



**BMC**

Baseboard Management Controller  
Designed for the X13 and H13 Series

**USER'S MANUAL**

Revision 1.0

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](http://www.supermicro.com).**

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

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

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

FCC Statement: This equipment has been tested and found to comply with the limits for a Class 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](http://www.dtsc.ca.gov/hazardouswaste/perchlorate)".



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

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

Manual Revision 1.0

Release Date: December 21, 2022

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

Copyright © 2022 by Super Micro Computer, Inc.  
All rights reserved.

**Printed in the United States of America**

# Preface

## About This Manual

This manual is written for system integrators, IT technicians, and knowledgeable end users 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, please 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.

## 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](http://www.supermicro.com)

### Europe

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

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: Sales\_Europe@supermicro.com (General Information)  
Support\_Europe@supermicro.com (Technical Support)  
RMA\_Europe@supermicro.com (Customer Support)

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

### Asia-Pacific

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

Tel: +886-(2) 8226-3990

**Asia-Pacific**

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

# Table of Contents

## **Chapter 1 Introduction**

1.1 Introduction to the BMC Platform.....	9
1.2 Overview of the ASPEED AST2600 BMC.....	9
1.3 Supermicro BMC Features.....	10
1.4 Software Licenses Available.....	13
1.5 Special Notes for Motherboard and Firmware Support .....	17

## **Chapter 2 Configuring the BMC Settings**

2.1 Configuring UEFI BIOS .....	18
2.2 Connecting to the Remote Server.....	29
2.3 Accessing the Remote Server Using the Browser.....	30
2.4 BMC Dashboard.....	31
2.5 System.....	36
2.6 Configuration .....	67
2.7 Remote Control .....	112
2.8 Maintenance .....	145

## **Chapter 3 Frequently Asked Questions**

### **Appendix A Firmware Update via WEB GUI and SUM**

A.1 Overview.....	188
A.2 Updating Firmware Using BMC WEB GUI.....	189
A.3 Updating Firmware Using SUM.....	197

### **Appendix B Introduction to SMASH**

B.1 Overview.....	201
B.2 An Important Note to the User.....	202
B.3 Using SMASH .....	202
B.4 Initiating the SMASH Protocol.....	203
B.5 SMASH-CLP Main Screen .....	204
B.6 Using SMASH for System Management.....	205
B.7 Definitions of Commands Verbs.....	206
B.8 SMASH Commands .....	208
B.9 Standard Command Options.....	209
B.10 Target Addressing .....	210

***Appendix C Unique Password for BMC***

C.1 Overview.....211

C.2 Notice and Shipping Label Identifier .....212

C.3 Label Specifications .....214

C.4 Restore Factory Default .....220

C.5 Change All Unique Passwords Using Script.....220

C.6 Frequently Asked Questions .....221



# 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 the Platform Controller Hub (PCH) to other onboard components, providing a remote network interface via 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 via 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 via PCI Express connections to communicate with the graphics core for the X13 series motherboards. Designed for the X13 series, the AST2600 connects with the host system via PCI Express Gen2 x1 bus to communicate with the graphics core. 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 and provides LPC interface support to control Super IO functions. ASPEED AST2600 includes Keyboard/Video/Mouse Redirection (KVMR). The BMC is connected to the network via 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 via PC.

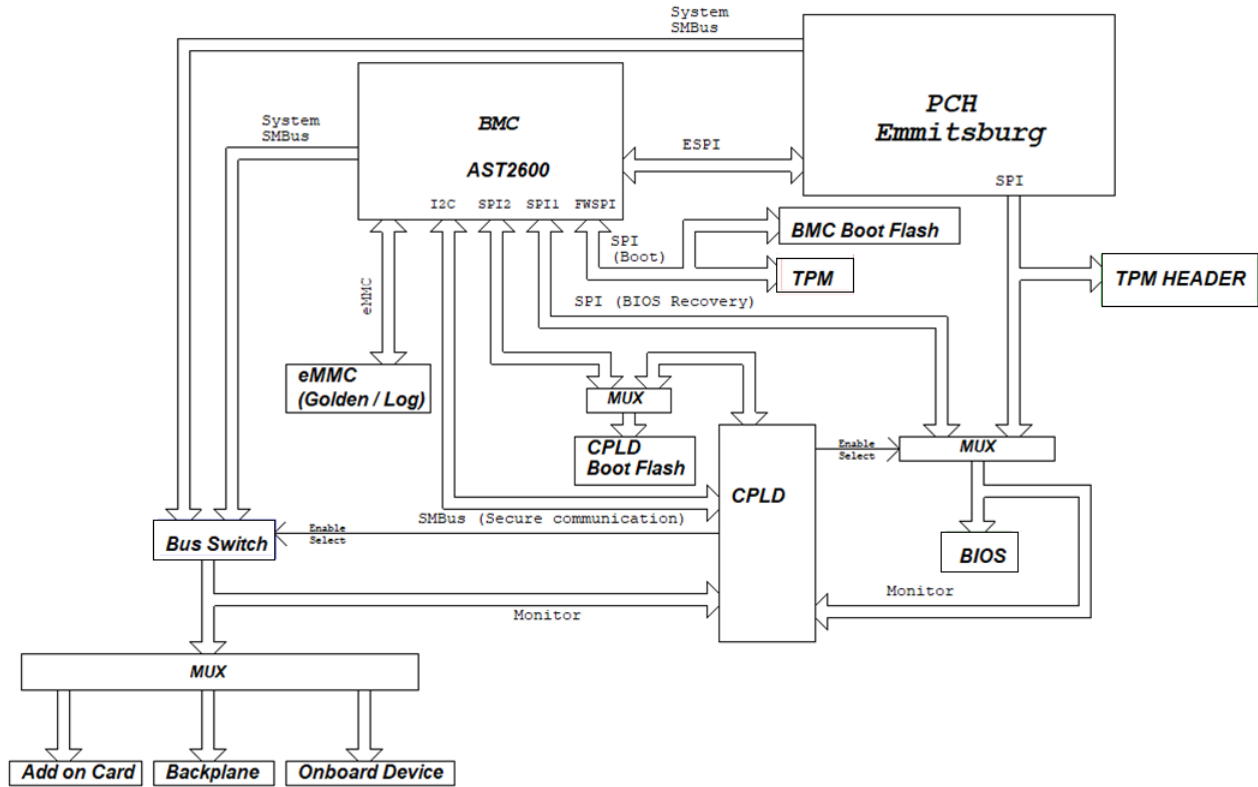
## 1.3 Supermicro BMC Features

- 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 display on the main page
- Out-of-band management through shared or dedicated LAN
- Option to change LAN connection interface at Runtime
- VLAN
- RMCP & RMCP+ protocols supported
- SMASH/CLP
- Secure command line interface (SSH) and Telnet
- RADIUS authentication support
- Secure browser interface (Secure socket layer - SSL 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 browser and OS
- OS-indentation
- KCS Privilege Control
- Unique pre-programmed password
- Redfish

## AST2600 Block Diagram

The following diagram represents a typical system setup for the AST2600 controller.



## 1.4 Software Licenses Available

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



**Warning:** Changing the MAC addresses will invalidate the Software License Keys activated in the system.

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

This license covers features such as UEFI BIOS/BMC firmware update and configuration, basic Redfish APIs, mounting ISO images, and asset info.

- SFT-DCMS-Single: Data Center Management Suite (Advanced)

This license covers all features in OOB as well as additional enterprise features. Features such as RAID Management, Advanced Redfish APIs, NIC FW management, and enabling Supermicro Server Manager (SSM) to manage and monitor Supermicro servers from a single console view.

Please refer to the following comparison chart for more info on what features are covered by these licenses.

(\*) 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) supported 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	✓	✓	✓
HW Root of Trust	✓	✓	✓
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 (3 users)	✓	✓	✓
Remote Keyboard Operation	✓	✓	✓

Temperature monitoring	✓	✓	✓
Real-time power reading	✓	✓	✓
Power thresholds & 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 via BIOS setup	✓	✓	✓
System Component Inventory	✓	✓	✓
Auto-Discovery (Via SSM web)			✓
Remote OS deployment (Via 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 (Via SMCIPMI-Tool)	✓	✓	✓
License Management	✓	✓	✓
Post Snooping	✓	✓	✓

Additionally, the following single-feature software licenses are available and can be used along with SFT-OOB-LIC and SFT-DCMS-Single.

- **SFT-SDDC-SINGLE**: Software-Defined Data Center Enterprise Management  
This license enables SuperCloud Composer to manage large data centers. This includes coordinating automated lifecycle management, software-defined infrastructure, and more in a single management frame.
- **SFT-DCMS-SVC-KEY**: Data Center Management Suite Service  
This license enables SSM Call-Home Support for automatic support ticket entry.
- **SFT-SPM-LIC**: Advanced Power Management  
SPM enables real-time power monitoring and managing system power in Supermicro servers with the Intel Node Manager enabled.

For more information about the Supermicro System Management Software, please refer to our website at <https://www.supermicro.com/en/solutions/management-software/>.



## 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, please refer to our website at <https://www.supermicro.com/en/solutions/management-software> for details.

Please refer to the motherboard product page at [www.supermicro.com](http://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 Supermicro's website at [https://www.supermicro.com/support/resources/bios\\_ipmi.php?type=BMC](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 X13 motherboard as a few newer features are not supported by this generation.

### 2.1 Configuring UEFI BIOS

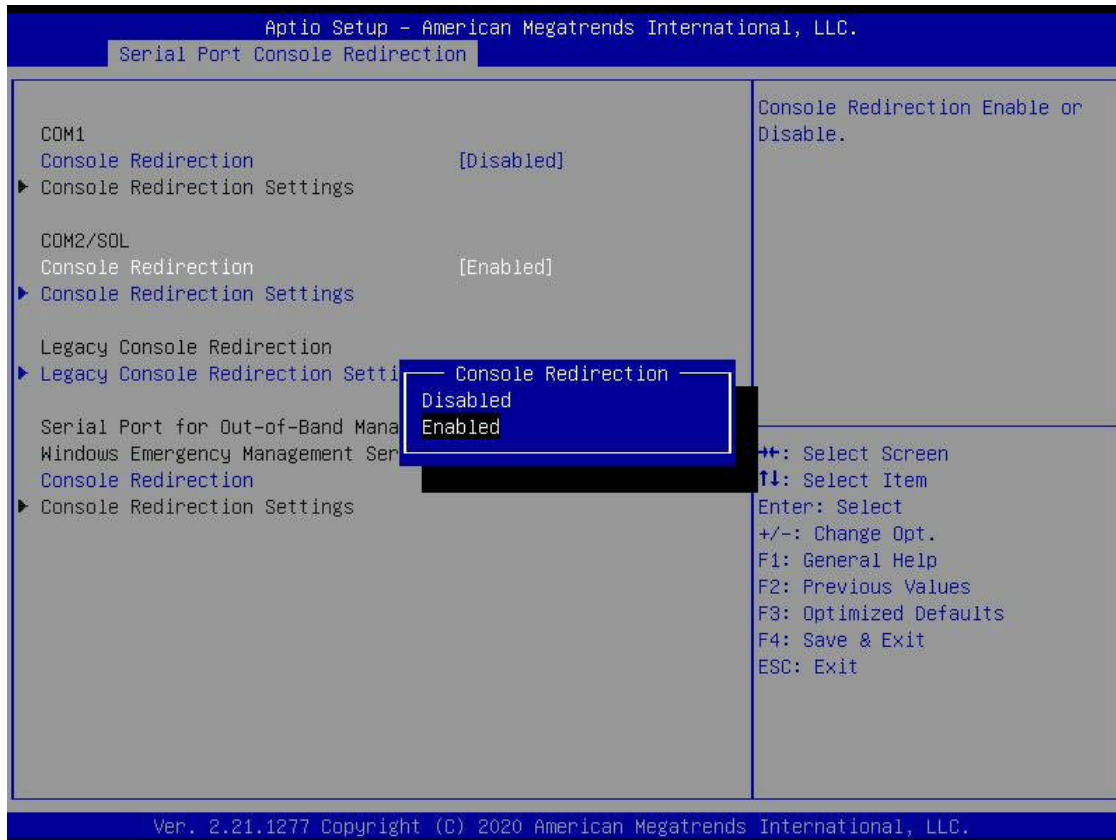
Before configuring the BMC, follow the instructions below to configure the system UEFI BIOS settings.

#### 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 go back to previous screens, press <Esc>.

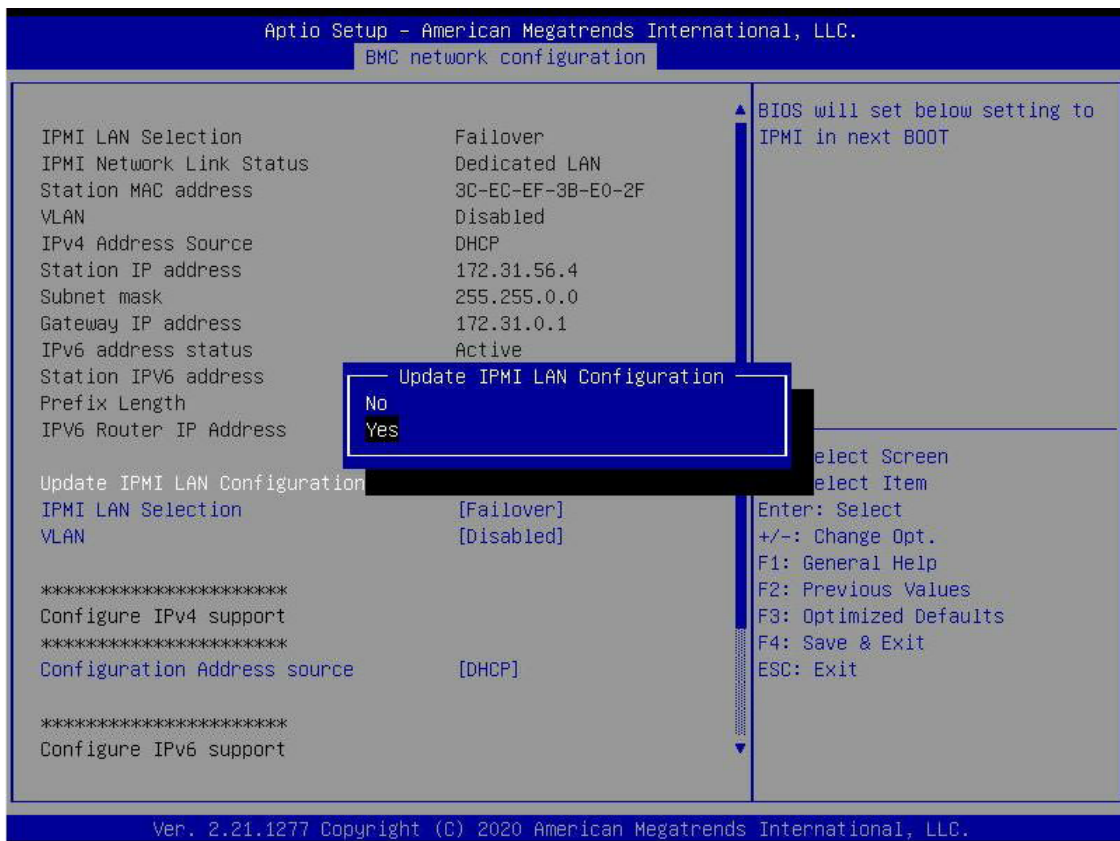
## Enabling the COM port for SOL (BMC)

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

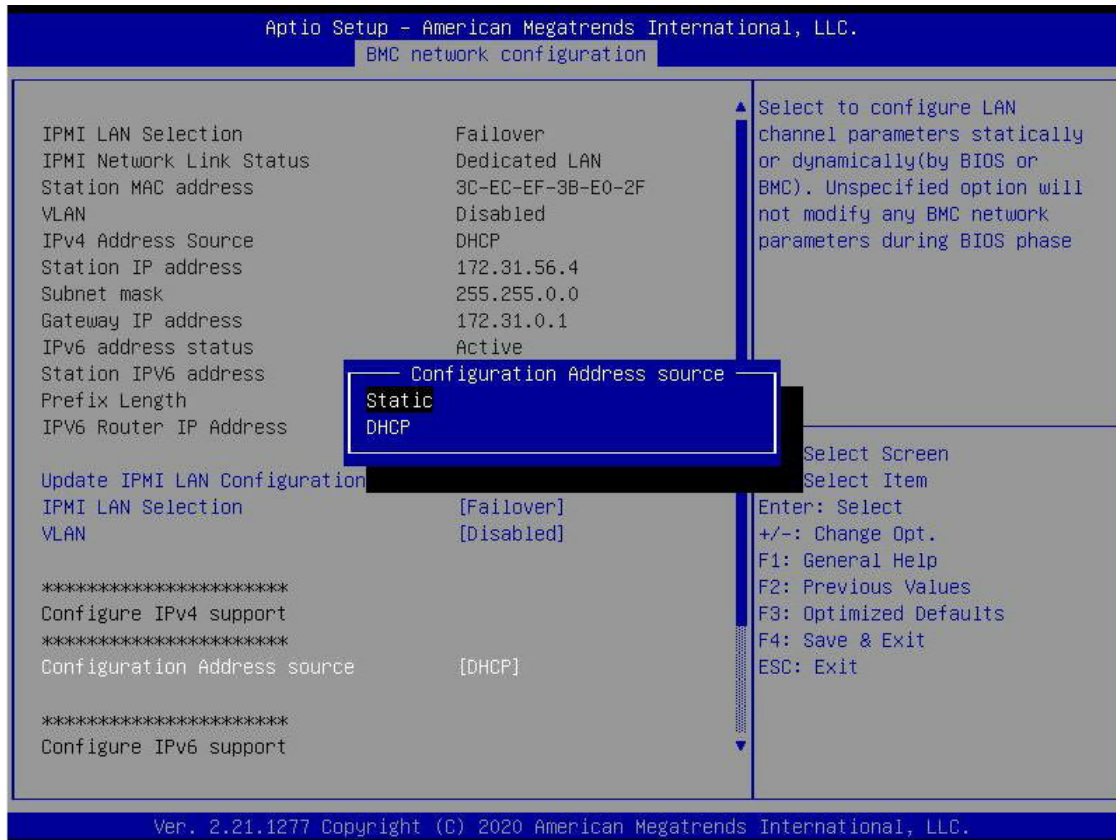


## Configuring IP Address Using the UEFI BIOS

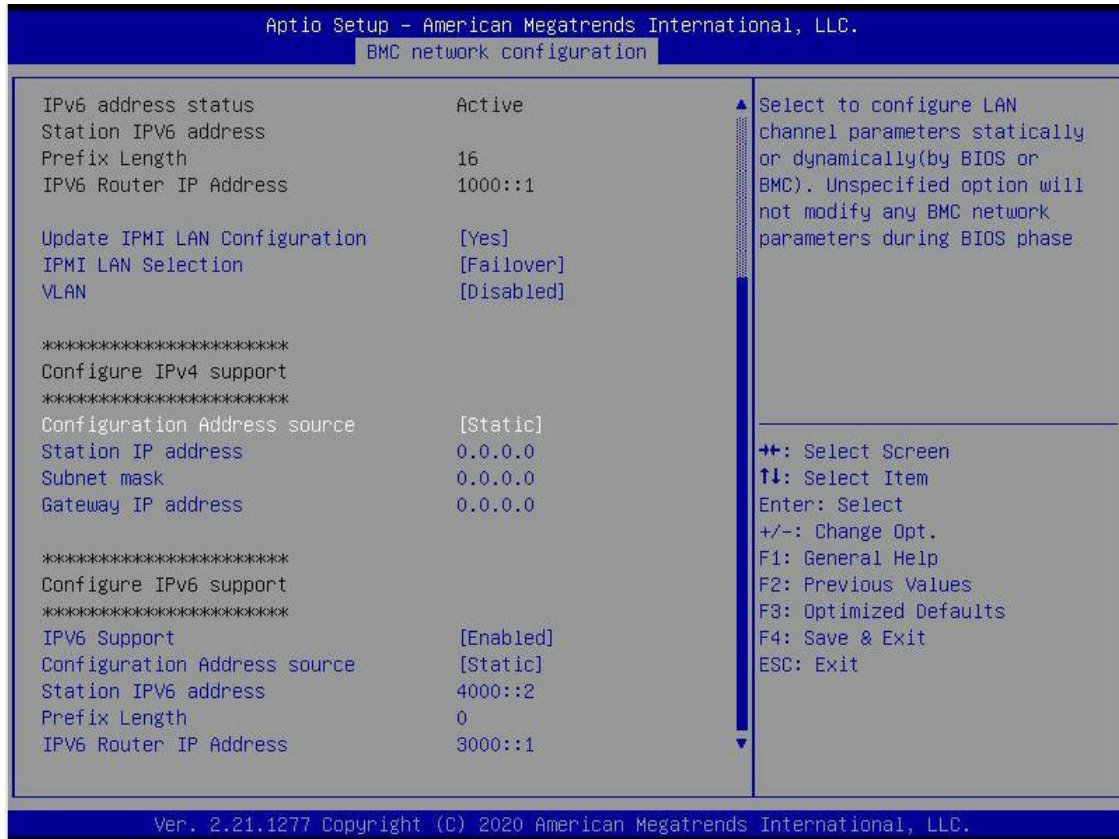
1. Select the *Server Management* tab.
2. Select *BMC Network Configuration*.
3. Press <Enter>.
4. Highlight *Update IPMI LAN Configuration*.
5. Press <Enter>.
6. Select [Yes].



7. Highlight *Configuration Address Source* and select [Static].



- 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, which indicates that these fields are ready for you to change to new values. Select each of the three items and enter the values. Press <Enter> when finished.

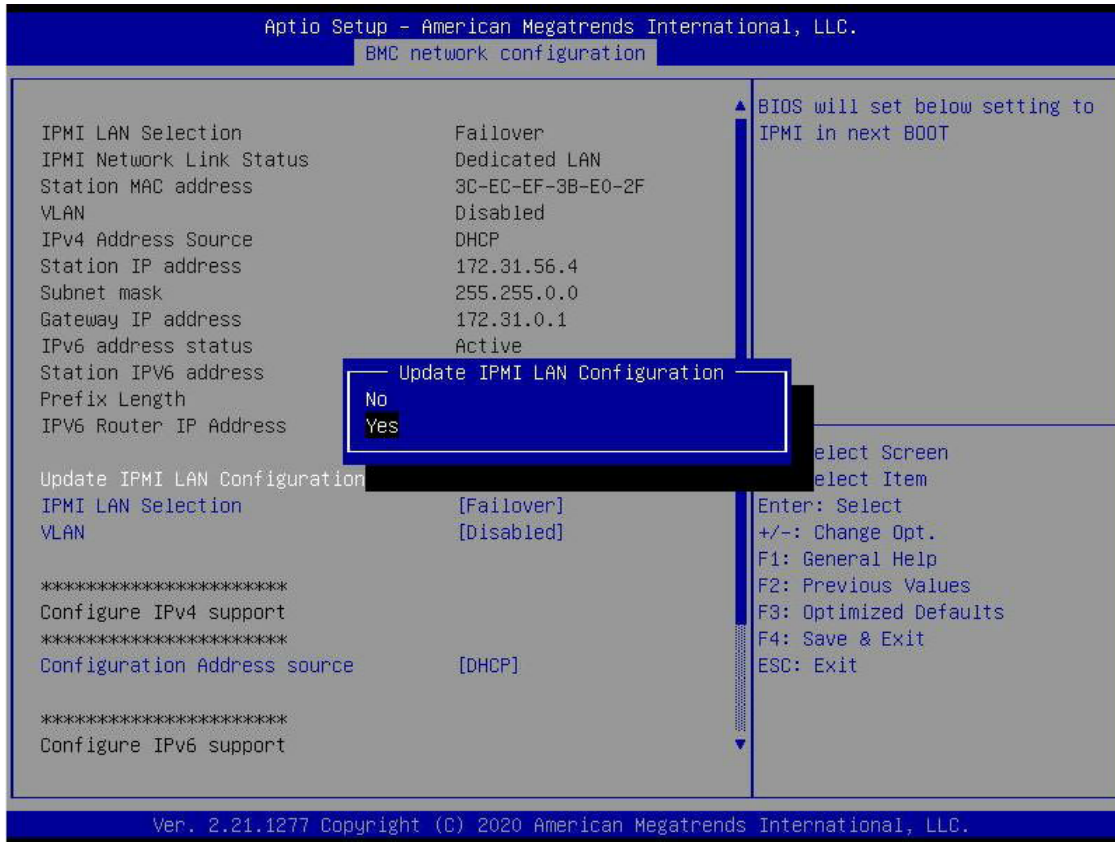


## Connecting to BMC Using the UEFI BIOS

1. To bring up the BIOS menu, connect one end of an Ethernet Cat 5 to the Ethernet port of the laptop or device being used.
2. Plug the other end of the cable into the IPMI / SHARED port of the server.
3. Power on the server by pressing the DEL key to enter the BIOS menu.
4. In the BIOS menu, follow the instructions below 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. Use the arrow key to navigate to *Server Management*.
6. Select *BMC Network Configuration*.

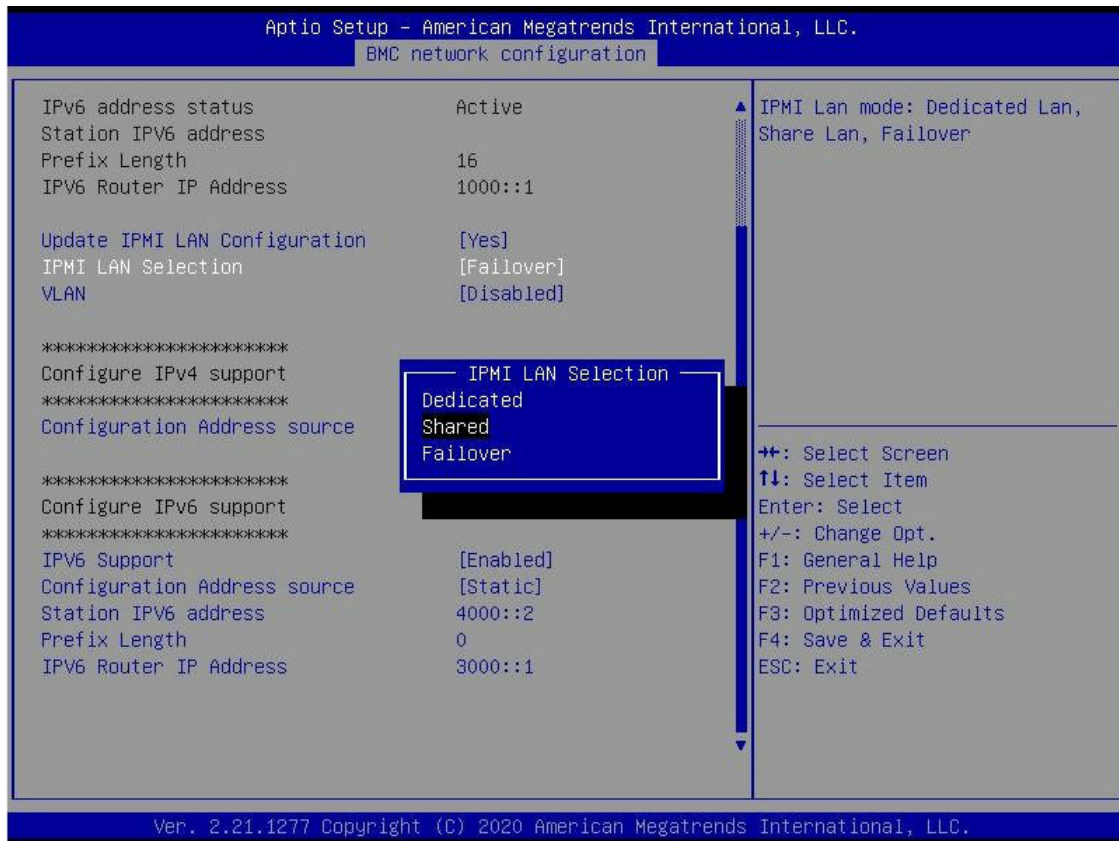


7. Select *Update IPMI LAN Configuration* and select [Yes].

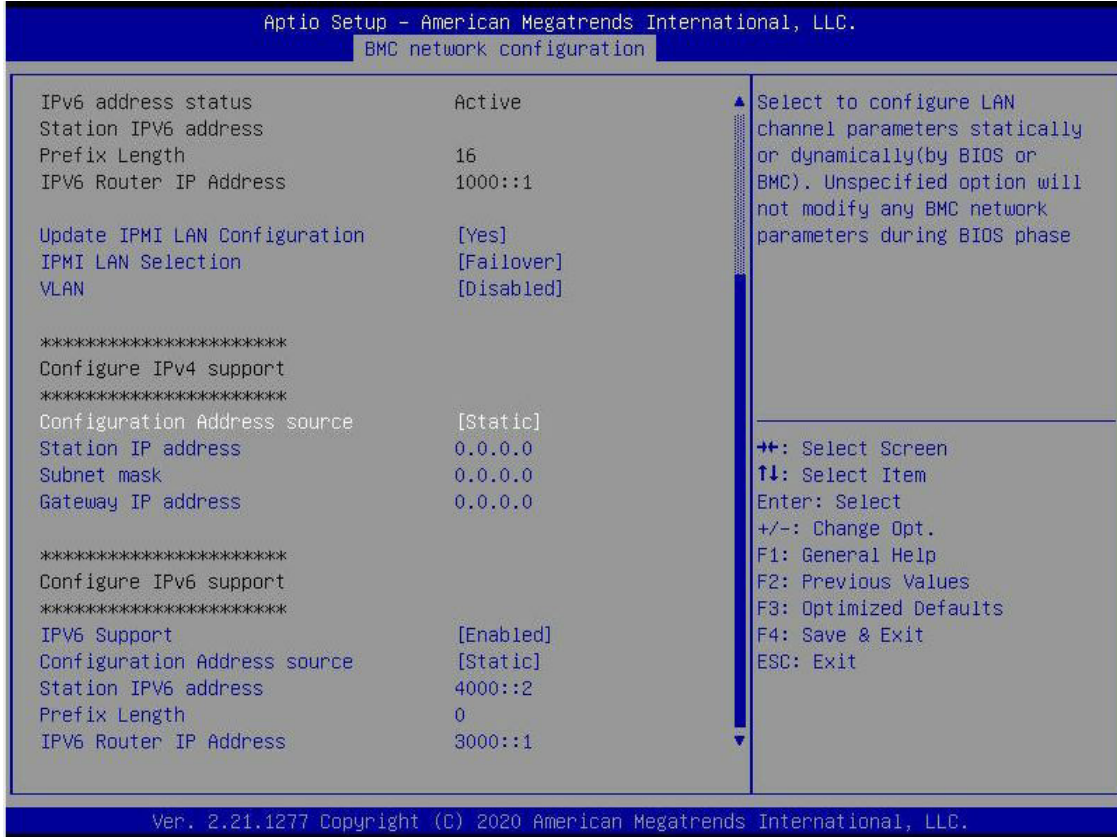




8. Navigate to *IPMI LAN Selection*, and you will see three options as shown below. Select [Shared].

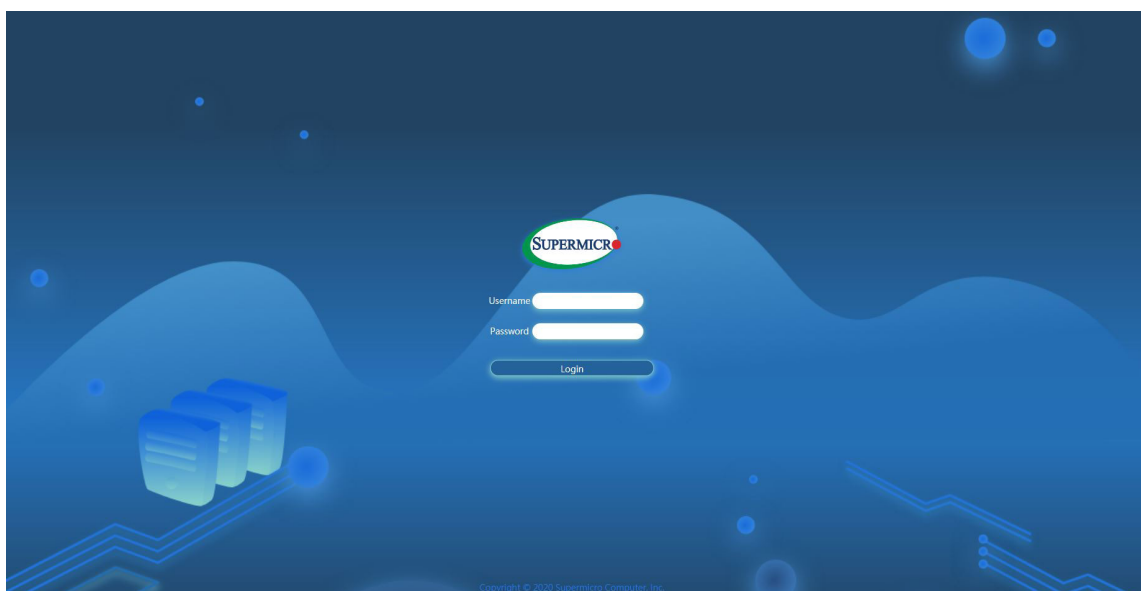


- Navigate to *Configuration Address Source* and select [Static]. Then you can assign an IP (such as 192.168.0.4) and subnet.

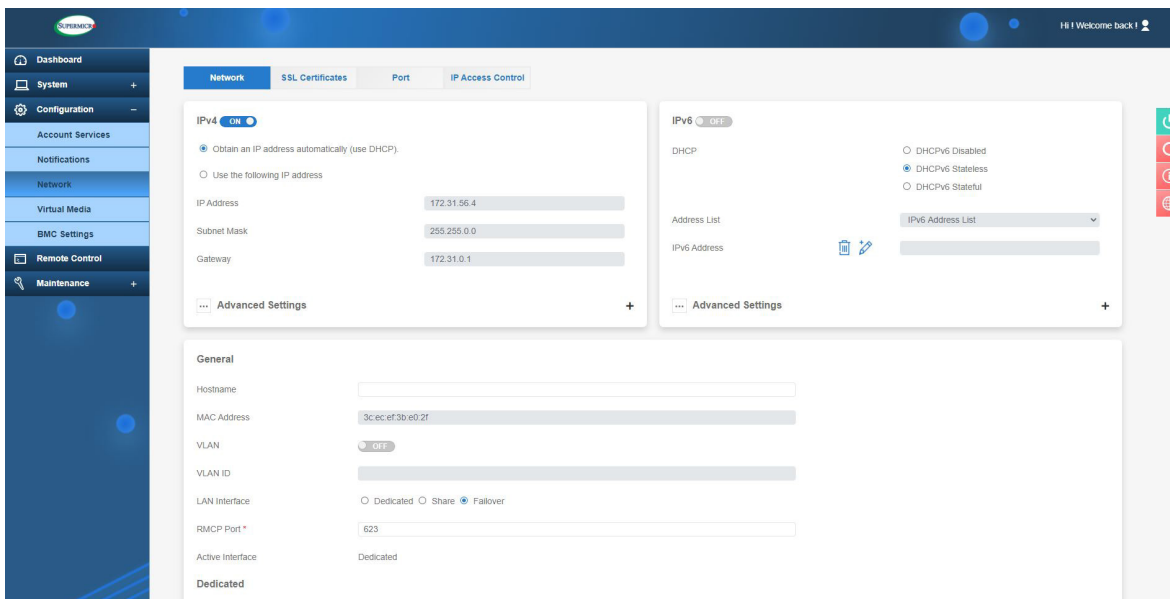


Now that both the laptop and BMC are on the same subnet. With the static IP connected, you should be able to communicate. To establish the connection, please follow the steps below.

1. Keep the terminal of the Windows/Laptop. Ping the IPMI IP, 192.168.0.4, and make sure that it is pingable.
2. If it is pingable, open a web browser on the laptop. Enter the IP in the URL bar, and the login screen will appear as shown below.
3. Enter the username, ADMIN, and a BMC unique password. Please refer to Appendix D on how to retrieve the BMC unique password.



4. After logging in, go over to <Network> under <Configuration>. You can then see all the IPv4 and IPv6 info to configure.



## 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 as shown on the next page will display.

## 2.3 Accessing the Remote Server Using the Browser

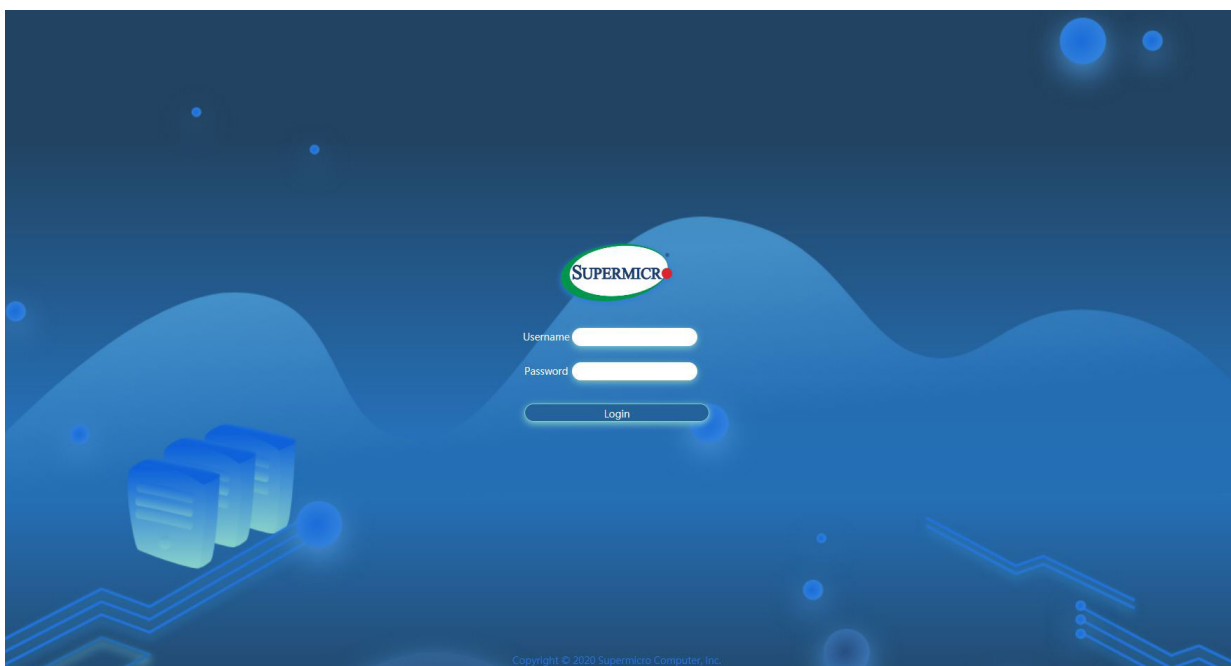
### To Log In to the Remote Console

Login 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. Users can view the hidden password by clicking on the eye icon. Once connected to the remote server via browser, the following BMC login screen will display.



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

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



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.

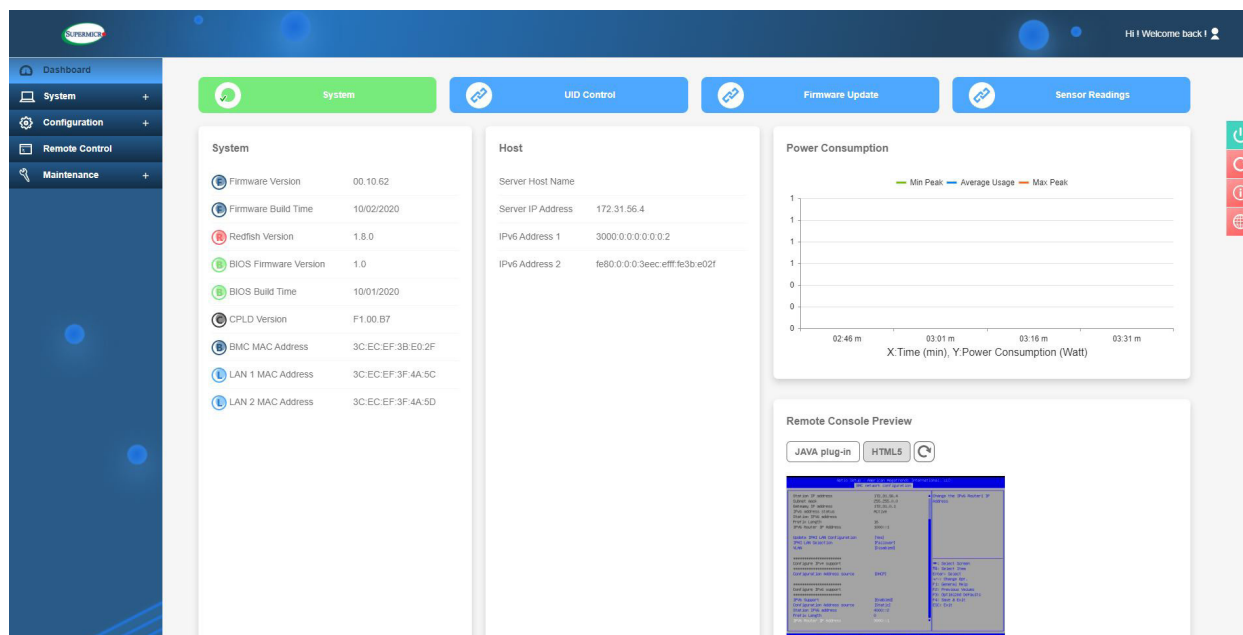


**Note 1:** To use the IPMIView utility for Console Redirection, please refer to the IPMI-View User's Guide for instructions.

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

## 2.4 BMC Dashboard

The BMC Dashboard provides an overview of the System, Host Information, Power Consumption, and System Health. Users can also access quick links to System, Storage, 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. This page will be displayed as shown below.



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



Information includes:

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

 **Note:** Action of power on and off will happen automatically. When the system is currently powered down (therefore not "on"), you can see and only choose the [Power ON] option. If the system is currently powered up (therefore is "off"), you will be able to see the [Reset] and [Off] options.

## Refresh

You can click on refresh to retrieve the latest update for the respective page.

## Help

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



## Language

You can select different languages from the pop-up window.

- English
- Simplified Chinese
- Japanese

The BMC Main displays 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 navigate to the System page.
- Storage: You can navigate to the Storage page if a storage component is connected.
- UID Control: To identify the server, users can click the UID icon to navigate to the UID control component to turn ON or OFF the blinking LED.
- Firmware Update: You can navigate to the Firmware Management page to update the firmware.
- Sensor Readings: You can 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 health 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 the health of one or more components is critical.

## Storage Health


In this section, users can find overall storage component health and notification if a storage component is connected and is detected as well as if the HOST is powered on. Click on the health status to get more details about a drive or controller's health. Symbols indicating the health 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 the health of one or more components is critical.

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


## System

The System frame displays brief summary of system components such as Firmware version, Firmware Build Time, Redfish Version, BIOS Firmware Version, BIOS Build Time, CPLD Version, BMC MAC Address, and LAN MAC Addresses.

 **Note:** In special motherboards without onboard LANs, AOC NIC information is displayed in place of onboard LANs. Additionally, no System LAN interfaces will be shown if LAN interfaces are not detected.

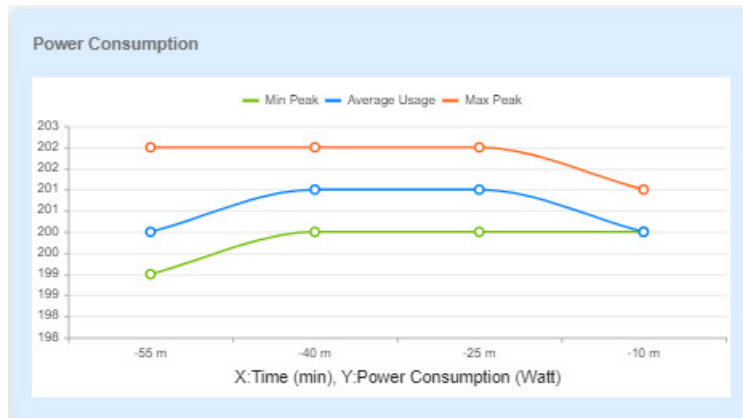
## Host

This section 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 the configuration in the Network Configuration.

## Power Consumption

This section displays a graphical representation of the system power consumption with time. 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. Click on settings to change 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.

## Recent Logs

This section displays the latest health event log entries.

## 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).

The screenshot displays the Super BMC System page. The interface includes a navigation sidebar on the left with options: Dashboard, System, Configuration, Remote Control, and Maintenance. The main content area is titled 'Overview' and features tabs for CPU, Memory, PSU, Power, Network, Sensor, Fan, and GPU. Below the tabs, there are six component health cards: UID Control (OFF), CPU, Memory, PSU, Sensor, and Fan, each with a green health indicator. A large 'Information' table provides system details:

Manufacturer	Supernovo
Product Name	X12DP-N(T)
Serial Number	
Power State	On
Host Name	
BMC IP Address	172.31.56.4
BMC MAC Address	3C EC EF 3B E0 2F
BMC Firmware Version	00.10.47
BIOS Firmware Version	1.0

Below the information table are four smaller sections: Chassis Info, FRU Device Info (Device ID: 0), Board Info (Language: English, Manufacturer: Supernovo), and Product Info (Language: English, Manufacturer: Supernovo).

### 2.5.1 Component Info

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



**Note:** Not all information on components 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 particular 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 details about the component.
  - **CPU** – This displays the overall health status of installed CPUs in the system. Issues that are occurred 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 are occurred in memory modules should not affect Sensor Health monitoring.

- PSU – This displays the overall health status of installed Power Supply Units in the system. Issues that are occurred in PSU units should not affect Sensor Health monitoring.
- Sensor – This displays the overall health status of the sensors present in the system.
- Fan – This displays the overall health status of installed fans in the system. Issues that are occurred in FAN units should not affect Sensor Health monitoring.
- Information: You can check detailed system information.
  - 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 SMCIPMITool utility and check detailed FRU information.
  - Device ID: You can view the System Device ID.
  - Chassis Info: The kind of chassis info displayed will depend on you the type of node system installed.

On Single-Node System, the following information will display for chassis info.

- Type – Chassis type detail
- Part Number – Chassis part number
- Serial Number – Chassis serial number

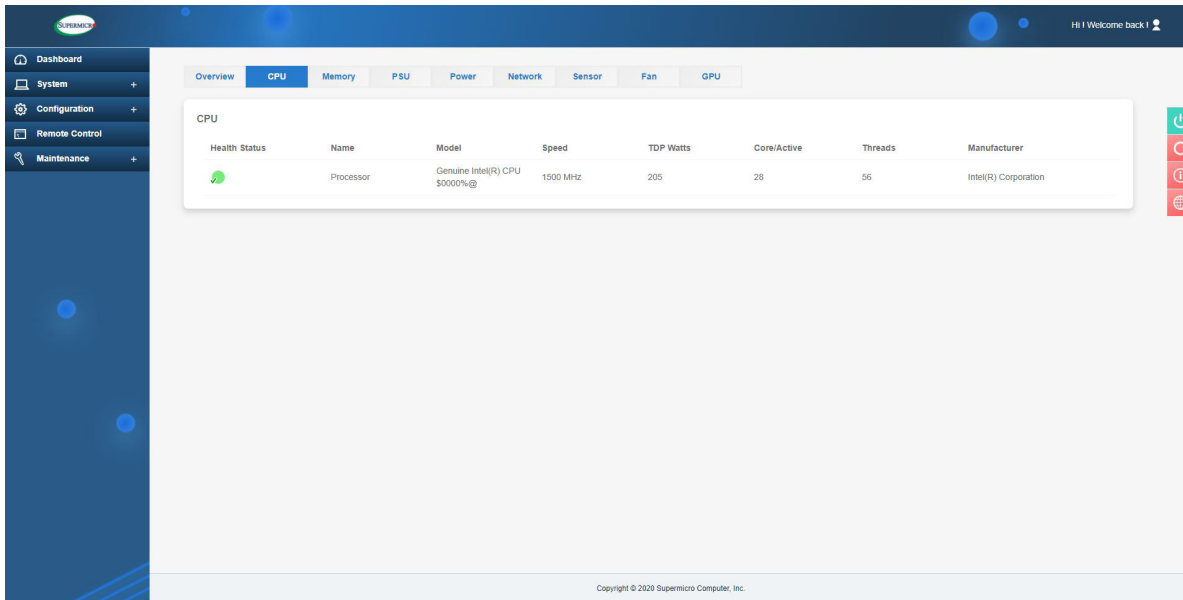
On Multi-Node System, the following information will display for chassis info.

- 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 the following information about each processor installed in the server.

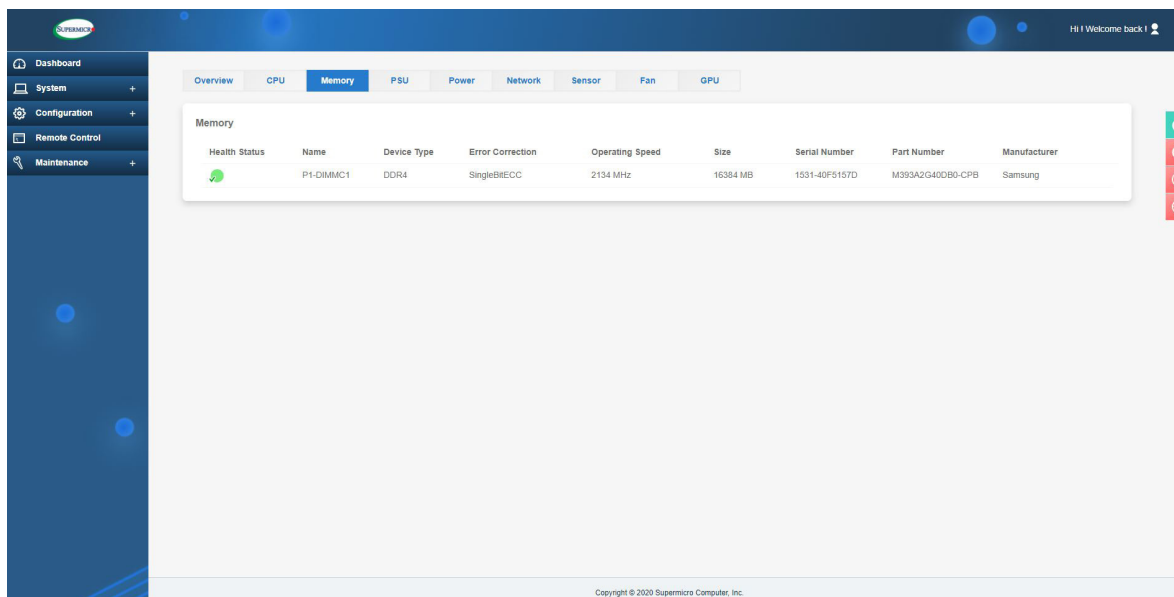


This page displays the following information.

