X11OPi Platform

with

X11OPi-CPU Board
AOM-X11OPi-LBG Card
RSC-X11OPi-PCIE Card
AOM-X11OPi-HDD Card
AOM-X11OPi-KVM Card
BPN-X11OPi Midplane

USER'S MANUAL

Revision 1.2

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

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

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

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

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

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

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

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

Manual Revision 1.2

Release Date: September 28, 2020

Preface

About This Manual

This manual is written for system integrators, IT professionals, and knowledgeable PC users. It provides information for the installation and use of the X11OPi Platform.

About This X11OPi Platform

The X11OPi platform consists of eight X11OPi-CPU boards, one AOM-X11OPi-LBG board, five RSC-X11OPi-PCIE cards, one AOM-X11OPi-HDD card, one AOM-X11OPi-KVM card, and a BPN-X11OPi midplane. Each X11OPi-CPU board supports an Intel® Xeon® Platinum 8XXX processor which offers Intel® Turbo Boost Technology, Intel® Hyper-Threading Technology, and Intel® UltraPath Interconnect (UPI) Technology with a transfer rate of up to 10.4 GT/s. It supports up to 3 TB DCPMM memory, 3 TB DDR4 memory, or up to 4.5 TB DCPMM & DDR4 combined memory of 2933/2666/2400 MHz in 12 DIMM modules per CPU board. With eight X11OPi-CPU boards built-in, the X11OPi Platform provides up to 24 TB of DCPMM/DDR4 memory or up to 36 TB of DCPMM & DDR4 combined memory in 96 DIMM slots. (See the notes below.) In addition, this platform also supports 32 NVMe connections and 12 SATA 3.0 connections. The X11OPi platform is optimized for High-Performance Computing (HPC) platforms and is ideal for use in virtualization and database servers. Please refer to our website at http://www.supermicro.com for processor and memory support updates. This product is intended to be installed and serviced by professional technicians.

Notes:

1. UPI/memory speeds are dependent on the processors installed in your system.

2. Eeach X11OPi-CPU board supports up to 3 TB 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 memory of 2933/2666/2400 MHz in 12 slots. 2933 MHz memory is supported by Second Generation Intel® Xeon® Platinum 82XX processors only.

3. Eeach X11OPi-CPU board supports up to 3 TB DCPMM memory of up 2933 MHz in 12 slots. DCPMM memory is supported by Second Generation Intel® Xeon® Platinum 82XX processors only.

4. Eeach X11OPi-CPU board supports up to 4.5 TB DCPMM & DDR4 combined memory of up 2933 MHz in 12 slots.

5. With eight (8) X11OPi-CPU boards built-in, theX11OPi Platform supports up to 24 TB of DCPMM/DDR4 memory or up to 36 TB of DCPMM & DDR4 combined memory in 96 DIMM slots.

Manual organization

Chapter 1 describes the features, specifications and performance of the X11OPi system. It also provides detailed information on hardware installation instructions.

Chapter 2 describes troubleshooting procedures for video, memory, and system setup stored in the CMOS.

Chapter 3 includes an introduction to the BIOS and provides detailed information on BIOS setup configuration.

Appendix A provides a list of BIOS POST beep codes.

Appendix B details software installation instructions.

Appendix C lists standardized warning statements.

Appendix D provides UEFI BIOS recovery instructions**.**

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

Appendix F provides information on how to configure secure boot settings.

Contacting Supermicro

Headquarters

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

Europe

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

Asia-Pacific

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

Table of Contents

Chapter 1

Introduction

1-1 Checklist

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

For more information regarding this product, please visit our website at www.supermicro.com.

Note: The X11OPi-CPU board is intended to be used in conjunction with the AOM-X11OPi-LBG card, the RSC-X11OPi-PCIE card, the AOM-X11OPi-HDD card, and the BPN-X11OPi midplane as an integrated server platform. These components are not to be used as stand-alone products and will not be shipped independently in a retail box.

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 system.

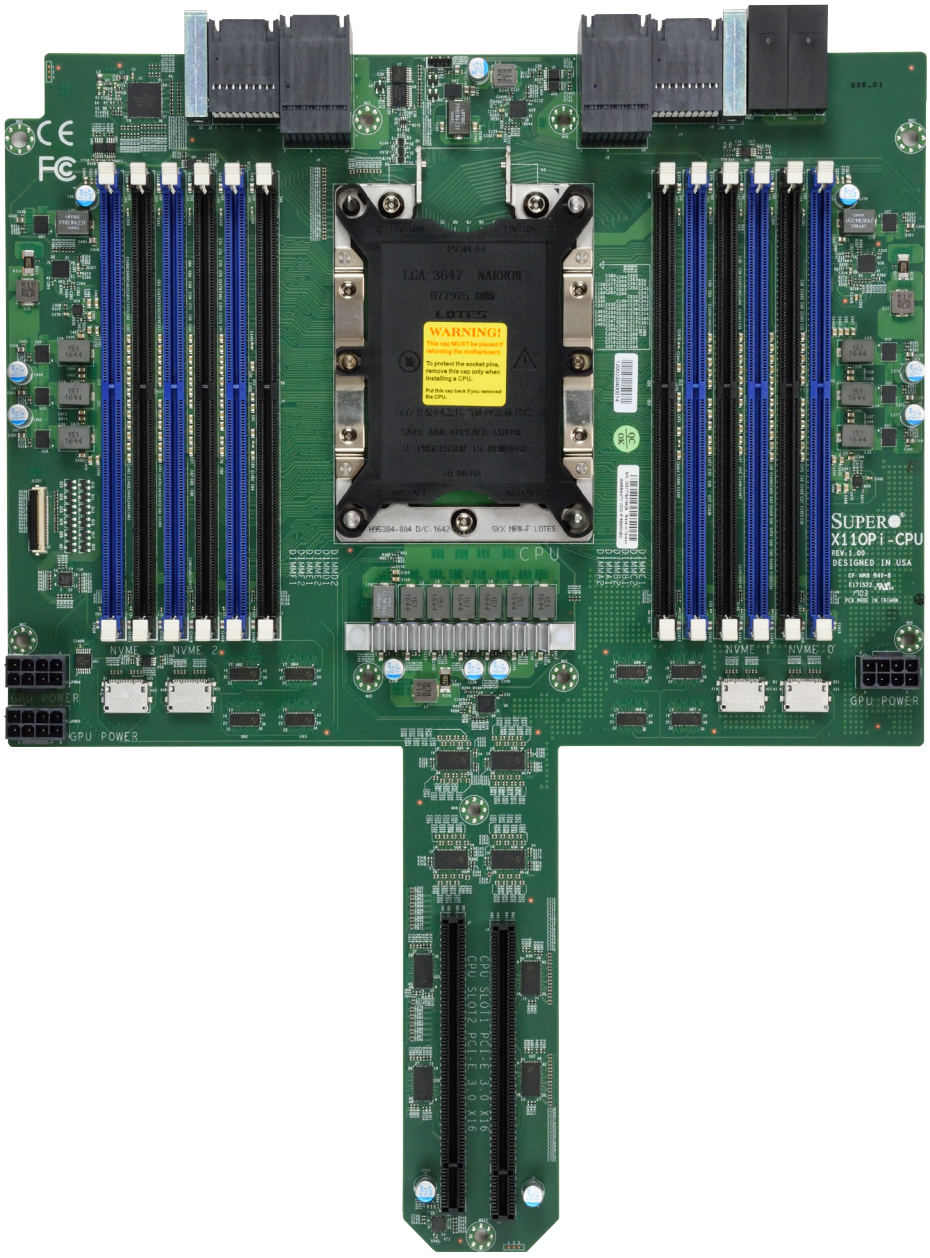
- Supermicro product manuals: http://www.supermicro.com/support/manuals/
- Product drivers and utilities: http://www.supermicro.com/wftp
- Product safety info: http://www.supermicro.com/about/policies/safety_information.cfm
- A secure data deletion tool designed to fully erase all data from storage devices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

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

1-2 The X11OPi-CPU Board

Your system can support up to eight X11OPi-CPU boards on the front side of the BPN-X11OPi midplane. The following section provides detailed information on the X11OPi-CPU board.

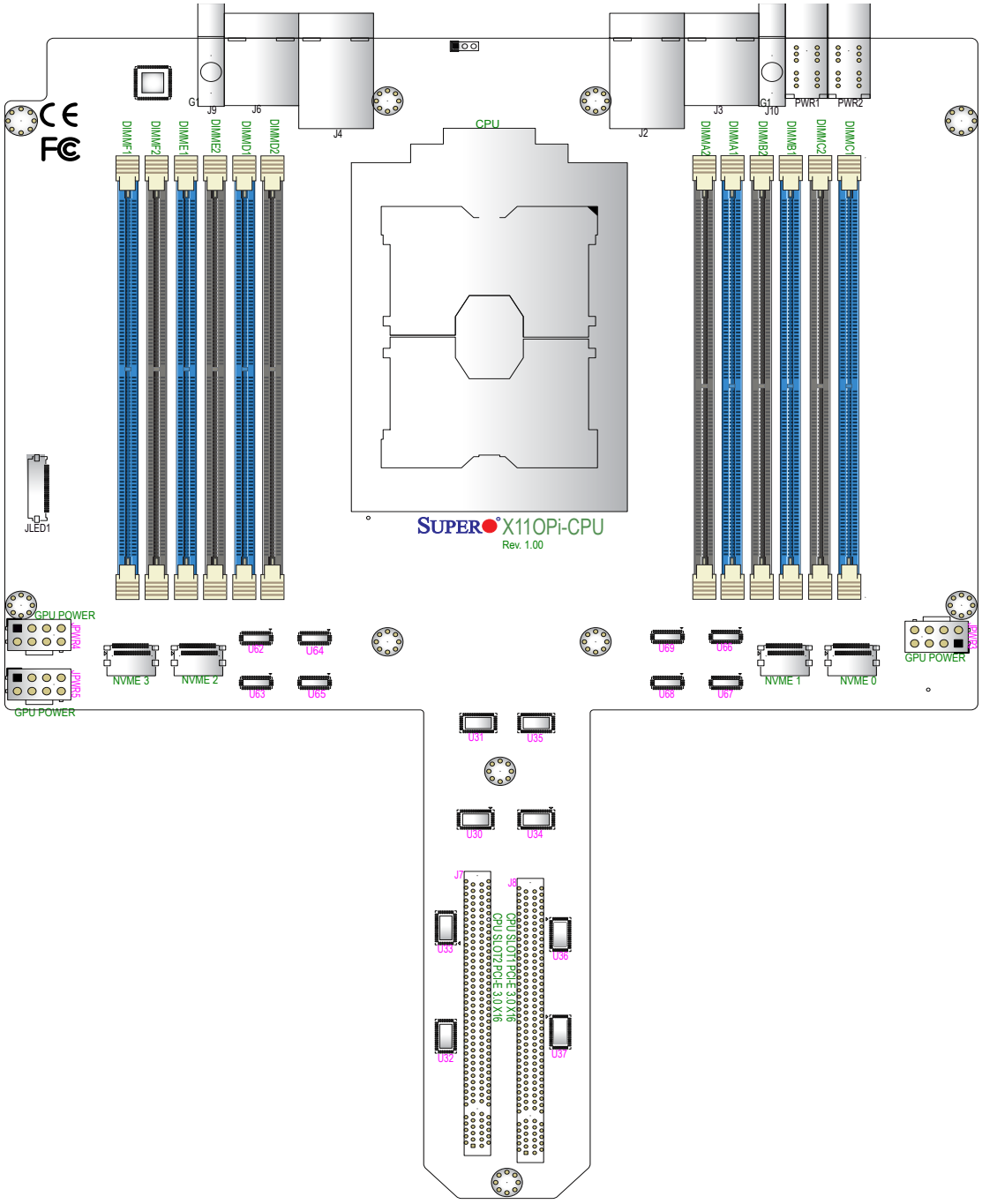
X11OPi-CPU Board Image (Rev. 1.00)



Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publishing this manual. The components installed in your system may or may not look exactly the same as the graphics shown in this manual.

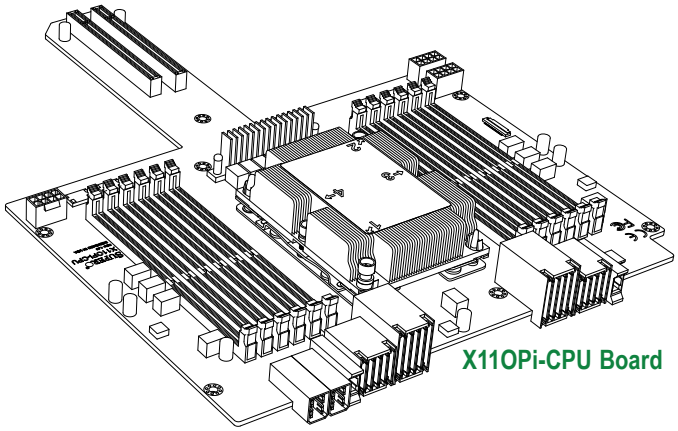
X11OPi-CPU Board Layout

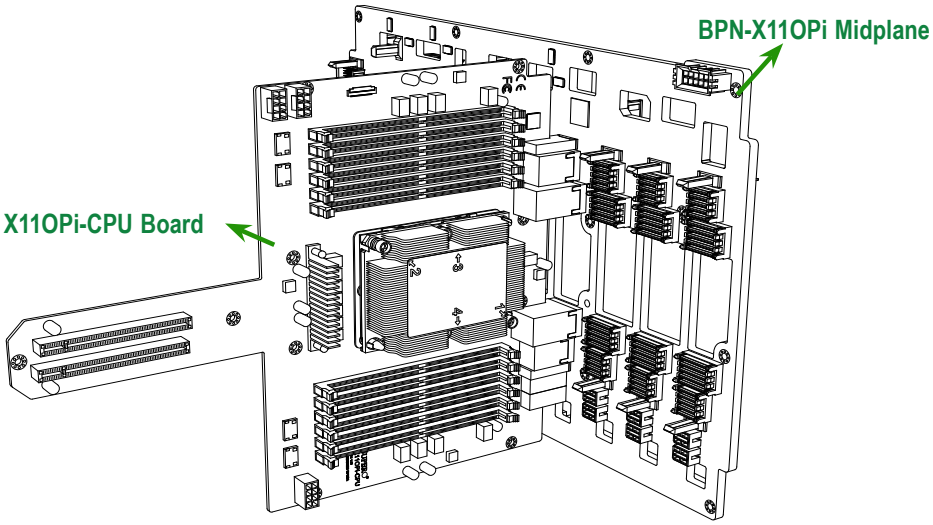
(not drawn to scale)



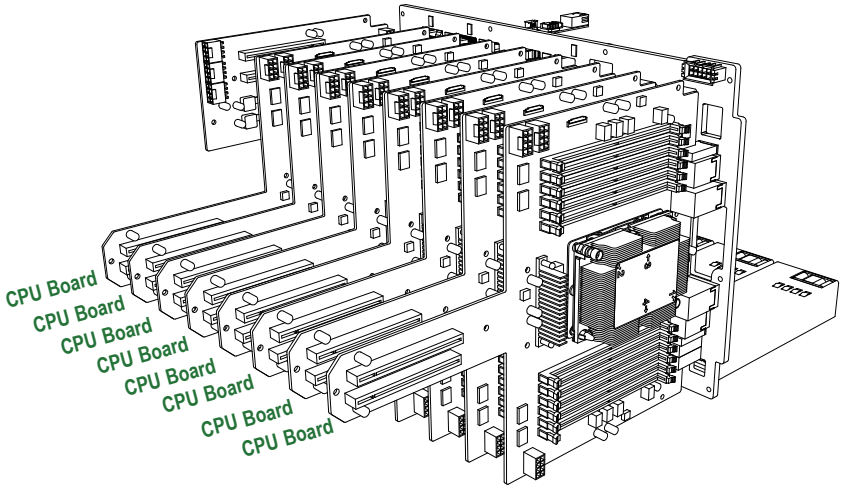
Note: Components not documented are for internal testing only.

Location of the X11OPi-CPU Board



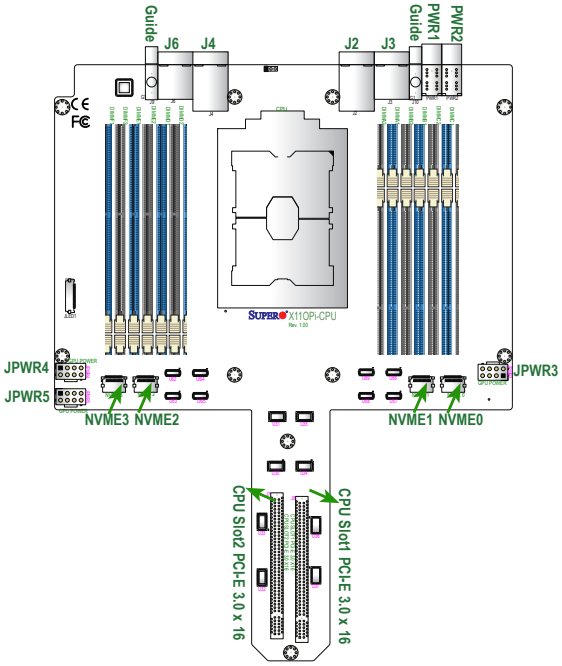


One (1) CPU Board on the Front Side of the X11OPi Midplane



Eight (8) CPU Boards (max.) on the Front Side of the X11OPi Midplane

Major Components on the X11OPi-CPU Board



Connectors on the X11OPi-CPU

Connector	Description
J3/J6	High speed interconnect
J2/J4	High speed interconnect
J7	PCI-E 3.0 x16 slot supported by the CPU (Slot1)
J8	PCI-E 3.0 x16 slot supported by the CPU (Slot2)
J9/J10	CPU card guides (to be used to attach the CPU cards to the midplane board)
JLED1	Memory error LED connector
JPWR3/JPWR4/JPWR5	GPU power connectors 3/4/5
PWR1/PWR2	12-pin CPU power connectors 1/2
NVME0-NVME3	Non-Volatile Memory Express (NVME) connectors 1/2/3/4
DIMMA1-F2	DIMM memory modules (DIMMA1/A2/B1/B2/C1/C2/D1/D2/E1/E2/F1/F2)

Notes:

- See Chapter 2 for detailed information on jumpers, I/O ports, and JF1 front panel connections.
- "■" indicates the location of Pin 1.
- Components/jumpers/LED indicators not documented are reserved for internal testing only.

Processor and Memory Support on the X11OPi-CPU Board

CPU & Memory Support on the X11OPi-CPU Board	
Component	**Description**
CPU	Intel® Xeonl® Platinum 8XXX processor with UPI up to 10.4GT/s
DIMM Slots: DIMMA1/A2, DIMMB1/B2, DIMMC1/C2, DIMMD1/D2, DIMME1/E2, DIMMF1/F2	**1.** Eeach X11OPi-CPU board supports up to 3 TB 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 memory of 2933*/2666/2400 MHz in 12 slots. 2933 MHz memory is supported by Second Generation Intel® Xeon® Platinum 82XX processors only. **2.** Eeach X11OPi-CPU board supports up to 3 TB DCPMM memory of up 2933 MHz in 12 slots. DCPMM memory is supported by Second Generation Intel® Xeon® Platinum 82XX processors only. **3.** Eeach X11OPi-CPU board supports up to 4.5 TB DCPMM & DDR4 combined memory of up 2933 MHz in 12 slots. **4.** With eight (8) X11OPi-CPU boards built-in, this platform supports up to 24 TB of DCPMM/DDR4 memory or up to 36 TB of DCPMM & DDR4 combined memory in 96 DIMM slots. **Notes: 1.** Memory speed support depends on the CPUs used in the motherboard. For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard. **2.** Please refer to the memory configuration & population tables to maximize memory performance.

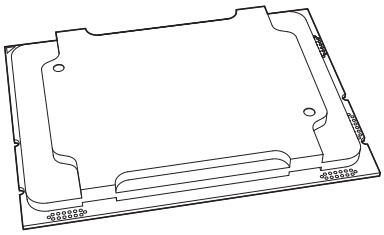
Installing the Intel® Xeon® Platinum 8XXX Processor

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. Electrostatic Discharge (ESD) can damage electronic components. To avoid damaging your system, it is crucial to follow the instructions given in the Static-Senstive Devices section in Appendix C to protect your equipment from ESD.

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.
- Please refer to Appendix C Standardized Warning Statements before installing or changing components of the system.
- If you buy a CPU separately, make sure that you use an Intel-certified multi-directional heatsink only.
- Make sure to install the processor and memory into the X11OPi-CPU board before you install the CPU board into the CPU board slot on the front side of the BPN-X11OPi midplane.
- When receiving a system 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.

The Intel® Xeon® Platinum 8XXX processor



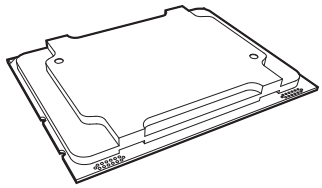
Note: All graphics shown in this manual were based upon the latest PCB revision available at the time of publishing this manual. The components installed in your system may or may not look exactly the same as the graphics shown in this manual.

Overview of the Processor Socket Assembly

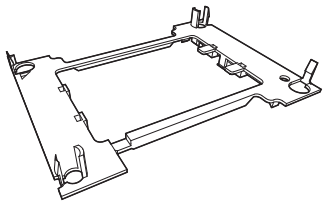
The processor socket assembly contains 1)Intel® Xeon® Platinum 8XXX processor (Note below), 2) the narrow processor clip, 3) the dust cover, and 4) the CPU socket.

Note: The Intel® Xeon® Platinum 8XXX processor contains the F model and the non-F model processors. This motherboard only supports non-F model processors.

1. Intel Xeon Platinum 8XXX Processor

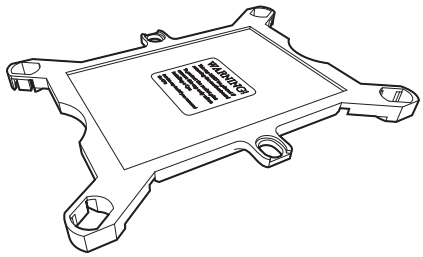


2. Narrow processor clip (the plastic processor package carrier used for the CPU)

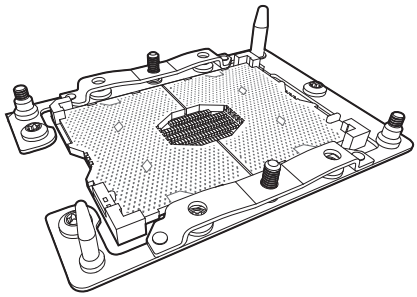


(for the non-F model processor - see the note above)

3. Dust Cover



4. CPU Socket



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

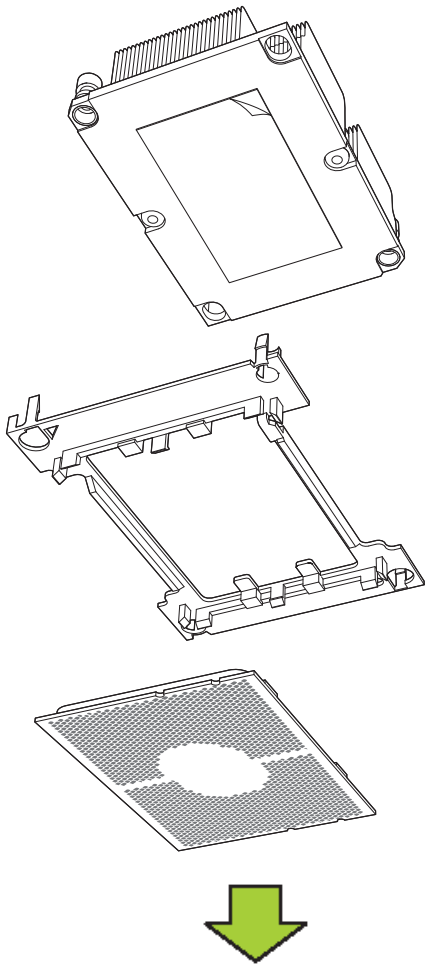
Overview of the Processor Heatsink Module (PHM)

The Processor Heatsink Module (PHM) contains 1) a heatsink, 2) a narrow processor clip, and 3) the Intel® Xeon® Platinum 8XXX processor.

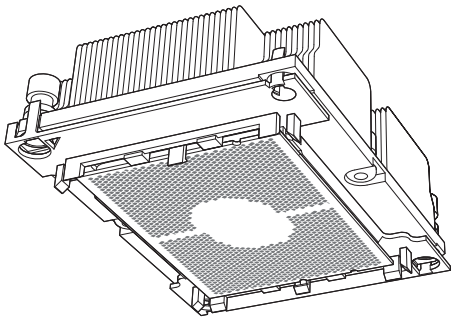
1. Heatsink

2. Narrow processor clip

3. Processor



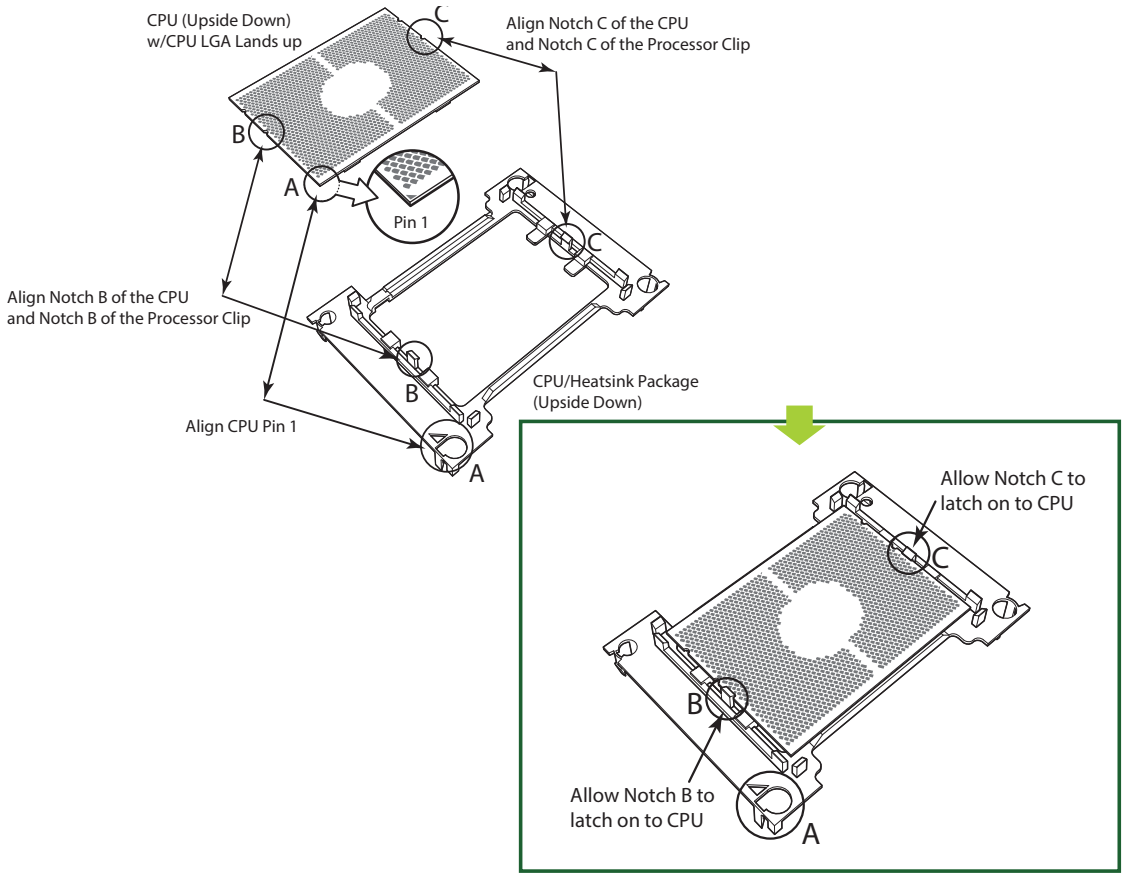
Processor Heatsink Module (PHM)



(Bottom View)

Attaching the Intel® Xeon® Platinum 8XXX Processor to the Narrow Processor Clip to Create the Processor Package Assembly

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).

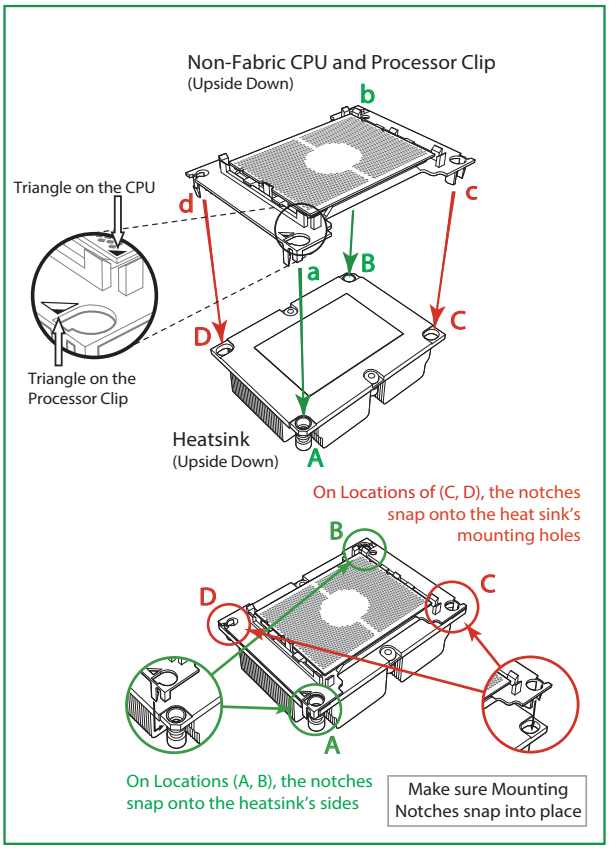
1. Locate "1" on the heatsink label and the triangular corner next to it on the heatsink. With your index finger pressing against the screw at this triangular corner, carefully hold and turn the heatsink upside down with the thermal-grease side facing up. Remove the protective thermal film if present,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

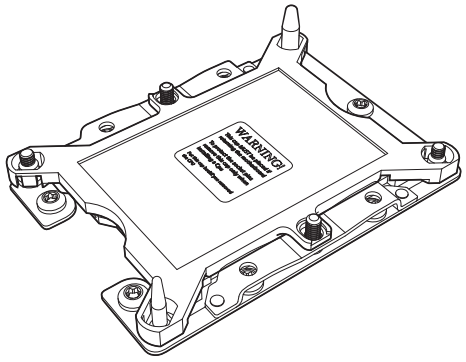
4. Also align the triangular corner ("B") at the diagonal side of the heatsink with the corresponding clips on the processor package assembly ("b").

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.



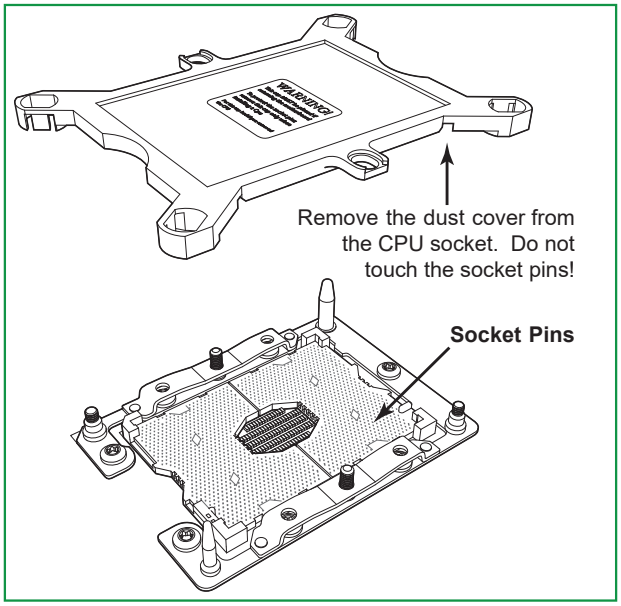
CPU Socket w/Dust Cover On

Removing the Dust Cover from the CPU Socket

Remove the dust cover from the CPU socket, exposing the processor 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.

Dusk Cover

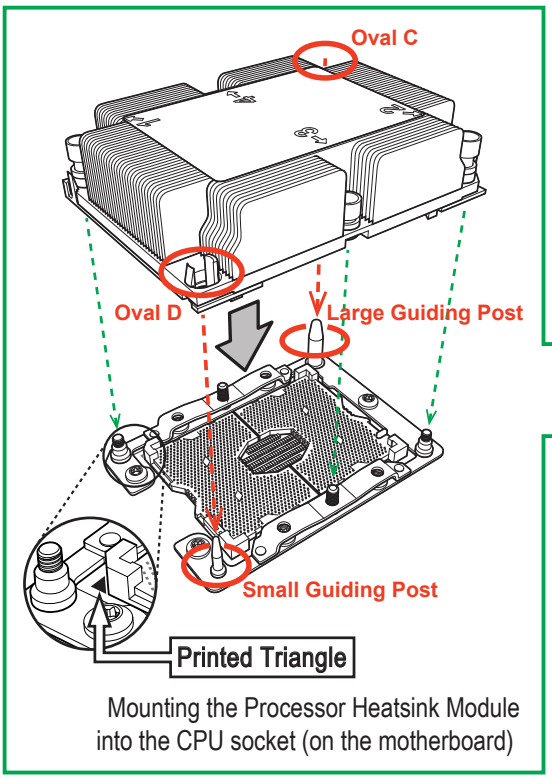


CPU Socket

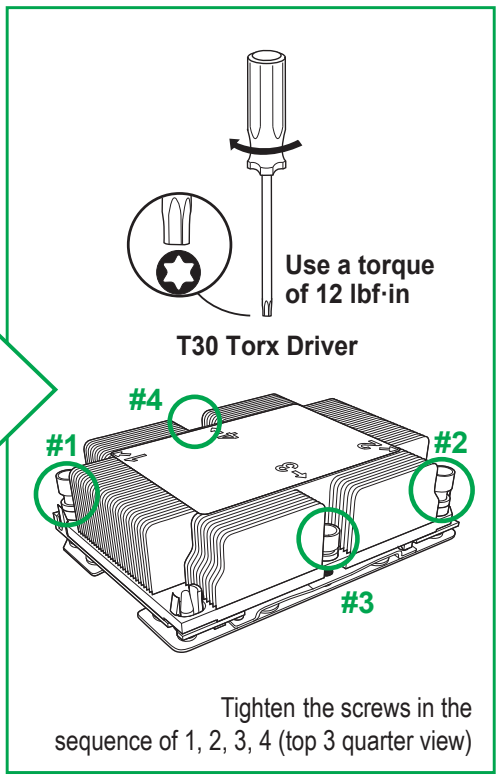
Installing the Processor Heatsink Module (PHM)

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

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



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



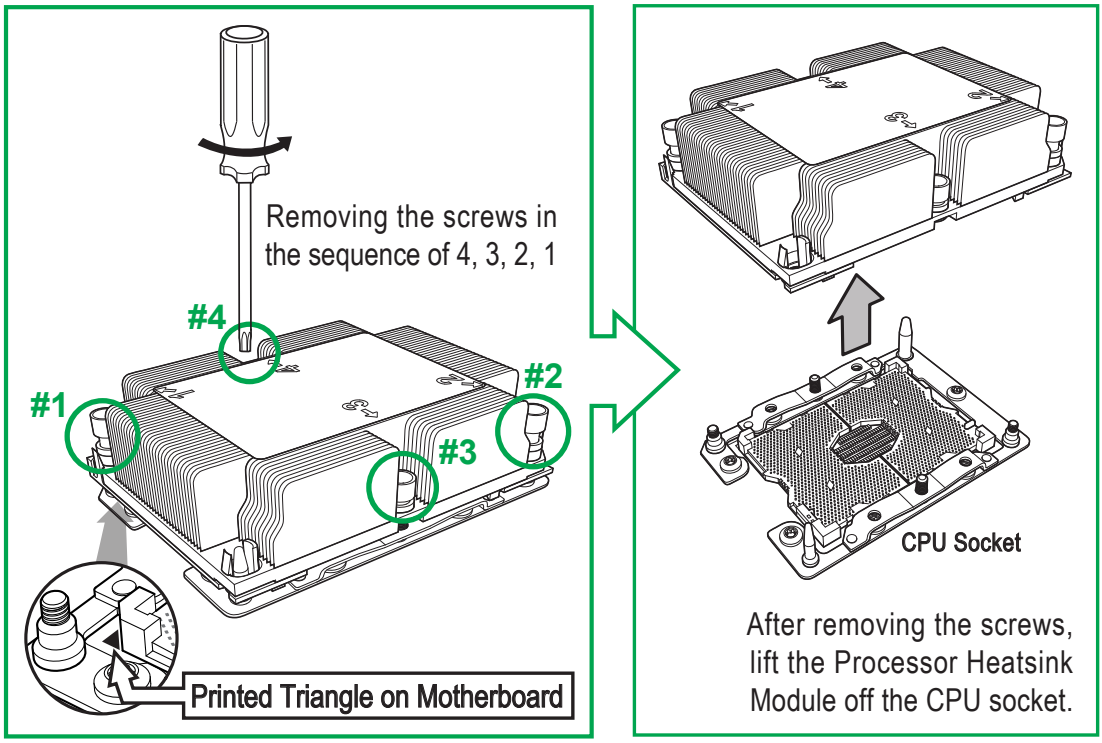
Tighten the screws in the sequence of 1, 2, 3, 4 (top 3 quarter view)

Removing the Processor Heatsink Module (PHM) from the Motherboard

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

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

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



Memory Support and Installation

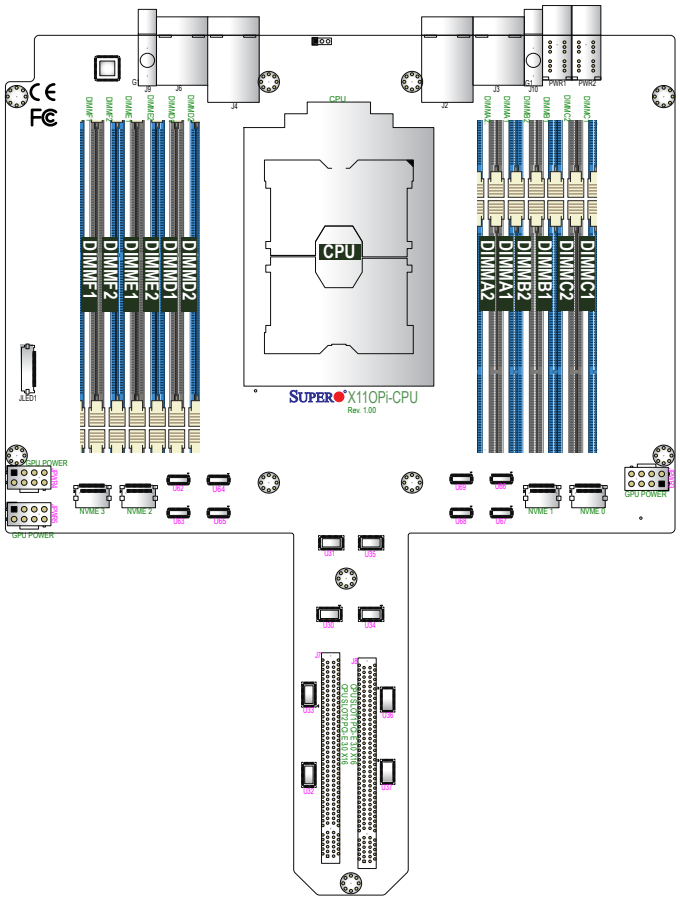
Note: Check the Supermicro website for recommended memory modules.

Memory Support

Each CPU board supports up to 3 TB DCPMM* or 3DS LRDIMM (Load Reduced)/ LRDIMM/3DS RDIMM (Regiestered)/RDIMM DDR4 memory of 2933*/2666/2400/2133 MHz in 12 DIMM slots. It also supports up to 4.5 TB DCPMM and DDR4 combined memory of up to 2933 MHz in 12 DIMM slots. With eight CPU boards installed, your system will support up to 24 TB of DCPMM/DDR4 memory or up to 36 TB DCPMM & DDR4 combined memory in 96 memory slots.

Notes: **1.** 2933 MHz memory and DCPMM Memory are supported by Second Generation Intel® Xeon® Platinum 82XX processors only. **2.** Populating DDR4 memory modules in a two-DIMMs per-channel (2DPC) configuration on this motherboard will affect memory bandwidth and performance. **3.** Mixing of memory modules of different types and speeds is not allowed. **4.** Memory speed support is dependent on the processors used in the system. For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.

Memory Slots



DDR4 Memory Support for Intel® Xeon® Platinum 8XXX 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)	
				2 Slots Per Channel	
		DRAM Density		1DPC (1-DIMM Per Channel)	2DPC (2-DIMM Per Channel)
		4Gb*	8Gb	1.2 V	1.2 V
RDIMM	SRx4	4GB	8GB	2666	2666
RDIMM	SRx8	8GB	16GB	2666	2666
RDIMM	DRx8	8GB	16GB	2666	2666
RDIMM	DRx4	16GB	32GB	2666	2666
RDIMM 3Ds	QRX4	N/A	2H-64GB	2666	2666
RDIMM 3Ds	8RX4	N/A	4H-128GB	2666	2666
LRDIMM	QRx4	32GB	64GB	2666	2666
LRDIMM 3Ds	QRX4	N/A	2H-64GB	2666	2666
LRDIMM 3Ds	8Rx4	N/A	4H-128GB	2666	2666

DDR4 Memory Support for 2nd Gen Intel® Xeon® Platinum 82XX 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)	
					2 Slots Per Channel	
		DRAM Density			1DPC (1-DIMM Per Channel)	2DPC (2-DIMM Per Channel)
		4Gb*	8Gb	16Gb	1.2 V	1.2 V
RDIMM	SRx4	4GB	8GB	16GB	2933	2933
RDIMM	SRx8	8GB	16GB	32GB	2933	2933
RDIMM	DRx8	8GB	16GB	32GB	2933	2933
RDIMM	DRx4	16GB	32GB	64GB	2933	2933
RDIMM 3Ds	QRX4	N/A	2H-64GB	2H-128GB	2933	2933
RDIMM 3Ds	8RX4	N/A	4H-128GB	4H-256GB	2933	2933
LRDIMM	QRx4	32GB	64GB	128GB	2933	2933
LRDIMM 3Ds	QRX4	N/A	2H-64GB	2H-128GB	2933	2933
LRDIMM 3Ds	8Rx4	N/A	4H-128GB	4H-256GB	2933	2933

Notes: **1.** 2933 MHz memory support in two-DIMMs per-channel (2DPC) configuration can be achieved by using memory purchased from Supermicro. **2.** 2933 MHz memory is supported by the Second Generation Intel® Xeon® Platinum 82XX processor only.

