



BMC

Baseboard Management Controller
Designed for the X13, H13, and B13 Series

USER'S MANUAL

Revision 1.0b

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

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

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

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

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

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



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

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

Manual Revision 1.0b

Release Date: December 13, 2024

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

Copyright © 2025 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 the functionalities of BMC.

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

Chapter 3 provides the answers to frequently asked questions.

An Important Note to the User

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

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

Conventions Used in the Manual

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



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



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



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



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

Important Links

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

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

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

Contacting Supermicro

Headquarters

Address: Super Micro Computer, Inc.
980 Rock Ave.
San Jose, CA 95131 U.S.A.

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: marketing@supermicro.com (General Information)
Sales-USA@supermicro.com (Sales Inquiries)
Government_Sales-USA@supermicro.com (Gov. Sales Inquiries)
support@supermicro.com (Technical Support)
RMA@supermicro.com (RMA Support)
Webmaster@supermicro.com (Webmaster)

Website: www.supermicro.com

Europe

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

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

Email: Sales_Europe@supermicro.com (Sales Inquiries)
Support_Europe@supermicro (Technical Support)
RMA_Europe@supermicro (RMA Support)

Website: www.supermicro.nl

Asia-Pacific

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

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

Email: Sales-Asia@supermicro.com.tw (Sales Inquiries)
Support@supermicro.com.tw (Technical Support)
RMA@supermicro.com.tw (RMA Support)

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Introduction to the BMC Platform.....	8
1.2 Overview of the ASPEED AST2600 BMC.....	8
1.3 Supermicro BMC Features.....	9
1.4 Software Licenses Available.....	12
1.5 Special Notes for Motherboard and Firmware Support	16

Chapter 2 Configuring the BMC Settings

2.1 Configuring UEFI BIOS	17
2.2 Connecting to the Remote Server.....	28
2.3 Accessing the Remote Server Using the Browser.....	29
2.4 BMC Dashboard.....	30
2.5 System.....	35
2.6 Configuration	69
2.7 Remote Control	120
2.8 Maintenance	154

Chapter 3 Frequently Asked Questions

Chapter 4 UEFI BIOS

4.1 Introduction.....	198
4.2 Main Setup	199
4.3 Advanced Setup Configurations.....	201
4.4 Event Logs	231
4.5 IPMI	233
4.6 Security.....	236
4.7 Boot	242
4.8 Save & Exit.....	245

Appendix A Firmware Update via WEB GUI and SUM

A.1 Overview.....	247
A.2 Updating Firmware Using BMC WEB GUI.....	248
A.3 Updating Firmware Using SUM.....	256

Appendix B Introduction to SMASH

B.1 Overview.....	260
-------------------	-----

B.2 An Important Note to the User	261
B.3 Using SMASH	261
B.4 Initiating the SMASH Protocol.....	262
B.5 SMASH-CLP Main Screen	263
B.6 Using SMASH for System Management.....	264
B.7 Definitions of Commands Verbs.....	265
B.8 SMASH Commands	267
B.9 Standard Command Options.....	268
B.10 Target Addressing	269
<i>Appendix C Unique Password for BMC</i>	
C.1 Overview.....	270
C.2 Notice and Shipping Label Identifier	271
C.3 Label Specifications	273
C.4 Restore Factory Default	279
C.5 Change All Unique Passwords Using Script.....	279
C.6 Frequently Asked Questions	280
<i>Appendix D Remote Attestation</i>	
D.1 Overview.....	282
D.2 License Requirements.....	282
D.3 Attest Your System Using the Supermicro Website.....	282
D.4 Attest Your System Using RESTful APIs	285

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 PCIeexpress connections to communicate with the graphics core for the X13 and H13 series motherboards. Designed for the X13 series, the AST2600 connects with the host system via PCIeexpress 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 provide LPC interface support to control Super IO functions. ASPEED AST2600 include 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.

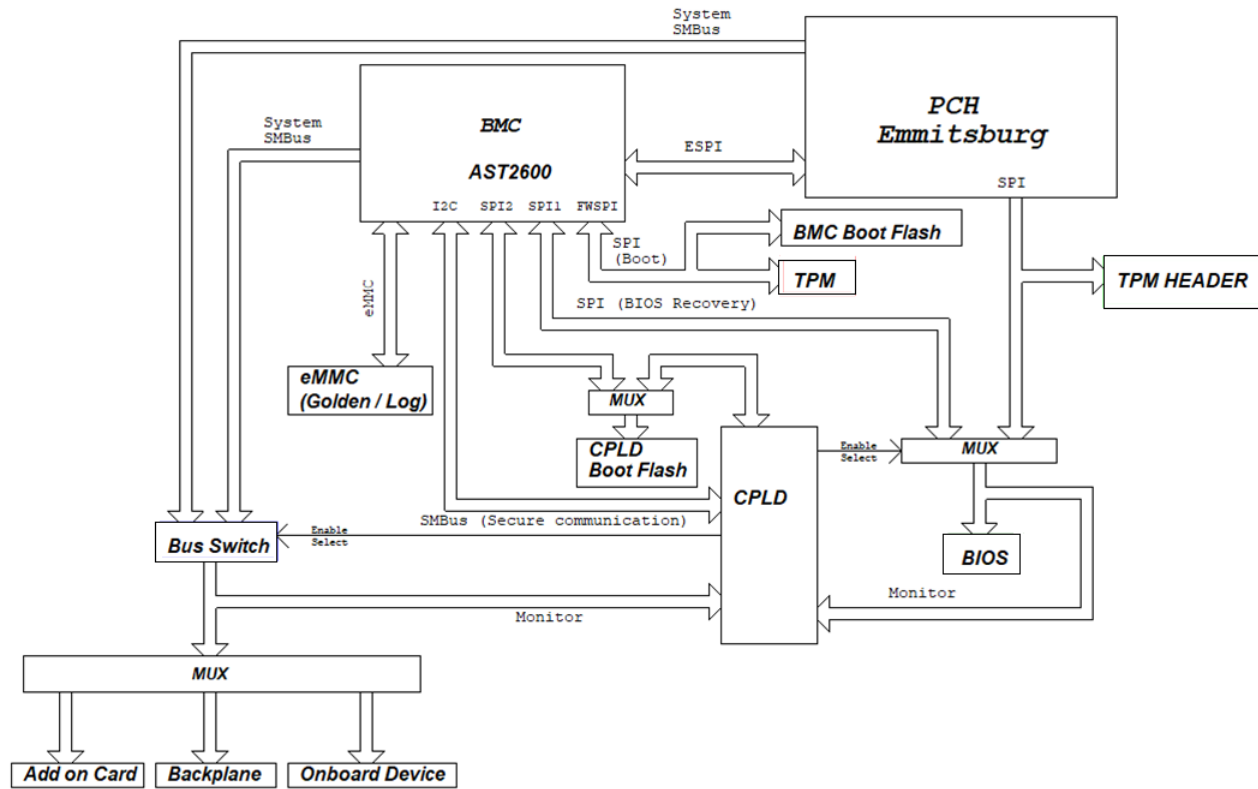
1.3 Supermicro BMC Features

- 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 and RMCP+ protocols supported
- SMASH/CLP
- Secure command line interface (SSH) and Telnet
- RADIUS authentication support
- Secure browser interface (Secure socket layer – SSL support)
- TLS (Transport Layer Security) v1.2 and v1.3 support
- Lightweight Directory Access Protocol (LDAP) supported
- System Lockdown
- Backup and restore the configuration file
- Factory defaults from web support
- Video quality settings
- Session video recording and playback

- Server data/information
- Preview of the remote screen on the main page
- Update Firmware through 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

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



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

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

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

- SFT-DCMS-Single: System Management Suite

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

Refer to the following comparison chart for more info.

(*) 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 and alerts	✓	✓	✓
Real-time power graphing	✓	✓	✓
Historical power values	✓	✓	✓
Power Capping (Through SPM)			✓
Out-of-Band System Checks	✓	✓	✓
Predictive failure monitoring (for Broadcom controller only)	✓	✓	✓
SNMPv1, v2, and v3 (traps and gets, SNMPv3 MIBs needs DCMS license)	✓	✓	✓
Email Alerting	✓	✓	✓
Fan monitoring	✓	✓	✓
Power Supply monitoring	✓	✓	✓
Memory monitoring	✓	✓	✓
CPU monitoring	✓	✓	✓
RAID monitoring and configuration (Broadcom/Marvell storage controller)			✓
GPU monitoring (NVIDIA GPUs)	✓	✓	✓
NIC monitoring	✓	✓	✓
HDD monitoring (Broadcom/Marvell/NVME controller)			✓
Remote agent-free out of band FW updates (BIOS, BMC, CPLD, Backplane)	✓	✓	✓
Component FW Update			✓
Inband FW Updates	✓	✓	✓
Local configuration 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, Chas- sis 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	✓	✓	✓

1.5 Special Notes for Motherboard and Firmware Support

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

Refer to the motherboard product page at 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 website at https://www.supermicro.com/support/resources/bios_ipmi.php?type=BMC. This section provides detailed information on how to configure BMC settings.



Note: Some features might not be available if you are using an X13 motherboard as a few newer features are not supported by this generation.

2.1 Configuring UEFI BIOS

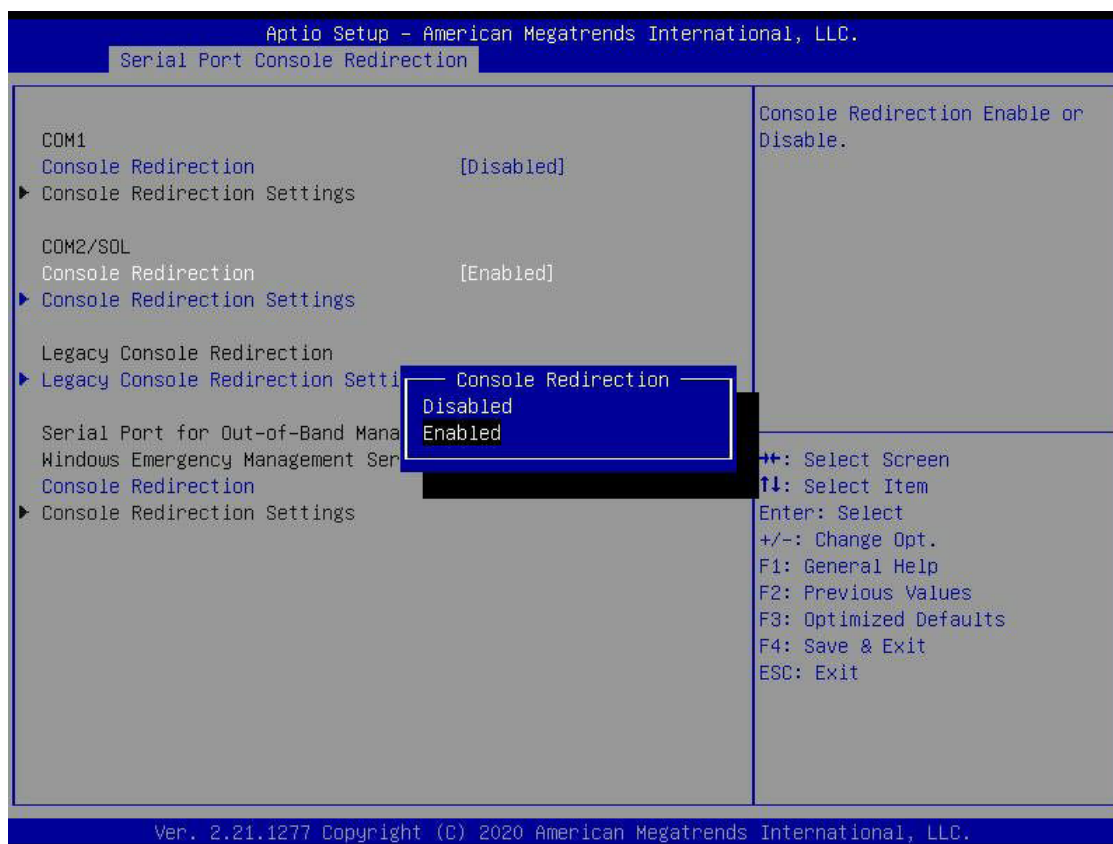
Before configuring the BMC, follow the instructions below to configure the system UEFI BIOS settings.

Entering and Using the UEFI BIOS

1. During the system bootup, press the 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>.

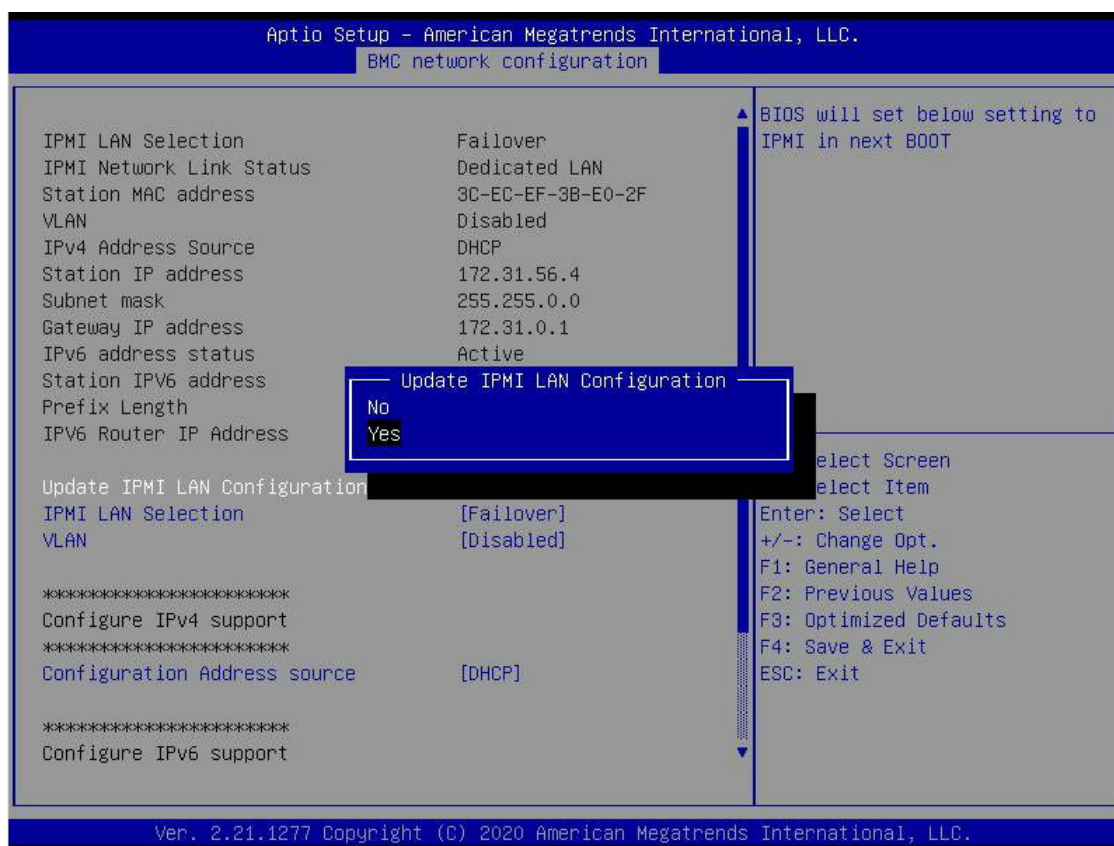
Enabling the COM port for SOL (BMC)

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].

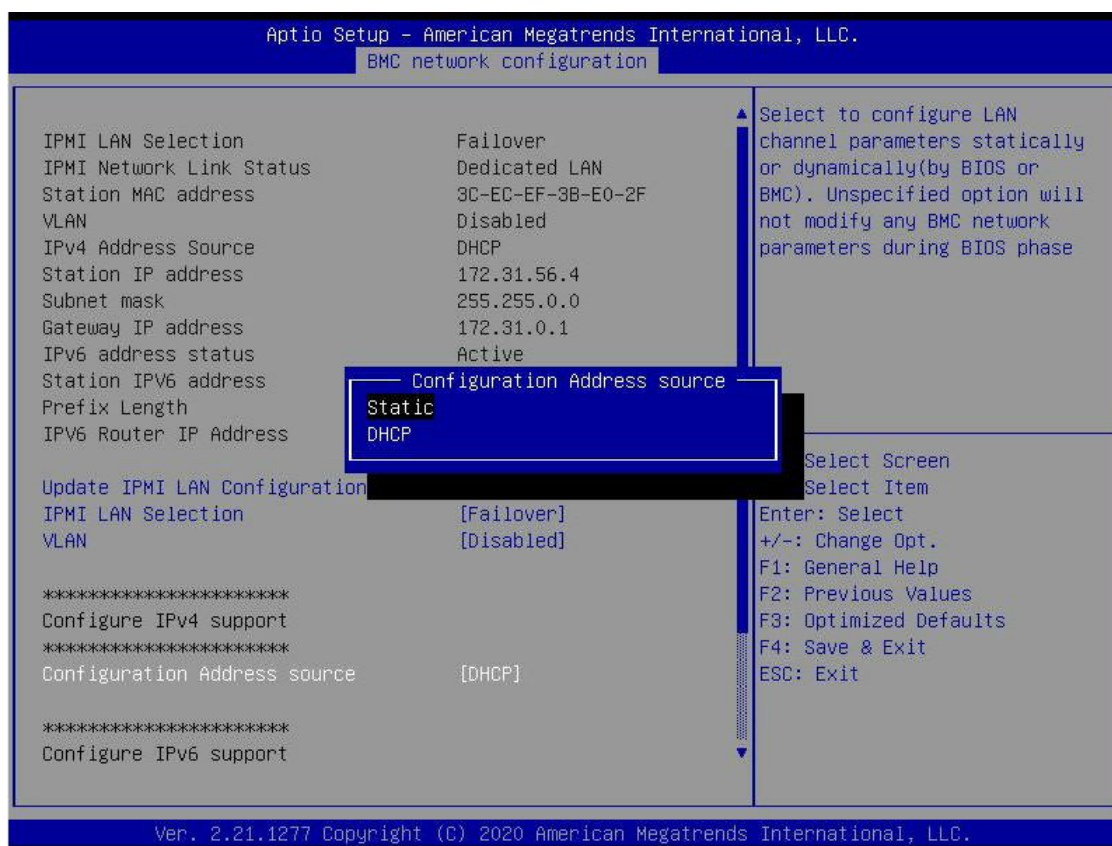


Configuring IP Address Using the UEFI BIOS

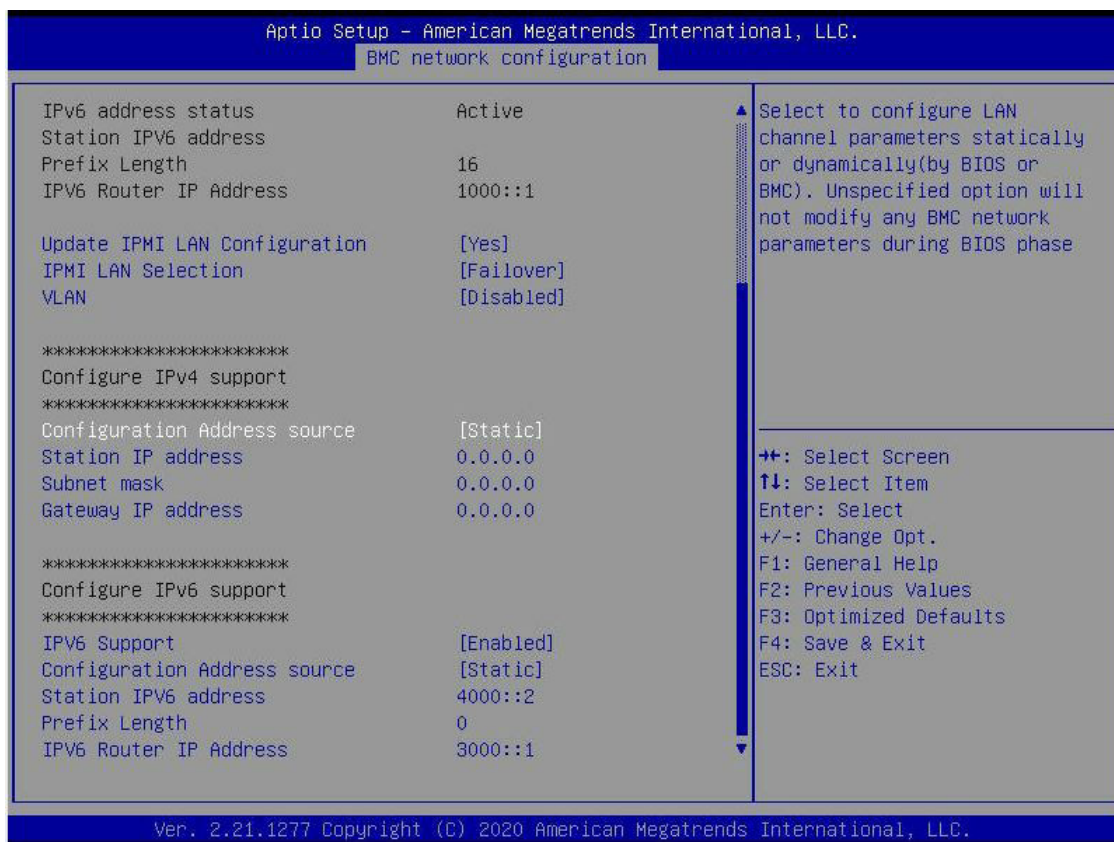
1. Select the *Server Management* tab.
2. Select *BMC Network Configuration* and press <Enter>.
3. Highlight *Update IPMI LAN Configuration*, press <Enter> and select [Yes].



4. 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.

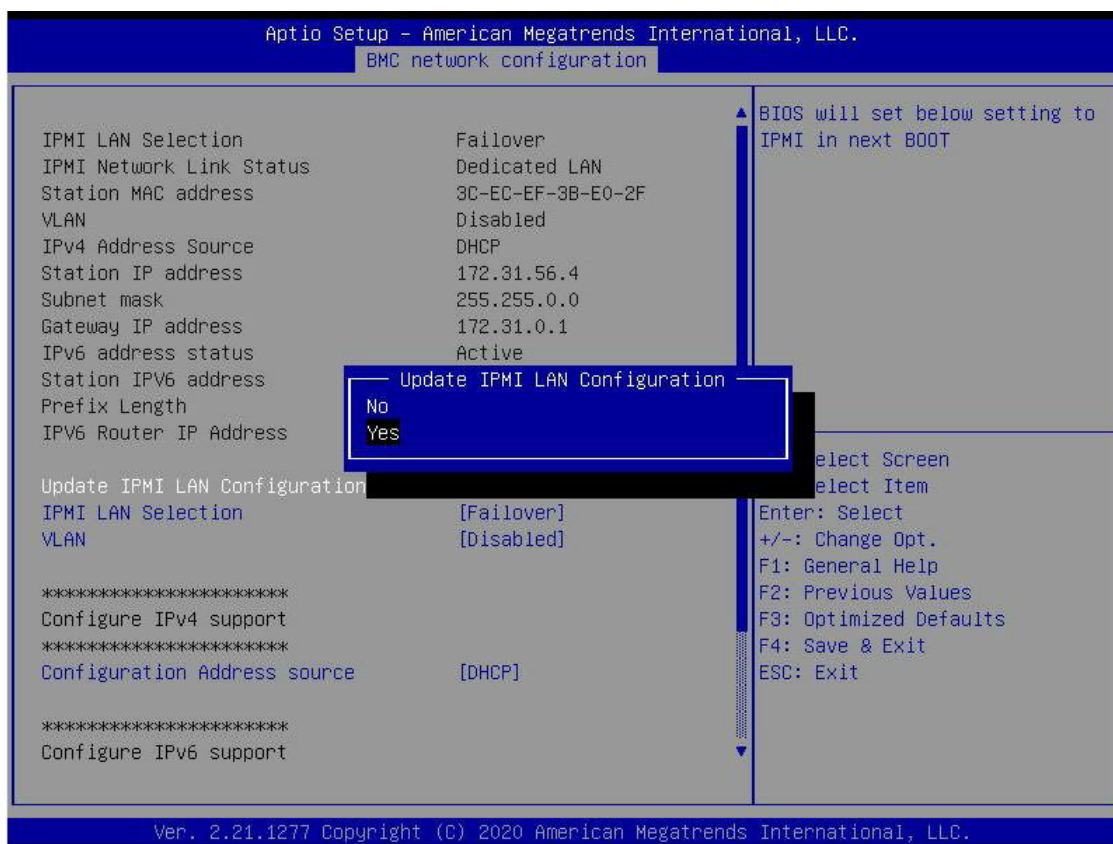


Connecting to BMC Using the UEFI BIOS

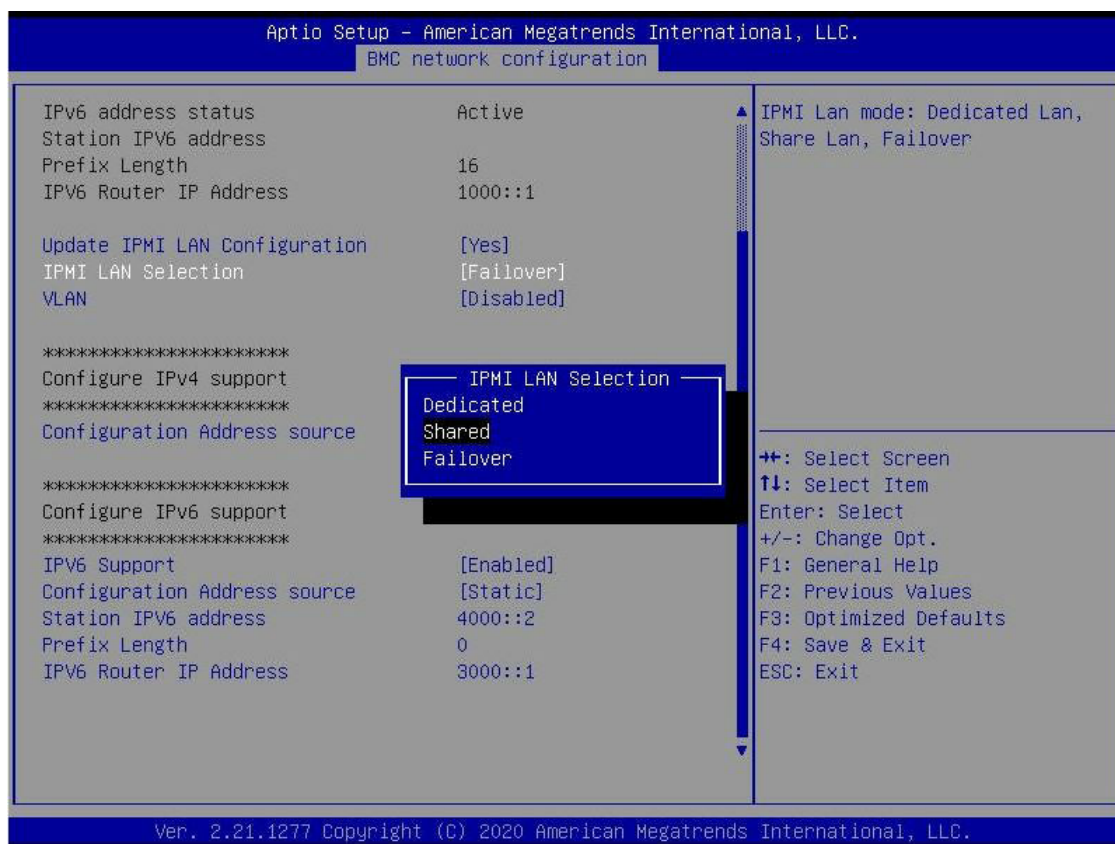
1. To bring up the BIOS menu, connect one end of an Ethernet Cat 5 to the Ethernet port of the laptop or device being used.
2. Plug the other end of the cable into the IPMI / SHARED port of the server.
3. Power on the server by pressing the DEL key to enter the BIOS menu.
4. In the BIOS menu, follow 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].



