 and I-SGPIO2) headers located on the motherboard. Refer to the table below for pin definitions.

I-SGPIO Header Pin Definitions

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

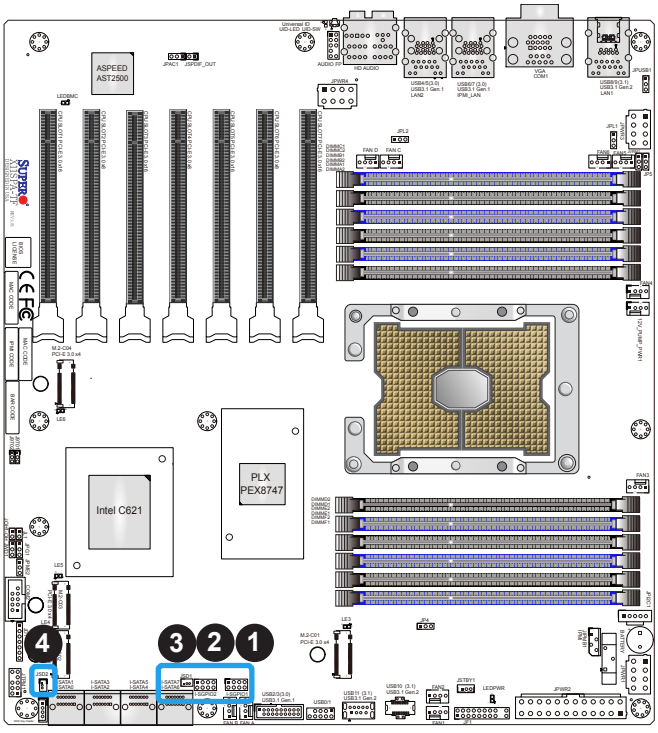
NC = No Connection

Disk-On-Module Power Connector

Two power connectors for SATA DOM (Disk-On-Module) devices are located at JSD1 and JSD2. Connect appropriate cables here to provide power support for your Serial Link DOM devices.

DOM Power Pin Definitions

Pin#	Definition
1	5V
2	Ground
3	Ground

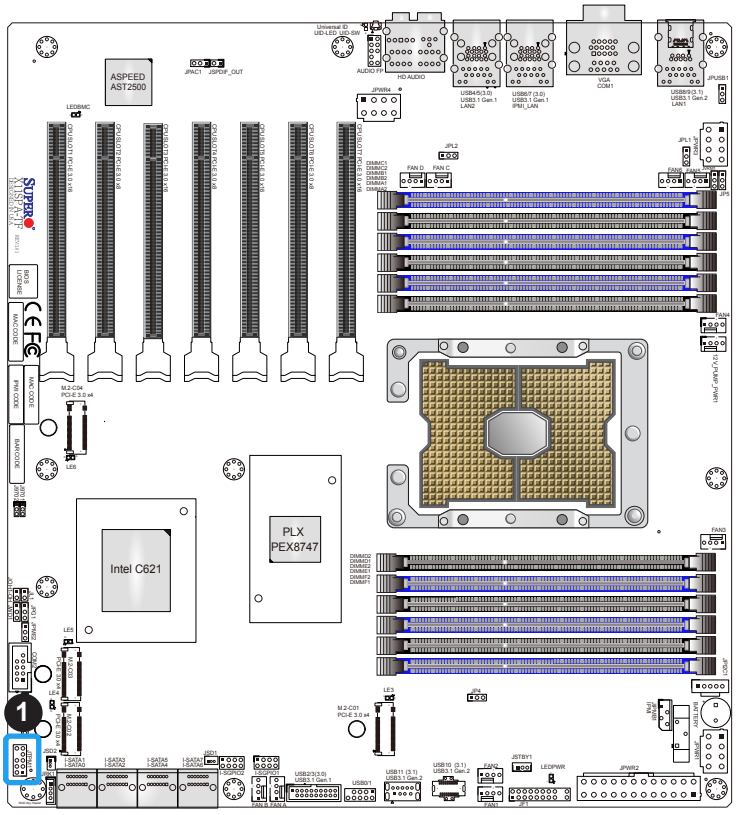


1. I-SGPIO1
2. I-SGPIO2
3. JSD1 (DOM PWR)
4. JSD2 (DOM PWR)

TPM/Port 80 Header

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

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

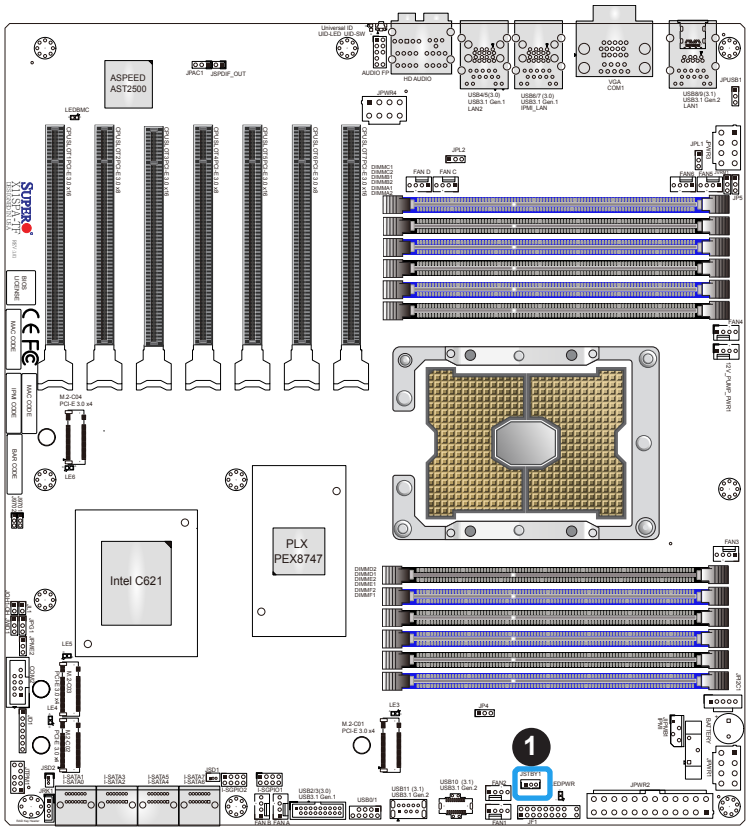


1. TPM/Port 80 Header

Standby Power Header

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

Standby Power Header Pin Definitions	
Pin#	**Definition**
1	+5V Standby
2	Ground
3	No Connection



1. Standby Power Header

Power SMB (I²C) Header

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

Power SMB Header Pin Definitions

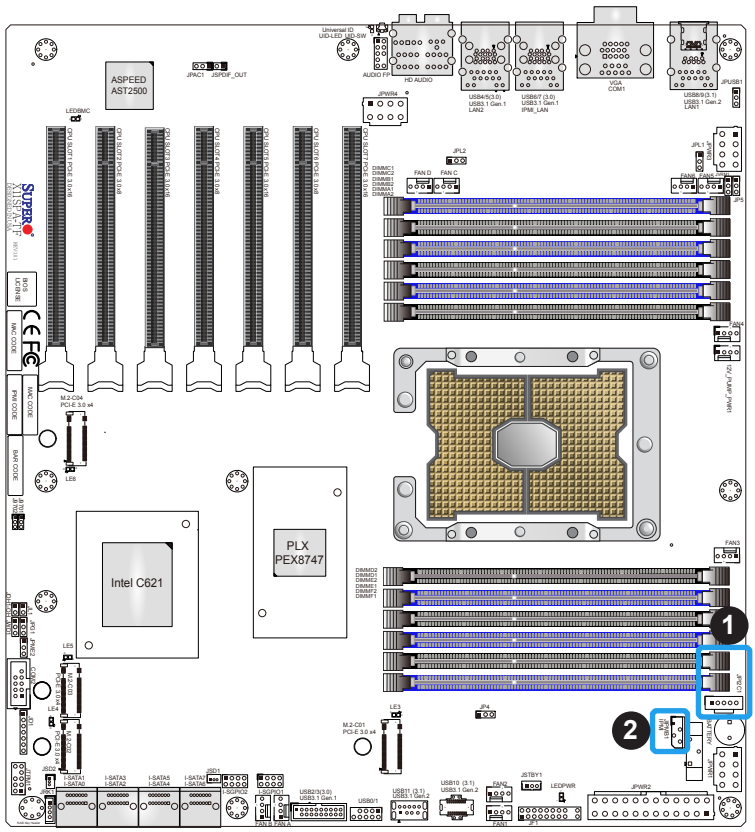
Pin#	Definition
1	Clock
2	Data
3	PMBUS_Alert
4	Ground
5	+3.3V

4-pin BMC External I2C Header

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

External I2C Header Pin Definitions

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

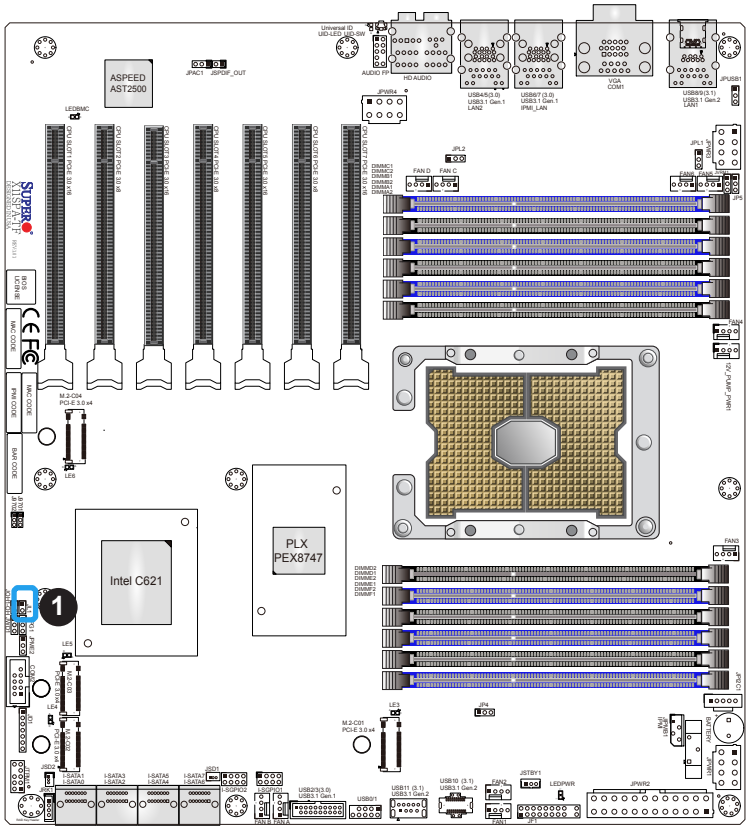


1. Power SMB Header
2. BMC External Header

Chassis Intrusion Header

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

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



1. Chassis Intrusion Header

Power LED/Speaker Header

Pins 1-3 of JD1 are used for power LED indication, and pins 4-7 are for the speaker. Please note that the speaker connector pins (4-7) are used with an external speaker. If you wish to use the onboard speaker, you should close pins 6-7 with a cap. Refer to the tables below for pin definitions.

PWR LED Connector Pin Definitions	
Pin#	**Signal**
1	JD1_PIN1
2	FP_PWR_LED
3	FP_PWR_LED

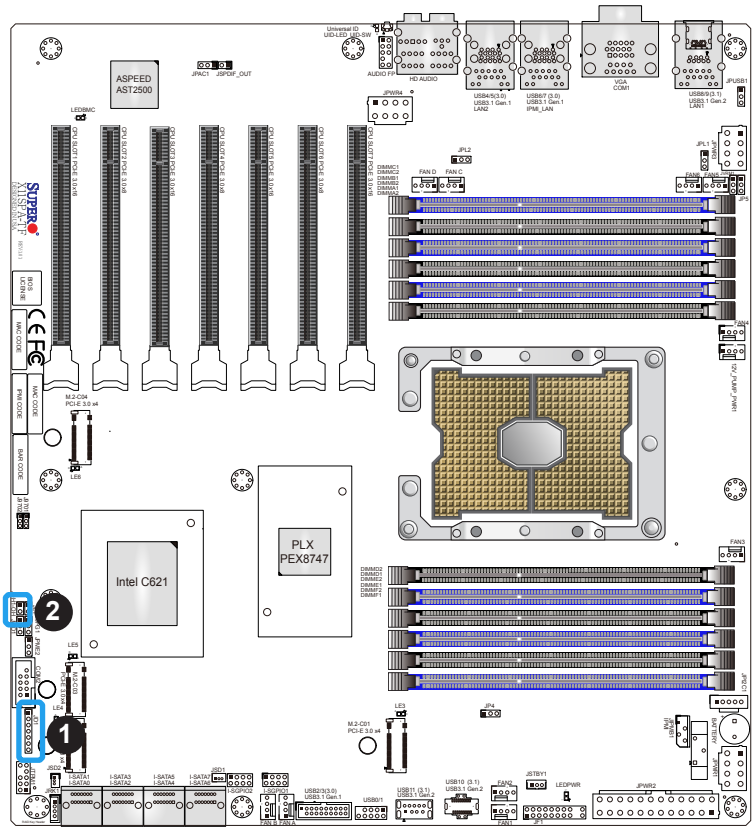
Speaker Connector Pin Definitions	
Pin#	**Signal**
4	P5V
5	Key
6	R_SPKPIN_N
7	R_SPKPIN

Overheat/Fan Fail LED Header

Header JOH1-OH is used to connect to an LED indicator to provide warnings of chassis overheating and fan failure. This LED will blink when a fan failure occurs. Refer to the tables below for pin definitions.

Overheat LED Header Status	
State	**Definition**
Solid	Overheat
Blinking	Fan Fail

Overheat LED Header Pin Definitions	
Pin#	**Signal**
1	Pull high to +3.3V power through 330-ohm resistor
2	OH Active



1. PWR LED/Speaker Header
2. Overheat/Fan Fail LED Header

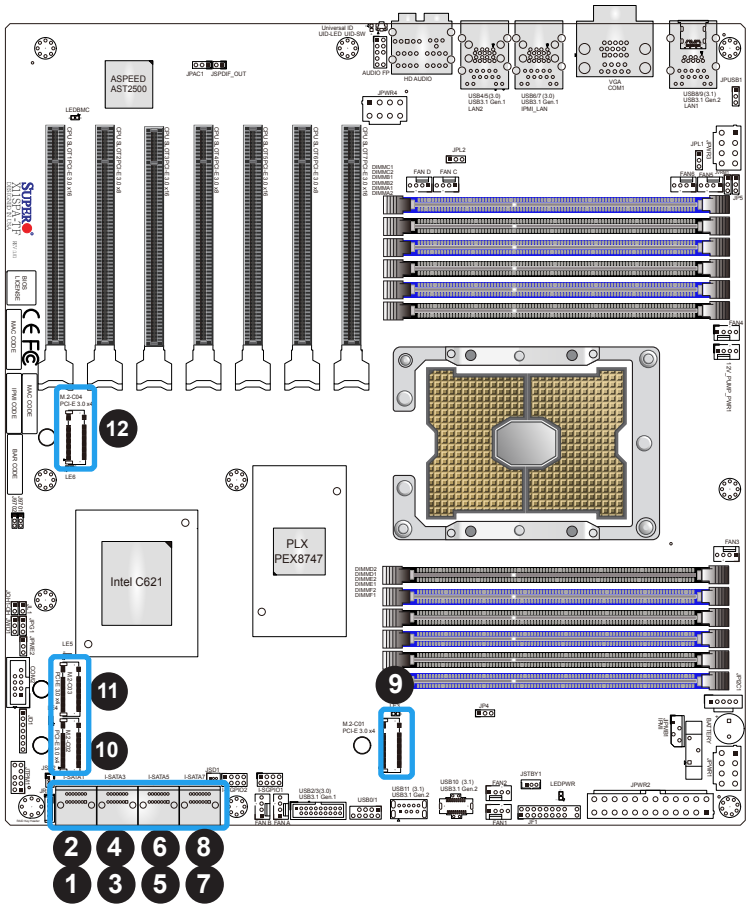
SATA Ports

Eight SATA 3.0 ports are located on the X11SPA-TF/-T motherboard supported by the C621 chipset. These SATA ports support RAID 0, 1, 5, and 10. SATA ports provide serial-link signal connections, which are faster than the connections of Parallel ATA.

Note: For more information on the SATA HostRAID configuration, please refer to the Intel SATA HostRAID user's guide posted on our website at http://www.supermicro.com.

M.2 Sockets

The X11SPA-TF/-T motherboard has four M.2 sockets. M.2 was formerly known as Next Generation Form Factor (NGFF) and serves to replace mini PCIe. M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. The M.2 sockets on the motherboard supports PCIe 3.0 x4 (32 Gb/s) SSD cards in 2260, 2280, and 22110 form factors.

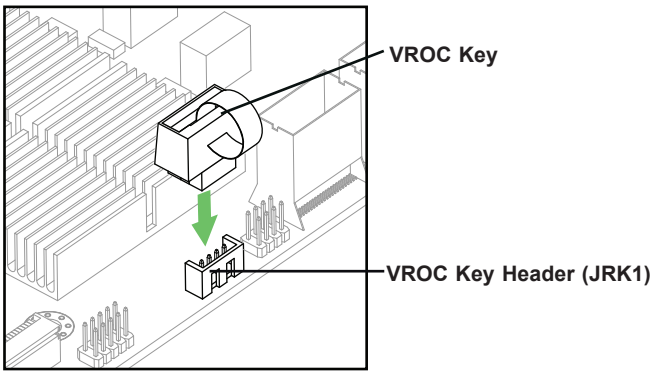


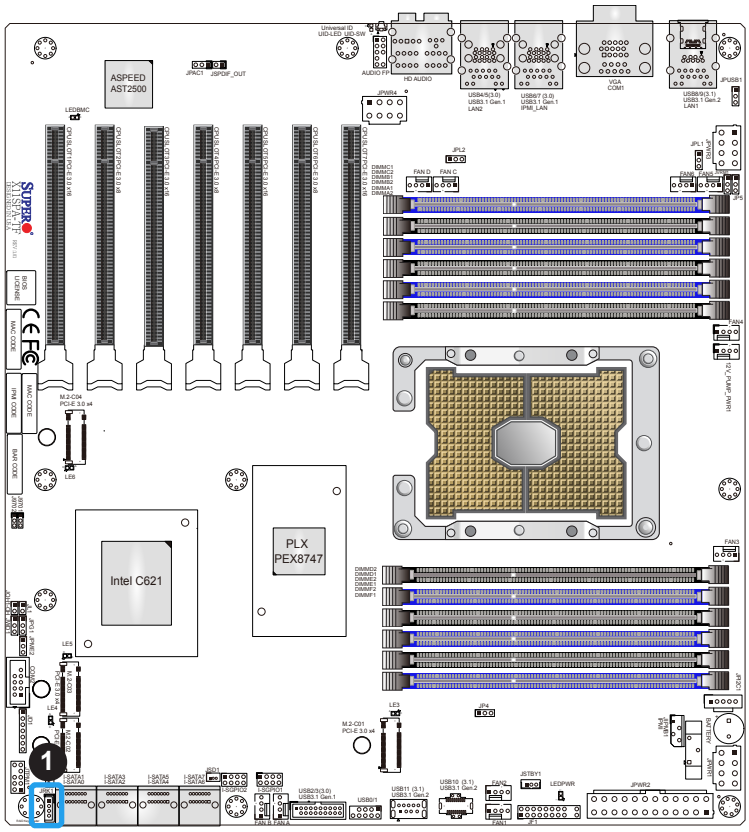
1. I-SATA0
2. I-SATA1
3. I-SATA2
4. I-SATA3
5. I-SATA4
6. I-SATA5
7. I-SATA6
8. I-SATA7
9. M.2-C01 PCI-E 3.0 x4
10. M.2-C02 PCI-E 3.0 x4
11. M.2-C03 PCI-E 3.0 x4
12. M.2-C04 PCI-E 3.0 x4

Intel RAID Key Header (VROC)

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 RAID Key Header (VROC) Pin Definitions	
Pin#	**Defintion**
1	GND
2	PU 3.3V Stdby
3	GND
4	PCH RAID KEY





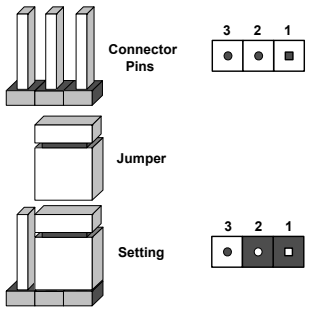
1. Intel RAID Key Header (VROC)

2.9 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.



Watchdog

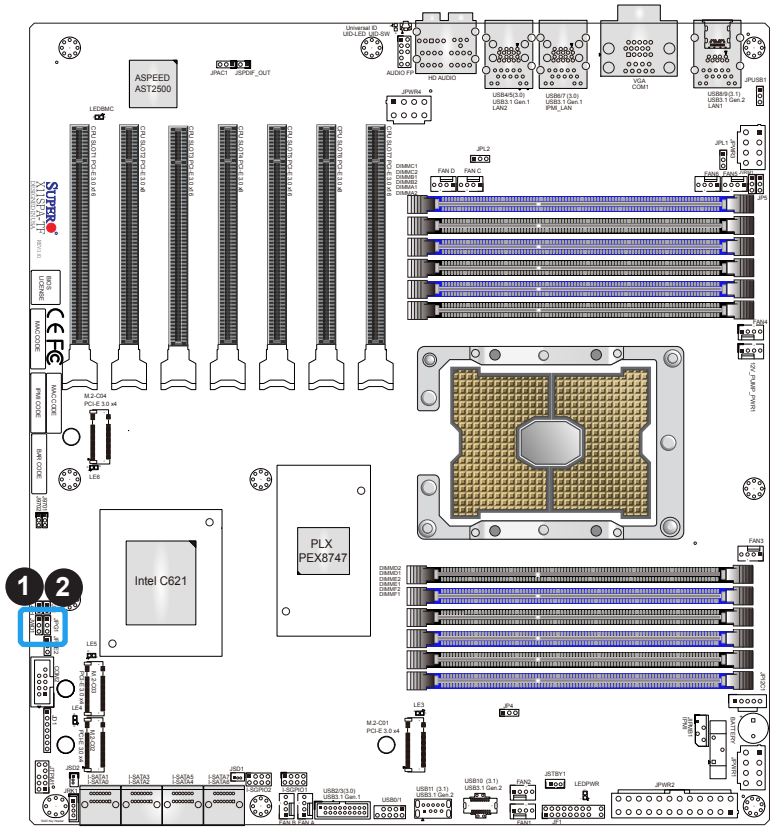
Watchdog (JWD1) is a system monitor that can reboot the system when a software application hangs. Close pins 1-2 to reset the system if an application hangs. Close pins 2-3 to generate a non-maskable interrupt (NMI) signal for the application that hangs. Refer to the table below for jumper settings. The Watchdog must also be enabled in the BIOS.

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

VGA Enable/Disable

Jumper JPG1 allows the user to enable the onboard VGA connector. The default setting is pins 1-2 to enable the connection. Refer to the table below for jumper settings.

VGA Enable/Disable Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Enabled (Default)
Pins 2-3	Disabled



1. Watchdog
2. VGA Enable/Disable

ME Manufacturing Mode

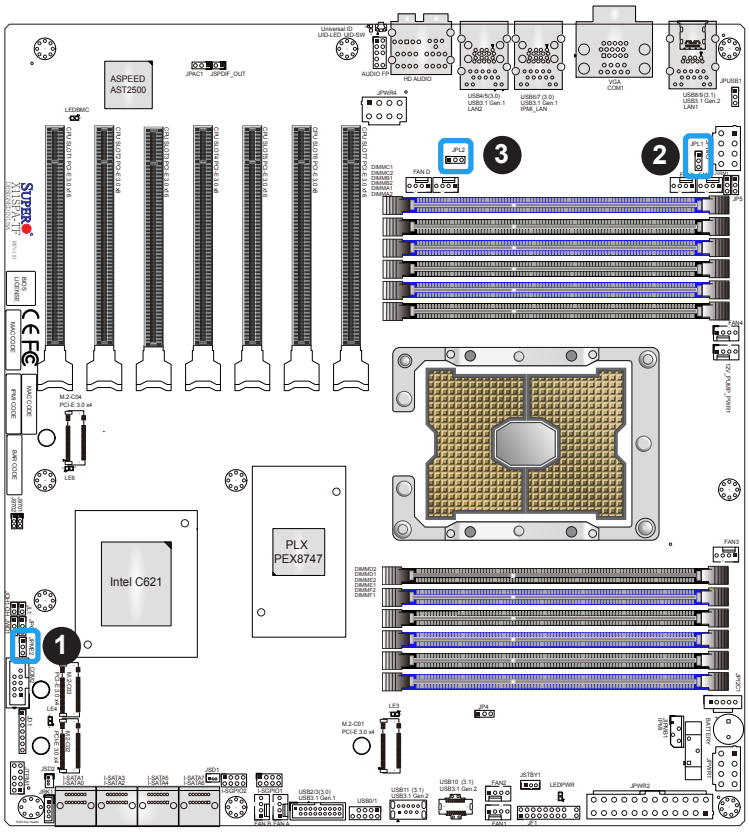
Close pins 2-3 of JPME2 to bypass SPI flash security and force the system to operate in the manufacturing mode, which will allow the user to flash the system firmware from a host server for system setting modifications. Refer to the table below for jumper settings. The default setting is Normal.

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

1Gb/10Gb LAN Enable/Disable

JPL1 and JPL2 allow the user to enable or disable the 1Gb/10Gb LAN Ports. The default setting is Enabled.

1Gb/10Gb LAN Enable/Disable Jumper Settings	
Jumper Setting	**Definition**
Pins 1-2	Enabled (Default)
Pins 2-3	Disabled

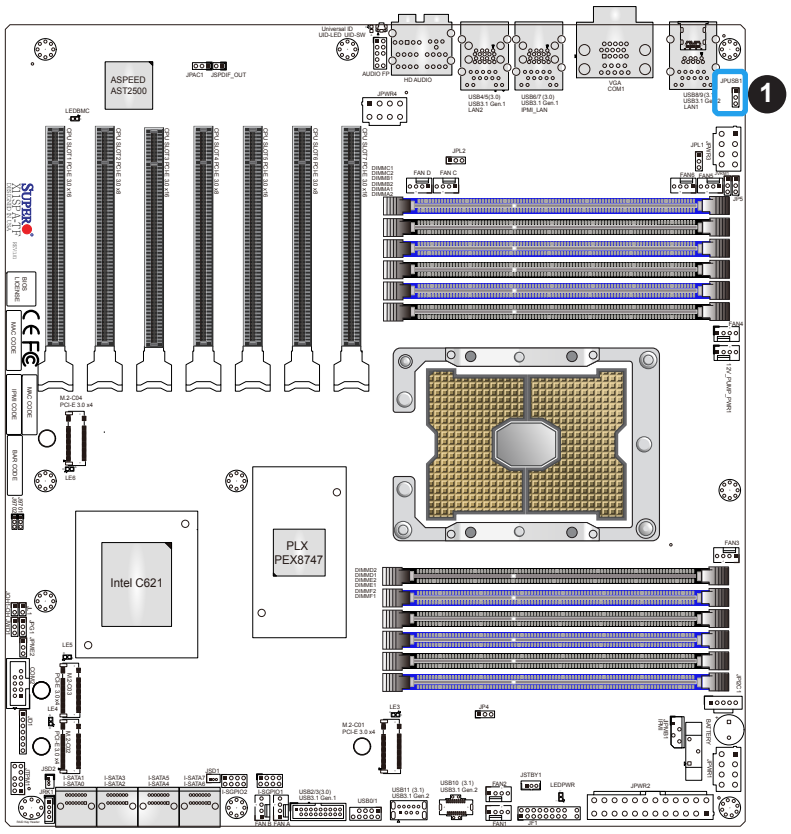


1. Manufacturing Mode
2. 1Gb LAN Enable/Disable
3.10Gb LAN Enable/Disable

USB Wake-Up

This jumper allows you to "wake up" the system by pressing a key on the USB keyboard or by clicking the USB mouse of your system. Jumper JPUSB1 is used together with the USB Wake-Up feature in BIOS. Both JPUSB1 and the BIOS setting must be enabled to use this feature. The default setting is Enabled.

Note: Please be sure to remove all other USB devices from the USB ports whose jumpers are set to disabled before the system goes into standby mode.



1. JPUSB1

2.10 LED Indicators

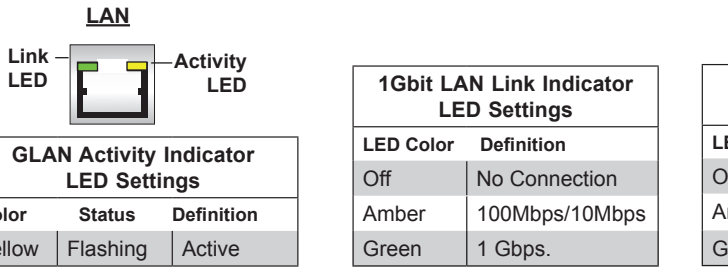
Unit ID LED

A rear UID LED indicator (UID-LED) 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 LED Indicator	
LED Color	**Definition**
Blue: On	Unit Identified

LAN LEDs

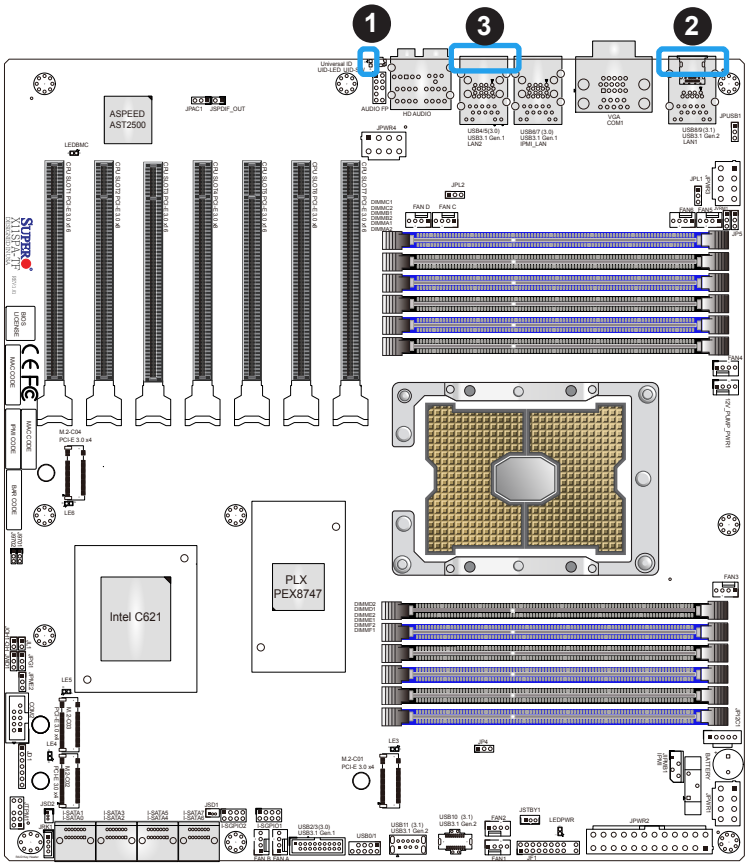
Two LAN ports are located on the I/O back panel of the motherboard. This Ethernet LAN port has two LEDs (Light Emitting Diode). The yellow LED indicates activity, while the Link LED may be green, amber, or off to indicate the speed of the connection. Refer to the tables below for more information.



GLAN Activity Indicator LED Settings		
Color	**Status**	**Definition**
Yellow	Flashing	Active

1Gbit LAN Link Indicator LED Settings	
LED Color	**Definition**
Off	No Connection
Amber	100Mbps/10Mbps
Green	1 Gbps.

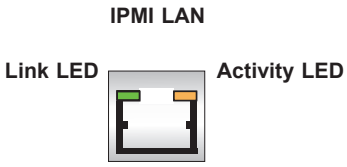
10Gbit LAN Link Indicator LED Settings	
LED Color	**Definition**
Off	No Connection
Amber	5Gbps/2.5Gbps/1Gbps/100Mbps
Green	10 Gbps.