DIMM Population Guidelines for Optimal Performance

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

Key Parameters for DIMM Configuration

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

DIMM Mixing Guidelines

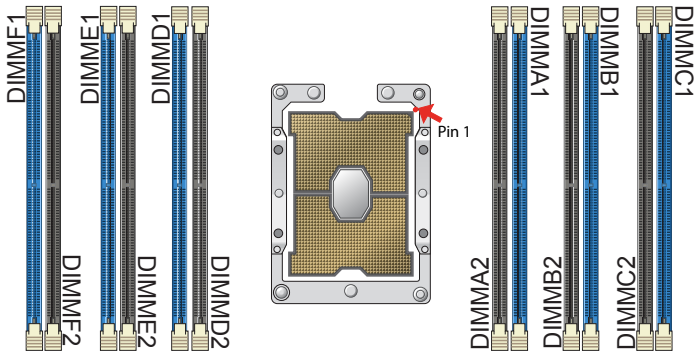
General DIMM Mixing Guidelines
DIMM Mixing Rules
• All DIMMs must be all DDR4 or DCPMM DIMMs. • x4 and x8 DIMMs can be mixed in the same channel. • Mixing of LRDIMMs and RDIMMs is not allowed in the same channel, across different channels, and across different sockets. • Mixing of non-3DS and 3DS LRDIMM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

Note: The drawing above shows DIMM module population for each CPU Board installed in your system. Please install your processors starting with CPU Board #1.

Memory Population Table

DCPMM Population Table (X11OPi+ w/8 CPU Boards & 96 DIMMs Installed)	
8 CPU boards & 96 DIMMs (12 DIMMs per CPU board)	**Memory Population Sequence**
CPU Board 1 + 12 DIMMs	CPU1: P1-DIMMC1/P1-DIMMC2/P1-DIMMB1/P1-DIMMB2/P1-DIMMA1/P1-DIMMA2/ P1-DIMMD2/P1-DIMMD1/P1-DIMME2/P1-DIMME1/P1-DIMMF2/P1-DIMMF1
CPU Board 2 + 12 DIMMs	CPU2: P2-DIMMC1/P2-DIMMC2/P2-DIMMB1/P2-DIMMB2/P2-DIMMA1/P2-DIMMA2/ P2-DIMMD2/P2-DIMMD1/P2-DIMME2/P2-DIMME1/P2-DIMMF2/P2-DIMMF1
CPU Board 3 + 12 DIMMs	CPU3: P3-DIMMC1/P3-DIMMC2/P3-DIMMB1/P3-DIMMB2/P3-DIMMA1/P3-DIMMA2/ P3-DIMMD2/P3-DIMMD1/P3-DIMME2/P3-DIMME1/P3-DIMMF2/P3-DIMMF1
CPU Board 4 + 12 DIMMs	CPU4: P4-DIMMC1/P4-DIMMC2/P4-DIMMB1/P4-DIMMB2/P4-DIMMA1/P4-DIMMA2/ P4-DIMMD2/P4-DIMMD1/P4-DIMME2/P4-DIMME1/P4-DIMMF2/P4-DIMMF1
CPU Board 5 + 12 DIMMs	CPU5: P5-DIMMC1/P5-DIMMC2/P5-DIMMB1/P5-DIMMB2/P5-DIMMA1/P5-DIMMA2/ P5-DIMMD2/P5-DIMMD1/P5-DIMME2/P5-DIMME1/P5-DIMMF2/P5-DIMMF1
CPU Board 6 + 12 DIMMs	CPU6: P6-DIMMC1/P6-DIMMC2/P6-DIMMB1/P6-DIMMB2/P6-DIMMA1/P6-DIMMA2/ P6-DIMMD2/P6-DIMMD1/P6-DIMME2/P6-DIMME1/P6-DIMMF2/P6-DIMMF1
CPU Board 7 + 12 DIMMs	CPU7: P7-DIMMC1/P7-DIMMC2/P7-DIMMB1/P7-DIMMB2/P7-DIMMA1/P7-DIMMA2/ P7-DIMMD2/P7-DIMMD1/P7-DIMME2/P7-DIMME1/P7-DIMMF2/P7-DIMMF1
CPU Board 8 + 12 DIMMs	CPU8: P8-DIMMC1/P8-DIMMC2/P8-DIMMB1/P8-DIMMB2/P8-DIMMA1/P8-DIMMA2/ P8-DIMMD2/P8-DIMMD1/P8-DIMME2/P8-DIMME1/P8-DIMMF2/P8-DIMMF1



Note: The drawing above shows DIMM module population for each CPU Board installed in your system. Please install your processors starting with CPU Board #1.

Symmetric Population												
2-1-1	**(For Channel Configuration: 2-1-1)**											
Modes												
CPU1	**P1-DIMMF1**	**P1-DIMMF2**	**P1-DIMME1**	**P1-DIMME2**	**P1-DIMMD1**	**P1-DIMMD2**	**P1-DIMMA2**	**P1-DIMMA1**	**P1-DIMMB2**	**P1-DIMMB1**	**P1-DIMMC2**	**P1-DIMMC1**
AD	DRAM1	-	DRAM1	-	DRAM1	***DCPMM***	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
MM	DRAM2	-	DRAM2	-	DRAM2	***DCPMM***	***DCPMM***	DRAM2	-	DRAM2	-	DRAM2
AD + MM	DRAM3	-	DRAM3	-	DRAM3	***DCPMM***	***DCPMM***	DRAM3	-	DRAM3	-	DRAM3
CPU2	**P2-DIMMF1**	**P2-DIMMF2**	**P2-DIMME1**	**P2-DIMME2**	**P2-DIMMD1**	**P2-DIMMD2**	**P2-DIMMA2**	**P2-DIMMA1**	**P2-DIMMB2**	**P2-DIMMB1**	**P2-DIMMC2**	**P2-DIMMC1**
AD	DRAM1	-	DRAM1	-	DRAM1	***DCPMM***	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
MM	DRAM2	-	DRAM2	-	DRAM2	***DCPMM***	***DCPMM***	DRAM2	-	DRAM2	-	DRAM2
AD + MM	DRAM3	-	DRAM3	-	DRAM3	***DCPMM***	***DCPMM***	DRAM3	-	DRAM3	-	DRAM3
CPU3	**P3-DIMMF1**	**P3-DIMMF2**	**P3-DIMME1**	**P3-DIMME2**	**P3-DIMMD1**	**P3-DIMMD2**	**P3-DIMMA2**	**P3-DIMMA1**	**P3-DIMMB2**	**P3-DIMMB1**	**P3-DIMMC2**	**P3-DIMMC1**
AD	DRAM1	-	DRAM1	-	DRAM1	***DCPMM***	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
MM	DRAM2	-	DRAM2	-	DRAM2	***DCPMM***	***DCPMM***	DRAM2	-	DRAM2	-	DRAM2
AD + MM	DRAM3	-	DRAM3	-	DRAM3	***DCPMM***	***DCPMM***	DRAM3	-	DRAM3	-	DRAM3
CPU4	**P4-DIMMF1**	**P4-DIMMF2**	**P4-DIMME1**	**P4-DIMME2**	**P4-DIMMD1**	**P4-DIMMD2**	**P4-DIMMA2**	**P4-DIMMA1**	**P4-DIMMB2**	**P4-DIMMB1**	**P4-DIMMC2**	**P4-DIMMC1**
AD	DRAM1	-	DRAM1	-	DRAM1	***DCPMM***	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
MM	DRAM2	-	DRAM2	-	DRAM2	***DCPMM***	***DCPMM***	DRAM2	-	DRAM2	-	DRAM2
AD + MM	DRAM3	-	DRAM3	-	DRAM3	***DCPMM***	***DCPMM***	DRAM3	-	DRAM3	-	DRAM3

Symmetric Population													
2-2-1	**(For Channel Configuration: 2-2-1)**												
Modes													
CPU1	**P1-DIMMF1**	**P1-DIMMF2**	**P1-DIMME1**	**P1-DIMME2**	**P1-DIMMD1**	**P1-DIMMD2**	**P1-DIMMA2**	**P1-DIMMA1**	**P1-DIMMB2**	**P1-DIMMB1**	**P1-DIMMC2**	**P1-DIMMC1**	
AD	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
MM	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
AD + MM	DRAM3	-	DRAM3	***DCPMM***	DRAM3	***DCPMM***	***DCPMM***	DRAM3	***DCPMM***	DRAM3	-	DRAM3	
AD	***DCPMM***	-	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	-	***DCPMM***	**2-2-1**
CPU2	**P2-DIMMF1**	**P2-DIMMF2**	**P2-DIMME1**	**P2-DIMME2**	**P2-DIMMD1**	**P2-DIMMD2**	**P2-DIMMA2**	**P2-DIMMA1**	**P2-DIMMB2**	**P2-DIMMB1**	**P2-DIMMC2**	**P2-DIMMC1**	
AD	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
MM	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
AD + MM	DRAM3	-	DRAM3	***DCPMM***	DRAM3	***DCPMM***	***DCPMM***	DRAM3	***DCPMM***	DRAM3	-	DRAM3	
AD	***DCPMM***	-	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	-	***DCPMM***	**2-2-1**
CPU3	**P3-DIMMF1**	**P3-DIMMF2**	**P3-DIMME1**	**P3-DIMME2**	**P3-DIMMD1**	**P3-DIMMD2**	**P3-DIMMA2**	**P3-DIMMA1**	**P3-DIMMB2**	**P3-DIMMB1**	**P3-DIMMC2**	**P3-DIMMC1**	
AD	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
MM	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
AD + MM	DRAM3	-	DRAM3	***DCPMM***	DRAM3	***DCPMM***	***DCPMM***	DRAM3	***DCPMM***	DRAM3	-	DRAM3	
AD	***DCPMM***	-	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	-	***DCPMM***	**2-2-1**
CPU4	**P4-DIMMF1**	**P4-DIMMF2**	**P4-DIMME1**	**P4-DIMME2**	**P4-DIMMD1**	**P4-DIMMD2**	**P4-DIMMA2**	**P4-DIMMA1**	**P4-DIMMB2**	**P4-DIMMB1**	**P4-DIMMC2**	**P4-DIMMC1**	
AD	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
MM	DRAM1	-	DRAM1	***DCPMM***	DRAM1	***DCPMM***	***DCPMM***	DRAM1	***DCPMM***	DRAM1	-	DRAM1	
AD + MM	DRAM3	-	DRAM3	***DCPMM***	DRAM3	***DCPMM***	***DCPMM***	DRAM3	***DCPMM***	DRAM3	-	DRAM3	
AD	***DCPMM***	-	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	DRAM1	-	***DCPMM***	**2-2-1**

Symmetric Population												
1-1-1	(For Channel Configuration: 1-1-1)											
Modes												
CPU1	P1-DIMMF1	P1-DIMMF2	P1-DIMME1	P1-DIMME2	P1-DIMMD1	P1-DIMMD2	P1-DIMMA2	P1-DIMMA1	P1-DIMMB2	P1-DIMMB1	P1-DIMMC2	P1-DIMMC1
AD	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
MM	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
AD + MM	***DCPMM***	-	DRAM3	-	DRAM3	-	-	DRAM3	-	DRAM3	-	***DCPMM***
CPU2	P2-DIMMF1	P2-DIMMF2	P2-DIMME1	P2-DIMME2	P2-DIMMD1	P2-DIMMD2	P2-DIMMA2	P2-DIMMA1	P2-DIMMB2	P2-DIMMB1	P2-DIMMC2	P2-DIMMC1
AD	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
MM	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
AD + MM	***DCPMM***	-	DRAM3	-	DRAM3	-	-	DRAM3	-	DRAM3	-	***DCPMM***
CPU3	P3-DIMMF1	P3-DIMMF2	P3-DIMME1	P3-DIMME2	P3-DIMMD1	P3-DIMMD2	P3-DIMMA2	P3-DIMMA1	P3-DIMMB2	P3-DIMMB1	P3-DIMMC2	P3-DIMMC1
AD	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
MM	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
AD + MM	***DCPMM***	-	DRAM3	-	DRAM3	-	-	DRAM3	-	DRAM3	-	***DCPMM***
CPU4	P4-DIMMF1	P4-DIMMF2	P4-DIMME1	P4-DIMME2	P4-DIMMD1	P4-DIMMD2	P4-DIMMA2	P4-DIMMA1	P4-DIMMB2	P4-DIMMB1	P4-DIMMC2	P4-DIMMC1
AD	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
MM	***DCPMM***	-	DRAM1	-	DRAM1	-	-	DRAM1	-	DRAM1	-	***DCPMM***
AD + MM	***DCPMM***	-	DRAM3	-	DRAM3	-	-	DRAM3	-	DRAM3	-	***DCPMM***

Asymmetric Population												
2/1-1-1	(For Channel Configuration: 2/1-1-1)											
Modes												
CPU1	P1-DIMMF1	P1-DIMMF2	P1-DIMME1	P1-DIMME2	P1-DIMMD1	P1-DIMMD2	P1-DIMMA2	P1-DIMMA1	P1-DIMMB2	P1-DIMMB1	P1-DIMMC2	P1-DIMMC1
AD	DRAM1	-	DRAM1	-	DRAM1	-	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
CPU2	P2-DIMMF1	P2-DIMMF2	P2-DIMME1	P2-DIMME2	P2-DIMMD1	P2-DIMMD2	P2-DIMMA2	P2-DIMMA1	P2-DIMMB2	P2-DIMMB1	P2-DIMMC2	P2-DIMMC1
AD	DRAM1	-	DRAM1	-	DRAM1	-	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
CPU3	P3-DIMMF1	P3-DIMMF2	P3-DIMME1	P3-DIMME2	P3-DIMMD1	P3-DIMMD2	P3-DIMMA2	P3-DIMMA1	P3-DIMMB2	P3-DIMMB1	P3-DIMMC2	P3-DIMMC1
AD	DRAM1	-	DRAM1	-	DRAM1	-	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1
CPU4	P4-DIMMF1	P4-DIMMF2	P4-DIMME1	P4-DIMME2	P4-DIMMD1	P4-DIMMD2	P4-DIMMA2	P4-DIMMA1	P4-DIMMB2	P4-DIMMB1	P4-DIMMC2	P4-DIMMC1
AD	DRAM1	-	DRAM1	-	DRAM1	-	***DCPMM***	DRAM1	-	DRAM1	-	DRAM1

Legend (for the five tables above)					
	DDR4 Type				Capacity
DRAM1	RDIMM	3DS RDIMM	LRDIMM	3DS LRDIMM	Refer to Validation Matrix (DDR4 DIMMs validated with DCPMM) on the next page.
DRAM2	RDIMM	-		-	
DRAM3	RDIMM	3DS RDIMM	LRDIMM	-	

Note: DDR4 single rank DIMMs based on x8 devices are not compatible with any DCPMM operating mode.

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

- For MM, general NM/FM ratio is between 1:4 and 1:16. Excessive capacity for FM can be used for AD. (NM = Near Memory; FM = Far Memory)
- For each individual population, rearrangements between channels are allowed as long as the resulting population is compliant with the X11 memory population rules for the 2nd Gen Intel® Xeon® Platinum 82XX processors.
- For each individual population, please use the same DDR4 DIMM in all slots.
- For each individual population, sockets are normally symmetric with exceptions for 1 DCPMM per socket and 1 DCPMM per node case.
- No mixing of DCPMM and NVMDIMMs within the same platform is allowed.
- This DCPMM population guide targets a balanced DCPMM-to-DRAM-cache ratio in MM and MM + AD modes.

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

Memory Rank Sparing Tables

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

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

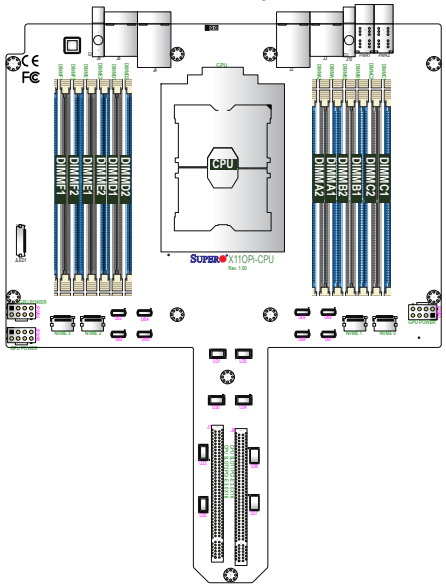
Installing DIMM Modules on the X11OPi-CPU Board

CAUTION

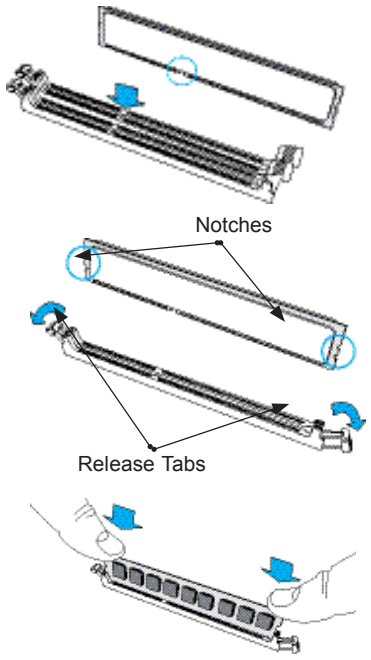
Exercise extreme care when installing or removing DIMM modules to prevent any possible damage. Check Supermicro's website for recommended memory modules.

1. Install the desired number of DIMM modules on the CPU board; each board supports up to 12 DIMMs. When installing memory, be sure to always populate the blue slots first, starting with DIMMA1, DIMMB1, DIMMC1, DIMMD1, DIMME1, and DIMMF1. For best performance, please use the memory modules of the same type and same speed in the same bank. For DIMM module locations, please refer to the layout below.

X11OPi-CPU Memory Support
DIMMA1/A2, DIMMB1/B2
DIMMC1/C2, DIMMD1/D2
DIMME1/E2, DIMMF1/F2



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 with the receptive points on the ends of the slot. Use two thumbs together to press module straight down into the slot until the module snaps into place.
5. Press the release tabs to the lock positions to lock the DIMM module into the slot.



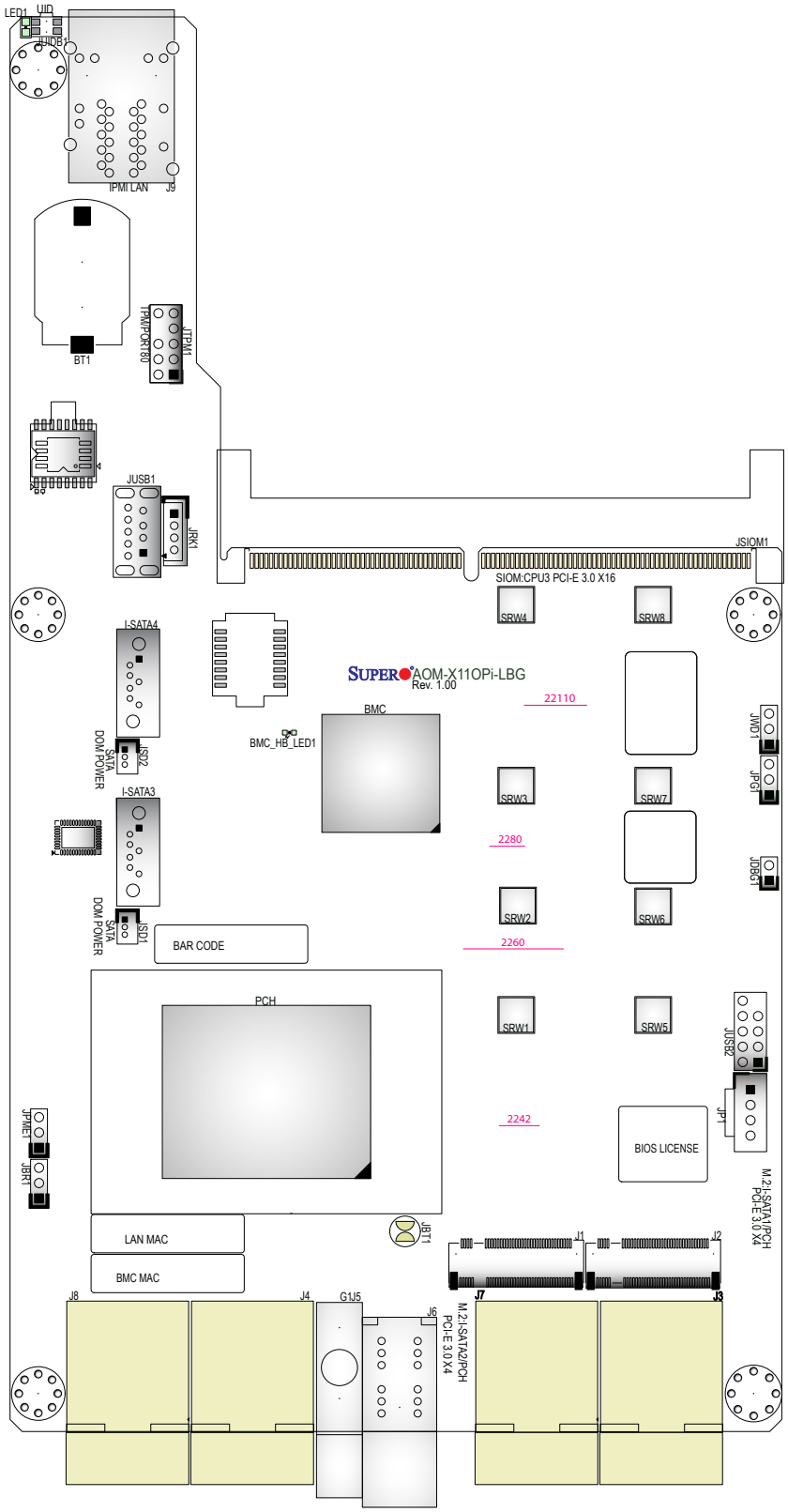
Note: Press the memory straight down into the slot until it is properly seated.

1-3 The AOM-X11OPi-LBG Card

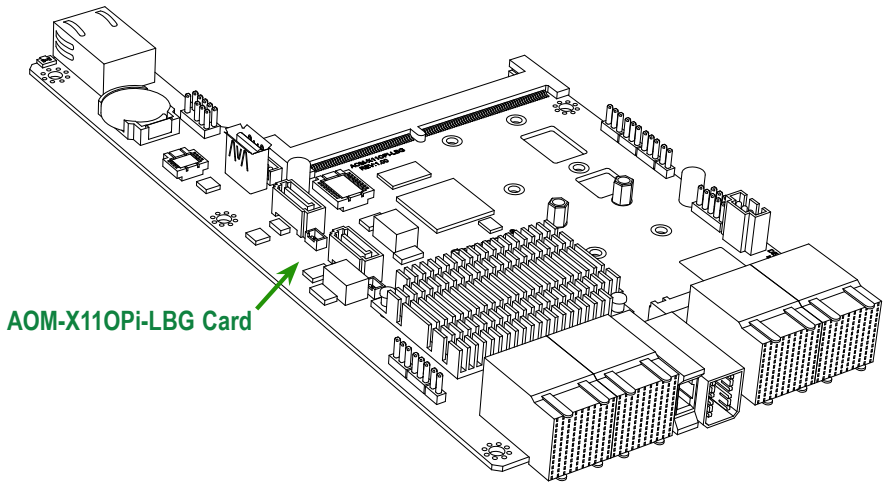
Your system comes with the AOM-X11OPi-LBG card, which is to be installed on the BPN-X11OPi midplane. This section provides the information on the Intel C621 chipset add-on module.

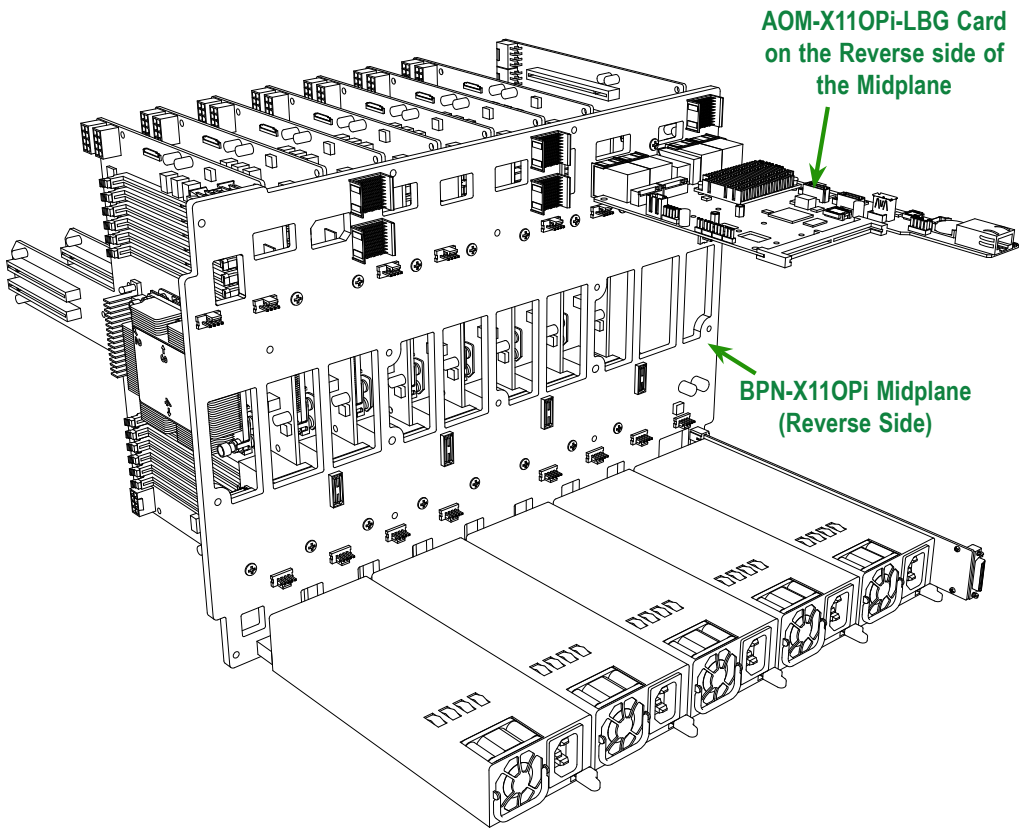
AOM-X11OPi-LBG Image

AOM-X11OPi-LBG Layout



Location of the AOM-X11OPi-LBG Card



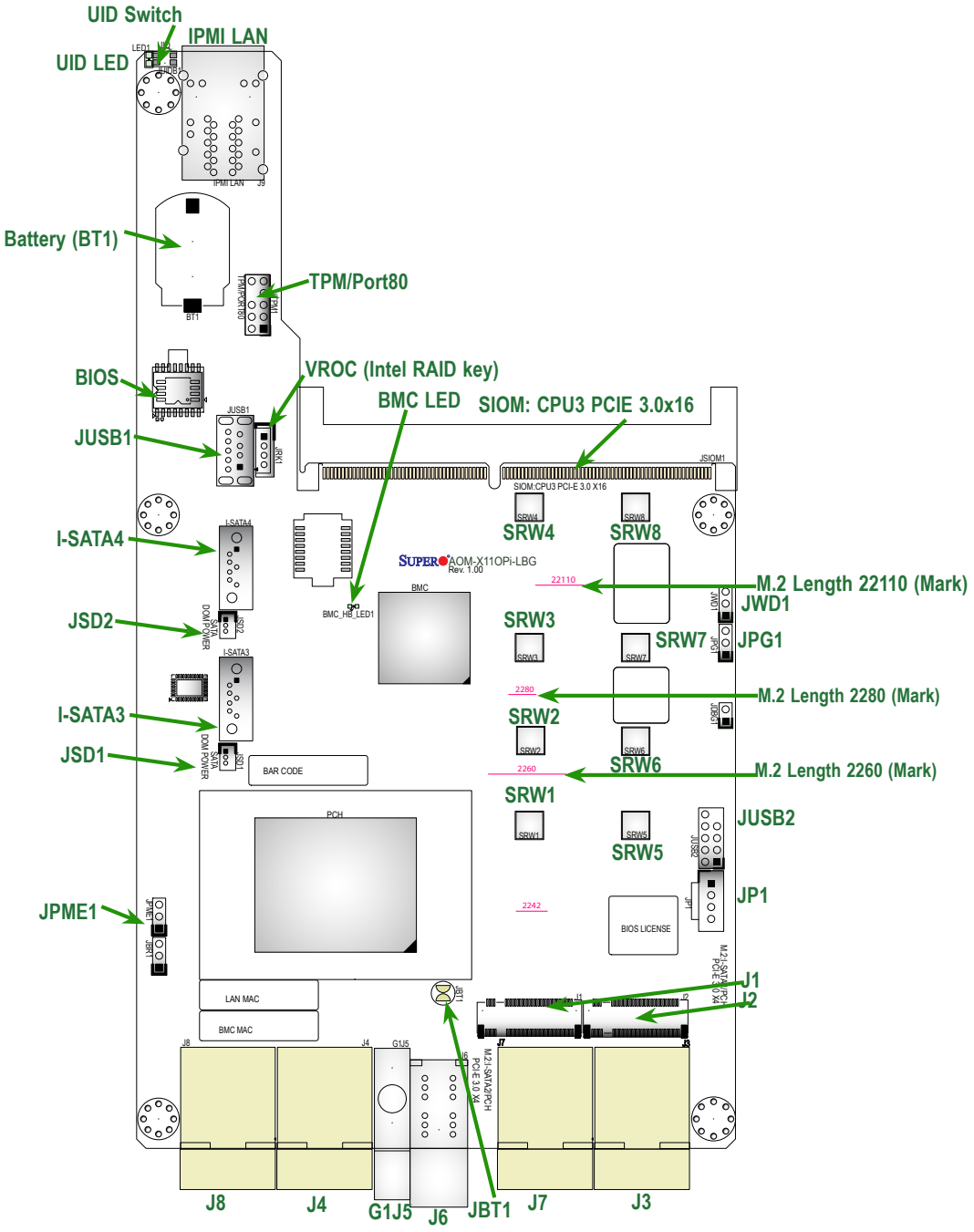


AOM-X11OPi-LBG Card on the Reverse Side of the X11OPi Midplane

Major Components on the AOM-X11OPi-LBG Card

This section provides detailed information of the major components on the AOM-X11OPi-LBG card.

AOM-X11OPi-LBG Layout



AOM-X11OPi-LBG I/O Connector Image

Note: M.2 modules come with 3 sizes in length. Horizontal lines marked "2260", "2280", "22110" on the layout above indicate the locations where M.2 modules should be installed depending on the sizes in length.

Quick Reference to the Components on the AOM-X11OPi-LBG

Jumpers on the AOM-X11OPi-LBG

Jumper	Description	Default Setting
JBT1	Clear CMOS	(See Note 1 below.)
JPME1	ME Manufacturing Mode Select	Pins 1-2 (Normal) (Note 1 below.)
JWD1	Watch Dog Timer Enable	Pins 1-2 (Reset) (Note 1 below.)

Connectors on the AOM-X11OPi-LBG

Connector	Description
Battery (BT1)	Onboard CMOS Battery (See Chpt. 3 for used battery disposal)
I-SATA3	Powered SATA 3.0 connector with a power pin built-in. (SuperDOM) supported by Intel PCH (See Note 2 below.)
I-SATA4	Powered SATA 3.0 connector with a power pin built-in. (SuperDOM) supported by Intel PCH (See Note 2 below.)
IPMI LAN	IPMI-dedicated LAN (J9) supported by the Baseboard Management Controller (BMC) (See Note 2 below.)
J1	M.2 connector used for SATA 3.0 or PCI-E 3.0 x4 support (Mounting hole locations: SWR1/SWR2/ SWR3/SWR4) (See Note 3 below.)
J2	M.2 connector used for SATA 3.0 or PCI-E 3.0 x4 support (Mounting hole locations: SWR5/SWR6/ SWR7/SWR8) (See Note 3 below.)
J5	Guide pin
J6	Power connector
JP1	DVD ROM power header (optional)
JSD1/JSD2	Power Connectors 1/2 for I-SATA DOM (Disk_on_Module) devices (See Note 2 below.)
JSIOM1	SIOM (Super I/O Module) PCI-E 3.0 x16 slot supported by CPU3 for use of a Supermicro-proprietary add-on card
JTPM1	TPM (Trusted Platform Module)/Port 80 header (See Note 2 below.)
JUSB1	Type A USB 3.0 header with support of USB 3.0 Port1, USB 2.0 Port2
JUSB2	USB 2.0 header with support of USB 5/USB 6
JUIDB1	UID (Unit Identification) button (See Note 2 below.)
VROC (JRK1)	Intel VROC RAID key header for NVMe SSD

LED Indicators on the AOM-X11OPi-LBG

LED	Description
BMC_HB_LED1	BMC Heartbeat LED indicator (Green Blinking: BMC Normal)
LED1	Unit Identifier LED indicator (Blue: Unit Identified) (See Note 2 below.)

Note 1: Please see next page for more jumper information.

Note 2: Please see the Connectors section for more information.

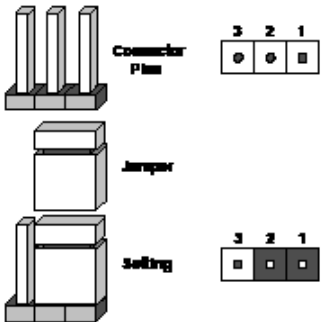
Note 3: M.2 modules come with 3 sizes in length. Horizontal lines marked "2260", "2280", "22110" on the layout on the previous page indicate the locations where M.2 modules should be installed depending on the sizes of the M.2 modules.

Jumpers and Connectors on the AOM-X11OPi-LBG

How Jumpers Work

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

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



CMOS Clear

JBT1 is used to clear the CMOS. Instead of pins, this "jumper" consists of contact pads to prevent the accidental clearing of the CMOS. To clear the CMOS, use a metal object such as a small screwdriver to touch both pads at the same time to short the connection. Always remove the AC power cord from the system before clearing the CMOS.

Note 1: For an ATX power supply, you must completely shut down the system, remove the AC power cord, and then short JBT1 to clear the CMOS.

Note 2: Be sure to remove the onboard CMOS Battery before you short JBT1 to clear the CMOS. Clearing the CMOS will also clear any passwords.

Do not use the PW_ON connector to clear CMOS.

JBT1 contact pads

Manufacturer Mode Select

Close pin 2 and pin 3 of Jumper JPME1 to bypass SPI flash security and force the system to operate in the Manufacturer mode, allowing the user to flash the system firmware from a host server for system-setting modifications. Refer to the table below for jumper settings.

ME Mode Select Jumper Settings	
Jumper Setting	**Definition**
1-2	Normal (Default)
2-3	Manufacturer Mode

Watch Dog Enable/Disable

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

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

Headers and Connectors

I-SATA 3/I-SATA 4 & Disk-on-Module Connectors

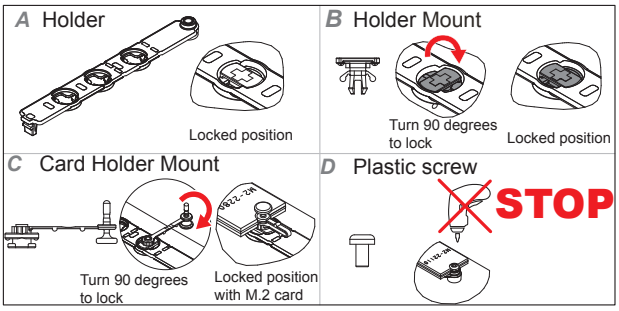
Two yellow SATA 3.0 compatible connectors (I-SATA 3 & I-SATA 4), driven by Intel C621 chipset, support two DOM storage devices. These modified SATA connectors have two power pins that allow Supermicro supplied DOM devices to operate without any extra power cables. For DOM devices that require external power, two extra two pin headers placed right next to I-SATA ports, are available. They are labeled JSD1 and JSD2.

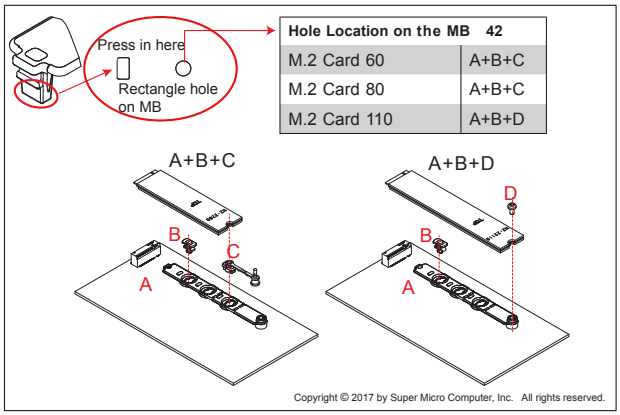
SATA 3.0 Pin Definitions

Pin#	Definition
1	Ground
2	TX_P
3	TX_N
4	Ground
5	RX_N
6	RX_P
7	Ground
8	Power
9	Ground

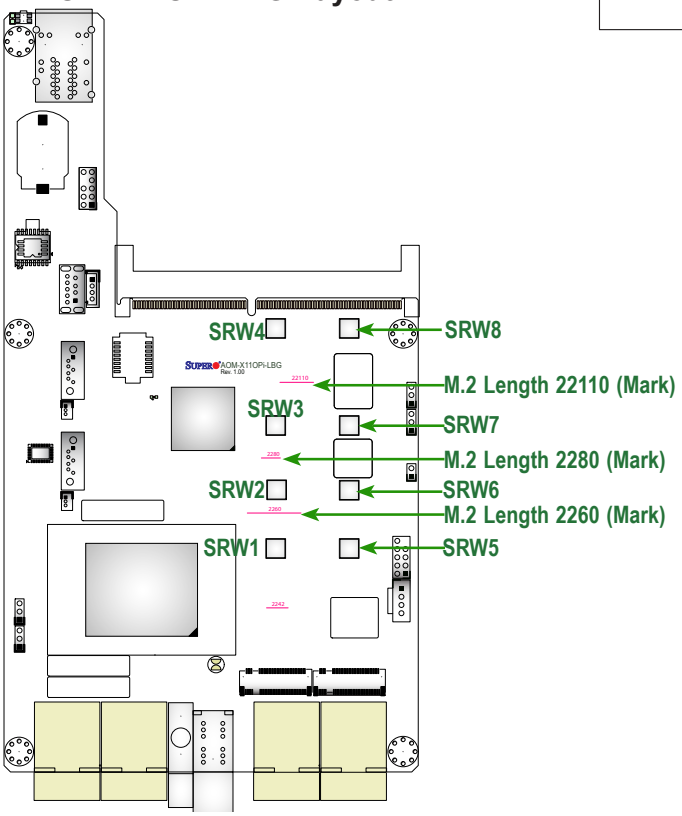
J1/J2 & M.2 Storage Module Connectors

Two M.2 connectors (J1/J2) provide support for two M.2 SSD storage modules. These connectors are keyed for PCIe 3.0 x4 and SATA 3.0 connectivity. The X11OPi-LBG board provides mounting holes for three lengths of M2 modules: 2260, 2280 and 22110 standards. Typically, these connectors are populated with the M.2 SSD in a RAID 1 configuration, containing a bootable Operating System. These connectors comply with PCI Express M.2





AOM-X11OPi-LBG Layout



Note 1: Moulding holes: SWR1 to SWR4 are used for the M.2 module located at J1.

Note 2: Moulding holes: SWR5 to SWR8 are used for the M.2 module located at J2.

Note 3: M.2 modules come with 3 sizes in length. Horizontal lines marked "2260", "2280", "22110" on the LBG layout indicate the locations where M.2 modules should be installed depending on the sizes of the modules. Please refer to the drawings above for M.2 installation instructions.

Universal Serial Bus (USB)

An internal USB header, located at JUSB1, provides two USB 2.0 connections (USB 5/USB6) for your system. In addition, a Type A 3.0 header (JUSB2) also provides USB 3.0 Port 1 and USB 2.0 Port 2 connections for internal access. (Cables are not included). See the tables below for pin definitions.

Type A USB 3.0 (USB1)/USB 2.0 (USB2) Pin Definitions

Pin#	Definition
1	VBUS
2	USB_PN1
3	USB_PP1
4	Ground
5	SSRX_N
6	SSRX_P
7	Ground
8	SSTX_N
9	SSTX_P

Front Panel USB (2.0) (USB 5/6) Pin Definitions

Pin#	Definition	Pin#	Definition
1	+5V	6	USB_PP6
2	+5V	7	Ground
3	USB_PN5	8	Ground
4	USB_PN6	9	Key
5	USB_PP5	10	OC

Unit Identifier Switch/LED

A Unit Identifier (UID) switch (JUIDB1) and an UID LED (indicator are located on the AOM-X11OPi-LBG. The UID LED (LED1) is located next to the UID switch. When you press the UID switch, the UID LED will be turned on. Press the UID switch again to turn it off. These UID indicator provide easy identification of a system unit that may be in need of service.

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

UID Switch Pin Definitions

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

DOM Power Connectors

Two power connectors for SATA DOM (Disk_On_Module) devices are located at JSD1/JSD2. Connect appropriate cables here to provide power support for your Serial Link DOM devices.

DOM PWR Pin Definitions

Pin#	Definition
1	+5V
2	Ground
3	Ground

TPM/Port 80 Header

A Trusted Platform Module (TPM)/Port 80 header is located at JTPM1 to provide TPM support and a Port 80 connection. Use this header to enhance system performance and data security. See the table below for pin definitions.

TPM/Port 80 Header Pin Definitions

Pin#	Definition	Pin#	Definition
1	+3.3V	6	Ground
2	SPI_CS_N	7	SPI_MOSI
3	TPM_REST		
4	SPI_MISO	9	+3V STBY
5	SPI_CLK	10	TPM_IRQ3.3

IPMI LAN

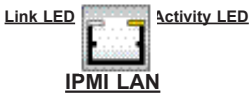
An IPMI_dedicated LAN, located on the AOM-X11OPi-LBG, provides KVM support for IPMI 2.0. This port accepts an RJ45_type cable.

IPMI LAN Activity LED (Right) LED State		
LED Color	**Status**	**Definition**
Yellow	Blinking	Active

IPMI LAN LED Indicators

The IPMI LAN has two LED indicators. The yellow LED on the right indicates activity, while the green LED on the left indicates the speed of the connection. Refer to the table below for LED settings.

