



X14DBT-FAP/-FLAP

USER'S MANUAL

Revision 1.1a MNL-2723

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 1.1a

Release Date: June 12, 2025

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

Copyright © 2025 by Super Micro Computer, Inc.
All rights reserved.

Published in the United States of America

Preface

About This Manual

This manual is written for professional system integrators and PC technicians. It provides information for the installation and use of the X14DBT-FAP/-FLAP 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 server.

- 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 10
- 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.

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

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

Contents

Contacting Supermicro	10
Chapter 1: Introduction	11
1.1 Quick Reference	12
Motherboard Layout	12
Quick Reference	15
Memory Slots	17
Motherboard Features	18
Block Diagram	22
1.2 Platform Overview	23
Flexible and Scalable Processor Architectural Design	23
New Software Capability and Performance Optimization	23
1.3 Special Features	24
Recovery from AC Power Loss	24
1.4 System Health Monitoring	25
Onboard Voltage Monitors	25
Fan Status Monitor with Firmware Control	25
Environmental Temperature Control	25
1.5 ACPI Features	26
1.6 Serial Port	27
Chapter 2: Component Installation	28
2.1 Static-Sensitive Devices	30
Precautions	30
Unpacking	30
2.2 Motherboard Installation	31
Tools Needed	31
Installing the Motherboard	32
Mounting Holes	33
Locations of Mounting Holes	35
2.3 Processor and Processor Liquid Cooling Module Installation	36
LGA 7529 Socket BR1A Processors	37
Processor Top View	37

Overview of the Processor Socket	38
Overview of the Processor Carrier	38
Installing the Processor	40
2.4 Memory Support and Installation	44
General Guidelines for Optimizing Memory Performance	44
Memory Support	44
The Intel Xeon 6900-series processors with P-cores	44
DIMM Installation	46
DIMM Removal	48
Cold Plate	49
X14DBT-FAP Cold Plate	49
X14DBT-FLAP Cold Plate	49
2.5 Battery Removal and Installation	50
Battery Removal	50
Proper Battery Disposal	50
Battery Installation	50
2.6 Connections, Jumpers, and LEDs	51
Power Supply and Power Connections	51
Power Supply	51
4-Pin Backplane/GPU Power Connectors (JPMW1–JPMW3)	51
Headers and Connections	52
4-pin BMC External I ² C Header	52
COM Header	52
Fan Header	52
Liquid Cooling Leakage Sensor Headers	53
M.2 Boot Tray Connector	53
MCIO PCIe 5.0 x8 Connectors	53
Motherboard CPLD Header	53
NC-SI Connection	53
PCIe 5.0 x16 Expansion Slot	54
I/O Module Connector	54
TPM/Port 80 Header	54
VRM Header	55
VROC RAID Key Header	55

I/O Ports	55
Jumper Settings	56
CMOS Clear	56
Power Button	57
UID LED and System_Reset Button Select Jumper	57
LED Indicators	57
+3.3 V AUX Power LED	58
BMC Heartbeat LED	58
Control Panel LEDs	58
Onboard Power LED	60
Unit ID (UID) LED	60
Chapter 3: Troubleshooting	61
3.1 Troubleshooting Procedures	62
Before Power On	62
No Power	62
No Video	62
System Boot Failure	62
Memory Errors	63
Losing the System's Setup Configuration	63
If the System Becomes Unstable	63
3.2 Technical Support Procedures	65
3.3 Motherboard Battery	66
3.4 Where to Get Replacement Components	67
3.5 Returning Merchandise for Service	68
3.6 Feedback	69
Chapter 4: UEFI BIOS	70
4.1 Introduction	71
Updating BIOS	71
Starting the Setup Utility	71
4.2 Main Setup	73
4.3 Advanced Setup Configurations	75
Boot Feature Menu	75
CPU Configuration Menu	76
Advanced Power Management Configuration Menu	80

CPU P State Control Menu	81
Hardware PM State Control Menu	82
CPU C State Control Menu	83
Package C State Control Menu	84
CPU1/CPU2 Core Disable Bitmap Menu	84
Chipset Configuration Menu	85
Uncore Configuration Menu	85
Memory Configuration Menu	87
Memory Topology Menu	88
Memory Map Menu	88
Memory RAS Configuration Menu	88
Security Configuration Menu	90
IIO Configuration Menu	95
CPU1/CPU2 Configuration Menu	96
Intel VT for Directed I/O (VT-d) Menu	97
PCIe Leaky Bucket Configuration Menu	98
Trusted Computing Menu	98
ACPI Settings Menu	100
Super IO Configuration Menu	101
Serial Port 1 Configuration Menu	101
Serial Port 2 Configuration Menu	102
Serial Port Console Redirection Menu	102
Network Stack Configuration Menu	105
PCIe/PCI/PnP Configuration Menu	106
HTTP Boot Configuration Menu	108
Supermicro KMS Server Configuration Menu	109
Super-Guardians Configuration Menu	111
System Diagnostics Configuration Menu	113
TLS Authenticate Configuration Menu	113
4.4 Event Logs	114
4.5 BMC	116
System Event Log Menu	116
BMC Network Configuration Menu	117
4.6 Security	120

Supramicro Security Erase Configuration Menu	121
Secure Boot Menu	122
TCG Storage Security Configuration Menu	125
HDD Security Configuration Menu	126
4.7 Boot	127
4.8 Save & Exit	129
Appendix A: Software	131
Microsoft Windows OS Installation	131
Installing the OS	131
A.1 Driver Installation	134
BMC	136
BMC ADMIN User Password	136
Battery Handling	136
Product Disposal	138

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	12
Motherboard Layout	12
Quick Reference	15
Memory Slots	17
Motherboard Features	18
Block Diagram	22
1.2 Platform Overview	23
Flexible and Scalable Processor Architectural Design	23
New Software Capability and Performance Optimization	23
1.3 Special Features	24
Recovery from AC Power Loss	24
1.4 System Health Monitoring	25
Onboard Voltage Monitors	25
Fan Status Monitor with Firmware Control	25
Environmental Temperature Control	25
1.5 ACPI Features	26
1.6 Serial Port	27

1.1 Quick Reference

For details on the X14DBT-FAP/-FLAP motherboard layout, features, and other quick reference information, refer to the content below.

Motherboard Layout

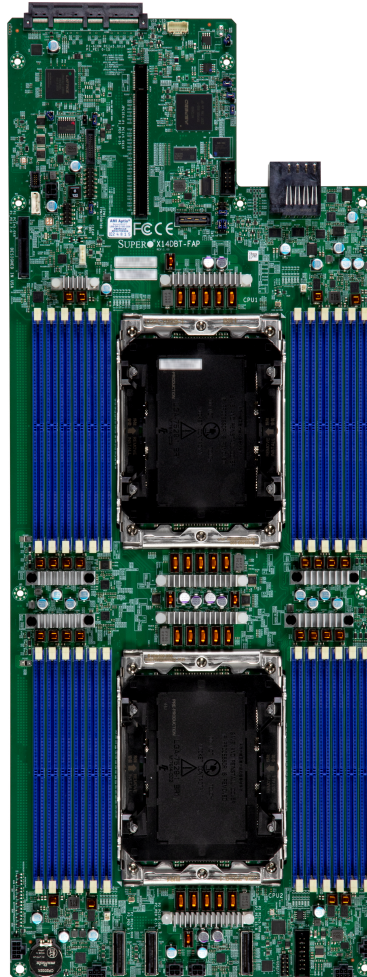


Figure 1-1. X14DBT-FAP Motherboard Image

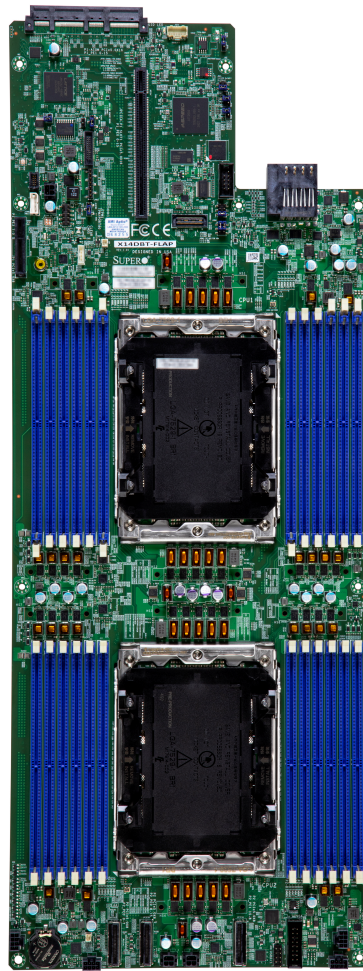


Figure 1-2. X14DBT-FLAP Motherboard Image

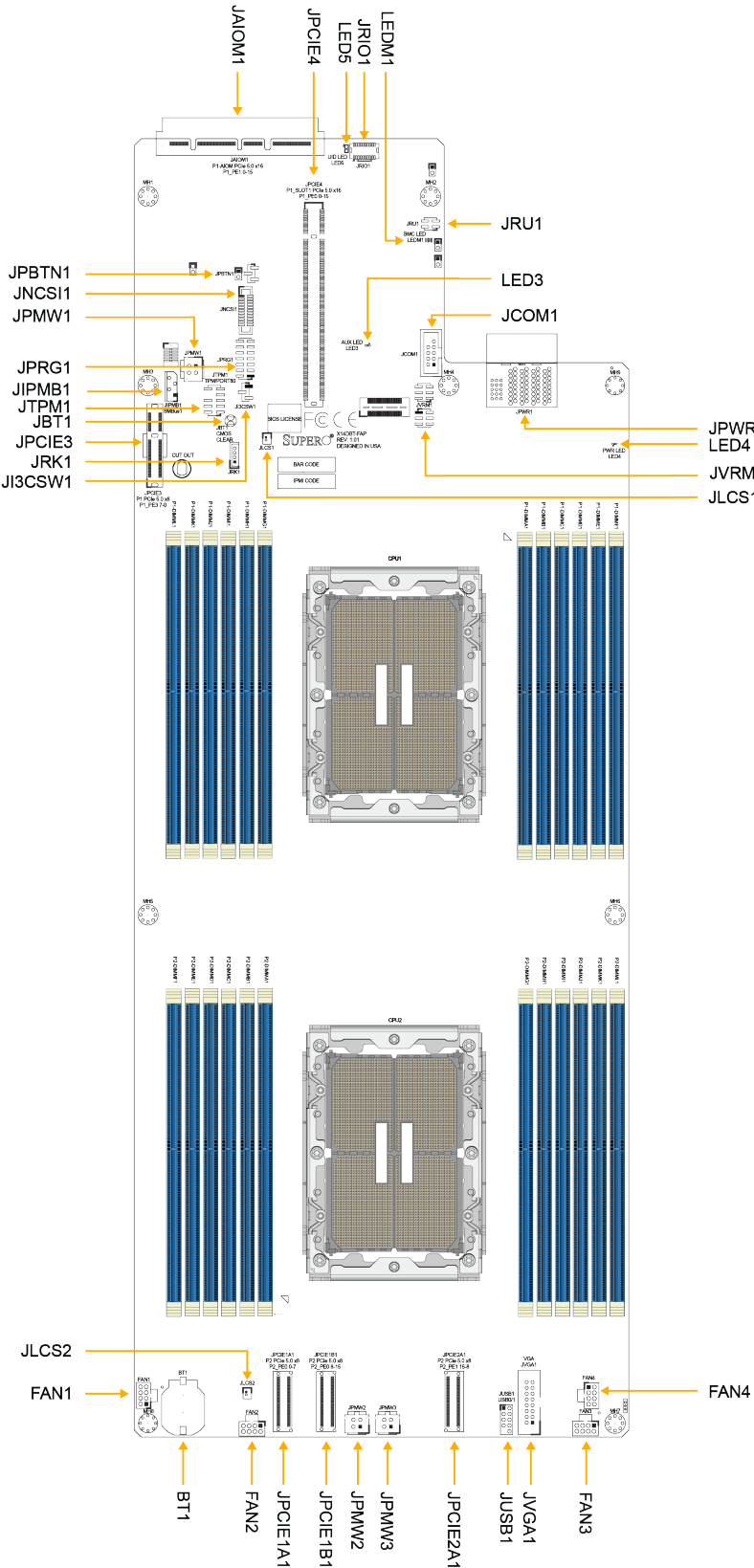


Figure 1-3. X14DBT-FAP/-FLAP Motherboard Layout

Notes:

- For detailed information on jumpers, connectors, and LED indicators, see "[Component Installation](#)" on page 28.
- "■" indicates the location of pin 1.
- 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

Jumper	Description	Jumper Settings
JBT1	CMOS Clear	Open (normal)

LED	Description	Status
LEDM1 (BMC LED)	BMC Heartbeat LED	Blinking Green: BMC Normal (Active), Solid Green: (During BMC Reset or during a Cold Reboot)
LED3 (AUX LED)	AUX LED	LED On: +3.3 V AUX Power On
LED4 (LEDPWR)	Onboard Power LED	LED On: Onboard Power On
LED5	Unit Identifier (UID) LED	Solid Blue: Unit Identification LED

Connector	Description
BT1	Onboard Battery
FAN1–FAN4	Four 8-pin Cooling Fan Header
JAIOM1 (P1_PE1 0-15)	Advanced Input/Output Module (AIOM) PCIe 5.0 x16 Connector for I/O Support
JCOM1	Serial (COM) Header
JIPMB1	4-pin BMC External I ² C Header
JLCS1/JLCS2	Coolant Leakage Sensors
JPBTN1	Power Button

Connector	Description
JPCIE1A1 (P2_PE0 0-7)	MCIO (P2) PCIe 5.0 x8 Connector
JPCIE1B1 (P2_PE0 8-15)	MCIO (P2) PCIe 5.0 x8 Connector
JPCIE2A1 (P2_PE1 15-8)	MCIO (P2) PCIe 5.0 x8 Connector
JPCIE3 (P1_PE3 7-0)	PCIe 5.0 x8 Connector for M.2 Riser Card
JPCIE4 (P1_PE0 0-15)	PCIe 5.0 x16 Connector for AOC
JPMW1–JPMW3	Three 4-pin +12 V Power Connectors
JPRG1	Programming Header for Motherboard Complex Programmable Logic Devices (CPLD)
JPWR1	Power Connector
JNSCI1	Network Controller Sideband Interface (NC-SI) connector
JRIO1	I/O Module Connector
JRK1	Intel VROC RAID Key Header
JRU1	UID LED and System_Reset Button Select Jumper
JTPM1	Trusted Platform Module/Port 80 connector
JUSB1 (USB0/1 (2.0))	USB Header
JVGA1	VGA port
JVRM1	VRM Header

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>.

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

Memory Slots

This motherboard supports up to 6144 GB of DDR5 memory with speeds of up to 6400 MT/s (1DPC) in 24 DIMM slots.