1. UID LED
2. LAN1 LEDs
3. LAN2 LEDs

IPMI LAN LEDs

In addition to LAN1 and LAN2, an IPMI LAN is also located on the I/O back panel. The amber LED on the right indicates activity, while the green LED on the left indicates the speed of the connection. Refer to the table below for more information.

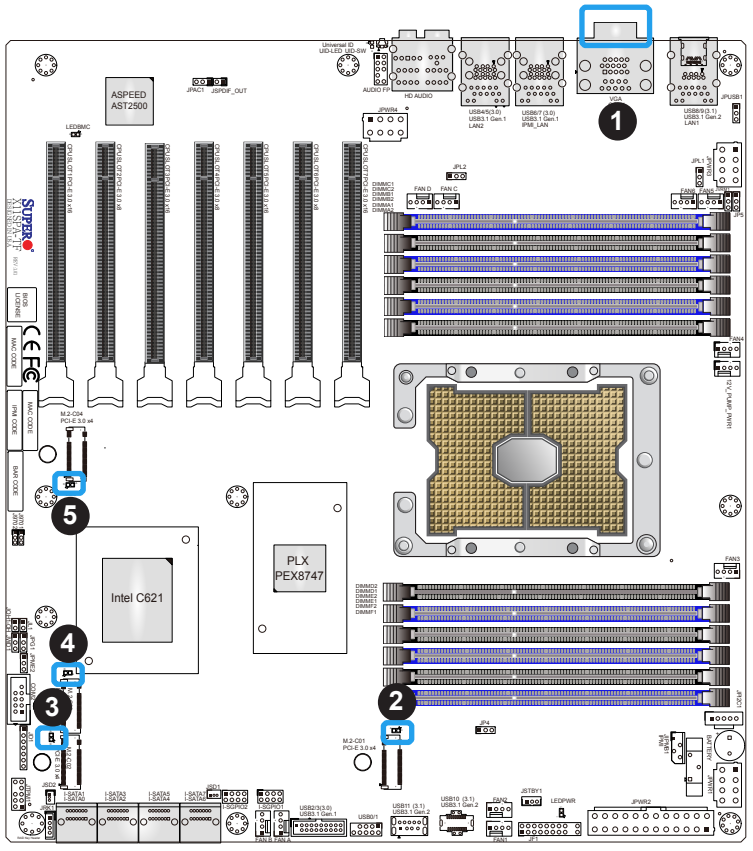


IPMI LAN LED		
	Color/State	**Definition**
Link (left)	Green: Solid Amber: Solid	100 Mbps 1Gbps
Activity (Right)	Amber: Blinking	Active

M.2 LEDs

M.2 LEDs are located at LE3, LE4, LE5, and LE6 on the motherboard. When a M.2 LED is blinking, its corresponding M.2 device functions normally. Refer to the table below for more information.

M.2 LED	
LED Color	**Definition**
Green: Blinking	Device Working



1. IPMI LAN LEDs
2. LE3
3. LE4
4. LE5
5. LE6

Onboard Power LED

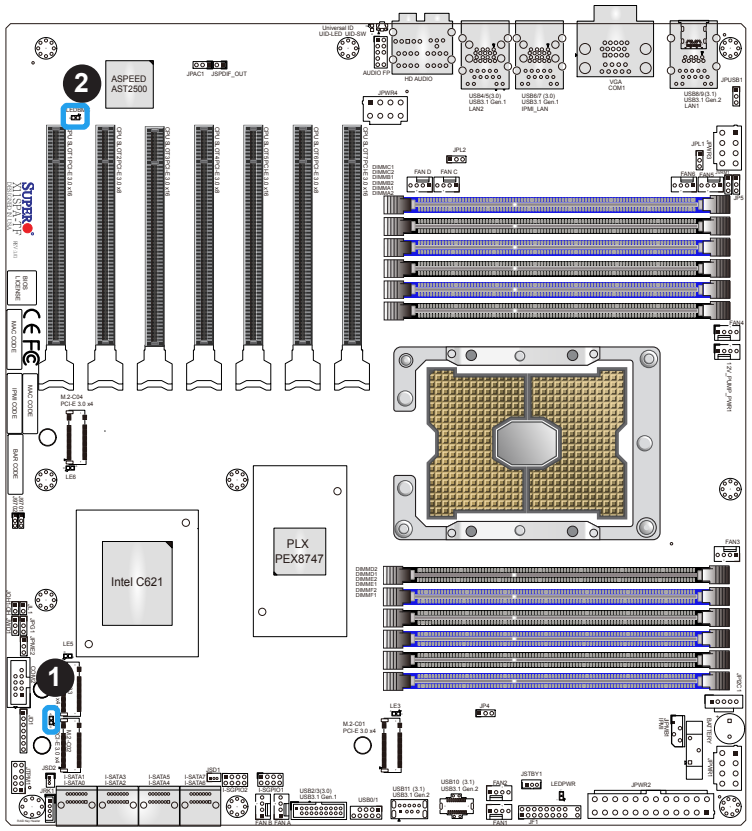
The Onboard Power LED is located at LEDPWR on the motherboard. When this LED is on, the system is on. Be sure to turn off the system and unplug the power cord before removing or installing any component. Refer to the table below for more information.

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

BMC Heartbeat LED

A BMC Heartbeat LED is located at LEDBMC on the motherboard. When LEDBMC is blinking, the BMC is functioning normally. Refer to the table below for more information.

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



1. Onboard Power LED
2. BMC Heartbeat LED

Chapter 3

Troubleshooting

3.1 Troubleshooting Procedures

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

Before Power On

1. Make sure that there are no short circuits between the motherboard and chassis.
2. Disconnect all ribbon/wire cables from the motherboard, including those for the keyboard and mouse.
3. Remove all add-on cards.
4. Install the CPU (making sure it is fully seated) and connect the front panel connectors to the motherboard.

No Power

1. Make sure that there are no short circuits between the motherboard and the chassis.
2. Make sure that the ATX power connectors are properly connected.
3. Check that the 115V/230V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. The battery on your motherboard may be old. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.

No Video

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

System Boot Failure

If the system does not display 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, follow the instructions stated in the Clear CMOS section to clear the CMOS settings.

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

Memory Errors

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

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the website of motherboard's product page to see a list of supported memory.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMMs in the system.
3. Make sure that you are using the correct type of ECC DDR4 modules recommended by the manufacturer.
4. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.

Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to Chapter 2 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies ~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: Click on the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.

3. HDD support: Make sure that all hard disk drives (HDDs) work properly. Replace the bad HDDs with good ones.
4. System cooling: Check the system cooling to make sure that all heatsink fans and CPU/system fans, etc., work properly. Check the hardware monitoring settings in the IPMI to make sure that the CPU and system temperatures are within the normal range. Also check the front panel Overheat LED and make sure that it is not on.
5. Adequate power supply: Make sure that the power supply provides adequate power to the system. Make sure that all power connectors are connected. Please refer to our website for more information on the minimum power requirements.
6. Proper software support: Make sure that the correct drivers are used.

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

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

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 and short the battery terminal socket for five seconds.

   Note: Clearing CMOS will also clear all passwords.

4. Refer to Section 3.4 for more battery notices.

3.2 Technical Support Procedures

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

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

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

4. An example of a Technical Support form is on our website at http://www.supermicro.com/RmaForm/.

- Distributors: For immediate assistance, please have your account number ready when placing a call to our Technical Support department. We can be reached by email at support@supermicro.com.

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: The motherboard supports DDR4 ECC RDIMM, 3DS RDIMM, LRDIMM, and 3DS LRDIMM modules. To enhance memory performance, do not mix memory modules of different speeds and sizes. Please follow all memory installation instructions given in Section 2.4 in Chapter 2.

Question: How do I update my BIOS?

Answer: It is recommended that you do not upgrade your BIOS if you are not experiencing any problems with your system. Updated BIOS files are located on our website at http://www.supermicro.com/ResourceApps/BIOS_IPMI_Intel.html. Please check our BIOS warning message and the information on how to update your BIOS on our website. Select your motherboard model and download the BIOS file to your computer. Also, check the current BIOS revision to make sure that it is newer than your BIOS before downloading. To update your BIOS under the UEFI shell, please unzip the BIOS file onto a USB device formatted with the FAT/FAT32 file system. 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. Enter flash.nsh BIOSname#.### at the prompt to start the BIOS update process. Reboot the system when you see the message that BIOS update has completed. Refer to Appendix D UEFI BIOS Recovery and/or the readme file for more information.

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

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

3.4 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

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

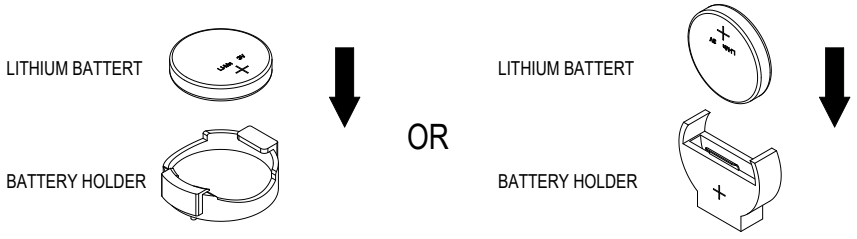
Proper Battery Disposal

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

Battery Installation

1. To install an onboard battery, follow steps 1 and 2 above and continue below:
2. Identify the battery's polarity. The positive (+) side should be facing up.
3. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.

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



3.5 Returning Merchandise for Service

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

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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

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

Starting the Setup Utility

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

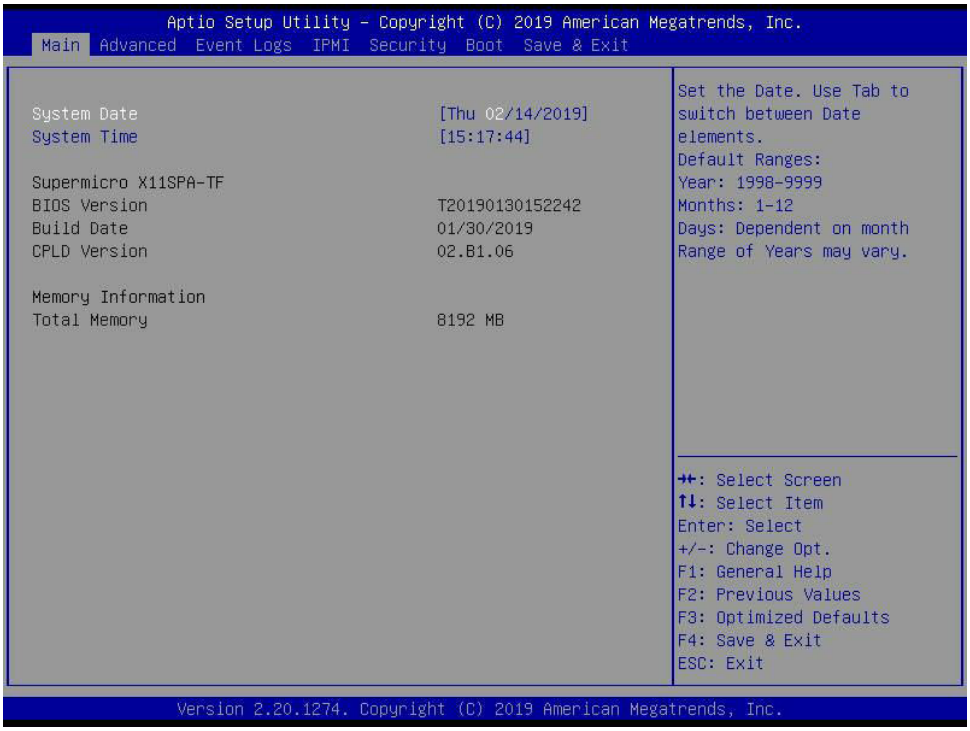
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

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

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

4.2 Main Setup

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



System Date/System Time

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

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

Supermicro X11SPA-TF

BIOS Version

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

Build Date

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

CPLD Version

This feature displays the Complex Programmable Logic Device version.

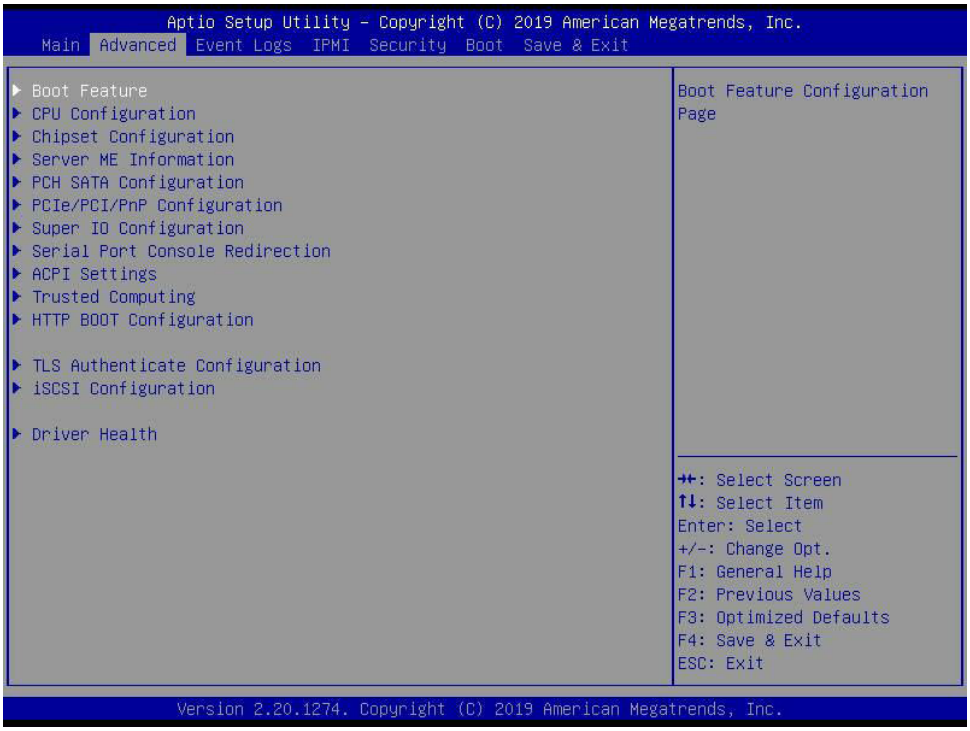
Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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



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

▶Boot Feature

Quiet Boot

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

Option ROM Messages

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

Bootup NumLock State

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

Wait For "F1" If Error

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

INT19 (Interrupt 19) Trap Response

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

Re-try Boot

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

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, and 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 enable 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 five minutes. The options are **Disabled** and Enabled**.**

Restore on AC Power Loss

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

Power Button Function

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

▶CPU Configuration

The following CPU information will display:

- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM
- L2 Cache RAM
- L3 Cache RAM
- Processor 0 Version
- Intel(R) Xeon(R) Gold 5118 CPU @ 2.30GHz

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

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

Cores Enabled

Use this feature to enable or disable CPU cores in the processor specified by the user. The default setting is 0.

Monitor/Mwait

This feature allows the user to configure Monitor/Mwait. 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. The options are Disable and **Enable**. (Refer to the Intel and Microsoft® websites for more information.)

Intel Virtualization Technology

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

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 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 Disable and **Enable**.

Adjacent Cache Prefetch (Available when supported by the CPU)

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

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enable to enable the DCU (Data Cache Unit) Streamer Prefetcher which will stream and prefetch data and send it to the Level 1 data cache to improve data processing and system performance. The options are Disable and **Enable**.

DCU IP Prefetcher (Available when supported by the CPU)

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

LLC Prefetch

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

Extended APIC

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

AES-NI

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

▶Advanced Power Management Configuration

Power Technology

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

If the feature is set to Custom, the following features will display:

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

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

ENERGY_PERF_BIAS_CFG mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode) (Available when supported by the Processor and when "Power Performance Tuning" is set to BIOS Controls EPB)

Use this feature to set the processor power use policy to achieve the desired operation settings for your machine by prioritizing system performance or energy savings. Select Maximum Performance to maximize system performance (to its highest potential); however, this may result in maximum power consumption as energy is needed to fuel the processor frequency. The higher the performance is, the higher the power consumption will be. Select Max Power Efficient to maximize power saving; however, system performance may be substantially impacted because limited power use decreases the processor frequency. The options are Performance, **Balanced Performance**, Balanced Power, and Power.

▶CPU P State Control

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

SpeedStep (P-States)

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**.

EIST PSD Function

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

Turbo Mode

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

▶Hardware PM State Control

Hardware P-States

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

▶CPU C State Control

Autonomous Core C-State

Enabling this feature allows the hardware to autonomously choose to enter a C-state based on power consumption and clock speed. 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 its clock cycle and voltage during a Halt-state. The options are Disable and **Enable**.

▶Package C State Control

Package C State

This feature allows 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

Use this feature to enable Software Controlled T-States. 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

The following UPI information will display:

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

Degrade Precedence

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

Link L0p Enable

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)

IO Directory Cache is an 8-entry cache that stores the directory state of remote IIO writes and memory lookups, and saves directory updates. Use this feature to lower cache to cache (C2C) transfer latencies. 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 WCiLF.

SNC

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

XPT Prefetch

Select Enable for Extended (Xtended) Prediction Table (XPT) Prefetch support which will allow a read request to be sent to the memory controller requesting the prefetch in parallel to an LLC (Last Level Cache) look-up. The options are **Disable** and Enable.

KTI Prefetch

KTI Prefetch is a feature that enables memory read to start early on a DDR bus, where the KTI Rx path will directly create a Memory Speculative Read command to the memory controller. The options are Disable and **Enable**.

Local/Remote Threshold

Use this feature to configure the threshold settings for local and remote systems that are connected in the network. The options are Disable, **Auto**, Low, Medium, and High.

Stale AtoS

Select Enable to remove the contents and the structures of the files that are no longer needed in the remote host server but are still in use by the local client machine from Directory A to Directory S in the NFS (Network File System) to optimize system performance. The options are Disable, Enable, and **Auto**.

LLC Dead Line Alloc

Select Enable to opportunistically fill the deadlines in LLC (Last Level Cache). The options are Disable, **Enable**, and Auto.

Isoc Mode

Select Enable for 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

Enforce POR

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

PPR Type

Use this feature to select Post Package Repair Type. 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.

Data Scrambling for DDR4

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

tCCD_L Relaxation

Select Enable to get TCDD settings from SPD (Serial Presence Detect) and implement into memory RC code to improve system reliability. Select Disable for TCCD to follow Intel POR. The options are **Auto** and Disable.

tRWSR Relaxation

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

2x Refresh

Use this feature to select the memory controller refresh rate to 2x refresh mode. The options are **Auto** and Enable.

Page Policy

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

IMC Interleaving

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

▶Memory Topology

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

▶Memory RAS Configuration

Static Virtual Lockstep Mode

Select Enable to run the system's memory channels in lockstep mode to minimize memory access latency. The options are **Disable** and Enable.

Mirror Mode

This feature allows memory to be mirrored between two channels, providing 100% redundancy. The options are **Disable**, Mirror Mode 1LM, and Mirror Mode 2LM.

Memory Rank Sparing

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

Correctable Error Threshold

Use this feature to specify the threshold value for correctable memory-error logging, which sets a limit on the maximum number of events that can be logged in the memory error log at a given time. The default setting is **100**.

Intel® Run Sure

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

SDDC Plus One

Single Device Data Correction (SDDC) organizes data in a single bundle (x4/x8 DRAM). If any or all the bits become corrupted, corrections occur. The x4 condition is corrected on all cases. The x8 condition is corrected only if the system is in Lockstep Mode. The options are **Disable** and Enable.

ADDDC Sparing

Adaptive Double Device Data Correction (ADDDC) Sparing detects when the predetermined threshold for correctable errors is reached, copying the contents of the failing DIMM to spare memory. The failing DIMM or memory rank will then be disabled. The options are **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, the IO hub will read and write back one cache line every 16K cycles if there is no delay caused by internal processing. By using this method, roughly 64 GB of memory behind the IO hub will be scrubbed every day. The options are Disable and **Enable**.

Patrol Scrub Interval

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

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.

▶CPU Configuration

IOU1 (II0 PCIe Br2)

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

IOU2 (II0 PCIe Br3)

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

▶CPU SLOT7 PCI-E 3.0 x16/CPU SLOT1 PCI-E 3.0 x16/M.2C01 PCI-E 3.0 x4/M.2C02 PCI-E 3.0 x4/M.2C03 PCI-E 3.0 x4/M.2C04 PCI-E 3.0 x4

Link Speed

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

The following information will also be displayed:

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

PCI-E Port Max Payload Size

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

▶IOAT Configuration

Disable TPH

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

Prioritize TPH

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

ACS Control

This feature allows users to choose whether they want to enable or disable PCIe Access Control Services (ACS) Extended Capability. The options are **Enable** and Disable.

Interrupt Remapping

Use this feature to enable Interrupt Remapping support, which detects and controls external interrupt requests. The options are **Enable** and Disable.

PassThrough DMA

Use this feature to allow devices such as network cards to access the system memory without using a processor. Select Enable to use the Non-Isoch VT-d Engine Pass Through Direct Memory Access (DMA) support. The options are **Enable** and Disable.

ATS

Use this feature to enable Non-Isoch VT-d Engine Address Translation Services (ATS) support. ATS translates virtual addresses to physical addresses. 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)

Use this feature to maintain setting coherency between processors or other devices. Select Enable for the Non-Isoch VT-d engine to pass through DMA to enhance system performance. The options are **Enable** and Disable.

▶Intel® VMD Technology

▶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 above is set to Enable, the following features will become available for configuration:

CPU SLOT2/3/4/5 PCI-E 3.0 VMD (Available when the device is detected by the system)

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

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

Use this feature to enable 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 above is set to Enable, the following features will become available for configuration:

CPU SLOT7 PCI-E 3.0 x16 VMD/CPU SLOT6 PCI-E 3.0 x8 VMD (Available when the device is detected by the system)

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

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

Use this feature to enable 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 above is set to Enable, the following features will become available for configuration:

CPU SLOT1 PCI-E 3.0 x16 VMD/M.2C01 PCI-E 3.0 x4 VMD/M.2C02 PCI-E 3.0 x4 VMD/M.2C03 PCI-E 3.0 x4 VMD/M.2C04 PCI-E 3.0 x4 VMD (Available when the device is detected by the system)

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

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

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

PCI-E Completion Timeout Disable

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

▶South Bridge

The following USB information will display:

- USB Module Version
- USB Devices

Legacy USB Support

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

XHCI Hand-off

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

Port 60/64 Emulation

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

PCIe PLL SSC

Select Enable for PCH PCIe Spread Spectrum Clocking support, which will allow the BIOS to monitor and attempt to reduce the level of Electromagnetic Interference caused by the components whenever needed. The options are Enable and **Disable**.

Azalia

Use this feature to enable or disable Azalia audio devices. If Auto is selected, BIOS will automatically enable Azalia once an Azalia device is detected. The options are Enable, Disable, and **Auto**.

Azalia PME Enable

Use this feature to enable or disable PME (Power Management Event) for Azalia. The options are Enable and **Disable**.

▶Server ME Configuration (for X11SPA-TF only)

The following General ME Configuration will display:

- Oper. Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1

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

▶Workstation Me Configuration (for X11SPA-T only)

The following General ME Configuration will display:

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

▶PCH SATA Configuration

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

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

This feature allows the user to remove any password-protected SATA disk drives. The options are **Enable** and Disable.

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 in a low power mode during extended periods of I/O inactivity, and will return the link to an active state when I/O activity resumes. The options are **Disable** and Enable.

If the feature "Configure SATA as" above is set to RAID, the following features will become available for 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

Port 0 ~ Port 7 Hot Plug

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

Port 0 ~ Port 7 Spin Up Device

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.

Port 0 ~ Port 7 SATA Device Type

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

▶PCIe/PCI/PnP Configuration

The following information will display:

- 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 I/O 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 I/O hub. The options are **56T**, 40T, 24T, 16T, 4T, 2T, and 1T.

MMIO High Granularity Size

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

Maximum Read Request

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

MMCFG Base

Use this feature to select the low base address for PCIe adapters to increase base memory. The options are 1G, 1.5G, 1.75G, **2G**, 2.25G, 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 VGA priority when multiple VGA devices are detected. Select Onboard to give priority to your onboard video device. Select Offboard to give priority to your graphics card. The options are **Onboard** and Offboard.

CPU SLOT1 PCI-E 3.0 x16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

CPU SLOT2 PCI-E 3.0 x8 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

CPU SLOT3 PCI-E 3.0 x16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

CPU SLOT4 PCI-E 3.0 x8 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

CPU SLOT5 PCI-E 3.0 x16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

CPU SLOT6 PCI-E 3.0 x8 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

CPU SLOT7 PCI-E 3.0 x16 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

M.2C01 PCI-E 3.0 x4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

M.2C02 PCI-E 3.0 x4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

M.2C03 PCI-E 3.0 x4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

M.2C04 PCI-E 3.0 x4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

Bus Master Enable

This feature allows users to change Bus Master Enable policy. If Disabled is selected, this policy will be enable based on device settings; if Enabled is selected, the policy will be enabled all the time. The options are Disabled and **Enabled**.

Onboard LAN Option ROM Type

Use this feature to select which firmware function to be loaded for LAN Port1 used for system boot. The options are **Legacy** and EFI.

Onboard LAN1 Option ROM

Use this feature to select which firmware function to be loaded for LAN Port1 used for system boot. The options are Disabled, **PXE**, and iSCSI.

Onboard LAN2 Option ROM

Use this feature to select which firmware function to be loaded for LAN Port 2 used for system boot. The options are **Disabled** and PXE.

Onboard Video Option ROM

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

►Network Stack Configuration

Network Stack

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

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 feature 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 feature 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

The following Super IO information will display:

- Super IO Chip AST2500

▶Serial Port 1 Configuration

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

Serial Port 1

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

Device Settings

This feature displays the status of 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 for Serial Port 1 are **Auto**, (IO=3F8h; IRQ=4;), (IO=2F8h; IRQ=4;), (IO=3E8h; IRQ=4;), and (IO=2E8h; IRQ=4;).

▶Serial Port 2 Configuration

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

Serial Port 2

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

Device Settings

This feature displays the status of 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 for Serial Port 2 are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3;), (IO=3E8h; IRQ=3;), and (IO=2E8h; IRQ=3;).

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

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

▶Serial Port Console Redirection

COM1 Console Redirection

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

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

▶COM1 Console Redirection Settings

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

COM1 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.

COM1 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).

COM1 Data Bits

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

COM1 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.

COM1 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.

COM1 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.

COM1 VT-UTF8 Combo Key Support

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

COM1 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.

COM1 Resolution 100x31

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

COM1 Legacy OS Redirection Resolution

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

COM1 Putty KeyPad

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

COM1 Redirection After BIOS POST

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

SOL/COM2 Console Redirection

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

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

►SOL/COM2 Console Redirection Settings

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

COM2 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 ANSI, VT100, **VT100+**, and VT-UTF8.

COM2 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).

COM2 Data Bits

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

COM2 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.

COM2 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.

COM2 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.

COM2 VT-UTF8 Combo Key Support

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

COM2 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.

COM2 Resolution 100x31

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

COM2 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**.

COM2 Putty KeyPad

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

COM2 Redirection After BIOS POST

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

Legacy Console Redirection

Legacy Serial Redirection Port

Use this feature to select a COM port to display redirection of Legacy OS and Legacy OPROM messages. The options are **COM1** and SOL/COM2.

EMS (Emergency Management Services) Console Redirection

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

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

▶EMS Console Redirection Settings

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

Out-of-Band Mgmt Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2.

Terminal Type

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

Bits Per Second

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

Flow Control

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

▶ACPI Settings

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

The X11SPA-TF/-T supports TPM 1.2 and 2.0. The following Trusted Platform Module (TPM) information will display if a TPM 2.0 module is detected:

- Vendor Name
- Firmware Version

Security Device Support

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

- Active PCR Bank
- SHA256 PCR Bank

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

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending Operation

Use this feature to schedule a TPM-related operation to be performed by a security device for system data integrity. Your system 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 (PH) Randomization. The options are **Disabled** and Enabled.

TXT Support

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

▶HTTP BOOT Configuration

Http Boot One Time

This feature allows the user to disable and enable HTTP Boot feature. If a Http Boot Option is created, the system will automatically boot into Http Boot. The options are **Disable** and Enable.

Input the description

This feature allows the user to key in descriptions for the HTTP Boot option.

Boot URI

A new Boot Option will be created according to this Boot URI.

▶TLS Authenticate Configuration

▶Server CA Configuration

▶Enroll Certification

▶Enroll Cert Using File

Cert GUID

▶Commit Changes and Exit

▶Discard Changes and Exit

▶Delete Certification

▶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

▶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: 1.45 TiB

App Direct capacity: 0 B

Memory capacity: 1.45 TiB

Unconfigured capacity: 0 TiB

Inaccessible capacity: 0 TiB

Reserved capacity: 2.7 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 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 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**.

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 27 Controller Healthy

Intel Persistent Memory DIMM 35 Controller Healthy

Intel Persistent Memory DIMM 29 Controller Healthy

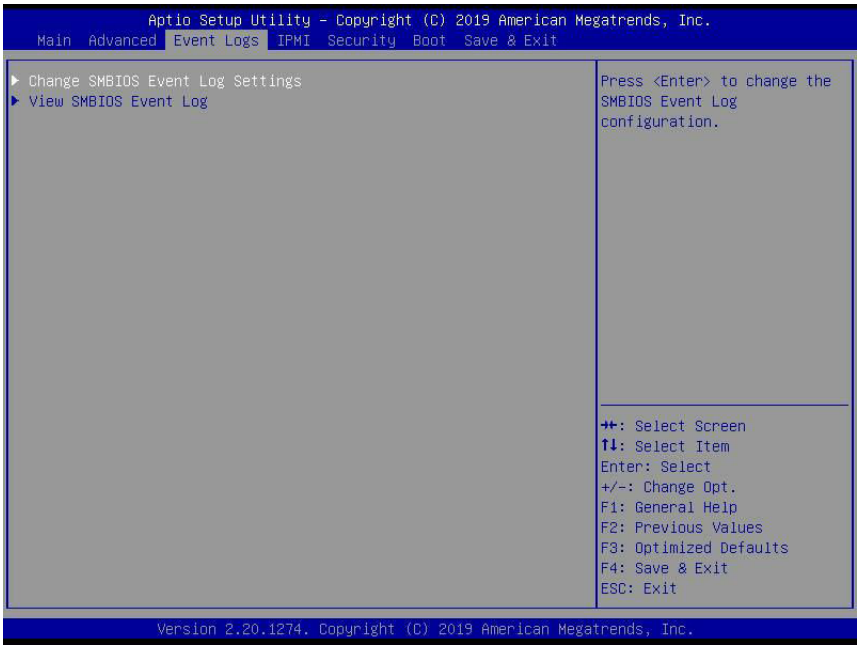
Intel Persistent Memory DIMM 37 Controller Healthy

▶Intel(R) DCPMM 1.0.0.3380 HII Driver Healthy

Controller 665c5c98 Child 0 Healthy

4.4 Event Logs

Use this feature to configure 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 Event Logging during system boot. The options are **Enabled** and Disabled.

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

MECI

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

METW

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

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

▶View SMBIOS Event Log

Select this submenu and press enter to see the contents of the SMBIOS event log. The following categories will be displayed: Date/Time/Error Codes/Severity

4.5 IPMI

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

BMC Firmware Revision

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

IPMI Status (Baseboard Management Controller)

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

▶System Event Log

Enabling/Disabling Options

SEL Components

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

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

▶BMC Network Configuration

BMC Network Configuration

Update IPMI LAN Configuration

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

Configure IPv4 Support

This section displays configuration features for IPv4 support.

IPMI LAN Selection

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

IPMI Network Link Status

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

If the feature above is set to Yes, the following feature will become available for 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 **DHCP** and Static.

If the feature above is set to Static, the following features will become available for configuration:

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

This feature displays the virtual LAN settings. The options are **Disable** and Enable.

Configure IPv6 Support

This section displays configuration features for IPv6 support.