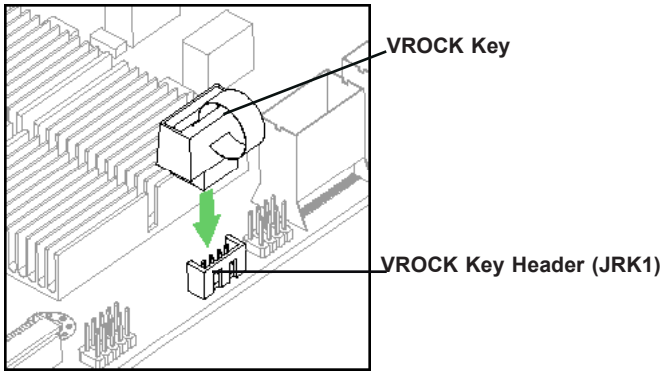
IPMI LAN Link LED (Left) LED State	
LED Color	**Definition**
Off	10 Mbps
Green	100 Mbps
Amber	1 Gbps



VROC RAID Key Header

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

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



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

LED Indicators

BMC Heartbeat LED

A BMC Heartbeat LED is located at BMC_HB_LED1 on the motherboard. When this LED is blinking, BMC functions normally. See the table below for more information.

BMC Heartbeat LED Status	
LED Color/State	**Definition**
Green: Blinking	BMC: Normal

UID LED

For UID LED (LED1), please refer to the UID Switch/LED section.

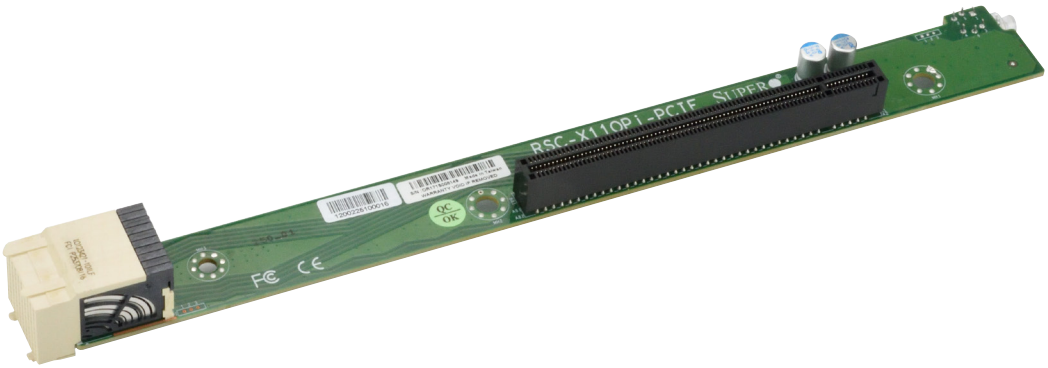
IPMI LAN LED Indicators

For IPMI LAN LED indicators, please refer to the IPMI LAN section.

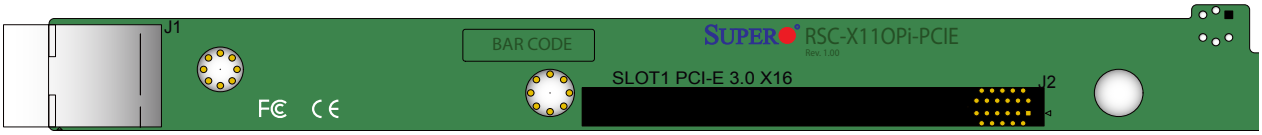
1-4 The RSC-X11OPi-PCIE Card

This section provides the information on the RSC-X11OPi-PCIE add-on card.

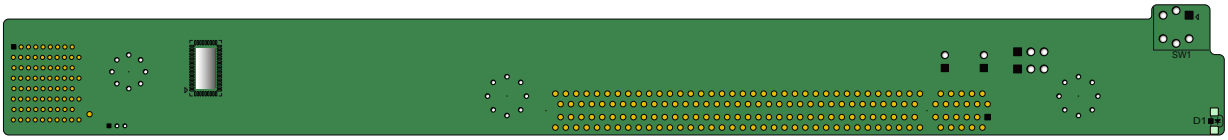
RSC-X11OPi-PCIE Card Image (Rev. 1.00)



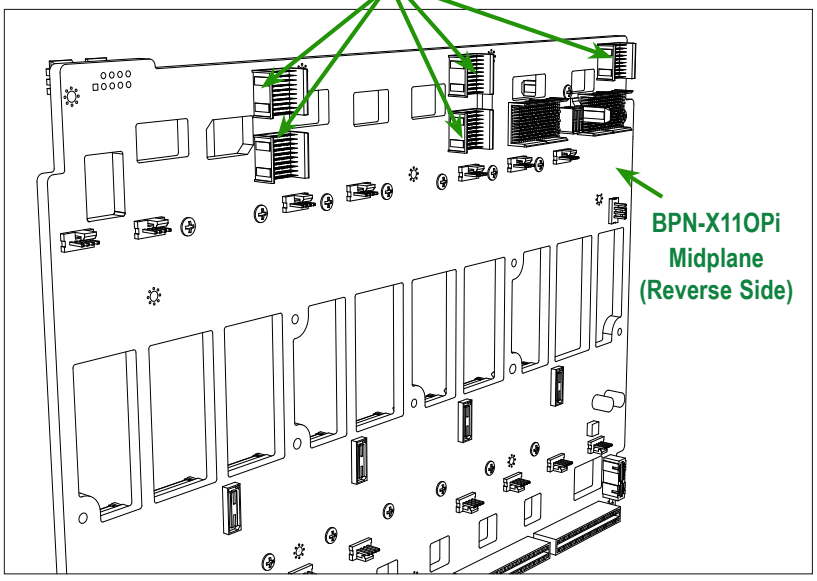
RSC-X11OPi-PCIE Card Layout (Front Side)



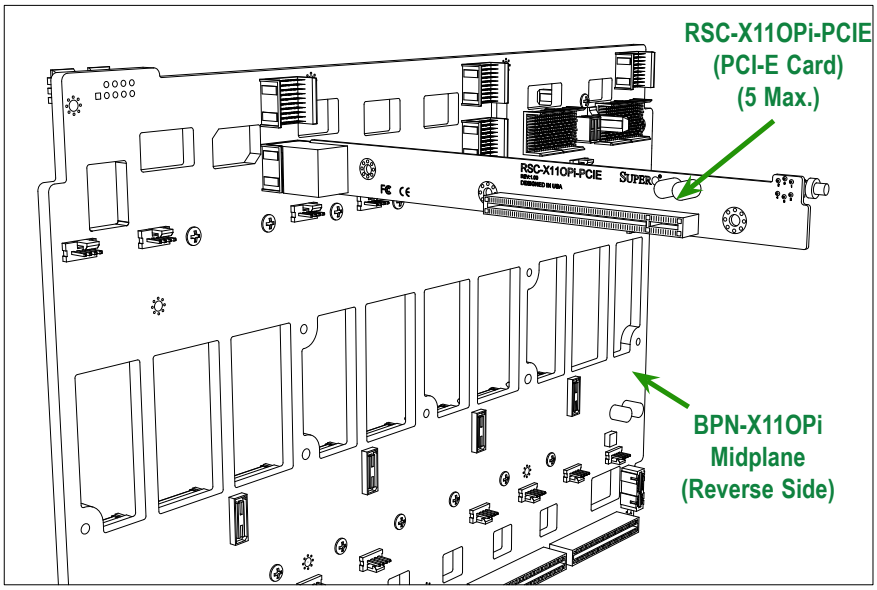
RSC-X11OPi-PCIE Card Layout (Reverse Side)



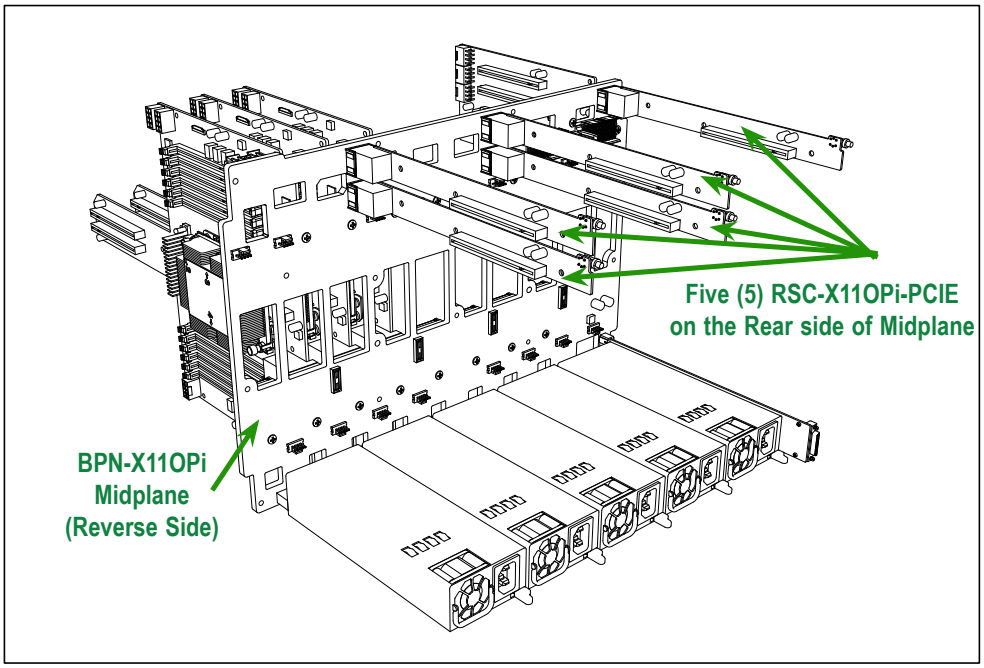
RSC-X11OPi-PCIE Connectors (5)



Location of the RSC-X11OPi-PCIE Cards

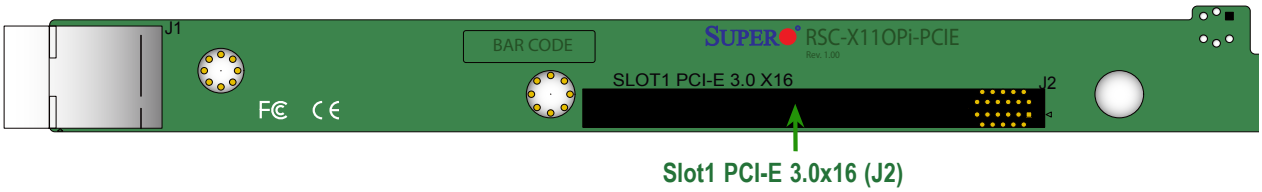


RSC-X11OPi-PCIE Card on the Reverse Side of the X11OPi Midplane (w/5 PCI-E Cards max.)

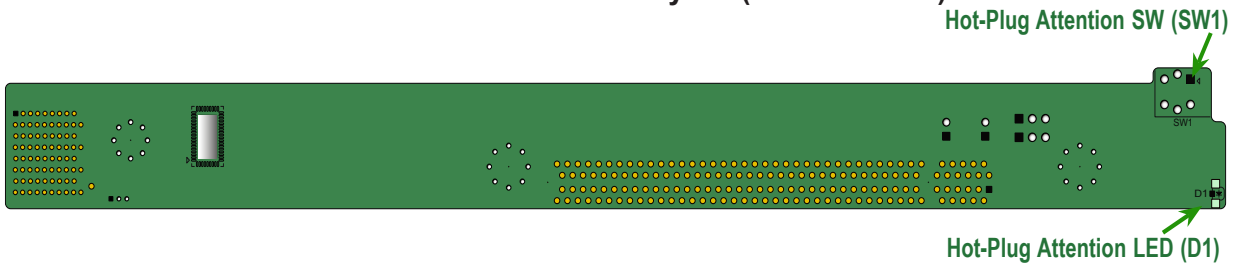


Major Components on the RSC-X11OPi-PCIE Card

RSC-X11OPi-PCIE Card Layout (Front)



RSC-X11OPi-PCIE Card Layout (Reverse Side)



Major Components on the RSC-X11OPi-PCIE

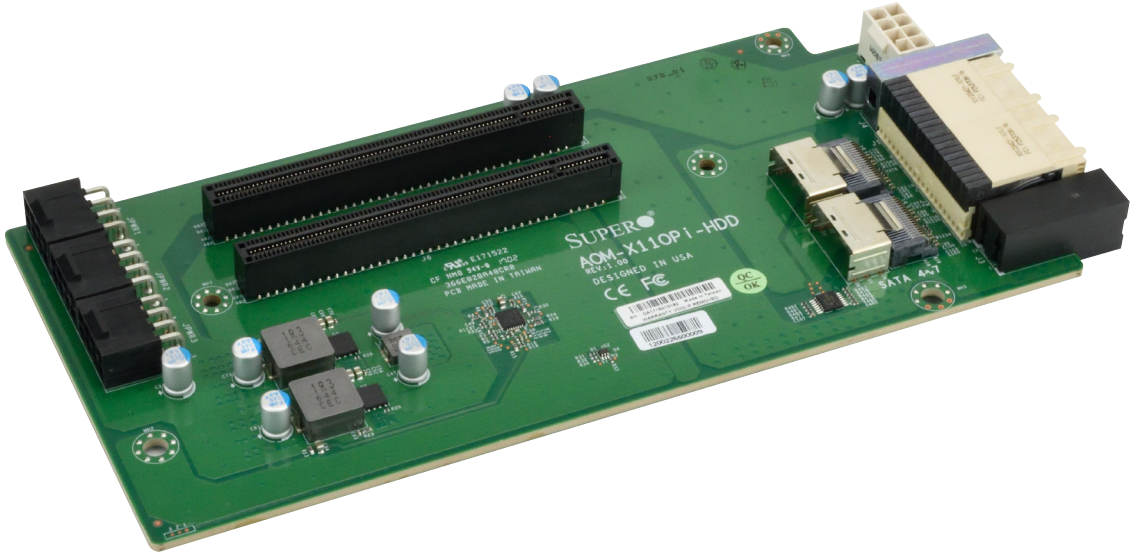
Major Components on the RSC-X11OPi-PCIE

Location	Description	Detailed Description
Front Side	J2	PCI-E Slot1: PCI-E 3.0 x16 slot
Reverse Side	SW1	Hot-plug attention button
Reverse Side	D1	Hot-plug attention LED (Orange: Hot-plug support needs attention)

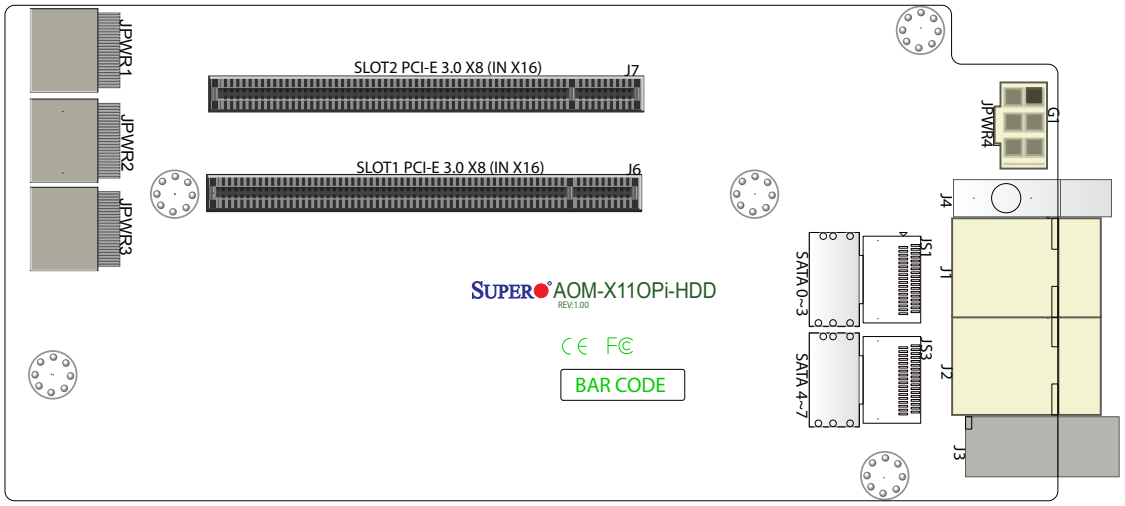
1-5 The AOM-X11OPi-HDD Card

This section provides the information on the AOM-X11OPi-HDD add-on card.

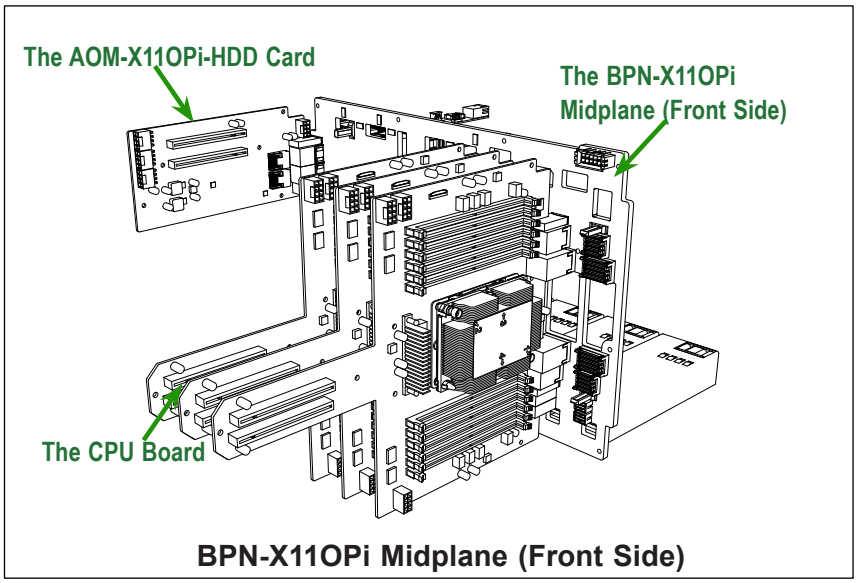
AOM-X11OPi-HDD Image (Rev. 1.00)



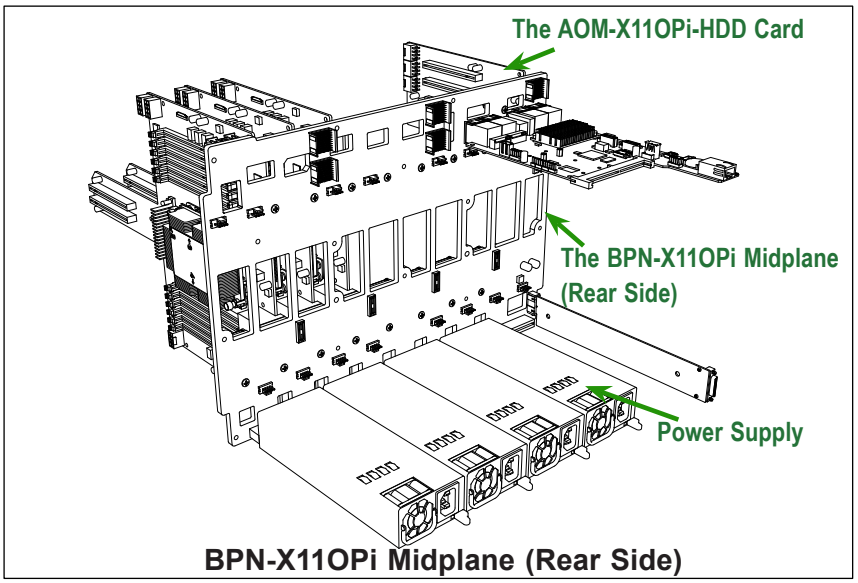
AOM-X11OPi-HDD Layout



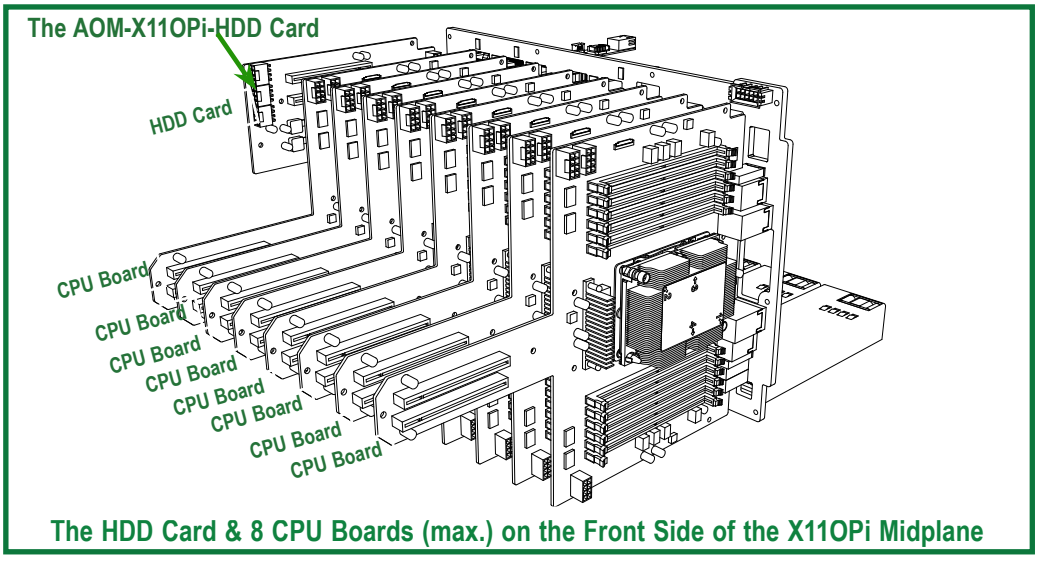
Location of the AOM-X11OPi-HDD Card



BPN-X11OPi Midplane (Front Side)

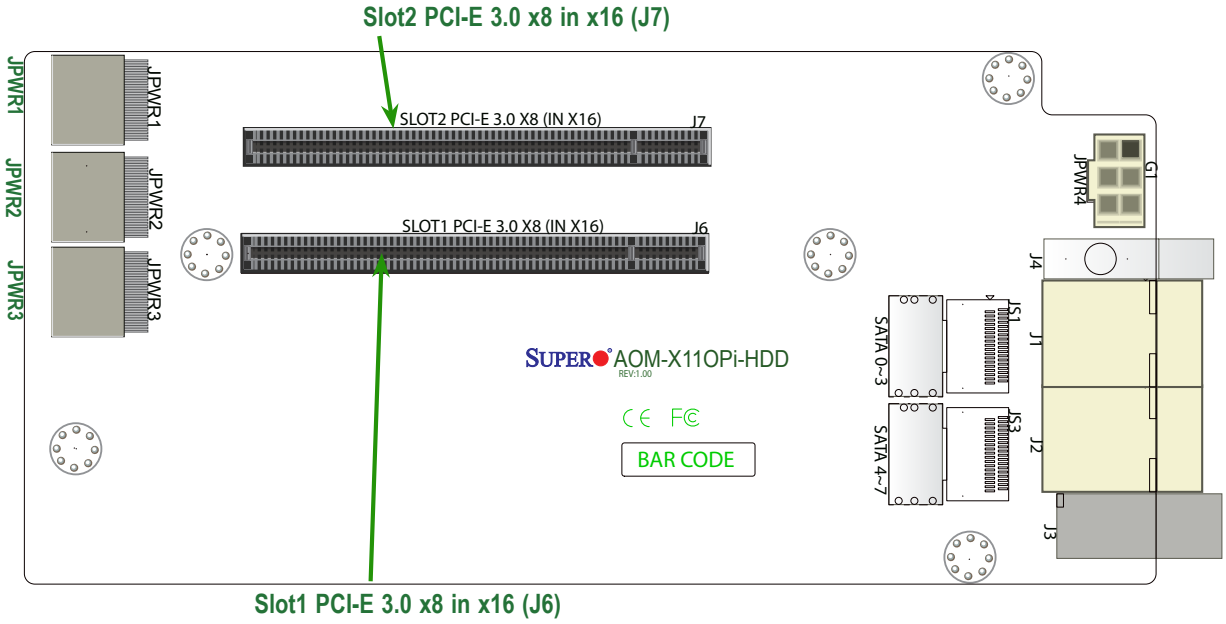


BPN-X11OPi Midplane (Rear Side)



The HDD Card & 8 CPU Boards (max.) on the Front Side of the X11OPi Midplane

Major Components on the AOM-X11OPi-HDD Card



Major Components on the AOM-X11OPi-HDD Card

Description	Default Setting
J1	High speed interconnect
J2	High Speed interconnect
J3	Guide pin
J4	Power connector
JPWR1/JPWR2/JPWR3/JPWR4	8-pin power connectors 1/2/3/4 for HDD use
Slot1/Slot2	PCI-E 3.0x8 in x16 slots (Slot1/Slot2)
SATA0-3, SATA 4-7 (JS1/JS3)	SATA connections 0-3, 4-7

Note: Refer to the following Connectors section for more information on the power connectors and SATA 3.0 ports.

HDD Power Connectors

Four 8-pin 12V power connectors (JPWR1/JPWR2/JPWR3/JPWR4) are located on the AOM-X11OPi-HDD to provide power supply for your HDD use.

12V 8-pin PWR Connector Pin Definitions	
Pin#	**Definition**
1-4	Ground
5, 6	+12V
7, 8	+5V

(Required)

SATA 3.0 Ports

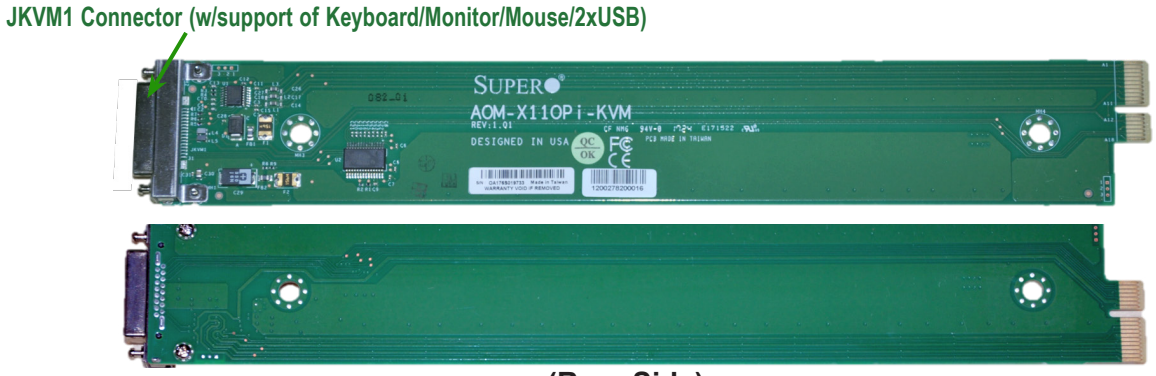
Two Serial ATA 3.0 headers (JS1/JS3) support eight SATA 3.0 connections (SATA0-3, 4-7) on the AOM-X11OPi-HDD card. These ports, supported by the Intel C621 Chipset, provide serial-link signal connections, which are faster than the connections of Parallel ATA.

Note: For more information on SATA HostRAID configuration, please refer to the Intel SATA HostRAID User's Guide posted on our Website @ http://www.supermicro.com.

1-6 The AOM-X11OPi-KVM Card

This section provides the information on the AOM-X11OPi-KVM add-on card.

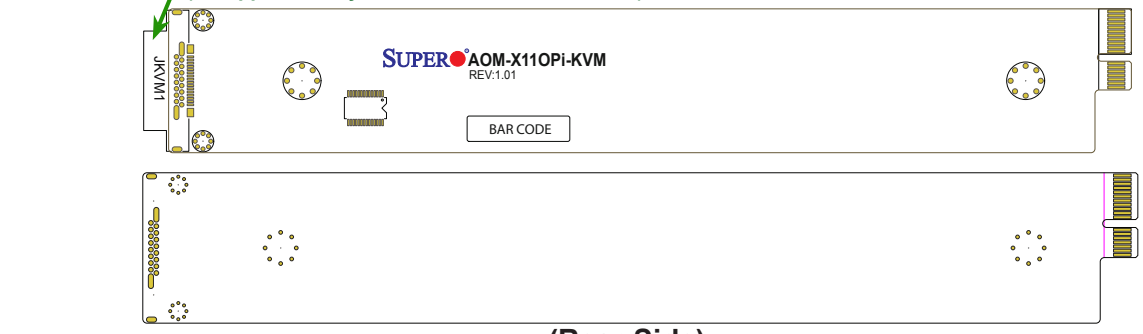
AOM-X11OPi-KVM Card Image (Rev. 1.01)



(Rear Side)

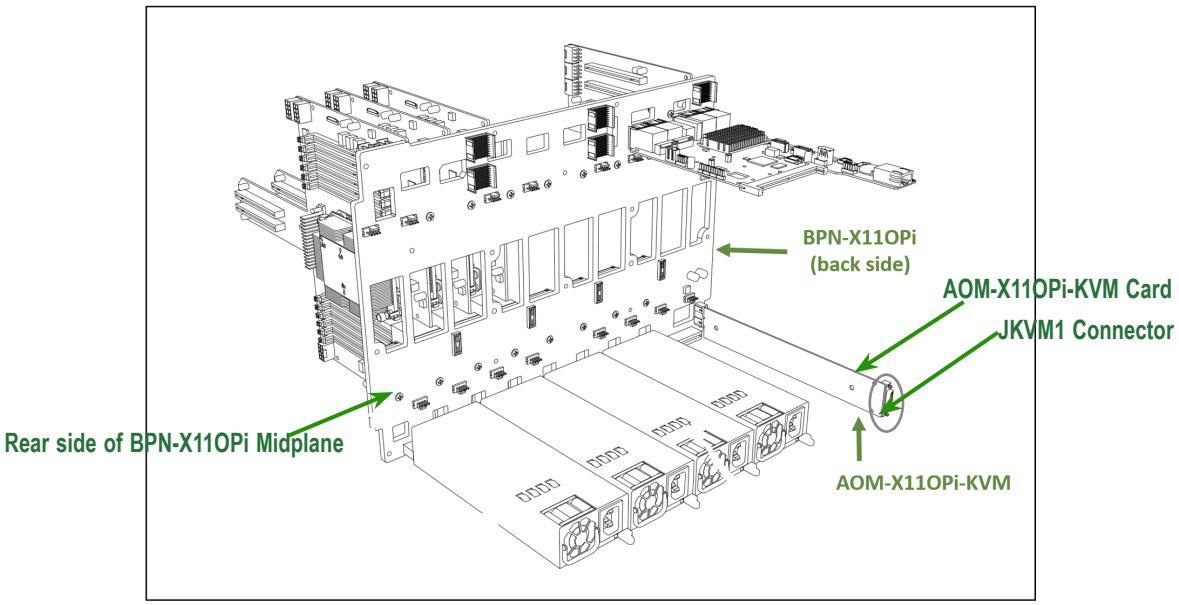
AOM-X11OPi-KVM Card Layout (Rev. 1.01)

(Front Side)



(Rear Side)

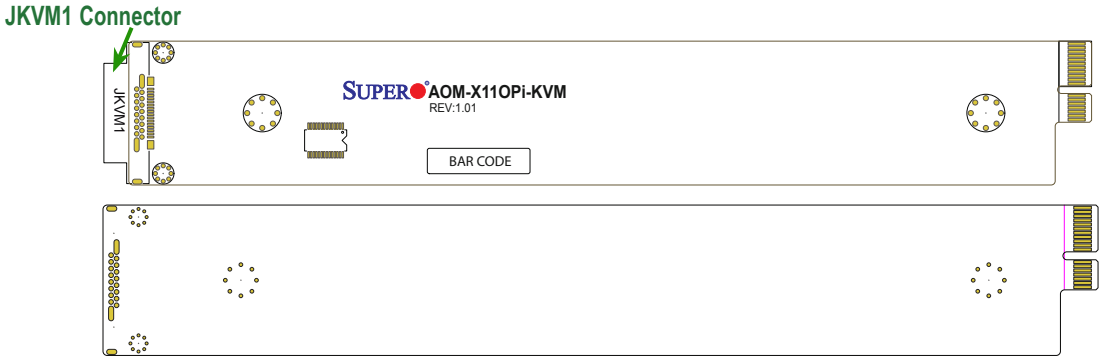
AOM-X11OPi-KVM Card Location



Major Components on the AOM-X11OPi-KVM Card

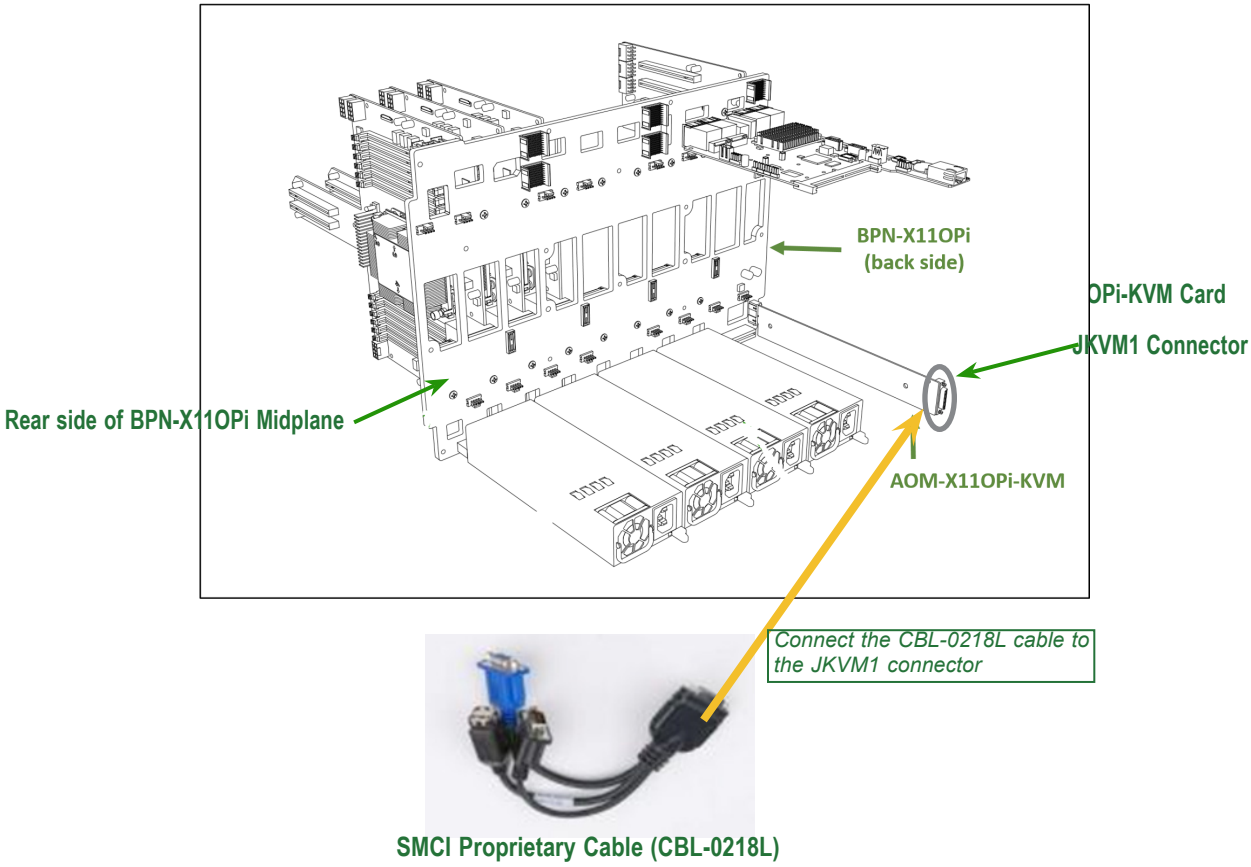
Your system comes with the AOM-X11OPi-KVM card, which is to be installed on the rear side of the BPN-X11OPi midplane. The JKVM1 connector, located at the end of the AOM-X11OPi-KVM card, provides connections for a keyboard, an external VGA monitor (from BMC), a serial COM port, and two USB 2.0 ports. Refer to the drawings below for the locations of the JKVM1 connector and the AOM-X11OPi-KVM card. (See the note on the next page.)

AOM-X11OPi-KVM Card Layout
(Front Side)



(Rear Side)

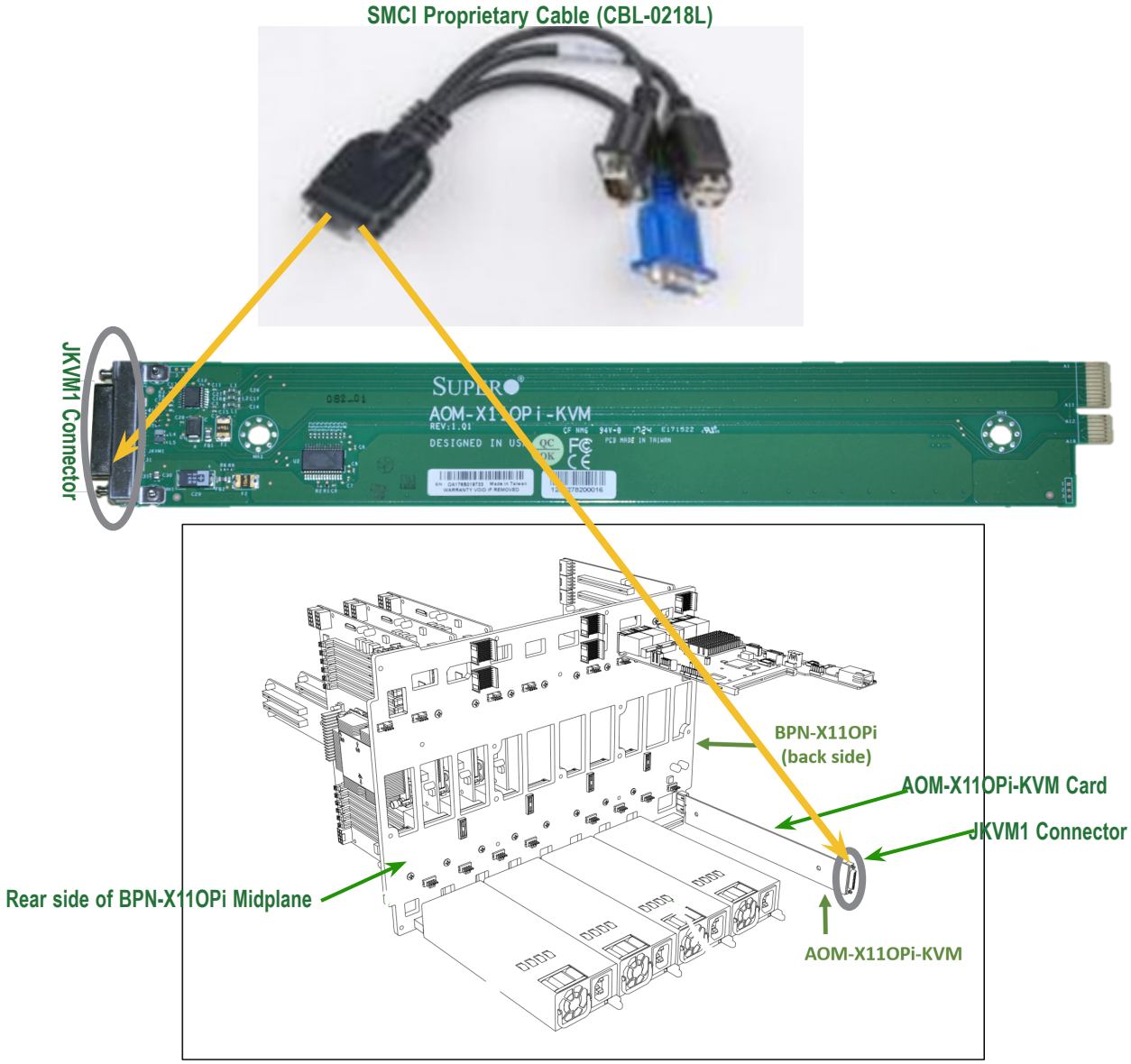
AOM-X11OPi-KVM Card Location



Major Components on the AOM-X11OPi-KVM Card

Connector	Description
JKVM1	36-pin connector used for keyboard, VGA monitor, COM port (RS232) & two USB 2.0 connections (See Note below.)

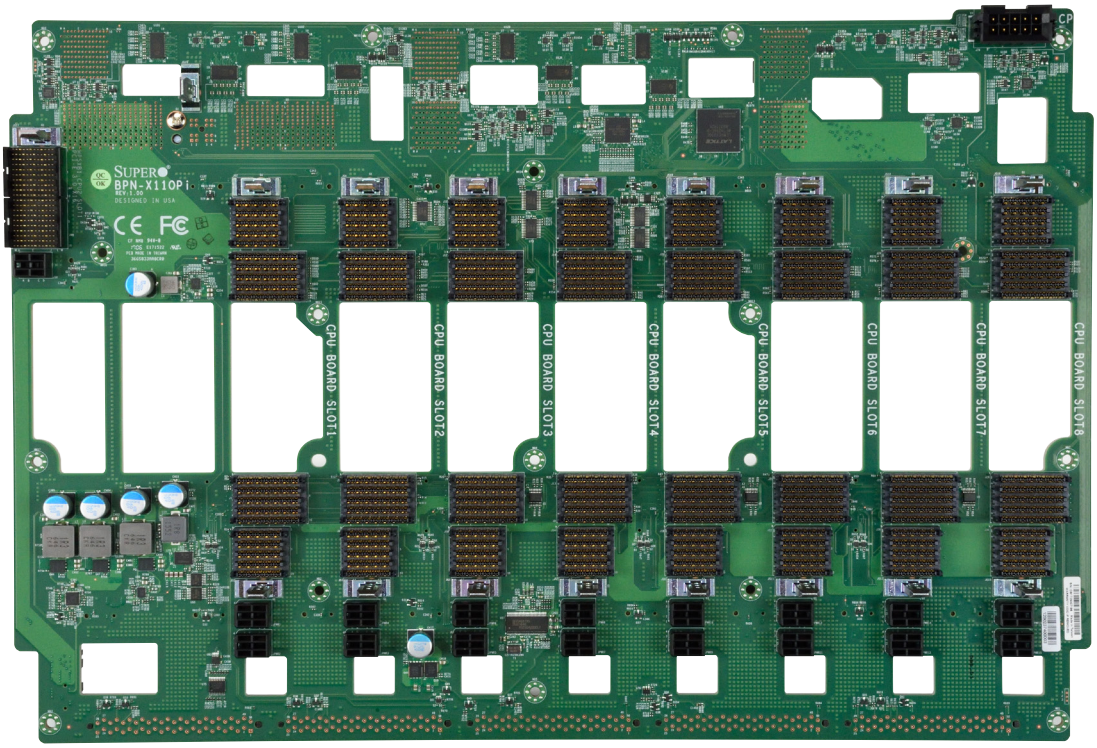
Note: For your I/O and communication devices to work properly, please use the SMCI proprietary cable(CBL-0218L) to connect the JKVM1 connector on the AOM-X11OPi-KVM carde to your keyboard, mouse, VGA monitor, com (serial) port and (two) USB 2.0 devices as shown below.