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

Aptio Setup - American Megatrends International, LLC.

BMC network configuration

IPv6 address status	Active	▲ Select to configure LAN channel parameters statically or dynamically (by BIOS or BMC). Unspecified option will not modify any BMC network parameters during BIOS phase
Station IPv6 address		
Prefix Length	16	
IPv6 Router IP Address	1000::1	
Update IPMI LAN Configuration	[Yes]	
IPMI LAN Selection	[Failover]	
VLAN	[Disabled]	

Configure IPv4 support		

Configuration Address source	[Static]	→+: Select Screen ↑↓: Select Item Enter: Select +/-: Change Opt. F1: General Help F2: Previous Values F3: Optimized Defaults F4: Save & Exit ESC: Exit
Station IP address	0.0.0.0	
Subnet mask	0.0.0.0	
Gateway IP address	0.0.0.0	

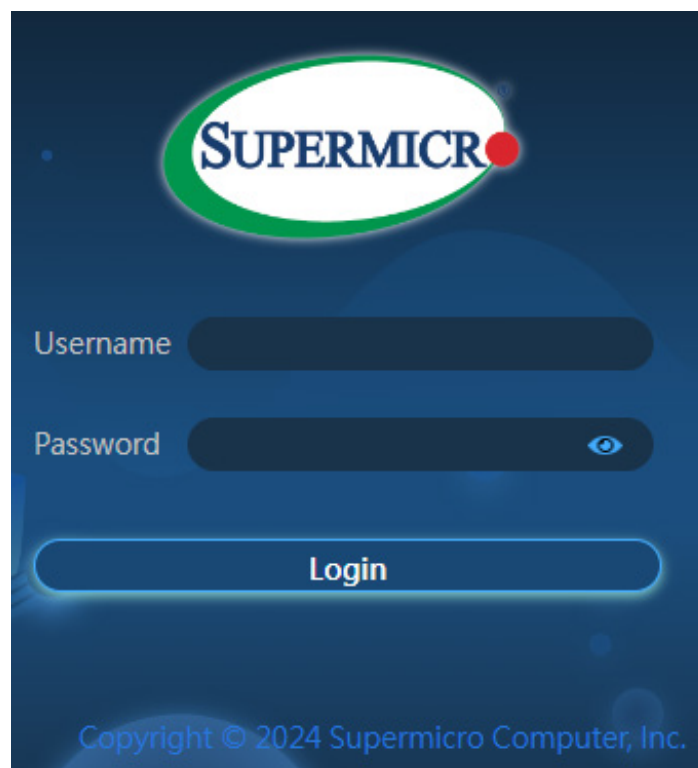
Configure IPv6 support		

IPv6 Support	[Enabled]	
Configuration Address source	[Static]	
Station IPv6 address	4000::2	
Prefix Length	0	
IPv6 Router IP Address	3000::1	

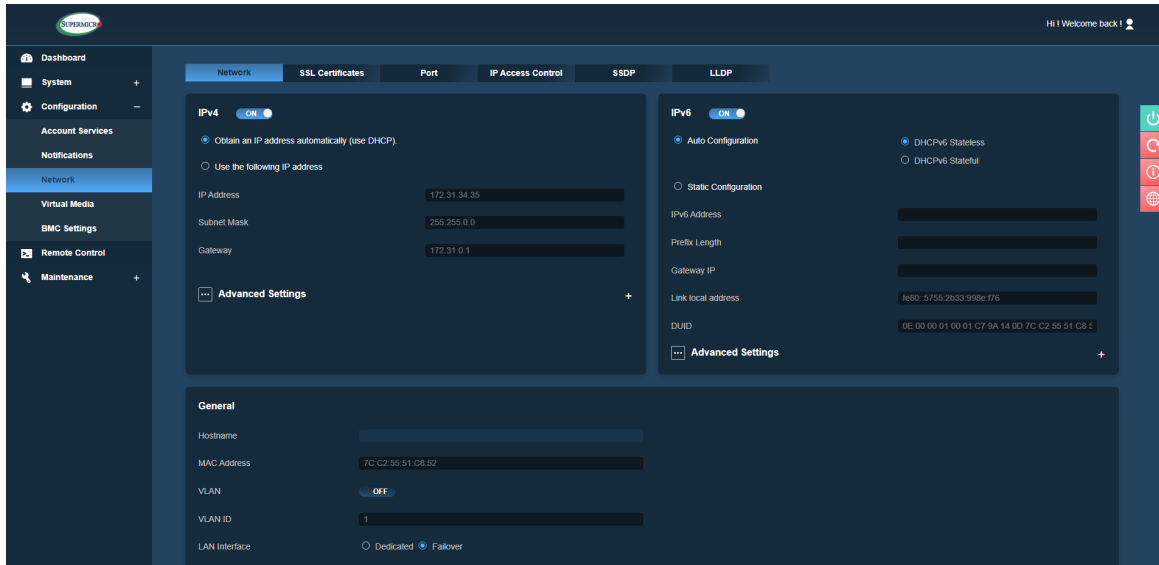
Ver. 2.21.1277 Copyright (C) 2020 American Megatrends International, LLC.

Now that both Laptop and the BMC are on the same subnet. With the static IP connected, you should be able to communicate. To establish the connection, 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 in the image below.
3. Enter the username, ADMIN, and a BMC unique password. Refer to Appendix D on how to retrieve the BMC unique password.



- 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

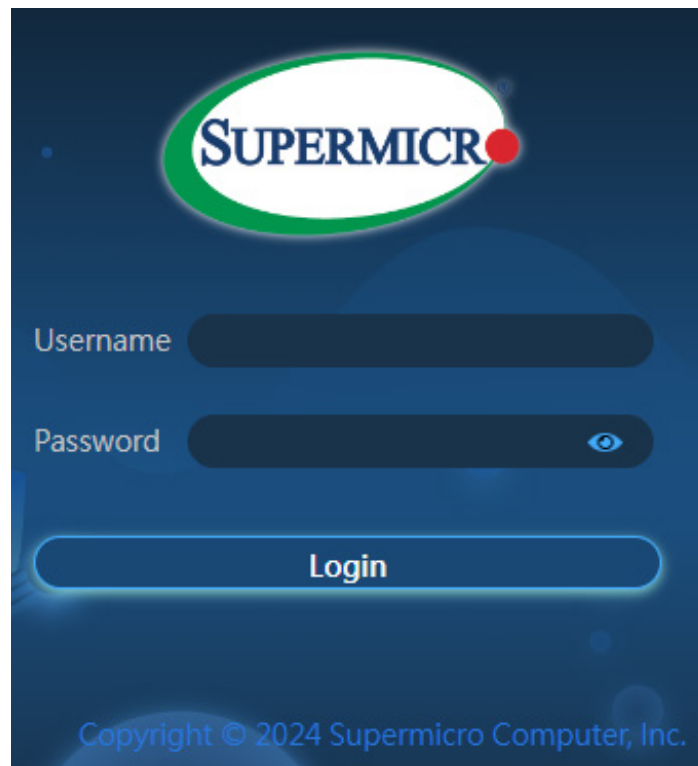
To Log In to the Remote Console

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. To view the hidden password, click 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: Keep 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.

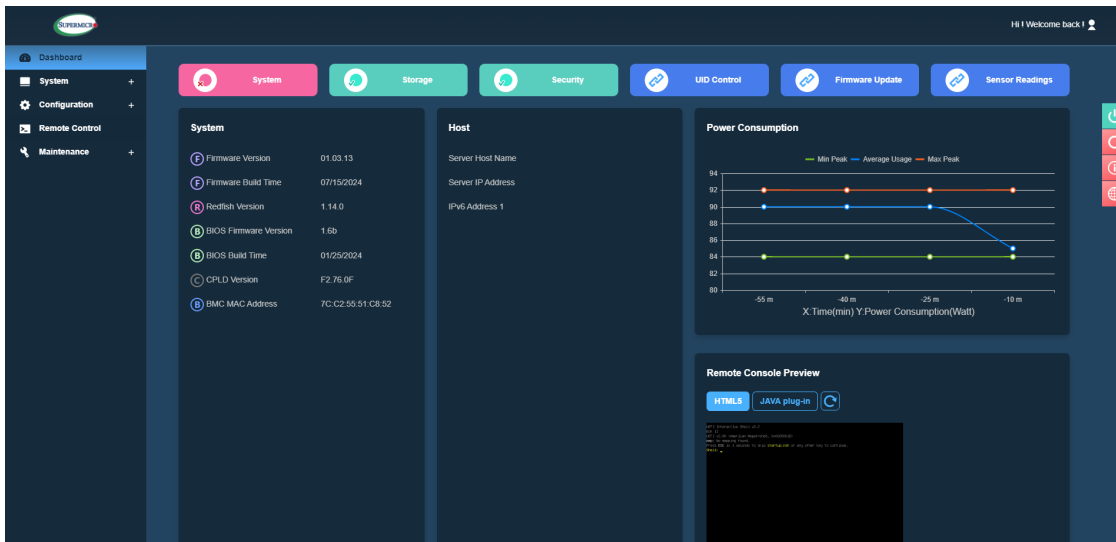


Note 1: To use the IPMIView utility for Console Redirection, refer to the IPMIView User's Guide for instructions.


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. You can also access quick links to System, Storage (if a storage component is connected), UID Control, Firmware Update and Sensor Readings, Power Consumption, Remote Console Preview, and Recent Logs. If storage components are connected, then you will also be able to access Storage from here.



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

User	ADMIN
Role	Administrator
Server	172.31.34.35
	

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



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

Storage Health

In this section, users can find overall storage component health and notification if a storage component is connected and detected, as well as HOST is powered on. Click on the health status to get more details about the hard drive or controller health. Symbols indicating the 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 one or more components health 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 a 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. Unless there is at least an AOC NIC in the system, BMC Dashboard will provide a Link to Network AOC and message to users that all Add-On-Cards' information can be viewed on the Network AOC page. The tooltip message will be *"Go to the Network AOC page."*



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 configured in the Network Configuration.

Power Consumption

This section displays a graphical representation of the system power consumption with time stamps. Click on the graph to go to Power page for more details about power consumption. The power consumption will be updated at least at a 5-minute interval.

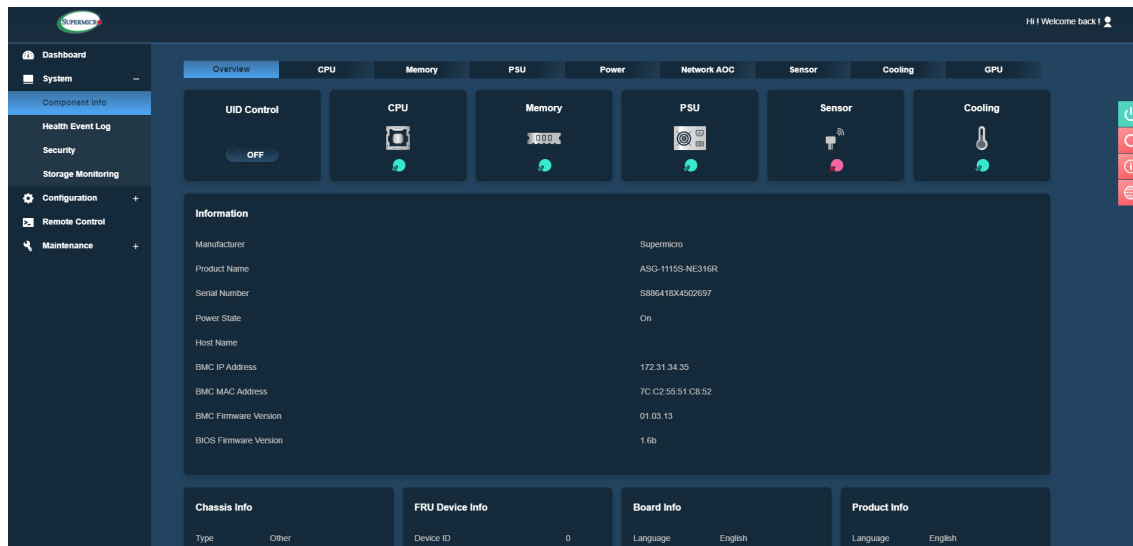
Remote Console Preview

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



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).



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 of components listed under Help Page are available for all types of servers. The Help Page is the General Guide for most system servers. See individual server manuals for any 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 for 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 for the sensors present in the system.
- Fan – This displays 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 the detailed system information.
 - Manufacturer – Manufacturer name
 - Product Part Number – Product part number of the product
 - Serial Number – Serial number of the product. For multi-node system, SN is from the Multi-node controller.
 - 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 System Device ID.
 - Chassis Info: The kind of chassis info displayed will depend you the type of node system installed.

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

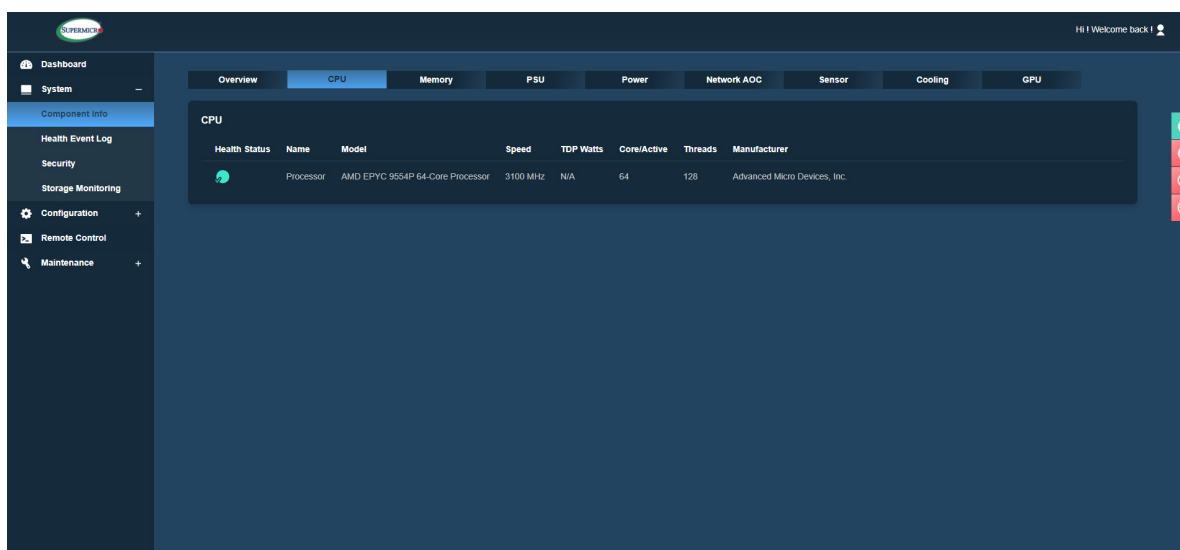
- Type – Chassis type detail
- Part Number – Chassis part number
- Serial Number – Chassis serial number.

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 the information about processor models.
- **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 number of cores of the processor as well as whether the processor is active or inactive.
- **Threads:** You can view the total number threads.
- **Manufacturer:** You can view the processor manufacturer info.

Memory

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

Overview	CPU	Memory	PSU	Power	Network ADC	Sensor	Fan	GPU
Memory								
Health Status	Name	Device Type	Error Correction	Operating Speed	Size	Serial Number	Part Number	Manufacturer
	P1-DIMMA1	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE04232245842963	M321R8GA38B6-CQKET	Samsung
	P1-DIMMA2	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE042322458429AA	M321R8GA38B6-CQKET	Samsung
	P1-DIMMB1	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE04232245842936	M321R8GA38B6-CQKET	Samsung
	P1-DIMMB2	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE04232245842805	M321R8GA38B6-CQKET	Samsung
	P1-DIMMC1	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE04232245842715	M321R8GA38B6-CQKET	Samsung
	P1-DIMMC2	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE04232245842772	M321R8GA38B6-CQKET	Samsung
	P1-DIMMD1	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE042322458427AA	M321R8GA38B6-CQKET	Samsung
	P1-DIMMD2	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE042322458428C9	M321R8GA38B6-CQKET	Samsung
	P1-DIMME1	DDR5	SingleBRECC	4400 MT/s	32768 MB	80CE04232245842906	M321R8GA38B6-CQKET	Samsung

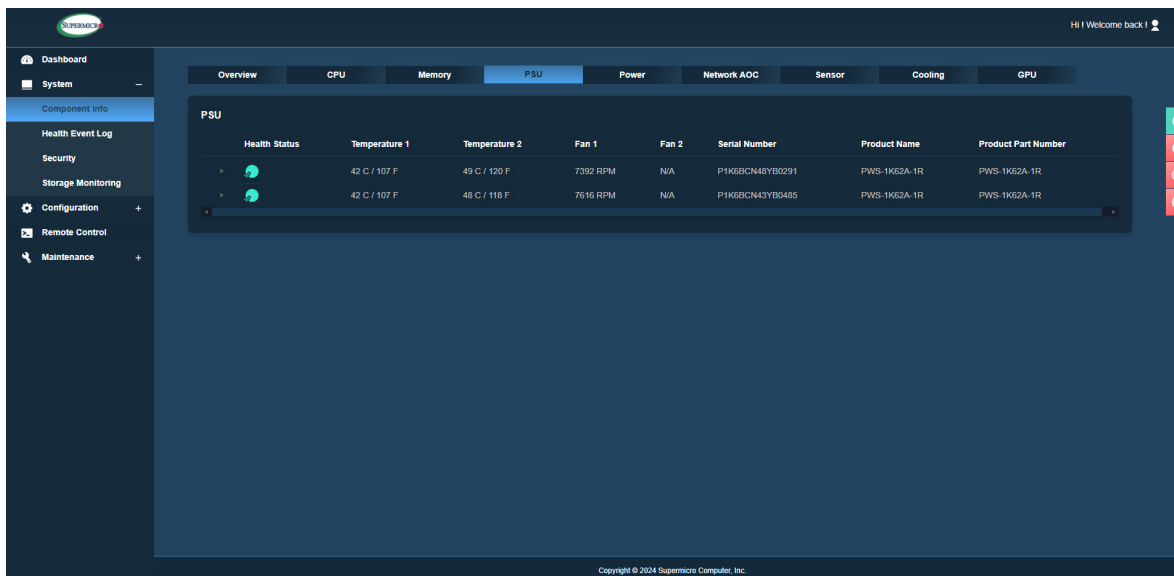
This page displays the following information.

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



Health Status	Temperature 1	Temperature 2	Fan 1	Fan 2	Serial Number	Product Name	Product Part Number
Normal	42 C / 107 F	49 C / 120 F	7392 RPM	N/A	P1K6BCN48YB0291	PWS-1K62A-1R	PWS-1K62A-1R
Normal	42 C / 107 F	48 C / 118 F	7616 RPM	N/A	P1K6BCN43YB0485	PWS-1K62A-1R	PWS-1K62A-1R

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 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)

Refer to the following samples provided below.

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

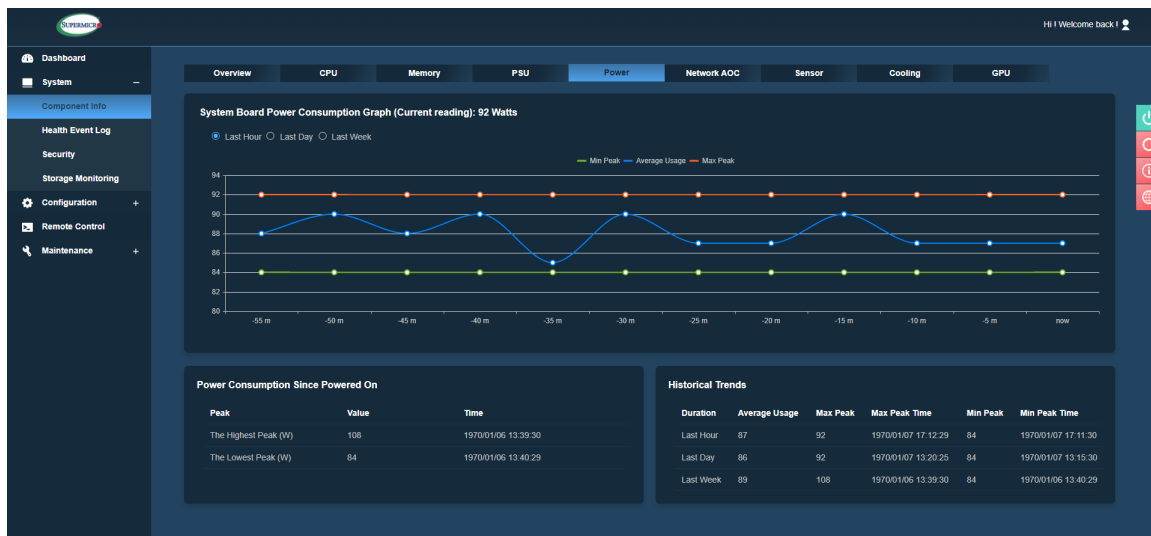
PSU								
	Health Status	Temperature 1	Temperature 2	Fan 1	Fan 2	Serial Number	Product Name	Product Part Number
>		27 C / 80 F	39 C / 102 F	11296 RPM	12256 RPM	P3K6GCN29DB8366	PWS-3K06G-2R	PWS-3K06G-2R
>		27 C / 80 F	38 C / 100 F	11296 RPM	12288 RPM	P3K6GCN29DB8364	PWS-3K06G-2R	PWS-3K06G-2R
>		27 C / 80 F	39 C / 102 F	11296 RPM	12288 RPM	P3K6GCN29DB8370	PWS-3K06G-2R	PWS-3K06G-2R

If the power cable is disconnected from the PSU, the expected display will appears as follows.

PSU								
	Health Status	Temperature 1	Temperature 2	Fan 1	Fan 2	Serial Number	Product Name	Product Part Number
>		N/A	N/A	N/A	N/A	N/A	N/A	N/A
>		38 C / 100.4 F	54 C / 129.2 F	2660 RPM	N/A	P2K08CL44UB0208	PWS-2K08A-1R	PWS-2K08A-1R
>		33 C / 91.4 F	50 C / 122 F	1400 RPM	N/A	P2K08CM47VB1366	PWS-2K08A-1R	PWS-2K08A-1R
>		37 C / 98.6 F	53 C / 127.4 F	1120 RPM	N/A	P2K08CM47VB1363	PWS-2K08A-1R	PWS-2K08A-1R

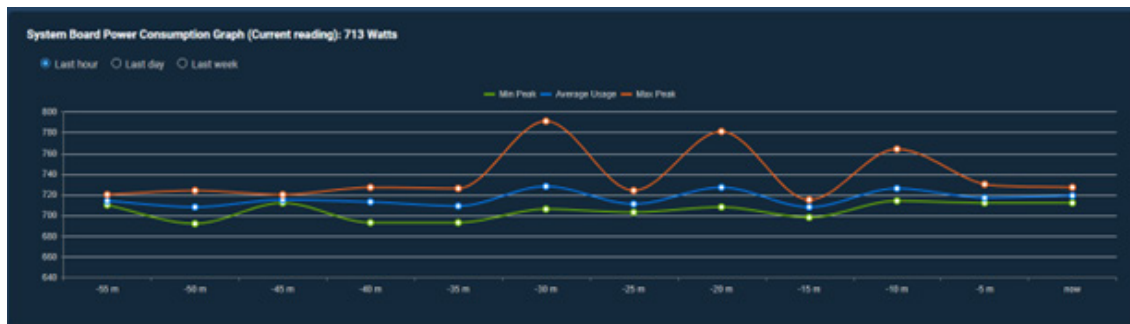
Power

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 Watt) with time. Readings can be checked for the last hour/days/week.



- 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


Power Consumption Since Powered On		
Peak	Value	Time
The Highest Peak (W)	966	2024/06/05 03:01:20
The Lowest Peak (W)	54	2024/06/05 02:58:23

- 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

Historical Trends					
Duration	Average Usage	Max Peak	Max Peak Time	Min Peak	Min Peak Time
Last hour	718	781	2024/06/05 14:44:25	698	2024/06/05 14:49:20
Last day	717	966	2024/06/05 03:01:20	54	2024/06/05 02:58:23
Last week	717	966	2024/06/05 03:01:20	54	2024/06/05 02:58:23

Network AOC

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

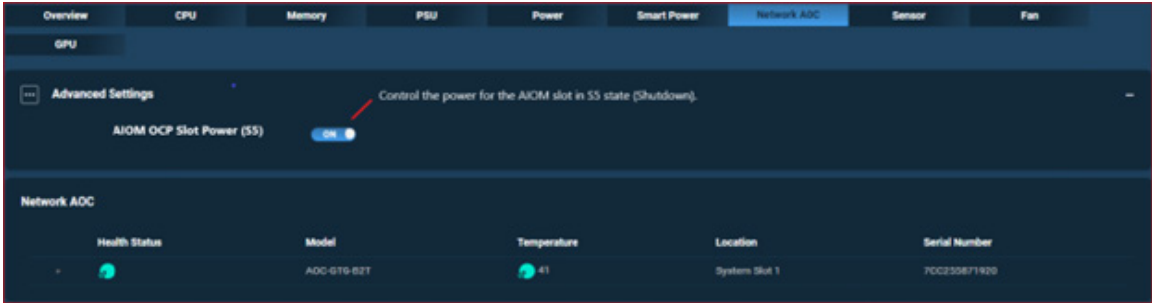
 **Note:** This page will only display AOC NIC card Information. Temperature will display as **Unsupported** for AOC NIC cards that do not support the temperature feature.



This page displays the following information.

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

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



The following is the naming rule for Physical LAN which is used by BMC to pass onto SSM. X and Y are numerical index (0...9).