LAN Channel 1

IPv6 Support

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

Configuration Address Source

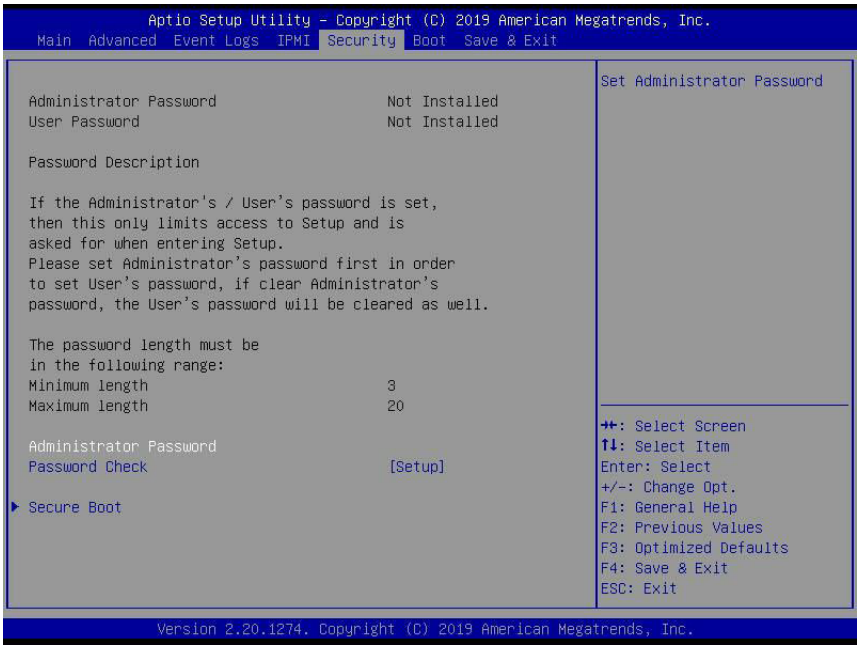
This feature allows the user to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol)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

If the feature above is set to Static, the following features will become available for configuration:

- Station IPv6 Address
- Prefix Length
- IPv6 Router1 IP Address

4.6 Security

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



Administrator Password

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

User Password

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

Password Check

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

▶Secure Boot

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

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

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

Secure Boot Mode

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

CSM Support

Select Enabled to support the EFI Compatibility Support Module (CSM), which provides compatibility support for traditional legacy BIOS for system boot. The options are **Enabled** and Disabled.

▶Key Management

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

Provision Factory Default Keys

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

▶Restore Factory Keys

Select Yes to install factory default Secure Boot keys set by the manufacturer. The options are **Yes** and No.

▶Reset to Setup Mode

Select Yes to delete all variables and reset the System to Setup Mode. The options are **Yes** and No.

▶Export Secure Boot variables

This feature allows the user to export Secure Boot variables to a folder in the system.

▶Enroll Efi Image

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

Device Guard Ready

▶Remove 'UEFI CA' from DB

This feature allows the user to remove 'UEFI CA' certificate from an authorized signature database. The options are **Yes** and No.

▶Restore DB defaults

This feature allows the user to restore DB variables to factory default. The options are **Yes** and No.

Secure Boot Variables

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

▶Platform Key (PK)

This feature allows the user to configure the settings of the platform keys. The options are **Details**, Export, Update, and Delete.

Update

Select Yes to load the new platform keys (PK) from the manufacturer's defaults. Select No to load the platform keys from a file. The options are **Yes** and No.

▶Key Exchange Keys

Update

Select Yes to load the KEK from the manufacturer's defaults. Select No to load the KEK from a file. The options are Yes and No.

Append

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

▶Authorized Signatures

Update

Select Yes to load the database from the manufacturer's defaults. Select No to load the DB from a file. The options are Yes and No.

Append

Select Yes to add the database from the manufacturer's defaults to the existing DB. Select No to load the DB from a file. The options are Yes and No.

▶Forbidden Signatures

Update

Select Yes to load the DBX from the manufacturer's defaults. Select No to load the DBX from a file. The options are Yes and No.

Append

Select Yes to add the DBX from the manufacturer's defaults to the existing DBX. Select No to load the DBX from a file. The options are Yes and No.

▶Authorized TimeStamps

Update

Select Yes to load the DBT from the manufacturer's defaults. Select No to load the DBT from a file. The options are Yes and No.

Append

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

▶OsRecovery Signatures

This feature uploads and installs an OSRecovery Signature. You may insert a factory default key or load from a file. The file formats accepted are:

1) Public Key Certificate

a. EFI Signature List

b. EFI CERT X509 (DER Encoded)

c. EFI CERT RSA2048 (bin)

d. EFI SERT SHA256 (bin)

2) EFI Time Based Authenticated Variable

When prompted, select "Yes" to load Factory Defaults or "No' to load from a file.

Update

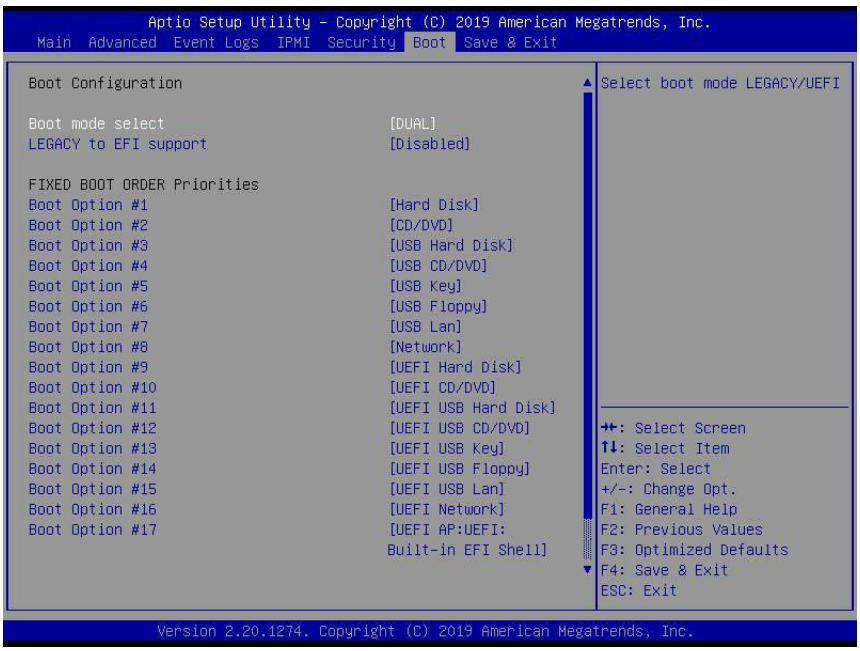
Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file. The options are Yes and No.

Append

This feature uploads and adds an OSRecovery Signature into the Key Management. You may insert a factory default key or load from a file. When prompted, select "Yes" to load Factory Defaults or "No' to load from a file.

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.**

Legacy to EFI Support

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

FIXED BOOT ORDER Priorities

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

If the feature "Boot Mode Select" above is set to Legacy, UEFI, or Dual, the following features will be displayed:

- Boot Option #1
- Boot Option #2
- Boot Option #3
- Boot Option #4
- Boot Option #5

- Boot Option #6
- Boot Option #7
- Boot Option #8
- Boot Option #9
- Boot Option #10
- Boot Option #11
- Boot Option #12
- Boot Option #13
- Boot Option #14
- Boot Option #15
- Boot Option #16
- Boot Option #17

▶Add New Boot Option

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

Add Boot Option

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

Path for Boot Option

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

Boot Option File Path

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

Create

Use this feature to set the name and the file path of the new boot option.

▶Delete Boot Option

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

Delete Boot Option

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

▶UEFI Application Boot Priorities

This feature sets the system boot order of detected devices. The options are **UEFI: Built-in EFI Shell** and Disabled.

- Boot Option #1

▶UEFI USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

▶USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

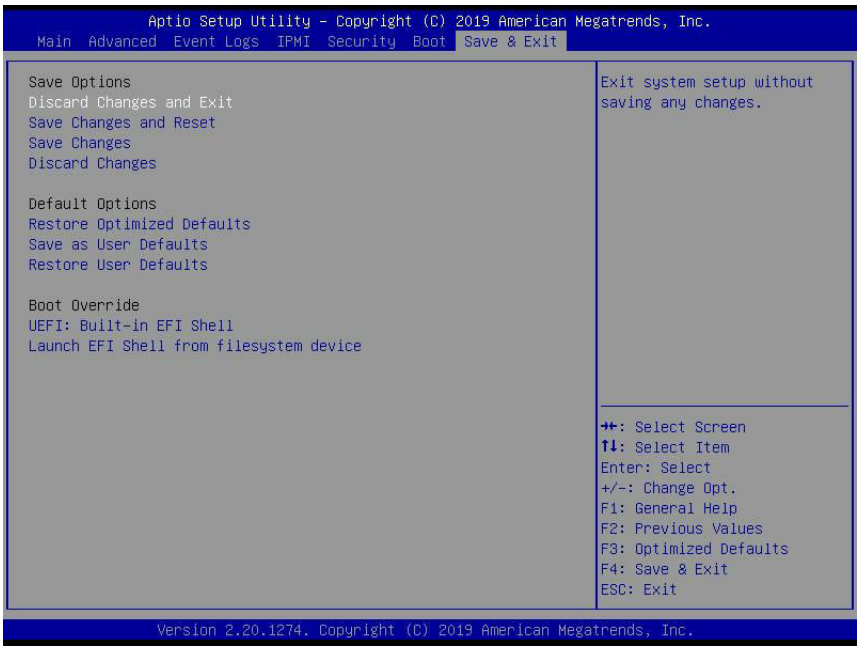
▶NETWORK Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

4.8 Save & Exit

Select the Save & Exit tab from the BIOS setup screen to configure the settings below:



Save Options

Discard Changes and Exit

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

Save Changes and Reset

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

Save Changes

When you have completed the system configuration changes, select this feature to leave the BIOS setup utility and reboot the computer for the new system configuration parameters to take effect. Select Save Changes from the Save & Exit menu and press <Enter>.

Discard Changes

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

Default Options

Restore Optimized Defaults

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

Boot Override

Listed in this section are other boot options for the system (i.e., Built-in EFI shell). Select an option and press <Enter>. Your system 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) routines, which are performed each time the system is powered on, errors may occur.

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

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

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

B.1 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.)

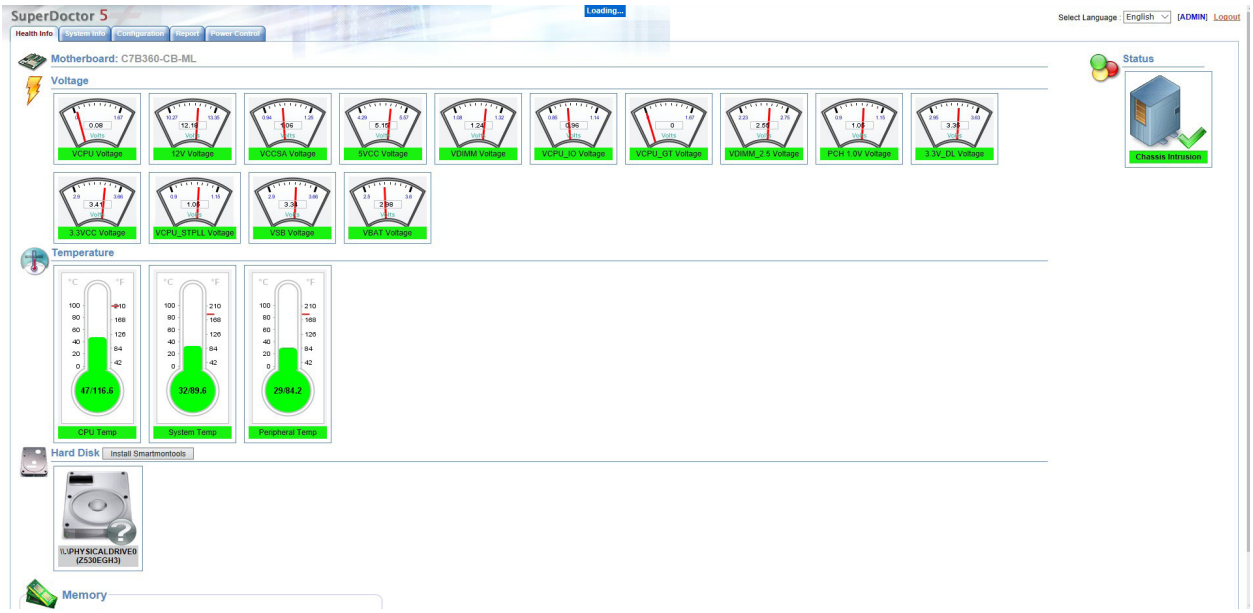
Another option is to go to the Supermicro website at http://www.supermicro.com/products/. Find the product page for your motherboard, and "Download the Latest Drivers and Utilities". Insert the flash drive or disk and the screenshot shown below should appear.

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.2 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.



B.3 IPMI

The X11SPA-TF/-F 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.4 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 اسحبذال البطارية بطريقة غير صحيحة فعليل
اسحبذال البطارية
فقط بنفس النبع أو ما يعادلها مما أوصث به الشرمة المصنعة
جخلص من البطاريات المسحعملة وفقا لحعليمات الشرمة الصانعة

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

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

Product Disposal

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

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

警告
本产品的废弃处理应根据所有国家的法律和规章进行。

警告
本產品的廢棄處理應根據所有國家的法律和規章進行。

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

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

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

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

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

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

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

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 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.

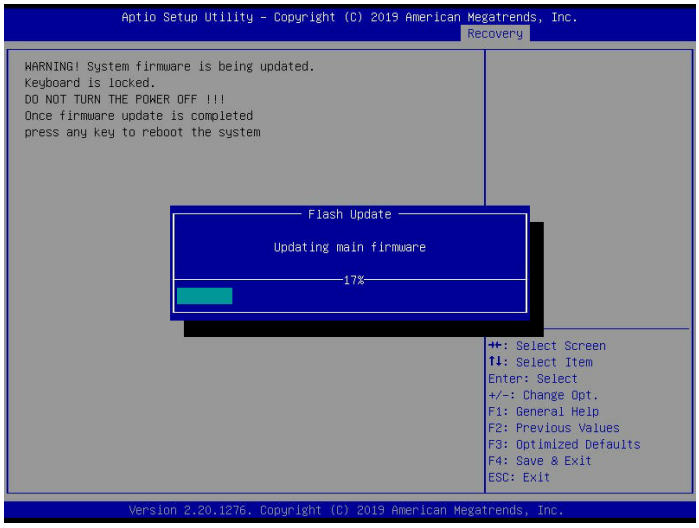
4. Insert the USB device that contains the SUPER.ROM file into the system before you power on the system or when the following screen appears.

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.

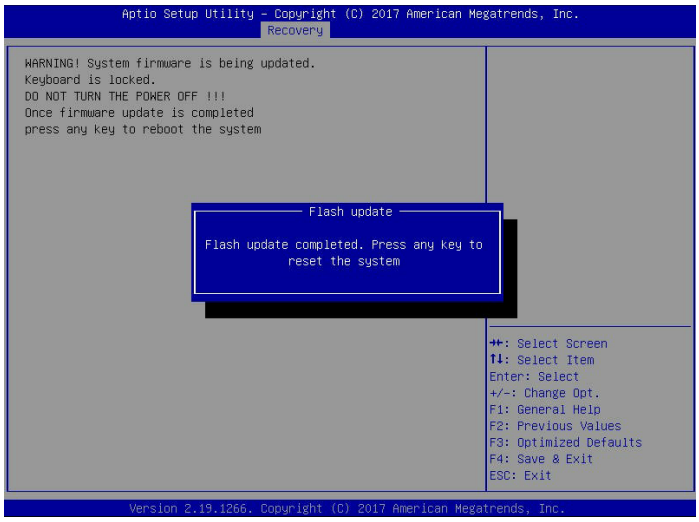
6. When the screen as shown above displays, use the arrow keys to select the item "Proceed with flash update" and press the <Enter> key. You will see the BIOS recovery progress as shown in the screen below.

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



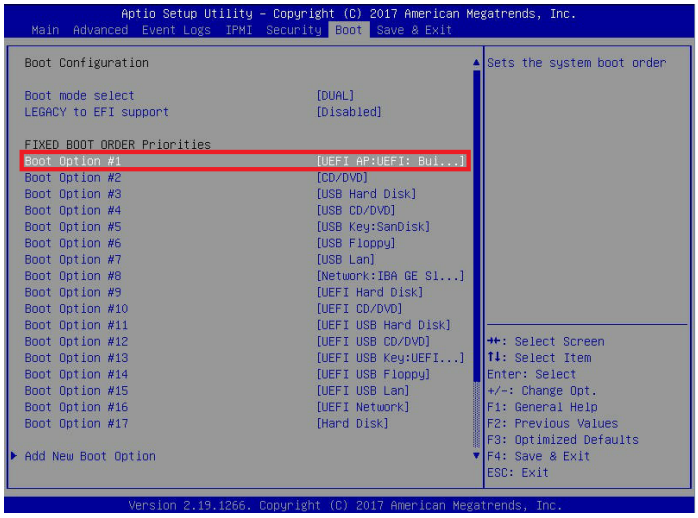
Note: *Do not interrupt this process* until the BIOS flashing is complete.

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

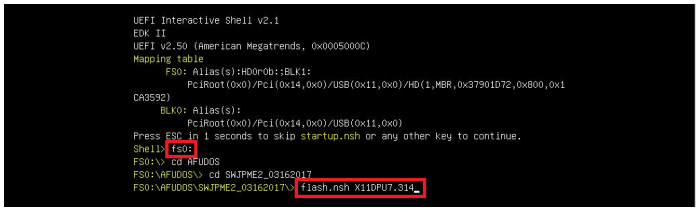


Note: It is recommended that you update your BIOS after BIOS recovery. Please refer to Chapter 3 for BIOS update instructions.

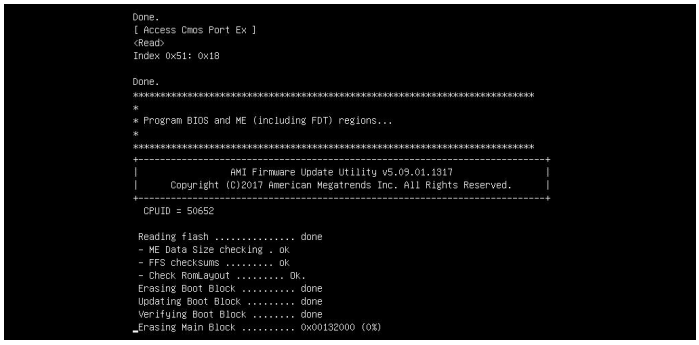
8. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the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



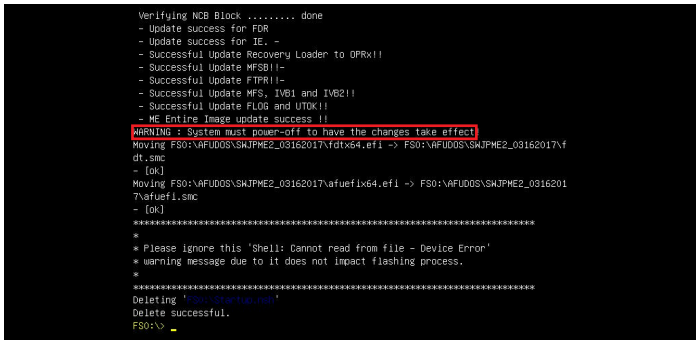
9. When the UEFI Shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 2. Enter flash.nsh BIOSname#.### at the prompt to start the BIOS update process.



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.



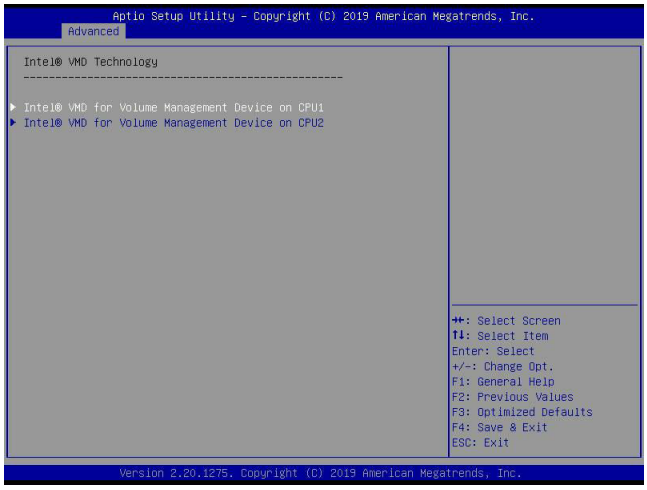
Appendix E

Configuring VROC RAID Settings

Intel Virtual RAID on CPU (Intel VROC) is a Redundant Array of Independent Disks (RAID) solution, which 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 All Intel VMD Controllers menu items. The E.2 section explains RAID settings. The E.3 section describes the use of journaling drive for the RAID5 volume (parity based RAID).

E.1 All Intel VMD Controllers Features

Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Advanced tab. Use the arrow keys and press <Enter> to select Chipset Configuration -> North Bridge -> IIO Configuration -> Intel VMD Technology. The following screen will appear.

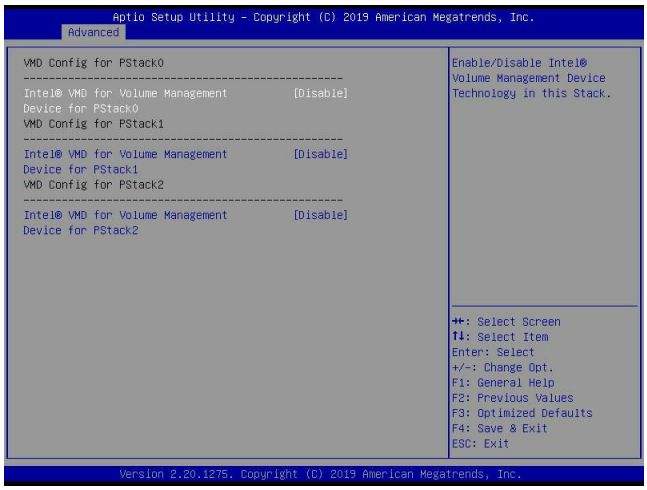


Step 1. Use the arrow keys to select Intel VMD for Volume Management Device on CPU1 and press <Enter> to access the menu items.

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.tw/.

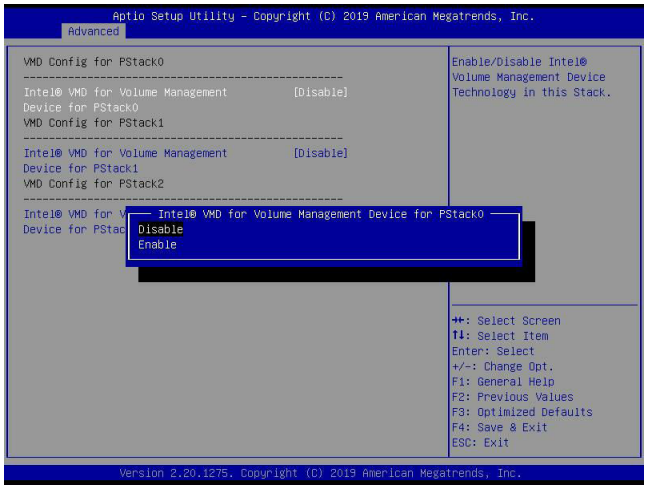
Note 2: Depending on the version of driver/utility/package, it may or may not have exactly the same as the BIOS settings/features shown in the appendix.

The following screen will appear.

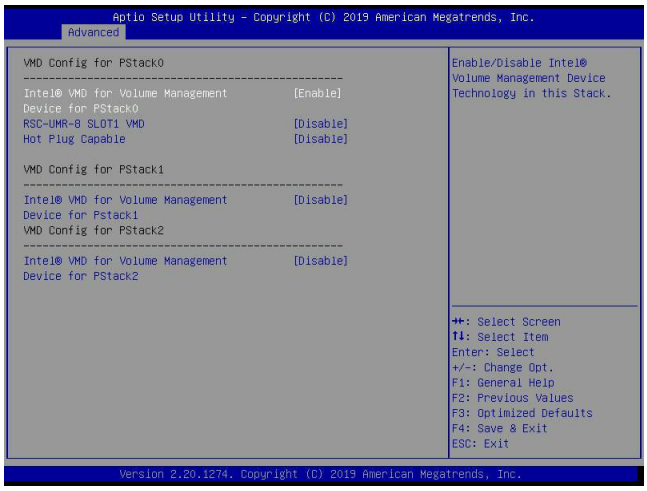


Step 2. **Intel VMD for Volume Management Device for PStack0**

The options are **Disable** and Enable. Set this feature to Enable.

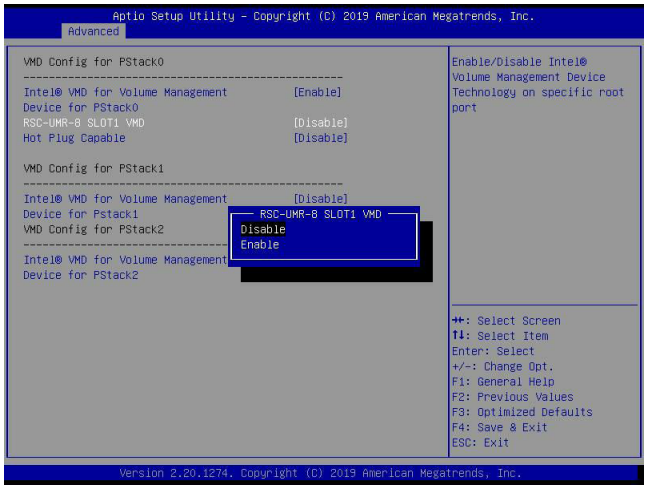


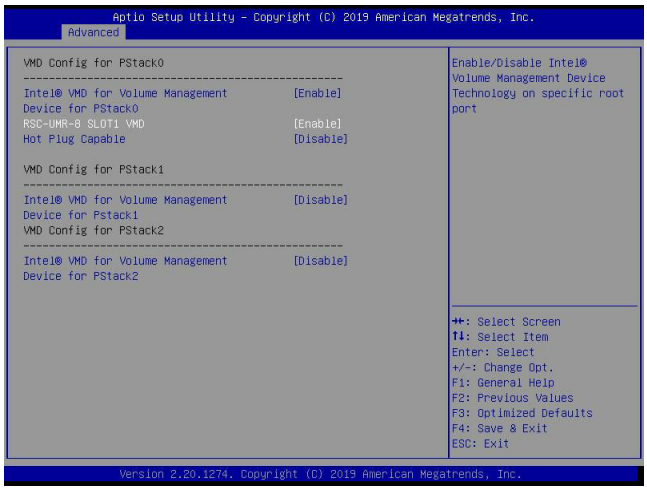
Press <Enter> and the following screen will appear.



Step 3. **RSC-UMR-8 SLOT1 VMD**

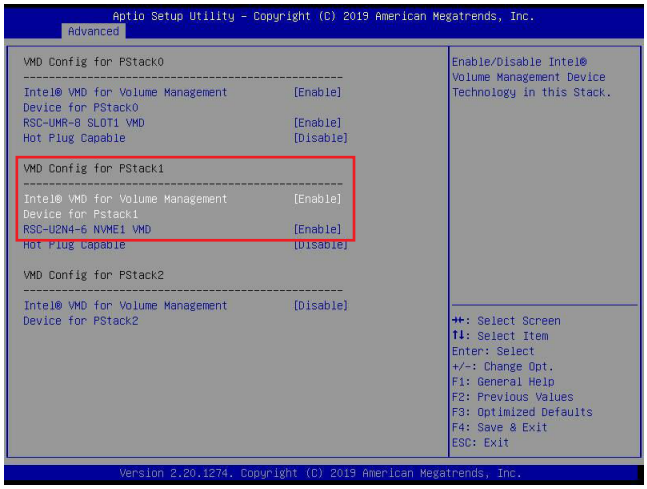
The feature is dependent on your motherboard/system and devices attached to the Intel VMD controllers. The options are **Disable** and Enable. Set this feature to Enable.





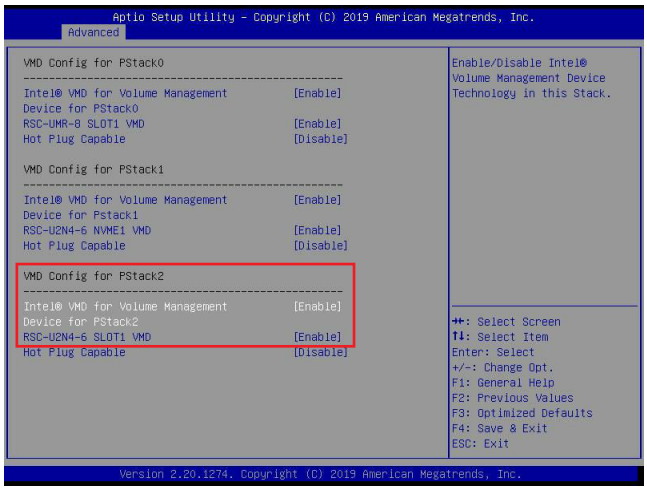
Step 4. **Intel VMD for Volume Management Device for PStack1, RSC-U2N4-6 NVME1 VMD**

The options are **Disable** and Enable. Set the two features to Enable. (Refer to pages 165 and 166 for more information.)

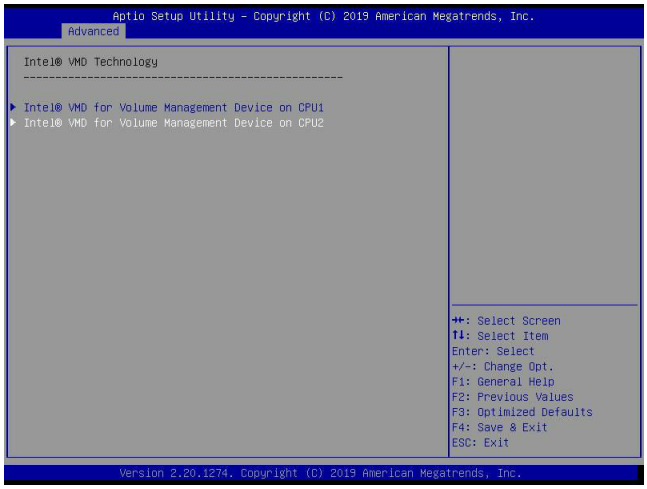


Step 5. **Intel VMD for Volume Management Device for PStack2, RSC-U2N4-6 SLOT1 VMD**

The options are **Disable** and Enable. Set the two features to Enable. (Refer to pages 165 and 166 for more information.)

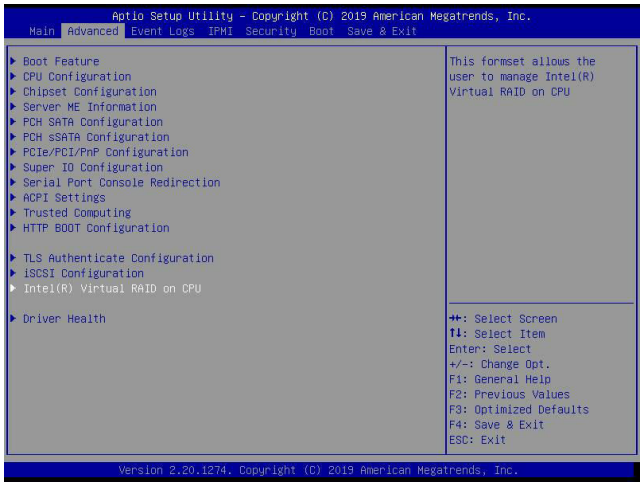


Press <Esc> and return to the main screen of Intel VMD Technology as shown below. Use the arrow keys to select Intel VMD for Volume Management Device on CPU2 and press <Enter> to access the menu items.

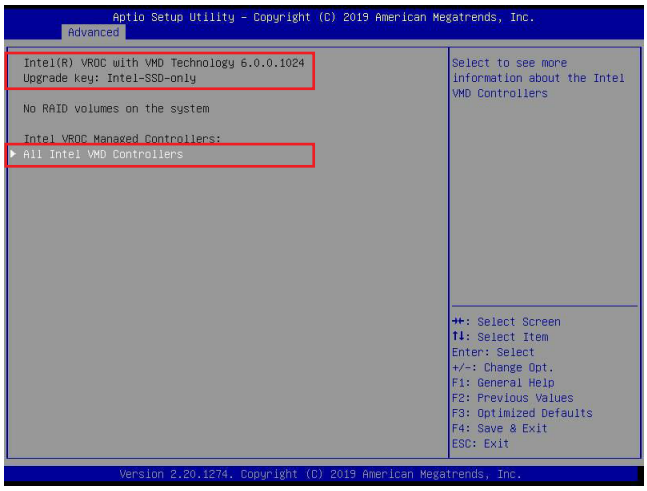


Repeat the steps (Step 1 ~ Step 5) on pages 164, 165, 166, and 167 to enable Intel VMD for Volume Management Device for PStack0/PStack1/PStack2 and devices attached to the Intel VMD controllers. For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility.