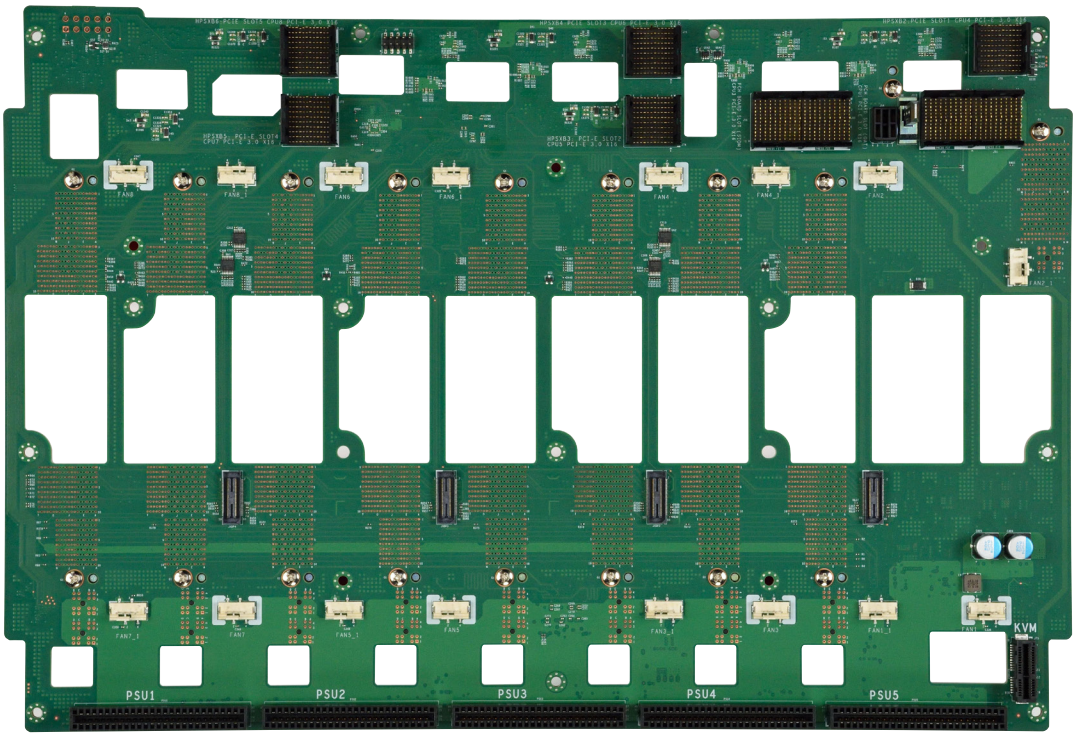
1-7 BPN-X11OPi Midplane

This section provides detailed information on the BPN-X11OPi midplane.

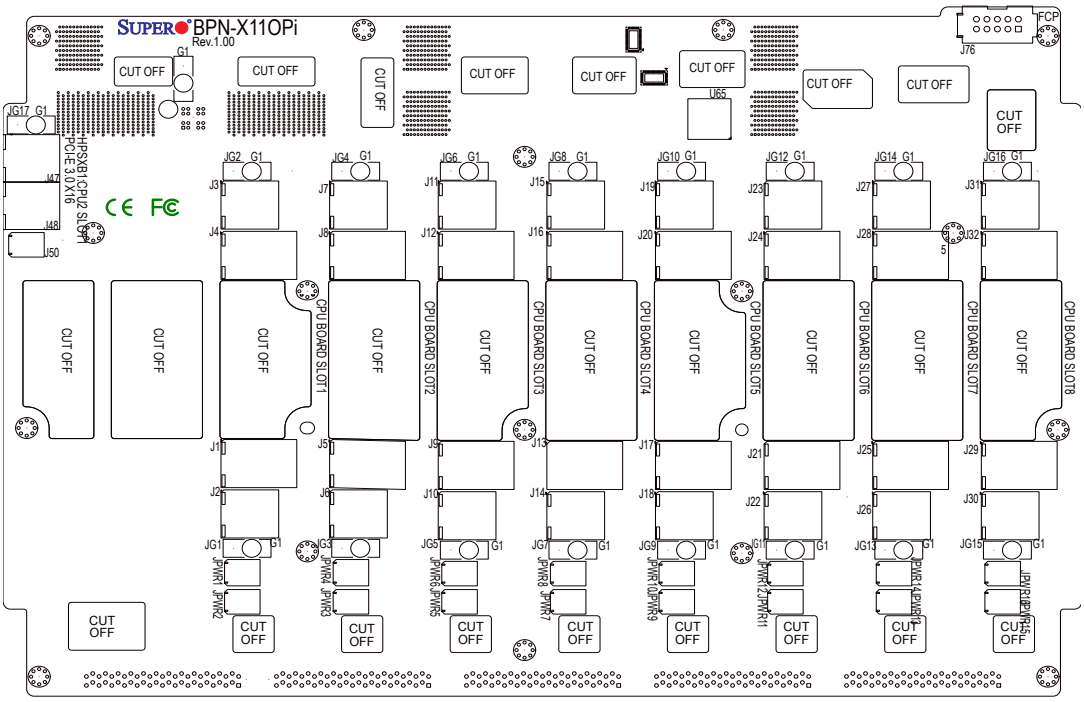
BPN-X11OPi Midplane Image (Front Side)



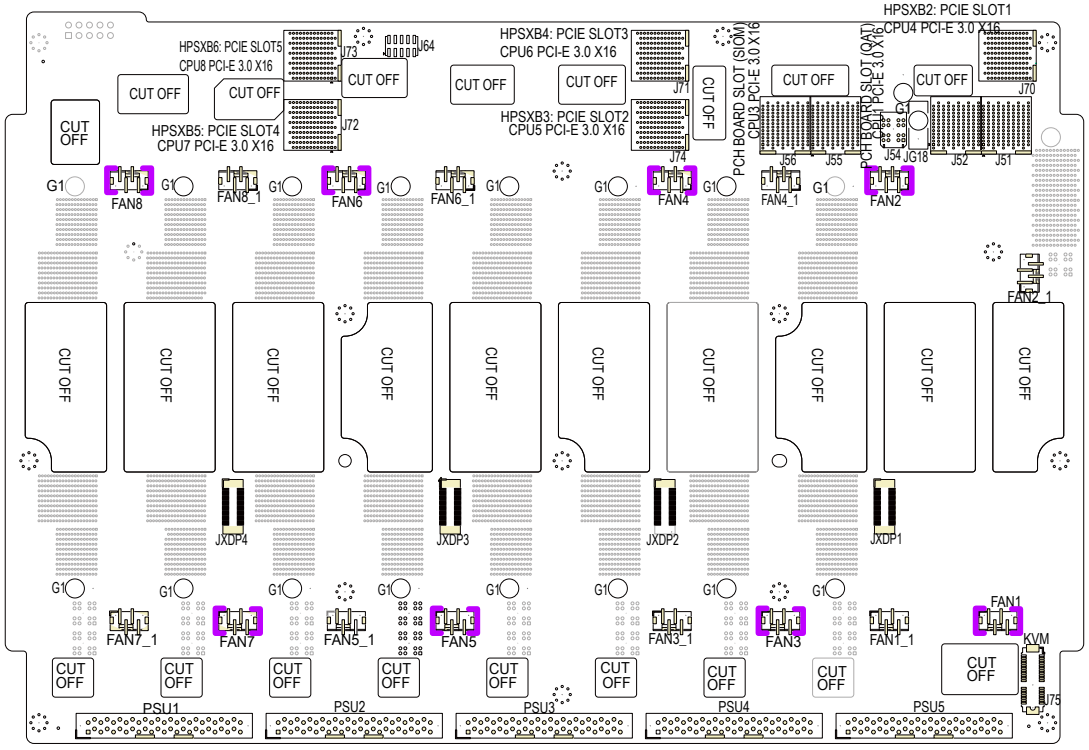
BPN-X11OPi Midplane Image (Reverse Side)



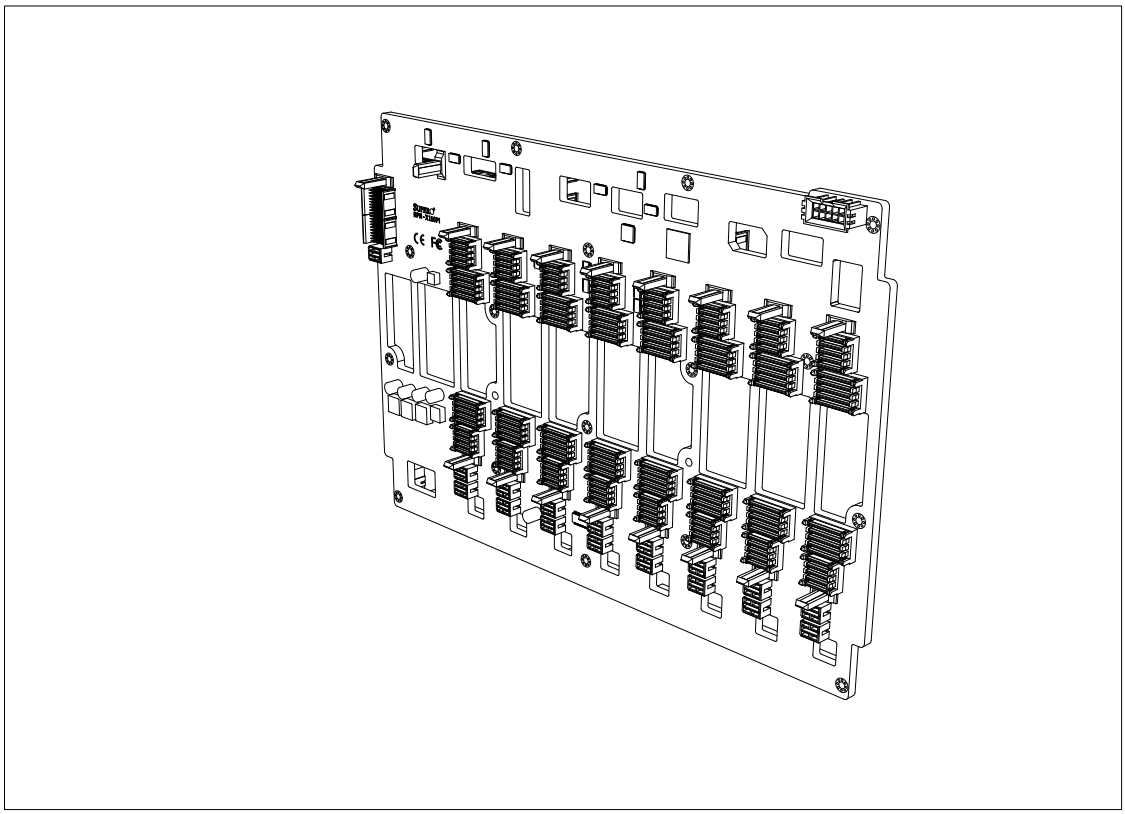
BPN-X11OPi Midplane Layout (Front Side)



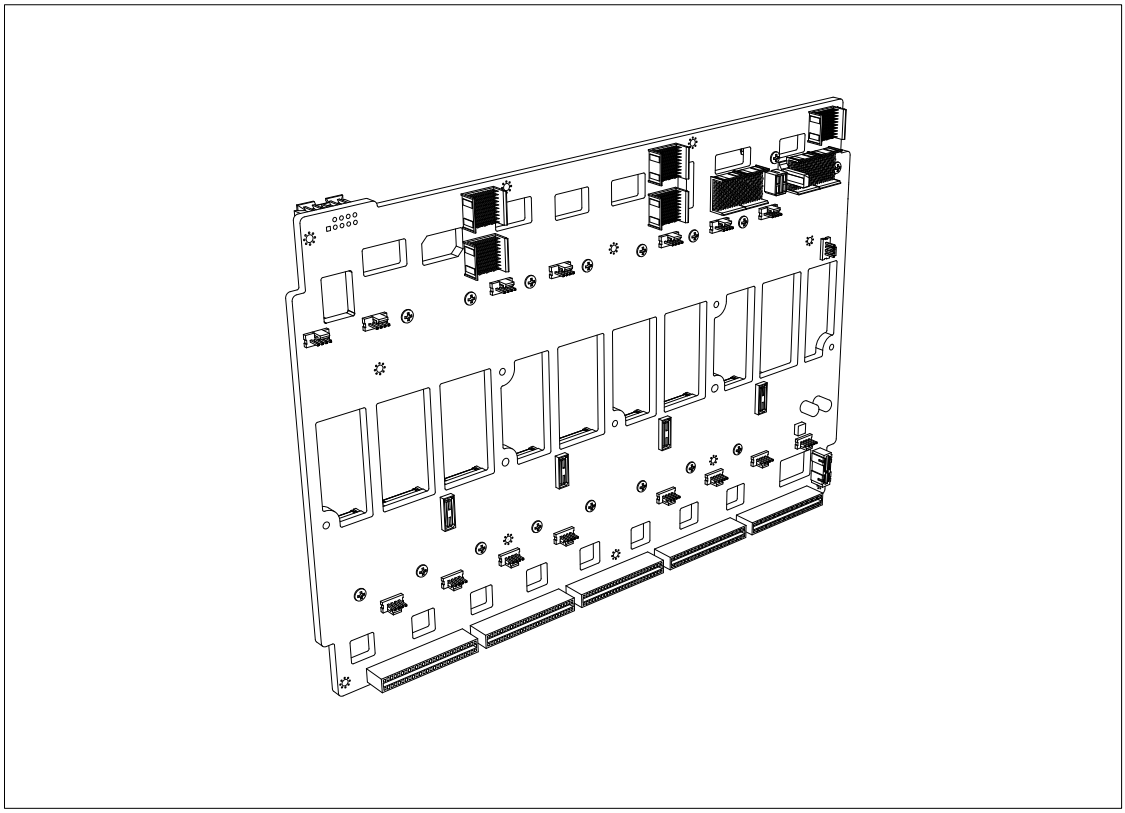
BPN-X11OPi Midplane Layout (Rear Side)



Front View of the BPN-X11OPi Midplane

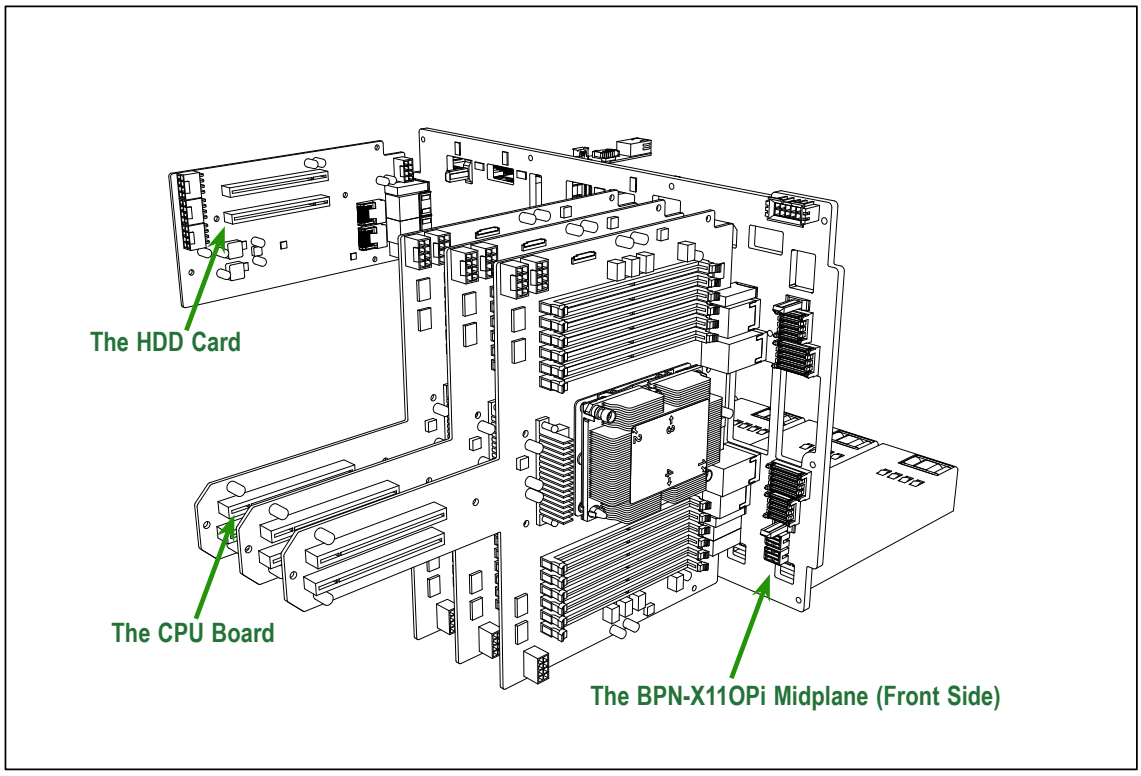


Rear View of the BPN-X11OPi Midplane

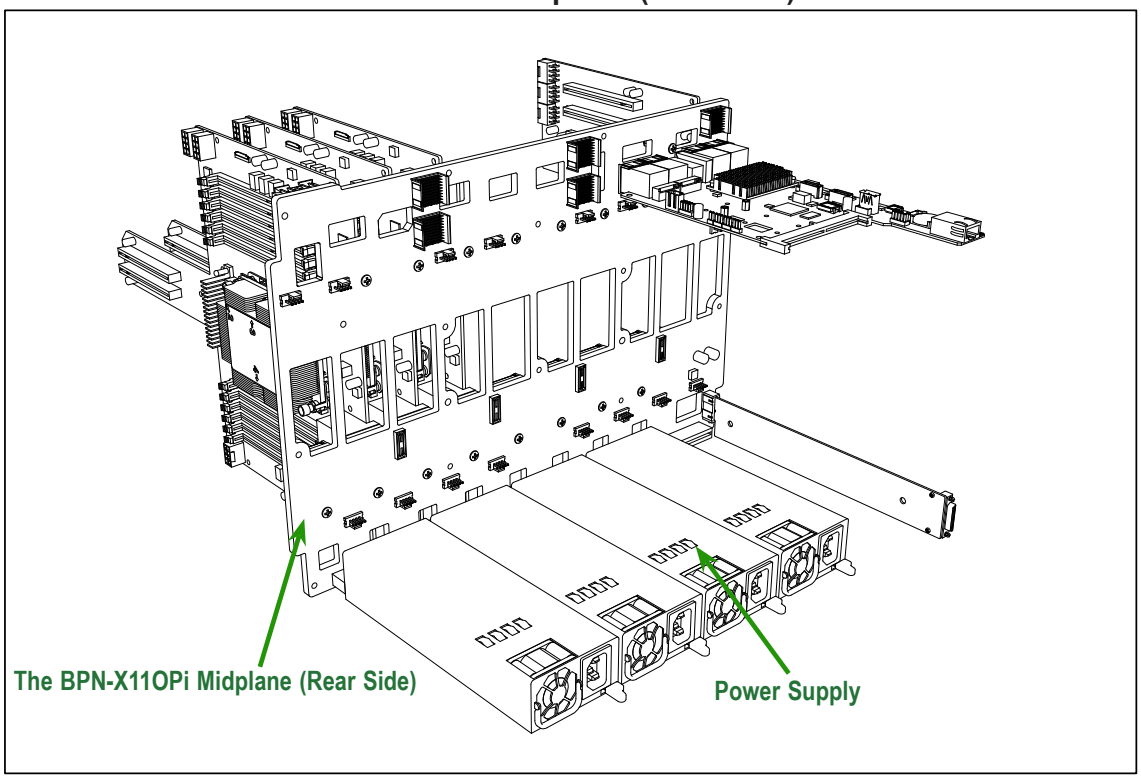


Location of the BPN-X11OPi Midplane

BPN-X11OPi Midplane (Front Side)



BPN-X11OPi Midplane (Rear Side)

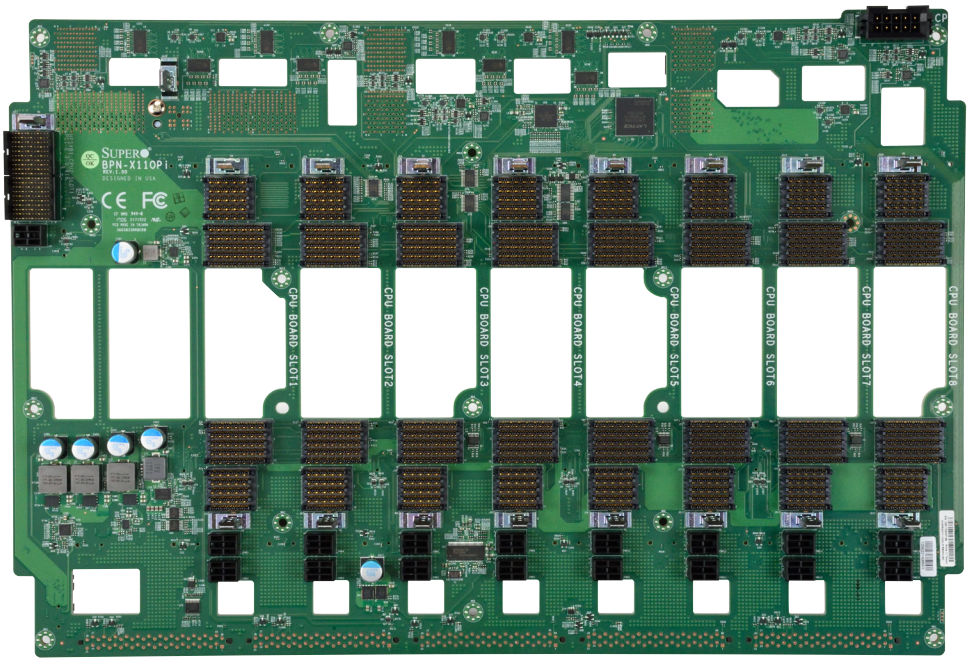


Major Components on the BPN-X11OPi Midplane

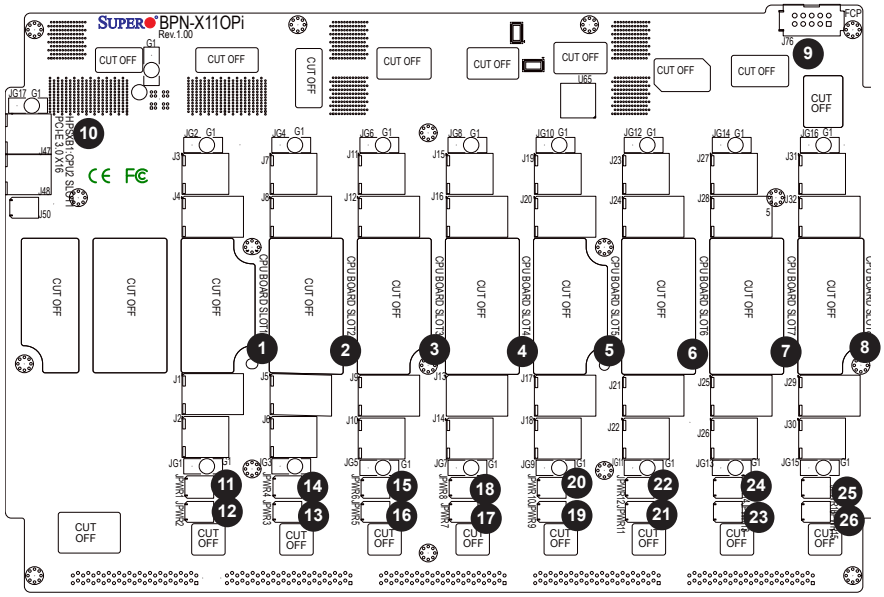
Components on the Front Side of the Midplane

The following section provides detailed information of the major components on the front side of the BPN-X11OPi midplane. Please note that all CPU boards and HDD card are installed on the front side of the midplane, and can be accessed from the front side of your system.

BPN-X11OPi Midplane Image (Front)



BPN-X11OPi Layout (Front)



Major Components on the Front Side of the BPN-X11OPi Midplane

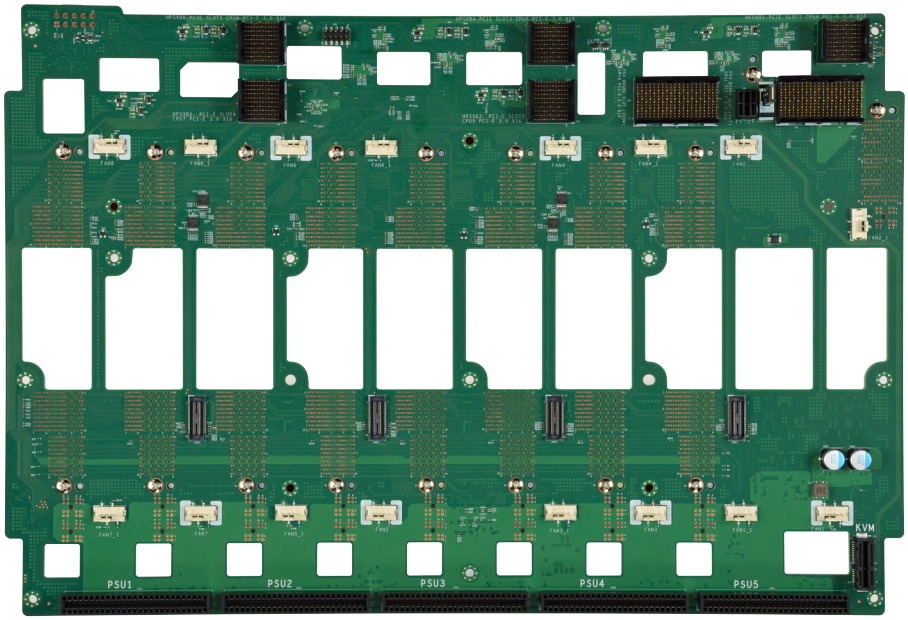
Major Components on the Front Side of the BPN-X11OPi

Item#	Description	Detailed Description
1	CPU BOARD SLOT1	CPU Board slot used for X11OPi-CPU Board 1
2	CPU BOARD SLOT2	CPU Board slot used for X11OPi-CPU Board 2
3	CPU BOARD SLOT3	CPU Board slot used for X11OPi-CPU Board 3
4	CPU BOARD SLOT4	CPU Board slot used for X11OPi-CPU Board 4
5	CPU BOARD SLOT5	CPU Board slot used for X11OPi-CPU Board 5
6	CPU BOARD SLOT6	CPU Board slot used for X11OPi-CPU Board 6
7	CPU BOARD SLOT7	CPU Board slot used for X11OPi-CPU Board 7
8	CPU BOARD SLOT8	CPU Board slot used for X11OPi-CPU Board 8
9	FCP (Front Control Panel)	Front Control Panel header
10	HPSXB1 (CPU2Slot1)	2 x PCI-E 3.0 x8 slot supported by CPU2 (for the AOM-X11OPi-HDD card)
11, 12	JPWR1/JPWR2	Power connectors 1/2 for X11OPi-CPU Board 1
13, 14	JPWR3/JPWR4	Power connectors 3/4 for X11OPi-CPU Board 2
15, 16	JPWR5/JPWR6	Power connectors 5/6 for X11OPi-CPU Board 3
17, 18	JPWR7/JPWR8	Power connectors 7/8 for X11OPi-CPU Board 4
19, 20	JPWR9/JPWR10	Power connectors 9/10 for X11OPi-CPU Board 5
21, 22	JPWR11/JPWR12	Power connectors 11/12 for X11OPi-CPU Board 6
23, 24	JPWR13/JPWR14	Power connectors 13/14 for X11OPi-CPU Board 7
25, 26	JPWR15/JPWR16	Power connectors 15/16 for X11OPi-CPU Board 8

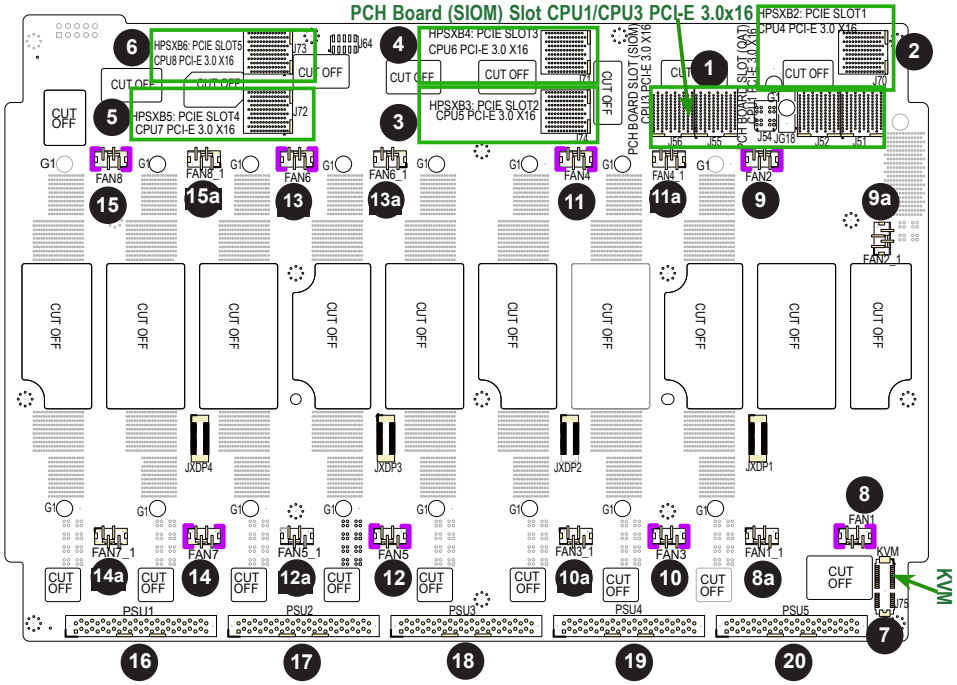
Major Components on the Rear Side of the BPN-X11OPi Midplane

The following section provides the information of the major components on the reverse side of the BPN-X11OPi midplane. Please note that the PCH card, PCI-E card, power supply modules, and cooling fans are installed on the reverse side of the midplane, and can be accessed from the rear side of your system.

BPN-X11OPi Midplane Image (Rear Side)



BPN-X11OPi Layout (Rear Side)



Major Components on the Reverse Side of the BPN-X11OPi Midplane

Major Components on the Reverse Side of the BPN-X11OPi

Item#	Location	Detailed Description
1	J51/J52/J54/J55/J56	PCH Board Slot (SIOM) CPU1/CPU3 PCI-E 3.0 x16 Slot (for the AOM-X11OPi-LBG)
2	J70	HPSXB2: Slot1 CPU4 PCI-E 3.0 x 16
3	J74	HPSXB3: Slot2 CPU5 PCI-E 3.0 x 16
4	J71	HPSXB4: Slot3 CPU6 PCI-E 3.0 x 16
5	J72	HPSXB5: Slot4 CPU7 PCI-E 3.0 x 16
6	J73	HPSXB6: Slot5 CPU8 PCI-E 3.0 x 16
7	J75	KVM header for KVM (Keyboard/Video/Mouse) support
8	FAN1	Rear Fan Connector 1
8a	FAN1_1	Rear Fan Connector 1_1
9	FAN2	Rear Fan Connector 2
9a	FAN2_1	Rear Fan Connector 2_1
10	FAN3	Rear Fan Connector 3
10a	FAN3_1	Rear Fan Connector 3_1
11	FAN4	Rear Fan Connector 4
11a	FAN4_1	Rear Fan Connector 4_1
12	FAN5	Rear Fan Connector 5
12a	FAN5_1	Rear Fan Connector 5_1
13	FAN6	Rear Fan Connector 6
13a	FAN6_1	Rear Fan Connector 6_1
14	FAN7	Rear Fan Connector 7
14a	FAN7_1	Rear Fan Connector 7_1
15	FAN8	Rear Fan Connector 8
15a	FAN8_1	Rear Fan Connector 8_1
16	PSU1	Power Supply Unit 1
17	PSU2	Power Supply Unit 2
18	PSU3	Power Supply Unit 3
19	PSU4	Power Supply Unit 4
20	PSU5	Power Supply Unit 5

Fan Headers

There are 16 system/CPU fan headers (Fans 1-8_1) on reverse side of the BPN-X11OPi midplane. All these 4-pin fans headers are backward-compatible with the traditional 3-pin fans. However, fan speed control is available for 4-pin fans only by Thermal Management via the IPMI 2.0 interface. See the table below for pin definitions.

Fan Header Pin Definitions

Pin#	Definition
1	Ground
2	+12V
3	Tachometer
4	PWM (Power Width Modulation)

1-8 X11OPi Platform Features

System Platform Features	
(Installed on the X11OPi-CPU board)	
• The X11OPi system supports up to eight X11OPi-CPU boards, and each CPU board supports an Intel® Xeon® Platinum 8XXX processor, which offers three full-width Intel UltraPath Interconnect (UPI) links with the data transfer rates of up to 10.4 GT/s in each direction	
Memory (installed on the X11OPi-CPU board)	
• Each CPU board supports up to 3 TB DCPMM or up to 3 TB 3DS Load Reduced (3DS LRDIMM)/Load Reduced (LRDIMM)/3DS Registered (RDIMM)/Registered (RDIMM) DDR4 memory of 2933*/2666/2400/2133 MHz in 12 DIMM slots. It also supports up to 4.5 TB DCPMM & DDR4 combined memory of up to 2933 MHz in 12 slots per CPU board. With eight X11OPi-CPU boards built-in, the X11OPi Platform provides up to 24 TB of DCPMM/DDR4 memory or up to 36 TB of DCPMM & DDR4 combined memory in 96 DIMM slots. **Notes: 1.** For your system memory to work properly, please use memory modules of the same type and the same speed on the motherboard. For more information on CPU, memory support, please refer to the X11OPi-CPU board section in this chapter. **2.** Memory speed support depends on the processors used on the motherboard. **3.** 2933 MHz memory and DCPMM memory are supported by Second Generation Intel® Xeon® Platinum 82XX processors only. **4.** Populating DDR4 memory modules in a two-DIMMs per-channel (2DPC) configuration on this motherboard will affect memory bandwidth and performance. • DDR4: 16GB, 32GB, 64GB, 128 GB, and 256 GB • DCPMM: 128 GB, 256 GB and 512 GB	
Chipset	
• Intel C621 PCH	
PCI-E 3.0 Slots	
• Two (2) PCI-E 3.0x16 slots (CPU Slot1/Slot2) on each X11OPi-CPU board (w/8 CPU boards max in the system) • One (1) PCI-E 3.0 x16 slot on the RSC-X11OPi-PCIE card (w/five PCI-E cards max. in the system) • Two (2) PCI-E 3.0x8 in x16 slots (Slot1/Slot2) on the AOM-X11OPi-HDD card, (w/one HDD-card in the system)	
I/O Module Slot	
• One (1) SIOM PCI-E 3.0x16 slot on the AOM-X11OPi-LBG card	
Graphics	
• ASPEED AST2500 BMC video controller via the BMC on the AOM-X11OPi-LBG card	
Network	
• One IPMI LAN 2.0 port is supported by the BMC on the AOM-X11OPi-LBG card	
I/O Devices	
• SATA	• Two M.2 connectors on the AOM-X11OPi-LBG card (J1, J2) support two S-SATA ports (S-SATA1/2) or two PCH PCI-E 3.0 x4 slots • Eight (8) SATA 3.0 ports on AOM-X11OPi-HDD. (PCH SATA 0-7)
• NVME Connectors	• Four (4) PCI-E 3.0 NVME connectors (NVME0/NVME1/NVME2/NVME3) on each X11OPi-CPU board
• Integrated IPMI 2.0	• IPMI 2.0 supported by the AST2500 Baseboard Management Controller (BMC) on the AOM-X11OPi-LBG card (See Note below)
• SIOM Support	• One SIOM slot (PCIe 3.0 x16 from CPU3) compatible with SMCI SIOM LAN modules

Peripheral Devices

- One (1) USB 3.0 header (JUSB1) provides a Type A 3.0 connector on the AOM-X11OPi-LBG card
- One (1) USB 2.0 header (JUSB2) provides two USB 2.0 connections on the AOM-X11OPi-LBG card
- 32 MB AMI BIOS® UEFI EEPROM Flash BIOS on the AOM-X11OPi-LBG card

Power Configuration

- Two (2) 8-pin power connectors (PWR1/2) used for CPU power and three (3) 8-pin power connectors (JPWR3/4/5) used for GPU power on each X11OPi-CPU board (w/8 CPU boards maximum)
- Two (2) 3-pin power connectors (JSD1/JSD2) used for SATA DOMs on the AOM-X11OPi-LBG card,
- Four (4) 8-pin HDD power connectors (JPWR1/JPWR2/JPWR3/JPWR4) used for HDD devices on the AOM-X11OPi-HDD card
- Sixteen (16) power connectors on the reverse side of the BPN-X11OPi midplane for cooling fan use
- Five (5) main system power supplies (PSU1-PSU5) on the reverse side of the BPN-X11OPi midplane for system use
- ACPI/ACPM Power Management
- Main switch override mechanism
- Power-on mode for AC power recovery
- Intel® Intelligent Power Node Manager (Available when the NMView utility is installed in the system)
- Manageability Engine

PC Health Monitoring

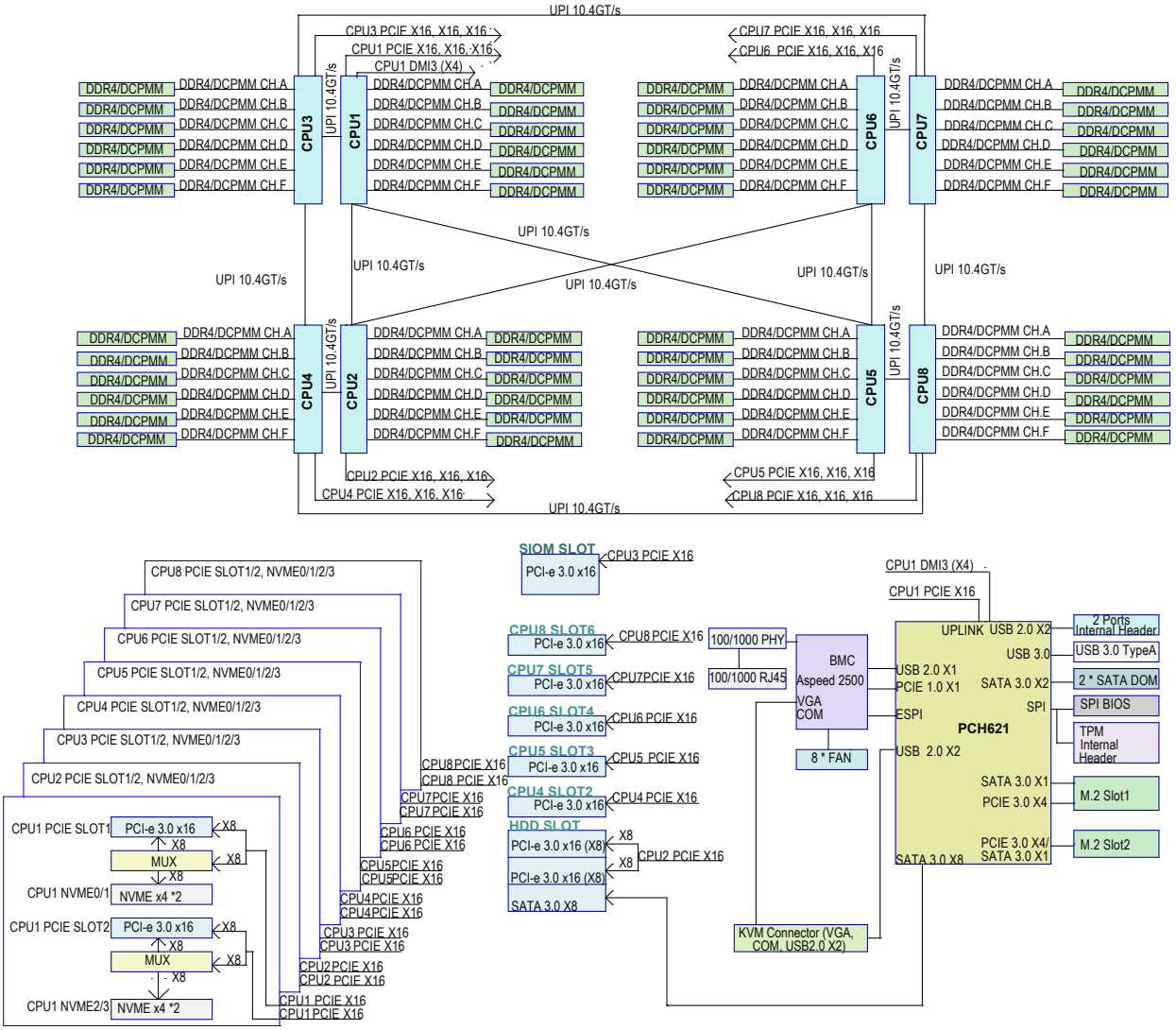
• CPU Health Monitoring	• Onboard voltage monitors for CPU Vcore (up to 8 CPU cores), 3.3VDD, 3.3VSB, 12V, 5V, memory voltage, and battery voltage • CPU 7 (6+1)-Phase switching voltage regulator • CPU/System overheat LED and control • CPU Thermal Trip support • Thermal Monitor 2 (TM2) support
• Fan Control	• Eight (8) pairs of cooling fans (16 fans total) are located on the reverse side of BPN-X11OPi midplane for rear chassis access

System Management

- PECI (Platform Environment Configuration Interface) 2.0 support
- System resource alert via SuperDoctor® 5
- SuperDoctor 5, Watch Dog, NMI

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

X11OPi System Block Diagram



X11OPi System Block Diagram

Note: This is a general block diagram and may not exactly represent the features on your system. See the "System Platform Features" pages for the actual specifications of the system.

1.9 Processor and Chipset Overview

Built upon the functionality and capability of the Intel® Xeon® Platinum 8XXX (Socket P) processors with support of Intel C621 chipset (Note 1 below), this platform provides superb system performance, efficient power management, and a rich feature set based on cutting-edge technologies to address the needs of next-generation users. It offers innovative solutions with unprecedented system reliability and scalability to meet the demands of High Performance Computing (HPC) platforms.

Features Supported by Intel® Xeon® Platinum 81XX Processors

Intel® Xeon® Platinum 81XX 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 Second Generation Intel® Xeon® Platinum 82XX Processors

Second Generation Intel® Xeon® Platinum 82XX processors support the following features:

- Higher performance for a wider range of workloads with per-core performance increase
- Support of Optane DC Persistent Memory (DCPMM) with affordable, persistent, and large capacity
- Up to 2993 MHz memory supported (Refer to Section 1.14 for details.)
- 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 and DCPMM memory are supported by the Second Generation Intel® Xeon® Platinum 82XX processors.

