



X11DPT-L

USER'S MANUAL

Revision 1.0a

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

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

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

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

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

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



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

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

Manual Revision 1.0a

Release Date: April 11, 2019

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document. Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2019 by Super Micro Computer, Inc.

All rights reserved.

Printed in the United States of America

Preface

About This Manual

This manual is written for system integrators, IT technicians, and knowledgeable end users. It provides information for the installation and use of the X11DPT-L motherboard.

About This Motherboard

The X11DPT-L motherboard supports dual Intel® Xeon® Scalable-SP series and 2nd Gen Intel Xeon Scalable-SP series processors in Socket P type with a TDP (Thermal Design Power) of up to 140W and two UPI (Ultra Path Interconnect) links of up to 10.4 GT/s. With the Intel C621 PCH built-in, this motherboard supports one PCI-E 3.0 x16 slot, one PCI-E 3.0 x4 proprietary slot for M.2, six SATA 3.0 connections, two SuperDOM ports, and 3DS LRDIMM/3DS RDIMM, NVDIMM DDR4 ECC of up to 2933*/2666 MHz memory in eight memory slots. The X11DPT-L provides maximum performance, system cooling, and PCI-E capacity currently available on the market. This motherboard is ideal for high-end, high-performance enterprise storage, database storage, and virtualization server platforms. Please note that this motherboard is intended to be installed and serviced by professional technicians only. For processor/memory updates, please refer to our website at <http://www.supermicro.com/products/>.



Notes: **1.** UPI/memory speeds are dependent on the processors installed in your system. **2.** 2933 MHz memory is supported by 2nd Gen Intel Xeon Scalable-SP (82xx/62xx series) processors only.

Manual Organization

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

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

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

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

Appendix A provides BIOS Error Beep Codes.

Appendix B lists software program installation instructions.

Appendix C lists standardized warning statements in various languages.

Appendix D provides UEFI BIOS Recovery instructions.

Appendix E explains Intel® VROC RAID settings.

Appendix F describes secure boot settings.

Appendix G provides Network Interface Card (NIC) settings.

Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)

Website: www.supermicro.com

Europe

Address: Super Micro Computer B.V.
Het Sterrenbeeld 28, 5215 ML
's-Hertogenbosch, The Netherlands

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: sales@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer Support)

Website: www.supermicro.nl

Asia-Pacific

Address: Super Micro Computer, Inc.
3F, No. 150, Jian 1st Rd.
Zhonghe Dist., New Taipei City 235
Taiwan (R.O.C)

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

Email: support@supermicro.com.tw

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Overview.....	8
Quick Reference Table.....	11
Motherboard Features.....	12
1.2 Processor and Chipset Overview.....	16
1.3 Special Features	17
Recovery from AC Power Loss.....	17
1.4 System Health Monitoring.....	17
Onboard Voltage Monitors	17
Fan Status Monitor with Firmware Control	17
Environmental Temperature Control	17
System Resource Alert.....	18
1.5 ACPI Features.....	18
1.6 Power Supply	18
1.7 Advanced Power Management.....	18
Intel® Intelligent Power Node Manager (IPNM).....	18
Management Engine (ME).....	19

Chapter 2 Installation

2.1 Static-Sensitive Devices.....	20
Precautions	20
Unpacking	20
2.2 Motherboard Installation.....	21
Tools Needed	21
Location of Mounting Holes	21
Installing the Motherboard.....	22
2.3 Processor and Heatsink Installation.....	23
Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processors	23
Overview of the Processor Socket Assembly	24
Overview of the Processor Heatsink Module (PHM)	25
Attaching the Processor to the Narrow Processor Clip to Create the Processor Package Assembly.....	26
Attaching the Processor Package Assembly to the Heatsink to Form the Processor	

Heatsink Module (PHM).....	27
Preparing the CPU Socket for Installation.....	28
Removing the Dust Cover from the CPU Socket.....	28
Installing the Processor Heatsink Module (PHM)	29
Removing the Processor Heatsink Module (PHM) from the Motherboard.....	30
2.4 Memory Support and Installation	31
Memory Support.....	31
General Memory Population Requirements.....	31
DDR4 Memory Support for Intel Xeon Scalable-SP Processors.....	32
DDR4 Memory Support for 2nd Gen Intel Xeon Scalable-SP Processors.....	32
DIMM Population Guidelines for Optimal Performance.....	33
DIMM Population Table.....	34
DIMM Installation	35
DIMM Removal	35
2.5 Rear I/O Ports.....	36
2.6 Connectors	40
Headers.....	40
2.7 Jumper Settings	44
How Jumpers Work.....	44
2.8 LED Indicators.....	48
Chapter 3 Troubleshooting	
3.1 Troubleshooting Procedures	52
Before Power On	52
No Power	52
No Video	53
System Boot Failure	53
Memory Errors	53
Losing the System's Setup Configuration.....	54
When the System Becomes Unstable	54
3.2 Technical Support Procedures	56
3.3 Frequently Asked Questions	57
3.4 Battery Removal and Installation	58
Battery Removal.....	58

Proper Battery Disposal	58
Battery Installation.....	58
3.5 Returning Merchandise for Service.....	59
Chapter 4 UEFI BIOS	
4.1 Introduction.....	60
4.2 Main Setup	61
4.3 Advanced Setup Configurations.....	63
4.4 Event Logs	91
4.5 IPMI	93
4.6 Security	96
4.7 Boot.....	99
4.8 Save & Exit	102
Appendix A BIOS Codes	
A.1 BIOS Error POST (Beep) Codes	104
Appendix B Software Installation	
B.1 Installing Software Programs	106
B.2 SuperDoctor® 5.....	107
Appendix C Standardized Warning Statements	
Appendix D UEFI BIOS Recovery	
D.1 Overview.....	111
D.2 Recovering the UEFI BIOS Image.....	111
D.3 Recovering the Main BIOS Block with a USB Device	112
Appendix E Configuring VROC RAID Settings	
E.1 All Intel® VMD Controllers Features.....	116
E.2 Configuring RAID Settings	123
E.3 Use of Journaling Drive.....	136
Appendix F Secure Boot Settings	
F.1 Boot mode select Feature.....	140
F.2 Secure Boot/ Secure Boot Mode/ CSM Support Features	141
F.3 Secure Boot Settings	142
F.4 Key Management Settings.....	145
Appendix G Configuring Network Interface Card (NIC) Settings	
G.1 Network Interface Card (NIC) Settings	162

Chapter 1

Introduction

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

1.1 Overview

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

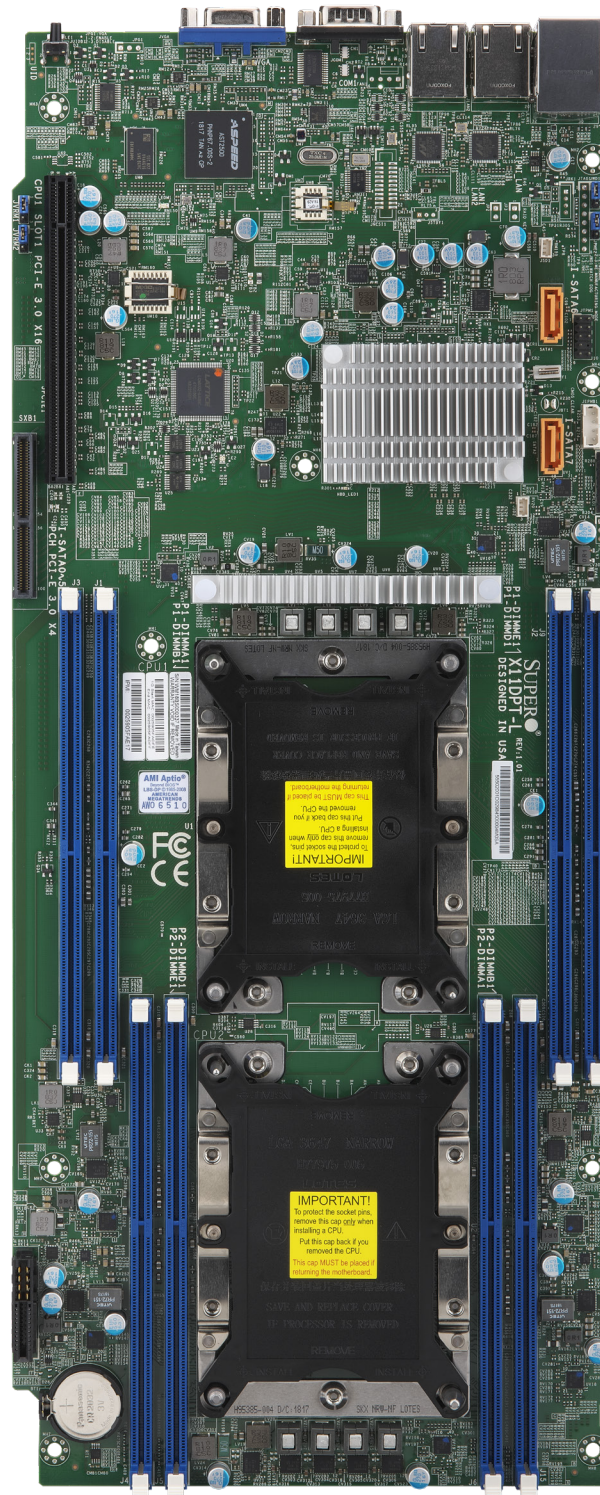
Important Links


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

- Supermicro product manuals: <http://www.supermicro.com/support/manuals/>
- Product drivers and utilities: <http://www.supermicro.com/wftp>
- Product safety info: http://www.supermicro.com/about/policies/safety_information.cfm
- If you have any questions, please contact our support team at: support@supermicro.com

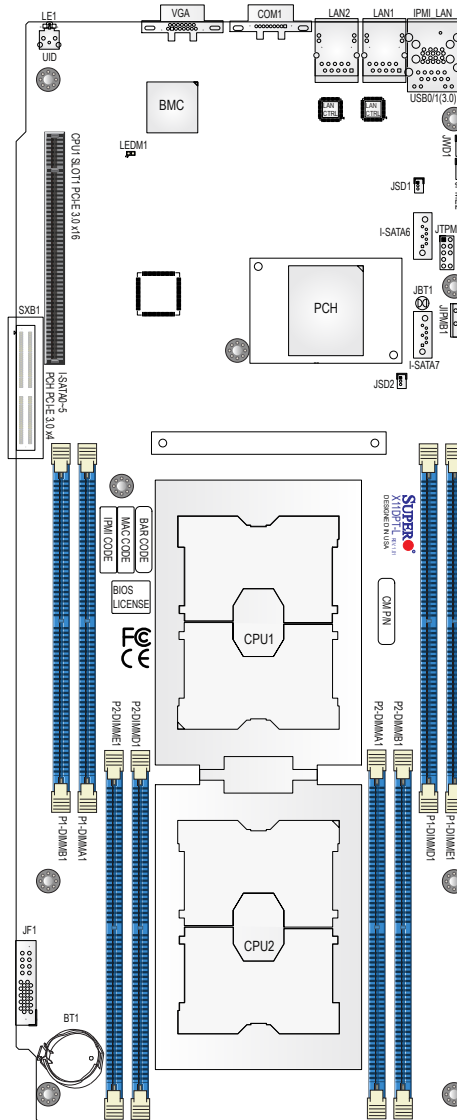
This manual may be periodically updated without notice. Please check the Supermicro website for possible updates to the manual revision level.

Figure 1-1. X11DPT-L Motherboard Image



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

**Figure 1-2. X11DPT-L Motherboard Layout
(not drawn to scale)**



Notes:

- See Chapter 2 for detailed information on jumpers, I/O ports, and JF1 front panel connections.
- "■" indicates the location of Pin 1.
- Jumpers/components/LED indicators not indicated are used for internal testing only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. Do not install the onboard battery upside down to avoid possible explosion.
- To avoid causing interference with other components, please be sure to use an add-on card that is fully compliant with the PCI-E standard on a PCI-E slot.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JPME2	Manufacturing Mode Select	Pins 1-2 (Normal)
JWD1	Watch Dog Timer Enable	Pins 1-2 (Enabled, Reset)

Connector	Description
BT1	Onboard Battery
COM1	Back Panel COM Port
I-SATA6/I-SATA7	I-SATA Ports with Built-in Power Pins and with Support of Supermicro SuperDOM (Disk On Module) Devices
IPMI_LAN	Dedicated IPMI_LAN Port
JF1	Front Panel Control Signals and Power Input Connector
JIPMB1	4-pin BMC External I ² C Header (for an IPMI-supported card)
JSD1/JSD2	SATA DOM Power Connectors 1/2
JTPM1	Trusted Platform Module (TPM)/Port 80 Connector
LAN1/LAN2	Gigabit LAN Ethernet Ports on the I/O Back Panel
(CPU1) SLOT1	PCI-Express 3.0 x16 Slot Supported by CPU1
SXB1	PCI-Express 3.0 x4 from PCH to SMCI- Proprietary Storage Slot for M.2 Hybrid (SATA/NVME) Support on ADP, SATA 0~5 Support on Back Panel
UID	Unit Identifier (UID) Switch
USB0/USB1	Back Panel USB 3.0 Ports
VGA	VGA Port




LED	Description	Status
LE1	UID (Unit Identifier) LED	Solid Blue: Unit identified
LEDM1	BMC Heartbeat LED	Blinking Green: BMC normal



Notes:

1. Components not documented are for internal testing only.
2. Intel VMD is supported by SXB1. After you've enabled VMD in the BIOS on a PCI-E slot of your choice, this PCI-E slot will be dedicated for VMD use only, and it will no longer support any PCI-E device. To re-activate this slot for PCI-E use, please disable VMD in the BIOS.

Motherboard Features

Motherboard Features	
CPU	
<ul style="list-style-type: none"> This motherboard supports dual Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP processors with two Intel UltraPath Interconnect (UPI) links of up to 10.4 GT/s  <p>Note: Both CPUs need to be installed for full access to the PCI-E slots, DIMM slots, and onboard controllers. Refer to the block diagram on page 15 to determine which slots or devices may be affected.</p>	
Memory	
<ul style="list-style-type: none"> Integrated memory controller embedded in the processor supports up to 2TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 1TB of Load Registered DIMM (LRDIMM), with speeds of 2933*/2666/2400/2133/1866/1600/1333 MHz modules in 8 memory slots  <p>Note: 1. 2933 MHz memory is supported by 2nd Gen Intel Xeon Scalable-SP (82xx/62xx series) processors only. 2. See section 2.4 for detailed DDR4 memory support list.</p>	
DIMM Size	
<ul style="list-style-type: none"> Up to 256GB at 1.2V  <p>Note: 1. Memory speed and maximum memory support depend on the processors used in the system. 2: For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.</p>	
Chipset	
<ul style="list-style-type: none"> Intel C621 for X11DPT-L 	
Expansion Slots	
<ul style="list-style-type: none"> One (1) PCI-E 3.0 x16 slot supported by CPU1 (CPU1 SLOT1) One (1) PCI-E 3.0 x4 from PCH to SMCI- proprietary storage slot for M.2 Hybrid (SATA/NVME) support on ADP 	
BaseBoard Management Controller (BMC)	
<ul style="list-style-type: none"> ASPEED AST2500 Baseboard Controller (BMC) supports IPMI 2.0 One (1) Dedicated IPMI LAN located on the I/O back panel 	
Graphics	
<ul style="list-style-type: none"> Graphics controller via AST2500 BMC (BaseBoard Management Controller) 	
Network Connection	
<ul style="list-style-type: none"> Two Gigabit Ethernet ports (LAN1/LAN2) supported by Intel PCH C621 One IPMI-dedicated LAN supported by the AST2500 BMC 	
I/O Devices	
<ul style="list-style-type: none"> Serial (COM) Port 	<ul style="list-style-type: none"> One (1) Fast UART 16550 port on the I/O back panel
<ul style="list-style-type: none"> SATA 3.0 	<ul style="list-style-type: none"> Six (6) SATA 3.0 ports supported by Intel® PCH (I-SATA0~5) Two (2) SATA 3.0 ports with power-pins built-in, w/support of Supermicro SuperDOM (I-SATA6/I-SATA7)
<ul style="list-style-type: none"> RAID (PCH) 	<ul style="list-style-type: none"> RAID 0, 1, 5, and 10
Peripheral Devices	
<ul style="list-style-type: none"> Two (2) USB 3.0 ports on the I/O back panel (USB0/USB1) 	

Motherboard Features

BIOS

- 32MB SPI AMI BIOS® SM Flash UEFI BIOS
- ACPI 3.0/4.0, USB keyboard, Plug-and-Play (PnP), SPI dual/quad speed support, riser-card auto detection support, and SMBIOS 2.7 or later

Power Management

- Main switch override mechanism
- Power-on mode for AC power recovery
- Intel® Intelligent Power Node Manager 4.0 (available when the Supermicro Power Manager [SPM] is installed and a special power supply is used)
- Management Engine (ME)

System Health Monitoring

- Onboard voltage monitoring for +1.8V, +3.3V, +5V, +3.3V standby, +5V standby, +12V, CPU core, memory, and PCH voltages
- CPU System LED and control
- CPU Thermal Trip support
- Status monitor for on/off control
- CPU Thermal Design Power (TDP) support of up to 140W (See Note 1 on next page.)

Fan Control

- Fan status monitoring via IPMI
- Single cooling zone
- Multi-speed fan control via onboard BMC
- Pulse Width Modulation (PWM) fan control

System Management


- Trusted Platform Module (TPM) support
- PECEI (Platform Environment Control Interface) 3.1 support
- UID (Unit Identification)/Remote UID
- System resource alert via SuperDoctor® 5
- SuperDoctor® 5, Watch Dog, NMI

LED Indicators

- CPU/system Overheating
- Power Indicator
- Fan Failure
- UID/remote UID
- LAN activity
- HDD activity

Dimensions

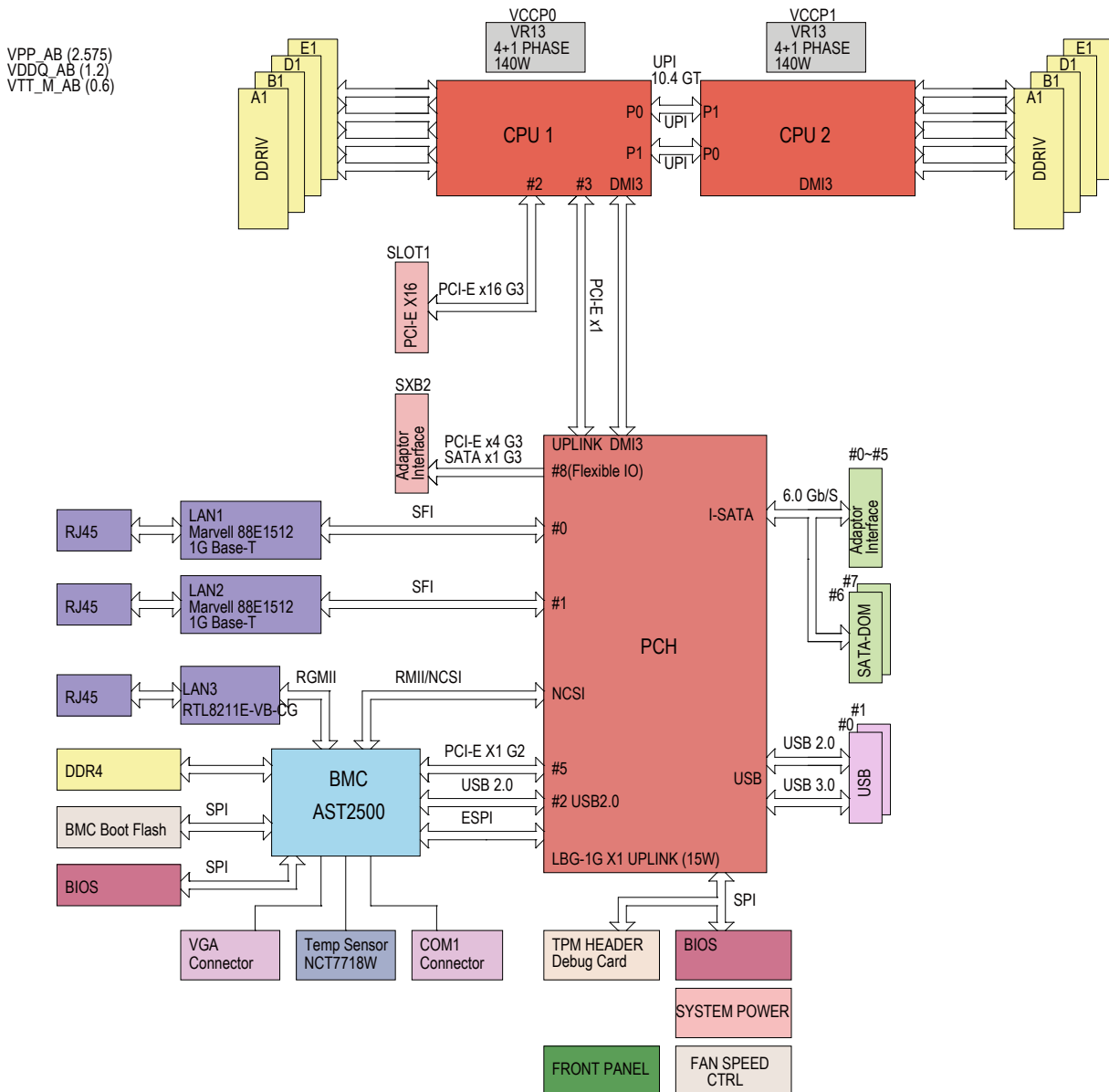
- 16.64" (L) x 6.8" (W) (422.7 mm x 172.7 mm)


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

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

Note 3: It is strongly recommended that you change BMC login information upon initial system power-on. The manufacturer default username is ADMIN and the password is ADMIN. For proper BMC configuration, please refer to <http://www.supermicro.com>.

Figure 1-3.
C621 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 Intel Xeon Scalable-SP and 2nd Generation Intel Xeon Scalable-SP processors (Socket P) and the C621 chipset, this motherboard provides superb system performance, efficient power management, and a rich feature set based on cutting edge technology to address the needs of next-generation computer users. With support of Intel® UltraPath Interconnect (UPI) of up to 10.4 GT/s, and Intel® AVX-512 new instructions, this motherboard drastically increases system performance for a multitude of server applications.

Features Supported by Intel Xeon Scalable-SP Processors

Intel Xeon Scalable-SP processors support the following features:

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

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

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

- Higher performance for a wider range of workloads with per-core performance increase
- Up to 2933 MHz memory supported
- Vector Neural Network Instruction (VNNI) support for Accelerate Deep Learning & Artificial Intelligence (AI) workloads
- Speed Select Technology provides multiple CPU profiles that can be set in the BIOS. (This feature is available on select CPU SKUs).
- Seamless hardware security mitigations & performance/frequency flexibility



Note: 2933 MHz memory are supported by 2nd Generation Intel Xeon Scalable-SP processors only.

1.3 Special Features

This section describes the health monitoring features of the X11DPT-L motherboard. The motherboard has an onboard ASPEED AST2500 Baseboard Management Controller (BMC) that supports system health monitoring.

Recovery from AC Power Loss

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

1.4 System Health Monitoring

This section describes the health monitoring features of the X11DPT-L motherboard. The motherboard has an onboard Baseboard Management Controller (BMC) chip that supports system health monitoring.

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

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



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

System Resource Alert

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

1.5 ACPI Features

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

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

1.6 Power Supply

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

1.7 Advanced Power Management

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

Intel® Intelligent Power Node Manager (IPNM)

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



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

Management Engine (ME)

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

Chapter 2

Installation

2.1 Static-Sensitive Devices

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

Precautions

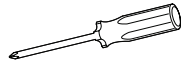
- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the board by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules,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

Unpacking

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

2.2 Motherboard Installation

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



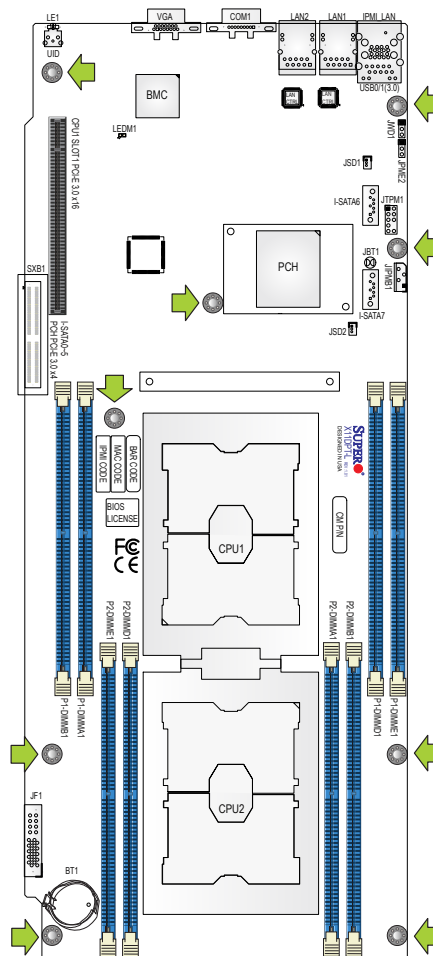
Phillips Screwdriver (1)



Phillips Screws (9)

Standoffs (9)
Only if Needed

Tools Needed



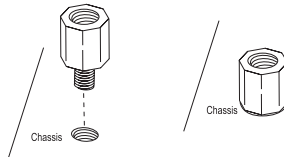
Location of Mounting Holes



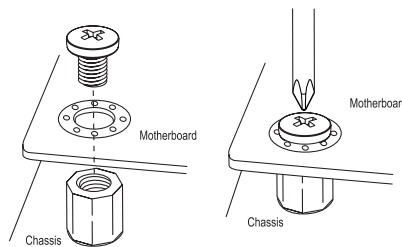
- Notes:**
1. To avoid damaging the motherboard and its components, please do not use a force greater than 8 lb/inch on each mounting screw during motherboard installation.
 2. Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components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

Installing the Motherboard


1. Install the I/O shield into the back of the chassis.
2. Locate the mounting holes on the motherboard. See the previous page for the location.



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



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

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

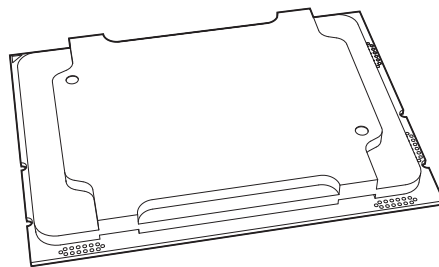
2.3 Processor and Heatsink Installation

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


 **Notes:**

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

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



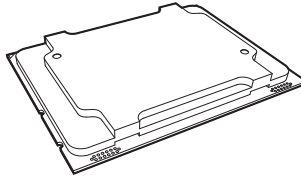
Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processor

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

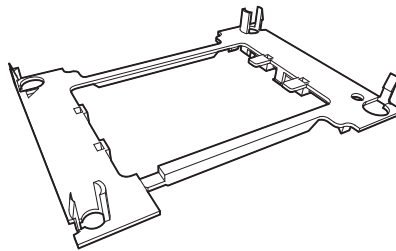
Overview of the Processor Socket Assembly

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

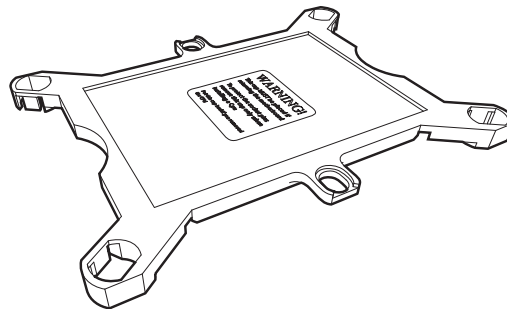
1. Intel® Processor



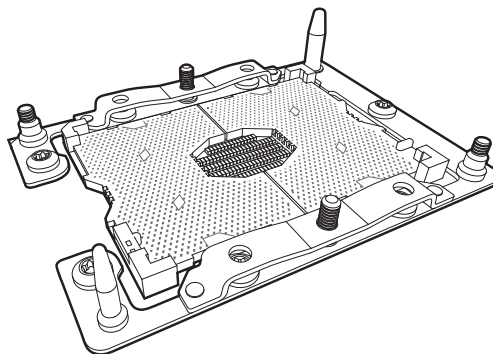
2. Narrow processor clip (the plastic processor package carrier used for the CPU)



3. Dust Cover



4. CPU Socket

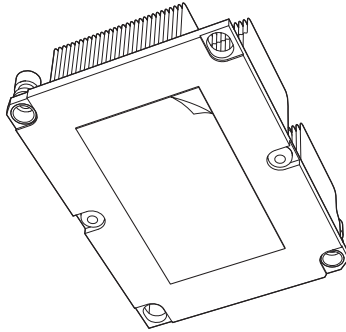


Note: Be sure to cover the CPU socket with the dust cover when the CPU is not installed.

