

X14SBSC

USER'S MANUAL

Revision 1.0c (MNL-2696)

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. Note: For the most up-to-date version of this manual, see our website at https://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 or Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in industrial environment for Class A device or in residential environment for Class B device. 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 https://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 https://www.P65Warnings.ca.gov.



AVERTISSEMENT : Ce produit peut vous exposer à des agents chimiques, y compris le plomb, identifié par l'État de Californie comme pouvant causer le cancer, des malformations congénitales ou d'autres troubles de la reproduction. Pour de plus amples informations, prière de consulter https://www.P65Warnings.ca.gov.

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

Manual Revision 1.0c

Release Date: June 02, 2026

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

Copyright © 2026 by Super Micro Computer, Inc.
All rights reserved.
Published in the United States of America

Preface

About This Manual

This manual is written for professional system integrators and PC technicians. It provides information for the installation and use of the X14SBSC motherboard. Installation and maintenance should be performed by certified service technicians only.

Notes

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

- Supermicro product manuals: https://www.supermicro.com/support/manuals
- Product drivers and utilities: https://www.supermicro.com/wdl
- Product safety info: https://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 on our website: https://www.supermicro.com/about/policies/disclaimer.cfm?url=/wdl/utility/Lot9_Secure_Data_Deletion_Utility
- Frequently Asked Questions: https://www.supermicro.com/FAQ/index.php
- If you still have questions after referring to our FAQs, contact our support team. Region-specific Technical Support email addresses can be found at: "Contacting Supermicro" on page 13
- If you have any feedback on Supermicro product manuals, contact our writing team at: Techwriterteam@supermicro.com

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

Conventions Used in the Manual

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



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



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



Warning! Indicates hazardous moving parts may be encountered while handling a fan or components near a fan.

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

Note: Additional information given to differentiate various models or to provide information for proper motherboard setup.

Contents

Contacting Supermicro ***13***
Chapter 1: Introduction ***14***
1.1 Quick Reference 15
Motherboard Layout 15
Quick Reference Table 16
Motherboard Features 18
Motherboard Block Diagram 21
1.2 Platform Overview 22
1.3 Special Features 23
Recovery from AC Power Loss 23
1.4 System Health Monitoring 24
Onboard Voltage Monitors 24
Fan Status Monitor with Firmware Control 24
Environmental Temperature Control 24
1.5 ACPI Features 25
Chapter 2: Component Installation ***26***
2.1 Static-Sensitive Devices 28
Precautions 28
Unpacking 28
2.2 Motherboard Installation 29
Tools Needed 29
Installing the Motherboard 29
2.3 Processor and Heatsink Installation 31
LGA 4710 Socket E2 Processors 31
Processor Top View 31
Overview of the Processor Carrier 32
Processor Carriers 32
Overview of the Processor Socket 33
Overview of the Processor Heatsink Module 33
Installing the Processor 35
Assembling the Processor Heatsink Module 37

Preparing the Processor Socket for Installation 40
Preparing to Install the PHM into the Processor Socket 41
Installing the Processor Heatsink Module 44
Removing the Processor Heatsink Module 46
2.4 Memory Support and Installation 52
Memory Support 52
General Guidelines for Optimizing Memory Performance 56
DIMM Installation 57
DIMM Removal 59
2.5 Battery Removal and Installation 61
Battery Removal 61
Proper Battery Disposal 61
Battery Installation 61
2.6 Connections, Jumpers, and LEDs 62
Power Supply and Power Connections 62
Power Supply 62
Power Connectors 62
Node Fan Board Power Connector 62
Onboard NVMe Power Connector 62
Node Power Connector from System 63
Headers and Connections 63
Fan Board Control Header 63
Inlet Sensor Header 64
M.2 M-Key PCIe 4.0 x2 Slots 64
MCIO PCIe 5.0 x8 Connectors 64
NC-SI Connection 64
Node Control Connector to System 65
Node Fan Board Control Connector 65
Node PCIe 5.0 Connectors to System 66
Node SAS 3.0 Connectors to System 68
NVMe I²C Header 70
8-Pin Onboard Standby Fan Header 70
SAS 3.0 Connections (SlimSAS) 71
TPM/Port 80 Header 71

VROC RAID Key Header 71
I/O Ports 72
LAN Ports 72
Unit Identifier Button 73
USB Ports 74
Jumper Settings 74
CMOS Clear 75
TPM Select 76
LED Indicators 76
BMC Heartbeat LED 76
Expander SAS35X48 Heartbeat LED 76
Front Panel Power LED 77
M.2 LEDs 77
SAS 3808N Heartbeat LED 77
Unit ID (UID) LED 77
Chapter 3: Troubleshooting ***79***
3.1 Troubleshooting Procedures 80
Before Power On 80
No Power 80
No Video 80
System Boot Failure 80
Memory Errors 81
Losing the System's Setup Configuration 81
If the System Becomes Unstable 81
3.2 Technical Support Procedures 83
3.3 Motherboard Battery 84
3.4 Where to Get Replacement Components 85
3.5 Returning Merchandise for Service 86
3.6 Feedback 87
Chapter 4: UEFI BIOS ***88***
4.1 Introduction 89
Updating BIOS 89
Starting the Setup Utility 89
4.2 Main Setup 91

4.3 Advanced Setup Configurations 93
Boot Feature Menu 93
CPU Configuration Menu 95
Advanced Power Management Configuration Menu 98
CPU P State Control Menu 99
Hardware PM State Control Menu 101
CPU C State Control Menu 101
Package C State Control Menu 102
CPU1 Core Disable Bitmap Menu 102
Chipset Configuration Menu 103
Uncore Configuration Menu 103
Memory Configuration Menu 105
Memory Topology Menu 105
Memory Map Menu 106
Memory RAS Configuration Menu 106
Security Configuration Menu 107
IIO Configuration Menu 113
CPU1 Configuration Menu 114
Intel VT for Directed I/O (VT-d) Menu 116
PCIe Leaky Bucket Configuration Menu 116
Trusted Computing Menu 117
ACPI Settings Menu 119
Super IO Configuration Menu 119
Serial Port 1 Configuration Menu 120
Serial Port 2 Configuration Menu 120
Serial Port Console Redirection Menu 121
Network Stack Configuration Menu 124
MAC:(MAC address)-IPv4 Network Configuration Menu 125
MAC:(MAC address)-IPv6 Network Configuration Menu 125
PCIe/PCI/PnP Configuration Menu 126
HTTP Boot Configuration Menu 128
Supermicro KMS Server Configuration Menu 129
Super-Guardians Configuration Menu 131
System Diagnostics Configuration Menu 134

Intel(R) Ethernet Controller Menu 134
System Diagnostics Configuration Menu 135
TLS Authenticate Configuration Menu 135
BROADCOM <SAS 3808N> Configuration Utility 136
Main Menu 136
Configuration Management 136
Create Virtual Drive 136
Create Profile Based Virtual Drive 138
Generic RAID 0 138
Generic RAID 1 138
Clear Configuration 139
Controller Management 140
Advanced Controller Management 140
Clear Controller Events 140
Save Controller Events 141
Save TTY Log 141
Enable Drive Security 141
Disable Drive Security 141
Disable Drive Security 142
Manage SAS Storage Link Speed 142
Manage PCIe Storage Interface 143
Manage MegaRAID Advanced Software Options 145
Schedule Consistency Check 145
Set Factory Defaults 146
Manage Personality Mode 146
Manage Controller Profiles 146
Manage Phy State 147
Advanced Controller Properties 147
Patrol Read 149
Spare 150
Task Rates 150
External Key Management 151
Spin Down Drives At Shutdown 151
Virtual Drive Management 152

Drive Management 152
Drive 152
Advanced... 153
Hardware Components 154
Help 154
PROPERTIES 154
View Server Profile 155
Controller Management 155
Advanced Controller Management 156
Clear Controller Events 156
Save Controller Events 156
Save TTY Log 156
Enable Drive Security 156
Disable Drive Security 157
Disable Drive Security 157
Manage SAS Storage Link Speed 157
Manage PCIe Storage Interface 158
Manage MegaRAID Advanced Software Options 160
Schedule Consistency Check 161
Set Factory Defaults 161
Manage Personality Mode 162
Manage Controller Profiles 162
Manage Phy State 162
Advanced Controller Properties 163
Patrol Read 164
Spare 165
Task Rates 166
External Key Management 167
Spin Down Drives At Shutdown 167
Virtual Drive Management 167
Drive Management 167
Drive 168
Advanced... 168
Hardware Components 169

Drive Management 170
Virtual Drive Management 170
ACTIONS 170
Configuration Management 170
Create Virtual Drive 170
Create Profile Based Virtual Drive 172
Generic RAID 0 172
Generic RAID 1 172
Clear Configuration 173
Set Factory Defaults 173
Update Firmware 174
BACKGROUND OPERATIONS 174
MegaRAID ADVANCED SOFTWARE OPTIONS 174
Manage MegaRAID Advanced Software Options 174
Driver Health Menu 175
4.4 Event Logs 176
4.5 BMC 178
System Event Log Menu 178
BMC Network Configuration Menu 179
4.6 Security 182
Supermicro Security Erase Configuration Menu 183
HDD Security Configuration Menu 184
Secure Boot Menu 185
TCG Storage Security Configuration Menu 188
4.7 Boot 189
4.8 Save & Exit 191
Appendix A: Software ***193***
Microsoft Windows OS Installation 193
Installing the OS 193
Driver Installation 195
BMC 197
BMC ADMIN User Password 197
Appendix B: Standardized Warning Statements ***198***
Battery Handling 198

Connection to Earth 200
Product Disposal 201

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) Sales-USA@supermicro.com (Sales Inquiries) Government_Sales-USA@supermicro.com (Gov. Sales Inquiries) Support@supermicro.com (Technical Support) RMA@Supermicro.com (RMA Support) Webmaster@supermicro.com (Webmaster)
Website:	https://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_Europe@supermicro.com (Sales Inquiries) Support_Europe@supermicro.com (Technical Support) RMA_Europe@supermicro.com (RMA Support)
Website:	https://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:	Sales-Asia@supermicro.com.tw (Sales Inquiries) Support@supermicro.com.tw (Technical Support) RMA@supermicro.com.tw (RMA Support)
Website:	https://www.supermicro.com.tw

Chapter 1:

Introduction

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

1.1 Quick Reference **15**
Motherboard Layout 15
Quick Reference Table 16
Motherboard Features 18
Motherboard Block Diagram 21
1.2 Platform Overview **22**
1.3 Special Features **23**
Recovery from AC Power Loss 23
1.4 System Health Monitoring **24**
Onboard Voltage Monitors 24
Fan Status Monitor with Firmware Control 24
Environmental Temperature Control 24
1.5 ACPI Features **25**

1.1 Quick Reference

For details on the X14SBSC motherboard layout, features, and other quick reference information, refer to the content below.

Motherboard Layout

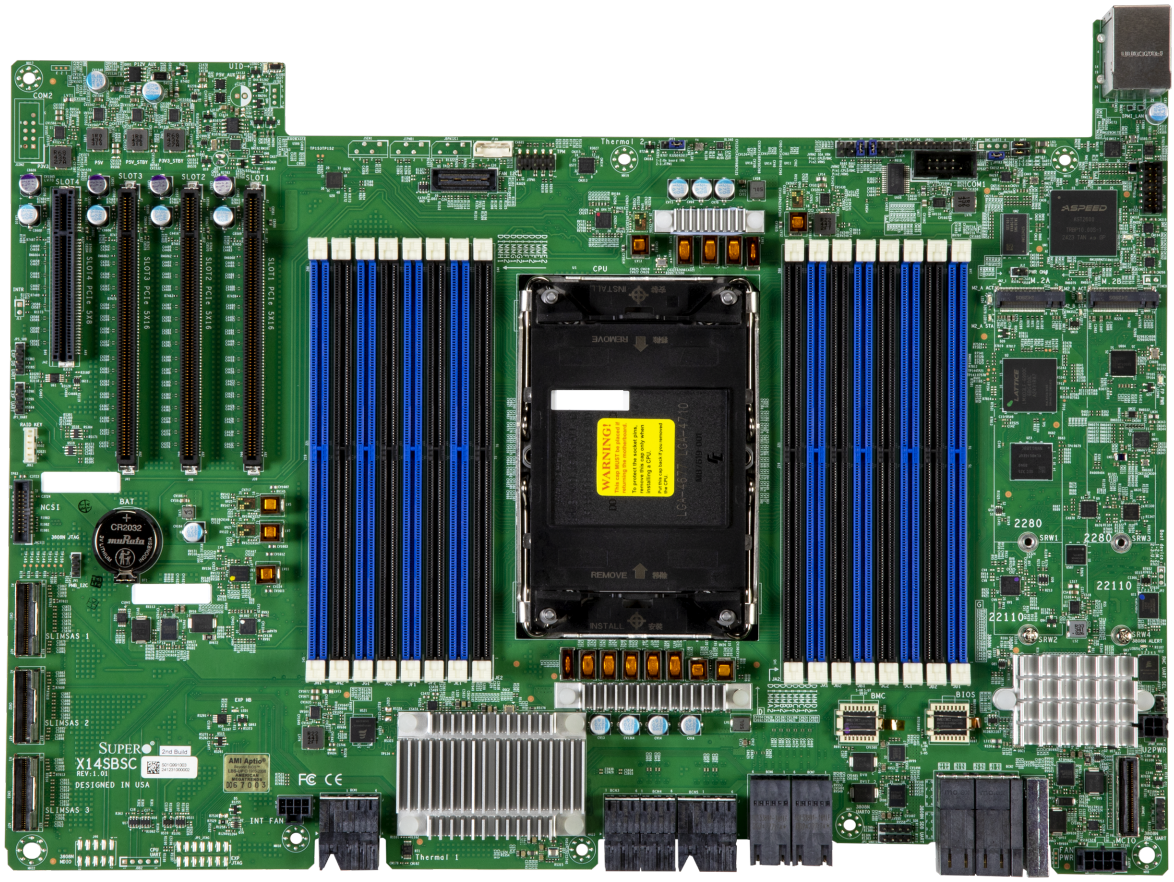


Figure 1-1. X14SBSC Motherboard Image

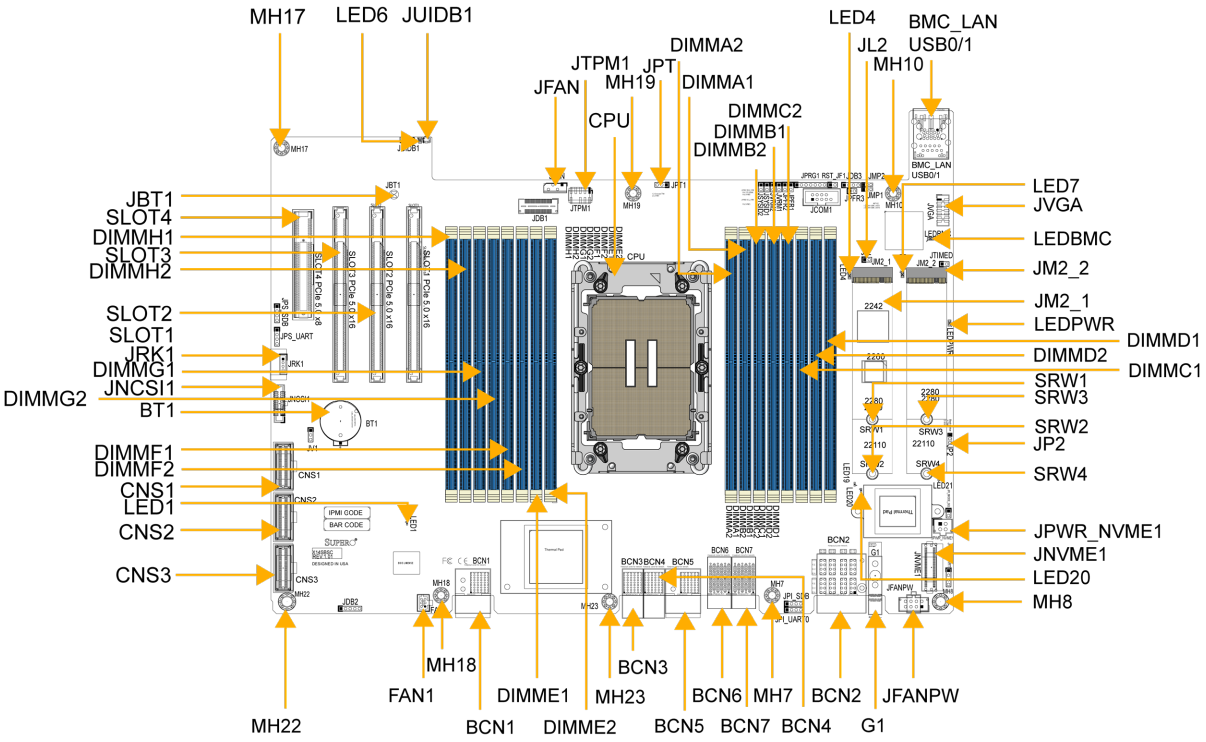


Figure 1-2. X14SBSC Motherboard Layout

Notes:

- For detailed information on jumpers, connectors, and LED indicators, see "Component Installation" on page 26.
- "■" indicates the location of pin 1.
- "MH" indicates the location of a mounting hole.
- Components not documented are for internal testing purposes only.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. To avoid possible explosion, do not install the onboard battery upside down.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JPT1	TPM Select	Pins 1–2: Onboard TPM

LED	Description	Status
LED1	Expander SAS35X48 Heartbeat LED	Blinking Green: Device Working
LED4	M.2 LED	Blinking: Device Working
LED6	Unit Identifier LED	Solid Blue: Unit Identified
LED7	M.2 LED	Blinking Green: Device Working
LED20	SAS 3808N Heartbeat LED	Blinking Green: Device Working
LEDBMC	BMC Heartbeat LED	Blinking Green: Device Working
LEDPWR	Front Panel Power LED	Solid Green: Power On

Connector	Description
BMC_LAN	Dedicated BMC LAN Port
BT1	Onboard Battery
BCN1	Node Control Connector to System
BCN2	Node Power Connector from System
BCN3, BCN4, BCN5	Node SAS 3.0 Connectors to System
BCN6, BCN7	Node PCIe 5.0 Connectors to System
CNS1	SLIMSAS1 Connector for SAS 3.0
CNS2	SLIMSAS2 Connector for SAS 3.0
CNS3	SLIMSAS3 Connector for SAS 3.0
FAN1	8-pin Onboard Standby FAN Header
JFAN	Node Fan Board Control Connector
JFANPW	Node FAN Power Connector
JM2_1, JM2_2	M.2 M-Key PCIe 4.0 x2 Connectors (supports 22110 form factor)
JNCSI1	NC-SI Port Selection
JNVME1	MCIO PCIe 5.0 x8 Connector
JPWR_NVME1	4-pin NVME Power Connector
JRK1	VROC RAID Key Header
JTPM1	Trusted Platform Module (TPM)/Port 80 Connector

Connector	Description
JUIDB1	Unit Identifier Button
JVGA	VGA Header
SLOT1	PCIe 5.0 x16 Slot
SLOT2	PCIe 5.0 x16 Slot
SLOT3	PCIe 5.0 x16 Slot
SLOT4	PCIe 5.0 x8 Slot
USB0/1	USB 3.2 Gen 1 Ports

Note: Jumpers, connectors, switches, and LED indicators that are not described in these tables are for manufacturing testing purposes only, and are not covered in this manual.

Motherboard Features

Motherboard Features
Processor
• Supports the Intel® Xeon® 6700/6500-series processors with P-cores or Intel® Xeon® 6700-series processor with E-cores, and a thermal design power (TDP) of up to 350 W
Memory
• Up to 512 GB MRDIMM with speeds up to 8000 MT/s (1DPC) or 4 TB of 3DS RDIMM with speeds up to 6400 MT/s (1DPC) or 6000 MT/s (2DPC) in 16 DIMM slots **Note:** Intel® Xeon® 6700/6500-series processors with P-cores is required to support MRDIMM.
DIMM Size
• DDR5 RDIMM:16 GB, 24 GB, 32 GB,48 GB, 64 GB, 96 GB, 128 GB • DDR5 3DS RDIMM: 256 GB • DDR5 MRDIMM (P-core only): 32 GB, 64 GB **Note:** Memory speed support depends on the processor used in the system.

Motherboard Features
Expansion Slots
• Three PCIe 5.0 x16 slots (SLOT1, SLOT2, SLOT3) • One PCIe 5.0 x8 slot (SLOT1) • One MCIO PCIe 5.0 x8 connector • Three SLIMSAS connectors for SAS 3.0 • Two M.2 M-Key PCIe 4.0 x2 connectors in the 22110/2280 form factors
Network Controllers
• One dedicated BMC LAN
Baseboard Management Controller (BMC)
• ASpeed AST2600 BMC
Graphics
• Graphics controller via ASpeed AST2600 BMC
I/O Devices
• One VGA header • One TPM header • One NC-SI header
Peripheral Devices
• Two rear-accessible USB 3.2 Gen 1 headers
BIOS
• 512 Mb AMI BIOS® SPI Flash BIOS • ACPI 6.5 or later, Plug and Play (PnP) SPI dual/quad speed support, riser card auto detection support, SMBIOS 3.7.0 or later
Power Management
• ACPI power management • Power button override mechanism • Power-on mode for AC power recovery • Power supply monitoring • RoHS

Motherboard Features
System Health Monitoring
• Onboard voltage monitoring for 3.3 V, +5 V, +12 V, +3.3 VStby, +5 VStby, Vcore, CPU temperature, system temperature, peripheral temperature, memory temperature, GPU temperature, and NVMe temperature • CPU thermal trip support • Platform Environment Control Interface (PECI)/TSI
Fan Control
• One 8-pin fan header • Fan speed control
System Management
• Onboard TPM9672: TCG2.0, FIPS 140-2 Level 2 certified • Platform Environment Control Interface (PECI) 3.0 support • Watchdog, NMI • Chassis intrusion header and detection • Intel Active Management Technology
LED Indicators
• CPU/system overheat LED • Power/suspend-state indicator LED • Fan failed LED • UID/remote UID • HDD activity LED • LAN activity LED
Dimensions
10.9" x 14.8" (276.86 mm x 375.92 mm) (W x L), proprietary FF

Motherboard Block Diagram

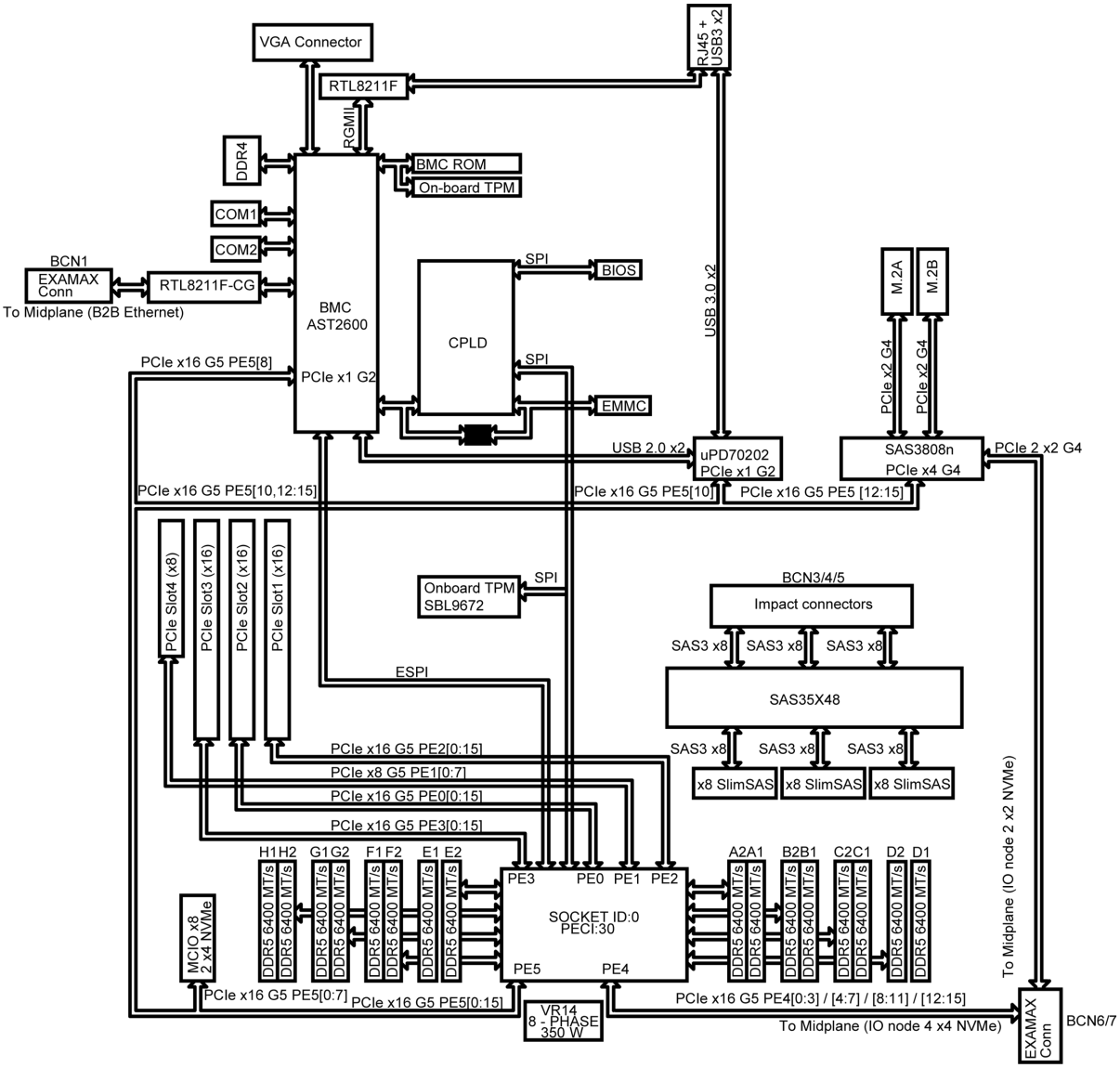


Figure 1-3. Motherboard Block Diagram

1.2 Platform Overview

Built upon the capability of the Intel® Xeon® 6700/6500-series processors with P-cores or Intel® Xeon® 6700-series processor with E-cores, the X14SBSC motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users.

The X14SBSC motherboard dramatically increases system performance for a multitude of server applications and supports the following features:

The X14SBSC motherboard dramatically increases system performance for a multitude of server applications and supports the following features:

- DDR5 287-pin memory support
- Support of SMBus speeds of up to 400 KHz for BMC connectivity
- Improved I/O capabilities to high-storage-capacity configurations
- SPI Enhancements
- BMC supports remote management, virtualization, and the security package for enterprise platforms
- PCIe 5.0, CXL 2.0
- Onboard TPM9672: TCG2.0, FIPS 140-2 Level 2, Intel TXT, and Microsoft Windows certification
- Intel Deep Learning Boost
- Intel Software Guard Extensions (SGX), Intel Trusted Domain Extensions (TDX)
- Intel QuickAssist Technology (QAT), Intel Dynamic Load Balancer (DLB) 2.5, Intel Data Streaming Accelerator, Intel In-Memory Analytics Accelerator (IAA) 2.0

1.3 Special Features

Recovery from AC Power Loss

The Basic I/O System (BIOS) provides a setting that determines how the system will respond when AC power is lost and then restored to the system. You can choose for the system to remain powered off (in which case you must press the power switch to turn it back on), or for it to automatically return to the power-on state. See Advanced Setup Configurations under "UEFI BIOS" on page 88 for this setting. The default setting is **Last State**.

1.4 System Health Monitoring

Onboard Voltage Monitors

An onboard voltage monitor will continuously scan the voltages of the onboard chipset, memory, processor, and battery. Once a voltage becomes unstable, a warning is given or an error message is sent to the screen. You can adjust the voltage thresholds to define the sensitivity of the voltage monitor. Real time voltage levels are 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 processor and chassis fans are controlled via IPMI.

Environmental Temperature Control

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

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

1.5 ACPI Features

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

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play, 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 Windows Server 2025.

Chapter 2:

Component Installation

This chapter provides instructions on installing and replacing main system components for the X14SBSC motherboard. To prevent compatibility issues, only use components that match the specifications and/or part numbers given.

Installation or replacement of most components require that power first be removed from the system. Follow the procedures given in each section.

2.1 Static-Sensitive Devices **28**
Precautions 28
Unpacking 28
2.2 Motherboard Installation **29**
Tools Needed 29
Installing the Motherboard 29
2.3 Processor and Heatsink Installation **31**
LGA 4710 Socket E2 Processors 31
Overview of the Processor Carrier 32
Overview of the Processor Socket 33
Overview of the Processor Heatsink Module 33
Installing the Processor 35
Assembling the Processor Heatsink Module 37
Preparing the Processor Socket for Installation 40
Preparing to Install the PHM into the Processor Socket 41
Installing the Processor Heatsink Module 44
Removing the Processor Heatsink Module 46
2.4 Memory Support and Installation **52**
Memory Support 52
General Guidelines for Optimizing Memory Performance 56
DIMM Installation 57
DIMM Removal 59
2.5 Battery Removal and Installation **61**
Battery Removal 61

Proper Battery Disposal 61
Battery Installation 61
2.6 Connections, Jumpers, and LEDs 62
Power Supply and Power Connections 62
Headers and Connections 63
I/O Ports 72
Jumper Settings 74
LED Indicators 76

2.1 Static-Sensitive Devices

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

Precautions

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

Unpacking

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

2.2 Motherboard Installation

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

Tools Needed

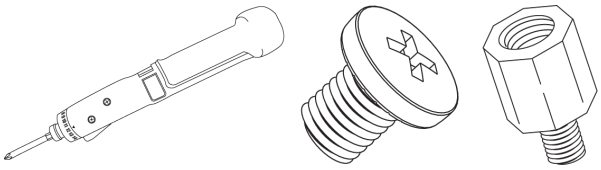


Figure 2-1. Torque Driver (1), Phillips Screws (8), Standoffs (8, only if needed)

Notes:

- To avoid damaging the motherboard and its components, do not use a force greater than 8 lbf-in on each mounting screw during motherboard installation.
- Some components are very close to the mounting holes. Take precautionary measures to avoid damaging these components when installing the motherboard to the chassis.

Installing the Motherboard

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

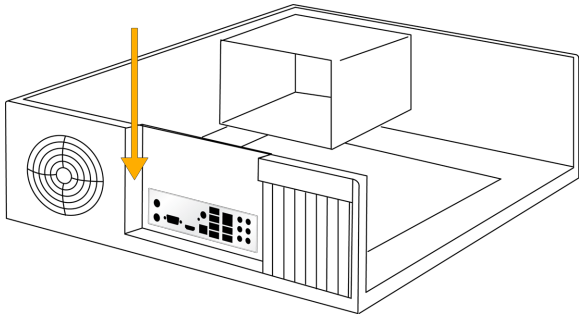


Figure 2-2. Installing the I/O Shield

Note: Images displayed are for illustration purposes only. The components installed in your system may or may not look exactly the same as the graphics shown in the manual.

2. Locate the mounting holes on the motherboard. See Motherboard Installation for the location.

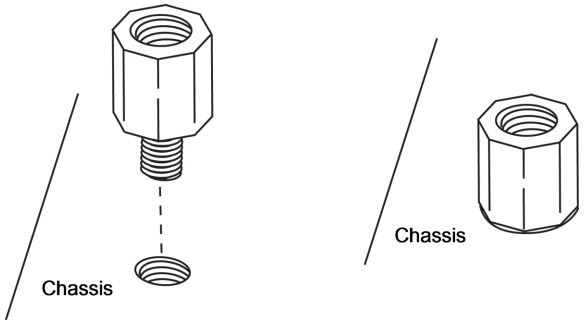


Figure 2-3. Locating the Mounting Holes

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

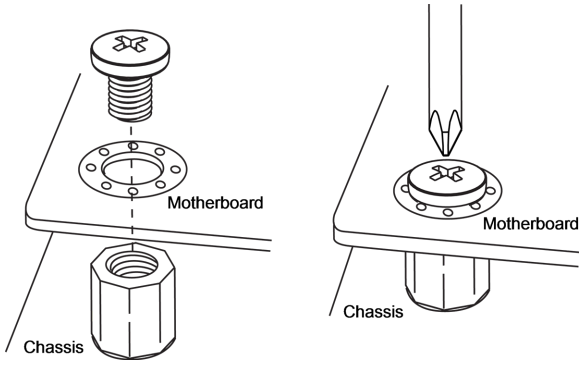


Figure 2-4. Aligning the Mounting Holes

4. Install standoffs in the chassis as needed.
5. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
6. Insert pan head #6 screws into the mounting holes on the motherboard and the matching mounting holes on the chassis.
7. Make sure that the motherboard is securely placed in the chassis.

2.3 Processor and Heatsink Installation

This section provides procedures to install the processor(s) and heatsink(s).

Notes:

- Take industry standard precautions to avoid ESD damage. For details, see "Static-Sensitive Devices" on page 28.
- Before starting, make sure that the plastic socket cap is in place and none of the socket pins are bent. If any damage is noted, contact your retailer.
- Do not connect the system power cord before the processor and heatsink installation is complete.
- When handling the processor, avoid touching or placing direct pressure on the LGA lands (gold contacts). Improper installation or socket misalignment can cause serious damage to the processor or processor socket.
- Install the processor in the socket and the motherboard into the chassis before installing the heatsink.
- When buying a processor separately, use only a Supermicro certified heatsink.
- Refer to the Supermicro website for the most recent processor support.
- When installing the heatsink, ensure a torque driver set to the correct force is used for each screw.
- Thermal grease is pre-applied on a new heatsink. No additional thermal grease is needed.

LGA 4710 Socket E2 Processors

Processor Top View

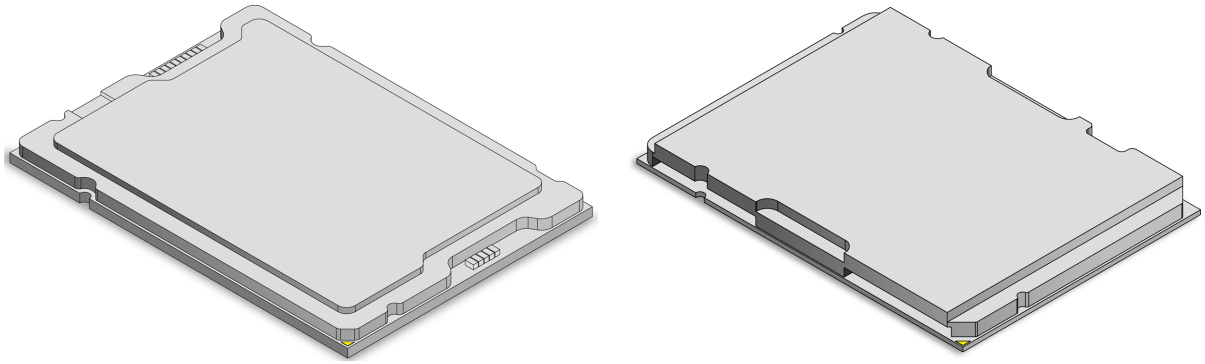


Figure 2-5. Processor (SP XCC left, SP HCC/LCC right)

Note: The motherboard supports three processor SKUs: SP XCC, SP HCC, and SP LCC. Each SKU supports a specific carrier; the SP XCC processor supports Carrier E2A while SP HCC and SP LCC support Carrier E2B. Make sure the processors of the same SKU are on the motherboard.

Overview of the Processor Carrier

The motherboard supports two types of processors and their associated processor carrier.

