



H13QSH

USER'S MANUAL

Revision 1.0

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

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

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

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

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A or Class B digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in industrial environment for Class A device or in residential environment for Class B device. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. "Perchlorate Material-special handling may apply. See 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 1.0

Release Date: October 21, 2024

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

Copyright © 2024 by Super Micro Computer, Inc.

All rights reserved.

Printed in the United States of America

Preface

About This Manual

This manual is written for system integrators, IT technicians and knowledgeable end users. It provides information for the installation and use of the H13QSH motherboard.

About This Motherboard

Built upon the functionality and capability of the Quad AMD Instinct™ MI300A APUs, the H13QSH motherboard provides superior graphics capability and system performance while consuming little power. 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 when performing a procedure.

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 (Sales Inquiries)
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 Inquiries)
Support@supermicro.com.tw (Technical Support)
RMA@supermicro.com.tw (RMA Support)

Website: www.supermicro.com.tw

Table of Contents

Contacting Supermicro.....	4
Chapter 1 Introduction	
1.1 H13QSH System Board Overview	7
1.2 Quick Reference.....	9
Quick Reference Table.....	10
Motherboard Features.....	12
Block Diagram.....	14
1.3 Processor and Chipset Overview.....	15
1.4 Special Features	15
Recovery from AC Power Loss.....	15
1.5 System Health Monitoring	16
Onboard Voltage Monitors	16
Fan Status Monitor with Firmware Control	16
Environmental Temperature Control	16
System Resource Alert.....	16
1.6 ACPI Features.....	17
1.7 Power Supply	17
1.8 Super I/O	17
Chapter 2 Installation	
2.1 Static-Sensitive Devices.....	18
Precautions	18
Unpacking	18
2.2 Motherboard Installation.....	19
Location of Mounting Holes	19
Installing the Motherboard.....	21
2.3 Processor and Heatsink Installation.....	22
2.4 Connectors	31
Power Connections	31
Headers.....	32
2.5 Jumper Settings	35
How Jumpers Work.....	35

2.6 LED Indicators	37
2.7 Front Control Panel	40
2.8 M.2 Solid State Drive Installation	45
Chapter 3 Troubleshooting	
3.1 Troubleshooting Procedures	46
Before Power On	46
No Power	46
No Video	47
System Boot Failure	47
The System Cannot Retain the Setup Configuration	47
When the System Becomes Unstable	47
3.2 Technical Support Procedures	48
3.3 Frequently Asked Questions	49
3.4 Returning Merchandise for Service	50
3.5 Battery Removal and Installation	51
Battery Removal	51
Proper Battery Disposal	51
Battery Installation	52
Chapter 4 BIOS	
4.1 Introduction	53
Starting the Setup Utility	53
4.2 Main Setup	54
4.3 Advanced	56
4.4 BMC	73
4.5 Event Logs	76
4.6 Security	78
4.7 Boot	82
4.8 Save & Exit	84
Appendix A Software	
Appendix B Standardized Warning Statements	

Chapter 1

Introduction

Congratulations on purchasing your computer motherboard from an industry leader. Supermicro motherboards are designed to provide you with the highest standards in quality and performance. This motherboard is intended to be used in a Supermicro 4-way server as an integrated solution. It will not be sold as an independent product; no shipping package will be provided.

1.1 H13QSH System Board Overview

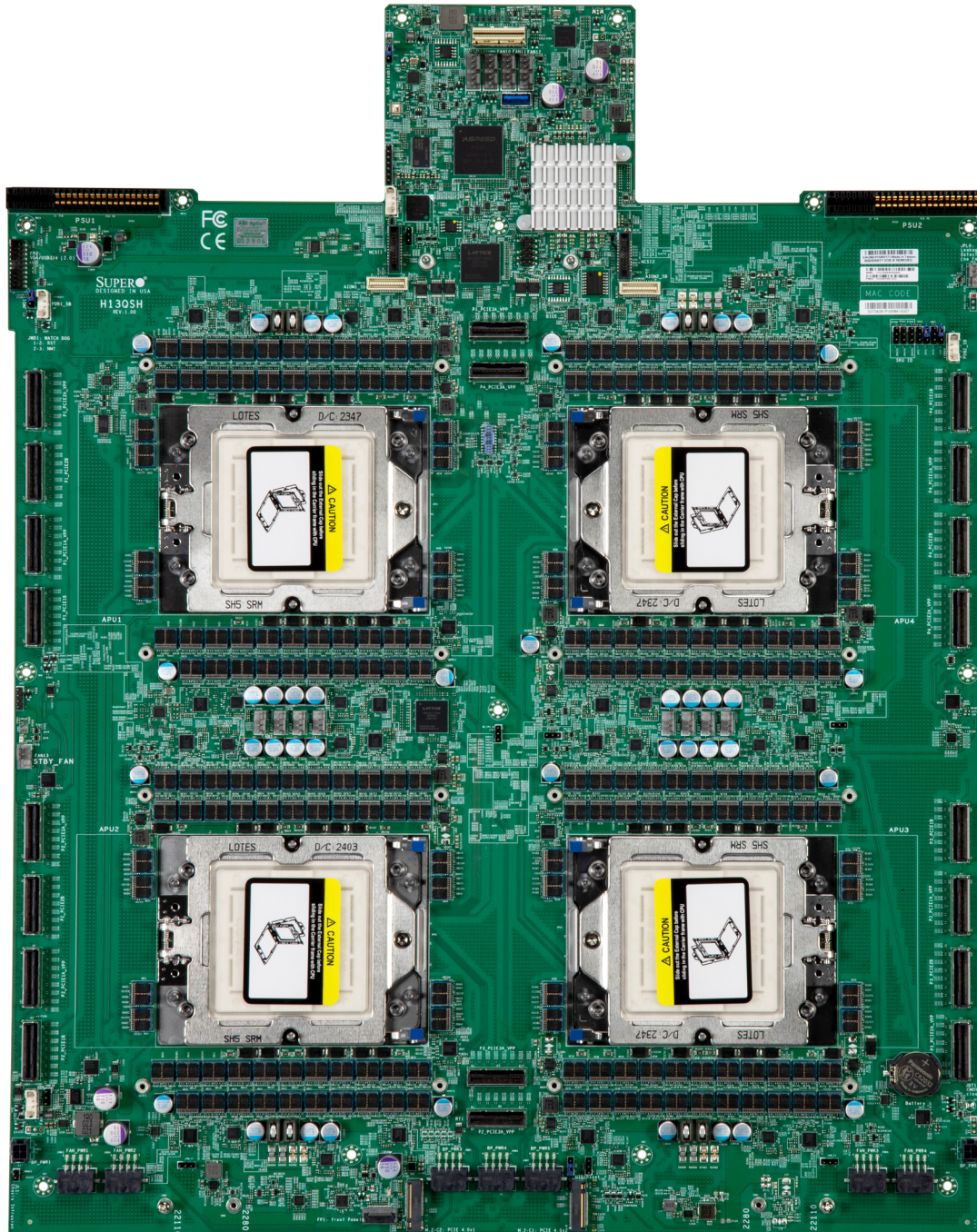
This chapter provides detailed information on the components installed on the H13QSH system board as well as specifications and features supported by your 4-way system.

Important Links

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

- Supermicro product manuals: <http://www.supermicro.com/support/manuals/>
- Product drivers and utilities: <https://www.supermicro.com/wdl>
- Product safety info: http://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, please contact our support team at: support@supermicro.com

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



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.

1.2 Quick Reference

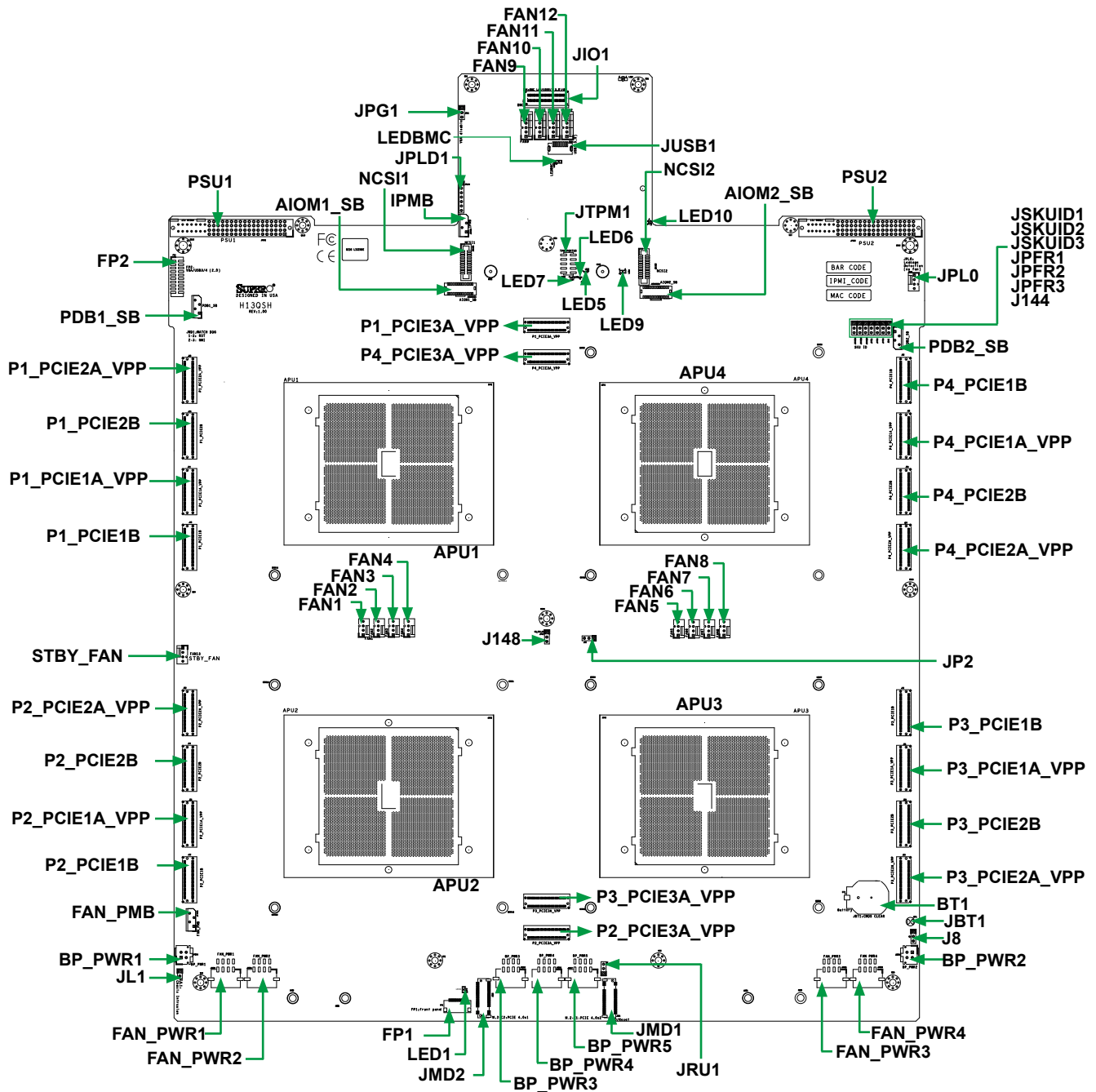


Figure 1-2. H13QSH Layout

Notes:

- Components not documented are for internal testing only.
- See [Chapter 2](#) for detailed information on jumpers, I/O ports.
- Use only the correct type of onboard CMOS battery as specified by the manufacturer. To avoid possible explosion, do not install the onboard battery upside down.

Quick Reference Table

Jumper	Description	Default Setting
JBT1	CMOS Clear	Open (Normal)
JPG1	Video Display Enable	Pins 1/2: Video Display Enabled
JRU1	UID LED/BMC Reset	Closed: Normal (UID LED)
JSKU1D1-3	Refer to system manual for details	

LED	Description	Status
LED1 (LEDPWR)	Power LED	LED On: Onboard Power On
LEDBMC (LED3)	BMC Heartbeat LED	Blinking Green: BMC Normal (Active), Solid Green: (During BMC Reset or during a Cold Reboot)
LED5	APU2 Power Status LED	Solid Red: Power Failure
LED6	APU3 Power Status LED	Solid Red: Power Failure
LED7	APU4 Power Status LED	Solid Red: Power Failure
LED9	PCIE SW Heartbeat	Blinking Green: PCIe SW Normal, Solid Green: (During PCIe Switch Reset or during a Cold Reboot)
LED10	PCIE SW Error	Solid Red: SystemError / No PCIe Link

Connector	Description
AIOM1_SB (JAIOM1SB1) /AIOM2_SB (JAIOM2SB1)	Advanced I/O Module (AIOM) PCIe 5.0 x8 Slot Supported by APU
BT1	Onboard CMOS Battery
BMC (JIO1)	Dedicated BMC LAN on the Rear I/O Panel
BP_PWR2 (JPWR1)	4-pin Power Connector for Backplane Devices
BP_PWR1 (JPWR2)	4-pin Power Connector for Backplane Devices
BP_PWR3 (JPWR5)	8-pin Power Connector for Backplane Devices
BP_PWR4 (JPWR6)	8-pin Power Connector for Backplane Devices
BP_PWR5 (JPWR7)	8-pin Power Connector for Backplane Devices
FAN1-8	4-pin Fan Headers
FAN9-12	6-pin Cooling Fan Headers
FAN_PMB (JFAN1)	Fan for I ² C Temperature Sensor
FAN_PWR1 (JPWR3)	8-pin Fan Power Connector
FAN_PWR2 (JPWR4)	8-pin Fan Power Connector
FAN_PWR3 (JPWR8)	8-pin Fan Power Connector
FAN_PWR4 (JPWR9)	8-pin Fan Power Connector
FP1	Front Control Panel header with I ² C
FP2	Front Control Panel Header with USB and VGA Support
IPMB (JIPMB1)	4-pin BMC External I ² C Header (for an IMPI card)
JL1	Chassis Intrusion Header
JMD1-2 (M.2-C1/M.2-C2)	M.2 M-Key 2280/22110 (supports PCIe 4.0 x2/x1) Slot
JPL0	4-pin Leakage Detection

Connector	Description
JTPM1	Trusted Platform Module/Port 80 Connector
NCSI1 (JNCSI1)/ NCSI2 (JNCSI2)	NCSI Headers for IPMI Support
PSU1 (JPSU1)/ PSU2 (JPSU2)	Supermicro Proprietary Power Supply Units 1/2 for System Use
PDB1_SB/PDB2_SB	SMB I ² C for 4U Power Distribution Board
P1_PCIE1B/P1_PCIE2B	JA2 and JA4: PCIe 5.0 x8 by APU1
P2_PCIE1B/P2_PCIE2B	JB2 and JB4: PCIe 5.0 x8 by APU2
P3_PCIE1B/P3_PCIE2B	JC2 and JC4: PCIe 5.0 x8 by APU3
P4_PCIE1B/P4_PCIE2B	JD2 and JD4: PCIe 5.0 x8 by APU4
P1_PCIE1A_VPP/ P1_PCIE2A_VPP	JA1 and JA3: PCIe 5.0 x8 by APU1
P1_PCIE3A_VPP	2x PCIe 5.0 x4 by PESW (APU1)
P2_PCIE1A_VPP/ P2_PCIE2A_VPP/ P2_PCIE3A_VPP	JB1 and JB3: PCIe 5.0 x8 by APU2, JB5: 2 x PCIe 5.0 x4 by APU2
P3_PCIE1A_VPP/ P3_PCIE2A_VPP/ P3_PCIE3A_VPP	JC1 and JC3: PCIe 5.0 x8 by APU3, JC5: 2 x PCIe 5.0 x4 by APU3
P4_PCIE1A_VPP/ P4_PCIE2A_VPP/ P4_PCIE3A_VPP	JD1 and JD3: PCIe 5.0 x8 by APU4, JD5: 2 x PCIe 5.0 x4 by APU4
STBY-FAN (FAN13)	Standby Fan Header
USB2 (3.0) (JUSB1)	Type A USB 3.0 Connector (USB2) for Front Access

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

Motherboard Features

APU

- Quad AMD Instinct™ MI300A APUs in sockets SH5

Memory

- 128 GB HBM3, bandwidth 5.3 TB/s

Chipset

- System on Chip (SoC)

Expansion Slots

- 20 MCIO connectors (16 PCIe 5.0 x8, three PCIe 5.0 x4 x4, one PCIe 5.0 x4 with PCIe 4.0 x4)
- Two M.2 in 22110/2280 (PCIe 4.0 x4 from MCIO connector)
- Two USB 3.2 (rear) + two USB 2.0 (front), one TPM 2.0 header
- Two OCP compatible AIOM slots
- One RJ45 1 GbE Dedicated IPMI LAN port, one VGA port, one DisplayPort

Network

- ASPEED AST2600 BMC with RoT support

Graphics

- ASPEED AST2600 BMC chip with one VGA port

BIOS

- AMI 32 MB SPI Flash EEPROM

Power Management

- ACPI power management (S1, S5)
- Power button override mechanism
- Wake-On-LAN (JWOL)
- Power-on mode for AC power recovery

System Health Monitoring

- Onboard voltage monitoring for +3.3V, +5V, +12V, +3.3V stby, +5V stby, CPU temperature, system temperature, memory temperature, and peripheral temperature
- CPU Thermal Trip support
- PECI/TSI

Fan Control

- Fan speed control

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

System Management

- IPMIView / SMCIPMITOOL
- SuperDoctor® 5
- Redundant power supply unit detection sensor
- SPM/SSM/SUM-OOB/InBand
- Trusted Platform Module (TPM) support

LED Indicators

- CPU / System Overheat LED
- Power / Suspend-state Indicator
- Fan Failed LED
- UID / Remote UID
- HDD Activity LED
- LAN Activity LED

Dimensions

- 17.04" (W) x 21.35" (L), (432.82 mm x 542.29 mm)

Block Diagram

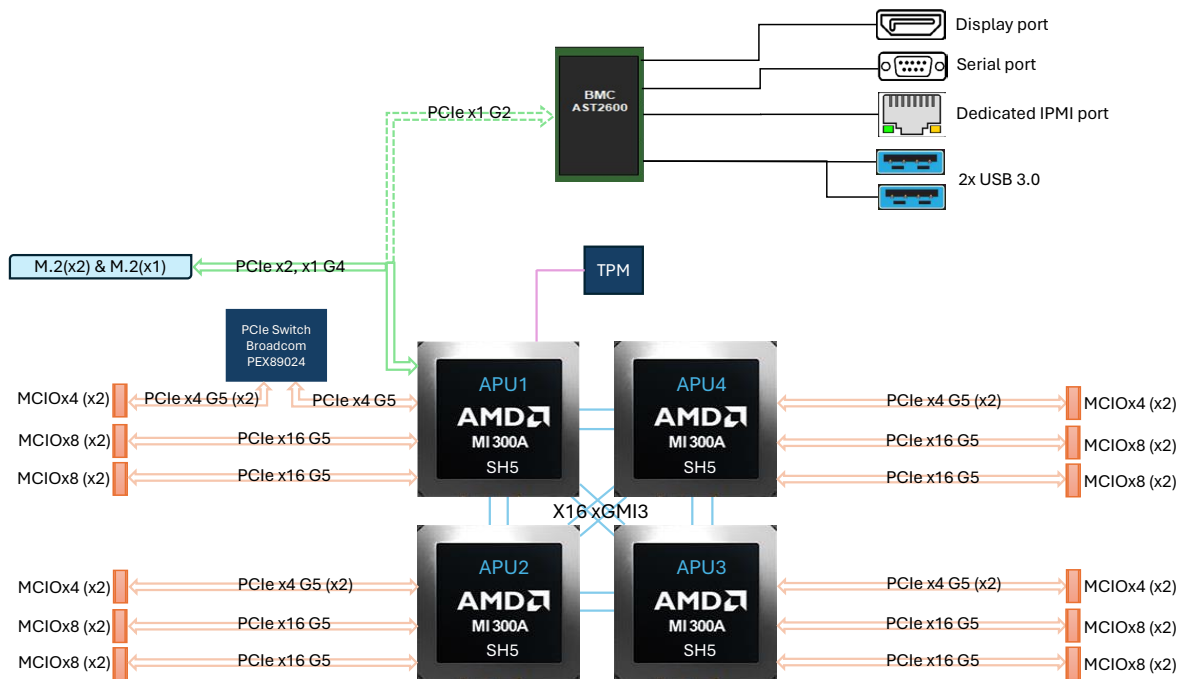


Figure 1-3. System Block Diagram

Note 1: 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.

1.3 Processor and Chipset Overview

Built upon the functionality and capability of the Quad AMD Instinct™ MI300A APUs in SH5 sockets, the H13QSH motherboard offers critical, pivotal technological breakthroughs that unleash unprecedented computing capabilities and provides a scalable platform optimized for applications used in High-performance Computing, Machine Learning, and Model Training. The key features supported by the platform include the following:

- ACPI Power Management Logic Support Rev. 6.4
- Adaptive Thermal Management/Monitoring
- PCIe 5.0 w/transfer rate of up to 32.0 GT/s and SATA 3.0 w/ transfer rate of up to 6.0 GB/s
- System Management Bus (SMBus) Specification Version 3.5

1.4 Special Features

This section describes the health monitoring features of the H13QSH motherboard. The motherboard has an onboard System Hardware Monitor chip that supports system health monitoring.

Recovery from AC Power Loss

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

1.5 System Health Monitoring

This section describes the health monitoring features of the H13QSH motherboard. The motherboard has an onboard Baseboard Management Controller (BMC) chip that supports system health monitoring. 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.

Onboard Voltage Monitors

An onboard voltage monitor will scan the voltages of the onboard chipset, memory, and APU continuously. Once a voltage becomes unstable, a warning is given, or an error message is sent to the screen.

Fan Status Monitor with Firmware Control

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

Environmental Temperature Control

System Health sensors monitor temperatures and voltage settings of onboard processors and the system in real time via the BMC interface. Whenever the temperature of the APU or the system exceeds Supermicro's pre-defined threshold, the system and APU cooling fan speed will increase to prevent the APU or system from overheating.

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

System Resource Alert

This feature is available when used with SuperDoctor 5[®]. SuperDoctor 5 is used to notify the user of certain system events. For example, you can configure SuperDoctor 5 to provide you with warnings when the system temperature, APU temperatures, voltages and fan speeds go beyond a predefined range.

1.6 ACPI Features

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

1.7 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 APU 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.

1.8 Super I/O

The ASpeed AST2600 Super I/O provides one high-speed, 16550 compatible Universal Asynchronous Receiver/Transmitter (UART), which supports serial infrared communications. This UART includes a send/receive FIFO, a programmable baud rate generator, complete modem control capability and a processor interrupt system. This UART provides legacy speed with baud rate of up to 115.2 Kbps as well as an advanced speed with baud rates of 250 K, 500 K, or 1 Mb/s, which support higher speed modems.

The Super I/O provides functions that comply with ACPI (Advanced Configuration and Power Interface), which includes support of legacy and ACPI power management through the System Management Interrupt (SMI) or System Control Interrupt (SCI). It also features auto power management to reduce power consumption.

Chapter 2

Installation

2.1 Static-Sensitive Devices

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

Precautions

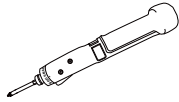
- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing the board from the antistatic bag.
- Handle the board by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules,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

Unpacking

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

2.2 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.



Torque Driver (1)



Philips Screws (13)



Standoffs (13)
Only if Needed

Tools Needed

Location of Mounting Holes

Notes:

1. Do not use a force greater than 10.8-13.0 in-lbf (12.5-15.0 kgf-cm) on each mounting screw during motherboard installation. Exceeding this force may over-torque the screw, causing damage to the motherboard and screw.
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.

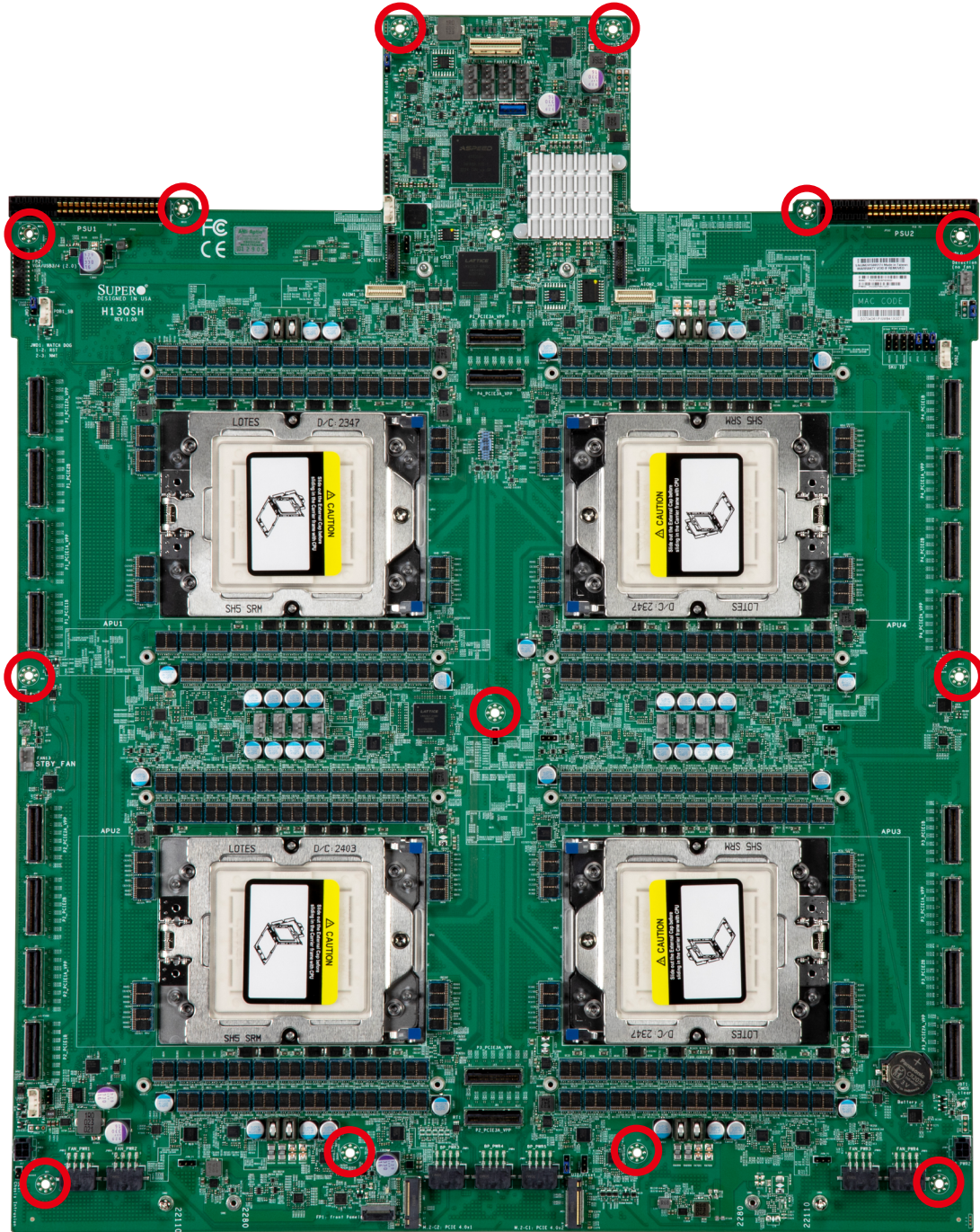
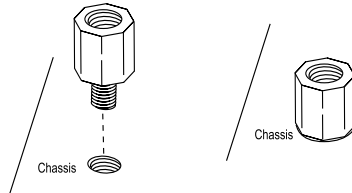


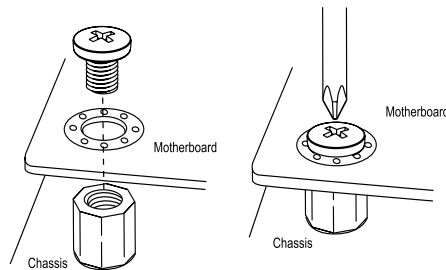
Figure 2-1. Motherboard Mounting Holes

Installing the Motherboard

1. Locate the mounting holes on the motherboard. See the previous page for the location.



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



3. Install standoffs in the chassis as needed.
4. Install the motherboard into the chassis carefully to avoid damaging other motherboard components.
5. Using the Phillips screwdriver, insert a Phillips head #6 screw into a mounting hole on the motherboard and its matching mounting hole on the chassis.
6. Repeat Step 5 to insert #6 screws into all mounting holes.
7. Make sure that the motherboard is securely placed in the chassis.

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

2.3 Processor and Heatsink Installation

The processor (APU) and processor carrier should be assembled together first to form the processor carrier assembly. This assembly will be then attached to the heatsink to form the processor heatsink module (PHM) before being installed into the APU socket. Before installation, be sure to perform the following steps below:

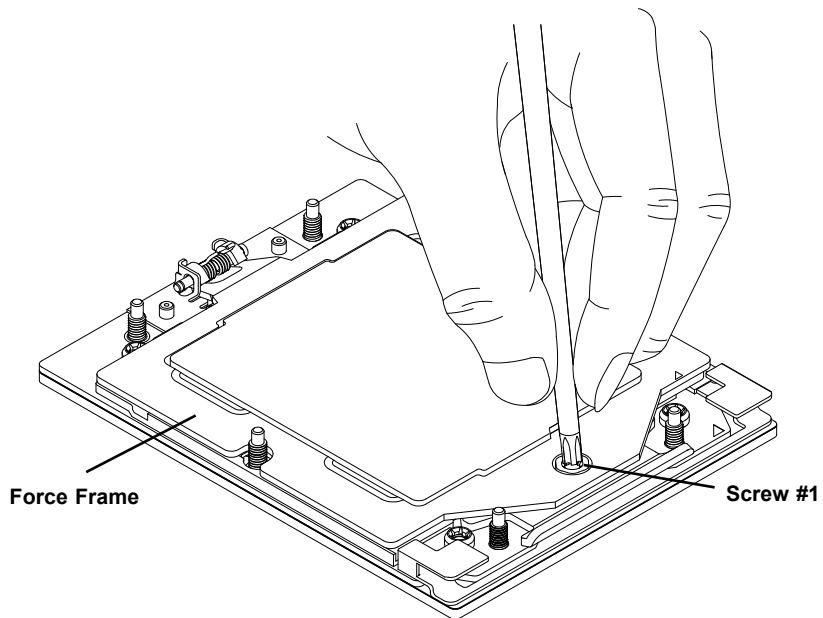
Warning: When handling the processor package, avoid placing direct pressure on the label area of the fan.

Important:

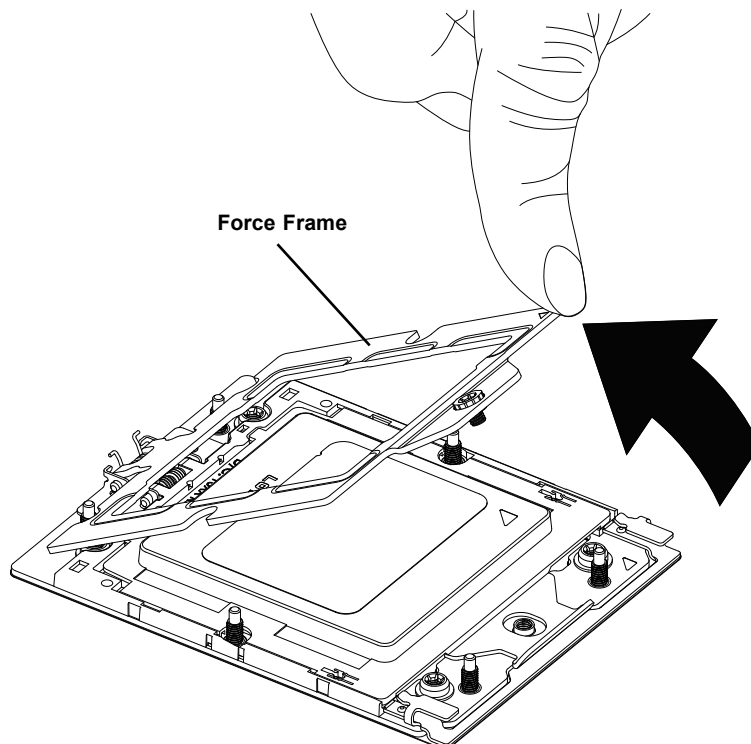
- Please carefully follow the instructions given on the previous page to avoid ESD-related damages.
- When receiving a motherboard without a processor pre-installed, make sure that the plastic APU socket cap is in place and none of the socket pins are bent; otherwise, contact your retailer immediately.
- 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 APU socket, which may require manufacturer repairs.
- When installing the processor and heatsink, ensure a torque driver set to the correct force is used for each screw.
- Thermal grease is pre-applied on a new heatsink. No additional thermal grease is needed.
- Refer to the Supermicro website for updates on APU support.
- All graphics in this manual are for illustrations only. Your components may look different.
- For the Processor/Heatsink installation you need to use a T20 bit torque driver when opening/closing the APU socket.
- Always connect the power cord last, and always remove it before adding, removing or changing any hardware components. Make sure that you install the processor into the APU socket before you install the APU heatsink.
- If you buy an APU separately, make sure that you use an AMD-certified multi-directional heatsink only.
- Make sure to install the motherboard into the chassis before you install the APU heatsink.

Installing the Processor and Heatsink

1. Unscrew the screw #1 holding down the force frame.

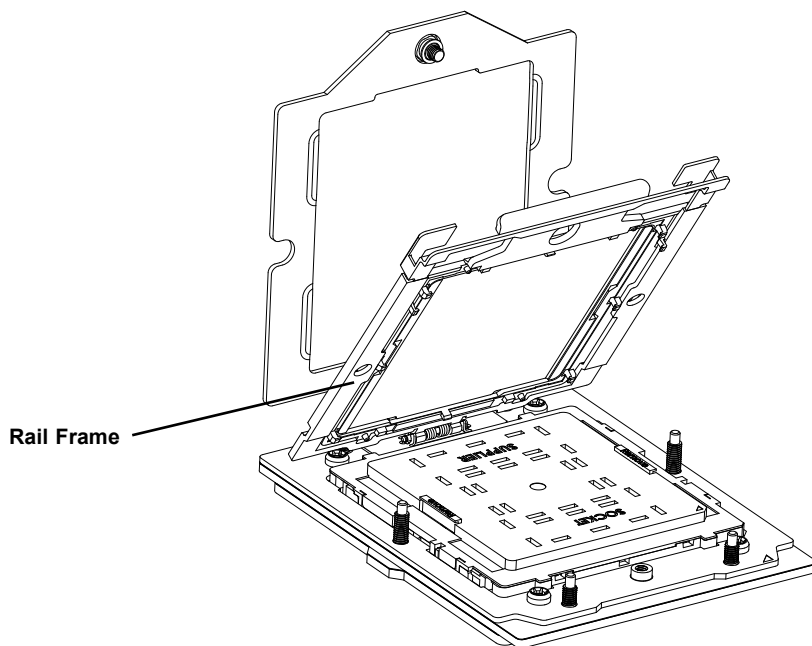


2. The spring-loaded force frame will raise up after the screw securing it (#1) is removed. Gently allow it to lift up to its stopping position.

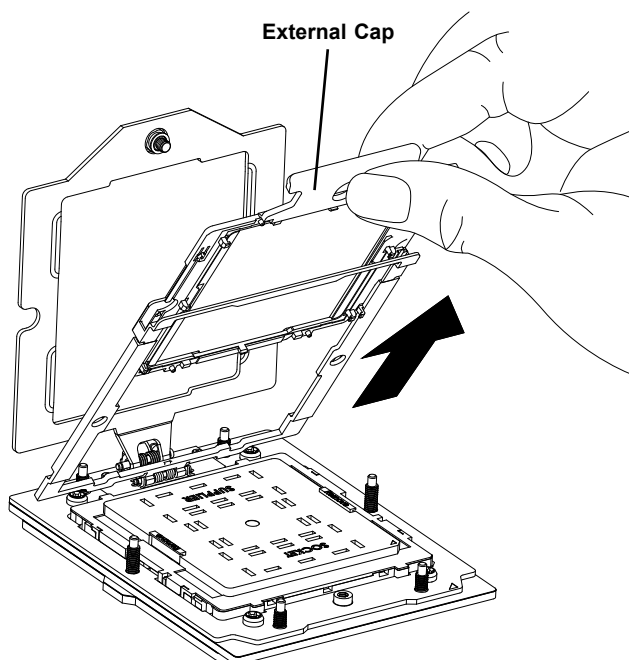


- Lift the rail frame up by gripping the lift tabs near the front end of the rail frame. While keeping a secure grip of the rail frame, lift it to a position so you can do the next step of removing the external cap.

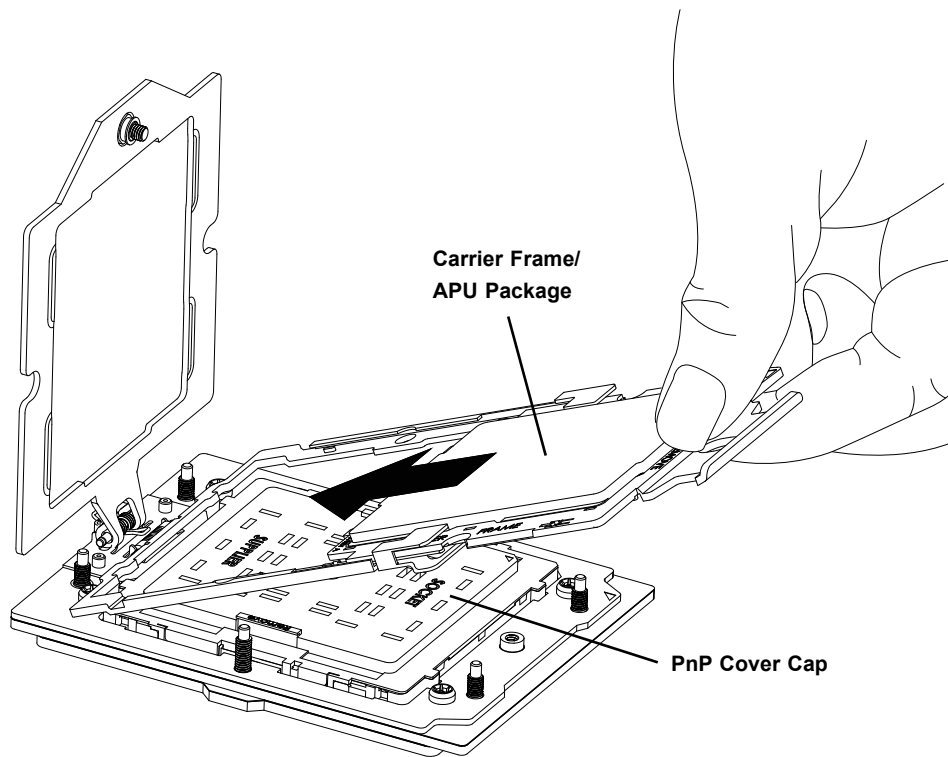
Note: The rail frame is spring loaded, so keep a secure grip on it as you lift it so it does not snap up.



- Remove the external cap from the rail frame by pulling it upwards through the rail guides on the rail frame.

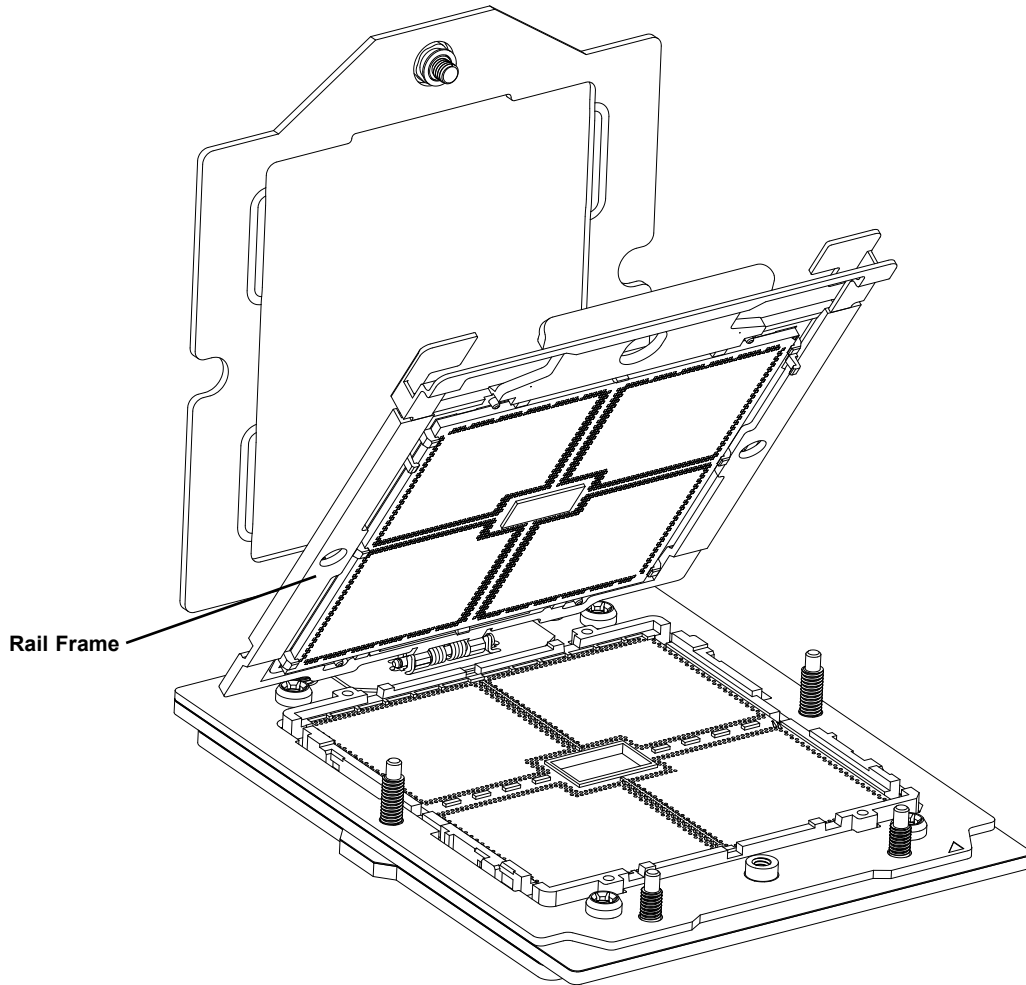


5. The APU package is shipped from the factory with the carrier frame pre-assembled. Grip the handle of the carrier frame/APU package assembly from its shipping tray, and while gripping the handle, align the flanges of the carrier frame onto the rails of the rail frame so its pins will be at the bottom when the rail frame is lowered later.
6. Slide the carrier frame/APU package downwards to the bottom of the rail frame. Ensure the flanges are secure on the rails as you lower it downwards.



