X14SRG-TF

USER'S MANUAL

Revision 1.0 (MNL-2877)

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 1.0

Release Date: May 29, 2026

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 X14SRG-TF 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 12
- 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

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

For details on the X14SRG-TF motherboard layout, features, and other quick reference information, refer to the content below.

Motherboard Layout

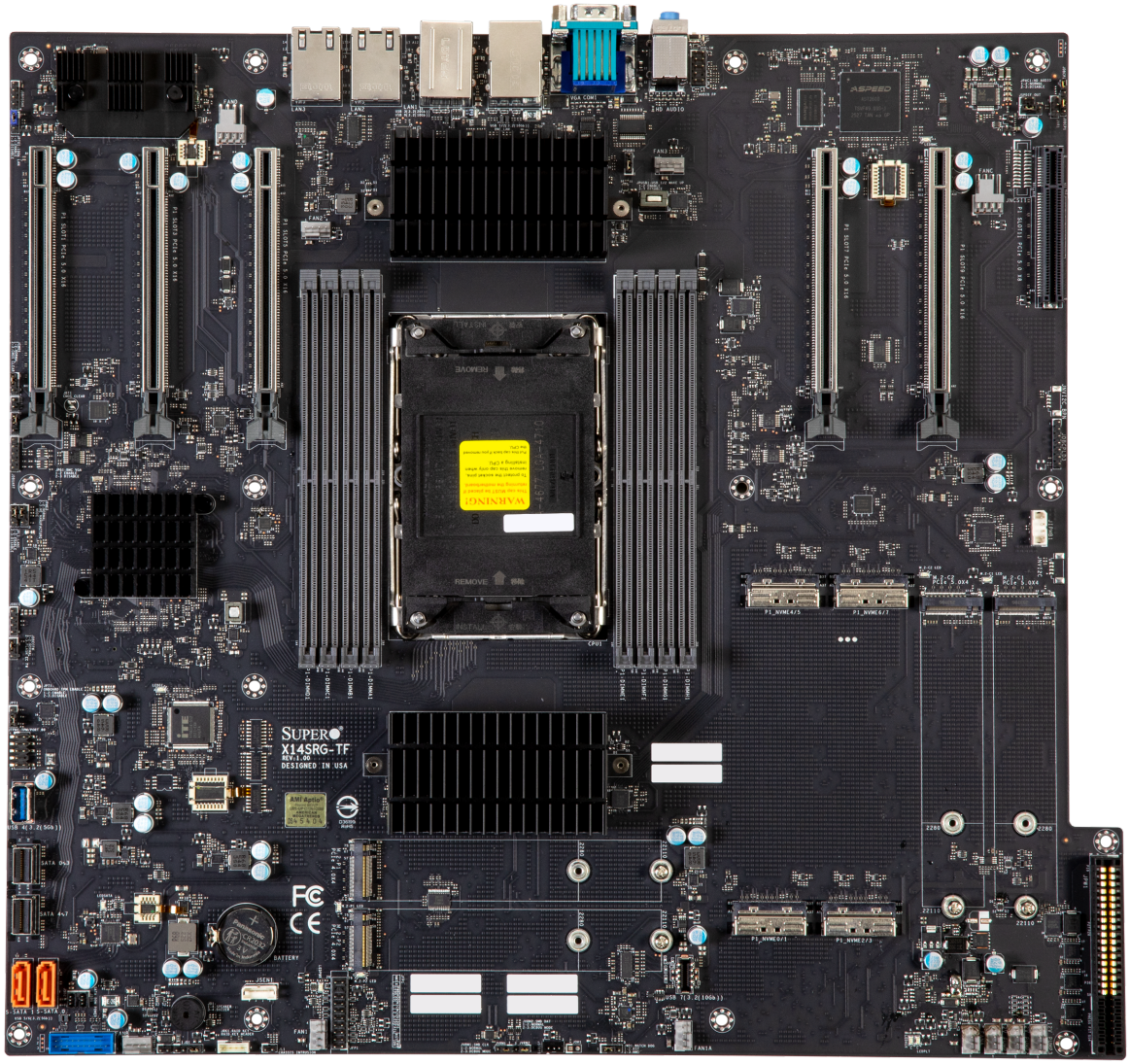
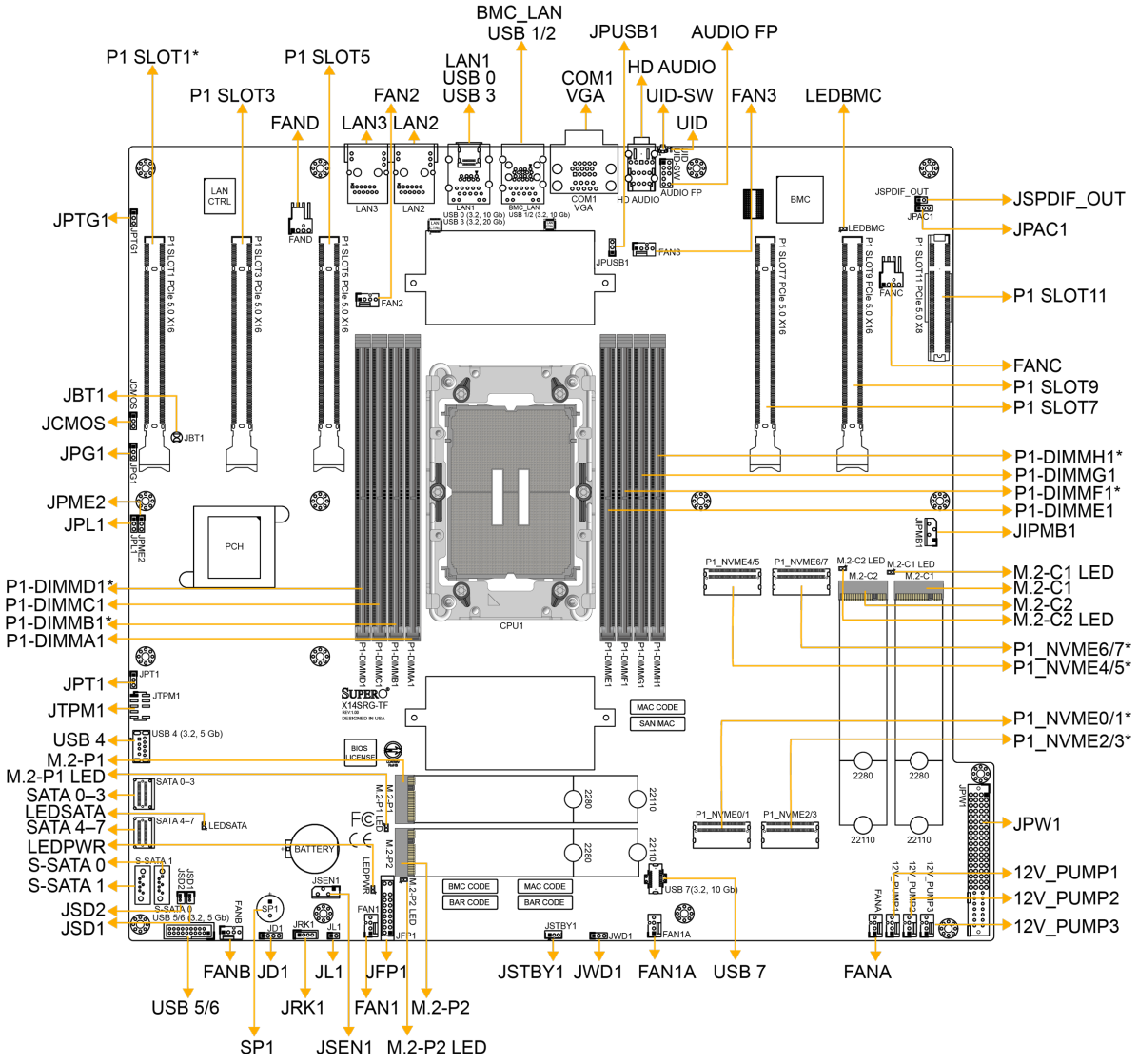


Figure 1-1. X14SRG-TF Motherboard Image



Notes:

- The slots/connectors marked with an asterisk (*) are supported only by Intel® Xeon® 690/670/650 Series processors.
- Intel Xeon 690/670/650 Series processors support all eight DIMM slots. Intel Xeon 630 Series processors only support slots DIMMC1, DIMMA1, DIMME1, and DIMMG1.

Figure 1-2. X14SRG-TF Motherboard Layout

Notes:

- For detailed information on jumpers, connectors, and LED indicators, see "Component Installation" on page 29.
- "■" 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
JBT1	Clear CMOS (Onboard)	Short Pads to Clear CMOS
JCMOS	Clear CMOS (Onboard)	Pins 1–2 (Normal)
JPAC1	HD Audio Normal/Disable	Pins 1–2 (Normal)
JPG1	BMC VGA Enable/Disable	Pins 1–2 (Enabled)
JPL1	LAN1 Enable/Disable	Pins 1–2 (Enabled)
JPME2	Intel Manufacturing Mode	Pins 1–2 (Normal)
JPT1	Onboard TPM 2.0 Enable/Disable	Pins 1–2 (Enabled)
JPTG1	LAN2/3 Enable/Disable	Pins 1-2 (Enabled)
JPUSB1	USB1/2 Standby Power	Pins 1–2 (Enabled)
JWD1	Watchdog Function Enable	Pins 1–2 (Reset)

LED	Description	Status
LEDBMC	BMC Heartbeat LED	Blinking Green: BMC Normal (Active) Solid Green: During a Cold Reboot
LEDPWR	Onboard Power LED	Solid Green: Power On
LEDSATA	S-SATA 0/ S-SATA 1 Access LED	Blinking Green: SATA Device Being Accessed
M.2-C1/M.2-C2 LED	M.2 LEDs for M.2-C1, M.2-C2	Blinking Green: Device Working
M.2-P1/M.2-P2 LED	M.2 LEDs for M.2-P1, M.2-P2	Blinking Green: Device Working
UID	Unit Identifier (UID) LED	Solid Blue: Unit Identified

Connector	Description
12V_PUMP1–3	12V 4-pin Power Headers for CPU Liquid Cooling Pump
AUDIO FP	Front Panel Audio Header
BATTERY	Onboard Battery

Connector	Description
BMC_LAN	Dedicated BMC 1 GbE LAN Port
COM1	Rear COM Port
FAN1–3	CPU Fan Headers
FAN1A, FANA–D	System Fan Headers *FANB and FAND support +12 V standby power
HD AUDIO	High Definition Audio Ports
JD1	Speaker/Buzzer Header
JFP1	Front Control Panel Header
JIPMB1	4-pin BMC External I^2C Header
JL1	Chassis Intrusion Header
JPW1	Power Distribution Board Slot
JRK1	Intel VROC Key Header
JSD1, JSD2	SATA DOM (Disk-On-Module) Power Connectors
JSEN1	Inlet Sensor Header
JSPDIF_OUT	Sony/Philips Digital Interface (S/PDIF) Out Header
JSTBY1	Standby Power Header (5 V)
JTPM1	Trusted Platform Module (TPM)/Port 80 Header (TPM 2.0 only)
LAN1	RJ45 1 GbE LAN Port (with support of Intel vPro®)
LAN2, LAN3	RJ45 10 GbE LAN Ports
M.2-C1, M.2-C2	PCIe 5.0 x4 M.2 M-key Slots (from CPU, with support of 2280/22110 form factors and RAID 0/1)
M.2-P1, M.2-P2	PCIe 4.0 x4 M.2 M-key Slots (from PCH, with support of 2280/22110 form factors)
P1 SLOT1/3/5/7/9	PCIe 5.0 x16 slots (from CPU) *Only Intel Xeon 690/670/650 Series processors support SLOT1, and SlOT1 supports single-width graphics cards only. **Supports up to four double-width FHFL graphics cards (SLOT3/5/7/9) or two triple-width FHFL graphics cards (SLOT5/9) (FHFL: Full-Height, Full-Length).

Connector	Description
P1 SLOT11	PCIe 5.0 x8 slot (from CPU) *SLOT11 supports both single-width and double-width graphics cards.
P1_NVME0/1, P1_ NVME2/3, P1_NVME4/5, P1_NVME6/7	PCIe 5.0 x8 MCIO Connectors (from CPU), providing up to eight NVMe connections with RAID 0/1/5/10 support *Supported by Intel Xeon 690/670/650 Series processors only.
SATA 0–3, SATA 4–7	PCIe 4.0 x8 SlimSAS 4i Vertical Connectors (from PCH), providing up to eight SATA 3.0 connections with RAID 0/1/5/10 support
S-SATA 0, S-SATA 1	SATA 3.0 Ports with support of SuperDOM devices * DOM: Disk on Module
SP1	Internal Speaker/Buzzer
UID-SW	Unit Identifier (UID) Button
USB 0	Rear USB 3.2 Gen 2x1 Port (10 Gb, Type-A)
USB 1/2	Rear USB 3.2 Gen 2x1 Ports (10 Gb, Type-A)
USB 3	Rear USB 3.2 Gen 2x2 Port (20 Gb, Type-C)
USB 4	Internal USB 3.2 Gen 1 Connector (5 Gb, vertical, Type-A)
USB 5/6	Front-accessible USB 3.2 Gen 1 Header (5 Gb)
USB 7	Front-accessible USB 3.2 Gen 2x1 Connector (10 Gb, Type-C)
VGA	VGA Port supported by BMC

Motherboard Features

Motherboard Features
Processor
• Supports a single Intel Xeon 600 Series processor (in LGA 4710-2/Socket E2), with up to 86 cores and a thermal design power (TDP) of up to 350 W for Intel Xeon 690/670/650 Series processors, and up to 16 cores and a TDP of up to 180 W for Intel Xeon 630 Series processors. **Note:** The processor TDP is subject to chassis and heatsink cooling restrictions. For proper thermal management, check the chassis and heatsink specifications for proper TDP sizing.

Motherboard Features
Memory
• Support up to 1 TB of ECC RDIMM and 2 TB 3DS RDIMM with speeds of up to 6400 MT/s (1DPC), or 512 GB of ECC MCRDIMM (1DPC) with speeds of up to 8000 MT/s (1DPC) in eight DDR5 DIMM slots for Intel Xeon 690/670/650 Series processors • Supports up to 512 GB of ECC RDIMM and 1 TB of 3DS RDIMM with speeds of up to 6400 MT/s (1DPC) in four DDR5 DIMM slots for Intel Xeon 630 Series processors **Note:** DPC stands for DIMMs per Channel. Memory speed and capacity support depends on the processor used in the system.
DIMM Size
• 16 GB, 24 GB, 32 GB, 48 GB, 64 GB, 96 GB, 128 GB, and 256 GB
Chipset
• Intel PCH W890
Network Controller
• Intel Ethernet i219-LM (LAN1, 1 GbE, with support of Intel vPro) • Intel Ethernet E610-XT2 (LAN2 and LAN3, 10 GbE)
Baseboard Management Controller (BMC)
• ASPEED AST2600 BMC supporting one VGA port and one dedicated BMC LAN port (BMC_LAN, 1 GbE)
Audio
• Realtek ALC888S (7.1 HD Audio ports)

Motherboard Features
Expansion Slots

• Five PCIe 5.0 x16 slots (P1 SLOT1/3/5/7/9) and one PCIe 5.0 x8 slot (P1 SLOT11)
Notes:
  • Only Intel Xeon 690/670/650 Series processors support P1 SLOT1, and P1 SlOT1 supports single-width graphics cards only.
  • Supports up to four double-width FHFL graphics cards (SLOT3/5/7/9) or two triple-width FHFL graphics cards (P1 SLOT5/9)
  • P1 SlOT11 supports both single-width and double-width graphics cards.
• Two PCIe 5.0 x4 M.2 M-Key slots (from CPU, with support of 2280 and 22110 form factors and RAID 0/1)
• Two PCIe 4.0 x4 M.2 M-Key slots (from PCH, with support of 2280 and 22110 form factors)
• Four PCIe 5.0 x8 MCIO connectors, providing up to eight NVMe connections with RAID 0/1/5/10 support, for Intel Xeon 690/670/650 Series processors only)

I/O Devices
• One serial port on the rear I/O (COM1) • Two SATA 3.0 ports at 6 Gb/s (S-SATA 0 and S-SATA 1, with support of SuperDOM devices) • Two PCIe 4.0 x8 SlimSAS 4i connectors (SATA 0–3 and SATA 4–7, providing up to eight SATA 3.0 connections with RAID 0/1/5/10 support) • One VGA connection on the rear I/O • 7.1 HD audio ports on the rear I/O
Peripheral Devices
• Three USB 3.2 Gen 2x1 ports on the rear I/O (USB 0 and USB 1/2, 10 Gb, Type-A,) • One USB 3.2 Gen 2x2 port on the rear I/O (USB 3, 20 Gb, Type-C) • One internal USB 3.2 Gen 1 connector (USB 4 , 5 Gb, vertical, Type-A) • One front-accessible USB 3.2 Gen 1 header (USB 5/6, 5 Gb, for two Type-A connections) • One front-accessible USB 3.2 Gen 2x1 header (USB 7, 10 Gb, for one Type-C connection)
BIOS
• AMI 64 MB 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 or later

Motherboard Features
Power Management
• ACPI power management • Power button override mechanism • Power-on mode for AC power recovery • Wake-on-LAN • Power supply monitoring
System Health Monitoring
• Onboard voltage monitoring for +5 V, +3.3 V, +12 V, +5 V stdby, +3.3 V stdby, +0.82V PCH, +1.8 V PCH, and +1.05 V PCH • Onboard temperature monitoring for VBAT, CPU, VRM, LAN, PCH, system, and memory • Five CPU switch phase voltage regulators • CPU thermal trip support • Platform Environment Control Interface (PECI)/TSI
Fan Control
• Triple cooling zones • Multi-speed fan control via Embedded Controller • 11 4-pin fan headers (Up to 11 fan headers)
System Management
• SuperServer Automation Assistant (SAA) • Trusted Platform Module (TPM) support • Chassis intrusion header and detection **Note:** Connect a cable from the Chassis Intrusion header at JL1 to the chassis to receive an alert.
LED Indicators
• BMC Heartbeat LED • LAN LEDs (on LAN ports) • M.2 LEDs • Onboard Power LED • SATA Access LED • UID LED

Motherboard Features
Dimensions
Proprietary form factor in 14.6" x 15.9" (370.8 mm × 403.9 mm) (L x W)

Motherboard Block Diagram

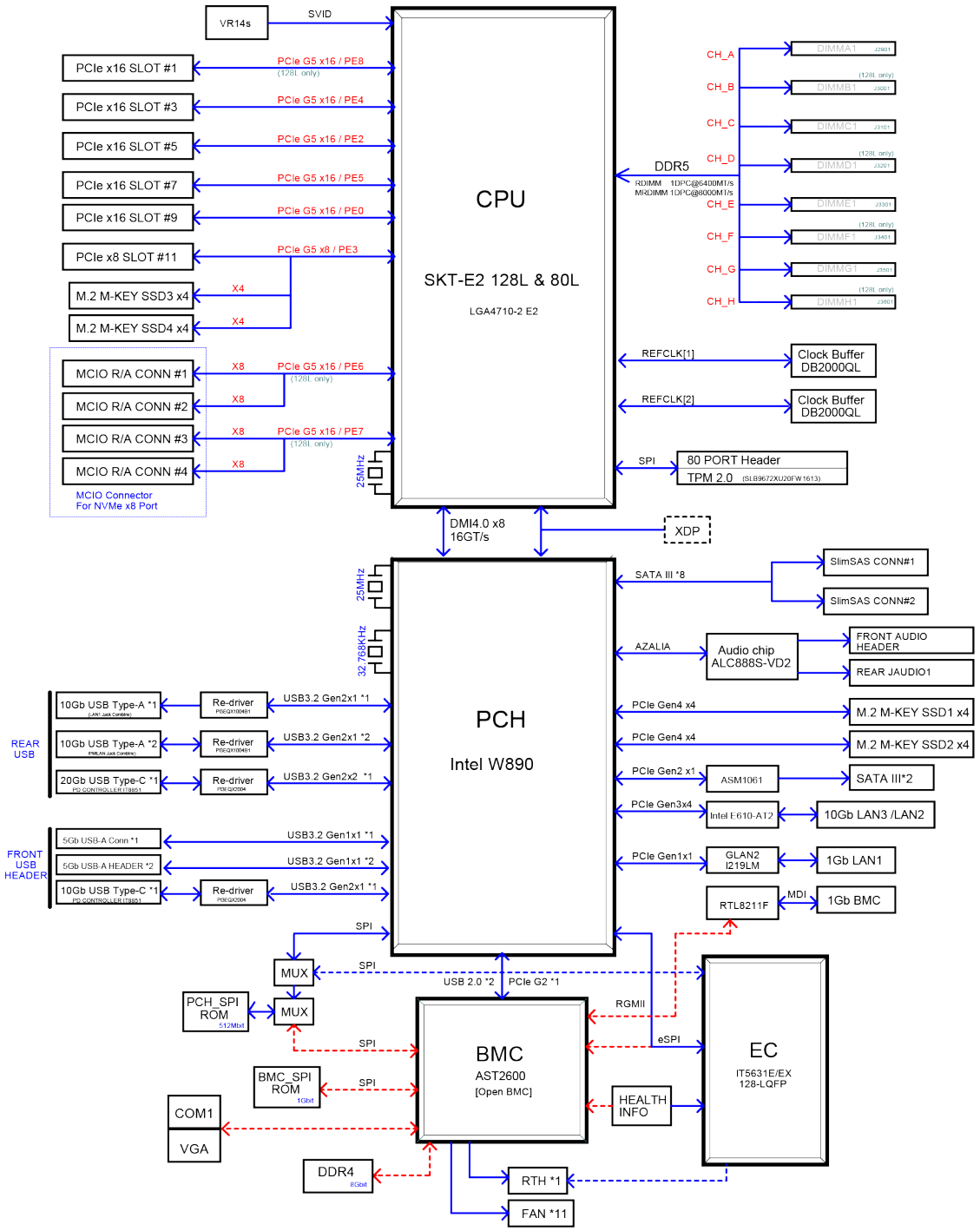


Figure 1-3. X14SRG-TF Motherboard Block Diagram

1.2 Platform Overview

Built upon the functionality and capability of the Intel Xeon 600 Series processors (in LGA 4710-2/Socket E2) and the Intel 800 Series chipset, the X14SRG-TF motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users.

With the support of the new Intel Microarchitecture 20A Enhanced SuperFin Process Technology, the X14SRG-TF motherboard dramatically increases system performance for a multitude of system applications and supports the following features:

- DDR5 288-pin memory support
- Direct Media Interface
- Intel Matrix Storage Technology and Intel Rapid Storage Technology
- Intel I/O Virtualization (VT-d) Support
- Intel Trusted Execution Technology Support
- PCIe 5.0 Interface (up to 32 GT/s)
- SATA Controller (up to 6 Gb/sec)
- Advanced Host Controller Interface (AHCI)

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 108 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 and an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures while providing a processor architecture-independent implementation that is compatible with operating systems such as Microsoft Windows, Red Hat Linux, and Ubuntu Linux. For detailed information about our certified operating systems, refer to OS Compatibility.

1.6 Embedded Controller

The Embedded Controller supports one high-speed, 16550 compatible serial communication port (UART). Each UART includes a 16-byte send/receive FIFO, a programmable baud rate generator, complete modem control capability and a processor interrupt system. The UART supports speeds with a baud rate of 115.2 Kbps, 57.6 Kbps, 38.4 Kbps, 19.2 Kbps, and 9.6 Kbps.

The Embedded Controller provides functions that comply with Advanced Configuration and Power Interface (ACPI), which includes support of legacy and ACPI power management through an SMI or SCI function pin. It also features auto power management to reduce power consumption.

Chapter 2:

Component Installation

This chapter provides instructions on installing and replacing main system components for the X14SRG-TF 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

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

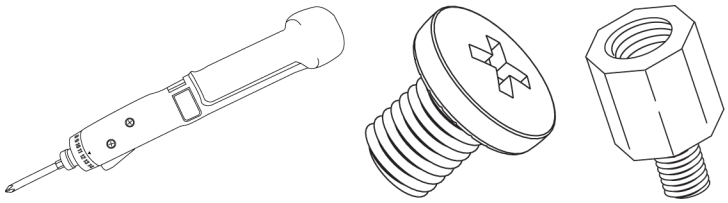


Figure 2-1. Torque Driver (1), Phillips Screws (15), Standoffs (15, only if needed)

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.

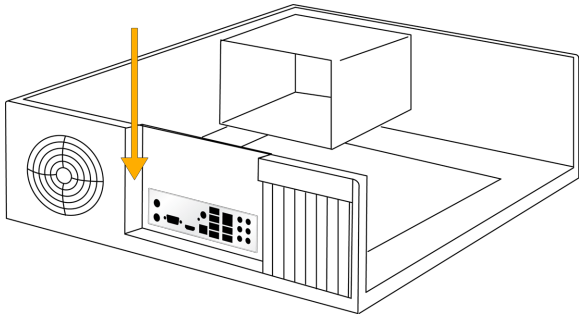


Figure 2-2. Installing the I/O Shield

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.

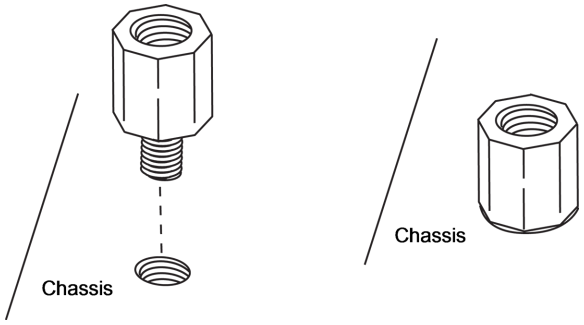


Figure 2-3. Locating the Mounting Holes

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

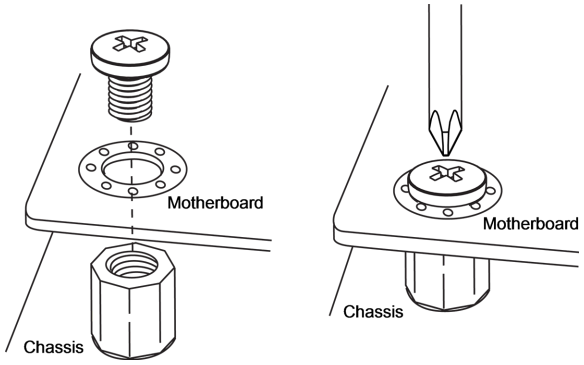


Figure 2-4. Aligning the Mounting Holes

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.

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 31.
- 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

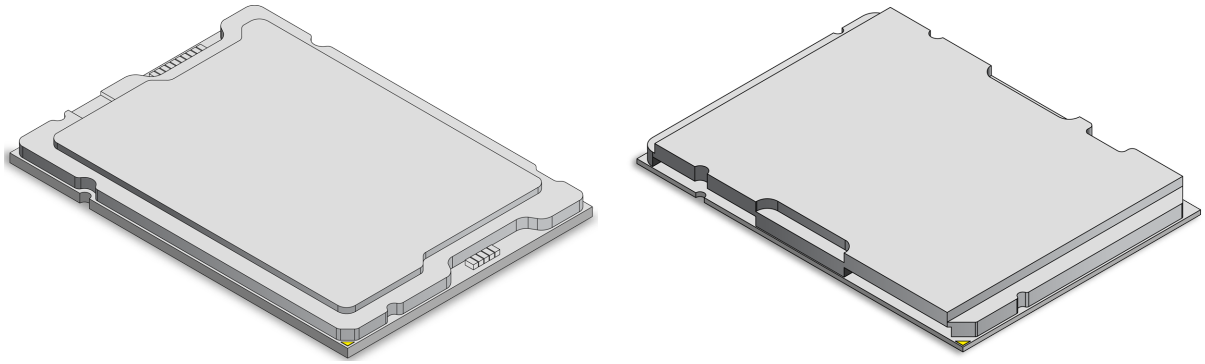


Figure 2-5. Processor (SP XCC left, SP HCC/LCC right)

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

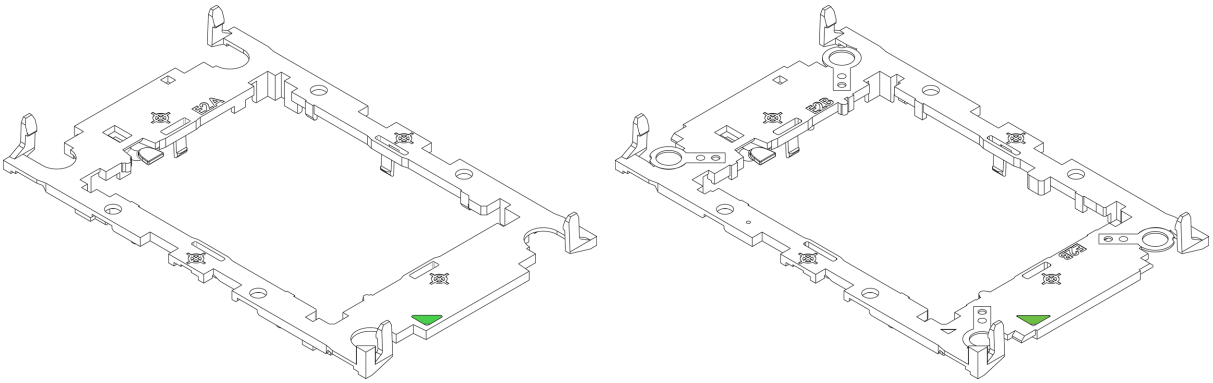


Figure 2-6. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)

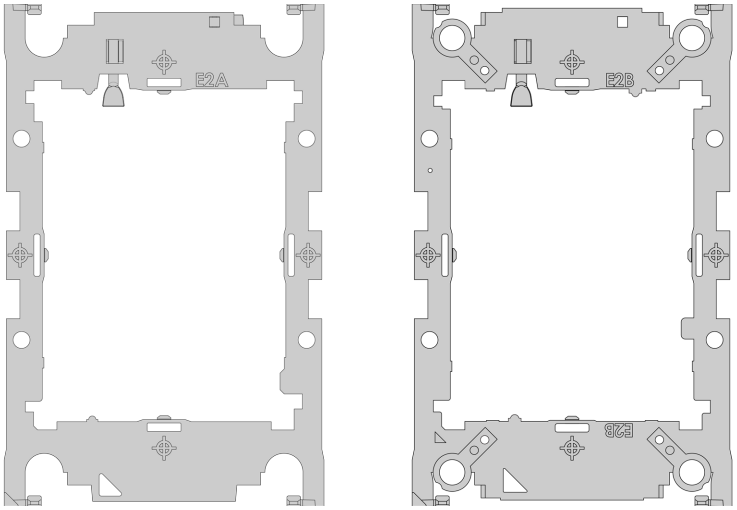


Figure 2-7. Carrier Top View (SP XCC E2A left, SP HCC/LCC E2B right)

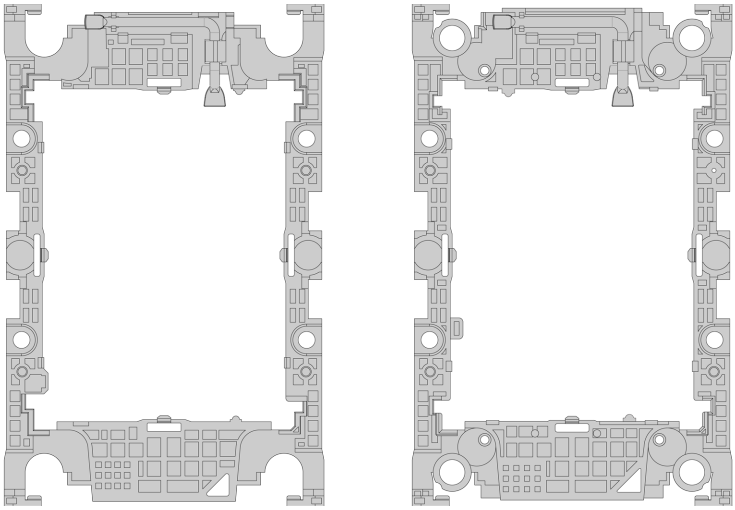


Figure 2-8. Carrier Bottom View (SP XCC E2A left, SP HCC/LCC E2B right)

Overview of the Processor Socket

The processor socket is protected by a plastic protective cover.

