



B11SRE-CPU-TF

USER'S MANUAL

Revision 1.0

The information in this user's manual has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our website at [www.supermicro.com](http://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 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 a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

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



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

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

Manual Revision 1.0

Release Date: August 16, 2019

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

Copyright © 2019 by Super Micro Computer, Inc.  
All rights reserved.

**Printed in the United States of America**

# Preface

## About This Manual

This manual is written for system integrators, IT technicians, and knowledgeable end users. It provides information for the installation and use of the B11SRE-CPU-TF motherboard.

## About This Motherboard

The B11SRE-CPU-TF motherboard supports an Intel® Xeon W in an LGA2066 socket. This motherboard provides maximum performance, supports up to 512GB DDR4 LRDIMM and 256GB DDR4 RDIMM DDR4 memory with speeds of up to 2666MHz, NVMe, two SAS drives, and is optimized for data centers and cloud computing. Please note that this motherboard is intended to be installed and serviced by professional technicians only. For processor and memory updates, please refer to our website at <http://www.supermicro.com/products/>.

## Manual Organization

**Chapter 1** describes the features, specifications and performance of the motherboard, and provides detailed information on the C422 chipset.

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

If you encounter any problems, see **Chapter 3**, which describes troubleshooting procedures for video, memory, and system setup stored in the CMOS.

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

**Appendix A** provides BIOS Error Beep Codes.

**Appendix B** lists software program installation instructions.

**Appendix C** lists standardized warning statements in various languages.

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

## 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](mailto:marketing@supermicro.com) (General Information)  
[support@supermicro.com](mailto:support@supermicro.com) (Technical Support)

Website: [www.supermicro.com](http://www.supermicro.com)

### Europe

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

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

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

Website: [www.supermicro.nl](http://www.supermicro.nl)

### Asia-Pacific

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

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

Email: [support@supermicro.com.tw](mailto:support@supermicro.com.tw)

Website: [www.supermicro.com.tw](http://www.supermicro.com.tw)

---

---

# Table of Contents

## **Chapter 1 Introduction**

1.1 Checklist .....	8
Quick Reference Table .....	11
Motherboard Features .....	12
1.2 Processor and Chipset Overview .....	15
1.3 Special Features .....	15
Recovery from AC Power Loss .....	15
1.4 System Health Monitoring .....	15
Onboard Voltage Monitors .....	15
Fan Status Monitor with Firmware Control .....	16
Environmental Temperature Control .....	16
System Resource Alert .....	16
1.5 ACPI Features .....	16

## **Chapter 2 Installation**

2.1 Static-Sensitive Devices .....	17
Precautions .....	17
Unpacking .....	17
2.2 Processor and Heatsink Installation .....	18
Installing a CPU .....	18
Installing a Passive CPU Heatsink .....	21
Removing the Heatsink .....	22
2.3 Memory Support and Installation .....	23
Memory Support .....	23
General Guidelines for Optimizing Memory Performance .....	24
DIMM Installation .....	25
DIMM Removal .....	25
2.4 Motherboard Installation .....	26
Tools Needed .....	26
Location of Mounting Holes .....	26
Installing the Motherboard into the Mounting Tray .....	27
Installing the Motherboard into the Superblade Chassis .....	28
2.5 Connectors .....	29

2.8 Jumper Settings .....	34
How Jumpers Work.....	34
2.9 LED Indicators.....	39
<b>Chapter 3 Troubleshooting</b>	
3.1 Troubleshooting Procedures .....	40
Before Power On .....	40
No Power .....	40
No Video .....	41
System Boot Failure.....	41
Memory Errors .....	41
Losing the System's Setup Configuration.....	42
When the System Becomes Unstable .....	42
3.2 Technical Support Procedures .....	44
3.3 Frequently Asked Questions .....	45
3.4 Battery Removal and Installation .....	46
Battery Removal.....	46
Proper Battery Disposal .....	46
Battery Installation.....	46
3.5 Returning Merchandise for Service.....	47
<b>Chapter 4 BIOS</b>	
4.1 Introduction.....	48
Starting the Setup Utility .....	48
4.2 Main Setup .....	49
4.3 Advanced.....	51
4.4 Event Logs .....	76
4.5 IPMI .....	78
4.6 Security.....	82
4.7 Boot .....	86
4.8 Save & Exit.....	88

**Appendix A BIOS Codes**

A.1 BIOS Error POST (Beep) Codes .....	90
----------------------------------------	----

**Appendix B Software Installation**

B.1 Installing Software Programs .....	92
----------------------------------------	----

B.2 SuperDoctor® 5.....	93
-------------------------	----

**Appendix C Standardized Warning Statements****Appendix D UEFI BIOS Recovery**

D.1 Overview.....	97
-------------------	----

D.2 Recovering the UEFI BIOS Image.....	97
-----------------------------------------	----

D.3 Recovering the BIOS Block with a USB Device .....	97
-------------------------------------------------------	----

# Chapter 1

## Introduction

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

Please check that the following items have all been included with your motherboard. If anything listed here is damaged or missing, contact your retailer. The following items are included in the retail box:

### 1.1 Checklist

Main Parts List (included in the retail box)		
Description	Part Number	Quantity
Supermicro motherboard	MBD-B11SRE-CPU-TF	1

### Important Links

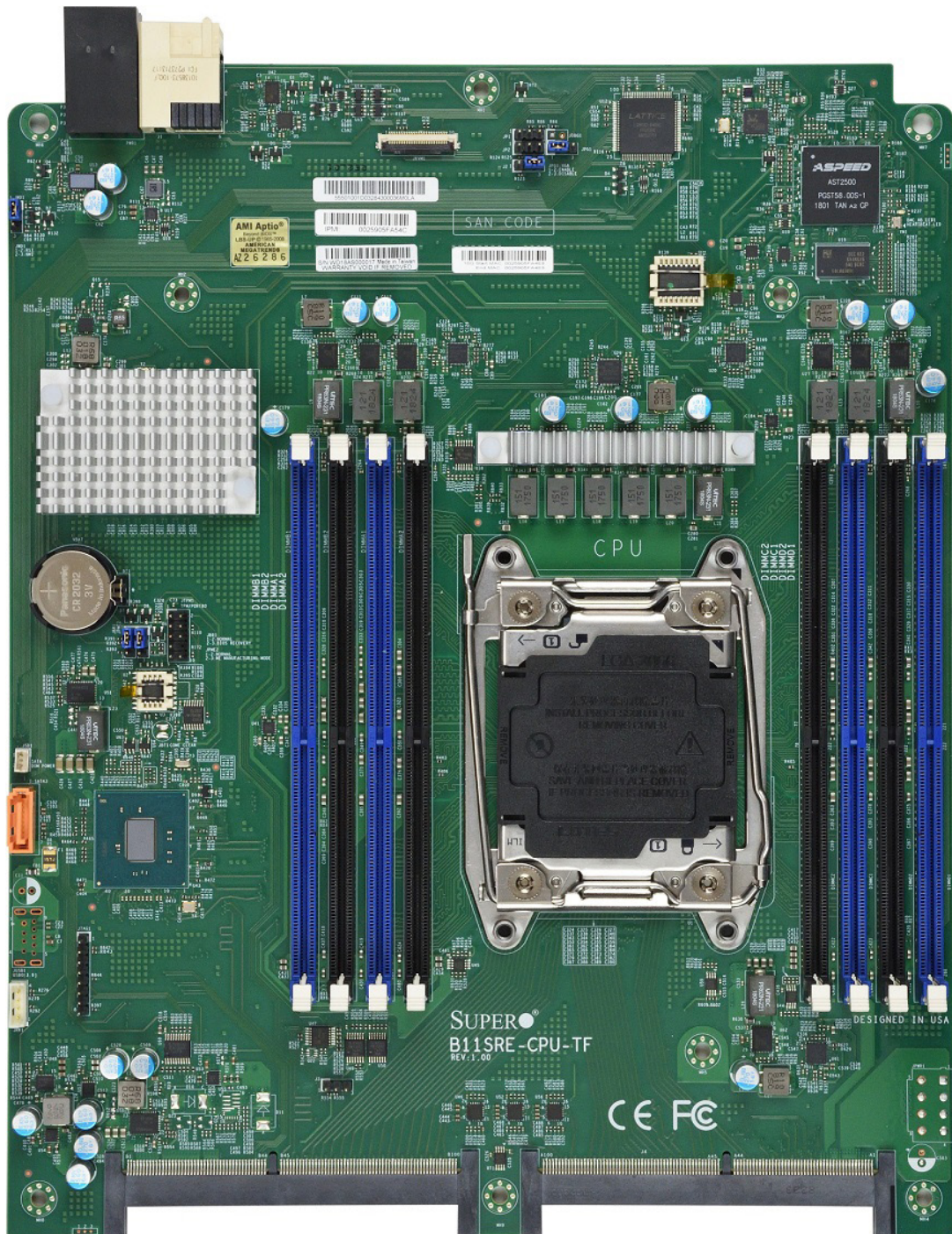
For your system to work properly, please follow the links below to download all necessary drivers/utilities and the user's manual for your server.

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

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

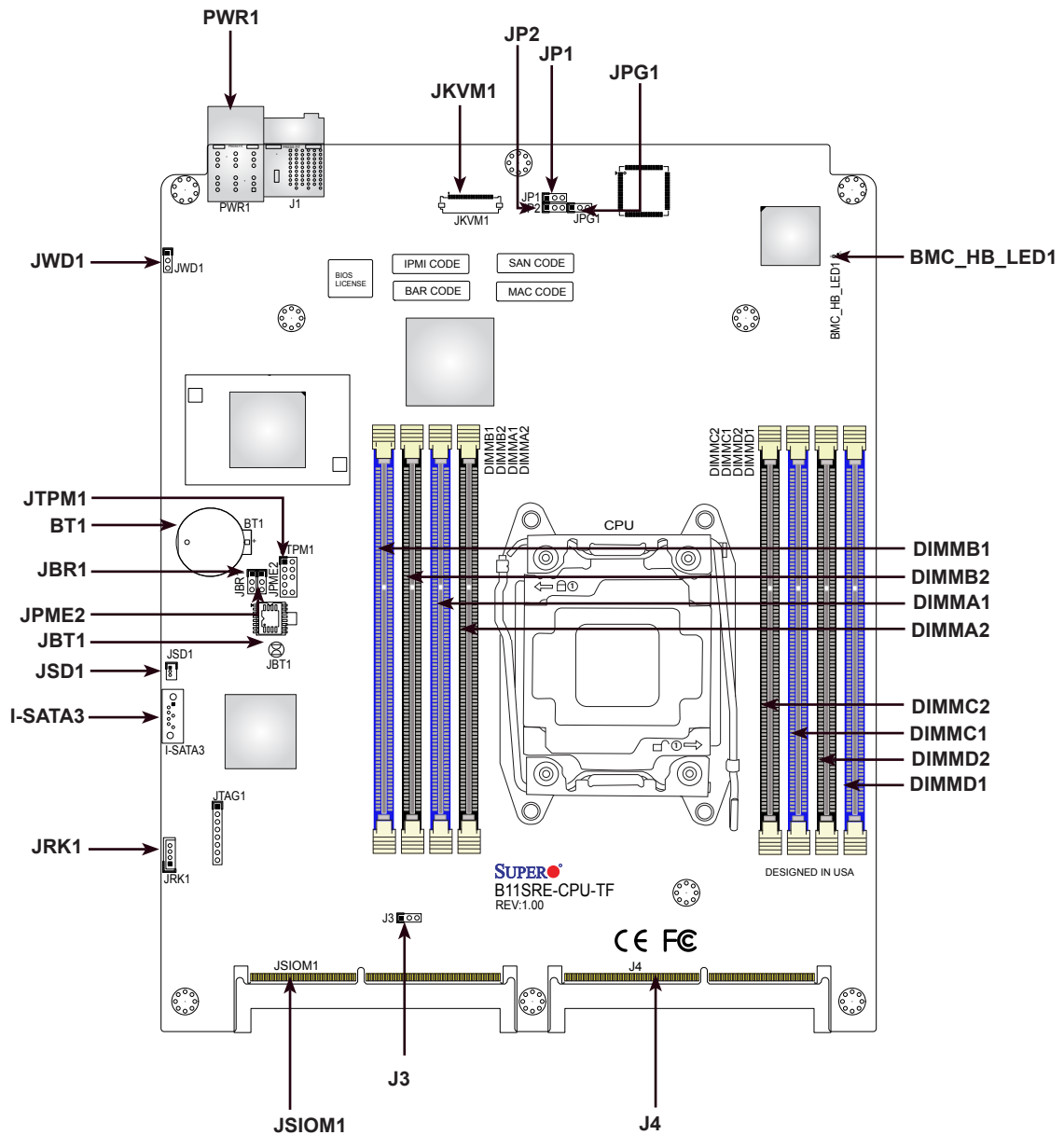


Figure 1-1. Motherboard Image



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

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



**Notes:**

- See Chapter 2 for detailed information on jumpers, and I/O ports. Jumpers/components/ LED indicators not indicated are used for internal testing only.
- "■" indicates the location of Pin 1.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. Do not install the onboard battery upside down to avoid possible explosion.


