BMC

Baseboard Management Controller
Designed for the X14 and H14 Series

USER'S MANUAL

Revision 1.1

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

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

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

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

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

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

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

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

Manual Revision 1.1

Release Date: December 22, 2025

Preface

About This Manual

This manual is written for system integrators, IT technicians, and knowledgeable end users who intend to configure the IPMI settings supported by the ASPEED AST2600 Baseboard Management Controller embedded in Supermicro® motherboards. It provides detailed information on how to configure the BMC settings supported by the AST2600 controller

User's Guide Organization

Chapter 1 provides an overview of the ASPEED AST2600 controller. It also introduces the features and functionalities of BMC.

Chapter 2 provides detailed instructions on how to configure the BMC settings supported by the AST2600 controller.

Chapter 3 provides the answers to frequently asked questions.

An Important Note to the User

For documents concerning utility support, such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, BIOS, RSD/SSC, TAS, and IPMIView, refer to our website at https://www.supermicro.com/en/solutions/management-software/bmc-resources for details.

The graphics shown in this user's guide were based on the latest information available at the time of publishing of this guide. The BMC screens shown on your computer may or may not look exactly like the screen shown in this user's guide.

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.

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

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

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

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

Important Links

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

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

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

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

Chapter 1

Introduction

1.1 Introduction to the BMC Platform

The Baseboard Management Controller (BMC) provides remote access to multiple users at different locations for networking. It also allows a system administrator to monitor system health and manage computer events remotely.

BMC operates independently from the operating system. When used with an IPMI Management utility installed on the motherboard, the ASPEED AST2600 BMC will connect to other onboard components, providing a remote network interface through serial links. With the AST2600 controller and the BMC firmware built in, the Supermicro motherboard allows you to access, monitor, diagnose, and manage a remote server through Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

1.2 Overview of the ASPEED AST2600 BMC

The ASPEED AST2600 BMC is designed to interface with the host system through PCI Express connections to communicate with the graphics core for the X14 and H14 series motherboards. It supports a 64-bit 2D Graphics Accelerator with 32-bit memory and 16-bit I/O space.

Additionally, AST2600 supports USB 1.1 and 2.0 for remote KVM emulation, provides LPC interface support to control Super IO functions, and Keyboard/Video/Mouse Redirection (KVMR). The BMC is connected to the network through an external Ethernet PHY module or a shared NCSI connection.

AST2600 DDR5 Memory Interface

The ASPEED AST2600 Baseboard Management Controller (BMC) is designed to interface with the host system using PC.

1.3 Supermicro BMC Features

- Remote KVM (graphics) console
- Virtual Media and ISO images
- Remote server power control
- Remote Serial over LAN (text console)
- Event Log support
- Automatic Notification and Alerts (SNMP and email)
- Hardware Monitoring
- Overall health displayed on the main page
- Out-of-band management through shared or dedicated LAN
- Option to change LAN connection interface at Runtime
- VLAN
- RMCP and RMCP+ protocols supported
- SMASH/CLP
- Secure command line interface (SSH) and Telnet
- RADIUS authentication support
- Secure browser interface (Secure Socket Layer — SSL Support)
- Transport Layer Security (TLS) v1.2 and v1.3 support
- Lightweight Directory Access Protocol (LDAP) supported
- System Lockdown
- Backup and restore the configuration file
- Factory defaults from web support
- Video quality settings
- Session video recording and playback

- Server data/information
- Preview of the remote screen on the main page
- Update Firmware through the browser and OS
- OS-indentation
- KCS Privilege Control
- Unique pre-programmed password
- Redfish

1.4 Software Licenses Available

Software license is required for respective features using different interfaces such as Web/ CLI/Redfish API.

Warning: Changing MAC addresses will wipe out Software License Keys.

- SFT-OOB-LIC: Basic Out of Band Management

  It covers features such as UEFI BIOS/BMC firmware update and configuration, mounting ISO images, asset information, and many more.

- SFT-DCMS-Single: System Management Suite

  It covers the above two license SKUs as well as all enterprise features, such as RAID Management, Advanced Redfish APIs, NIC FW management, and many more.

Refer to the following comparison chart for more information.

(*) Available through Redfish APIs.

(**) Additional SKU is required.

Features	Standard Package	SFT-OOB-LIC	SFT-DCMS-Single
IPMI 2.0	✓	✓	✓
DCMI 1.5	✓	✓	✓
BMC Web GUI	✓	✓	✓
SMASH-CLP	✓	✓	✓
Serial Redirection (COM2/ SOL)	✓	✓	✓
Redfish APIs (Basic Redfish APIs (Redfish 1.0) support-ed with OOB license)	✓	✓	✓
Shared NIC (LOM, LAN1 with automatic failover)	✓	✓	✓
Dedicated NIC	✓	✓	✓
VLAN tagging	✓	✓	✓
IPv4	✓	✓	✓
IPv6	✓	✓	✓

DHCP	✓	✓	✓
Dynamic DNS	✓	✓	✓
KCS	✓	✓	✓
LAN over USB	✓	✓	✓
Unique pre-programmed default password	✓	✓	✓
Signed BMC/BIOS images	✓	✓	✓
Host secure communication (LAN over USB)	✓	✓	✓
User account management and Role-based authority (User, Operator, Administrator)	✓	✓	✓
SSL Redirection	✓	✓	✓
SSL Encryption (HTTPS)	✓	✓	✓
IP Access Control	✓	✓	✓
SNMPv3.0	✓	✓	✓
AD / LDAP		✓	✓
RADIUS	✓	✓	✓
PK authentication (for SSH)	✓	✓	✓
KCS Control	✓	✓	✓
Port Configuration	✓	✓	✓
UEFI Secure Boot			✓
System Lock down			✓
TEE-OS	✓	✓	✓
BIOS/BMC automatic recovery (ROT)			✓
Disk secure erase of internal storage devices (For Broadcom controller connected drives)			✓
Power control	✓	✓	✓
Boot configuration	✓	✓	✓
Serial-over-LAN	✓	✓	✓
Virtual Media	✓	✓	✓
Virtual Console	✓	✓	✓
HTML5 access to Virtual Console	✓	✓	✓
HTML5 VM			✓
Virtual Console collaboration (three users)	✓	✓	✓
Remote Keyboard Operation	✓	✓	✓
Temperature monitoring	✓	✓	✓

Real-time power reading	✓	✓	✓
Power thresholds and alerts	✓	✓	✓
Real-time power graphing	✓	✓	✓
Historical power values	✓	✓	✓
Power Capping (Through SPM)			✓
Out-of-Band System Checks	✓	✓	✓
Predictive failure monitoring (for Broadcom controller only)	✓	✓	✓
SNMPv1, v2, and v3 (traps and gets SNMPv3 MIBs needs DCMS license)	✓	✓	✓
Email Alerting	✓	✓	✓
Fan monitoring	✓	✓	✓
Power Supply monitoring	✓	✓	✓
Memory monitoring	✓	✓	✓
CPU monitoring	✓	✓	✓
RAID monitoring and configuration (Broadcom/Marvell storage controller)			✓
GPU monitoring (NVIDIA GPUs)	✓	✓	✓
NIC monitoring	✓	✓	✓
HDD monitoring (Broadcom/Marvell/NVMe controller)			✓
Remote agent-free out of band FW updates (BIOS, BMC, CPLD, Backplane)	✓	✓	✓
Component FW Update			✓
Inband FW Updates	✓	✓	✓
Local configuration through BIOS setup	✓	✓	✓
System Component Inventory	✓	✓	✓
Auto-Discovery (through SSM web)			✓
Remote OS deployment (through SSM)			✓
BMC/BIOS configurations (Redfish/SSM/SUM)		✓	✓

Remote configuration (Mousemode, Fanmode, Radius, AD, NTP, Chassis intrusion, SNMP, SMTP alerts, Syslog etc.)	✓	✓	✓
CMM Management		✓	✓
FW update policy (through SUM)			✓
TPM Management (through SUM)			✓
HGX2 FPGA, CEC FW Update			✓
Offline Diagnostic	✓	✓	✓
Crash Dump	✓	✓	✓
Health/System Events	✓	✓	✓
Events acknowledgement			✓
Crash screen capture			✓
Crash video capture			✓
Virtual NMI (through SMCIPMITool)	✓	✓	✓
License Management	✓	✓	✓
Post Snooping	✓	✓	✓

1.5 Special Notes for Motherboard and Firmware Support

For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI BIOS, TAS, and IPMIView, refer to our website at https://www.supermicro.com/en/solutions/management-software for details.

Refer to the motherboard product page at https://www.supermicro.com/ to see if the motherboard supports BMC.

Chapter 2

Configuring the BMC Settings

With the ASPEED AST2600 BMC and the BMC firmware built in, Supermicro motherboards allow you to access, monitor, manage, and interface with multiple systems from different remote locations. The necessary firmware for accessing and configuring the BMC settings is available on the Supermicro website at https://www.supermicro.com/support/resources/bios_ipmi.php?type=BMC. This section provides detailed information on how to configure BMC settings.

Note: Some features might not be available if you are using an X14 or H14 motherboard, as a few newer features are not supported by this generation.

2.1 Configuring UEFI BIOS

Before configuring the BMC, follow the instructions to configure the system's UEFI BIOS settings.

Entering and Using the UEFI BIOS

1. During the system bootup, press the <Del> key to enter the UEFI BIOS.
2. To navigate in the UEFI BIOS, use the arrow keys and press <Enter> to select. To go back to previous screens or exit a menu, press <Esc>.

Enabling the COM port for SOL (BMC)

1. Select the *Advanced* tab from the UEFI BIOS Setup menu display.
2. Select *Serial Port Console Redirection*.
3. Highlight and select *Console Redirection* under *COM2/SOL*.
4. Select [Enabled].

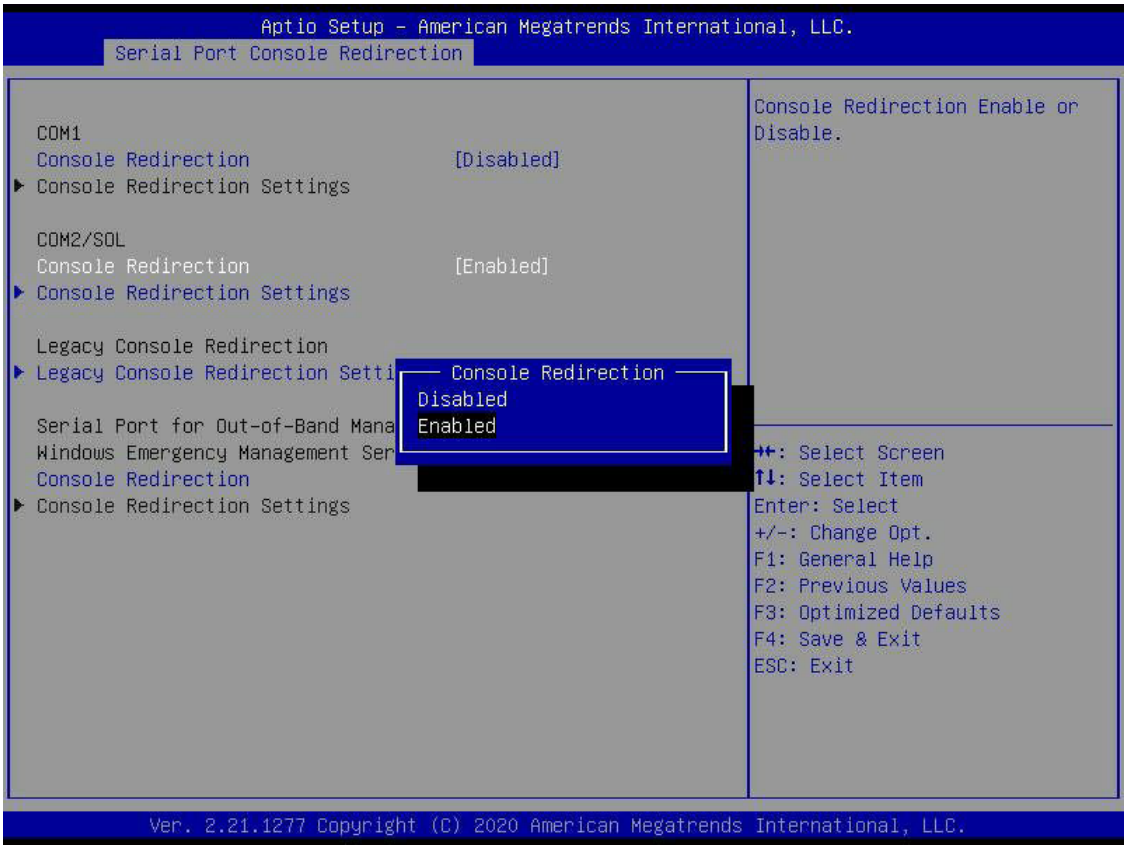


Figure 2-1: Console Redirection Enabled Option Selected

Configuring IP Address Using the UEFI BIOS

1. Select the *Server Management* tab.
2. Select *BMC Network Configuration* and press <Enter>.
3. Highlight and select *Update IPMI LAN Configuration*.
4. Select [Yes].

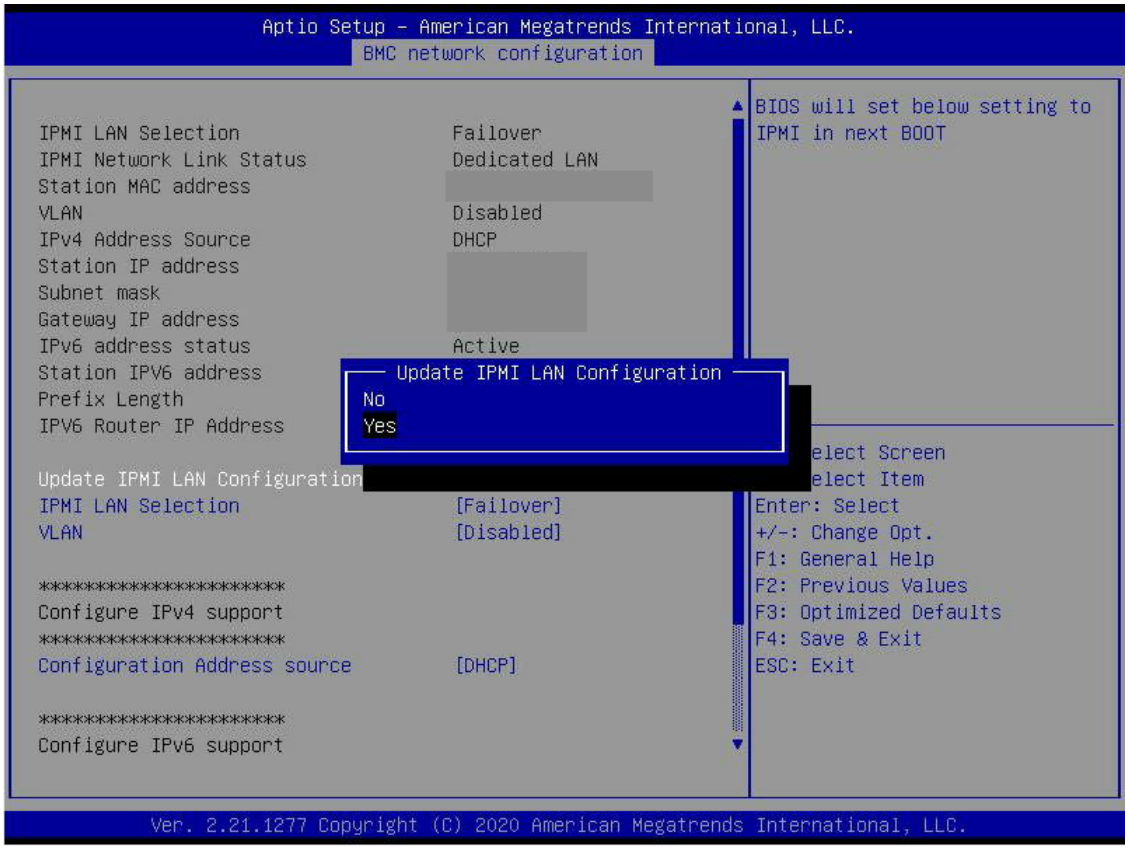


Figure 2-2: Update LAN IPMI LAN Configuration Yes Option Selected

5. Highlight and select *Configuration Address Source*.

6. Select [Static].

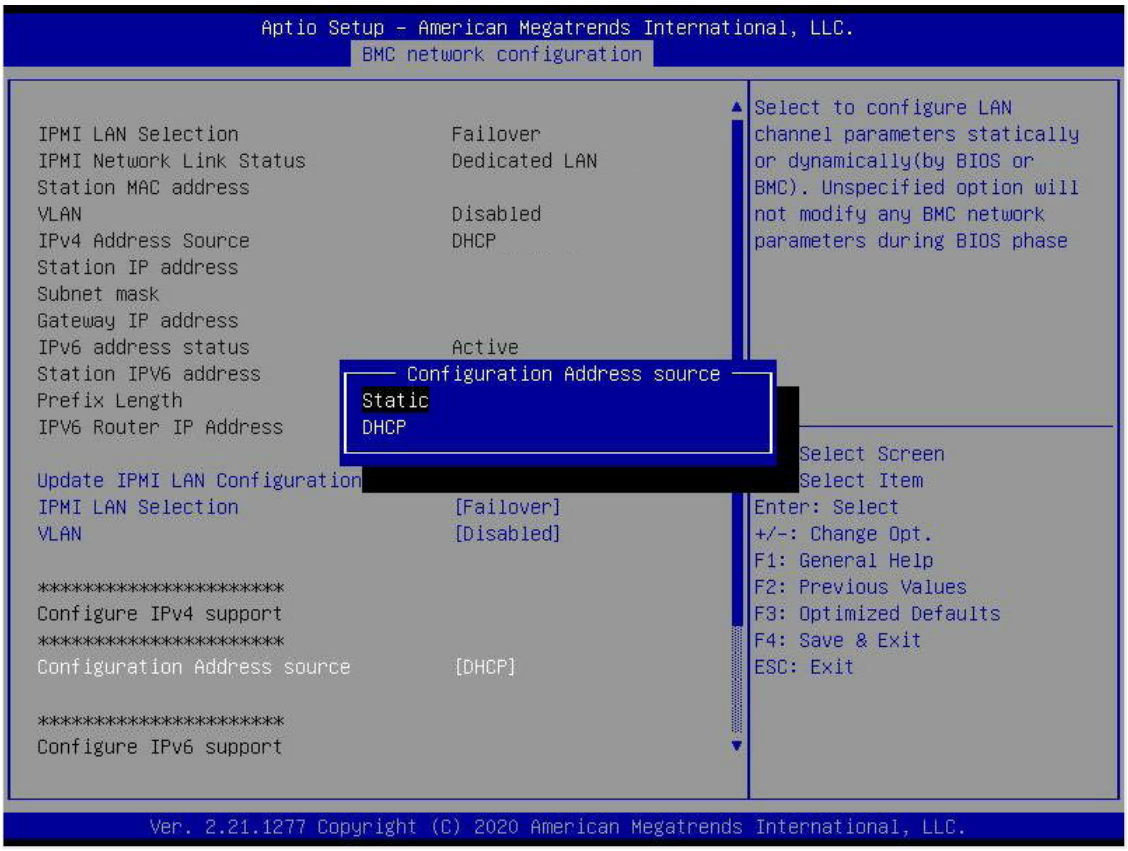


Figure 2-3: Configuration Address Source Static Option Selected

7. Once the Configuration Address Source is set to [Static], the Station IP Address, Subnet Mask, and Gateway IP Address fields will display 0.0.0.0. This indicates that these fields are ready for you to change to new values. Select each of the three options to enter the values.

8. Press <Enter> when finished.

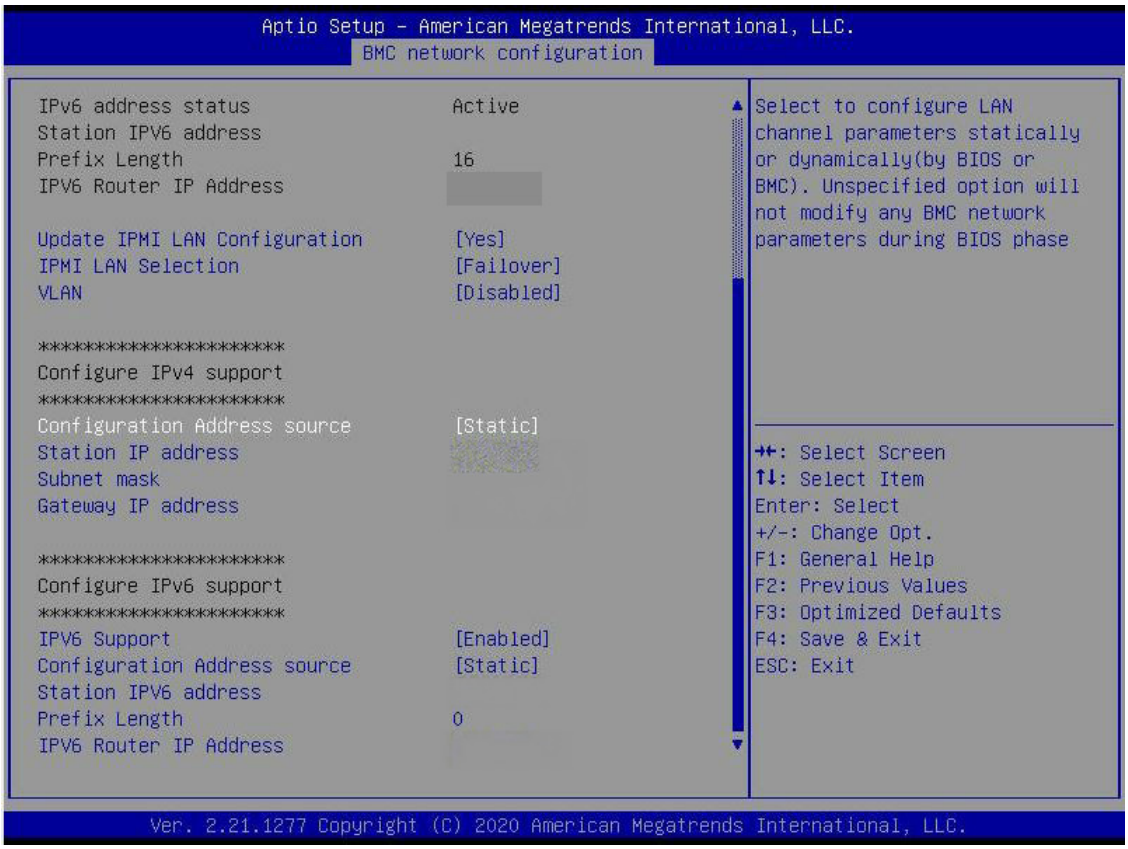


Figure 2-4: BMC Network Configuration Page

Connecting to BMC Using the UEFI BIOS

1. To bring up the BIOS menu, connect one end of an Ethernet Cat 5 cable to the Ethernet port of the laptop or device being used.
2. Plug the other end of the cable into the server's IPMI / SHARED port.
3. Power on the server by pressing the DEL key to enter the BIOS menu.
4. In the BIOS menu, follow the instructions to configure the Network settings for Static IP as well as assign an IP Address (i.e., 192.168.0.4) and a subnet.
5. Navigate to *Server Management*.
6. Select *BMC Network Configuration*.

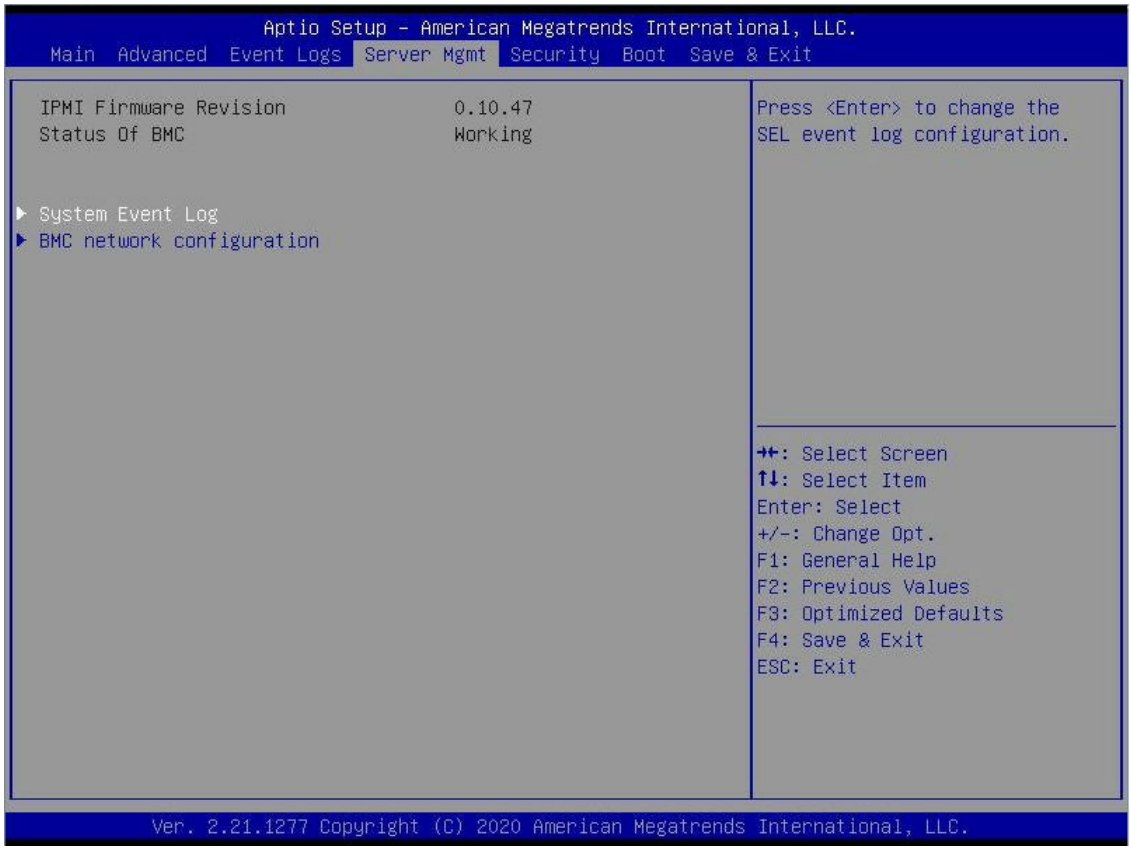


Figure 2-5: Server Management

7. Select *Update IPMI LAN Configuration*.

8. Select [Yes].

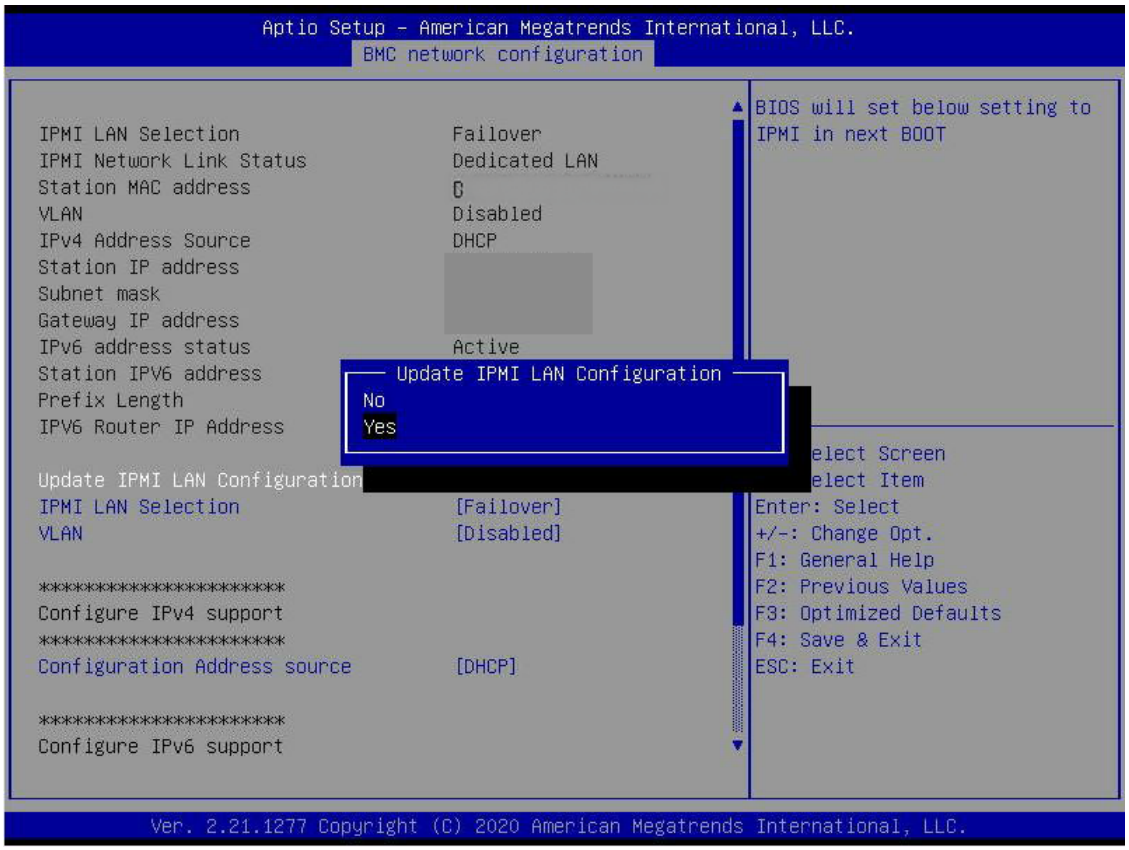


Figure 2-6: Update IPMI LAN Configuration

9. Navigate to *IPMI LAN Selection*, and you will see three options.
10. Select [Shared].

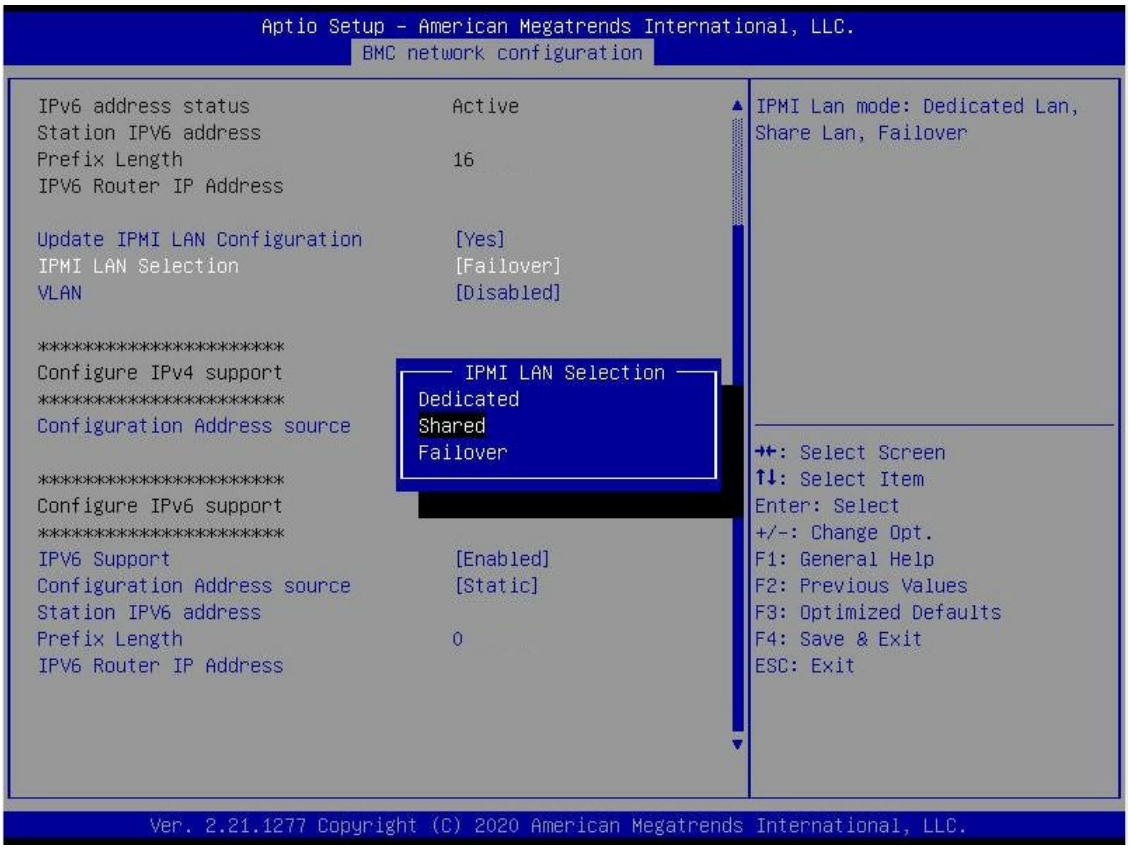


Figure 2-7: IPMI LAN Selection Shared Option Selected

11. Navigate to *Configuration Address Source*.
12. Select [Static].
13. You can assign an IP address (such as 192.168.0.4) and subnet.

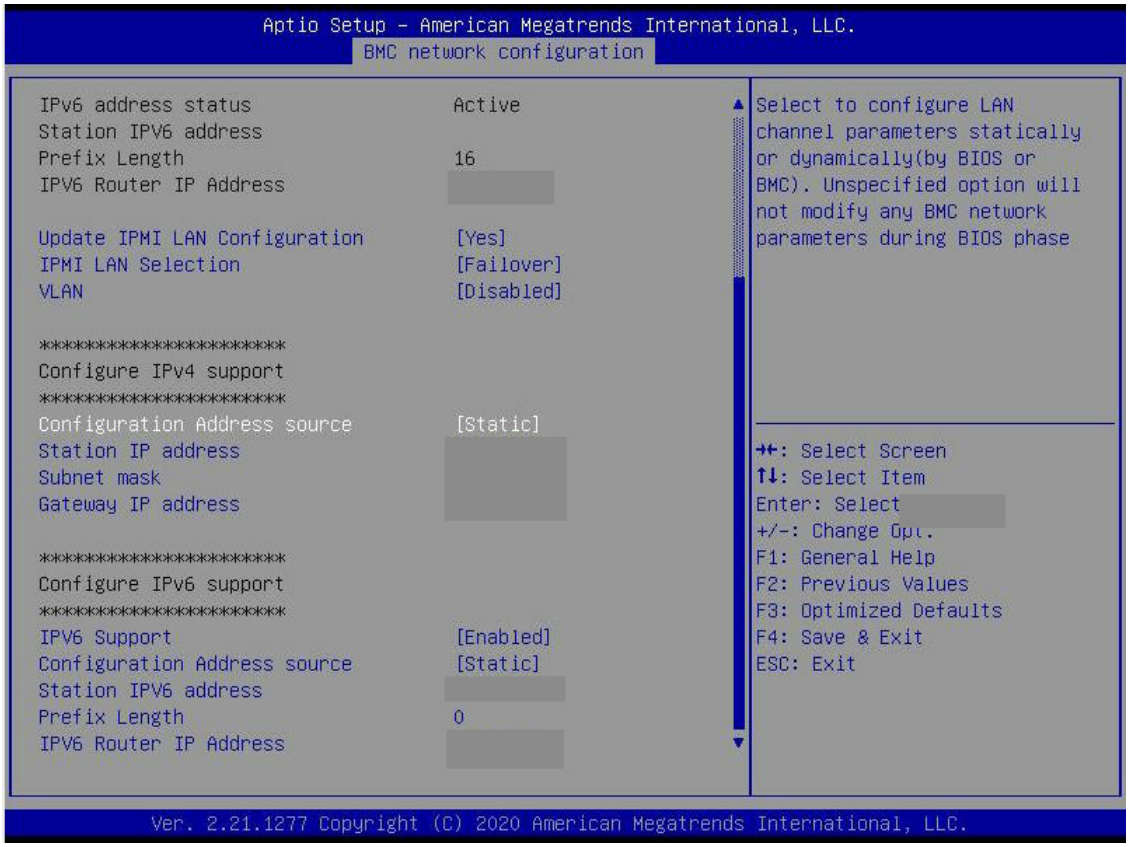


Figure 2-8: Configuration Address Source Selected

When your computer and the BMC are on the same subnet, you should be able to communicate with the static IP. To establish the connection, take the following steps:

1. Open a Windows/Laptop terminal on your computer.
2. Ping the IPMI IP (e.g.,192.168.0.4) and make sure that it is pingable.
3. If it is pingable, open a web browser on the laptop.
4. Enter the IP in the URL bar, and the login screen will appear.

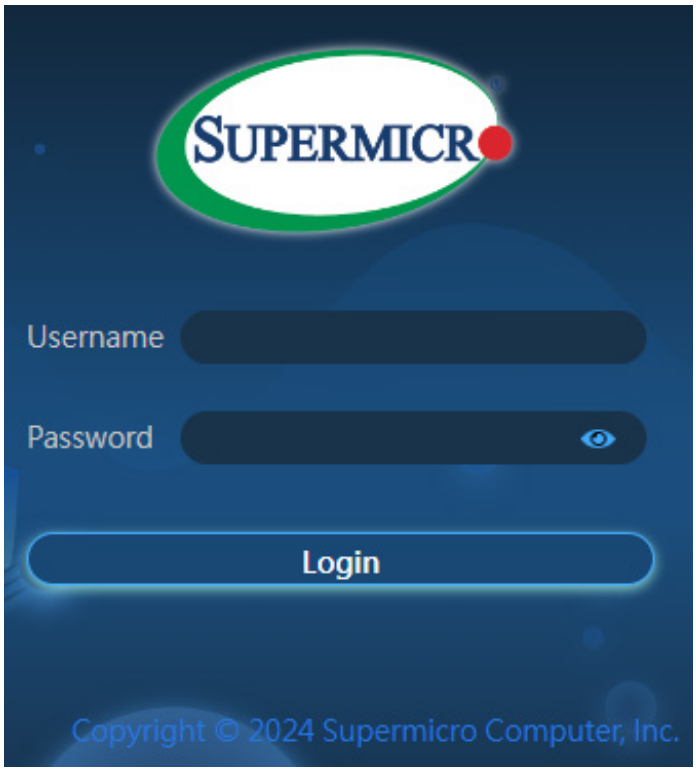


Figure 2-9: Login Screen

5. Enter the username (the default is ADMIN) and a BMC unique password. Refer to Appendix D on how to retrieve the BMC unique password.

6. After logging in, navigate to <Network> under <Configuration>. You can then see all the IPv4 and IPv6 information to configure.

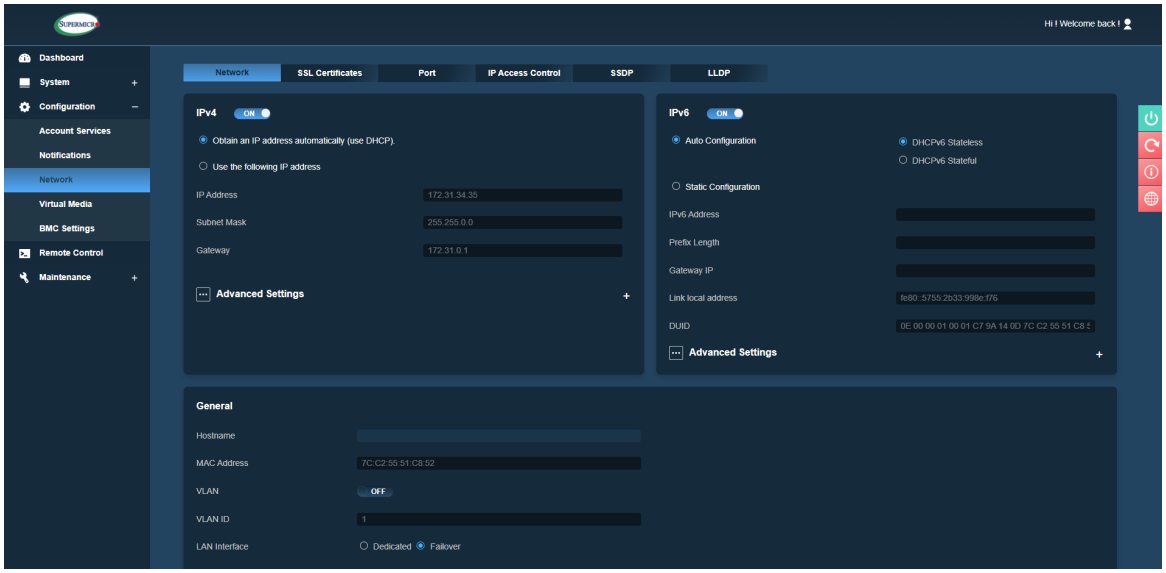


Figure 2-10: Network Page

2.2 Connecting to the Remote Server

Using the Browser to Connect to the Remote Server

1. Connect a LAN cable to the onboard LAN1 port or the BMC LAN port.
2. Choose a computer that is connected to the same network and open the browser.
3. For each server that you want to connect to, enter the IP address in the address bar of the browser.
4. Once the connection is made, the Login screen will display as shown on the next page.

2.3 Accessing the Remote Server Using the Browser

To Log In to the Remote Console

Log in with your local BMC user credentials or as a user from Active Directory, LDAP, or RADIUS. You will be able to navigate pages based on your assigned user privilege. To view the hidden password, click on the eye icon. Once connected to the remote server through a browser, the following BMC login screen will display:

Note 1: A (*) symbol indicates the feature is an optional field.

Note 2: Keep the page zoom level at 100% to avoid any overlapping icons or tabs.

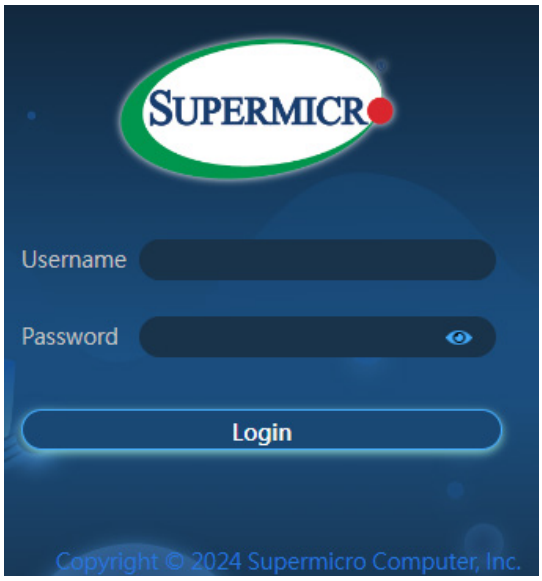


Figure 2-11: Login Screen

1. Enter the username in the *Username* box.
2. Enter the password in the *Password* box and click on <Login>.
3. The home page will display as shown on the next page.

Note 1: To use the IPMIView utility for Console Redirection, refer to the IPMIView User's Guide for instructions.

Note 2: The *Administrator* account cannot be deleted or disabled.

Note 3: In the event that BMC encounters technical issues, you will receive a prompt to reset BMC and log in again.

2.4 BMC Dashboard

The BMC Dashboard provides an overview of the System, Host Information, Power Consumption, and System Health. You can also access quick links to System, Storage (if a storage component is connected), UID Control, Firmware Update and Sensor Readings, Power Consumption, Remote Console Preview, and Recent Logs. If storage components are connected, then you will also be able to access Storage from here.

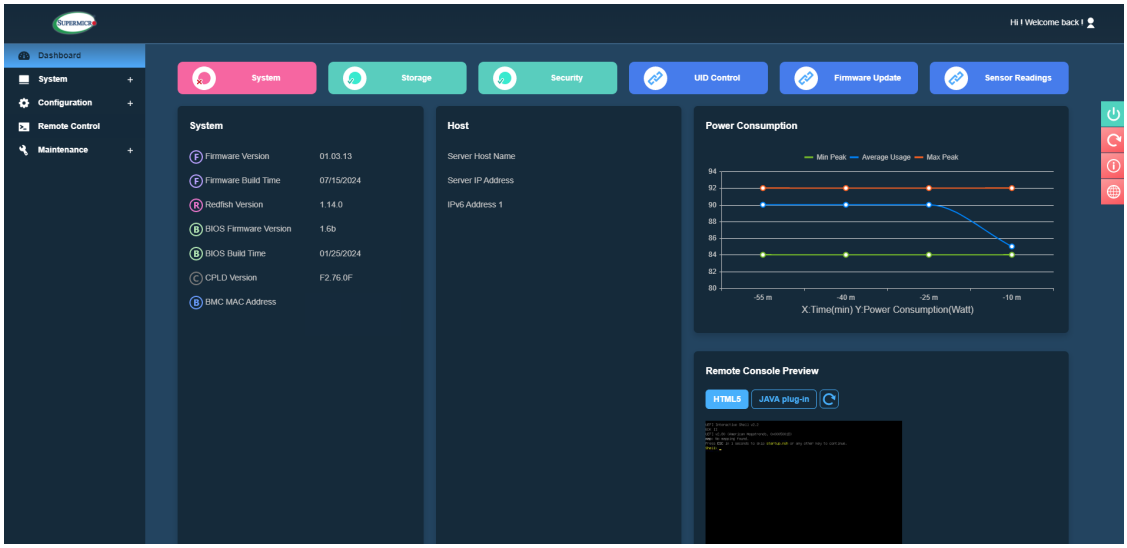


Figure 2-12: Dashboard Page

In the upper right-hand corner, hover over the icon to view user status.

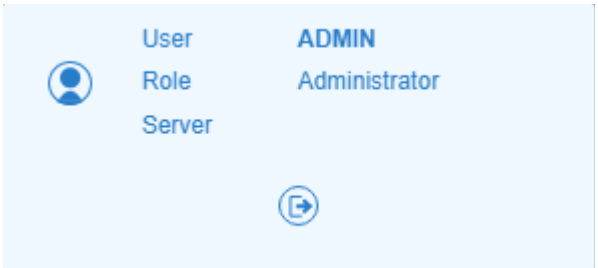


Figure 2-13: User Status Window

Information includes the following:

- User
- Role
- Server
- Logout

The following WebGUIs indicate different purposes:

: Power Control

: Refresh

: Help

: Language

Power Options

The following power options are available to turn on and off the system:

- Power ON: You can do this to power on the server system. Once the device is powered on and it becomes responsive, its software and hardware components start functioning. You will be able to interact with the system and use its various features and functionalities.
- Force Shutdown: You can do this to power off the server system immediately as a non-graceful shutdown. This is the immediate action of turning off the system without any delay. When a system is powered down immediately, all power supply to its components is cut off instantly, leading to an abrupt, non-graceful shutdown.
- Graceful Shutdown: You can do this to power off the server system gracefully by properly shutting down the operating system before turning off the system. This behavior is akin to a quick press and release of the physical power button, allowing the system OS to safely offload necessary services and save critical data before smoothly terminating the operating system.
- Power Cycle: You can do this to power off the server system completely and power it back on.
- Power Reset: You can do this to perform a warm restart on the server system. This action is typically performed to resolve issues or clear temporary glitches in the system's operation. During a power reset, the server is turned off completely before power is restored after a brief interval. This initiates the device's startup sequence from an initial state.
- AC Cycle: This action will momentarily disconnect the power cable from the system before reconnecting it. This action will completely disconnect the system from the power source, which may result in data loss of unsaved data. The power is restored after 10 to 20 seconds, and BMC is automatically reset. Use it with caution.

Note: The action of powering on and off will happen automatically. When the system is powered down (therefore not 'on'), you can only choose the [Power ON] option. However, if the system is currently powered up ('off'), you can see the 'Reset' and 'Off' options.

Behavior for Remote AC Power Cycle

Upon an AC power cycle, the system will restore or stay off based on the current BIOS settings.

Expected Behavior After AC Power Reset

The power is restored after 10 to 20 seconds, and BMC is automatically reset. The system will behave according to the BIOS setting for 'RestoreOnAcPowerLoss':

1. **Last State:** The system returns to the last power state before the reset.
   - If the system is in the **S5** (off) state, it will remain off.
   - If the system is in the **S0** (on) state, it will power back on.
2. **Power On:** The system will power on after the AC reset, regardless of its previous state.
   - If in **S5**, it will power on.
   - If in **S0**, it will stay powered on.
3. **Stay Off:** The system will remain off after the AC reset, regardless of its previous state.
   - If in S5, it will stay off.
   - If in S0, it will power off and remain off.

Exception

If the BMC cannot retrieve the 'RestoreOnAcPowerLoss' value from the BIOS, the system will default to **S5** (off). In this case, the BMC will take no action, and the system will remain off.

Note for A.2

The BMC will ensure the system resumes power-on in cases where the system was previously powered on before the AC reset.

Refresh

You can click on refresh to retrieve the latest update for the respective page. If you click the icon to refresh the Web UI using a web browser, you will be logged out.

Help

You can click on Help to get additional information regarding every page.

Language

You can select different languages from the pop-up window, including:

- English
- Simplified Chinese
- Japanese

The BMC Main Menu will display the following information:

Quick Links

You can use the options in the upper bar to navigate to widely used pages for quick actions. Quick actions include the following:

- System: You can use this link to navigate to the System page.
- Storage: You can use this link to navigate to the Storage page if a storage component is connected.
- UID Control: To identify the server, you can click the UID icon to navigate to the UID control component to turn **ON** or **OFF** the blinking LED.
- Firmware Update: You can use this link to navigate to the Firmware Management page to update firmware.
- Sensor Readings: You can use this link to navigate to the Sensor Readings page.

System Health

This section contains the overall system health status notifications. You can click on the health status to get more details about the system component health. Symbols indicating the status include the following:

 [Good]: This symbol means that the overall health of all system components is good.

 [Warning]: This symbol means that one or more components need attention and could fail.

 [Critical]: This symbol means that one or more components' health is in critical condition.

Storage Health

In this section, you can find the overall storage component health and notifications if a storage component is connected and detected, as well as HOST is powered on. Click on the health status to get more details about the hard drive or controller health. Symbols indicating the status include the following:

 [Good]: This symbol means that the overall health of all system components is good.

 [Warning]: This symbol means that one or more components need attention and could fail.

 [Critical]: This symbol means that one or more components' health is in critical condition.

 **Note:** Storage Information will be displayed only when the monitored system has the respective storage component(s) installed, and HOST is powered up.

System

The System frame displays a brief summary of system components such as Firmware version, Firmware Build Time, Supermicro Redfish Version, BIOS Firmware Version, BIOS Build Time, CPLD Version or MCU Version (if the motherboard of the system is using MCU instead of CPLD), BMC MAC Address, and LAN MAC Addresses. Unless there is at least one AOC NIC in the system, the BMC Dashboard will provide a link to the Network AOC and a message to you that all Add-On-Cards' information can be viewed on the Network AOC page. The tooltip message will be "Go to the Network AOC page."

Host

This host frame displays a brief summary of host information, such as Server Host Name, Server IPv4 Address, and Server IPv6 Address.

Note: IPv4 Address or IPv6 Address(es) will only be shown upon configuration in the Network Configuration.

Power Consumption

This section displays a graphical representation of the system power consumption with time stamps. Click on the graph to go to the Power page for more details about power consumption.

Remote Console Preview

This section displays the preview of the remote console state. You can click on the settings to modify the Virtual Console configurations. The page will automatically continue on its own, or you can use the mouse to click to continue. You can choose HTML5 or Java plug-in for your preferred virtual console option, with HTML5 being selected by default.

Note: X14/H14 BMC based on Open BMC will not have a JAVA console, so you will only have HTML5 as an option.

Recent Logs

This section displays the latest health event log entries.

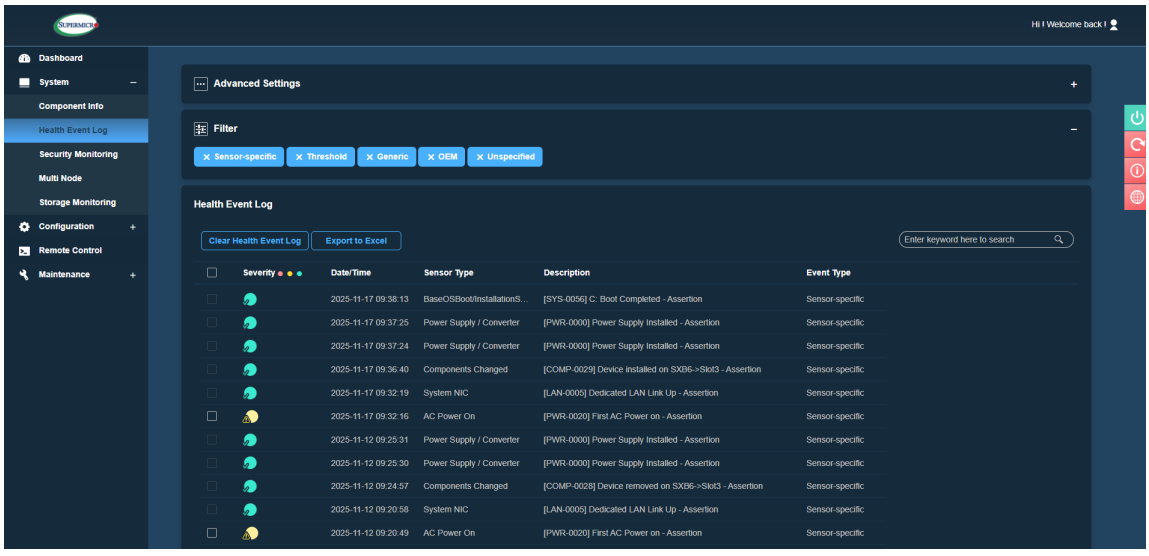


Figure 2-14: Recent Logs Section

2.5 System

The BMC System page displays system component details and health information, health events, sensor readings, and storage monitoring if the server is connected to the storage component(s).

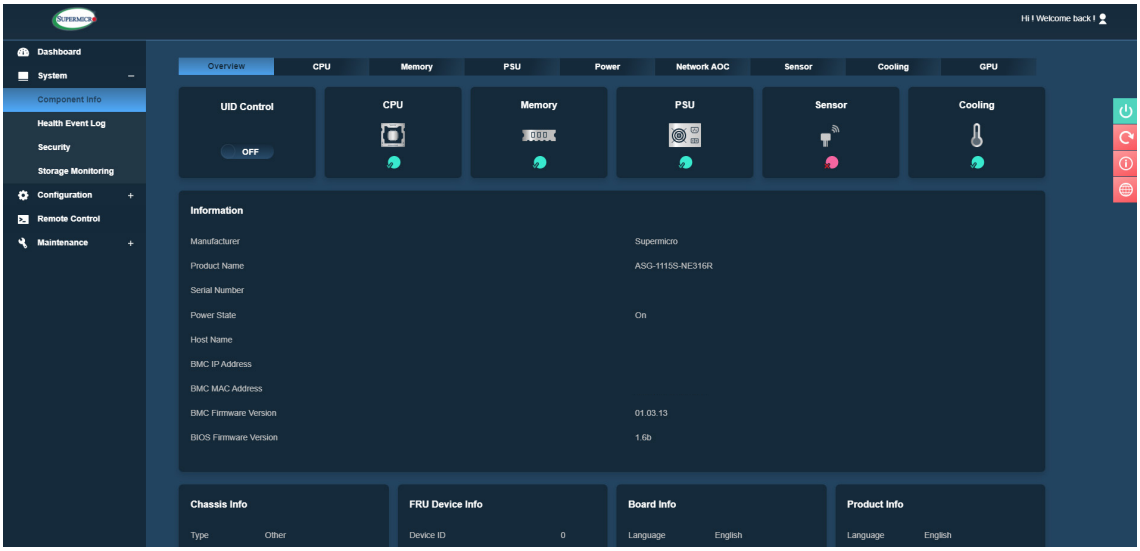


Figure 2-15: System Page

2.5.1 Component Information

You can use this page to view details about the system, installed components, health, and sensor readings.

> **Note:** Not all information on components listed under the Help Page is available for all types of servers. The Help Page is the general guide for most system servers. See individual server manuals for further information.

Overview

- UID Control: You can use this to turn on or off the UID for you to identify the server.
- Health Status Summary: You can use this to check the health status of each installed component. Click on the individual health status icons to view the details about the component.
  - CPU — This displays the overall health status of installed CPUs in the system. Issues that occur in CPU modules should not affect Sensor Health monitoring.
  - Memory — This displays the overall health status of installed memory components in the system. Issues that occur in memory modules should not affect Sensor Health monitoring.

  - PSU — This displays the overall health status of installed Power Supply Units (PSU) in the system. Issues that occur in PSU units should not affect Sensor Health monitoring.
  - Sensor — This displays the overall health status for the sensors present in the system.
  - Fan — This displays the overall health status of installed fans in the system. Issues that occur in FAN units should not affect Sensor Health monitoring.
- Information: This page displays the system information and details.
  - Manufacturer — Manufacturer name
  - Product Part Number — Product part number of the product
  - Serial Number — Serial number of the product.
  - Power State — System power status
  - Host Name — Host name of the system
  - BMC IP Address — IP address of the BMC host
  - BMC MAC Address — MAC address of the BMC
  - BMC Firmware Version — BMC Firmware version
  - BIOS Firmware Version — BIOS Firmware version
- FRU Reading: You can configure the FRU settings by using the SMCIPMITool utility and checking the detailed FRU information.
  - Device ID — System device ID
  - Chassis Info — The kind of chassis information displayed will depend on the type of node system installed.

    On a Single-Node System, the following chassis detail information will be displayed:
    - Type — Chassis type detail
    - Part Number — Chassis part number
    - Serial Number — Chassis serial number

On a Multi-Node System, the following chassis detail information will be displayed:

- Configuration ID — Chassis configuration ID
- MCU Firmware Version — Chassis MCU firmware version
- User Defined System Name — Chassis user-defined system name
- BP Model Name — Backplane model name
- BP Serial Number — Backplane serial number
- BP Revision — Backplane revision

- Board Info: You can view detailed board information.
  - Language — Supported language for the board
  - Manufacturer — Manufacturer details
  - Product Name — Product details
  - Serial Number — Board serial number
  - Part Number — Board part number
- Product Info: You can view detailed product information.
  - Language — Product supported language
  - Manufacturer — Manufacturer details
  - Product Name — Product details
  - Serial Number — Product serial number
  - Part Number — Product part number
  - Version — Product version
  - Asset Tag — Product asset tag

CPU

This tab provides information about each processor installed in the server.

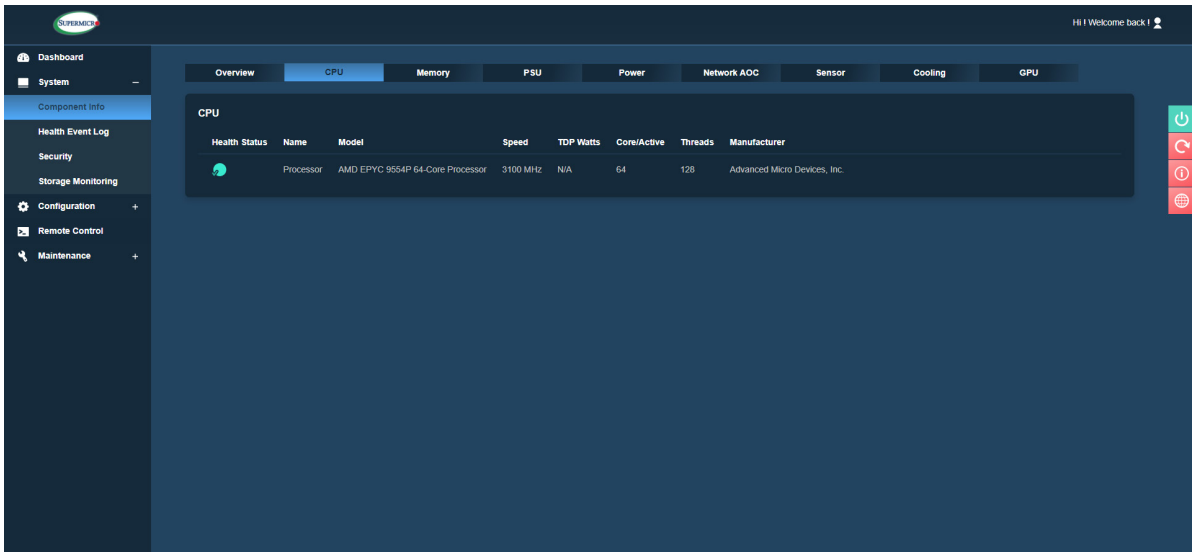


Figure 2-16: CPU Page

This page displays the following details:

- Health Status: You can view the health status of the CPU. There are three statuses that can be viewed.
  - Normal
  - Warning
  - Critical
- Name: You can view the name of the processor.
- Model: You can view the information about the processor model.
- Speed: You can view the speed (current speed in MHz) of the processor.
- TDP Watts: You can view the supported values for Thermal Design Power (TDP).
- Cores / Active: You can view the total number of cores of the processor as well as whether the processor is active or inactive.
- Threads: You can view the total number of threads.
- Manufacturer: You can view the processor manufacturer information.

Memory

The tab provides information about each DIMM(s) installed in the server.

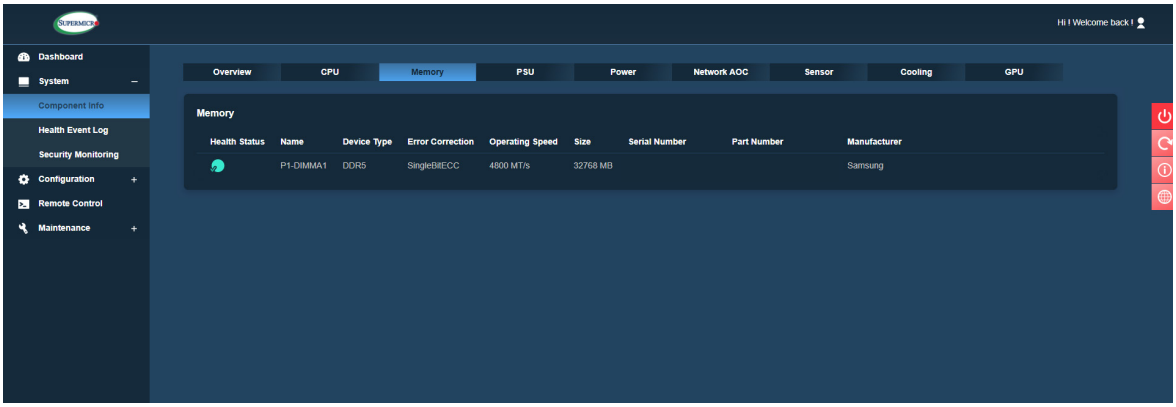


Figure 2-17: Memory Page

This page displays the following information:

- Status: You can view one of three statuses indicating the health status of the DIMM.
  - Normal
  - Warning
  - Critical
- Name: You can view the memory device name.
- Device Type: You can view the memory device type defined by SMBIOS (e.g., DDR4, DDR5, RDIMM, LRDIMM, or DCPMM).
- Error Correction: You can view the supported error correction information defined by SMBIOS.
  - AddressParity — Address parity errors can be corrected.
  - MultiBitECC — Multibit data errors can be corrected by ECC.
  - SingleBitECC — Single bit data errors can be corrected by ECC.
- Operating Speed: You can view the operating speed of memory in MT/s as reported by the memory device. Memory devices that operate at your bus speed shall report the operating speed in MT/s (bus speed).
- Size: You can view the size of the memory region in mebibytes (MiB).

- Serial Number: You can view the product serial number of the memory device.
- Part Number: You can view the product part number of the memory device.
- Manufacturer: You can view the manufacturer information of the memory device.

PSU

This tab shows power supply unit information. BMC is designed to display information for all Power Supply Units (PSUs) that are currently inserted into the system. In instances where power cables are disconnected, the BMC will indicate 'N/A' values for the corresponding PSUs. To ensure a streamlined and accurate representation, the BMC will NOT display information for PSUs that have been removed or are identified as non-real/dummy PSUs. This functionality is specifically intended to exclude any 'dummy' PSUs inserted into the system, providing a more precise overview of the active and connected power supply units. Any action taken to remove a Power Supply Unit (PSU) or disconnect a power cable will generate a Machine Event Log (MEL) entry for documentation and tracking purposes.

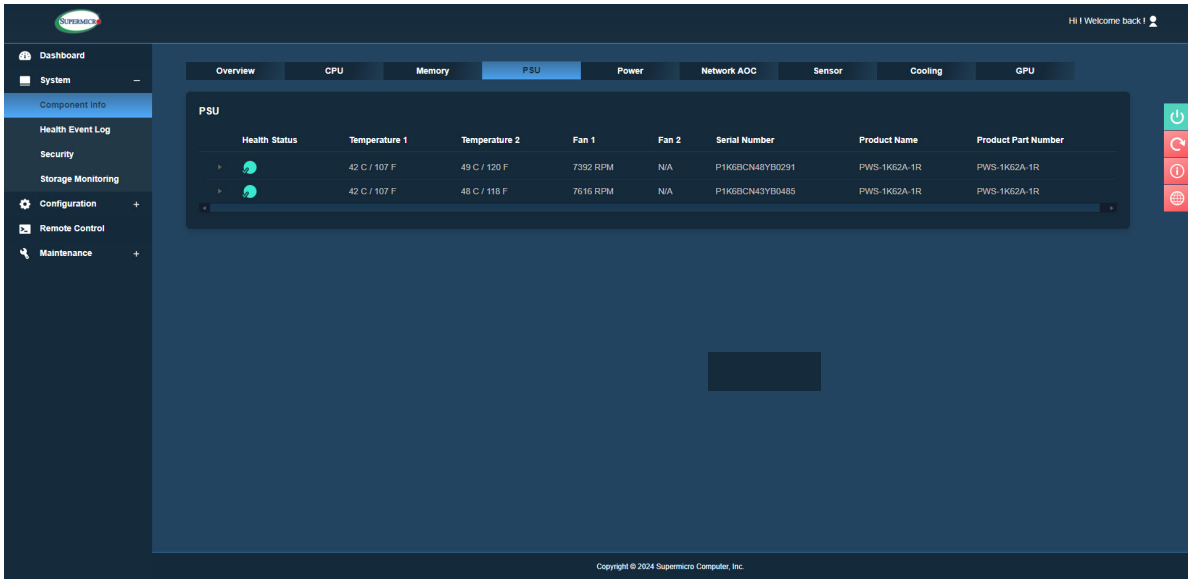


Figure 2-18: PSU Page

This page displays the following information:

- Health Status: You can view the health status of the PSU. There are three statuses that can be viewed.
  - Normal
  - Warning
  - Critical
- Temperature 1: You can view the temperature reading of the PSU.
- Temperature 2: You can view the temperature reading of the PSU (if present).

- Fan 1: You can view the FAN reading of the PSU.
- Fan 2: You can view the FAN reading of the PSU (if present).

Note: 'N/A' will display for Fan 2 if not detected.

- Serial Number: You can view the serial number of the PSU.
- Product Name: You can view the name of the PSU.
- Product Part Number: You can view the part number of the PSU.

You can also view the following additional information under the drop-down menu:

- AC Input Voltage (V)
- AC Input Current (V)
- AC Input Power (W)
- DC Main Output Voltage (V)
- DC Main Output Current (A)
- DC Main Output Power (W)

If the PSU module is removed, the expected display will be as follows:

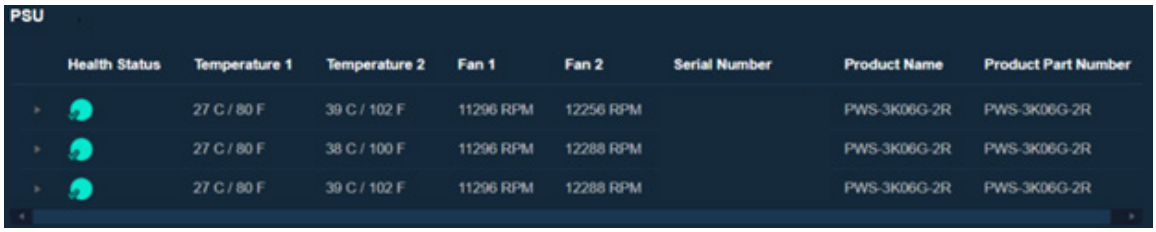


Figure 2-19: Display Resulting from PSU Module Being Removed

If the power cable is disconnected from the PSU, the expected display will appear as follows:

Figure 2-20: Display Resulting from Power Cable Disconnected from PSU

Power

The tab displays system board power consumption information.

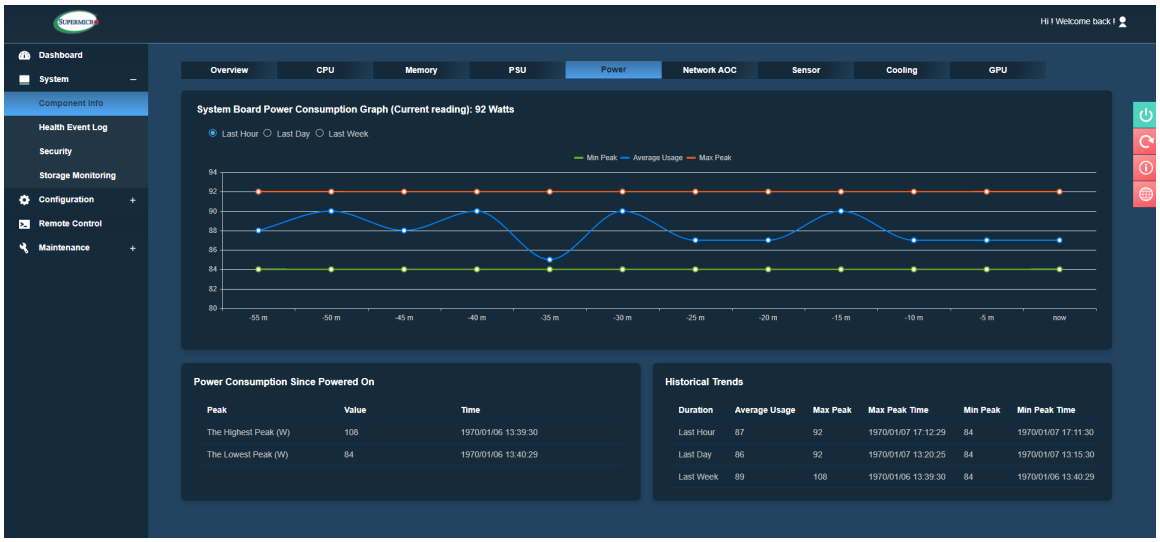


Figure 2-21: Power Page

This page displays the following information:

- System Board Power Consumption Graph: You can view the system power consumption value (in watts) over time. Readings can be checked for the last hour/days/week.