1-10 Special Features

Recovery from AC Power Loss

Basic I/O System (BIOS) provides a setting for you to determine 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 the system to automatically return to a power-on state. See the Advanced BIOS Setup section to change this setting. The default setting is **Last State**.

1-11 System Health Monitoring

This section describes the health monitoring features of the X11OPi Platform. The system has an onboard Baseboard Management Controller (BMC) that supports system health monitoring.

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

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

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

System Resource Alert

This feature is available when used with SuperDoctor 5® which will 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.

1-12 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.

1-13 Power Supply

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

The X11OPi system comes with five Supermicro Model PWS-1K62A-1R, 1600W redundant power supplies, serving as main system power supplies, on the rear side of the chassis. Please note that your system will function properly only when Supermicro Model PWS-1K62A-IR power supplies are used in the system. It is also recommended that you install a power surge protector to help avoid problems caused by power surges.

In addition to these five power supplies, there are individual power connectors installed on an add-on card or a component board to provide power supply to the components installed on that particular add-on card or component board. These power connectors include the following:

- Two (2) 8-pin power connectors (PWR1/2) used for CPU power (on the BPN-X11OPi mid-plane) and three (3) 8-pin power connectors (JPWR3/4/5) used for GPU power on each X11OPi-CPU board (w/8 CPU boards maximum),
- Two (2) 3-pin power connectors (JSD1/JSD2) used for SATA DOMs on the AOM-X11OPi-LBG card,
- Four (4) 8-pin HDD power connectors (JPWR1/JPWR2/JPWR3/JPWR4) used for HDD devices on the AOM-X11OPi-HDD card,
- Sixteen (16) power connectors on the rear side of the BPN-X11OPi midplane for cooling fan use

Please connect these power connectors to the power supply to provide adequate power to the components and the system.

Warning! To avoid damaging the power supply or the system, be sure to connect all the power connectors mentioned above to the power supplies. Failure to do so will void the manufacturer warranties on both your power supply and your system.

1-14 Advanced Power Management

The new advanced power management features supported by the motherboard includes the following:

Intel® Intelligent Power Node Manager (NM) (Available when the NMView utility is installed in the system)

The Intel® Intelligent Power Node Manager (IPNM) provides your system with real-time thermal control and power management for maximum energy efficiency. Although IPNM Specification Version 1.5/20 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 Specification Version 1.5 or Version 2.0 depends on the power supply used in the system.

Management Engine (ME)

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

Note: For more information regarding the Intel C621 chipset, please refer to the AOM-X11OPi-LBG section.

1-15 Intel® Optane DC Persistent Memory Overview

The Second Generation Intel® Xeon® Platinum 82XX processor supports new DCPMM (Optane™ DC Persistent Memory Modules) technology that offers data persistence with higher capacity than existing memory modules and lower latency than NVMe SSDs. DCPMM memory provides hyper-speed storage capability for high performance computing platforms with flexible configuration options.

Chapter 2

Troubleshooting

2-1 Troubleshooting Procedures

Use the following procedures to troubleshoot your system. If you have followed all of the procedures below and still need assistance, refer to the 'Technical Support Procedures' and/or 'Returning Merchandise for Service' section(s) in this chapter.

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

Before Power On

1. Check that the power LED on the motherboard is on.
2. Make sure that the power connector is connected to your power supply.
3. Make sure that no short circuits exist between the motherboard and chassis.
4. Disconnect all cables from the system board, including those for the keyboard and mouse.
5. Remove all I/O modules and add-on cards.
6. Install the X11OPi-CPU cards on the BPN-X11OPi midplane first (-making sure the CPU is fully seated), and connect the front panel connectors to the system board.

No Power

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

No Video

If the power is on, but you have no video, remove the I/O module, all the add-on cards and cables.

Memory Errors

When a memory error occurs, check the following:

1. Make sure that the memory modules are compatible with the system and that the DIMM modules are properly and fully installed. (For memory compatibility, refer to the Memory Compatibility chart posted on our website at http://www.supermicro.com.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that the same RAM speed of DIMMs are used in the system.
3. Make sure that you are using the correct type of memory modules as recommended by Supermicro. Please refer to the memory support section on the CPU board section in Chapter 1.
4. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.
5. Make sure that all memory modules are fully seated in their slots. Follow the instructions given in the Memory Tables in the CPU card section in Chapter 1.

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.
2. The battery on your motherboard may be old. Check to verify that it still supplies ~3VDC. If it does not, replace it with a new one.
3. If the above steps do not fix the setup configuration problem, contact your vendor for repairs.

When the System Becomes Unstable

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

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

Note: Refer to the product page on our website at http:\\www.supermicro.com for memory and CPU support and updates.

3. HDD support: Check whether all hard disk drives (HDDs) work properly. Replace the bad HDDs with good ones. (HDDs are on the AOM-X11OPi-HDD card.)

4. System cooling: Check system cooling to make sure that all heatsink fans, and CPU/system fans, etc., work properly. Check Hardware Monitoring settings in the BIOS to make sure that the CPU and system temperatures are within the normal range. Also, check the Overheat LED, if available, to make sure that the Overheat LED is not on.

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

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

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

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

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

- System board 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
- Distributors: For immediate assistance, please have your account number ready when placing a call to our technical support department. We can be reached by e-mail at support@supermicro.com.
- An example of a Technical Support form is on our website at (http://www.supermicro.com). 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.

2-3 Battery Removal and Installation

Battery Removal (Located on the AOM-X11OPi-LBG card)

To remove the onboard battery, follow the steps below:

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

Proper Battery Disposal

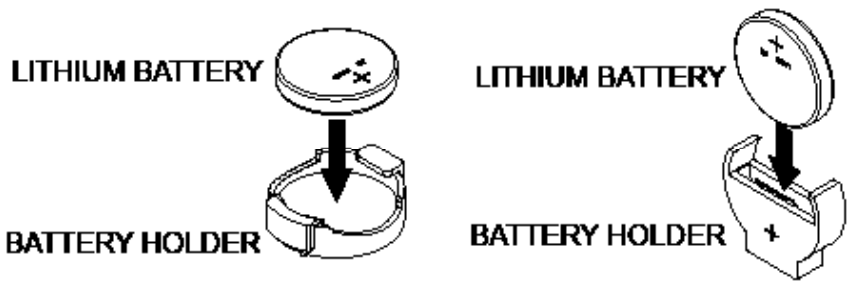
Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency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

Battery Installation

To install an onboard battery, follow the steps below:

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

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



2-4 Frequently Asked Questions

Question: What type of memory does my system support?

Answer: The X11OPi supports up to 3 TB DCPMM or 3DS LRDIMM/LRDIMM/3DS RDIMM/RDIMM DDR4 memory of 2933*/2666/2400 MHz in 12 memory modules per CPU board. It also supports up to 4.5 TB of DCPMM & DDR4 combined memory in 12 DIMM slots. With eight CPU boards embedded in the platform, the provides up to 24 TB of DCPMM/DDR4 memory or 36 TB of DCPMM & DDR4 combined memory in 96 modules. (See the notes below.) It is strongly recommended that you do not mix memory modules of different types, speeds and sizes. Please follow all memory installation instructions given in the memory section in the X11OPi-CPU board section in Chapter 1.

Notes: 2933 MHz memory and DCPMM memory are supported by Second Generation Intel® Xeon® Platinum 82XX processors.

Question: How do I handle the used battery (on the AOM-X11OPi-LBG card)?

Answer: 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.

Question: How do I update my BIOS (on the AOM-X11OPi-LBG card)?

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

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

Question: How do I update my BIOS under UEFI Shell?

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

1. Download and save the BIOS update package to your computer.
2. Extract the files from the UEFI folder of the BIOS package to a USB stick.

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

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

Shell> fs0:

fs0:\> cd UEFI

fs0:\UEFI> flash.nsh BIOSname#.###

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

a. If a different FDT is found

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

b. If the FDT is the same

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

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

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

2-5 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 3

UEFI BIOS

3.1 Introduction

This chapter describes the AMIBIOS™ setup utility for the X11OPi Platform motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.

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

Starting the Setup Utility

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

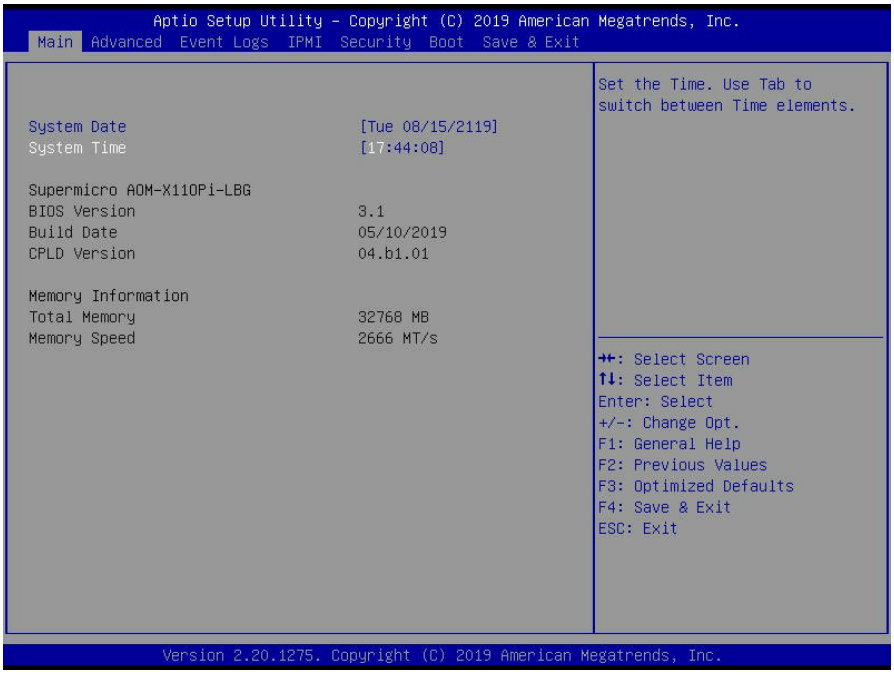
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

3.2 Main Setup

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



System Date/System Time

Use this item 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 Day MM/DD/YYYY format. The time is entered in HH:MM:SS format.

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

Supermicro X11OPi

BIOS Version

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

Build Date

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

CPLD Version

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

Memory Information

Total Memory

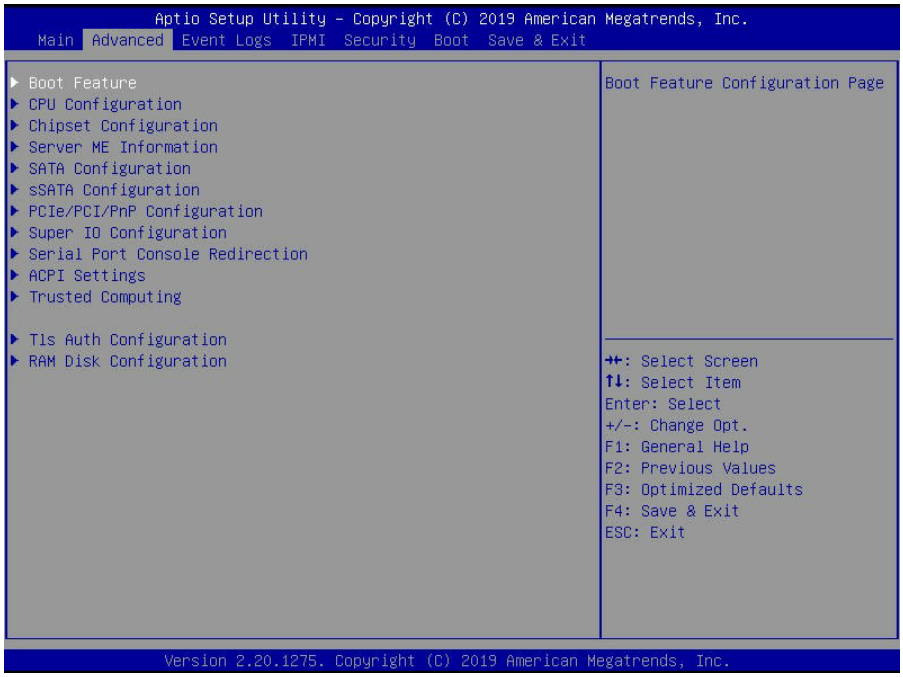
This feature displays the total size of memory available in the system.

Memory Speed

This feature displays the default speed of the memory modules installed in the system.

3.3 Advanced Setup Configurations

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



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

▶Boot Configuration

Quiet Boot

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

Note: POST message will always display regardless of the setting of this feature.

Option ROM Messages

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

Bootup NumLock State

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

Wait For 'F1' If Error

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

Interrupt 19 Capture

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

Re-try Boot

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

Power Configuration

Watch Dog Function

Select Enabled to allow the Watch Dog timer to reboot the system when it is inactive for more than 5 minutes. The options are Enabled and **Disabled.**

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 4 Seconds Override and **Instant Off.**

Restore on AC Power Loss

Use this feature to set the power state after a power outage. Select Power 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**.

▶CPU Configuration

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

▶Processor Configuration

The following CPU information will display:

- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM
- L2 Cache RAM
- L3 Cache RAM
- Processor 1 Version through Processor 8 Version

Hyper-Threading (ALL)

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

Core Enabled

Use this feature to enable or disable CPU cores in the processor specified by the user. Use the <+> key and the <-> key on the keyboard to set the desired number of CPU cores you want to enable in a processor. Please note that the maximum of 28 CPU cores are currently available in each CPU package. The default setting is **0**.

Monitor/Mwait

Select Enable to enable the Monitor/Mwait instructions in the processor. The options are **Enable** and Disable.

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

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

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

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

PPIN Control

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

Hardware Prefetcher (Available when supported by the CPU)

If this feature is set to Enable, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the Level 2 (L2) cache to improve CPU performance. The options are Disable and **Enable**.

Adjacent Cache Prefetch (Available when supported by the CPU)

Select Enable for the CPU to prefetch both cache lines for 128 bytes as comprised. Select Disable for the CPU to prefetch both cache lines for 64 bytes. The options are Disable and **Enable**.

Note: Please power off and reboot the system for the changes you've made to take effect. Please refer to Intel's website for detailed information.

DCU Streamer Prefetcher (Available when supported by the CPU)

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

DCU IP Prefetcher

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

LLC Prefetch

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

Extended APIC (Extended Advanced Programmable Interrupt Controller)

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

Force x2APIC (Extended Advanced Programmable Interrupt Controller)

Select Enable to force the BIOS to use the x2 APIC mode which will allow the operating system to perform more efficiently on high-core CPU configurations and optimize interrupt distribution in virtualization. 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 **Enable** and Disable.

▶Advanced Power Management Configuration

Power Technology

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

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

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

Energy Performance BIOS Setting (Available when "Power Performance Tuning" is set to BIOS Controls EPB)

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

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

Select Enable to support Super Performance to enhance system performance. The options are Enable and **Disable**.

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

SpeedStep (PStates)

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

Config (Configure) TDP (Available when SpeedStep is set to Enable)

Use this feature to set the appropriate TDP (Thermal Design Power) level for the system. The TDP refers to the maximum amount of power allowed for running "real applications" without triggering an overheating event. The options are **Normal**, Level 1, and Level 2.

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

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

Turbo Mode (Available when SpeedStep is set to Enable)

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

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

Hardware P-States

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

▶CPU C State Control

Autonomous Core C-State

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

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

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

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

Select Enable to enable "Enhanced Halt State" support, which will significantly reduce the CPU's power consumption by minimizing CPU's clock cycles and reduce voltage during a "Halt State." The options are Disable and **Enable**.

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

Package C State

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

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

Software Controlled T-States

If this feature is set to Enable, CPU throttling settings will be supported by the software of the system. The options are **Enable** and Disable.

▶Chipset Configuration

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

▶North Bridge

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

▶UPI (Ultra Path Interconnect) Configuration

This section displays the following UPI General Configuration information:

- Number of CPU
- Number of Active UPI Link
- Current UPI Link Speed
- Current UPI Link Frequency

- UPI Global MMIO Low Base/Limit
- UPI Global MMIO High Base/Limit
- UPI PCI-E Configuration Base/Size

Degrade Precedence

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

Link L0p Enable

Select Enable to enable Link L0p. The options are Disable, Enable, and **Auto**.

Link L1 Enable

Select Enable to enable Link L1 (Level 1 link). The options are Disable, Enable, and **Auto**.

IO Directory Cache (IODC)

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

SNC

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

XPT Prefetch

Select Enable to support XPT Prefetching to enhance system performance. The options are Enable, **Disable**, and Auto.

KTI Prefetch

Select Enable to support KTI Prefetching to enhance system performance. The options are **Enable** and Disable.

Local/Remote Threshold

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

Stale AtoS (A to S)

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

LLC Dead Line Alloc

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

Isoc Mode

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

▶Memory Configuration

Enforce POR (Plan of Record)

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

PPR Type

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

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 1866, 2000, 2133, 2400, 2666, and 2933. (**Note**: 2933 MHz memory is supported by the Second Generation Intel® Xeon® Platinum 82XX processor only.)

Data Scrambling for DDR4

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

tCCD_L Relaxation

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

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

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

Enable ADR

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

Data Scrambling for NVDIMM

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

Erase-Arm NVDIMMs

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

Restore NVDIMMs

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

Interleave NVDIMMs

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

Reset Trigger ADR (Async DIMM Self-Refresh)

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

S5 Trigger ADR

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

2X Refresh

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

Page Policy

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

IMC Interleaving

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

▶Memory Topology

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

- P1 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2
- P2 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2
- P3 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2
- P4 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2
- P5 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2
- P6 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2

- P7 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/DIMME1/DIMME2/DIMMF1/DIMMF2
- P8 DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/DIMME1/DIMME2/DIMMF1/DIMMF2

▶Memory Map

Use this submenu to configure the following Memory Map settings.

Volatile Memory Mode

Select 1LM to use 1LM memory mode for volatile memory modules installed in the system. Select 2LM to use 2LM memory mode for volatile memory modules installed in the system. The options are **Auto**, 1LM, and 2LM.

AppDirect Cache

Select Enable to support memory caching for the memory region. The options are **Disable**, Enable, and Auto.

eADR Support

Select Enable to utilize eADR capability in the platform. The options are **Disable**, Enable, and Auto.

1LM Memory Interleave Granularity

Use this feature to select 1LM memory interleave granularity setting to improve memory performance. The options are **Auto**, 256B Target, 256B Channel, and 64B Target, 64B Channel.

Channel Interleaving

Use this feature to configure interleave settings for memory channels to enhance memory performance. The options are **Auto**, 1-way Interleave, 2-way Interleave, and 3-way Interleave.

Rank Interleaving

Use this feature to configure interleave settings for memory ranks to enhance memory performance. The options are **Auto**, 1-way Interleave, 2-way Interleave, 4-way Interleave, and 8-way Interleave.

Socket Interleave Below 4GB

If this feature is set to Enable, memory located at 0-4GB address will be split between two sockets for memory interleaving. The options are **Disable** and Enable.

▶Memory RAS (Reliability_Availability_Serviceability) Configuration

Use this submenu to configure the following Memory RAS settings.

Static Virtual Lockstep Mode

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

Mirror Mode

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

UEFI ARM Mirror

If this feature is set to Enable, mirror mode configuration settings for UEFI-based Address Range memory will be enabled upon system boot. This will create a duplicate copy of data stored in the memory to increase memory security, but it will reduce the memory capacity into half. The options are **Disable** and Enable.

Memory Rank Sparing

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

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

Correctable Error Threshold

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

Intel Run Sure

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

SDDC Plus One (Available when supported by the CPUs installed)

Select Enable for SDDC (Single Device Data Correction) Plus One support, which will activate memory ECC mode for memory error checking and correction. It will also protect against memory failures caused by 'single-bit' errors in the same memory rank. The options are **Disable** and Enable.

ADDDC (Adaptive Double Device Data Correction) Sparing (Available when Intel Run Sure is set to Enable and when supported by the CPUs installed)

Select Enable for Adaptive Double Device Data Correction (ADDDC) support, which will not only provide memory error checking and correction but will also prevent the system

from issuing a performance penalty before a device fails. Please note that virtual lockstep mode will only start to work for ADDDC after a faulty DRAM module is spared. The options are Disable and **Enable**.

Patrol Scrub

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

Patrol Scrub Interval (Available when Patrol Scrub is set to Enable)

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

▶IIO Configuration

EV DFX (Device Function On-Hide) Features

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

▶Socket1 Configuration - Socket8 Configuration

IOU0 (IIO PCIe Br1)

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

IOU1 (IIO PCIe Br2)

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

IOU2 (IIO PCIe Br3)

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

MCP0 (IIO PCIe Br4)

Use this feature to configure the PCI-E Bifurcation setting for a PCI-E port specified by the user. The options are x16 and **Auto**.

MCP1 (IIO PCIe Br5)

Use this feature to configure the PCI-E Bifurcation setting for a PCI-E port specified by the user. The options are x16 and **Auto**.

▶Socket 1 PCI-E Br0D00F0 - Port 0/DMI (Available for Socket 1 Configuration)

Link Speed

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

The following information will display:

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

PCI-E Port Max (Maximum) Payload Size (Available for CPU 1 Configuration only)

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

▶IOAT Configuration

▶Socket1 IOAT Configuration - Socket8 IOAT Configuration

IOAT Function 0 Items - IOAT Function 7 Items

DMA

Select Enable to enable DMA (Direct Memory Access) support for the CB device specified by the user. The options are **Enable** and Disable.

No Snoop

Select Enable for No Snoop support for the CB device specified by the user. The options are **Disable** and Enable.

Disable TPH (TLP Processing Hint)

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

Prioritize TPH (TLP Processing Hint)

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

Relaxed Ordering

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

▶Intel VT for Directed I/O (VT-d)

Intel® VT for Directed I/O (VT-d)

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

ACS (Access Control Services) Control

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

Interrupt Remapping

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

PassThrough DMA

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

ATS

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

Posted Interrupt

Select Enable to support VT_D Posted Interrupt which will allow external interrupts to be sent directly from a direct-assigned device to a client machine in non-root mode to improve virtualization efficiency by simplifying interrupt migration and lessening the need of physical interrupts. The options are **Enable** and Disable.

Coherency Support (Non-Isoch)

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

▶Intel® VMD Technology

Use this feature to configure Intel Volume Management Device (VMD) Technology settings.

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

▶Intel® VMD for Volume Management Device on CPU1 BPN1 through Intel® VMD for Volume Management Device on CPU8 BPN2

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

▶IIO-PCIE Express Global Options

IIO-PCIE Express Global Options

The section allows the user to configure the following PCI-E global options:

PCI-E Hot Plug

Select Enable to support Hot-plugging for the selected PCI-E slots which will allow the user to replace the devices installed in the slots without shutting down the system. The options are Disable, **Enable**, Auto, and Manual.

PCI-E Completion Timeout (Global) Disable

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

▶South Bridge

The following South Bridge information will display:

- USB Module Version
- USB Devices

Legacy USB Support

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

XHCI Hand-Off

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

Port 60/64 Emulation

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

PCIe PLL SSC

Select Enabled for PCH PCI-E 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 Enabled and **Disabled**.

Port 61h Bit-4 Emulation

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

Install Windows 7 USB Support

Select Enabled to install the Windows 7 USB utility to support legacy USB devices for Windows 7 systems. The options are Enabled and **Disabled**.

▶Server ME (Management Engine) Configuration

This feature displays the following system ME configuration settings.

General ME Configuration

- Oper. (Operational) Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1/ME Firmware Status #2
  - Current State
  - Error Code

▶SATA Configuration

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

SATA Controller

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

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

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

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

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

SATA/sSATA RAID Boot Select (Available when Configure SATA as is set to RAID)

This feature allows the user to decide which controller should be used to boot the system. The options are None, SATA Controller, **sSATA Controller**, and Both.

Aggressive Link Power Management

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

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

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

SATA Port 0 - SATA Port 7

Hot Plug

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

Spin Up Device

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

SATA Device Type

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

▶sSATA Configuration

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

sSATA Controller

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

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

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

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

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

SATA/sSATA RAID Boot Select (Available when Configure sSATA as is set to RAID)

This feature allows the user to decide which controller should be used to boot the system. The options are None, SATA Controller, **sSATA Controller**, and Both.

Aggressive Link Power Management

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

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

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

sSATA Port 0 - sSATA Port 5

Hot Plug

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

Spin Up Device

This setting allows the SATA device installed on the SATA port specified by the user to start a COMRESET initialization when an edge is detected from 0 to 1. The options are Enable and **Disable**.

sSATA Device Type

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

▶PCIe/PCI/PnP Configuration

Note: PCIe/PCI/PnP Configuration settings may differ depending on the PCI-E devices installed on the motherboard.

The following PCI 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 **Enabled** and Disabled.

SR-IOV Support (Available if the system supports Single-Root Virtualization)

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

MMIOHBase

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

MMIO High Granularity Size

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

Maximum Read Request

Select Auto for the system BIOS to automatically set the maximum size for a read request for a 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

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

VGA Priority

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

Onboard Devices Option ROM Setting

Use this feature to configure the Option ROM setting for an onboard device specified by the user to be used for system boot.

Onboard Video OPROM (Option ROM)

Use this feature to set the type of the onboard video device specified by the user for system boot. The options are Do Not Launch, **Legacy**, and UEFI.

SIOM Module OPROM (Option ROM)

Use this feature to set the type of the SIOM (Super I/O Module) specified by the user for system boot. The options are Disabled, **Legacy**, and UEFI.

NVMe Module OPROM (Option ROM)

Use this feature to set the type of the NVMe module specified by the user for system boot. The options are Disabled, **Legacy**, and UEFI.

GPU Module OPROM (Option ROM)

Use this feature to set the type of the GPU module specified by the user for system boot. The options are Disabled, **Legacy**, and UEFI.

HDD Module OPROM (Option ROM)

Use this feature to set the type of the GPU module specified by the user for system boot. The options are Disabled, **Legacy**, and UEFI.

PCIE Module SLOT1 x16 OPROM/PCIE Module SLOT2 x16 OPROM/PCIE Module SLOT3 x16 OPROM/ PCIE Module SLOT4 x16 OPROM/PCIE Module SLOT5 x16 OPROM

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

▶Network Stack Configuration

Network Stack

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

If "Network Stack" is set to Enabled, the following items will display:

Ipv4 PXE Support

Select Enabled to enable Ipv4 PXE boot support. If this feature is disabled, it will not create the Ipv4 PXE boot option. The options are Disabled and **Enabled**.

Ipv4 HTTP Support

Select Enabled to enable Ipv4 HTTP boot support. If this feature is disabled, it will not create the Ipv4 HTTP boot option. The options are Enabled and **Disabled**.

Ipv6 PXE Support

Select Enabled to enable Ipv6 PXE boot support. If this feature is disabled, it will not create the Ipv6 PXE boot option. The options are Disabled and **Enabled**.

Ipv6 HTTP Support

Select Enabled to enable Ipv6 HTTP boot support. If this feature is disabled, it will not create the Ipv6 HTTP boot option. The options are Enabled and **Disabled**.

IPSEC Certificate

Select Enable to enable the IPSEC certificate for Ikev support. The options are Disabled and **Enabled**.

PXE Boot Wait Time

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

Media Detect Time

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

▶Super IO Configuration

Super IO Chip AST2500

▶Serial Port 1 Configuration

Serial Port

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

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

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

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of Serial Port 1. Select **Auto** for the BIOS to automatically assign the base I/O and IRQ address to a serial port specified.

The options 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).

▶Serial Port 2 Configuration

Serial Port

Select Enabled to enable Serial Port 2. The options are **Enabled** and Disabled.

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

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

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of Serial Port 2. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to a serial port specified.

The options for Serial Port 2 are **Auto**, (IO=2F8h; IRQ=3), (IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12), (IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12); (IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12), and (IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12).

Serial Port 2 Attribute

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

▶Serial Port Console Redirection

COM 1

Console Redirection

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

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

▶Console Redirection Settings (for COM 1)

Terminal Type

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

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

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**.

Putty KeyPad

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

COM2/SOL (Serial-Over-LAN)

Console Redirection (for SOL/COM2)

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

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

▶Console Redirection Settings (for SOL/COM2)

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

Terminal Type

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

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 data-sending 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 **Enabled** and Disabled**.**

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**.

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.

▶Legacy Console Redirection Settings

Legacy Console Redirection Settings

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

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.

Redirection After BIOS Post

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

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

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

Console Redirection (for EMS)

Select Enabled to use a COM port specified 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 user's configuration:*

▶Console Redirection Settings (for EMS)

Out-of-Band Management Port

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

Terminal Type

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

Bits Per Second

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

Flow Control

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

The setting for each these features is displayed:

Data Bits, Parity, Stop Bits

▶ACPI Settings

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

NUMA Support (Available when the OS supports this feature)

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

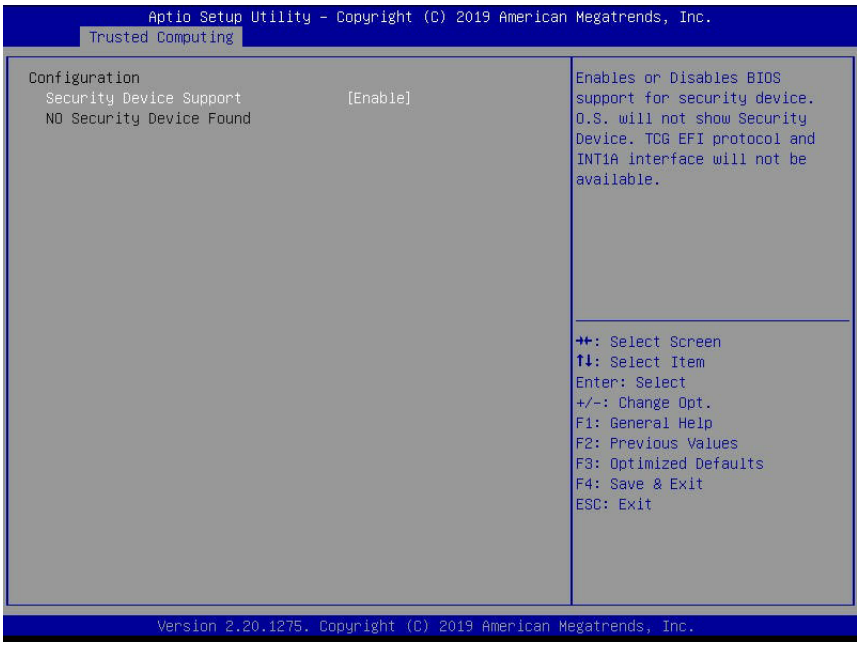
WHEA Support

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 **Enabled** and Disabled.

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

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

- TPM2.0 Device Found
- Firmware Version
- Vendor



Security Device Support

If 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 changes to take effect. The options are Disable and **Enable**. If this option is set to Enable, the following screen and items will display:

- Active PCR Banks
- Available PCR Banks

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending Operation

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

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

Platform Hierarchy (for TPM Version 2.0 and above)

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

Storage Hierarchy

Select Enabled for TPM Storage Hierarchy support that is intended to be used for non-privacy-sensitive operations by 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 the manufacturer to be used as an authentic TPM device attached to an authentic platform. A primary key can be 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 "IIO Configuration" in the "Chipset/North Bridge" submenu).

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

▶TLS Authenticate Configuration

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

▶Server CA Configuration

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

▸Enroll Certification

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

▸Enroll Cert (Certification) Using File

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

Cert (Certification) GUID (Global Unique Identifier)

This feature displays the GUID for this system.

▶Commit Changes and Exit

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

▶Discard Changes and Exit

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

▶Delete Certification

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

▶Client Certification Configuration

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

▶Enroll Certification

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

▶Enroll Cert (Certification) Using File

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

Cert (Certification) GUID (Global Unique Identifier)

This feature displays the GUID for this system.

▶Commit Changes and Exit

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

▶Discard Changes and Exit

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

▶Delete Certification

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

▶RAM Disk Configuration

This feature allows the user to configure the settings for the RAM disks installed in the system. When you select this submenu and press <Enter>, the following items will display:

Disk Memory

- Disk Memory Type: This feature specifies the type of memory that is available for you to create a RAM disk. The options are **Boot Service Data** and Reserved.

▶Create Raw

This feature allows the user to create a raw RAM disk from all available memory modules in the system. When you select this submenu and press <Enter>, the following items will display:

- **Size (Hex)**: Use this feature to set the size of the raw RAM disk. The default setting is **1**.
- **Create & Exit**: Select this feature when you want to exit from this submenu after you've created a raw RAM disk.
- **Discard & Exit**: Select this feature when you want to abandon the changes you've made and to exit from the submenu.

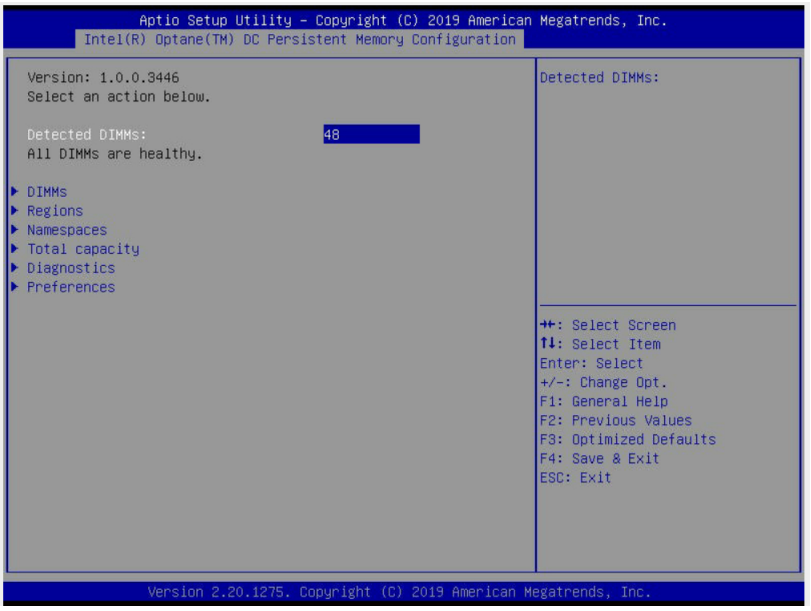
▶Create from File

This feature allows the user to create a RAM disk from a file specified by the user. Select this submenu and press <Enter>, the following items will display:

- **Create RAM Disk List**: Use this feature to create a RAM disk list.
- **Remove Selected RAM Disk(s)**: Use this feature to delete the RAM disk(s) specified by the user.

▶Intel® Optane® DC Persistent Memory Configuration

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



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

▶DIMMs

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

Select a specific DIMM that you want to view.

DIMMs on Socket 0x0000:/DIMMs on Socket 0x0001:/DIMMs on Socket 0x0002:/ DIMMs on Socket 0x0004:/DIMMs on Socket 0x0005:/DIMMs on Socket 0x0006:/ DIMMs on Socket 0x0007:

▶DIMM ID 0x0011 - DIMM ID 0x7101

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

- **DIMM UID**: This feature displays the unique ID of the DCPMM module.
- **DIMM Handle:** This feature displays the unique handle that the CPU assigns to the DCPMM module.

- **DIMM Physical ID:** This feature displays the physical ID of the DCPMM module.
- **Manageability State:** This feature indicates the manageability state of the DCPMM module.
- **Health State:** This feature indicates the health state of the DCPMM module.
- **Health State Reason:** This feature indicates the reason that effectuates the health state of the DCPMM module.
- **Capacity:** This feature indicates the capacity of the DCPMM module.
- **Firmware Version:** This feature indicates the firmware version of the DCPMM module.
- **Firmware API Version:** This feature indicates the firmware API version of the DCPMM module.
- **Lock State:** This feature indicates the lock state of the DCPMM module.
- **Staged Firmware Version:** This feature indicates the staged firmware version of the DCPMM module.
- **Firmware Update Status:** This feature indicates the firmware update status of the DCPMM module.
- **Manufacturer:** This feature indicates the manufacturer of the DCPMM module.

Show More Details

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

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

- Serial Number
- Part Number
- Socket
- Memory Controller ID
- Vendor ID
- Device ID
- System Vendor ID
- Subsystem Vendor ID
- Subsystem Device ID
- Device Locator
- Subsystem Revision ID

- Interface Format Code
- Manufacturing Information Valid
- Manufacturing Date
- Manufacturing Location
- Memory Type
- Memory Bank Label
- Data Width Label [b]
- Total Width [b]
- Speed [MHz]
- Channel ID
- Channel Position
- Revision ID
- Form Factor
- Manufacturer ID
- Controller Revision ID
- IS New
- Memory Capacity
- APP Direct Capacity
- Unconfigured Capacity
- Inaccessible Capacity
- Reserved Capacity
- Peak Power Budget [mW]
- Avg (Average) Power Budget [mW]
- Max Average Power Budget [mW]
- Package Sparing Capable

- Package Sparing Enabled
- Package Spares Available
- Configuration Status
- SKU Violation
- ARS Status
- Overwrite DIMM Status
- Last Shutdown Time
- First Fast Refresh
- Viral Policy Enable
- Viral State
- Latched Last Shutdown Status
- Unlatched Last Shutdown Status
- Security Capabilities
- Modes Supported
- Boot Status
- AIT DRAM Enabled
- Error Injection Enabled
- Media Temperature Injection Enabled
- Software Triggers Enabled
- Software Triggers Enabled Details
- Poison Error Injections Counter
- Poison Error Clear Counter
- Media Temperature Injections Counter
- Software Triggers Counter
- Master Passphrase Enabled

▶Monitor Health

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

- **Sensor Type**: This feature displays the type of health items that are being monitored.
- **Value**: This feature displays the value of the monitor sensor mentioned above.
- **Non-critical Thresholds:** This feature displays the normal threshold value for the DCPMM module to maintain normal operations.
- **Critical Lower Threshold:** This feature displays the lowest threshold value for the DCPMM module to maintain normal operations.
- **Critical Upper Threshold:** This feature displays the higher threshold value for the DCPMM module to maintain normal operations.
- **Fatal Threshold:** This feature indicates the highest value allowed for the DCPMM module to remain functional. Beyond this value, the DCPMM selected will become non-operational.
- **State:** This feature indicates the health state of the DCPMM module.
- A**larm Enabled State:** This feature indicates the status of the non-critical threshold alarm for the DCPMM module specified by the user.
- **Modify Non-critical Thresholds:** Use this feature to modify non-critical thresholds.
- **Controller Temperature:** This feature displays the controller temperature in Celsius.
- **Media Temperature:** This feature displays the media temperature in Celsius.
- **Percentage Remaining**

▶Apply Changes

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

▶Back to Main Menu

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

▶Update Firmware

Use this feature to select the firmware image to be loaded on the DCPMM module. Once it is loaded to the system, please reboot the system and select update for the firmware to take effect. The following items will display:

- **Current Firmware Version**: This feature displays the current firmware version.
- **Selected Firmware Version**: This feature allows the user to select a new firmware version to use.

- **File:** This feature allows the user to specify the file path in the root directory that contains the new firmware for firmware update.
- **Staged Firmware Version:** This feature indicates the staged firmware version of the DCPMM module specified by the user.

▶Update

Select this feature to update the firmware settings.

▶Back to Main Menu

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

▶Configure Security

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

State

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

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

▶Back to Main Menu

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

▶Configure Data Policy

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

First Fast Fresh State

Select Enabled to display the First Fast Fresh state for onboard DCPMM modules.

▶Enable First Fast Fresh State

Select Enabled to support the first fast fresh state of DCPMM data policy.

▶Disable First Fast Fresh State

Select Disable to disable the first fast fresh state of DCPMM data policy.

▶Back to Main Menu

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

▶Regions

Current Configuration

▶Region ID 1/Region ID 2/Region ID 3

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

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

Persistent Memory Type

Capacity

Free Capacity

▶Create Goal Configuration

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

- **Create Goal Configuration for**: Use this feature to select the target to create goal configuration for the DCPMM modules. The options are **Platform** and Socket.
- **Reserved [%]:** Use this feature to reserve a percentage of the DCPMM capacity for a particular purpose and keep this portion of memory space from being mapped into the physical address of system for system use.
- **Memory Mode [%]:** Use this feature to reserve a percentage of the DCPMM capacity for special use in a specific Memory Mode. Please note that this value can be automatically set by the system.

Persistent Memory Type

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

Namespace Label Version

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

▶Back to Regions Menu

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

▶Back to Main Menu

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

▶Namespaces

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

Namespace ID/Name/Heath Status

▶0x00000101/0x00000201/0x00000301/0x00000401/0x00000501/0x00000601/ 0x00000701

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

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

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

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

▶**Back to Namespaces**

▶**Back to Main Menu**

▶Create Namespace

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

Name

Region ID

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

Mode

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

Capacity Input

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

Units

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

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

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

▶Back to Namespace

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

▶Back to Main Menu

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

▶Total Capacity

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

- **Raw Capacity**: This feature specifies the raw capacity of the DCPMM module.

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

▶Back to Main Menu

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

▶Diagnostics

Perform Diagnostic Tests on DIMMs

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

Choose Diagnostics Type:

Quick Diagnostics

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

DIMM ID 0x0101/DIMM ID 0x0111/DIMM ID 0x0121/DIMM ID 0x0131/DIMM ID 0x0141/ DIMM ID 0x0151/DIMM ID 0x0161/DIMM ID 0x0171

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

Config (Configure) Diagnostics

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

FW (Firmware) Diagnostics

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

Security Diagnostics

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

▶Execute Tests

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

- TestName
- State
- Message

▶Back to Main Menu

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

▶Preferences

View and/or modify user preferences

Default DIMM ID

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

Capacity Units

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

App Direct Settings

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

App Direct Granularity

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

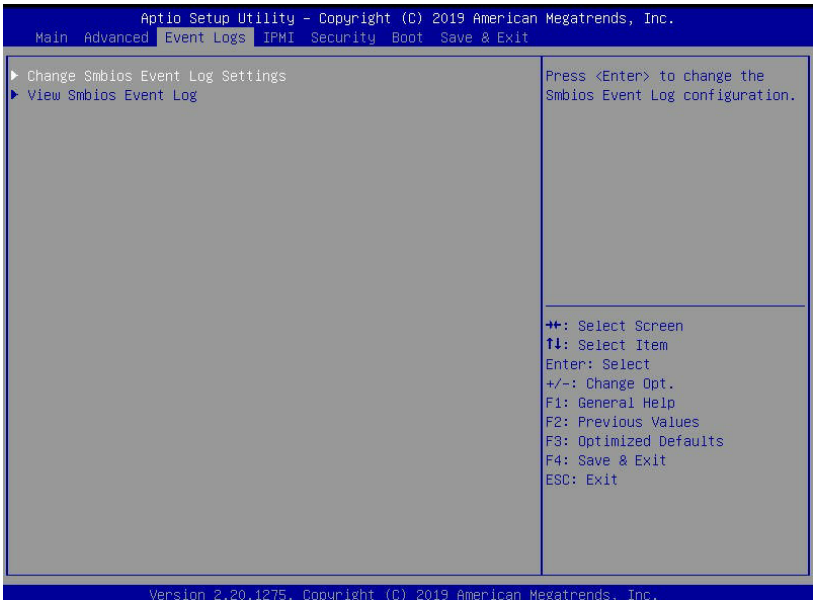
▶Back to Main Menu

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

3.4 Event Logs

Use this feature to configure Event Log settings.