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

Sensor



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



The screenshot shows the 'Sensor Readings' tab in a BMC interface. It features a dark blue header with 'Intrusion Reset' and 'Export to Excel' buttons, and a search bar on the right. The table below lists various sensors with their status, names, readings, and types.

Severity	Name	Reading	Type
	CPU1 Temp	50	Temperature
	CPU2 Temp	48	Temperature
	CPU3 Temp	54	Temperature
	CPU4 Temp	53	Temperature
	Inlet Temp	32	Temperature
	PCH Temp	53	Temperature
	System Temp	42	Temperature
	Peripheral Temp	43	Temperature
	CPU1_VRMIN Temp	59	Temperature
	CPU1_VRMON Temp	43	Temperature

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

- **Health:** Sensor status indicates the health state of the sensors.
 -  This symbol means that the sensor reading is normal.
 -  This symbol means that the sensor reading is not within the range and needs attention.
- **Name:** This column displays sensor names of currently available sensors from the system.
- **Reading:** This column displays the value of the current sensor's reading.
- **Type:** This column displays sensor type categories from the following list.
 - Temperature Sensors
 - Voltage Sensors
 - Physical Security
 - Battery (aka Power Supply)
- **Low NR:** This column displays a lower non-recoverable threshold value for each sensor.
- **Low CT:** This column displays a lower critical threshold value for each sensor.

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



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

Sensor Type Categories

By default, [All Sensors] categories are selected and sorted by the order received by BMC; users can sort Sensor Readings by:

- Severity
- Name
- Reading
- Type
- Low NR
- Low CT
- High CT
- High NR

Furthermore, you can filter the sensors by using the following categories:

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

Export to Excel

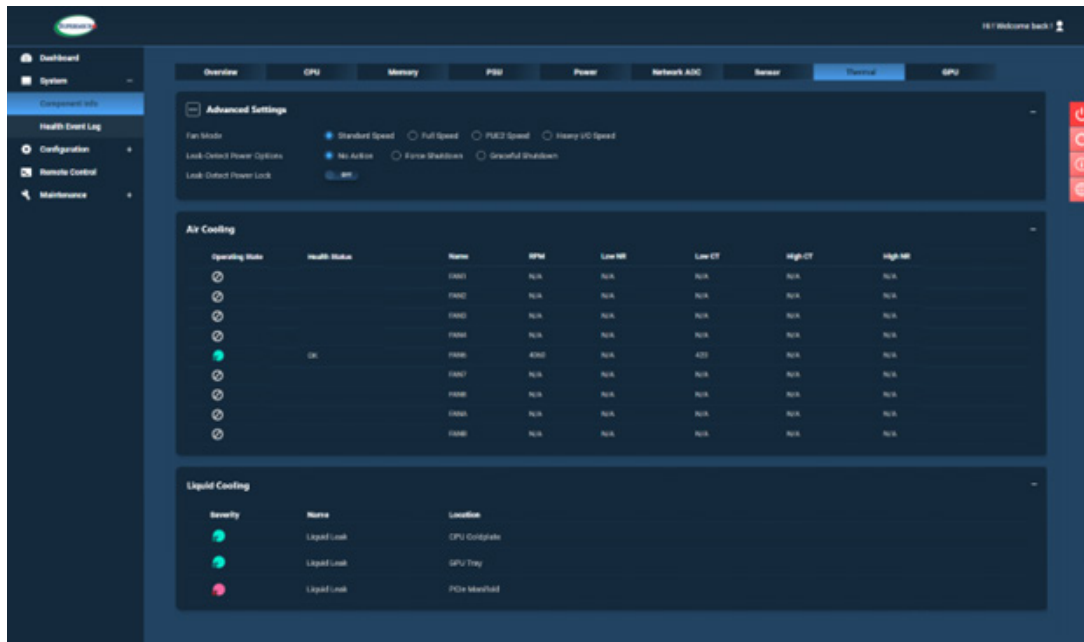
You can export sensor reading in Excel format.

Intrusion Reset

You can use this button to reset chassis intrusion.

Thermal (or Cooling)

In this tab, you can manage both air cooling and liquid cooling functionalities. For air cooling, this tab shows the FAN status and will allow you to configure the FAN speed for installed fans. For liquid cooling, this tab will show the liquid leak detection status and options for power control. All fan sensors will be detected once the system HOST is powered on. Currently, fan data is obtained from BMC Sensor Data Record (SDR) noted in the Supermicro Thermal System Thermal Design Guide (SSTDG).



This page displays the following air cooling information.

- **Operating Status:** This column indicates whether the fans are in operating state or not.
 - ⊗ This symbol means the fan is not installed or that it has lost the connection to the system.
 - 🟢 This symbol means that the fan is not in a good operating state.
 - 🔴 This symbol means that the fan is in a good, normal operating state.
- **Health Status:** This column indicates the fan health status.
- **Name:** This column indicates the system fan number.
- **RPM:** This column indicates the revolution per minute for each fan. The RPM should provide the actual, real value detected in the system. If there is a faulty FAN present, RPM should be shown zero (0) if the fan does not work. PSU FAN A or FAN B speeds will be the same as speed of PSU FAN 1.

- Low NR: This column displays a lower non-recoverable threshold value for the fan sensor.
- Low CT: This column displays a lower critical threshold value for the fan sensor.
- High CT: This column displays a higher critical threshold value for the fan sensor.
- High NR: This column displays a higher non-recoverable threshold value for the fan sensor.

Sample from ipmitool (# ipmitool sdr | grep Fan)

```
Front Fan RPM      | 5400 RPM          | ok
Rear Fan RPM       | 5400 RPM          | ok
PS 1-4 Fan RPM     | 5600 RPM          | ok
PS 5-8 Fan RPM     | 6000 RPM          | ok
```

Liquid Cooling

This feature provides details about possible sensors leakages.

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



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



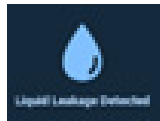
This symbol indicates there is no leakage and operating in good and normal condition.

- Name: This column provides the sensor name.
- Location: This column indicates the location of the leakage. It will provide one of three of the following locations.
 - CPU Coldplate
 - CPU Tray
 - PCIe Manifold

Advanced Settings

For Fan control, users can configure the following Fan Mode settings. Fan modes are dynamically received from Redfish API. Hence, Web UI will display all available speed settings for users to select. The following possible fan speeds are as follow:

- **Standard Speed:** This is the standard fan speed setting is for standard power saving and efficiency.
- **Full Speed:** This is the full speed setting is for maximum system performance.
- **Optimal or PUE2 Speed:** This is the optimal fan speed setting. It will adjust the fan speed by balancing the needs between system performance and power savings. This is the most efficient cooling setting under normal usage.



- **Heavy I/O Speed:** This is the heavy I/O fan speed setting, which will boost cooling to the add-on card zone.

For liquid leak detection control, users can configure different power mode settings. The available power options including the following:

- **No Action:** When a leak occurs, the following alert icon will notify you about the leakage. You must acknowledge that the area is dry and operational before turning off the alert.
- **Force Shutdown:** If a leak is detected, the system will immediately power down, lock the power options, and notify users with the same alert. Before turning the system back on, you must navigate to the Thermal page to unlock the power lock. To unlock the power lock, you must first confirm that the leak area is dry and operational. Once the power lock is unlocked, users can power on the system.
- **Graceful Shutdown:** Selecting this option will cause the system to power down gracefully and save all data before shutting down. You must confirm that the area is dry and operational before powering the system back on.

Additionally, the prompt for the disabled power button after liquid leakage detection will display: *"Power button is currently disabled due to detected liquid leakage. Please go to the Thermal page to unlock the Leak-Detect Power Lock."* The unlocking prompt addresses both the 'Leak-Detect Power Lock' option and the 'Liquid Leak Detected' icon: *"Liquid leakage detected. Please confirm that the area is dry and all conditions for safe operation have been met."*

GPU

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

DPU

Health Status	Manufacturer	Model	Location	Temperature	Firmware Version	Serial Number	Part Number
	MELLANX	ADC-S2506-M25	System Slot 2	44	26.35.2000	WA2289012879	ADC-S2506-M25
	BROADCOM	ADC-S1000-62c	System Slot 3	37	218.0.169.0	GA2189062104	ADC-S1000-62c

GPU

Health Status	Manufacturer	Model	Location	Temperature	Firmware Version	Serial Number	Part Number
	INTEL	ATS-M3	GPU6	36	6.6.0.0	LQAC14702871	Yet to get

FPGA

Health Status	Manufacturer	Product Name	Location	Temperature	Firmware Version	Serial Number	Part Number
	XILINX	AMPVLD U55C PQ	System Slot 4	36	Not Supported	XFL1K0WJ04	005030-02

NIC AOC

Health Status	Manufacturer	Model	Location	Temperature	Firmware Version	Serial Number	Part Number
	Yet to get	ADC-S1000G-QC	System Slot 5	N/A	4.20 (3d800177C3)	WA2025007857	Yet to get

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

AIP

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

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


PCIe AOC

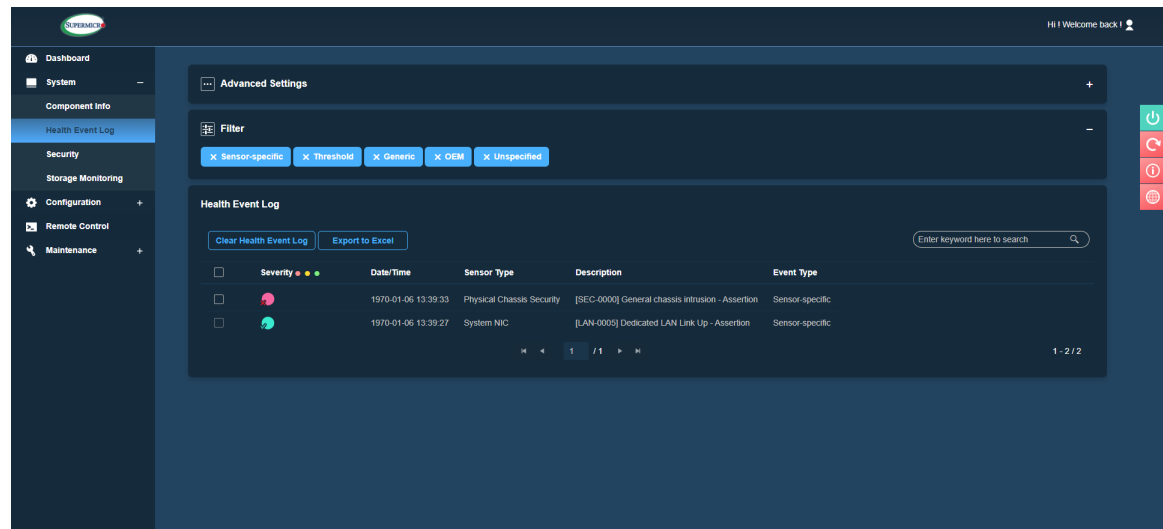
This tab provides the following details about each installed PCIe AOC such as BlueField-3 DPU in the system.

- Status: This column displays the health of the AOC card.
- Location: This column displays the location of the AOC card.
- Temperature: This column displays the temperature of the AOC card.
- Manufacturer: This column displays the manufacturer of the AOC card.
- Vendor Model Name: This column displays the vendor model name of the AOC card.
- AOC Serial Number: This column displays the serial number of the AOC card.
- AOC Part Number: This column displays the part number of the AOC card.
- AOC Firmware Version: This column displays the firmware version of the AOC card.

2.5.2 Health Event Log


This page provides a record of events that occurred on the management system. You can view, export to Excel files, clear, and acknowledge events from the monitored system. Logged events can help you to diagnose issues or detect potential issues. You can also perform prohibitive actions to resolve any such issues for the managed system and configure it to send notification alerts, SNMP Traps, or Syslog server entries for specific types of system events. You can **Enable/Disable AC Power On Event Log** and **Enable/Disable FIFO Event Log** using **ON/OFF** switches in **Advanced Settings**. The default option is **enabled**.

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




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

- Severity: This column indicates the 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: This column indicates the timestamp of event occurrence
- Sensor: This column indicates the type (Name) of the sensor that triggered the event.
- Description: This column indicates view the basic description of the event.
- Event Type: This column indicates 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 use this acknowledge warning/critical events. Select a log entry that you want to acknowledge and click on Mark as Acknowledged.
- Clear Acknowledgements: You can clear all acknowledgements and click on Clear Acknowledgement.

Multi Node

This page is used to view details about the current node as well as other nodes in the server. Under System Tab, you can view the nodes of the server in **Logical Front View of Node** and general information of 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 or MCU Version (if motherboard of the system is using MCU instead of CPLD), and BMC Version 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. 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.


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

2.5.3 Storage Monitoring

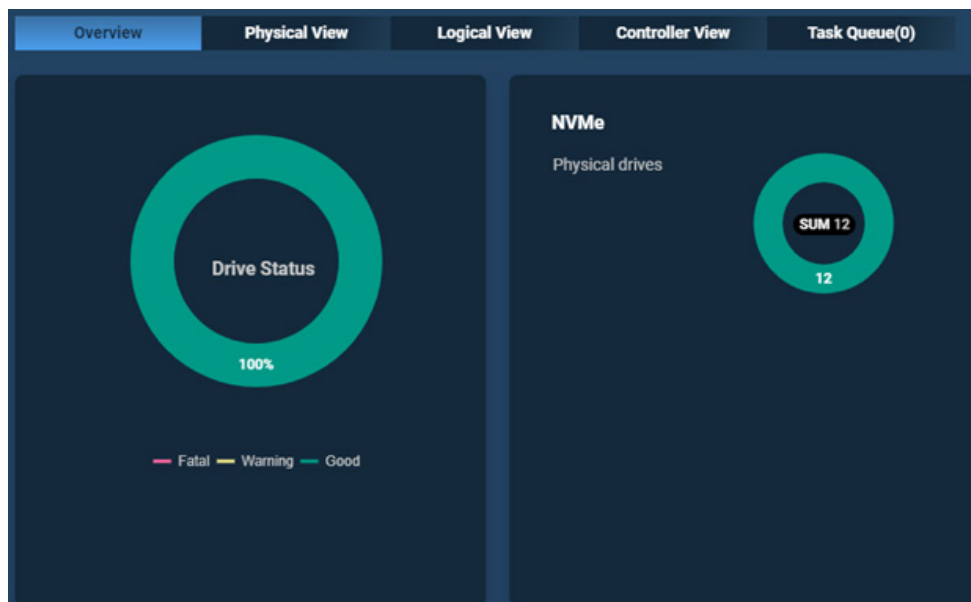
You can use this page to view details about installed storage components if the server is connected to those storage component(s). This page will not be available if a storage component is not connected. If you do not have a storage device installed in your system, the system will not display this page. 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 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, drive status will show **YELLOW**. If BMC detects that one or more connected drives is not functional, drive status will show **RED**.

 **Note:** BMC Web UI storage page currently only supports NVMe drives (U.2 or M.2) which are directly connected to a backplane. As BMC detects the NVMe Backplane, if backplane is there, the storage page will be shown and drive hot plug in-out will be monitored. For Onboard U.2, onboard M.2, or M.2 installed on an AOC storage controller, BMC would provide only temperature sensor readings.

If the system supports only direct NVMe without NVMe Backplane, hot-plugged NVMe drives WILL NOT be supported. Hence, the storage page will not display any NVMe drives when NVMe drives are hot plugged after the system is booted up. Furthermore, BMC memory space is limited. The maximum number of Storage AOC controllers for OOB/BMC support is **three**.







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. For additional information about the physical disk, click on the button to expand the menu.

	Slot#	LED	Status	Supported Actions	Disk Info#	Capacity	Link Speed	Connected Logical Drive	Connected Controller
+	0.0	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.1	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.2	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.3	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.4	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.5	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.6	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	0.7	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device0
+	1.0	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device1
+	1.1	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device1
+	1.2	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device1
+	1.3	⬢	✓	🔦 ⚙️	M7QL215THBLA-00A07	15362 GB	N/A	N/A	NVMe Device1

You can also perform actions associated with each disk. All actions are available and applicable based on the selected disk.

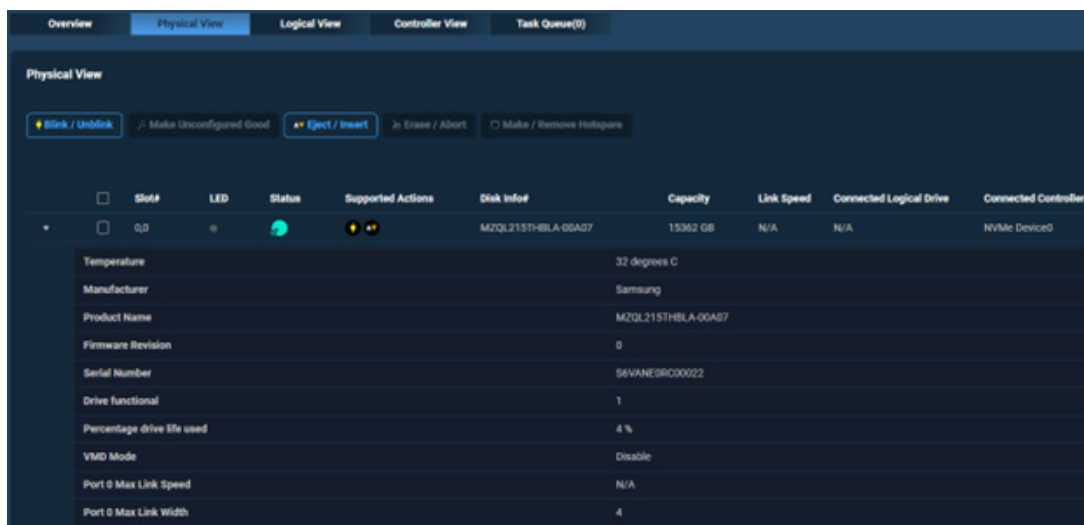
 **Note:** The function of button(s) will be greyed out if the function(s) is not available. For instance, LED blinking button will be disabled and greyed out if the connected disk does not possess the capability.

- Slot Number: This column displays the connected physical disk's slot number.
- LED: This column displays the LED blinking status of the corresponding disk.
- Status: This column displays the indicated health of the connected disk.
 -  This symbol indicates the health of all the storage component is good.
 -  This symbol indicates the storage component needs attention and could fail.
 -  This symbol indicates the storage component health is critical.
- Supported Actions: This column displays the indicated what actions are supported based on HDD type.
- Disk Info#: This column displays the available disk info.

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

Physical View Actions

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



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

The following table provides details on which storage controller is supported. In X12 and later motherboards, BMC users can select more than one NVMe drive at a time. Therefore, the Eject and Insert buttons would appear whether VMD is enabled or disabled. If there is only SATA drive connected to Broadcom storage controller, there would be no Eject nor Insert buttons appear.

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


Table for Supported Controller(s)		
	Disk Erase	Erase Abort
Broadcom	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).
Marvell (88NR2241)	<i>Not supported</i>	
NVMe	<i>Not supported</i>	<i>Not supported</i>

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

- Temperature (in Celsius)
- Name of Manufacturer
- Product Name of the storage controller
- Serial Number
- Drive functional (1 or 0)
- Percentage of drive life used (in %)
- VMD Mode (Disable / Enable)
- Port 0 Max Link Speed (in GT/s)
- Port 0 Max Link Width (i.e. 4)
- Port 1 Max Link Speed (this will not show if HDD drives have only single port)
- Port 1 Max Link Width (this will not show if HDD drives have only single port)

Logical View

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

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



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

Logical View Actions

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

- Blink: This action can be used to locate a virtual disk.
- Un-blink: This action can be used to stop the blink action.
- Delete: This action can be used 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 user to create RAID and apply changes to Controller actions. BMC supports all RAID levels from available RAID level 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 controller and click on 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.



Note: This page will be empty unless a storage controller is installed in the system.

- Product Number
- Product Revision
- Controller Name
- Controller Revision
- Location
- FW Version
- BIOS Version
- Serial Number
- Link Speed
- Controller PCIE Link Width
- Vendor ID
- Device ID
- SubVendor ID
- SubDevice ID
- Manufacture Date Timestamp
- Controller Chip Revision
- Manufacture Batch

- SAS Address (Optional)
- Checksum/Reserved (Optional)



Note: The system slot allows for the viewing of location. Below are examples illustrating how the system displays location based on its position within the system.

PCI-E Card: Onboard, Slot 2 to PCIE card: Onboard, System Slot 2

PCI-E Card: SXB1, Slot: 2 to PCIE card: SXB1, System Slot: 2

PCI-E Card: Riser, Slot: 2 to PCIE card: Riser, System Slot: 2

Create RAID

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

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

Controller Actions

You can perform the following controller actions.

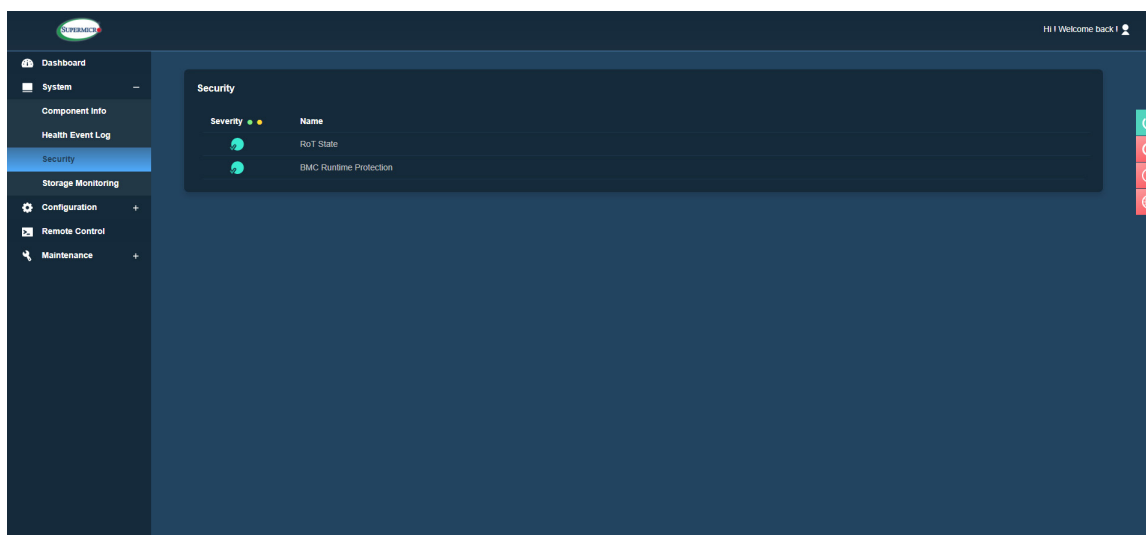


Note: Available actions will change based on the controller selection.

- Import Foreign Configurations: This option is used to import foreign RAID configurations.
- Clear Foreign Configurations: This option is used to clear foreign RAID configurations.
- Clear All Configurations: This option is used to clear all current configurations.
- BIOS Boot Mode: This option is used to 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: This option is used to enable or disable JBOD mode.

2.5.4 Secure State Monitoring

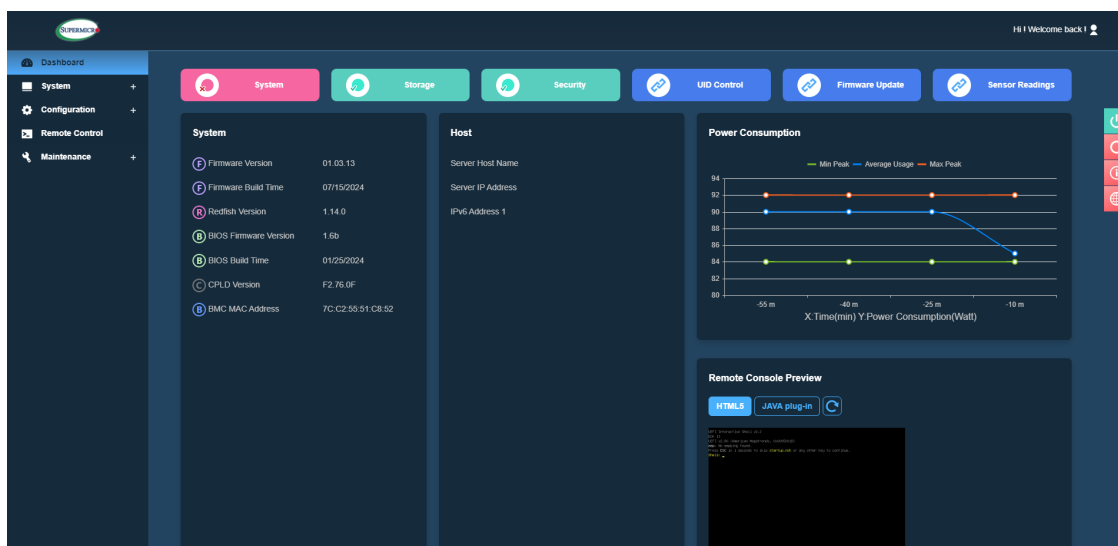
The Secure State Monitoring feature allows users to monitor the security status of the system through the supply-chain manufacturing process and its entire life cycle. Security measures allow users to be aware of any state changes and may take necessary remediation if they are caused by unexpected activities. This page allows users to view security state of the system. When users click on the tab, they will drill down to the security monitoring page which lists all indicated monitored security states. Such security states include: RoT State, BMC Runtime Protection, and Attestation Certificate Verification. When the status of any monitored states changes, an alert is sent to notify users.



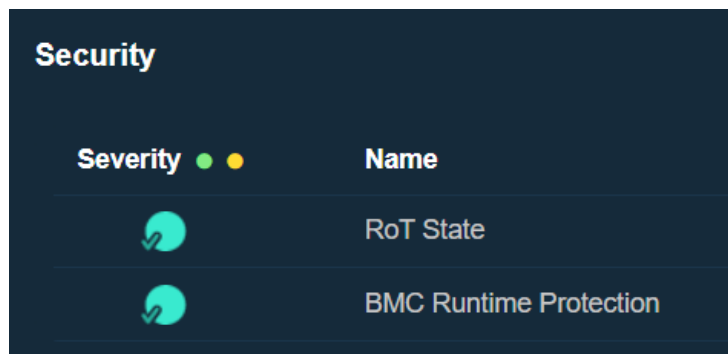
- RoT State – When green, Root of Trust in the BMC has been provisioned.
- BMC Runtime Protection – When green, the BMC monitoring of the runtime environment has not found unexpected changes to the environment.
- Attestation Certificate Verification – When green, the supply chain Remote Attestation has been provisioned and contains a valid certificate chain.



If the system does not support Remote Attestation, Attestation Certificate Verification will not be available in the WebUI.

If the system does not support Root of Trust, Security Monitoring tab will not be visible.