- Health Status: You can view the health status of the CPU. It will include one of the following options.
  - Normal
  - Warning
  - Critical
- Name: You can view the name of the processor.
- Model: You can view 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 TDP (Thermal Design Power).
- Cores / Active: You can view the total 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 info.

## Memory

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



This page displays the following information.

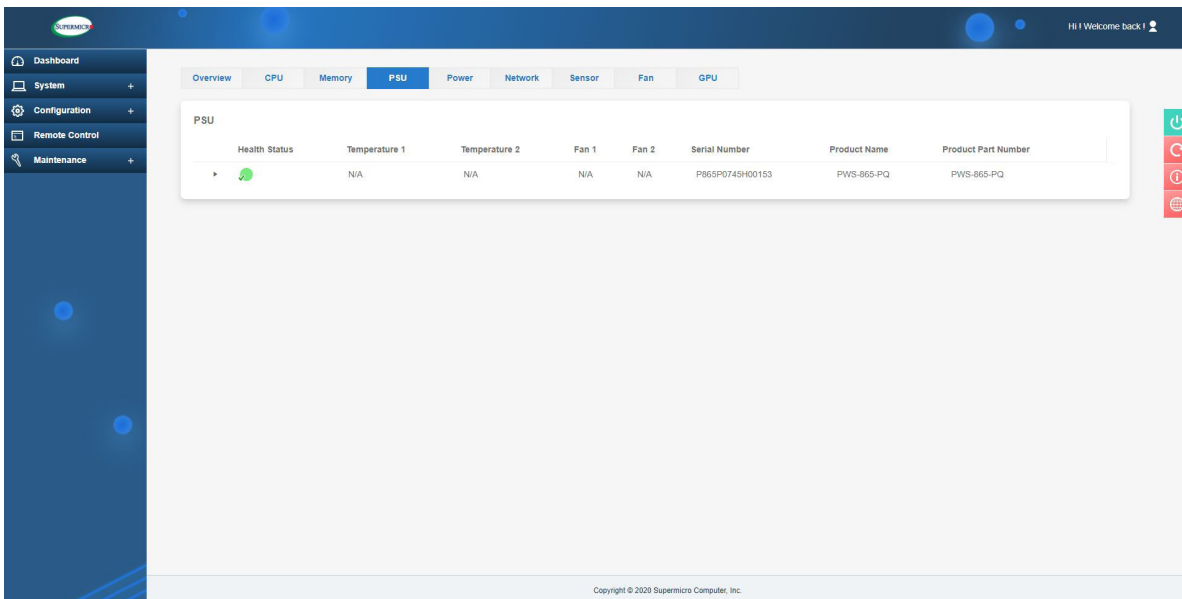
- Status: You can view the health status of the DIMM. It will include one of the following options.
  - Normal
  - Warning
  - Critical
- Name: You can view the memory device name.
- Device Type: You can view the memory device type defined by SMBIOS (e.g., DDR4, DDR5, RDIMM, LRDIMM, or DCPMM).
- Error Correction: You can view the supported error correction info 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 MHz as reported by the memory device. Memory devices that operate at your bus speed shall report the operating speed in MHz (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 info of the memory device.

## PSU

This tab shows power supply unit information.



This page displays the following information.

- Health Status: You can view the health status of the PSU. It will include one of the following options.
  - 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 FAN2 if not detected.

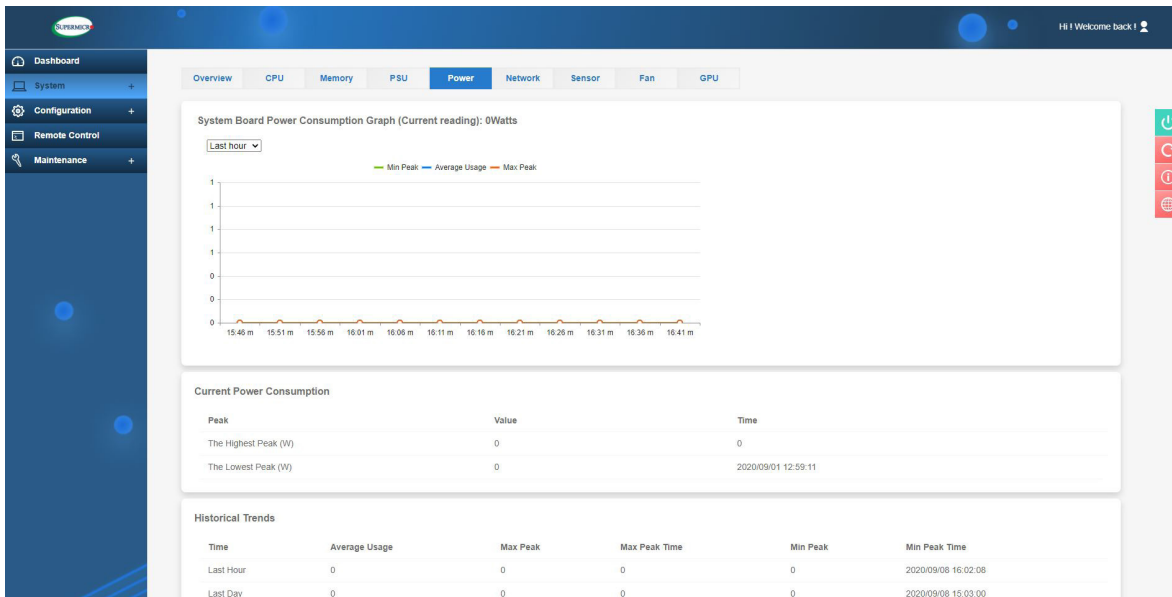
- Serial Number: You can view the serial number of the PSU.
- Product Name: You can view the name of the PSU.
- Product Part Number: You can view the part number of the PSU.

You can also view the following additional information under 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)

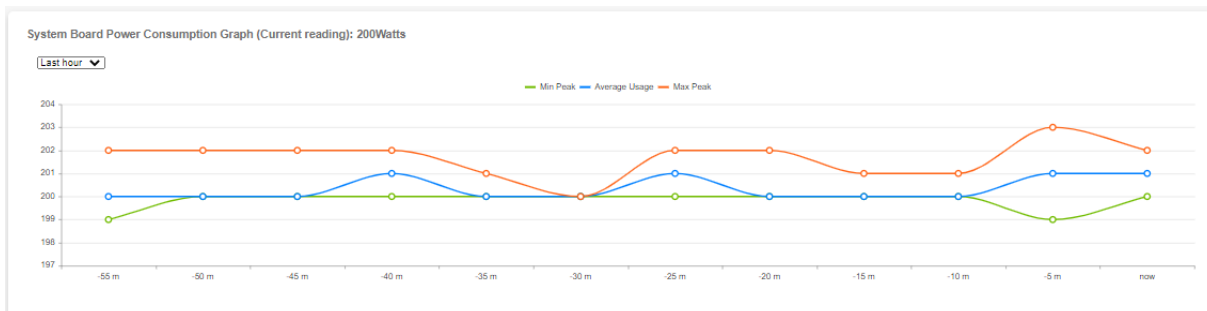
## Power

The tab displays system board power consumption information.



This page displays the following information.

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



Power Consumption Since Powered On		
Peak	Value	Time
The Highest Peak (W)	302	2021/08/13 03:49:42
The Lowest Peak (W)	0	2021/08/11 19:00:05


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

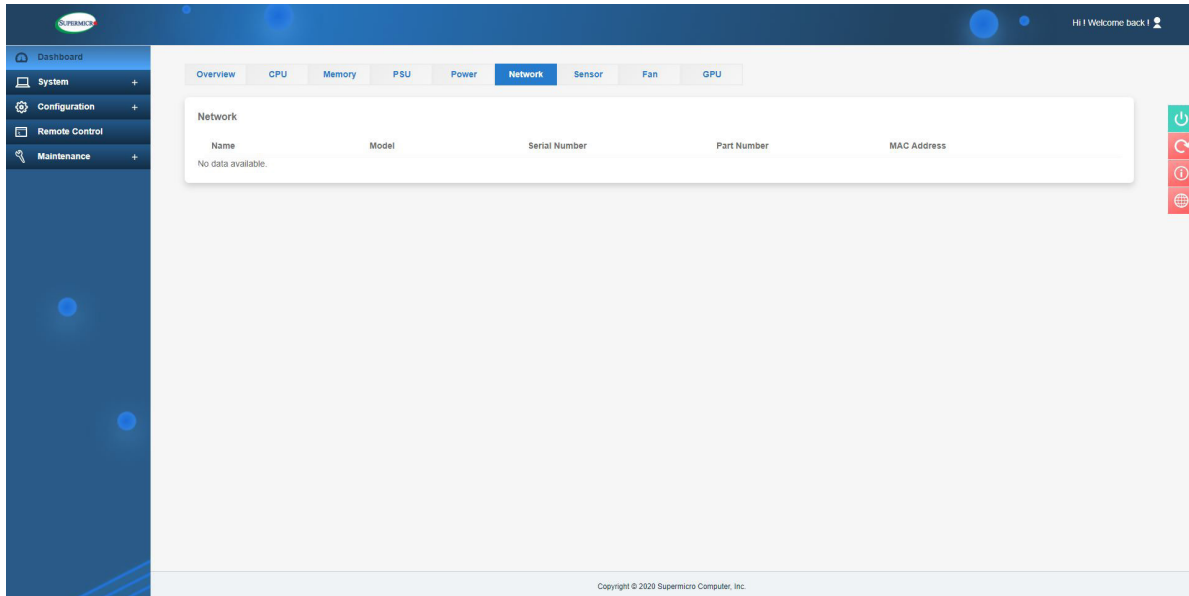
Historical Trends					
Duration	Average Usage	Max Peak	Max Peak Time	Min Peak	Min Peak Time
Last hour	200	203	2021/08/17 23:56:39	199	2021/08/17 23:54:41
Last day	199	241	2021/08/17 17:51:50	197	2021/08/17 16:09:33
Last week	198	302	2021/08/13 03:49:42	0	2021/08/11 14:43:30

- Historical Trend: You can view the past data of 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

## Network AOC

This tab provides the following information about add-on network devices installed in the system.

 **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.



This page displays the following information.

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

Overview CPU Memory PSU Power Smart Power **Network AOC** Sensor Fan GPU

**Network AOC**

Health Status	Model	Temperature	Location	Serial Number				
	AOC-2UR68G4-4XTS	39	SXB 3 slot 0	OA20AS003306				
<table border="1"> <tr> <td>Port 1 MAC Address 3C:EC:EF:1F:32:9A Link Status </td> <td>Port 2 MAC Address 3C:EC:EF:1F:32:9B Link Status </td> <td>Port 3 MAC Address 3C:EC:EF:1F:32:9C Link Status </td> <td>Port 4 MAC Address 3C:EC:EF:1F:32:9D Link Status </td> </tr> </table>					Port 1 MAC Address 3C:EC:EF:1F:32:9A Link Status	Port 2 MAC Address 3C:EC:EF:1F:32:9B Link Status	Port 3 MAC Address 3C:EC:EF:1F:32:9C Link Status	Port 4 MAC Address 3C:EC:EF:1F:32:9D Link Status
Port 1 MAC Address 3C:EC:EF:1F:32:9A Link Status	Port 2 MAC Address 3C:EC:EF:1F:32:9B Link Status	Port 3 MAC Address 3C:EC:EF:1F:32:9C Link Status	Port 4 MAC Address 3C:EC:EF:1F:32:9D Link Status					
	AOC-S100G-b2C	43	SXB 1 slot 2	OA19CS040217				
<table border="1"> <tr> <td>Port 1 MAC Address AC:1F:6B:CF:39:0A</td> <td>Port 2 MAC Address AC:1F:6B:CF:39:0B</td> </tr> </table>					Port 1 MAC Address AC:1F:6B:CF:39:0A	Port 2 MAC Address AC:1F:6B:CF:39:0B		
Port 1 MAC Address AC:1F:6B:CF:39:0A	Port 2 MAC Address AC:1F:6B:CF:39:0B							

Overview CPU Memory **Network AOC** Sensor

**Network AOC**

Health Status	Model	Temperature	Location
	AOC-A100G-b2CM	58	Unknown Slot 1
	AOC-AG-I2M	Unsupported	Unknown Slot 1

**Network AOC**

Health Status	Model	Temperature	Location	Serial Number				
	AOC-AH25G-m2S2TM	55	AIOM slot 1	OA205S026565				
<table border="1"> <tr> <td>Port 1 MAC Address 3C:EC:EF:4F:09:2C FW Version 14.26.4012</td> <td>Port 2 MAC Address 3C:EC:EF:4F:09:2D FW Version 14.26.4012</td> <td>Port 1 MAC Address 3C:EC:EF:1B:E2:F8 FW Version 14.26.4012</td> <td>Port 2 MAC Address 3C:EC:EF:1B:E2:F9 FW Version 14.26.4012</td> </tr> </table>					Port 1 MAC Address 3C:EC:EF:4F:09:2C FW Version 14.26.4012	Port 2 MAC Address 3C:EC:EF:4F:09:2D FW Version 14.26.4012	Port 1 MAC Address 3C:EC:EF:1B:E2:F8 FW Version 14.26.4012	Port 2 MAC Address 3C:EC:EF:1B:E2:F9 FW Version 14.26.4012
Port 1 MAC Address 3C:EC:EF:4F:09:2C FW Version 14.26.4012	Port 2 MAC Address 3C:EC:EF:4F:09:2D FW Version 14.26.4012	Port 1 MAC Address 3C:EC:EF:1B:E2:F8 FW Version 14.26.4012	Port 2 MAC Address 3C:EC:EF:1B:E2:F9 FW Version 14.26.4012					

Overview CPU Memory PSU Power Smart Power **Network AOC** Sensor Fan GPU

**Network AOC**

Health Status	Model	Temperature	Location	Serial Number		
	AOC-AG-I2M	Unsupported	AIOM slot 1	OA212S012160		
<table border="1"> <tr> <td>Port 1 MAC Address 3C:EC:EF:57:9C:4C</td> <td>Port 2 MAC Address 3C:EC:EF:57:9C:4D</td> </tr> </table>					Port 1 MAC Address 3C:EC:EF:57:9C:4C	Port 2 MAC Address 3C:EC:EF:57:9C:4D
Port 1 MAC Address 3C:EC:EF:57:9C:4C	Port 2 MAC Address 3C:EC:EF:57:9C:4D					

## Sensor

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

Severity	Name	Reading	Type
✔	CPU1 Temp	51	Temperature
✘	CPU2 Temp	N/A	Temperature
✔	PCH Temp	29	Temperature
✔	System Temp	26	Temperature
✔	Peripheral Temp	31	Temperature
✔	VRMCpu1 Temp	61	Temperature
✔	VRMCpu1IO Temp	54	Temperature
✘	VRMCpu2 Temp	N/A	Temperature
✘	VRMCpu2IO Temp	N/A	Temperature
✔	VRMP1ABCD Temp	55	Temperature
✔	VRMP1EFGH Temp	37	Temperature
✘	VRMP2ABCD Temp	N/A	Temperature

The sensor table displays the following information.

- Health: You can view the sensor statuses of the sensors' health state.
  - ✔ 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: You can view the sensor names of currently available sensors from the system.
- Reading: You can view the value of the current sensors' reading.
- Type: You can view the sensor type, which is categorized in the following list.
  - Temperature Sensors
  - Voltage Sensors
  - Physical Security
  - Battery (aka Power Supply)
- Low NR: You can view the lower non-recoverable threshold value for each sensor.
- Low CT: You can view the lower critical threshold value for each sensor.

- High NR: You can view the higher non-recoverable threshold value for each sensor.
- High CT: You can view the higher critical threshold value for each sensor.



**Note:** If components are not installed then static sensor values will display N/A.

### **Sensor Type Categories**

By default, [All Sensors] categories are selected. You can filter sensors by following categories.

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

### **Export to Excel**

You can export sensor readings in Excel format.

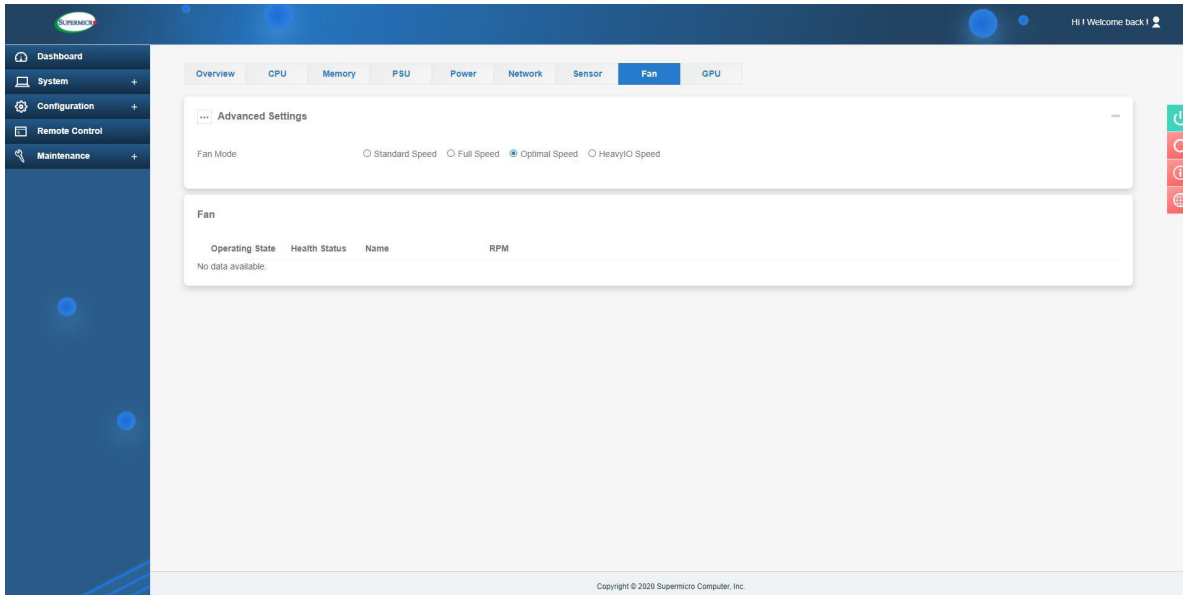
### **Intrusion Reset**

You can use this button to reset chassis intrusion.



## Fans

This tab shows FAN status and allows you to configure the speed for installed fans in the system.

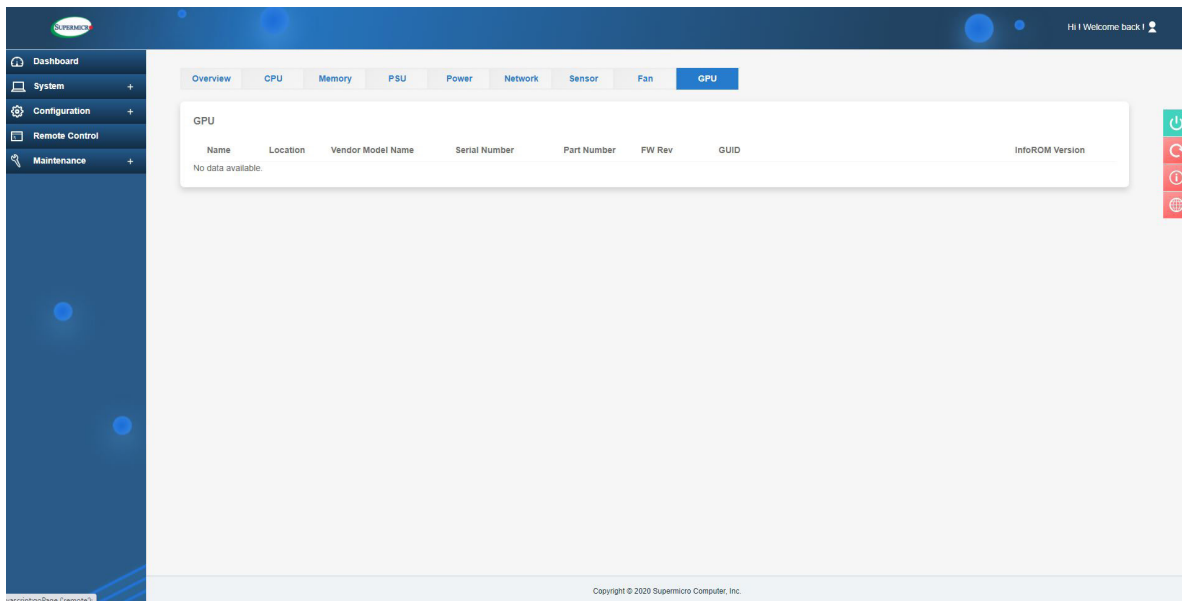


This page displays the following information.

- Status: You can view the fan's health status.
- Name: You can view the indicated system fan number.
- RPM: You can view the indicated revolution per minute for each fan.
- Advanced Settings: Fan modes are dynamically received from Redfish API. Hence, Web UI will display all available speed settings for users to select. You can configure the following possible fan mode speed settings.
  - Standard Speed – The standard fan speed setting for standard power saving and efficiency.
  - Full Speed – The full speed setting for maximum system performance.
  - Optimal or PUE2 Speed – The optimal fan speed setting, which 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 – The heavy I/O fan speed setting, which will boost cooling to the add-on card zone.

## GPU

This tab provides details about each installed GPU unit in the system.



This page displays the following information.

- Location: You can view the add-on device slot location.
- Model: You can view the vendor and model names of the attached GPU device.
- Serial Number: You can view the serial number of the GPU device.
- Part Number: You can view the part number of the GPU device.
- Firmware Revision: You can view the firmware revision info for the GPU device.


## AIP

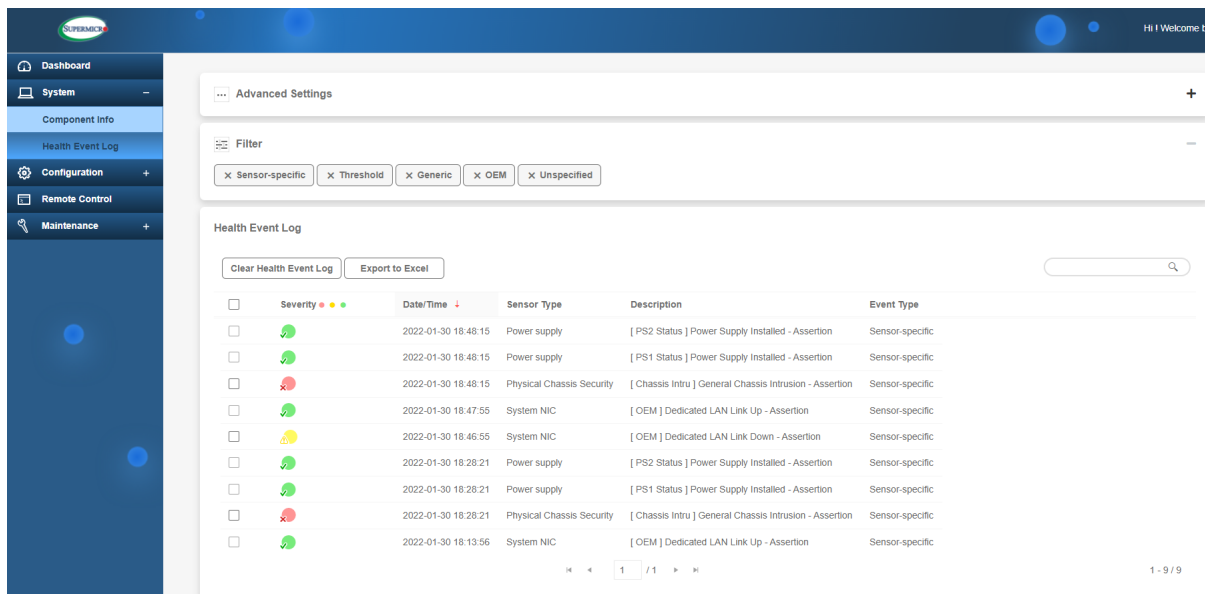
This tab provides the following details about each installed AIP (HaBaNa Gaudi) unit in the system. For the HaBaNa system, the AIP (Advanced Integrated Peripheral) tab will be in place of the GPU tab. Therefore, the following tab will be displayed instead.

- Location: You can view the add-on device slot location.
- Model: You can view the vendor and model names of the AIP device.
- Serial Number: You can view the serial number of the AIP device.
- Part Number: You can view the part number of the AIP device.
- Firmware Revision: You can view the firmware revision info for the AIP device.

## 2.5.2 Health Event Log

This page provides a record of events that occurred in the management system. You can view, export to Excel files, clear events, 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. Options include **Enable AC Power On Event Log** and **Enable FIFO Event Log** by using the ON/OFF switches in **Advanced Settings**.

 **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). Currently, the number of Health Event logs is limited to 4096.



<input type="checkbox"/>	Severity	Date/Time	Sensor Type	Description	Event Type
<input type="checkbox"/>		2022-01-30 18:48:15	Power supply	[ PS2 Status ] Power Supply Installed - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:48:15	Power supply	[ PS1 Status ] Power Supply Installed - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:48:15	Physical Chassis Security	[ Chassis Intru ] General Chassis Intrusion - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:47:55	System NIC	[ OEM ] Dedicated LAN Link Up - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:46:55	System NIC	[ OEM ] Dedicated LAN Link Down - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:28:21	Power supply	[ PS2 Status ] Power Supply Installed - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:28:21	Power supply	[ PS1 Status ] Power Supply Installed - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:28:21	Physical Chassis Security	[ Chassis Intru ] General Chassis Intrusion - Assertion	Sensor-specific
<input type="checkbox"/>		2022-01-30 18:13:56	System NIC	[ OEM ] Dedicated LAN Link Up - Assertion	Sensor-specific

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

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



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



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



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

- Date/Time: You can view the timestamp of event occurrence
- Sensor: You can view the type the name of the sensor that triggered the event.
- Description: You can view the basic description of the event.
- Event Type: You can view the events that will be listed based on the following categories.
  - Sensor-Specific
  - Threshold
  - Generic
  - OEM
  - Unspecified

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 acknowledge warning/critical events. Select a log entry that you want to acknowledge and click on Mark as Acknowledged.
- Clear Acknowledgments: You can clear all acknowledgments and click on Clear Acknowledgement.

## Multi Node

Use this page to view details about the current node as well as other nodes in the server. Under 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, and 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, BMC Version, and BMC MAC Address of the node in interest. For H12 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, users under 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.

The screenshot illustrates the BMC interface for a multi-node system. It shows two 'Logical Front View of Node' panels at the top, with a red arrow pointing from the left panel to the right panel. Below these panels is a 'Node A' details section. On the left, a table lists various system parameters for Node A. On the right, there are four main tabs: System, UID Control, Firmware Update, and Sensor Readings. The 'System' tab is active, displaying system information. A red arrow points from the IP address '10.140.179.16' in the table to the 'System' tab, and another red arrow points from the 'System' tab to the 'Open new page and auto login' text above the tabs.

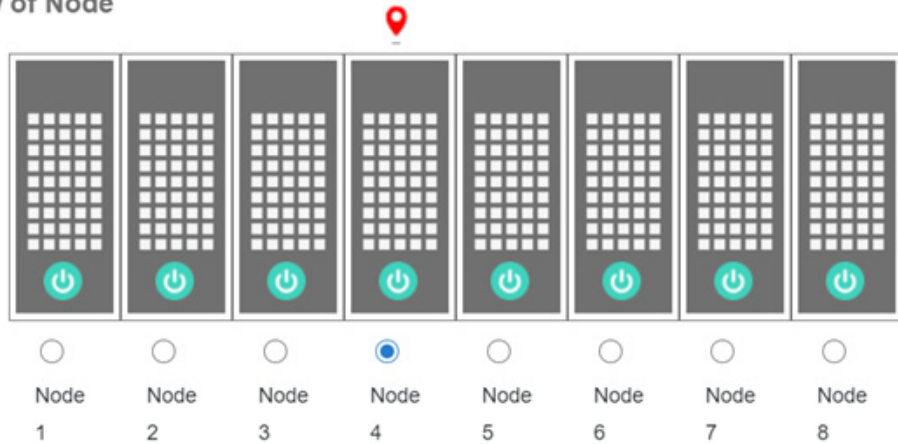
Node A	
Status	Present
Power State	On
DC Output Power	108 W
DC Output Current	9 A
CPU 1	38 °C
System Temperature	38 °C
Part Number	BP_202109101733
Board Serial Number	UM218S003563
IP Address	10.140.179.16
BIOS Version	1.1c

System	
Firmware Version	00.23.51
Firmware Build Time	11/10/2021
Redfish Version	1.8.0
BIOS Firmware Version	1.1c
BIOS Build Time	10/12/2021

Host	
Server Host Name	X12SPG-NF
Server IP Address	10.140.179.16


As shown in the Multi-Node image below, you can click on any of these nodes to get a BMC/ Web UI redirected. From there, you can log in to the BMC as a single or individual node to perform tasks, including firmware updates.

Logical Front View of Node




## 2.5.3 Storage Monitoring

You can use this page to view details about installed storage components if the server is connected to the storage component(s). This page will not be available if a storage component is not connected.

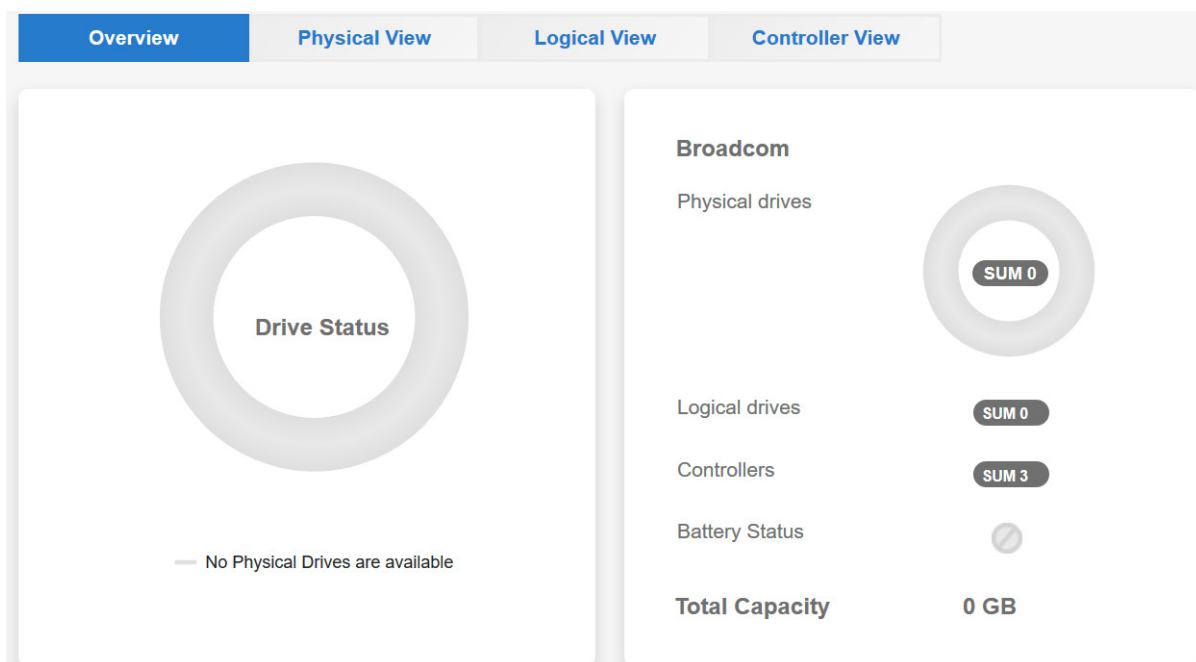
 **Note:** If you do not have a storage device installed in your system, the system will not display this page. Use this page to view details about installed storage components if the server is connected to storage component(s).

### Overview

This page shows the 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 disks. If BMC detects that all connected drives are functional, the drive status will show **GREEN**. If BMC detects one or more drives 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**.

 **Note:** BMC detects the NVMe backplane. If the backplane is there, the storage page will be shown and the drive's hot plug (in-out) will be monitored.

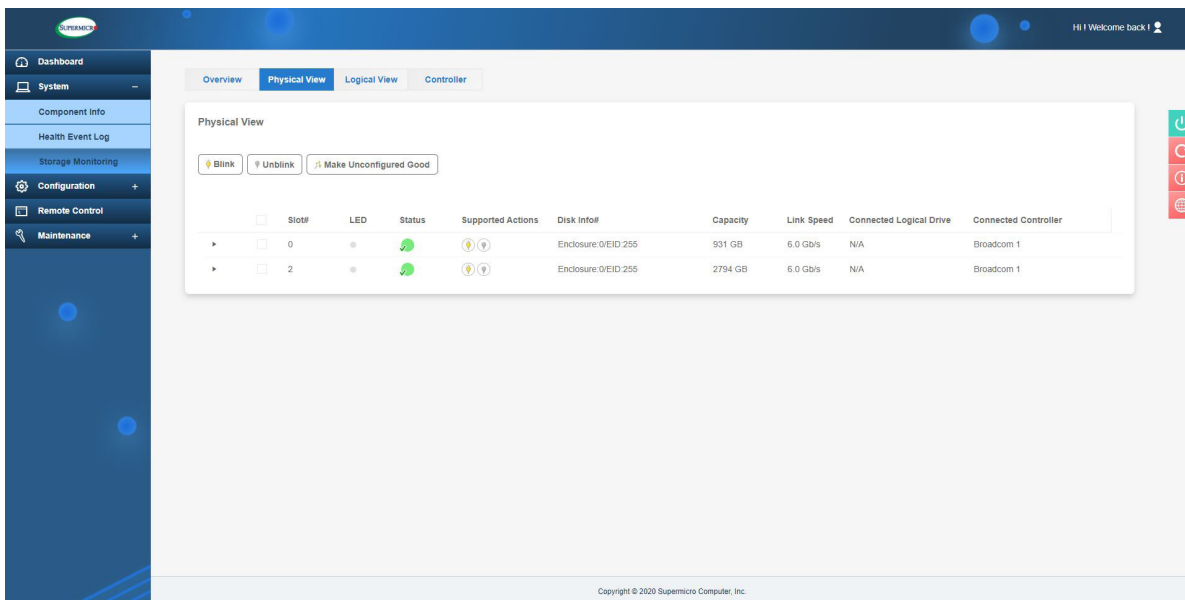
If the system only supports direct NVME, the drive will not support hot plug (in-out). Additionally, with the drive inserted, the storage page will not display after boot up.





## Physical View

Physical view shows physical disk information for SAS, SATA, NVMe SSDs, etc. It also shows the details about physical disks attached to the controller or present in the storage subsystem.



You can also perform actions associated with each disk. All actions are available and applicable based on the selected disk. Click on the expandable button to get the following detailed information about the physical disk.

- Slot Number: You can view the connected physical disk's slot number.
- LED: You can view the LED blinking status of the corresponding disk.
- Status: You can view the indicated the health of the connected disk.
  - 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 critical.
- Supported Actions: You can view the indicated actions are supported based on HDD type.
- Disk Info#: You can view the available disk info.
- Capacity: You can view the capacity of the physical disk (GB).
- Link Speed: You can view the link speed of the physical disk (b/s).
- Connected Logical Drive: You can view the connected logical drive info (if any).
- Connected Controller: You can view the connected controller info (if any).

Overview **Physical View** Logical View Controller

Physical View

<input type="checkbox"/>	Slot#	LED	Status	Supported Actions	Disk Info#	Capacity	Link Speed	Connected Logical Drive	Connected Controller
▶	<input type="checkbox"/> 0	●			Enclosure:0/EID:10	478 GB	N/A		SAS 3408 Device 2
▶	<input type="checkbox"/> 0	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1
▶	<input type="checkbox"/> 1	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1
▶	<input type="checkbox"/> 3	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 237	SAS 3918 Device 1
▶	<input type="checkbox"/> 4	●			Enclosure:0/EID:250	138 GB	6.0 Gb/s	Slot: 238	SAS 3918 Device 1
▶	<input type="checkbox"/> 6	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 238	SAS 3918 Device 1
▶	<input type="checkbox"/> 7	●			Enclosure:0/EID:250	138 GB	6.0 Gb/s	Slot: 237	SAS 3918 Device 1
▶	<input type="checkbox"/> 9	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1
▶	<input type="checkbox"/> 10	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1

Overview **Physical View** Logical View Controller

Physical View

<input type="checkbox"/>	Slot#	LED	Status	Supported Actions	Disk Info#	Capacity	Link Speed	Connected Logical Drive	Connected Controller																
▼	<input type="checkbox"/> 0	●			Enclosure:0/EID:10	478 GB	N/A		SAS 3408 Device 2																
					<table border="1"> <tr> <td>Manufacturer</td> <td>NVMe</td> </tr> <tr> <td>Product Name</td> <td>INTEL SSDPEKKW51</td> </tr> <tr> <td>Firmware Revision</td> <td>004C</td> </tr> <tr> <td>Serial Number</td> <td>PHHH928002NS912H</td> </tr> <tr> <td>Firmware State</td> <td>Unconfigured good drive</td> </tr> <tr> <td>Other Error Count</td> <td>0</td> </tr> <tr> <td>SMART Event/Message Received</td> <td>0</td> </tr> <tr> <td>Media Error Count</td> <td>0</td> </tr> </table>					Manufacturer	NVMe	Product Name	INTEL SSDPEKKW51	Firmware Revision	004C	Serial Number	PHHH928002NS912H	Firmware State	Unconfigured good drive	Other Error Count	0	SMART Event/Message Received	0	Media Error Count	0
Manufacturer	NVMe																								
Product Name	INTEL SSDPEKKW51																								
Firmware Revision	004C																								
Serial Number	PHHH928002NS912H																								
Firmware State	Unconfigured good drive																								
Other Error Count	0																								
SMART Event/Message Received	0																								
Media Error Count	0																								
▶	<input type="checkbox"/> 0	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1																
▶	<input type="checkbox"/> 1	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1																
▶	<input type="checkbox"/> 3	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 237	SAS 3918 Device 1																
▶	<input type="checkbox"/> 4	●			Enclosure:0/EID:250	138 GB	6.0 Gb/s	Slot: 238	SAS 3918 Device 1																
▶	<input type="checkbox"/> 6	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 238	SAS 3918 Device 1																
▶	<input type="checkbox"/> 7	●			Enclosure:0/EID:250	138 GB	6.0 Gb/s	Slot: 237	SAS 3918 Device 1																
▶	<input type="checkbox"/> 9	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1																
▶	<input type="checkbox"/> 10	●			Enclosure:0/EID:250	138 GB	3.0 Gb/s	Slot: 239	SAS 3918 Device 1																

All physical actions are available and applicable based on the selected disk. You can perform the following physical actions correlated to each disk.

- Blink: You can use this feature to locate a physical disk.
- Un-blink: You can use this feature to stop the blink action.
- Make Unconfigured Good: You can use this feature to select an unconfigured drive to make an unconfigured good drive.
- Insert: You can use this feature to insert a new NVMe disk if the VMD mode is disabled.
- Eject: You can use this feature to eject an existing NVMe disk if VMD mode is disabled.
- Disk Erase: You can apply an action to erase the disk connected to the Broadcom 3108 controller. It allows you to instantly and securely render data on attached drives.
- Erase Abort: You can select this option to stop/abort the erase action once you start the Secure Erase action.



**Note:** The following table provides details on which storage controller is supported. In the X13 series, 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, then neither the Eject nor Insert buttons would appear.

You can also view the following HDD detailed information by clicking the arrow pointer next to a particular HDD (NVMe or SATA).

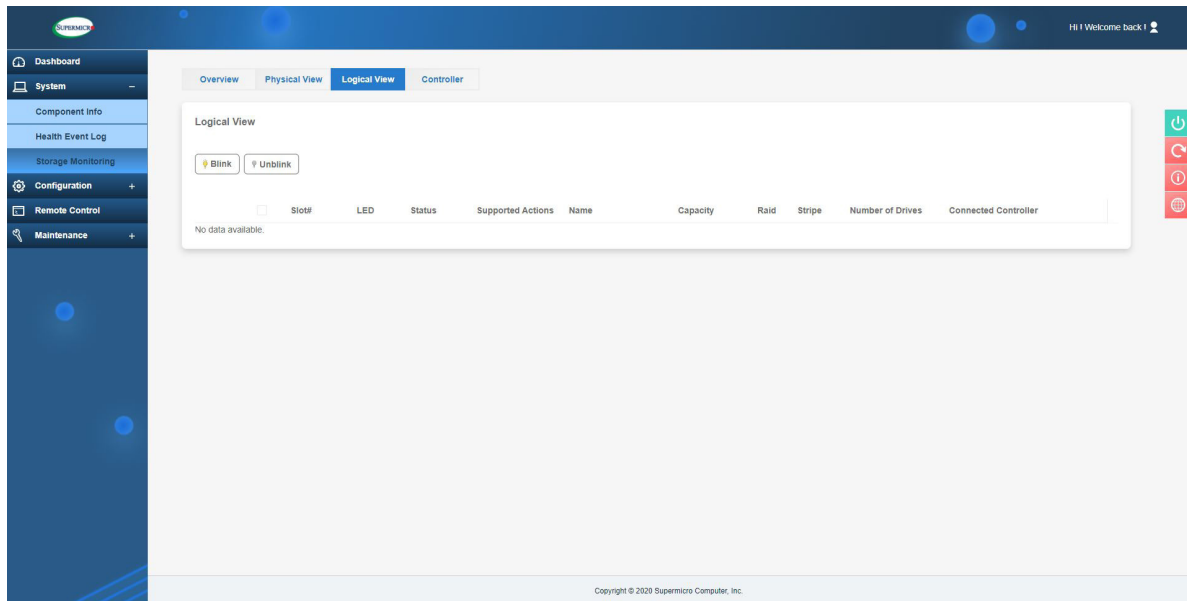
- Temperature (in Celsius)
- Manufacturer – Name of manufacturer
- Product Name – Product name of the storage controller
- Serial Number
- Drive functional (1 or 0)
- Percentage of drive life used (in %)
- VMD Mode (Disable / Enable)
- Port 0 Max Link Speed (in GT/s)
- Port 0 Max Link Width

- Port 1 Max Link Speed
- Port 1 Max Link Width

Table for Supported Controller(s)					
	<b>Blink</b>	<b>Unblink</b>	<b>Make Unconfigured Good</b>	<b>Eject</b>	<b>Insert</b>
<b>Broadcom</b>	Supported	Supported	Supported	<i>Not supported</i>	<i>Not supported</i>
<b>Marvell</b>	<i>Not supported</i>				
<b>NVMe</b>	Supported	Supported	<i>Not supported</i>	<i>Not supported if NVMe in VMD mode</i>	<i>Not supported if NVMe in VMD mode</i>

Table for Supported Controller(s)		
	<b>Disk Erase</b>	<b>Erase Abort</b>
<b>Broadcom</b>	Supported only for Broadcom Mega RAID controllers such as AOC-S3108L-H8IR, AOC-S3908L-H8IR (-16DD/-32DD), and AOC-S3916L-H16IR (-32DD).	Supported only for Broadcom Mega RAID controllers such as AOC-S3108L-H8IR, AOC-S3908L-H8IR (-16DD/-32DD), and AOC-S3916L-H16IR (-32DD).
<b>Marvell</b>	<i>Not supported</i>	
<b>NVMe</b>	<i>Not supported</i>	<i>Not supported</i>

## Logical View

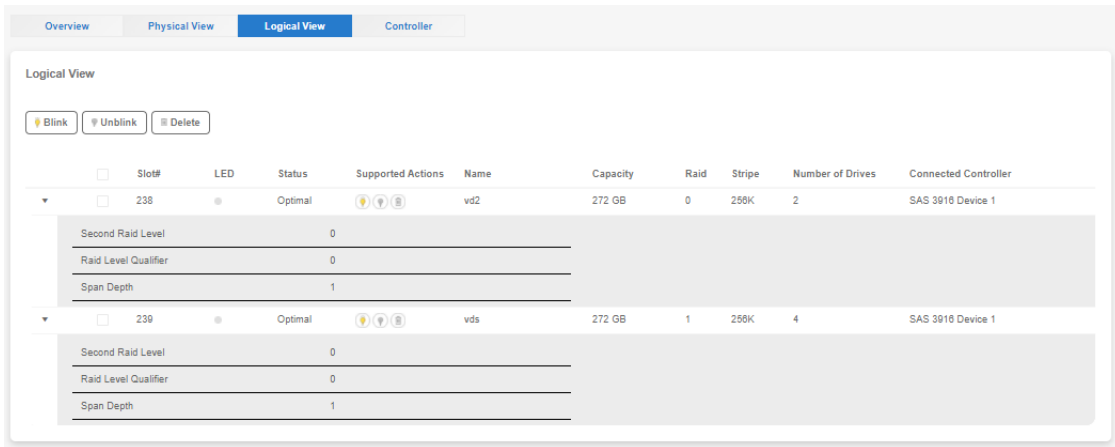


This page shows the details about virtual disks created with respective physical disks in the storage subsystem, including the following information.

- Slot Number: You can view the slot info of the logical disk.
- State: You can view the logical disk state info (Offline/Partially Degraded/Degraded/Optimal/Foreign, etc.).
- Blink: You can view the blinking status of the disk.
- Name: You can view the given name of the logical disk.
- Capacity: You can view the capacity of the logical disk (GB).
- RAID: You can view the configured RAID level.
- Stripe: You can view the stripe level of the logical disk.
- Number of drives: You can view the number of drives connected to a logical disk.
- Connected Controller: You can view the connected controller info.

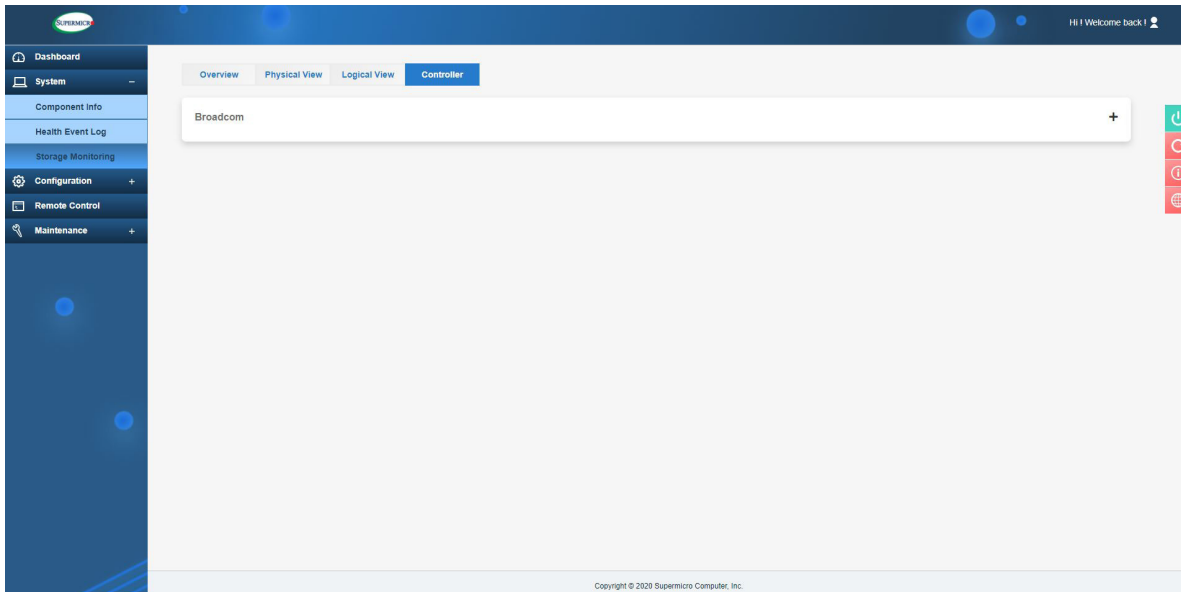
All logical view actions are available and applicable based on the selected disk. You can perform the following actions correlated to each disk.

- Blink: You can use this action to locate a virtual disk.
- Un-blink: You can use this action to stop the blink action.
- Delete: You can use this action to delete a virtual disk.



## Controller

This page shows the information about the connected controllers to the system. It displays different controller info and allows users to create RAID and apply changes to Controller actions. BMC supports all RAID levels from the available RAID levels of the manufacturers. (e.g., If AOC-S3916L-H16IR (-32DD) supports RAID 0, 1, 5, 6, 10, 50, and 60, then BMC will also provide the same RAID levels.) Select the controller and click on the expandable button to view details about the controller.



You can see the following collection of configuration and informational data associated with a particular Storage Controller.

- Product Part Number
- Product Revision
- Controller Name
- Controller Revision
- Serial Number
- Link Speed (Protocol)
- Link Width
- Vendor ID
- Device ID

- SubVendor ID
- SubDevice ID
- Manufacture Date (timestamp)
- Manufacture Batch
- SAS Address (Optional)
- Checksum/Reserved (Optional)



## Create RAID

Broadcom	
SAS 3816 Device 0 ▾	
Controller Name	SAS 3816
Controller Status	OK
Location	PCIE card: SXB3, Slot: 1
FW Version	16.00.08.00
BIOS Version	09.31.00.00_16.00.00.00
Link Speed	12GB/s, SAS3
Controller PCIE Link Width	8x
Product Name	AOC-S3816L-L16iT
Serial	UA203S034138
Revision	Rev 1.00
Vendor ID	14E4
Device ID	00E6
Sub Vendor ID	15D9
Sub Device ID	1B65
Controller Chip revision	A1
Manufactured Date Timestamp	08/11/2020, 09:20:40
Batch	1

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

- **Create:** You can select an available physical disk and add configuration options such as RAID level, capacity, name, stripe size, R/W policy, access policy, initialization state, etc. To confirm the action, click Submit.
- **Add [Select Group]:** You can use this action to select or add a logical drive to the existing group.