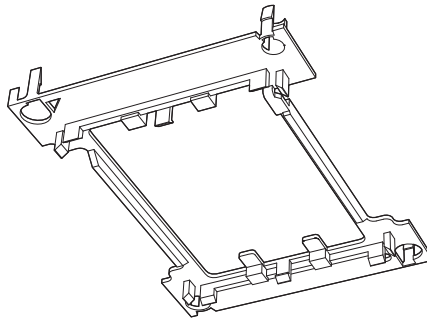
Overview of the Processor Heatsink Module (PHM)

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

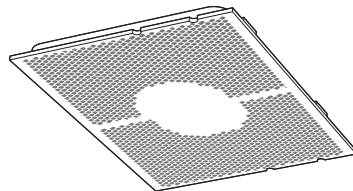
1. Heatsink



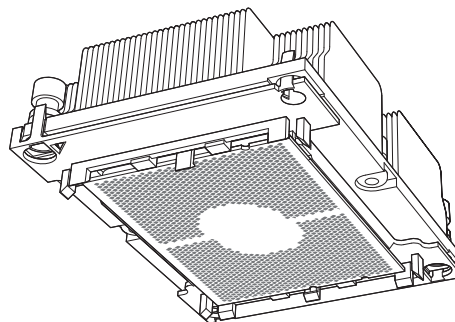
2. Narrow processor clip



3. Intel® Processor



Processor Heatsink Module (PHM)




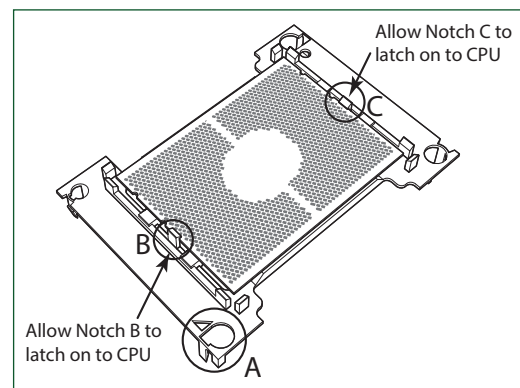
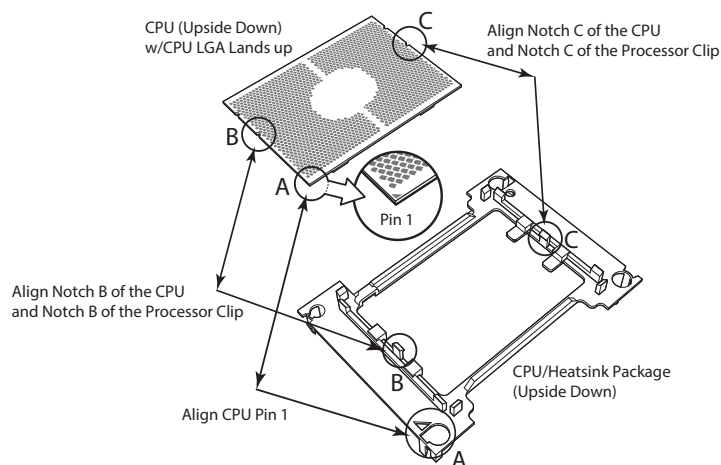
(Bottom View)

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

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

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

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

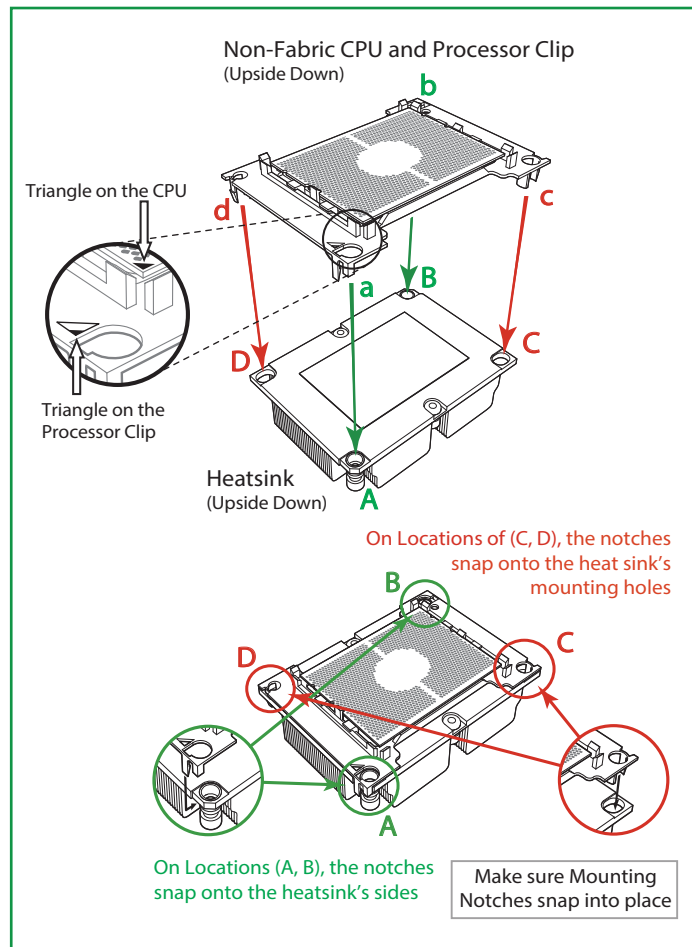


Processor Package Carrier (w/CPU mounted on the Processor Clip)

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

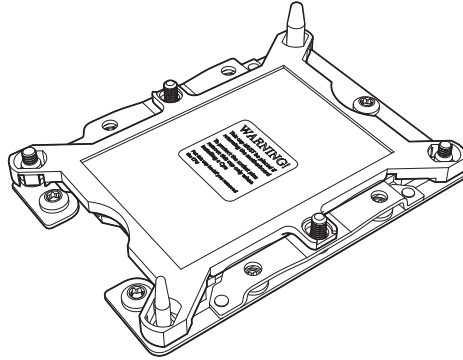
After you have made a processor package assembly by following the instructions on the previous page, please follow the steps below to mount the processor package assembly onto the heatsink to create the Processor Heatsink Module (PHM).

1. Locate "1" on the heatsink label and the triangular corner next to it on the heatsink. With your index finger pressing against the screw at this triangular corner, carefully hold and turn the heatsink upside down with the thermal-grease side facing up. Remove the protective thermal film if present, and apply the proper amount of the thermal grease as needed. (Skip this step if you have a new heatsink because the necessary thermal grease is pre-applied in the factory.)
2. Holding the processor package assembly at the center edge, turn it upside down. With the thermal-grease side facing up, locate the hollow triangle located at the corner of the processor carrier assembly ("a" in the graphic). Note a larger hole and plastic mounting clicks located next to the hollow triangle. Also locate another set of mounting clicks and a larger hole at the diagonal corner of the same (reverse) side of the processor carrier assembly ("b" in the graphic).
3. With the back of heatsink and the reverse side of the processor package assembly facing up, align the triangular corner on the heatsink ("A" in the graphic) against the mounting clips next to the hollow triangle ("a") on the processor package assembly.
4. Also align the triangular corner ("B") at the diagonal side of the heatsink with the corresponding clips on the processor package assembly ("b").
5. Once the mounting clips on the processor package assembly are properly aligned with the corresponding holes on the back of heatsink, securely attach the heatsink to the processor package assembly by snapping the mounting clips at the proper places on the heatsink to create the processor heatsink module (PHM).



Preparing the CPU Socket for Installation


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

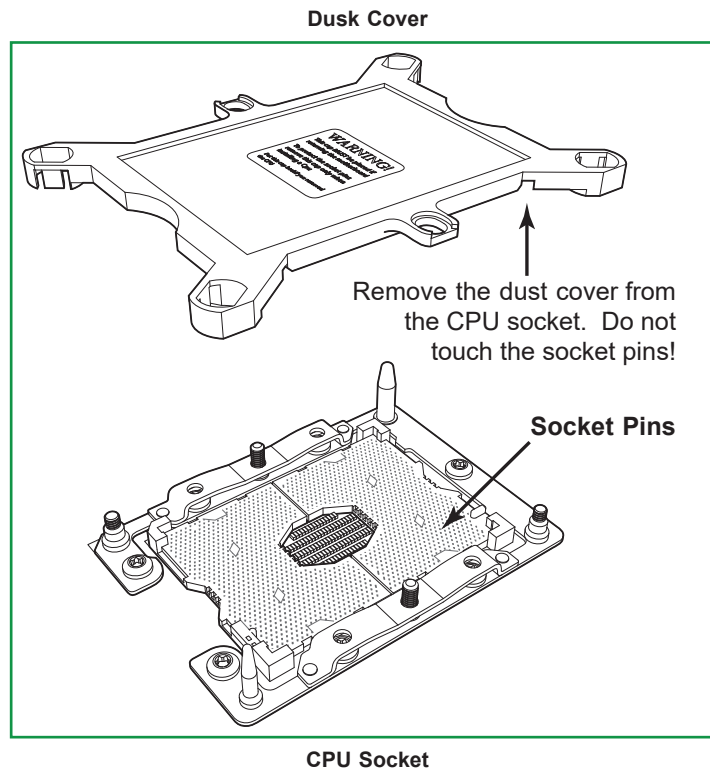


CPU Socket w/Dust Cover On

Removing the Dust Cover from the CPU Socket


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

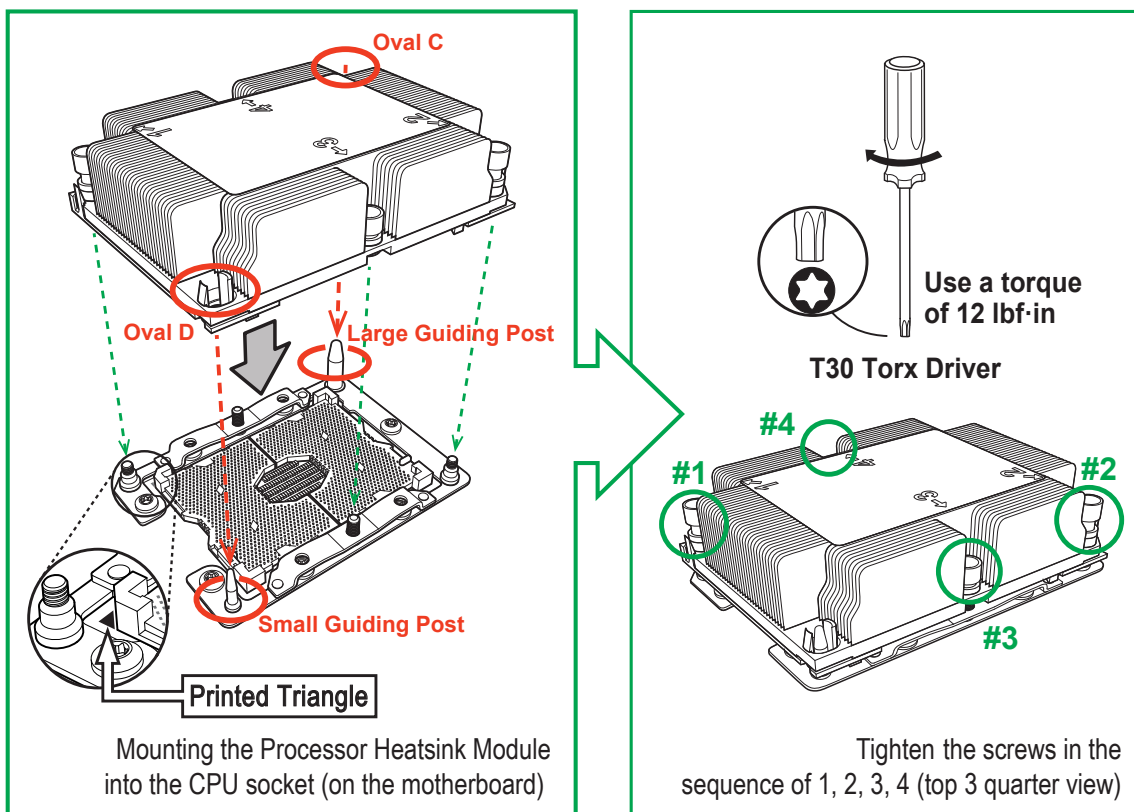
 **Note:** Do not touch the socket pins to avoid damaging them, causing the CPU to malfunction.



Installing the Processor Heatsink Module (PHM)

1. Once you have assembled the processor heatsink module (PHM) by following the instructions listed on page 30 or page 31, you are ready to install the processor heatsink module (PHM) into the CPU socket on the motherboard. To install the PHM into the CPU socket, follow the instructions below.
2. Locate the triangle (pin 1) on the CPU socket, and locate the triangle (pin 1) at the corner of the PHM that is closest to "1." (If you have difficulty locating pin 1 of the PHM, turn the PHM upside down. With the LGA-lands side facing up, you will note the hollow triangle located next to a screw at the corner. Turn the PHM right side up, and you will see a triangle marked on the processor clip at the same corner of hollow triangle.)
3. Carefully align pin 1 (the triangle) on the PHM against pin 1 (the triangle) on the CPU socket.
4. Once they are properly aligned, insert the two diagonal oval holes on the heatsink into the guiding posts.
5. Using a T30 Torx-bit screwdriver, install four screws into the mounting holes on the socket to securely attach the PHM onto the motherboard starting with the screw marked "1" (in the sequence of 1, 2, 3, and 4).


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

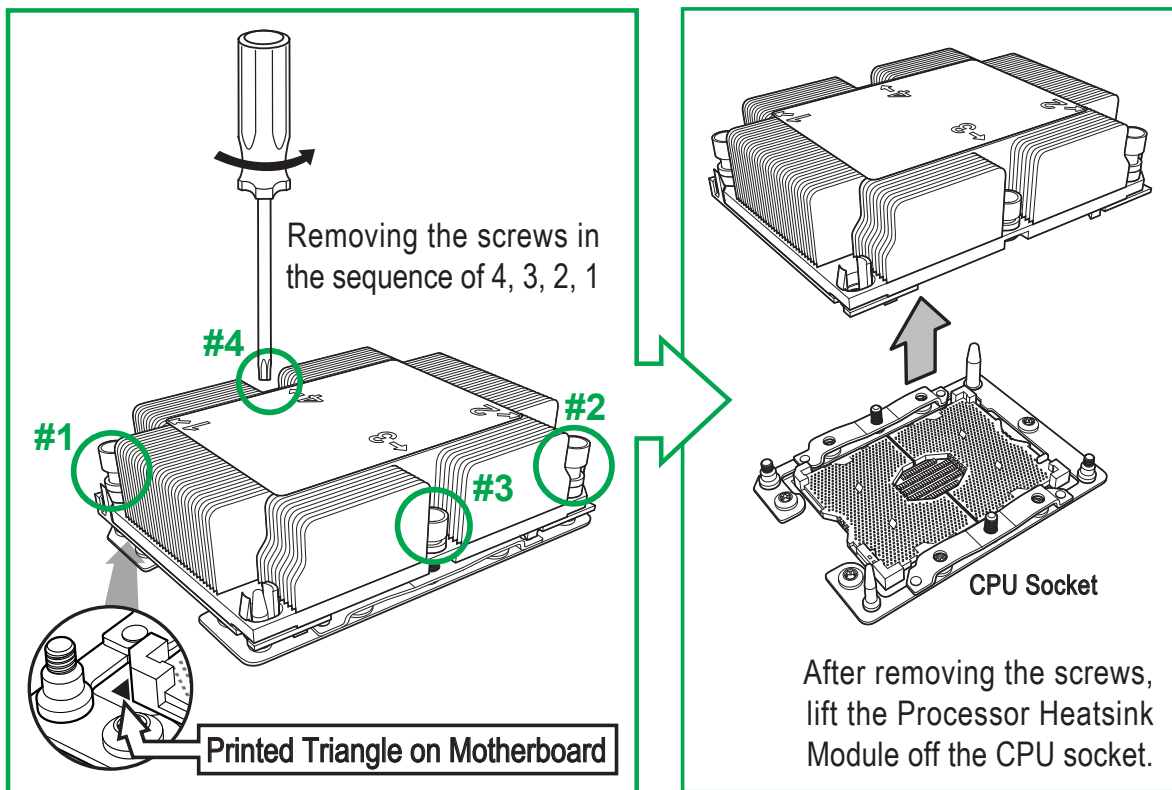


Removing the Processor Heatsink Module (PHM) from the Motherboard


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

1. Using a T30 Torx-bit screwdriver, turn the screws on the PHM counterclockwise to loosen them from the socket, starting with screw marked #4 (in the sequence of 4, 3, 2, 1).
2. After all four screws are removed, wiggle the PHM gently and pull it up to remove it from the socket.

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




2.4 Memory Support and Installation

 **Notes:** Check the Supermicro website for recommended memory modules. Exercise extreme care when installing or removing DIMM modules to prevent any damage.

Memory Support

The motherboard supports up to 2TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 1TB of Load Registered DIMM (LRDIMM), with speeds of 2933*/2666/2400/2133/1866/1600/1333 MHz modules in 8 memory slots. (***Notes** below). Populating the DIMM slots in a 1DPC (one DIMMs per channel) configuration with pairs of memory modules of the same type, speed, and size will result in interleaved memory, which improves performance.

 **Notes:** **1.** 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. **2.** Unbalanced memory configuration is not recommended. **3.** 2933 MHz memory is supported by 2nd Generation Intel Xeon Scalable-SP (82xx/62xx series) processors only. **4.** The memory capacity support will differ according to the processor SKUs.

General Memory Population Requirements

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.

DDR4 Memory Support for Intel Xeon Scalable-SP Processors

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

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

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



Notes: 2933 MHz memory is supported by 2nd Generation Intel Xeon Scalable-SP processors only.

DIMM Population Guidelines for Optimal Performance

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

Key Parameters for DIMM Configuration


Key Parameters for DIMM Configurations	
Parameters	Possible Values
Number of Channels	1, 2, 3, 4, 5, or 6
Number of DIMMs per Channel	1DPC (1 DIMM Per Channel)
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	
<ul style="list-style-type: none"> All DIMMs must be all DDR4 DIMMs. x4 and x8 DIMMs can be mixed in the same channel. Mixing of LRDIMMs and RDIMMs is not allowed in the same channel, across different channels, and across different sockets. Mixing of non-3DS and 3DS LRDIMM is not allowed in the same channel, across different channels, and across different sockets. 	


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

DIMM Population Table

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

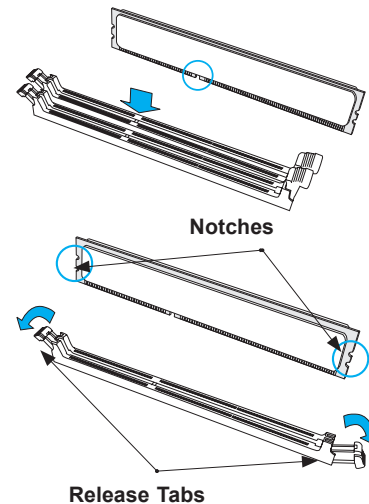
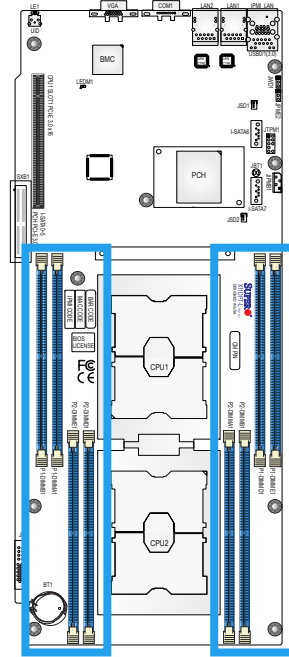
Memory Population Table for the Motherboard Using Intel Xeon Scalable-SP and 2nd Gen Intel Xeon Scalable-SP Processors

Memory Population Table for the X11DP Motherboard w/8 DIMM Slots Onboard	
When 1 CPU is used:	Memory Population Sequence
1 CPU & 1 DIMM	CPU1: P1-DIMMA1
1 CPU & 2 DIMMs	CPU1: P1-DIMMA1/P1-DIMMD1
1 CPU & 3 DIMMs (Unbalanced: not recommended)	CPU1: P1-DIMMB1/P1-DIMMA1/P1-DIMMD1
1 CPU & 4 DIMMs	CPU1: P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1
When 2 CPUs are used:	Memory Population Sequence
2 CPUs & 2 DIMMs	CPU1: P1-DIMMA1 CPU2: P2-DIMMA1
2 CPUs & 4 DIMMs	CPU1: P1-DIMMA1/P1-DIMMD1 CPU2: P2-DIMMA1/P2-DIMMD1
2 CPUs & 6 DIMMs	CPU1: P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1 CPU2: P2-DIMMA1/P2-DIMMD1
2 CPUs & 8 DIMMs	CPU1: P1-DIMMB1/P1-DIMMA1/P1-DIMMD1/P1-DIMME1 CPU2: P2-DIMMB1/P2-DIMMA1/P2-DIMMD1/P2-DIMME1

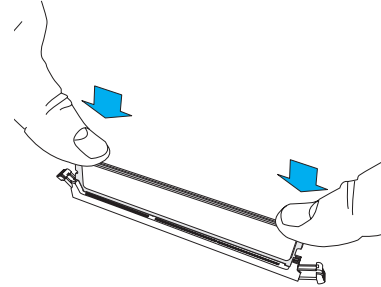
 **Note:** Please refer to the Memory Configuration User Guide for the X11 UP/DP/MP Motherboards that is posted on our website for detailed information on memory support for this motherboard.

DIMM Installation

1. Insert DIMM modules in the following order: P1-DIMMA1, P1-DIMMD1, P1-DIMMB1, and P1-DIMME1. For the system to work properly, please use memory modules of the same type and speed on the motherboard.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.
3. Align the key of the DIMM module with the receptive point on the memory slot.
4. Align the notches on both ends of the module against the receptive points on the ends of the slot.
5. Use two thumbs together to press the notches on both ends of the module straight down into the slot until the module snaps into place.
6. Press the release tabs to the lock positions to secure the DIMM module into the slot.

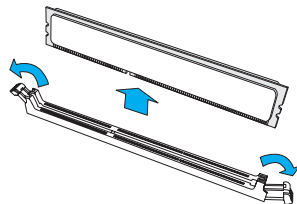


Insert the DIMM module into the memory slot.



DIMM Removal

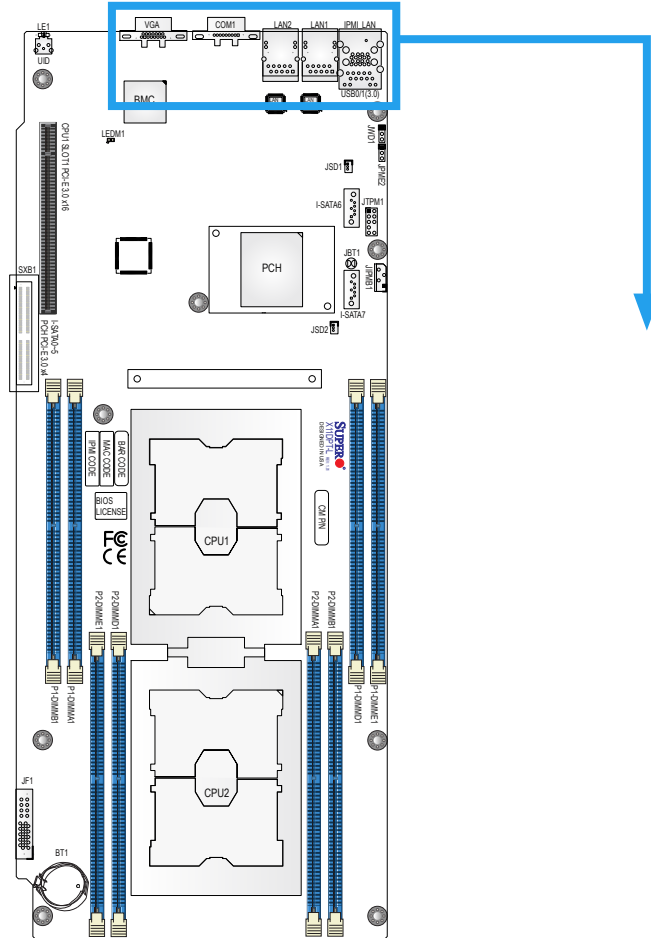
Press the release tabs on both ends of the DIMM socket to release the DIMM module from the socket as shown in the drawing below.



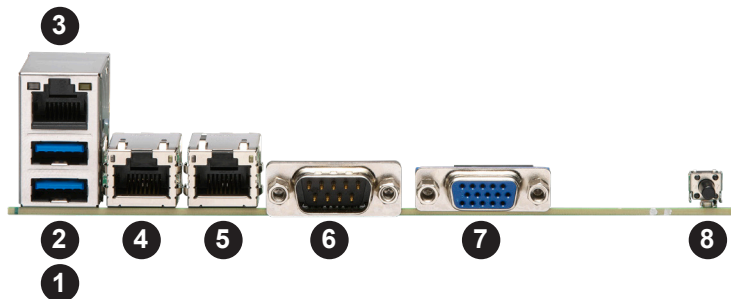
Warnings: 1. Please do not use excessive force when pressing the release tabs on the ends of the DIMM socket to avoid causing any damage to the DIMM module or the DIMM socket. 2. Please handle DIMM modules with care. Carefully follow all the instructions given on Page 1 of this chapter to prevent ESD-related damages to your memory modules or components.

2.5 Rear I/O Ports

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



Back Panel I/O Port Locations and Definitions



Back Panel I/O Ports					
No.	Description	No.	Description	No.	Description
1.	USB0 (USB 3.0)	4.	LAN1	7.	VGA
2.	USB1 (USB 3.0)	5.	LAN2	8.	Unit Identifier Switch (UID)
3.	IPMI LAN	6.	COM1		

VGA Port

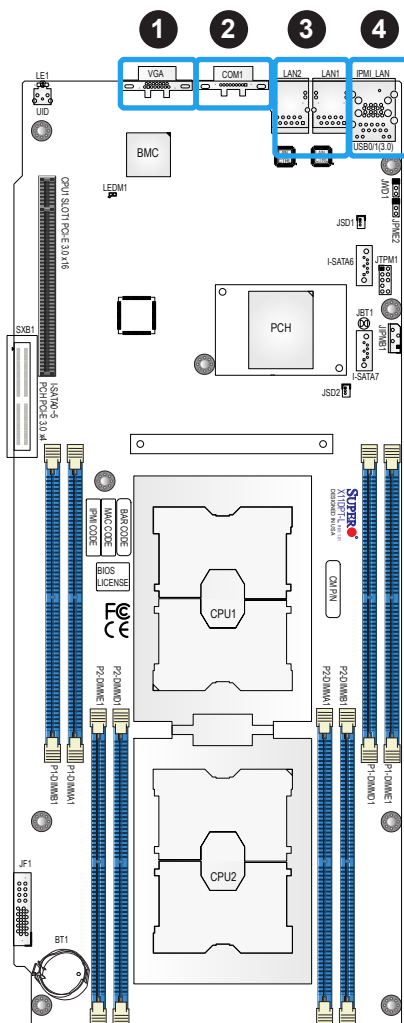
The onboard VGA port is located on the I/O back panel. Use this connection for VGA display.

Serial Port

There is one COM port (COM1) on the I/O back panel. The COM port provides serial communication support.

Ethernet Ports

Two Ethernet ports (LAN1, LAN2) are located on the I/O back panel. These Ethernet ports support GbE LAN connections on the motherboard. In addition, an IPMI-dedicated LAN that supports GbE LAN is located next to USB 0/1 ports on the back panel. All Ethernet ports accept RJ45 type cables. Please refer to the LED Indicator Section for LAN LED information.



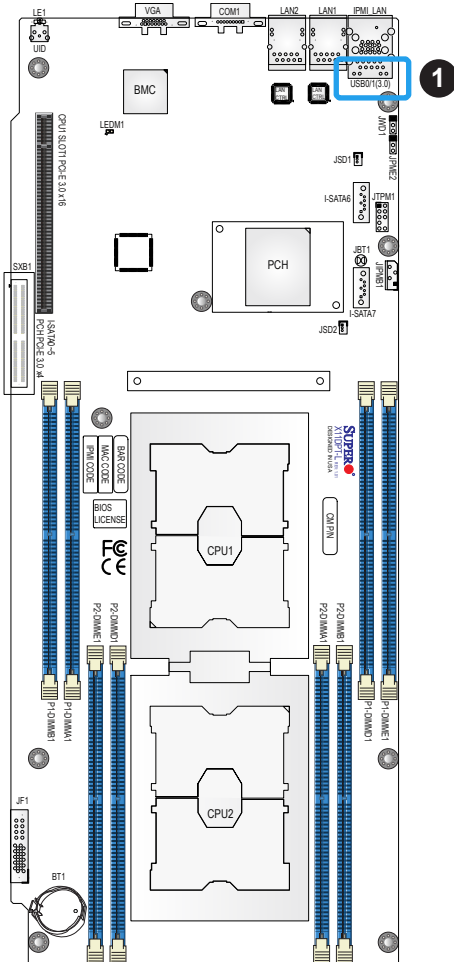
1. VGA Port
2. COM1
3. LAN Ports 1/2
4. IPMI LAN

Universal Serial Bus (USB) Ports

There are two USB 3.0 ports (USB0/USB1) on the I/O back panel. See the table below for pin definitions.