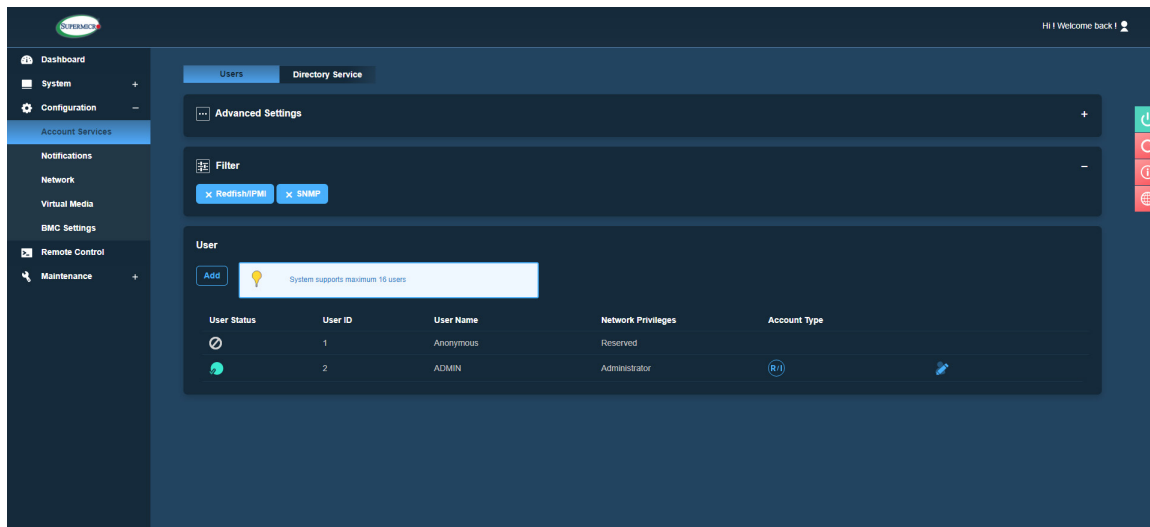
Green icon denotes the security status is active or enabled while Yellow (warning) icon indicates the security status is disabled or inactive. Users should take action if non-green states are caused by unexpected activities. When the status for monitored security state changes, SEL will be generated.



State	Green 	Yellow 	Grey/Not shown
RoT State	RoT is enabled.	The Root of Trust (RoT) is deactivated or disabled. Contact Supermicro for further clarification.	Not supported
BMC Runtime Protection	BMC Runtime Protection is enabled.	BMC Runtime Protection is deactivated or disabled. This should not occur unless debug or engineering firmware has been provided. Check the System Event Log (SEL) and Management Event Log (MEL) for relevant entries	
Attestation Certificate Verification	The provisioned device cert is validated.	<ul style="list-style-type: none"> The certificate validation for the provisioned device certificate is invalid. This issue may be caused by BMC configuration errors, such as an incorrect BMC date/time leading to a Certificate Path Validation (CPV) error. To resolve this, try synchronizing the BMC time and recheck the status. If the warning persists, contact Supermicro for assistance in identifying the cause. 	

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. Refer to the additional information in the following sections.



2.6.1 Account Services

Users

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

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



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

To add a user with Redfish or IPMI account type, the Administrator can click the Add button to enter Username and Password parameters after selecting Network Privileges and Account Type options. The Administrator can then enable or disable the new user account. If the Administrator selects Redfish or IPMI account type, Username and Password are required.

The screenshot shows the 'Add New User' form with the following fields and options:

- User Name ***: A text input field.
- Password ***: A text input field with a toggle icon to show/hide the password.
- Confirm Password ***: A text input field.
- Network Privileges**: Radio buttons for ☒ Administrator, ☐ Operator, and ☐ User.
- Enabled**: Radio buttons for ☒ Enable and ☐ Disable.
- Account Type**: Checkboxes for ☒ Redfish/IPMI and ☐ SNMP.

A light blue informational box on the right contains a lightbulb icon and the text: "Password require 8 to 20 characters includes at least 3 of character classes from 'a-z','A-Z','0-9' or Special characters."

At the bottom right, there are two buttons: "Close" and "Save".

When Administrator wants to open an SNMP account type, there are some more parameters that need to be selected. Extra parameters include Authentication Protocol (MD5 or SHA1), Encryption Protocol (DES and AES), Authentication Key, and Encryption Key.

User Table

The user table displays the following details for each user:

Add New User

User Name *

Password *

Confirm Password *

Network Privileges ☒ Administrator ☐ Operator ☐ User

Enabled ☒ Enable ☐ Disable

Account Type ☒ Redfish/IPMI ☒ SNMP

Auth Protocol ☒ MD5 ☐ SHA1

Private Protocol ☒ DES ☐ AES


Auth Key *

Private Key *

Password require 8 to 20 characters includes at least 3 of character classes from 'a-z','A-Z','0-9' or Special characters.

- **User Status:** This feature indicates whether 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:** This feature indicates the ID number used to identify the configured users. The BMC manages user access through unique IDs. It supports a maximum of 15 configurable user accounts, with one reserved for anonymous access (restricted use). This allows for up to 16 concurrent login sessions for authorized users.
- **User Name:** This feature shows the list of current users which have been created.
- **Network Privilege:** This feature will indicate one of the following types of privilege level 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 (Delete User): Administrator users can delete any user account, including those not in use. you cannot delete the default administrator account (the default ADMIN user) that are currently being logged into. 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.
 - Required password length: 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

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

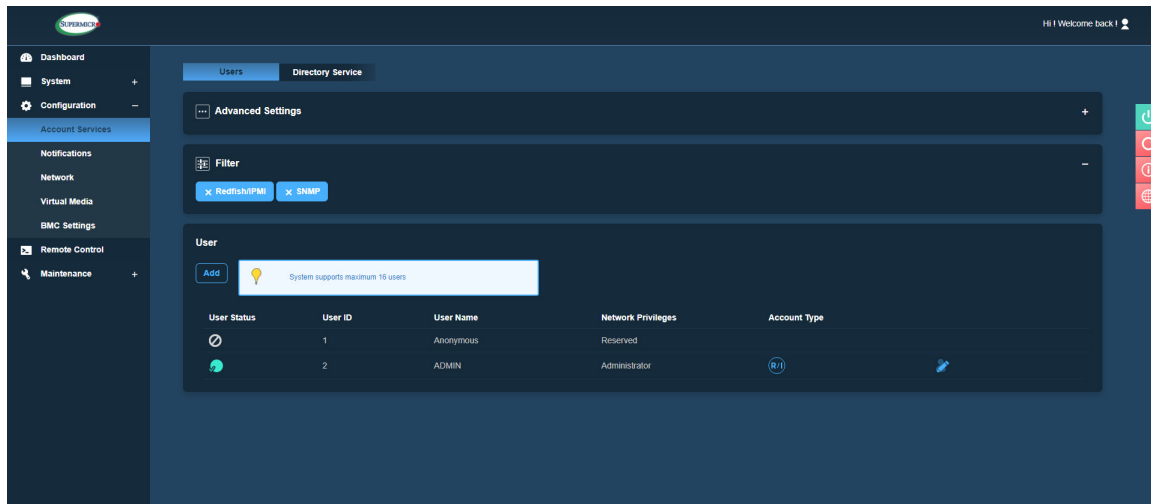
Password	<input type="password"/>
Confirm Password	<input type="password"/>

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 login) 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

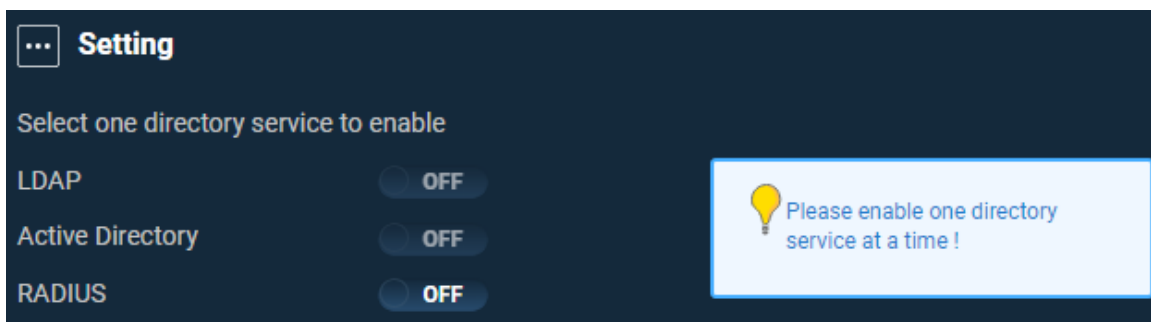


Settings

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 you to view and configure LDAP authentication by logging in to BMC Web UI or access Redfish API. This page displays a list of role groups, their group IDs, group names, domains, and network privilege settings.



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

- **Bind DN:** This feature refers to 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:** This feature refers to the bind password for LDAP server authentication. Passwords can be previewed by clicking the eye-icon button.



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

- **Username Attribute:** This feature is used to enter the username login attribute.
- **Groups Attribute:** This feature is used to enter the group membership attribute.
- **StartTLS:** When enabled, this feature allows users to initiate a secure connection. Upon activation, the connection between the client and the server is encrypted using the TLS (Transport Layer Security) or SSL (Secure Sockets Layer) protocol. This ensures that data exchanged between them is protected from eavesdropping and tampering.
- **Server Address:** This section is used to enter up to three addresses for the LDAP server. Click on [Add] to add server addresses.

- Prefix – Select to use LDAP or SSL LDAP (ldap:// or ldaps://).
- IP Address or Domain Name – Select to enter the server IP or domain name.
- 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 – Choose to use either LDAP or SSL LDAP (ldap:// or ldaps://).
 - Role – Select the privilege level for a user or role group (Administrator, Operator, or User).
 - Remote User – Enter the LDAP username.
 - Remote Group – Enter the name of the LDAP group. For example: cn=PowerUsers,ou=Groups,dc=example,dc=org.

Active Directory

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



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

- **DNS Lookup:** This field can be used to turn on DNS Lookup to allow BMC to add Active Directory servers through LDAP or LDAPS protocol.
- **Domain Name:** This field can be used to add up to five domain names to the Domain Name list for Active Directory servers.
- **Server Address:** This is a read-only field that shows up to three addresses for the Active Directory server(s).
 - **Prefix** – Select to use LDAP or SSL LDAP (ldap:// or ldaps://).
 - **IP Address or Domain Name** – Enter the server IP or domain name.
- **Port Number:** This field displays the port number of the server.
- **Static Server Address:** This field can be used 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: In this field, you can enter up to five rules for Role, Remote User, and Remote Group. Click on [Add] to add rules and enter the following fields.
 - Roles – Select 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 the **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: This field is used to 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: This field is used to select to enter the server IP or Domain name.
- Port Number: This field is used to enter the port number. Values range between 1 and 65535 (half-width).



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


No	Server Address
1	0.0.0.0:1812

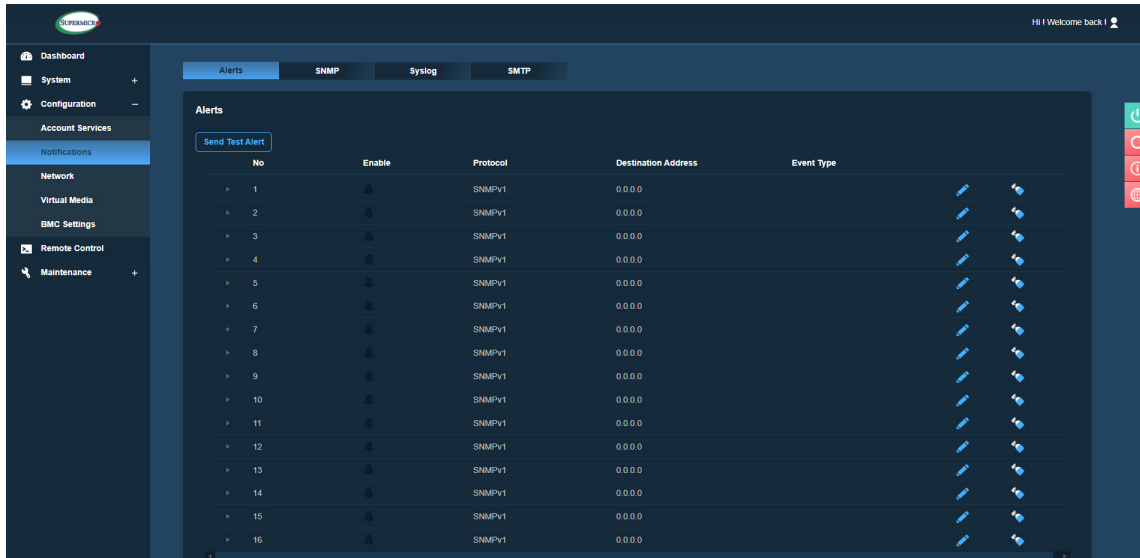
2.6.2 Notifications

































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

Alerts



You can use this page to configure the 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:** 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		SNMPv1	0.0.0.0	
2		SNMPv1	0.0.0.0	
3		SNMPv1	0.0.0.0	
4		SNMPv1	0.0.0.0	
5		SNMPv1	0.0.0.0	
6		SNMPv1	0.0.0.0	
7		SNMPv1	0.0.0.0	
8		SNMPv1	0.0.0.0	
9		SNMPv1	0.0.0.0	
10		SNMPv1	0.0.0.0	
11		SNMPv1	0.0.0.0	
12		SNMPv1	0.0.0.0	
13		SNMPv1	0.0.0.0	
14		SNMPv1	0.0.0.0	
15		SNMPv1	0.0.0.0	
16		SNMPv1	0.0.0.0	

The Alerts table will display the following information:

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

- Alert
- ResourceAdded
- ResourceRemoved
- ResourceUpdated
- StatusChange
- Modify: Click on the pencil icon  on the row of an alert to configure the settings or make changes to the alert.
- Modify Alert: This field can be used to 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.



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

- Message – Enter a message to send out to the destination. This field is available when SMTP protocol is selected. This field is required prior 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 a content for the Subject field. This field is only available for SMTP protocol.



Note: This field is displayed only when SMTP is selected and required for SMTP protocol. You must fill in the Subject field for SMTP protocol.

- Trap Community – Enter information for traps.



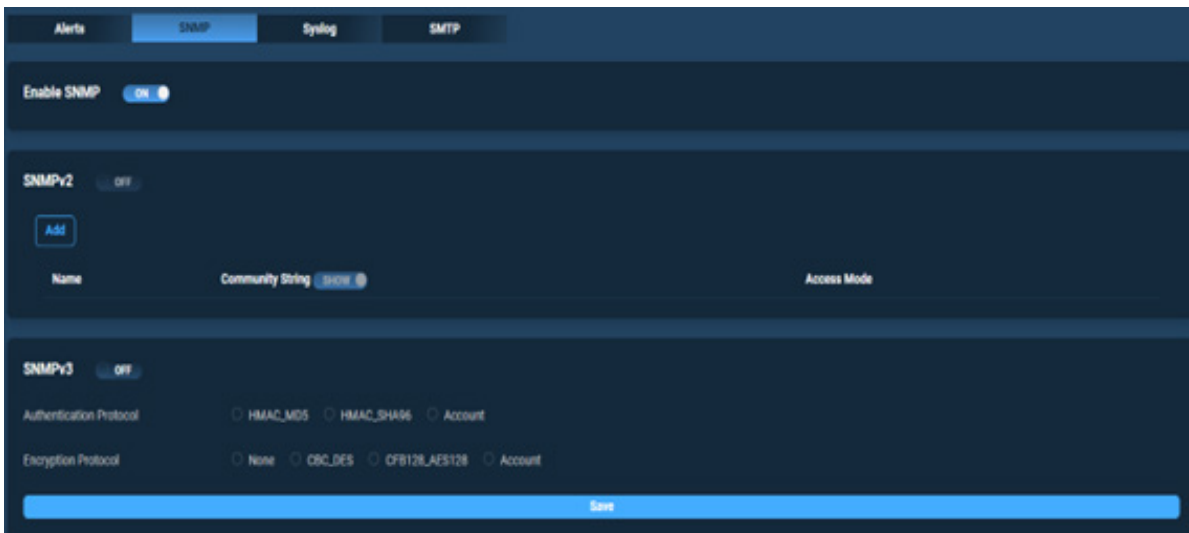
Note: This field is only displayed when SNMPv1 is selected.

- Delete – You can delete respective 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.

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.



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

- Navigation tabs: Alerts, **SNMP**, Syslog, SMTP.
- Enable SNMP: A toggle switch set to ON.
- SNMPv2 section:
 - SNMPv2 toggle switch: OFF.
 - Add button: A blue button labeled 'Add'.
 - Table headers: Name, Community String, Access Mode.
- SNMPv3 section:
 - SNMPv3 toggle switch: OFF.
 - Authentication Protocol: Radio buttons for HMAC_MD5, HMAC_SHA96, and Account.
 - Encryption Protocol: Radio buttons for None, CBC_DES, CFB128_AES128, and Account.
- Save button: A blue button labeled 'Save' at the bottom.

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 afterwards.
3. To enable SNMPv3, you can select one of the following protocols.
 - Authentication Protocol: You can select either HMAC_MD5, HMAC_SHA96, or Account for Authentication Protocol.
 - Encryption Protocol: You can select either None, CBC_DES, CFB128_AES128, or Account for the Encryption protocol.

4. Click [Save] to save user settings. The saved configurations are to be used whenever you start or stop the SNMP daemon.



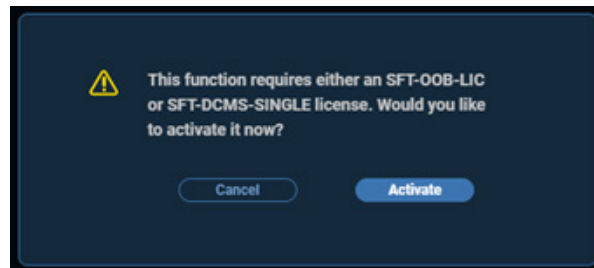
Note: By default, all SNMP settings are disabled (OFF) and SNMP port is set to UDP port 161. You can go to the Port page (Configuration → Network → Port) to change the SNMP port number. Once SNMP setting is ON, you can turn ON SNMPv2 or SNMPv3 using the ON/OFF buttons. Once SNMP is turned OFF, SNMPv2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

Syslog

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



Note: This feature requires a software license.



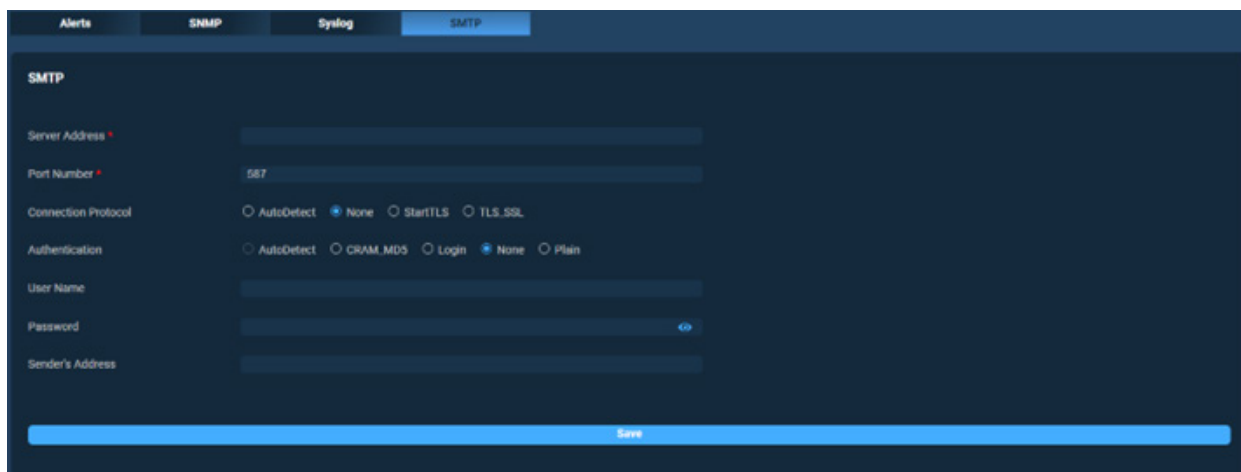
To configure the syslog settings, refer to the following steps.

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 SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network by selecting the SMTP tab..

The screenshot shows the SMTP configuration page in a BMC interface. At the top, there are tabs for Alerts, SNMP, Syslog, and SMTP, with SMTP being the active tab. Below the tabs, the page is titled "SMTP". The configuration fields include: "Server Address" with a text input field; "Port Number" with a text input field containing "587"; "Connection Protocol" with radio buttons for AutoDetect, None (selected), StartTLS, and TLS_SSL; "Authentication" with radio buttons for AutoDetect, CRAM_MD5, Login, None (selected), and Plain; "User Name" with a text input field; "Password" with a text input field and a toggle icon; and "Sender's Address" with a text input field. At the bottom of the form is a large blue "Save" button.

To configure SMTP settings, refer to the following options:

- **Server Address:** Use this field to enter the address for the SMTP mail server to configure SMTP.
- **Port Number:** Use this field to enter a SMTP port number. By default, the port number is 587.
- **Connection Protocol:** Use this field to choose one of the following protocols to set up 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: Use this field to enter the user name for SMTP mail server. This is optional.
- Password: Use this field to set up the user password if User Name is added for the SMTP mail. Passwords can be previewed by clicking the eye-icon button.



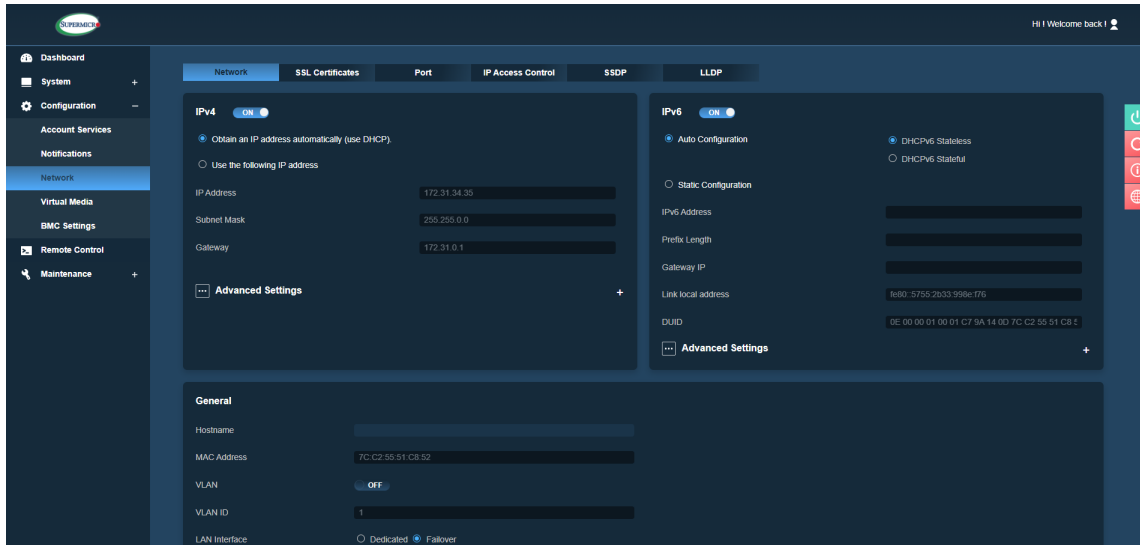
Note: By default, the password characters are hidden under periods or dots (...).

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

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


2.6.3 Network

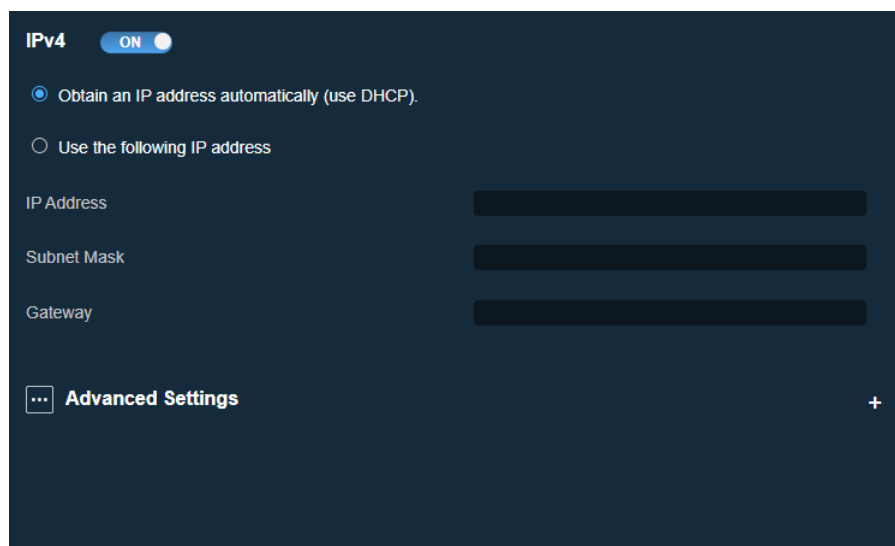
Use this page to configure BMC network settings such as IPv4, IPv6, SSL Certification, Ports, IP Access Control, and SSDP. Network setting values should be non-negative integer values. In addition, both IPv4 and IPv6 ports are ON (enabled) by default.



IPv4

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

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



IPv4 Configuration

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

- **ON/OFF:** This field has the ON/OFF toggle button to enable or disable the IPv4 network connection for BMC.
- **Automatically Obtain IP Address (via DHCP):** This field gives you the choice to enable automatic IPv4 configuration using DHCP (Dynamic Host Configuration Protocol). This option streamlines the process, allowing the system to dynamically assign and manage IP addresses, enhancing convenience, and efficiency.
- **Manually Configure IPv4 Address:** This features gives you the option to configure a static IP address. Enter the following details.
 - **IP Address** – Manually enter IPv4 address for BMC
 - **Subnet Mask** – Specify the IPv4 Subnet Mask
 - **Gateway** – Enter IPv4 Gateway address

IPv4 Advanced Settings

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

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




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

IPv6


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

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

 **Note 1:** When DHCPv6 Stateful 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. Auto Configuration must be enabled (ON) for BMC to receive IPv6 IP address(es) when DHCPv6 Stateful mode is selected.

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

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

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

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

IPv6 Advanced Settings

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

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

General

In this section, you can set up a name for server identification in Hostname, view 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 hyphen are allowed for interior. Except for hyphen, 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 BMC interface was set to a member of VLAN 1 prior saving the setting if VLAN ID was decided to set to 1. Otherwise, once the configuration is saved, users would lose access to BMC via OOB unless BMC interface is connected to a Switch port which is configured as VLAN 1.)

- LAN Interface: You can select the type of the LAN interface.
 - Failover
 - Dedicated
 - Shared

- Shared LAN: You can select one of the LAN modes.
 - Auto
 - Onboard (Onboard1 or Onboard2)
 - AIOM (AIOM1 and AIOM2, if there is more than one AIOM)
 - AOC (AOC1 and AOC2, if there is more than one AOC)



Note: When LAN Interface is set to **Dedicated**, only Dedicated cards will be available. When LAN Interface is set to **Shared**, only Shared cards will be available. When LAN Interface is set to **Failover**, Dedicated and Shared cards will be available.