## Controller Actions

You can perform the following controller actions.



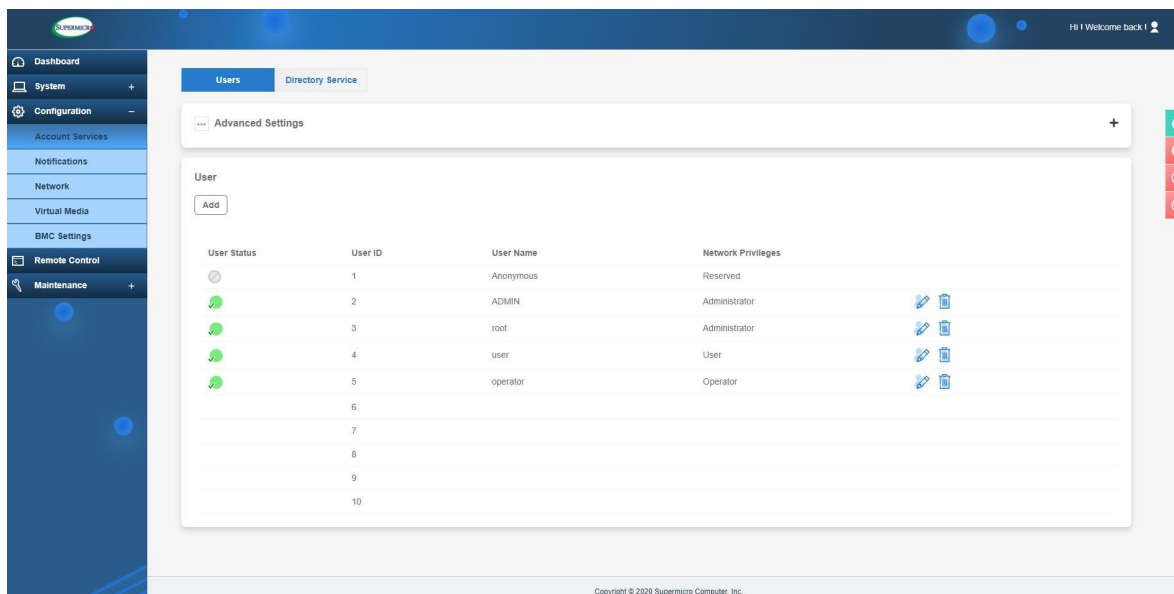
**Note:** Available actions will change based on the controller selection.

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

## 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. Please refer to the additional information for each page below.

## 2.6.1 Account Services



### Users

This feature allows administrators to monitor and configure user accounts for BMC privileges. The Users tab provides 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 with User privileges.

- **Add New User:** As an Administrator user, you can click the [Add] button to add a new user. Users will then be able to define the User Name, Password, and Network Privilege (Administrator, Operator, or User). They will also be able to 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.


The users table displays the following details for each user. You can edit, lock, or delete a user from the table.

- **User Status:** You can view whether the user login is enabled, disabled, or locked. The green icon indicates that the corresponding user account is enabled and the grey icon indicates that it is disabled or locked.
- **User ID:** You can view the ID number used to identify the configured users. BMC supports up to 16 user accounts.

- User Name: You can view the list of current users which have been created.
- Network Privilege: You can view 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).
- Trash Icon Icon (Delete User): Administrator users can delete any user account, including those not in use. However, you cannot delete the default administrator account (the default ADMIN user) or are being logged on. If there is an attempt to do so, there will be a prompt to alert the administrator users.
- Password Requirements: You can preview the password by clicking on the eye icon.
  - Password requires a length of 8 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

Password

Confirm Password

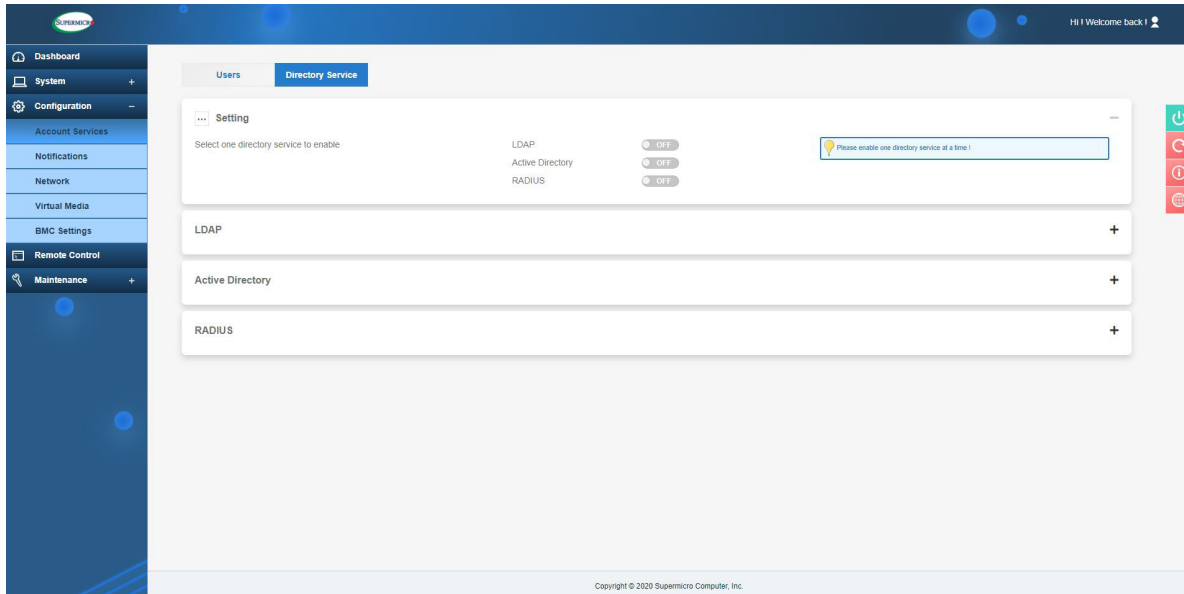
 **Note:** The maximum number of user profiles that can be created and exist at a time is 16.

## 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 the users will be locked out (unable to log in) after Failed Login Attempt Lockout Threshold failed login attempts. If it is set to "Never", the Failed Login Lockout Controls will be disabled.

## Directory Services

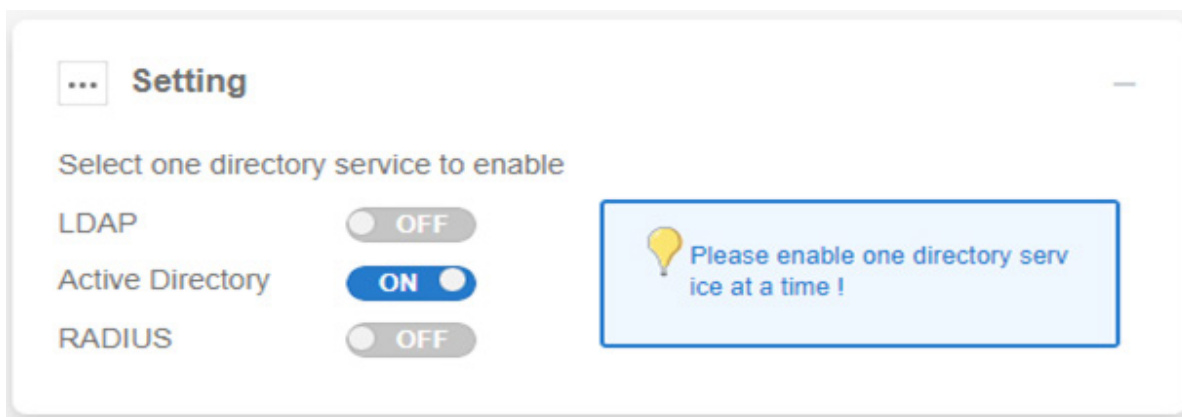


## Settings

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



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



## LDAP (Lightweight Directory Access Protocol)

LDAP allows users 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 the LDAP service.

- Bind DN: The bind DN (Distinguished Name) 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: You can enter the bind password for LDAP server authentication.



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

- Username Attribute: You can enter the username login attribute.
- Groups Attribute: You can enter the group membership attribute.
- Server Address: You can 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.
  - Port Number – Enter the number of the LDAP server. The default port number for LDAP is 389 and SSL LDAP is 636. You can edit or delete 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 – You can choose to use either LDAP or SSL LDAP (`ldap://` or `ldaps://`).
  - Role – You can select the privilege level for a user or role group (Administrator, Operator, or User).
  - Remote User – You can enter the LDAP username.
  - Remote Group – You can enter the name of the LDAP group. For example, `cn=Power Users,ou=Groups,dc=example,dc=org`.



## Active Directory

This page allows you to view and configure Active Directory authentication. Using the credentials, Active directory users can also 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.

- **DNS Lookup:** You can turn on DNS Lookup to allow BMC to add Active Directory servers through LDAP or LDAPS protocol.
- **Domain Name:** You can 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 displays the port number of the server.
- **Static Server Address:** You can add up to three static server addresses instead of getting Active Directory Server Addresses from 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:** You can enter up to five rules for Role, Remote User, and Remote Group. Click on [Add] to add rules and enter the following fields.
  - **Roles** – Select the privilege level for that user or role group (Administrator/Operator/User).
  - **Remote User** – Enter the AD/LDAP username.
  - **Remote Group** – Enter the name of the LDAP group folder.



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

## RADIUS

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

- **Secret:** You can enter a bind password for the user to access the RADIUS server. Password can be previewed with the eye-icon button.
- **IP Address or Domain Name:** You can select to enter the server IP or domain name.
- **Port Number:** You can enter the port number. Values range between 1 and 65535 (half-width).



**Note:** You must click on Submit button to allow BMC to make changes to RADIUS settings.

## 2.6.2 Notifications

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

### Alerts

Use this page to configure the alerts 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:** Please 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.

No.	Enable	Protocol	Destination Address	Event Type
1	false	SNMPv1	0.0.0.0	
2	false	SNMPv1	0.0.0.0	
3	false	SNMPv1	0.0.0.0	
4	false	SNMPv1	0.0.0.0	
5	false	SNMPv1	0.0.0.0	
6	false	SNMPv1	0.0.0.0	
7	false	SNMPv1	0.0.0.0	
8	false	SNMPv1	0.0.0.0	
9	false	SNMPv1	0.0.0.0	
10	false	SNMPv1	0.0.0.0	
11	false	SNMPv1	0.0.0.0	
12	false	SNMPv1	0.0.0.0	
13	false	SNMPv1	0.0.0.0	
14	false	SNMPv1	0.0.0.0	
15	false	SNMPv1	0.0.0.0	
16	false	SNMPv1	0.0.0.0	

Alerts table will display the following information.

- No.: You can view the number of available alert entries.
- Enable: You can whether the alerts are enabled or disabled with the 🔔 and 🔕 bell icons.
- Protocol: You can view the supported protocol being set for the particular alert transmission (e.g., Redfish, SMTP, or SNMPv1).
- Destination: You can view the destination address where the alerts will be sent.
- Event Types: You can view the configured event types for respective alerts. Supported event types include the following.
  - Alert
  - ResourceAdded


- ResourceRemoved
- ResourceUpdated
- StatusChange
- Modify: You can click on the pencil icon  on the row of an alert to configure the settings.
- Modify Alert: You can configure the alert using the following options.
  - 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.

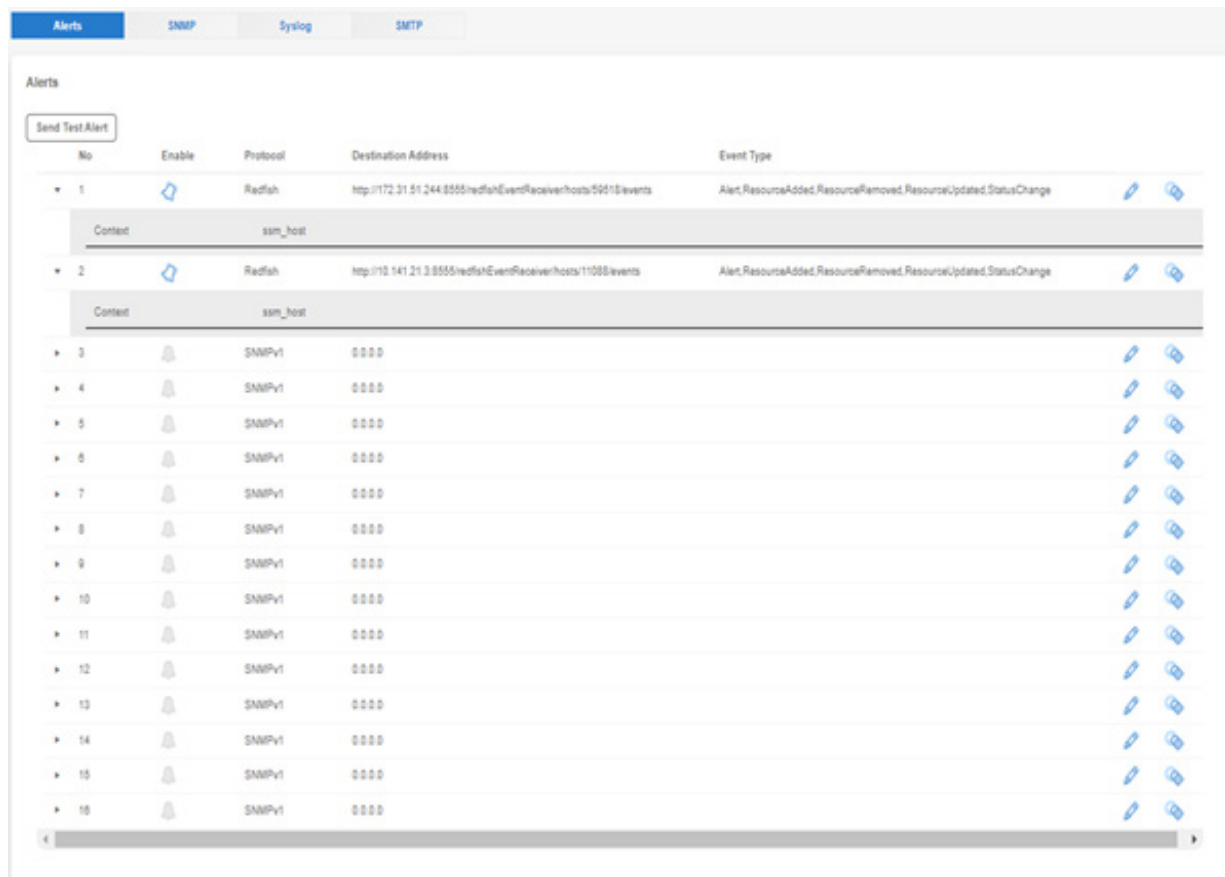
- Event Type – Select one or more of the following event types if protocol SMTP or Redfish is selected. Alert protocol will be preset if SNMPv1 or SNMPv3 is selected.
  - Alert
  - ResourceAdded
  - ResourceRemoved
  - ResourceUpdated
  - StatusChange
- Destination Address – Enter an IPv4 or an IPv6 address where alerts will be sent. 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 context field for Redfish protocols.

- Subject – You must provide content for the Subject field. This field is displayed only when SMTP is selected and required for the SMTP protocol.
- Trap Community – Enter information for trap. This field is only displayed when SNMPv1 is selected.
- Delete – You can delete the respective alert alert by clicking on the trash can icon.

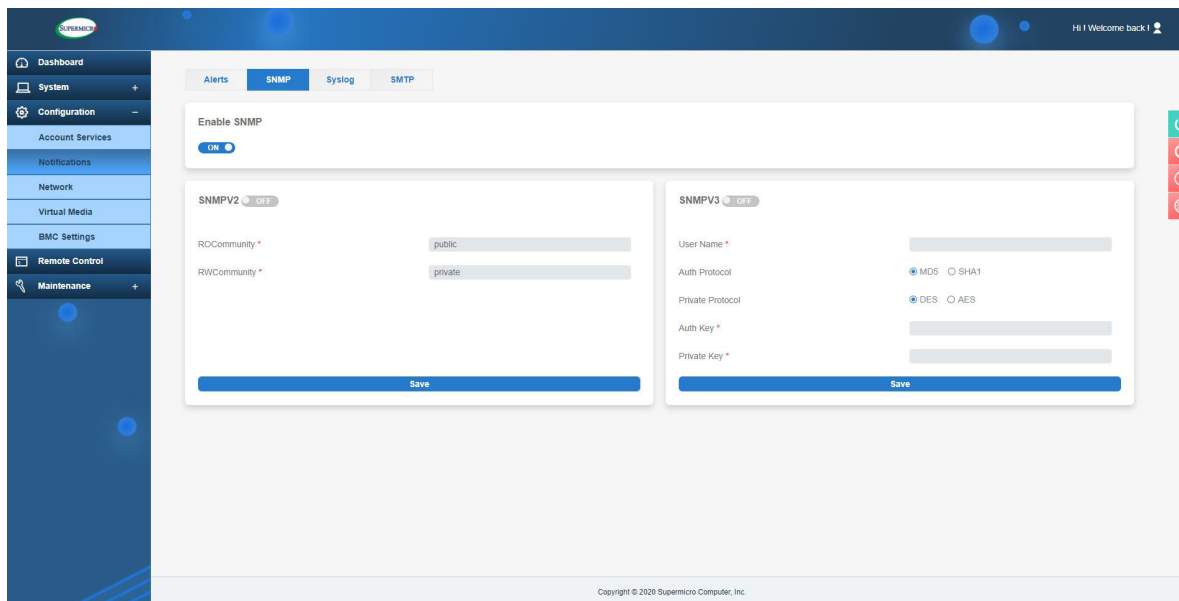
You can click on [Send Test Alert] to check if the alerts have been set and sent out correctly. Respectively configured alerts will be sent for test purposes.



No	Enable	Protocol	Destination Address	Event Type
1	<input checked="" type="checkbox"/>	Redfish	http://172.31.31.244:8555/redfish/EventReceiver/hosts/50013/events	Alert.ResourceAdded.ResourceRemoved.ResourceUpdated.StatusChange
		Context	ssm_host	
2	<input checked="" type="checkbox"/>	Redfish	http://10.141.21.3:8555/redfish/EventReceiver/hosts/11088/events	Alert.ResourceAdded.ResourceRemoved.ResourceUpdated.StatusChange
		Context	ssm_host	
3	<input type="checkbox"/>	SNMPv1	0.0.0.0	
4	<input type="checkbox"/>	SNMPv1	0.0.0.0	
5	<input type="checkbox"/>	SNMPv1	0.0.0.0	
6	<input type="checkbox"/>	SNMPv1	0.0.0.0	
7	<input type="checkbox"/>	SNMPv1	0.0.0.0	
8	<input type="checkbox"/>	SNMPv1	0.0.0.0	
9	<input type="checkbox"/>	SNMPv1	0.0.0.0	
10	<input type="checkbox"/>	SNMPv1	0.0.0.0	
11	<input type="checkbox"/>	SNMPv1	0.0.0.0	
12	<input type="checkbox"/>	SNMPv1	0.0.0.0	
13	<input type="checkbox"/>	SNMPv1	0.0.0.0	
14	<input type="checkbox"/>	SNMPv1	0.0.0.0	
15	<input type="checkbox"/>	SNMPv1	0.0.0.0	
16	<input type="checkbox"/>	SNMPv1	0.0.0.0	

## SNMP

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



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. Add SNMP2 Community by selecting one or more SNMPv2 Communities and clicking on [Add] to add a community with either Access Mode - ReadOnly or ReadWrite to configure a 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.
  - Auth Protocol: You can select MD5, SHA1, or Account for the authentication protocol.
  - Private Protocol: Users can select None, DES, AES, or Account for the private protocol.
4. Click [Save] to save user settings. The saved configurations are to be used whenever you start or stop the SNMP daemon.



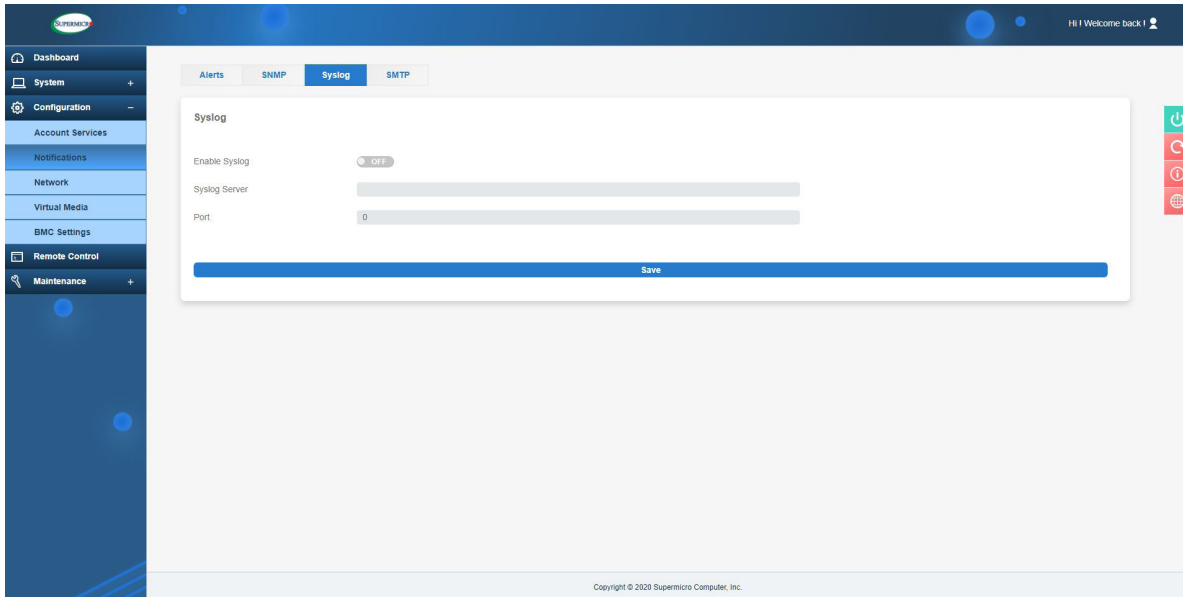
**Note:** By default, all SNMP settings are disabled (OFF) and the SNMP port is set to UDP port 161. You can go to the Port page (Configuration → Network → Port) to change the SNMP port number. Once the SNMP setting is ON, you can turn ON SNMPv2 or SNMPv3 using the ON/OFF buttons. Once SNMP is turned OFF, SNMPv2 and SNMPv3 will also be turned OFF. Thereafter, no trap will be sent out.

The screenshot shows the SNMP configuration page with the following elements:

- Navigation tabs: Alerts, **SNMP**, Syslog, SMTP.
- Enable SNMP:  OFF
- SNMPv2:  OFF
- Hide Community Strings:  OFF
- Add button
- Table with columns: Name, Community String, Access Mode
- SNMPv3:  OFF
- Auth Protocol:  MD5  SHA1  Account
- Private Protocol:  None  DES  AES  Account
- Save button

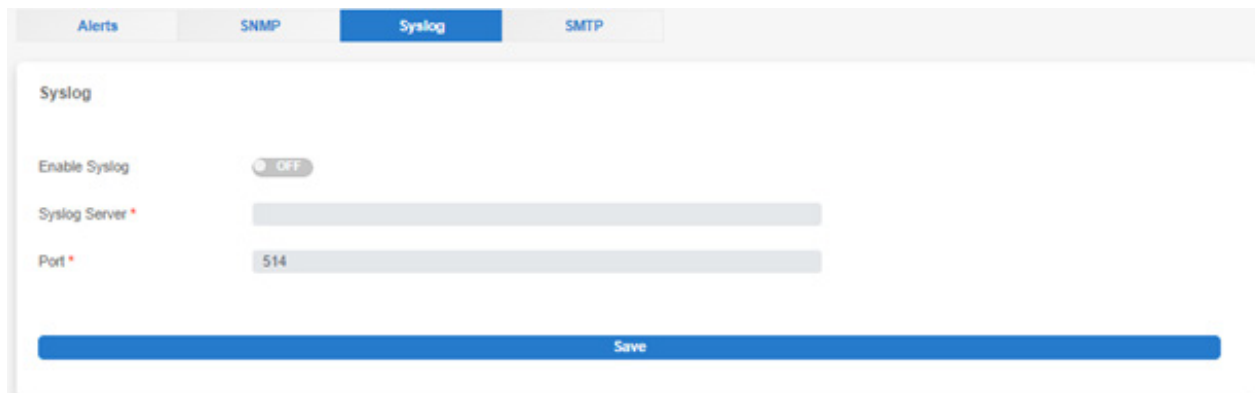
## Syslog

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



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

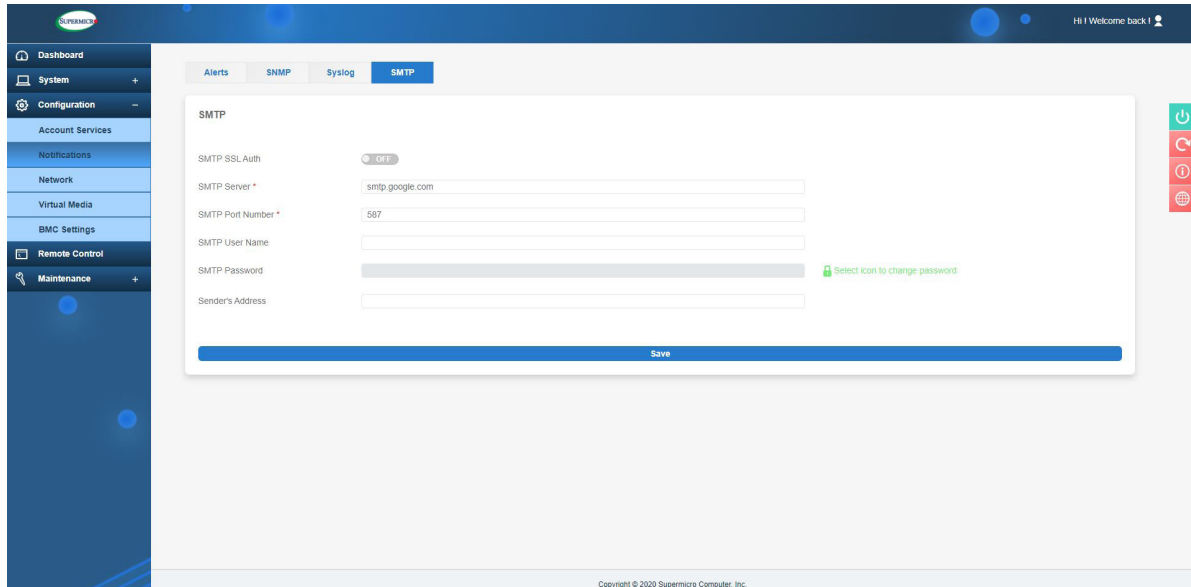
1. Select [Enable Syslog] to turn on Syslog.
2. Enter the address into the Syslog server field.
3. Enter the port number for the Syslog server.
4. Click [Save] to complete the configuration.





## SMTP (Simple Mail Transfer Protocol)


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




To configure the SMTP settings, refer to the following options.

- Server Address: You need to enter the address for the SMTP mail server to configure SMTP.
- Port Number: You need to enter a SMTP port number. By default, the port number is 587.
- Connection Protocol: You can choose one of the following protocols to set up the SMTP authentication.
  - AutoDetect
  - None
  - StartTLS
  - TLS\_SSL
- Authentication: You can choose one of the following authentication methods to set up SMTP.
  - AutoDetect
  - CRAM\_MD5
  - Login

- None
- Plain

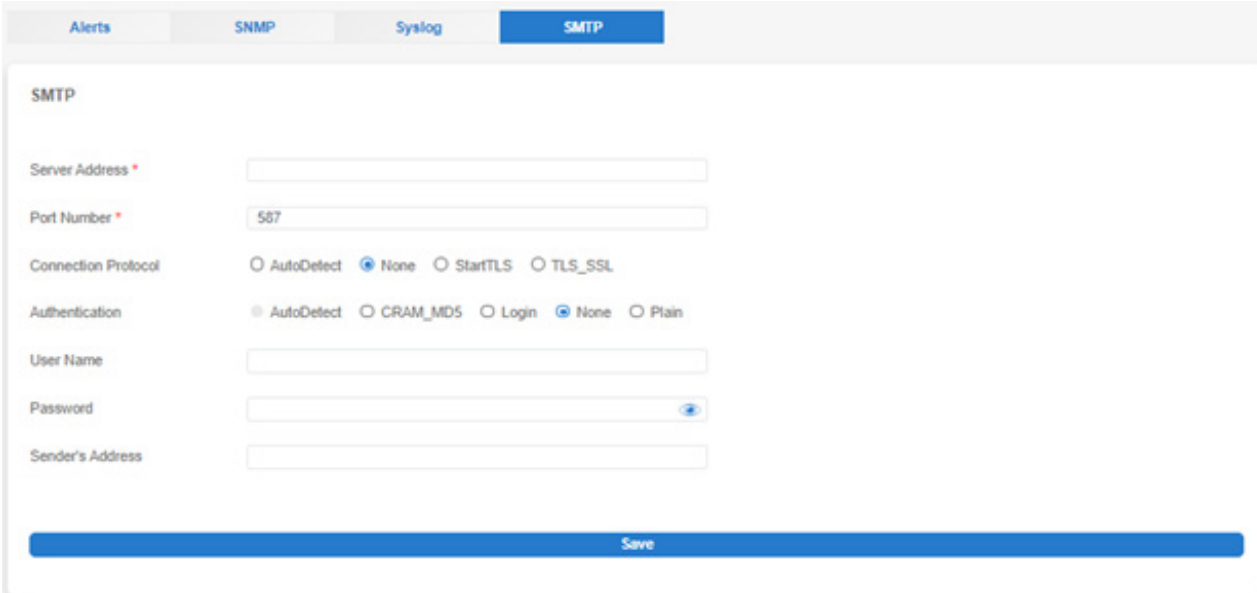
 **Note:** The types of authentication method that will be available depends on which Connection Protocol is selected. For example, when you choose None as the Connection Protocol, the AutoDetect option in Authentication will be greyed out.

- User Name: You can enter the user name for the SMTP mail server. This is optional.
- Password: You need to set up the user password if a User Name is added for the SMTP mail. Passwords can be previewed with the eye-icon button.

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

- Sender's Address: You have the option to add the Sender's address.

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



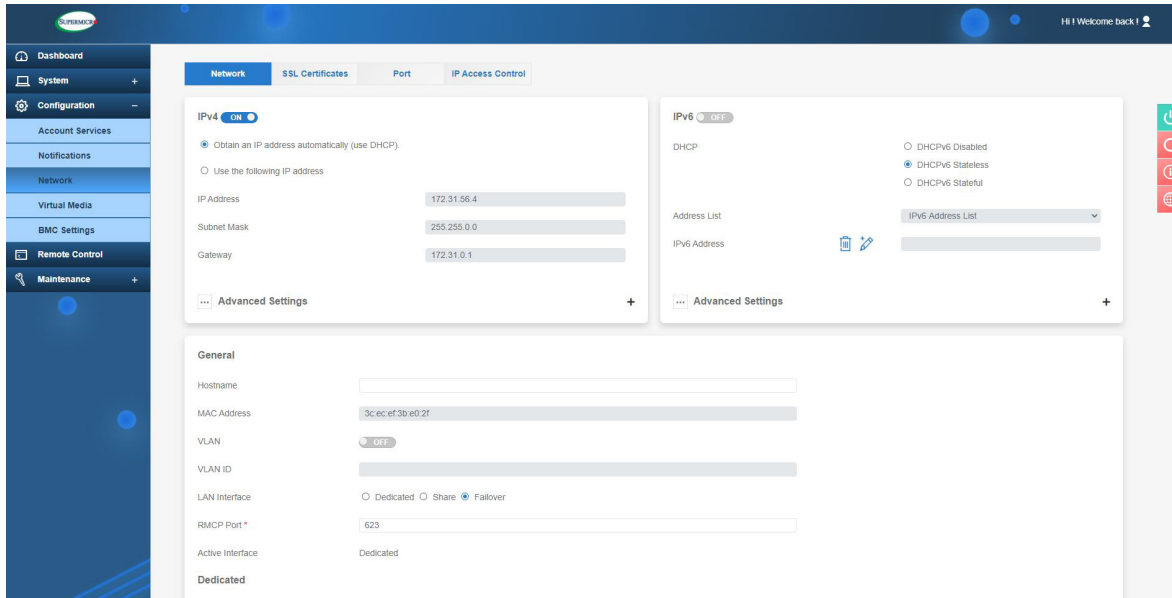
The screenshot displays the SMTP configuration page. At the top, there are navigation tabs: Alerts, SNMP, Syslog, and SMTP (highlighted in blue). Below the tabs, the page title is "SMTP". The configuration area contains several fields and options:

- Server Address \***: An empty text input field.
- Port Number \***: A text input field containing the value "587".
- Connection Protocol**: A group of radio buttons with options: AutoDetect, None (selected), StartTLS, and TLS\_SSL.
- Authentication**: A group of radio buttons with options: AutoDetect, CRAM\_MD5, Login, None (selected), and Plain.
- User Name**: An empty text input field.
- Password**: An empty text input field with a small blue eye icon to the right, used for toggling password visibility.
- Sender's Address**: An empty text input field.

At the bottom of the configuration area, there is a large, prominent blue button labeled "Save".

## 2.6.3 Network

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



### IPv4

- ON: You can enable/disable the IPv4 network connection for BMC.
- Obtain an IP address automatically (use DHCP): You can select this option to configure the IPv4 address automatically through DHCP (Dynamic Host Configuration Protocol).
- Use the following IP address: You can select this option to set up a static IP address by entering the following details.
  - IP Address – Manually entering the IPv4 address for BMC
  - Subnet Mask – Enter the IPv4 Subnet Mask Value
  - Gateway – Enter the IPv4 Gateway address

### IPv4 Advanced Settings



DNS Server IP: You can enter DNS Server IP to retrieve hostname from the DNS (Domain Name Server).

## IPv6

- ON: You can enable/disable IPv6 network connection for BMC.
- DHCPv6 Disabled: You can choose this option to disable the DHCPv6 Stateful connection.
- DHCPv6 Stateless: When selected, BMC will NOT apply the prefix/IPv6 address from the DHCPv6 server.
- DHCPv6 Stateful: When selected, BMC will apply the prefix/IPv6 address from the DHCPv6 server.



**Note:** When DHCPv6 Stateful is selected and Auto Configuration is disabled, 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. Hence, Auto Configuration must be enabled (ON) for BMC to receive IPv6 IP address(es) when DHCPv6 Stateful mode is selected.

- Address List: The drop-down lists all the possible IPv6 address(es) on the BMC network interface that is currently available. Link-local address is also included.
- IPv6 Address: You can take the following actions.
  - Add IP  – Add static IPv6 address. Please note that the prefix length is required.
  - Delete IP  – When selected, the IP address in IPv6 Address field will be deleted.



**Note:** Only Static IPv6 Address can be deleted.


## IPv6 Advanced Settings

- Auto Configuration: You can select auto configuration ON or OFF. When checked, BMC will calculate a stateless auto configuration address based on the prefix information from RA. Auto Configuration must be enabled (ON) when users want to enable either DHCPv6 stateless or DHCPv6 stateful mode.



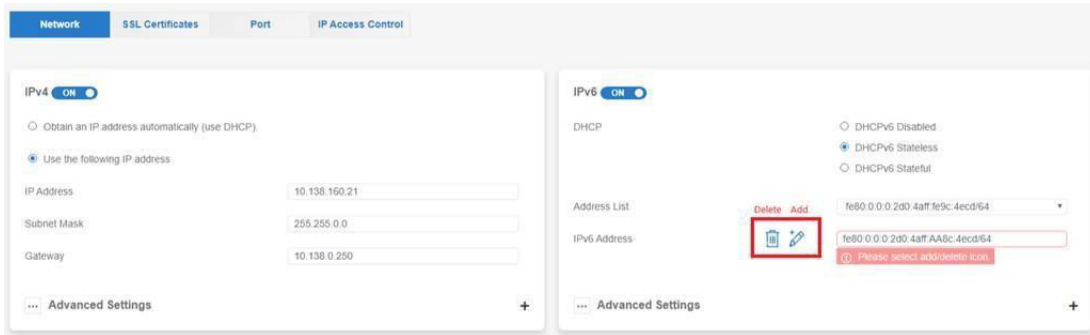
**Note:** To disable IPv6 addresses from getting DHCPv6 Stateless, users must toggle the button to OFF.

- DNS Server IP: You can assign a DNS server IP address in IPv6 form.
- DUID: You can use the Unit ID to get the DHCP IP from the DHCP server. The DUID includes client network information (address, lease time, and DNS server info). This is READ ONLY.

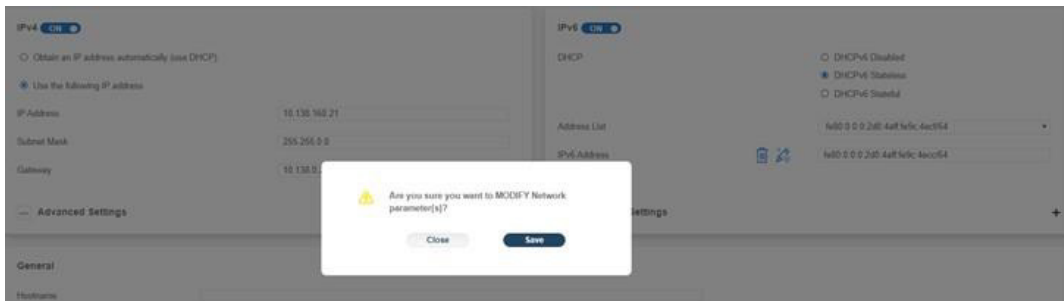
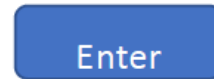
- **Enable Static Route:** When enabled, the route rules listed in Static Route List will be applied to the IPv6 routing table.
- **Static Route List:** You can view the static route list.
- **Prefix to Route:** You can input the prefix to route in this field. While there is an IPv6 packet whose destination address fits the Prefix to Route, the packet will be destined via the specific router which is defined in the Router Address field. Please note that the prefix length is required.
- **Delete Static Route ** : You can choose this option to delete the route rule selected at Static Route List drop down.
- **Router Address:** You can input the router address in this field. While there is an IPv6 packet whose destination address fits the Prefix to Route, the packet will be destined via the specific router which is defined in the Router Address field.

## Additional Reference Steps to Add/Delete IPv6 Address

To add an IPv6 address, refer to the following steps.



1. Select add icon.
2. Input the address to be configured.
3. Save.



The updated address will appear on the Address List.



To delete an IPv6 address, refer to the following steps.

1. Select add icon.

Enter

2. Input the address to be configured.

The screenshot shows the IPv6 configuration panel. At the top, the IPv6 toggle is set to 'ON'. Under the 'DHCP' section, 'DHCPv6 Stateless' is selected with a radio button. The 'Address List' dropdown menu is open, showing the address 'fe80:0:0:0:2d0:4aff:fe9c:4ecf/64'. Below it, the 'IPv6 Address' input field also contains the same address. At the bottom left, there is an 'Advanced Settings' link, and at the bottom right, there is a plus sign icon.

3. Save.

This screenshot shows the same IPv6 configuration interface as the previous one, but with a confirmation dialog box overlaid in the center. The dialog box has a yellow warning icon and the text: 'Are you sure you want to MODIFY Network parameter(s)?'. Below the text are two buttons: 'Close' and 'Save'. The background configuration is dimmed.


The updated List address will disappear from the address list as shown below.

The screenshot shows the IPv6 configuration panel. The 'Address List' dropdown menu is open, displaying a list of items. The first two items are 'IPv6 Address List -'. The third item is 'fe80:0:0:0:2d0:4aff:fe9c:4ecc/64', which is highlighted in blue. The 'IPv6 Address' field below is empty. The 'Advanced Settings' link and plus sign icon are visible at the bottom.


## General

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

- 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. Hence, except for hyphens, no special characters are not allowed. All hostnames must be 63 characters or shorter in length.

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

 **Note:** By default, VLAN ID is preset to 1 when VLAN is enabled. Users need to make sure the BMC interface was set to a member of VLAN 1 prior to saving the setting if the VLAN ID was decided to be set to 1. Otherwise, once the configuration is saved, users would lose access to BMC via OOB unless the BMC interface is connected to a Switch port which is configured as VLAN 1.)

- LAN Interface: You can select the type of LAN interface.
  - Failover
  - Dedicated
  - Shared
- Shared LAN: You can select one of the LAN modes.
  - Auto
  - Onboard
  - AIOM
  - AOC



Network Mode Table	
Network Combination Mode	Definition
Dedicated	“Dedicated” LAN
Shared (Auto Mode)	Onboard Shared LAN or AIOM Shared LAN if no Onboard Shared LAN designed in.
Failover (Auto Mode)	Failover between the first Shared LAN and Dedicated LAN
Shared - AIOM	AIOM Shared LAN
Shared - AOC	AOC Shared LAN
Failover - AIOM	Failover between “Shared - AIOM” and “Dedicated”
Failover - AOC	Failover between “Shared - AOC” 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 select one of the following link speeds.
  - 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.

## Network General Frame of WebUI

Dedicated	
Link	<input checked="" type="radio"/> Auto Negotiation <input type="radio"/> 100M Half Duplex <input type="radio"/> 100M Full Duplex <input type="radio"/> 1G Full Duplex
Status	Connected
Speed	1G
Duplex	Full Duplex

### LAN Interface when in Dedicated Mode

Active Interface	Share
<b>Share</b>	
Status	Connected
Speed	1G
Duplex	Full Duplex

### LAN Interface is in Shared Mode



**Note:** 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 display LAN Interface. On the next page is some special X13 motherboards.

Motherboard	MAC3	MAC4
X13DEM	AIOM	AOC
X13DET_B	AIOM	AOC
X13OEI	Onboard	AIOM
X13SEDW_F	AIOM	AIOM and AOC
X13SEFR_A	AIOM	AIOM and AOC
X13SEM_TF	Onboard and AOC	AOC



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

## Web UI LAN Design for X13

Shared LAN Auto and NCSI Shared LAN will stay in MAC3 unless MAC3 is down. When MAC3 is down, BMC will then switch to MAC4 and stay in MAC4 even when MAC3 is back. LAN Web UI can now be dynamically retrieved from Redfish API. Hence, when there is no Onboard Dedicated LAN, Shared LAN is used. Only active and available LAN Interface is ENABLED and shown. Thus, inactive and non-available LAN Interface are to be hidden.

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

There are five special scenarios to consider for non-LOM (non-LAN-on-Motherboard).

1. When X13SEDW is installed to AIOM, BMC will display the following.




**Note:** Not all AIOM2 can be used as Shared LAN.

- LAN Interface
    - Dedicated
    - Shared
    - Failover
  - Shared LAN
    - Auto Mode
    - AIOM1
    - AIOM2
2. When X13SEFR is installed AIOM1 but the second NCSI is a jumper, BMC will not be able to differentiate which device is AOC or AIOM. Hence, it will display Shared LAN on WebUI as follows.

- LAN Interface
  - Dedicated
  - Shared
  - Failover

- Shared LAN
    - Auto Mode
    - AIOM
    - AOC
3. When AIOM is installed in X13DEM and the second NCSI only supports AOC, BMC will display AIOM and AOC on WebUI as follows.
- LAN Interface
    - Dedicated
    - Shared
    - Failover
  - Shared LAN
    - Auto Mode
    - AIOM
    - AOC
4. When X13SEED does not have the Dedicated and Failover options, BMC will display AOCs on WebUI as follows.
- LAN Interface
    - Shared
  - Shared LAN
    - Auto Mode
    - Onboard
    - AOC
5. When X13SEDW-F has two AIOM and one AOC installed, thus does not have the Dedicated and Failover options, BMC will show AOCs on WebUI.
- LAN Interface
    - Shared

- Shared LAN
  - Auto Mode
  - AIOM1
  - AIOM2
  - AOC

 **Note:** BMC can use VPD to determine which names to be shown. If BMC gets the string “AOC-S” in VPD, then the NIC card will be a standard PCI-E card and BMC will show the NIC card as an AOC. If BMC gets string “AOC-A”, the NIC card will be the AIOM card and BMC will show it as AIOM2.

**General**

Hostname	<input type="text" value="LukeX13SEFRA101"/>
MAC Address	<input type="text" value="3c-ec-ef-34-91-45"/>
VLAN	<input checked="" type="radio"/> OFF
VLAN ID	<input type="text" value="0"/>
LAN Interface	<input type="radio"/> Dedicated <input type="radio"/> Share <input checked="" type="radio"/> Failover
Share LAN	<input type="checkbox"/> Auto Mode <input checked="" type="radio"/> AIOM1 <input type="radio"/> AIOM2

**General**

Hostname	<input type="text" value="LukeX13SEFRA101"/>
MAC Address	<input type="text" value="3c-ec-ef-34-91-45"/>
VLAN	<input checked="" type="radio"/> OFF
VLAN ID	<input type="text" value="0"/>
LAN Interface	<input type="radio"/> Dedicated <input checked="" type="radio"/> Share <input type="radio"/> Failover
Share LAN	<input type="checkbox"/> Auto Mode <input checked="" type="radio"/> AIOM1 <input type="radio"/> AIOM2
Active Interface	Dedicated

---

**Sample Web UI for X13XEFR**

## SSL Certificates

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

- Certification Valid From and Until: You can view current SSL certification validity in the greyed-out fields.
- New SSL Certificate: You can upload a new SSL Certificate by clicking on the 'Select File' button to select a supported SSL Certification 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, the BMC will reset itself for the new certificate to take effect.



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

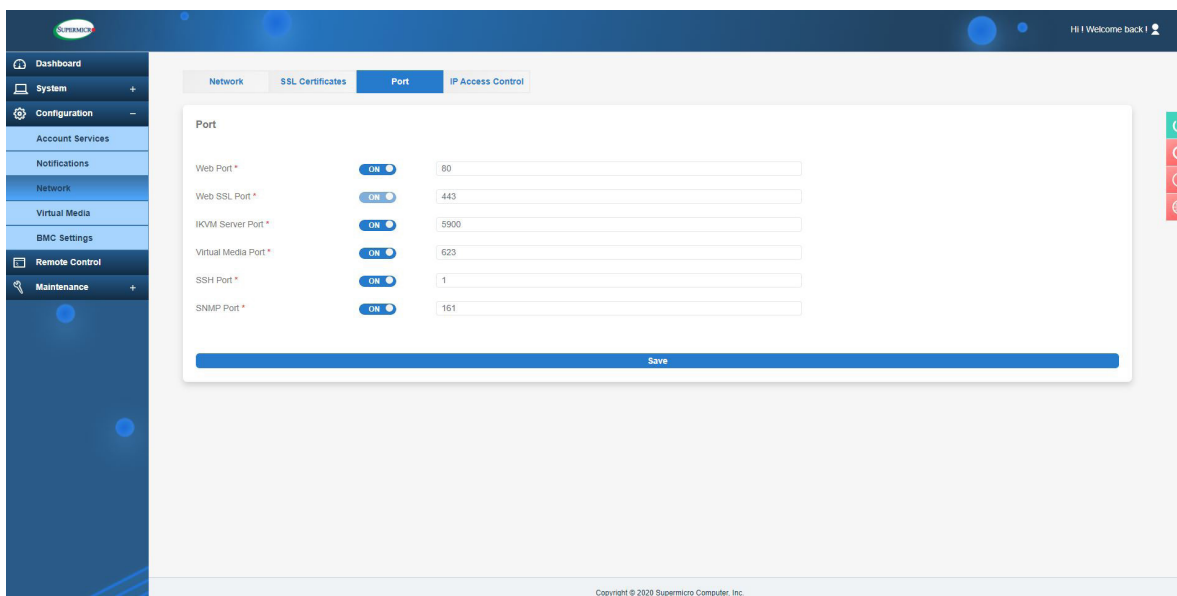
The screenshot shows the BMC Settings interface for SSL Certificates. The left sidebar contains navigation options: Dashboard, System, Configuration, Account Services, Notifications, Network, Virtual Media, BMC Settings, Remote Control, and Maintenance. The main content area is titled 'SSL Certificates' and includes the following fields and controls:

- Network, SSL Certificates, Port, IP Access Control (tabs)
- SSL Certificates (title)
- Certification Valid From: Aug 19 00:00:00 2020 GMT
- Certification Valid Until: Aug 19 00:00:00 2023 GMT
- New SSL Certificate: Select File
- New Private Key: Select File
- Two warning messages: Certificate file should end with .pem or .cer.
- Upload button

Copyright © 2020 Supermicro Computer, Inc.

## Port

This tab provides the following ports along with the associated standard port numbers. Most ports can be modified, except Web SSL Port. Users can turn ON an individual port to modify the port number. Click on [Save] to apply changes.



The default states and numbers for TCP ports are as follow.

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

The default states and numbers for UDP ports are as follow.


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

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




The screenshot displays the 'Port' configuration page in a BMC interface. It features a navigation bar with tabs for 'Network', 'SSL Certificates', 'Port', 'IP Access Control', and 'SSDP'. The 'Port' tab is active. Below the navigation bar, there are two sections: 'TCP Ports' and 'UDP Ports'. Each section contains a list of ports with their respective status (ON/OFF) and a text input field for the port number. A 'Save' button is located at the bottom right of the configuration area.

