B3ST1-CPU-001

USER'S MANUAL

Revision 1.0b

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

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

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

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

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in 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".

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

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

Manual Revision 1.0b

Release Date: April 22, 2025

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 motherboard.

About This Motherboard

The Supermicro B3ST1-CPU-001 motherboard supports the Intel® Xeon E-2300 Family processor with up to 8 cores. Built with the Intel PCH C256 chipset, the B3ST1-CPU-001 supports 128 GB DDR4 ECC and Non-ECC UDIMM memory with speeds of up to 3200 MHz in four memory slots, one dedicated BMC port via BPN, 1G Base-T ports, and a Trusted Platform Module (TPM) header on board. This motherboard also features superior IO expandability, which includes one SATA 3.0 port and one M.2 M Key supporting both PCIe 3.0 x4 and SATA. Please note that this motherboard is intended to be installed and serviced by professional technicians only. For processor/memory updates, please refer to our website at http://www.supermicro.com/products/.

Conventions Used in the Manual

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

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

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

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

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

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	Marketing@supermicro.com (General Information) Sales-USA@supermicro.com (Sales Inquiries) Government_Sales-USA@supermicro.com (Gov. Sales Inquiries) Support@supermicro.com (Technical Support) RMA@supermicro.com (RMA Support) Webmaster@supermicro.com (Webmaster)
Website:	www.supermicro.com

Europe

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

Asia-Pacific

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

Table of Contents

Chapter 1

Introduction

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

In additon to the motherboard, several important parts that are included with the system are listed below. If anything listed is damaged or missing, contact your retailer.

1.1 Checklist

Main Parts List		
Description	**Part Number**	**Quantity**
Supermicro Motherboard	B3ST1-CPU-001	1
Quick Reference Guide	MNL-2430-QRG	1

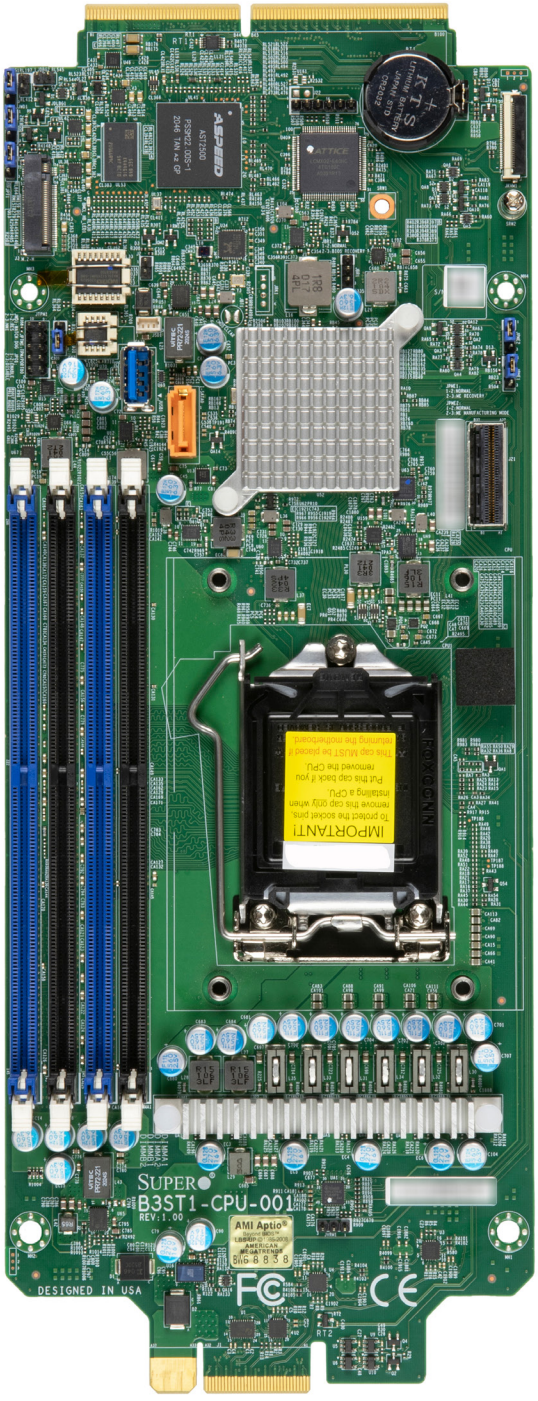
Important Links

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

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

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

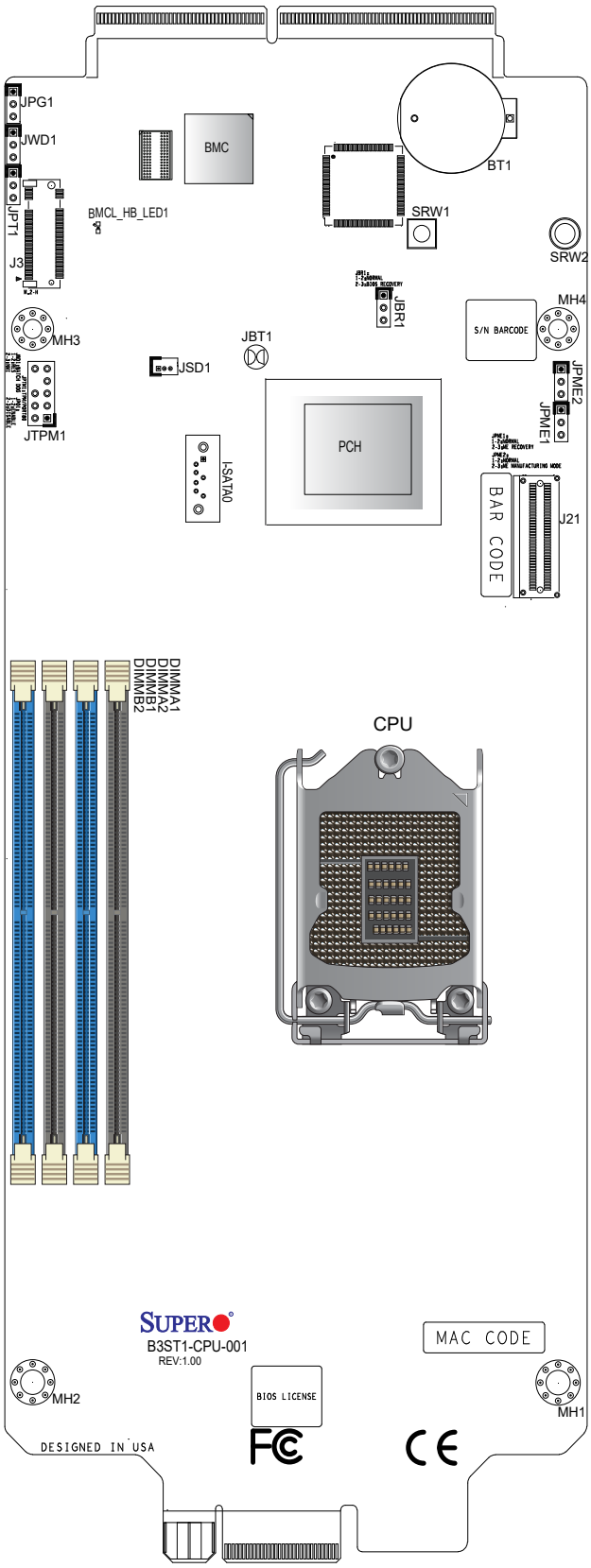
Figure 1-1. B3ST1-CPU-001 Motherboard Image



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.

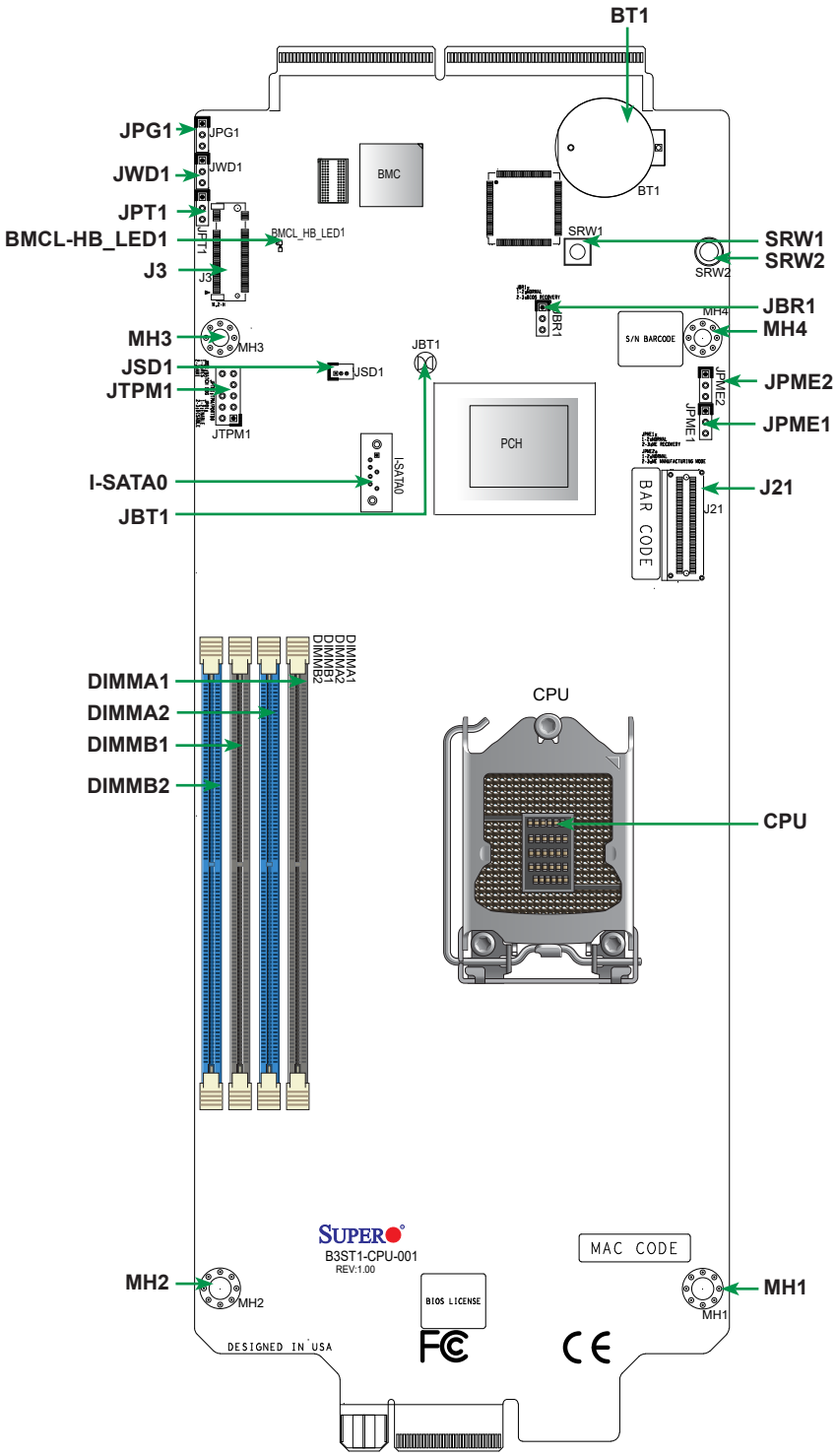
Figure 1-2. Motherboard Layout

(not drawn to scale)



Note: Components not documented are for internal testing only.

Quick Reference



Notes:

- See Chapter 2 for detailed information on jumpers, I/O ports, and connections. Jumpers and LED indicators not indicated are used for testing only.
- ▣indicates the location of Pin 1.

Quick Reference Table

Jumper	Description	Default Setting
JBR1	BIOS Recovery	Pins 1–2 (Normal)
JBT1	CMOS Clear	Open (Normal)
JPG1	VGA Enable/Disable	Pins 1–2 (Enabled)
JPME1	ME Recovery	Pins 1–2 (Normal)
JPME2	ME Manufacturing Mode	Pins 1–2 (Normal)
JPT1	Onboard TPM 2.0 Enable/Disable	Pins 2–3 (Disabled)
JWD1	Watchdog Timer	Pins 1–2 (Reset)

LED	Description	Status
BMCL_HB_LED1	BMC Heartbeat LED	Blinking Green: BMC Normal

Connector	Description
BT1	Onboard Battery
I-SATA0	SATA 3.0 Port
J3	M.2 Connector
J21	Slim SAS Connector (connects U.2 NVMe drives on AOM-BPNIO-MSH2 through Slim SAS cable)
JSD1	SATA DOM Power Connector
JTPM1	Trusted Platform Module/Port 80 Connector
SRW1, SRW2	M.2 Holding Screws

Motherboard Features

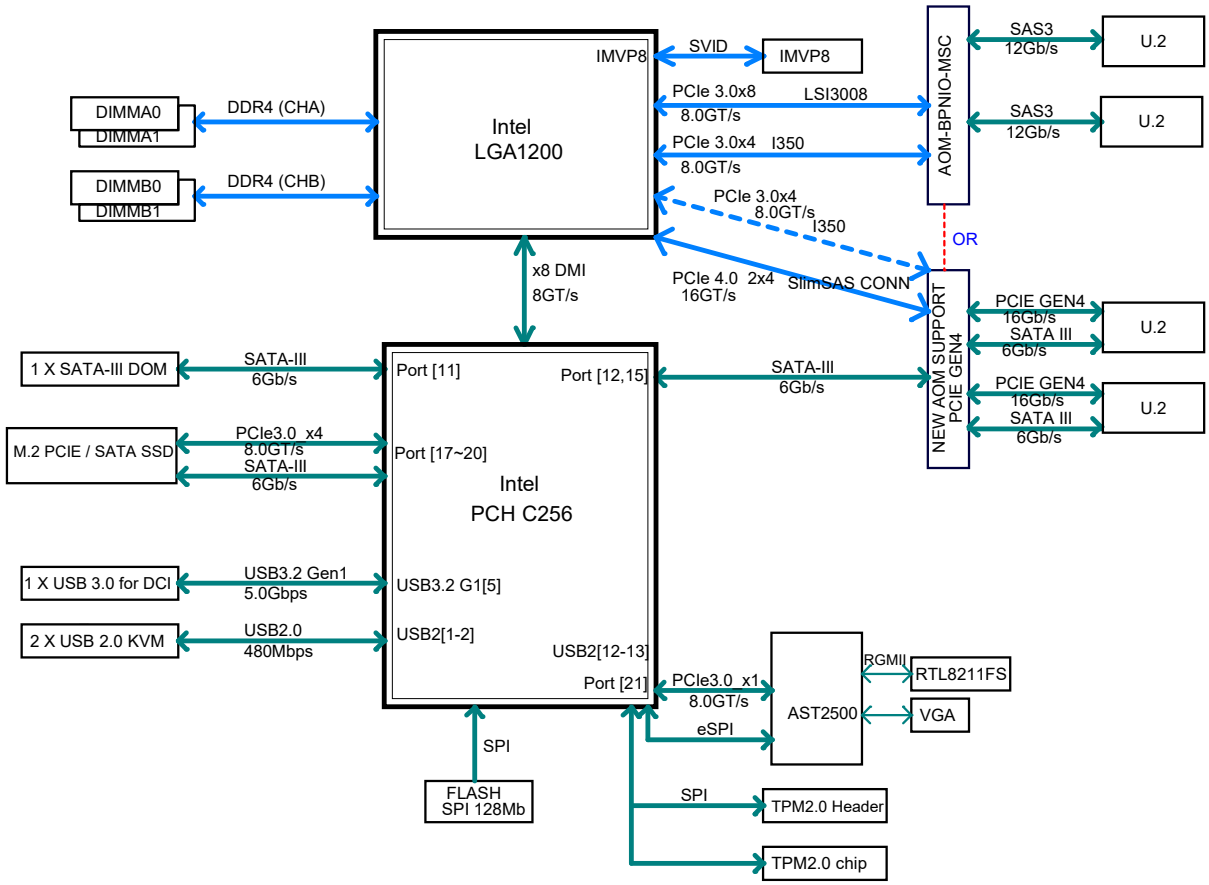
Motherboard Features
CPU
• Supports an Intel Xeon E-2300 Family processor in an LGA1200 socket
Memory
• Up to 128 GB of ECC and Non-ECC UDIMM DDR4 memory with speeds of up to 3200 MHz in four memory slots
DIMM Size
• 4 GB, 8 GB, 16 GB, 32 GB at 1.2V **Note 1:** For the latest CPU/memory updates, please refer to our website at http://www.supermicro.com/products/motherboard.
Chipset
• Intel C256
Expansion Slots
• One SATA 3.0 (I-SATA0) port • One M.2 PCIe 4.0 x4/SATA 3.0 Key-M (2280/22110)
Super I/O
• AST2500
Graphics
• Intel UHD Graphics
I/O Devices
• One SATA DOM • One Slim SAS connector • IPMI 2.0 supported by ASpeed AST2500 BMC
Optimized Chassis
• MBE-314E, MBE-628E
BIOS
• 256Mb AMI BIOS® SPI Flash BIOS • ACPI 6.0, Plug and Play (PnP), BIOS rescue hot-key, and SMBIOS 3.0 or later
Power Management
• ACPI power management • Power button override mechanism • Power-on mode for AC power recovery • Wake-on-LAN

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

Motherboard Features
System Health Monitoring
• Onboard voltage monitoring for +12 V, +5 V, +3.3 V, CPU, Memory, VBAT, +3.3 V stdby, CPU temperature, PCH temperature, system temperature • 6 CPU switch phase voltage regulator • CPU thermal trip support • Platform Environment Control Interface (PECI)/TSI
Fan Control
• Low noise fan speed control
System Management
• Trusted Platform Module (TPM) support • SuperDoctor® 5 • Chassis intrusion header and detection
LED Indicator
• BMC Heartbeat LED
Dimensions
• Dimensions: 4.8" (W) x 12.6" (L) (121.9 mm x 320.0 mm)

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

Figure 1-3.
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

Built upon the functionality and capability of the Intel® Xeon E-2300 Family processor and the Intel C256 chipset, the B3ST1-CPU-001 motherboard provides system performance, power efficiency, and feature sets to address the needs of next-generation computer users.