Navigate to the Advanced tab.



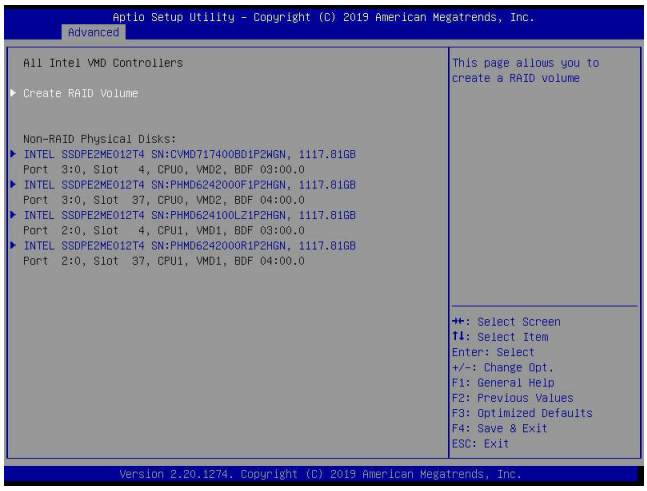
Use the arrow keys to select Intel(R) Virtual RAID on CPU and press <Enter> to access the menu items. The following screen will appear and the All Intel VMD Controllers feature has become available.



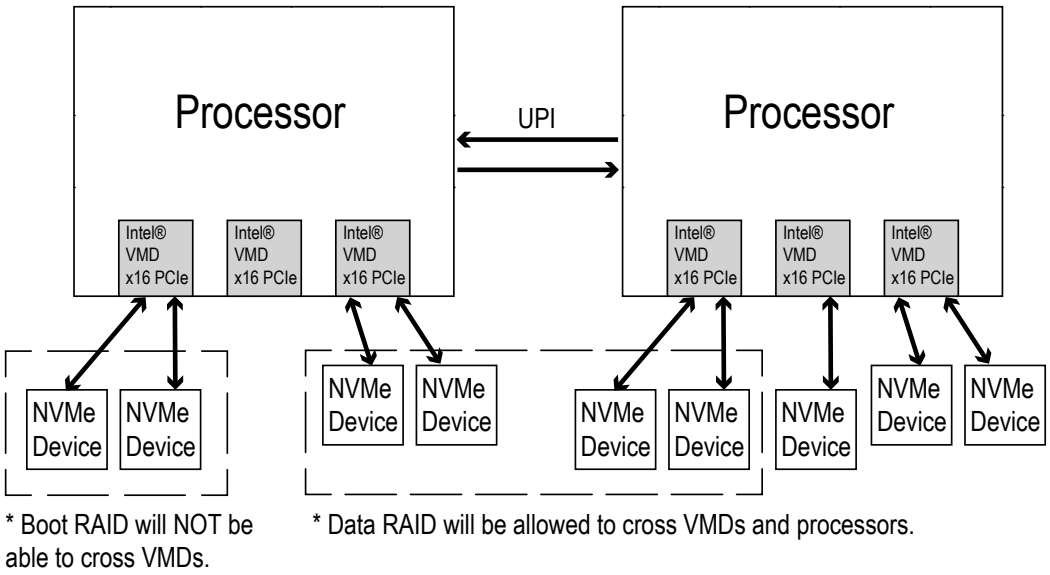
Note 1: The license and header (on the motherboard) for Intel VROC hardware key are required. Also, be sure the version of Intel Rapid Storage Technology enterprise (Intel RSTe) VROC utility is 5 or above (look for Intel(R) VROC with VMD Technology x.x.x.xxxx shown on the screen).

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

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.

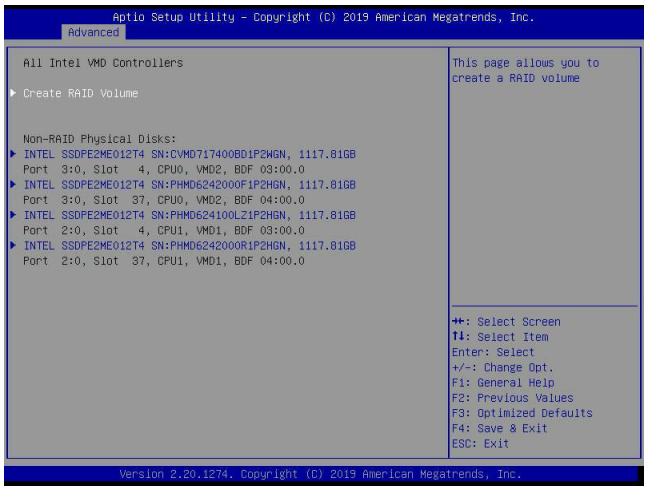


Note : A single Intel VMD supported processor supplies 48 PCIe lanes and contains three Intel VMD controllers (domains). Refer to the following illustration for more information.

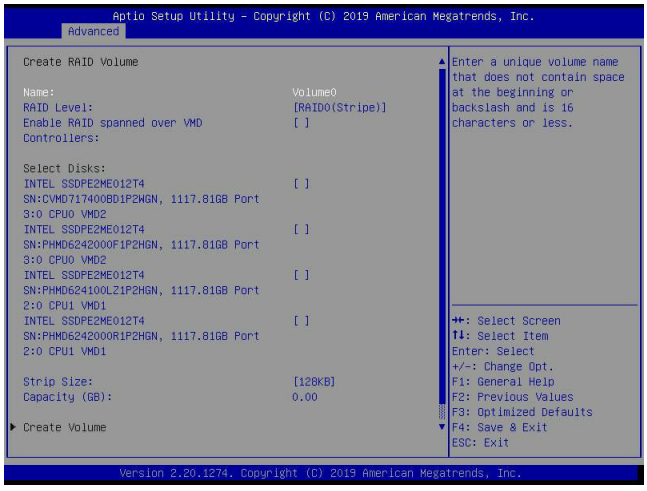


E.2 Configuring RAID Settings

Refer to the instructions stated in E.1 section to access All Intel VMD Controllers menu items. Follow the steps below to create RAID volume(s).

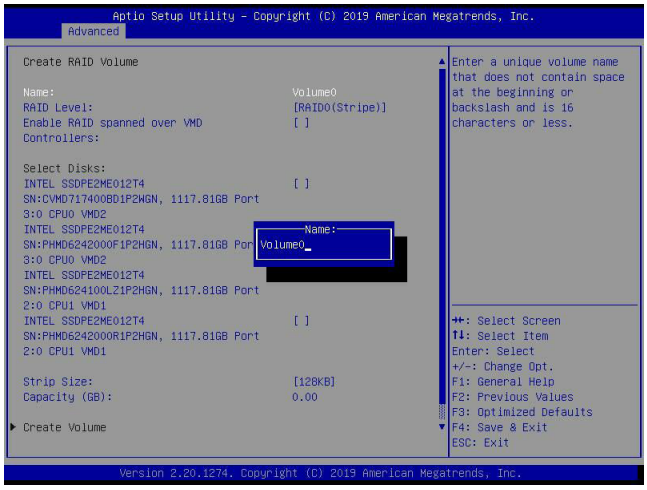


Step 1. To create RAID volume(s), use the arrow keys to select Create RAID Volume and press <Enter>. The following screen will appear.



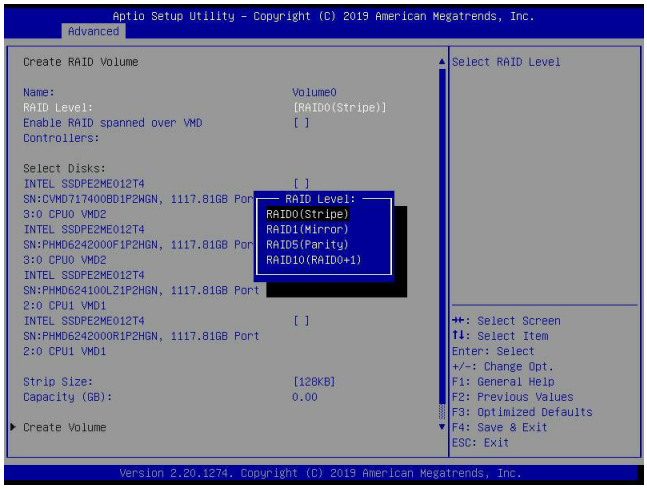
Step 2. **Name:**

This feature allows the user to enter the unique name of the RAID volume.



Step 3. **RAID Level:**

This feature allows the user to select the RAID level. The options are **RAID0(Stripe)**, RAID1(Mirror), RAID5(Parity), and RAID10(RAID0+1).

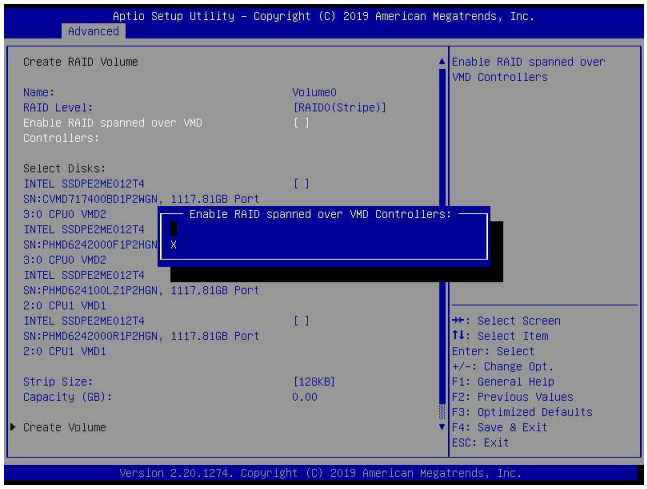


Note 1: The RAID level(s) displayed is(are) based on the number of NVMe devices connected to the system.

Note 2: 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.

Step 4. **Enable RAID spanned over VMD Controllers**

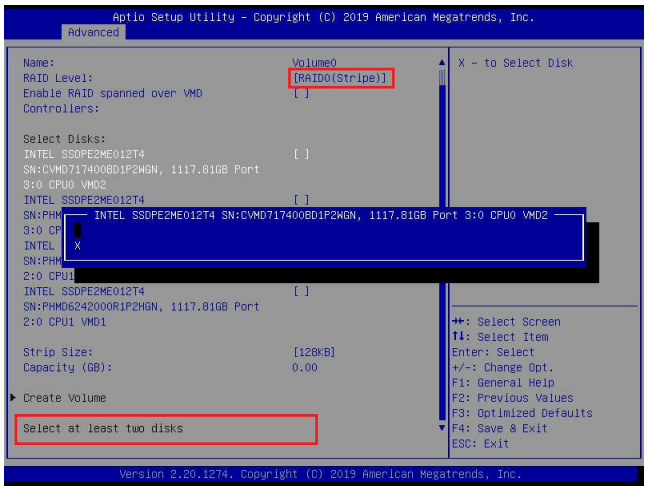
The options are **(not selected)** and X (selected). Set this feature to X if the RAID level you selected earlier from Step 3 will cross VMD domains.



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

Step 5. **Select Disks:**

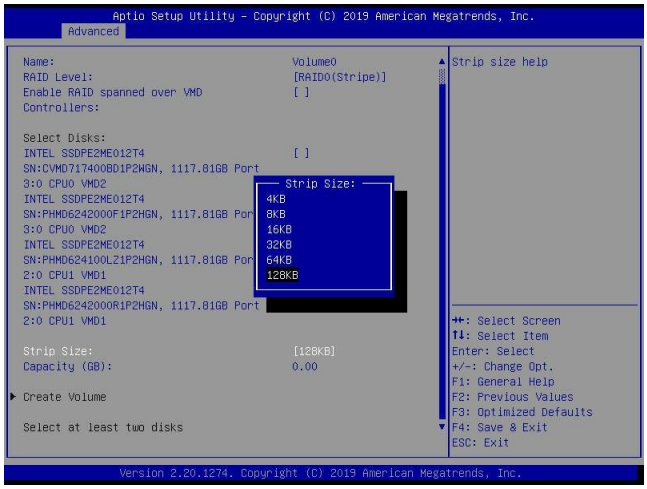
The options are **(not selected)** and X (selected). Set the features one by one to X to select the desired RAID disks.



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

Step 6. **Strip Size:**

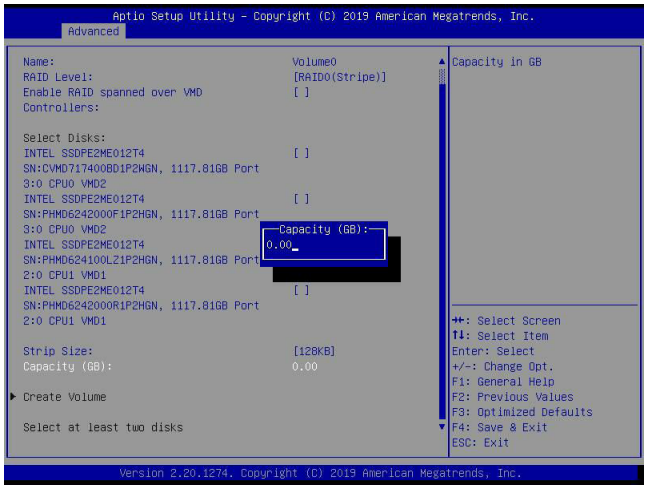
Use this feature to select the RAID strip size. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**.



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

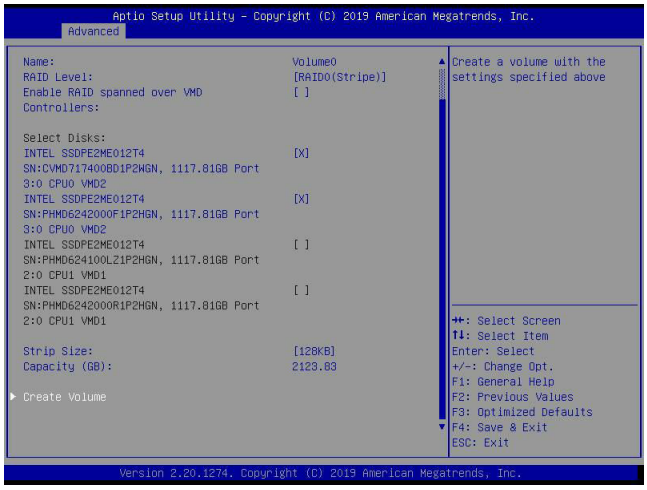
Step 7. **Capacity (GB):**

This feature allows the user to enter the desired RAID capacity (in GB).

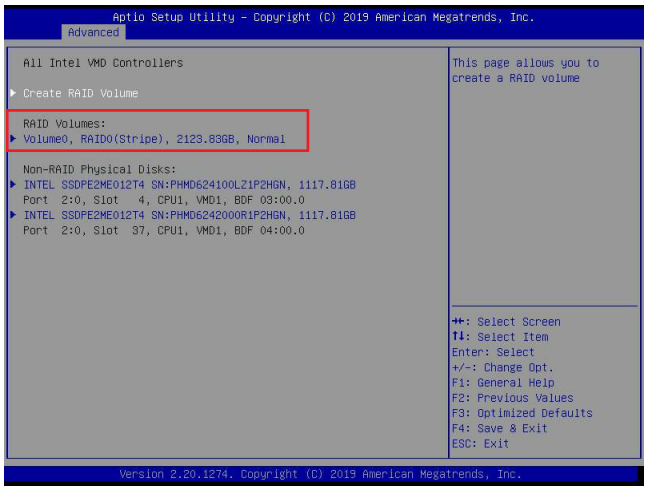


Step 8. **Create Volume**

Use the arrow keys to select Create Volume.

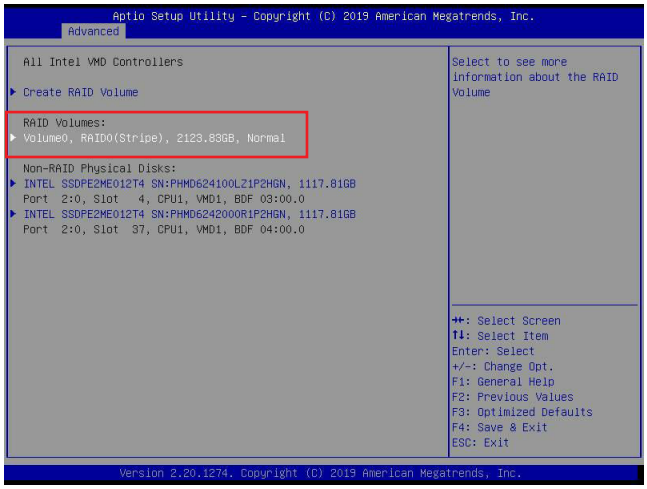


This feature is to create a RAID level with settings shown on the screen. Press <Enter> and the following screen will appear. It displays all RAID volumes.



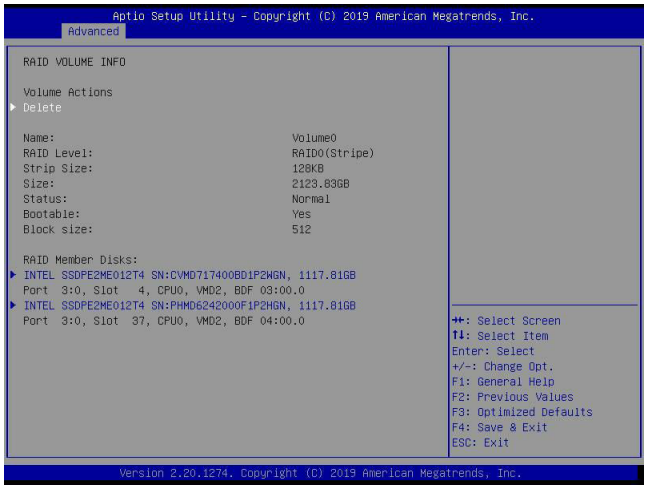
RAID Volumes:

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



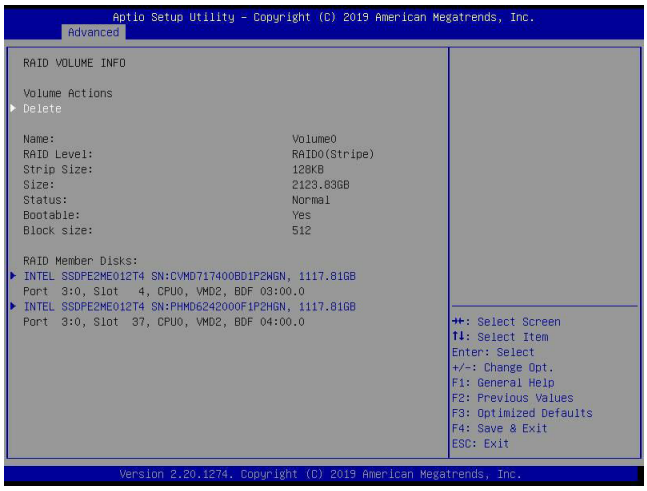
RAID VOLUME INFO

Press <Enter> and the following screen will appear.

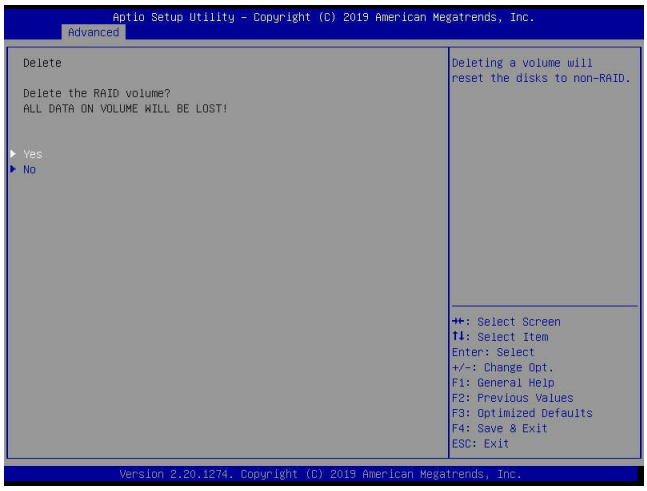


Delete

On the RAID VOLUME INFO screen, use the arrow keys to select Delete and press <Enter> to delete the RAID volume you have selected earlier (see the previous page for the RAID volume selection).

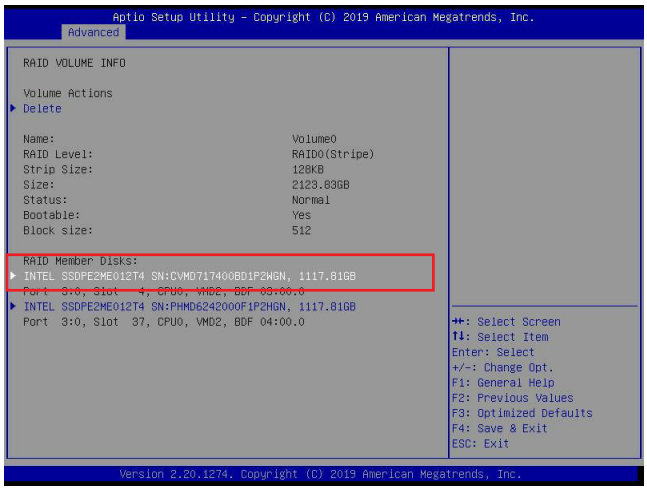


The following screen will appear. The options are **Yes** and No.

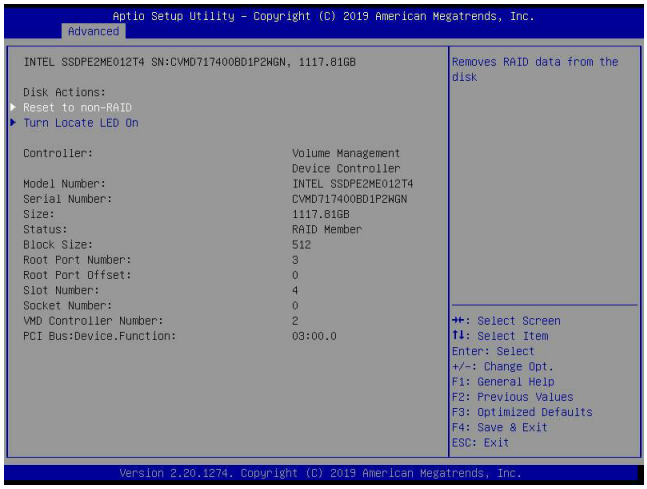


Reset to non-RAID

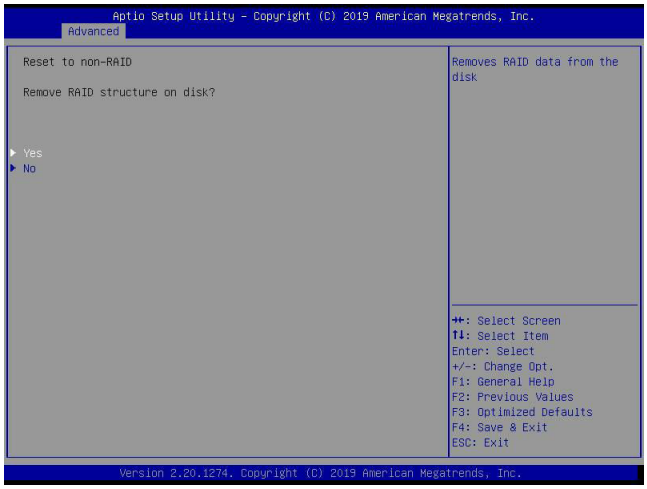
On the RAID VOLUME INFO screen (see page 176 for more information), select the desired NVMe device from the list of RAID Member Disks.



Press <Enter> and the following screen will appear.



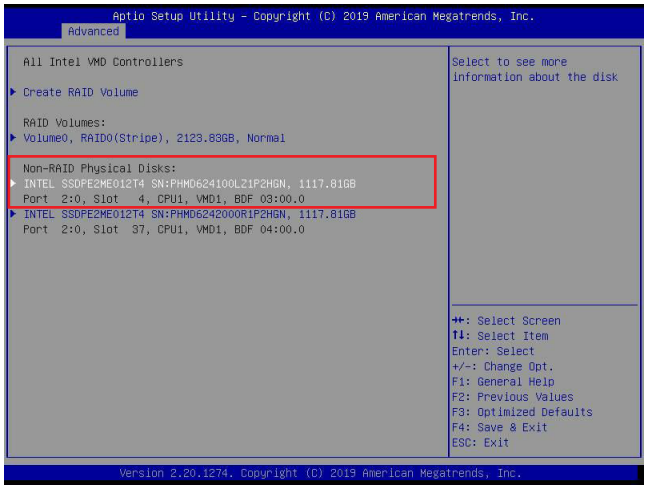
The feature, Reset to non-RAID, allows the user to remove RAID data from the selected NVMe device. Press <Enter> and the following screen will appear. The options are **Yes** and No.



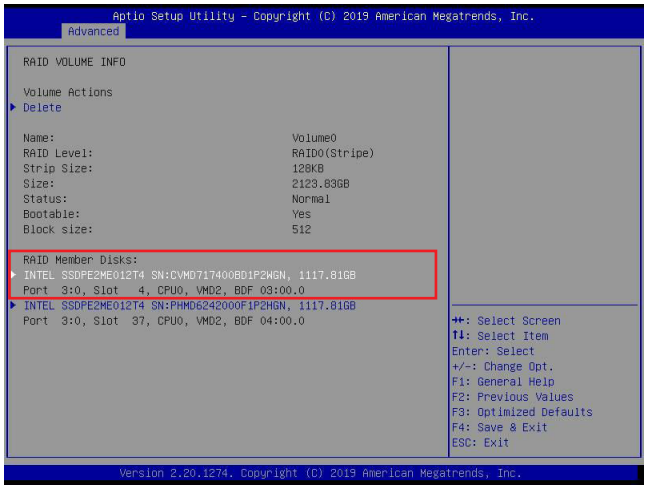
Turn Locate LED On

Use this feature to locate the selected device.

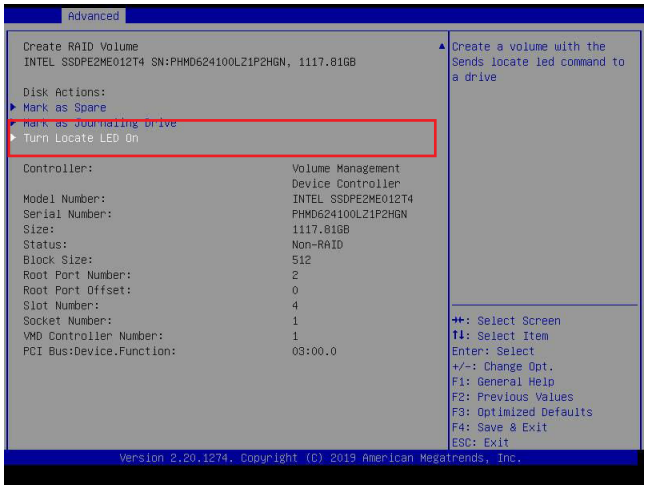
Select a non-RAID physical disk.



Or select a RAID member disk.

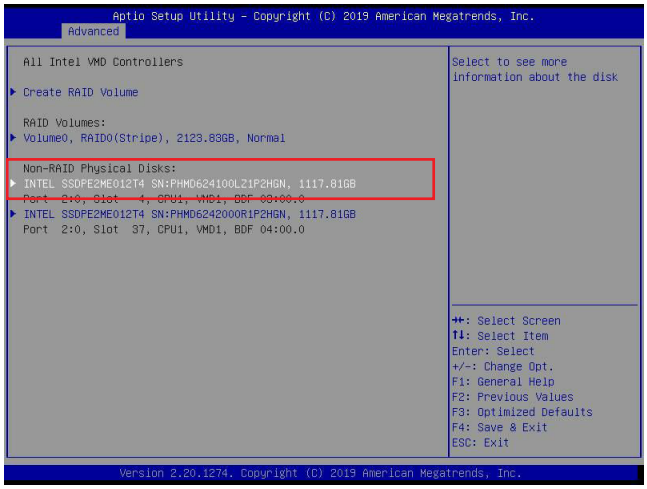


When the following screen appears, use the arrow keys to select Turn Locate LED On. Press <Enter> to locate the selected device.

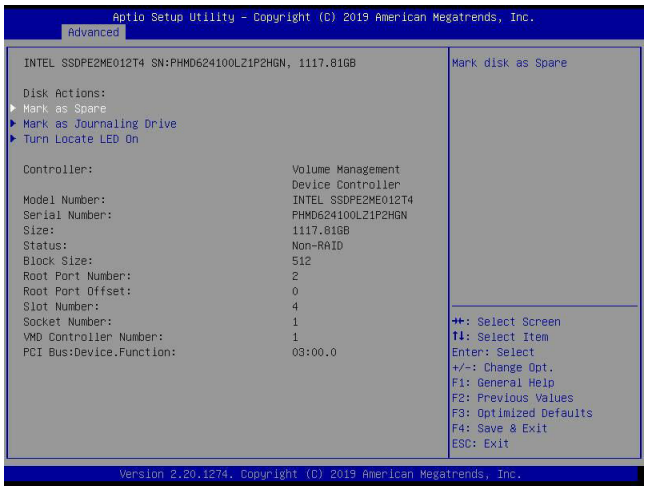


Mark as Spare

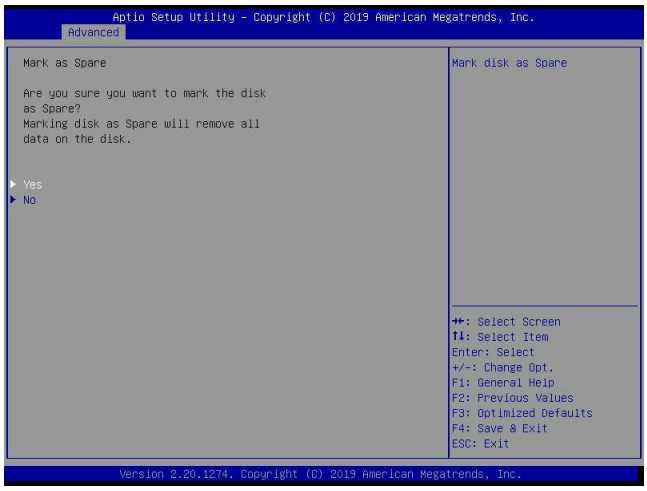
Refer to the instructions stated in E.1 section to access All Intel VMD Controllers menu items. When the following screen appears, select the desired NVMe device from the list of Non-RAID Physical Disks.



Press <Enter> and the following screen will appear.



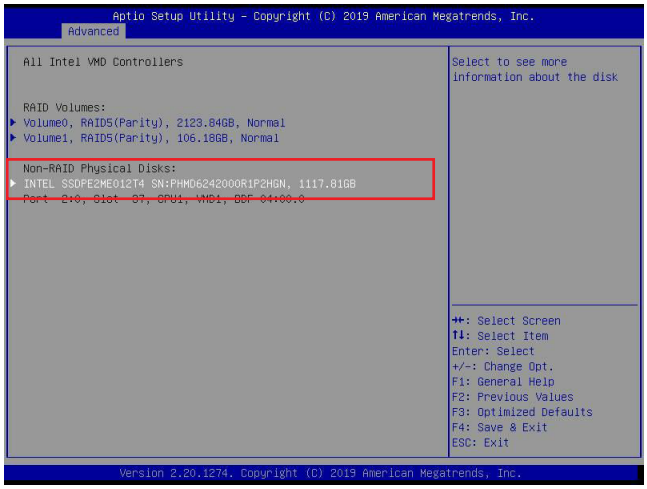
The feature, Mark as Spare, allows the user to set the selected NVMe device as a spare disk. Use the arrow keys to select Mark as Spare and press <Enter>. The following screen will appear. The options are **Yes** and No.