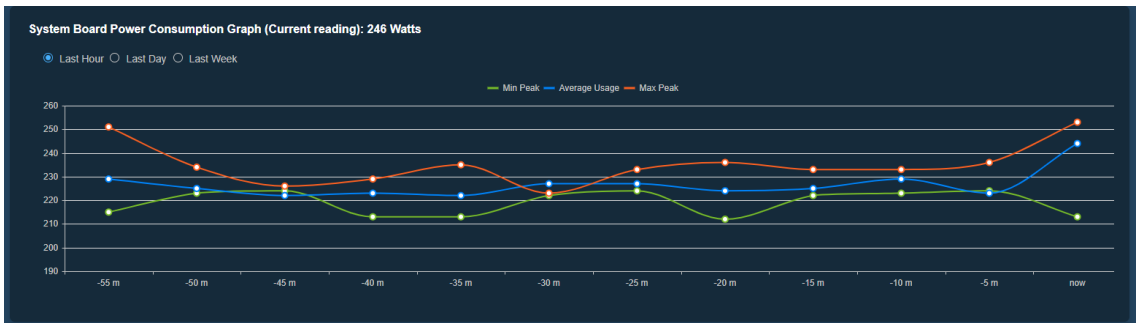


Figure 2-22: System Board Power Consumption Graph

- Power Consumption Since Power On: You can view the power consumption at the current time.
  - Peak — Highest peak/Lower peak
  - Value — Power consumption value in watts
  - Time — Timestamp value

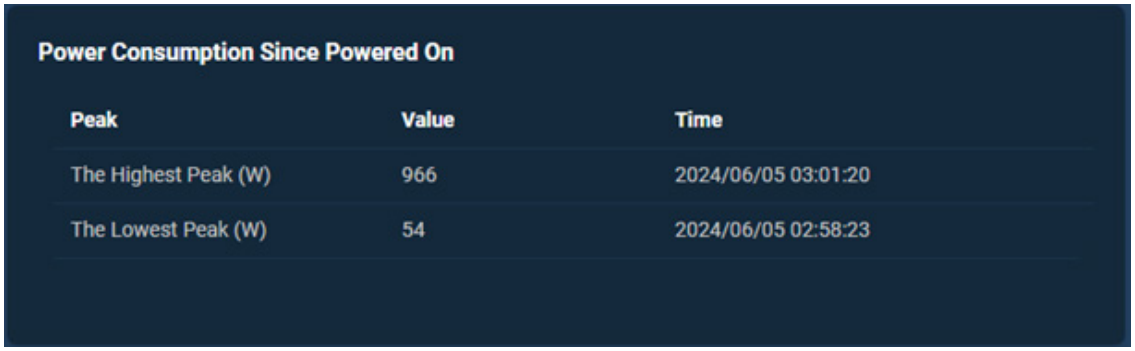


Figure 2-23: Power Consumption Since Power On

- Historical Trend: You can view the past data on power consumption.
  - Time — Last hour/day/week
  - Average Usage — Average power usage
  - Max Peak — Maximum peak power value (W)
  - Max Peak Time — Maximum peak time stamp
  - Min Peak — Minimum peak power value (W)
  - Min Peak Time — Minimum peak time stamp

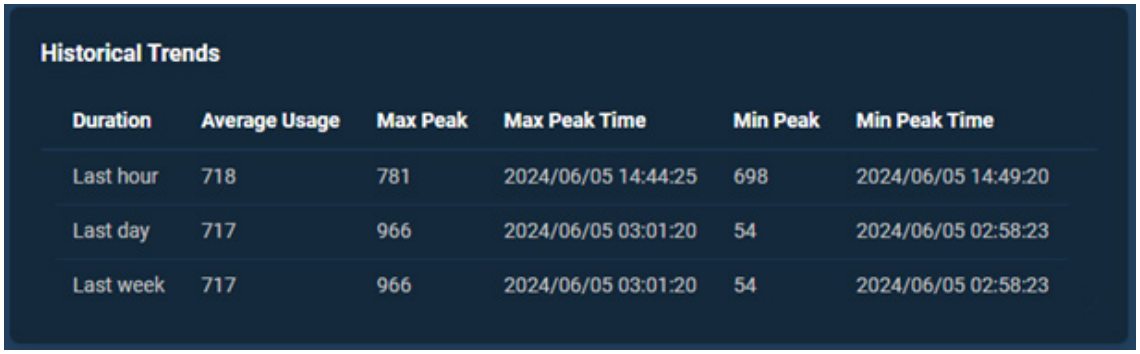


Figure 2-24: Historical Trends

Network AOC

This tab provides information about add-on network devices installed in the system. As part of the X14/H14 advanced settings, you will be able to turn 'AIOM NIC Power in S5 State' on and off.

Note: This page will only display AOC NIC card Information. Temperature will display as 'Unsupported' for AOC NIC cards that do not support the temperature feature.

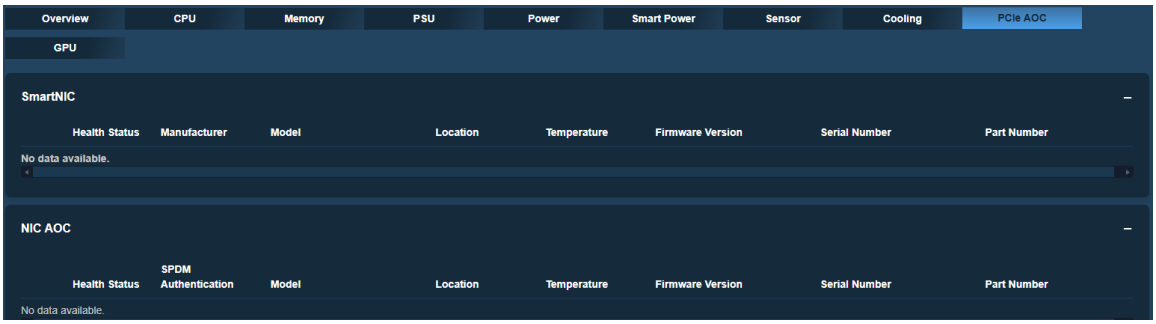


Figure 2-25: Network AOC Page

This page displays the following information:

- Health Status: This displays the health of the AOC NIC card.
- Model: This displays the model number of the AOC NIC card.
- Temperature: This displays the temperature of the AOC NIC card.
- Location: This displays the location of the AOC NIC card.
- Serial Number: This displays the serial number of the AOC NIC card.
- Port: This displays the port number of the AOC NIC card.
- MAC Address: This displays the MAC address of the AOC NIC card.
- FW Version: This displays the firmware version of the AOC NIC card.

In certain system platforms, such as the X14 RIO GrandTwin (which supports OCP NIC in the S5 state), there is a power option for the AIOM slot. You can power on the AIOM slot when the system is in the S5 state. This feature allows the NIC card to remain operational even when the system is powered down. The button's purpose is to enable you to maintain NIC functionality in the AIOM slot during the S5 state.

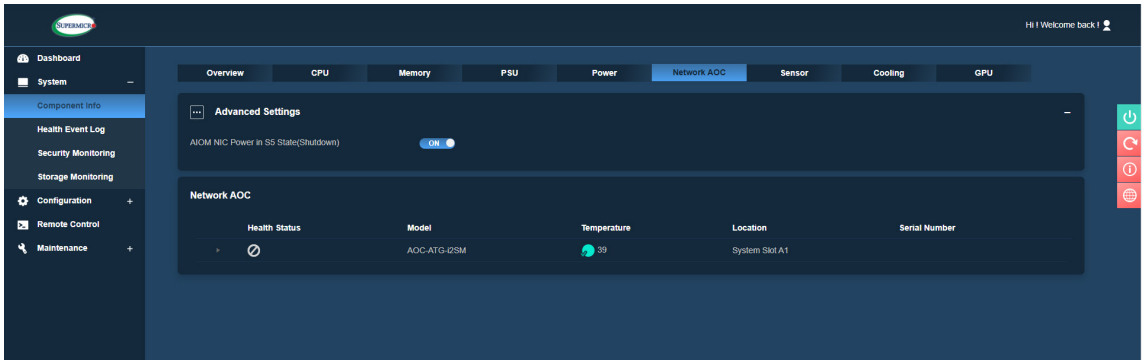


Figure 2-26: AIOM NIC Power in S5 State (Shutdown) Toggle

The table describes the naming rule for Physical LAN, which is used by BMC to pass onto SSM. X and Y are numerical indices (0…9).

Physical LAN	A system WITH / WITHOUT TAS installed and running / WITH TAS REMOVED
AOC NIC	**Redfish API:** /redfish/v1/Systems/1/EthernetInterfaces/X **Name:** AOC LAN Y **Description:** AOC-STGS-i2T #Y
Onboard NIC	**Redfish API:** /redfish/v1/Systems/1/EthernetInterfaces/X **Name:** Onboard_NIC Y **Description:** OnBoard #Y

Sensor

This tab provides information about the sensors' status, corresponding readings, and their threshold value.

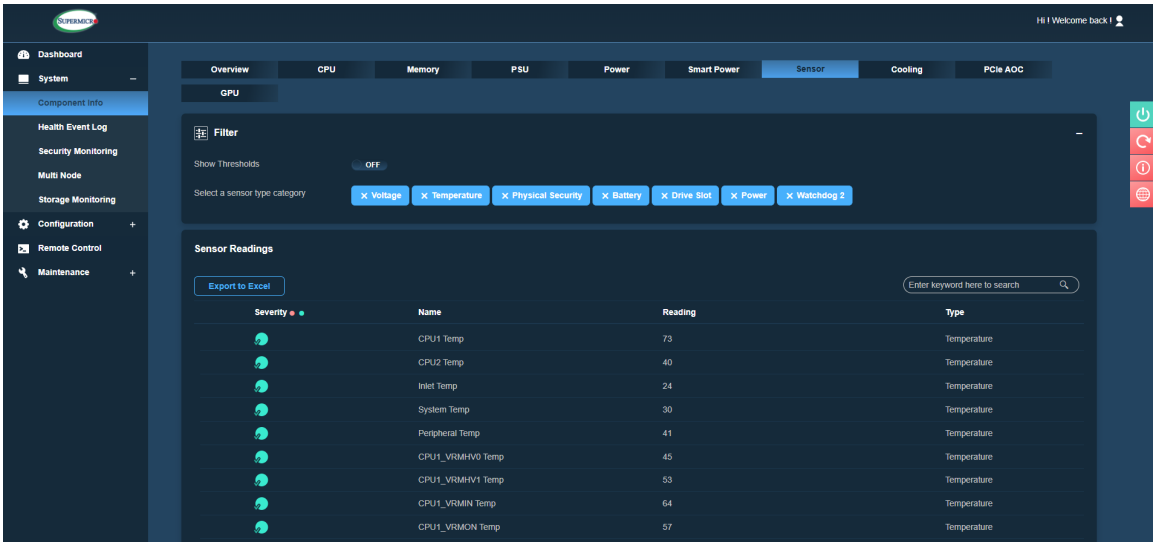


Figure 2-27: Sensor Page

The sensor table displays the following information about each sensor(s):

- Health: Sensor status indicates that the health state of the sensors.

  This symbol means that the sensor reading is normal.

  This symbol means that the sensor reading is not within the range and needs attention.

- Name: This column displays sensor names of currently available sensors from the system.
- Reading: This column displays the value of the current sensor's reading.
- Type: This column displays sensor type categories that can be selected.
  - Temperature Sensors
  - Voltage Sensors
  - Physical Security
  - Battery (aka Power Supply)
- Low NR: This column displays a lower non-recoverable threshold value for each sensor.
- Low CT: This column displays a lower critical threshold value for each sensor.

- High NR: This column displays a higher non-recoverable threshold value for each sensor.
- High CT: This column displays a higher critical threshold value for each sensor.

Note: If components are not installed, then static sensor values will display 'N/A.' All sensors with “N/A” values will not be displayed on the Web UI.

Sensor Type Categories

By default, [All Sensors] categories are selected and sorted by the orders from the BMC. You can also sort Sensor Readings by the following categories:

- Temperature Sensors
- Voltage Sensors
- VBAT Status
- Physical Security

Export to Excel

You can export sensor readings to Excel format.

Intrusion Reset

You can use this button to reset chassis intrusion.

Severity	Name	Reading	Type
	P1_DIMMA~D Temp	35	Temperature
	P1_DIMME~H Temp	N/A	Temperature
	P2_DIMMA~D Temp	45	Temperature
	P2_DIMME~H Temp	N/A	Temperature

Figure 2-28: Sensors for Memory Example

Cooling

This tab shows Air Cooling and Liquid Cooling status and allows you to configure FAN speeds for installed fans and liquid detect power options in the system. All fan sensors will be detected once the system HOST is powered on. Fan data is obtained from the BMC Sensor Data Record (SDR) noted in the Supermicro Thermal System Thermal Design Guide (SSTDG).

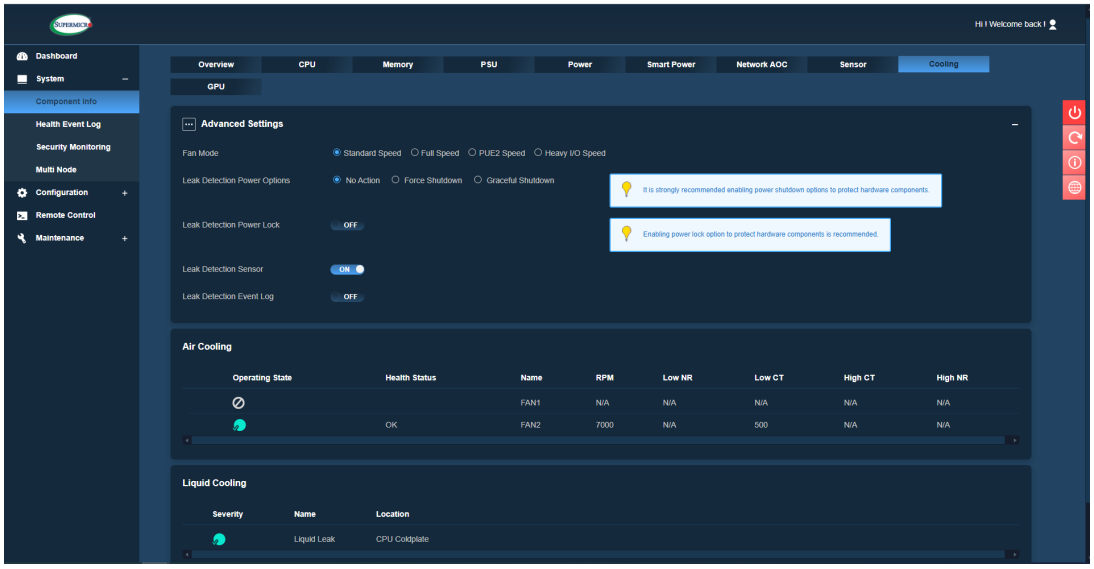


Figure 2-29: Cooling Page

This page displays the following air cooling information:

- Operating Status: This column indicates whether the fans are in an operating state or not.

  This symbol means the fan is not installed or that it has lost the connection to the system.

  This symbol means that the fan is in a good, normal operating condition.

  This symbol means that the fan is not in good operating state.

- Health Status: This column indicates the fan's health status.
- Name: This column indicates the system fan number.

- RPM: This column indicates the revolutions per minute for each fan. The RPM should provide the actual/real value detected in the system. If there is a faulty FAN present, RPM should be shown as zero (0) if the fan does not work. PSU FAN A or FAN B speeds will be the same as the speed of PSU FAN 1.
- Low NR: This column displays a lower non-recoverable threshold value for the fan sensor.
- Low CT: This column displays a lower critical threshold value for the fan sensor.
- High CT: This column displays a higher critical threshold value for the fan sensor.
- High NR: This column displays a higher non-recoverable threshold value for the fan sensor.

The following is a sample from IPMITool:

```
(# ipmitool sdr | grep Fan)
Front Fan RPM    | 5400 RPM            | ok
Rear Fan RPM     | 5400 RPM            | ok
PS 1-4 Fan RPM   | 5600 RPM            | ok
PS 5-8 Fan RPM   | 6000 RPM            | ok
```

Advanced Settings

For Cooling control, you can configure the Fan Mode settings. Cooling modes are dynamically received from the Redfish API. As a result, the Web UI will display all available speed settings for you to select. The possible fan speeds are as follows:

- Standard Speed: This is the standard fan speed setting for standard power saving and efficiency.
- Full Speed: This is the full speed setting for maximum system performance.
- Optimal *or* PUE2 Speed: This is the optimal fan speed setting. It will adjust the fan speed by balancing the needs between system performance and power savings. This is the most efficient cooling setting under normal usage.
- Heavy I/O Speed: This is the heavy I/O fan speed setting, which will boost cooling to the add-on card zone.

You can configure the following Leak-Detect Power Options to manage the system's response in the event of a detected leak. Additionally, you can enable a Leak-Detect Lock to protect hardware components if a leak is detected and the selected power option is not 'No Action.'

- No Action: System will remain powered on even if a leak is detected. By default, No Action is selected.
- Force Shutdown: If a leak is detected, the system will immediately power down, lock the power options, and notify users with the same alert.
- Graceful Shutdown: Selecting this option will cause the system to power down gracefully and save all data before shutting down when a leak is detected. You must confirm that the area is dry and operational before powering the system back on.
- Leak-Detect Lock: This option enables a lock to protect hardware components after a leak is detected, provided the selected power option is not 'No Action.' By default, this option is enabled.
- Leak-Detect Event Log: This option allows you to disable logs being sent to the SEL tab. By default, the option is enabled.

Liquid Cooling

This feature provides details about possible sensor leakages.

- Operating Status: This column indicates whether there is any leakage.

   This symbol indicates there is a leakage and that cooling is not in good operating state.

   This symbol indicates there is no leakage and that cooling is operating in good and normal condition.

- Name: This column provides the sensor name.
- Location: This column indicates which one of the three locations has leakage.
  - CPU Coldplate
  - CPU Tray
  - PCIe Manifold

For non-featured platforms, the "Liquid Cooling" section will be hidden in the BMC Web UI.

When you select to disable SEL for Senor using the toggle button, you will receive the prompt message to confirm, *“All sensors will be disabled for leakage detection. Are you sure you want to disable the sensors?"*

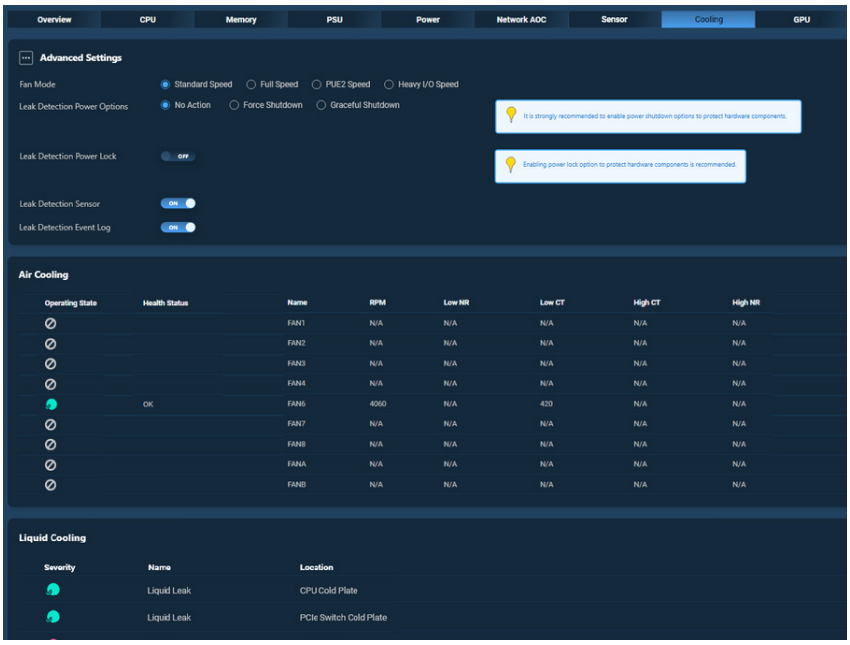


Figure 2-30: Cooling Page

When you click the power control button located on the right side of the dashboard page, an alert window about the disabled "power button" post-liquid leakage detection will appear. It will include the following prompt message: *“Power button is currently disabled due to liquid leakage was detected. Please go to Cooling page to unlock Leak-Detect Lock.”*

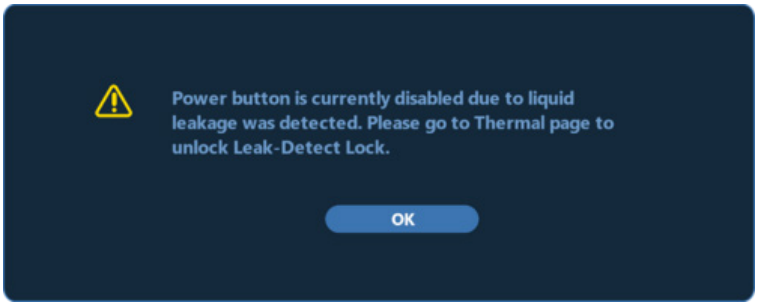


Figure 2-31: Power Button Alert Message

When unlocking the Leak Detection Power Lock, there will be a prompt for you to confirm: *“Liquid leakage detected. To disable the lock feature, please confirm that the area is dry and all conditions for safe operation have been met."*

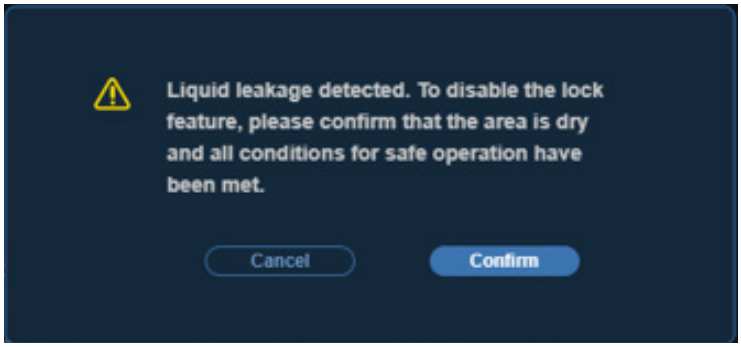


Figure 2-32: Liquid Leakage Alert Message

When you want to disable getting an SEL log for leak detection, there will be a prompt to confirm: *“Users will no longer receive the system event logs of liquid leak detection. Are you sure you want to disable the System Event Log?"*

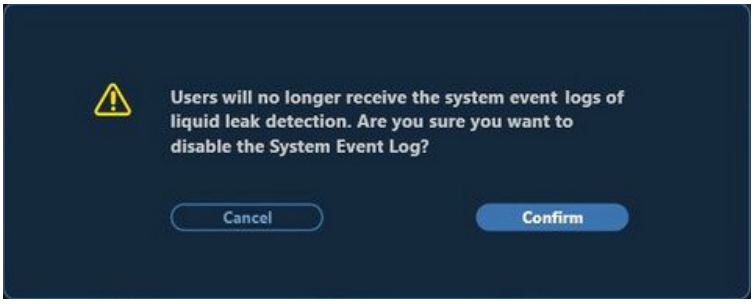


Figure 2-33: SEL Log Alert Message

Changes Related to S5 Standby Fan Requirement

For a dedicated fan in S0 state, the 'Name' column should show 'FANSTBY.' The 'Low CT' and 'High CT' columns should show 'N/A' as the dedicated fan is not being used in the S0 state.

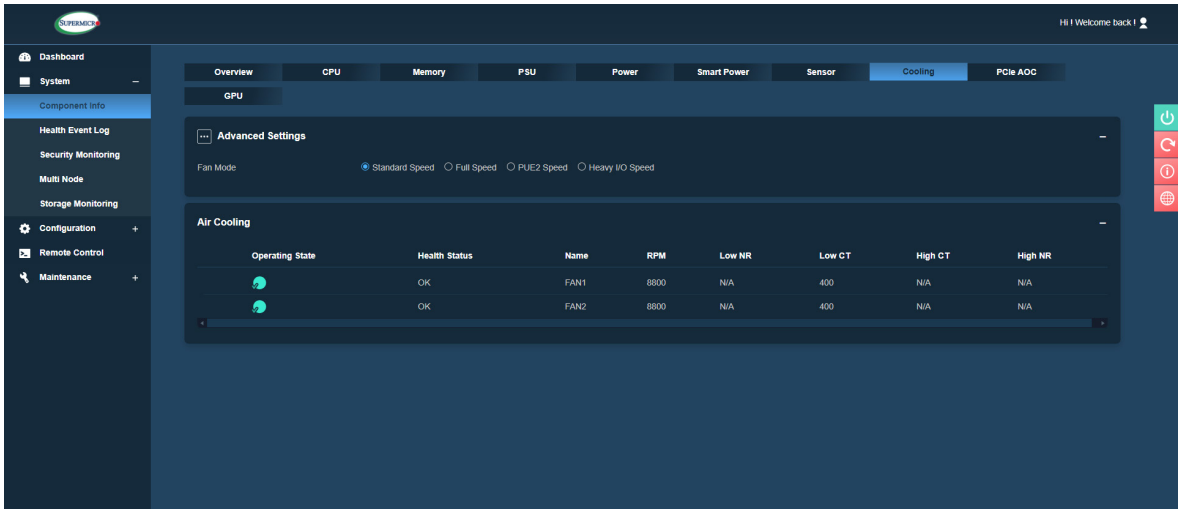


Figure 2-34: Dedicated Fan S0 State

For a dedicated fan in the S5 state, the 'Name' column should show 'FANSTBY.' The 'Low CT' and 'High CT' columns should list the threshold values received from the sensors.

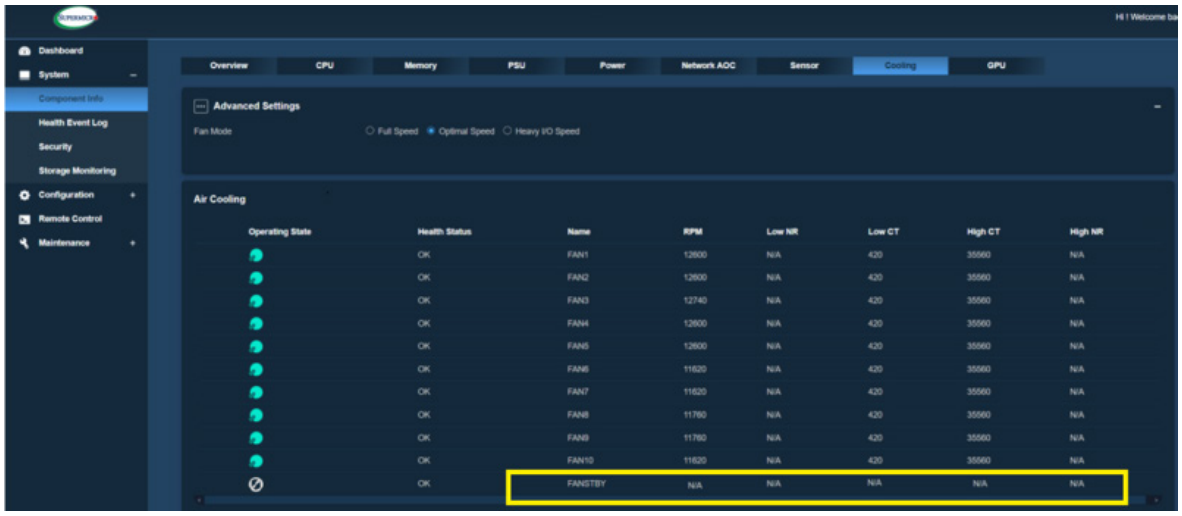


Figure 2-35: Dedicated Fan S5 State

For a system S5 fan in S0 mode, the ‘Name’ column should show ‘FAN[n]/STBY’ to notify you which system fan will be used as the standby fan in the S5 state.

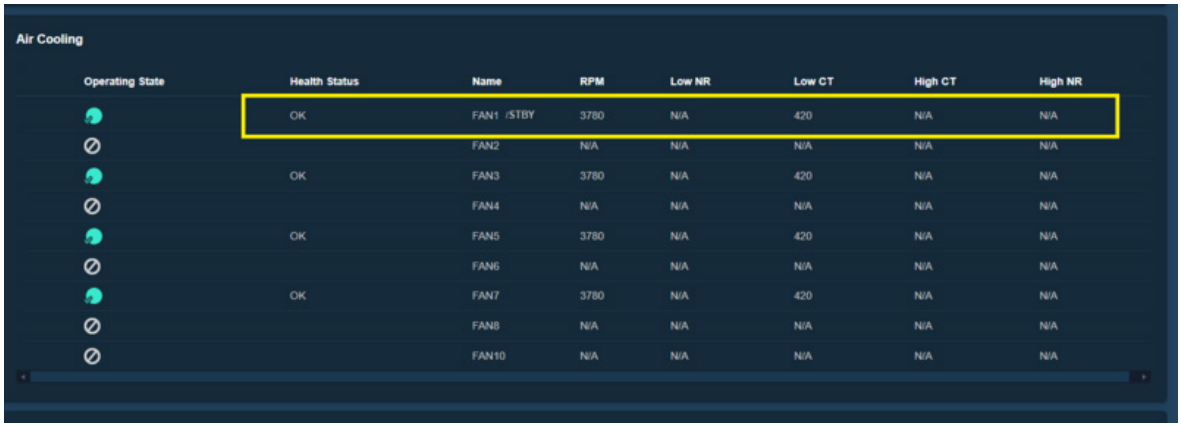


Figure 2-36: System S5 in S0 Mode

GPU

This tab provides details about each installed GPU unit in the system. For the HaBaNa system, the Advanced Integrated Peripheral (AIP) tab will be in place of the GPU tab.

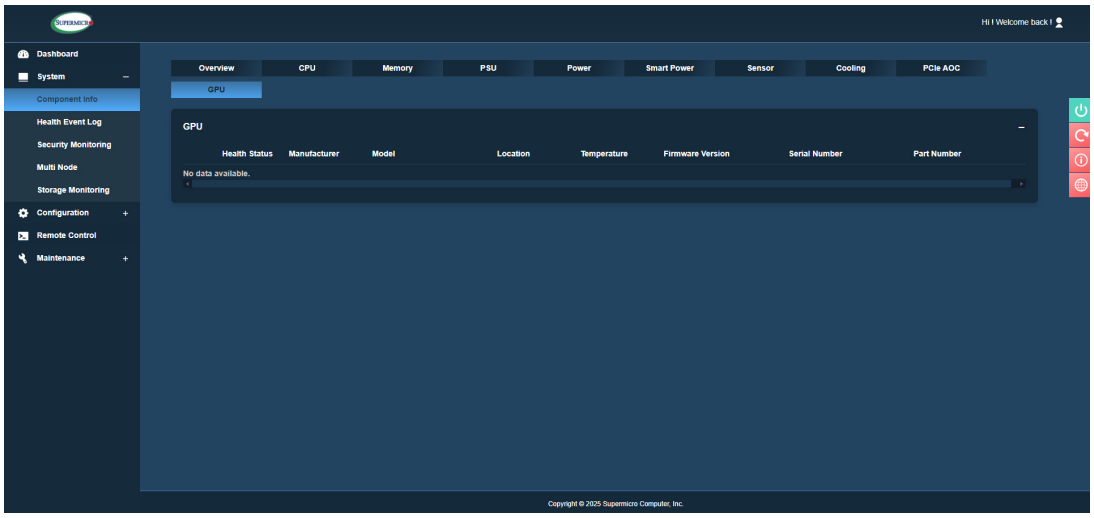


Figure 2-37: GPU Page

You can view the following information:

- Location: This column displays add-on device slot locations.
- Model: This column displays the vendor and model name of the GPU device.
- Serial Number: This column displays the serial number of the GPU device.
- Part Number: This column displays the part number of the GPU device.
- Firmware Version: This column displays the firmware version for GPU device.

AIP

This tab provides the following details about each installed AIP (HaBaNa Gaudi) unit in the system.

- Location: This column displays the add-on device slot location.
- Model: This column displays the vendor and model names of the AIP device.
- Serial Number: This column displays the serial number of the AIP device.
- Part Number: This column displays the part number of the AIP device.
- Firmware Revision: This column displays the firmware revision information for the AIP device.

2.5.2 Health Event Log

This page provides a record of events that occurred on the management system. You can view and export to Excel files, as well as clear and acknowledge events from the monitored system. Logged events can help you to diagnose issues or detect potential issues. You can also perform prohibitive actions to resolve any such issues for the managed system and configure it to send notification alerts, SNMP Traps, or Syslog server entries for specific types of system events. You can enable the following options in the Advanced settings:

- Enable/Disable AC Power On Event Log
- Enable/Disable FIFO Event Log using the ON/OFF switches

The default option is enabled.

Note: By default, all event types will be selected so that you can view all events. You can apply filters for event selection based on event types (Supported event types: Sensor-Specific, Threshold, Generic, OEM, Unspecified). The number of Health Event logs is limited to **4096**.

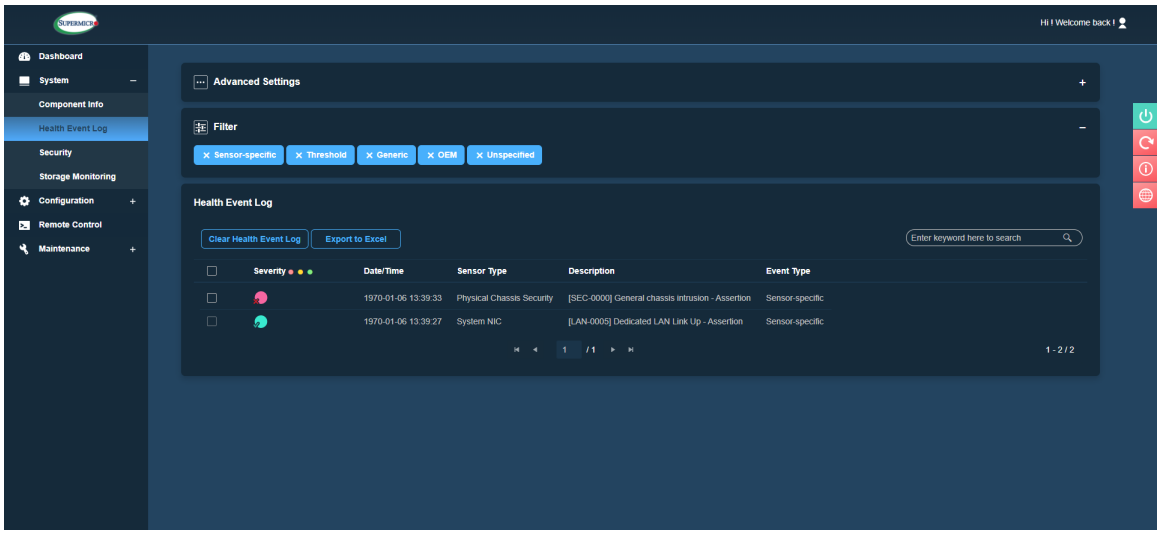


Figure 2-38: Health Event Log

The Health Event Log table shows the following information about each event(s):

- Severity: This column indicates one of the three statuses indicating the severity of the events.

 [Green]: This symbol indicates information or de-assertion events.

 [Yellow]: This symbol indicates warning events that need attention.

 [Red]: This symbol indicates critical events that need immediate action in case of possible failure.

  - Date/Time: This column indicates the timestamp of event occurrence.
  - Sensor: This column indicates the type (Name) of the sensor that triggered the event.
  - Description: This column provides a basic description of the event.
  - Event Type: This column indicates the events that will be listed based on the following categories.
    - Sensor-Specific
    - Threshold
    - Generic
    - OEM
    - Unspecified

Administrator Options

You can apply the following administrator options:

- Export to Excel: You can use this option to export the current event log to an Excel file.
- Clear Health Event Log: You can use this to select all rows to clear the recorded event log.
- Mark as Acknowledged: You can use this to mark acknowledged warning/critical events. Select a log entry that you want to acknowledge and click on Mark as Acknowledged.
- Clear Acknowledgements: You can clear all acknowledgments by clicking on Clear Acknowledgement.

Multi Node

This page is used to view details about the current node as well as other nodes in the server. Under the System Tab, you can view the nodes of the server in 'Logical Front View of Node' and general information about the present nodes. In 'Logical Front View of Node,' you can see the number of nodes, whether the node is present or not, as well as the power status of a particular node. Detailed information for a particular node can be viewed when you select the node. You can view Status, Power State, DC Output Power, DC Output Current, CPUs, System Temperature, Part Number, Board Serial Number, IP Address, BIOS Version, CPLD Version, or MCU Version (if the motherboard of the system is using MCU instead of CPLD), and BMC Version for the node of interest. For H14 Multi Node systems, you can also view POST CODE as well as Max Power. This page will not be available for non-multi-node servers. For H14 Multi Node systems, you can also view POST CODE as well as Max Power. This page will not be available for non-multi-node servers.

Note: Under User Privilege, you are limited to View Only mode. However, all users with User Privilege can automatically log into another BMC window. The first method is by clicking on a **white** arrow on the current node in the Logical Front View Node frame of the Multi Node page. The second is by clicking on the IP Address in the Node frame to open up the current node into a new web browser tab or window.

You can click on any of these nodes to get a BMC/Web UI redirected. From there, log in to BMC as a single or individual node to perform tasks, including firmware updates.

2.5.3 Storage Monitoring

This page allows you to view detailed information about installed storage components, including Intel VROC, Broadcom controllers, and other onboard storage devices. This page will not be available if a storage component/device is not connected and available actions in each view will depend on the system configuration and components selected. When using the Intel VROC interface, it is supported by firmware version 1.02 and provides added support for VROC. This version of the Storage Monitoring page should have five tabs: Overview, Physical View, Logical View, Controller View, and Task Queue. Otherwise, the page will only have four tabs.

Note: Each action will create a task in the task queue tab.

Overview

This page shows the supported drive status, the sum of physical drives, logical drives, controllers, battery status, and the total capacity of all physical drives. Drive status provides the health overview of connected drives as represented using the circle, segmented proportionally by quantity and status. If BMC detects that all connected drives are functional, the drive status will show **GREEN**. If BMC detects one or more drives that are offline or being rebuilt, the drive status will show **YELLOW**. If BMC detects that one or more connected drives are not functional, the drive status will show **RED**. When hovering on the colored segments, it will display tags with the corresponding quantity and status information.

Note: Intel VROC only applies to X14 generation systems, and not H14 generation systems.

Figure 2-39: Overview Section with Intel VROC

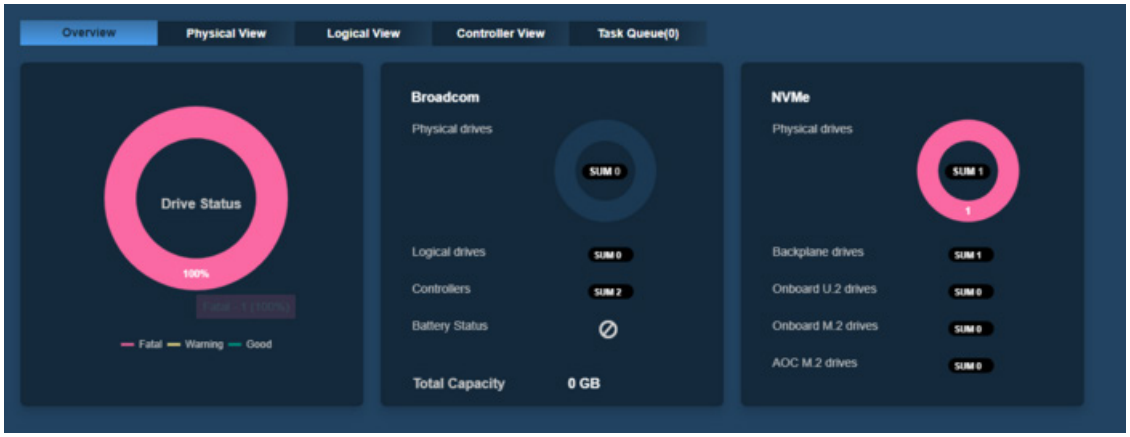


Figure 2-40: Overview with Broadcom and NVMe

Physical View

Physical view shows physical drive information for SAS, SATA, NVMe SSDs, etc. It also shows the details about physical drives attached to the controller or present in the storage subsystem. For additional information about the physical drive, click on the listing to expand the menu.

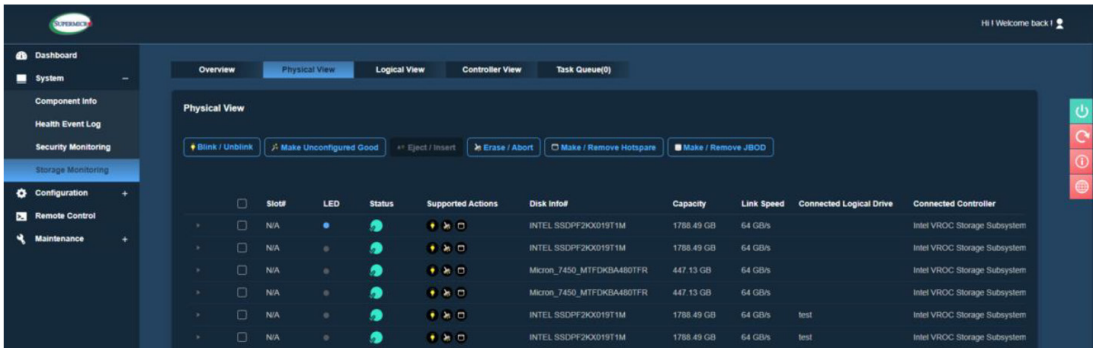


Figure 2-41: Physical View Page

You can also perform actions associated with each drive. All actions are available and applicable based on the selected available components in the system and system configuration.

> **Note:** The function of button(s) will be grayed out if the function(s) is not available. For instance, the LED blinking button will be disabled and grayed out if the connected drive does not possess the capability.

- Slot Number: This column displays the connected physical drive's slot number.
- LED: This column displays the LED blinking status of the corresponding drive.
- Status: This column displays the indicated health of the connected drive.

  This symbol indicates the health of all the storage components is good.

  This symbol indicates the storage component needs attention and could fail.

  This symbol indicates the storage component's health is in critical condition.
- Supported Actions: This column displays what actions are supported based on HDD type.
- Disk Info Number: This column displays the available drive information.

- Capacity: This column displays the capacity of the physical drive (GB).
- Link Speed: This column displays the link speed of the physical drive (b/s).
- Connected Logical Drive: This column displays the connected logical drive information (if any).
- Connected Controller: This column displays the connected controller information (if any).

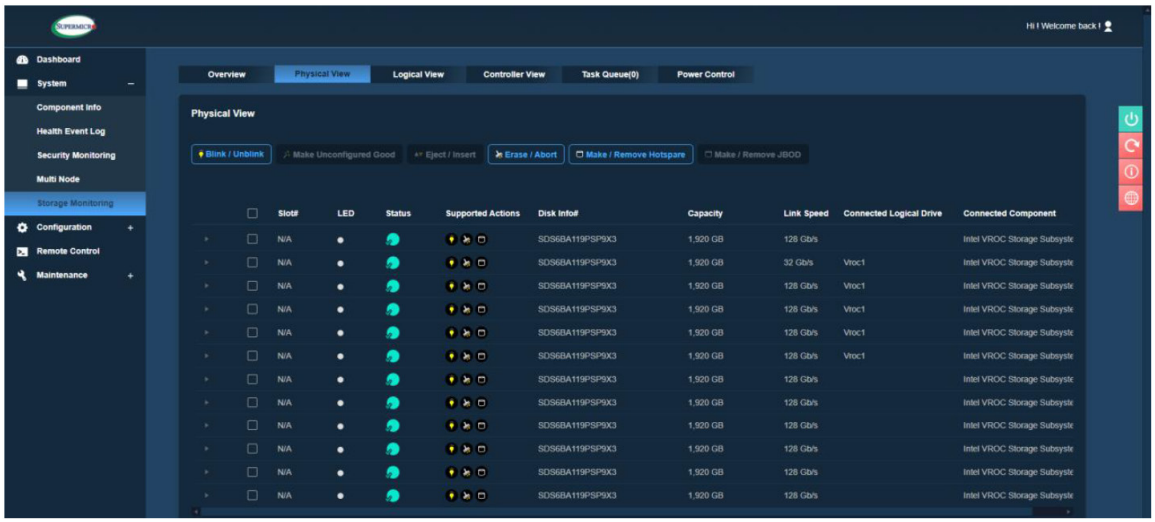


Figure 2-42: Physical View Page

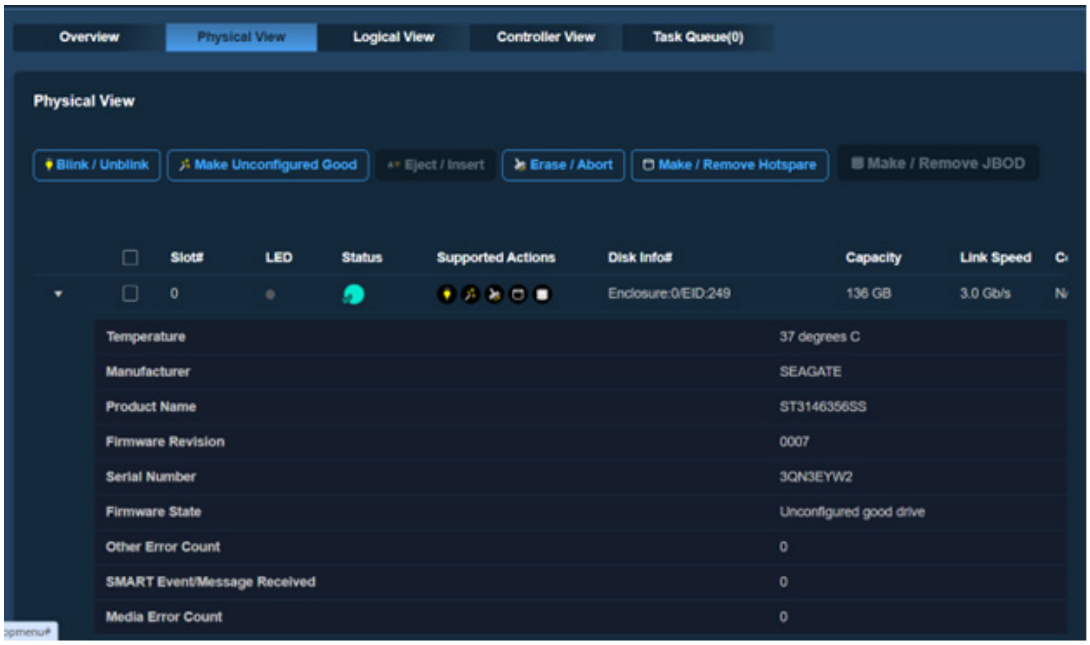


Figure 2-43: Physical View Expanded Menu for Listing

You can also view the following HDD detailed information by clicking the arrow pointer next to a particular HDD (NVMe or SATA). Web UI will only display available and supported features.

- Temperature (in Celsius)
- Name of Manufacturer
- Product Name of the storage controller
- Serial Number
- Drive functional (1 or 0)
- Percentage of drive life used (in %)
- VMD Mode (Disable / Enable)
- Port 0 Max Link Speed (in GT/s)
- Port 0 Max Link Width
- Port 1 Max Link Speed
- Port 1 Max Link Width

Physical View Actions

All physical actions are available and applicable based on the selected drive. BMC WEB will retain the last selected action and use it to display the corresponding tooltip when the leftmost checkbox is checked. This selection is preserved across interactions within the same tab session.

The selected action will only be reset under the following conditions:

- Navigating away from and re-entering the tab.
- Selecting the Refresh button on the right side.

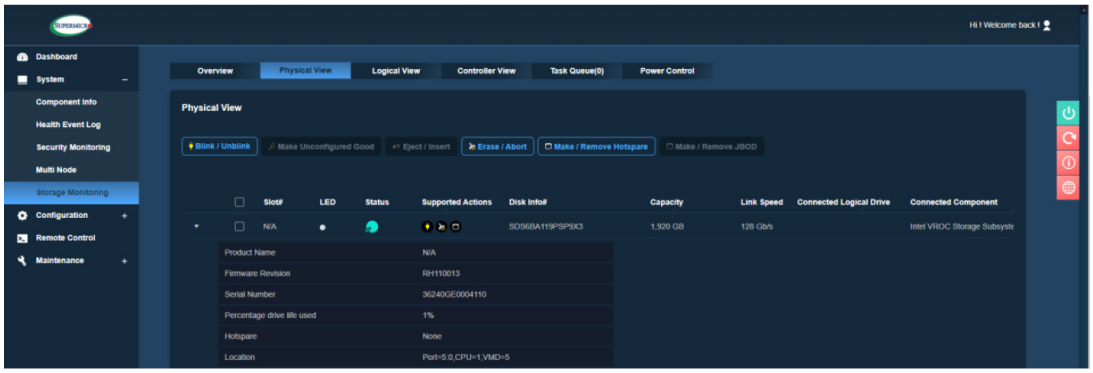


Figure 2-44: Physical Views Action Page

You can perform the following physical actions correlated to each drive:

- Blink: This action is used to locate a physical drive.
- Un-blink: This action is used to stop the blink action.
- Make Unconfigured Good: This action is used to select an unconfigured drive to make an unconfigured good drive.
- Insert: This action is used to insert a new NVMe drive if the VMD mode is disabled.
- Eject: This action is used to eject an existing NVMe drive if the VMD mode is disabled.

- Erase: This action is applied to erase the drive connected with the Broadcom 3108 controller. It allows you to instantly and securely render data on attached drives.

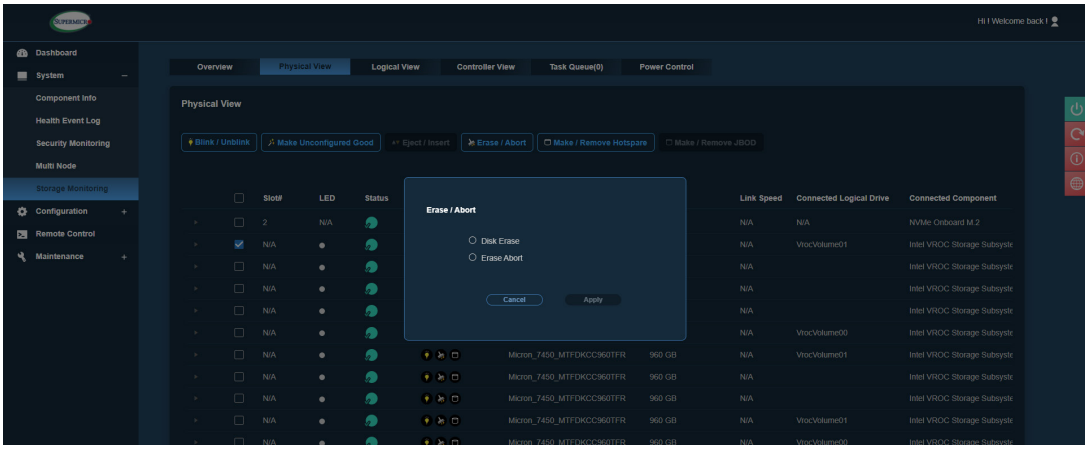


Figure 2-45: Physical Views Action Page

- Make Hotspare: This option is used to assign a spare drive that will automatically replace a failed dedicated or global drive. This will allow the system to continue operating without data loss.
- Remove Hotspare: This option is used to remove the spare drive.

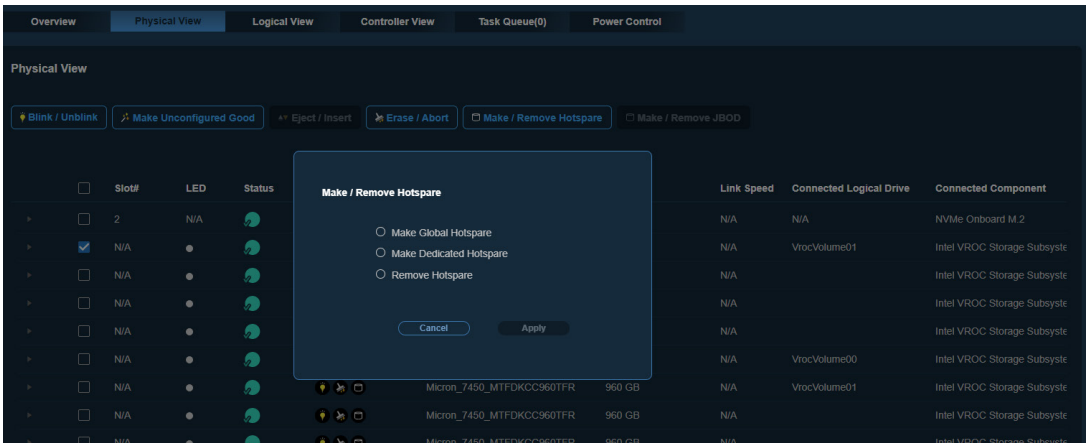


Figure 2-46: Physical Views Action Page

- Make JBOD: This option is used to make a JBOD pool out of the selected drives.
- Remove JBOD: This option is used to remove the selected drive from the JBOD pool.

The following table provides details on which storage controller is supported. In X12 and later motherboards, BMC users can select more than one NVMe drive at a time. Therefore, the Eject and Insert buttons would appear whether VMD is enabled or disabled. If there is only a SATA drive connected to the Broadcom storage controller, the Eject and Insert buttons will not appear.

Table for Supported Controller(s)					
	Blink	**Unblink**	**Make Unconfigured Good**	**Eject**	**Insert**
Broadcom	Supported	Supported	Supported	*Not supported*	*Not supported*
Marvell (88NR2241)	*Not supported*				
NVMe	*Supported*	*Supported*	*Not supported*	Not supported if NVMe is in VMD mode	Not supported if NVMe is in VMD mode

Table for Supported Controller(s)		
	Disk Erase	**Erase Abort**
Broadcom	Supported only for Broadcom Mega RAID controllers such as: AOM-S3808NI-4NM AOM-M3808NI-4HM AOCS3108L-H8IR, AOC-S3908L-H8IR(-16DD/-32DD), AOC-S3916LH16IR(-32DD). AOC-S4116L-H16IR-16DD/-96DD AOC-SMG4-2M2 AOC-SMG4-2E1S AOC-SLG4-2H8M2 AOC-S3808L-L8iR AOC-S3816L-L8iR AOC-S3816L-L16iR	Supported only for Broadcom Mega RAID controllers such as: AOM-S3808NI-4NM AOM-M3808NI-4HM AOCS3108L-H8IR, AOC-S3908L-H8IR(-16DD/-32DD), AOC-S3916LH16IR(-32DD). AOC-S4116L-H16IR-16DD/-96DD AOC-SMG4-2M2 AOC-SMG4-2E1S AOC-SLG4-2H8M2 AOC-S3808L-L8iR AOC-S3816L-L8iR AOC-S3816L-L16iR
Marvell (88NR2241)	*Not supported*	
NVMe	*Not supported*	*Not supported*

Logical View

This page shows the details about virtual drives created with the respective physical drives in the storage subsystem. Depending on the system configuration and selected available components, the available actions will be different.

Note: The function of button(s) will be grayed out if the function(s) is not available. For instance, the LED blinking button will be disabled and grayed out if the connected drive does not possess the capability.

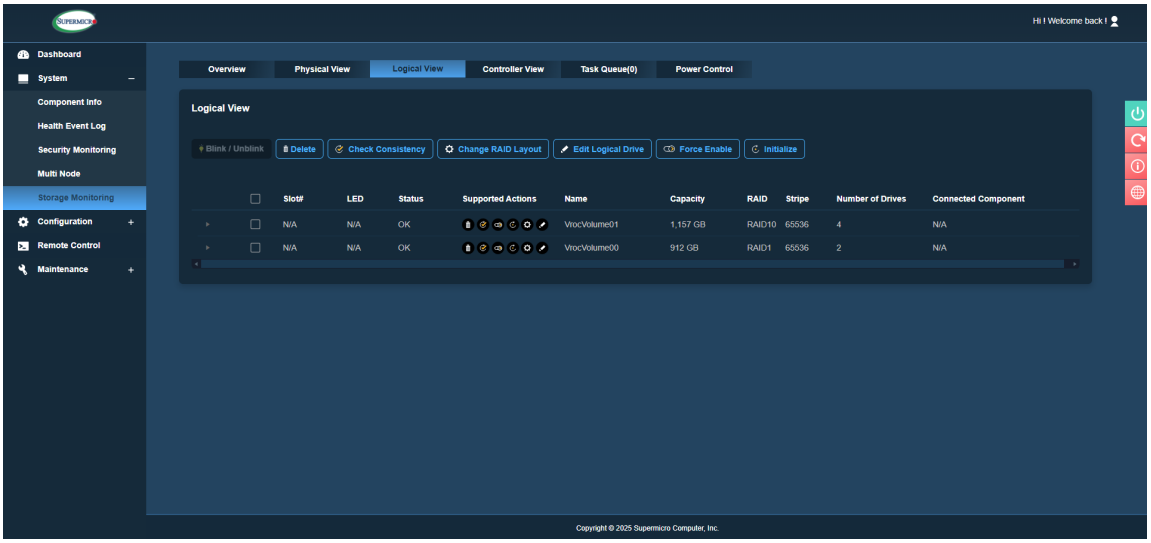


Figure 2-47: Logical View Page

You can view the following information:

- Slot Number: This will display the slot information of the logical drive.
- Status: This will display the logical disk state info (Offline/Partially Degraded/Degraded/ Optimal/Foreign, etc.).
- Blink: This will display the blinking status of the disk.
- Name: This will display the given name of the logical drive.
- Capacity: This will display the capacity of the logical drive (GB).
- RAID: This will display the configured RAID level.
- Stripe: This will display the stripe level of the logical drive.
- Number of Drives: This will display the number of drives connected to a logical drive.
- Connected Component: This will display the connected component.

Logical View Actions

All logical view actions are available and applicable based on the selected drive. You can perform the following actions correlated to each drive:

- Blink: This will cause the drive to blink so you can locate the virtual disk.
- Unblink: This will cause the drive to stop blinking/dislocate the virtual disk.

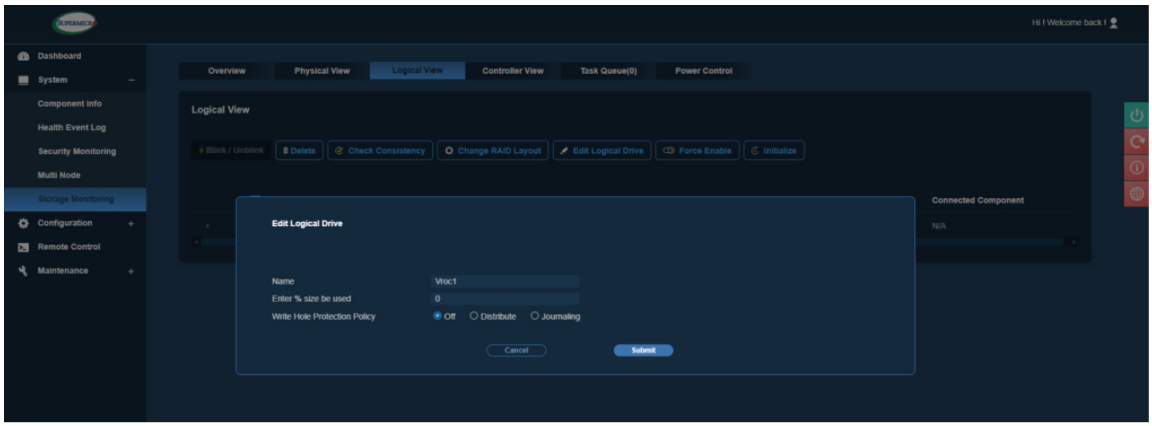


Figure 2-48: Edit Logical Drive Window

- Delete: This will delete the virtual disk.
- Check Consistency: This verifies the data and parity consistency across the selected logical drive.

- Change RAID Layout: This allows you to change the RAID type and strip size.

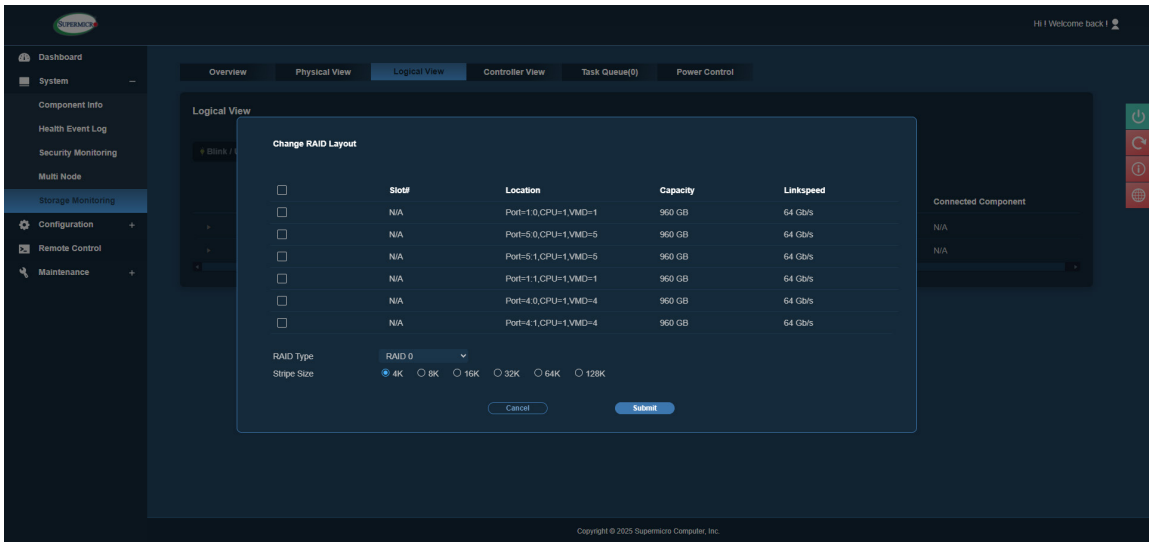


Figure 2-49: Change RAID Layout Window

- Edit Logical Drive: This allows you to modify the logical drive settings, including the name, capacity, and write hole protection policy.
- Force Enable: This allows you to force the activation of the logical drive.
- Initialize: This allows you to initialize the logical drive.

> **Note:** If Change RAID Layout is in progress, other actions will be disabled. The other actions will be enabled upon completion of the Change RAID Layout task.

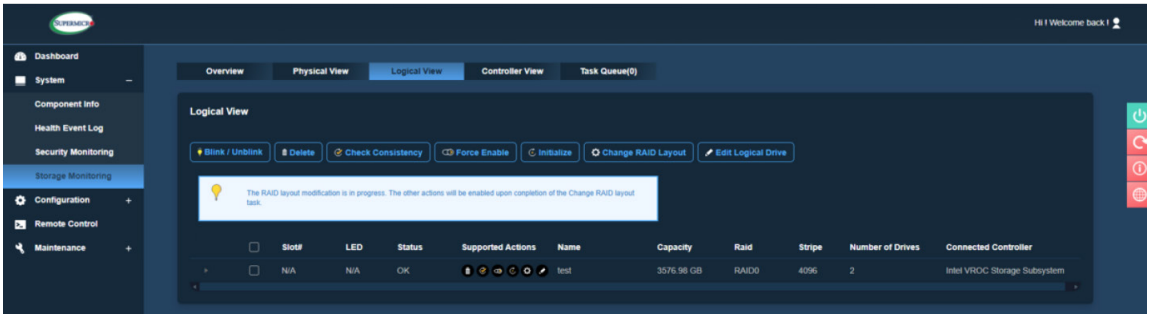


Figure 2-50: Notice For When RAID Layout Modification is in Progress

Controller View

This page shows information about the connected controllers to the system. You can select a device from the dropdown menu to see the details of each controller if multiple controllers are present in the system. Devices will be displayed as the chip name and Device ID (e.g., SAS 3908 Device 0). It displays different controller information and allows you to create RAID and apply changes to Controller actions. BMC supports all RAID levels from the available RAID levels of the manufacturers. For example, if AOC-S3916L-H16IR(-32DD) supports RAID 0, 1, 5, 6, 10, 50, and 60, then BMC will also provide the same RAID levels. Depending on the system configuration and selected available components, the available actions will be different.

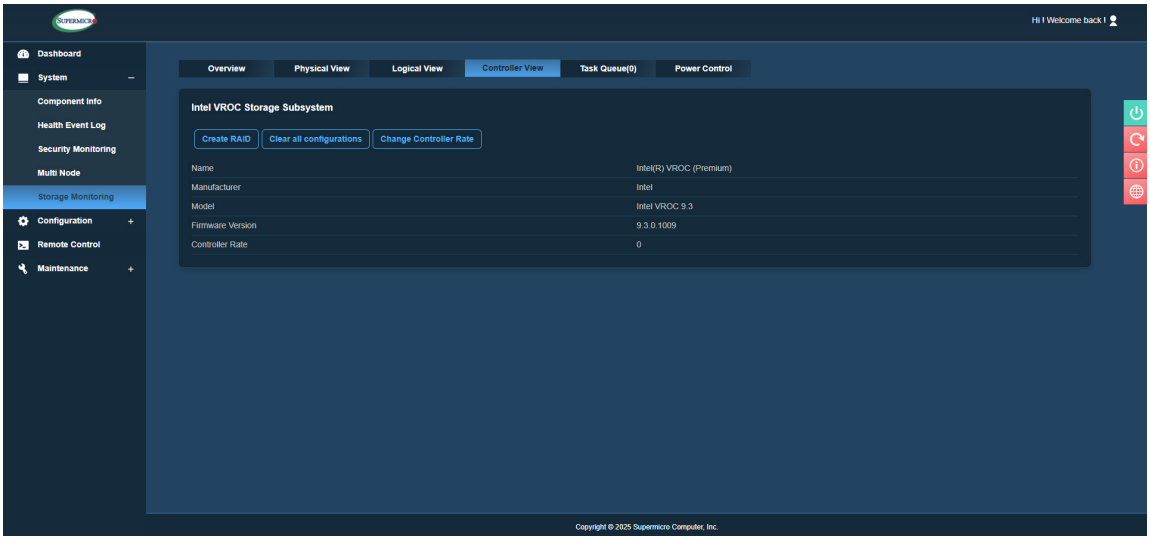


Figure 2-51: Controller View Page

You can see the following collection of configuration and informational data associated with a particular storage controller:

- Controller Name
- Controller Status
- Product Name
- Product Revision
- SPDM Authentication
- Location

- Link Speed (Protocol)
- PCIe Link Width
- Firmware Package Version
- Firmware Version
- BIOS Version
- SAS Address
- Serial Number
- Vendor ID
- Device ID
- SubVendor ID
- SubDevice ID
- Battery Status
- BIOS Boot Mode
- Manufacturer Date (Timestamp)
- Batch Number

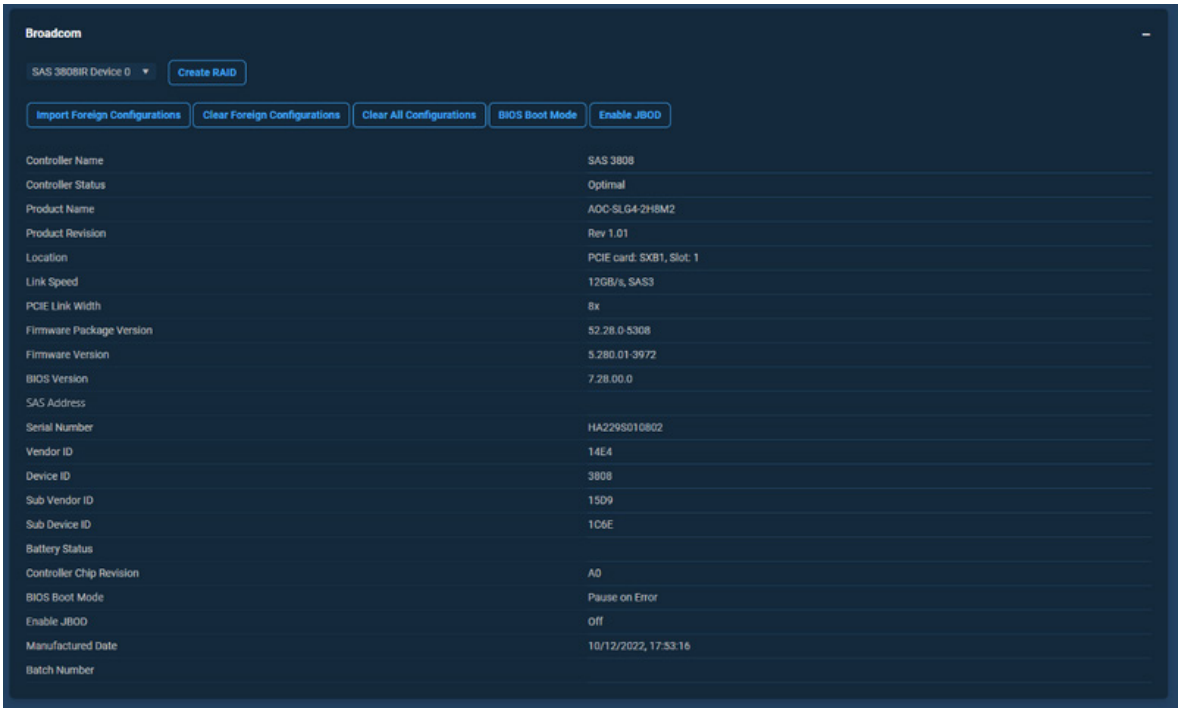


Figure 2-52: Controller View Page

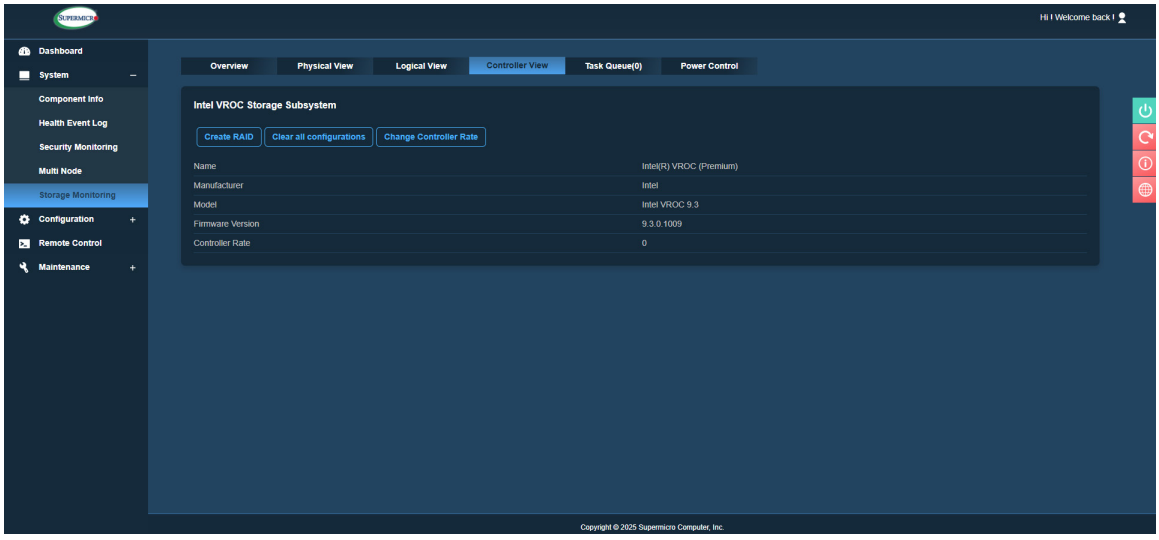


Figure 2-53: Controller View Page

Controller View Actions

All controller actions are available and applicable based on the selected drive.