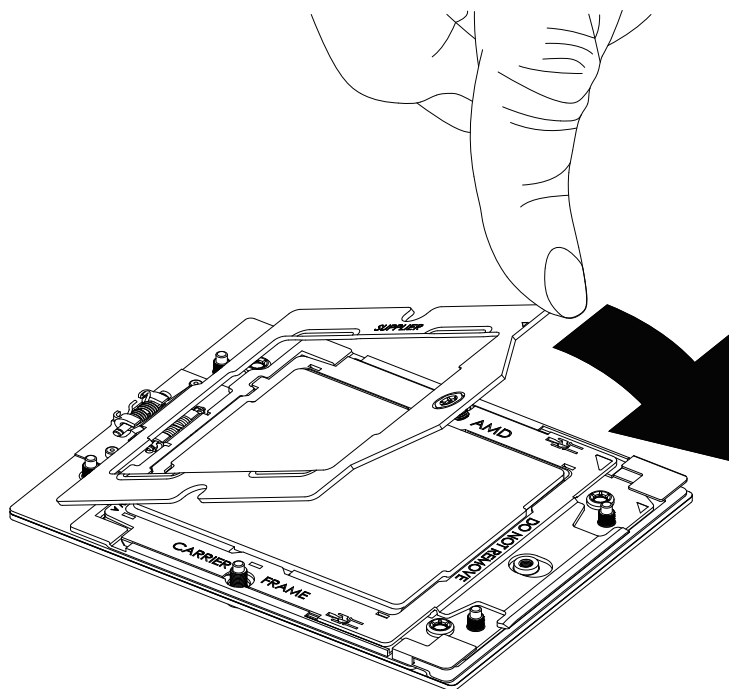
Note: You can only install the APU inside the socket in one direction with the handle at the top. Make sure that it is properly inserted into the APU socket before closing the rail frame plate. If it doesn't close properly, do not force it as it may damage your APU. Instead, open the rail frame plate again, and double-check that the APU is aligned properly.

7. Lift up the rail frame till it securely rests in upright position. Then remove the PnP cover cap from the APU socket below. Grip the two lift tabs marked "Remove" at the middle of the cap and pull vertically upwards to remove the PnP cover cap.

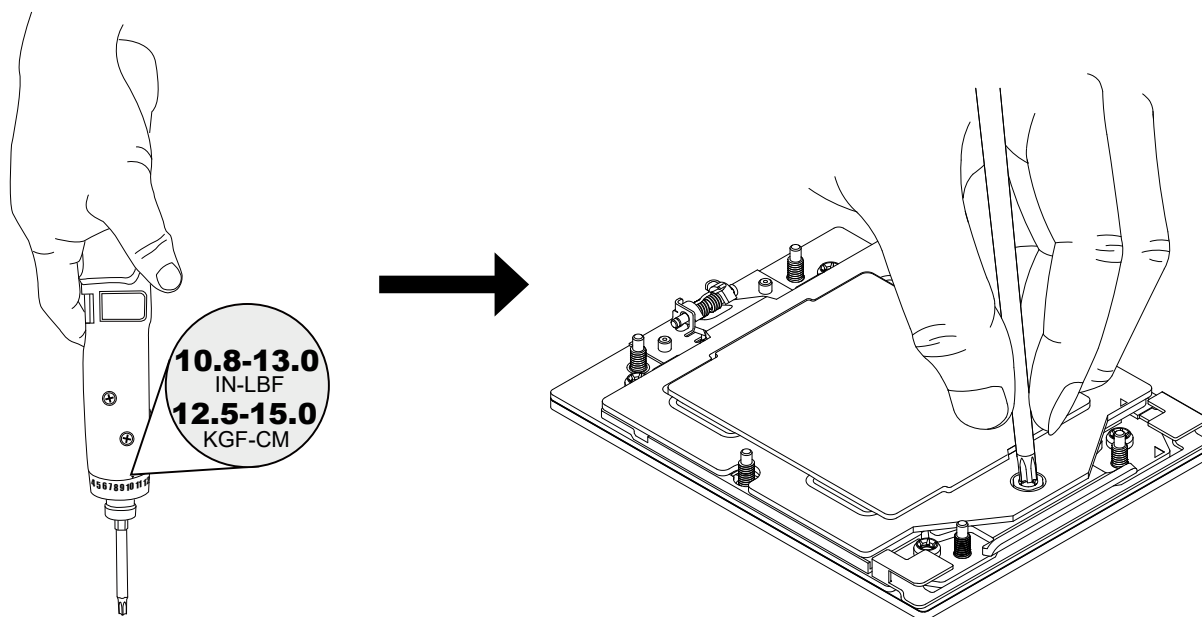


Warning! The exposed socket contacts are extremely vulnerable and can be damaged easily. Do not touch or drop objects onto the contacts and be careful removing the PnP cover cap and when placing the rail frame over the socket.

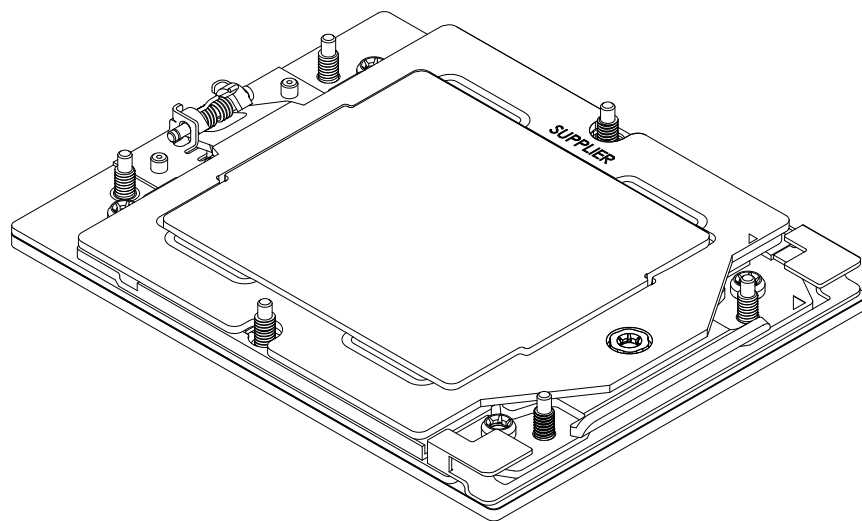
8. Gently lower the rail frame down onto the socket until the latches on the rail frame engage with the socket housing and it rests in place. **DO NOT** force it into place!



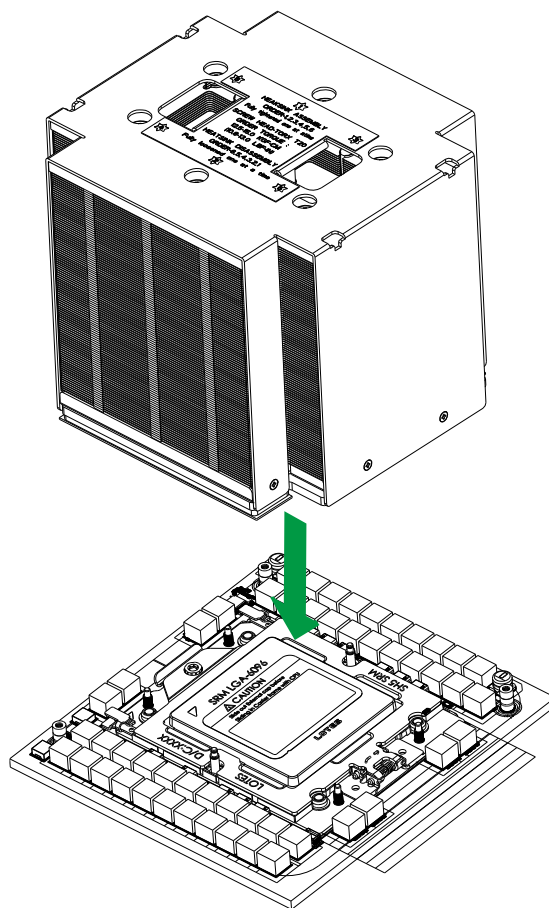
9. The force frame is spring loaded and has to be held in place before it is secured. **Important: Use a T20 bit torque driver with a torque of 12.5-15.0 kgf-cm (10.8-13.0 in-lbf) to prevent damage to the processor.**



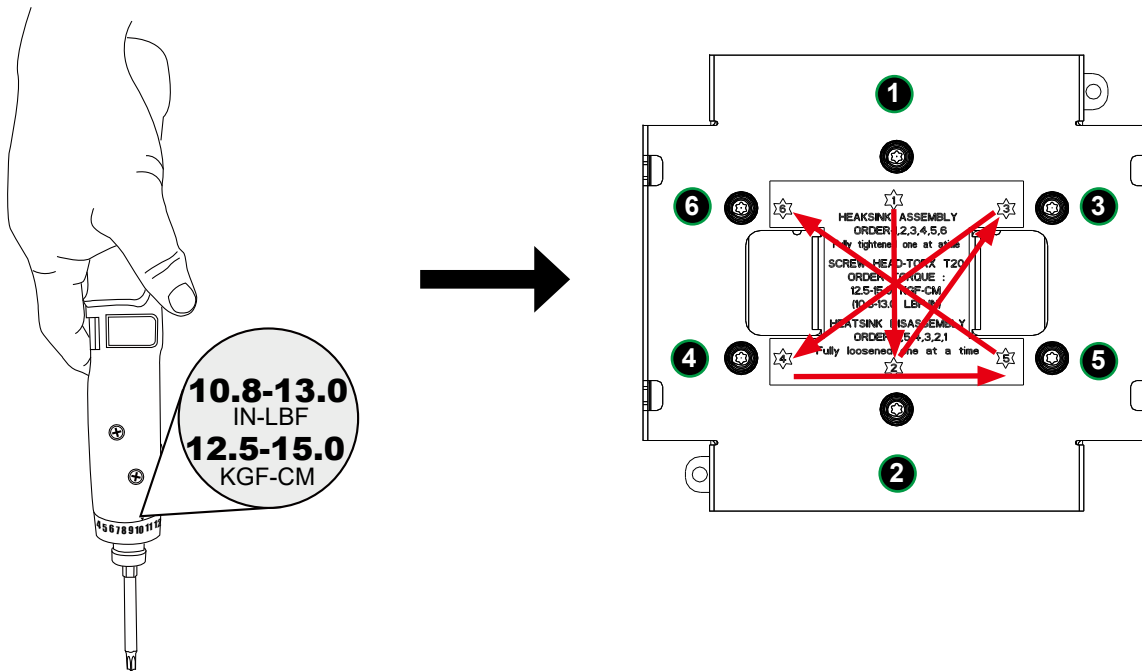
10. Replace and tighten the screws in the same order they were removed. When finished, the force frame will be secure over both the rail frame and APU package.



11. After the force frame is secured and the APU package is in place, now you must install the heatsink to the frame. Lower the heatsink down till it rests securely over the six screw holes on APU package on the socket frame.



12. Using a diagonal pattern, tighten the six screws down on the heatsink in a clockwise fashion until secure. Use a **T20 bit torque driver with a torque of 12.5-15.0 kgf-cm (10.8-13.0 in-lbf)** to prevent damage to the processor. The heatsink will now be secured and you have finished installing the processor and heatsink onto the motherboard. Repeat this procedure for any remaining APU sockets on the motherboard.



Note: Refer to system manual for detailed information of 2U (liquid cooling) and 4U (air cooling) installation.

Un-installing the Processor and Heatsink

1. Remove the heatsink attached to the top of the APU package by reversing the installation procedure.
2. Clean the thermal grease left by the heatsink on the APU package lid to limit the risk of it contaminating the APU package land pads or contacts in the socket housing.
3. Unscrew the plate and lift the force frame to the vertical position.
4. Lift the rail frame using the lift tabs near the front end of the rail frame. Note that the rail frame is spring loaded, so be careful lifting it up into a vertical position.
5. Grip the handle of the carrier frame and pull upwards to extract it from the rail frame. Return the carrier frame/APU package to its original shipping container.
6. Grip the handle on the external cap and return it to the rail frame sliding it downwards till it rests in the frame.
7. Grip the rail frame, rotate it downwards till it rests above and locks over the socket housing in its horizontal position.
8. Push and rotate down the force frame till it is over the external cap and rail frame into a horizontal position.
9. While holding down the force frame, secure it back to the socket frame by securing screw #1 in place.

2.4 Connectors

Power Connections

Power Supply Connectors (PSU1/PSU2)

Two PDUs (Power Distribution Units) can be connected to PSU1/PSU2 and support a total of four Supermicro proprietary power supply units that provide the main power to your system.

4-Pin Backplane Power Connector (JPWR1-2)

Four 4-pin power connectors for backplane devices. Refer to the table below for pin definitions.

Power Connector Pin Definitions	
Pin#	Definition
1	GND
2	GND
3	12 V
4	5 V

8-Pin Fan Power Connector (JPWR3-9)

Seven 8-pin fan power connectors. Refer to the table below for pin definitions.

Power Connector Pin Definitions			
Pin#	Definition	Pin#	Definition
1	GND	5	12 V
2	GND	6	12 V
3	GND	7	12 V
4	GND	8	12 V

Headers

Fan Headers

There are eight 4-pin fan headers (FAN 1-FAN 8) used for your system cooling fans. Additionally, four 6-pin fan headers (FAN 9-FAN 12), located at the rear side of the chassis, are for fans used to cool the backplane. In addition, an Fan_PMB header used for I²C temperature sensor cooling is located at JFAN1. Fan speed control for these fans is supported by thermal management via the BMC interface. Refer to the table below for pin definitions.

4-Pin Fan Headers Pin Definitions	
Pin#	Definition
1	GND
2	12 V
3	FANIO
4	PWM

6-Pin Fan Headers Pin Definitions	
Pin#	Definition
1	GND
2	12 V
3	FANIO
4	PWM
5	12 V
6	GND

Fan_PMB Header Pin Definitions			
Pin#	Definition	Pin#	Definition
1	SDA	5	GND
2	GND	6	12 V
3	SCL	7	FANIO
4	P3V3_AUX	8	PWM

STBY-FAN (FAN13)

STBY-FAN is a standby power header for the fan board. Refer to the table below for pin definitions.

STBY-FAN (FAN13) Pin Definitions	
Pin#	Definition
1	Fan PWM
2	Fan IO
3	12 V
4	GND

NC-SI Connector

A Network-Controller Sideband Interface (NC-SI) header is located at JNCSI1 on the motherboard. The NCSI header is used to connect a Network Interface Card (NIC) to the motherboard so that the BMC is able to poll the temperature reading from it.

TPM/Port 80 Header

A Trusted Platform Module (TPM)/Port 80 header is located at JTPM1 to provide TPM support and Port 80 connection. Use this header to enhance system performance and data security. Refer to the table below for pin definitions. Please 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	NC
9	3.3 V Stby	10	SPI_IRQ#

PCIe I²C Header

A PCIe I²C (SMBus) header is located at JRSI2C1 on the motherboard. The PCIe SMBus connector is used for PCIe cards to allow the BMC or the BIOS to read storage drive information or FRUs more effectively.

BMC SMB I²C Header

A System Management Bus I²C header for the BMC is located at JIPMB1. Connect the appropriate cable here to use the 4-pin BMC external I²C connection on your system.

SMB I²C for 2U Power Distribution Board (PDB) Headers

Two System Management Bus I²C for the power distribution boards are located at PDB1_SB and PDB2_SB. Connect a cable to PDB1_SB for Power Distribution Board 1 support, and connect a cable to PDB2_SB for Power Distribution Board 2 support.

4-pin Leakage Detection (JPL0)

Refer to the table below for pin definitions.

4-pin Leakage Detection Jumper Settings (JPL0)	
Pin#	Definition
1	GND
2	12 V
3	Liquid Detect
4	Present

Chassis Intrusion

A chassis intrusion header is located at JL1 on the motherboard. Attach the appropriate cable from the chassis to inform you when the chassis is opened. Refer to the table below for pin definitions.

Chassis Intrusion Pin Definitions	
Pin#	Definition
1	Intrusion Input
2	Ground

JMD1/JMD2

Two hybrid M.2 slots are located at JMD1 and JMD2. JMD1 supports an M.2 SATA 2:0/PCIe 4.0 x2 hybrid slot, and JMD2 supports an M.2 SATA 2:4/PCIe 4.0 x1 slot. Both JMD1 and JMD2 slots support PCIe 4.0 devices in the 2280/22110 form factors. M.2 allows for a variety of card sizes, increased functionality, and spatial efficiency.

AIOM Sideband Signal Headers (AIOM1_SB/AIOM2_SB)

Advanced I/O Module (AIOM) PCIe 5.0 x8 slot supported by the APU.

Onboard Battery (BT1)

The onboard backup battery is located at BT1. It provides backup power to the on-chip CMOS, which stores the BIOS setup information. It also provides power to the Real-Time-Clock (RTC) to keep it running.

BMC (JIO1)

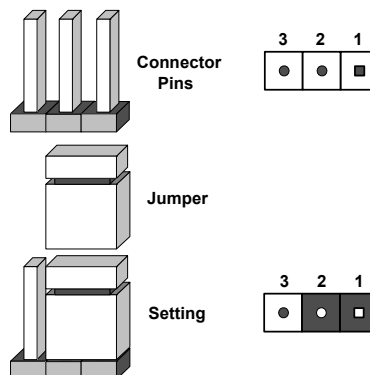
This is the I/O board socket used to connect the I/O board to the motherboard.

2.5 Jumper Settings

How Jumpers Work

To modify the operation of the motherboard, jumpers are used to choose between optional settings. Jumpers create shorts between two pins to change the function associated with it. Pin 1 is identified with a square solder pad on the printed circuit board. See the motherboard layout page for jumper locations.

Note: On a two-pin jumper, "Closed" means the jumper is on both pins and "Open" indicates the jumper is either on only one pin or has been completely removed.



Clear CMOS

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. Pull out the motherboard tray to access the motherboard.
3. Remove the CMOS battery from the motherboard.
4. Wait for around 30 seconds, and then re-install the CMOS battery on the motherboard.
5. Re-install the motherboard tray, reconnect the power cord(s), and power on the system.

Notes: Clearing CMOS will also clear all passwords.

Power Button and Front IUD Button Select Jumper

Jumper JRU1 is used to configure pin 2 of Front Control Panel header 1 (FP1) to function as a Power button or as the Front UID button. To set pin 2 of FP1 for Front UID use in a chassis that supports front UID connection, close pin 1 and pin 2 of Jumper JRU1. To set pin 2 of FP1 for Power Signal use, keep jumper JRU1 open. Refer to the table below for JRU1 settings.

Front UID Button/Power Button Select Jumper (JRU1) Jumper Settings	
State	Description
Close pin 1 and pin 2 of JRU1	Pin 2 of FP1: used for Front UID button (Default)
Keep pin 1 and pin 2 of JRU1 Open	Pin 2 of FP1: used for Power button

Video Display Enable

Jumper JPG1 is used to enable or disable the onboard VGA connector. The default setting is pins 1-2 to enable the connection. See the table below for jumper settings.

Video Display Enable Jumper Settings (JPG1)	
Jumper Setting	Definition
Pins 1-2	Video Display Enabled (Default)
Pins 2-3	Video Display Disabled

SKUID Jumpers (JSKUID1-3)

Refer to system manual for details.

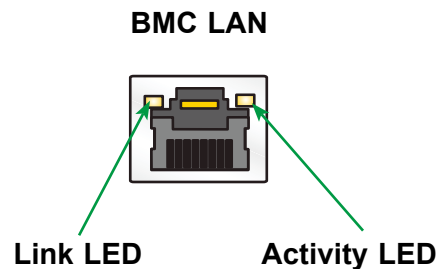
2.6 LED Indicators

BMC LAN Port LEDs

A dedicated BMC LAN connection is located on the rear I/O panel and has two LED indicators. The LED on the right indicates connection and activity, while the LED on the left indicates the speed of the connection. The Link LED may amber, green, or off to indicate the speed of the connection. Refer to the tables below for more information.

Link LED, Connection Link Speed Indicator	
LED Color	Definition
Amber	1 Gb/s
Green	100 Mb/s
Off	10 Mb/s

Activity LED		
Color	State	Definition
None	No Connection	
Yellow	Solid On	Link
Yellow	Flashing	Active



UID LED Indicator

The rear UID LED is located on the I/O board, while the front UID LED is located on the front panel. When you press the UID switch, both the rear and front UID LED indicators will turn on. Press the UID switch again to turn off the LED indicators. Use this UID Indicator to 'mark' the system, so it can be easily identified whether on the front or back (e.g., a system rack with multiple units installed).

UID LED Indicator		
Color	State	Definition
None	Off	UID Off
Blue	Solid On	Unit Identified by Local Site
Blue	Slow Blinking	Unit Identified by Remote Site
Blue	Fast Blinking	System Recovery

Onboard Power LED (LED1)

The Onboard Power LED (LEDPWR) is located at LED1 on the motherboard. When this LED is on, the system power is on. Be sure to turn off the system power and unplug the power cords before removing or installing components. Refer to the table below for more information.

Onboard Power LED Indicator (LED1) LED Status	
LED Color	Definition
Off	System Power Off (power cable not connected)
Green	System Power On

BMC Heartbeat LED (LED3)

A BMC Heartbeat LED is located at LED3 on the motherboard. When LED3 is blinking green, the BMC is functioning normally. Refer to the table below for more information.

BMC Heartbeat LED Indicator (LED3) LED Status		
Color	State	Definition
Green	Solid On	BMC is not ready
Green	Blinking	BMC Normal
Green	Fast Blinking	BMC: Initializing

PCIe Switch Heartbeat LED (LED9)

A PCIe Switch Heartbeat LED is located at LED9 on the motherboard. When LED9 is blinking green, the PCIe Switch is functioning normally. Refer to the table below for more information.

PCIe Switch Heartbeat LED Indicator (LED9) LED Status		
Color	State	Definition
Green	Solid On	PCIe Switch is not ready
Green	Blinking	PCIe Switch Normal
Green	Fast Blinking	PCIe Switch: Initializing

PCIe Switch Error (LED10)

This LED will be solid red when the board is in standby power mode. If this LED is solid red when the board is on, there is an error with the PCIe switch.

APU Power Status LED Indicators

APU Power Status LED indicators are located at LED5, LED6, and LED7. When an APU power supply fails, the corresponding Power Status LED will turn solid red. Refer to the table below for more details.

APU Power Status LED Indicators (LED5, LED6, and LED7)		
LED Status		
LED#	Color	Definition
LED5	Solid Red	APU2 Power Failure
LED6	Solid Red	APU3 Power Failure
LED7	Solid Red	APU4 Power Failure

2.7 Front Control Panel

There are two front control panel headers located on this motherboard. Front control panel header 1, located at FP1, contains header pins for various buttons and LED indications with I²C support for front access. Front control panel header 2, located at FP2, provides additional functions, including USB and VGA support to the system. These front control panel headers are designed specifically for use with Supermicro chassis.

Pin Definitions of FP1 (JF1)

Front Control Panel		
1	○	Power Button
2	○	Reset/UID Button
3	○	UID LED_N
4	○	Fail LED_N (OH/FF/PF)
5	○	LAN-2 Activity LED
6	○	LAN-1 Activity LED (Aggregate all LAN)
7	○	HDD Activity LED
8	○	Standby LED_N
9	○	Power/RoT LED_N
10	○	P3V3_STBY
11	○	Ground
12	○	I ² C Data
13	○	I ² C Clock
14	○	Ground
15	○	Power Fail LED_P
16	○	P5V_USB
17	○	P5V_USB
18	○	P5V_USB
19	○	Power Fail LED_N
20	○	Ground

Figure 4-2. FP1 (JF1) Header Pins

Power On and BMC/BIOS Status LED Button

The Power On and BMC/BIOS Status LED button is located on pin 1 of front control panel header 1 (FP1). Momentarily contacting pin 1 of FP1 will power on/off the system or display BMC/BIOS status. Refer to the table below for more information.

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

BMC Reset Button/Front UID Switch

The BMC Reset button/Front UID switch connection is on pin 2 of FP1, and it is used in conjunction with the JRU1 Reset button/UID switch select jumper. Close pin 1 and pin 2 of jumper JRU1 to configure pin 2 of FP1 for front UID switch use in a chassis that supports front UID connection. To set pin 2 of FP1 for BMC Reset, close pin 3 and pin 4 of jumper JRU1.

Front UID Switch/Reset Button Select Jumper (JRU1) Jumper Settings	
State	Description
Close pin 1 and pin 2 of JRU1	Pin 2 of FP1: used for front UID switch support
Close pin 3 and pin 4 of JRU1	Pin 2 of FP1: used for BMC Reset support

UID LED

The unit identifier LED connection is located on pin 3 of FP1.

Fail LED (Information LED for OH/FF/PF)

The Fail LED (Information LED for OH/Fan Fail/PWR Fail) connection is located on pin 4 of FP1. This LED provides warnings of overheating, power failure, or fan failure. See the table below for FP1 pin definitions.

Power Button BMC/BIOS Status LED Indicator	
Status	Description
Solid red (on)	An overheat condition has occurred.
Blinking red (1 Hz)	Fan failure: check for an inoperative fan
Blinking red (0.25 Hz)	Power failure: check for a non-operational power supply
Blinking red (10 Hz) (FP red LED)	CPLD recovery mode error(s)
Solid blue	UID has been activated locally. Use this function to locate a unit in a rack mount environment that might be in need of service.
Blinking blue (1 Hz)	Local UID has been activated remotely. Use this function to identify a unit that might be in need of service.
BIOS/BMC blinking blue (10 Hz)	BIOS/BMC: recovery and/or update in progress
Red Info LED blinking (10 Hz) and MB UID LED blue blinking (10 Hz)	CPLD: recovery and/or update in progress

LAN1/LAN2 (NIC1/NIC2)

The NIC (Network Interface Controller) LED connection for LAN Port 1 is located on pin 6 of FP1, and LAN Port 2 is on pin 5. See the table below for FP1 pin definitions.

LAN1/LAN2 LED LED States	
Color	State
NIC 2: Blinking green	LAN 2: Active
NIC 1: Blinking green	LAN 1: Active

Drive Activity LED

The drive activity LED connection is located on pin 7 of FP1. When this LED is blinking green, it indicates drive activity. Refer to the table below.

Drive Activity LED LED State	
Color	State
Blinking Green	Drive Active

Standby Power LED

The LED indicator for standby power is located on pin 8 of FP1. If this LED is on, standby power is on.

RoT (Root of Trust) Power LED

The Power LED for RoT (Root of Trust) connection is located on pin 9 of FP1. If this LED is on, power for the RoT chip is on.

Standby Power

A Standby Power (I²C) connection is located on pin 10 - pin 14 of FP1 to provide power to the system when it is in standby mode. Refer to the table below for pin definitions.

3.3V Standby PWR Pin Definitions	
Pin#	Definition
10	P3V3 Standby
11	Ground
12	I ² C Data
13	I ² C Clock
14	Ground

Power Fail LED Indicator connections

Power Failure LED Indicator connections are located on pin 15 and pin 19 of FP1. Refer to the table below for pin definitions.

FP Power LED Pin Definitions (FP1)	
Pin#	Definition
15	PWR Failure LED-Positive
19	PWR Failure LED-Negative

FP USB Power

Front Panel USB power connections are located on pin 16 - pin 18 of FP1 to provide power to front USB devices. Refer to the table below for pin definitions.

FP USB PWR Pin Definitions	
Pin#	Definition
16	+5V USB PWR
17	
18	

2. Front Control Panel Header with I²C (FP1)

In addition to Front Control Panel header 1 (FP1), another Front Control Panel header, located at FP2, supports a VGA connector and two USB 2.0 ports (USB 3/4).

Front Control Panel Header 2 (FP2)

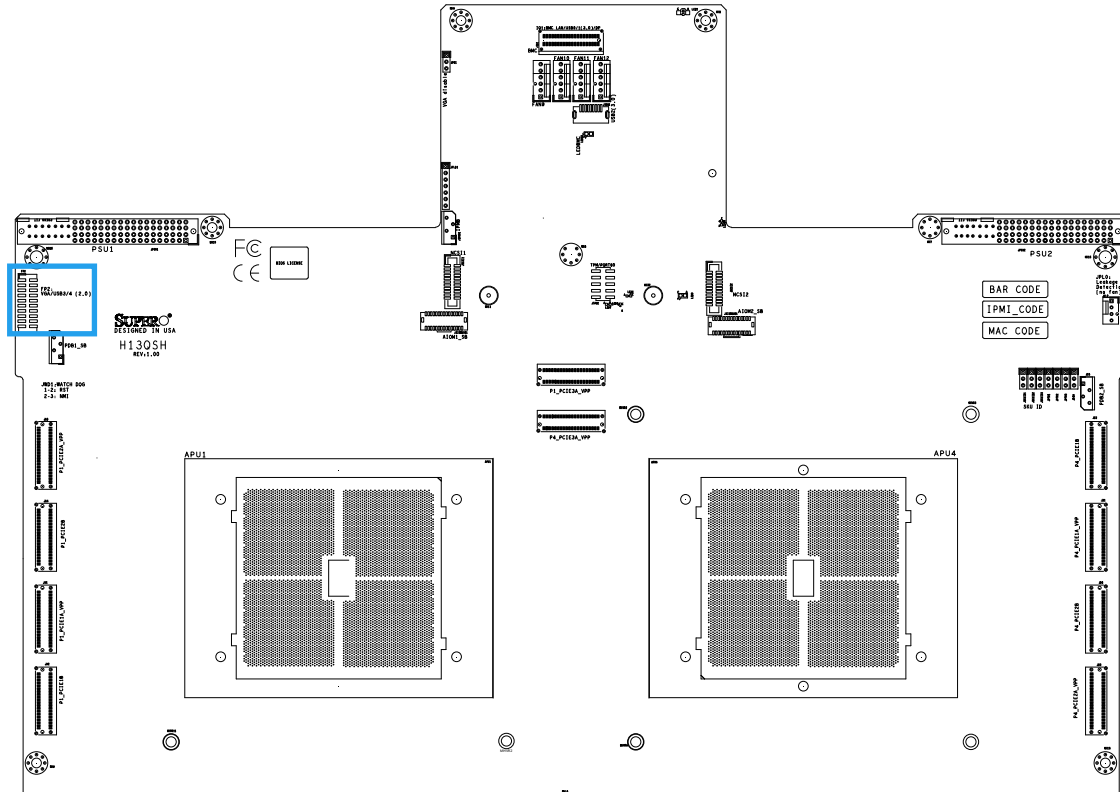


Figure 2-3. Location of FP2

2.8 M.2 Solid State Drive Installation

Installing Dual M.2 SSDs

1. Disconnect power from the system.
2. Refer to the [motherboard layout](#) and locate the M.2 dual slots (JMD1/2).
3. Insert the lower M.2 sideways into the connector so that it lays flat, then follow the instructions below from ① to ③.
4. Insert the upper M.2 sideways into the connector so that it lays flat, then follow the instructions below from ④ to ⑥.

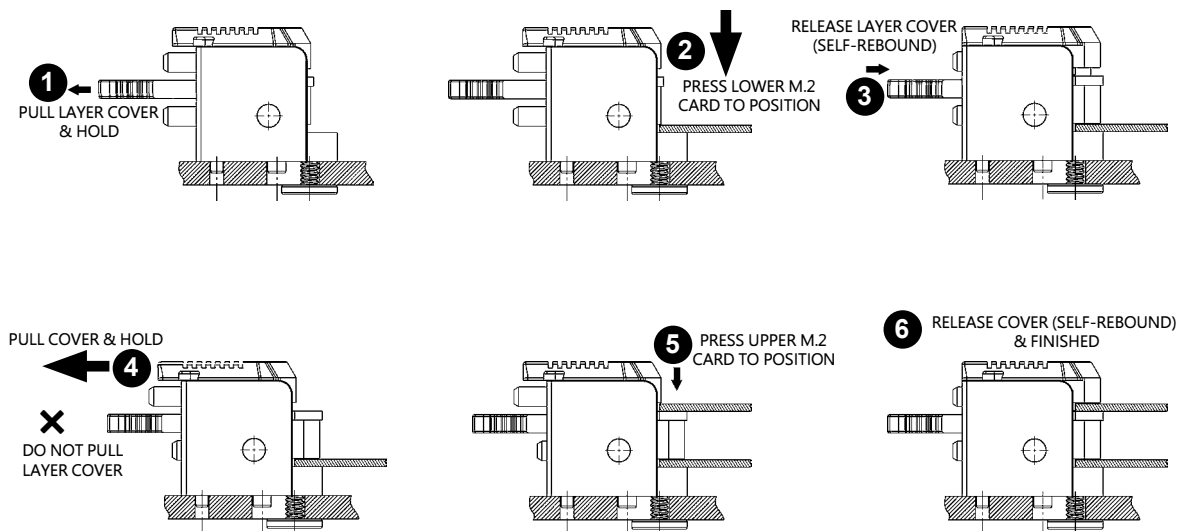


Figure 2-4. Installing Dual M.2 SSDs

Releasing Dual M.2 SSDs

1. Follow the instructions below from ① to ⑤ to remove M.2 SSDs.

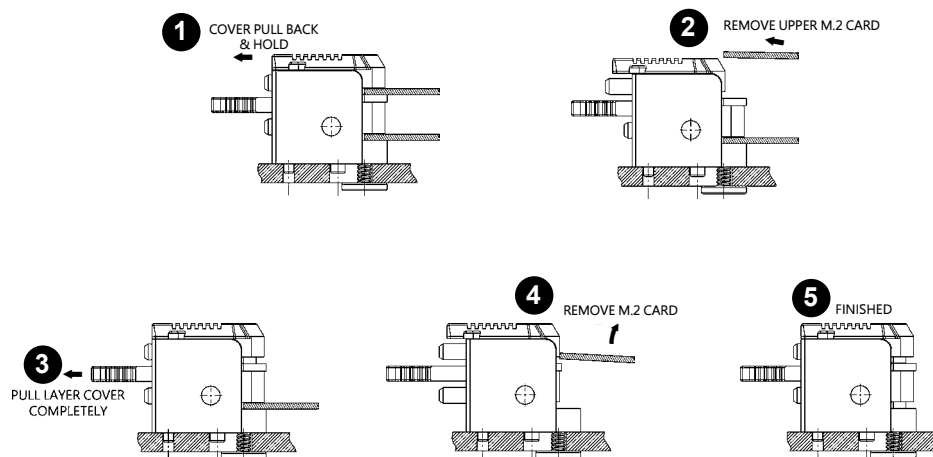


Figure 2-5. Releasing Dual M.2 SSDs

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. Check that the BMC_HB LED is blinking before the motherboard is turned on.
2. Check that the PWROK LED on the motherboard is on.
3. Make sure that the power connector is connected to your power supply.
4. Make sure that no short circuits exist between the motherboard and chassis.
5. Disconnect all cables from the motherboard, including those for the keyboard and mouse.
6. Remove all add-on cards.
7. Install an APU and a heatsink* on the motherboard. Check all jumper settings properly.
*Make sure that the heatsink is fully seated.
8. Use the correct type of onboard CMOS battery (CR2032) as recommended by the manufacturer. To avoid possible explosion, do not install the CMOS battery upside down.

No Power

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

No Video

1. Check that the VGA cable is connected properly, and the monitor is on.

Note: If you are a system integrator, VAR or OEM, a POST diagnostics card is recommended.

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. Clear the CMOS settings by unplugging the power cord and remove the battery for 30 seconds. Refer to Chapter 2, [Section 2.5](#).
2. Remove all components from the motherboard, especially the DIMM modules.

The System Cannot Retain the Setup Configuration

1. Make sure that you are using a high quality power supply. A poor quality power supply may cause the system to lose the CMOS setup information. Refer to [Section 1](#) for details on power supplies.
2. The battery on your motherboard may be old. Check to verify that it still supplies approximately 3 VDC. If it does not, replace it with a new one.
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. APU/BIOS support: Make sure that your APU is supported and that you have the latest BIOS installed in your system.

Note: Refer to the product page on our website at <http://www.supermicro.com> for memory and APU support and updates.

2. Storage drives support: Make sure that all storage drives work properly. Replace the bad storage drives with good ones.
3. System cooling: Check the system cooling to make sure that all heatsink fans and APU/system fans, etc., work properly. Check the hardware monitoring settings in the IPMI to make sure that the APU and system temperatures are within the normal range. Also check the front panel Overheat LED and make sure that it is not on.

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

3.2 Technical Support Procedures

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

1. Please review the 'Troubleshooting Procedures' and 'Frequently Asked Questions' (FAQs) sections in this chapter or see the FAQs on our website before contacting Technical Support.
2. BIOS upgrades can be downloaded from our website.

Note: Not all BIOS can be flashed depending on the modifications to the boot block code.

3. If you still cannot resolve the problem, include the following information when contacting us for technical support:
 - Motherboard model and PCB revision number
 - BIOS release date/version (this can be seen on the initial display when your system first boots up)
 - System configuration

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

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

3.3 Frequently Asked Questions

Question: What type of memory does my motherboard support?

Answer: The H13QSH motherboard supports up to 512 GB HBM3 (128 GB per Socket) which is embedded in the APU.

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>.

To update your BIOS:

1. Please check the BIOS warning message and the information on how to update your BIOS on our website.
2. Select your motherboard model and check the current BIOS revision to make sure it is newer than your motherboard's installed BIOS before downloading.
3. Download the zip file and save the BIOS package to your computer.
4. Unzip the BIOS files onto a USB stick with FAT/FAT32 file system.
5. Boot to the motherboard's built-in UEFI Shell and type the following to start the BIOS update process:

```
FLASH.nsh BIOSname#.### <ENTER>
```

Note: Supermicro no longer supports the BIOS update method in DOS.

6. Perform an A/C power cycle after the message indicating the BIOS update has completed. You may refer to the "Readme" file in BIOS package for more details.

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

Answer: The instant power off function is controlled in BIOS by the Power Button Mode setting. When the On/Off feature is enabled, the motherboard will have instant off capabilities as long as the BIOS has control of the system. When the 4 Seconds Override feature is enabled or when the BIOS is not in control such as during memory count (the first screen that appears when the system is turned on), the momentary on/off switch must be held for more than four seconds to shutdown the system. This feature is required to implement the ACPI features on the motherboard.

3.4 Returning Merchandise for Service

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

For faster service, RMA authorizations may be requested online (<http://www.supermicro.com/support/rma/>).

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

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

3.5 Battery Removal and Installation

Battery Removal

To remove the onboard battery, follow the steps below:

1. Power off your system and unplug your power cable.
2. Locate the onboard battery (see Figure 3-1).
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

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 in Battery Removal section 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.

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

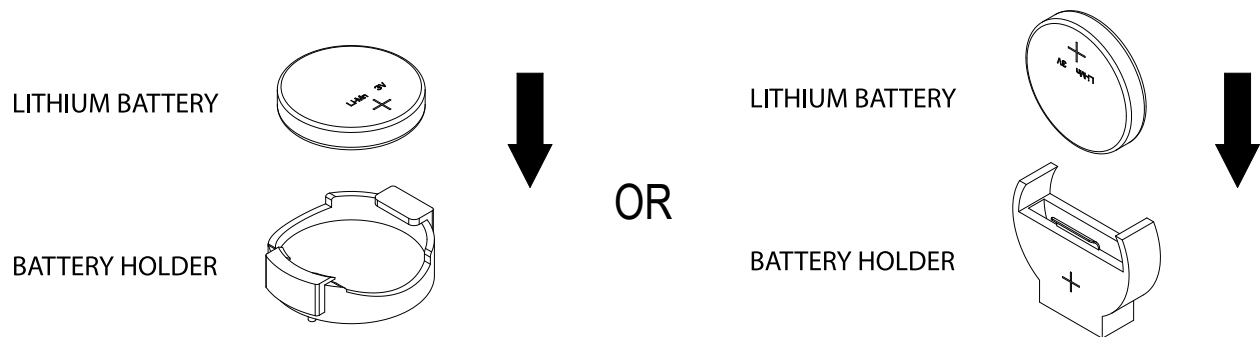


Figure 3-1. Battery Installation

Chapter 4

BIOS

4.1 Introduction

This chapter describes the AMIBIOS™ Setup utility for the H13QSH motherboard. The BIOS is stored on a chip and can be easily upgraded using a flash program.