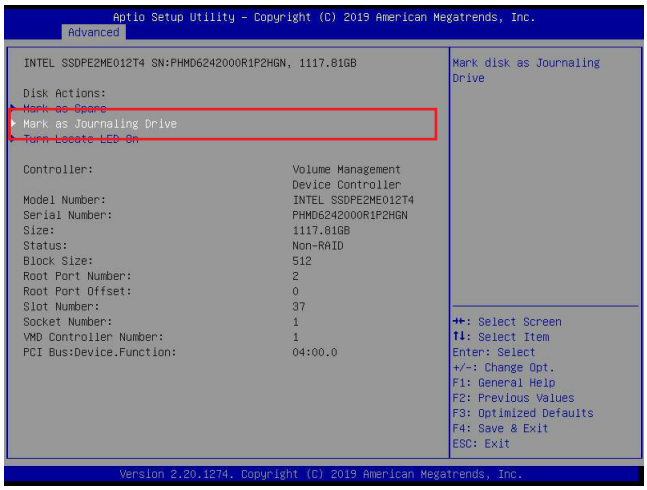
Note: A spare disk is used for automatic RAID volume rebuilds when status of failed, missing, or at risk is detected on the array disk. For a RAID0 volume, only status of at risk will trigger automatic RAID volume rebuilds.

Mark as Journaling Drive

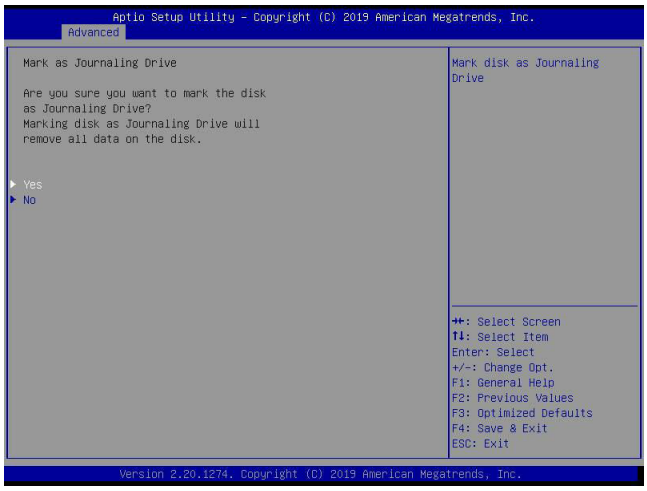
Refer to the instructions stated in E.1 section to access All Intel VMD Controllers menu items. When the following screen appears, select the desired NVMe device from the list of Non-RAID Physical Disks.



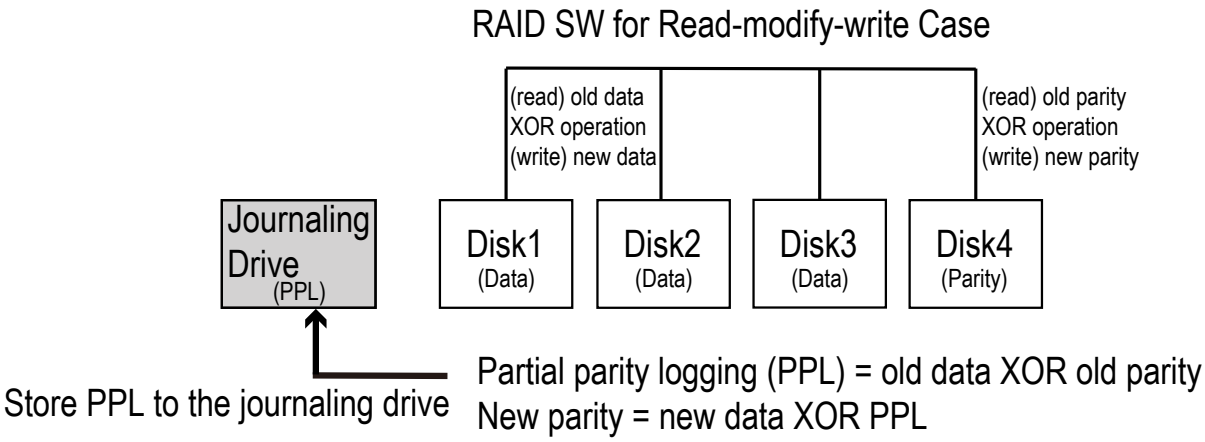
Press <Enter> and the following screen will appear.



The feature, Mark as Journaling Drive, allows the user to set the selected NVMe device as a journaling drive. Use the arrow keys to select Mark as Journaling Drive and press <Enter>. The following screen will appear. The options are **Yes** and No.



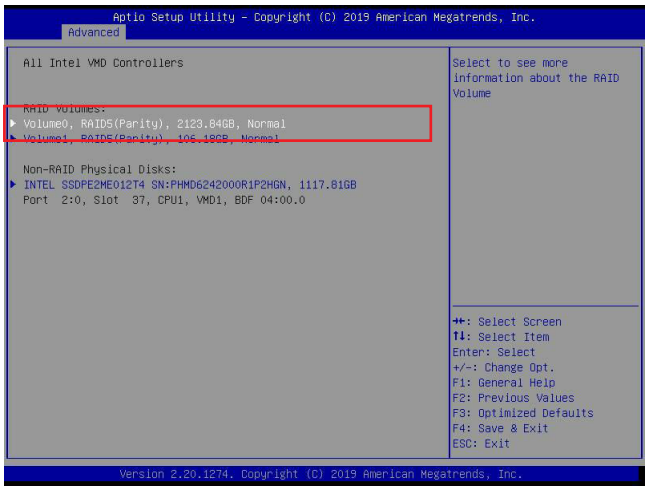
Note: RAID Write Hole (RWH) is a condition associated with a power/drive-failure/crash while writing to a RAID5 volume. The use of journaling drive that contains partial parity logging (PPL) can reduce the potential data loss. Refer to the following illustration for the use of journaling drive.



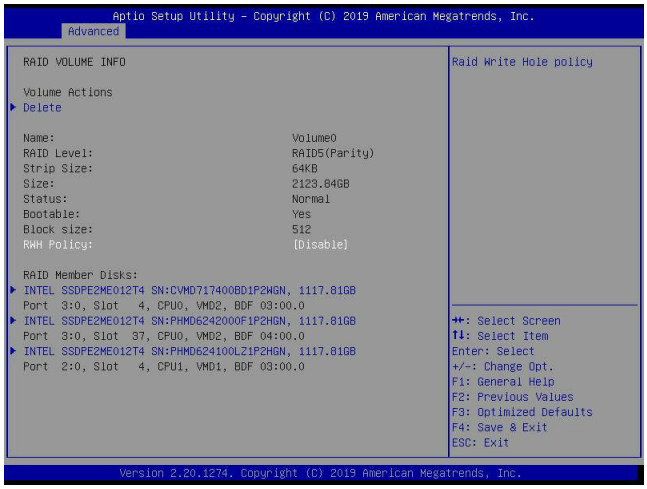
E.3 Use of Journaling Drive

The following steps describe the use of journaling drive for the RAID5 volume (parity based RAID).

Step 1. Refer to the instructions stated in 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.



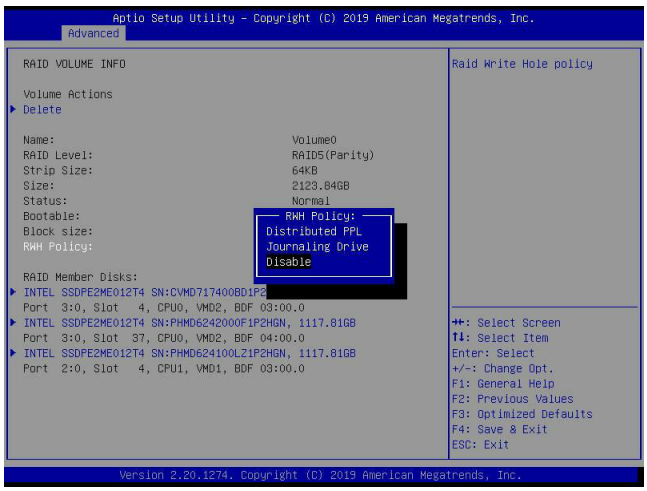
Press <Enter> and the following screen will appear.



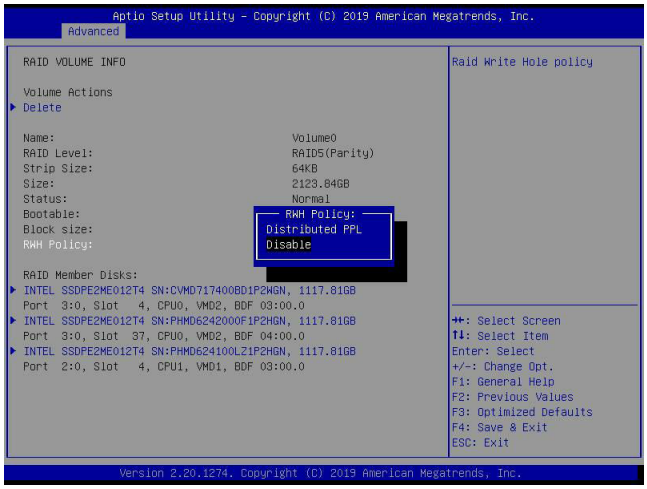
Step 2. Use the arrow keys to select RWH Policy. RWH is a scenario related to a power/drive-failure/crash.

RWH Policy

Press <Enter> and the following screen will appear. If any device has been set as a journaling drive (see pages 182 and 183), the options are Distributed PPL, Journaling Drive, and **Disable**.



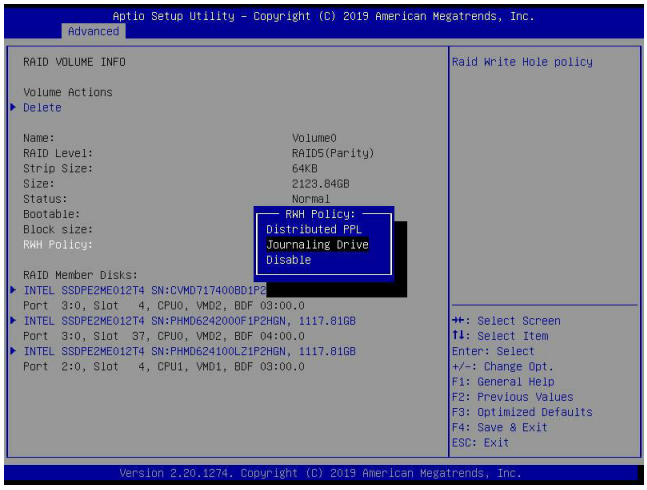
If no device has been set as a journaling drive, the options are Distributed PPL and **Disable**.



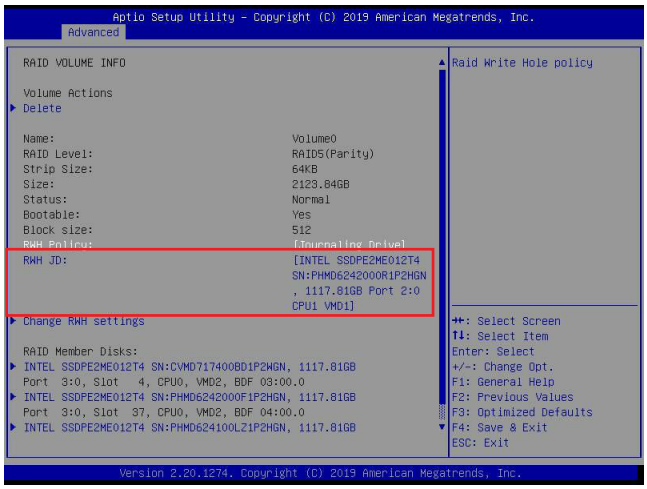
Note 1: Partial parity logging (PPL) can be defined as the result of XOR calculation of old data and old parity. PPL is a feature available for RAID5 volumes. While a power/drive-failure/crash occurring, PPL information helps rebuild the RAID volume and reduce the potential data loss.

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.

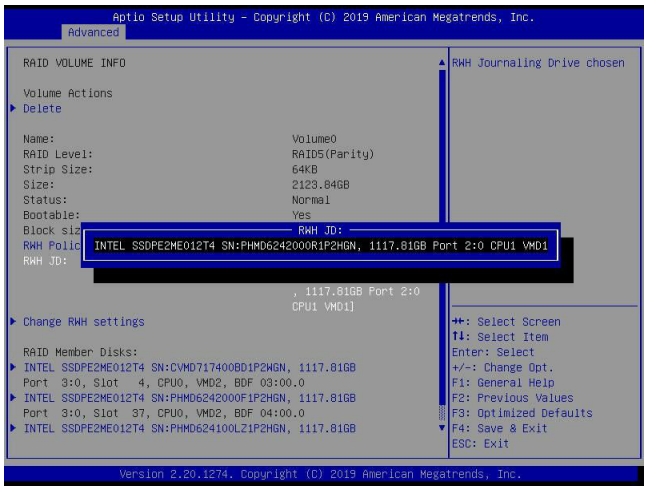


Press <Enter> and the RWH JD feature will become available as shown below.



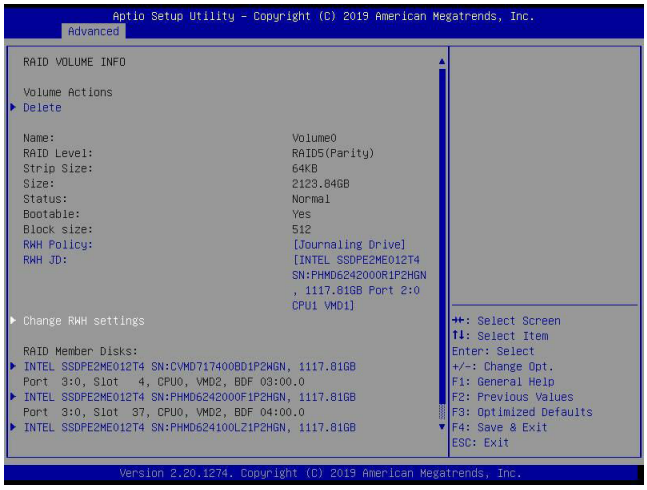
RWH JD

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).

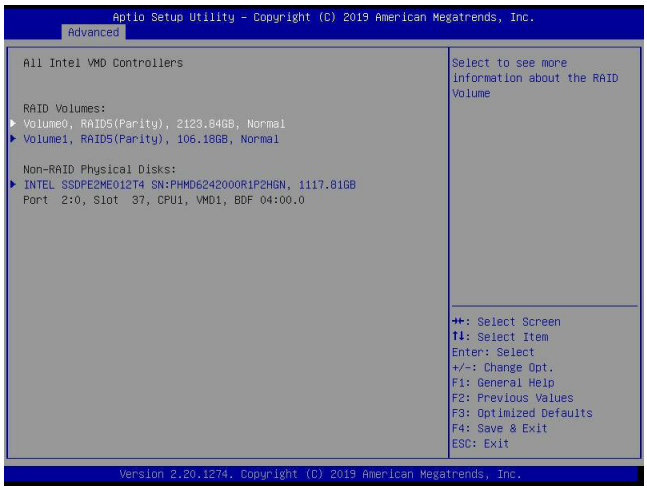


Step 4. Use the arrow keys and press <Enter> to select the desired journaling drive from the option list of RWH JD.

Step 5. For the changes to take effect, use the arrow keys to select Change RWH settings and press <Enter>.



The user will be returned to the main screen of All Intel VMD Controllers as shown below.



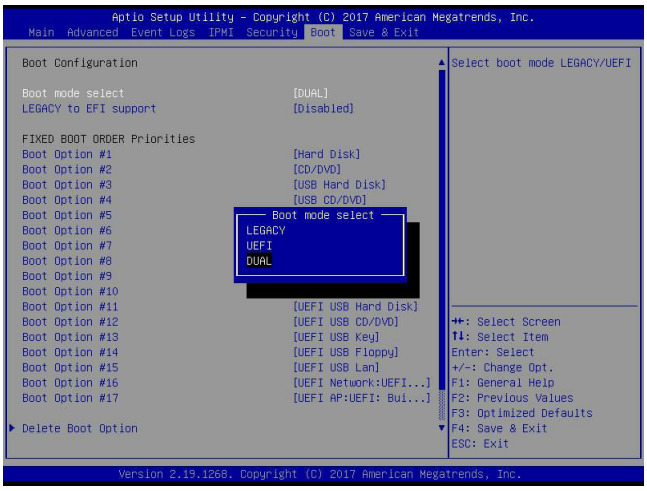
Appendix F

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.

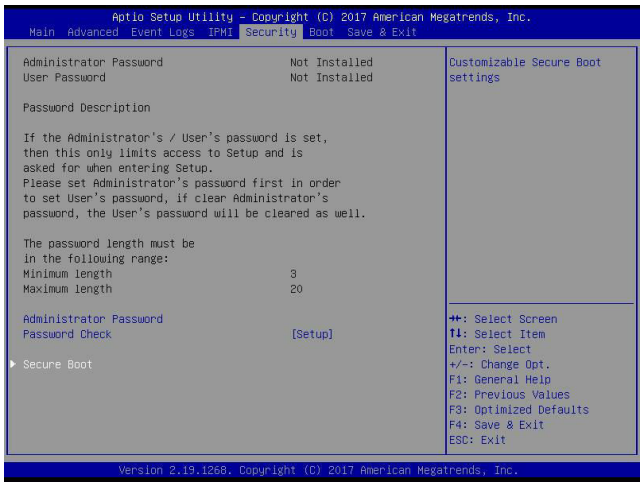
F.1 Boot mode select Feature

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.

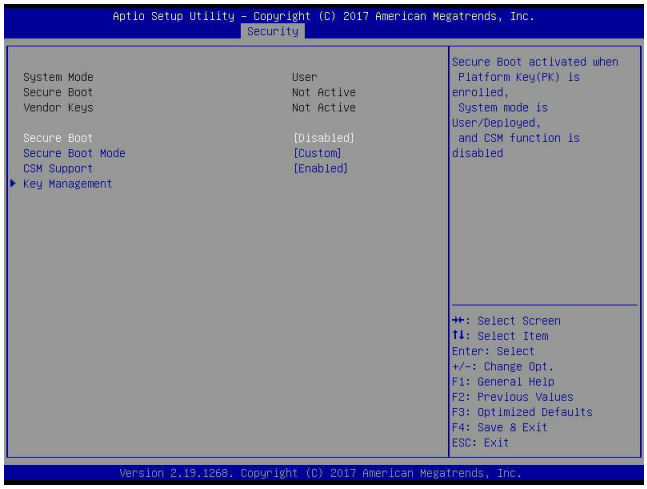


F.2 Secure Boot/ Secure Boot Mode/ CSM Support Features

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 preregistered 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.

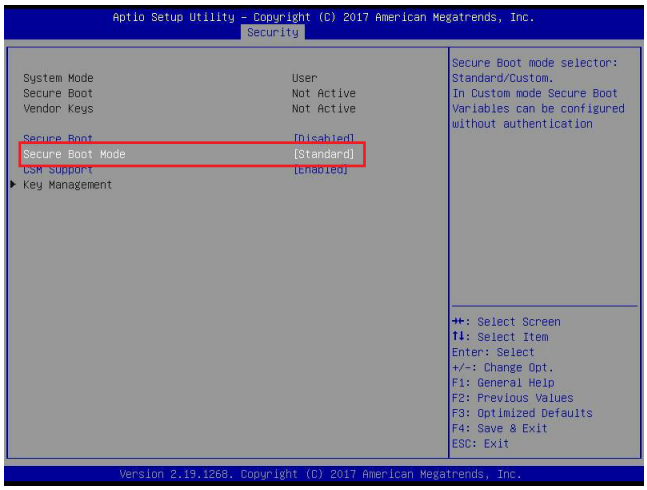
CSM Support

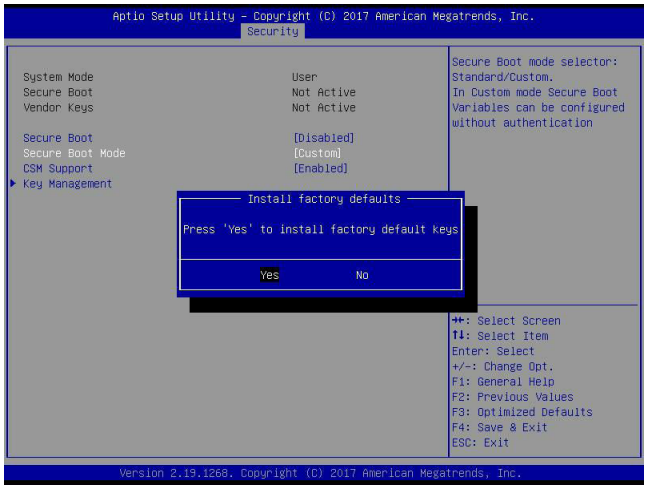
Select Enabled to support the legacy CSM, which provides compatibility support for traditional legacy BIOS for system boot. The options are Disabled and **Enabled**.

F.3 Secure Boot Settings

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

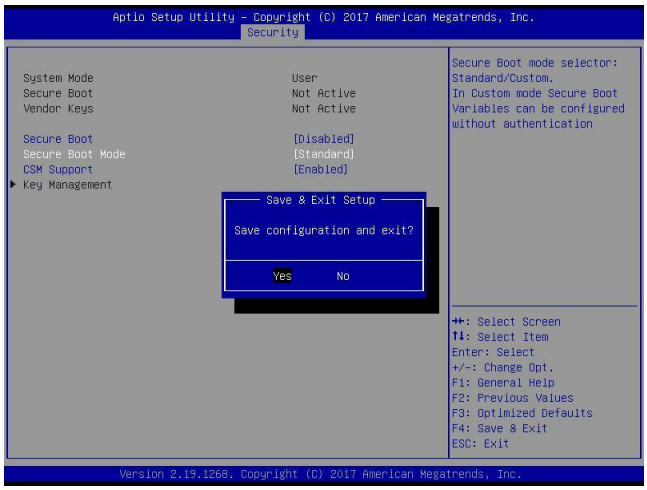
Step 1. Set Secure Boot Mode to Standard. Press Yes to install factory default keys as needed.



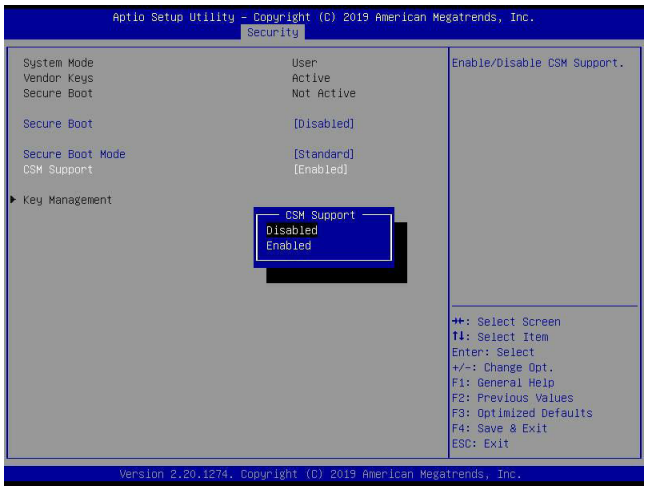


Note: The Key Management menu will become unavailable when Secure Boot Mode is set to Standard.

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

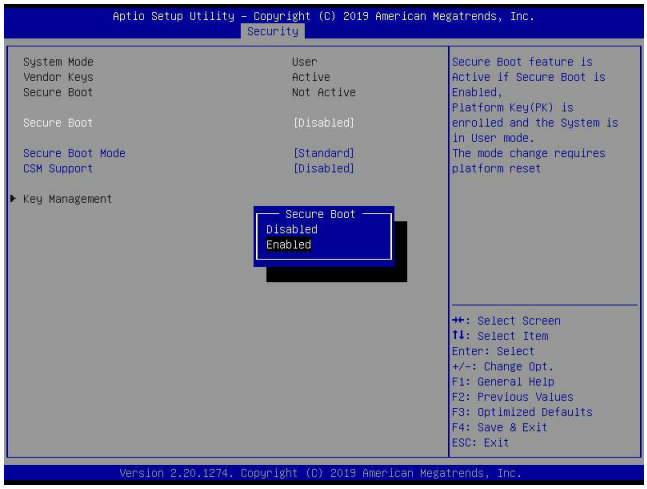


Step 3. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. Set CSM Support to Disabled.

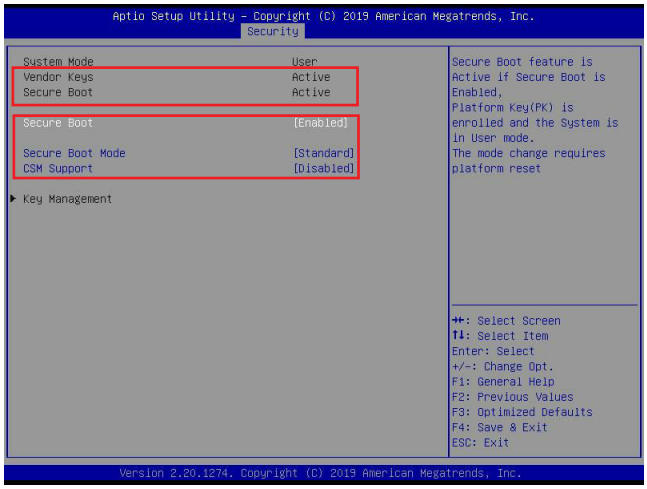


For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

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.



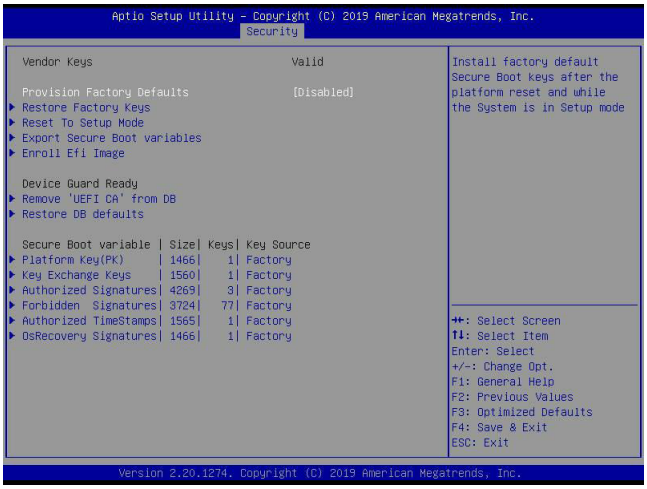
For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. The following screen will appear.



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.

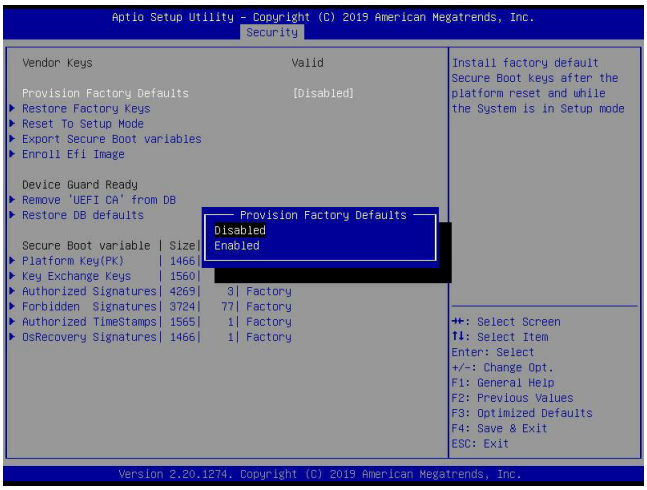
F.4 Key Management Settings

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.



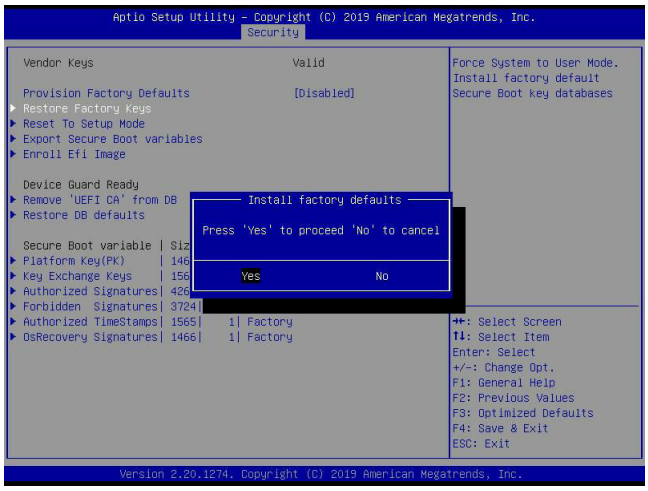
Provision Factory Defaults

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.



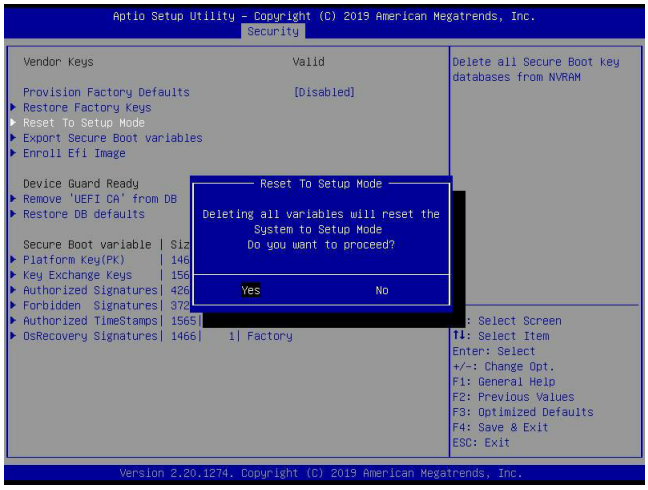
▶Restore Factory Keys

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.



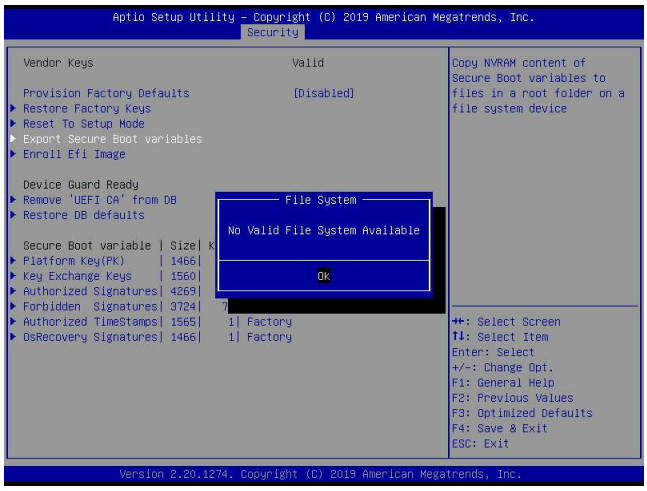
▶Reset To Setup Mode (available when the System Mode is in User mode)

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



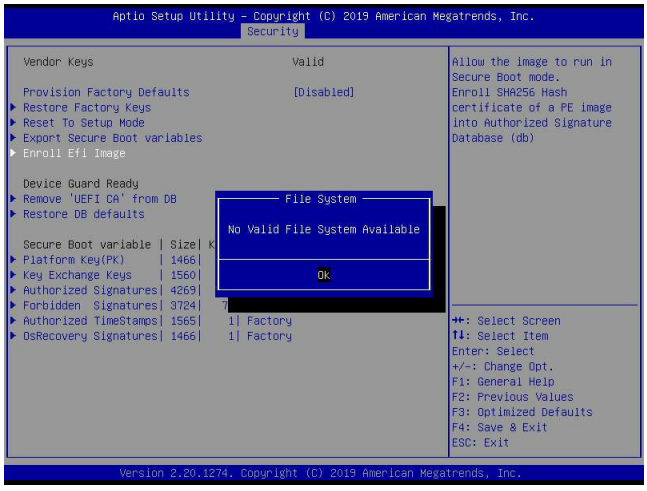
▶Export Secure Boot variables

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



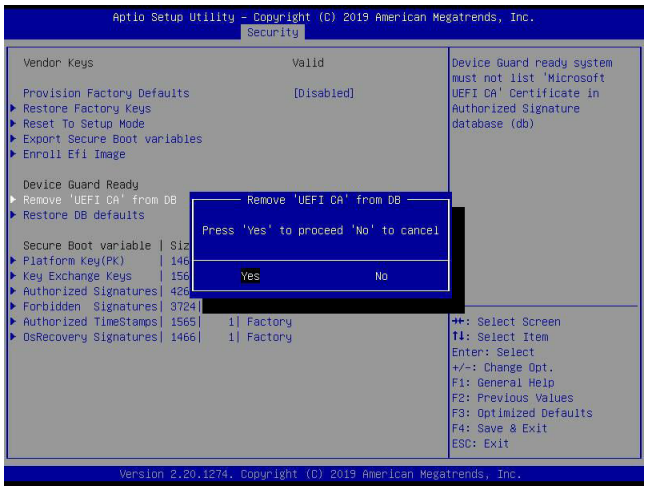
▶Enroll Efi Image

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.