The B3ST1-CPU-001 dramatically increases system performance for a multitude of server applications.

The Intel PCH C256 chipset provides the following features:

- Intel AMT 12.0, TXT (only supported in UEFI boot), and AMT vPro
- SATA 3.0
- Intel Hyper-Threading, Intel VT-D, VT-x
- TSX-NI, AES, SGX
- Intel Turbo Boost Technology
- Intel Rapid Storage Technology
- 128 GB Non-ECC UDIMM DDR4 memory support with speeds of up to 3200 MHz

Note: Intel TXT is only supported in the UEFI boot mode. Please install the UEFI OS and then enable the Intel TXT feature.

1.3 Special Features

Recovery from AC Power Loss

The Basic I/O System (BIOS) provides a setting that determines how the system will respond when AC power is lost and then restored to the system. You can choose for the system to remain powered off (in which case you must press the power switch to turn it back on), or for it to automatically return to the power-on state. See 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, a warning is given, or an error message is sent to the screen. The user can adjust the voltage thresholds to define the sensitivity of the voltage monitor.

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

1.5 ACPI Features

The Advanced Configuration and Power Interface (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 CD-ROMs, network cards, hard disk drives and printers.

In addition to enabling operating system-directed power management, ACPI also provides a generic system event mechanism for Plug and Play, and an operating system-independent interface for configuration control. ACPI leverages the Plug and Play BIOS data structures, while providing a processor architecture-independent implementation that is compatible with appropriate Windows operating systems. For detailed information regarding OS support, please refer to the Supermicro website.

1.6 Power Supply

As with all computer products, a stable power source is necessary for proper and reliable operation. It is even more important for processors that have high CPU clock rates. In areas where noisy power transmission is present, you may choose to install a line filter to shield the computer from noise. It is recommended that you also install a power surge protector to help avoid problems caused by power surges.

Chapter 2

Installation

2.1 Static-Sensitive Devices

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

Precautions

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the motherboard 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 computer chassis provides excellent conductivity between the power supply, the case, the mounting fasteners and the motherboard.
- Use only the correct type of onboard CMOS battery. Do not install the onboard battery upside down to avoid 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

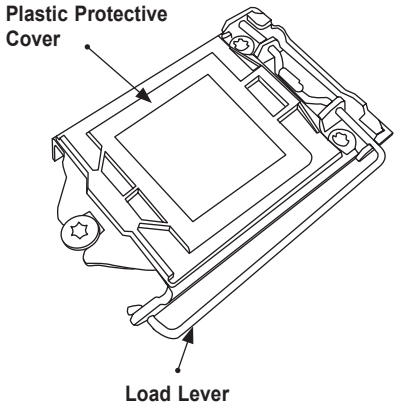
Warning: When handling the processor package, avoid placing direct pressure on the label area of the fan.

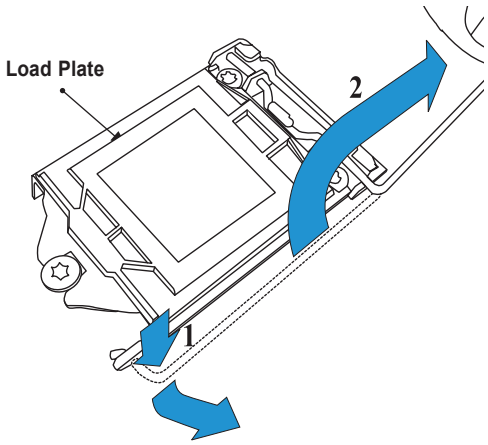
Important:

- Use ESD protection.
- Unplug the AC power cord from all power supplies after shutting down the system.
- Check that the plastic protective cover is on the CPU socket and none of the socket pins are bent. If they are, contact your retailer.
- When handling the processor, avoid touching or placing direct pressure on the LGA lands (gold contacts). Improper installation or socket misalignment can cause serious damage to the processor or CPU socket, which may require manufacturer repairs.
- Thermal grease is pre-applied on a new heatsink. No additional thermal grease is needed.
- Refer to the Supermicro website for updates on processor support.
- All graphics in this manual are for illustrations only. Your components may look different.

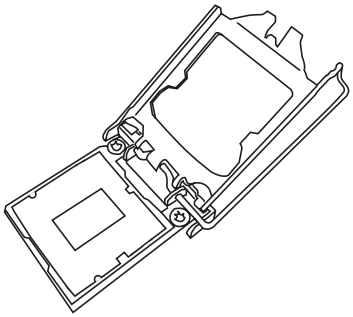
Installing the LGA1200 Processor

1. Press the load lever down to release the load plate from its locking position.

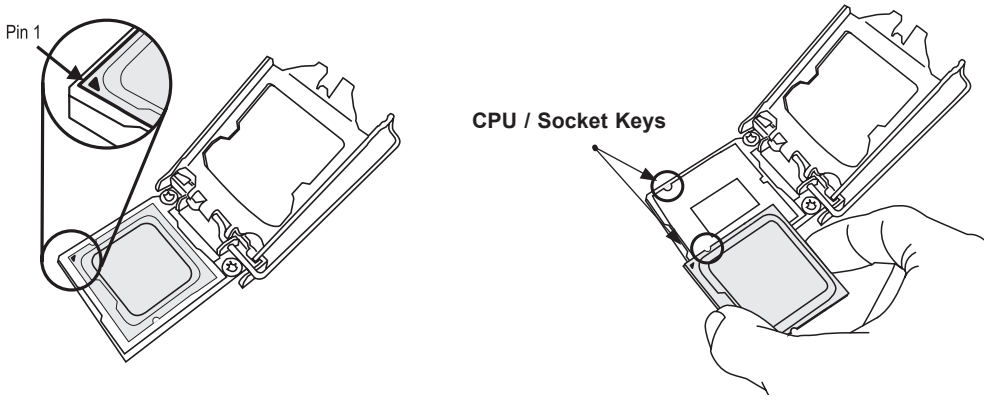




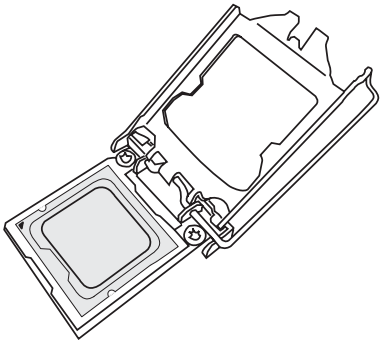
2. Gently lift the load lever to open the load plate. Remove the plastic protective cover. Do not touch the CPU socket contacts.



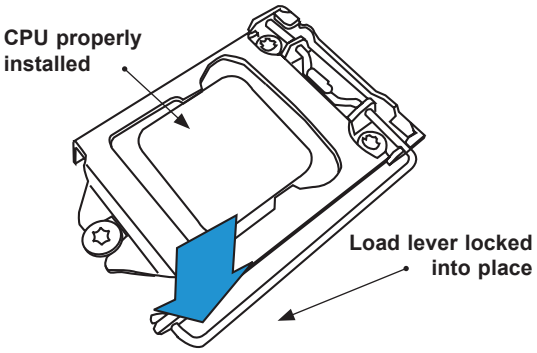
3. Locate the triangle on the CPU and CPU socket, which indicates the location of Pin 1. Holding the CPU by the edges with your thumb and index finger, align the triangle on the CPU with the triangle on the socket. The CPU keys (the semi-circle cutouts) may also be aligned against the socket keys as a guide.



4. Carefully lower the CPU straight down into the socket. Do not drop the CPU on the socket, or move it horizontally or vertically to avoid damaging the CPU or socket. Inspect the four corners of the CPU to make sure that the CPU is properly installed.

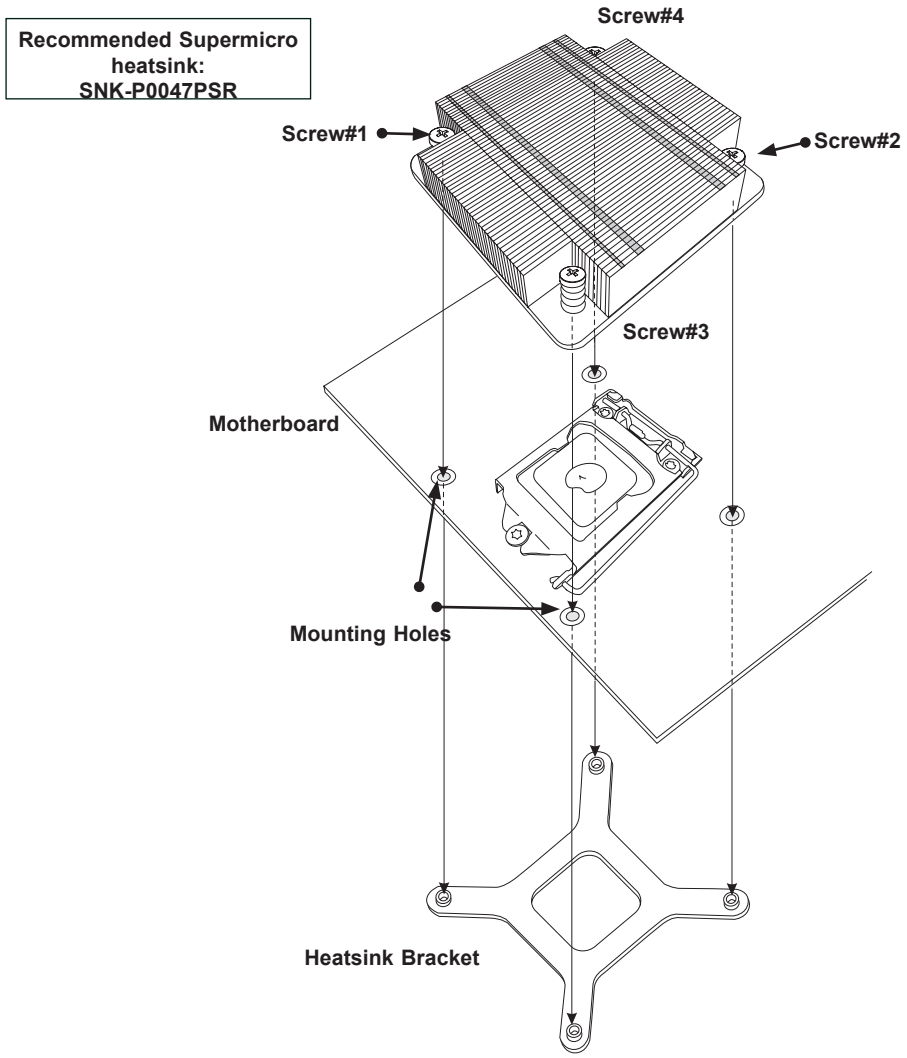


5. Close the load plate, then gently push down the load lever into its locking position.



Installing an Active CPU Heatsink with Fan

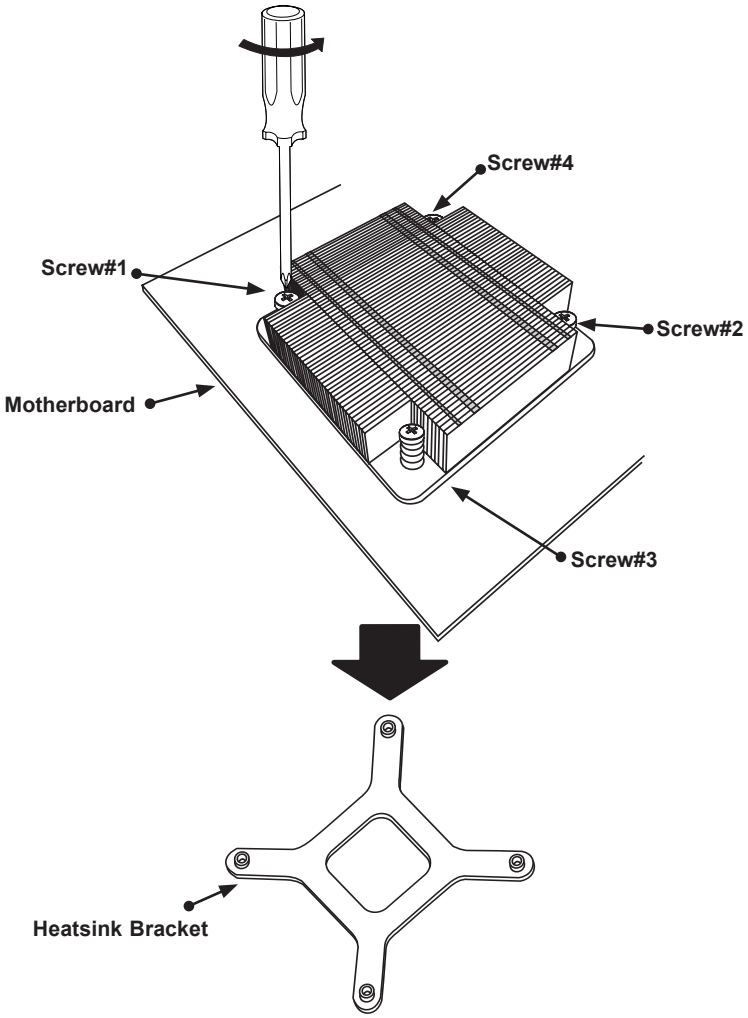
1. Do not apply thermal grease to the heatsink or the CPU; the required amount has already been applied.
2. Align the four holes of the heatsink with the four mounting holes on the motherboard.
3. With a Phillips screwdriver, gradually tighten screws #1, #2, then #3, #4 to ensure even pressure. The order of the screws is shown below. To avoid damaging the processor or socket, do not use a force greater than 12 lbf-in when tightening the screw.
4. Examine all corners to ensure the heatsink is firmly attached to the motherboard.