Processor Carriers

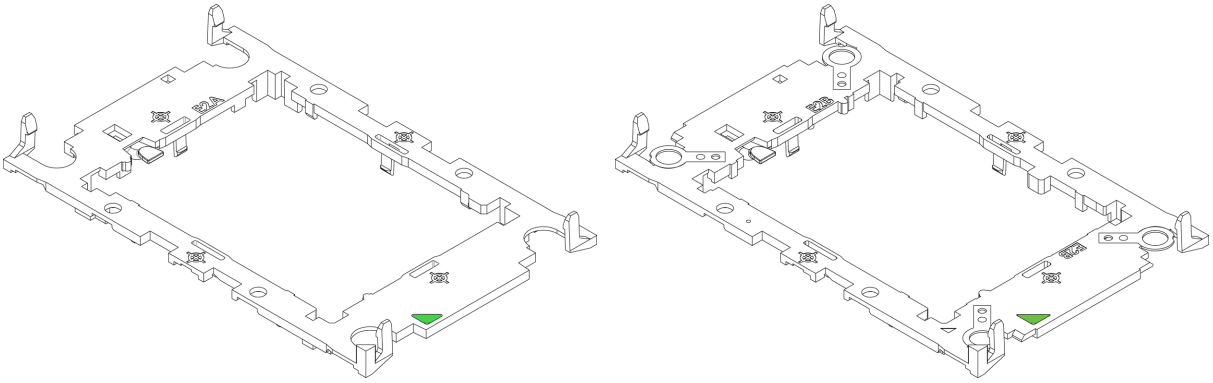


Figure 2-6. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)

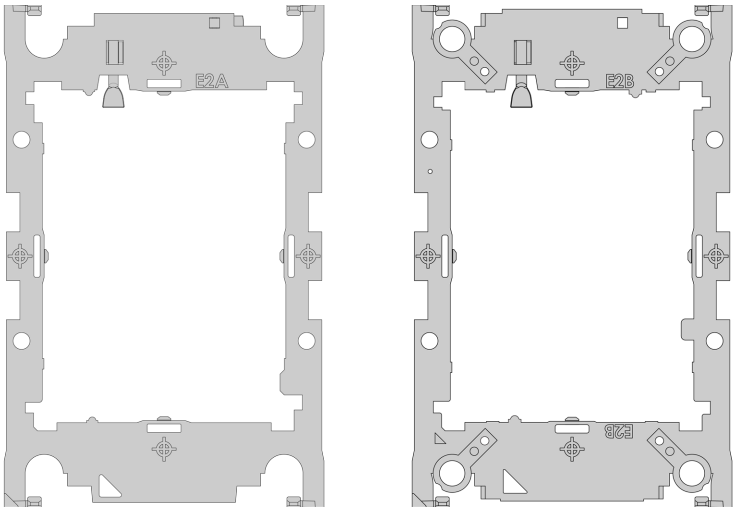


Figure 2-7. Carrier Top View (SP XCC E2A left, SP HCC/LCC E2B right)

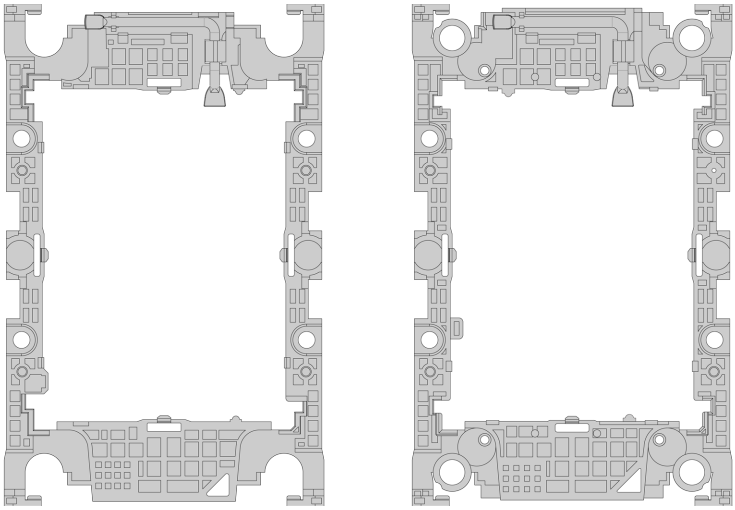


Figure 2-8. Carrier Bottom View (SP XCC E2A left, SP HCC/LCC E2B right)

Overview of the Processor Socket

The processor socket is protected by a plastic protective cover.

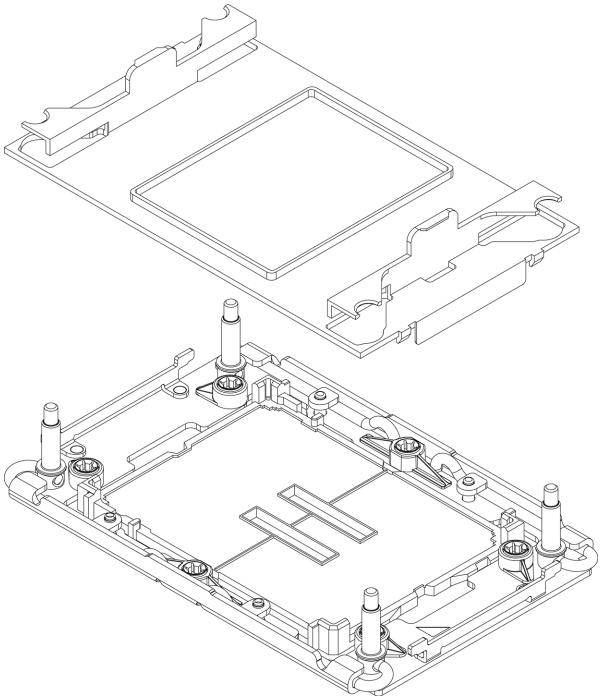


Figure 2-9. Plastic Protective Cover and Processor Socket

Overview of the Processor Heatsink Module

The Processor Heatsink Module (PHM) contains a heatsink, a processor carrier, and the processor.

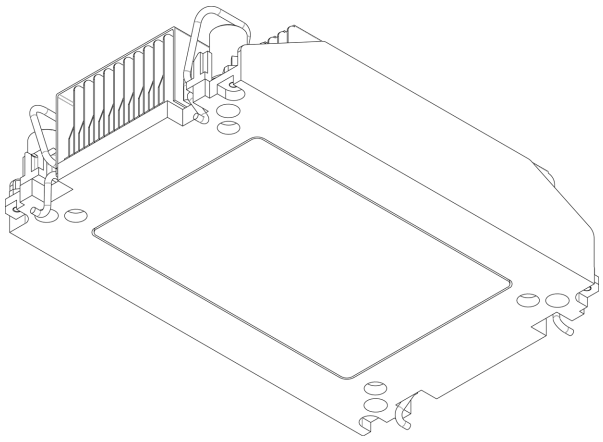


Figure 2-10. Heatsink (1U)

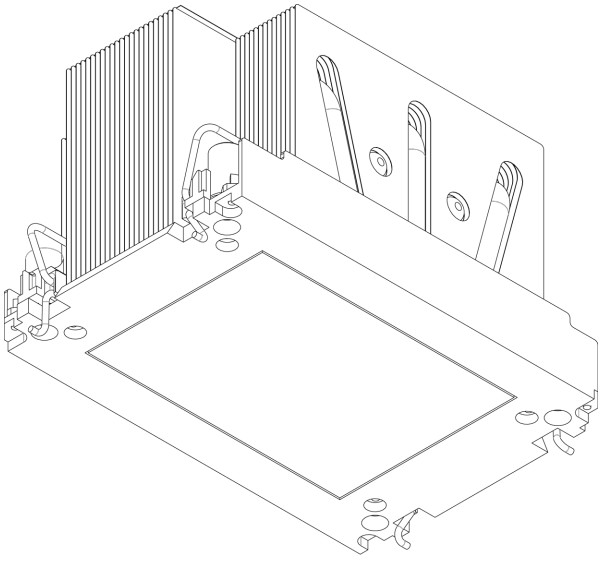


Figure 2-11. Heatsink (2U)

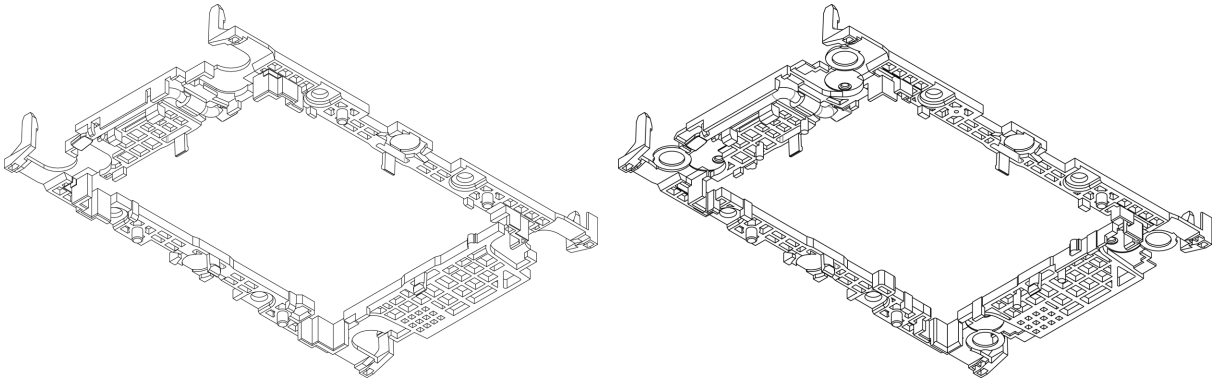


Figure 2-12. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)

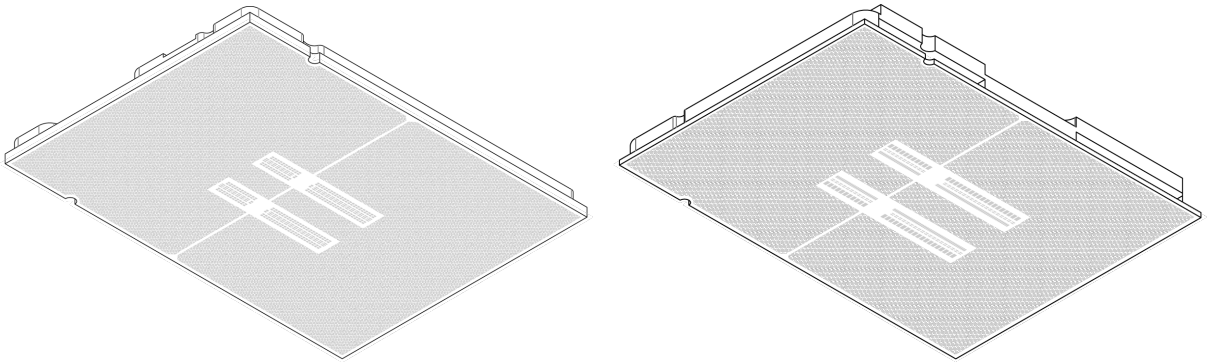


Figure 2-13. Processor (SP XCC E2A left, SP HCC/LCC E2B right)

Installing the Processor

To install the processor, follow the steps below:

1. Before installation, make sure the lever on the processor carrier is pressed down as shown below.

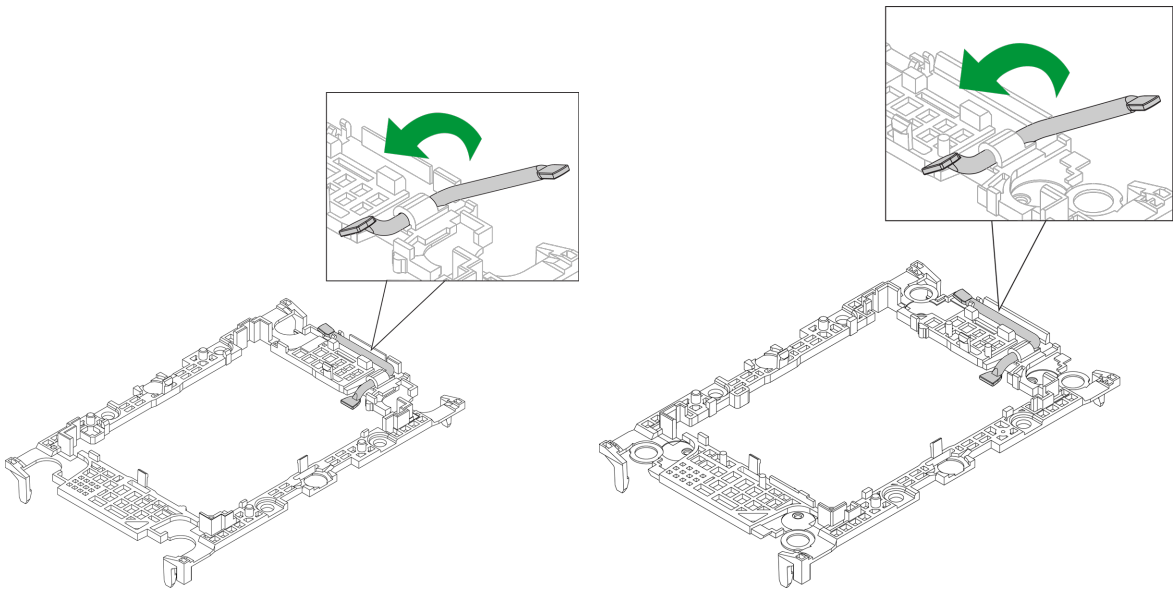


Figure 2-14. Carrier Lever (SP XCC left, SP HCC/LCC right)

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

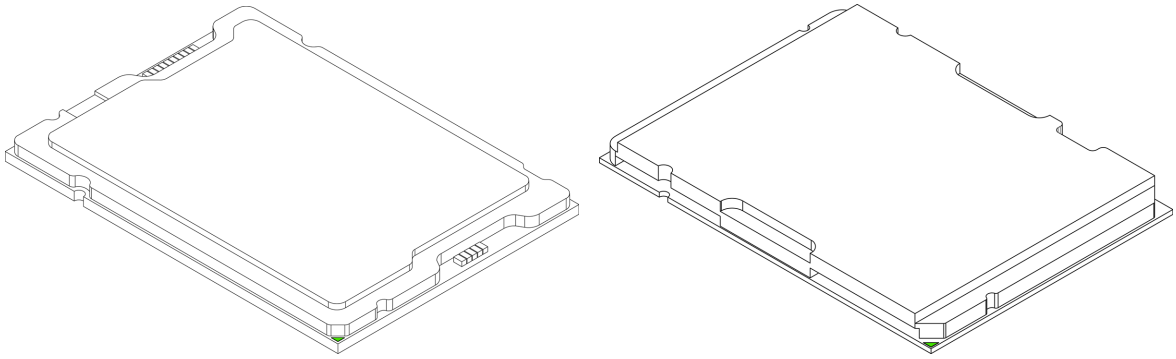


Figure 2-15. Processor (SP XCC E2A left, SP HCC/LCC E2B right)

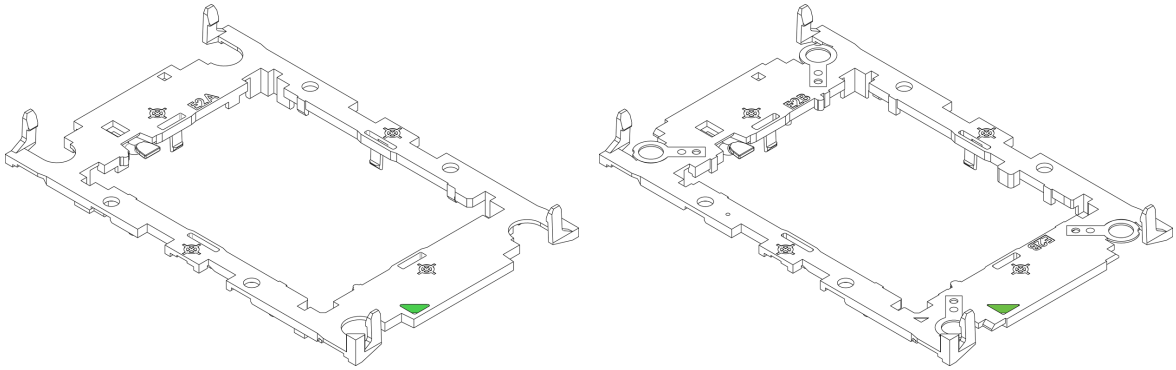


Figure 2-16. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)

3. Use the triangles as a guide to carefully align and place one end of the processor into the latch marked A, and place the other end of the processor into the latch marked B as shown below.

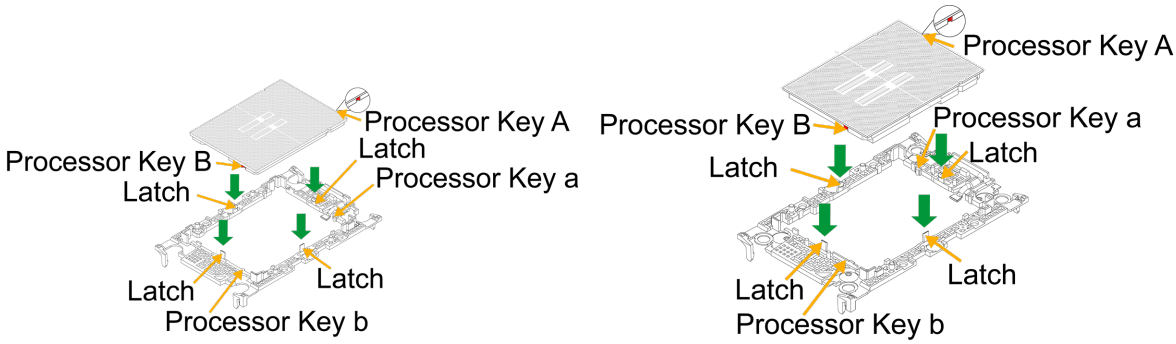


Figure 2-17. Keys and Latches Locations (SP XCC E2A left, SP HCC/LCC E2B right)

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

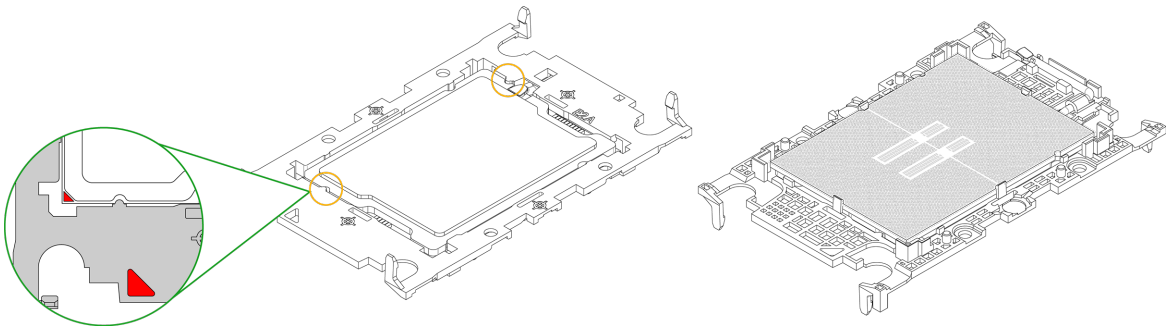


Figure 2-18. SP XCC E2A Keys and Latches

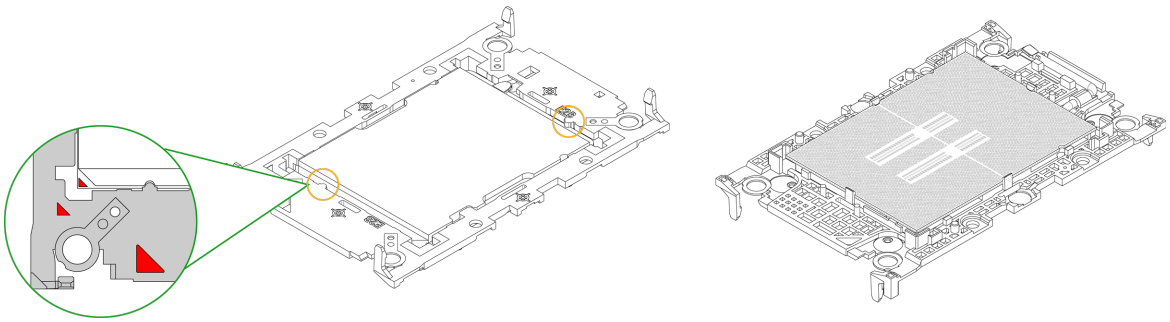


Figure 2-19. SP HCC/LCC E2B Keys and Latches Together

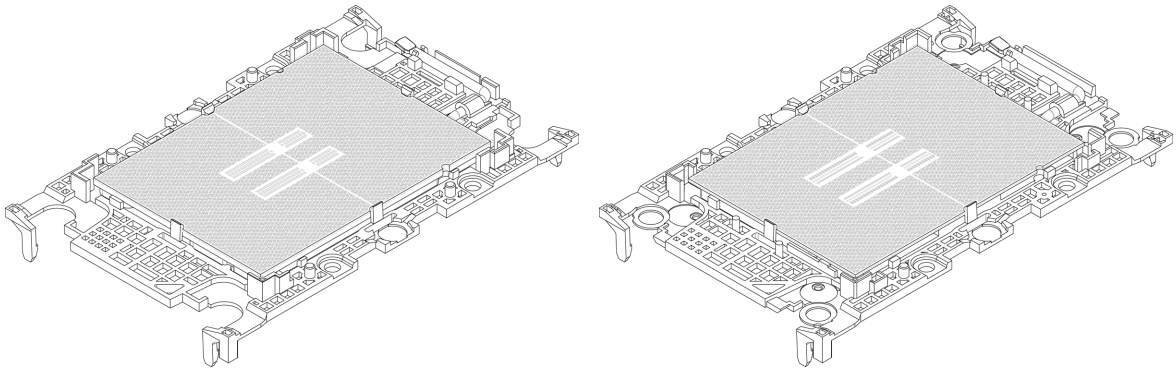


Figure 2-20. Carrier Assembly Completed (SP XCC E2A left, SP HCC/LCC E2B right)

Assembling the Processor Heatsink Module

After installing the processor into the carrier, mount it onto the heatsink to create the processor heatsink module (PHM):

1. Note the label on top of the heatsink, which marks the airflow direction. Turn the heatsink over and orient the heatsink so the airflow arrow is pointing towards the triangle on the processor.

2. If this is a new heatsink, the thermal grease has been pre-applied. Otherwise, apply the proper amount of thermal grease.
3. Hold the processor carrier so the processor's gold contacts are facing up, then align the holes of the processor carrier with the holes on the heatsink. Press the processor carrier down until it snaps into place. The plastic clips of the processor carrier will lock at the four corners.

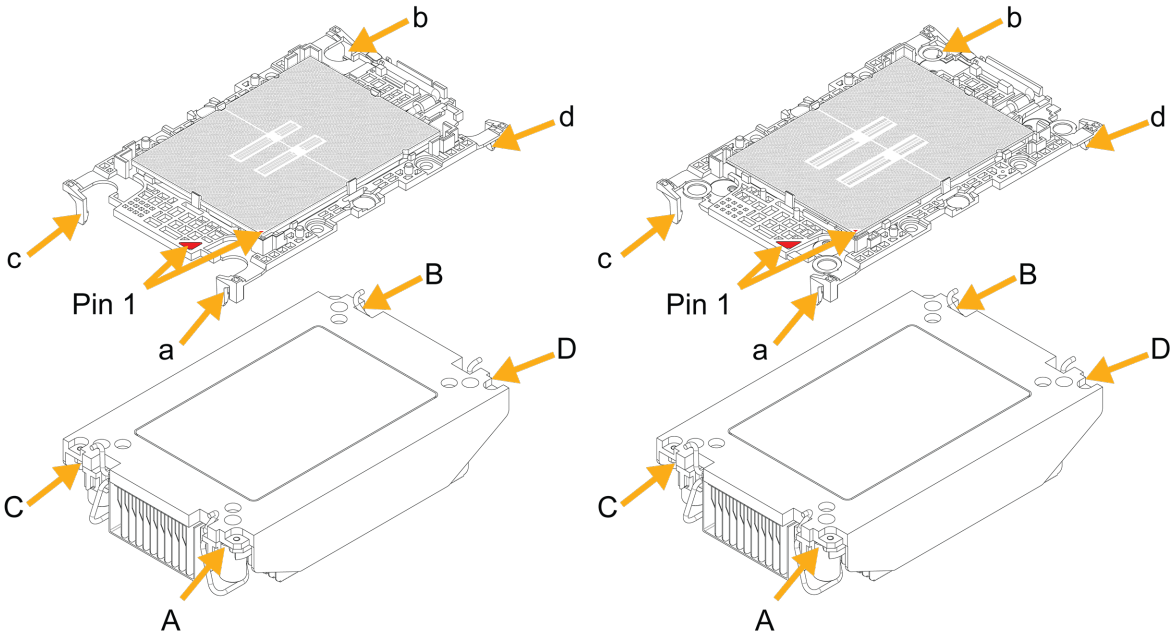


Figure 2-21. Carrier with 1U Heatsink (SP XCC left, SP HCC/LCC right)

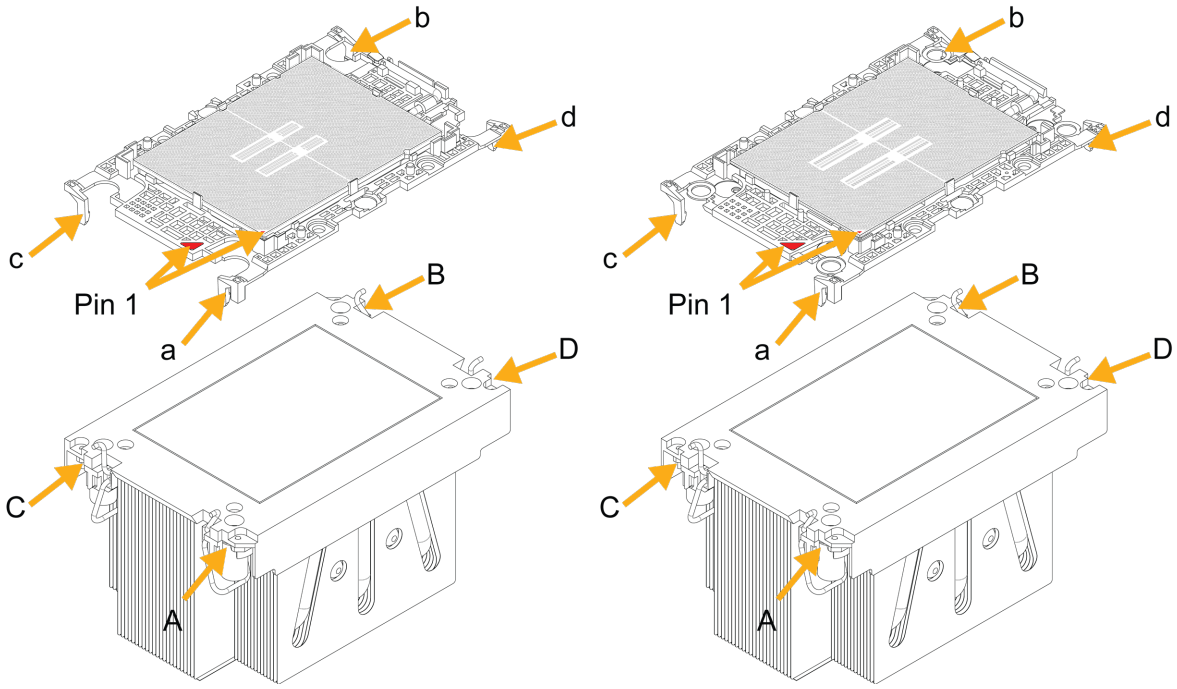


Figure 2-22. Carrier with 2U Heatsink (SP XCC left, SP HCC/LCC right)

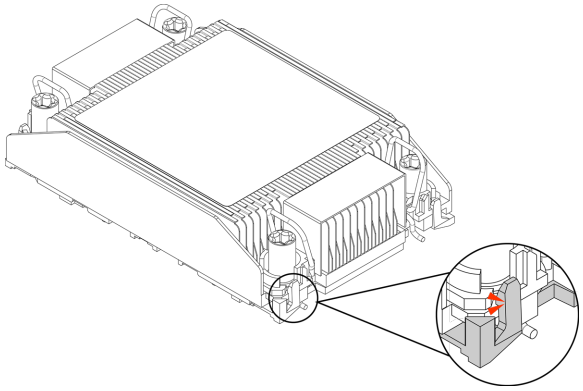


Figure 2-23. PHM Plastic Clips Locked (1U)

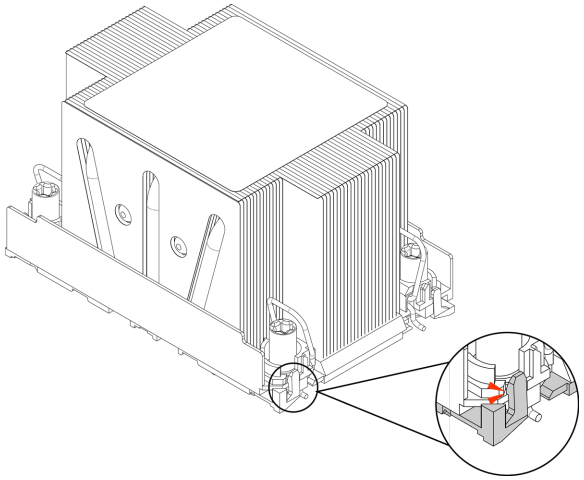


Figure 2-24. PHM Plastic Clips Locked (2U)

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

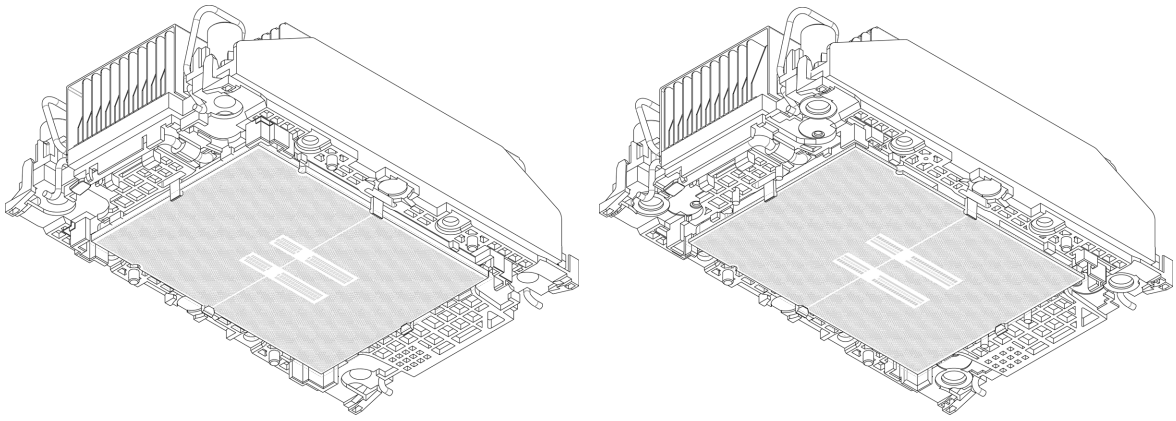


Figure 2-25. 1U PHM Completed (SP XCC left, SP HCC/LCC right)

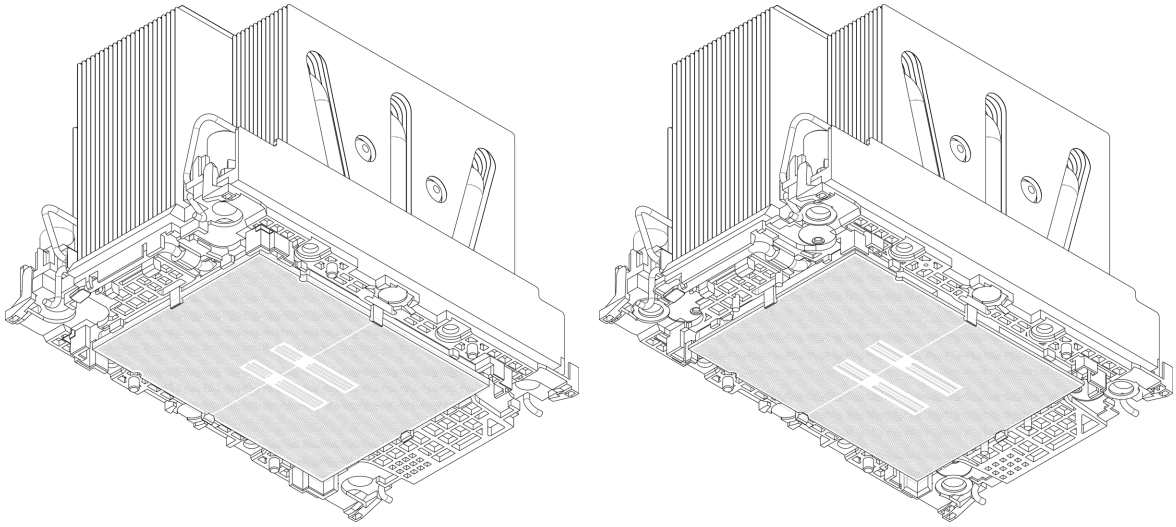


Figure 2-26. 2U PHM Completed (SP XCC left, SP HCC/LCC right)

Preparing the Processor Socket for Installation

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

1. Press the tabs inward.

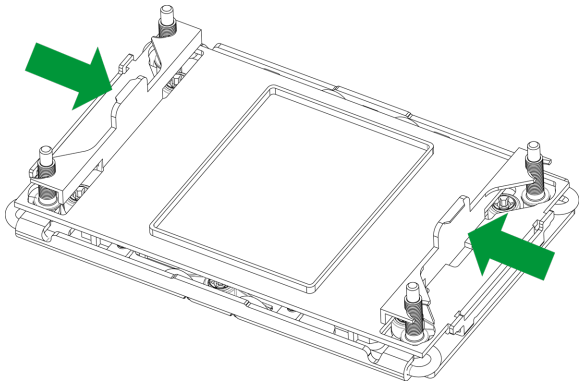


Figure 2-27. Processor Socket with Plastic Protective Cover

2. Pull up the protective cover from the socket.

Note: Do not touch or bend the socket pins.