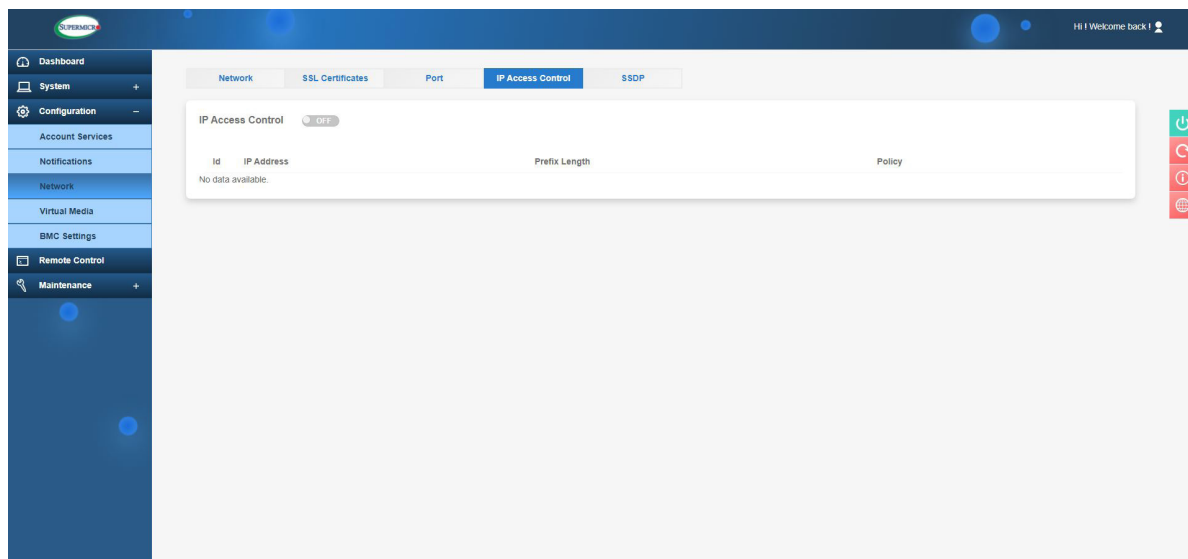
Port Name	Status	Port Number
IKVM Server Port *	ON	5900
SSH Port *	ON	22
Web Port *	ON	80
Web SSL Port *	ON	443
Virtual Media Port *	ON	623
UDP Ports		
IPMI LAN Port *	ON	623
SNMP Port *	OFF	161

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

## IP Access Control

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



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



In the IP Access Control frame, you can view the following access control information.

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

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 .

The following rules apply to ACCEPT and DROP policies.

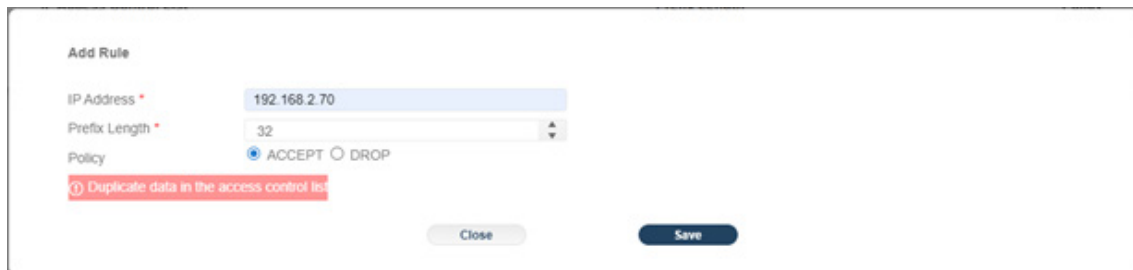
- You can set your own preferred policies.
- BMC Web UI will follow ID order. BMC always follows the previous ID number when you set a new policy.
- You can add the same IP Address with different prefixes to the same policy of either ACCEPT or DROP. BMC Web UI will still follow ID order.
- If you add 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 pressing [Save]. See the examples below for details.



IP Access Control **ON**

Add

Id	IP Access Control List	Prefix Length	Policy	
1	192.168.2.70	32	Accept	 



**Add Rule**

IP Address

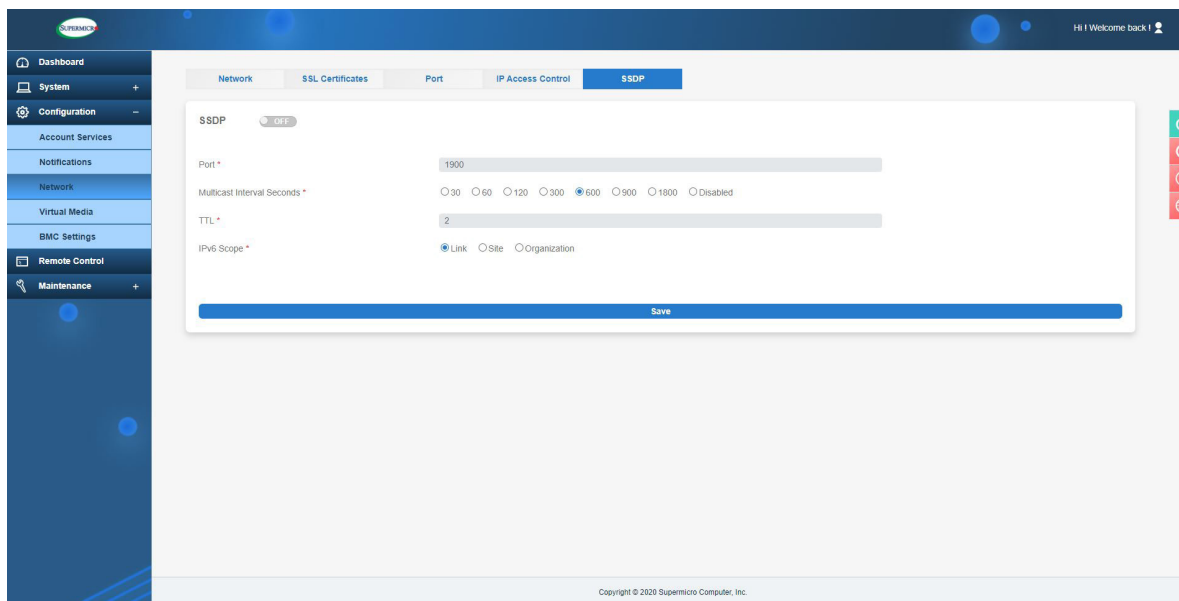
Prefix Length

Policy  ACCEPT  DROP

**Duplicate data in the access control list**

## SSDP (Simple Service Discovery Protocol)

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

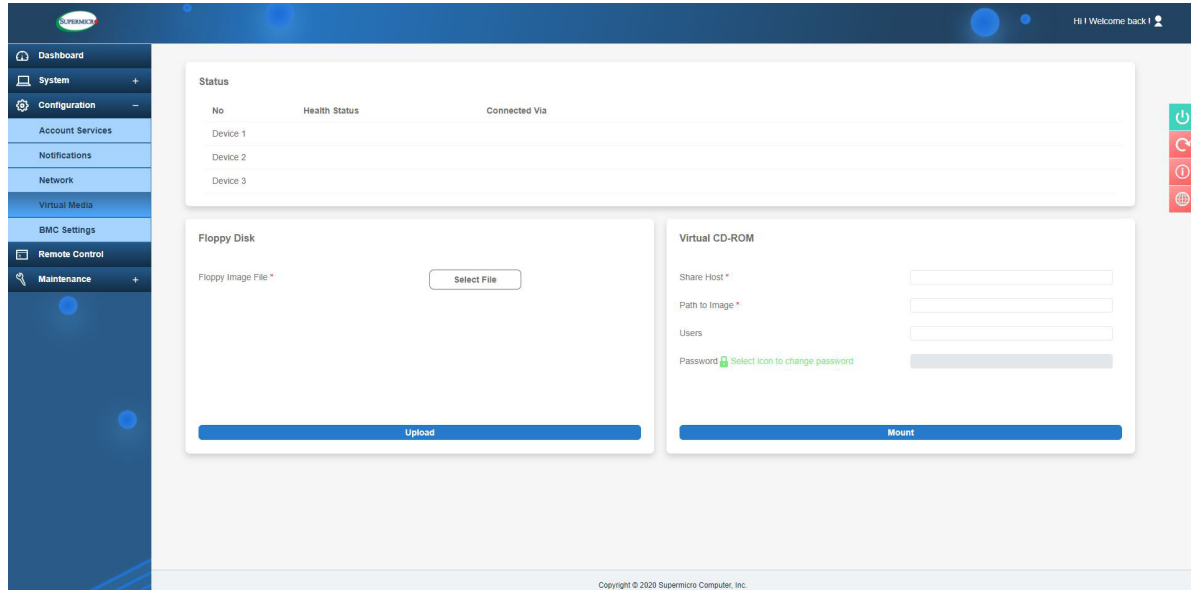


You can enable or modify SSDP with the following settings on this page.

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

## 2.7.4 Virtual Media

Use this page to upload a floppy or CD-ROM image and check the status of connected devices respectively.



### Status

This field displays the status of currently connected devices such as floppy/USB flash and/or CD-ROM/ISO devices. You can also disconnect respective devices.

### Floppy Disk

To upload the floppy image file, refer to the following steps.

1. Choose File: You can upload a floppy image. The allowed file types include img and .ima type files.
2. Upload: You can click on [Upload] to upload the image file to the server.

## Virtual CD-ROM

- Share Host: The host server is for the console redirection. This will only accept the following character classes as part of the URL domain name.
  - a through z
  - A through Z
  - 0 through 9
  - Special characters (e.g., – and .)

Moreover, the domain part will only accept http:// or https:// at the beginning (e.g., HTTP+ IP Address and HTTPS + IP Address). Port numbers can be used after IP Address as an option. For example: http(s):/192.188.8.8:443 for the IPv4 Address and http(s):/[2021::8888:443].

- Path to Image: The Path of the CD-ROM image file will only accept the following character classes.
  - a through z
  - 0 through 9
  - Special characters (e.g., @ ^ / . - \_)

All other special characters will be rejected, including space and tab. Slashes (/ and \) should only be accepted when used alone and not repeated or used repeatedly. This means you cannot use /, \, ^, and \\. The path must be started with / or \* character and ends with “.iso” file extension.

- Users: This feature allows you access to the CD-ROM image files and will only accept the following character classes. All other special characters, including space and tab, will be rejected.
  - a through z
  - A through Z
  - ^
- Password: This feature will only accept the following character classes. All other special characters, including space and tab, will be rejected.
  - a through z

- A through Z
- 0 through 9
- ^



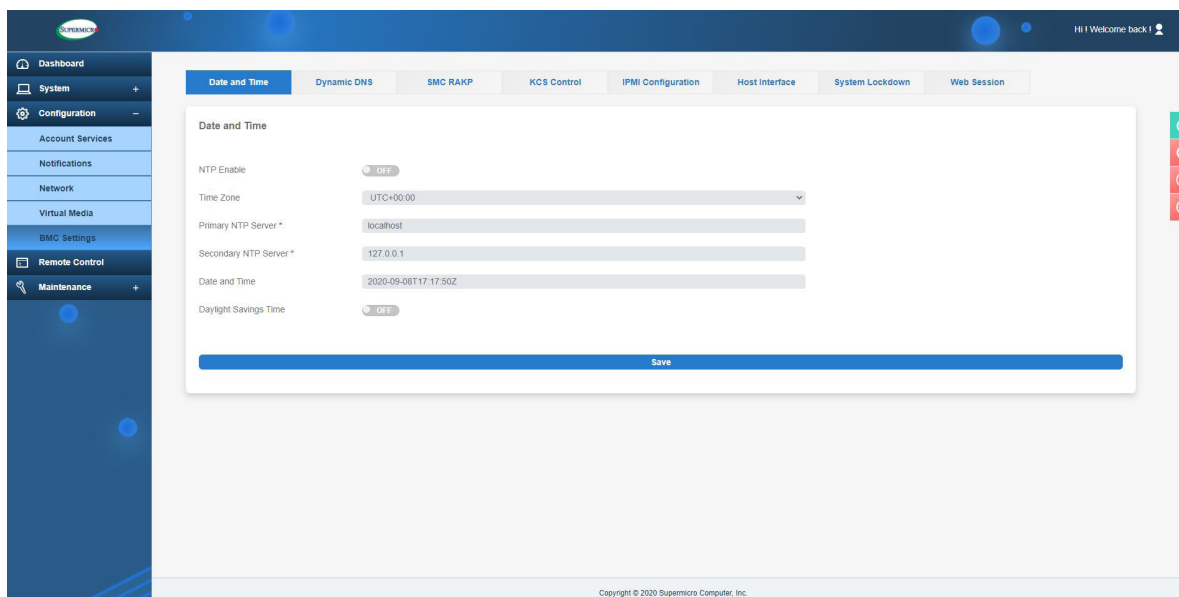
**Note:** CD-ROM mounting supports HTTP, HTTPS, Samba, and the Windows CIFS method.

Virtual Media (VM) License						
	SMBV2	SMBV3	CIFS	SAMBA	HTTP	HTTPS
Current X13 License	STANDARD	STANDARD	STANDARD	STANDARD	SFT-OOB-LIC	SFT-OOB-LIC

## 2.6.4 BMC Settings

### Date and Time

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



You can adjust the following fields.

- **NTP Enable:** You can enable or disable NTP server settings. If NTP is disabled, the system time is used to set the date and time. 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 system time (e.g., from BIOS). If NTP was enabled and BMC has been using NTP for 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. A log will be sent to 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 +12:00 hr.



- Primary NTP Server: You can enter primary NTP server info.
- Secondary NTP Server: You can enter secondary NTP server info. This is optional.
- Date/Time: You can view the time in HH:MM:SS format.
- Daylight Savings Time: You can turn ON this field for applying 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.

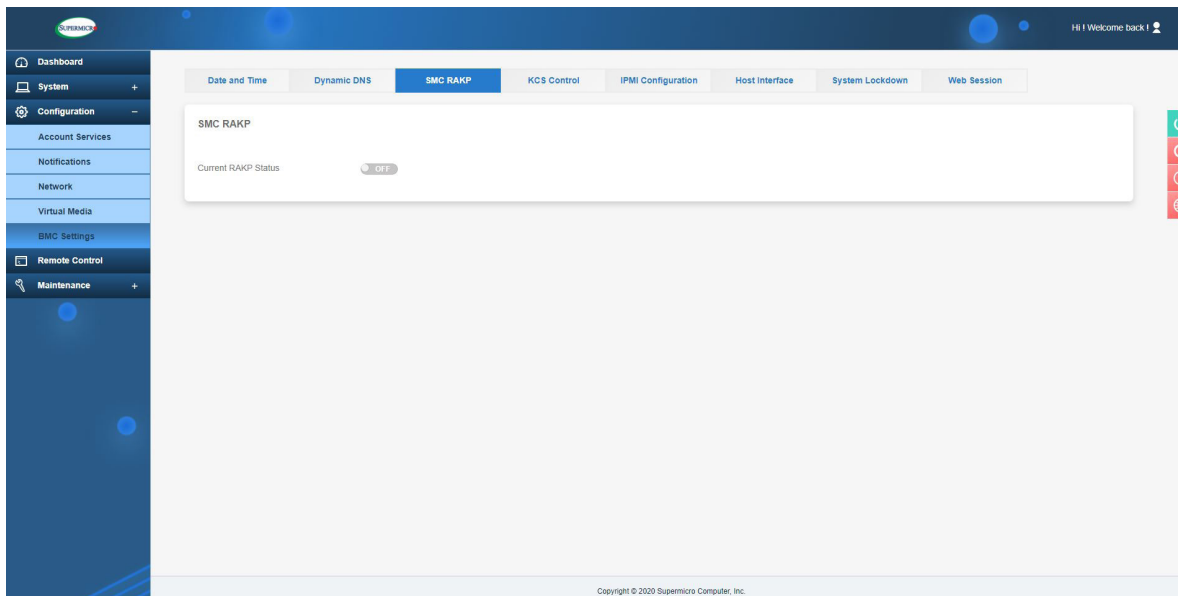
- Dynamic Update Enable: You can enable/disable Dynamic DNS update support.
- Dynamic DNS Server Address: You can view the server address of your Dynamic DNS server.
- BMC Hostname: You can name the BMC (Baseboard Management Controller) host server.
- TSIG Authentication: You can enable TSIG (Transaction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



**Note:** Fields with \* are optional.

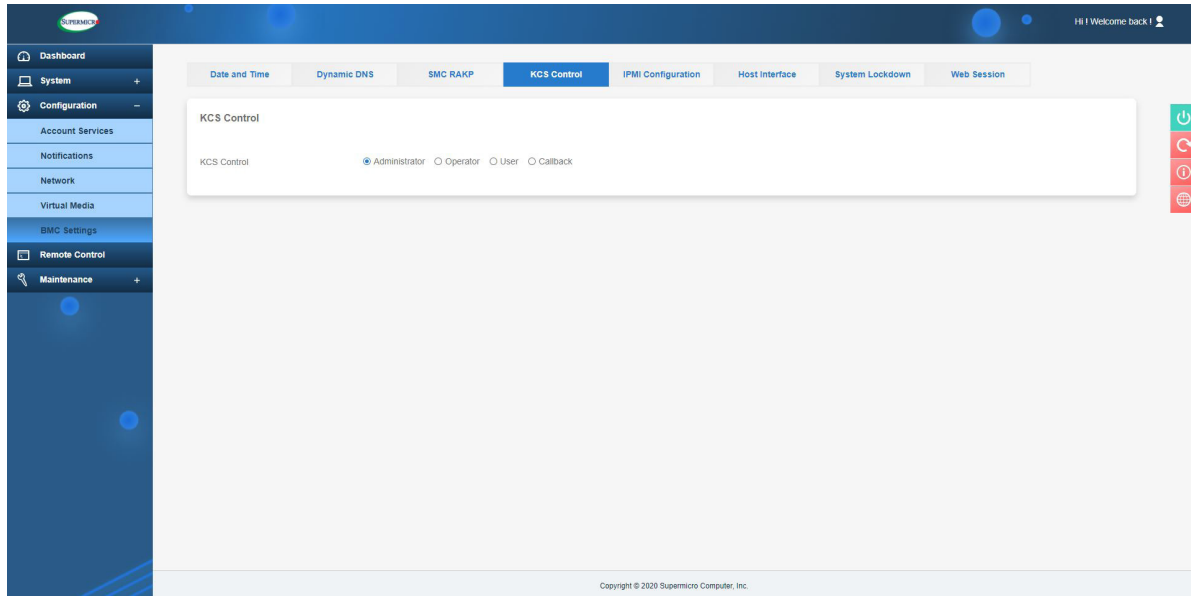
## SMC RAKP

This page allows you to enable or disable the Supermicro-supported RAKP (Remote Authenticated KeyExchange Protocol).



## KCS Control

This feature allows you to secure your environment by configuring appropriate privileges to access the KCS interface.



You can select one of the following options to configure the appropriate privileges for users to access the KCS interface. The supported privileges include the following.

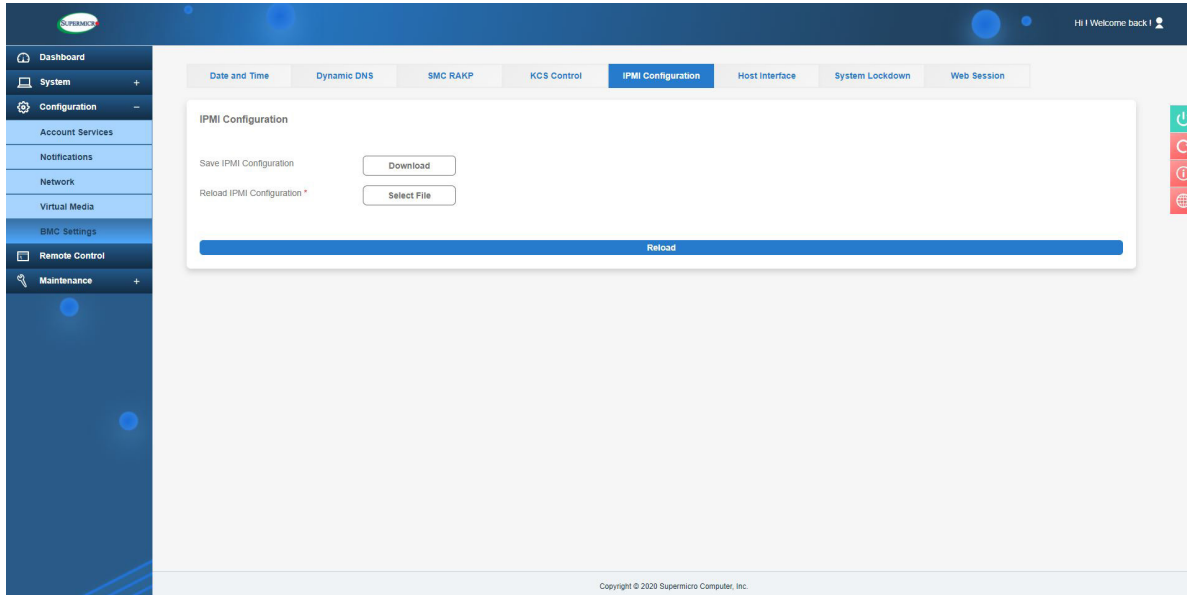
- Administrator: Any user accessing the KCS interface will be able to do all the operations that an administrator user can do.
- Operator: Any user accessing the KCS interface will be able to do all the operations that a user with Operator privilege can do.
- User: Any user accessing the KCS interface 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.

## IPMI Configuration

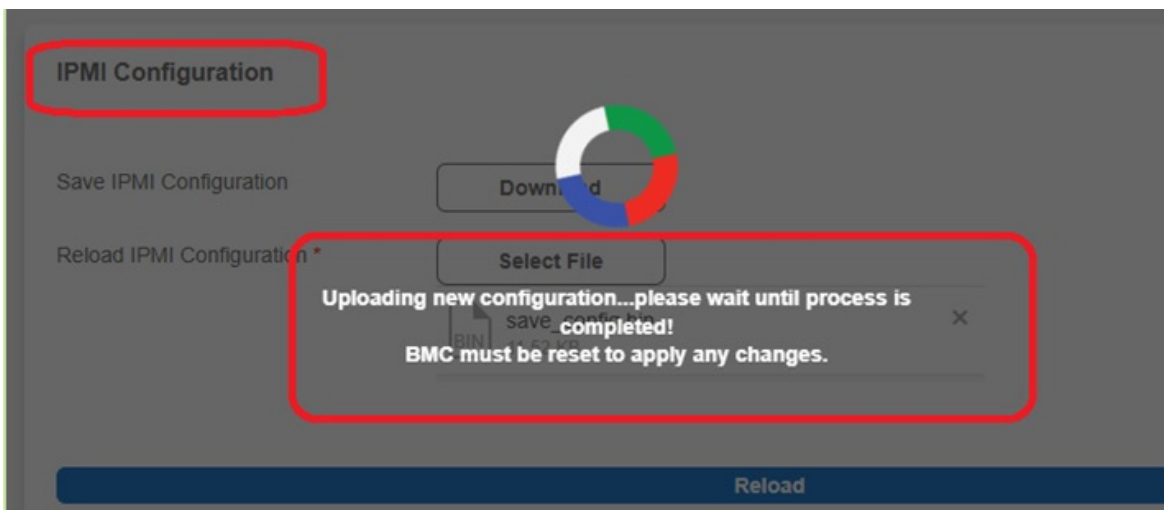
You can use this page to save or restore IPMI configuration settings.



**Note:** The saved IPMI Configuration option will download the IPMI configuration .bin file.

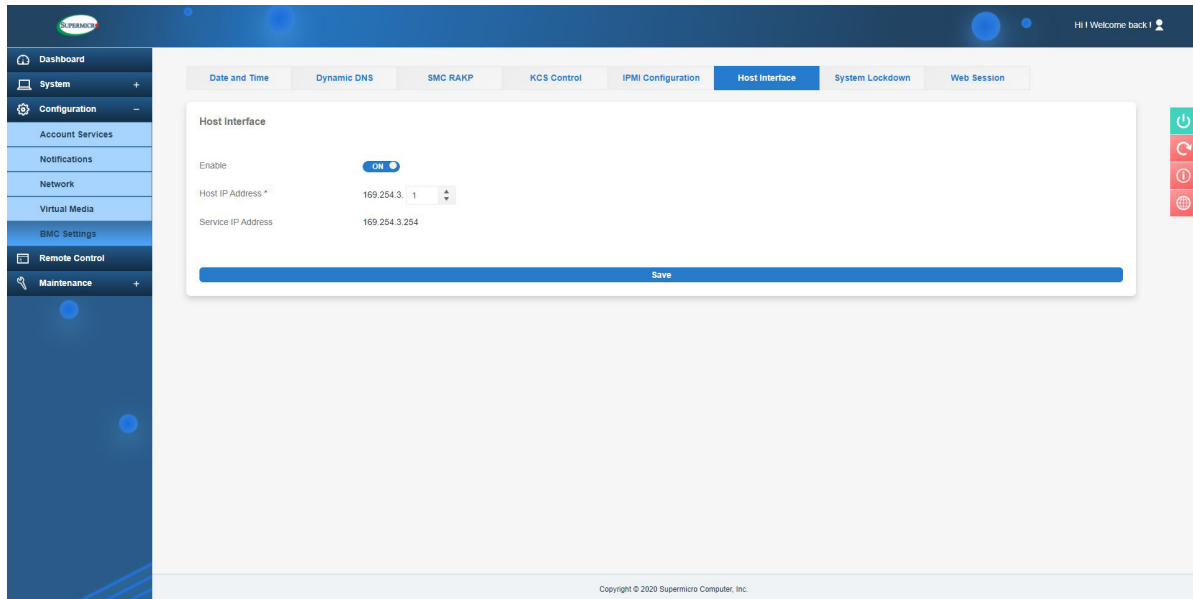


If the file is good, you will receive the prompt message: "Uploading new configuration...please reconnect once process is completed! BMC must be reset to apply new changes." If the file is corrupted, you will receive the prompt message: "Corrupted file! Click here to return". If the file is not the correct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



## Host Interface

The Host Interface (HI) provides an Ethernet over USB solution, which has the ability to connect Ethernet devices via USB.



You can adjust the following fields to configure the host interface.

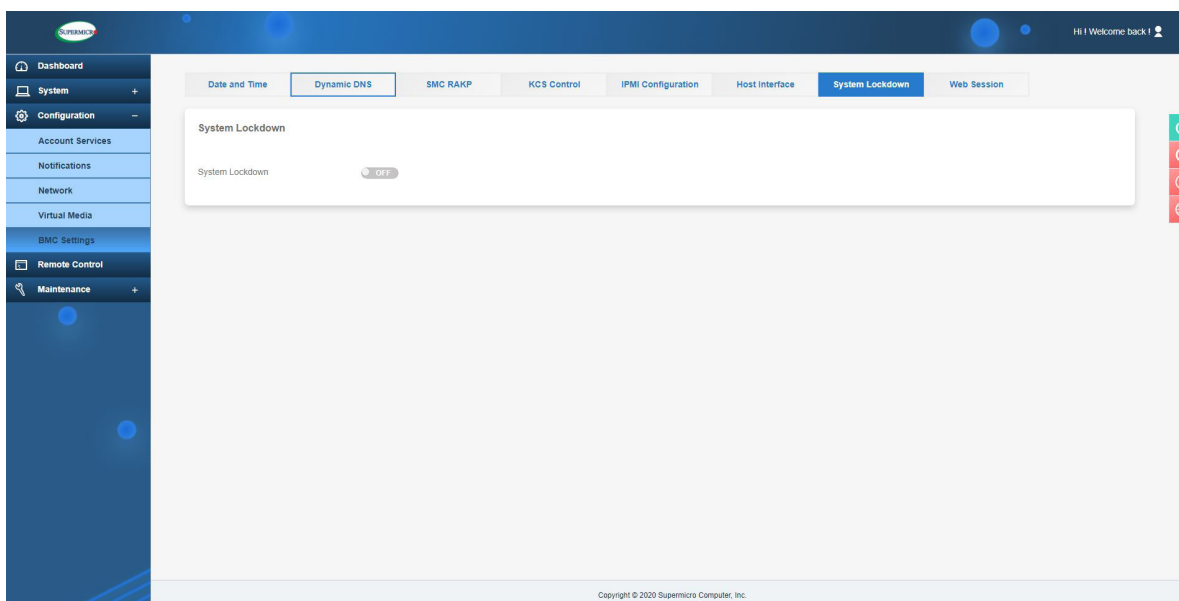
- Enable: You can enable or disable this service.
- Host IP Address: You can set up a host IP address that is assigned to the host OS.
- Service IP Address: You can view the management host interface service IP. This is READ ONLY.

## System Lockdown

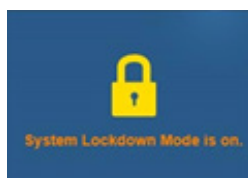
System lockdown will prevent unintentional system configuration changes when the system is running. When the system lockdown is turned on, all system configuration changes (including firmware updates) will be prevented and you will be notified accordingly.



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



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

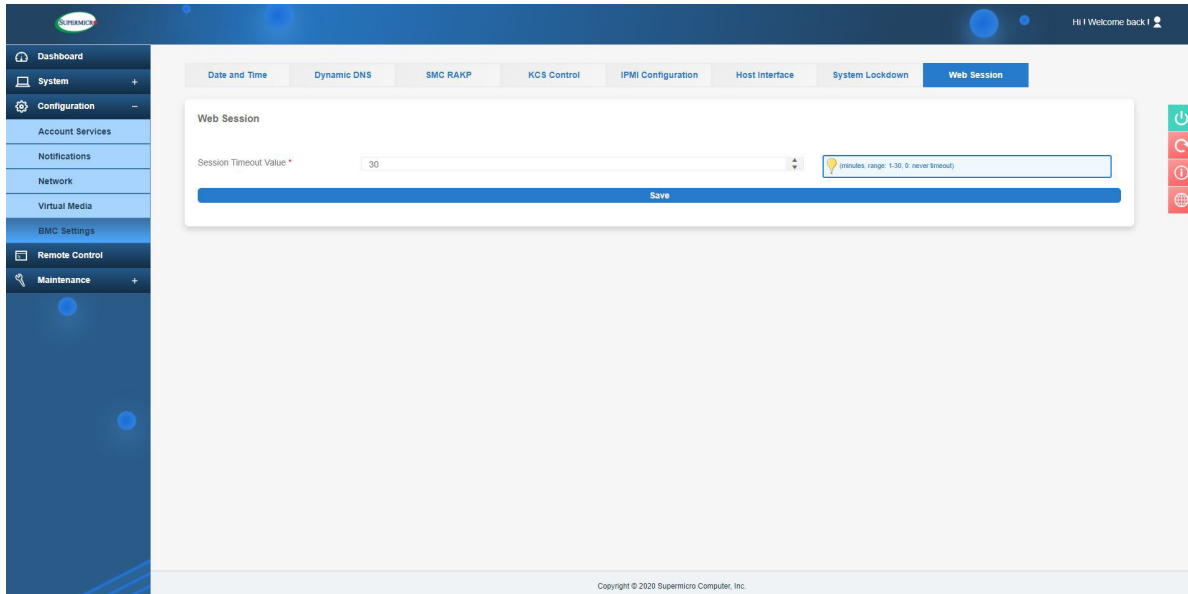


The following features will be functional during the system lockdown.

- System power operations (Power On, Power Off, Reset)
- Identify operations (chassis identify)
- IPMI configuration download
- Maintenance events download
- UID control

## Web Session

You can set the web session timeout to a value from 1 to 30 (minutes); or set it to 0 for no timeout. The default timeout value is 30 minutes.



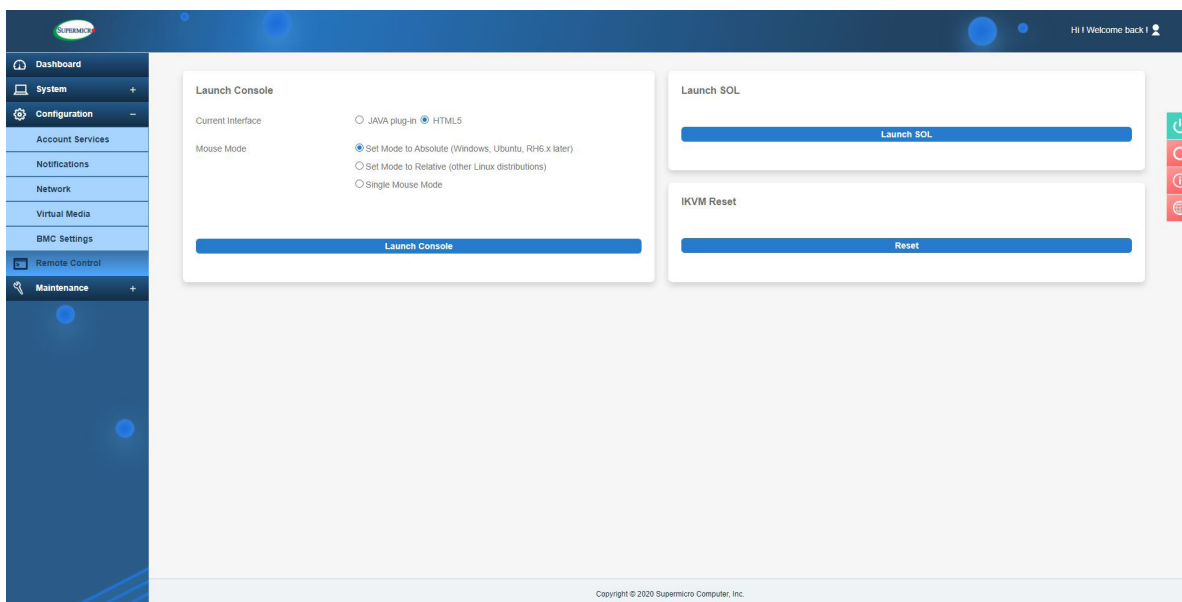
## Smart Power

Currently, you can turn on or enable Smart Power Option for the “Big Twin” and “H12DST-B” systems on this page. Additional supported systems will be added accordingly. 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 can be enabled or disabled using the ON/OFF button, a feature that 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 sending a surplus of power into the system. In those cases, IPMI/BMC will find out the power supply and set the CPU power limit. ‘Enable Smart Power Event Log’ allows users to show Smart Power logs on supported platforms.

## 2.7 Remote Control

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



### Launch Console

Use this page to launch or configure current remote console interface settings. You can select the JAVA plug-in or HTML5 interface.

**Note:** HTML5 is the default selection for X13 platforms. If you decide to change the remote console interface, it will prompt the message, “Once a remote console session is connected, switching between JAVA and HTML5 is not allowed.” The maximum number of sessions for either Java or iKVM console is four. Hence, when there are more than four sessions open, there it will prompt the message, “The maximum number of open sessions has been reached!”

To launch a remote console via the default, Java, refer to the following steps.

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

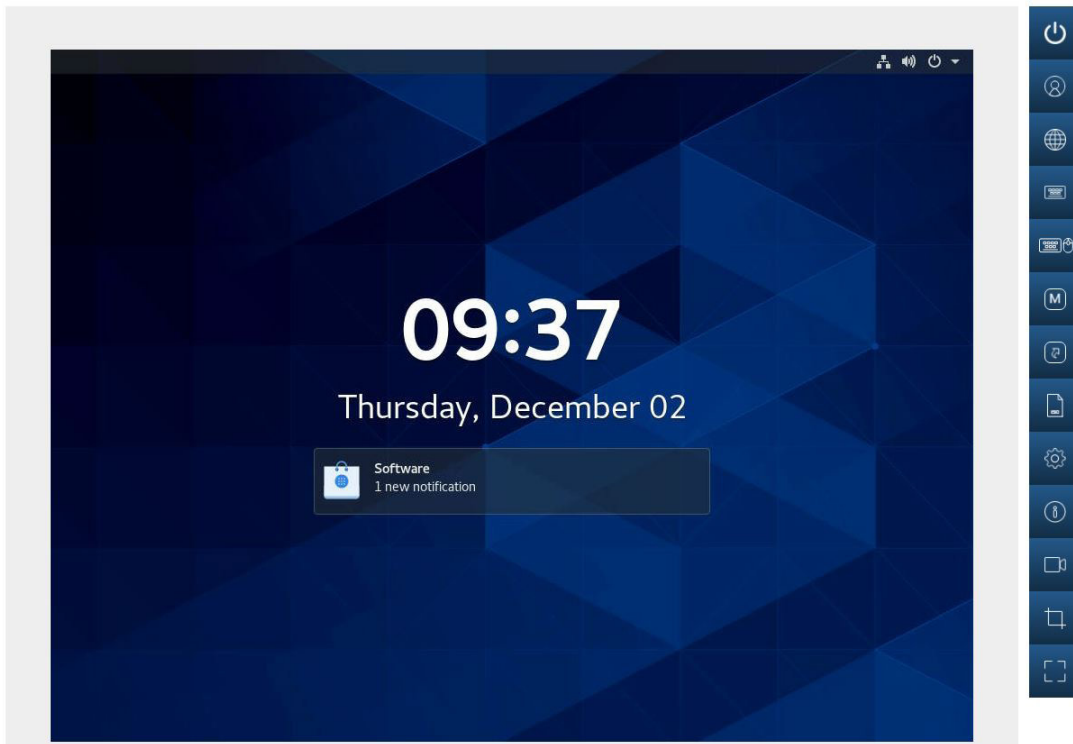


To launch a HTML5 remote console, refer to the following steps.

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



**Note:** Video recording only works with Chrome browser.



## Mouse Mode

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

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



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

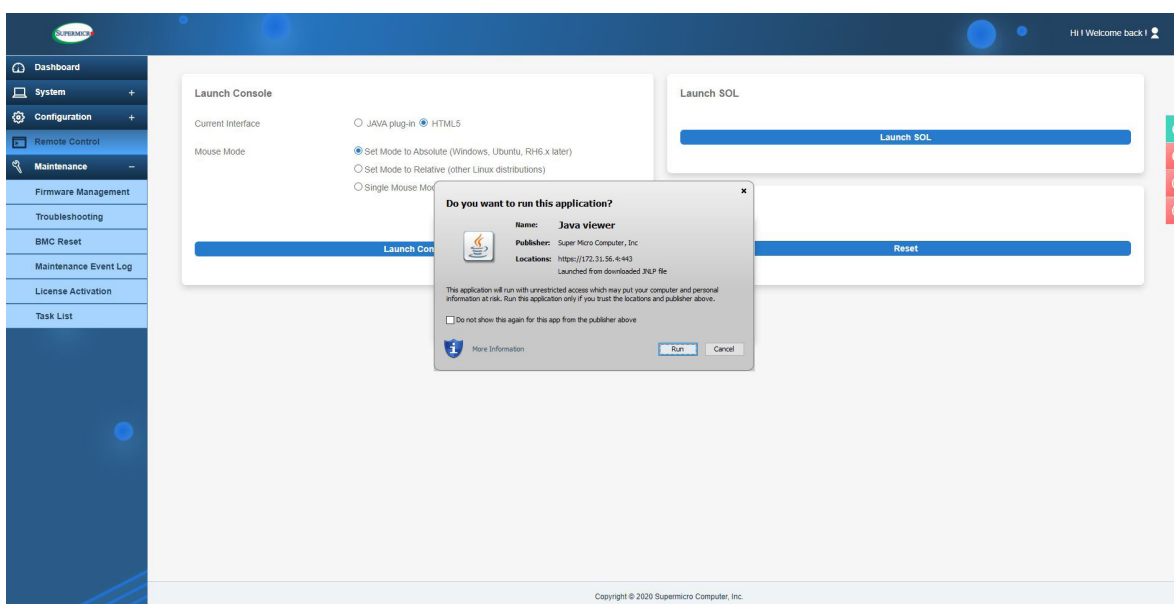
## Launch SOL

This page allows you to launch a remote console using SOL (Serial over LAN), which provides serial port connections over LAN to access a host server via console redirection. It also allows the system administrator to monitor and manage servers from a remote site. In order to connect the console through SOL, please consider the following setups.

- Console redirection must be enabled in BIOS.
- The remote system has been configured properly based on the operating system in use.



**Note:** SOL function will be disabled when IPMI LAN Port is turned OFF.



## iKVM Reset

This option allows you to reset iKVM, which will reset the virtual media, iKVM keyboard, and mouse.

## 2.7.1 Console Redirection

This feature allows you to launch Console Redirection via IKVM (keyboard, video/monitor, mouse) support. Refer to page 95 on how to first launch the Remote Console. Refer to the image for the options available. The same descriptions for each icon are displayed when the mouse hovers over it.



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.

### Power Control

- Power Down - Immediately
- Graceful Shutdown
- Power Cycle
- Power Reset



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 that are currently accessing the HTML5-iKVM.

### User List

Session ID	User Name	IP Address
258	ADMIN	010.001.035.207

[Close](#)

## 2.7.1c Console Redirection – Language

This feature allows you to configure the language setting and select one of the following support languages.

### Language Setting

- English
- 日本語
- 简体中文
- 한국어
- Deutsch
- Français
- Español
- Italiano

Close

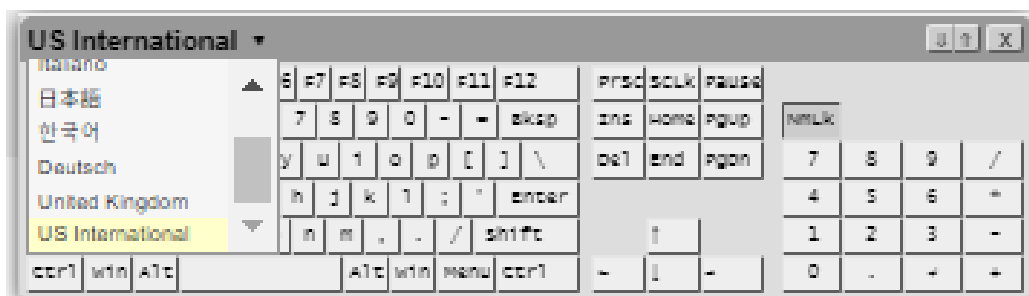
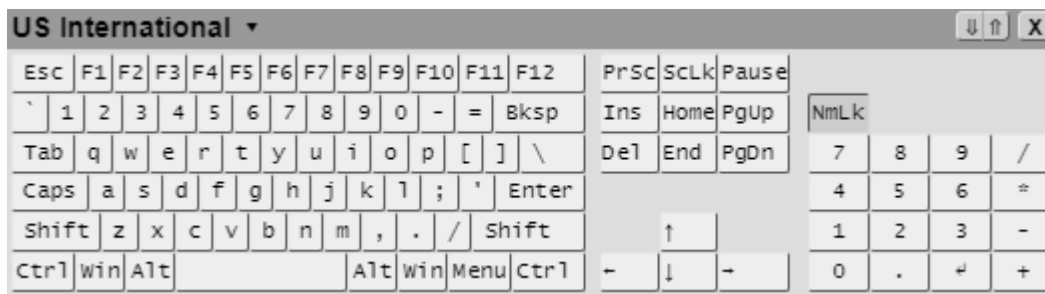
Apply

- 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



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 be using a US-international virtual keyboard regardless of whether any of the supported languages are set. Please also note that due to language differences in size and shape, the sizes of supported virtual keyboards will be varied. Thus, 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.

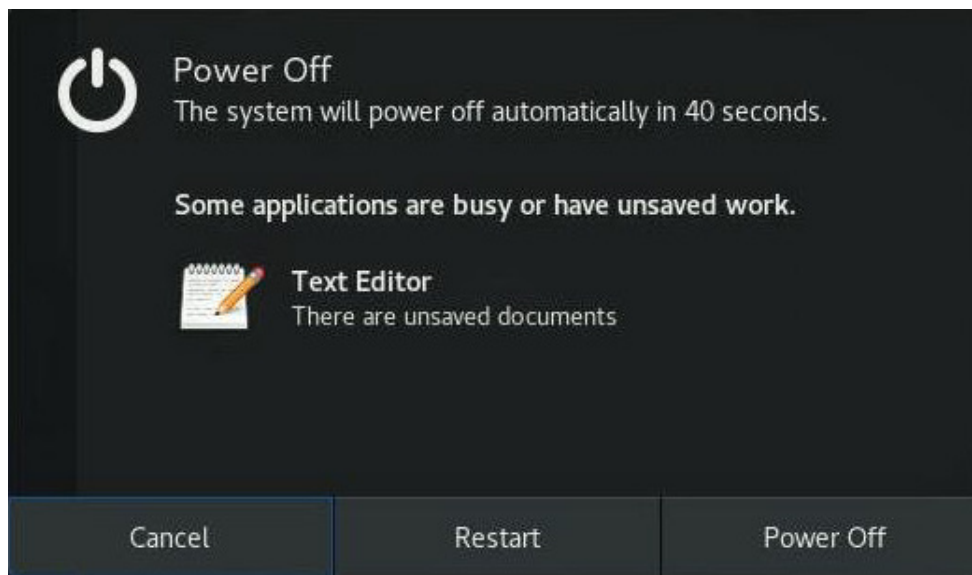


**Note:** The action of this function is on the server side, not the client's side. The server side is the server on which BMC is installed.

## 2.7.1f Console Redirection – Macro

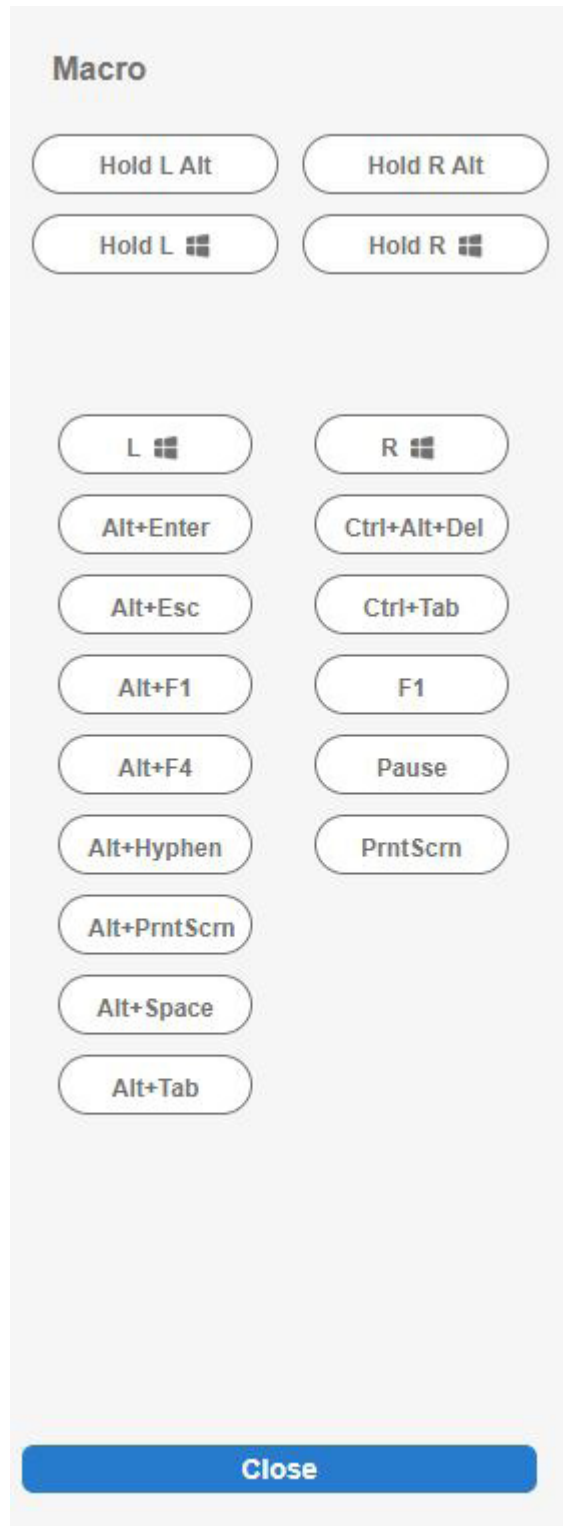
This feature provides you the ability to set up patterns or rules for hotkeys and other function keys. However, you can use the 19 pre-defined buttons for your convenience. Instead of using multiple keys (at least two keys) to virtually access the remote window, you can just click on one of the options.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



Example of pressing *Ctrl+Alt+Del*








**Macro UI**

## 2.7.1g Console Redirection – Hotkey

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

### Hotkey Settings

Display	Hotkey	
Adjust Mouse	Ctrl+Shift+F2	 
Exit Remote Location	Ctrl+Shift+F3	 
Refresh Screen	Ctrl+Shift+F4	 
Send Ctrl+Alt+Del	Ctrl+Shift+F5	 
Toggle Mouse Display	Ctrl+Shift+F6	 

Close

Default











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, as shown below. 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."









**Hotkey Settings**

Display	Hotkeys	
Adjust Mouse	Ctrl+Shift+0	 
Exit Remote Location	Ctrl+Shift+F3	 
Refresh Screen	<input type="text" value="Ctrl+Shift+ "/>	 
Send Ctrl+Alt+Del	Ctrl+Shift+F5	 
Toggle Mouse Display	Ctrl+Shift+F6	 

 Please enter a valid shortcut.

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

### Hotkey Settings

Display	Hotkeys	
Adjust Mouse	Ctrl+Shift+0	 
Exit Remote Location	Ctrl+Shift+F3	 
Refresh Screen	Ctrl+Shift+8	 
Send Ctrl+Alt+Del	Ctrl+Shift+F5	 
Toggle Mouse Display	Ctrl+Shift+F6	 

✔ New shortcut key has been assigned successfully!

Close

Default


## 2.7.1h Console Redirection – Virtual Media

This feature allows you to upload and share images via the BMC (Baseboard Management Controller). 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.


● Device 1
● Device 2
● Device 3

⚠ No disk emulation set.

**Select Device Type**



**ISO Image**



**IMG/IMA Image**

**Select File**

Select File

Close
Mount

Display
Input
Video Stream Control
Record

**Display Scale**

60%
 70%
 80%
 90%
 100%

**Image Quality**

Low
 Medium
 High

Close

## 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.

The screenshot shows a preference panel with four tabs: Display, Input, Video Stream Control, and Record. The 'Display' tab is selected. Below the tabs, there are two sections: 'Display Scale' and 'Image Quality'. Under 'Display Scale', there are five radio buttons: 60%, 70%, 80%, 90%, and 100%. The 100% option is selected. Under 'Image Quality', there are three radio buttons: Low, Medium, and High. The Medium option is selected. At the bottom of the panel is a blue 'Close' button.