Removing the Heatsink

Note: We do not recommend that the CPU or heatsink be removed. However, if you do need to remove the heatsink, please follow the instructions below to remove the heatsink and prevent damage done to the CPU or other components.

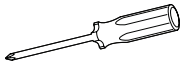
1. Unplug the power connector from the power supply.
2. Unscrew the heatsink screws in the sequence shown below.
3. Gently lift the heatsink up and remove it from the CPU.



2.3 Motherboard Installation

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

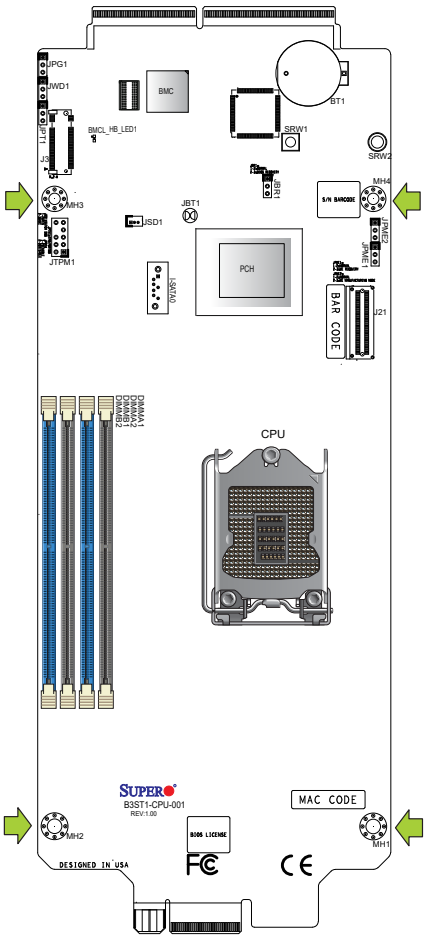
Tools Needed



Phillips Screwdriver (1)

Phillips Screws (4)

Standoffs (4) Only if Needed



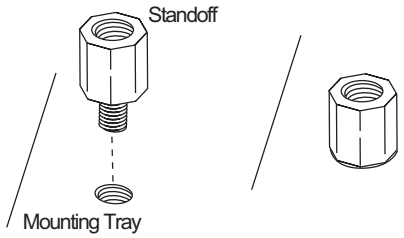
Location of Mounting Holes

Note: 1) To avoid damaging the motherboard and its components, please do not use a force greater than 8 lbf-in 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.

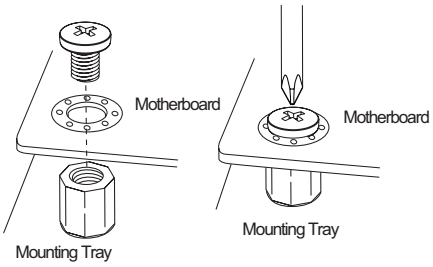
Installing the Motherboard

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.



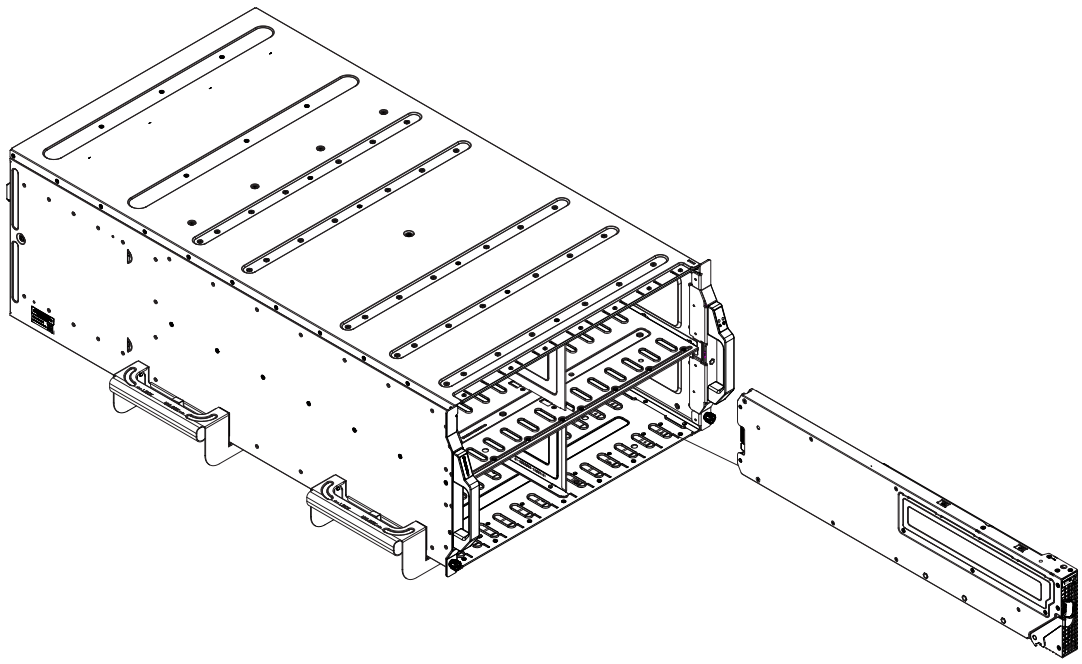
3. Using the Phillips screwdriver, insert a Phillips head #6 screw into a mounting hole on the motherboard and its matching hole on the tray.



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 Microblade Chassis

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



2. Once the mounting tray is pushed in 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.

2.4 Memory Support and Installation

Note: Check the Supermicro website for recommended memory modules.

Important: Exercise extreme care when installing or removing DIMM modules to prevent any possible damage.

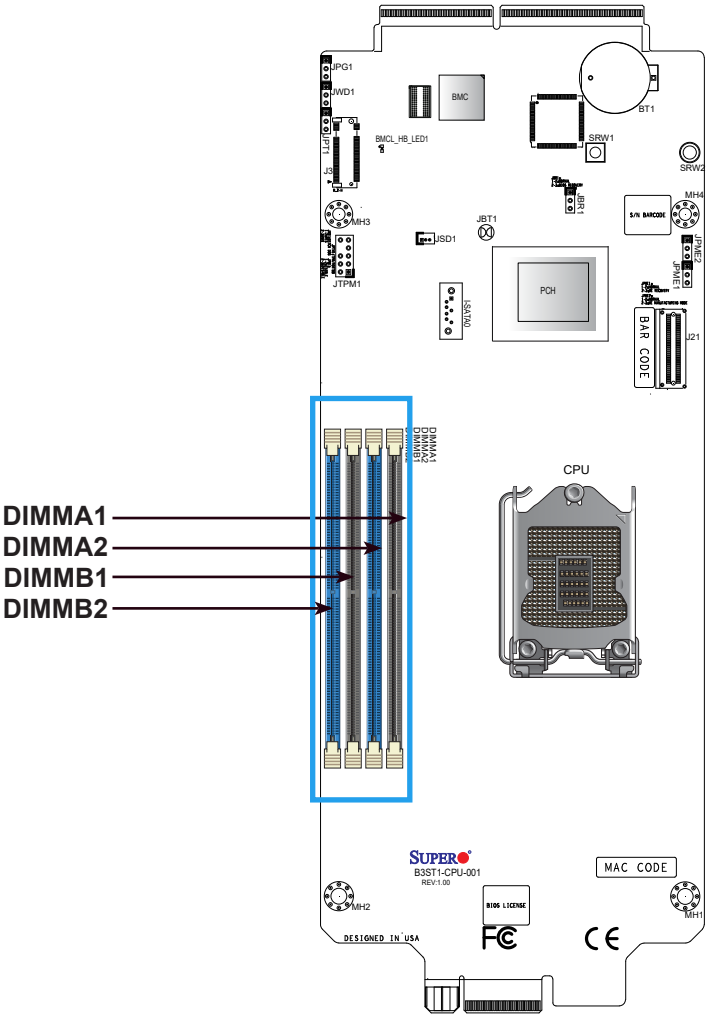
Memory Support

The B3ST1-CPU-001 supports up to 128 GB of ECC and Non-ECC UDIMM memory with speeds of up to 3200 MHz in four memory slots. Refer to the table below for the recommended DIMM population order.

Recommended Population (Balanced)				
DIMMA1	**DIMMB1**	**DIMMA2**	**DIMMB2**	**Total System Memory**
		4 GB	4 GB	8 GB
4 GB	4 GB	4 GB	4 GB	16 GB
		8 GB	8 GB	16 GB
8 GB	8 GB	8 GB	8 GB	32 GB
		16 GB	16 GB	32 GB
16 GB	16 GB	16 GB	16 GB	64 GB
		32 GB	32 GB	64 GB
32 GB	32 GB	32 GB	32 GB	128 GB
		64 GB	64 GB	128 GB

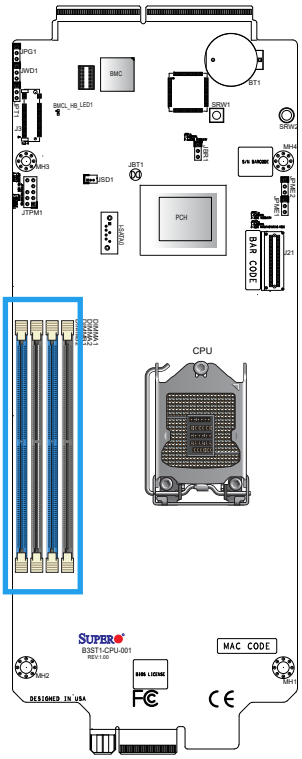
General Guidelines for Optimizing Memory Performance

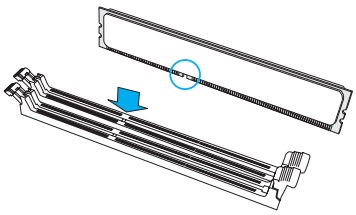
- The blue slots must be populated first.
- Always use DDR4 memory of the same type, size, and speed.
- Mixed DIMM speeds can be installed. However, all DIMMs will run at the speed of the slowest DIMM.
- The motherboard will support odd-numbered modules (one or three modules installed). However, to achieve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



DIMM Installation

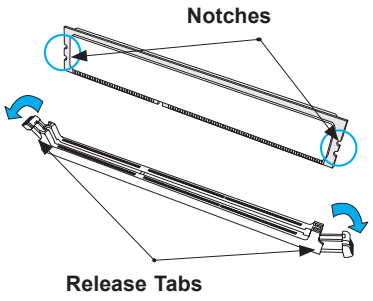
1. Insert DIMM modules in the following order: DIMMB2, DIMMA2, then DIMMB1, DIMMA1. For the system to work properly, please use memory modules of the same type and speed.
2. Push the release tabs outwards on both ends of the DIMM slot to unlock it.
3. Align the key of the DIMM module with the receptive 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. Push 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.

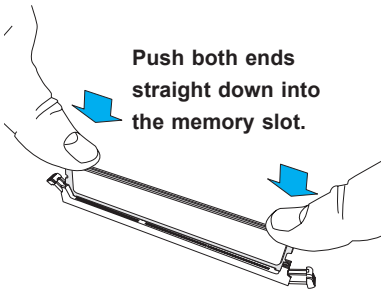




DIMM Removal

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



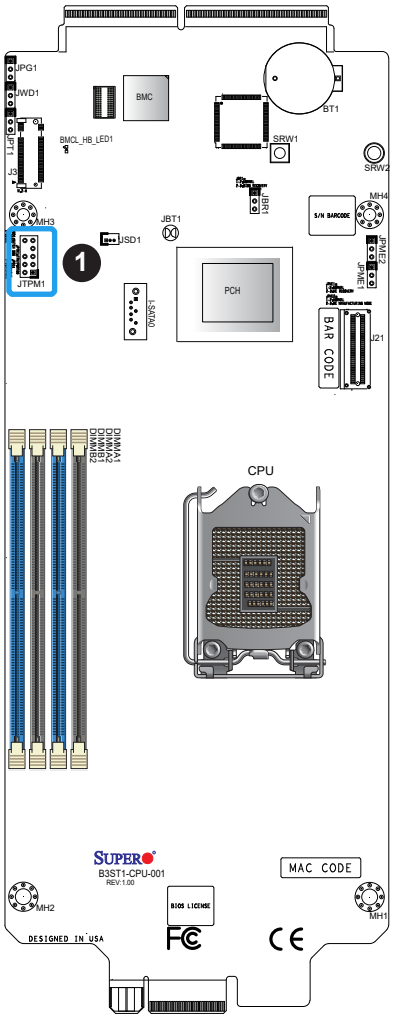


2.5 Connectors

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. Go to the following link for more information on the TPM: http://www.supermicro.com/manuals/other/TPM.pdf.

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



1. TPM Header

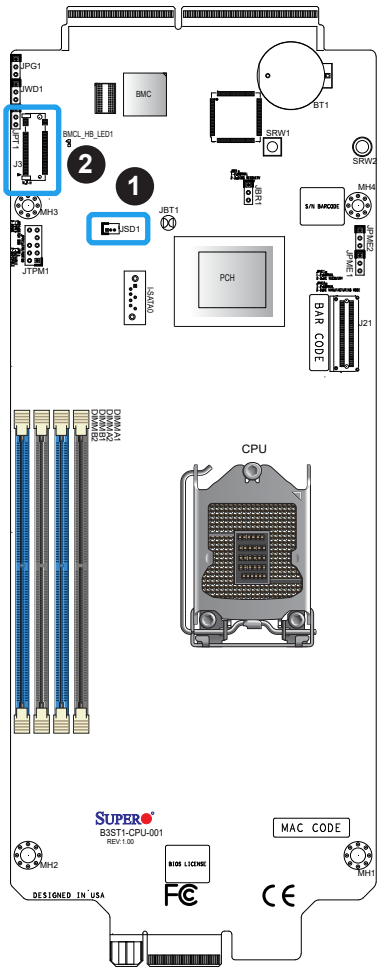
Disk-On-Module Power Connector

One power connector for SATA DOM (Disk-On-Module) devices is located at JSD1. Connect the appropriate cables here to provide power support for your Serial Link DOM devices.

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

M.2 Slot

This motherboard has one M.2 slot (J3). M.2 was formerly known as Next Generation Form Factor (NGFF) and serves to replace mini PCIe. M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency. The M.2 slot supports PCIe 4.0 x4/SATA 3.0 (32 Gb/s) SSD cards in the 2280 and 22110 form factors.

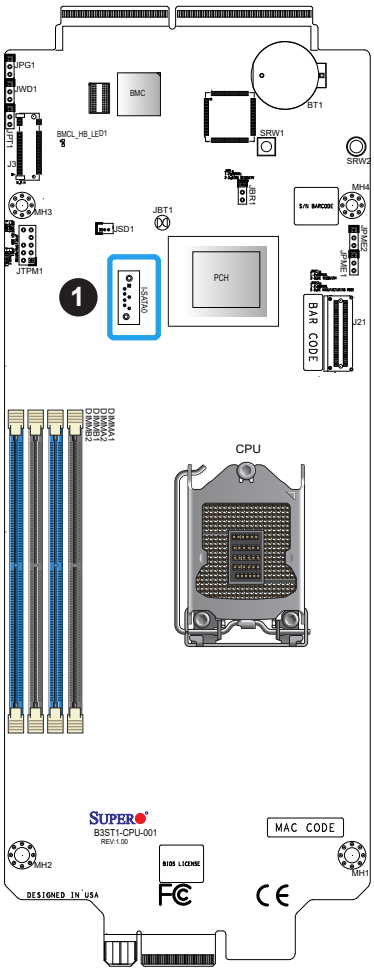


1. SATA DOM
2. M.2 Slot

SATA Port

There is one SATA 3.0 port (I-SATA0) on the motherboard, which provides connections for five SATA 3.0 (RAID 0, 1, 5, 10), with four to 2.5" SATA BPN and one to 3.5" SATA BPN, one SATA 3.0 with DOM power receptacle connector and one SATA 3.0 right angle receptacle connector. SATA ports provide serial-link signal connections, which are faster than legacy Parallel ATA. Supermicro SuperDOMs are backward compatible with regular SATA HDDs or SATA DOMs that need external power cables. Set J3 to pins 1–2 to use the SATA port as onboard SATA or pins 2–3 as AOC SAS.