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

Network Mode Table	
Network Combination Mode	Definition
Dedicated	"Dedicated" LAN
Shared (Auto Mode)	Onboard Shared LAN or AIOM Shared LAN (if there is no Onboard Shared LAN designed in)
Failover (Auto Mode)	Failover between the first Shared LAN and Dedicated LAN
Shared – Onboard/Onboard1/Onboard2	Onboard Shared LAN; Onboard1 and Onboard2 Shared LAN if there is more than one Onboard LAN
Shared – AIOM/AIOM1/AIOM2	AIOM Shared LAN; AIOM1 and AIOM2 Shared LAN if there is more than 1 AIOM LAN
Shared – AOC/AOC/AOC1/AOC2	AOC Shared LAN; AOC1 and AOC2 Shared LAN if there is more than 1 AOC LAN
Failover – AOC	Failover between "Shared - AOC" and "Dedicated"
Failover – AOC1	Failover between "Shared – AOC1" and "Dedicated"
Failover – AOC2	Failover between "Shared – AOC2" and "Dedicated"
Failover – AIOM	Failover between "Shared – AIOM" and "Dedicated"
Failover – AIOM1	Failover between "Shared – AIOM1" and "Dedicated"
Failover – AIOM2	Failover between "Shared – AIOM2" and "Dedicated"
Failover – AOC1/AOC2	Failover between "Shared – AOC1" and "Shared – AOC2"
Failover – AIOM1/AIOM2	Failover between "Shared – AIOM1" and "Shared – AIOM2"

- 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 the speed of the system link connection.
- Duplex: You can view whether the BMC link is a full or half duplex.

SSL Certificates

This tab allows you to upload custom SSL certificates. Supported SSL Certificate files 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 textboxes.
- New SSL Certificate: You can upload a new SSL Certificate by clicking on Select File button to select a supported SSL Certification file.
- New Private Key: You can upload a new private key by clicking on 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 is supported.

The screenshot shows the 'SSL Certificates' configuration page. It features a dark blue background with white text. At the top, the title 'SSL Certificates' is displayed. Below it, there are two rows of input fields for 'Certification Valid From' and 'Certification Valid Until', both showing 'Jul 15 00:00:00 2024 GMT' and 'Jul 15 00:00:00 2027 GMT' respectively. To the right of these fields are two yellow lightbulb icons with the text 'Certificate file should end with .pem or .cert'. Below the input fields, there are two rows for 'New SSL Certificate' and 'New Private Key', each with a 'Select File' button. At the bottom of the form, there is a large blue 'Upload' button.

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 individual port to modify the port number. Click on [Save] to apply changes. The following ports are ON or OFF by default.


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

- 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 shows the 'Port' configuration tab in a web interface. It has a dark blue background with white text. At the top, there are tabs: 'Network', 'SSL Certificates', 'Port' (selected), 'IP Access Control', 'SSDP', and 'LLDP'. Below the tabs, there are two sections: 'TCP Ports' and 'UDP Ports'. Each section contains a list of ports with a toggle switch and a text input field for the port number. The 'Web SSL Port' toggle is greyed out. At the bottom right, there is a 'Save' button.

Port Name	Status	Port Number
SSH Port	ON	22
Web Port	ON	80
Web SSL Port	ON (disabled)	443
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.

Network General Frame of WebUI

LAN Interface when in Dedicated Mode

Dedicated	
Status	Connected
Speed	1G
Duplex	Full Duplex
Switch Chassis ID	94:18:82:9e:92:c0
Switch Port ID	34
Switch VLAN ID	41
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

LAN Interface is in Shared Mode


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

Active Interface	Share
Share	
Status	Connected
Speed	1G
Duplex	Full Duplex


Shared	
Status	Connected
Speed	10G
Duplex	Full Duplex
Switch Chassis ID	N/A
Switch Port ID	N/A
Switch VLAN ID	N/A

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

Shared	
Status	Disconnected
Speed	Unknown
Duplex	Unknown

 **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. Some examples of special motherboards are included in the table below..

Motherboard	MAC3	MAC4
X13DEM	AIOM	AOC
X13DET_B	AIOM	AOC
X13OEI	Onboard	AIOM
X13SEDW_F	AIOM	AIOM and AOC
X13SEFR_A	AIOM	AIOM or AOC
X13SEM_TF	Onboard and AOC	AOC
X13SCW	Onboard	

 **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

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

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

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

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

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

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.

Sample Web UI for X13XEFR

General


Hostname	<input type="text" value="LukeX13SEFRA101"/>
MAC Address	<input type="text" value="3c-ec-ef-34-91-45"/>
VLAN	<input 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

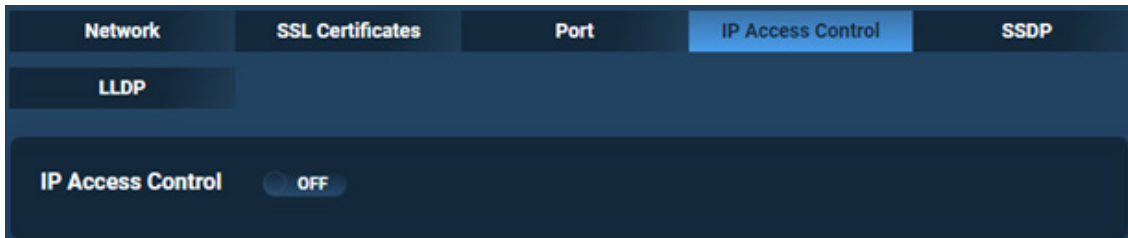
General

Hostname	<input type="text" value="LukeX13SEFRA101"/>
MAC Address	<input type="text" value="3c-ec-ef-34-91-45"/>
VLAN	<input 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

IP Access Control

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

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





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

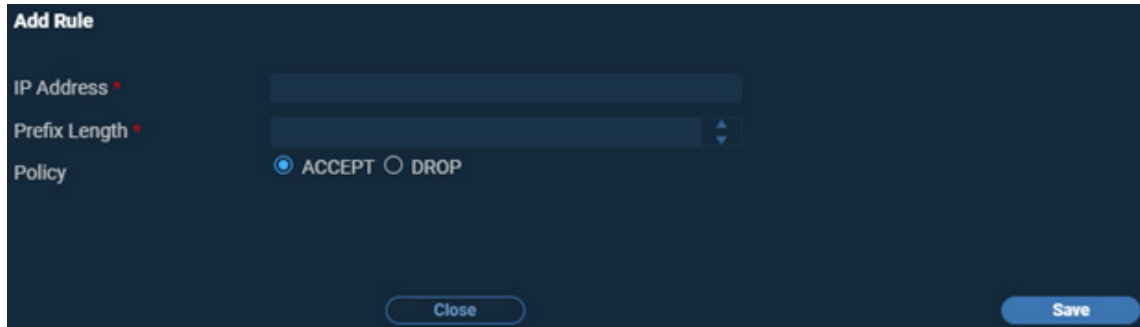
- ID: This column shows the number of IP Access Control rules.
- IP Address Control List: This column shows the list of possible network rules for IP addresses that can be accessed by users.
- Prefix Length: This column shows the Mask settings. The length should be an integer value between 0 and 128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



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 .

A dark-themed dialog box titled "Add Rule". It contains three input fields: "IP Address" with a red asterisk, "Prefix Length" with a red asterisk, and "Policy". The "Policy" field has two radio buttons: "ACCEPT" (selected) and "DROP". At the bottom, there are two buttons: "Close" and "Save".

Add Rule

IP Address *

Prefix Length *

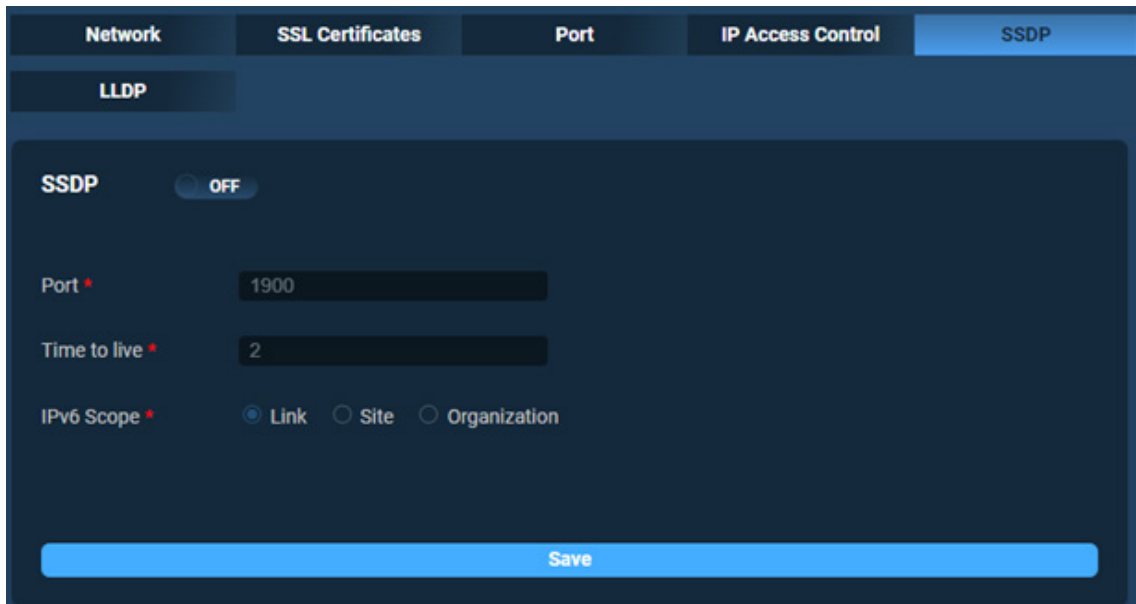
Policy ☒ ACCEPT ☐ DROP

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 previous ID number when you set a new policy.
- You can add the same IP Address with the 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 the **Save** button. If users click **Save**, no change will be made to the IP Access Control List.
- If you add the same IP Address with the same prefix and the different policy of either ACCEPT or DROP, then you will see the new policy will be applied to the existing listing. For example, if the existing IP Address is 10.2.3.4 with prefix 32 and ACCEPT policy in ID 3 (line 3), when you add 10.2.3.4, prefix 32, and DROP policy, line 3 will display 10.2.3.4, prefix 32 and DROP policy.

SSDP (Simple Service Discovery Protocol)

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



The screenshot shows a web-based configuration interface for SSDP. At the top, there are five tabs: 'Network', 'SSL Certificates', 'Port', 'IP Access Control', and 'SSDP'. The 'SSDP' tab is selected and highlighted in blue. Below the tabs, there is a sub-tab labeled 'LLDP'. The main content area is titled 'SSDP' and contains a toggle switch set to 'OFF'. Below the toggle, there are three configuration fields: 'Port' with a value of '1900', 'Time to live' with a value of '2', and 'IPv6 Scope' with three radio button options: 'Link' (selected), 'Site', and 'Organization'. At the bottom of the form is a large blue button labeled 'Save'.

You can enable or modify SSDP 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.

LLDP (Link Layer Discovery Protocol)

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

The screenshot shows the LLDP configuration page with the 'Enable LLDP' toggle set to 'OFF'. The 'LLDP Receive' and 'LLDP Transmit' sections are empty, indicating no LLDP information is being received or transmitted.

The screenshot shows the LLDP configuration page with the 'Enable LLDP' toggle set to 'ON'. The 'LLDP Receive' and 'LLDP Transmit' sections are populated with network information.

LLDP Receive	
Chassis ID Subtype	MacAddress
Chassis ID	94:18:32:9c:12:c0
Port ID Subtype	Local Storage
Port ID	34

LLDP Transmit	
Chassis ID Subtype	MacAddress
Chassis ID	46:ac:59:5a:17:69
Port ID Subtype	MacAddress
Port ID	26:ac:59:5a:17:69

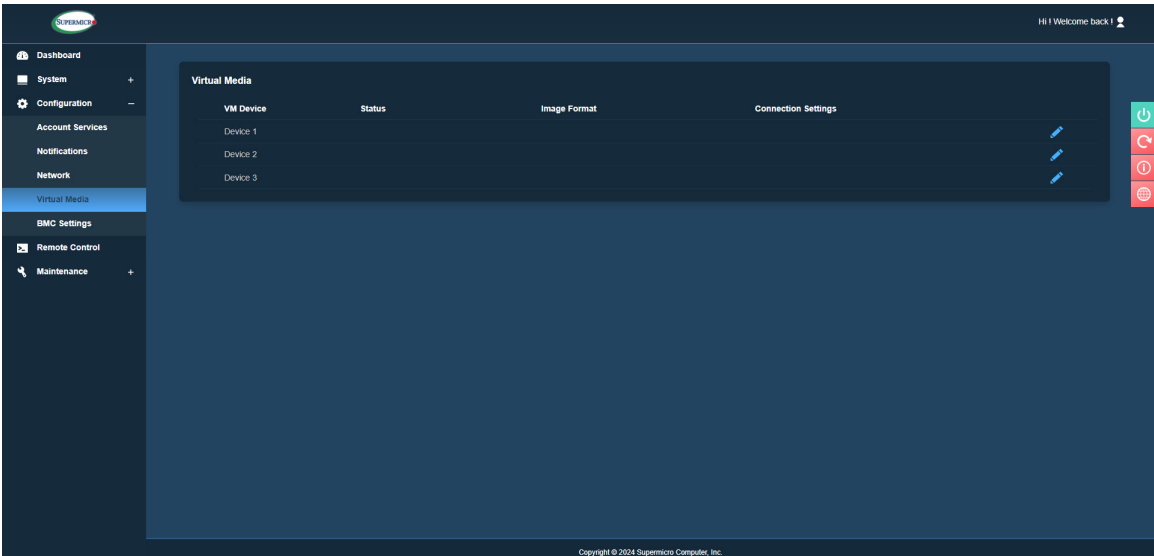
When active, LLDP provides essential network information, including:

- **Chassis ID Subtype:** This field specifies the format of the identifier used to uniquely identify the connected network device, such as a MAC address or network address.
- **Chassis ID:** This field represents the actual identifier of the connected network device, helping to uniquely identify it.

- **IPv4 Address:** This field displays the IPv4 network address associated with the interface or connected device.
- **IPv6 Address:** This field indicates the IPv6 network address, crucial for configuring connectivity in IPv6 networks.
- **MAC Address:** This is unique hardware address assigned to the network interface or device, facilitating local network communication.
- **VLAN ID:** This field identifies the Virtual LAN (VLAN) to which the interface or device belongs, aiding in traffic categorization and network management.
- **Port ID Subtype:** This specifies the format of the identifier used to uniquely identify the connected port.
- **Port ID:** Represents the actual identifier of the connected network port, aiding in precise port identification within the network.

2.7.4 Virtual Media

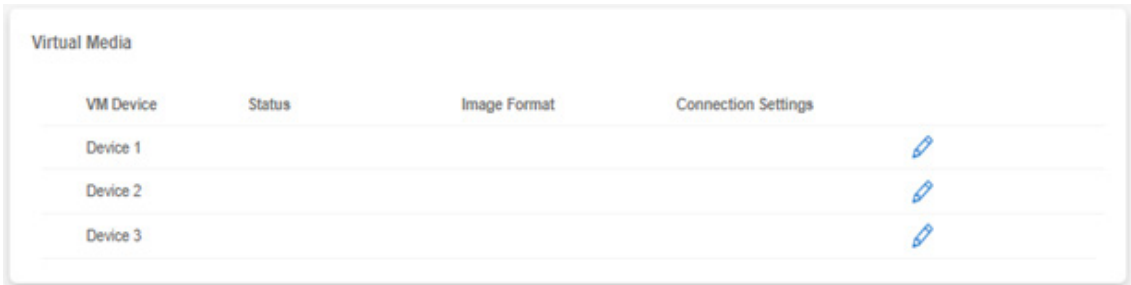
Using BMC Web UI, users can go to this page to connect to Floppy (IMA/IMG format file) or CD-ROM (ISO format file) images residing in remote file server(s) and check status of connected devices respectively. SFT-DCMS-SINGLE software license is required for HTTP and HTTPS usage.



- Users can mount VM Devices to the same source of media.
- Web UI Users cannot unmount VM sources that are mounted via iKVM interface and vice versa.

VM Device

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



VM Mounting and Unmounting Notes

Status

This field provides the status of currently connected CD-ROM/ISO devices, indicating that the connection to the source is successfully established. You can also use this feature to disconnect respective devices as well. The status of mounting devices should be in sync from Virtual Media page in BMC Web UI and iKVM remote control. For example, if a user mounted an image in Device 1 from Virtual Media page, the expected status should be shown in iKVM remote control as well. The connection would show either URI or Applet depending on how the images are mounted. If mounted via BMC Web UI, it is considered as mounted via URI and if mounted via iKVM. The image is shown as mounted via Applet. Mounting and unmounting a device can only be done by the initial method/interface (via Web UI or via iKVM).



Image Format

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

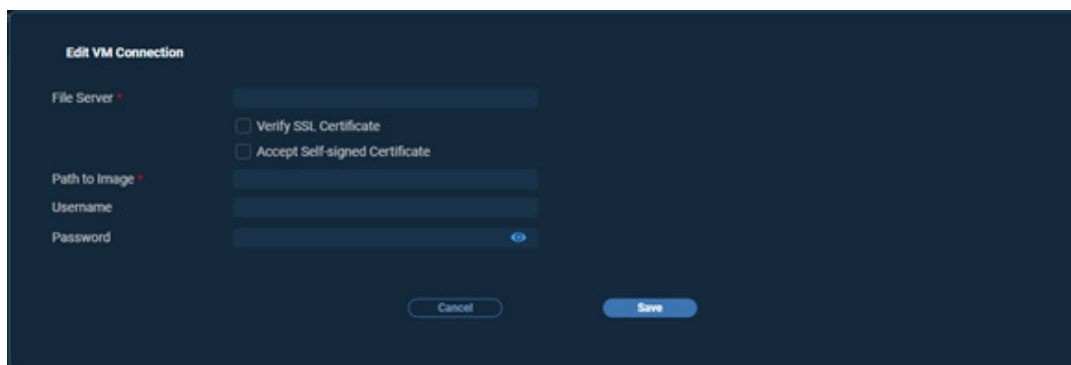
Connection Settings

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

Click on the Connect/Disconnect Icons

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

Edit VM Connection



Users can access to VM devices by clicking on pencil icon  :

- File Server: The host server for your console redirection. File Server can only accept alphanumeric characters, dash, and periods (i.e. a-z, A-Z, 0-9, – and .) for the URL domain part. Moreover, the domain part will only accept http:// or https:// at the beginning of the string (i.e. HTTP+ IP Address, HTTPS + IP Address).]. Port number can be used after the IP Address as an option.
- For example: http(s)://192.188.8.8:443 for IPv4 Address and http(s)://[2021::8888:443].
- Path to Image: The Path of the CD-ROM image file will only accept a-z, 0-9, @^/._- and will reject all other special characters, including space and tab. The '/' character should only be accepted when using them alone, not continuously, which means you cannot use //, \\, \/, and V. The path must be started with '/' or * character and ends with ".iso" file extension.
- Username: Users that have access to the CD-ROM image files will only accept a through z and A through Z. All other special characters will be rejected, including space and tab.
- Password: The user password will only accept a-z, A-Z, and 0-9. All other special characters will be rejected, including space and tab. Passwords can be previewed by clicking eye-icon button to view password.



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

iKVM Interface

Users can access HTML5 iKVM Console using the [Launch Console] icon. The following image is a VM from the HTML5 iKVM Console.

IMG/IMA Image

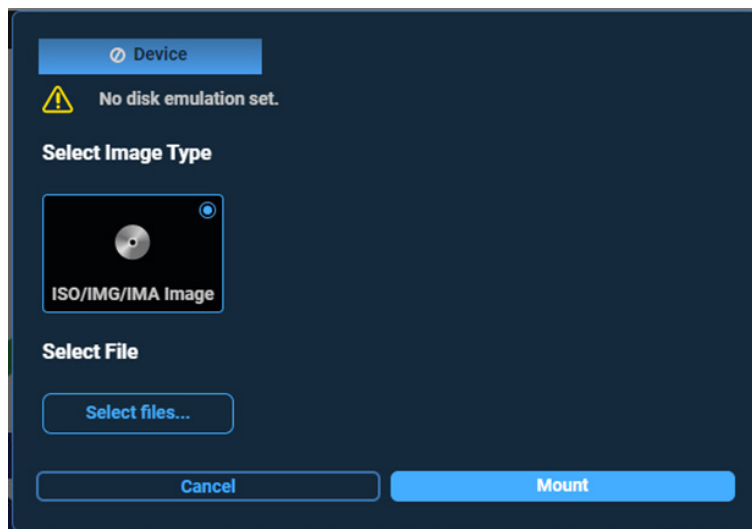
Use the following options to upload floppy images:

- Choose File: Upload a floppy image (Allowed file type: img and .ima type file)
- Upload: Click on [Upload] to upload the IMA or IMG format file to the server

ISO Image

Use the following options to upload and mount ISO files:

- Select File: Select an ISO file to upload from a local host (i.e. Laptop, workstation, etc.).
- Mount: Upon clicking [Mount] button, the ISO would be mounted.

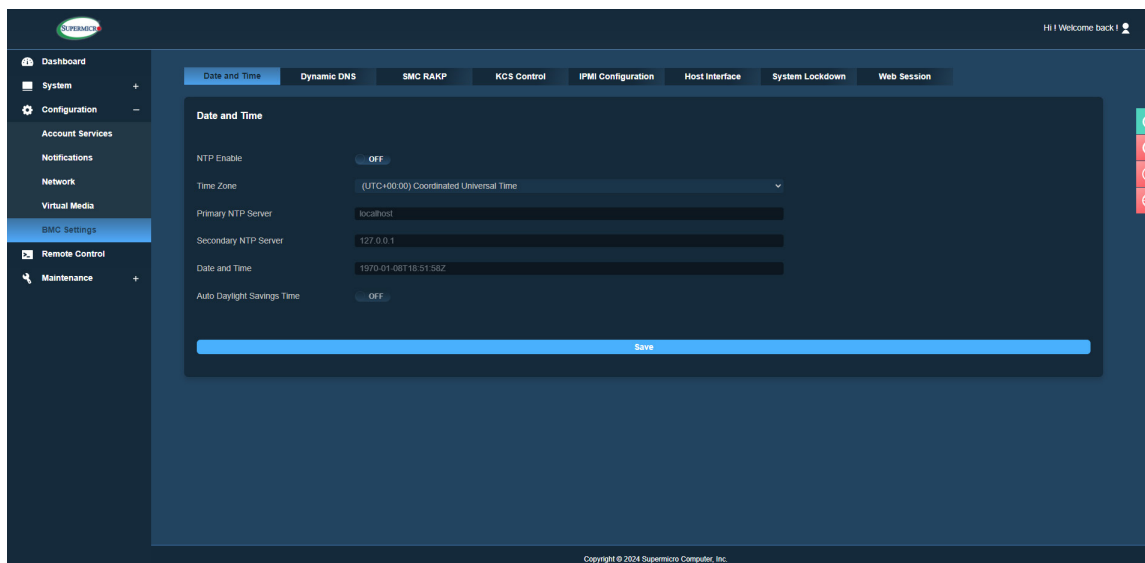


Virtual Media (VM) License						
	SMBV2	SMBV3	CIFS	SAMBA	HTTP	HTTPS
Current X13 License	STANDARD	STANDARD	STANDARD	STANDARD	SFT-OOB-LIC	SFT-OOB-LIC

2.6.4 BMC Settings

Date and Time

You can use the NTP (Network Time Protocol) server setting to set 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 by toggling the ON/OFF button. If NTP is disabled, the system time is used to set date and time. The Time Zone can be adjusted as required. (in X12 BMC FW 01.03.xx and X13 BMC FW 01.01.xx). If NTP is enabled, the NTP server is used to set date and time. However, before BMC successfully gets the date and time from 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, 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. 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 +14:00 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 YYYY-MM-DD/hh:mm:ss (date is in YYYY-MM-DD and Time is in HH:MM).
- **Auto Daylight Savings Time (ON/OFF):** The ON-OFF button can be toggled to enable or disable Auto Daylight Savings Time. When the Auto Daylight Savings feature is enabled, users will see adjusted time if the Time Zone observes Daylight Savings Time. For example, being in the Spring Pacific Time will add one hour, as shown below

DST is disabled (OFF), 2023-01-18T 09:09:18

DST is enabled (ON), 2023-01-18T 10:09:18

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 of the BMC (Baseboard Management Controller) host server.



Note: BMC will pop up the message: *“Only alphanumeric are allowed (i.e. a-z, A-Z, 0-9), hyphen (-), and period (.) characters are allowed.”* if users enter incorrect characters.

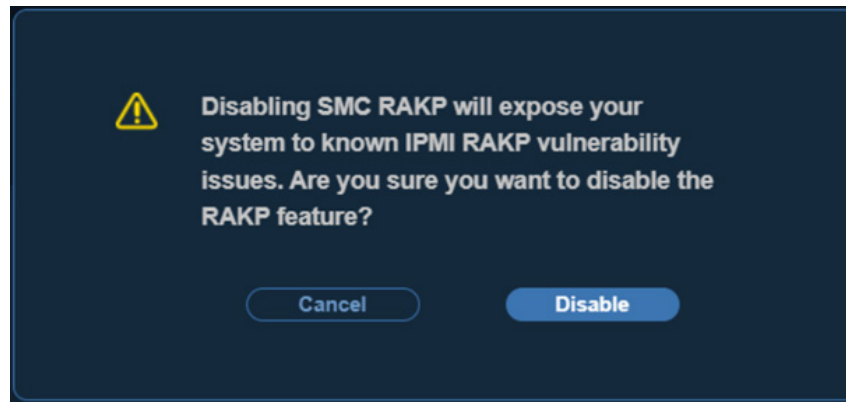
- **TSIG Authentication:** You can enable TSIG (Transaction Signature) authentication support and upload TSIG.key files.



Note: Fields with * are optional.