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



▶Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

Erase Event Log

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

When Log is Full

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

SMBIOS Event Log Standard Settings

Log System Boot Event

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

MECI (Multiple Event Count Increment)

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

METW (Multiple Event Count Time Window)

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

▶View System Event Log

This feature allows the user to view the event in the system event log. Select this item and press <Enter> to view the status of an event in the log. The following categories are displayed: **Date/Time/Error Code/Severity**

3.5 IPMI

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

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

- **IPMI Firmware Revision**: This feature indicates the IPMI firmware revision used in your system.
- **Status of BMC**: This feature indicates the status of the BMC (Baseboard Management Controller) installed in your system.

▶System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

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

▶BMC Network Configuration

The following items will be displayed:

- IPMI LAN Selection: This feature displays the IPMI LAN setting. The default setting is **Dedicated**.
- IPMI Network Link Status: This feature displays the IPMI Network Link status. The default setting is **Dedicated LAN**.
- Station MAC Address: This feature displays the Station MAC address for this computer. Mac addresses are 6 two-digit hexadecimal numbers.
- VLAN: This feature displays the status of VLAN support. The default setting is **Disabled**.
- IPv4 Address Source: This feature displays the source of IPv4 addresses. The default setting is **DHCP**.
- Station IP Address: This feature displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).
- Subnet Mask: This feature displays the sub-network that this computer belongs to. The value of each three-digit number separated by dots should not exceed 255.
- Gateway IP Address: This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).
- IPv6 Address Status: This feature displays the IPv6 address status. The default setting is **Disabled**.
- Station IPv6 Address: This feature displays the station IPv6 address.
- Prefix Length: This item displays the prefix length.
- IPv6 Router IP Address: This feature displays the IPv6 router IP address.

Update IPMI LAN Configuration

Select Yes for the BIOS to implement all IP/MAC address changes upon next system boot. The options are **No** and Yes. If this option is set to Yes, the following items will display:

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

Use this feature to select the type of the IPMI LAN. The options are Dedicated, Shared, and **Failover**.

VLAN

Select Enabled to enable IPMI VLAN function support. The options are **Disabled** and Enabled.

Configuration Address Source

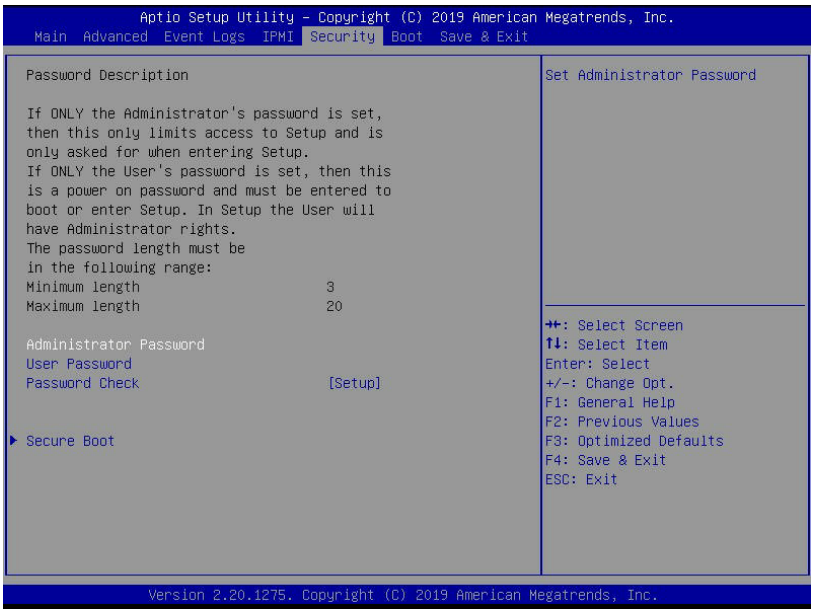
Use this feature to select the IP address source for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, AMI BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server attached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

IPv6 Support: Select Enabled for IPv6 support. The options are Enabled and **Disabled**. If this option is set to Enabled, the following item will display:

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

3.6 Security Settings

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



Administrator Password

Use this feature to set the administrator password which is required to enter the BIOS setup utility. The length of the password should be from 3 characters to 20 characters long.

User Password

Use this feature to set the user password which is required to enter the BIOS setup utility. The length of the password should be from 3 characters to 20 characters long.

Password Check

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

▸Secure Boot

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

- System Mode

Secure Boot

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

Secure Boot Mode

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

CMS Support

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

▸Restore Factory Keys

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

▸Reset to Setup Mode

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

▸Key Management

Vendor Keys

Factory Key Provision

Select Yes to install manufacturer default keys for system security use. The options are Enabled and **Disabled**.

▸Restore Factory Keys

Select Yes to restore all manufacturer default keys for system security use. The options are **Yes** and No.

▸Reset to Setup Mode

This feature resets the system to Setup Mode.

▸Export Secure Boot Variables

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

▸Enroll EFI Image

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

Device Guard Ready

▸Remove 'UEFI CA' from DB

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

▸Restore DB defaults

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

Secure Boot Variable/Size/Keys/Key Source

▸Platform Key (PK)

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

▸Key Exchange Keys

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

▸Authorized Signatures

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

▸Forbidden Signatures

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

▸Authorized TimeStamps

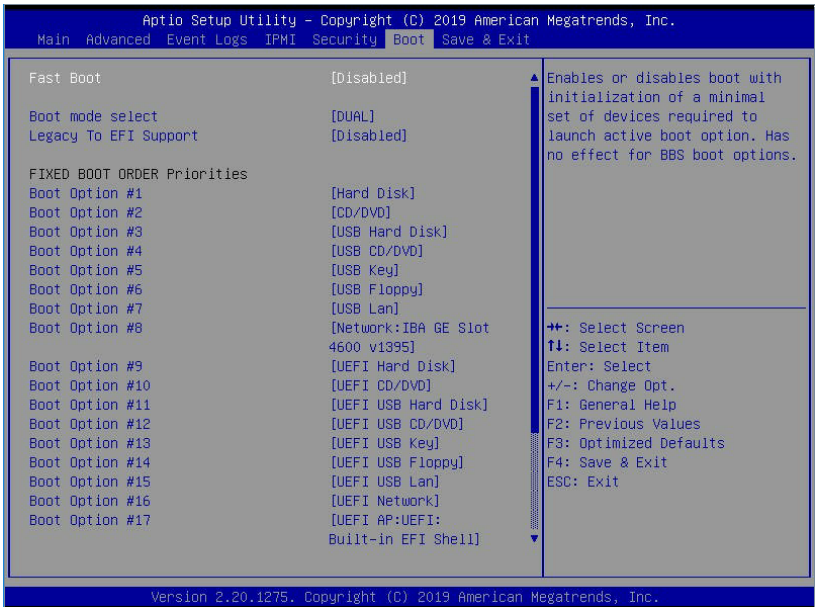
This feature allows the user to set and save the timestamps for the authorized signatures which will indicate the time when these signatures are entered into the system. Select Update to update your "Authorized TimeStamps". Select Append to append your "Authorized TimeStamps". The settings are Update,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

▸Os Recovery Signatures

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

3.7 Boot Settings

Use this feature to configure Boot Settings:



Fast Boot

Select Enabled to support fast boot by initializing a minimal set of devices that are required to boot up the system. The options are Enabled and **Disabled.**

Boot Mode Select

Use this feature to select the type of devices from which the system will boot. The options are Legacy, UEFI (Unified Extensible Firmware Interface), and **Dual.**

Legacy to EFI Support

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

Fixed Boot Order Priorities

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

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

- Boot Option #1 - Boot Option #17

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

- Boot Option #1 - Boot Option #8

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

- Boot Option #1 - Boot Option #9

Add New Boot Option

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

Add Boot Option

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

Path for Boot Option

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

Boot Option File Path

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

Create

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

▶Delete Boot Option

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

Delete Boot Option

Use this feature to remove an EFI boot option from the boot priority list.

▶Add New Driver Option

Use this feature to select a new driver to add to the boot priority list.

Add Driver Option

Use this feature to specify the name of the driver to be added to the boot priority list.

Path for Drover Option

Use this feature to specify the path to the driver that will be added to the boot priority list.

Driver Option File Path

Use this feature to specify the file path of the driver that will be added to the boot priority list.

Create

After the driver option name and the file path are set, press <Enter> to enter to submenu and click OK to create the new boot option drive.

▶Delete Driver Option

Use this item to select a boot driver to delete from the boot priority list.

Delete Drive Option

Select the target boot driver to delete from the boot priority list.

▶Hard Disk Drive BBS Priorities

- Boot Option #1 - #5

▶USB Key Drive BBS Priorities

- Boot Option #1

▶UEFI Application Boot Priorities

- Boot Option #1

▶Network Drive BBS Priorities

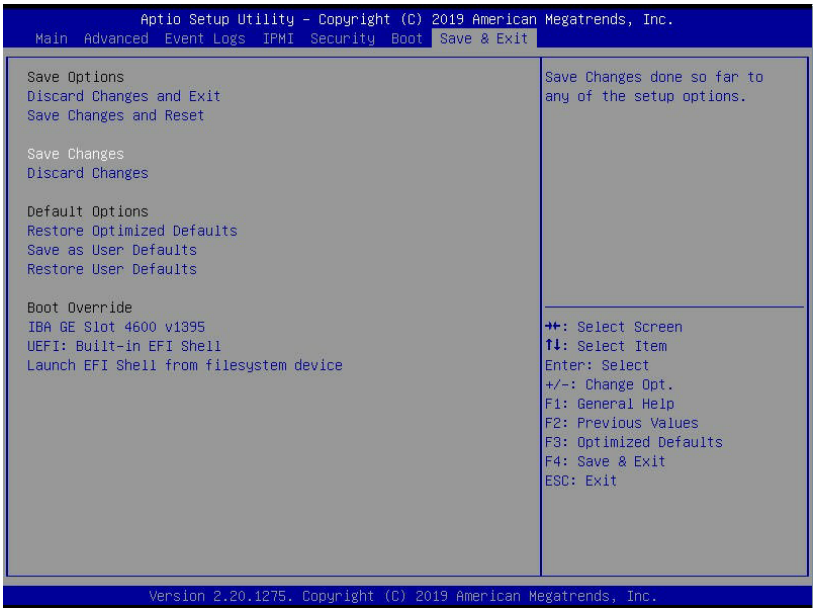
- Boot Option #1

▶UEFI Application Boot Priorities

- UEFI Boot Order #1 - This feature sets the system boot order of detected devices. The options are **UEFI: Built-in EFI Shell** and Disabled.

3.8 Save & Exit

Select the Save & Exit menu from the BIOS setup screen to configure the settings below.



Save Options

Discard Changes and Exit

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

Save Changes and Reset

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

Save Changes

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

Discard Changes

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

Default Options

Restore Optimized Defaults

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

Save As User Defaults

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

Restore User Defaults

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

Boot Override

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

Appendix A

BIOS POST Codes

A.1 BIOS POST Codes

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

Non-fatal errors are those which, in most cases, allow the system to continue with the 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. If a fatal error occurs, you should consult with your system manufacturer to best solutions.

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").

Appendix B

Software

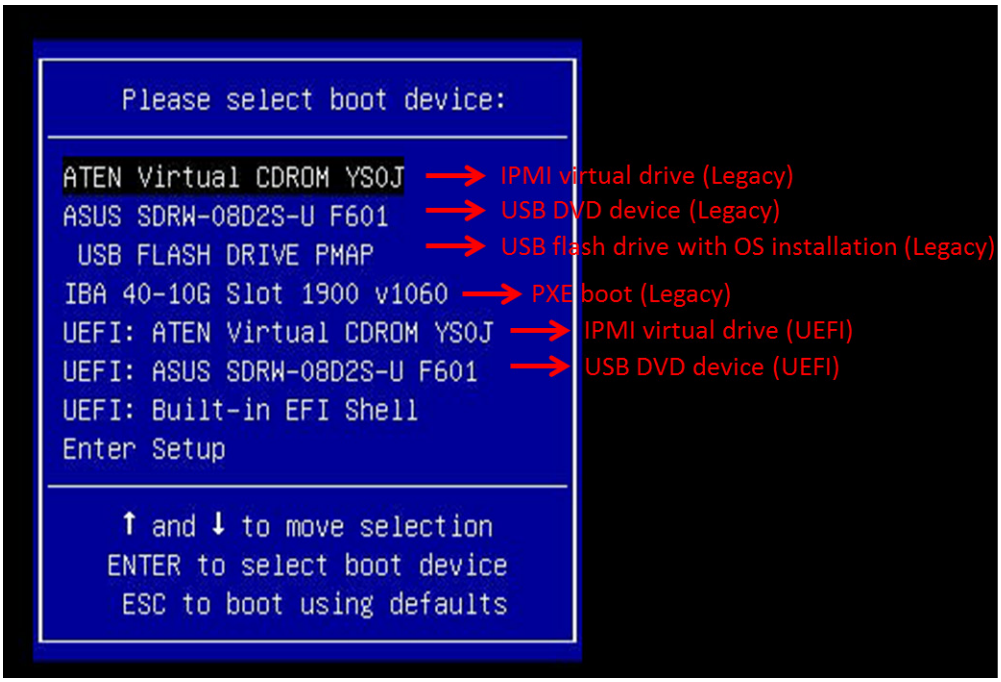
After the hardware has been installed, you can install the Operating System (OS), configure RAID settings and install the drivers.

B.1 Microsoft Windows OS Installation

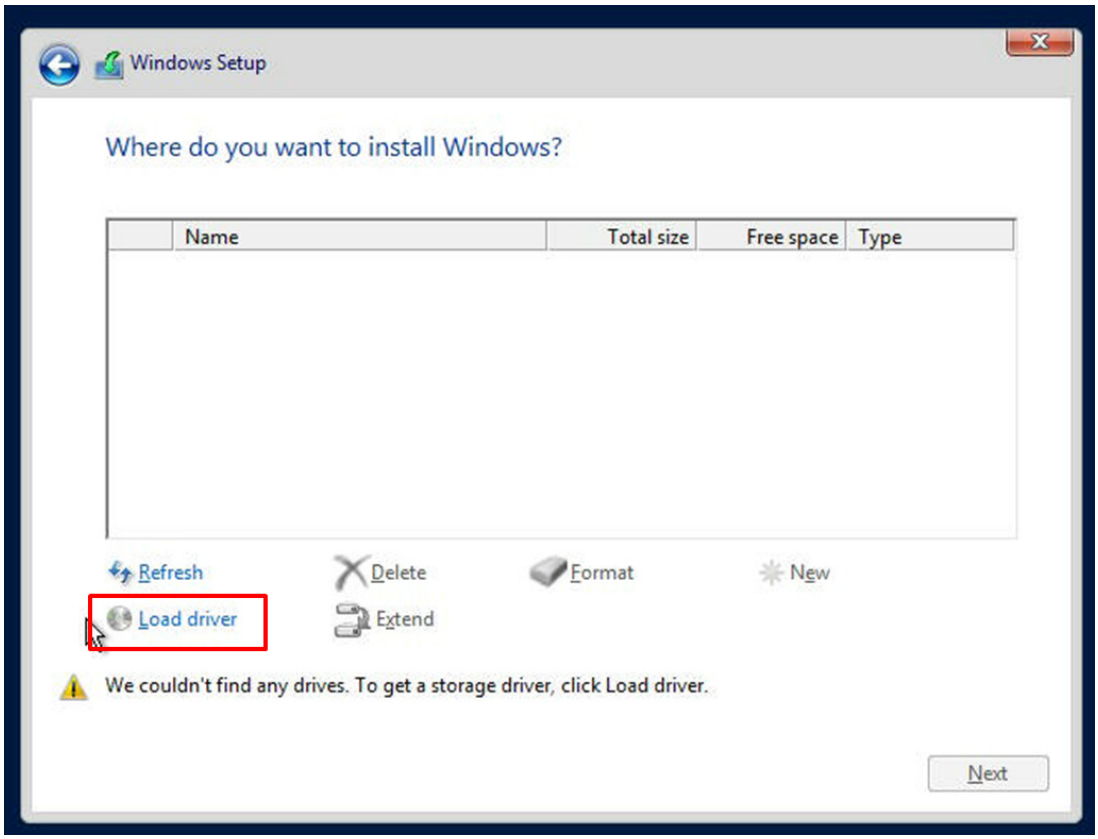
If you will be using RAID, you must configure RAID settings before installing the Windows OS and the RAID driver. Refer to the RAID Configuration User Guides posted on our website at www.supermicro.com/support/manuals.

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That might be a DVD, perhaps using an external USB/SATA DVD drive, or a USB flash drive, or the IPMI KVM console.
2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.
3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing **F11** during the system startup.



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



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

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

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

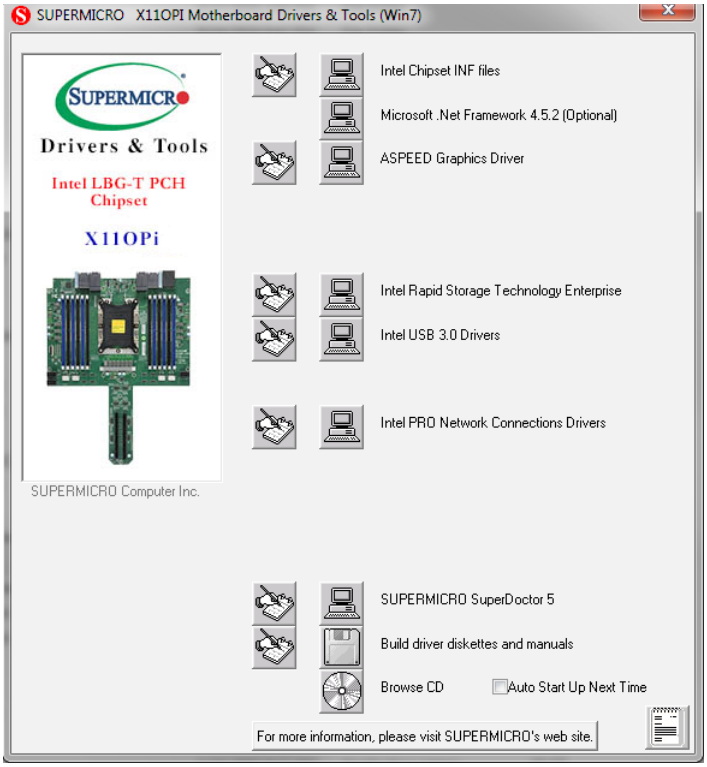
B.2 Driver Installation

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

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

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

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



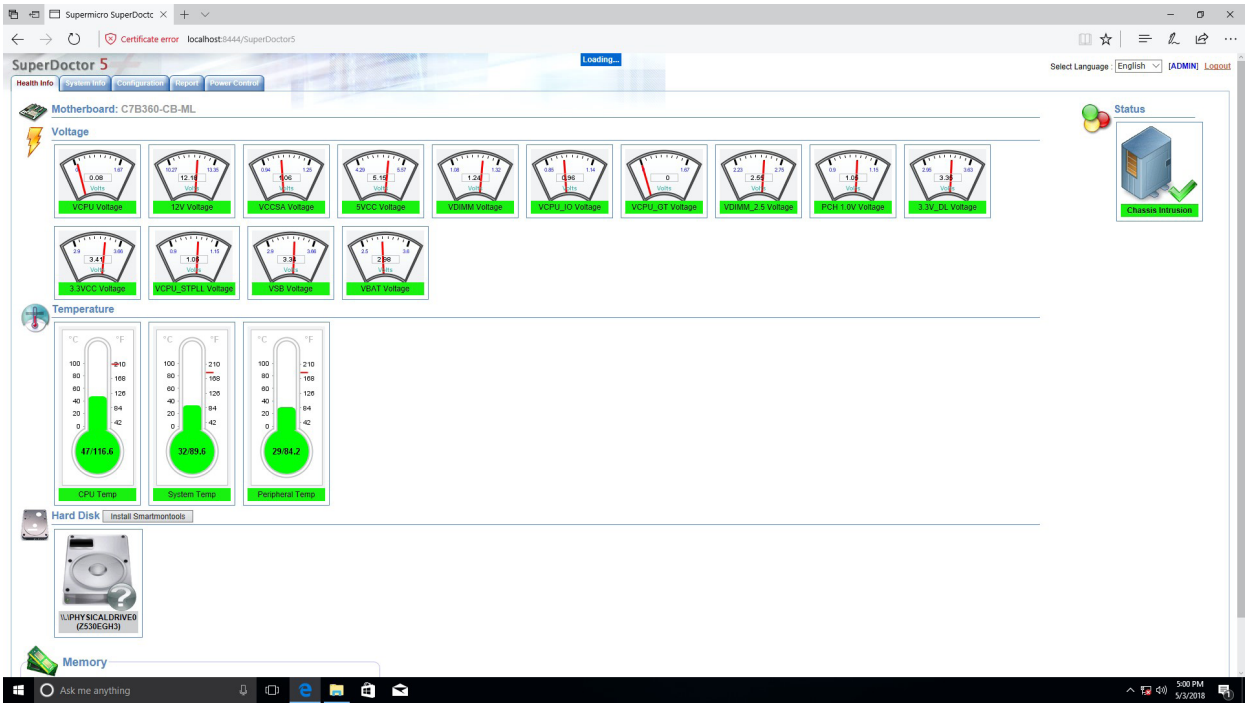
Note: Click the icons showing a hand writing on paper to view the readme files for each item. Click the computer icons to the right of these items to install each item (from top to the bottom) one at a time. **After installing each item, you must re-boot the system before moving on to the next item on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

B.3 SuperDoctor® 5

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

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

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



B.4 IPMI

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

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

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

Supermicro ships standard products with a unique password for the BMC user. This password can be found on a label on the motherboard.

When logging in to the BMC for the first time, please use the unique password provided by Supermicro to log in. You can change the unique password to a user name and password of your choice for subsequent logins.

For more information regarding BMC passwords, please visit our website at *http://www.supermicro.com/bmcpassword.*

Appendix C

Standardized Warning Statements

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

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

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

Battery Handling

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

電池の取り扱い

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

警告

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

警告

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

Warnung

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

Attention

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

¡Advertencia!

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

אזהרה !
קיימת סכנת פיצוץ של הסוללה במידה והוחלפה בדרך לא תקינה. יש להחליף את הסוללה בסוג התואם מחברת יצרן מומלצת.

סילוק הסוללות המשומשות יש לבצע לפי הוראות היצרן.

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

경고!

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

Waarschuwing

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

Product Disposal

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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה !

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

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

경고!

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

Waarschuwing

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

Appendix D

UEFI BIOS Recovery

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

D.1 Overview

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

D.2 Recovering the UEFI BIOS Image

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

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

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

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

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

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

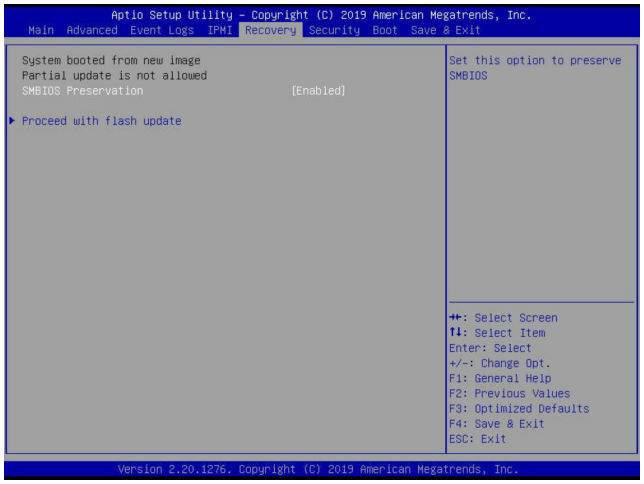
To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below.

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

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

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

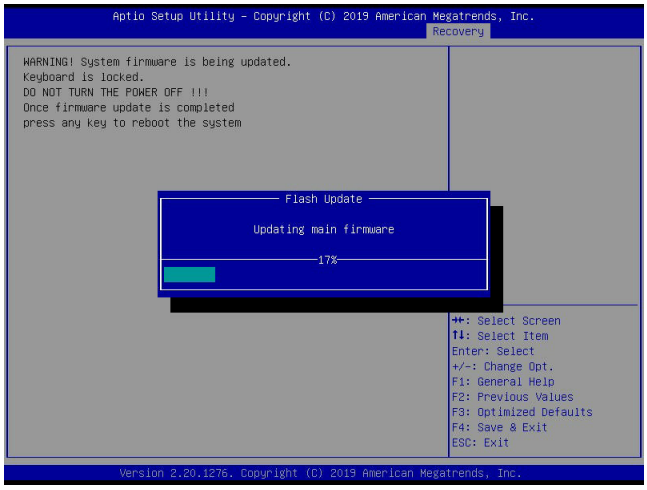
5. After locating the SUPER.ROM file, the system will enter the BIOS Recovery menu as shown below.



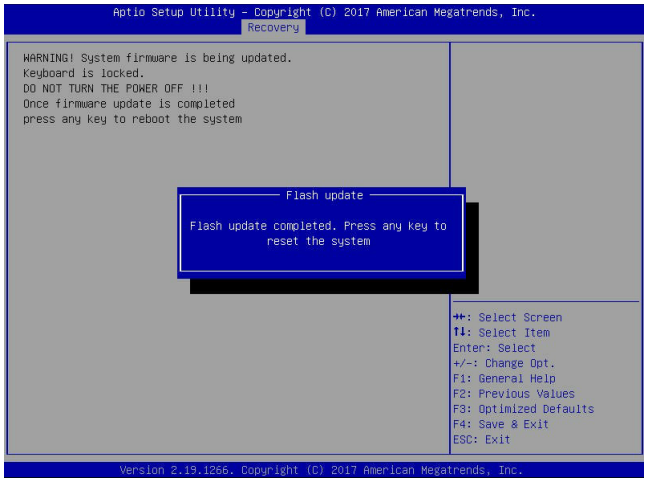
Note: At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

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

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

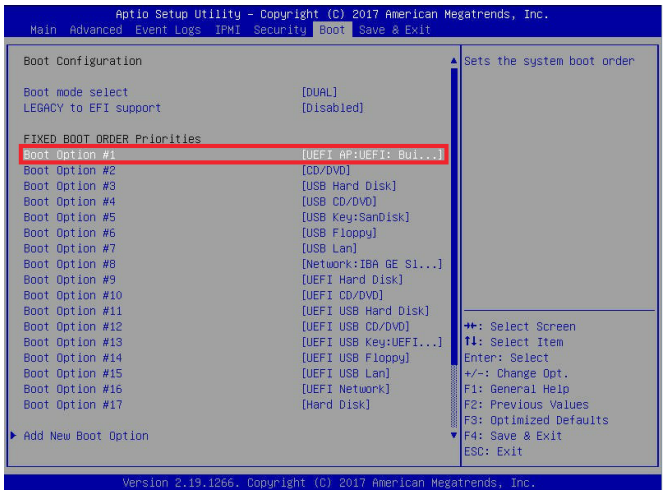


7. After the BIOS recovery process is complete, press any key to reboot the system.

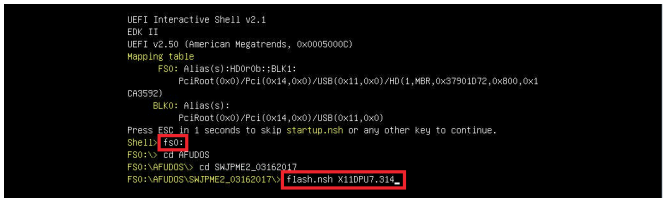


Note: It is recommended that you update your BIOS after BIOS recovery. Please refer to Chapter 3 for BIOS update instructions.

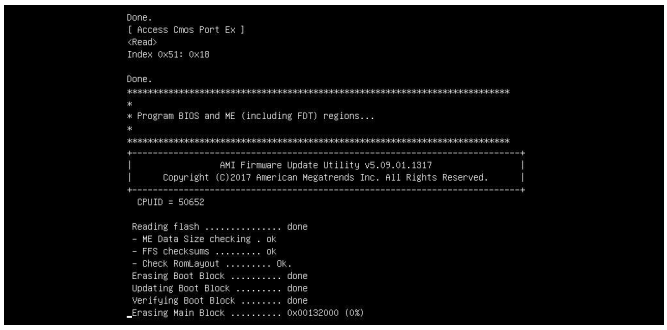
8. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the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



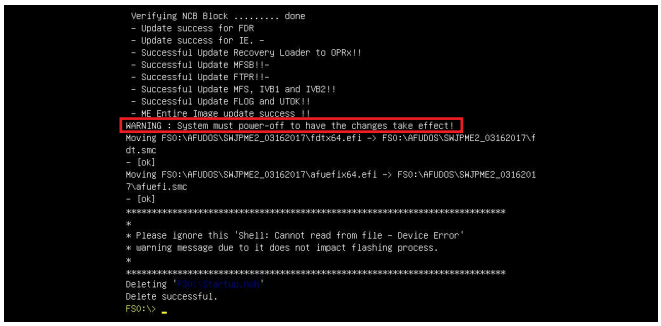
9. When the UEFI Shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 1. Enter flash.nsh BIOSname#.### at the prompt to start the BIOS update process.



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



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



Appendix E

Configuring VROC RAID Settings

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

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

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

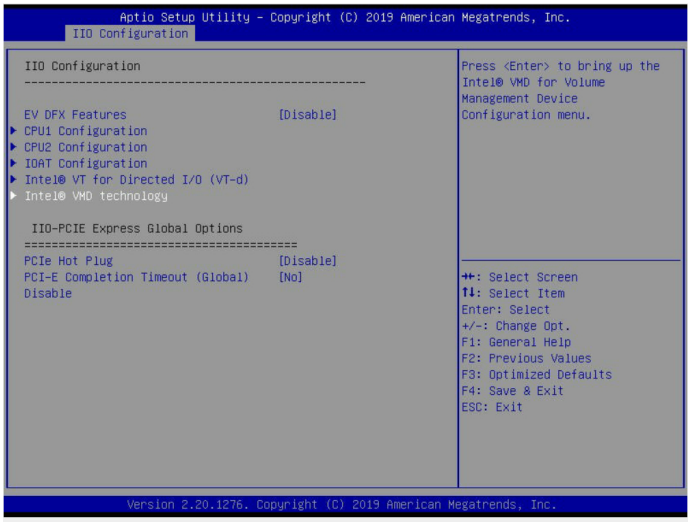
E.1 All Intel VMD Controllers Menu

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

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

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

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



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

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

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

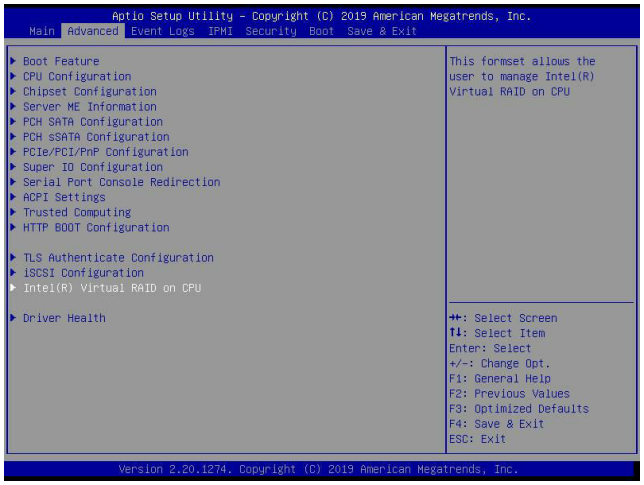
10. Repeat Step 8 ~ Step 9 to select and enable all the PCI slots of your choice for VMD support.

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

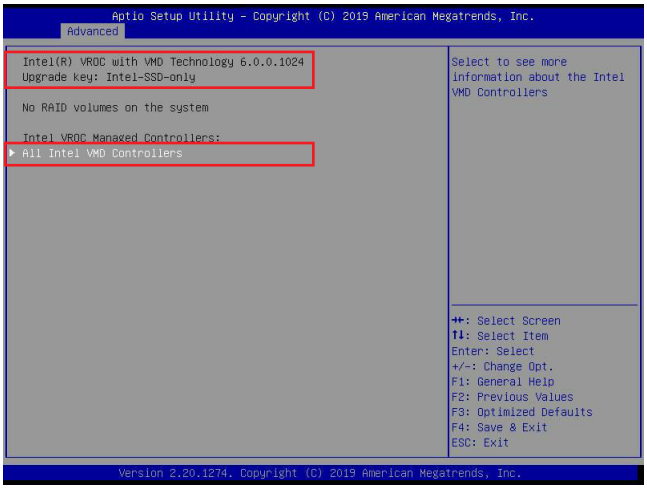
12. Press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility.

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

13. Navigate to the Advanced tab.



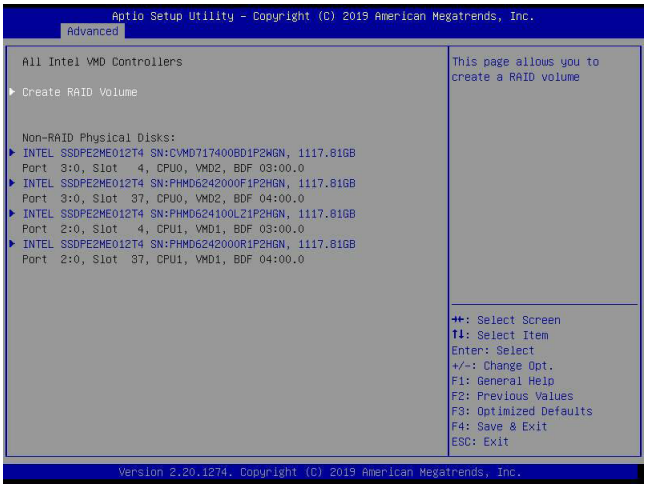
14. Use the arrow keys to select Intel(R) Virtual RAID on CPU and press <Enter> to access the menu items. The following screen will appear showing that the feature "**All Intel VMD Controllers**" has become available.



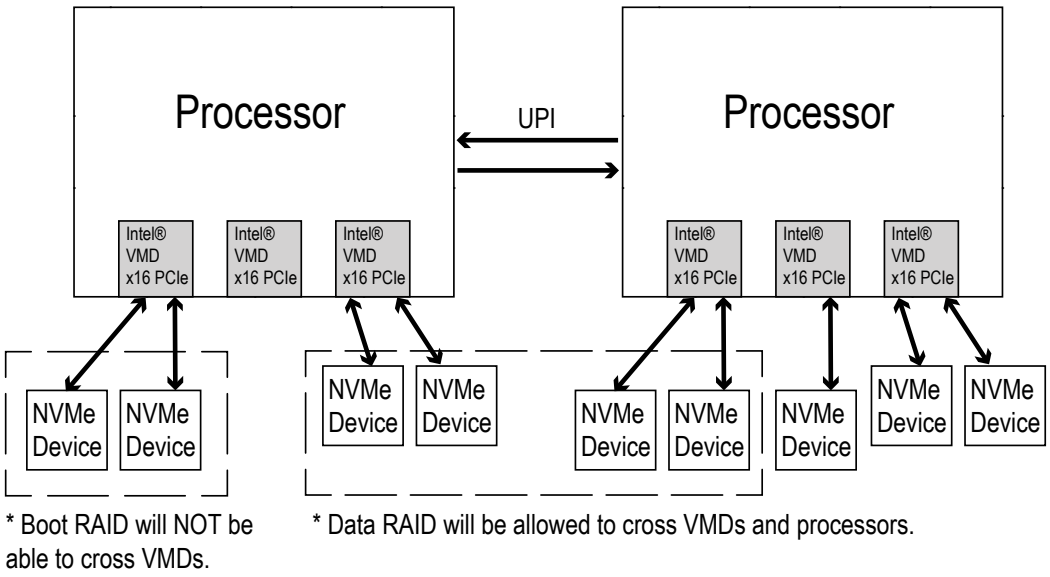
Note 1: The license and header (on the motherboard) for Intel® VROC hardware key are required. Also, be sure the version of Intel® Rapid Storage Technology enterprise (Intel® RSTe) VROC utility is 5 or above (look for Intel(R) VROC with VMD Technology x.x.x.xxxx shown on the screen).

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

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

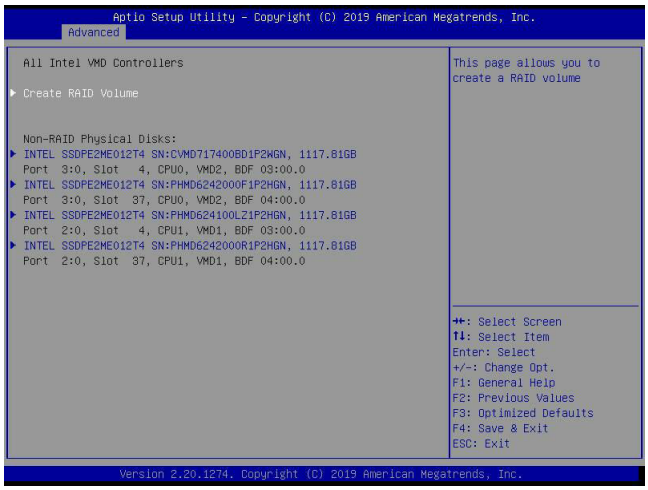


Note : A single Intel® VMD supported processor supplies 48 PCIe lanes and contains three Intel® VMD controllers (domains). Refer to the following illustration for more information.



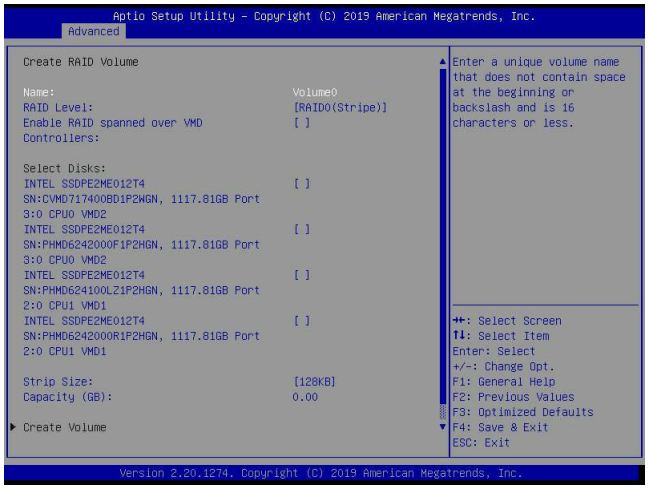
E.2 Configuring RAID Settings

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



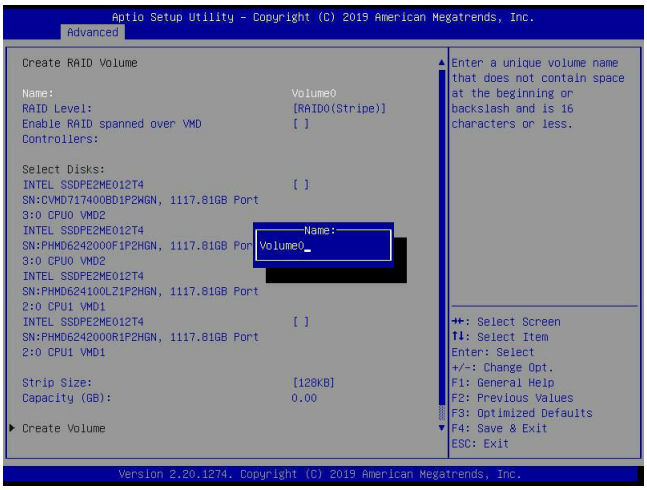
To Create a RAID Volume

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



To Enter a Name for the RAID Volume

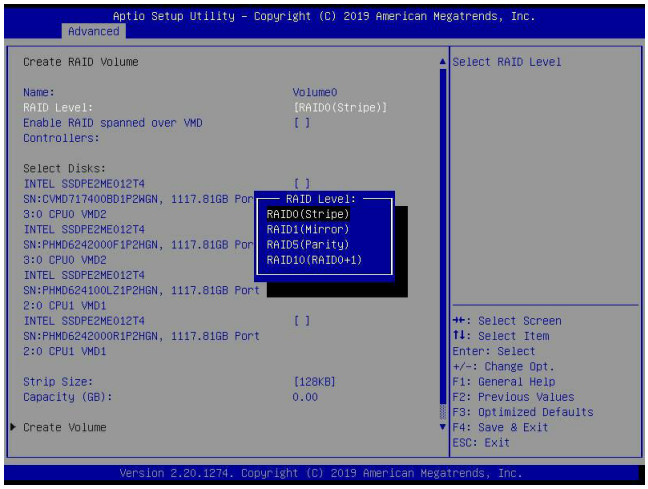
From the **Create RAID Volume** submenu as shown on the previous screen, use the arrow keys to select **Name** and press <Enter>, and the following screen will display.



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

To Set the RAID Level for the RAID Volume

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



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

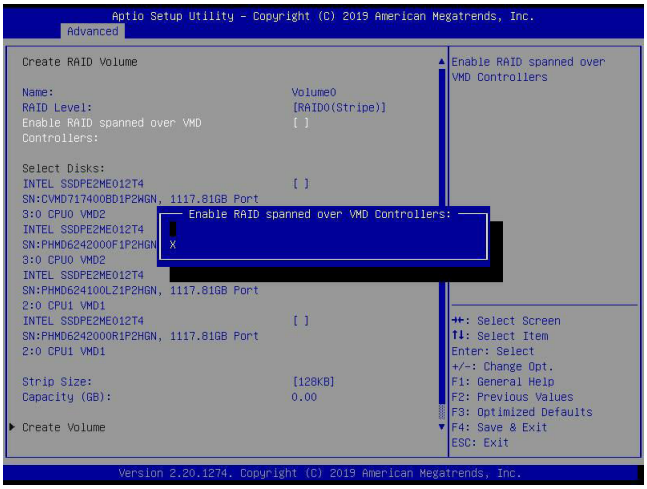
Note 1: The RAID level(s) displayed is(are) based on the number of NVMe devices connected to the system.