Note: For more information on the SATA HostRAID configuration, refer to the Intel SATA HostRAID user's guide posted at https://www.supermicro.com/support/manuals/.



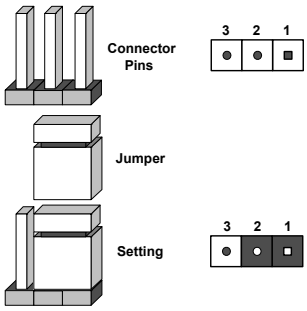
1. I-SATA0

2.6 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 below for an example of jumping pins 1 and 2. Refer to the motherboard layout page for jumper locations.

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



CMOS Clear

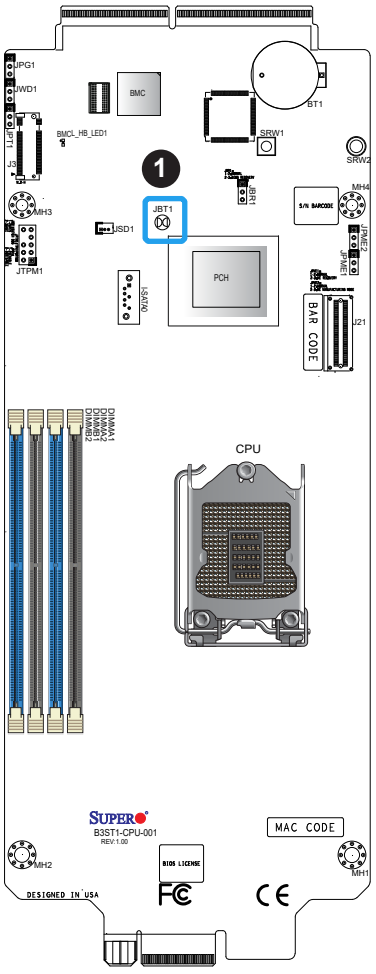
JBT1 is used to clear CMOS, which will also clear any passwords. Instead of pins, this jumper consists of contact pads to prevent accidentally clearing the contents of CMOS.

To Clear CMOS

1. First power down the system and unplug the power cord(s).
2. Remove the cover of the chassis to access the motherboard.
3. Remove the onboard battery from the motherboard.
4. Short the CMOS pads 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(s), and power on the system.

Note: Clearing CMOS will also clear all passwords.

JBT1 contact pads

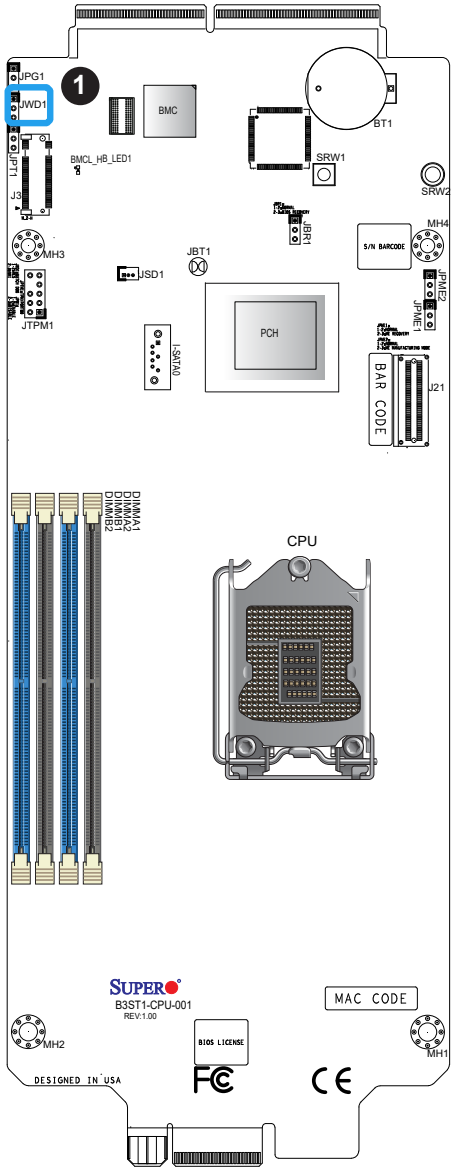


1. CMOS Clear

Watchdog

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

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



1. Watch Dog

Onboard TPM2.0 Enable/Disable

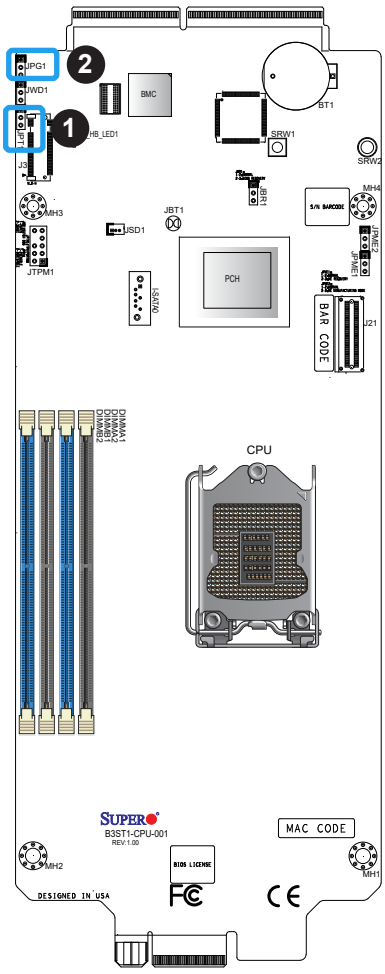
Use JPT1 to enable or disable support for the onboard TPM 2.0 module. The default setting is Enabled.

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

VGA Enable/Disable

Use jumper JPG1 to enable or disable the VGA port using the onboard graphics controller.

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



1. TPM Enable/Disable
2. VGA Enable/Disable

ME Recovery

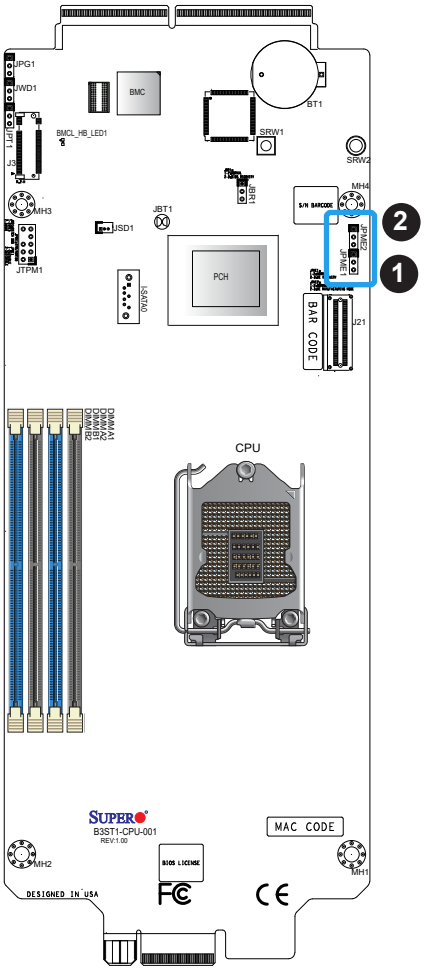
JPME1 is used for ME Firmware Recovery mode, which will limit system resource for essential function use only without putting restrictions on power use. In the single operation mode, online upgrade will be available via Recovery mode. Refer to the table below for pin definitions.

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

ME Manufacturing Mode

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

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



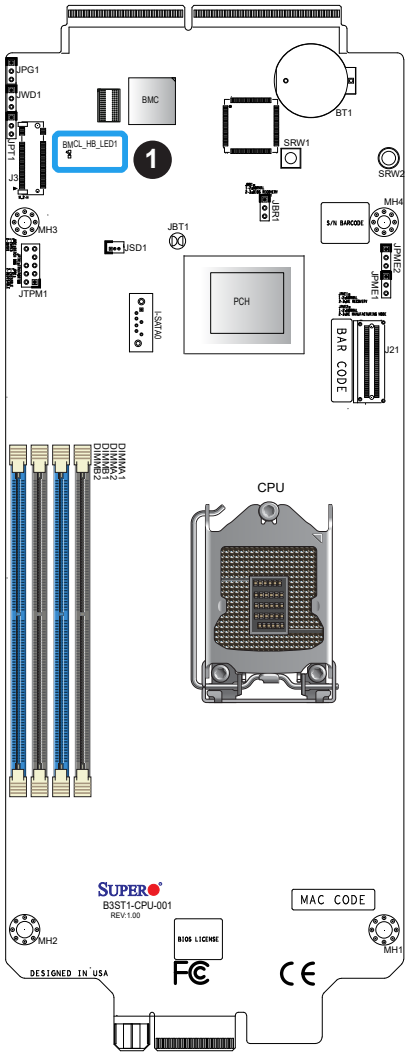
1. ME Recovery
2. Manufacturing Mode

2.9 LED Indicators

BMC Heartbeat LED

BMCL-HB-LED1 is the BMC Heartbeat LED. When the LED is blinking green, BMC is working. Refer to the table below for the LED status.

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



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

No Power

1. Make sure that there are no short circuits between the motherboard and the chassis.
2. Make sure that the ATX power connectors are properly connected.
3. Check that the 115V/230V switch, if available, on the power supply is properly set.
4. Turn the power switch on and off to test the system, if applicable.
5. The battery on your motherboard may be old. Check to verify that it still supplies approximately 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 add-on cards and cables.
2. Use the speaker to determine if any beep codes are present. Refer to Appendix A for details on beep codes.
3. Remove all memory modules and turn on the system (if the alarm is on, check the specs of memory modules, reset the memory or try a different one).

System Boot Failure

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

1. Check for any error beep 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 Section 2-8 in 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

When a no-memory beep code is issued by the system, check the following:

1. Make sure that the memory modules are compatible with the system and are properly installed. See Chapter 2 for installation instructions. (For memory compatibility, refer to the "Tested Memory List" link on the motherboard's product page to see a list of supported memory.)
2. Check if different speeds of DIMMs have been installed. It is strongly recommended that you use the same RAM type and speed for all DIMMs in the system.
3. Make sure that you are using the correct type of Non-ECC DDR4 modules recommended by the manufacturer.
4. Check for bad DIMM modules or slots by swapping a single module among all memory slots and check the results.

Losing the System's Setup Configuration

1. Make sure that you are using a high-quality power supply. A poor-quality power supply may cause the system to lose the CMOS setup information. Refer to Chapter 2 for details on recommended power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 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's 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 in the BIOS 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/DVD.
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 the 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, please note that as a motherboard manufacturer, Supermicro also sells motherboards through its channels, so it is best to first check with your distributor or reseller for troubleshooting services. They should know of any possible problems with the specific system configuration that was sold to you.

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

- Motherboard model and PCB revision number
- BIOS release date/version (This can be seen on the initial display when your system first boots up.)
- System configuration

4. An example of a Technical Support form is on our website at http://www.supermicro.com/RmaForm/.
5. Distributors: For immediate assistance, please have your account number ready when placing a call to our Technical Support department. We can be reached by email at support@supermicro.com.

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: The motherboard supports up to 128 GB of Non-ECC UDIMM DDR4 memory with speeds of up to 3200 MHz in four memory slots. To enhance memory performance, do not mix memory modules of different speeds and sizes. Please follow all memory installation instructions given on Section 2-4 in Chapter 2.

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. 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 bootable USB device. Run the batch file using the format FLASH.BAT filename.rom from your bootable USB device to flash the BIOS. Then, your system will automatically reboot.

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

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

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. Locate the onboard battery as shown below.
3. Using a tool such as a pen or a small screwdriver, push the battery lock outwards to unlock it. Once unlocked, the battery will pop out from the holder.
4. Remove the battery.

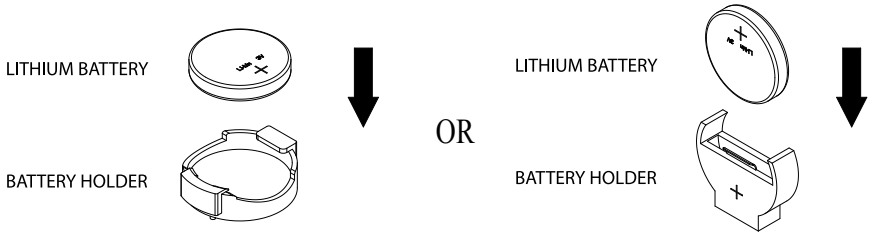
Proper Battery Disposal

Warning: 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 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.

Warning: 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 the motherboard to the manufacturer, the RMA number should be prominently displayed on the outside of the shipping carton, and the shipping package is mailed prepaid or hand-carried. Shipping and handling charges will be applied for all orders that must be mailed when service is complete. For faster service, you can also request a RMA authorization online (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 alternation, misuse, abuse or improper maintenance of products.

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

Chapter 4

BIOS

4.1 Introduction

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

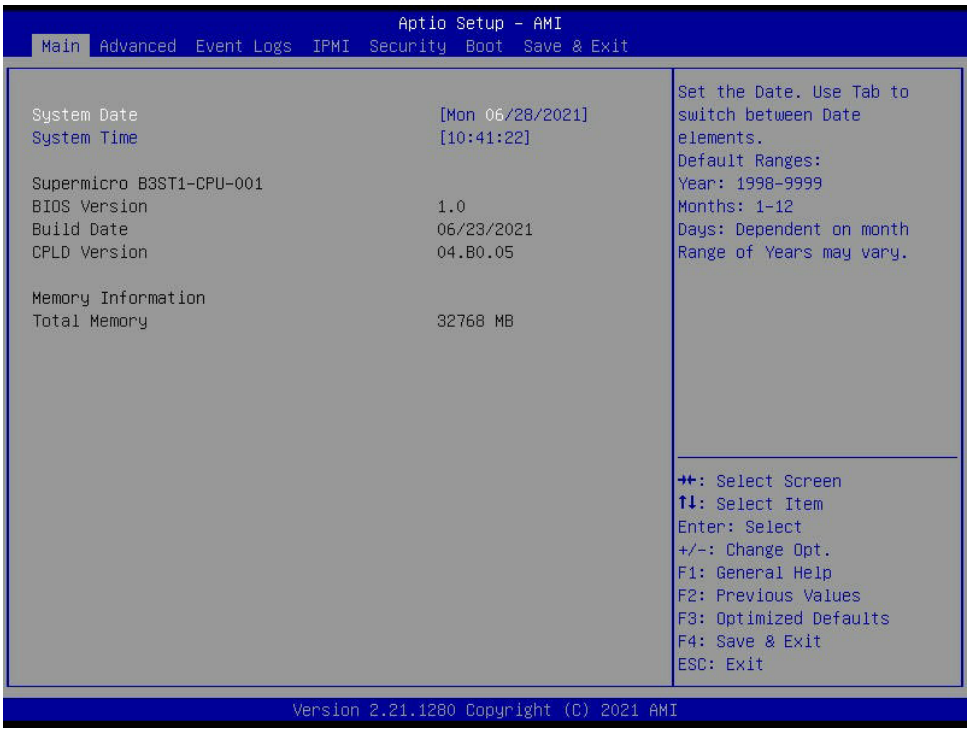
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. “Grayed-out” options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message 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 opens 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>, <F10>, <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 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. The following Main menu items be displayed:



System Date/System Time

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

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

Supermicro B3ST1-CPU-001

BIOS Version

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

Build Date

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

CPLD Version

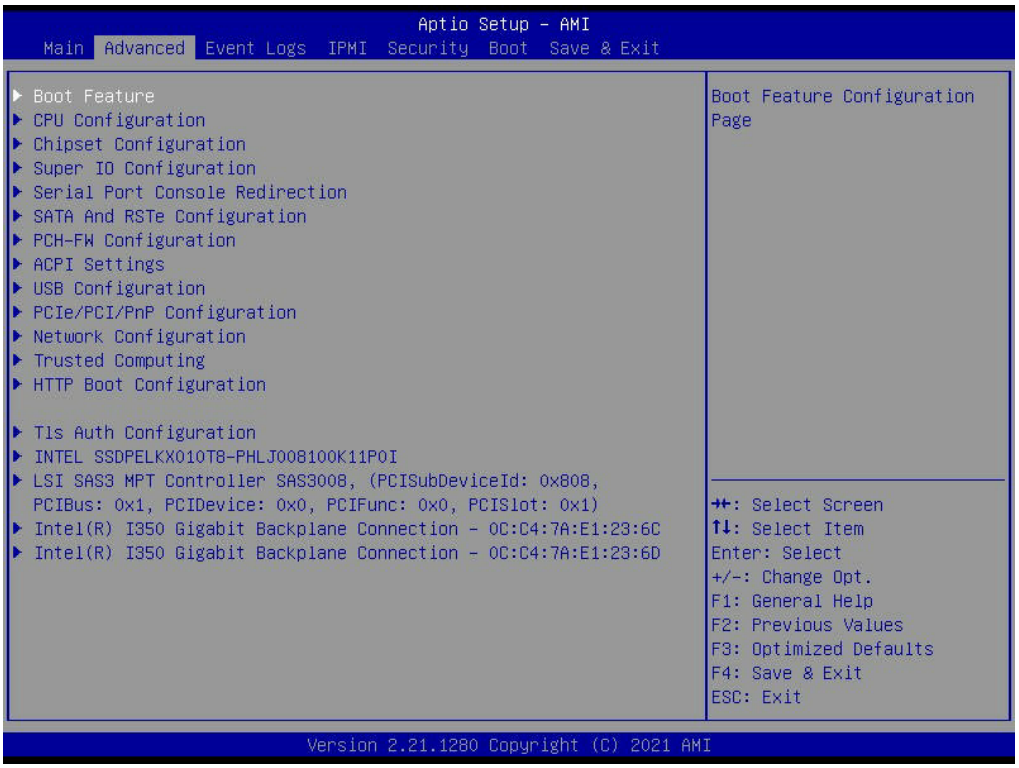
Memory Information

Total Memory

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

4.3 Advanced

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



Warning: Take caution when changing the Advanced settings. An incorrect value, a very high DRAM frequency, or an incorrect DRAM timing setting may make the system unstable. When this occurs, revert to the default to the manufacture default settings.

▶Boot Feature

Quiet Boot

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

Option ROM Messages

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

Bootup NumLock State

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

Wait For "F1" If Error

Use this feature to force the system to wait until the F1 key is pressed if an error occurs. The options are Disabled and **Enabled**.

Interrupt 19 Capture

Interrupt 19 is the software interrupt that handles the boot disk function. When this feature is set to Immediate, the ROM BIOS of the host adaptors capture Interrupt 19 at boot up immediately and allow the drives that are attached to these host adaptors to function as bootable disks. If this feature 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 boot up. The options are **Immediate** and Postponed.

Re-try Boot

If this feature is enabled, the BIOS automatically reboots the system from a specified boot device after its initial boot failure. The options are **Disabled**, Legacy Boot, and EFI Boot.

NMI on Uncorrectable Memory Error

Uncorrectable memory error will trigger NMI. The options are Disabled and **Enabled**.

Power Configuration

Watch Dog Function

If enabled, the Watch Dog Timer allows the system to reset or generate NMI based on jumper settings when it is expired for more than five minutes. The options are **Disabled** and Enabled.

Restore on AC Power Loss

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

Power Button Function

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

▶CPU Configuration

The following CPU information is displayed:

- Type
- CPU Signature
- Microcode Revision
- CPU Speed
- L1 Data Cache
- L1 Instruction Cache
- L2 Cache
- L3 Cache
- VMX
- SMX/TXT

CPU Flex Ratio Override

Use this feature to enable or disable CPU Flex Ratio Prgoramming. The options are **Disabled** and Enabled.

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

CPU Core Flex Ratio

Use this feature to set the non-turbo mode processor core ratio multiplier. The default value is **32**.

Hardware Prefetcher (Available when supported by the CPU)

If set to Enabled, the hardware prefetcher prefetches streams of data and instructions from the main memory to the L2 cache to improve CPU performance. The options are **Enabled** and Disabled.

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 **Enabled**. The options are **Enabled** and Disabled.

Intel (VMX) Virtualization Technology

Select Enable to enable the Intel Vanderpool Technology for Virtualization platform support, which will allow multiple operating systems to run simultaneously on the same computer to maximize system resources for performance enhancement. The options are Disabled and **Enabled**.

PECI

This feature allows you to enable or disable Platform Environment Control Interface (PECI). The options are Disabled and **Enabled**.

AVX

Use this feature to enable or disable the AVX 2/3 instructions. This is applicable for Big Core only. The options are Disabled and **Enabled**.

AVX3

Use this feature to enable or disable the AVX 3 instructions. This is applicable for Big Core only. The options are Disabled and **Enabled**.

Active Processor Cores

This feature determines how many CPU cores will be activated for each CPU. When all is selected, all cores in the CPU will be activated. The options are **All**, 1, 2, 3, 4, 5, 6, and 7.

Hyper-threading

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

BIST

This feature allows you to enable or disable BIST (Built-In Self Test) on reset. The options are **Disabled** and Enabled.

AP threads Idle Manner

AP threads Idle Manner for waiting signal to run. The options are HALT Loop, **MWAIT Loop**, and RUN Loop.

AES

Select Enabled to enable Intel CPU Advanced Encryption Standard (AES) Instructions for CPU to enhance data integrity. The options are **Enabled** and Disabled.

MachineCheck

Use this feature to enable or disable Machine Check. The options are Disabled and **Enabled**.

Monitor/Mwait

Select Enabled to enable the Monitor/Mwait instructions. The Monitor instructions monitors a region of memory for writes, and MWait instructions instruct the CPU to stop until the monitored region begins to write. The options are Disabled and **Enabled**.

▶ Power & Performance Configuration

▶CPU - Power Management Control

Use this feature to enable or disable processor power management features.

Boot Performance Mode

This feature allows you to select the performance state that the BIOS will set from reset vector. The options are Power Saving, Max Non-Turbo Performance and **Turbo Performance**.

Intel® SpeedStep™

Intel SpeedStep Technology allows the system to automatically adjust processor voltage and core frequency to reduce power consumption and heat dissipation. The options are Disabled and **Enabled**.

Intel® Speed Shift Technology

Use this feature to enable or disable Intel Speed Shift Technology support. When this feature is enabled, the Collaborative Processor Performance Control (CPPC) version 2 interface will be available to control CPU P-States. The options are **Disabled**, Out of Band mode and Native Mode.

Per Core P State OS control mode

Use this feature to enable or disable Per Core P State OS control mode. Disabling will set Bit 31 = 1 command 0x06. When set, the highest core request is used for all other core request. The options are Disabled and **Enabled.**

HwP Autonomous Per Core P State

Disabling Autonomous PCPS will request the same value for all cores all the time. The options are Disabled and **Enabled**.

HwP Autonomous EPP Grouping

Enable EPP grouping autonomous will request the same values for all cores with EPP. Disabling EPP grouping autonomous will not necessarily request the same values for all cores with EPP. The options are Disabled and **Enabled**.

Turbo Mode

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

Power Limit 1

Use this feature to enable or disable Platform Power Limit 1 programming. If enabled, it activates the PL1 value to be used by the processor to limit the average power of given time window. The options are **Disabled** and Enabled.

Power Limit 2

Use this feature to enable or disable Platform Power Limit 2 programming. If disabled, it BIOS will program the default values for Platform Power Limit 2. The options are **Disabled** and Enabled.

Power Limit 3 Override

Use this feature to enable or disable Power Limit 3 override. Power Limit 3 Lock needs to disable for power Limit 3 override. If disabled, BIOS will leave the hardware default values for Power Limit 3. The options are **Disabled** and Enabled.

Power Limit 4 Override

Use this feature to enable or disable Platform Power Limit 4 programming. If disabled, BIOS will program the default values for Platform Power Limit 4. The options are **Disabled** and Enabled.

C States

Use this feature to enable or disable CPU power management and allows CPU to go to C states when it is not 100% utilized. The options are Disabled and **Enabled**.

Enhanced C-states

Use this feature to enable the enhanced C-State of the CPU. The options are Disabled and **Enabled**.

C-State Auto Demotion

Use this feature to prevent unnecessary excursions into the C-states to improve latency. The options are Disabled and **C1**.

C-State Un-Demotion

This feature allows you to enable or disable the un-demotion of C-State. The options are Disabled and **C1.**

Package C-State Demotion

Use this feature to enable or disable the Package C-State demotion. The options are Disabled and **Enabled**.

Package C-State Un-Demotion

Use this feature to enable or disable the Package C-State un-demotion. The options are Disabled and **Enabled**.

C-State Pre-Wake

This feature allows you to enable or disable the C-State Pre-Wake. The options are Disabled and **Enabled**.

IO MWait Redirection

This feature maps IO_read instructions sent to the IO registers. The options are **Disabled** and Enabled.

Package C-State Limit

Use this feature to set the Package C-State limit. The options are C0/C1, C2, C3, C6, C7, C7s, C8, C9, C10, Cpu Default, and **Auto**.

ACPI T-States

Use this feature to enable or disable ACPI T-States. The options are Disabled and **Enabled**.

▶ SGX Settings

SW Guard Extensions (SGX)

Use this feature to enable or disable Intel Software Guard Extensions (SGX). SGX is a set of CPU instructions that increases software security. The options are Software Controlled, Enabled, and **Disabled.**

▶Chipset Configuration

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

▶System Agent (SA) Configuration

- VT-d (supported)

▶Memory Configuration

The following memory information will display:

- Memory RC Version
- Memory Frequency
- Memory Timings (tCL-tRCD-tRP-tRAS)
- Memory Timings
- DIMMA1
- DIMMA2
- DIMMB1
- DIMMB2
    - Number of Ranks
    - Manufacturer

DDR Speed Control

Use this feature to set the DDR speed. The options are **Auto** and Manual.

Maximum Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 1067, 1200, 1333, 1400, 1600, 1800, 1867, 2000, 2133, 2200, 2400, 2600, 2667, 2800, 2933, 3000, and 3200.

ECC Support

This feature allows you to enable or disable DDR ECC support. The options are Disable and **Enable**.

Max TOLUD

This feature sets the maximum TOLUD value, which specifies the "Top of Low Usable DRAM" memory space to be used by internal graphics devices, GTT Stolen Memory, and TSEG, respectively, if these devices are enabled. The options are **Dynamic**, 1 GB, 1.25 GB, 1.5 GB, 1.75 GB, 2 GB, 2.25 GB, 2.5 GB, 2.75 GB, 3 GB, 3.25 GB, and 3.5 GB.

SA GV High Gear

This feature enables Gear Selection for SAGV High point, or when SAGV is disabled. The options are Gear1 and **Gear2**.

Retrain on Fast Fail

This feature restarts MRC in Cold mode if SW MemTest fails during Fast flow. The options are Disable and **Enable**.

Enable RH Prevention

Use this feature to actively prevent row hammer. The options are **Disabled** and Enabled.

Power Down Mode

Use this feature to manage CKE Power Down Mode Control. The options are **Auto**, No Power Down, APD, and PPD-DLLoff.

Power Down Idle Timer

Use this feature to schedule power down after the system has been idle. The minimum value should equal to the worst case Roundtrip delay plus Burst_Length. The value 0 means Auto: 64 for ULX/ULT, 128 for DT/Halo. The default setting is 0.

Memory Scrambler

Use this feature to enable or disable memory scrambler support. The options are Disable and **Enable**.

Force ColdReset

Use this feature to enable or disable a cold boot during a MRC execution. The options are Enabled and **Disabled**.

Force Single Rank

Select enabled to use only Rank 0 in each DIMM. The options are **Disabled** and Enabled.

Fast Boot

Use this feature to enable or disable fast path through the memory reference code (MRC). The options are Disabled and **Enabled**.

Train on Warm Boot

Use this feature to enable or disable training on warm boot. The options are **Disable** and Enable.

Memory Test on Warm Boot

Use this feature to enable or disable base memory test run on warm boot. The options are **Disable** and Enable.

REFRESH_2X_MODE

Use this feature to enable 2x memory refresh support to enhance memory performance. The options are **Disabled**, 1- Enabled for WARM or HOT, and 2- Enabled HOT only.

▶DMI Configuration

DMI Max Link Speed

Use this feature to set the DMI speed. The options are **Gen3**, Gen2, and Gen1.

DMI Gen3 ASPM Control

Use this feature to enable DMI Gen3 ASPM Control Support. The options are Disabled, **Auto**, ASPM L0s, ASPM L1 and ASPM L0sL1.

DMI De-emphasis Control

Use this feature to configure the De-emphasis control on DMI. The options are **-3.5 dB** and -6 dB.

▶PEG Port Configuration

PCI Express Root Port 1/ Port 2/ Port3/ Port4

Use this feature to control the PCIe Root Port. The options are Disabled and **Enabled**.

ASPM

Use this feature to set the Active State Power Management (ASPM) level for a PCIe device. Select Auto for the system BIOS to automatically set the ASPM level based on the system configuration. Select Disabled to disable ASPM support. The options are Disabled, L0s, **L1**, and L0sL1.

PCIe Speed

Use this to configure PCIe speed. The options are **Auto,** Gen1, Gen2, Gen3 and Gen4

Internal Graphics

Keep IGFX enabled based on the setup options. The options are **Disable** and Enable.

Stop Grant Configuration

This feature controls automatic/manual Stop Grant configuration. The options are Manual and **Auto**.

VT-d

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

X2APIC Opt Out

Use this feature to enable or disable X2APIC_OPT_Out bit. The options are **Disable** and Enable.

DMA Control Guarantee

Use this feature to enable or disable DMA_Control_Guarantee bit. The options are **Disabled** and Enabled.

IGD VTD Enable

Use this feature to enable or disable IGD VTD. The options are **Enable** and Disable.

IOP VTD Enable

Use this feature to enable or disable IOP VTD. The options are **Enable** and Disable.

Thermal Device

Use this feature to enable or disable SA thermal device. Always enable for ICL A0 stepping. The options are Enable and **Disable**.

GNA Device (B0:D8:F0)

Use this feature to enable or disable SA GNA device. The options are **Enable** and Disable.

▶PCH-IO Configuration

PCH-IO Configuration

▶PCI Express Configuration

Peer Memory Write Enable

Use this feature to enable or disable peer memory write. The options are **Disabled** and Enabled.

▶PCI Express Root Port (1 ~ 24)

This submenu allows you to configure each PCIe Root port. Click on each available port and configure the settings accordingly. The options are Disabled and **Enabled**.

ASPM

Use this feature to activate the Active State Power Management (ASPM) level for a PCIe device. Select Auto for the system BIOS to automatically set the ASPM level based on the system configuration. Select Disabled to disable ASPM support. The options are Disabled, L0s, L1, L0sL1, and **Auto**.

L1 Substrates

Use this feature to configure the L1 substates . The options are Disabled, L1.1, and **L1.1 & L1.2**.

PCIe Speed

Use this feature to select the PCIe speed. The options are **Auto**, Gen1, Gen2, Gen3, and Gen4.

Port 61h Bit-4 Emulation

Use this feature to enable or disable emulation of Port 61fh bit-4 toggling in SMM. The options are **Disabled** and Enabled.