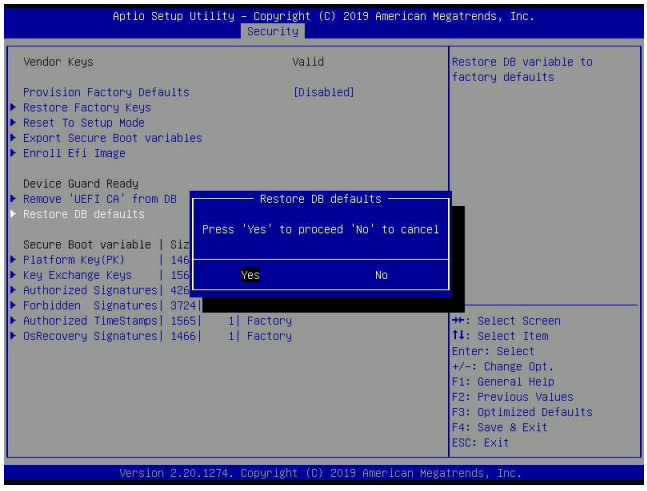
▶Remove 'UEFI CA' from DB (available when the system is not in Device Guard Ready)

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



▶Restore DB defaults

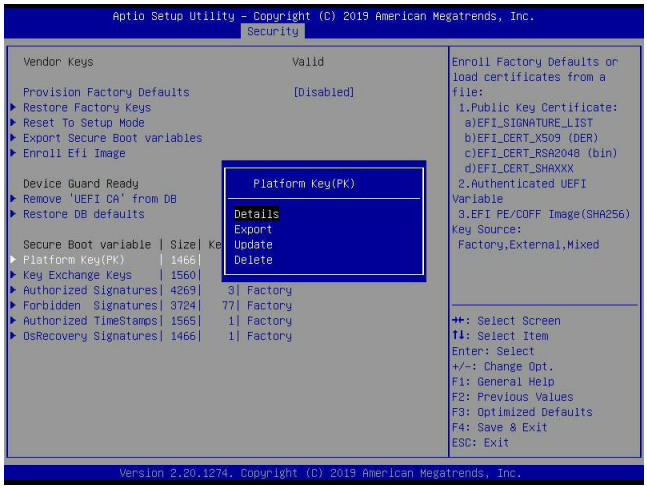
Select and press Yes to restore the DB variables to factory defaults. The options are **Yes** and No.



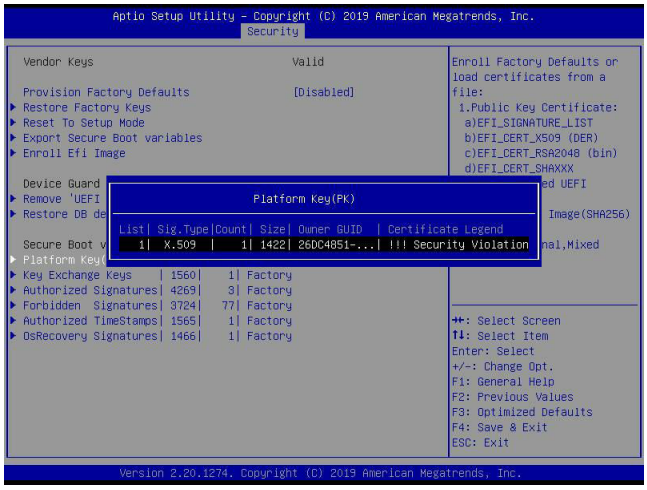
Refer to the following settings for keys and signatures related to secure boot.

▶Platform Key (PK)

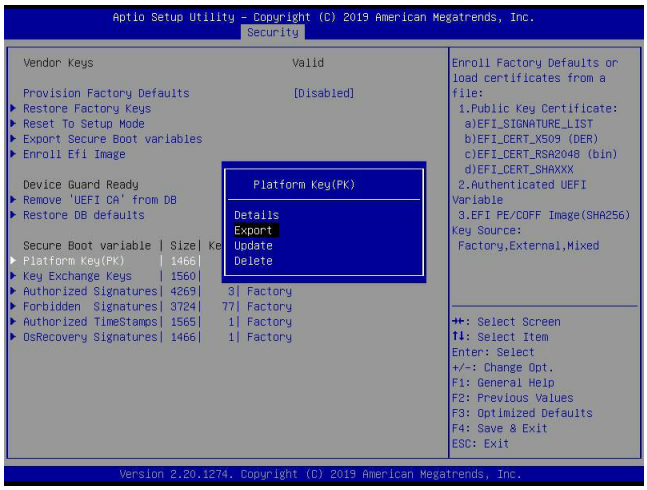
The Platform Key (PK), which is preinstalled in firmware during manufacturing, provides full control of the secure boot key hierarchy. The options are **Details**, Export, Update, and Delete. Select Details to display detailed information of PK. Select Export to save the current PKs to a FAT formatted 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.



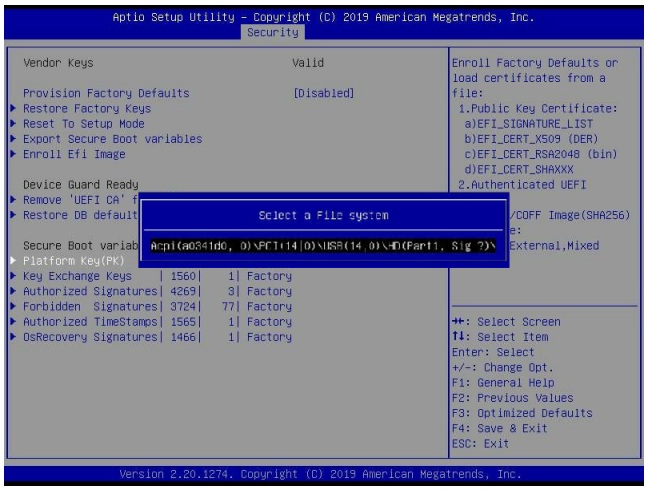
Details: Use the arrow keys to select Details and press <Enter>. It displays detailed information of PK as shown below.



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

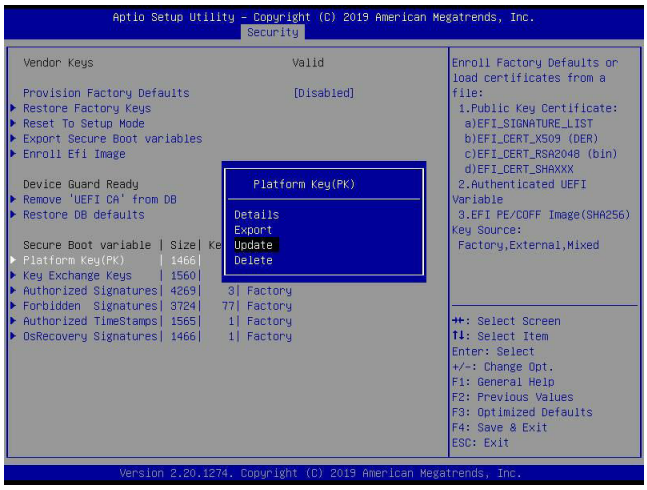


Press <Enter> and the following screen will appear.

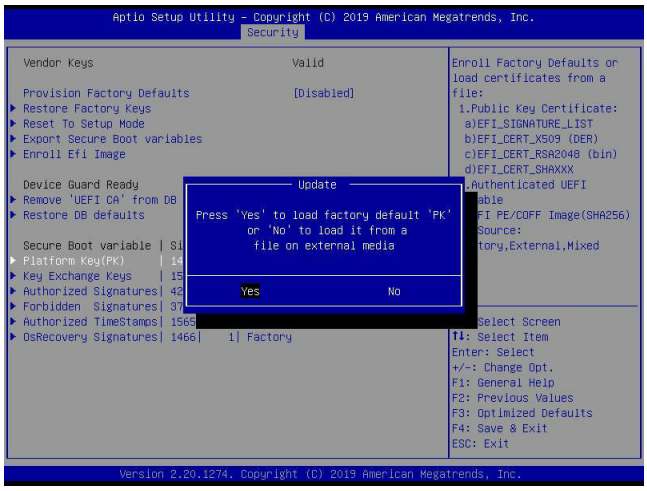


Note: Refer to the right panel of the screen for the file formats accepted.

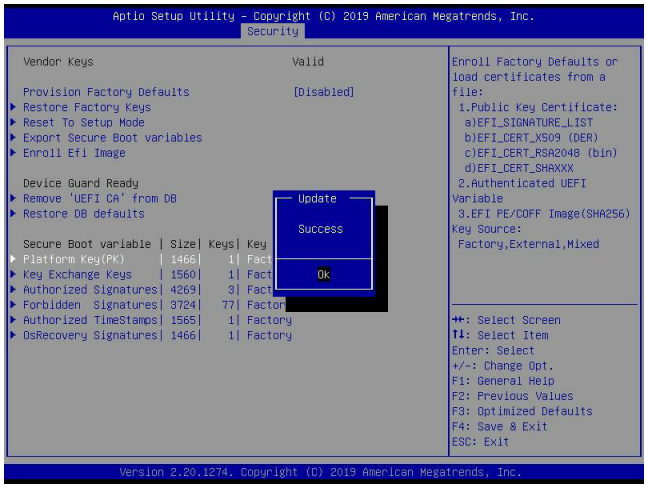
Update: Use the arrow keys to select Update. It is to load the factory defaults or load PKs from a file on the external device.



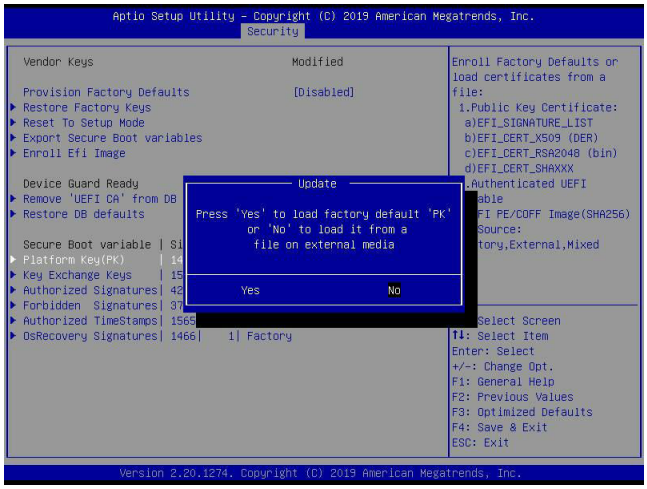
Press <Enter> and the following screen will appear.



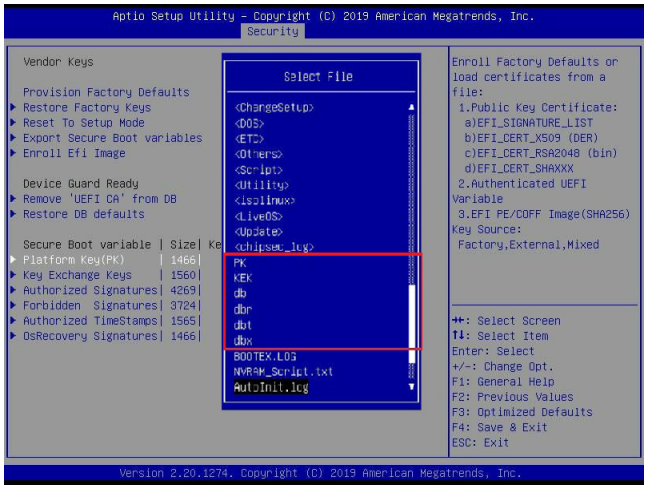
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.

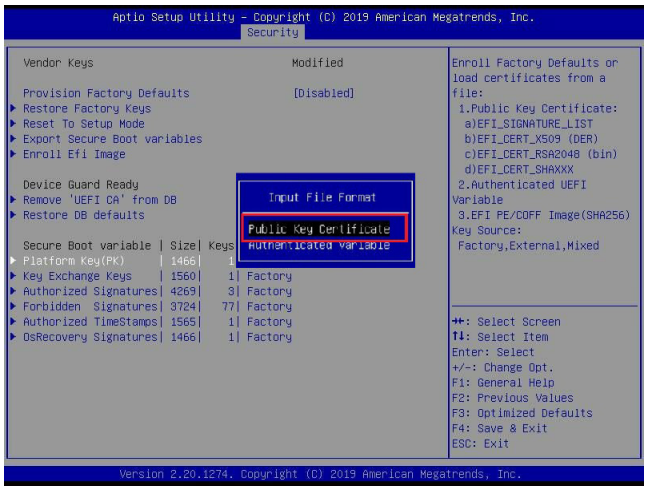


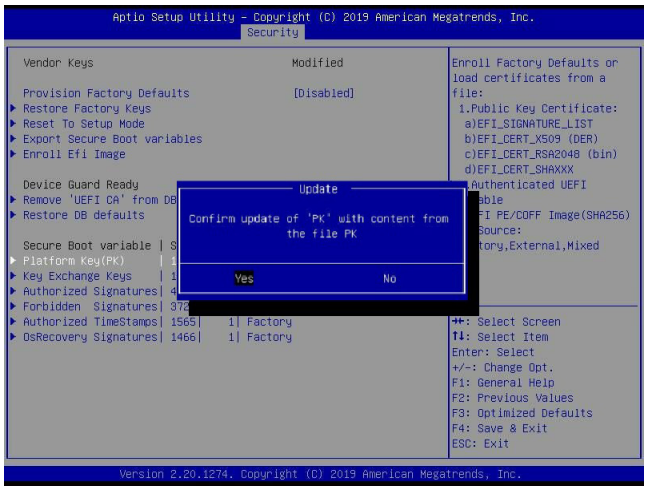
To load PKs from a file on the external device, navigate to No and press <Enter>.



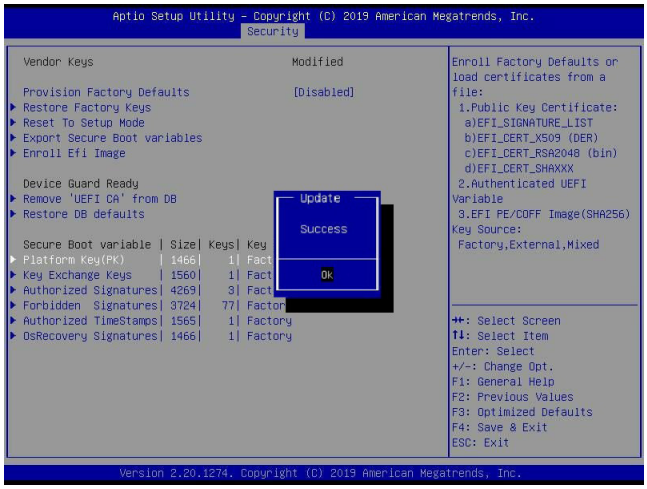
When the following screen appears, select the USB flash drive that contains the desired file.



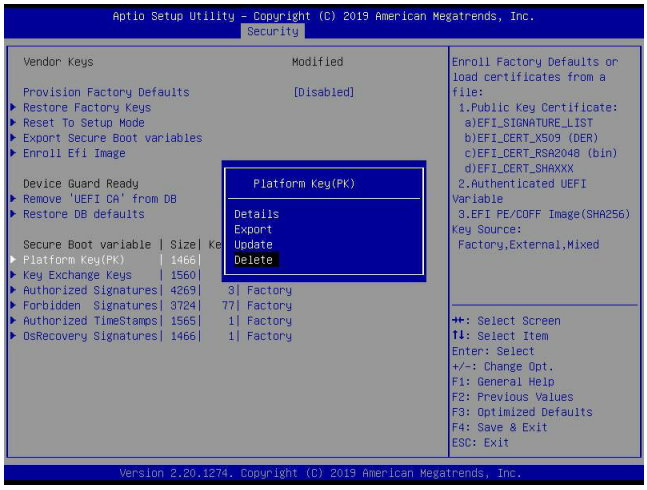


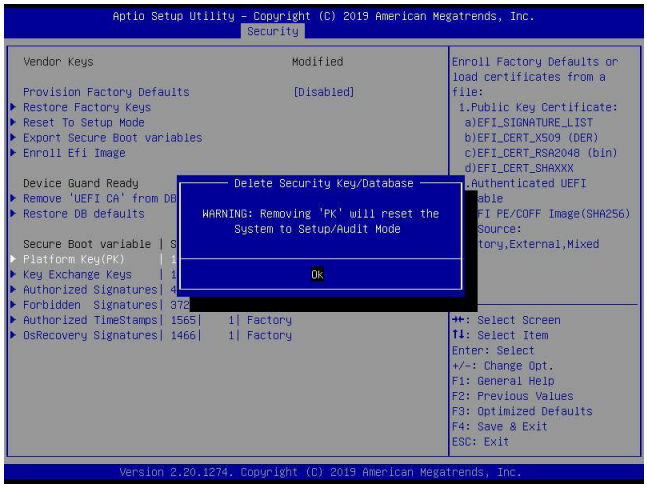


Press <Enter> and the following screen will appear.



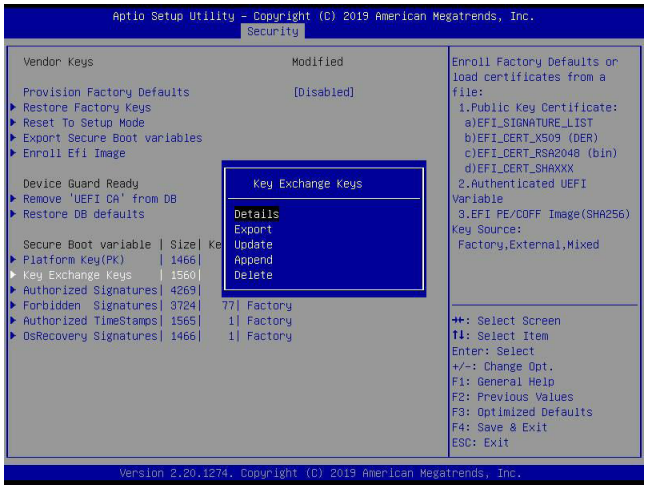
Delete: Use the arrow keys to select Delete and press <Enter> to clear the current PKs and reset the system to the Setup mode.



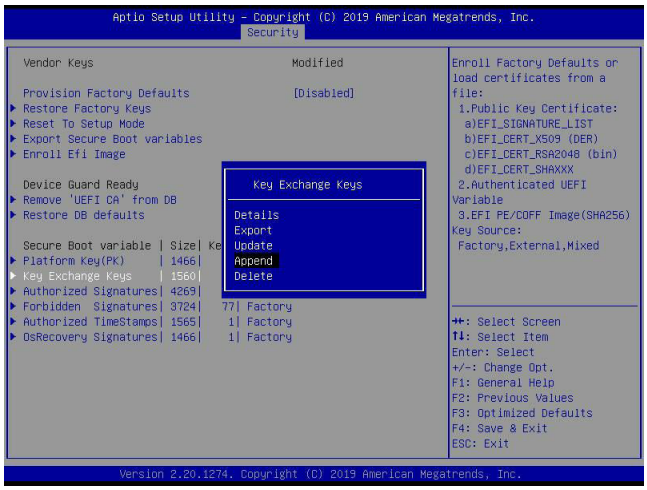


▶Key Exchange Key

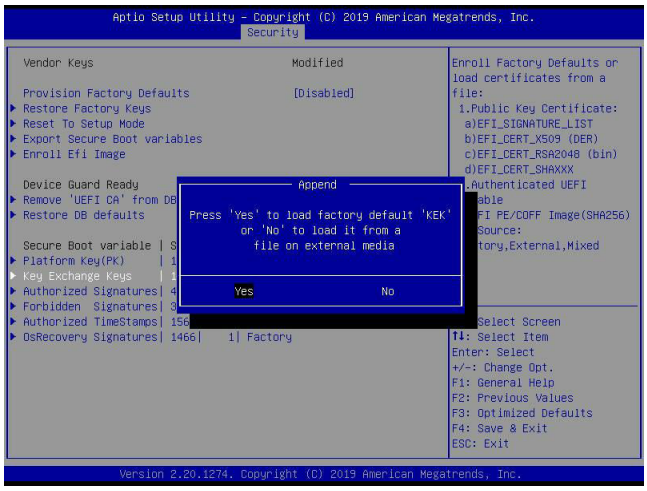
The Key Exchange Key (KEK), which is held by the operating system vendor, can be updated by the holder of the PK and be used by secure boot to protect access to signatures databases. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of KEKs. 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 198 for the Export process. Refer to pages 199, 200, 201, and 202 for the Update process.)



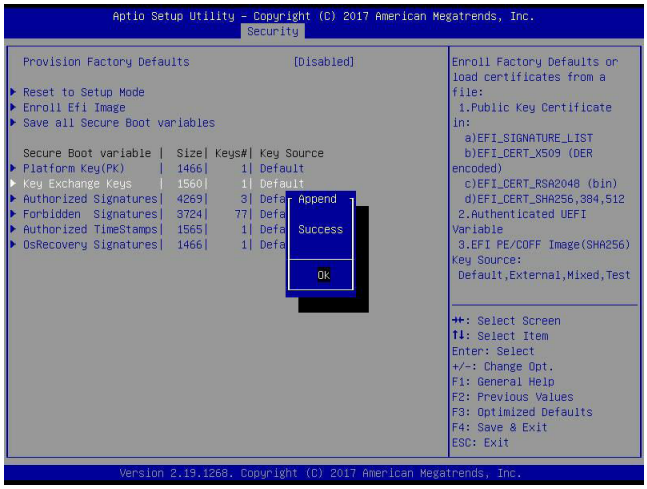
Append: Use the arrow keys to select Append.



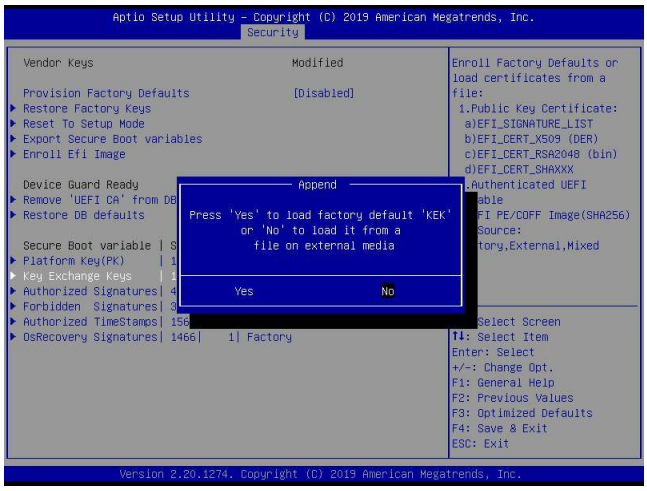
Press <Enter> and the following screen will appear.



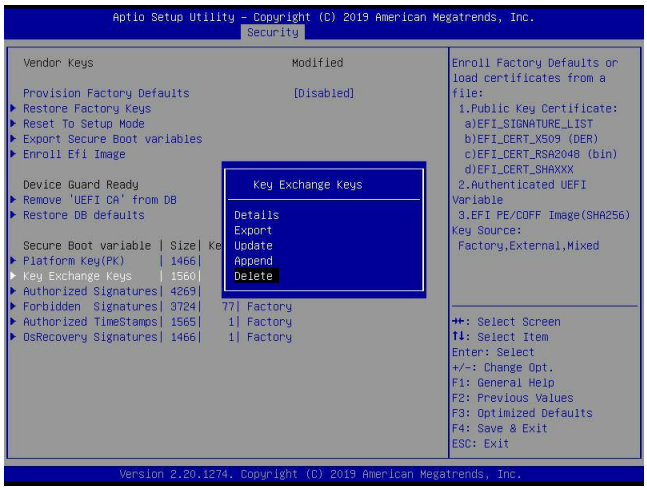
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.

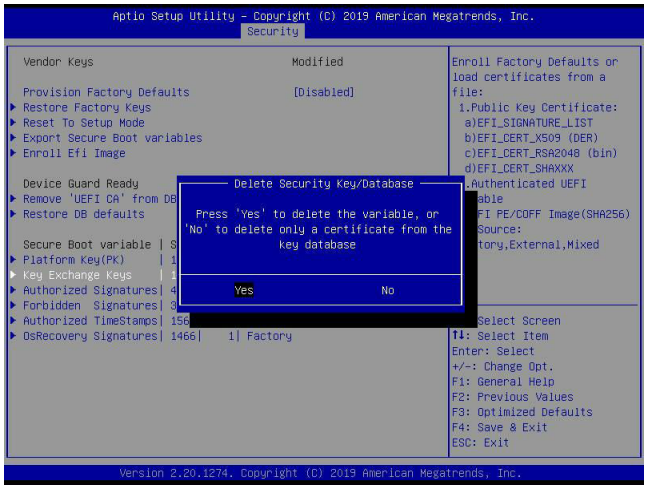


To load KEKs from a file on the external device, navigate to No and press <Enter>. Refer to pages 201 and 202 on how to load KEKs from a file on the external device.

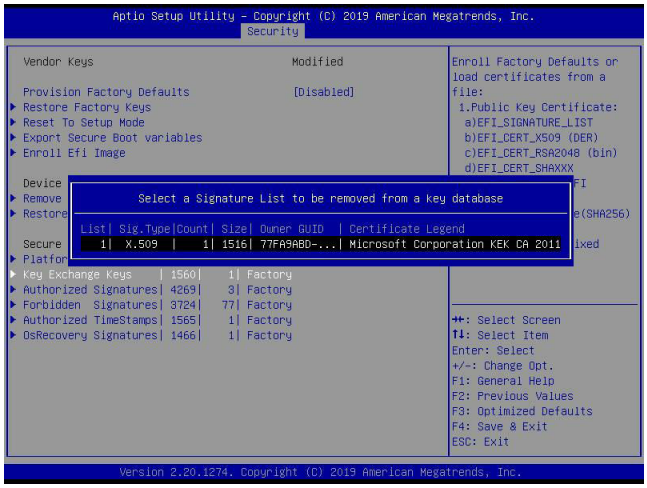


Delete: Use the arrow keys to select Delete and press <Enter>. Navigate to Yes and press <Enter> to clear the current KEKs.



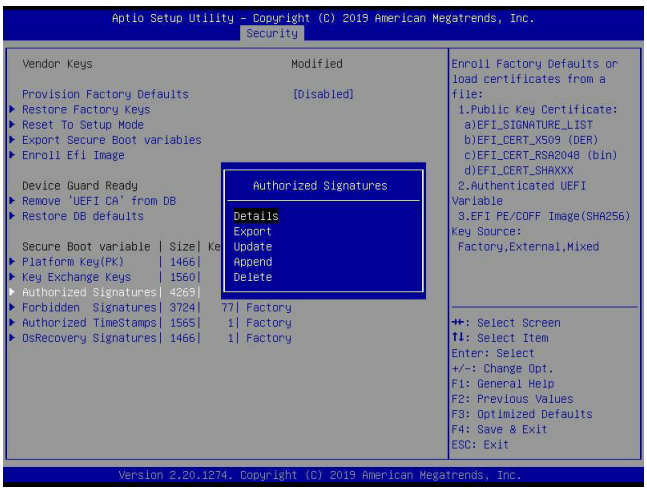


Navigate to No and press <Enter> to delete only one certificate from the key database.



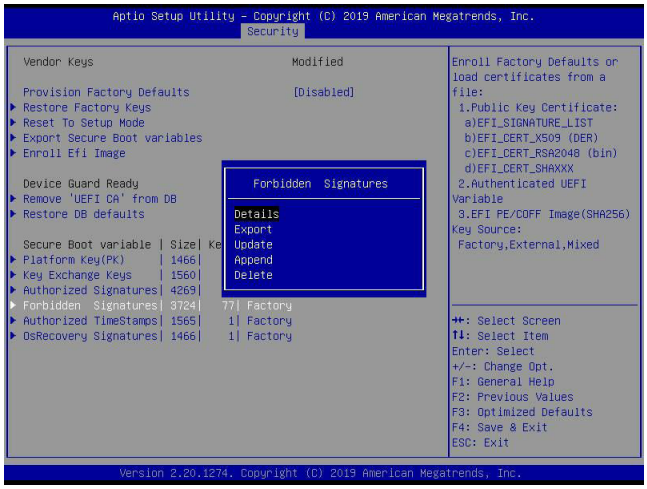
▶Authorized Signatures

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 198 for the Export process. Refer to pages 199, 200, 201, and 202 for the Update process. Refer to pages 203 and 204 for the Append process. Refer to page 205 for the Delete process.)



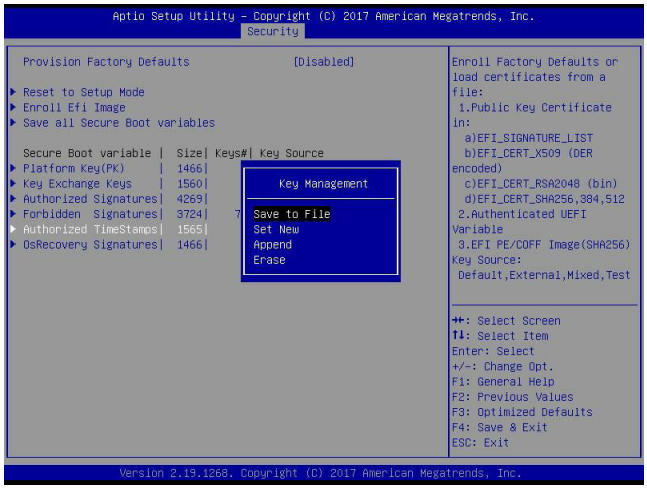
▶Forbidden Signatures

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 198 for the Export process. Refer to pages 199, 200, 201, and 202 for the Update process. Refer to pages 203 and 204 for the Append process. Refer to page 205 for the Delete process.)



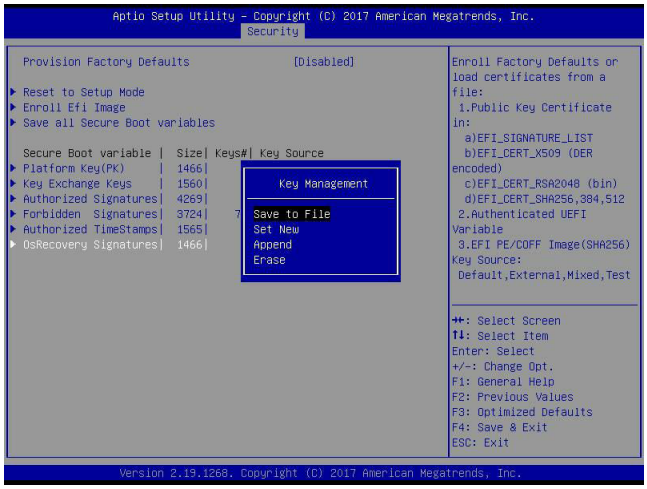
▶Authorized TimeStamps

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 198 for the Export process. Refer to pages 199, 200, 201, and 202 for the Update process. Refer to pages 203 and 204 for the Append process. Refer to page 205 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 198 for the Export process. Refer to pages 199, 200, 201, and 202 for the Update process. Refer to pages 203 and 204 for the Append process. Refer to page 205 for the Delete process.)