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

Starting the Setup Utility

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

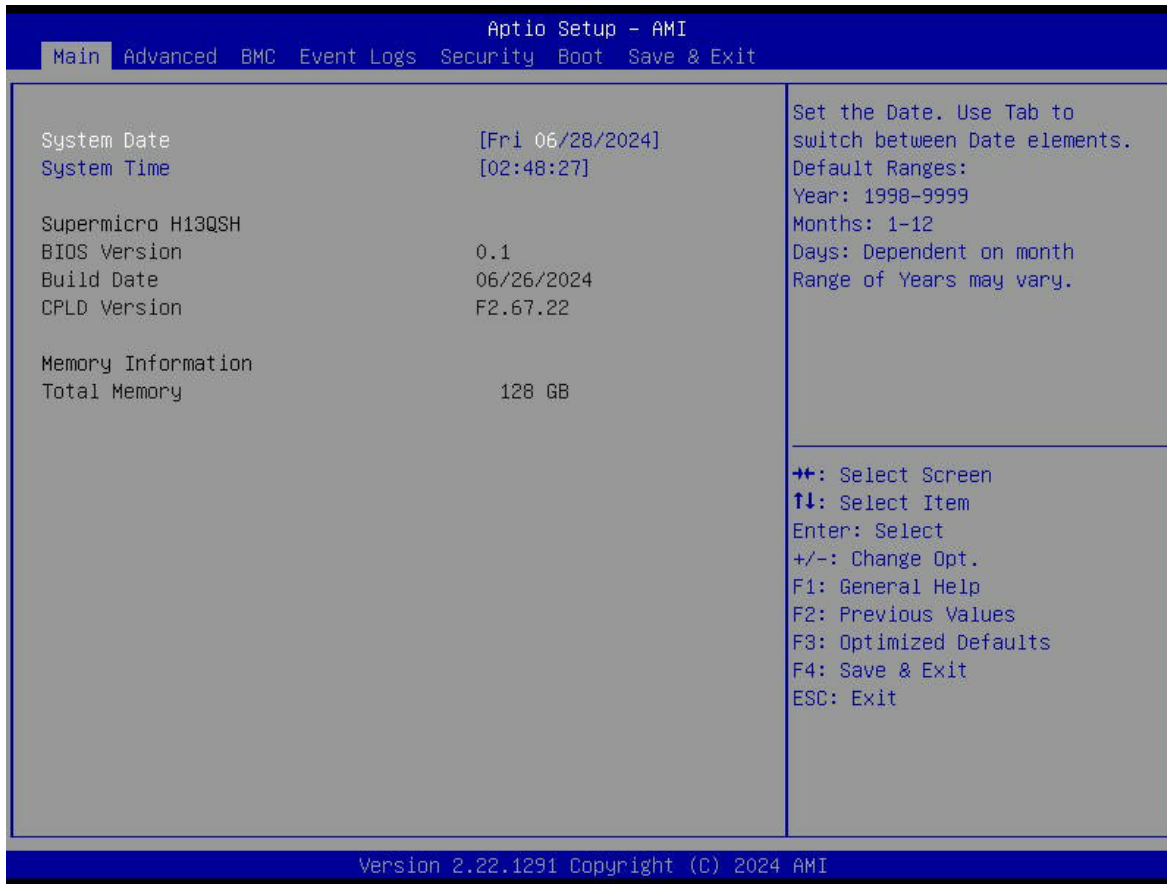
The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. "Grayed-out" options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is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

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

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

4.2 Main Setup

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



System Date/System Time

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

Note: The time is in the 24-hour format. For example, 5:30 P.M. appears as 17:30:00. The date's default value is 01/01/2015 after RTC reset.

Supermicro H13QSH**BIOS Version**

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

Build Date

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

CPLD Version

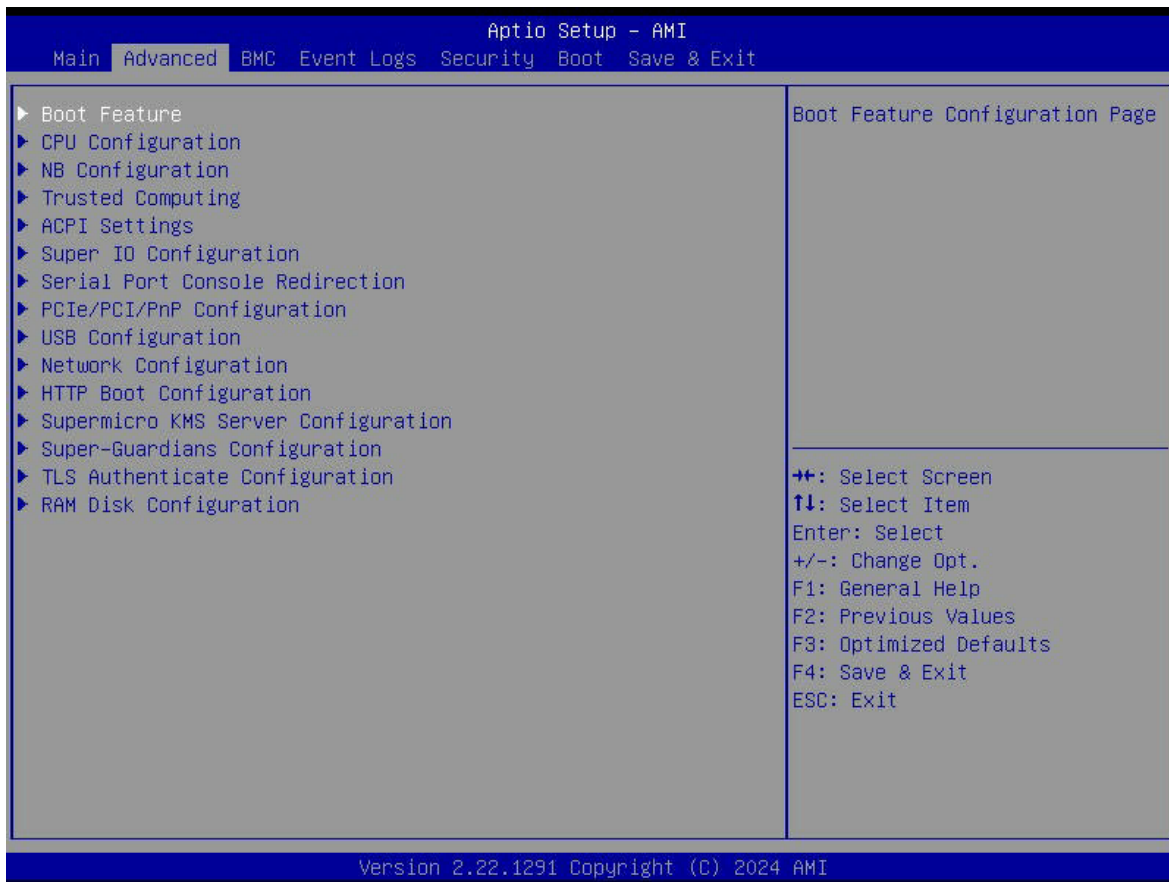
This item displays the CPLD version of the BIOS ROM used in the system.

Memory Information**Total Memory**

This item 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

Boot Configuration

Quiet Boot

Use this feature to select the screen display between the Power-on Self Test (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**.

Bootup NumLock State

Use this feature to select the keyboard <Numlock> state. 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**.

Re-try Boot

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

Power Configuration**Watch Dog Function**

If enabled, the Watch Dog Timer will allow the system to reset or generate NMI based on jumper settings when it is expired for more than 5 minutes. The options are **Disabled** and Enabled.

Restore on AC Power Loss

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

Power Button Function

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

►CPU Configuration**CPU Configuration****SMT Control**

Use this setting to specify Symmetric Multithreading. Options include Disabled, Enabled, and **Auto**.

Core Performance Boost

This setting is used to configure for Core Performance Boost. Options include Disabled and **Auto**.

Global C-state Control

This setting is used to configure for Global C-state Control. Options include Disabled, Enabled, and **Auto**.

SEV-ES ASID Space Limit

This setting customize SEV-VS ASID space limit. The default value is **1**.

PPIN Opt-in

The Protected Processor Identification Number (PPIN) is a unique serial number for each processor. The options include Disabled, Enabled, and **Auto**.

SNP Memory (RMP Table) Coverage

Select Enabled to set the entire system memory covered. The options include Disabled, Enabled, Custom, and **Auto**.

SMEE

This feature sets the option to enable or disable Secure Memory Encryption. The options are Disabled, Enabled, and **Auto**.

Fast Short REP MOVSB (FSRM)

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

Enhanced REP MOVSB/STOSB (ERSM)

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

L1 Stream HW Prefetcher / L2 Stream HW Prefetcher

This setting is used to enable or disable the L1/L2 Stream Hardware Prefetcher. The options are Disabled, Enabled, and **Auto**.

CCD Control

Use this setting to disable CCDs in the CPU. Options include **Auto**, 2 CCDs, 3 CCDs, 4 CCDs, 5 CCDs, 6 CCDs, 7 CCDs, 8 CCDs, 9 CCDs, 10 CCDs, and 11 CCDs.

Core Control

This sets the number of cores to be used by your system. Once this option has been used to remove any cores, a power cycle is required in order for the future selections to take effect. Options include **Auto**, ONE (1+0), TWO (2+0), THREE (3+0), FOUR (4+0), FIVE (5+0), SIX (6+0), and SEVEN (7+0). If unsure, leave this to Auto.

SVM Mode

This setting Disables or **Enables** CPU Virtualization.

▶ CPU1 Information**CPU Information**

These sections are for informational purposes. They will display some details about the detected CPUs on the motherboard, such as:

- CPU Version
- Number of Cores Running
- Processor Family
- Processor Model
- Microcode Patch Level
- L1 Instruction Cache (Size/Method)
- L1 Data Cache (Size/Method)
- L2 Cache (Size/Method)
- L3 Cache per Socket (Size/Method)

CPU1 PCIe Package Group G0

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

CPU1 PCIe Package Group G1

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

► CPU2 Information

CPU2 Information

CPU2 PCIe Package Group G0

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

CP2 PCIe Package Group G1

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

► CPU3 Information

CPU3 Information

CPU3 PCIe Package Group G0

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

CP3 PCIe Package Group G1

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

► CPU4 Information

CPU4 Information

CPU4 PCIe Package Group G0

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

CP4 PCIe Package Group G1

This setting selects the PCIe port bifurcation configuration for the selected slot. The options include **Auto**, x4x4x4x4, x8x4x4, x8x8, and x16.

► NB Configuration

North Bridge Configuration

IOMMU

Use this setting to enable/disable IOMMU. Options include **Disabled**, Enabled, and Auto.

DMAR Support

Use this setting to enable/disable DMAR system protection during POST. Options include Disabled, Enabled, and **Auto**.

DRTM Virtual Device Support

Use this setting to enable/disable DRTM ACPI virtual device. Options include Disabled, Enabled, and **Auto**.

ACS Enable

Options include **Enabled**, Disabled, and Auto.

TDP Control

Use this setting to configure the cTDP Control. Options include Manual and **Auto**.

Package Power Limit Control

Use this setting for Package Power Limit Control. Options include Manual and **Auto**.

Determinism Control

Use this setting to configure the Determinism Slider. Options include Manual and **Auto**.

APBDIS

Use this setting to set APBDIS. Options include 0, 1, and **Auto**.

Data Link Feature Cap

Use this setting to set Data Link Feature Cap. Options include Enabled, Disabled, and **Auto**.

SEV-SNP Support

Use this setting for SEV-SNP Support. Options include **Disabled**, Enabled, and Auto.

▶ xGMI Configuration

xGMI Link Width Control

Options include Manual and **Auto**.

▶ Memory Configuration

Memory Interleaving

This setting controls fabric level memory interleaving. Note that the channel, die and socket have requirements on memory populations and it will be ignored if the memory doesn't support the selected option. Options include Disabled and **Auto**.

▶ CPU1/2/3/4 Memory Information

CPU1 Memory Information

These sections are for informational purposes. They will display some details about the detected memory according to each CPU on the motherboard, such as:

- Detected Size (per slot, in MB)
- Current Speed (MT/s)

▶ Trusted Computing

Configuration

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 **Disabled** and Enabled.

▶ ACPI Settings

ACPI Settings

High Precision Event Timer

The High Precision Event Timer (HPET) can produce periodic interrupts and is used to synchronize multimedia streams, providing smooth playback and reducing the need to use other timestamp calculations. The options are Disabled and **Enabled**.

PCI AER Support

Enables Advanced error reporting capability. The options are **Disabled** and Enabled.

NUMA Nodes Per Socket

Use this feature to specify the number of desired NUMA nodes per socket. The options are NPS0, NPS1, NPS2, NPS4, and **Auto**.

ACPI SRAT L3 Cache As NUMA Domain

Use this setting to enable/disable ACPI SRAT L3 Cache As NUMA Domain. The options are Disabled, Enabled, and **Auto**.

► Super IO Configuration

Super IO Configuration

The following Super IO information will display:

- Super IO Chip AST2600

► Serial Port 1 Configuration

Serial Port 1 Configuration

Serial Port

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

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. 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=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), and (IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;).

► Serial Port 2 Configuration

Serial Port 2 Configuration

Serial Port

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

Change Settings

This feature specifies the base I/O port address and the Interrupt Request address of a serial port specified by the user. Select Auto to allow the BIOS to automatically assign the base I/O and IRQ address. The options are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=2F8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), (IO=3E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;), and (IO=2E8h; IRQ=3, 4, 5, 6, 7, 9, 10, 11, 12;).

► Serial Port Console Redirection

COM1

Console Redirection

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

SOL

Console Redirection

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

► Console Redirection Settings

Terminal Type

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

Bits Per Second

Use this feature to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 384000, 57600, and **115200** (bits per second).

Data Bits

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

Parity

A parity bit can be sent with the data bits to detect some transmission errors. Options include **None**, Even, Odd, Mark, and Space.

Stop Bits

The setting indicates the end of a serial data packet. (A start bit indicates the beginning.) The standard setting is one stop bit. Communication with slow devices may require more than one stop bit. Options include 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

The options include 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 include Disabled and **Enabled**.

Legacy OS Redirection Resolution

Options include 80x24 and **80x25**.

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 include **VT100**, LINUX, XTERMR6, SC0, ESCN, and VT400.

Redirection After BIOS POST

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

Console Redirection

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

► Console Redirection Settings

Out-of-Band Mgmt Port

Microsoft Windows Emergency Management Services (EMS) allows for remote management of a Windows Server OS through a serial port. The options are **COM1** and SOL.

Terminal Type

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

Bits Per Second

Use this feature to set the transmission speed for a serial port used in Console Redirection. Make sure that the same speed is used in the host computer and the client computer. A lower transmission speed may be required for long and busy lines. The options are 9600, 19200, 384000, 57600, **115200**, 230400, 460800, 921600 (bits per second).

Flow Control

This feature can prevent data loss from buffer overflow. The options are **None**, Hardware RTS/CTS, Software Xon/Xoff.

► PCIe/PCI/PnP Configuration

This menu provides PCIe/PCI/PnP configuration settings and information.

PCI Bus Driver Version: A5.01.31

PCI Devices Common Settings:

Above 4G Decoding

This setting Disables or **Enables** 64-bit capable devices ability to be decoded in above 4G address space (only if the system supports 64-bit PCI decoding).

Re-Size BAR Support

If system has resizable BAR capable PCIe devices, use the options **Disable** or Enable resizable BAR support.

SR-IOV Support

If the system has SR-IOV capable PCIe devices, this setting will **Disable** or Enable the Single Root IO Virtualization Support for the system.

BME DMA Mitigation

Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridges after SMM Locked. The options are **Disabled** and Enabled.

ASPM Support

Use this setting to set the ASPM level. The options are **Disabled**, Auto, and Force L1.

PCIe ARI Support

Use this setting to Disable, Enable, or **Auto** control the Alternative Routing-ID Interpretation.

PCIe ARI Enumeration

Use this setting to Disable, Enable, or **Auto** control the ARI Forwarding Enable for each downstream port.

Relaxed Ordering

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

Clock Spread Spectrum

Use this setting to Disable or Enable CG1_PLL Spread Spectrum for your system. The options are **Disabled** and Enabled.

No Snoop

Select Enable to support no-snoop mode for each CB device. The options are Disabled and **Enabled**.

OnBrd/Ext VGA Select

Use this setting to select between onboard or external VGA support. The options are **Auto**, Onboard, and External.

PCIe Ten Bit Tag Support

Use this setting to Disable, Enable, or **Auto** control the PCIe ten bit tags for supported devices.

NVMe Firmware Source

Use this setting to select between the AMI Native firmware support or the device vendor-defined firmware support. The options are **Vendor Defined Firmware** and AMI Native Support.

PCI Devices Option Rom Setting

SLOT1 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

SLOT2 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

SLOT3 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

SLOT4 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

SLOT5 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

SLOT6 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

SLOT7 PCIe5.0 x16 OPROM

Use this feature to enable or disable PCIe Slot OPROM option. The options are Disabled and **EFI**.

Onboard LAN 1 OPROM

Use this feature to control the execution of UEFI and Legacy Video OpROM. The options include Disabled and **EFI**.

►USB Configuration

USB Configuration

USB Module Version: 33

USB Controllers: 1 XHCI

USB Devices: 1 Drive, 2 Keyboards, 1 Mouse, 4 Hubs

Legacy USB Support

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

XHCI Hand-Off

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

Port 60/64 Emulation

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

► Network Configuration

Network Configuration

Network Stack

This setting allows you to Disable or **Enable** the UEFI Network Stack.

IPv4 PXE Support

This setting allows you to Disable or **Enable** IPv4 PXE boot support. If disabled, IPv4 PXE boot support will not be available.

IPv4 HTTP Support

This setting allows you to **Disable** or Enable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.

IPv6 PXE Support

This setting allows you to Disable or **Enable** IPv6 PXE boot support. If disabled, IPv6 PXE boot support will not be available.

IPv6 HTTP Support

This setting allows you to **Disable** or Enable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support will not be available.

PXE Boot Wait Time

This setting allows you to set in a number field the wait time to press the ESC key to abort the PXE boot. The default value is **0**.

Media Detect Count

This setting allows you set in a number field the number of times presence of media will be checked. The default value is **1**.

▶ HTTP Boot Configuration

HTTP Boot Configuration

HTTP Boot Policy

Sets the HTTP boot policy to Apply to all LANs, **Apply to each LAN**, or Boot Priority #1 instantly.

HTTPS Boot Checks Hostname

Selects whether HTTPS Boot checks the hostname of TLS certificates matches the hostname provided by the remote server. The options include **Enabled** and Disabled (WARNING: Security Risk!!).

Priority of HTTP Boot

Instance of Priority 1: 1

Select IPv4 or IPv6

Choose to set the targeted LAN port to boot from **IPv4** or IPv6.

Boot Description

This setting must be filled out, otherwise the boot option for the URI cannot be created.

Boot URI

This option is an input field used to enter a web or network address to point to the HTTP boot files. This supports the HTTP or HTTPS protocols only.

▶ Supermicro KMS Server Configuration

Supermicro KMS Server IP address

Enter IP4 address in dotted-decimal notation.

Second Supermicro KMS Server IP address

Enter IP4 address in dotted-decimal notation.

Supermicro KMS TCP Port number

Enter Supermicro KMS TCP port number. The default value is **5696**.

KMS Time Out

KMS Server connecting time-out, unit is second, in the range of 5~30 seconds. The default value is **5**.

TimeZone

Enter the correct timezone. The default value is **0**.

Client UserName

Use this setting to enter the client identity. Choose a username 0-63 characters long.

Client Password

Use this setting to enter the client password. Choose a password 0-31 characters long.

KMS TLS Certificate / Size**▶ CA Certificate**

The options include Update, Delete, and Export.

▶ Client Certificate

The options include Update, Delete, and Export.

▶ Client Private Key

The options include Update, Delete, and Export.

▶ Super-Guardians Configuration**Super-Guardians Protection Policy**

The options include **Storage**, System, and System and Storage.

KMS Security Policy

The options include **Disabled** and Enabled.

KMS Server Retry Count

The default value is **5**.

TPM Security Policy

The options include **Disabled** and Enabled.

Load Authentication-Key

The options include **Disabled** and Enabled.

USB Security Policy

The options include **Disabled** and Enabled.

▶ TLS Authenticate Configuration

This submenu allows the user 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.

Certification GUID

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

▶ Delete Certification

Use this feature to delete certification. The options include **Disabled** and Enabled.

▶ RAM Disk Configuration

Disk Memory Type: **Boot Service Data**

The setting specifies type of memory to use from an available memory pool in system to create a disk.

▶ Create raw

Size (Hex): 1

Create & Exit

Discard & Exit

▶ **Create from file**

Create a RAM disk from a given file.

Created RAM disk list:

Remove selected RAM disk(s).

▶ **Driver Health**

The setting provides the health status for the Drivers/controllers.

4.4 BMC

This tab allows you to configure the following IPMI settings for the system.



BMC Firmware Revision

This item indicates the IPMI firmware revision used in your system.

BMC Status

This item indicates the status of the IPMI firmware installed in your system.

▶ System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

This feature allows the user to 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, be sure to reboot the system for the changes to take effect.

► BMC Network Configuration

Update BMC LAN Configuration

Select Yes to enable BMC Network Configuration. The options include **No** and Yes. If set to Yes, the following option becomes available.

Configure IPv4 Support

This section displays static configuration features for IPV4 support.

BMC LAN Selection

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

BMC Network Link Status

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

Configuration Address Source

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

Station IP Address

This item displays the Station IP address for this computer. This should be in decimal and in dotted quad form.

Subnet Mask

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

Gateway IP Address

This item displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.31.0.1).

VLAN

The options include **Disabled** and Enabled.

Configure IPv6 Support

This section displays configuration features for IPv6 support.

IPv6 Address Status: Active**IPv6 Support**

Use this feature to enable or disable LAN1 IPv6 support. The default setting is **Enabled**.

Configuration Address Source

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

Station IPv6 Address

Prefix Length: 64

Configure VLAN Support

Lan Channel: 1

VLAN Support: Unspecified

Current Configuration Address: Disabled

VLAN ID: 1

VLAN Priority: 0

4.5 Event Logs

This tab allows the user to configure the following event logs settings for the system.



► Change Smbios Event Log Settings

This feature allows the user to configure SMBIOS Event settings.

Enabling/Disabling Options

SMBIOS Event Log

Select Enabled to enable SMBIOS (System Management BIOS) Event Logging during system boot. The options are Disabled and **Enabled**.

Erasing Settings

Erase Event Log

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

When Log is Full

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

SMBIOS Event Log Standard Settings**Log System Boot Event**

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

MECI (Multiple Event Count Increment)

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

METW (Multiple Event Count Time Window)

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

Note: Please reboot the system for these changes to take effect.

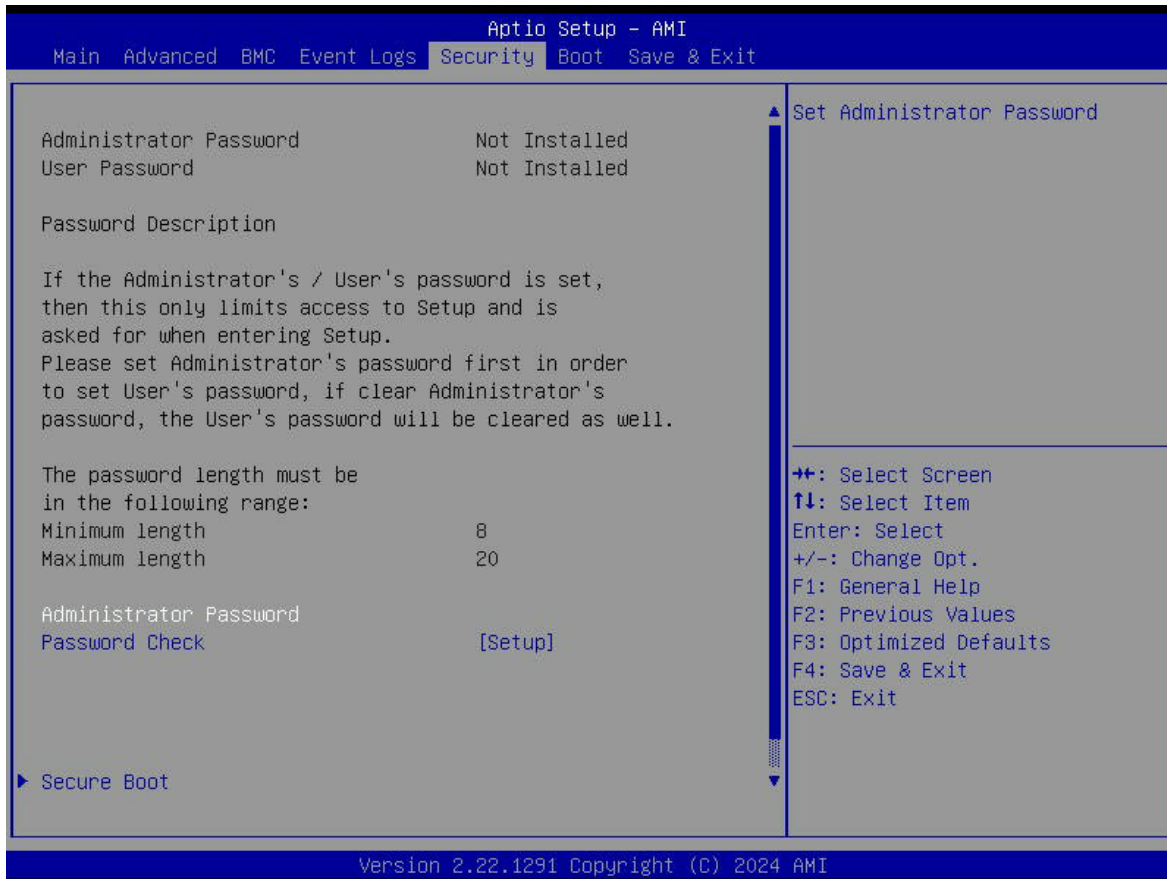
▶View Smbios Event Log

When Event Logging is on, this item allows the user to view the entries in the SMBIOS event log. The following categories are displayed:

Date/Time/Error Code/Severity

4.6 Security

This tab allows you to configure the following security settings for the system.



Administrator Password

Press <Enter> to create a new, or change an existing Administrator password. Note that if the Administrator Password is erased, the User Password will be cleared as well.

Password Check

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

Secure Boot

This option allows you specify when the Platform Key (PK) is enrolled. When enabled, the System Mode is user deployed, and the CSM function is disabled. Options include **Disabled** and **Enabled**.

Secure Boot Mode

Use this item to select the secure boot mode. The options are Standard and **Custom**.

▶ Expert Key Management

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

Vendor Keys/Valid

Provision Factory Defaults

Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode. The default setting is **Disabled**.

▶ Restore Factory Keys

Select and press Yes to restore factory default secure boot keys and key variables. Also, it will reset the system to the User mode. Select Yes to install all default secure keys set by the manufacturer. The options are Yes and No.

▶ Reset To Setup Mode

▶ Enroll Efi Image

This feature is to enroll SHA256 hash of the binary into the Authorized Signature Database (DB) and to allow the image to run in the secure boot mode.

▶ Export Secure Boot Variables

Use this feature to export NVRAM content of secure boot variables to files in a root folder on a file system device.

Secure Boot Variable/Size/Key Numbers/Key Source

▶ Platform Key (PK)

This feature allows the user to enter and configure a set of values to be used as platform firmware keys for the system. The sizes, keys numbers, and key sources of the platform keys will be indicated as well. Select Update to update the platform key. Select Yes to load a factory default PK or No to load from a file on an external media.

► **Key Exchange Keys (KEK)**

This feature allows the user to enter and configure a set of values to be used as Key-Exchange-Keys for the system. The sizes, keys numbers, and key sources of the Key-Exchange-Keys will be indicated as well. Select Update to update your "Key Exchange Keys". Select Append to append your "Key Exchange Keys".

► **Authorized Signatures (db)**

This feature allows the user to enter and configure a set of values to be used as Authorized Signatures for the system. These values also indicate the sizes, keys numbers, and the sources of the authorized signatures. Select Update to update your "Authorized Signatures". Select Append to append your "Authorized Signatures". The settings are Update and Append.

► **Forbidden Signatures (dbx)**

This feature allows the user to enter and configure a set of values to be used as Forbidden Signatures for the system. These values also indicate sizes, keys numbers, and key sources of the forbidden signatures. Select Update to update your "Forbidden. Signatures". Select Append to append your "Forbidden Signatures". The settings are Update and Append.

► **Authorized TimeStamps (dbt)**

This feature allows the user to set and save the timestamps for the authorized signatures which will indicate the time when these signatures are entered into the system. Select Update to update your "Authorized TimeStamps". Select Append to append your "Authorized TimeStamps". The settings are Update and Append.

► **OsRecovery Signature (dbr)**

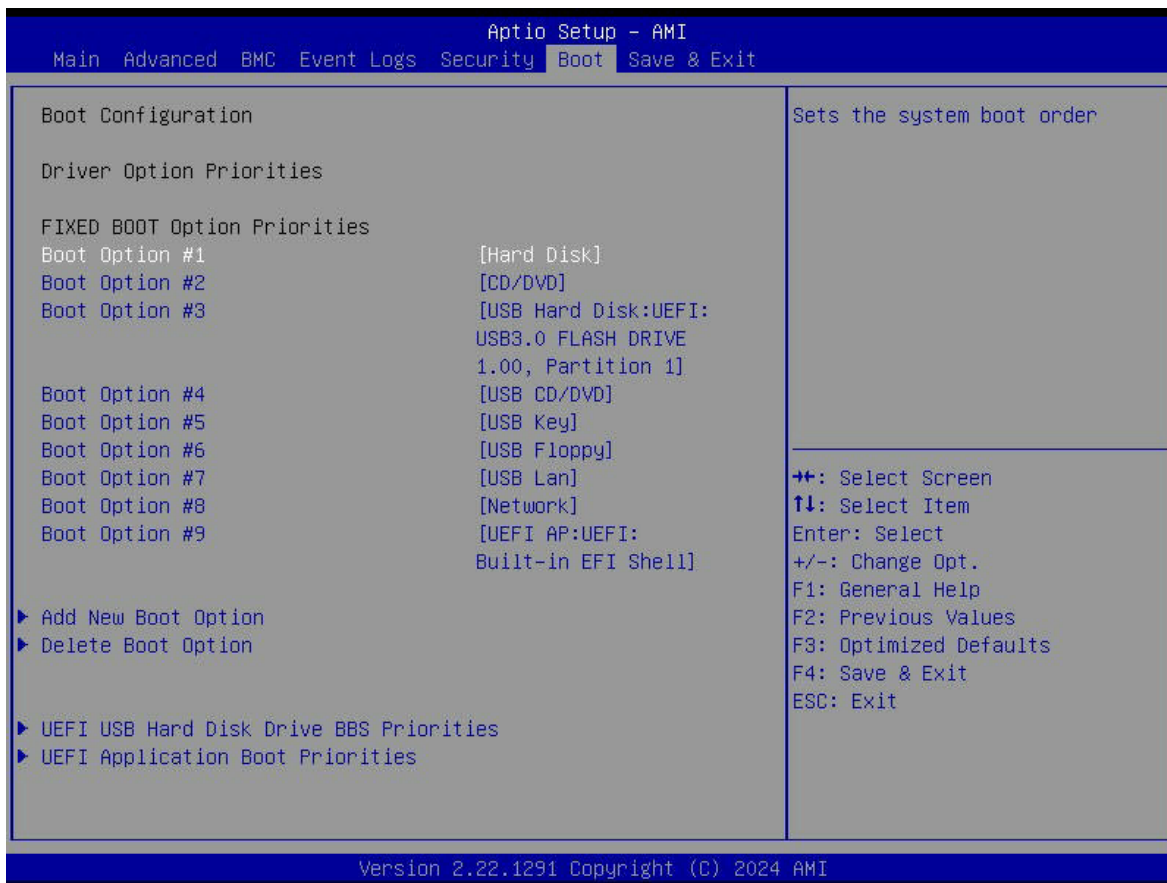
This item uploads and installs an OSRecovery Signature. Use this feature to export NVRAM content of secure boot variables to files in a root folder on a file system device. The settings are Update and Append.

The file formats accepted are:

- 1) Public Key Certificate
 - a. EFI Signature List
 - b. EFI CERT X509 (DER Encoded)
 - c. EFI CERT RSA2048 (bin)
 - d. EFI SERT SHA256 (bin)
- 2) Authenticated UEFI Variable
- 3) EFI PE/COFF Image (SHA256)

4.7 Boot

Use this tab to configure Boot Settings:



Boot Configuration

Driver Option Priorities

Fixed Boot Option Priorities

Boot Option #1 Hard Disk

Boot Option #2 CD/DVD

Boot Option #3 USB Hard Disk: UEFI: USB3.0 FLASH DRIVE 1.00, Partition 1

Boot Option #4 USB CD/DVD

Boot Option #5 USB Key

Boot Option #6 USB Floppy

Boot Option #7 USB Lan

Boot Option #8 Network

Boot Option #9 UEFI AP: UEFI: Built-in EFI Shell

▶ **Add New Boot Option**

Add New Boot Option

Add boot option

Specify name for new boot option.

Path for boot option

Enter the path to the boot option in the format.

Boot option File Path

Create

Creates the newly formed boot option.

▶ **Delete Boot Option**

Use this feature to remove a pre-defined boot device from which the system will boot during startup. The default is **Select one to Delete**.

▶ **UEFI USB Hard Disk Drive BBS Priorities**

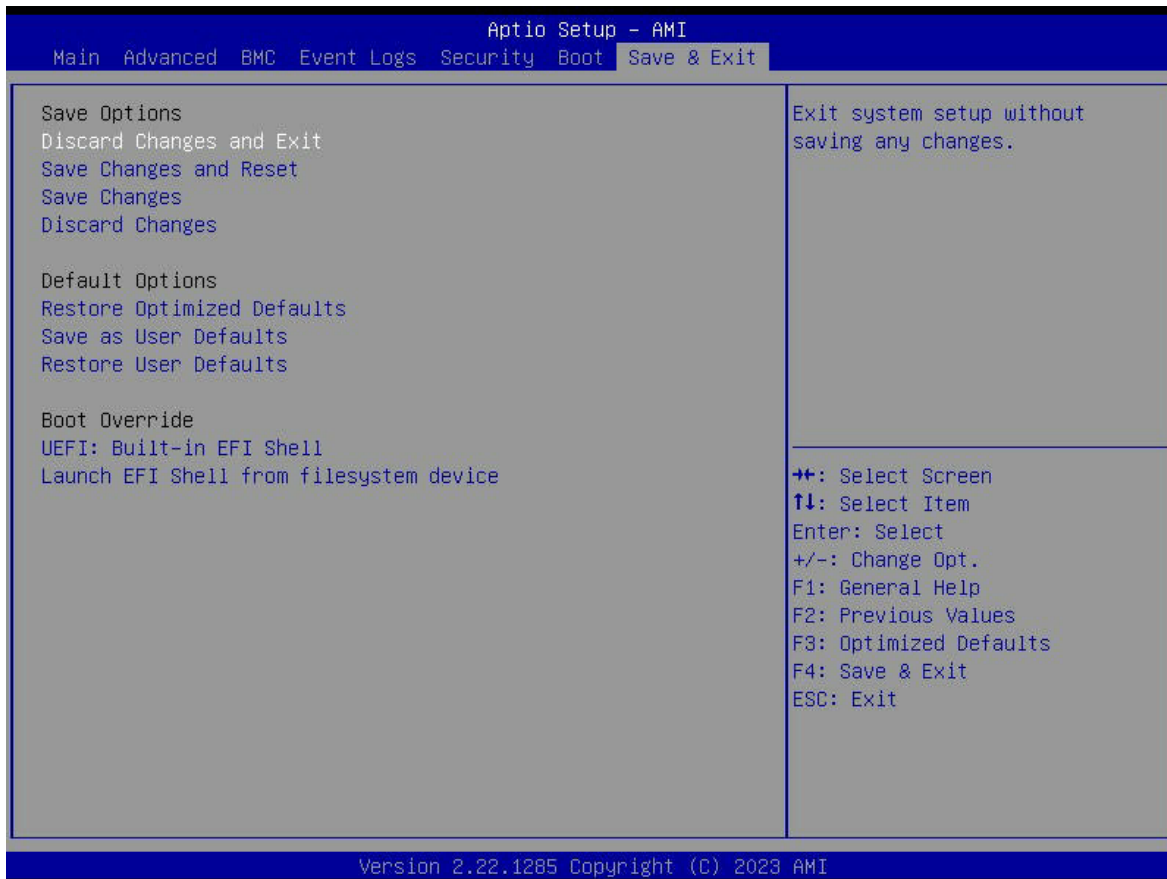
This feature allows users to set the system boot order.

▶ **UEFI Application Boot Priorities**

This feature allows users to specify the Boot Device Priority sequence from available UEFI Application.

4.8 Save & Exit

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



Save Options

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

Select this option to reset the system after saving the changes.

Save Changes

After completing the system configuration changes, select this option to save the changes you have made. This will 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 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 Section

Listed in this section are other boot options for the system (i.e., UEFI: Built-in EFI Shell). Select an option and press <Enter>. Your system will boot to the selected boot option.

Launch EFI Shell from filesystem device

Attempts to launch EFI Shell application (Shell.efi) from one of the available filesystem devices.

Appendix A

Software

After the hardware has been installed, you can boot the Operating System (OS). In addition, the following software is supported on the H13QSH.

A.1 Ubuntu® Server 22.04 ISO Installation

Prerequisites

Ubuntu Server 22.04 ISO Image

Obtaining the Ubuntu Server 22.04 ISO for AMD64 CPU architecture (amd64) and save it to your local drive or a shared server. It's recommended to use Ubuntu Server 22.04.4 LTS.

BMC Network Connection

To utilize the BMC remote functionality, ensure that the network is connected to the BMC.

Ethernet Network Connection via a Network Card

During the Ubuntu 22.04 installation process, network configuration is essential to test the connection to mirror locations for Ubuntu repositories and archives. Please ensure Ethernet connectivity by using a network card. If there's a firewall configuration within your network, the mirror location test may fail. In such cases, disconnect the Ethernet cable for the OS installation. The OS installation can still be successful without an Ethernet connection **for** obtaining the latest updates. For further details, please refer to [Step 6. Installing Ubuntu 22.04 OS](#).

Installing Ubuntu Server 22.04 OS

Step 1. Obtaining the BMC IP Address

Connect the system to a monitor or display using a VGA port or a DisplayPort (Mini DP). Ensure that network is connected to BMC using a network cable and power on the system. The BMC IP address will appear on the right corner of the Supermicro Logo screen.

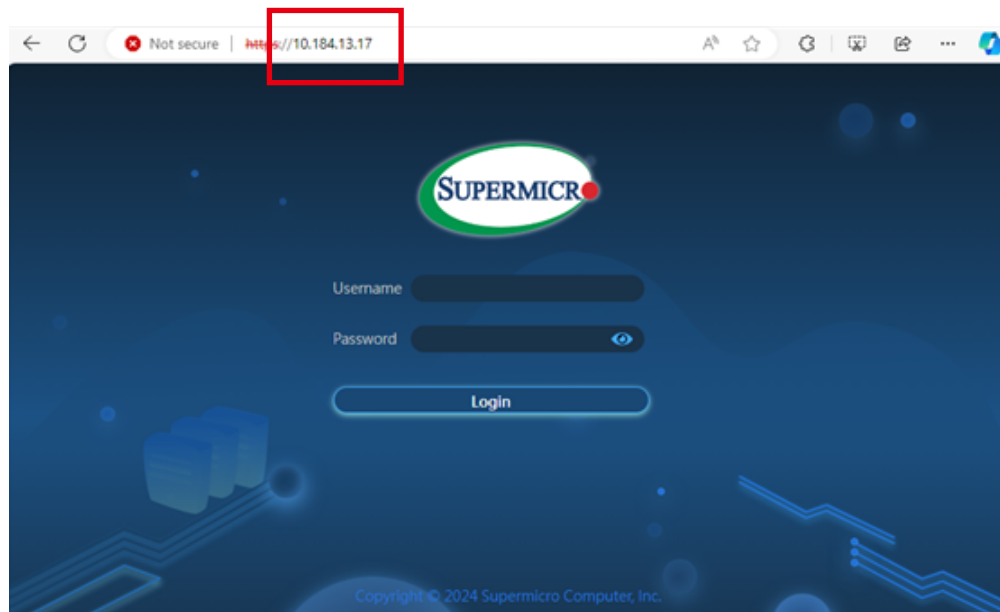


Step 2. Accessing the BMC Remote Server

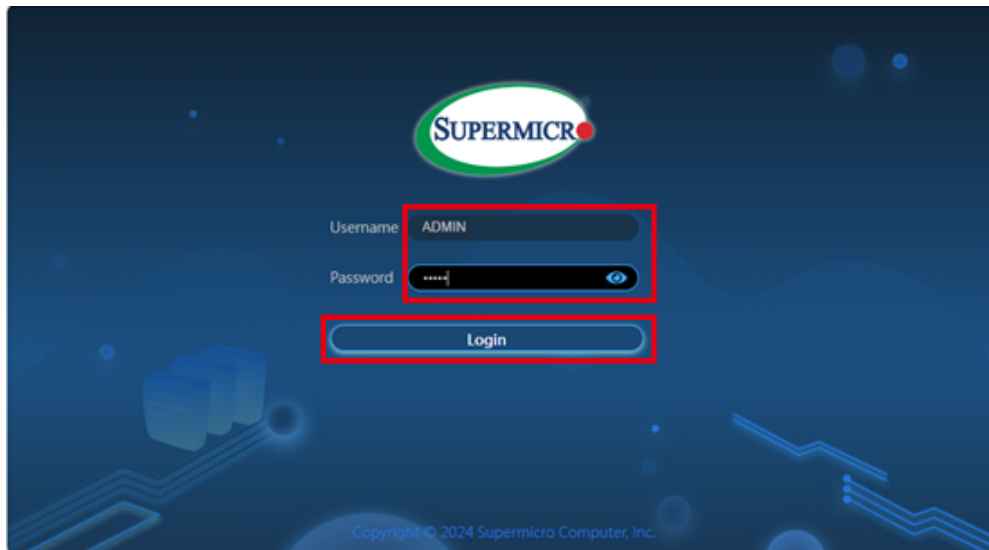
Log in to BMC Remote Server

1. In the terminal, execute a ping command to the BMC IP address, such as 10.184.13.17, to verify its connectivity.
2. Launch a new web browser and input the BMC IP address into the URL field.

Outcome: The BMC Remote Console login screen will be displayed.



3. Input the username "**ADMIN**" and the unique BMC password, which is located on the label on the opposite side of the service tag of the system. Click the "**Login**" to proceed.



Outcome: The BMC Dashboard offers insights into system overview, configuration, health status, and maintenance.