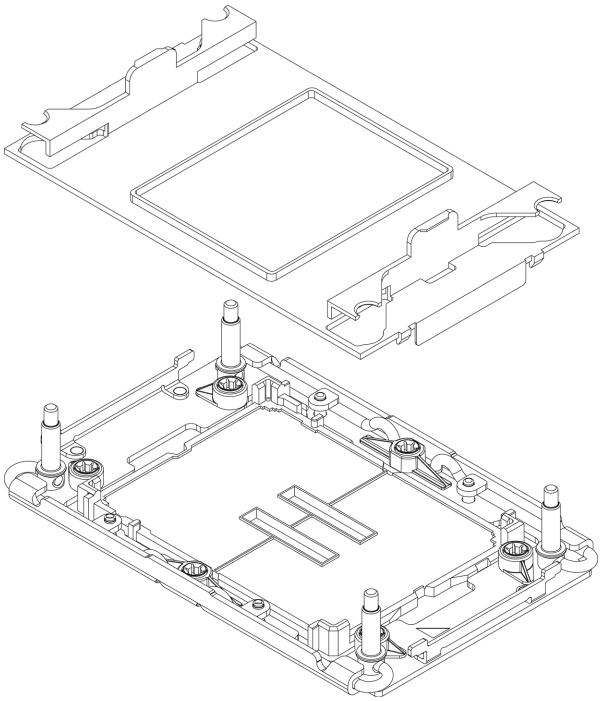


Figure 2-9. Plastic Protective Cover and Processor Socket

Overview of the Processor Heatsink Module

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

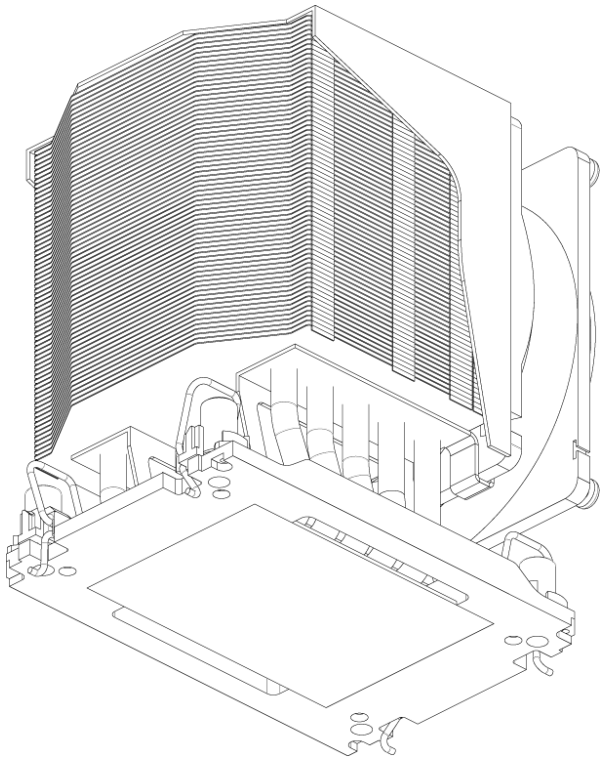


Figure 2-10. Heatsink (4U)

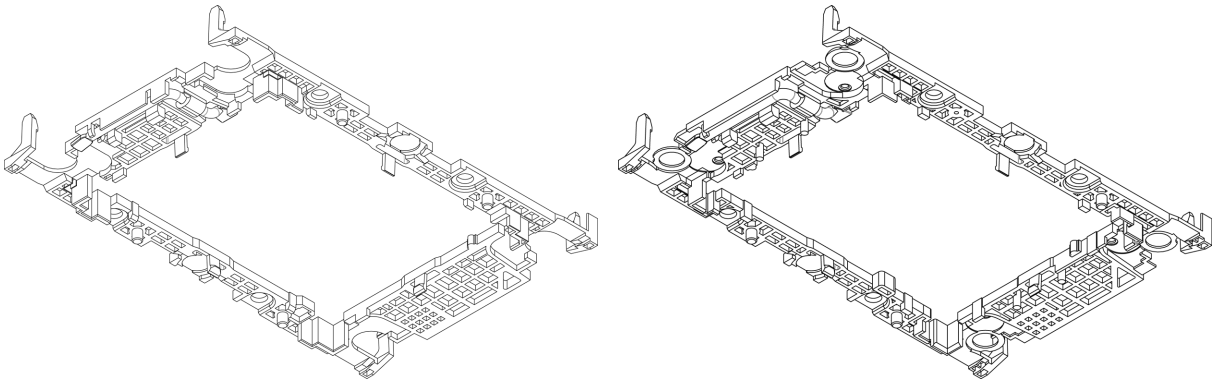


Figure 2-11. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)

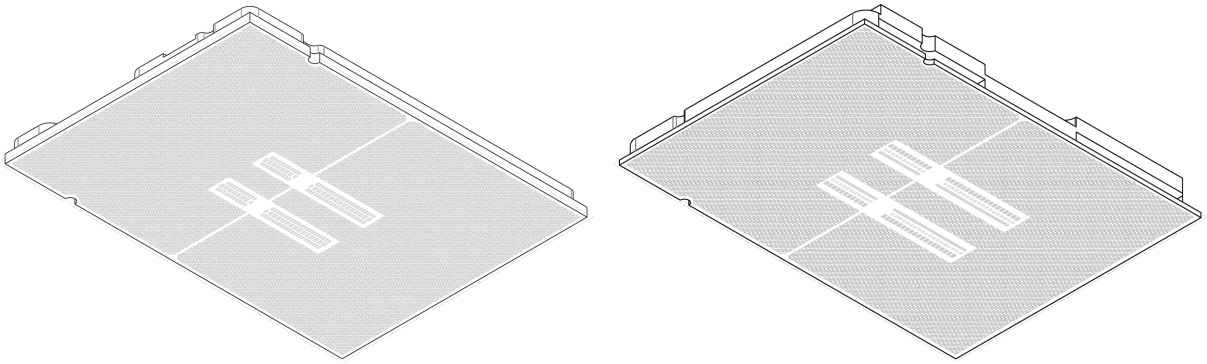


Figure 2-12. Processor (SP XCC E2A left, SP HCC/LCC E2B right)

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.

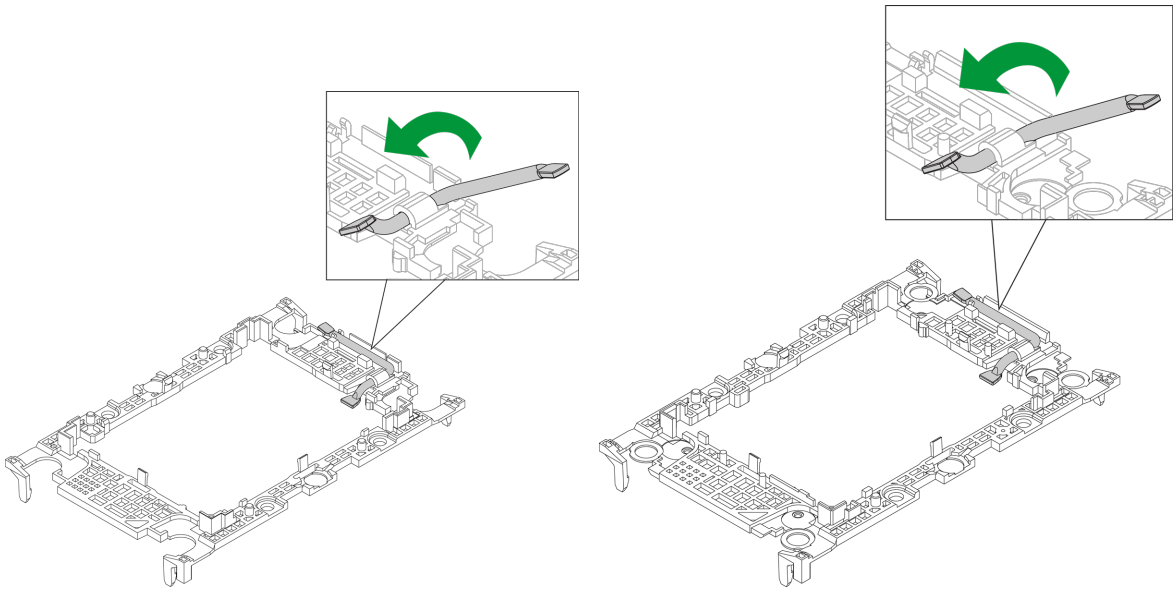


Figure 2-13. Carrier Lever (SP XCC left, SP HCC/LCC right)

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.

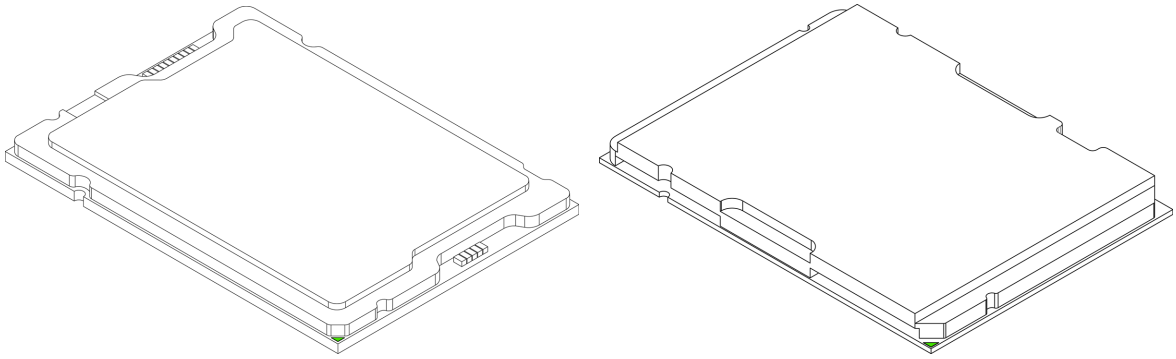


Figure 2-14. Processor (SP XCC E2A left, SP HCC/LCC E2B right)

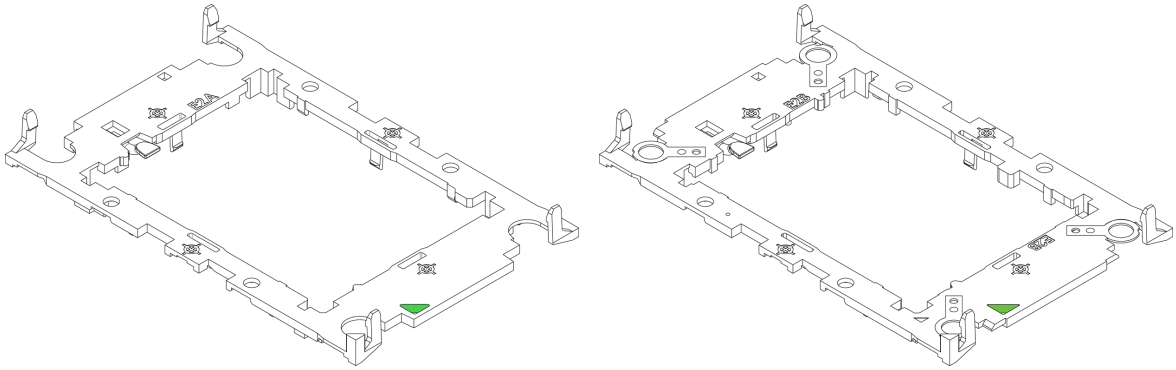


Figure 2-15. Carrier (SP XCC E2A left, SP HCC/LCC E2B right)

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.

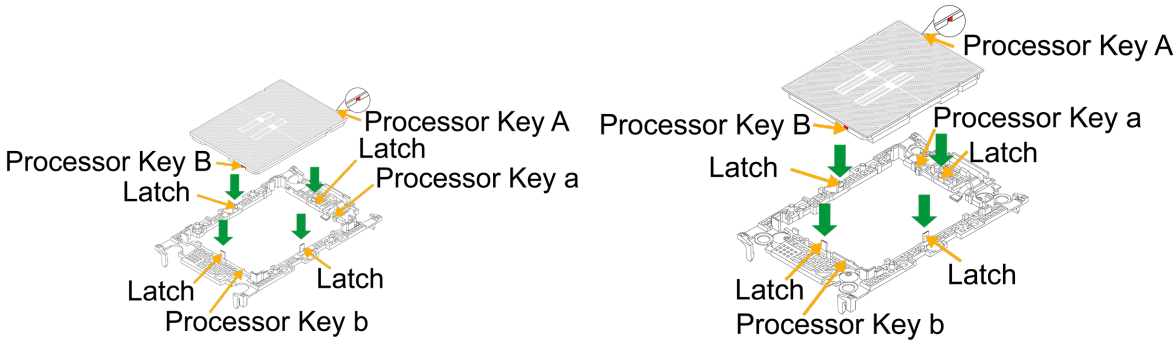


Figure 2-16. Keys and Latches Locations (SP XCC E2A left, SP HCC/LCC E2B right)

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

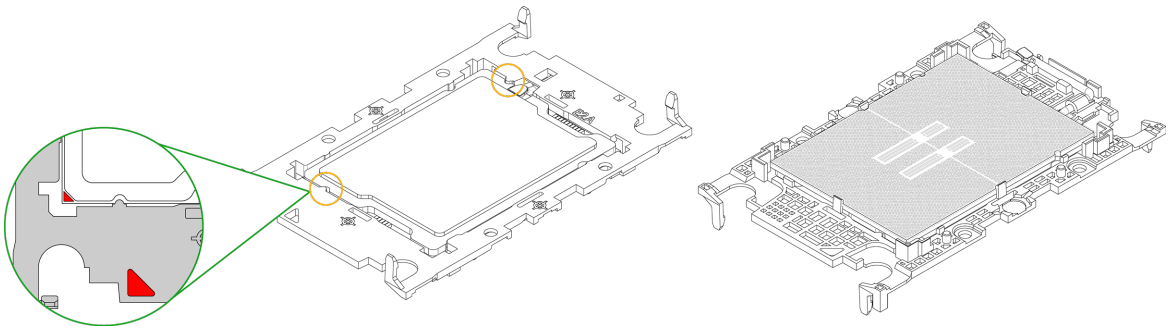


Figure 2-17. SP XCC E2A Keys and Latches

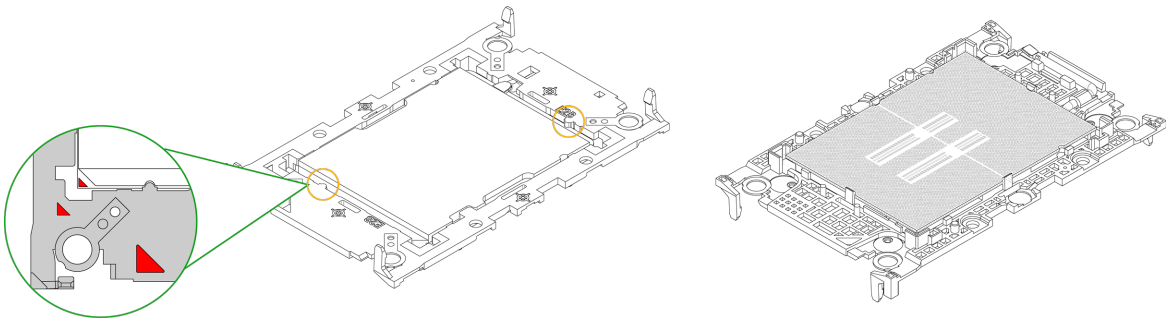


Figure 2-18. SP HCC/LCC E2B Keys and Latches Together

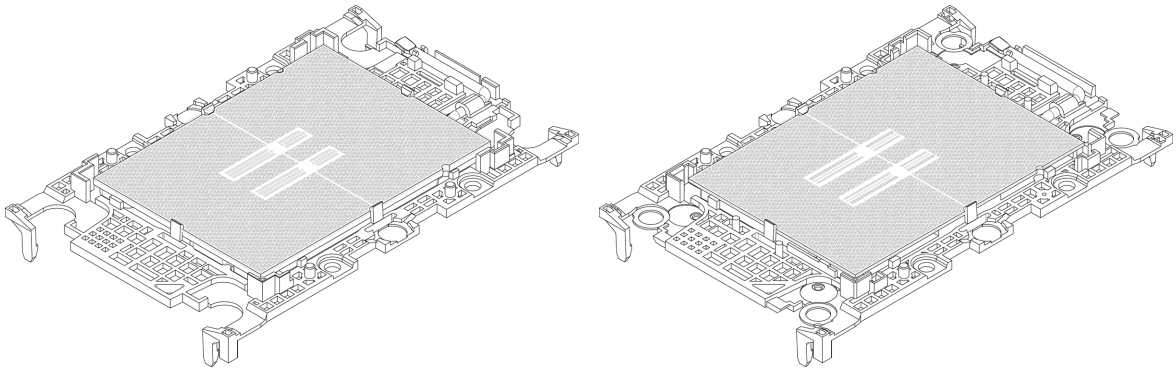


Figure 2-19. Carrier Assembly Completed (SP XCC E2A left, SP HCC/LCC E2B right)

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. Loosen the Torx screw from the heatsink.

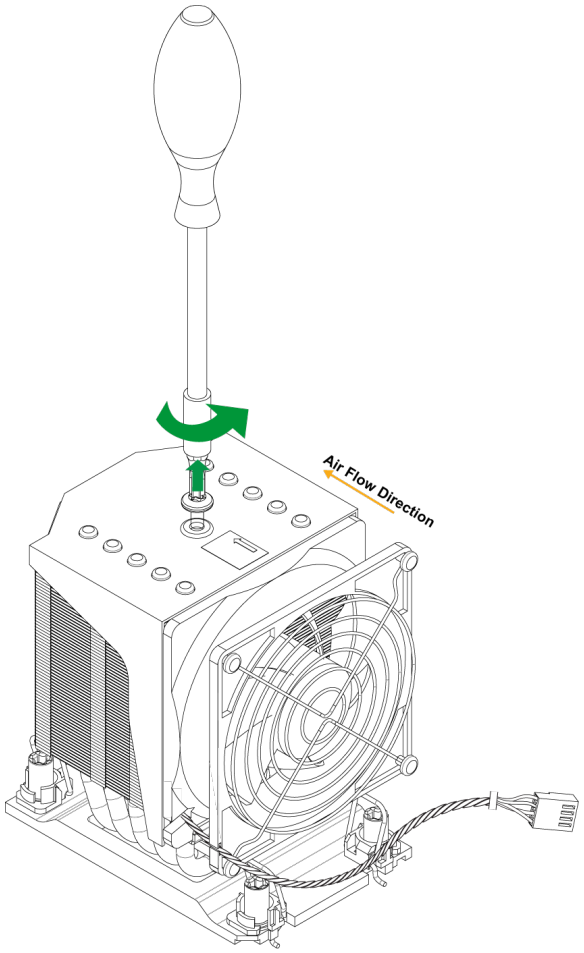


Figure 2-20. Loosening the Screw

2. Gently pull the heatsink fan upward to detach it from the heatsink.

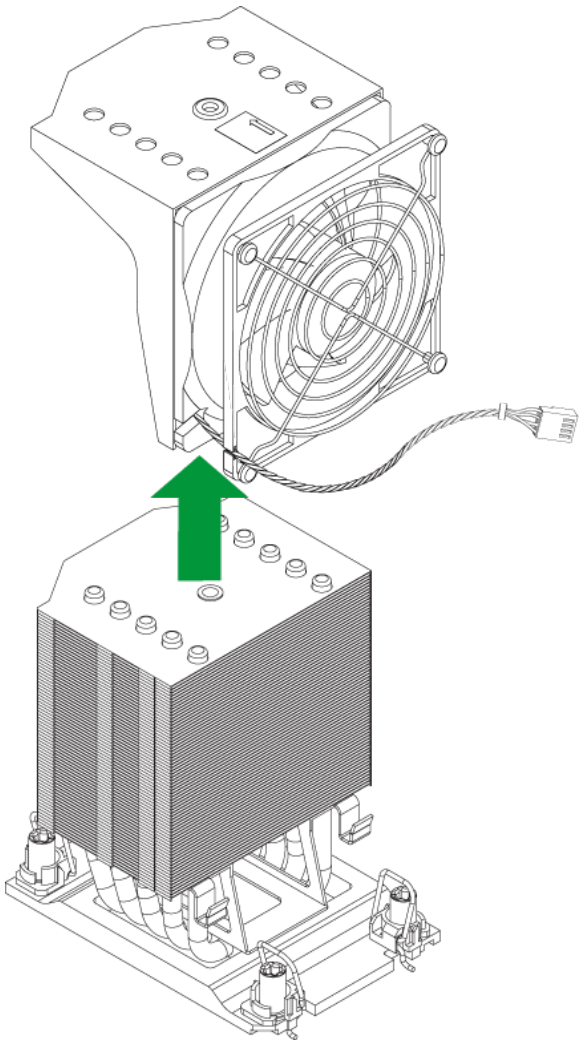


Figure 2-21. Heatsink Fan Detached

3. 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.
4. If this is a new heatsink, the thermal grease has been pre-applied. Otherwise, apply the proper amount of thermal grease.
5. 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.

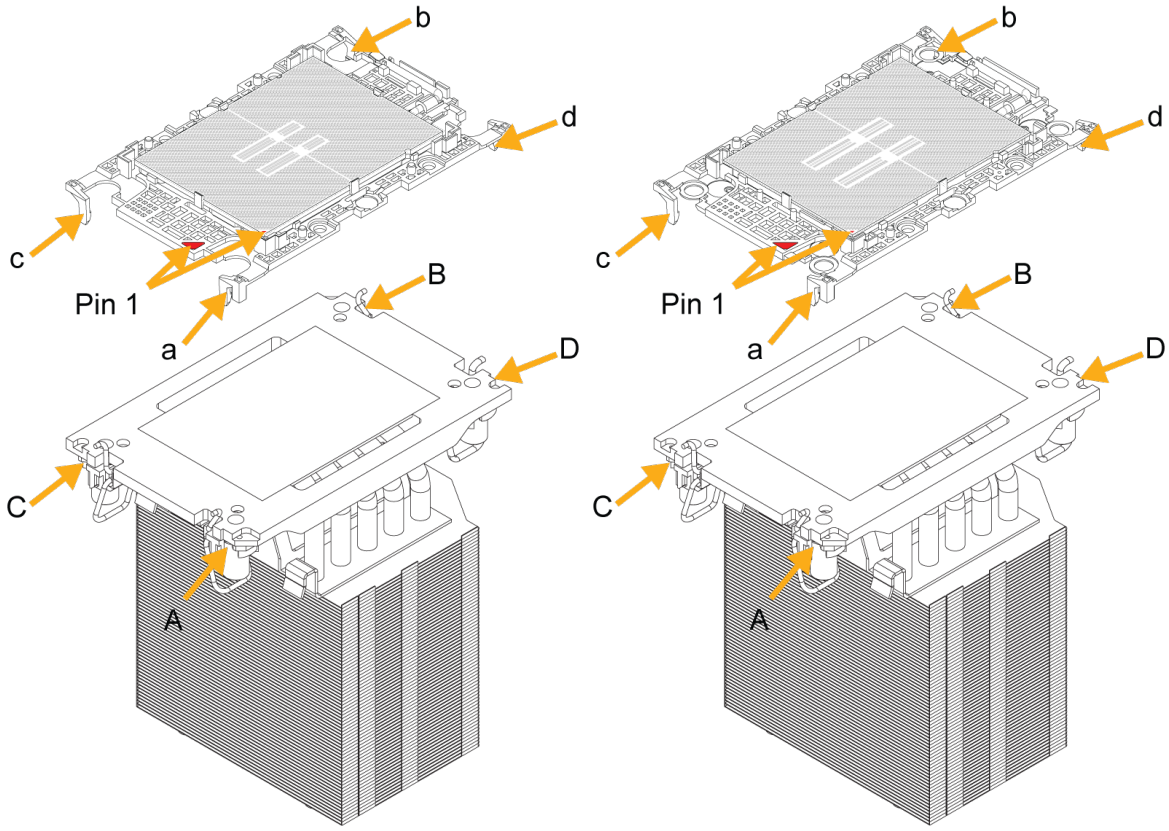


Figure 2-22. Carrier with 4U Heatsink (SP XCC left, SP HCC/LCC right)

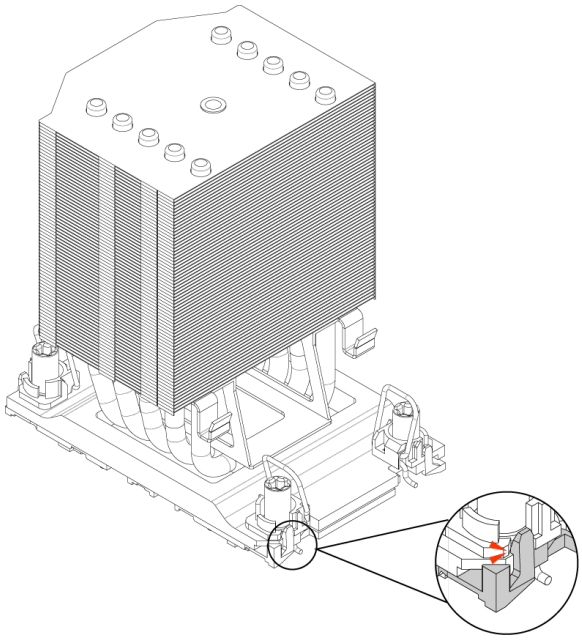


Figure 2-23. PHM Plastic Clips Locked (4U)

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

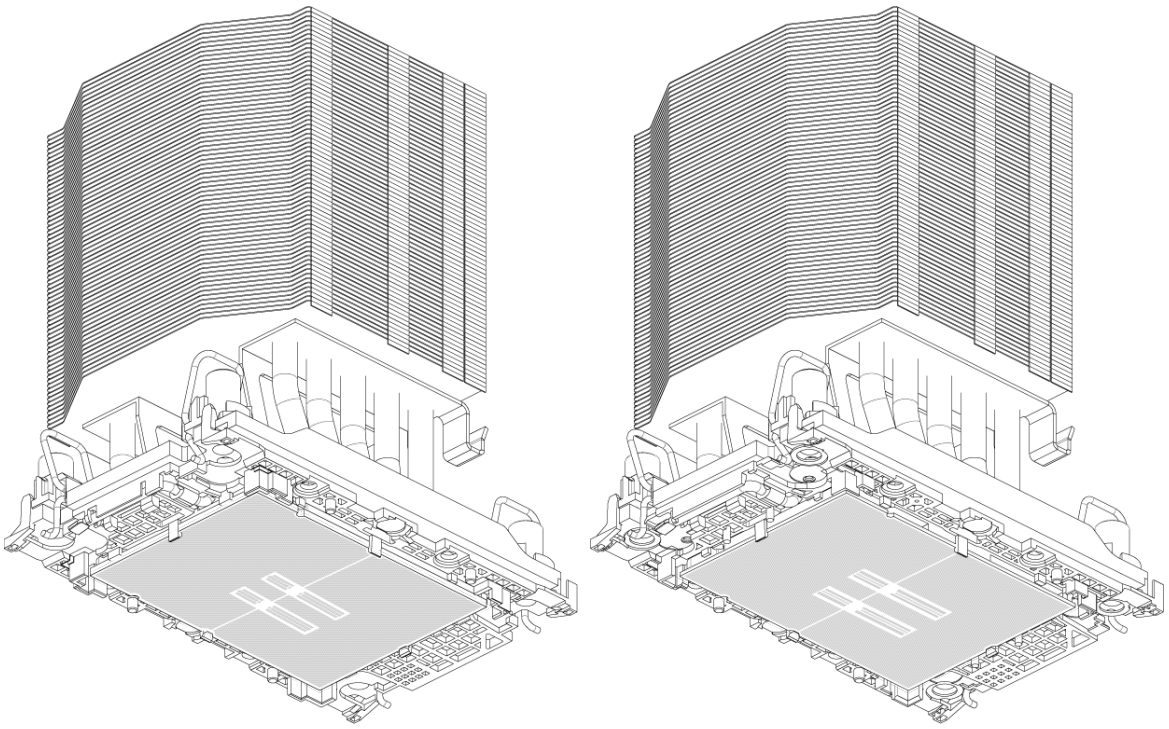


Figure 2-24. 4U PHM Completed (SP XCC left, SP HCC/LCC right)

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.

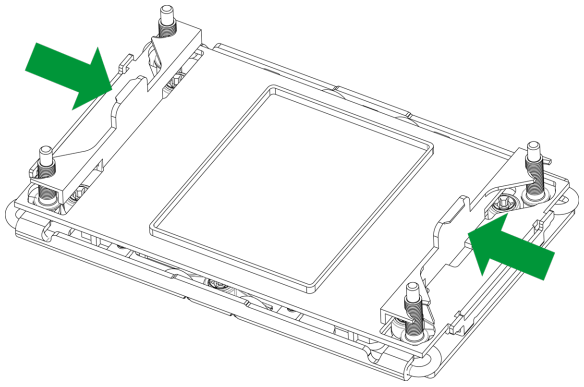


Figure 2-25. Processor Socket with Plastic Protective Cover

2. Pull up the protective cover from the socket.

Note: Do not touch or bend the socket pins.

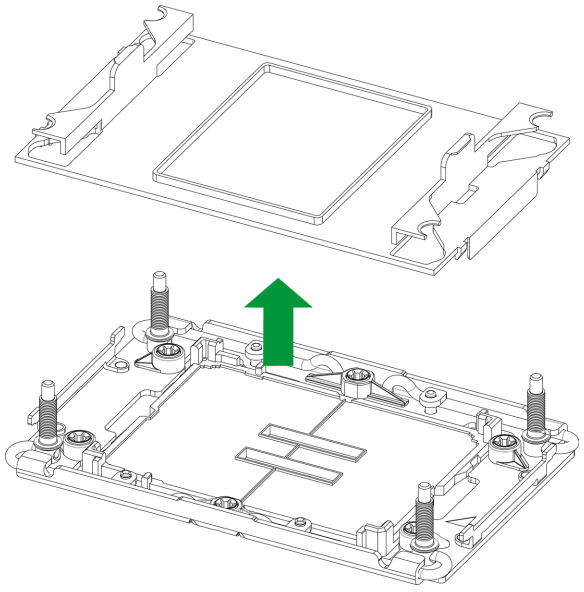
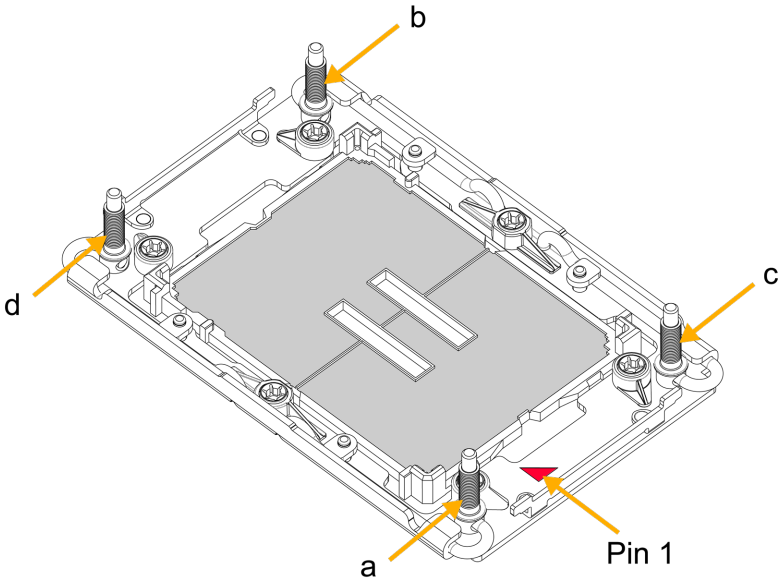


Figure 2-26. Plastic Protective Cover Removed

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 2-27. 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.