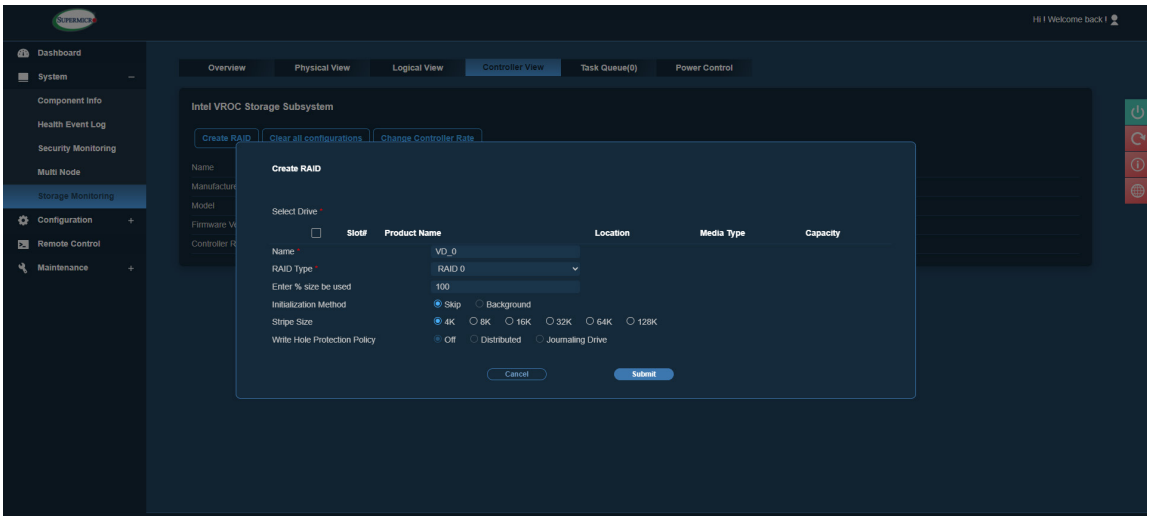


Figure 2-54: Create RAID Submenu

You can perform the following controller actions correlated to each drive:

- Create: This allows you to select available physical disks and add configuration options, such as the RAID level, capacity, name, stripe size, R/W policy, access policy, initialization state, etc. When you want to confirm your configuration, select Submit to create the controller.
- Add [Select Group]: This allows you to select or add a logical drive to the existing group.

Create RAID

You can perform the following actions to create and configure RAID:

Note: Available actions will change based on the selected controller and configuration.

- Import Foreign Configurations: This allows you to import foreign RAID configurations.
- Clear Foreign Configurations: This allows you to clear foreign RAID configurations.
- Clear All Configurations: This allows you to clear all current configurations.
- BIOS Boot Mode: This allows you to select one of the following BIOS Boot mode options.
  - Stop on error
  - Pause on error
  - Ignore on error
  - Safe mode on error
- JBOD Mode: This allows you to enable or disable JBOD mode.

Task Queue

This feature allows you to view all actions in the physical view, logical view, and controller. All actions will create a new task that you will then be listed in this queue, along with the task's health status, task name, status, progress, and task message. If you want to find a specific task, you can enter keywords in the search bar. By default, all task types will be selected so that you can view all tasks.

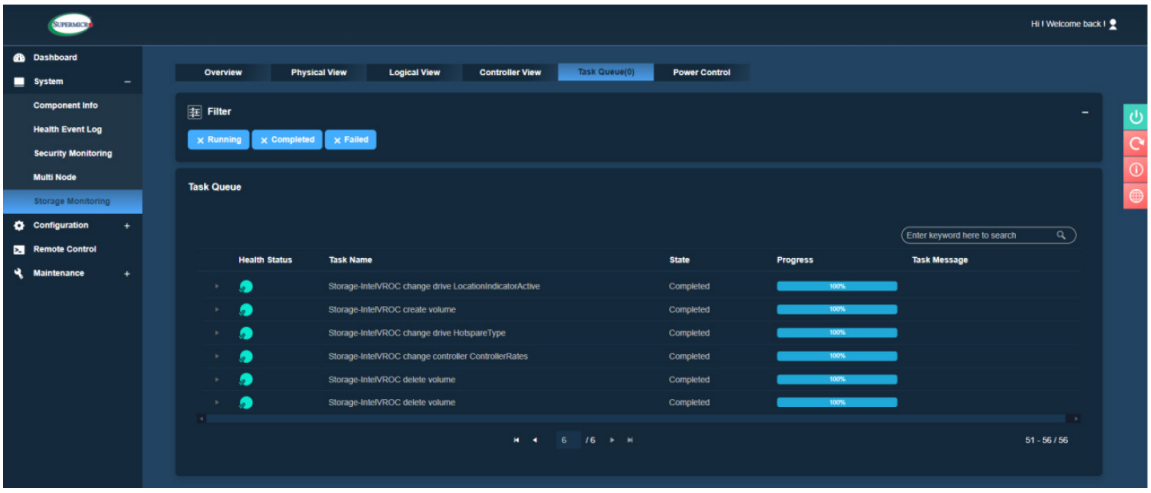


Figure 2-55: Task Queue Page

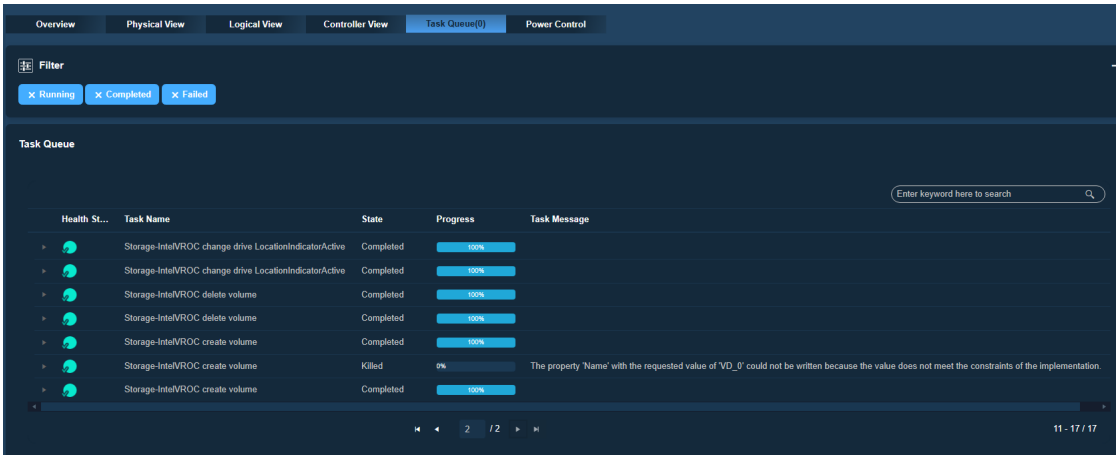


Figure 2-56: Task Queue Dashboard

You can apply filters for event selection based on the following task types:

- Running
- Completed
- Failed

Drive Carrier LED Display

You will need to install the latest version of the Intel® Virtual RAID (Intel® VROC) utility to ensure all components start properly and are able to receive the RAID status signals. To proceed with installing the latest version of the Intel VROC installation application, be sure to obtain and download the latest version of the .NET Framework. The drive carrier LED display will then light up in different colors and blinking patterns to indicate different behaviors and activities for the corresponding drive. The LED blinking blue indicates HDD activity. The red status LED blinking at 1 Hz indicates that the RAID is rebuilding. For further status definitions, consult the following table.

Drive Carrier LED Indicators			
	Color	**Blinking Pattern**	**Behavior for Device**
Activity LED	Blue	Solid On	Idle SAS or NVMe Drive Installed
	Blue	Blinking	I/O Activity
	Off	Off	Idle SATA or No Drive
Status LED	Red	Solid	Failure of Drive with Intel VROC Support
	Red	Blinking at 1 Hz	Rebuild Drive with Intel VROC Support
	Red	Blinking at 4 Hz	Identify Drive with Intel VROC Support
	Red	Blinking with Two Blinks and One Stop at 1 Hz	Hot Spare for Drive with Intel VROC Support
	Red	On for Five Seconds, Then Off	Power On for Drive with Intel VROC Support
	Amber	Blinking	Not to Remove NVMe Drives
	Green	Solid On	Safe to Remove NVMe Drives
	Off	Off	Idle SATA or No Drive

2.5.4 Security Monitoring

This page allows administrators to view the security status of the system. Use this page to enable or disable DMTF Security Protocol and Data Model (SPDM) authentication and view the real-time status of the BMC's security posture. Web UI will generate a System Event Log (SEL) entry whenever a security state alteration occurs (e.g., enable or disable) for any monitored components. Timely updates are integral to this process, and the entry will be created within a 30-second timeframe.

Device Security

SPDM authentication permits an attestor (BMC) to cryptographically confirm SPDM-capable devices are what they say they are. Typically, these devices are add-on cards, CPUs, and storage devices.

- On: Selecting this will enable the SPDM authentication.
- Off: Selecting this will disable the SPDM authentication.

SPDM authentication status is shown in System > Component Info under each component subtab. For example, the network AOC SPDM authentication status will be shown in System > Component Info > Network | PCIe AOC.

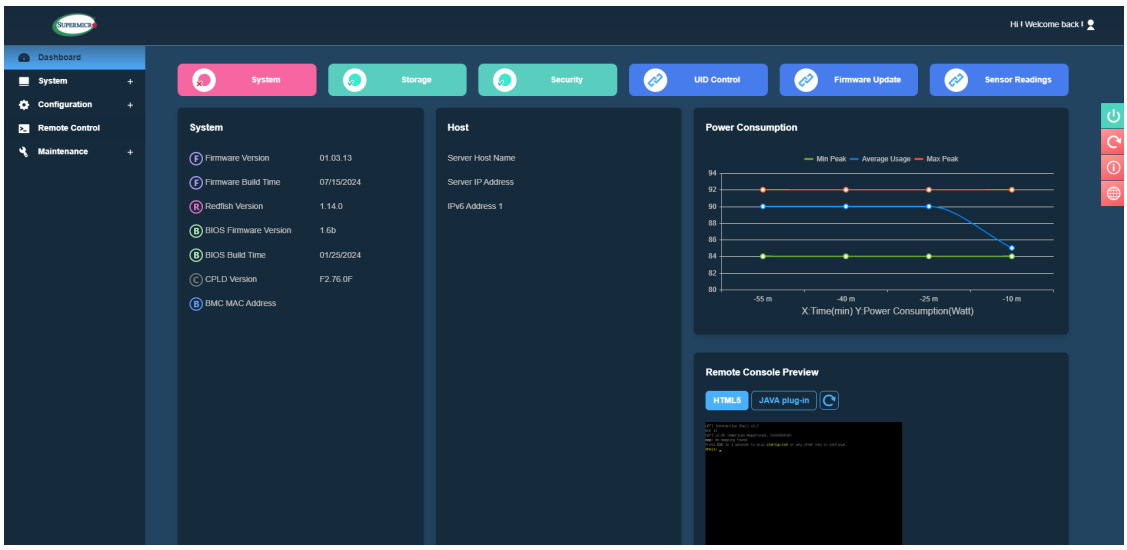


Figure 2-57: Dashboard Page

The green icon denotes that the security status is enabled or validated. The yellow (warning) icon indicates that the BMC Runtime Protection is disabled, deactivated, or cannot be validated. The red (warning) icon indicates that the RoT is deactivated or disabled. You should take action if non-green states are caused by unexpected activities. When the status of the monitored security state changes, SEL will be generated.

State	Green	Yellow	Red	Gray/Not shown
RoT	Root of Trust (RoT) is enabled. Supermicro designates the BMC as the root of trust by having an immutable piece of code with a unique signature to validate each step of the BMC's boot process. The RoT subsystem will identify when any stage of the boot process does not conform to expectations. If any stage of the boot process does not meet expectations, backup or golden images are automatically committed to conform to the policy.	N/A	RoT is deactivated or disabled. Contact Supermicro for further clarification.	N/A
BMC Runtime Protection	BMC Runtime Protection is enabled. The BMC performs runtime checks to ensure its runtime environment is in a secure state by monitoring all running programs. Programs not recognized as authorized are noted in the Health Event Log (SEL).	BMC Runtime Protection is deactivated or disabled. This should not occur unless debug or engineering firmware has been provided. Check the System Event Log (SEL) and Management Event Log (MEL) for relevant entries.	N/A	N/A

	The provisioned device certificate for remote attestation is validated. Remote attestation permits the administrator to extract component measurements installed in the system as a manifest signed by the BMC. A reference manifest is also created during manufacturing and assembly, where it could be used to compare with the current one to ensure no unauthorized changes have occurred between shipment and receipt of the system. Remote attestation manifest comparison requires an SDDC license installed on the BMC and is facilitated through a Supermicro portal and SAA utility. Please contact Supermicro support for further details.	The certificate validation for the provisioned device certificate cannot be validated. This state may be caused by BMC configuration errors, such as an incorrect BMC date/time, leading to a Certificate Path Validation (CPV) error. To resolve, synchronize the BMC's time by enabling NTP or manually setting the BMC date and time. If the warning persists, contact Supermicro for assistance in identifying the root cause.	N/A	N/A

Platform Security

This section displays a view of the system's security state. When the status of any monitored states changes, an alert is created in the Health Event Log (SEL / System > Health Event Log).

2.6 Configuration

This page allows you to perform various configuration settings such as Account Services (user account management and directory services), Notifications (Alert, SNMP, Syslog, and SMTP), Network (IPv4 and IPv6 settings, SSL Certificates, Ports, IP Access Control, and SSDP), Virtual Media (status for connected devices such as Floppy Disk and Virtual CD-ROM), and BMC Settings (Date and Time, Dynamic DNS, SMC RAKP, KCS Control, IPMI Configuration, Host Interface, System Lockdown, and Web Session). Network setting values should be integer values and cannot be negative values.

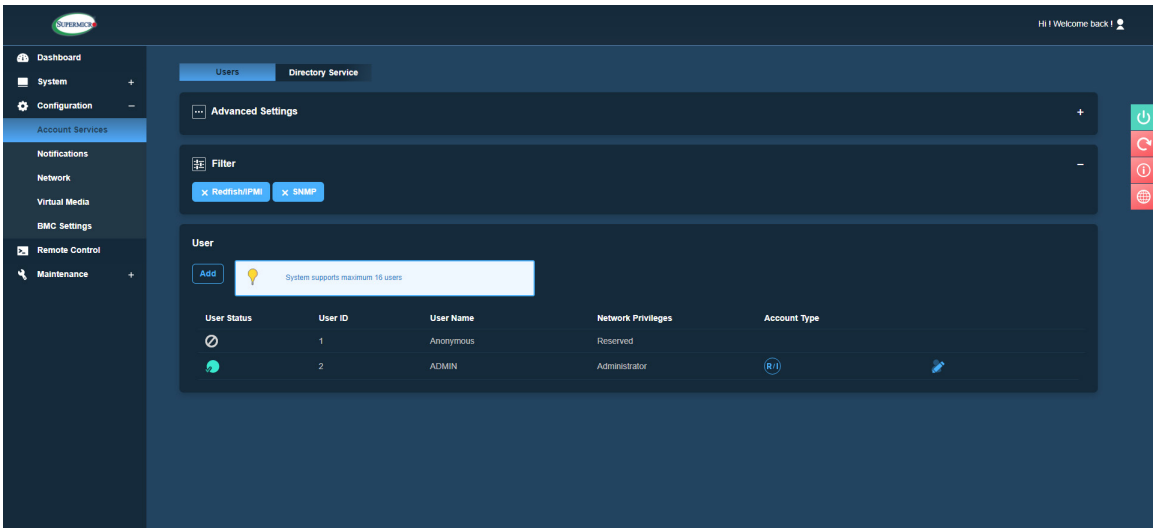


Figure 2-58: Configuration Page

2.6.1 Account Services

Users

This page allows administrators to monitor and configure user accounts for BMC privileges. The Users tab provides the current user information, including User Status, User ID, User Name, and Network Privilege settings. Administrator users can add, delete, or modify settings for all user-access levels and privileges in this tab, as well as control login settings in Advanced Settings. Users with Operator privileges can only modify their own passwords and view the status of other users with Operator and User privileges. If you have User privileges, you can only modify your own passwords and view the status of other users.

- Add New User: If you have Administrator privileges, you can click the [Add] button to add a new user. You can also define User Name, Password, Network Privilege (Administrator, Operator, or User), enable or disable the user account, and set up the Account Type (Redfish/IPMI or SNMP).

  Note: Administrative users can edit, lock, or delete any users from the table except for the default and reserved Anonymous and ADMIN users.

- Authentication Protocol: This field is the radio button with the following options.
  - None
  - HMAC_MD5
  - HMAC_SHA96
- Encryption Protocol: This field is the radio button with the following options.
  - None
  - CBC_DES
  - CFB128_AES128
- Authentication Key: This field is required when you select the Authentication protocol HMAC_MD5/HMAC_SHA96.
- Encryption Key: This field is required when you select the Authentication protocol CBC_DES/CFB128_AES128.

User Table

The user table displays the following details about each user:

- User Status: This feature indicates whether the user login is enabled, disabled, or locked. The green icon indicates that the corresponding user account is enabled, and the gray icon indicates that it is disabled or locked.

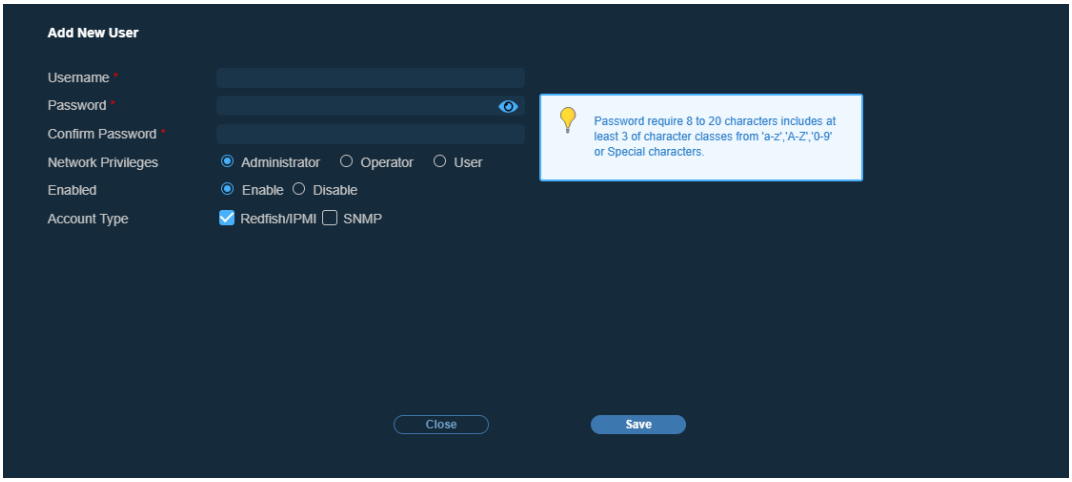


Figure 2-59: Add New User Section

- User ID: This feature indicates the ID number used to identify the configured users. BMC manages user access through unique IDs. It supports a maximum of 15 configurable user accounts, with one reserved for anonymous access (restricted use). This allows for up to 16 concurrent login sessions for authorized users.
- User Name: This feature shows the list of current users.
- Network Privilege: This feature will indicate one of the following types of privilege levels assigned to users.
  - Administrator
  - Operator
  - User
- Pencil Icon (Modify User): Administrator users can modify any other user account except the default administrator account (the default ADMIN user).

- Delete Icon (Delete User): Administrator users can delete any user account except the default administrator account (the default ADMIN user). User accounts that are not in use can be deleted, but you cannot delete any user accounts that are being logged into. There will be a prompt to alert the administrator users if such an action is attempted.
- Password Requirements: You can preview the password by clicking on the eye icon.
  - Required password length is eight to 20 characters.
  - Password cannot be the reverse of the username.
  - Password must include characters from at least three of the listed character classes. Allowed character classes include the following:
    - a through z
    - A through Z
    - 0 through 9
    - Special characters

Note: The maximum number of user profiles that can be created and exist at a time is 16.

Figure 2-60: Password and Confirm Password Text Fields

Advanced Settings

You can perform the following actions to configure advanced settings:

- Failed Login Lockout Control: The **On** or **Off** status indicates whether the Account Lockout control for the User Account is enabled or disabled. If enabled, the user account will be locked due to excessive failed login attempts.
- Failed Login Attempt Lockout Threshold: The user account will be locked out after this number of consecutive failed login attempts in less than the Failed Login Counter Reset time. The allowed range is from one to five attempts. If the value is zero (0), there is no limit on the number of failed attempts allowed.
- Failed Login Counter Reset: This is the count reset. The count of consecutive failed login attempts will be reset after this interval without a failed login attempt. If it is set to “Never," the Failed Login Lockout Controls will be disabled. The counter is also reset upon successful login.
- Account Lockout Duration: This indicates the amount of time you will be locked out (unable to log in) after failing the number of login attempts specified in the Failed Login Attempt Lockout Threshold setting. If it is set to “Never," the Failed Login Lockout Controls will be disabled.

Directory Services

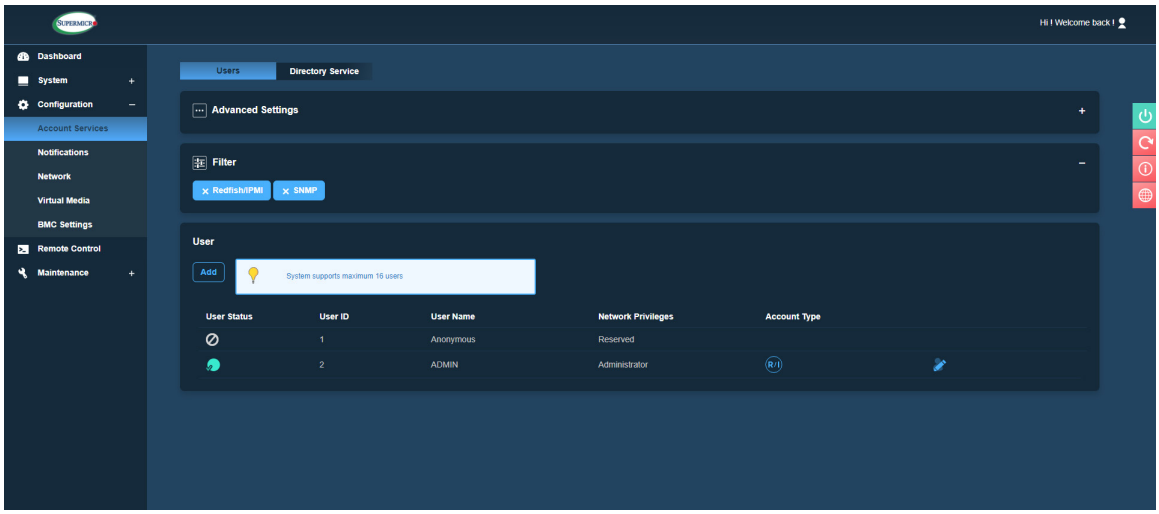


Figure 2-61: Directory Services Page

Settings

You can use this page to configure either LDAP, Active Directory, or RADIUS directory services by toggling the ON/OFF button in any of the directory services to enable or disable the service.

Note: You can only enable one directory service at a time.

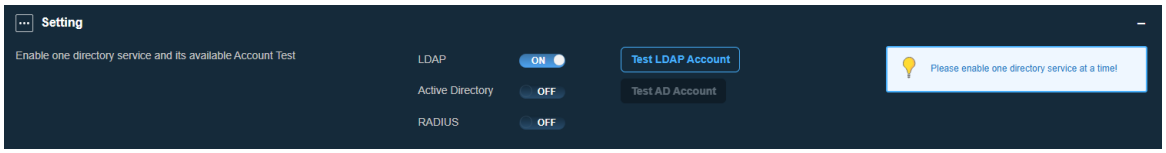


Figure 2-62: Directory Services Setting

Lightweight Directory Access Protocol (LDAP)

Lightweight Directory Access Protocol (LDAP) allows you to view and configure LDAP authentication by logging in to BMC Web UI or accessing Redfish API. This page displays a list of role groups, their group IDs, group names, domains, and network privilege settings.

Note: You can configure the following settings only after enabling LDAP service.

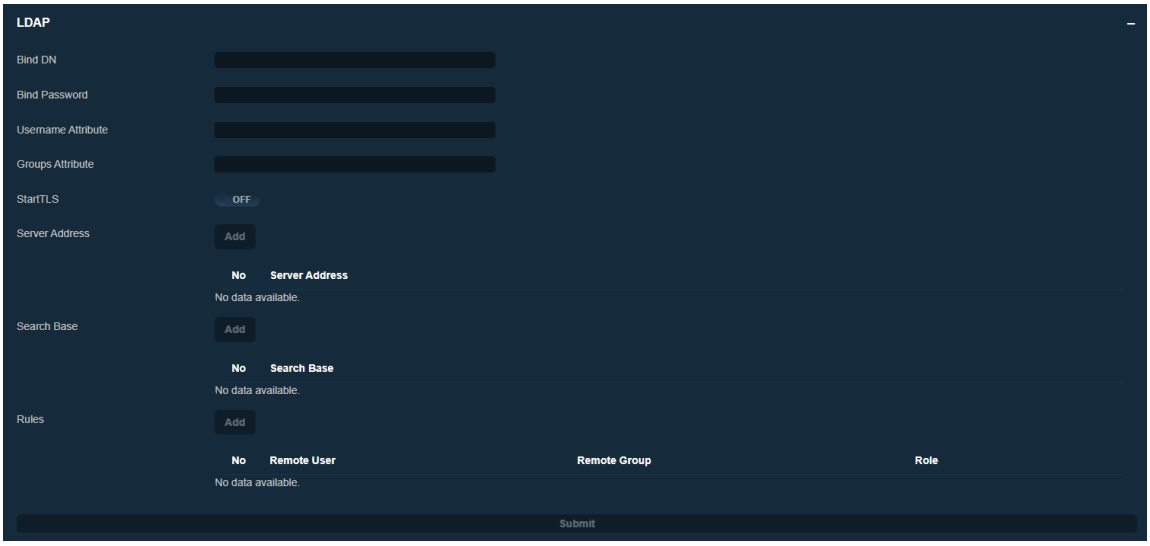


Figure 2-63: LDAP Section

- Bind DN: This feature refers to the bind Distinguished Name (DN), which is the username or the LDAP server that is permitted to search in the LDAP directory within a defined search base. For example: cn=admin,dc=example,dc=com.
- Bind Password: This feature refers to the bind password for LDAP server authentication. Passwords can be previewed by clicking the eye icon button.

  Note: By default, the password characters are hidden under periods or dots (…).

- Username Attribute: This feature is used to enter the username login attribute.
- Groups Attribute: This feature is used to enter the group membership attribute.
- Server Address: This section is used to enter up to three addresses for the LDAP server. Click on [Add] to add server addresses.
  - Prefix — Select to use LDAP or SSL LDAP (ldap:// or ldaps://).
  - IP Address or Domain Name — Select to enter the server IP or domain name. When creating a name, refer to the character check rules. If the user entry does not match

the character rule, an info message will appear saying, *"Invalid IPv4/IPv6 address or domain name!"*

- Port Number — Enter the number of the LDAP server. The default port number for LDAP is 389, and the default for SSL LDAP is 636. You can edit or delete the current settings.

- Search Base: Search base is the distinguished name used to search an external LDAP service. Click on [Add] to add search base values. You can enter up to three search base values as well as edit or delete current settings.

- Rules: You can enter up to five rules. Click on [Add] to configure the following settings.

  - Prefix — Choose to use either LDAP or SSL LDAP (ldap:// or ldaps://).

  - Role — Select the privilege level for a user or role group (Administrator, Operator, or User).

  - Remote User — Enter the LDAP username.

  - Remote Group — Enter the name of the LDAP group. For example: cn=PowerUsers, ou=Groups, dc=example, dc=org.

Active Directory

This page allows you to view and configure Active Directory (AD) authentication. Using the credentials, Active Directory users can also use their credentials to log in to BMC UI and Redfish API to update or delete current directory settings. You can obtain Active Directory server addresses by DNS Lookup or by entering the directory server IP address.

Note: You can configure the following settings only after enabling the AD service.

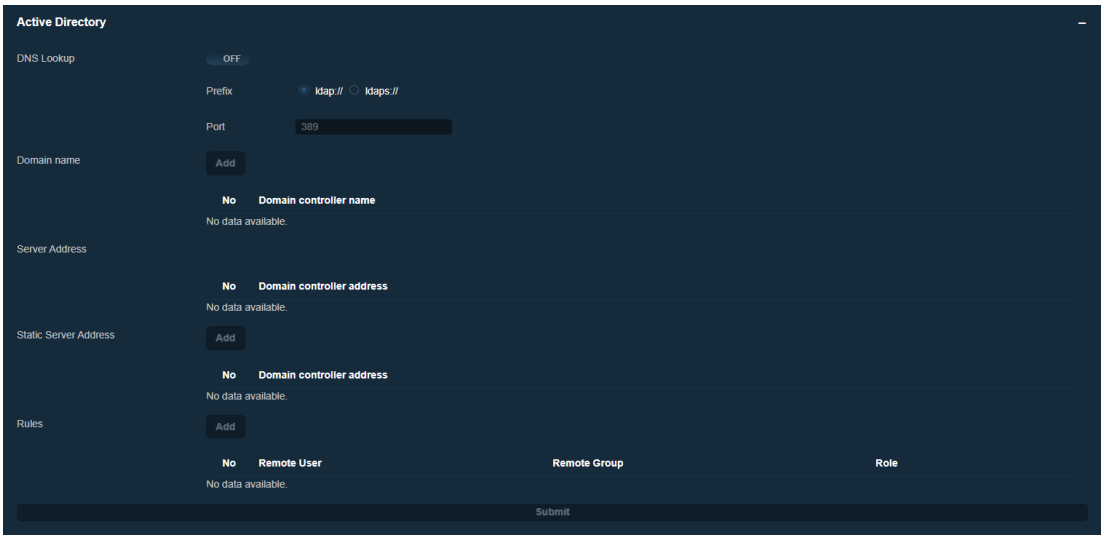


Figure 2-64: Active Directory Section

- DNS Lookup: This field can be used to turn on DNS Lookup to allow BMC to add Active Directory servers through LDAP or LDAPS protocol.
- Domain Name: This field can be used to add up to five domain names to the Domain Name list for Active Directory servers.
- Server Address: This is a read-only field that shows up to three addresses for the Active Directory server(s).
  - Prefix — Select to use LDAP or SSL LDAP (ldap:// or ldaps:///).
  - IP Address or Domain Name — Enter the server IP or domain name.
- Port Number: This field displays the port number of the server.
- Static Server Address: This field can be used to add up to three static server addresses instead of getting Active Directory Server Addresses from the DNS Lookup for the Active Directory servers.

- Prefix — Select to use LDAP or SSL LDAP (ldap:// or ldaps:///).
- IP Address or Domain Name — Enter the server IP or domain name.
- Port Number — Enter the port number. Values range between 1 and 65535 (half-width).

- Rules: In this field, you can enter up to five rules for Role, Remote User, and Remote Group. Click on [Add] to add rules and enter values into the following fields.
  - Roles — Select one of the following privilege levels for that user or role group.
    - Administrator
    - Operator
    - User
  - Remote User — Enter the AD/LDAP username.
  - Remote Group — Enter the name of the AD/LDAP group folder.

Note: You must click on the **<Submit>** button to allow BMC to make changes to Active Directory settings.

RADIUS

This page allows you to view and configure RADIUS authentication. You can also edit or delete the current settings.

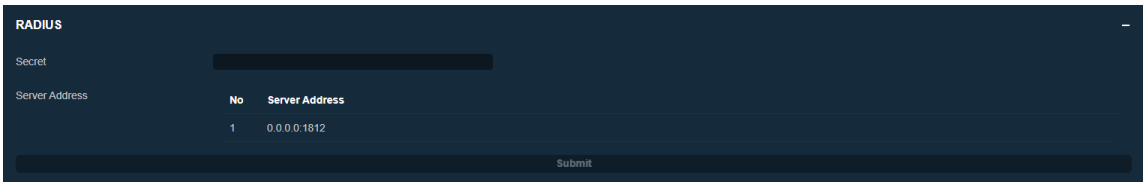


Figure 2-65: RADIUS Section

The Alerts table will display the following information:

- Secret: This field is used to enter a bind password for you to access the RADIUS server. The password can be previewed with the eye-icon button.
- IP Address or Domain Name: This field is used to enter the server IP or Domain name.
- Port Number: This field is used to enter the port number. Values range between 1 and 65535 (half-width).

2.6.2 Notifications

Use this page to configure alerts for remote management using SNMP, Syslog, and SMTP.

Alerts

You can use this page to configure the alert policies used for sending the event(s) out to the predetermined destination. This alert will be sent out through HTTP or HTTPS to a web service that is subscribed to the service.

Note: Must use half-width characters (e.g., English letters and numbers) when entering data into the textbox. You will encounter expected errors when using full-width characters.

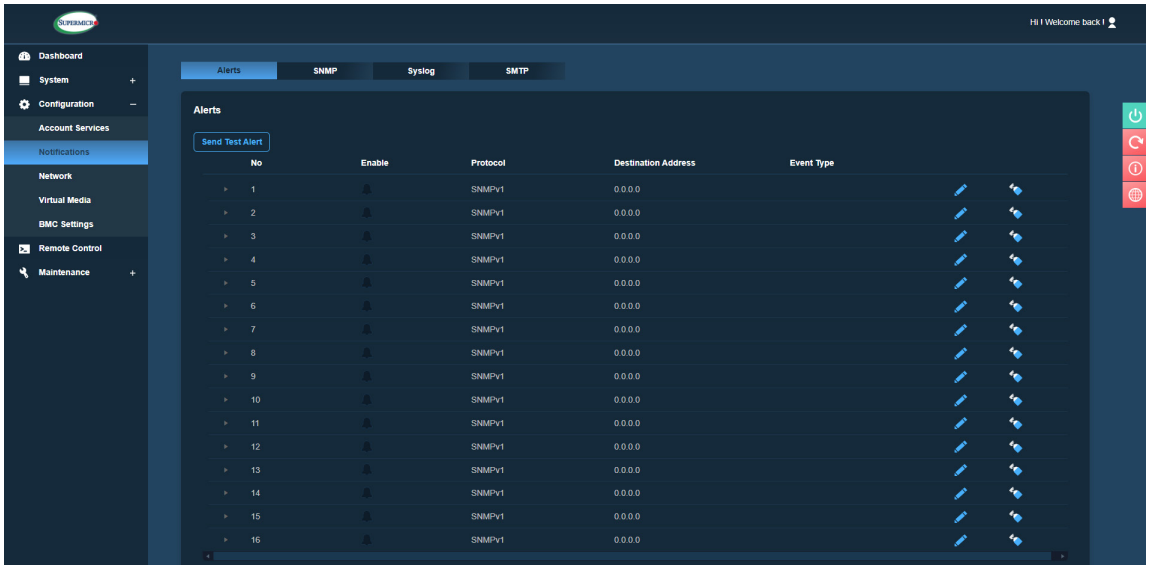


Figure 2-66: Alerts Page

The Alerts table will display the following information:

- No: This field shows the number of available alert entries.
- Enable: This field shows whether the alerts are enabled or disabled with the and bell icons.
- Protocol: This field shows the supported protocol being set for the particular alert transmission (e.g., Redfish, SMTP, or SNMPv1).
- Destination: This field shows the destination address where the alerts will be sent.

- Event Types: This field shows the available configured event types for their respective alerts.
  - Alert
  - ResourceAdded
  - ResourceRemoved
  - ResourceUpdated
  - StatusChange
- Modify: Click on the pencil icon on the row of an alert to configure the settings or make changes to the alert.
- Modify Alert: This field is used to configure the settings for the alert.
  - Enable — Select to enable or disable the alert by clicking on the **ON** or **OFF** button.
  - Protocol — Select one of the following protocol types to set up the alert:
    - SNMPv1
    - SMTP
    - Redfish
    - SNMPv3
  - Severity — Select one of the following severity levels to configure the alert:
    - Information
    - Warning
    - Critical

  Note: This field will only be displayed when SNMPv1, SMTP, or SNMPv3 is selected.
  - Event Type — Select one or more of the following event types if the protocol SMTP or Redfish is selected. Alert protocol will be preset if SNMPv1 or SNMPv3 is selected.
    - Alert
    - ResourceAdded

  - ResourceRemoved
  - ResourceUpdated
  - StatusChange
- Destination Address — Enter an IPv4 or an IPv6 address where alerts will be sent.

Note: The format for IPv4 or IPv6 should not contain a prefix length.

- Message — Enter a message to send out to the destination. This field is available when the SMTP protocol is selected. This field is required prior to saving the configuration.
- Context — Enter a message string to send out to the destination.

Note: This field is required for Redfish protocols. You must fill in the required context field for Redfish protocols.

- Subject — You must provide content for the Subject field. This field is only available for the SMTP protocol.

Note: This field is displayed only when SMTP is selected and required for the SMTP protocol. The protocol also requires you to fill in the Subject field.

- Trap Community — Enter information for traps.

Note: This field is only displayed when SNMPv1 is selected.

- Delete — You can delete the respective alert by clicking on the trash can icon.

You can click on [Test Information Alert], [Test Warning Alert], and [Test Critical Alert] to check if the alerts have been set and sent out correctly. Respectively configured alerts will be sent out for testing purposes. Clicking 'Test Information Alert, 'Test Warning Alert,' and 'Test Critical Alert' would trigger the enabled and associated Alerts.

SNMP

Use this page to configure the SNMP settings. You can choose either SNMPv2 or SNMPv3 as the protocol for communicating with the SNMP client program.

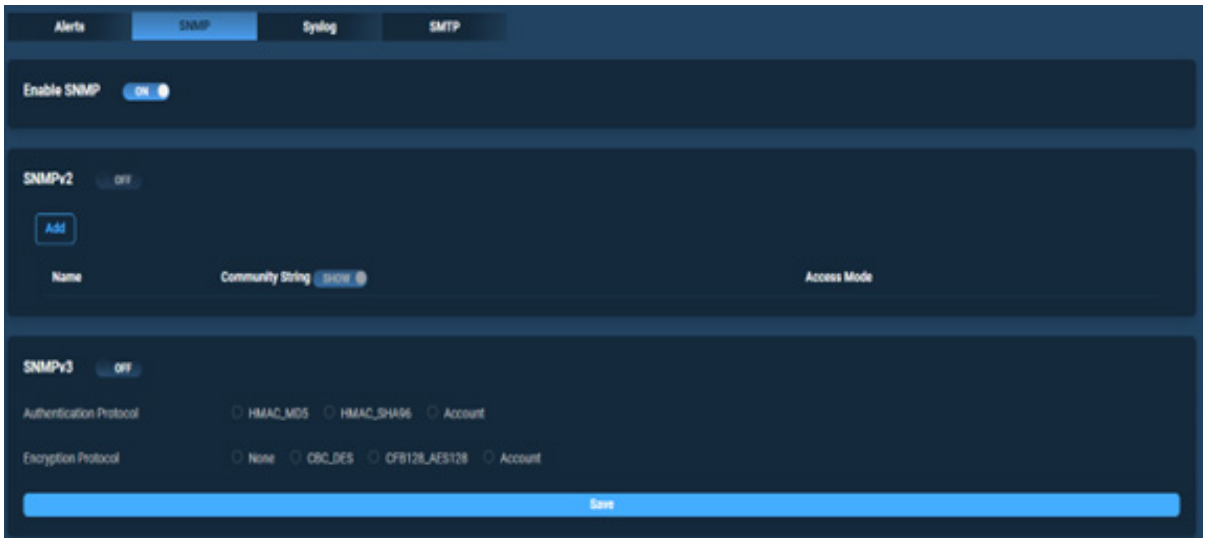


Figure 2-67: SNMP Section

To configure SNMP settings, refer to the following steps:

1. Enable SNMP by toggling the [Enable SNMP] button to ON before choosing the SNMP version.

   Note: By default, enabling SNMP will enable SNMPv1.

2. Once SNMP is enabled, add one or more SNMPv2 Communities by clicking on the [Add] button. You can then add a Community with either Access Mode — ReadOnly or ReadWrite to configure the new Community for SNMPv2. Community String and Name can be left empty and added later on, and you can make changes afterward.

3. To enable SNMPv3, you can select one of the following protocols:

   - Authentication Protocol: You can select either HMAC_MD5, HMAC_SHA96, or Account for Authentication Protocol.
   - Encryption Protocol: You can select either None, CBC_DES, CFB128_AES128, or Account for the Encryption protocol.

4. Click [Save] to save user settings. The saved configurations are to be used whenever you start or stop the SNMP daemon.
5. If you need to change the SNMP port number, you can do so on the Port page.

Note: By default, all SNMP settings are disabled (OFF). Once the SNMP setting is enabled (ON), you can turn on SNMPv2 or SNMPv3 using the ON/OFF toggles. Once SNMP is disabled, SNMPv2 and SNMPv3 will also be turned OFF. No traps will be sent out.

Syslog

This page allows you to configure the Syslog server settings. Before using this feature, ensure that the Syslog server is ready.

Note: This feature requires a software license.

Figure 2-68: Syslog Activitation Warning

To configure the syslog settings, refer to the following steps:

1. Select [Enable Syslog] to turn on Syslog.
2. Enter the address into the Syslog server field.
3. Enter the port number for the Syslog server.
4. Click [Save] to complete the configuration.

Figure 2-69: Syslog Section

Simple Mail Transfer Protocol (SMTP)

This page allows you to configure Simple Mail Transfer Protocol (SMTP) settings for email transmission through the network by selecting the SMTP tab.

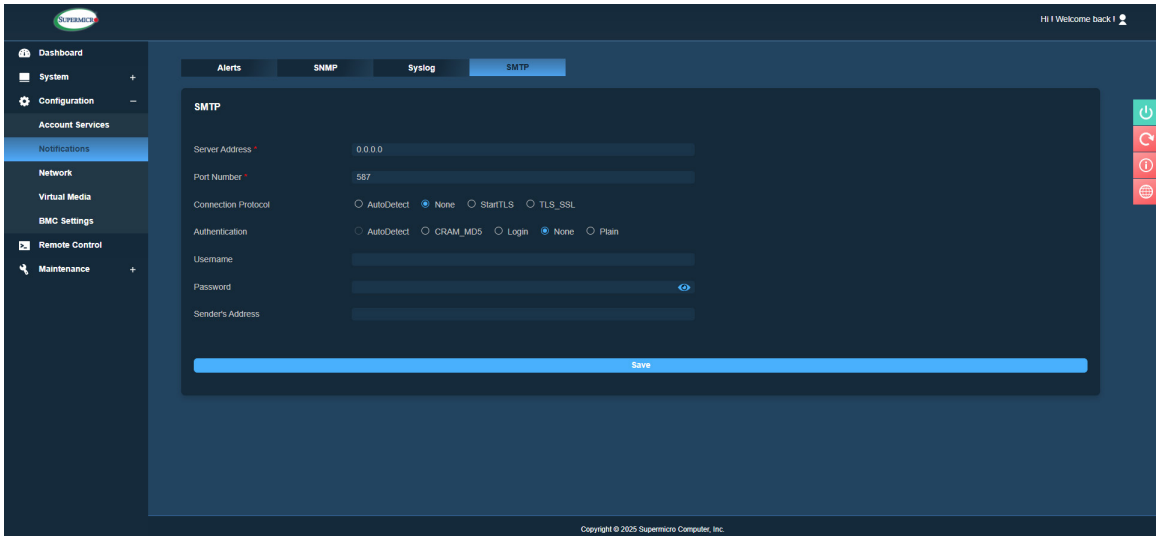


Figure 2-70: SMTP Page

To configure SMTP settings, refer to the following options:

- Server Address: Use this field to enter the address for the SMTP mail server to configure SMTP.
- Port Number: Use this field to enter an SMTP port number. By default, the port number is 587.
- Connection Protocol: Use this field to choose one of the available protocols to set up SMTP authentication.
  - AutoDetect
  - None
  - StartTLS
  - TLS_SSL

- Authentication: You can choose one of the available authentication methods to set up SMTP.
  - AutoDetect
  - CRAM_MD5
  - Login
  - None
  - Plain

  Note: The types of authentication methods that will be available depend on which Connection Protocol is selected. For example, when you choose None as the Connection Protocol, the AutoDetect option in Authentication will be grayed out.

- User Name: Use this field to enter the username for the SMTP mail server. This is optional.
- Password: Use this field to set up the user password if the username is added for the SMTP mail. Passwords can be previewed by clicking the eye-icon button.

  Note: By default, the password characters are hidden under periods or dots (…).

- Sender’s Address: Use this field to add the Sender's address.

  Note: If you enter an invalid email address, you should see the error tip "Invalid Email Address Format."

Once you have completed entering the information above, click [Save] to retain all the settings for the SMTP configuration.

2.6.3 Network

Use this page to configure BMC network settings, such as IPv4, IPv6, SSL Certification, Ports, IP Access Control, SSDP, and LLDP. Network setting values should be non-negative integer values. In addition, both IPv4 and IPv6 ports are ON (enabled) by default.

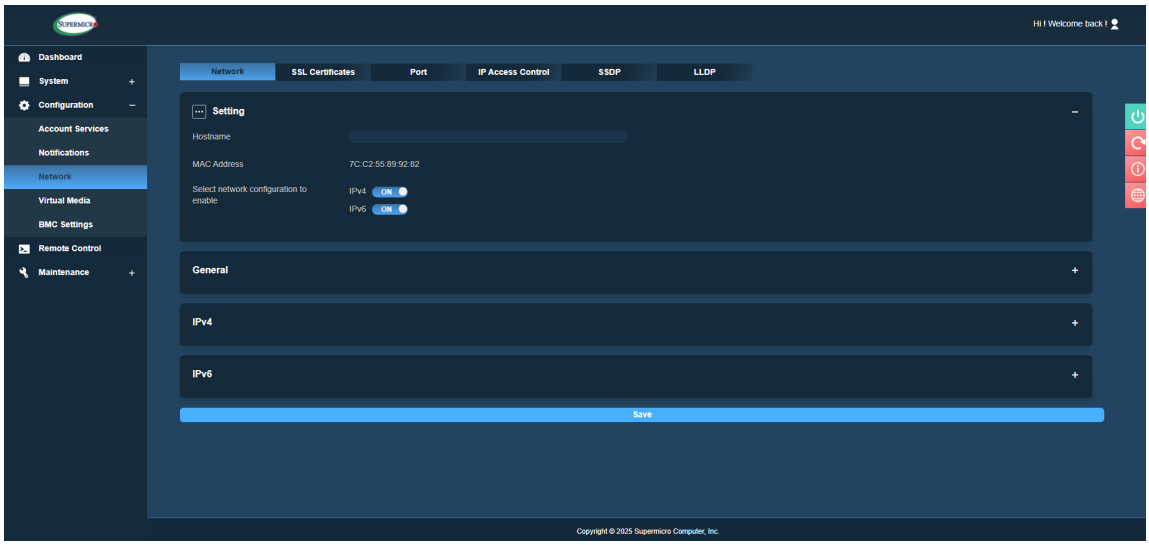


Figure 2-71: Network Page

IPv4

This page allows you to configure the BMC network settings, such as IPv4, IPv6, and BMC LAN connectivity.

Note: Network setting values should be integer values and should not be negative values. Both IPv4 and IPv6 ports are ON (Enabled) by default.

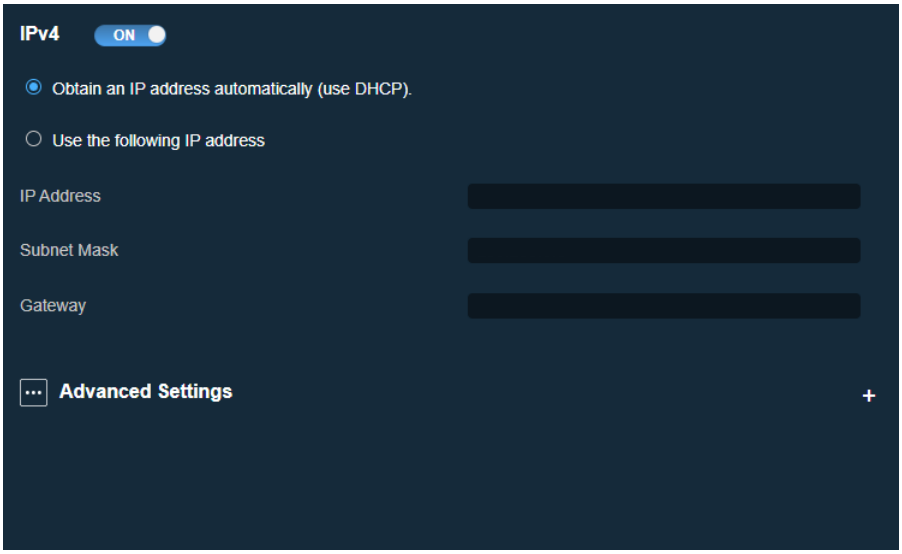


Figure 2-72: IPv4 Section

IPv4 Configuration

Use the following features to configure the IPv4 BMC network settings:

- ON/OFF: This field has the toggle button to enable or disable the IPv4 network connection for BMC.
- Automatically Obtain IP Address (use DHCP): This field gives you the choice to enable automatic IPv4 configuration using Dynamic Host Configuration Protocol (DHCP). This option streamlines the process, allowing the system to dynamically assign and manage IP addresses, enhancing convenience, and encouraging efficiency.

Note: When a hostname is entered and DHCPv4 is enabled, it will automatically be sent to the DHCP server using DHCPv4 Option 12.

- Use the following IP address: This feature gives you the option to configure a static IP address and enter the following details.
  - IP Address — Manually enter the IPv4 address for BMC.
  - Subnet Mask — Enter the IPv4 Subnet Mask value.
  - Gateway — Enter the IPv4 Gateway address into the field.

IPv4 Advanced Settings

Use the following features to configure the advanced IPv4 BMC network settings:

- Auto Obtain DNS Server IP: If enabled, the Domain Name Server (DNS) Server IP Addresses will be obtained automatically.
- Manually obtain DNS Server IP: This field can be used to manually assign a DNS server IP address in IPv4 format.
- DNS Server IP: This field can be used to assign an IP address for the primary DNS Server to retrieve host names from DNS.
- DNS Server IP 2: This field can be used to assign a secondary IP address for the backup DNS Server.

Note: If DNS Server IP Addresses remain unassigned, the string length is 0.

IPv6

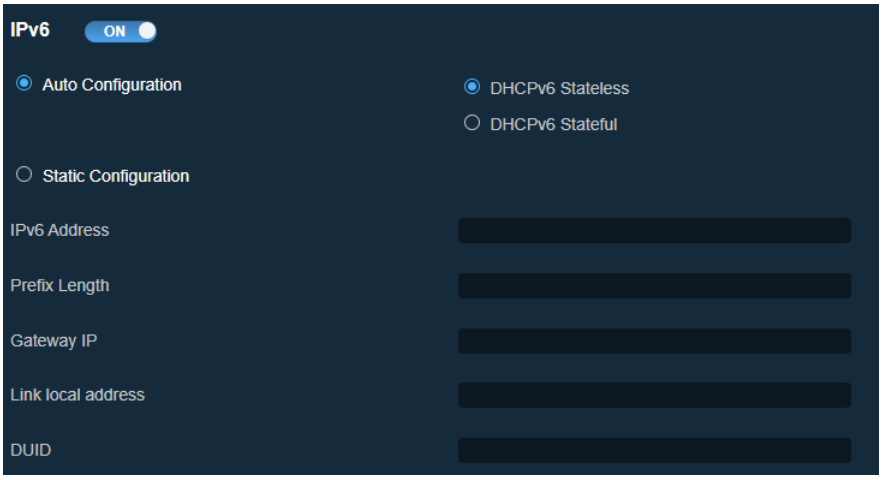


Figure 2-73: IPv6 Section

Use the following features to configure the IPv6 BMC network settings:

- ON: This feature enables/disables the IPv6 network connection for BMC.
- Auto Configuration: This feature allows the BMC to obtain DHCPv6 Stateless or DHCPv6 Stateful.
  - DHCPv6 Stateless: When selected, the BMC will NOT apply the prefix/IPv6 address from the DHCPv6 server. Stateless Address Autoconfiguration (SLAAC) must be enabled for BMC to receive IP addresses when DHCPv6 Stateless mode is selected.
  - DHCPv6 Stateful: When selected, the BMC will apply the prefix/IPv6 address from the DHCPv6 server. Auto Configuration will be disabled when DHCPv6 Stateful mode is selected.

Note 1: When DHCPv6 Stateful is selected and Auto Configuration is disabled, the BMC is unable to get the IPv6 IP Address from the DHCPv6 server unless HOST OS, BMC IP Address, and the DHCPv6 server are on the same network segmentation. Auto Configuration must be enabled (ON) for BMC to receive IPv6 IP address(es) when DHCPv6 Stateful mode is selected.

Note 2: When transitioning from DHCPv6 Stateful or Stateless mode to Static mode, BMC should allocate a new IP address and discontinue the use of its previous IPv6 address.

- Static Configuration: This option allows you to manually enter the IPv6 Address.

  Note: When transitioning from DHCPv6 Stateful or Stateless mode to Static mode, BMC should allocate a new IP address and discontinue the use of its previous IPv6 address.

- IPv6 Address: This option allows you to input the IPv6 Address in the text field.
- Prefix Length: This option allows you to set a prefix length in the text field.
- Gateway IP: This option allows you to set a Gateway IP in the text field.
- Link local address: The IPv6 Address is primarily used for communication on the same local network and is not meant to be routed beyond that network segment.
- DUID: This is the Unit ID for you to get the DHCP IP from the DHCP server. The DUID includes client network information (address, lease time, and DNS server information). This is READ ONLY.

IPv6 Advanced Settings

Use the following features to configure the advanced IPv6 BMC network settings:

- Auto Obtain DNS server IP: To enable this feature, Auto Configuration must be enabled (ON) when you want to enable either DHCPv6 Stateless or DHCPv6 Stateful Mode.
- Manually obtain DNS server IP: This allows you to assign a DNS server IP address in IPv6 form.
  - Preferred DNS server IP: This allows you to input the first choice of DNS server IP in this field.
  - Alternative DNS server IP: This allows you to input the second choice of DNS server IP in this field.

General

In this section, you can set up a name for server identification in Hostname, view the MAC Address, set up the VLAN for BMC, and view current network settings for BMC connectivity.

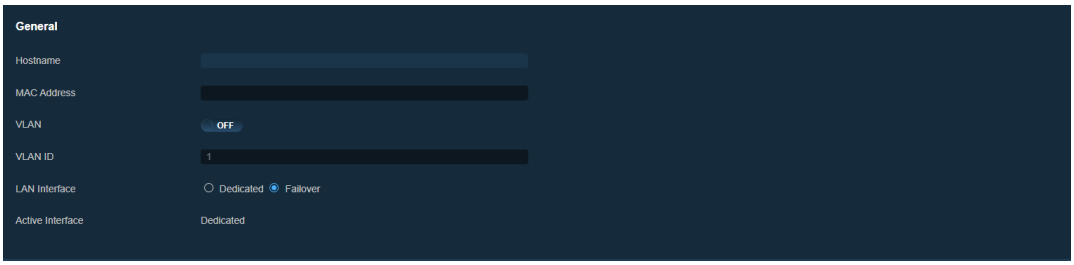


Figure 2-74: General Section

- Hostname: You can enter a name for the server as in Server Identification.

  Note: Hostname must start with a letter and end with a letter or digit. Alphanumerical characters and hyphens are allowed for the interior. Except for hyphens, no special characters are allowed. All hostnames must be 63 characters or shorter in length. If you try to enter more than 63 characters, an info message will appear saying, *"Your hostname is too long. Please shorten it to a maximum of 63 characters."*

- MAC Address: You can view the MAC Address of BMC.
- VLAN: You can enable or disable the Virtual LAN support.
- VLAN ID: You can enter the VLAN ID.

  Note: By default, the VLAN ID is preset to 1 when the VLAN is enabled. If it is decided that VLAN ID should be set to 1, you need to make sure the BMC interface is set to a member of VLAN 1. Otherwise, once the configuration is saved, you would lose access to BMC using OOB unless the BMC interface is connected to a Switch port configured as VLAN 1.

- LAN Interface: You can view and select one of the available LAN interface options.
  - Failover
  - Dedicated
  - Shared

- Shared LAN: You can view and select an available LAN mode.
  - Auto
  - Onboard
  - AIOM
  - AOC

Network mode will DYNAMICALLY display the LAN Interface and Shared LAN options based on the hardware detected in the system. However, the display still follows the alphanumerical order. The LAN Interface options include: Dedicated, Failover, Failover-AOC, Failover-AIOM1, Failover-AIOM2, Shared, Shared-AOC, Shared-AIOM1, and Shared-AIOM2.

Network Mode Table	
Network Combination Mode	**Definition**
Dedicated	"Dedicated" LAN
Shared (Auto Mode)	Onboard Shared LAN or AIOM Shared LAN (if there is no Onboard Shared LAN designed in)
Failover (Auto Mode)	Failover between the first Shared LAN and Dedicated LAN
Shared — Onboard/Onboard1/Onboard2	Onboard Shared LAN; Onboard1 and Onboard2 Shared LAN if there is more than one Onboard LAN
Shared — AIOM/AIOM1/AIOM2	AIOM Shared LAN; AIOM1 and AIOM2 Shared LAN if there is more than one AIOM LAN
Shared — AOC/AOC/AOC1/AOC2	AOC Shared LAN; AOC1 and AOC2 Shared LAN if there is more than one AOC LAN
Failover — AOC	Failover between "Shared — AOC" and "Dedicated"
Failover — AIOM	Failover between "Shared — AIOM" and "Dedicated"
Shared — Onboard	Onboard Shared LAN
Failover — Onboard	Failover between "Shared — Onboard" and "Dedicated"

- Active Interface: You can view the parameter showing the type of LAN interface that is currently selected.
- Link: You can view and select an available link speed.
  - Auto negotiation
  - 100M half-duplex
  - 100M full duplex
  - 1G full duplex

  Note: Link options are only enabled when the LAN Interface is in Dedicated mode.
- Status: You can view the status of the BMC link.
- Speed: You can view the indicated speed of the system link connection.
- Duplex: You can view whether the BMC link is a full or half duplex.

SSL Certificates

This tab allows you to upload custom SSL certificates. Supported SSL Certificate files have the .pem, .cer. , or .crt extensions. The files are in Private Enhanced Mail (PEM) certificate formats.

- Certification Valid From and Until: You can view current SSL certification validity in the grayed-out text boxes.
- New SSL Certificate: You can upload a new SSL Certificate by clicking on the Select File button to select a supported SSL Certificate file.
- New Private Key: You can upload a new private key by clicking on the Select File button.

You can click [Upload] to upload the certificate and the private key to the server. Once uploaded, BMC will reset itself for the new certificate to take effect.

Note: SHA2 and RSA 2048-bit SSL are supported.

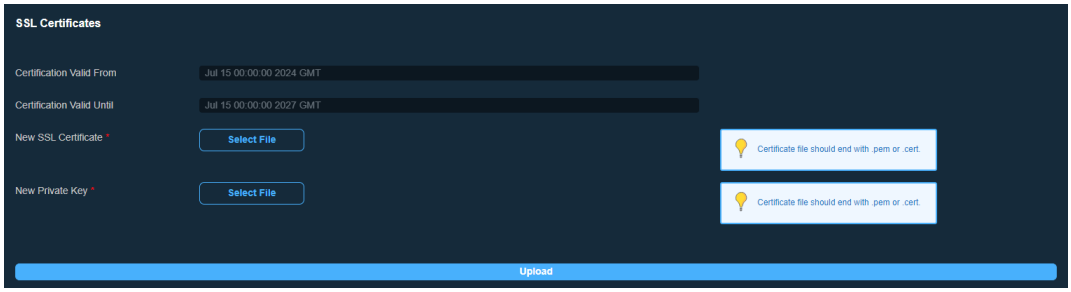


Figure 2-75: SSL Certificates

Port

This tab provides the following ports along with the associated standard port numbers. Most ports can be modified, except the Web SSL Port. You can turn ON individual ports to modify the port number. Click on [Save] to apply changes. The following ports are ON or OFF by default.

The default states and numbers for TCP ports are as follows:

- IKVM Server Port: ON (5900)
- SSH Port: ON (22)
- Web Port: ON (80)
- Web SSL Port: ON (443)
- Virtual Media Port: ON (623)

Note: IKVM server port and Virtual Media Port are not available for Open BMC. For X14 projects with Supermicro OBMC, you do not need to set IKVM and Virtual media port settings.

The default states and numbers for UDP ports are as follows:

- IPMI LAN Port: ON (623)
- SNMP Port: OFF (161)

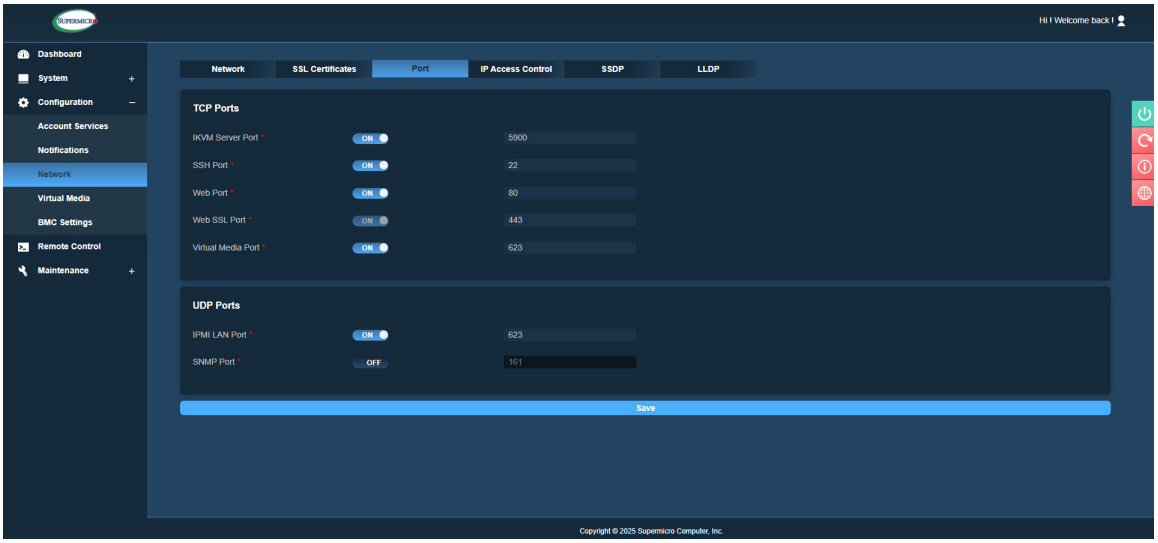


Figure 2-76: Port Page

Once you have finished configuring the settings, click on [Save] to apply changes.

Note: SSL Web Port cannot be configured by users. Doing so will cause a loss of HTTPS communication. SSL Redirection was removed, and SSL Web Port is **ON** and grayed/disabled out by default.

Network General Frame of WebUI

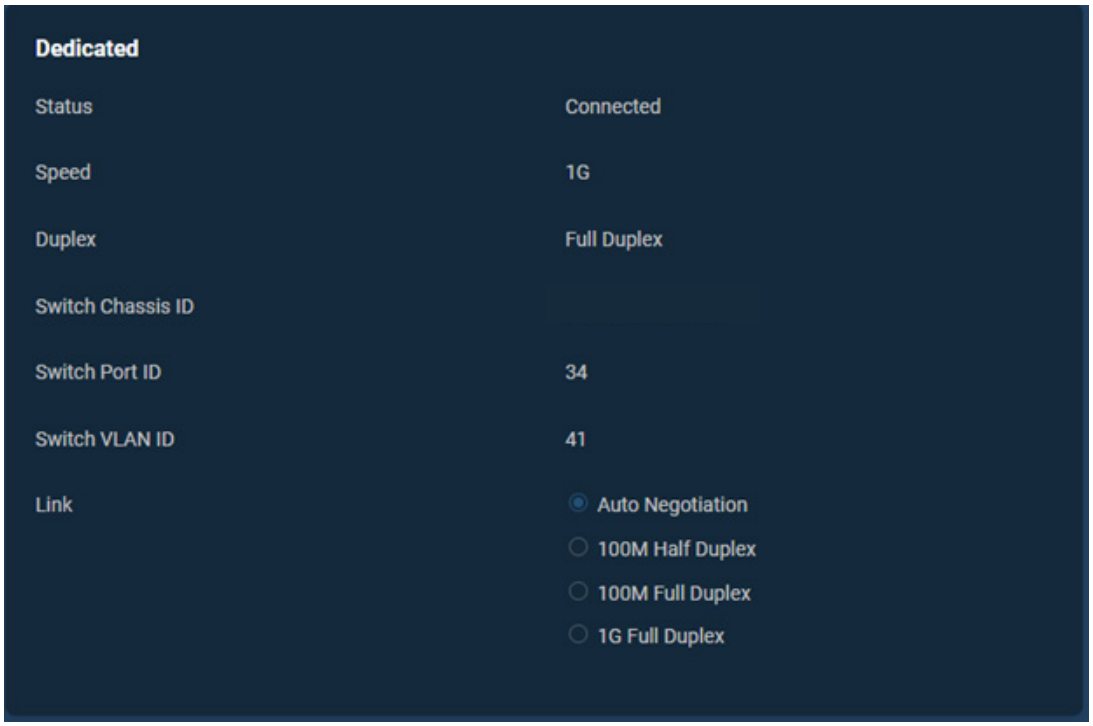


Figure 2-77: LAN Interface When in Dedicated Mode

When the LAN Interface is in Shared mode and connected, the following information will be displayed on Web UI:

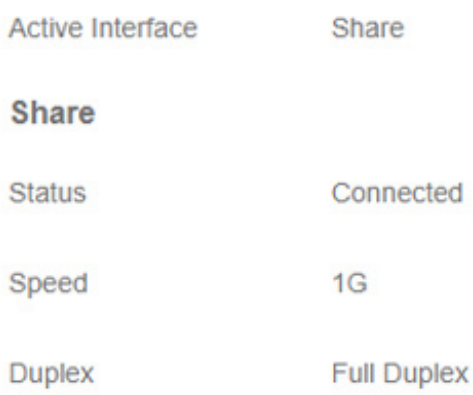


Figure 2-78: LAN Interface in Shared Mode and Connected

Figure 2-79: LAN Interface in Shared Mode and Connected (Dark Mode)

When the LAN Interface is in Shared mode and disconnected, the following information will be displayed on Web UI:

Figure 2-80: LAN Interface in Shared Mode and Disconnected

Note 1: In special motherboards without onboard LANs, AOC NIC information is displayed instead of onboard LANs. Redfish API will retrieve data and provide Web UI display when it comes to displaying LAN Interface.

Note 2: If there is a riser card used to allow an add-on card or AIOM, the BMC will determine if the card is an add-on card or an AIOM by using VPD in the firmware. You must ensure VPD is present to get the correct reading.

Web UI LAN Design for X14 and H14

In 'Shared LAN Auto' mode, the NC-SI Shared LAN defaults to using MAC3. However, if MAC3 becomes unavailable, the BMC will switch to MAC4. Notably, even if MAC3 resumes operation, the system will continue using MAC4. Additionally, the LAN Web UI now dynamically integrates with the Redfish API. In scenarios lacking a dedicated onboard LAN, the system defaults to the Shared LAN. The UI displays only those LAN interfaces that are active and available while hiding inactive or unavailable ones. It's important to note that Auto Mode is the default setting. If only one LAN option is available, Auto Mode becomes disabled and will appear grayed out.

When the onboard LAN is available, the following options will be shown:

- LAN Interface
  - Dedicated
  - Shared
  - Failover
- Shared LAN
  - Auto Mode
  - Onboard
  - AIOM
  - AOC

When the onboard Dedicated and/or Failover LAN is absent, the following options will be shown:

- LAN Interface
  - Shared
  - Failover
- Shared LAN
  - Auto Mode
  - AIOM
  - AOC

IP Access Control

Use this page to configure the IP access control policy. You can set up to 10 rules on this page for either the IP Access Control List.

Note: The default policy is OFF (disabled), and the default rule is ACCEPT. You can set up rules using either IPv4 or IPv6 IP addresses.

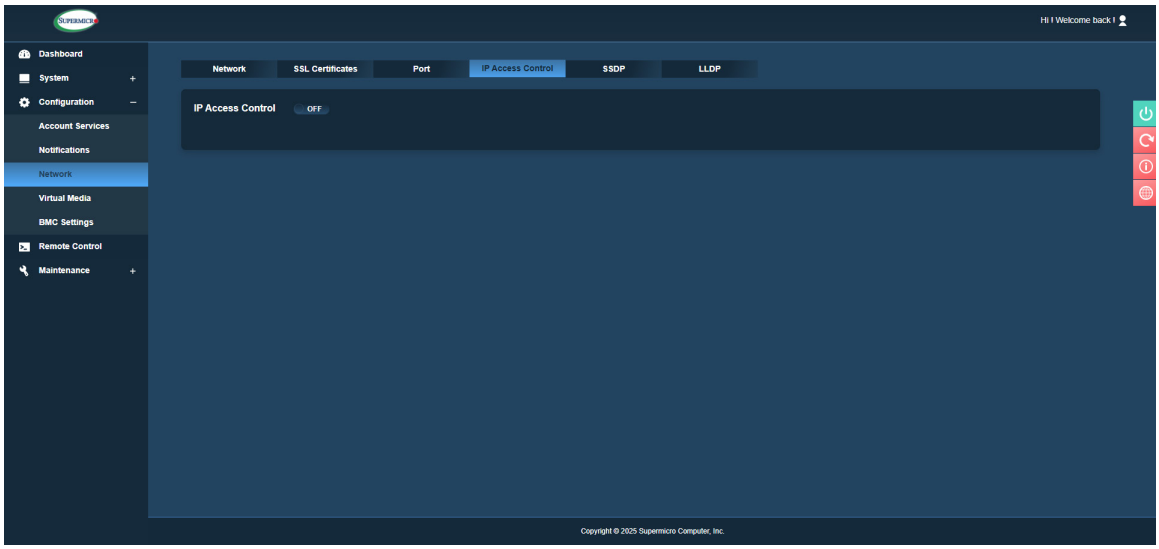


Figure 2-81: IP Access Control Page

In the IP Access Control frame, you can view the following Access Control information:

- ID: This column shows the number of IP Access Control rules.
- IP Address Control List: This column shows the list of possible network rules for IP addresses that can be accessed by users.
- Prefix Length: This column shows the Mask settings. The length should be an integer value between 0 and 128 and should not be a negative value.
- Policy: This column shows the status of an IP access policy of either ACCEPT or DROP.