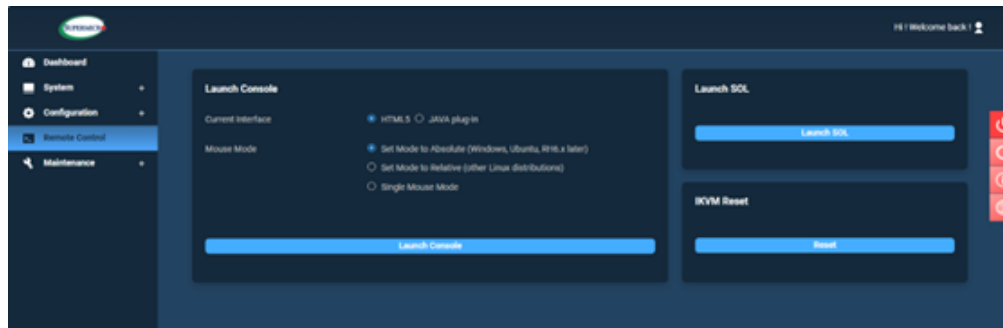


Step 3. Controlling the System Remotely

1. The Remote Control menu in the RMC Remote Server enables remote server operations.

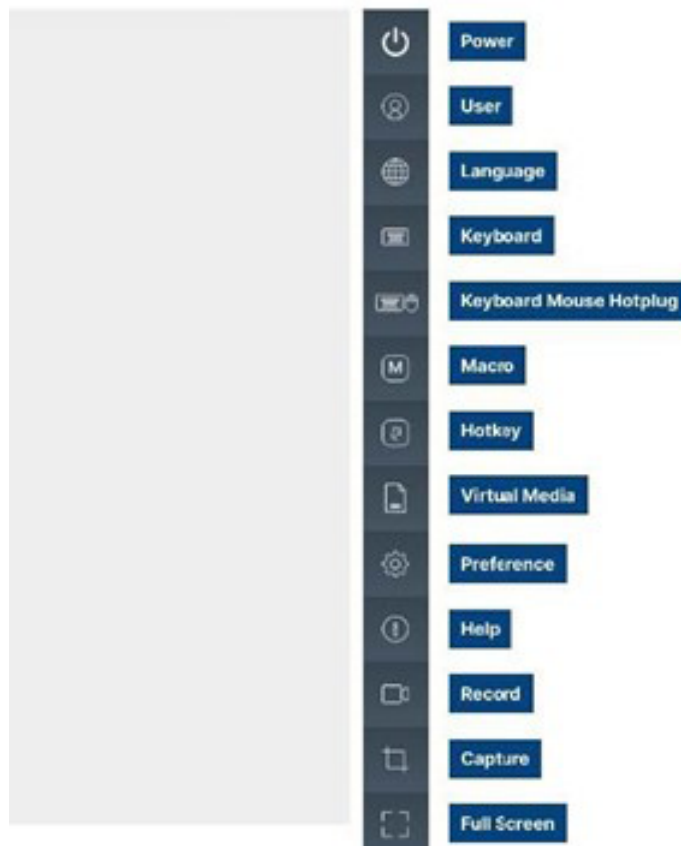
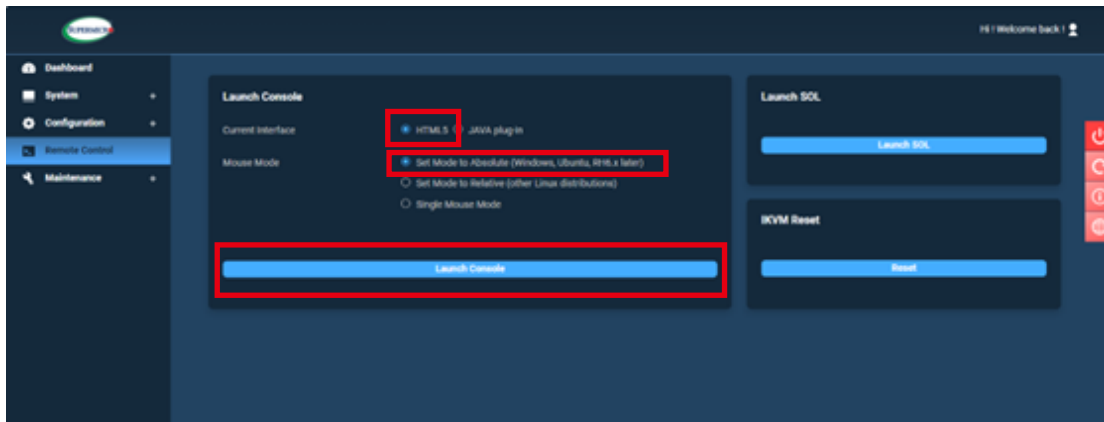


2. Use the Launch Console section to configure the remote console interface settings. Choose between the HTML5 interface or a JAVA plug-in.



Launch a HTML5 Remote Browser

1. Set HTML5 as the current interface.
2. Choose the mouse mode according to your operating system, such as **"Set Mode to Absolute (Windows, Ubuntu, RH6.x, or later)"**.
3. Click the **"Launch Console"** button to open a console in a new browser window.

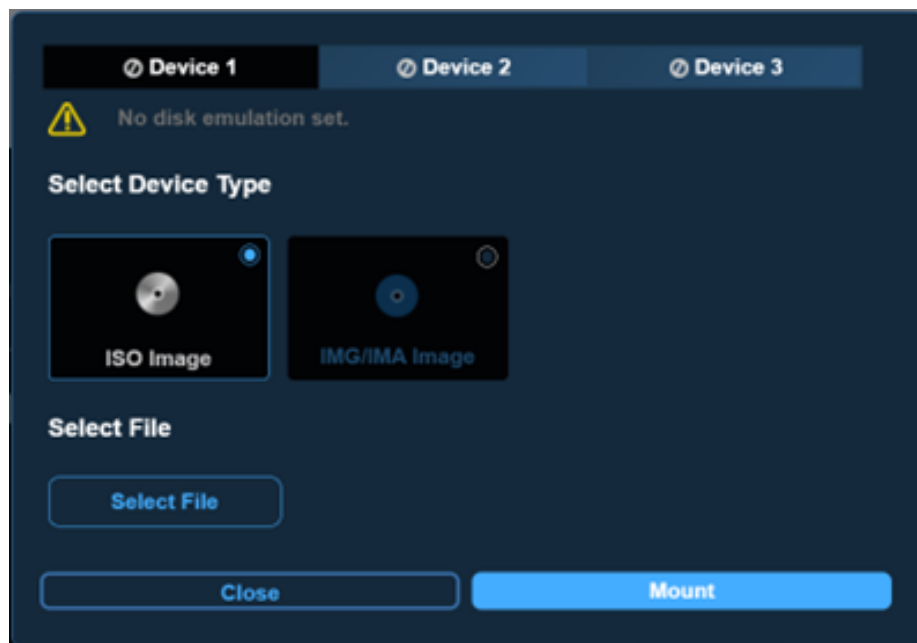
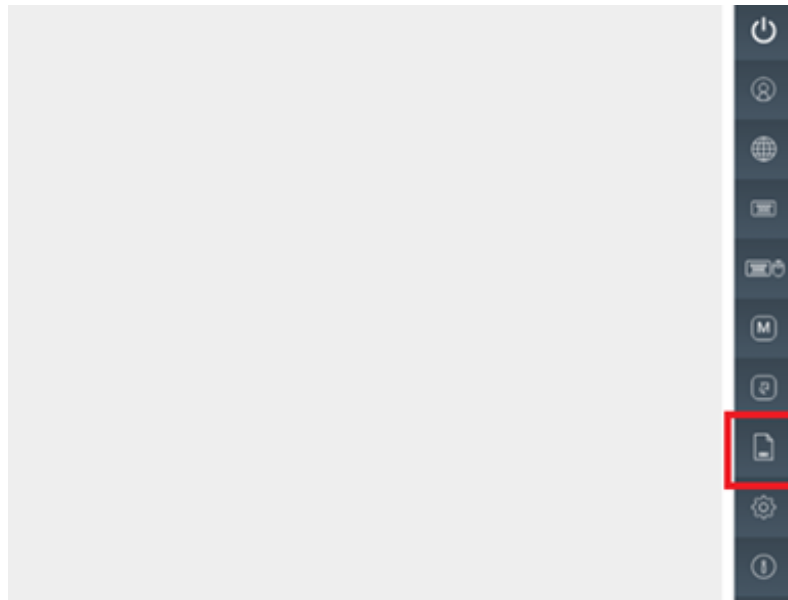


Step 4. Mounting the ISO Image

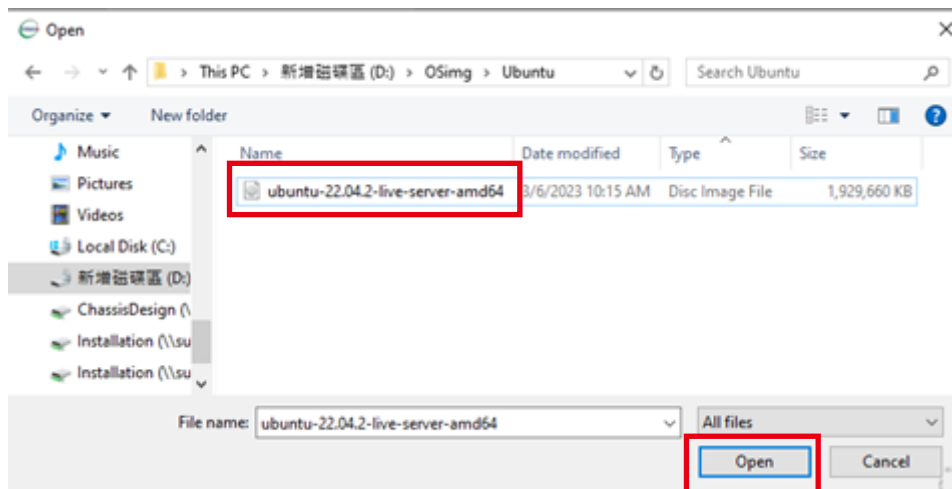
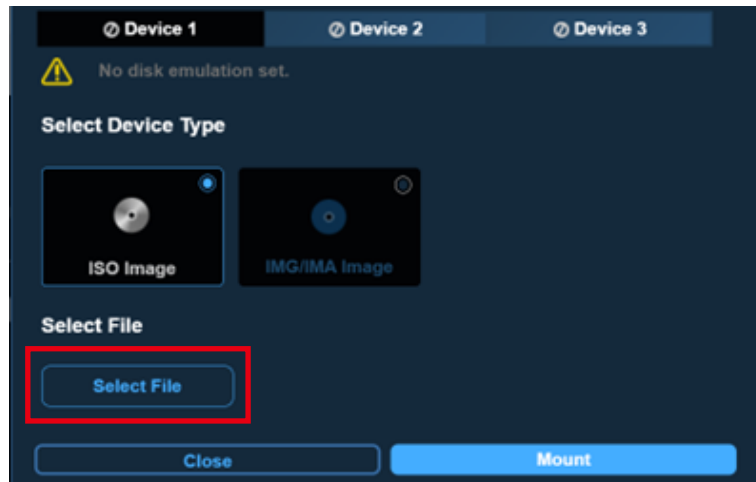
There are two methods to mount ISO images. If the ISO files are stored locally on your drive, you can mount them directly within the remote control browser. Alternatively, if the ISO files are located on a shared server, you can mount them via the Configuration > Virtual Media menu.

Method One: Mount the ISO Image Using a Local File

1. In the remote control browser, click the "**Virtual Media**" icon. This action will prompt a dialog box to appear, enabling you to select the image type and files for mounting.



2. Select the "**Choose File**" button to browse and select the RHEL ISO image on your local drive for use.



3. Click the "**Mount**" button to attach the chosen iso image.

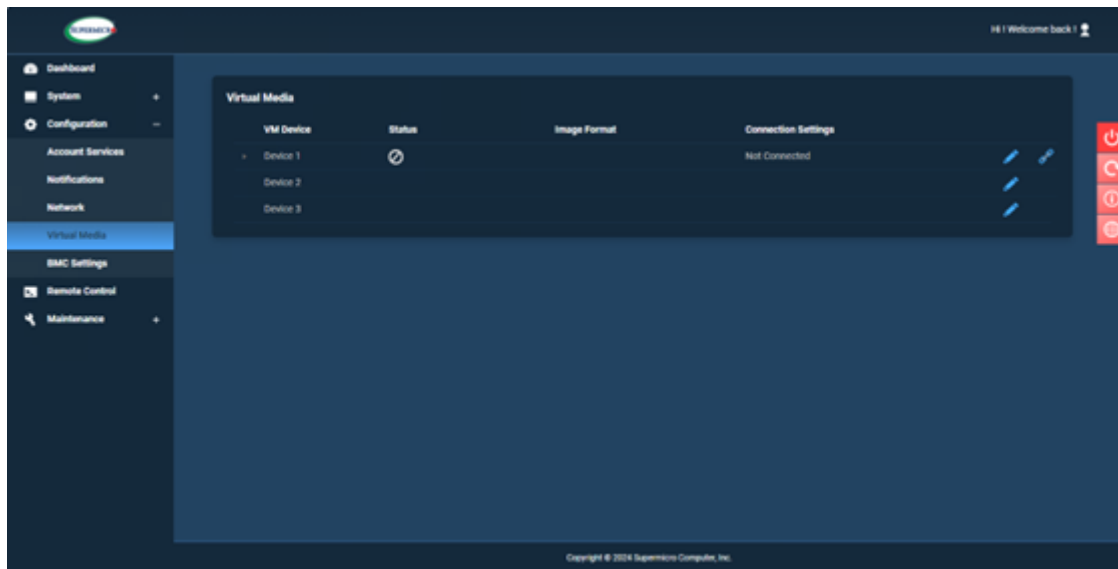


Result: Upon successful mounting of the ISO image, a green indicator will appear in the "Device" tab. Close the dialog to continue.

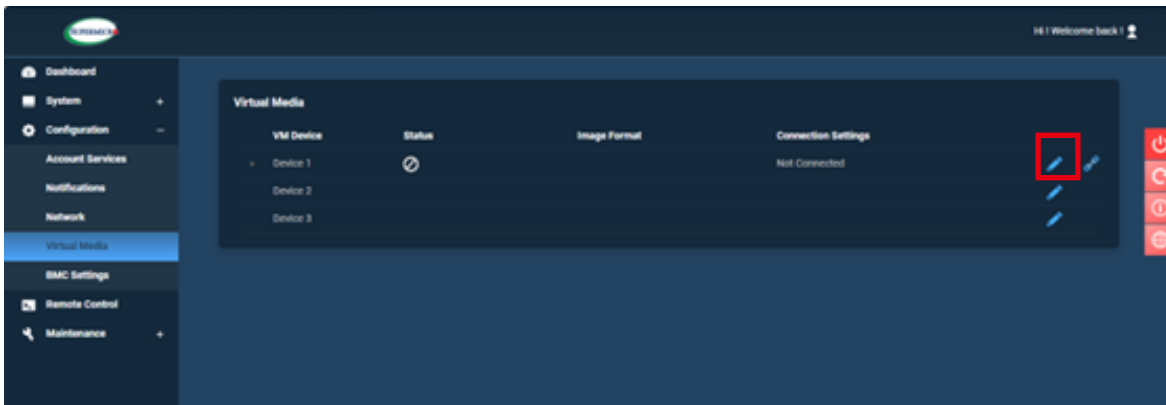


Method Two: Mount the ISO Image through Shared Server

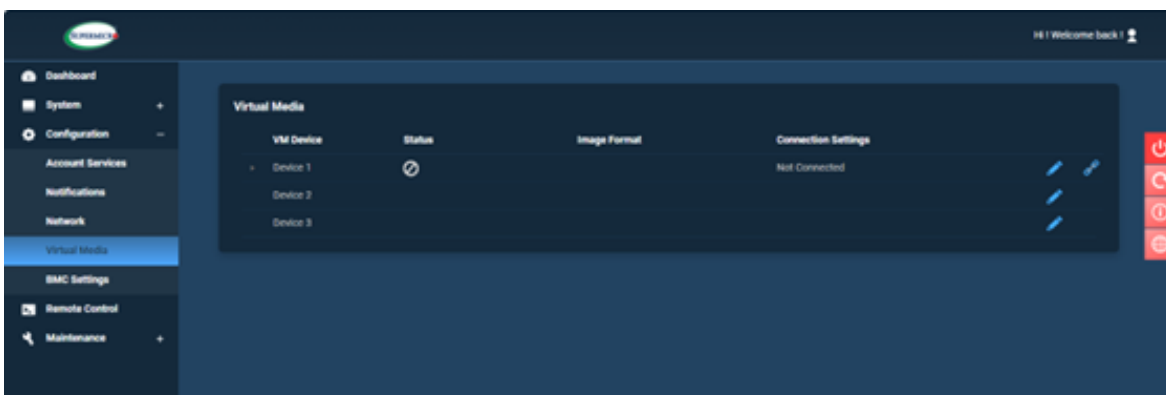
1. On the BMC dashboard, go to Configuration > Virtual Media, this allows you to attach an iso image from the server.

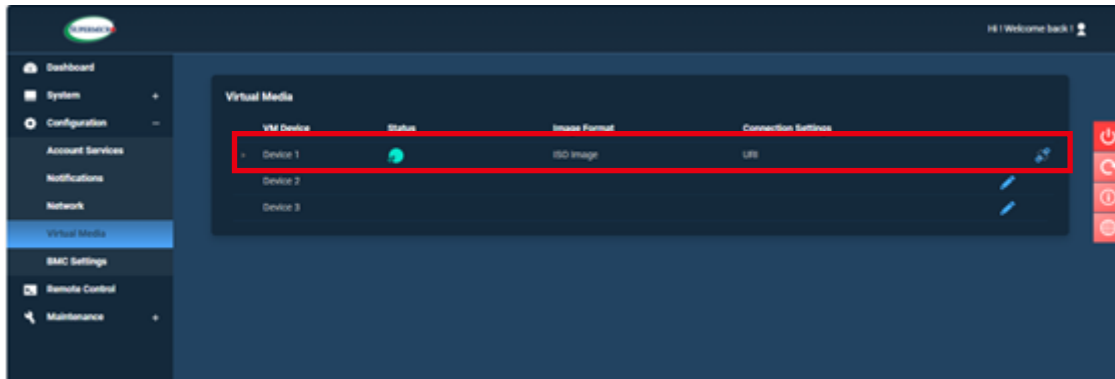


- Click the **"Edit"** icon to adjust the VM configuration. Enter the server host address and the path to the ISO image. Then, click the **"Save"** to apply the changes.



- Click the **"Connect"** icon to mount the virtual media. The device status will display as green once the VM is successfully configured.





Step 5. Boot from Virtual Media

To boot from the mounted image in virtual media, users must manually select the boot device from the Boot Menu during BIOS POST.

1. Power on the system and wait for the Log screen to display. To access the Boot Menu, repeatedly press <F11> until "Invoke Boot Menu" appears at the bottom left corner of the screen.



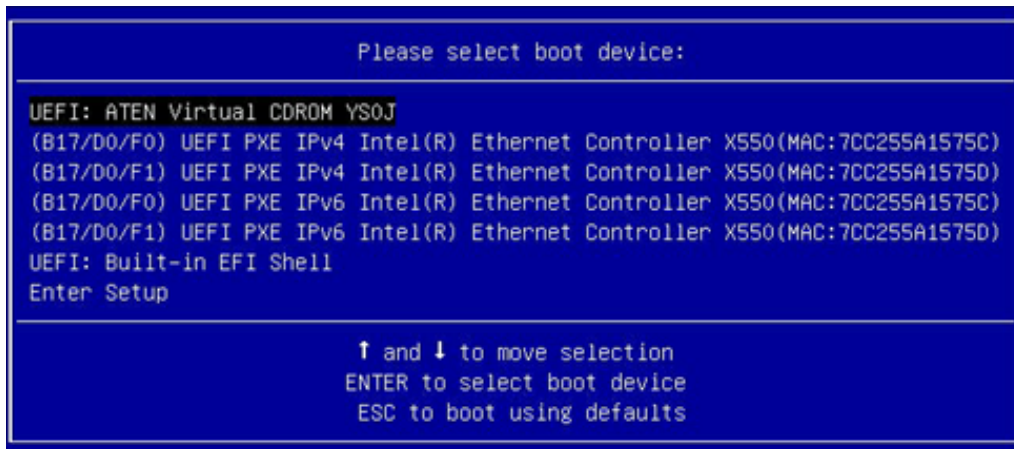
www.supermicro.com

Press <TRF> to display BIOS POST Message Press to run Setup
Press <F11> to invoke boot menu Press <F12> to boot from PXE/LAN

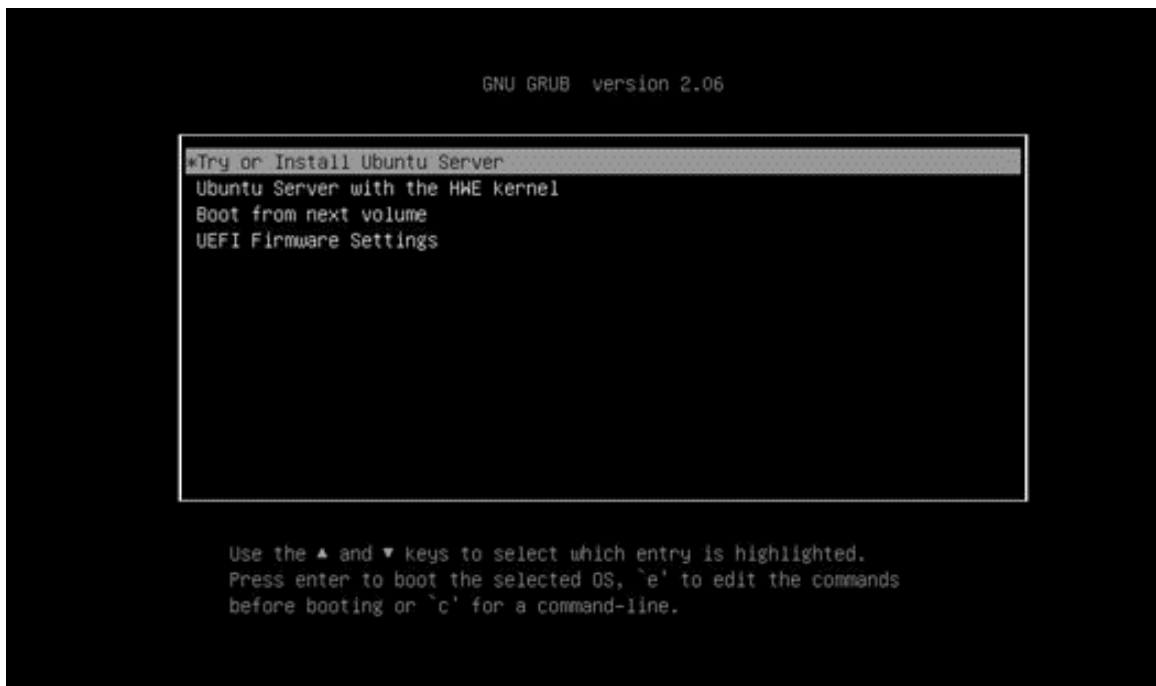
Invoking Boot Menu

96

Subsequently, the Boot Menu is displayed.

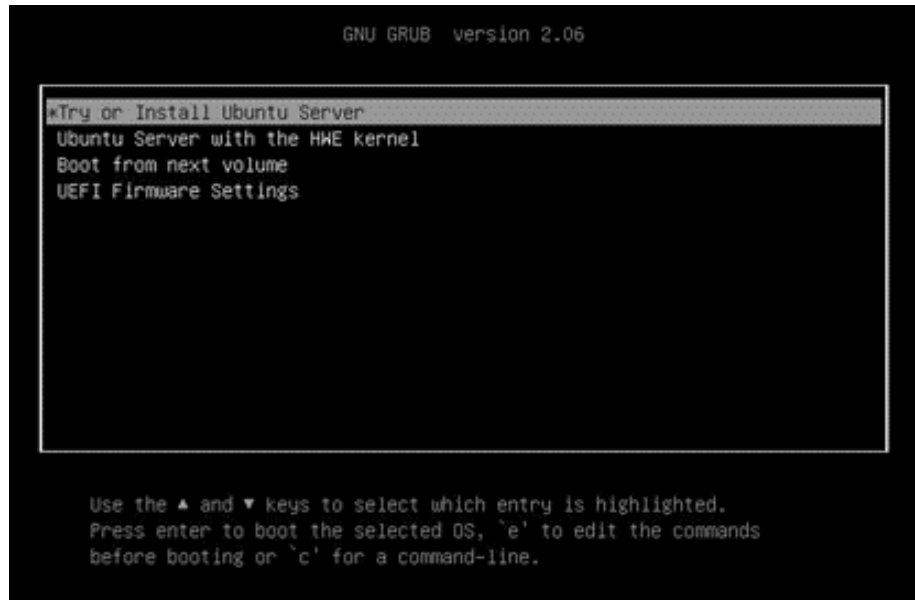


2. Select "**UEFI: ATEN Virtual CDROM YSOJ**" as the boot menu. This selection mounts the ISO image mounted in Virtual Media. Press "Enter" to proceed. The GRUB menu will be displayed.

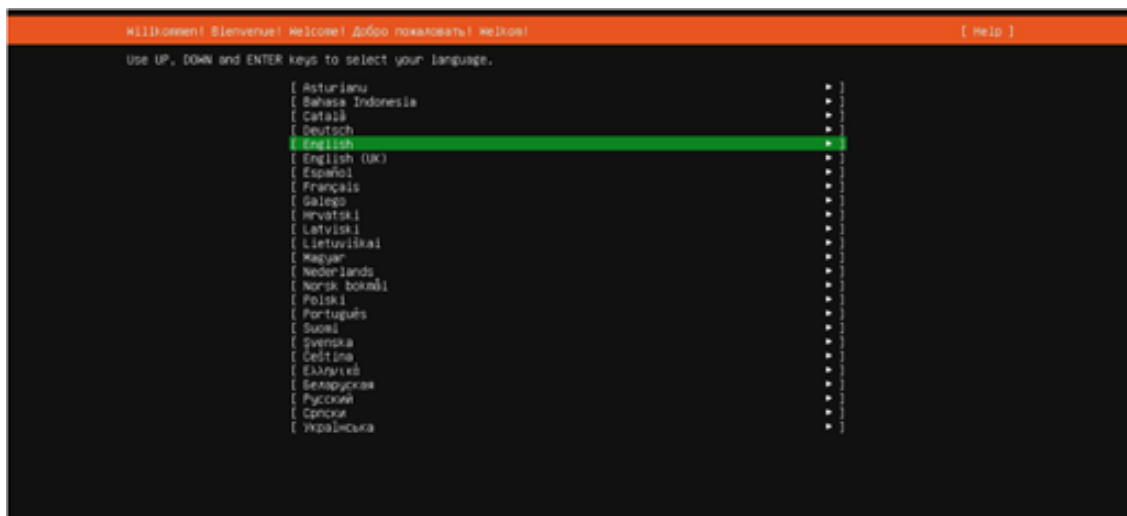


Step 6. Installing Ubuntu Server 22.04 OS

1. Follow the Ubuntu installer steps to continue installation. Choose **"Try or Install Ubuntu Server"** to proceed.

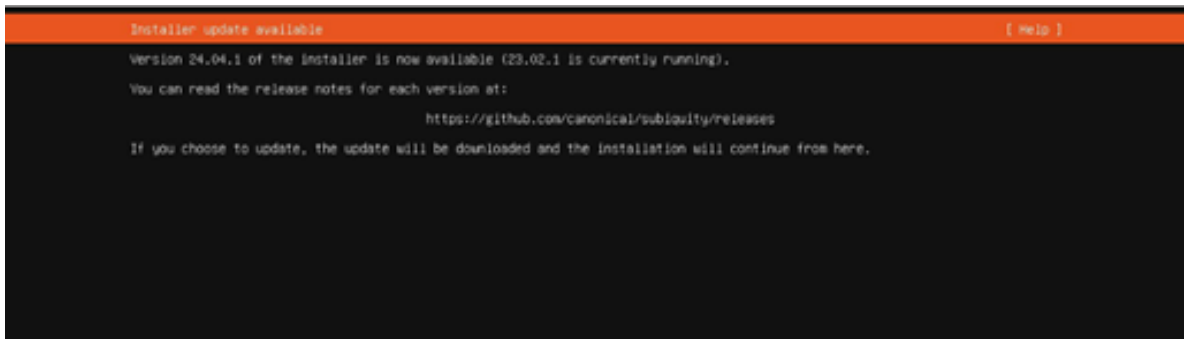


2. Select the language.

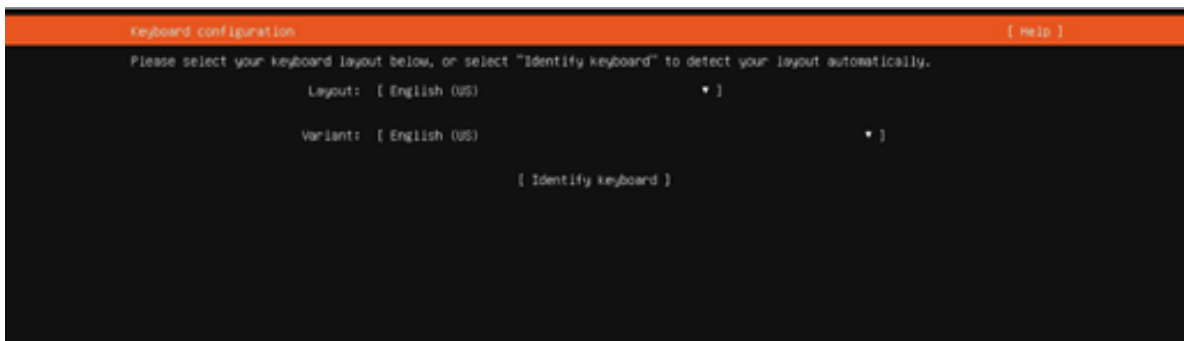


3. Determine whether to update to the new installer or not.

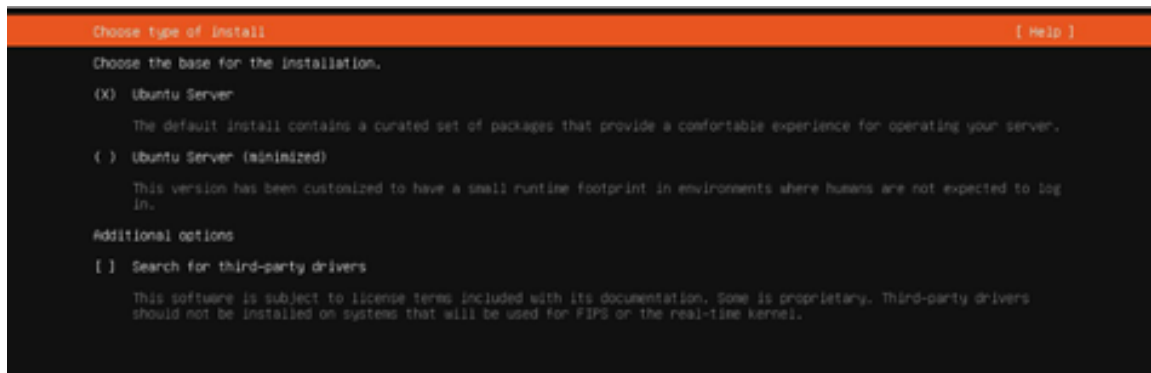
Note: Check whether the system supports the new version before installation.



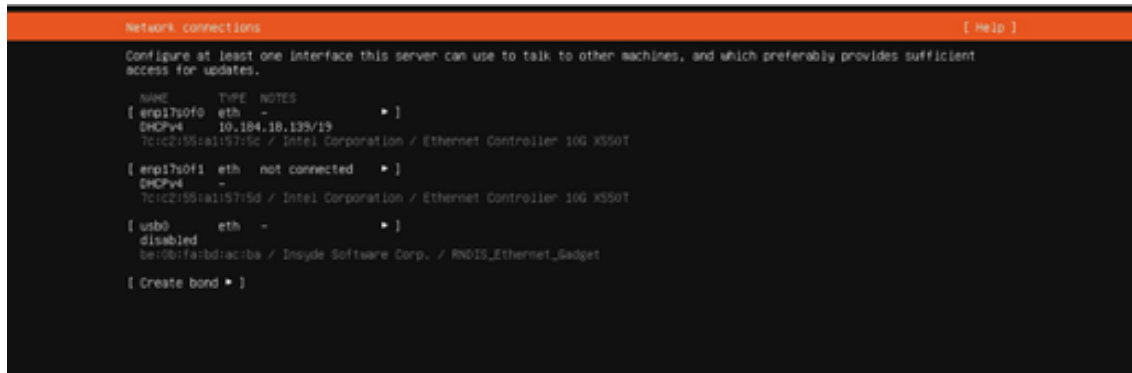
4. Select the keyboard layout.



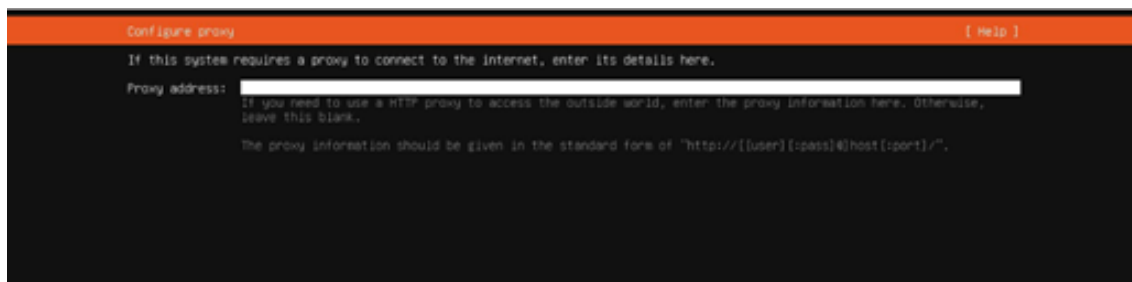
5. Select the installation type.



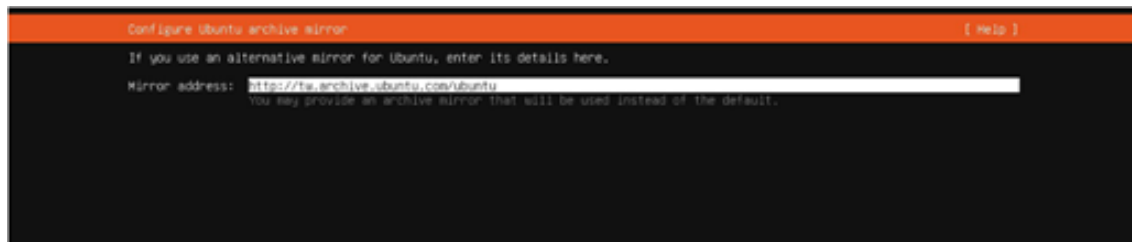
6. Configure the network connection to proceed. If an Ethernet network connection is available, proceed by selecting at least one network configuration option displayed on the installation UI.



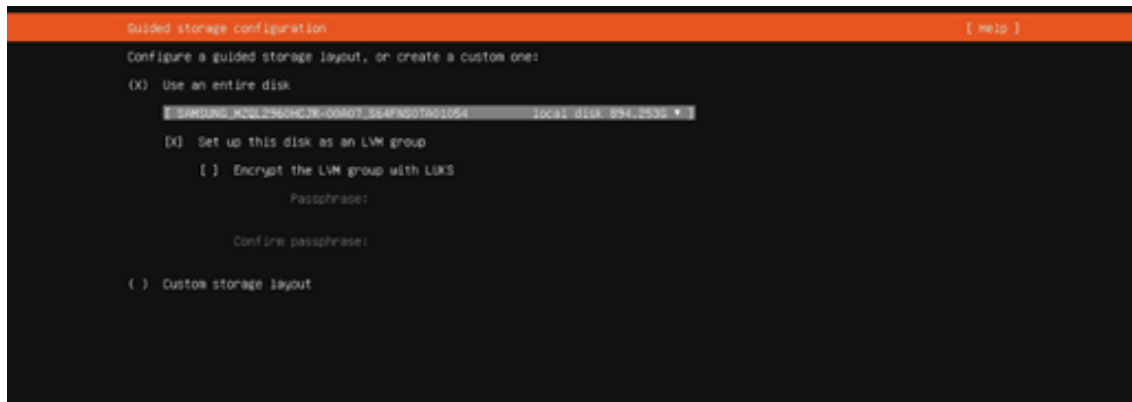
7. Configure a proxy server or not.



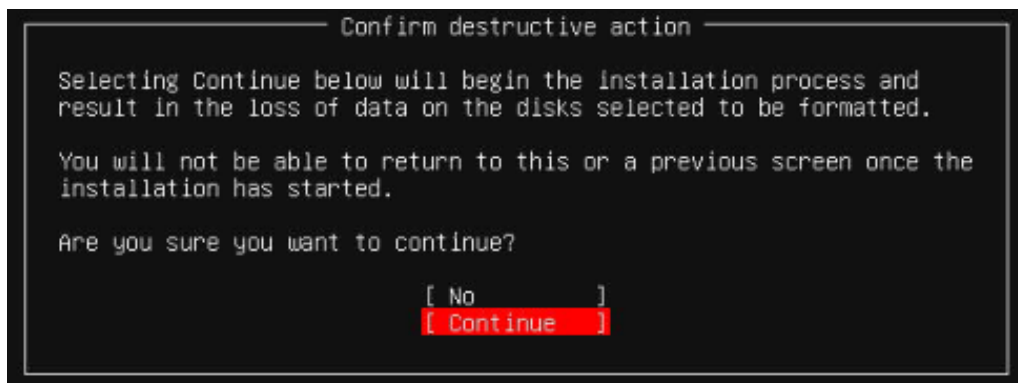
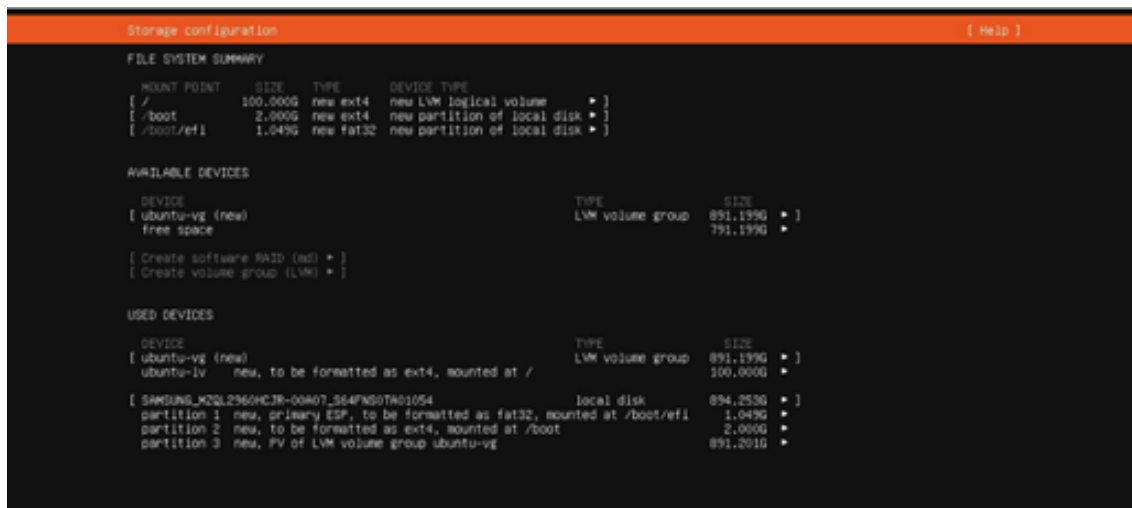
8. Configure an Ubuntu archive mirror.