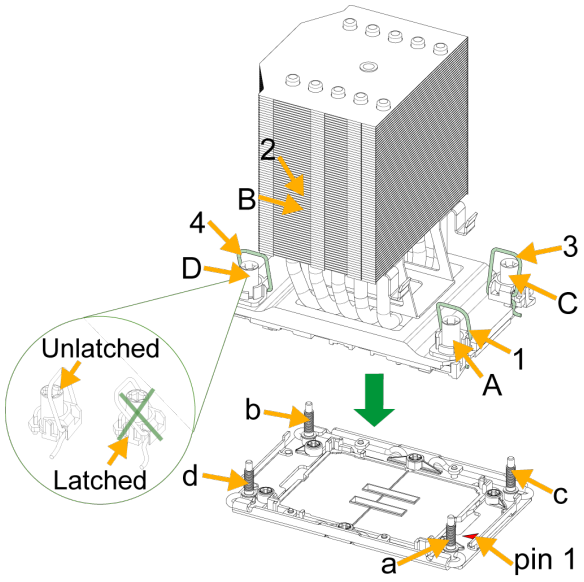


Figure 2-28. PEEK Nuts and Rotating Wires (4U)

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.

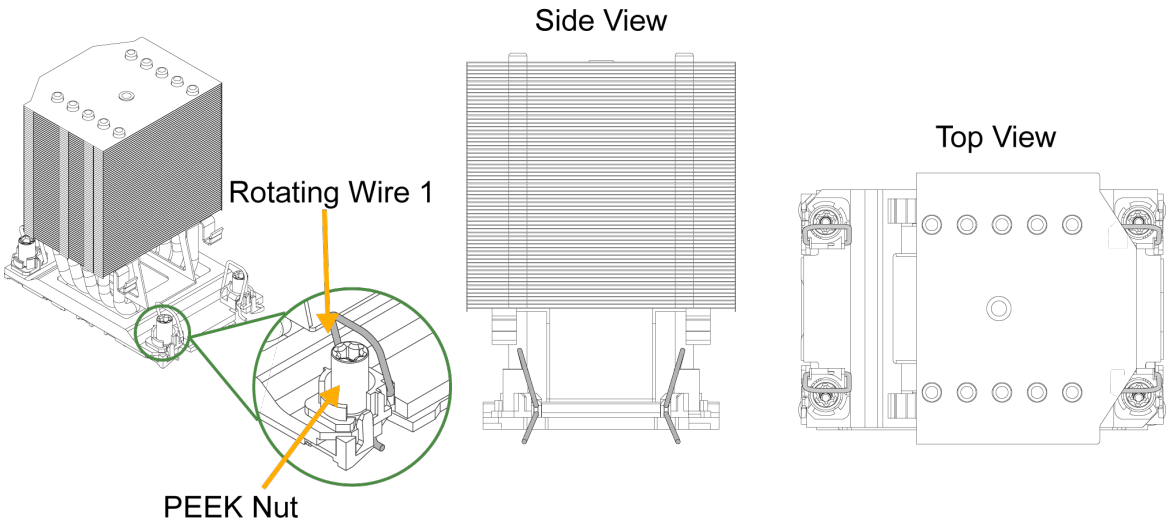


Figure 2-29. 4U Unlatched Positions

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.

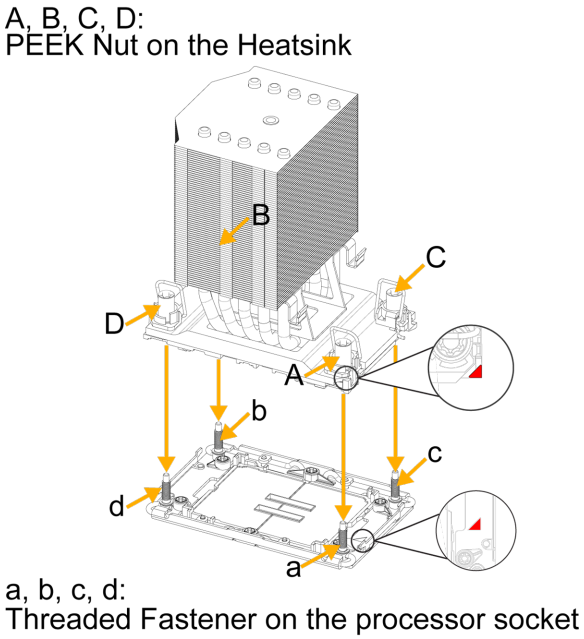


Figure 2-30. Aligning the Heatsink with the Socket (4U)

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

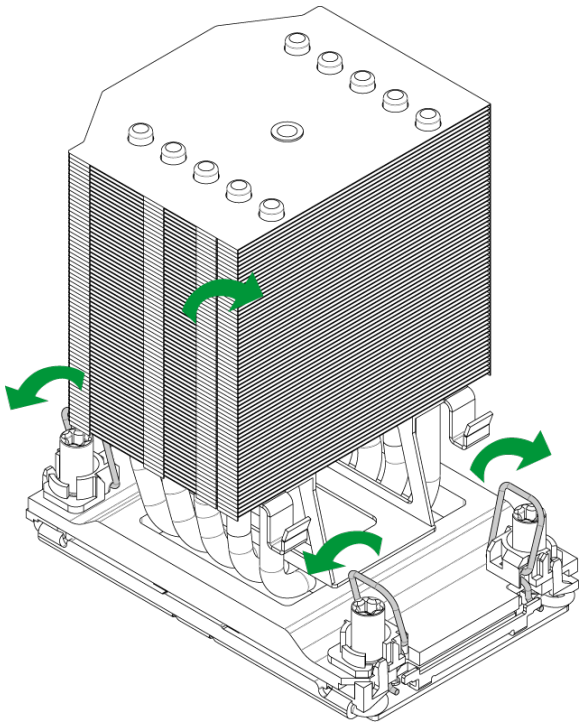


Figure 2-31. Latching the PHM (4U)

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.

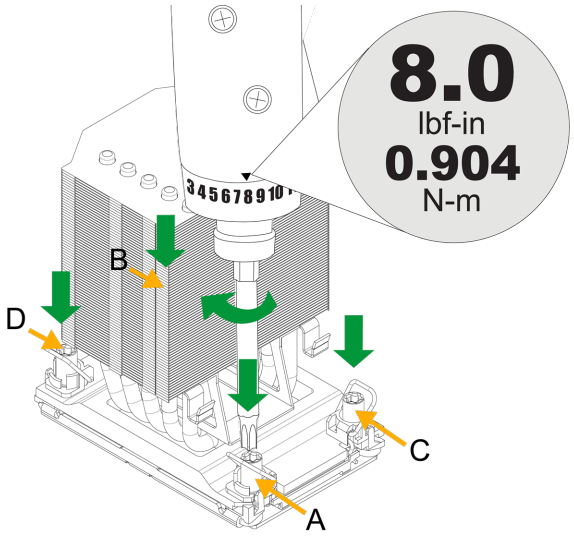


Figure 2-32. Installing the PHM with a Torque Driver (4U)

6. Align the aluminum fan shroud against the top of the 4U heatsink. The fan shroud was designed to match perfectly with the top of the heatsink in terms of geometric shape.

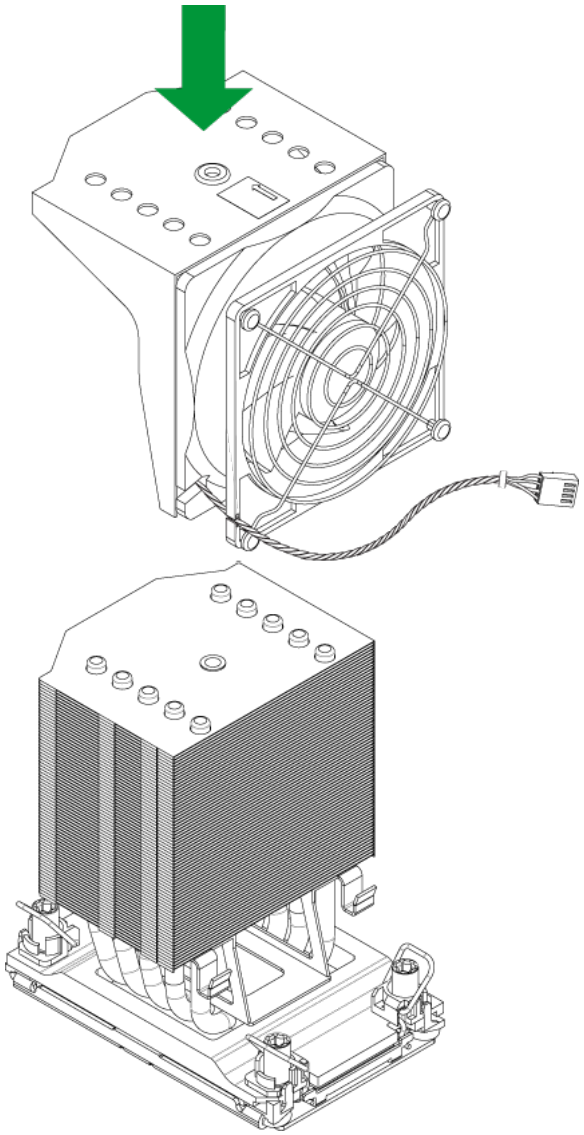


Figure 2-33. Aligning the Heatsink Fan

7. When the fan shroud and the top of the heatsink are properly aligned, gently push the fan onto the heatsink until the bottom of the fan properly rests on the two hooks of the heatsink.

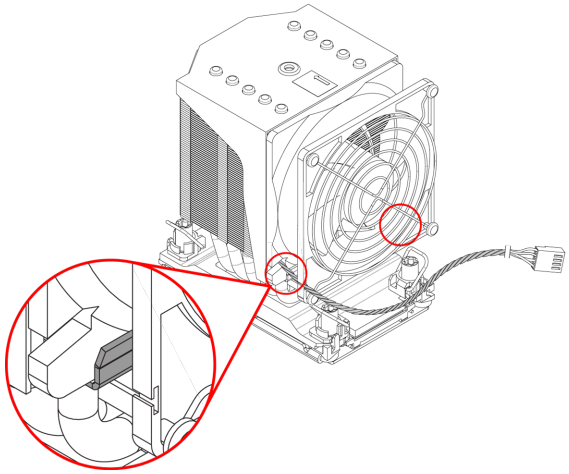


Figure 2-34. Installing the Heatsink Fan

8. Insert the Torx screw into the screw hole on top of the heatsink and turn it clockwise to tighten the screw.

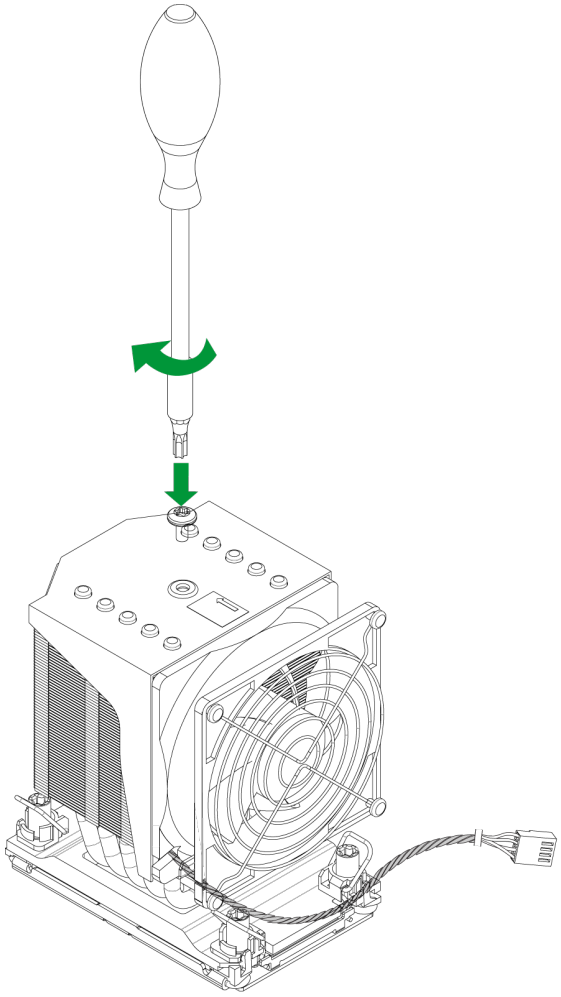


Figure 2-35. Tightening the Screw

9. Connect the fan power connector to a 4-pin fan header on the motherboard.

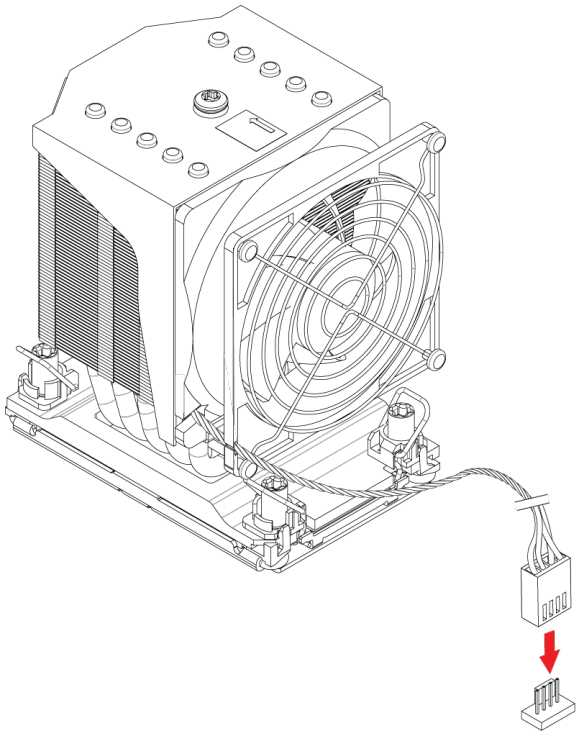


Figure 2-36. Connecting the Fan Power

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. Loosen the Torx screw from the heatsink. Unplug the fan power connector from the fan header.

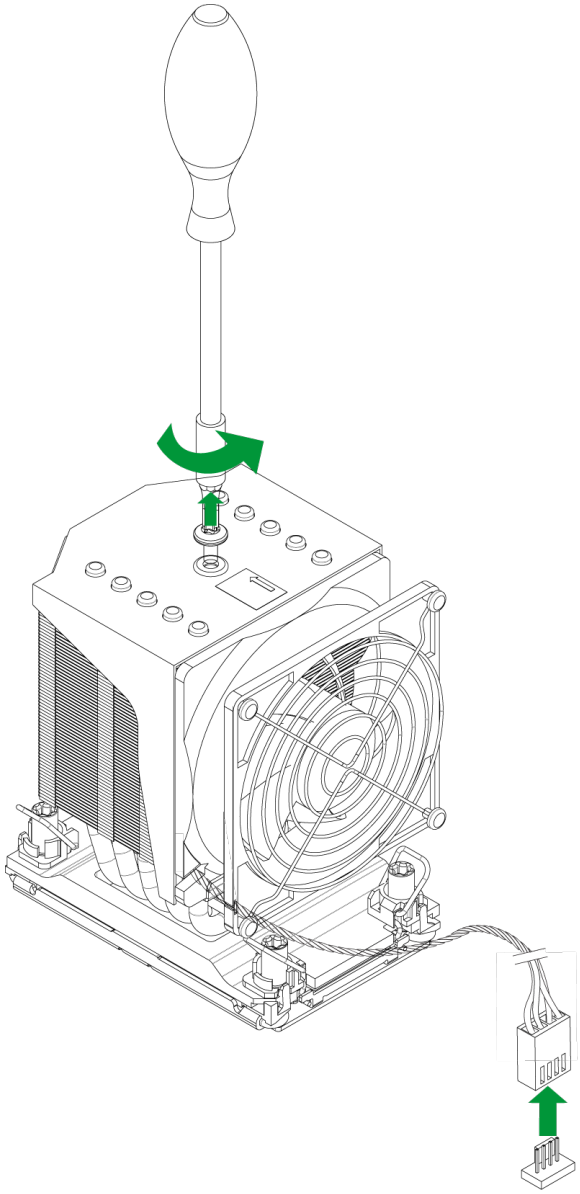


Figure 2-37. Loosening the Screw and Unplugging the Fan Power Header

2. Gently pull the heatsink fan upward to detach it from the heatsink.

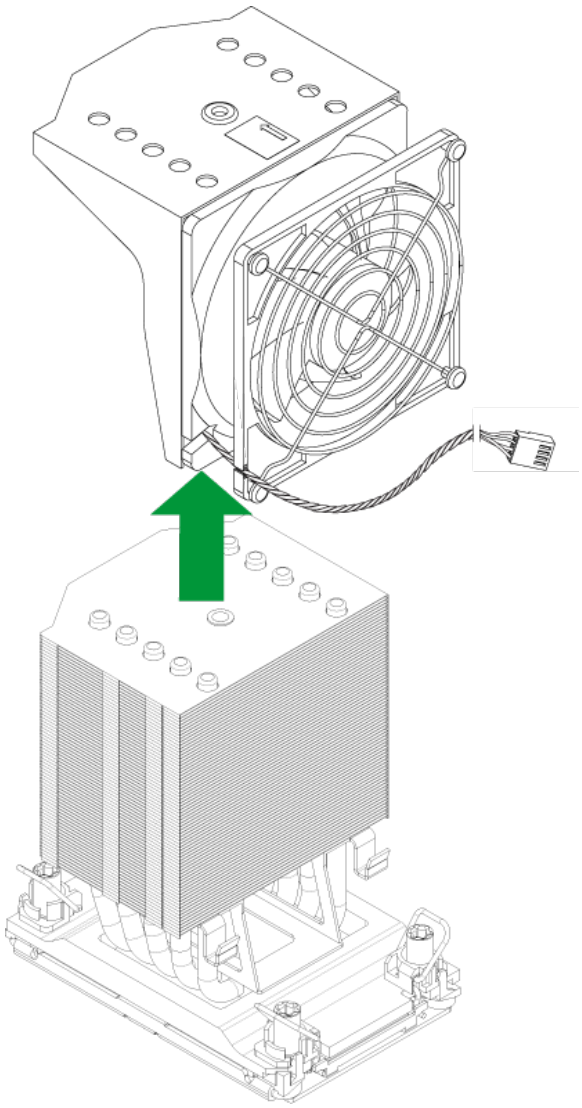


Figure 2-38. Removing the Fan

3. 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.

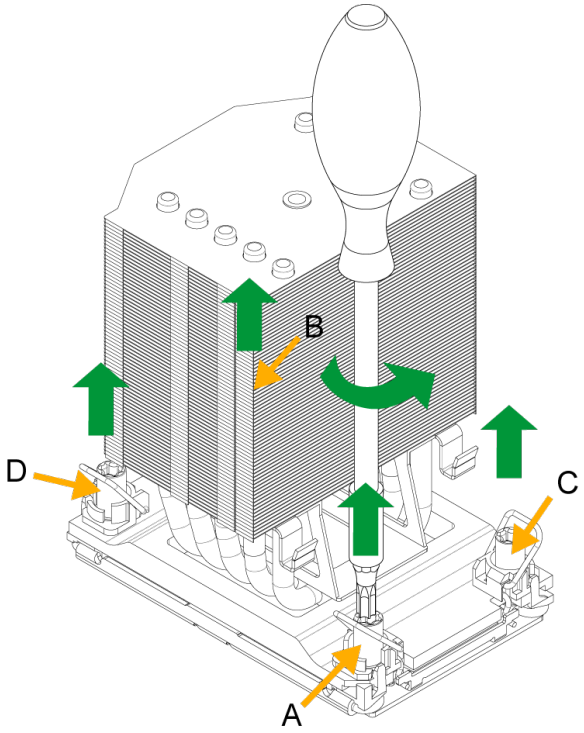


Figure 2-39. Loosening the Screws (4U)

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

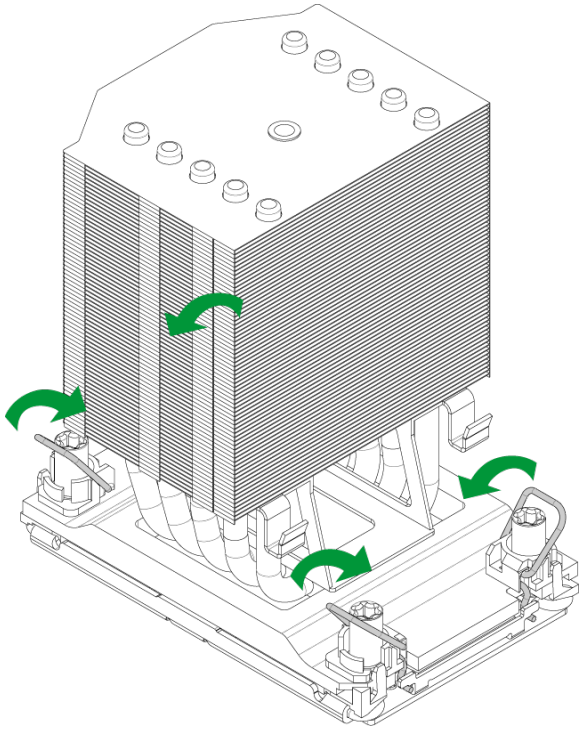


Figure 2-40. Unlatching the PHM (4U)

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

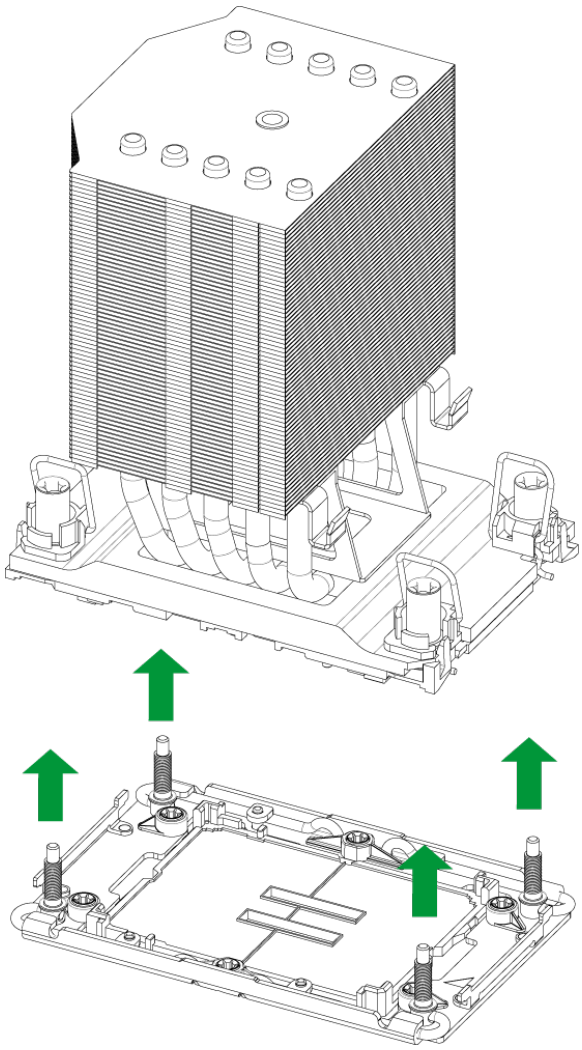


Figure 2-41. Removing the PHM from the Socket (4U)

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

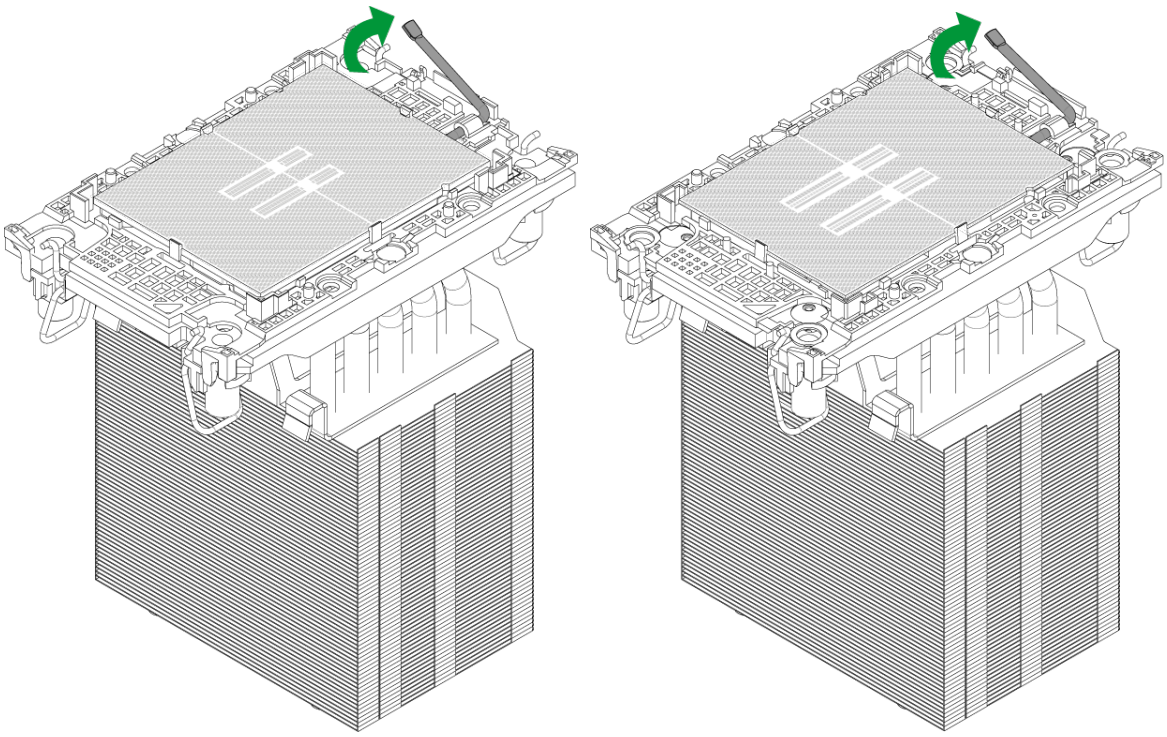


Figure 2-42. Carrier with 4U Heatsink (SP XCC left, SP HCC/LCC right)

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

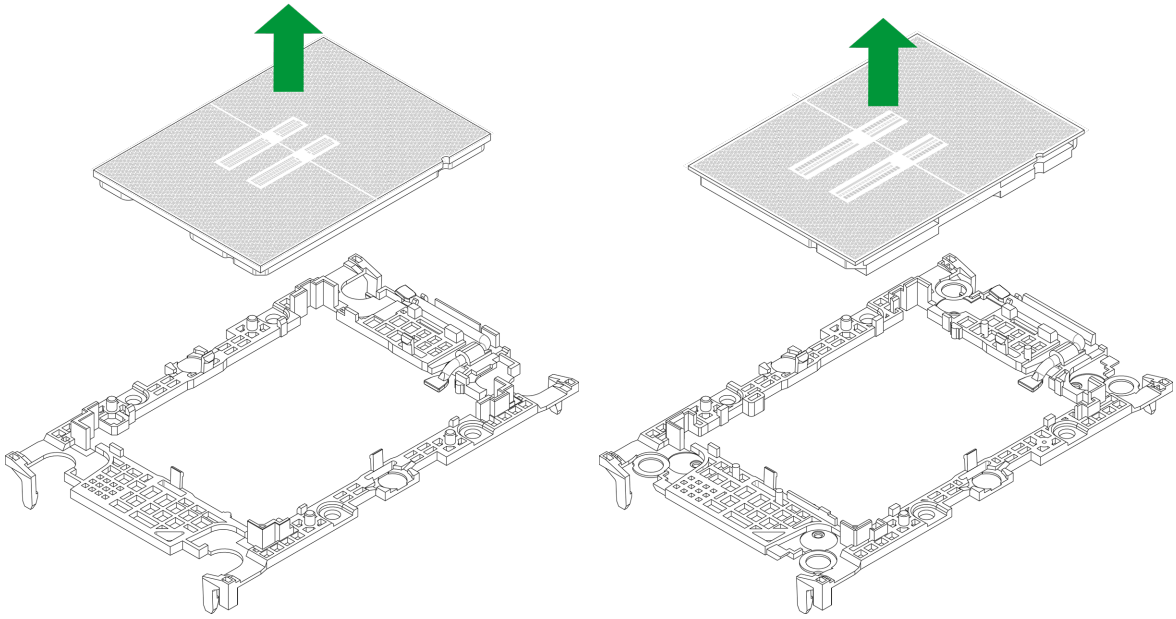


Figure 2-43. Removing the Processor (SP XCC left, SP HCC/LCC right)

2.3 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

For Intel Xeon 690/670/650 Series processors, the X14SRG-TF motherboard supports up to 1 TB of ECC RDIMM and 2 TB 3DS RDIMM with speeds of up to 6400 MT/s (1DPC), or 512 GB of ECC MRDIMM (1DPC) with speeds of up to 8000 MT/s (1DPC) in eight DDR5 DIMM slots. For Intel Xeon 630 Series processors, it supports up to 512 GB of ECC RDIMM and 1 TB of 3DS RDIMM with speeds of up to 6400 MT/s (1DPC) in four DDR5 DIMM slots.

DDR5 Memory Support

DDR5 Memory Support for Intel Xeon 600 Series Processors

Type	Ranks Per DIMM, Data Width (Stack)	DIMM Capacity (GB)			Voltage (V); DIMMs per Channel (DPC)	
		DRAM Density (Gb)			+1.1 V	
		16 Gb	24 Gb	32 Gb	DIMM Speed (MT/s)	1DPC Speed (MT/s)
		1DPC	1DPC	1DPC		
RDIMM	1Rx8	16 GB	24 GB	-	6400	Up to 6400*
	1Rx4	32 GB	48 GB	-		
	2Rx8	32 GB	48 GB	-		
	2Rx4	64 GB	96 GB	128 GB		
3DS RDIMM	4Rx4	-	-	256 GB		
	8Rx4	256 GB	-	-		
MRDIMM	2Rx8	32 GB	-	-	8800	Up to 8000*
	2Rx4	64 GB	-	-		

Notes:

- The supported 1DPC speeds are based on Intel POR.
- The speeds marked with an asterisk (*) are based on the top-tier processor SKUs. Other processor SKUs may support lower memory speeds. Refer to http://ark.intel.com for specific SKU's maximum memory speed.
- Only Intel Xeon 690/670/650 Series processors support MRDIMM.

Memory Population Table

DDR5 Memory Population Table for Intel Xeon 690/670/650 Series Processors									
DDR5	DIMMD1	DIMMC1	DIMMB1	DIMMA1	CPU	DIMME1	DIMMF1	DIMMG1	DIMMH1
1				DDR5					
						DDR5			
2		DDR5				DDR5			
				DDR5				DDR5	
4		DDR5		DDR5		DDR5		DDR5	
	DDR5		DDR5				DDR5		DDR5
8	DDR5	DDR5	DDR5	DDR5		DDR5	DDR5	DDR5	DDR5

DDR5 Memory Population Table for Intel Xeon 630 Series Processors					
DDR5	DIMMC1	DIMMA1	CPU	DIMME1	DIMMG1
1		DDR5			
				DDR5	
2	DDR5			DDR5	
		DDR5			DDR5
4	DDR5	DDR5		DDR5	DDR5

Note: Intel Xeon 690/670/650 Series processors support all eight DIMM slots. Intel Xeon 630 Series processors only support slots DIMMC1, DIMMA1, DIMME1, and DIMMG1.

General Guidelines for Optimizing Memory Performance

- It is recommended to use DDR5 memory of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.

- This motherboard supports installation of one DIMM. However, to achieve the best memory performance, a balanced memory population is recommended.