Back Panel USB0 (3.0) Pin Definitions			
Pin#	Definition	Pin#	Definition
1	VBUS1	33	SGND
2	D1N	34	SGND
3	D1P	35	SGND
4	GND	36	SGND
5	Stda_SSRX1N		
6	Stda_SSRX1P		
7	GND_DRAIN		
8	Stda_SSTX1N		
9	Stda_SSTX1P		

Back Panel USB1 (3.0) Pin Definitions	
Pin#	Definition
10	VBUS2
11	D2N
12	D2P
13	GND
14	Stda_SSRX2N
15	Stda_SSRX2P
16	GND_DRAIN
17	Stda_SSTX2N
18	Stda_SSTX2P



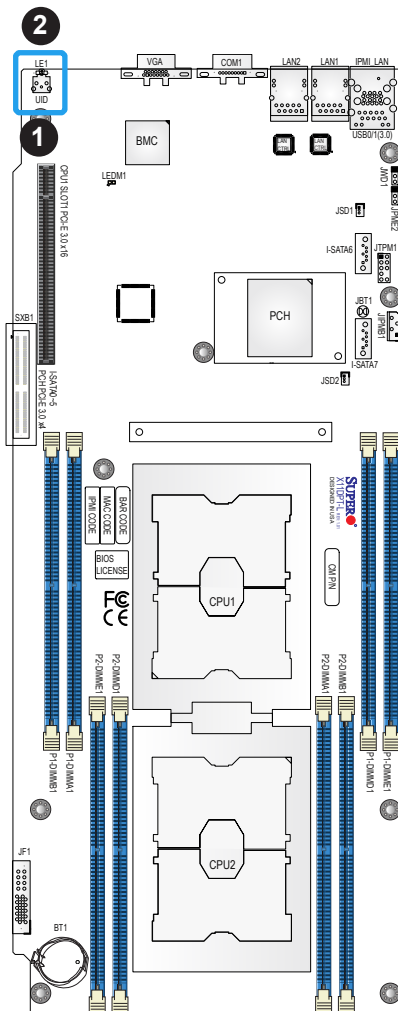
1. USB0/USB1 (3.0)

Unit Identifier Switch/UID LED Indicator

A Unit Identifier (UID) switch and a rear UID LED (LE1) are located on the rear side of the motherboard. When you press the rear UID switch, the rear UID LED (LE1) will be turned on. Press the UID switch again to turn off the LED indicator. The UID indicator provide easy identification of a system that may be in need of service. (**Note:** UID can also be triggered via IPMI on the motherboard. For more information, please refer to the IPMI User's Guide posted on our website at <http://www.supernmicro.com>.)

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

UID LED Pin Definitions	
Color	Status
Blue: On	Unit Identified



1. UID
2. UID LED Indicator

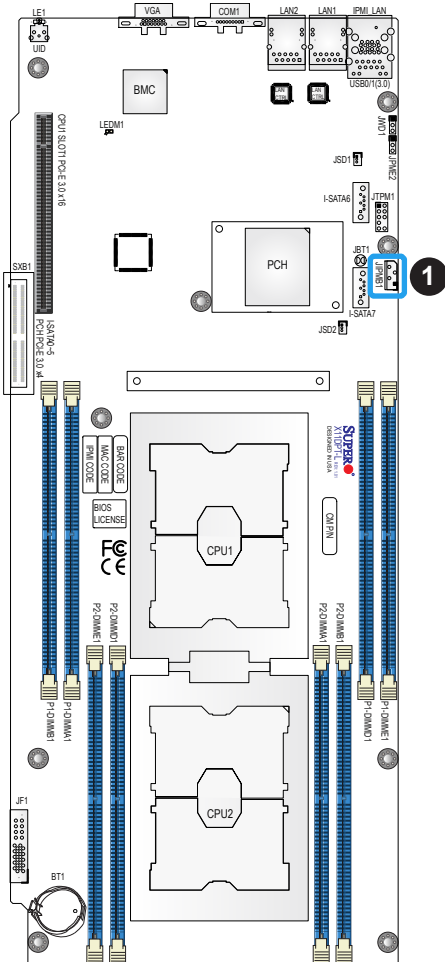
2.6 Connectors

Headers

4-pin BMC External I²C Header

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

External I ² C Header Pin Definitions	
Pin#	Definition
1	Data
2	Ground
3	Clock
4	No Connection

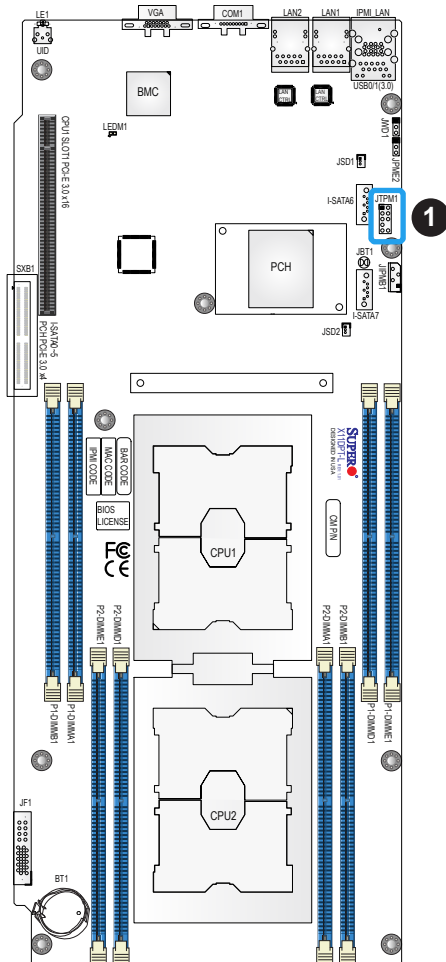


1. BMC External I²C Header

TPM Header

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

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

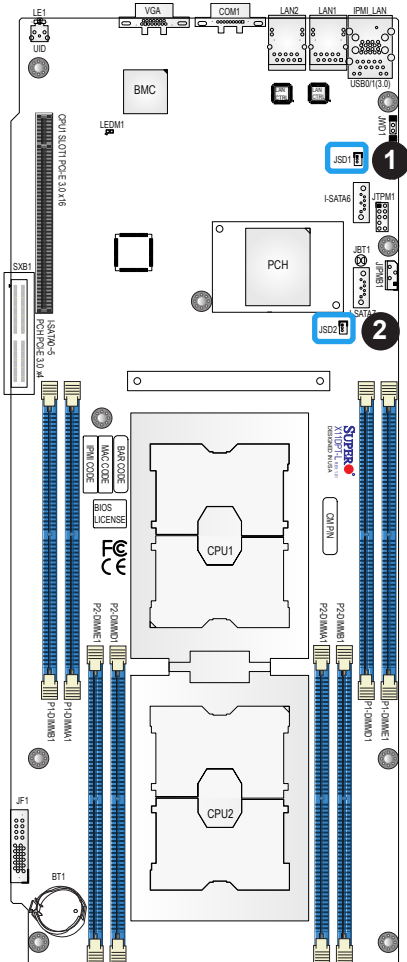


1. TPM/Port 80 Header

Disk-On-Module Power Connector

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


DOM Power Pin Definitions	
Pin#	Definition
1	5V
2	Ground
3	Ground

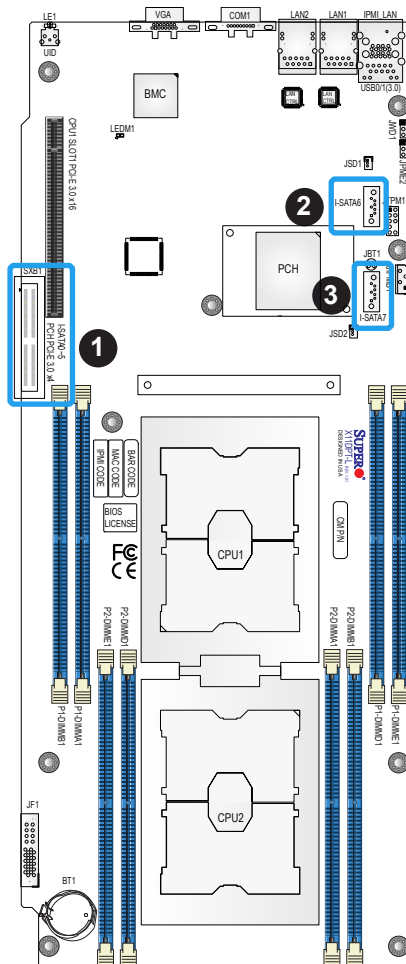


1. JSD1
2. JSD2

I-SATA 3.0 Ports

The X11DPT-L has eight I-SATA 3.0 ports (I-SATA0 ~ I-SATA7) on the motherboard. These SATA ports are supported by the C621 chipset. I-SATA ports 0~5 are supported by SXB1. I-SATA6/I-SATA7 can be used with Supermicro SuperDOMs which are yellow SATA DOM connectors with power pins built in, and do not require external power cables. Supermicro SuperDOMs are backward-compatible with regular SATA HDDs or SATA DOMs that need external power cables. All these SATA ports provide serial-link signal connections, which are faster than the connections of Parallel ATA.

 **Note:** pinout tables are NOT NEEDED for COM ports, LAN ports, and SAS/SATA ports.




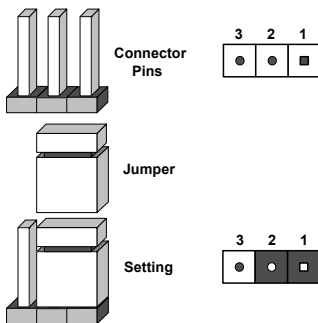
1. I-SATA0~5
2. I-SATA6
3. I-SATA7

2.7 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 at right for an example of jumping pins 1 and 2. Refer to the motherboard layout page for jumper locations.

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



CMOS Clear

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

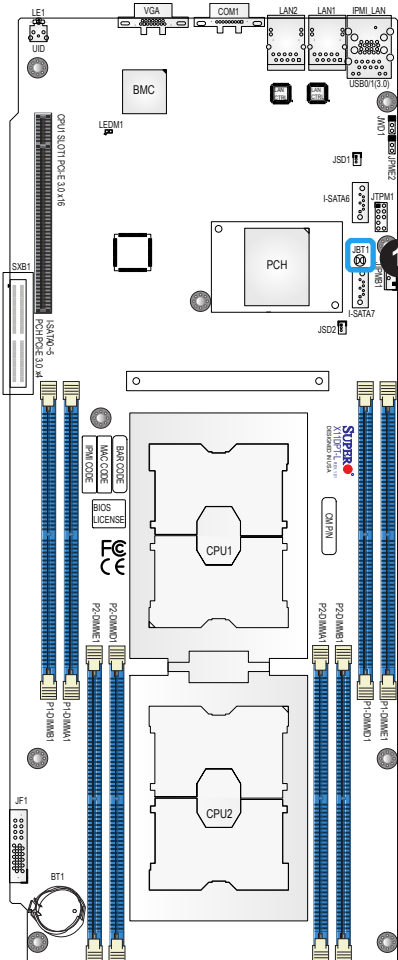
To Clear CMOS

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



Note: Clearing CMOS will also clear all passwords.

Do not use the PW_ON connector to clear CMOS.



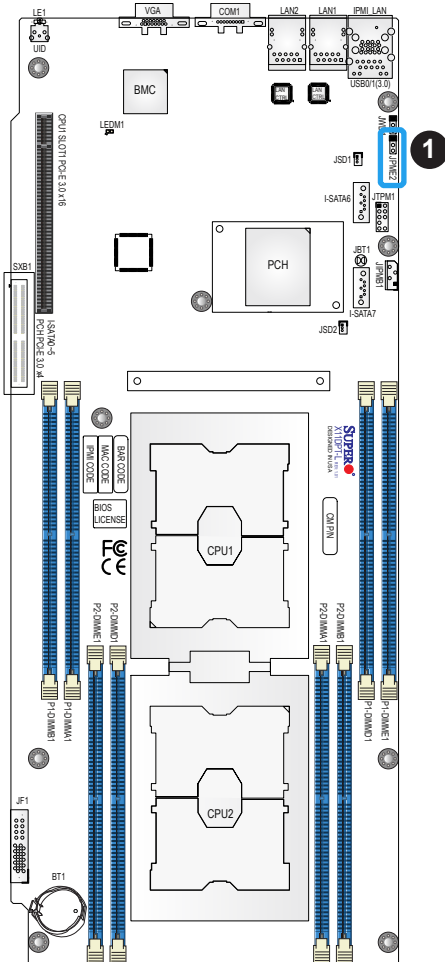
JBT1 contact pads

1. Clear CMOS

Manufacturing Mode Select

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


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



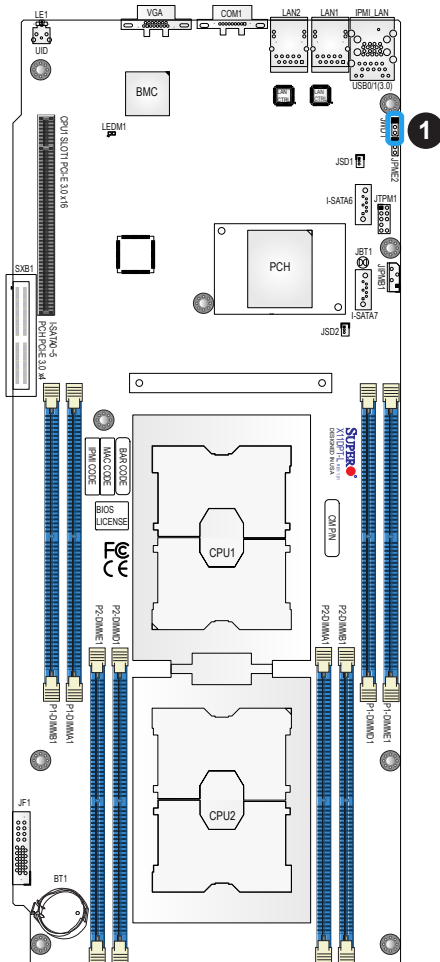
1. Manufacturing Mode Select

Watch Dog

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

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

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



1. Watch Dog

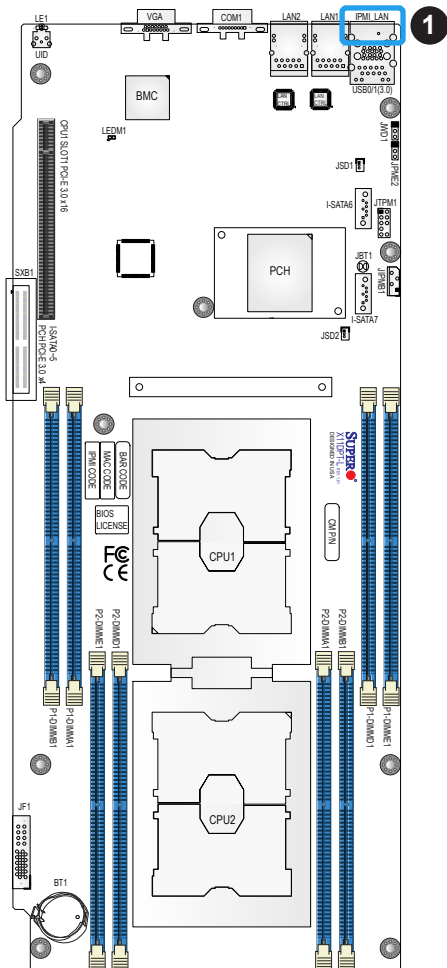
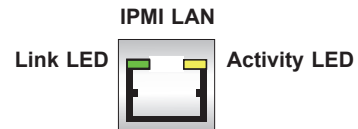
2.8 LED Indicators

IPMI-Dedicated LAN LEDs

An IPMI- dedicated LAN is located on the I/O back panel of the motherboard. The amber LED on the right indicates activity, while the green LED on the left indicates the speed of the connection. See the tables below for more information.

IPMI LAN Connection LED	
LED Color	Definition
Off	No Connection, 10 Mbps or 100 Mbps
Green	100 Mbps
Orange	1 Gbps

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



1. IPMI LAN LEDs

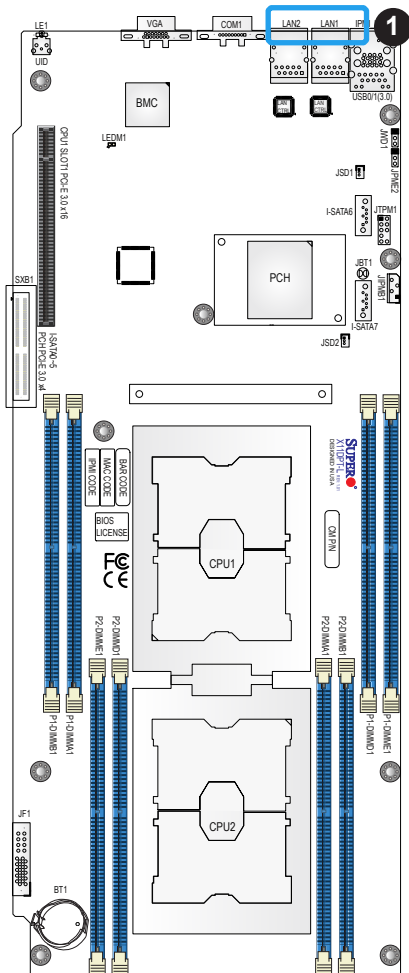


LAN1/LAN2 LEDs

Two LAN ports (LAN1/LAN2) are located on the I/O back panel of the motherboard. Each Ethernet LAN port has two LEDs. The amber LED on the right indicates activity, while the other Link LED on the left may be orange or off to indicate the speed of the connection. See the tables below for more information.

LAN1/LAN2 Link LED (Left)	
LED Color	Definition
Off	No Connection
Orange	1 Gbps

LAN1/LAN2 Activity LED (Right)		
LED Color	Status	Definition
Amber	Blinking	1 Gbps (Active)



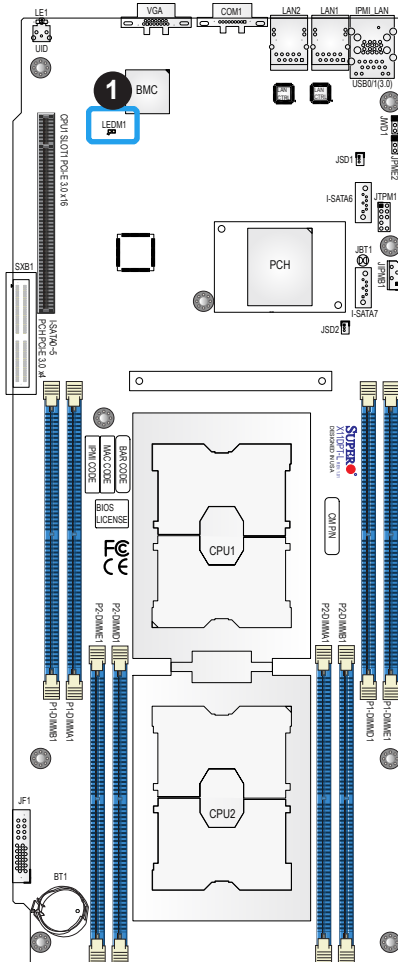
1. LAN1/LAN2 LEDs



BMC Heartbeat LED

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

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

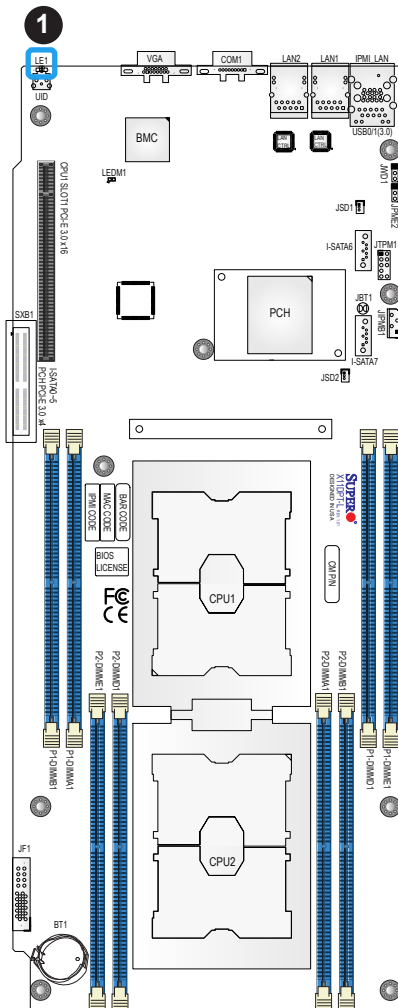


1. BMC Heartbeat LED

Unit ID LED

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

UID LED Indicator	
LED Color	Definition
Blue: On	Unit Identified



1. UID LED

Chapter 3

Troubleshooting

3.1 Troubleshooting Procedures

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

Before Power On

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

No Power

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

No Video

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

System Boot Failure

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

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

Memory Errors

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

Losing the System's Setup Configuration

1. Make sure that you are using a high quality power supply. A poor quality power supply may cause the system to lose the CMOS setup information. Refer to Section 1.6 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.
3. If the above steps do not fix the setup configuration problem, contact your vendor for repairs.

When the System Becomes Unstable

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

1. CPU/BIOS support: Make sure that your CPU is supported and that you have the latest BIOS installed in your system.
2. Memory support: Make sure that the memory modules are supported by testing the modules using memtest86 or a similar utility.



Note: Refer to the product page on our website at <http://www.supernmicro.com> for memory and CPU support and updates.

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

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

1. Source of installation: Make sure that the devices used for installation are working properly, including boot devices such as CD.
2. Cable connection: Check to make sure that all cables are connected and working properly.

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

3.2 Technical Support Procedures

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

1. Please review the 'Troubleshooting Procedures' and 'Frequently Asked Questions' (FAQs) sections in this chapter or see the FAQs on our website before contacting Technical Support.
2. BIOS upgrades can be downloaded from our website. **Note:** Not all BIOS can be flashed depending on the modifications to the boot block code.
3. If you still cannot resolve the problem, include the following information when contacting us for technical support:
 - Motherboard model and PCB revision number
 - BIOS release date/version (this can be seen on the initial display when your system first boots up)
 - System configuration

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

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

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: The X11DPT-L motherboard supports up to 2TB of 3DS Load Reduced DIMM (3DS LRDIMM), 3DS Registered DIMM (3DS RDIMM), or up to 1TB of Load Registered DIMM (LRDIMM), with speeds of 2933*/2666/2400/2133/1866/1600/1333 MHz modules in 8 memory slots. See Section 2.4 for details on Memory Support and Installation. (**Note: 1.** 2933 MHz memory is supported by 2nd Gen Intel Xeon Scalable-SP (82xx/62xx series) processors only. **2.** The memory capacity support will differ according to the processor SKUs.)

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>. 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. You can choose from the zip file and the .exe file. If you choose the zip BIOS file, please unzip the BIOS file onto a bootable USB device. Run the batch file using the format FLASH.BAT filename.rom from your bootable USB device to flash the BIOS. Then, your system will automatically reboot.

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

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

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. 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.
3. Remove the battery.

Proper Battery Disposal

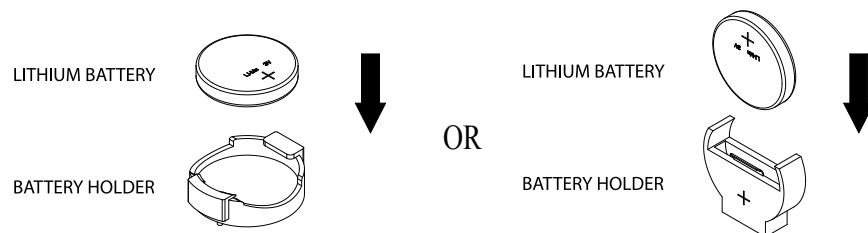
Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency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

Battery Installation

1. To install an onboard battery, follow the steps 1 & 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.



Note: 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 to the manufacturer, the RMA number should be prominently displayed on the outside of the shipping carton and mailed prepaid or hand-carried. Shipping and handling charges will be applied for all orders that must be mailed when service is complete.

For faster service, RMA authorizations may be requested online (<http://www.supermicro.com/support/rma/>).

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

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

Chapter 4

UEFI BIOS

4.1 Introduction

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



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

Starting the Setup Utility

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

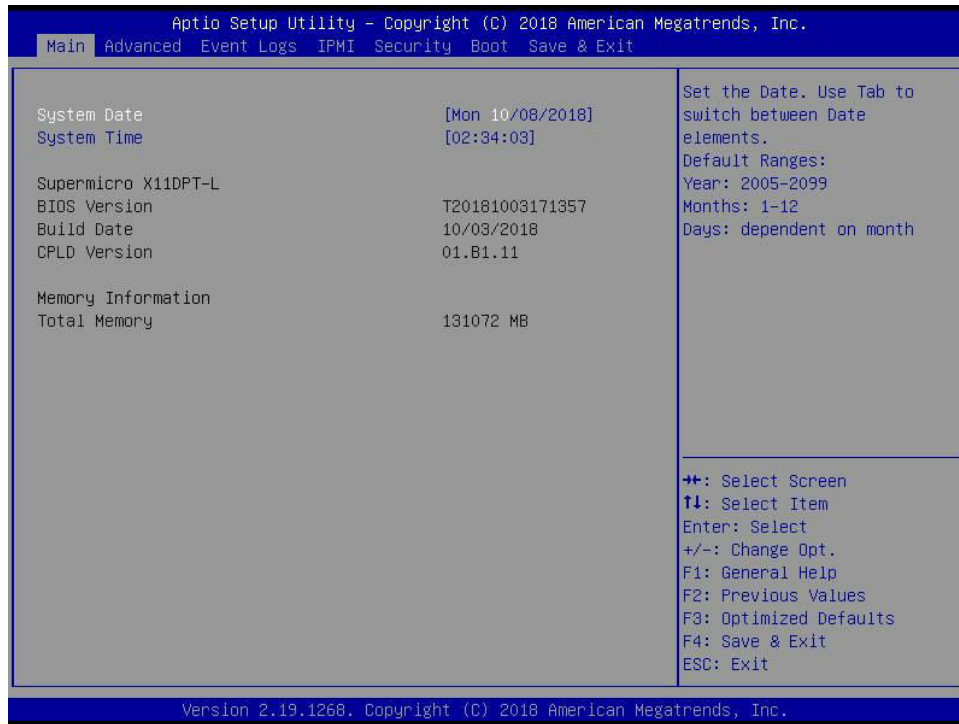
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it. (Note that 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. The following Main menu items will be displayed:



System Date/System Time

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

 **Note:** The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00. The date's default value is 01/01/2015 after RTC reset.

Supermicro X11DPT-L

BIOS Version

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

Build Date

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

CPLD Version

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

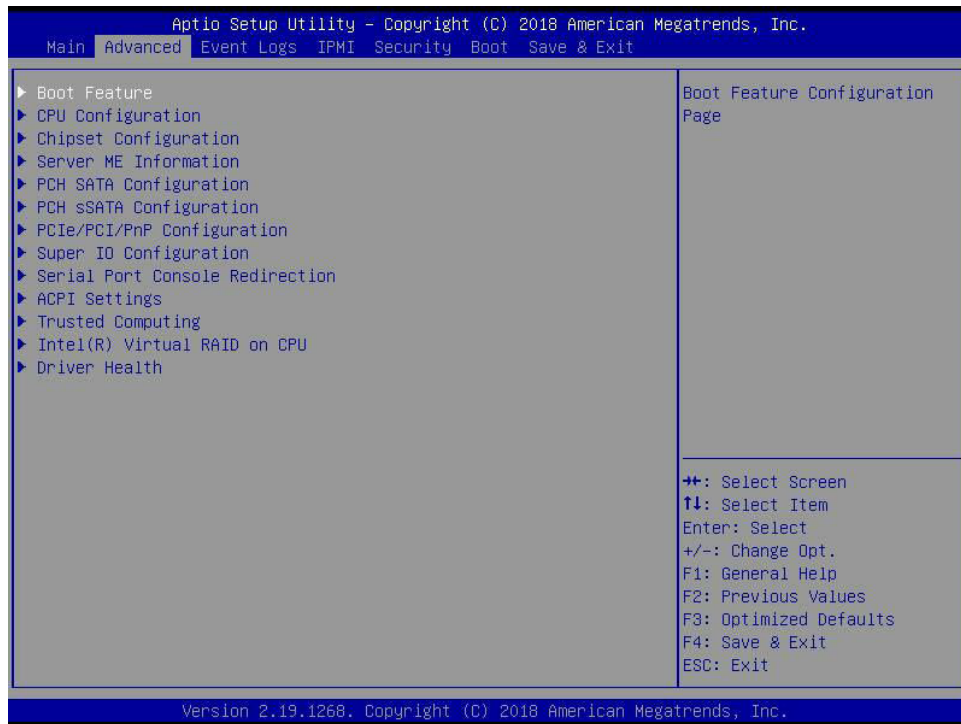
Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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



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

► Boot Feature

Quiet Boot

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

Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to display the current Add On 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 item is set to Immediate, the ROM BIOS of the host adaptors will "capture" Interrupt 19 at bootup immediately and allow the drives that are attached to these host adaptors to function as bootable disks. If this item is set to Postponed, the ROM BIOS of the host adaptors will not capture Interrupt 19 immediately and allow the drives attached to these adaptors to function as bootable devices at bootup. The options are **Immediate** and Postponed.

Re-try Boot

If this item 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 4 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

Processor Configuration

The following CPU information will be displayed:

- 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 6140 CPU @ 2.30GHz
- Processor 1 Version
- Intel(R) Xeon (R) Gold 6140 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

Streaming SIMD Extensions 3 (SSE3) includes Monitor and Mwait instructions, which are used for thread synchronization. The Monitor instruction monitors a region of memory for writes, and Mwait instructions instruct the CPU to stop until the monitored region begins to write. Select Enable to enable the Monitor/Mwait instructions. The options are Disable and **Enable**.

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

Select Enabled 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 default is **Enable**. (Refer to the Intel® and Microsoft® websites for more information.)