9. Select a drive for OS deployment and customize the storage layout or not.



10. Confirm the storage layout and accept the irreversible change.



11. Enter the username and password.

```
Profile setup [ help ]
(Enter the username and password you will use to log in to the system. You can configure SSH access on the next screen but a password is still needed for sudo.)
Your name: joe
Your server's name: joe
Pick a username: joe
Choose a password: *****
Confirm your password: *****
```

12. Determine to upgrade to Ubuntu Pro or not.

```
Upgrade to Ubuntu Pro [ help ]
Upgrade this machine to Ubuntu Pro for security updates on a much wider range of packages, until 2032. Assists with FedRAMP, FIPS, STIG, HIPAA and other compliance or hardening requirements.
[ About Ubuntu Pro > ]
( ) Enable Ubuntu Pro
(X) Skip for now
You can always enable Ubuntu Pro later via the "pro attach" command.
```

13. Determine to install OpenSSH server or not.

```
SSH Setup [ help ]
You can choose to install the OpenSSH server package to enable secure remote access to your server.
[ ] Install OpenSSH server
Import SSH identity: [ No ▼ ]
You can import your SSH keys from GitHub or Launchpad.
Import Username:
(X) Allow password authentication over SSH
```

14. Choose the software packages on demand.

```

Featured Server Snaps [ Help ]
-----
These are popular snaps in server environments. Select or deselect with SPACE, press ENTER to see more details of the package,
publisher and versions available.

[ ] microk8s          canonical/      Kubernetes for workstations and appliances
[ ] nextcloud         nextcloud/    Nextcloud Server - A safe home for all your data
[ ] kubernetes        kubernetes/   Open-Source k8s
[ ] kata-containers   katacontainers/ Build lightweight VMs that seamlessly plug into the containers ecosystem
[ ] docker            canonical/    Docker container runtime
[ ] canonical-livepatch canonical/     Canonical Livepatch Client
[ ] rocketchat-server rocketchat/   Rocket.Chat server
[ ] mosquitto         mosquitto/   Eclipse Mosquitto MQTT broker
[ ] etcd              canonical/    Resilient key-value store by CoreOS
[ ] powershell       microsoft-powershell/ PowerShell for every system!
[ ] sdnzb             safire/      SDNzb
[ ] wormhole          snoochrafters/ get things from one computer to another, safely
[ ] aws-cli           aws/         Universal Command Line Interface for Amazon Web Services
[ ] google-cloud-sdk  google-cloud-sdk/ Google Cloud SDK
[ ] scli              softlayer/   Python based SoftLayer API Tool.
[ ] doctl             digitalocean/ The official DigitalOcean command line interface
[ ] conjure-up        canonical/    Package runtime for conjure-up spells
[ ] postgresql        cd/          PostgreSQL is a powerful, open source object-relational database system.
[ ] heroku            heroku/      CLI client for Heroku
[ ] keepalived        keepalived-project/ High availability VRRP/SRD and load-balancing for Linux
[ ] prometheus        canonical/    The Prometheus monitoring system and time series database

```

15. Installation begin and wait for the completion.

```

Installing system [ Help ]
-----
subiquity/early/apply_autoinstall_config
subiquity/reporting/apply_autoinstall_config
subiquity/error/apply_autoinstall_config
subiquity/userdata/apply_autoinstall_config
subiquity/packages/apply_autoinstall_config
subiquity/obconf/apply_autoinstall_config
subiquity/kernel/apply_autoinstall_config
subiquity/udev/apply_autoinstall_config
subiquity/late/apply_autoinstall_config
configuring apt
  curtin command in-target
installing system
  executing curtin install initial step
  executing curtin install partitioning step
  curtin command install
    configuring storage
      running 'curtin block-meta simple'
      curtin command block-meta
      removing previous storage devices
      configuring disk: disk-nvme01
      configuring partition: partition-0
      configuring format: format-0
      configuring partition: partition-1
      configuring format: format-1
      configuring partition: partition-2
      configuring lvm_volgroup: lvm_volgroup-0
      configuring lvm_partition: lvm_partition-0
      configuring format: format-2
      configuring mount: mount-2
      configuring mount: mount-1
      configuring mount: mount-0
  executing curtin install extract step
  curtin command install
    writing install sources to disk
    running 'curtin extract'
    curtin command extract
      acquiring and extracting image from cpi:///tsp/tsp0eb2c7vs/mount
  executing curtin install curthooks step
  curtin command install
    configuring installed system
    running 'mount --bind /cdrom /target/cdrom'
    running 'curtin in-target -- setupcon --save-only'
    curtin command in-target
    running 'curtin curthooks'
    curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      installing packages on target system: ['efibootmgr', 'grub-efi-aa64', 'grub-efi-aa64-signed', 'shim-signed']
      configuring iscsi service
      configuring raid (mdadm) service
      installing kernel |

```

[View full log]

16. Reboot the system to complete the installation.

```

Install complete! [ help ]

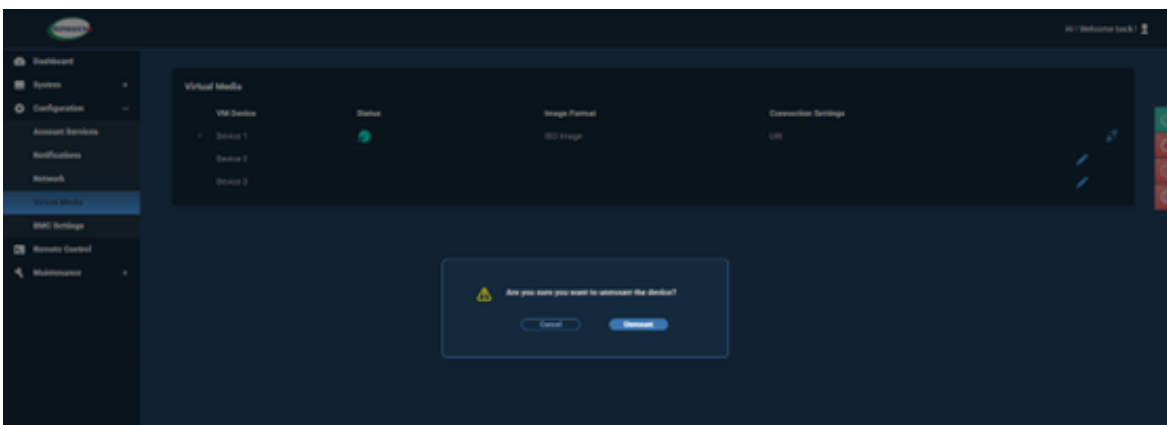
configuring storage
  running 'curtin block-meta simple'
  curtin command block-meta
    removing previous storage devices
    configuring disk: disk-rwecmd1
    configuring partition: partition-0
    configuring format: format-0
    configuring partition: partition-1
    configuring format: format-1
    configuring partition: partition-2
    configuring lvm_voigroup: lvm_voigroup-0
    configuring lvm_partition: lvm_partition-0
    configuring format: format-2
    configuring mount: mount-2
    configuring mount: mount-1
    configuring mount: mount-0
  executing curtin install extract step
  curtin command install
    writing install sources to disk
    running 'curtin extract'
    curtin command extract
      acquiring and extracting image from csi:///trp/taptebl2hvs/mount
  executing curtin install curthooks step
  curtin command install
    configuring installed system
    running 'mount --bind /cdrom /target/cdrom'
    running 'curtin in-target -- setupcon --save-only'
    curtin command in-target
    running 'curtin curthooks'
    curtin command curthooks
      configuring apt configuring apt
      installing missing packages
      installing packages on target system: ['efibootmgr', 'grub-efi-amd64', 'grub-efi-amd64-signed', 'shim-signed']
      configuring iscsi service
      configuring raid (mdadm) service
      installing kernel
      setting up swap
      apply networking config
      writing etc/fstab
      configuring multipath
      updating packages on target system
      configuring pollinate user-agent on target
      updating initramfs configuration
      configuring target system bootloader
      installing grub to target devices
  final system configuration
  configuring cloud-init
  calculating extra packages to install
  installing openssh-server
  curtin command system-install
  downloading and installing security updates
  curtin command in-target
  restoring apt configuration
  curtin command in-target
  subiquity/late/run
  
```

[View full log]
[Reboot Now]

17. Remove the installation medium and press "ENTER" to continue the OS initialization.

```

[FAIL] Failed unmounting /cdrom.
Please remove the installation medium, then press ENTER:
_
  