Notes for DIMM Installation and Removal

Notes:

- The DDR5 DIMM module is NOT hot-swappable and be sure to disconnect power for a minimum of 20 seconds before inserting or removing it.
- Removing a DDR5 DIMM module at a slanted angle will cause damages. It is strongly recommended that you lift the module straight up out of the slot.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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 31.

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 tab outwards to unlock the slot.

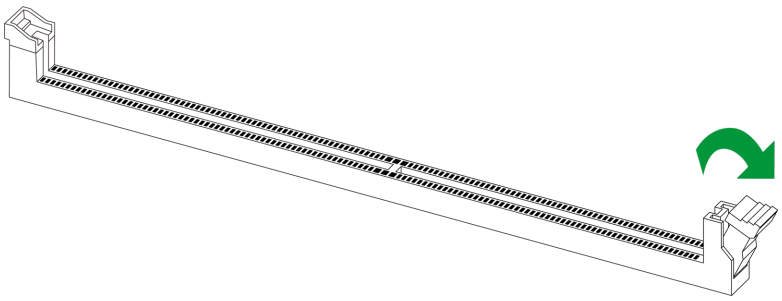


Figure 2-44. Unlocking the DIMM Slot

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

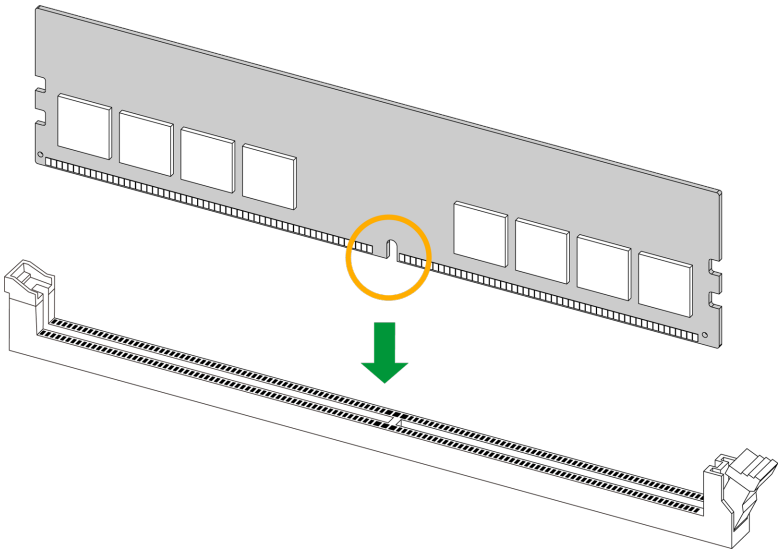


Figure 2-45. Aligning the DIMM Slot with the Receptive Point

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

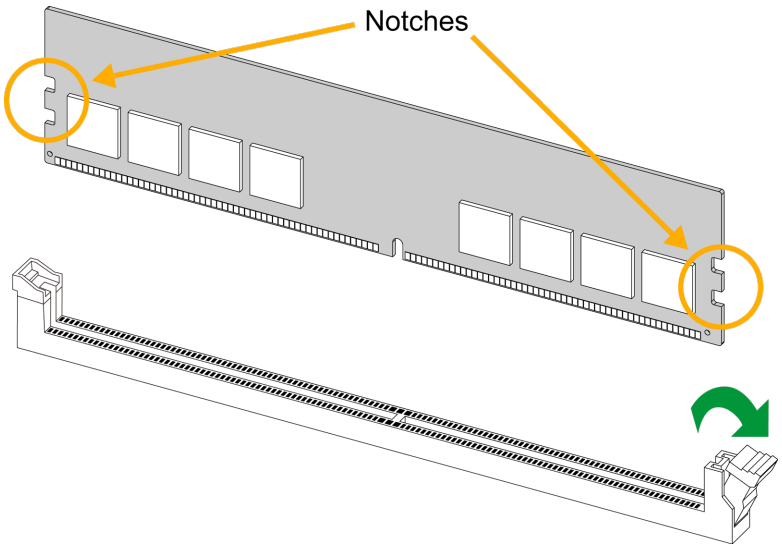


Figure 2-46. Aligning the Notches

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

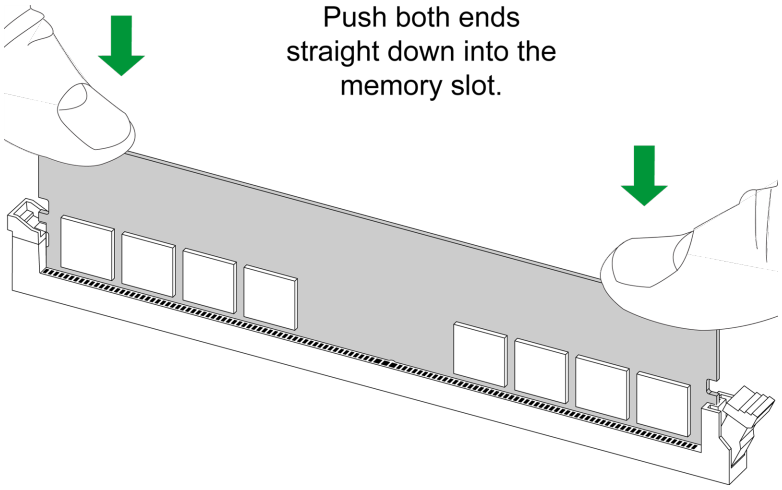


Figure 2-47. Securing the DIMM

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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 31.

Press the release tab of the DIMM socket to unlock it. Once the DIMM is loosened, remove it from the memory slot.

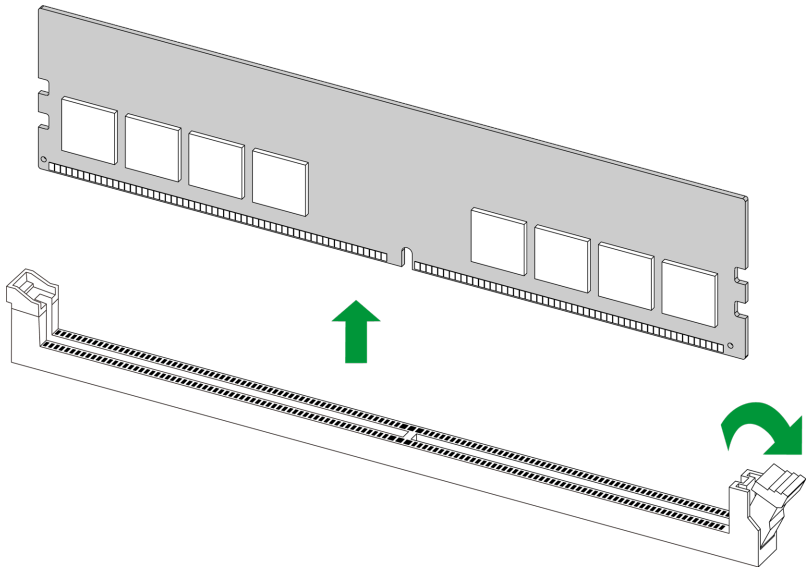


Figure 2-48. Unlocking the DIMM Slot

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

2.4 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

1. Power off your system and unplug your power cable.
2. 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.

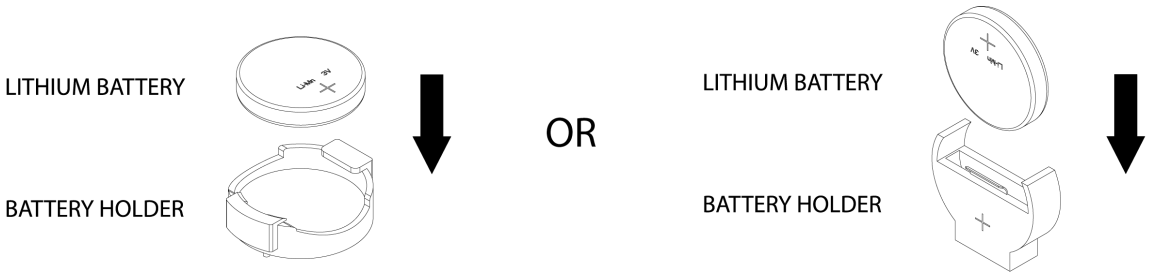


Figure 2-49. Installing a Battery

2.5 M.2 Device Installation

This motherboard has two PCIe 5.0 x4 and two PCIe 4.0 x4 M.2 M-key slots that support the M.2 2280/22110 modules. One standoff is pre-installed in the position of each 22110 mounting hole. Follow the steps below to install the M.2 device.

Notes:

- The installation described in this section is for reference only. The actual installation steps may vary depending on the supported M.2 form factors and the standoff pre-installed location.
- Images displayed are for illustration purposes only. Your components might look different from those shown in this manual.

Installing a Standard M.2 Device

1. Locate the screw on the pre-installed standoff. Remove the screw and set it aside.

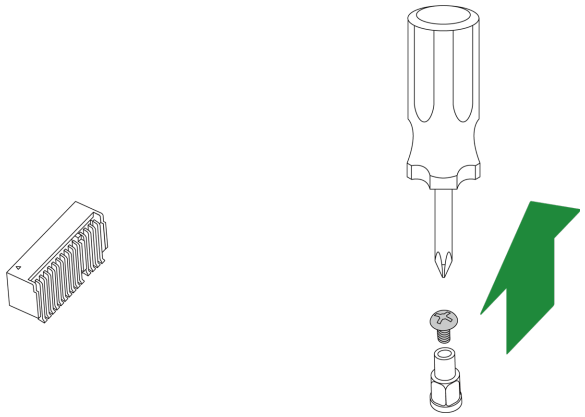


Figure 2-50. Removing the Screw on the Pre-Installed Standoff

2. If the soon-to-be used mounting hole doesn't have a standoff, move the pre-installed one to that mounting hole.

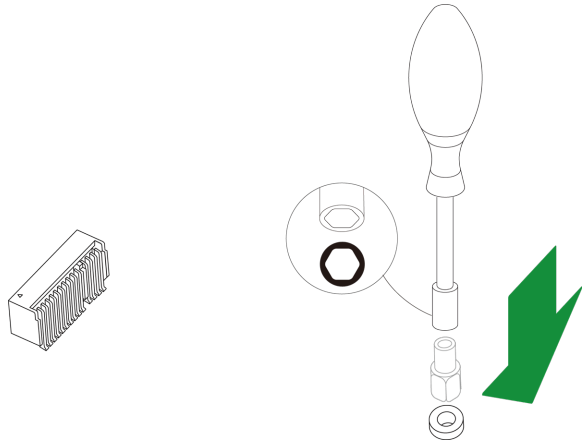


Figure 2-51. Changing the Standoff Position as Needed

3. Carefully insert the M.2 device into the M.2 slot at a 30-degree angle and lower the semi-circle notched end onto the standoff.

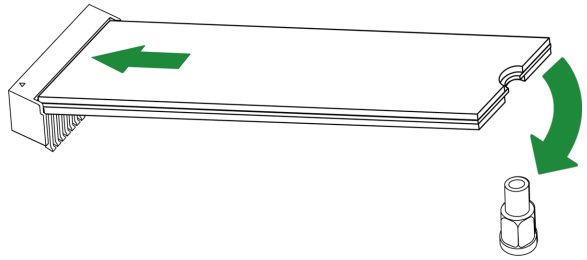


Figure 2-52. Inserting the M.2 Device and Pressing it Down

4. Tighten the standoff screw to secure the M.2 device into place. Do not overtighten so as to avoid damaging the M.2 device.

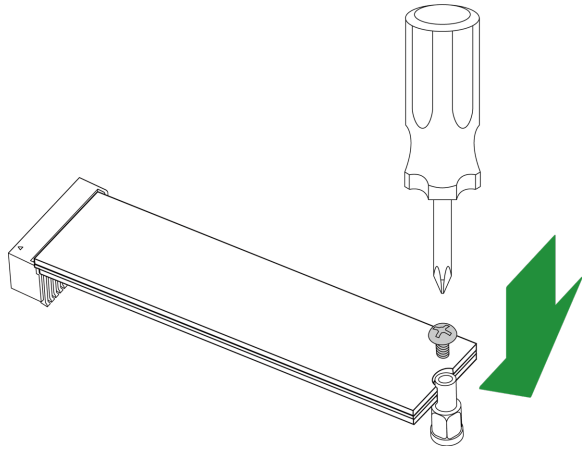


Figure 2-53. Securing the M.2 Device

Installing an M.2 Device with Heatsink (Optional)

It is strongly recommended that you install an M.2 heatsink provided by the M.2 device supplier. If you are using a Supermicro M.2 heatsink, follow the steps below:

1. Remove the thermal pad protective films from the cover and the tray of the M.2 heatsink.

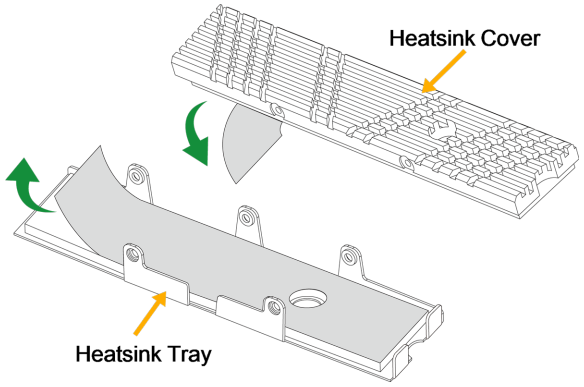


Figure 2-54. Removing the Protective Films from the Heatsink

Note: Images displayed are for illustration only. Your M.2 heatsink may not look exactly the same as the graphics shown in the manual.

2. Place the M.2 device into the tray, then put the heatsink cover in place. Be careful to align the tray holes with the cover holes.

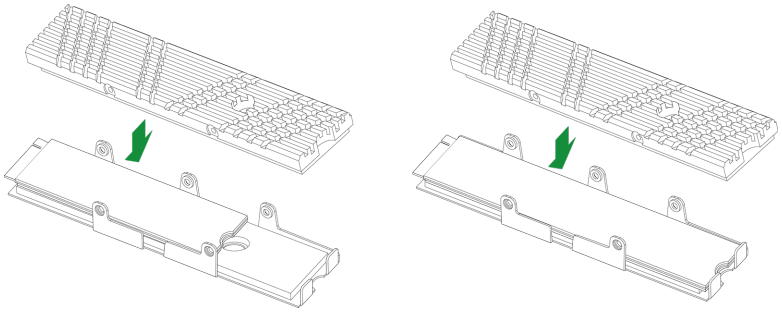


Figure 2-55. Creating the M.2 Heatsink Assembly

3. Tighten the screws to secure the M.2 heatsink assembly.

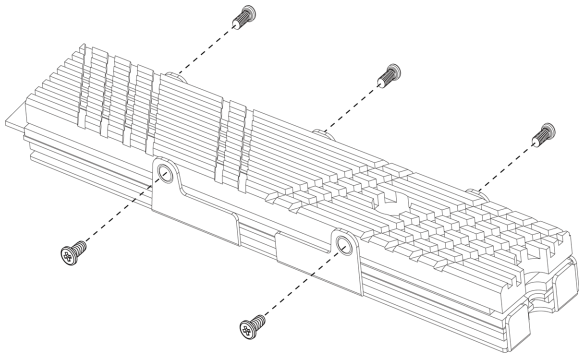


Figure 2-56. Securing the M.2 Heatsink Assembly

4. Locate the pre-installed standoff and screw . Remove the screw and set it aside.

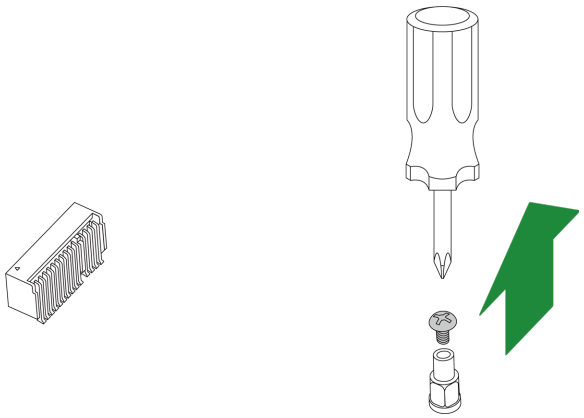


Figure 2-57. Removing the Screw on the Pre-Installed Standoff

5. If the soon-to-be used mounting hole doesn't have a standoff, move the pre-installed one to that mounting hole.

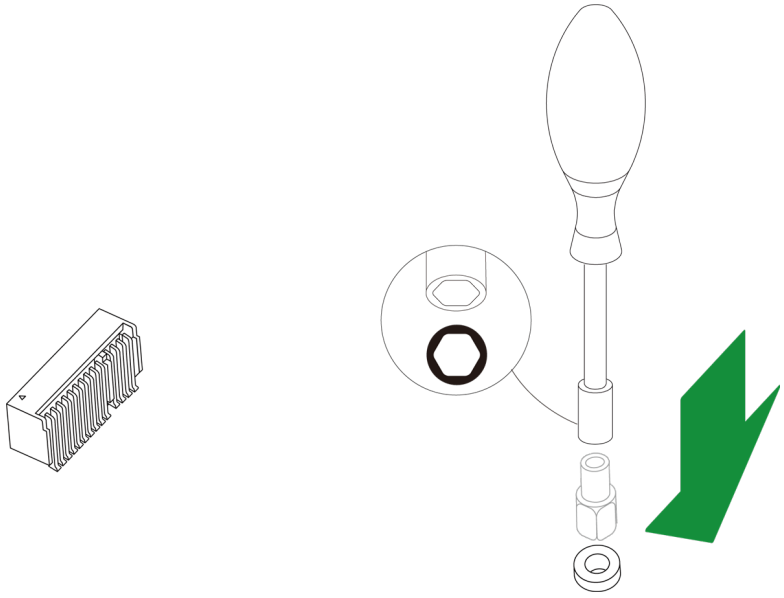


Figure 2-58. Changing the Standoff Position as Needed

6. Carefully insert the M.2 assembly into the M.2 slot at a 30-degree angle and lower the assembly onto the standoff.

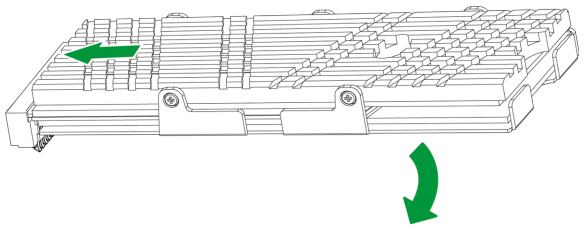


Figure 2-59. Inserting the M.2 Heatsink Assembly and Pressing it Down

7. Tighten the standoff screw to secure the M.2 heatsink assembly into place. Do not overtighten so as to avoid damaging the M.2 assembly.

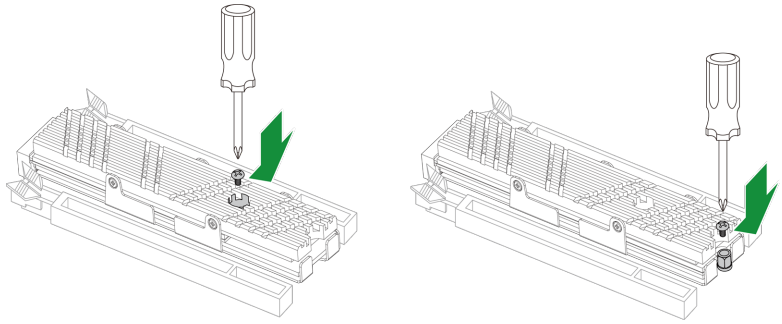


Figure 2-60. Securing the M.2 Heatsink Assembly

2.6 Rear I/O Ports

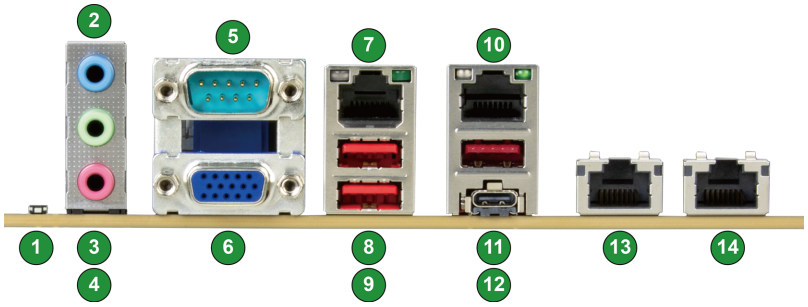


Figure 2-61. Rear I/O Ports

Rear I/O Ports					
No.	**Descriptions**	**No.**	**Descriptions**	**No.**	**Descriptions**
1	UID Button	6	VGA Port	11	USB 0: USB 3.2 Gen 2x1 Port (10 Gb, Type-A)
2	Line In (default)	7	Dedicated BMC LAN Port	12	USB 3: USB 3.2 Gen 2x2 Port (20 Gb, Type-C)
3	Line Out (default)	8	USB 1: USB 3.2 Gen 2x1 Port (10 Gb, Type-A)	13	LAN2: RJ45 10 GbE LAN Port
4	Mic In (default)	9	USB 2: USB 3.2 Gen 2x1 Port (10 Gb, Type-A)	14	LAN3: RJ45 10 GbE LAN Port
5	COM Port (COM1)	10	LAN1: RJ45 1 GbE LAN Port		

Unit Identifier Button

A Unit Identifier (UID) button is located on the rear I/O of the X14SRG-TF motherboard, and a UID LED is located near the UID button . When you press the UID button on and off, it will turn the UID LED on and off to identify a system unit that may need services.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

High Definition Audio (HD Audio) Ports

This X14SRG-TF motherboard features a 7.1+2 Channel High Definition Audio (HDA) codec that provides 10 DAC channels. The HD Audio connections simultaneously supports multiple-streaming 7.1 sound playback with 2 channels of independent stereo output through the front panel stereo out for front, rear, center and subwoofer speakers. Use the Advanced software included in the CD-ROM with your motherboard to enable this function.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

Audio Configuration					
		2 Channel	**4.1 Channel**	**5.1 Channel**	**7.1 Channel**
Audio ports on the rear I/O of the motherboard					
1	Blue ("Line In" by default)	*	Rear Speaker Out	Rear Speaker Out	Rear Speaker Out
2	Green ("Line Out" by default)	Front Speaker Out	Front Speaker Out	Front Speaker Out	Front Speaker Out
3	Pink ("Mic In" by default)	*	*	Center/Subwoofer Speaker Out	Center/Subwoofer Speaker Out
Audio ports on the front panel of the Supermicro system					
	(Front Panel) Green	*	*	*	*
	(Front Panel) Pink	*	*	*	Side Speaker Out

* Function depends on the driver and configuration.

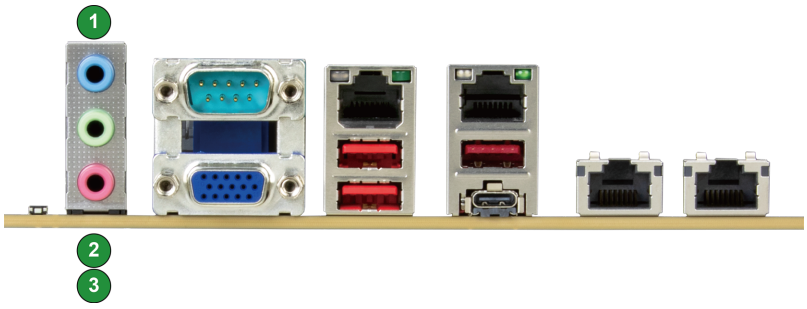


Figure 2-62. X14SRG-TF HD Audio Ports

COM Port

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

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

COM Port Pin Definitions: 11 Total			
Pin#	**Definition**	**Pin#**	**Definition**
1	SP_DCD0	6	SP_DSR0
2	SP_RXD0	7	SP_RTS0
3	SP_TXD0	8	SP_CTS0
4	SP_DTR0	9	SP_RI0
5	GND	10	GND
		11	GND

VGA Port

For the X14SRG-TF motherboard, a video (VGA) port supported by the BMC is located on the rear I/O. The VGA port provides analog interface support between the computer and the video displays.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

LAN Ports

There are four LAN ports on the rear I/O to provide network connections. BMC_LAN is the dedicated BMC LAN port. LAN1 is the 1 GbE port. LAN2 and LAN3 are the 10 GbE ports.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

USB Ports

There are three USB 3.2 Gen 2x1 Type-A ports (USB 0 and USB 1/ 2), and one USB 3.2 Gen 2x2 Type-C port (USB 3) on the rear I/O of the X14SRG-TF motherboard.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

2.7 Front Control Panel

JFP1 on the X14SRG-TF motherboard contains header pins for various buttons and indicators that are normally located on a control panel at the front of the chassis. These connectors are designed specifically for use with Supermicro chassis. See the figure below for the descriptions of the front control panel buttons and LED indicators.

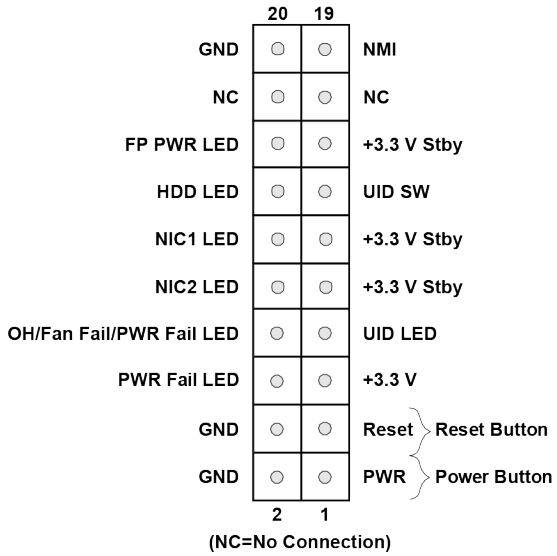


Figure 2-63. Front Control Panel Pin Definitions

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Power On and BMC/BIOS Status LED Button

The Power On button connection is located on pins 1 and 2 of JFP1 on the X14SRG-TF motherboard. The BMC/BIOS Status LED button connection is also located on pins 1 and 2. Momentarily contacting both pins will power on/off the system or display BMC/BIOS status.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Power Button Pin Definitions (JFP1)	
Pin#	**Definition**
1	Signal
2	GND

Power Button & BMC/BIOS Status LED Indicator Pin Definitions (JFP1)	
Status	**Event**
Solid green	System power on
BMC/BIOS blinking green at 4 Hz	BMC/BIOS checking
BIOS blinking green at 4 Hz	BIOS recovery/update in progress
BMC blinking red x2 (2 blinks red) at 4 Hz, 1 pause at 2 Hz (on-on-off-off)	BMC recovery/update in progress
BMC/BIOS blinking green at 1 Hz	Flash not detected or golden image checking failure

Reset Button

The Reset Button connection is located on pins 3 and 4 of JFP1 on the X14SRG-TF motherboard. Attach it to a hardware reset button on the computer case to reset the system.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Reset Button Pin Definitions (JFP1)	
Pin#	**Definition**
3	Reset
4	GND

Power Fail LED

The Power Fail LED connection is located on pins 5 and 6 of JFP1 on the X14SRG-TF motherboard.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Power Fail LED Pin Definitions (JFP1)	
Pin#	**Definition**
5	+3.3 V
6	PWR Supply Fail

OH/Fan Fail/PWR Fail and UID LED

The Overheat (OH)/Fan Fail/Power Fail and UID LED connection is located on pins 7 and 8 of JFP1 on the X14SRG-TF motherboard. The LED on pin 8 provides warnings of overheat, fan failure, or power failure. The LED on pin 7 is active when the UID button on the rear I/O of X14SRG-TF is pressed.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

OH/Fan Fail/PWR Fail/UID LED Pin Definitions (JFP1)	
Pin#	**Definition**
7	UID LED
8	OH/Fan Fail/PWR Fail LED

OH/Fan Fail/PWR Fail LED State (JFP1)	
State	**Definition**
Off	Normal
On	Overheat
Flashing	Fan/Power Fail

OH/Fan Fail/PWR Fail/UID LED LED State	
Status	**Description**
Solid red (on)	An overheating has occurred.
Blinking red at 1 Hz	Fan failure: check for an inoperative fan.
Blinking red at 0.25 Hz	Power failure: check for a non-operational power supply.
Solid blue	Local UID is activated. Use this function to locate a unit in the system that might be in need of service.
Blinking blue at 1 Hz	Remote UID is on. Use this function to identify a unit from a remote location that might be in need of service.
BIOS/BMC blinking blue at 10 Hz	BIOS/BMC: recovery and/or update in progress.

NIC1/NIC2 (LAN1/LAN2) LED

The Network Interface Controller (NIC) LED connection for LAN port 1 is located on pins 11 and 12 of JFP1 on the X14SRG-TF motherboard, and LAN port 2 is on pins 9 and 10. Attach the NIC LED cables here to display network activity.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

LAN1/LAN2 LED Pin Definitions (JFP1)	
Pin#	**Definition**
9	VCC
10	NIC2 Link/Active LED
11	VCC
12	NIC1 Link/Active LED

UID Button and HDD LED

The UID Button/HDD LED connection is located on pins 13 and 14 of JFP1 on the X14SRG-TF motherboard. Attach a cable to pin 14 to show storage drive activity status. The UID Button connection is located on pin 13 of JFP1. Attach a cable to pin 13 to use the UID button.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

UID Button/HDD LED Pin Definitions (JFP1)	
Pin#	**Definition**
13	+3.3 V Standby/UID Button
14	HDD Activity

FP Power LED

The Front Panel (FP) Power LED connection is located on pins 15 and 16 of JFP1 on the X14SRG-TF motherboard.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

FP Power LED Pin Definitions (JFP1)	
Pin#	**Definition**
15	+3.3 V
16	PWR LED

NMI Button

The non-maskable interrupt (NMI) button header is located on pins 19 and 20 of JFP1 on the X14SRG-TF motherboard.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

NMI Button Pin Definitions (JFP1)	
Pin#	**Definition**
19	Control
20	GND

2.8 Connections, Jumpers, and LEDs

Refer to the following sections for information about connections, jumpers, and LEDs for the X14SRG-TF motherboard.

Power Supply and Power Connections

For information about the power supply and power connections of the X14SRG- TF motherboard, refer to the following content.

Power Distribution Board Slot

There is one 12V DC power slot (JPW1) on the motherboard to provide adequate power supply to your system. Refer to the table below for pin definitions.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

12 V DC Power Slot Pin Definitions: 14 Total	
Pin#	**Definition**
1–9, 19–27, C, D, J, K	GND
10–18, 28–36	+12 V
A, B, E, F, G, H, I, L, M, N	Sideband

Headers and Connections

For information about the headers on the X14SRG-TF motherboard, refer to the following content.