SMC RAKP

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



KCS Control

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

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

BMC Configuration

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

Restore BMC/IPMI Configuration from Self Config file

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

Restoring BMC/IPMI configurations from a file of another system with the same platform

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

Restoring BMC/IPMI configurations from a file of the same platforms with the same GUID

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

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

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

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

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

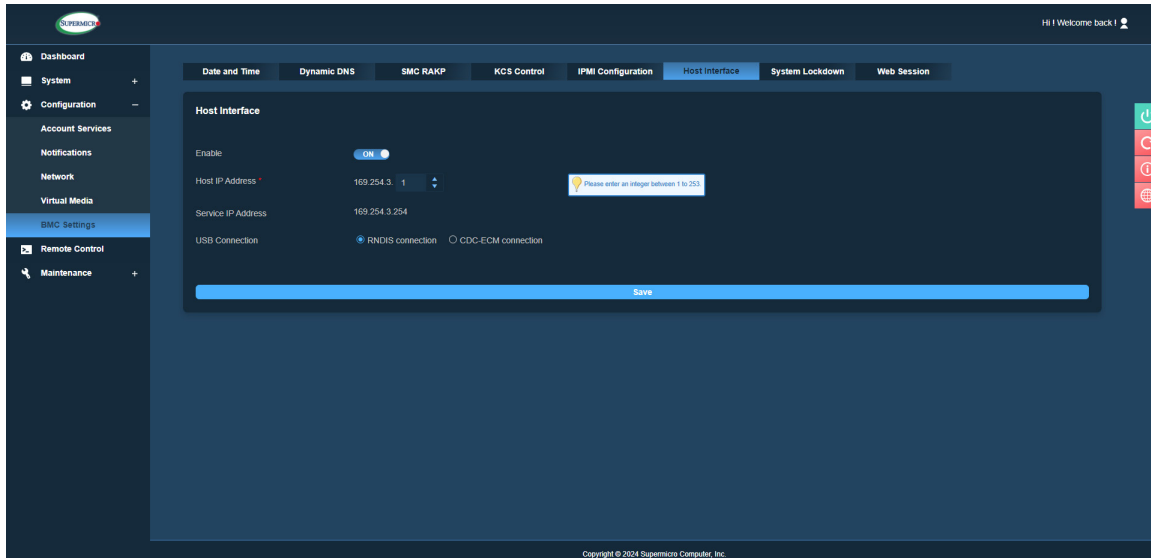


Note: The 'Save BMC/IPMI Configuration' option will download an IPMI configuration .bin file. Hostnames cannot be transferred from one system to another. Passwords cannot be transferred or overridden by another BMC/IPMI Configuration. IP addresses are unaffected since they are not saved when saving the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

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

Host Interface

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




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

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

System Lockdown

The implementation of a System Lockdown feature enhances the system security by safeguarding against inadvertent or unauthorized modifications to the system configuration while it is operational. Once activated, System Lockdown rigorously blocks all attempts to alter system configurations, including firmware updates. Any attempt to make changes during this lockdown state will be promptly intercepted, and the user will be duly notified of such attempts. Additionally, to provide a clear visual indication of the system's secured state, the BMC will display a specific icon when the system is under lockdown. This proactive approach ensures a robust defense against unintended changes, bolstering the overall integrity and reliability of the system.

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

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

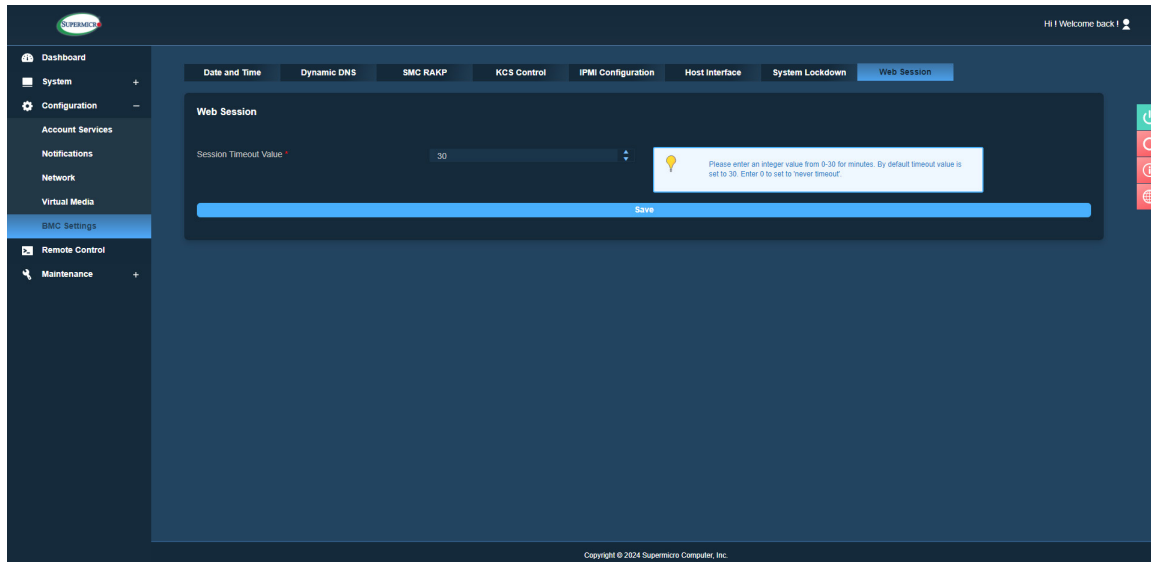


The following features will be functional during system lockdown.

- 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.



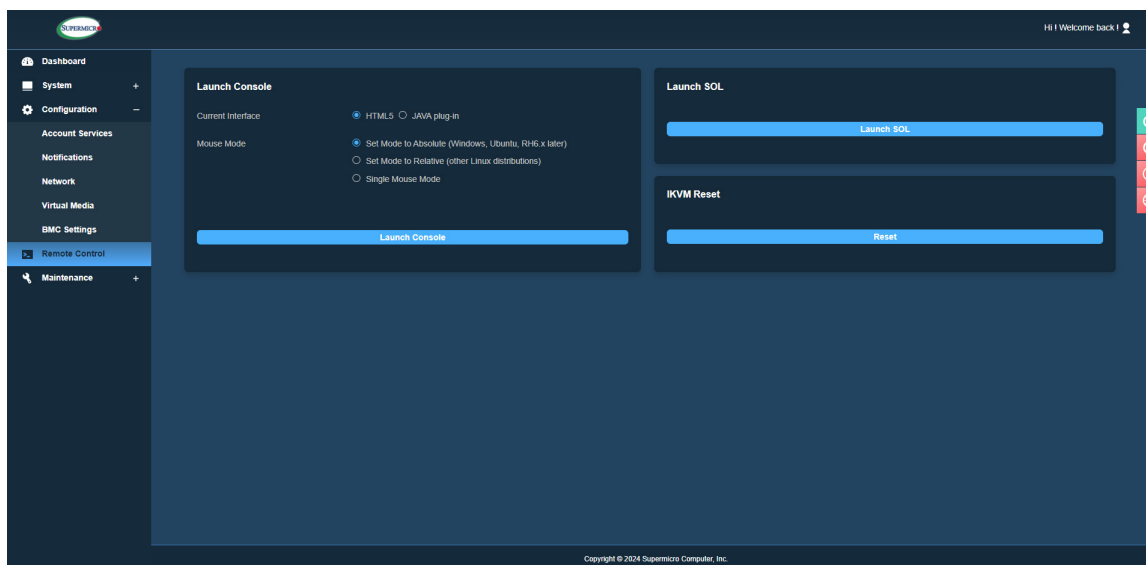
Smart Power

Smart Power is a new feature on X12 MB systems and later generations. Admin users of the Master node of a Multi-node systems like 'Big-Twin' and 'H12DST-B' systems can turn on or enable Smart Power Option in the Smart Power page. The feature will involve Power Supply, BMC, and CPLD. Smart Power will be activated when a PMBUS alert happens. Alerts will be sent to 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 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

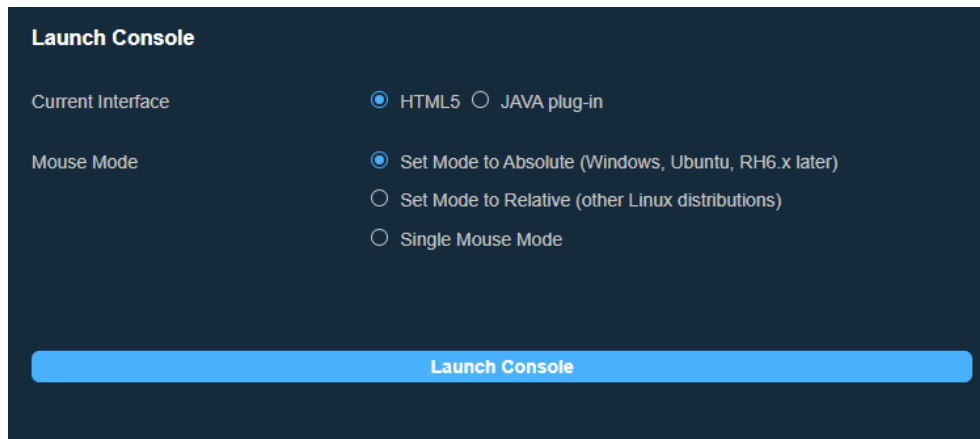
Remote control options allow you to perform operations on a remote server via remote access



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. After establishing a remote console session, users will be unable to switch between JAVA and HTML5 interfaces. A message *“Once a remote console session is connected, switching between JAVA and HTML5 is not allowed.”* will prompt users if they attempt to change the remote console interface after a session has been established. The maximum number of sessions for either Java or iKVM console is 4. Hence, when there are more than 4 sessions open, there will be a message to users, *“The maximum number of open sessions has been reached!”*



To launch a remote console via the default, iKVM, refer to the following steps:


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

Utilize OpenJDK as Oracle Java is no longer supported.

To launch 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.

A new console will open in a separate browser window. For more detailed options, consider launching iKVM.

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

Launch SOL

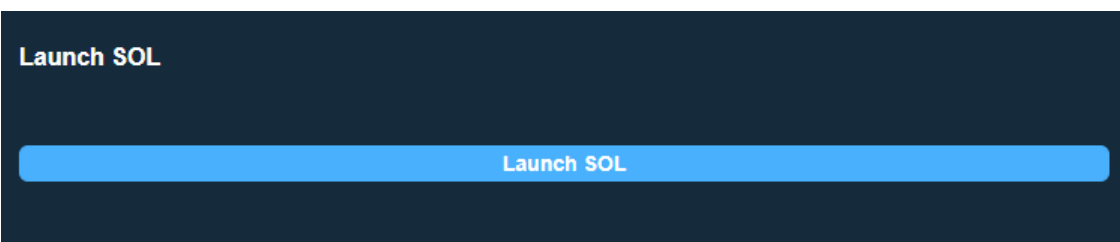
This feature allows you to launch a remote console using SOL (Serial over LAN), which provides serial port connections over LAN to access a host server via console redirection. It also allows the system administrator to monitor and manage servers from a remote site. In order to connect the console through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

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



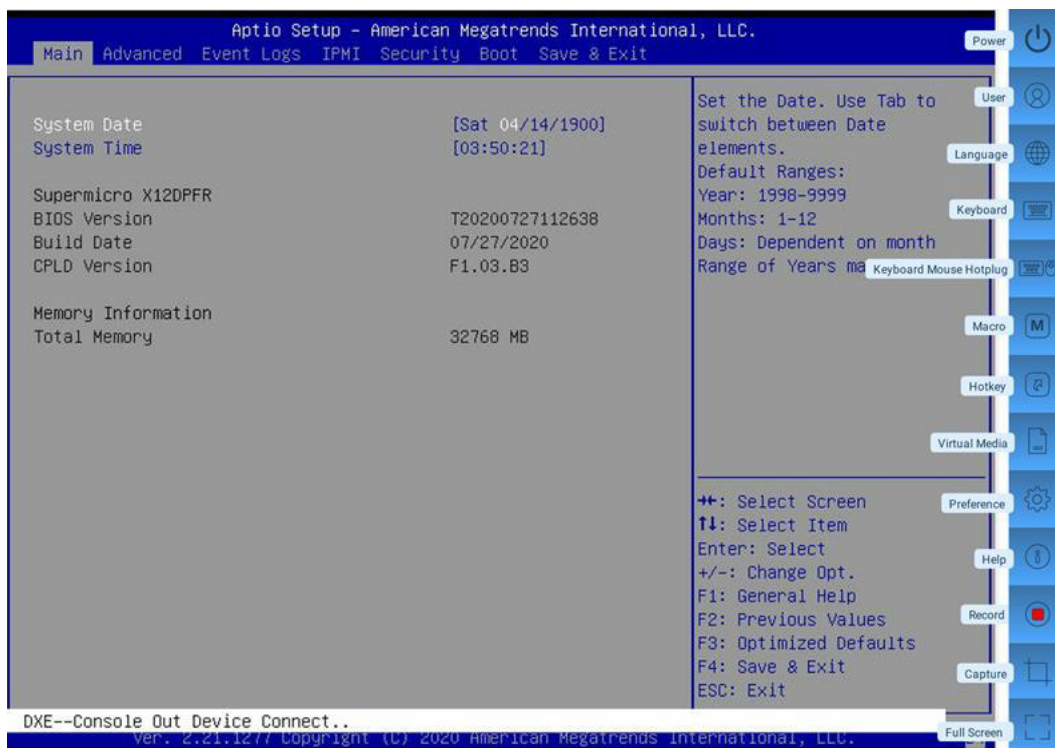
iKVM Reset

If iKVM service is reset, all active iKVM sessions will be disconnected and open iKVM windows will be closed. The following message will be prompted, *“iKVM service has been reset, leading to the closure of all active iKVM windows. Please relaunch iKVM windows to resume your activities.”*



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

Close

Apply

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 operation 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

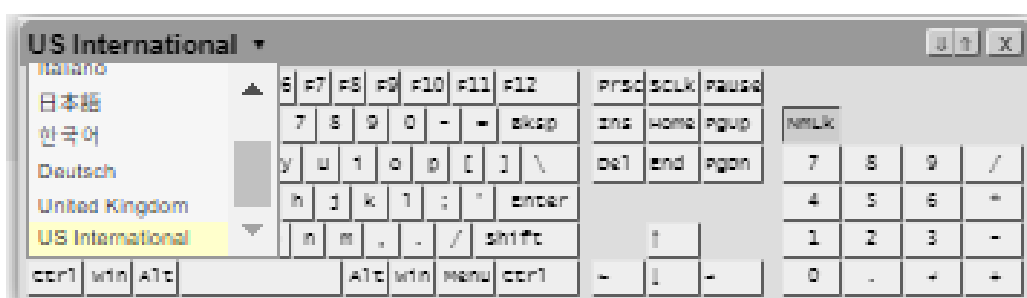
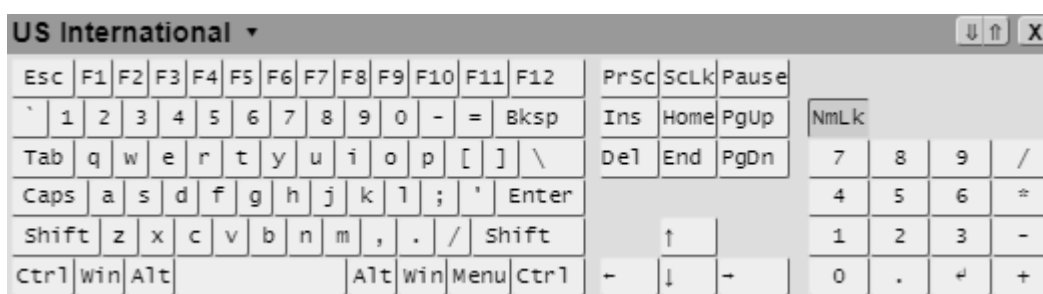
[Close](#)[Apply](#)

- 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 US-international virtual keyboard regardless of any of the supported languages is set. 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

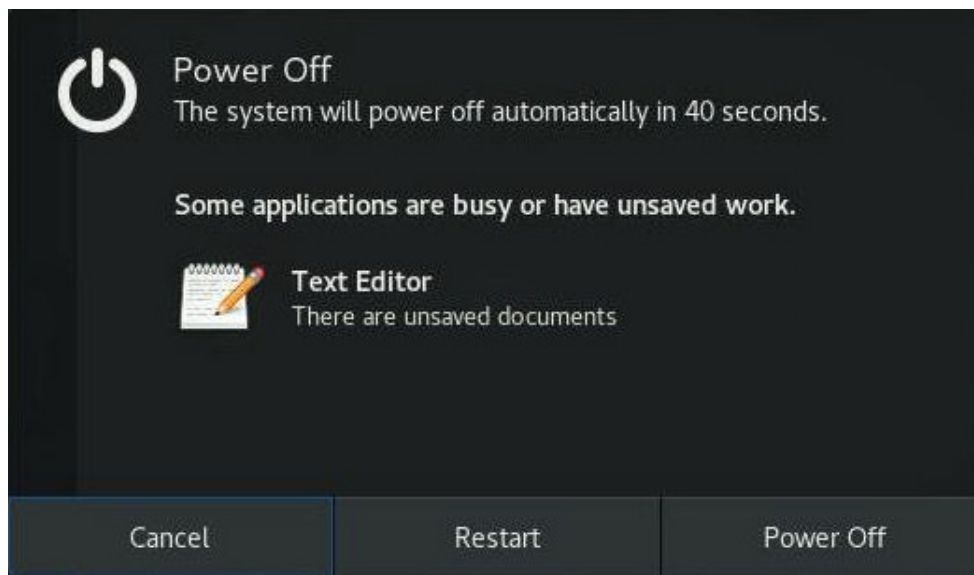
This option allows you to hot-plug the server-side Keyboard and Mouse devices using the Hotplug icon.

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

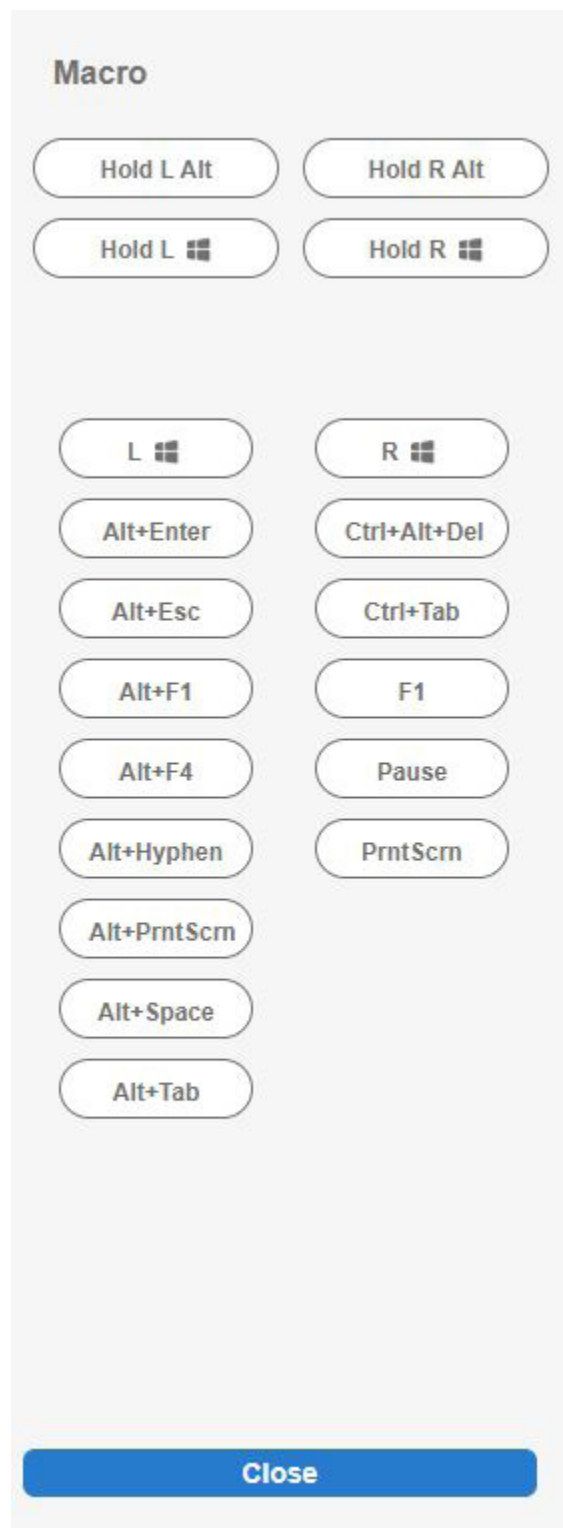
2.7.1f Console Redirection – Macro

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.

Close

Default

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.

Display
Input
Video Stream Control
Record

Display Scale

☐ 60%
 ☐ 70%
 ☐ 80%
 ☐ 90%
 ☒ 100%

Image Quality

☐ Low
 ☒ Medium
 ☐ High

Close

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.

Display
Input
Video Stream Control
Record

Mouse Settings

☒ Absolute Mouse (Windows, Ubuntu, RHEL 6.x and later)

☐ Relative Mouse (Other Linux distributions)

☐ Single Mouse

Close

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 for 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 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

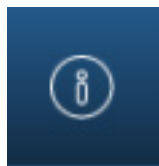
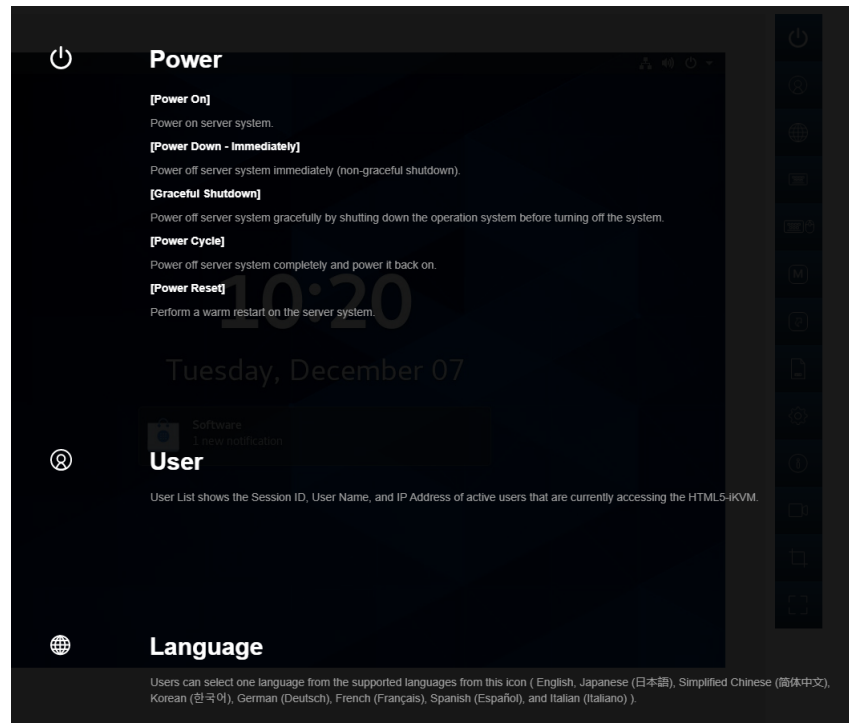
ON Enable auto stop after minute(s)

 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.



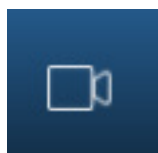
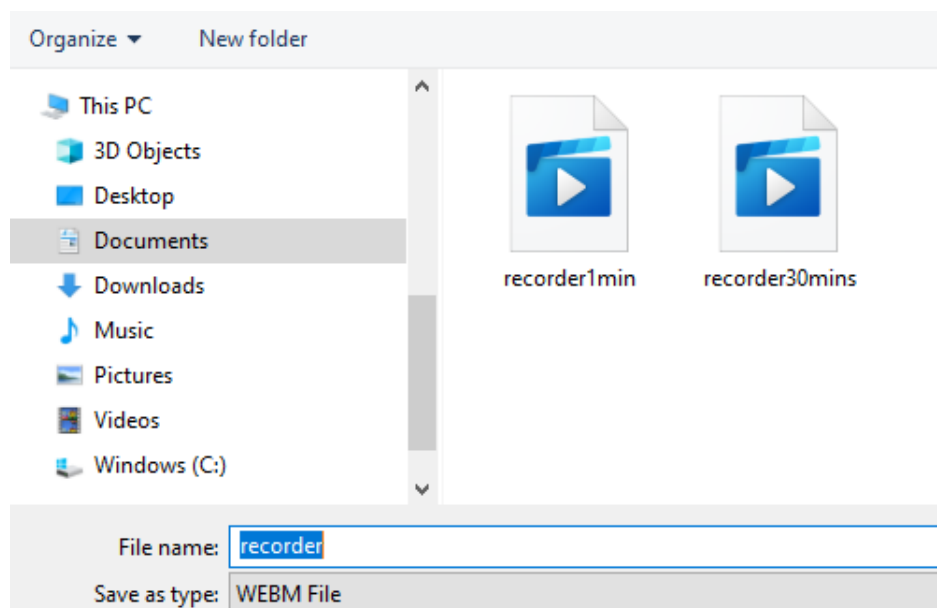
Help Icon

2.7.1k Console Redirection – Record

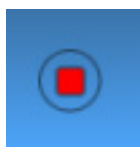
Use this feature to record Video during BIOS booting. After you press the Record button then the Stop button, the recording will be available to be saved as shown below.



Note: Video recording only works with the Chrome browser.



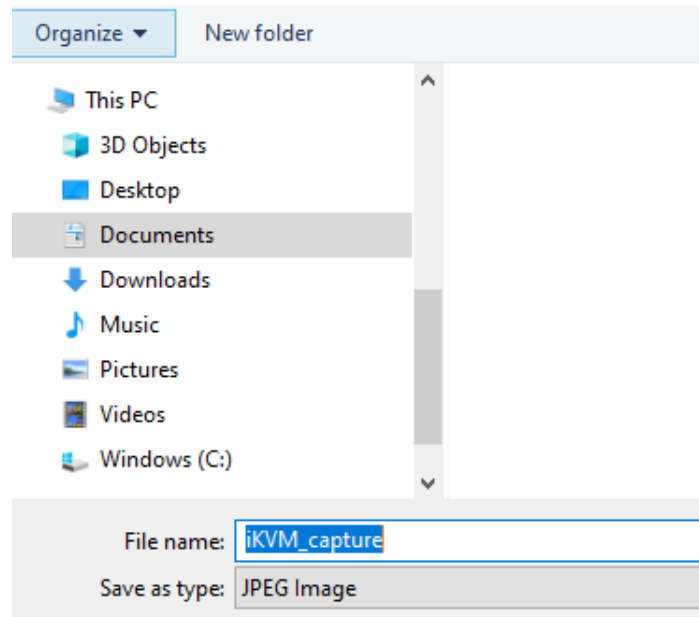
Record Icon



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.