```



18. Boot into OS successfully

```
ubuntu 22.04.2 LTS sncl tty1
sncl login: _
```

19. Login with the username and password and start to operate the system as demand.

```
ubuntu 22.04.2 LTS sncl tty1
sncl login: sncl
Password:
```

```
ubuntu 22.04.2 LTS sncl tty1
sncl login: sncl
Password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-119-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage
```

```
System information as of Tue Sep 10 11:05:08 UTC 2024

System load:          1.34033203125
Usage of /:           11.7% of 97.87GB
Memory usage:         0%
Swap usage:           0%
Processes:            1039
Users logged in:      0
IPv4 address for docker0: 172.17.0.1
IPv4 address for enp17s0f0: 10.184.18.139
IPv6 address for enp17s0f0: 2001:db8::7ec2:55ff:feaf:575c
```

```
 * Introducing Expanded Security Maintenance for Applications.
   Receive updates to over 25,000 software packages with your
   Ubuntu Pro subscription. Free for personal use.
```

```
https://ubuntu.com/pro
```

```
Expanded Security Maintenance for Applications is not enabled.
```

```
0 updates can be applied immediately.
```

```
Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status
```

```
The list of available updates is more than a week old.
To check for new updates run: sudo apt update
New release '24.04.1 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
```

```
Last login: Tue Sep 10 11:05:09 UTC 2024 on tty1
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

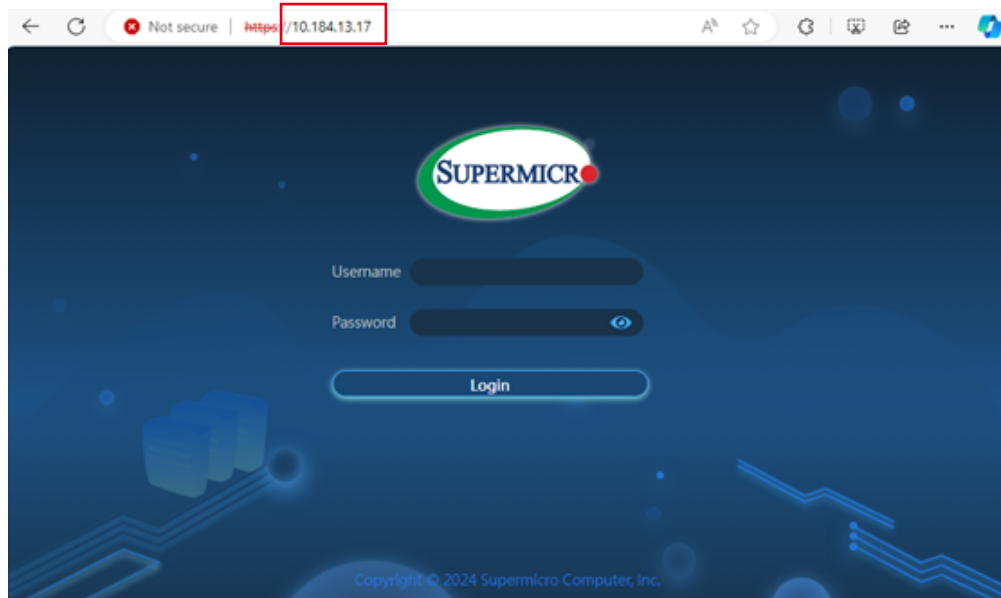
```
sncl@sncl:~$ _
```


Step 2. Accessing the BMC Remote Server

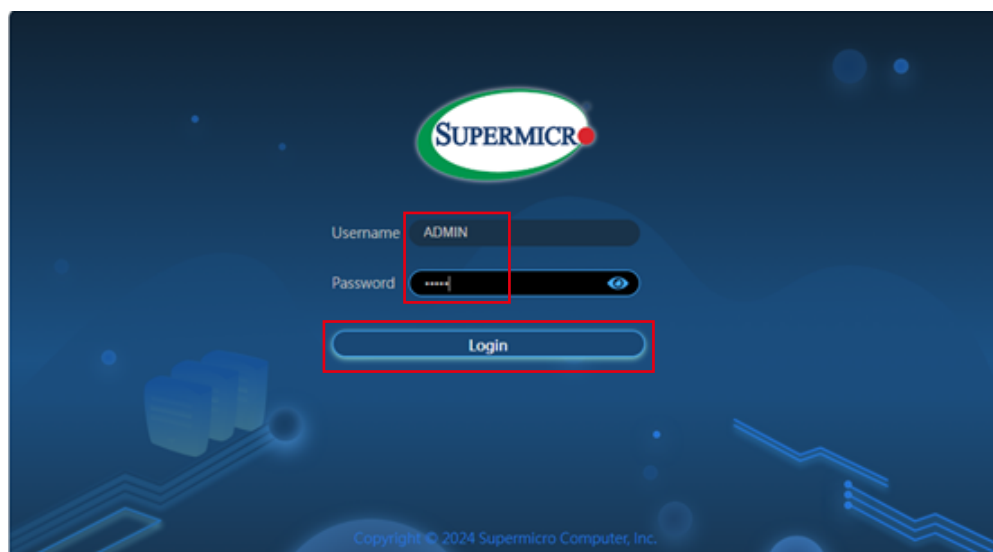
Log in to the BMC Remote Server

1. In the terminal, execute a ping command to the BMC IP address, such as 10.184.13.17, to verify its connectivity.
2. Launch a new web browser and input the BMC IP address into the URL field.

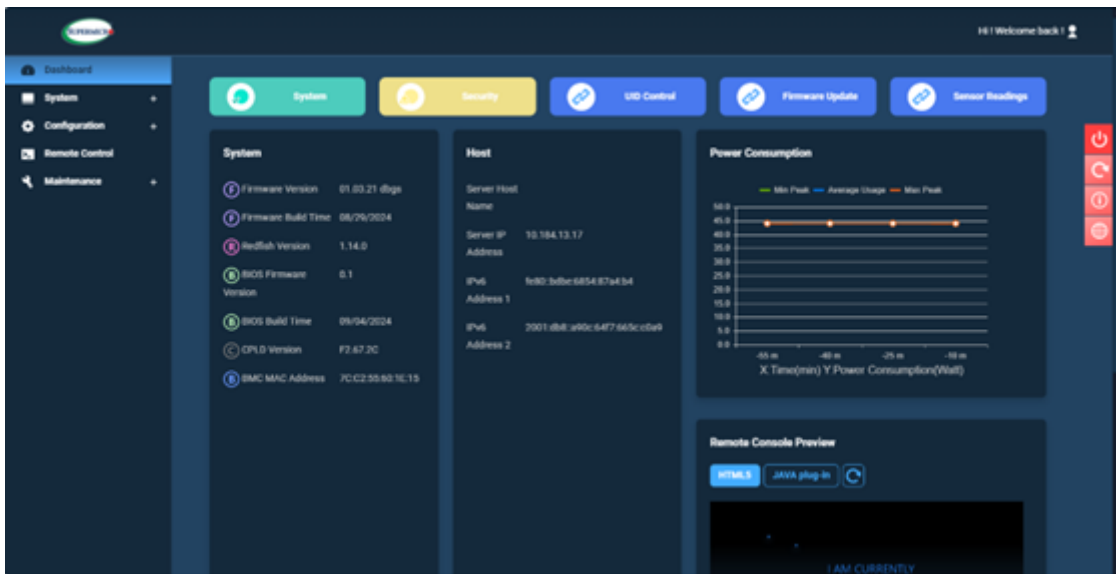
Outcome: The BMC Remote Console login screen will be displayed.



3. Input the username "**ADMIN**" and the unique BMC password, which is located on the label on the opposite side of the service tag of the system. Click the "**Login**" to proceed.

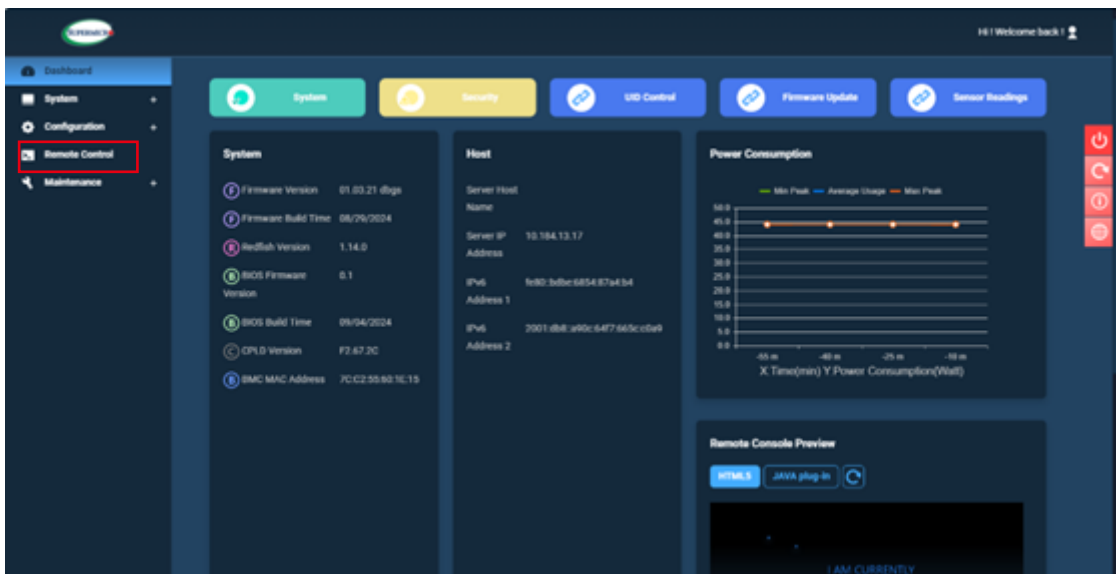


Outcome: The BMC Dashboard offers insights into system overview, configuration, health status, and maintenance.

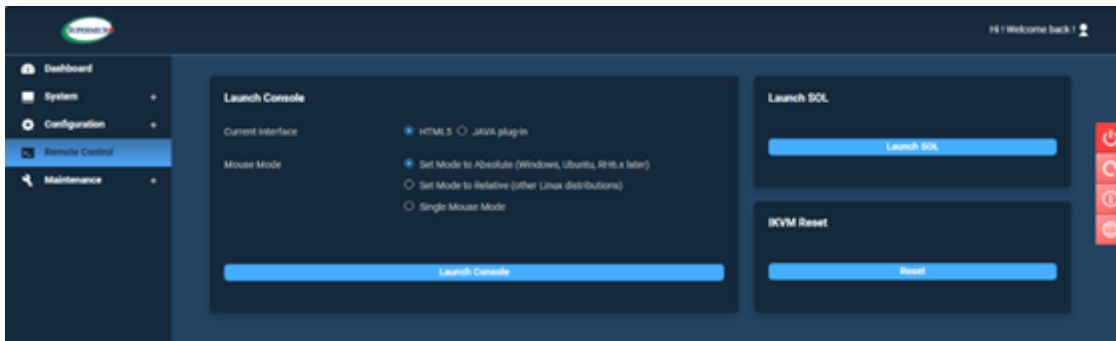


Step 3. Accessing the BMC Remote Server

1. The Remote Control menu in the BMC Remote Server enables remote server operations.

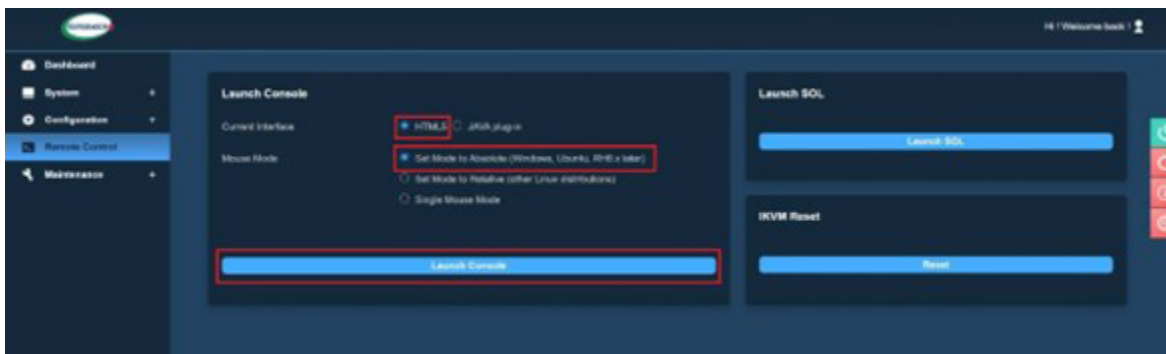


- Use the Launch Console section to configure the remote console interface settings. Choose between the HTML5 interface or a JAVA plug-in.



Launch an HTML5 Remote Browser

- Set HTML5 as the current interface.
- Choose the mouse mode according to your operating system, such as "**Set Mode to Absolute (Windows, Ubuntu, RH6.x, or later).**"
- Click the "**Launch Console**" button to open a console in a new browser window.

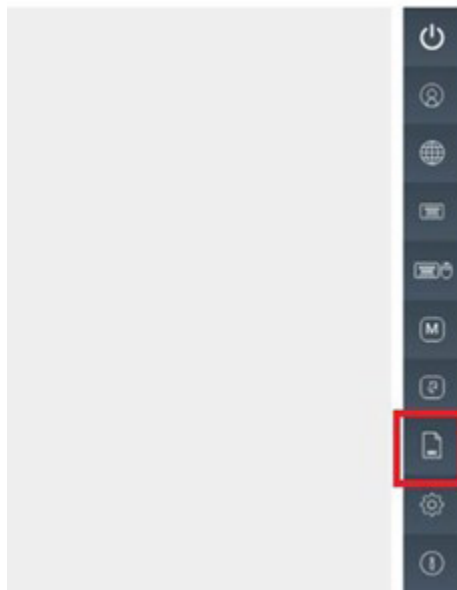


Step 4. Mounting the ISO Image

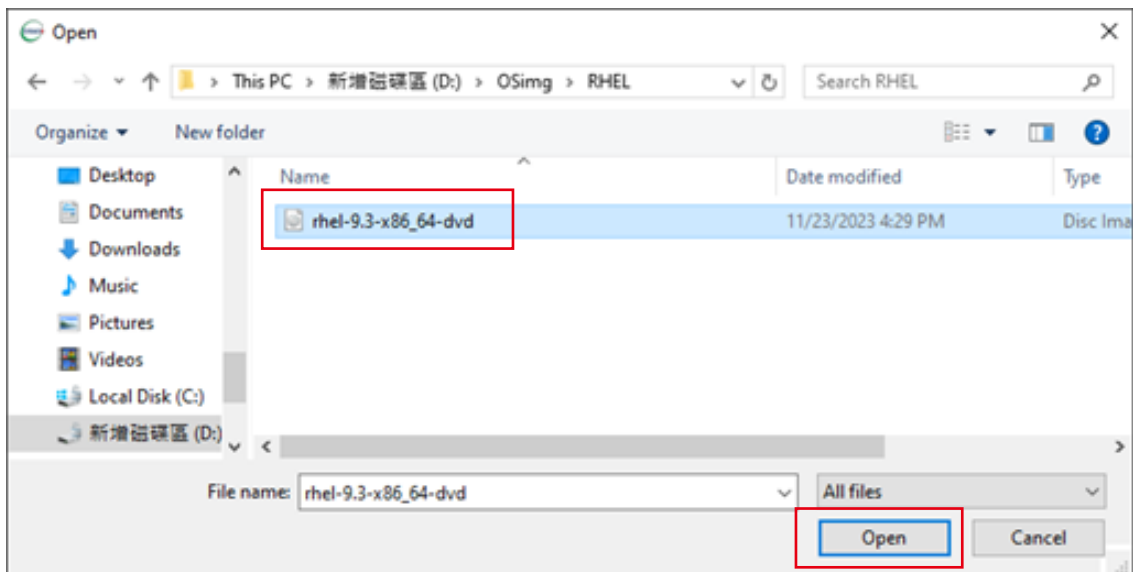
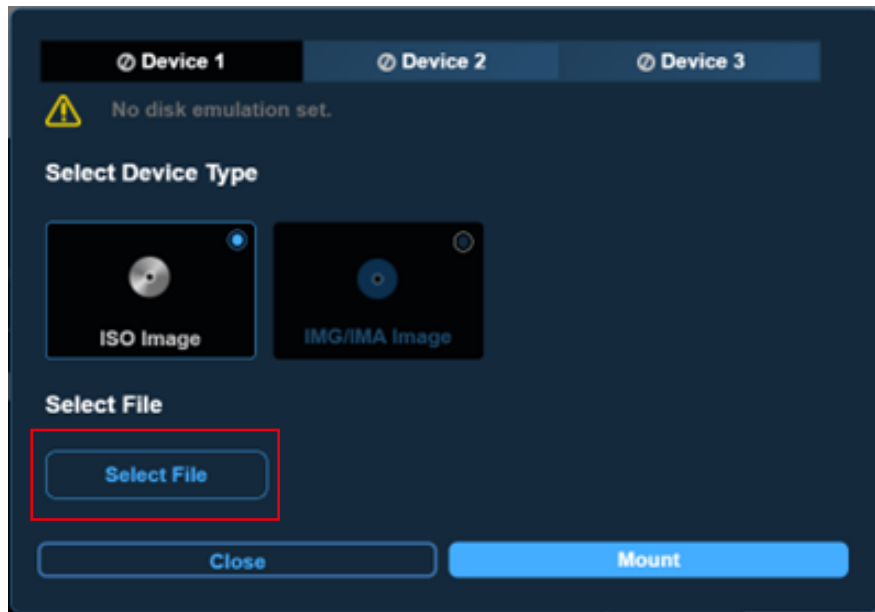
There are two methods to mount ISO images. If the ISO files are stored locally on your drive, you can mount them directly within the remote control browser. Alternatively, if the ISO files are located on a shared server, you can mount them via the Configuration > Virtual Media menu.

Method One: Mount the ISO Image Using a Local File

1. In the remote control browser, click the "**Virtual Media**" icon. This action will prompt a dialogue box to appear, enabling you to select the image type and files for mounting.



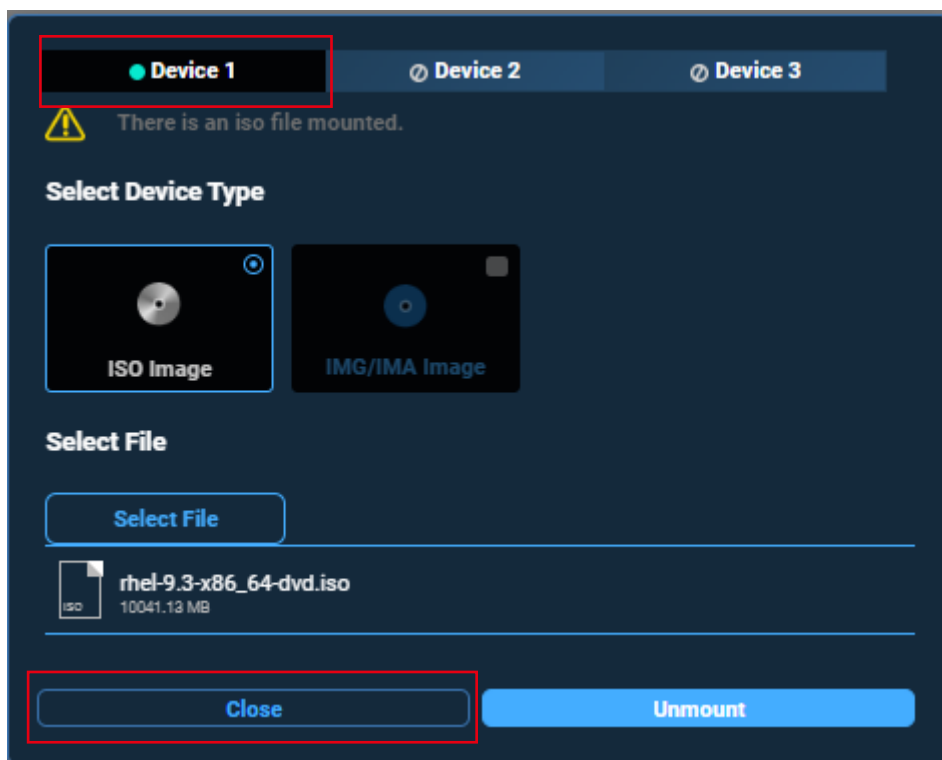
2. Select the "**Choose File**" button to browse and select the RHEL ISO image on your local driver for use.



3. Click the **"Mount"** button to attach the chosen ISO image.

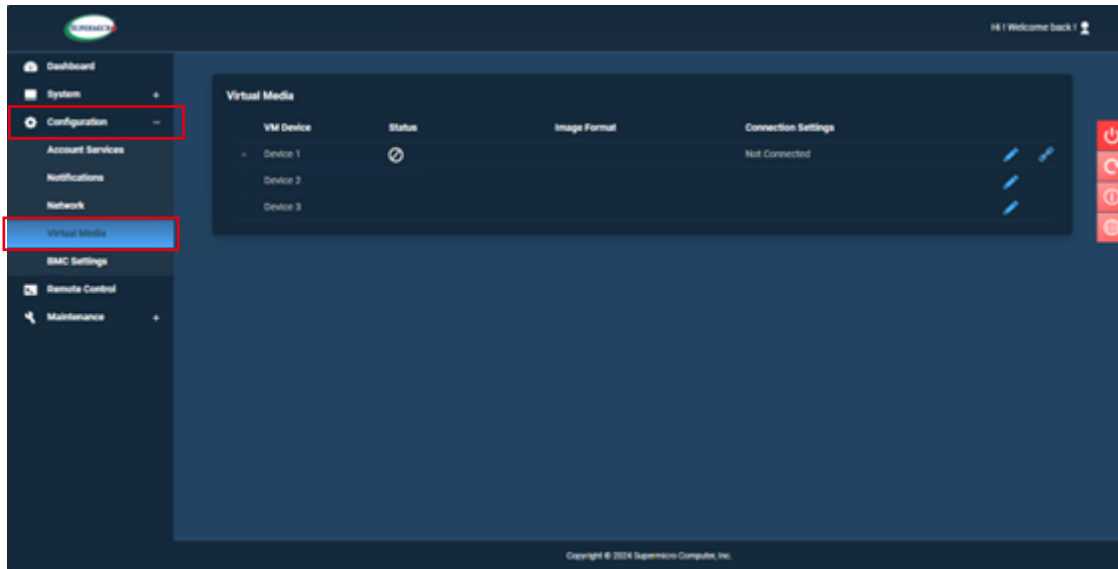


Result: Upon successful mounting of the ISO image, a green indicator will appear in the "Device" tab. Close the dialogue to continue.

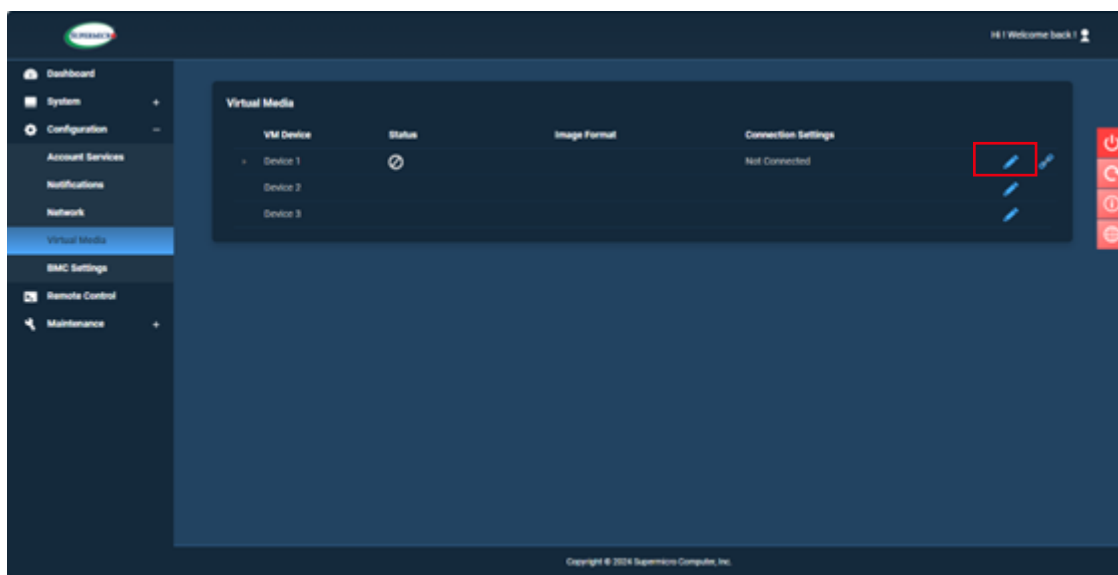


Method Two: Mount the ISO Image through a Shared Server

1. On the BMC dashboard, go to Configuration > Virtual Media. This allows you to attach an ISO image from the server.

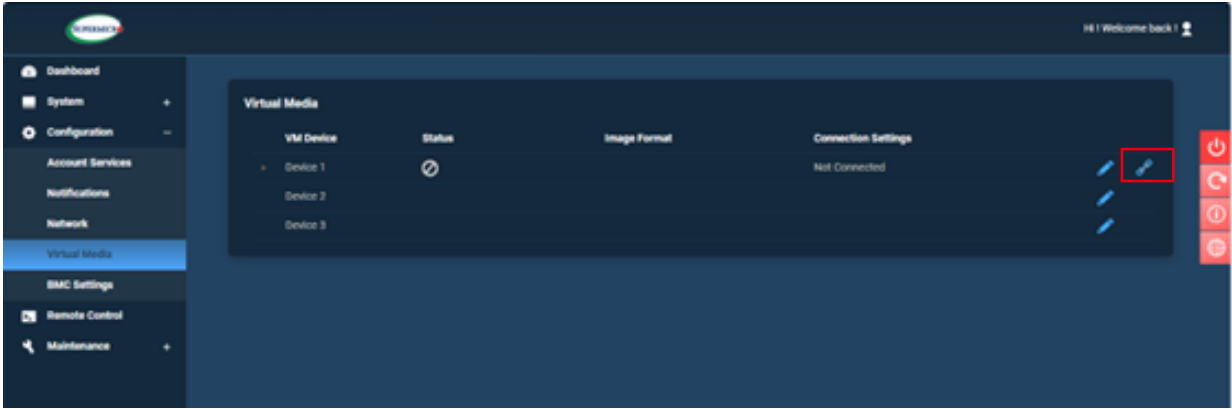


2. Click the "Edit" icon to adjust the VM configuration. Enter the server host address and the path to the ISO image. Then, click the "Save" to apply the changes.

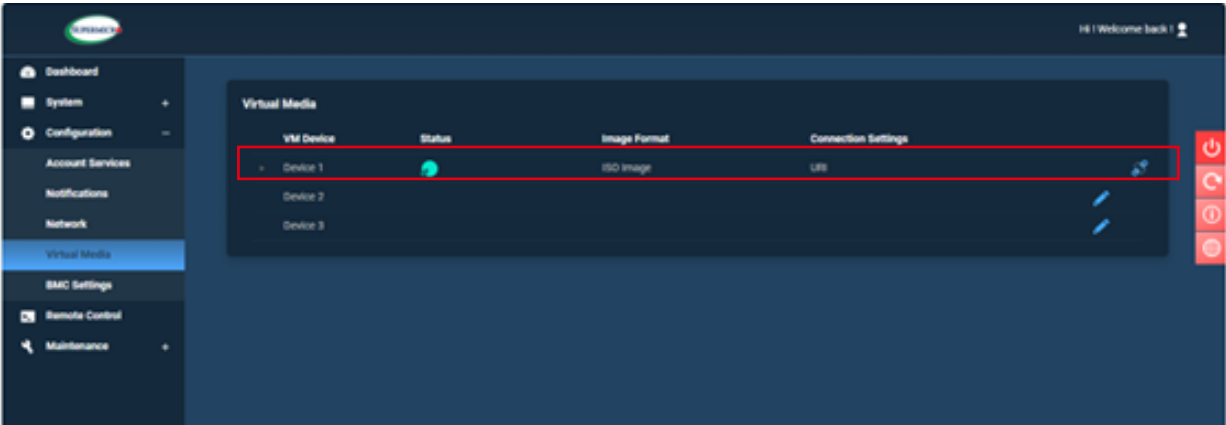




3. Click the "Connect" icon to mount the virtual media.



4. The device status will display as green once the VM is successfully configured.



Step 5. Boot from Virtual Media

To boot from the mounted image in virtual media, users must manually select the boot device from the Boot Menu during BIOS POST.

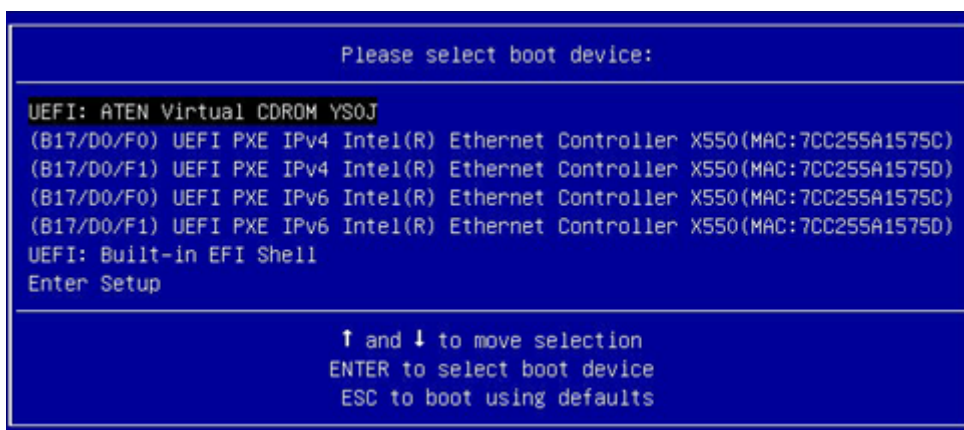
1. Power on the system and wait for the Log screen to display. To access the BIOS setup menu, repeatedly press <F11> until "Invoke Boot Menu" appears at the bottom left corner of the screen.



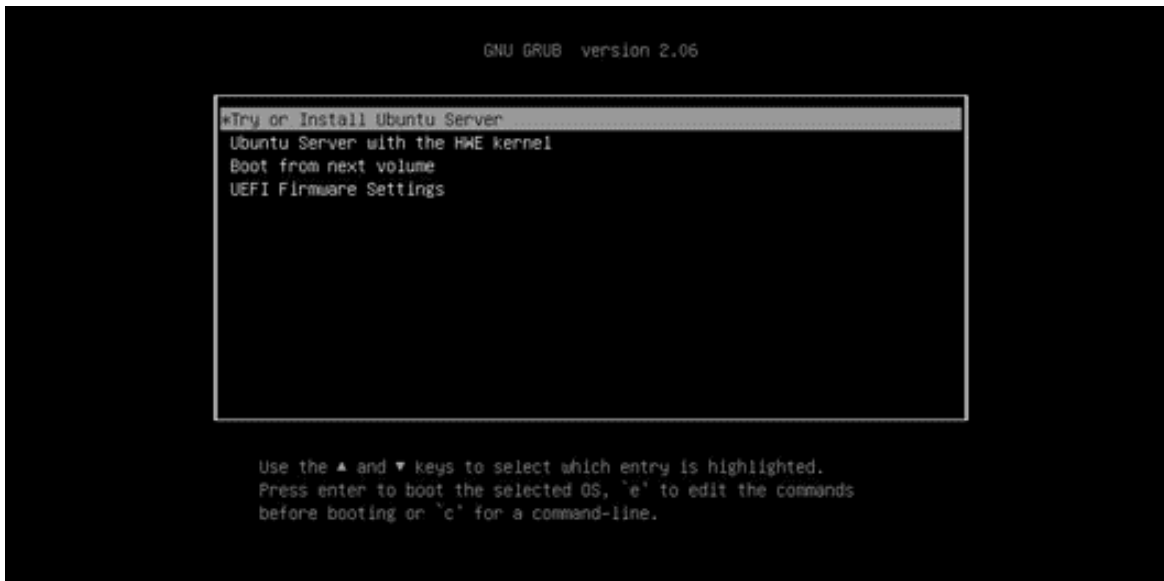
Invoking Boot Menu

90

Subsequently, the Boot Menu is displayed.



2. Select **"UEFI: ATEN Virtual CDROM YSOJ"** as the boot menu. This selection mounts the ISO image mounted in Virtual Media. Press "Enter" to proceed. The GRUB menu will be displayed.

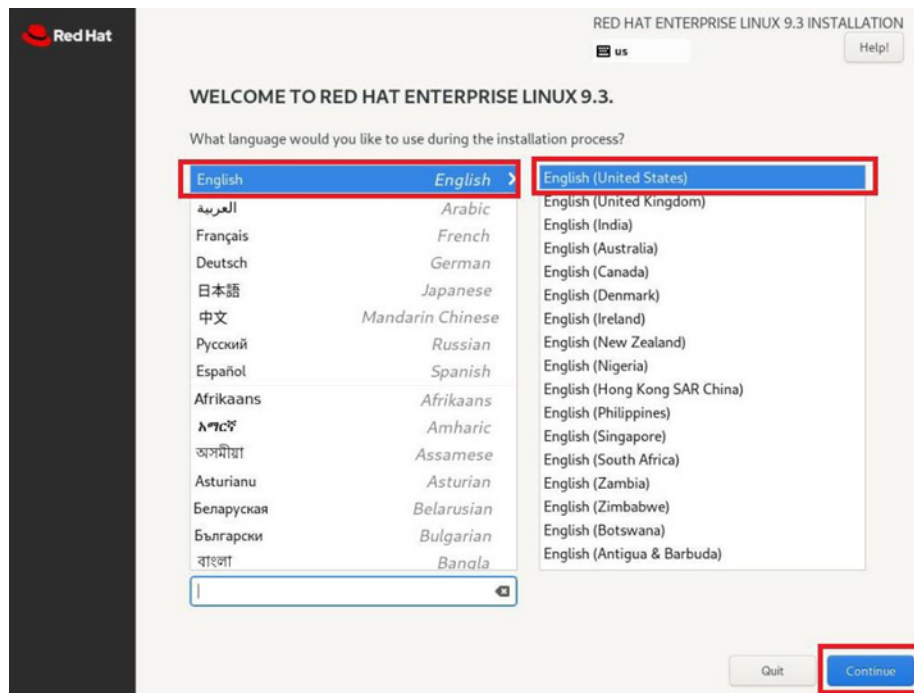


Step 6. Installing the RHEL 9.3 OS

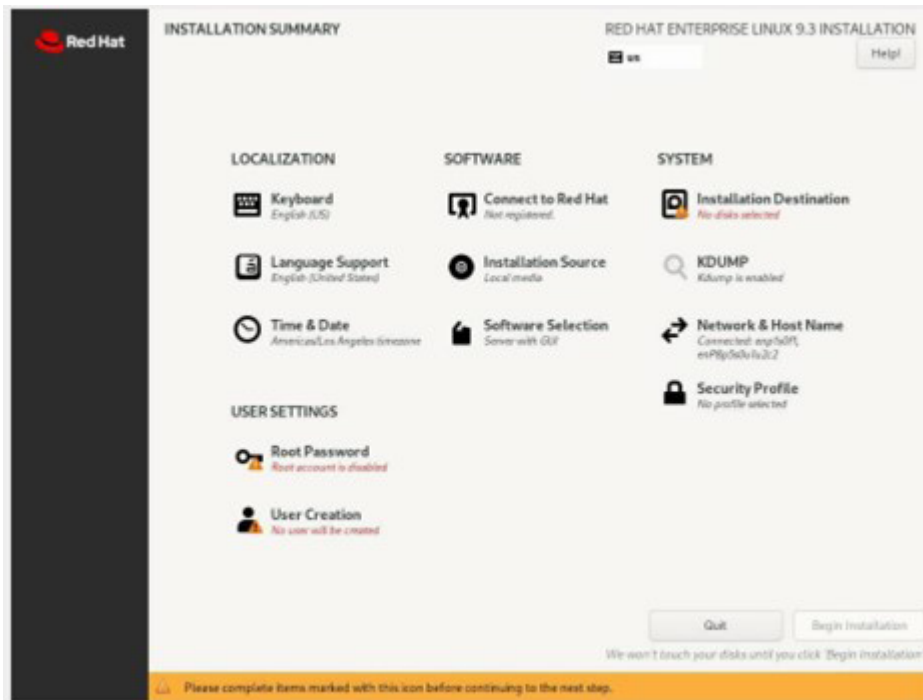
1. Follow the Ubuntu installer steps to continue installation. Choose **"Try or Install Ubuntu Server"** to proceed.



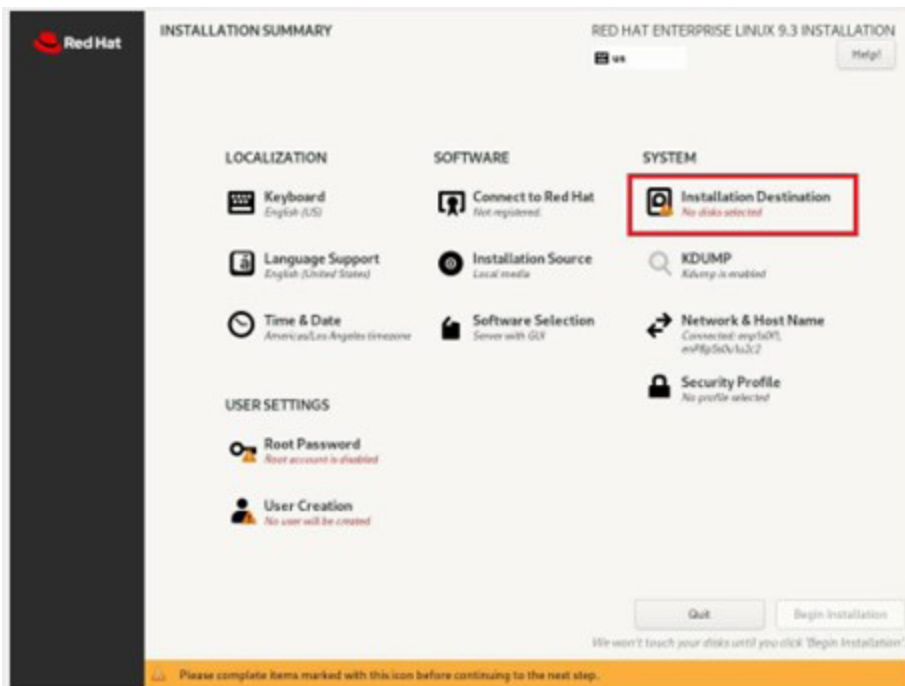
2. Select the language.



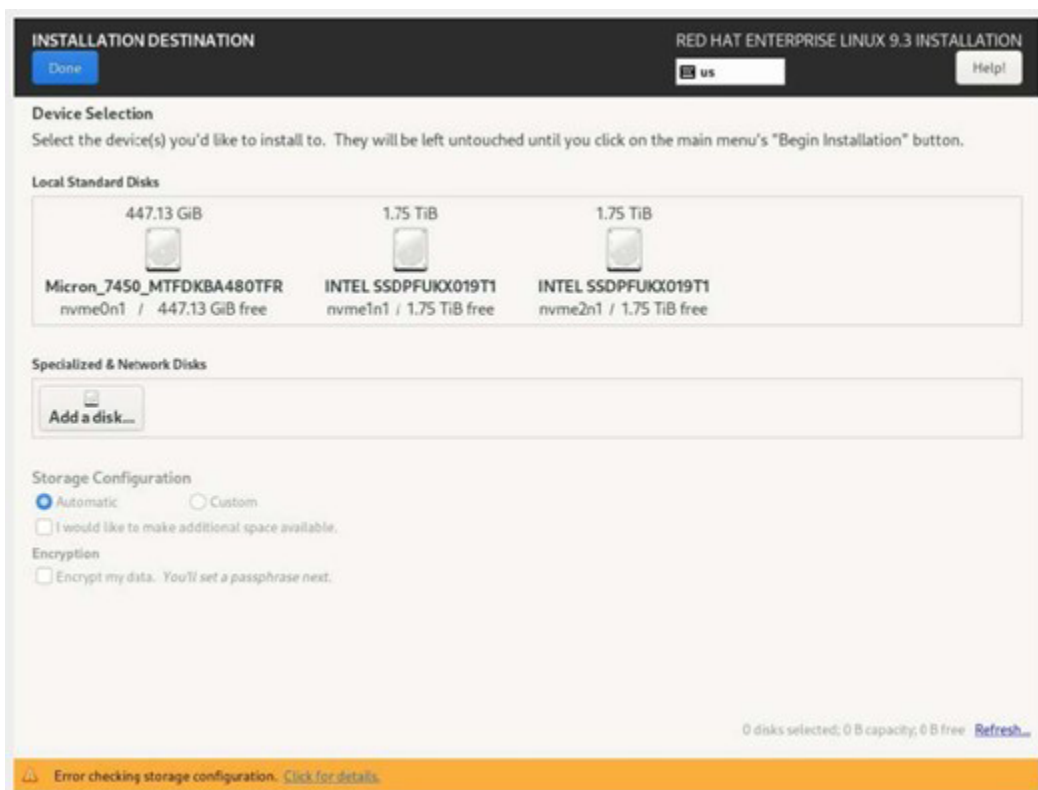
3. The Installation Summary window provides a glance of the configuration you need before you begin the installation.



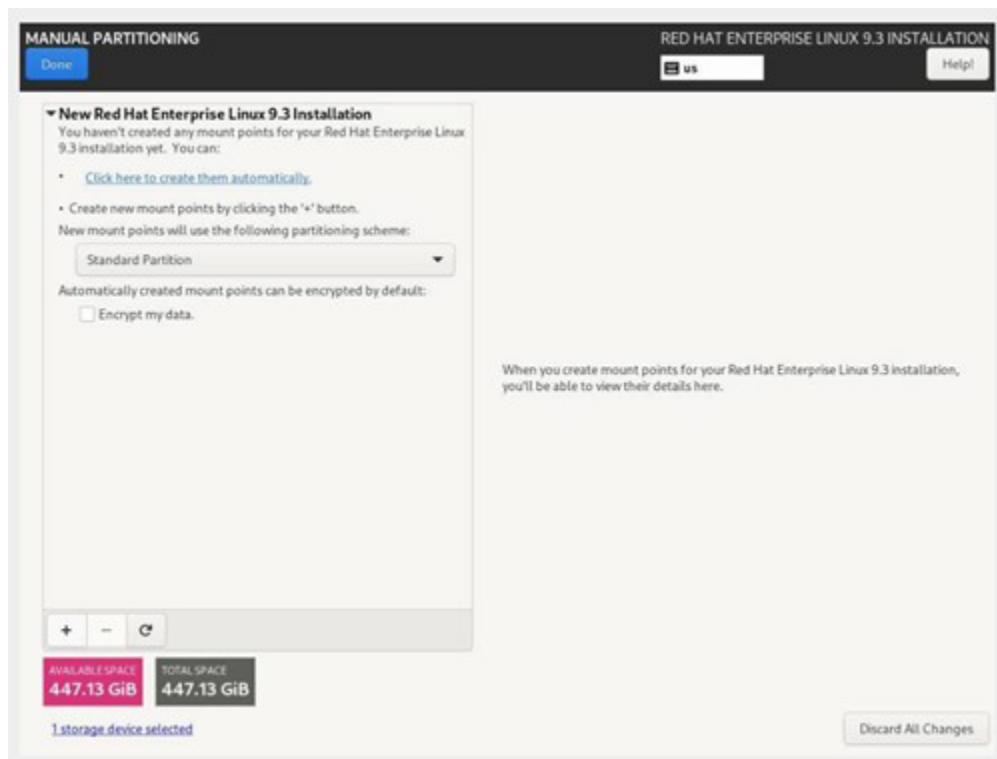
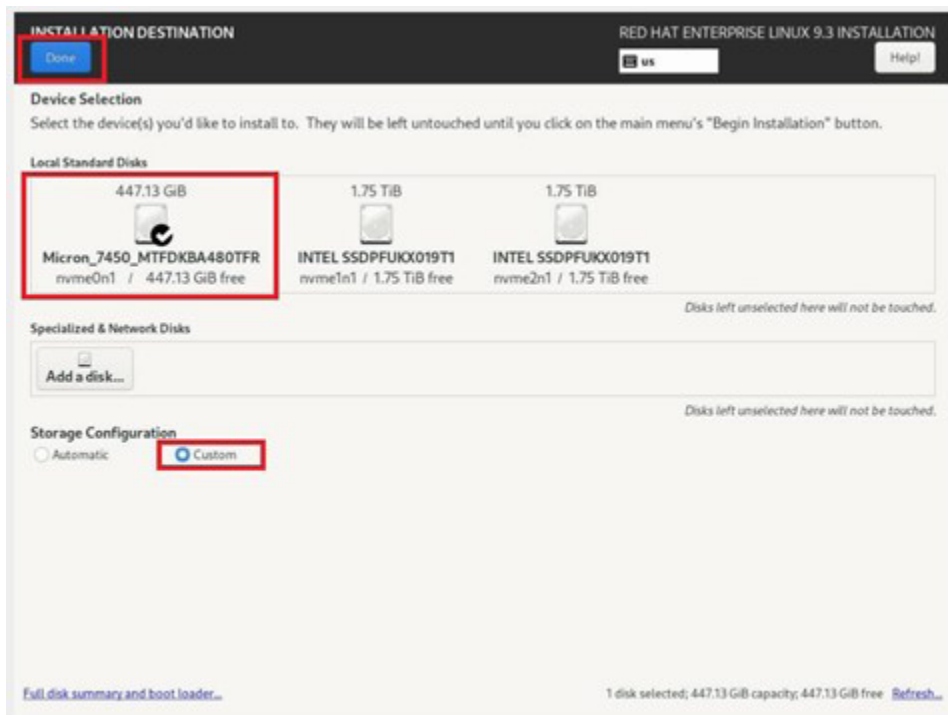
- Click the "Installation Destination" button to select the storage drive.



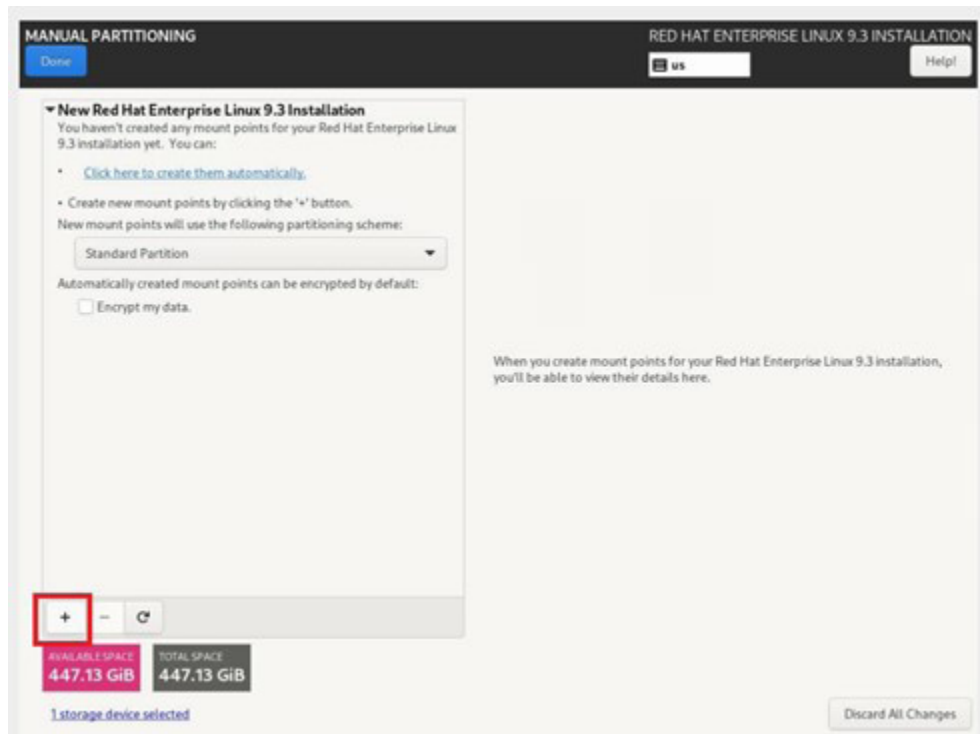
- Select the drive to which you want to install the RHEL OS.



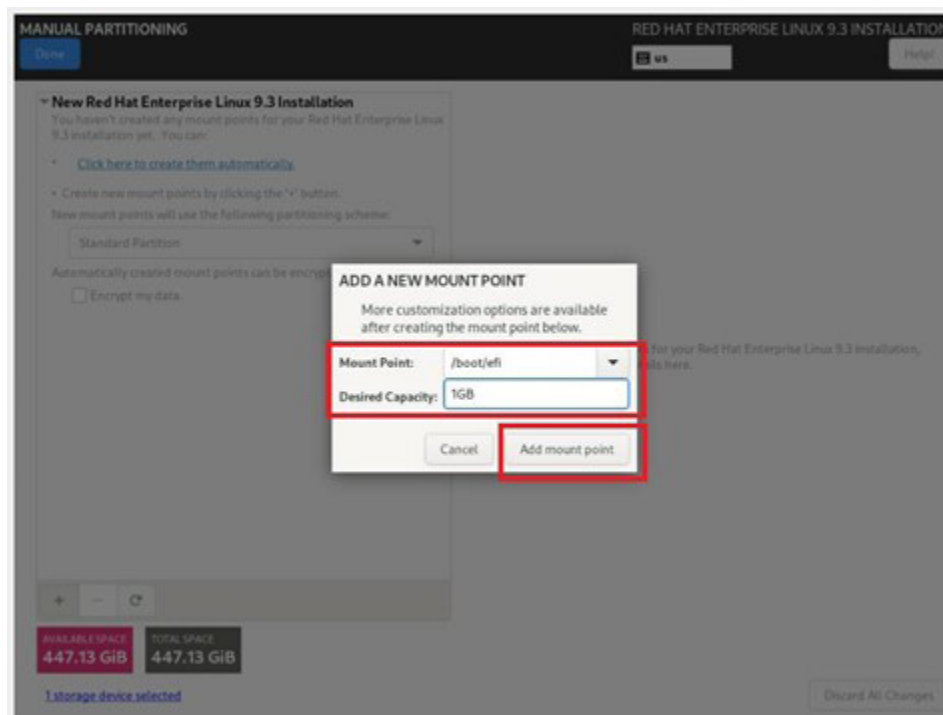
6. Select one of the drives and choose **"Custom"** if you want to customize the drive's volume. This will display the available space on the selected drive.



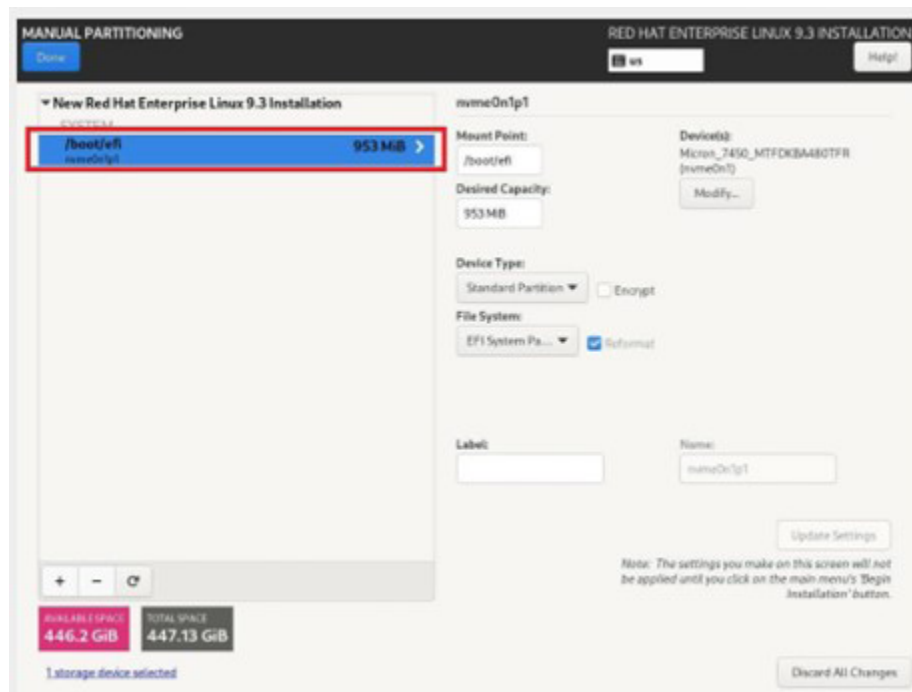
- For RHEL, you need to have at least three mount points (/boot/efi, /, and swap). Click the "+" button to create new mount point **"/boot/efi"** as the boot partition for EFI system.



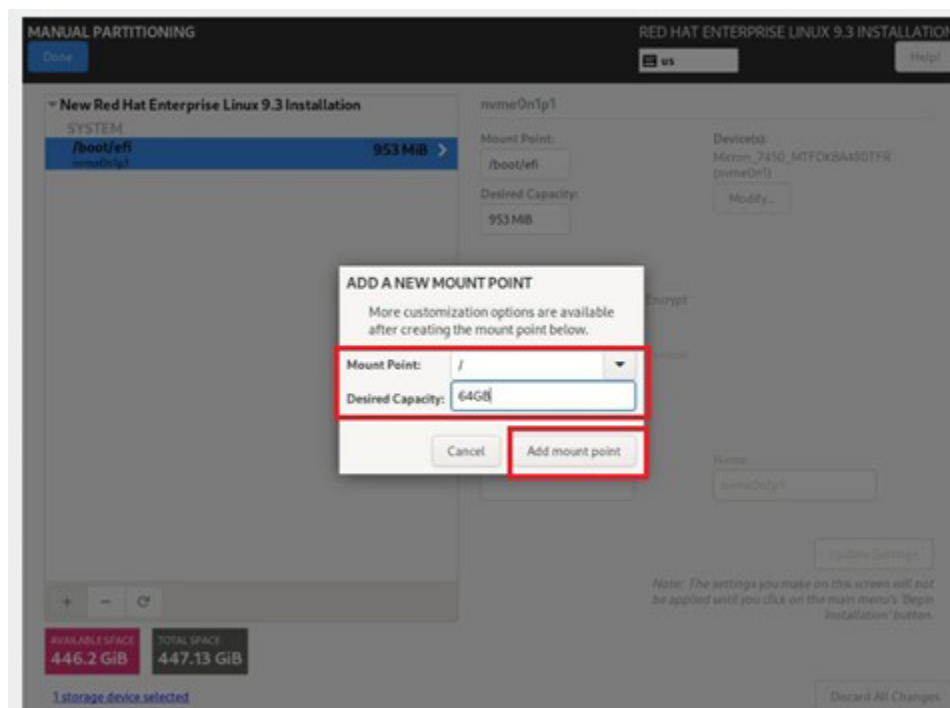