Intel Virtualization Technology

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

Adjacent Cache Prefetch (Available when supported by the CPU)

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

DCU Streamer Prefetcher (Available when supported by the CPU)

Select Enabled 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 **Enable** and Disable.

DCU IP Prefetcher (Available when supported by the CPU)

Select Enabled 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 this feature is set to Enabled, 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**.

► Chipset Configuration

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

► North Bridge

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

► UPI Configuration

UPI Configuration

The following UPI information will be displayed:

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

Degrade Precedence

Use this feature to 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 Link L0p support. The options are Disable, Enable, and **Auto**.

Link L1 Enable

Select Enable for Link L1 support. 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 InvltoM Hybrid Push, InvltoM AllocFlow, Enable for Remote InvltoM Hybrid AllocNonAlloc, and Enable for Remote InvltoM and Remote WViLF.

SNC

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

XPT Prefetch

Select Enable for 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 Enabled 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**Integrated Memory Controller (IMC)****Enforce POR**

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

PPR Type

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

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 1866, 2000, 2133, 2400, and 2666.

Data Scrambling for NVDIMM

Use this feature to enable or disable data scrambling for non-volatile DIMM (NVDIMM) memory. The options are **Auto**, Disable, and Enable.

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

If Enabled, the tCCD_L overrides the SPD. When disabled, it is enforced based on memory frequency. The options are Disable and **Auto**.

2X REFRESH

This option allows the user to select 2X refresh mode. The options are **Auto** and Enabled.

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 DIMM population information.

P1 DIMMA1: 2666MT/S Micron SRx4 16GB RDIMM

P1 DIMMB1: 2666MT/S Micron SRx4 16GB RDIMM

P1 DIMMD1: 2666MT/S Micron SRx4 16GB RDIMM

P1 DIMME1: 2666MT/S Micron SRx4 16GB RDIMM

P2 DIMMA1: 2666MT/S Micron SRx4 16GB RDIMM

P2 DIMMB1: 2666MT/S Micron SRx4 16GB RDIMM

P2 DIMMD1: 2666MT/S Micron SRx4 16GB RDIMM

P2 DIMME1: 2666MT/S Micron SRx4 16GB RDIMM

► Memory RAS Configuration

Memory RAS Configuration Setup

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.

UEFI ARM Mirror

This options allows the system to imitate the behavior of the UEFI based Address Range Mirror with setup option. The options are **Disable** and Enable.

Memory Rank Sparing

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

Correctable Error Threshold

Use this item 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 item 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 in a processor will always remain clear during electric tuning. The options are **Disable** and **Enable**.

► CPU1 Configuration

IOU1 (IIO PCIe Br2)

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

► RSC-T2R-884 SLOT1



Note 1: The feature above is available when the device is detected by the system.

Note 2: The feature above displays depending on the device being installed in and detected by the system.

Note 3: Otherwise, the BIOS screen displays CPU SLOT1.

Link Speed

Use this feature to select the link speed for the PCI-E 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).

PCI-E Port Link Status

This feature displays current PCI-E Link Status.

PCI-E Port Link Max

This feature displays PCI-E Link maximum value.

PCI-E Port Link Speed

This feature displays current PCI-E 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 PCI-E device, allowing for maximum I/O efficiency. Selecting 128B or 256B will designate maximum packet size of 128 or 256. Options are 128B, 256B, and **Auto**. Auto is enabled by default.

►RSC-T2R-884 SLOT2 (Available when the device is detected by the system)

Link Speed

Use this feature to select the link speed for the PCI-E 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).

PCI-E Port Link Status

This feature displays current PCI-E Link Status.

PCI-E Port Link Max

This feature displays PCI-E Link maximum value.

PCI-E Port Link Speed

This feature displays current PCI-E 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 PCI-E device, allowing for maximum I/O efficiency. Selecting 128B or 256B will designate maximum packet size of 128 or 256. Options are 128B, 256B, and **Auto**. Auto is enabled by default.

► IOAT Configuration

Disable TPH

Transparent Hugepages is a Linux memory management system that enables communication in larger blocks (pages). Enabling this feature will increase performance. 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 **Enabled** and **Disabled**.

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 **Enabled** and **Disabled**.

Interrupt Remapping

Select **Enable** for Interrupt Remapping support to enhance system performance. 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

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



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

► Intel® VMD for Volume Management Device on CPU1

VMD Config for PStack0

Intel® VMD for Volume Management Device

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

****If the feature "Intel VMD for Volume Management Device" is set to Enable, the following features will be available:***

CPU1 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.

CPU1 SLOT4 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 1A~1D. The options are **Disable** and Enable.

VMD Config for PStack1

Intel® VMD for Volume Management Device

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

****If the feature "Intel VMD for Volume Management Device" is set to Enable, the following features will be available:***

CPU1 SLOT5 PCI-E 3.0 X16 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 "Intel VMD for Volume Management Device" is set to Enable, the following features will be available:*

CPU1 SLOT1 PCI-E 3.0 X4 (IN 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

CPU1 SLOT2 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 3A~3D. This will allow the user to replace the components without shutting down the system. The options are **Disable** and Enable.

► Intel® VMD for Volume Management Device on CPU2

VMD Config for PStack2

Intel® VMD for Volume Management Device

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

**If the feature "Intel VMD for Volume Management Device" is set to Enable, the following features will be available:*

CPU2 SLOT3 PCI-E 3.0 X16 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.

II0-PCI-E Express Global Options

PCI-E Completion Timeout Disable

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

► South Bridge

USB Module Version

This feature display current USB module version.

USB Devices

This feature display current USB device.

Legacy USB Support

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

XHCI Hand-off

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

Port 60/64 Emulation

Select Enabled for legacy I/O support for USB devices such as mice and keyboards. The options are **Enabled** and disabled. Default setting is **Enabled**.

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 **Disable** and Enable.

► Server ME (Management Engine) Information

This feature displays the following system ME configuration settings.

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

► PCH SATA Configuration

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

SATA Controller

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

Configure SATA as

Select IDE to configure a SATA drive specified by the user as an IDE drive. 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 Disable and **Enable**.

Aggressive Link Power Management

When this item is set to Enabled, 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 **Disabled** and Enabled.

**If the item "Configure SATA as" is set to RAID, the following items will be displayed:*

SATA RAID Option ROM/UEFI Driver

Use this feature to select the Raid Option ROM type. The options are Disable, EFI, and **Legacy**.

SATA Port 0 ~ Port 7

This item 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 item to Enabled for hot-plugging support, which will allow the user to replace a SATA drive without shutting down the system. The options are Disabled and **Enabled**.

Port 0 ~ Port 7 Spin Up Device

On an edge detect from 0 to 1, set this item to allow the PCH to initialize the device. The options are **Disabled** and Enabled.

Port 0 ~ Port 7 SATA Device Type

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

►PCH sSATA Configuration

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

sSATA Controller

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

SATA HDD Unlock

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

Aggressive Link Power Management

When this item is set to Enabled, 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 **Disabled** and Enabled.

sSATA Port 5

This item displays the information detected on the installed Solid State Drive (SSD) on the particular SATA port.

►PCI/PCI/PnP Configuration

The following information will be displayed:

- PCI Bus Driver Version
- PCI Devices Common Settings:

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

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

SR-IOV Support

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

MMIO High Base

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

MMIO High Granularity Size

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

Maximum Read Request

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

MMCFG Base

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



Note 1: The three items below are available when the device is detected by the system.

Note 2: The three items below display depending on the device being installed in and detected by the system.

RSC-T2R-884

RSC-T2R-884 SLOT1 PCI-E 3.0 X8 OPROM

Select Enabled to enable Option ROM support to boot the computer using a device installed on the slot specified by the user. The options are Disabled, Legacy and EFI. 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.

RSC-T2R-884 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.

M.2-H 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 **Enabled** and Disabled.

Onboard LAN Device

Select Enabled to enable the Onbaord LAN device. The options are Disabled and **Enabled**.

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, **Legacy**, and EFI.

Onboard LAN2 Option ROM

Use this feature to select which firmware function to be loaded for LAN Port2 used for system boot. The options are **Disabled**, Legacy, and EFI.

Onboard Video Option ROM

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

► Network Stack Configuration**Network Stack**

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

IPv4 PXE Support

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

IPv4 HTTP Support

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

IPv6 PXE Support

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

IPv6 HTTP Support

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

PXE Boot Wait Time

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

Media Detect Count

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

► Super IO Configuration

The following Super IO information will be displayed:

- Super IO Chip AST2500

► Serial Port 1 Configuration

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

Serial Port 1

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

Device Settings

This item 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=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

► SOL Configuration

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

SOL

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

Device Settings

This item displays the status of a serial port specified by the user.

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of 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=4;), (IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

SOL Attribute

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

► Serial Port Console Redirection

COM1

Console Redirection

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

**If the item above is set to Enabled, the following items will become available for user's configuration:*

► Console Redirection Settings

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

Terminal Type

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

Bits per second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

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

SOL

Console Redirection

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

► 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.

****If the item above is set to Enabled, the following items will become available for configuration:***

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Legacy OS Redirection Resolution

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

Putty KeyPad

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

Redirection After BIOS POST

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

Legacy Console Redirection**Legacy Serial Redirection Port**

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

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

The submenu allows the user to configure Console Redirection settings to support Out-of-Band Serial Port management.

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.

Console Redirection

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

****If the item above is set to Enabled, the following items will become available for configuration:***

► Console Redirection Settings

Out-of-Band Mgmt Port

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

Terminal Type

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

Bits Per Second

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

Flow Control

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

Data Bits: 8

Parity: None

Stop Bits: 1

► **ACPI Settings**

Numa

This setting enables or disables Non-Uniform Memory Access (NUMA), a feature that improves memory-to-processor communication and performance. The options are Disabled and **Enabled**.

WHEA Support

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

High Precision 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 Configuration (Available when a TPM device is installed and detected by the BIOS)**

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

- Security Device Support
- No Security Device Found

Security Device Support

If this feature and the TPM jumper (JPT1) on the motherboard are both enabled, the onboard security (TPM) device will be enabled in the BIOS to enhance data integrity and system security. Please note that the OS will not show the security device. Neither TCG EFI protocol nor INT1A interaction will be made available for use. If you have made changes on the setting on this item, be sure to reboot the system for the change to take effect. The options are Disable and **Enable**. If this option is set to Enable, the following screen and items will display:

Pending Operation

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



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

Platform Hierarchy (for TPM Version 2.0 and above)

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

Storage Hierarchy

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

Endorsement Hierarchy

Select Enabled for Endorsement Hierarchy support, which contains separate controls to address the user's privacy concerns because the primary keys in this hierarchy are certified by the TPM or a manufacturer to be constrained to an authentic TPM device that is attached to an authentic platform. A primary key can be an encrypted, and a certificate can be created using TPM2_ActivateCredential. It allows the user to independently enable "flag, policy, and authorization value" without involving other hierarchies. A user with privacy concerns can disable the endorsement hierarchy while still using the storage hierarchy for TPM applications and permitting the platform software to use the TPM. The options are **Enabled** and Disabled.

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

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

TXT Support

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



Note 1: If the option for this item (TXT Support) is set to Enabled, be sure to disable EV DFX (Device Function On-Hide) support for the system to work properly. (EV DFX is under "I/O Configuration" in the "Chipset/North Bridge" submenu).

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

► Intel(R) Virtual RAID on CPU

When this submenu is selected and the RAID devices are detected, the BIOS screen displays the following items:

Intel(R) VROC with VMD Technology 5.4.0.1039

► Intel(R) RSTe SATA Controller (Available when "Configure SATA as" is set to RAID and "SATA RAID option ROM/UEFI" is set to EFI)

Intel(R) RSTe 5.4.0.1039 SATA Driver

This feature displays RSTe Driver version.

► Intel(R) Ethernet Connection X722 for 1GbE - xx:xx:xx:xx:xx:xx (Available when "Onboard Lan option ROM" is set to EFI)

► NIC Configuration

Link Speed

This feature allows the user to specify the port speed used for the selected boot protocol. The options are **Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, and 100 Mbps Full.

Wake On LAN

Select Enabled for Wake_On_LAN support, which will allow the system to "wake up" when an onboard device receives an incoming signal. The options are Disabled and **Enabled**.

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. Use the keyboard to select a value.

UEFI Driver

This item displays the UEFI driver version.

Adapter PBA

This item displays the Processor Bus Adapter (PBA) model number. The PBA number is a nine digit number (i.e., 010B00-000) located near the serial number.

Device Name

This item displays the adapter device name.

Chip Type

This item displays the network adapter chipset name.

PCI Device ID

This item displays the device ID number.

PCI Address

This item displays the PCI address for this computer. PCI addresses are 3 two-digit hexadecimal numbers.

Link Status

This item displays the connection status.

MAC Address

This item displays the MAC address for this computer. Mac addresses are 6 two-digit hexadecimal numbers.

Virtual MAC Address

This item displays the Virtual MAC address for this computer. Mac addresses are 6 two-digit hexadecimal numbers.

►Driver Health

Intel(R) VROC with VMD Technology 5.4.0.1039 Healthy

Controller 678e4718 Child 0 Healthy

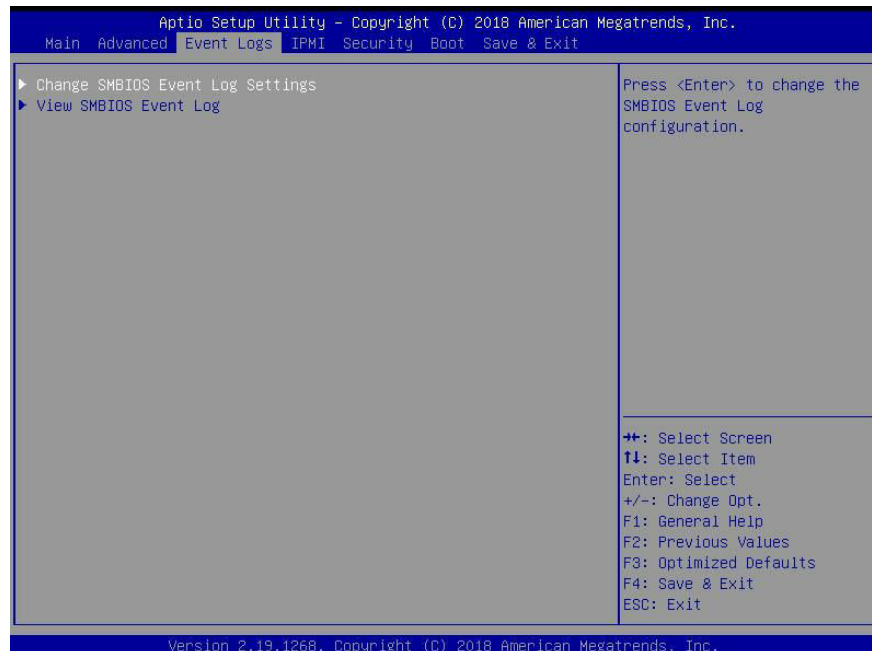
This item displays the information/status of driver installed in the system.

Apache Pass 1.0.0.1011 Driver Healthy

This item displays the information/status of driver installed in the system.

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

Erasing Settings

Erase Event Log

If No is selected, data stored in the event log 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 Long Standard Settings

Log System Boot Event

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

MECI

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

METW

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

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

►View SMBIOS Event Log

This section displays the contents of the SMBIOS Event Log.

4.5 IPMI

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



BMC Firmware Revision

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

IPMI STATUS (Baseboard Management Controller)

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

► System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

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

NOTE: 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

IPMI LAN Selection

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

IPMI Network Link Status

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

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

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**.

Station IP Address

This item displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 10.135.174.29).

Subnet Mask

This item 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 item displays the Station MAC address for this computer. Mac addresses are 6 two-digit hexadecimal numbers.

Gateway IP Address

This item displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 10.135.0.250).

VLAN

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

Configure IPV6 Support

This section displays configuration features for IPV6 support.

IPV6 address status

This section displays status of station IPV6 address to BMC. The default setting is Disabled.

IPV6 Support

Use this feature to enable IPV6 support. The options are **Enabled** and Disabled.

Configuration Address Source

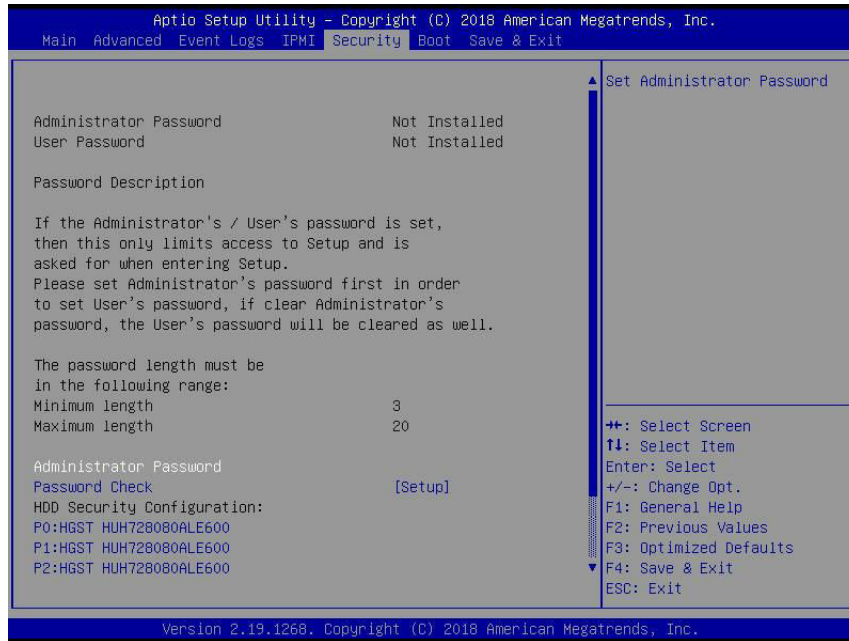
This feature allows the user to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol) 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 item "Configuration Address Source" is set to Static, the following items 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.

Administrator Password

Password Check

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

HDD Security Configuration:

P0:HGST HUH728080ALE600

P1:HGST HUH728080ALE600

P2:HGST HUH728080ALE600

P3:HGST HUH728080ALE600

P4:HGST HUH728080ALE600

P5:HGST HUH728080ALE600

► Secure Boot

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

- System Mode
- Secure Boot
- Vendor Keys

Secure Boot

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

Secure Boot Mode

Use this item 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 Disabled and **Enabled**.

► 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.

► Enroll all Factory Default keys

► Enroll Efi Image

► Save all Secure Boot variables

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 option is Set New.

► Key Exchange Keys

This feature allows the user to configure the settings of the Key Exchange Keys. The options are **Set New** and Append.

▶ **Authorized Signatures**

This feature allows the user to configure the settings of the Authorized Signatures. The options are **Set New** and Append.

▶ **Forbidden Signatures**

This feature allows the user to configure the settings of the Forbidden Signatures. The options are **Set New** and Append.

▶ **Authorized TimeStamps**

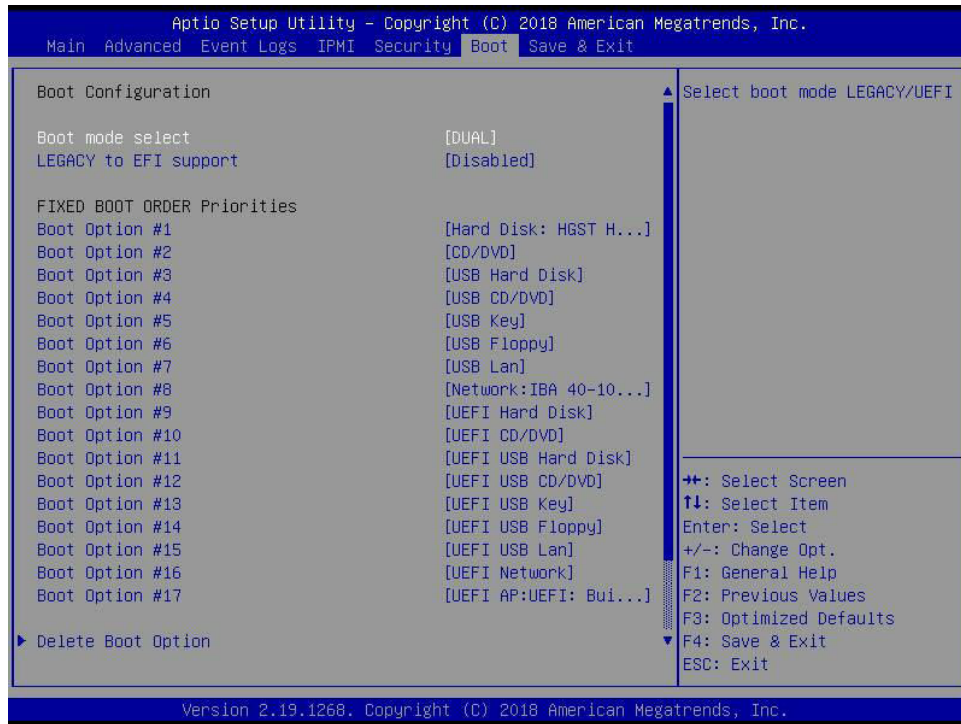
This feature allows the user to configure the settings of the authorized TimeStamps. The options are **Set New** and Append.

▶ **OsRecovery Signature**

This item uploads and installs an OSRecovery Signature. You may insert a factory default key or load from a file. The options are **Set New** and Append.

4.7 Boot

Use this feature to configure Boot Settings:



Boot Mode Select

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

Legacy to EFI Support

This feature enables the system to boot to EFI OS if boot fails from Legacy boot order. The options are **Disabled** and Enabled.

Fixed Boot Order Priorities

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

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

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

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

► Delete Boot Option

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

► UEFI Application Boot Priorities

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

Boot Option #1

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

► Hard Disk Drive BBS Priorities

UEFI Boot Option #1

The options are **ISATA P0:HGST HUH728080ALE600 (SATA,Port:0)**, ISATA P1:HGST HUH728080ALE600 (SATA,Port:1), ISATA P2:HGST HUH728080ALE600 (SATA,Port:2), ISATA P3:HGST HUH728080ALE600 (SATA,Port:3), ISATA P4:HGST HUH728080ALE600 (SATA,Port:4), ISATA P5:HGST HUH728080ALE600 (SATA,Port:5), and Disabled.

UEFI Boot Option #2

The options are ISATA P0:HGST HUH728080ALE600 (SATA,Port:0), **ISATA P1:HGST HUH728080ALE600 (SATA,Port:1)**, ISATA P2:HGST HUH728080ALE600 (SATA,Port:2), ISATA P3:HGST HUH728080ALE600 (SATA,Port:3), ISATA P4:HGST HUH728080ALE600 (SATA,Port:4), ISATA P5:HGST HUH728080ALE600 (SATA,Port:5), and Disabled.

UEFI Boot Option #3

The options are ISATA P0:HGST HUH728080ALE600 (SATA,Port:0), ISATA P1:HGST HUH728080ALE600 (SATA,Port:1), **ISATA P2:HGST HUH728080ALE600 (SATA,Port:2)**, ISATA P3:HGST HUH728080ALE600 (SATA,Port:3), ISATA P4:HGST HUH728080ALE600 (SATA,Port:4), ISATA P5:HGST HUH728080ALE600 (SATA,Port:5), and Disabled.

UEFI Boot Option #4

The options are ISATA P0:HGST HUH728080ALE600 (SATA,Port:0), ISATA P1:HGST HUH728080ALE600 (SATA,Port:1), ISATA P2:HGST HUH728080ALE600 (SATA,Port:2), **ISATA P3:HGST HUH728080ALE600 (SATA,Port:3)**, ISATA P4:HGST HUH728080ALE600 (SATA,Port:4), ISATA P5:HGST HUH728080ALE600 (SATA,Port:5), and Disabled.

UEFI Boot Option #5

The options are ISATA P0:HGST HUH728080ALE600 (SATA,Port:0), ISATA P1:HGST HUH728080ALE600 (SATA,Port:1), ISATA P2:HGST HUH728080ALE600 (SATA,Port:2), ISATA P3:HGST HUH728080ALE600 (SATA,Port:3), **ISATA P4:HGST HUH728080ALE600 (SATA,Port:4)**, ISATA P5:HGST HUH728080ALE600 (SATA,Port:5), and Disabled.

UEFI Boot Option #6

The options are ISATA P0:HGST HUH728080ALE600 (SATA,Port:0), ISATA P1:HGST HUH728080ALE600 (SATA,Port:1), ISATA P2:HGST HUH728080ALE600 (SATA,Port:2), ISATA P3:HGST HUH728080ALE600 (SATA,Port:3), ISATA P4:HGST HUH728080ALE600 (SATA,Port:4), **ISATA P5:HGST HUH728080ALE600 (SATA,Port:5)**, and Disabled.

► NETWORK Drive BBS Priorities

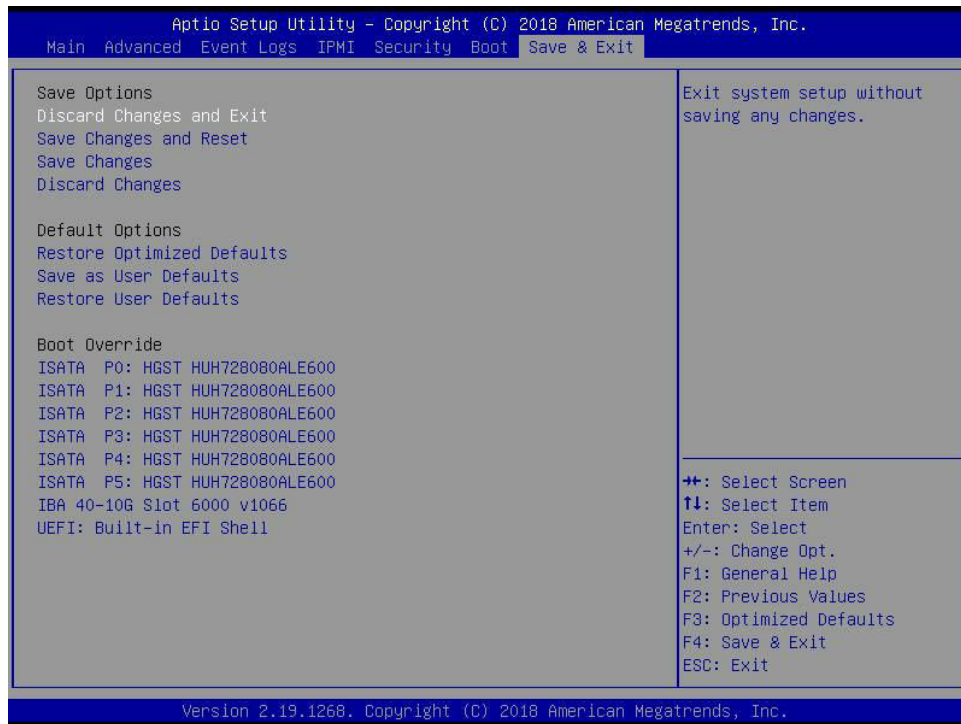
This feature allows the user to specify which UEFI network drive devices are boot devices.

Boot Option #1

The options are **IBA 40-10G Slot 6000 v1066** and Disabled.

4.8 Save & Exit

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



Save Options

Discard Changes and Exit

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

Save Changes and Reset

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

Save Changes

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

Discard Changes

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

Default Options

Restore Optimized Defaults

To set this feature, select Restore 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.

- ISATA P0: HGST HUH728080ALE600
- ISATA P1: HGST HUH728080ALE600
- ISATA P2: HGST HUH728080ALE600
- ISATA P3: HGST HUH728080ALE600
- ISATA P4: HGST HUH728080ALE600
- ISATA P5: HGST HUH728080ALE600
- IBA 40-10G Slot 6000 v1066
- UEFI: Built-in EFI Shell

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 Installation


B.1 Installing Software Programs

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

After accessing the product drivers and utilities page, go into the CDR_Images directory and locate the ISO file for your motherboard. Download this file to create a DVD of the drivers and utilities it contains. (You may also use a utility to extract the ISO file if preferred.)

After creating a DVD with the ISO files, insert the disk into the DVD drive on your system and the display shown in Figure B-1 should appear.

Another option is to go to the Supermicro website at <http://www.supermicro.com/products/>. Find the product page for your motherboard here, where you may download individual drivers and utilities to your hard drive or a USB flash drive and install from there.

 **Note:** Please refer to the documents posted on our website at <http://www.supermicro.com/support/manuals/> for additional instructions that may be applicable to your system.