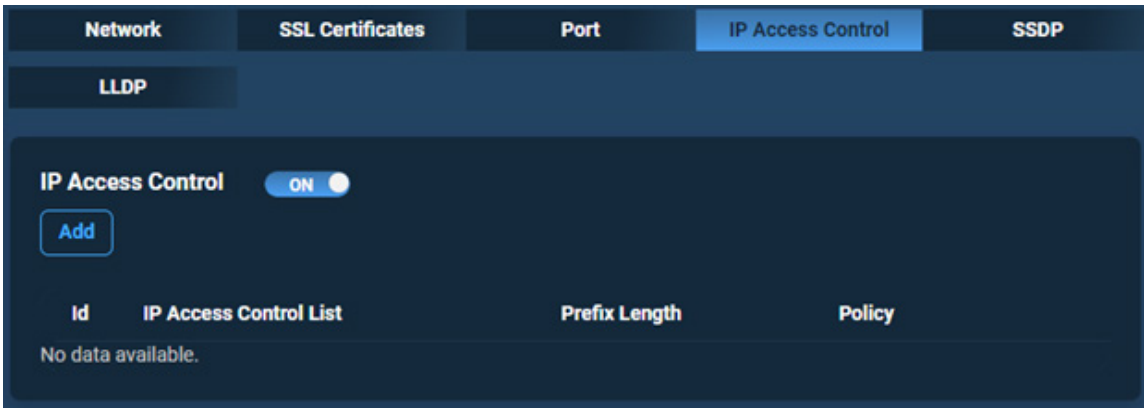


Figure 2-82: IP Access Control Section

You can adjust the following options:

- [Enable] button: You can click this button to enable or disable IP access control features.
- [Add] button: You can use the button to add a new rule to the IP access control list.
- [Pencil] icon: You can click on the Pencil icon of a policy to modify its rule.
- [Trash can] icon: You can delete a policy by clicking on the trash can icon .

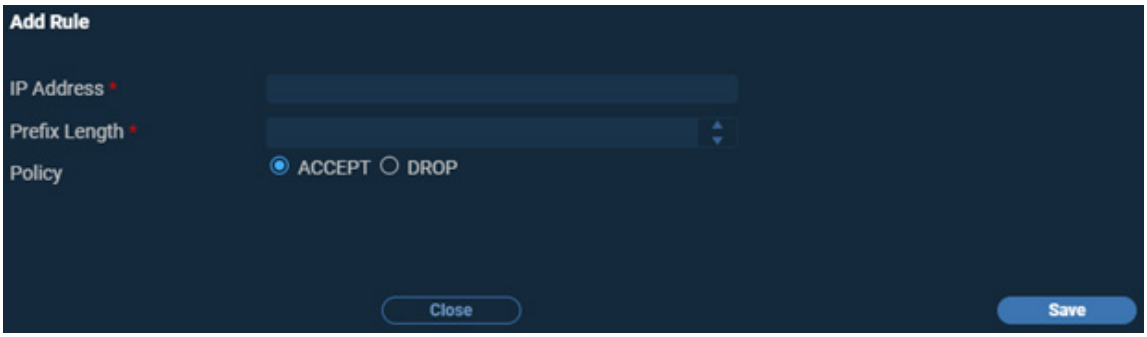


Figure 2-83: Add Rule Section

The following rules apply to ACCEPT and DROP policies:

- You can set your preferred policies.
- BMC Web UI will follow ID order. BMC always follows the previous ID number when you set a new policy.
- You can add the same IP Address with different prefixes to the same policy of either ACCEPT or DROP. BMC Web UI will still follow ID order.
- If you add the same IP Address with the same prefix and the same policy of either ACCEPT or DROP, then you will see a prompt “Duplicate data in the access control list” before you press the [Save] button. If you click [Save], no change will be made to the IP Access Control List.

Simple Service Discovery Protocol (SSDP)

Use this page for broadcast and discovery of network services on your local network.

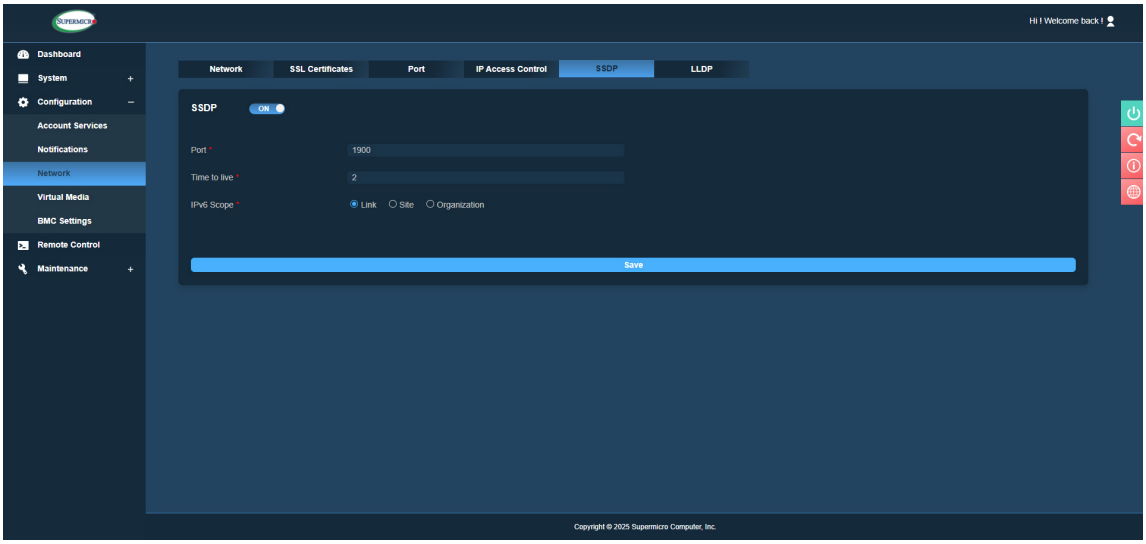


Figure 2-84: SSDP Page

You can enable or modify SSDP using the following settings on this page:

- SSDP: You can toggle (ON/OFF) to enable or disable SSDP.
- Port: You can enter a port number (0 to 65535) for the SSDP. The default port is 1900.
- TTL: You can enter the Time To Live (TTL) hop count value for the SSDPs Notify messages.
- IPv6 Scope: You can select to set the scope of the IPv6 Notify messages for SSDP.

Link Layer Discovery Protocol (LLDP)

Utilize this tab to enable or disable Link Layer Discovery Protocol (LLDP) for the network interface.

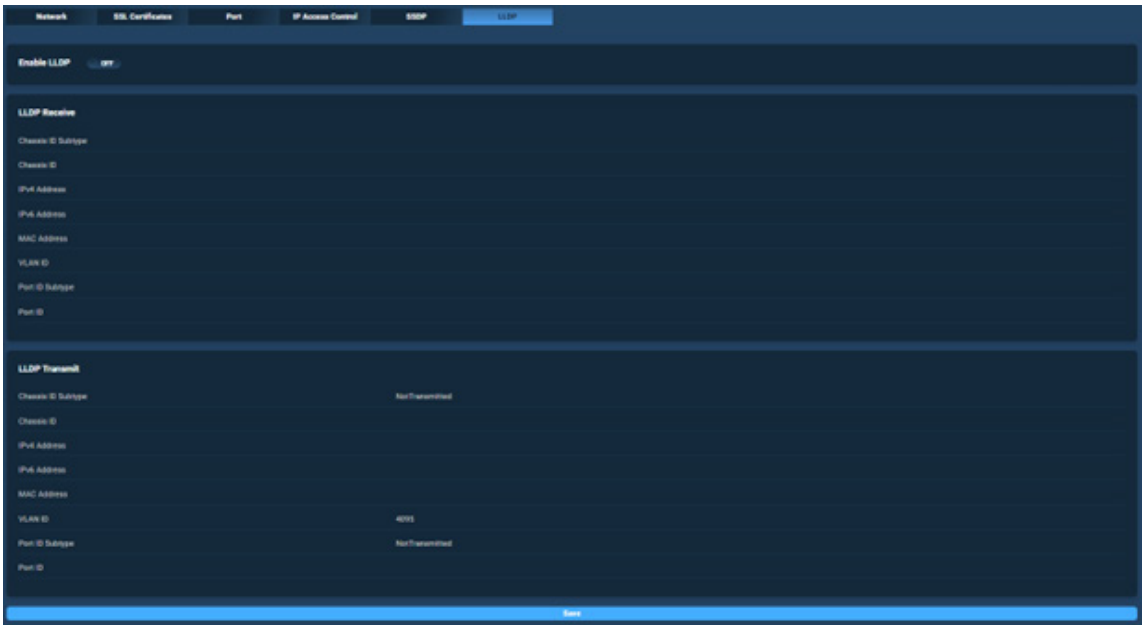


Figure 2-85: Enable LLDP OFF Samples

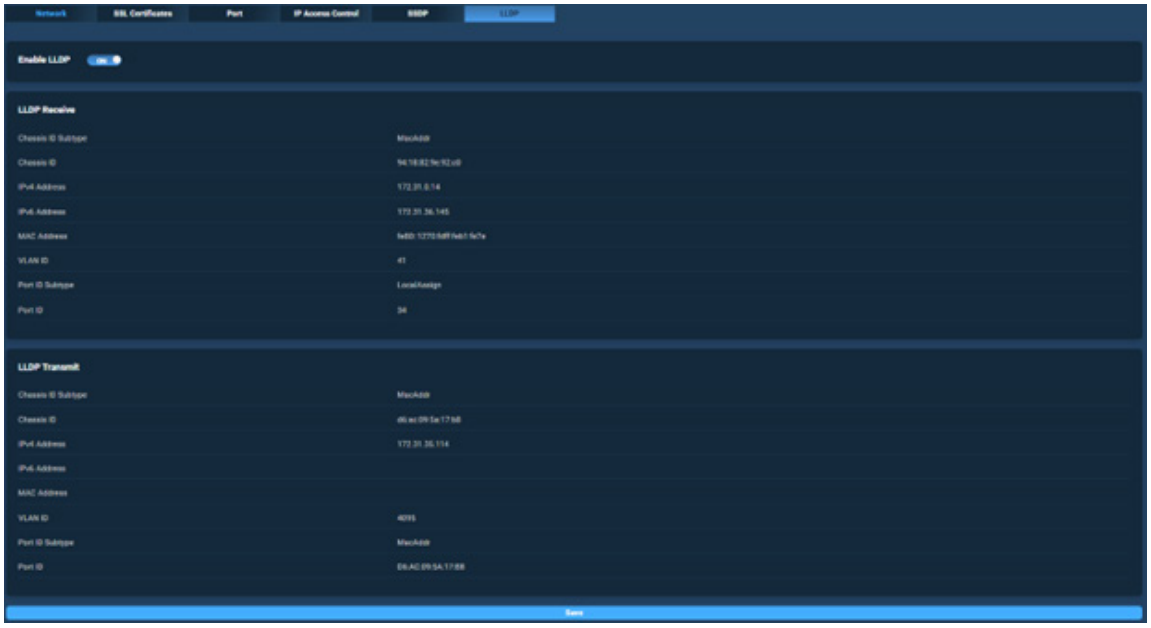


Figure 2-86: Enable LLDP ON Samples

When active, LLDP provides essential network information. You can use this page to enable/disable or modify the LLDP settings: Check ON or OFF to enable or disable LLDP.

The LLDP Receive section should show the following details:

- Chassis ID Subtype
- Chassis ID
- IPv4 Address
- IPv6 Address
- MAC Address
- VLAN ID
- Port ID Subtype
- Port ID

The LLDP Transmit section can be used to enable or disable LLDP Transmit, and will show the following details. Check ON or OFF to enable or disable the LLDP transmit.

- Chassis ID Subtype
- Chassis ID
- IPv4 Address
- IPv6 Address
- MAC Address
- VLAN ID
- Port ID Subtype
- Port ID

2.7.4 Virtual Media

Using BMC Web UI, you can go to this page to connect to Floppy (IMA/IMG format file) or CD-ROM (ISO format file) images residing in remote file server(s) and check the status of connected devices, respectively. SFT-DCMS-SINGLE software license is required for HTTP and HTTPS usage.

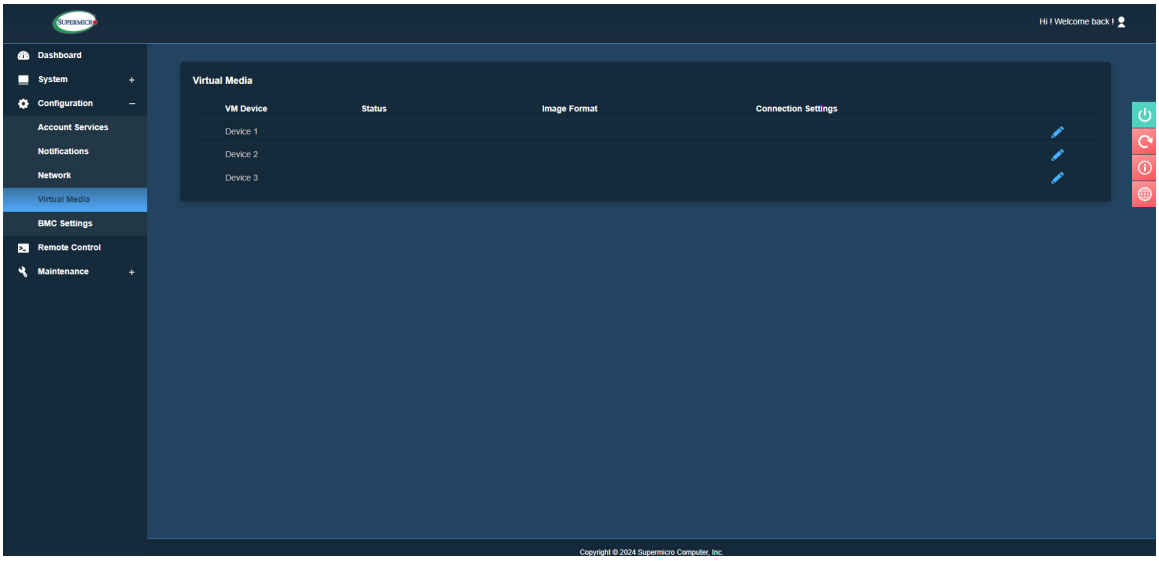


Figure 2-87: Virtual Media Page

- You can mount VM Devices to the same source of media.
- Web UI users cannot unmount VM sources that are mounted using the IKVM interface and vice versa.

VM Device

This field provides three devices that you can use to mount remote virtual media sources.

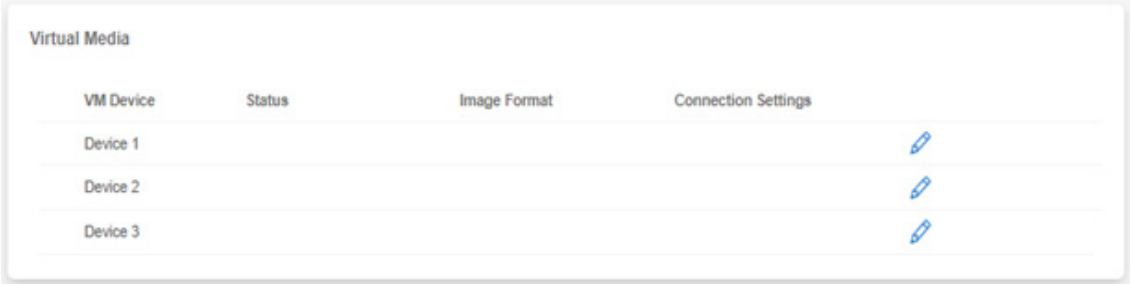


Figure 2-88: VM Mounting and Unmounting Notes

Status

This field provides the status of currently connected CD-ROM/ISO devices, indicating that the connection to the source is successfully established. You can also use this feature to disconnect respective devices as well. The status of mounting devices should be in sync from the Virtual Media page in BMC Web UI and IKVM remote control. For example, if a user mounted an image in Device 1 from the Virtual Media page, the expected status should be shown in IKVM remote control. The connection would show either URI or Applet, depending on how the images are mounted. If mounted using BMC Web UI, it is considered as mounted using URI or IKVM. If mounted using IKVM, the image is shown as mounted through Applet. Mounting and unmounting a device can only be done by the initial method/interface (using Web UI or IKVM). Web UI users are unable to unmount VM sources that have been mounted using the IKVM interface, and IKVM users cannot unmount sources that were mounted using the Web UI.

Image Format

This field showcases the format of the connected images. For example, when the image source is in ISO format, you will see the 'ISO Image' file type displayed on the user interface.

Connection Settings

This field in the Common Settings section specifies the connection type. For example, when the VM source is connected through HTTP/HTTPS, you will be able to observe the URI in the Connection Settings.

Click on the Connect/Disconnect Icons

Utilize the 'Click to Connect'  and 'Click to Disconnect'  icons to enable users to seamlessly establish or terminate connections to the VM source(s).

Edit VM Connection

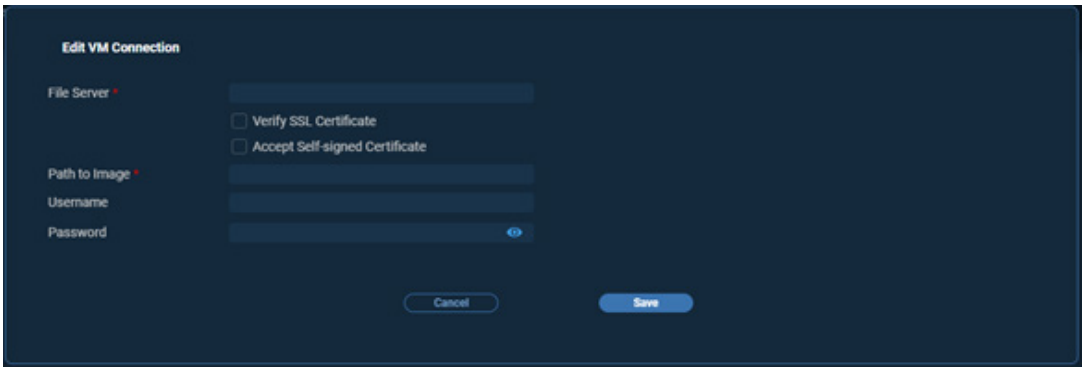


Figure 2-89: Edit VM Connection Settings

You can access VM devices by clicking on the pencil icon :

- File Server: The host server for your console redirection. File Server can only accept alphanumeric characters, dash, and periods (i.e., a-z, A-Z, 0-9, – and .) for the URL domain part. Moreover, the domain part will only accept 'http://' or 'https://' at the beginning of the string (i.e., HTTP+ IP Address, HTTPS + IP Address). Port number can be used after the IP Address as an option.

  For example: http(s):/192.188.8.8:443 for IPv4 Address and http(s):///[2021::8888:443].

- Path to Image: The Path of the CD-ROM image file will only accept alphanumeric characters, dash, periods, and symbols (i.e., a-z, 0-9, @^/.-_). All other special characters, including space and tab, will be rejected. The '/' character should only be accepted when using them alone, not continuously, which means you cannot use '//,' '\\,' '/\,; and '\/.' The path must be started with the '/' or '*' character and end with the '.iso' file extension.

- Username: Users that have access to the CD-ROM image files will only accept alphanumeric characters and carets (i.e., a-z, A-Z, 0-9, ^). All other special characters will be rejected, including space and tab.

- Password: The user password will only accept alphanumeric characters and carets (i.e., a-z, A-Z, 0-9, ^). All other special characters will be rejected, including space and tab. Passwords can be previewed by clicking the eye-icon button.

Note: CD-ROM mounting supports HTTP, HTTPS, Samba, and Windows CIFS methods.

Virtual Media (VM) License						
	SMBV2	**SMBV3**	**CIFS**	**SAMBA**	**HTTP**	**HTTPS**
Current X14 License	STANDARD	STANDARD	STANDARD	STANDARD	SFT-OOB-LIC	SFT-OOB-LIC

2.6.4 BMC Settings

Date and Time

You can use the Network Time Protocol (NTP) server setting to set the date and time. NTP is designed to synchronize the clocks of computers over a network.

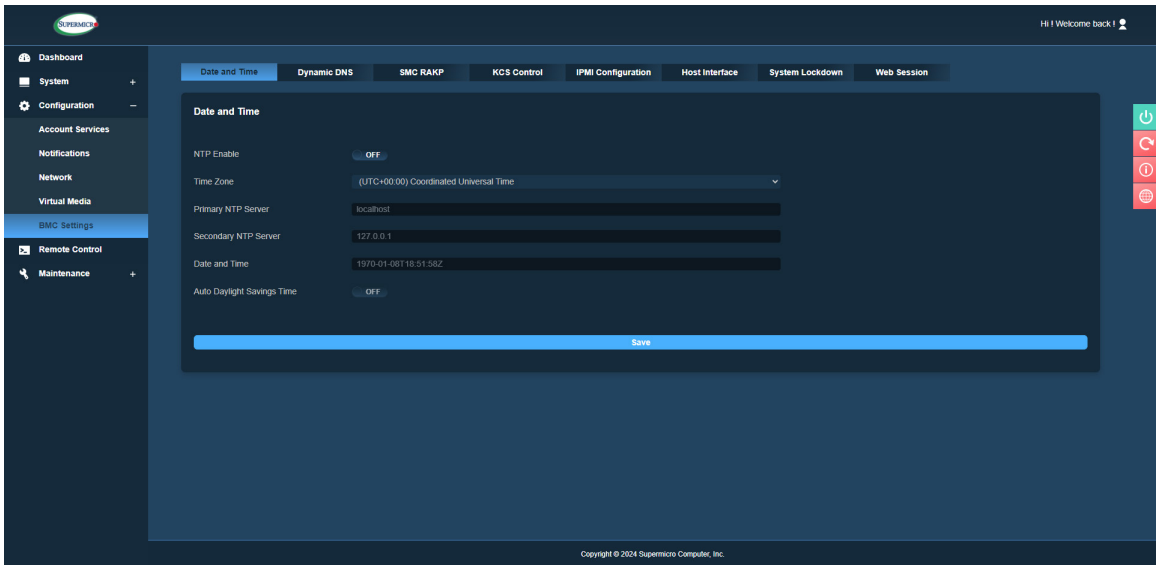


Figure 2-90: Date and Time Page

You can adjust the following fields:

- NTP Enable: You can enable or disable NTP server settings by toggling the ON/OFF button. If NTP is disabled, the system time is used to set the date and time. The Time Zone can be adjusted as required. If NTP is enabled, the NTP server is used to set the date and time. However, before BMC successfully gets the date and time from the NTP server, BMC will sync with the system time (e.g., from BIOS). If NTP is enabled and BMC has been using NTP for the date and time, the date and time will sync with system time (from BIOS) upon a system reboot when NTP is then set to disable.

  Note: NTP will automatically be disabled whenever NTP servers cannot be reached or whenever NTP servers become disconnected. The log will be sent to the Maintenance Event Log to notify you.

- Time Zone: You can select Coordinated Universal Time (or UTC) after enabling NTP.

  Note: Time zone is enabled when NTP is selected. The options are UTC -12:00 hr. through +14:00 hr.

- Primary NTP Server: You can enter the primary NTP server information.

  Note: Be sure to only use the allowed special characters. If a user entry does not match the character rule, you will receive an info message: "Invalid IPv4/IPv6 address or domain name!"

- Secondary NTP Server: You can enter secondary NTP server information. This is optional.

  Note: Be sure to only use the allowed special characters. If a user entry does not match the character rule, you will receive an info message: "Invalid IPv4/IPv6 address or domain name!"

- Date/Time: You can view the time in HH:MM:SS format.
- Auto Daylight Savings Time: The ON-OFF button can be toggled to enable or disable Auto Daylight Savings Time.

Dynamic DNS

You can configure Dynamic Domain Name System (DDNS) properties.

Note: NTP service should be enabled prior to Dynamic DNS configuration.

- Dynamic Update Enable: You can enable/disable Dynamic DNS update support.
- Dynamic DNS Server Address: You can view the server address of your Dynamic DNS server.
- BMC Hostname: You can view the name of the Baseboard Management Controller (BMC) host server.
- TSIG Authentication: You can enable Transaction Signature (TSIG) authentication support and upload TSIG.key files.

Note: Fields with ' * ' icon are optional.

SMC RAKP

This page allows you to enable or disable the Supermicro-supported Remote Authenticated KeyExchange Protocol (RAKP). When you disable SMC RAKP, there will be a prompt to inform users.

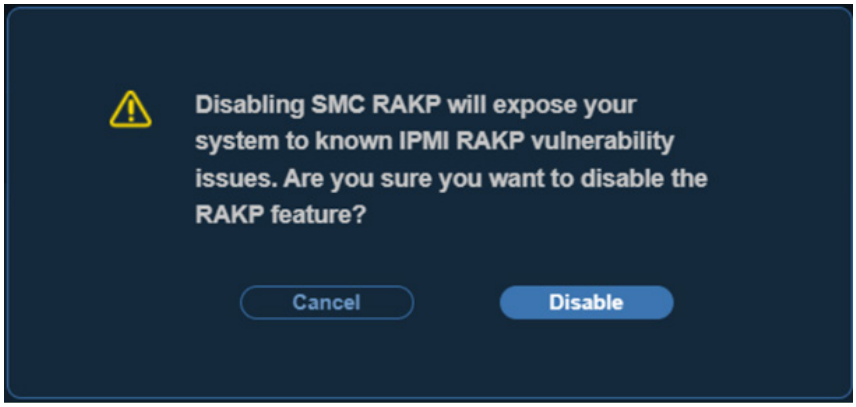


Figure 2-91: SMC RAKP Disable Warning

KCS Control

This feature allows you to secure your environment by configuring appropriate supported privileges to access the KCS interface. The supported privileges include the following:

- Administrator: Any users accessing the KCS interface will be able to do all the operations that an administrator user can do.
- Operator: Any users accessing the KCS interface will be able to do all the operations that a user with Operator privilege can do.
- User: Any users accessing the KCS interface will be able to do all the operations that a user with User privilege can do.
- Callback: This may be considered the lowest privilege level. Only commands necessary to support initiating a Callback are allowed.
- Disable KCS: You can disable the KCS interface by choosing this option.

BMC Configuration

This page can be used to save or restore BMC/IPMI configuration settings. You can save the BMC/IPMI Configuration settings of the system in the “Self-Config Backup” or “Platform-Config Backup” option. Listed are some of the key points highlighting the functionality of BMC/IPMI configuration.

Restore BMC/IPMI Configuration from Self Config File

You can restore all information from their own configuration file. BMC will restore all information with configurations previously saved in the configuration file when you want to reload BMC/IPMI Configurations to the same system.

Restoring BMC/IPMI Configurations from a File of Another System with the Same Platform

This option requires a software license. BMC does not modify the hardware dependency configurations. After restoring the BMC/IPMI configuration, hardware dependencies will retain their current configuration. For example, current storage card settings will not be modified.

Restoring BMC/IPMI Configurations from a File of the Same Platforms with the Same GUID

For this restoration process to take place successfully, a crucial condition needs to be met: the Globally Unique Identifier (GUID) of both system A and system B must be identical. The GUID serves as a unique identifier for each device and ensures that the correct configuration is being transferred to the intended recipient. If the GUID of system A matches that of system B, it indicates that the two devices share a common identification, making it possible to restore the BMC or IPMI configuration from one device to the other.

The key factor that determines whether the restoration process can take place is the GUID of both system A and system B. If the GUID of system A does not match that of system B, it indicates that the two systems have distinct identification codes or belong to different code bases. As a result, the system is unable to perform the restoration of BMC or IPMI configuration from one device to the other.

The requirement for the GUID to be the same is essential because it ensures that the correct and compatible configuration settings are being transferred between the systems. When the GUID differs (indicating different code bases or distinct systems), it implies that the configurations might not be compatible or applicable to the target device, making the restoration process unfeasible.

Furthermore, BMC/IPMI configurations cannot be transferred across different BMC firmware.

The restoration of BMC or IPMI configurations cannot occur between different BMC firmware due to differences in the code base and GUID. These differences imply potential incompatibility, making it challenging to ensure that the configurations from one firmware are suitable and applicable to the other. Consequently, seamless restoration across the diverse firmware is not feasible.

Note: The Save BMC/IPMI Configuration option will download an IPMI configuration .bin file. Hostnames cannot be transferred from one system to another. Passwords cannot be transferred or overridden by another BMC/IPMI Configuration. IP addresses are unaffected since they are not saved when saving the BMC/IPMI configuration. This restriction is in place to maintain the security and integrity of the account settings, ensuring that unauthorized changes cannot be made through the restoration process.

If the file is good, you will receive the prompt message: "*Uploading new configuration…please reconnect once process is completed! BMC must be reset to apply new changes."* If the file is corrupted, you will receive the prompt message: *"Corrupted file! Click here to return."* If the file is not the correct file type, you will receive the prompt message: *"Invalid file type! Please upload a valid file. Click here to return."*

Host Interface

The BMC Host Interface (HI) provides an Ethernet-over-USB solution, offering the capability to establish connections with Ethernet devices through USB.

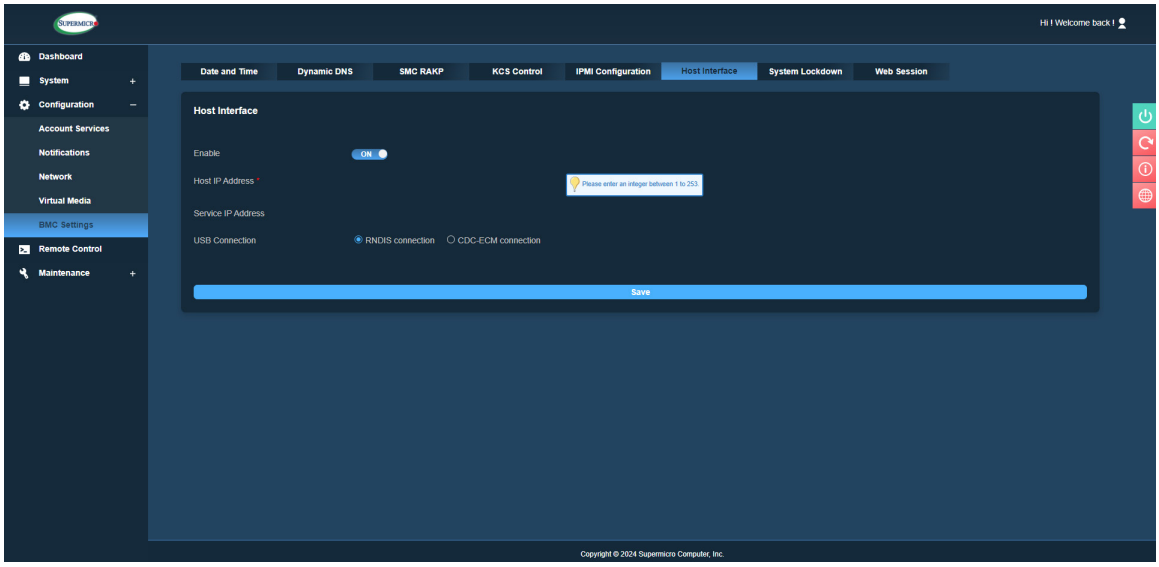


Figure 2-92: Host Interface Page

You can adjust the following key features to configure the host interface:

- Enable (ON/OFF): This option allows you to enable or disable the BMC Host Interface service based on their requirements.
- Host IP Address: This option allows you to set up a host IP address, assigning it to the host operating system for seamless communication.
- Service IP Address: This is the service IP address for the Management Host Interface is available in read-only mode, providing essential information about the current configuration.
- USB Connection Options: This option allows you to choose between a Remote Network Driver Interface Specification (RNDIS) Connection or a Communication Device Class — Ethernet Control Model (CDC-ECM) Connection, tailoring the USB connection to specific needs.

> **Note:** It is not advisable to change the Host Interface mode during system boot. If you attempt to switch the Host Interface mode from 'OFF to ON' or 'ON to OFF' while the system is in POST, BMC will display the following error message, *"ERROR: Please ensure that system hardware initialization is complete before making changes to the Host Interface."*

System Lockdown

The implementation of a System Lockdown feature enhances the system security by safeguarding against inadvertent or unauthorized modifications to the system configuration while it is operational. Once activated, System Lockdown rigorously blocks all attempts to alter system configurations, including firmware updates. Any attempt to make changes during this lockdown state will be promptly intercepted, and you will be duly notified of such attempts.

Note: To enable System lockdown, you should have the DCMS license and BMC Administration privilege.

When the system is under lockdown, BMC will show the following icon.

Figure 2-93: Lockdown Icon

The following features will be functional during the system lockdown.

- System power operations (Power On, Power Off, Reset)
- Identify operations (Chassis Identify)
- IPMI Configuration download
- Maintenance Events download
- Maintenance Unit Reset
- UID control

Web Session

You can set the web session timeout to a value from one to 30 (minutes) or set it to 0 for no timeout. The default timeout value is 0 minutes.

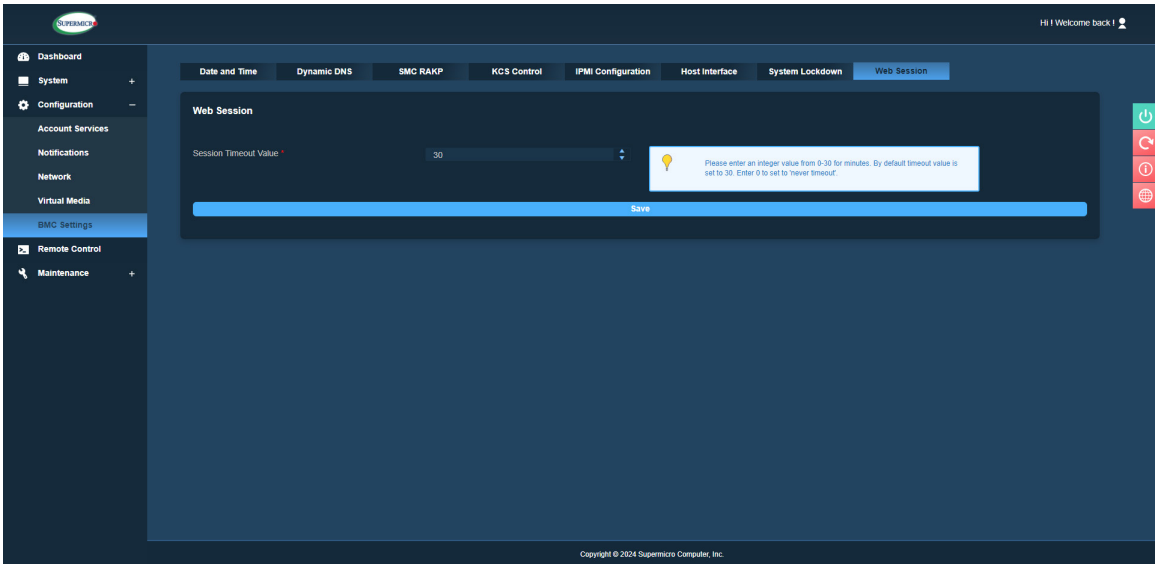


Figure 2-94: Web Session Page

Reset BIOS

This feature is only available for X14, H14, and later generation systems. You can remotely reset BIOS to factory default settings by clicking the [Reset] button. They can cancel or proceed with the execution by following the pop-up prompt.

> *Clearing the CMOS will restore the BIOS to its default settings. This action will first shut down the system and then temporarily cut off AC power. Afterward, you must manually turn the system back on. Do you wish to proceed?*
>
> *[Cancel] [Proceed]*

Note: The Reset BIOS feature is not supported in X14SBH.

Smart Power

The feature will involve Power Supply, BMC, and CPLD. Smart Power will be activated when a PMBUS alert happens. Alerts will be sent to the “Health Event Log." The smart power feature can be enabled or disabled using the ON/OFF button, and it will be applied to all nodes at the same time. The Smart Power page provides Status, Input Voltage, Max Watts, and Total Watts for each Power Supply Unit. It also provides Power Status, Max Watts, Smart Power, Power Consumption, and Total Consumption for each respective node available in the system.

Note: IPMI/BMC will only set the power limitation if a) IPMI/BMC is reset or b) there is a lost or additional power supply to the system. In those cases, IPMI/BMC will identify the power supply and set the CPU power limit. ‘Enable Smart Power Event Log’ allows you to view Smart Power logs on supported platforms.

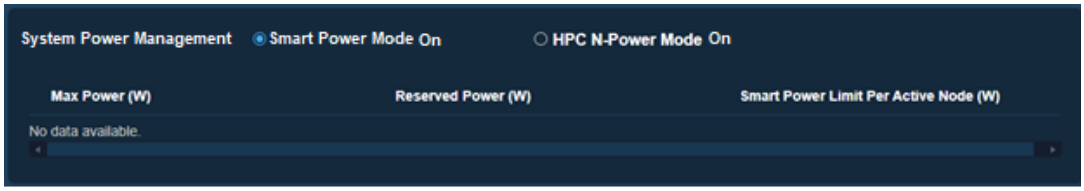


Figure 2-95: For FlexTwin™ Only

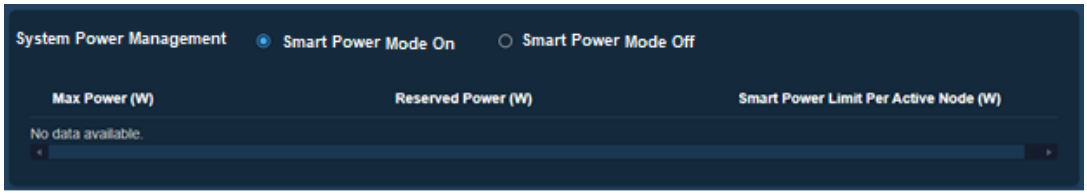


Figure 2-96: For Other Platforms

2.7 Remote Control

Remote control options allow you to perform operations on a remote server using remote access.

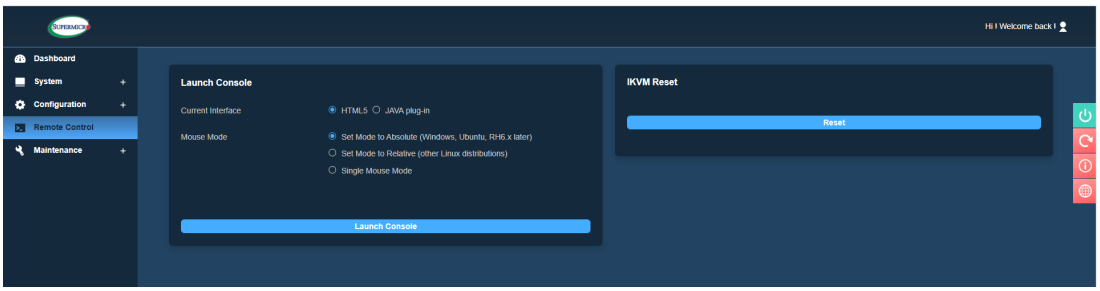


Figure 2-97: Remote Control Page

Launch Console

Use this page to launch or configure the current remote console interface settings. You can select using a JAVA plug-in or HTML5 interface. If you decide to change the remote console interface, they will receive a prompt message: *"Once a remote console session is connected, switching between JAVA and HTML5 is not allowed."* The maximum number of sessions for either the Java or IKVM console is four. If there are more than four sessions open, there will be a message: *"The maximum number of open sessions has been reached! Please close this IKVM window."*

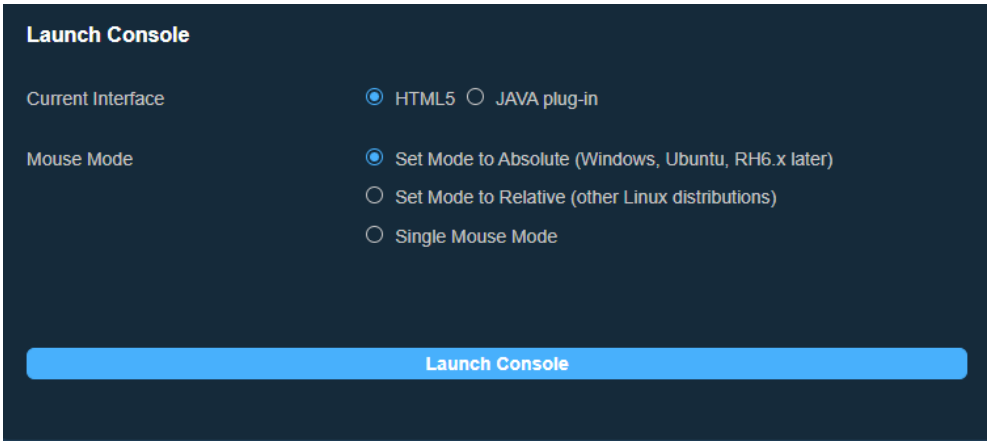


Figure 2-98: Launch Console Settings

To launch a remote console using Java or Active X (for Internet Explorer), refer to the following steps:

1. Select the JAVA plug-in interface option.
2. Click on [Launch Console] to launch Console Redirection or KVM Console.

Utilize OpenJDK as Oracle Java is no longer supported.

To launch an HTML5 remote console, refer to the following steps:

1. Select the HTML5 interface option.
2. Click on [Launch Console] to launch Console Redirection or KVM Console. A console in a new browser window will automatically open.

Note: Video recording only works with Chrome and Edge browsers. If you choose any other browser for recording, it will show a message saying, *"Your current browser doesn't support the video recording capability. Please use Google Chrome or Microsoft Edge browser for this functionality."*

Mouse Mode

You can modify mouse mode based on the OS environment for the remote console.

- Select Absolute Mode for Windows, Ubuntu, RH6.x, or later.
- Select Relative Mode for other Linux/Unix distributions.
- Select Single Mouse Mode to use single mouse mode.

Note: IPMI is an OS-independent platform, and IKVM support is an add-on feature of BMC. For the mouse to function properly, configure the Mouse Mode settings (see above) according to the type of OS used in the system.

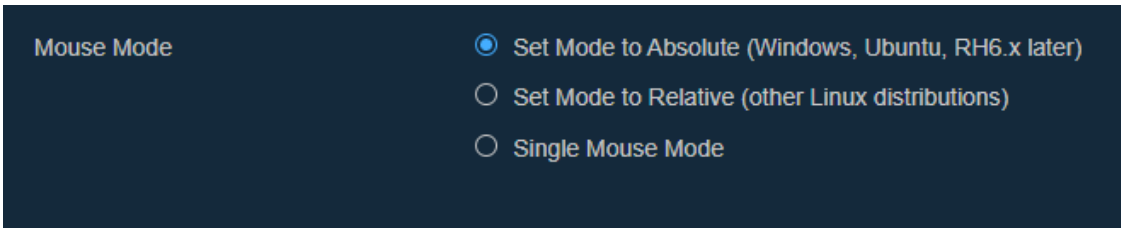


Figure 2-99: Mouse Mode

IKVM Reset

This option allows users to reset IKVM, which will reset virtual media as well as the IKVM keyboard and mouse. If the IKVM service is reset, all active IKVM sessions will be disconnected, and any open IKVM windows will be closed. The following message will be prompted: *"IKVM service has been reset, leading to the closure of all active IKVM windows. Relaunch IKVM windows to resume your activities. Please close this IKVM window."*

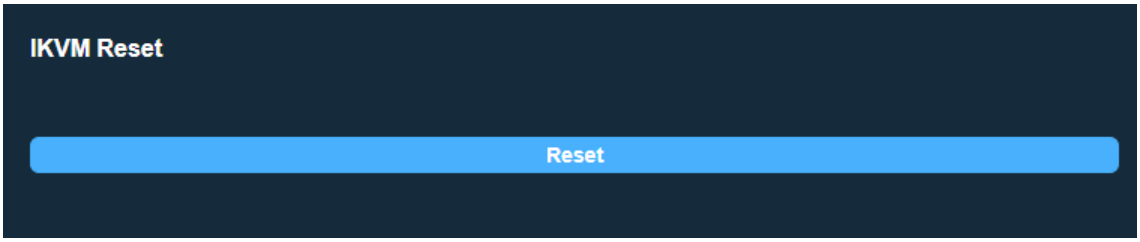


Figure 2-100: IKVM Reset Reset Button

2.7.1 Console Redirection

This feature allows you to launch Console Redirection through IKVM (keyboard, video/monitor, mouse) support. Refer to the image for the options available. The same descriptions for each icon are displayed when the mouse hovers over it.

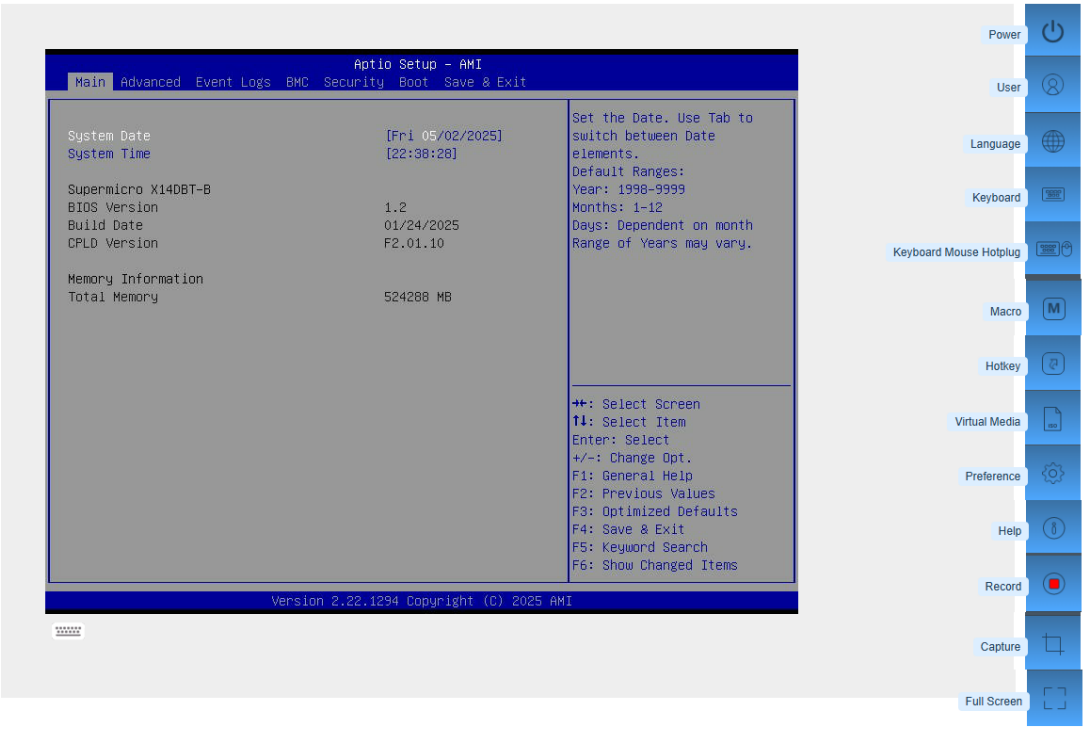


Figure 2-101: Main Tab with Console Redirection

Click [Help] for further assistance if needed.

2.7.1a Console Redirection — Power

This feature allows you to configure the power settings of the system.

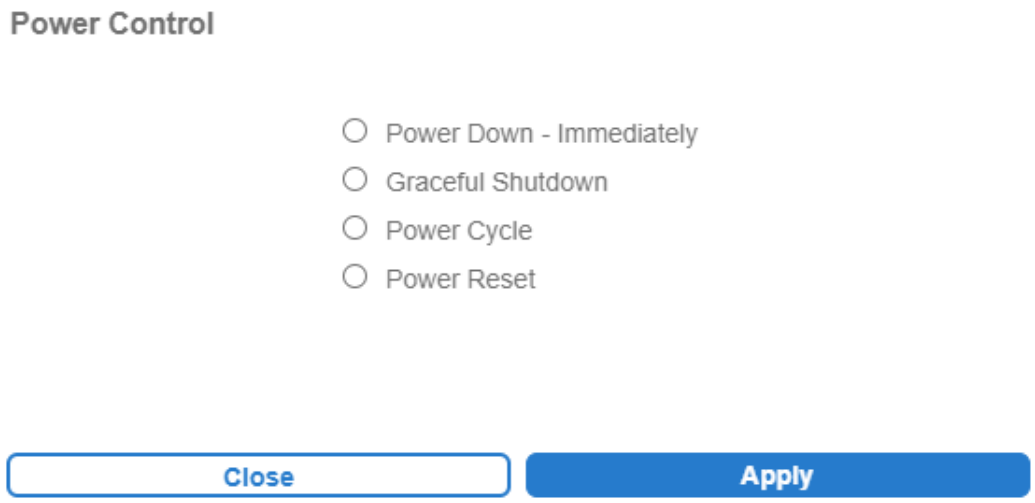


Figure 2-102: Power Control Settings

Once you have reached the window shown above, the following options are available:

- Power On: You can power on the server system.
- Power Down — Immediately: You can power off the server system immediately (non-graceful shutdown).
- Graceful Shutdown: You can power off the server system gracefully by shutting down the operating system before turning off the system.
- Power Cycle: You can power off the server system completely and power it back on.
- Power Reset: You can perform a warm restart on the server system.

2.7.1b Console Redirection — Users

This feature displays the user list, which shows the Session ID, User Name, and IP Address of active users who are currently accessing the HTML5-IKVM.

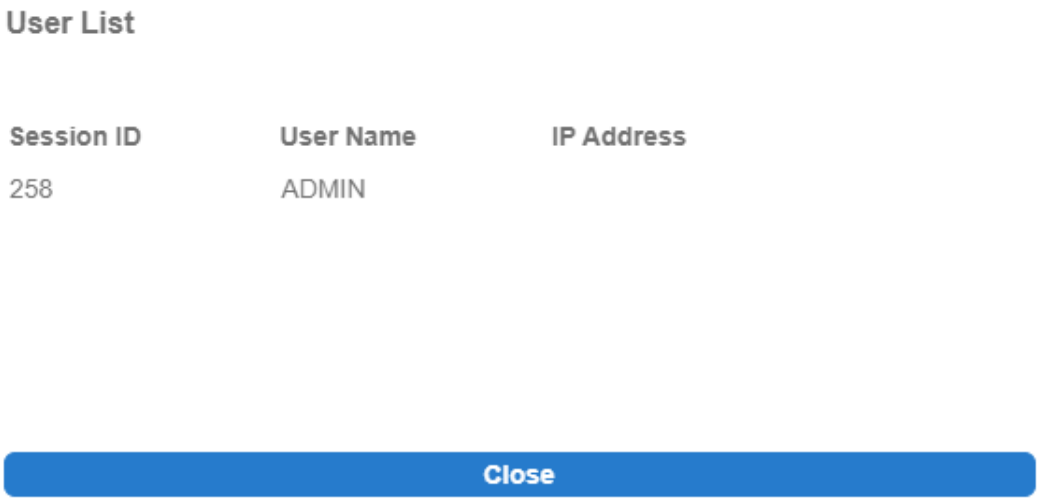


Figure 2-103: Users Setting

2.7.1c Console Redirection — Language

This feature allows you to configure the language settings.

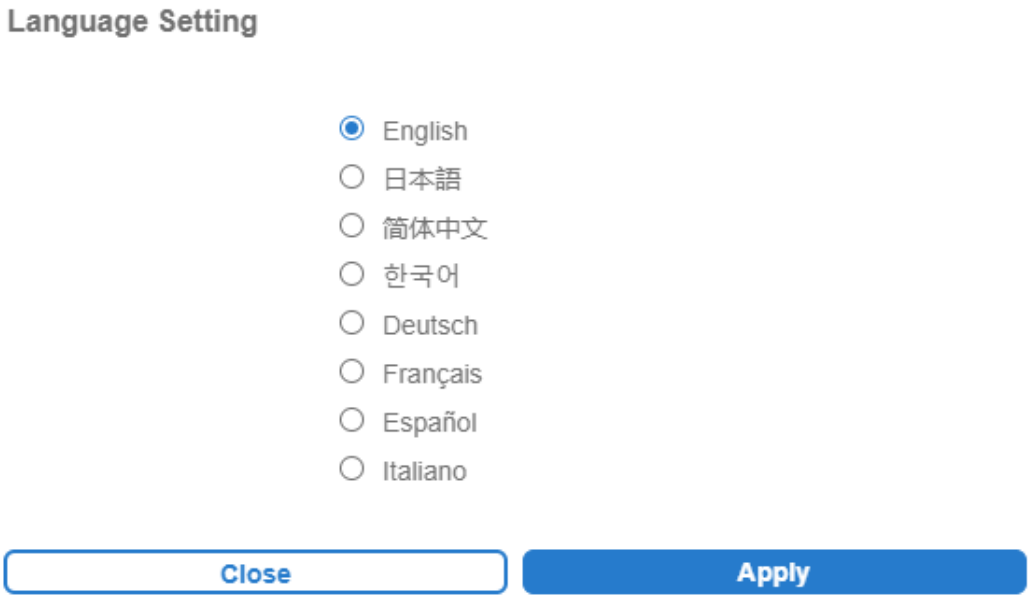


Figure 2-104: Language Settings

Select one of the following support languages:

- English
- Japanese
- Simplified Chinese
- Korean
- German
- French
- Spanish
- Italian

2.7.1d Console Redirection — Keyboard

This feature allows you to access the virtual keyboard as an alternative input mechanism if you are unable to use a physical keyboard. You can now select one of the following supported languages.

- English (US International and the United Kingdom)
- Spanish
- French
- Italian
- Japanese
- Korean
- German

Figure 2-105: Virtual Keyboard Language Settings

After one of the languages is selected and set, the HTML5-IKVM virtual keyboard's language will be set to the selected language.

Note: JAVA-IKVM virtual keyboard's language will use a US-international virtual keyboard regardless of which of the supported languages is set. Also note that due to language differences in size and shape, the sizes of supported virtual keyboards will vary. As a result, they will not be the same.

2.7.1e Console Redirection — Keyboard Mouse Hotplug

This option allows you to hot-plug the server-side Keyboard and Mouse devices using the Hotplug icon.

Note: The action of this function is on the server side, not the client's side. Server side is the server on which BMC is installed.

2.7.1f Console Redirection — Macro

This feature provides you with the ability to set up patterns or rules for hotkeys and other function keys. However, you can use the 19 pre-defined buttons for your convenience. Instead of using multiple keys (at least two keys) to virtually access the remote window, you can just click on one of the options. The following are some example definitions for the Macro keys.

- *Alt+Spacebar*: A keyboard shortcut most often used to open the window menu of the program currently open in Microsoft Windows.
- *Alt+Esc*: A keyboard shortcut most often used to switch between windows in the order they were first opened. When this macro is pressed, it will perform the same action.
- *Alt+Tab*: A keyboard shortcut to switch between all open applications.

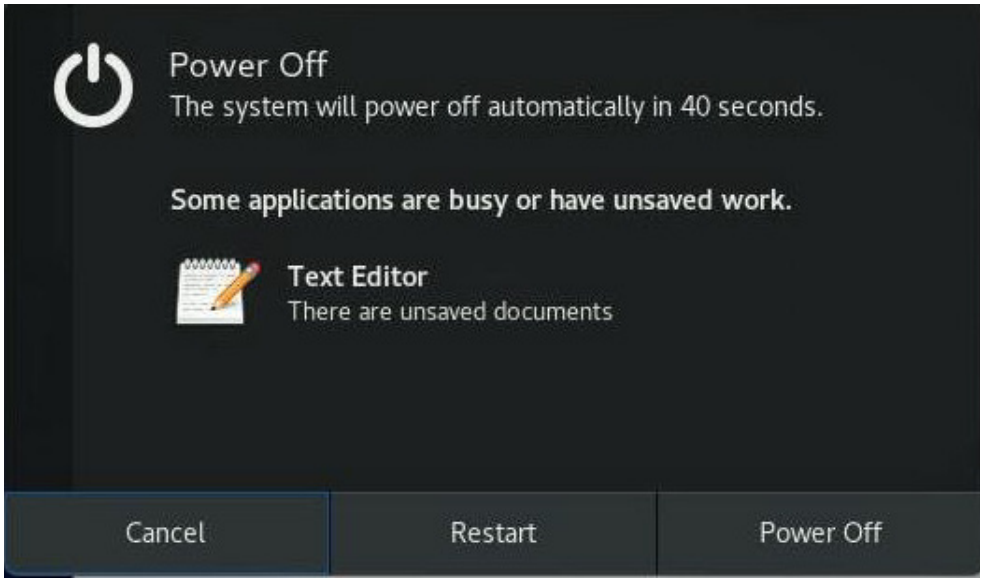


Figure 2-106: Example of Pressing *Ctrl+Alt+Del*

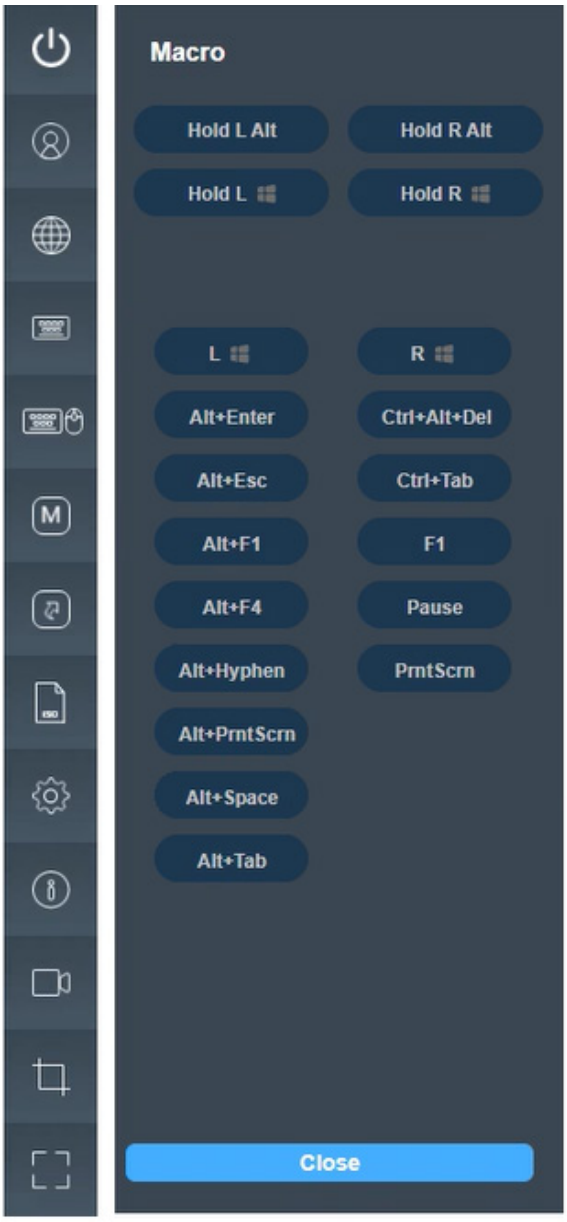


Figure 2-107: Macro UI

2.7.1g Console Redirection — Hotkey

Hotkey settings allow you to define your own set of keys to do predetermined actions.

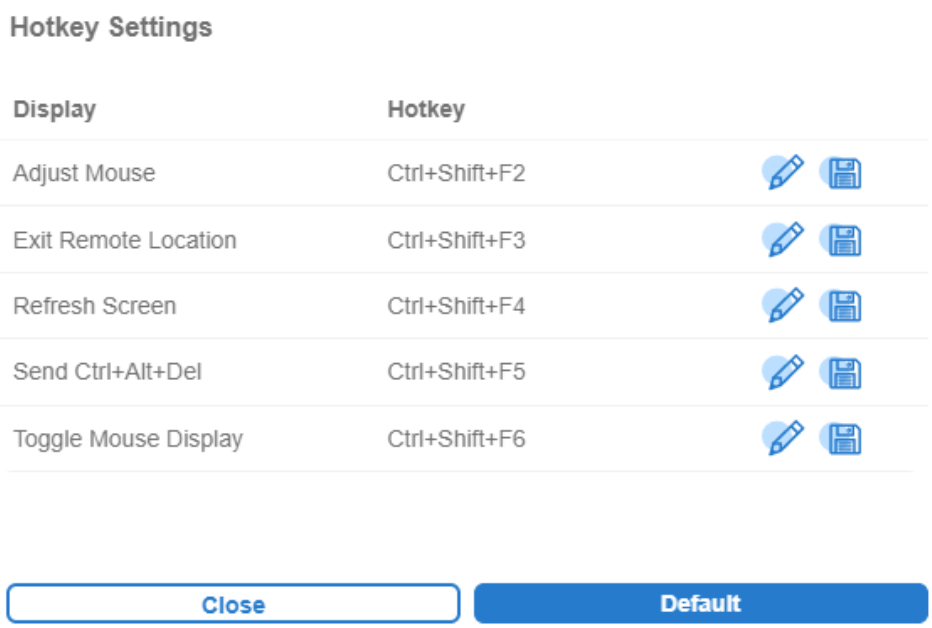


Figure 2-108: Hotkey Settings

The following display options are available:

- Adjust Mouse: You can switch between mouse modes.
- Exit Remote Location: You can exit/close IKVM.
- Refresh Screen: You can recapture one frame of the screen.
- Send Ctrl+Alt+Del: You can restart the Host OS.
- Toggle Mouse Display: You can hide or unhide the mouse cursor.

The hotkeys for the display options can be modified to multiple users' preferences by choosing any function keys (F2 to F12) and numbers (0 to 9) to combine with Ctrl+Shift. For example, one user can set the hotkey for Refresh Screen by combining Ctrl+Shift and F2 for "Ctrl+Shift+F2." Another user can also set Refresh Screen by combining Ctrl+Shift and 8 to set a new hotkey "Ctrl+Shift+8." Thus, when the second user presses the "Ctrl," "Shift," and number "8" keys, IKVM recaptures one frame of the screen.

If you do not complete choosing the third key to save, an error prompt will display *"Please enter a valid shortcut."*

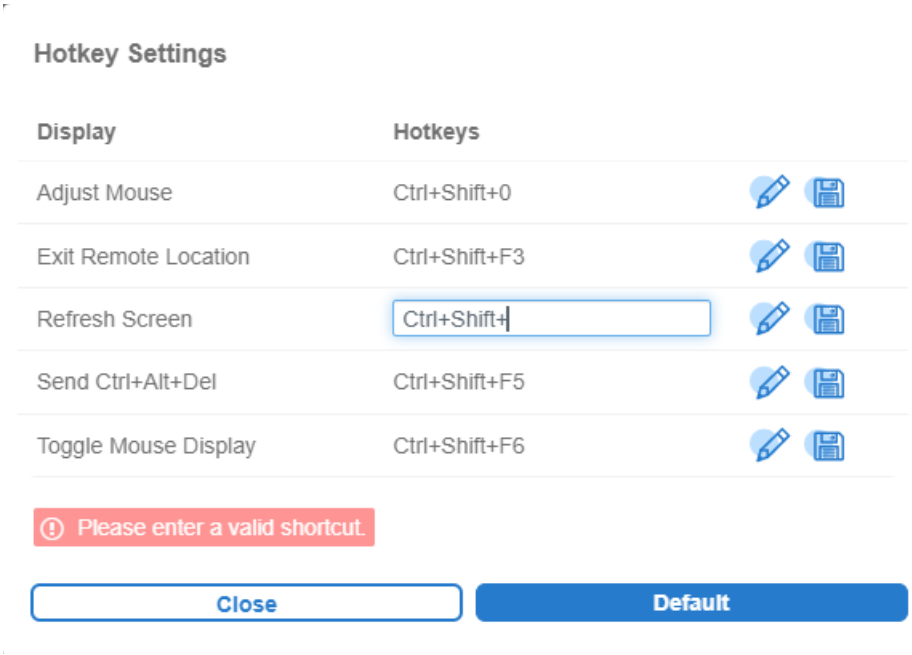


Figure 2-109: Changing Hotkeys Shortcut

If you complete choosing the third key to save, a successful prompt will display the green text.

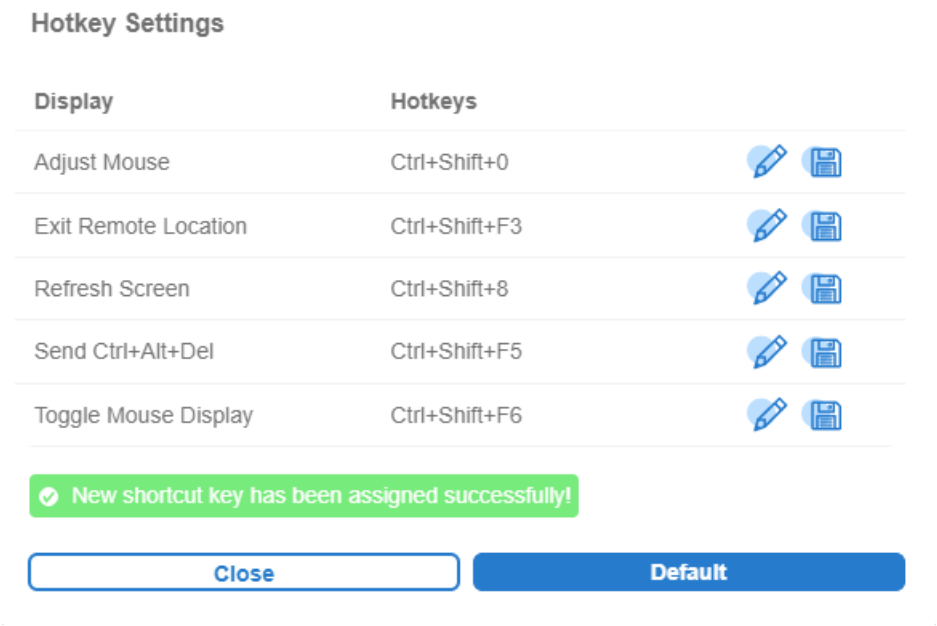


Figure 2-110: Hotkey Settings Prompt For Successful Shortcut Assignment

2.7.1h Console Redirection — Virtual Media

This feature allows you to upload and share images the the Baseboard Management Controller (BMC). These images will be emulated to the host server as USB applications. You need to first activate a Super Micro Software License to enable this feature.

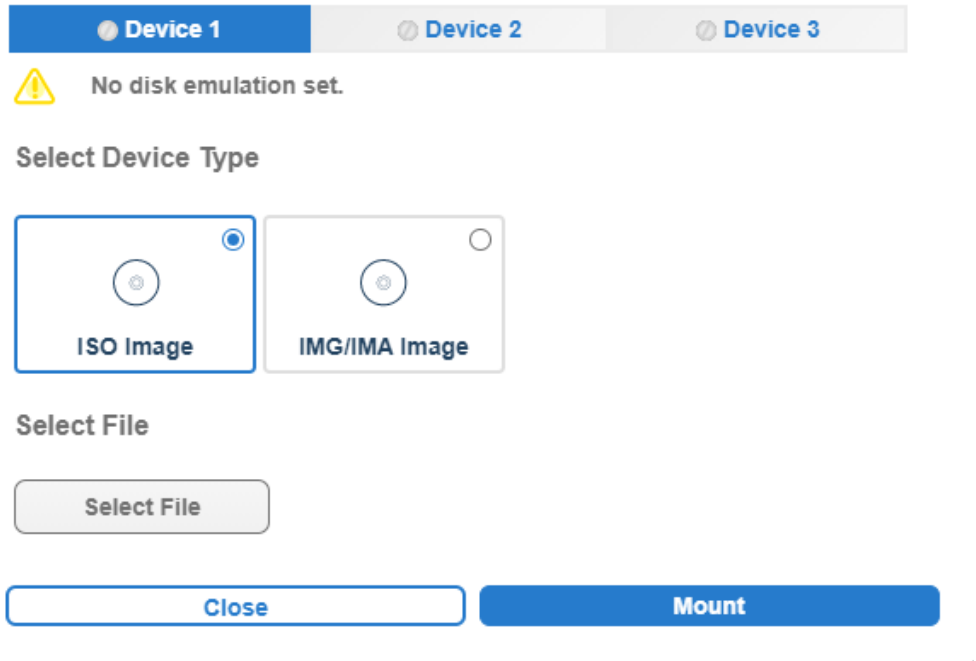


Figure 2-111: Virtual Media Device Type Setting

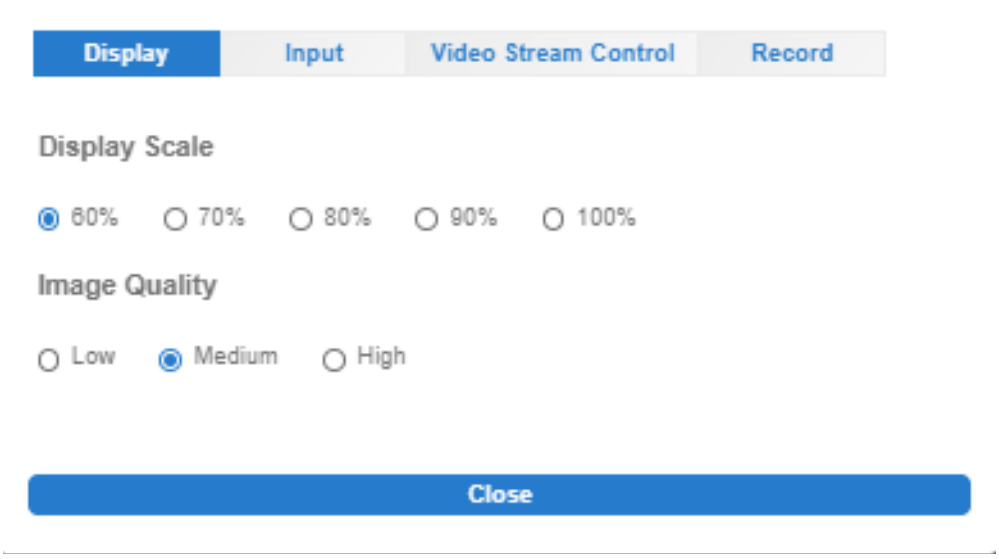


Figure 2-112: Virtual Media Display Setting

2.7.1i Console Redirection — Preference

This feature allows you to control Display, Input, Video Stream Control, and Record properties.

Console Redirection — Display

You can reduce the display's size and image quality. There are five size choices to choose from: 60%, 70%, 80%, 90%, or 100% (the original size). For image quality, you can select low, medium, or high quality depending on the bandwidth of your network.