- The **"Add a new mount point"** dialogue will pop up. Select the mount point **"/boot/efi"** and the storage size. Then, click the **"Add mount point"** button.



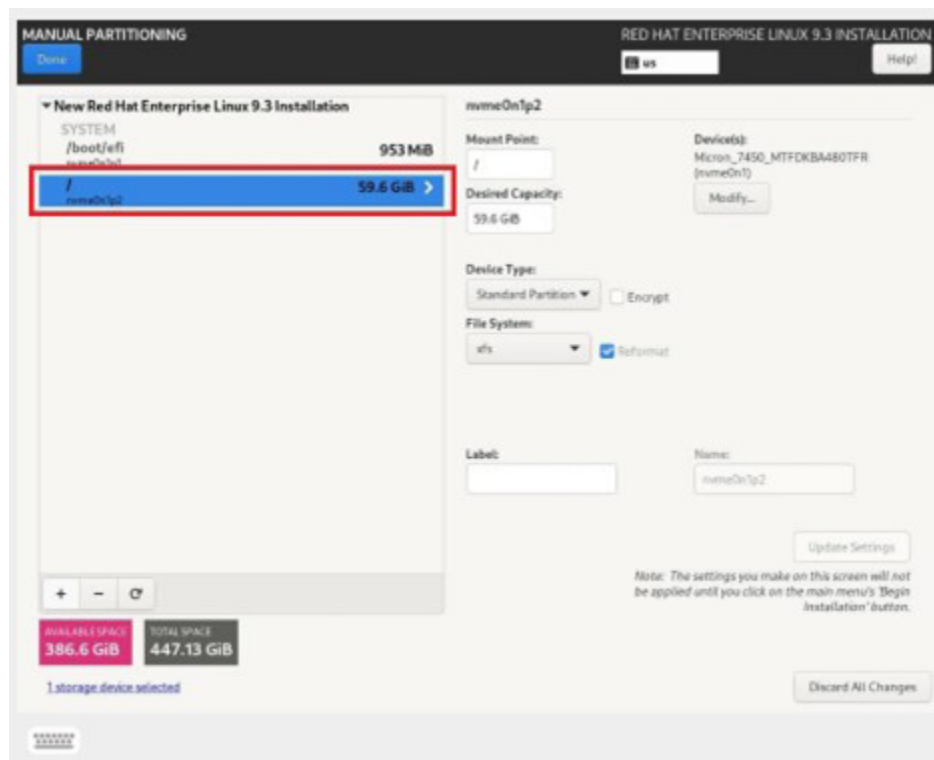
Result: The new mount point `"/boot/efi"` will be added under the **"New Red Hat Enterprise Linux 9.3 Installation"**.



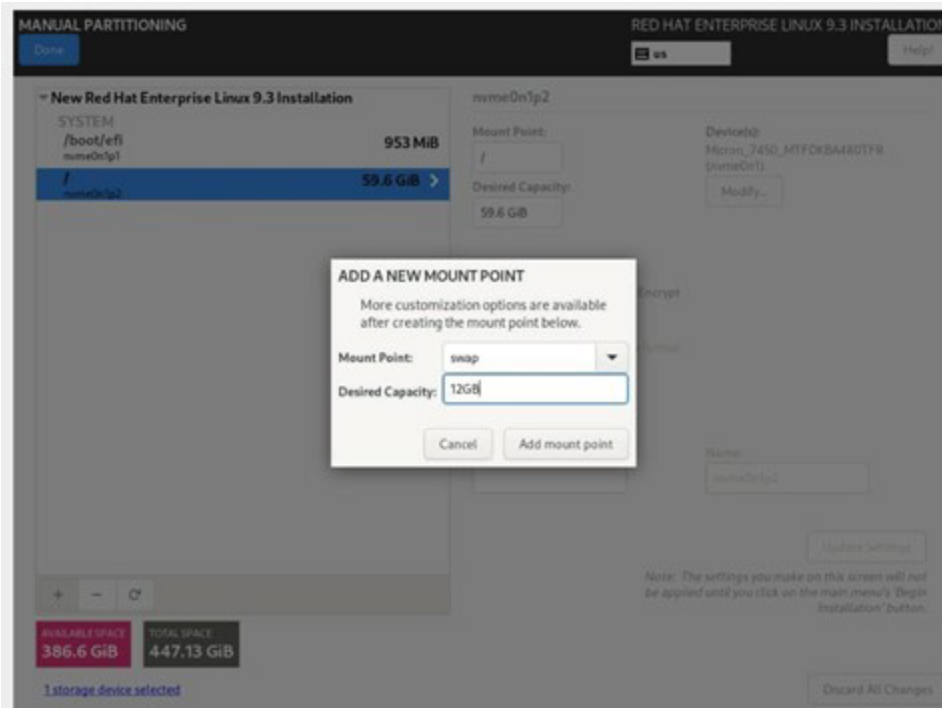
- Click the **"+"** button to create another new mount point `"/"` as the root directory. Configure the mount point `"/"` and the desired storage size. Then, click the **"Add mount point"** button.



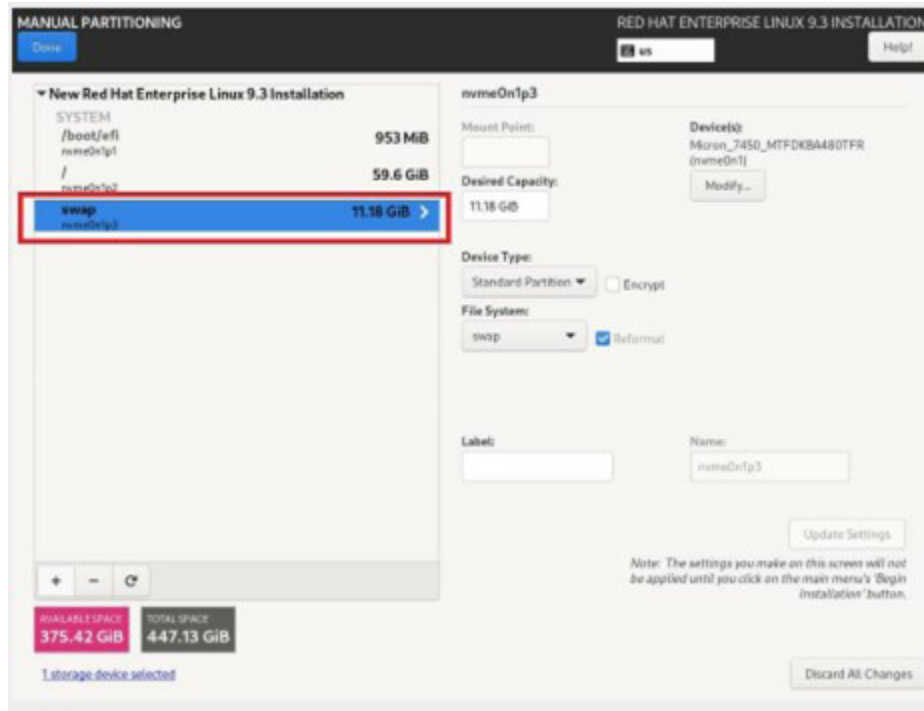
Result: The new mount point "/" will be added under the "New Red Hat Enterprise Linux 9.3 Installation".



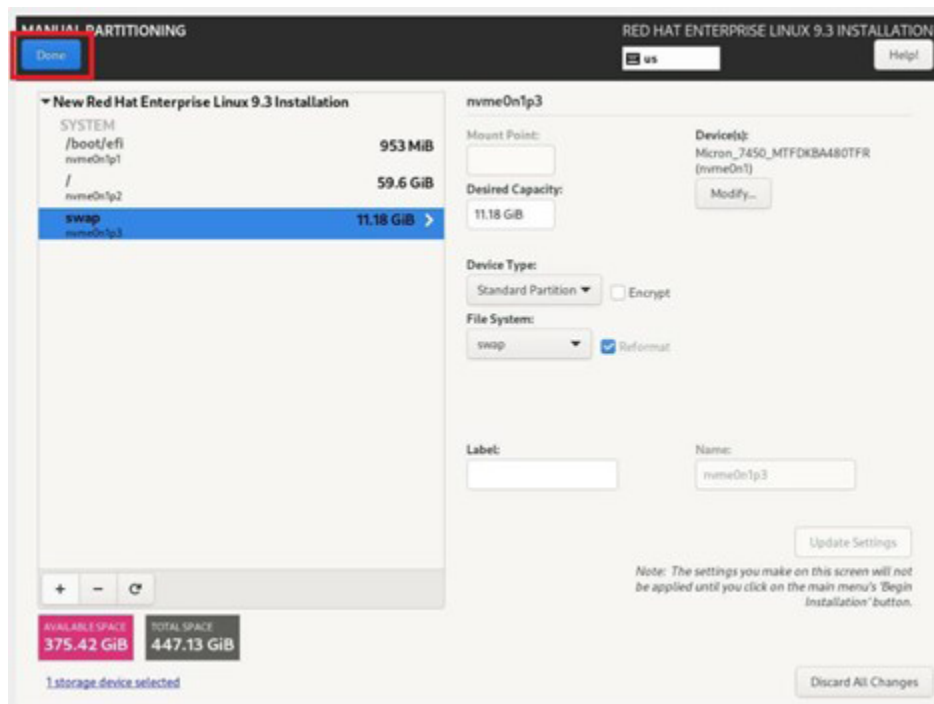
- Click the "+" button to create another new mount point "swap" for virtual memory space. Configure the mount point "swap" and the desired storage size. Then, click the "Add mount point" button.



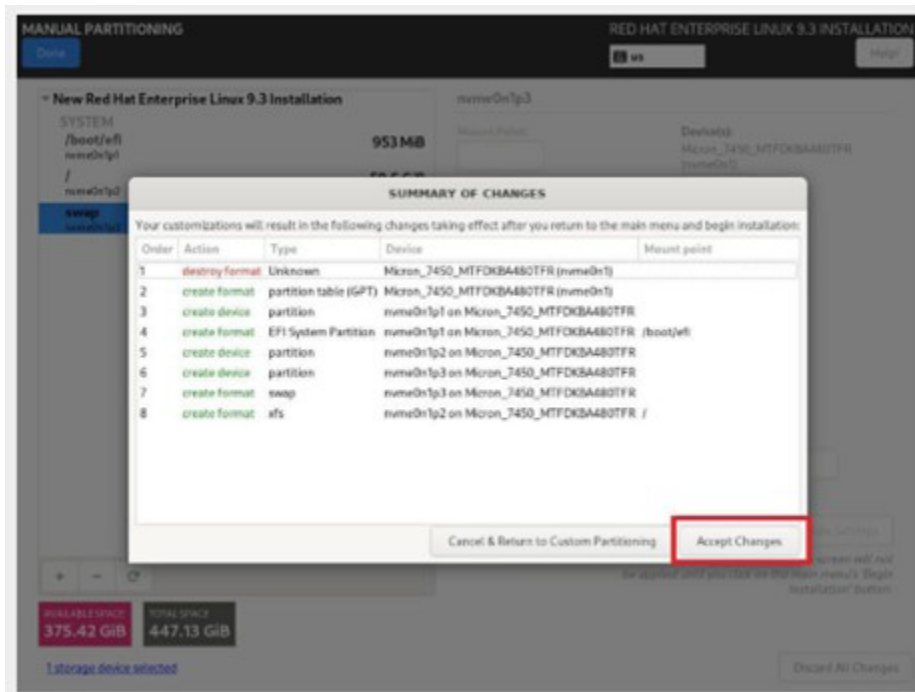
Result: The new mount point "swap" will be added under the "New Red Hat Enterprise Linux 9.3 Installation".



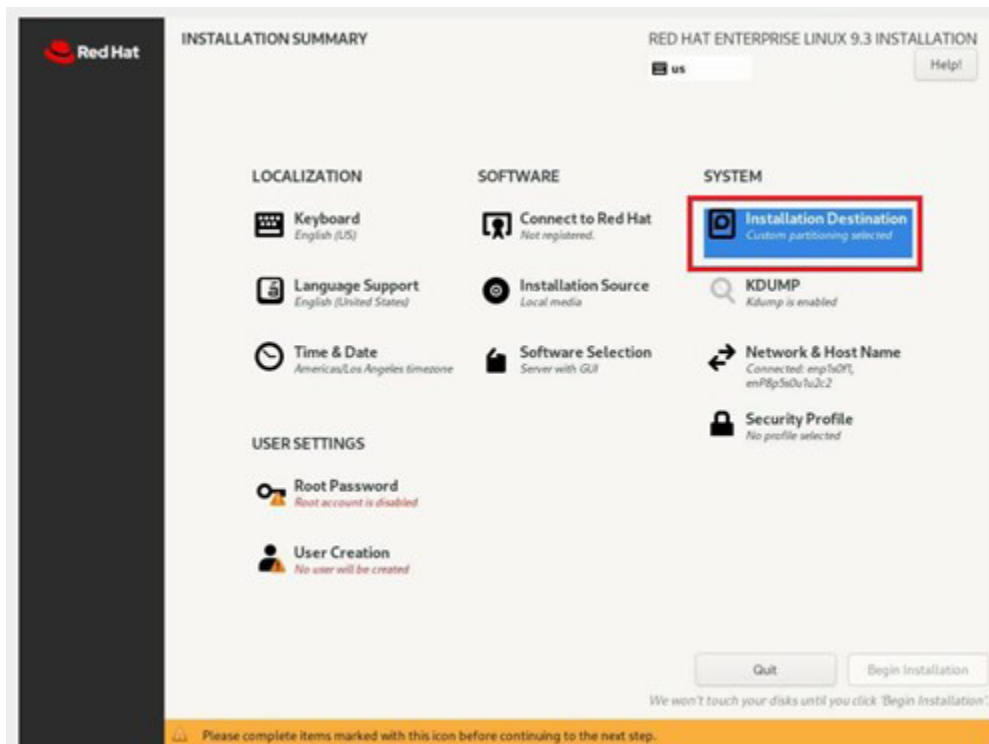
11. Click the "Done" button at the left top corner after all the required partitions are created.



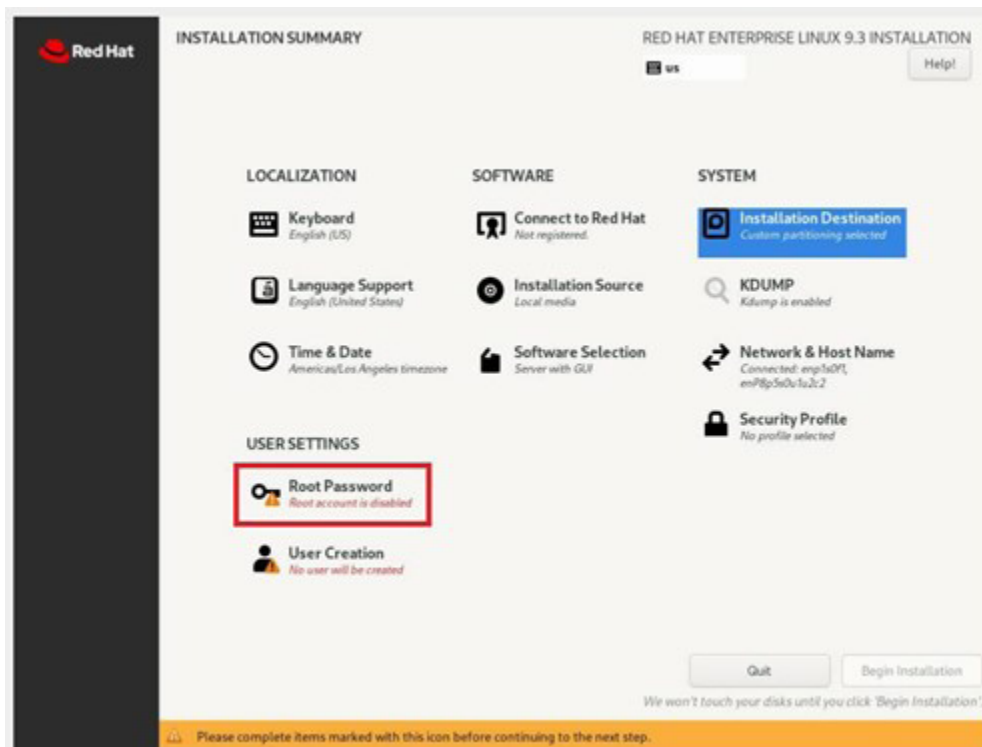
12. Accept the changes to customize the partitions.



Result: In the "Installation Summary" screen, Installation Destination has been updated to "Custom partitioning selected."



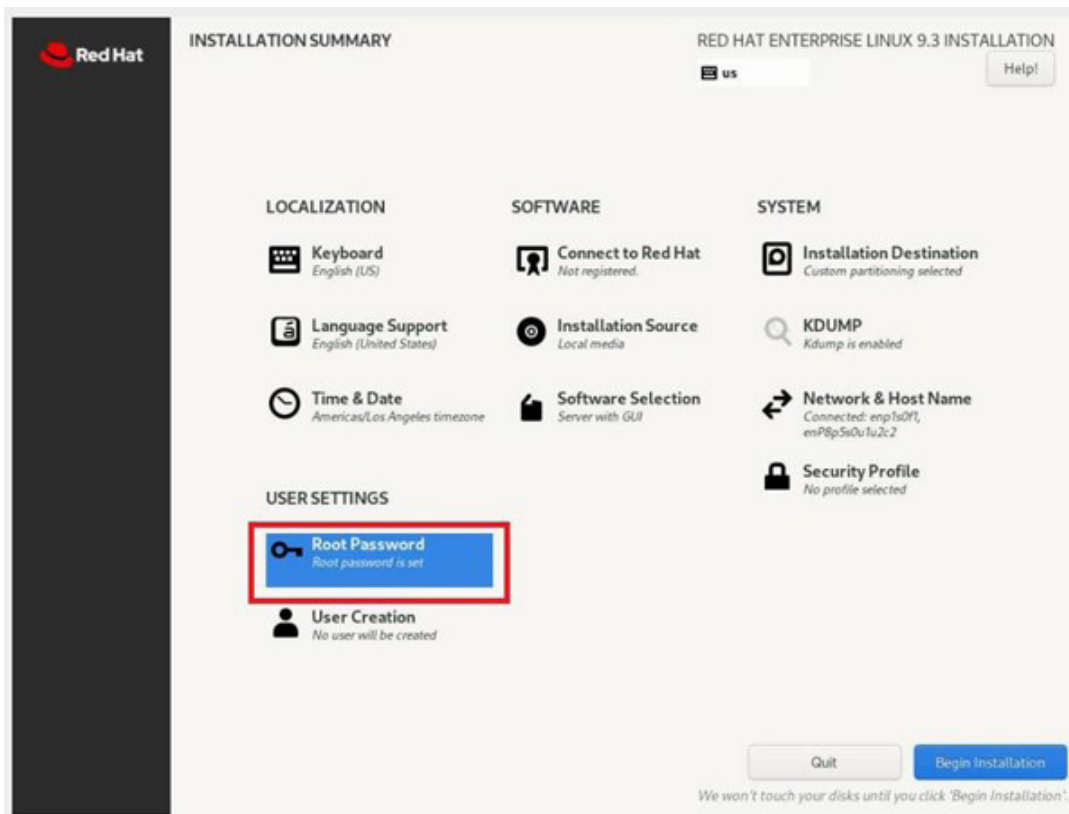
13. Click the "Root Password" in the "Installation Summary".



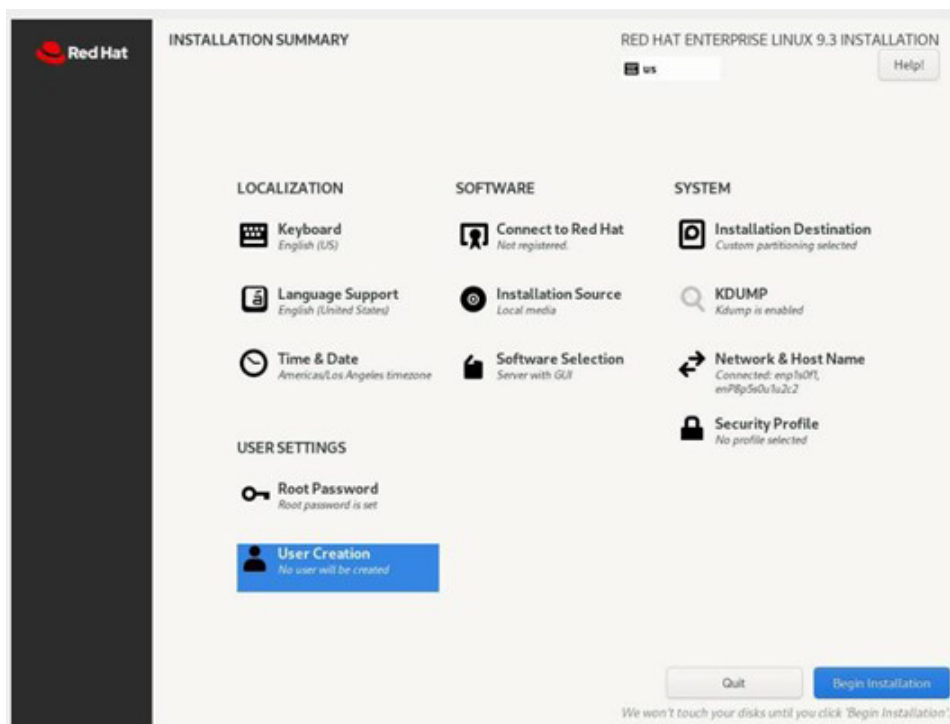
14. Enter the password for the root user.



Result: The status of the Root User becomes "Root Password is set".



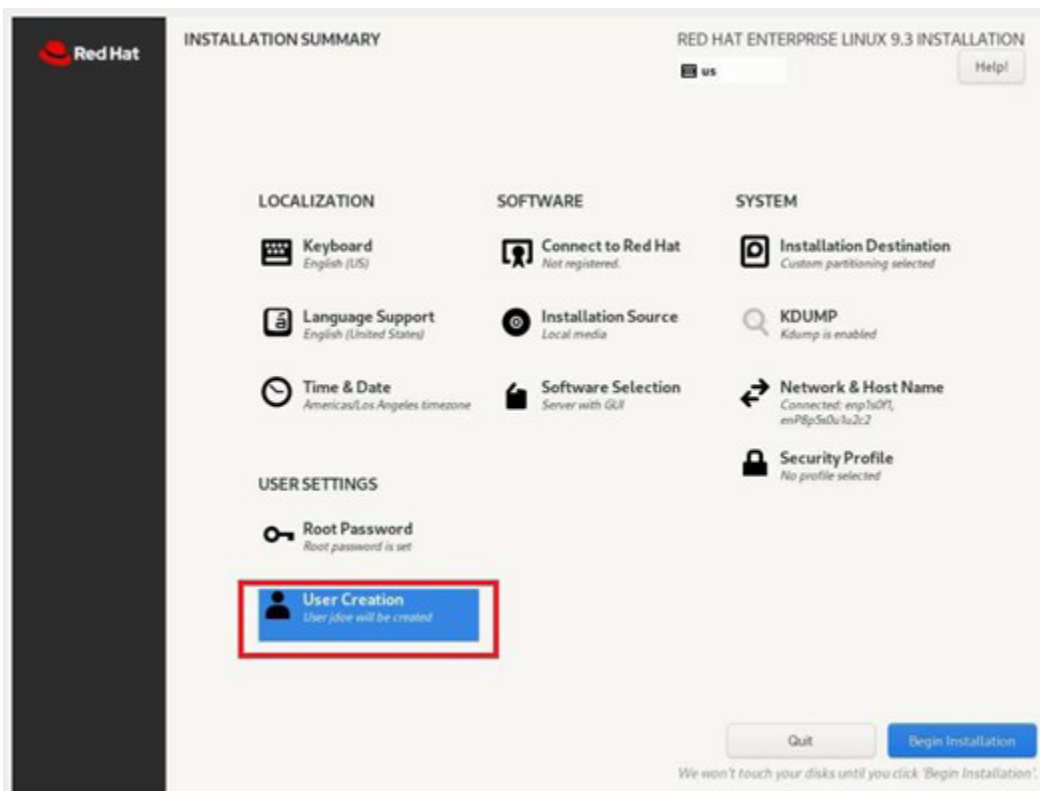
15. Click the "User Password" in "Installation Summary".



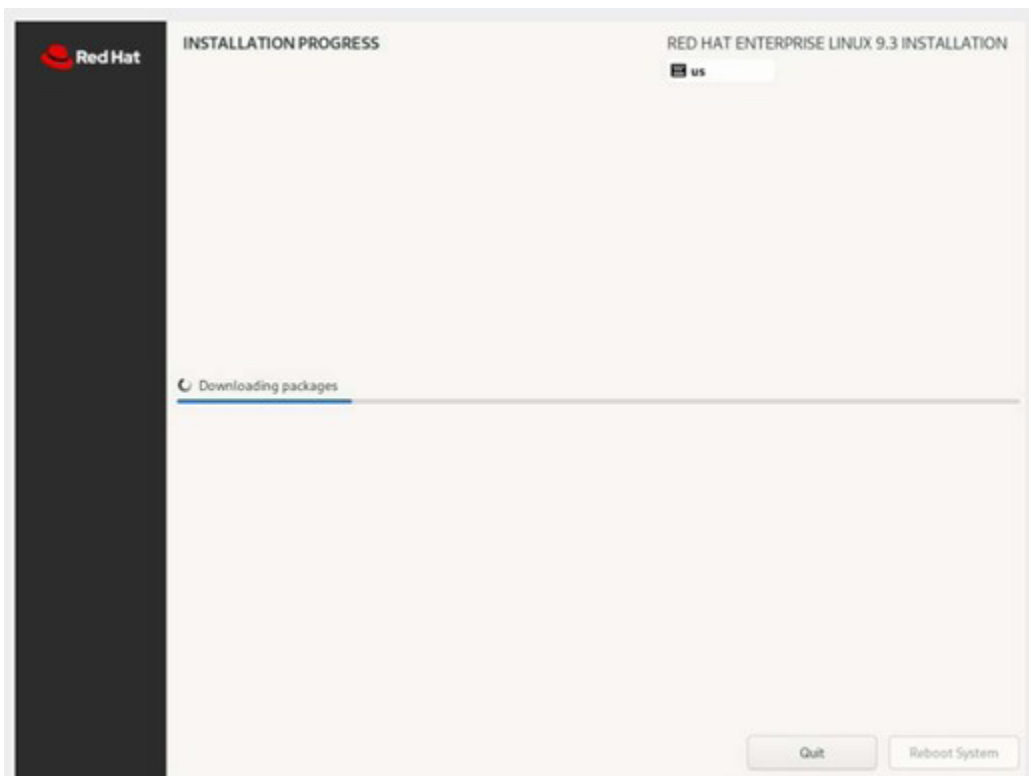
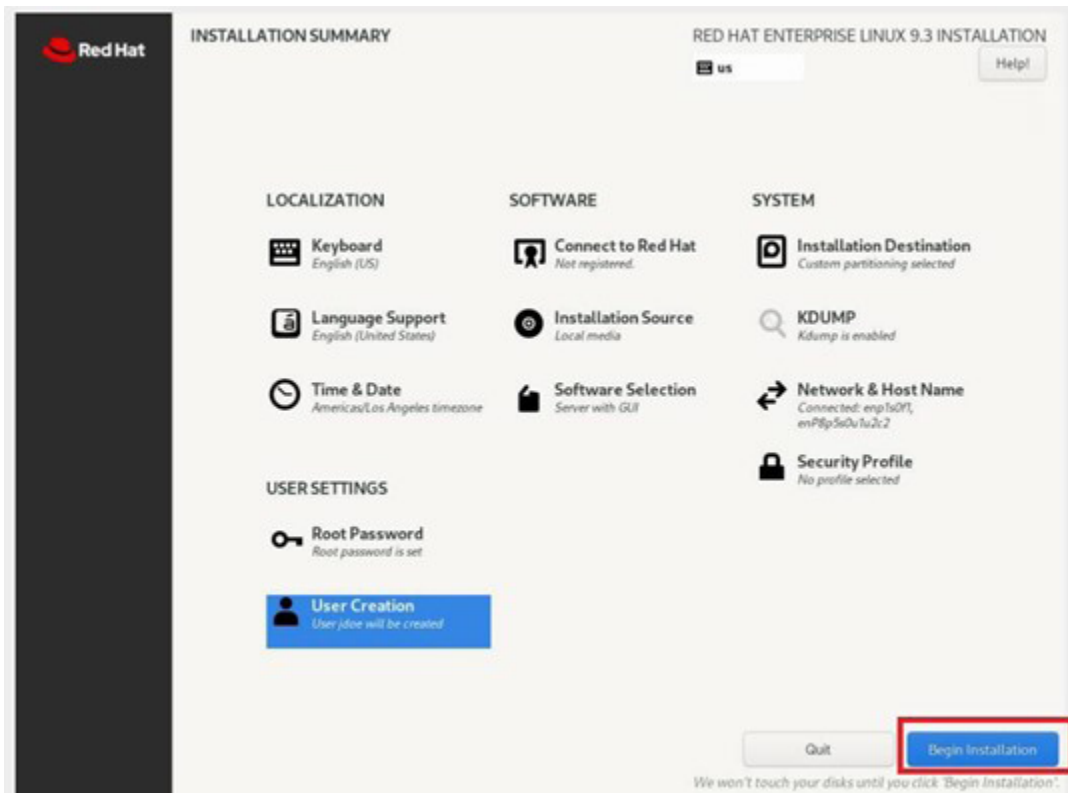
16. Enter "Full Name", "User Name", "Password", and "Confirm Password" details. Once done, click the "Done" button.

The screenshot shows the 'CREATE USER' window. At the top left, a blue 'Done' button is highlighted with a red box. The main area contains several input fields: 'Full name' with 'Jane Doe', 'User name' with 'jdoe', 'Password' with masked characters and a 'Too short' error message, and 'Confirm password' with masked characters. There are also checkboxes for 'Make this user administrator' (unchecked) and 'Require a password to use this account' (checked). An 'Advanced...' button is at the bottom.

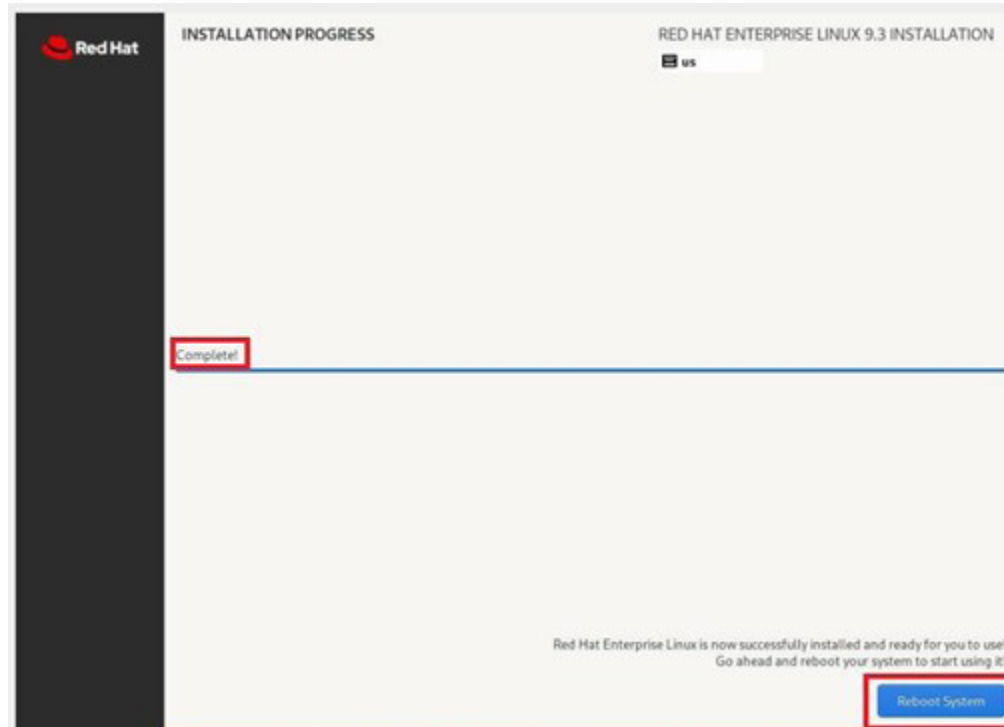
Result: The status of User Creation becomes "User username is set".



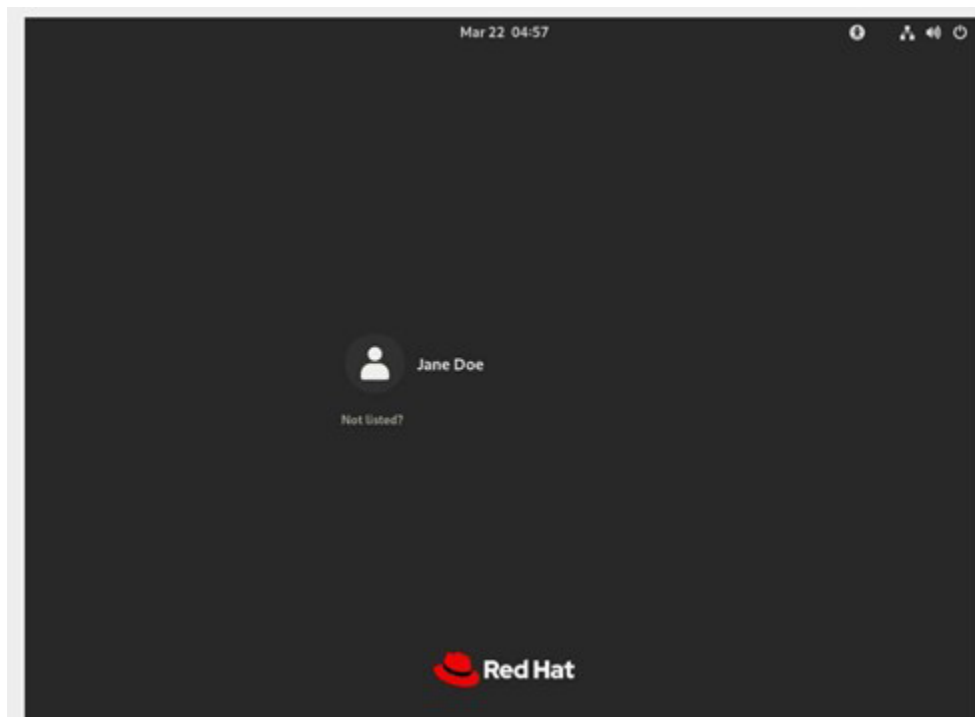
17. After completing all the above steps, click the **"Begin Installation"** to start the installation process.



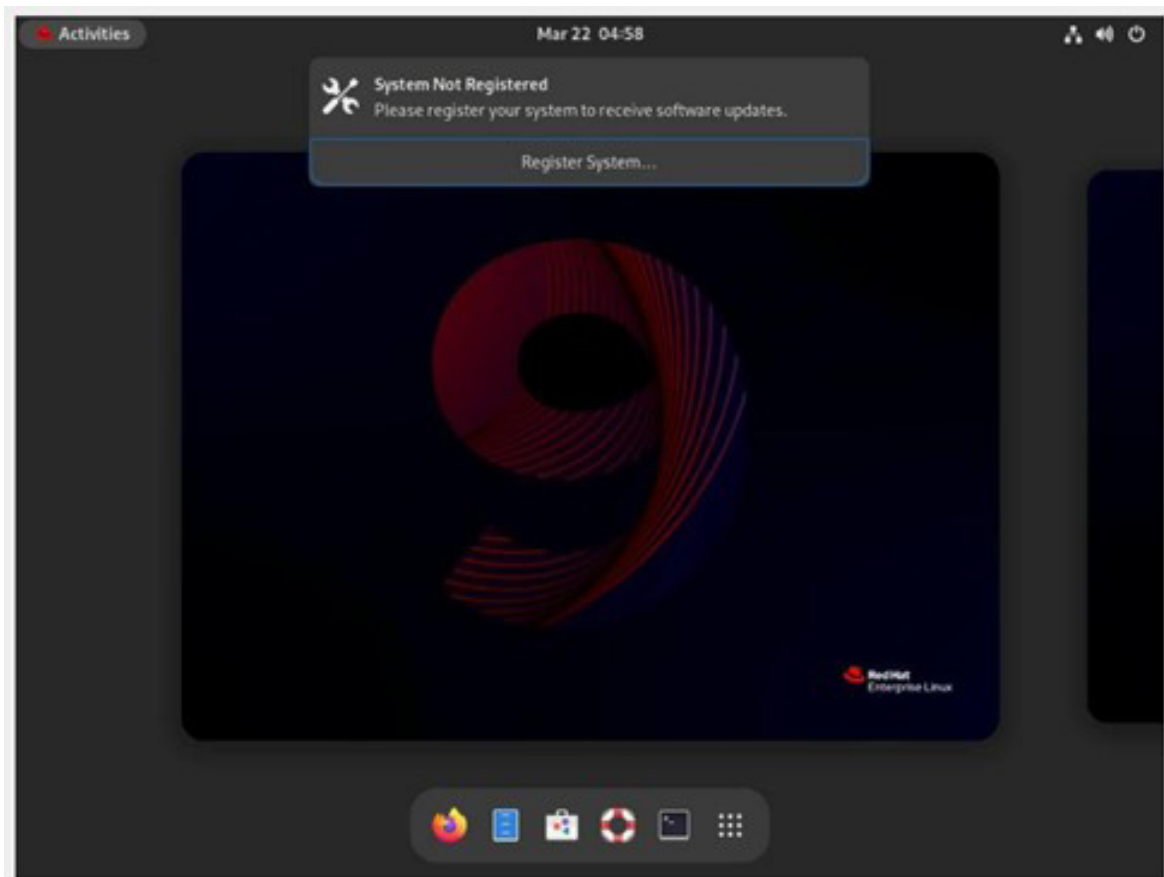
18. After the installation is complete, click the **"Reboot System"** to reboot.



19. After rebooting, the user login page shows up. Enter the user password to log in.



Result: Log in successfully. You can start using this system.

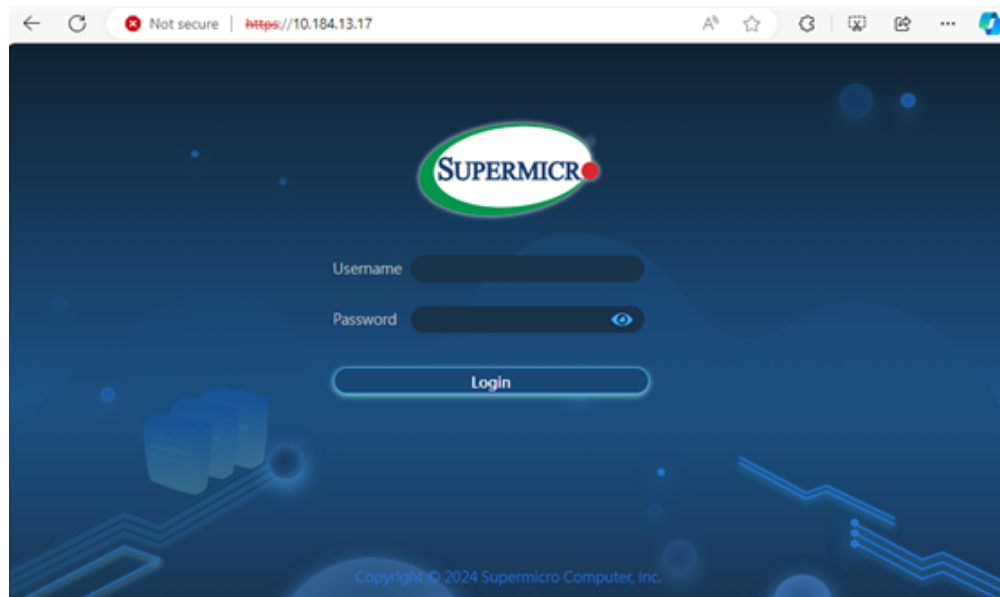


Step 1. Accessing the BMC Remote Server

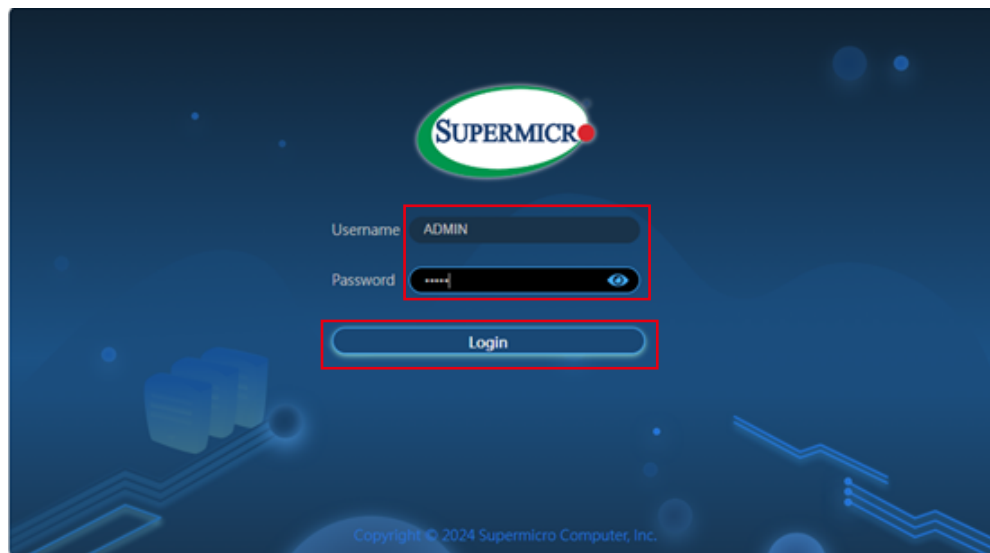
Log in to BMC Remote Server

1. In the terminal, execute a ping command to the BMC IP address, such as 10.184.13.17, to verify its connectivity.
2. Launch a new web browser and input the BMC IP address into the URL field.

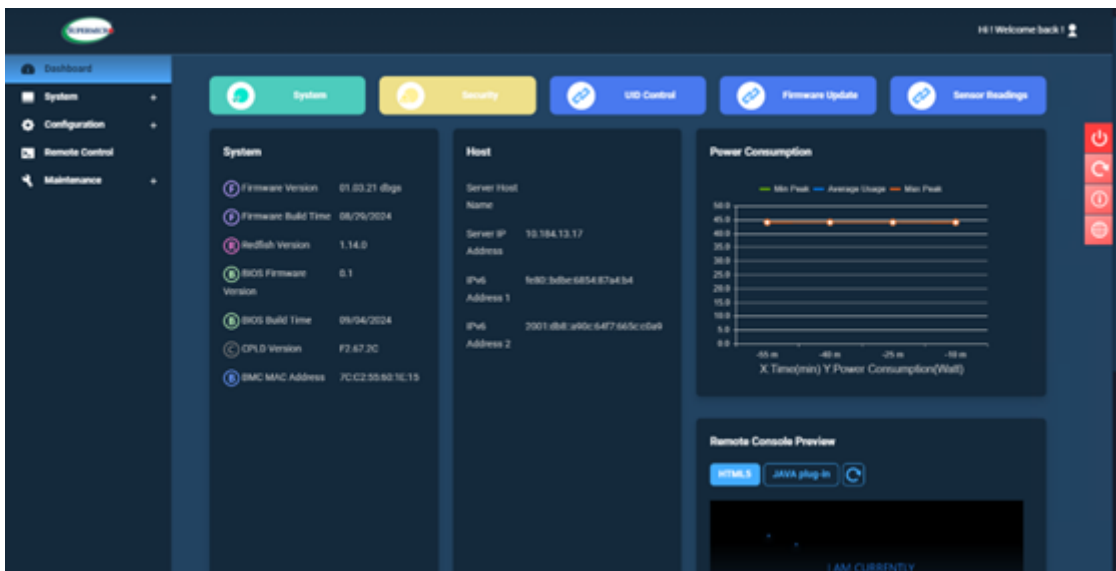
Outcome: The BMC Remote Console login screen will be displayed.



3. Input the username "**ADMIN**" and the unique BMC password, which is located on the label on the opposite side of the service tag of the system. Click the "**Login**" to proceed.



Outcome: The BMC Dashboard offers insights into system overview, configuration, health status, and maintenance.

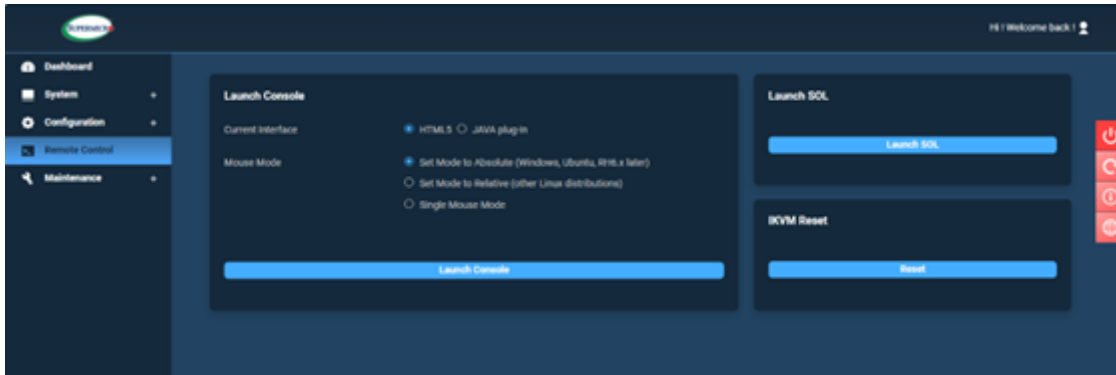


Step 3. Controlling the System Remotely

1. The Remote Control menu in the BMC Remote Server enables remote server operations.

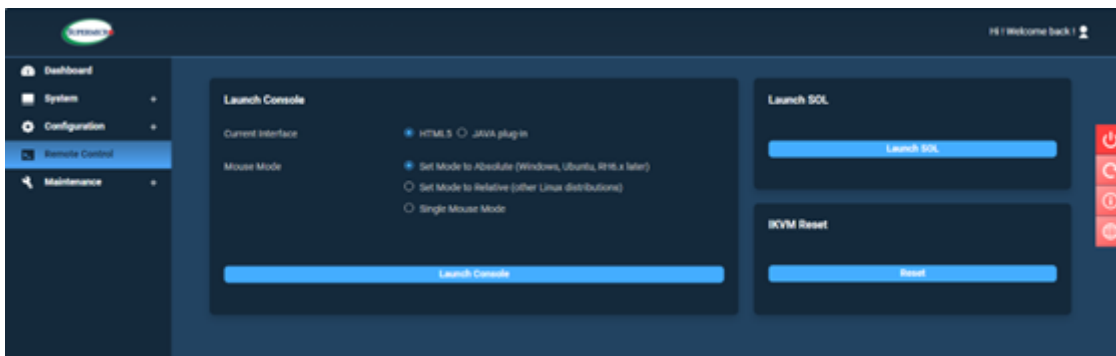


- Use the Launch Console section to configure the remote console interface settings. Choose between the HTML5 interface or a JAVA plug-in. Launch an HTML5 remote browser.



To launch an HTML5 Remote Browser

- Set HTML5 as the current interface.
- Choose the mouse mode according to your operating system, such as "**Set Mode to Absolute**" (Windows, Ubuntu, RH6.x, or later)."
- Click the "**Launch Console**" button to open a console in a new browser window.

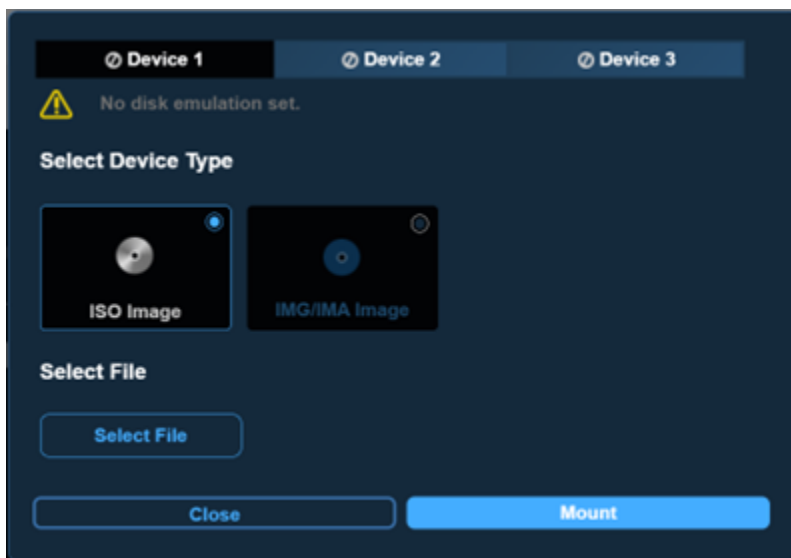
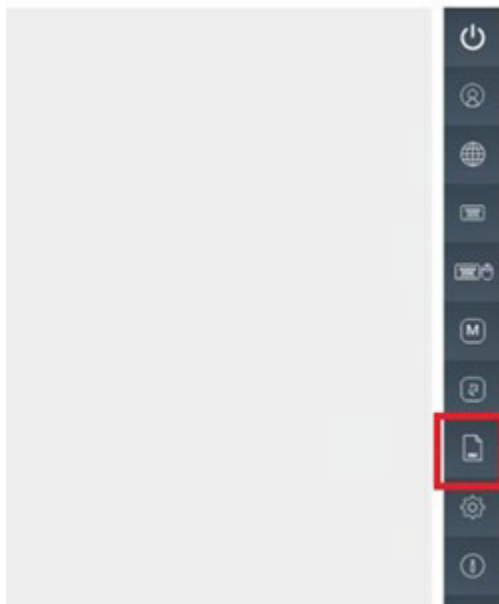


Step 4. Mounting the ISO Image

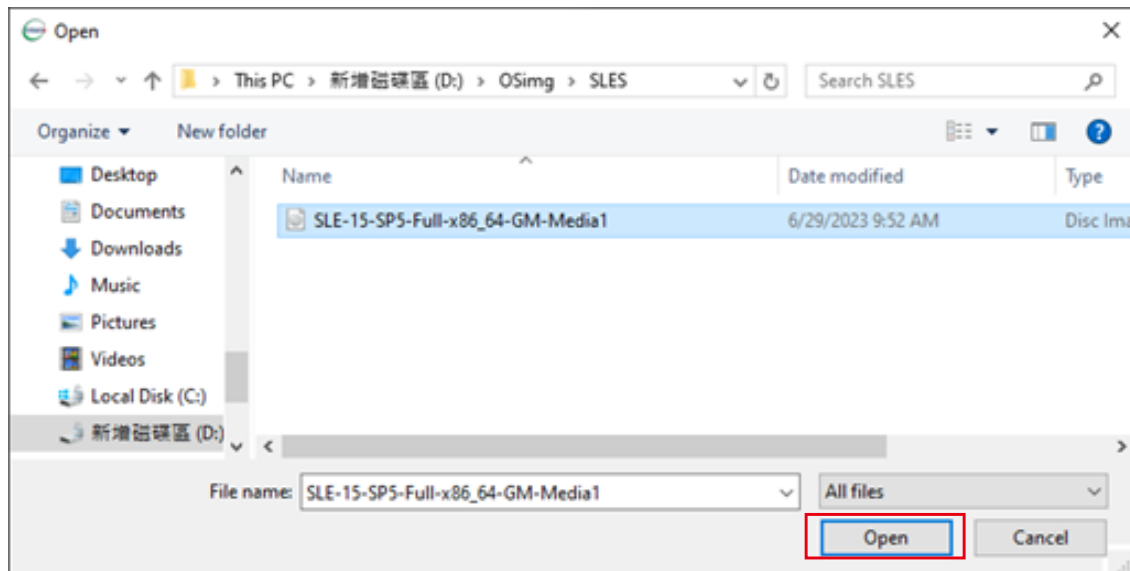
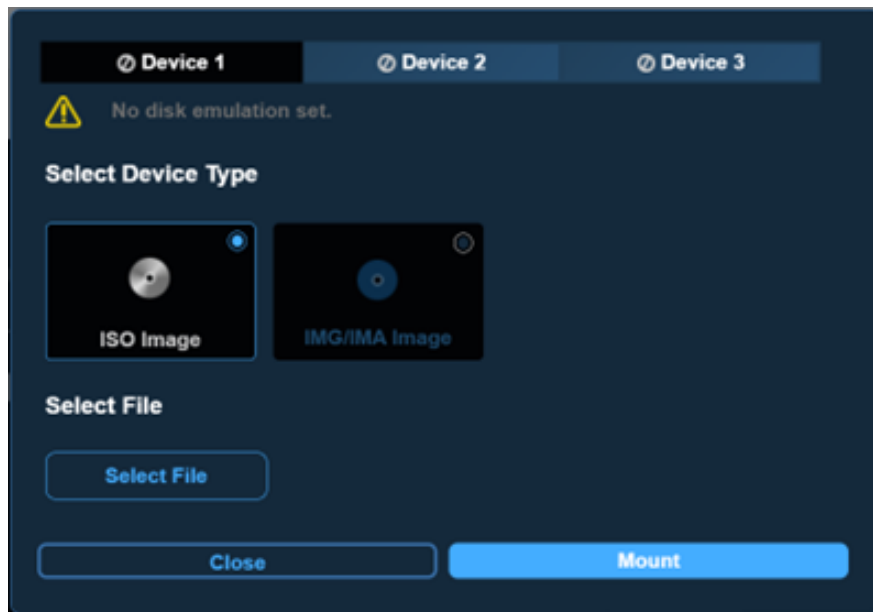
There are two methods to mount ISO images. If the ISO files are stored locally on your drive, you can mount them directly within the remote control browser. Alternatively, if the ISO files are located on a shared server, you can mount them via the Configuration > Virtual Media menu.

Method One: Mounting the ISO Image Using a Local File

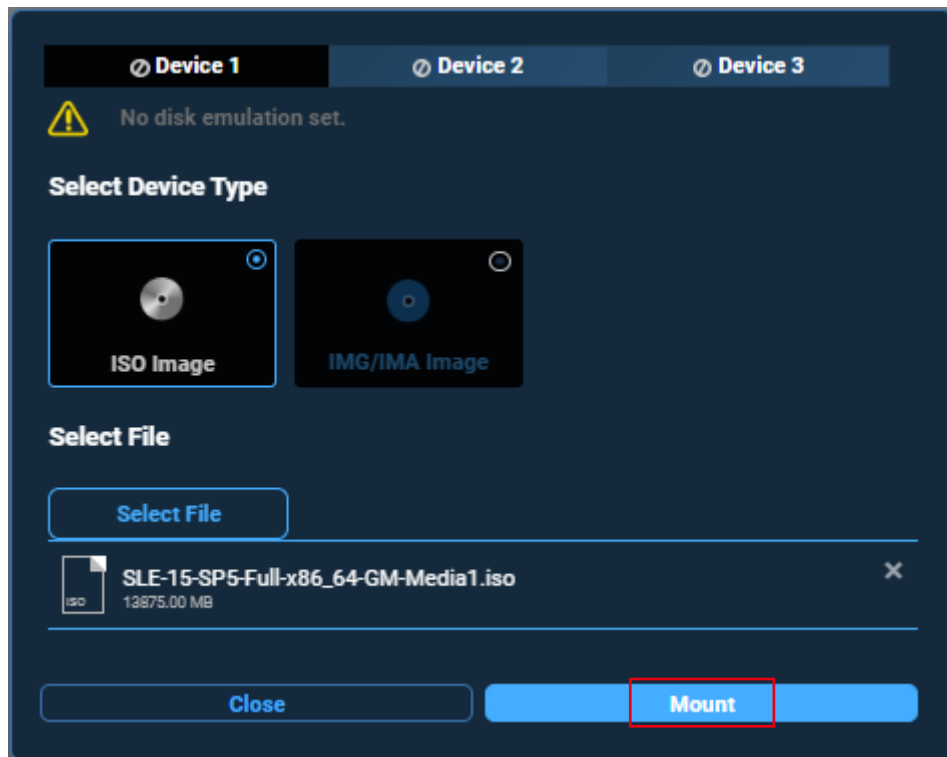
1. In the remote control browser, click the "**Virtual Media**" icon. This action will prompt a dialogue box to appear, enabling you to select the image type and files for mounting.



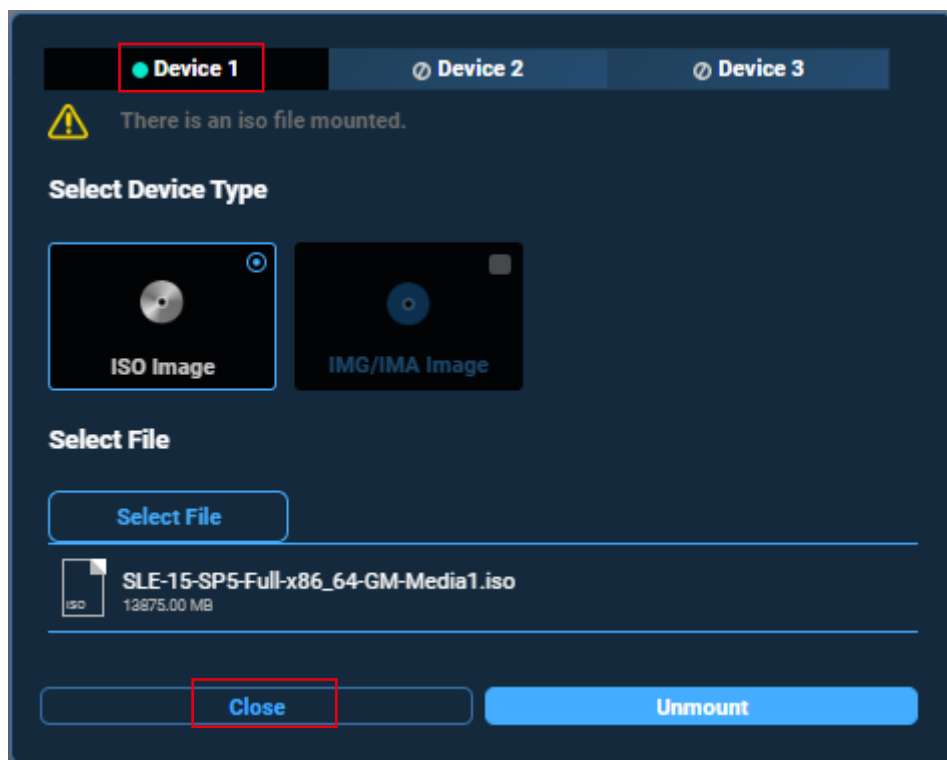
2. Select the **"Choose File"** button to browse and select the SLES ISO image on your local drive for use.



3. Click the **"Mount"** button to attach the chosen ISO image.

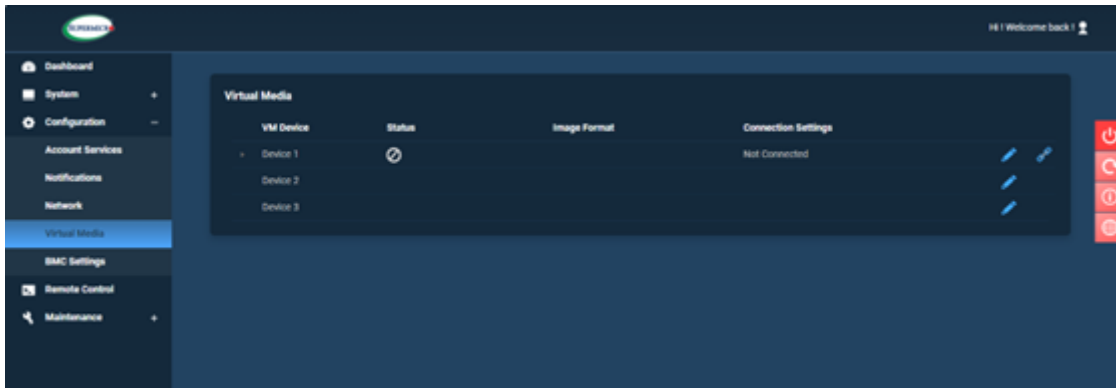


Result: Upon successful mounting of the ISO image, a green indicator will appear in the "Device" tab. Close the dialogue to continue.

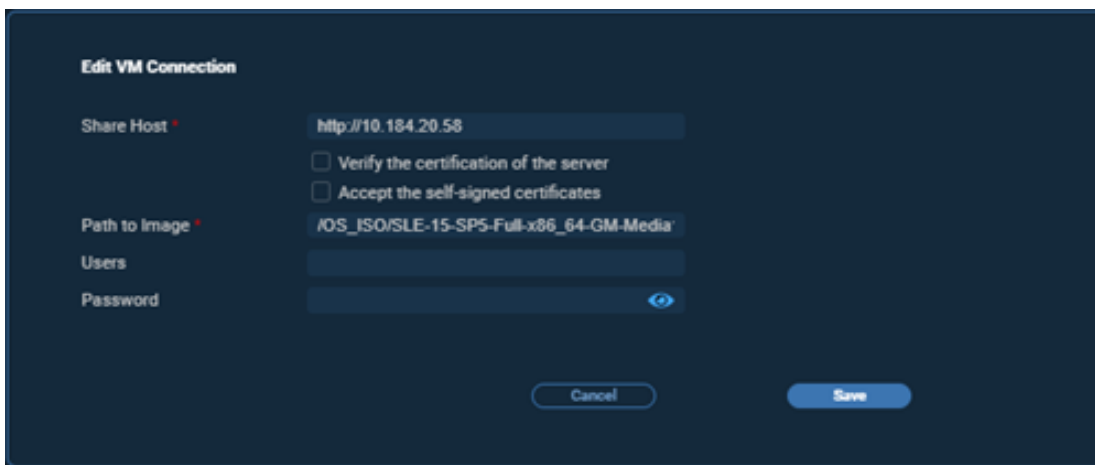
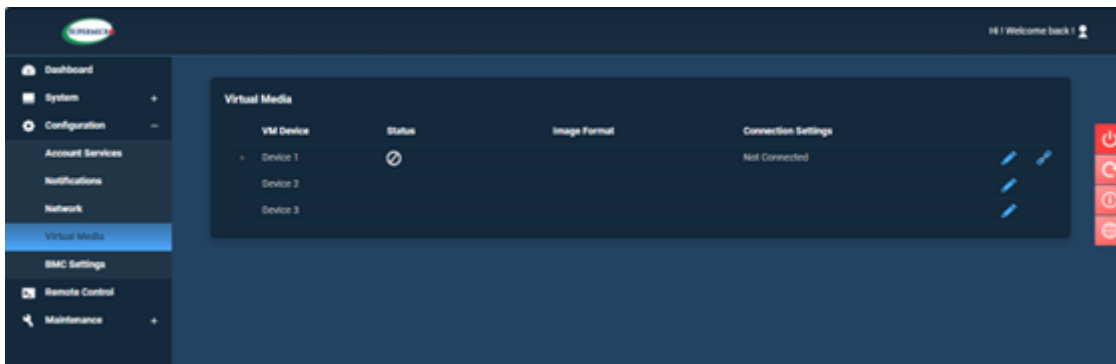


Method Two: Mounting the ISO Image through Shared Server

1. On the BMC dashboard, go to Configuration > Virtual Media. This allows you to attach an ISO image from the server.



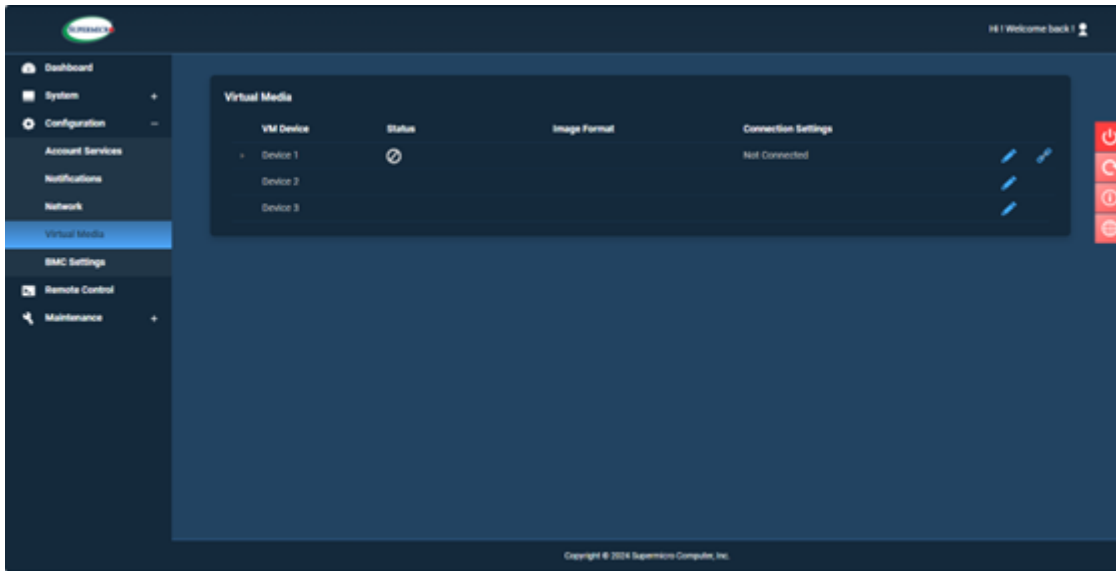
2. Click the **"Edit"** icon to adjust the VM configuration. Enter the server host address and the path to the ISO image. Then, click the **"Save"** to apply the changes.

The screenshot shows a dialog box titled 'Edit VM Connection'. It contains the following fields and options:

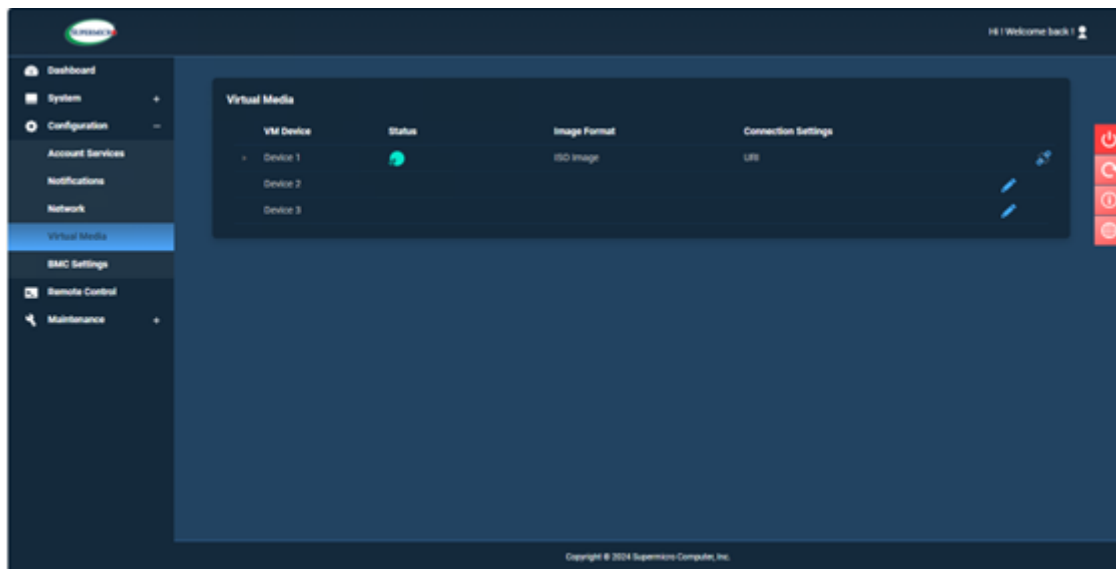
- Share Host ***: A text input field containing 'http://10.184.20.58'.
- Verify the certification of the server
- Accept the self-signed certificates
- Path to Image ***: A text input field containing '/OS_ISO/SLE-15-SP5-Full-x86_64-GM-Media'.
- Users**: An empty text input field.
- Password**: An empty text input field with an eye icon to toggle visibility.

At the bottom of the dialog, there are two buttons: 'Cancel' and 'Save'.