Chassis Intrusion

A Chassis Intrusion header is located at JL1 on the X14SRG-TF motherboard. Attach the appropriate cable from the chassis to inform you when the chassis is opened.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Chassis Intrusion Pin Definitions: Two Total	
Pin#	**Definition**
1	Intrusion Input
2	GND

DOM Power Connectors

The Disk-On-Module (DOM) power connectors, located at JSD1 and JSD2, provide 5 V power to solid state DOM storage devices connected to the S-SATA 0 and S-SATA 1 SATA ports.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

DOM Power Connector Pin Definitions: Three Total	
Pin#	**Definition**
1	+5 V
2	GND
3	GND

External BMC I²C Header

A System Management Bus header for the BMC is located at JIPMB1 on the X14SRG-TF motherboard. Connect the appropriate cable here to use the IPMB I²C connection on your system.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

External Speaker / Buzzer

On the JD1 header, close pins 3 and 4 with a cap to use the onboard buzzer. If you wish to use an external speaker, close pins 1–4 with a cable.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

External Speaker/Buzzer Jumper Settings	
Pin#	**Definition**
Pins 1–4	External Speaker
Pins 3–4	Buzzer (Default)

Fan Headers

There are eight 4-pin fan headers (FAN1–3, FAN1A, and FANA–D) on the X14SRG-TF motherboard. Although pins 1-3 of the system fan headers are backwards compatible with the traditional 3-pin fans, the 4-pin fans are recommended to take advantage of the fan speed control. This allows fan speeds to be automatically adjusted based on the motherboard temperature.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

4-pin Fan Header Pin Definitions: Four Total	
Pin#	**Definition**
1	GND (Black)
2	+12 V (Red)
3	Tachometer
4	PWM Control

Front Panel Audio Header

A 10-pin audio header located at AUDIO_FP/AUDIO FP is supported on the X14SRG-TF motherboard. This header allows you to connect the motherboard to the audio port on the front panel. If needed, connect an audio cable (not supplied) to the audio header to use this feature.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Front Panel Audio Header Pin Definitions: 10 Total			
Pin#	**Definition**	**Pin#**	**Definition**
1	Microphone_Left	6	GND
2	Audio_GND	7	Jack_Detect
3	Microphone_Right	8	Key
4	Audio_Detect	9	Line_2_Left
5	Line_2_Right	10	GND

Inlet Sensor Header

An inlet sensor header is located at JSEN1 on the X14SRG-TF 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 X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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

Internal Speaker/Buzzer

The Internal Speaker/Buzzer (SP1) is used to provide audible indications for various beep codes.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Internal Speaker/Buzzer Pin Definitions: Two Total		
Pin#	**Definition**	
1	Pos (+)	Beep In
2	Neg (-)	Alarm Speaker

M.2 Slots

Two PCIe 5.0 x4 M.2 slots supported by CPU are located at M.2-C1 and M.2-C1, and two PCIe 4.0 x4 M.2 slots supported by PCH are located at M.2-P1 an M.2-P2. These M.2 slots support M.2 NVMe SSDs in the M-key 2280 and 22110 form factors. The M.2-C1 and M.2-C1 slots support RAID 0 and 1. Note that you cannot mix CPU-supportd and PCH-supported M.2 slots for a single NVMe RAID array.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

MCIO Connectors

Four PCIe 5.0 x8 MCIO connectors are located at P1_NVME0/1, P1_NVME2/3, P1_NVME4/5, and P1_NVME6/7 on the X14SRG-TF motherboard, with each supporting two NVMe connections. Use these MCIO connectors to support high-speed PCIe NVMe storage devices. The connectors are supported by the CPU and support RAID 0, 1, 5, and 10.

Notes:

- Only Intel Xeon 690/670/650 Series processors support these MCIO connectors.
- When installing an NVMe device on a motherboard, be sure to connect the NVMe port (P1_NVME0/1) first for your system to work properly.
- Install a VROC RAID Key on JRK1 on the X14SRG-TF motherboard for RAID support. A VROC Premium Key supports RAID 0/1/5/10, while a VROC Standard Key supports RAID 0/1/10.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Pump Power Headers

The X14SRG-TF motherboard has three +12 V header for optional CPU liquid cooling systems. When using a liquid cooling system, attach the pump power cables to the 12V_PUMP1–3 headers.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

Pump Power Header Pin Definitions: Four Total	
Pin#	**Definition**
1	GND (Black)
2	2 A/+12 V (Red)
3	No Connection
4	No Connection

SATA 3.0 Ports

Two SATA 3.0 ports are located at S-SATA 0 and S-SATA 1 on the X14SRG-TF motherboard. These SATA 3.0 ports are supported by the PCH. With power pins built in, these connectors can be used with Supermicro SuperDOMs and do not require external power cables. They are also compatible with regular SATA DOMs and SATA HDDs.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

S/PDIF Out Header

The X14SRG-TF motherboard has one Sony/Philips Digital InterFace (S/PDIF) output header for digital audio output. You will need the appropriate cable to use this feature.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

S/PDIF Out Header Pin Definitions: Two Total	
Pin#	**Definition**
1	S/PDIF_OUT
2	GND

SlimSAS 4i Connectors

Two PCIe 4.0 x8 SlimSAS 4i connectors are located at SATA 0–3 and SATA 4–7 on the X14SRG-TF motherboard, with each supporting four SATA connections. These SATA 3.0 ports are supported by the PCH and support RAID 0, 1, 5, and 10.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Standby Power

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

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

Standby Power Pin Definitions: Three Total	
Pin#	**Definition**
1	+5 V Standby
2	GND
3	No Connection

TPM/Port 80 Header

The JTPM1 header on the X14SRG-TF 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 X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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#

USB Headers

There is one internal USB 3.2 Gen 1 Type-A connector (USB 4) on the X14SRG-TF motherboard. There is also one USB 3.2 Gen 1 header (USB 5/6) supporting two USB Type-A connections and one USB 3.2 Gen 2x1 connector (USB 7) supporting one USB Type-C connection. USB 5/6 and USB 7 provide front access using USB cables (not included).

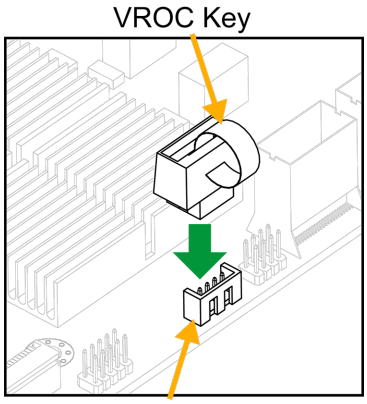
For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

USB 3.2 Gen 1 Header Pin Definitions: 19 Total			
Pin#	**Definitions**	**Pin#**	**Definitions**
1	VBUS	11	IntA_P2_D+
2	IntA_P1_SSRX-	12	IntA_P2_D-
3	IntA_P1_SSRX+	13	GND
4	GND	14	IntA_P2_SSTX+
5	IntA_P1_SSTX-	15	IntA_P2_SSTX-
6	IntA_P1_SSTX+	16	GND
7	GND	17	IntA_P2_SSRX+
8	IntA_P1_D-	18	IntA_P2_SSRX-
9	IntA_P1_D+	19	VBUS
10	GND		

VROC RAID Key Header

A VROC RAID Key header is located at JRK1 on the X14SRG-TF motherboard. Install a VROC RAID key on JRK1 for NVMe RAID support as shown in the illustration below.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.



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.

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.

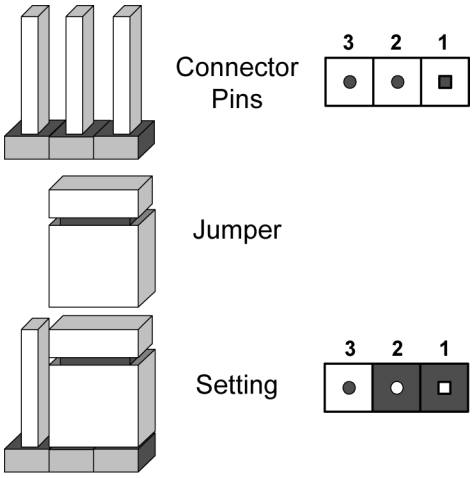


Figure 2-64. Jumping Connector Pins

BMC VGA Enable/Disable

Jumper JPG1 allows you to enable the onboard VGA connection supported by BMC. The default setting is pins 1–2 to enable the connection.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

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

CMOS Clear

JBT1 and JCMOS on the X14SRG-TF motherboard are used to clear CMOS, which will also clear any passwords. Instead of pins, the JBT1 jumper consists of contact pads to prevent accidentally clearing the contents of CMOS.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.


JBT1 contact pads

JCMOS Jumper Settings	
Pin#	**Definition**
Pins 1–2	Normal (Default)
Pins 2–3	CMOS Clear

1. Power down the system.
2. Unplug the power cord(s).
3. Remove the cover of the chassis to access the motherboard.
4. Remove the onboard battery from the motherboard.
5. To clear CMOS via JBT1: Short the CMOS pads with a metal object such as a small screwdriver for at least four seconds. Then remove the screwdriver or shorting device.

   To clear CMOS via JCMOS: Close pins 2 and 3 of JCMOS. Then remove the jumper.

   Note: Clearing CMOS will also clear all passwords.
6. Reinsert the battery.
7. Replace the cover.
8. Reconnect the power cord(s).
9. Power on the system.

HD Audio Enable/Disable

Use JPAC1 to enable or disable HD Audio on the X14SRG-TF motherboard. The default setting is Enabled.

HD Audio Enable/Disable Jumper Settings	
Jumper Setting	**Definition**
Pins 1–2	Enabled (Default)
Pins 2–3	Disabled

LAN Enable/Disable

Use JPL1 to enable or disable LAN1 and JPTG1 to enable or disable LAN2/LAN3 on the X14SRG-TF motherboard. The default setting is Enabled.

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

ME Manufacturing Mode

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

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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

Onboard TPM Enable/Disable

Use JPT1 to enable or disable the onboard TPM.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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

USB 1/2 Standby Power

JPUSB1 on the X14SRG-TF motherboard allows you to enable or disable the USB 1/2 power in S5 standby mode. The default is on pins 1-2 to enable USB 1/2 power in S5 standby mode.

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

USB 1/2 Standy Power Enable/Disable Jumper Settings	
Jumper Setting	**Definition**
Pins 1–2	Enabled (Default)
Pins 2–3	Disabled

Watchdog Timer

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

For a detailed diagram of the X14SRG- TF motherboard, see the layout under "Quick Reference" on page 14.

Watchdog Timer Jumper Settings	
Jumper Setting	**Definition**
Pins 1–2	Reset (Default)
Pins 2–3	NMI
Open	Disabled

LED Indicators

For information about the LED indicators on the X14SRG-TF motherboard, refer to the following content.

BMC Heartbeat LED

A BMC Heartbeat LED is located at LEDBMC on the X14SRG-TF motherboard. When this LED is blinking, the BMC is functioning normally.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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

LAN LEDs

Each LAN port on the rear I/O of the X14SRG-TF motherboard features two LEDs. The LED on the right indicates activity, and the LED on the left indicates the speed of the connection.

LAN1 LEDs		
	Color/State	**Definition**
Link (Left)	Solid Green Solid Amber Solid Amber	1 Gbps 100 Mbps 10 Mbps
Activity (Right)	Blinking Green	Active

LAN2/LAN3 LEDs		
	Color/State	**Definition**
Link (Left)	Solid Green Solid Amber Solid Amber	10 Gbps 1/5/2.5 Gbps 100 Mbps
Activity (Right)	Blinking Green	Active

M.2 LEDs

M.2 LEDs are located at M.C-C1/C2 LEDs (for M.2-C1/C2) and M.C-P1/P2 LEDs (for M.2-P1/P2) on the X14SRG-TF motherboard. When an M.2 LED is blinking, the corresponding M.2 device is functioning normally.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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

SATA Access LED

One SATA access LED is located at LEDSATA on the X14SRG-TF motherboard. When this LED is blinking, either S-SATA 0 or S-SATA 1 (or both) is being accessed.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

SATA Access LED	
LED Color	**Definition**
Solid Green	Device Detected
Blinking Green	Device Being Accessed

Unit ID (UID) LED

The UID LED indicator is located at UID on the X14SRG-TF motherboard. This UID indicator provides easy identification of a system that may need to be serviced.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

UID LED LED Indicator	
LED Color	**Definitions**
Solid Blue	System Identified

Onboard Power LED

The Onboard Power LED is located at LEDPWR on the X14SRG-TF motherboard. When this LED is on, the system is on. Be sure to turn off the system and unplug the power cord before removing or installing components.

For a detailed diagram of the X14SRG-TF motherboard, see the layout under "Quick Reference" on page 14.

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

Chapter 3:

Troubleshooting

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

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 103 or "Returning Merchandise for Service" on page 106 section(s) in this chapter. Always disconnect the AC power cord before adding, changing or installing any non hot-swap 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 92.
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 29 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 13 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

A. 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.

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

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

Intel E610 LAN Ports Failure on Certain Linux OS

The Intel E610 LAN ports are not functional by default on Red Hat Enterprise Linux (RHEL) 9.5 and RHEL 10. This is because the built-in drivers in these versions do not support the Intel E610 LAN controller. To manually install the driver, see "Installing the Intel E610 LAN Driver on RHEL 9.5 and RHEL 10" on page 192.

Furthermore, if you want to allow the E610 LAN driver to be loaded when Secure Boot is enabled, see "C. Enrolling Intel's Public Key for UEFI Secure Boot" on page 194 to enroll Intel's Public Key.

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 99 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 12.

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 65.

3.4 Where to Get Replacement Components

If you need replacement parts for your X14SRG-TF 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 alteration, 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 X14SRG-TF motherboard.

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.

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.

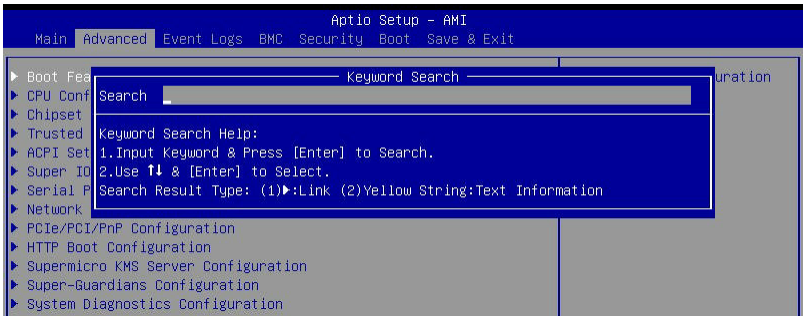
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When a BIOS submenu or item is selected in the left 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.

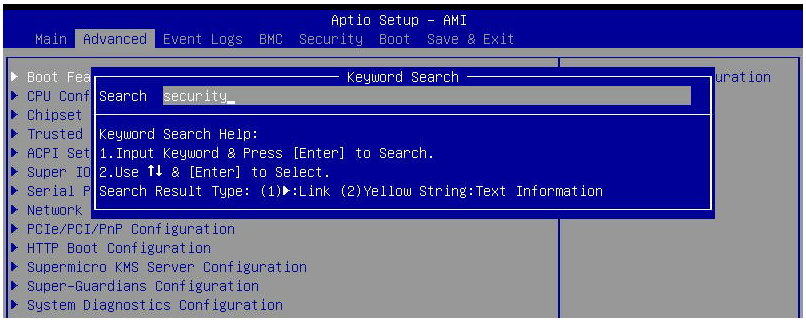
The BIOS Setup utility uses a key-based navigation system called hot keys. Most of these hot keys (<F1>, <F2>, <F3>, <F4>, <F5>, <F6>, <Enter>, <ESC>, the arrow keys, etc.) can be used at any time during the setup navigation process.

Tips on using the <F5> key:

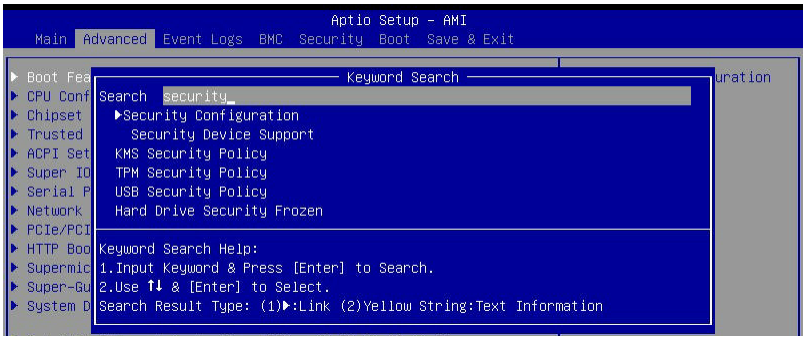
To search for a BIOS menu, submenu, or item using the <F5> key, press <F5> and the Keyword Search screen will appear as shown below.



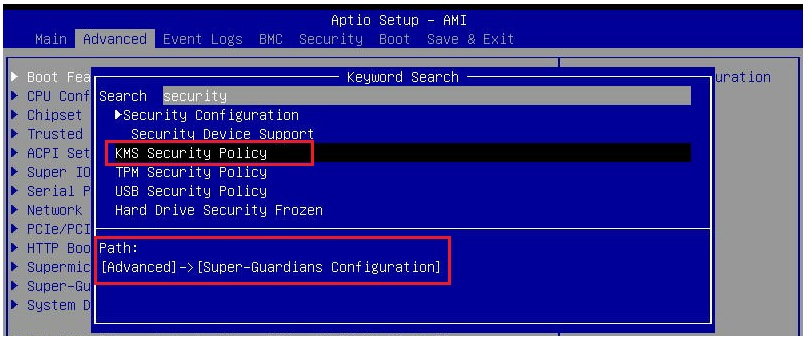
In the Search field, enter a keyword (e.g., security).



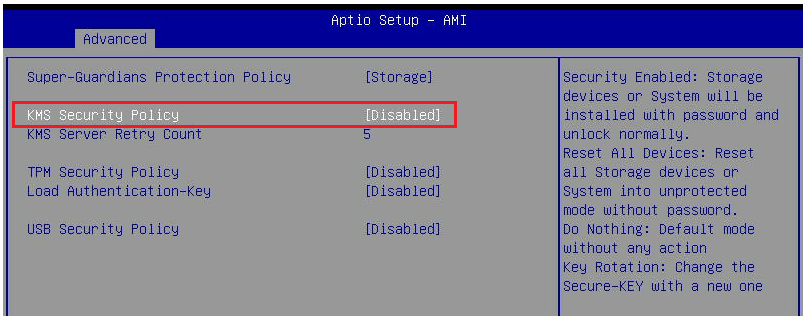
Pressing <Enter> will list the search results.



Use the arrow keys to select, for example, KMS Security Policy. The Keyword Search screen will display the path information for KMS Security Policy.

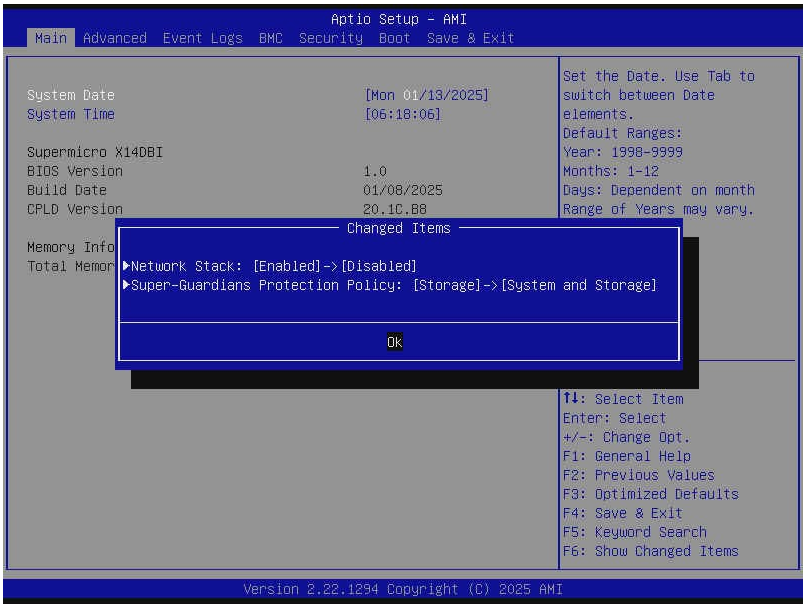


In this case, pressing <Enter> will go to the page that contains the selected BIOS item, which is KMS Security Policy.



Tips on using the <F6> key:

The <F6> key can be used as a hot key to display the BIOS settings that have been changed. After pressing <F6>, for example, the BIOS screen below appears. This BIOS screen indicates that "Network Stack" has been set to Disabled and "Super-Guardians Protection Policy" has been set to System and Storage.



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.

Unzip the BIOS file onto a USB device formatted with the FAT/FAT32 file system. When the UEFI shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier. Enter flash.nsh BIOSname#.### at the prompt to start the BIOS update process. Reboot the system when you see the message that BIOS update has completed.

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.

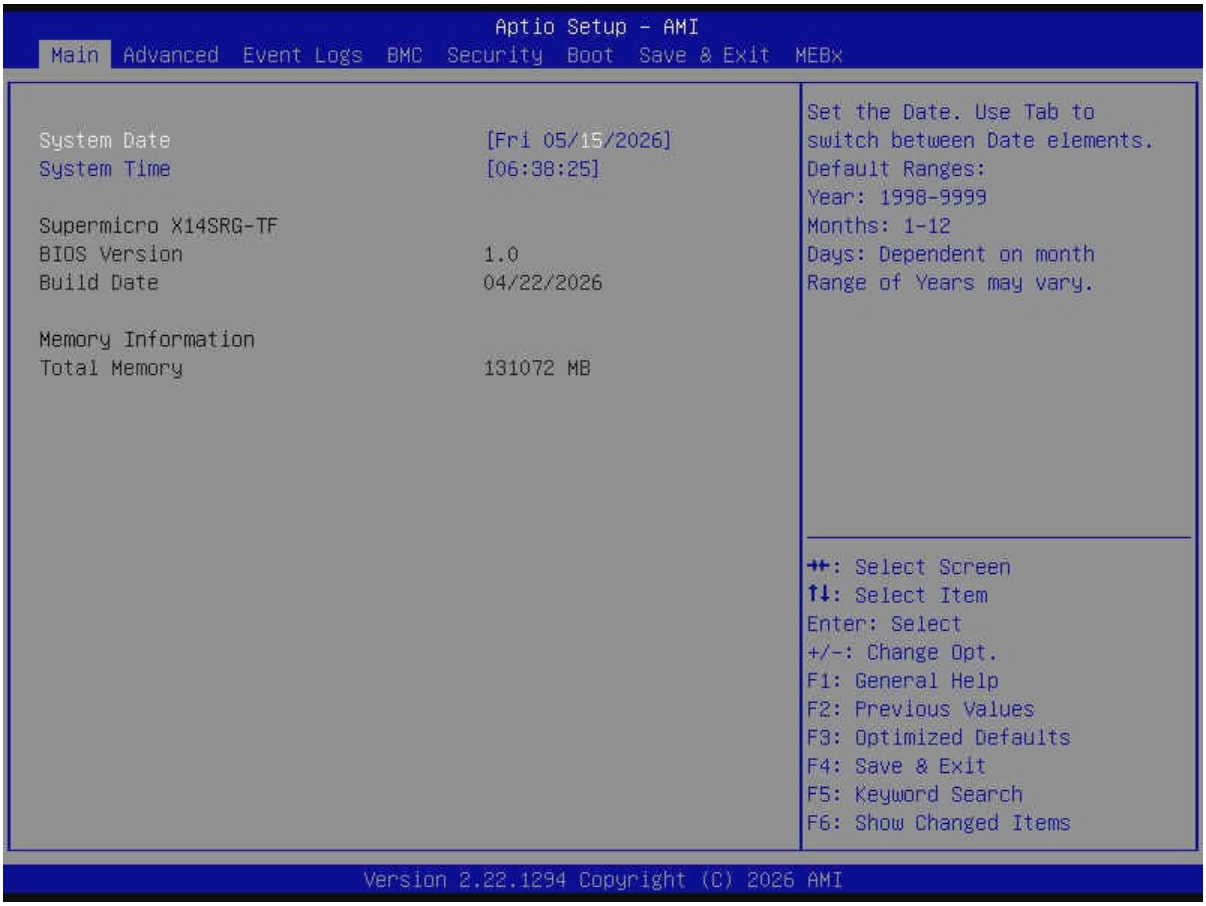


Figure 4-1. Main Screen

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.

SupermicroX14SRG-TF

BIOS Version

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

Build Date

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

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.

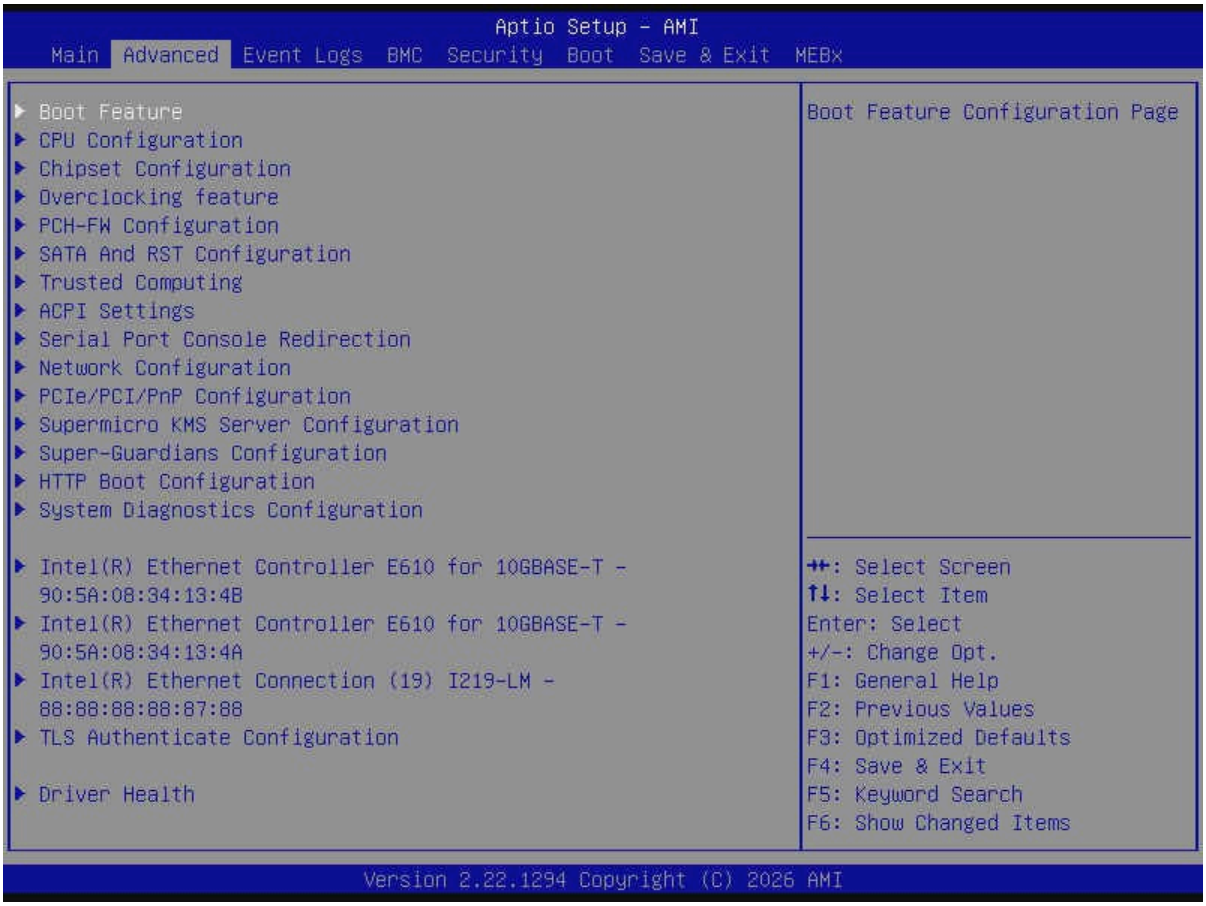


Figure 4-2. Advanced Setup Configuration Screen

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.

Re-try Boot

If this feature is set to EFI Boot, 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 EFI Boot.

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.

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 data transaction to enhance memory performance. The options are **Enabled** and Disabled.

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.

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**.

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.

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.

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 Advanced Programmable Interrupt Controller.)

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.

Note: This feature is NOT available when "TXT Support" is set to Enabled.

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.

Power Performance Tuning

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

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 Performance, **Balanced Performance**, Balanced Power, and Power. Please note that the options of Extreme Performance and Max Power Efficient are motherboard-dependent.

Note: This feature is available when "Power Performance Tuning" is set to BIOS Controls EPB.

CPU P State Control Menu

►CPU P State Control

AVX P1

Use this feature to set the appropriate TDP level for the system. The Intel Advanced Vector Extensions (Intel AVX) P1 feature allows you to set the base P1 ratio for Streaming SIMD Extensions (SSE) and AVX workloads. Each P1 ratio has the corresponding AVX Impressed Current Cathodic Protection (ICCP) pre-grant license level, which refers to the selection between different AVX ICCP transition levels. The options are **Nominal**, Level 1, and Level 2. This feature is CPU-dependent.

Note: This feature is available 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. Please refer to Intel's website for detailed information. The options are Disabled and **Enabled**.

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.

Note: This feature is available when "SpeedStep (P-States)" is set to Enabled.

Turbo Mode (Available when "SpeedStep (P-States)" is set to Enable")

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**.

Note: This feature is available when "SpeedStep (P-States)" is set to Enabled.

Hardware PM State Control Menu

►Hardware PM State Control

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

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**.

C1 to C1e Promotion

If this feature is set to Enabled, CPU will run at its minimum frequency for lower power consumption in the C1 state. The options are Disabled and **Enabled**. This feature is CPU-dependent.

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**.

Package C State Control Menu

►Package C State Control

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**.

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**.

SOCKET RAPL Config Menu

►SOCKET RAPL Config

Package RAPL Limit OSR Lock

Use this feature to enable or disable the locking of Package RAPL Limit CSR, and a reset will be required to unlock the register. The options are Disabled and **Enabled**.

PL1 Power Limit

This feature configures the PL1 Power Limit in Watts. The value may vary from 0 to the Fused TDP Value. If the value is 0, the Fused TOP value will be programmed. A value greater than the Fused TOP value will not be programmed. The default is **0**.

PL1 Time Window

This feature configures the PL1 value in seconds. The value may vary from 1 to 448. It indicates the time window over which TOP value should be maintained. The default is **20**.

PL2 Power Limit

This feature configures the PL2 Power Limit in Watts. The value may vary from 0 to 120% of the Fused TDP Value. If the value is 0, the BIOS will program 120% of the Fused TOP value. The default is **0**.

PL2 Time Window

This feature configures the PL2 value in seconds. The value may vary from 0.012 to 0.039. It indicates the time window over which the TDP value should be maintained. The default is **0.012**.

CPU Core Disable Bitmap Menu

►CPU Core Disable Bitmap

Available Bitmap[0]:

This feature displays the available Bitmap[0]. This feature is CPU-dependent.

Available Bitmap[1]:

This feature displays the available Bitmap[1]. This feature is CPU-dependent.

Disable Bitmap[0]:

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**.

Disable Bitmap[1]:

Enter 0 to enable this feature for CPU Core Bitmap[1]. Enter FFFFFFFFFF to disable CPU Core Bitmap[1]. 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**. This feature is available when the number of CPU cores is greater than 128.

Chipset Configuration Menu

►Chipset Configuration

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

North Bridge Menu

►North Bridge

Uncore Configuration Menu

►Uncore Configuration

The following information is displayed.

- Number of CPU
- Global MMIO Low Base / Limit
- Global MMIO High Base / Limit
- PCIe Configuration Base / Size

SNC

Sub NUMA Clustering (SNC) is a feature that breaks up the Last Level Cache (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.

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

Integrated Memory Controller (IMC)

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.

Memory Frequency

Enforce Population POR

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

Memory Frequency

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

DDR 2x Refresh Enable

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

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 RAS Configuration Menu

►Memory RAS Configuration Setup

Memory RAS Configuration Setup

Mirror Mode

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

Mirror Mode.

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 **200**.

ADDDC Sparing (Available when "Mirror Mode" 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.

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.

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**.

In Field Scan (IFS) Menu

►In Field Scan (IFS)

Scan at Field (SAF, S@F) [Outputs]

SAF activation state

This feature displays the Scan at Field (SAF) activation state.

Scan at Field (SAF, S@F) [Inputs]

Enable SAF

Select Enabled to enable the Intel SAF feature, which tests the CPU core logic for faults by using scan test images. The options are **Disabled** and Enabled.

IIO Configuration Menu

►IIO Configuration

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 Per-Port.

IIO eDPC Support

Use this feature to enable or disable the IIO eDPC support. The options are **Disabled**, On Fatal Error, and On Fatal and Non-Fatal Errors.

IIO eDPC Interrupt (Not available when "IIO eDPC Support" is set to Disabled)

Use this feature to enable or disable IIO enhanced DPC interrupt. The options are **Disabled** and Enabled.