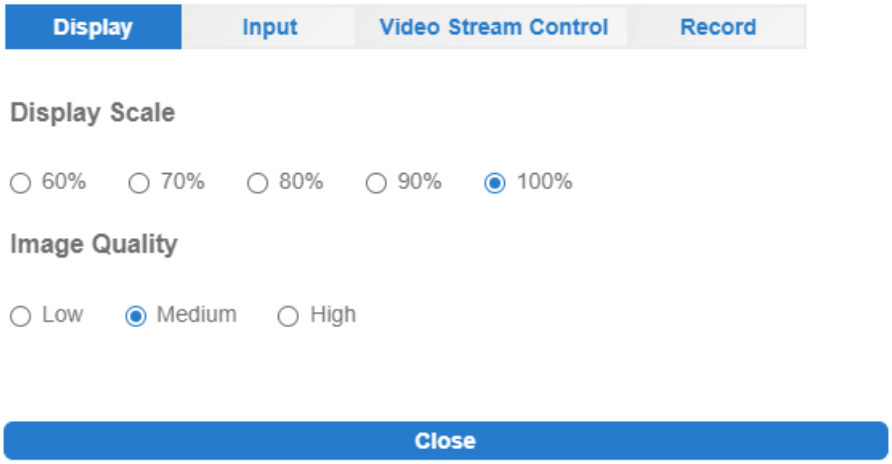


Figure 2-113: Virtual Media Display Setting

Console Redirection — Input

This allows you to select one of the following mouse modes to improve mouse performance: Absolute Mouse when using in Windows, Ubuntu, RHEL 6.x and later, Relative Mouse while using in other Linux distributions, and Single Mouse when using for other usages.

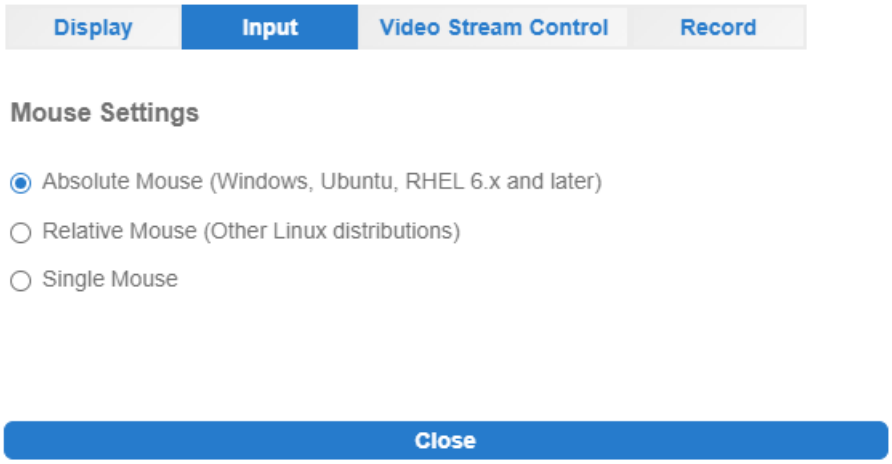


Figure 2-114: Virtual Media Input Settings

Console Redirection — Video Stream Control

You can select one of the three options depending on the speed of your network. The 256K Cable/DSL is preselected, while T1 (1.5 Mbps) and T2 (6.3 Mbps) are options if you have higher network bandwidth.

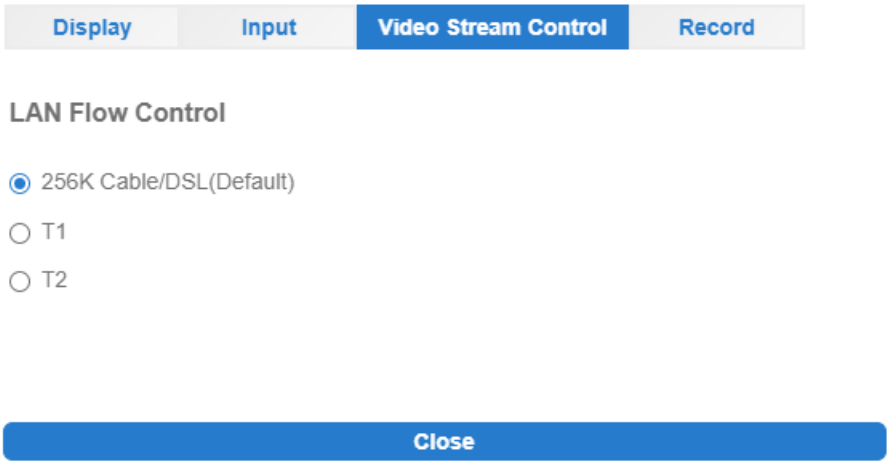


Figure 2-115: Virtual Media Video Stream Control Settings

Console Redirection — Record

This feature is used to adjust the recording time setting when recording video during BIOS booting. You can turn on/off the recording time in this tab. A preset two-minute recording time is enabled by default, but you can modify the recording time from one minute to a maximum of 30 minutes. New settings will take effect in the next recording.

Note: Video Recording only works with the Chrome browser.

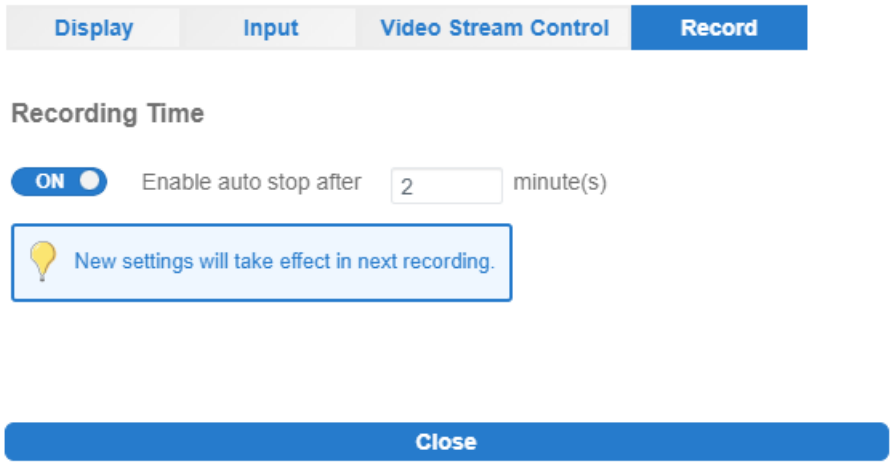


Figure 2-116: Virtual Media Record Settings

2.7.1j Console Redirection — Help

You can click on Help to get more information for most of the icons. The following images show the Help content and the Help icon.

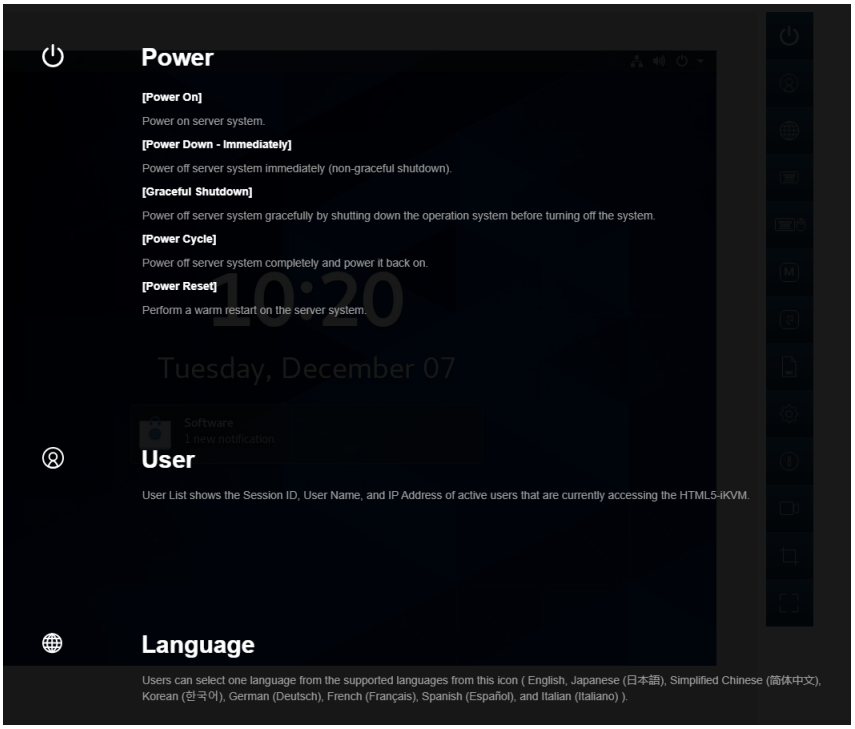


Figure 2-117: Help Page

Figure 2-118: Help Icon

2.7.1k Console Redirection — Record

Use this feature to record video during BIOS booting. After you press the Record button and then the Stop button, the recording will be available to be saved.

Note: Video recording only works with the Chrome browser.

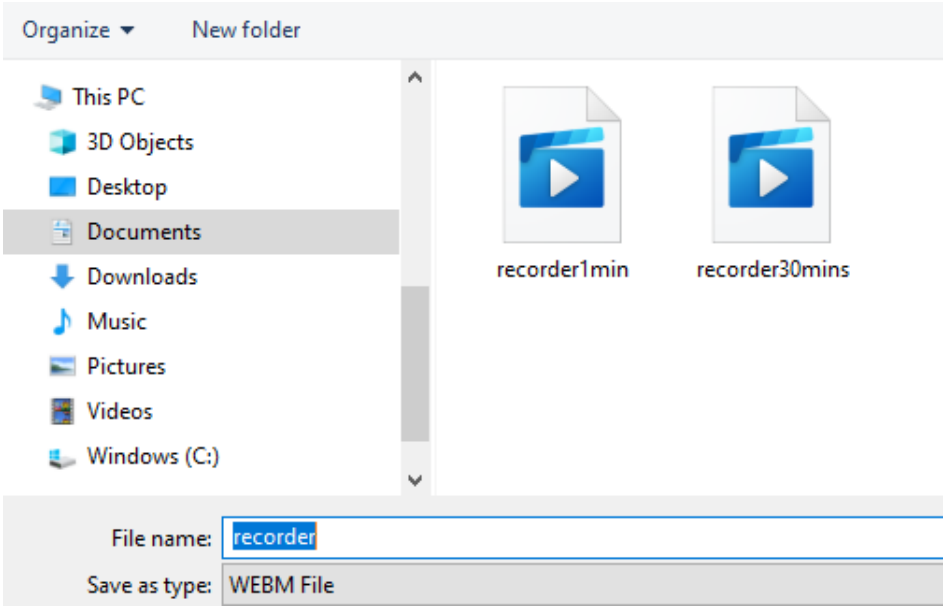


Figure 2-119: Saving Video

Figure 2-120: Record Icon

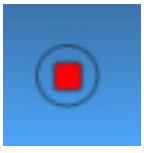


Figure 2-121: Stop (Recording) Icon

2.7.1l Console Redirection — Capture

Capture allows you to save an image of the current screen. After you press the Capture button, a JPEG image will be available to be saved.

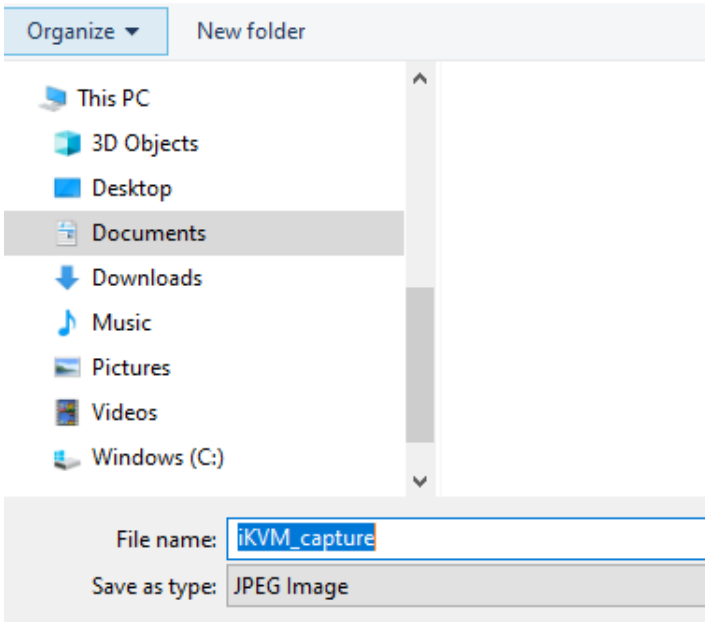


Figure 2-122: Saving JPEG Image

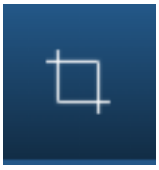


Figure 2-123: Capture Icon

2.7.1m Console Redirection — Full-Screen

This feature allows you to expand the HTML5-IKVM screen to the maximum display of the monitor screen.

2.7.2 IKVM/HTML5

This feature allows you to launch IKVM/HTML5 through IKVM (keyboard, video/monitor, mouse) support. Click [Help] for further assistance if needed.

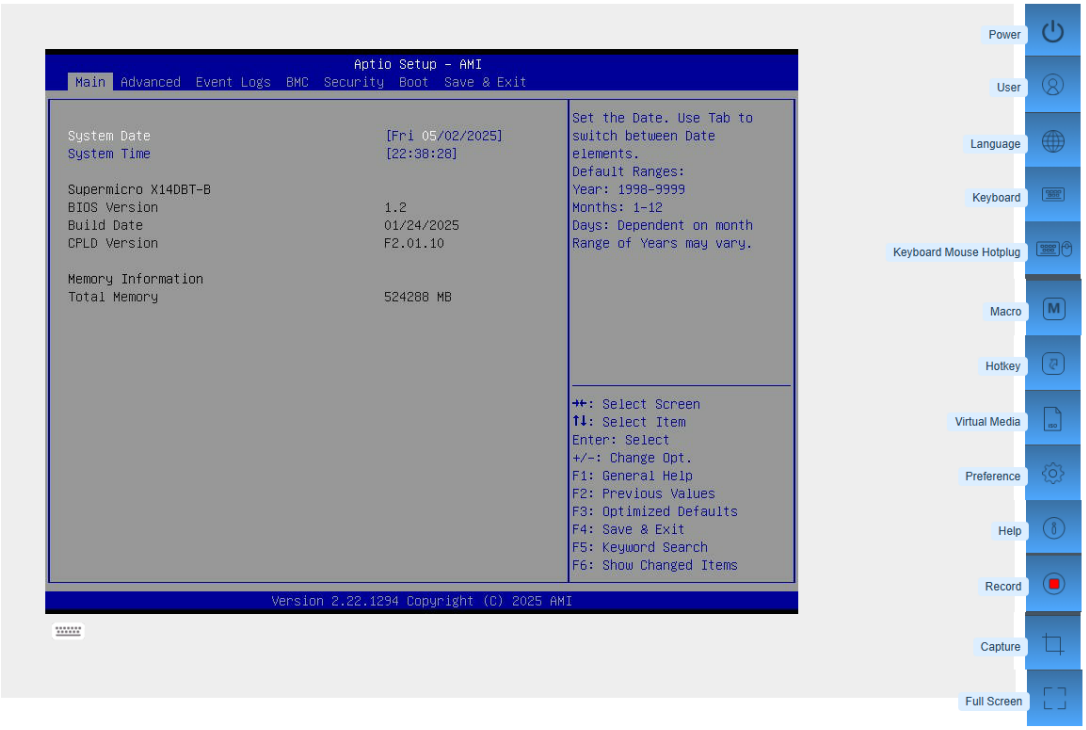


Figure 2-124: IKVM/HTML5 Launched Through IKVM

2.7.2a IKVM/HTML5 — Virtual Keyboard

The virtual keyboard provides an alternative input mechanism if you are unable to use a conventional keyboard. To access the keyboard, click on "Keyboard" on the side bar to open the virtual keyboard.

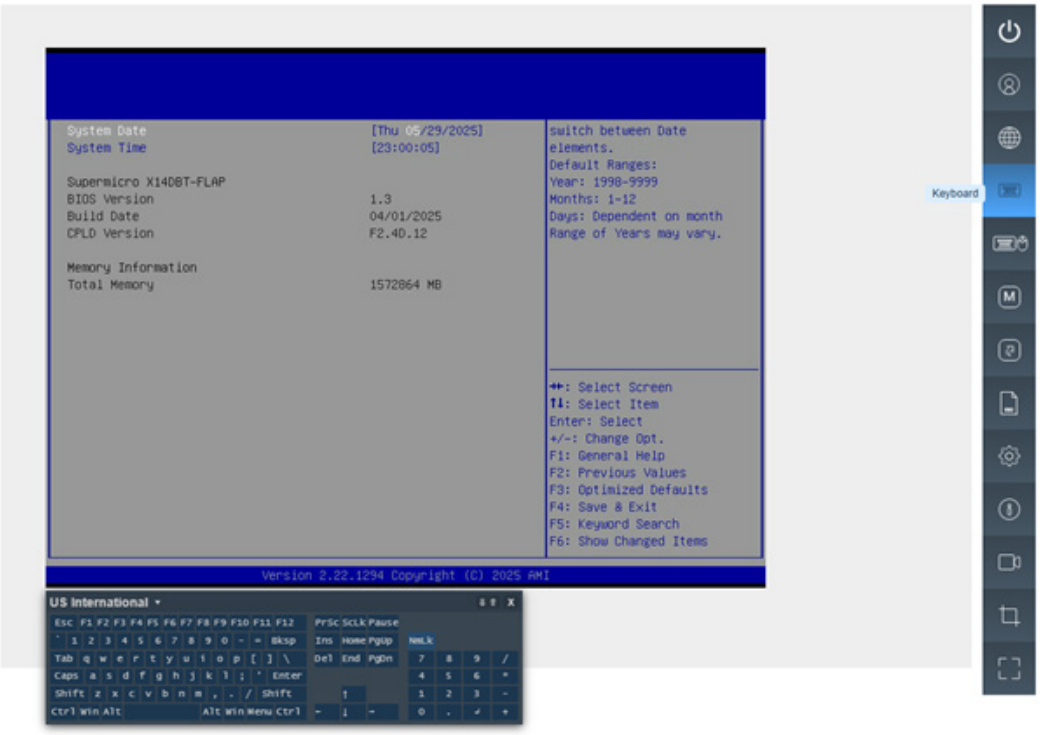


Figure 2-125: Virtual Keyboard on Submenu

- Click on the "Virtual Keyboard" icon located at the bottom left of the display.

Figure 2-126: Virtual Keyboard

2.7.2b IKVM/HTML5 — Virtual Media

This feature allows you to upload and share images through the Baseboard Management Controller (BMC). These images will be emulated to the host server as USB applications. You need to first activate a Super Micro Software License to enable this feature.

2.7.2c IKVM/HTML5 — Record

This feature allows for video recording of the display. Use the Record button to start and stop the recording manually. Recorded videos will be automatically saved to your drive.

Note: This new HTML5 implementation is only supported by the Chrome browser.

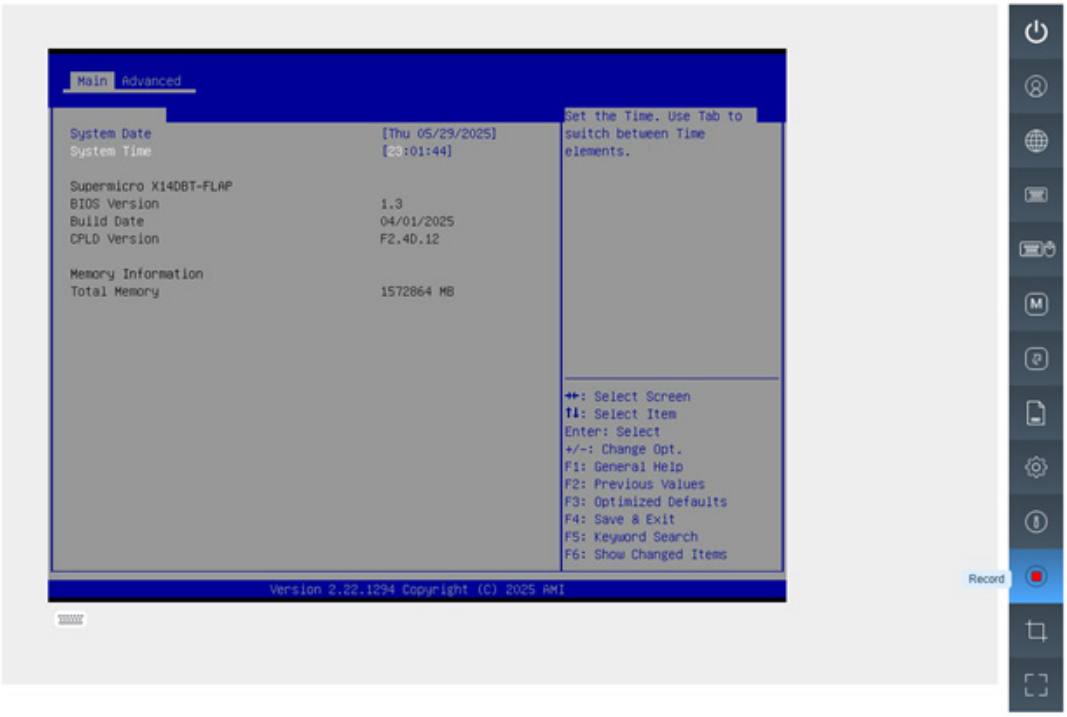


Figure 2-127: Record Button

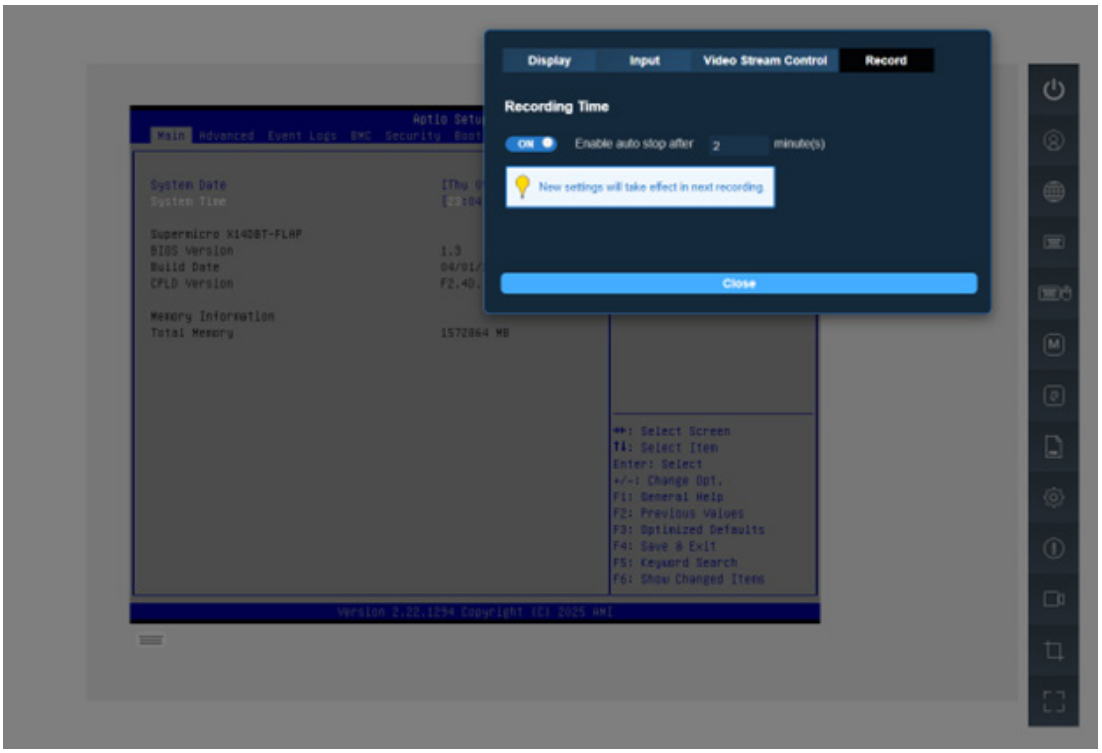


Figure 2-128: Record Submenu

2.7.2d IKVM/HTML5 — Macro

This feature allows you quick access to combo keys.

- Hold Right Alt Key: This feature performs the same function as holding down the right <Alt> key. Deselect to release action.
- Hold Left Alt Key: This feature performs the same function as holding down the left <Alt> key. Deselect to release action.
- Right Windows Key: This feature performs the same function as pressing the right <Windows> key. Select [Hold Down] or [Press and Release].
- Left Windows Key: This feature performs the same function as pressing the left <Windows> key. Select [Hold Down] or [Press and Release].
- Macro: You can click this feature to view the pull-down submenu and select one of the available series of access keys.
    - Ctrl+Alt+Del
    - Alt+Tab
    - Alt+Esc
    - Ctrl+Tab
    - Alt+Space
    - Alt+Enter
    - Alt+Hyphen
    - Alt+F4
    - Alt+PrntScrn
    - PrntScrn
    - F1
    - Alt+F1
    - Pause

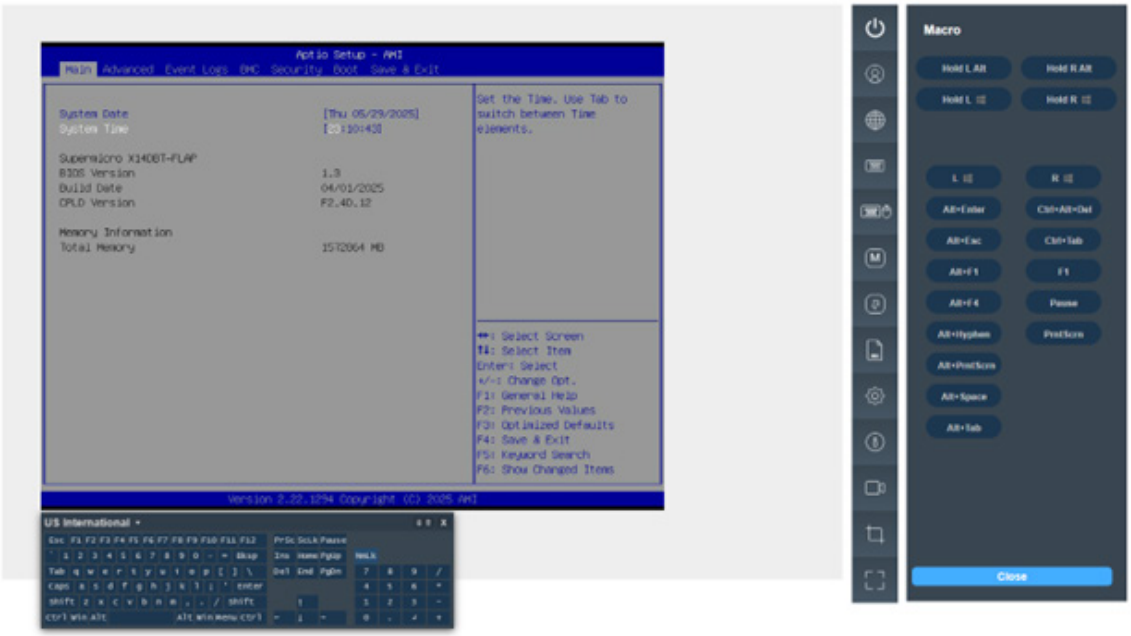


Figure 2-129: Macro Options Submenus

2.7.2e IKVM/HTML5 — Options

This feature provides hotkeys for the following functions:

- Adjust Mouse
- Exit Remote Location
- Refresh Screen
- Send Ctrl+Alt+Del
- Toggle Mouse Display

These hotkeys can be adjusted according to your preference. However, the adjustable key after Ctrl+Shift is limited to function keys F2 to F12 and numbers 0 to 9. Preference allows you to adjust Display, Input, Language Setting, and Video Stream Control properties.

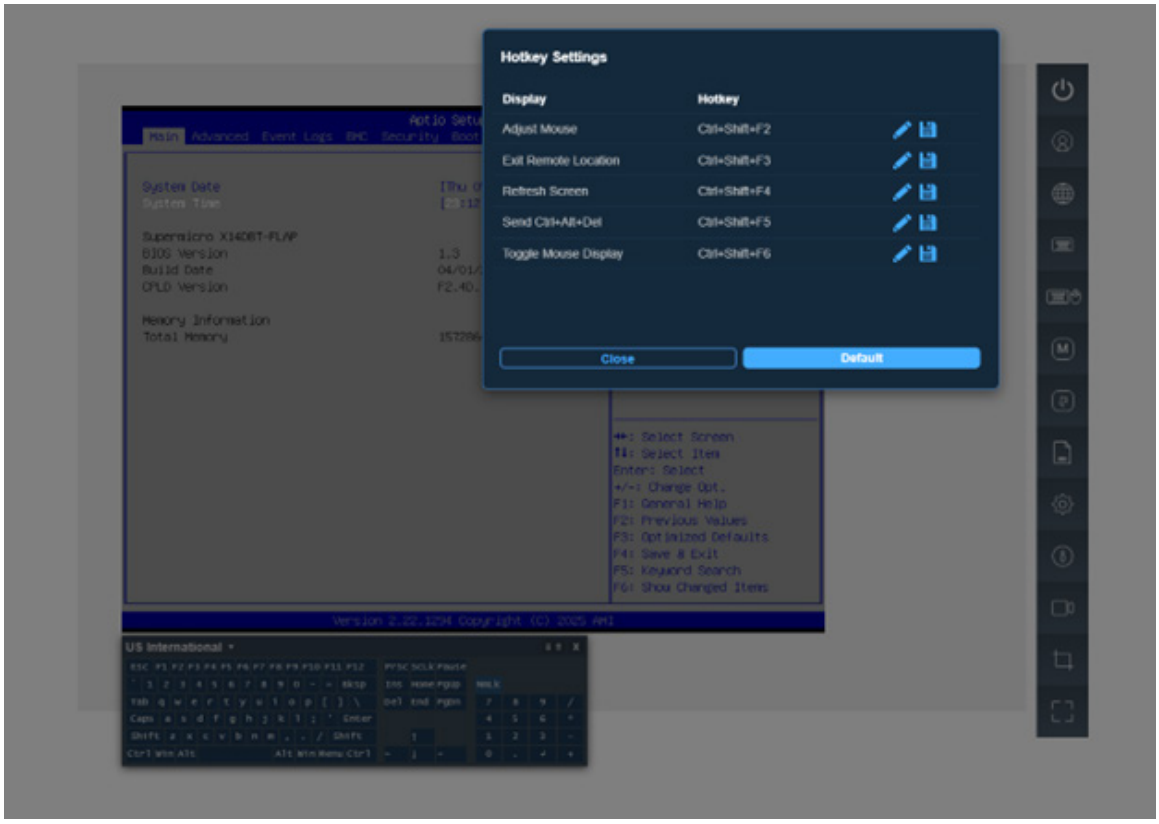


Figure 2-130: Hotkeys Settings

Preference — Display

This feature enables auto-stop after the inputted number of minutes, with the default set to two. You can adjust the maximum duration of video recordings using the following functions:

- Display Scale: You can adjust the display scale.
- Image Quality: You can adjust the image quality.

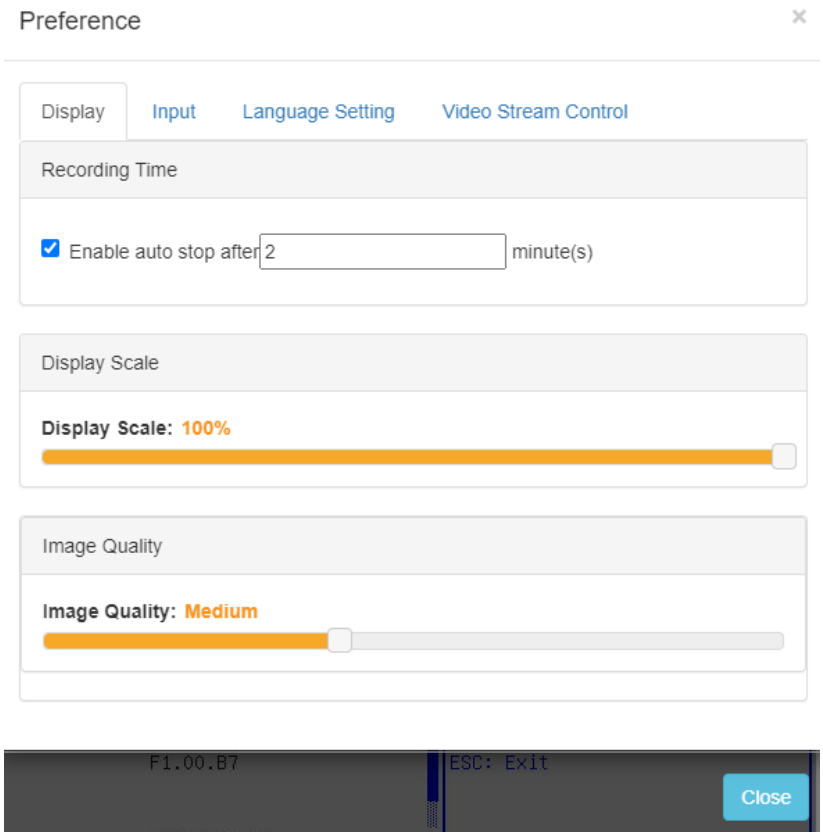


Figure 2-131: Preference Display Settings

Preference — Input

This feature allows you to select one of the following mouse modes:

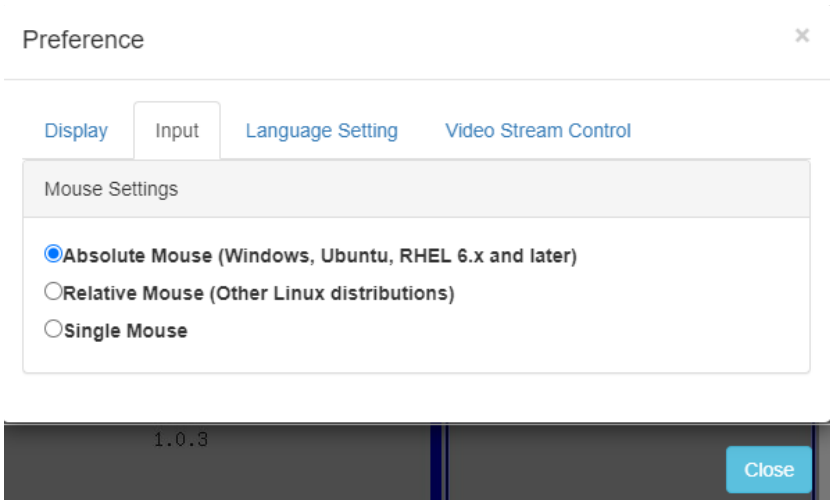


Figure 2-132: Input Settings

- Absolute Mouse
- Relative Mouse
- Single Mouse

Note: Single Mouse mode is not supported by Internet Explorer.

Preference — Language Setting

This feature allows you to select one of the following languages to be used by the IKVM/ HTML5 interface:

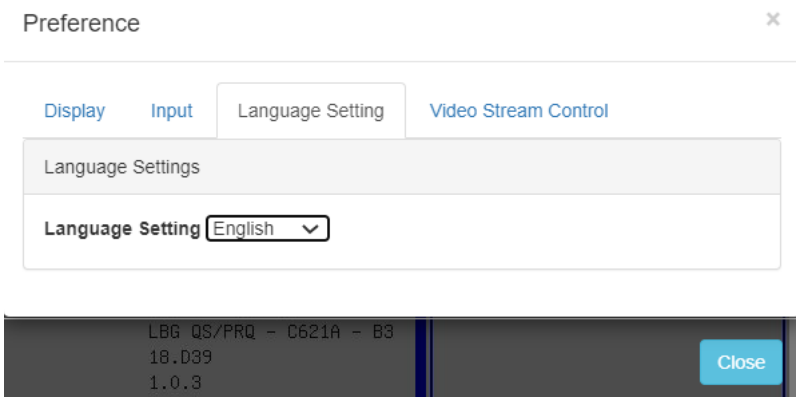


Figure 2-133: Language Settings

Select one of the following support languages:

- English
- Japanese
- German
- French
- Spanish
- Italian

Preference — Video Stream Control

This feature allows you to enable video flow control for LAN Quality of Service (QoS) by selecting one of the following options:

- 256K Cable/DSL
- T1
- T2

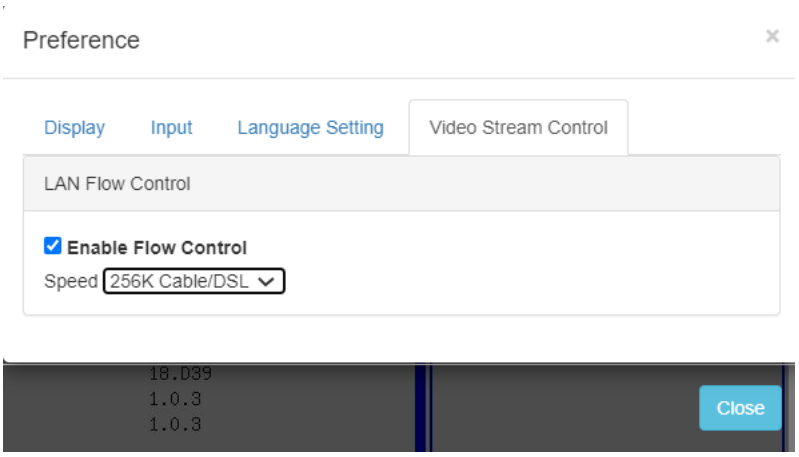


Figure 2-134: Video Stream Control Settings

2.7.2f IKVM/HTML5 — User List

This feature displays the user list, which shows the Session ID, User Name, and IP Address of active users who are currently accessing the HTML5-IKVM.

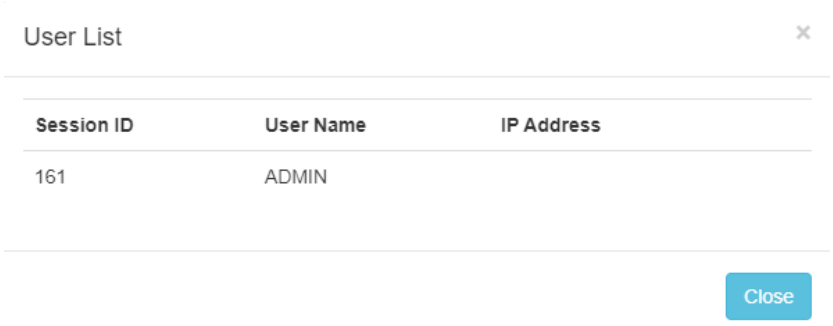


Figure 2-135: User List Settings

2.7.2g IKVM/HTML5 — Capture

Capture allows you to save an image of the current screen.

Figure 2-136: Capture Setting on Side Bar

2.7.2h IKVM/HTML5 — Power Control

This feature allows you to perform Power On, Power Off, Software Shutdown, and Power Reset operations.

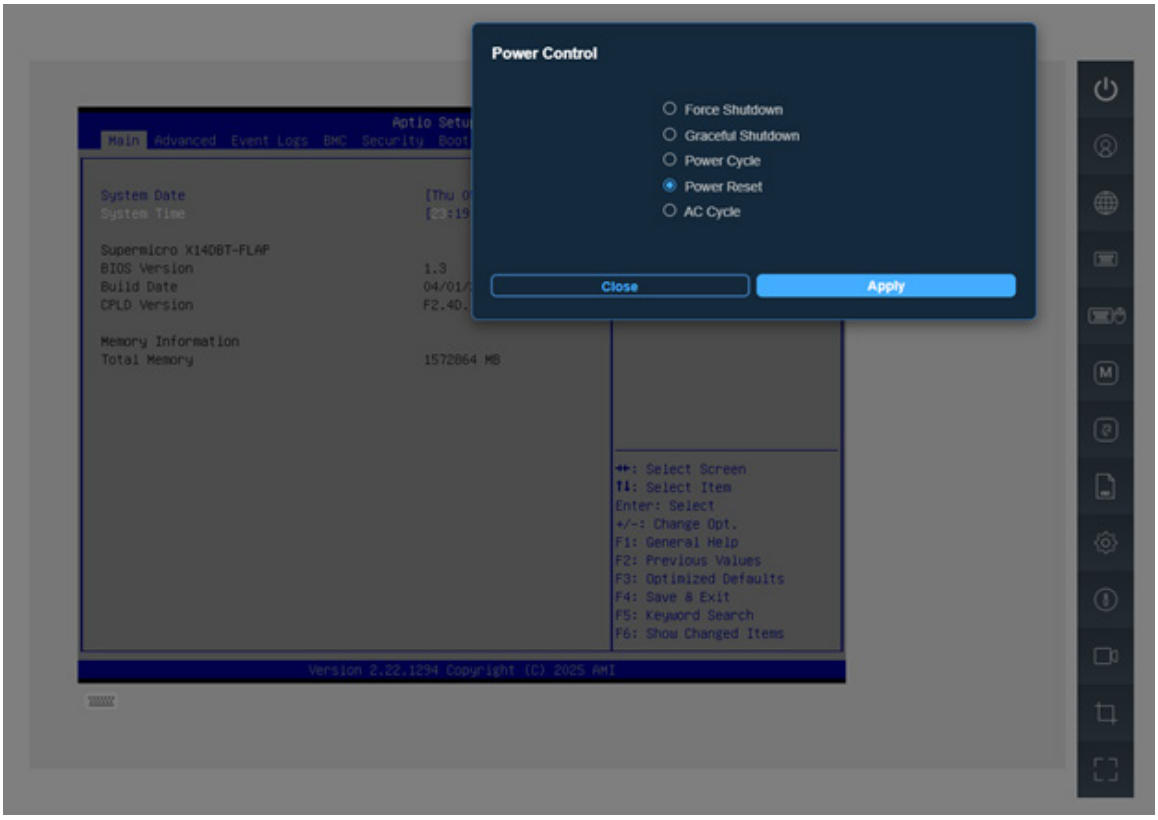


Figure 2-137: Power Control Submenu

2.8 Maintenance

This page allows you to perform maintenance activities such as firmware management, maintenance events, troubleshooting, BMC reset operations, and many more.

Note: The number of Maintenance Event Log entries is limited to 4096.

2.8.1. Firmware Management

The firmware management page allows administrators to update firmware for BMC, BIOS, Motherboard CPLD, Backplane CPLD, Network AOC, GPU AOC, Storage AOC, Retimers, etc.

Note: Systems are required to power down prior to BIOS update and are required to reboot after firmware updates for network AOC and/or storage AOC.

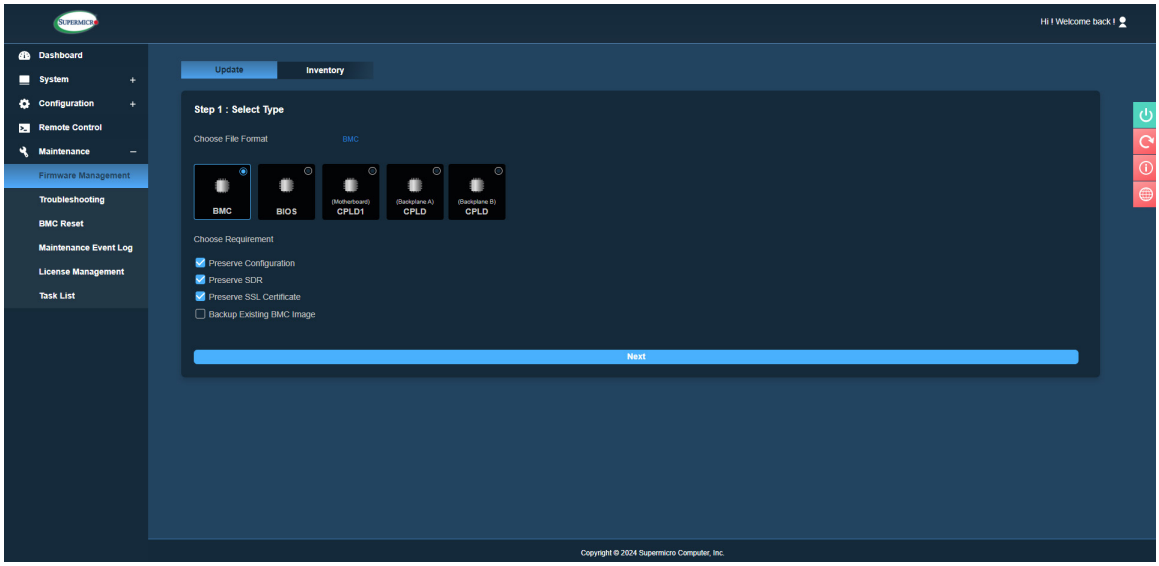


Figure 2-138: Firmware Management Page

Update

If you have administrator privileges, this page allows you to update component firmware. You can view the current and new firmware versions through the Web UI during the update process (BMC, BIOS, etc.). The update typically completes within five to ten minutes.

To update firmware, refer to the following steps:

1. Select a component to update firmware.
2. If applicable, select preserve configuration options.
3. Select a firmware file to upload. If you click the 'Upload' button without a firmware image, a message will inform you to *“Please select an image file. Click here to return.”*

   Note: If you select an invalid or incorrect file, the error message should be, *"Invalid update package. The firmware update failed. Click here to return."* MEL-0184 should be logged to the Maintenance event logs for BMC/BIOS image verification failed.

4. Update the firmware by clicking the “Update” button. You can check firmware update progress in the Task List page. Once the firmware is in the update mode, the device will be reset, and the server will reboot even if you cancel the firmware update. If you cancel the firmware updating process, there will be an alert message that pops up to ask you: *“Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode.”* Upon confirmation, BMC is then reset with the message: *“BMC is restarting to continue the BMC firmware update process. To prevent data loss, please Do Not Remove power source until BMC is back online!”*

   Note: Refresh the Web Browser / BMC UI of the secondary UI (viewing web browser) needs to renew the BMC connection since the viewing web browser has stopped sending the request after the firmware update was initiated. A message for you to wait for BMC will be, *“BMC is restarting to continue the BMC firmware update process. To prevent data loss, please Do Not Remove power source until BMC is back online!"*

A BMC update supports the following preserve configuration options:

- Preserve Configuration
- Preserve SDR
- Preserve SSL Certificate
- Backup Existing BMC Image

To update the BIOS firmware, navigate to the 'Update' tab within the Firmware Management section. You can choose the appropriate radio button for the BIOS option. You have the flexibility to select either the 'Next-boot Update' or 'Immediate Update' mode, allowing you to schedule when the BIOS firmware will undergo an update.

Following this, you can proceed to select the desired BIOS options that you wish to preserve. Opting for the 'Next-boot Update' mode will ensure that the BIOS firmware update is scheduled for execution after the system undergoes a reboot. If you've uploaded the BIOS firmware and need to halt the process, you have the option to abort the pending update.

For your convenience, you can monitor the update status of the BIOS firmware. If necessary, you can cancel the 'Next-boot Update' procedure by utilizing the delete icon located on the Task List page.

BIOS update supports the following preserve configuration options. The specific options available depend on the platform.

- Preserve SMBIOS
- Preserve BIOS Boot Options Configuration
- Backup Existing BIOS image
- Preserve OA
- Preserve BIOS Setup Configuration
- Preserve BIOS Setup Password
- Preserve BIOS Setup Secure Boot Keys
- Preserve BIOS Setup Options Configuration

Note: If the Rollback ID of the current firmware is higher than that of the previous firmware, a prompt will appear asking, *" Flashing the new firmware will make the system incompatible with any firmware versions lower than the uploaded firmware. As a result, the Backup and Golden images will be updated to the new firmware version. Are you sure you want to proceed?"* This confirmation is designed to ensure your consent before proceeding with the BIOS firmware update. After the firmware update process is complete, both the backup and golden images will be updated as well.

Note 2: Select the 'Backup existing image' option to back up the existing BMC or BIOS image. Backup image will be used for auto-recovery in case of failed integrity at any time. You can also manually recover the BMC or BIOS from the backup image. Go to the Inventory tab to manually recover BMC or BIOS.

Note 3: Due to the limitation of the current BMC implementation, you might experience a long waiting period to refresh the web browser after the update is completed. You might also see the rebooting message for a minute or two when logging back in before the update is completed.

How BMC Firmware is Updated

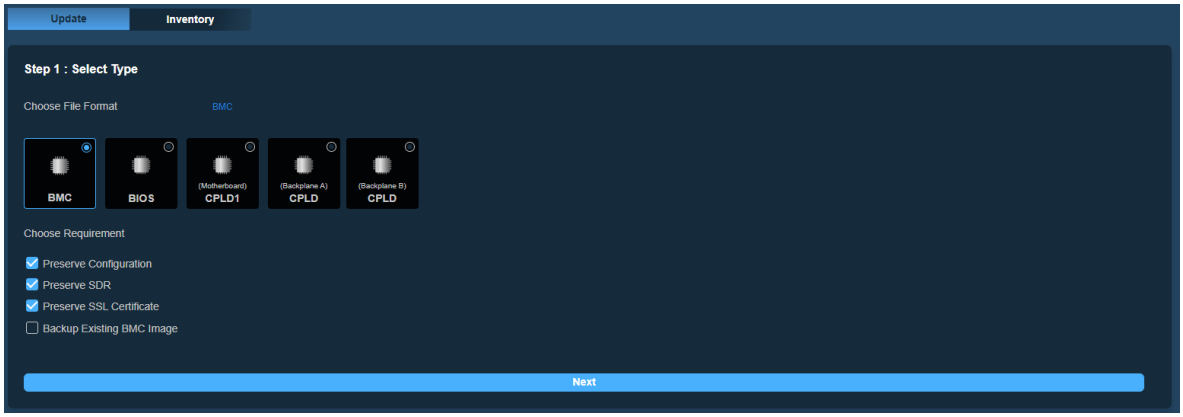


Figure 2-139: BMC Firmware Update Step 1

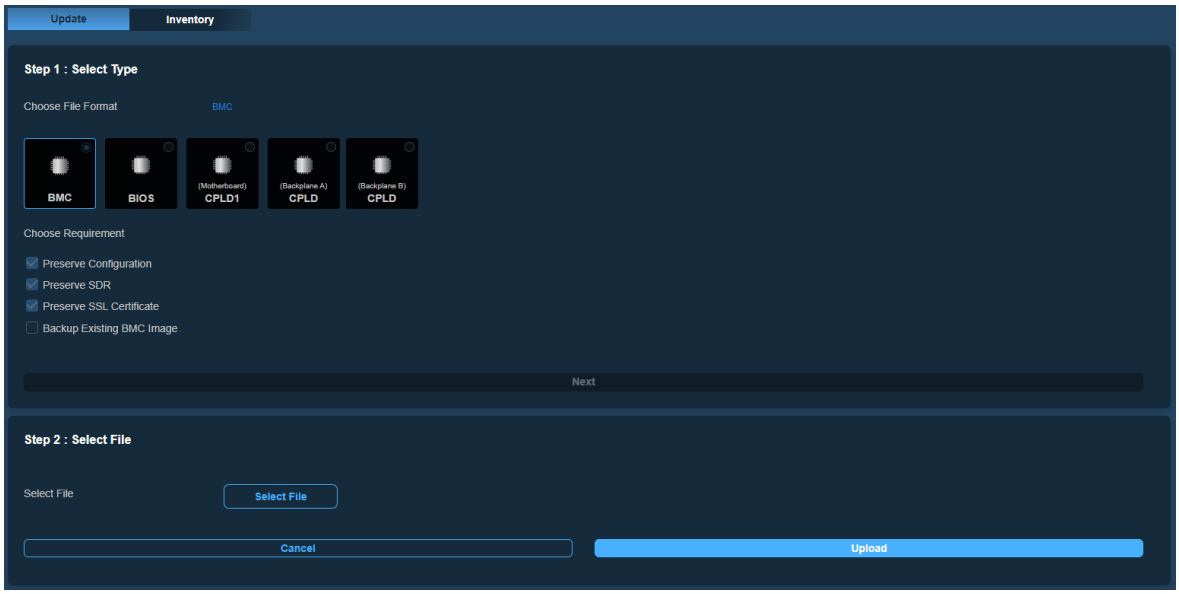


Figure 2-140: BMC Firmware Update Step 2

If you click the “Upload” button without the BMC image, a message will inform you to “*Please select an image file. Click here to return.*”

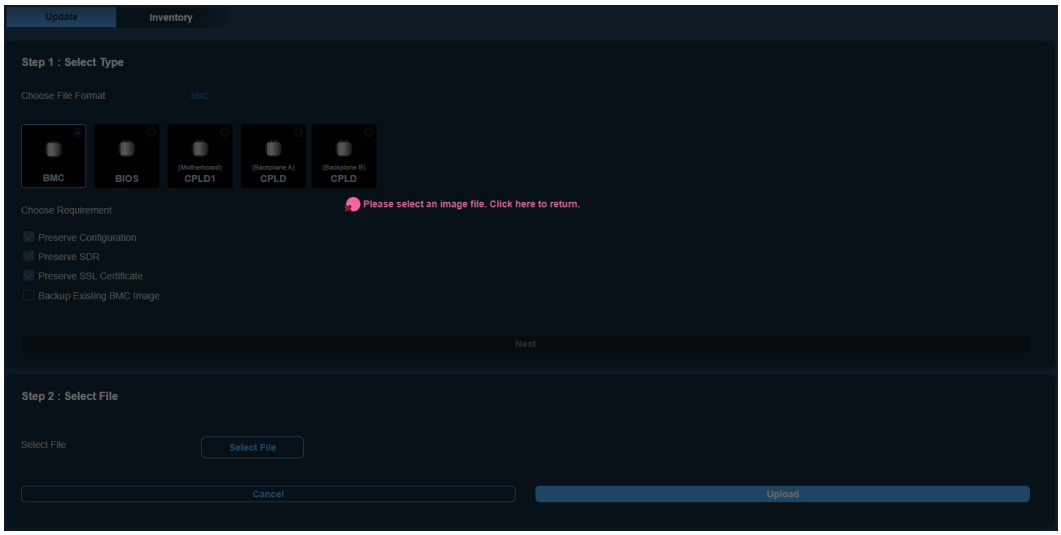


Figure 2-141: Error Message If An Image File is Not Selected

If you continue with the BMC update, the BMC will provide a timely percentage of completion.

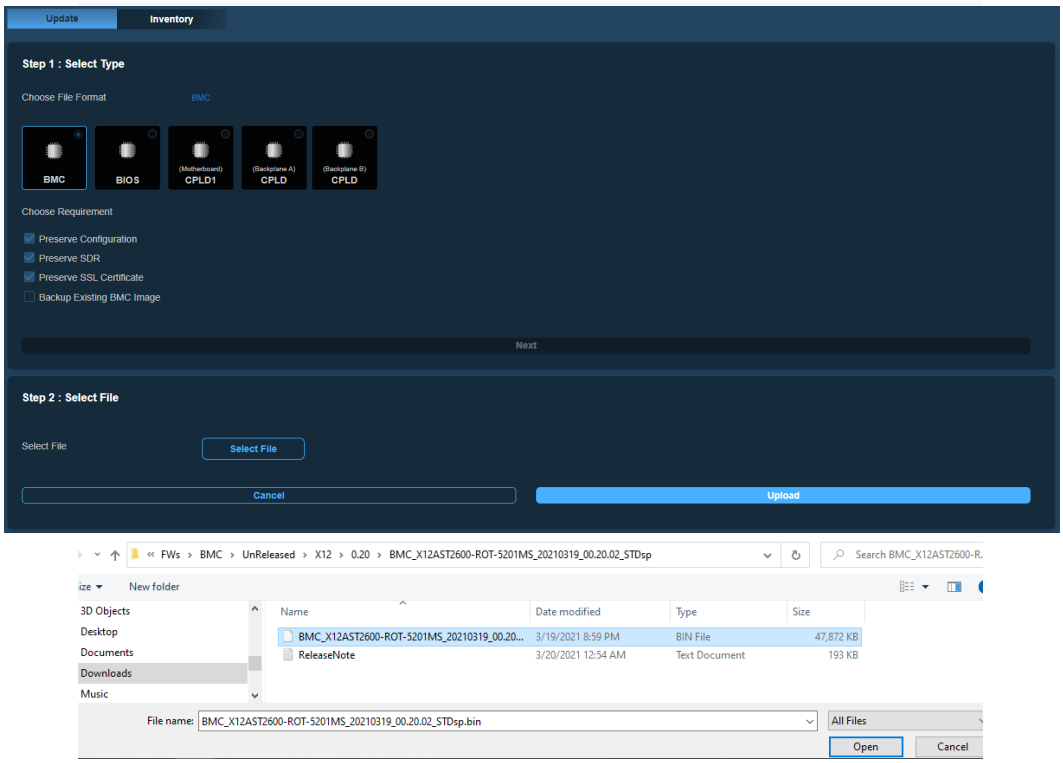


Figure 2-142: BMC Firmware Update Step 2 Selecting a File

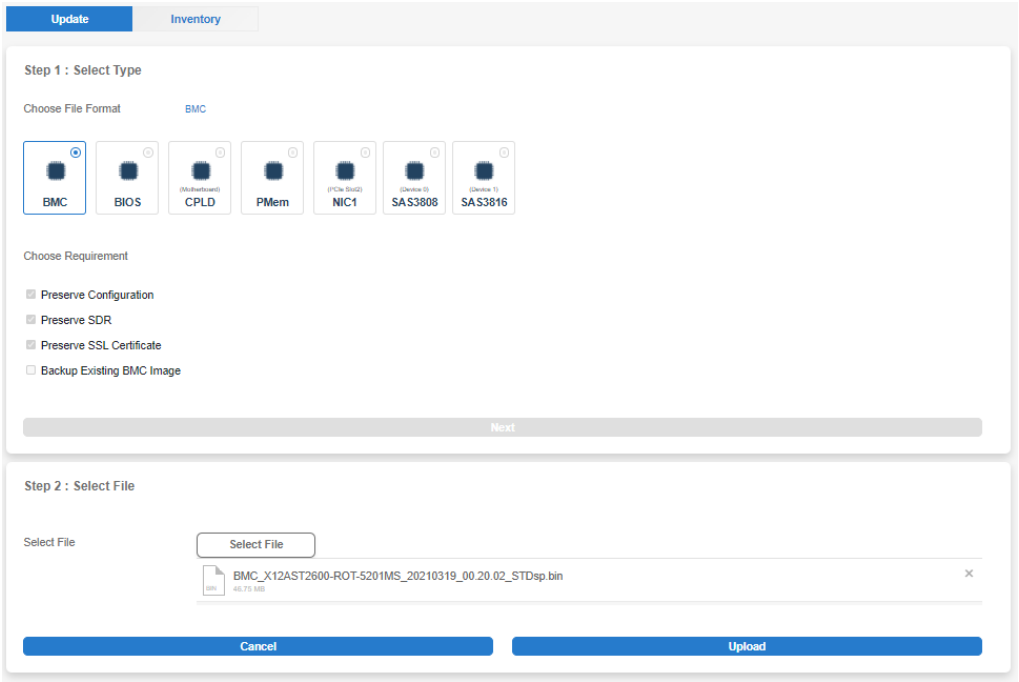


Figure 2-143: BMC Firmware Update Step 2 File Selected

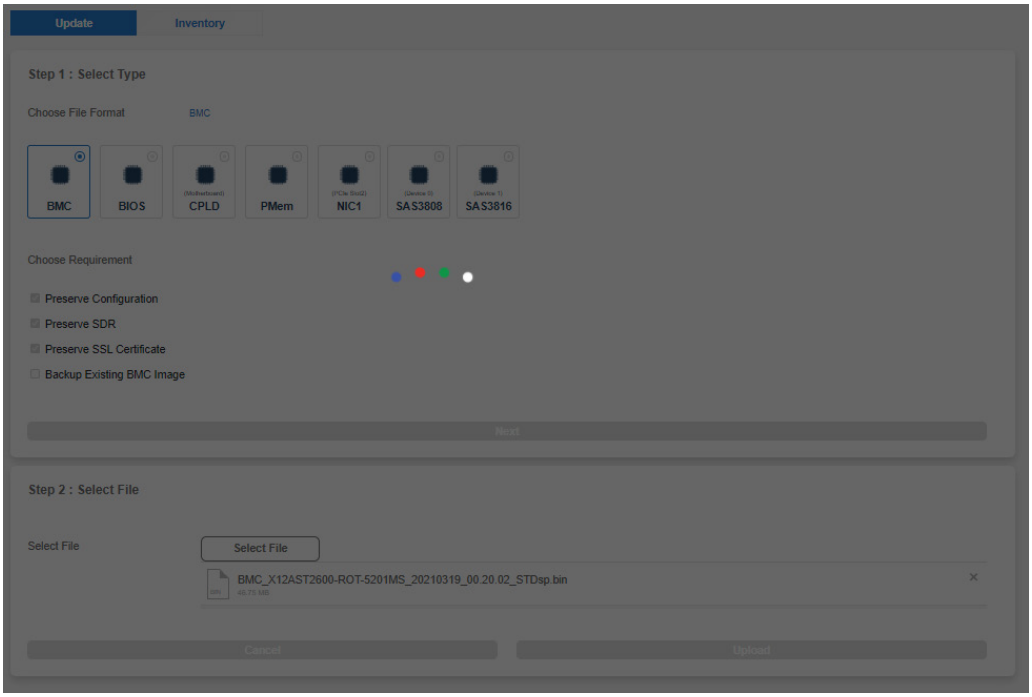


Figure 2-144: File Upload Loading

Note: You can view the current firmware version and the new firmware version through Web UI when they update the firmwares.