PCIe PLL SSC

Use this feature to enable or disable PCIe PLL spread spectrum clocking. The options are **Enable** and Disable.

▶Super IO Configuration

The following Super IO information is displayed:

- Super IO Chip AST2500

▶Serial Port 1 Configuration

This submenu allows you to configure the settings of Serial Port 1.

Serial Port

Select Enabled to enable the selected onboard serial port. The options are Disabled and **Enabled**.

Device Settings

This feature displays the status of the serial port.

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of the serial port. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. 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

This submenu allows you to configure the settings of Serial Port 2.

Serial Port

Select Enabled to enable the selected onboard serial port. The options are Disabled and **Enabled**.

Device Settings

This feature displays the status of the serial port.

Change Settings

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

▶Serial Port Console Redirection

COM1 Console Redirection

Select Enabled to enable console redirection support for the serial port. The options are Enabled and **Disabled**.

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

▶COM1 Console Redirection Settings

Use this feature to specify how the host computer exchanges data with the client computer.

Terminal Type

This feature allows you 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 (Bits) and **8 (Bits)**.

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

SOL/COM2 Console Redirection

Select Enabled to use the 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:

▶SOL Console Redirection Settings

Use this feature to specify how the host computer exchanges data with the client computer.

Terminal Type

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

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

▶Legacy Console Redirection Settings

Redirection COM Port

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

Legacy OS Redirection Resolution

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

Redirection After BIOS POST

Use this feature to enable or disable legacy Console Redirection after BIOS POST. When 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.

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

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

Console Redirection EMS (Emergency Management Services)

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

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

▶Console Redirection Settings

This feature allows you to specify how the host computer exchanges 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** and SOL.

Terminal Type EMS

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

Bits Per Second EMS

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

Flow Control EMS

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

Data Bits EMS, Parity EMS, Stop Bits EMS

▶SATA And RSTe 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

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

Aggressive LPM Support

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

Serial ATA Port 0-7

Port 0-7 Hot Plug

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

Port 0-7 Spin Up Device

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

Port 0-7 SATA Device Type

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

▶PCH-FW Configuration

The following firmware information is displayed:

- General ME Configuration
- Oper. Firmware Version
- Backup Firmware Version
- Recovery Firmware Version
- ME Firmware Status #1
- ME Firmware Status #2
  - Current State
  - Error Code

▶ACPI Settings

High Precision Event Timer

Select Enabled to activate the High Performance 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 **Enabled** and Disabled.

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.

▶USB Configuration

- USB Configuration
- USB Module Version
- USB Controllers
- USB Devices

Legacy USB Support

This feature enables support for USB 2.0 and older. The options are **Enabled,** Disabled, and Auto.

XHCI Hand-off

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

USB Mass Storage Driver Support

Select Enabled for USB mass storage device support. The options are Disabled and **Enabled**.

USB Hardware Delays and Time-outs:

USB Transfer Time-out

Use this feature to set the timeout value for Control, Bulk, and Interrupt transfers. The options are 1 sec, 5 sec, 10 sec, and **20 sec**.

Device Reset Time-out

Use this feature to set the timeout value for a USB mass storage device. The options are 10 sec, **20 sec**, 30 sec, and 40 sec.

Device Power-up Delay

Use this feature to set the maximum time a device takes to report itself to the host controller. The options are **Auto** and Manual.

▶PCIe/PCI/PnP Configuration

Option ROM Execution

Onboard Video Option ROM

Use this feature to select the onboard video firmware type. The options are Disabled and **EFI**.

Above 4GB MMIO BIOS Assignment (Available if the system supports 64-bit PCI decoding)

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

NVMe Firmware Source

The feature determines which type of NVMe firmware should be used in your system. The options are **Vendor Defined Firmware** and AMI Native Support.

Storage Option ROM/UEFI Driver

Select UEFI to load the EFI driver for system boot. Select Legacy to load a legacy driver for system boot. The options are Do not Launch, U**EFI**, and Legacy.

PCIe/PCI/PnP Configuration

M.2-H PCI-E 3.0 X4 OPROM

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

Intel I350 PCI-E 3.0 X4 OPROM

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

Broadcom 3008 PCI-E 3.0 X8 OPROM

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

▶Network Configuration

Network Stack

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

IPv4 PXE Support

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 is checked. Press "+" or "-" on your keyboard to change the value. The default setting is **1**.

▶MAC:0CC47AE1236C-IPv4 Network Configuration
▶MAC:0CC47AE1236D-IPv4 Network Configuration

Configured

Use this feature to specify whether the network address is configured successfully or not. The options are **Disabled** and Enabled.

Save Changes And Exit

Use this feature to save changes and exit.

▶MAC:0CC47AE1236C-IPv6 Network Configuration
▶MAC:0CC47AE1236D-IPv6 Network Configuration

▶Enter Configuration Menu

- Interface Name
- Interface Type

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

Interface ID

This feature shows the interface ID for the specified network device.

DAD Transmit Count

This feature sends Neighbor Solicitation messages while performing a Duplicate Address Detection (DAD) to make sure there is no IP address duplication. A value of zero means a DAD has not been performed.

Policy

Use this feature to select an automatic or manual policy. The options are **Automatic** and Manual.

Save Changes And Exit

When you have completed the changes for this section, select this option to save all changes made and exit.

▶Trusted Computing

This motherboard supports TPM 1.2 and 2.0. The following Trusted Platform Module (TPM) information displays if a TPM 2.0 module is detected:

- Firmware Version
- Vendor (Name)

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 (Trusted Platform Module) 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**.

- Active PCR Bank
- SHA256 PCR Bank

If the* feature *above is set to Enable, "SHA-1 PCR Bank" and "SHA256 PCR Bank" are available for configuration:

SHA-1 PCR Bank

Use this feature 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 reboots 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 select the Trusted Computing Group (TCG) specification version. Version TCG_1_2 is compatible with Windows 8 and 10. Version TCG_2 is compatible with Windows 10 or later. The options are TCG_1_2 and **TCG_2**.

Physical Presence Spec Version

Use this feature to select the Physical Presence Interface version. This interface uses the ACPI and allows the operating system and BIOS to work together to provide a platform for users to administer the TPM. The options are 1.2 and **1.3**.

PH Randomization

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

TXT Support

Intel Trusted Execution Technology (TXT) 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 **Disable** and Enable.

▶HTTP Boot Configuration

HTTP Boot Configuration

HTTP Boot Policy

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

HTTP Boot Checks Hostname

Use this feature to select whether HTTPS Boot checks the hostname of TLS certificates matches the hostname provided by the remote server. The options are **Enabled** and Disabled (Warning: Security Risk!!)

Priority of HTTP Boot:

Instance of Priority 1:

Use this feature to set the rank target port. The default value is **1**.

Select IPv4 or IPv6

Use this feature to select which LAN port to boot from. The options are **IPv4** and IPv6.

Boot Description

Highlight the feature and press enter to create a boot description. The description cannot be more than 75 characters.

Boot URI

Highlight the feature and press enter to create a boot URI.

▶Tls Auth Configuration

This submenu allows you to configure Transport Layer Security (TLS) settings.

▶Server CA Configuration

▶Enroll Certification

Enroll Certification Using File

Use this feature to enroll certification from a file.

Cert GUID

Use this feature to input the certification GUID.

Commit Changes and Exit

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

Discard Changes and Exit

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

▶Delete Certification

Use this feature to delete certification.

▶INTEL SSDPELKX010T8-PHLJ008100K11P0I

- PCI Generic Information
- Bus Protocol:
- PCI Vendor/Device ID:
- PCI Vendor subsystem id:
- PCI subsystem id:
- Model Number:
- Serial Number:
- IEEE Organization Unique Id:
- PCIe Maximum Link Width:
- PCIe Maximum Speed:
- PCIe Negotiated Link Width:
- PCIe Negotiated Link Speed:
- NVMe Drive Information
- Drive Health:
- Firmware Revision:
- Option ROM Revision:
- Total Drive Capacity:
- Number of Namespaces:
- Namespace Id:

- Device Capacity
- Device Size

▶LSI SAS3 MPT Controller SAS3008, (PCISubDeviceID: 0x808, PCIBus: 0x1, PCIDevice: 0x0, PCIFunc: 0x0, PCISlot: 0x1)

▶View Controller Properties

Select to view Controller properties:

- Chip Name
- Chip Revision
- PCI ID (Bus: Dev: Func)
- Host Interface
- Virtual Disk Count
- Virtual Disk Count
- Firmware Type
- Firmware Version
- Default NVData Version
- Persistent NVData Version

▶Change Controller Properties

Select to change Controller properties.

Rebuilt Rate

Select to change rebuild rate. The options are Default, 1%, 10%, 20%, 30%, 40%, 50%, **60%**, 70%, 80%, 90%, and 100%.

Legacy BIOS

Select current status of Legacy BIOS. Select and apply to modify. The options are Disabled and **Enabled**.

▶Save Controller Events

Select to save events to a file on an external USB disk.

Available File Systems

Use this feature to choose the available file system to save the controller logs.

Available Directories

Use this feature to choose the available directory to save the controller logs. The options are **RootDirectory**, EFI, and System Volume Information.

Enter File Name

Assign a filename to identify the event log.

▶Save Events

Saves the log to the specified file system and directory.

▶OK

Press OK to continue after the operation was completed successfully.

▶Intel(R) I350 Gigabit Backplane Connection - OC:C4:7A:E1:23:6C
▶Intel(R) I350 Gigabit Backplane Connection - OC:C4:7A:E1:23:6D

▶NIC Configuration

Link Speed

This feature allows you to specify the port speed used for the selected boot protocol. The options are **Auto Negotiated**, 10 Mbps Half, 10 Mbps Full, 100 Mbps Half, and 100 Mbps Full.

Wake On LAN

Select Enabled for Wake_On_LAN support, which will allow the system to "wake up" when an onboard device receives an incoming signal. The options are Disabled and **Enabled**.

Blink LEDs

Use this feature to identify the physical network port by blinking the associated LED. Use the keyboard to select a value.

UEFI Driver

This feature displays the UEFI driver version.

Adapter PBA

This feature displays the Processor Bus Adapter (PBA) model number. The PBA number is a nine-digit number (i.e., 010B00-000) located near the serial number.

Chip Type

This feature displays the network adapter chipset name.

PCI Device ID

This feature displays the device ID number.

PCI Bus:Device:Function

Link Status

This feature displays the connection status.

Factory MAC Address

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

Alternate MAC Address

Alternate assigned MAC address of Ethernet port.

4.4 Event Logs

Use this menu to configure Event Log settings.

▶Change SMBIOS Event Log Settings

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase Event Log

If No is selected, data stored in the event log not be erased. Select "Yes, Next Reset," data in the event log will be erased upon next system reboot. Select "Yes, Every Reset," data in the event log will be erased upon every system reboot. The options are **No**, "Yes, Next reset," and "Yes, Every reset."

When Log is Full

Select Erase Immediately for all messages to be automatically erased from the event log when the event log memory is full. The options are **Do Nothing** and Erase Immediately.

SMBIOS Event Log Standard Settings

Log System Boot Event

This option toggles the System Boot Event logging to enabled or disabled. The options are **Disabled** and Enabled.

MECI

The Multiple Event Count Increment (MECI) counter counts the number of occurrences that a duplicate event must happen before the MECI counter is incremented. This is a numeric value. The default value is **1**.

METW

The Multiple Event Time Window (METW) defines the number of minutes must pass between duplicate log events before MECI is incremented. This is in minutes, from 0 to 99. The default value is **60**.

Note: After making changes to a setting, reboot the system for the changes to take effect.

▶View SMBIOS Event Log

This section displays the contents of the SMBIOS Event Log.

4.5 IPMI

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

IPMI 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 you to decide 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: After making changes on a setting, reboot the system for the changes to take effect.

▶BMC Network Configuration

--BMC Network Configuration--

Update IPMI LAN Configuration

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

Configure IPv4 Support

IPMI LAN Selection

Use this feature to select the type of the IPMI LAN. The default setting is **Failover**.

IPMI Network Link Status

This feature displays the status of the IPMI network link for this system. The default setting is **Dedicated LAN**.

Configuration Address Source

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

If the feature above is set to Static, the following 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., 172.29.176.131).

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.

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

Gateway IP Address: This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1).

VLAN: This feature displays the status of VLAN support. The default setting is **Disable**.

Configure IPv6 Support

IPv6 Address Status: (This feature displays the status of IPv6 addresses).

IPv6 Support: IPv6 is supported in BMC. The options are **Enabled** and Disabled.

Configuration Address Source

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

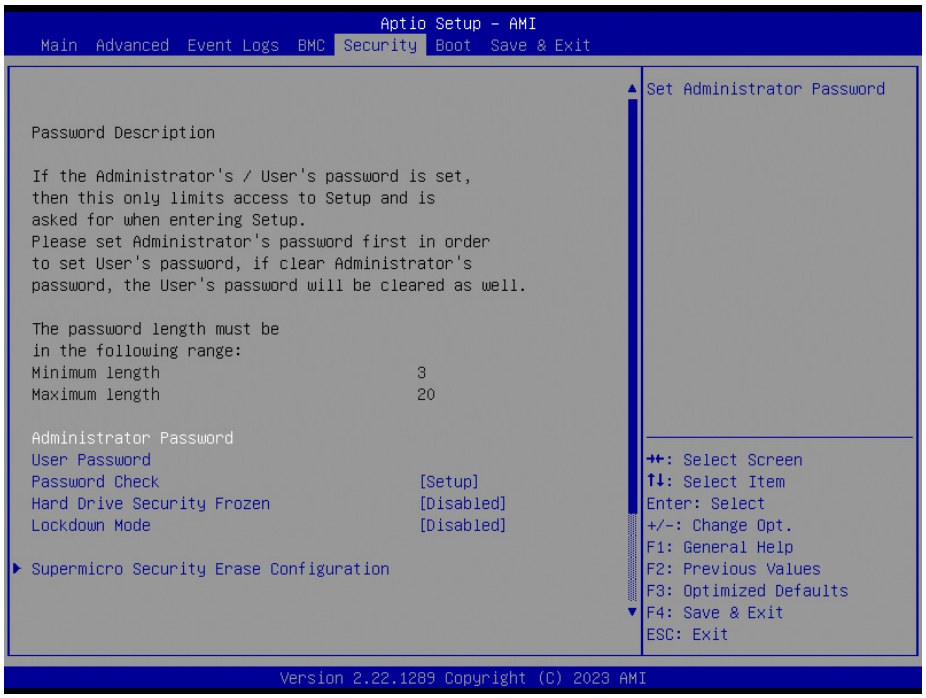
Station IPv6 Address: This feature displays the station IPv6 address.

Prefix Length: This feature displays the prefix length.

IPv6 Router1 IP Address: This feature displays the IP address of the IPv6 router.

4.6 Security

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



Administrator Password

Press Enter to create a new, or change an existing, Administrator password.

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.

Hard Drive Security Frozen

Use this feature to enable or disable the BIOS security frozen command for SATA and NVMe devices. The options are Enable and **Disable**.

▶SMCI Security Erase Configuration

This section allows you to configure the SMCI-proprietary Security Erase settings. When this section is selected, the following features will display:

- HDD Name: This feature displays the name of the HDD/SATA drive that is connected to the SMCI Security Erase Configuration submenu.
- HDD Serial Number: This feature displays the serial number of the HDD/SATA device that is connected to the SMCI Security Erase Configuration submenu.

- Security Mode: SAT3 supported.
- Estimated Time: This feature displays the estimate time needed to perform the selected Security Erase features.
- HDD User Pwd Status: This feature indicates if a password has been set as a SATA user password which will allow you to configure SMCI Security Erase settings on the HDD (SATA) device by using this SATA user password.