### 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.

The screenshot shows a preference panel with four tabs: Display, Input, Video Stream Control, and Record. The 'Input' tab is selected. Below the tabs, there is a section titled 'Mouse Settings'. Under this section, there are three radio buttons: Absolute Mouse (Windows, Ubuntu, RHEL 6.x and later), Relative Mouse (Other Linux distributions), and Single Mouse. The Absolute Mouse option is selected. At the bottom of the panel is a blue 'Close' button.

## 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 available if you have higher network bandwidth.

Display
Input
Video Stream Control
Record

**LAN Flow Control**

256K Cable/DSL(Default)

T1

T2

Close

## Console Redirection – Record

This feature is used to record Video during BIOS booting. You can turn on/off recording time in this tab. A preset two minutes recording time is enabled by default, but you can modify the recording time from 1 minute to a maximum of 30 minutes.



**Note:** Video Recording only works with the Chrome browser.

Display
Input
Video Stream Control
Record

**Recording Time**

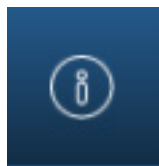
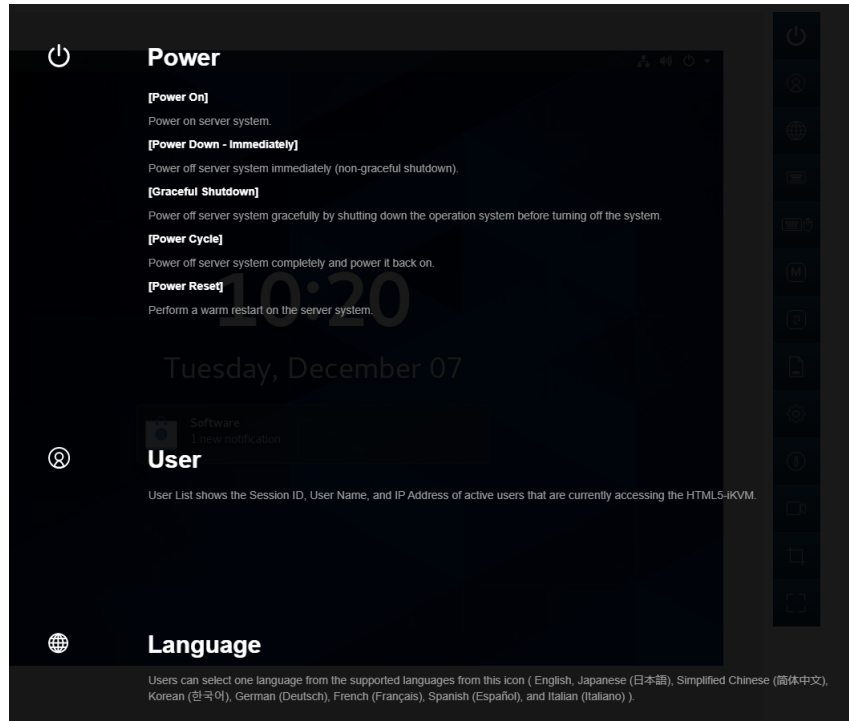
ON Enable auto stop after  minute(s)

New settings will take effect in next recording.

Close

## 2.7.1j Console Redirection – Help

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



**Help Icon**

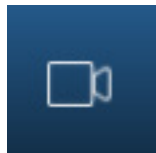
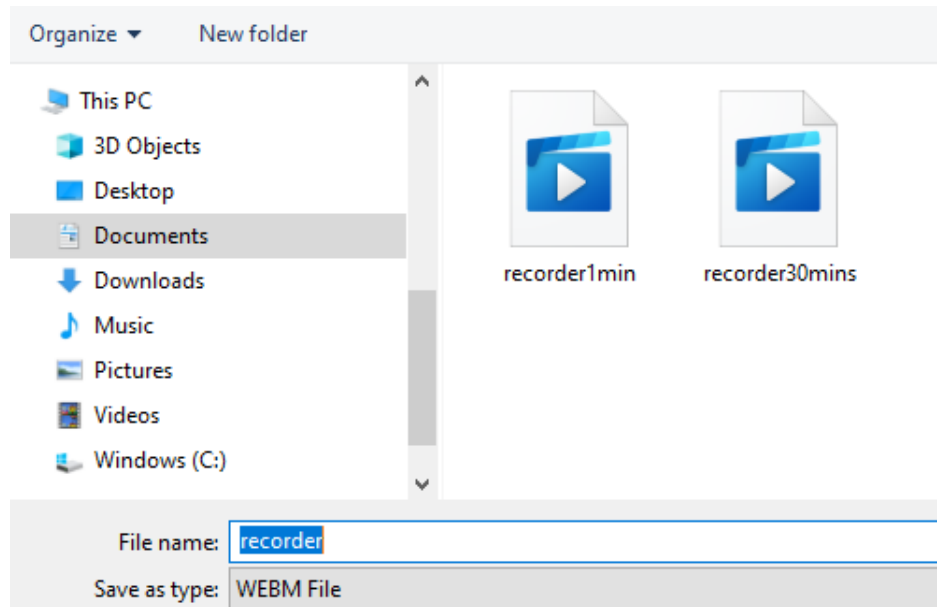


## 2.7.1k Console Redirection – Record

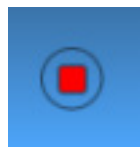
Use this feature to record Video during BIOS booting. After you press the Record button and then the Stop button, the recording will be available to be saved as shown below.



**Note:** Video recording only works with the Chrome browser.



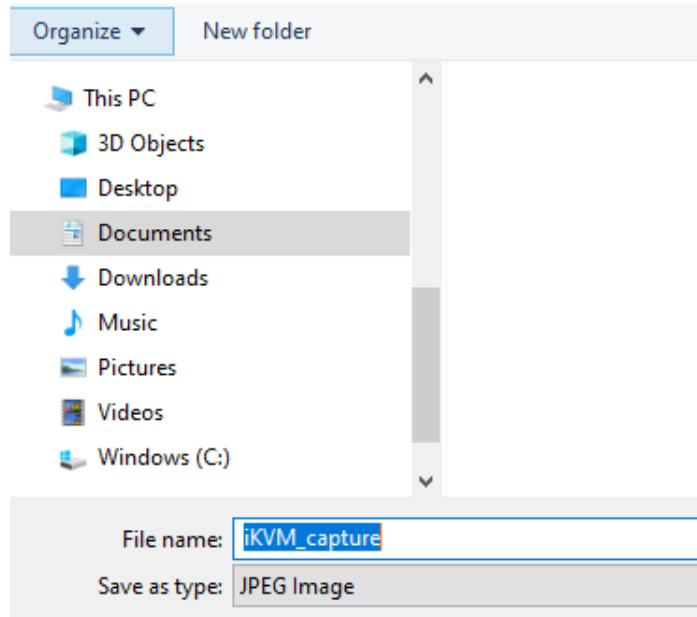
**Record Icon**



**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 as shown below.



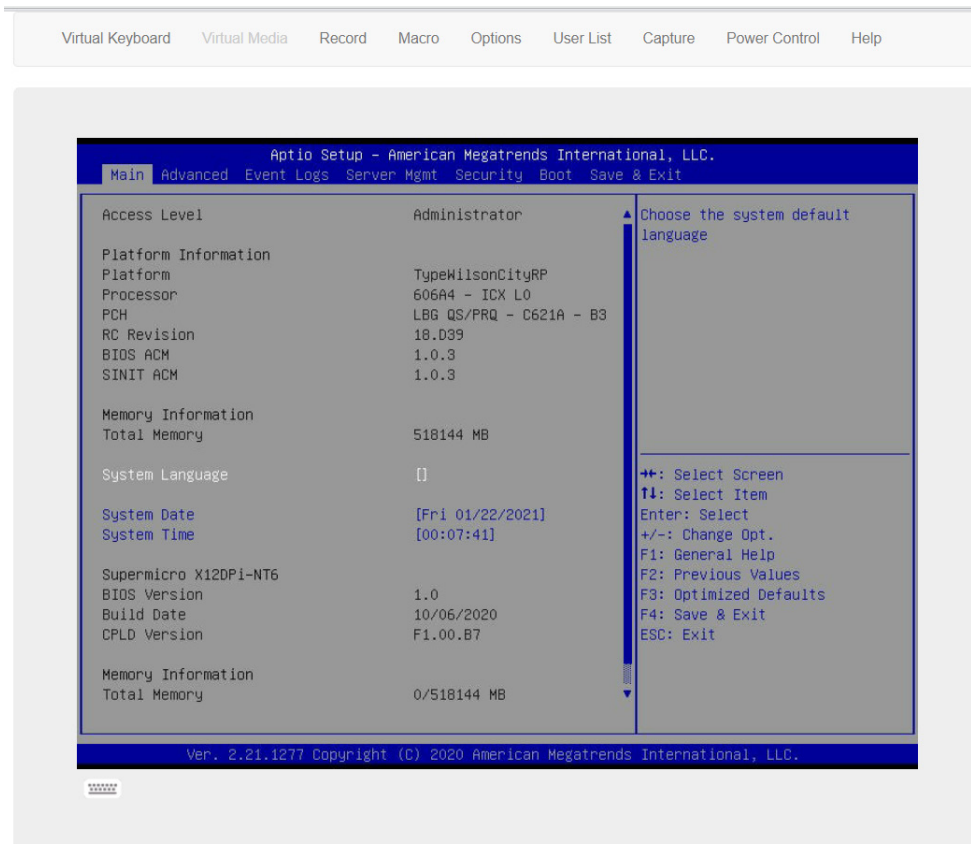
**Capture Icon**

## 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.

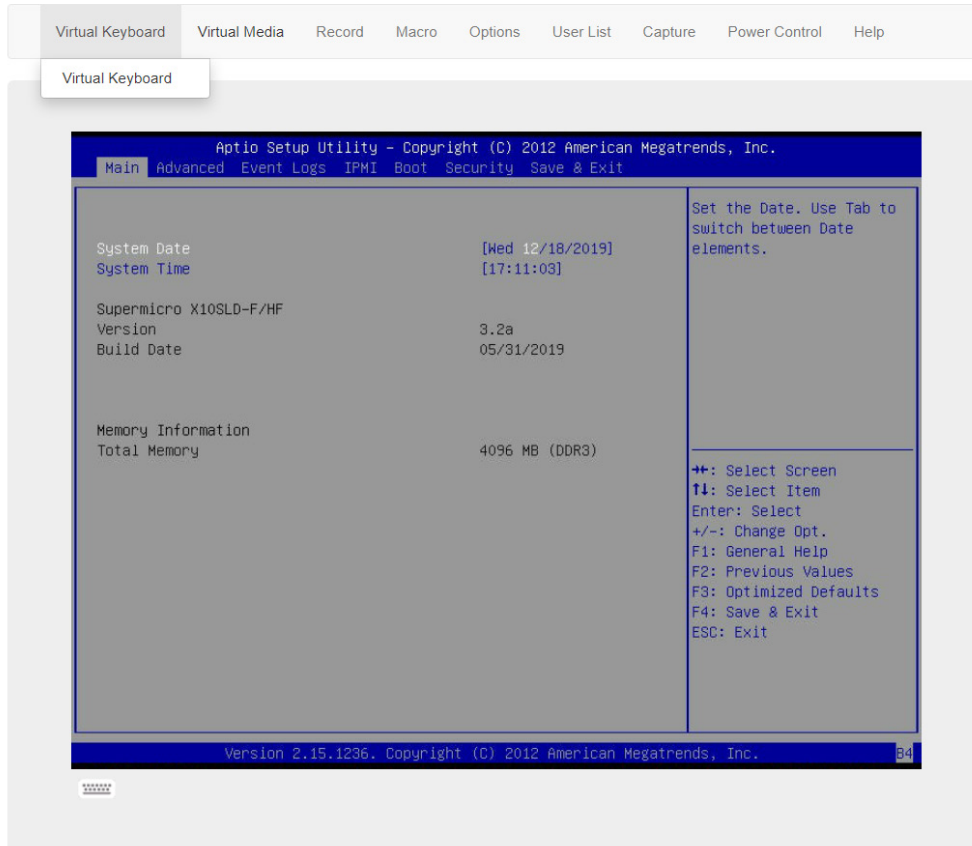
## 2.7.2 iKVM/HTML5

This feature allows you to launch iKVM/HTML5 via iKVM (keyboard, video/monitor, mouse) support. Refer to page 75 on how to first launch the Remote Console. Click [Help] for further assistance if needed.

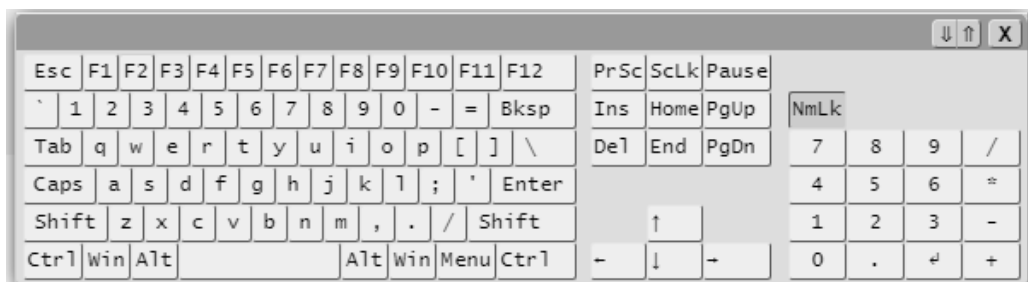


## 2.7.2a iKVM/HTML5 – Virtual Keyboard

The virtual keyboard provides an alternative input mechanism if you are unable to use a conventional keyboard. The two ways to access the keyboard are as follows.



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




## 2.7.2b iKVM/HTML5 – Virtual Media

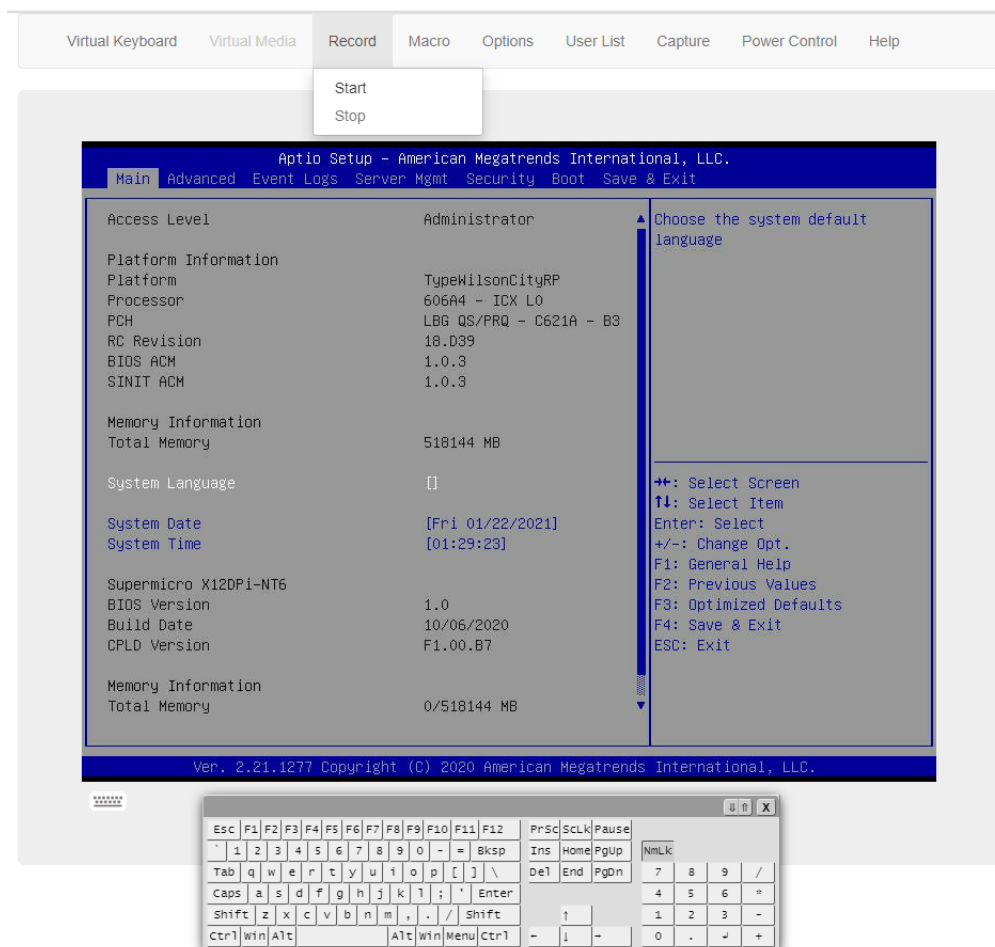
This feature allows you to upload and share images via the BMC (Baseboard Management Controller). These images will be emulated to the host server as USB applications. You need to first activate a Super Micro Software License to enable this feature.

## 2.7.2c iKVM/HTML5 – Record

This feature allows for video recording of the display and includes the following options.

- Start: You can use this submenu to start the recording function. By default, the recording duration is two minutes. This can be adjusted in Preferences (found under the Options tab).
- Stop: You can use this submenu to manually stop the recording process. Recorded videos will be automatically saved onto your drive.

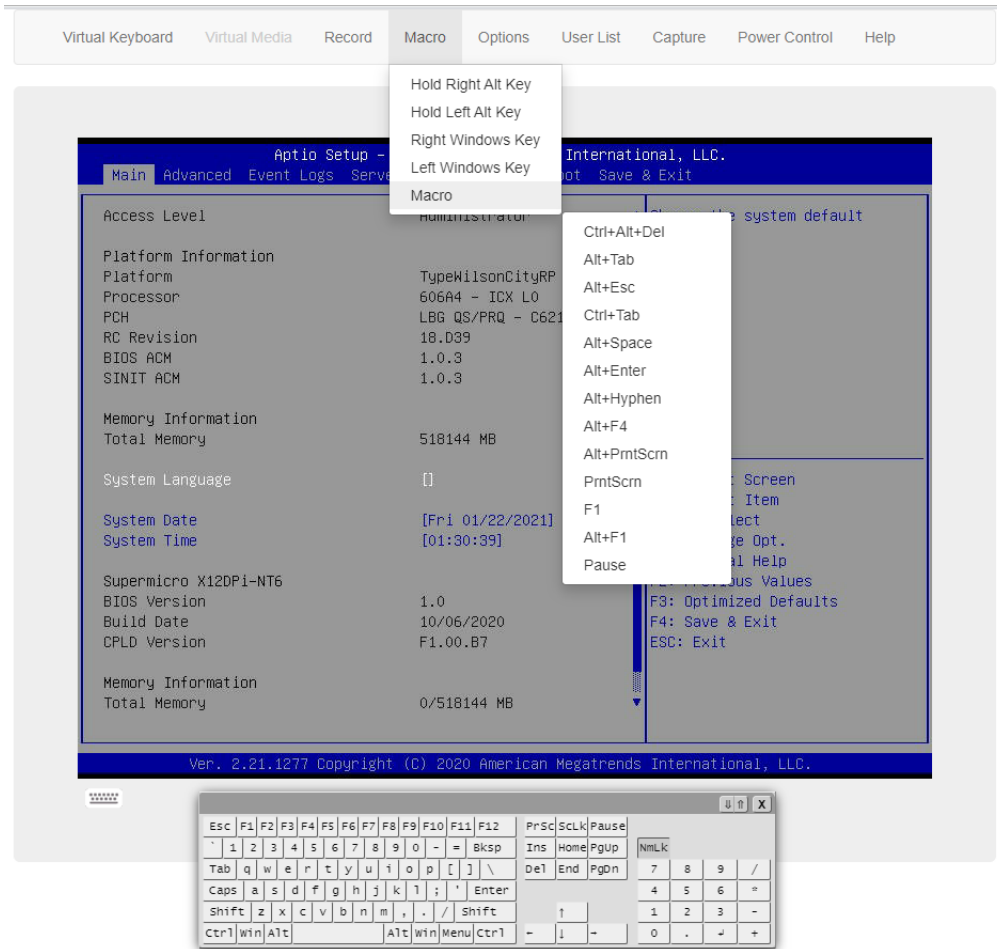
 **Note:** This new HTML5 implementation is currently only supported by the Chrome browser.



## 2.7.2d iKVM/HTML5 – Macro

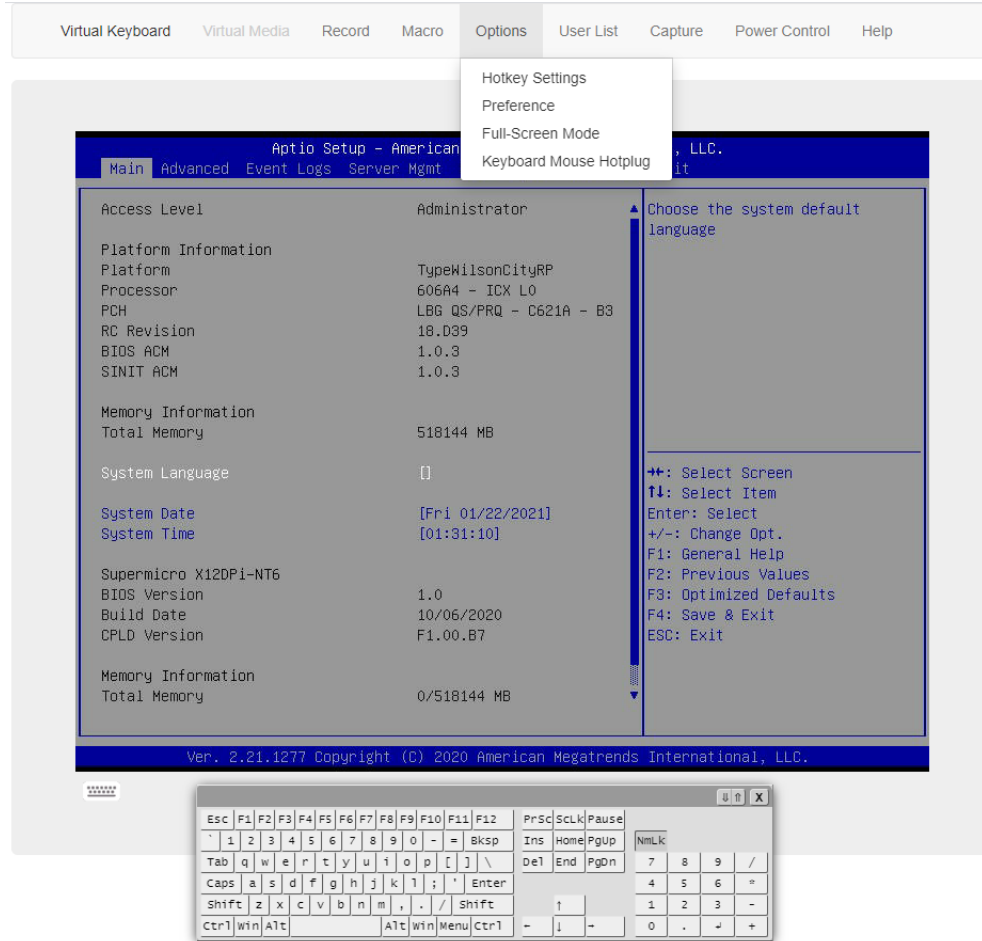
This feature allows you quick access to combo keys.

- Hold Right Alt Key: This item performs the same function as holding down the right <Alt> key. Deselect to release action.
- Hold Left Alt Key: This item performs the same function as holding down the left <Alt> key. Deselect to release action.
- Right Windows Key: This item performs the same function as pressing the right <Windows> key. Select [Hold Down] or [Press and Release].
- Left Windows Key: This item performs the same function as pressing the left <Windows> key. Select [Hold Down] or [Press and Release].
- Macro: You can click this item to view the pull-down submenu which includes the following 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



## 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.

### Hotkey Settings

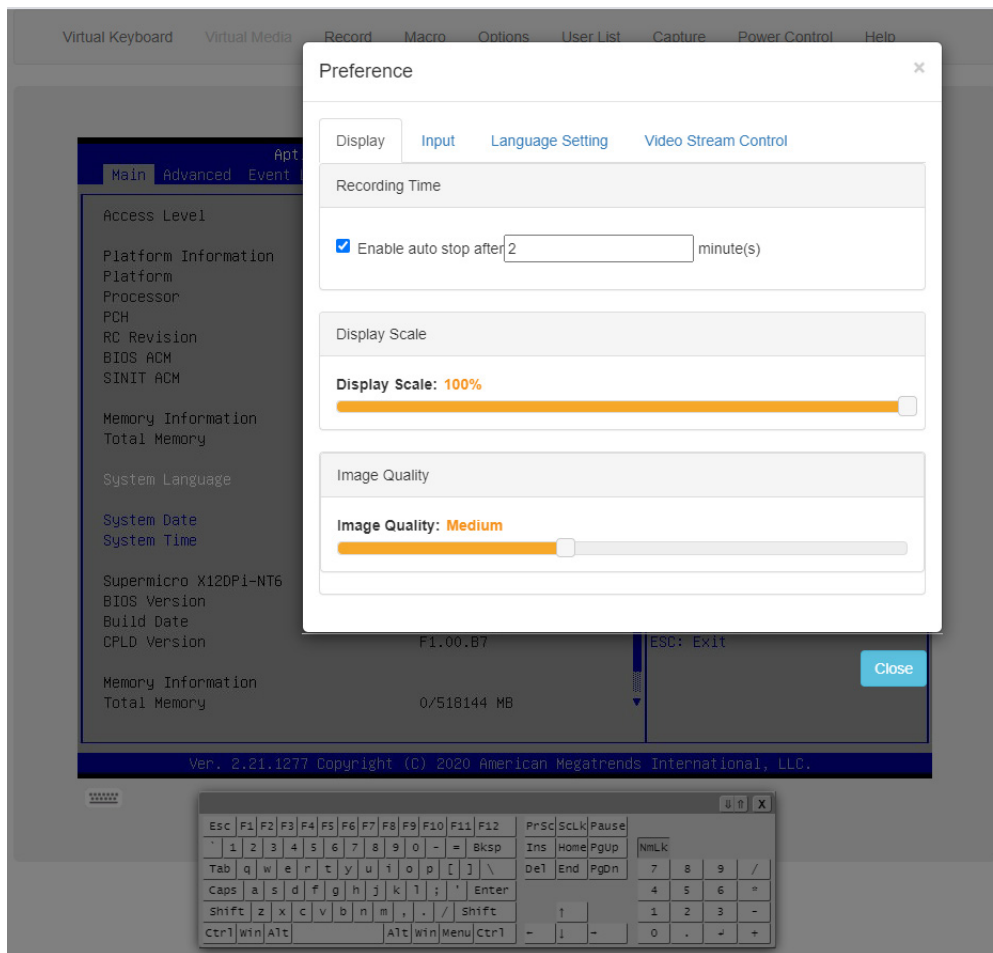
Display	Hotkeys	
Adjust Mouse	Ctrl+Shift+F2	 
Exit Remote Location	Ctrl+Shift+F3	 
Refresh Screen	Ctrl+Shift+F4	 
Send Ctrl+Alt+Del	Ctrl+Shift+F5	 
Toggle Mouse Display	Ctrl+Shift+F6	 

Close

Default

## Preference – Display

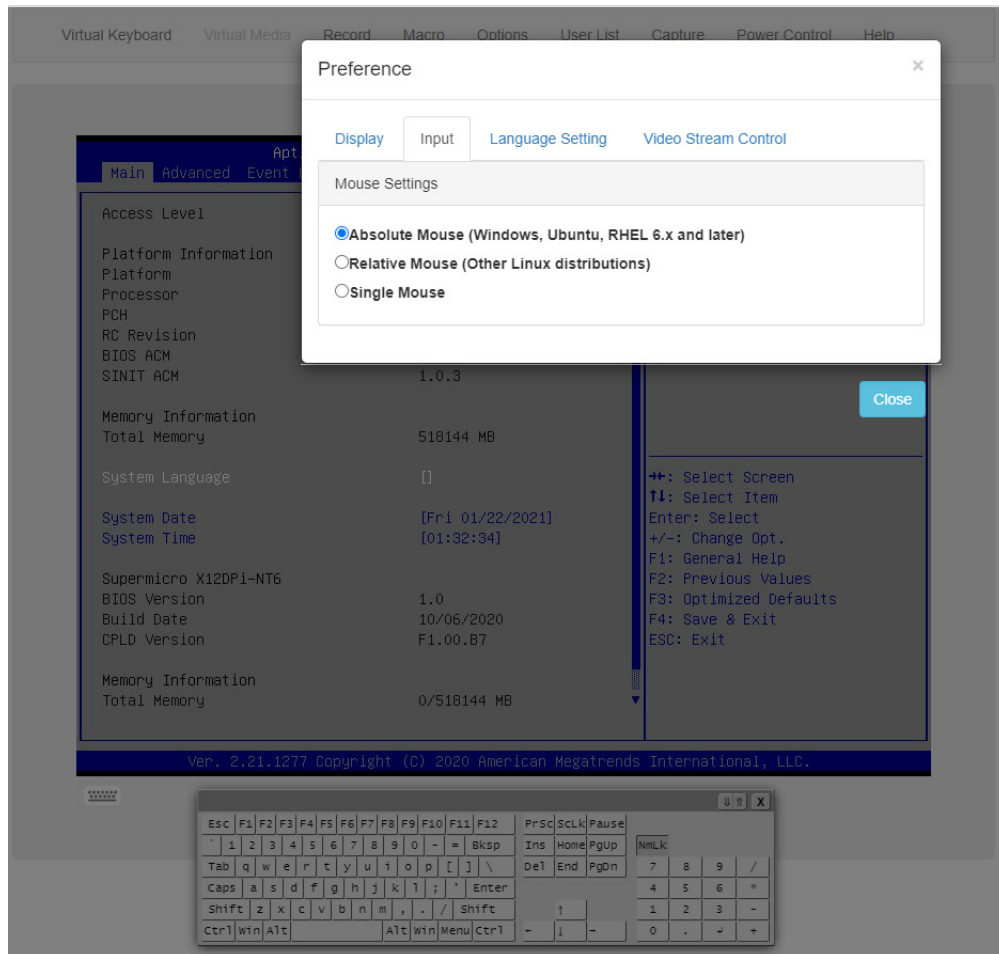
This feature enables auto-stop after n (default: 2) minutes. Adjust the maximum duration of video recordings.



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

## Preference – Input

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



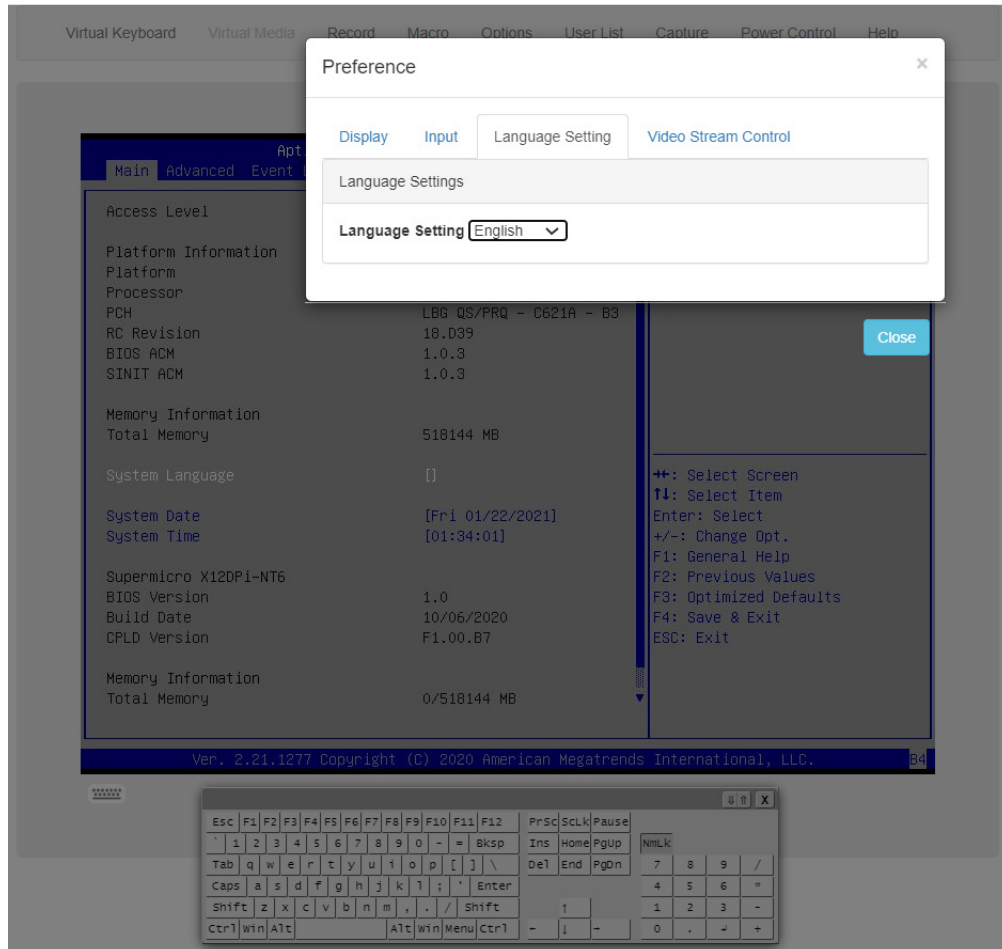
- Absolute Mouse
- Relative Mouse
- Single Mouse



**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.

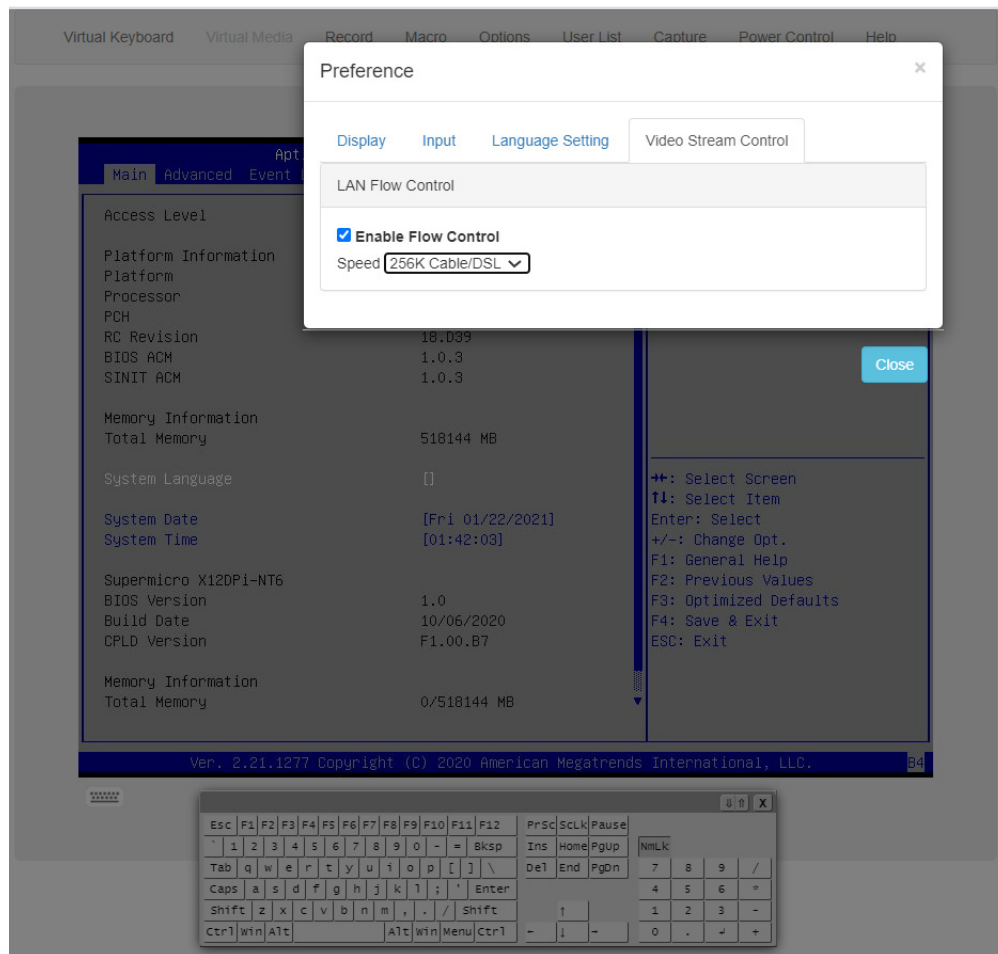


- English
- Japanese
- German
- French
- Spanish
- Italian

## Preference – Video Stream Control

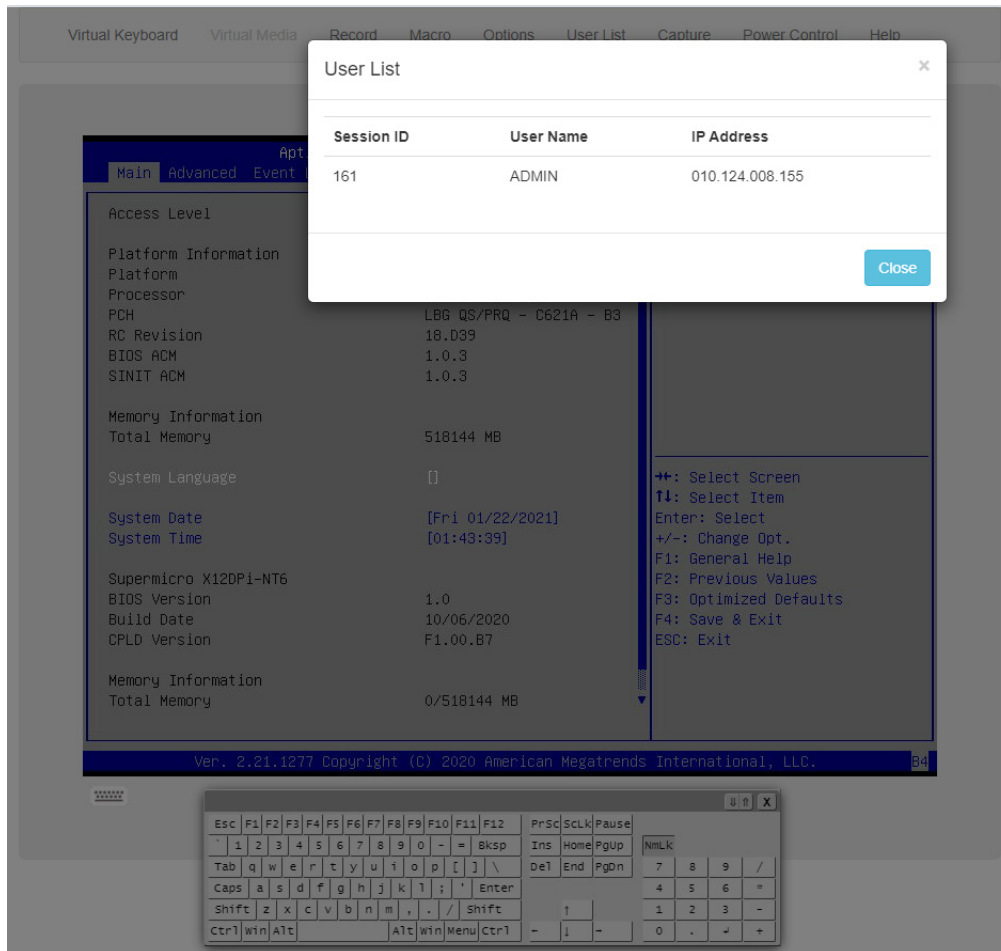
This feature allows you to enable video flow control for LAN Quality of Service (QoS) by selecting one of the following options.

- 256K Cable/DSL
- T1
- T2



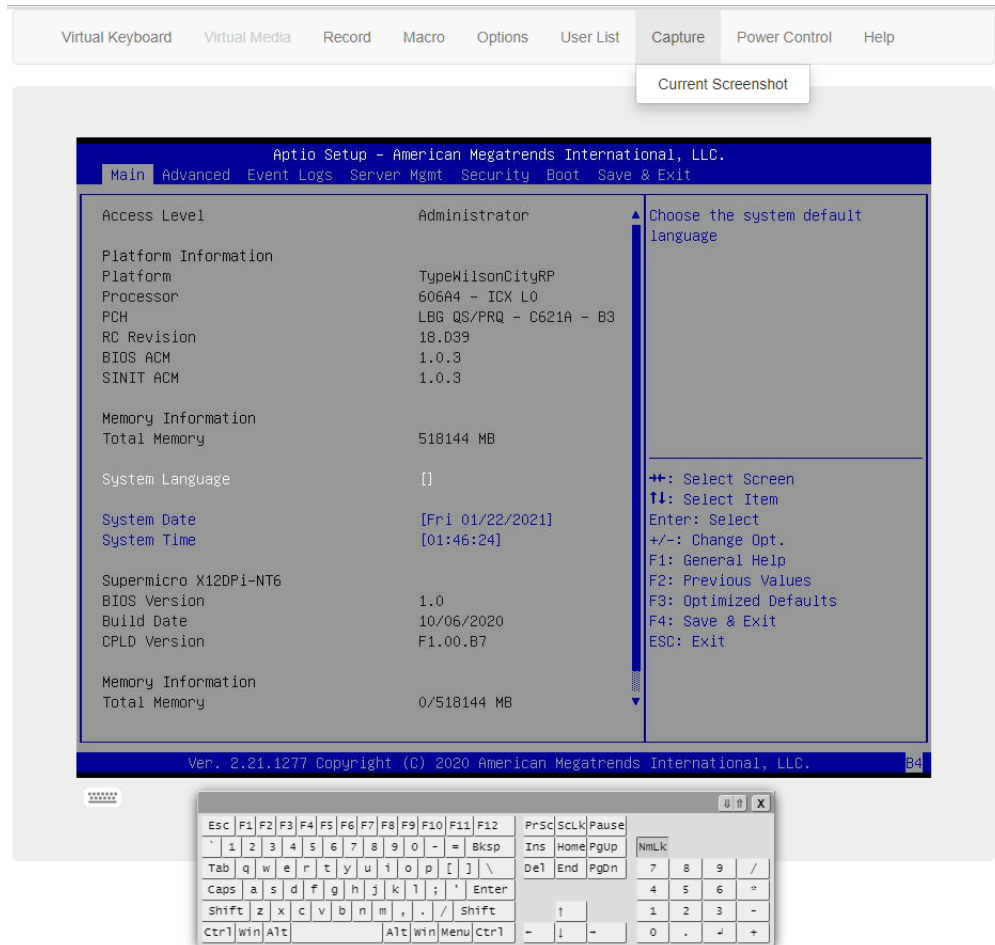
## 2.7.2f iKVM/HTML5 – User List

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



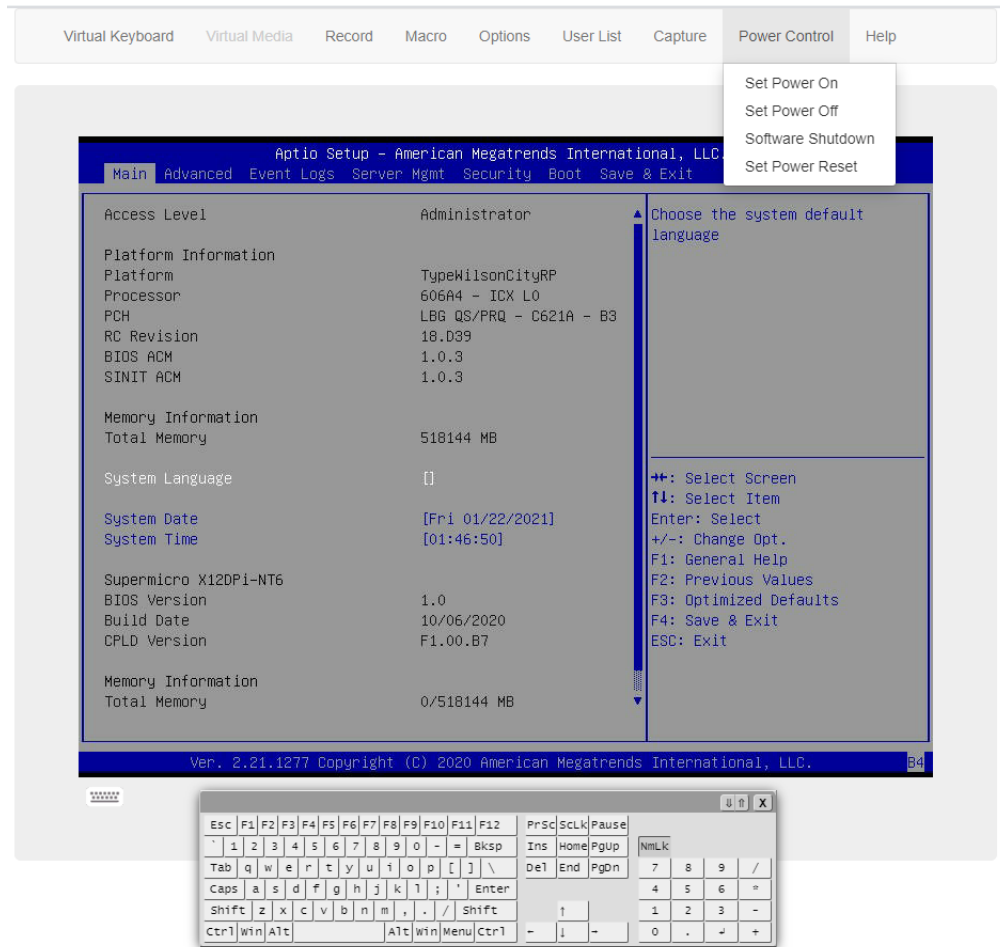
## 2.7.2g iKVM/HTML5 – Capture

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



## 2.7.2h iKVM/HTML5 – Power Control

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





## 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:** Currently, the number of Maintenance Event Log entries is limited to 4096.

### 2.8.1. Firmware Management

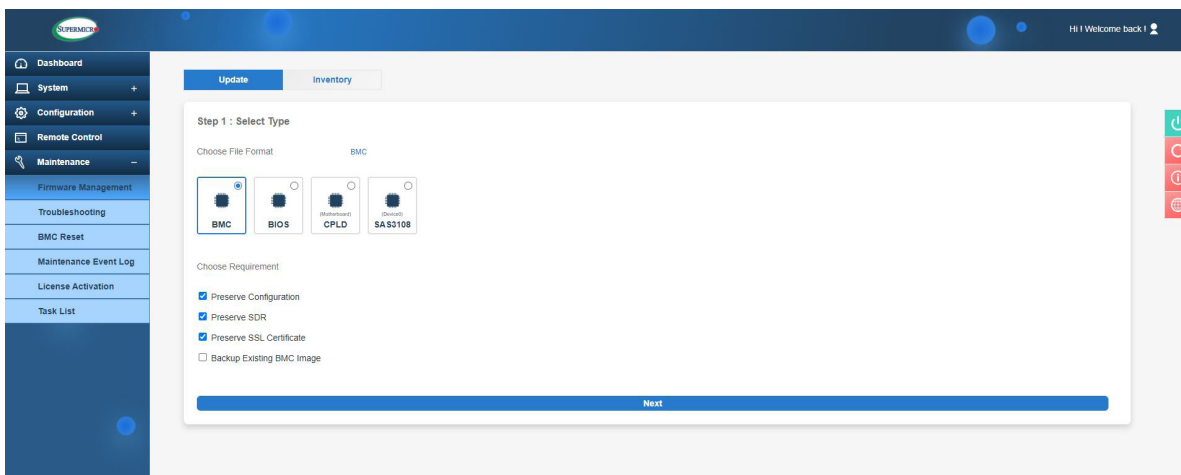
The firmware management page allows administrators to update firmware for BMC, BIOS, Motherboard CPLD, BackPlane CPLD, network AOC, or storage AOC as well as manage Platform Firmware Resiliency (PFR) options.



**Note:** Systems are required to power down all HOSTs from single-node or multi-node systems prior to Motherboard CPLD, Backplane CPLD, LCMC PDB CPLD, and BIOS FW updates. After firmware updates for network AOC and/or storage AOC, they will need to reboot. Lastly, BMC may be required to reset after the motherboard CPLD firmware update, especially in multi-node systems like GrandTwin.

### Update


If you have administrator privileges, this page allows you to update component firmware.



To update firmware, please refer to the following steps.

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

4. Update the firmware by clicking the “Update” button. You can check firmware update progress on 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 while it is in progress. 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:** After the firmware update is initiated, viewing the web browser will cause it to stop sending requests. As a result, the Web Browser/BMC UI of the secondary UI (viewing web browser) needs to refresh in order to renew the BMC connection. It will prompt the following message to wait for the BMC, “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!”

BMC update supports the following preserve configuration options.

- Preserve configuration
- Preserve SDR
- Preserve SSL certificate
- Backup existing BMC image

BIOS update supports following preserve configuration options for all X13 platforms except Tatlow platforms.

- Preserve SMBIOS
- Backup existing BIOS image

 **Note 1:** You can select the “Backup existing image” option to back up existing BMC or BIOS images. This option is used for auto recovery in case of firmware integrity check fails at any time. You can also manually recover BMC or BIOS from backup images. Go to the inventory page to manually recover BMC or BIOS. Non-ROT platforms will not display the “Backup existing image” option.

**Note 2:** Due to the limitations of the current BMC implementation, it may take a long time to refresh the web browser after you complete updating the firmware. You might also still see the rebooting message for a minute or two when logging back in.

The following preserve configuration options for Tatlow platforms.