DIMM Slots Supported by CPU1	DIMM Slots Supported by CPU2
P1-DIMMA1	P2-DIMMA1
P1-DIMMB1	P2-DIMMB1
P1-DIMMC1	P2-DIMMC1
P1-DIMMD1	P2-DIMMD1
P1-DIMME1	P2-DIMME1
P1-DIMMF1	P2-DIMMF1
P1-DIMMG1	P2-DIMMG1
P1-DIMMH1	P2-DIMMH1
P1-DIMMI1	P2-DIMMI1
P1-DIMMJ1	P2-DIMMJ1
P1-DIMMK1	P2-DIMMK1
P1-DIMML1	P2-DIMML1

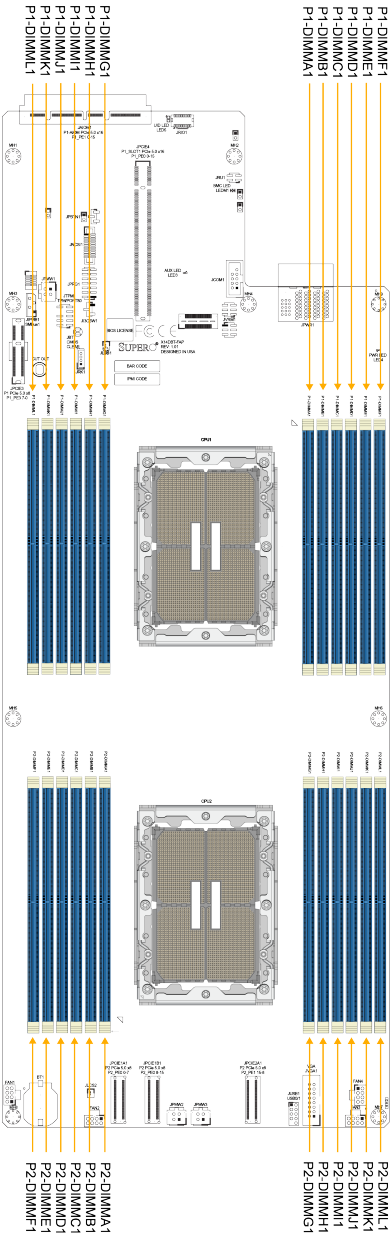


Figure 1-4. X14DBT-FAP/-FLAP DIMM Slots

Motherboard Features

Processors
<ul style="list-style-type: none"> Supports dual Intel® Xeon® 6900-series processors with P-cores (in LGA 7529 Socket BR1A) with six UPIs (24 GT/s max.) and a thermal design power (TDP) up to 500 W

Memory
<ul style="list-style-type: none"> • Supports ECC DDR5 memory with speeds of up to 6400 MT/s (1DPC) in 12 DIMM slots per processor. (Memory speed/capacity support depends on the processors used in the system.) • With Intel Xeon 6900-series processors with P-cores, the X14DBT-FAPX14DBT-FLAP motherboard supports MRDIMM memory with speeds up to 8800 MT/s in 1DPC configurations.
DIMM Size
<ul style="list-style-type: none"> • 16 GB, 32 GB, 64 GB, 128 GB, and 256 GB <p>Note: For the latest processor/memory updates, refer to our website at https://www.supermicro.com/en/products/motherboards.</p>
Expansion Slots
<ul style="list-style-type: none"> • One PCIe connector for PCIe 5.0 x16 AOC • Two MCIO connectors for PCIe 5.0 x16 AOC • One MCIO connector for two ports of NVME E1.S storage • One GenZ 4C+ for one Advanced IO Module (AIOM) • One Gen5 connector for a M.2 riser card
Baseboard Management Controller (BMC)/Network
<ul style="list-style-type: none"> • ASPEED AST2600 BMC • One dedicated BMC LAN/VGA
Graphics
<ul style="list-style-type: none"> • Graphics controller and VGA support via ASPEED AST2600 BMC
I/O Devices
<ul style="list-style-type: none"> • One VGA connector
Peripheral Devices
<ul style="list-style-type: none"> • Two USB 2.0 ports
BIOS
<ul style="list-style-type: none"> • AMI SPI BIOS • NAND Flash 64 MB support • SPI dual/quad speed control, Real Time Clock (RTC) wakeup, riser card auto detection support, SuperServer Automation Assistant (SAA), Redundant power supply unit detection, SPM, SUM-OOB/InBand

Power Connections
<ul style="list-style-type: none"> • One power supply connector (JPWR1) • Three 4-pin +12 V power connectors (JPMW1–JPMW3)
Power Management
<ul style="list-style-type: none"> • ACPI power management • S1, S5 support • Power button override mechanism • Power-on mode for AC power recovery • Wake-on-LAN • Power supply monitoring
System Health Monitoring
<ul style="list-style-type: none"> • Onboard voltage monitoring for +3.3 V, +3.3 V Standby, +5 V, +5 V Standby, +12 V, Vcore, Vmem • Onboard temperature monitoring for processor, GPU, VRM, LAN, system, peripheral, memory, NIC, M.2 SSD, AOM, and NVMe devices • Eight processor switch phase voltage regulator • Processor thermal trip support • Platform Environment Control Interface (PECI)
Fan Control
<ul style="list-style-type: none"> • Fan status monitoring via BMC connections • Three cooling zones • Low-noise fan speed control • 8-pin proprietary fans supported
Cooling
<ul style="list-style-type: none"> • Liquid cooling only <ul style="list-style-type: none"> • Refer to Cold Plate for more information
System Management
<ul style="list-style-type: none"> • Server platform service • RoHS support

Firmware Integrity / System Security
<ul style="list-style-type: none">• Trusted Platform Module (TPM) support (optional part needed)• Root of Trust (RoT) support to protect firmware security by detecting critical data corruption, and restoring platform integrity
LED Indicators
<ul style="list-style-type: none">• Processor/system overheat LED• Power/suspend state indicator LED• Fan-Failed LED• UID/remote UID• LAN activity LED• BMC/CPLD firmware LED
Dimensions
<ul style="list-style-type: none">• 27.0" x 8.7" (685.8 mm x 220.98 mm) (L X W) Proprietary

Note: The processor maximum Thermal Design Power (TDP) is subject to chassis and cooling module restrictions, and it also depends on server SKUs. For proper thermal management, please check the chassis and cooling module specifications.

Block Diagram

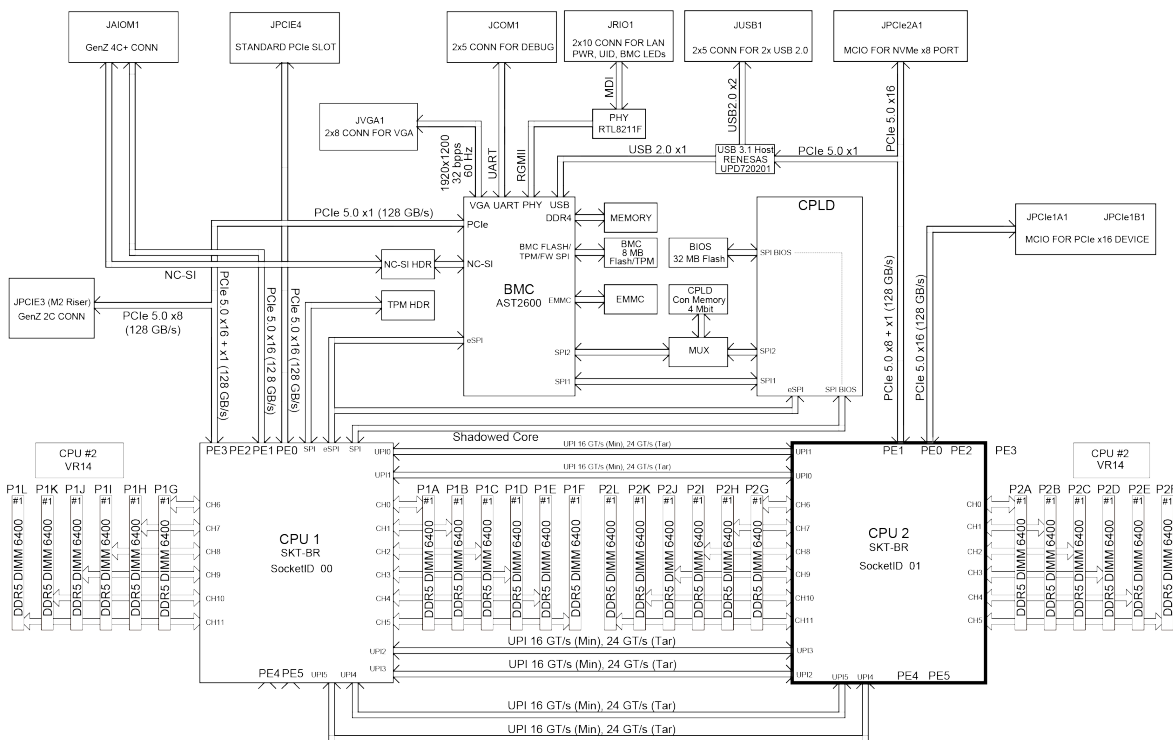


Figure 1-5. X14DBT-FAP/-FLAP Block Diagram

Note: This is a general block diagram and may not exactly represent the features on your motherboard. For the actual specifications of your motherboard, see the previous pages.

1.2 Platform Overview

Built upon the capability of the Intel Xeon 6 processors, the X14DBT-FAP/-FLAP motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users.

The X14DBT-FAP/-FLAP motherboard dramatically increases system performance for a multitude of server applications and supports the following features:

Flexible and Scalable Processor Architectural Design

The Intel Xeon 6 processors platform is built upon System-on-Chip (SoC) modular design, which offers computer systems with flexible, unrestrictive expansion options. The features include the following:

- Separate Compute and IO silicon chiplets
- Modular die fabric that enables flexible construction
- EmiB packaging with high bandwidth/low latency support
- Common IP, Firmware, OS, and platform ingredients
- A wide range of core counts and thermals supported
- Memory: up to 12 channels of DDR/MCR with 1 DIMM per channel support
- 96 lanes of PCIe 5.0, including 64 lanes of CXL 2.0, up to six UPI links support (x24 width) at speeds up to 24 GT/s
- Self boot

New Software Capability and Performance Optimization

- AMX supports FP16 (Floating Point 16-bit format) for AI/ML
- 2K memory encryption keys with 256b strength
- 64 KB, 16-way I-cache with improved branch predictor and miss recovery
- More outstanding memory requests and prefetch capabilities
- New Intel Xeon Architecture optimized for power efficiency throughput performance

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 70](#) for this setting. The default setting is **Last State**.

1.4 System Health Monitoring

Onboard Voltage Monitors

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

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

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

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

1.5 ACPI Features

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

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play, an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures while providing a processor architecture-independent implementation that is compatible with Windows Server 2022.

1.6 Serial Port

The X14DBT-FAP/-FLAP motherboard supports one serial port through a header on the I/O board. COM Port 1 is used for input / output. The UART provides legacy speeds with a baud rate of up to 115.2 Kbps.

Chapter 2:

Component Installation

This chapter provides instructions on installing and replacing main system components for the X14DBT-FAP/-FLAP 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	30
Precautions	30
Unpacking	30
2.2 Motherboard Installation	31
Tools Needed	31
Installing the Motherboard	32
Mounting Holes	33
2.3 Processor and Processor Liquid Cooling Module Installation	36
LGA 7529 Socket BR1A Processors	37
Overview of the Processor Socket	38
Overview of the Processor Carrier	38
Installing the Processor	40
2.4 Memory Support and Installation	44
General Guidelines for Optimizing Memory Performance	44
Memory Support	44
DIMM Installation	46
DIMM Removal	48
Cold Plate	49
X14DBT-FAP Cold Plate	49
X14DBT-FLAP Cold Plate	49
2.5 Battery Removal and Installation	50
Battery Removal	50
Proper Battery Disposal	50
Battery Installation	50

2.6 Connections, Jumpers, and LEDs	51
Power Supply and Power Connections	51
Headers and Connections	52
I/O Ports	55
Jumper Settings	56
LED Indicators	57

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.

Before installing the motherboard in the chassis, carefully read the instructions below.

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.

Tools Needed

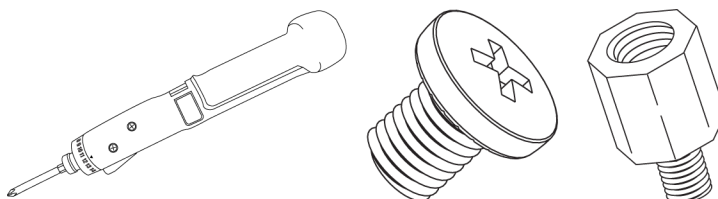


Figure 2-1. Driver (1) (Right), Phillips Screws (10) (Middle), Standoffs (10 or As Needed) (Left)

Installing the Motherboard

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

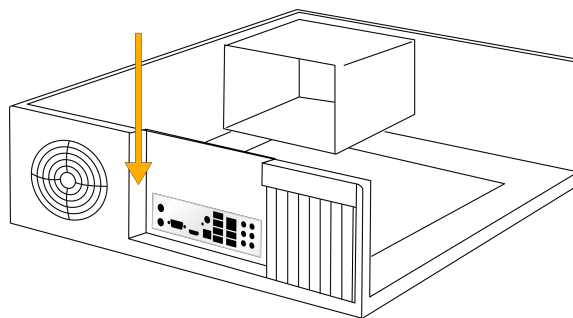


Figure 2-2. Installing the I/O Shield

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.

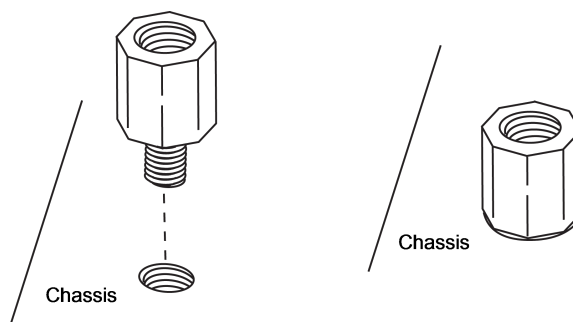


Figure 2-3. Locating the Mounting Holes

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

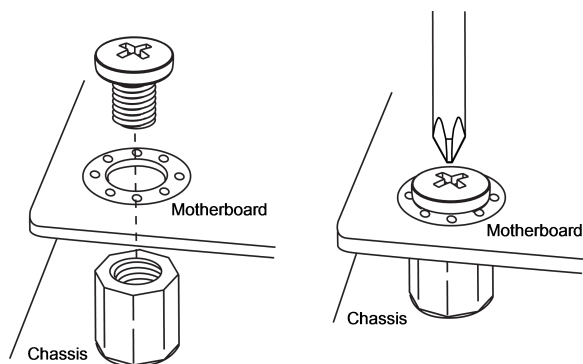


Figure 2-4. Aligning the Mounting Holes

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.

Mounting Holes

The following section provides information on the mounting holes on this motherboard.

- Motherboard mounting holes (9)

Nine mounting holes, located at MH1–MH9, are used to secure the motherboard onto the chassis.

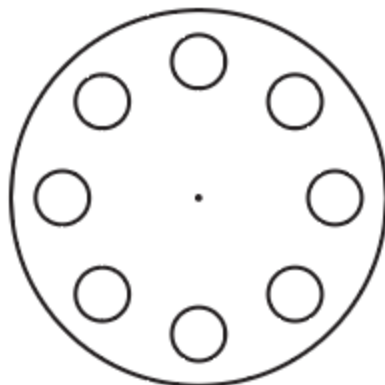


Figure 2-5. Motherboard Mounting Hole

- Cut out (1)

One cut out is used to fix the cool plate onto the X14DBT-FLAP motherboard.

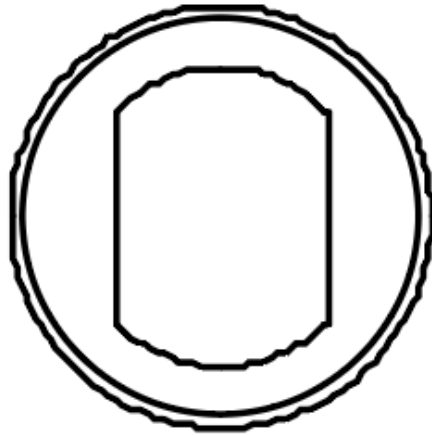


Figure 2-6. Cut Out

2.3 Processor and Processor Liquid Cooling Module Installation

This section provides procedures to install the processor(s) and processor liquid cooling module.

Notes:

- Take industry standard precautions to avoid ESD damage. For details, see "[Static-Sensitive Devices](#)" on page 30.
- 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 liquid cooling module 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 processor liquid cooling module.
- Refer to the Supermicro website for the most recent processor support.
- When installing the processor liquid cooling module, ensure a torque driver set to the correct force is used for each screw.
- Thermal grease is pre-applied on the processor liquid cooling module. No additional thermal grease is needed.

LGA 7529 Socket BR1A Processors

Processor Top View



Figure 2-8. Processor

Overview of the Processor Socket

The processor socket is protected by a plastic protective cover.

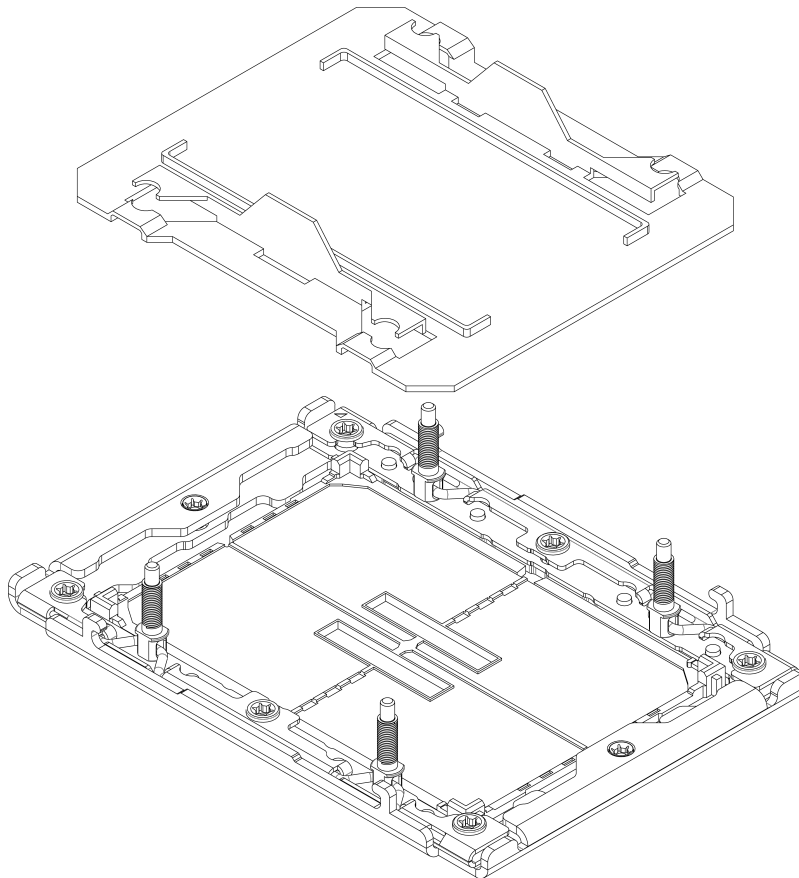


Figure 2-9. Plastic Protective Cover and Processor Socket

Overview of the Processor Carrier

This section displays the X14DBT-FAP/-FLAP motherboard processor carrier.