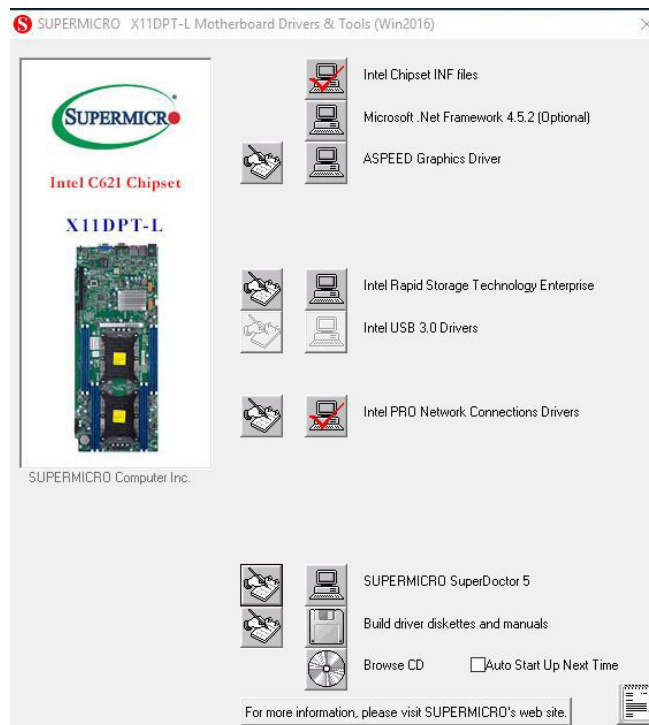


Figure B-1. Driver/Tool Installation Display Screen

Click the icons showing a hand writing on the paper to view the readme files for each item. Click a computer icon to the right of an item to install an item (from top to the bottom) one at a time. After installing each item, you must reboot the system before proceeding with the next item on the list. The bottom icon with a DVD on it allows you to view the entire contents of the DVD.

When making a storage driver diskette by booting into a driver DVD, please set the SATA Configuration to "Compatible Mode" and configure SATA as IDE in the BIOS Setup. After making the driver diskette, be sure to change the SATA settings back to your original settings.

B.2 SuperDoctor® 5

The Supermicro SuperDoctor 5 is a hardware monitoring program that functions in a command-line or web-based interface in Windows and Linux operating systems. The program monitors system health information such 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. SD5 Management Server monitors HTTP and SMTP services to optimize the efficiency of your operation.



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

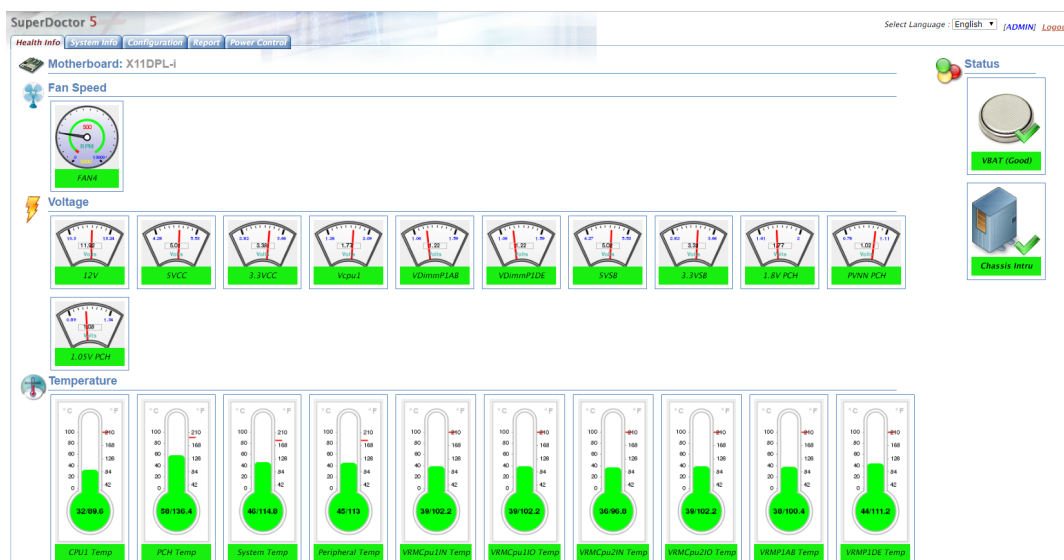


Figure B-2. SuperDoctor 5 Interface Display Screen (Health Information)



Note: The SuperDoctor 5 program and user's manual can be downloaded from the Supermicro website at http://www.supermicro.com/products/nfo/sms_sd5.cfm.

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

電池更換不當會有爆炸危險。請只使用同類電池或制造商推薦的功能相當的電池更換原有電池。請按製造商的說明處理廢舊電池。

警告

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

Warnung

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

Attention

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

¡Advertencia!

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

אזהרה!

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

هناك خطر من انفجار في حالة اسبدال البطارية بطريقة غير صحيحة فعلياً
اسبدال البطارية
فقط بنفس النوع أو ما يعادلها مما أوصت به الشركة المصنعة
جخلص من البطاريات المسحمة وفقاً لتعليمات الشركة الصانعة

경고!

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

Waarschuwing

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

Product Disposal



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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

التخلص النهائي من هذا المنتج ينبغي التعامل معه وفقا لجميع القوانين واللوائح الوطنية عند

경고!

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

Waarschuwing

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

Appendix D

UEFI BIOS Recovery

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

D.1 Overview

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

D.2 Recovering the UEFI BIOS Image

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

Note 2: When the BIOS recovery block crashes, you will need to follow the procedures to make a Returned Merchandise Authorization (RMA) request. (For a RMA request, please see section 3.5 for more information). Also, you may use the Supermicro Update Manager (SUM) Out-of-Band (OOB) (https://www.supermicro.com.tw/products/nfo/SMS_SUM.cfm) to reflash the BIOS.


D.3 Recovering the 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 device can be used for this purpose. However, a USB Hard Disk drive cannot be used for BIOS recovery at this time.

The file system supported by the recovery block is FAT (including FAT12, FAT16, and FAT32) which is installed on a bootable or non-bootable USB-attached device. However, the BIOS might need several minutes to locate the SUPER.ROM file if the media size becomes too large due to the huge volumes of folders and files stored in the device.

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

1. Using a different machine, copy the "Super.ROM" binary image file into the Root "\ " directory of a USB device or a writable CD/DVD.


 **Notes:** **1.** If you cannot locate the "Super.ROM" file in your drive disk, visit our website at www.supermicro.com to download the BIOS package. Extract the BIOS binary image into a USB flash device and rename it "Super.ROM" for the BIOS recovery use. **2.** Before recovering the main BIOS image, confirm that the "Super.ROM" binary image file you download is the same version or a close version meant for your motherboard.

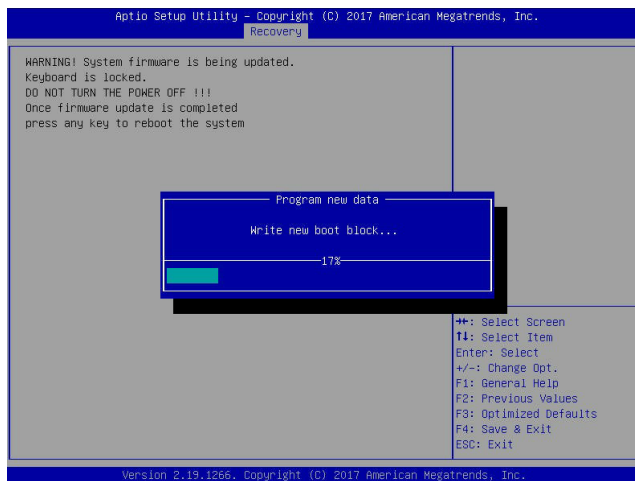


2. Insert the USB device that contains the new BIOS image ("Super.ROM") into your USB drive and reset the system when the following screen appears.

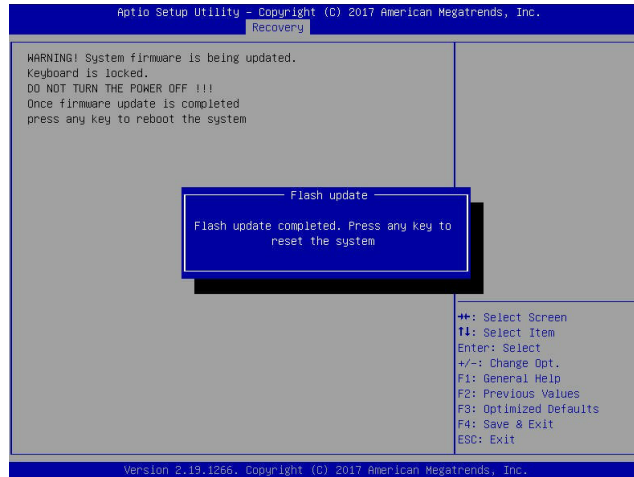


3. After locating the healthy BIOS binary image, the system will enter the BIOS Recovery menu as shown below.

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

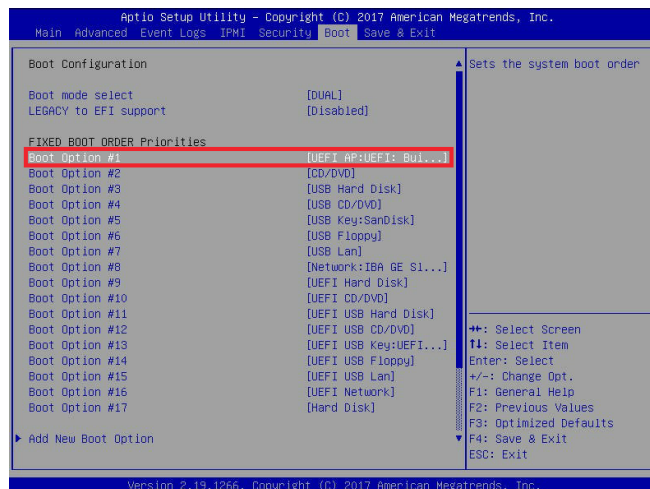


- When the screen as shown above displays, use the arrow keys to select the item "Proceed with flash update" and press the <Enter> key. You will see the BIOS recovery progress as shown in the screen below.



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

- After the BIOS recovery process is complete, press any key to reboot the system.
- Using a different system, extract the BIOS package into a USB flash drive.
- Press during system boot to enter the BIOS Setup utility. From the top of the toolbar, 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.



- When the UEFI Shell prompt appears, type `fs#` to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 6. Enter `flash.nsh BIOSname.###` at the prompt to start the BIOS update process.

```

UEFI Interactive Shell v2.1
EDK II
UEFI v2.50 (American Megatrends, 0x0005000C)
Mapping Table
  FS0: Alias(s):HD0:0:0:BLK1:
        PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)/HD(1,MBR,0x37901D72,0x800,0x1
DR959C)
  BLK0: Alias(s):
        PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)
Press F8 in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> cd \AFUDOS
FS0:\AFUDOS> cd \SNIPME2_03162017
FS0:\AFUDOS\SNIPME2_03162017> flash.nsh X110PU7_314

```



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

```

Done.
[ Access Cmos Part Ex ]
<Read>
Index 0x51: 0x10

Done.
*****
* Program BIOS and ME (including FDT) regions...
*****
| AMT Firmware Update Utility v5.09.01.1917
| Copyright (C)2017 American Megatrends Inc. All Rights Reserved.
|-----|
CPUID = 50652

Reading flash ..... done
- ME Data Size checking - ok
- FFS checksums ..... ok
- Check RomLayout ..... Ok
Erasing Boot Block ..... done
Updating Boot Block ..... done
Verifying Boot Block ..... done
Erasing Main Block ..... 0x00132000 (0x)

```

- The screen above indicates that the BIOS update process is complete. When you see the screen above, unplug the AC power cable from the power supply, clear CMOS, and plug the AC power cable in the power supply again to power on the system.

```

Verifying NDB Block ..... done
- Update success for FDR
- Update success for IE
- Successful Update Recovery Loader to OPRx!!
- Successful Update MFSB!!
- Successful Update FPR!!
- Successful Update MFS, IVBI and IVB2!!
- Successful Update FLOG and UTDK!!
- ME Entire Image update success !!
WARNING : System must power-off to have the changes take effect!
Moving FS0:\AFUDOS\SNIPME2_03162017\Fdtv64.efi -> FS0:\AFUDOS\SNIPME2_03162017\F
dt1.smc
- [ok]
Moving FS0:\AFUDOS\SNIPME2_03162017\Fuef1x64.efi -> FS0:\AFUDOS\SNIPME2_0316201
7\Fuef1.smc
- [ok]
*****
* Please ignore this 'Shell: Cannot read from file - Device Error'
* warning message due to it does not impact flashing process.
*****
Deleting "FS0:\uefiprom"
Delete successful.
FS0:\>

```

- Press `` to enter the BIOS Setup utility.
- Press `<F3>` to load the default settings.
- After loading the default settings, press `<F4>` to save the settings and exit the BIOS Setup utility.

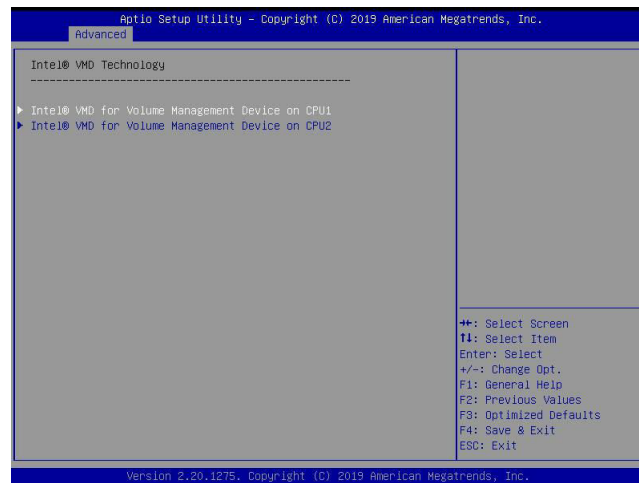
Appendix E

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 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/>.

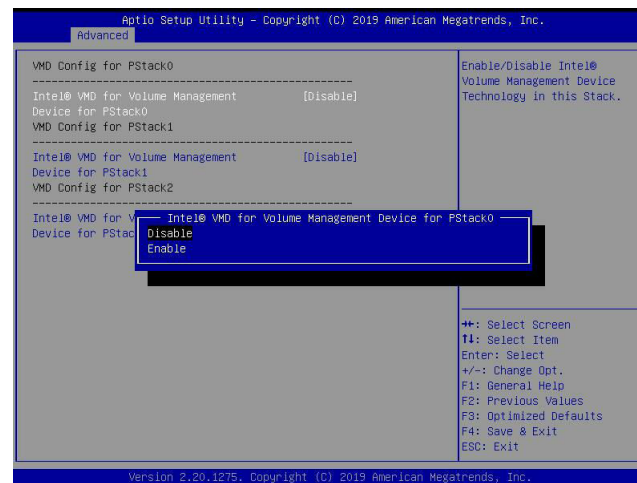
Note 2: Depending on the version of driver/utility/package, it may or may not have exactly the same as the BIOS settings/features shown in the appendix.

The following screen will appear.

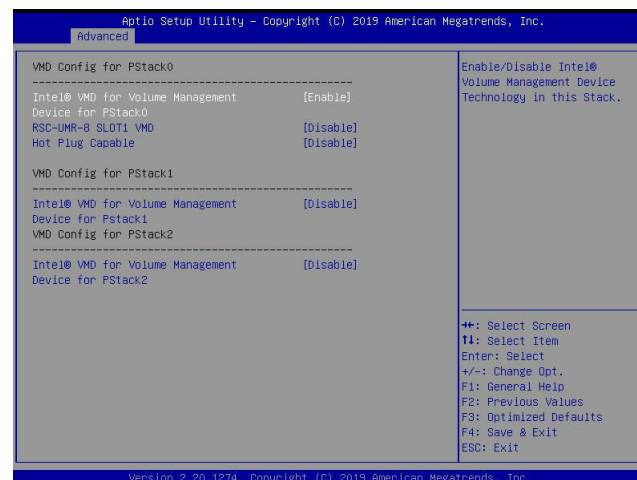


Step 2. Intel® VMD for Volume Management Device for PStack0

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

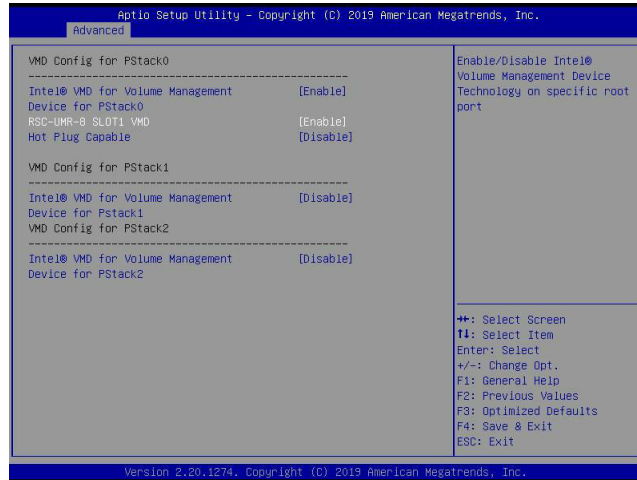
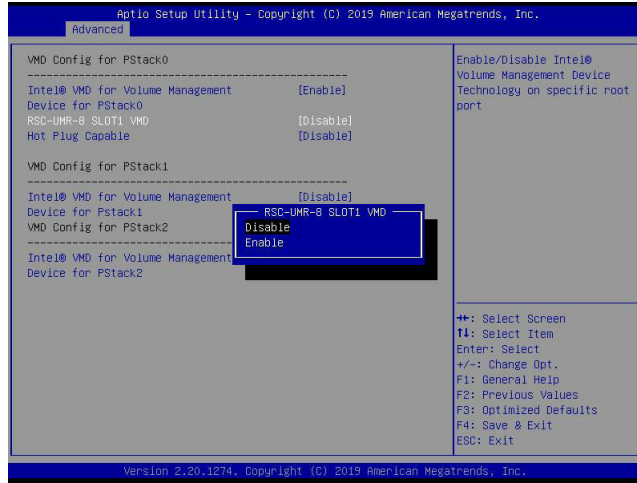


Press <Enter> and the following screen will appear.



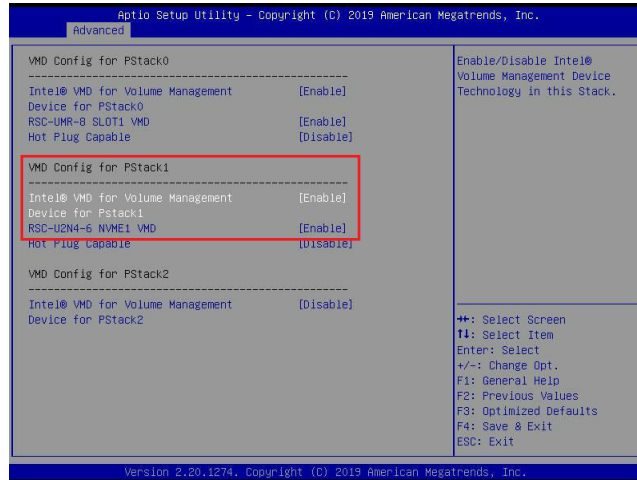
Step 3. RSC-UMR-8 SLOT1 VMD

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**.



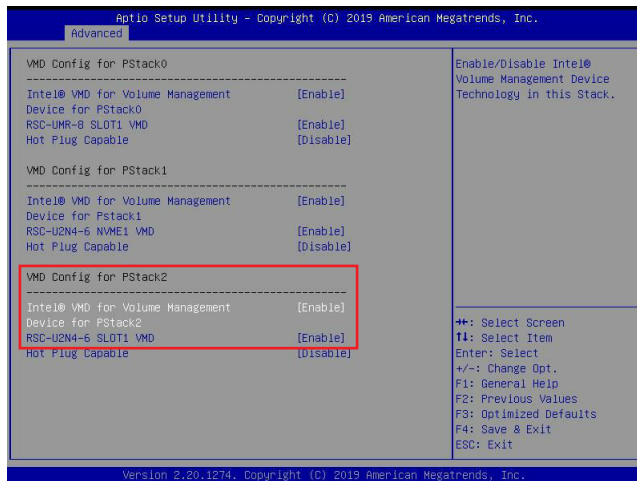
Step 4. Intel® VMD for Volume Management Device for PStack1, RSC-U2N4-6 NVME1 VMD

The options are **Disable** and Enable. Set the two features to Enable. (Refer to pages 117 and 118 for more information.)

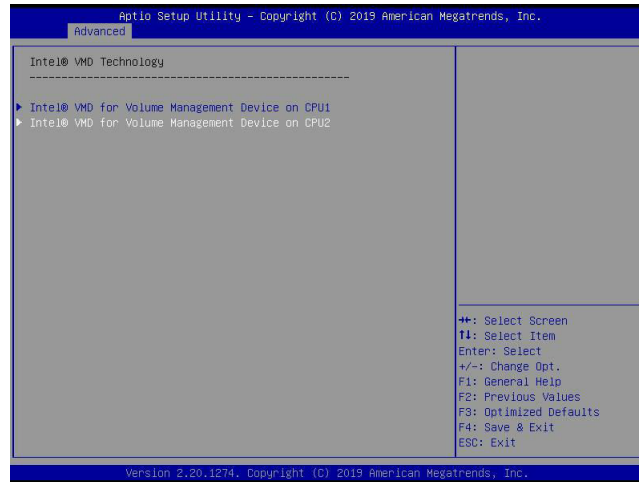


Step 5. Intel® VMD for Volume Management Device for PStack2, RSC-U2N4-6 SLOT1 VMD

The options are **Disable** and Enable. Set the two features to Enable. (Refer to pages 117 and 118 for more information.)

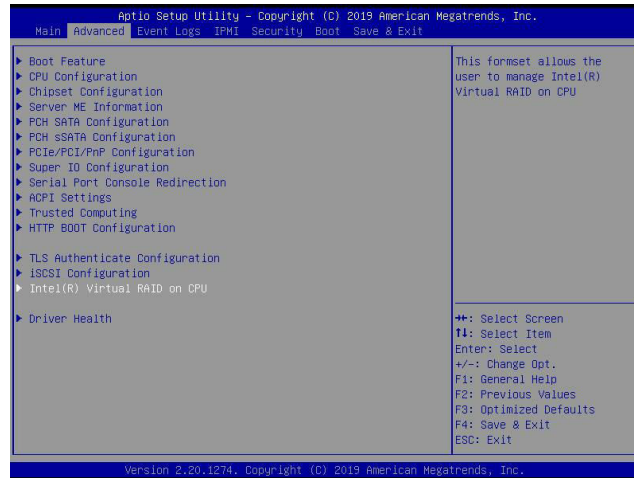


Press <Esc> and return to the main screen of Intel® VMD Technology as shown below. Use the arrow keys to select Intel® VMD for Volume Management Device on CPU2 and press <Enter> to access the menu items.

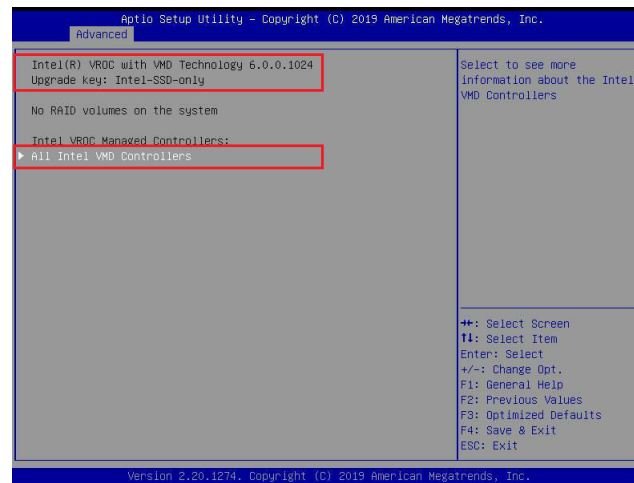


Repeat the steps (Step 1 ~ Step 5) on pages 116, 117, 118, and 119 to enable Intel® VMD for Volume Management Device for PStack0/PStack1/PStack2 and devices attached to the Intel® VMD controllers. For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press during system boot to enter the BIOS Setup utility.

Navigate to the Advanced tab.



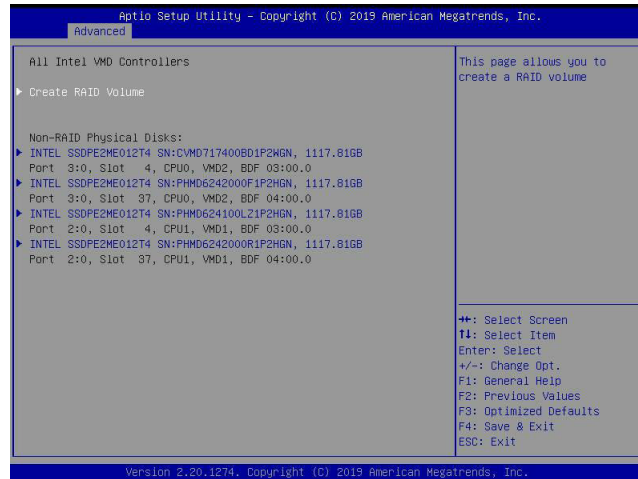
Use the arrow keys to select Intel(R) Virtual RAID on CPU and press <Enter> to access the menu items. The following screen will appear and the All Intel VMD Controllers feature has become available.



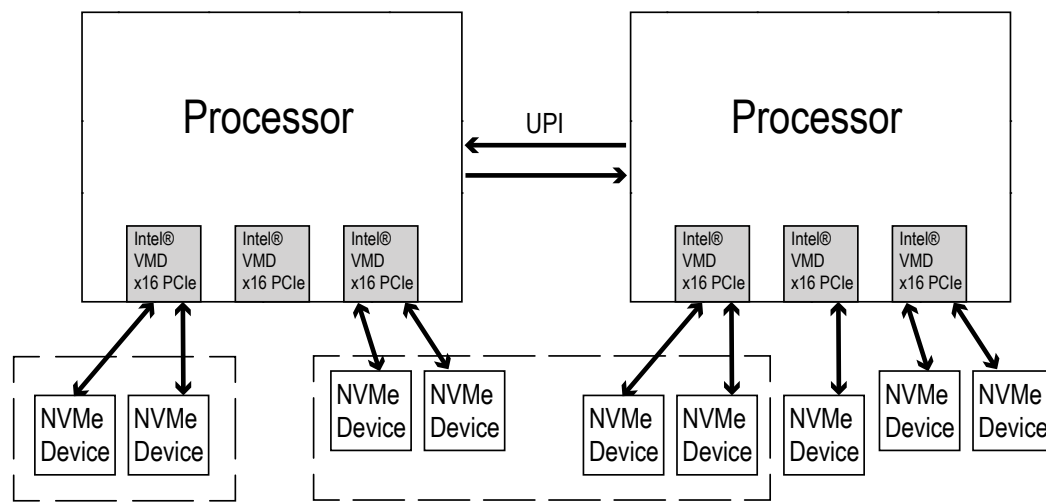
Note 1: The license and header (on the motherboard) for Intel® VROC hardware key are required. Also, be sure the version of Intel® Rapid Storage Technology enterprise (Intel® RSTe) VROC utility is 5 or above (look for Intel(R) VROC with VMD Technology x.x.x.xxxx shown on the screen).

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.

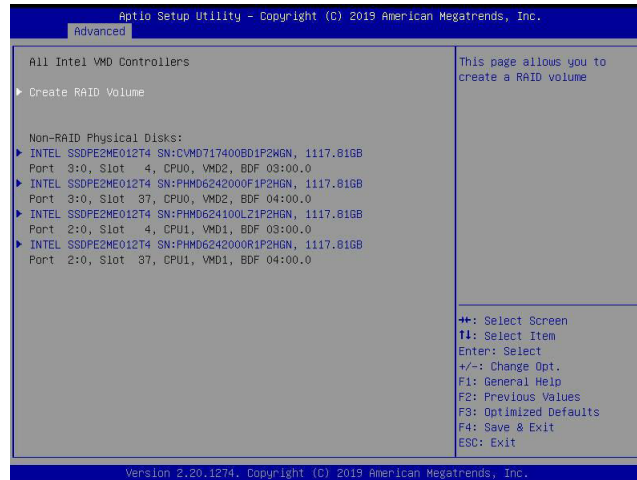


* Boot RAID will NOT be able to cross VMDs.

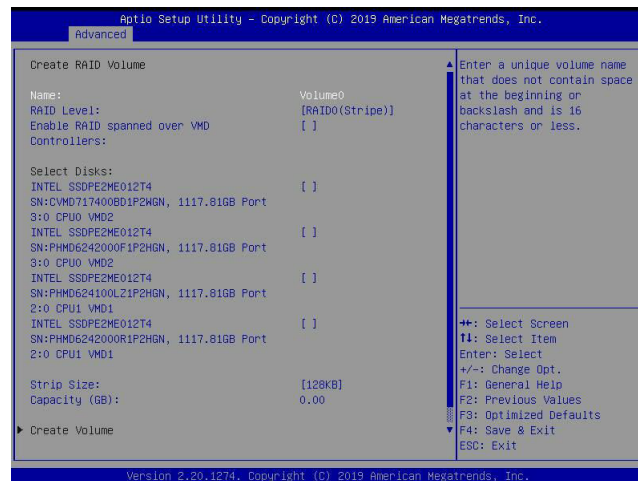
* Data RAID will be allowed to cross VMDs and processors.

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).

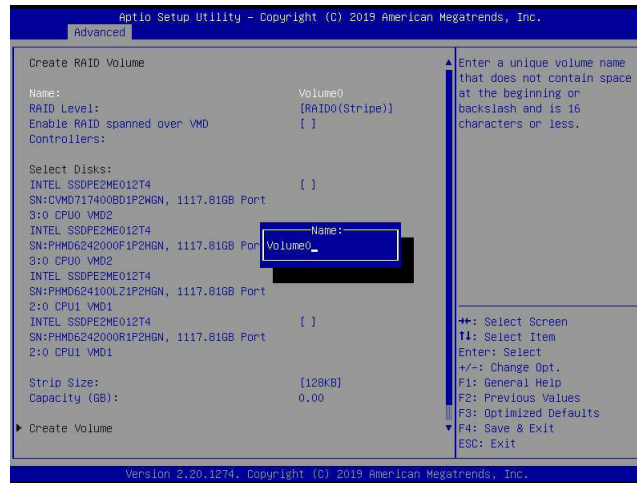


Step 1. To create RAID volume(s), use the arrow keys to select Create RAID Volume and press <Enter>. The following screen will appear.