Security Function

Select Password to set an HDD/SATA password which will allow you to configure the security settings of the HDD/SATA device. Select Security Erase - Password to enter a SATA user password to allow you to to erase the password and the contents previously stored in the HDD/SATA device. Select Security Erase - Without Password to use the manufacturer default password "111111111" as the SATA user password and allow you to erase the contents of the HDD/SATA device by using this default password. The options are **Disabled**, Set Password, Security Erase-Password, and Security Erase-Without Password.

Password

Use this feature to set the SATA user password which will allow you to configure the SMCI Security Erase settings by using the SATA user password.

▶P0: SATADOM-SH 3ME3 V2

This section is for HDD Security Configuration for selected drives.

▶Secure Boot

This section displays the contents of the following secure boot features:

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

Use this feature to enable secure boot. The options are **Disabled** and Enabled**.**

Secure Boot Mode

Use this feature to configure Secure Boot variables without authentication. The options are Standard and **Custom**.

CSM Support

This feature is used to enable or disable CSM support. The options are Disabled and **Enabled.**

▶Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot key databases.

▶Reset to Setup Mode

This feature deletes all Secure Boot key databases from NVRAM.

▶Enter Audit Mode

This submenu can only be used if current System Mode is set to User (refer to Exit Deployed Mode). The PK variable will be erased on transition to Audit Mode.

▶Key Management

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

Vendor Keys

Provision Factory Defaults

Select Enabled to install factory default Secure Boot keys after the platform reset while the system is in the Setup mode. The options are **Disabled** and Enabled.

▶Restore Factory Keys

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

▶Export Secure Boot Variables

This feature allows you to copy NVRAM content of Secure boot variables to files in a root folder on a file system device.

▶Enroll EFI Image

This feature allows the image to run in Secure Boot Mode. Enroll SHA256 Hash Certificate of the image into the Authorized Signature Database.

Device Guard Ready

▶Remove 'UEFI CA' from DB

This feature allows you to decide if all secure boot variables should be saved.

▶Restore DB Defaults

Select Yes to restore the DB defaults.

Secure Boot Variable

▶Platform Key (PK)

Update

Select Yes to load the new Platform Keys (PK) from the manufacturer's defaults. Select No to load the Platform Keys from a file.

▶Key Exchange Keys

Update

Select Yes to load the KEK from the manufacturer's defaults. Select No to load the Key Exchange Keys from a file.

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.

▶Authorized Signatures

Update

Select Yes to load the DB from the manufacturer's defaults. Select No to load the DB from a file.

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.

▶Forbidden Signatures

Update

Select Yes to load the DBX from the manufacturer's defaults. Select No to load the DBX from a file.

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.

▶Authorized TimeStamps

Update

Select Yes to load the DBT from the manufacturer's defaults. Select No to load the DBT from a file.

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.

▶OsRecovery Signature

Update

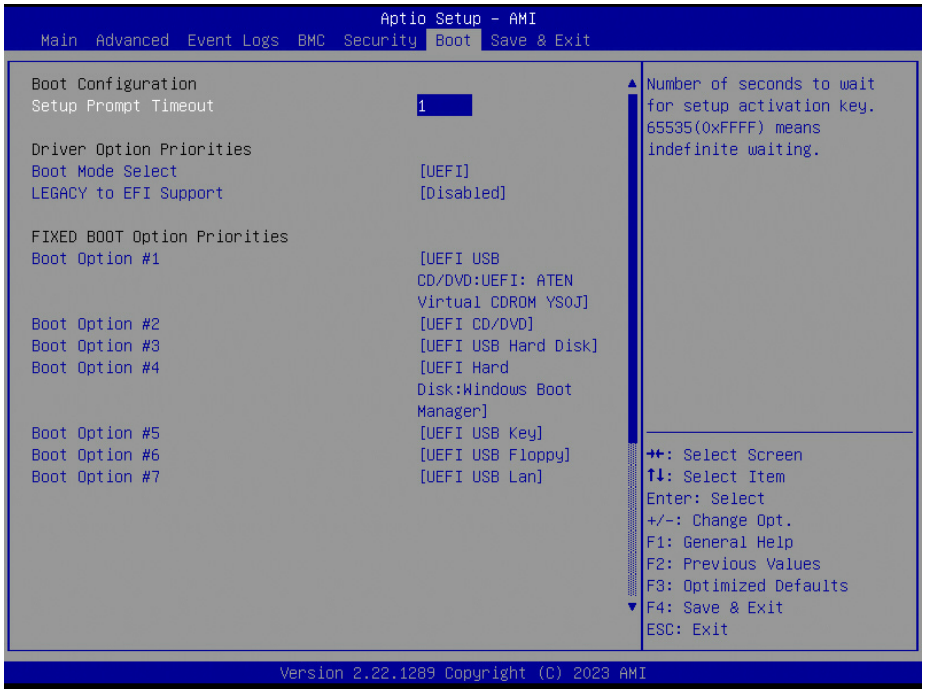
Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file.

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.

4.7 Boot

Use this submenu to configure Boot Settings:



Boot Mode Select

Use this feature to select the type of device that the system is going to boot from. The options are Legacy, **UEFI**, and Dual**.**

FIXED BOOT ORDER Priorities

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

- Boot Option #1
- Boot Option #2
- Boot Option #3
- Boot Option #4
- Boot Option #5
- Boot Option #6
- Boot Option #7
- Boot Option #8
- Boot Option #9

▶Add New Boot Option

Use this feature to add a new UEFI boot option to the boot order.

Add Boot option

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

Path for Boot option

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

Boot Option File Path

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

Create

Use this feature to create the newly formed boot option.

▶Delete Boot Option

This option allows you to select and delete an EFI boot option from the boot order.

Delete Boot Option

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

▶Add New Driver Option

Use this feature to add a new EFI driver option to the driver order for your system.

Add Driver Option

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

Path for Driver Option

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

Boot option File Path

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

Create

Use this feature to create the newly formed driver option.

▶Delete Drive Option

This option allows you to select and delete an EFI driver option from the driver list.

Delete Driver Option

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

▶UEFI Hard Disk Drive BBS Priorities

- Boot Option #1 - This feature sets the system boot order of detected devices. The options are **Windows Boot Manager** and Disabled.
- Boot Option #2 - This feature sets the system boot order of detected devices. The options are **Windows Boot Manager** and Disabled.

▶UEFI Network Drive BBS Priorities

This option sets the system boot order of detected devices.

- Boot Option #1
- Boot Option #2
- Boot Option #3
- Boot Option #4

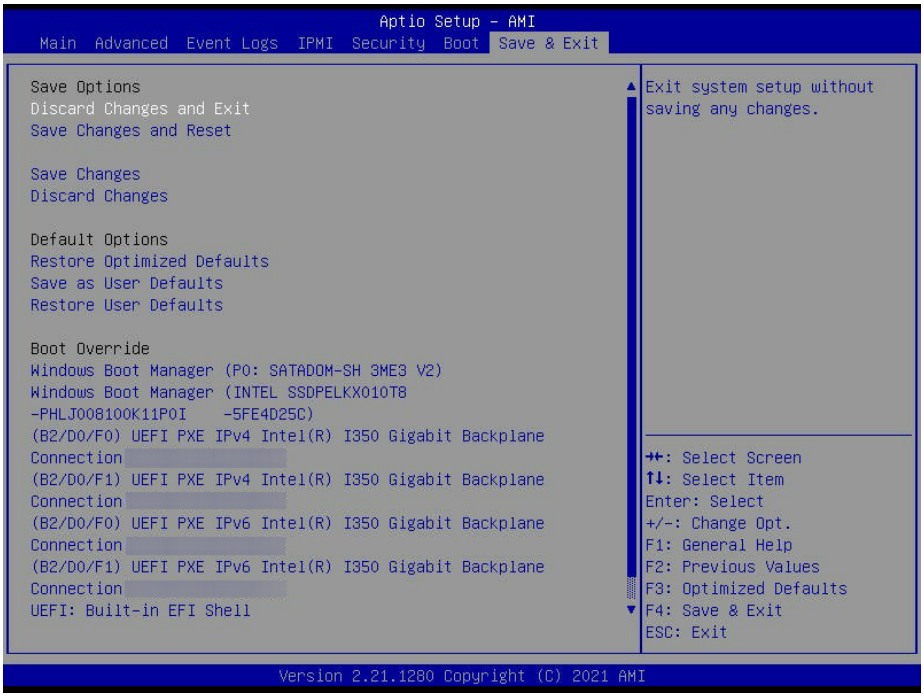
▶UEFI Application Boot Priorities

This option sets the system boot order of detected devices.

- Boot Option #1

4.8 Save & Exit

Select the Save & Exit tab from the BIOS setup utility screen to enter the Exit BIOS Setup screen.



Discard Changes and Exit

Select this option 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 leave the BIOS setup utility and reboot the computer, so the new system configuration parameters can take effect. Select Save Changes and Exit from the Exit menu and press <Enter>.

Save Changes

After completing the system configuration changes, select this option to save the changes you have made. This does not reset (reboot) the system.

Discard Changes

Select this option 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 from the Save & Exit menu and press <Enter>. These are factory settings designed for maximum system stability, but not for maximum performance.

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

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

Windows Boot Manager (P0: SATADOM-SH 3ME3 V2)

Windows Boot Manager (INTEL SSDPELKX010T8 - PHLJ00B100K11P0I -5FE4D25C)

(B2/D0/F0) UEFI PXE IPv4 Intel(R) I350 Gigabit Backplane Connection (MAC:0cc47ae1236c)

(B2/D0/F1) UEFI PXE IPv4 Intel(R) I350 Gigabit Backplane Connection (MAC:0cc47ae1236d)

(B2/D0/F0) UEFI PXE IPv6 Intel(R) I350 Gigabit Backplane Connection (MAC:0cc47ae1236c)

(B2/D0/F1) UEFI PXE IPv6 Intel(R) I350 Gigabit Backplane Connection (MAC:0cc47ae1236d)

UEFI: Built-in EFI Shell

Launch EFI Shell from Filesystem Device

This option allows you to launce EFI Shell application (Shell.efi) from one of the available file system devices.

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 process. If a fatal error occurs, you should consult with your system manufacturer for possible repairs.

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

BIOS Beep (POST) Codes		
Beep Code	**Error Message**	**Description**
1 beep	Refresh	Circuits have been reset (Ready to power up)
5 short, 1 long	Memory error	No memory detected in system
5 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 AOC-LPC80-20).

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

Appendix B

Software

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

B.1 Microsoft Windows OS Installation

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

Installing the OS

1. Create a method to access the MS Windows installation ISO file. That might be a DVD, perhaps using an external USB/SATA DVD drive or a USB flash drive.

2. Retrieve the proper RST/RSTe driver. Go to the Supermicro web page for your motherboard and click on "Download the Latest Drivers and Utilities", select the proper driver, and copy it to a USB flash drive.

3. Boot from a bootable device with Windows OS installation. You can see a bootable device list by pressing **F11** during the system startup.

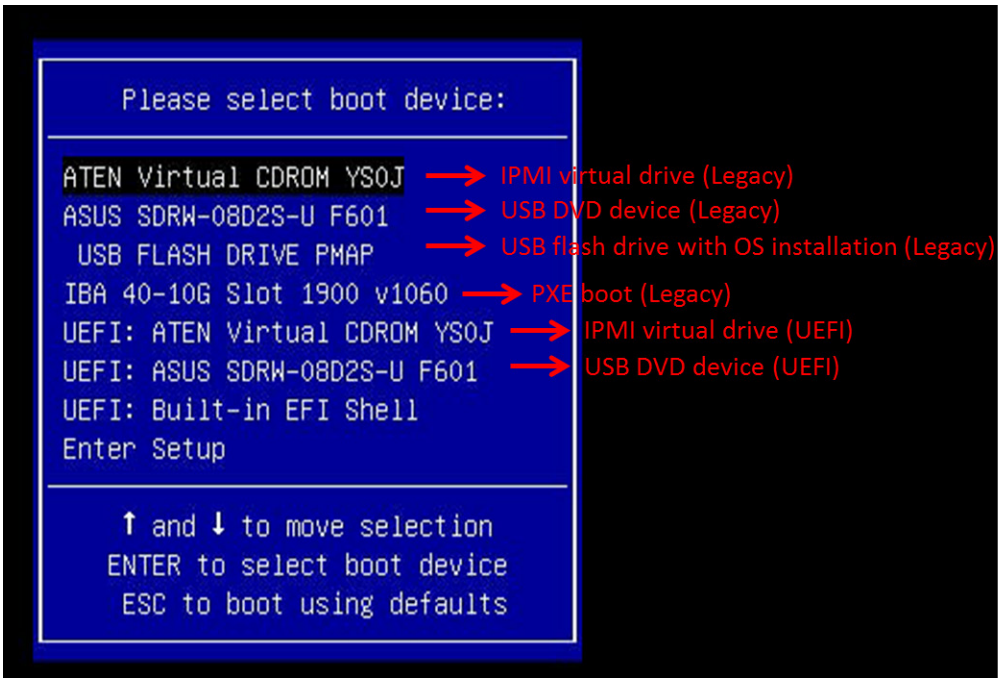


Figure B-1. Select Boot Device

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

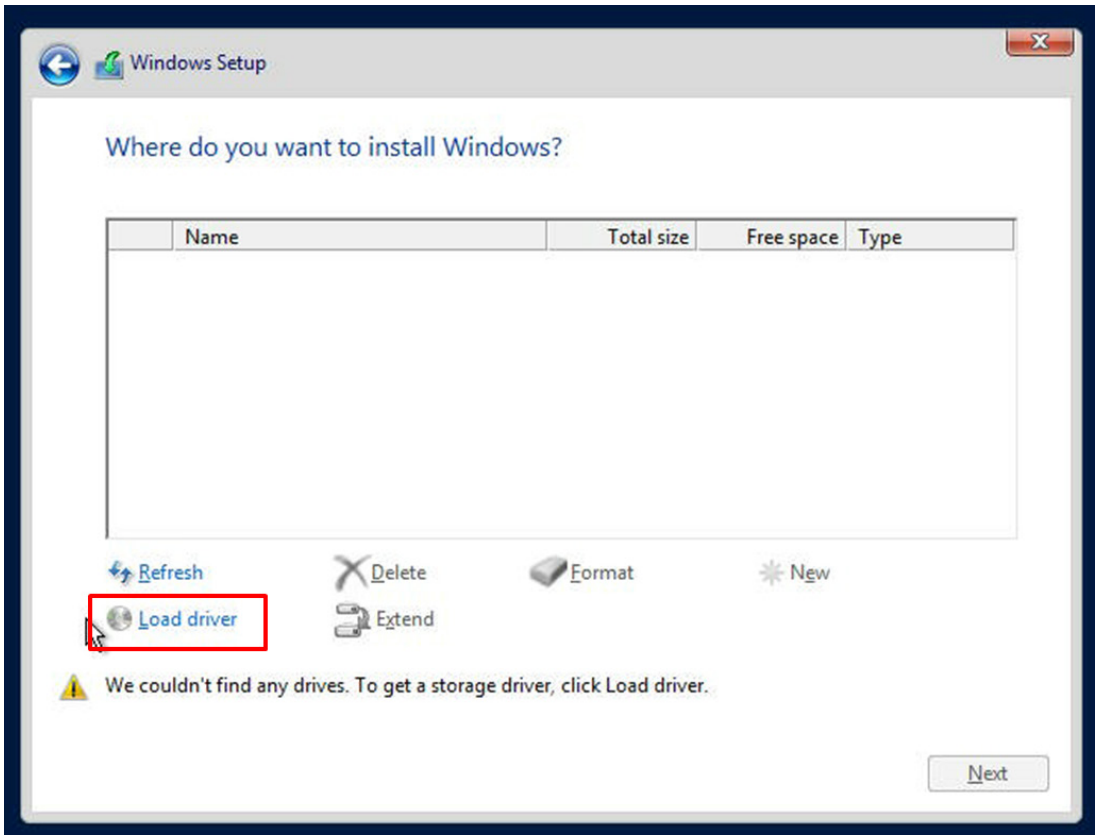


Figure B-2. Load Driver Link

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

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

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

B.2 Driver Installation

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

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

Another option is to go to the Supermicro website at http://www.supermicro.com/products/. Find the product page for your motherboard and download the latest drivers and utilities.