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

## How BMC Firmware is Updated

**Update** | Inventory

Step 1 : Select Type

Choose File Format **BMC**

BMC  BIOS  (Motherboard) CPLD  PMem  (Device 0) SAS3808  (Device 0) NIC1  (Device 1) SAS3816

Choose Requirement

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

**Next**

**Update** | Inventory

Step 1 : Select Type

Choose File Format **BMC**

BMC  BIOS  (Motherboard) CPLD  PMem  (Device 0) NIC1  (Device 0) SAS3808  (Device 1) SAS3816

Choose Requirement

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

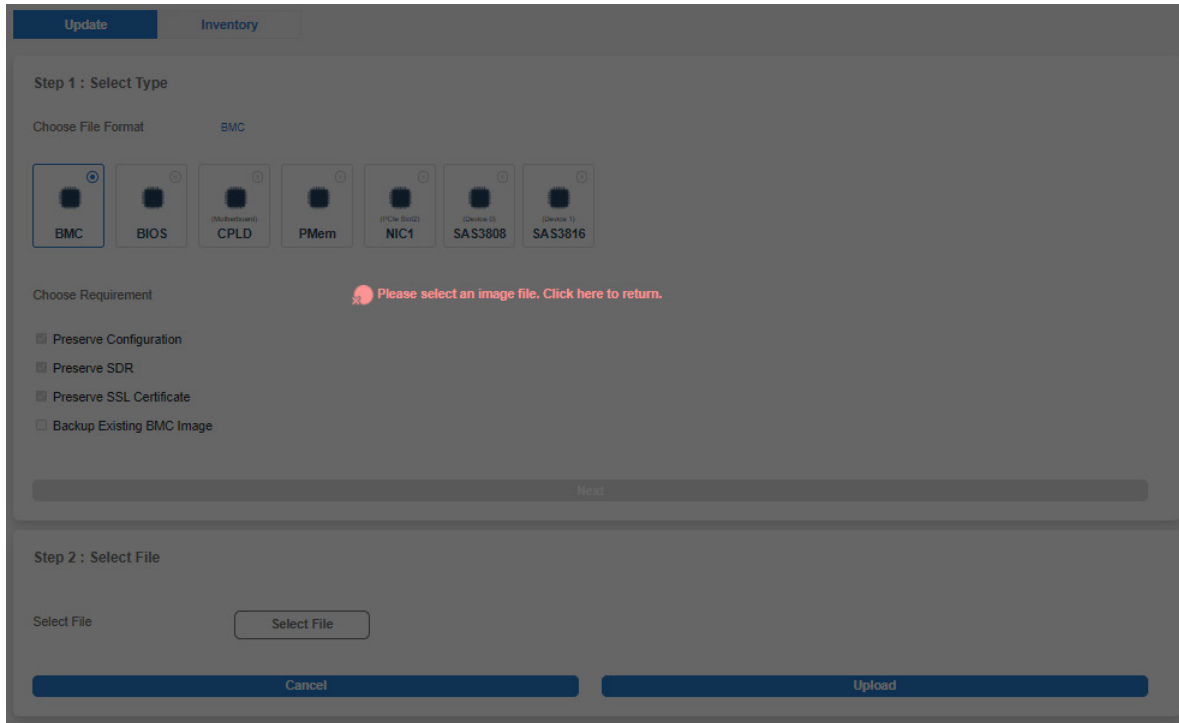
Next

Step 2 : Select File

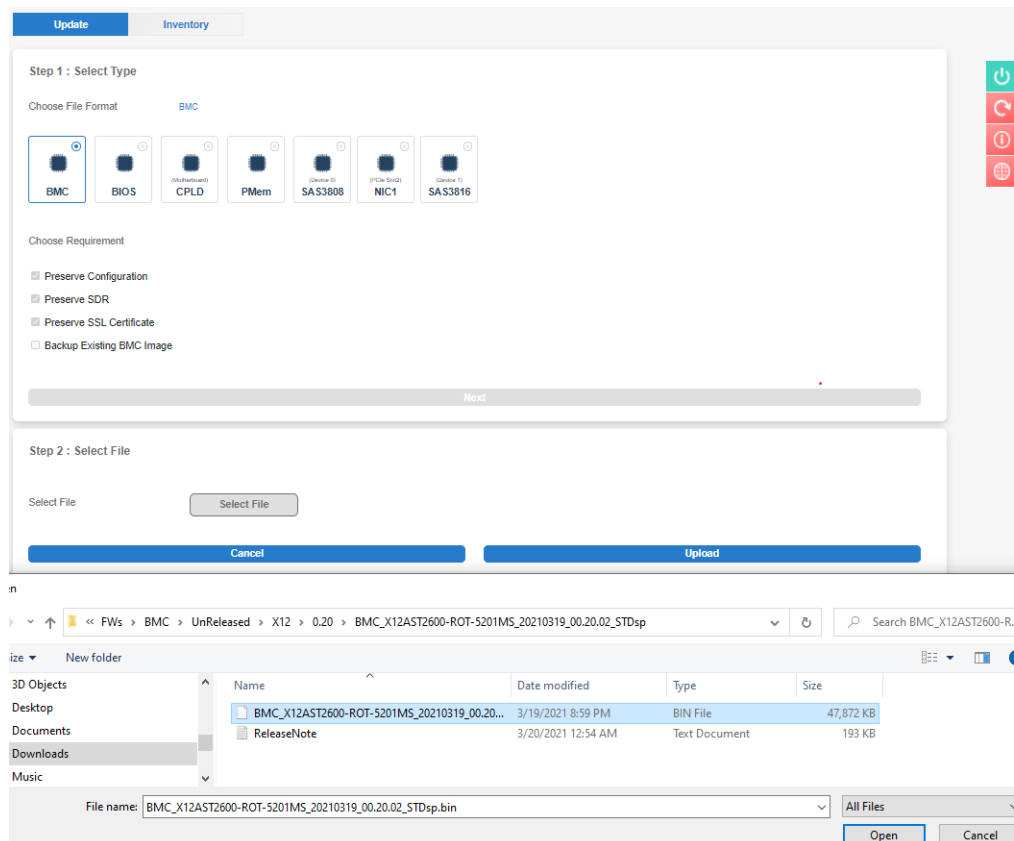
Select File

**Cancel** **Upload**

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



If you continue on with the BMC update, BMC will provide a timely percentage of completion. See the example below for details.



**Update** | Inventory

Step 1 : Select Type

Choose File Format **BMC**

BMC  BIOS  (Motherboard) CPLD  PMem  (PCIe Slot2) NIC1  (Device 1) SAS3808  (Device 1) SAS3816

Choose Requirement


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

Next

---

Step 2 : Select File

Select File

 BMC\_X12AST2600-ROT-5201MS\_20210319\_00.20.02\_STDsp.bin 46.75 MB

**Update** | Inventory

Step 1 : Select Type

Choose File Format **BMC**

BMC  BIOS  (Motherboard) CPLD  PMem  (PCIe Slot2) NIC1  (Device 1) SAS3808  (Device 1) SAS3816

Choose Requirement


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

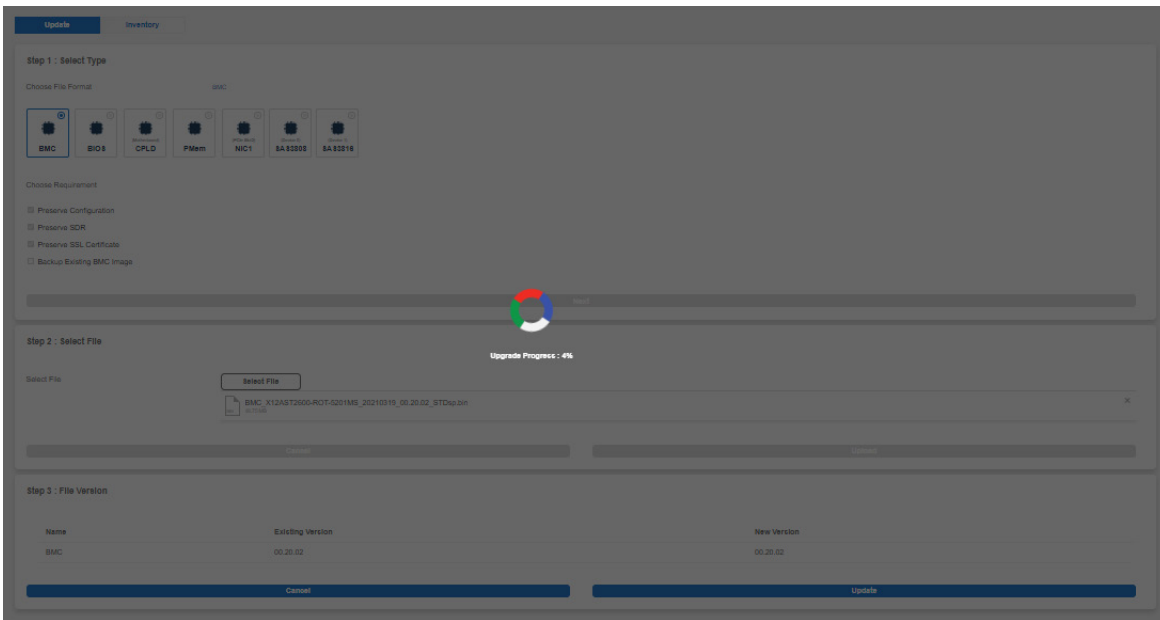
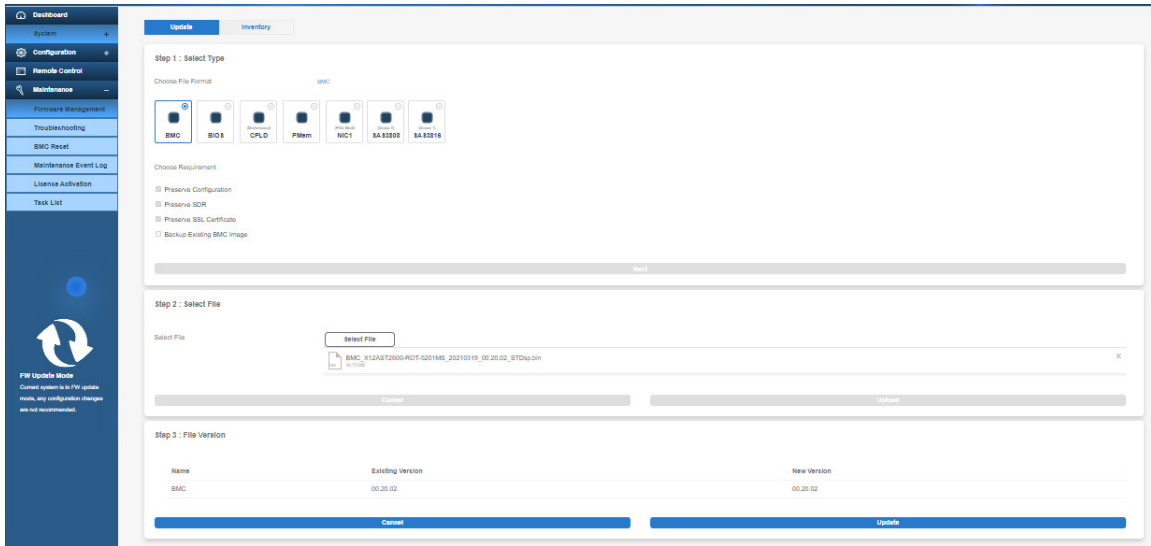
Next

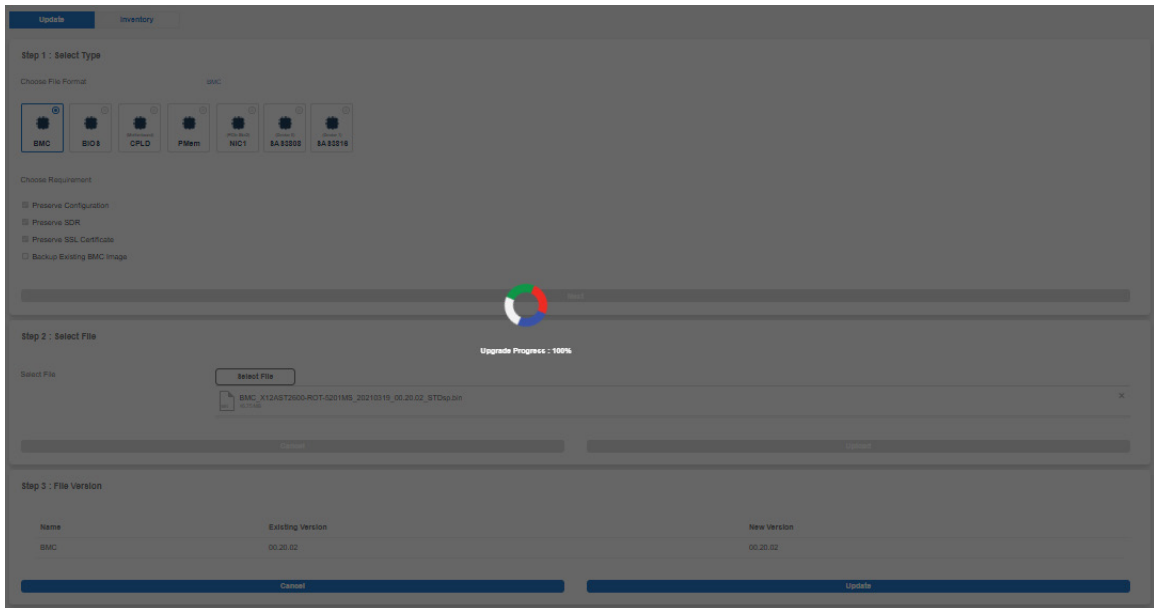
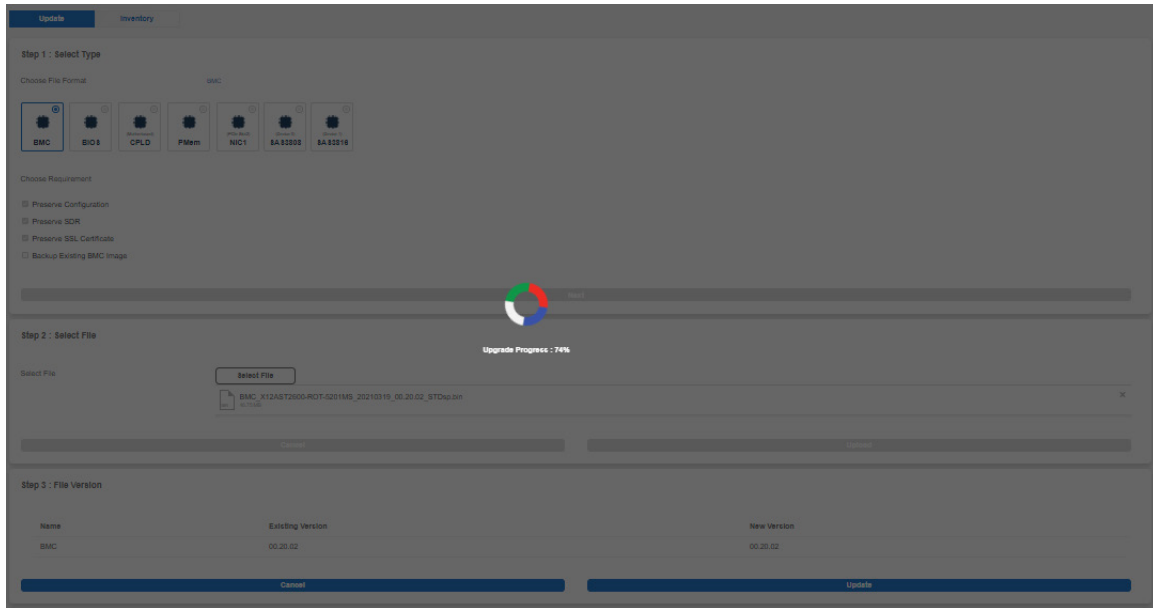
---

Step 2 : Select File

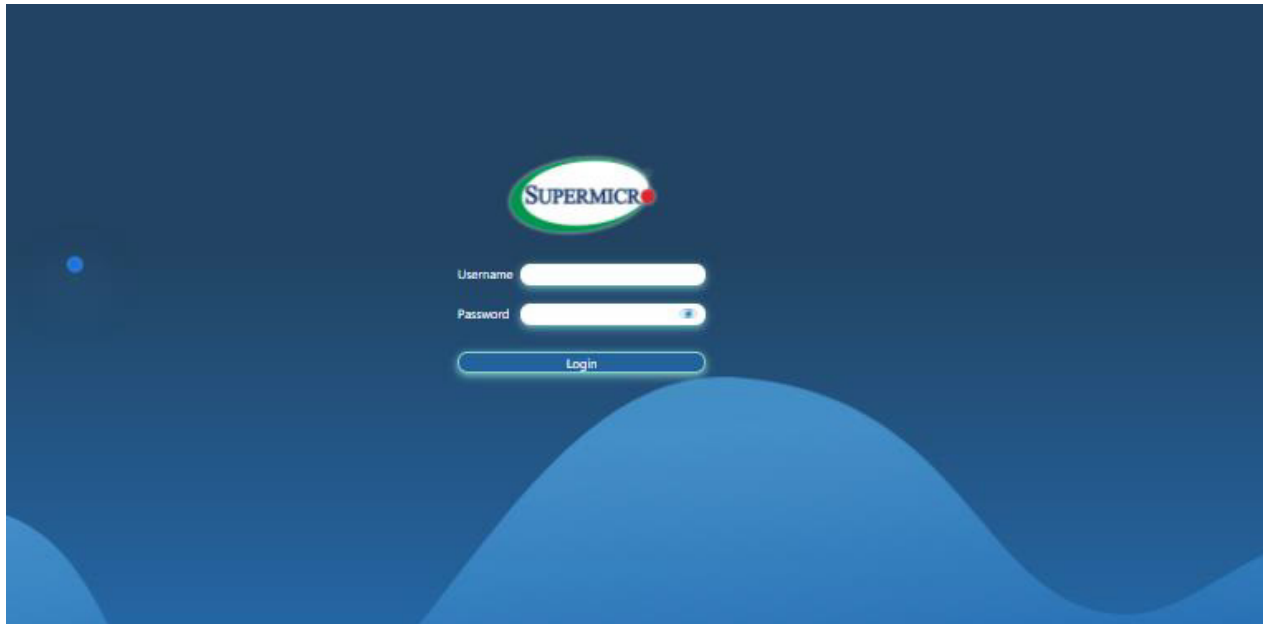
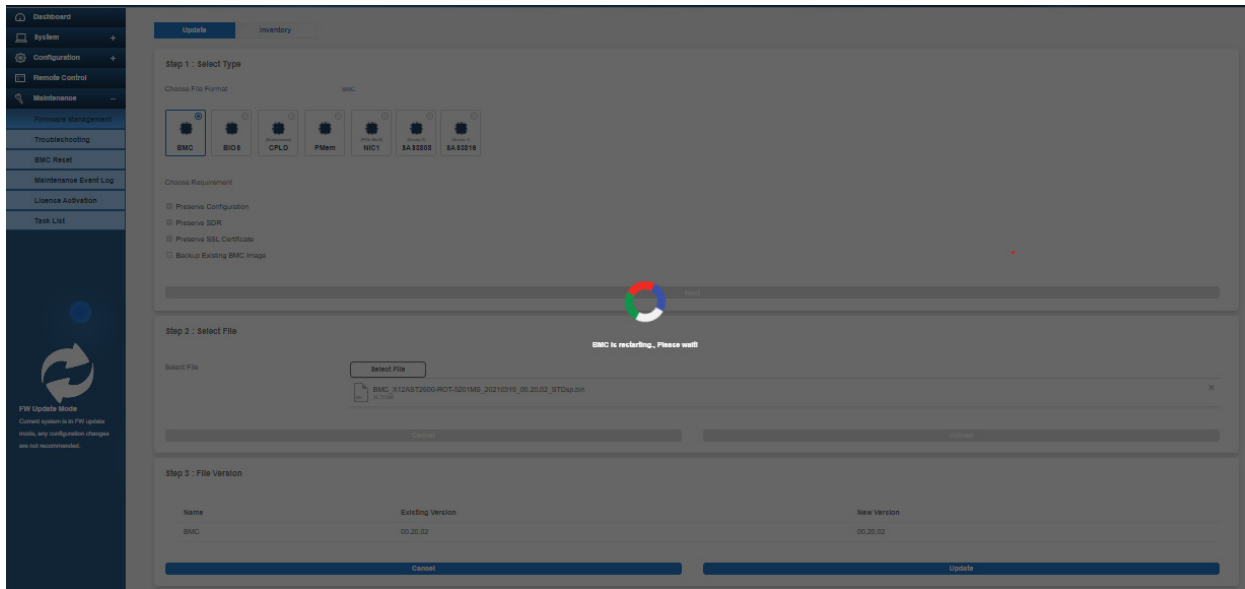
Select File


 BMC\_X12AST2600-ROT-5201MS\_20210319\_00.20.02\_STDsp.bin 46.75 MB

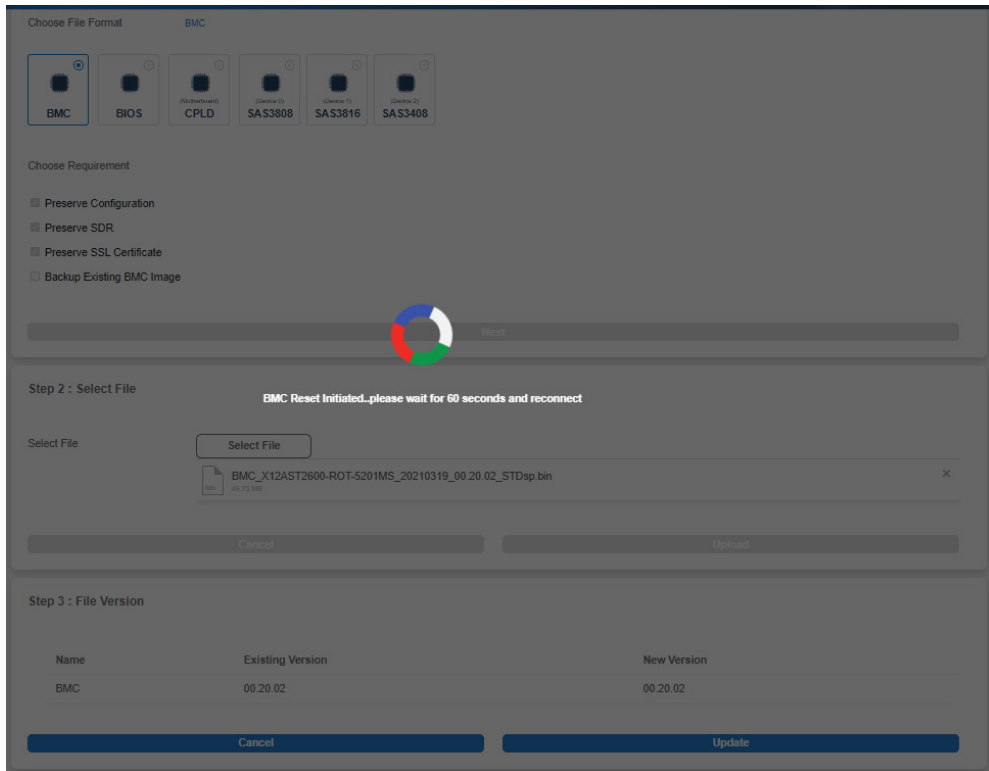
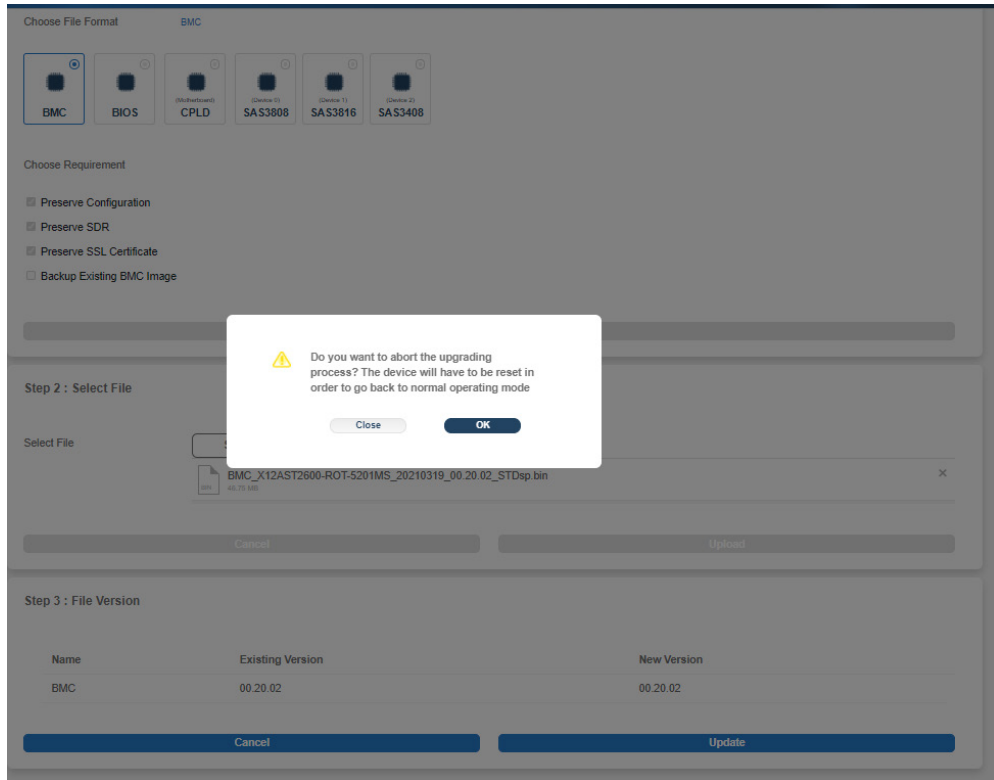




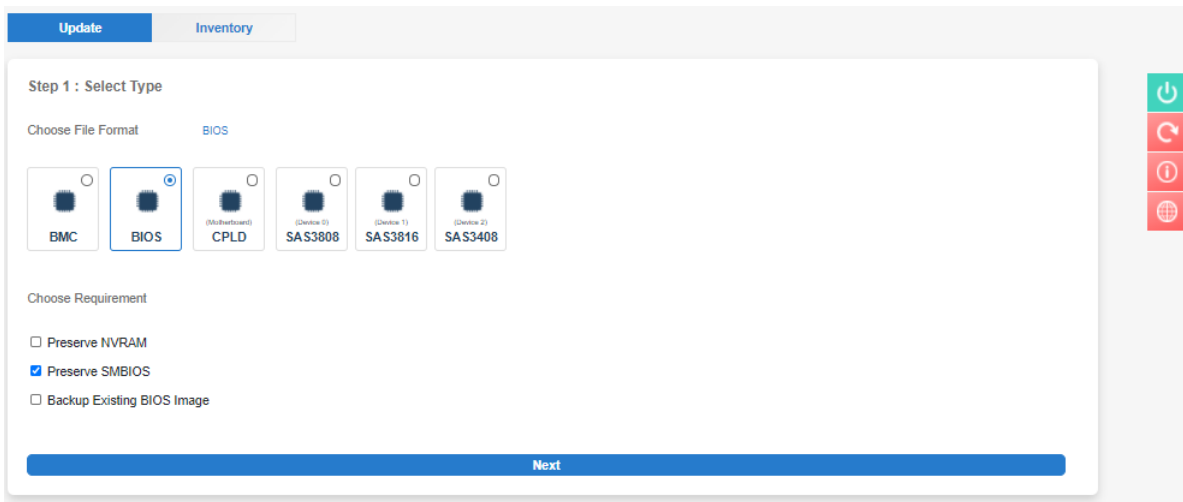
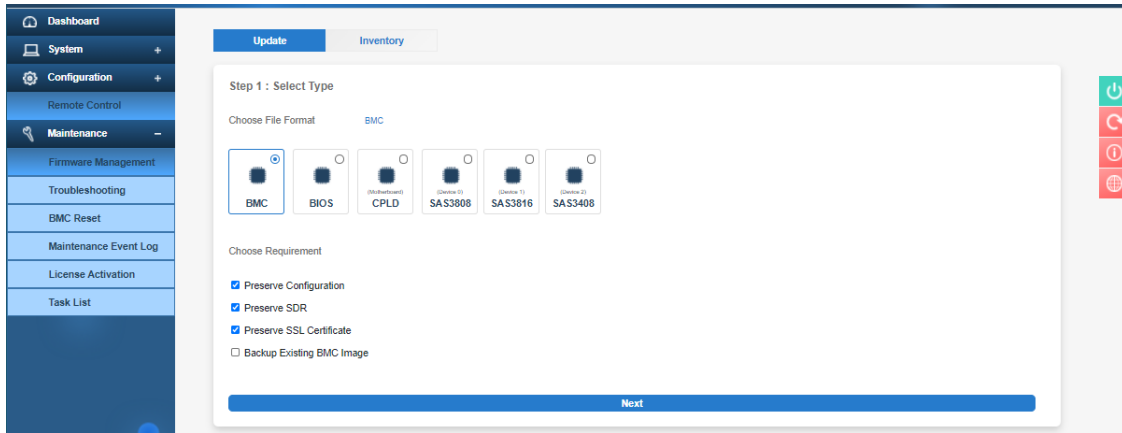


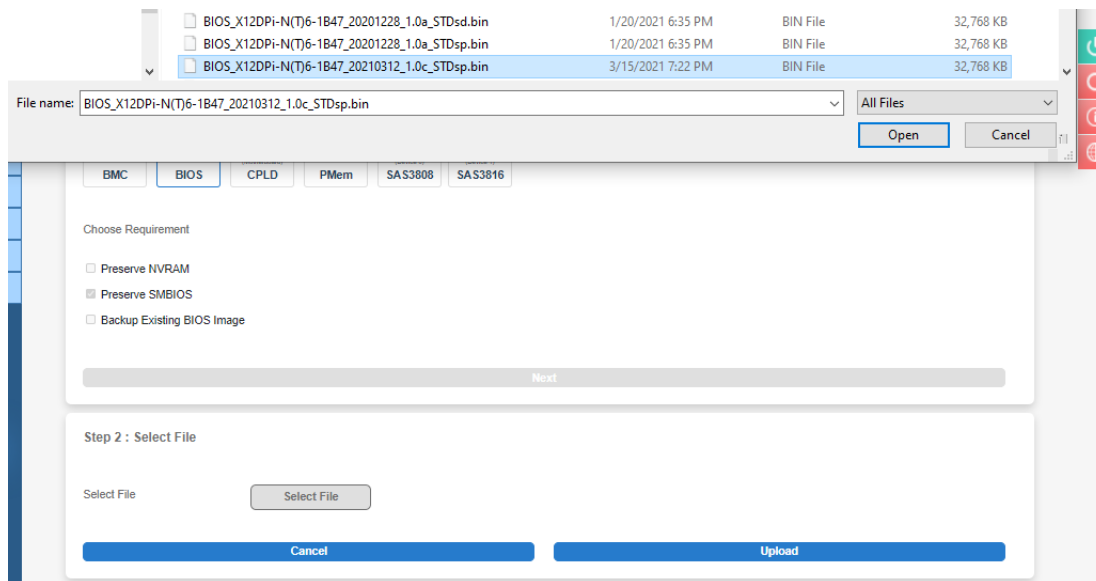
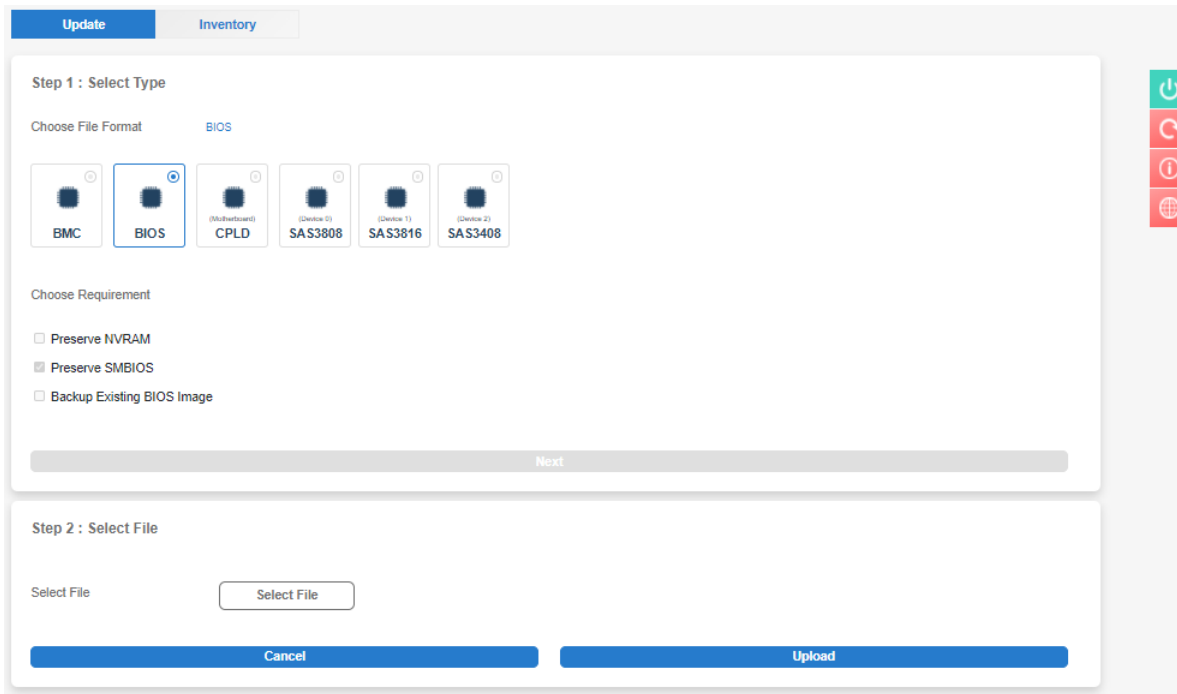


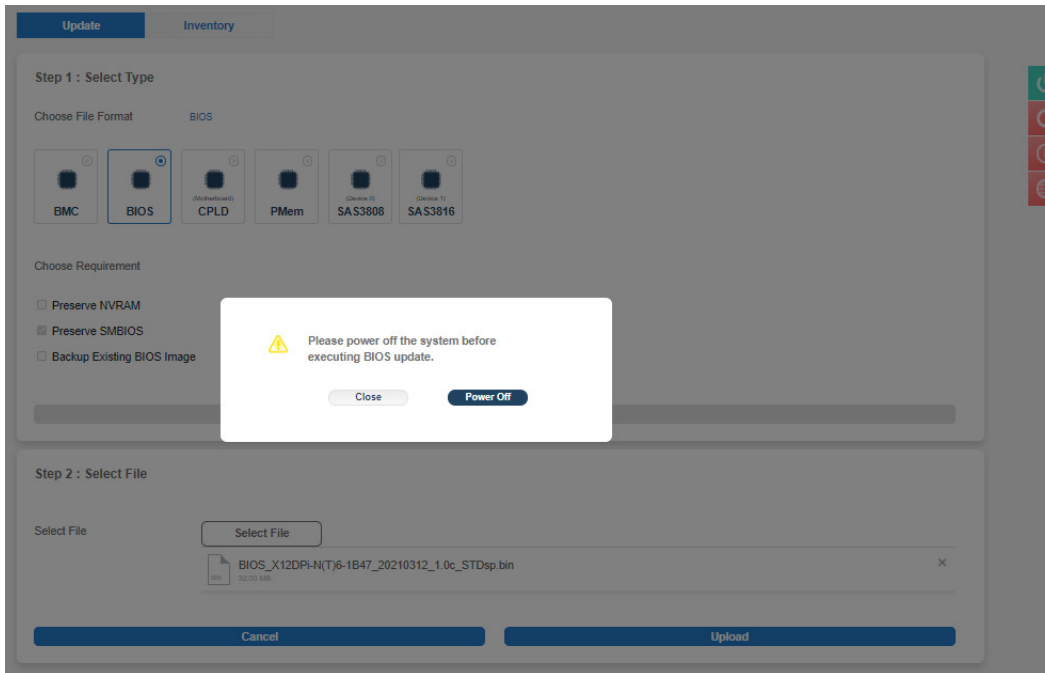
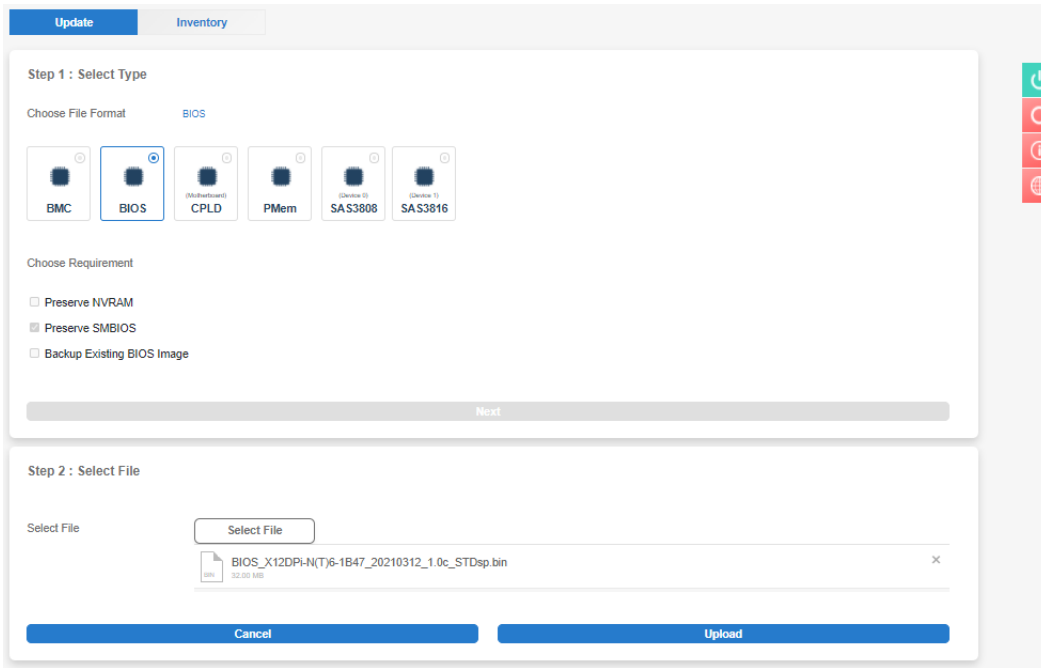
 **Note:** If you cancel the BMC updating process, there will be an alert message pops up to ask you “Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode.” BMC is then reset with the message “BMC is restarting. To prevent data loss,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

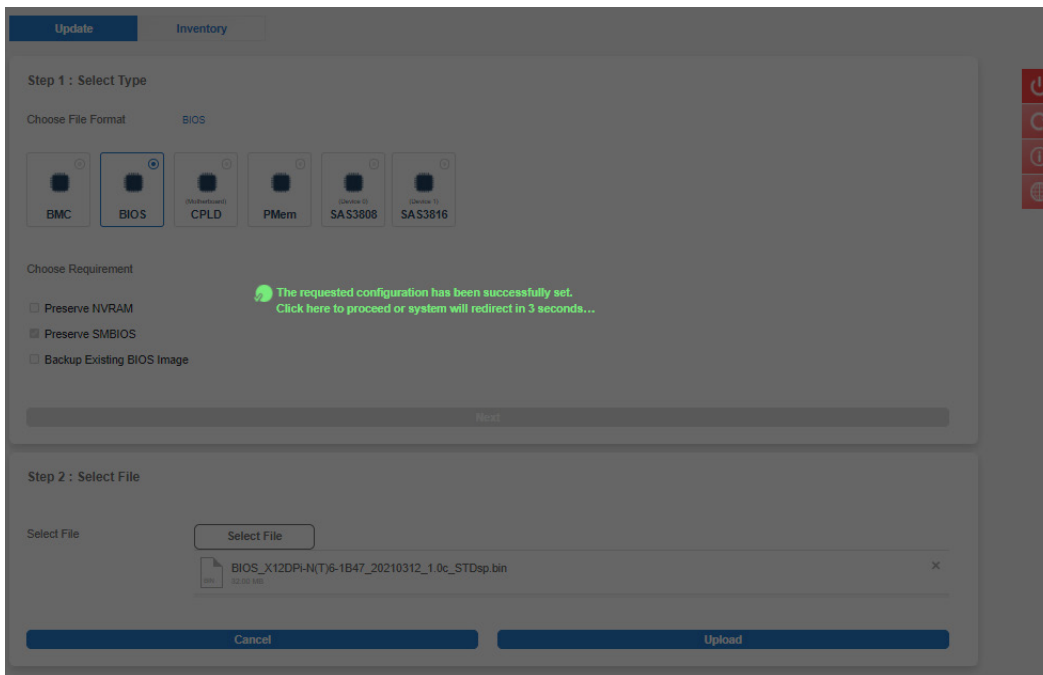
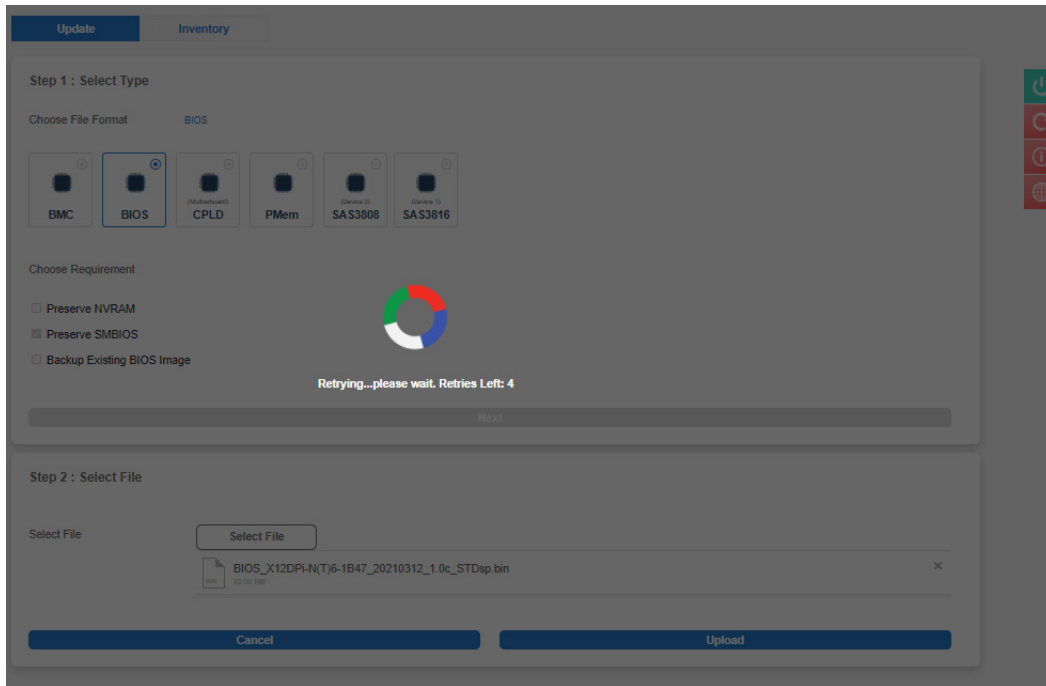


## How BIOS Firmware is Updated

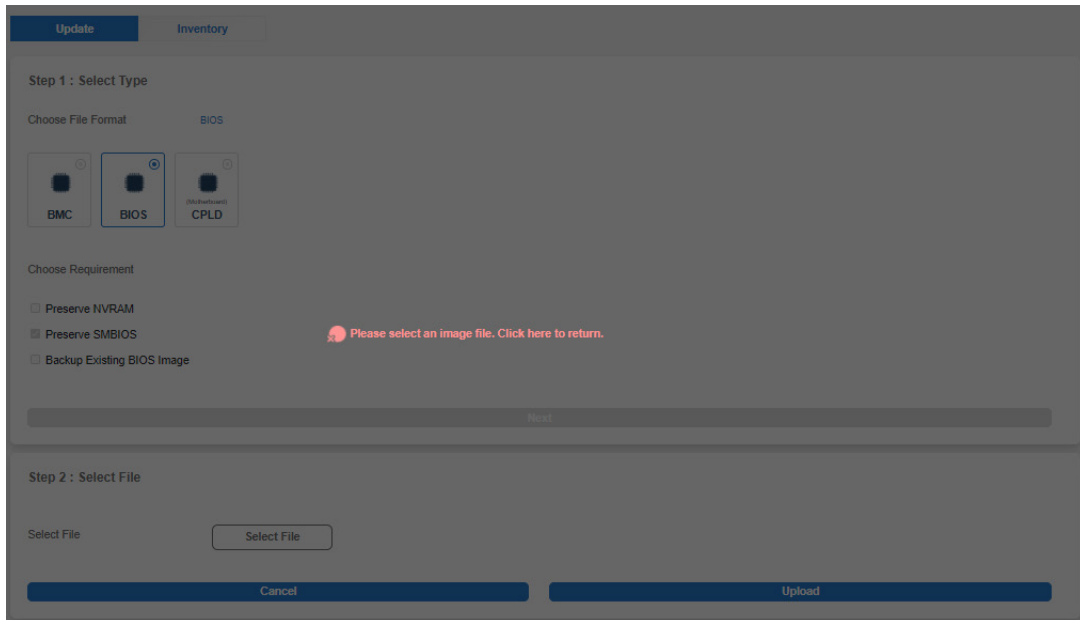




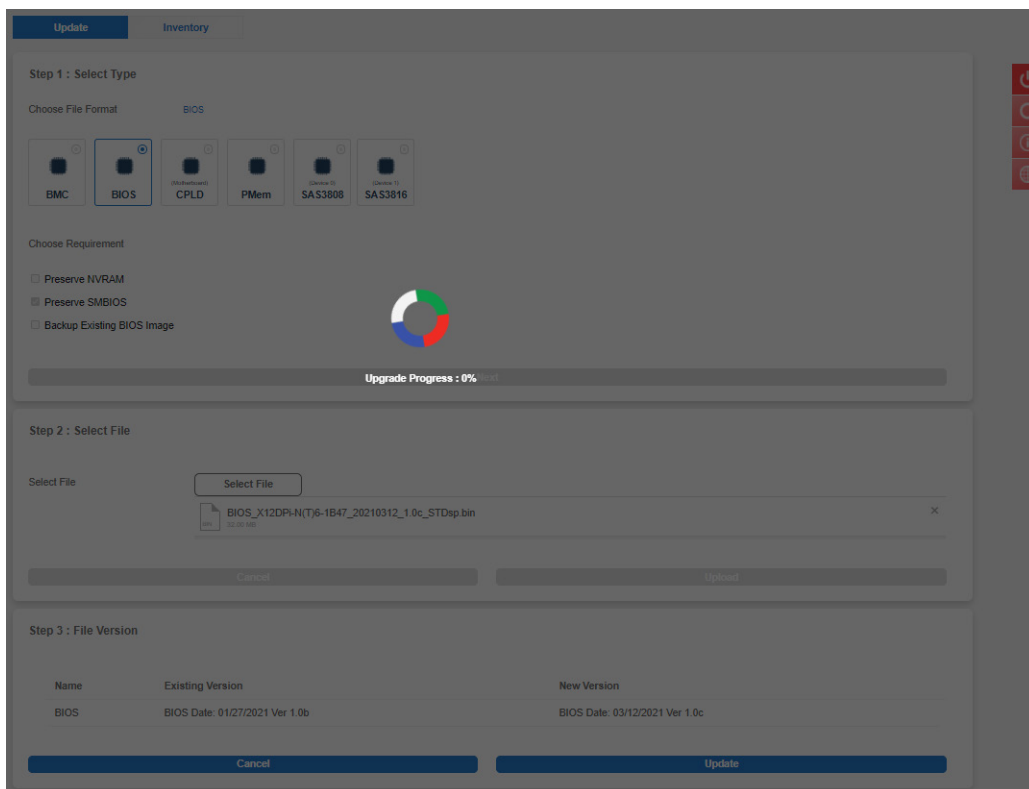


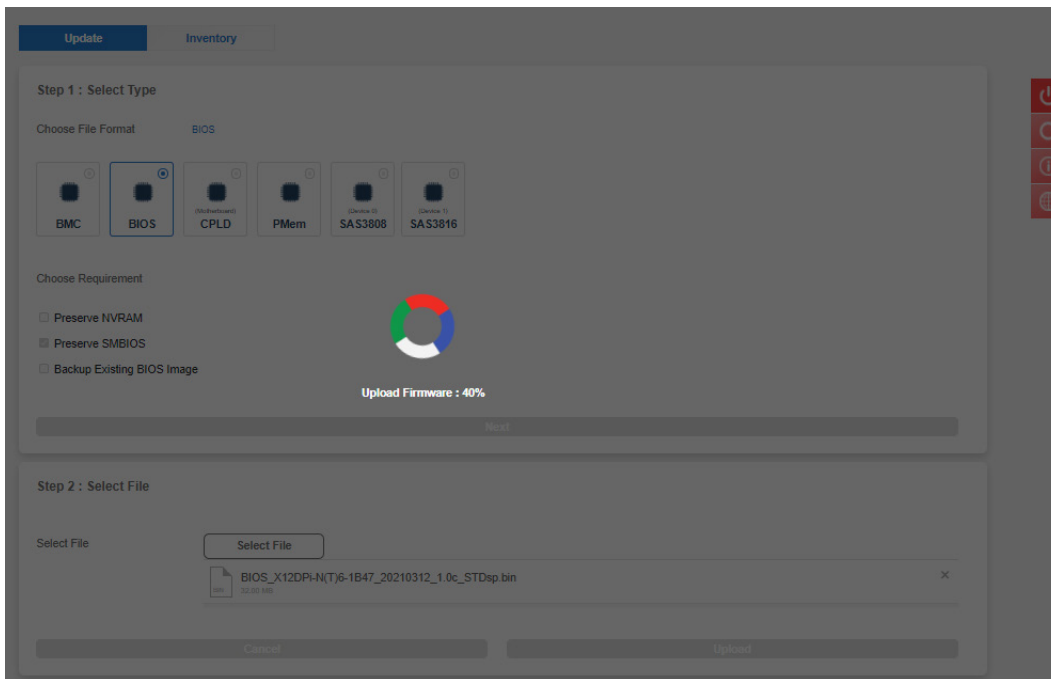
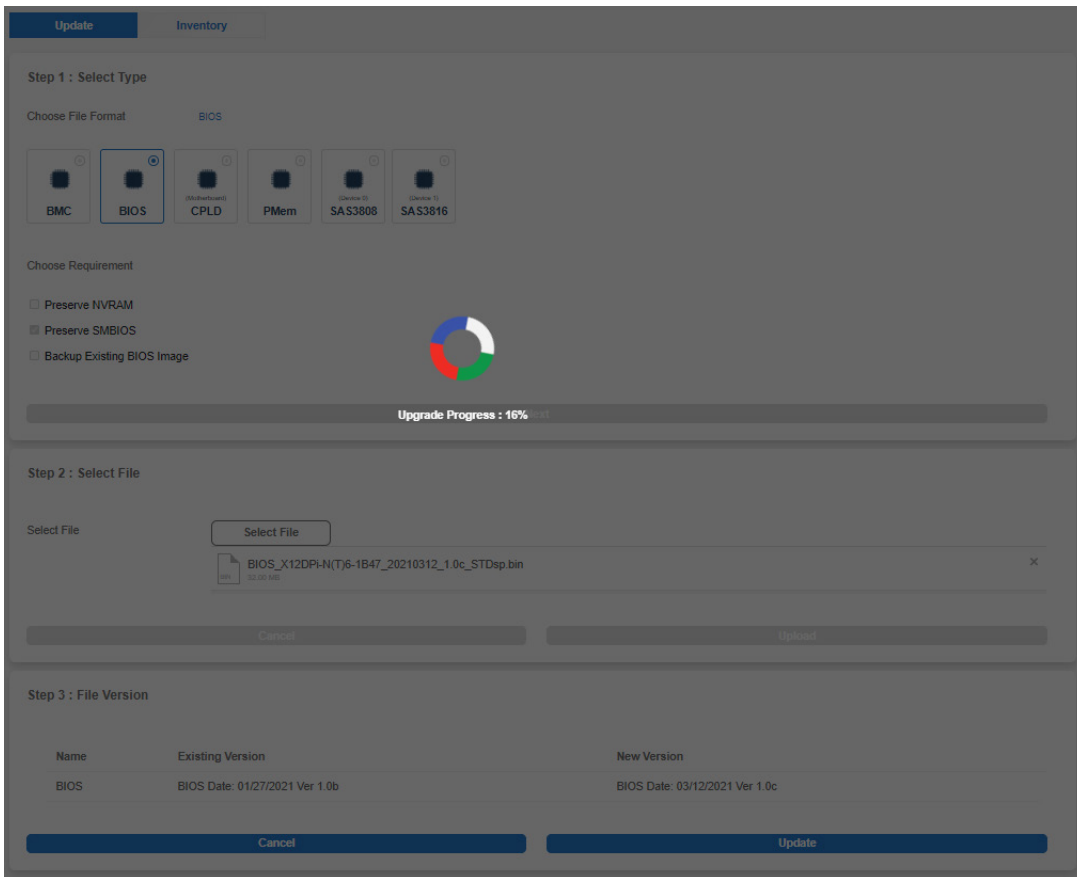


If you click “Upload” without a BIOS image included, a message will inform you to “Please select an image file. Click here to return.”