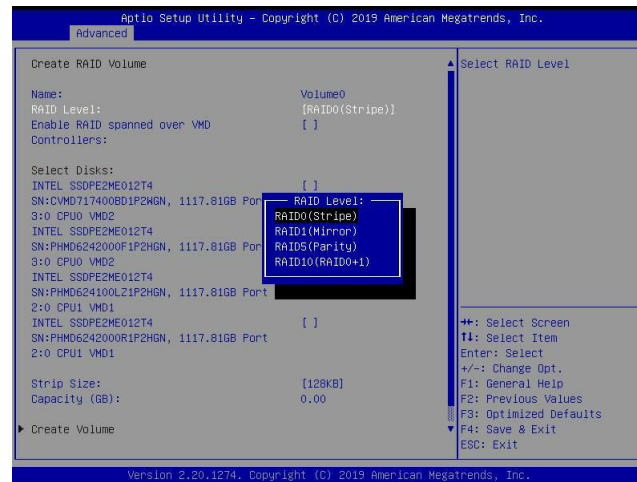
Step 2. Name:

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)**.

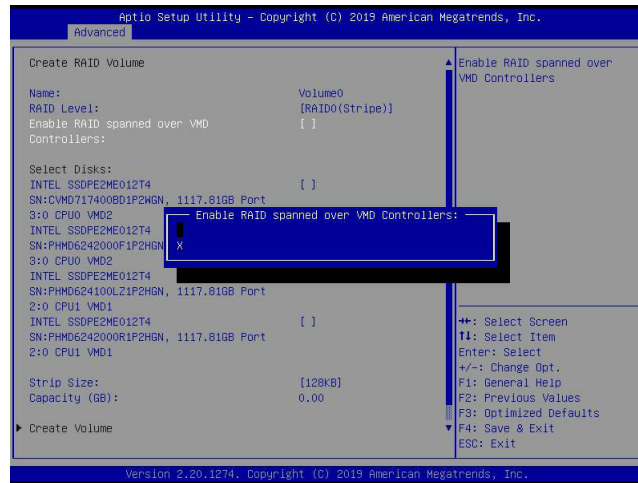



Note 1: The RAID level(s) displayed is(are) based on the number of NVMe devices connected to the system.

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

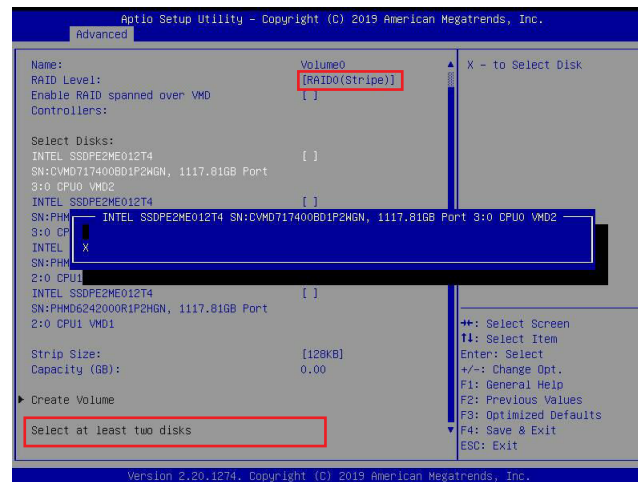
The options are **(not selected)** and X (selected). Set this feature to X if the RAID level you selected earlier from Step 3 will cross VMD domains.




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

Step 5. Select Disks:

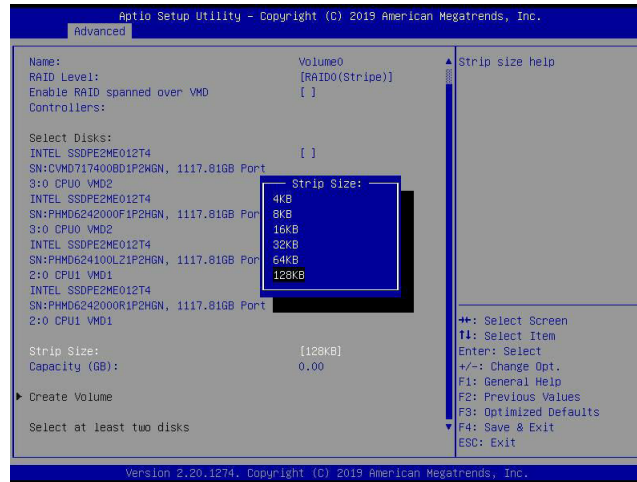
The options are **(not selected)** and X (selected). Set the features one by one to X to select the desired RAID disks.




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

Step 6. Strip Size:

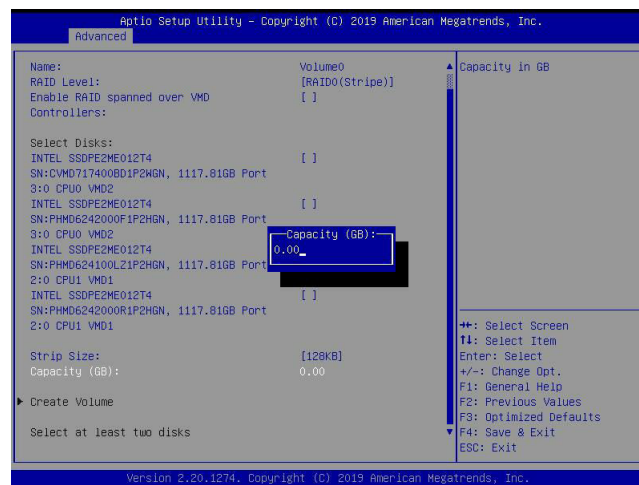
Use this feature to select the RAID strip size. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**.



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

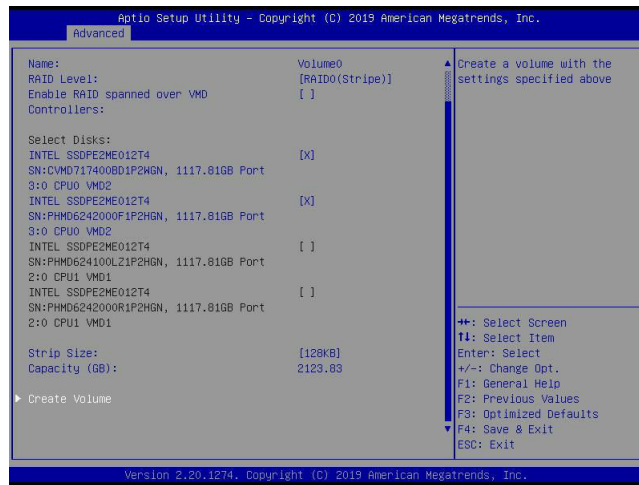
Step 7. Capacity (GB):

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

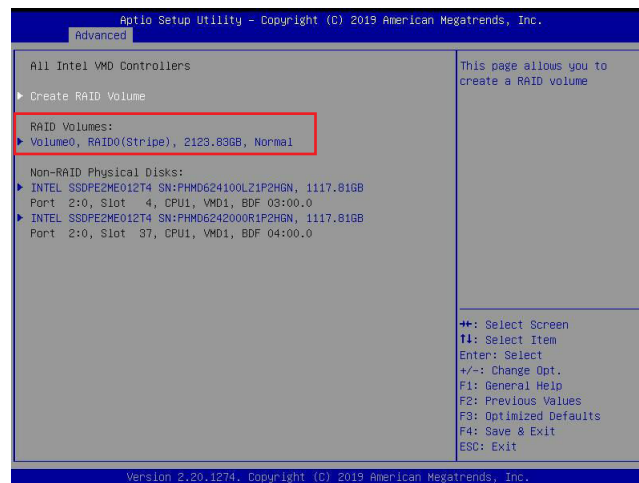


Step 8. Create Volume

Use the arrow keys to select Create Volume.

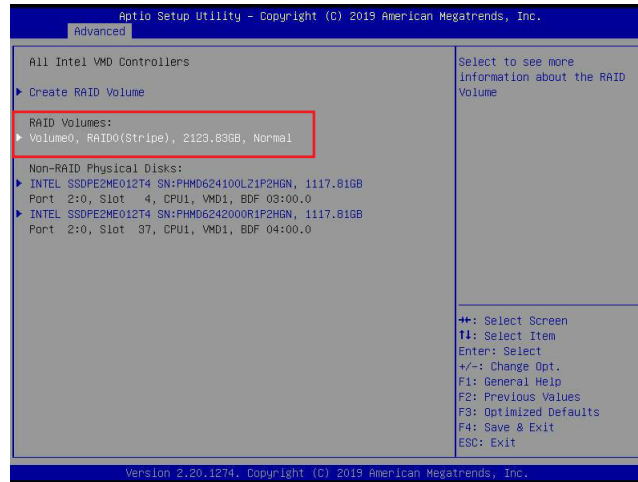


This feature is to create a RAID level with settings shown on the screen. Press <Enter> and the following screen will appear. It displays all RAID volumes.



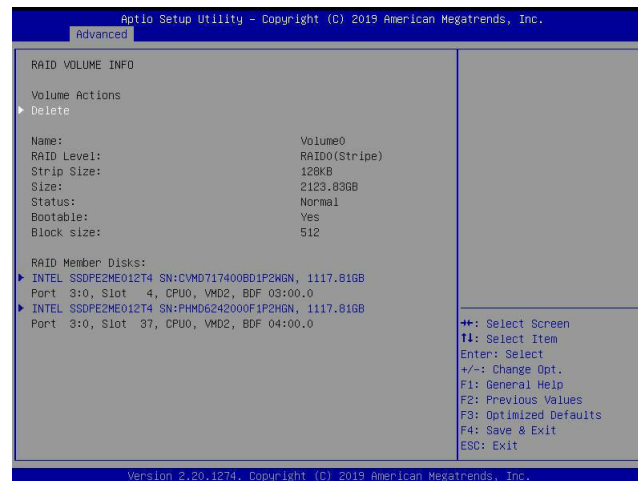
RAID Volumes:

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



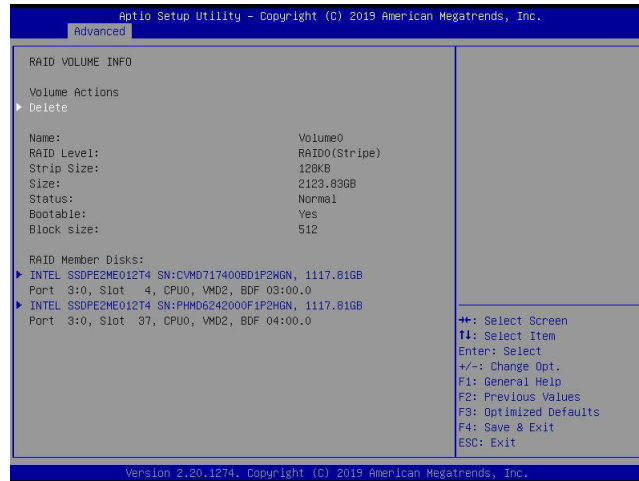
RAID VOLUME INFO

Press <Enter> and the following screen will appear.

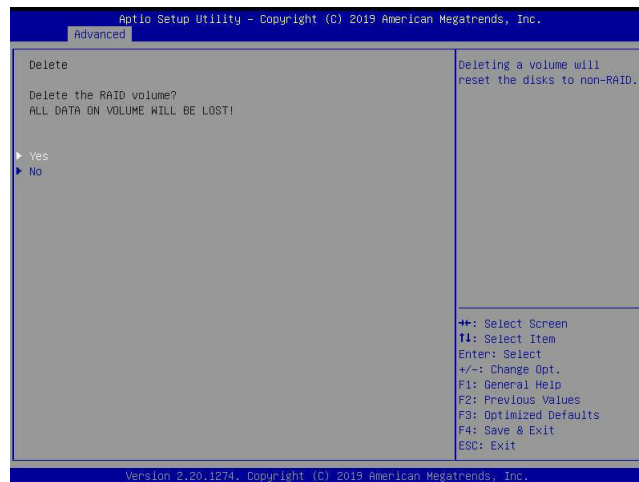


Delete

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).

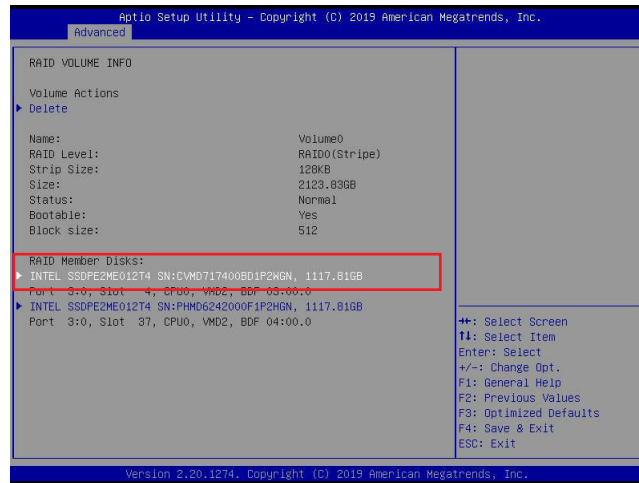


The following screen will appear. The options are **Yes** and **No**.

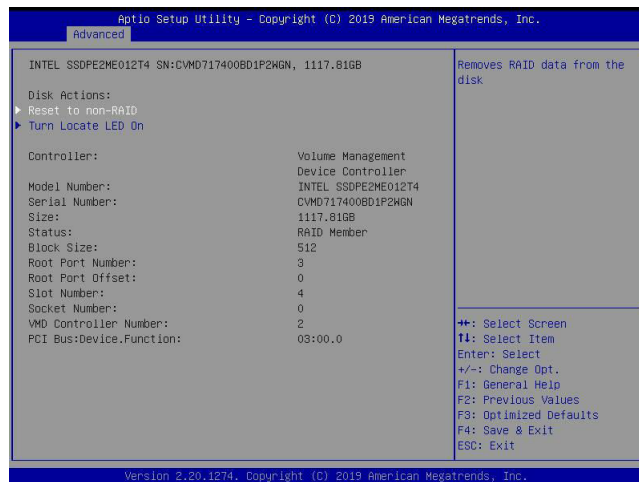


Reset to non-RAID

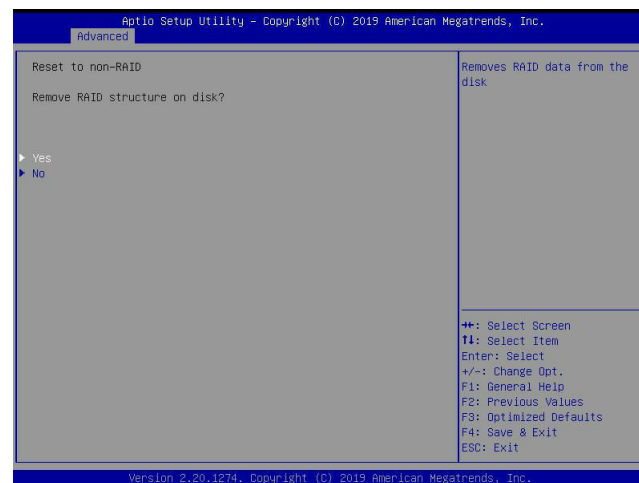
On the RAID VOLUME INFO screen (see page 128 for more information), select the desired NVMe device from the list of RAID Member Disks.



Press <Enter> and the following screen will appear.

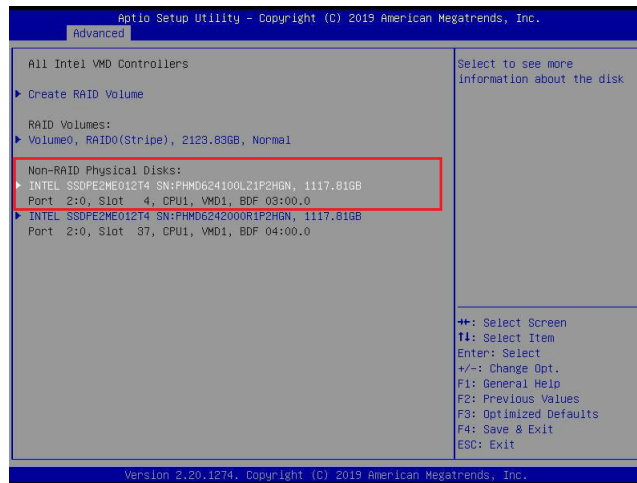


The feature, Reset to non-RAID, allows the user to remove RAID data from the selected NVMe device. Press <Enter> and the following screen will appear. The options are **Yes** and **No**.

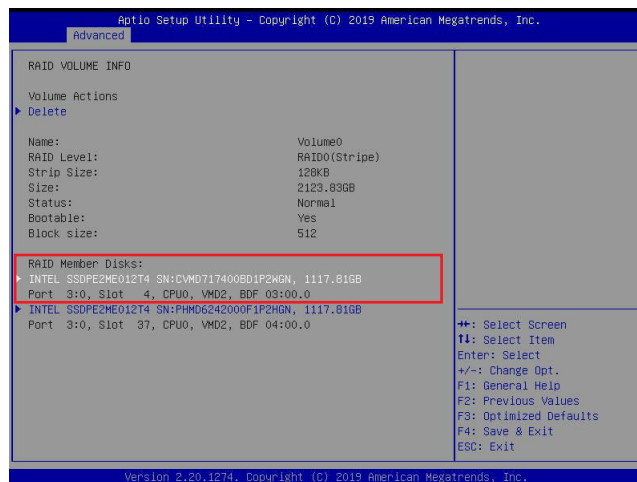


Turn Locate LED On

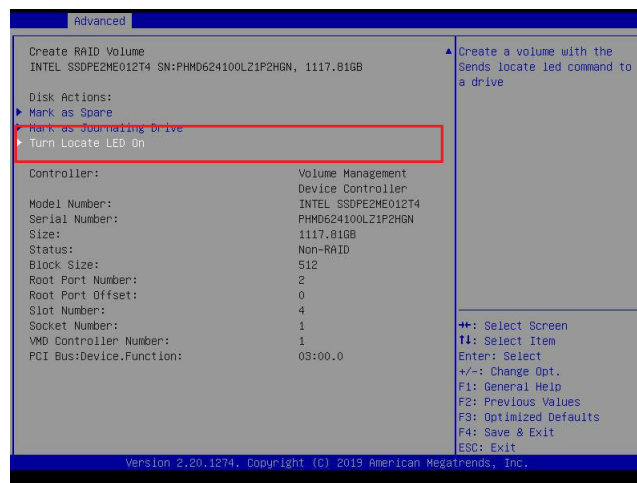
Use this feature to locate the selected device.
Select a non-RAID physical disk.



Or select a RAID member disk.

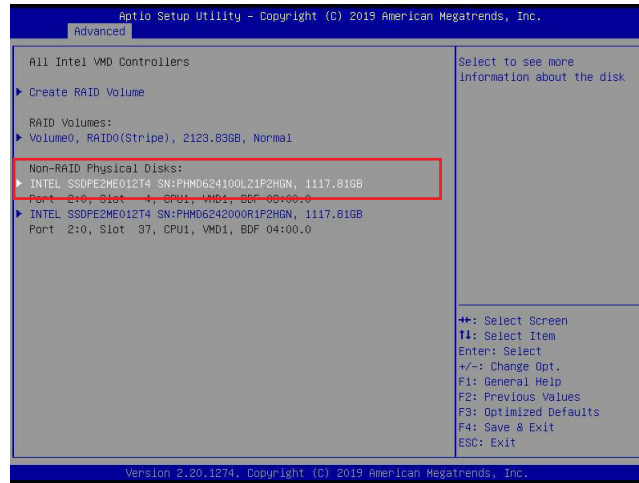


When the following screen appears, use the arrow keys to select Turn Locate LED On. Press <Enter> to locate the selected device.

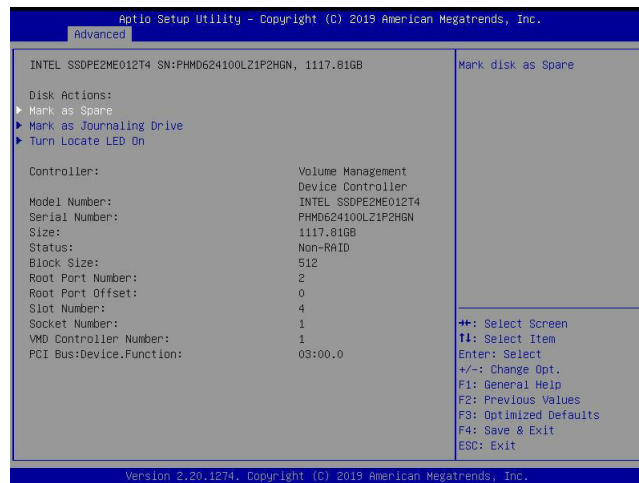


Mark as Spare

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.



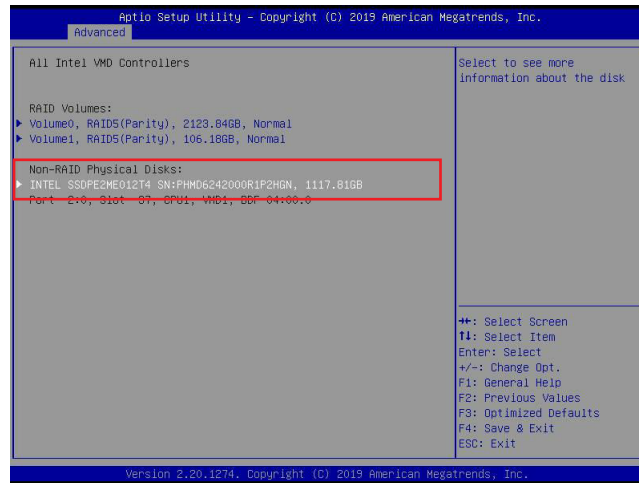
The feature, Mark as Spare, allows the user to set the selected NVMe device as a spare disk. Use the arrow keys to select Mark as Spare and press <Enter>. The following screen will appear. The options are **Yes** and No.



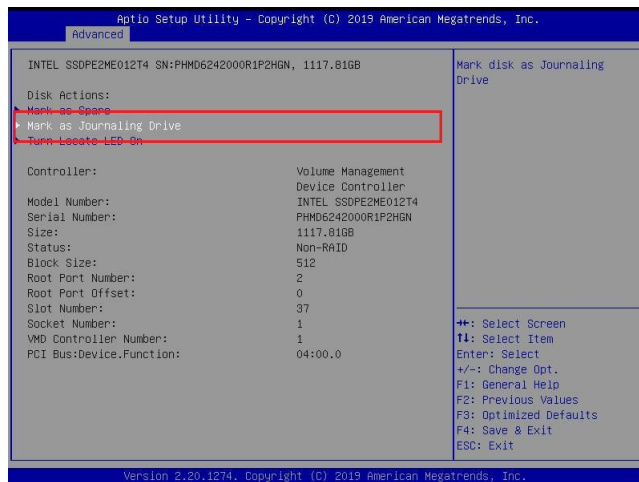
 **Note:** A spare disk is used for automatic RAID volume rebuilds when status of failed, missing, or at risk is detected on the array disk. For a RAID0 volume, only status of at risk will trigger automatic RAID volume rebuilds.

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.



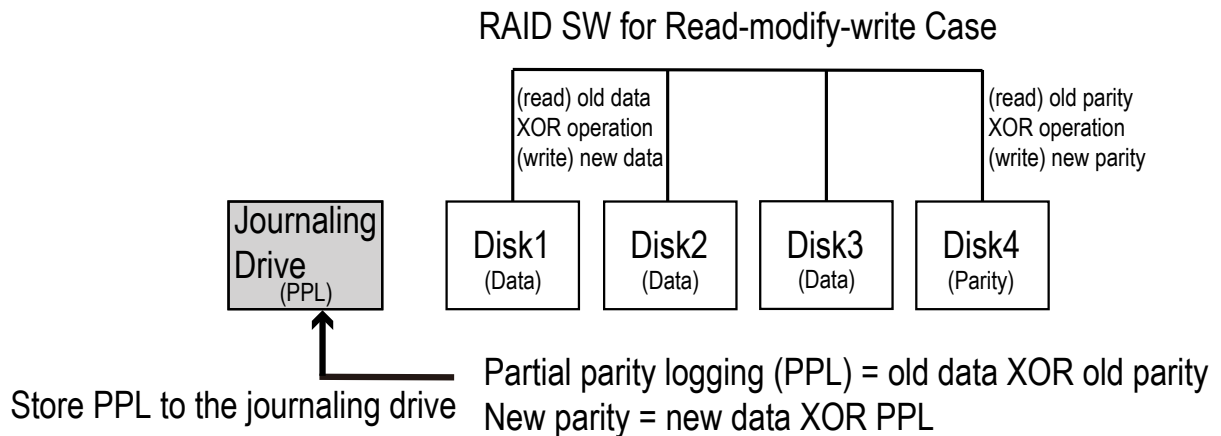
Press <Enter> and the following screen will appear.



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.



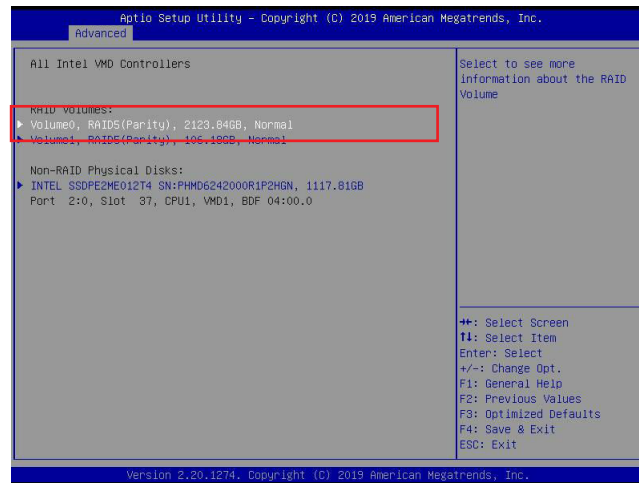
Note: RAID Write Hole (RWH) is a condition associated with a power/drive-failure/crash while writing to a RAID5 volume. The use of journaling drive that contains partial parity logging (PPL) can reduce the potential data loss. Refer to the following illustration for the use of journaling drive.



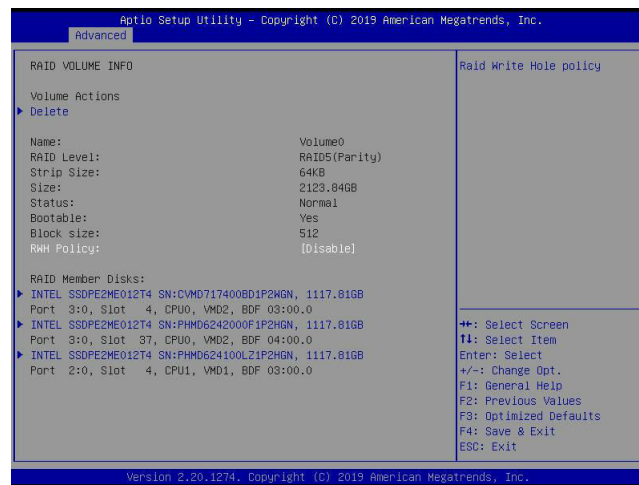
E.3 Use of Journaling Drive

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.



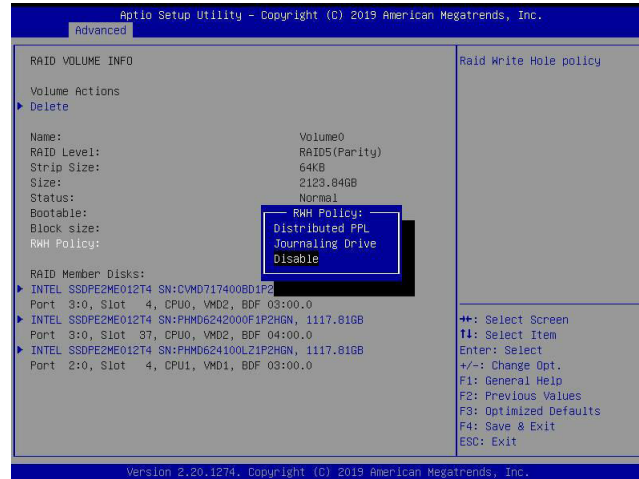
Press <Enter> and the following screen will appear.



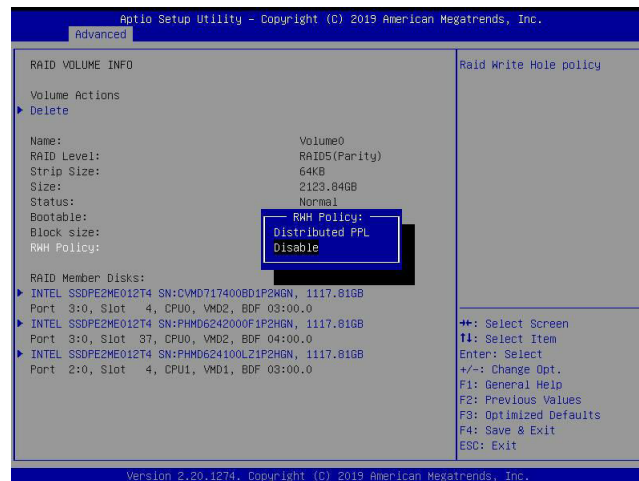
Step 2. Use the arrow keys to select RW Policy. RW Policy is a scenario related to a power/drive-failure/crash.