## Quick Reference Table

Jumper	Description	Default Setting
JBR1	BIOS Recovery	Pins 1-2 (Enable)
JBT1	CMOS Clear	Open (Normal)
JPG1	VGA Enable/Disable	Pins 1-2 (Enabled)
JPME2	Manufacturing Mode	Pins 1-2 (Normal)
JWD1	Watch Dog Timer	Pins 1-2 (Reset)

Connector	Description
BT1	Onboard Battery
I-SATA3	SATA 3.0 Port
J3	VRM Debug Jumper (Manufacturing Use Only)
J4	PCI-E x16 Slot for I/O Expandability
JKVM1	VGA/USB Module Connector
JP1	PLD Header (Manufacturing Use Only)
JP2	PLD Header (Manufacturing Use Only)
JRK1	Intel RAID Key Header
JSD1	SATA DOM Power Header
JTPM1	Trusted Platform Module (TPM)/Port 80 Header
PWR1	Power Receptacle to Chassis Backplane

LED	Description	Status
BMC_HB_LED1	BMC Heartbeat	Blinking Green: BMC Normal


## Motherboard Features

<b>Motherboard Features</b>	
<b>CPU</b>	
<ul style="list-style-type: none"> <li>Supports an Intel Xeon W family processor in an LGA2066 socket.</li> </ul>	
<b>Memory</b>	
<ul style="list-style-type: none"> <li>Supports up to 512GB LRDIMM/256GB RDIMM DDR4 memory with speeds of up to 2666MHz in eight slots.</li> </ul>	
<b>DIMM Size</b>	
<ul style="list-style-type: none"> <li>4GB, 8GB, 16GB, 32GB, and 64GB</li> </ul>	
 <b>Note 1:</b> Refer to the motherboard product page for the list of supported memory.	
<b>Chipset</b>	
<ul style="list-style-type: none"> <li>Intel C422</li> </ul>	
<b>Network Controller</b>	
<ul style="list-style-type: none"> <li>Intel Dual X710 10GbE via Blade Backplane</li> </ul>	
<b>Baseboard Management Controller</b>	
<ul style="list-style-type: none"> <li>Aspeed AST2500</li> </ul>	
<b>Graphics</b>	
<ul style="list-style-type: none"> <li>Graphics controller via ASpeed AST2500</li> </ul>	
<b>I/O Devices</b>	
<ul style="list-style-type: none"> <li>SATA 3.0</li> <li>AOM-BPNIO-SCE (connected via J4)</li> <li>AOM-BPNIO-SNE (connected via J4)</li> </ul>	<ul style="list-style-type: none"> <li>One SATA 3.0 port</li> <li>2x 2.5" NVMe + 1x SAS3/SATA3 or 3x SAS3/SATA3</li> <li>3x 2.5" NVMe or 3x SATA3</li> </ul>
<b>Peripheral Devices</b>	
<ul style="list-style-type: none"> <li>Two (2) USB 2.0 ports via JKVM1 header (debug only)</li> </ul>	
<b>BIOS</b>	
<ul style="list-style-type: none"> <li>256Mb SPI AMI BIOS® SM Flash UEFI BIOS</li> <li>ACPI 6.2, SMBIOS 2.8/3.2, UEFI 2.7 specification, PCI F/W 3.1, Plug and Play (PnP), RTC wake up</li> </ul>	



**Note:** The table above is continued on the next page.

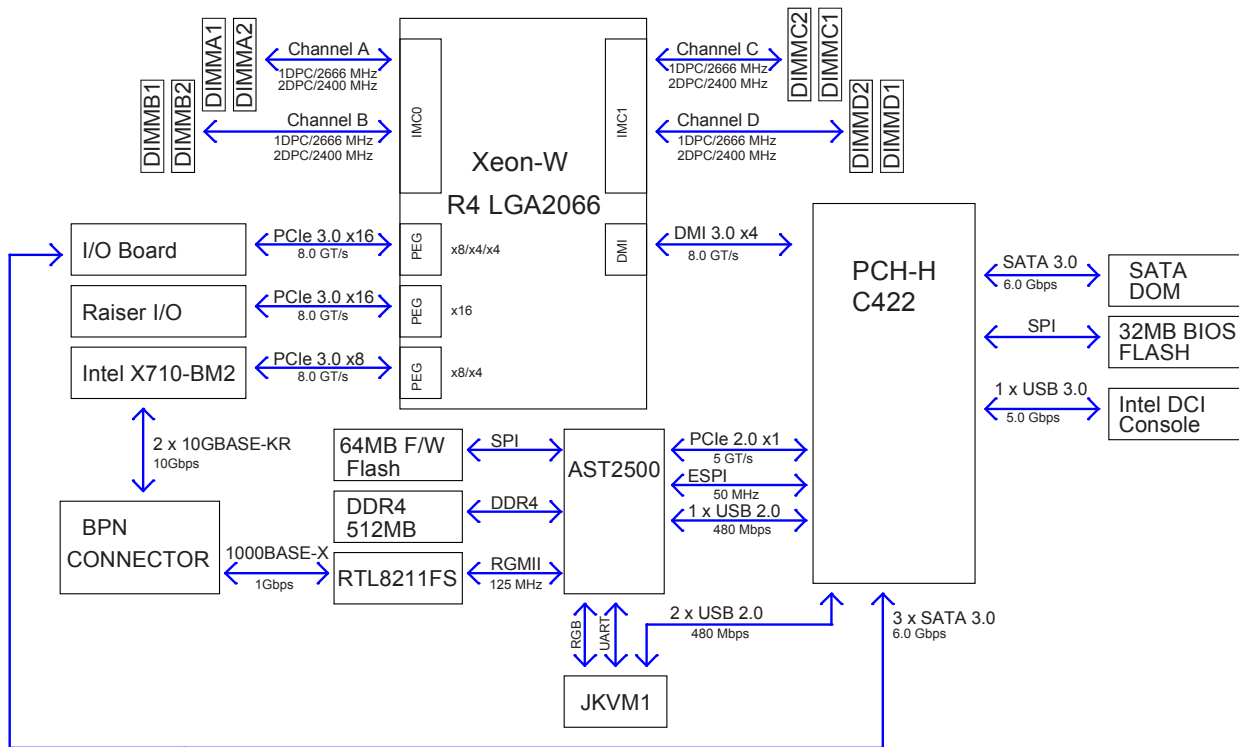
<b>Motherboard Features</b>	
<b>Power Management</b>	
<ul style="list-style-type: none"> <li>• Power button override mechanism</li> <li>• Management Engine (ME)</li> <li>• Power-on mode for AC recovery</li> </ul>	
<b>System Health Monitoring</b>	
<ul style="list-style-type: none"> <li>• Onboard voltage monitoring for +1.8V, +3.3V, +3.3V Stdby, +5V, +5V Stdby, +12V, VBAT, HT, Memory</li> <li>• 6+2 CPU switching phase voltage regulator</li> <li>• CPU Thermal Trip support</li> </ul>	
<b>System Management</b>	
<ul style="list-style-type: none"> <li>• Trusted Platform Module (TPM) support</li> <li>• PECI (Platform Environment Control Interface) 2.0 support</li> <li>• IPMI 2.0</li> <li>• Watch Dog, NMI</li> </ul>	
<b>LED Indicators</b>	
<ul style="list-style-type: none"> <li>• CPU/System Overheat LED</li> <li>• Power/Suspend State Indicator LED</li> <li>• Fan Fail LED</li> <li>• UID/Remote LED</li> <li>• LAN Activity LED</li> </ul>	
<b>Dimensions</b>	
<ul style="list-style-type: none"> <li>• 9.36" (W) x 11.61" (L) (237.74 mm x 294.89 mm)</li> </ul>	


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

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

**Note 3:** If you purchase a Supermicro Out of Band (OOB) software license key (Supermicro P/N: SFT-OOB-LIC), please DO NOT change the IPMI MAC address. Once the Mac address has been changed, the OOB license key will be invalid.

**Figure 1-3.**  
**B11SRE-CPU-TF System Block Diagram**



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

## 1.2 Processor and Chipset Overview

The Supermicro B11SRE-CPU-TF motherboard, using the C422 chipset, supports Intel Xeon W processors and provides superb performance, efficient power management, all the while providing a rich feature set based on cutting edge technology to address today's needs in advanced computing, engineering simulation, automation, etc.

The Intel Xeon W processor and the C422 chipset support the following features:

- Intel Hyper-Threading, Intel VT-D, VT-x
- Intel Turbo Boost Technology
- Intel Rapid Storage Technology
- 64GB DDR4 Load Reduced RDIMM memory support with speeds of up to 2666MHz
- ACPI Power Management

## 1.3 Special Features

This section describes the health monitoring features of the B11SRE-CPU-TF motherboard. The motherboard has an onboard System Hardware Monitor chip that supports system health monitoring.

### Recovery from AC Power Loss

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

## 1.4 System Health Monitoring

### Onboard Voltage Monitors

The onboard voltage monitor will continuously scan crucial voltage levels. Once a voltage becomes unstable, it will give a warning or send an error message to the screen. The user can adjust the voltage thresholds to define the sensitivity of the voltage monitor. Real time readings of these voltage levels are all displayed in BIOS.

## Fan Status Monitor with Firmware Control

The system health monitor chip can check the RPM status of a cooling fan. The CPU and chassis fans are controlled by the BIOS Thermal Management.

## Environmental Temperature Control

The thermal control sensor monitors the CPU temperature in real time and will turn on the thermal control fan whenever the CPU temperature exceeds a user-defined threshold. The overheat circuitry runs independently from the CPU. Once the thermal sensor detects that the CPU temperature is too high, it will automatically turn on the thermal fans to prevent the CPU from overheating. The onboard chassis thermal circuitry can monitor the overall system temperature and alert the user when the chassis temperature is too high.



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

## System Resource Alert

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

## 1.5 ACPI Features

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

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play and an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures while providing a processor architecture-independent implementation that is compatible with Windows® 10 operating system.



# Chapter 2

## Installation

### 2.1 Static-Sensitive Devices

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

#### Precautions

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

#### Unpacking

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

## 2.2 Processor and Heatsink Installation

**Warning:** When handling the processor package, avoid placing direct pressure on the label area of the fan.



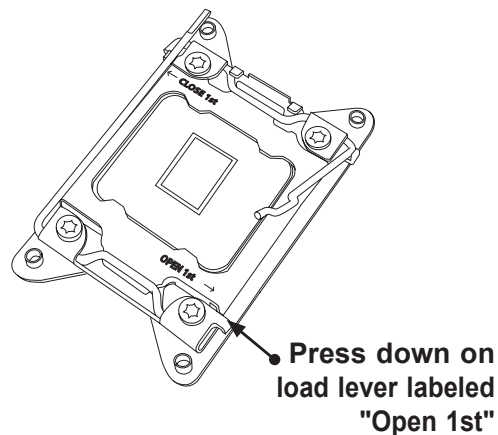
### Important:

- Always connect the power cord last, and always remove it before adding, removing or changing any hardware components. Make sure that you install the processor into the CPU socket before you install the CPU heatsink.
- If you buy a CPU separately, make sure that you use an Intel-certified multi-directional heatsink only.
- Make sure to install the motherboard into the chassis before you install the CPU heatsink.
- When receiving a motherboard without a processor pre-installed, make sure that the plastic CPU socket cap is in place and none of the socket pins are bent; otherwise, contact your retailer immediately.
- Refer to the Supermicro website for updates on CPU support.

### Installing a CPU

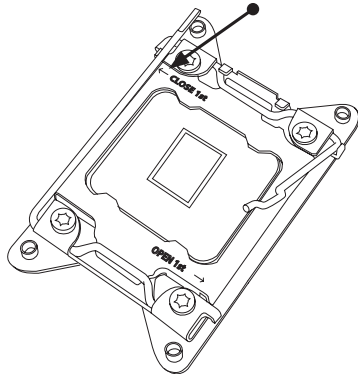
1. There are two load levers on the LGA 2066 socket. To open the socket cover, press and release the load lever labeled "Open 1st".

1

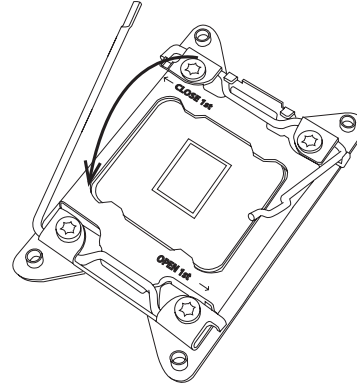


2. Press the second load lever labeled "Close 1st" to release the load plate that covers the CPU socket from its locking position.

**1** Press down on load lever  
"Close 1st"

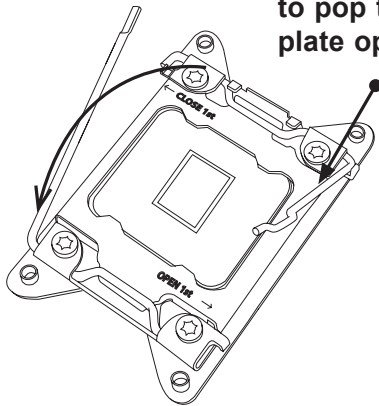


**2** Pull lever away from  
socket

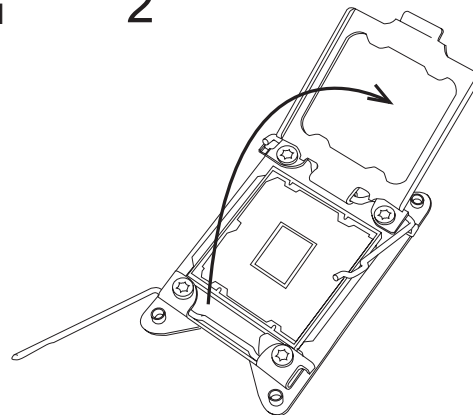


3. With the "Close 1st" lever fully retracted, gently push down on the "Open 1st" lever to open the load plate. Lift the load plate to open it completely.

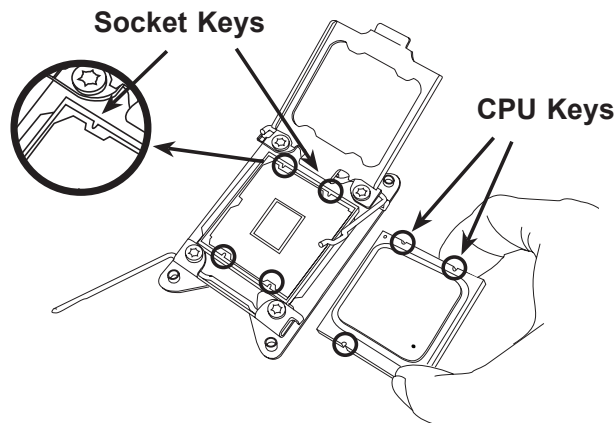
**1** Gently push down  
to pop the load  
plate open



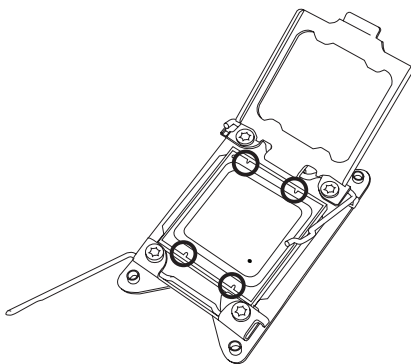
**2**



4. Use your thumb and index finger to hold the CPU by its edges. Align the CPU keys, which are semi-circle cutouts, against the socket keys.

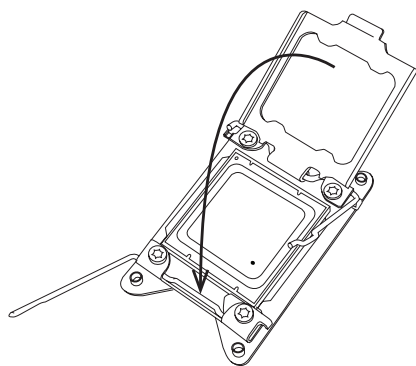


5. Once they are aligned, carefully lower the CPU straight down into the socket. To avoid damaging the CPU or socket, do not drop the CPU onto the socket, move it horizontally or vertically, or rub it against the socket pins. Note that you can only install the CPU inside the socket in one direction.
6. With the CPU inside the socket, inspect the four corners of the CPU to make sure that it is properly installed.

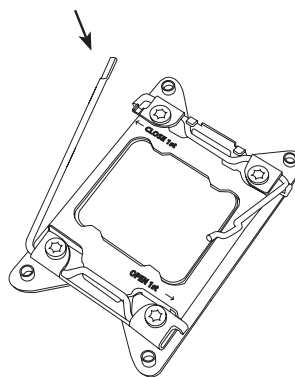


7. Close the load plate with the CPU inside the socket. Lock the "Close 1st" lever first, then lock the "Open 1st" lever second. Gently push the load levers down to the lever locks.