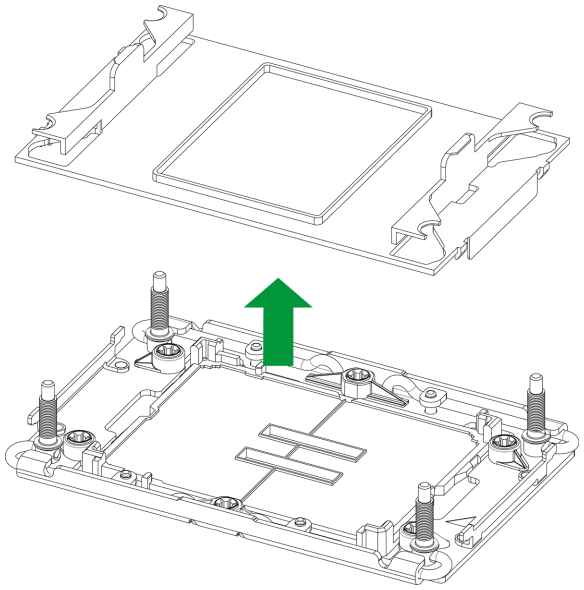
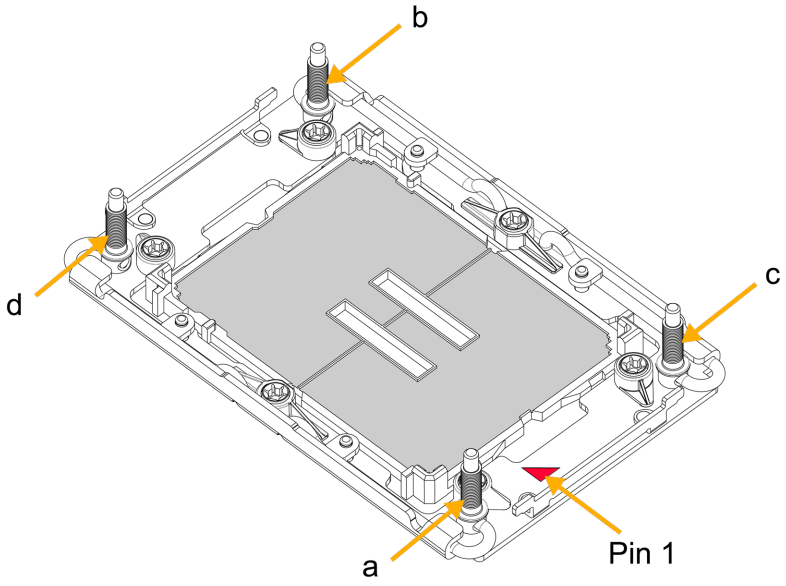


Figure 2-28. Plastic Protective Cover Removed

Preparing to Install the PHM into the Processor Socket

After assembling the Processor Heatsink Module (PHM), you are ready to install it into the processor socket. To ensure the proper installation, follow the procedures below:

1. Locate four threaded fasteners (marked a, b, c, and d) on the processor socket.



a, b, c, d: Threaded Fasteners

Figure 2-29. Threaded Fasteners

2. Locate four PEEK nuts (marked A, B, C, and D) and four rotating wires (marked 1, 2, 3, and 4) on the heatsink.

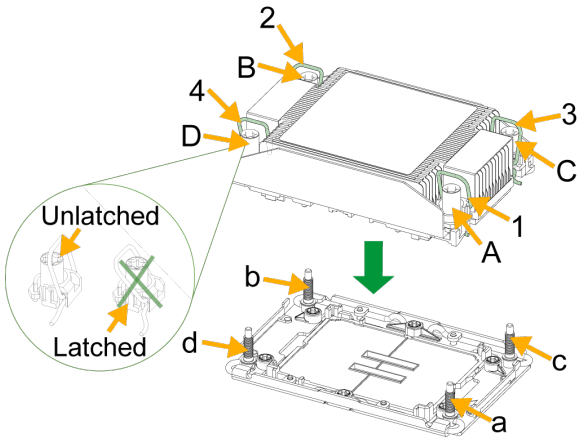


Figure 2-30. PEEK Nuts and Rotating Wires (1U)

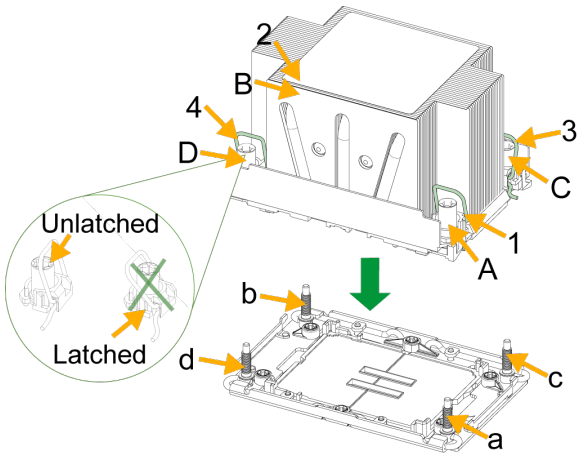


Figure 2-31. PEEK Nuts and Rotating Wires (2U)

3. Check the rotating wires (marked 1, 2, 3, and 4) to make sure that they are at unlatched positions before installing the PHM into the processor socket.

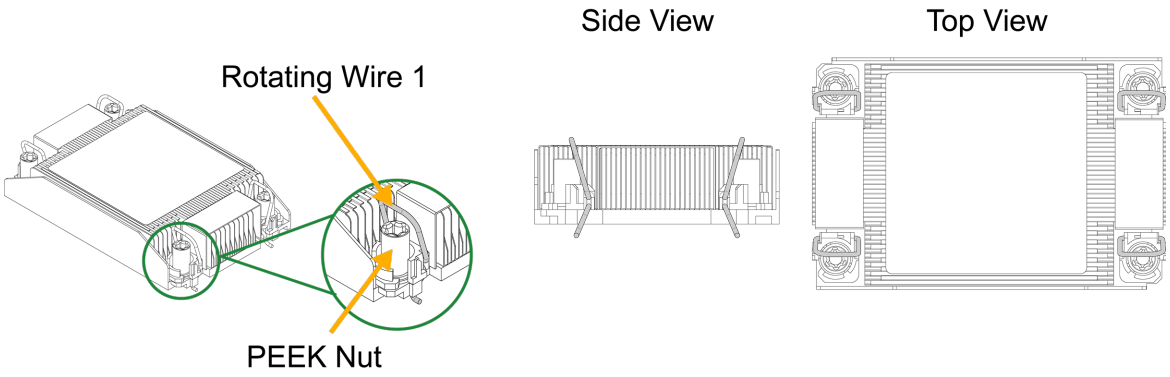


Figure 2-32. 1U Unlatched Positions

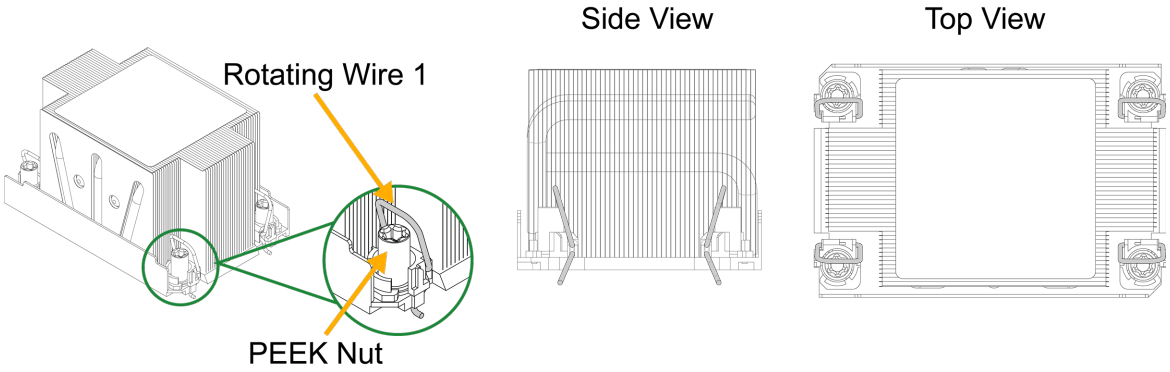


Figure 2-33. 2U Unlatched Positions

Installing the Processor Heatsink Module

1. Align pin 1 of the PHM with the printed triangle on the processor socket.
2. Make sure all four PEEK nuts of the heatsink (marked A, B, C, and D) are aligned with the threaded fasteners (marked a, b, c, and d), then gently place the heatsink on top of the processor socket.

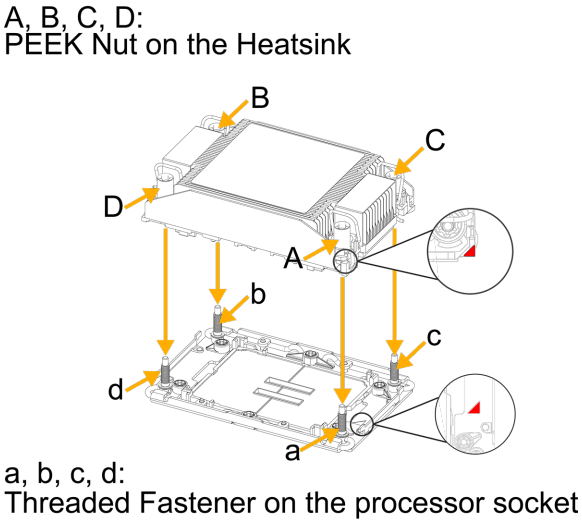


Figure 2-34. Aligning the Heatsink with the Socket (1U)

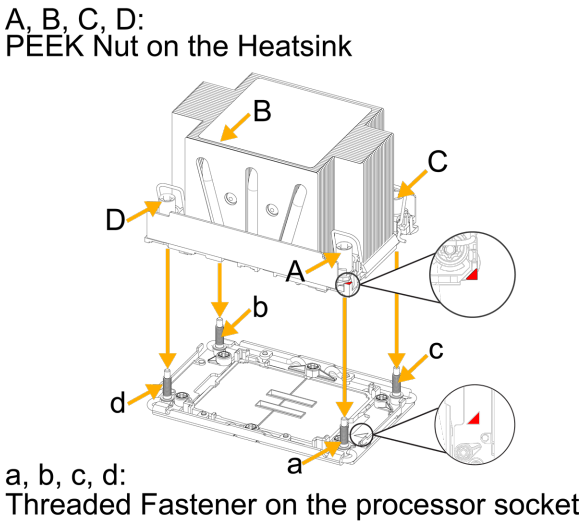


Figure 2-35. Aligning the Heatsink with the Socket (2U)

3. Press all four rotating wires outwards and make sure that the heatsink is securely latched into the processor socket.

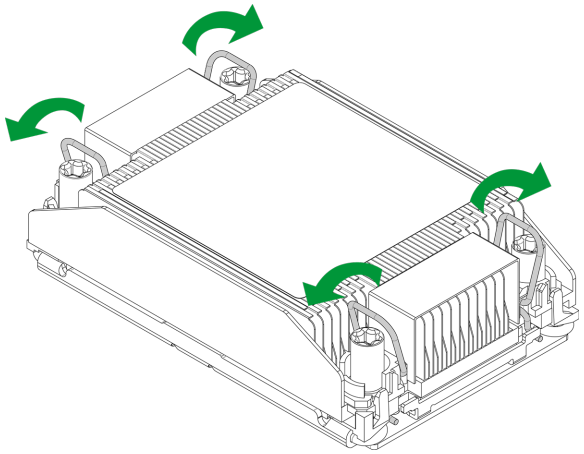


Figure 2-36. Latching the PHM (1U)

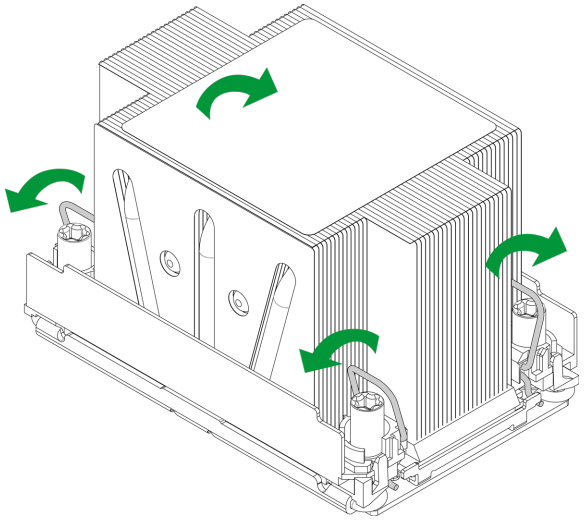


Figure 2-37. Latching the PHM (2U)

4. With a T30 bit torque driver set to a force of 8.0 lbf-in (0.904 N-m), gradually tighten the four screws to ensure even pressure. You can start with any screw, but make sure to tighten the screws in a diagonal pattern.

Important: Do not use a force greater than 8.0 lbf-in (0.904 N-m). Exceeding this force may over-torque the screw, causing damage to the processor, heatsink, and screw.

5. Examine all corners to ensure that the PHM is firmly attached to the socket.

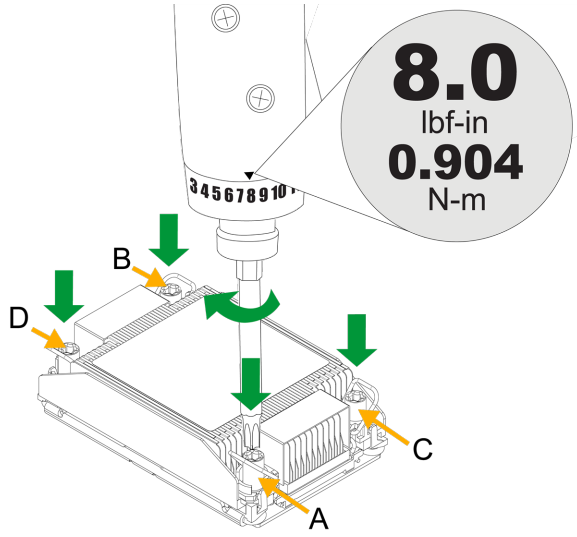


Figure 2-38. Installing the PHM with a Torque Driver (1U)

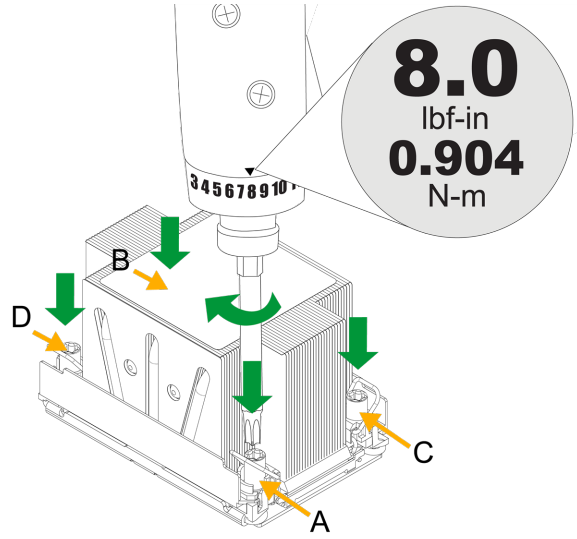


Figure 2-39. Installing the PHM with a Torque Driver (2U)

Removing the Processor Heatsink Module

Before removing the processor heatsink module (PHM) from the motherboard, shut down the system and then unplug the AC power cord from all power supplies.

Then follow the steps below:

1. Use a screwdriver to loosen the four screws. You can start with any screw, but make sure to loosen the screws in a diagonal pattern.

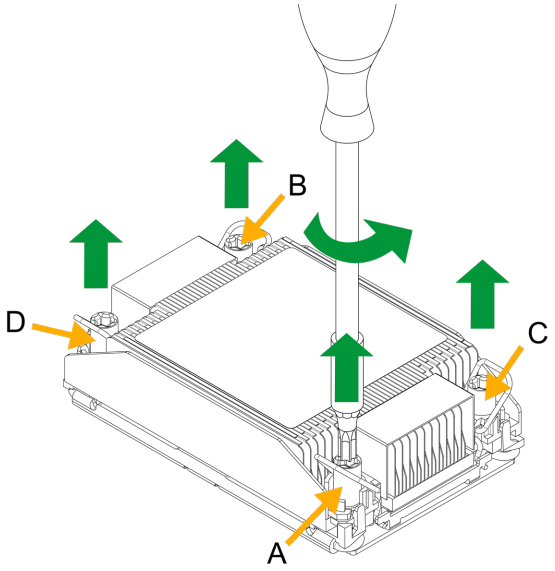


Figure 2-40. Loosening the Screws (1U)

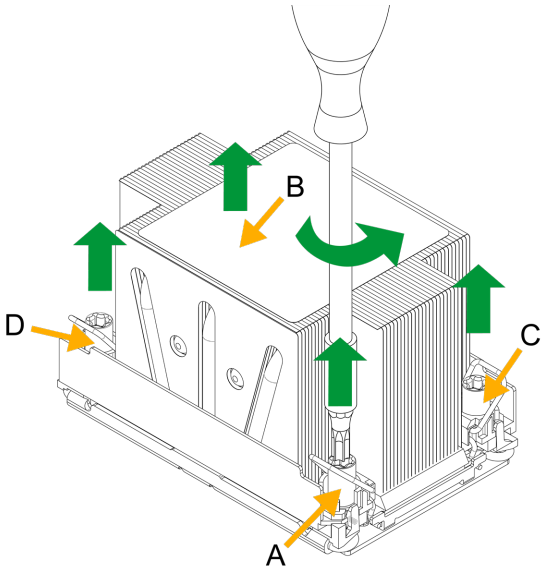


Figure 2-41. Loosening the Screws (2U)

2. Press the four rotating wires inwards to unlatch the PHM from the socket.

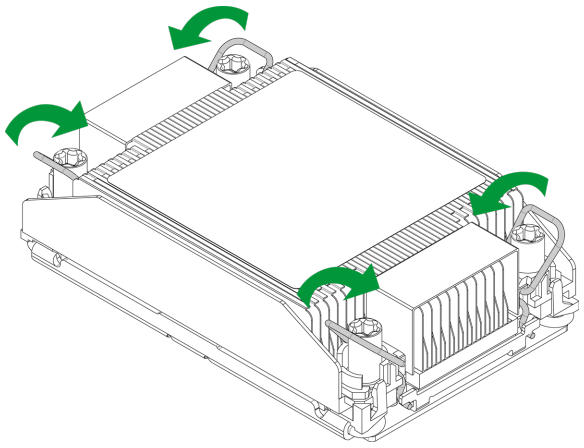


Figure 2-42. Unlatching the PHM (1U)

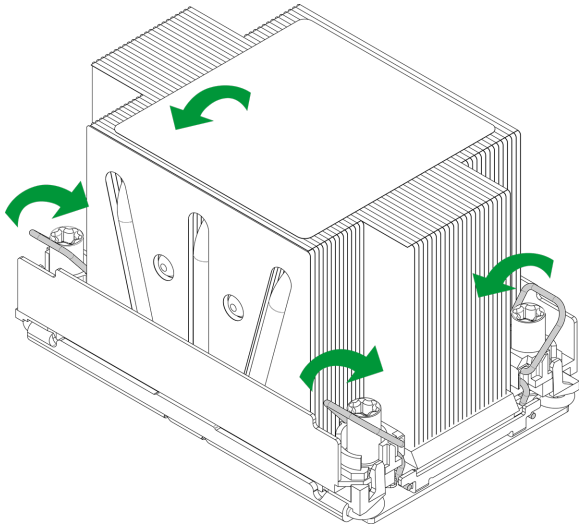


Figure 2-43. Unlatching the PHM (2U)

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

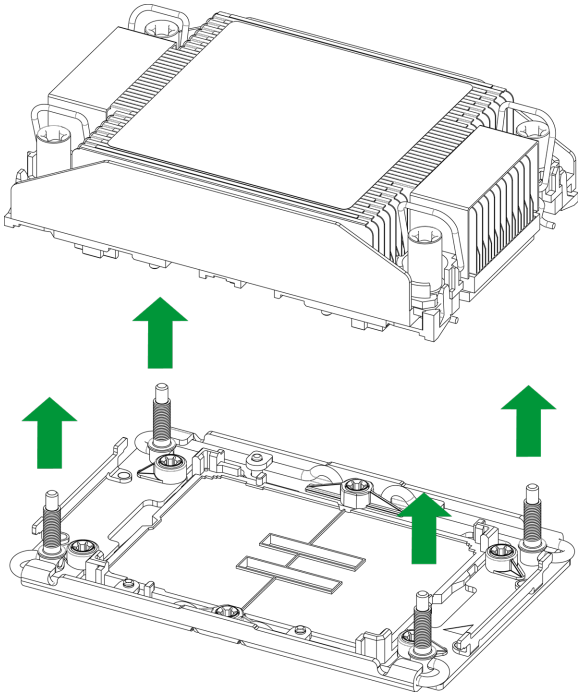


Figure 2-44. Removing the PHM from the Socket (1U)

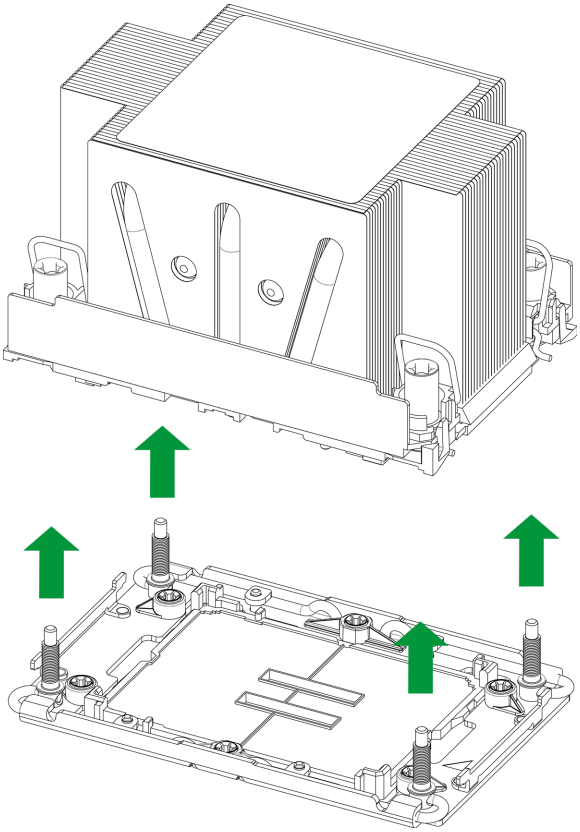


Figure 2-45. Removing the PHM from the Socket (2U)

4. To remove the processor from the heatsink, gently lift the lever from the processor carrier.

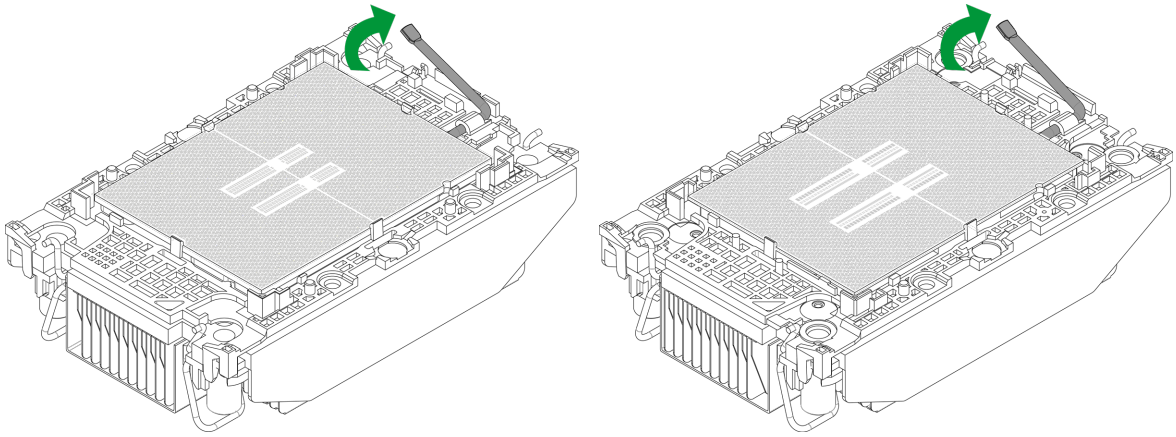


Figure 2-46. Carrier with 1U Heatsink (SP XCC left, SP HCC/LCC right)

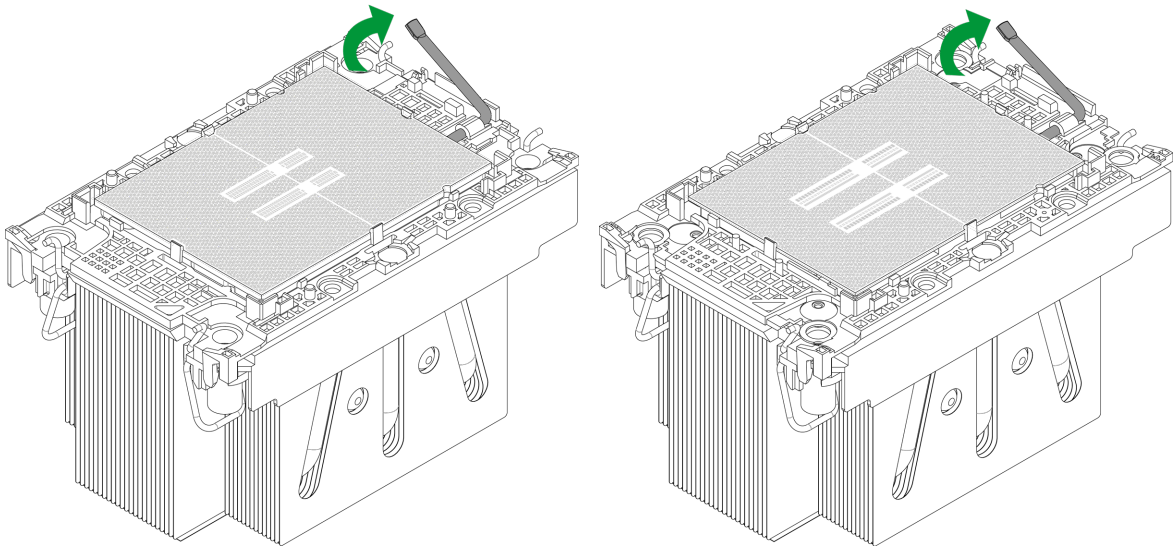


Figure 2-47. Carrier with 2U Heatsink (SP XCC left, SP HCC/LCC right)

5. To remove the processor, move the lever to its unlocked position and gently remove the processor.

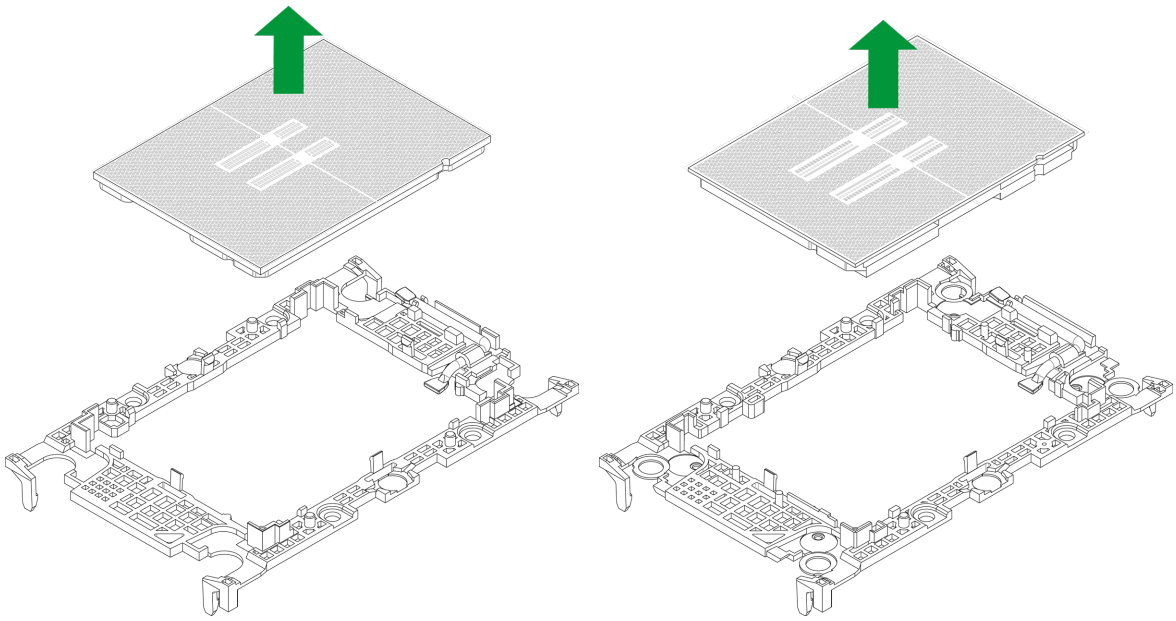


Figure 2-48. Removing the Processor (SP XCC left, SP HCC/LCC right)

2.4 Memory Support and Installation

Important: To prevent any damage, exercise extreme care when installing or removing memory modules.

Note: Check the Supermicro website for recommended memory modules.

Memory Support

The X14SBSC motherboard supports to 512 GB MRDIMM with speeds up to 8000 MT/s (1DPC) or 4 TB of 3DS RDIMM with speeds up to 6400 MT/s (1DPC) or 6000 MT/s (2DPC) in 16 memory slots.

Note: Intel® Xeon® 6700/6500-series processors with P-cores are required to support MRDIMM.

DDR5-6400 Memory Support for Intel® Xeon® 6700/6500-Series Processors with P-Cores									
Type	Ranks Per DIMM, Data Width (Stack)	DIMM Capacity (GB)						Speed (MT/s); Voltage (V); Slots per Channel (SPC) and DIMMs per Channel (DPC)	
		DRAM Density							
		16 Gb		24 Gb		32 Gb		1DPC/2SPC	2DPC/2SPC
		1DPC	2DPC	1DPC	2DPC	1DPC	2DPC	+1.1 V	
RDIMM	1Rx8	16 GB	-	24 GB	-	-	-	6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMs only)	6000**, 5200, 4800 (DDR5-6400 rated RDIMMs only)
	1Rx4	32 GB	-	48 GB	-	-	-		
	2Rx8	32 GB	32 GB	48 GB	-	-	-		
	2Rx4	64 GB	64 GB*^	96 GB	96 GB*^	128 GB*	128 GB*		
3DS RDIMM	4Rx4	-	-	-	-	256 GB*^	256 GB*^		6000**, 5200, 4800 (4H 3DS not supported for 6000)
	8Rx4	-	256 GB	-	-	-	-		
MRDIMM	2Rx8	32 GB	-	-	-	-	-	8000, 7200 (MRDIMM-8800 only)	N/A
	2Rx4	64 GB	-	-	-	-	-		N/A

Notes:

- The items marked with an asterisk (*) are supported in 1S/2S/4S systems. The items with circumflex (^) are supported in 8S systems. All others support 1S/2S only

  MRDIMM is supported with only 1DPC configurations only.

- The items marked with two asterisks: 6000 MT/s support for 2DPC is for 1S, 2S, 4S, 8S and mixed vendor population. 4H 3DS memory is not supported at 6000 MT/s with 2DPC.
- Intel Xeon 6700/6500 series processors with P-cores support 2DPC configurations with 6400 MT/s DIMMs only. 5600 MT/s DIMMs are not supported.
- Intel Xeon 6700/6500-series processors with P-cores supports 1 DIMM per processor socket with the following DIMM configurations only: 16 GB/24 GB 1Rx8 and 32 GB/48 GB 1Rx8.

CXL Memory Configuration Support for Intel® Xeon® 6700/6500-Series Processors with P-Cores									
Native DDR5 Memory Per Socket				CXL Memory Per Socket					
Slot 0 DIMM Ranks	Slot 0 DIMM Capacity (GB)	DIMM Type	DRAM Density (Gb)	CXL Memory Channels	CXL Memory Type	CXL Capacity Per Device/ Module	CXL Inter leave	CXL Mode	4S and 8S support
2Rx4	96	10x4	24	2+2	DDR5 x8	96 GB	1x4*, 2x2, 4x1	1LM+Vol	Yes
2Rx4	128	10x4	32	2+2	DDR4 x8, DDR x8	128 GB	1x4*, 2x2, 4x1	1LM+Vol	Yes
2Rx4	128	10x4	32	2+2	DDR5 x8	128 GB	hetero x12	Hetero	Yes
2Rx4	64	10x4	16	2+2+2	DDR5 x8	128 GB	1x6*, 2x3, 3x2	1LM+Vol	No
2Rx4	64	10x4	16	2	DDR5 x8	128 GB	1x2*	1LM+Vol	No
2Rx4	64	10x4	16	1+1	DDR5 x16	2ch 128 GB	1x2*	Intel Flat Memory Mode	Yes

Notes:

- The items with an asterisk (*) are the default settings in the BIOS.
- The Intel® Xeon® 6700/6500-series processors with P-cores CXL memory configurations are 1DPC ('Slot 0') only for native DDR5.
- CXL Memory Channel: number of devices per root port, with root ports separated by "+". e.g. 2+2+2+2 = four root ports populated with two devices per root port.
- CXL Interleave: sets x ways, e.g. 2x4 = One set of two modules, interleaved four-way
- CXL Modes:
  - 1LM+Vol= Native DDR5 ('1LM') and (volatile) CXL memory visible to SW as separate tiers, separately interleaved.
  - Hetero x12 = DDR5 and (volatile) CXL memory interleaved together in one 12-way set.
  - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW

Intel® Xeon® 6700/6500-Series Processors with P-Cores DDR5 Memory Population Table **(1 Processor and 16 DIMMs Installed, 2DPC)**	
DIMM Counts	***Memory Population Sequence (2DPC)***
1 DIMM (Recommended)	DIMMA1
4 DIMMs (Recommended)	DIMMA1/DIMMC1/DIMME1/DIMMG1 DIMMB1/DIMMD1/DIMMF1/DIMMH1
8 DIMMs	DIMMA1/DIMMA2/DIMMC1/DIMMC2/DIMME1/DIMME2/DIMMG1/DIMMG2 DIMMB1/DIMMB2/DIMMD1/DIMMD2/DIMMF1/DIMMF2/DIMMH1/DIMMH2 **DIMMA1/DIMMB1/DIMMC1/DIMMD1/DIMME1/DIMMF1/DIMMG1/DIMMH1 (Recommended)**
12 DIMMs (Recommended)	DIMMA1/DIMMA2/DIMMB1/DIMMC1/DIMMC2/DIMMD1/ DIMME1/DIMME2/DIMMF1/DIMMG1/DIMMG2/DIMMH1
16 DIMMs (Recommended)	DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2/DIMMG1/DIMMG2/DIMMH1/DIMMH2

DDR5-6400 Memory Support for Intel® Xeon® 6700-Series Processors with E-Cores									
Type	Ranks Per DIMM, Data Width (Stack)	DIMM Capacity (GB)						Speed (MT/s); Voltage (V); Slots per Channel (SPC) and DIMMs per Channel (DPC)	
		DRAM Density							
		16 Gb		24 Gb		32 Gb		1DPC/2SPC	2DPC/2SPC
		1DPC	2DPC	1DPC	2DPC	1DPC	2DPC	+1.1 V	
RDIMM	1Rx4	32 GB	-	-	-	-	-	6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMs only)	N/A
	2Rx8	32 GB	-	-	-	-	-		N/A
	2Rx4	64 GB	64 GB	96 GB	96 GB	-	-		5200, 4800 (DDR5-6400 rated RDIMMs only)
	2Rx4	-	-	-	-	128 GB	128 GB		
3DS RDIMM	4Rx4					256 GB	256 GB		

CXL Memory Configuration Support for Intel® Xeon® 6700-Series Processors with E-Cores								
Native DDR5 Memory Per Socket				CXL Memory Per Socket				
Slot 0 DIMM Ranks	Slot 0 DIMM Capacity (GB)	DIMM Type	DRAM Density (Gb)	CXL Memory Channels	CXL Memory Type	CXL Capacity Per Device/ Module	CXL Interleave	CXL Mode
2Rx4	64	10x4	16	2+2	DDR5 x8	64 GB	1x4*, 2x2, 4x1	1LM+Vol
2Rx4	64	10x4	16	1+1	DDR5 x16	128 GB	1x2*, 2x1	1LM+Vol
1Rx4	32	10x4	16	2	DDR5 x8	128 GB	1x2*	Intel Flat Memory Mode

Notes:

- The items with an asterisk (*) are the default settings in the BIOS.
- The Intel® Xeon® 6700-series processors with E-cores CXL memory configurations are 1DPC ('Slot 0') only for native DDR5.
- CXL Memory Channel: number of devices per root port, with root ports separated by "+," e.g. 2+2+2+2 = four root ports populated with two devices per root port.
- CXL Interleave: sets x ways, e.g. 2x4 = One set of two modules, interleaved four-way.
- CXL Modes:
  - 1LM + Vol = DDR5 ('1LM') and (volatile) CXL memory visible to SW as separate tiers, separately interleaved.
  - Flat Memory Mode = HW manages data movement between DDR5 and CXL memory, total capacity visible to SW.

Intel® Xeon® 6700-Series Processors with E-Cores DDR5 Memory Population Table (1 Processor and 16 DIMMs Installed, 2DPC)	
DIMM Counts	***Memory Population Sequence (2DPC)***
1 DIMM (Recommended)	DIMMA1
4 DIMMs	DIMMA1/DIMMC1/DIMME1/DIMMG1 DIMMB1/DIMMD1/DIMMF1/DIMMH1
8 DIMMs	DIMMA1/DIMMA2/DIMMC1/DIMMC2/DIMME1/DIMME2/DIMMG1/DIMMG2 DIMMB1/DIMMB2/DIMMD1/DIMMD2/DIMMF1/DIMMF2/DIMMH1/DIMMH2 **DIMMA1/DIMMB1/DIMMC1/DIMMD1/DIMME1/DIMMF1/DIMMG1/DIMMH1 (Recommended)**
16 DIMMs (Recommended)	DIMMA1/DIMMA2/DIMMB1/DIMMB2/DIMMC1/DIMMC2/DIMMD1/DIMMD2/ DIMME1/DIMME2/DIMMF1/DIMMF2/DIMMG1/DIMMG2/DIMMH1/DIMMH2

General Guidelines for Optimizing Memory Performance

- Using DDR5 memories with the same type, size, speed, ranking, and density is a mandatory requirement.
- First, confirm whether the installed CPU supports P-cores or E-cores, then refer to the corresponding memory population table and install the memory correctly.