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

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

Enabling RAID Spanned over VMD Controllers

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

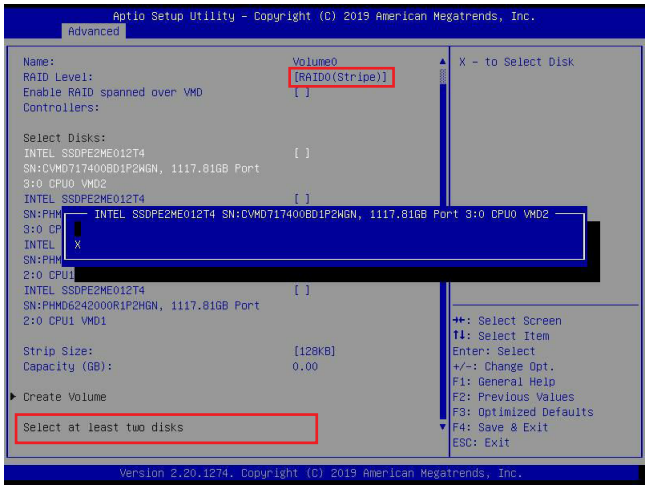


Enter a desired setting for your RAID volume in the pop-up menu. The options are **(not selected)** and X (selected). Please set this feature to X if the RAID level you selected earlier from Step 3 will cross VMD domains.

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

To Select Disks for the RAID Volumes

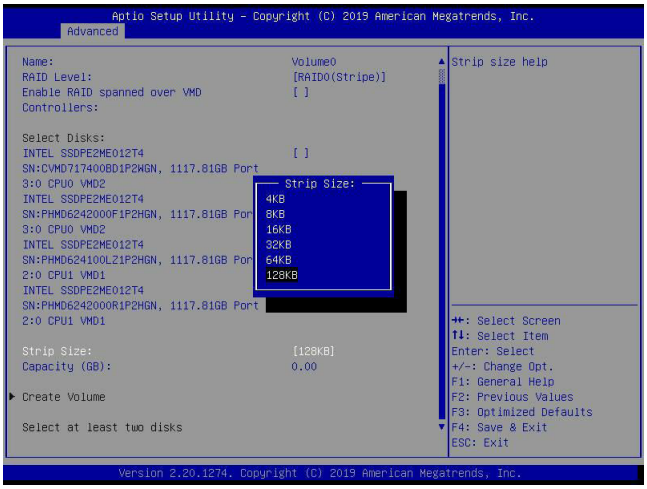
From the **Create RAID Volume** submenu, use the arrow keys to highlight **Select Disk:** and press <Enter>. The following screen will display.



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

To Set Strip Size for the RAID Volume

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

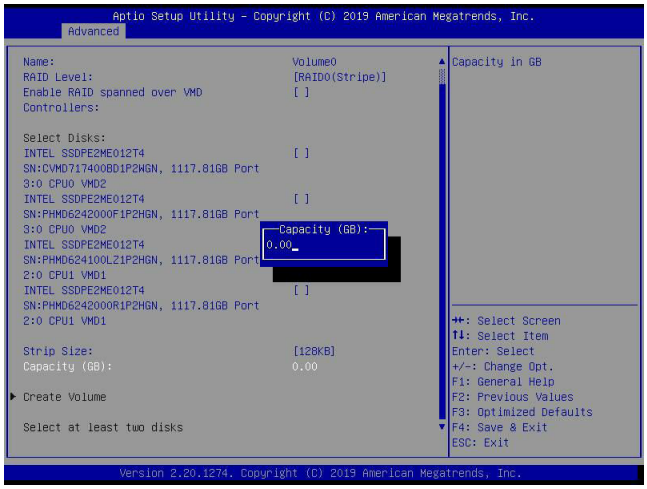


From the pop-up menu as shown above, select the desired RAID strip size for your RAID volume and press <Enter>. The options are 4KB, 8KB, 16KB, 32KB, 64KB, and **128KB**.

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

To Set the Capacity (GB) for the RAID Volume

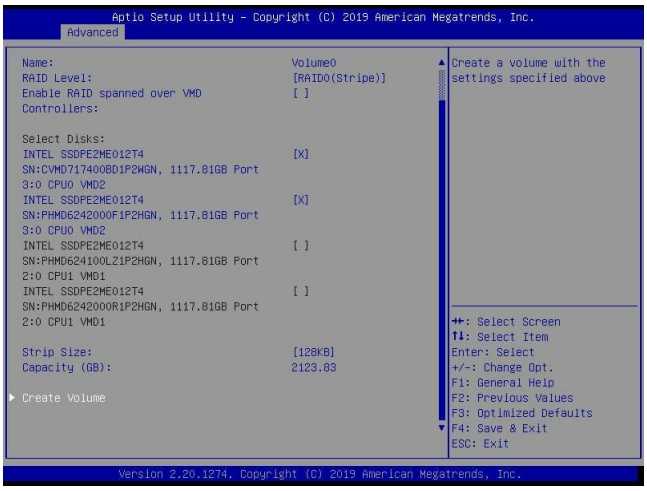
From the **Create RAID Volume** submenu, use the arrow keys to select **Capacity (GB):** and press <Enter>. The following screen will display.



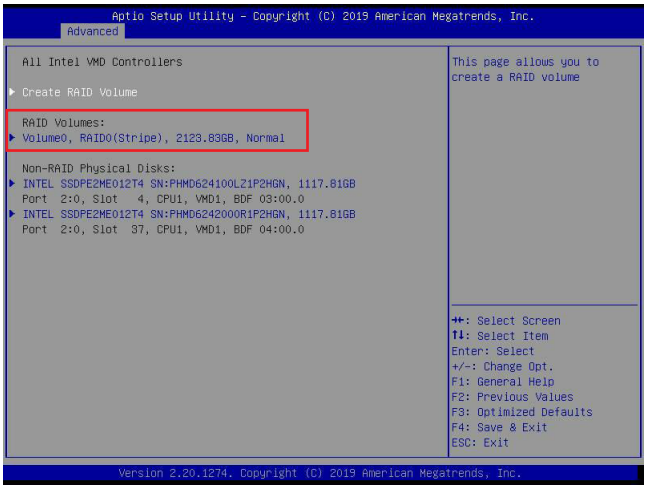
Enter the desired RAID capacity (in GB) in the pop-up menu to set the capacity for your RAID volume.

To Create Volumes

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

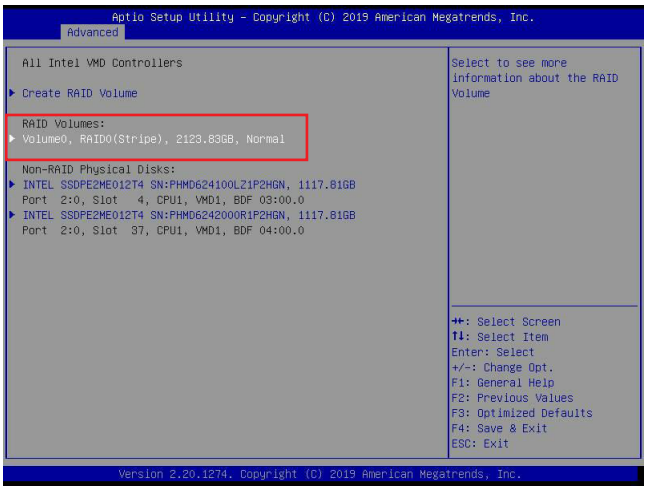


After selecting **Create Volume**, press <Enter>. The following screen will appear and display RAID volumes as shown below.



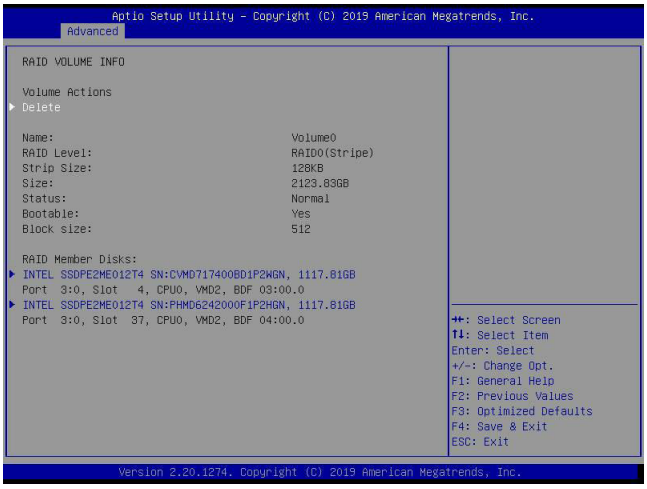
To Display RAID Volumes

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



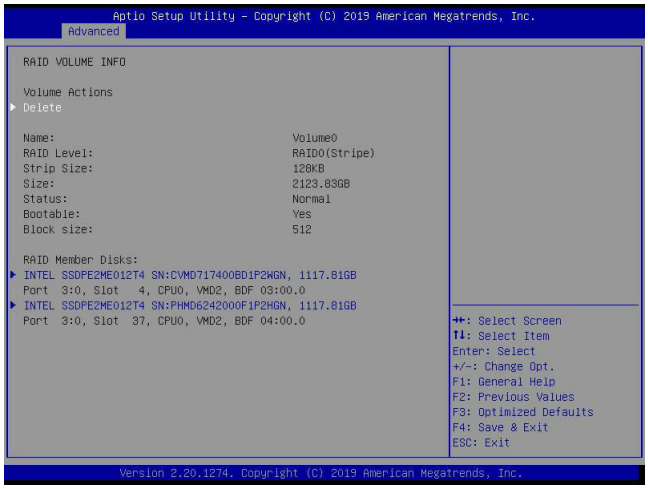
To Display RAID VOLUME Information

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



To Delete a RAID Volume

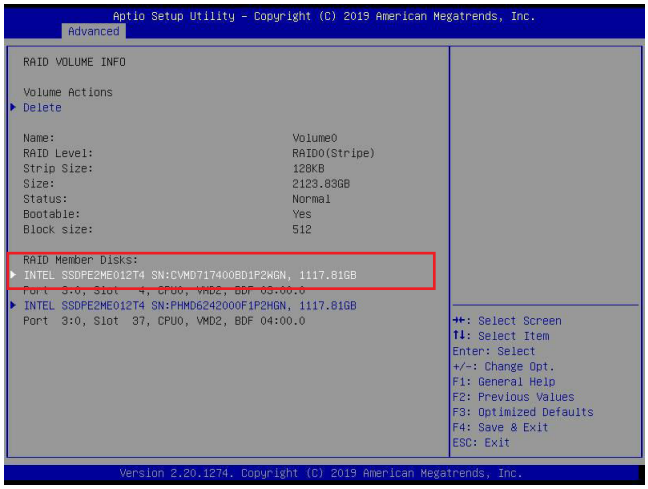
On the **RAID VOLUME INFO** menu, use the arrow keys to select Delete and press <Enter> to delete the RAID volume you have selected.



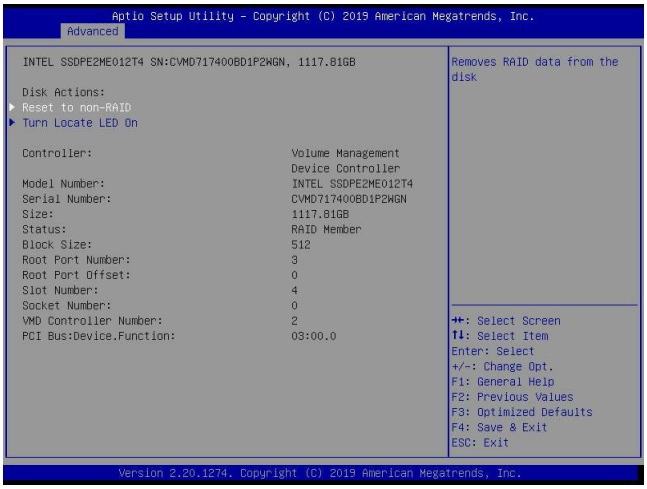
The following screen will appear to confirm if you want to delete the RAID Volume. Select Yes to delete the RAID Volume. The options are **Yes** and No.

To Reset the RAID Volume to non-RAID

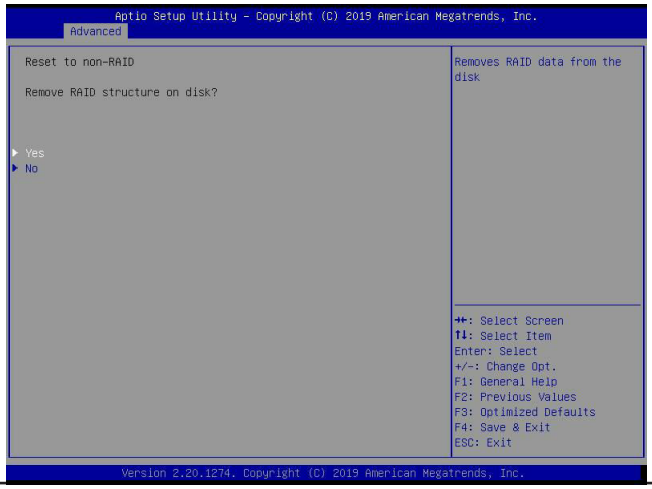
On the **RAID VOLUME INFO** submenu shown on the bottom screen of page 167, select the desired NVMe device from the list of RAID Member Disks and press <Enter> as shown below.



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

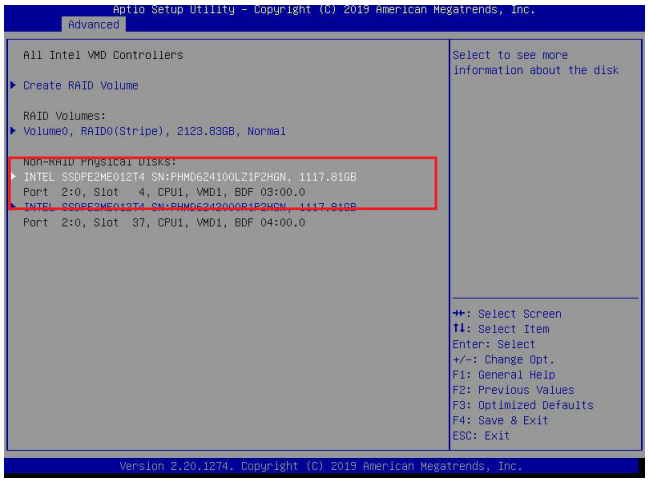


When the following screen appears, select Yes to confirm that you want to set the selected NVMe device to non-RAID. The options are **Yes** and No.

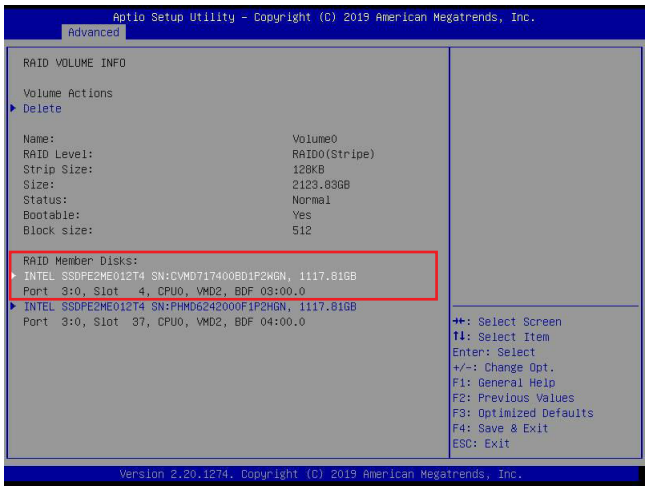


To Turn on the Disk Locator LED

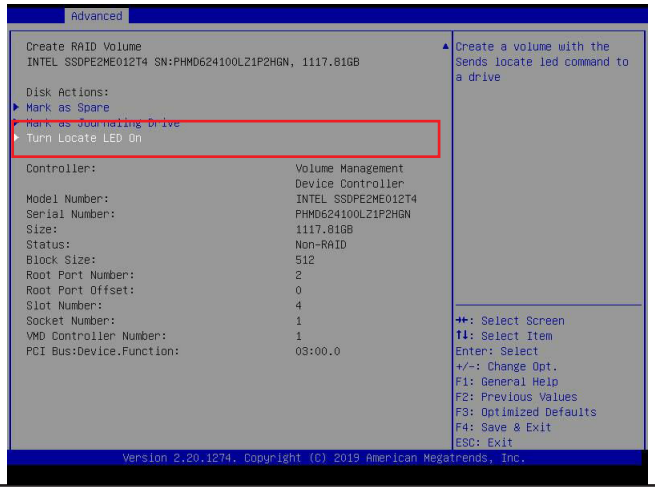
Follow the instructions stated in the E.1 section to access the **All Intel VMD Controllers** menu. When the following screen displays, select a non-RAID physical disk to turn on the disk locator LED to locate a selected device.



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

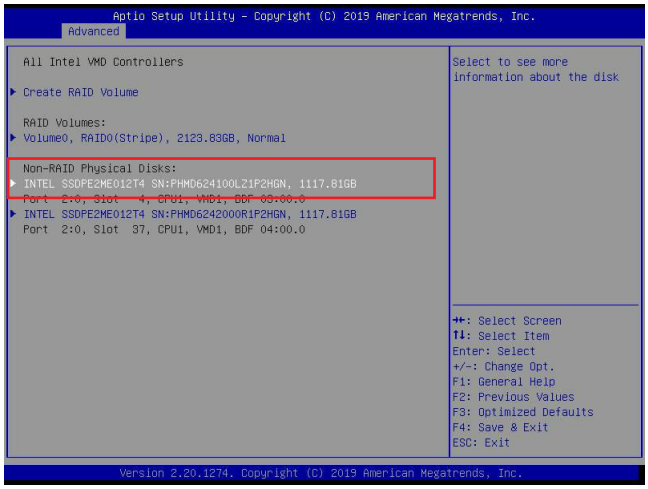


When the following screen appears, use the arrow keys to select **Turn Locate LED On**. Press <Enter> to turn on the locator LED to show the location of the selected device.

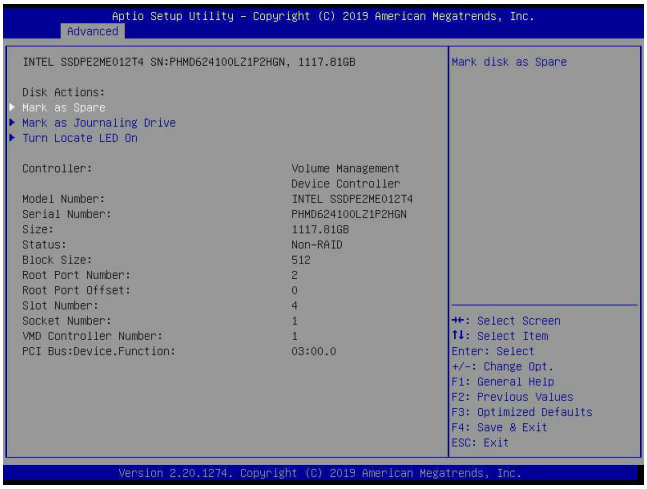


To Mark a RAID Volume as Spare

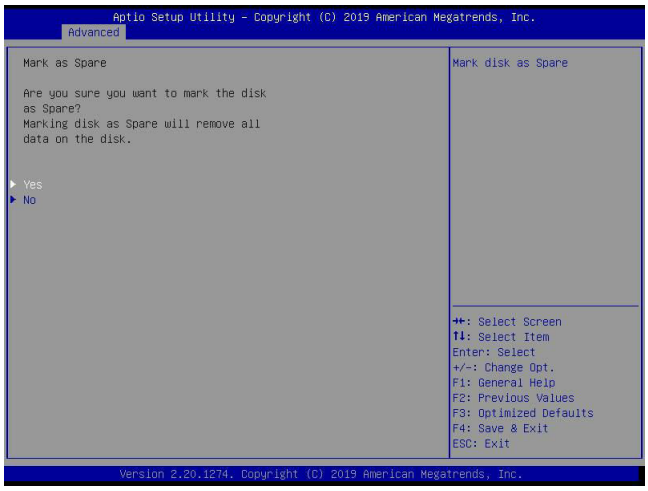
Follow the instructions stated in the E.1 section to access the **All Intel VMD Controllers** menu. When the following screen appears, select a desired NVMe device from the list of Non-RAID Physical Disks.



After a NVMe device is selected, press <Enter> and the following screen will appear. Select **Mark as Spare** and press <Enter> to mark the selected device as a spare device.



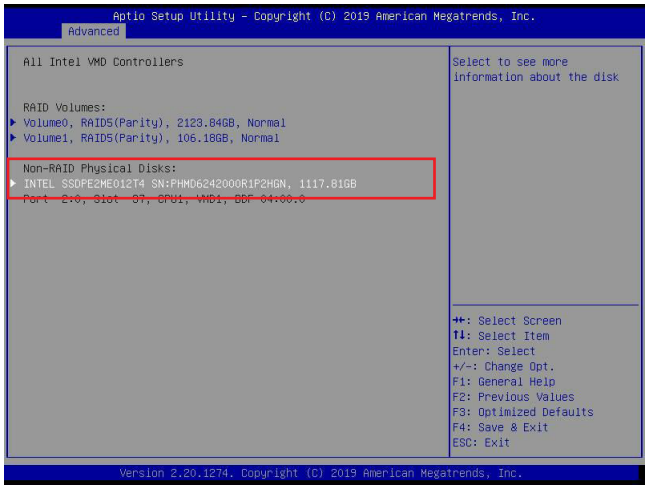
When the following screen appears, select Yes to confirm that you want the selected device to be used as a spare device. The options are **Yes** and No.



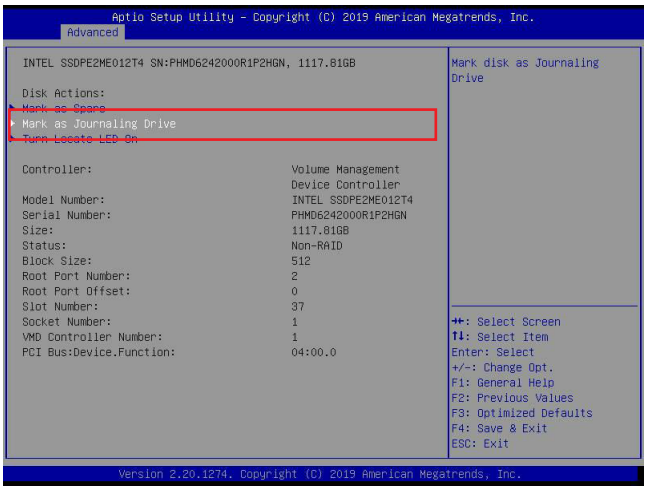
Note: A spare disk is used for automatic RAID volume rebuilds when status of failed, missing, or at risk is detected on the array disk. For a RAID0 volume, only status of at risk will trigger automatic RAID volume rebuilds.

To Mark a RAID Volume as a Journaling Drive

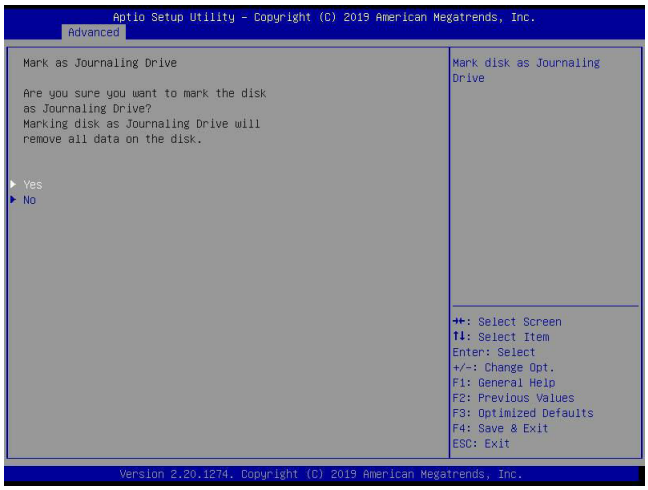
Refer to the instructions stated in the E.1 section to access the All Intel VMD Controllers menu. When the following screen appears, select a desired NVMe device from the list of Non-RAID Physical Disks for use as a journaling drive.



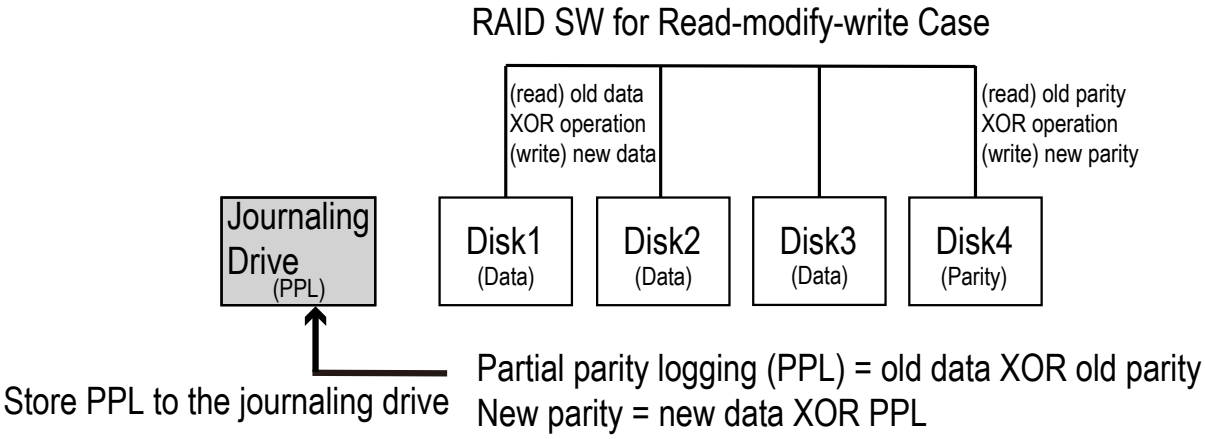
After selecting a NVMe device, press <Enter> and the following screen will appear. Select **Mark as Journaling Drive** and press <Enter>.



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



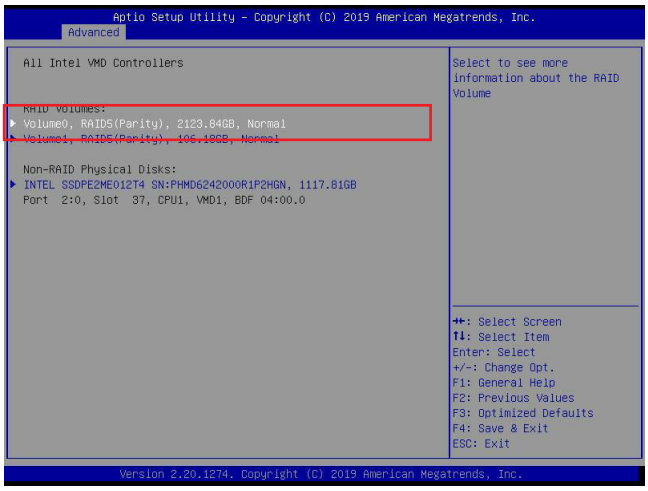
Note: RAID Write Hole (RWH) is a condition associated with a power/drive-failure/crash while writing to a RAID5 volume. The use of journaling drive that contains partial parity logging (PPL) can reduce the potential data loss. Refer to the following illustration for the use of journaling drive.



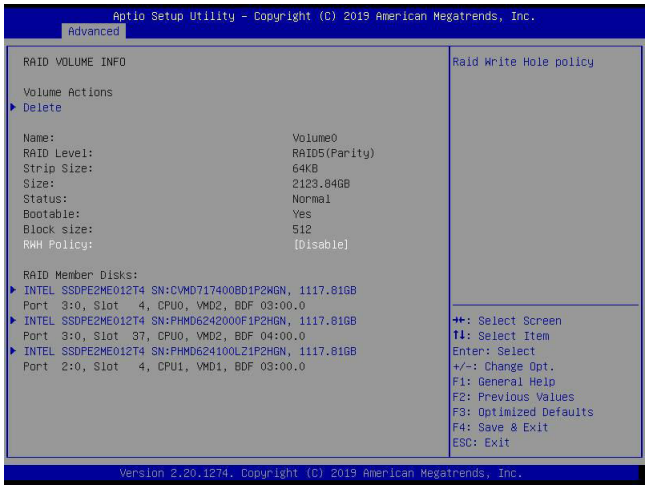
E.3 Use of Journaling Drive

The following section describes the use of a journaling drive for the RAID5 volume, which is a parity-based RAID.

Step 1. Refer to the instructions stated in the E.1 section to access All Intel VMD Controllers menu items. When the following screen appears, use the arrow keys to select the desired RAID5 volume.



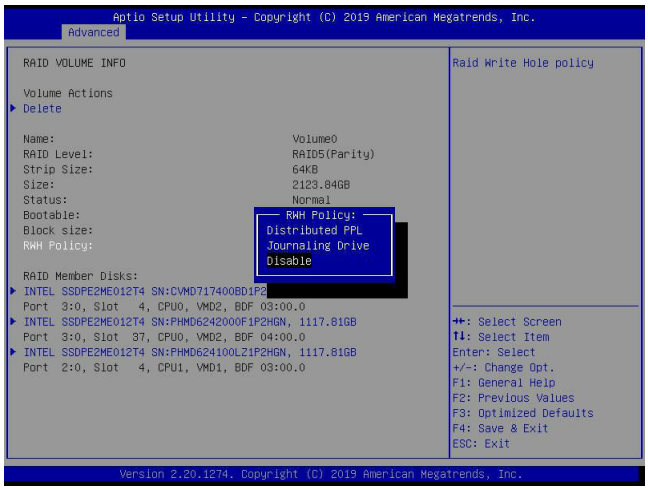
Press <Enter> and the following screen will appear.



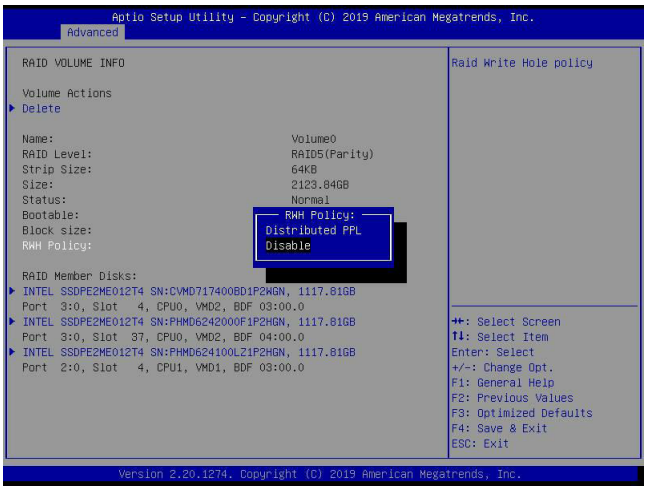
Step 2. Use the arrow keys to select RWH Policy. RWH is a scenario related to a power/drive-failure/crash.

RWH Policy

Press <Enter> and the following screen will appear. If any device has been set as a journaling drive (see pages 173 and 170), the options are Distributed PPL, Journaling Drive, and **Disable**.



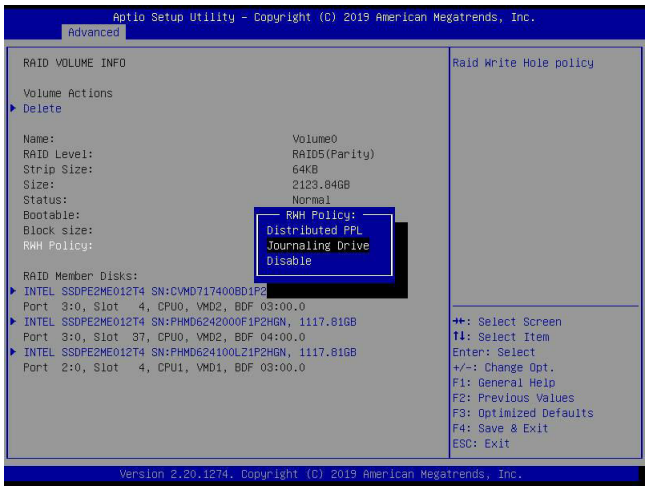
If no device has been set as a journaling drive, the options are Distributed PPL and **Disable**.



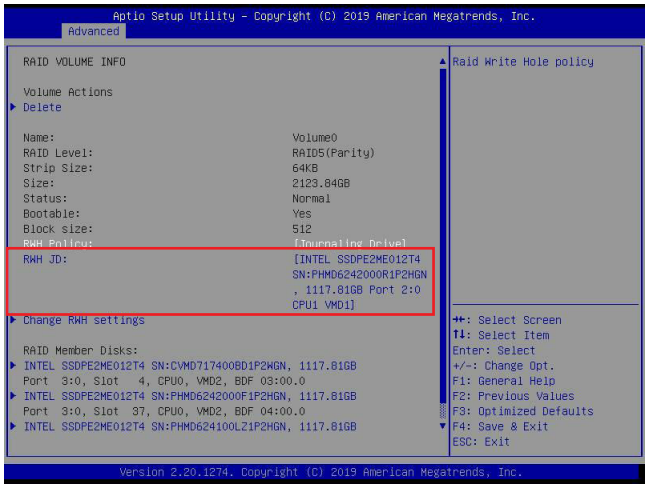
Note 1: Partial parity logging (PPL) can be defined as the result of XOR calculation of old data and old parity. PPL is a feature available for RAID5 volumes. While a power/drive-failure/crash occurring, PPL information helps rebuild the RAID volume and reduce the potential data loss.

Note 2: For the RWH condition, the Intel® RSTe 5.X or above RWH closure algorithm provides the option of use of an additional NVMe device for RAID volume rebuilds (Journaling Drive RWH closure mode). Without the use of an additional NVMe device, PPL distributed RWH closure mode can be utilized to close the RWH by using the parity drive for example.

Step 3. Set the feature, RWH Policy, to **Journaling Drive**.

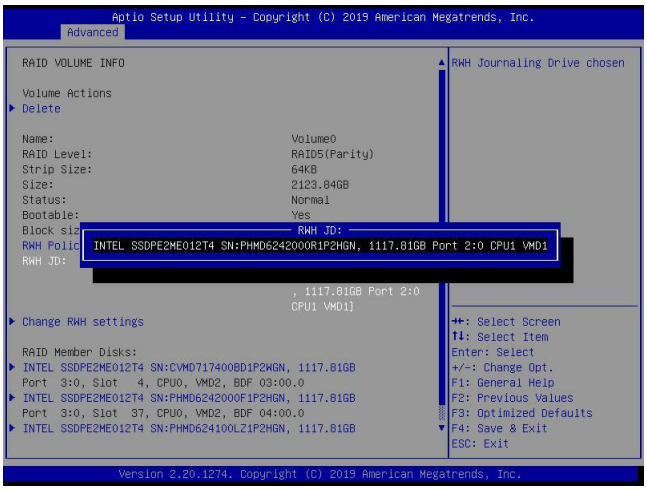


Press <Enter> and the RWH JD feature will become available as shown below.



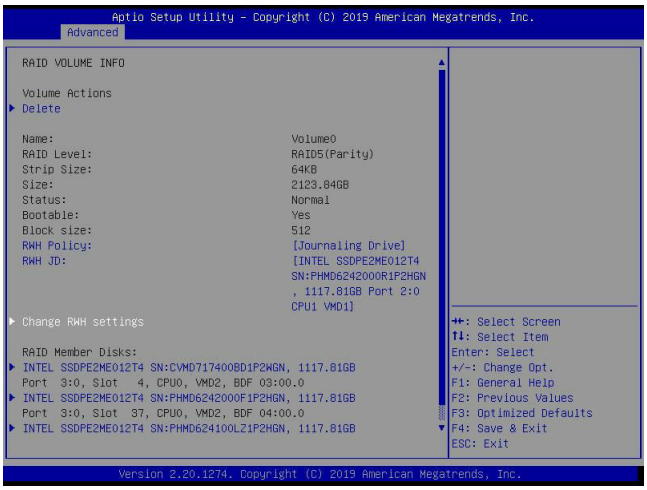
RWH JD

Use the arrow keys to select RWH JD. Press <Enter> and the following screen will appear. The feature displays the information of journaling drive(s).

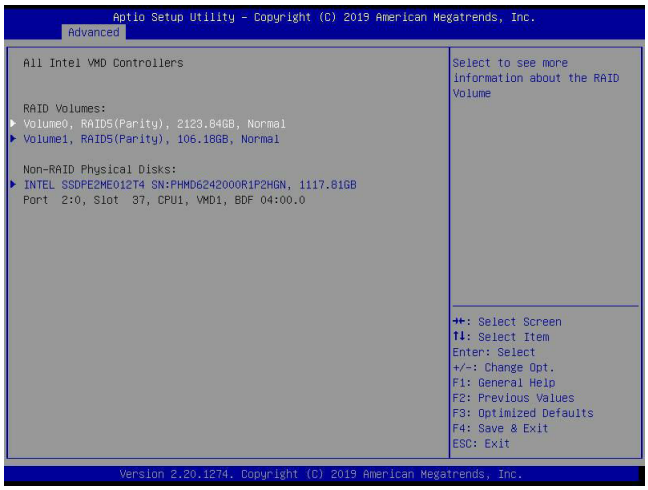


Step 4. Use the arrow keys and press <Enter> to select the desired journaling drive from the option list of RWH JD.

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



Your computer will return to the main screen of All Intel VMD Controllers as shown below.



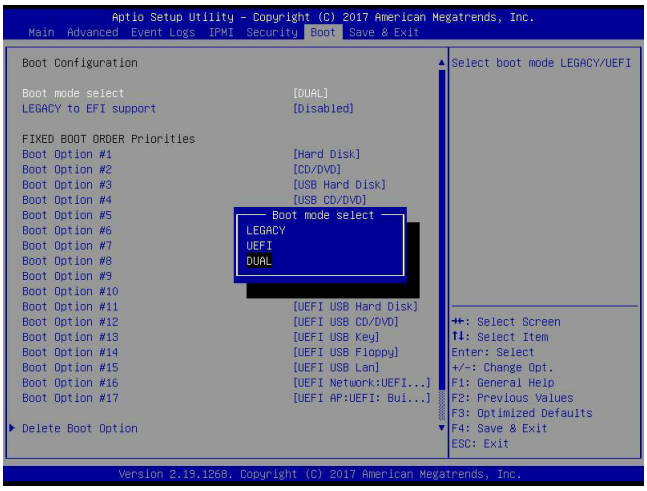
Appendix F

Secure Boot Settings

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

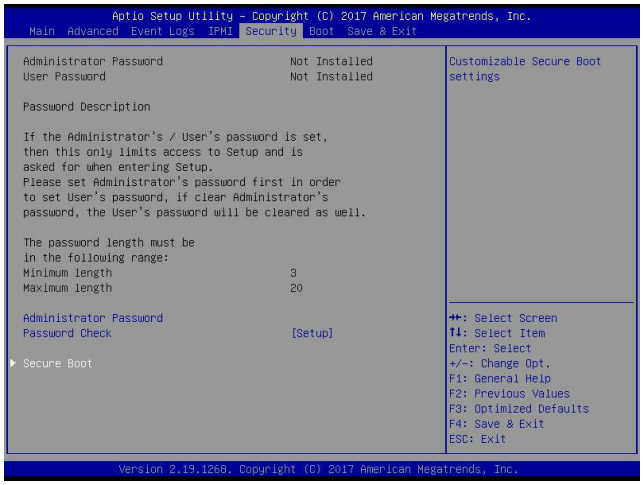
F.1 Boot mode select Feature

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

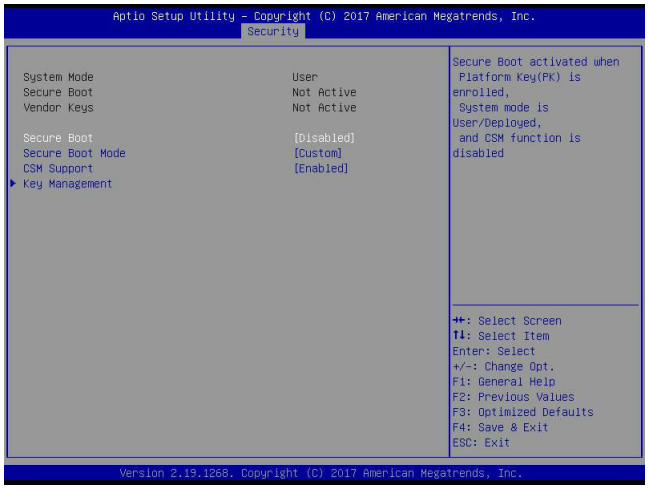


F.2 Secure Boot/ Secure Boot Mode/ CSM Support Features

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



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



Secure Boot

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

Secure Boot Mode

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

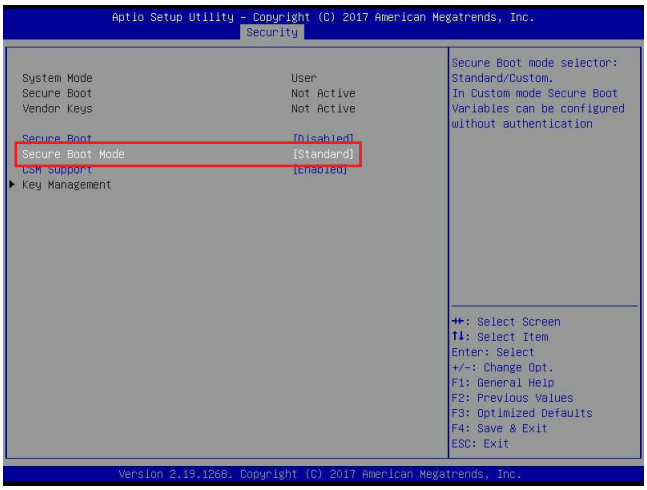
CSM Support

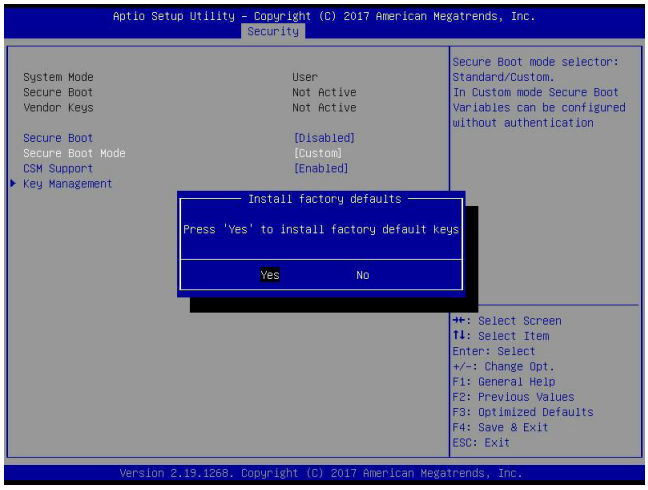
Select Enabled to support the legacy CSM, which provides compatibility support for traditional legacy BIOS for system boot. The options are Disabled and **Enabled**.