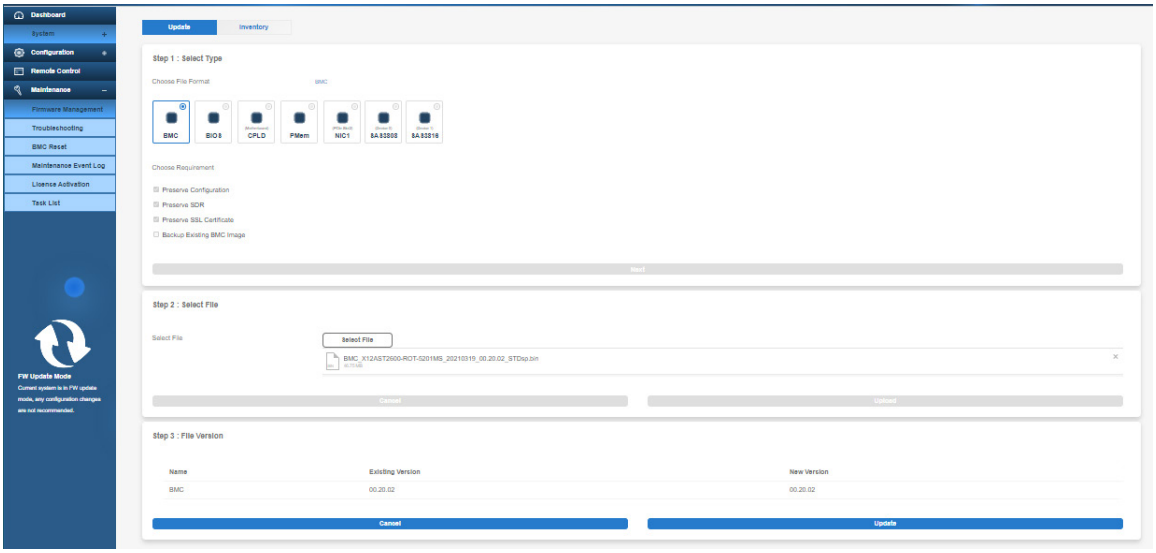


Figure 2-145: Firmware Management Step 3

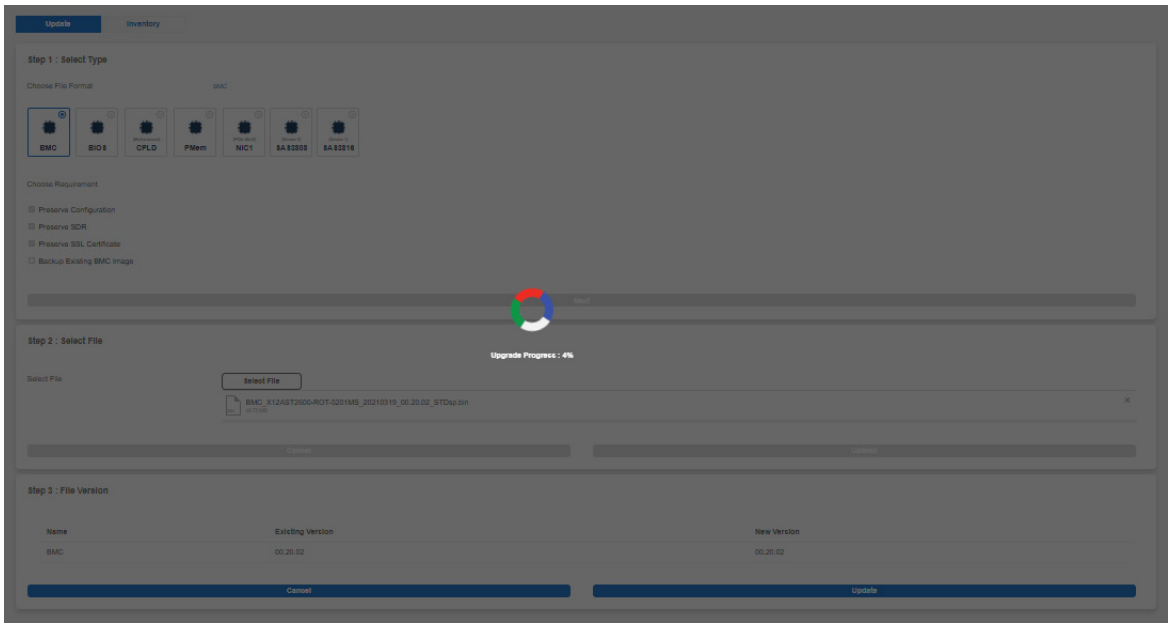


Figure 2-146: Upgrade Progress 4%

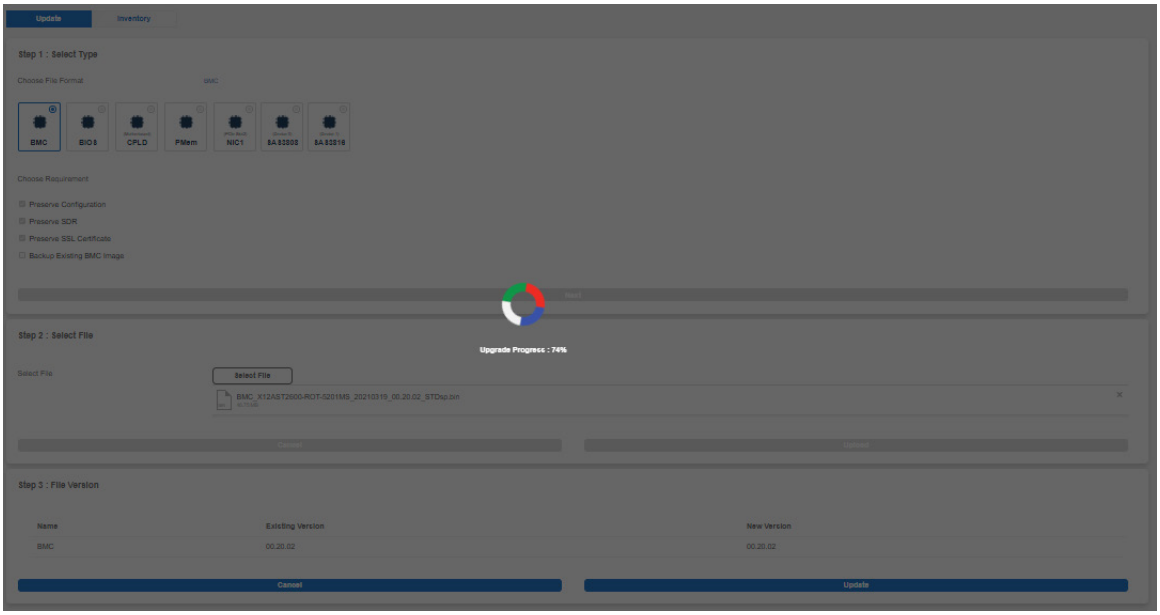


Figure 2-147: Upgrade Progress 74%

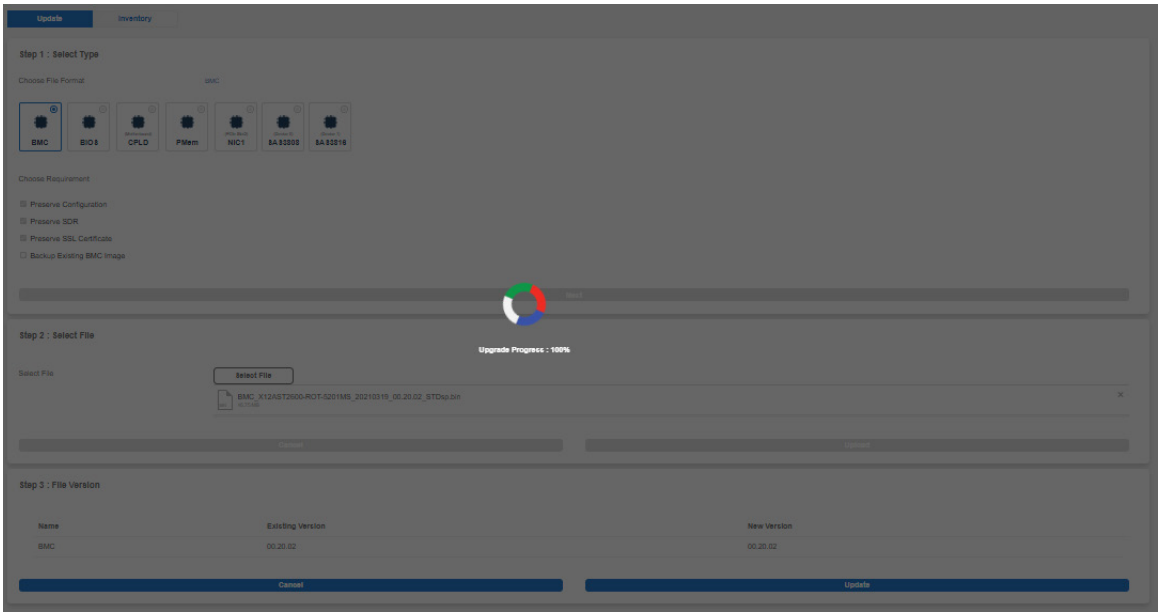


Figure 2-148: Upgrade Progress 100%

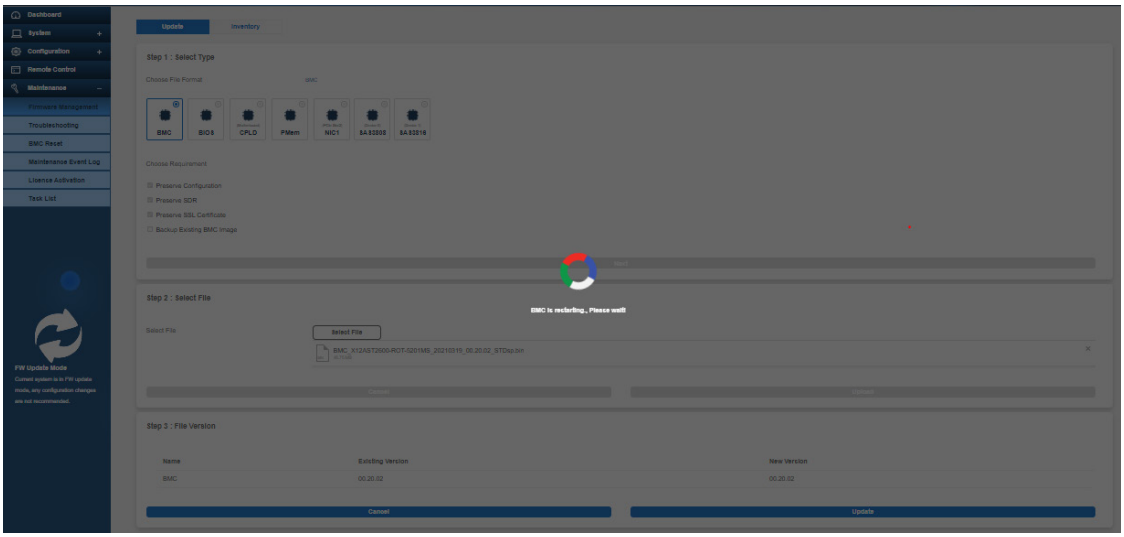


Figure 2-149: BMC Restart Loading Message

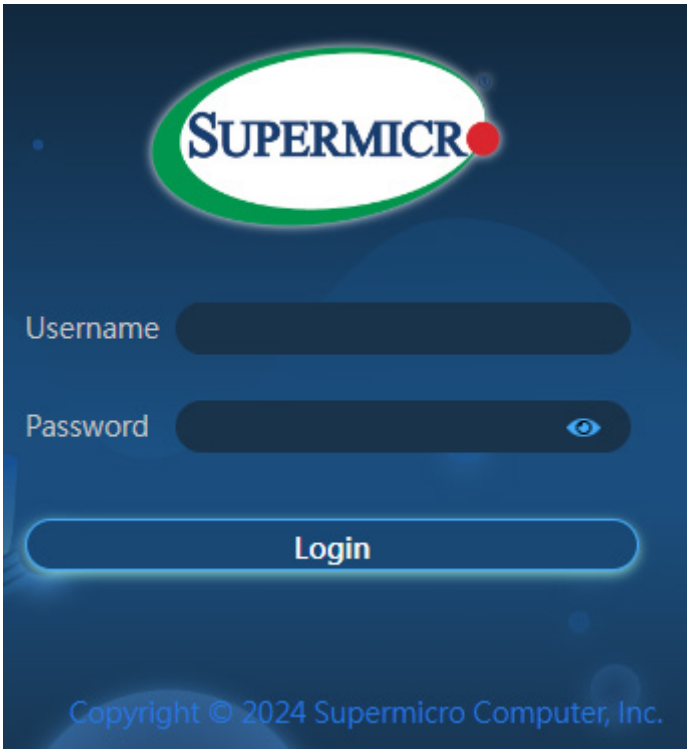


Figure 2-150: Login Screen

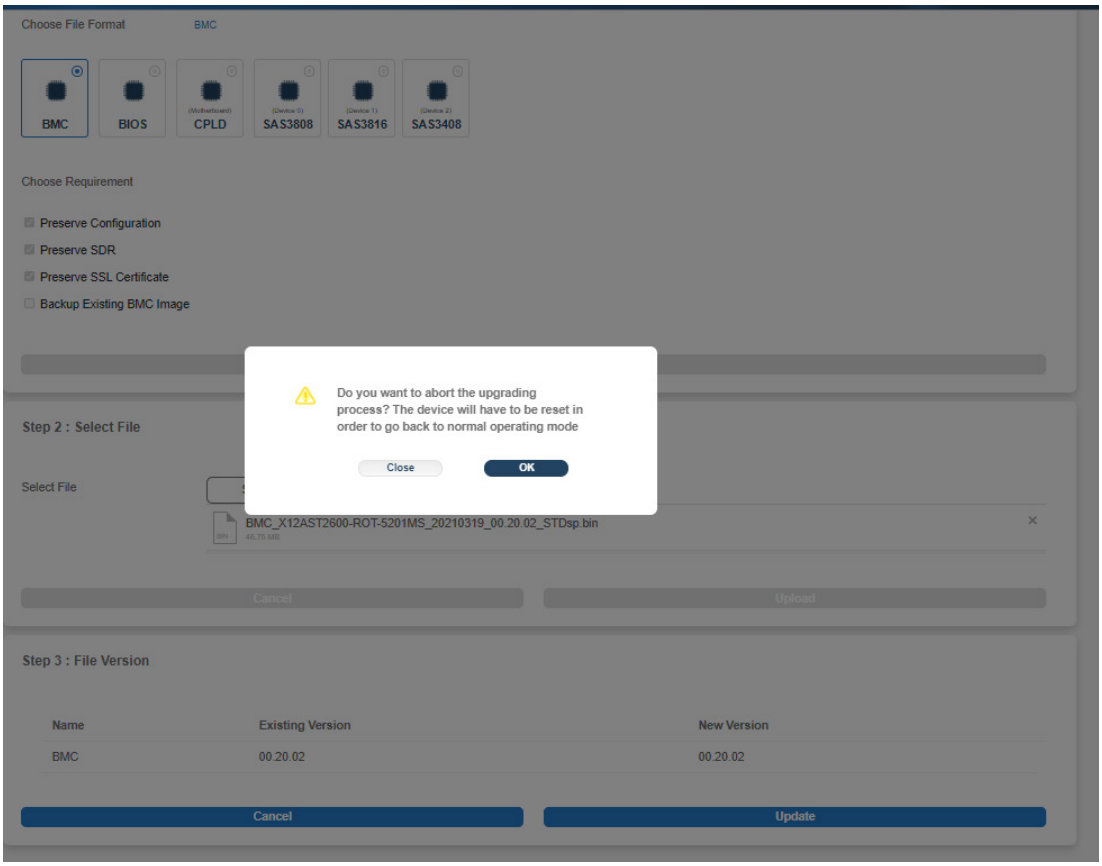


Figure 2-151: Abort Upgrading Process Alert Message

Note: If you cancel the BMC updating process, there will be an alert message popping up to ask you, "*Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode."* BMC is then reset with the message *"BMC is restarting. To prevent data loss, upon confirmation, please do NOT remove the power source until BMC is back online!"*

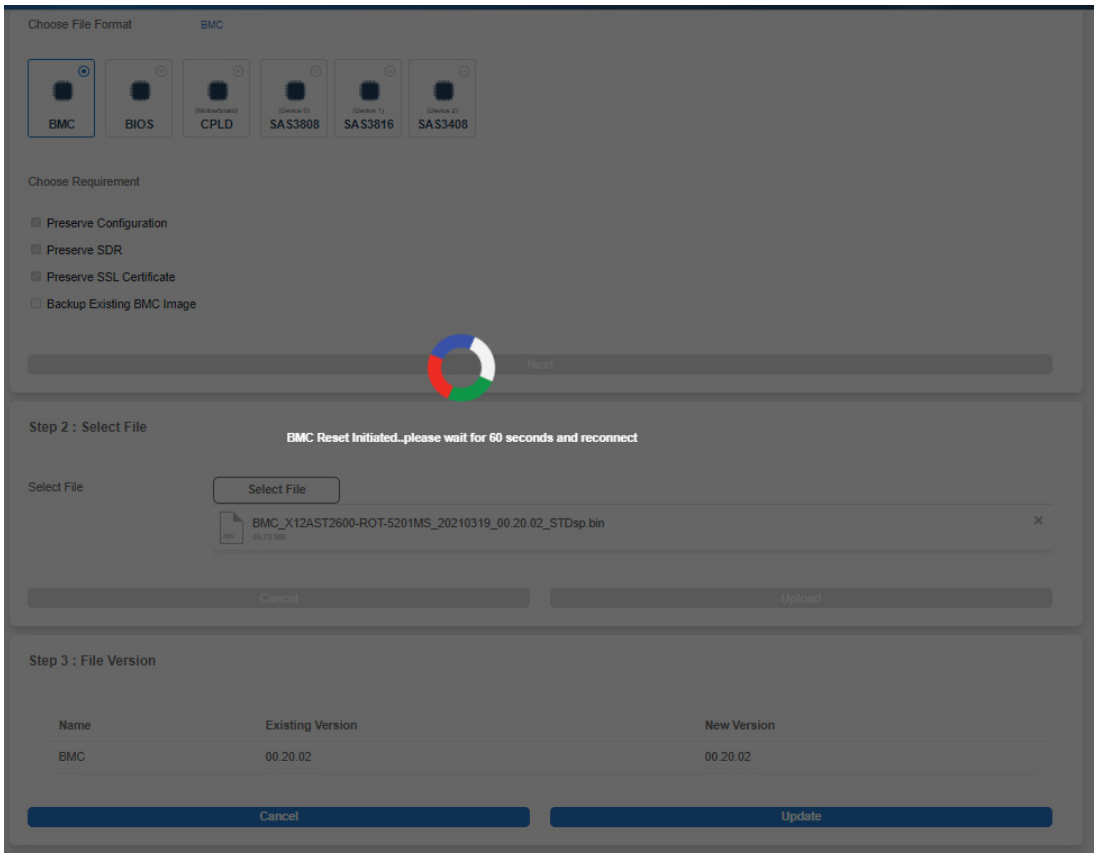


Figure 2-152: BMC Reset Intiated Loading Message

How BIOS Firmware is Updated

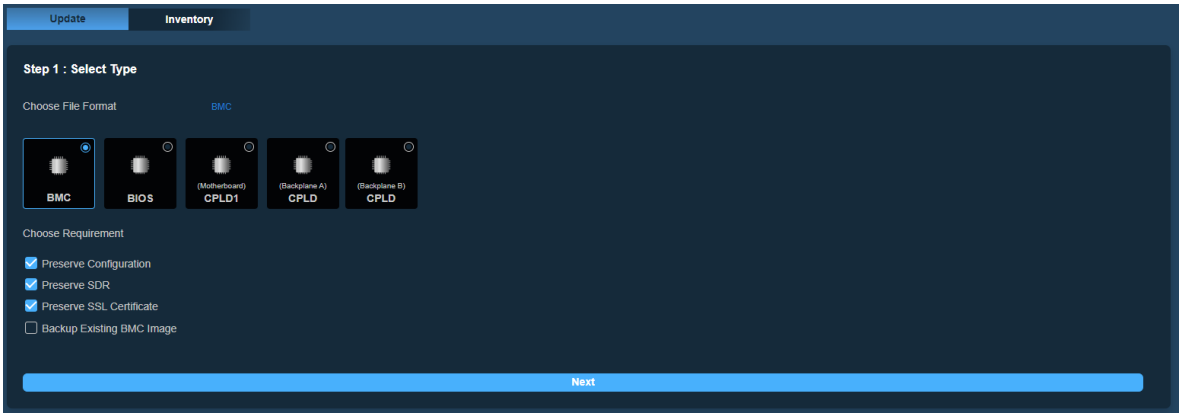


Figure 2-153: Select File Format

Figure 2-154: Choose Requirement

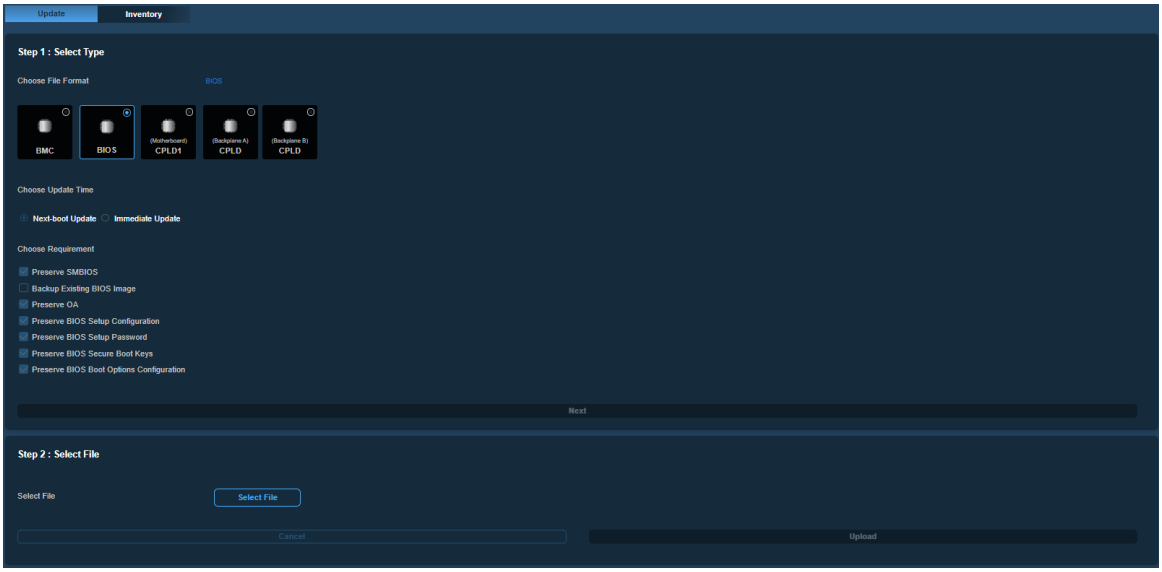


Figure 2-155: Select File

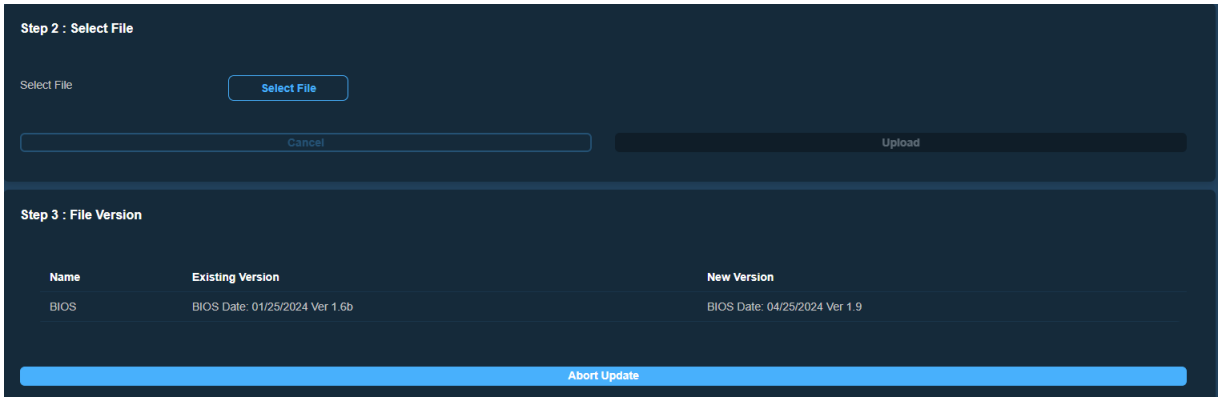


Figure 2-156: File Version

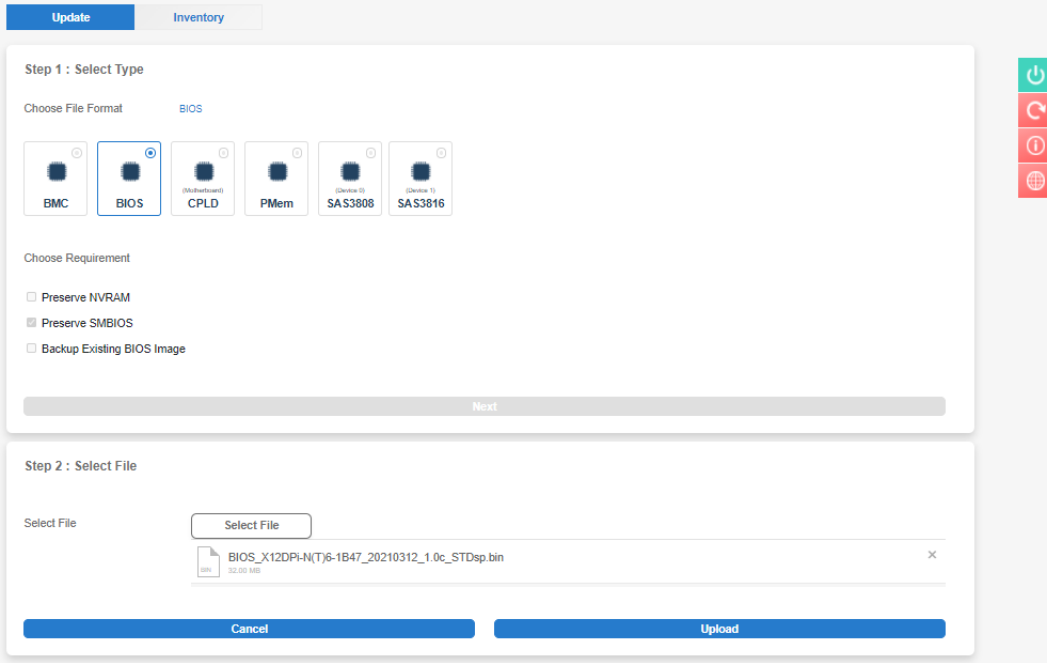


Figure 2-157: File Selected

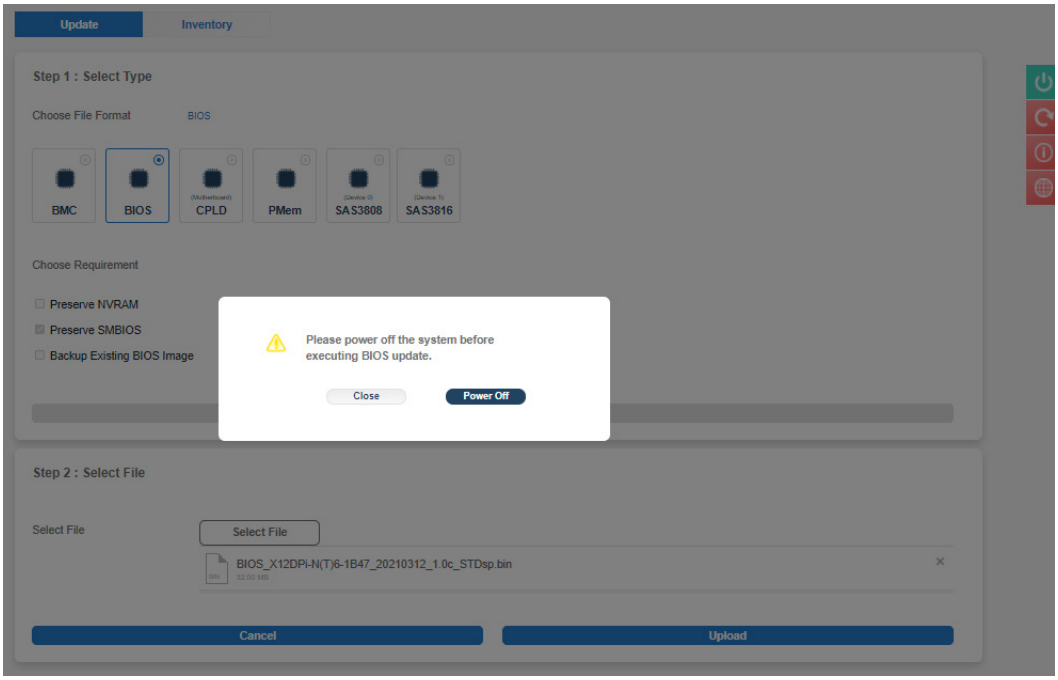


Figure 2-158: Alert Message to Power Off System Before Update

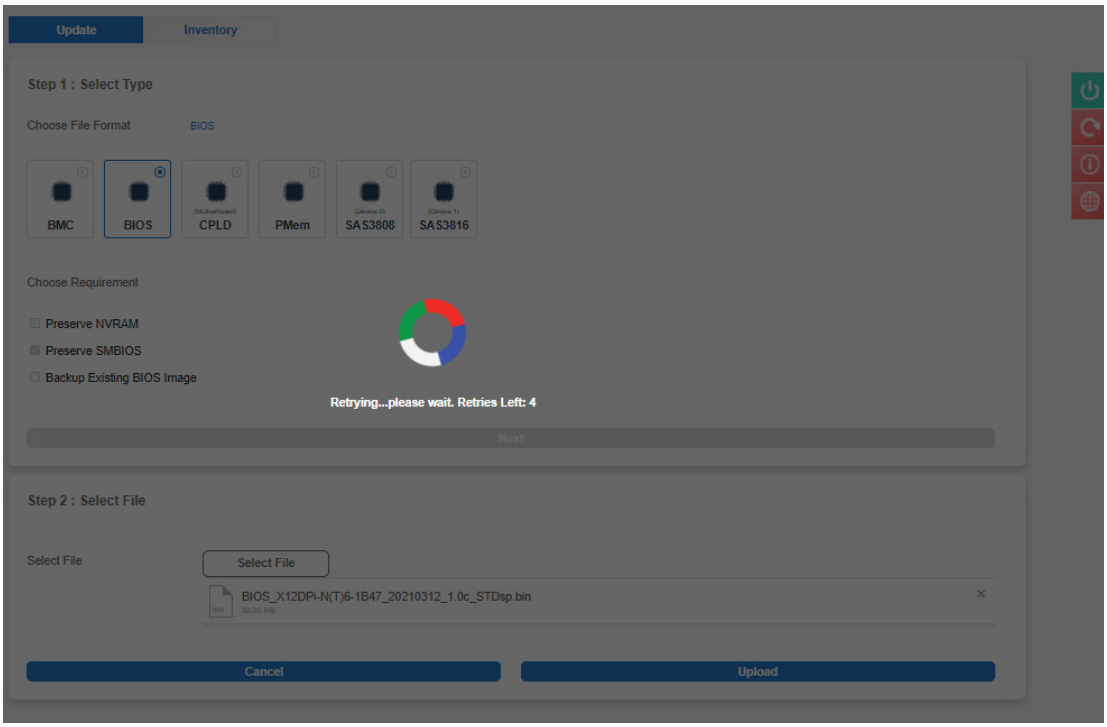


Figure 2-159: Retrying Loading Message

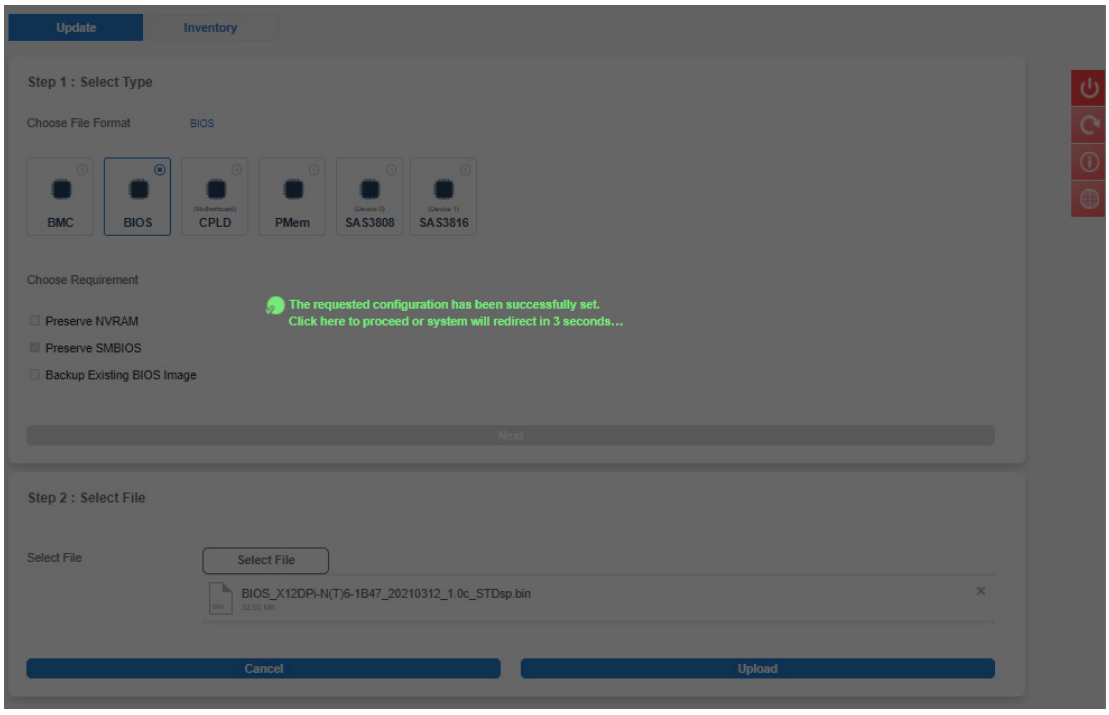


Figure 2-160: Requested Configuration Successfully Set Message

If you click "Upload" without a BIOS image included, a message will inform you to *"Please select an image file. Click here to return."*

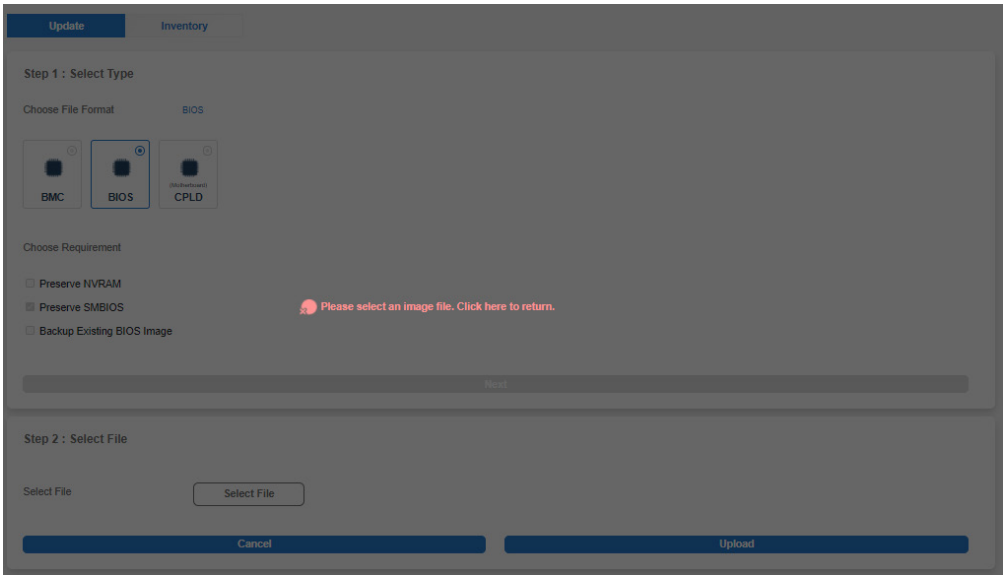


Figure 2-161: Uploading Without BIOS Image Alert Message

If you continue with the BIOS update, BMC will provide a timely percentage of completion.

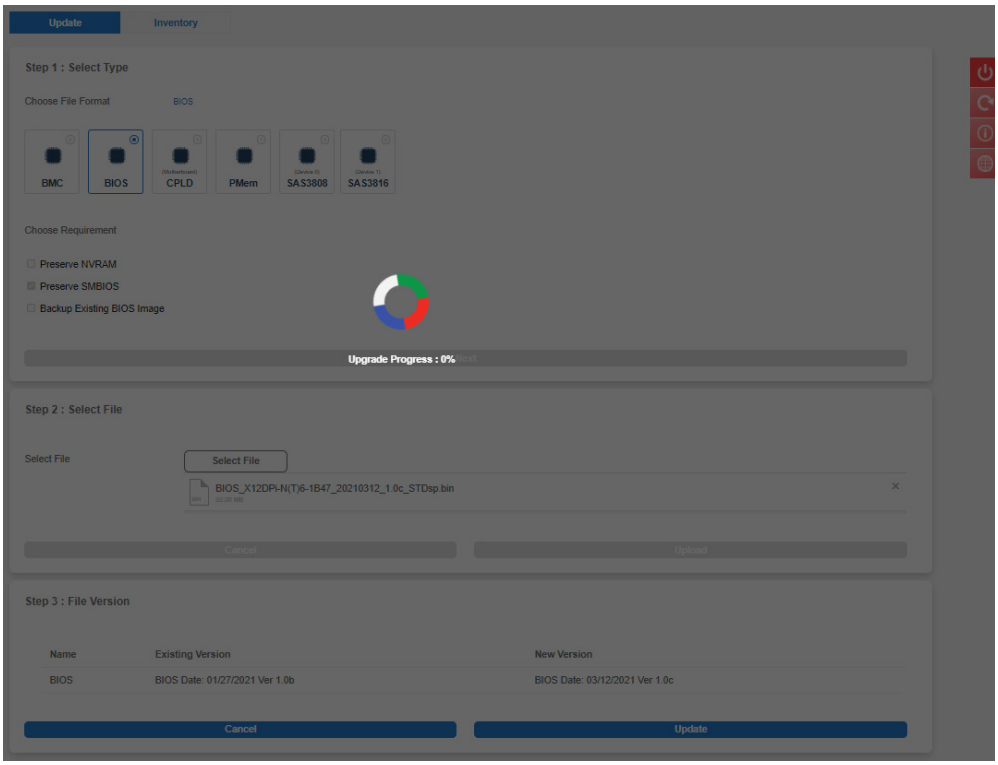


Figure 2-162: Upgrade Progress 0%

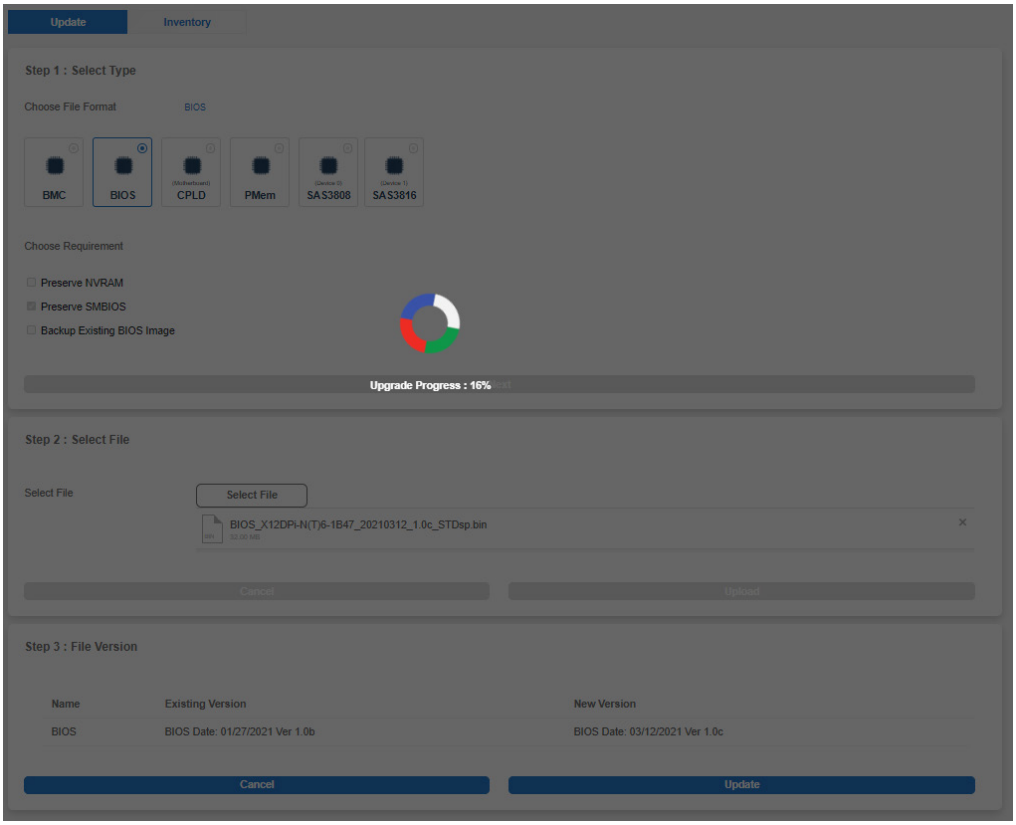


Figure 2-163: Upgrade Firmware Progress 16%

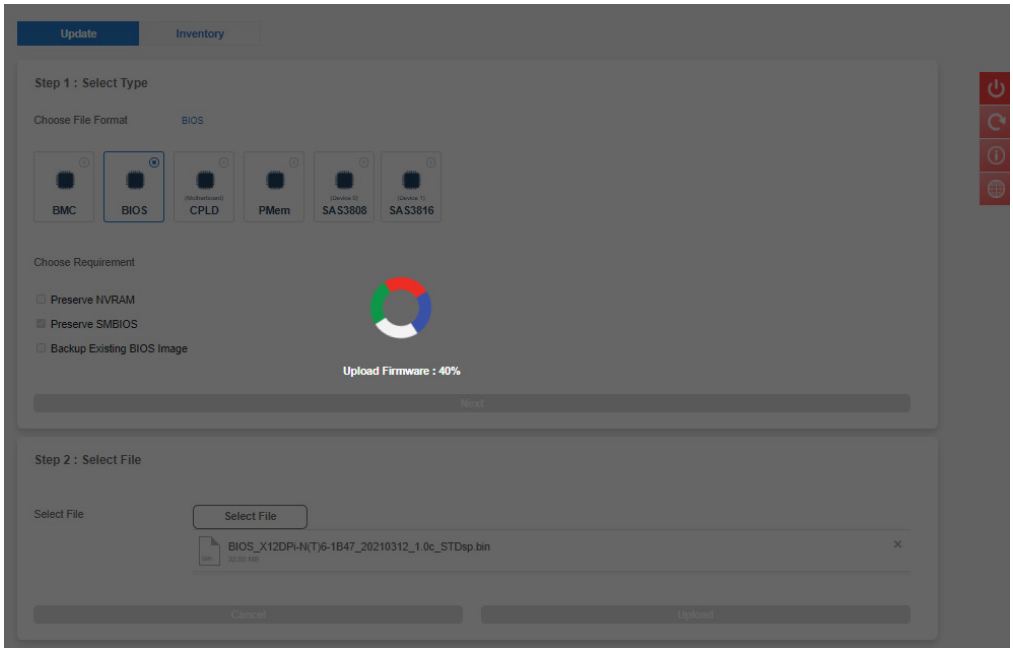


Figure 2-164: Upload Firmware Progress 40%

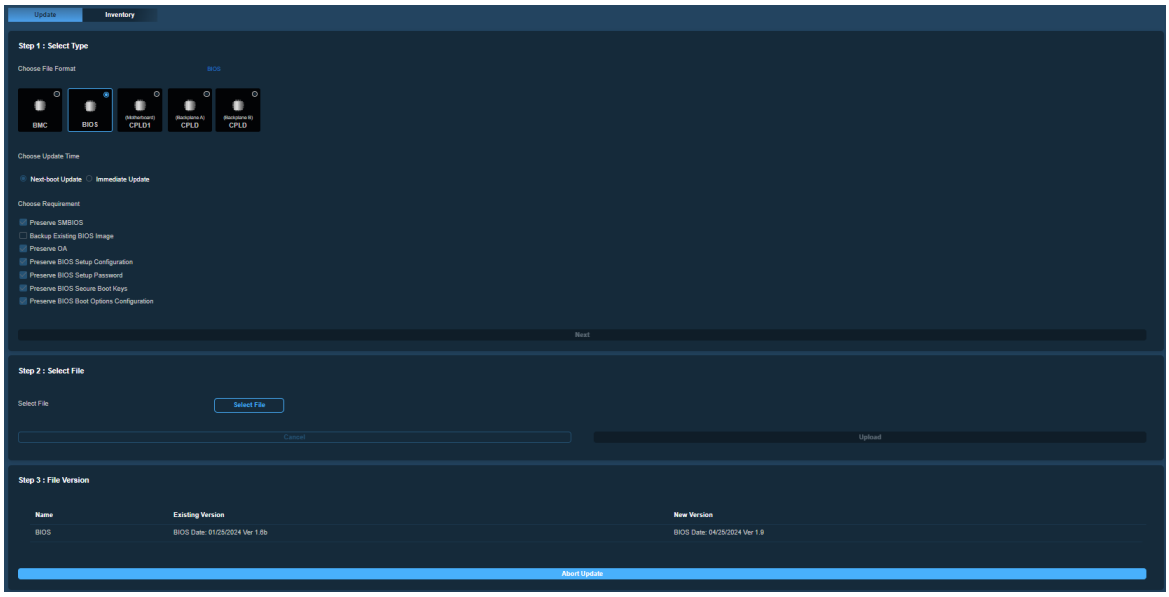


Figure 2-165: File Uploaded

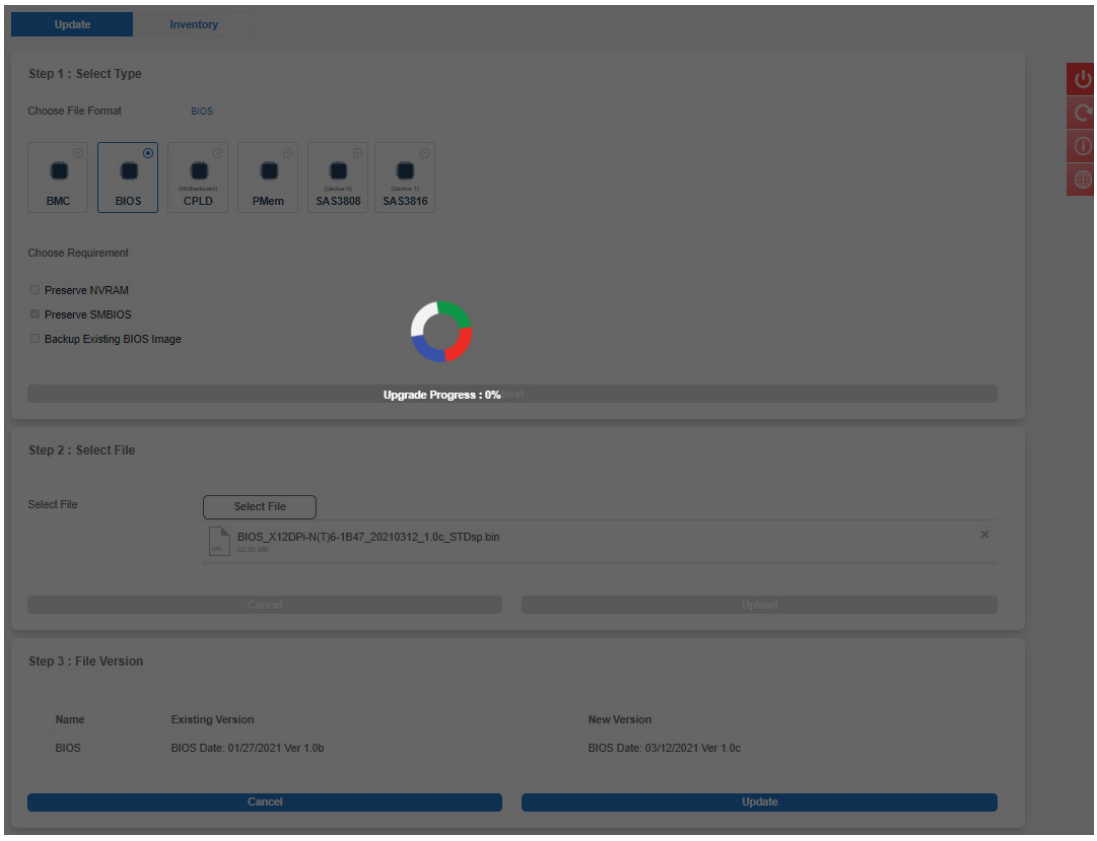


Figure 2-166: Upgrade Progress 0%

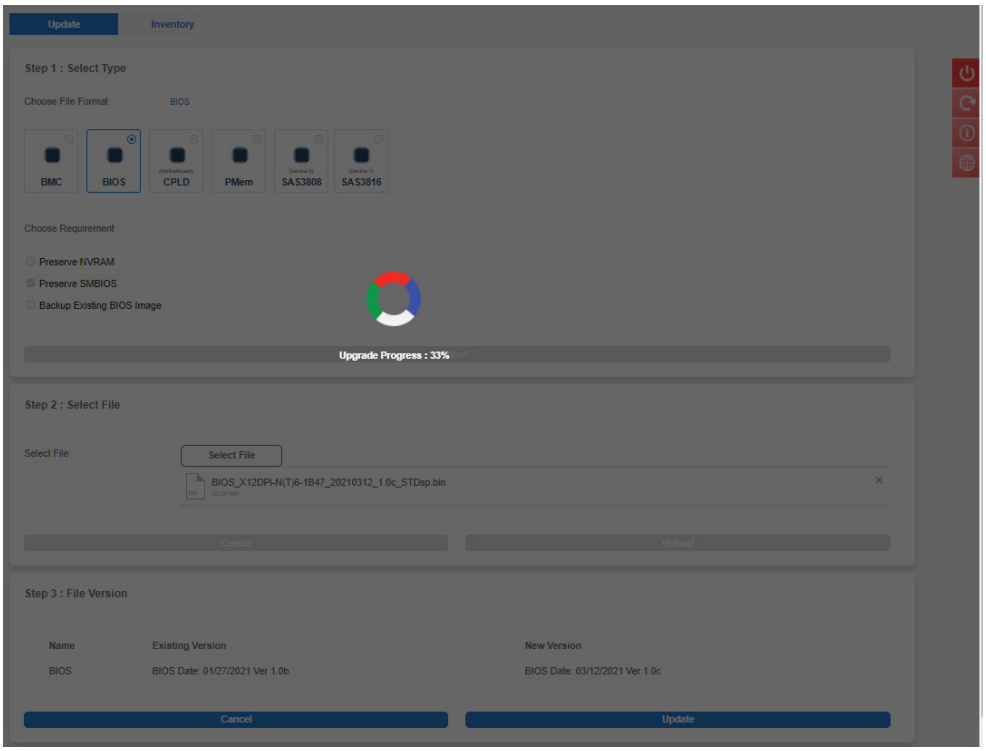


Figure 2-167: Upgrade Progress 33%

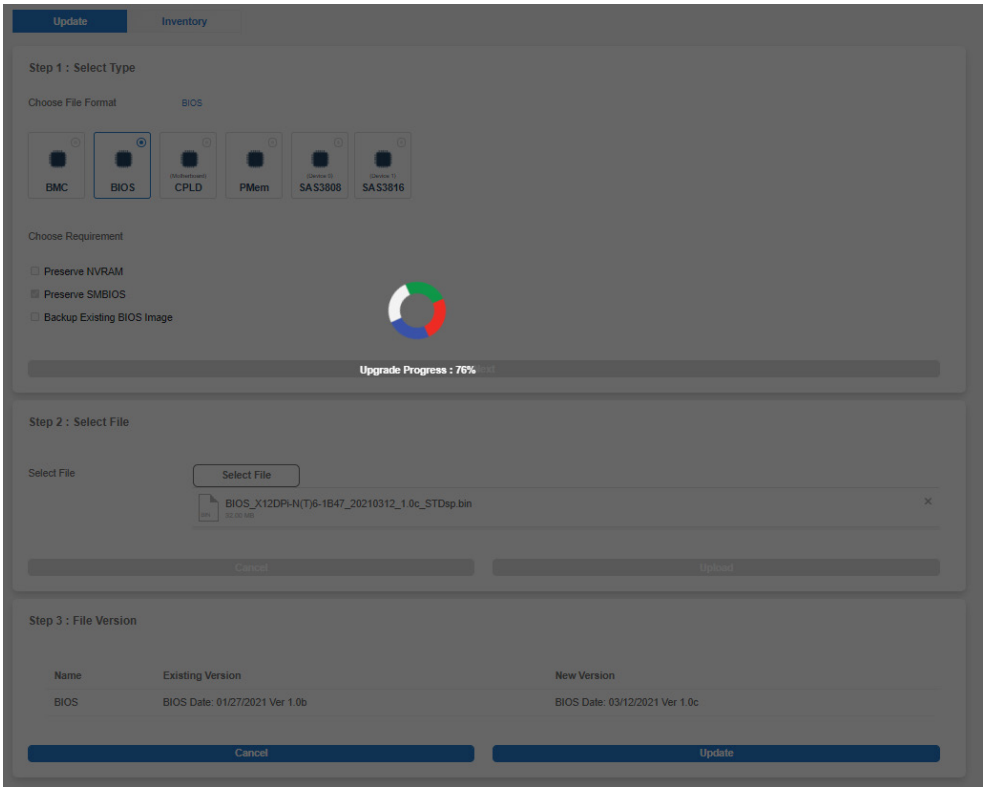


Figure 2-168: Upgrade Progress 70%

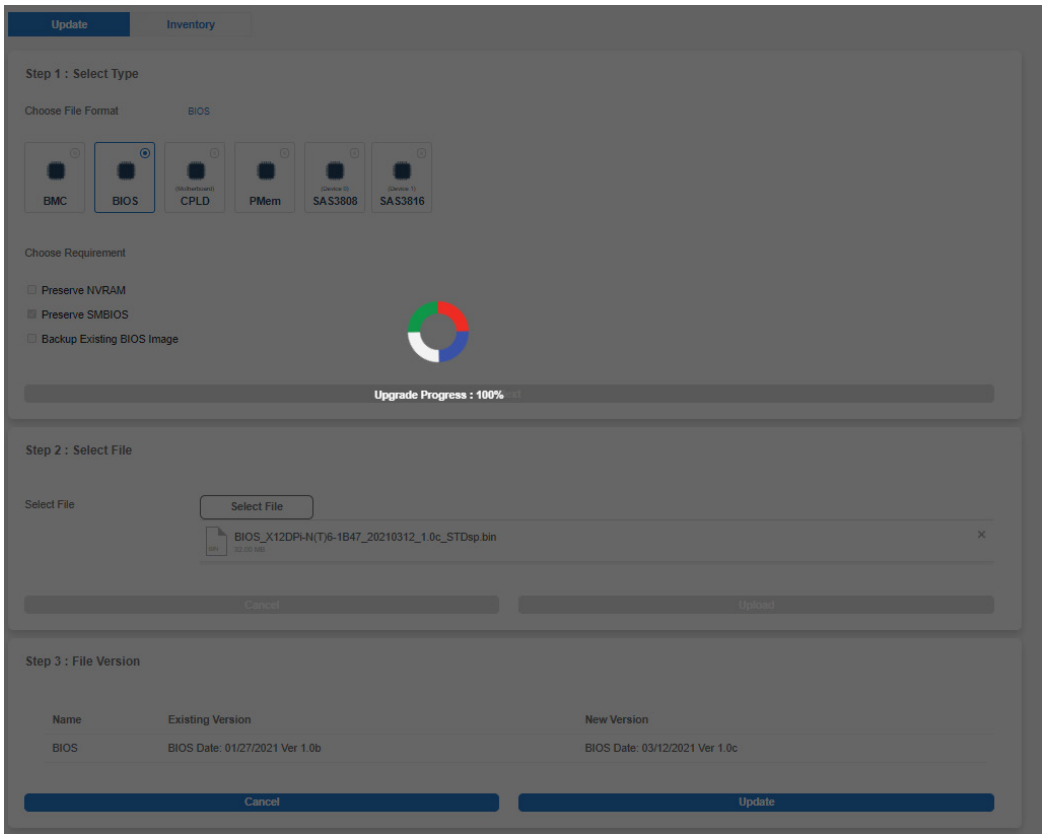


Figure 2-169: Upgrade Progress 100%

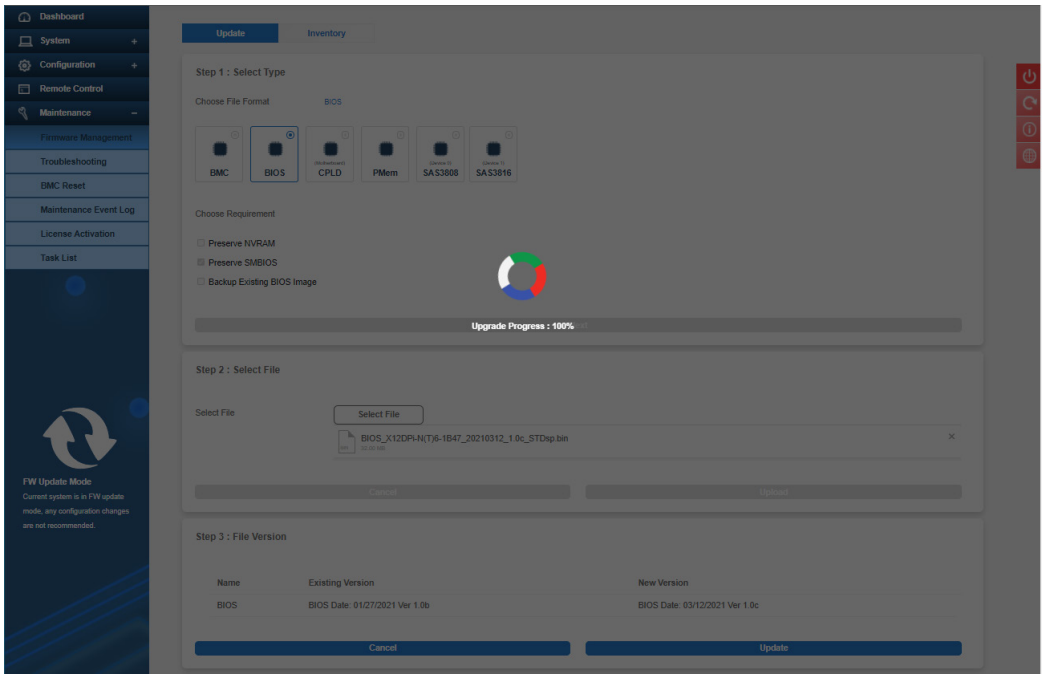


Figure 2-170: Upgrade Progess 100%

Note: If you cancel the BIOS updating process, there will be an alert message that pops up to ask you, *"Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode."* BMC is then reset with a message *"BMC Reset Initiated..please wait for 60 seconds and reconnect"* upon confirmation.

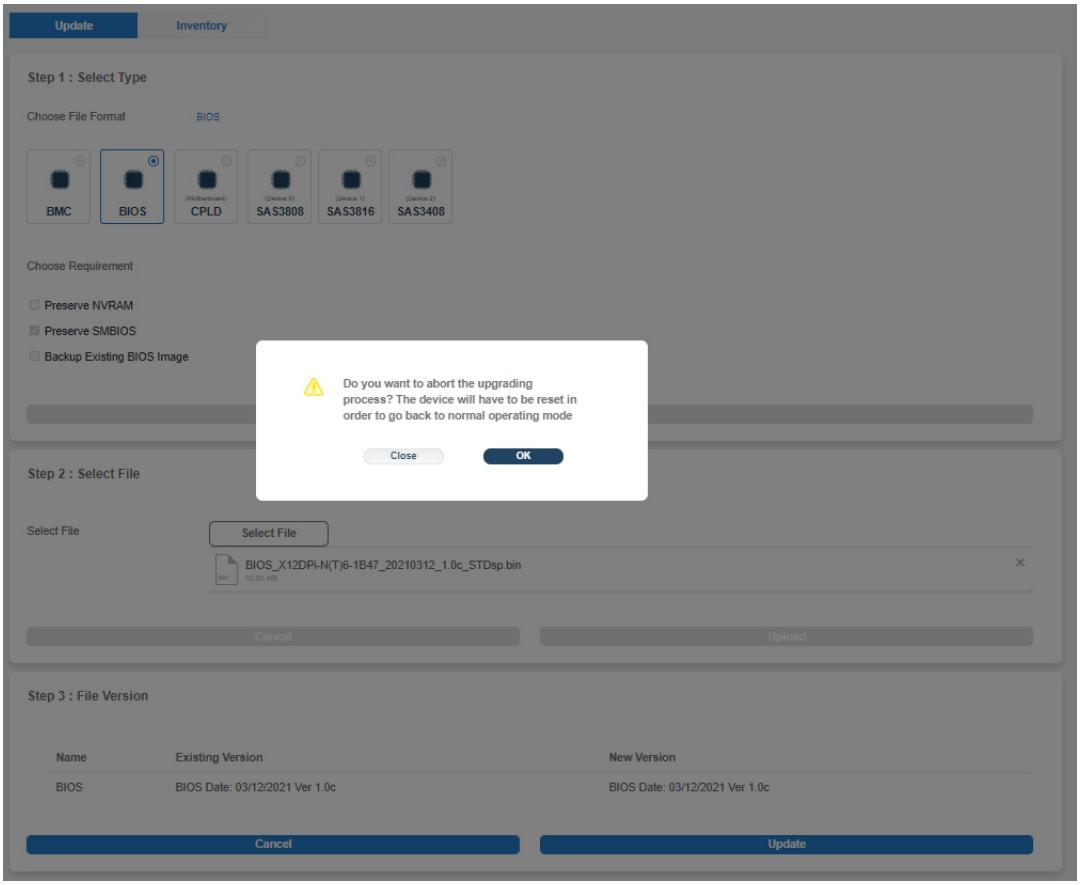


Figure 2-171: BIOS Update Alert Message

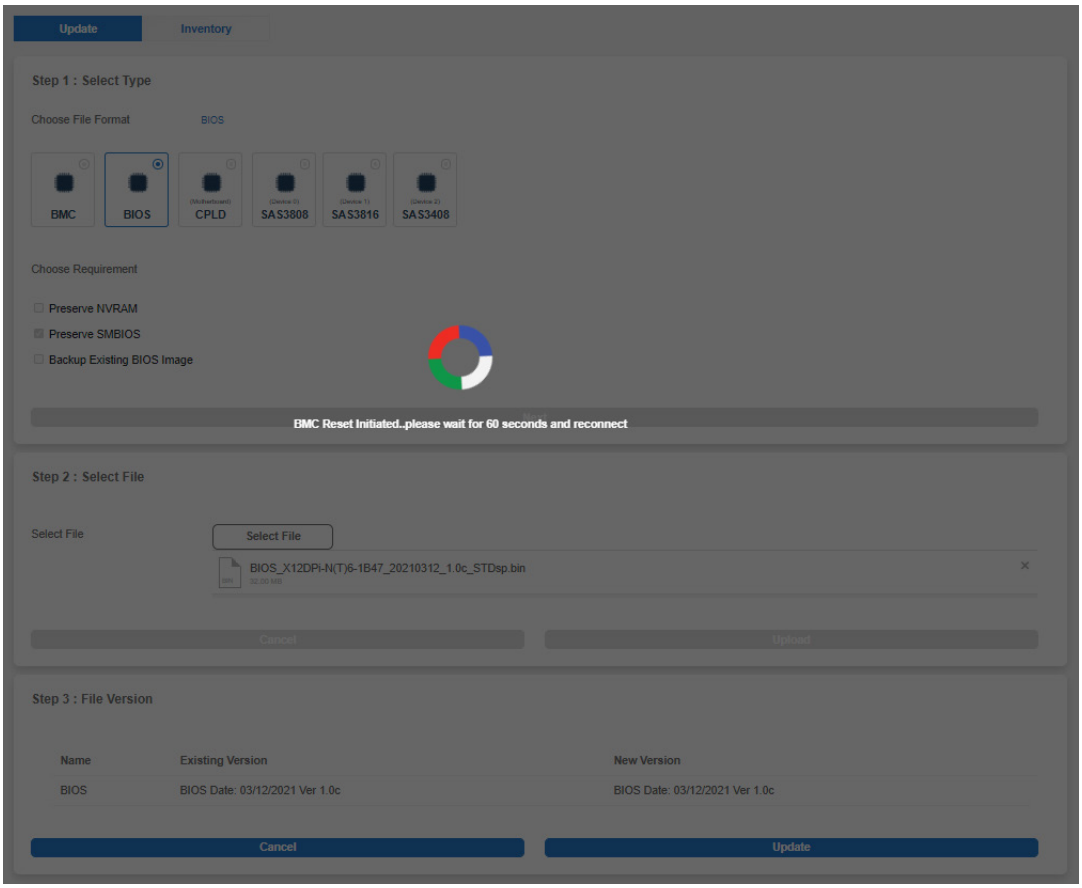


Figure 2-172: BMC Reset Initiated Loading Page

Inventory

Use this page to view the component firmware inventory.

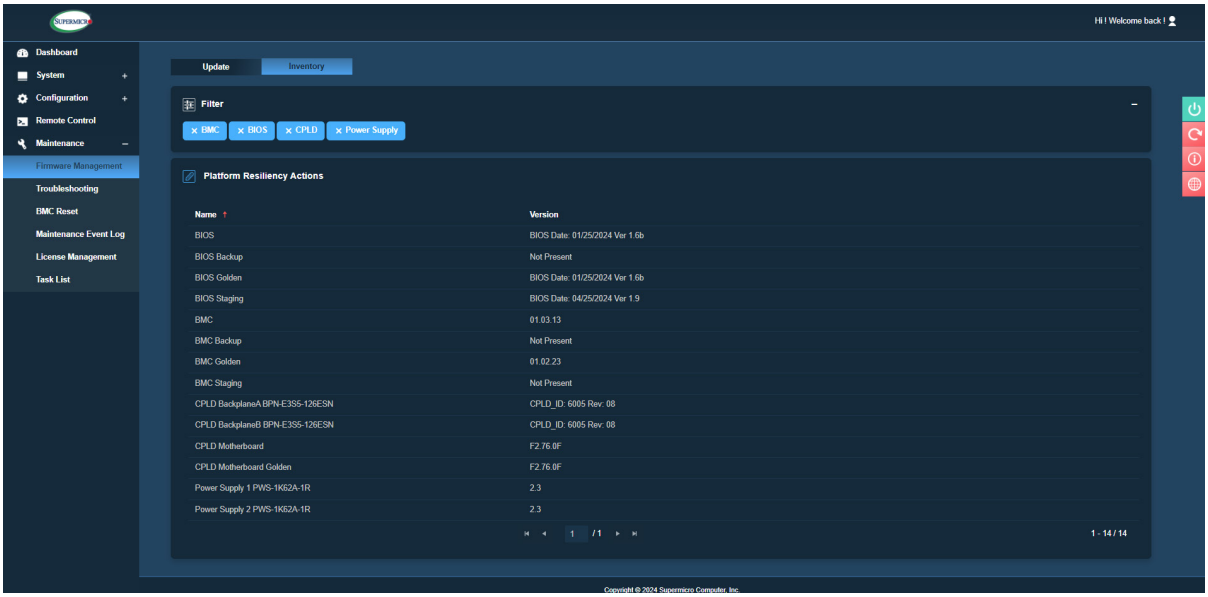


Figure 2-173: Inventory Page

You can see the following component firmware inventory based on supported components in the system:

Note: The backup fields only show when there are valid images.

- BMC
- BMC Backup
- BMC Golden
- BMC Staging
- BIOS
- BIOS Backup
- BIOS Golden
- BIOS Staging
- BIOS ME

- Broadcom
- 88NR2241
- PMem
- NIC AOC
- Capsule BIOS (X13/H13 and later motherboards)
- Capsule MCU (X13/H13 and later motherboards)
- Capsule ME (X13/H13 and later motherboards)
- CPLD Backplane (If there are multiple CPLD backplanes, append [num] at the end.)
- CPLD Motherboard
- CPLD Motherboard Golden (X13/H13 and later motherboards)
- Multi-node EC
- NIC AOC
- Power Supply (If there are multiple PSUs, append [num] at the end.)
- CPLD1 Backplane1
- PMem
- Storage AOC (Broadcom, Marvell)

Name	Version
====	=======
88NR2241 Device 0	1.0.0.9447
BIOS	BIOS Date: 09/13/2022 Ver 1.4
BIOS Backup	BIOS Date: 02/15/2022 Ver 1.2
BIOS Golden	BIOS Date: 06/09/2021 Ver 1.1
BIOS ME	4.4.4.202
BIOS Staging	BIOS Date: 09/13/2022 Ver 1.4
BMC	01.01.35
BMC Backup	Not Present
BMC Golden	09.01.99
BMC Staging	01.01.35
Capsule BIOS	1.00
Capsule MCU	1.00
Capsule ME	1.0.0.0
CPLD Motherboard	F1.00.D5
CPLD Motherboard Golden	F1.00.D5
Motherboard EC	01.C2.02
NIC1 System Slot5	
NIC2 System Slot0 AOC-2UR68G4-i4XTS	8.50 0x8000BE22
PowerSupply	1.4
PowerSupply2	1.4
SAS3808 Device 0	16.00.08.00
SAS3808IR Device 1	5.220.01-3691
SAS3916 Device 2	16.00.02.00
SAS3816IR Device 3	5.220.01-3691
SAS3916 Device 4	5.130.02-3170

Figure 2-174: Sample of Inventory Page

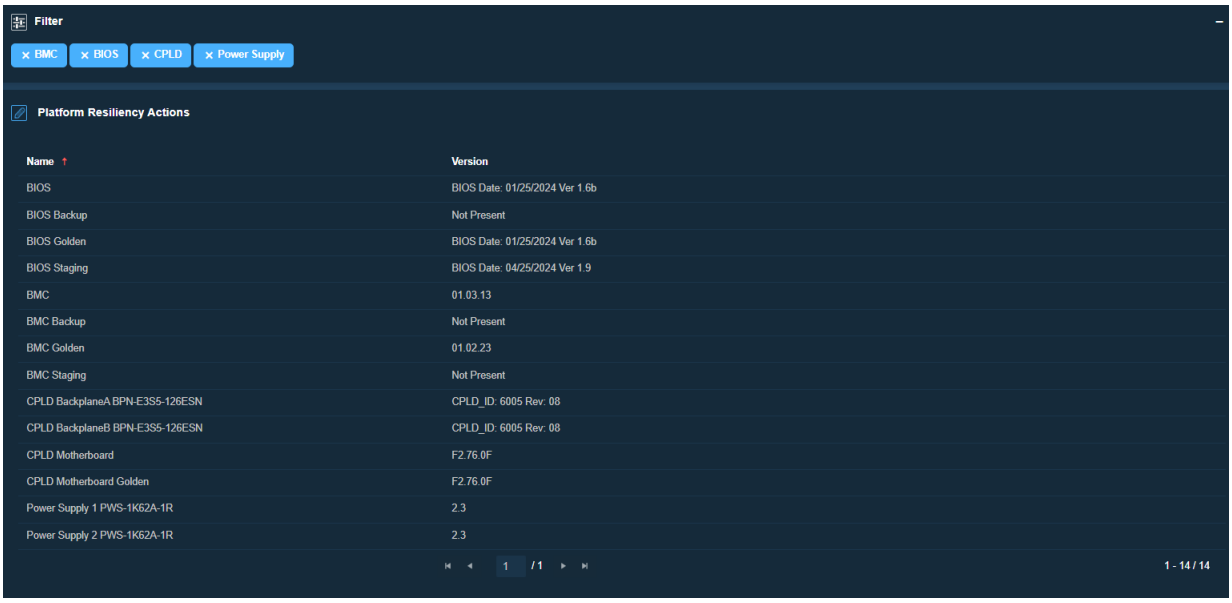


Figure 2-175: Inventory Page Sample

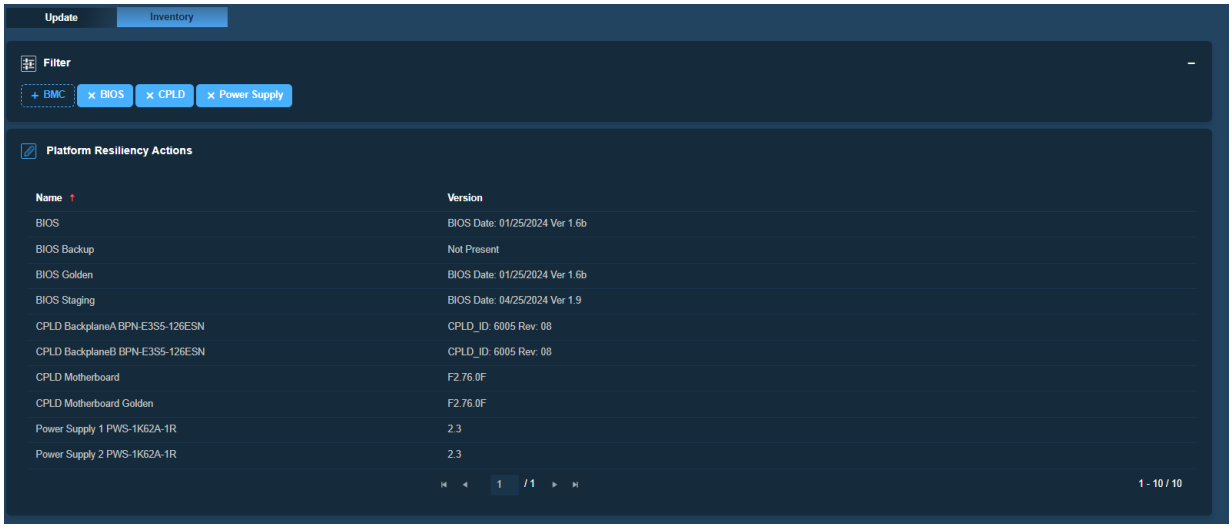


Figure 2-176: Inventory Page Sample

Platform Resiliency Actions

If you have administrator privileges, this page allows you to manage Platform Firmware Resiliency options. Only BMC and BIOS images are available in the Platform Resiliency Actions page. Click on the Editor button (✎) next to **Platform Resiliency Actions** to perform the following Platform Firmware Resiliency actions:

- Recover: If the administrator suspects that there are any issues with the current image or if the current image is compromised, then the administrator can manually recover BMC or BIOS from the backup image. You can select the current BMC/BIOS image and click on [Recover].

  Note: This action is supported under the SFT-DCMS-SINGLE license.

- Update: You can update the current active image as a golden template. If recommended by Supermicro or if the administrator prefers that the current image be used as a golden template, then use this option to update the golden image with the active image. You can select golden firmware options such as Golden BMC, Golden BIOS, or Golden CPLD Motherboard options and click on [Update].

  Note: When you upload the wrong firmware, a prompt will display to notify you with an explanation of the failure. A Maintenance Event Log will also be sent to the MEL page for records.

- Generate Evidence: When BMC or BIOS is recovered manually or automatically from the last known good image or golden image, the active image will be stored in the evidence region, where you can download evidence. If evidence is available, the Generate Evidence button will be enabled. Generate Evidence options create a compressed file for the evidence image. You can track the progress in the task list.

  Note 1: If one of the BMC or BIOS evidence is in the process of being generated, you cannot generate other evidence or update other firmware.

  Note 2: A BMC or BIOS firmware update will delete the evidence from the evidence region. Make sure to download evidence before initiating a firmware update.

- Download Evidence: Once a compressed evidence file is generated, the Download Evidence button will be enabled. Click to download the evidence.

  Note: Compressed evidence fill will be deleted during the BMC reset operation. You can regenerate the compressed evidence file if needed.

When one of the action buttons is selected on the inventory page, unavailable or non-applicable action buttons (e.g., Generate Evidence, Download Evidence, Recover, and Update buttons) are to be grayed out.

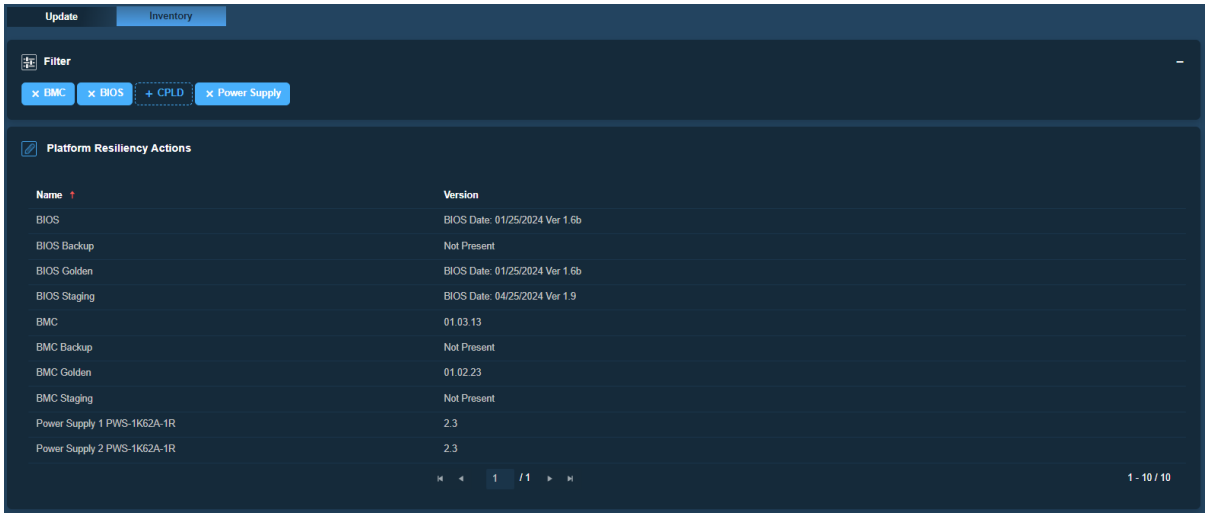


Figure 2-177: Sample of Inventory Platform Resiliency Actions Page

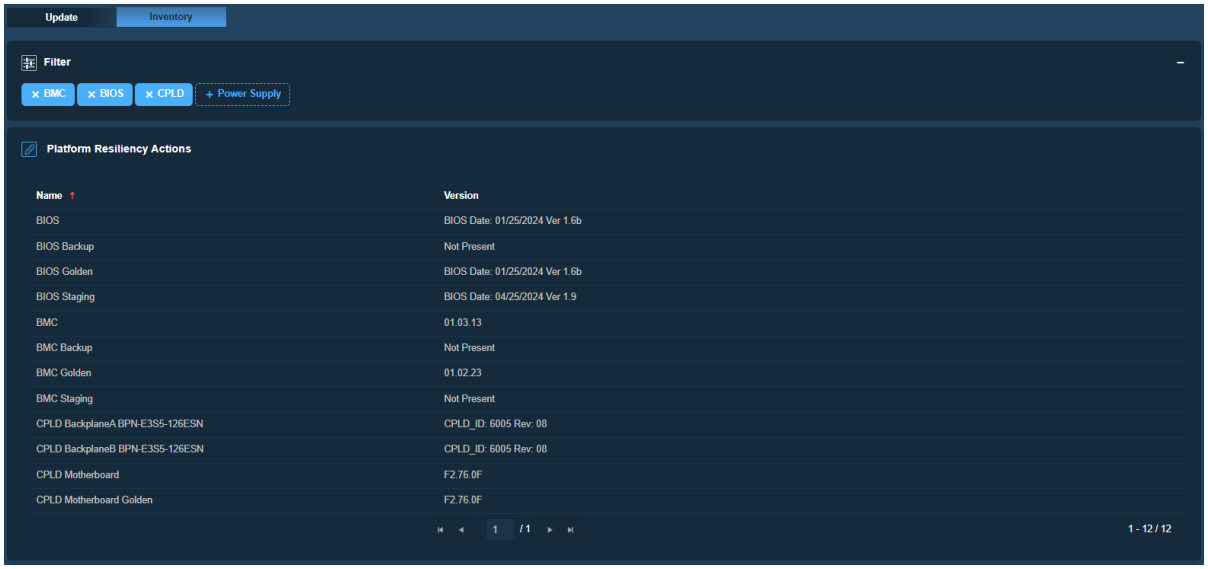


Figure 2-178: Sample of Inventory Platform Resiliency Actions Page

Note: Starting from X14 or H14, staging areas will be cleaned out after firmware updates. Hence, the Staging areas will be “Not Present” after BMC, BIOS, or other firmware update processes are completed. If you enter the wrong file type or a bad image for the new firmware, a prompt message *“Please upload a valid file!”* will appear, prompting you to re-enter a valid file.