- The motherboard will support an odd number of memory modules. However, to achieve the best memory performance, a balanced memory population is recommended.

DIMM Installation

Important: To avoid causing any damage to the memory module or the DIMM socket, do not use excessive force when pressing the release tabs on the ends of the DIMM socket. Handle memory modules with care. To avoid ESD-related damage to your memory modules or components, carefully follow all the instructions given in "Static-Sensitive Devices" on page 28.

1. Insert the desired number of DIMMs into the memory slots based on the recommended DIMM population table earlier in this section.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.

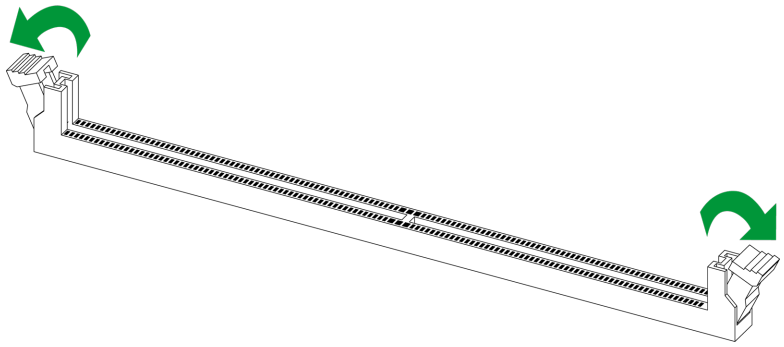


Figure 2-49. Unlocking the DIMM Slot

3. Align the key of the DIMM with the receptive point on the memory slot.

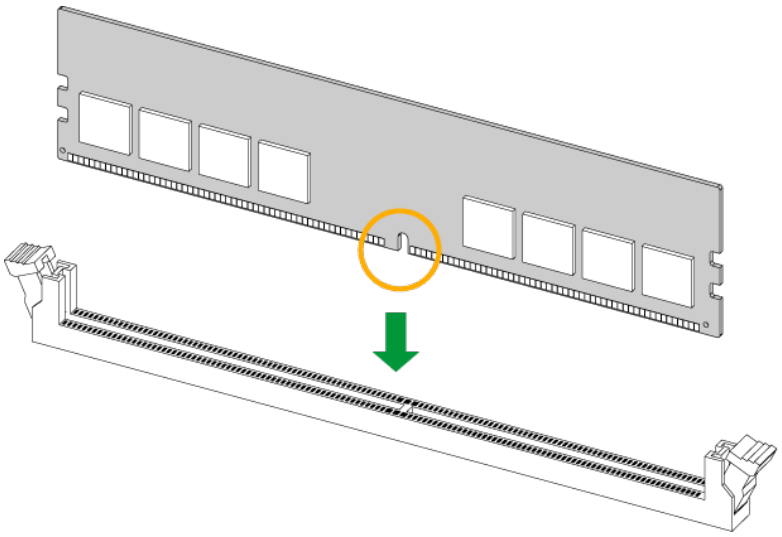


Figure 2-50. Aligning the DIMM Slot with the Receptive Point

4. Align the notches on both ends of the module against the receptive points on the ends of the slot.

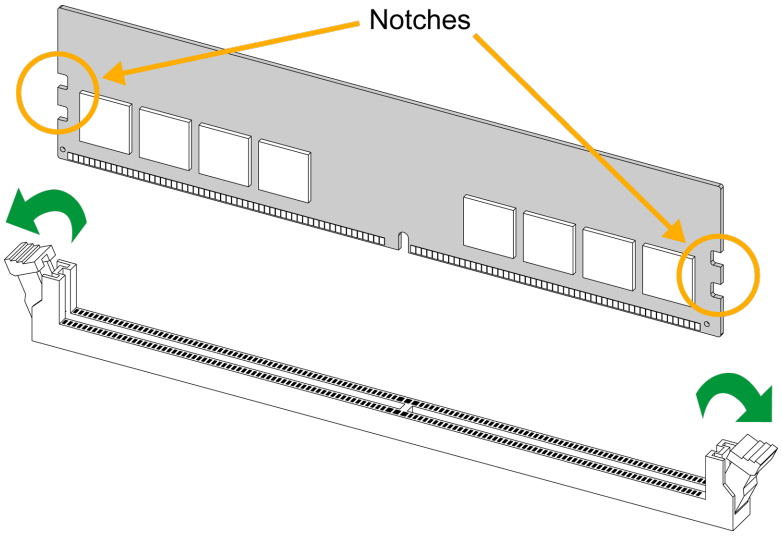


Figure 2-51. Aligning the Notches

5. Press both ends of the module straight down into the slot until the module snaps into place.
6. Press the release tabs to the lock positions to secure the DIMM into the slot.

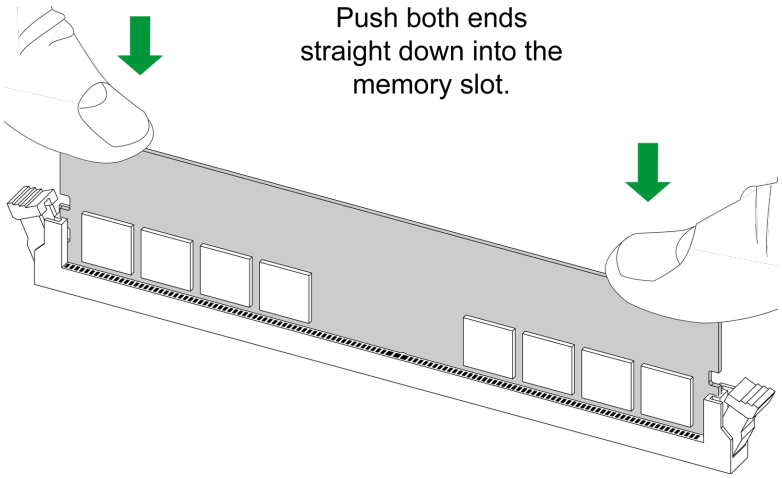


Figure 2-52. Securing the DIMM

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

DIMM Removal

Important: To avoid causing any damage to the memory module or the DIMM socket, do not use excessive force when pressing the release tabs on the ends of the DIMM socket. Handle memory modules with care. To avoid ESD-related damage to your memory modules or components, carefully follow all the instructions given in "Static-Sensitive Devices" on page 28.

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

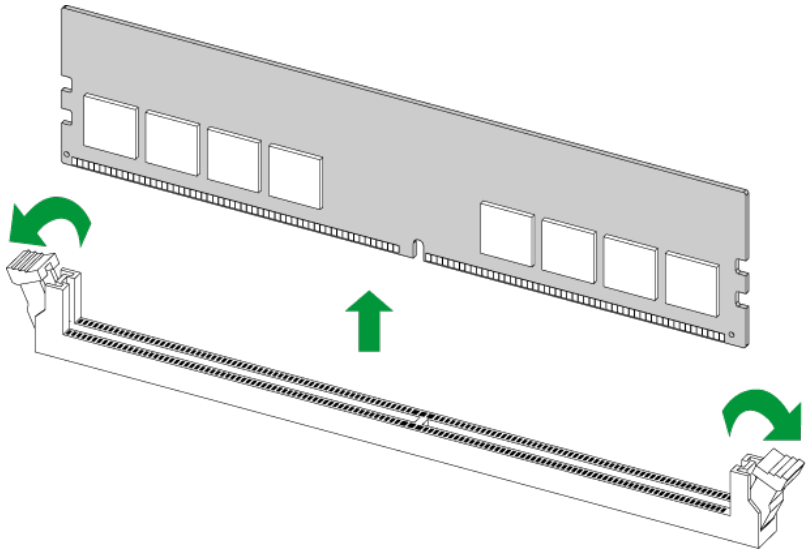


Figure 2-53. Unlocking the DIMM Slot

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

2.5 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

1. Power off your system and unplug your power cable.
2. Place the system on a workbench.
3. Remove the top cover from the system.
4. Locate the onboard battery as shown below.
5. 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.
6. Remove the battery.

Proper Battery Disposal

Important: 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. 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 steps 1 and 2 above and continue below:

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

1. Identify the battery's polarity. The positive (+) side should be facing up.
2. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.

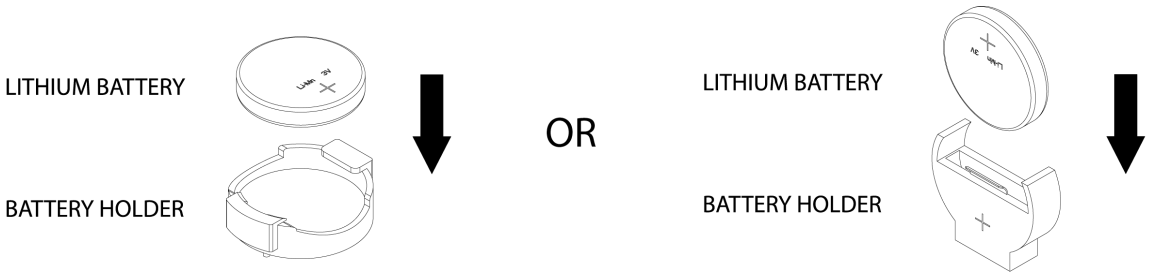


Figure 2-54. Installing a Battery

2.6 Connections, Jumpers, and LEDs

Refer to the following sections for information about connections, jumpers, and LEDs for the X14SBSC motherboard.

Power Supply and Power Connections

For information about the power supply and power connections of the X14SBSC motherboard, refer to the following content.

Power Supply

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

For detailed power supply support for your server, refer to your Top Loading server user manual.

Power Connectors

There is one power connector, BCN2, that connects to the backplane.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Node Fan Board Power Connector

A node fan board power connector is located at JFANPW on the X14SBSC motherboard to provide power to the fan.

Node Fan Board Power Connector Pin Definitions: 8 Total			
Pin#	**Definition**	**Pin#**	**Definition**
1	GND	5	+12 V_FAN
2	GND	6	+12 V_FAN
3	GND	7	+12 V_FAN
4	GND	8	+12 V_FAN

Onboard NVMe Power Connector

An onboard NVMe power connector is located at JPWR_ NVME1 on the X14SBSC motherboard.

Onboard NVMe Power Connector Pin Definitions: 4 Total	
Pin#	**Definition**
1	GND
2	GND
3	+12 V
4	+3.3_V1

Node Power Connector from System

There is one backplane connector located at BCN2 (connects to BPN-SAS3-947SB-1) on the X14SBSC motherboard.

Node Power Connector from System Pin Definitions: 8 Total					
BCN2	Column				
Row		4	3	2	1
	B	+12 V	+12 V	+12 V	+12 V_STBY
	A	GND	GND	GND	GND

Headers and Connections

For information about the headers on the X14SBSC motherboard, refer to the following content.

Fan Board Control Header

A fan board control header is located at JFAN on the X14SBSC motherboard to control the fan speed.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

FAN Board Control Header Pin Definitions: 4 Total	
Pin#	**Definition**
1	I2C_SDA
2	GND
3	I2C_SCL
4	No Connection

Inlet Sensor Header

An inlet sensor header is located on the X14SBSC motherboard. The inlet temperature sensor represents the ambient air temperature entering the system. The equivalent temperature sensor retrievable by the onboard BMC is RT0.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Inlet Sensor Header Pin Definitions: Four Total	
Pin#	**Definition**
1	Data
2	GND
3	Clock
4	+3.3 V Standby

M.2 M-Key PCIe 4.0 x2 Slots

Two M.2 M-key slots are located at JM2_1 and JM2_2 on the X14SBSC motherboard. The M.2 M-key slots on the motherboard support PCIe 4.0 x2 devices in a 22110 form factor.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

MCIO PCIe 5.0 x8 Connectors

Mini Cool Edge IO (MCIO) PCIe 5.0 x8 connectors are located at JNVME1 on the X14SBSC motherboard.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

NC-SI Connection

The Network Controller Sideband Interface (NC-SI) connection is located at JNCSI1 on the X14SBSC motherboard. This connection is used to connect a Network Interface Card (NIC) to the motherboard to allow the onboard Baseboard Management Controller (BMC) to communicate with a network.

Note: For detailed instructions on how to configure Network Interface Card (NIC) settings, refer to the Network Interface Card Configuration User's Guide posted on the web page under the link: https://www.supermicro.com/support/manuals.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Node Control Connector to System

A node control connector is located at BCN1 on the X14SBSC motherboard to control the node and communicate with other system boards such as IO board and middle plane.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Node Control Connector to System Pin Definitions: 54 Total							
BCN1	Column						
Row		1	2	3	4	5	6
	J	SLINK_MP	GND	SLINK_ Node	GND	EXP_I2C1_ SCL	GND
	H	RSVD	I2C1_ SDA	PSU_Alert#	I2C3_ SDA	EXP_I2C1_ SDA	NODE_PRSNT#
	G	GND	I2C1_ SCL	GND	I2C3_ SCL	GND	OTH NODE_ PRSNT#
	F	BMC_PHY_RX_ N	GND	Slot ID	GND	MDI_N1	GND
	E	BMC_PHY_RX_ P	I2C2_ SDA	MATED#	+12 V_ DIS	MDI_P1	MDI_N3
	D	GND	I2C2_ SCL	GND	HS_EN#	GND	MDI_P3
	C	BMC_PHY_TX_ N	GND	PMB_SDA	GND	MDI_N0	GND
	B	BMC_PHY_TX_ P	BMC_ SCL	PMB_SCL	VPP_ SCL	MDI_P0	MDI_N2
	A	GND	BMC_ SDA	GND	VPP_ SDA	GND	MDI_P2

Node Fan Board Control Connector

A node fan board control connector is located at JFAN1 on the X14SBSC motherboard. This connector provides power to the fan board.

Fan Board Control Header Pin Definitions: 4 Total	
Pin#	**Definition**
1	I2C_SDA
2	GND
3	I2C_SCL
4	No Connection

Node PCIe 5.0 Connectors to System

High speed PCIe 5.0 connectors are located at BCN6 and BCN7 on the X14SBSC motherboard, which transmit the PCIe 5.0 signal to the I/O board.

Node PCIe 5.0 Connector to System (BCN6) Pin Definitions: 84 Total	
BCN6	Column

Node PCIe 5.0 Connector to System (BCN6) Pin Definitions: 84 Total							
Row		6	5	4	3	2	1
	N		GND		GND		GND
	M	GND	PE4_TX_N0 (12)	GND	PE3_TX_N0 (8)	GND	PE2_TX_N0 (4)
	L	PE4_TX_N2 (14)	PE4_TX_P0 (12)	PE3_TX_N2 (10)	PE3_TX_P0 (8)	PE2_TX_N2 (6)	PE2_TX_P0 (4)
	K	PE4_TX_P2 (14)	GND	PE3_TX_P2 (10)	GND	PE2_TX_P2 (6)	GND
	J	GND	PE4_TX_N1 (13)	GND	PE3_TX_N1 (9)	GND	PE2_TX_N1 (5)
	I	PE4_TX_N3 (15)	PE4_TX_P1 (13)	PE3_TX_N3 (11)	PE3_TX_P1 (9)	PE2_TX_N3 (7)	PE2_TX_P1 (5)
	H	PE4_TX_P3 (15)	GND	PE3_TX_P3 (11)	GND	PE2_TX_P3 (7)	GND
	G	GND	PE4_RX_N0 (12)	GND	PE3_RX_N0 (8)	GND	PE2_RX_N0 (4)
	F	PE4_RX_N2 (14)	PE4_RX_P0 (12)	PE3_RX_N2 (10)	PE3_RX_P0 (8)	PE2_RX_N2 (6)	PE2_RX_P0 (4)
	E	PE4_RX_P2 (14)	GND	PE3_RX_P2 (10)	GND	PE2_RX_P2 (6)	GND
	D	GND	PE4_RX_N1 (13)	GND	PE3_RX_N1 (9)	GND	PE2_RX_N1 (5)
	C	PE4_RX_N3 (15)	PE4_RX_P1 (13)	PE3_RX_N3 (11)	PE3_RX_P1 (9)	PE2_RX_N3 (7)	PE2_RX_P1 (5)
	B	PE4_RX_P3 (15)	GND	PE3_RX_P3 (11)	GND	PE2_RX_P3 (7)	GND
	A	GND		GND		GND	

Node PCIe 5.0 Connector to System (BCN7) Pin Definitions: 84 Total	
BCN7	Column

Node PCIe 5.0 Connector to System (BCN7) Pin Definitions: 84 Total							
Row		6	5	4	3	2	1
	N		GND		GND	PE_RESET	GND
	M	GND	PE1_TX_N0 (0)	GND	PE2_REFCLK_N	GND	PE5_TX_N1 (5)
	L	PE1_TX_N2 (2)	PE1_TX_P0 (0)	PE4_REFCLK_N	PE2_REFCLK_P	PE6_TX_N1 (7)	PE5_TX_P1 (5)
	K	PE1_TX_P2 (2)	GND	PE4_REFCLK_P	GND	PE6_TX_P1 (7)	GND
	J	GND	PE1_TX_N1 (1)	GND	PE1_REFCLK_N	GND	PE5_TX_N0 (4)
	I	PE1_TX_N3 (3)	PE1_TX_P1 (1)	PE3_REFCLK_N	PE1_REFCLK_P	PE6_TX_N0 (6)	PE5_TX_P0 (4)
	H	PE1_TX_P3 (3)	GND	PE3_REFCLK_P	GND	PE6_TX_P0 (6)	GND
	G	GND	PE1_RX_N0 (0)	GND	PE6_REFCLK_N	GND	PE5_RX_N1 (5)
	F	PE1_RX_N2 (2)	PE1_RX_P0 (0)	RSVD	PE6_REFCLK_P	PE6_RX_N1 (7)	PE5_RX_P1 (5)
	E	PE1_RX_P2 (2)	GND	RSVD	GND	PE6_RX_P1 (7)	GND
	D	GND	PE1_RX_N1 (1)	GND	PE5_REFCLK_N	GND	PE5_RX_N0 (4)
	C	PE1_RX_N3 (3)	PE1_RX_P1 (1)	RSVD	PE5_REFCLK_P	PE6_RX_N0 (6)	PE5_RX_P0 (4)
	B	PE1_RX_P3 (3)	GND	RSVD	GND	PE6_RX_P0 (6)	GND
	A	GND	MBD_CPLD_RSVD	GND	3808N_PERST_N_B	GND	3808N_PERST_N_A

Node SAS 3.0 Connectors to System

High speed PCIe 5.0 connectors are located at BCN3, BCN4, and BCN5 on the X14SBSC motherboard, which transmit the SAS 3.0 signal to the expander board.

Node SAS 3.0 Connector to System (BCN3) Pin Definitions: 54 Total	
BCN3	Column

Node SAS 3.0 Connector to System (BCN3) Pin Definitions: 54 Total							
Row		1	2	3	4	5	6
	J	SAS_TX_N0	GND	SAS_TX_N2	GND	SAS_TX_N6	GND
	H	SAS_TX_P0	SAS_TX_N1	SAS_TX_P2	SAS_TX_N4	SAS_TX_P6	SAS_TX_N7
	G	GND	SAS_TX_P1	GND	SAS_TX_P4	GND	SAS_TX_P7
	F	SAS_RX_N1	GND	RSVD	GND	SAS_TX_N5	GND
	E	SAS_RX_P1	SAS_RX_N3	RSVD	SAS_TX_N3	SAS_TX_P5	RSVD
	D	GND	SAS_RX_P3	GND	SAS_TX_P3	GND	RSVD
	C	SAS_RX_N0	GND	SAS_RX_N4	GND	SAS_RX_N6	GND
	B	SAS_RX_P0	SAS_RX_N2	SAS_RX_P4	SAS_RX_N5	SAS_RX_P6	SAS_RX_N7
	A	GND	SAS_RX_P2	GND	SAS_RX_P5	GND	SAS_RX_P7

Node SAS 3.0 Connector to System (BCN4) Pin Definitions: 54 Total							
BCN4	Column						
Row		1	2	3	4	5	6
	J	SAS_TX_N8	GND	SAS_TX_N10	GND	SAS_TX_N14	GND
	H	SAS_TX_P8	SAS_TX_N9	SAS_TX_P10	SAS_TX_N12	SAS_TX_P14	SAS_TX_N15
	G	GND	SAS_TX_P9	GND	SAS_TX_P12	GND	SAS_TX_P15
	F	SAS_RX_N9	GND	RSVD	GND	SAS_TX_N13	GND
	E	SAS_RX_P9	SAS_RX_N11	RSVD	SAS_TX_N11	SAS_TX_P13	RSVD
	D	GND	SAS_RX_P11	GND	SAS_TX_P11	GND	RSVD
	C	SAS_RX_N8	GND	SAS_RX_N12	GND	SAS_RX_N14	GND
	B	SAS_RX_P8	SAS_RX_N10	SAS_RX_P12	SAS_RX_N13	SAS_RX_P14	SAS_RX_N15
	A	GND	SAS_RX_P10	GND	SAS_RX_P13	GND	SAS_RX_P15

Node SAS 3.0 Connector to System (BCN5) Pin Definitions: 54 Total	
BCN5	Column

Node SAS 3.0 Connector to System (BCN5) Pin Definitions: 54 Total							
Row		1	2	3	4	5	6
	J	SAS_TX_N16	GND	SAS_TX_N18	GND	SAS_TX_N22	GND
	H	SAS_TX_P16	SAS_TX_N17	SAS_TX_P18	SAS_TX_N20	SAS_TX_P22	SAS_TX_N23
	G	GND	SAS_TX_P17	GND	SAS_TX_P20	GND	SAS_TX_P23
	F	SAS_RX_N17	GND	RSVD	GND	SAS_TX_N21	GND
	E	SAS_RX_P17	SAS_RX_N19	RSVD	SAS_TX_N19	SAS_TX_P21	RSVD
	D	GND	SAS_RX_P19	GND	SAS_TX_P19	GND	RSVD
	C	SAS_RX_N16	GND	SAS_RX_N20	GND	SAS_RX_N22	GND
	B	SAS_RX_P16	SAS_RX_N18	SAS_RX_P20	SAS_RX_N21	SAS_RX_P22	SAS_RX_N23
	A	GND	SAS_RX_P18	GND	SAS_RX_P21	GND	SAS_RX_P23

NVMe I²C Header

Connector JNVI²C1 on the X14SBSC motherboard is a management header for the Supermicro AOC NVMe PCIe peripheral card. Connect the I²C cable to this connector.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

8-Pin Onboard Standby Fan Header

An onboard standby fan header is located at FAN1 on the X14SBSC motherboard.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Onboard Standby FAN Header Pin Definitions: 8 Total			
Pin#	**Definition**	**Pin#**	**Definition**
1	GND	5	GND
2	+12 V_FAN	6	+12 V_FAN
3	FAN_TACH0	7	FAN_TACH1
4	FAN_PWM	8	FAN_PRSNT#

SAS 3.0 Connections (SlimSAS)

Three SAS 3.0 connections are located at CNS1, CNS2, and CNS3 on the X14SBSC motherboard. Use a SlimSAS cable to connect SATA 3.0 or PCIe devices to the motherboard.

TPM/Port 80 Header

The JTPM1 header on the X14SBSC motherboard is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from Supermicro (optional). A TPM/Port 80 connector is a security device that supports encryption and authentication in storage drives. It allows the motherboard to deny access if the TPM associated with the storage drive is not installed in the system. Information on the TPM is available at the following page:

https://www.supermicro.com/manuals/other/AOM-TPM-9670V_9670H__X12_H12.pdf

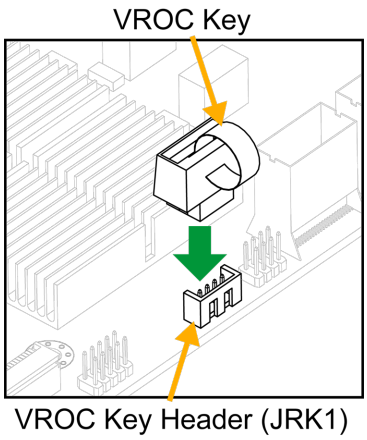
For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Trusted Platform Module Header Pin Definitions: 10 Total			
Pin#	**Definition**	**Pin#**	**Definition**
1	+3.3 V	2	SPI_CS#
3	RESET#	4	SPI_MISO
5	SPI_CLK	6	GND
7	SPI_MOSI	8	No Connection
9	+1.8 V Standby	10	SPI_IRQ#

VROC RAID Key Header

A VROC RAID Key header is located at JRK1 on the X14SBSC motherboard. Install a VROC RAID key on JRK1 for NVMe RAID support as shown in the illustration below.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.



Intel VROC Key Pin Definitions: Four Total	
Pin#	**Definition**
1	GND
2	+3.3 V Standby
3	GND
4	CPU RAID Key

Note: Images displayed are for illustrative purposes only. The components installed in your system may or may not look exactly the same as the graphics shown in the manual.

Note: For detailed instructions on how to configure VROC RAID settings, refer to the VROC RAID Configuration User's Guide posted on the web page under the following link: https://www.supermicro.com/support/manuals.

I/O Ports



Figure 2-55. X14SBSC I/O Ports

I/O Ports	
#	**Description**
1	BMC_LAN
2	USB0 (3.2 Gen 1)
3	USB1 (3.2 Gen 1)

LAN Ports

The motherboard has one dedicated BMC LAN port.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

BMC LAN Pin Definitions: 19 Total			
Pin#	**Definition**	**Pin#**	**Definition**
		29	Link 1000 LED (Amber)
20	TD0+	30	Link 100 LED (Green)
21	TD0-	31	Active LED (Yellow)
22	TD1+	32	GND
23	TD1-	33	SGND
24	TD2+	34	SGND
25	TD2-	35	SGND
26	TD3+	36	SGND
27	TD3-		
28	GND		

Unit Identifier Button

A Unit Identifier (UID) button and two LED indicators are located on the motherboard. The UID button is located near the I/O ports of the X14SBSC motherboard.

Note: After pushing and holding the UID button for 12 seconds, all BMC settings including username and password will revert back to the factory default. Only the network settings and FRU are retained.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Function	User Input	Behavior	LED Activity
UID LED Indicator	Push once Push again	Turns on the UID LED Turns off the UID LED	UID LED turns solid blue UID LED turns off
BMC Reset	Push and hold for 6 seconds Push and hold for 12 seconds	BMC will do a cold boot BMC will reset to factory default	BMC Heartbeat LED turns solid green BMC Heartbeat LED turns solid green

UID Button Pin Definitions: Four Total	
Pin#	**Definition**
1	Button In
2	GND
G1	GND
G2	GND

UID LED Pin Definitions: Four Total	
Color	**Status**
1	Button In
2	GND
G1	GND
G2	GND

USB Ports

There are two USB 3.2 Gen 1 ports (USB0/1) on the rear I/O panel of the X14SBSC motherboard. There is also one USB header (J35) on the front panel.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

USB0/1 (USB 3.2 Gen 1) Port Pin Definitions: 18 Total			
Pin#	**Definitions**	**Pin#**	**Definitions**
1	VBUS	10	VBUS
2	D-	11	D-
3	D+	12	D+
4	GND	13	GND
5	STDA_SSRX-	14	STDA_SSRX-
6	STDA_SSRX+	15	STDA_SSRX+
7	GND	16	GND
8	STDA_SSTX-	17	STDA_SSTX-
9	STDA_SSTX+	18	STDA_SSTX+

Jumper Settings

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.

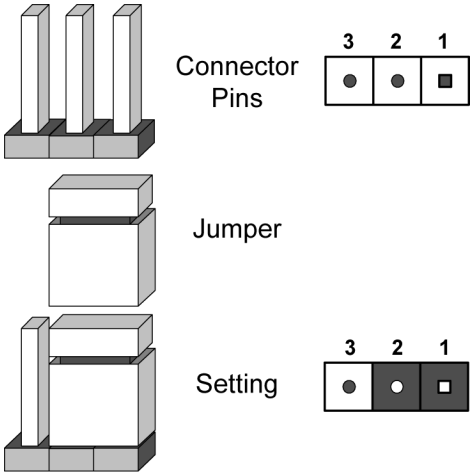


Figure 2-56. Jumping Connector Pins

CMOS Clear

JBT1 on the X14SBSC motherboard is used to clear CMOS, which will also clear any passwords. Instead of pins, this jumper consists of contact pads to prevent accidentally clearing the contents of CMOS.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.



1. First power down the system and unplug the power cord(s).
2. Remove the cover of the chassis to access the motherboard.
3. Remove the onboard battery from the motherboard.
4. Short the CMOS pads, JBT1, with a metal object such as a small screwdriver for at least four seconds.

   Note: Clearing CMOS will also clear all passwords.

5. Remove the screwdriver (or shorting device).
6. Replace the cover, reconnect the power cord(s), and power on the system.

TPM Select

Use JPT1 to select between the onboard TPM or external TPM. The default setting is Onboard TPM.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

TPM Select Jumper Settings	
Jumper Setting	**Definition**
Pins 1–2	Pins 1–2: Onboard TPM (Default)
Pins 2–3	Pins 2–3 External TPM

LED Indicators

For information about the LED indicators on the X14SBSC motherboard, refer to the following content.

BMC Heartbeat LED

A BMC Heartbeat LED is located at LEDBMC on the X14SBSC motherboard. When this LED is blinking, the BMC is functioning normally.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

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

Expander SAS35X48 Heartbeat LED

An Expander SAS35X48 Heartbeat LED is located at LED1 on the X14SBSC motherboard. When this LED is blinking, the expander is working normally.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Expander SAS35X48 Heartbeat LED	
LED Color	**Definition**
Green: Blinking	Expander working

Front Panel Power LED

The Front Panel Power LED is located at LEDPWR on the X14SBSC motherboard. When this LED is on, the front panel is on.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

Front Panel Power LED Indicator	
LED Color	**Definition**
Off	Front Panel Power Off (power cable not connected)
Green	Front Panel Power On

M.2 LEDs

M.2 LEDs are located at LED4 and LED7 on the X14SBSC motherboard. When these LEDs are blinking, the M.2 devices are functioning normally.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

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

SAS 3808N Heartbeat LED

A SAS 3808N Heartbeat LED is located at LED20 on the X14SBSC motherboard. When this LED is blinking green, SAS 3808N is working normally.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

SAS 3808N Alert LED	
LED Color	**Definition**
Green: Blinking	SAS 3808N Working

Unit ID (UID) LED

The UID LED indicator is located at LED6 on the X14SBSC motherboard. This UID indicator provides easy identification of a system that may need to be serviced.

For a detailed diagram of the X14SBSC motherboard, see the layout under "Quick Reference" on page 15.

UID LED LED Indicator	
LED Color	**Definitions**
Blue: On	System Identified

Chapter 3:

Troubleshooting

The following content contains information on common issues and how to resolve them.

3.1 Troubleshooting Procedures **80**
Before Power On 80
No Power 80
No Video 80
System Boot Failure 80
Memory Errors 81
Losing the System's Setup Configuration 81
If the System Becomes Unstable 81
3.2 Technical Support Procedures **83**
3.3 Motherboard Battery **84**
3.4 Where to Get Replacement Components **85**
3.5 Returning Merchandise for Service **86**
3.6 Feedback **87**

3.1 Troubleshooting Procedures

Use the following procedures to troubleshoot your system. If you have followed all of the procedures below and still need assistance, refer to the "Technical Support Procedures" on page 83 or "Returning Merchandise for Service" on page 86 section(s) in this chapter. Always disconnect the AC power cord before adding, changing or installing any non hot-swappable hardware components. If the below steps do not fix the setup configuration problem, contact your vendor for repairs.

Before Power On

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

No Power

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

No Video

1. If the power is on, but you do not have video, remove all add-on cards and cables.
2. Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory, or try a different one).

System Boot Failure

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

1. Check the screen for an error message.
2. Clear the CMOS settings by unplugging the power cord and contacting both pads on the CMOS clear jumper. Restart the system. Refer to "CMOS Clear" on page 75.
3. Remove all components from the motherboard and turn on the system with only one DIMM installed. If the system boots, turn off the system and repopulate the components back into the system to retest. Add one component at a time to isolate which one may have caused the system boot issue.

Memory Errors

When suspecting faulty memory is causing the system issue, check the following:

1. Make sure that the memory modules are compatible with the system and are properly installed. See "Component Installation" on page 26 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMMs in the system.
3. Make sure that you are using the correct type of DIMMs recommended by the manufacturer.
4. Check for bad DIMMs or slots by swapping a single module among all memory slots and check the results.

Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to "Introduction" on page 14 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.

If the System Becomes Unstable

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

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

2. Memory support: Make sure that the memory modules are supported. Refer to the product page on our website at https://www.supermicro.com. Test the modules using memtest86 or a similar utility.

   Note: Click on the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.

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

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 a USB flash or media device.
2. Cable connection: Check to make sure that all cables are connected and working properly.
3. Use the minimum configuration for troubleshooting: Remove all unnecessary components (starting with add-on cards first), and use the minimum configuration (but with the processor and a memory module installed) to identify the trouble areas. Refer to the steps listed above in this section 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.

3.2 Technical Support Procedures

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

1. Refer to "Troubleshooting Procedures" on page 80 or see the FAQs on our website (https://www.supermicro.com/FAQ/index.php) before contacting Technical Support.
2. BIOS upgrades can be downloaded from our website (https://www.supermicro.com/support/resources/bios_ipmi.php).
3. If you still cannot resolve the problem, include the following information when contacting Supermicro for technical support:
   - Motherboard model and PCB revision number
   - BIOS release date/version (This can be seen on the initial display when your system first boots up.)
   - System configuration
4. An example of a Technical Support form is on our website at https://webpr3.supermicro.com/SupportPortal.
5. Distributors: For immediate assistance, have your account number ready when placing a call to our Technical Support department. For Supermicro contact information, refer to "Contacting Supermicro" on page 13.

3.3 Motherboard Battery

For information on removing, disposing of, and replacing the motherboard battery of your system, refer to "Battery Removal and Installation" on page 61.

3.4 Where to Get Replacement Components

If you need replacement parts for your X14SBSC motherboard, to ensure the highest level of professional service and technical support, purchase exclusively from our Supermicro Authorized Distributors/System Integrators/Resellers. A list can be found on the Supermicro website:

https://www.supermicro.com

Under the "Buy" menu, click the "Where to Buy" link.

3.5 Returning Merchandise for Service

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

For faster service, RMA authorizations can be requested online at the following page:

https://www.supermicro.com/RmaForm

Whenever possible, repack the motherboard in the original Supermicro carton, using the original packaging material. If these are no longer available, be sure to pack the motherboard securely, using packaging material to surround the motherboard so that it does not shift within the carton and become damaged during shipping.

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

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

3.6 Feedback

Supermicro values your feedback as we strive to improve our customer experience in all facets of our business. Email us at Techwriterteam@supermicro.com to provide feedback on our manuals.

Chapter 4:

UEFI BIOS

The following content contains information on BIOS configuration with the X14SBSC motherboard.

4.1 Introduction **89**
4.2 Main Setup **91**
4.3 Advanced Setup Configurations **93**
4.4 Event Logs **176**
4.5 BMC **178**
4.6 Security **182**
4.7 Boot **189**
4.8 Save & Exit **191**

4.1 Introduction

This chapter describes the AMIBIOS™ Setup utility for the motherboard. The BIOS is stored on a chip and can be easily upgraded using the UEFI script (flash.nsh), the BMC WebUI, or the SuperServer Automation Assistant (SAA) utility.

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. Refer to the Manual Download area of our website for any changes to BIOS that may not be reflected in this manual.

Updating BIOS

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 the following page:

https://www.supermicro.com/support/resources/bios_ipmi.php

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.