IIO eDPC ERR_COR Message (Not available when "IIO eDPC Support" is set to Disabled)

Use this feature to enable or disable IIO enhanced DPC error correction message. 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

VMD must be enabled on PCIe ports which have NVMe drives attached to them in order for those drives to be added to a VROC RAID configuration. The default setting for the NVMe Mode Switch is **Manual** which allows you to select specific NVMe ports on which to enable VMD. When this feature is set to VMD, VMD support will be automatically enabled for all NVMe ports despite the lack of the VROC Key.

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.

Hot Plug

Set this feature to Enable for hot plug support, which allows you to replace a SATA drive without shutting down the system. The options are Disabled and **Enabled**.

CPU Configuration Menu

►PCI Express 0 / PCI Express 2 / PCI Express 3 / PCI Express 4 / PCI Express 5 / PCI Express 6 / PCI Express 7 / PCI Express 8

Note: Available PCI Express # features are CPU-dependent. Refer to the table below for the mapping of PCI Express # to PCIe slots of the motherboard.

PCI Express #	PCIe slots	Availability
PCI Express 0	P1 SLOT9 PCIe 5.0 X16	Available to Intel Xeon 600 Series processors
PCI Express 2	P1 SLOT5 PCIe 5.0 X16	
PCI Express 3	M.2-C1 5.0X4 M.2-C2 5.0X4 P1 SLOT11 PCIe 5.0 X8	
PCI Express 4	P1 SLOT3 PCIe 5.0 X16	
PCI Express 5	P1 SLOT7 PCIe 5.0 X16	
PCI Express 6	P1_NVME0 P1_NVME1 P1_NVME2 P1_NVME3	Only available to Intel Xeon 690/670/650 Series processors
PCI Express 7	P1_NVME4 P1_NVME5 P1_NVME6 P1_NVME7	
PCI Express 8	P1 SLOT1 PCIe 5.0 X16	

Intel VMD Technology

When this feature is set to Enabled, VMD support will be enabled on the IIO domain. The options are **Disabled** and Enabled.

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, x4x4x_x8, x_x8x4x4, x_x8x_x8, x_x_x_x16, x2x2x4x_x8, x4x2x2x_x8, x_x8x2x2x4, x2x2x4x4x4, x4x2x2x4x4, x4x4x2x2x4, x2x2x2x2x_x8, x2x2x2x2x4x4, x2x2x4x2x2x4, x4x2x4x2x2x4, x2x2x2x2x2x2x4, x_x8x4x2x2, x4x4x4x2x2, x_x8x2x2x2x2, x2x2x4x4x2x2, x4x2x2x4x2x2, x4x4x2x2x2x2, x2x2x2x2x4x2x2, x2x2x4x2x2x2x2, x4x2x2x2x2x2x2, and x2x2x2x2x2x2x2x2.

►P1 SLOT9 PCIe 5.0 X16 / P1 SLOT5 PCIe 5.0 X16 / M.2-C1 5.0X4 / M.2-C2 5.0X4 / P1 SLOT11 PCIe 5.0 X8 / P1 SLOT3 PCIe 5.0 X16 / P1 SLOT7 PCIe 5.0 X16 / P1_NVME0–3 / P1_NVME4–7 / P1 SLOT1 PCIe 5.0 X16

Note: The P1_NVME0–3, P1_NVME4–7, and P1 SLOT1 PCIe 5.0 X16 features are only available to Intel Xeon 690/670/650 Series processors.

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**.

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 on Port

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 enabled on the specific root port. The options are **Disabled** and Enabled.

Note: 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.

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

►Intel VT for Directed I/O (VT-d)

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. The options are Enabled and **Disabled**. (ACS is the abbreviation for Access Control Services.)

South Bridge Menu

►South Bridge

XHCI Hand-off

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

PCI Express Configuration

PCI Express Configuration

►M.2-P2 PCIe 4.0X4 / M.2-P1 PCIe 4.0X4

ASPM

Use this feature to activate the Active State Power Management (ASPM) level for a PCIe device. Select Auto for the system BIOS to automatically set the ASPM level based on the system configuration. Select Disabled to disable ASPM support. The options are Disabled, L1, and **Auto**.

L1 Substates

Use this feature to set the PCI Express L1 Substate. The options are Disabled, L1.1 and **L1.1 & L1.2**.

PCIe Speed

Use this feature to set the PCI Express port speed. The options are **Auto**, Gen1, Gen2, Gen3, and Gen4.

Overclocking Feature Menu

Note: This menu is only available for processors that support overclocking feature.

Overclocking Feature

Select Enabled to enable performance(overclocking) menu for processor and memory. The options are Disabled and **Enabled**.

Important: The overclocking configuration is intended for validation and system characterization purposes only. Operating outside Supermicro's reference values may cause overheating, system crashes, or data loss, and may void the product warranty.

The following features are available when "Overclocking Feature" is set to Enabled.

OCMB Interface Version

This feature displays the version of the OCMB interface .

OverVolt Protection

When this feature is enabled, you will not be able to program over voltage in OS runtime. It’s recommended to keep it enabled by default. The options are Disabled and **Enabled**.

Thermal Turbo

Select Enabled to enable the Intel Thermal Turbo feature. The options are Disabled and **Enabled**.

FII Overclocking Mode Select

Enter a FLL mode value in the range of 0–1. 0x0 means no overclocking, and 0x1 means ratio overclocking with nominal (0.5–1x) reference clock frequency.The default is **0**.

Overclocking Information Menu

►Overclocking Information

This feature displays the processor and specific domain overclocking capabilities.

►Overclocking Capability

This feature displays the overclocking capability information of the CPU being detected. The information is retrieved from the CPU using OC Mailbox Command 0x02.

- Domain 0 : CPU
- Domain 2 : Mesh/Ring
- Domain 4 : VCC_CFN
- Domain 7 : VCC_HDC
- Domain 8 : VCC_DDRD
- Domain 9 : VCC_INF

►Per-Core Turbo Ratio Limit

This feature displays the turbo ratio limit for each individual CPU core. The information is retrieved from the CPU using OC Mailbox Command 0x02, for example:

- Level 0: IA/SSE
  - Bucket 3:0
  - Bucket 7:4
- Level 1: Light Intensity (AVX2)
  - Bucket 3:0
  - Bucket 7:4
- Level 2: Medium Intensity (AVX512)

- Bucket 3:0
- Bucket 7:4

- Level 3: High Intensity (AMX/TMUL)
  - Bucket 3:0
  - Bucket 7:4

►P0 Ratio and Voltage

This feature displays P0 ratio and P0 voltage information, which is retrieved from the CPU using OC Mailbox Command 0x07.

P0 Ratio

P0 Voltage

Per Core Ratio Configurations Menu

►Per Core Ratio Configurations

Per Core Control

This feature allows you to configure the maximum overclocking ratio for each CPU core. When enabled, it sets the maximum overclocking ratio to each individual core by using OCMB 0x1D command. When disabled, it sets the ratio to all cores by OCMB 0x11 command. The options are **Disabled** and Enabled.

Processor Menu

►Processor

VF Configuration Scope

Use this feature to select whether to use a single Voltage Frequency (VF) curve for all cores or a separate VF curve for each individual core. The options are **All-core** and Per-core.

Light Intensity Ratio Offset

This feature controls the Light Intensity (AVX2) ratio offset. Use this feature to specify the number of bins to decrease Light Intensity ratio vs. Core Ratio. Light Intensity is a more stressful workload, and it is helpful to lower the Light Intensity ratio to ensure maximum possible ratio for SSE workloads. The configuration uses Mailbox MSR 0x150, cmd 0x1B. The range is 0–31 and the default is **0**.

Medium Intensity Ratio Offset

This feature controls the Medium Intensity (AVX2) ratio offset. Use this feature to specify the number of bins to decrease Medium Intensity ratio vs. Core Ratio. Medium Intensity is a more stressful workload, and it is helpful to lower the Medium Intensity ratio to ensure maximum possible ratio for SSE workloads. The configuration uses Mailbox MSR 0x150, cmd 0x1B. The range is 0–31 and the default is **0**.

High Intensity Ratio Offset

This feature controls the High Intensity (AVX2) ratio offset. Use this feature to specify the number of bins to decrease High Intensity ratio vs. Core Ratio. High Intensity is a more stressful workload, and it is helpful to lower the High Intensity ratio to ensure maximum possible ratio for SSE workloads. The configuration uses Mailbox MSR 0x150, cmd 0x1B. The range is 0–31 and the default is **0**.

TjMax Override

Use this feature to specify the value to support TjMax in the range of 105 to 115 degree Celsius. The configuration uses Pcode Mailbox 0xAC. The range is 105–115 and the default is **0** (no override).

Core Min Ratio

Use this feature to specify the minimum core ratio allowed during overclocking. Enter a value ranging from Min Operating Ratio (IaMinRatio) to Max Non-Turbo Ratio in the unit of 100 Mhz. The BIOS will dynamically clip to the boundary values if the value is out of range. The default is **0**.

Mesh (Ring) Menu

►Mesh (Ring)

Mesh(Ring) on TPMI

Max Ratio

Use this feature to specify the maximum ratio for the Mesh (Ring) Domain. It uses TPMI UFS Register. The range is 0–127 and the default is **0**. Note that the Max Ratio SHOULD NOT be less than the Min Ratio. If Max Ratio and Min Ratio are both 0, then the process will be skipped. The default is **0**.

Min Ratio

Use this feature to specify the minimum ratio for the Mesh (Ring) Domain. It uses TPMI UFS Register. The range is 0–127 and the default is **0**. Note that the Max Ratio SHOULD NOT be less than the Min Ratio. If Max Ratio and Min Ratio are both 0, then the process will be skipped.

The default is **0**.

Mesh(Ring) on OC Mailbox

Uncore Menu

►Uncore

VCCCFN Voltage Offset

Use this feature to specify the voltage offset (in mV) applied to the VCCCFN. The range is -500–500 and the default is **0**.

Offset Prefix

Use this feature to set the offset prefix value as a positive (+) or a negative (-). The options are "**+**" and "-".

VCCHDC Voltage Override

Use this feature to specify the override voltage (in mV) applied to the VCCHDC domain. The configuration uses Mailbox MSR 0x150, cmd 0x11. The range is 500–1395 and the default is **0** (no override).

VCCDDRD Voltage Override

Use this feature to specify the override voltage (in mV) applied to the VCCDDRD domain. The configuration uses Mailbox MSR 0x150, cmd 0x11. The range is 500–1325 and the default is **0** (no override).

VCCINF Voltage Override

Use this feature to specify the override voltage (in mV) applied to the VCCINF domain. The configuration uses Mailbox MSR 0x150, cmd 0x11. The range is 550–1235 and the default is **0** (no override).

SVID/VCCIN Menu

►SVID/VCCIN

SVID Support

Use this feature to enable Serial Voltage Identification (SVID). Disabling SVID will disable input voltage overrides. The configuration uses Mailbox MSR 0x150, cmd 0x13. The options are Disabled and **Enabled**.

VccIn Voltage

This feature is available when "SVID Support" is set to Enabled. This feature overrides the Vccin input voltage. It controls the input voltage to the CPU and will affect all CPU domains. The configuration uses Mailbox MSR 0x150, cmd 0x13. The range is 0–3000 mV and the default is **0**.

CPU VccIn Voltage Level

This feature is available when "SVID Support" is set to Disabled. Use this feature to specify the VID value (in decimal) for the CPU VccIn voltage level. Each step is 10 mV and default is **1800**. The range is 500–3050mV.

Voltage PLL Trim Controls

► Voltage PLL Trim Controls

Voltage PLL Trim Controls

Core PLL Voltage Offset / RING PLL Voltage Offset / Memory Controller PLL Voltage Offset

Enter a value to set the Phase-locked Loop (PLL) voltage offset for each domain. This control can be used to increase the range of this domain frequency in extreme overclocking conditions. The range is 0–63 and the default is **0**. Units are in 17.5 mV.

Max Voltage Limits Menu

►Max Voltage Limits

Process Vmax Limit

Use this feature to enable the Vmax limit. Disabling the Vmax limit will allow you to set any voltage. However, disabling the voltage limit checks may cause permanent damage to processor. Disabling limit check will persist until next cold boot. The options are Disabled and **Enabled**.

Package Scope Configurations

Domain 4 : VCC_CFN / Domain 7 : VCC_HDC / Domain 8 : VCC_DDRD / Domain 9 : VCC_INF

Max Voltage Limits

Enter a value (in mV) to set the maximum voltage limits for the overclocking. The range is 0–2000 and the default is **0**.

Note: Only CPU and Ring domains support multi-die; other domains use the settings across the package scope.

Per Core Hyper Threading Configuration Menu

This setting can't override global hyper-threading is disabled. When global hyper-threading is disabled, the Per Core Hyper Threading Configuration menu will be hidden.

Overclocking Menu

►Overclocking

Extreme Edition

This feature enables or disables the Extreme Edition support. The options are Disabled and **Enabled**.

Overclocking Lock

This feature enables or disables the overclocking lock feature. The options are Disabled and **Enabled**.

AVX Support

This feature enables or disables the AVX instructions. The options are Disabled and **Enabled**. This feature is CPU-dependent.

AVX3 Support (Available when "AVX Support" is set to Enabled)

This feature enables or disables the AVX3 instructions. The options are Disabled and **Enabled**. This feature is CPU-dependent.

AMX Support (Available when "AVX3 Support" is set to Enabled)

This feature enables or disables the AMX instructions. The options are Disabled and **Enabled**. This feature is CPU-dependent.

CurrentTurboRatioLimit0–7 (Available when "Extreme Edition" is set to Enabled)

This features displays the current turbo ratio limit for each individual CPU core.

TurboRatioLimit0–7 (Available when "Extreme Edition" is to Enabled)

This feature allows you to set the turbo ratio limit for an individual CPU core. If Processor Clocking Technology (PCT) is enabled, the ratio is forced to OxFF unless you manually set a ratio. The default is **0**.

Memory Overclocking Menu

►Memory Overclocking

When configuring the Extreme Memory Profile (XMP), note that:

- Parameters updated for user profile will only take effect after the boot.
- Only one user profile can be updated in a single boot.

XMP Profile

This feature controls the XMP profile. When this feature is set to Manual, the system selects the XMP profile interactively. The options are **Disabled** and Manual.

The following features are available when "XMP Profile" is set to Manual.

Memory Voltage

Use this feature to select the desired voltage value. To select 1.500V, enter 1500. The default is **1115**.

Pmic Vdd Voltage

Use this feature to select the desired voltage value. To select 1.500V, enter 1500. The default is **1100**.

Pmic VddQ Voltage

Use this feature to select the desired voltage value. To select 1.500V, enter 1500. The default is **1100**.

Pmic Vpp Voltage

Use this feature to select the desired voltage value. To select 1.500V, enter 1500. The default is **1800**.

Memory Frequency

Use this feature to set the Maximum Host DDR Memory Frequency in MT/s. If this feature is set to Auto, a frequency will be chosen automatically based on the minimum tCK given by the SPD. If Enforce POR is disabled, the system will be able to run at higher frequencies than the memory support (limited by processor support). The options are **Auto**, 4800, 5200, 5600, 6000, 6400, 6800, 7200, 7600, and 8000. Note that the available options are CPU-dependent.

CL Support

Enter a value for desired CL Support. The default is **0** (Auto).

Command Timing

This feature controls the desired memory controller command timing. The options are **Auto**, 1N, and 2N.

CAS Latency / tRP / tRCD

Enter a value for desired latency. 0–4 means "Auto" while 5–11 means " Desired".

tRAS / tWR

Enter a value for desired latency. The default is **0** (Auto).

tRC / tRFC1 / tRFC2 / tRFCsb

Enter a value for each of these features. The default is **0** (Auto).

tCCD_Lmin / tCCD_L_WRmin / tCCD_L_WR2min / tCCD_L_WTRmin / tCCD_S_WTRmin / tRRD_Lmin / tRTP min / tFAW min

Enter a value for each of these features. The default is **0** (Auto).

PCH-FW Configuration

The following PCH firmware information is displayed

- ME Firmware Version
- ME Firmware Mode
- ME Firmware SKU

SATA and RST Configuration

Controller 1 SATA And RST Configuration

SATA Configuration

Use this feature to enable or disable the onboard SATA controller(s) supported by the Intel PCH chip. The options are Disabled and **Enabled**.

The following features are available when "SATA Configuration" is set to Enabled.

SATA Mode Selection

Use this feature to select the mode of installed SATA drives. The options are **AHCI** and RAID.

Notes:

- After changing the SATA mode, make sure to reboot the system for the changes to take effect.
- To create RAID for the SATA drives, refer to the "Intel(R) VROC SATA Controller Menu" on page 160 section for more information.

Support Aggressive Link Power Management

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

SATA SGPIO Enable

Use this feature to change the serial GPIO mode for SATA controller. The options are **Disabled** and Enabled.

SATA0 / SATA1 / SATA2 / SATA3 / SATA4 / SATA5 / SATA6 / SATA7

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

Software Preserve Support

Hot Plug

Set this feature to Enable for hot plug support, which allows you to replace a SATA drive without shutting down the system. The options are Disabled and **Enabled**.

Spin Up Device

Set this feature to enable or disable the PCH to initialize the device. The options are **Disabled** and Enabled.

SATA Device Type

Use this feature to specify if the SATA port is connected to a Solid State Drive or a Hard Disk Drive. The options are **Hard Disk Drive** and Solid State Drive.

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.

SHA-1 PCR Bank (Available when "Security Device Support" is set to Enabled)

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

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**.

TPM 2.0 Interface Type

This feature displays the interface type of the TPM 2.0 device.

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.

ACPI Settings Menu

►ACPI Settings

WHEA Support

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

Serial Port Console Redirection Menu

►Serial Port Console Redirection

COM1 / SOL/COM2 / AMT SOL

Console Redirection

Select Enabled to enable COM1, SOL/COM2, or AMT SOL 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**.

Notes:

- The "SOL/COM2" here indicates a shared serial port, and SOL is used as the default.
- The Console Redirection feature for "AMT SOL" can be configured only when "Intel(R) AMT" under the MEBx menu is set to Enabled and "Network Access State" under "Intel(R) AMT Configuration" is set to Network Active. The AMT changes take effect after you save settings and reboot the system.

►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 Configuration Menu

►Network 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:

Above 4G Decoding

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

MMIO High Base

Use this feature to select the base memory size according to memory-address mapping for the I/O hub. The options are 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, 1024G, and **Auto**. This feature is motherboard-dependent.

Re-Size BAR Support

Use this feature to enable Resizable Base Address Register (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

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**.

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.

Consistent Device Name Support

This feature controls the device naming for network devices and slots. 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**.

Onboard LAN1 Option ROM

Select EFI to boot the computer using the EFI device installed on LAN port 1. The options are Disabled and **EFI**.

Note: This feature is available when your motherboard supports onboard LAN ports.

P1 SLOT1/3/5/7/9 PCIe 5.0 X16 OPROM / P1 SLOT11 PCIe 5.0 X8 OPROM

M.2-P1/M.2-P2/M.2-C1/M.2-C1 OPROM

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

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.

Note: This feature is available when "TPM-KMS Support" is set to Disabled.

Second Supermicro KMS Server IP address

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

Note: This feature is available when "TPM-KMS Support" is set to Disabled.

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.

Note: This feature is available when "TPM-KMS Support" is set to Disabled.

KMS Time Out

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

Note: This feature is available when "TPM-KMS Support" is set to Disabled.

TimeZone

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

Note: This feature is available when "TPM-KMS Support" is set to Disabled.

Client UserName (Available when "Client Private Key" below has been set)

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

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

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

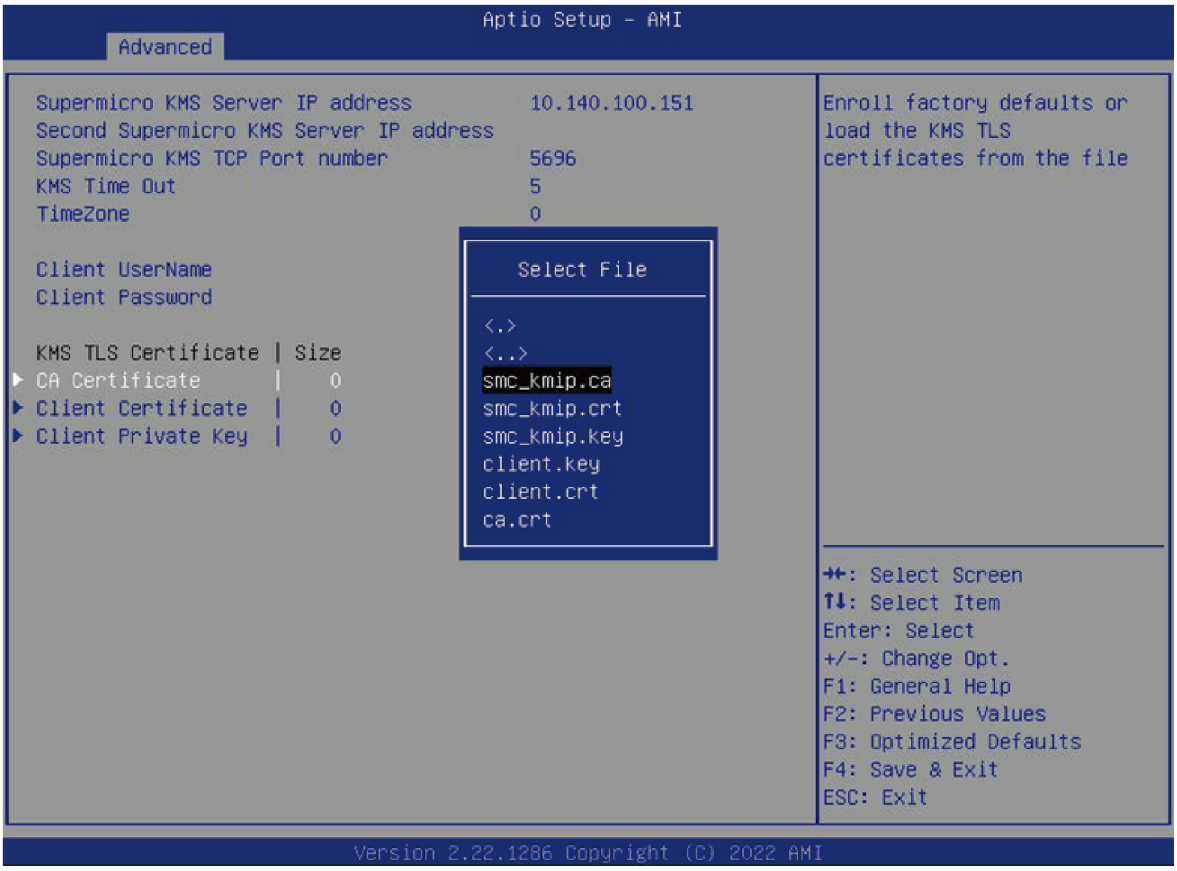
►CA Certificate

►Client Certificate

►Client Private Key

Note: The three features above are available for configuration when "TPM-KMS Support" is set to Disabled.

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.

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. 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.

System Diagnostics Configuration Menu

►System Diagnostics Configuration

Launch System Diagnostics

Set this feature to Launch Once to launch system diagnostics on next system boot. This feature is used to run hardware tests that check the health of system components and help identify any issues. The options are **Disabled** and Launch Once.

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

Intel(R) Ethernet Controller E610 for 10GBASE-T - (MAC address) Menu

►Intel(R) Ethernet Controller E610 for 10GBASE-T - (MAC address)

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. Highlight this feature and enter a number of seconds in the range of 0 to 15 to set the amount of seconds to blink the LED. The default setting is **0**.

The following LAN port information will be displayed:

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

- MAC Address
- Virtual MAC Address

Firmware Image Properties

The following firmware image information is displayed.

- Option ROM version
- Unique NVM/EEPROM ID
- NVM Version

NIC Configuration

Link Speed

This feature displays the connection speed of a LAN port. It is set to **Auto Negotiated**.

Wake On LAN

If this feature is set to Enabled, the LAN port you specified will be enabled when the system is powered on. The options are Disabled and **Enabled**.

Legacy Virtual LAN ID

This feature specifies the VLAN ID used for PXE VLAN Mode. The valid VLAN ID range is from 10 to 4094. PXE VLAN is disabled if the VLAN ID is set to 0. The default is **0**.

Note: This setting is only applicable when the System ROM boots in Legacy BIOS Mode.

Intel(R) Ethernet Controller E610 for 10GBASE-T - (MAC address) Menu

►Intel(R) Ethernet Controller E610 for 10GBASE-T - (MAC address)

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. Highlight this feature and enter a number of seconds in the range of 0 to 15 to set the amount of seconds to blink the LED. The default setting is **0**.

The following LAN port information will be displayed:

- UEFI Driver
- Adapter PBA
- Device Name

- Chip Type
- PCI Device ID
- PCI Address
- Link Status
- MAC Address
- Virtual MAC Address

Firmware Image Properties

The following firmware image information is displayed.

- Option ROM version
- Unique NVM/EEPROM ID
- NVM Version

NIC Configuration

Link Speed

This feature displays the connection speed of a LAN port. It is set to **Auto Negotiated**.

Wake On LAN

If this feature is set to Enabled, the LAN port you specified will be enabled when the system is powered on. The options are Disabled and **Enabled**.

Legacy Virtual LAN ID

This feature specifies the VLAN ID used for PXE VLAN Mode. The valid VLAN ID range is from 10 to 4094. PXE VLAN is disabled if the VLAN ID is set to 0. The default is **0**.

Note: This setting is only applicable when the System ROM boots in Legacy BIOS Mode.

Intel(R) Ethernet Connection (19) I219-LM - (MAC address) Menu

Autonegotiation Timeout

This features controls how long the UEFI PXE driver should wait for link. The default is **8**.

PORT CONFIGURATION INFORMATION

The following LAN port information will be displayed:

- UEFI Driver
- Adapter PBA

- PCI Device ID
- PCI Address
- MAC Address

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 server Certificate Authority (CA).

►Enroll Certification

Use this feature to enroll the certificates in the system.

►Enroll Certification Using File

Use this feature to enroll the security certificates 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 certificates that have been enrolled in the system.

►Client Certification Configuration

This feature is to manage the certificates used to authenticate remote clients connecting to your system. Add, view, or delete client certificates as needed.

Intel(R) VROC SATA Controller Menu

Note: This submenu is available after you set the Advanced -> SATA And RST Configuration -> "SATA Mode Selection" feature to RAID, save the changes, and reboot the system for the changes to take effect.

Intel(R) VROC x.x.x.xxxx SATA Driver

This feature displays the Intel VROC SATA driver version.

►Create RAID Volume

This submenu is available when the BIOS detects two or more SATA storage devices.

Name

Enter a unique name for the RAID volume. The name must not contain space at the beginning or backslash and must be under 16 characters. The default is Volume1.

RAID Level

Select the desired RAID level for the RAID volume. The options are RAID0 (Stripe), RAID1 (Mirror), RAID5 (Parity), and RAID10 (RAID0+1). Available RAID levels depend on the number of disks connected to the system.

Select Disks

To select a desired RAID disk, select X from the drop-down list. Repeat this step to select all the desired disks for the RAID volume. For RAID0/RAID1/RAID5/RAID10, the minimum number of disks required is two/two/three/four respectively.

Strip Size (Available for RAID0/RAID5/RAID10 Only)

Select the desired RAID strip size for your RAID volume. The options vary according the RAID level you select.

Capacity (MB)

Enter the capacity in megabytes(MB) of the RAID volume to be created.

►Create Volume

After finishing the configuration of the Create RAID Volume feature, select Create Volume and you will return to the previous screen displaying the information about the created RAID volume.

RAID Volumes

This feature displays the RAID volumes you have created. You can click the created RAID volume to view more information.

RAID VOLUME INFO

Volume Actions

►Delete

This feature allows you to delete a RAID volume. When asked to confirm deletion of the RAID volume, select Yes to delete the RAID volume.

Note: When deleting a RAID volume, all data on the disks will be deleted as well.

If a RAID Volume has been created, the following information will be displayed:

- Name
- RAID Level
- Strip Size
- Size
- Status
- Bootable

RAID Member Disks

This feature displays the RAID member disks.

Reset to non-RAID

This feature allows you to reset a RAID member disks to non-RAID disk. When asked to remove the RAID structure on the disk, select Yes to reset the disk.

Note: When resetting a disk, all data on the disk will be deleted as well.

Non-RAID Physical Disks

This feature lists the disks which have not been added to a RAID volume. Selecting a non-RAID physical disk allowing you to take disk actions, and view disk information.

Disk Actions:

►Mark as Spare

A spare disk is used for automatic RAID volume rebuilds when the status of “failed”, “missing”, or “at risk” is detected on the array disk. For a RAID0 volume, only the status of “at risk” will trigger automatic RAID volume rebuilds. Marking a disk as a spare one will remove all data on the disk.

►Mark as Journaling Drive

A journaling drive is used as an error event log to record an event when an error occurs to a RAID5 volume. Marking a disk as a journaling drive will remove all data on the disk.

►Reset to Non-RAID

This submenu is available when a disk which has been marked as a spare or journaling drive.

For a spare or journaling disk, you can reset it to a non-RAID disk. Resetting a disk to non-RAID will remove all data on the disk.

Locate LED

The feature is not applicable to this motherboard. Please ignore this feature.

The following information is displayed.

- Port
- Controller
- Model Number
- Serial Number
- Size
- Status
- Block size
- Encryption ability
- Encryption status

Intel(R) Virtual RAID on CPU Menu

This submenu is only available when VMD is enabled on PCIe ports by either of the following methods:

- Go to Advanced -> Chipset -> North Bridge -> IIO Configuration > CPU Configuration -> PCI Express# and set the Intel VMD Technology to Enabled.
- Go to Advanced -> Chipset -> North Bridge -> IIO Configuration and set the NVMe Mode Switch feature to VMD.

Note: All the VMD changes take effect only after you save settings and reboot the system.

The following information is displayed:

- Intel(R) VROC x.x.x.xxxx VMD Driver
- Upgrade key
- Intel VROC Managed Controllers

►All Intel VMD Controllers

The device information will be displayed in the Non-RAID Physical Disks.

For detailed instructions on how to configure VROC RAID settings, refer to the RAID Configuration User Guides posted on our website at https://www.supermicro.com/support/manuals.

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. 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.