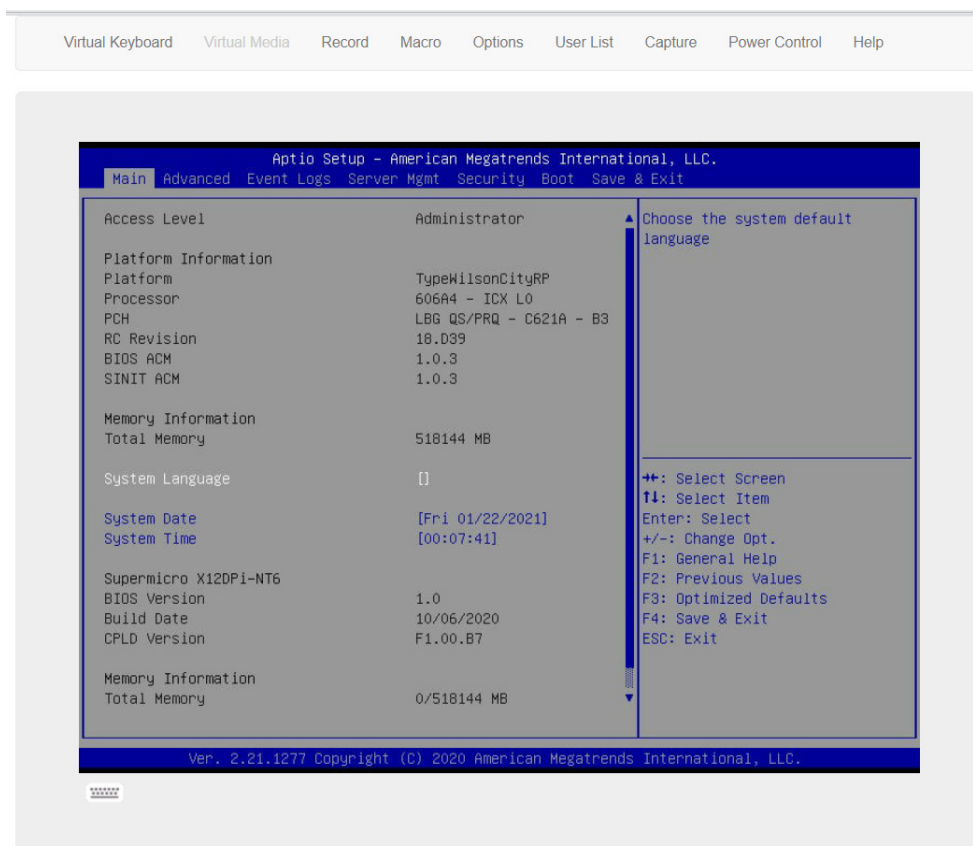
Capture Icon

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.

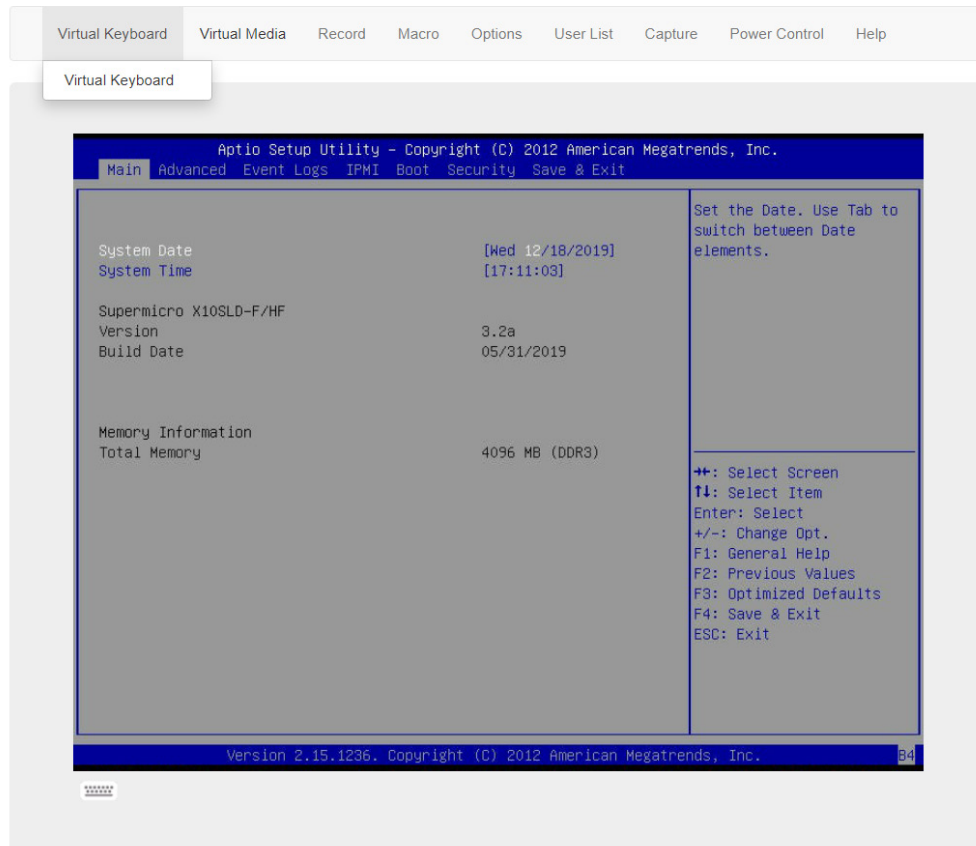
2.7.2 iKVM/HTML5

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.

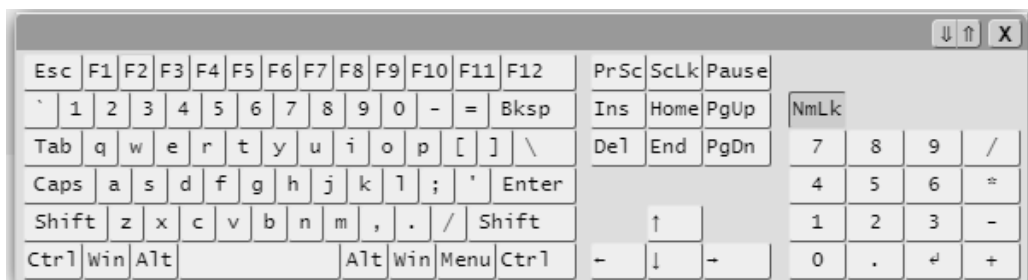


2.7.2a iKVM/HTML5 – Virtual Keyboard

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.

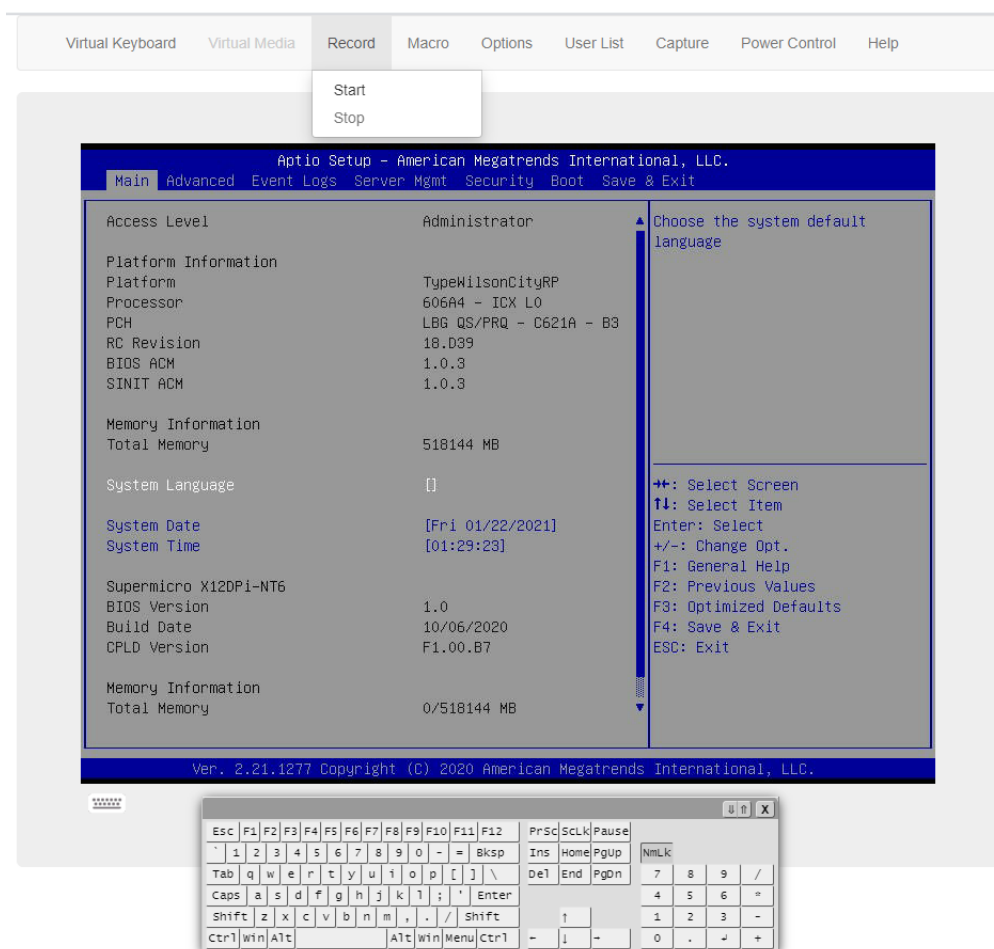
2.7.2c iKVM/HTML5 – Record

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.



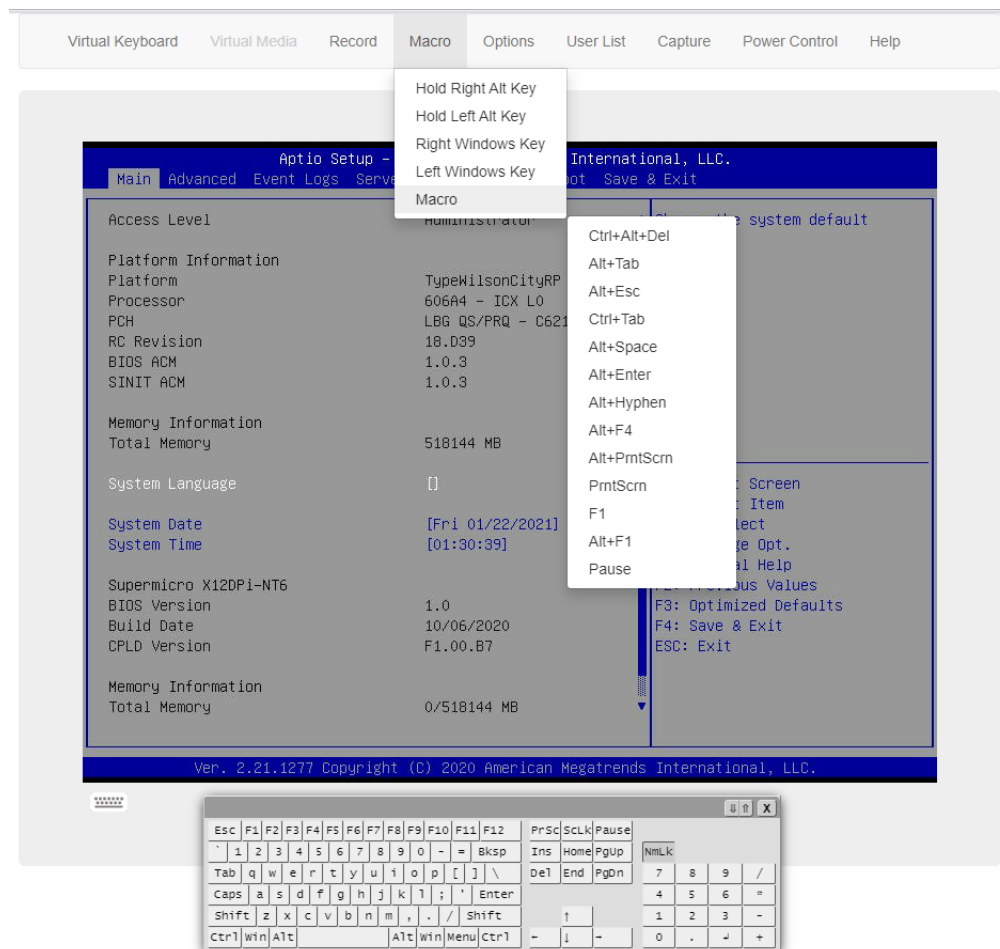
Note: This new HTML5 implementation is currently only supported by the Chrome browser.



2.7.2d iKVM/HTML5 – Macro

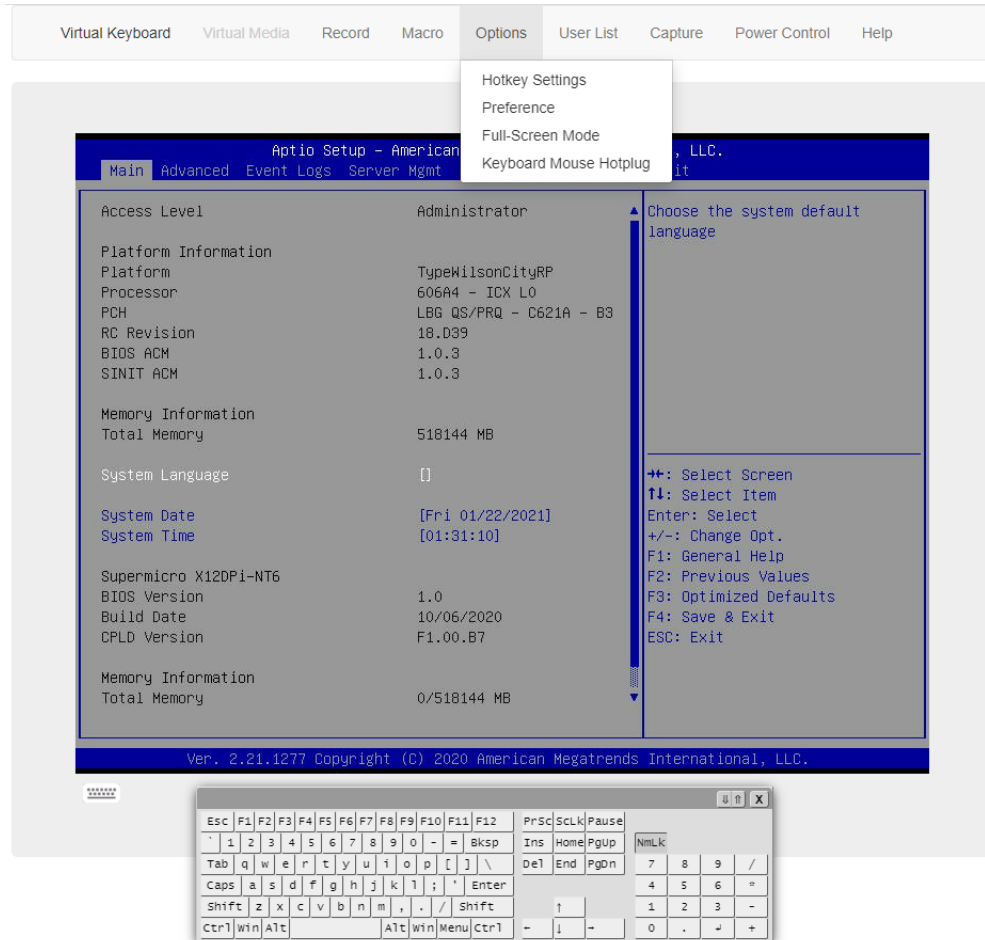
This feature allows you quick access to combo keys.

- 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.

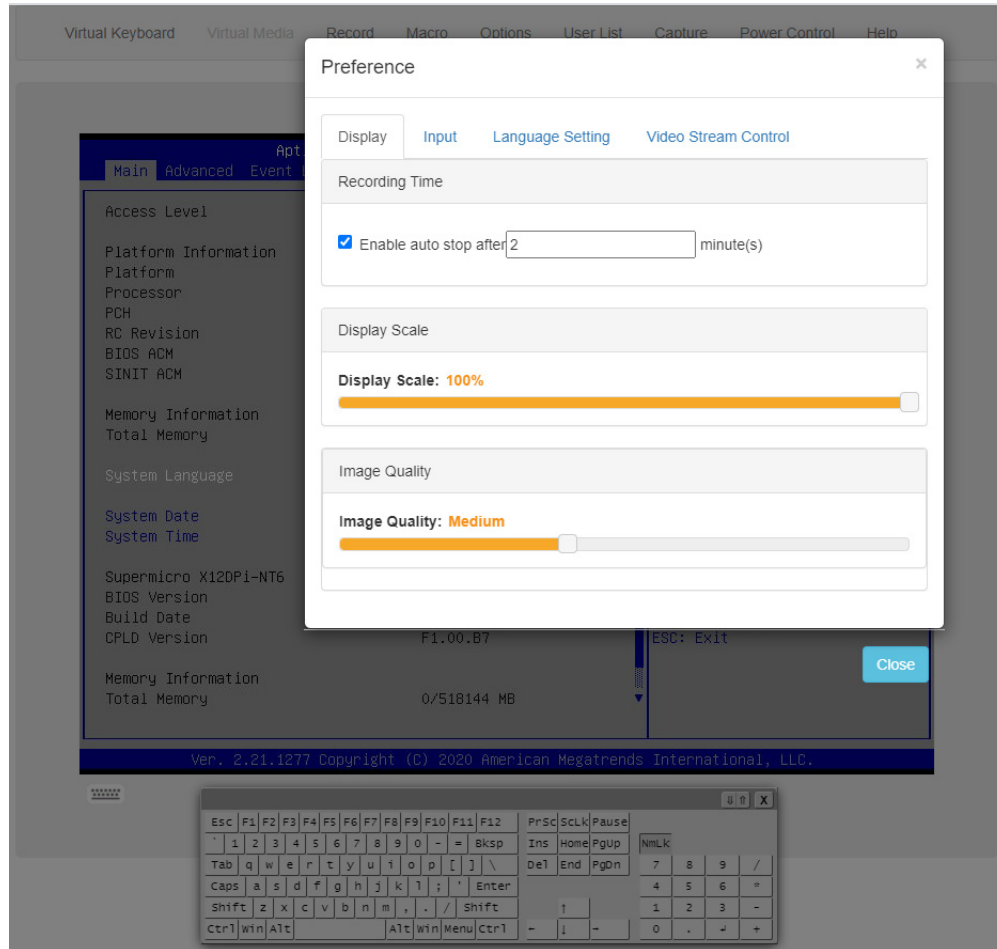
Hotkey Settings

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

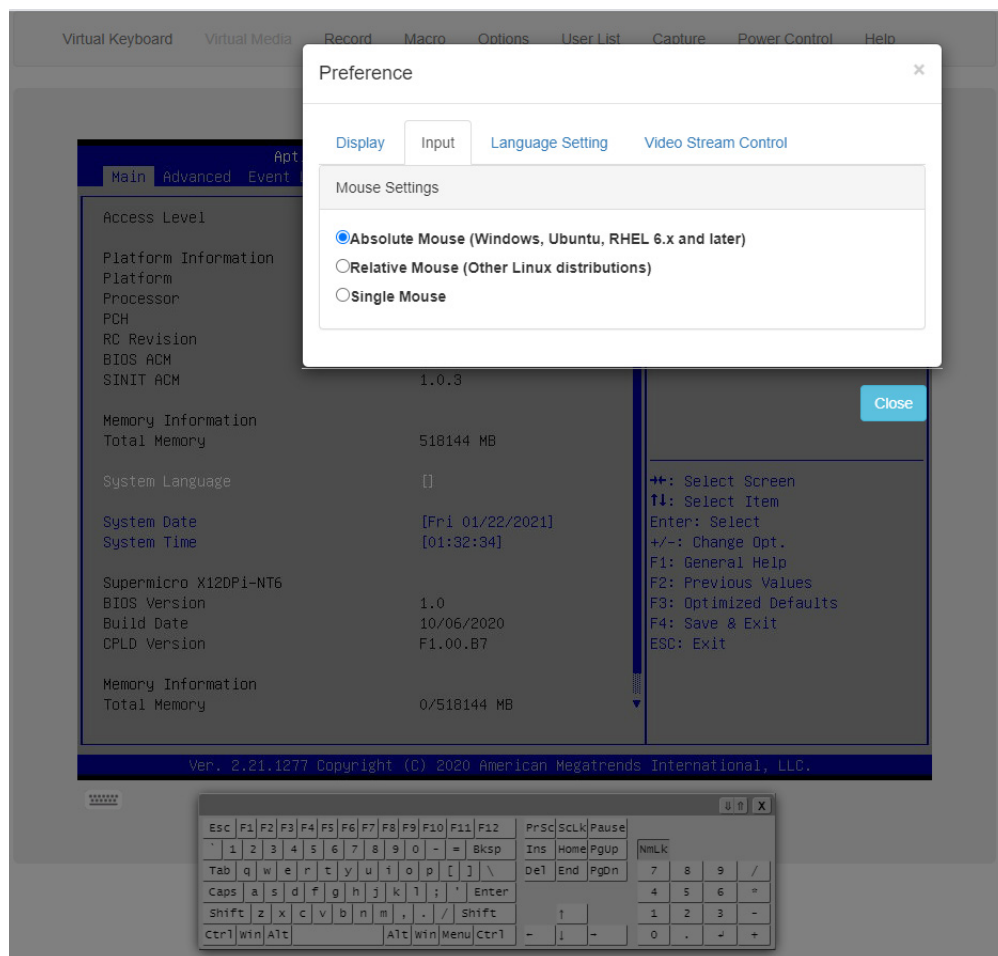
This feature enables auto-stop after n (default: 2) minutes. Adjust the maximum duration of video recordings.



- 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.



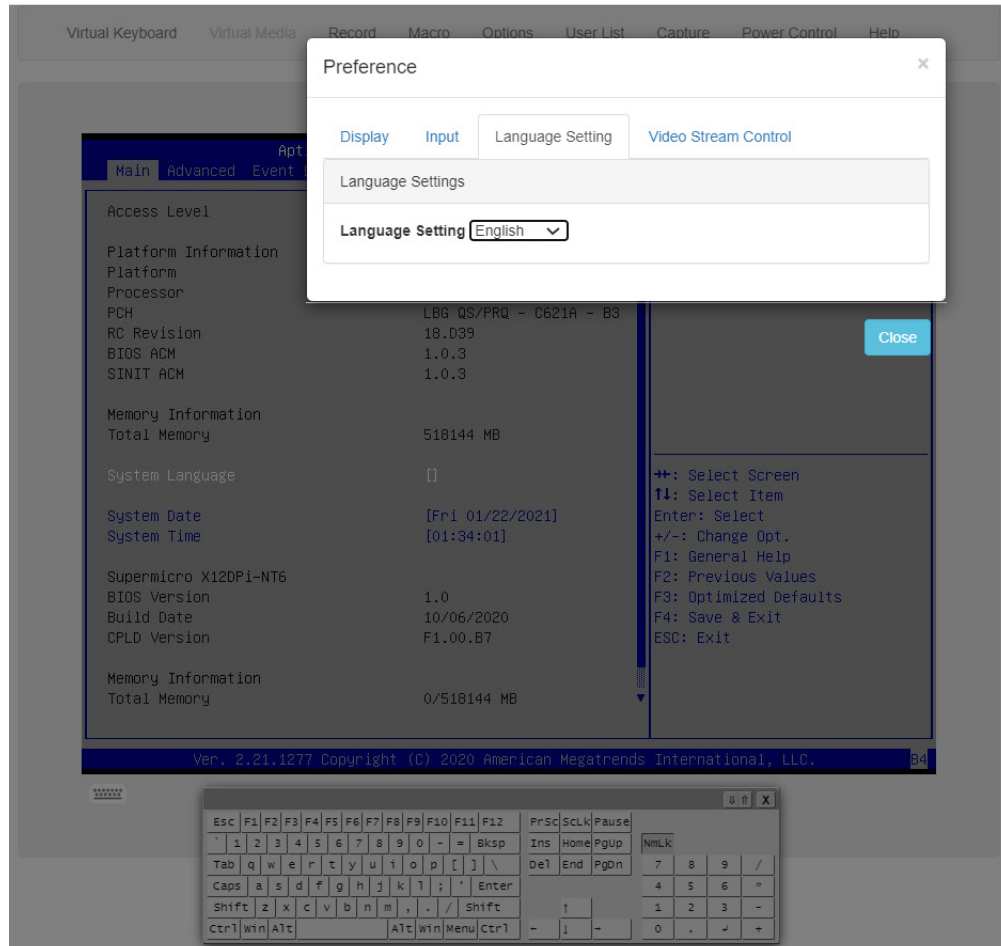
- Absolute Mouse
- Relative Mouse
- Single Mouse



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.