2.8.2. Troubleshooting

System Crash Dump

This feature allows you to dump and download CPU register information for debugging purposes.

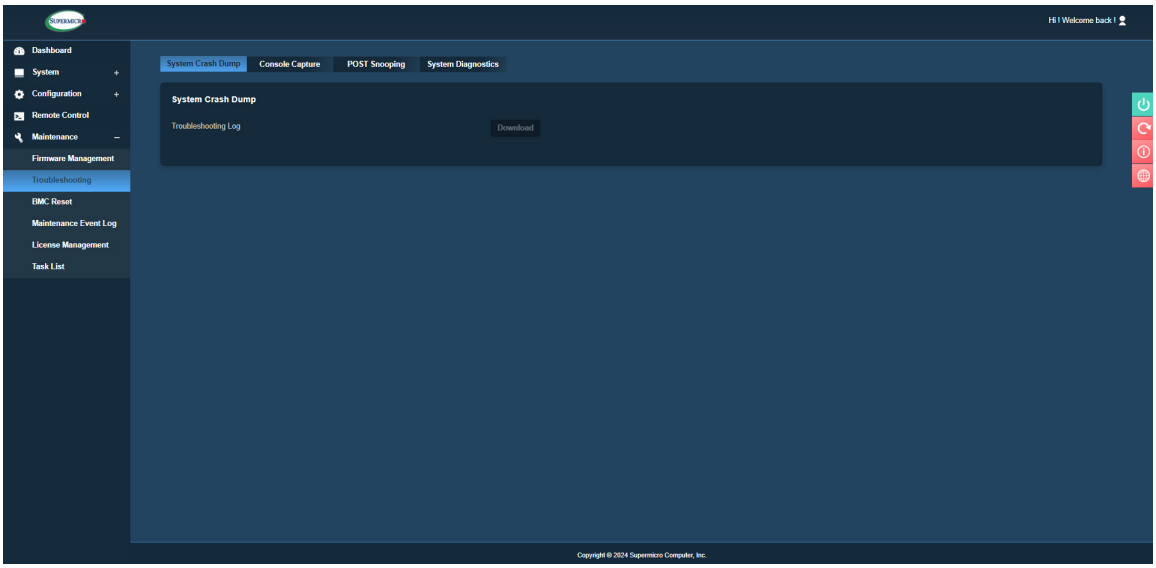


Figure 2-179: System Crash Dump Page

You can adjust the following options:

- Auto reset system after CPU CATERR/IERR interrupt happens: The check box allows you to select the reset option after CPU CATERR/IERR interruption happens. If checked (ON), the system will restart automatically. If not, the system will remain in a failed state.
- Generate: Use this to generate a new crash dump.

  Note: Upon clicking [Generate], the system will remove previous error logs or dump available files and regenerate a new dump file.

- Download: Use this to download the current crash dump file.

Console Capture

This page displays Crash Capture for Screenshot and Video for Console with the running Operating System.

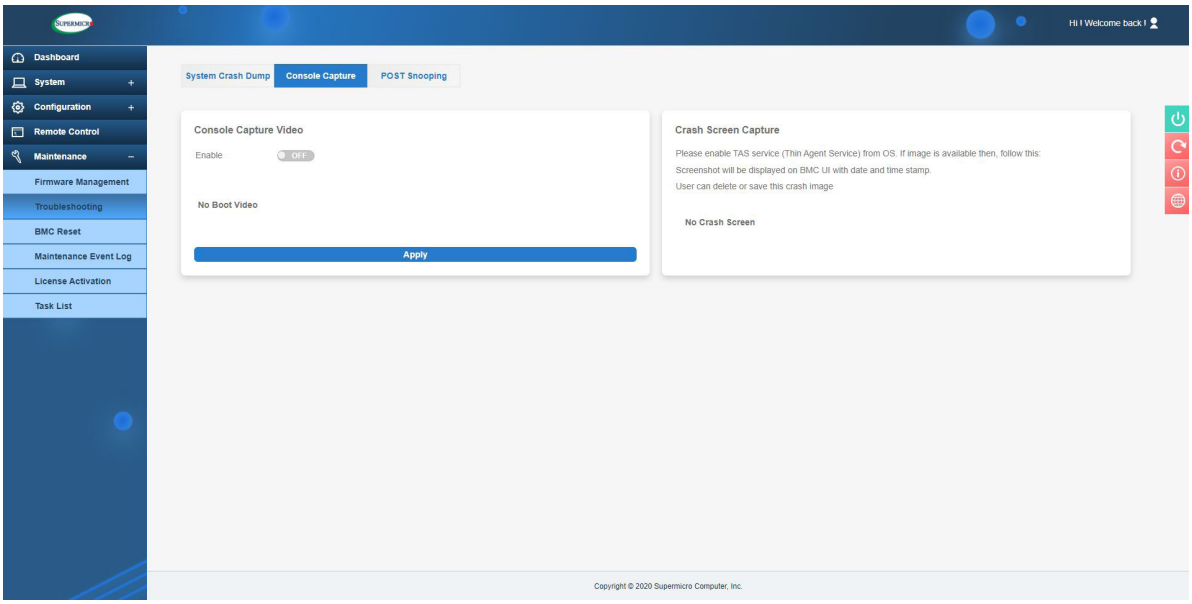


Figure 2-180: Console Capture Page

Console Capture

This page displays Crash Capture for Screenshot and Video for Console while running the operating system.

Console Capture Video

The Console Capture Video function allows you to record video of the console while the system is running the OS. You can use the following options to configure the function settings:

- Disable/Enable: You can enable or disable this function. By default, it will be disabled.
- Record until buffer is full: You can record video of the console until the buffer is full. Video will be saved as AVI format, and the maximum buffer size is 7 to 8 MB (approximately four minutes; time calculated based on video size).
- Record until POST ends: You can record video until POST ends or record until the timeout value (approximately four minutes). BMC will receive POST completion information from BIOS and record video until that time. If any delay is introduced, then BMC will record video until the timeout period of approximately four minutes.

- Apply: You can record all videos with the title and time stamp. It will also allow you to delete a specific video.
- Download: You can play and download videos from here.
- AC Cycle/Factory Reset: Upon reset, all videos will be deleted.

Crash Screen Capture

The Crash Screen Capture feature allows you to capture the crash screen. You have to enable Thin Agent Service (TAS) from the OS. Once TAS is enabled and running in the OS, BMC will capture the last crash screen. Screenshot will be displayed on BMC UI with the date and time stamp. Then you can delete or save the crash image.

Note 1: The table shows the supported and unsupported server platforms (non-workstations) for System Crash Dump, Console Capture Video, and Crash Screen Capture features. We will enable the functions when they are supported. Due to time constraints, Console Capture Video and Crash Screen Capture on Intel Platforms with AST2500 are not supported at this time. All workstations and Atom-based motherboard platforms are not supported.

Note 2: This feature is available only for select platforms.

POST Snooping

This page displays the current BIOS POST codes. Refresh the page to query the POST snooping code for BIOS LPC port 80.

BMC Self-Test

This page allows you to conduct a BMC Self-Test.

System Diagnostics

This page provides you with the ability to perform system diagnostics through BMC Web UI. To navigate to the System Diagnostics page, take the following steps:

1. Navigate to the Maintenance page.
2. Navigate to the Troubleshooting page.
3. Select System Diagnostics.
4. Select Diagnostics to initiate.
5. Before execution, a prompt appears with the message: *"To begin System Diagnostic, a system reboot is required. Do you wish to proceed with the reboot?"* Select 'Proceed' to perform system diagnostics.
6. If you do not want to perform system diagnostics, select 'Cancel.'

When you click ‘Proceed,’ the system diagnostics process will begin. The system will reboot to perform the diagnostics automatically. After the diagnostics are completed, the system reboots again to boot into the default boot option as configured in the BIOS settings. During this process, the BMC Web UI displays the message: *"System diagnostics in progress, please wait."*

The test report is also uploaded to BMC in a compressed format. The ‘Download’ button in the BMC Web UI will also become available (changing from a grayed-out state) if there is a report. If no report is saved in BMC, the download button will remain grayed out. You can then click the ‘Download’ button to download the test report from the previous system diagnostics action. If you initiate System Diagnostics again, the saved test report will be cleared from BMC, and the ‘Download’ button will become grayed out until the diagnostics are completed and a new report is saved in BMC for download. The test report from the last diagnostics is saved in BMC, allowing you to download it even if the AC power is off and BMC is re-initialized.

You can also access the Maintenance Event Log through the Maintenance page to view logs for events such as "System Diagnostics started" and "System Diagnostics report download success." This provides a comprehensive log of the system diagnostic events for you to review.

Note 1: This feature is only available for server-grade (Xeon Scalable and EPYC) platforms of BIOS on X13 and later generation platforms.

Note 2: This feature is only available for select server-grade products.

CPER

This feature allows you to view all the event logs for CPU, Memory, PCIe, and Firmware errors. You can also use this to export the logs to an Excel file for record purposes.

2.8.3. BMC Reset

Factory Default

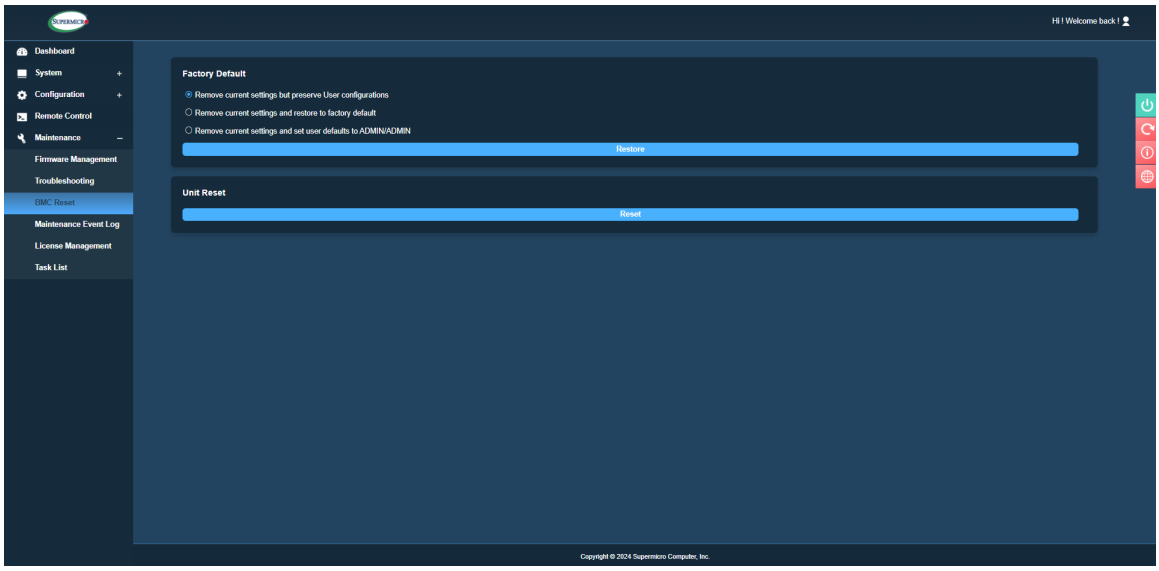


Figure 2-181: BMC Reset Page

You can select the following options to restore BMC to the factory default settings. This feature includes the following options:

- Remove current settings but preserve user configurations: You can restore all configurations to factory default and preserve all user configurations.
- Remove current settings and restore to factory default: You can restore all the configuration to factory default. This option will remove all users and reset the ADMIN user password to the factory default password.

- Remove current settings and set user defaults to ADMIN/ADMIN: You can restore all the configuration to factory default. This option will remove all users and reset ADMIN user password to ADMIN.

Note: There will be a prompt saying *"BMC is resetting to default. To prevent data loss, please do NOT remove power source until BMC is back online!"*

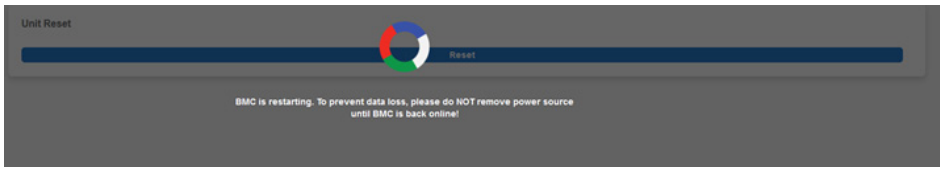


Figure 2-182: BMC Restart Loading

Unit Reset

This feature allows you to reset an IPMI device.

Note: You will get a prompt that says, *"BMC is restarting. To prevent data loss, do NOT remove power source until BMC is back online!"*

2.8.4. Maintenance Event Log

This page displays the record of maintenance events, such as administrative events.

Note: By default, all event categories are selected so you can view all events. You can apply event category filters to view respective events (e.g., Storage, Account, Network, Service, or others).

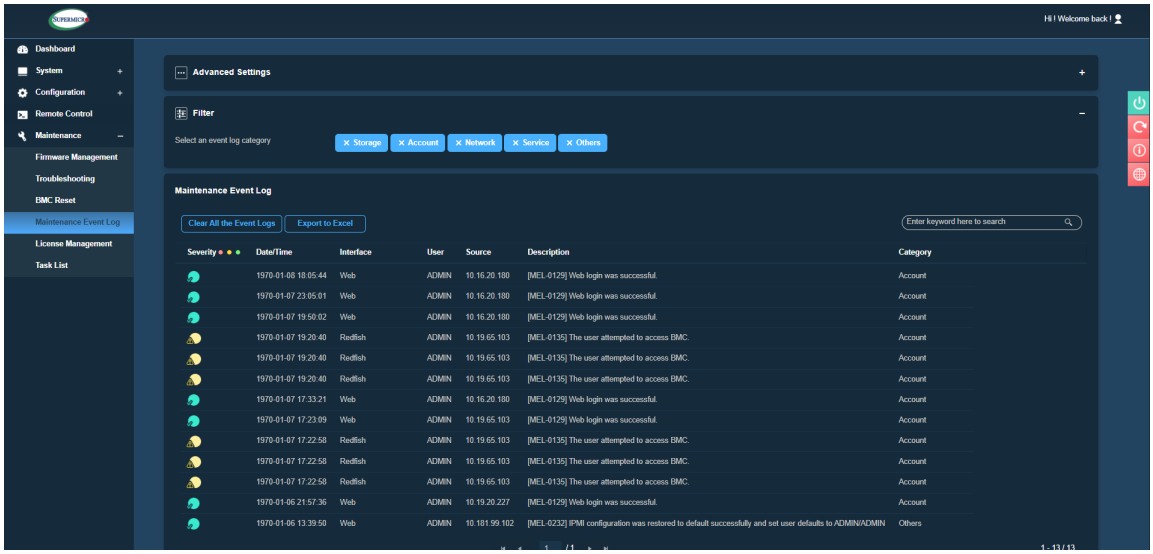


Figure 2-183: Maintenance Event Log Page

The Maintenance Event Log table displays the following details about each log entry:

- Severity: You can view the severity of the events with one of the following states.

  Informational event

  Warning event which needs attention

  Critical event which needs immediate action to prevent possible failure

- Date/Time: You can view the time stamp of the event occurrence.
- Interface: You can view the interface that triggered the event (e.g., RMCP, Redfish, Web).
- User: You can view the name of the user that triggered the event (e.g., ADMIN, N/A, BIOS).
- Source: You can view the source that triggered the event (e.g., N/A, IPv4 Address, IPv6 Address, etc.).

- Description: You can view the basic description of the event (e.g., Web login was successful, etc.).
- Category: You can view the event category based on the type of event (e.g., Storage, Account, Network, Service, or others).
- Keyword Search: You can search for keyword-related events.

Administrators can perform one of the following operations for the event logs:

- Enable/Disable Maintenance Event Log: You can enable or disable maintenance event logs. This option is available under Advanced settings.
- Clear: You can select the respective event and click [Clear] to remove the maintenance event log entry. To "Clear All the Event Logs," you must enable Maintenance Event Log in Advanced Settings.
- Export to Excel: You can export the current maintenance event log to an Excel file.

2.8.5. License Management

Use this page to view and configure software license activation for BMC through the License Activation tab. The licenses supported for BMC include SFT-OOB-LIC or SFT-DCMS-SINGLE. Under the CPU tab, you can access information about Intel Capability Activation Payload (CAP) for Intel CPUs.

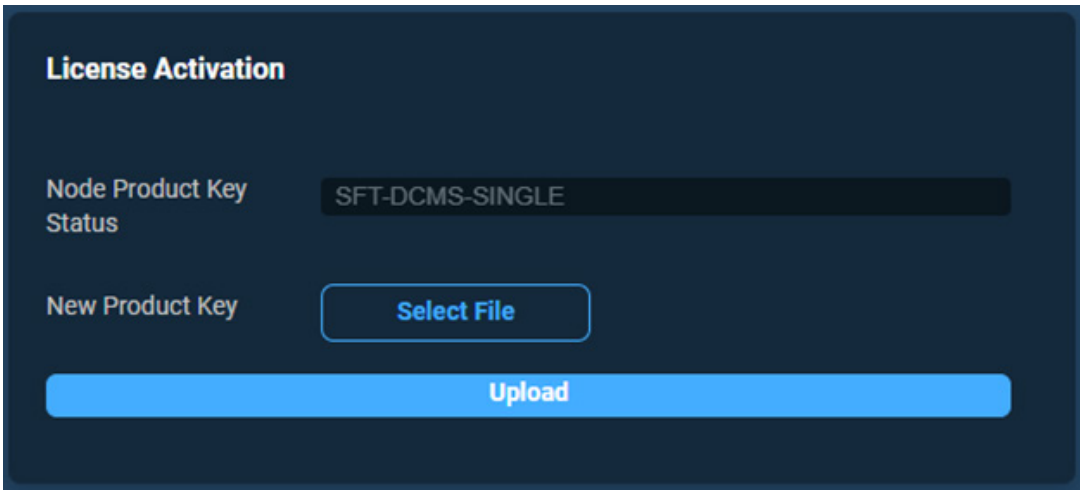


Figure 2-184: License Management Section

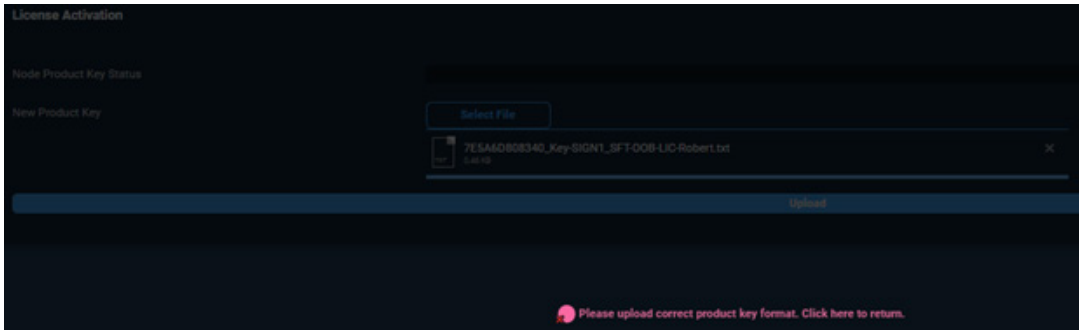


Figure 2-185: Inorrect Product Key Format Error Message

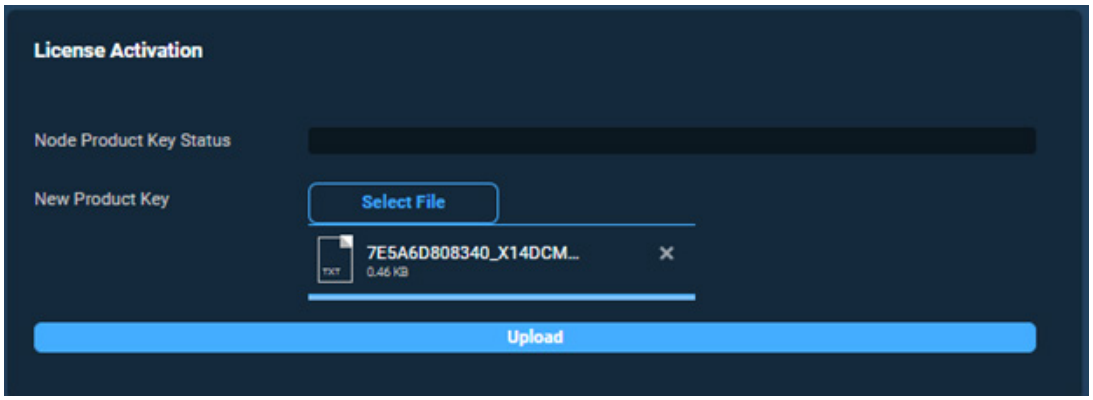


Figure 2-186: License Management Product Key File Selected

You can adjust the following settings to configure this feature:

- Node Product Key Status: You can view the currently activated license type.
- Activate License: You can upload a new license file and activate it to enable comprehensive end-to-end systems management functions.

You can easily determine whether the SFT-OOB-LIC or SFT-DCMS-SINGLE license has been activated for BMC features. If a specific software license, such as SFT-OOB-LIC, is required, relevant notifications will appear in pop-up messages. For instance, *"This function requires an SFT-OOB-LIC license. Would you like to activate it now?"*

In the event of users uploading an invalid product key format, a prompt message will appear stating, *"Please upload the correct product key format. Click here to return."* Importantly, no MEL log will be generated in this instance.

If you upload a product key with a valid format but an invalid license, a prompt message will appear stating, *"Product key is invalid. Click here to return."* Additionally, a log will be generated.

2.8.6. Task List

The Task List provides the task status for different management operations running on this device.

Note: The BMC supports BMC and BIOS FW updates along with storage controller drives, which can erase task progress.

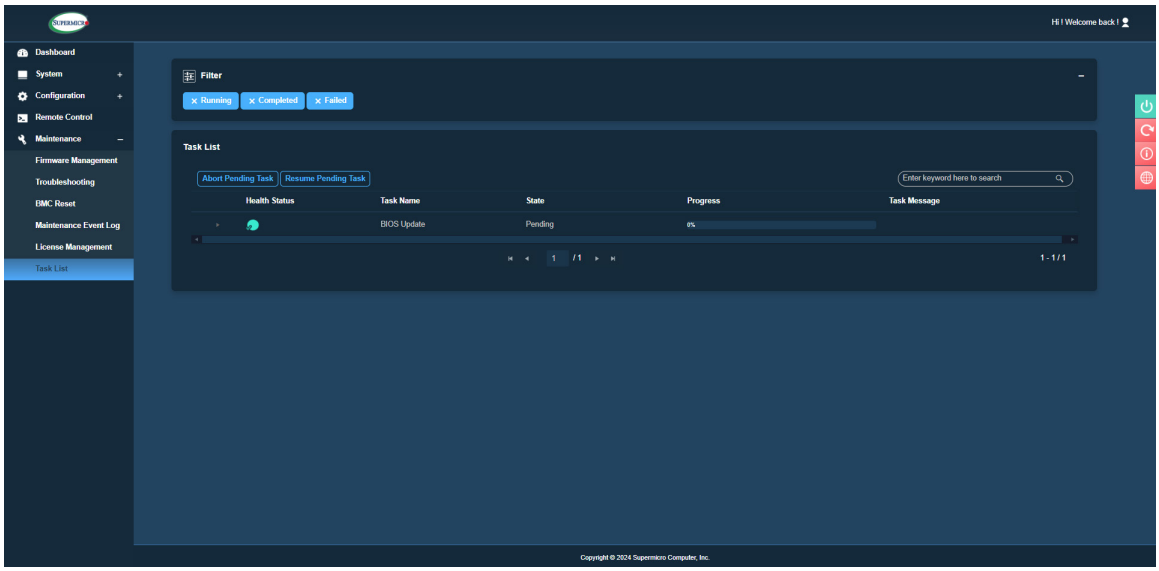


Figure 2-187: Task List Page

You can search the state (Running/Completed/Failed) of the following tasks:

- Health Status: You can view the status of current tasks.
- Job: You can view the lists of current job types.
- State: You can view current state values (Running, Completed, or Failed).
- Create Time: You can view the timestamp for when the task began.
- Progress: You can view the progress of current running task(s).
- Total Duration: You can view the total time taken to finish current task(s).
- Completed Time: You can view the task completion time stamp.

You can use the filter to show interested tasks based on three criteria: Running, Completed, and Failed. The following table shows the corresponding Redfish state to filter criteria.

UI Task Filter	*Task List State*
Running	New
	Starting
	Running
	Suspended
	Interrupted
	Pending
	Stopping
	Service
	Cancelling
Completed	Completed
	Killed
	Cancelled
Failed	Exception

Chapter 3

Frequently Asked Questions

Question: How do I flash the BMC firmware?

Answer:

1. Click the <Maintenance> button. Browse the files available and select the correct file to flash the firmware.
2. Click the <Update Firmware> button to proceed with firmware flashing.

Question: If I am using a firewall for my network connections, which ports should I open so that I can access my BMC connection?

Answer: In order to access your BMC connection behind a firewall, open the following ports:

HTTP: 80 (TCP)

HTTPS: 443 (TCP)

BMC: 623 (UDP)

Remote console: 5900 (TCP)

Virtual media: 623 (TCP)

SMASH: 22 (TCP)

WS-MAN: 8889 (TCP)

Question: When I update the BMC firmware through the web, why do I get a file download pop-up even though the firmware was not updated?

Answer: This may be caused by your anti-virus software. Disable your antivirus software temporarily and update your firmware.

Question: My system seems to function properly. Why does the BMC event log indicate that my voltage and temperatures are beyond the limits?

Answer: It is not a normal condition. Make sure that there is no other device accessing the I^2C bus. If another device accesses the I^2C bus frequently, it might cause a collision with the BMC when this device accesses the I^2C bus. When you see this error, uninstall lm_sensors in Linux.

Chapter 4

UEFI BIOS

4.1 Introduction

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

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

Updating BIOS

It is recommended that you do not upgrade your BIOS if you are not experiencing any problems with your system. Updated BIOS files are located on our website at https://www.supermicro.com/support/resources/bios_ ipmi.php. Check our BIOS warning message and the information on how to update your BIOS on our website. Select your motherboard model and download the BIOS file to your computer. Also, check the current BIOS revision to make sure that it is newer than your current BIOS before downloading.

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

Note: Do not shut down or reset the system while updating the BIOS to prevent possible system boot failure! Read the X14 README file carefully before you perform the BIOS update.

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 accompanies 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 option 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>, <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 at the top of the screen. The Main BIOS setup screen and the following features will be displayed:

Figure 4-1: Main Page

System Date/System Time

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

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

Supermicro Motherboard Name

BIOS Version

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

Build Date

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

CPLD Version

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

Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

Use the arrow keys to select the Advanced menu and press <Enter> to access the submenu features:

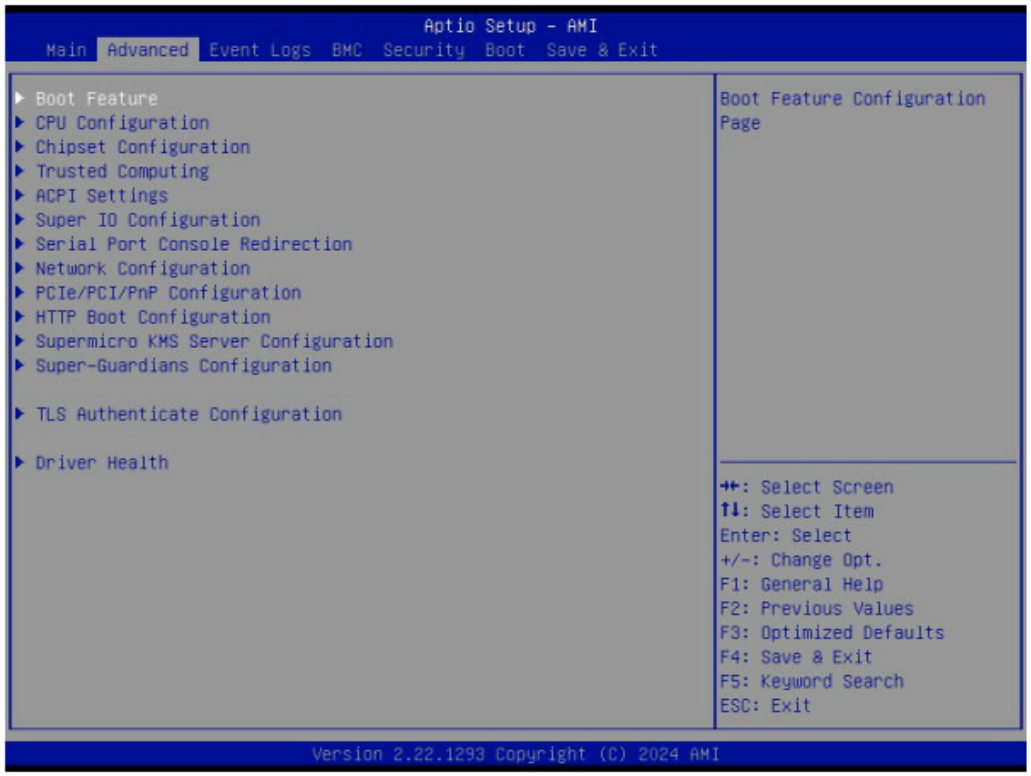


Figure 4-2: Advanced Page

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

Boot Feature Menu

▶Boot Feature

Quiet Boot

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

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

Bootup NumLock State

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

Wait For "F1" If Error

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

Power Configuration

Watch Dog Function

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

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

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

Restore on AC Power Loss

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

Power Button Function

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

CPU Configuration Menu

▶CPU Configuration

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

The following CPU information will display:

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

Hyper-Threading [ALL]

Select Enabled to use Intel Hyper-Threading Technology to enhance CPU performance. The options are Disabled and **Enabled.** This feature is CPU-dependent.

Hardware Prefetcher

If this feature is set to Enabled, the hardware prefetcher will prefetch data from the main system memory to the Level 2 cache to help expedite data transactions to enhance memory performance. The options are **Enabled** and Disabled.

Adjacent Cache Prefetch

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

DCU Streamer Prefetcher

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

DCU IP Prefetcher

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

LLC Prefetch

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

Homeless Prefetch

Select Enabled for Homeless Prefetch support on all threads, which is an Effective Prefetch Strategy (EPS) used to enhance memory performance by reducing communication overhead, network latency, and the wait time needed for barrier synchronization in memory prefetching commonly associated with the home-based software Distributed Shared Memory (DSM) system. The options are Disabled, Enabled, and **Auto**. Note that the option of Auto is program-specific. This feature is CPU-dependent.

AMP Prefetch

Select Enabled to use a machine learning algorithm to predict the best L2 prefetcher configuration for the currently running workload. This feature can improve the performance of various general-purpose workloads. The options are Disabled and **Enabled**. This feature is CPU-dependent.

APIC Physical Mode

This feature allows you to enable/disable the APIC physical destination mode. The options are **Disabled** and Enabled. APIC is the abbreviation for Extended Advanced Programmable Interrupt Controller.

TXT Support

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

Note:

- If this feature is set to Enabled, be sure to disable Device Function On-Hide (EV DFX) support when it is present in the BIOS for the system to work properly.
- For more information on TPM, refer to the TPM manual at https://www.supermicro.com/manuals/other/AOM-TPM-9670V_9670H.pdf.

Intel Virtualization Technology (Unavailable when "TXT Support" is set to Enabled)

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

Note: Reboot the system for any changes to the setting to take effect.

Enable SMX (Available when "TXT Support" is set to Disabled)

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

PPIN Control

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

AES-NI

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

Advanced Power Management Configuration Menu

▶Advanced Power Management Configuration

Power Technology

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

ENERGY_PERF_BIAS_CFG Mode (ENERGY PERFORMANCE BIAS CONFIGURATION Mode) (Available when "Power Performance Tuning" is set to BIOS Controls EPB)

Use this feature to configure the proper operation settings for your machine by achieving the desired system performance level and energy saving (efficiency) level at the same time. Select Performance to enhance system performance; however, this may consume more power as energy is needed to fuel the processors for operation. The options are Performance, **Balanced Performance**, Balanced Power, and Power.

CPU P State Control Menu

▶CPU P State Control

AVX P1 (Available when "SpeedStep (P-States)" is set to Enabled)

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

The following information is CPU-dependent and will be displayed when "SpeedStep (PStates)" is set to Enabled:

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

- Package TDP (W)
- DTS_Max

SpeedStep (P-States)

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

EIST PSD Function

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

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

Select Enable to allow the CPU to operate at the manufacturer-defined turbo speed by increasing the CPU clock frequency. This feature is available when it is supported by the processors used in the system. The options are Disabled and Enabled.

Hardware PM State Control Menu

▶Hardware PM State Control

Hardware P-States

If this feature is set to Disabled, the system hardware will choose a P-state setting for the system based on an OS request. If this feature is set to Native Mode, the hardware will choose a P-state setting based on the OS guidance. If this feature is set to Native Mode with No Legacy Support, the system hardware will choose a P-state setting independently without OS guidance. The options are Disabled, **Native Mode**, Out of Band Mode, and Native Mode with No Legacy Support.

CPU C State Control Menu

▶CPU C State Control

Monitor MWAIT

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

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

C1 to C1e Promotion

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

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

ACPI C1 Enumeration

Use this feature to select the ACPI C1 state or the ACPI C1e state. The options are C1 and **C1e**. This feature is CPU-dependent. (ACPI is the abbreviation for Advanced Configuration and Power Interface.)

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

ACPI C6x Enumeration

Use this feature to configure C6 state or C6 P-state as ACPI C2 or ACPI C3 state. The options are Disabled, C6S as ACPI C2, C6S as ACPI C3, C6S-P as ACPI C2, C6S-P as ACPI C3, and **Auto**.

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

Package C State Control Menu

▶Package C State Control

Package C State

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

LTR IIO Input

Use this feature to set the MSR 1FCh Bit[35]. The options are Take IIO LTR input and **Ignore IIO LTR input**.

CPU1/CPU2 Core Disable Bitmap Menu

▶CPU1/CPU2 Core Disable Bitmap

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

Available Bitmap[0]:

This feature displays the available Bitmap[0].

Available Bitmap[1]:

This feature displays the available Bitmap[1]. It is available when the number of CPU cores is greater than 128.

Disable Bitmap[0]

Enter 0 to enable this feature for CPU Core Bitmap[0]. Enter FFFFFFFFFF to disable CPU Core Bitmap[0]. Note that the maximum CPU cores is available in each CPU package, and at least one core per CPU must be enabled. Disabling all cores is not allowed. The default setting is **0**.

Disable Bitmap[1]

Enter 0 to enable this feature for CPU Core Bitmap[1]. Enter FFFFFFFFFF to disable CPU Core Bitmap[1]. Note that the maximum CPU cores is available in each CPU package, and at least one core per CPU must be enabled. Disabling all cores is not allowed. The default setting is **0**. This feature is available when the number of CPU cores is greater than 128.

CPU Configuration Menu

▶Chipset Configuration

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

Uncore Configuration Menu

▶Uncore Configuration

The following information is displayed.

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

Degrade Precedence

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

Link L0p Enable

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

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

Link L1 Enable

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

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

KTI Prefetch

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

IO Directory Cache (IODC)

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

SNC

Sub NUMA Clustering (SNC) is a feature that breaks up the Last Level Cache (LLC) into clusters based on address range. Each cluster is connected to a subset of the memory controller. Enable this feature to improve average latency and reduce memory access congestion for higher performance. The options are Disabled, Enabled, and **Auto**. This feature is CPU-dependent.

XPT Prefetch

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

Stale AtoS

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

LLC Dead Line Alloc

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

Memory Configuration Menu

▶Memory Configuration

This submenu allows you to configure the Integrated Memory Controller (iMC) settings.

Enforce DDR Memory Frequency POR

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

Host Memory Frequency

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

Global Scrambling

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

Memory Configuration Menu

▶Memory Topology

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

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

Memory Map Menu

▶Memory Map

Intel(R) Flat Memory Mode Support

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

DDR CXL Heterogeneous Interleave Support

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

Memory RAS Configuration Menu

▶Memory RAS Configuration

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

Mirror Mode

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

UEFI ARM Mirror

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

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

Mirror TAD0

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

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

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

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

Correctable Error Threshold

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

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

Leaky Bucket Low Bit

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

Leaky Bucket High Bit

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

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

Select Enabled for Adaptive Double Device Data Correction (ADDDC) support, which will not only provide memory error checking and correction but will also prevent the system from issuing a performance penalty before a device fails. Note that virtual lock-step mode will only start to work for ADDDC after a faulty DRAM module is spared. The options are Disabled and **Enabled**.

DDR PPR Type

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

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

Enhanced PPR

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

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

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

Security Configuration Menu

▶Security Configuration

Memory Encryption (TME) [Outputs]

The following information is displayed.

- MSE activation state
- MK-TME activation state

- CI activation state
- Cryptographic Algorithm configured

Memory Encryption (TME) [Outputs]

Memory Encryption (TME)

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

Total Memory Encryption Multi-Tenant (TME-MT)

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

Memory Integrity

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

The following information is displayed.

- KEY stock amount
- TME-MT key ID bits

TME Encryption Algorithm

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

Trust Domain Extension (TDX) [Outputs]

The following information is displayed.

- TDX activation state

Trust Domain Extension (TDX) [Inputs]

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

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

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

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

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

▶TDX Physical PCIe Configuration (Available when "Trust Domain Extension (TDX)" is set to Enabled)

The following information is displayed.

- Available port bitmap [HEX]
- Disable port bitmap [HEX]

Processor Reserved Memory [Capabilities]

The following information is displayed.

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

Processor Reserved Memory [Outputs]

The following information is displayed.

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

Software Guard Extension (SGX) [Outputs]

The following information is displayed when your motherboard supports SGX.

- SGX activation state
- SGX error code [HEX]

Software Guard Extension (SGX) [Inputs]

The following features are available when your motherboard supports SGX.

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

SGX Factory Reset

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

SW Guard Extensions (SGX)

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

SGX Package Info In-Band Access

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

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

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

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

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

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

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

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

Software Guard Extensions Epoch 0

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

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

Software Guard Extensions Epoch 1

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

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

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

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

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

Use this feature to enter the bytes 0 to 7 of SGX Launch Enclave Public Key Hash. The default setting is **0**.

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

Use this feature to enter the bytes 16 to 23 of SGX Launch Enclave Public Key Hash. The default setting is **0**.

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

Use this feature to enter the bytes 24 to 31 of SGX Launch Enclave Public Key Hash. The default setting is **0**.

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

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

IIO Configuration Menu

▶IIO Configuration

PCIe ASPM Support (Global)

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

CPU1/CPU2 Configuration Menu

▶CPU1/CPU2 Configuration

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

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

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

Bifurcation

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

▶Intel VMD Technology

Note: After you've enabled VMD in the BIOS on a PCIe slot, this PCIe slot will be dedicated for VMD use only, and it will no longer support any PCIe device. To reactivate this slot for PCIe use, disable VMD in the BIOS.

Intel VMD Technology

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

▶PCI Express 5 Port A/Port C/Port E/Port G

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

Requested Link Speed

Use this feature to configure the link speed for the PCIe port you specified. The options are **Auto**, Gen 1 (2.5 GT/s), Gen 2 (5 GT/s), Gen 3 (8 GT/s), Gen 4 (16 GT/s), and Gen 5 (32 GT/s).

The following information is displayed:

- Max Link Width
- Current Link Width
- Current Link Speed

PCIe Port Max Payload Size

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

MCTP

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

Intel VMD Technology

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

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

▶Intel VT for Directed I/O (VT-d)

Pre-boot DMA Protection

Select Enabled to establish DMA protection during pre-boot processing by setting DMA_CTRL_PLATFORM_OPT_IN_FLAG in the DMAR ACPI table. The options are **Enabled** and Disabled. (DMA is the abbreviation for Direct Memory Access. DMAR is the abbreviation for DMA Remapping Reporting.)

PCIe ACSCTL

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

PCIe Leaky Bucket Configuration Menu

▶PCIe Leaky Bucket Configuration

Gen2 Link Degradation

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

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

Gen3 Link Degradation

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

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

Gen4 Link Degradation

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

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

Gen5 Link Degradation

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

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

Trusted Computing Menu

▶Trusted Computing

Note: This submenu is available when a TPM device is installed and detected by the BIOS.

When a Trusted Platform Module (TPM) device is detected by your system, the following information is displayed.

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

Security Device Support

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

When "Security Device Support" is set to Enabled and a TPM 2.0 device is detected by the BIOS, the following information is displayed.

- Active PCR Bank
- Available PCR banks
- SHA256 PCR Bank

The following features are available when a TPM 2.0 device is detected by the BIOS.

ACPI Settings Menu

▶ACPI Settings

NUMA

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

Virtual NUMA

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

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

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

WHEA Support

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

Super IO Configuration Menu

▶Super IO Configuration

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

The following information is displayed.

- Super IO Chip

Serial Port 1 Configuration Menu

▶Serial Port 1 Configuration

Serial Port 1

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

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

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

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

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

Serial Port 2 Configuration Menu

▶Serial Port 2 Configuration

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

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

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

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

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

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

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

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

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

Serial Port Console Redirection Menu

▶Serial Port Console Redirection

COM1 (Available when your system supports the serial port of COM1)

Console Redirection

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

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

▶Console Redirection Settings

Note: This submenu is available when "Console Redirection" for COM1 or SOL/COM2 is set to Enabled.

Terminal Type

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF-8 encoding to map Unicode characters into one or more bytes. The options are VT100, **VT100+**, VT-UTF8, and ANSI.

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

SOL/COM2

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

Console Redirection

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

▶Console Redirection Settings

Note: This submenu is available when "Console Redirection" for COM1 or SOL/COM2 is set to Enabled.

Terminal Type

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII Character set. Select VT100+ to add color and function key support. Select ANSI to use the Extended ASCII Character Set. Select VT-UTF8 to use UTF-8 encoding to map Unicode characters into one or more bytes. The options are VT100, **VT100+**, VT-UTF8, and ANSI.

Bits Per Second

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

Data Bits

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

Parity

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

Stop Bits

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

Flow Control

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

VT-UTF8 Combo Key Support

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

Recorder Mode

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

Resolution 100x31

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

Putty KeyPad

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

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

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

Console Redirection EMS

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

▶Console Redirection Settings

Note: This submenu is available when "Console Redirection EMS" is set to Enabled.

Out-of-Band Mgmt Port

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

Terminal Type EMS

Use this feature to select the target terminal emulation type for Console Redirection. Select VT100 to use the ASCII character set. Select VT100+ to add color and function key support. Select ANSI to use the extended ASCII character set. Select VT-UTF8 to use UTF-8 encoding to map Unicode characters into one or more bytes. The options are VT100, VT100+, **VT-UTF8**, and ANSI.

Bits Per Second EMS

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

Flow Control EMS

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

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

Network Stack Configuration Menu

▶Network Stack Configuration

Network Stack

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

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

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

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

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

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

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

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

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

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

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

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

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

MAC:(MAC address)-IPv4 Network Configuration Menu

▶MAC:(MAC address)-IPv4 Network Configuration

Configured

Enable this feature to configure network addresses for DHCP, local IP address, local netmask, local gateway, and local DNS server. The options are **Disabled** and Enabled.

Enable DHCP (Available when "Configured" is set to Enabled)

Select Enabled to support Dynamic Host Configuration Protocol (DHCP), which allows the BIOS to search for a DHCP server attached to the network and request the next available IP address for this computer. The options are **Disabled** and Enabled.

Local IP Address (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to enter an IP address for the local machine.

Local NetMask (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to set the netmask for the local machine.

Local Gateway (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

Use this feature to set the gateway address for the local machine.

Local DNS Servers (Available when "Configured" is set to Enabled and "Enabled DHCP" is set to Disabled)

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

Save Changes and Exit

Press <Enter> to save changes and exit

MAC:(MAC address)-IPv6 Network Configuration Menu

▶MAC:(MAC address)-IPv6 Network Configuration

▶Enter Configuration Menu

The following information is displayed.

- Interface Name
- Interface Type
- MAC address
- Host address
- Route Table
- Gateway addresses
- DNS addresses

Interface ID

Use this feature to change/enter the 64-bit alternative interface ID for the device. The string format is colon-separated. The default setting is the MAC address above.

DAD Transmit Count

Use this feature to set the number of consecutive neighbor solicitation messages that have been sent while performing duplicate address detection on a tentative address. The default setting is **1**.

Policy

Use this feature to select how the policy is to be configured. The options are **automatic** and manual.

▶Advanced Configuration

Note: This submenu is available when "Policy" is set to manual.

New IPv6 Address

Use this feature to enter the IPv6 address for the local machine.

New Gateway Addresses

Use this feature to set the gateway address for the local machine.

New DNS Addresses

Use this feature to set the DNS server address for the local machine.

Commit Changes and Exit

Press <Enter> to save changes and exit.

Discard Changes and Exit

Press <Enter> to discard changes and exit.

Save Changes and Exit

Press <Enter> to save changes and exit.

PCIe/PCI/PnP Configuration Menu

▶PCIe/PCI/PnP Configuration

The following information is displayed.

- PCI Bus Driver Version

PCI Devices Common Settings:

Re-Size BAR Support

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

SR-IOV Support

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

ARI Support

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

MMIO High Base

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

MMIO High Granularity Size

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

Bus Master Enable

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

NVMe Firmware Source

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

VGA Priority

Use this feature to select the graphics device to be used as the primary video display for system boot. The options are **Onboard** and Offboard.

Onboard Video Option ROM

Select EFI to boot the computer using the Extensible Firmware Interface (EFI) device installed on the onboard video port. The options are Disabled and **EFI**.

AOC-ATG-i2S LAN1 OPROM / Onboard SAS Option ROM / Onboard LAN1 Option ROM / Onboard NVMe1 Option ROM — Onboard NVMe24 Option ROM

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

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

HTTP Boot Configuration Menu

▶HTTP Boot Configuration

HTTP Boot Policy

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

HTTP Boot Checks Hostname

Enable this feature for HTTPS boot to check the hostname of the TLS certificates to see if it matches the hostname provided by the remote server. The options are **Enabled** and Disabled.

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

Priority of HTTP Boot

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

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

Select IPv4 or IPv6

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

Boot Description

Use this feature to enter a boot description, which cannot be longer than 75 characters. Be sure to enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI

Enter a Boot Uniform Research Identifier (URI) with 128 characters or fewer. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created. This feature is only supported on Dual or EFI Boot Mode.

Instance of Priority 2: (Available when "HTTP Boot Policy" is set to Apply to each LAN or Boot Priority #1 instantly)

This feature sets the rank target port. The default setting is **0**.

Select IPv4 or IPv6 (Unavailable when "Instance of Priority x:" is set to 0)

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

Boot Description (Unavailable when "Instance of Priority x:" is set to 0

Use this feature to enter a boot description, which cannot be longer than 75 characters. Be sure to enter a boot description; otherwise, the boot option for the URI cannot be created.

Boot URI (Unavailable when "Instance of Priority x:" is set to 0)

Enter a Boot URI with a maximum of 128 characters. This Boot URI determines how IPv4 Boot Option and IPv6 Boot Option will be created. This feature is only supported on Dual or EFI Boot Mode.

Supermicro KMS Server Configuration Menu

▶Supermicro KMS Server Configuration

Note: Be sure to configure all the features in the submenu of Supermicro KMS Server Configuration and the feature of "KMS Security Policy" in the submenu of Super-Guardians Configuration so that your system can communicate with the KMS server.

Supermicro KMS Server IP address

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

Second Supermicro KMS Server IP address

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

Supermicro KMS TCP Port number

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

KMS Time Out

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

TimeZone

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

Client UserName

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

Client Password

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

▶CA Certificate

▶Client Certificate

▶Client Private Key

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

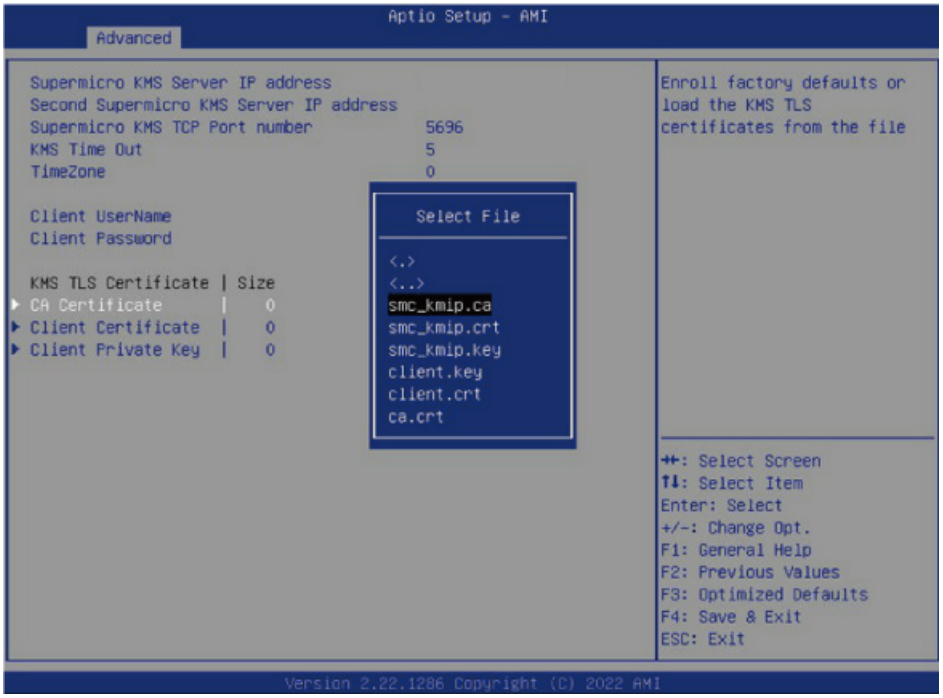


Figure 4-3: Select File Option Menu

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

Use this feature to change the private key password.

Super-Guardians Configuration Menu

▶Super-Guardians Configuration

Super-Guardians Protection Policy

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

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

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

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

Notes:

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

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

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

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

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

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

Note: Be sure to install a TPM 2.0 device to your system before configuring this feature.

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

The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save the settings and reboot the system. While booting, the BIOS will automatically load the Authentication-Key (filename: TPMAuth.bin) from the USB flash drive. Afterwards, the default setting will be set to Disabled by the BIOS.

Notes:

- Be sure to connect a USB flare drive with the Authentication-Key (filename: TPM-Auth.bin) to your system before the system reboot.
- Be sure to save the Authentication-Key (filename: TPMAuth.bin) to the USB flash drive and have a backup. Load the Authentication-Key (filename: TPMAuth.bin) after installing a TPM device. Otherwise, the TPM function can not work properly.

Save Authentication-Key (Available when "TPM Security Policy" is set to Enabled)

The options are **Disabled** and Enabled. Set this feature to Enabled. Changes take effect after you save the settings and reboot the system. While booting, the BIOS will automatically save the Authentication-Key (filename: TPMAuth.bin) to the USB flash drive. Afterwards, the default setting will be set to Disabled by the BIOS.

Note: Be sure to connect a USB flash drive to your system before the system reboot.

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

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

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

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

TLS Authenticate Configuration Menu

▶TLS Authenticate Configuration Menu

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

▶Server CA Configuration

This feature allows you to configure the client certificate that is to be used by the server.

▶Enroll Certification

This feature allows you to enroll the certificate in the system.

▶Enroll Certification Using File

This feature allows you to enroll the security certificate in the system by using a file.

Certification GUID

Press <Enter> and input the certification Global Unique Identifier (GUID).

▶Commit Changes and Exit

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

▶Discard Changes and Exit

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

▶Delete Certification

This feature is used to delete the certificate if a certificate has been enrolled in the system.

▶Client Certification Configuration

Driver Health Menu

▶Driver Health

This feature displays the health information of the drivers installed in your system, including LAN controllers, as detected by the BIOS. Select one and press <Enter> to see the details.

Note: This section is provided for reference only, as the driver health status will differ depending on the drivers installed in your system. It's also based on your system configuration and the environment that your system is operating in.

4.4 Event Logs

Use this menu to configure Event Log settings.

Figure 4-4: Event Logs Page

▶Change SMBIOS Event Log Settings

Note: Reboot the system for the changes in this section to take effect.

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

Erase Event Log (Available when "SMBIOS Event Log" is set to Enabled)

Select No to keep the event log without erasing it upon next system bootup. Select (Yes, Next reset) to erase the event log upon the next system reboot. The options are **No**, (Yes, Next reset), and (Yes, Every reset).

When Log is Full (Available when "SMBIOS Event Log" is set to Enabled)

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

SMBIOS Event Log Standard Settings

Log System Boot Event (Available when "SMBIOS Event Log" is set to Enabled)

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

MECI (Available when "SMBIOS Event Log" is set to Enabled)

Enter the increment value for the multiple event counter. Enter a number between 1 to 255. The default setting is **1**. (MECI is the abbreviation for Multiple Event Count Increment.)

METW (Available when "SMBIOS Event Log" is set to Enabled)

This feature is used to determine how long (in minutes) the multiple event counter should wait before generating a new event log. Enter a number between 0 to 99. The default value is **60**. (METW is the abbreviation for Multiple Event Count Time Window.)

▶View SMBIOS Event Log

This feature allows you to view the event in the system event log. Select this feature and press <Enter> to view the status of an event in the log. The following information is displayed:

DATE / TIME / ERROR CODE / SEVERITY.

4.5 BMC

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

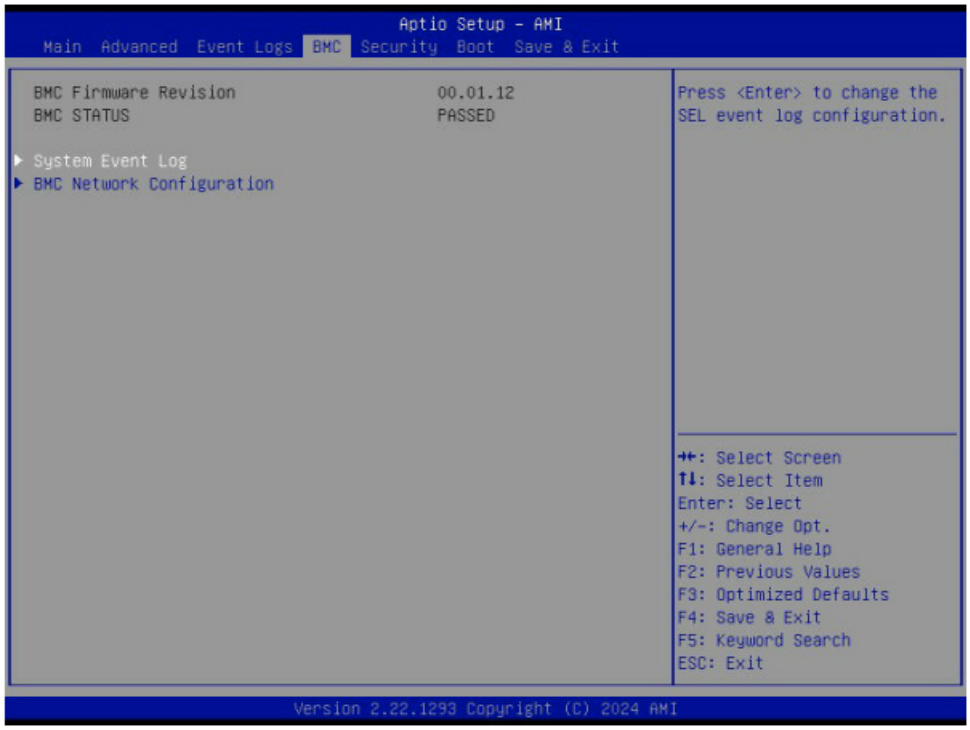


Figure 4-5: BMC Page

BMC Firmware Revision

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

BMC STATUS

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

System Event Log Menu

▶System Event Log

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

Enabling/Disabling Options

SEL Components

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

Erasing Settings

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

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

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

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

BMC Network Configuration Menu

▶BMC Network Configuration

Update BMC LAN Configuration

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

****

Configure IPv4 Support

****

BMC LAN Selection

This feature displays the type of BMC LAN.

BMC Network Link Status:

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

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

Use this feature to select the source of the IPv4 connection. If Static is selected, you will need to know the IP address of the IPv4 connection and enter it into the system manually in the field. If DHCP is selected, the BIOS will search for a Dynamic Host Configuration Protocol (DHCP) server in the network that is attached to and request the next available IP address for this computer. The options are Static and **DHCP**.

Station IP Address

This feature displays the Station IP address in decimal and in dotted quad form (i.e., 172.29.176.131). It is available for configuration when "Configuration Address Source" above is set to Static.

Subnet Mask

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

Station MAC Address

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

Gateway IP Address

This feature displays the Gateway IP address for this computer. This should be in decimal and in dotted quad form (i.e., 172.29.0.1). It is available for configuration when "Configuration Address Source" above is set to Static.

****

Configure IPv6 Support

****

IPv6 Address Status

This feature displays the status of the IPv6 address.

IPv6 Support (Available when "Update BMC LAN Configuration" is set to Yes)

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

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

Use this feature to select the source of the IPv6 connection. If Static Configuration is selected, you will need to know the IP address of IPv6 connection and enter it into the system manually in the field. If the other two options are selected, the BIOS will search for a DHCP server in the network to which it is attached and request the next available IP address for this computer. The options are Static Configuration, **DHCPv6 Stateless**, and DHCPv6 Stateful.

IPv6 Address ("Static," "DHCPv6 Stateless," or "DHCPv6 Stateful," depending on the option you selected for "Configuration Address Source" above)

This feature displays the station IPv6 address. It is available for configuration when "Configuration Address Source" above is set to Static Configuration.

Prefix Length

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

Gateway IP

This feature displays the IPv6 gateway IP address. It is available for configuration when "Configuration Address Source" above is set to Static Configuration.

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

Use this feature to set the DNS server IP. The default setting allows your system to obtain the DNS server IP automatically. The options are Auto obtain DNS server IP and Manually obtain DNS server IP.

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

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

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

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

****

Configure VLAN Support

****

LAN Channel 1

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

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

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

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

4.6 Security

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

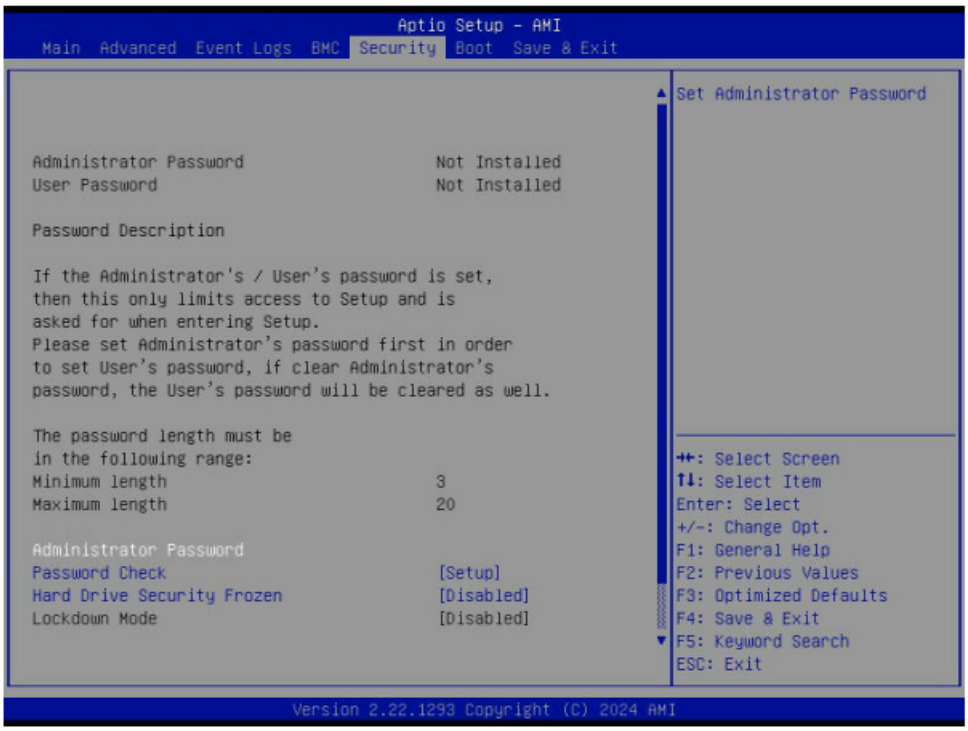


Figure 4-6: Security Page

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

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

The following information is displayed.

- Administrator Password
- User Password
- Password Description

Administrator Password

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

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

This feature indicates if a user password has been installed. It also allows you to set the user password, which is required to enter the BIOS Setup utility. The length of the password can be between three to 20 characters long.

Password Check

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

Hard Drive Security Frozen

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

Lockdown Mode (Available when the DCMS key is activated)

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

Secure Boot Menu

▶Secure Boot

Note: For detailed instructions on how to configure Security Boot settings, refer to the Security Boot Configuration User's Guide at https://www.supermicro.com/support/manuals.

The following information is displayed.

- System Mode
- Secure Boot

Secure Boot

Select Enabled to configure Secure Boot settings. The options are **Disabled** and Enabled.

Secure Boot Mode

Use this feature to select the desired secure boot mode for the system. The options are Standard and **Custom**.

▶Enter Audit Mode

Note: This submenu is available when "Secure Boot Mode" is set to Custom.

Select Ok to enter the Audit Mode workflow. It will result in erasing of Platform Key (PK) variables and reset the system to the Setup/Audit Mode.

▶Key Management

Note: This submenu is available when "Secure Boot Mode" is set to Custom.

The following information is displayed.

- Vendor Keys

Provision Factory Default Keys

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

▶Restore Factory Keys

Note: This submenu is available when any secure keys have been installed.

Select Yes to restore the manufacturer's default keys to ensure system security. The options are **Yes** and No. Selecting Yes will reset the system to the Deployed mode.

▶Reset to Setup Mode

Note: This submenu is available when any secure keys have been installed.

This feature resets the system to the Setup Mode. The options are **Yes** and No.

▶Enroll EFI Image

This feature allows the EFI image to run in the secure boot mode, which will enroll the SHA256 Hash certificate of a PE image into the Authorized Signature Database (DB).

▶Export Secure Boot Variables

Note: This submenu is available when any secure keys have been installed.

This feature exports the NVRAM contents of secure boot variables to a storage device. The options are **Yes** and No.

Secure Boot variable / Size / Keys / Key Source

▶Platform Key (PK)

Use this feature to enter and configure a set of values to be used as platform firmware keys for the system. These values also indicate the sizes, key numbers, and the sources of the authorized signatures. Select Update to update the platform key.

▶Key Exchange Keys (KEK)

Use this feature to enter and configure a set of values to be used as Key Exchange Keys for the system. These values also indicate the sizes, key numbers, and the sources of the authorized signatures. Select Update to update your Key Exchange Keys. Select Append to append your Key Exchange Keys.

▶Authorized Signatures (db)

Use this feature to enter and configure a set of values to be used as Authorized Signatures for the system. These values also indicate the sizes, key numbers, and the sources of the authorized signatures. Select Update to update your Authorized Signatures. Select Append to append your Authorized Signatures.

▶Forbidden Signatures (dbx)

Use this feature to enter and configure a set of values to be used as Forbidden Signatures for the system. These values also indicate sizes, key numbers, and key sources of the forbidden signatures. Select Update to update your Forbidden Signatures. Select Append to append your Forbidden Signature.

▶Authorized TimeStamps (dbt)

This feature allows you to set and save the timestamps for the Authorized Signatures, which will indicate the time when these signatures are entered into the system. These values also indicate sizes, keys, and key sources of the authorized timestamps. Select Update to update your Authorized TimeStamps. Select Append to append your Authorized TimeStamps.

▶OsRecovery Signatures (dbr)

This feature allows you to set and save the Authorized Signatures used for OS recovery. Select Update to update your OsRecovery Signatures. These values also indicate sizes, keys, and key sources of the OsRecovery Signatures. Select Append to append your OsRecovery Signatures.

4.7 Boot

Use this menu to configure Boot settings.

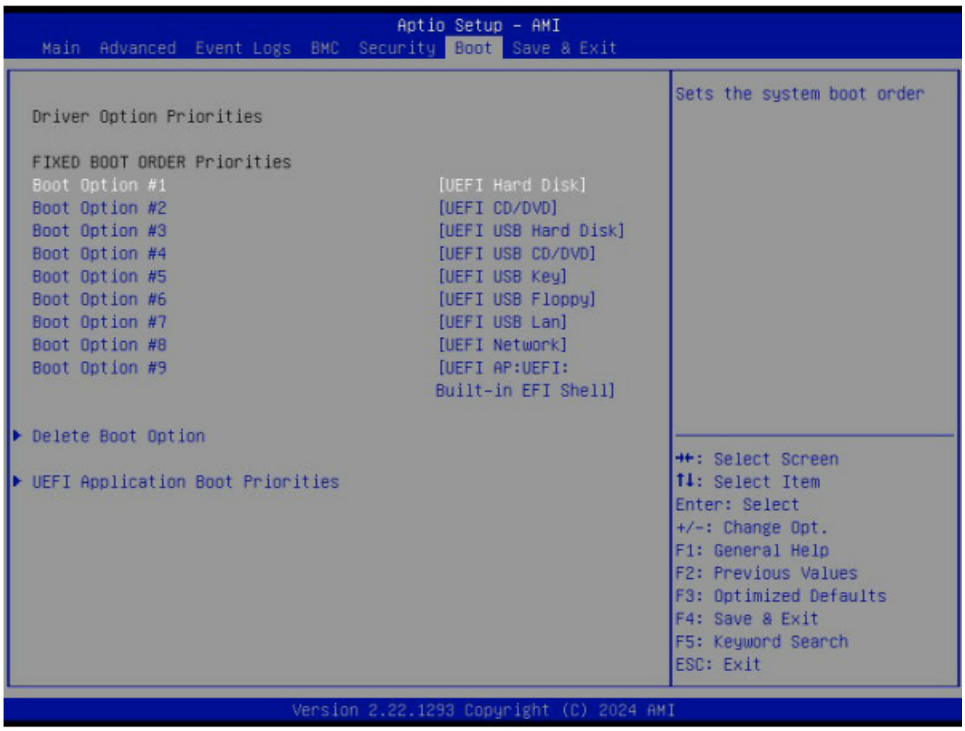


Figure 4-7: Boot Page

Driver Option Priorities

FIXED BOOT ORDER Priorities

This feature prioritizes the order of a bootable device from which the system will boot. Press <Enter> on each feature sequentially to select the device.

- Boot Option #1 — Boot Option #9

▶Add New Boot Option

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

This feature allows you to add a new boot option to the boot priority features for system boot.

Add boot option

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

Path for boot option

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

Boot option File Path

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

Create

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

▶Delete Boot Option

This feature allows you to select a boot device to delete from the boot priority list.

Delete Boot Option

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

▶UEFI Application Boot Priorities

This feature allows you to set the system boot order of detected devices.

4.8 Save & Exit

Select Save & Exit from the BIOS Setup screen to configure the following settings and options:

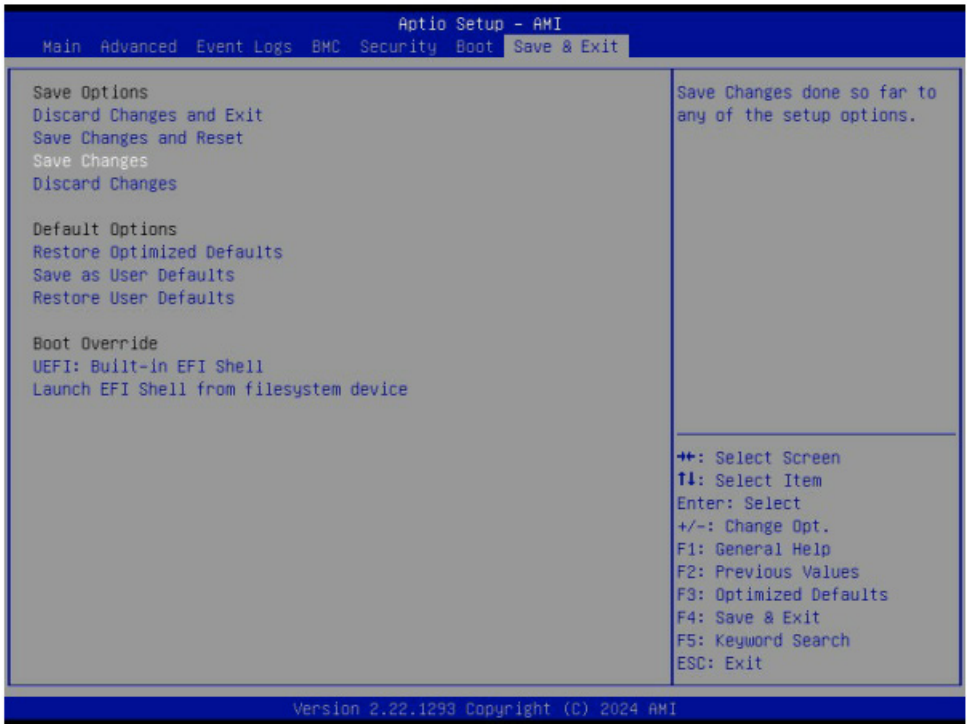


Figure 4-8: Save & Exit Page

Save Options

Discard Changes and Exit

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

Save Changes and Reset

When you have completed the system configuration changes, use this feature to exit the BIOS Setup utility and reboot the computer for the new system configuration parameters to become effective.

Save Changes

When you have completed the system configuration changes, use this feature to save all changes you've made. This will not reset (reboot) the system.

Discard Changes

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

Default Options

Restore Optimized Defaults

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

Note: Reboot the system for the changes to take effect, and ensure that your system has the optimized default settings

Save As User Defaults

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

Restore User Defaults

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

Boot Override

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

Launch EFI Shell from filesystem device

Launches EFI Shell application from one of the available filesystem devices.

Appendix A

Firmware Update Through WEB GUI and SUM

A.1 Overview

This user's guide provides detailed information on how to update the Supermicro BMC firmware on X14 and H14 series motherboards using BMC WEB GUI or SUM (Supermicro Update Manager).

Note: For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI UEFI BIOS, RSD/SCC, TAS, and IPMIView, \ refer to our website at https://www.supermicro.com/en/solutions/management-software/bmc-resources for details.