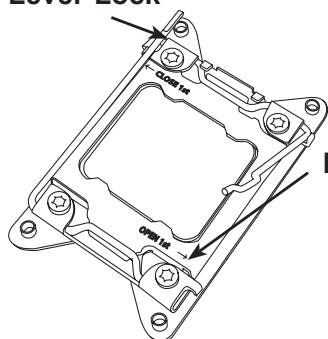
**1 Gently close the load plate**



**2 Push down and lock the lever labeled "Close 1st"**

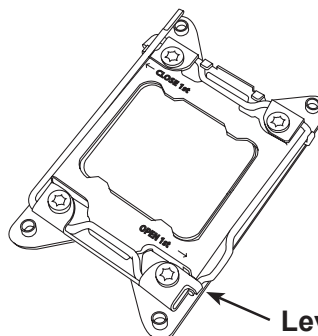


**3 Lever Lock**



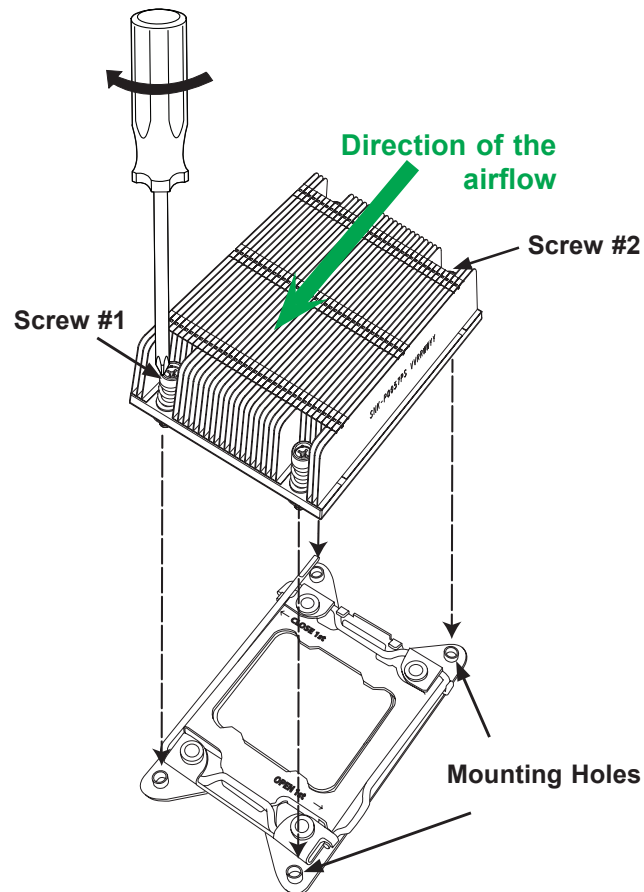
**Push down and lock the lever labeled "Open 1st"**

**4**



## Installing a Passive CPU Heatsink

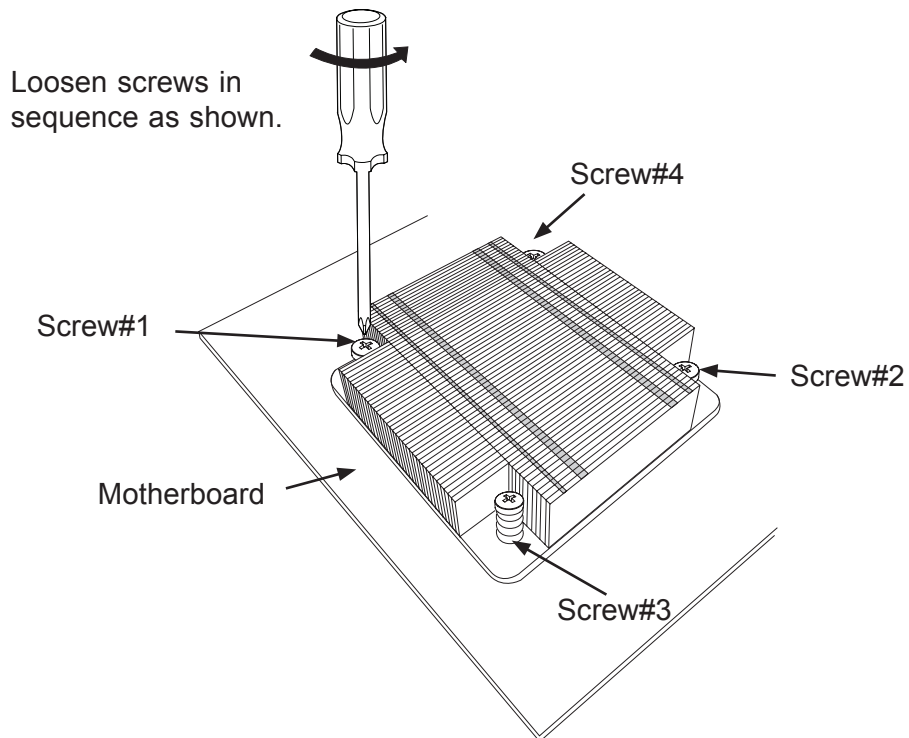
1. Do not apply any thermal grease to the heatsink or the CPU die -- the required amount has already been applied.
2. Place the heatsink on top of the CPU so that the four mounting holes are aligned with those on the motherboard and the heatsink bracket underneath.
3. Screw in two diagonal screws (e.g., the #1 and the #2 screws) until just snug. Do not over-tighten the screws to avoid damaging the CPU and the motherboard.
4. Finish the installation by fully tightening all four screws.



## Removing the Heatsink

**Warning:** We do not recommend that the CPU or the heatsink be removed. However, if you do need to uninstall the CPU or the heatsink, please follow the instructions below to uninstall the heatsink to avoid damaging the CPU or other components.

1. Unscrew the heatsink screws from the motherboard in the sequence as shown in the illustration below.
2. Gently wriggle the heatsink to loosen it from the CPU. Do not use excessive force when loosening the heatsink.
3. Once the heatsink is loosened from the socket, remove the heatsink from the CPU socket. Next, remove the CPU from the socket if needed.
4. Remove the used thermal grease and clean the surface of the CPU and the heatsink. Reapply the proper amount of thermal grease on the surface before reinstalling the CPU and the heatsink.



## 2.3 Memory Support and Installation



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

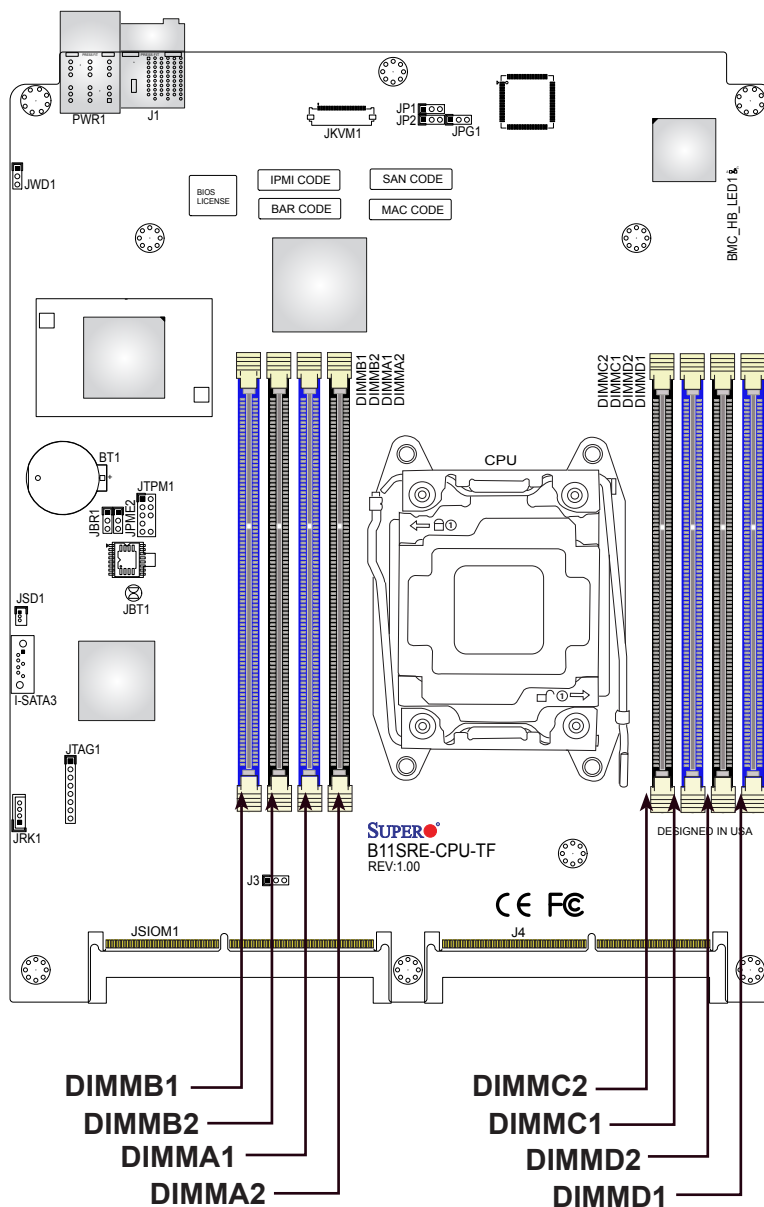
### Memory Support

The B11SRE-CPU-TF motherboard supports up to 512GB of LRDIMM or 256GB of RDIMM DDR4 memory with speeds of up to 2666MHz in eight slots. Populating the DIMM slots with a pair of memory modules of the same type, speed, and size will result in interleaved memory, which improves performance. See the table below for the recommended DIMM population order.

1 CPU, 8 DIMM Slots	
Number of DIMMs	Memory Population Sequence
1	DIMMA1
2	DIMMA1 / DIMMB1
3	DIMMA1 / DIMMB1 / DIMMC1
4	DIMMA1 / DIMMB1 / DIMMC1 / DIMMD1
5	DIMMA1 / DIMMB1 / DIMMC1 / DIMMD1 / DIMMA2
6	DIMMA1 / DIMMB1 / DIMMC1 / DIMMD1 / DIMMA2 / DIMMB2
7	DIMMA1 / DIMMB1 / DIMMC1 / DIMMD1 / DIMMA2 / DIMMB2 / DIMMC2
8	DIMMA1 / DIMMB1 / DIMMC1 / DIMMD1 / DIMMA2 / DIMMB2 / DIMMC2 / DIMMD2

## General Guidelines for Optimizing Memory Performance

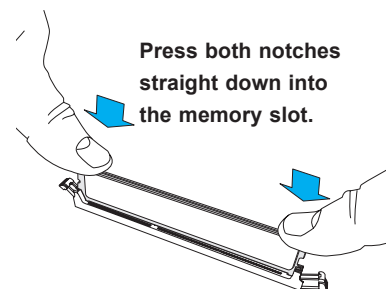
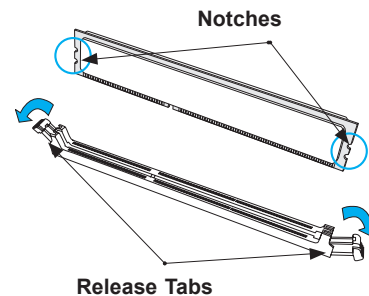
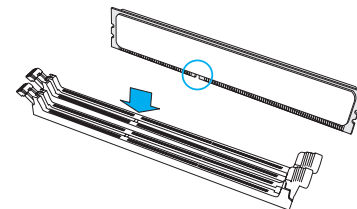
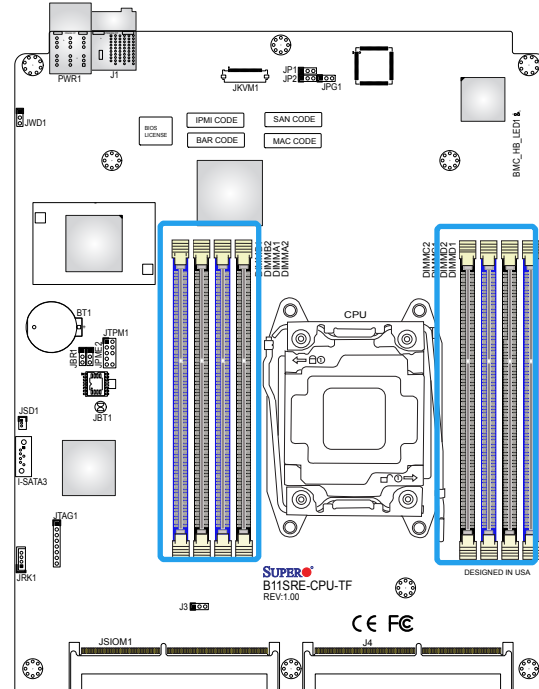
- The blue slots must be populated first.
- Always use DDR4 memory of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- The motherboard will support odd-numbered modules (one or three modules installed). However, to achieve the best memory performance, a balanced memory population is recommended.





## DIMM Installation

1. Insert the desired number of DIMM modules into the memory slots based on the recommended DIMM population table on page 24.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.
3. Align the key of the DIMM module with the receptive point on the memory slot.
4. Align the notches on both ends of the module against the receptive points on the ends of the slot.
5. 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 module into the slot.



## DIMM Removal

Reverse the steps above to remove the DIMM modules from the motherboard.

## 2.4 Motherboard Installation

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



Phillips Screwdriver (1)

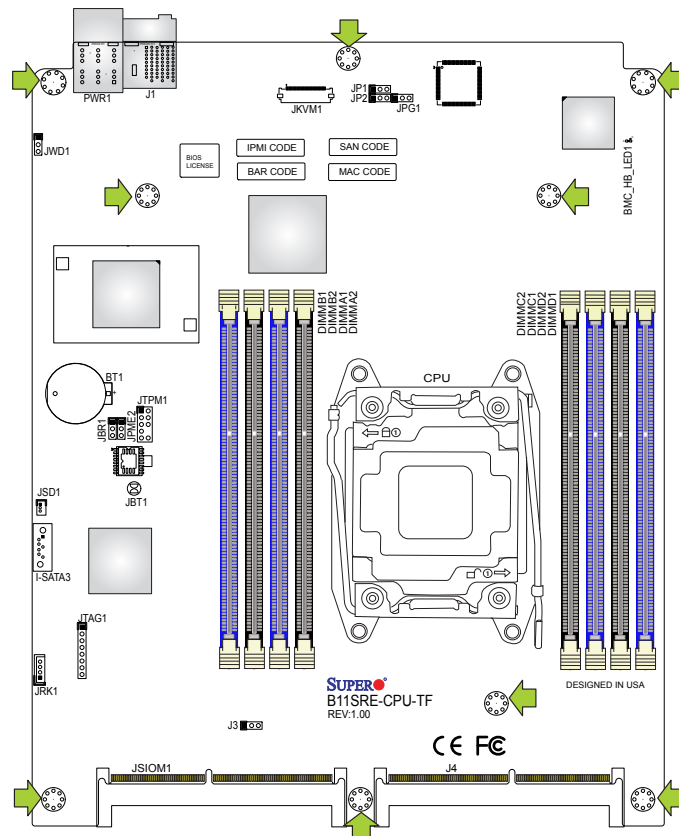


Phillips Screws (9)



Standoffs (9)  
Only if Needed

### Tools Needed



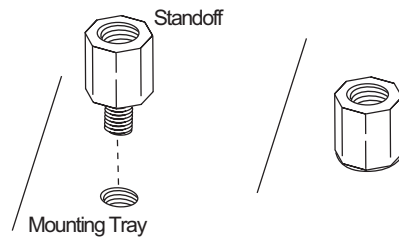
### Location of Mounting Holes



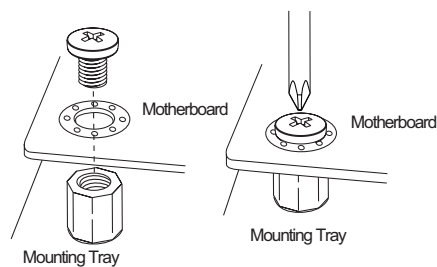
- Notes:**
- 1) To avoid damaging the motherboard and its components, please do not use a force greater than 8 lb/inch on each mounting screw during motherboard installation.
  - 2) Some components are very close to the mounting holes. Please take precautionary measures to avoid damaging these components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

## Installing the Motherboard into the Mounting Tray

1. Locate the mounting holes on the motherboard and the mounting tray. Refer to the previous page for the mounting holes.
2. Install the standoffs on the mounting tray. Align the mounting holes on the motherboard against the mounting holes on the tray.