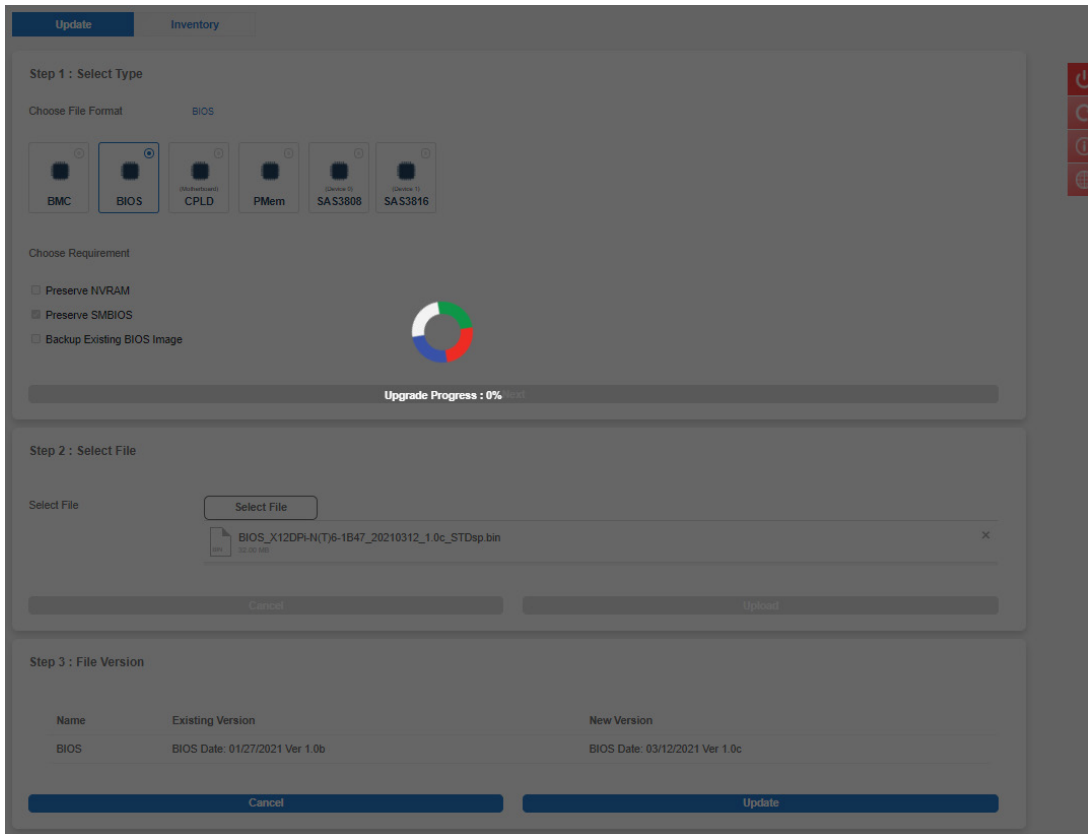
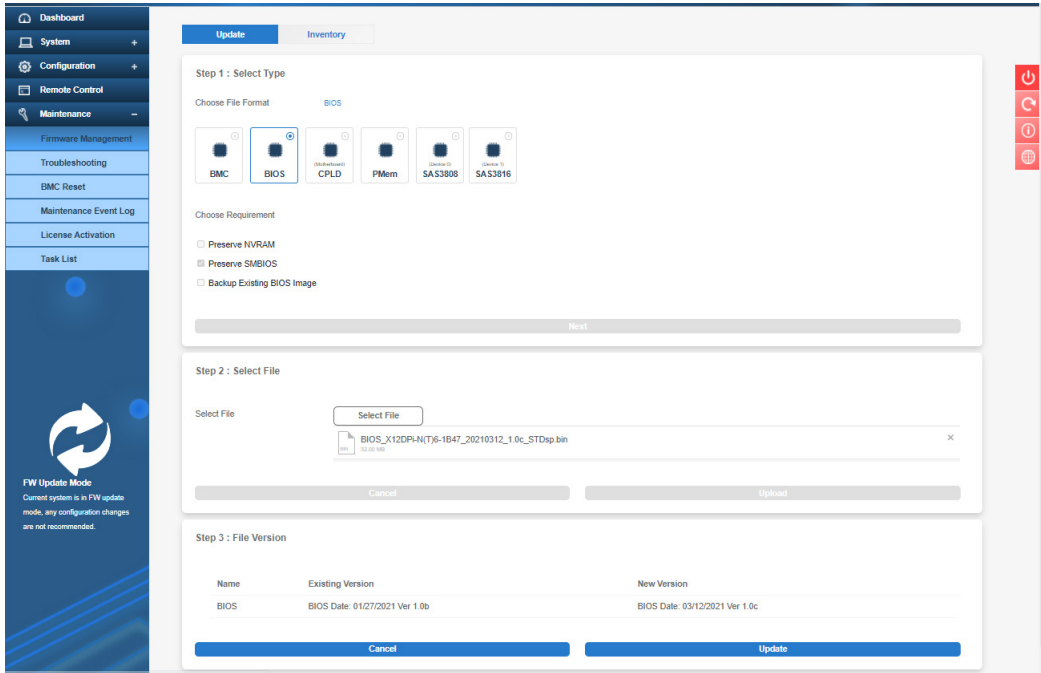


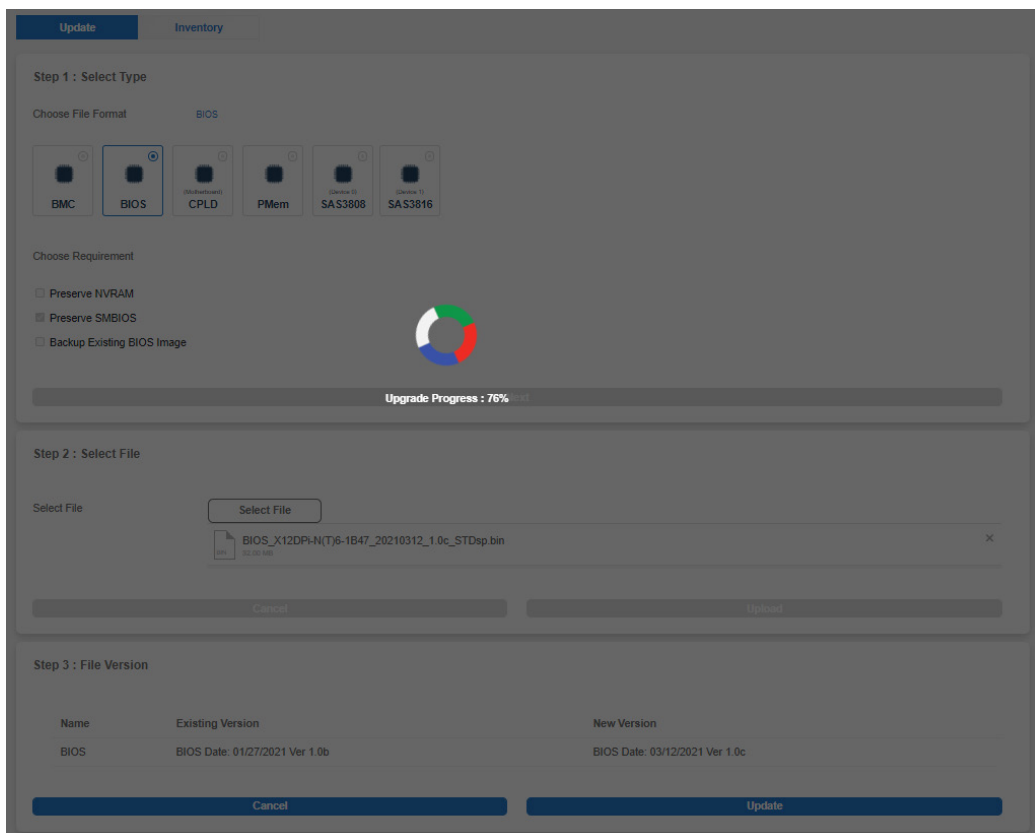
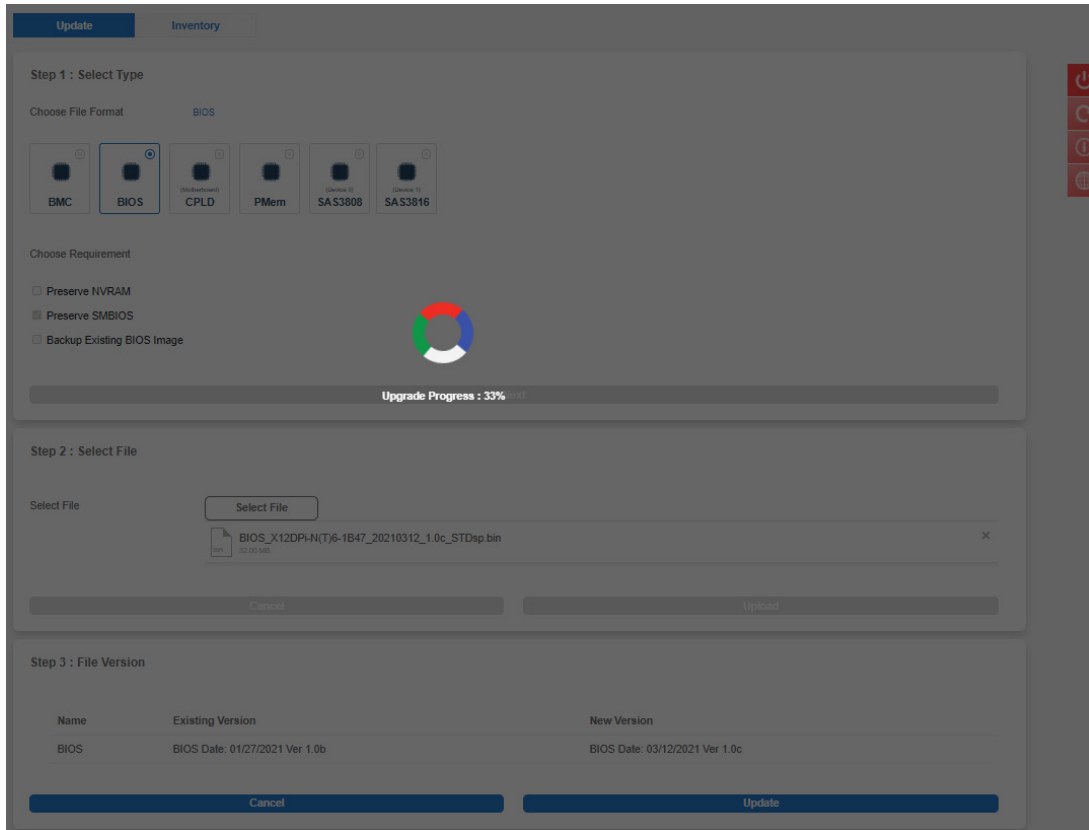
If you continue on with the BIOS update, BMC will provide a timely percentage of completion. See the example below for details.

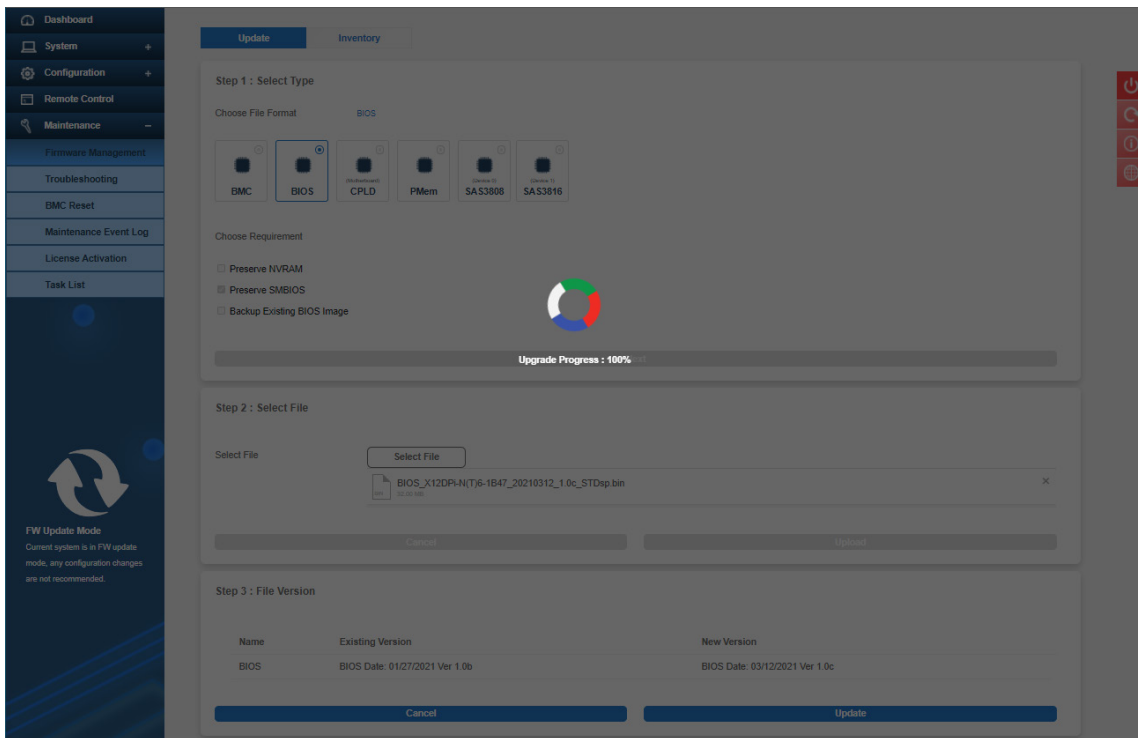
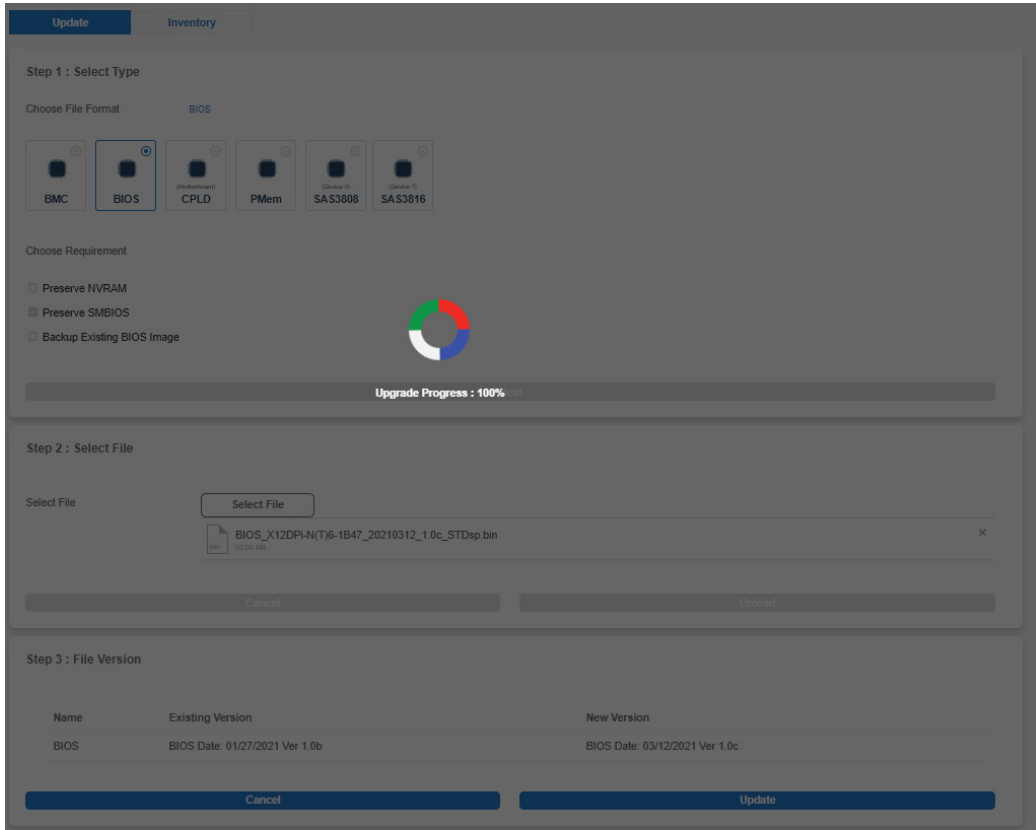














**Note:** If you cancel the BIOS updating process, there will be an alert message that pops up to ask you “Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode.” BMC is then reset with the message “BMC Reset Initiated..please wait for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

The screenshot shows the BIOS update interface with a confirmation dialog box overlaid. The dialog box contains the following text:

⚠ Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode

Buttons: Close, OK

The background interface shows the following steps:

- Step 1 : Select Type**
  - Choose File Format: BIOS (selected)
  - Choose Requirement:
    - Preserve NVRAM
    - Preserve SMBIOS
    - Backup Existing BIOS Image
- Step 2 : Select File**
  - Select File: BIOS\_X12DPi-N(T)6-1B47\_20210312\_1.0c\_STDsp.bin
- Step 3 : File Version**

Name	Existing Version	New Version
BIOS	BIOS Date: 03/12/2021 Ver 1.0c	BIOS Date: 03/12/2021 Ver 1.0c

**Update** | Inventory

Step 1 : Select Type

Choose File Format: BIOS

BMC | BIOS | CPLD | SAS3808 | SAS3816 | SAS3408

Choose Requirement

Preserve NVRAM  
 Preserve SMBIOS  
 Backup Existing BIOS Image

BMC Reset Initiated...please wait for 60 seconds and reconnect

Step 2 : Select File

Select File: Select File

BIOS\_X12DPI-N(T)6-1B47\_20210312\_1.0c\_STDsp.bin

Cancel | Updated

Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 03/12/2021 Ver 1.0c	BIOS Date: 03/12/2021 Ver 1.0c

Cancel | Update

## BIOS Update Page for Tatlow Platforms

**Update**   Inventory

**Step 1 : Select Type**

Choose File Format   BIOS

BMC    BIOS

Choose Requirement

- Preserve SMBIOS
- Preserve OA
- Preserve BIOS Setup Configuration
- Preserve BIOS Setup password
- Preserve BIOS Secure Boot Keys
- Preserve BIOS Boot Options Configuration

**Next**

## Inventory

Use this page to view the component firmware inventory and manage the Platform Firmware Resiliency (PFR) options for Root of Trusted (RoT) supported devices.

Name	Version
BIOS	BIOS Date: 08/14/2020 Rev 1.0
BIOS Backup	BIOS Date: 06/17/2020 Rev 1.0
BIOS Golden	BIOS Date: 06/17/2020 Rev 1.0
BIOS Staging	BIOS Date: 08/14/2020 Rev 1.0
BMC	00.10.47
BMC Backup	00.10.21
BMC Golden	00.10.21
BMC Staging	00.10.46
CPLD Motherboard	F1.00.B7

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
- CPLD Backplane (\* If multiple CPLD backplane than append [num] at the end)
- CPLD Motherboard
- Multi-node EC
- Power Supply (\* if multiple PSU than append [num] at the end)



**Note:** Staging Firmware – RoT stores firmware in a temporary staging area for back-up, recovery, or evidence. To be consistent, the word “Ver” is used after the firmware date for BIOS. The list on the next page is a sample of possible firmware in Inventory.



---

---

Name	Version
====	=====
88NR2241 Device 0	1.0.0.9447
BIOS	BIOS Date: 03/12/2021 Ver 1.0c
BIOS Backup	BIOS Date: 03/12/2021 Ver 1.0c
BIOS Golden	BIOS Date: 10/06/2020 Ver 1.0
BIOS Staging	BIOS Date: 03/12/2021 Ver 1.0c
BMC	01.00.15
BMC Backup	Not Present
BMC Golden	00.10.85
BMC Staging	01.00.15
CPLD Motherboard	F1.00.B7
PowerSupply1	1.4
PowerSupply2	1.4
SAS3808 Device 1	16.00.08.00
SAS3816 Device 0	16.00.02.00
SAS3916 Device 2	5.130.02-3170
NIC1_ SXB1 Slot2	N:014000000:010A1500T:00000000
NIC2_AOC-2UR68G4-i4XTS SXB3 Slot0	01C3

**Samples of Inventory Page**

Update **Inventory**

Filter

Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 10/06/2020 Ver 1.0
BIOS Backup	BIOS Date: 07/31/2020 Ver 1.0
BIOS Golden	BIOS Date: 05/14/2020 Ver 1.0
BIOS Staging	BIOS Date: 10/06/2020 Ver 1.0
BMC	00.10.83
BMC Backup	00.10.41
BMC Golden	00.10.37
BMC Staging	00.10.83
CPLD Motherboard	F1.00.B7

1 / 9

Update **Inventory**

Add Filter

Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 01/12/2021 Rev 1.0a
BIOS Backup	BIOS Date: 01/12/2021 Rev 1.0a
BIOS Golden	BIOS Date: 01/12/2021 Rev 1.0a
BIOS ME	4.4.3.203
BIOS Staging	BIOS Date: 01/12/2021 Rev 1.0a
BMC	55.04.10 dbgs
BMC Backup	55.04.10 dbgs
BMC Golden	Not Present
BMC Staging	55.04.10 dbgs
CPLD Backplane0	N/A
CPLD Motherboard	f0.0a.50

Page 1 of 1

1 - 11 of 11 items

Update Inventory

Add Filter +

Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 01/12/2021 Rev 1.0a
BIOS Backup	Not Present
BIOS Golden	Not Present
BIOS ME	4.4.3.263
BIOS Staging	BIOS Date: 1/12/2021 Rev 1.0a
BMC	00.11.32 dbgs
BMC Backup	9.08.25
BMC Golden	Not Present
BMC Staging	00.11.32 dbgs
CPLD Backplane0	CPLD_ID: 0023 Rev: 0b
CPLD Motherboard	f0.0d.50
Multi-node EC	1.17

Page 1 of 1 1 - 12 of 12 items

Update Inventory

Filter

X BMC X BIOS X CPLD X SAS

Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 12/17/2020 Ver 1.0a
BIOS Backup	BIOS Date: 08/18/2020 Ver 1.00
BIOS Golden	BIOS Date: 08/18/2020 Ver 1.00
BIOS Staging	BIOS Date: 12/17/2020 Ver 1.0a
BMC	00.10.83
BMC Backup	00.10.77
BMC Golden	00.10.24
BMC Staging	00.10.83
CPLD Motherboard	F1.00 BE
SAS3108 Device 0	4.880.00-8485

1 / 1 1 - 10 / 10

Update **Inventory**

Filter


X BMC X BIOS X CPLD X SAS

Platform Resiliency Actions

Name ↑	Version
BIOS Golden	BIOS Date: 09/16/2020 Ver 1.0
BIOS Staging	BIOS Date: 09/16/2020 Ver 1.0
BMC	09.20.19
BMC Backup	09.25.09
BMC Golden	09.25.09
BMC Staging	09.20.19
CPLD Motherboard	F1.00.00
SAS3408 Device 2	5.140.01-3319
SAS3819 Device 0	18.00.04.219
SAS3919 Device 1	5.140.02-3408

1 / 1 1 - 10 / 10

## 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 on the Platform Resiliency Actions page. Click on the Editor button () next to **Platform Resiliency Actions** to perform following the 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, 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 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. Options include Golden BMC and Golden BIOS. Once finished, click on [Update].
- **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 creates 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. Please make sure to download evidence before initiating a firmware update.

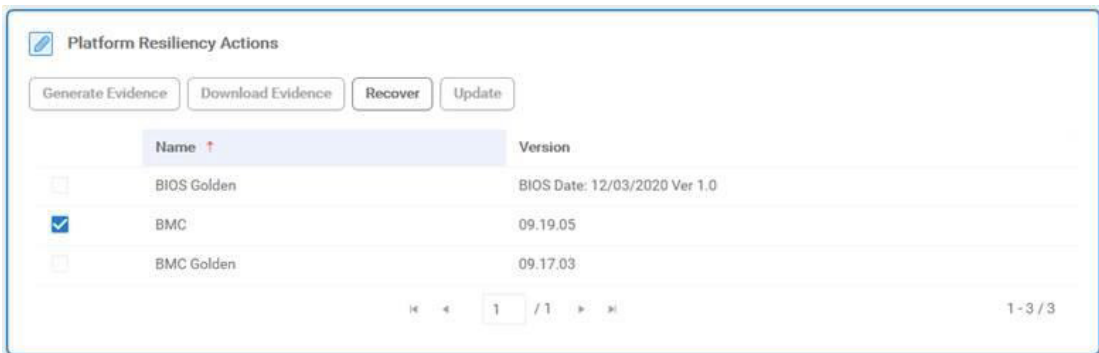
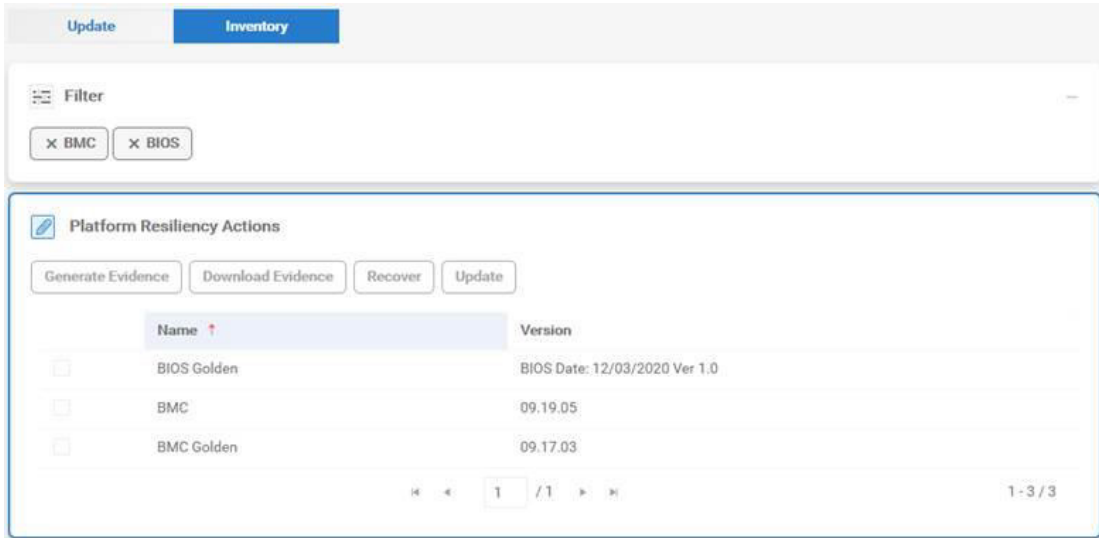
- **Download Evidence:** Once a compressed evidence file is generated, the Download Evidence button will be enabled. Click to download the evidence.



**Note 1:** Compressed evidence fill will be deleted during the BMC reset operation. You can regenerate the compressed evidence file if needed.

**Note 2:** Non-RoT platforms will not support Platform Firmware Resiliency actions.

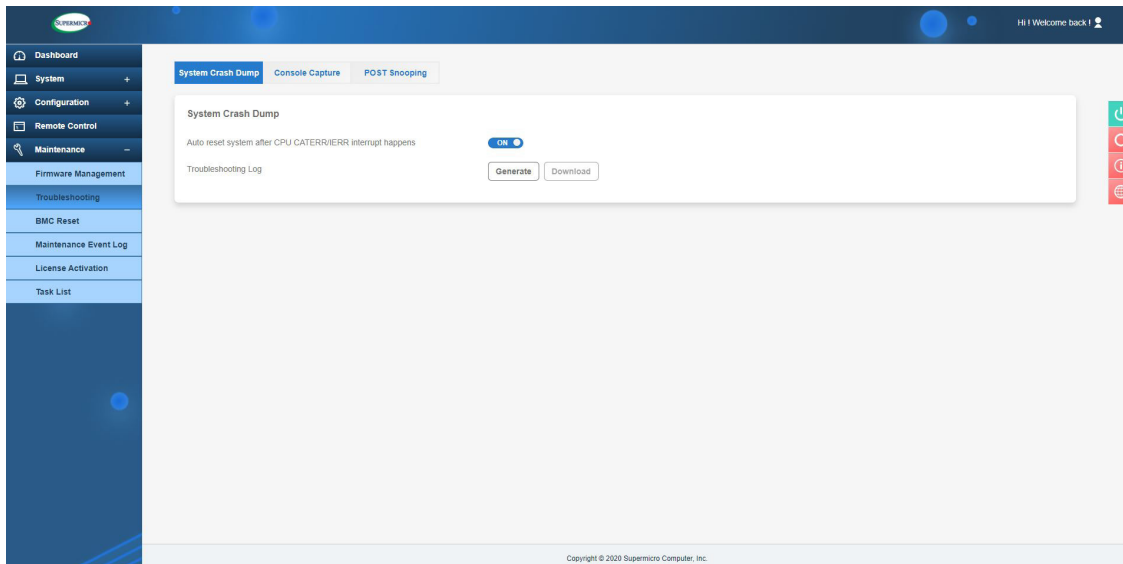
The below images are snapshots of the Inventory page. When one of the action buttons is selected, unavailable or non-applicable action buttons (e.g., Generate Evidence, Download Evidence, Recover, and Update buttons) will be greyed out.



## 2.8.2. Troubleshooting

### System Crash Dump

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



You can adjust the following options.

- Auto reset system after CPU CATERR/IERR interrupt happens: The check box allows you to select reset the 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: You can generate a new crash dump.

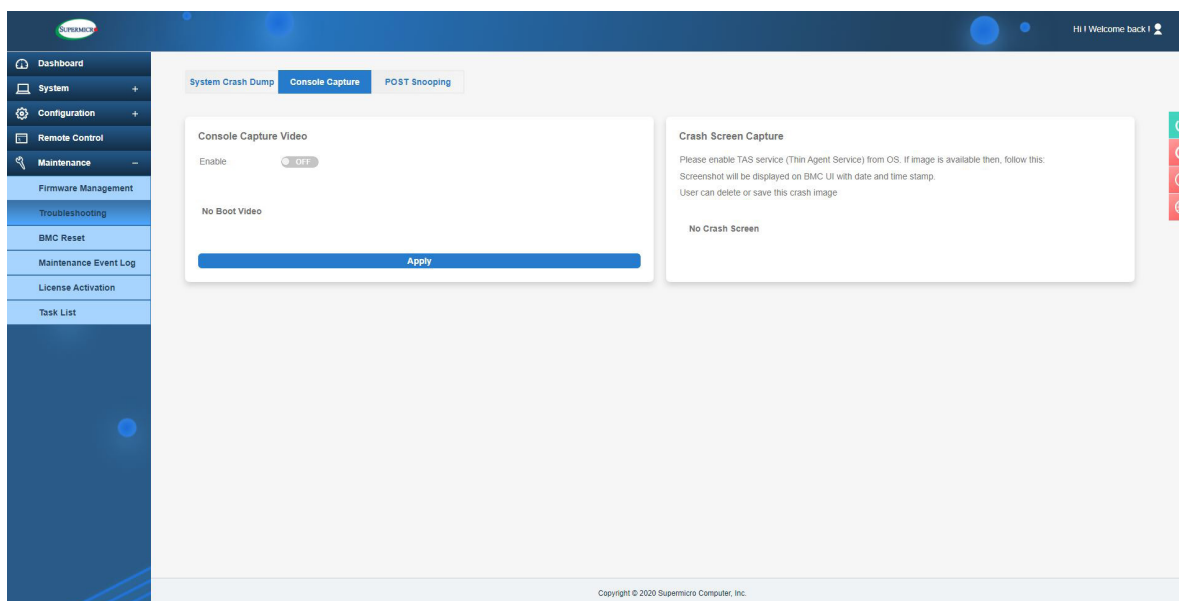


**Note:** Upon clicking [Generate], the system will remove previous error logs or dump available files and regenerate a new dump file.

- Download: You can download the current crash dump file.

## Console Capture

This page displays Crash Capture for a screenshot and video of the console with the running operating System.



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

- Disable/Enable: You can enable or disable this option. By default, it will be disabled.
- Record until buffer is full: You can record video of the console until the buffer is full. The video will be saved in AVI format and the maximum buffer size is 32 MB (approximate time calculated based on video size).
- Record until POST ends: You can record video until POST ends or record until the timeout value is reached. BMC will receive POST completion information from BIOS and record video until that time. If any delay is introduced, then BMC will record until a timeout period of approximately **eight 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 the selected video from here.
- AC Cycle/Factory Reset: Upon reset, all videos will be deleted.



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



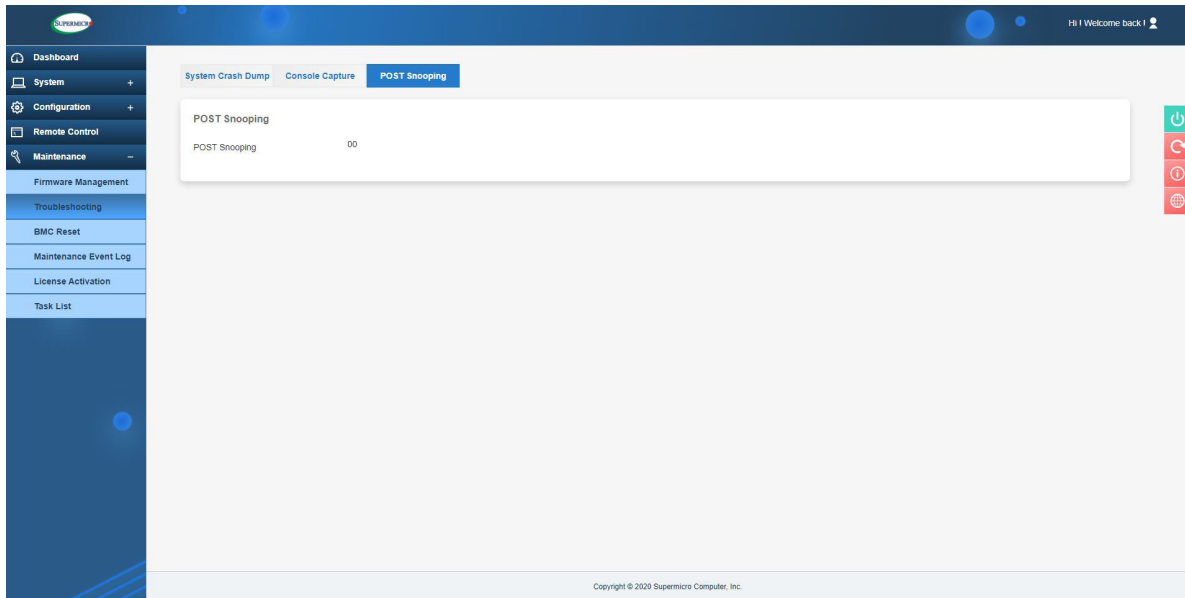
**Note 1:** The table below shows the supported and unsupported server platforms (non-workstations) for System Crash Dump, Console Capture Video, and Crash Screen Capture features. We will enable the functions when they are supported. Due to time constraints, Console Capture Video and Crash Screen Capture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

**Note 2:** All workstations and Atom-based motherboard platforms are not supported.

<b>Supported and Unsupported Server Platforms (Non-Workstation)</b>			
	<b>System Crash Dump</b>	<b>Console Capture Video</b>	<b>Crash Screen Capture</b>
<b>Whitley Non-Workstation Platforms (Intel ICE Lake)</b>	Supported	Supported	Supported
<b>Purley Platforms Non-Workstation (Intel Sky Lake)</b>	Supported	<b>Not Yet Supported</b>	<b>Not Yet Supported</b>
<b>MicroCloud Non-Workstation (Intel Rocket Lake)</b>	<i>Unsupported</i>	<i>Unsupported</i>	<i>Unsupported</i>
<b>IoT Solutions (Intel Atom based MB)</b>	<i>Unsupported</i>	<i>Unsupported</i>	<i>Unsupported</i>
<b>AMD H12_AST2600 Platforms (RoT and non-RoT)</b>	Supported (download only)	Supported	Supported
<b>AMD H12_AST2500 Non-Workstation Platforms (RoT and non-RoT)</b>	Supported (download only)	<i>Unsupported</i>	<i>Unsupported</i>
<b>AMD H11_AST2500 (Non-Workstation)</b>	Supported (download only)	<i>Unsupported</i>	<i>Unsupported</i>

## POST Snooping

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



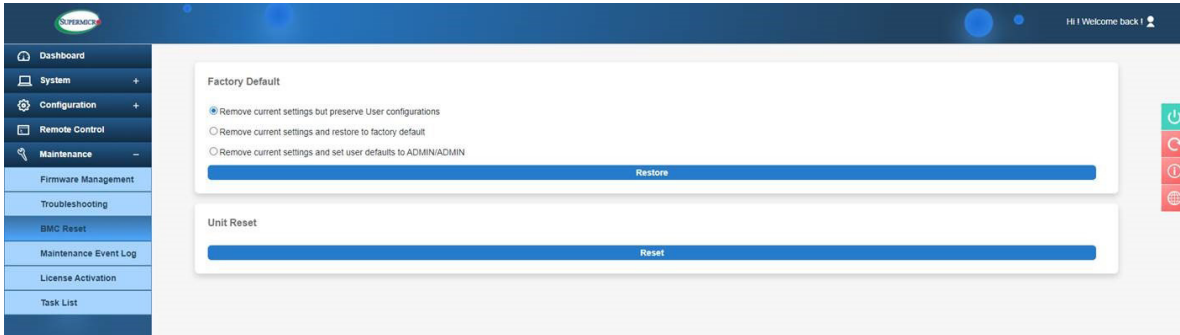
## 2.8.3. BMC Reset

### Factory Default

You can select the following options to restore BMC to the factory default settings.

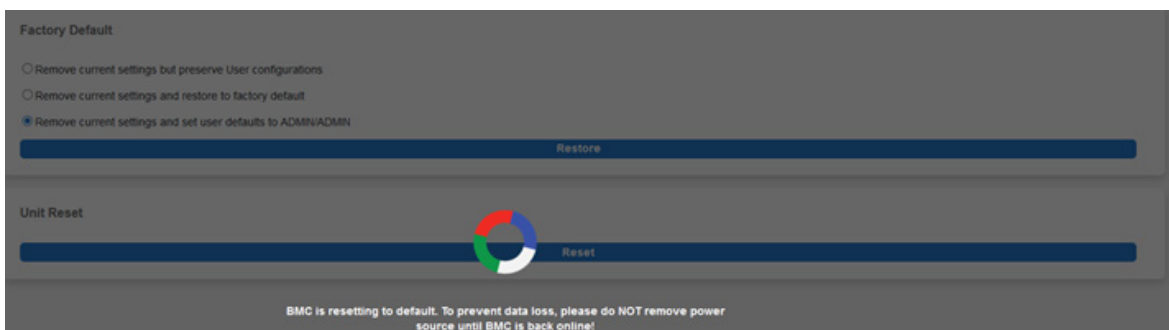


**Note:** You will get a prompt that “BMC is resetting to default. To prevent data loss, please do NOT remove the power source until BMC is back online!”




This feature includes the following options.

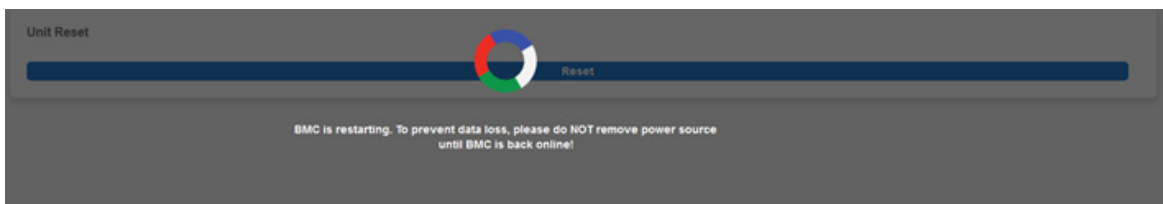
- Remove current settings but preserve user configurations: You can restore all configurations to factory default and preserve all user configurations.
- Remove current settings and restore to factory default: You can restore all the configurations to factory default. This option will remove all users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



## Unit Reset


This feature allows you to reset an IPMI device.

 **Note:** You will get a prompt that “BMC is restarting. To prevent data loss, please 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).

Advanced Settings

Filter

Select an event log category:  Storage  Account  Network  Service  Others

Maintenance Event Log


Clear All the Event Logs


Export to Excel

Severity	Date/Time	Interface	User	Source	Description	Category
	2020-10-03 16:02:58	DRTM	ADMIN(ADMIN)	Localhost	ID 0x00 - TEE FW Start (0000.00.17)	service
	2020-10-03 16:02:59	DRTM	ADMIN(ADMIN)	Localhost	ID 0x01 - SMC1_TEE_SERVICE (ST3) Start	service
	2020-10-03 16:03:00	DRTM	ADMIN(ADMIN)	Localhost	ID 0x02 - Security Functions Start (TA5)	service
	2020-10-03 16:03:01	DRTM	ADMIN(ADMIN)	Localhost	ID 0x02 - Security Functions Start (TA0)	service
	2020-10-03 16:03:02	DRTM	ADMIN(ADMIN)	Localhost	ID 0x02 - Security Functions Start (TA3)	service
	2020-10-03 16:03:43	DRTM	ADMIN(ADMIN)	Localhost	ID 0x02 - Security Functions Start (TA1)	service
	2020-10-03 16:03:44	DRTM	ADMIN(ADMIN)	Localhost	ID 0x02 - Security Functions Start (TA2)	service
	2020-10-03 16:05:02	Redfish	ADMIN(ADMIN)	10.124.8.53	Redfish session was created successfully.	account
	2020-10-03 16:05:02	Web	ADMIN(ADMIN)	10.124.8.53	Web login was successful.	account
	2020-10-03 16:05:48	Web	ADMIN(ADMIN)	10.124.8.53	Hostname was configured to NULL successfully.	network
	2020-10-03 16:05:48	Web	ADMIN(ADMIN)	10.124.8.53	IPv6 DNS server 10.2.1.225 was deleted unsuccessfully.	network
	2020-10-03 16:05:48	Web	ADMIN(ADMIN)	10.124.8.53	IPv6 address 1000:0000:0000:0000:0000:0000:0002:64 was added successfully.	network

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.

 Info event

 Warning event which needs attention

 Critical event which needs immediate actions 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 keyword-related events.

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

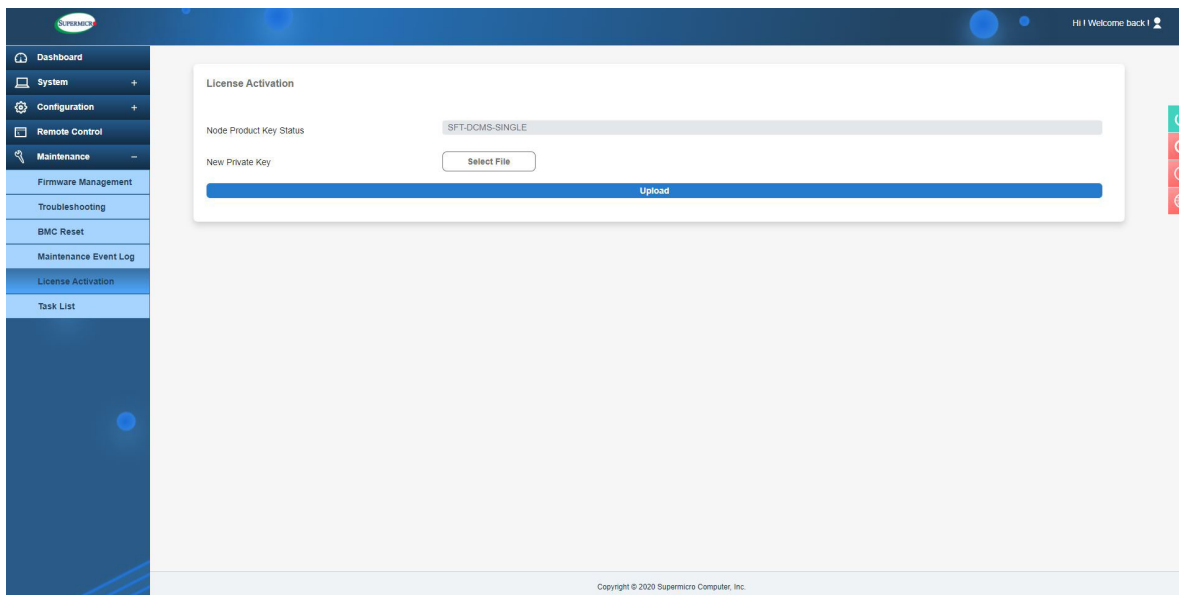
- Enable/Disable Maintenance Event Log: You can enable or disable maintenance event logs. This option is available under Advanced settings.
- Clear: You can select the respective event and click [Clear] to remove the maintenance event log entry. To clear “All the Event Logs”, enable Maintenance Event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

## 2.8.5. License Activation

This page allows you to view and configure software license activation.



**Note:** This page allows SFT-OOB-LIC and SFT-DCMS-SINGLE license activation.

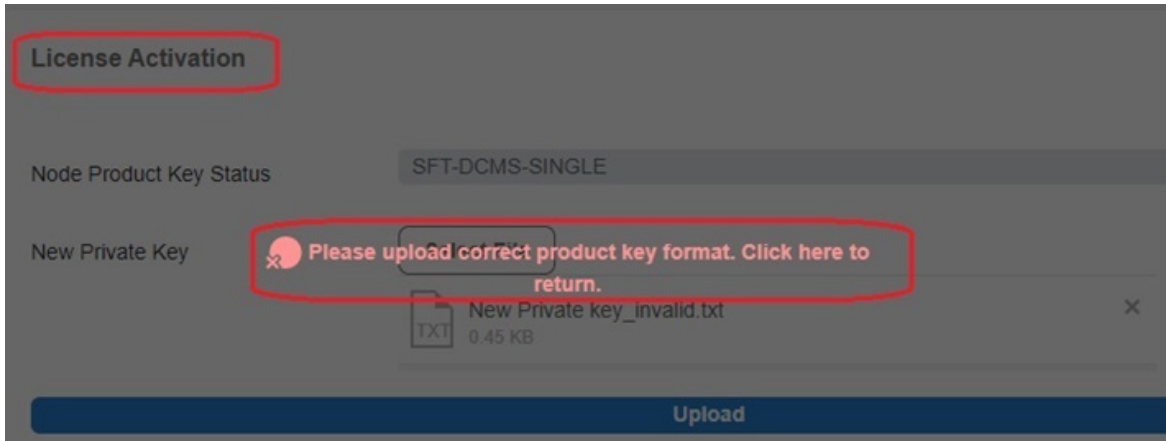


You can adjust the following settings to configure this feature.