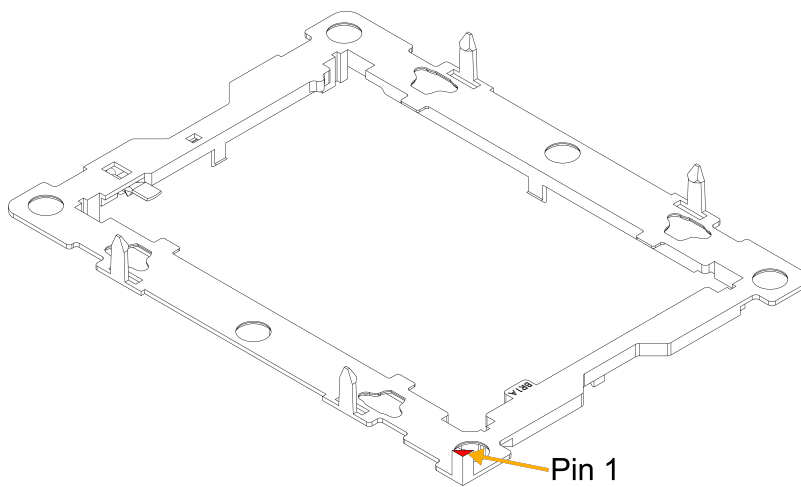


Figure 2-10. Carrier BR1A

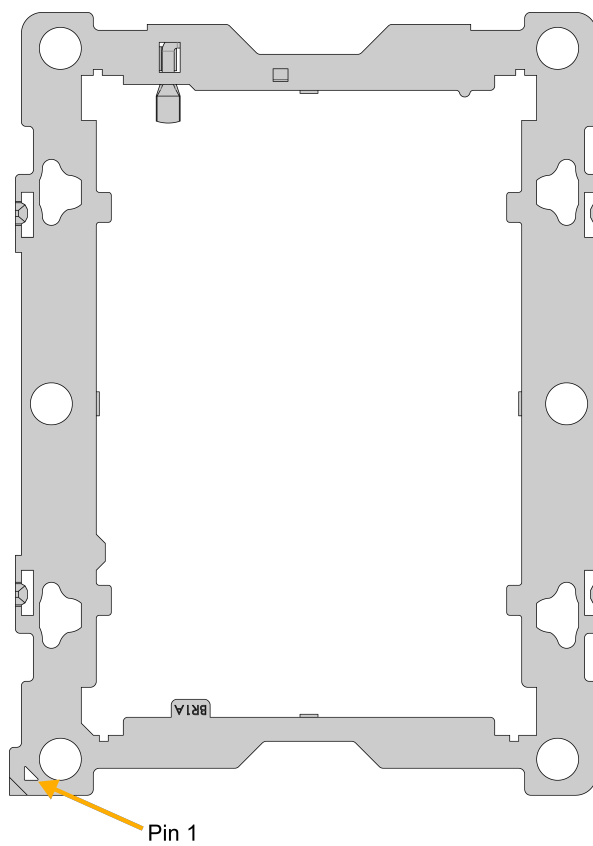


Figure 2-11. Carrier Top View

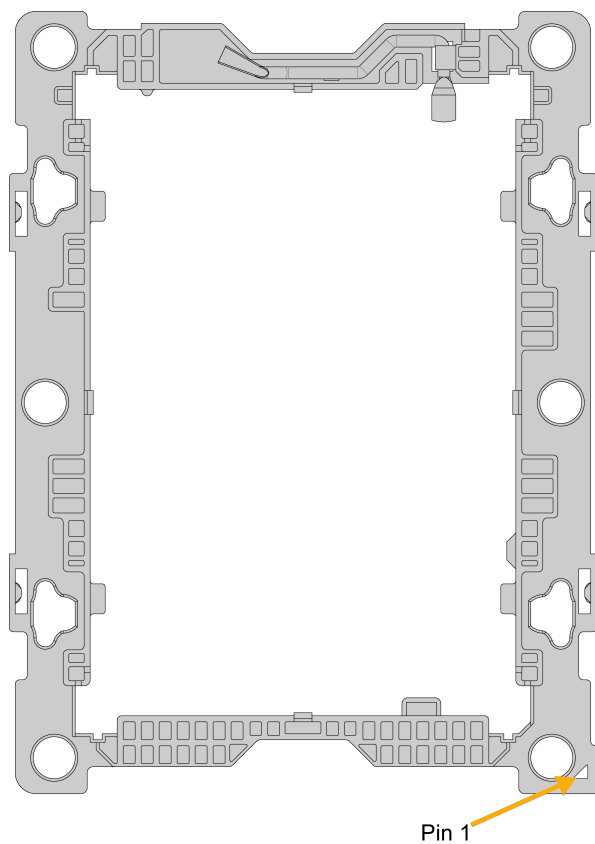


Figure 2-12. Carrier Bottom View

Installing the Processor

To install a processor into the processor carrier, follow the steps below:

1. Ensure the lever on the processor carrier is pressed down and held by a latch on the processor carrier as shown below.

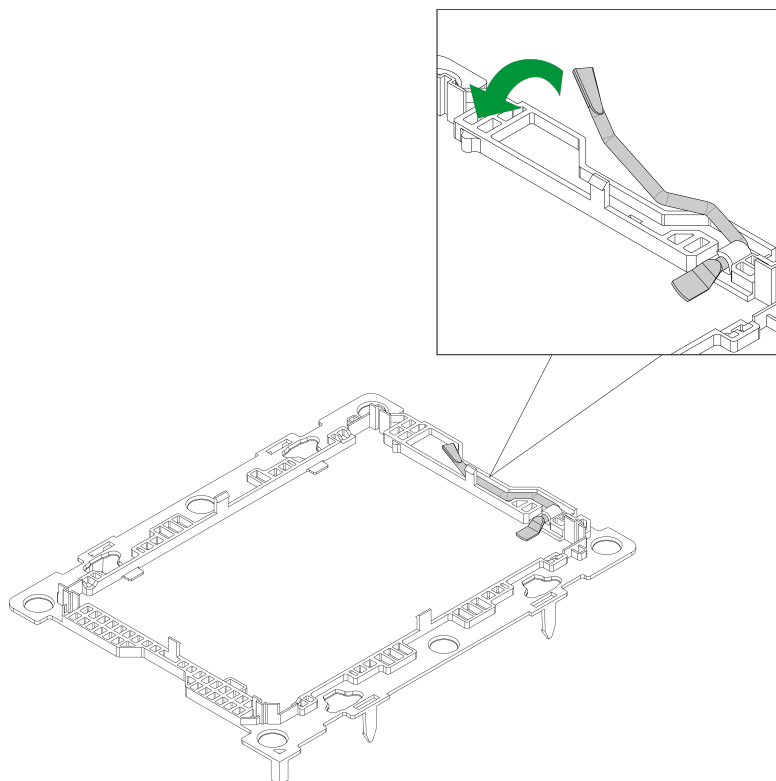


Figure 2-13. Carrier Lever

2. Hold the processor with the LGA lands (gold contacts) facing down. 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.

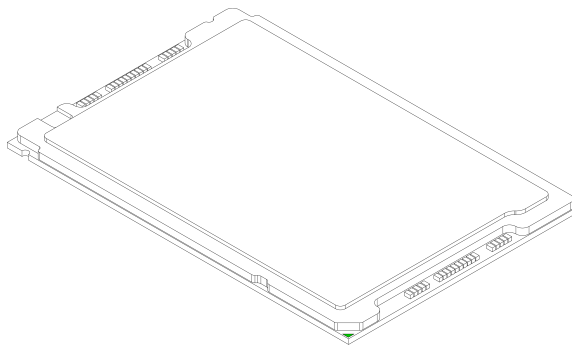


Figure 2-14. Processor

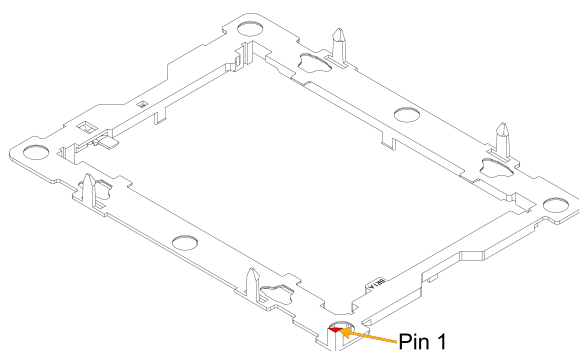


Figure 2-15. Carrier

3. While ensuring that the pin 1 triangles point towards the same direction, flip over the processor and processor carrier. Use the latches on the processor carrier to secure the processor onto the processor carrier. Processor keys on the processor and processor carrier will prevent securing the processor in an incorrect orientation.

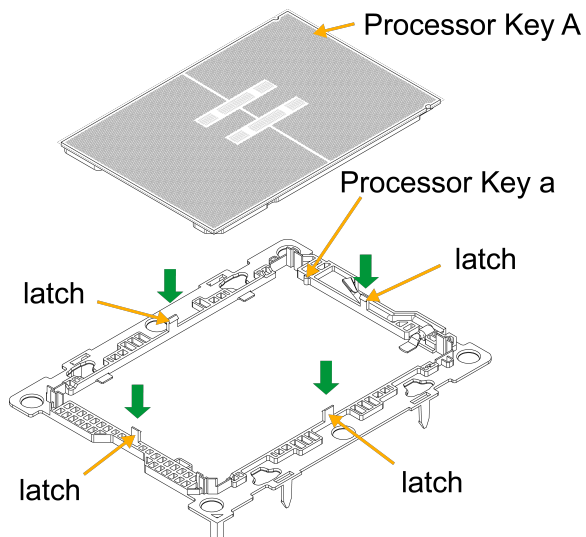


Figure 2-16. Key and Latch Locations

4. Examine all corners to verify that the processor is secured to the carrier. Two triangles indicating pin 1 on the processor and processor carrier should point towards the same direction.

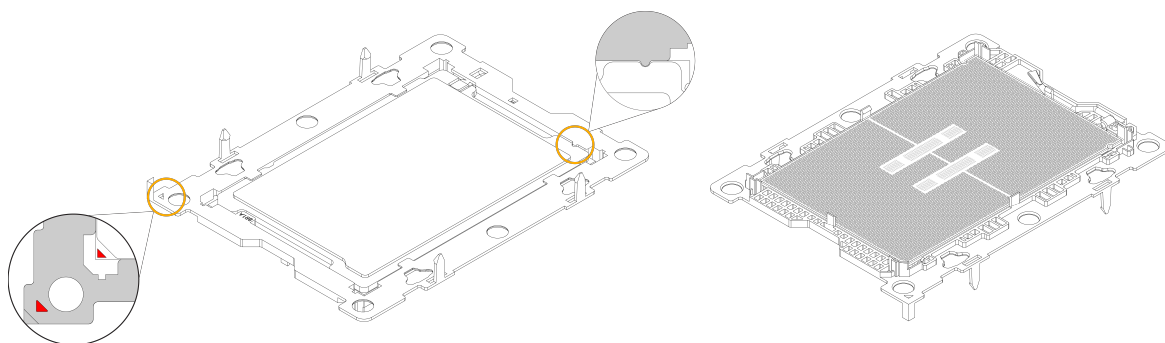


Figure 2-17. Processor and BR1A Keys and Latches

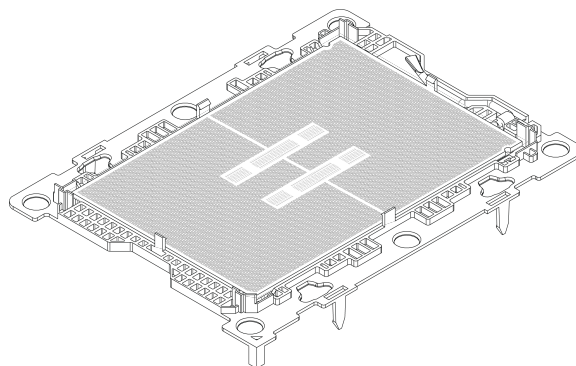


Figure 2-18. Completed Processor Carrier Installation

2.4 Memory Support and Installation

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

Note: Check the Supermicro website for recommended memory modules.

General Guidelines for Optimizing Memory Performance

- Use only 6400 MT/s rated DDR5 memory.
- DIMMs must be all DDR5 RDIMM, 3DS RDIMM, or MRDIMM.
- All DIMMs must operate at the same speed per processor socket.
- Density mixing is not allowed.
- Frequency mixing is not allowed.
- Rank mixing is not allowed.

Memory Support

The X14DBT-FAP/-FLAP motherboard supports ECC DDR5 memory with speeds rated 6400 MT/s (1DPC) and MRDIMM memory with speeds up to 8800 MT/s (1DPC) in 12 DIMM slots per processor.

To enhance memory performance and ensure system stability, do not mix memory modules of different speeds, different sizes, and different types in your server.

Note: Memory speed/capacity support depends on the processors used in the system.

The Intel Xeon 6900-series processors with P-cores

DDR5 Memory Support for Intel® Xeon® 6900-Series Processors with P-Cores					
Type	Ranks Per DIMM, Data Width (Stack)	DIMM Capacity (GB)			Speed (MT/s); Voltage (V); Slots per Channel (SPC) and DIMMs per Channel (DPC)
		DRAM Density			1DPC/1SPC
		16 Gb	24 Gb	32 Gb	+1.1 V

DDR5 Memory Support for Intel® Xeon® 6900-Series Processors with P-Cores					
RDIMM	1Rx4	32 GB	48 GB	-	6400, 6000, 5600, 5200, 4800 (DDR5-6400 rated RDIMMs only)
	2Rx8	32 GB	48 GB	-	
	2Rx4	64 GB	96 GB	128 GB	
3DS RDIMM	8Rx4	256 GB	-	-	
	4Rx4	-	-	256 GB	
MRDIMM	2Rx8	32 GB	48 GB	-	
	2Rx4	64 GB	96 GB	128 GB	
	4Rx8	64 GB	96 GB	-	
	4Rx4 (2U)	128 GB	-	-	
	4Rx4 (2U)	-	-	256 GB	

The Intel® Xeon® 6900-series processors with P-cores DDR5 Memory Population Table (2 Processors and 24 DIMMs Installed, 1DPC)	
2 Processor DIMM Counts (Recommended)	Memory Population Sequence (1DPC)
2 Processors and 2 DIMMs	P1-DIMMA1 P2-DIMMA1
2 Processors and 16 DIMMs	P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMI1/P1-DIMMJ1/P1-DIMMK1/P1-DIMML1 P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMI1/P2-DIMMJ1/P2-DIMMK1/P2-DIMML1
2 Processors and 16 DIMMs	P1-DIMMA1/P1-DIMMB1/P1-DIMMD1/P1-DIMME1/P1-DIMMG1/P1-DIMMH1/P1-DIMMJ1/P1-DIMMK1 P2-DIMMA1/P2-DIMMB1/P2-DIMMD1/P2-DIMME1/P2-DIMMG1/P2-DIMMH1/P2-DIMMJ1/P2-DIMMK1
2 Processors and 16 DIMMs	P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1/P1-DIMMI1/P1-DIMML1 P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1/P2-DIMMI1/P2-DIMML1

The Intel® Xeon® 6900-series processors with P-cores
DDR5 Memory Population Table
(2 Processors and 24 DIMMs Installed, 1DPC)

2 Processors and 24 DIMMs	P1-DIMMA1/P1-DIMMB1/P1-DIMMC1/P1-DIMMD1/P1-DIMME1/P1-DIMMF1/P1-DIMMG1/P1-DIMMH1/P1-DIMMI1/P1-DIMMJ1/P1-DIMMK1/P1-DIMML1 P2-DIMMA1/P2-DIMMB1/P2-DIMMC1/P2-DIMMD1/P2-DIMME1/P2-DIMMF1/P2-DIMMG1/P2-DIMMH1/P2-DIMMI1/P2-DIMMJ1/P2-DIMMK1/P2-DIMML1
--------------------------------------	--

Note: DIMM rank mixing is not allowed.