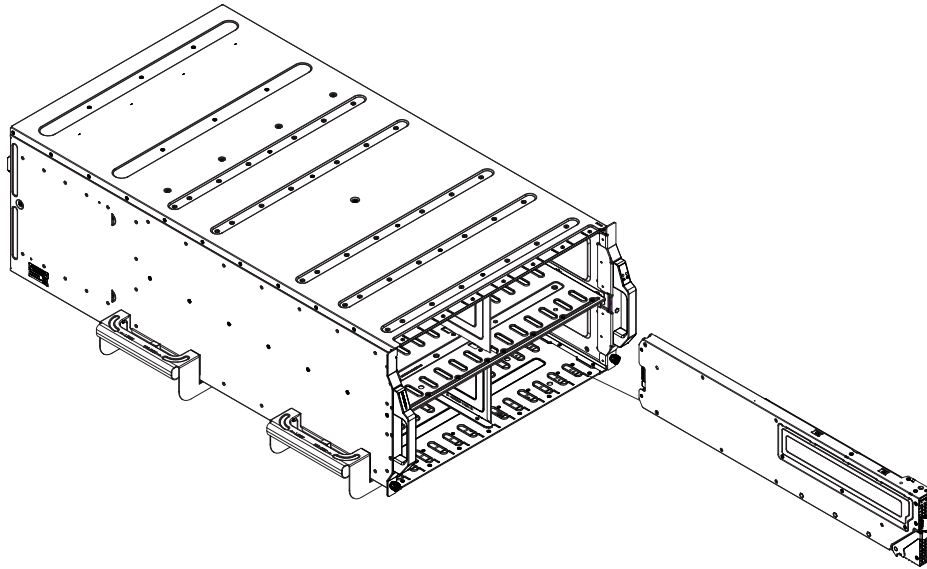
3. Using the Phillips screwdriver, insert a Phillips head #6 screw into a mounting hole on the motherboard and its matching hole on the tray.




4. Repeat step 2 to insert #6 screws to all mounting holes located on the motherboard and tray and securely install the motherboard onto the tray.

## Installing the Motherboard into the Superblade Chassis

1. When the motherboard is securely installed on the mounting tray, push the tray into the Superblade chassis shown below.



2. Once the mounting tray is pushed into the chassis, the connectors on the motherboard's edge will make contact with the chassis' backplane, which provides the connections to the chassis power, network, and other I/O devices.

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

## 2.5 Connectors

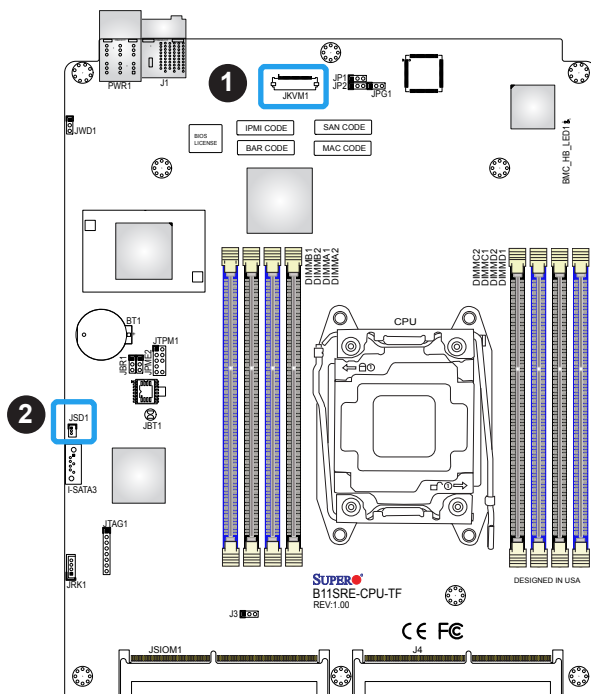
### KVM Connector

The JKVM1 connector supports a keyboard, mouse, and VGA connection. Attach a compatible KVM connector/switch to this port.

### Disk On Module Power Connector

The Disk On Module (DOM) power connector at JSD1 provides 5V power to a solid-state DOM storage device connected to the I-SATA0 port. Refer to the table below for pin definitions.

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



1. KVM Connector
2. SATA DOM Power

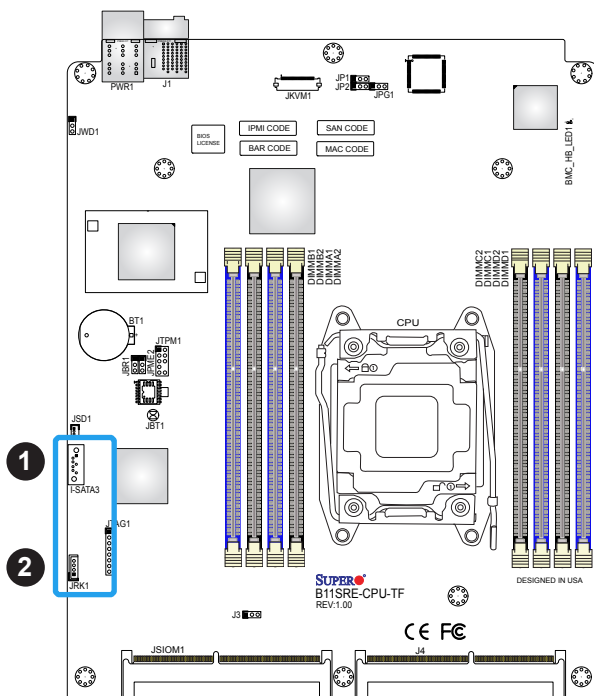
### SATA 3.0 Port

The B11SRE-CPU-TF has one I-SATA 3.0 port (I-SATA3). The port can be used with Supermicro SuperDOMs that are yellow SATA DOM connectors with power pins built in, and do not require external power cables. Supermicro SuperDOMs are backward compatible with regular SATA HDDs or SATA DOMs that need external power cables. All these SATA ports provide serial-link signal connections, which are faster than the connections of Parallel ATA.

### Intel RAID Key Header

The JRK1 header allows the user to enable RAID functions. Refer to the table below for pin definitions.

Intel RAID Key Pin Definitions	
Pins	Definition
1	GND
2	PU 3.3V Stdby
3	GND
4	PCH RAID KEY

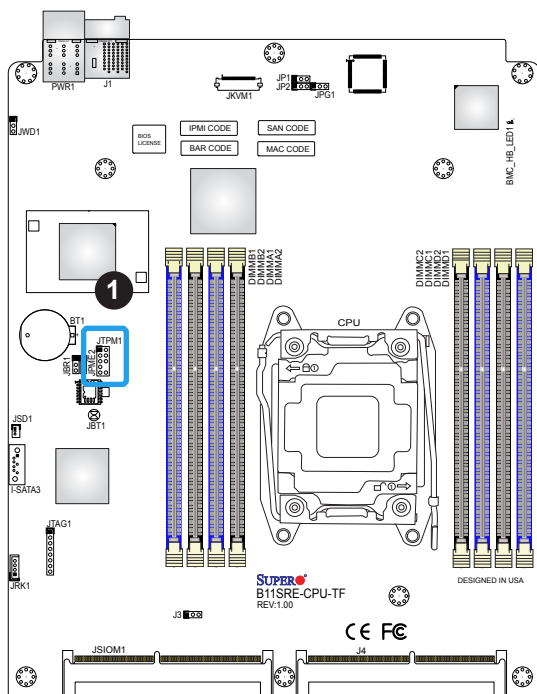


1. I-SATA1
2. RAID Key Header

## TPM Header

The JTPM1 header is used to connect a Trusted Platform Module (TPM)/Port 80, which is available from a third-party vendor. A TPM/Port 80 connector is a security device that supports encryption and authentication in hard drives. It allows the motherboard to deny access if the TPM associated with the hard drive is not installed in the system.

Trusted Platform Module Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	+3.3V	2	SPI_CS#
3	RESET#	4	SPI_MISO
5	SPI_CLK	6	GND
7	SPI_MOSI	8	
9	+3.3V Stby	10	SPI_IRQ#



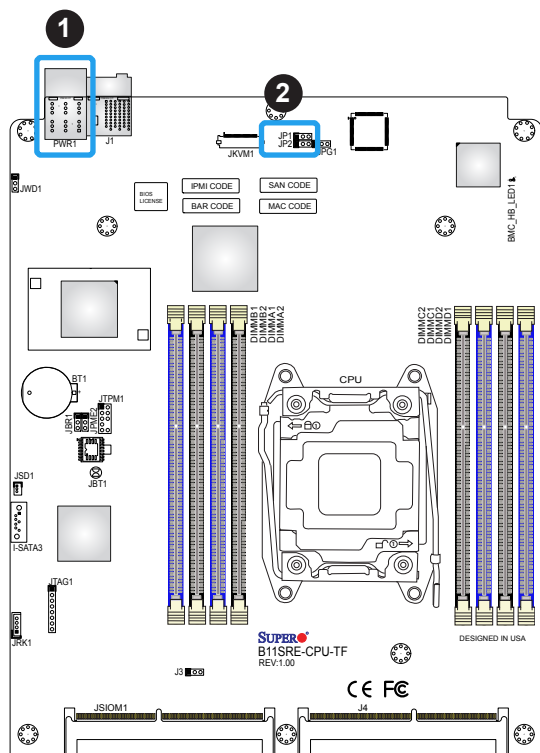
### 1. TPM

### Main Power Connector

The primary power supply connector (PWR1) provides power to the motherboard via the chassis backplane.

### PLD Header

JP1 and JP2 are PLD header for manufacturing use only.



- 1. PWR1
- 2. PLD Headers



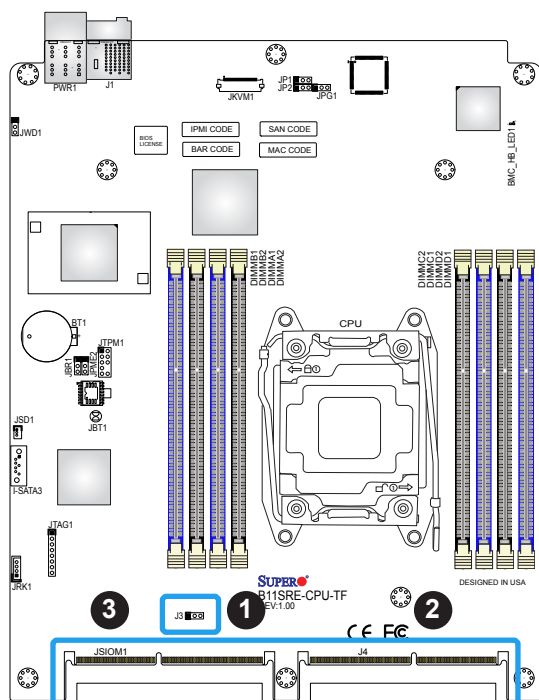
## VRM SMBus Management Header

J3 is a header for VRM SMBus management for manufacturing use only.

## I/O Board Connector

J4 is a header for Supermicro PCI-E storage I/O expansion. Pair with the bridge board (AOM-BPNIO-BRGE), customer can install either the PN: AOM-BPNIO-SCE for NVMe/SAS3/SATA3 or PN: AOM-BPNIO-SNE for NVMe/SATA3 drive connections in a Superblade node.

JSIOM1 is a header reserved for PCI-E x16 I/O expandability.




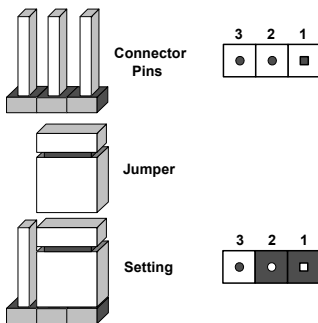
1. VRM SMBus Header
2. I/O Board Connector
3. JSIOM1

## 2.8 Jumper Settings

### How Jumpers Work

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

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



## CMOS Clear

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

### To Clear CMOS

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

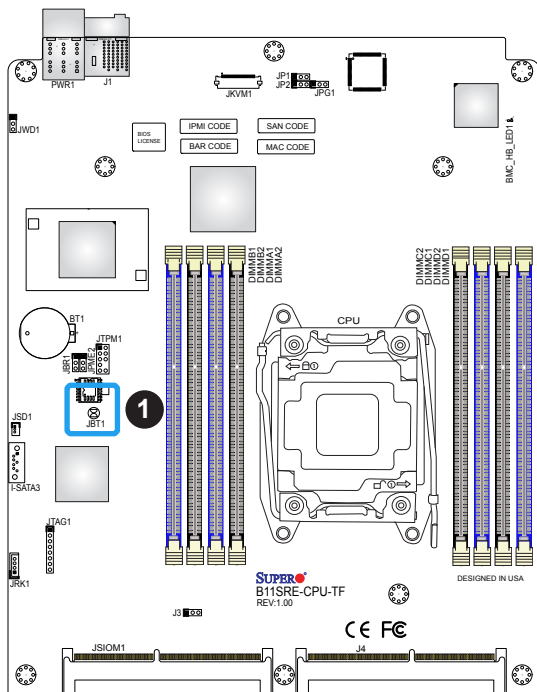


**Note:** Clearing CMOS will also clear all passwords.



JBT1 contact pads

### 1. Clear CMOS



## BIOS Recovery

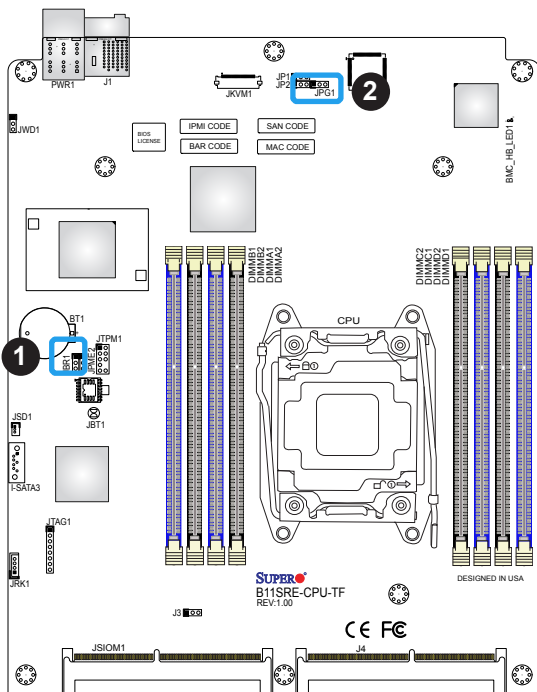
Close pins 2-3 of jumper JBR1 for BIOS recovery. The default setting is on pins 1 and 2 for normal operation. Refer to the table below for jumper settings. The default setting is Normal.