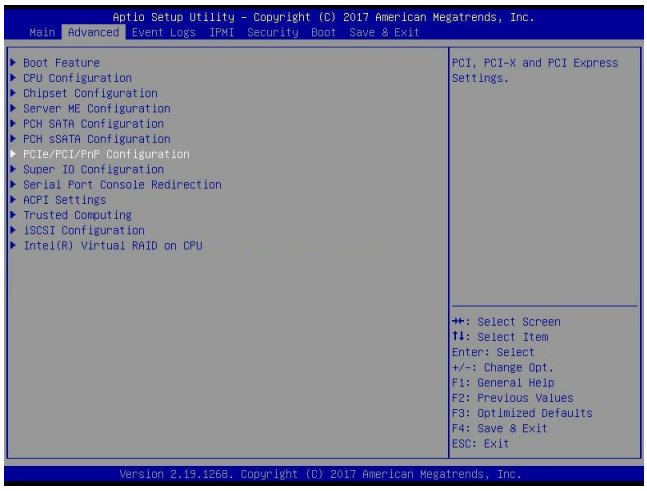
Appendix G

Configuring iSCSI Settings

Internet small computer system interface (iSCSI) is a protocol that defines how block-level data transports between the iSCSI initiator and iSCSI target over an Internet protocol (IP) network. The iSCSI initiator (client/host) enables a connection to the iSCSI target and initiates I/O requests. The iSCSI target can be a group of storage devices or an intermediate device attached to storage devices. The iSCSI initiator and iSCSI target must connect to an IP network. To have iSCSI settings available, refer to instructions stated in the G.1 section. The G.2 section explains iSCSI settings.

G.1 PCIe/PCI/PnP Features

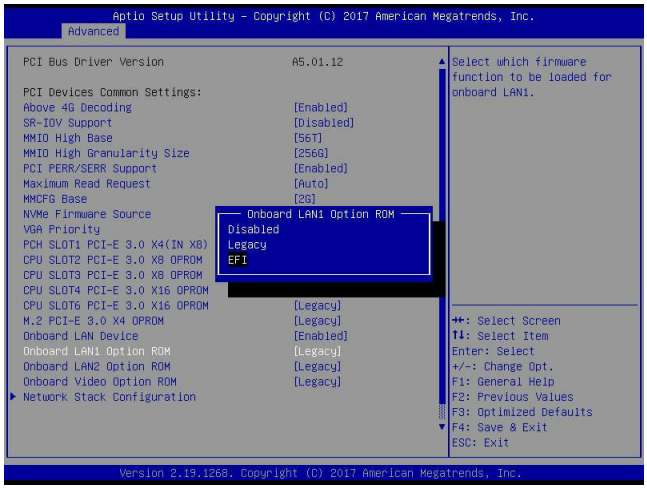
Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Advanced tab. Use the arrow keys to select PCIe/PCI/PnP Configuration and press <Enter> to access the menu items.



Note: Be sure to have configuration information for the iSCSI initiator and iSCSI target before starting iSCSI settings.

Onboard LAN1 Option ROM

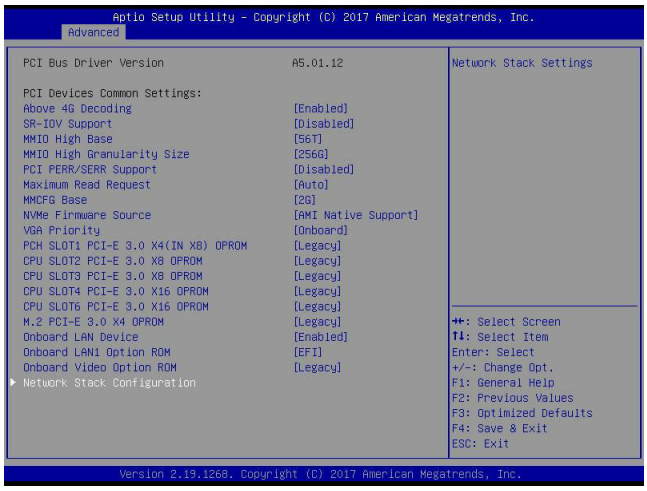
Use the arrow keys to select Onboard LAN1 Option ROM and press <Enter>. The options are Disabled, **Legacy**, and EFI. Set this feature to EFI.



Note: If Onboard LAN1 Option ROM is set to EFI, all features for onboard LAN option ROM will be set to EFI by the EFI driver. Additionally, these features will become unavailable except Onboard LAN1 Option ROM.

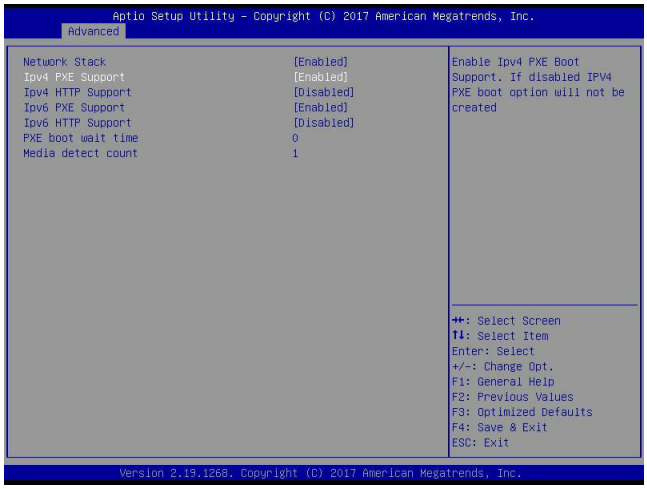
Network Stack Configuration

Use the arrow keys to select Network Stack Configuration and press <Enter> to access the menu items.



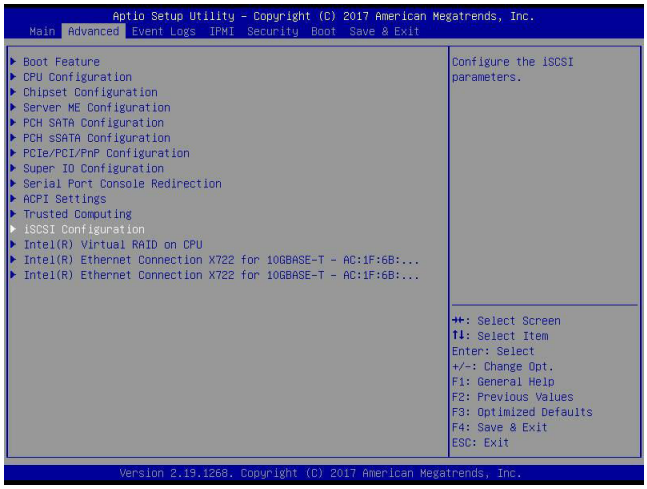
Ipv4 PXE Support/Ipv6 PXE Support

To enable Ipv4/Ipv6 PXE boot support, use the arrow keys to select and set Ipv4 PXE Support/ Ipv6 PXE Support to Enabled.



Note: Enable both Ipv4 PXE Support and Ipv6 PXE Support to have iSCSI settings available. In some cases, enabling either one feature may also have iSCSI settings available depending on the configuration of iSCSI initiator and iSCSI target.

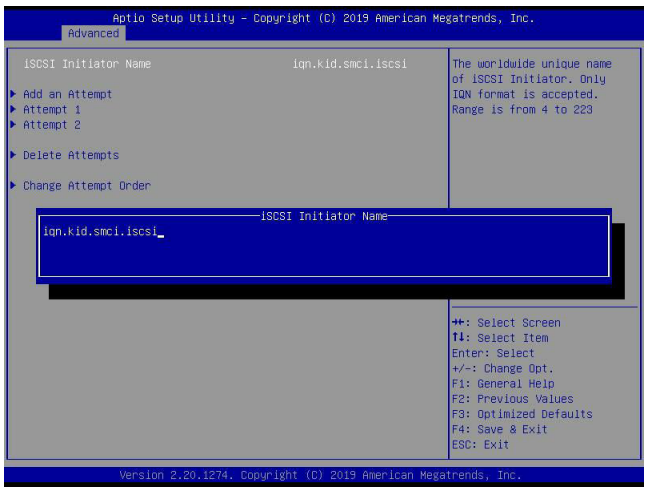
For the changes to take effect, save settings and restart the system. Press <Del> during system boot to enter the BIOS Setup utility. When the BIOS main screen appears, navigate to the Advanced tab. Use the arrow keys to select iSCSI Configuration and press <Enter> to access the menu items.



G.2 Configuring iSCSI Settings

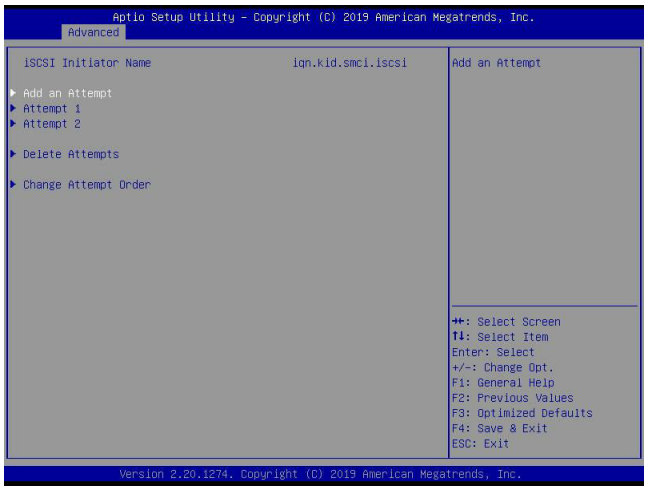
iSCSI Initiator Name

Use this feature to enter the unique initiator name in iSCSI qualified name (IQN) format.

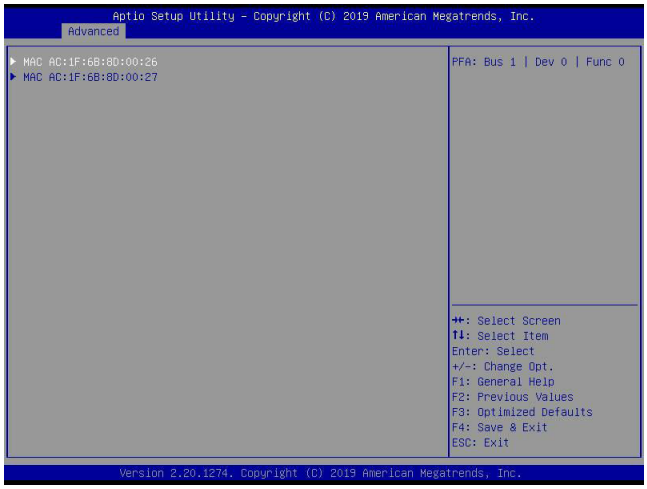


Add an Attempt

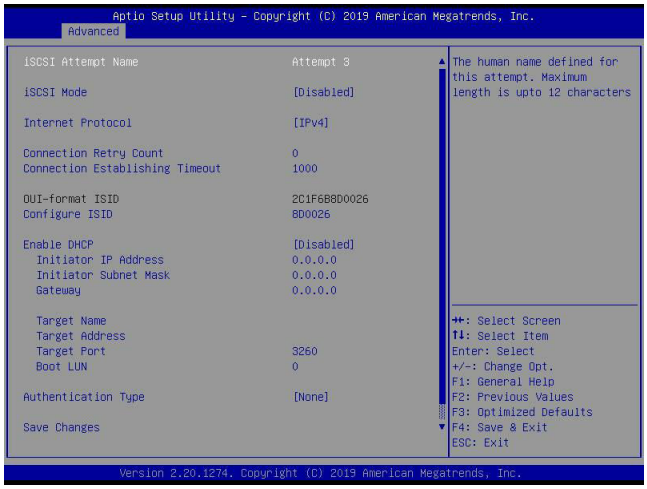
Use the arrow keys to select Add an Attempt.



Press <Enter> and the following screen will appear. Use the arrow keys to select the desired media access control address (MAC address), network interface card (NIC) port.

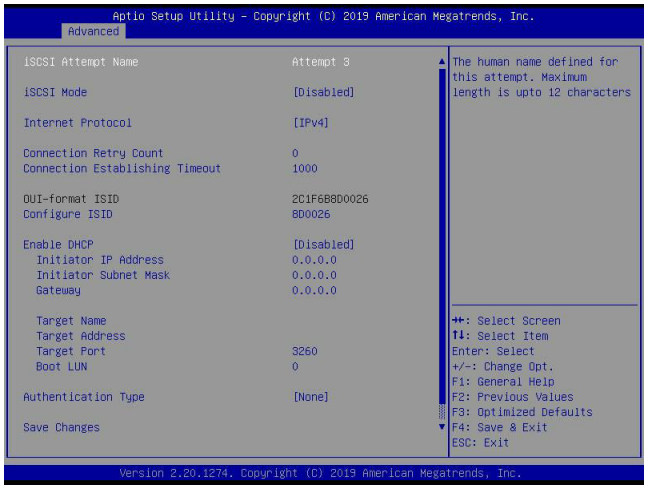


Press <Enter> and the following screen will appear.



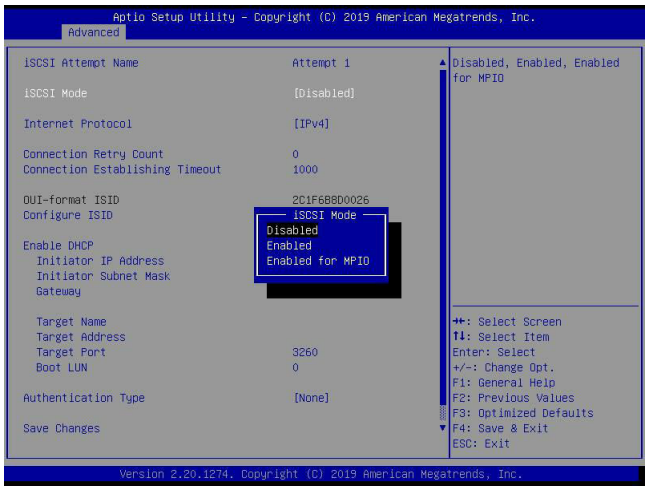
iSCSI Attempt Name

This feature displays the iSCSI attempt name.



iSCSI Mode

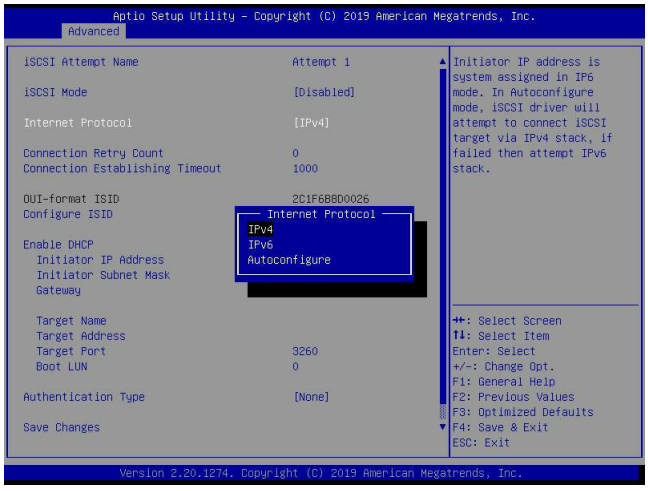
Use this feature to set the iSCSI mode. The options are **Disabled**, Enabled, and Enabled for MPIO. Multipath I/O (MPIO) is a feature that allows the system to route I/O through the available paths if the active path fails (be sure to have more than one physical path connected to the system).



Note: Enabling the feature, iSCSI Mode, is required for iSCSI configuration.

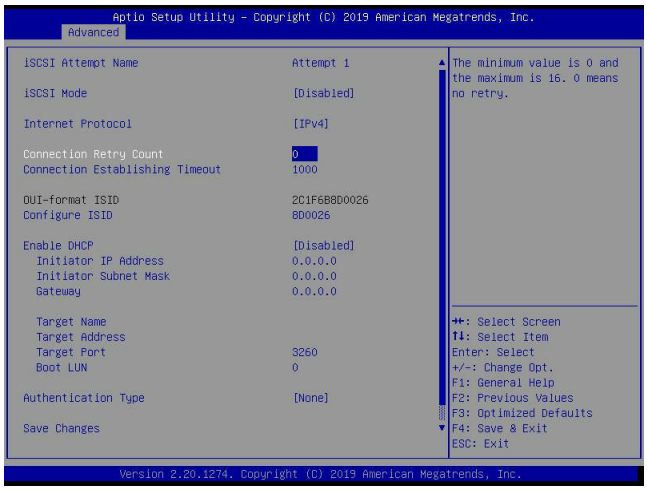
Internet Protocol

Use this feature to set the Internet protocol. The options are **IPv4**, IPv6, and Autoconfigure.



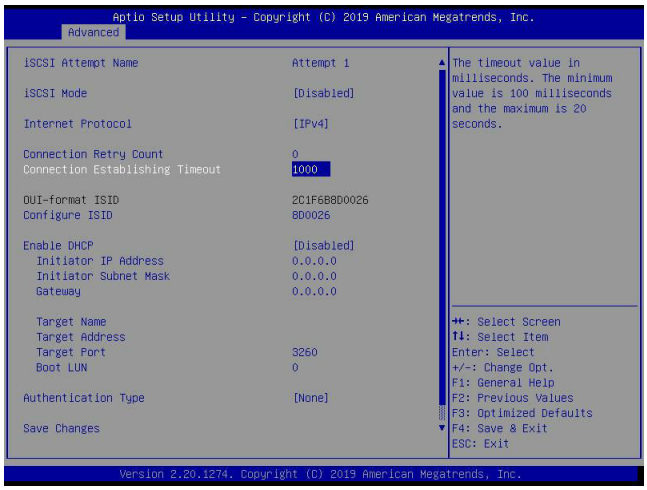
Connection Retry Count

The valid range is 0~16. Use this feature to enter the number of logon sessions allowed for the iSCSI initiator to restart with the iSCSI target if the first logon connection fails.



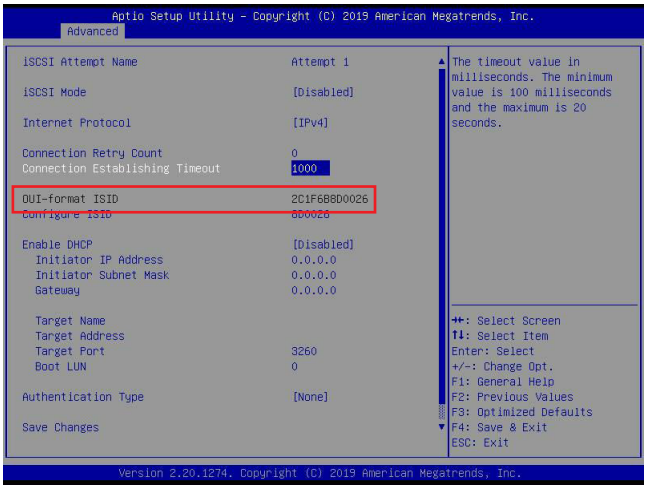
Connection Establishing Timeout

Use this feature to set the logon connection establishing timeout (in milliseconds). The valid range is from 100 milliseconds to 20 seconds.



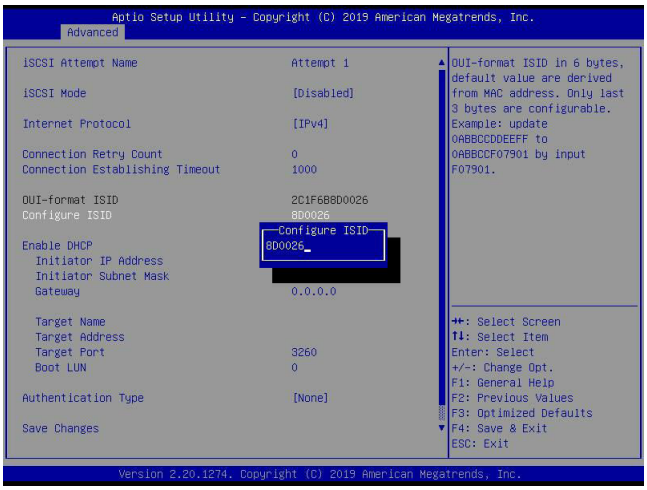
OUI-format ISID

This feature displays the default ISID in OUI format. The value (in six bytes) is derived from the MAC address of the NIC port that you selected earlier.



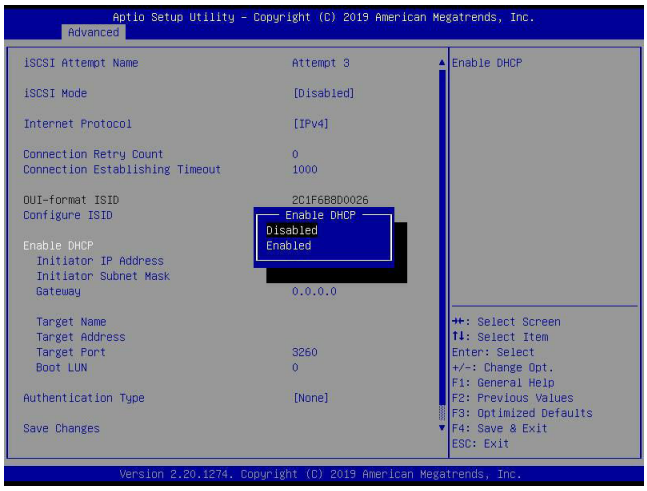
Configure ISID

Press <Enter> to configure the ISID. The default value is derived from the last three bytes of the OUI-format ISID. Also, only the last three bytes of the ISID are configurable.



Enable DHCP

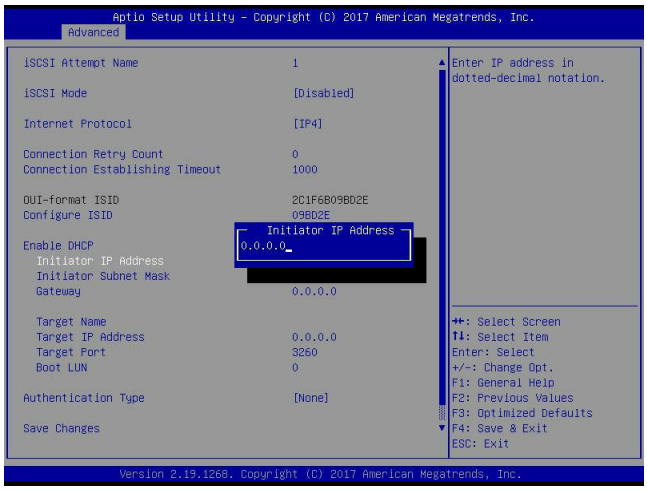
Use this feature to disable/enable dynamic host configuration protocol (DHCP) server service for the iSCSI initiator. The options are **Disabled** and Enabled.



Note: Set the feature, Enable DHCP, to Disabled if you would like to specify the iSCSI initiator IP address/subnet mask/gateway.

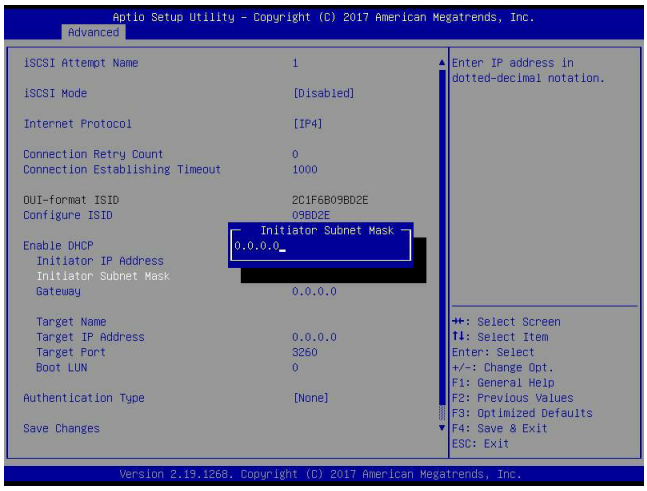
Initiator IP Address (available when Enable DHCP is set to Disabled)

Use this feature to enter the desired iSCSI initiator IP address.



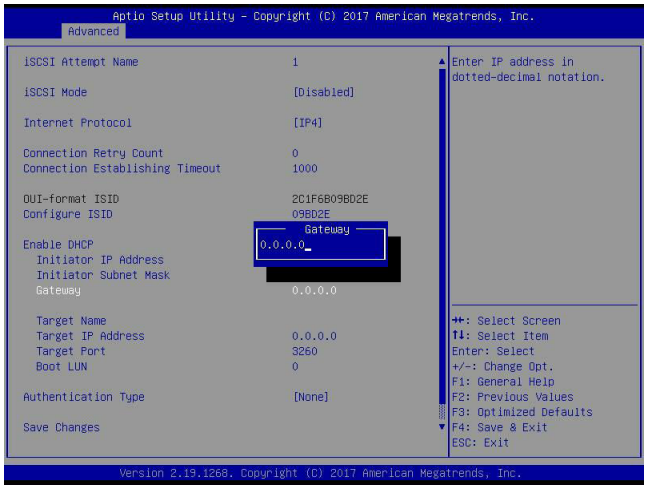
Initiator Subnet Mask (available when Enable DHCP is set to Disabled)

Use this feature to enter the desired iSCSI initiator subnet mask.



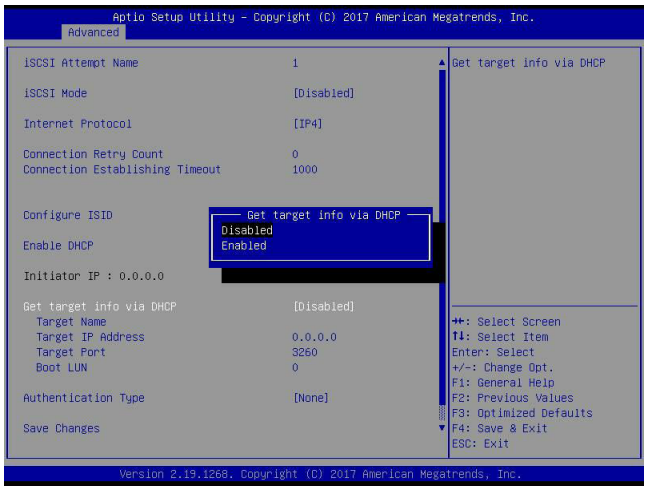
Gateway (available when Enable DHCP is set to Disabled)

Use this feature to enter the desired iSCSI initiator gateway.



Get target info via DHCP (available when Enable DHCP is set to Enabled)

Use this feature to disable/enable dynamic host configuration protocol (DHCP) server service for the iSCSI target. The options are **Disabled** and Enabled.

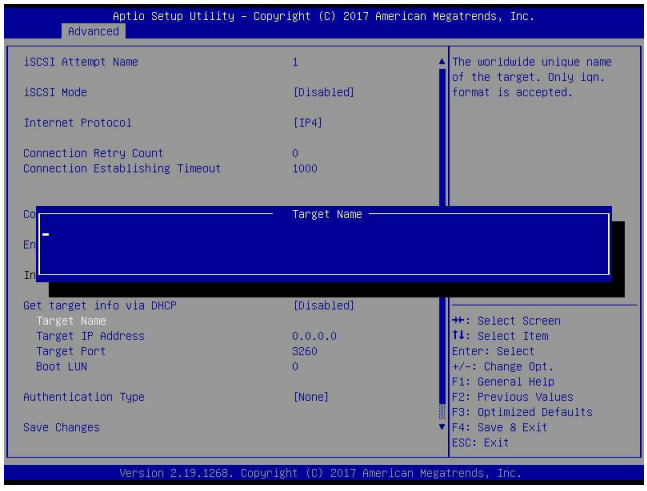


Note 1: Set the feature, Get target info via DHCP, to Disabled if you would like to specify the iSCSI target name/IP address/boot LUN.

Note 2: LUN stands for logical unit number, which is used to identify a logical/physical disk.

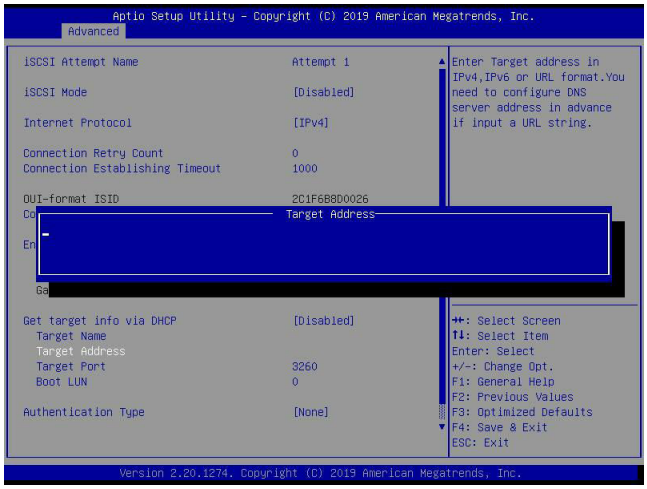
Target Name

Use this feature to enter the desired iSCSI target name in IQN format.



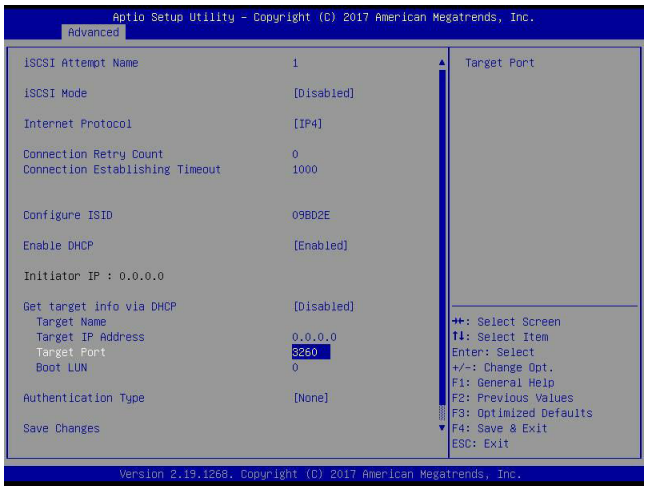
Target Address

Use this feature to enter the desired iSCSI target IP address.



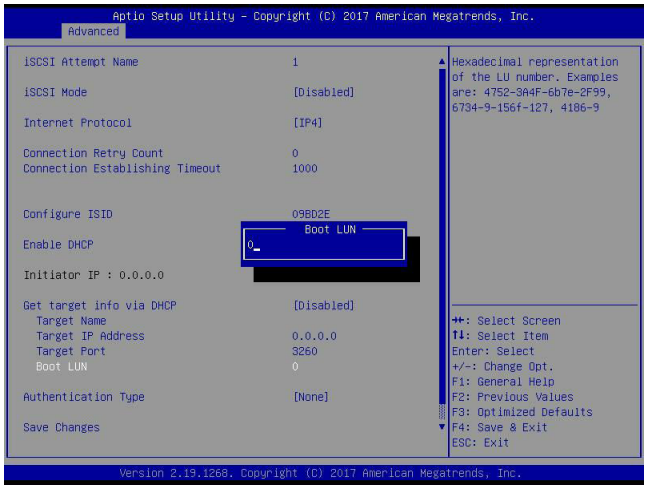
Target Port

This feature displays the iSCSI target port.



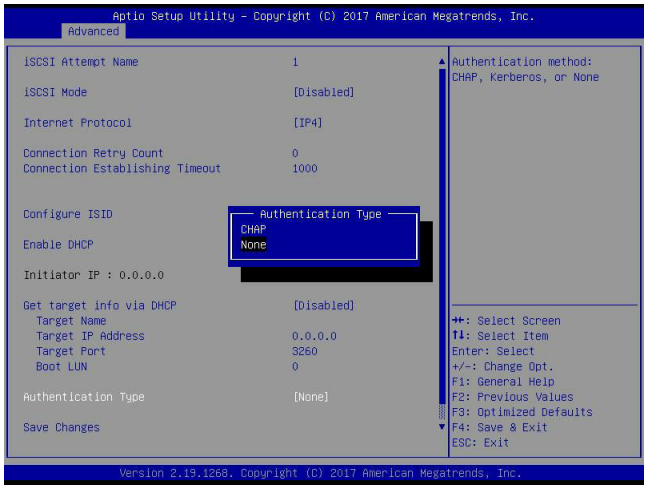
Boot LUN

Use this feature to enter the LUN ID of boot LUN.