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 30](#).

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

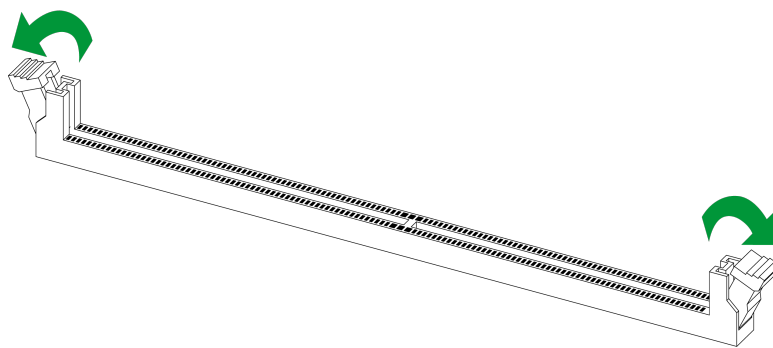


Figure 2-19. Unlocking the DIMM Slot

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

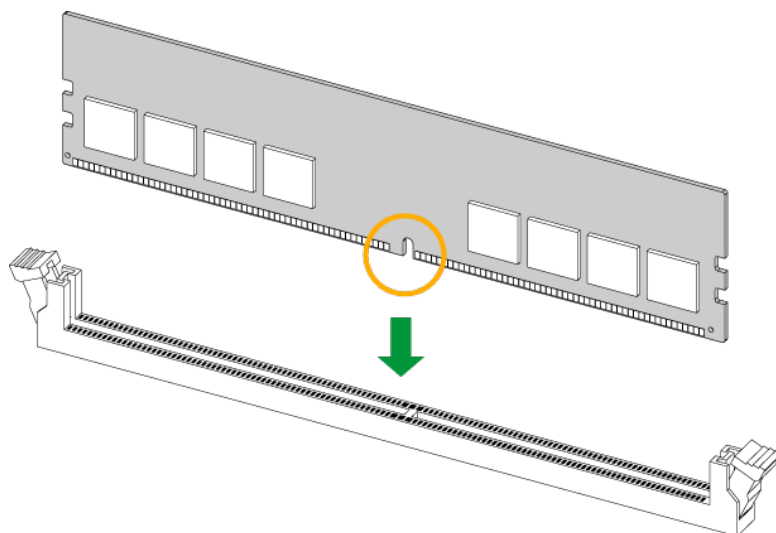


Figure 2-20. Aligning the DIMM Slot with the Receptive Point

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

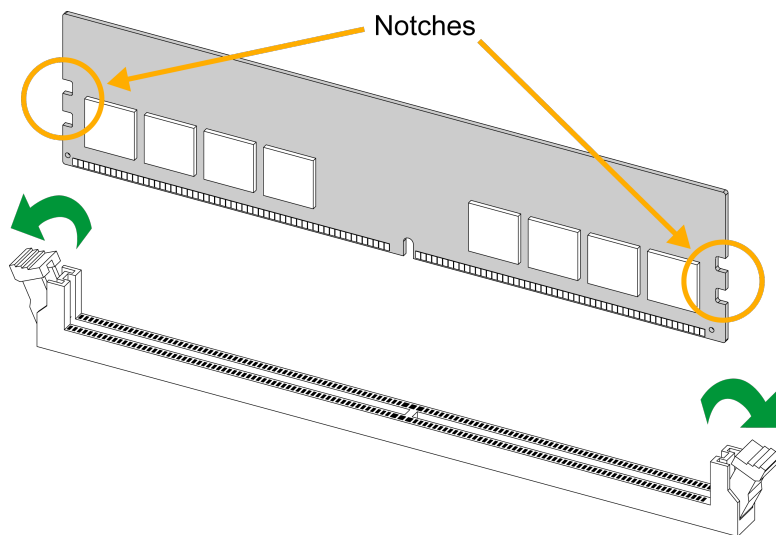


Figure 2-21. Aligning the Notches

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

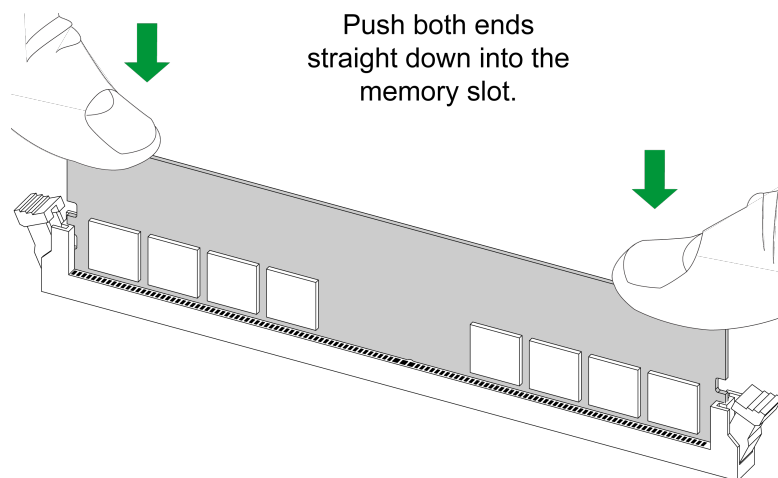


Figure 2-22. Securing the DIMM

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

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 30.

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

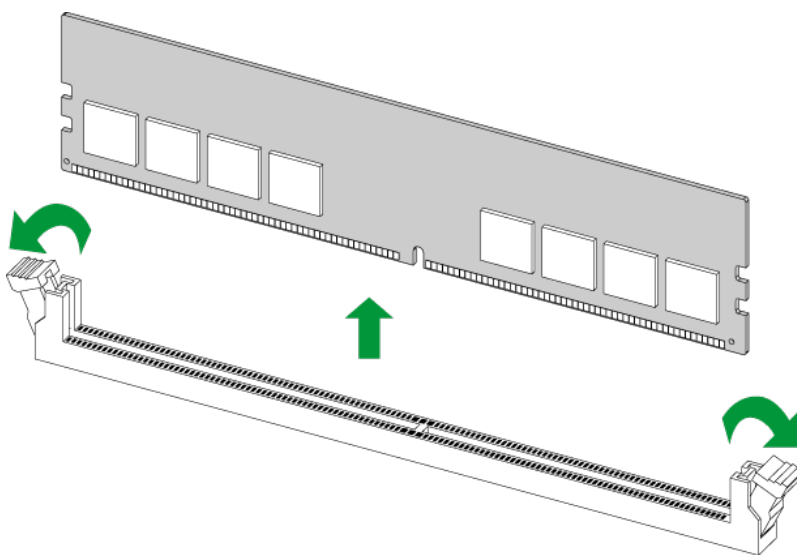


Figure 2-23. Unlocking the DIMM Slot

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

Cold Plate

FlexTwin architectures provide liquid cooling to disperse the heat from the components. The cold plate is placed over several components, such as the processors, DIMMs, and VRM chips, to transfer the heat from the components to the liquid coolant and maintain optimal temperature.

X14DBT-FAP Cold Plate

In X14DBT-FAP, the cold plate only covers the processor.

X14DBT-FLAP Cold Plate

In X14DBT-FLAP, the cold plate covers the processor, DIMMs, and the VRM chips. The cold plate covers every two DIMMs, and both sides will be liquid cooled on each DIMM.

A cylindrical pin near the DIMMs helps secure the cold plate.

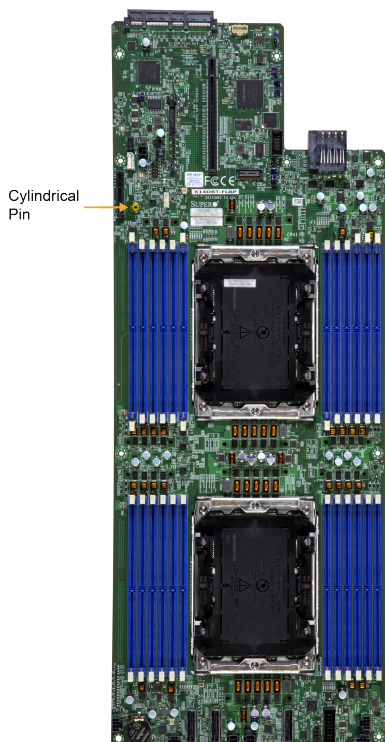


Figure 2-24. Cylindrical Pin on X14DBT-FLAP

2.5 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

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

Proper Battery Disposal

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.

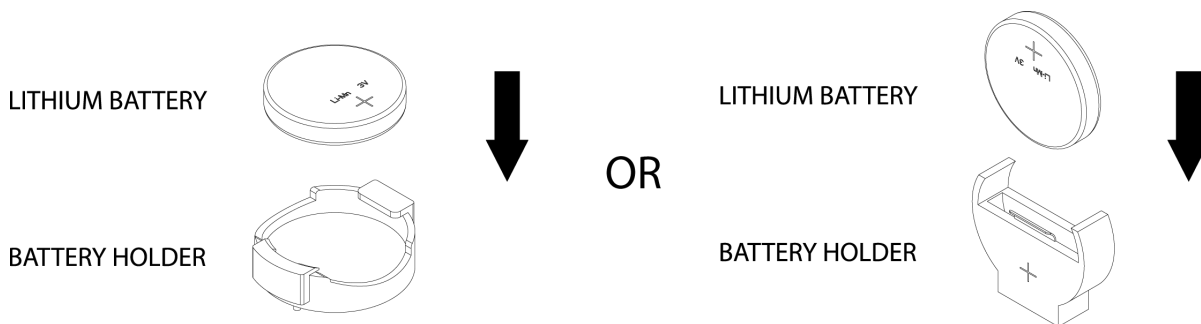


Figure 2-25. Installing a Battery

2.6 Connections, Jumpers, and LEDs

Refer to the following sections for information about connections, jumpers, and LEDs for the X14DBT-FAP/-FLAP motherboard.

Power Supply and Power Connections

For information about the power supply and power connections of the X14DBT-FAP/-FLAP motherboard, refer to the following content.

Power Supply

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

The X14DBT-FAP/-FLAP FlexTwin Server board accommodates one Supermicro proprietary power supply unit (JPWR1), and three 4-pin +12 V power connectors (JPMW1–JPMW3). Although most power supplies generally meet the specifications required by the processors, some are inadequate. All these power connections are also required to ensure adequate power supply to the system.

Important: To avoid damaging the power supply or the motherboard, be sure to use a power supply that accommodates two power supply units. Be sure to also connect the power supplies to the proprietary power supply unit (JPWR1), and three 4-pin +12 V power connectors (JPMW1–JPMW3) on the motherboard. Failure in doing so may void the manufacturer warranty on your power supply and motherboard.

It is strongly recommended that you use a high quality power supply that meets ATX power supply Specification 2.02 or above. It must also be SSI compliant.

4-Pin Backplane/GPU Power Connectors (JPMW1–JPMW3)

Three 4-pin +12 V power supply connectors (PMW1–JPMW3) are used to provide power to backplane and GPU devices via cables.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

4-pin Power Connectors for Backplane/GPU Devices	
Pin Definitions: Four Total	
Pin#	Definition
1–2	GND
3–4	P12 V (12 V Power)

Headers and Connections

For information about the headers on the X14DBT-FAP/-FLAP motherboard, refer to the following content.

4-pin BMC External I²C Header

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

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under [Quick Reference](#).

COM Header

There is one COM header at JCOM1 on the X14DBT-FAP/-FLAP motherboard. Use a cable with the COM header to access the COM1 COM port. COM ports provide serial communication support.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

COM Header			
Pin Definitions: Nine 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		

Fan Header

There are four 8-pin fan headers (FAN1–FAN4) on the motherboard. These fan headers are used for cooling fans for your system. Fan speed control for these fans is supported by thermal management via BMC 2.0 interface.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under ["Quick Reference" on page 12](#).

Liquid Cooling Leakage Sensor Headers

Liquid cooling leakage sensor headers are located at JLCS1 and JLCS2 on the X14DBT-FAP/-FLAP motherboard. This header is reserved for liquid cooling support in systems. Liquid cooling leakage sensor headers are used to detect leakage of the coolant used in your liquid cooling system.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under ["Quick Reference" on page 12](#).

M.2 Boot Tray Connector

Use the PCIe 5.0 x8 connector located at JPCIE3 on the X14DBT-FAP/-FLAP motherboard to connect an M.2 boot tray.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under ["Quick Reference" on page 12](#).

MCIO PCIe 5.0 x8 Connectors

Mini Cool Edge IO (MCIO) PCIe 5.0 x8 connectors are located at JPCIE1A1 (P2_PE0 0-7), JPCIE1B1 (P2_PE0 8-15), and JPCIE2A1 (P2_PE1 15-8) on the X14DBT-FAP/-FLAP motherboard.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under ["Quick Reference" on page 12](#).

Motherboard CPLD Header

A Motherboard Complex Programmable Logic Device header, located at JPRG1 on the side of the X14DBT-FAP/-FLAP motherboard, allows for engineering programming for firmware/software performance.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under ["Quick Reference" on page 12](#).

NC-SI Connection

The Network Controller Sideband Interface (NC-SI) connection is located at JNCSI1 on the X14DBT-FAP/-FLAP motherboard. This connection is used to connect a Network Interface Card (NIC) to the motherboard to allow the onboard Baseboard Management Controller (BMC) to communicate with a network.

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

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

PCIe 5.0 x16 Expansion Slot

There is a PCIe 5.0 x16 expansion slot for AOC located at JPCIE4 (P1_PE0 0-15) on the X14DBT-FAP/-FLAP motherboard. This expansion slot supports PCIe 5.0 x16 devices.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

I/O Module Connector

There is an I/O Module Connector on the motherboard at JRIO1. Connect this to provide a 2x10 connection Dedicated BMC LAN access, UID, and BMC LED to the motherboard.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

TPM/Port 80 Header

The JTPM1 header on the X14DBT-FAP/-FLAP 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 X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

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	Ground
7	SPI_MOSI	8	No Connection
9	+1.8 V Standby	10	SPI_IRQ#

VRM Header

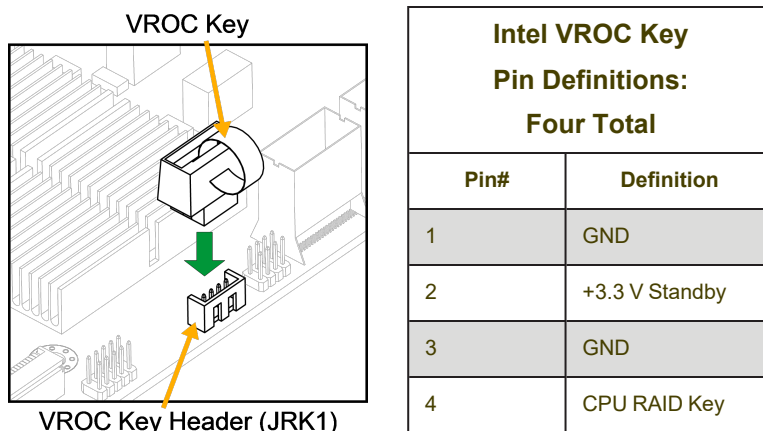
A Voltage Regulator Module (VRM) header is located at JVRM1 on the X14DBT-FAP/-FLAP motherboard. The VRM header adjusts the voltages heading to the processor and other components to prevent exceeded or insufficient voltage supplies.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "Quick Reference" on page 12.

VROC RAID Key Header

A VROC RAID Key header is located at JRK1 on the X14DBT-FAP/-FLAP motherboard. Install a VROC RAID key on JRK1 for NVMe RAID support as shown in the illustration below.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "Quick Reference" on page 12.



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

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

I/O Ports

For information about the I/O connectors and ports of the X14DBT-FAP/-FLAP motherboard, refer to the following content.

I/O Port	Function	Description
JAIOM1 (P1-AIOM PCIe 5.0 x16)	Advanced I/O Module (AIOM) for I/O Support	Provides input/output connections on the I/O face of your system
JVGA1	VGA Port	Provides analog interface support between the computer and the video displays
JUSB1 (USB0/1)	Universal Serial Bus (USB) 2.0 Ports	Provides USB support via USB cables (not included)

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.