BIOS Recovery Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Normal
Pins 2-3	BIOS Recovery

## VGA Enable/Disable

Use jumper JPG1 to enable or disable the VGA port using the onboard graphics controller. The default setting is Enabled.

VGA Enable/Disable Jumper Settings	
Jumper Setting	Definition
Pins 1-2	Enabled
Pins 2-3	Disabled

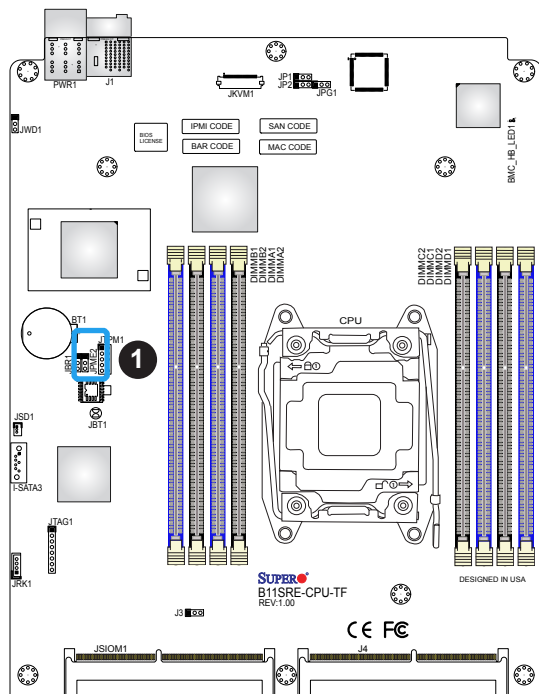


1. BIOS Recovery
2. VGA Enable/Disable

## ME Manufacturing Mode

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


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



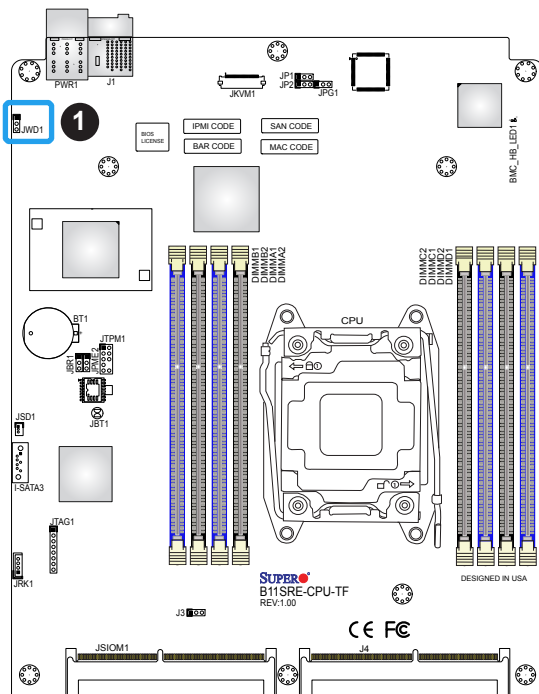
### 1. ME Manufacturing Mode

## Watch Dog

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

 **Note:** When Watch Dog is enabled, users need to write their own application software to disable it.

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



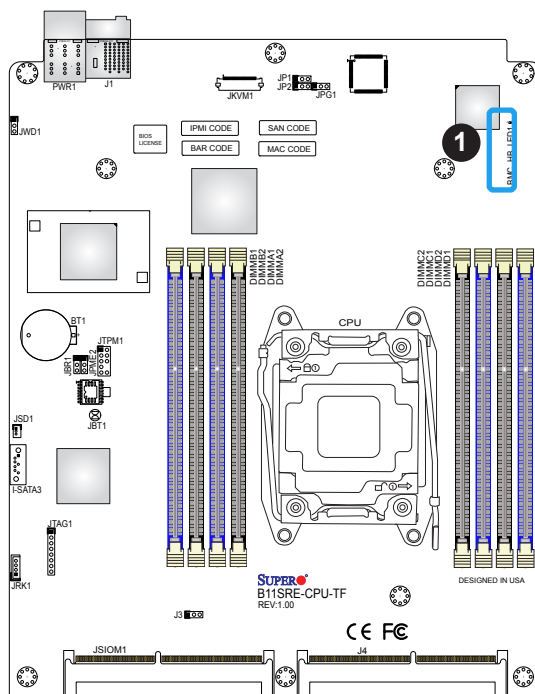
### 1. Watch Dog Timer

## 2.9 LED Indicators

### BMC Heartbeat LED

BMC\_HB\_LED1 is the BMC heartbeat LED. When the LED is blinking green, BMC is functioning normally.

BMC LED Indicator	
LED Color	Definition
Blinking Green	BMC Normal



### 1. BMC LED

# Chapter 3

## Troubleshooting

### 3.1 Troubleshooting Procedures

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

#### **Before Power On**

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

#### **No Power**

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



## No Video

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

## System Boot Failure

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

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

## Memory Errors

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

## Losing the System's Setup Configuration

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

## When the System Becomes Unstable

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

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



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

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

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

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

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

## 3.2 Technical Support Procedures

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

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

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

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

### 3.3 Frequently Asked Questions

**Question: What type of memory does my motherboard support?**

**Answer:** The B11SRE-CPU-TF supports up to 512GB ECC LRDIMM and 256GB ECC RDIMM DDR4 memory with speeds of up to 2666MHz in eight slots.

**Question: How do I update my BIOS?**

**Answer:** It is recommended that you **do not** upgrade your BIOS if you are not experiencing any problems with your system. Updated BIOS files are located on our website at [http://www.supermicro.com/ResourceApps/BIOS\\_IPMI\\_Intel.html](http://www.supermicro.com/ResourceApps/BIOS_IPMI_Intel.html). Please check our BIOS warning message and the information on how to update your BIOS on our website. Select your motherboard model and download the BIOS file to your computer. Also, check the current BIOS revision to make sure that it is newer than your BIOS before downloading. Please unzip the BIOS file onto a USB stick. (Note: The USB stick doesn't have to be bootable, but has to be formatted with the FAT/FAT32 file system.) Plug the USB stick into any USB port, boot to the Build-In UEFI Shell, select the item in the boot menu by pressing F11 key during boot up, and type FLASH.nsh BIOSname#.### to start the BIOS update. After the message indicating BIOS update has completed, perform an A/C power cycle.

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

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

## 3.4 Battery Removal and Installation

### Battery Removal

To remove the onboard battery, follow the steps below:

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

### Proper Battery Disposal

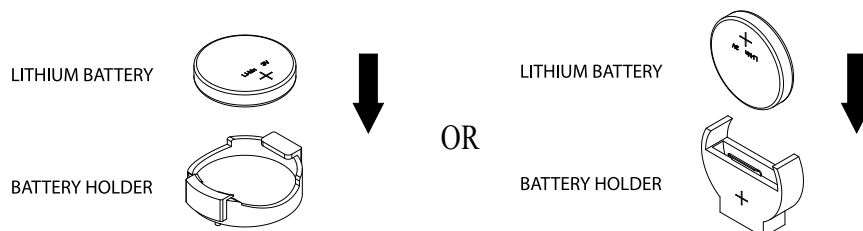
Please handle used batteries carefully. Do not damage the battery in any way; a damaged battery may release hazardous materials into the environment. Do not discard a used battery in the garbage or a public landfill. Please comply with the regulations set up by your local hazardous waste management agency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

### Battery Installation

1. To install an onboard battery, follow the steps 1 and 2 above and continue below:
2. Identify the battery's polarity. The positive (+) side should be facing up.
3. Insert the battery into the battery holder and push it down until you hear a click to ensure that the battery is securely locked.



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



### 3.5 Returning Merchandise for Service

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

For faster service, RMA authorizations may be requested online at <http://www.supermicro.com/RmaForm/>.

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

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

## Chapter 4

# UEFI BIOS

### 4.1 Introduction

This chapter describes the AMIBIOS™ Setup utility for the B11SRE motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.



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

#### Starting the Setup Utility

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

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

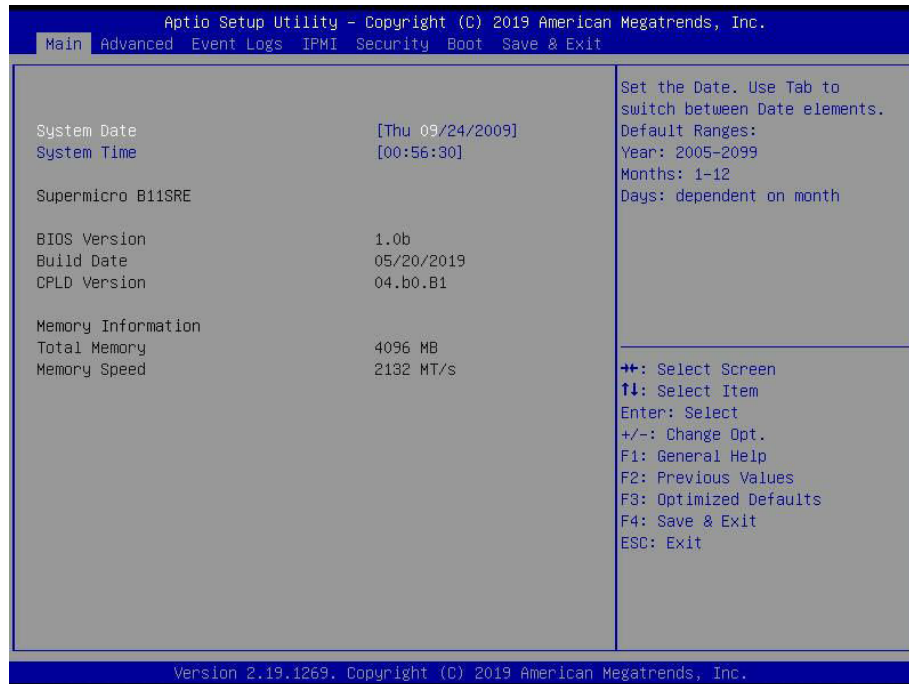
A " ►" indicates a submenu. Highlighting such an item and pressing the <Enter> key will open the list of settings within that submenu.

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




## 4.2 Main Setup

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



### System Date/System Time

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

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

### Supermicro B11SRE

#### BIOS Version

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

#### Build Date

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

## **Memory Information**

### **Total Memory**

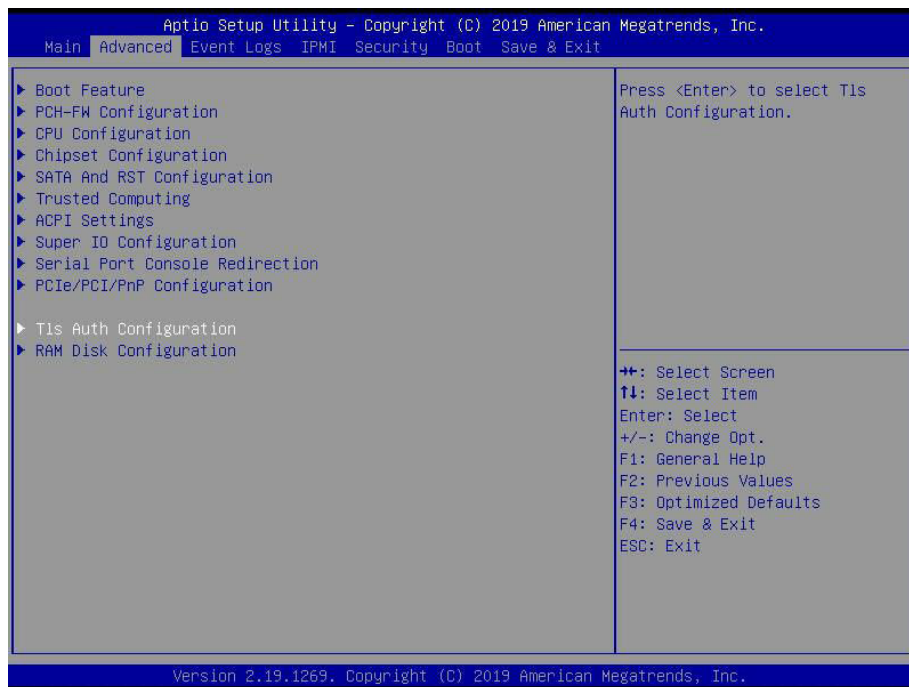
This feature displays the total size of memory available in the system.

### **Memory Speed**

This feature displays

## 4.3 Advanced

Use this menu to configure advanced settings.



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

### ► Boot Feature

#### Fast Boot

Enable this feature to reduce the time it takes to boot the system. A minimal set of devices will be initialized during boot up. The options are **Disabled** and **Enabled**.

#### Quiet Boot

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

#### Bootup NumLock State

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

#### Option ROM Messages

Use this feature to set the display mode for the Option ROM. The options are **Force BIOS** and **Keep Current**.

### **INT19 (Interrupt 19) Trap Response**

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

### **Port 61h Bit-4 Emulation**

Select Enabled to enable the emulation of Port 61h bit-4 toggling in SMM (System Management Mode). The options are **Disabled** and Enabled.

### **Wait For "F1" If Error**

This feature forces 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 enabled, the BIOS will automatically reboot the system from a specified boot device after its initial boot failure. The options are **Disabled**, and Legacy Boot, and EFI Boot.

### **Power Configuration**

#### **Watch Dog Function**

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

#### **Power Button Function**

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

#### **Restore on AC Power Loss**

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

## **►PCH-FW Configuration**

The following firmware information will display:

- ME Firmware Version
- ME Firmware Mode

- ME Firmware SKU
- ME File System Integrity Value
- ME Firmware Status 1
- ME Firmware Status 2

### **ME FW Image Re-Flash**

Use this feature to update the Management Engine firmware. The options are **Disabled** and **Enabled**.

### **►CPU Configuration**

The following CPU information will display:

- Processor BSP Revision
- Processor ID
- Processor Frequency
- Processor Max Ratio
- Processor Min Ratio
- Microcode Revision
- L1 Cache RAM
- L2 Cache RAM
- L3 Cache RAM
- Processor 0 Version

### **Hyper-Threading (ALL)**

Select **Enabled** to support Intel Hyper-threading Technology to enhance CPU performance. The options are **Disable** and **Enable**.

### **Max CPUID Value Limit**

Use this feature to set the maximum CPU ID value. Enable this feature to boot the legacy operating systems that cannot support processors with extended CPUID functions. The options are **Enable** and **Disable** (for the Windows OS).

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

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

### **Intel (VMX) Virtualization Technology**

Use this feature to enable the Vanderpool Technology. This technology allows the system to run several operating systems simultaneously. The options are Disable and **Enable**.

### **PPIN Control**

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

### **Hardware Prefetcher (Available when supported by the CPU)**

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

### **Adjacent Cache Prefetch (Available when supported by the CPU)**

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

### **DCU Streamer Prefetcher (Available when supported by the CPU)**

Select Enable to enable the DCU (Data Cache Unit) Streamer Prefetcher which will stream and prefetch data and send it to the Level 1 data cache to improve data processing and system performance. The options are Disable and **Enable**.