Important: Do not shut down or reset the system while updating the BIOS to prevent possible system boot failure! Read the motherboard README file carefully before you perform the BIOS update.

To update the BIOS under the UEFI Shell, unzip the BIOS file onto a bootable USB device and then boot into the built-in UEFI Shell. For motherboards with BMC support, type "flash.nsh <BIOS filename><BMC Username><BMC Password>" to start the BIOS update. The flash.nsh script will invoke the SAA (EFI) tool automatically to perform the BIOS update, beginning with uploading the BIOS image to BMC. After uploading the BIOS image, the system will reboot to continue the process. The BMC will take over and continue the BIOS update in the background. The process will take 3–5 minutes. Refer to the README file for more information.

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 hot keys are used, such as <F1>, <F2>, etc. Each main BIOS menu option is described in this manual.

The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When a BIOS submenu or item 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 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>, <F5>, <F6>, <Enter>, <ESC>, the arrow keys, etc.) can be used at any time during the setup navigation process.

4.2 Main Setup

The Main setup screen appears when the AMI BIOS Setup utility is first entered. To return to the Main setup screen, select the Main tab at the top of the screen. The Main BIOS setup screen is shown below.

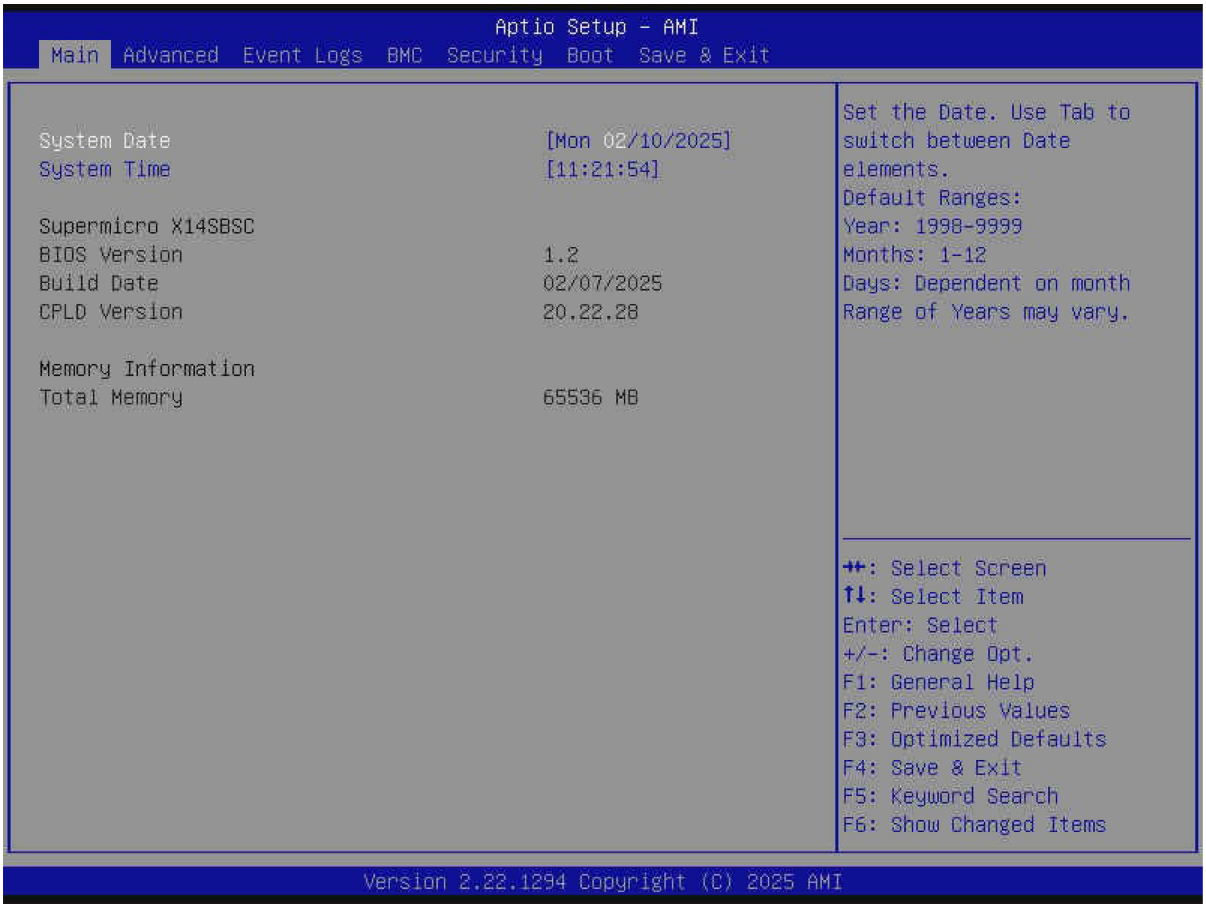


Figure 4-1. Main Setup Screen

System Date/System Time

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

Note: The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00.

Supermicro X14SBSC

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 Complex-Programmable Logical Device (CPLD) used in the system.

Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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

Important: Use 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, revert the settings to the default manufacturing settings.

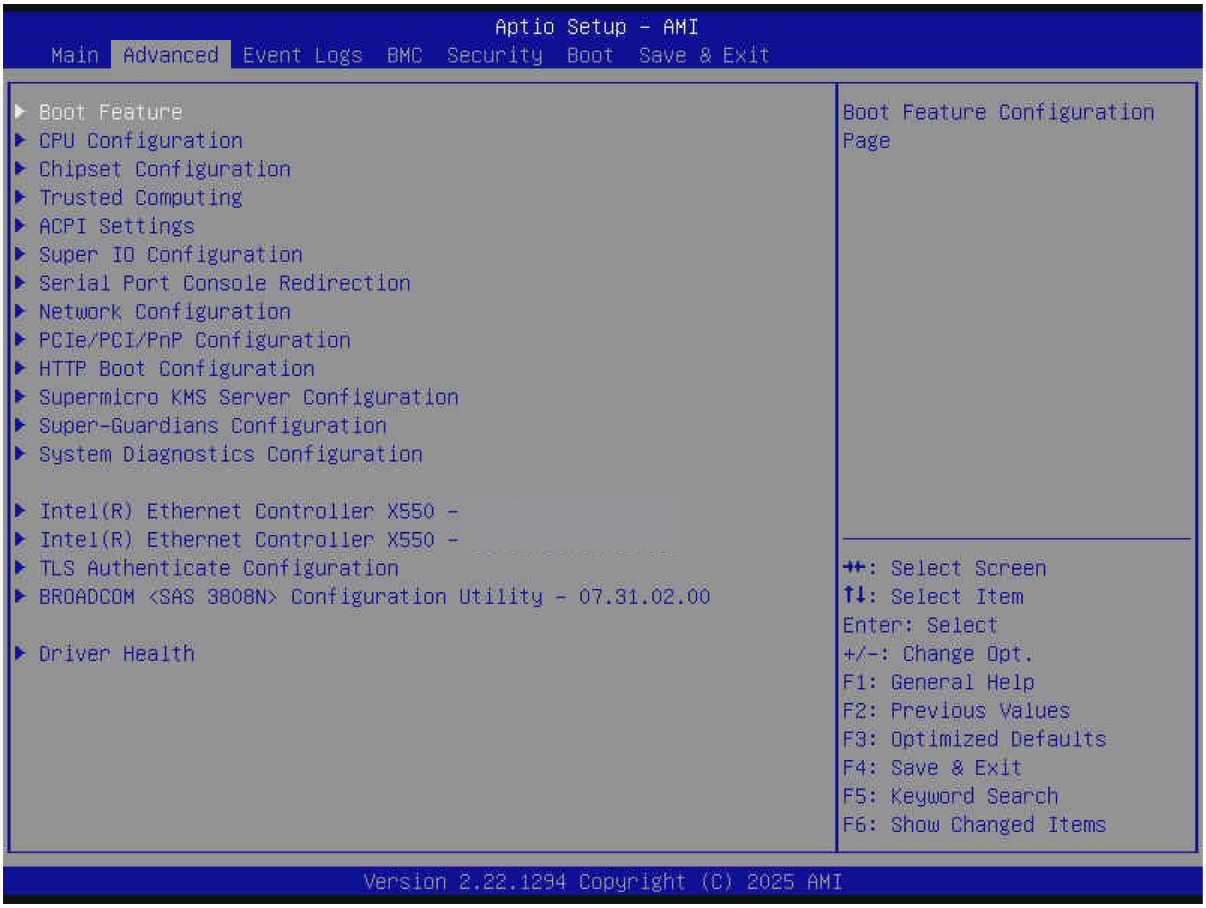


Figure 4-2. Advanced Setup Configurations Screen

Boot Feature Menu

►Boot Feature

Quiet Boot

Use this feature to select the screen between displaying the Power On Self Test (POST) messages or the OEM logo upon bootup. Select Disabled to display the POST messages. Select Enabled to display the OEM logo instead of the normal POST messages. The options

are Disabled and **Enabled**.

Note: BIOS POST messages are always displayed regardless of the setting of this feature.

Bootup NumLock State

Use this feature to set the power on state for the <Num Lock> key. The options are **On** and Off.

Wait For "F1" If Error

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

Re-try Boot

If this feature is set to Enabled, the system BIOS will automatically reboot the system from an Extensible Firmware Interface (EFI) boot device after an initial boot failure. The options are **Disabled** and Enabled.

Runtime Variable Lock

Enable this feature to manage access to non-volatile memory (NVRAM) variables and use specific runtime services with write protection. The options are **Disabled** and Enabled.

Power Configuration

Watch Dog Function

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

Watch Dog Action (Available when "Watch Dog Function" is set to Enabled)

Use this feature to configure the Watchdog timeout setting. The options are **Reset** and NMI.

Restore on AC Power Loss

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

Power Button Function

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

CPU Configuration Menu

►CPU Configuration

Important: Setting the wrong values for the features included in the following sections may cause the system to malfunction.

The following processor information is displayed:

- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM (Per Core)
- L2 Cache RAM (Per Core)
- L3 Cache RAM (Per Package)
- Processor 0 Version

Hyper-Threading [ALL]

Select Enabled to use Intel Hyper-Threading Technology to enhance CPU performance. The options are Disabled and **Enabled**. This feature is CPU-dependent.

Hardware Prefetcher

If this feature is set to Enabled, the hardware prefetcher will prefetch data from the main system memory to Level 2 cache to help expedite the data transaction to enhance memory performance. The options are **Enabled** and Disabled.

Note: This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

Adjacent Cache Prefetch

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

Note: This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

DCU Streamer Prefetcher

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

Note: This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

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 **Enabled** and Disabled.

Note: This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

LLC Prefetch

If this feature is set to Enabled, LLC (hardware cache) prefetching on all threads will be supported. The options are **Disabled** and Enabled. This feature is CPU-dependent.

Note: This feature is NOT available when "Workload Profile" is set to HPC, I/O, or Virtualization.

Homeless Prefetch

Select Enabled for Homeless Prefetch support on all threads, which is an Effective Prefetch Strategy (EPS) used to enhance memory performance by reducing communication overhead, network latency, and the wait time needed for barrier synchronization in memory prefetching commonly associated with the home-based software Distributed Shared Memory (DSM) system. The options are Disabled, Enabled, and **Auto**. Please note that the option of Auto is program-specific. This feature is CPU-dependent.

AMP Prefetch

Select Enabled to use a machine learning algorithm to predict the best L2 prefetcher configuration for the currently running workload. This feature can improve the performance of various general-purpose workloads. The options are Disabled and **Enabled**. This feature is CPU-dependent.

APIC Physical Mode

Use this feature to enable the APIC physical destination mode. The options are **Disabled** and Enabled. (APIC is the abbreviation for Extended Advanced Programmable Interrupt Controller.)

IIO LLC Ways Mask (Hex)

This feature sets a specific temporary register bit mask that is used to control or monitor Last Level Cache (LLC) cache configuration and allocation. The default setting is **0**. (IIO is the abbreviation for Intel I/O.)

TXT Support

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

Note: If this feature is set to Enabled, be sure to disable Device Function On-Hide (EV DFX) support when it is present in the BIOS for the system to work properly.

Intel Virtualization Technology

Select Enabled to enable the Intel Vanderpool Technology for Virtualization platform support, which allows multiple operating systems to run simultaneously on the same computer to maximize system resources for performance enhancement. The options are Disabled and **Enabled**. Changes take effect after you save settings and reboot the system.

Notes:

- This feature is NOT available when "TXT Support" is set to Enabled.
- This feature is NOT available when "Workload Profile" is set to Virtualization.

Enable SMX

Select Enabled to support Safer Mode Extensions (SMX), which provides a programming interface for system software to establish a controlled environment to support the trusted platform configured by the end user and to verify a virtual machine monitor before it is allowed to run. The options are **Disabled** and Enabled.

Note: This feature is available when "TXT Support" is set to Disabled.

PPIN Control

Select Unlock/Enabled to use the Protected Processor Inventory Number (PPIN) in the system. The PPIN is a unique number set for tracking a given Intel Xeon server processor. The options are Lock/Disabled and **Unlock/Enabled**.

AES-NI

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

Advanced Power Management Configuration Menu

►Advanced Power Management Configuration

Latency Optimized Mode

Select Enabled to set the power mode to the latency optimized mode to improve the latency. The options are **Disabled** and Enabled. This feature is motherboard-dependent.

Note: This feature is NOT available when "Workload Profile" is set to HPC or Virtualization.

Workload Profile

Use this feature to select a preconfigured workload profile, which is used to tune the resources in your system. The options are **Disabled**, HPC, I/O, Virtualization, Telco NFVI, Telco NFVI-FP, and Telco FlexRAN. Changes take effect after you save settings and reboot the system. (NFVI is the abbreviation for Network Functions Virtualization Infrastructure. NFVI-FP is the abbreviation for Network Functions Virtualization Infrastructure Forwarding Platform. RAN is the abbreviation for Radio Access Network.)

Note: Select HPC to optimize power performance of High Performance Computing (HPC) workloads for your system running in the HPC environment. Select I/O for I/O intensive workloads to optimize power performance of high volume of data transfers to and from system memory and storage devices or any program. Select Virtualization to optimize power performance of the workload for your system running in the virtualization environment. Select Telco NFVI to optimize power performance of NFVI workloads for your system. Select Telco NFVI-FP to optimize power performance of NFVI-FP workloads for your system. Select Telco FlexRAN to achieve optimal performance with low power consumption for Intel FlexRANTM based implementations.

Power Performance Tuning

This feature allows either operating system (OS) or BIOS to control the EPB. The options are **OS Controls EPB** and BIOS Controls EPB. (PECI is the abbreviation for Platform Environment Control Interface. EPB is the abbreviation for Intel Performance and Energy Bias Hint.)

Note: This feature is available when "Workload Profile" is set to Disabled.

ENERGY_PERF_BIAS_CFG Mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode)

Use this feature to configure the proper operation setting for your machine by achieving the desired system performance level and energy saving (efficiency) level at the same time. Select Maximum Performance to maximize system performance to its highest potential; however, this may consume maximal amount of power as energy is needed to fuel processor operation. Select Performance to enhance system performance; however, this may consume more power as energy is needed to fuel the processors for operation. The options are Extreme Performance, Maximum Performance, Performance, **Balanced Performance**, Balanced Power, Power, and Max Power Efficient. Note that the options of Extreme Performance and Max Power Efficient are motherboard-dependent.

Notes:

- This feature is available when "Power Performance Tuning" is set to BIOS Controls EPB.
- This feature is available when "Workload Profile" is set to Disabled.

CPU P State Control Menu

►CPU P State Control

Note: This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.

Intel SST-PP

Use this feature to choose from two additional Base-Frequency conditions maximum for CPU P State Control. The options are **Auto**, Level 0, Level 1, Level 2, Level 3, and Level 4. The options regarding SST-PP levels are CPU-dependent. (SST-PP is the abbreviation for Speed Select Technology-Performance Profile.)

Notes:

- This feature is available when "SpeedStep (P-States)" is set to Enabled and when the number of SST-PP levels supported by your CPU is no less than two.
- This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

When "SpeedStep (P-States)" is set to Enabled, the information about SST-PP levels supported by your CPU is displayed.

- SST-PP Level
- Capable
- Core Count
- P1 Ratio
- Package TDP (W)
- DTS_Max

SpeedStep (P-States)

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

Note: This feature is available when "Workload Profile" is set to Disabled.

EIST PSD Function

This feature reduces the latency that occurs when one P-state changes to another, thus allowing the transitions to occur more frequently. This will allow for more demand-based P-state switching to occur based on the real-time energy needs of applications so that the power-to-performance balance can be optimized for energy efficiency. The options are **HW_ALL** and SW_ALL.

Notes:

- This feature is available when "SpeedStep (P-States)" is set to Enabled.
- This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

Turbo Mode

Select Enabled to allow the CPU to operate at the manufacturer-defined turbo speed by increasing CPU clock frequency. This feature is available when it is supported by the processors used in the system. The options are Disabled and **Enabled**.

Notes:

- This feature is available when "SpeedStep (P-States)" is set to Enabled.
- This feature is available when "Workload Profile" is set to Disabled.

Hardware PM State Control Menu

►Hardware PM State Control

Notes:

- This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.
- This submenu is NOT available when “Workload Profile” is set to HPC or Virtualization.

Hardware P-States

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

CPU C State Control Menu

►CPU C State Control

Note: This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.

Monitor MWAIT

Select Enabled to support MONITOR and MWAIT, which are two instructions in Streaming SIMD Extension 3 (SSE3) to improve synchronization between multiple threads for CPU performance enhancement. The options are Disabled and **Enabled**.

Note: This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

ACPI C1 Enumeration

Use this feature to select the ACPI C1 state or the ACPI C1e state. The options are C1 and **C1e**. This feature is CPU-dependent. (ACPI is the abbreviation for Advanced Configuration and Power Interface.)

Note: This feature is available when "Workload Profile" is set to Disabled.

ACPI C6x Enumeration

Use this feature to configure C6 state or C6 P-state as ACPI C2 or ACPI C3 state. The options are Disabled, C6 as ACPI C2, C6 as ACPI C3, C6-P as ACPI C2, C6-P as ACPI C3, and **Auto**.

Note: This feature is available when "Workload Profile" is set to Disabled.

Package C State Control Menu

►Package C State Control

Note: This submenu is available when “Power Performance Tuning” is set to BIOS Controls EPB.

Package C State

Use this feature to optimize and reduce CPU package power consumption in the idle mode. Please note that the changes you've made in this setting will affect all CPU cores or the circuits of the entire system. The options are C0/C1 state, C2 state, C6 (non Retention) state, No Limit, and **Auto**.

Note: This feature is NOT available when "Workload Profile" is set to I/O.

LTR IIO Input

Use this feature to set the MSR 1FCh Bit[29]. The options are Take IIO LTR input and **Ignore IIO LTR input**.

CPU1 Core Disable Bitmap Menu

►CPU1 Core Disable Bitmap

Available Bitmap:

This feature displays the available Bitmap[0].

Disable Bitmap:

Enter 0 to enable this feature for CPU Core Bitmap[0]. Enter FFFFFFFFFF to disable CPU Core Bitmap[0]. Please note that the maximum CPU cores are available in each CPU package and at least one core per CPU must be enabled. Disabling all cores is not allowed. The default setting is **0**.

Chipset Configuration Menu

►Chipset Configuration

Important: Setting the wrong values in this section may cause the system to malfunction.

Uncore Configuration Menu

►Uncore Configuration

The following information is displayed.

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

Degrade Precedence

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

Link L0p Enable

Select Enabled for the system BIOS to enable Link L0p support, which allows the CPU to reduce the UPI links from full width to half width in the event when the CPU's workload is low in an attempt to save power. This feature is available for the system that uses Intel processors with UPI technology support. The options are **Disabled**, Enabled, and Auto.

Note: You can change the performance settings for non-standard applications by using this parameter. It is recommended that the default settings be used for standard applications.

Link L1 Enable

Select Enabled for the BIOS to activate Link L1 support, which will power down the UPI links to save power when the system is idle. This feature is available for the system that uses Intel processors with UPI technology support. The options are **Disabled**, Enabled, and Auto.

Note: Link L1 is an excellent feature for an idle system. L1 is used during Package C-States when its latency is hidden by other components during a wakeup.

KTI Prefetch

Keizer Technology Interconnect (KTI) is also known as the Intel Ultra Path Interconnect (UPI) technology. Select Enabled for the KTI prefetcher to preload the L1 cache with data deemed relevant, which allows the memory read to start earlier on a DDR bus in an effort to reduce latency. Select Auto for the KTI prefetcher to automatically preload the L1 cache with relevant data whenever it is needed. The options are Disabled, Enabled, and **Auto**.

IO Directory Cache (IODC)

This feature allows the IODC 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 Disabled, **Auto**, Enable for Remote InvItoM Hybrid Push, Enable for Remote InvItoM AllocFlow, Enable for Remote InvItoM Hybrid AllocNonAlloc, and Enable for Remote InvItoM and Remote WCiLF.

SNC

Sub NUMA Clustering (SNC) is a feature that breaks up the LLC into clusters based on address range. Each cluster is connected to a subset of the memory controller. Enable this feature to improve average latency and reduce memory access congestion for higher performance. The options are Disabled, Enabled, and **Auto**. This feature is CPU-dependent.

Note: This feature is NOT available when "Workload Profile" is set to I/O, Virtualization, or Telco FlexRAN.

XPT Prefetch

XPT Prefetch is a feature that speculatively makes a copy to the memory controller of a read request being sent to the LLC. If the read request maps to the local memory address and the recent memory reads are likely to miss the LLC, a speculative read is sent to the local memory controller. The options are Disabled, Enabled, and **Auto**.

Stale AtoS

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 "Stale AtoS" 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 Disabled, Enabled, and **Auto**.

LLC Dead Line Alloc

Select Enabled to optimally fill the dead lines in the LLC. The options are Disabled, **Enabled**, and Auto.

Memory Configuration Menu

►Memory Configuration

This submenu is used to configure the Integrated Memory Controller (IMC) settings.

Enforce DDR Memory Frequency POR

Select Enforce POR to enforce Plan of Record (POR) restrictions for DDR memory frequency and voltage programming. The options are **Enforce POR**, Enforce Stretch Goals, and Disabled.

Host Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 4800, 5200, 5600, 6000, 6400, and 7200. Note that the available options are CPU-dependent.

Global Scrambling

Select Enabled to enable data scrambling to enhance system performance and data integrity. The options are Disabled and **Enabled**.

Memory Topology Menu

►Memory Topology

This submenu displays the information of onboard memory modules as detected by the BIOS, for example:

P1-DIMMA1: 5600MT/s Hynix SRx8 16GB RDIMM

Memory Map Menu

►Memory Map

Intel(R) Flat Memory Mode Support

Enable this feature to allow hardware-managed data movement between DDR5 and CXL memory, making total memory capacity visible to your system. The options are **Disabled** and Enabled.

DDR CXL Heterogeneous Interleave Support

Select Enabled to support heterogeneous interleaving for physical DDR5 and CXL memory. The options are **Disabled** and Enabled.

Memory RAS Configuration Menu

►Memory RAS Configuration

Use this submenu to configure the memory mirroring, Reliability Availability Serviceability (RAS) settings.

Mirror Mode

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

Note: This feature is available when "UEFI ARM Mirror" is set to Disabled.

Correctable Error Threshold

Use this feature to specify the threshold value for correctable memory-error logging, which sets a limit on the maximum number of events that can be logged in the memory error log at a given time. The default setting is **512**.

Note: This feature is available when "Memory PFA Support" is set to Disabled.

Leaky Bucket Low Bit

Use this feature to set the Low Bit value for the Leaky Bucket algorithm, which is used to check the data transmissions between CPU sockets and the memory controller. The default setting is **12**.

Leaky Bucket High Bit

Use this feature to set the High Bit value for the Leaky Bucket algorithm, which is used to check the data transmissions between CPU sockets and the memory controller. The default setting is **13**.

ADDDC Sparing (Available when populating 1Rx4, 2Rx4, and 4Rx4 DIMMs and when "Memory PFA Support" is set to Disabled)

Select Enabled 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. Note that virtual lockstep mode will only start to work for ADDDC after a faulty DRAM module is spared. The options are Disabled and **Enabled**.

DDR PPR Type

Post Package Repair (PPR) is a new feature available for the DDR4/DDR5 technology. PPR provides additional spare capacity within a DDR4/DDR5 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/DDR5 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 PPR Disabled, **Hard PPR**, and Soft PPR.

Note: This feature is available when "Memory PFA Support" is set to Disabled.

Enhanced PPR

Use this feature to set advanced memory test. Select Enabled to always execute for every boot. The options are **Disabled**, Enabled, and Persistent.

Memory PFA Support (Available when the DCMS key is activated)

Select Enabled to enable memory Predictive Failure Analysis (PFA) support. PFA can be used to avoid uncorrectable faults on the same memory page. The options are **Disabled** and Enabled.

Security Configuration Menu

►Security Configuration

Memory Encryption (TME) [Outputs]

The following information is displayed.

- MSE activation state
- MK-TME activation state
- CI activation state
- Cryptographic Algorithm configured

Memory Encryption (TME) [Inputs]

Memory Encryption (TME)

Select Enabled for Intel Total Memory Encryption (TME) support to enhance memory data security. The options are **Disabled** and Enabled.

Total Memory Encryption Multi-Tenant (TME-MT)

Use this feature to support tenant-provided (SW-provided) keys. The options are **Disabled** and Enabled.

Memory Integrity

Use this feature to enable TME-MT memory integrity protection for memory transactions. The options are **Disabled** and Enabled.

The following information is displayed.

- KEY stock amount
- TME-MT key ID bits

TME Encryption Algorithm

Use this feature to set the TME encryption algorithm. The options are AES-XTS-128 and **AES-XTS-256**.

Trust Domain Extensions (TDX) [Outputs]

The following information is displayed.

- TDX activation state

Trust Domain Extensions (TDX) [Inputs]

Trust Domain Extensions (TDX) (Available when your motherboard supports Intel TDX)

Use this feature to enable Intel Trust Domain Extensions (TDX) technology support to enhance control of data security. The options are **Disabled** and Enabled.

Note: To support TDX features, DIMM population must be symmetric across integrated Memory Controllers (IMCs) and at least eight DIMMs per socket. For each memory controller, populating the first slots (Px-DIMMX1 or DIMMX1 depending on the motherboard design) in all channels is required. Refer to memory population below for your motherboard.

TDX Memory Population for Intel Xeon 6700-Series Processors with E-Cores																	
IMC#	IMC4				IMC3				CPU	IMC1				IMC2			
Channel	DIMMH		DIMMG		DIMMF		DIMME			DIMMA		DIMMB		DIMMC		DIMMD	
	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2		Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1
8	DDR5		DDR5		DDR5		DDR5				DDR5		DDR5		DDR5		DDR5
16	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5		DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5

TDX Memory Population for Intel Xeon 6700/6500-Series Processors with P-Cores																	
IMC#	IMC4				IMC3				CPU	IMC1				IMC2			
Channel	DIMMH		DIMMG		DIMMF		DIMME			DIMMA		DIMMB		DIMMC		DIMMD	
	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2		Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1
8	DDR5		DDR5		DDR5		DDR5				DDR5		DDR5		DDR5		DDR5
12	DDR5		DDR5	DDR5	DDR5		DDR5	DDR5		DDR5	DDR5		DDR5	DDR5	DDR5		DDR5
16	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5		DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5

TDX Secure Arbitration Mode Loader (SEAM Loader) (Available when your motherboard supports Intel TDX and when "Trust Domain Extensions (TDX)" is set to Enabled)

The SEAM Loader (SEAMLDR) is used to load and update Intel TDX modules into the SEAM memory range by verifying the digital signature. The options are **Disabled** and Enabled.

TME-MT/TDX Key Split (Available when "Trust Domain Extensions (TDX)" is set to Enabled)

Use this feature to set the number of bits for TDX. The other bits will be used by TME-MT. The default setting is **1**.

The following information is displayed when "Trust Domain Extensions (TDX)" is set to Enabled.

- TME-MT Keys:
- TDX Keys:

Processor Reserved Memory [Capabilities]

The following information is displayed.

- PRMRR Min Size per domain
- PRMRR Max Size per domain

Processor Reserved Memory [Outputs]

The following information is displayed.

- PRMRR Size per domain
- PRM Size per socket
- PRM Size per system

Software Guard Extensions (SGX) [Outputs]

The following information is displayed when your motherboard supports SGX.

- SGX activation state
- SGX error code [HEX]

Software Guard Extensions (SGX) [Inputs]

The following features are available when your motherboard supports SGX.

Note: To support SGX features, DIMM population must be symmetric across Integrated Memory Controllers (IMCs) and at least eight DIMMs per socket. For each memory controller, populating the first slots (Px-DIMMX1 or DIMMX1 depending on the motherboard design) in all channels is required. Refer to memory population below for your motherboard.

SGX Memory Population for Intel Xeon 6700-Series Processors with E-Cores

IMC#	IMC4				IMC3				CPU	IMC1				IMC2			
Channel	DIMMH		DIMMG		DIMMF		DIMME			DIMMA		DIMMB		DIMMC		DIMMD	
	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2		Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1
8	DDR5		DDR5		DDR5		DDR5				DDR5		DDR5		DDR5		DDR5
16	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5		DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5

SGX Memory Population for Intel Xeon 6700/6500-Series Processors with P-Cores																	
IMC#	IMC4				IMC3				CPU	IMC1				IMC2			
Channel	DIMMH		DIMMG		DIMMF		DIMME			DIMMA		DIMMB		DIMMC		DIMMD	
	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2		Slot2	Slot1	Slot2	Slot1	Slot2	Slot1	Slot2	Slot1
8	DDR5		DDR5		DDR5		DDR5				DDR5		DDR5		DDR5		DDR5
12	DDR5		DDR5	DDR5	DDR5		DDR5	DDR5		DDR5	DDR5		DDR5	DDR5	DDR5		DDR5
16	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5		DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5

SGX Factory Reset

Use this feature to perform an SGX factory reset to delete all registration data and force an Initial Platform Establishment flow. Reboot the system for the changes to take effect. The options are **Disabled** and Enabled.

SW Guard Extensions (SGX)

Use this feature to enable Intel Software Guard Extensions (SGX) support. Intel SGX is a set of extensions that increases the security of application code and data by using enclaves in memory to protect sensitive information. The options are **Disabled** and Enabled.

SGX Package Info In-Band Access

Setting this feature to Enabled is required before the BIOS provides software with the key blobs, which are generated for each CPU package. The options are **Disabled** and Enabled.

SGX PRMRR Size Requested (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Use this feature to set the Processor Reserved Memory Range Register (PRMRR) size. The options are **Auto**, 128M, 256M, 512M, 1G, 2G, 4G, 8G, 16G, 32G, 64G, 128G, 256G, and 512G. Note that the available options are based on your motherboard features, memory size, and memory map.

Select Owner EPOCH Input Type (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Owner EPOCH is used as a parameter to add personal entropy into the key derivation process. A correct Owner EPOCH is required to have access to personal data previously sealed by other platform users. There are two Owner EPOCH modes. One is New Random Owner

EPOCH, and the other is manually entered by the user. Each EPOCH is 64-bit. The options are **SGX Owner EPOCH deactivated**, Change to New Random Owner EPOCHs, and Manual User Defined Owner EPOCHs.

Note: Changing the Owner EPOCH value will lose the data in enclaves.

Software Guard Extensions Epoch 0

Use this feature to enter the EPOCH value. The default setting is **0**.

Note: This feature is available when "SW Guard Extensions (SGX)" is set to Enabled. This feature is NOT available when "Select Owner EPOCH Input Type" is set to SGX Owner EPOCH deactivated.

Software Guard Extensions Epoch 1

Use this feature to enter the EPOCH value. The default setting is **0**.

Note: This feature is available when "SW Guard Extensions (SGX)" is set to Enabled. This feature is NOT available when "Select Owner EPOCH Input Type" is set to SGX Owner EPOCH deactivated.

SGXLEPUBKEYHASHx Write Enable (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Use this feature to enable writes to SGXLEPUBKEYHASH[3..0] from OS/SW. The options are Disabled and **Enabled**. Only those CPUs that support the Intel SGX Flexible Launch Control (FLC) feature have SGXLEPUBKEYHASH, which contains the hash of the public key for the SGX Launch Enclave (LE) to be signed with.

SGXLEPUBKEYHASH0 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 0–7 of SGX Launch Enclave Public Key Hash.

SGXLEPUBKEYHASH1 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 8–15 of SGX Launch Enclave Public Key Hash.

SGXLEPUBKEYHASH2 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 16–23 of SGX Launch Enclave Public Key Hash.

SGXLEPUBKEYHASH3 (Available when both "SW Guard Extensions (SGX)" and "SGXLEPUBKEYHASHx Write Enable" are set to Enabled)

Use this feature to enter the bytes 24–31 of SGX Launch Enclave Public Key Hash.

IIO Configuration Menu

►IIO Configuration

PCIe Completion Timeout

Use this feature to set the PCIe completion timeout. The options are 50us to 50ms, 50us to 100us, 1ms to 10ms, 16ms to 55ms, 65ms to 210ms, **260ms to 900ms**, 1s to 3.5s, and Disabled.

PCIe ASPM Support (Global)

Use this feature to disable the Active State Power Management (ASPM) support for all PCIe root ports. The options are **Disabled** and Auto.

PRM Feature Control

Use this feature to enable the Platform Runtime Mechanism (PRM). The PRM is a mechanism to reduce the System Management Mode (SMM) usages and to provide an alternate means to invoke native code through the Advanced Configuration and Power Interface (ACPI) context of runtime events. The options are **Disabled** and Enabled.

Equalization Bypass To Highest Rate

Set this feature to Enabled to reduce the link training time for PCIe 5.0 device by skipping equalization of intermediate data rates. The options are Disabled and **Enabled**.

NVMe Mode Switch

When this feature is set to Auto, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are Manual, VMD, and **Auto**. This feature is available for configuration when the system supports a VROC key.

PCIe PLL SSC

Select Enabled for PCIe Spread Spectrum Clocking (SSC) support, which allows the BIOS to monitor and attempt to reduce the level of electromagnetic interference caused by the components whenever needed. The options are **Disabled** and Enabled. The available options are CPU-dependent.

Snoop Response Hold Off for PCIe Stack

Use this feature to set the IIO snoop response hold-off value to improve throughput and reduce latency. The default setting is **9**. The valid range is 0 to F. Set this feature to 0 to disable the hold-off time.

CXL Security Level

By defining security protocols, CXL standards provide protection against the data security threats. Use this feature to set the CXL security level for data transiting the CXL link. The options are Fully Trusted, Partially Trusted, Untrusted, and **Auto**.

- Fully Trusted: This option allows the CXL device to access CXL.$ for both host-attached and device-attached memory ranges in the write-back (WB) address space.
- Partially Trusted: This option allows the CXL device to access CXL.$ for device-attached memory ranges only.
- Untrusted: If this option is selected, the host (your system) will abort all requests on CXL.$.
- Auto: This option is based on Si Compatibility.

CXL Header Bypass

Use this feature to enable the CXL header bypass. The options are **Disabled** and Enabled.

CPU1 Configuration Menu

►CPU1 Configuration

►PCI Express 0 / PCI Express 1 / PCI Express 2 / PCI Express 3 / PCI Express 4 / PCI Express 5

Note: The number of PCIe slots and the slot naming can differ depending on the PCIe devices connected to your motherboard.

Intel VMD Technology

When this feature is set to Enabled, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are **Disabled** and Enabled. This feature is available for configuration when the system supports a VROC key.

Notes:

- This feature is available when "NVMe Mode Switch" is set to Manual.
- After you've enabled VMD in the BIOS on a PCIe slot, this PCIe slot will be dedicated for VMD use only, and it will no longer support any PCIe device. To re-activate this slot for PCIe use, disable VMD in the BIOS.