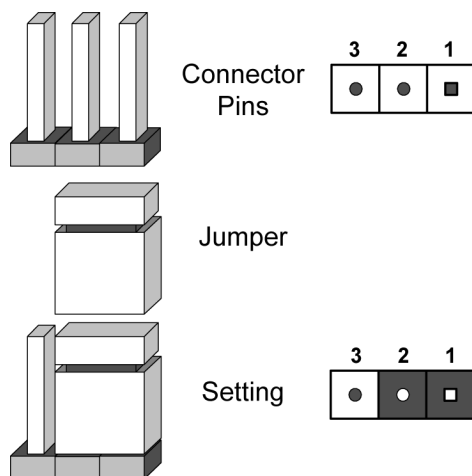


Figure 2-26. Jumping Connector Pins

CMOS Clear

JBT1 on the X14DBT-FAP/-FLAP motherboard is used to clear CMOS, which will also clear any passwords. Instead of pins, this jumper consists of contact pads to prevent accidentally clearing the contents of CMOS.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.



JBT1 contact pads

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

Note: Clearing CMOS will also clear all passwords.

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

Power Button

There is a power button located at JPBTN1 on the X14DBT-FAP/-FLAP motherboard. Momentarily contacting the button will power on/off the system.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

UID LED and System_Reset Button Select Jumper

Jumper JRU1 on the X14DBT-FAP/-FLAP motherboard is used in conjunction with the I/O Module Connector (JRIO1) to function as a System_Reset button or a UID LED button. To configure for UID button use in a chassis that supports front UID connection, close pins 1 and 2 of jumper JRU1. To set for the reset button function, close pins 3 and 4 of jumper JRU1.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

UID Switch/Reset Button Select Jumper (JRU1)	
Jumper Settings	
State	Description
Close pins 1 and 2 of JRU1	Used for UID switch support
Close pins 2 and 3 of JRU1	Used for System Reset support

LED Indicators

For information about the LED indicators on the X14DBT-FAP/-FLAP motherboard, refer to the following content.

+3.3 V AUX Power LED

The +3.3 V AUX Power LED at LED3 on the X14DBT-FAP/-FLAP motherboard monitors the status of +3.3 V AUX power.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

+3.3 V AUX Power LED State	
LED Color	Definition
Solid Yellow	Power On

BMC Heartbeat LED

A BMC Heartbeat LED is located at LEDM1 on the X14DBT-FAP/-FLAP motherboard. When this LED is blinking, the BMC is functioning normally. During a BMC Reset or a Cold Boot, LEDM1 will turn solid green.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

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

Control Panel LEDs

There are a total of four control panels, one for each node.

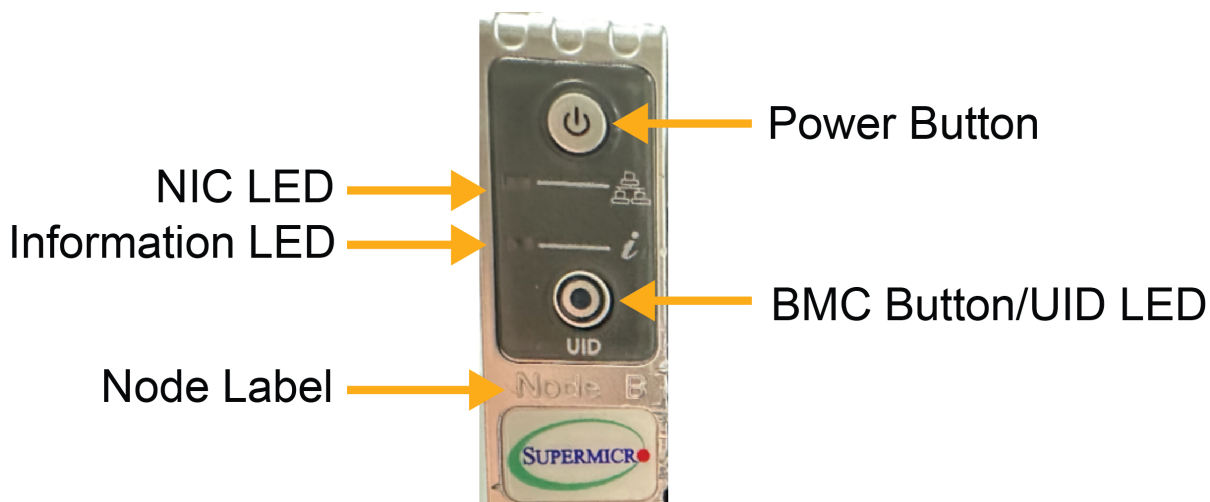


Figure 2-27. Control Panel

Control Panel Features	
Feature	Description
Power Button	Applies or removes primary power from the power supply to the server but maintains standby power
NIC LED	Indicates network activity on the LAN when flashing
Information LED	Provides universal information about each node Universal information LED (see the Information LED table for details)
BMC Button/UID LED	BMC button: Resets the BMC firmware when pressed Unit Identification (UID) button: Powers the blue indicator of the Information LED and a blue LED on the rear of the chassis; used to locate the server in large racks and server banks
Node Label	Identifies the node connected to the control panel Nodes A and C: Labels are above their control panel Nodes B and D: Labels are below their control panel

Information LED	
Color, Status	Description
Red, solid	An overheat condition has occurred.
Red, blinking at 1 Hz	Fan failure, check for an inoperative fan.
Red, blinking at 0.25 Hz	Power failure, check for a non-operational power supply.
Red, solid, with Power LED blinking green	Fault detected.
Blue and red, blinking at 10 Hz	Recovery mode.
Blue, solid	UID has been activated locally to locate the server in a rack environment.
Blue, blinking at 1 Hz	UID has been activated using the BMC to locate the server in a rack environment.
Blue, blinking at 2 Hz	BMC is resetting.
Blue, blinking at 4 Hz	BMC is setting factory defaults.
Blue, blinking at 10 Hz with Power LED blinking green	BMC/BIOS is updating
Red, blinking at 4 Hz	Leakage event
Red, blinking at 10 Hz	Power failure to trigger HPC N Power Mode

UID Switch/BMC Reset			
Feature	User Action	Color, Status	Behavior
UID Switch	Press UID button once	Blue, solid on	UID LED turns on/off

UID Switch/BMC Reset			
Feature	User Action	Color, Status	Behavior
BMC Reset	Hold for 6s	Blue, blinking at 4 Hz	BMC resets
	Hold for 12s	Blue, blinking at 4 Hz	Restore factory default

Onboard Power LED

The Onboard Power LED is located at LED4 on the X14DBT-FAP/-FLAP 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 X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

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

Unit ID (UID) LED

The UID LED indicator is located at LED5 on the X14DBT-FAP/-FLAP motherboard. This UID indicator provides easy identification of a system that may need to be serviced.

For a detailed diagram of the X14DBT-FAP/-FLAP motherboard, see the layout under "[Quick Reference](#)" on page 12.

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

Chapter 3:

Troubleshooting

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

3.1 Troubleshooting Procedures	62
Before Power On	62
No Power	62
No Video	62
System Boot Failure	62
Memory Errors	63
Losing the System's Setup Configuration	63
If the System Becomes Unstable	63
3.2 Technical Support Procedures	65
3.3 Motherboard Battery	66
3.4 Where to Get Replacement Components	67
3.5 Returning Merchandise for Service	68
3.6 Feedback	69

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 65](#) or ["Returning Merchandise for Service" on page 68](#) 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 56](#).
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 28](#) 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 11](#) for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.

If the System Becomes Unstable

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

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

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

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

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

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

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

3.2 Technical Support Procedures

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

1. Refer to "Troubleshooting Procedures" on page 62 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 10.

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 50.

3.4 Where to Get Replacement Components

If you need replacement parts for your X14DBT-FAP/-FLAP motherboard, to ensure the highest level of professional service and technical support, purchase exclusively from our Supermicro Authorized Distributors/System Integrators/Resellers. A list can be found on the Supermicro website:

<https://www.supermicro.com>

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

3.5 Returning Merchandise for Service

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

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

<https://www.supermicro.com/RmaForm>

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

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

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

3.6 Feedback

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

Chapter 4:

UEFI BIOS

The following content contains information on BIOS configuration with the X14DBT-FAP/-FLAP motherboard.

4.1 Introduction	71
4.2 Main Setup	73
4.3 Advanced Setup Configurations	75
4.4 Event Logs	114
4.5 BMC	116
4.6 Security	120
4.7 Boot	127
4.8 Save & Exit	129

4.1 Introduction

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

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

Updating BIOS

It is recommended that you do not upgrade your BIOS if you are not experiencing any problems with your system. Updated BIOS files are located on our website at the following page:

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

Check our BIOS warning message and the information on how to update your BIOS on our website. Select your motherboard model and download the BIOS file to your computer. Also, check the current BIOS revision to make sure that it is newer than your BIOS before downloading.

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

Unzip the BIOS file onto a bootable USB device and then boot into the built-in UEFI Shell and type "flash.nsh <BIOS filename><BMC Username><BMC Password>" to start the BIOS update. The flash script will invoke the SCC (EFI) tool automatically to perform the BIOS update, beginning with uploading the BIOS image to BMC. After uploading the firmware, the system will reboot to continue the process. The BMC will take over and continue the BIOS update in the background. The process will take 3–5 minutes.

Starting the Setup Utility

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

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

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

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

4.2 Main Setup

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

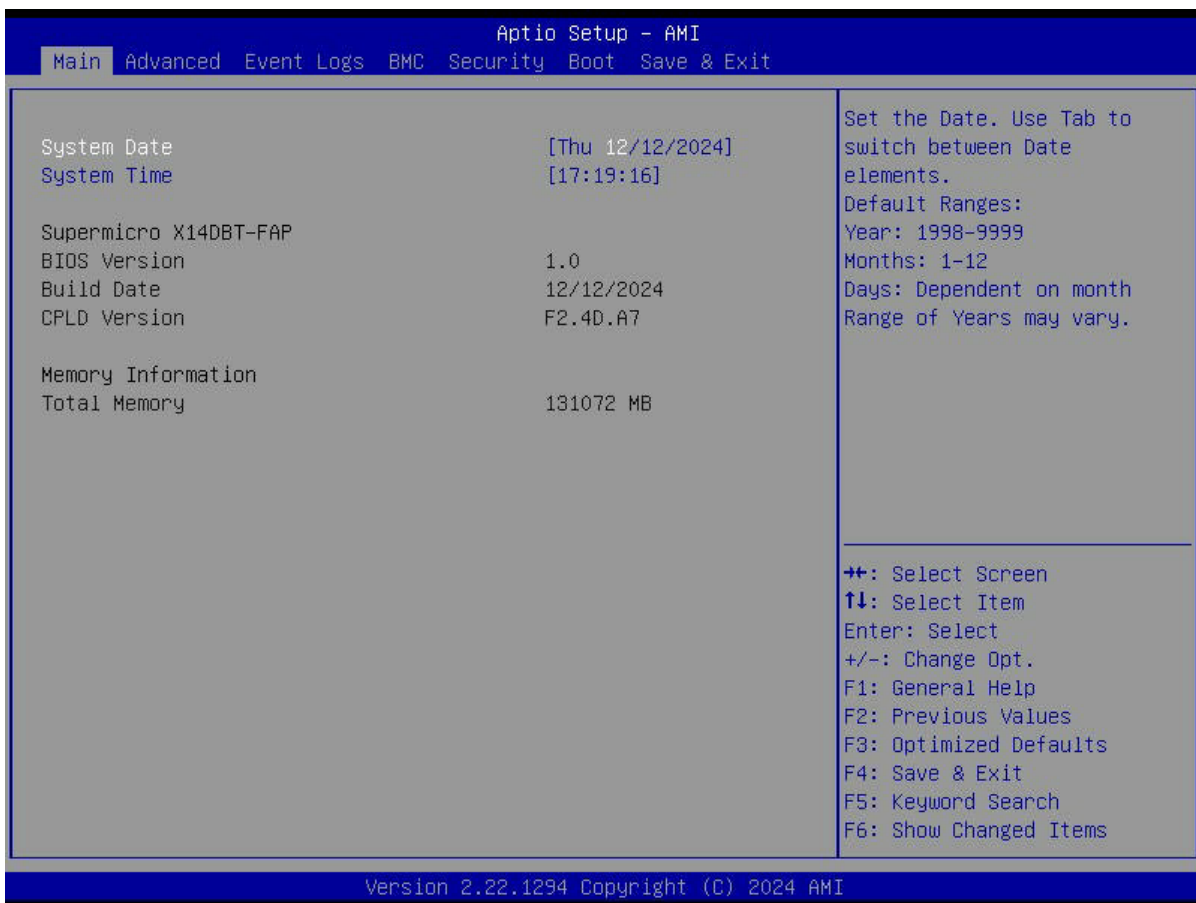


Figure 4-1. Main Setup Screen

System Date/System Time

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

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

Supermicro X14DBT-FAP/-FLAP

BIOS Version

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

Build Date

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

CPLD Version

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

Memory Information**Total Memory**

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

4.3 Advanced Setup Configurations

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

Important: Use caution when changing the Advanced settings. An incorrect value, an improper DRAM frequency, or a wrong BIOS timing setting may cause the system to malfunction. When this occurs, revert the setting to the manufacture default settings.

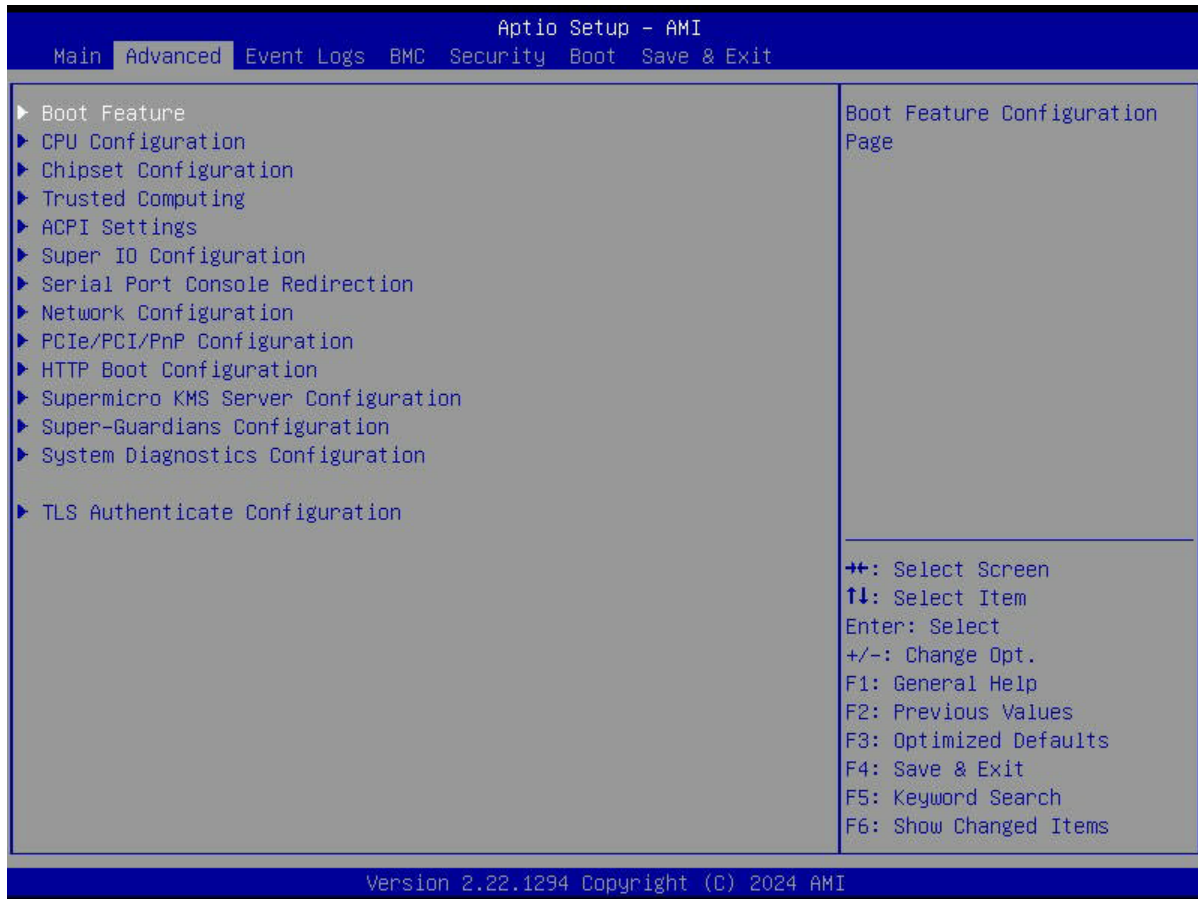


Figure 4-2. Advanced Setup Configurations Screen

Boot Feature Menu

► Boot Feature

Quiet Boot

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

are Disabled and **Enabled**.

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

Bootup NumLock State

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

Wait For "F1" If Error

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

Re-try Boot

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

Power Configuration

Watch Dog Function

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

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

Use this feature to configure the Watch Dog Time_out setting. The options are **Reset** and NMI.