Authentication Type

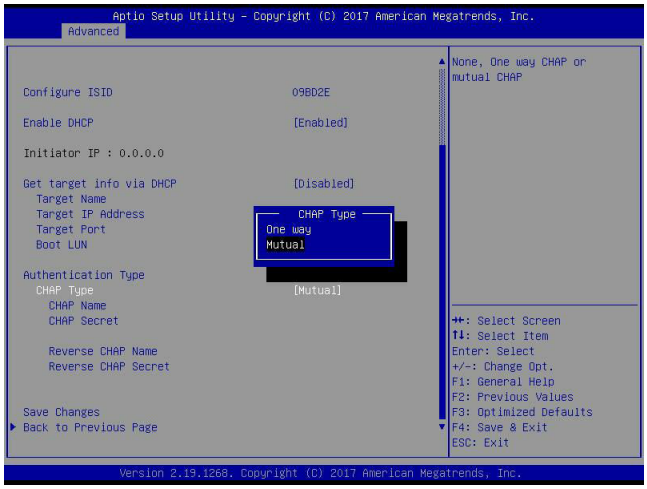
Use this feature to set the authentication method. The options are CHAP and **None**.



Note: Challenge handshake authentication protocol (CHAP) is a protocol used to verify the identity of the peer of a connection.

CHAP Type (available when Authentication Type is set to CHAP)

Use this feature to set the CHAP type. The options are One way and **Mutual**.

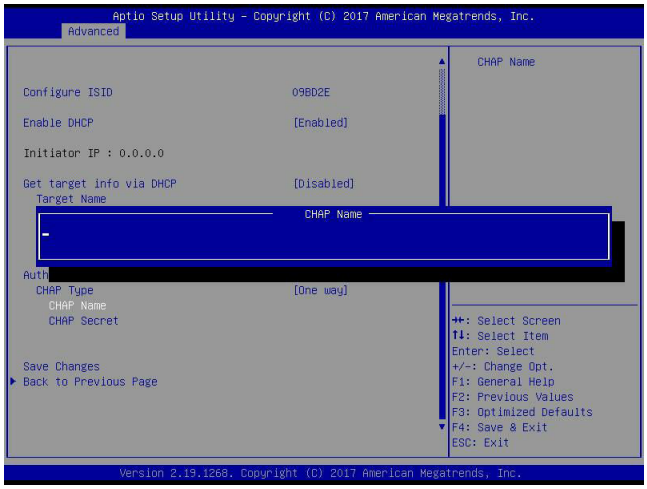


Note 1: If one way (unidirectional) CHAP authentication is performed, the iSCSI target authenticates the iSCSI initiator.

Note 2: If mutual (bidirectional) CHAP authentication is performed, the iSCSI target and iSCSI initiator authenticate each other.

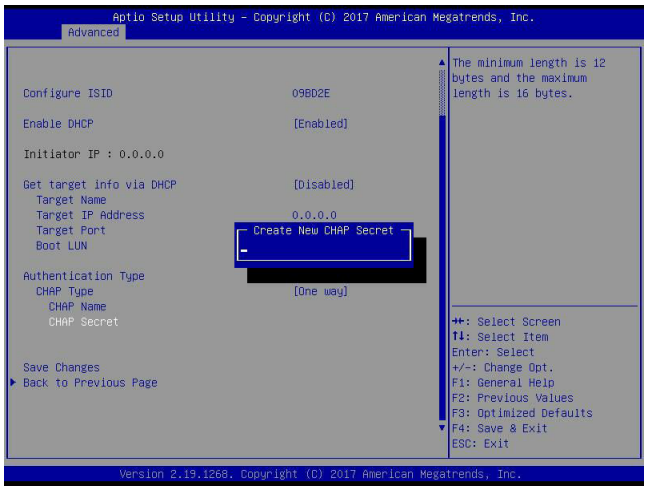
CHAP Name (available when Authentication Type is set to CHAP)

Use this feature to enter the CHAP name authenticated by the iSCSI target.



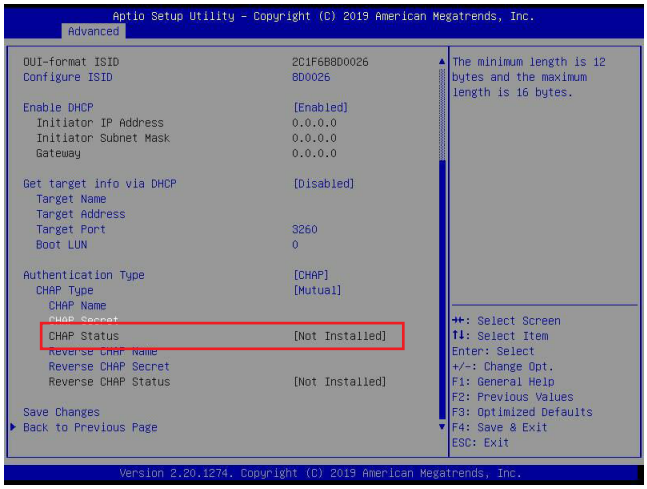
CHAP Secret (available when Authentication Type is set to CHAP)

Use this feature to enter the CHAP secret (12~16 characters) authenticated by the iSCSI target.



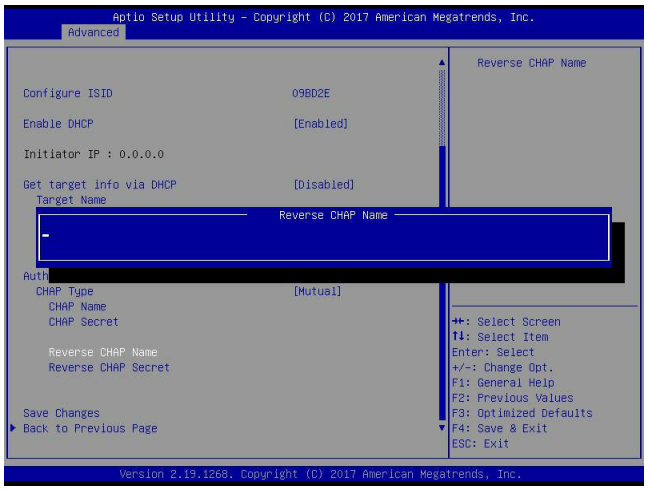
CHAP Status

This feature displays the CHAP status.



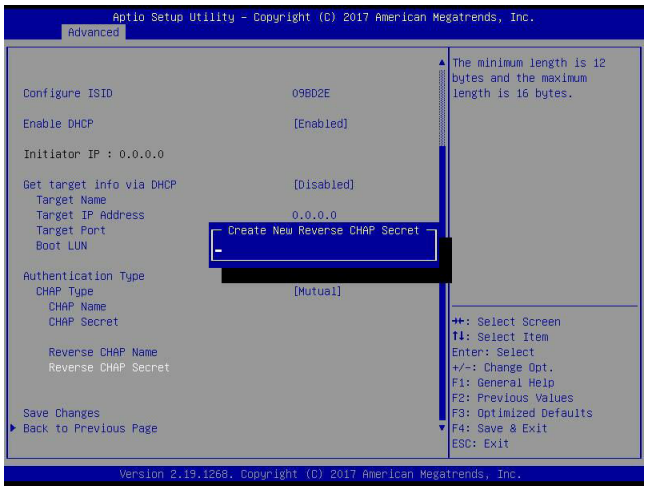
Reverse CHAP Name (available when CHAP Type is set to Mutual)

Use this feature to enter the CHAP name authenticated by the iSCSI initiator.



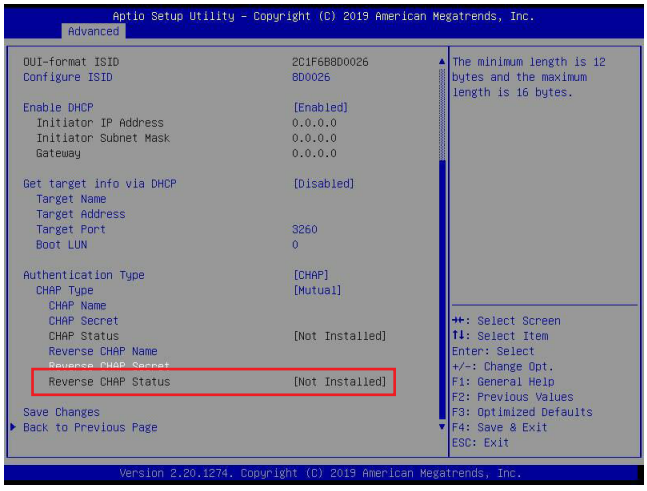
Reverse CHAP Secret (available when CHAP Type is set to Mutual)

Use this feature to enter the CHAP secret (12~16 characters) authenticated by the iSCSI initiator.



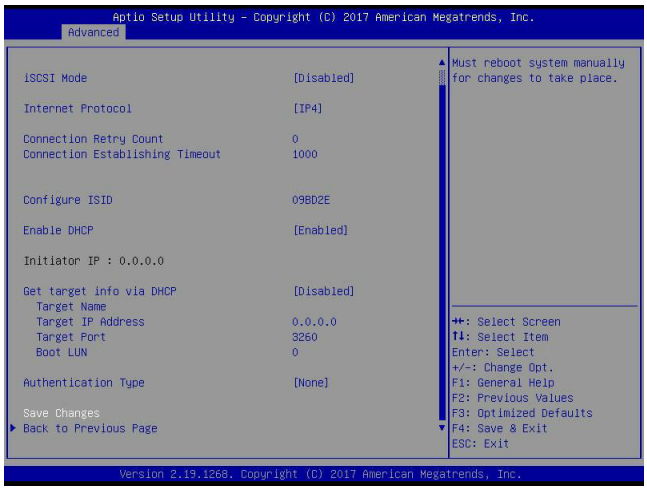
Reverse CHAP Status (available when CHAP Type is set to Mutual)

This feature displays the reverse CHAP status.



Save Changes

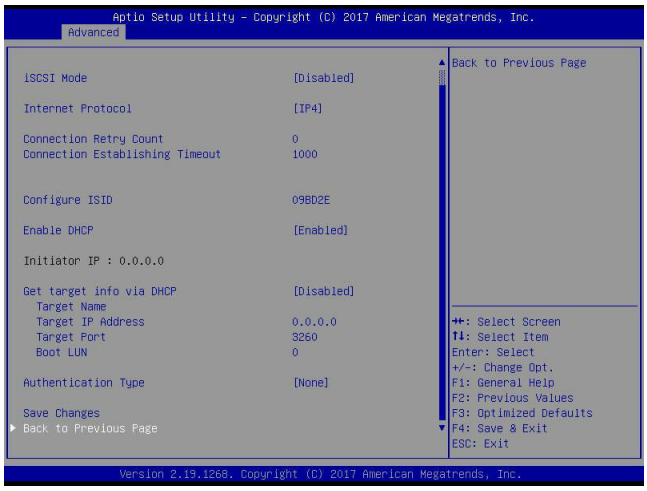
Use the arrow keys to select Save Changes and press <Enter> to save settings shown on the screen.



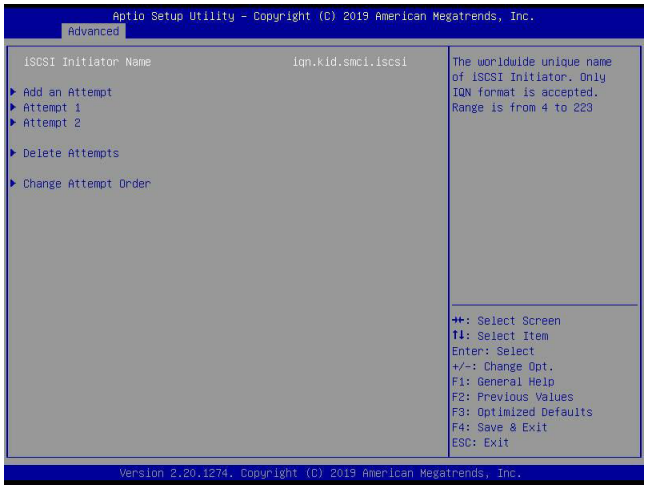
Note: For the changes to take effect, save settings and restart the system.

Back to Previous Page

Use the arrow keys to select Back to Previous Page and press <Enter>.

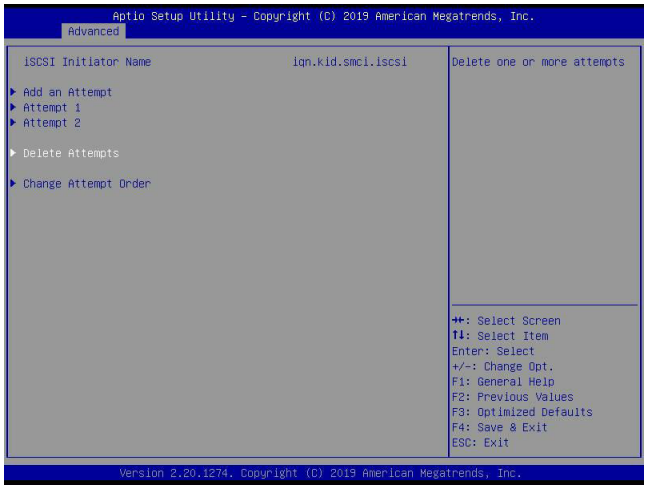


The user will be returned to the main screen of iSCSI Configuration as shown below.

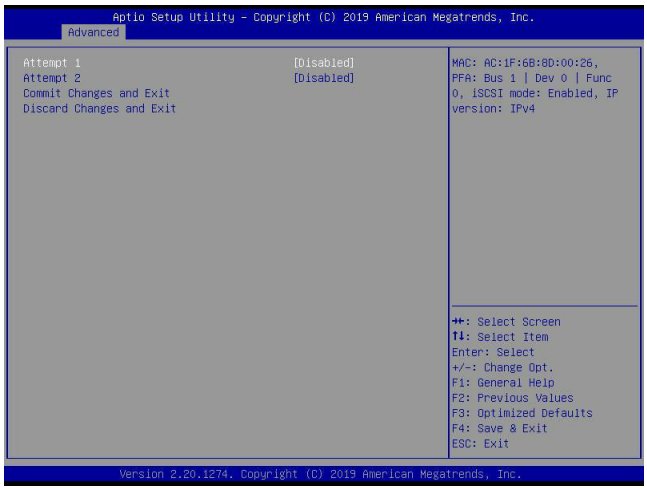


Delete Attempts

Use the arrow keys to select Delete Attempts.

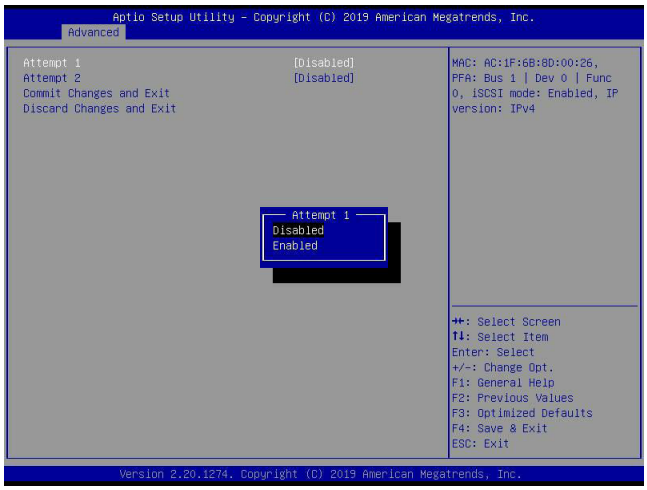


Press <Enter> and the following screen will appear.



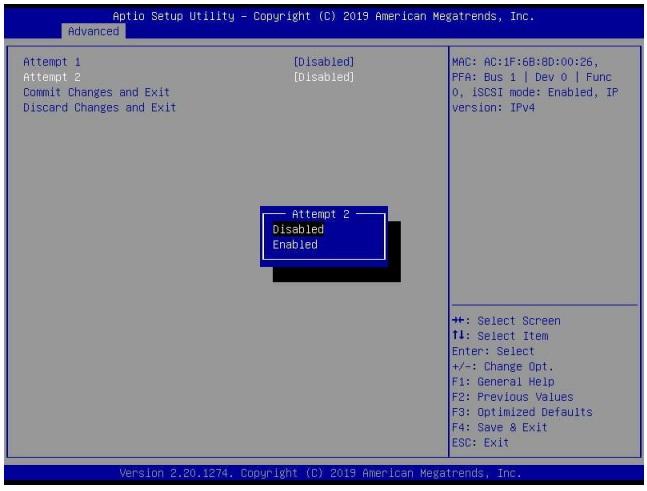
Attempt 1

Use the feature to disable/enable Attempt 1. The options are **Disabled** and Enabled.



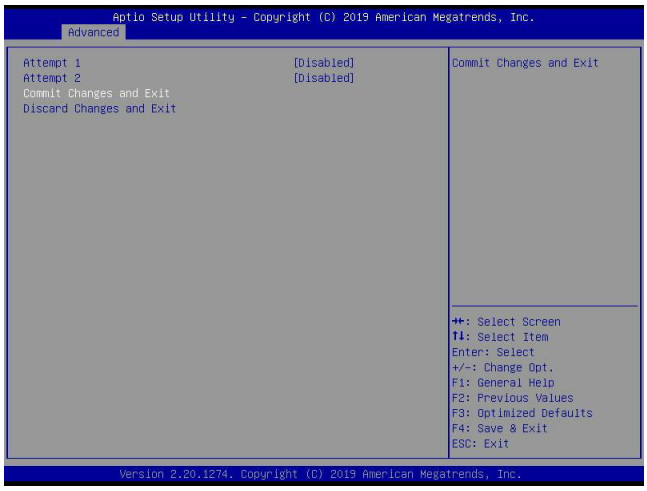
Attempt 2

Use the feature to disable/enable Attempt 2. The options are **Disabled** and Enabled.



Commit Changes and Exit

Press <Enter> to save changes and return to the main screen of iSCSI Configuration.

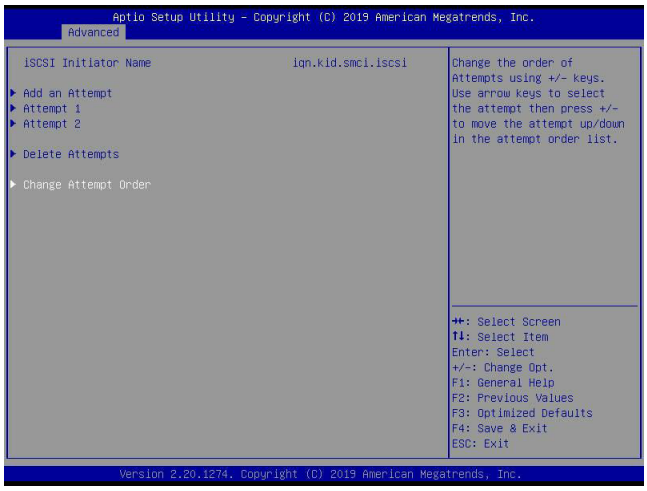


Discard Changes and Exit

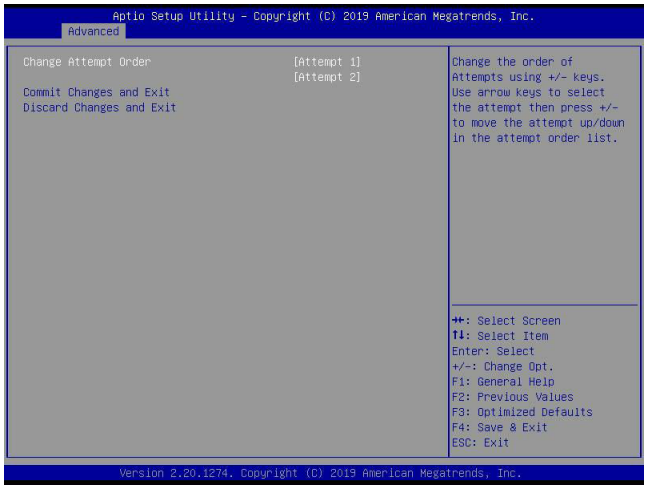
Press <Enter> to return to the main screen of iSCSI Configuration without any change.

Change Attempt Order

Use the arrow keys to select Change Attempt Order.

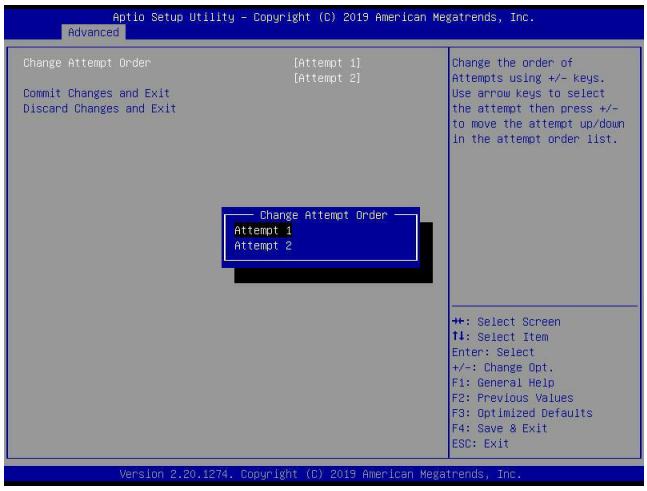


Press <Enter> and the following screen will appear.



Change Attempt Order

This feature is to change the Attempt order. Use arrow keys to select the desired Attempt, then <+/-> keys to move up/down the selected Attempt. For instance, move up the selected Attempt by using <+> key. Move down the selected Attempt by using <-> key.

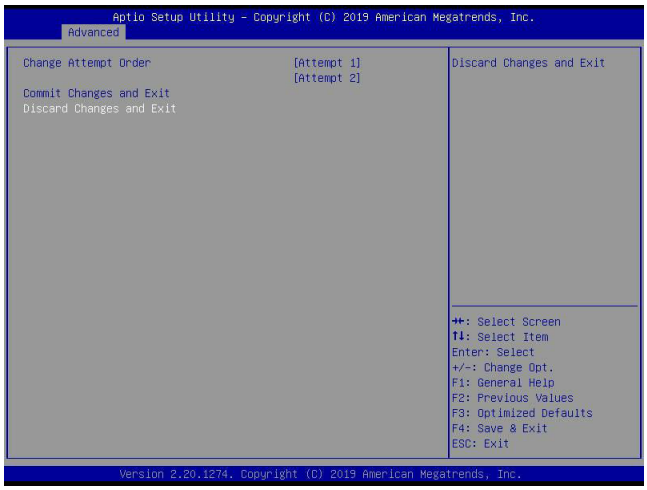


Commit Changes and Exit

Press <Enter> to save changes and return to the main screen of iSCSI Configuration.

Discard Changes and Exit

Press <Enter> to return to the main screen of iSCSI Configuration without any change.



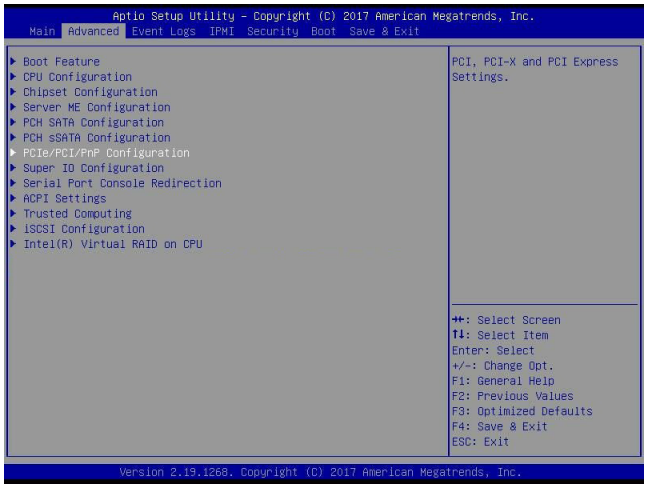
Appendix H

Configuring Network Interface Card (NIC) Settings

The appendix describes settings of onboard Intel LAN devices via the BIOS Setup utility supported by the Unified Extensible Firmware Interface (UEFI) driver.

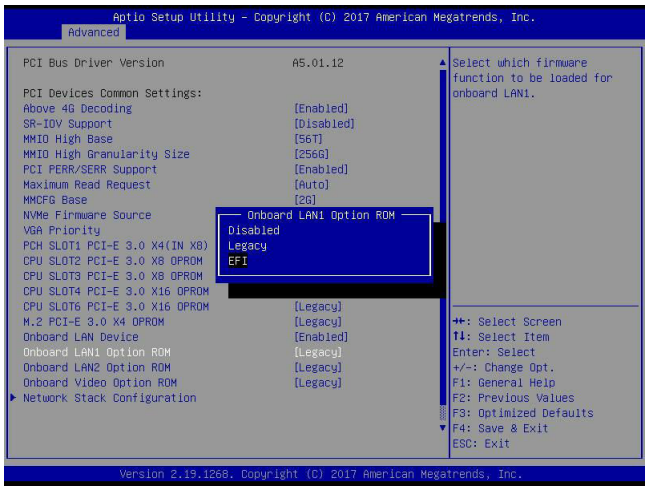
H.1 Network Interface Card (NIC) Settings

Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Advanced tab. Use the arrow keys to select PCIe/PCI/PnP Configuration and press <Enter> to access the menu items.



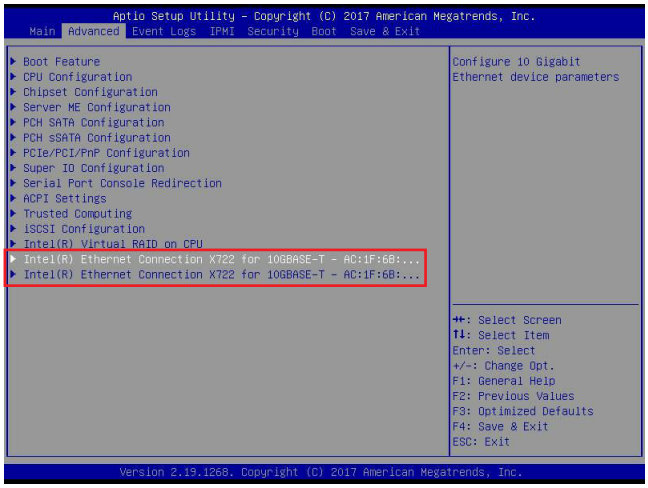
Onboard LAN1 Option ROM (available when NIC(s) is(are) detected by the system)

Use the arrow keys to select Onboard LAN1 Option ROM and press <Enter>. The options are Disabled, **Legacy**, and EFI. Set this feature to EFI.

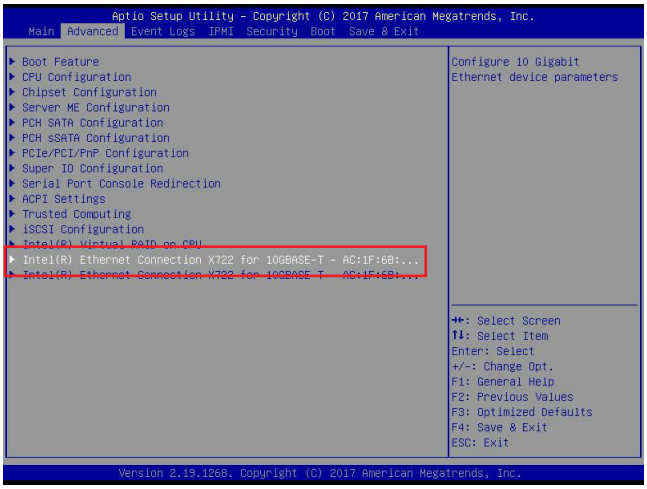


Note : If Onboard LAN1 Option ROM is set to EFI, all features for onboard LAN option ROM will be set to EFI by the EFI driver. Additionally, these features will become unavailable except Onboard LAN1 Option ROM.

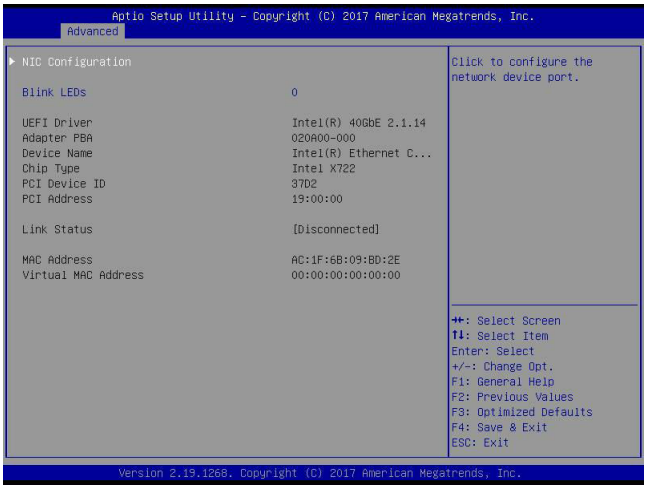
For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Advanced tab. The feature(s) for onboard Intel LAN device(s) will become available for configuration as shown below.



Use the arrow keys to select the desired onboard LAN device as shown below.

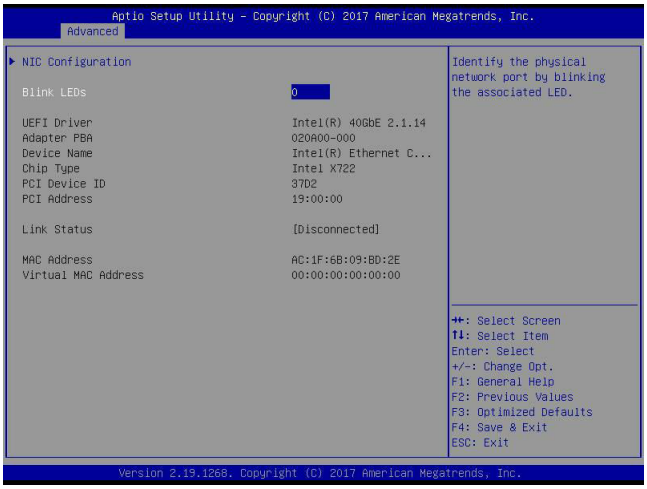


Press <Enter> and the following screen will appear. It displays the detailed information for the selected onboard LAN device.



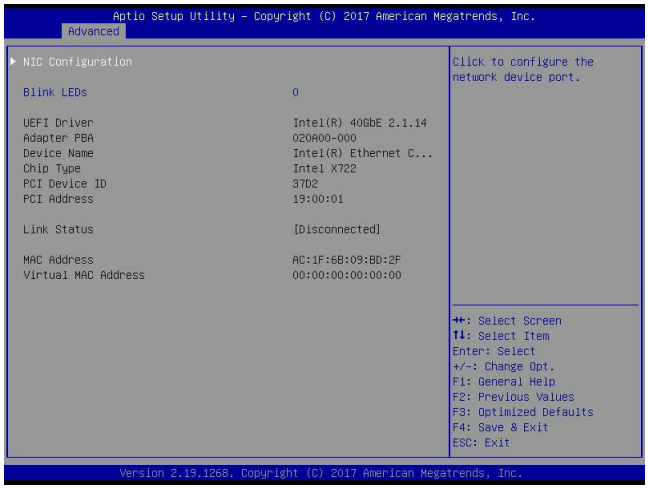
Blink LEDs

This feature allows the user to set the LED blink duration (in seconds). The valid range is 0~15 (seconds).

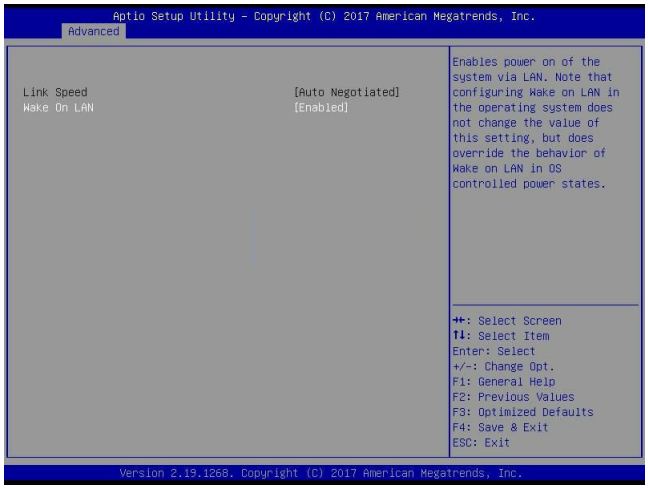


NIC Configuration

Use the arrow keys to select NIC Configuration.



Press <Enter> and the following screen will appear.



Wake on LAN

Use the arrow keys to select Wake On LAN and press <Enter>. The following screen will appear. The options are **Disabled** and Enabled. Set this feature to support system wake-up via the selected LAN device.