Bifurcation

This feature is CPU-dependent. Use this feature to configure the PCIe Bifurcation setting for the PCIe port you specified. The options are **Auto**, x4x4x4x4, x4x4x8, x8x4x4, x8x8, and x16.

►PCI Express 5 Port A/Port C/Port E/Port G

Note: The number of PCIe slots and the slot naming can differ depending on the PCIe devices connected to your motherboard.

Requested Link Speed

Use this feature to configure the link speed of the PCIe port you specified. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), Gen 3 (8 GT/s), Gen 4 (16 GT/s), and Gen 5 (32 GT/s).

The following information is displayed.

- Max Link Width
- Current Link Width
- Current Link Speed

Data Link Feature Exchange

Use this feature to enable data link feature negotiation in the Data Link Feature Capabilities (DLFCAP) register. The options are Disabled and **Enabled**.

PCIe Port Max Payload Size

Use this feature to configure the maximum payload size supported in PCIe device capabilities register for the device installed in the PCIe port. The options are 128B, 256B, 512B, and **Auto**.

MCTP

Enable this feature, Management Component Transport Protocol (MCTP), to support communications between devices in a platform management subsystem. MCTP's underlying device buses include SMBus/I^2C, serial links, PCIe, and USB. The options are Disabled and **Enabled**.

Equalization Bypass To Highest Rate

Set this feature to Enabled to reduce the link training time for PCIe 5.0 device by skipping equalization of intermediate data rates. The options are Disabled and **Enabled**.

Intel VMD Technology

When this feature is set to Enabled, VMD support will be automatically enabled when a VROC key is detected by the BIOS. The options are **Disabled** and Enabled. This feature is available for configuration when the system supports a VROC key.

Intel VT for Directed I/O (VT-d) Menu

►Intel VT for Directed I/O (VT-d)

Note: This submenu is NOT available when "Workload Profile" is set to Virtualization.

Kernel DMA Protection

Select Enabled to notify OS to enable DMA protection after the system has booted by setting DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR ACPI table. The options are Enabled and **Disabled**. (DMA is the abbreviation for Direct Memory Access. DMAR is the abbreviation for DMA Remapping Reporting.)

Pre-boot DMA Protection

Select Enabled to establish DMA protection during pre-boot processing by setting DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR ACPI table. The options are Enabled and **Disabled**.

PCIe ACSCTL

Select Enabled to program ACS control to Chipset PCIe Root Port bridges. Select Disabled to program ACS control to all PCIe Root Port bridges. The options are Enabled and **Disabled**.

PCIe Leaky Bucket Configuration Menu

►PCIe Leaky Bucket Configuration

Gen2 Link Degradation

Use this feature to enable PCIe Gen2 link degradation. The options are Disabled and **Enabled**.

Note: The default setting is Enabled when your motherboard supports PCIe Gen2 link. Otherwise, the default setting is Disabled.

Gen3 Link Degradation

Use this feature to enable PCIe Gen3 link degradation. The options are Disabled and **Enabled**.

Note: The default setting is Enabled when your motherboard supports PCIe Gen3 link. Otherwise, the default setting is Disabled.

Gen4 Link Degradation

Use this feature to enable PCIe Gen4 link degradation. The options are Disabled and **Enabled**.

Note: The default setting is Enabled when your motherboard supports PCIe Gen4 link. Otherwise, the default setting is Disabled.

Gen5 Link Degradation

Use this feature to enable PCIe Gen5 link degradation. The options are Disabled and **Enabled**.

Note: The default setting is Enabled when your motherboard supports PCIe Gen5 link. Otherwise, the default setting is Disabled.

Trusted Computing Menu

►Trusted Computing

When the TPM 2.0 (either onboard or external) is detected by your system, the following information is displayed.

- TPM 2.0 Device Found
- Firmware Version:
- Vendor:

Note: This submenu is available when the TPM 2.0 (either onboard or external) is detected by the BIOS.

Security Device Support

Select Enabled to enable BIOS support for onboard security devices, which are not displayed in the OS. If this feature is set to Enabled, TCG EFI protocol and INT1A interface will not be available. The options are Disabled and **Enabled**.

When "Security Device Support" is set to Enabled and the TPM 2.0 (either onboard or external) is detected by the BIOS, the following information is displayed.

- Active PCR banks
- Available PCR banks

Note: The following features are available when the TPM 2.0 (either onboard or external) is detected by the BIOS.

SHA256 PCR Bank (Available when "Security Device Support" is set to Enabled)

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

SHA384 PCR Bank (Available when "Security Device Support" is set to Enabled)

Select Enabled to enable SHA384 PCR Bank support to enhance system integrity and data security. The options are **Disabled** and Enabled.

Pending Operation (Available when "Security Device Support" is set to Enabled)

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

Note: If this feature is used, your system will reboot to carry out a pending TPM operation.

Platform Hierarchy (Available when "Security Device Support" is set to Enabled)

Select Enabled for TPM Platform Hierarchy support, which allows 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 the TPM (either onboard or external). The options are Disabled and **Enabled**.

Storage Hierarchy (Available when "Security Device Support" is set to Enabled)

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

Endorsement Hierarchy (Available when "Security Device Support" is set to Enabled)

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

PH Randomization

Select Enabled for Platform Hierarchy (PH) 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.

Supermicro BIOS-Based TPM Provision Support

Set this feature to Enabled to unlock the TPM. Save settings and exit the BIOS Setup utility. The Non-volatile (NV) indexes can be deleted after the system reboot. The options are **Disabled** and Enabled.

ACPI Settings Menu

►ACPI Settings

Virtual NUMA

Enable this feature to optimize the memory-access performance for VMware virtual machines. The options are **Disabled** and Enabled.

Note: This feature is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

Number of Virtual NUMA Nodes (Available when "Virtual NUMA" is set to Enabled)

This feature displays the number of virtual NUMA nodes. A NUMA architecture divides hardware resources (including processors, memory, and I/O buses) into groups, called NUMA nodes. This feature indicates the available number of virtual NUMA nodes that can be assigned to the virtual machine. By default, this setting is automatically adjusted to match the physical NUMA topology.

WHEA Support

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

Super IO Configuration Menu

►Super IO Configuration

The following information is displayed.

- Super IO Chip

Note: This submenu is available when your system supports this feature.

Serial Port 1 Configuration Menu

►Serial Port 1 Configuration

Serial Port 1

Select Enabled to enable serial port 1. The options are Disabled and **Enabled**.

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

This feature displays the base I/O port address and the Interrupt Request address of serial port 1.

Change Settings (Available when "Serial Port 1" above is set to Enabled)

Use this feature to specify 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 serial port 1. The options are **Auto**, (IO=3F8h; IRQ=4;), (IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

Serial Port 2 Configuration Menu

►Serial Port 2 Configuration

Note: It can be "Serial Port 2 Configuration" or "SOL Configuration" based on your system support.

Serial Port 2/SOL ("Serial Port 2" or "SOL" based on your system support)

Select Enabled to enable serial port 2 (or SOL). The options are Disabled and **Enabled**.

Device Settings (Available when "Serial Port 2/SOL" above is set to Enabled)

This feature displays the base I/O port address and the Interrupt Request address of serial port 2 (or SOL).

Change Settings (Available when "Serial Port 2/SOL" above is set to Enabled)

Use this feature to specify the base I/O port address and the Interrupt Request address of serial port 2 (or SOL). Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 2 (or SOL).

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

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

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

Serial Port Console Redirection Menu

►Serial Port Console Redirection

COM1 (Available when your system supports the serial port of COM1)

Console Redirection

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

Note: This feature will be set to Enabled if there is no BMC support.

SOL/COM2

Note: This feature is available when your system supports serial port of SOL and/or COM2. The "SOL/COM2" here indicates a shared serial port, and SOL is used as the default.

Console Redirection

Select Enabled to use the SOL/COM2 port for Console Redirection. The options are Disabled and **Enabled**.

►Console Redirection Settings

Note: This submenu is available when "Console Redirection" for COM1 or SOL/COM2 is set to Enabled.

Terminal Type

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

Bits Per Second

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

Data Bits

Use this feature to set the data transmission size for Console Redirection. The options are 7 and **8** (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 1s in data bits is even. Select Odd if the parity bit is set to 0 and the number of 1s in data bits is odd. Select None if you do not want to send a parity bit with your data bits in transmission. Select Mark to add a mark as a parity bit to be sent along with the data bits. Select Space to add a space as a parity bit to be sent with your data bits. The options are **None**, Even, Odd, Mark, and Space.

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

Use this feature to select the function key and keypad settings on Putty, which is a terminal emulator designed for the Windows OS. The options are **VT100**, LINUX, XTERMR6, SCO, ESCN, and VT400.

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

Use the features below to configure Console Redirection settings to support Out-of-Band Serial Port management.

Console Redirection EMS

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

►Console Redirection Settings

Note: This submenu is available when "Console Redirection EMS" is set to Enabled.

Out-of-Band Mgmt Port

Use this feature to select a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2. Note that the option of SOL/COM2 indicates a shared serial port. SOL is available with BMC support.

Terminal Type EMS

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

Bits Per Second EMS

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

Flow Control EMS

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffer overflow. Send a "Stop" signal to stop sending data when the receiving buffer is full. Send a "Start" signal to start sending data when the receiving buffer is empty. The options

are **None**, Hardware RTS/CTS, and Software Xon/Xoff.

The following information is displayed.

- **Data Bits EMS**
- **Parity EMS**
- **Stop Bits EMS**

Network Stack Configuration Menu

►Network Stack Configuration

Network Stack

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

IPv4 PXE Support (Available when "Network Stack" is set to Enabled)

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 (Available when "Network Stack" is set to Enabled)

Select Enabled to enable IPv4 HTTP boot support. If this feature is disabled, it will not create the IPv4 HTTP boot option. The options are **Disabled** and Enabled.

IPv6 PXE Support (Available when "Network Stack" is set to Enabled)

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 (Available when "Network Stack" is set to Enabled)

Select Enabled to enable IPv6 HTTP boot support. If this feature is disabled, it will not create the IPv6 HTTP boot option. The options are **Disabled** and Enabled.

PXE Boot Wait Time (Available when "Network Stack" is set to Enabled)

Use this feature to set the wait time (in seconds) upon which the system BIOS will wait for you to press the <ESC> key to abort PXE boot instead of proceeding with PXE boot by connecting to a network server immediately. Press the <+> or <-> key on your keyboard to change the value. The default setting is **0**.

Media Detect Count (Available when "Network Stack" is set to Enabled)

Use this feature to set the wait time (in seconds) for the BIOS ROM to detect the presence of a LAN media either via the Internet connection or via a LAN port. Press the <+> or <-> key on your keyboard to change the value. The default setting is **1**.

MAC:(MAC address)-IPv4 Network Configuration Menu

►MAC:(MAC address)-IPv4 Network Configuration

Configured

Enable this feature to configure network addresses for DHCP, local IP address, local netmask, local gateway, and local DNS server. The options are **Disabled** and Enabled.

Enable DHCP (Available when "Configured" is set to Enabled)

Select Enabled to support Dynamic Host Configuration Protocol (DHCP), which allows the BIOS to search for a DHCP server attached to the network and request the next available IP address for this computer. The options are **Disabled** and Enabled.

Local IP Address (Available when "Configured" is set to Enabled and "Enable DHCP" is set to Disabled)

Use this feature to enter an IP address for the local machine.

Local NetMask (Available when "Configured" is set to Enabled and "Enable DHCP" is set to Disabled)

Use this feature to set the netmask for the local machine.

Local Gateway (Available when "Configured" is set to Enabled and "Enable DHCP" is set to Disabled)

Use this feature to set the gateway address for the local machine.

Local DNS Servers (Available when "Configured" is set to Enabled and "Enable DHCP" is set to Disabled)

Use this feature to set the Domain Name System (DNS) server address for the local machine.

Save Changes and Exit

Press <Enter> to save changes and exit.

MAC:(MAC address)-IPv6 Network Configuration Menu

►MAC:(MAC address)-IPv6 Network Configuration

►Enter Configuration Menu

The following information is displayed.

- Interface Name
- Interface Type
- MAC address

- Host address
- Route Table
- Gateway addresses
- DNS addresses

Interface ID

Use this feature to change/enter the 64-bit alternative interface ID for the device. The string format is colon separated. The default setting is the MAC address above.

DAD Transmit Count

Use this feature to set the number of consecutive neighbor solicitation messages that have been sent while performing duplicate address detection on a tentative address. The default setting is **1**.

Policy

Use this feature to select how the policy is to be configured. The options are **automatic** and manual.

►Advanced Configuration

Note: This submenu is available when "Policy" is set to manual.

New IPv6 address: Use this feature to enter the IPv6 address for the local machine.

New Gateway addresses: Use this feature to set the gateway address for the local machine.

New DNS addresses: Use this feature to set the DNS server address for the local machine.

Commit Changes and Exit: Press <Enter> to save changes and exit.

Discard Changes and Exit: Press <Enter> to discard changes and exit.

Save Changes and Exit

Press <Enter> to save changes and exit.

PCIe/PCI/PnP Configuration Menu

►PCIe/PCI/PnP Configuration

The following information is displayed.

- PCI Bus Driver Version

PCI Devices Common Settings:

Re-Size BAR Support

Use this feature to enable the Resizable BAR support. Resizable BAR is a PCIe interface technology that allows the CPU to access the entire frame buffer. With this technology, your system will be able to handle multiple CPU to GPU transfers simultaneously rather than queuing, which can improve the frame rate performance. The options are **Disabled** and Enabled.

SR-IOV Support (Unavailable when "Workload Profile" is set to Virtualization)

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

ARI Support

Select Enabled for Alternative Routing- ID Interpretation (ARI) support. The options are Disabled and **Enabled**.

MMCFG Base

This feature determines how the lowest Memory Mapped Configuration (MMCFG) base is assigned to onboard PCI devices. The options are 1G, 1.5G, 1.75G, 2G, 2.25G, 3G, and **Auto**. The options of 2G and 2.25G are not available when the MMCFG size is 2G. The option of 3G is not available when the MMCFG size is 1G or 2G.

MMCFG Size

Use this feature to set the MMCFG size. The options are 64M, 128M, 256M, 512M, 1G, 2G, and **Auto**. Note that the MMCFG size is based on the memory populated.

MMIO High Base

Use this feature to select the base memory size according to memory-address mapping for the I/O hub. The options are 248T, 120T, 88T, 60T, 30T, 56T, 40T, 32T, 24T, 16T, 4T, 2T, 1T, 512G, 3584T, and **Auto**. The options of 248T, 120T, 88T, 60T, 30T, and 3584T are CPU-dependent.

MMIO High Granularity Size

Use this feature to select the high memory size according to memory-address mapping for the I/O hub. The options are 1G, 4G, 16G, 32G, 64G, 256G, and **1024G**. This feature is motherboard-dependent.

Bus Master Enable

If this feature is set to Enabled, the PCI Bus Driver will enable the Bus Master Attribute for DMA transactions. If this feature is set to Disabled, the PCI Bus Driver will disable the Bus Master Attribute for Pre-Boot DMA protection. The options are Disabled and **Enabled**.

NVMe Firmware Source

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

VGA Priority

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

Onboard Video Option ROM

Select EFI to boot the computer using the Extensible Firmware Interface (EFI) device installed on the onboard video port. The options are Disabled and **EFI**.

AOC-ATG-i2S LAN1 OPROM / Onboard SAS Option ROM / Onboard LAN1 Option ROM / Onboard NVMe1 Option ROM – Onboard NVMe24 Option ROM

Select EFI to boot the computer using the EFI device installed on the PCIe slot specified. The options are Disabled and **EFI**.

Note: The number of slots and slot naming vary based on your motherboard features.

HTTP Boot Configuration Menu

►HTTP Boot Configuration

HTTP Boot Policy

Use this feature to set the HTTP boot policy. The options are Apply to all LANs, **Apply to each LAN**, and Boot Priority #1 instantly.

HTTPS Boot Checks Hostname

Important: Disabling "HTTPS Boot Checks Hostname" is a violation of RFC 6125 and may expose you to Man-in-the-Middle Attacks. Supermicro is not responsible for any and all security risks incurred by you disabling this feature.

Enable this feature for HTTPS boot to check the hostname of the TLS certificates to see if it matches the host name provided by the remote server. The options are **Enabled** and Disabled (WARNING: Security Risk!!).

Priority of HTTP Boot

Instance of Priority 1: (Available when your motherboard supports this feature)

This feature sets the rank target port. The default setting is **1**.

Select IPv4 or IPv6

This feature specifies which connection the target LAN port should boot from. The options are **IPv4** and IPv6.

Boot Description

Use this feature to enter a boot description, which cannot be longer than 75 characters. Be sure to enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI

Enter a Boot Uniform Research Identifier (URI) with 128 characters or shorter. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created.

Instance of Priority 2: (Available when your motherboard supports this feature)

This feature sets the rank target port. The default setting is **0**.

Select IPv4 or IPv6 (Unavailable when "Instance of Priority 2:" above is set to 0)

This feature specifies which connection the target LAN port should boot from. The options are **IPv4** and IPv6.

Boot Description (Unavailable when "Instance of Priority 2:" above is set to 0)

Use this feature to enter a boot description, which cannot be longer than 75 characters. Please be sure to enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI (Unavailable when "Instance of Priority 2:" above is set to 0)

Enter a Boot URI with 128 characters or shorter. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created.

Supermicro KMS Server Configuration Menu

►Supermicro KMS Server Configuration

Note: Be sure to configure all the features in the submenu of Supermicro KMS Server Configuration and the feature of "KMS Security Policy" in the submenu of Super-Guardians Configuration so that your system can communicate with the KMS server.

TPM-KMS Support

This feature combines the capabilities of a hardware-based security module (TPM) with the Key Management Service (KMS) to enhance security by managing cryptographic keys and ensuring secure access to sensitive data. The options are **Disabled** and Enabled.

Supermicro KMS Server IP address

Use this feature to set the Supermicro KMS server IPv4 address in dotted-decimal notation.

Second Supermicro KMS Server IP address

Use this feature to set the second Supermicro KMS server IPv4 address in dotted-decimal notation.

Supermicro KMS TCP Port number

Use this feature to set the TCP port number used in the Supermicro KMS server. The valid range is 100–9999. The default setting is **5696**. Do not change the default setting unless a different TCP port number has been specified and used in the Supermicro KMS server.

KMS Time Out

Use this feature to enter the KMS server connecting time-out (in seconds). The default setting is **5** (seconds).

TimeZone

Use this feature to set the correct time zone. The default setting is **0** (not specified).

Client UserName

Press <Enter> to set the client identity (UserName). The length is 0–63 characters.

Client Password

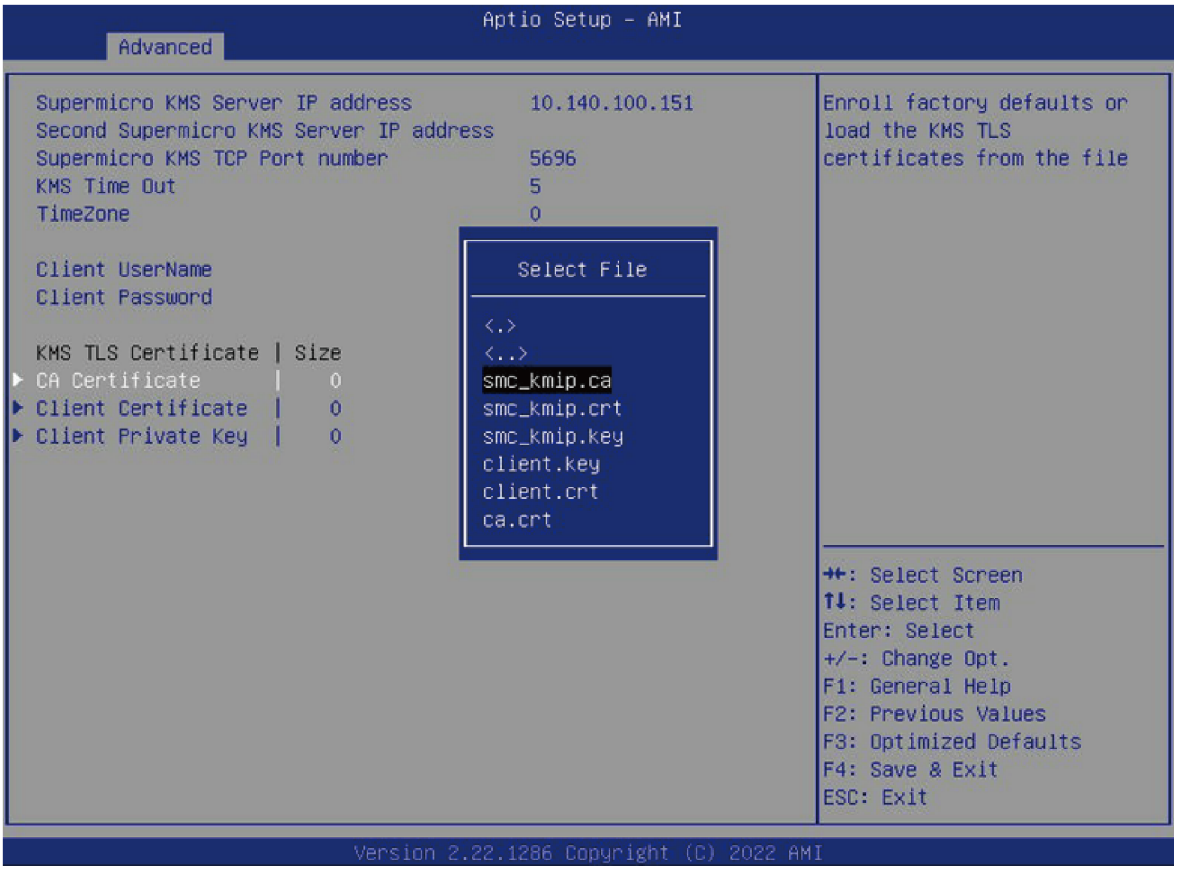
Press <Enter> to set the client identity (Password). The length is 0–31 characters.

►CA Certificate

►Client Certificate

►Client Private Key

Use the three features above to enroll factory defaults or load the KMS Transport Layer Security (TLS) certificates, which are generated by the KMS server, from the file stored in the USB flash drive as shown below.



Private Key Password (Available when "Client Private Key" above has been set)

Use this feature to change the private key password.

Super-Guardians Configuration Menu

►Super-Guardians Configuration

Super-Guardians Protection Policy

Use this feature to enable the Super-Guardians Protection Policy. The options are **Storage**, System, and System and Storage. Set this feature to Storage to protect and have secure access to the Trusted Computing Group (TCG) NVMe devices with the Authentication-Key (AK). Set this feature to System to protect and have secure access to your system/motherboard with the AK. Set this feature to System and Storage to protect and have secure access to your system/motherboard/storage devices with the AK.

KMS Security Policy (Available when "TPM Security Policy" and "USB Security Policy" are set to Disabled)

Set this feature to Enabled to enable the KMS Security Policy. When this feature has not previously been set to Enabled, the options are **Disabled** and Enabled. Changes take effect after you save settings and reboot the system.

When this feature has previously been set to Enabled, the options are **Enabled**, Reset, and Key Rotation. Set this feature to Key Rotation to obtain an existing AK from the KMS server and create a new AK. To disable the KMS Security Policy, set this feature to Reset. When this feature is set to Reset, the system and TCG NVMe devices chosen in "Super-Guardians Protection Policy" will be in the unprotected mode.

Notes:

- Be sure that the KMS server is ready before configuring this feature.
- Use the professional KMS server solutions (e.g., Thales Server) or the Supermicro PyKMIP Software Package to establish the KMS server.

KMS Server Retry Count (Available when "TPM Security Policy" and "USB Security Policy" are set to Disabled)

Use this feature to specify how many times the system will attempt reconnecting to the KMS server. The valid range is 0–10. Press the <+> or <-> key on your keyboard to change the value. The default setting is **5**. If the value is 0, the system will retry infinitely.

TPM Security Policy (Available when "KMS Security Policy" and "USB Security Policy" are set to Disabled)

Set this feature to Enabled to enable the TPM Security Policy. When this feature has not previously been set to Enabled, the options are **Disabled** and Enabled. Changes take effect after you save settings and reboot the system.

When this feature has previously been set to Enabled, the options are **Enabled**, Reset, and Key Rotation. To disable the TPM Security Policy, set this feature to Reset. When this feature is set to Reset, the system and TCG NVMe devices chosen in "Super-Guardians Protection Policy" will be in the unprotected mode.

Note: The TPM 2.0 (either onboard or external) is required to configure this feature.

Load Authentication-Key (Available when "KMS Security Policy," "TPM Security Policy," and "USB Security Policy" are set to Disabled)

Use this feature to load the Authentication-Key. The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save settings and reboot the system. While booting, the BIOS will automatically load the Authentication-Key (filename: TPMAuth.bin) from the USB flash drive. Afterwards, the default setting will be set to Disabled by the BIOS.

Notes:

- Be sure to connect a USB flash drive with the Authentication-Key (filename: TPMAuth.bin) to your system before the system reboot.
- Be sure to save the Authentication-Key (filename: TPMAuth.bin) to the USB flash drive and keep a backup. Load the Authentication-Key (filename: TPMAuth.bin) after the TPM (either onboard or external) is detected by your system. Otherwise, the TPM function can not work properly.

Save Authentication-Key (Available when "TPM Security Policy" is set to Enabled)

Use this feature to save the Authentication-Key. The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save settings and reboot the system. While booting, the BIOS will automatically save the Authentication- Key (filename: TPMAuth.bin) to the USB flash drive. Afterwards, the default setting will be set to Disabled by the BIOS.

Note: Be sure to connect a USB flash drive to your system before the system reboot.

USB Security Policy (Available when "KMS Security Policy" and "TPM Security Policy" are set to Disabled)

Use this feature to enable the USB Security Policy. The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save settings and reboot the system. Connect a USB flash drive to your system before the system reboot. While booting, the BIOS will automatically create the USB Authentication-Key (filename: USBAuth.bin) and save it to the USB flash drive.

When this feature has been previously set to Enabled, the options are **Enabled** and Reset. To disable the USB Security Policy, set this feature to Reset. When this feature is set to Reset, the system and TCG NVMe devices chosen in "Super-Guardians Protection Policy" will be in the unprotected mode.

Note: Be sure to connect a USB flash drive to your system before configuring this feature. Save the USB Authentication-Key (filename: USBAuth.bin) to the USB flash drive and keep a backup.

System Diagnostics Configuration Menu

►System Diagnostics Configuration

Launch System Diagnostics

Set this feature to Launch Once to launch system diagnostics on next system boot. The options are **Disabled** and Launch Once.

Note: Pressing <F7> during system bootup can also launch system diagnostics.

Intel(R) Ethernet Controller Menu

►Intel(R) Ethernet Controller (Ethernet controller) - (MAC address)

Notes:

- The Ethernet controller and MAC address shown above are based on your system features.
- This submenu is available when the LAN Option ROM type is EFI.

►NIC Configuration

Link Speed

Use this feature to set the connection speed of a selected LAN port. The options are **Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, and 100 Mbps Full.

Wake On LAN

Set this feature to support system wake-up via the selected LAN port. If this feature is set to Enabled, the LAN port selected will be enabled when the system is powered on. The options are Disabled and **Enabled**.

LLDP Agent

Use this feature to enable or disable Link Layer Discovery Protocol (LLDP) agent support on a long-term basis. The LLDP, a vendor-neutral link layer protocol, is used by a network device to identify itself and announce its capability to the neighboring devices in a network environment for networking. When disabling the LLDP agent in the firmware, the function of Data Center Bridging (DCB) will also be disabled. The options are Disabled and **Enabled**.

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LEDs. The default setting is **0** (up to 15 seconds).

The following information is displayed.

- UEFI Driver
- Adapter PBA
- Device Name
- Chip Type
- PCI Device ID
- PCI Address
- Link Status
- MAC Address
- Virtual MAC Address

System Diagnostics Configuration Menu

►System Diagnostics Configuration

Launch System Diagnostics

Set this feature to Launch Once to launch system diagnostics on next system boot. The options are **Disabled** and Launch Once.

Note: Pressing <F7> during system bootup can also launch system diagnostics.

TLS Authenticate Configuration Menu

►TLS Authenticate Configuration

Use this submenu to configure Transport Layer Security (TLS) settings.

►Server CA Configuration

Use this feature to configure the client certificate that is to be used by the server.

►Enroll Certification

Use this feature to enroll the certificate in the system.

►Enroll Certification Using File

Use this feature to enroll the security certificate in the system by using a file.

►Commit Changes and Exit

Use this feature to save all changes and exit TLS settings.

►Discard Changes and Exit

Use this feature to discard all changes and exit TLS settings.

►Delete Certification

Use this feature to delete the certificate if a certificate has been enrolled in the system.

►Client Certification Configuration

BROADCOM <SAS 3808N> Configuration Utility

►BROADCOM <SAS 3808N> Configuration Utility

Use this menu to manage the RAID controller configurations.

Main Menu

►Main Menu

Use this menu to view Configuration Management, Controller Management, Virtual Drive Management, Drive Management and Hardware Components.

Configuration Management

►Configuration Management

This menu displays configuration options, some of which will only appear if the controller supports them.

Create Virtual Drive

►Create Virtual Drive

Use this menu to create a virtual drive.

►Save Configuration

Press the <Enter> key to save the configuration.

Select RAID Level

This feature allows you to select a RAID level. The options are **RAID0**, RAID1, and RAID00.

Secure Virtual Drive

Unmap Capability

This feature allows you to enable or disable the unmap capability for the virtual drive. The options are Enabled and **Disabled**.

Select Drives From

Use this feature to select drives from Unconfigured Capacity or Free Capacity. The options are **Unconfigured Capacity** and Free Capacity.

CONFIGURE VIRTUAL DRIVE PARAMETERS:

Virtual Drive Name

Enter a name for the virtual drive.

Virtual Drive Size

This displays the amount of storage space on the virtual drive.

Virtual Drive Size Unit

This displays the unit of which the size is measured by.

Strip Size

This feature allows you to select the strip size or the virtual drive. The default option is **64 KB**.

Read Policy

Write Policy

I/O Policy

Access Policy

Use this feature to select the access policy for the virtual drive. The option are **Read/Write**, Read Only, and Blocked.

Drive Cache

Use this feature to select the virtual drive's cache setting. The options are **Unchanged**, Enable, and Disable.

Disable Background Initialization

This feature allows you to allow disabling of the background initialization. No enables the background initialization and Yes disables the background Initialization. The options are **No** and Yes.

Default Initialization

This feature allows you to choose the default for initialization. The options are **No**, Fast, and Full.

Emulation Type

This feature allows you to choose an emulation type. The options are **Default**, Disable, and Force.

►Save Configuration

Press the <Enter> key to save the configuration.

Create Profile Based Virtual Drive

►Create Profile Based Virtual Drive

This menu allows you to create a virtual drive through a wizard.

Generic RAID 0

►Generic RAID 0

This menu provides information on generic RAID 0, which uses drive striping to store data across multiple disks.

Drive Selection Criteria

This allows you to select a drive.

PROFILE PARAMETERS:

The following information is displayed:

- Virtual Drive Name
- RAID Level
- Virtual Drive Size
- Strip Size
- Read Policy
- Write Policy
- IO Policy
- Drive Cache
- Default Initialization

►Save Configuration

Press the <Enter> key to save the configuration.

Generic RAID 1

►Generic RAID 1

This menu provides information on generic RAID 1, which is drive mirroring that information can be simultaneously written to more than one drive.

Drive Selection Criteria

This allows you to select a drive.

PROFILE PARAMETERS:

The following information is displayed:

- Virtual Drive Name
- RAID Level
- Virtual Drive Size
- Strip Size
- Read Policy
- Write Policy
- IO Policy
- Drive Cache
- Default Initialization

►Save Configuration

Press the <Enter> key to save the configuration.

Clear Configuration

►Clear Configuration

This feature deletes all existing configurations on the RAID controller and discards the pinned cache on missing configuration.

Clear Configuration will delete all of the Virtual Drives, Hot Spare Drives, Pinned Cache and JBODs (if applicable) attached to this controller.

Are you sure you want to clear the configuration?

Confirm

Use this feature to confirm you want to clear the configuration. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

►No

Press <Enter> to return to the main menu.

Controller Management

►Controller Management

Use this menu to view the controller status and basic properties of the controller.

BASIC PROPERTIES:

The following information is displayed:

- Product Name
- Serial Number
- Controller Status
- Personality Mode
- Select Boot Device
- PCI ID
- PCI Segment:Bus:Device:Function
- PCI Slot Number
- Package Version
- Firmware Version
- NVDATA Version
- Supported Device Interfaces
- Drive Count
- JBOD Count
- Virtual Drive Count

Advanced Controller Management

►Advanced Controller Management

Use this menu to modify various controller management activities.

Clear Controller Events

►Clear Controller Events

Use this menu to delete all of the existing controller events.

Are you sure you want to clear the controller events?

Confirm

Use this feature to confirm whether you want to clear all controller events. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

Save Controller Events

►Save Controller Events

Use this menu to save all of the existing controller events.

Save TTY Log

►Save TTY Log

This menu allows you to save a copy of the controller's firmware terminal log entries. The Diagnostics report includes this information.

Enable Drive Security

►Enable Drive Security

Use this menu to activate the controller's drive security.

CHOOSE THE SECURITY KEY MANAGEMENT MODE:

External Key Management (EKM)

Local Key Management (LKM)

This mode provides key management using keys within the controller itself. This mode does not require any external entity. Local Key Management is preferred in deployments that involve fewer systems. The options are Disabled and **Enabled**.

OK

Press the <Enter> key to proceed with the selected security key management option.

►Cancel

This cancels the chosen drive security mode operation.

Disable Drive Security

►Disable Drive Security

Disable Drive Security

►Disable Drive Security

Manage SAS Storage Link Speed

►Manage SAS Storage Link Speed

Use this menu to manage the SAS storage link speed.

VIEW THE PHY SETTINGS FOR THE CONTROLLER AND CHANGE THEM IF NEEDED:

Phy# 00, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 01, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 02, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 03, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 04, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 05, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 06, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 07, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

►OK

Press the <Enter> key to commit to the changes.

►Cancel

Press the <Enter> key to cancel the changes.

Manage PCIe Storage Interface

►Manage PCIe Storage Interface

Use this menu to manage the controller's link width and lane speed.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

VIEW LINK WIDTH AND CHANGE THEM IF NEEDED:

Link Width for C0, C1, C2, C3

Use this feature to select the desired link width (if supported). The options are 0–3:x3, 4–7:x4, **0–1:x2, 2–3:x2, 4–5:x2, 6–7:x2**, and 0:x1, 1:x1, 2:x1, 3:x1, 4:x1, 5:x1, 6:x1, 7:x1.

Important: If the speed for some of the lanes that are participating in the same link are configured differently, then the lowest speed will be used by the link. Recommendation: Choose the same speed for all lanes that belong to the same link.

VIEW THE LANE SPEED AND CHANGE THEM IF NEEDED:

Lane# 00, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 01, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 02, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 03, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 04, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 05, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 06, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 07, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Manage MegaRAID Advanced Software Options

►Manage MegaRAID Advanced Software Options

This menu enables you set the controller's MegaRAID Advanced Software Options. This menu also shows the Advanced Software Options that are active on the controller.

MegaRAID SafeStore (Unlimited)

MegaRAID FastPath (Unlimited)

The following information is displayed:

- SAFE ID
- Serial Number

Activation Key

Enter a 40 alpha-numeric character value.

►Activate

Press <Enter> to see a summary and activate the advanced software options.

►Deactivate All Trial Software

Schedule Consistency Check

►Schedule Consistency Check

This menu allows you to schedule a Consistency Check (CC) operation.

Consistency Check Frequency

Use this feature to select the frequency of the consistency check runs. The options are Disable, Hourly, Daily, **Weekly**, and Monthly.

Consistency Check Start Date

Use this feature to set the start date for the consistency check operation. Enter the date in the format of MM/DD/YYYY.