RWH Policy

Press <Enter> and the following screen will appear. If any device has been set as a journaling drive (see pages 134 and 135), the options are Distributed PPL, Journaling Drive, and Disable.



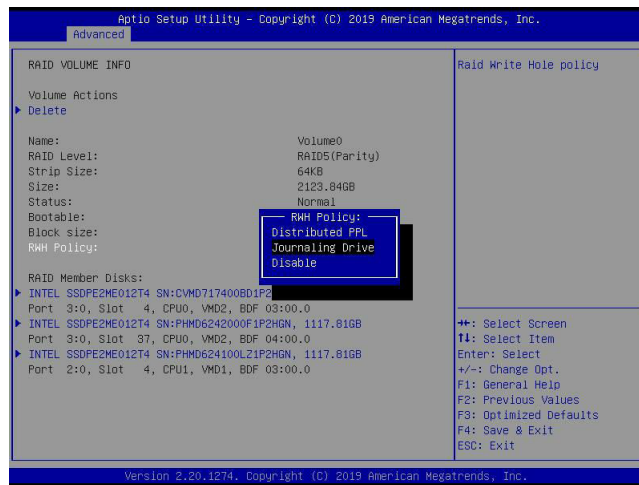
If no device has been set as a journaling drive, the options are Distributed PPL and **Disable**.



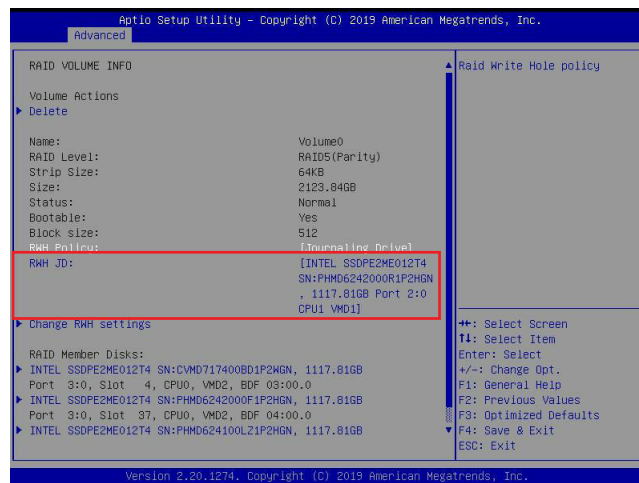
Note 1: Partial parity logging (PPL) can be defined as the result of XOR calculation of old data and old parity. PPL is a feature available for RAID5 volumes. While a power/drive-failure/crash occurring, PPL information helps rebuild the RAID volume and reduce the potential data loss.

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.

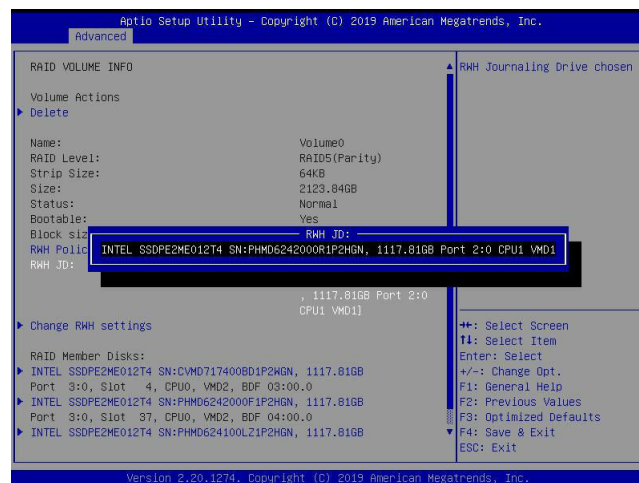


Press <Enter> and the RWH JD feature will become available as shown below.



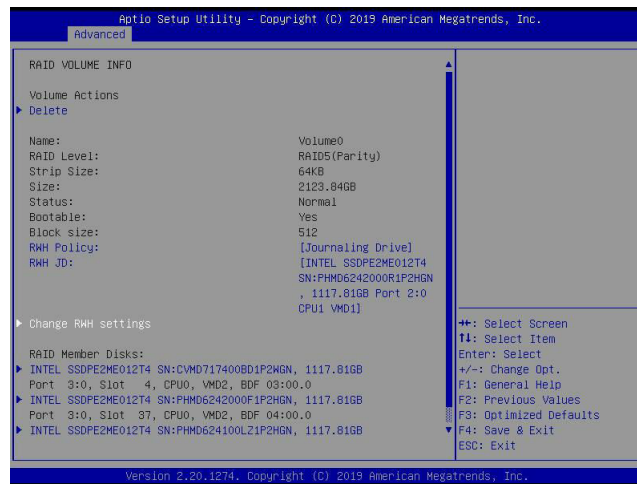
RWH JD

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).

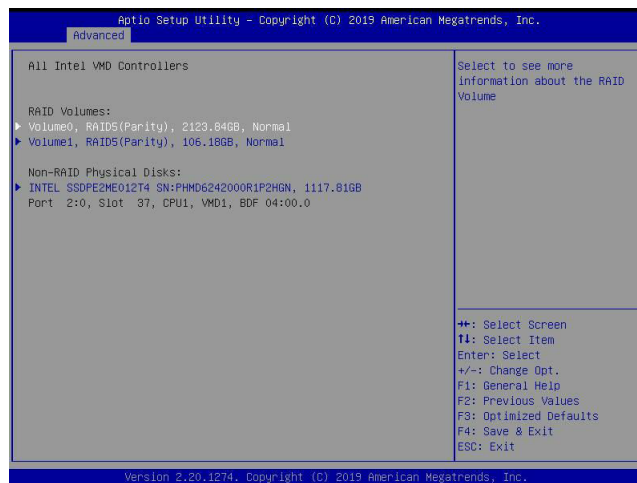


Step 4. Use the arrow keys and press <Enter> to select the desired journaling drive from the option list of RWH JD.

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.



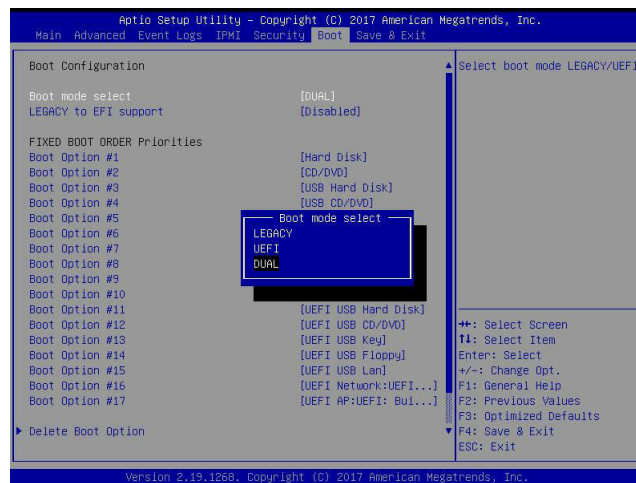
Appendix F

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.

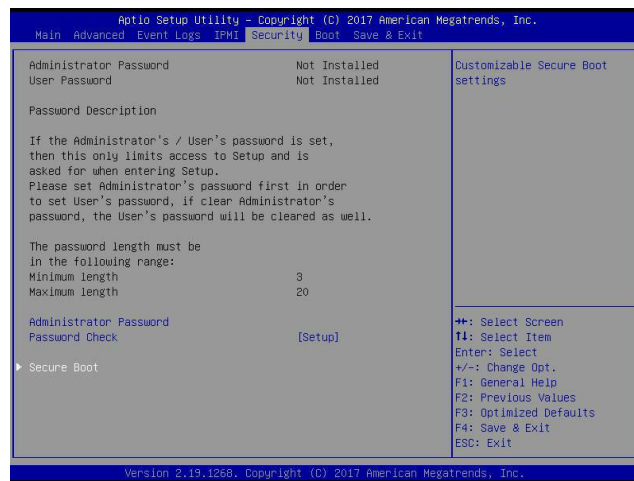
F.1 Boot mode select Feature

Press 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.

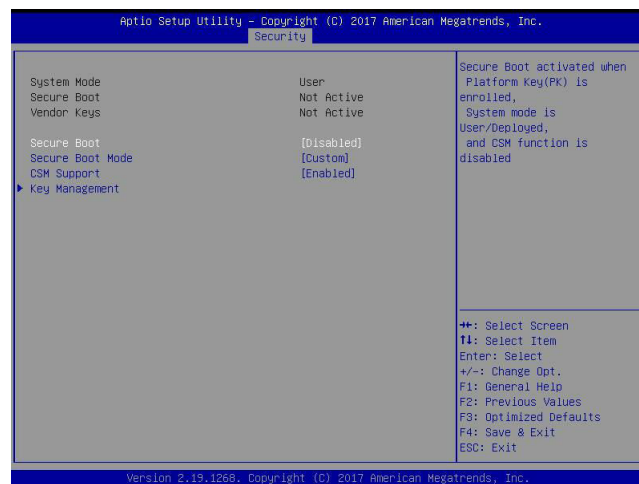


F.2 Secure Boot/ Secure Boot Mode/ CSM Support Features

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



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



Secure Boot

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

Secure Boot Mode

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

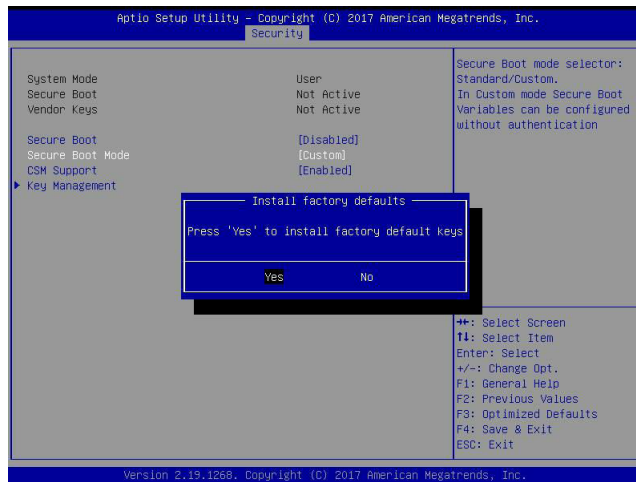
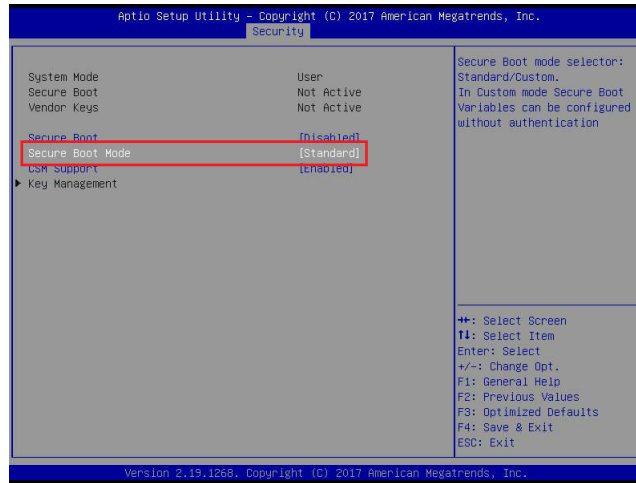
CSM Support


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

F.3 Secure Boot Settings

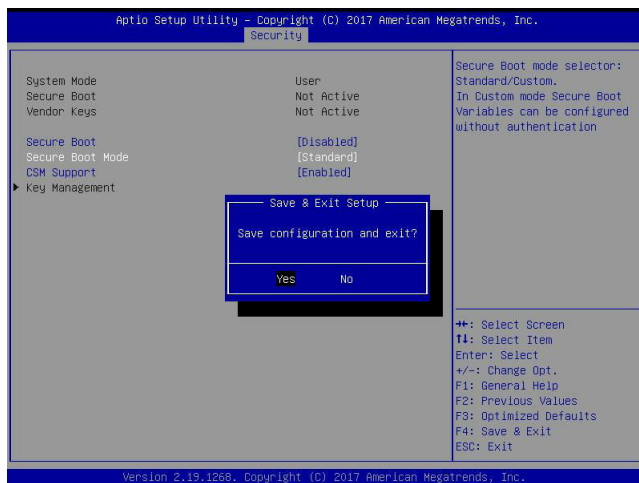
To have the secure boot support, be sure to follow the steps below (Step 1 ~ Step 4).

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

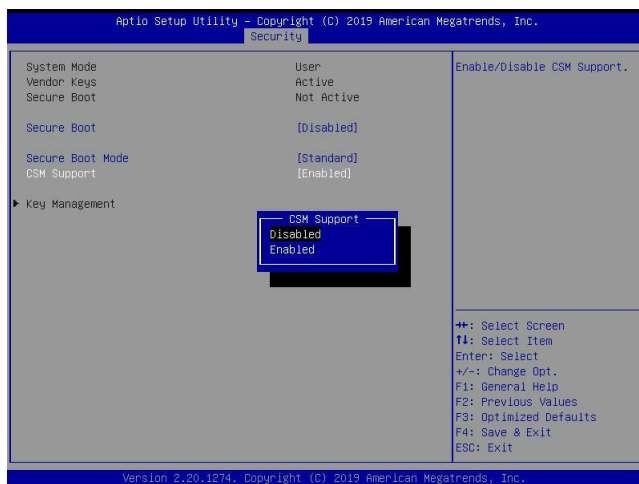


 **Note:** The Key Management menu will become unavailable when Secure Boot Mode is set to Standard.

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



Step 3. Press 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.

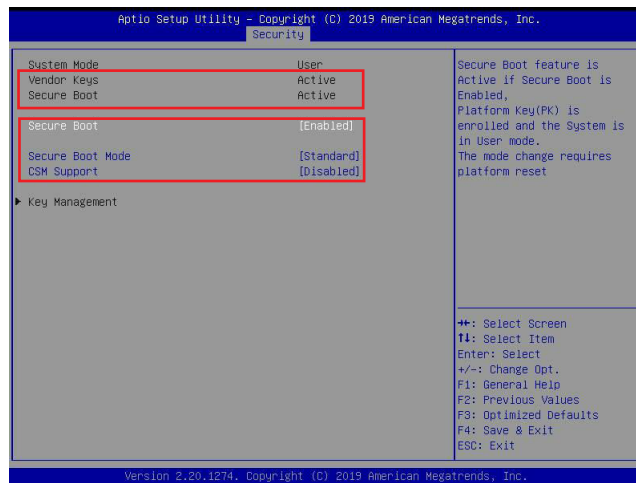


For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

Step 4. Press 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.



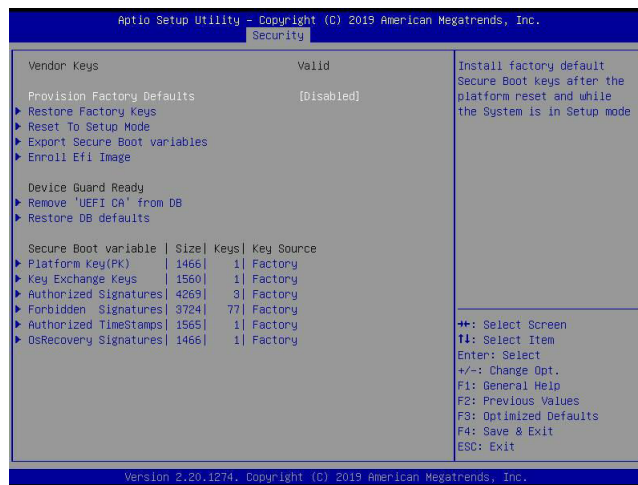
For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. The following screen will appear.



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

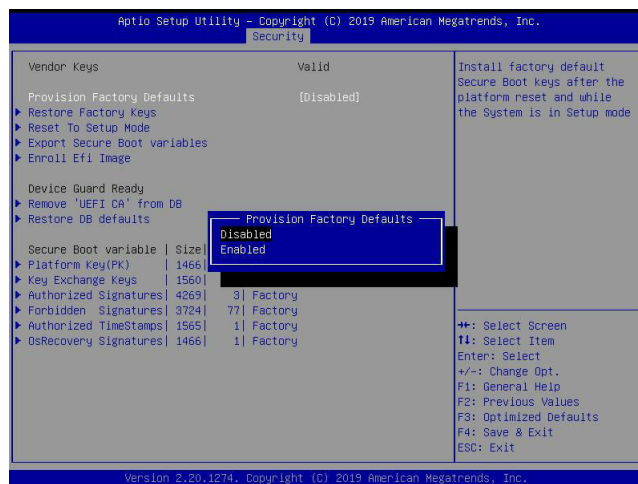
F.4 Key Management Settings

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



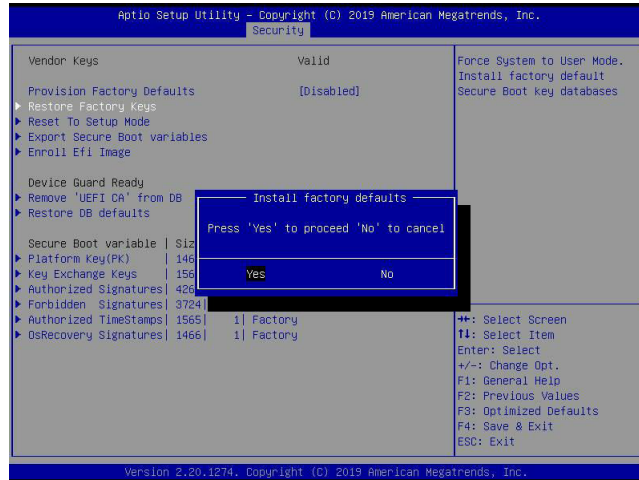
Provision Factory Defaults

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



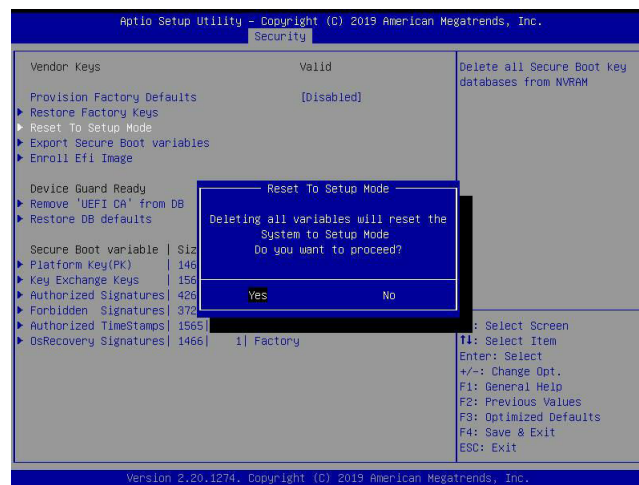
► Restore Factory Keys

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



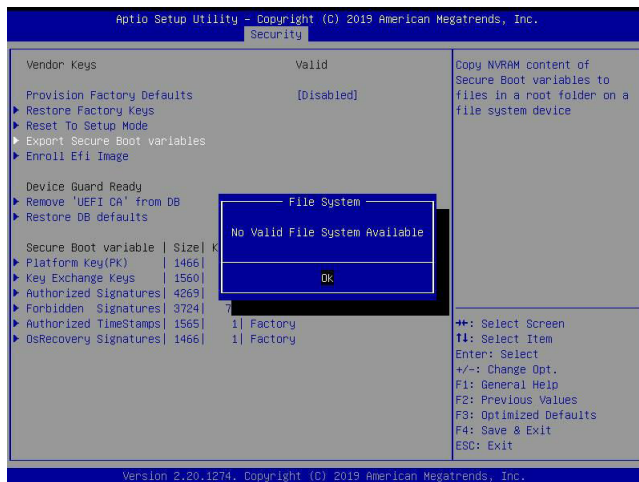
► Reset To Setup Mode (available when the System Mode is in User mode)

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



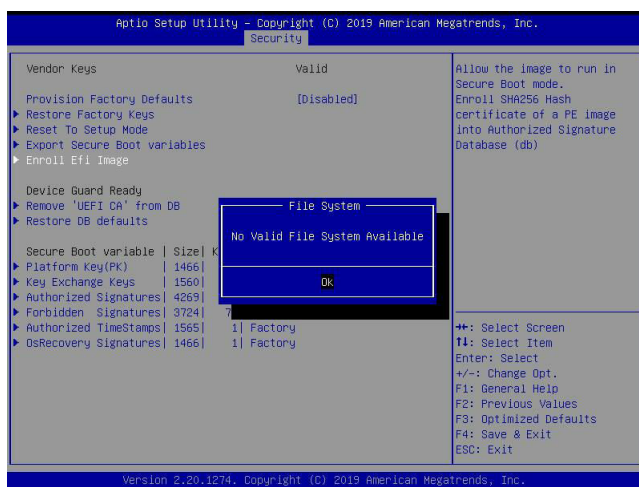
► Export Secure Boot variables

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



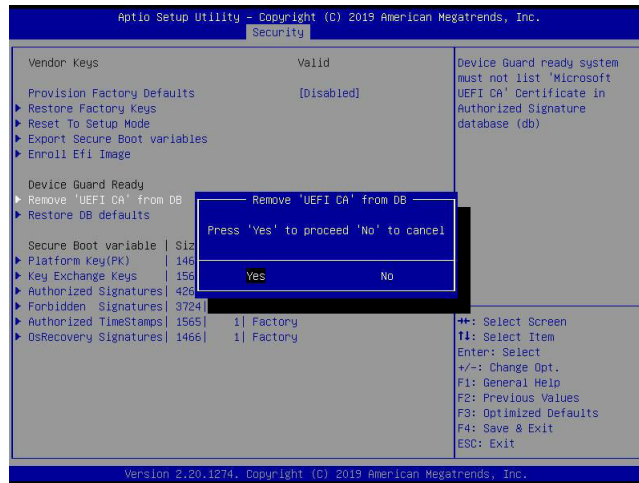
► Enroll Efi Image

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



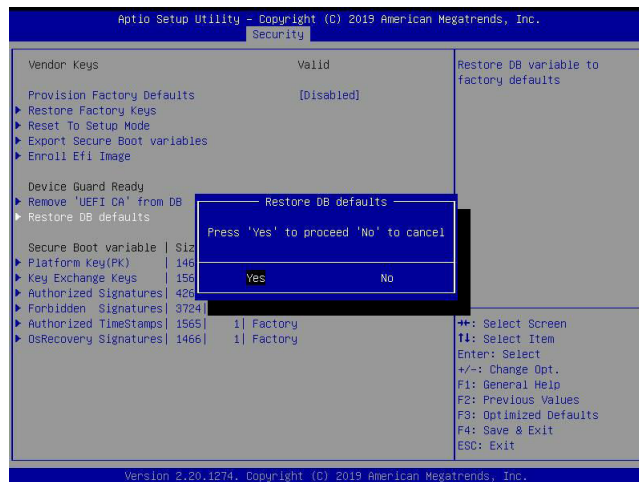
► **Remove 'UEFI CA' from DB (available when the system is not in Device Guard Ready)**

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



► **Restore DB defaults**

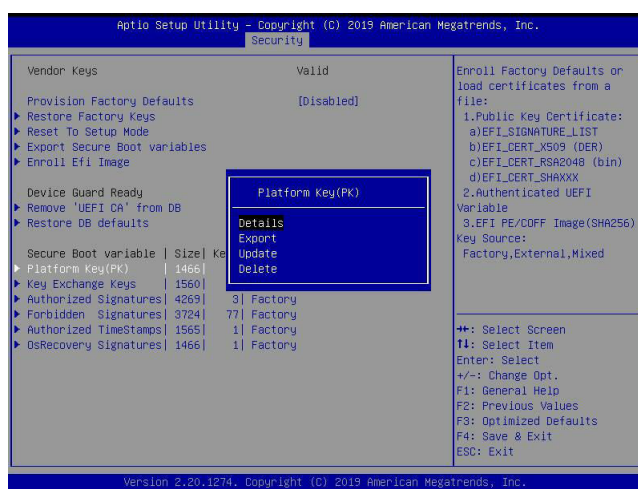
Select and press Yes to restore the DB variables to factory defaults. The options are **Yes** and **No**.



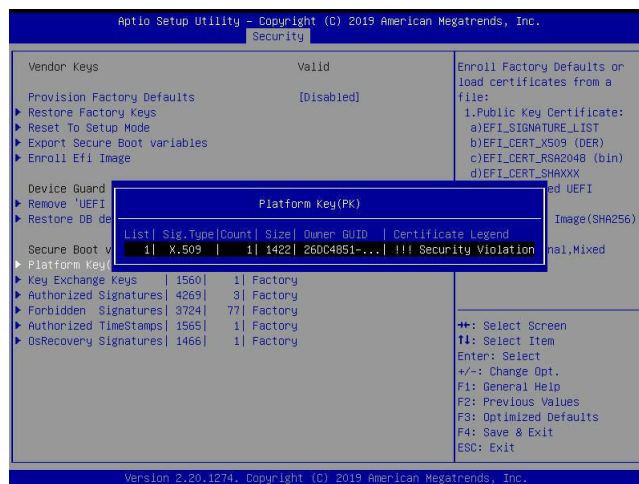
**Refer to the following settings for keys and signatures related to secure boot.*

► Platform Key (PK)

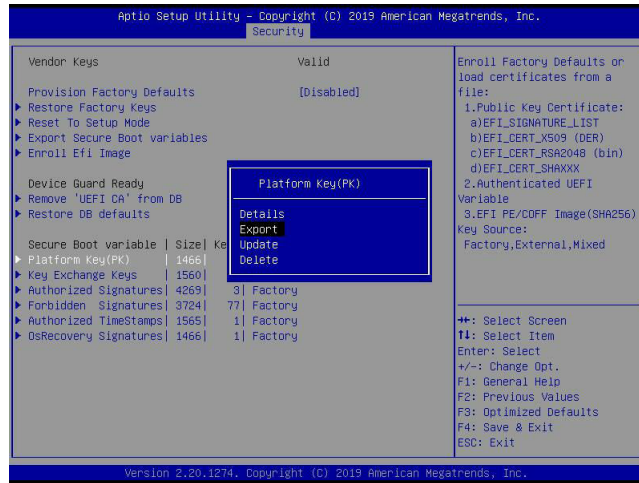
The Platform Key (PK), which is pre-installed in firmware during manufacturing, provides full control of the secure boot key hierarchy. The options are **Details**, Export, Update, and Delete. Select Details to display detailed information of PK. Select Export to save the current PKs to a FAT formatted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



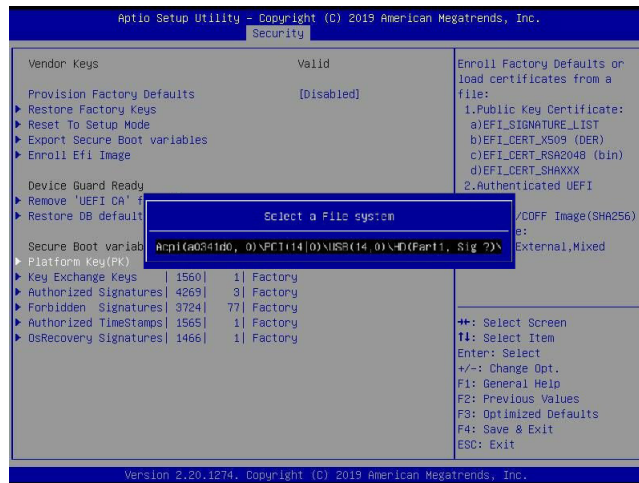
Details: Use the arrow keys to select Details and press <Enter>. It displays detailed information of PK as shown below.




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

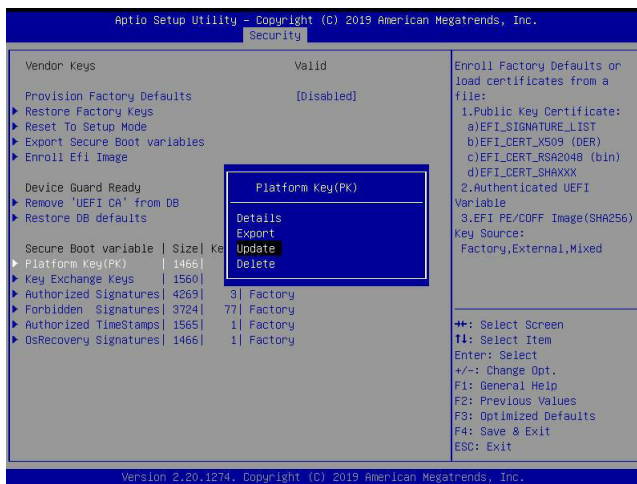


Press <Enter> and the following screen will appear.