### **DCU IP Prefetcher (Available when supported by the CPU)**

Select Enable for DCU (Data Cache Unit) IP Prefetcher support, which will prefetch IP addresses to improve network connectivity and system performance. The options are **Enable** and Disable.

### **LLC Prefetch**

If set to Enable, the hardware prefetcher will prefetch streams of data and instructions from the main memory to the L3 cache to improve CPU performance. The options are **Disable** and Enable.

### **DCU Mode**

Use this feature to set the data prefetching mode for the Data Cache Unit. The options are **32KB 8Way Without ECC** and 16KB 4Way With ECC.

**Extended APIC**

Select Enable to activate APIC (Advanced Programmable Interrupt Controller) support. The options are **Disable** and Enable.

*\*If the feature above is set to **Enable**, the next feature is available for configuration:*

**Force x2APIC IDs**

Use this feature to enable or disable the 8-bit APIC IDs. The options are **Disable** and Enable.

**AES-NI**

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

**APIC Physical Mode**

Use this feature to enable or disable the Advanced Programmable Interrupt Controller. The options are **Disable** and Enable.

**► Advanced Power Management Configuration****► CPU P State Control**

This feature allows the user to configure the following CPU power settings:

**SpeedStep (Pstates)**

Intel SpeedStep Technology allows the system to automatically adjust processor voltage and core frequency to reduce power consumption and heat dissipation. The options are Disable and **Enable**. This feature must be set to Enable to be able to configure the next two features.

**EIST PSD Function**

This feature allows the user to choose between Hardware and Software to control the processor's frequency and performance (P-state). In HW\_ALL mode, the processor hardware is responsible for coordinating the P-state, and the OS is responsible for keeping the P-state request up to date on all Logical Processors. In SW\_ALL mode, the OS Power Manager is responsible for coordinating the P-state, and must initiate the transition on all Logical Processors. In SW\_ANY mode, the OS Power Manager is responsible for coordinating the P-state and may initiate the transition on any Logical Processors. The options are **HW\_ALL**, SW\_ALL, and SW\_ANY.

**Turbo Mode**

This feature will enable dynamic control of the processor, allowing it to run above stock frequency. The options are Disable and **Enable**.

## ► Hardware PM State Control

### Hardware P-States

This setting allows the user to select between OS and hardware-controlled P-states. Selecting Native Mode allows the OS to choose a P-state. Selecting Out of Band Mode allows the hardware to autonomously choose a P-state without OS guidance. Selecting Native Mode with No Legacy Support functions as Native Mode with no support for older hardware. The options are **Disable**, Native Mode, Out of Band Mode, and Native Mode with No Legacy Support.

## ► CPU C State Control

### Autonomous Core C-State

Enabling this setting allows the hardware to autonomously choose to enter a C-state based on power consumption and clock speed. The options are **Disable** and Enable. This feature must be set to Disable to be able to configure the next two features.

### CPU C6 report

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

### Enhanced Halt State (C1E)

Select Enable to use Enhanced Halt State technology, which will significantly reduce the CPU's power consumption by reducing its clock cycle and voltage during a Halt state. The options are Disable and **Enable**.

## ► Package C State Control

### Package C State

This feature allows the user to set the limit on the C State package register. The options are C0/C1 State, C2 State, C6 (Non Retention) State, C6 (Retention) State, No Limit, and **Auto**.

## ► CPU T State Control

### Software Controlled T-States

Use this feature to enable Software Controlled T-States. The options are Disable and **Enable**.



## ▶ Chipset Configuration

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

### ▶ North Bridge

#### ▶ Memory Configuration

##### Integrated Memory Controller

###### Enforce POR

Select POR (Plan of Record) to enforce POR restrictions on DDR4 frequency and voltage programming. The options are **POR** and Disable.

###### Memory Frequency

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

###### Custom Refresh Enable

Use this feature to perform a custom memory refresh rate. The options are **Disable** and Enable.

###### MC BGF threshold

Enter a value for the HA to MC BGF threshold, which is used for scheduling an MC request in bypass conditions. The default is **0**.

###### DLL Reset Test

Enter a value for the amount of loops to execute RMT for during DLL reset tests. The default is **0**.

#### ▶ Memory Topology

This menu displays memory information detected by the system.

#### ▶ Memory RAS Configuration

##### Static Virtual Lockstep Mode

Select Enable to run the system's memory channels in lockstep mode to minimize memory access latency. The options are Disable and **Enable**.

### **Mirror mode**

This feature allows memory to be mirrored between two channels, providing 100% redundancy. The options are **Disable**, Mirror Mode 1LM, and Mirror Mode 2LM.

### **ADDDC Sparing**

Adaptive Double Device Data Correction (ADDDC) Sparing detects when the predetermined threshold for correctable errors is reached, copying the contents of the failing DIMM to spare memory. The failing DIMM or memory rank will then be disabled. The options are **Disable** and **Enable**.

***\*If the feature above is set to Enable, Enable ADDDC Error Injection will be available for configuration:***

### **Enable ADDDC Error Injection**

Error injection is a technique used to enhance memory error recovery. Select **Enable** to propagate error injection equally between the primary device and the buddy device (with half of the cache line to each device). Enable this feature when ADDDC Sparing is set to **Enable**. The options are **Disable** and **Enable**.

### **Patrol Scrub**

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

***\*If the feature above is set to Enable, the next two features are available for configuration:***

### **Patrol Scrub Interval**

This feature allows you to decide how many hours the system should wait before the next complete patrol scrub is performed. Use the keyboard to enter a value from 0-24. The default setting is **24**.

### **Patrol Scrub Address Mode**

Use this feature to select the address mode between Reverse Address or System Physical Address. The options are **Reverse Address** or System Physical Address.

## ► IIO Configuration

### EV DFX Features

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

### ► CPU1 Configuration

#### IOU0 (IIO PCIe Br1)

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

#### IOU1 (IIO PCIe Br2)

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

#### IOU2 (IIO PCIe Br3)

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

- **Socket 0 PcieBr0D00F0 - Port 0/DMI**
- **Socket 0 PcieBr1D00F0 - Port 1A**
- **Socket 0 PcieBr2D00F0 - Port 2A**
- **Socket 0 PcieBr3D00F0 - Port 3A**
- **Socket 0 PcieBr3D02F0 - Port 3C**

#### Link Speed

Use this feature to select the link speed for this port. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), and Gen 3 (8 GT/s).

#### PCI-E Port Link Status

This feature shows the status of the device plugged into this slot.

#### PCI-E Port Link Max

This feature shows the status of the device plugged into this slot.

#### PCI-E Port Link Speed

This feature shows the status of the device plugged into this slot.

### PCI-E Port Max Payload Size

Use this feature to select the maximum payload size for this port. The options are 128B, 256B, and **Auto**.

## ► IOAT Configuration

### Disable TPH

Transparent Huge Pages (TPH) is a Linux memory management system that enables communication in larger blocks (pages). Enabling this feature will increase performance. The options are **No** and Yes.

***\*If the feature above is set to No, Relax Ordering will be available for configuration:***

### Prioritize TPH

Use this feature to enable Prioritize TPH support. The options are Enable and **Disable**.

### Relaxed Ordering

Select Enable to enable Relaxed Ordering support, which will allow certain transactions to violate the strict-ordering rules of PCI bus for a transaction to be completed prior to other transactions that have already been queued. The options are **Disable** and Enable.

## ► Intel® VT for Directed I/O (VT-d)

### Intel® VT for Directed I/O (VT-d)

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

***\*If the feature above is set to Enable, the five features below will be available for configuration:***

### Interrupt Remapping

Use this feature to enable Interrupt Remapping support, which detects and controls external interrupt requests. The options are **Enable** and Disable.

### PassThrough DMA

Use this feature to allow devices such as network cards to access the system memory without using a processor. Select Enable to use the Non-Isoch VT-d Engine Pass Through Direct Memory Access (DMA) support. The options are **Enable** and Disable.

## ATS

Use this feature to enable Non-Isoch VT-d Engine Address Translation Services (ATS) support. ATS translates virtual addresses to physical addresses. The options are **Enable** and Disable.

## Posted Interrupt

Use this feature to enable VT-d Posted Interrupt. The options are **Enable** and Disable.

## Coherency Support (Non-Isoch)

Use this feature to maintain setting coherency between processors or other devices. Select Enable for the Non-Isoch VT-d engine to pass through DMA to enhance system performance. The options are **Enable** and Disable.

## ► Intel® VMD Technology

### ► Intel® VMD for Volume Management Device on CPU1

#### Intel® VMD for Volume Management Device for PStack0

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

## PCIe Hot Plug

Use this feature to enable the hot plugging feature for PCI slots. The options are Disable, **Enable**, Auto, and Manual.

## PCI-E Completion Timeout (Global) Disable

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

## ► South Bridge

The following South Bridge information will display:

- USB Module Version
- USB Devices

## Legacy USB Support

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

### **XHCI Hand-off**

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

### **Port 60/64 Emulation**

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

## **► SATA And RST Configuration**

### **SATA Controller(s)**

This feature enables or disables the onboard SATA controller supported by the Intel PCH chip. The options are **Enabled** and Disabled.

### **SATA Mode Selection**

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

### **PCI-E M.2-M1**

This feature appears if an M.2 device is plugged in and RAID is selected in the SATA Mode Selection feature. Use this feature to enable or disable RST PCIe storage remapping. The options are RST Controlled and **Not RST Controlled**.

### **Aggressive LPM Support**

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

### **Serial ATA Port 0-3**

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

- Model number of drive and capacity
- Software Preserve Support

### **Serial ATA Port 0-3 Hot Plug**

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

**Serial ATA Port 0-3 Spin Up Device**

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

**Serial ATA Port 0-3 SATA Device Type**

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

**► Trusted Computing****TPM20 Device Found****Vendor****Firmware Version****Security Device Support**

If this feature and the TPM jumper on the motherboard are both set to **Enabled**, onboard security devices will be enabled for TPM support to enhance data integrity and network security. Please reboot the system for a change on this setting to take effect. The options are **Disable** and **Enable**.

The following TPM information will be displayed:

- Active PCR banks
- Available PCR banks

***\*If the feature "Security Device Support" is enabled, the following features are available for configuration:***

**SHA-1 PCR Bank**

Use this item to disable or enable the SHA-1 Platform Configuration Register (PCR) bank for the installed TPM device. The options are **Disabled** and **Enabled**.

**SHA256 PCR Bank**

Use this feature to disable or enable the SHA256 Platform Configuration Register (PCR) bank for the installed TPM device. The options are **Disabled** and **Enabled**.

**Pending operation**

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

### **Platform Hierarchy**

Use this feature to disable or enable platform hierarchy for platform protection. The options are Disabled and **Enabled**.

### **Storage Hierarchy**

Use this feature to disable or enable storage hierarchy for cryptographic protection. The options are Disabled and **Enabled**.

### **Endorsement Hierarchy**

Use this feature to disable or enable endorsement hierarchy for privacy control. The options are Disabled and **Enabled**.

### **TPM2.0 UEFI Spec Version**

Use this feature to specify the TPM UEFI spec version. TCG 1.2 has support for Windows® 2012, Windows 8, and Windows 10. TCG 2 has support for Windows 10 or later. The options are TCG\_1\_2 and **TCG\_2**.

### **Physical Presence Spec Version**

Use this feature to select the PPI spec version. The options are 1.2 and **1.3**.

### **TPM 20 InterfaceType**

### **PH Randomization**

Use this feature to disable or enable Platform Hierarchy (PH) Randomization. The options are **Disabled** and Enabled.

### **Device Select**

Use this feature to select the TPM version. TPM 1.2 will restrict support to TPM 1.2 devices. TPM 2.0 will restrict support for TPM 2.0 devices. Select Auto to enable support for both versions. The options are TPM 1.2, TPM 2.0, **Auto**.

### **TXT support**

Intel TXT (Trusted Execution Technology) helps protect against software-based attacks and ensures protection, confidentiality and integrity of data stored or created on the system. Use this feature to enable or disable TXT Support. The options are **Disabled** and Enabled.



## ►ACPI Settings

### 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 in order to reduce system crashes and enhance system recovery and health monitoring. The options are Disabled and **Enabled**.

### High Precision Event Timer

Select Enabled to activate the High Precision Event Timer (HPET) that produces periodic interrupts at a much higher frequency than a Real-time Clock (RTC) does in synchronizing multimedia streams, providing smooth playback and reducing the dependency on other timestamp calculation devices, such as an x86 RDTSC Instruction embedded in the CPU. The High Performance Event Timer is used to replace the 8254 Programmable Interval Timer. The options are Disabled and **Enabled**.

### Native PCIE Enable

Enable this feature to grant control of PCI Express Native hot plug, PCI Express Power Management Events, and PCI Express Capability Structure Control. The options are Disabled and **Enabled**.

### Native ASPM

Select Enabled for the operating system to control the ASPM, or Disabled for the BIOS to control the ASPM. The options are Auto, Enabled, and **Disabled**.

### Headless Mode Support

Select Enabled for the system to function without a keyboard, mouse, or monitor. The options are **Disabled** and Enabled.

### NUMA (Available when the OS supports this feature)

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

## ►Super IO Configuration

### Super IO Chip AST2500

#### ►Serial Port 1 Configuration

##### Serial Port 1

Select Enabled to enable the onboard serial port specified by the user. The options are **Enabled** and Disabled. Enable this feature for the next two features to display and only the Change Settings feature is available for configuration.

### **Device Settings**

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

### **Change Settings**

This feature specifies the base I/O port address and the Interrupt Request address of Serial Port 1. Select **Auto** for the BIOS to automatically assign the base I/O and IRQ address to a serial port specified. The options are **Auto**, (IO=3F8h; IRQ=4), (IO=2F8h; IRQ=4), (IO=3E8h; IRQ=4), and (IO=2E8h; IRQ=4).

## **►Serial Port 2 Configuration**

### **Serial Port 2**

Select Enabled to enable the onboard serial port specified by the user. The options are **Enabled** and Disabled. Enable this feature for the next two features to display and only the Change Settings feature is available for configuration.

### **Device Settings**

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

### **Change Settings**

This feature specifies the base I/O port address and the Interrupt Request address of Serial Port 1. Select Auto for the BIOS to automatically assign the base I/O and IRQ address to a serial port specified. The options are **Auto**, (IO=2F8h; IRQ=3), (IO=3F8h; IRQ=3), (IO=3E8h; IRQ=3), and (IO=2E8h; IRQ=3).

### **Serial Port 2 Attribute**

Use this feature to select the serial port 2 mode. The options are **SOL** and COM.