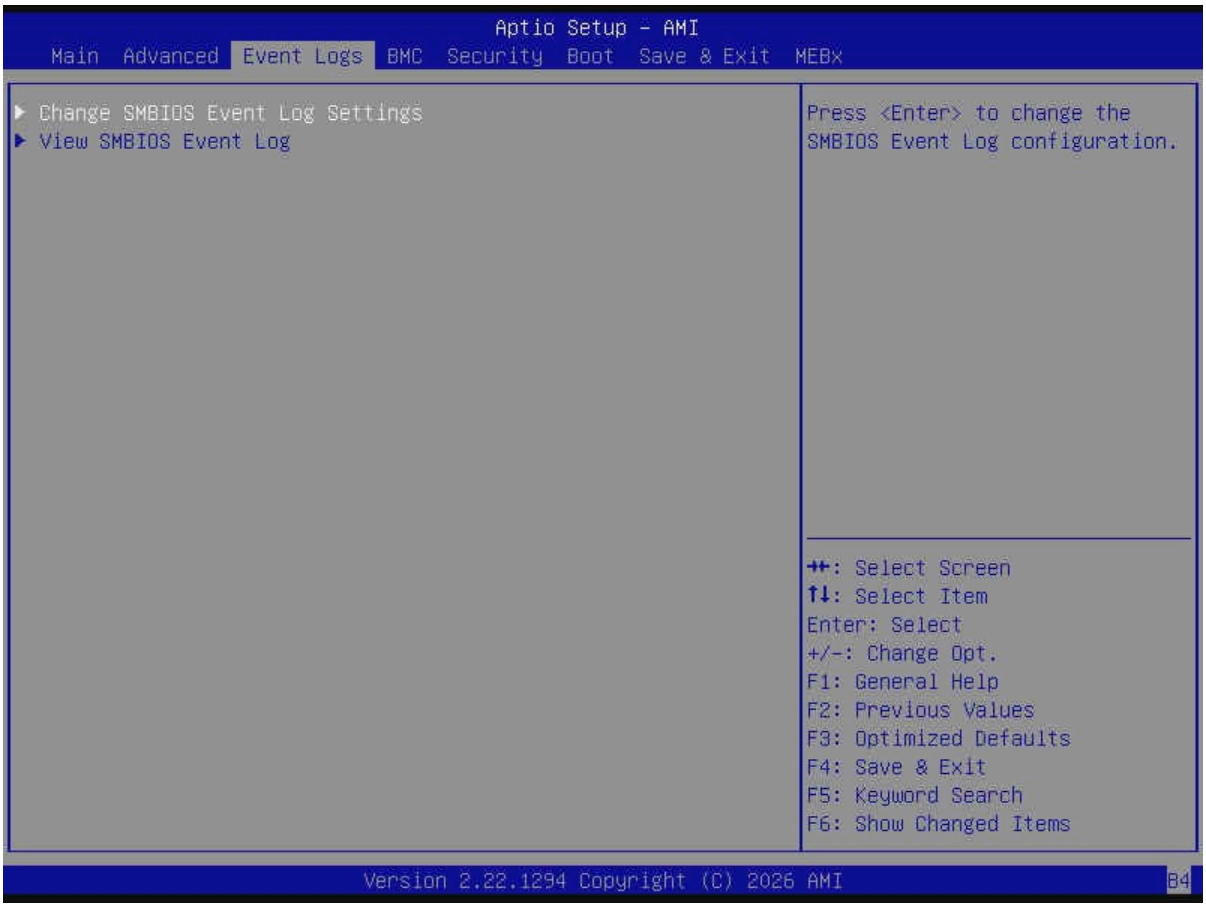


Figure 4-3. Event Logs Screen

►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.

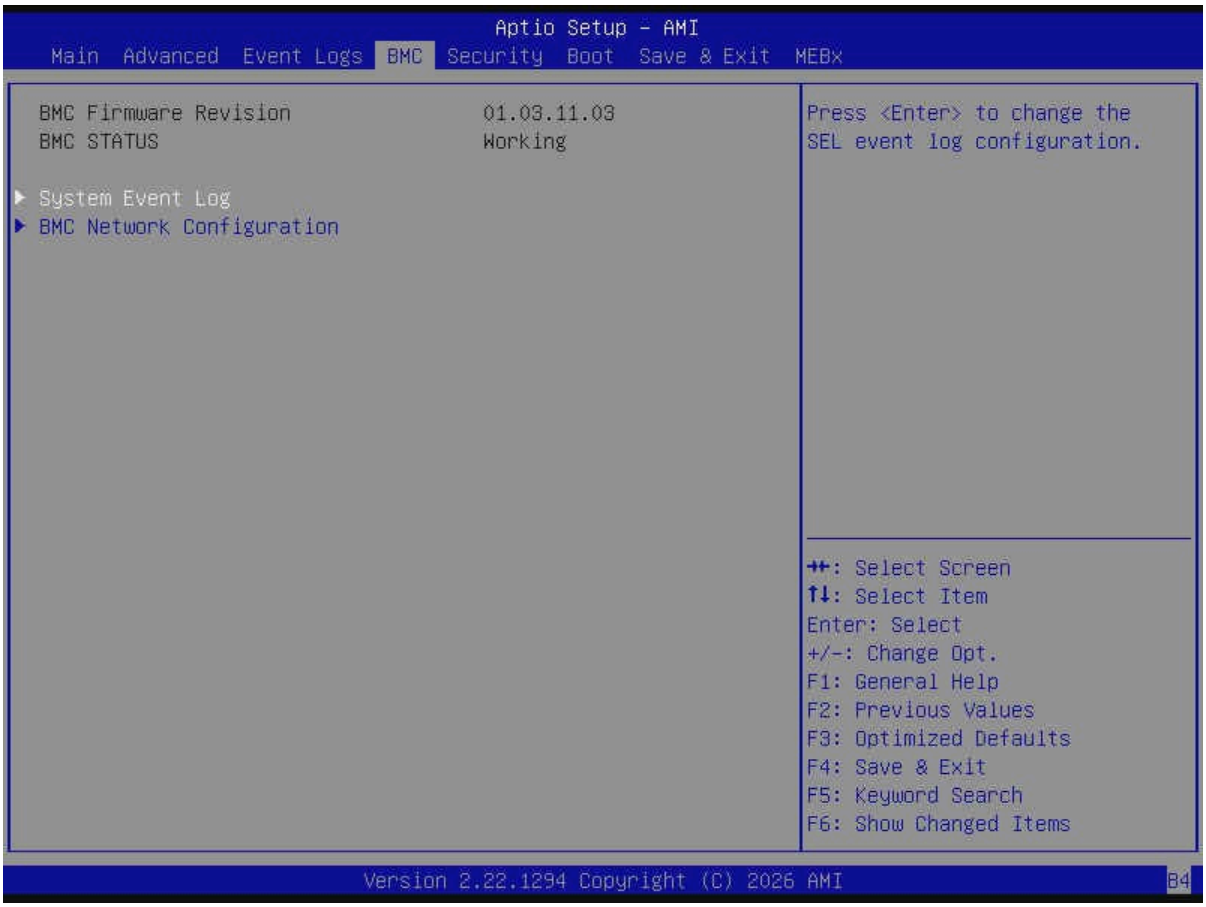


Figure 4-4. BMC Screen

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 next system reboot.

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 the system 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 the system. MAC addresses are six two-digit hexadecimal numbers.

Gateway IP Address

This feature displays the IPv4 gateway IP address for the system. 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.

4.6 Security

Use this menu to configure the following security settings for the system.

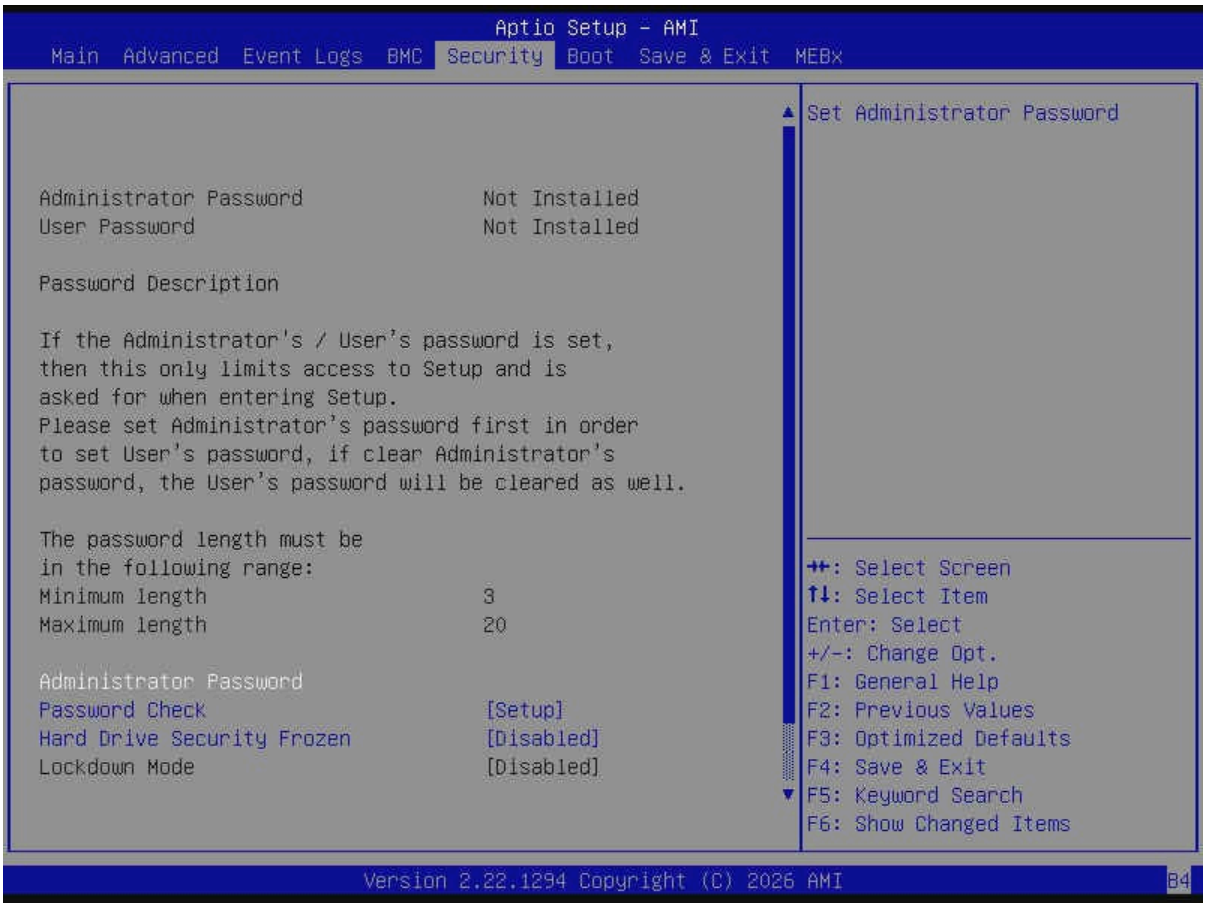


Figure 4-5. Security Screen

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. (SID is the abbreviation for Storage ID Authority.)

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.

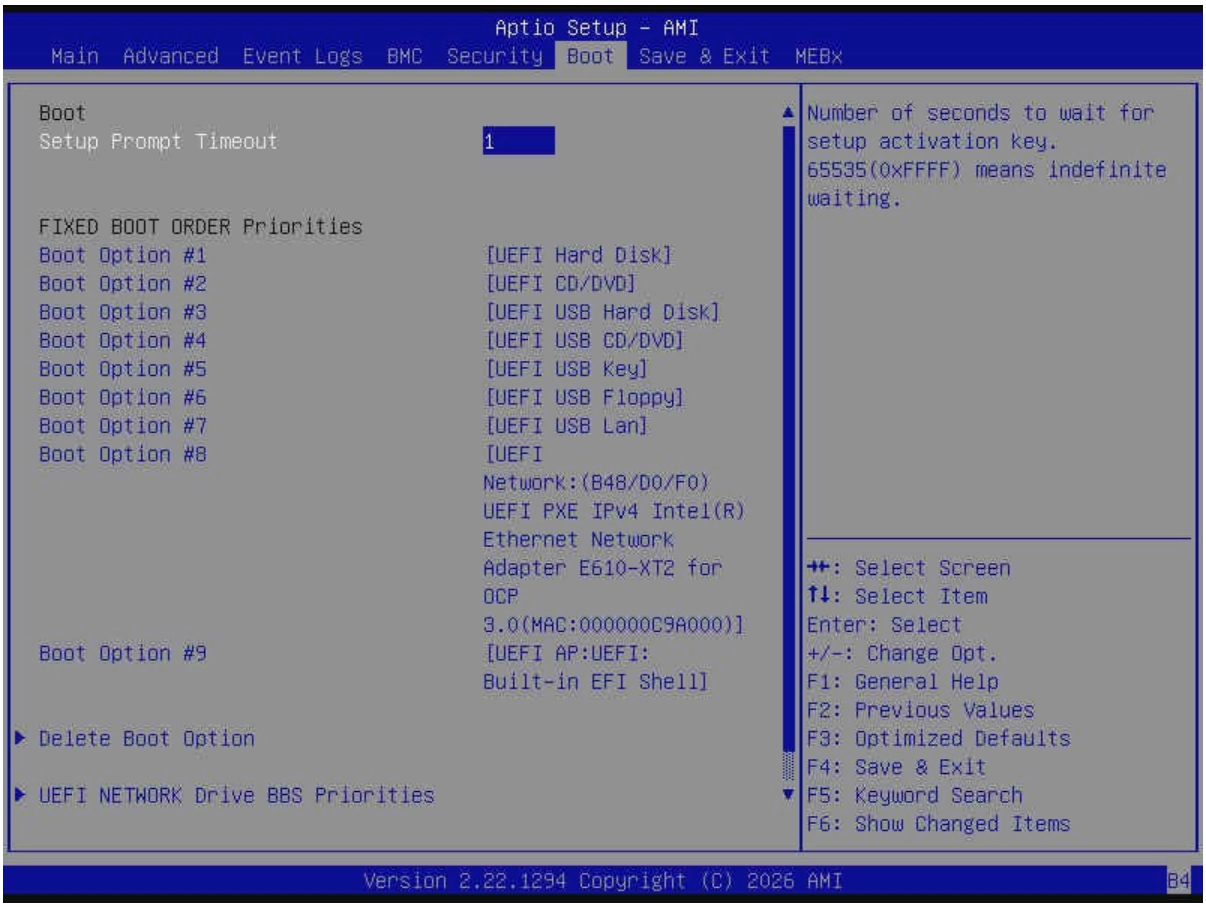


Figure 4-6. Boot Screen

FIXED BOOT ORDER Priorities

Use this feature to prioritize the order of bootable devices 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.

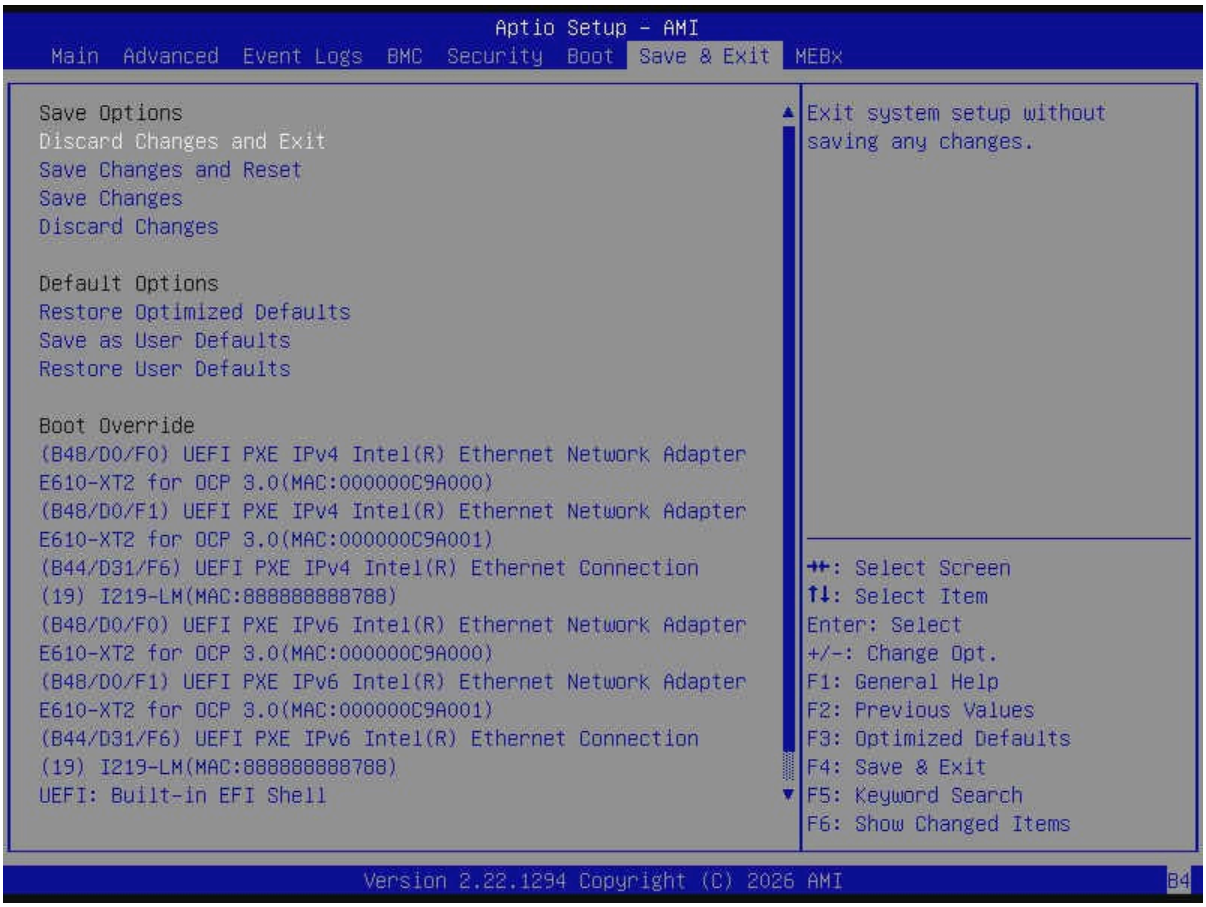


Figure 4-7. Save & Exit Screen

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 system.

Save Changes and Reset

On completing the system configuration changes, use this feature to exit the BIOS Setup utility and reboot the system 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 restore 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.

4.9 MEBx

Use this menu to create a password for MEBx.

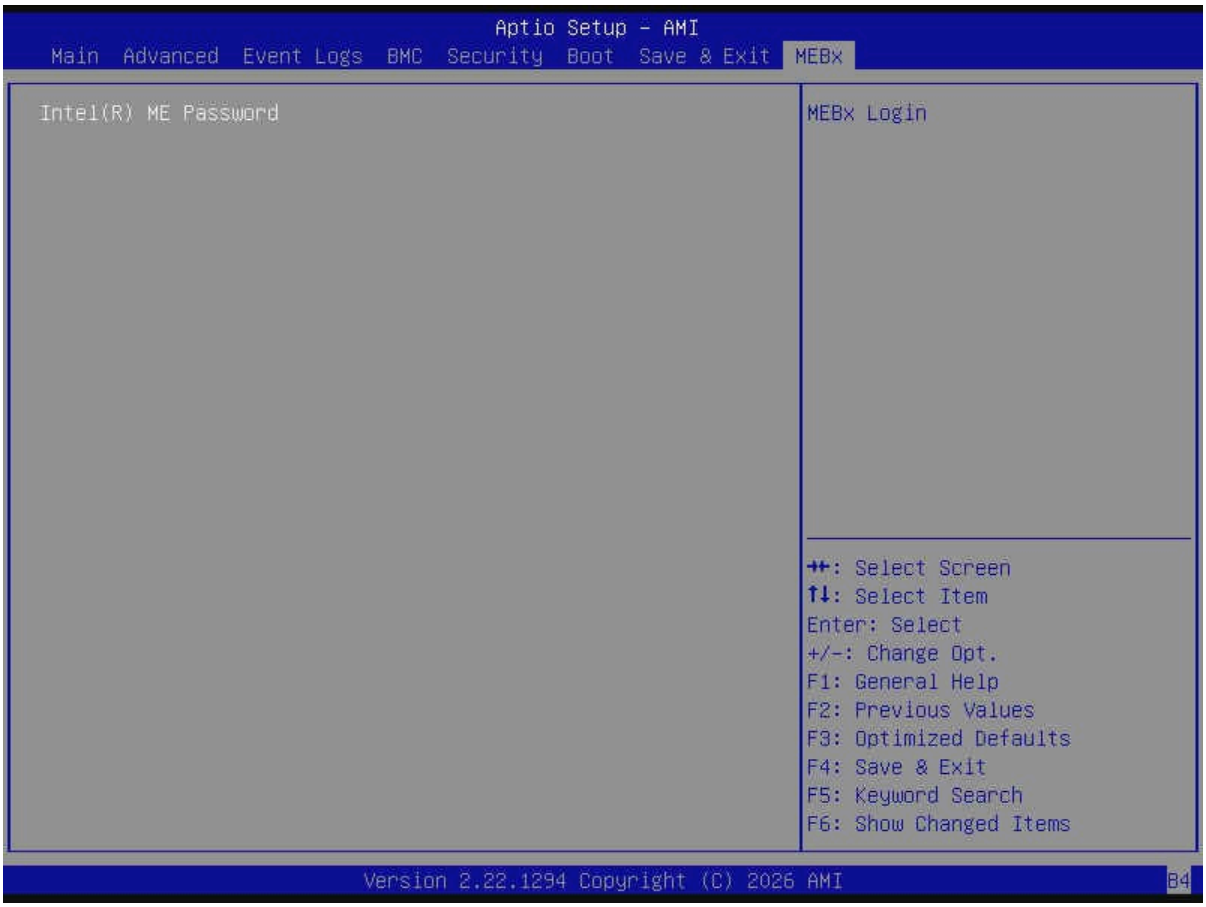


Figure 4-8. MEBx Screen

Intel(R) ME Password

Enter the password to bring up the Intel Management Engine (ME) setting menu. If you are the first time login, you will need to enter the default password. Intel ME will then prompt you to generate a new password. Please follow the guidelines below to set a new password.

- Password length must be between 8 and 32 characters.
- Must contain both upper and lower case letter.
- Must have at least one numeric character.
- Must have at least one ASCII non-alphanumeric character (!, @, #, $, %, ^, &, *).

Intel(R) AMT (Available after entering a password for Intel(R) ME Password)

Use this feature to enable or disable Active Management Technology (AMT). The options are Disabled, Partially Disabled, and **Enabled**. Changes take effect after you save settings and reboot the system.

Change Password (Available after entering a password for Intel(R) ME Password)

Press Enter and follow the prompt to change the password.

Intel(R) AMT Configuration

►Intel(R) AMT Configuration Menu

This feature is available when Intel(R) AMT is set to Enabled and take effect after you save settings and reboot the system.

Redirection features

►Redirection features Menu

SOL

Use this feature to enable the SOL firmware interface. The options are Disabled and **Enabled**.

Storage Redirection

Use this feature to enable the firmware remote storage redirection. The options are Disabled and **Enabled**.

User Consent

►User Consent Menu

User Opt-in

Use this feature to configure when user consent is required. The options are **None** and ALL.

Opt-in Configurable from Remote IT

Use this feature to enable or disable the remote change capability of the User Opt-in feature. The options are Disabled and **Enabled**.

Password Policy

Password Policy

Use this feature to set the password policy. The options are Default Password Only, During Setup And Configuration, and **Anytime**.

Network Setup

►Network Setup

Intel(R) ME Network Name Settings

►Intel(R) ME Network Name Settings Menu

FQDN

Use this feature to specify the fully qualified domain name.

Shared/Dedicated FQDN

Use this feature to select dedicated or shared for the fully qualified domain name. The options are Dedicated and **Shared**.

TCP/IP Settings

►TCP/IP Settings

►Wired LAN IPv4 Configuration

DHCP Mode

Use this feature to enable or disable IPv4 DHCP mode. The options are Disable and **Enabled**.

The following features are available when "DHCP Mode" is set to Disabled.

IPV4 Address

Use this feature to enter an IP address for the wired LAN.

Subnet Mask Address

Use this feature to set the subnet mask for the wired LAN.

Default Gateway Address

Use this feature to set the gateway address for the wired LAN.

Preferred DNS Address

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

Alternate DNS Address

Use this feature to set the alternative Domain Name System (DNS) server address for the wired LAN.

Network Access State

Network Access State

Use this feature to change the state of the network state of ME. The options are Network Active, **Network Inactive**, and Full Unprovision.

Remote Setup And Configuration

►Remote Setup And Configuration Menu

Provisioning Server address

Use this feature to enter the provisioning server address. It's either a host name, IPv4, or IPv6.

Provisioning server port number

Use this feature to enter the provisioning server port number. The port numbers can range from 0 to 65535. The default is **9971**.

Remote Configuration **

Use this feature to enable or disable remote configuration. The options are Disabled and **Enabled**.

PKI DNS Suffix

Use this feature to enter the PKI DNS suffix.

Activate Remote Configuration

Use this feature to activate remote configuration.

Manage Certificates

►Manage Certificates Menu

►Go Daddy Class 2 CA

►Go Daddy Root CA-G2

►Comodo AAA CA

►Starfield Class 2 CA

►Starfield Root CA-G2

►VeriSign Class 3 Primary CA-G5

►Baltimore CyberTrust Root

►USERTrust RSA CA

►Verizon Global Root

►Entrust.net CA (2048)

►Entrust Root CA

►Entrust Root CA-G2

►VeriSign Universal Root CA

►Affirm Trust Premium

►DigiCert Global Root CA / G2 / G3

►DigiCert Trusted Root G4

►GlobalSign Root CA - R3

►GlobalSign ECC Root CA - R5

►GlobalSign Root CA - R6

Active

Use this feature to set the certificate to active. The options are NO and **YES**.

Default

This feature displays if this certificate is the default.

Hash type

This feature displays the hash type of the certificate.

Hash data

This feature displays the hash data of the certificate.

Power Control

►Power Control Menu

Note that the following configurations are effective only after ME provisioning has started.

ME ON in Host Sleep States

Use this feature to select the host sleep states. The options are Desktop: ON in S0 and **Desktop: ON in S0, ME Wake in S3, S4-5**.

Idle Timeout

Use this feature to enter the timeout value. The value can range from 1 to 65535. The default is **15**.

Appendix A:

BIOS Codes

For information about BIOS codes for the X14SRG-TF motherboard, refer to the following content.

BIOS Error POST (Beep) Codes

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

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

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

These fatal errors are usually communicated through a series of audible beeps that can be heard on an external buzzer connected to JD1. The table shown below lists some common errors and their corresponding beep codes encountered by users.

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

Additional BIOS POST Codes

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

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

Appendix B:

Software

After the X14SRG-TF 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.

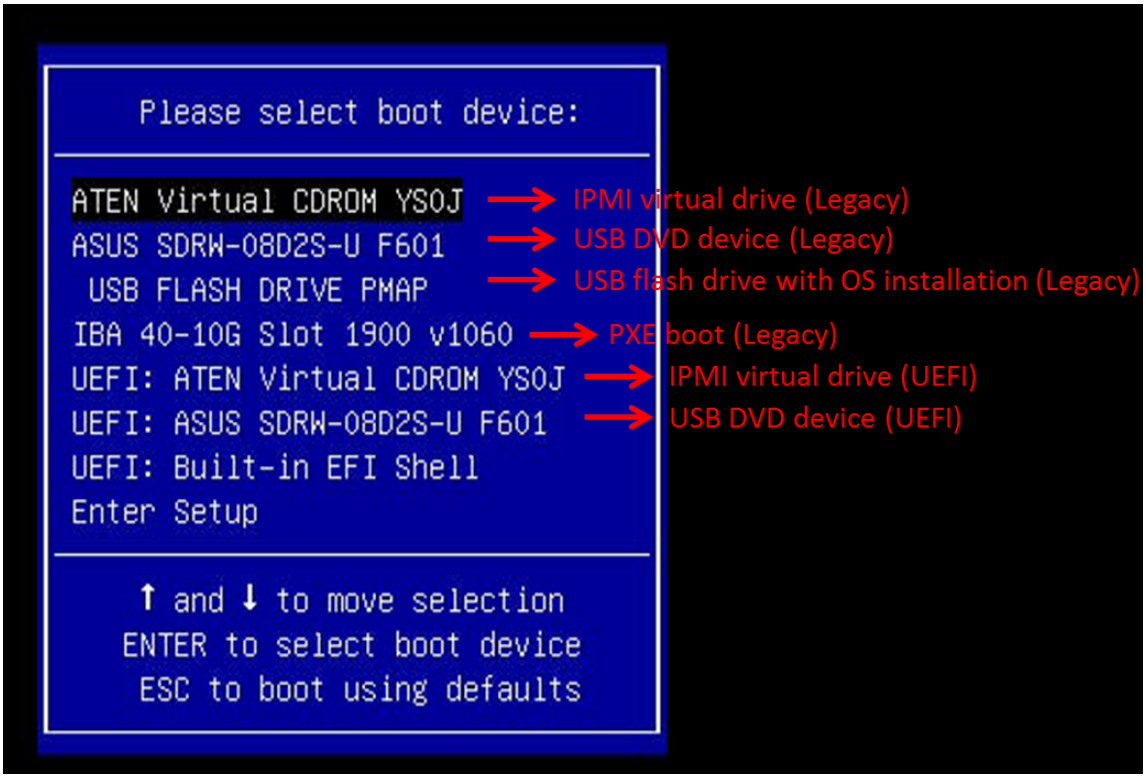


Figure B-1. Selecting the Boot Device

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.

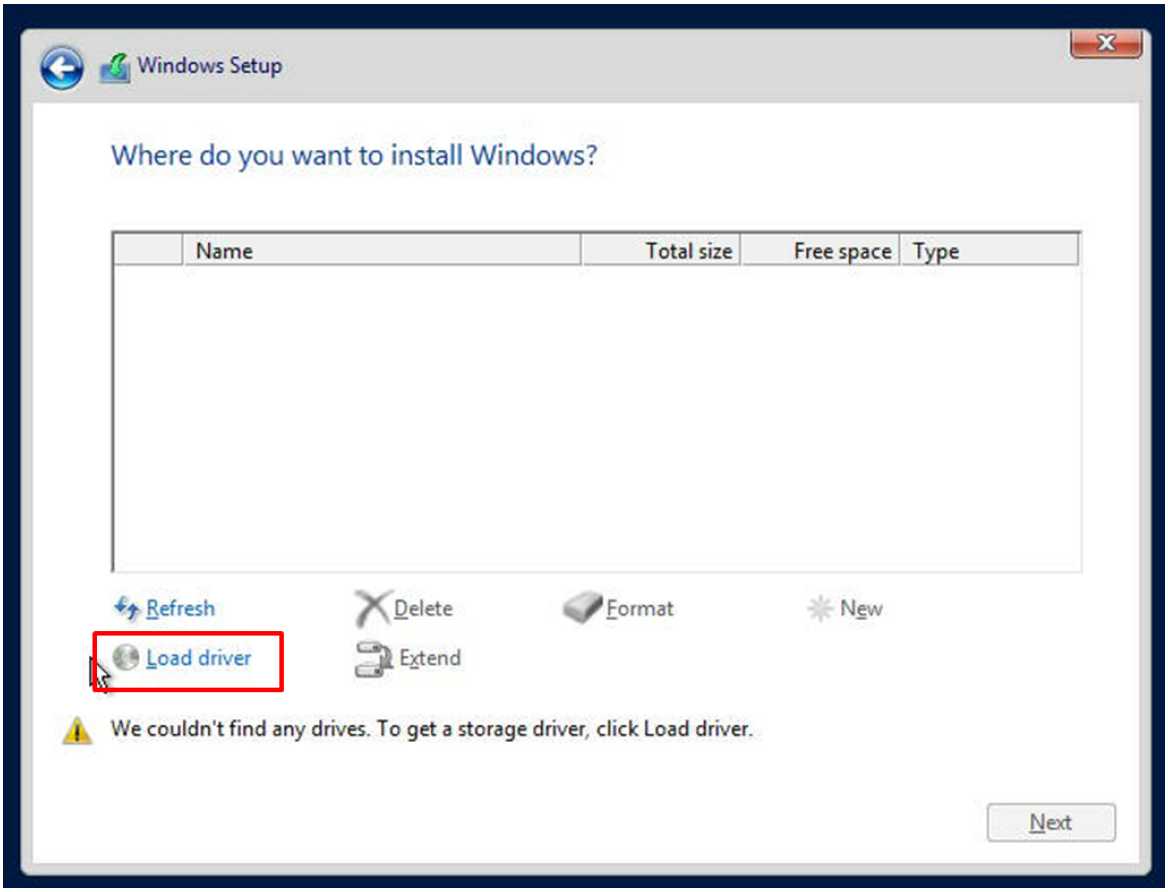


Figure B-2. Loading the Driver Link

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.

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.