Consistency Check Start Time

Use this feature to set the consistency check start time. Enter the time in the format of HH:MM:SS.

Consistency Check Mode

Use this feature to select the consistency check mode. Sequential checks the virtual drives one at a time. **Concurrent** checks all of the selected virtual drives simultaneously.

Start Immediately

SELECT VIRTUAL DRIVES TO CHECK:

►Exclude Virtual Drives

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Set Factory Defaults

►Set Factory Defaults

Use this menu to restore the controller settings to factory defaults.

Are you sure you want to reset the controller settings to factory defaults?

Confirm

Use this feature to confirm whether you want to reset the controller settings to factory defaults. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

►No

Press <Enter> to return to the main menu.

Manage Personality Mode

►Manage Personality Mode

Use this menu to change the controller's parameters and personality.

The following information is displayed:

- Personality Mode

Manage Controller Profiles

►Manage Controller Profiles

Use this menu to view the controller's profile information and to choose a profile.

The following information is displayed:

- Number of Profiles

Choose Profile

Use this feature to select the desired controller profile.

DETAILS OF THE PROFILE:

The following information is displayed:

- Personality Mode
- Profile ID
- Default Profile
- Compatible
- Max PD Count
- Max VD Count
- Max NVMe Count

►Set Profile

Manage Phy State

►Manage Phy State

Use this menu to modify the phy state to enabled or disabled.

VIEW THE PHY SETTINGS FOR THE CONTROLLER AND CHANGE THEM IF NEEDED.

Phy# 00 / Phy# 01 / Phy# 03 / Phy# 04 / Phy# 05 / Phy# 06 / Phy# 07

Use this feature to enable or disable the phy state. The options are **Disabled** and Enabled.

►OK

Press the <Enter> key to commit to the changes.

►Cancel

Press the <Enter> key to cancel the changes.

Advanced Controller Properties

►Advanced Controller Properties

This menu allows you to view and modify advanced controller properties.

CONTROLLER PROPERTIES:

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Auto Import Foreign Configuration

Enabling this feature allows automatic import of foreign configurations without you needing to intervene. The options are **Enabled** and Disabled.

Coercion Mode

Use this feature to set the drive coercion mode. The options are **None**, 128 MB, and 1 GB.

Boot Mode

Use this feature to set how to handle errors that may occur during boot time. The options are Stop on errors, **Pause on errors**, Ignore errors, and Safe mode on errors.

Controller BIOS

Use this feature to enable or disable the controller BIOS. The options are **Enabled** and Disabled.

ROC Temperature (C)

This displays the temperature of the ROC.

Shield State Supported

This displays whether the shield state is supported or not.

Drive Security

This displays the status of the drive security feature.

T10-PI

This displays the status of the data protection feature.

Maintain Drive Fail History

Enabling this feature allows you to track the fail history of the drives. The options are Disabled and **Enabled**.

SMART Polling

Enter a numeric value to set how frequently the controller polls for drives that are reporting a Predictive Drive Failure. The default option is **300** seconds.

Stop Consistency Check on Error

Enabling this feature stops the consistency check operation on a redundant virtual drive if there is an inconsistency found in the data. Disabling this allows the consistency check operation to continue on a redundant virtual drive if there is an inconsistency found in the data. The options are **Disabled** and Enabled.

JBOD Mode

Use this feature to enable or disable the JBOD mode. The options are **Disabled** and Enabled.

Large IO Support

Unmap Capability

Use this feature to enable or disable the unmap capability for the controller. The options are Disabled and **Enabled**.

Firmware Device Order

Use this feature to select the firmware device order. The options are **Disabled** and Enabled.

PCIe Reference Clock

This feature displays or allows you to change the PCIe reference clock settings. The options are **Default (No Override)**, Enabled, and Disabled.

PERST

This feature displays or allows you to change the PCIe Reset Side-Band Signal (PERST) settings. The options are **Default (No Override)**, Deasserted, and Asserted.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Patrol Read

►Patrol Read

This menu enables you to view and set patrol read properties.

►Start

Press the <Enter> key to start the patrol read for the selected controller.

►Suspend

Press the <Enter> key to suspend the patrol read.

►Resume

Press the <Enter> key to resume the patrol read.

►Stop

Press the <Enter> key to stop the patrol read.

State

This displays the current state of the patrol read operation.

Iterations

This displays the number of patrol read iterations.

Mode

This feature allows you to modify the patrol read mode for the controller. The options are **Auto**, Manual, and Disabled.

Rate

Enter a numerical value to set the percentage of system resources dedicated to perform a patrol read operation on configured drives.

Setting for Unconfigured Space

This setting indicates the patrol read settings for the unconfigured space.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Spare

►Spare

Use this menu to view and change controller properties related to emergency spares, hot spares, and replace drives.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Persistent Hot Spare

Replace Drive

Use this feature to enable or disable the ability to copy data back from a hot spare drive to a drive. The options are Enabled and **Disabled**.

Replace Hard Disk Drive on SMART Error

Replace Solid State Drive on SMART Error

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Task Rates

►Task Rates

Use this menu to view and change the percentage of controller resources allotted for various operations.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Background Initialization (BGI) Rate

This feature displays the percentage at which the system resources are dedicated to perform a background initialization on a redundant virtual drive. Enter a number to modify the percentage.

Consistency Check Rate

This feature displays the percentage at which the system resources are dedicated to perform a consistency check operation on a redundant virtual drive. Enter a number to modify the percentage.

Patrol Read Rate

This feature displays the percentage at which the system resources are dedicated to perform a patrol read operation on the configured drives. Enter a number to modify the percentage.

Rebuild Rate

This feature displays the percentage at which the system resources are dedicated to rebuild data on a new drive after a storage configuration drive has failed. Enter a number to modify the percentage.

Reconstruction Rate

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

External Key Management

►External Key Management

Use this menu to view the properties for the External Key Management (EKM) feature.

The following information is displayed:

- Capability
- Boot Agent
- Configured

Spin Down Drives At Shutdown

►Spin Down Drives At Shutdown

Use this menu to view and modify the spin down of drives at shutdown.

SATA HDD / SAS HDD / SAS SSD / NVMe SSD

This feature allows you to enable or disable the spin down of the selected drive. The options are **Disabled** and Enabled.

SATA SSD

This feature allows you to enable or disable the spin down of the selected drive. The options are Disabled and **Enabled**.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Virtual Drive Management

►Virtual Drive Management

Use this menu to view and modify the virtual drive properties.

Drive Management

►Drive Management

Use this menu to view and modify basic drive properties.

Drive

►Drive

This menu allows you to view and modify specific drive properties. The number of drives may differ depending on your setup.

Operation

Select the operation that you want to perform on the drive. The options are **Select operation**, Initialize Drive, Cryptographic Erase, Make Unconfigured Bad, Prepare For Removal, and Sanitize.

BASIC PROPERTIES:

The following information is displayed:

- Device ID
- Status

- Size
- Type
- Model
- Serial Number
- Hardware Vendor

Advanced...

►Advanced...

This menu displays additional information about the specific drive.

The following information is displayed:

- Certified
- Logical Sector Size
- Physical Sector Size
- SMART Status
- Revision
- Media Errors
- Predicted Fail Count
- WWID
- Multipath
- Drive Power State
- Cache Setting
- Disk Protocol
- Capable Speed
- Negotiated Speed
- PCIe Capable Link Width
- PCIe Negotiated Link Width
- Number of Connections
- FDE Capable
- Secured

- Cryptographic Erase Capable
- Unmap Capable
- Unmap Capability for Configuration
- Temperature (C)

Hardware Components

►Hardware Components

This menu allows you to view enclosure status.

BASIC HARDWARE STATUS:

►Enclosure Management

This menu allows you to view enclosure information.

Select Enclosure

This feature allows you to view all attached enclosures.

The following information is displayed:

- Vendor ID
- Enclosure ID
- Enclosure Model

Help

►Help

This menu displays additional information on configurations.

CONFIGURE:

Allows you to create a virtual drive or a JBOD if applicable by clicking on the Configure option present in the ACTIONS section in the Dashboard View. This option takes you to the Configuration Management page that displays the configuration options. Some options appear only if the controller supports them. As an example, Create Virtual Drive, Create Profile Based Virtual Drive, Make JBOD, Make Unconfigured Good, Clear Configuration, Manage Foreign Configuration, View Drive Group Properties and View Global Hot Spares Drives.

PROPERTIES

PROPERTIES:

The following information is displayed:

- Status
- Backplane
- CacheVault
- Enclosure
- Drives
- JBODs
- Drive Groups
- Virtual Drives

View Server Profile

►View Server Profile

SERVER:

The following information is displayed:

- UEFI Spec Version

CONTROLLER COMPONENTS

Controller Management

►Controller Management

Use this menu to view the controller status and basic properties of the controller.

BASIC PROPERTIES:

The following information is displayed:

- Product Name
- Serial Number
- Controller Status
- Personality Mode
- Select Boot Device
- PCI ID
- PCI Segment:Bus:Device:Function
- PCI Slot Number

- Package Version
- Firmware Version
- NVDATA Version
- Supported Device Interfaces
- Drive Count
- JBOD Count
- Virtual Drive Count

Advanced Controller Management

►Advanced Controller Management

Use this menu to modify various controller management activities.

Clear Controller Events

►Clear Controller Events

Use this menu to delete all of the existing controller events.

Are you sure you want to clear the controller events?

Confirm

Use this feature to confirm whether you want to clear all controller events. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

Save Controller Events

►Save Controller Events

Use this menu to save all of the existing controller events.

Save TTY Log

►Save TTY Log

This menu allows you to save a copy of the controller's firmware terminal log entries. The Diagnostics report includes this information.

Enable Drive Security

►Enable Drive Security

Use this menu to activate the controller's drive security.

CHOOSE THE SECURITY KEY MANAGEMENT MODE:

External Key Management (EKM)

Local Key Management (LKM)

This mode provides key management using keys within the controller itself. This mode does not require any external entity. Local Key Management is preferred in deployments that involve fewer systems. The options are Disabled and **Enabled**.

OK

Press the <Enter> key to proceed with the selected security key management option.

►Cancel

This cancels the chosen drive security mode operation.

Disable Drive Security

►Disable Drive Security

Disable Drive Security

►Disable Drive Security

Manage SAS Storage Link Speed

►Manage SAS Storage Link Speed

Use this menu to manage the SAS storage link speed.

VIEW THE PHY SETTINGS FOR THE CONTROLLER AND CHANGE THEM IF NEEDED:

Phy# 00, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 01, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 02, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 03, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 04, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 05, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 06, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

Phy# 07, Disabled, , Port# 255, Neg. Speed N/A SAS Address: (0x0000000000000000)

This lists the supported link speed by the phy and allows you to select the desired speed (if supported). The default selected speed in the list points to the max link speed supported by the phy. The options are **Auto**, 3 Gbps, 6 Gbps, and 12 Gbps.

►OK

Press the <Enter> key to commit to the changes.

►Cancel

Press the <Enter> key to cancel the changes.

Manage PCIe Storage Interface

►Manage PCIe Storage Interface

Use this menu to manage the controller's link width and lane speed.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

VIEW LINK WIDTH AND CHANGE THEM IF NEEDED:

Link Width for C0, C1, C2, C3

Use this feature to select the desired link width (if supported). The options are 0–3:x3, 4–7:x4, **0–1:x2, 2–3:x2, 4–5:x2, 6–7:x2**, and 0:x1, 1:x1, 2:x1, 3:x1, 4:x1, 5:x1, 6:x1, 7:x1.

Important: If the speed for some of the lanes that are participating in the same link are configured differently, then the lowest speed will be used by the link. Recommendation: Choose the same speed for all lanes that belong to the same link.

VIEW THE LANE SPEED AND CHANGE THEM IF NEEDED:

Lane# 00, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 01, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 02, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 03, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 04, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 05, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 06, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

Lane# 07, Enabled, C0, Link#, 00, Neg. Speed: N/A, WWID: (0x0000000000000000), Device Type: N/A

This feature lists the supported speed by the lane and allows you to select the desired speed (if supported). The default selected speed in the list points to the max supported speed by the lane. The options are 2.5 GT/s, 5 GT/s, 8 GT/s, and **16 GT/s**.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Manage MegaRAID Advanced Software Options

►Manage MegaRAID Advanced Software Options

This menu enables you set the controller's MegaRAID Advanced Software Options. This menu also shows the Advanced Software Options that are active on the controller.

MegaRAID SafeStore (Unlimited)

MegaRAID FastPath (Unlimited)

The following information is displayed:

- SAFE ID
- Serial Number

Activation Key

Enter a 40 alpha-numeric character value.

►Activate

Press <Enter> to see a summary and activate the advanced software options.

►Deactivate All Trial Software

Schedule Consistency Check

►Schedule Consistency Check

This menu allows you to schedule a Consistency Check (CC) operation.

Consistency Check Frequency

Use this feature to select the frequency of the consistency check runs. The options are Disable, Hourly, Daily, **Weekly**, and Monthly.

Consistency Check Start Date

Use this feature to set the start date for the consistency check operation. Enter the date in the format of MM/DD/YYYY.

Consistency Check Start Time

Use this feature to set the consistency check start time. Enter the time in the format of HH:MM:SS.

Consistency Check Mode

Use this feature to select the consistency check mode. Sequential checks the virtual drives one at a time. **Concurrent** checks all of the selected virtual drives simultaneously.

Start Immediately

SELECT VIRTUAL DRIVES TO CHECK:

►Exclude Virtual Drives

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Set Factory Defaults

►Set Factory Defaults

Use this menu to restore the controller settings to factory defaults.

Are you sure you want to reset the controller settings to factory defaults?

Confirm

Use this feature to confirm whether you want to reset the controller settings to factory defaults. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

►No

Press <Enter> to return to the main menu.

Manage Personality Mode

►Manage Personality Mode

Use this menu to change the controller's parameters and personality.

The following information is displayed:

- Personality Mode

Manage Controller Profiles

►Manage Controller Profiles

Use this menu to view the controller's profile information and to choose a profile.

The following information is displayed:

- Number of Profiles

Choose Profile

Use this feature to select the desired controller profile.

DETAILS OF THE PROFILE:

The following information is displayed:

- Personality Mode
- Profile ID
- Default Profile
- Compatible
- Max PD Count
- Max VD Count
- Max NVMe Count

►Set Profile

Manage Phy State

►Manage Phy State

Use this menu to modify the phy state to enabled or disabled.

VIEW THE PHY SETTINGS FOR THE CONTROLLER AND CHANGE THEM IF NEEDED.

Phy# 00 / Phy# 01 / Phy# 03 / Phy# 04 / Phy# 05 / Phy# 06 / Phy# 07

Use this feature to enable or disable the phy state. The options are **Disabled** and Enabled.

►OK

Press the <Enter> key to commit to the changes.

►Cancel

Press the <Enter> key to cancel the changes.

Advanced Controller Properties

►Advanced Controller Properties

This menu allows you to view and modify advanced controller properties.

CONTROLLER PROPERTIES:

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Auto Import Foreign Configuration

Enabling this feature allows automatic import of foreign configurations without you needing to intervene. The options are **Enabled** and Disabled.

Coercion Mode

Use this feature to set the drive coercion mode. The options are **None**, 128 MB, and 1 GB.

Boot Mode

Use this feature to set how to handle errors that may occur during boot time. The options are Stop on errors, **Pause on errors**, Ignore errors, and Safe mode on errors.

Controller BIOS

Use this feature to enable or disable the controller BIOS. The options are **Enabled** and Disabled.

ROC Temperature (C)

This displays the temperature of the ROC.

Shield State Supported

This displays whether the shield state is supported or not.

Drive Security

This displays the status of the drive security feature.

T10-PI

This displays the status of the data protection feature.

Maintain Drive Fail History

Enabling this feature allows you to track the fail history of the drives. The options are Disabled and **Enabled**.

SMART Polling

Enter a numeric value to set how frequently the controller polls for drives that are reporting a Predictive Drive Failure. The default option is **300** seconds.

Stop Consistency Check on Error

Enabling this feature stops the consistency check operation on a redundant virtual drive if there is an inconsistency found in the data. Disabling this allows the consistency check operation to continue on a redundant virtual drive if there is an inconsistency found in the data. The options are **Disabled** and Enabled.

JBOD Mode

Use this feature to enable or disable the JBOD mode. The options are **Disabled** and Enabled.

Large IO Support

Unmap Capability

Use this feature to enable or disable the unmap capability for the controller. The options are Disabled and **Enabled**.

Firmware Device Order

Use this feature to select the firmware device order. The options are **Disabled** and Enabled.

PCIe Reference Clock

This feature displays or allows you to change the PCIe reference clock settings. The options are **Default (No Override)**, Enabled, and Disabled.

PERST

This feature displays or allows you to change the PCIe Reset Side-Band Signal (PERST) settings. The options are **Default (No Override)**, Deasserted, and Asserted.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Patrol Read

►Patrol Read

This menu enables you to view and set patrol read properties.

►Start

Press the <Enter> key to start the patrol read for the selected controller.

►Suspend

Press the <Enter> key to suspend the patrol read.

►Resume

Press the <Enter> key to resume the patrol read.

►Stop

Press the <Enter> key to stop the patrol read.

State

This displays the current state of the patrol read operation.

Iterations

This displays the number of patrol read iterations.

Mode

This feature allows you to modify the patrol read mode for the controller. The options are **Auto**, Manual, and Disabled.

Rate

Enter a numerical value to set the percentage of system resources dedicated to perform a patrol read operation on configured drives.

Setting for Unconfigured Space

This setting indicates the patrol read settings for the unconfigured space.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Spare

►Spare

Use this menu to view and change controller properties related to emergency spares, hot spares, and replace drives.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Persistent Hot Spare

Replace Drive

Use this feature to enable or disable the ability to copy data back from a hot spare drive to a drive. The options are Enabled and **Disabled**.

Replace Hard Disk Drive on SMART Error

Replace Solid State Drive on SMART Error

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Task Rates

►Task Rates

Use this menu to view and change the percentage of controller resources allotted for various operations.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Background Initialization (BGI) Rate

This feature displays the percentage at which the system resources are dedicated to perform a background initialization on a redundant virtual drive. Enter a number to modify the percentage.

Consistency Check Rate

This feature displays the percentage at which the system resources are dedicated to perform a consistency check operation on a redundant virtual drive. Enter a number to modify the percentage.

Patrol Read Rate

This feature displays the percentage at which the system resources are dedicated to perform a patrol read operation on the configured drives. Enter a number to modify the percentage.

Rebuild Rate

This feature displays the percentage at which the system resources are dedicated to rebuild data on a new drive after a storage configuration drive has failed. Enter a number to modify the percentage.

Reconstruction Rate

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

External Key Management

►External Key Management

Use this menu to view the properties for the External Key Management (EKM) feature.

The following information is displayed:

- Capability
- Boot Agent
- Configured

Spin Down Drives At Shutdown

►Spin Down Drives At Shutdown

Use this menu to view and modify the spin down of drives at shutdown.

SATA HDD / SAS HDD / SAS SSD / NVMe SSD

This feature allows you to enable or disable the spin down of the selected drive. The options are **Disabled** and Enabled.

SATA SSD

This feature allows you to enable or disable the spin down of the selected drive. The options are Disabled and **Enabled**.

►Apply Changes

Press <Enter> to submit the changes made to the entire form.

Virtual Drive Management

►Virtual Drive Management

Use this menu to view and modify the virtual drive properties.

Drive Management

►Drive Management

Use this menu to view and modify basic drive properties.

Drive

►Drive

This menu allows you to view and modify specific drive properties. The number of drives may differ depending on your setup.

Operation

Select the operation that you want to perform on the drive. The options are **Select operation**, Initialize Drive, Cryptographic Erase, Make Unconfigured Bad, Prepare For Removal, and Sanitize.

BASIC PROPERTIES:

The following information is displayed:

- Device ID
- Status
- Size
- Type
- Model
- Serial Number
- Hardware Vendor

Advanced...

►Advanced...

This menu displays additional information about the specific drive.

The following information is displayed:

- Certified
- Logical Sector Size
- Physical Sector Size
- SMART Status
- Revision

- Media Errors
- Predicted Fail Count
- WWID
- Multipath
- Drive Power State
- Cache Setting
- Disk Protocol
- Capable Speed
- Negotiated Speed
- PCIe Capable Link Width
- PCIe Negotiated Link Width
- Number of Connections
- FDE Capable
- Secured
- Cryptographic Erase Capable
- Unmap Capable
- Unmap Capability for Configuration
- Temperature (C)

Hardware Components

►Hardware Components

This menu allows you to view enclosure status.

BASIC HARDWARE STATUS:

►Enclosure Management

This menu allows you to view enclosure information.

Select Enclosure

This feature allows you to view all attached enclosures.

The following information is displayed:

- Vendor ID
- Enclosure ID
- Enclosure Model

Drive Management

►Drive Management

Use this menu to view and modify basic drive properties.

Virtual Drive Management

►Virtual Drive Management

Use this menu to view and modify the virtual drive properties.

ACTIONS

Configuration Management

►Configuration Management

This menu displays configuration options, some of which will only appear if the controller supports them.

Create Virtual Drive

►Create Virtual Drive

Use this menu to create a virtual drive.

►Save Configuration

Press the <Enter> key to save the configuration.

Select RAID Level

This feature allows you to select a RAID level. The options are **RAID0**, RAID1, and RAID00.

Secure Virtual Drive

Unmap Capability

This feature allows you to enable or disable the unmap capability for the virtual drive. The options are Enabled and **Disabled**.

Select Drives From

Use this feature to select drives from Unconfigured Capacity or Free Capacity. The options are **Unconfigured Capacity** and Free Capacity.

CONFIGURE VIRTUAL DRIVE PARAMETERS:

Virtual Drive Name

Enter a name for the virtual drive.

Virtual Drive Size

This displays the amount of storage space on the virtual drive.

Virtual Drive Size Unit

This displays the unit of which the size is measured by.

Strip Size

This feature allows you to select the strip size or the virtual drive. The default option is **64 KB**.

Read Policy

Write Policy

I/O Policy

Access Policy

Use this feature to select the access policy for the virtual drive. The option are **Read/Write**, Read Only, and Blocked.

Drive Cache

Use this feature to select the virtual drive's cache setting. The options are **Unchanged**, Enable, and Disable.

Disable Background Initialization

This feature allows you to allow disabling of the background initialization. No enables the background initialization and Yes disables the background Initialization. The options are **No** and Yes.

Default Initialization

This feature allows you to choose the default for initialization. The options are **No**, Fast, and Full.

Emulation Type

This feature allows you to choose an emulation type. The options are **Default**, Disable, and Force.

►Save Configuration

Press the <Enter> key to save the configuration.

Create Profile Based Virtual Drive

►Create Profile Based Virtual Drive

This menu allows you to create a virtual drive through a wizard.

Generic RAID 0

►Generic RAID 0

This menu provides information on generic RAID 0, which uses drive striping to store data across multiple disks.

Drive Selection Criteria

This allows you to select a drive.

PROFILE PARAMETERS:

The following information is displayed:

- Virtual Drive Name
- RAID Level
- Virtual Drive Size
- Strip Size
- Read Policy
- Write Policy
- IO Policy
- Drive Cache
- Default Initialization

►Save Configuration

Press the <Enter> key to save the configuration.

Generic RAID 1

►Generic RAID 1

This menu provides information on generic RAID 1, which is drive mirroring that information can be simultaneously written to more than one drive.

Drive Selection Criteria

This allows you to select a drive.

PROFILE PARAMETERS:

The following information is displayed:

- Virtual Drive Name
- RAID Level
- Virtual Drive Size
- Strip Size
- Read Policy
- Write Policy
- IO Policy
- Drive Cache
- Default Initialization

►Save Configuration

Press the <Enter> key to save the configuration.

Clear Configuration

►Clear Configuration

This feature deletes all existing configurations on the RAID controller and discards the pinned cache on missing configuration.

Clear Configuration will delete all of the Virtual Drives, Hot Spare Drives, Pinned Cache and JBODs (if applicable) attached to this controller.

Are you sure you want to clear the configuration?

Confirm

Use this feature to confirm you want to clear the configuration. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

►No

Press <Enter> to return to the main menu.

Set Factory Defaults

►Set Factory Defaults

Use this menu to restore the controller settings to factory defaults.

Are you sure you want to reset the controller settings to factory defaults?

Confirm

Use this feature to confirm whether you want to reset the controller settings to factory defaults. The options are **Disabled** and Enabled. Disabling this feature disables Yes. Enabling this feature enables Yes.

►No

Press <Enter> to return to the main menu.

Update Firmware

BACKGROUND OPERATIONS

BACKGROUND OPERATIONS:

The following information is displayed:

- Virtual Drive Operations in Progress
- Drive Operations in Progress

MegaRAID ADVANCED SOFTWARE OPTIONS

MegaRAID ADVANCED SOFTWARE OPTIONS:

The following information is displayed:

- MegaRAID SafeStore
- MegaRAID FastPath

Manage MegaRAID Advanced Software Options

►Manage MegaRAID Advanced Software Options

This menu enables you set the controller's MegaRAID Advanced Software Options. This menu also shows the Advanced Software Options that are active on the controller.

MegaRAID SafeStore (Unlimited)

MegaRAID FastPath (Unlimited)

The following information is displayed:

- SAFE ID
- Serial Number

Activation Key

Enter a 40 alpha-numeric character value.

►Activate

Press <Enter> to see a summary and activate the advanced software options.

►Deactivate All Trial Software

Driver Health Menu

►Driver Health

This feature displays the health information of the drivers installed in your system, including LAN controllers, as detected by the BIOS. Select one and press <Enter> to see the details.

Note: This section is provided for reference only, for the driver health status will differ depending on the drivers installed in your system. It's also based on your system configuration and the environment that your system is operating in.

4.4 Event Logs

Use this menu to configure Event Logs settings.

Note: After making any changes in this section, be sure to reboot the system for the changes to take effect.

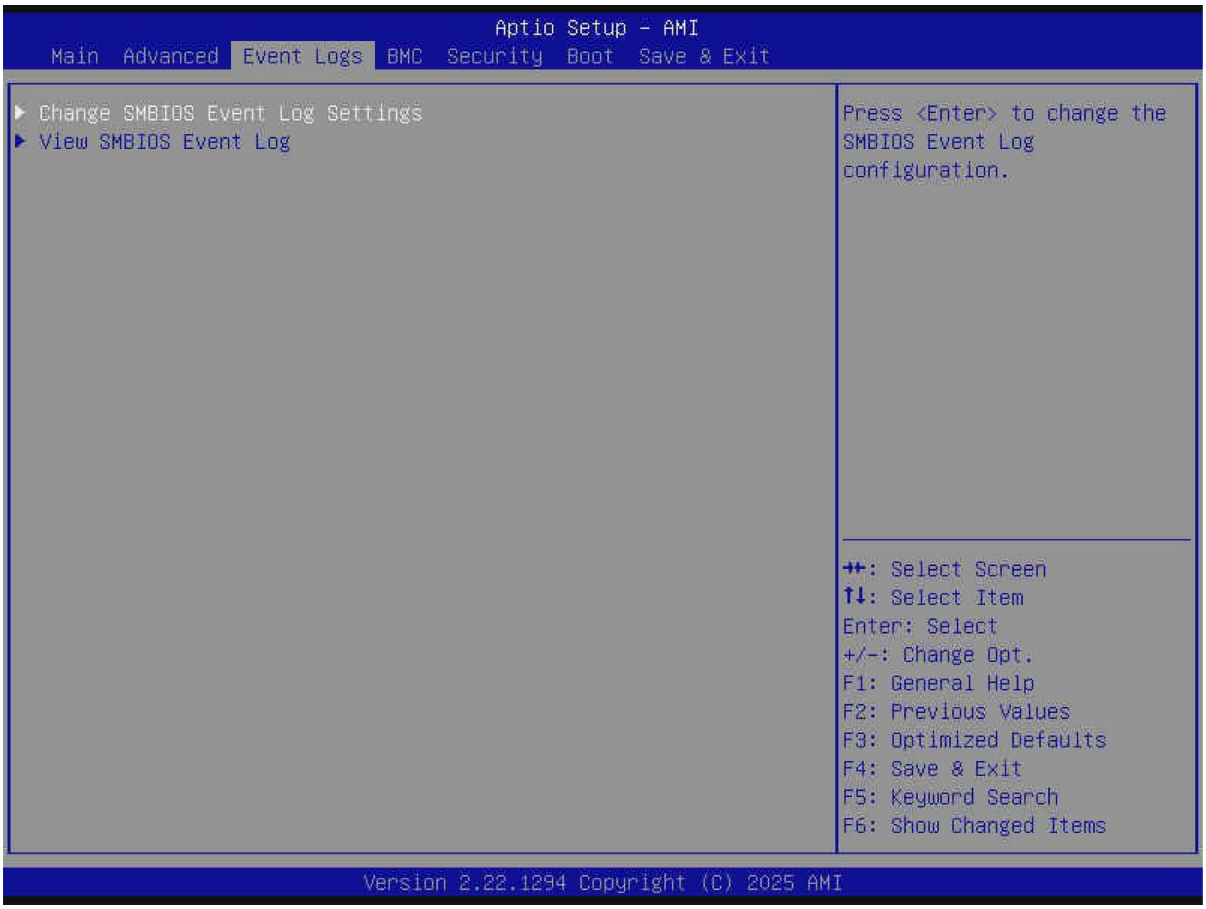


Figure 4-3. Event Logs Screen

►Change SMBIOS Event Log Settings

Note: Reboot the system for the changes in this section to take effect.

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

Erase Event Log (Available when "SMBIOS Event Log" is set to Enabled)

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 (Available when "SMBIOS Event Log" is set to Enabled)

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 (Available when "SMBIOS Event Log" is set to Enabled)

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

MECI (Available when "SMBIOS Event Log" is set to Enabled)

Enter the increment value for the multiple event counter. Enter a number between 1 and 255. The default setting is **1**. (MECI is the abbreviation for Multiple Event Count Increment.)

METW (Available when "SMBIOS Event Log" is set to Enabled)

Use this feature to determine how long (in minutes) should the multiple event counter wait before generating a new event log. Enter a number between 0 and 99. The default value is **60**. (METW is the abbreviation for Multiple Event Count Time Window.)

►View SMBIOS Event Log

Use this feature to view the events in the system event log. Select this feature and press <Enter> to view the status of an event in the log. The following information is displayed: DATE / TIME / ERROR CODE / SEVERITY.

4.5 BMC

Use this menu to configure Baseboard Management Console (BMC) settings.



Figure 4-4. BMC Screen

BMC Firmware Revision

This feature indicates the BMC firmware revision used in this system.

BMC STATUS

This feature indicates the status of the BMC firmware installed in this system.

System Event Log Menu

►System Event Log

Note: All values changed in this submenu do not take effect until computer is restarted.

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL (Available when "SEL Components" is set to Enabled)

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 (Available when "SEL Components" is set to Enabled)

This feature defines 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 Menu

►BMC Network Configuration

Update BMC LAN Configuration

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

****

Configure IPv4 Support

****

BMC LAN Selection

This feature displays the type of the BMC LAN.

BMC Network Link Status:

This feature displays the status of the BMC network link for this system.

Configuration Address Source

Use this feature to select the source of the IPv4 connection. If Static is selected, note the IP address of the IPv4 connection and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a Dynamic Host Configuration Protocol (DHCP) server in the

network that is attached to and request the next available IP address for this computer. The options are Static and **DHCP**. It is available for configuration when "Update BMC LAN Configuration" is set to Yes.

Station IP Address

This feature displays the Station IP address in decimal and in dotted quad form (i.e., 172.29.176.131). It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static.

Subnet Mask

This feature displays the sub- network that this computer belongs to. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static.

Station MAC Address

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

Gateway IP Address

This feature displays the IPv4 gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1). It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static.

****

Configure IPv6 Support

****

IPv6 Address Status

This feature displays the status of the IPv6 address.

IPv6 Support

Use this feature to enable IPv6 support. The options are **Enabled** and Disabled. It is available for configuration when "Update BMC LAN Configuration" is set to Yes.

Configuration Address Source

Use this feature to select the source of the IPv6 connection. If Static Configuration is selected, note the IP address of IPv6 connection and enter it to the system manually in the field. If the other two options are selected, the BIOS will search for a DHCP server in the network that is attached to and request the next available IP address for this computer. The options are Static Configuration, **DHCPv6 Stateless**, and DHCPv6 Stateful. It is available for configuration when "Update BMC LAN Configuration" is set to Yes.

IPv6 Address ("Static," "DHCPv6 Stateless," or "DHCPv6 Stateful," depending on the option you selected for "Configuration Address Source" above)

This feature displays the station IPv6 address. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static Configuration.

Prefix Length

This feature displays the prefix length. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static Configuration.

Gateway IP

This feature displays the IPv6 gateway IP address. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to Static Configuration.

Advanced Settings

Use this feature to set the DNS server IP. The default setting allows this system to obtain the DNS server IP automatically. The options are **Auto obtain DNS server IP** and Manually obtain DNS server IP. It is available for configuration when "Update BMC LAN Configuration" is set to Yes and "Configuration Address Source" above is set to DHCPv6 Stateless.

Preferred DNS server IP (Available when "Advanced Settings" above is set to Manually obtain DNS server IP)

This feature displays the preferred DNS server IP. It can be configured via Redfish.

Alternative DNS server IP (Available when "Advanced Settings" above is set to Manually obtain DNS server IP)

This feature displays the alternative DNS server IP. It can be configured via Redfish.

****

Configure VLAN Support

****

VLAN Support

Use this feature to enable the virtual LAN (VLAN) support. The options are Enabled and **Disabled**.

VLAN ID (Available when "VLAN Support" is set to Enabled)

Use this feature to create a new VLAN ID. The valid range is 1–4094. The default setting is **1**.

4.6 Security

Use this menu to configure the following security settings for the system.

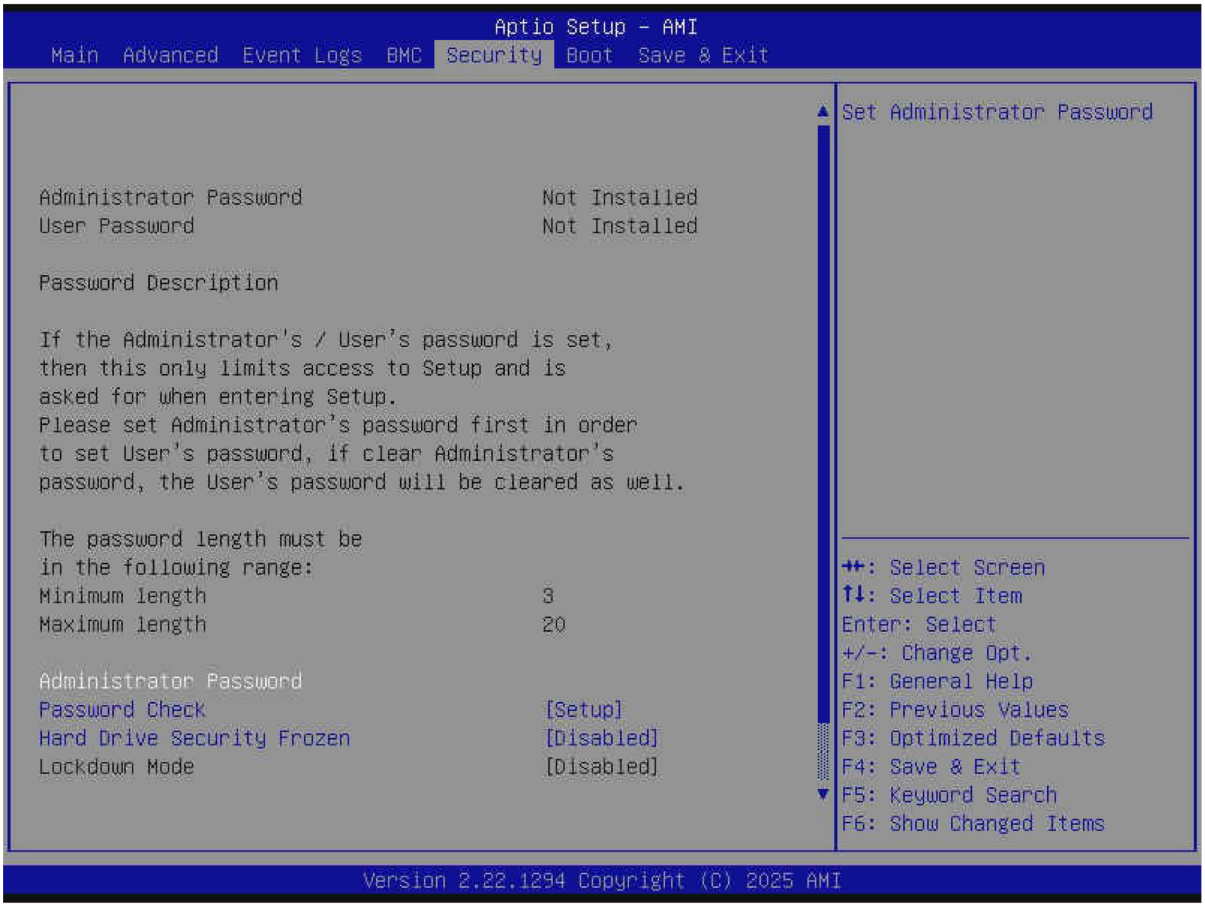


Figure 4-5. Security Screen

Disable Block Sid and Freeze Lock (Available when your storage devices support TCG)

Select Enabled to allow SID authentication to be performed in TCG storage devices. The options are **Disabled** and Enabled.