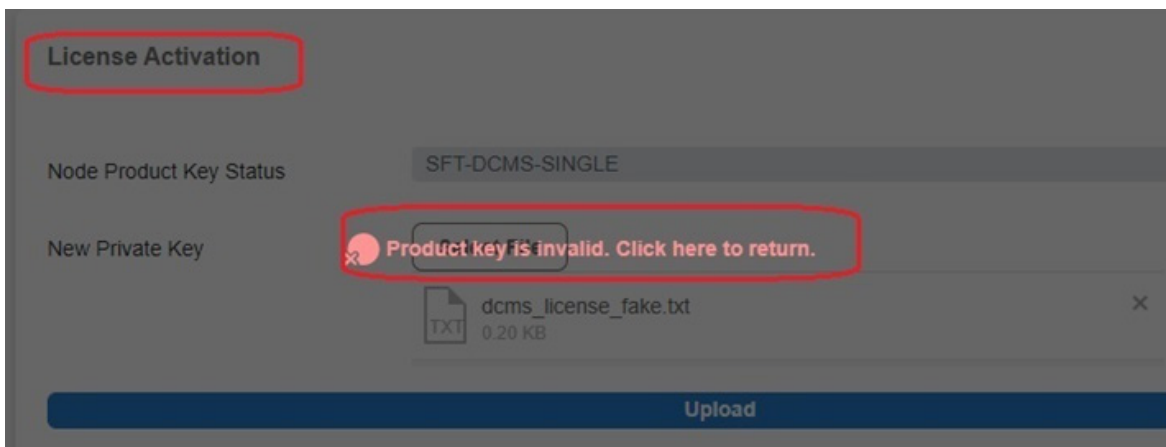
- **Node Product Key Status:** You can view the currently activated license type.
- **Activate License:** You can upload a new license file and activate it to receive end-to-end systems management functions.

When uploading the product key format, you may get a prompt message warning you of an error. Please refer to the following two cases.

1. If you upload a product key format that is invalid, you will get the prompt message, “Please upload correct product key format. Click here to return.” There is no MEL log to be generated.




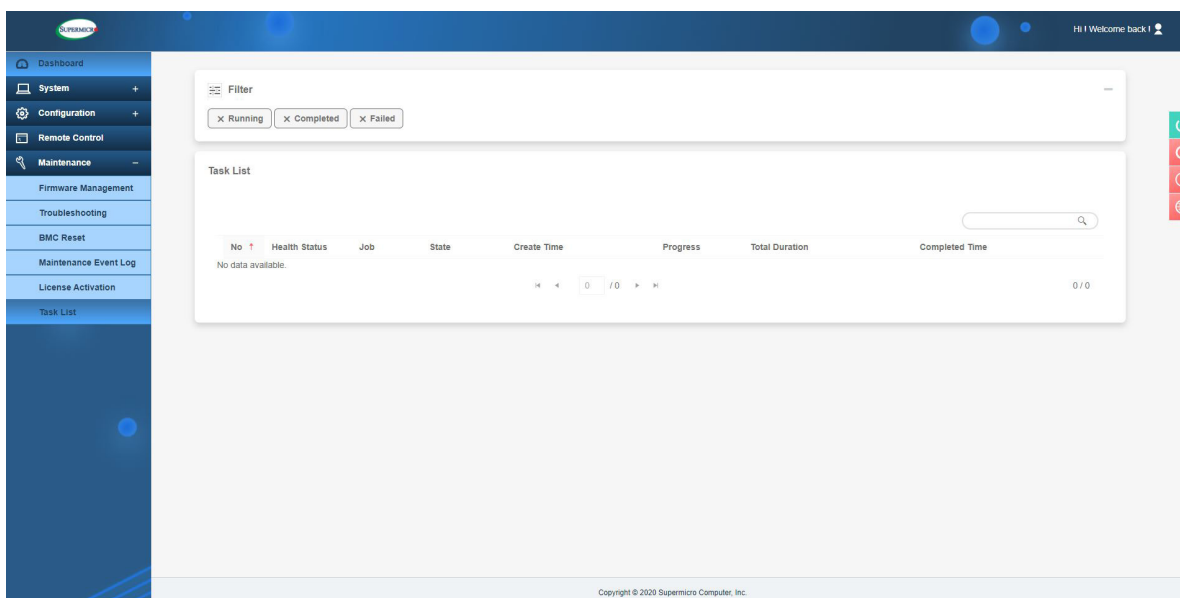
2. If you upload a product key format that is valid but the license is invalid, you will get the prompt message, “Product key is invalid. Click here to return.” A [MEL-0272] log will be generated.



## 2.8.6. Task List

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

 **Note:** Currently, it supports BMC and BIOS FW updates along with storage controller disks, which can erase task progress.



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 the task beginning.
- Progress: You can view the progress of the current task(s) being run.
- Total Duration: You can view the total time taken to finish the 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.

<b><i>UI Task Filter</i></b>	<b><i>Task List State</i></b>
<b>Running</b>	New
	Starting
	Running
	Suspended
	Interrupted
	Pending
	Stopping
	Service
	Cancelling
<b>Completed</b>	Completed
	Killed
	Cancelled
<b>Failed</b>	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, please 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<sup>2</sup>C bus. If another device accesses the I<sup>2</sup>C bus frequently, it might cause a collision with the BMC when this device accesses the I<sup>2</sup>C bus. When you see this error, please uninstall `lm_sensors` in Linux.

## Appendix A

# Firmware Update via WEB GUI and SUM

### A.1 Overview

This user's guide provides detailed information on how to update Supermicro BMC firmware on X13 series motherboards using BMC WEB GUI or SUM (Supermicro® Update Manager).

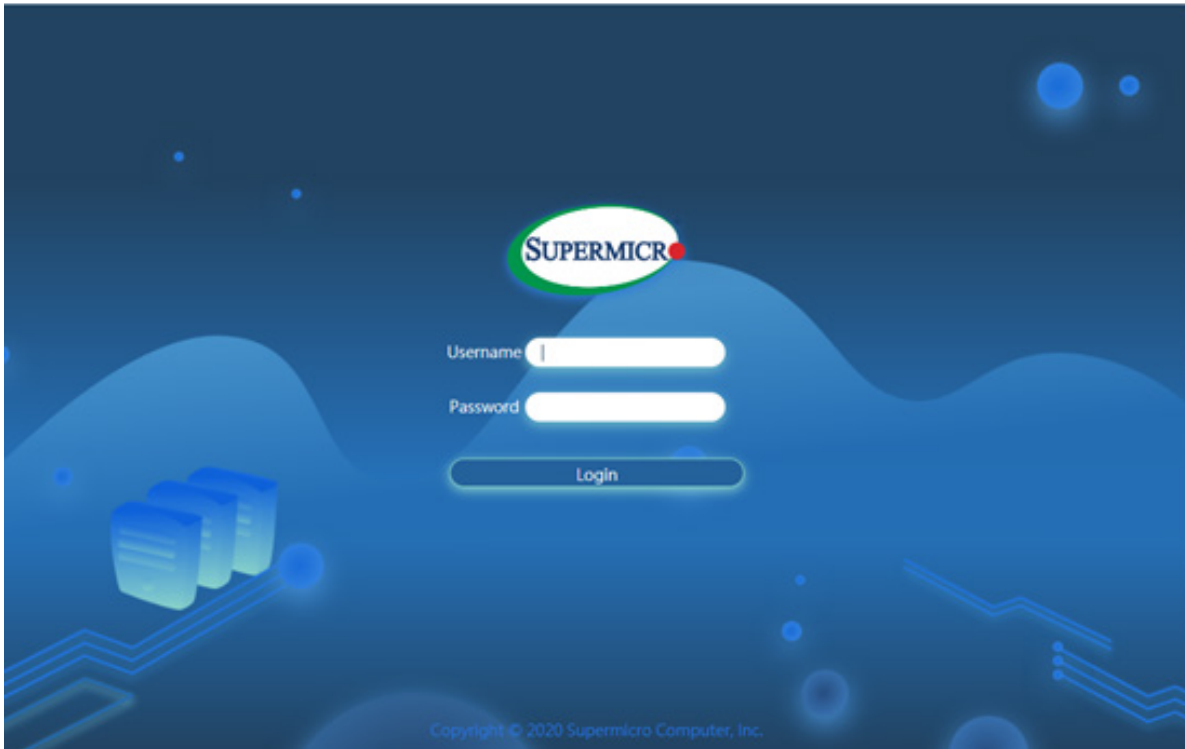


**Note:** For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI UEFI BIOS, RSD/SCC, TAS, and IPMIView, please refer to our website at <https://www.supermicro.com/en/solutions/management-software/bmc-resources> for details.

## A.2 Updating Firmware Using BMC WEB GUI

In order to keep the system working properly, please follow the steps below to update BMC firmware through BMC WEB GUI:

1. Log into the account by entering the IP address on a web browser and follow the prompts on the screen.

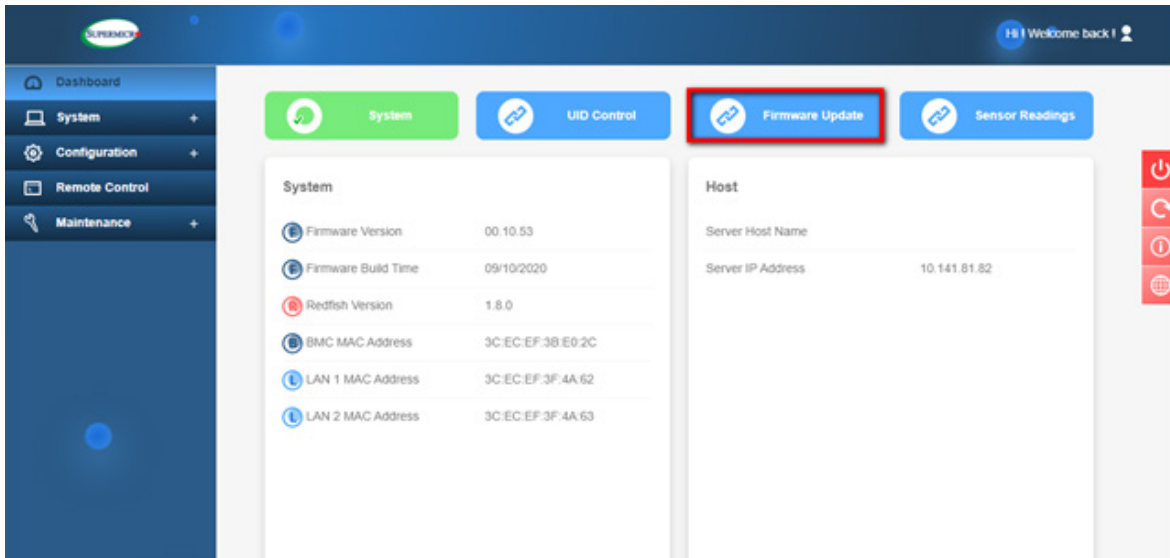


**Figure 1: BMC Firmware Web User Login**



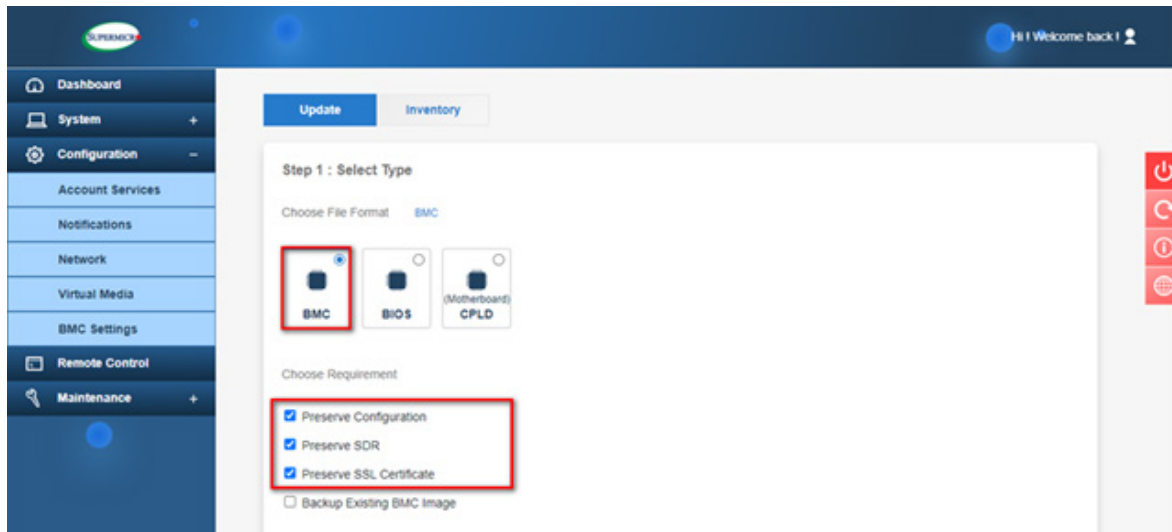
**Note:** Please contact Supermicro sales or FAE if you do not know your username or password.

2. Click on the Firmware Update tab on the BMC dashboard.



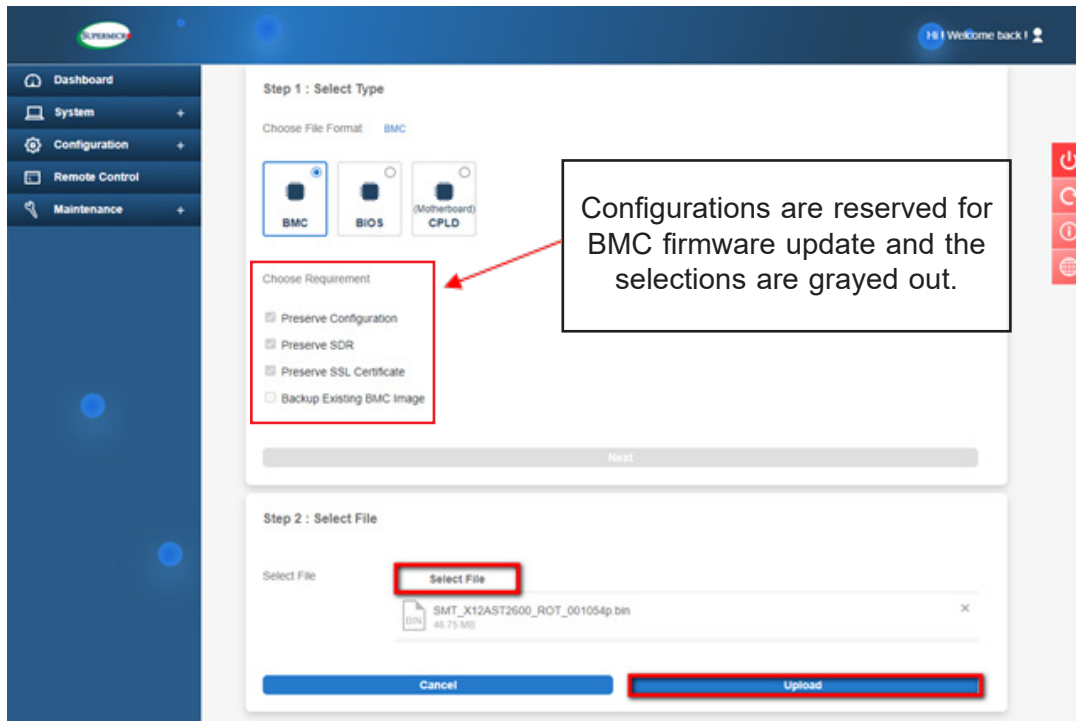
**Figure 2: BMC Firmware Update Dashboard**

3. When the following screen appears, select the [BMC] option and click [Next].



**Figure 3: BMC Firmware Update Default Setting**

4. Press [Select File] to select the new BMC firmware file and press [Upload] as shown below.



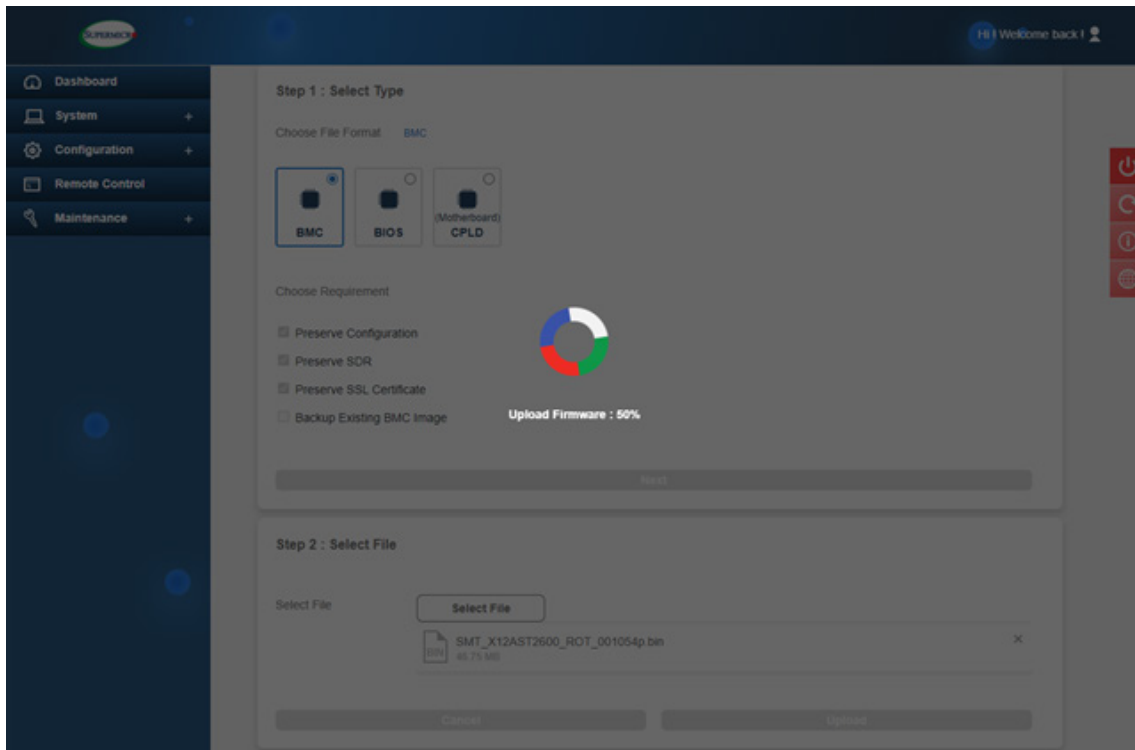
**Figure 4: Select and Upload New BMC Firmware File**

**Note 1:** By default, the firmware update process preserves the existing configuration, SDR, and SSL certificates for the new BMC firmware. You can unselect any of the preservation options if applicable.

**Note 2:** Select the "Backup existing image" option to backup existing BMC or BIOS images. 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. Non-ROT platforms will not display the "Backup existing image" option.



5. Wait for the upload process to complete, which might take a few minutes.



**Figure 5: New BMC Firmware Uploading**

6. Verify the new firmware version and press [Update] to perform the firmware update.

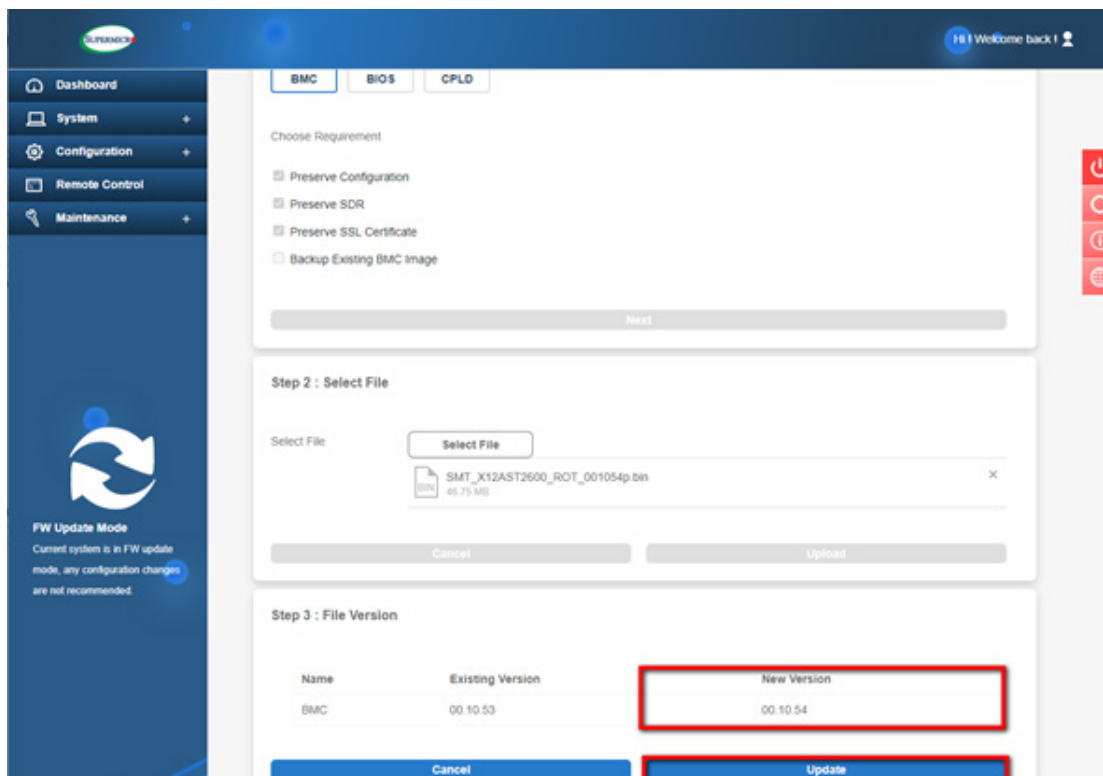
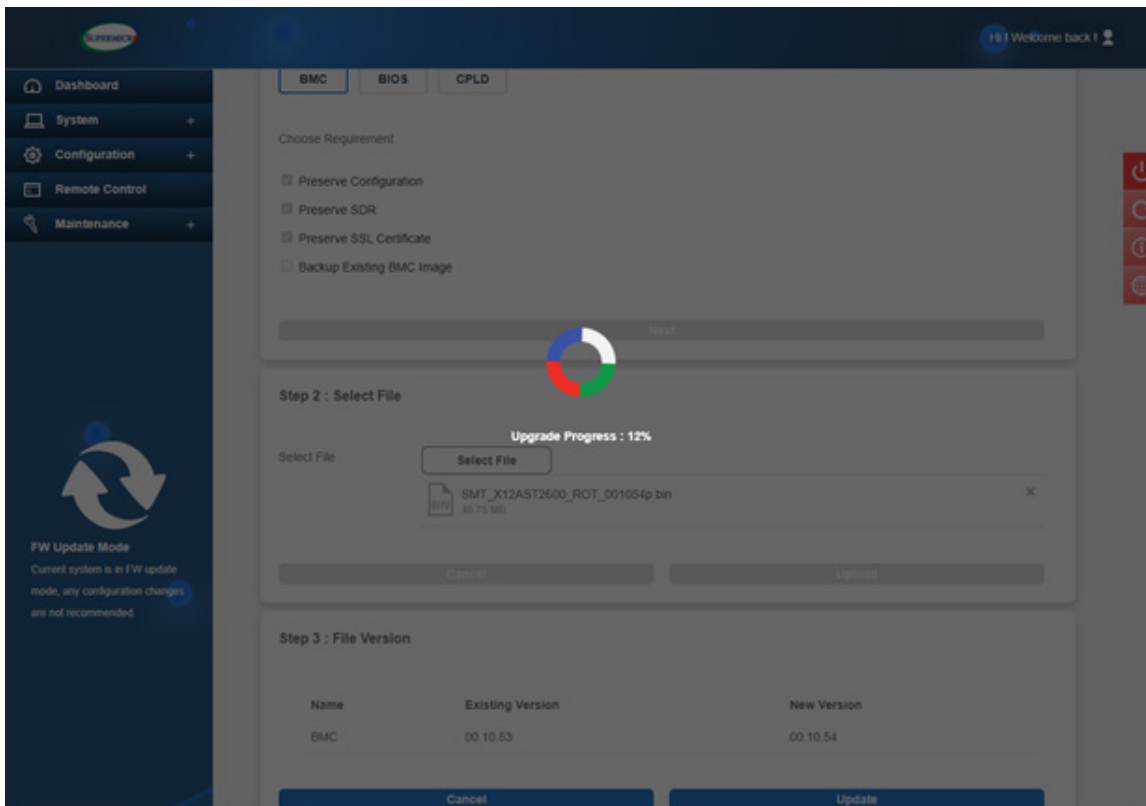


Figure 6: Verify the New BMC Firmware Version

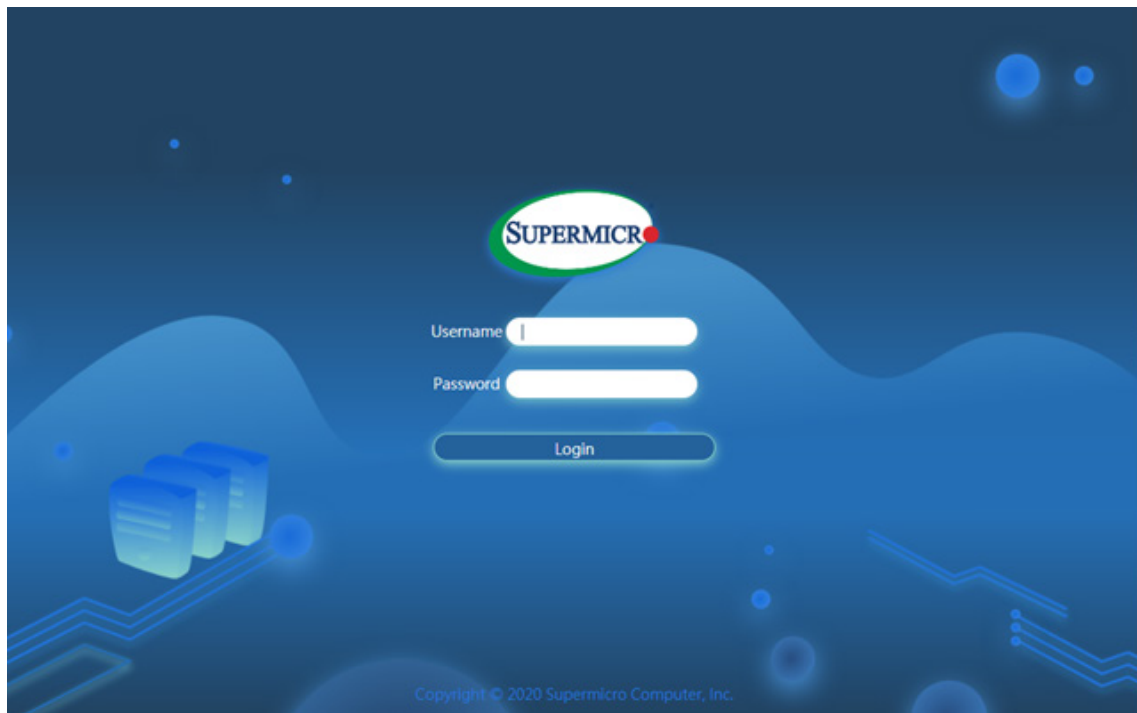
7. Wait for the update process to be completed. It might take a few minutes. Any system configuration change is not recommended during the update process.



**Figure 7: BMC Firmware Updating in Progress**

8. BMC will reboot after the firmware is completely updated. Please wait for BMC to complete the system reboot.

9. Once the reboot process is complete, WEB GUI will return to the login screen, and you will need to log in to the system again.



**Figure 8: BMC Firmware Web User Login**

## A.3 Updating Firmware Using SUM

Please follow the procedure below to update BMC firmware in SUM (Supermicro® Update Manager).

### Step 1: Installing SUM

To install SUM in Linux/FreeBSD OS, following the steps below. Windows installation is similar.

1. Extract the `sum_x.x.x_Linux_x86_64_YYYYMMDD.tar.gz` archive file.
2. Go to the extracted `sum_x.x.x_Linux_x86_64` directory. Rename this directory to "SUM\_HOME".
3. Run SUM in the `SUM_HOME` directory.

#### 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 steps below to update BMC firmware:

1. Use the command “UpdateBmc” to run SUM to update BMC firmware.

**Syntax:**

```
sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>]  
-c UpdateBmc --file <filename> [--overwrite_cfg] [--overwrite_sdr]  
[--backup] [--forward]
```

2. The progress of the firmware update will be displayed as shown below. DO NOT interrupt the process until it is complete. BMC will reboot after the firmware is completely updated. Please wait for BMC to complete the system reboot. (Figure 9)

**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.
- 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>`







## Appendix B

# Introduction to SMASH

## B.1 Overview

The SMASH (System Management Architecture for Server Hardware) 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-servers 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.

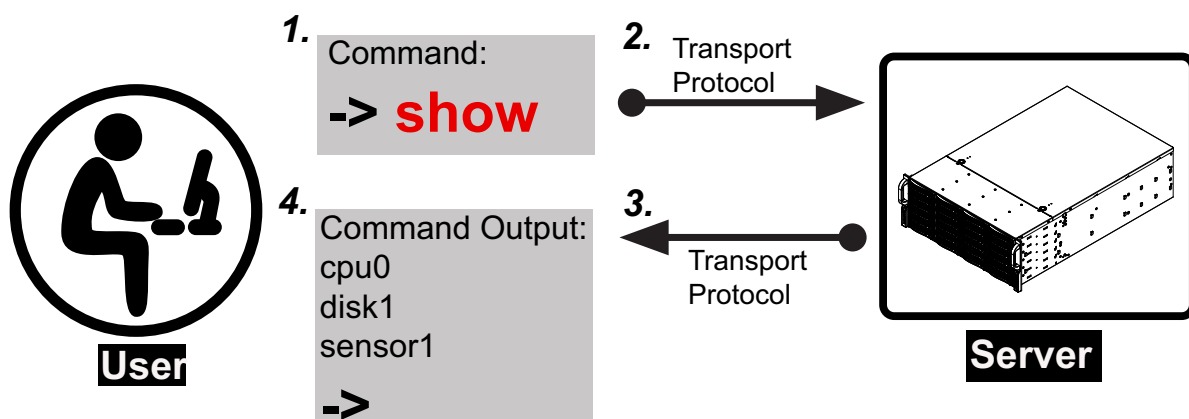


Figure 1 SMASH-CLP User Interface

## 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 (DSP0004)
- 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 the 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, please 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 the system management in a web-based environment. Refer to the SMASH script provided below to curtail a server management protocol for the systems.



**Note:** The instructions listed below are applicable to both Windows and Linux systems. We use the Windows platform as our default setting.

## 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 (Baseboard Management Controller) via 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 in to the SSL network, the SMASH Command Line Protocol Main screen will display as shown below.

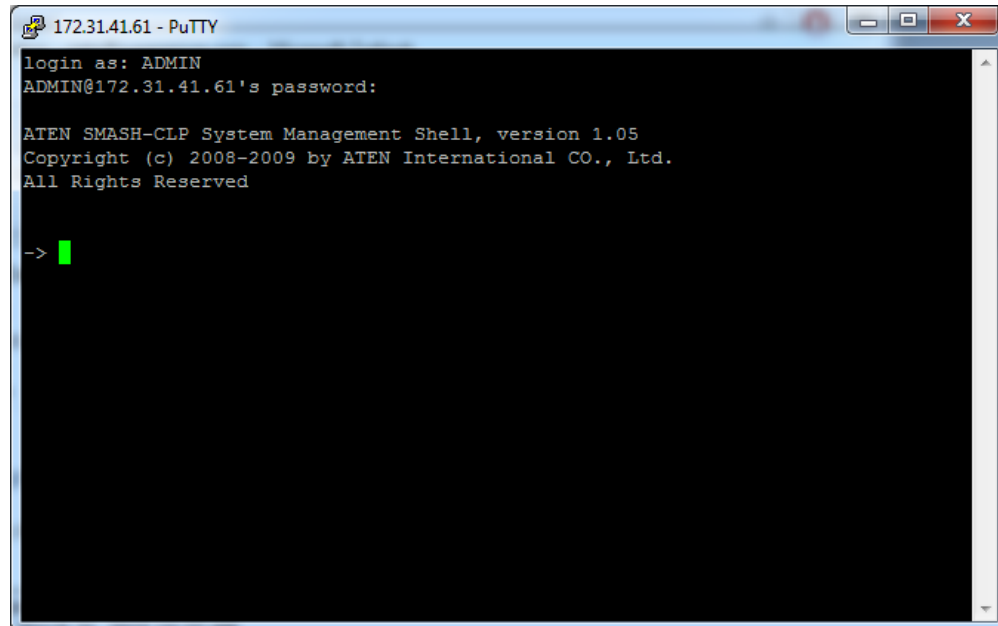



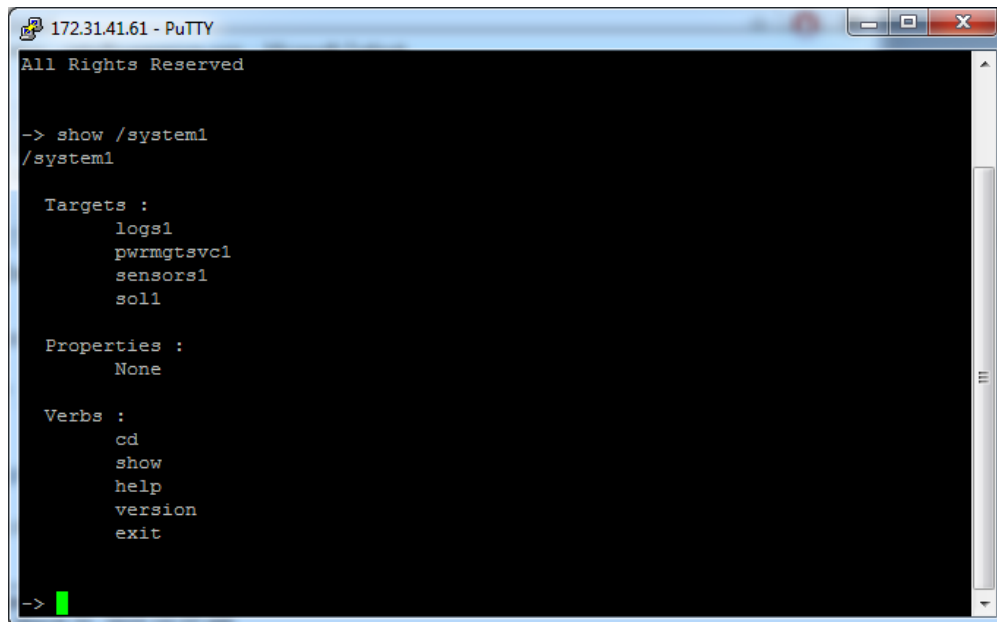
Figure 2 SMASH-CLP Main Screen

## 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 follow the instructions below.

 **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.



```
172.31.41.61 - PuTTY
All Rights Reserved

-> show /system1
/system1

Targets :
  logs1
  pwrmgtsvc1
  sensors1
  sol1

Properties :
  None

Verbs :
  cd
  show
  help
  version
  exit

->
```

Figure 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, group of targets, and a sub-groups of the target(s). This will include properties, contents, supported operations related to the target, the group of targets, or their sub-targets.

- ***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 item. 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, stop a process, or 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 item in the MAP. It can only be used in a specific target as defined in the SMASH profile or in 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 executing 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, 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

**Table 1 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													

Table 2 Standard Command Options

## B.10 Target Addressing

To simplify the process of SMASH command execution, a file system called Target Addressing was created as shown in the diagram below.

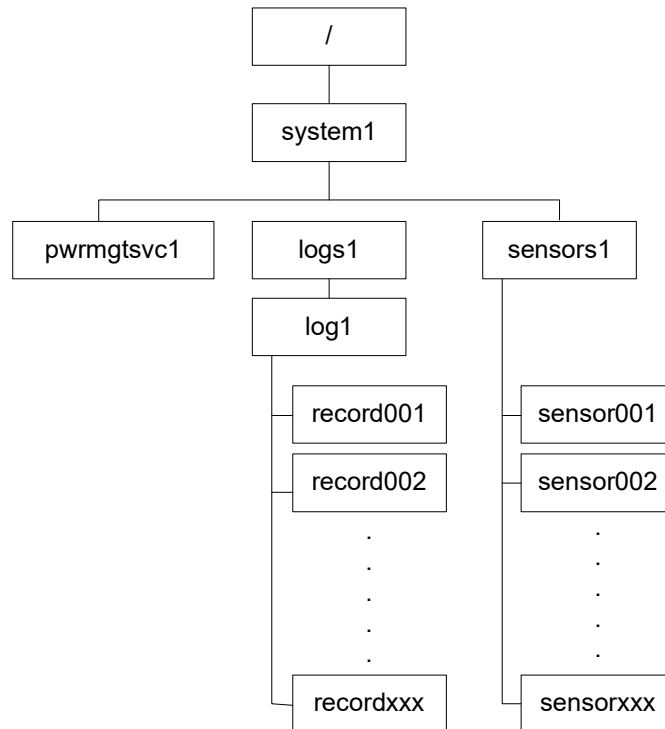


Figure 4 Target Addressing Diagram

### Terms Used in the Target Addressing Diagram

This section provides the 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 BMC (Baseboard Management Controller) chip and/or close to the MB 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, please 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, please 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.



### Important Notice for BMC "ADMIN" Login Credentials

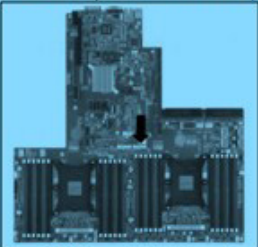
Supermicro has implemented new security feature enhancements on this product that will change the current default BMC login credentials to a **unique password** for the ADMIN user.

BMC barcode labels (see figure 1) containing the unique password for the ADMIN user may be found on this product:





*Figure 1: BMC barcode label containing BMC MAC address and ADMIN user unique password*

1. On the system motherboard (label locations will vary depending on motherboard model)
 



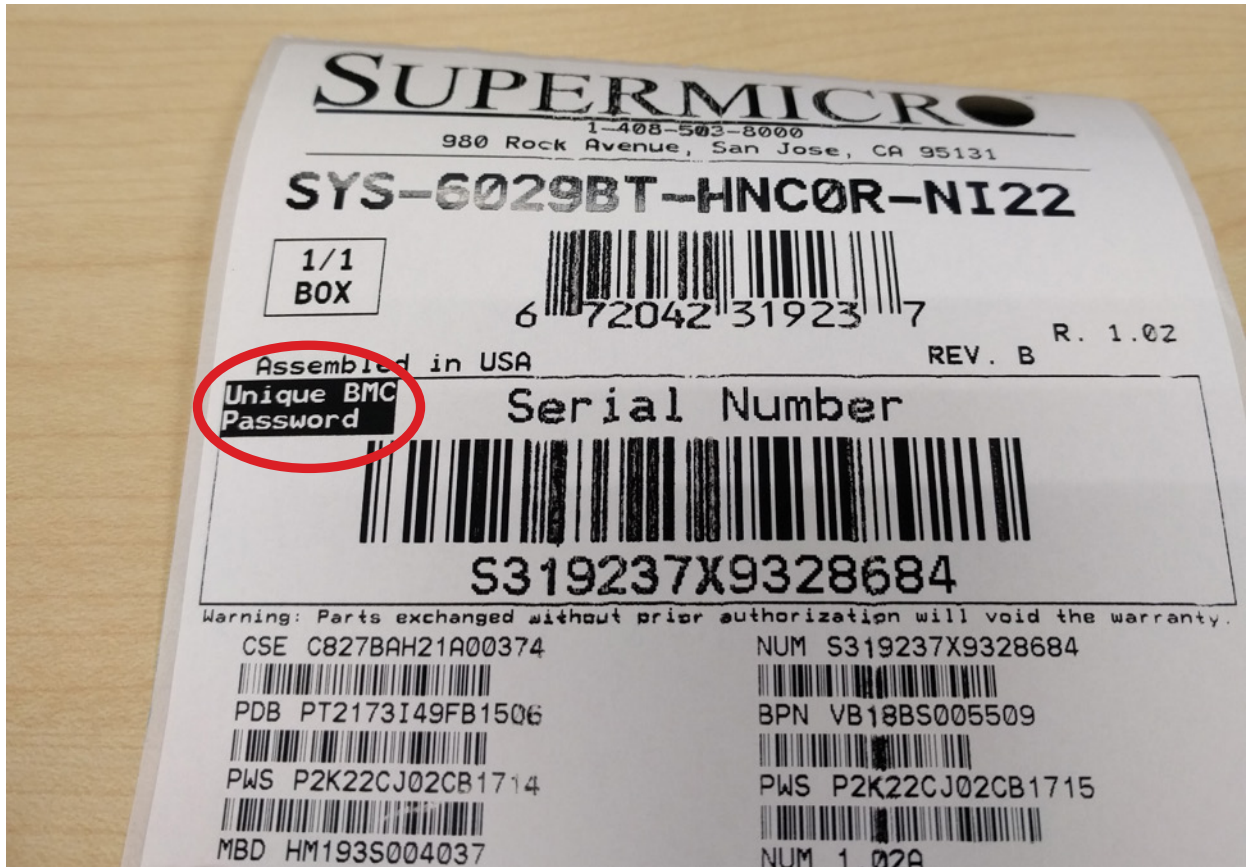
*Figure 2: BMC barcode labels located on the motherboard*
2. On the system service tag or chassis (label locations will vary depending on system model)
 

*Figure 3: BMC barcode label located on the chassis service tag and chassis*

For assistance or more information, contact Supermicro Technical Support online at [www.supermicro.com/support](http://www.supermicro.com/support)

### BMC Unique Password Notice for servers



Shipping Label Identifier

### C.3 Label Specifications

The unique password will consist of at least 10 alphabetic uppercase characters. To avoid confusion, provided passwords will not include any lowercase alphabetic characters or numbers.

One password label will be located near the BMC (Baseboard Management Controller) 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.

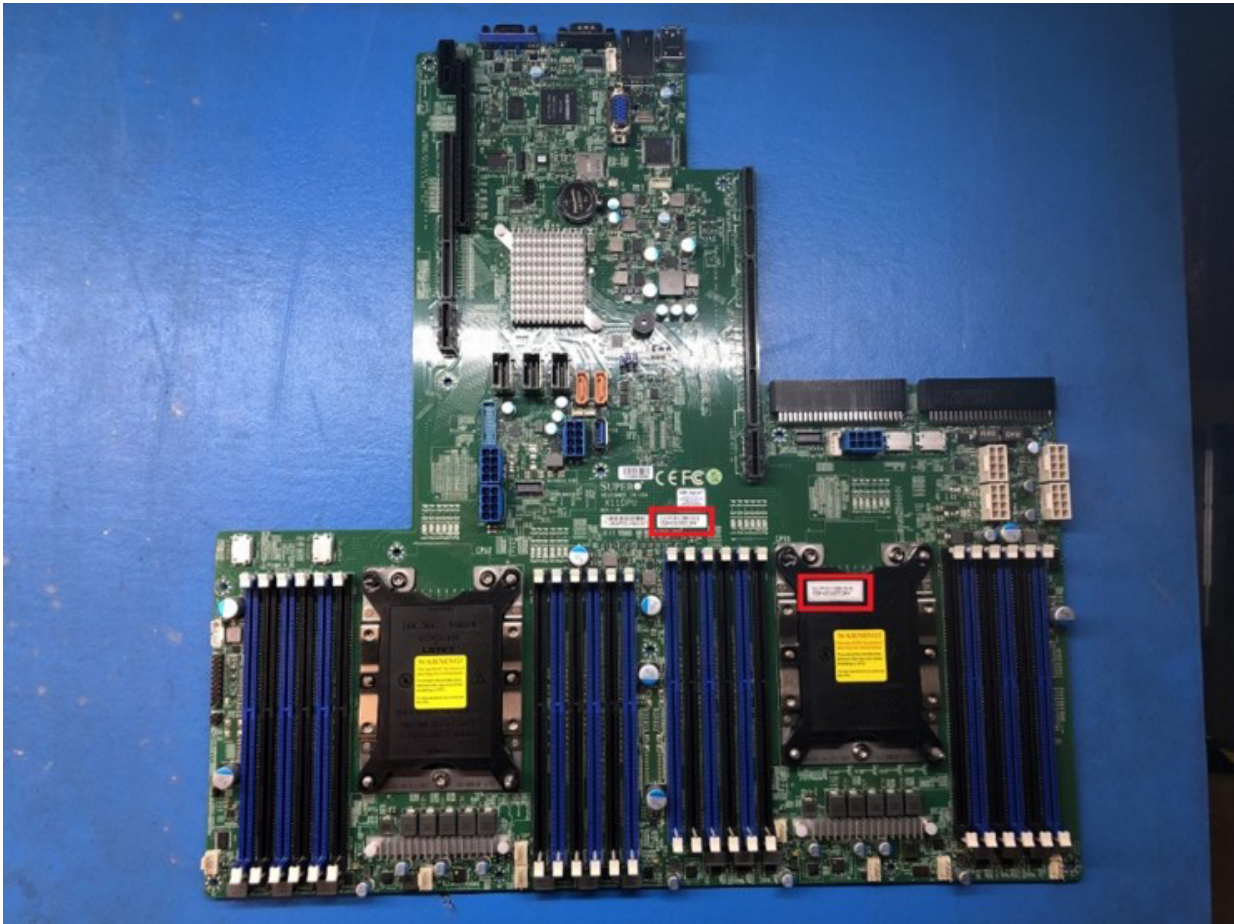
Most systems have a pull-out tag to display the BMC MAC address and the preprogrammed unique password. The rest of the systems will have the sticker on top/front of the chassis.



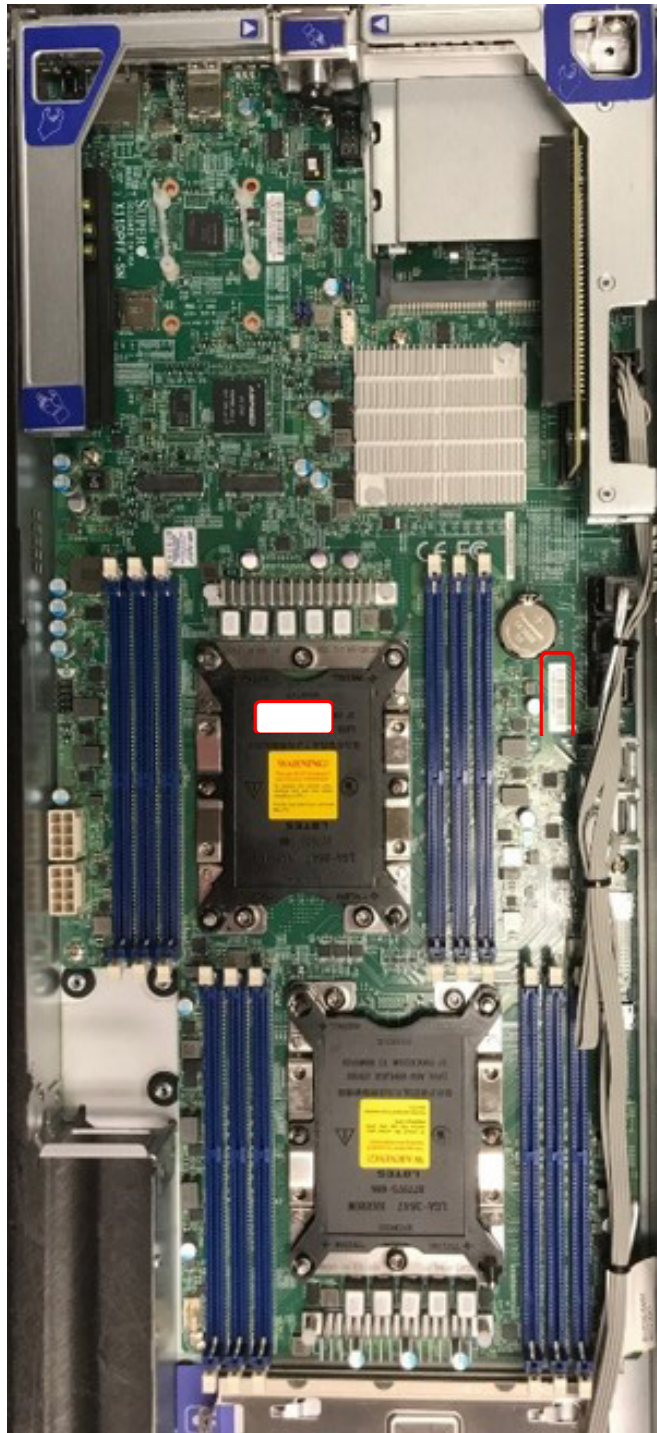
**Default password label**



**Label location on BMC chip**



**Label locations on motherboard PCB and the cover of CPU1**



Label locations on motherboard PCB and the cover of CPU1





**Label on the opposite side of the service tag**



**Label on the opposite side of the service tag**



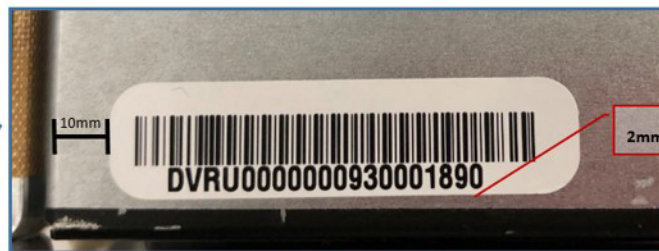
Label on the opposite side of the service tag



Label on the opposite side of the service tag



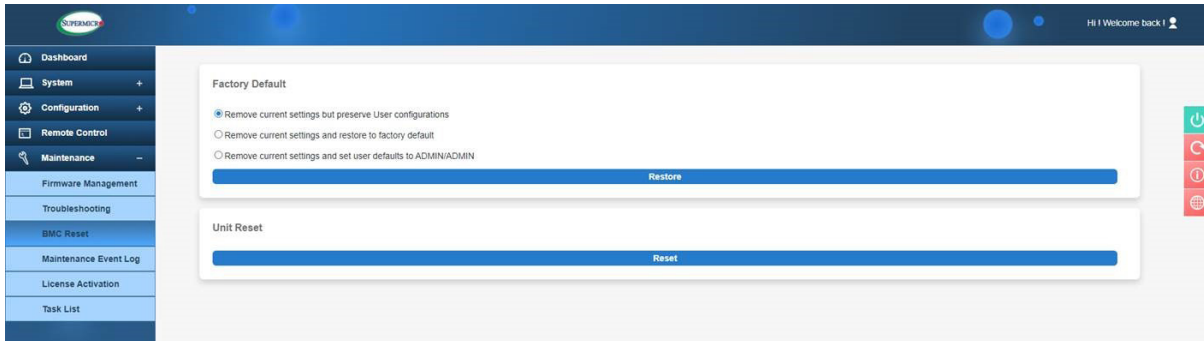
Label on the opposite side of the service tag



Label location on chassis

## C.4 Restore Factory Default

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 an incident, please 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 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, please 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 where 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:** Please 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.

(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.