## **►Serial Port Console Redirection**

### **COM1**

#### **Console Redirection**

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

***\*If the feature above is set to Enabled, the following features will become available for configuration:***

## ► Console Redirection Settings

### Terminal Type

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

### Bits per second

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

### Data Bits

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

### Parity

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

### Stop Bits

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

### Flow Control

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

### VT-UTF8 Combo Key Support

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

### **Recorder Mode**

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

### **Resolution 100x31**

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

### **Legacy OS Redirection Resolution**

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

### **Putty KeyPad**

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

### **Redirection After BIOS POST**

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

### **COM2/SOL Console Redirection**

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

***\*If the feature above is set to Enabled, the following features are available for configuration:***

#### **► Console Redirection Settings**

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

#### **Terminal Type**

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

**Parity**

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

**Stop Bits**

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

**Flow Control**

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

**VT-UTF8 Combo Key Support**

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

**Recorder Mode**

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

**Resolution 100x31**

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

### **Legacy OS Redirection Resolution**

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

### **Putty KeyPad**

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

### **Redirection After BIOS POST**

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

## **Legacy Console Redirection**

### **► Legacy Console Redirection Settings**

#### **Legacy Serial Redirection Port**

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

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

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

### **Console Redirection**

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

***\*If the feature above is set to Enabled, the following features are available for configuration:***

### **► Console Redirection Settings**

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

**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**, COM2, COM3, COM4, COM5, COM6, and AMT SOL.

**Terminal Type**

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

**Bits per second**

This 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**

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.

**Data Bits**

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

**Parity**

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

**Stop Bits**

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

## ► PCIe/PCI/PnP Configuration

The following information will display:

- PCI Bus Driver Version
- PCI Devices Common Settings:

### SR-IOV Support

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

### MMCFG Size

Use this feature to select the MMCFG size. The options are 64M, 128M, **256M**, 512M, 1G, and 2G.

### MMIO High Base

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

### MMIO High Granularity Size

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

### Above 4G MMIO BIOS Assignment

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

## PCIe/PCI/PnP Configuration

### Onboard Video

Use this feature to select the onboard video option ROM type. The options are Do Not Launch, EFI, and **Legacy**.

### Onboard Storage

Use this feature to select the UEFI and Legacy storage option ROM type. The options are Do Not Launch, EFI, and **Legacy**.

### Onboard LAN Device

Use this feature to select which firmware function to be loaded for onboard LAN devices. The options are **Auto**, Disabled, and Enabled.

### Onboard LAN 1 OPROM

Use this feature to select which firmware type to be loaded for LAN Port 2 used for system boot. The options are Disabled, EFI, and **Legacy**.



### **Onboard LAN2 OPROM**

Use this feature to select which firmware function to be loaded for LAN Port 2 used for system boot. The options are **Disabled**, PXE, and iSCSI.

### **AOM Board**

AOM board information will be listed here if detected by the system.

### **CPU SLOT1 PCI-E 3.0 X16**

Use this feature to select which firmware to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

### **CPU SLOT2 PCI-E 3.0 X16**

Use this feature to select which firmware to be loaded for the add-on card in this slot. The options are Disabled, **Legacy**, and EFI.

## **► Network Stack Configuration**

### **Network Stack**

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

***\*If the feature above is set to Enabled, the next six features will be available for configuration:***

#### **Ipv4 PXE Support**

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

#### **Ipv4 HTTP Support**

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

#### **Ipv6 PXE Support**

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

#### **Ipv6 HTTP Support**

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

#### **PXE boot Wait Time**

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

#### **Media detect count**

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

## ▶Tls Auth Configuration

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

### ▶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 Cert (Certification) Using File

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

#### Cert GUID

This feature displays the GUID for this system.

#### ▶Commit Changes and Exit

Use this feature to commit to the changes you have made and exit from the system.

#### ▶Discard Changes and Exit

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

#### ▶Delete Certification

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

## ▶Client Certification 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 Cert (Certification) Using File

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

#### Cert (Certification) GUID (Global Unique Identifier)

This feature displays the GUID for this system.

**▶ Commit Changes and Exit**

Use this feature to commit to the changes you have made and exit from the system.

**▶ Discard Changes and Exit**

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

**▶ Delete Certification**

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

**▶ RAM Disk Configuration****Disk Memory Type**

Use this feature to specify the type of memory use from the available memory pool in the system to create a disk. The options are **Boot Service Data** and **Reserved**.

**▶ Create Raw**

Use this feature to create a RAW RAM disk from all available memory in the system. When you select this submenu, the following features will display:

- **Size (Hex):** The default setting is **1**.
- **Create & Exit:** Create a new disk and exit the submenu.
- **Discard & Exit:** Discard changes and exit the submenu.

**▶ Create from File**

Use this feature to create a RAM disk from a specified file.

**Create RAM Disk List:****Remove Selected RAM Disk(s):**

Use this feature to delete the RAM disk.

## 4.4 Event Logs

Use this menu to configure event log settings.



### ► Change SMBIOS Event Log Settings

#### Enabling/Disabling Options

#### SMBIOS Event Log

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

#### Erasing Settings

#### Erase Event Log

Select Enabled to erase all error events in the SMBIOS (System Management BIOS) log before an event logging is initialized at bootup. The options are **No**, "Yes, Next reset," and "Yes, Every reset."

#### When Log is Full

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

## **SMBIOS Event Log Standard Settings**

### **Log System Boot Event**

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

### **MECI (Multiple Event Count Increment)**

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

### **METW (Multiple Event Count Time Window)**

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



**Note:** Reboot the system for the changes to take effect.

## **Custom Options**

### **Log EFI Status Code**

Use this feature to enable or disable the logging of EFI status codes. The options are Disabled and **Enabled**.

### **Convert EFI Status Codes to Standard Smbios Type**

Use this feature to enable or disable the converting of EFI status codes to standard Smbios types. The options are Disabled and **Enabled**.

## **►View SMBIOS Event Log**

This feature allows the user to view the event in the SMBIOS event log. The following categories are displayed:

**DATE/TIME/ERROR CODE/SEVERITY**

## 4.5 IPMI

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



### BMC Firmware Revision

This feature displays the IPMI firmware revision used in your system.

### IPMI STATUS

This feature displays the status of the IPMI firmware installed in your system.

### ► System Event Log

#### Enabling/Disabling Options

#### SEL Components

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

#### Erasing Settings

#### Erase SEL

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

### When SEL is Full

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



**Note:** Reboot the system for the changes to take effect.

## ► BMC Network Configuration

### IPMI LAN Selection

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

### IPMI Network Link Status

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

### Station MAC Address

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

### VLAN

This feature is configurable if the Update IPMI LAN Configuration feature is set to Yes. Use this feature to enable or disable the IPMI VLAN function. The options are **Disable** and Enable.

### Station IP Address

This feature displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).

### Subnet Mask

This feature displays the sub-network that this computer belongs to. The value of each three-digit number separated by dots should not exceed 255.

### Gateway IP Address

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).

### IPV6 Status Address

### Station IPV6 Address

Use this feature to enter the IPV6 address.

### Prefix Length

Use this feature to change the prefix length.

### **IPV6 Router1 IP Address**

Use this feature to change the IPV6 Router 1 IP address.

### **Update IPMI LAN Configuration**

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

***\*If the feature above is set to Yes, the VLAN and Configuration Address Source features are available for configuration:***

### **VLAN**

This feature is configurable if the Update IPMI LAN Configuration feature is set to Yes. Use this feature to enable or disable the IPMI VLAN function. The options are **Disable** and Enable.

***\*If the feature above is set to Enable, the VLAN feature below is available for configuration:***

### **VLAN**

Use this feature to select a value for VLAN ID.

### **Configure IPV4 support**

#### **Configuration Address Source**

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

***\*If the feature above is set to Static, the Station IP Address/Prefix Length/IPV6 Router1 IP Address features are available for configuration:***

#### **Station IP Address**

This feature displays the Station IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).

#### **Subnet Mask**

This feature displays the sub-network that this computer belongs to. The value of each three-digit number separated by dots should not exceed 255.

#### **Gateway IP Address**

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 192.168.10.253).



## Configure IPV6 support

### IPV6 Support

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

## 4.6 Security

Use this menu to configure the security settings.



### Administrator Password

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

### Password Check

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

### Password Check

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

## ▶ Secure Boot

### System Mode

### Vendor Keys

### Secure Boot

#### Secure Boot Mode

This feature allows the user to select the desired secure boot mode for the system. The options are Standard and **Custom**.

*\*If Secure Boot Mode is set to Custom, Key Management features are available for configuration:*

#### ▶ Restore Factory Keys

Select Yes to restore all factory keys to the default settings. The options are Yes and No.

## ▶ Key Management

This submenu allows the user to configure the following Key Management settings.

### Factory Key Provision

Select Enabled to install the default Secure Boot keys set by the manufacturer. The options are **Disabled** and Enabled.

#### ▶ Restore Factory Keys

Select Yes to restore all factory keys to the default settings. The options are Yes and No.

#### ▶ Reset to Setup Mode

Select Yes to delete all Secure Boot key databases and force the system to Setup Mode. The options are Yes and No.

#### ▶ Export Secure Boot variables

Use this feature to copy the NVRAM contents of the secure boot variables to a file.

#### ▶ Enroll Efi Image

This feature allows the image to run in Secure Boot mode.

### Device Guard Ready

#### ▶ Remove 'UEFI CA' from DB

Use this feature to remove the Microsoft UEFI CA certificate from the database. The options are Yes and No.

▶ **Restore DB defaults**

Select Yes to restore the DB defaults.

▶ **Platform Key (PK)**

This feature allows the user to configure the settings of the platform keys.

**Update**

Select Yes to load a factory default PK or No to load from a file on an external media.

▶ **Key Exchange Keys (KEK)**

**Update**

Select Yes to load a factory default KEK or No to load from a file on an external media.

**Append**

Select Yes to add the KEK from the manufacturer's defaults list to the existing KEK. Select No to load the KEK from a file. The options are Yes and No.

▶ **Authorized Signatures**

**Update**

Select Yes to load a factory default db or No to load from a file on an external media.

**Append**

Select Yes to add the db from the manufacturer's defaults list to the existing db. Select No to load the db from a file. The options are Yes and No.

▶ **Forbidden Signatures**

**Update**

Select Yes to load a factory default dbx or No to load from a file on an external media.

**Append**

Select Yes to add the dbx from the manufacturer's defaults list to the existing dbx. Select No to load the dbx from a file. The options are Yes and No.

▶ **Authorized TimeStamps**

**Update**

Select Yes to load a factory default dbt or No to load from a file on an external media.

**Append**

Select Yes to add the dbt from the manufacturer's defaults list to the existing dbt. Select No to load the dbt from a file. The options are Yes and No.

**► OsRecovery Signatures****Update**

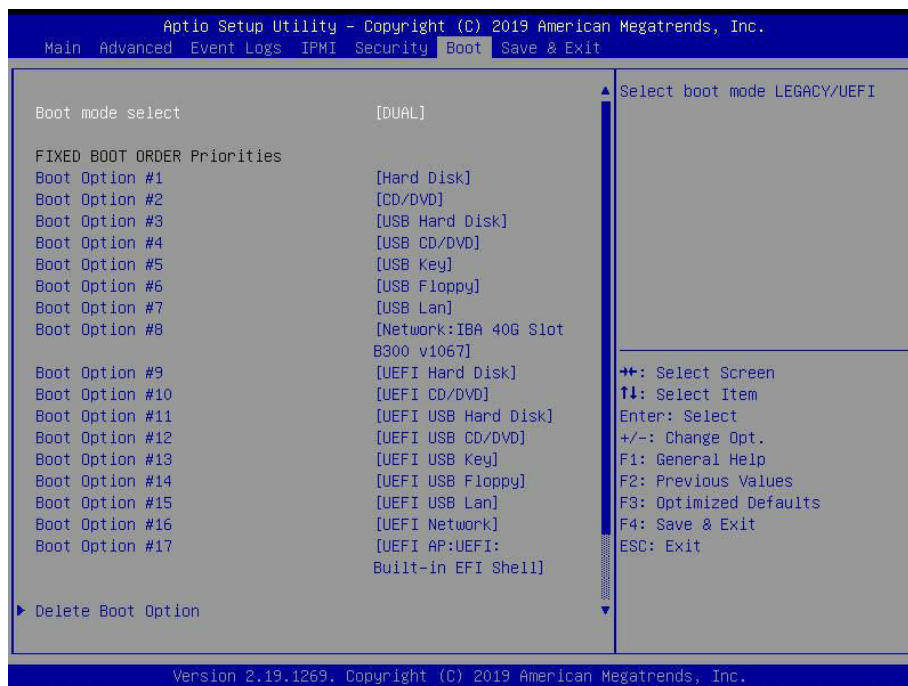
Select Yes to load a factory default dbr or No to load from a file on an external media.

**Append**

Select Yes to add the dbr from the manufacturer's defaults list to the existing dbr. Select No to load the dbr from a file. The options are Yes and No.

## 4.7 Boot

Use this menu to configure boot settings:



### Boot mode select

Use this feature to select the boot mode. The options are LEGACY, UEFI, and **DUAL**.

### FIXED BOOT ORDER Priorities

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

- LEGACY/UEFI/DUAL Boot Option #1
- LEGACY/UEFI/DUAL Boot Option #2
- LEGACY/UEFI/DUAL Boot Option #3
- LEGACY/UEFI/DUAL Boot Option #4
- LEGACY/UEFI/DUAL Boot Option #5
- LEGACY/UEFI/DUAL Boot Option #6
- LEGACY/UEFI/DUAL Boot Option #7
- LEGACY/UEFI/DUAL Boot Option #8
- LEGACY/UEFI/DUAL Boot Option #9
- LEGACY/UEFI/DUAL Boot Option #10

- LEGACY/UEFI/DUAL Boot Option #11
- LEGACY/UEFI/DUAL Boot Option #12
- LEGACY/UEFI/DUAL Boot Option #13
- LEGACY/UEFI/DUAL Boot Option #14
- LEGACY/UEFI/DUAL Boot Option #15
- LEGACY/UEFI/DUAL Boot Option #16
- LEGACY/UEFI/DUAL Boot Option #17

▶ **Delete Boot Option**

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

▶ **Delete Driver Option**

Use this feature to remove an EFI driver option from the driver order.

▶ **UEFI Application Boot Priorities**

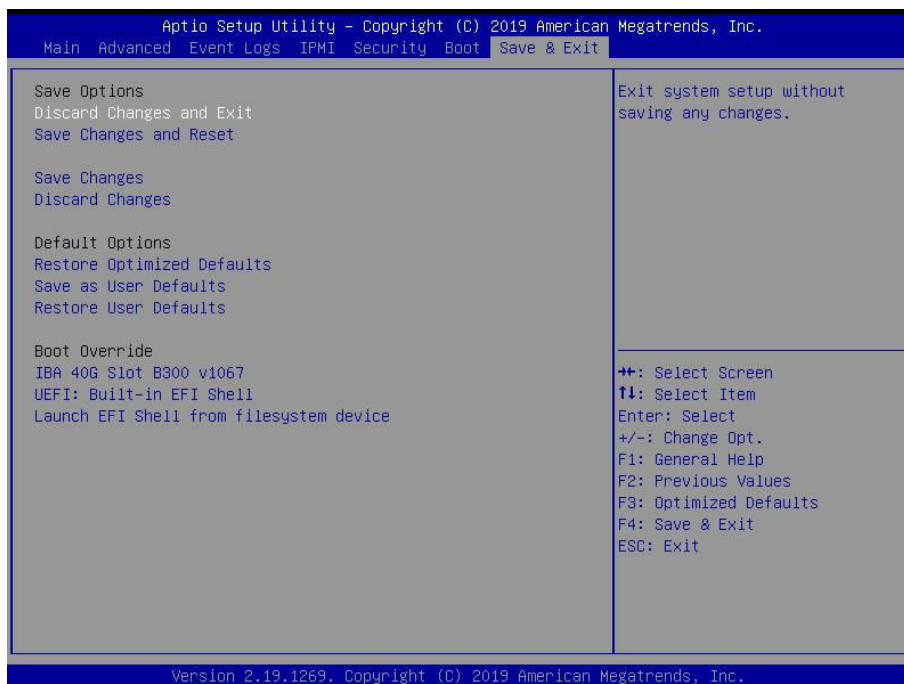
- Boot Option # - This feature sets the system boot order of detected devices. The options are **[the list of detected boot device(s)]** and Disabled.