3. Click the **"Connect"** icon to mount the virtual media.



4. The device status will display as green once the VM is successfully configured.



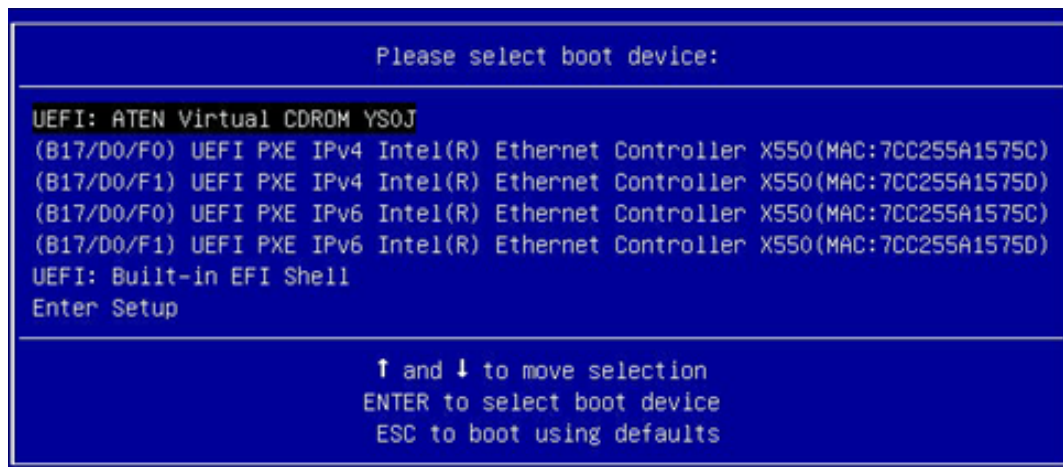
Step 5. Boot from Virtual Media

To boot from the mounted image in virtual media, users must manually select the boot device from the Boot Menu during BIOS POST.

1. Power on the system and wait for the Log screen to display. To access the BIOS setup menu, repeatedly press <F11> until "Invoke Boot Menu" appears at the bottom left corner of the screen.



Subsequently, the Boot Menu is displayed.



2. Select "**UEFI: ATEN Virtual CDROM YSOJ**" as the boot menu. This option will present the ISO image mounted in Virtual Media. Press "**Enter**" to proceed. You will see the GRUB Menu.

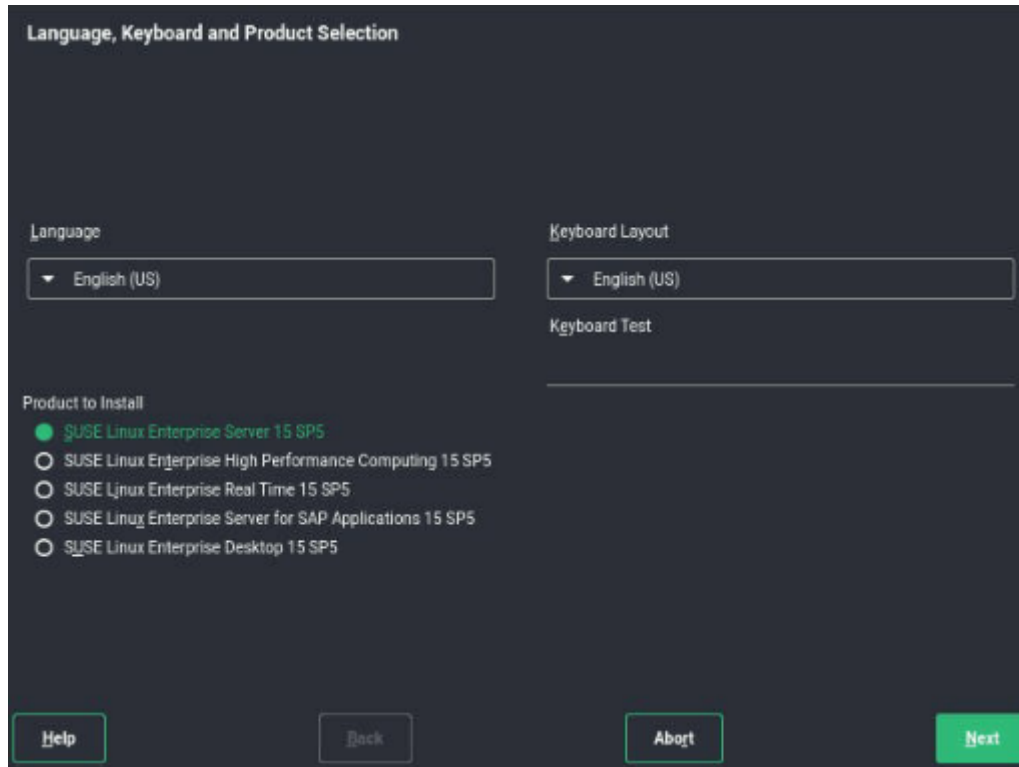


Step 6. Installing SLES 15 SP5 OS

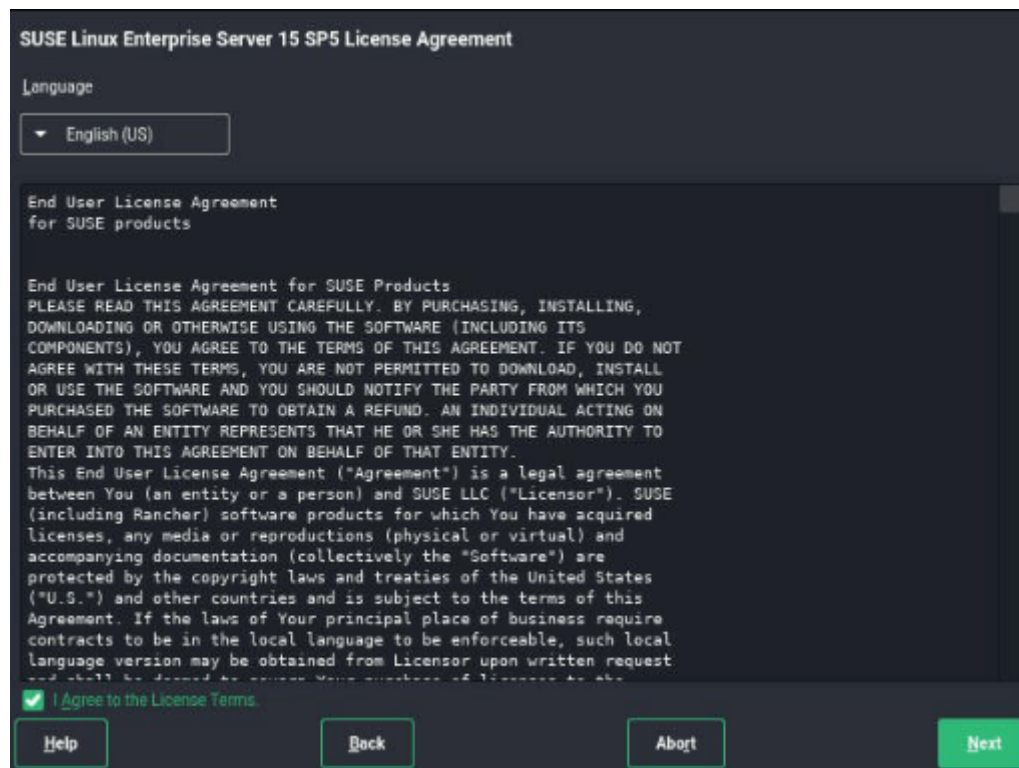
1. Follow the SUSE installer steps to continue the installation. Select "**Installation**" to proceed.



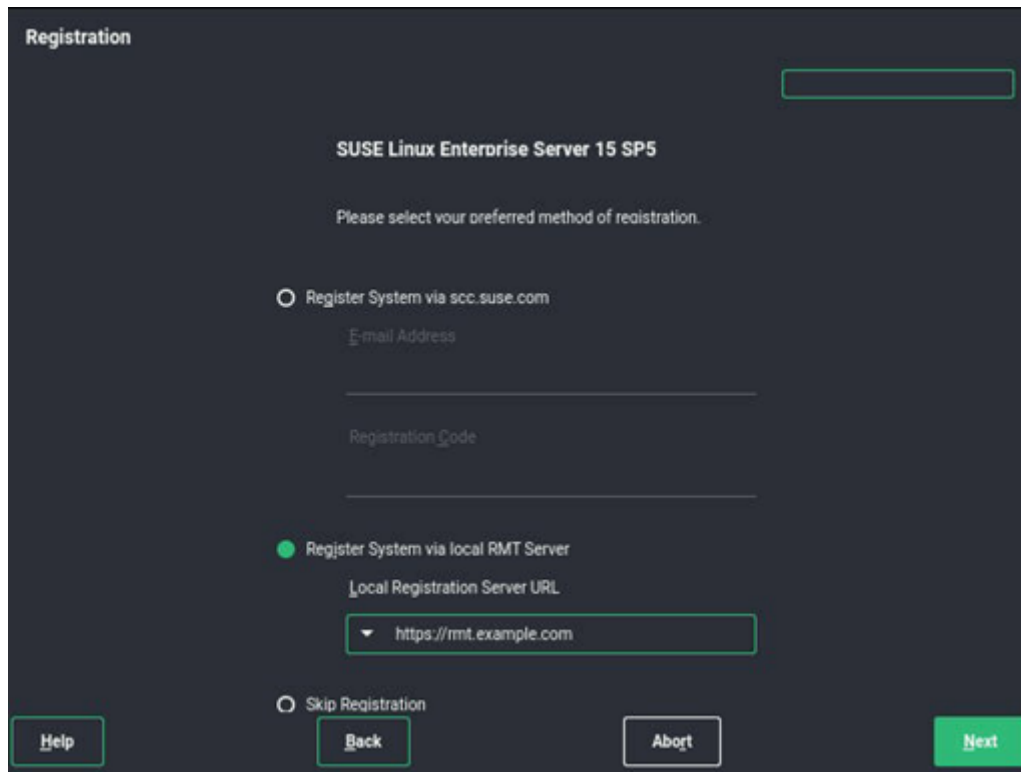
2. Select the **Language**, **Keyboard Layout**, and **Product to Install**.



3. Read and agree the License Agreement to continue.

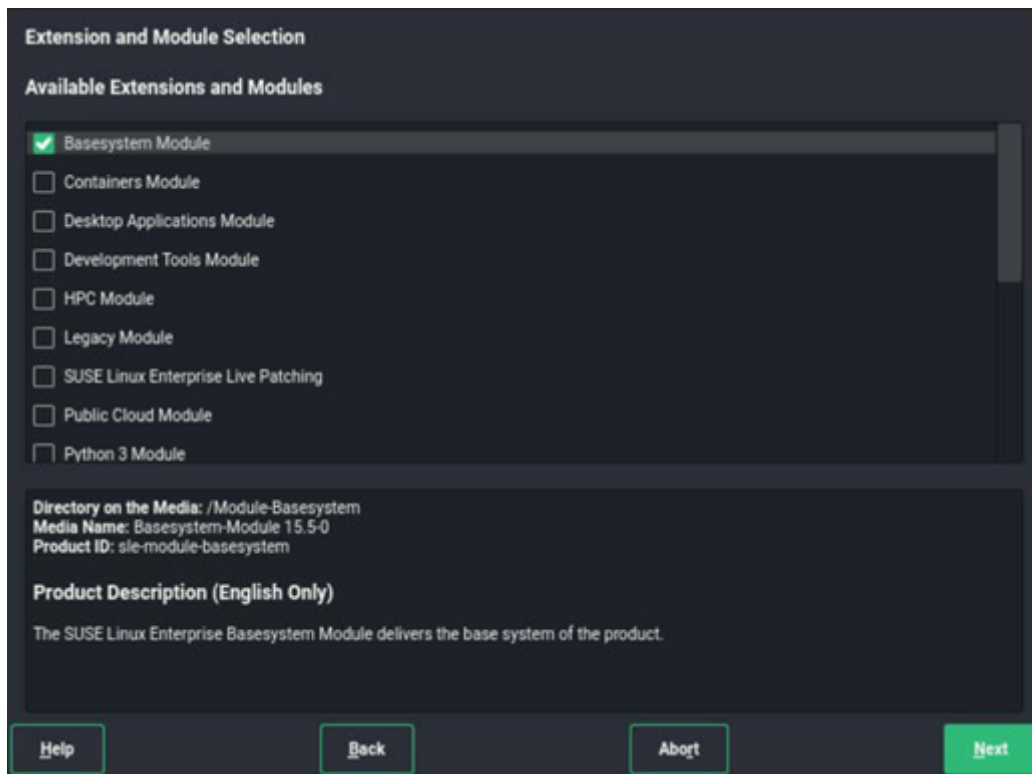


4. Register the system according to the requirements.



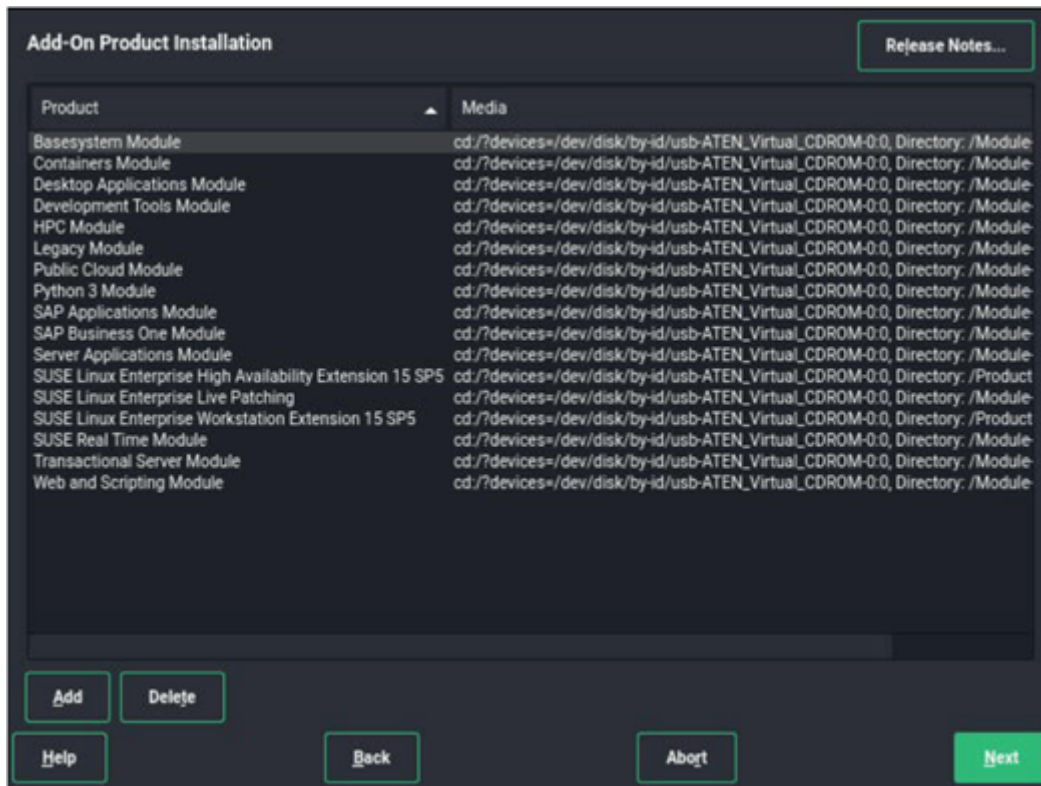
The screenshot shows the 'Registration' window for SUSE Linux Enterprise Server 15 SP5. The window title is 'Registration'. The main heading is 'SUSE Linux Enterprise Server 15 SP5'. Below the heading, it says 'Please select your preferred method of registration.' There are three radio button options: 'Register System via scc.suse.com', 'Register System via local RMT Server', and 'Skip Registration'. The 'Register System via local RMT Server' option is selected. Under this option, there is a text input field for 'Local Registration Server URL' containing 'https://rmt.example.com'. At the bottom, there are four buttons: 'Help', 'Back', 'Abort', and 'Next'.

5. Select the Extensions and Modules for installation.

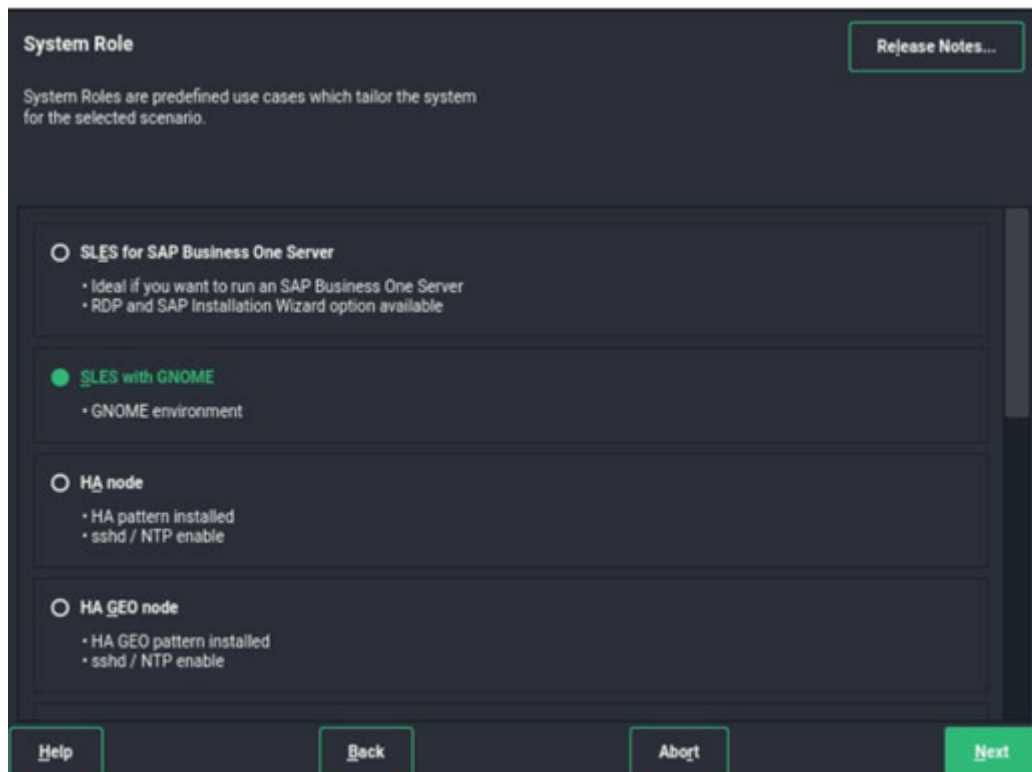


The screenshot shows the 'Extension and Module Selection' window. The title is 'Extension and Module Selection'. Below the title, it says 'Available Extensions and Modules'. There is a list of modules with checkboxes: 'Basesystem Module' (checked), 'Containers Module', 'Desktop Applications Module', 'Development Tools Module', 'HPC Module', 'Legacy Module', 'SUSE Linux Enterprise Live Patching', 'Public Cloud Module', and 'Python 3 Module'. Below the list, there is a section for 'Directory on the Media: /Module-Basesystem', 'Media Name: Basesystem-Module 15.5-0', and 'Product ID: sle-module-basesystem'. Below that, there is a section for 'Product Description (English Only)' with the text 'The SUSE Linux Enterprise Basesystem Module delivers the base system of the product.' At the bottom, there are four buttons: 'Help', 'Back', 'Abort', and 'Next'.

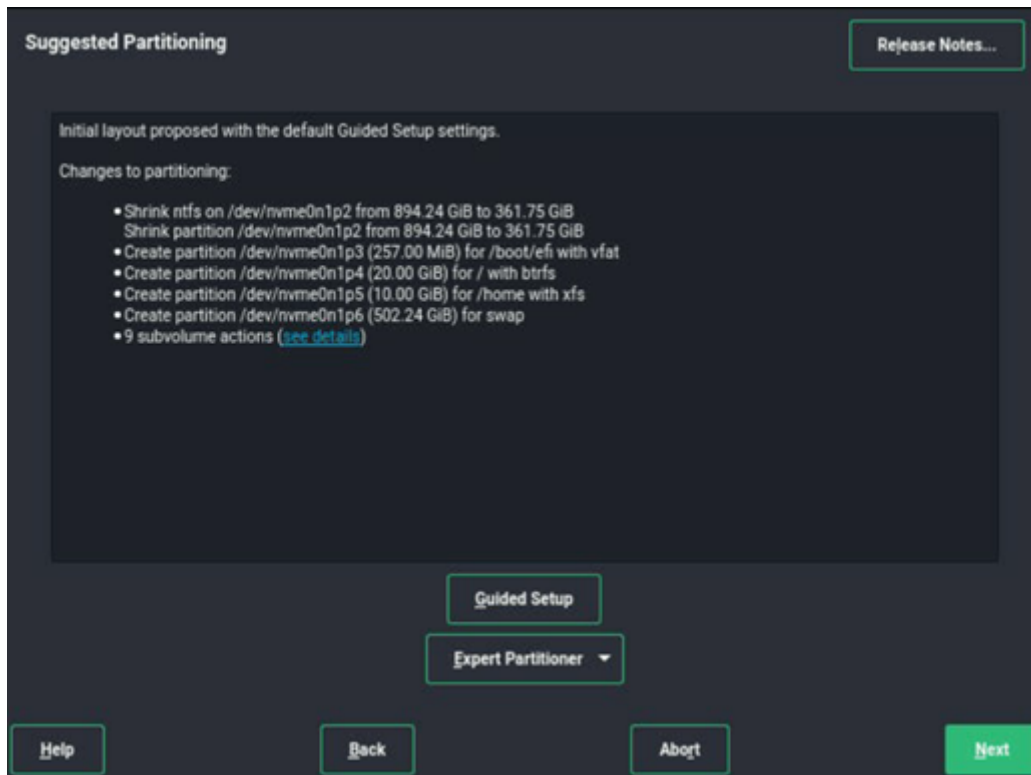
6. Confirm the media sources for the Add-On Product.



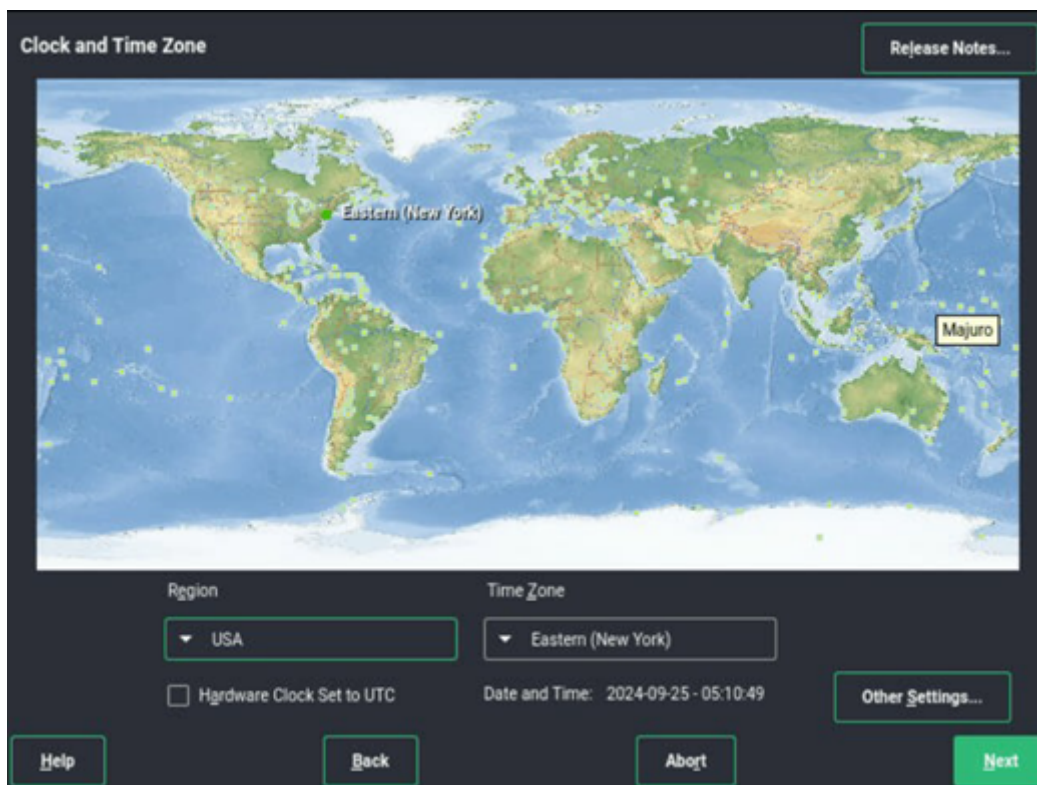
7. Select the System Role.



8. Define the partitions.



9. Choose the time zone.



10. Create a new user.

Local User Release Notes...

Create New User

User's Full Name

Username

Password

Confirm Password

Use this password for system administrator

Automatic Login

Skip User Creation

Help Back Abort Next

11. Set the password for the system administrator root.

Authentication for the System Administrator "root" Release Notes...

Do not forget what you enter here.

Password for root User

Confirm Password

Test Keyboard Layout

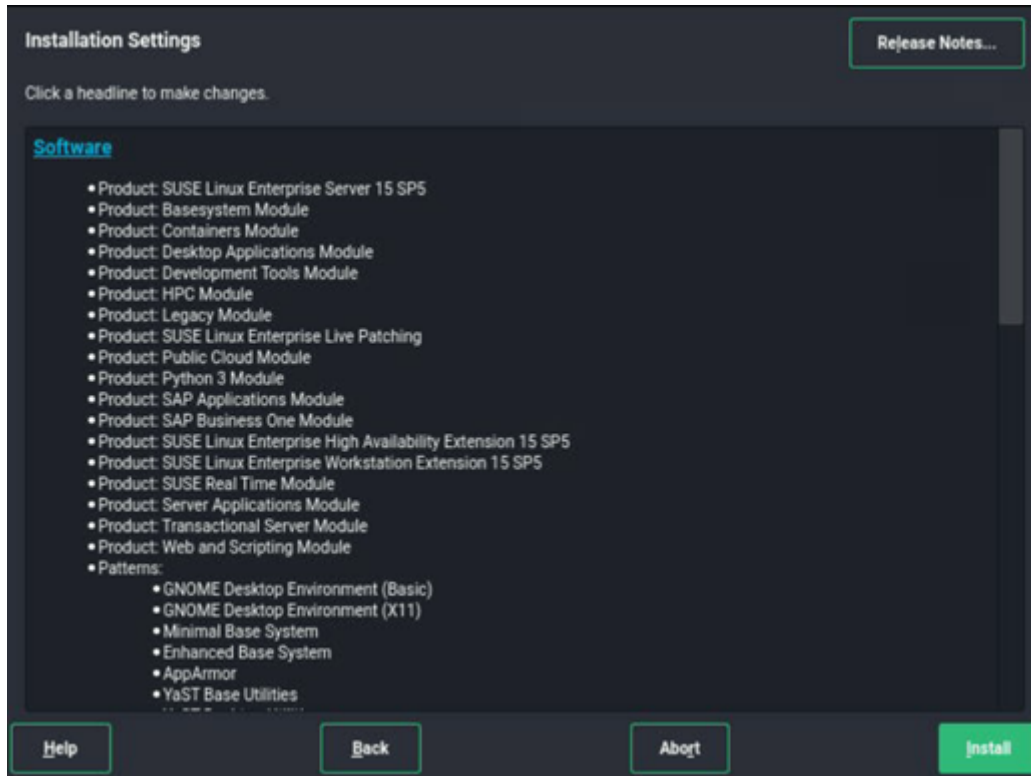
Import Public SSH Key

Virtual CDROM (/dev/sr0) Refresh

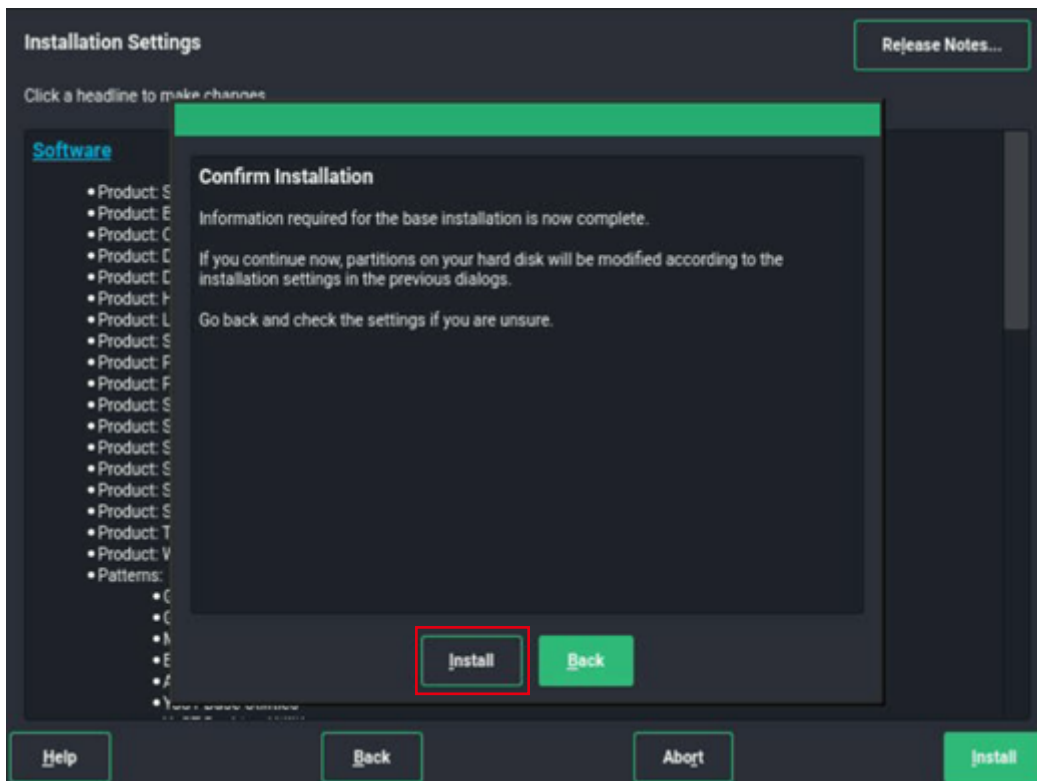
Browse...

Help Back Abort Next

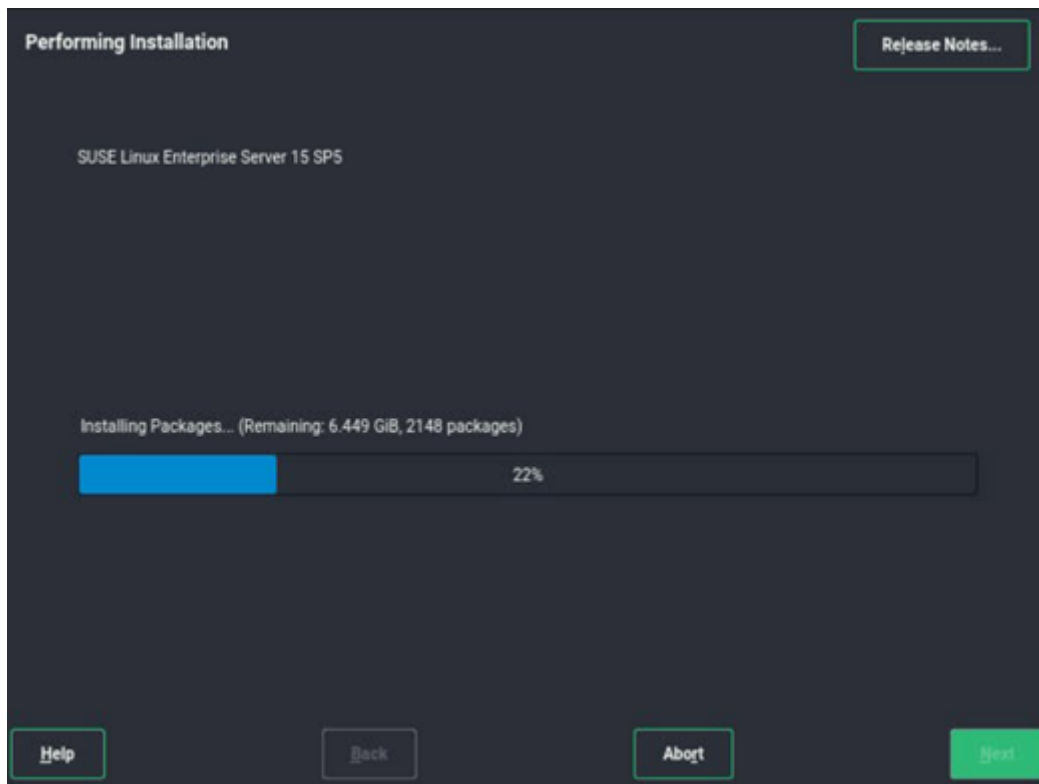
12. Confirm the installation settings before starting the installation.



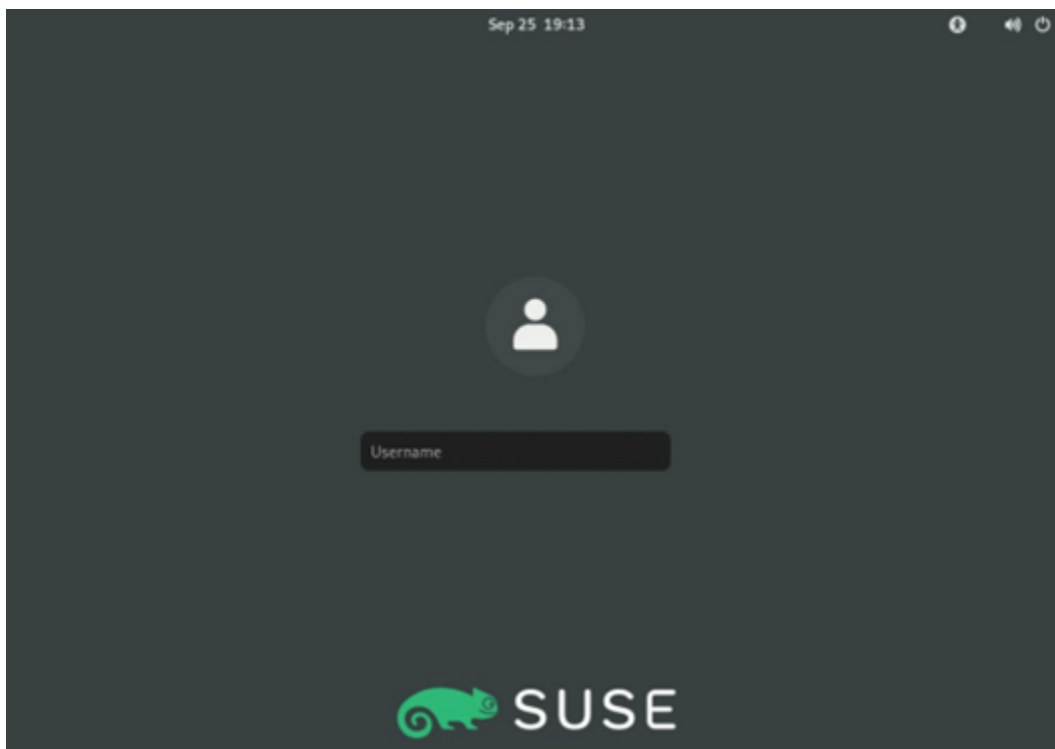
13. Press "Install" to begin the installation.



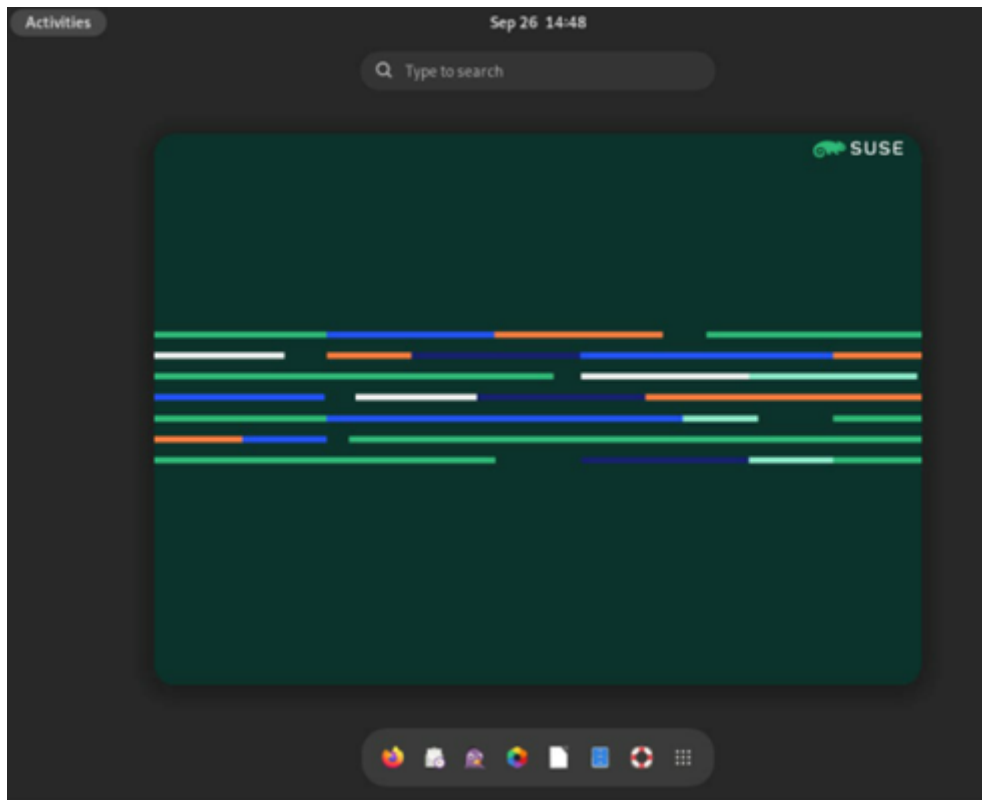
14. The Installation begins.



15. After the installation is complete, the system will automatically reboot until the user login page appears. Enter your user password to log in.



Result: You have successfully logged in and can now start using this system.



A.4 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 or IPMI. SuperDoctor 5 Management Server monitors HTTP, FTP, and SMTP services to optimize the efficiency of your operation.

SuperDoctor® Manual and Resources



Figure 5-1. SuperDoctor 5 Interface Display Screen (Health Information)

A.5 IPMI

The H13QSH supports the Intelligent Platform Management Interface (IPMI). IPMI is used to provide remote access, monitoring and management. There are several BIOS settings that are related to IPMI.

Supermicro ships standard products with a unique password for the BMC ADMIN user. This password can be found on a label on the motherboard.

For general documentation and information on IPMI, please visit our website at:

<http://www.supermicro.com/products/nfo/IPMI.cfm>.

Appendix B

Standardized Warning Statements

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

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

These warnings may also be found on our website at http://www.supermicro.com/about/policies/safety_information.cfm.

B.1 Battery Handling



CAUTION: There is risk of explosion if the battery is replaced by an incorrect type. Replace the battery only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions

電池の取り扱い

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

警告

如果更換的電池類型不正確，則存在爆炸危險。請只使用同類電池或制造商推薦的功能相當的電池更換原有電池。請按製造商的說明處理廢舊電池。

警告

如果更換的電池類型不正確，則有爆炸危險。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

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

ATTENTION

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

ADVERTENCIA

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

אזהרה!

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

هناك خطر الانفجار إذا تم استبدال البطارية بنوع غير صحيح.

استبدال البطارية

فقط بنفس النوع أو ما يعادلها مما أوصت به الشركة المصنعة
جخلص من البطاريات المسحمة وفقاً لتعليمات الشركة الصانعة

경고!

배터리를 잘못된 종류로 교체하면 폭발의 위험이 있습니다. 기존 배터리와 동일하거나 제조사에서 권장하는 동등한 종류의 배터리로만 교체해야 합니다. 제조사의 안내에 따라 사용된 배터리를 처리하여 주십시오.

WAARSCHUWING

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

B.2 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.

تركيب المعدات الكهربائية يجب أن يمثل للقوايه المحلية والسطية المتعلقة
بالكهرباء

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.