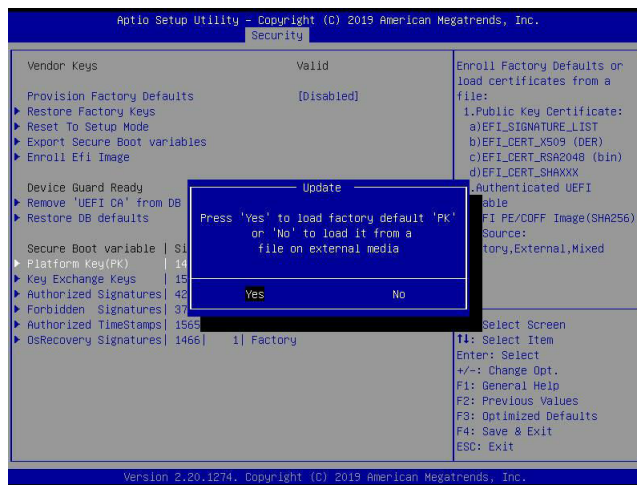


 **Note:** Refer to the right panel of the screen for the file formats accepted.

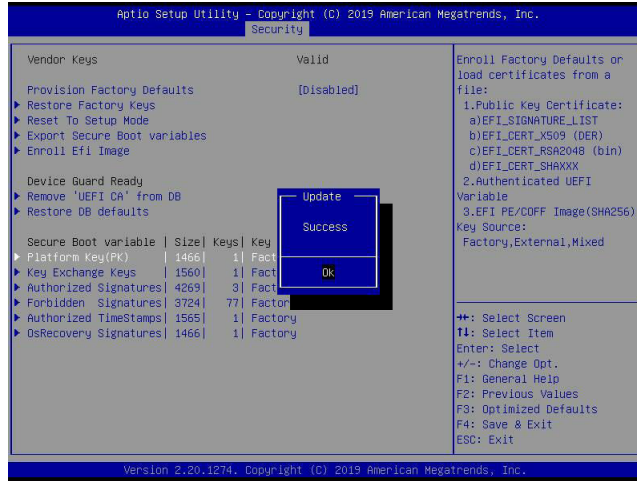
Update: Use the arrow keys to select Update. It is to load the factory defaults or load PKs from a file on the external device.



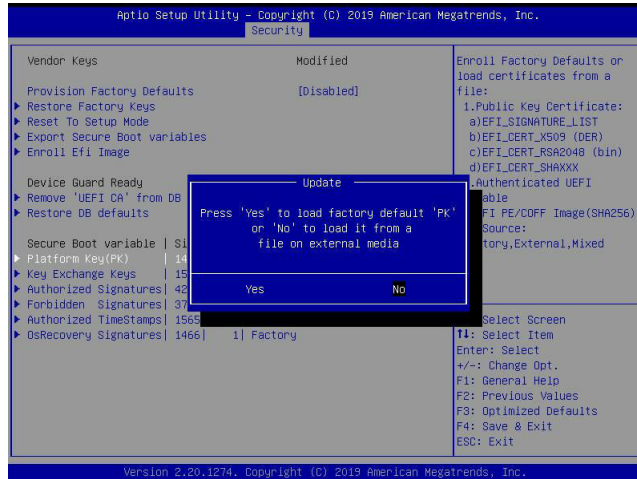
Press <Enter> and the following screen will appear.



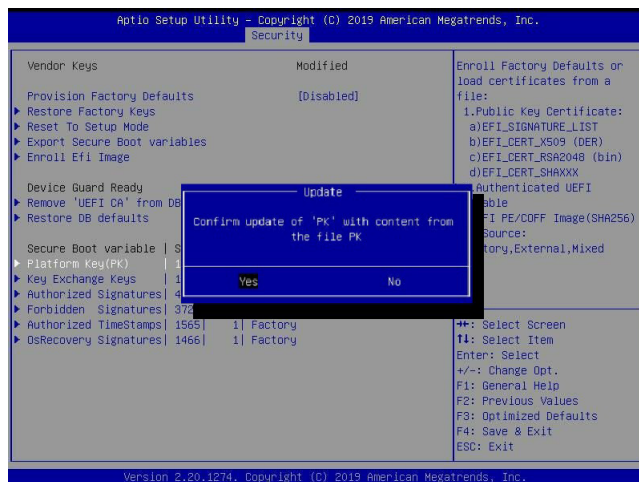
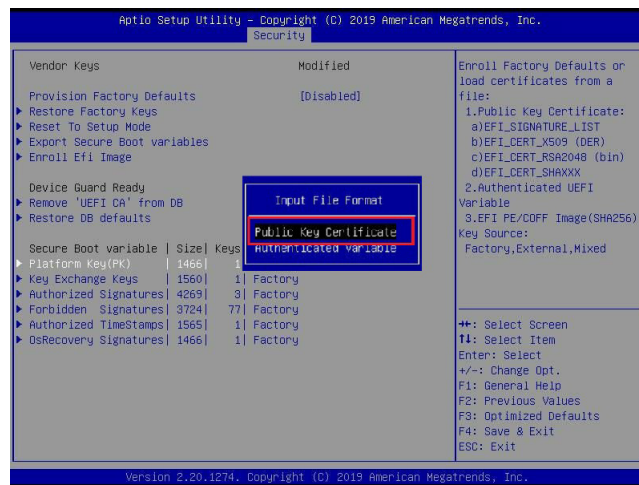
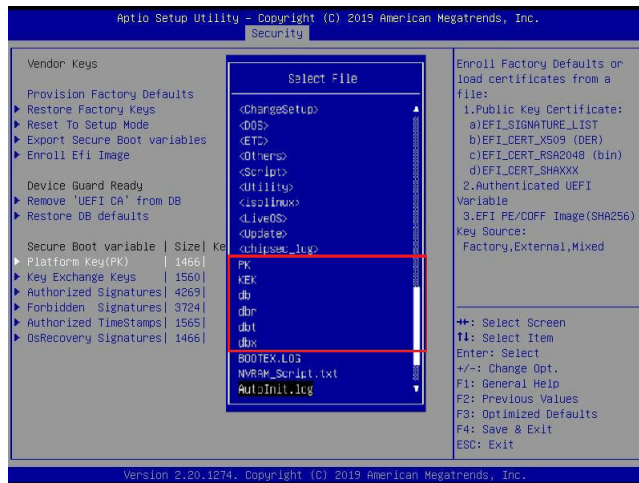
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.



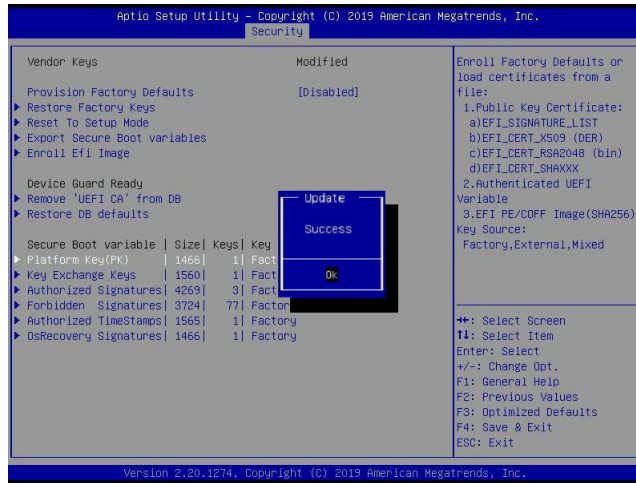
To load PKs from a file on the external device, navigate to No and press <Enter>.



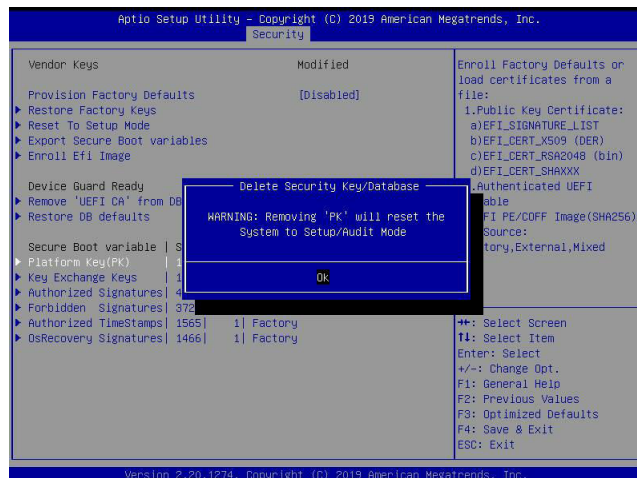
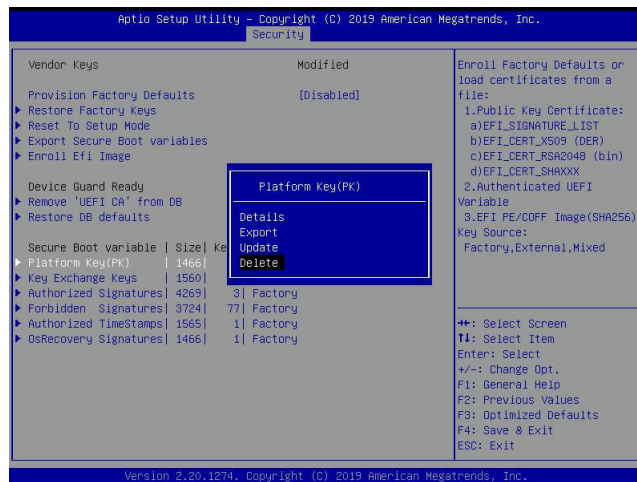
When the following screen appears, select the USB flash drive that contains the desired file.



Press <Enter> and the following screen will appear.

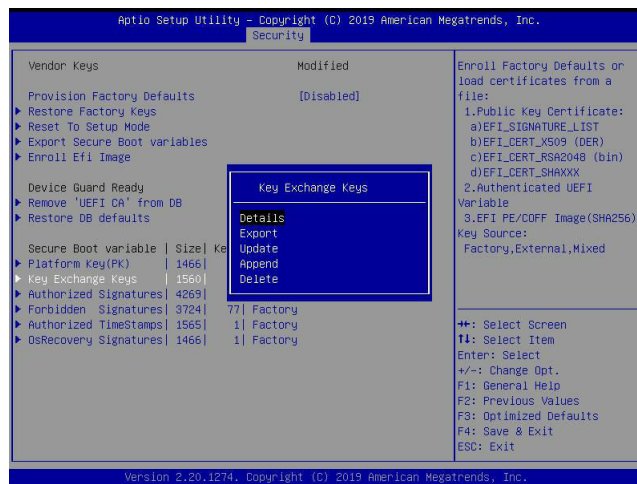


Delete: Use the arrow keys to select Delete and press <Enter> to clear the current PKs and reset the system to the Setup mode.

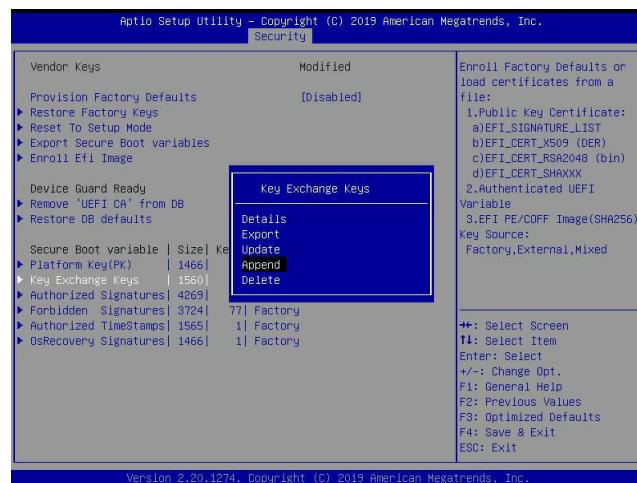


► Key Exchange Key

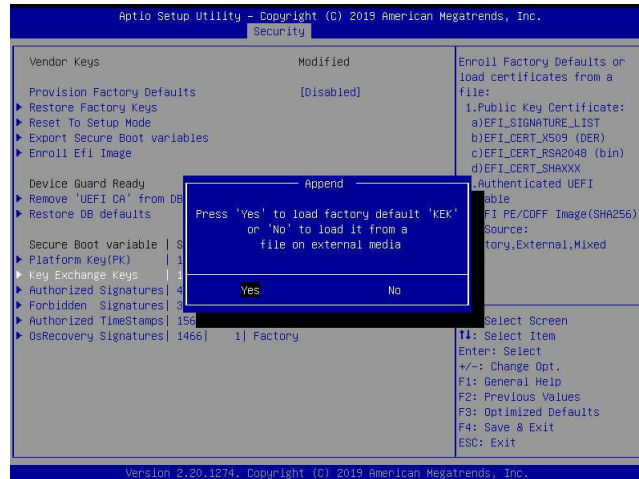
The Key Exchange Key (KEK), which is held by the operating system vendor, can be updated by the holder of the PK and be used by secure boot to protect access to signatures databases. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of KEKs. Select Export to save the current KEKs to a FAT formatted USB flash drive. Select Update to load the factory defaults or load KEKs from a file on the external device. Select Append to load the factory defaults or load KEKs from a file on the external device. Select Delete to clear the current KEKs or to delete only one certificate from the key database. (Refer to page 150 for the Export process. Refer to pages 151, 152, 153, and 154 for the Update process.)



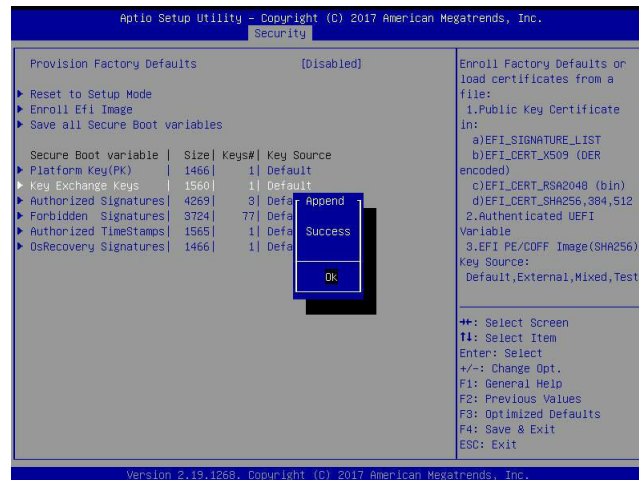
Append: Use the arrow keys to select Append.



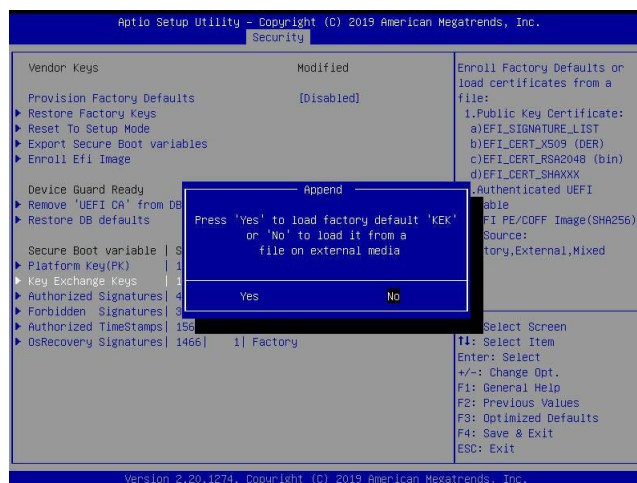
Press <Enter> and the following screen will appear.



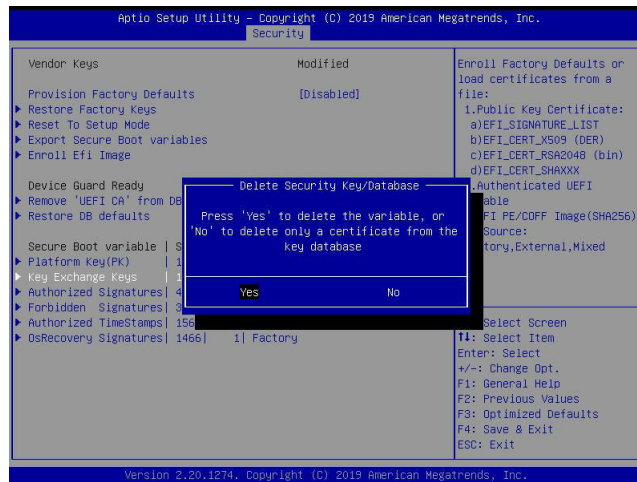
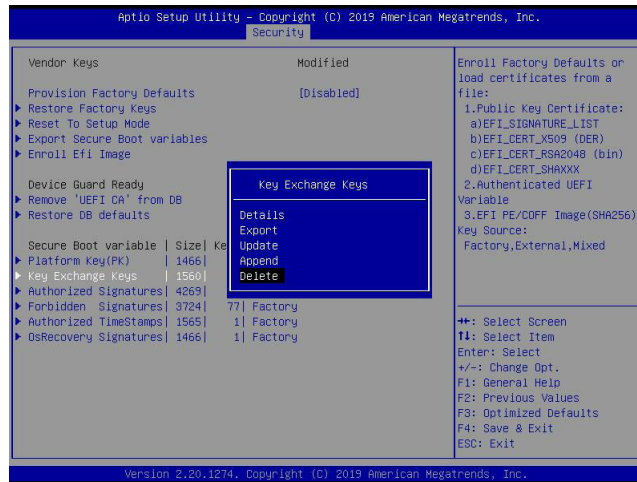
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.



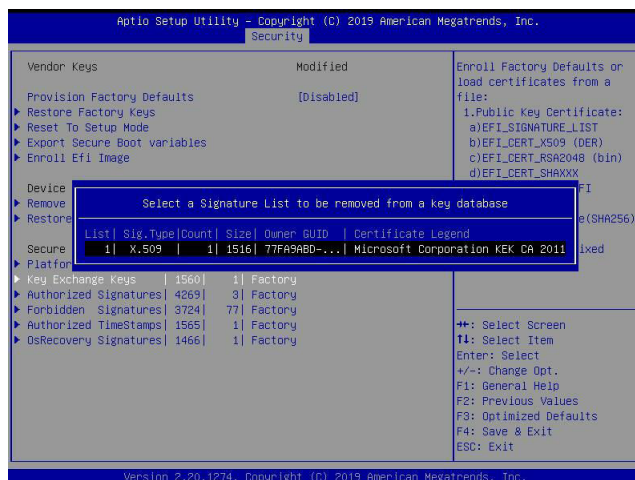
To load KEKs from a file on the external device, navigate to No and press <Enter>. Refer to pages 153 and 154 on how to load KEKs from a file on the external device.



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

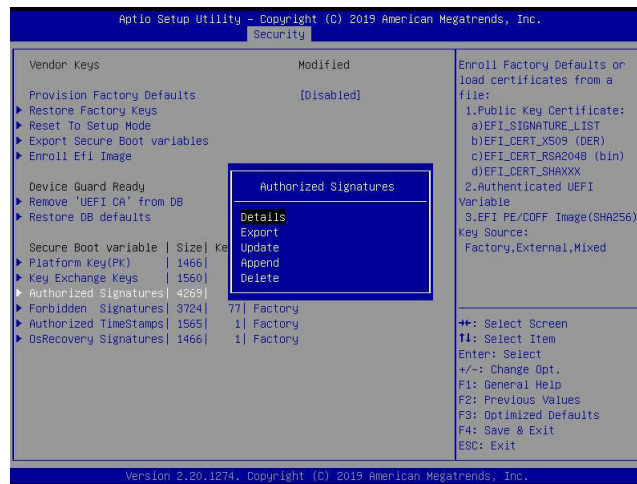


Navigate to No and press <Enter> to delete only one certificate from the key database.



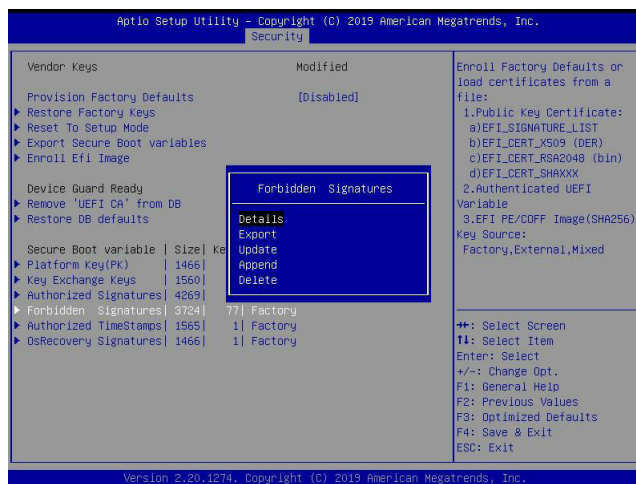
► Authorized Signatures

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 150 for the Export process. Refer to pages 151, 152, 153, and 154 for the Update process. Refer to pages 155 and 156 for the Append process. Refer to page 157 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 150 for the Export process. Refer to pages 151, 152, 153, and 154 for the Update process. Refer to pages 155 and 156 for the Append process. Refer to page 157 for the Delete process.)



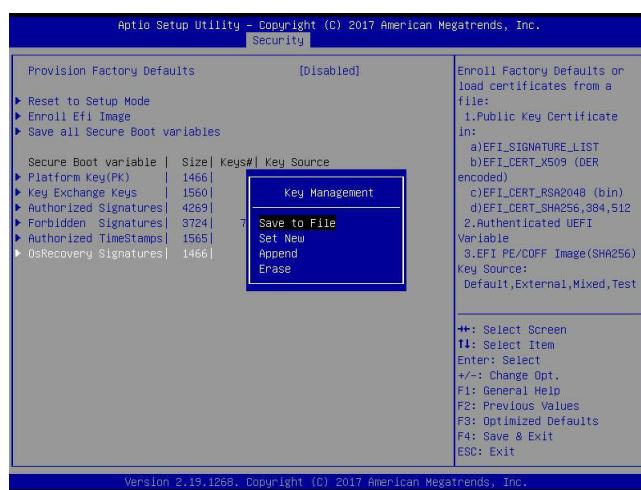
► Authorized TimeStamps

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 150 for the Export process. Refer to pages 151, 152, 153, and 154 for the Update process. Refer to pages 155 and 156 for the Append process. Refer to page 157 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 150 for the Export process. Refer to pages 151, 152, 153, and 154 for the Update process. Refer to pages 155 and 156 for the Append process. Refer to page 157 for the Delete process.)



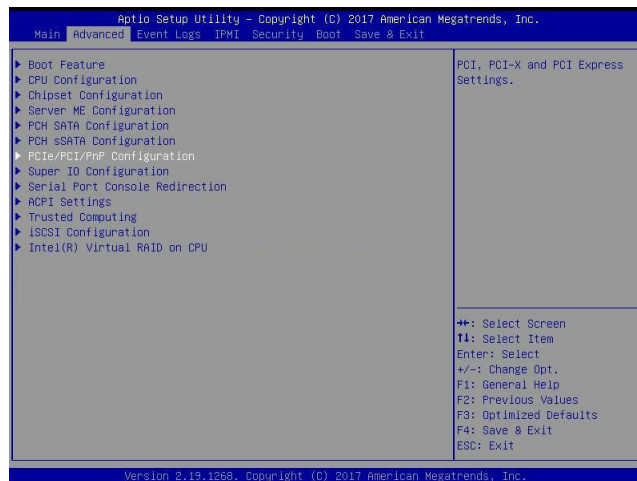
Appendix G

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.

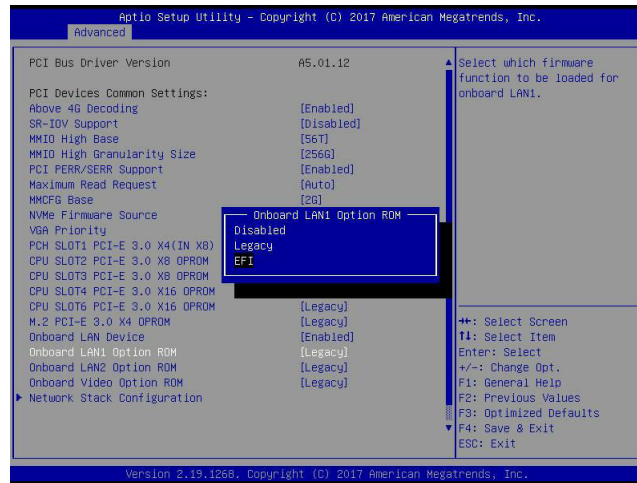
G.1 Network Interface Card (NIC) Settings

Press 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.



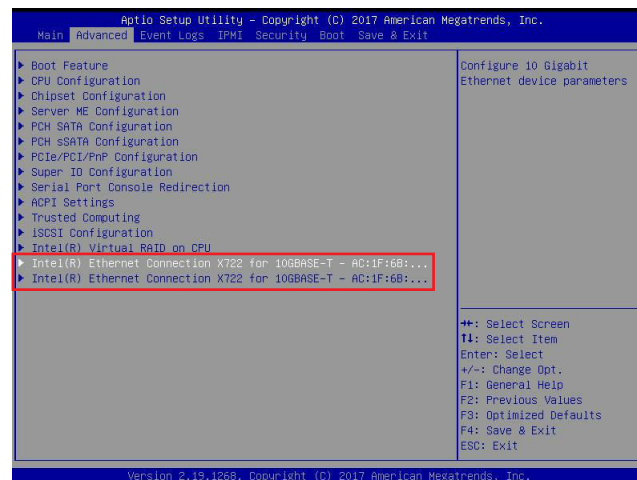
Onboard LAN1 Option ROM (available when NIC(s) is(are) detected by the system)

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.

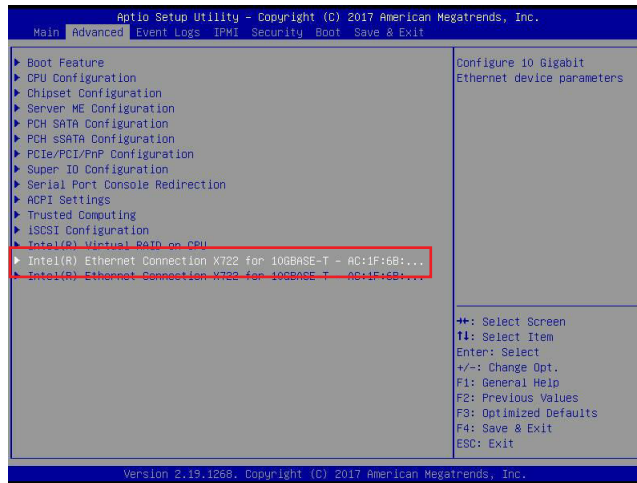


Note : If Onboard LAN1 Option ROM is set to EFI, all features for onboard LAN option ROM will be set to EFI by the EFI driver. Additionally, these features will become unavailable except Onboard LAN1 Option ROM.

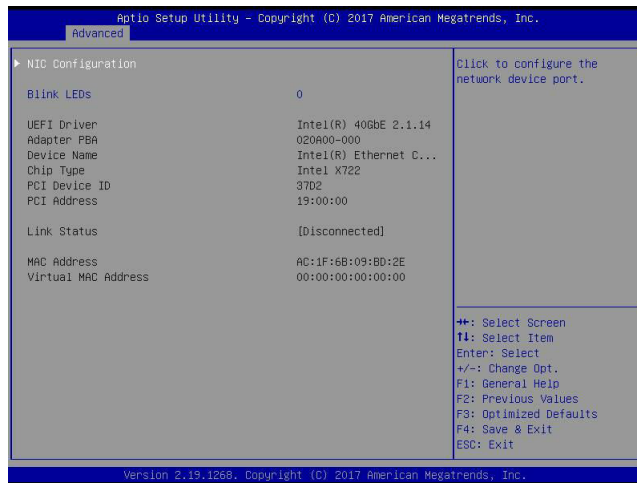
For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press during system boot to enter the BIOS Setup utility. Navigate to the Advanced tab. The feature(s) for onboard Intel® LAN device(s) will become available for configuration as shown below.



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

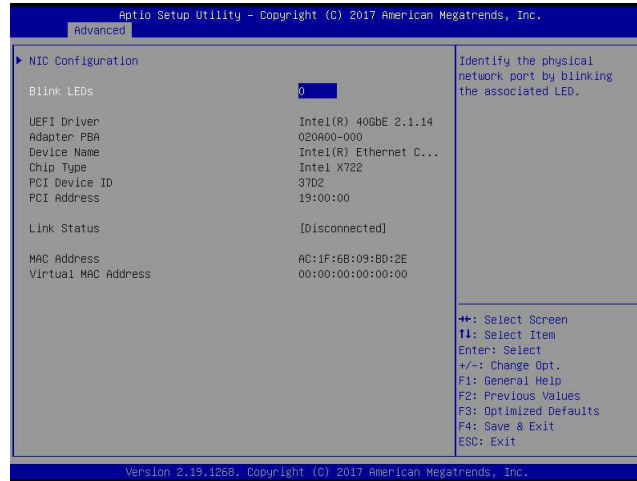


Press <Enter> and the following screen will appear. It displays the detailed information for the selected onboard LAN device.



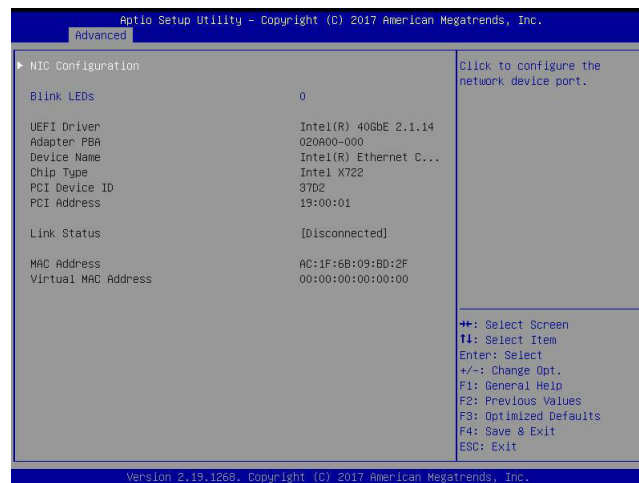
Blink LEDs

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.