Restore on AC Power Loss

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

Power Button Function

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

CPU Configuration Menu

► CPU Configuration

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

The following processor information is displayed:

- Processor BSP Revision
- Processor Socket
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM (Per Core)
- L2 Cache RAM (Per Core)
- L3 Cache RAM (Per Package)
- Processor 0 Version
- Processor 1 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.

Note: This feature is NOT available when "Workload Profile" is set to Telco FlexRAN.

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.

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

Adjacent Cache Prefetch

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

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

DCU Streamer Prefetcher

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

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

DCU IP Prefetcher

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

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

LLC Prefetch

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

Note: This feature is available when "Workload Profile" is set to Disabled, Telco NFVI, or Telco NFVI-FP.

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.

Note: This feature is NOT available when "Workload Profile" is set to Telco FlexRAN.

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.

Note: This feature is NOT available when "Workload Profile" is set to Telco FlexRAN.

APIC Physical Mode

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

TXT Support

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

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

Intel Virtualization Technology

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

Notes:

- This feature is NOT available when "TXT Support" is set to Enabled.
- This feature is NOT available when "Workload Profile" is set to Virtualization, Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

Enable SMX

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

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

PPIN Control

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

AES-NI

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

Advanced Power Management Configuration Menu

► Advanced Power Management Configuration

Latency Optimized Mode

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

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

Workload Profile

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

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

Power Performance Tuning

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

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

ENERGY_PERF_BIAS_CFG Mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode)

Use this feature to configure the proper operation setting for your machine by achieving the desired system performance level and energy saving (efficiency) level at the same time. Select Maximum Performance to maximize system performance to its highest potential; however, this may consume maximal amount of power as energy is needed to fuel processor operation.

Select Performance to enhance system performance; however, this may consume more power as energy is needed to fuel the processors for operation. The options are Extreme Performance, Maximum Performance, Performance, **Balanced Performance**, Balanced Power, Power, and Max Power Efficient. Please note that the options of Extreme Performance and Max Power Efficient are motherboard-dependent.

Notes:

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

CPU P State Control Menu

► CPU P State Control

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

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.

Notes:

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

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

- SST-PP Level
- Capable
- Core Count
- P1 Ratio

- Package TDP (W)
- DTS_Max

SpeedStep (P-States)

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

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

EIST PSD Function

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

Notes:

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

Turbo Mode (Available when "SpeedStep (P-States)" is set to Enabled and when "Workload Profile" is set to Disabled)

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**.

Hardware PM State Control Menu

► Hardware PM State Control

Notes:

- This submenu is available when "Power Performance Tuning" is set to BIOS Controls EPB.
- This submenu is NOT available when "Workload Profile" is set to HPC, Virtualization, Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

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**

Notes:

- This submenu is available when "Power Performance Tuning" is set to BIOS Controls EPB.
- This submenu is NOT available when "Workload Profile" is set to Telco NFVI, Telco NFVI-FP, or Telco FlexRAN.

Monitor MWAIT

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

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

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.

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

ACPI C6x Enumeration

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

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

Package C State Control Menu

► **Package C State Control**

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

Package C State

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

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

LTR IIO Input

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

CPU1/CPU2 Core Disable Bitmap Menu

► **CPU1/CPU2 Core Disable Bitmap**

Note: The submenu of CPU2 Core Disable Bitmap is available when your motherboard supports dual processors.

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.

Available Bitmap[2]:

This feature displays the available Bitmap[2]. 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.

Disable Bitmap[2]:

Enter 0 to enable this feature for CPU Core Bitmap[2]. Enter FFFFFFFFFF to disable CPU Core Bitmap[2]. 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 192.

Chipset Configuration Menu

► Chipset Configuration

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

Uncore Configuration Menu

► Uncore Configuration

The following information is displayed.

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

Degrade Precedence

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

Link L0p Enable

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

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

Link L1 Enable

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

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

KTI Prefetch

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

IO Directory Cache (IODC)

This feature allows the IODC to generate snoops instead of generating memory lockups for remote IIO (InvlToM) and/or WCiLF (Cores). Select Auto for the IODC to generate snoops (instead of memory lockups) for WCiLF (Cores). The options are Disabled, **Auto**, Enable for Remote InvltoM Hybrid Push, Enable for Remote InvltoM AllocFlow, Enable for Remote InvltoM Hybrid AllocNonAlloc, and Enable for Remote InvltoM and Remote WCiLF.

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.

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

XPT Prefetch

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

Stale AtoS

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

LLC Dead Line Alloc

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

Memory Configuration Menu

► Memory Configuration

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

Enforce DDR Memory Frequency POR

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

Host Memory Frequency

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

Global Scrambling

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

Bank Idle Bypass

Select the Bank Idle Bypass value. The options are **Disabled**, Enabled, and Auto.

Memory Topology Menu

▶ **Memory Topology**

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

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

Memory Map Menu

▶ **Memory Map**

Intel(R) Flat Memory Mode Support

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

DDR CXL Heterogeneous Interleave Support

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

Memory RAS Configuration Menu

▶ **Memory RAS Configuration**

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

Mirror Mode

Use this feature to configure the mirror mode settings for all 1LM/2LM memory modules in the system, 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.

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

UEFI ARM Mirror

If this feature is set to Enabled, mirror mode configuration settings for UEFI-based Address Range memory will be enabled upon system boot. This will create a duplicate copy of data stored in the memory to increase memory security, but it will reduce the memory capacity into half. The options are **Disabled** and Enabled. The Address Range Mirroring (ARM) feature supports partial memory mirroring. This feature is CPU-dependent.

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

Mirror TAD0

Use this feature to enable the mirror mode on entire memory for Target Address Decoder 0 (TAD0). The options are **Disabled** and Enabled. This feature is CPU-dependent.

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

ARM Mirror Percentage (Available when "UEFI ARM Mirror" is set to Enabled)

Use this feature to set the percentage of memory space to be used for UEFI ARM mirroring for memory security enhancement. The default setting is **2500**.

Correctable Error Threshold

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

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

Leaky Bucket Low Bit

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

Leaky Bucket High Bit

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

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

Select Enabled for Adaptive Double Device Data Correction (ADDDC) support, which will not only provide memory error checking and correction but will also prevent the system from issuing a performance penalty before a device fails. Please note that virtual lockstep mode will

only start to work for ADDDC after a faulty DRAM module is spared. The options are Disabled and **Enabled**.

DDR PPR Type

Post Package Repair (PPR) is a new feature available for the DDR4/DDR5 technology. PPR provides additional spare capacity within a DDR4/DDR5 DRAM module that is used to replace faulty cell areas detected during system boot. PPR offers two types of memory repairs. Soft Post Package Repair (sPPR) provides a quick, temporary fix on a raw element in a bank group of a DDR4/DDR5 DRAM device, while hard Post Package Repair (hPPR) will take a longer time to provide a permanent repair on a raw element. The options are PPR Disabled, **Hard PPR**, and Soft PPR.

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

Enhanced PPR

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

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

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

Security Configuration Menu

► Security Configuration

Memory Encryption (TME) [Outputs]

The following information is displayed.

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

Memory Encryption (TME) [Inputs]

Memory Encryption (TME)

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

Total Memory Encryption Multi-Tenant (TME-MT)

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

Memory Integrity

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

The following information is displayed.

- KEY stock amount
- TME-MT key ID bits

TME Encryption Algorithm

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

Trust Domain Extensions (TDX) [Outputs]

The following information is displayed.

- TDX activation state

Trust Domain Extensions (TDX) [Inputs]

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

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

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

IMC#	IMC12	IMC11	IMC10	IMC9	IMC8	IMC7	CPU	IMC1	IMC2	IMC3	IMC4	IMC5	IMC6	
Channel	P1/P2-	P1/P2-	P1/P2-	P1/P2-	P1/P2-	P1/P2-		P1/P2-	P1/P2-	P1/P2-	P1/P2-	P1/P2-	P1/P2-	P1/P2-
	DIMML	DIMMK	DIMMJ	DIMMI	DIMMH	DIMMG		DIMMA	DIMMB	DIMMC	DIMMD	DIMME	DIMMF	
	Slot1	Slot1	Slot1	Slot1	Slot1	Slot1		Slot1	Slot1	Slot1	Slot1	Slot1	Slot1	
12	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5		

Trust Domain Extensions - Connect (TDX Connect) (Available when "Trust Domain Extensions (TDX)" is set to Enabled)

Use this feature to enable Intel TDX Connect support to improve I/O virtualization by removing the need to establish a secure TD-Device transport-level session. The options are **Disabled** and **Enabled**. This feature is CPU-dependent.

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

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

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

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

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

- TME-MT Keys:
- TDX Keys:

Processor Reserved Memory [Capabilities]

The following information is displayed.

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

Processor Reserved Memory [Outputs]

The following information is displayed.

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

Software Guard Extensions (SGX) [Outputs]

The following information is displayed when your motherboard supports SGX.

- SGX activation state
- SGX error code [HEX]

Software Guard Extensions (SGX) [Inputs]

The following features are available when your motherboard supports SGX.

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

IMC#	IMC12	IMC11	IMC10	IMC9	IMC8	IMC7	CPU	IMC1	IMC2	IMC3	IMC4	IMC5	IMC6	
Channel	P1/P2- DIMML	P1/P2- DIMMK	P1/P2- DIMMJ	P1/P2- DIMMI	P1/P2- DIMMH	P1/P2- DIMMG			P1/P2- DIMMA	P1/P2- DIMMB	P1/P2- DIMMC	P1/P2- DIMMD	P1/P2- DIMME	P1/P2- DIMMF
	Slot1	Slot1	Slot1	Slot1	Slot1	Slot1			Slot1	Slot1	Slot1	Slot1	Slot1	Slot1
12	DDR5	DDR5	DDR5	DDR5	DDR5	DDR5			DDR5	DDR5	DDR5	DDR5	DDR5	DDR5

SGX Factory Reset

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

SW Guard Extensions (SGX)

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

SGX Package Info In-Band Access

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

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

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

SGX QoS (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Use this feature to enable Intel SGX Quality of Service (QoS) support. QoS can enhance network performance by prioritizing network traffic. The options are Disabled and **Enabled**.

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

Owner EPOCH is used as a parameter to add personal entropy into the key derivation process. A correct Owner EPOCH is required to have access to personal data previously sealed by other platform users. There are two Owner EPOCH modes. One is New Random Owner EPOCH, and the other is manually entered by the user. Each EPOCH is 64-bit. The options are **SGX Owner EPOCH deactivated**, Change to New Random Owner EPOCHs, and Manual User Defined Owner EPOCHs.

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

Software Guard Extensions Epoch 0

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

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

Software Guard Extensions Epoch 1

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

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

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

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

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

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

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

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

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

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

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

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

SGX Auto MP Registration (Available when "SW Guard Extensions (SGX)" is set to Enabled)

Use this feature to enable/disable SGX Auto Multi-Package Registration Agent (MPA) running automatically at boot time. The options are **Disabled** and Enabled.

I/O Configuration Menu

► I/O Configuration

PCIe Completion Timeout

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

PCIe ASPM Support (Global)

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

Equalization Bypass To Highest Rate

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

NVMe Mode Switch

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

PCIe PLL SSC

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

*CPU1/CPU2 Configuration Menu***► CPU1/CPU2 Configuration**

Note: The submenu of CPU2 Configuration is motherboard-dependent.

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

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

Bifurcation

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

Intel VMD Technology

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

► PCI Express 0 Port A/B/C/D/E/F/G/H – PCI Express 5 Port A/B/C/D/E/F/G/H**Requested Link Speed**

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

PCIe Port Max Payload Size

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

MCTP

Enable this feature, Management Component Transport Protocol (MCTP), to support communications between devices in a platform management subsystem. MCTP's underlying device buses include SMBus/I²C, serial links, PCIe, and USB. The options are Disabled and **Enabled**.

Intel VMD Technology

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

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

► Intel VT for Directed I/O (VT-d)

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

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. (DMA is the abbreviation for Direct Memory Access. DMAR is the abbreviation for DMA Remapping Reporting.)

PCIe ACSCTL

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

PCIe Leaky Bucket Configuration Menu

► PCIe Leaky Bucket Configuration

Gen2 Link Degradation

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

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

Gen3 Link Degradation

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

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

Gen4 Link Degradation

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

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

Gen5 Link Degradation

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

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

Trusted Computing Menu

► Trusted Computing

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

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

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

Security Device Support

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

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

- Active PCR banks
- Available PCR banks

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

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**.

PH Randomization

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

Supermicro BIOS-Based TPM Provision Support

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

ACPI Settings Menu

▶ ACPI Settings

NUMA

Use this feature to enable Non-Uniform Memory Access (NUMA) support to minimize memory access latencies. The options are Disabled and **Enabled**. This feature is CPU-dependent.

Virtual NUMA

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

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

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

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

WHEA Support

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

Super IO Configuration Menu

► Super IO Configuration

The following information is displayed.

- Super IO Chip

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

Serial Port 1 Configuration Menu

► Serial Port 1 Configuration

Serial Port 1

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

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

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

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

Use this feature to specify the base I/O port address and the Interrupt Request address of serial port 1. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 1. The options are **Auto**, (IO=3F8h; IRQ=4;), (IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

Serial Port 2 Configuration Menu**► Serial Port 2 Configuration**

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

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

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

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

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

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

Use this feature to specify the base I/O port address and the Interrupt Request address of serial port 2 (or SOL). Select Auto for the BIOS to automatically assign the base I/O and IRQ address to serial port 2 (or SOL). The options are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=2F8h; IRQ=3,4,5,6,7,9,10,11,12;), (IO=3E8h; IRQ=3,4,5,6,7,9,10,11,12;), and (IO=2E8h; IRQ=3,4,5,6,7,9,10,11,12;).

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

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

Serial Port Console Redirection Menu**► Serial Port Console Redirection****COM1 (Available when your system supports the serial port of COM1)****Console Redirection**

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

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

SOL/COM2

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

► Console Redirection 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 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

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

Terminal Type EMS

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

Bits Per Second EMS

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

Flow Control EMS

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

The following information is displayed.

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

Network Stack Configuration Menu

► Network Stack Configuration

Network Stack

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

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

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

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

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

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

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

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

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

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

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

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

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

PCIe/PCI/PnP Configuration Menu

► PCIe/PCI/PnP Configuration

The following information is displayed.

- PCI Bus Driver Version

PCI Devices Common Settings:**Re-Size BAR Support**

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

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

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

ARI Support

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

MMCFG Base

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

MMCFG Size

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

MMIO High Base

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

MMIO High Granularity Size

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

Bus Master Enable

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

NVMe Firmware Source

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

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.

Onboard LAN2 Option ROM

Use this feature to boot the computer using the EFI device installed on LAN port 2. Select Disabled to disable this feature. The default setting is **Disabled**.

Note: This feature is available when your motherboard supports onboard LAN ports and when "Onboard LAN1 Option ROM" is set to Disabled.

JPCIE1 SLOT OPROM / SCC_P2N2M2_F1 M.2-1 OPROM / SCC_P2N2M2_F1 M.2-2 OPROM / RSC_F_6G5 SLOT OPROM / OPROM / Onboard NVMe1 Option ROM – Onboard NVMe24 Option ROM

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

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

HTTP Boot Configuration Menu

► HTTP Boot Configuration

HTTP Boot Policy

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

HTTPS Boot Checks Hostname

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

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

Priority of HTTP Boot

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

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

Select IPv4 or IPv6

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

Boot Description

Use this feature to enter a boot description, which cannot be longer than 75 characters. Please 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.

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.

Supermicro KMS Server IP address

Use this feature to set the Supermicro Key Management Service (KMS) server IPv4 address in dotted-decimal notation.

Second Supermicro KMS Server IP address

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

Supermicro KMS TCP Port number

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

KMS Time Out

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

TimeZone

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

Client UserName

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

Client Password

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

▶ CA Certificate

▶ Client Certificate

▶ Client Private Key

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



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

Use this feature to change the private key password.

Super-Guardians Configuration Menu

► Super-Guardians Configuration

Super-Guardians Protection Policy

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

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

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

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

Notes:

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

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

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

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

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

When this feature has previously been set to Enabled, the options are **Enabled** and Reset. 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.

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

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.

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

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

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

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

System Diagnostics Configuration Menu

▶ System Diagnostics Configuration

Launch System Diagnostics

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

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

TLS Authenticate Configuration Menu

▶ TLS Authenticate Configuration

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

▶ Server CA Configuration

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

▶ Enroll Certification

Use this feature to enroll the certificate in the system.

▶ Enroll Certification Using File

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

▶ Commit Changes and Exit

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

▶ Discard Changes and Exit

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

▶ Delete Certification

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

▶ Client Certification Configuration

4.4 Event Logs

Use this menu to configure Event Logs settings.