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

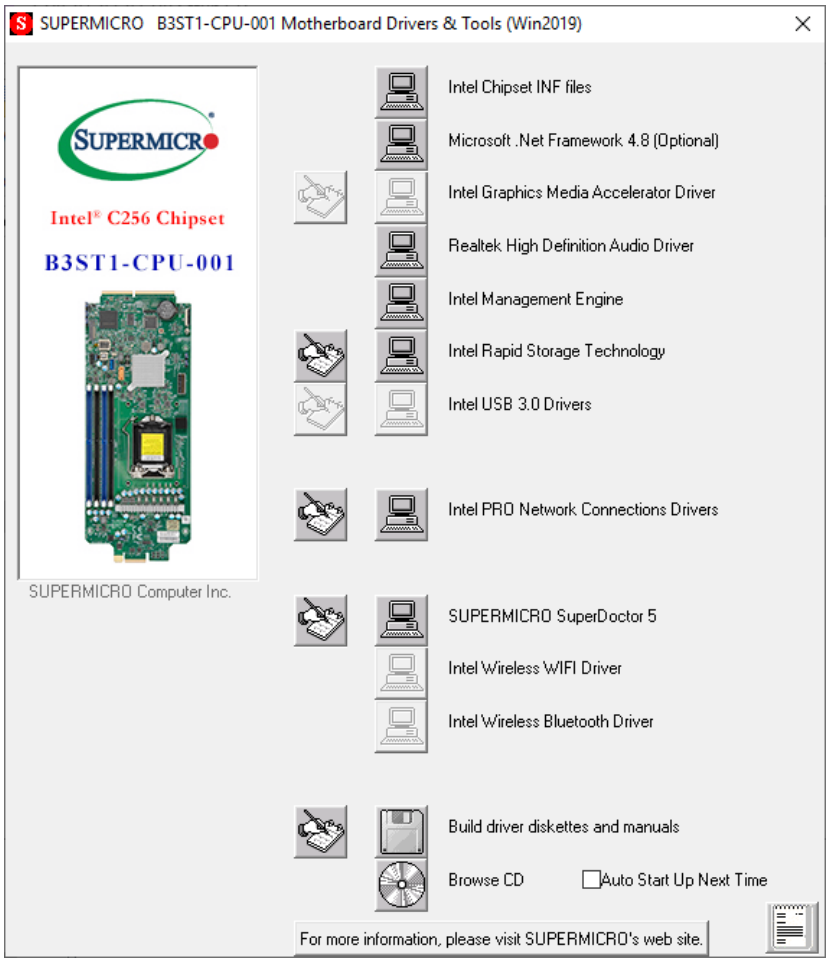


Figure B-3. Driver & Tool Installation Screen

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

B.3 SuperDoctor® 5

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

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

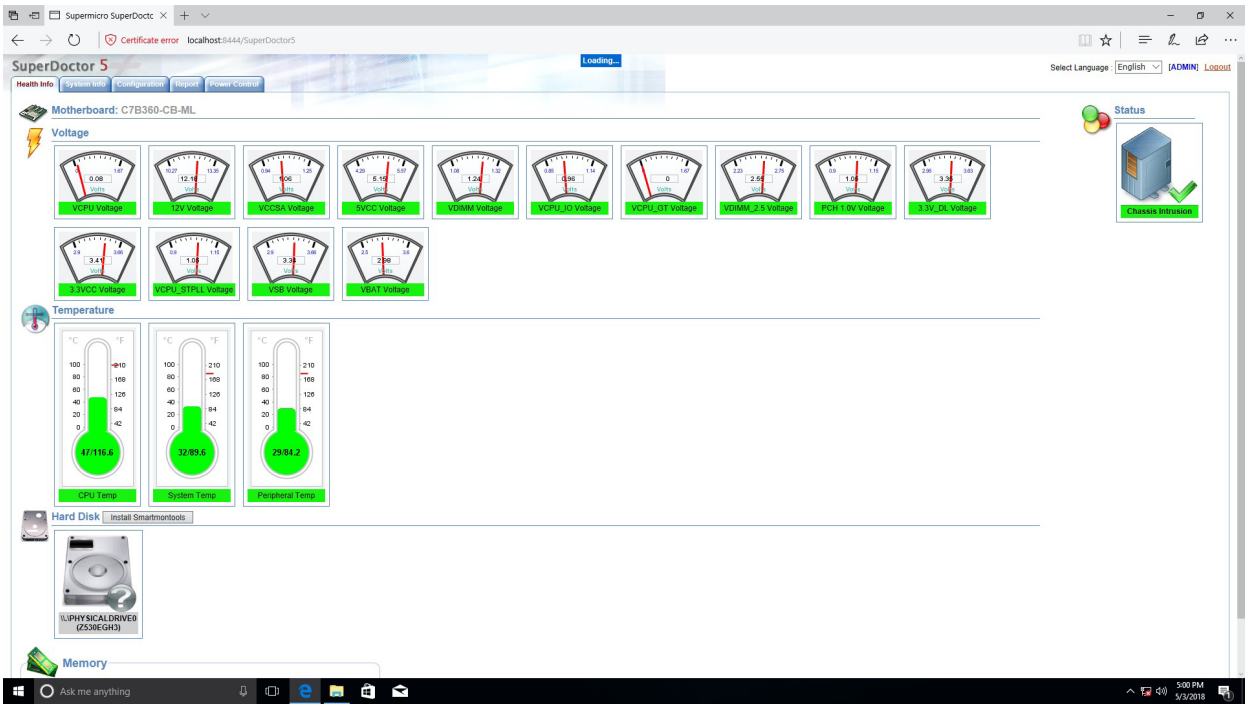


Figure B-4. SuperDoctor 5 Interface Display Screen (Health Information)

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.

Battery Handling

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

電池の取り扱い

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

警告

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

警告

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

Warnung

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

Attention

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

¡Advertencia!

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

אזהרה!

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

هناك خطر من انفجار في حالة اسحبذال البطارية بطريقة غير صحيحة فعليل
اسحبذال البطارية
فقط بنفس النع أو ما يعادلها مما أوصث به الشرمة المصنعة
جخلص من البطاريات المسحعملة وفقا لحعليمات الشرمة الصانعة

경고!

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

Waarschuwing

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

Product Disposal

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

製品の廃棄

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

警告

本产品的废弃处理应根据所有国家的法律和规章进行。

警告

本產品的廢棄處理應根據所有國家的法律和規章進行。

Warnung

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

¡Advertencia!

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

Attention

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

סילוק המוצר

אזהרה!

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

عند التخلص النهائي من هذا المنتج ينبغي التعامل معه وفقا لجميع القانين واللائح البطنية

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

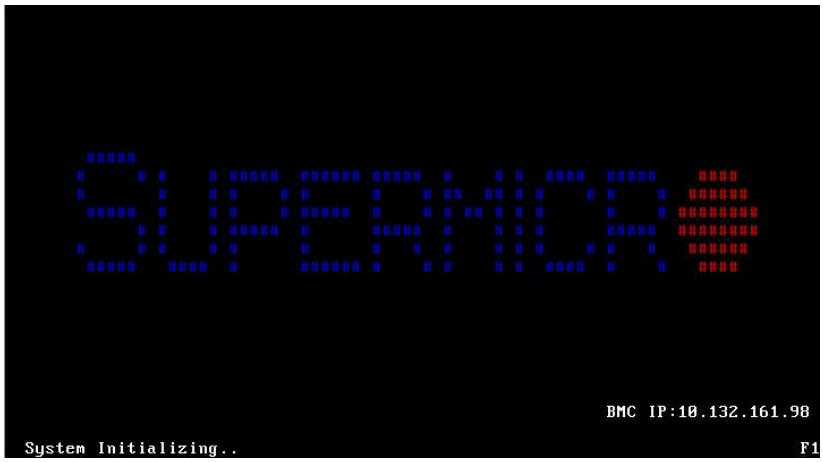
This feature allows the user to recover the main BIOS image using a USB-attached device without additional utilities used. A USB flash device such as a USB Flash Drive, or a USB CD/DVD ROM/RW device can be used for this purpose. However, a USB Hard Disk drive cannot be used for BIOS recovery at this 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.

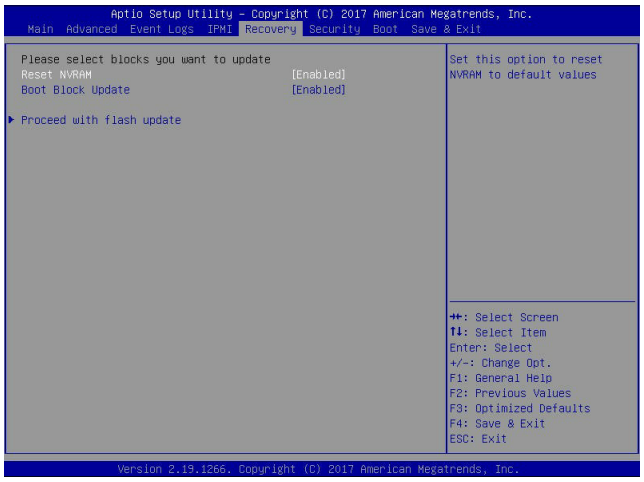
To perform UEFI BIOS recovery using a USB-attached device, follow the instructions below:

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 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.



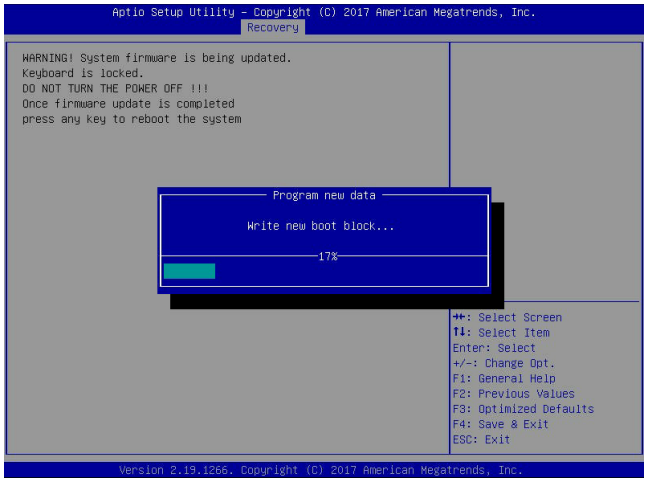
Note 2: Before recovering the main BIOS image, confirm that the "Super.ROM" binary image file you download is the same version or a close version meant for your motherboard.



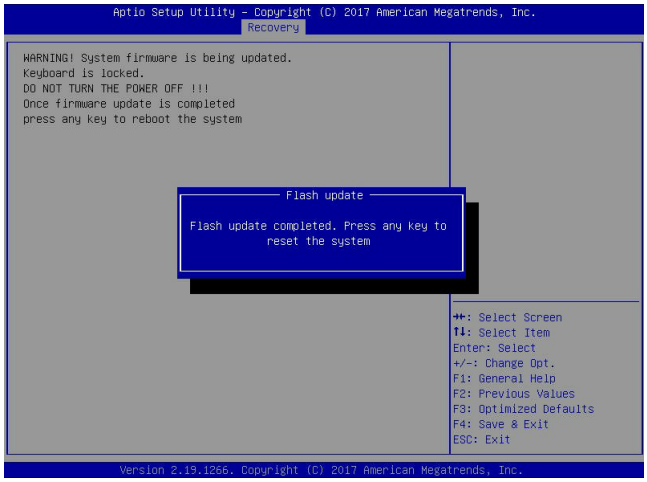
2. Insert the USB device that contains the new BIOS image ("Super.ROM") into your USB port and reset the system until the following screen appears:

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:

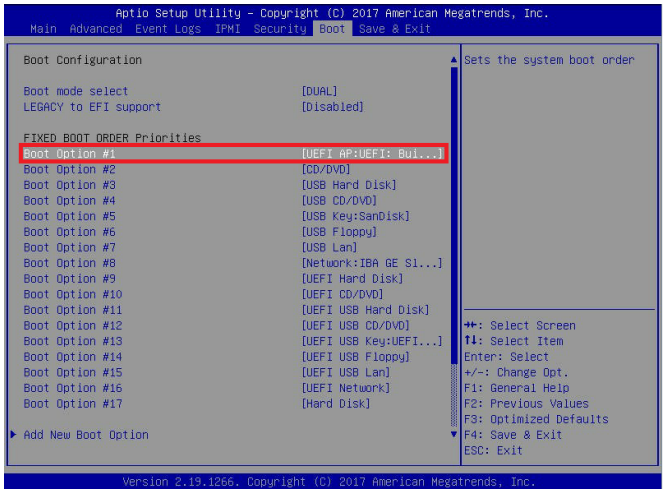


Note: *Do not interrupt the BIOS flashing process until it has completed*.

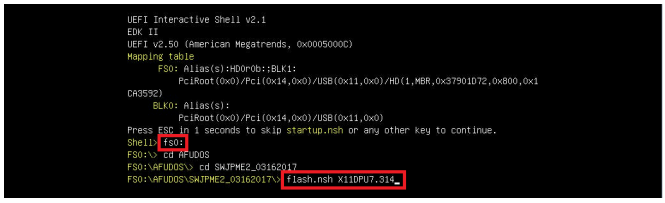
5. After the BIOS recovery process is completed, press any key to reboot the system.

6. Using a different system, extract the BIOS package into a USB flash drive.

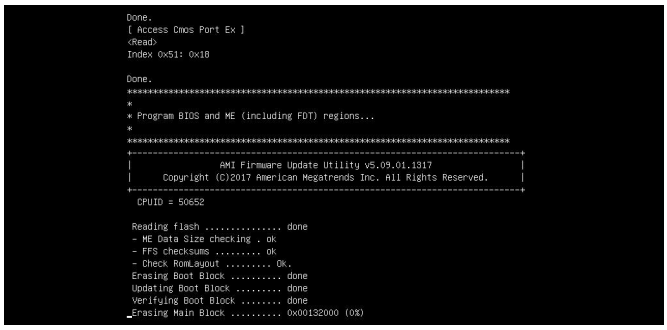
7. Press <Del> during system boot to enter the BIOS Setup utility. From the top of the tool bar, select Boot to enter the submenu. From the submenu list, select Boot Option #1 as shown below. Then, set Boot Option #1 to [UEFI AP:UEFI: Built-in EFI Shell]. Press <F4> to save the settings and exit the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

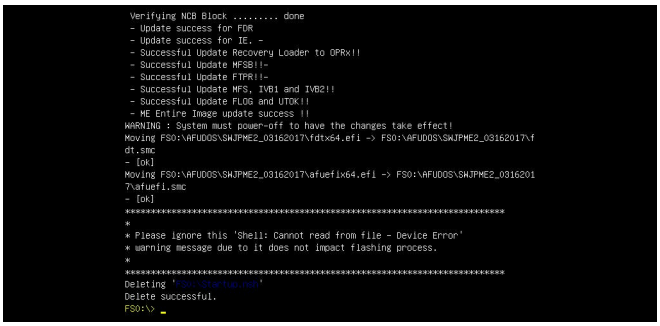


8. When the UEFI Shell prompt appears, type fs# to change the device directory path. Go to the directory that contains the BIOS package you extracted earlier from Step 6. Enter flash.nsh BIOSname.### at the prompt to start the BIOS update process.



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





9. 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.

10. Press <Del> to enter the BIOS Setup utility.

11. Press <F3> to load the default settings.

12. After loading the default settings, press <F4> to save the settings and exit the BIOS Setup utility.