A.2 Updating Firmware Using BMC WEB GUI

In order to keep the system working properly, follow the steps to update BMC firmware through BMC WebGUI:

1. Log in to the account by entering the IP address into a web browser and following the prompts on the screen.

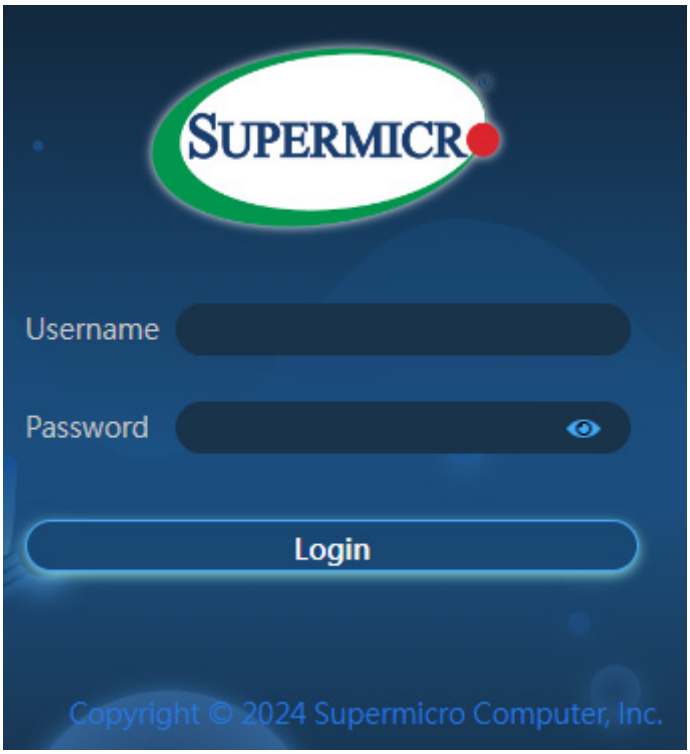


Figure A-1: BMC Firmware Web User Login

Note: Contact Supermicro sales or FAE if you do not know your username or password.

2. Click on the Firmware Update tab on the BMC dashboard.

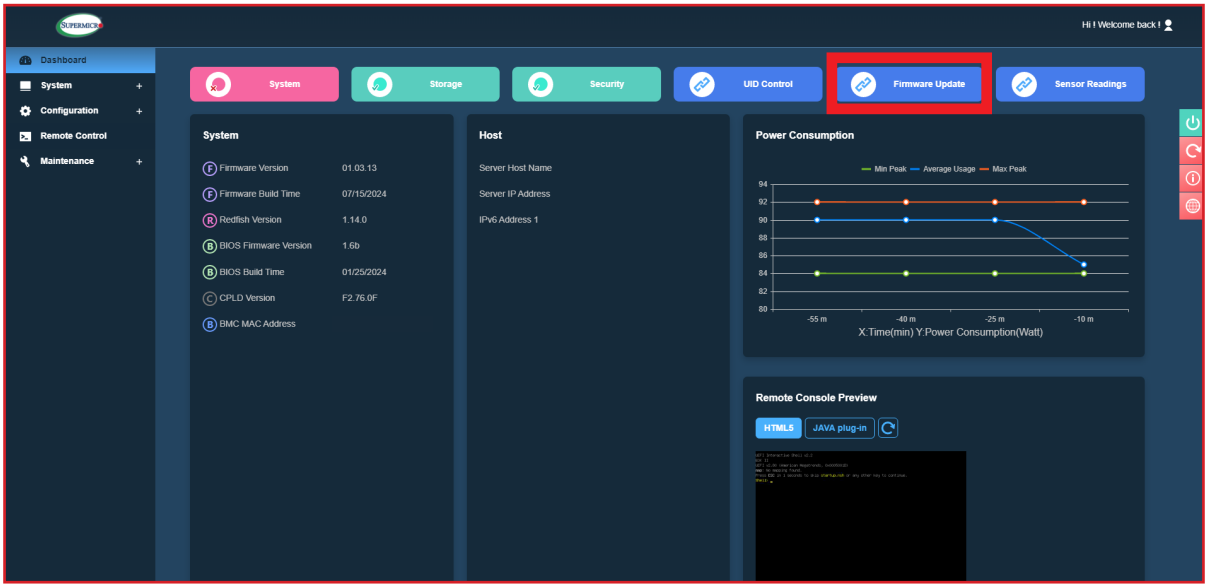


Figure A-2: BMC Firmware Update Dashboard

3. When the following screen appears, select the [BMC] option and click [Next].

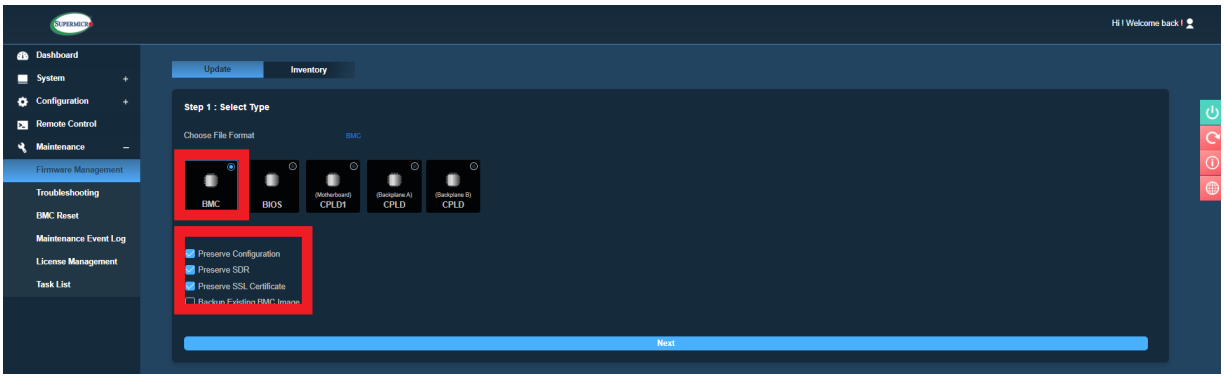


Figure A-3: BMC Firmware Update Default Setting

4. Press [Select File] to select the new BMC firmware file and press [Upload].

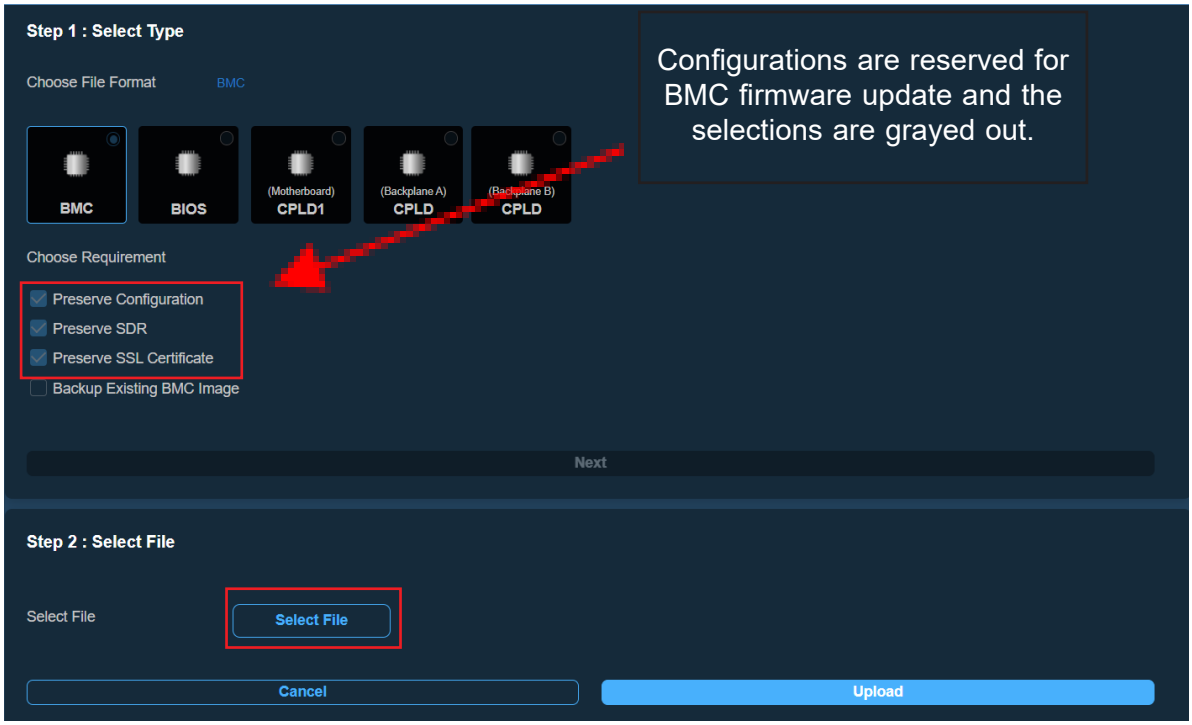


Figure A-4: Select and Upload New BMC Firmware File

Note 1: By default, the firmware update process preserves the existing configuration, SDR, and SSL certificates for the new BMC firmware. You can deselect any of the preservation options if applicable.

Note 2: Select the "Backup existing image" option to back up the existing BMC or BIOS image. The backup image will be used for auto-recovery in case of a firmware integrity check fails at any time. You can also manually recover BMC or BIOS from the backup image. Go to the inventory page to manually recover BMC or BIOS.

5. Wait for the upload process to complete, which might take a few minutes.

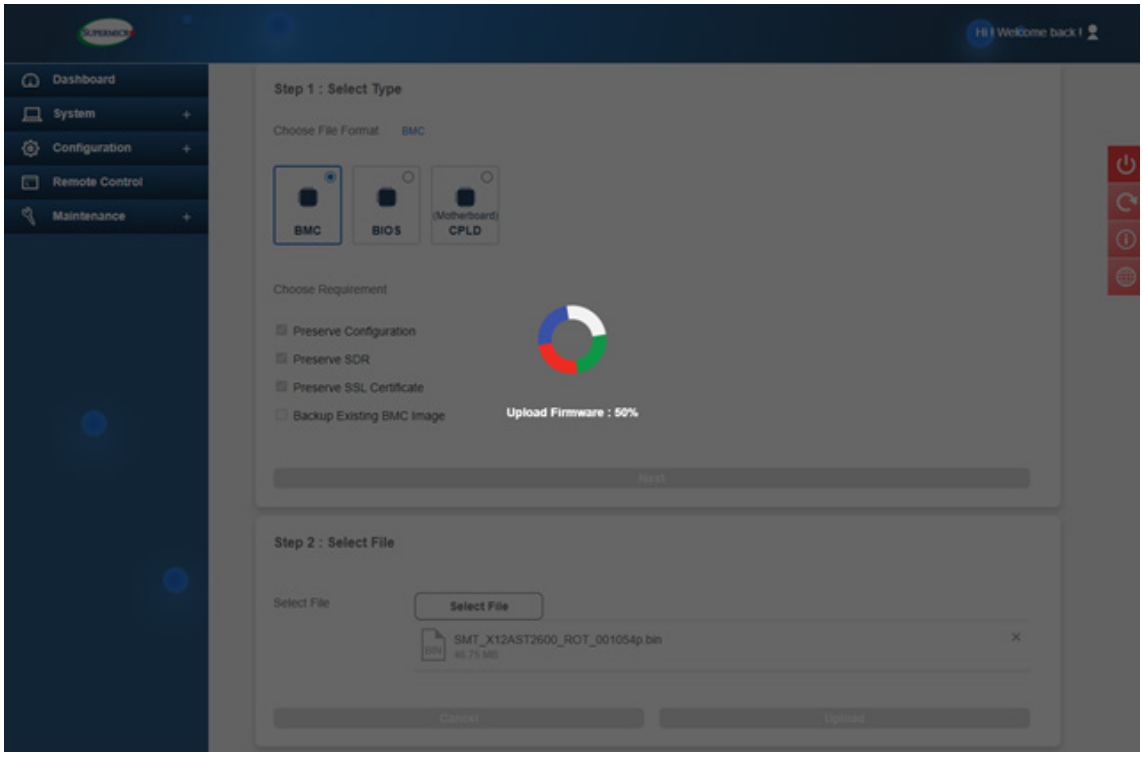


Figure A-5: New BMC Firmware Uploading

6. Verify the new firmware version and press [Update] to perform the firmware update.

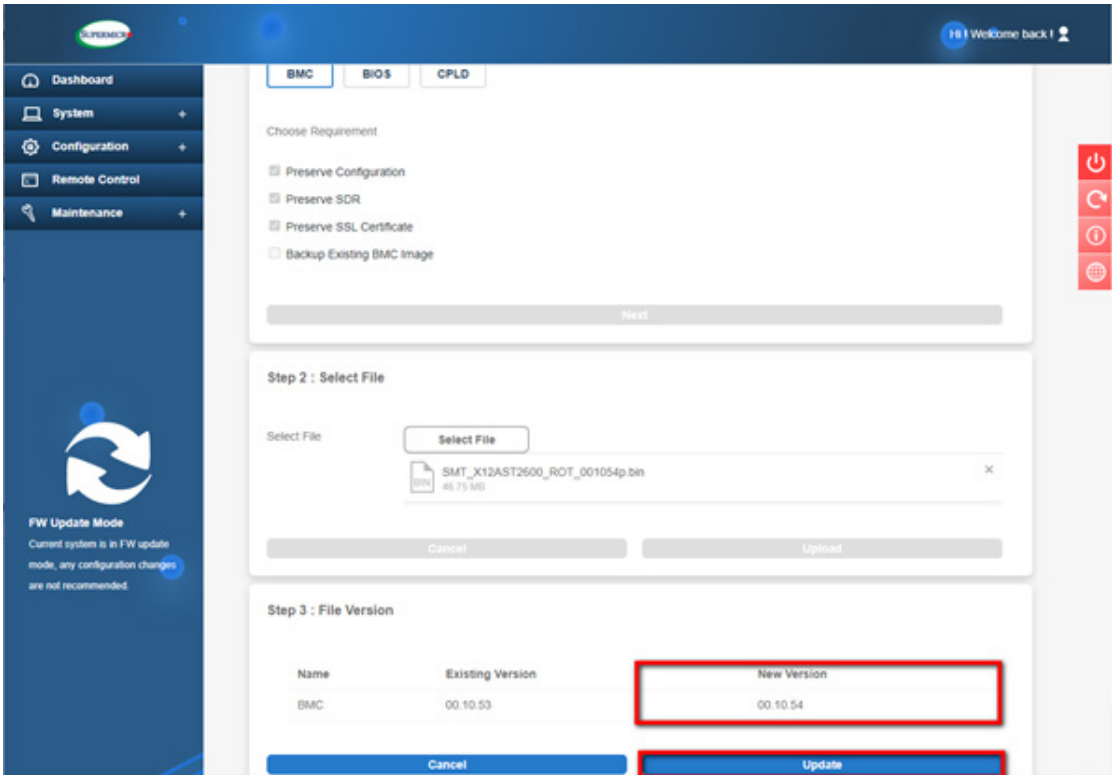


Figure A-6: Verify the New BMC Firmware Version

7. Wait for the update process to be completed. It might take a few minutes. Any system configuration change is not recommended during the update process.

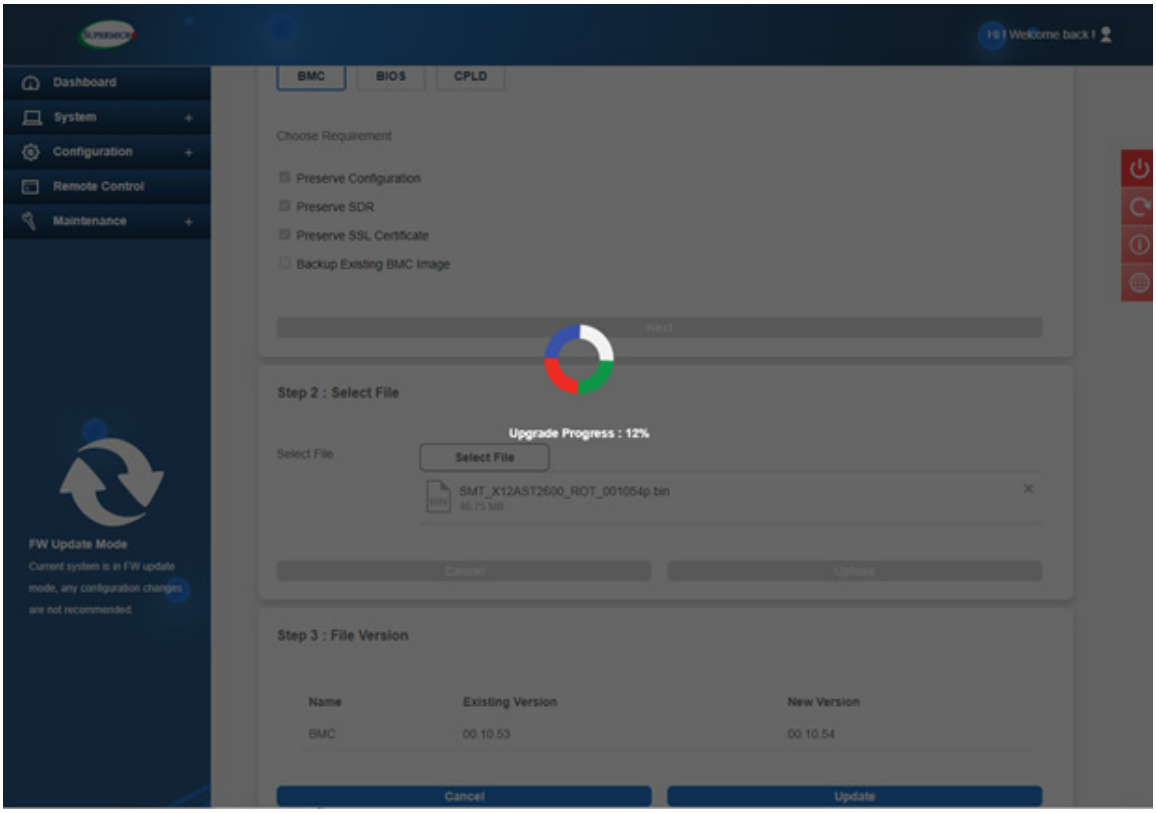


Figure A-7: BMC Firmware Updating in Progress

8. BMC will reboot after the firmware is completely updated. Wait for BMC to complete the system reboot**.**

9. Once the reboot process is complete, WebGUI will return to the login screen, and you will need to log in to the system again.

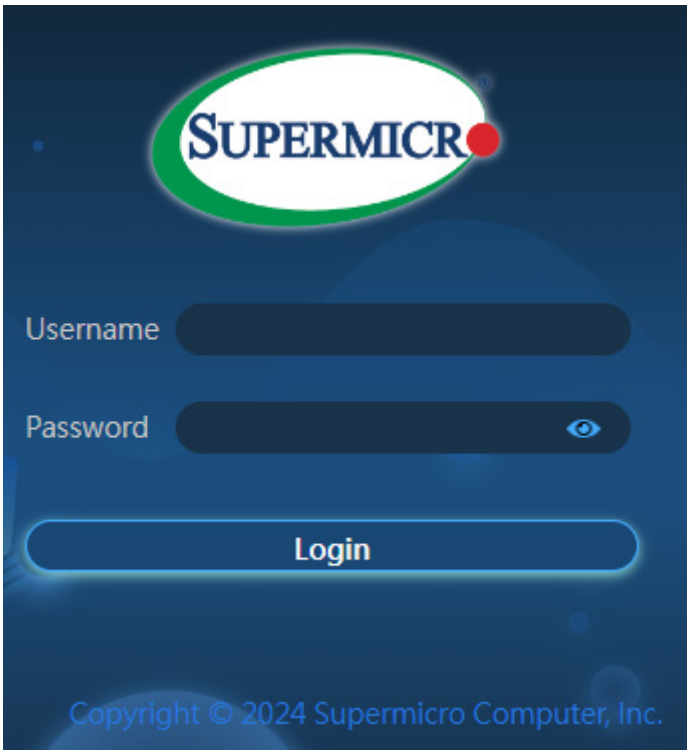


Figure A-8: BMC Firmware Web User Login

A.3 Updating Firmware Using SUM

Follow the procedure to update BMC firmware in Supermicro Update Manager (SUM).

Step 1: Installing SUM

To install SUM in Linux/FreeBSD OS, take the following steps. The Windows installation is similar.

1. Extract the following archive file:

   ```
   sum_x.x.x_Linux_x86_64_YYYYMMDD.tar.gz
   ```

2. Go to the extracted directory:

   ```
   sum_x.x.x_Linux_x86_64
   ```

3. Rename this directory to:

   ```
   SUM_HOME
   ```

4. Run SUM in the following directory:

   ```
   SUM_HOME
   ```

   Linux Example:

   ```
   [shell]# tar xzf sum_x.x.x_Linux_x64_YYYYMMDD.tar.gz
   [shell]# cd sum_x.x.x_Linux_x86_64
   [SUM_HOME]# ./sum
   ```

Step 2: Updating BMC Firmware

Complete the following steps to update BMC firmware:

1. Use the following command to run SUM to update BMC firmware:

```
UpdateBmc
```

Syntax:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p
<password>] -c UpdateBmc --file <filename> [--overwrite_cfg]
[--overwrite_sdr] [--backup] [--forward]
```

Notes:

- BMC SOC will be updated after the firmware update process is completed.
- BMC configuration settings will be preserved by default for the new BMC firmware unless the --overwrite_cfg option is used.
- DO NOT flash BIOS and BMC firmware images at the same time.
- The --overwrite_cfg option overwrites the current BMC configuration using the factory default values in the given BMC image file.
- The --overwrite_sdr option overwrites the current BMC SDR data.
- The following SUM command is recommended for BMC firmware updates:

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p
<password>] -c UpdateBmc --file <filename>
```

2. The progress of the firmware update will be displayed. DO NOT interrupt the process until it is complete. BMC will reboot after the firmware is completely updated. Wait for BMC to complete the system reboot.

Example:

Remote Update

You can use SUM to update BMC firmware through a IPMI port.

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p XXXXXX -c UpdateBmc
--file SMCI_BMC.rom
```

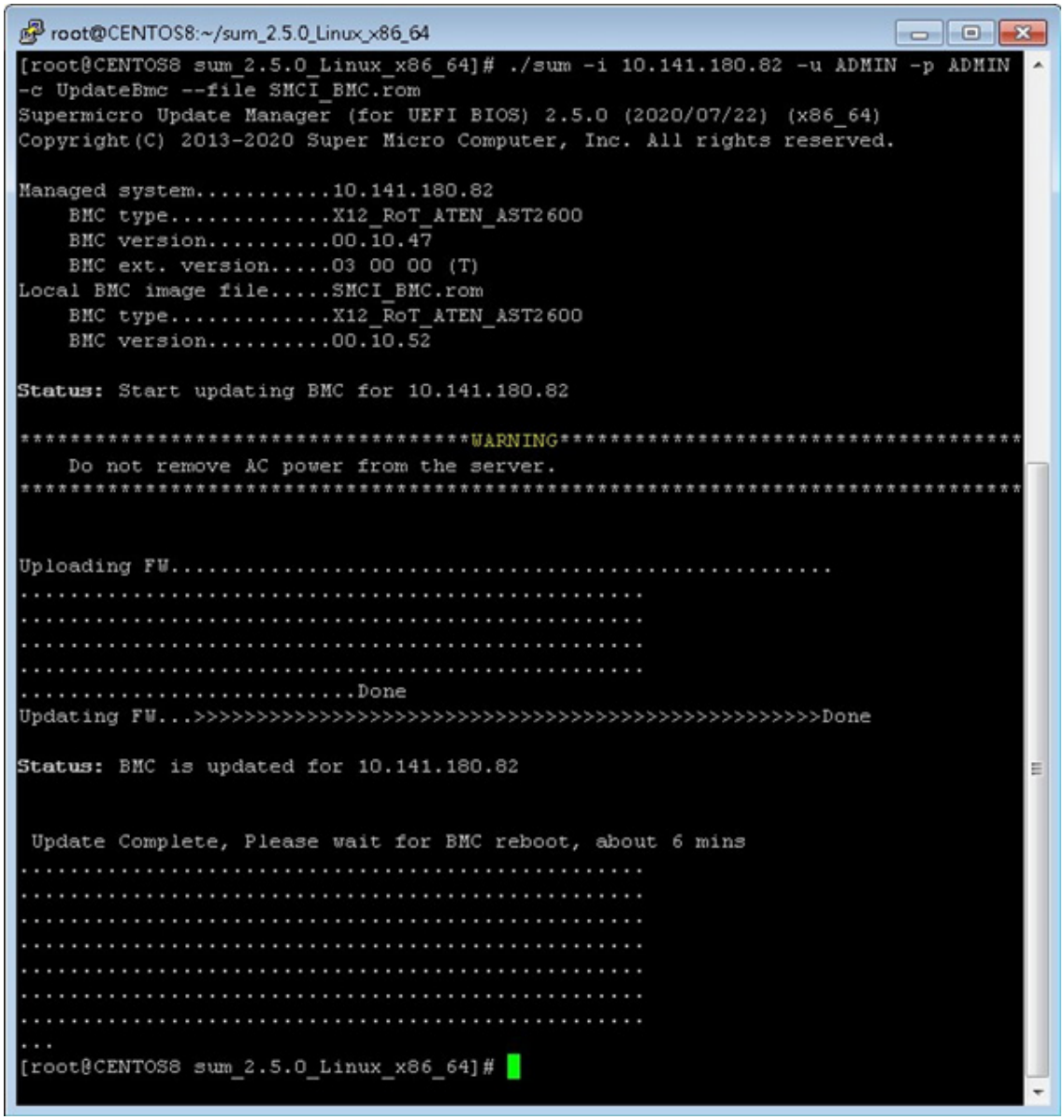


Figure A-9: Output of BMC Remote Update in SUM

Local Update

You can use SUM to update BMC firmware under Linux, Windows, or FreeBSD.

```
SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p XXXXXX -c UpdateBmc --file
SMCI_BMC.rom
```

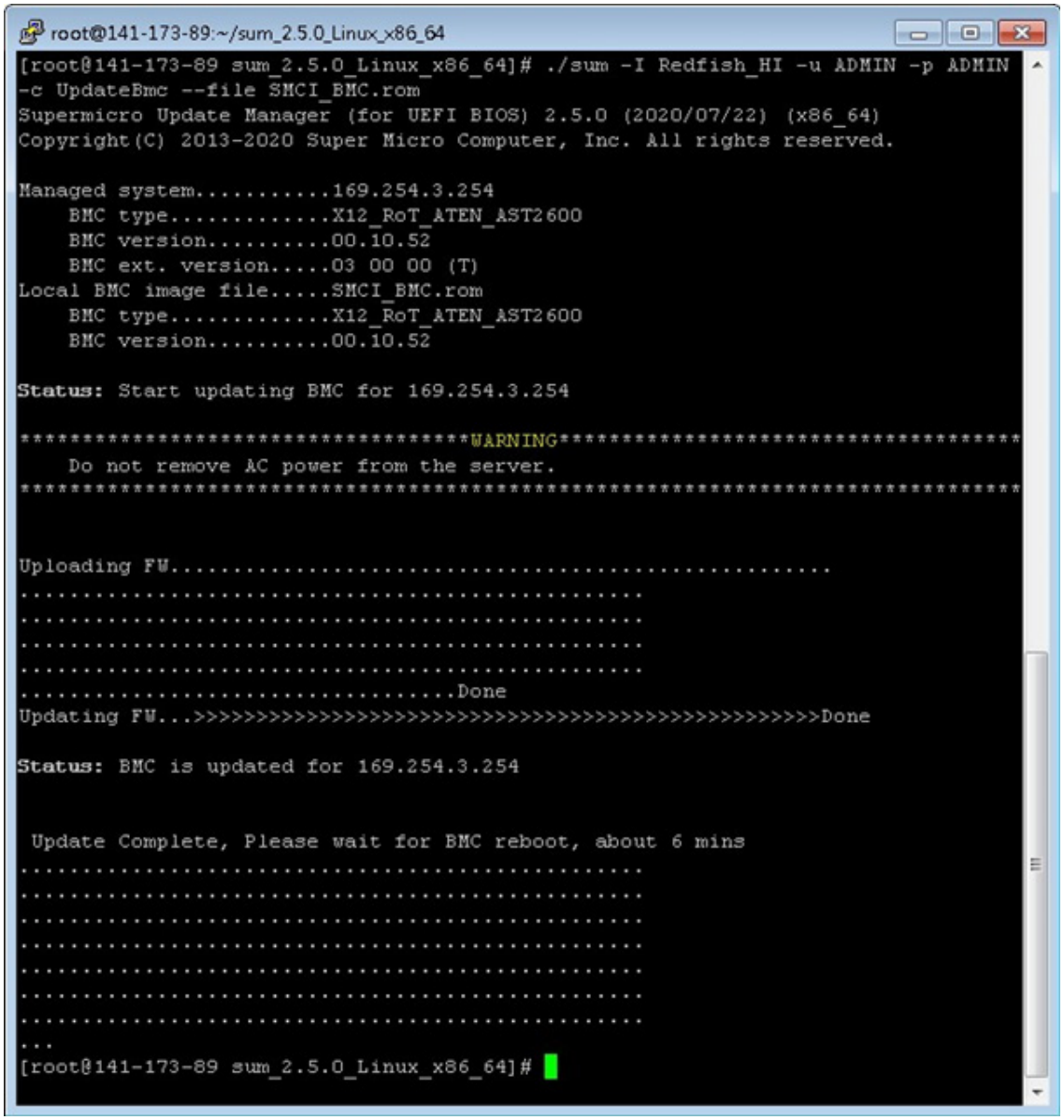


Figure A-10: Output of BMC Local Update in SUM

Appendix B

Introduction to SMASH

B.1 Overview

The System Management Architecture for Server Hardware (SMASH) platform, developed by Distributed Management Task Force, Inc. (DMTF), delivers a host of architecture-based and industry-standard protocols that will allow IT professionals to simplify the task of managing multiple network systems in a data center. This platform offers a simple, intuitive solution to manage heterogeneous servers in a web environment, regardless of differences in hardware, software, OS, or network configuration. It also provides the end-users and the ISV community with interoperable management technology for multi-vendor server platforms.

How SMASH Works

SMASH simplifies typical SMASH scripts by reducing commands to simple verbs. Although designed to manage multi-server configurations as a whole, SMASH can address individual components in a specific machine by using the SSH command-line protocol. Even when multiple processors, add-on cards, logical devices, and cooling systems are installed in a server, SMASH can be directed at a particular component in the server. A manager can use a text console to access, monitor, and manage all servers that are connected to the same SSL connection. This platform can be programmed to periodically check all sensors in all machines or monitor a particular component in a specific server at any time. By adjusting the scope of tasks and the schedules of monitoring, SMASH allows IT professionals to effectively manage multi-system clusters, minimize power consumption, and achieve system management efficiency.

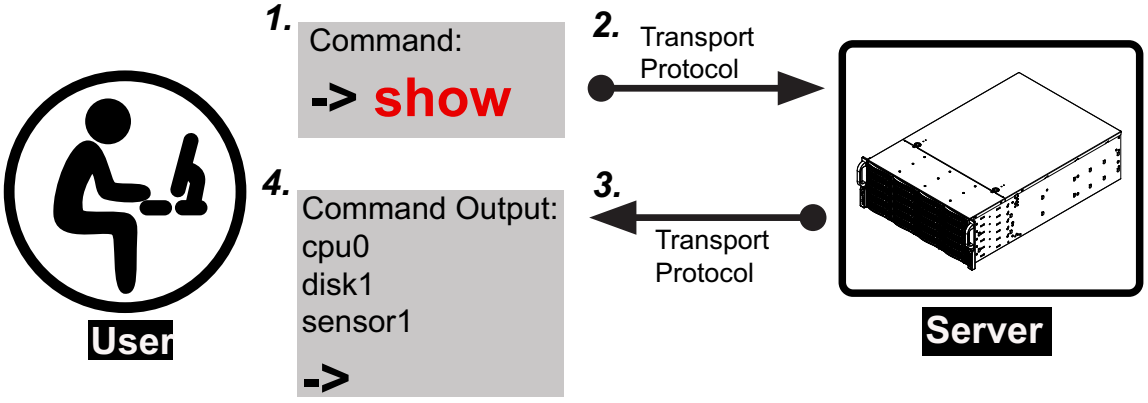


Figure B-1: SMASH-CLP User Interface

SMASH Compliance Information

The SMASH platform documented in this user's guide is developed in reference to and in compliance with the SMASH Initiative Standards based on the following DMTF documents.

- System Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP) Architecture White Paper (DSP 2001)
- SM CLP Specification (DSP 0214)
- SM ME Addressing Specifications (DSP 0215)
- SM SLP to CIM Common Mapping Specification (DSP 0216)
- Common Information Model (CIM) Infrastructure Specification (DSP 0004)
- The Secure Shell (SSH) Protocol Architecture (RFC4251)
- The Secure Shell (SSH) Connection Protocol (RFC4254)

B.2 An Important Note to the User

The information included in this user's guide provides a general guideline on how to use the SMASH protocol for system management. Instructions given in this document may or may not be applicable to the system, depending on the configuration of the system or the environment it operates in.

For documents concerning utility support, such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI BIOS, RSD/SCC, TAS, and IPMIView, refer to our website at https://www.supermicro.com/en/solutions/management-software for details.

B.3 Using SMASH

This section provides a general guideline on how to use SMASH for system management in a web-based environment. Refer to the SMASH script provided to curtail a server management protocol for the systems.

Note: The instructions listed are applicable to both Windows and Linux systems. The default setting is the Windows platform.

B.4 Initiating the SMASH Protocol

There are two ways of initiating the SMASH protocol.

To Initiate SMASH Automatically

You can initiate SMASH automatically by connecting the BMC using the Secure Shell protocol (SSH) from a client machine.

To Connect From a Linux Machine

1. Use 'ssh<BMC ip address>'.
2. Enter the password.

To Connect From Other Machines

1. Use a terminal emulator application such as *Putty*.
2. Enter the *BMC IP* address in the terminal emulator application.
3. Choose *SSH* as the connection type.
4. Enter the password at the prompt.
5. If successfully logged in, the SMASH prompt will be displayed.

B.5 SMASH-CLP Main Screen

After successfully logging into the SSL network, the SMASH Command Line Protocol Main screen will display.

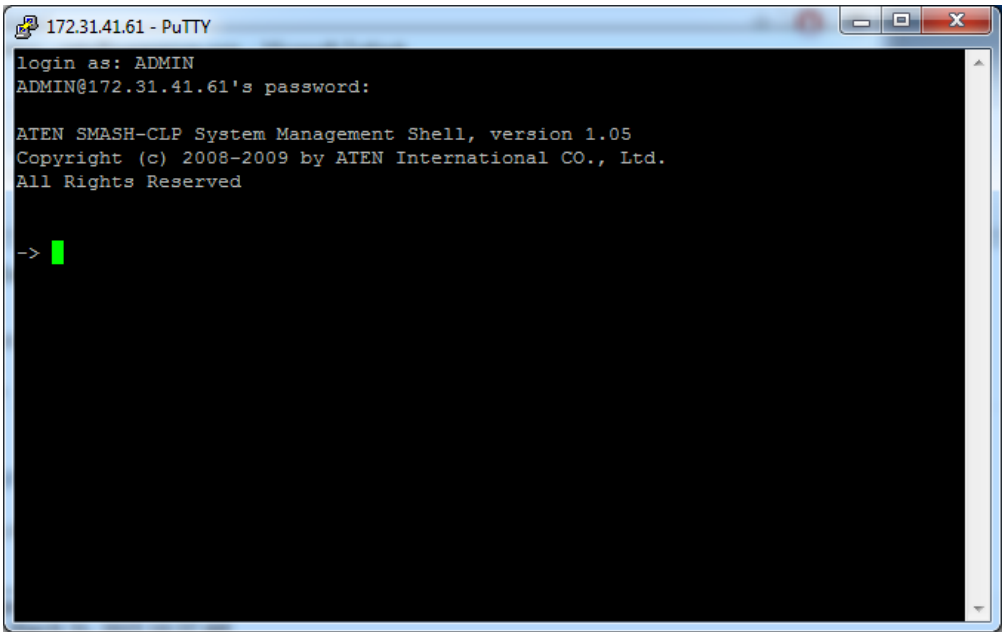


Figure B-2: SMASH-CLP Main Screen

B.6 Using SMASH for System Management

After you have familiarized yourself with the SMASH commands, you will be able to use these commands to manage the system. To properly manage the network system, be sure to take the following steps:

Note: Make sure that the format of all commands is compliant with the DMTF specification, which is "<Verb> [<option>] [<target>] [<properties>]," where:

- A ***Verb*** means a *command*.
- An ***Option*** works according to the definition of a command given in Section B-7: Definitions of Command Verbs.
- A ***Target*** is a managed device.
- ***Properties*** are the specific attributes that you want to assign to a target machine or to get from a target machine.

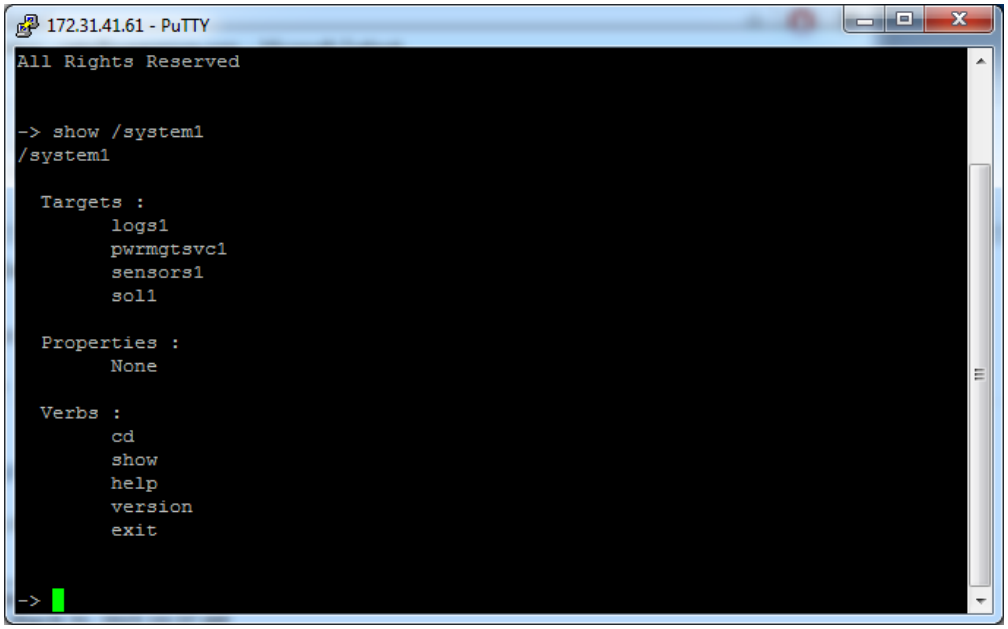


Figure B-3: Using SMASH for System Management

B.7 Definitions of Commands Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow you to issue commands to a target system to perform certain tasks. For example, the verbs supported by the *admin* target group include: cd, help, load, dump, create, delete, exit, version, show, etc.

- ***cd***

The command verb *cd* is used to navigate to a specific target address using the SSL protocol. For example, issuing the command *cd/admin1* will direct you to the target *admin* (AdminDomain).

- ***show***

The command verb *show* is used to display the properties and the contents of a target, a group of targets, or a subgroup of the target(s). Properties, contents, and supported operations related to the target, the group of targets, or their sub-targets will be displayed.

- ***exit***

The command verb *exit* is used when you want to exit from a SMASH session or close a session.

- ***help***

The command verb *help* is used when you want to get helpful hints or information on a context-specific feature. This command has the same function as the *help option* listed for the target group.

- ***Version***

Use the command verb *version* to display the CLP version used in a specific machine.

- ***set***

Use the command verb *set* to assign a set of values to the properties of a target machine.

- ***start***

The command verb *start* is used to turn on the power control, to start a process, or to change an operation state from a lower level to a higher level in a system.

- ***stop***

The command verb *stop* is used to turn off the power, to stop a process, or to change an operation state from a higher level to a lower level.

- ***reset***

The command verb *reset* is used to enable or disable the power control of or the processes of the machine.

- ***delete***

The command verb *delete* is used to delete or destroy an entry or a value previously entered. It can only be used in a specific target as defined according to the SAMSHCLP Standards.

- ***load***

The command verb *load* is used to move a binary image file from a URI source to the MAP. This command will achieve different results depending on the setting of a target system and how the verb *load* is defined in the DSP specification used in the system.

- ***dump***

The command verb *dump* is used to move a binary image file from the MAP to a URI source. This command will achieve different results depending on the setting of a target system and how the verb *dump* is defined in the DSP specification implemented in the system.

- ***create***

The command verb *create* is used to create a new address entry or a new feature in the MAP. It can only be used in a specific target as defined in the SMASH profile or MAP specifications.

B.8 SMASH Commands

The following table provides the definitions and descriptions of SMASH commands. The most useful commands are *show* and *help*, which will provide you with information on how to navigate through the SSL network connection.

Option Name	Short Form	Definition	Notes
-all	-a	Instructs a command verb to perform all tasks possible	None
-destination <*URI*>	None	Indicates the final location of an image or selected data	URI or SM instance address
-display	-d	Selects data that you wish to display	This can generate multiple query results
-examine	-x	Instructs the Command Processor to examine a command for syntax or semantic errors without executing it	None
-force	-f	Instructs the verb to ignore any warnings triggered by default, but go ahead and execute the command instead	None
-help	-h	Displays all information and documentation regarding the command verb	None
-keep <m[.s]	-k	Sets a time period to hold and keep the Job ID and the status of a command	The amount of time set to hold a command Job ID or its status can differ
-level <n>	-l	Instructs the Command Processor to execute the command for the current target and for all target machines within the level specified by you	Levels should be expressed in a natural number or "all"
-Output <args>	-o	Controls the format and the content of a command output. This only supports "format=clpxml" and "format=keyword"	Many variables or factors can affect the outcome of format, language, and level of details of the output
-Source <URI>	None	Indicates the location of a source image or a target	URI or SM Instance Address
-Version	-v	Displays the version of the command verb	None
-Wait	-w	Instructs the Command Processor to hold the command response or query result until all spawned jobs are completed	None

Figure B-4: SMASH Commands

B.9 Standard Command Options

The following table lists the standard command options.

CLP Option	CLP Verbs												
	CD	Create	delete	dump	exit	help	load	reset	set	show	start	Stop	version
all										x			
destination				x									
display										x			
examine	x	x	x	x	x	x	x	x	x	x	x	x	x
force			x	x			x	x	x	x	x	x	
help	x	x	x	x	x	x	x	x	x	x	x	x	x
keep													
level										x			
Output	x	x	x	x	x	x	x	x	x	x	x	x	x
Source							x						
Version	x	x	x	x	x	x	x	x	x	x	x	x	x
Wait													

Figure B-5: Standard Command Options

B.10 Target Addressing

To simplify the process of SMASH command execution, a file system called Target Addressing was created as illustrated in the diagram.

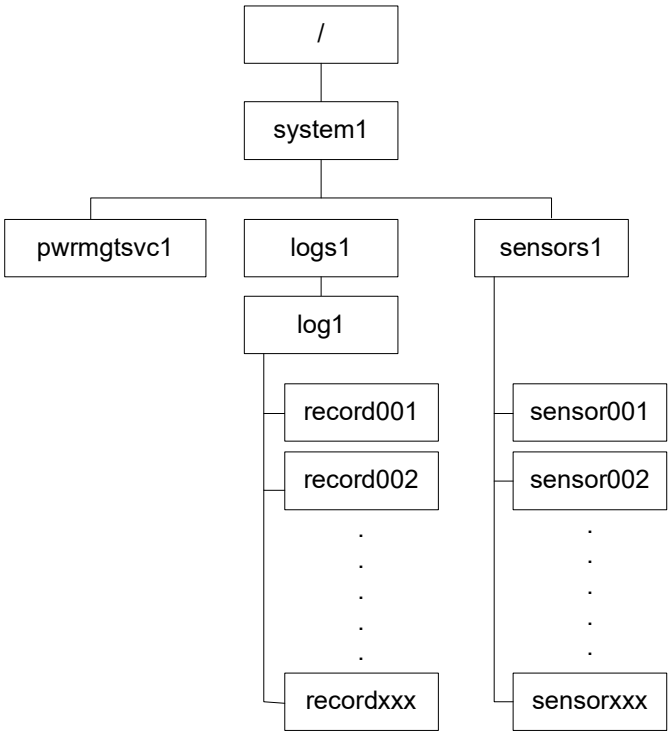


Figure B-6: Target Addressing Diagram

Terms Used in the Target Addressing Diagram

This section provides descriptions of the terms used in the Target Addressing Diagram above.

- ***"/"*** indicates *the root* of the system.
- ***"/system1"*** includes all major *Targets*.
- ***"/system1/logs1/log1"*** includes all sensor event logs.
- ***"/system1/sensors1"*** contains the readings and information of all sensors.
- ***"/system1/pwrmgtsvc1"*** is used for chassis control.
- ***"show../logs1"*** allows you to issue SMASH commands for the system to perform the tasks of your choice. For example:
  - Issuing the command ***"show/system1/logs1"*** *while you are in* ***"show../logs1"*** will allow you to set the *Absolute* or the *Relative* target path.

Appendix C

Unique Password for BMC

C.1 Overview

Due to California Senate Bill No. 327, a common default password is required to be available in a connected device that is capable of connecting to an IP network. Supermicro will no longer use the default password “ADMIN” for new devices or systems. Instead, we will assign a unique password that is specific to each new motherboard.

Effective as of January 1, 2020, each new Supermicro motherboard will come with two labels that contain a unique password assigned to that motherboard. One unique password label will be placed near the Baseboard Management Controller (BMC) chip and/or close to the motherboard serial number label. This label is not to be removed. The other unique password label will be placed on the CPU1 socket cover. This label is removable and can be placed in any location, such as on the side of the chassis or a service tag.

When logging in to the BMC for the first time, use the unique password provided by Supermicro to log in. Afterward, the unique password can be changed to the customer's chosen username and password for subsequent logins.

For more information regarding BMC passwords, visit our website at http://www.supermicro.com/bmcpassword.

C.2 Notice and Shipping Label Identifier

Every server that has a BMC unique password will include a notice in the plastic wrap on the top side of the plastic wrap, as well as an identifier on its shipping label.

C.3 Label Specifications

The unique password will consist of at least 10 alphabetic uppercase characters. To avoid confusion, the provided passwords will not include any lowercase alphabetic characters or numbers.

One password label will be located near the BMC chip and/or close to the motherboard serial number label. Do not remove this label. The other label will be placed on the CPU1 socket cover. This label may be removed and placed in another location, such as on the side of the chassis or a service tag.

Most systems have a pull-out tag to display the BMC MAC address and the preprogrammed unique password. The rest of the systems will have the sticker on the top/front of the chassis.

Figure C-1: Label Location on the BMC Chip

Figure C-2: Label Locations on Motherboard PCB and the Cover of CPU1

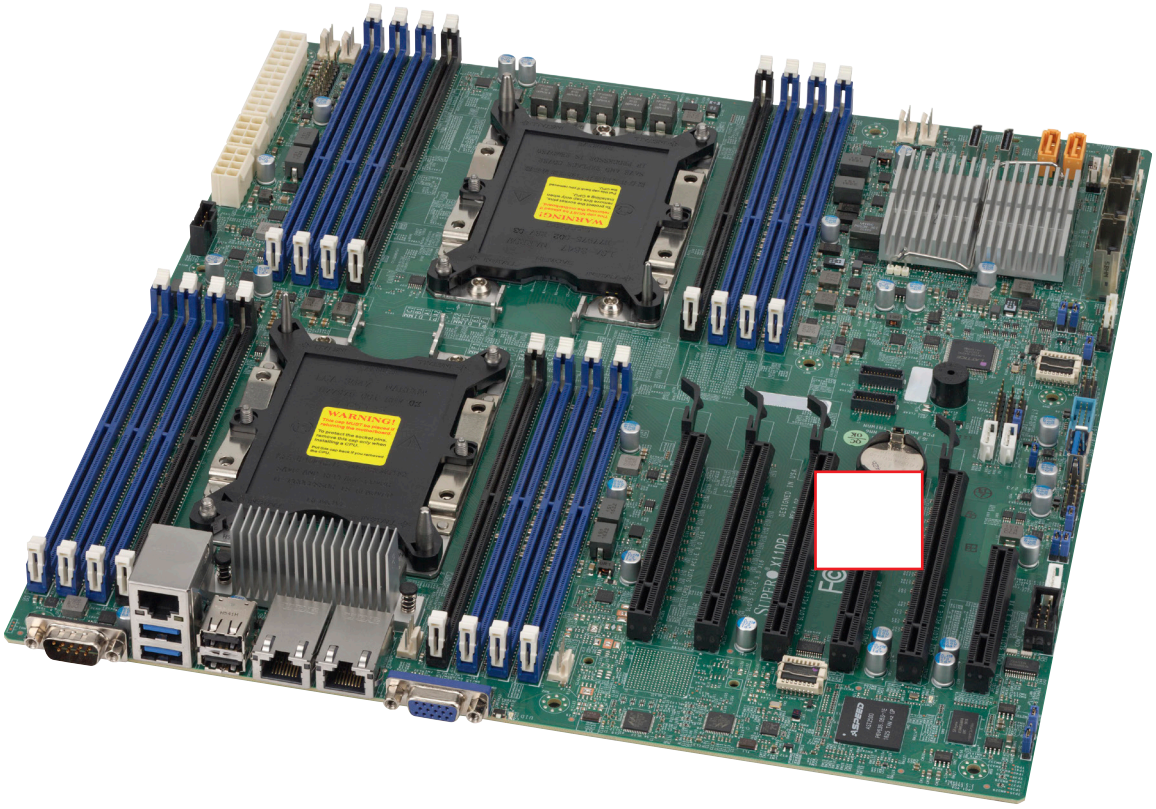


Figure C-3: Label Locations on Motherboard PCB and the Cover of CPU1

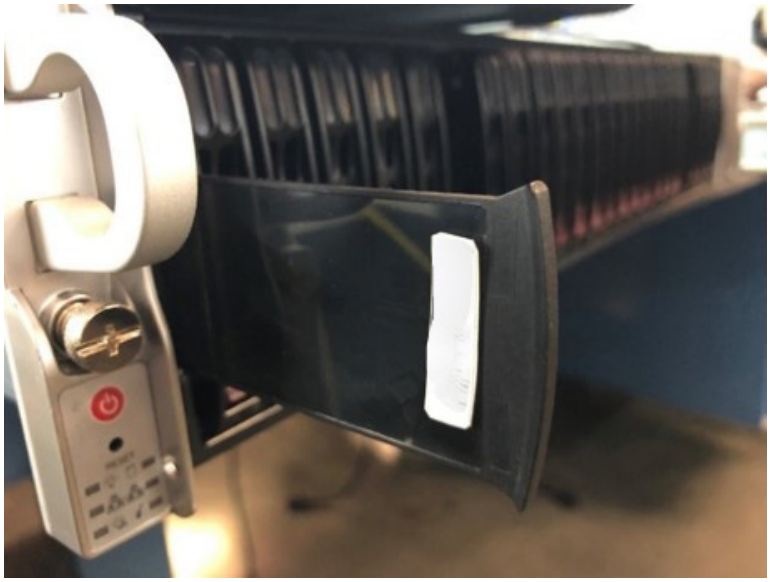


Figure C-4: Label on the Opposite Side of the Service Tag

Figure C-5: Label on the Opposite Side of the Service Tag

Figure C-6: Label On the Opposite Side of the Service Tag

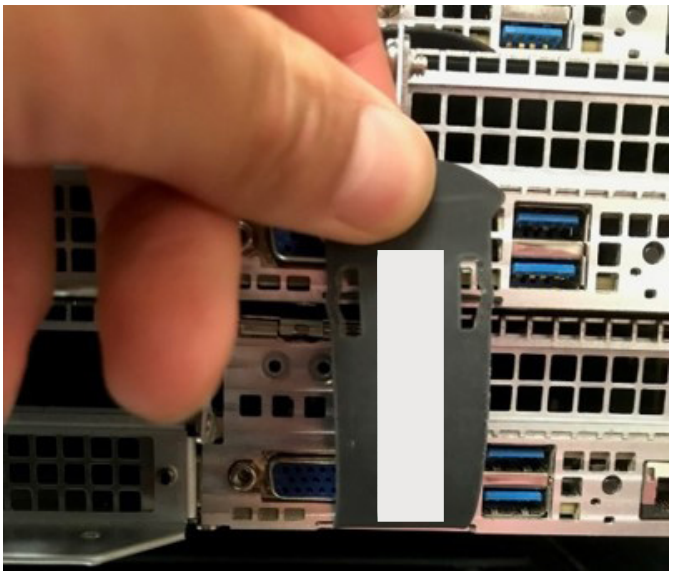


Figure C-7: Label On the Opposite Side of the Service Tag

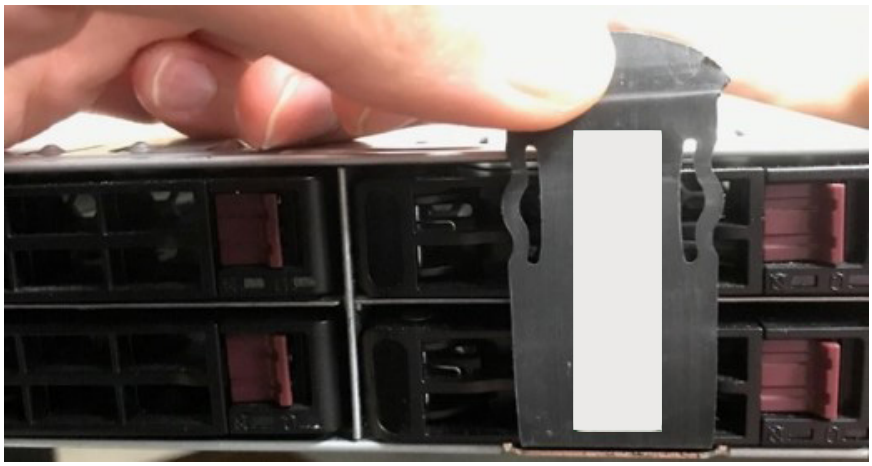


Figure C-8: Label on the Opposite Side of the Service Tag

Figure C-9: Label Location on the Chassis

C.4 Restore Factory Default

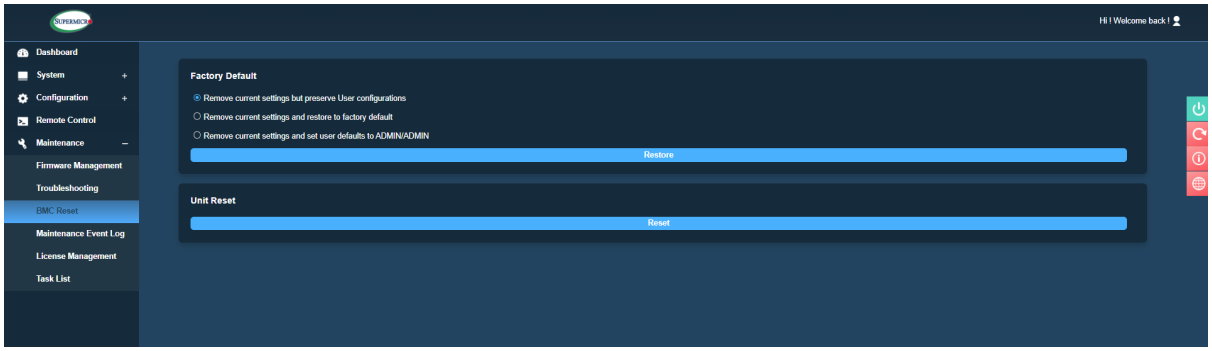


Figure C-10: Factory Default Page

You can select the following options to restore BMC to the factory default settings:

- Remove current settings but preserve user configurations: This option will restore all configurations to factory default and preserve all user configurations.
- Remove current settings and restore to factory default: This option will restore all the configurations to factory default. It will remove all users and reset the ADMIN user password to the factory default password.
- Remove current settings and set user defaults to ADMIN/ADMIN: This option will restore all the configurations to factory default. It will remove all users and reset the ADMIN user password to ADMIN.

C.5 Change All Unique Passwords Using Script

Due to possible different operating environments, you are given the option to modify the provisioning script and unique passwords.

C.6 Frequently Asked Questions

Question: What if a password sticker is lost? How do I get my unique password?

Answer: There is a minimum of two stickers on each product. One sticker will be placed on the motherboard, and a second sticker will be on the server chassis. At this time, Supermicro has not encountered any instances of lost or misplaced stickers. In the rare case of such incidents, contact the direct sales support to receive the soft copy of the password.

Question: What if the password stickers on the chassis and the motherboard are different?

Answer: If there is a discrepancy, use the motherboard sticker. The motherboard sticker is always correct.

Question: I purchased my products from a distributor. Can Supermicro provide me with soft copies of the unique preprogrammed passwords?

Answer: At this time, we only have the ability to provide soft copies to our direct customers. You will need to register your products to obtain soft copies of your passwords. For direct customers, use the Supermicro Customer Registration portal.

Question: Do you have a script that can change all unique passwords to my password?

Answer: We will provide a sample script with documentation. Of course, the operating environment may change from customer to customer. It is the end user's responsibility to modify the provisioning script.

Question: Will this law affect customers in Europe and Asia when shipments are from the Netherlands or Taiwan manufacturing facilities?

Answer: Since our standard SKUs will be rendered from California, we keep the same design across our portfolio, so it gives a unified experience across all platforms.

Question: Will customers purchasing Supermicro products from an OEM vendor be subject to the preprogrammed password initiative?

Answer: Yes, customers will still receive products with a unique preprogrammed password. You will be able to change the preprogrammed password yourselves, or you can work with your OEM vendor to make the necessary password updates.

Question: I am purchasing multiple systems for my data center. How do I change all of the unique preprogrammed passwords for these systems in an efficient manner to support my operations?

Answer: Contact the systems integrator (SI) or value-added reseller (VAR) to assist you in this process.

Question: Can Supermicro apply a single unique customer-specified password for all my systems? Will this comply with SB327?

Answer: All systems from Supermicro will ship with a unique preprogrammed password. Customers will be able to change the password on each system. In order for Supermicro to comply with SB327, we are not able to use customer-specified passwords. All passwords will be unique and assigned at the time of manufacturing.

Question: When will my motherboard have this change rolled out?

Answer: Supermicro plans to have new stickers rolled out starting mid-December 2019.

Appendix D

Remote Attestation

D.1 Overview

Supermicro trusted supply chain assurance offers to verify the identity of the Supermicro server that is received by the customer matches with what Supermicro has manufactured. The IT administrator and security teams can confidently deploy servers in data centers after validating the servers manufactured by Supermicro and unexpected modifications have not occurred during the journey from Supermicro to data centers.

To ensure smooth Day One operation, it is highly recommended that your systems be verified using Supermicro's system attestation process. Attestation will detect any changes in the composition of your hardware and firmware through cryptographic signing, thereby guaranteeing the state of your server, while identifying and reporting any unauthorized changes.

D.2 License Requirements

An Enterprise SFT-SDDC-SINGLE license is required to perform attestation. You may inquire about this license through your Supermicro sales representative.

D.3 Attest Your System Using the Supermicro Website

Follow these steps to attest your system:

1. Run Supermicro Update Manager (SUM) to create a measurement file containing your current system configuration. Use the following command to get the measurement dump from your system.

```
sum -i <BMC IP> -u <BMC_USER> -p <BMC_USER_PASSWORD> -c Attestation
--dump --file <MEASUREMENT_FILE>
```

2. Log in to the Attestation Portal at https://www.supermicro.com/attestation.

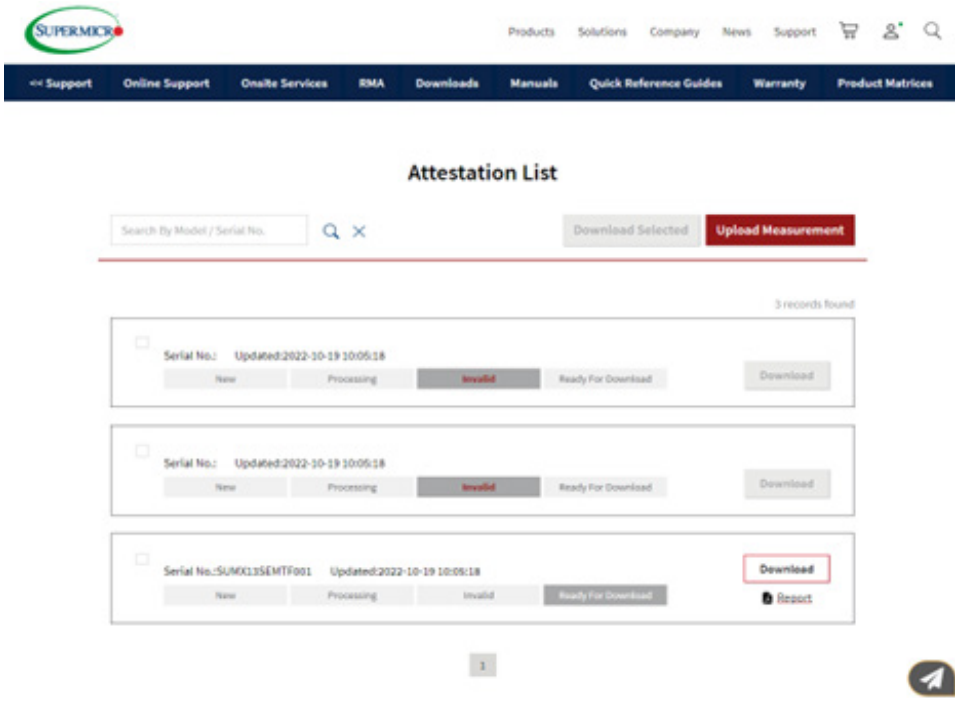


Figure D-1: Attestation Portal

3. Upload the measurement file obtained in step 1 to the Measurement Validation Server, which will compare the configuration to Supermicro's reference manifest file.

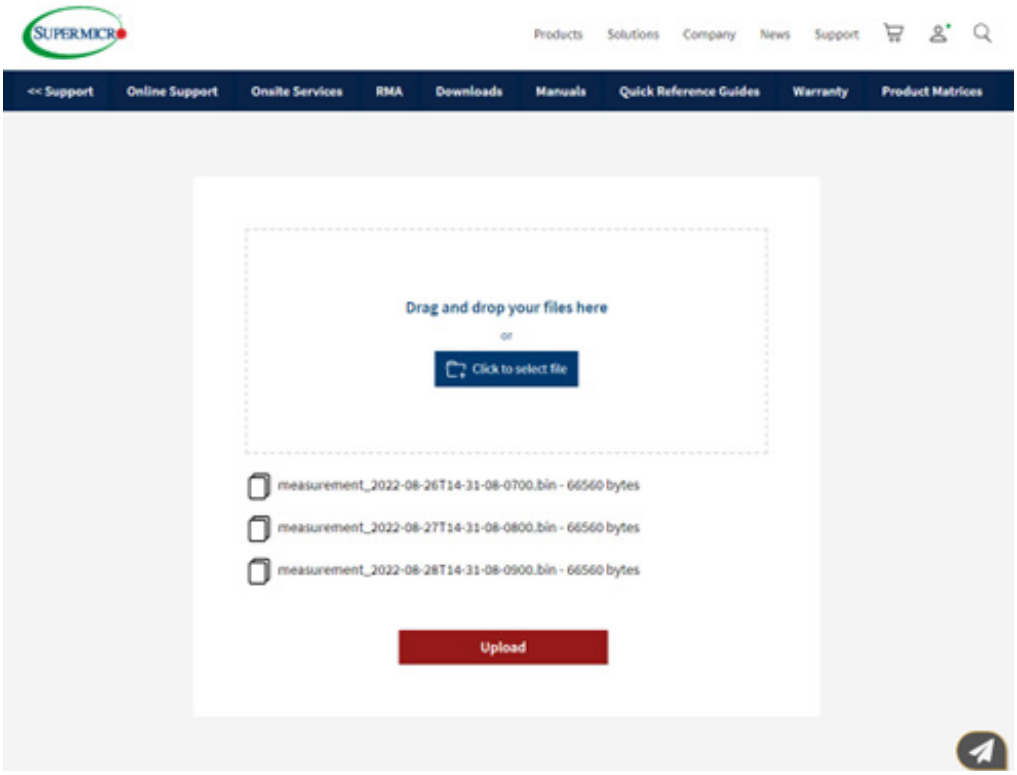
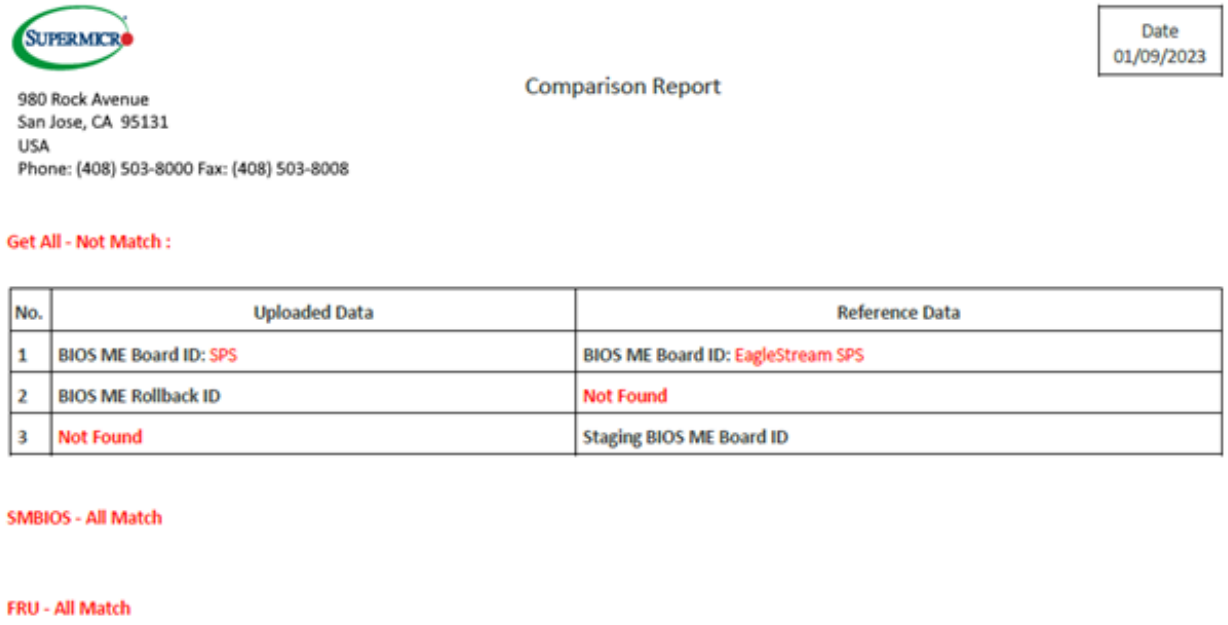


Figure D-2: Measurement Validation Server

4. Download the verification report that compares the uploaded measurements with Supermicro's reference manifest. The verification report includes:

   - System components
   - Firmware
   - FRU



980 Rock Avenue
San Jose, CA 95131
USA
Phone: (408) 503-8000 Fax: (408) 503-8008

Comparison Report

Date
01/09/2023

Get All - Not Match :

No.	Uploaded Data	Reference Data
1	BIOS ME Board ID: SPS	BIOS ME Board ID: EagleStream SPS
2	BIOS ME Rollback ID	Not Found
3	Not Found	Staging BIOS ME Board ID

SMBIOS - All Match

FRU - All Match

Figure D-3: Sample Report

In addition to an interactive web interface, you may also use the Attestation RESTful API to automate the process using your own script.

D.4 Attest Your System Using RESTful APIs

Bearer Authentication

Token Generation

Users need to generate the bearer token from https://www.supermicro.com/attestion using a web browser. Tokens expire after 60 minutes.

User of Token

There should be generated tokens included in the API request header.

API Calls

Refresh Tokens

To refresh the token data, utilize the following:

Method: GET

End Point: https://rots.supermicro.com/api/v1/attestation/refreshtoken

Request Params: None

Sample query: https://rots.supermicro.com/api/v1/attestation/refreshtoken

List of Attestation Data

To query all attestation data by pagination, utilize the following:

Method: GET

End Point: https://rots.supermicro.com/api/v1/attestation

Request JSON: (Optional)


```
{
  "pagination": {
    "offset":20,
    "limit":10,
    "order_by":"serial_no",
    "asc_desc":"desc"
  }
}
```


Figure D-4: Data Sample

Response JSON: Users need to generate the bearer token from https://www.supermicro.com/attestion using a web browser before using these RESTful APIs.


```
{
  "data":[
    {
      "uuid":"163690ab-749e-4dd2-bbbd-
      41c10d8befc8",
      "upload_name":"measurement.bin",
      "serial_no":"SUMX13SEMTF001",
      "status":"Ready for Download",
      "ref_manifest_base64":"....",
      "report_log_base64":"....",
      "last_updated":"2022-10-13 19:55:40"
    }
  ],
  "pagination":{
    "offset":20,
    "limit":10,
    "order_by":"last_updated",
    "asc_desc":"desc"
  }
}
```


Figure D-5: Bearer Token Sample

Query Attestation Data

To query individual Attestation Data by UUID or serial number, utilize the following data. You may attest an entire system and/or motherboard by using the appropriate serial number. The report is base64 encoded and must be decoded before use.

Method: GET

End Point:

https://rots.supermicro.com/api/v1/uuid/{uuid}

https://rots.supermicro.com/api/v1/sn/{sn}

Request JSON: None

Response JSON:

Upload Attestation Data

To upload base64-encoded measurement file to query and validate against RoTS, utilize the following:

Method: POST

End Point:

https://rots.supermicro.com/api/v1/upload

Request JSON:

Figure D-6: Data Sample

Response JSON:


```
{
  "data": [
    {
      "upload_name":"measurement1.bin",
      "uuid":"163690ab-749e-4dd2-bbbd-
      41c10d8befc8",
      "status":"New",
      "last_updated":"2022-10-13 19:55:40"
    },
    {
      "upload_name":"measurement2.bin",
      "uuid":"193690ab-749e-4dd2-bbbd-
      41c10d8becs3",
      "status":"New",
      "last_updated":"2022-10-13 19:55:36"
    },
    {
      "upload_name":"measurement3.bin",
      "uuid":"188690ab-749e-4dd2-bbbd-
      41c10d8be111",
      "status":"Processing",
      "last_updated":"2022-10-13 19:55:32"
    }
  ]
}
```


Figure D-7: Response JSON Sample

(Disclaimer Continued)

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.