Note: After making any changes in this section, please be sure to reboot the system for the changes to take effect.

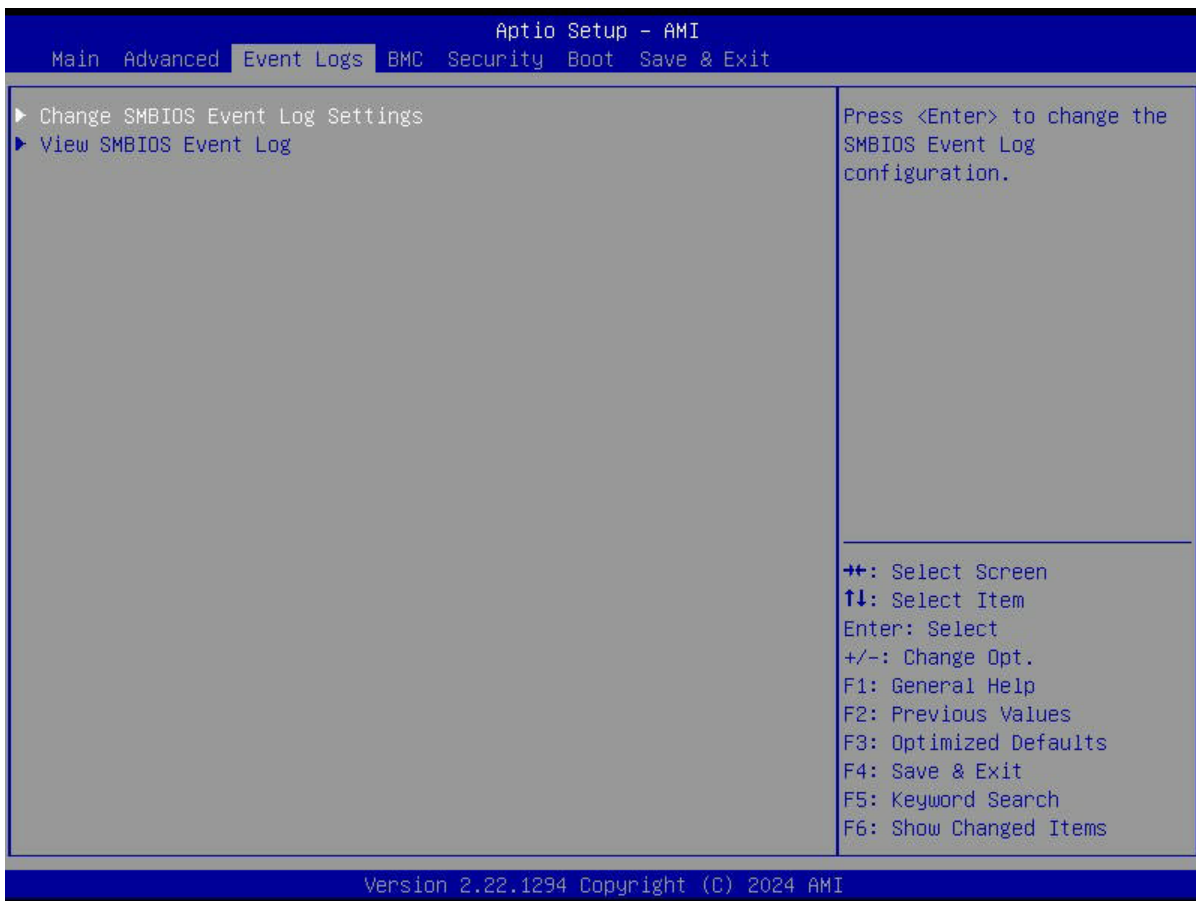


Figure 4-3. Event Logs Screen

► 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 event in the system event log. Select this feature and press <Enter> to view the status of an event in the log. The following information is displayed: DATE / TIME / ERROR CODE / SEVERITY.

4.5 BMC

Use this menu to configure Baseboard Management Console (BMC) settings.



Figure 4-4. BMC Screen

BMC Firmware Revision

This feature indicates the BMC firmware revision used in this system.

BMC STATUS

This feature indicates the status of the BMC firmware installed in this system.

System Event Log Menu

► System Event Log

Note: All values changed in this submenu do not take effect until computer is restarted.

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL (Available when "SEL Components" is set to Enabled)

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

When SEL is Full (Available when "SEL Components" is set to Enabled)

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

BMC Network Configuration Menu

► BMC Network Configuration

Update BMC LAN Configuration

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

Configure IPv4 Support

BMC LAN Selection

This feature displays the type of the BMC LAN.

BMC Network Link Status:

This feature displays the status of the BMC network link for this system.

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

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**.

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 "Configuration Address Source" above is set to Static.

Subnet Mask

This feature displays the sub-network that this computer belongs to. It is available for configuration when "Configuration Address Source" above is set to Static.

Station MAC Address

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

Gateway IP Address

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1). It is available for configuration when "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 (Available when "Update BMC LAN Configuration" is set to Yes)

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

Configuration Address Source (Available when "IPv6 Support" is set to Enabled)

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.

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 "Configuration Address Source" above is set to Static Configuration.

Prefix Length

This feature displays the prefix length. It is available for configuration when "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 "Configuration Address Source" above is set to Static Configuration.

Advanced Settings (Available when "Configuration Address Source" is set to DHCPv6 Stateless)

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.

Preferred DNS server IP (Available when "Advanced Settings" above is set to Manually obtain DNS server IP)

This feature displays the preferred DNS server IP. It can be configured via Redfish.

Alternative DNS server IP (Available when "Advanced Settings" above is set to Manually obtain DNS server IP)

This feature displays the alternative DNS server IP. It can be configured via Redfish.

Configure VLAN Support

VLAN Support (Available when "Update BMC LAN Configuration" is set to Yes)

Use this feature to enable the virtual LAN (VLAN) support. The options are Enabled and Disabled.

VLAN ID (Available when "VLAN Support" is set to Enabled)

Use this feature to create a new VLAN ID. The valid range is 1–4094. The default setting is 1.

4.6 Security

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

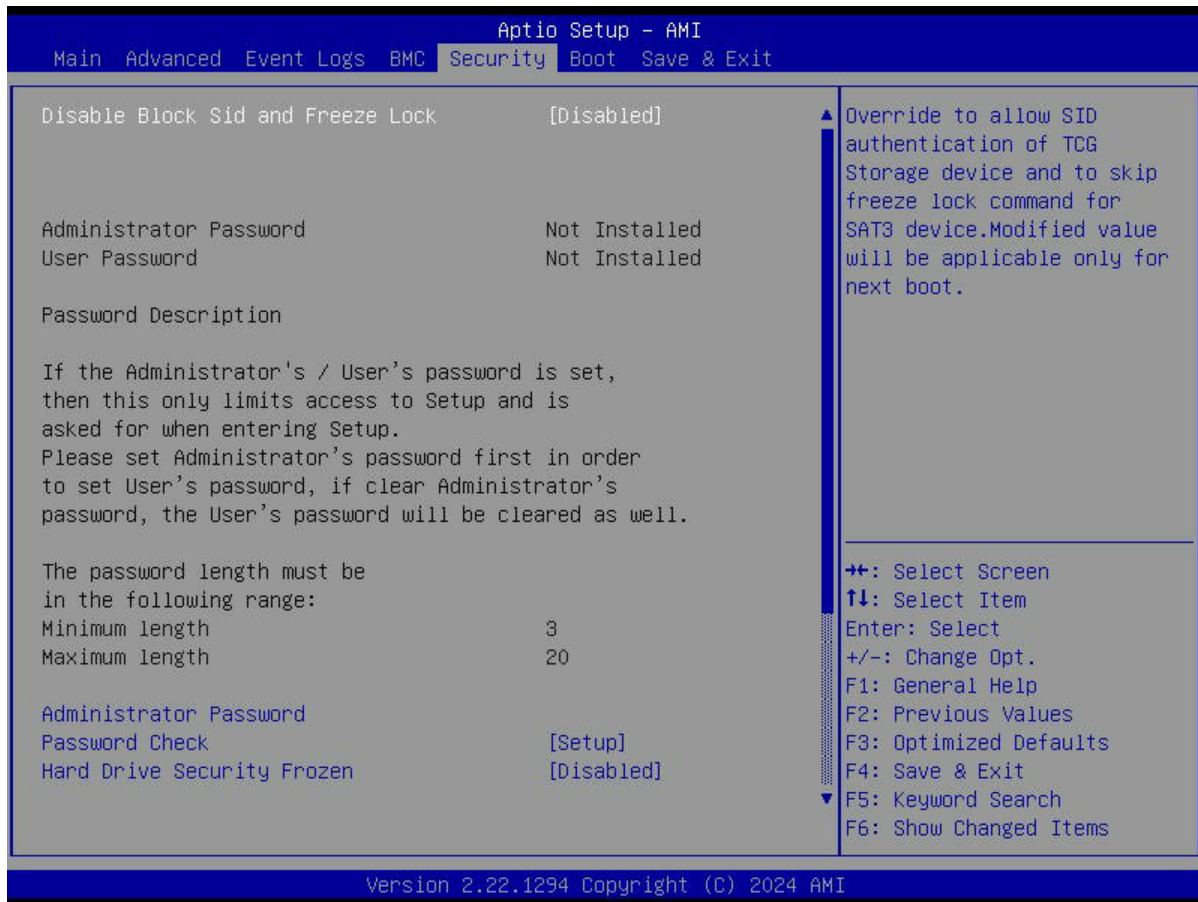


Figure 4-5. Security Screen

Disable Block Sid and Freeze Lock (Available when your storage devices support TCG)

Select Enabled to allow SID authentication to be performed in TCG storage devices. The options are **Disabled** and Enabled.

The following information is displayed:

- Administrator Password
- User Password
- Password Description

Administrator Password

This feature indicates if an administrator password has been installed. Use this feature to set the administrator password, which is required to enter the BIOS Setup utility. The length of the password can be between three and 20 characters long.

User Password (Available when "Administrator Password" has been set)

This feature indicates if a user password has been installed. Use this feature to set the user password which is required to enter the BIOS Setup utility. The length of the password can be between three and 20 characters long.

Password Check

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

Hard Drive Security Frozen

Select Enabled to freeze the Lock Security feature for HDD to protect key data in hard drives from being altered. The options are **Disabled** and Enabled.

Lockdown Mode (Available when the DCMS key is activated)

Select Enabled to support the Lockdown Mode, which prevents the existing data or keys stored in the system from being altered or changed in an effort to preserve system integrity and security. The options are **Disabled** and Enabled.

Supermicro Security Erase Configuration Menu

► Supermicro Security Erase Configuration

Use this submenu to configure the Supermicro-proprietary Security Erase settings. When this submenu is selected, the following information is displayed. Please 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 "1111111111" 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.

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 provision factory default settings after a platform reset while the system is in the Setup Mode. 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 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.

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.

4.7 Boot

Use this menu to configure Boot settings.

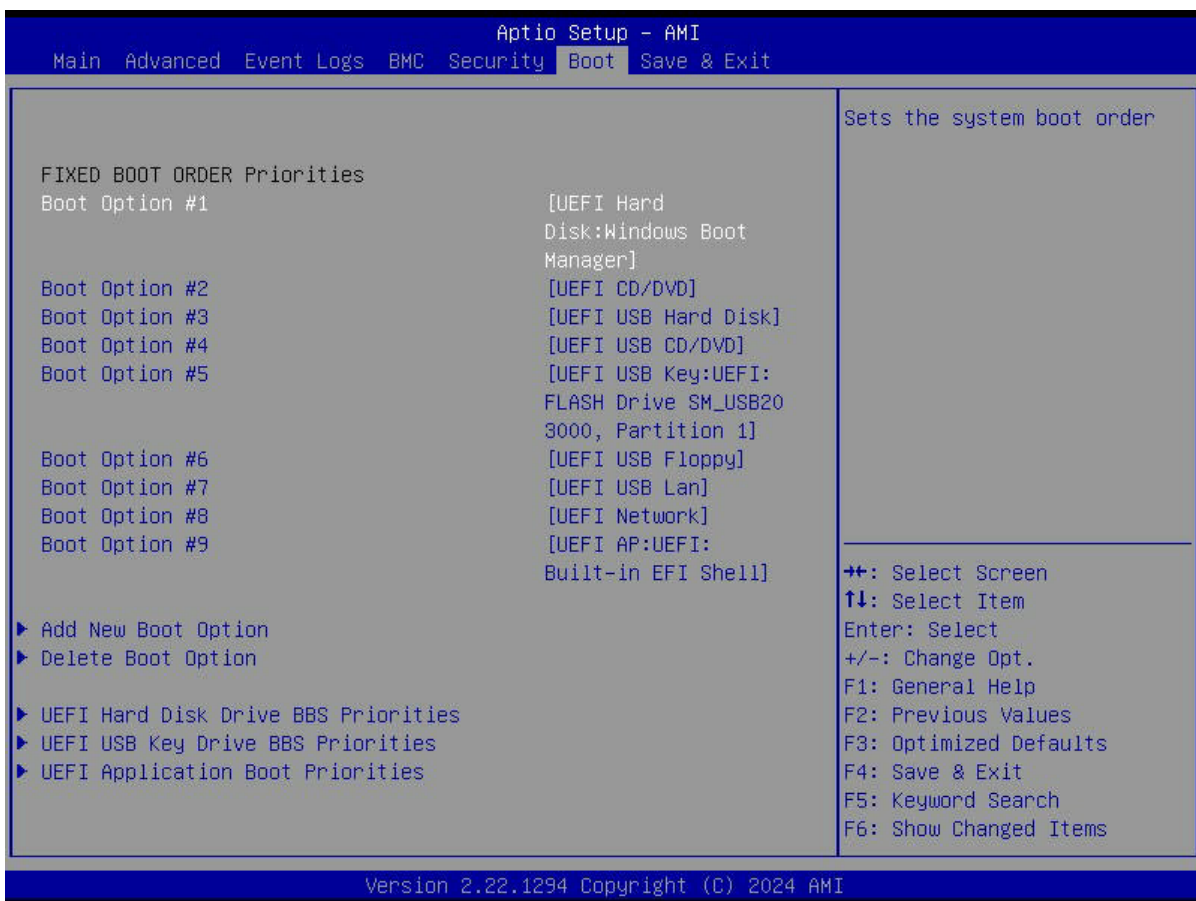


Figure 4-6. Boot Screen

FIXED BOOT ORDER Priorities

Use this feature to prioritize the order of a bootable device from which the system will boot. Press <Enter> on each item sequentially to select the device.

- Boot Option #1 – Boot Option #9

► Add New Boot Option

Use this feature to add a new boot option to the boot priority features for system boot.

Note: This submenu is available when any storage device is detected by the BIOS.

Add boot option

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

Path for boot option

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

Boot option File Path

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

Create

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

▶ Delete Boot Option

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

Delete Boot Option

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

▶ UEFI Hard Disk Drive BBS 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 Application Boot Priorities

Use this feature to set the system boot order of detected devices.