The following information is displayed:

- Administrator Password
- User Password
- Password Description

Administrator Password

This feature indicates if an administrator password has been installed. Use this feature to set the administrator password, which is required to enter the BIOS Setup utility. The length of the password can be between three and 20 characters long.

User Password (Available when "Administrator Password" has been set)

This feature indicates if a user password has been installed. Use this feature to set the user password which is required to enter the BIOS Setup utility. The length of the password can be between three and 20 characters long.

Password Check

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

Hard Drive Security Frozen

Select Enabled to freeze the Lock Security feature for HDD to protect key data in hard drives from being altered. The options are **Disabled** and Enabled.

Lockdown Mode (Available when the DCMS key is activated)

Select Enabled to support the Lockdown Mode, which prevents the existing data or keys stored in the system from being altered or changed in an effort to preserve system integrity and security. The options are **Disabled** and Enabled.

Supermicro Security Erase Configuration Menu

►Supermicro Security Erase Configuration

Use this submenu to configure the Supermicro-proprietary Security Erase settings. When this submenu is selected, the following information is displayed. Note that the order of the following information may differ based on the storage devices being detected.

- HDD Name: This feature displays the model name of the storage device that is detected by the BIOS.
- HDD Serial Number: This feature displays the serial number of the storage device that is detected by the BIOS.
- Security Mode: This feature displays the security mode of the storage device that is detected by the BIOS.
- Estimated Time: This feature displays the estimate time needed to perform the selected Security Erase features.
- HDD User Pwd Status: This feature indicates if a password has been set as a storage device user password, which enables configuring Supermicro Security Erase settings on this storage device.
- TCG Device Type: This feature displays the TCG device type detected by the system.

- Admin Pwd Status: This feature indicates if a password has been set as a storage device administrator password, which enables configuring Supermicro Security Erase settings on this storage device.

Note: This submenu is available when any storage device is detected by the BIOS. For more information about this feature, refer to our website.

Security Function

Select Set Password to set a storage device user password to enable configuring the security settings on the storage device. Select Security Erase - Password to enter a storage device user password to enable erasing the password and the contents previously stored in the storage device. Select Security Erase - Without Password to use the manufacturer default password "111111111" as the storage device user password and enable erasing the contents of the storage device by using this default password. The options are **Disabled**, Set Password, Change Password, Clear Password, Security Erase - Password, Security Erase - PSID, and Security Erase - Without Password.

Notes:

- The option of Security Erase - PSID is based on the storage device support. PSID is the abbreviation for Physical Security Identification.
- The options of Change Password and Clear Password are available when "Password" below has been set.
- The option of Set Password is NOT available when "Password" below has been set.

Password

Use this feature to set the storage device user password, which enables configuring the Supermicro Security Erase settings by using this user password.

New Password (Available when "Password" above has been set)

Use this feature to set the new user password for the storage device, which enables configuring the Supermicro Security Erase settings by using this new user password.

HDD Security Configuration Menu

►P4: (Storage device model name)

This submenu is available when the storage device is detected by the BIOS. Select this device. Press <Enter> and the following information is displayed:

- HDD Password Description:
- HDD PASSWORD CONFIGURATION:
- Security Supported:
- Security Enabled:
- Security Locked:
- Security Frozen:
- HDD User Pwd Status:
- HDD Master Pwd Status:

Set User Password (Available when "Security Frozen:" above is No)

Press <Enter> to set the HDD user password.

Secure Boot Menu

►Secure Boot

The following information is displayed:

- System Mode
- Secure Boot

Note: For detailed instructions on configuring Security Boot settings, refer to the Security Boot Configuration User's Guide at https://www.supermicro.com/support/manuals.

Secure Boot

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

Secure Boot Mode

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

►Enter Audit Mode

Select Ok to enter the Audit Mode workflow. It will result in erasing the Platform Key (PK) variables and resetting the system to the Setup/Audit Mode.

Note: This submenu is available when "Secure Boot Mode" is set to Custom.

►Enter Deployed Mode / Exit Deployed Mode

Select Ok to reset system to the User Mode or to the Deployed Mode.

Note: This submenu is available when "Secure Boot Mode" is set to Custom.

►Key Management

The following information is displayed:

- Vendor Keys

Note: This submenu is available when "Secure Boot Mode" is set to Custom.

Provision Factory Defaults

Select Enabled to install the default secure boot keys when the system is in the Setup Mode. Changes take effect after you save settings and reboot the system. The options are **Disabled** and Enabled.

►Restore Factory Keys

Select Yes to restore manufacturer default keys to ensure system security. The options are **Yes** and No. Selecting Yes will reset the system to the User Mode.

Note: This submenu is available when any secure keys have been installed.

►Reset To Setup Mode

This feature resets the system to the Setup Mode. The options are **Yes** and No.

Note: This submenu is available when any secure keys have been installed.

►Enroll Efi Image

This feature allows the Efi image to run in the secure boot mode and enroll the SHA256 Hash certificate of a PE image into the Authorized Signature Database (DB).

►Export Secure Boot Variables

This feature exports the NVRAM contents of secure boot variables to a storage device. The options are **Yes** and No.

Note: This submenu is available when any secure keys have been installed.

Secure Boot variable / Size / Keys / Key Source

►Platform Key (PK)

Use this feature to enter and configure a set of values to be used as platform firmware keys for the system. These values also indicate the sizes, key numbers, and the sources of the authorized signatures. Select Update to update the platform key.

►Key Exchange Keys (KEK)

Use this feature to enter and configure a set of values to be used as Key Exchange Keys for the system. These values also indicate the sizes, key numbers, and the sources of the authorized signatures. Select Update to update the Key Exchange Keys. Select Append to append the Key Exchange Keys.

►Authorized Signatures (db)

Use this feature to enter and configure a set of values to be used as Authorized Signatures for the system. These values also indicate the sizes, key numbers, and sources of the authorized signatures. Select Update to update the Authorized Signatures. Select Append to append the new Authorized Signatures.

►Forbidden Signatures (dbx)

Use this feature to enter and configure a set of values to be used as Forbidden Signatures for the system. These values also indicate sizes, key numbers, and key sources of the forbidden signatures. Select Update to update the Forbidden Signatures. Select Append to append the Forbidden Signature.

►Authorized TimeStamps (dbt)

Use this feature to set and save the timestamps for the Authorized Signatures, which will indicate the time when these signatures are entered into the system. These values also indicate sizes, keys, and key sources of the authorized timestamps. Select Update to update the Authorized TimeStamps. Select Append to append the Authorized TimeStamps.

►OsRecovery Signatures (dbr)

Use this feature to set and save the Authorized Signatures used for OS recovery. Select Update to update the OsRecovery Signatures. These values also indicate sizes, keys, and key sources of the OsRecovery Signatures. Select Append to append the OsRecovery Signatures.

TCG Storage Security Configuration Menu

►(Storage device model name)

Select this device. Press <Enter> and the following information is displayed:

- TCG Storage Security Password Description:
- PASSWORD CONFIGURATION:
- Security Subsystem Class:
- Security Supported:
- Security Enabled:
- Security Locked:
- Security Frozen:
- User Pwd Status:
- Admin Pwd Status:

Note: This submenu is available when the storage device is compliant with TCG specifications.

Set Admin Password

Use this feature to set the administrator password for this storage device.

Set User Password (Available when "Set Admin Password" has been set)

Use this feature to set the user password for this storage device.

Device Reset

Use this feature to reset the password configuration for this storage device.

4.7 Boot

Use this menu to configure Boot settings.

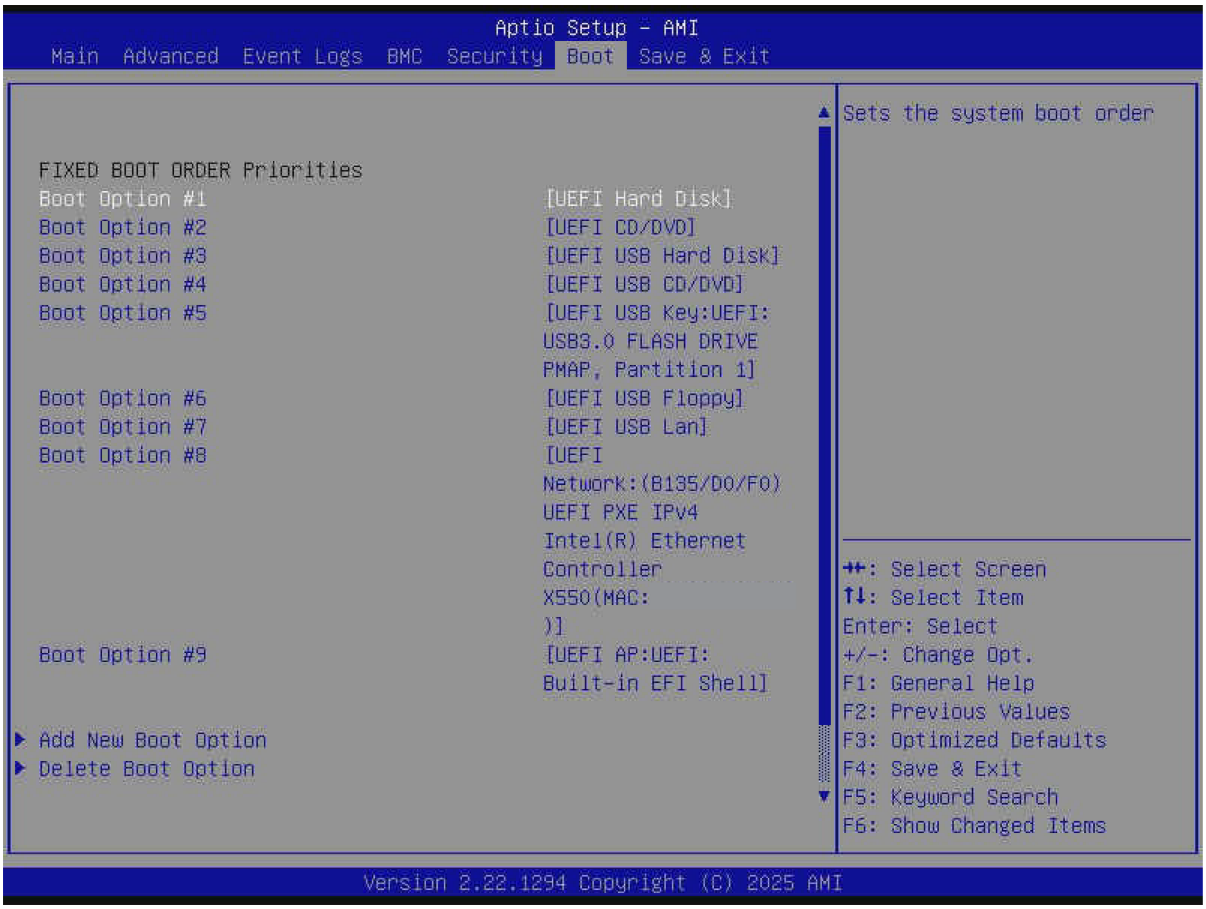


Figure 4-6. Boot Screen

FIXED BOOT ORDER Priorities

Use this feature to prioritize the order of a bootable device from which the system will boot. Press <Enter> on each item sequentially to select the device.

- Boot Option #1 – Boot Option #9

►Add New Boot Option

Use this feature to add a new boot option to the boot priority features for system boot.

Note: This submenu is available when any storage device is detected by the BIOS.

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 setting the name and the file path for the boot option, 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.

►UEFI NETWORK Drive BBS Priorities

Use this feature to set the system boot order of detected devices.

►UEFI Application Boot Priorities

Use this feature to set the system boot order of detected devices.

►UEFI USB Key Drive BBS Priorities

Use this feature to set the system boot order of detected devices.

►UEFI Hard Disk Drive BBS Priorities

Use this feature to set the system boot order of detected devices.

4.8 Save & Exit

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

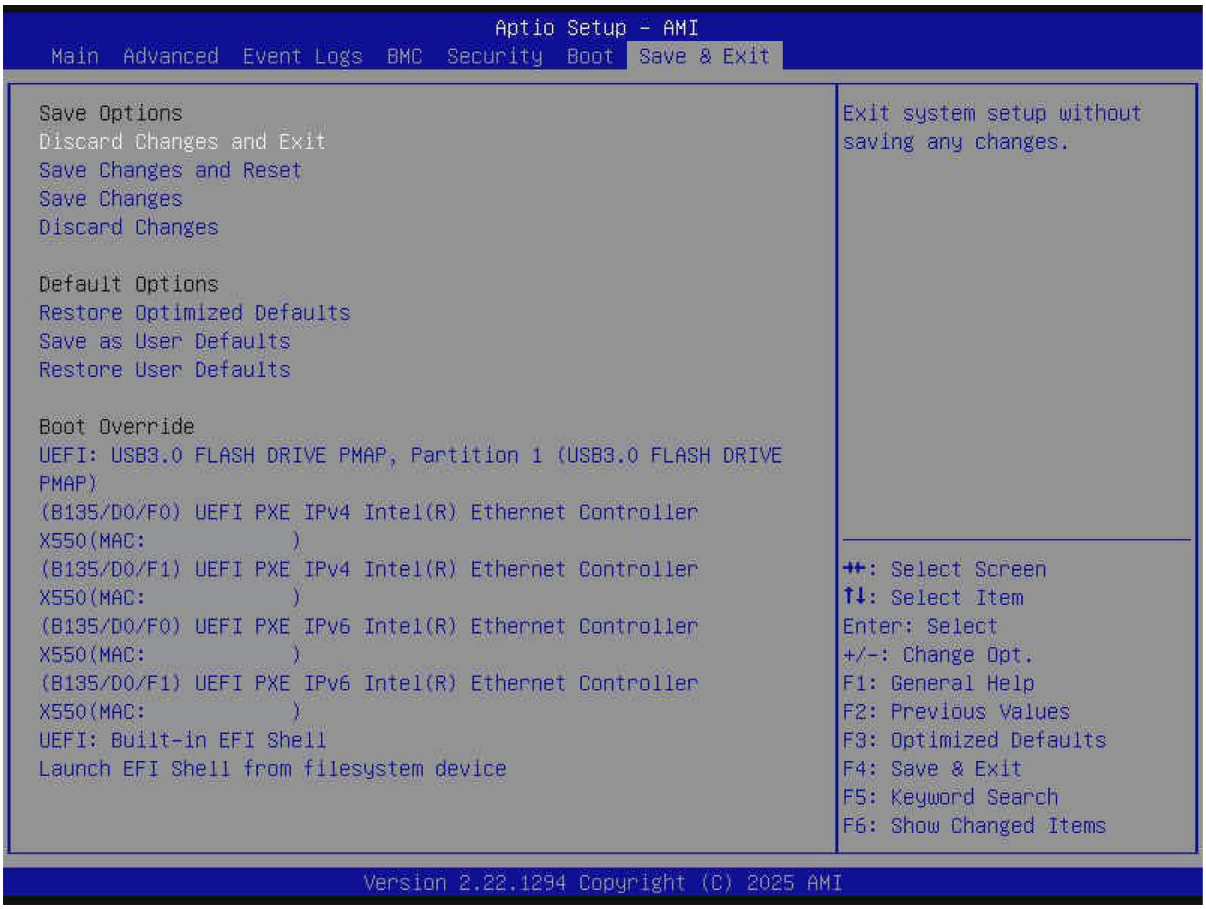


Figure 4-7. Save & Exit Screen

Save Options

Discard Changes and Exit

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

Save Changes and Reset

On completing the system configuration changes, use this feature to exit the BIOS Setup utility and reboot the computer for the new system configuration parameters to take effect.

Save Changes

On completing the system configuration changes, use this feature to save all changes made. This will not reset (reboot) the system.

Discard Changes

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

Default Options

Restore Optimized Defaults

Select this feature and press <Enter> to load manufacturer optimized default settings, which are intended for maximum system performance but not for maximum stability.

Note: Reboot the system for the changes to take effect to ensure that the system has the optimized default settings.

Save as User Defaults

Select this feature and press <Enter> to save all changes as the default values specified to the BIOS Setup utility for future use.

Restore User Defaults

Select this feature and press <Enter> to retrieve user-defined default settings that have been saved previously.

Boot Override

Note: Use this section to override the Boot priorities sequence in the Boot menu, and immediately boot the system with a device specified here instead of the one specified in the boot list. This is a one-time boot override.

Launch EFI Shell from filesystem device

Use this feature to launch the EFI shell application (Shell.efi) from one of the available filesystem devices. A filesystem is a virtual, logical, or physical system for organizing, managing, and accessing the files and directories on devices such as SSDs, HDDs, or other storage devices.

Appendix A:

Software

After the X14SBSC motherboard has been installed, you can install the Operating System (OS), configure RAID settings, and install the drivers.

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 https://www.supermicro.com/support/manuals.

Installing the OS

1. Create a method to access the Microsoft Windows installation ISO file. That can be a USB flash or media drive, or the BMC KVM console.
2. Retrieve the proper drivers. 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 bootup.

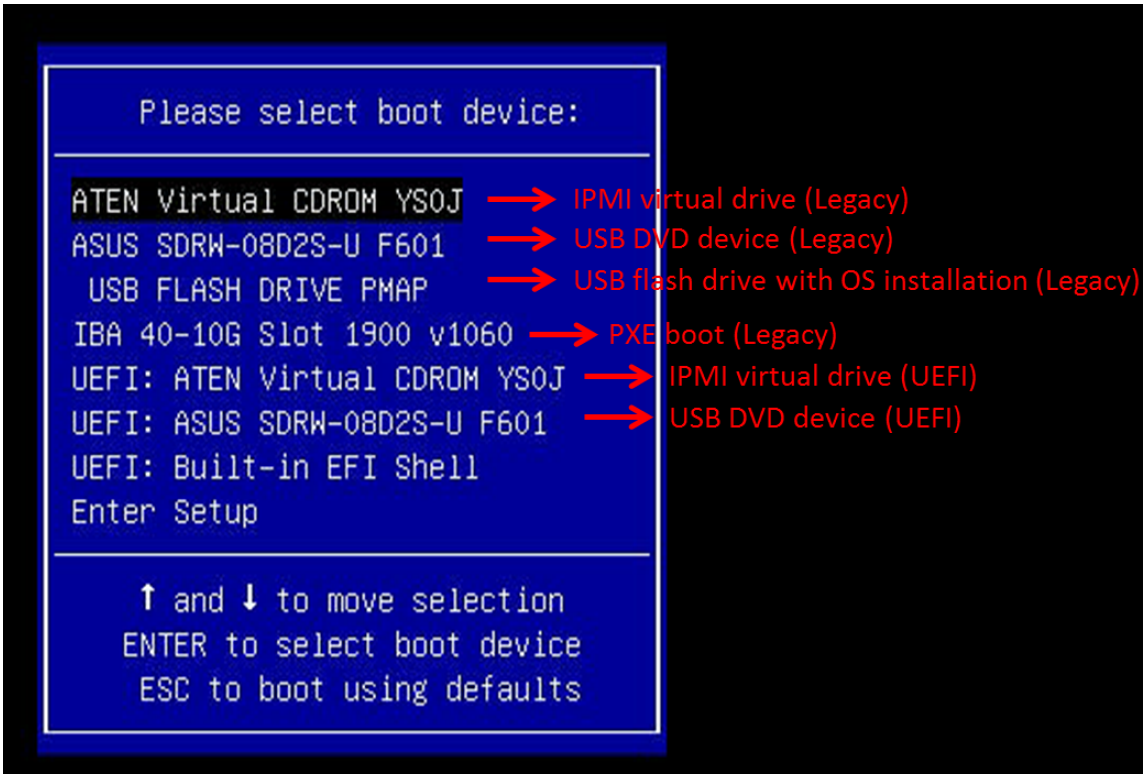


Figure A-1. Selecting the Boot Device

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

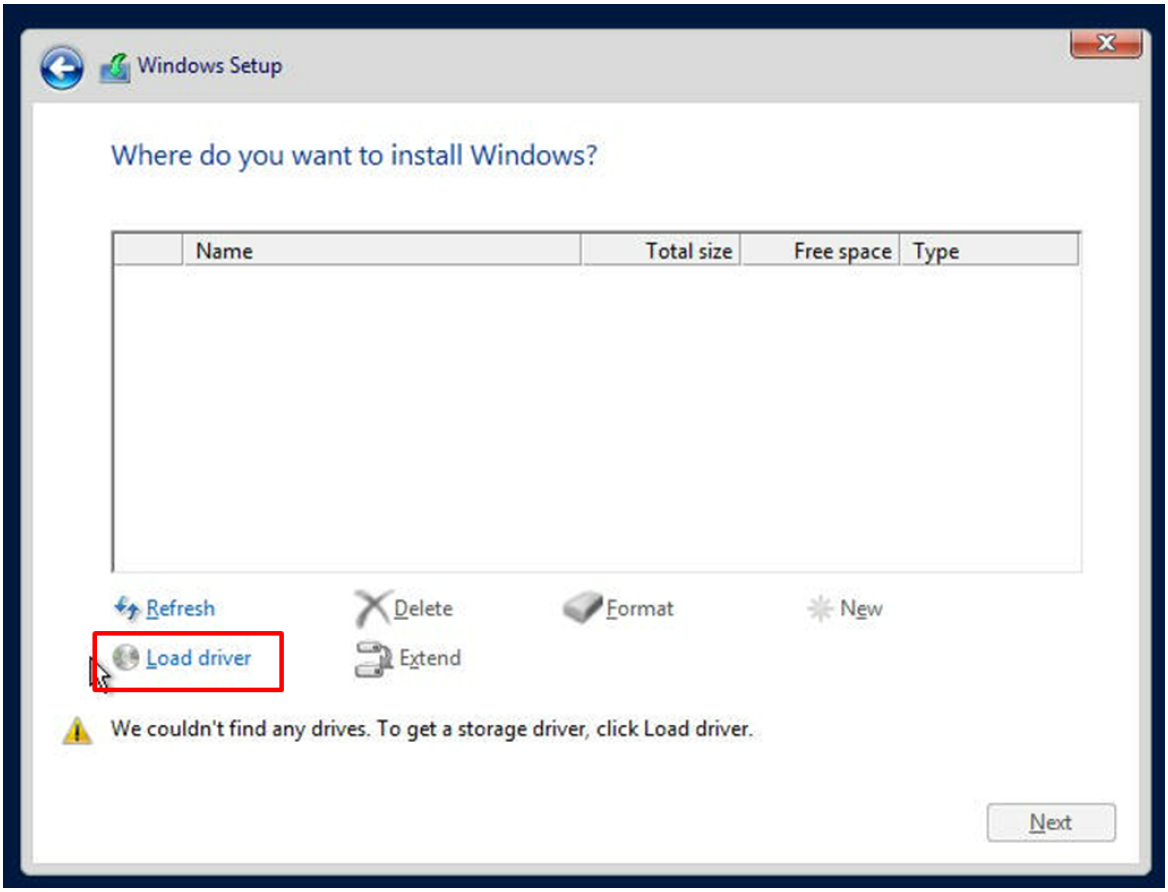


Figure A-2. Loading the Driver Link

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

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 for system updates.

Driver Installation

The Supermicro website contains drivers and utilities for your system at the following page:

https://www.supermicro.com/wdl.

Some of these drivers and utilities 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 or media drive. You may also use a utility to extract the ISO file if preferred.

Another option is to go to the Supermicro website at https://www.supermicro.com. Find the product page for your motherboard and download the latest drivers and utilities. Insert the flash drive or disk, and the screenshot shown below should appear.

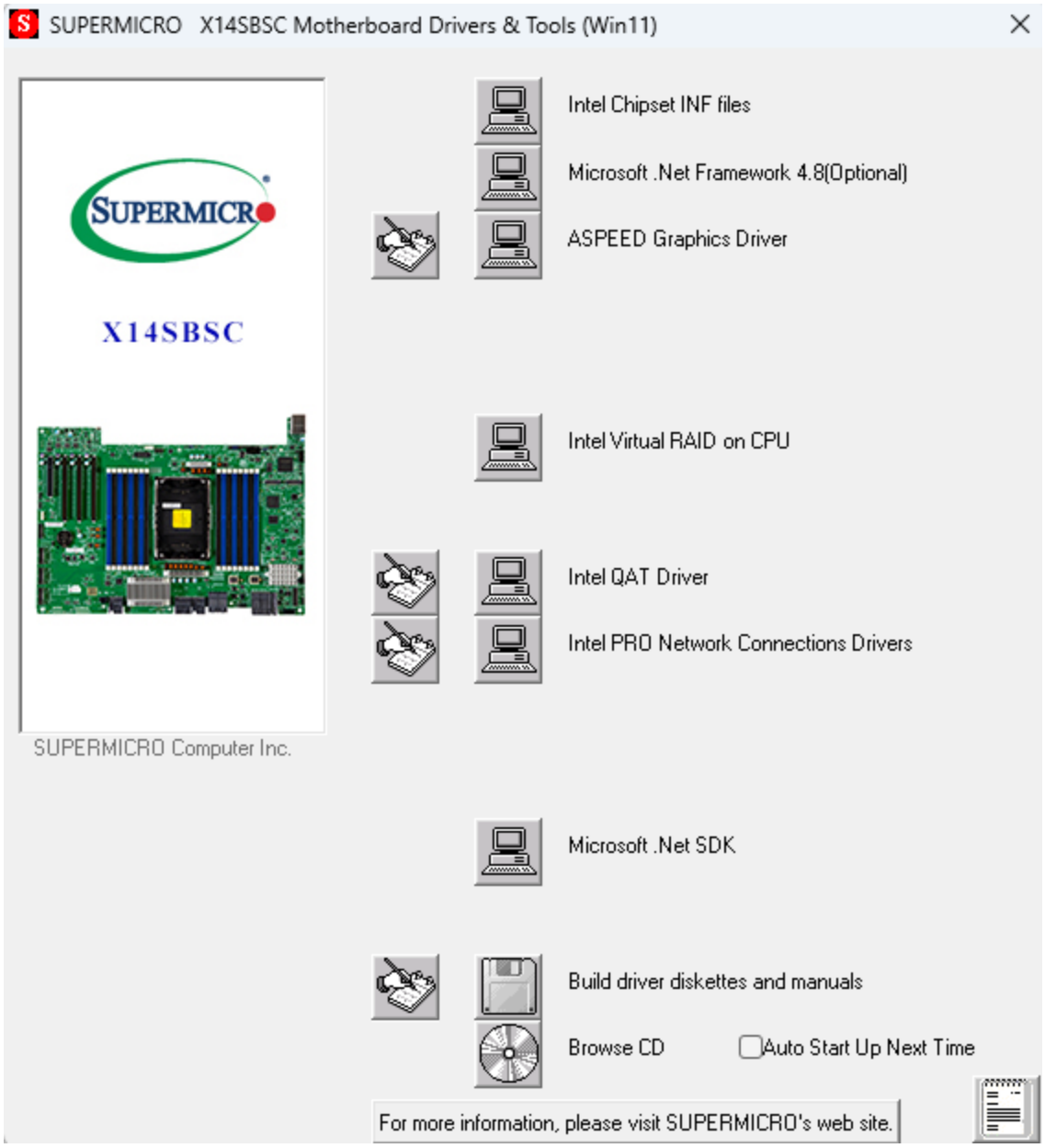


Figure A-3. Driver & Tools Installation Screen

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

BMC

The X14SBSC motherboard provides remote access, monitoring, and management through the baseboard management controller (BMC) and other management controllers distributed among different system modules. There are several BIOS settings that are related to BMC. For general documentation and information on BMC, visit our website at the following page:

https://www.supermicro.com/en/solutions/management-software/bmc-resources

BMC ADMIN User Password

For security, each system is assigned a unique default BMC password for the ADMIN user. The password can be found on a sticker on the motherboard and a sticker on the chassis, for Supermicro chassis. The sticker also displays the BMC MAC address. If necessary, the password can be reset using the Supermicro IPMICFG tool.



Figure A-4. BMC Password Label

Appendix B:

Standardized Warning Statements

The following statements are industry standard warnings, provided to warn the user of situations which have the potential for bodily injury. 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 in the Supermicro X14SBSC motherboard.

These warnings may also be found on our website at the following page:

https://www.supermicro.com/about/policies/safety_information.cfm

Battery Handling



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

تحذير! يوجد خطر حدوث انفجار إذا تم استبدال البطارية بنوع غير صحيح. استبدل البطارية بنفس النوع أو نوع مكافئ موصى به من قبل الشركة المصنعة فقط. يجب التخلص من البطاريات المستخدمة وفقًا لإرشادات الجهة المصنعة.

警告！ 如果更换的电池类型不正确，有爆炸危险。更换电池时，请使用制造商推荐的相同或同等型号的电池。请按制造商的说明处理废旧电池。

警告！ 如果更換的電池類型不正確。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。

Advarsel! Der er risiko for eksplosion, hvis batteriet skiftes med et batteri af den forkerte type. Batteriet må kun skiftes med et batteri af samme eller tilsvarende type, der anbefales af producenten. Opbrugte batterier skal bortskaffes i henhold til vejledningerne fra producenten.

Waarschuwing! Er bestaat een explosiegevaar als de batterij wordt vervangen door een onjuist type. Vervang de batterij alleen door hetzelfde type of een soortgelijk type aanbevolen door de fabrikant. Verwijder gebruikte batterijen overeenkomstig de instructies van de fabrikant.

Varoitus! Väärän tyyppisen akun käyttö voi aiheuttaa räjähdysvaaran. Vaihda akku vain valmistajan suosittelemaan samaan tai vastaavaan tyyppiseen akkuun. Hävitä käytetyt paristot valmistajan ohjeiden mukaisesti.

Attention! Il y a un risque d'explosion si la batterie est remplacée par une d'un type incorrect. Remplacez la batterie uniquement par une d'un type identique ou équivalent recommandé par le fabricant. Éliminez les batteries usagées conformément aux instructions du fabricant.

Warnung! Es besteht Explosionsgefahr, wenn die Batterie durch einen falschen Typ ersetzt wird. Ersetzen Sie die Batterie ausschließlich durch denselben oder einen vom Hersteller empfohlenen gleichwertigen Typ. Entsorgen Sie gebrauchte Batterien gemäß den Anweisungen des Herstellers.

אזהרה! קיימת סכנת פיצוץ אם הסוללה תוחלף בסוללה מסוג שגוי. החלף את הסוללה רק בסוללה מאותו סוג או בסוללה מקבילה המומלצת על ידי היצרן. השלך סוללות משומשות בהתאם להוראות היצרן.

चेतावनी! यदि बैटरी को गलत प्रकार से बदला जाता है तो विस्फोट का जोखिम है। बैटरी को केवल निर्माता द्वारा अनुशंसित समान या समकक्ष प्रकार से ही बदलें। इस्तेमाल की गई बैटरियों का निपटान निर्माता के निर्देशों के अनुसार करें।

警告！ 電池を間違ったタイプに交換すると爆発する危険があります。交換する電池はメーカーが推奨するタイプ、または同等のものを使用してください。使用済み電池は、メーカーの指示に従って廃棄してください。

경고!배터리를 잘못된 종류로 교체하면 폭발의 위험이 있습니다. 기존 배터리와 동일하거나 제조사에서 권장하는 동등한 종류의 배터리로만 교체해야 합니다. 제조사의 안내에 따라 사용된 배터리를 처리하여 주십시오.

Advarsel! Det er fare for eksplosjon hvis batteriet byttes ut med et av feil type. Batterier skal kun byttes ut med et av lik eller tilsvarende type, som anbefalt av produsenten. Kast brukte batterier i henhold til produsentens instruksjoner.

¡Advertencia! Existe riesgo de explosión si se sustituye la batería por una de tipo incorrecto. Reemplace la batería únicamente con el mismo tipo o uno equivalente recomendado por el fabricante. Deseche las baterías usadas de acuerdo con las instrucciones del fabricante.

Varning! Det finns risk för explosion om batteriet byts ut mot en felaktig typ. Byt endast ut batteriet mot ett batteri av samma eller likvärdig typ som rekommenderas av tillverkaren. Kassera förbrukade batterier i enlighet med tillverkarens anvisningar.

Connection to Earth



Warning! Equipment shall be connected to an Earth mains socket-outlet.

تحذير! يجب توصيل الأجهزة بمقبس كهربائي أرضي.

警告！ 设备应连接到接地电源插座。

警告！ 應將設備連接至接地電源插座。

Advarsel! Dette udstyr skal sluttes til en jordforbundet stikkontakt.

Waarschuwing! De apparatuur moet worden aangesloten op een geaard netstopcontact.

Varoitus! Laitteet on kytkettävä maadoitettuun pistorasiaan.

Attention! L'équipement doit être connecté à une prise de courant avec mise à la terre.

Warnung! Das Gerät muss an eine geerdete Netzsteckdose angeschlossen werden.

אזהרה! יש לחבר את הציוד לשקע חשמל עם הארקה.

चेतावनी! उपकरण को एक अर्थ मेन्स सॉकेट-आउटलेट से जोड़ा जाना चाहिए।

警告！ 機器は、接地主電源コンセントに接続するものとします。

경고! 장비는 접지된 전원 콘센트에 연결해야 합니다.

Advarsel! Utstyret skal kobles til en jordet stikkontakt.

¡Advertencia! El equipo deberá conectarse a una toma de corriente con conexión a tierra.

Varning! Utrustningen ska vara ansluten till ett jordat eluttag.

Product Disposal

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

تحذير! يجب التخلص النهائي من هذا المنتج وفقًا لجميع القوانين واللوائح الوطنية.

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。

Advarsel! Dette produkt skal bortskaffes i henhold til alle nationale love og regler.

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

Varoitus! Tämän tuotteen lopullinen hävittäminen on suoritettava kaikkien kansallisten lakien ja määräysten mukaisesti.

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.

Warnung! Die endgültige Entsorgung dieses Produkts muss gemäß allen nationalen Gesetzen und Vorschriften erfolgen.

אזהרה! סילוק סופי של מוצר זה חייב להתבצע בהתאם לכל החוקים והתקנות הלאומיים.

चेतावनी! इस उत्पाद का अंतिम निपटान सभी राष्ट्रीय कानूनों और नियमों के अनुसार किया जाना चाहिए।

警告！ 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。

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

Advarsel! Når produktet til slutt skal kasseres, må det håndteres i henhold til alle nasjonale lover og forskrifter.

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

Varning! Slutgiltigt bortskaffande av denna produkt ska ske i enlighet med alla nationella lagar och förordningar.