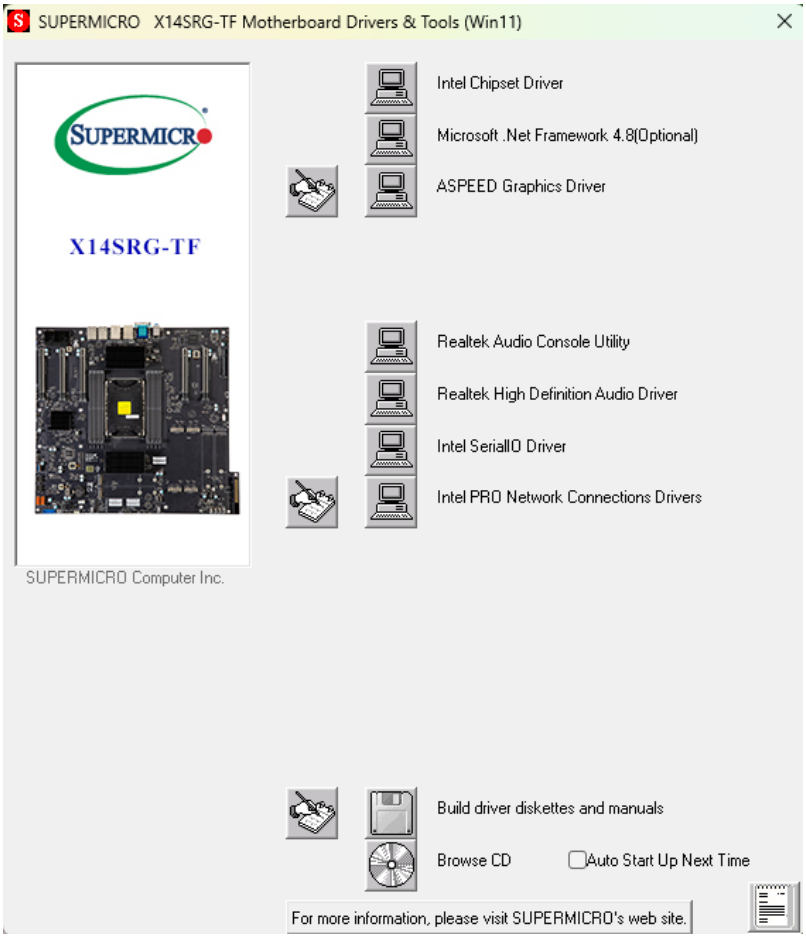


Figure B-3. Driver & Tools Installation Screen

Installing the Intel E610 LAN Driver on RHEL 9.5 and RHEL 10

This section describes how to install the Intel E610 LAN driver on RHEL 9.5 and RHEL 10, and to enroll Intel's Public Key for UEFI Secure Boot.

Note: If you are using RHEL 9.7, there is no need to manually install the E610 driver and enroll a Secure Boot key, as the driver is built in.

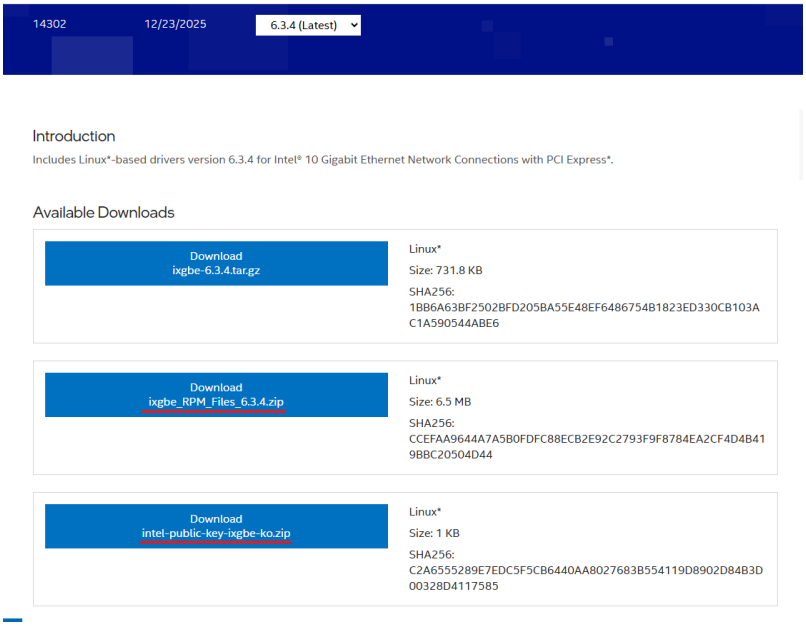
A. Downloading the Intel E610 LAN Driver

Download the driver package from the official Intel website at the following page:

https://www.intel.com/content/www/us/en/download/14302/869930/intel-network-adapter-driver-for-pcieintel-10-gigabit-ethernet-network-connections-under-linux.html

The download package includes:

- ixgbe_RPM_Files_<x.x.x>.zip: Contains the network adapter driver (precompiled kernel module) signed with Intel's private key.
- intel-public-key-ixgbe-ko.zip: Contains Intel's public key (intel-public-key-ixgbe-ko.rsa).



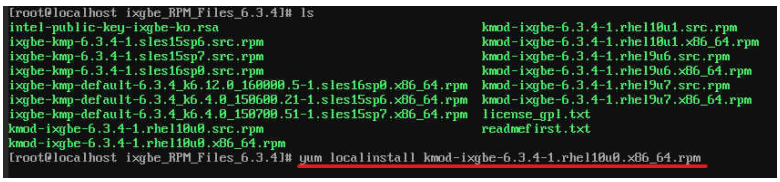
B. Installing the Intel E610 LAN Driver

1. Locate the RPM package corresponding to the OS version within the ixgbe_RPM_Files_<x.x.x>.zip file. For example, if the OS is Red Hat 10.0, the file name of the driver will be kmod-ixgbe-<x.x.x>-<x>.rhel10u0.x86_64.rpm

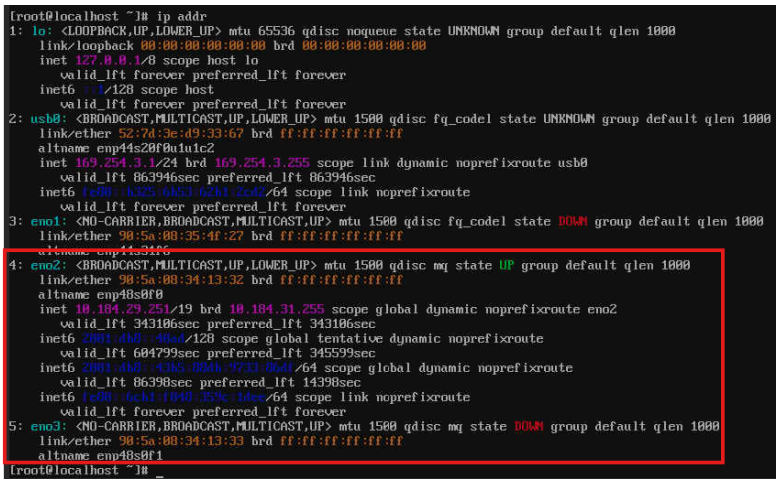
   Note: If the driver for the specific Red Hat Enterprise Linux version is not included in the current zip file, check previous versions of the driver release.

2. Install the driver using the following command:

   `yum localinstall kmod-ixgbe-<x.x.x>-<x>.rhel<xx>u<x>.x86_64.rpm`



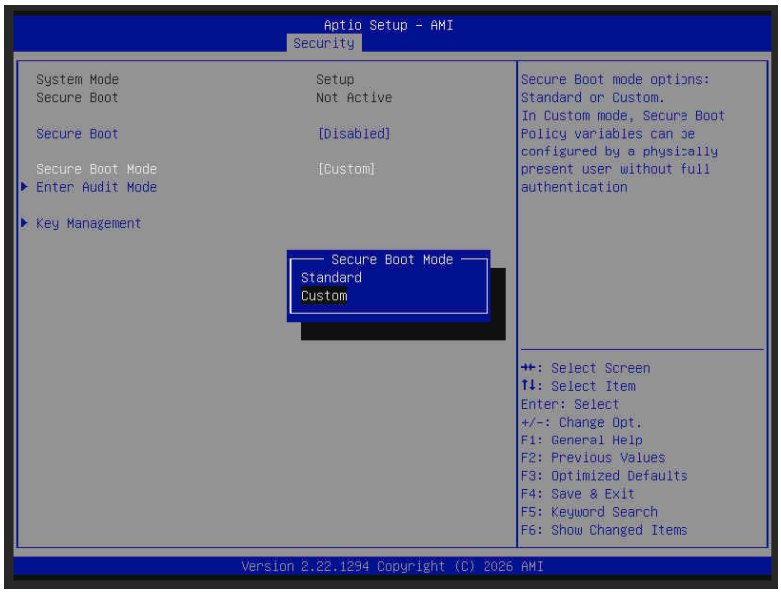
3. Once installed, verify that the E610 LAN driver is functioning correctly.



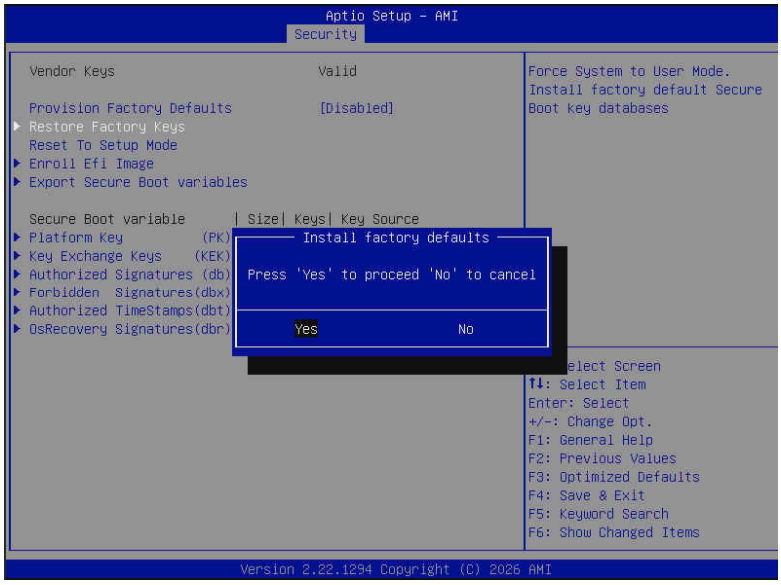
C. Enrolling Intel's Public Key for UEFI Secure Boot

To allow the E610 LAN driver to be loaded when Secure Boot is enabled, Intel's public key must be appended to the system's authorized signature database (db).

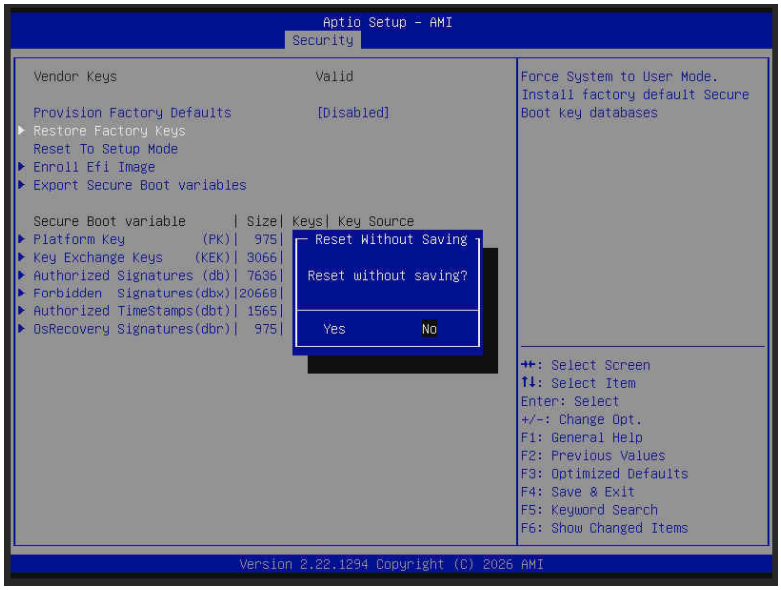
1. Copy Intel's public key (intel-public-key-ixgbe-ko.rsa) to a USB drive and insert it into the system. Boot into the BIOS Setup utility.
2. Navigate to Security -> Secure Boot and set Secure Boot Mode to Custom.



3. Select the Key Management feature.
4. To enable the Secure Boot, the Platform Key (PK) is necessary. If the Platform Key (PK) is not installed (status is "No Keys"), select Restore Factory Keys.

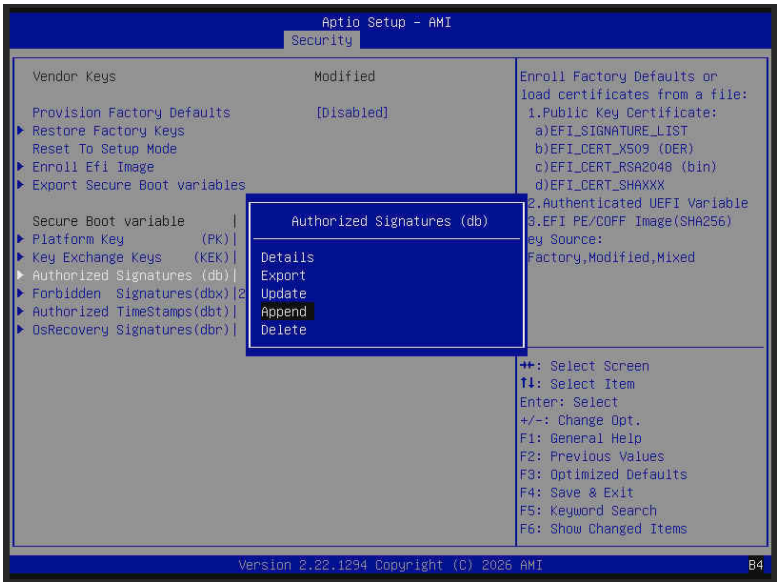


Select No to proceed without resetting the system immediately.

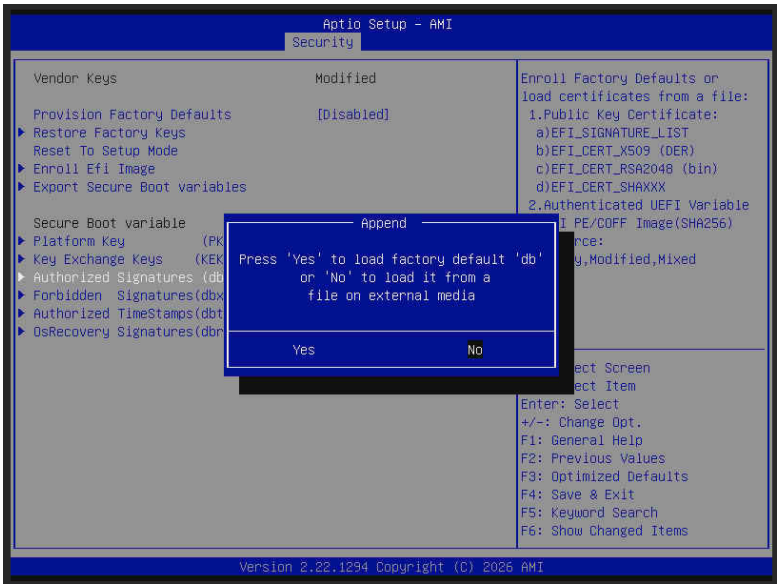


5. Select Authorized Signatures (db) and append Intel's public key from the USB drive.

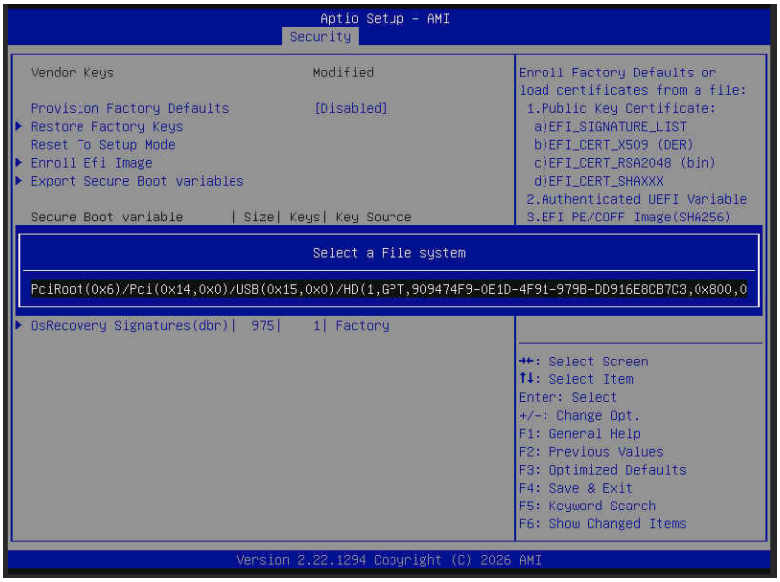
   (1) Select Authorized Signatures and choose Append.



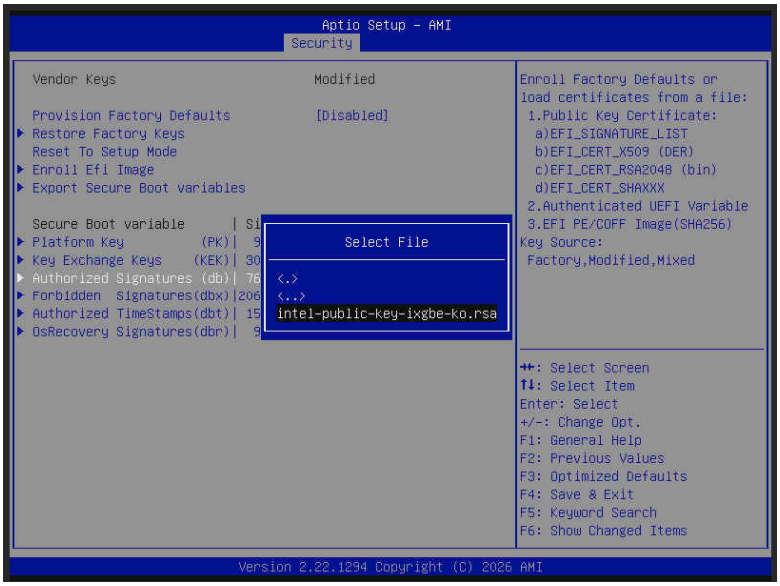
(2) Select No to append Intel's public key from the USB drive.



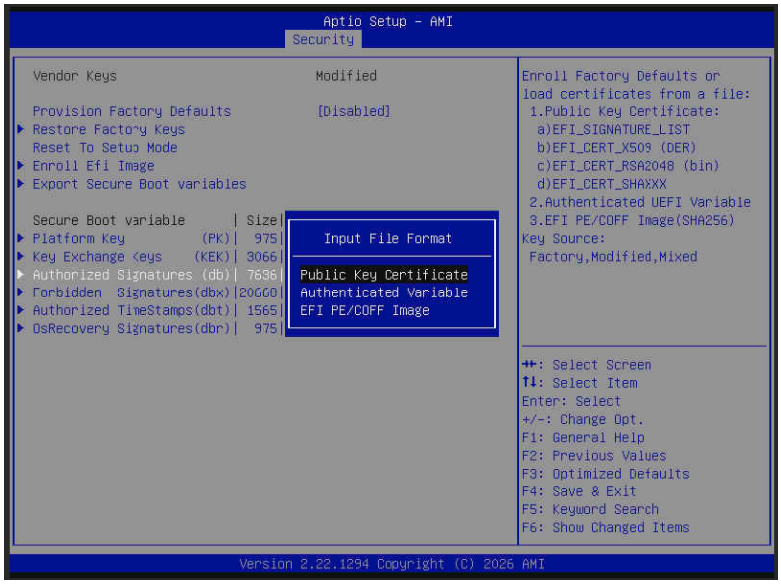
(3) Select the USB device and press Enter.



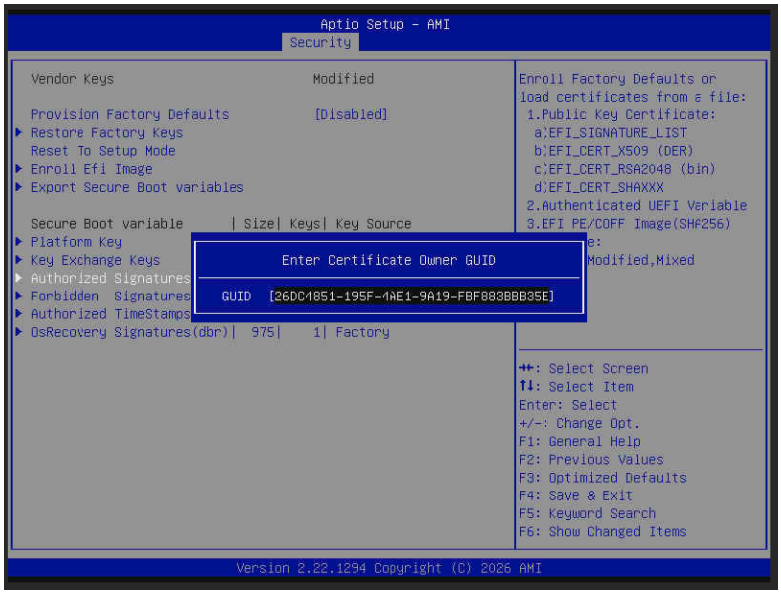
(4) Locate and select the intel-public-key-ixgbe-ko.rsa file on the USB drive.



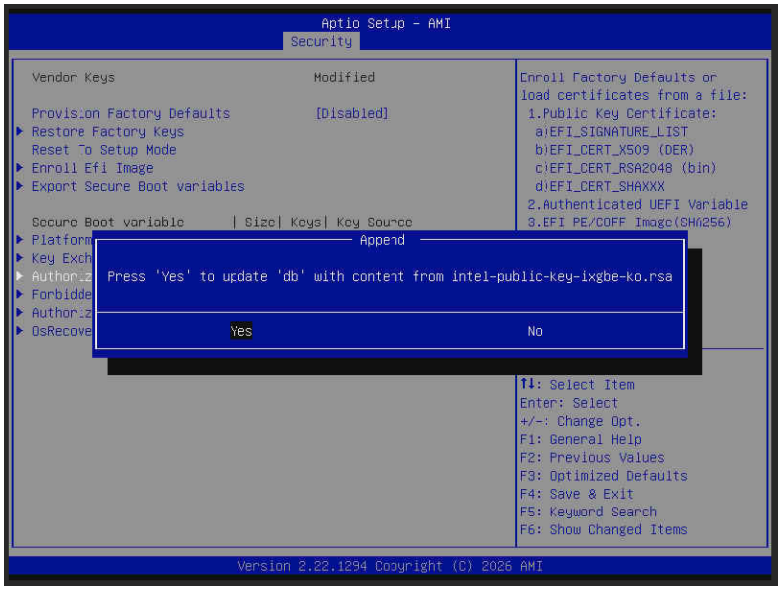
(5) Select Public Key Certificate.

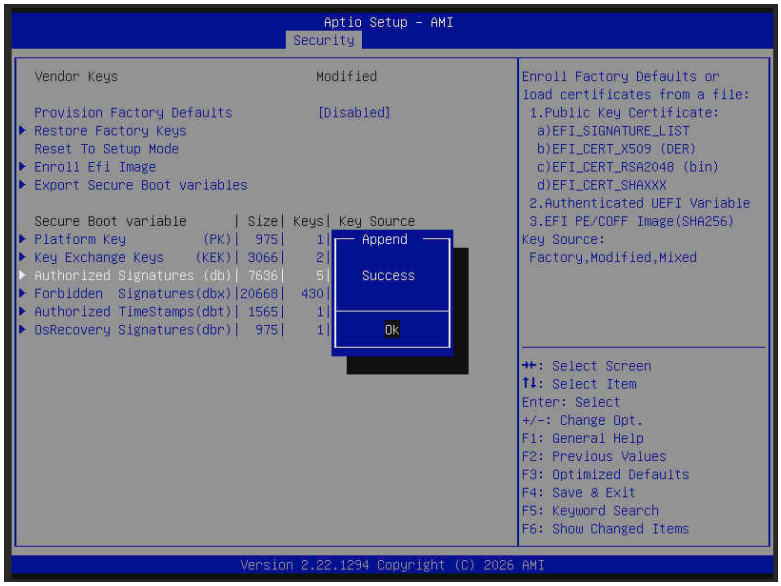


(6) Press Enter to confirm.

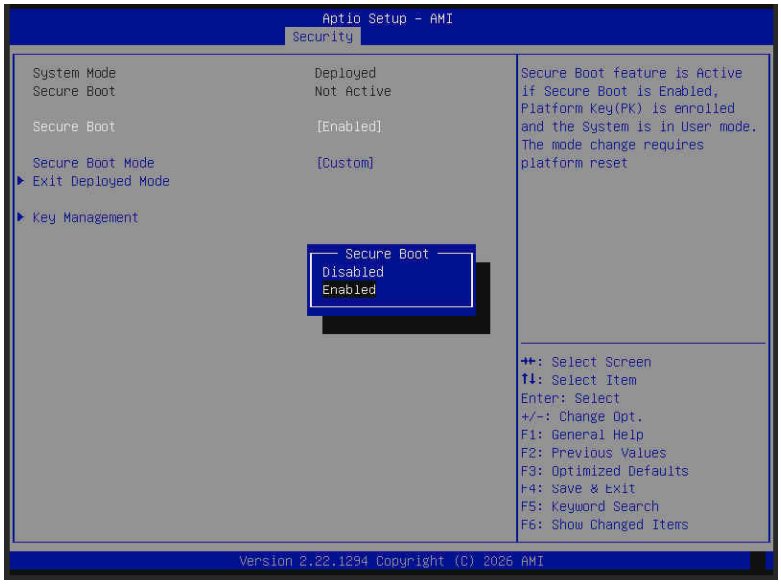


(7) Select Yes to update the db key database. A "Success" message should appear.

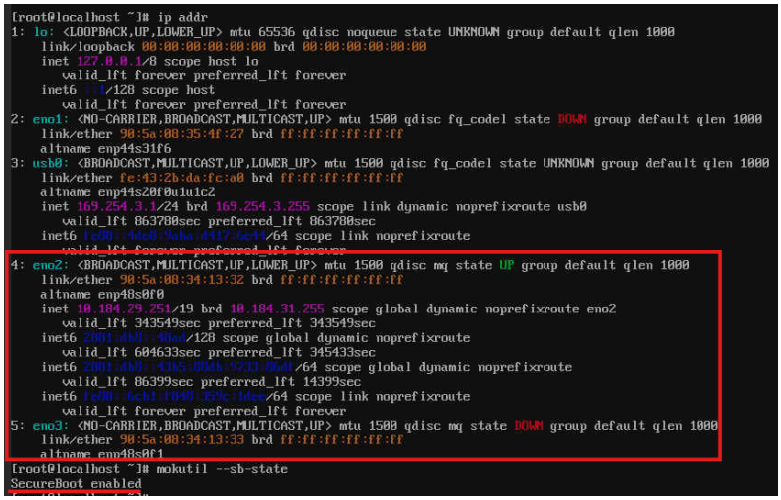




6. Press Esc to navigate to the previous page and set Secure Boot to Enabled. Then save and reset.



7. Boot to OS and confirm the E610 network adapter is still functioning correctly when Secure Boot is enabled.



BMC

The X14SRG-TF 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 B-4. BMC Password Label

Appendix C:

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 X14SRG-TF 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，有爆炸危險。請使用製造商建議之相同或功能相當的電池更換原有電池。請按照製造商的說明指示處理廢棄舊電池。

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.

Appendix D:

UEFI BIOS Recovery

The following content contains information on BIOS configuration with the X14SRG-TF motherboard.

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

Overview

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

Recovering the UEFI BIOS Image

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

Notes:

- Follow the BIOS recovery instructions for BIOS recovery when the main BIOS block crashes.
- If the recovery block processes fail, you will need to follow the procedures to make a Returned Merchandise Authorization (RMA) request. Refer to the instructions under "Returning Merchandise for Service" on page 106.

Recovering the Main BIOS Block with a USB Device

This feature allows the user to recover the main BIOS image using a USB device without additional utilities used. A USB flash or media drive can be used for this purpose. However, a USB hard disk drive cannot be used for BIOS recovery at this time.

Note: The USB flash drive doesn't have to be bootable; however, it has to be formatted to FAT16/FAT32 file system.

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

Use a different machine to download the BIOS package for your motherboard or your system from the product page available on our website at www.supermicro.com.

1. Extract the BIOS package to a USB device. Copy the BIOS ROM file [BIOSname#.###] that is included in the BIOS package into the Root "\" directory of the USB device.
2. Rename the BIOS ROM file [BIOSname#.###] in the root directory to SUPER.ROM for BIOS recovery use.

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

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

Figure D-1. Startup Screen

4. After locating the SUPER.ROM file, the system will enter the BIOS Recovery menu. Select the item "Proceed with flash update" and press the <Enter> key.

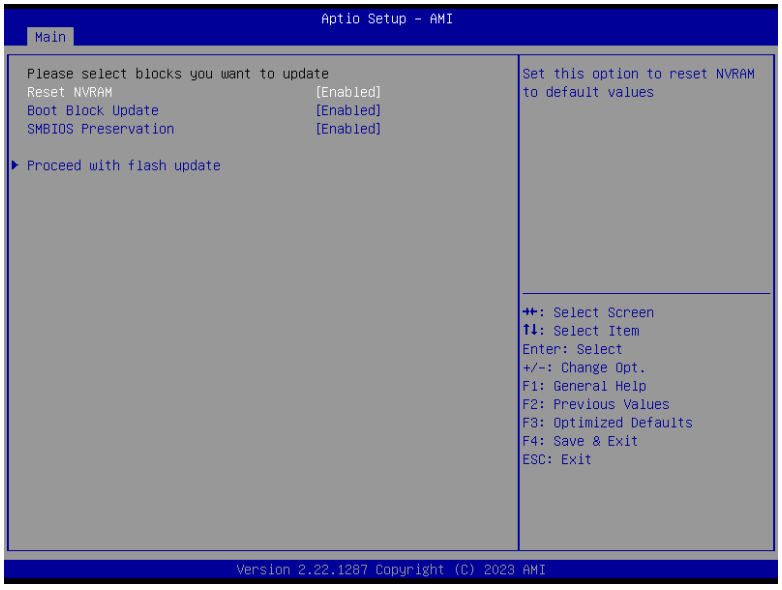


Figure D-2. BIOS Recovery Menu

5. You will see the BIOS recovery progress as shown in the screen below. Wait for the BIOS flashing process to complete.

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

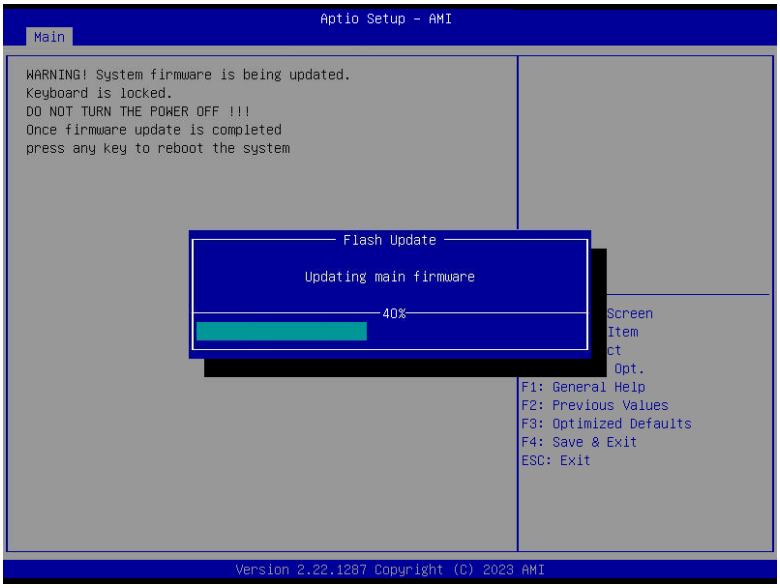


Figure D-3. BIOS Recovery In Progress Screen

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

Note: After BIOS recovery, it is recommended that you update your BIOS. Please refer to the "Updating BIOS" on page 111 section for more information.