4.8 Save & Exit

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

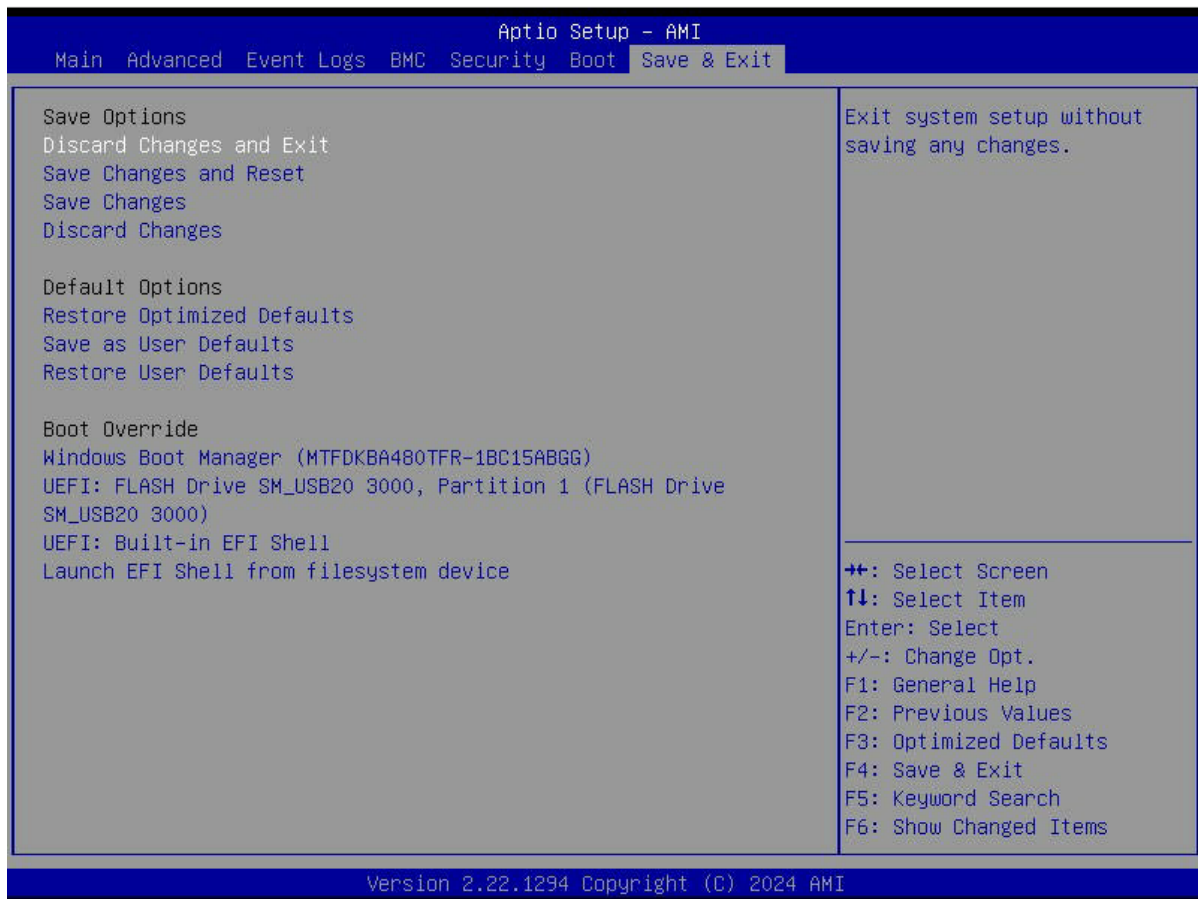


Figure 4-7. Save & Exit Screen

Save Options

Discard Changes and Exit

Use this feature to exit from the BIOS Setup utility without making any permanent changes to the system configuration and reboot the computer.

Save Changes and Reset

On completing the system configuration changes, use this feature to exit the BIOS Setup utility and reboot the computer for the new system configuration parameters to take effect.

Save Changes

On completing the system configuration changes, use this feature to save all changes made. This will not reset (reboot) the system.

Discard Changes

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

Default Options**Restore Optimized Defaults**

Select this feature and press <Enter> to load manufacturer optimized default settings, which are intended for maximum system performance but not for maximum stability.

Note: After pressing <Enter>, reboot the system for the changes to take effect, which ensures that this system has the optimized default settings.

Save as User Defaults

Select this feature and press <Enter> to save all changes as the default values specified to the BIOS Setup utility for future use.

Restore User Defaults

Select this feature and press <Enter> to retrieve user-defined default settings that have been saved previously.

Boot Override

Note: Use this section to override the Boot priorities sequence in the Boot menu, and immediately boot the system with a device specified here instead of the one specified in the boot list. This is a one-time boot override.

UEFI: Built-in EFI Shell

Use this feature to launch the built-in EFI shell environment.

Launch EFI Shell from filesystem device

Use this feature to launch the EFI shell application (Shell.efi) from one of the available filesystem devices. A filesystem is a virtual, logical, or physical system for organizing, managing, and accessing the files and directories on devices such as SSDs, HDDs, or other storage devices.

Appendix A:

Software

After the X14DBT-FAP/-FLAP motherboard has been installed, you can install the Operating System (OS), configure RAID settings, and install the drivers.

Microsoft Windows OS Installation

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

Installing the OS

1. Create a method to access the Microsoft Windows installation ISO file. That can be a USB flash or media drive, or the BMC KVM console.
2. Retrieve the proper drivers. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities," select the proper driver, and copy it to a USB flash drive.
3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing <F11> during the system bootup.

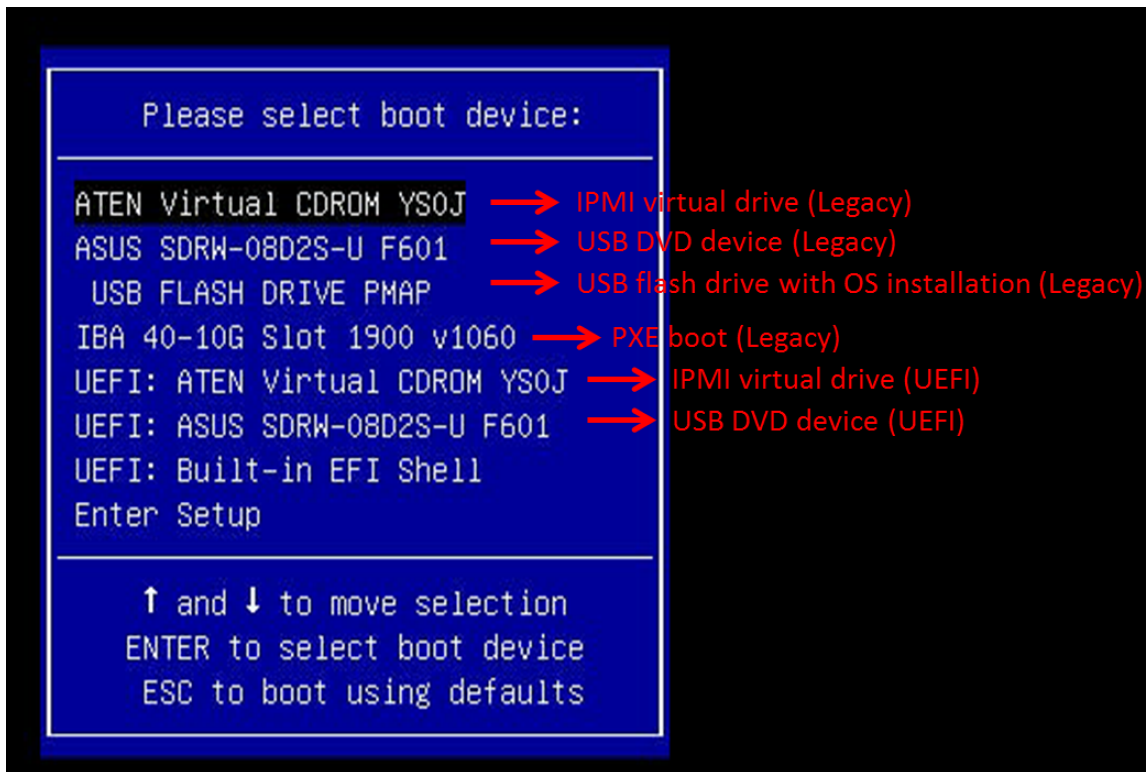


Figure A-1. Selecting the Boot Device

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

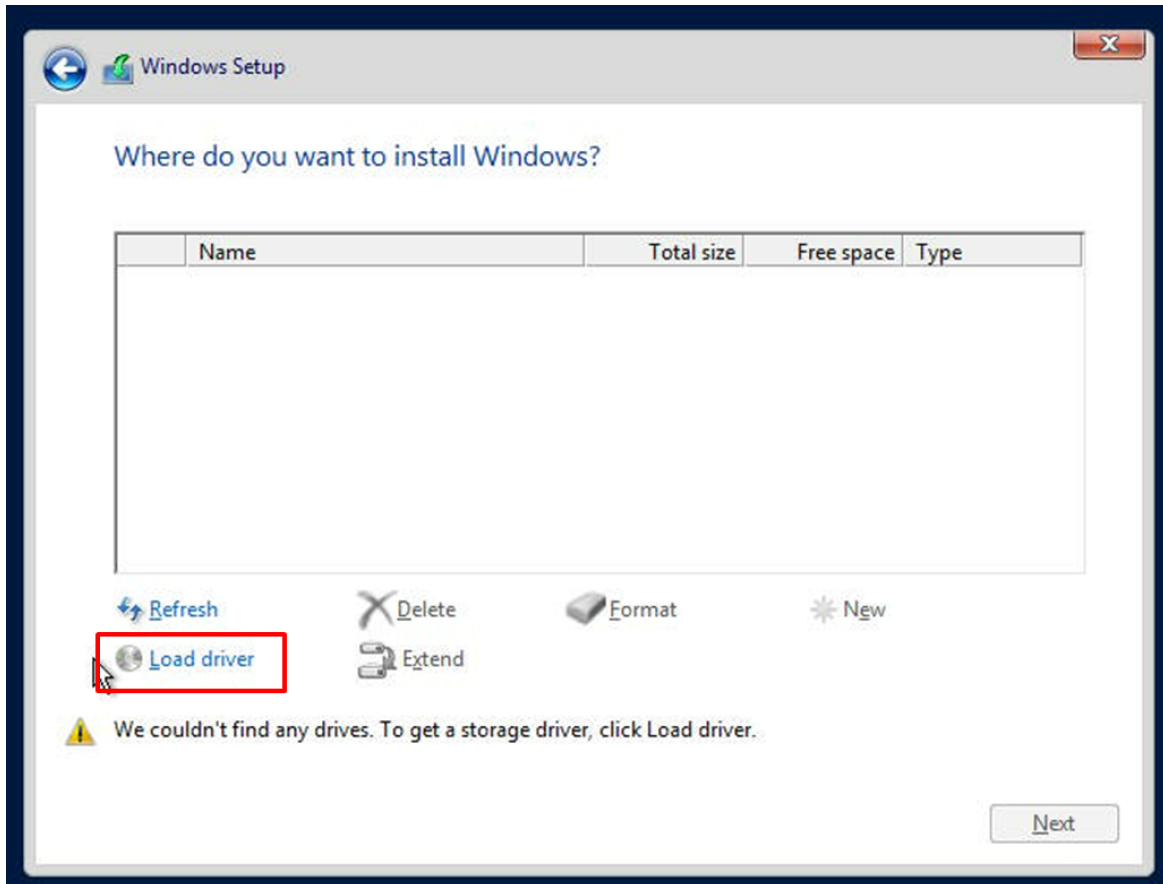


Figure A-2. Loading the Driver Link

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

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

A.1 Driver Installation

The Supermicro website contains drivers and utilities for your system at the following page:

<https://www.supermicro.com/wdl>.

Some of these drivers and utilities must be installed, such as the chipset driver. After accessing the website, go into the CDR_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to a USB flash or media drive. You may also use a utility to extract the ISO file if preferred.

Another option is to go to the Supermicro website at <https://www.supermicro.com>. Find the product page for your motherboard and download the latest drivers and utilities. Insert the flash drive or disk, and the screenshot shown below should appear.

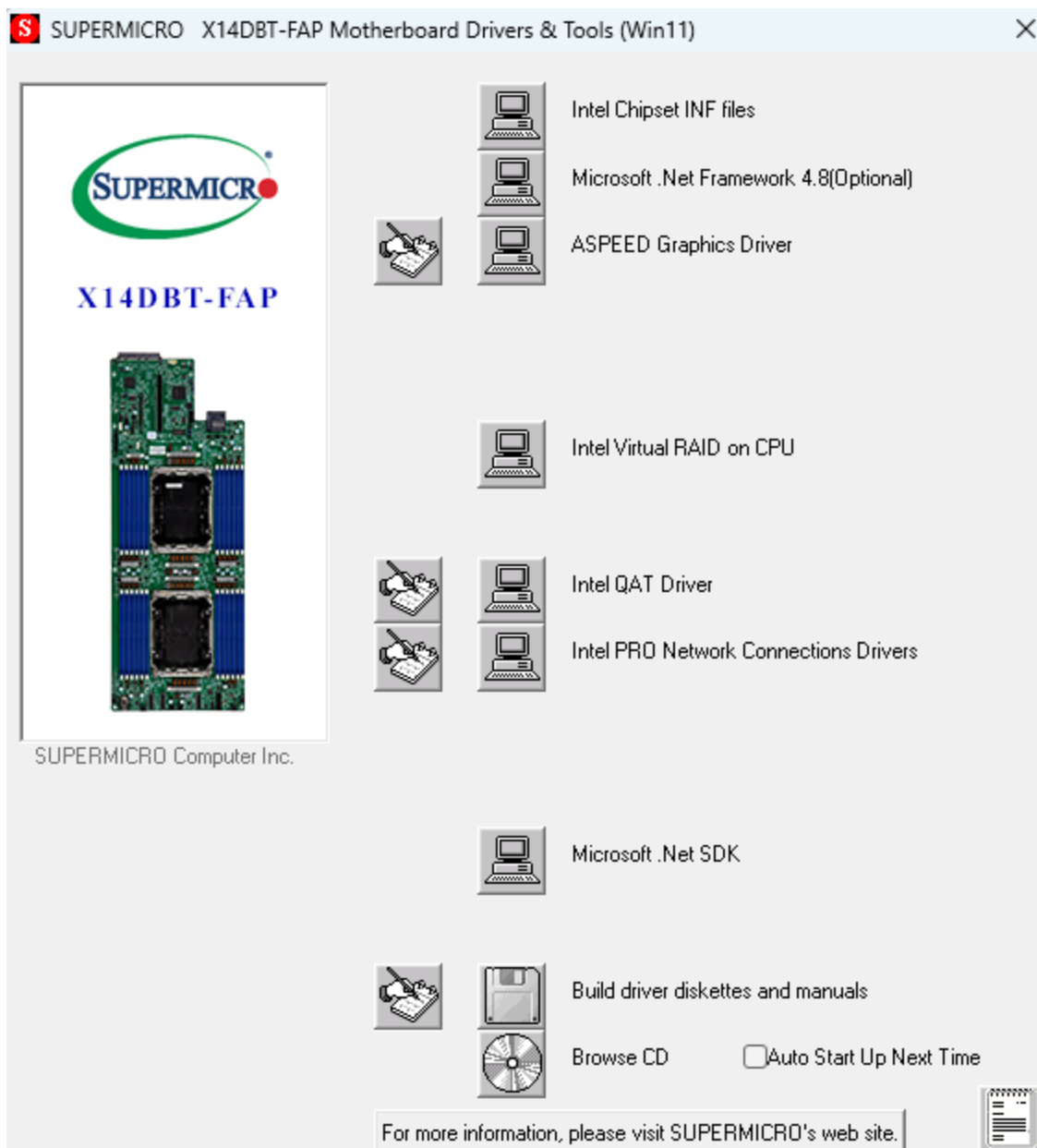


Figure A-3. Driver Installation

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

BMC

The X14DBT-FAP/-FLAP motherboard provides remote access, monitoring, and management through the baseboard management controller (BMC) and other management controllers distributed among different system modules. There are several BIOS settings that are related to BMC. For general documentation and information on BMC, visit our website at the following page:

<https://www.supermicro.com/en/solutions/management-software/bmc-resources>

BMC ADMIN User Password

For security, each system is assigned a unique default BMC password for the ADMIN user. The password can be found on a sticker on the motherboard and a sticker on the chassis, for Supermicro chassis. The sticker also displays the BMC MAC address. If necessary, the password can be reset using the Supermicro IPMICFG tool.



Figure A-4. BMC Password Label

Battery Handling



CAUTION 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.

電池の取り扱い

バッテリーを間違ったタイプに交換すると爆発の危険があります。交換する電池はメーカーが推奨する型、または同等のものを使用下さい。使用済電池は製造元の指示に従って処分して下さい。

警告

如果更换的电池类型不正确。请只使用同类电池或制造商推荐的功能相当的电池更换原有电池。请按制造商的说明处理废旧电池。

警告

如果更換的電池類型不正確。請使用製造商建議之相同或功能相當的電池更換原有電池。請按照製造商的說明指示處理廢棄舊電池。

WARNUNG

Es besteht Explosionsgefahr, wenn die Batterie durch einen falschen Typ ersetzt wird. Ersetzen Sie die Batterie nur durch den gleichen oder vom Hersteller empfohlenen Batterietyp. Entsorgen Sie die benutzten Batterien nach den Anweisungen des Herstellers.

ADVERTENCIA

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

ATTENTION

Il existe un risque d'explosion si la batterie est remplacée par un type incorrect. Ne la remplacer que par une pile de type semblable ou équivalent, recommandée par le fabricant. Jeter les piles usagées conformément aux instructions du fabricant.

אזהרה!

קיימת סכנת פיצוץ אם הסוללה תוחלף בסוג שגוי. יש להחליף את הסוללה בסוג התואם מחברת יצרן מומלצת. סילוק הסוללות המשומשות יש לבצע לפי הוראות היצרן.

.هناك خطر الانفجار إذا تم استبدال البطارية بنوع غير صحيح

استبدال البطارية

فقط بنفس النوع أو ما يعادلها مما أوصت به الشركة المصنعة

جخلص من البطاريات المسحومة وفقاً لتعليمات الشركة الصانعة

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.

WAARSCHUWING

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

Product Disposal

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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

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

경고!

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

Waarschuwing

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