F.3 Secure Boot Settings

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

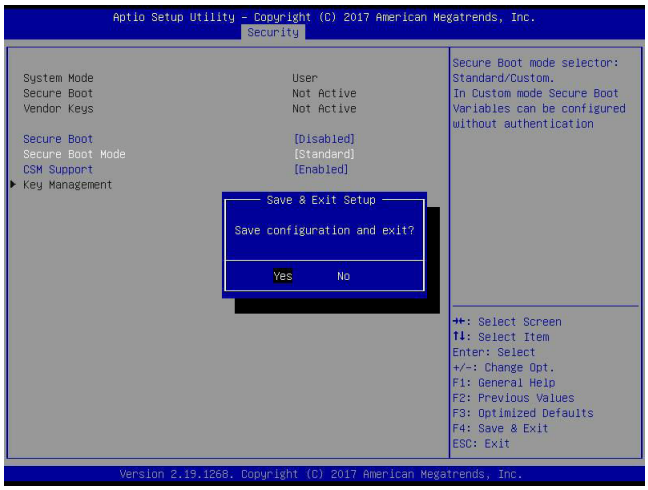
Step 1. Set Secure Boot Mode to Standard. Press Yes to install factory default keys as needed.



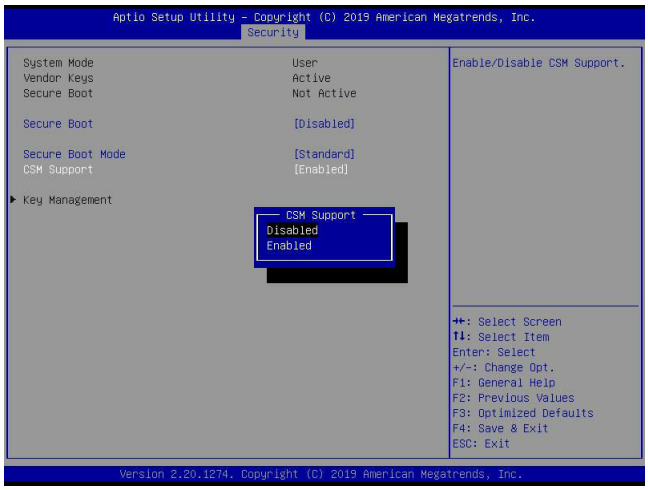


Note: The Key Management menu will become unavailable when Secure Boot Mode is set to Standard.

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

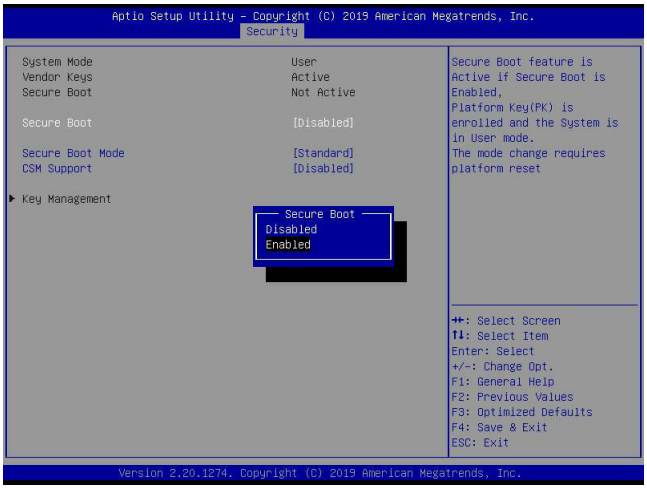


Step 3. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. Set CSM Support to Disabled.

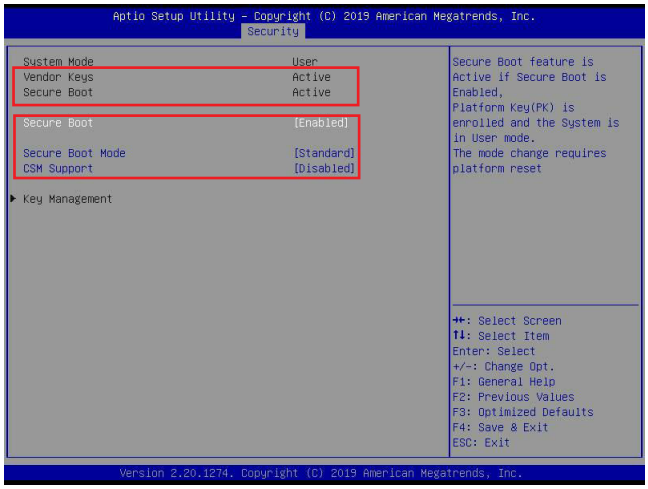


For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility.

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



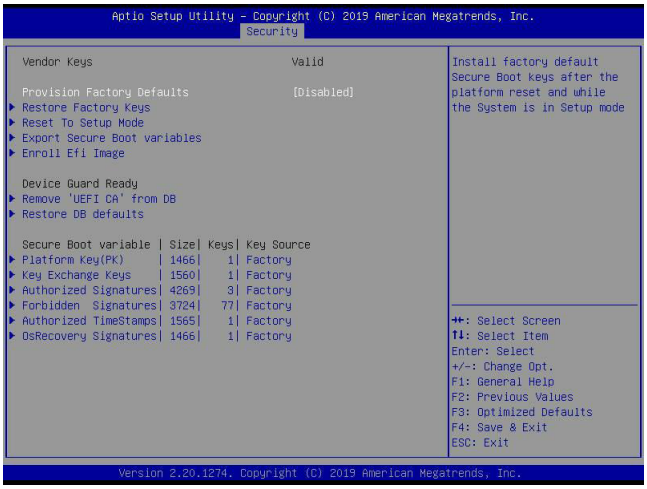
For the changes to take effect, press <F4> to save the settings and exit the BIOS Setup utility. Press <Del> during system boot to enter the BIOS Setup utility. Navigate to the Security tab and enter the Secure Boot menu. The following screen will appear.



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

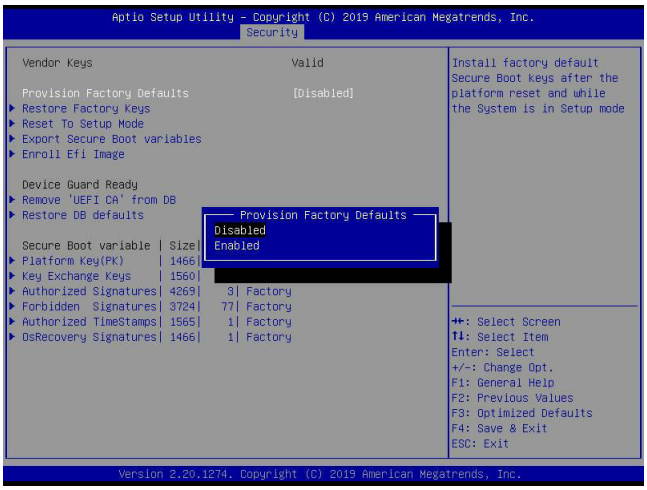
F.4 Key Management Settings

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



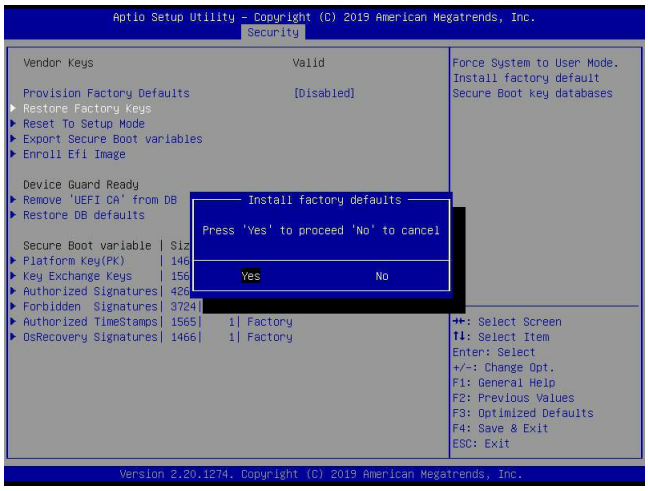
Provision Factory Defaults

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



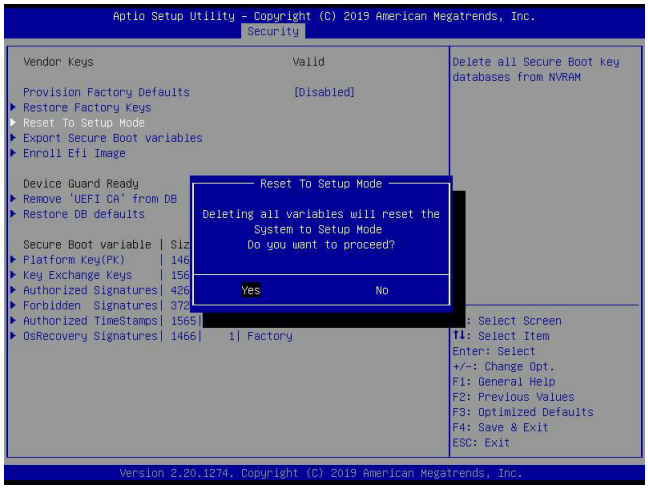
▶Restore Factory Keys

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



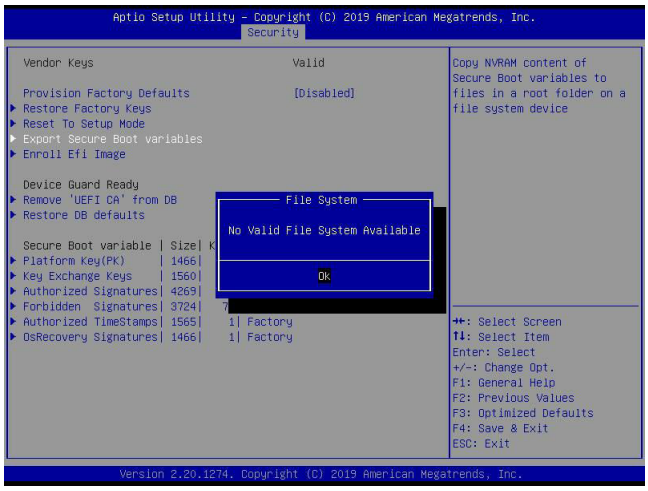
▶Reset To Setup Mode (available when the System Mode is in User mode)

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



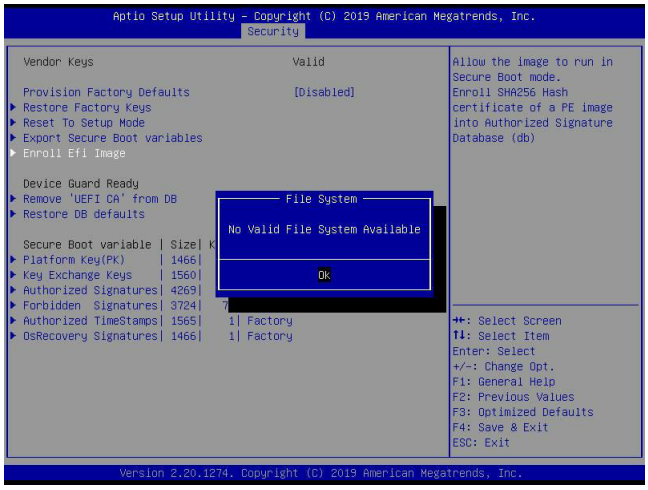
▶Export Secure Boot variables

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



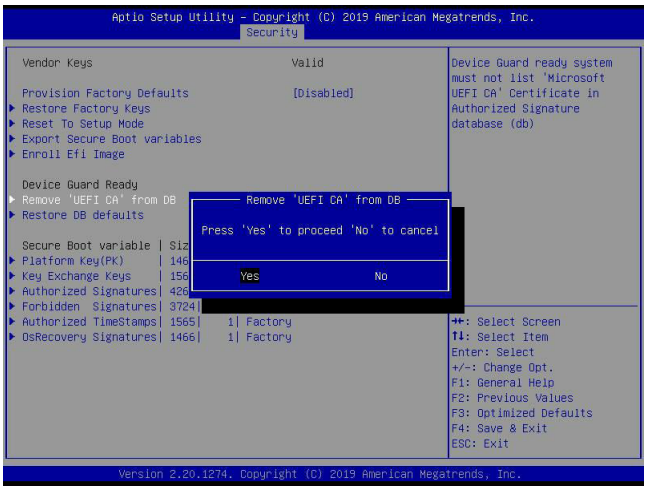
▶Enroll Efi Image

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



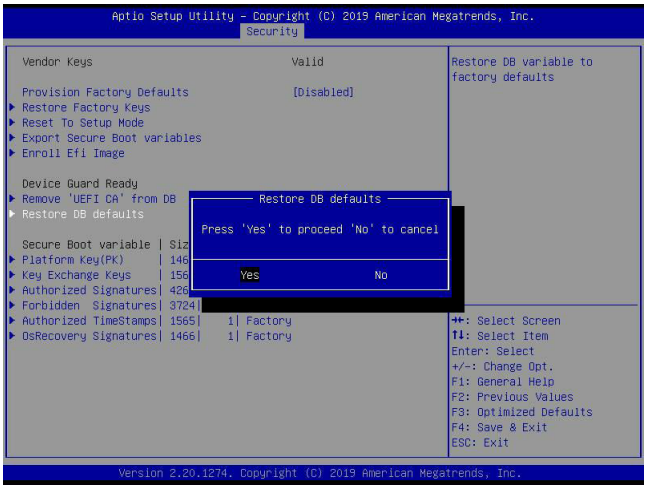
▶Remove 'UEFI CA' from DB (available when the system is not in Device Guard Ready)

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



▶Restore DB defaults

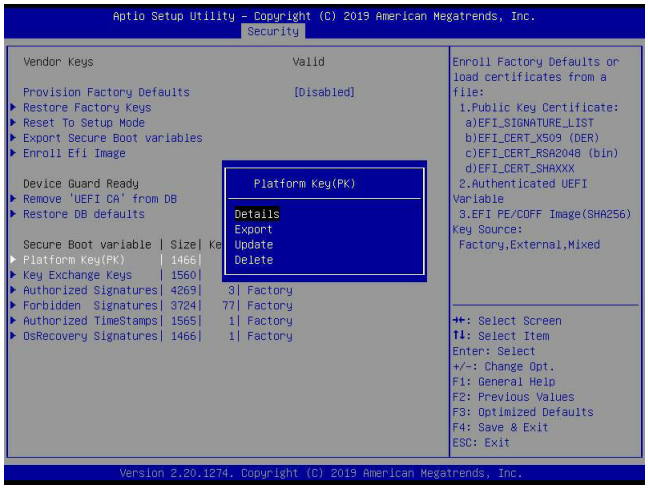
Select and press Yes to restore the DB variables to factory defaults. The options are **Yes** and No.



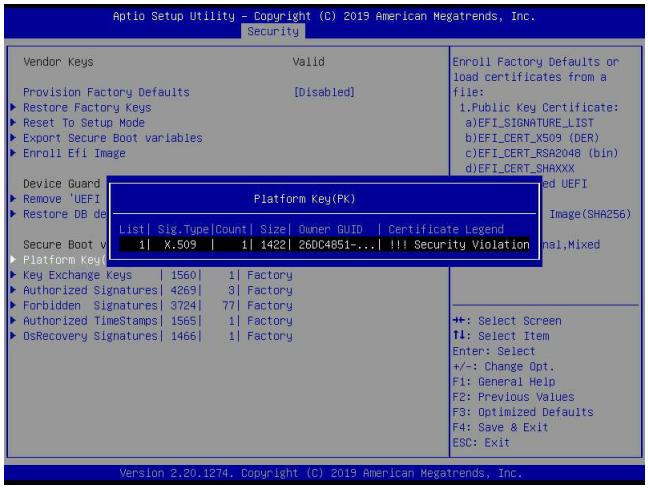
Refer to the following settings for keys and signatures related to secure boot.

▶Platform Key (PK)

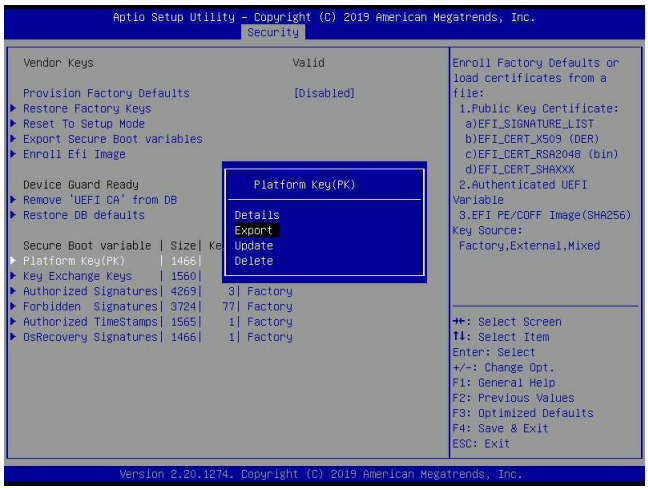
The Platform Key (PK), which is pre-installed in firmware during manufacturing, provides full control of the secure boot key hierarchy. The options are **Details**, Export, Update, and Delete. Select Details to display detailed information of PK. Select Export to save the current PKs to a FAT formatted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



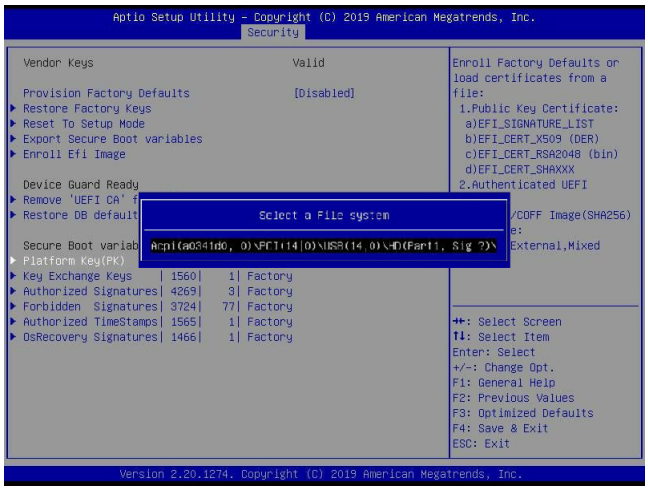
Details: Use the arrow keys to select Details and press <Enter>. It displays detailed information of PK as shown below.



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

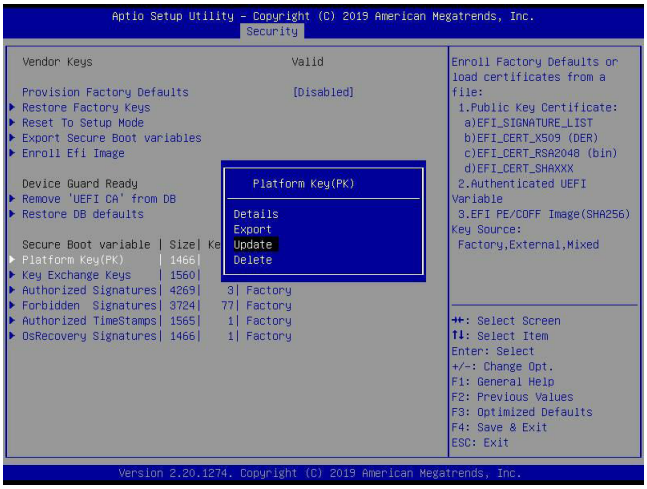


Press <Enter> and the following screen will appear.

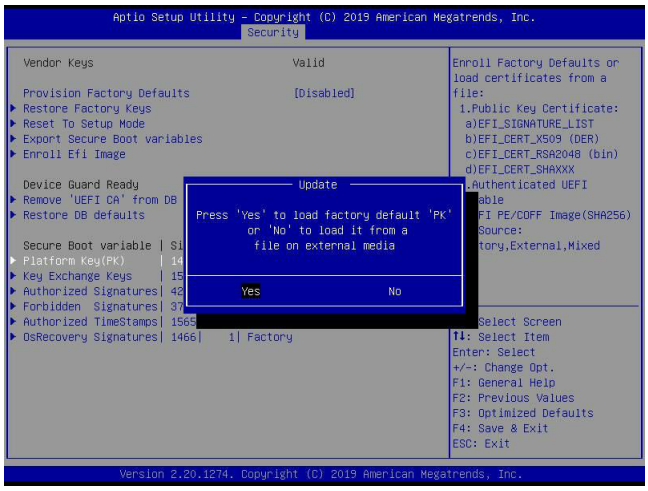


Note: Refer to the right panel of the screen for the file formats accepted.

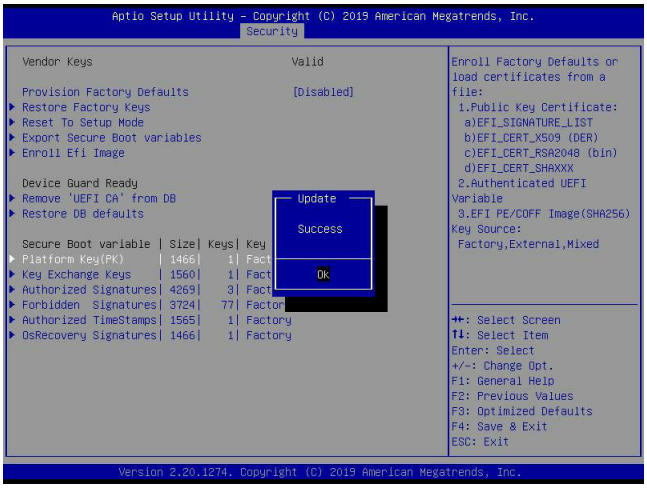
Update: Use the arrow keys to select Update. It is to load the factory defaults or load PKs from a file on the external device.



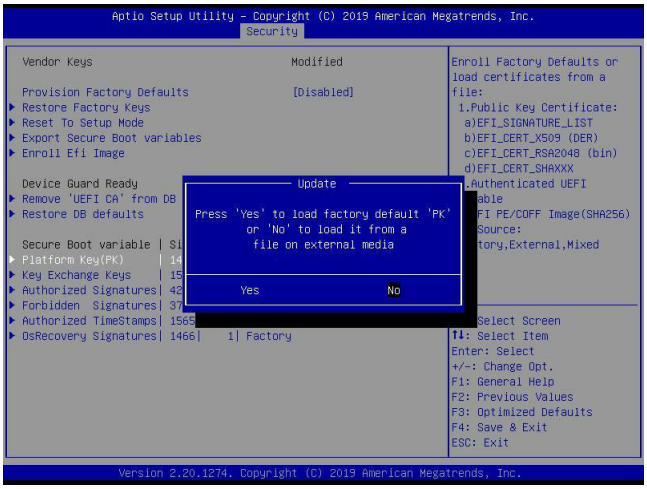
Press <Enter> and the following screen will appear.



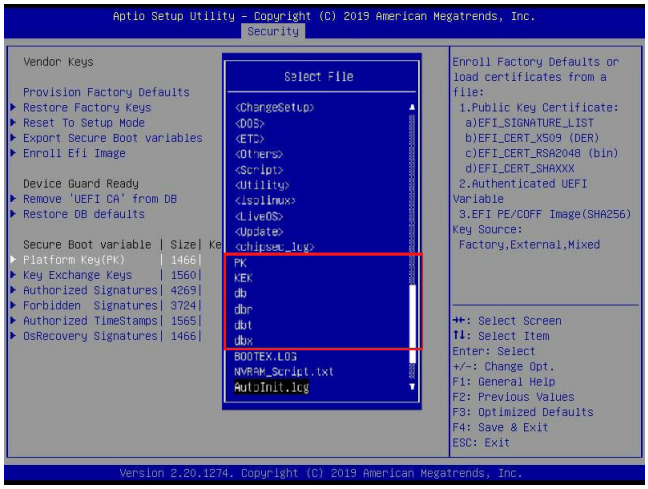
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.

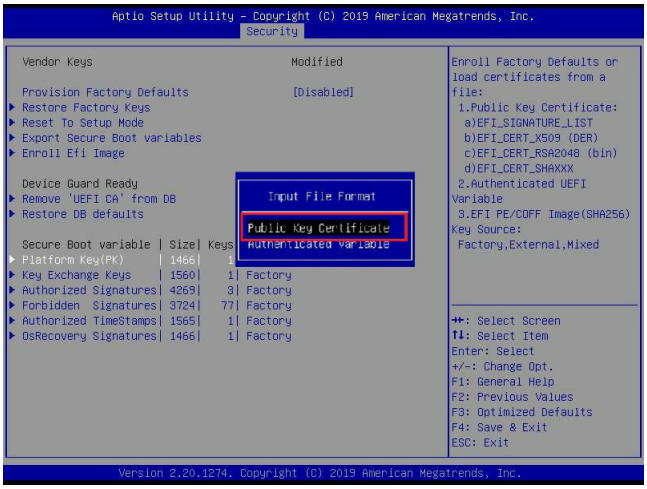


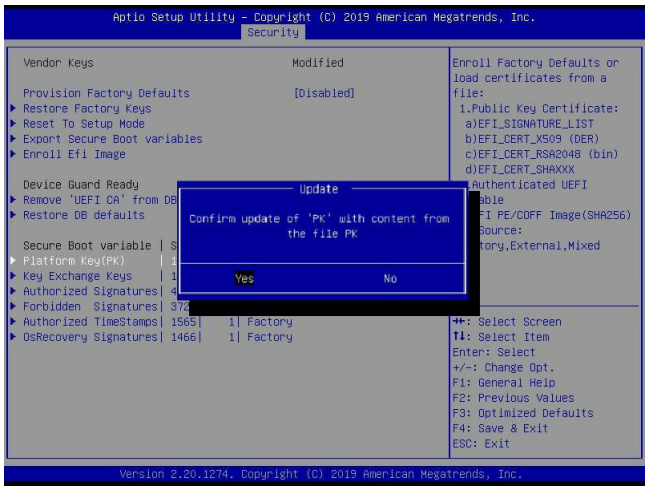
To load PKs from a file on the external device, navigate to No and press <Enter>.



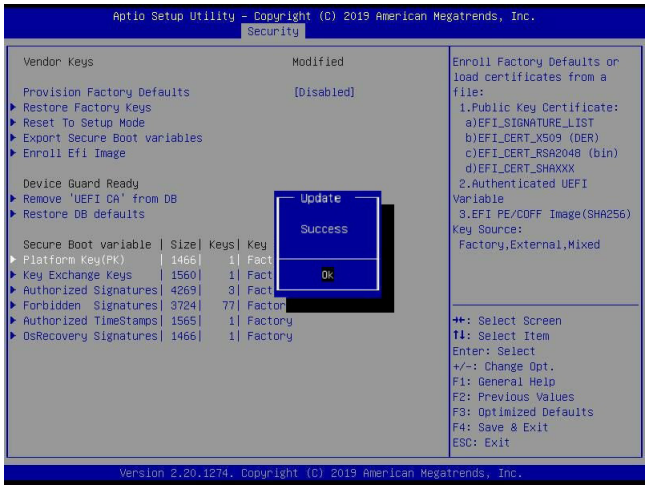
When the following screen appears, select the USB flash drive that contains the desired file.



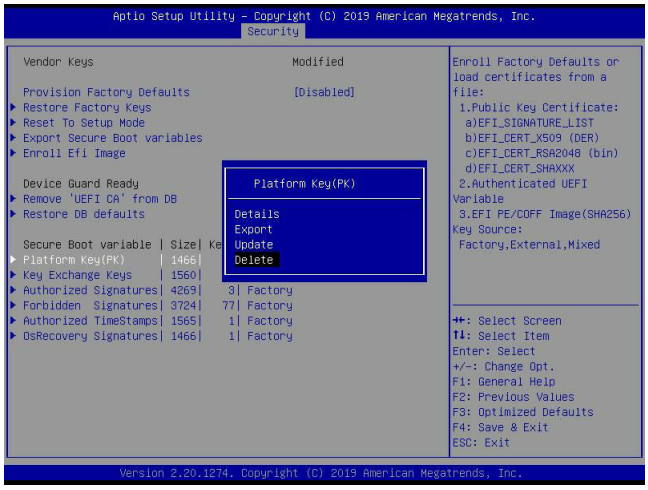


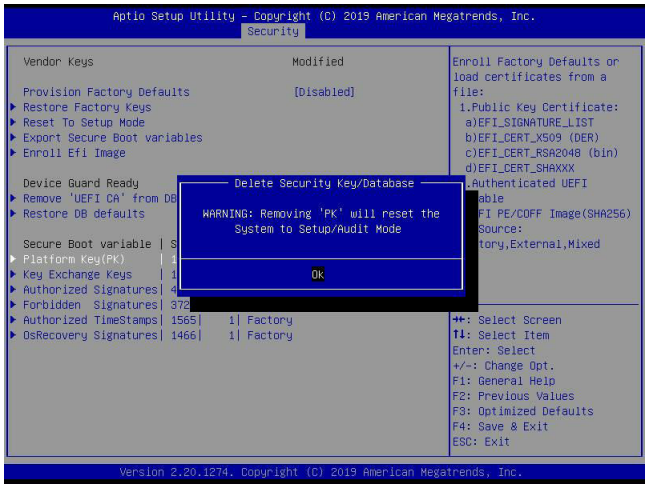


Press <Enter> and the following screen will appear.



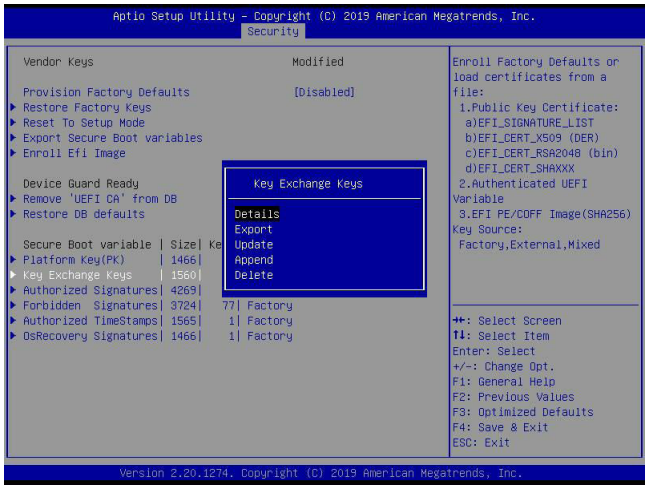
Delete: Use the arrow keys to select Delete and press <Enter> to clear the current PKs and reset the system to the Setup mode.



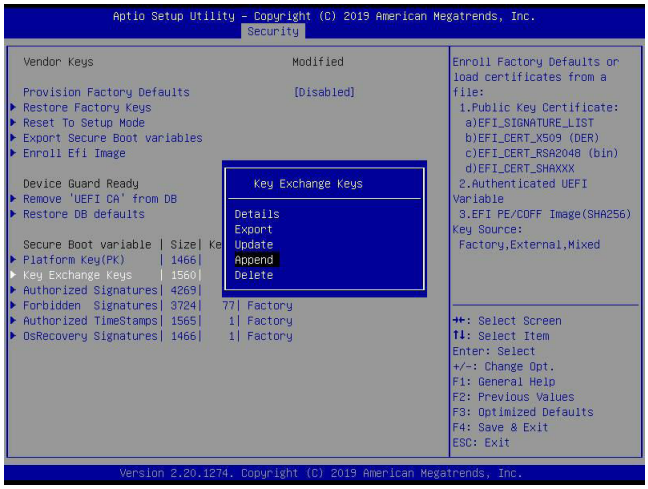


▶Key Exchange Key

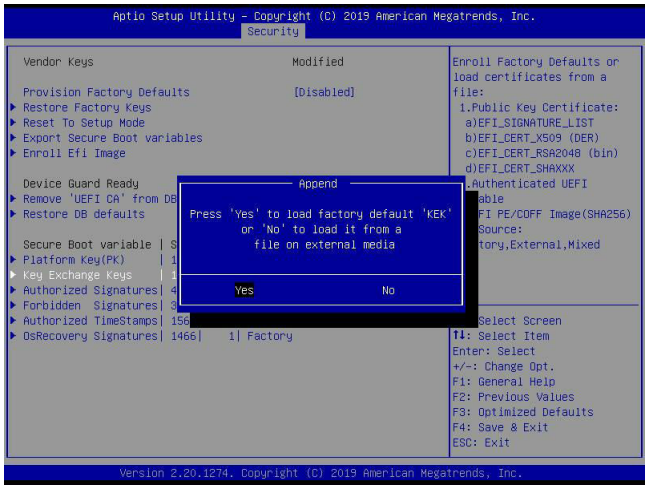
The Key Exchange Key (KEK), which is held by the operating system vendor, can be updated by the holder of the PK and be used by secure boot to protect access to signatures databases. The options are **Details**, Export, Update, Append, and Delete. Select Details to display detailed information of KEKs. Select Export to save the current KEKs to a FAT formatted USB flash drive. Select Update to load the factory defaults or load KEKs from a file on the external device. Select Append to load the factory defaults or load KEKs from a file on the external device. Select Delete to clear the current KEKs or to delete only one certificate from the key database. (Refer to page 189 for the Export process. Refer to pages 190, 191, 192, and 193 for the Update process.)



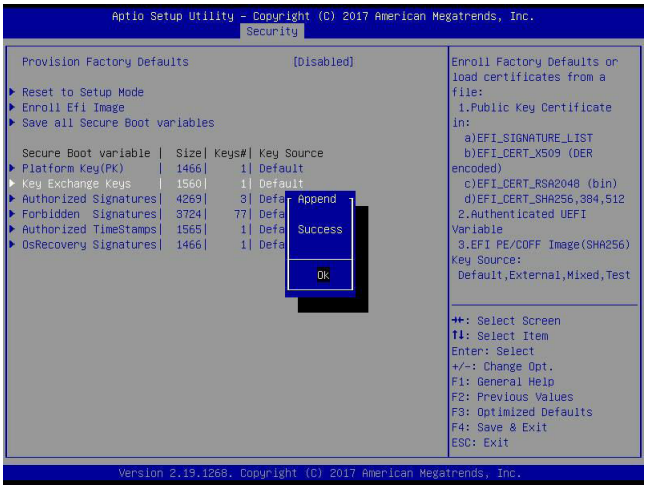
Append: Use the arrow keys to select Append.



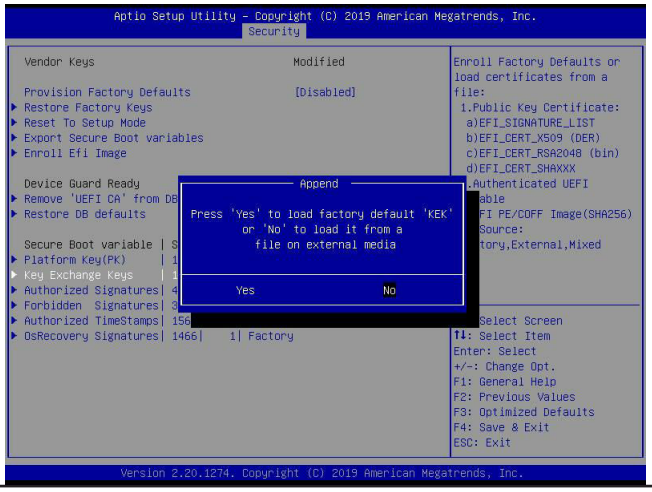
Press <Enter> and the following screen will appear.



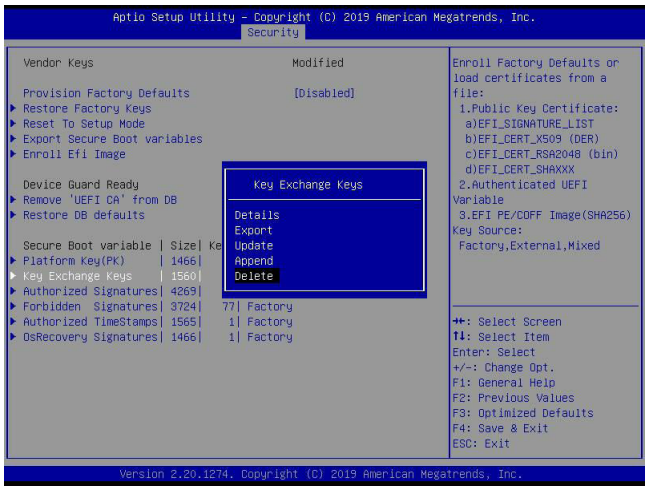
To load the factory defaults, navigate to Yes and press <Enter>. The following screen will appear.

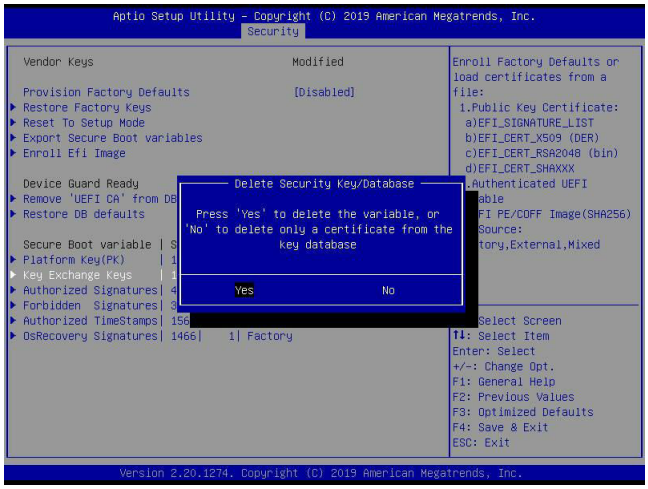


To load KEKs from a file on the external device, navigate to No and press <Enter>. Refer to pages 192 and 193 on how to load KEKs from a file on the external device.

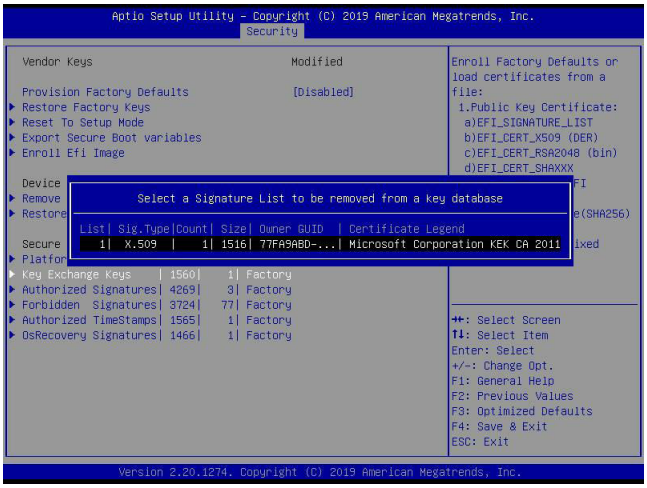


Delete: Use the arrow keys to select Delete and press <Enter>. Navigate to Yes and press <Enter> to clear the current KEKs.



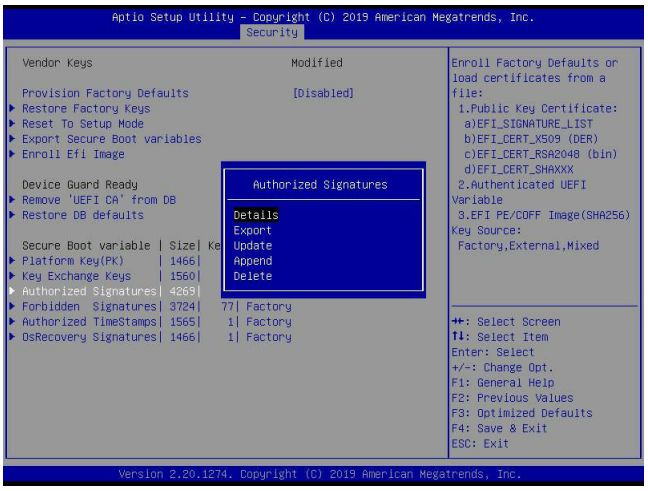


Navigate to No and press <Enter> to delete only one certificate from the key database.



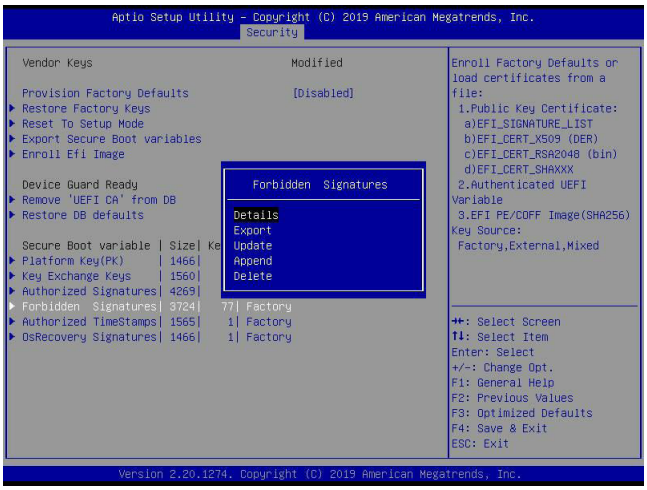
▶Authorized Signatures

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 189 for the Export process. Refer to pages 190, 191, 192, and 193 for the Update process. Refer to pages 194 and 195 for the Append process. Refer to page 196 for the Delete process.)



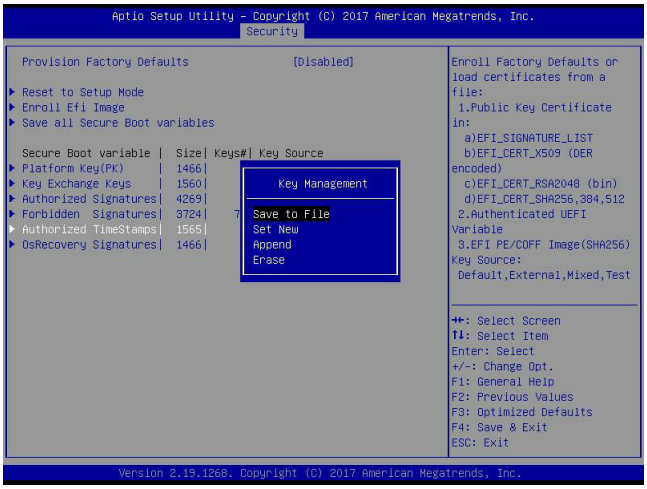
▶Forbidden Signatures

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 189 for the Export process. Refer to pages 190, 191, 192, and 193 for the Update process. Refer to pages 194 and 195 for the Append process. Refer to page 196 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 189 for the Export process. Refer to pages 190, 191, 192, and 193 for the Update process. Refer to pages 194 and 195 for the Append process. Refer to page 196 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 189 for the Export process. Refer to pages 190, 191, 192, and 193 for the Update process. Refer to pages 194 and 195 for the Append process. Refer to page 196 for the Delete process.)