▶ **NETWORK Drive BBS Priorities**

- Boot Option # - This feature sets the system boot order of detected devices. The options are **[the list of detected boot device(s)]** and Disabled.

## 4.8 Save & Exit

Use this menu to configure save and exit settings.



### Save Options

#### Discard Changes and Exit

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

#### Save Changes and Reset

When you have completed the system configuration changes, select this option to save all changes made and reset the system.

#### Save Changes

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

#### Discard Changes

Select this feature and press <Enter> to discard all the changes and return to the AMI BIOS Utility Program.



## **Default Options**

### **Restore Optimized Defaults**

To set this feature, select Restore Optimized Defaults and press <Enter>. These are factory settings designed for maximum system performance but not for maximum stability.

### **Save as User Defaults**

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

### **Restore User Defaults**

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

### **Boot Override**

Other boot options are listed in this section. The system will boot to the selected boot option.

### **IBA 40G Slot B300 v1067**

### **UEFI: Built-in EFI Shell**

### **Launch EFI Shell from filesystem device**

# Appendix A

## BIOS Codes

### A.1 BIOS Error POST (Beep) Codes

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

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

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

These fatal errors are usually communicated through a series of audible beeps. The table below lists some common errors and their corresponding beep codes encountered by users.

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

## A.2 Additional BIOS POST Codes

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

When BIOS performs the Power On Self Test, it writes checkpoint codes to I/O port 0080h. If the computer cannot complete the boot process, a diagnostic card can be attached to the computer to read I/O port 0080h (Supermicro p/n AOM-SPI80-V).

For information on AMI updates, please refer to <http://www.ami.com/products/>.

## Appendix B

# Software Installation


### B.1 Installing Software Programs

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

After accessing the website, go into the CDR\_Images (in the parent directory of the above link) and locate the ISO file for your motherboard. Download this file to create a DVD of the drivers and utilities it contains. (You may also use a utility to extract the ISO file if preferred.)

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

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

 **Note:** To install the Windows operating system, please refer to the instructions posted on our website at <http://www.supermicro.com/support/manuals/>.

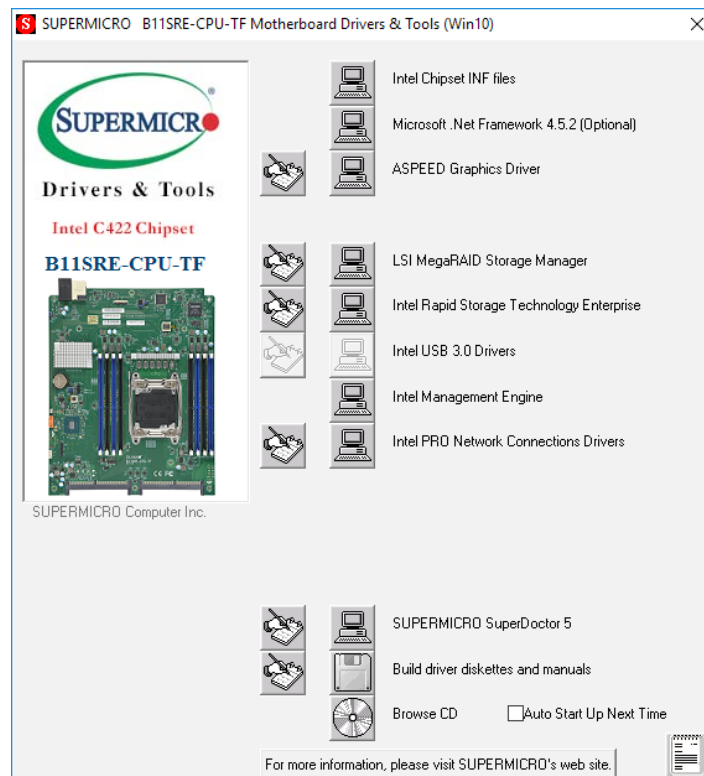


Figure B-1. Driver/Tool Installation Display Screen


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

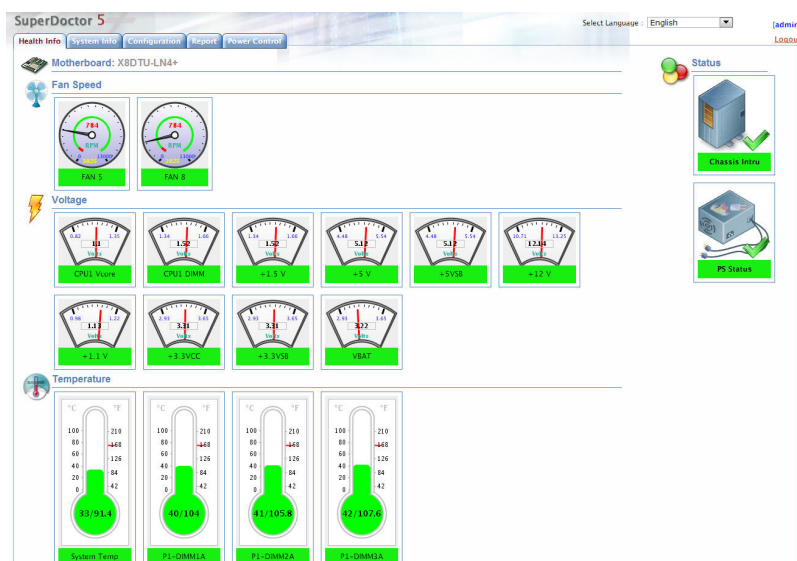
When making a storage driver diskette by booting into a driver DVD, please set the SATA Configuration to "Compatible Mode" and configure SATA as IDE in the BIOS Setup. After making the driver diskette, be sure to change the SATA settings back to your original settings.

## B.2 SuperDoctor® 5


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

SuperDoctor 5 comes in local and remote management versions and can be used with Nagios to maximize your system monitoring needs. With SuperDoctor 5 Management Server (SSM Server), you can remotely control power on/off and reset chassis intrusion for multiple systems with SuperDoctor 5 or IPMI. SD5 Management Server monitors HTTP, FTP, and SMTP services to optimize the efficiency of your operation.

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



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

 **Note:** The SuperDoctor 5 program and user's manual can be downloaded from the Supermicro website at [http://www.supermicro.com/products/nfo/sms\\_sd5.cfm](http://www.supermicro.com/products/nfo/sms_sd5.cfm).

## Appendix C

### Standardized Warning Statements

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

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

These warnings may also be found on our website at [http://www.supermicro.com/about/policies/safety\\_information.cfm](http://www.supermicro.com/about/policies/safety_information.cfm).

#### Battery Handling



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

#### 電池の取り扱い

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

#### 警告

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

#### 警告

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

#### Warnung

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

## Attention

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

## ¡Advertencia!

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

## אזהרה!

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

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

## 경고!

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

## Waarschuwing

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

## Product Disposal



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

### 製品の廃棄

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

### 警告

本产品的废弃处理应根据所有国家的法律和规章进行。

### 警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

### Warnung

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

### ¡Advertencia!

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

### Attention

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

סילוק המוצר

אזהרה!

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

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

### 경고!

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

### Waarschuwing

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



# Appendix D

## UEFI BIOS Recovery


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


### D.1 Overview

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

### D.2 Recovering the UEFI BIOS Image

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

 **Note 1:** Follow the BIOS recovery instructions below for BIOS recovery when the main BIOS block crashes.

 **Note 2:** When the BIOS recovery block crashes, you will need to follow the procedures to make a Returned Merchandise Authorization (RMA) request. (For a RMA request, please see section 3.5 for more information).

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


This feature allows the user to recover the main BIOS image using a USB-attached device without additional utilities used. A USB flash device such as a USB Flash Drive, or a USB


CD/DVD ROM/RW device can be used for this purpose. However, a USB Hard Disk drive cannot be used for BIOS recovery at this time.

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

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

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

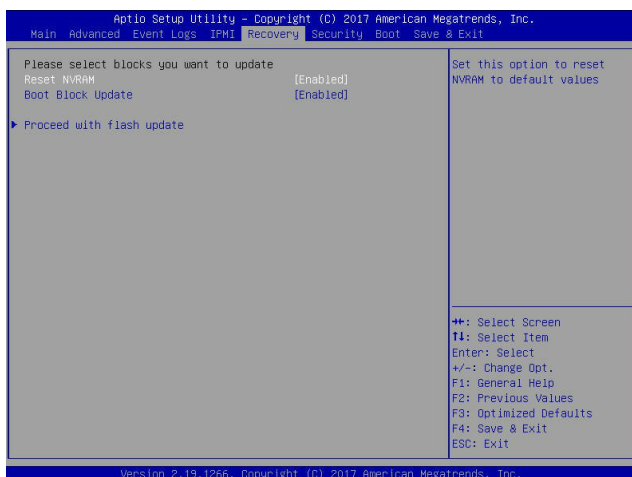
 **Note 1:** If you cannot locate the "Super.ROM" file in your driver disk, visit our website at [www.supermicro.com](http://www.supermicro.com) to download the BIOS package. Extract the BIOS binary image into a USB flash device and rename it "Super.ROM" for the BIOS recovery use.

 **Note 2:** Before recovering the main BIOS image, confirm that the "Super.ROM" binary image file you download is the same version or a close version meant for your motherboard.

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



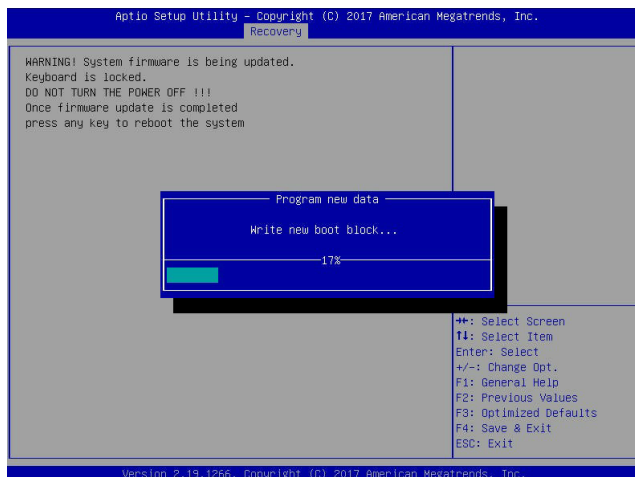
3. After locating the new BIOS binary image, the system will enter the BIOS Recovery menu as shown below:



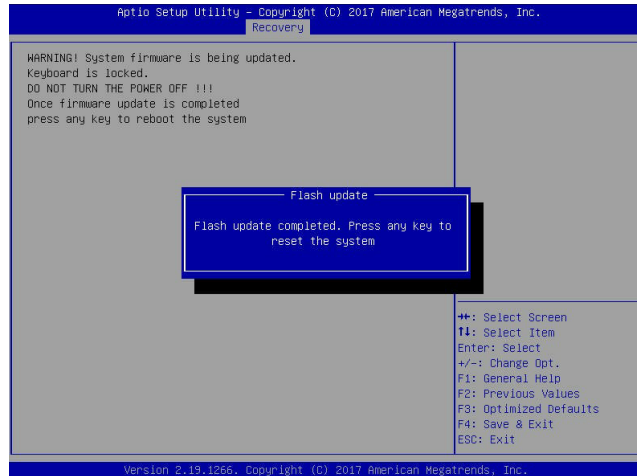
**Note:** At this point, you may decide if you want to start the BIOS recovery. If you decide to proceed with BIOS recovery, follow the procedures below.

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

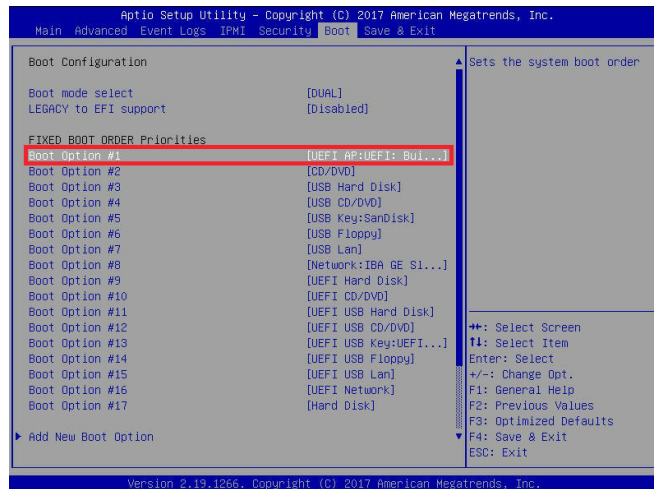
**Note:** Do not interrupt the BIOS flashing process until it has completed.



- After the BIOS recovery process is completed, press any key to reboot the system.



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



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

```

UEFI Interactive Shell v2.1
EDK II
UEFI v2.50 (American Megatrends, 0x0005000C)
Mapping Table
  FS0: Alias(s):HD(0):BIOS:BLK1:
        PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)/HD(1,MBR,0x3791072,0x800,0x1
DR9592)
  BLK0: Alias(s):
        PciRoot(0x0)/Pci(0x14,0x0)/USB(0x11,0x0)
Press F8 in 1 seconds to skip startup.nsh or any other key to continue.
Shell> fs0:
FS0:\> cd AFUDOS
FS0:\AFUDOS> cd SNIPME2_03162017
FS0:\AFUDOS\SNIPME2_03162017> flash.nsh X110PU7_314

```



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

```

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

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

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

```

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

```

Verifying MBR Block ..... done
- Update success for F8P
- Update success for IE
- Successful Update Recovery Loader to OPRx11
- Successful Update MFSB11
- Successful Update FTRx11
- Successful Update MFS, IVB1 and IVB211
- Successful Update FLOG and UTOK11
- ME Entire Image update success !!
WARNING : system must power-off to have the changes take effect!
Moving FS0:\AFUDOS\SNIPME2_03162017\fdt\k64.efi -> FS0:\AFUDOS\SNIPME2_03162017\fdt\k64.efi
dt.smc
- [ok]
Moving FS0:\AFUDOS\SNIPME2_03162017\afuef1\k64.efi -> FS0:\AFUDOS\SNIPME2_03162017\afuef1\k64.efi
7\afuef1.smc
- [ok]
*****
* Please ignore this 'Shell: Cannot read from file - Device Error'
* warning message due to it does not impact flashing process.
*****
Deleting .....
Delete successful.
FS0:\>

```

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