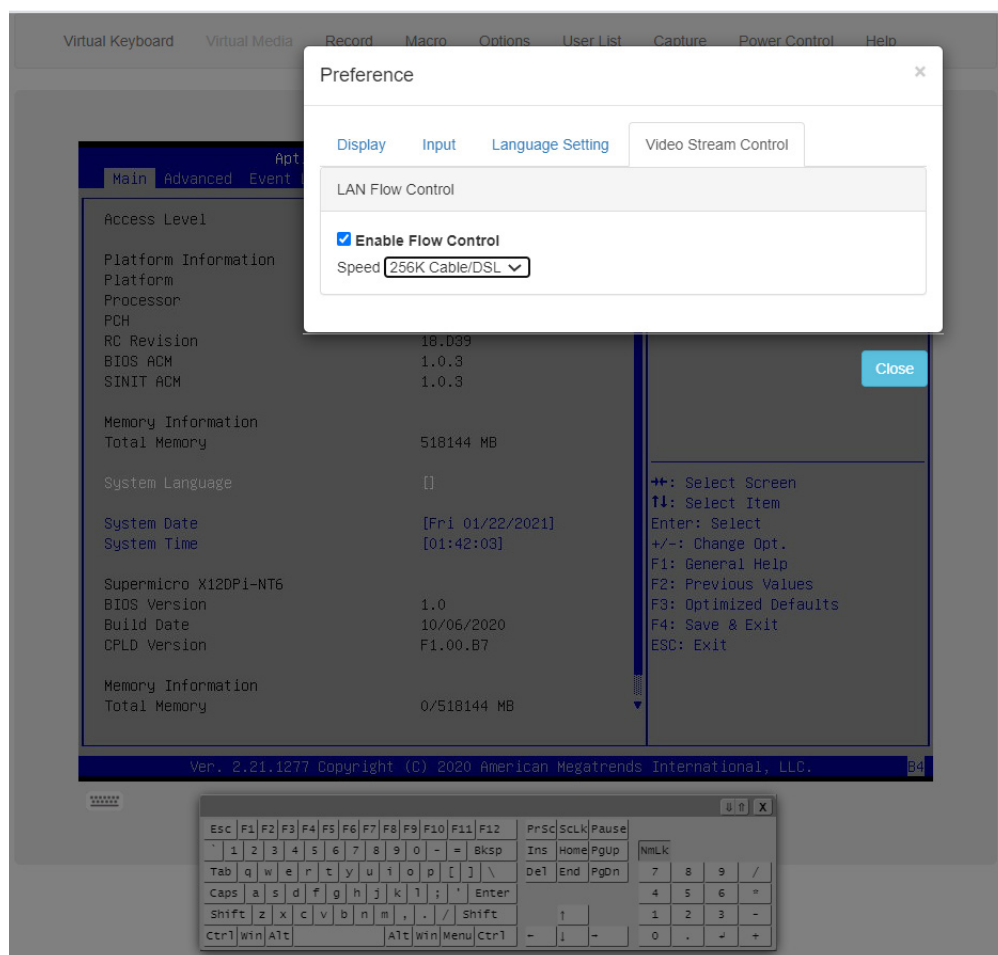


- English
- Japanese
- German
- French
- Spanish
- Italian

Preference – Video Stream Control

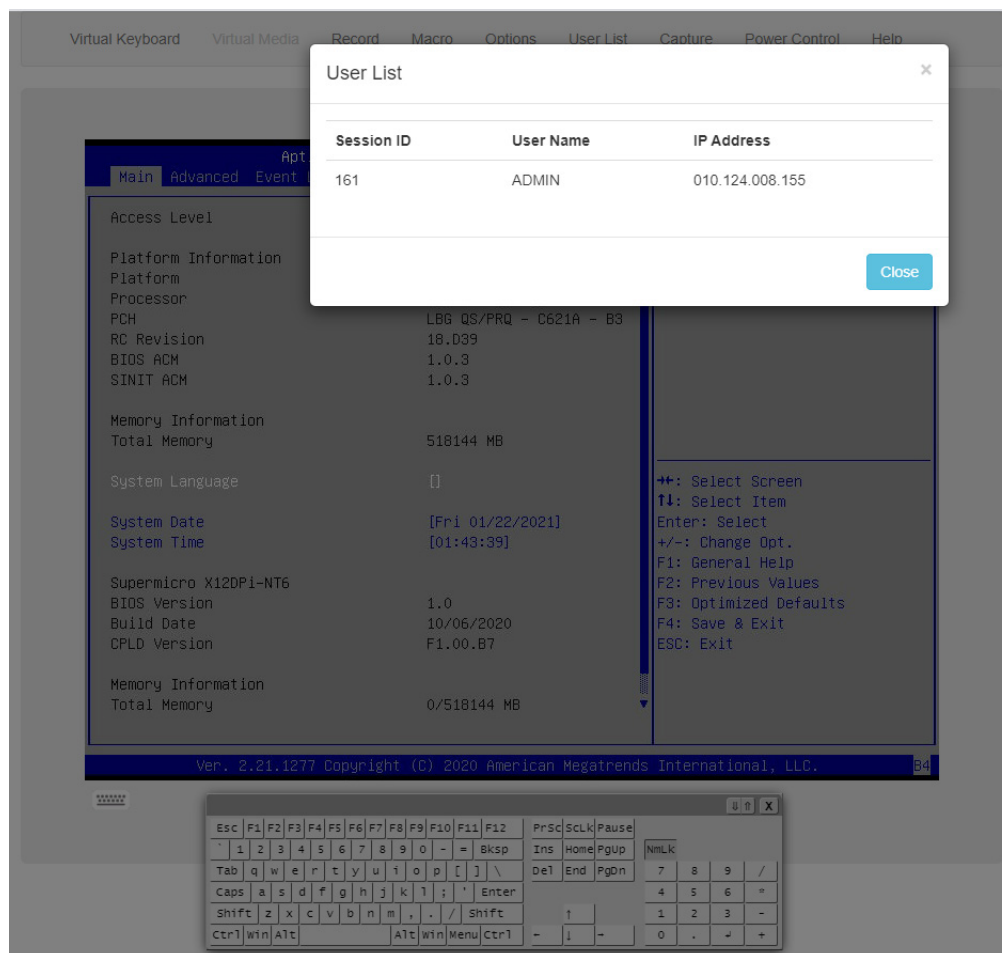
This feature allows you to enable video flow control for LAN Quality of Service (QoS) by selecting one of the following options.

- 256K Cable/DSL
- T1
- T2



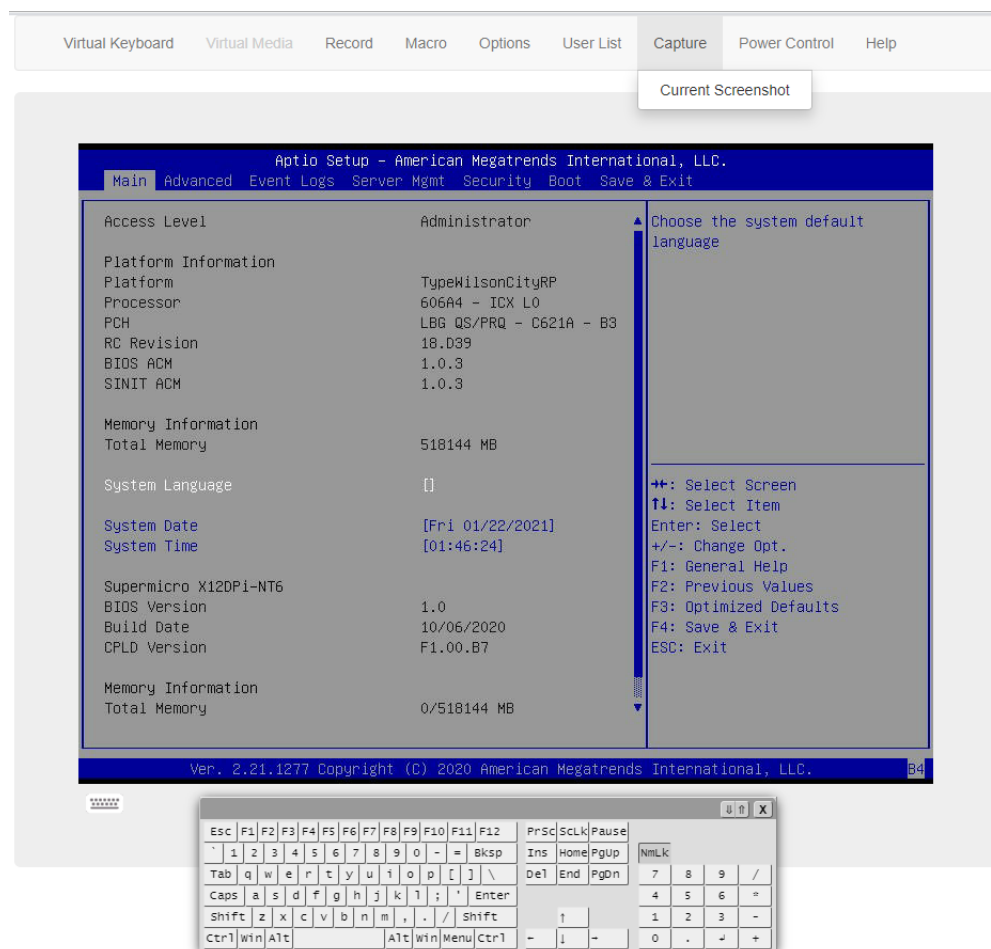
2.7.2f iKVM/HTML5 – User List

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.



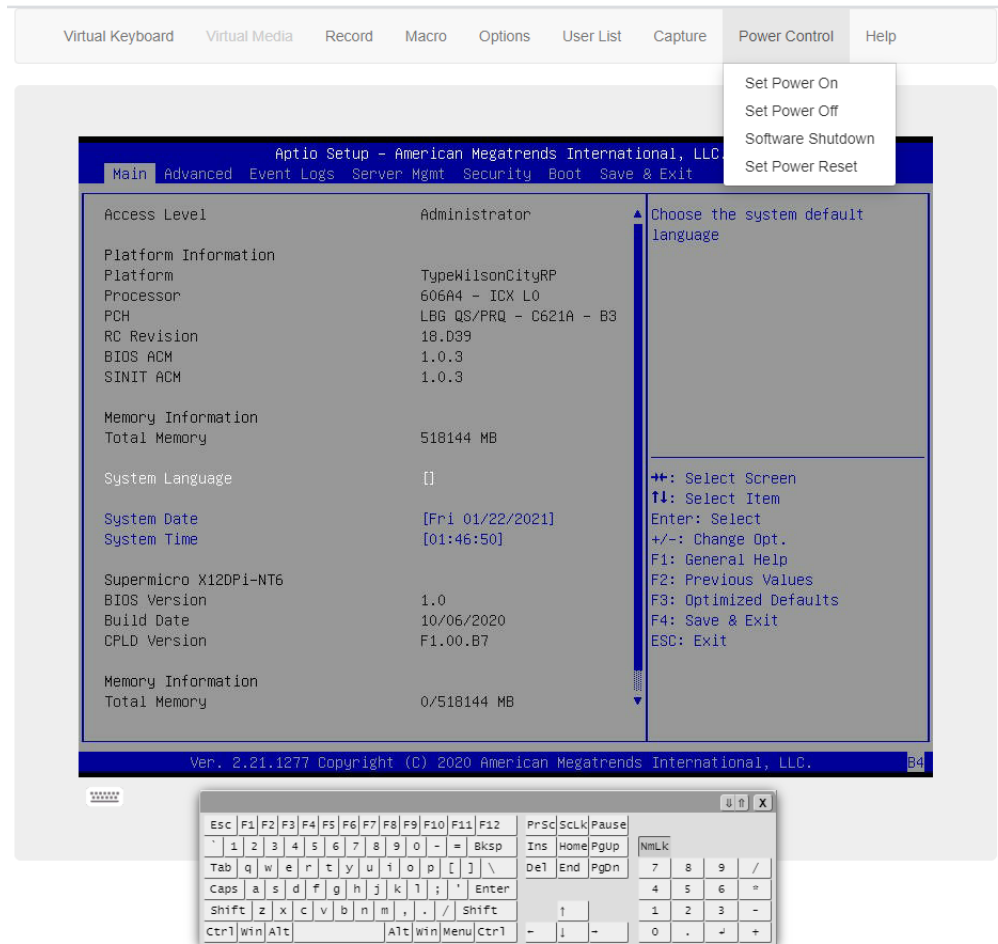
2.7.2g iKVM/HTML5 – Capture

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.



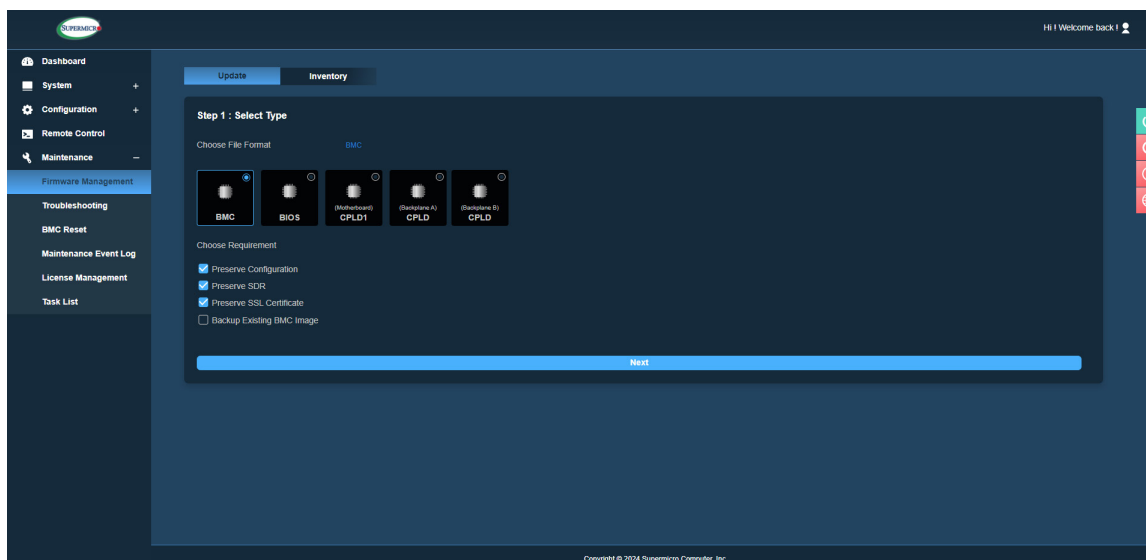
Note: Currently, the number of Maintenance Event Log entries is limited to 4096.

2.8.1. Firmware Management

Firmware management page allows administrators to update firmware for BMC, BIOS, Motherboard CPLD, BackPlane CPLD, network AOC, and 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 firmware 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

This page allows users with administrator privileges to update component firmware. You can view the current and new firmware versions through the Web UI during the update process (BMC, BIOS, etc.). The update typically completes within 5 to 10 minutes.

To update firmware, refer to the following steps:

1. Select a component to update firmware.
2. If applicable, select preserve configuration options.
3. Select a firmware file to upload. If you click **<Upload>** button 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 in the Task List page. Once the firmware is in the update mode, the device will be reset and the server will reboot even if you cancels the firmware updating. 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 a 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: Web Browser / BMC UI of secondary UI (viewing web browser) needs to refresh to renew BMC connection since viewing web browser has stopped sending request after FW update was initiated. A message for users to wait for BMC will be *"BMC is restarting to continue the BMC firmware update process. To prevent data loss, please Do Not Remove power source until BMC is back online!"*

To update BMC firmware, go to Update tab from Firmware Management to select radio button for BMC. You can select available options to preserve.

BMC update supports the following preserve configuration options.

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


To update the BIOS firmware, navigate to the **<Update>** tab within the Firmware Management section. Here, you can choose the appropriate radio button for the BIOS option. You have the flexibility to select either **Next-boot Update** or **Immediate Update** modes, which would allow you to schedule when the BIOS firmware will undergo an update.

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

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

BIOS update supports the following preserve configuration options for all X12 platforms except Tatlow platforms (i.e., X12STH-LN4F, X12STL-F, etc.).

- Preserve SMBIOS
- Preserve BIOS Boot Options Configuration
- Backup existing BIOS image

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

The following preserve configuration options for Tatlow platforms (i.e., X12STH-LN4F, X12STL-F, etc.).

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



Note 1: Select the **Backup existing image** option to backup exiting BMC or BIOS image. Backup image will be used for auto recovery in case of failed integrity at any time. Users can also manually recover BMC or BIOS from backup image. Go to Inventory tab to manually recover BMC or BIOS. Non-ROT platforms will not display the **Backup existing image** option.

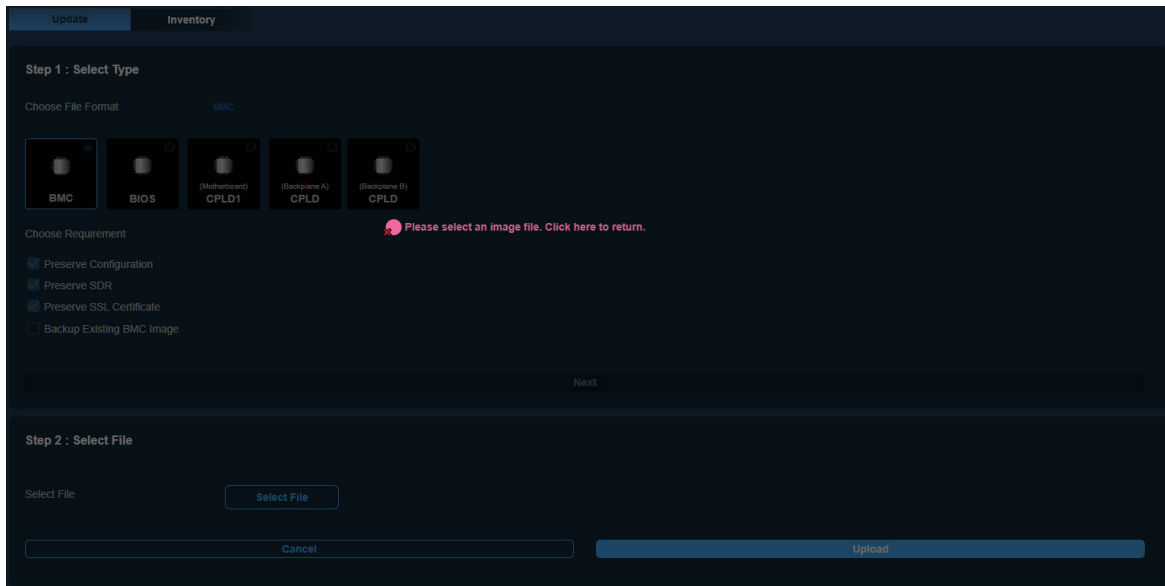
Note 2: Due to limitation of current BMC implementation, when updating firmware, users might experience a long time to refresh the web browser after update is completed. You might also see the rebooting message for a minute or two when logging back in before updating is completed.

How BMC Firmware is Updated

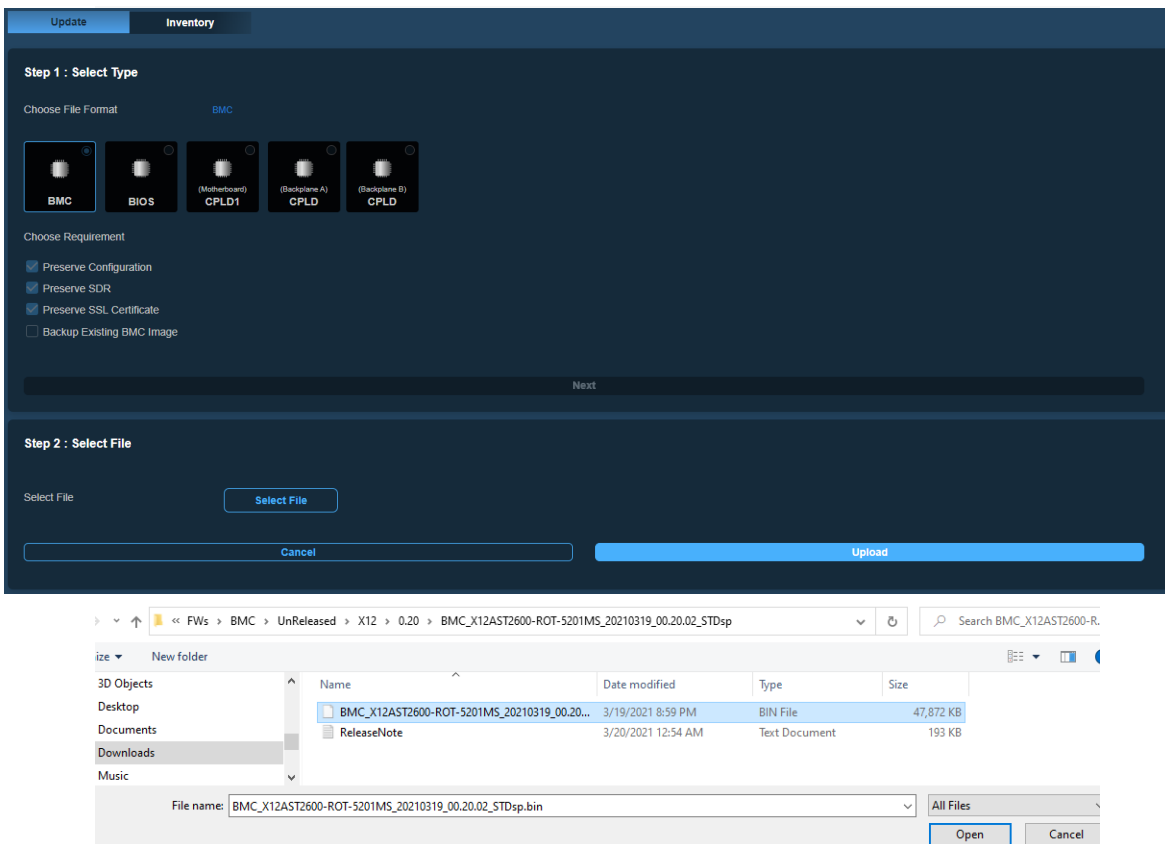
The screenshot shows the 'Update' tab in the Super BMC interface. Under 'Step 1 : Select Type', there are two sections: 'Choose File Format' and 'Choose Requirement'. In 'Choose File Format', the 'BMC' option is selected with a plus icon, while 'BIOS', '(Motherboard) CPLD1', '(Backplane A) CPLD', and '(Backplane B) CPLD' are deselected with minus icons. In 'Choose Requirement', the checkboxes for 'Preserve Configuration', 'Preserve SDR', and 'Preserve SSL Certificate' are all checked, while 'Backup Existing BMC Image' is unchecked. A blue 'Next' button is at the bottom right.

This screenshot shows the same interface as the previous one, but with 'Step 2 : Select File' active. The 'Next' button from Step 1 is now disabled and greyed out. In Step 2, there is a 'Select File' button. Below it, there are two buttons: 'Cancel' and 'Upload'. The 'Upload' button is highlighted in blue, indicating it is the primary action.

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



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



UpdateInventory

Step 1 : Select Type

Choose File Format

BMC

BMC

BIOS

CPLD

PMem

NIC1

SAS3808

SAS3816

Choose Requirement

☒ Preserve Configuration
 ☒ Preserve SDR
 ☒ Preserve SSL Certificate
 ☐ Backup Existing BMC Image

Next

Step 2 : Select File

Select File

Select File

BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp.bin

46.75 MB

×

Cancel

Upload

UpdateInventory

Step 1 : Select Type

Choose File Format

BMC

BMC

BIOS

CPLD

PMem

NIC1

SAS3808

SAS3816

Choose Requirement

☒ Preserve Configuration
 ☒ Preserve SDR
 ☒ Preserve SSL Certificate
 ☐ Backup Existing BMC Image

Next

Step 2 : Select File

Select File

Select File


BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp.bin

46.75 MB

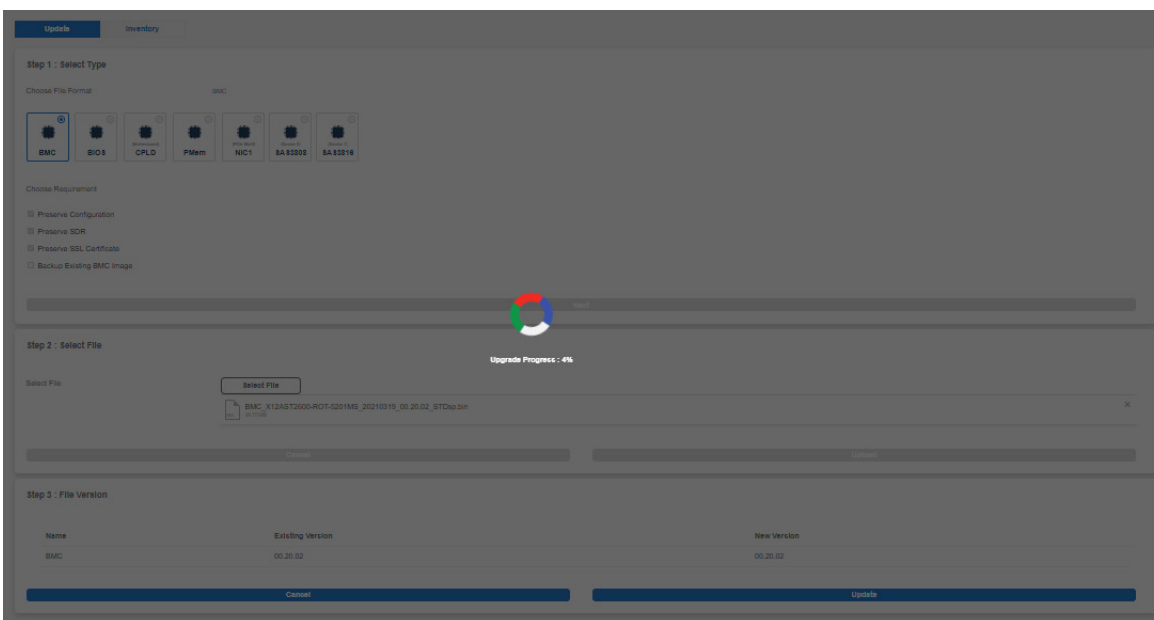
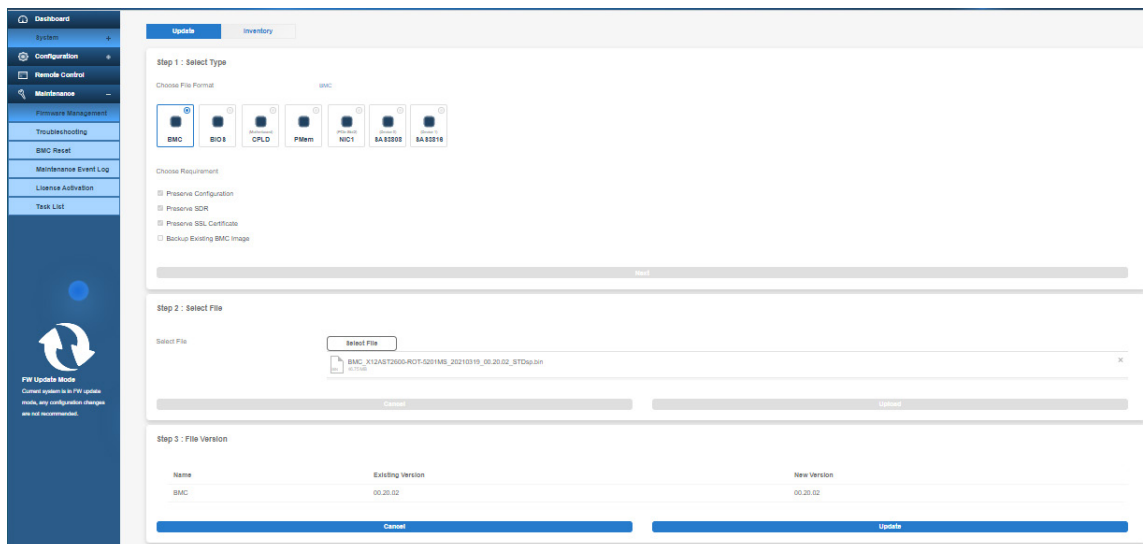
×

Cancel

Upload

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

160



Update

Inventory

Step 1 : Select Type

Choose File Format

BMC

BIO S

CPUD

PMem

NIC1

SA S2008

SA S2018

Choose Requirement

☐ Preserve Configuration

☐ Preserve SDR

☐ Preserve SSL Certificate

☐ Backup Existing BMC Image

Upgrade Progress : 70%

Step 2 : Select File

Select File

BMC_X12AS72008-ROTY-0201MS_20210319_00.20.02_STDep.bin

Cancel

Upload

Step 3 : File Version

Name	Existing Version	New Version
BMC	00.20.02	00.20.02

Cancel

Update

Update

Inventory

Step 1 : Select Type

Choose File Format

BMC

BIO S

CPUD

PMem

NIC1

SA S2008

SA S2018

Choose Requirement

☐ Preserve Configuration

☐ Preserve SDR

☐ Preserve SSL Certificate

☐ Backup Existing BMC Image

Upgrade Progress : 100%

Step 2 : Select File

Select File

BMC_X12AS72008-ROTY-0201MS_20210319_00.20.02_STDep.bin

Cancel

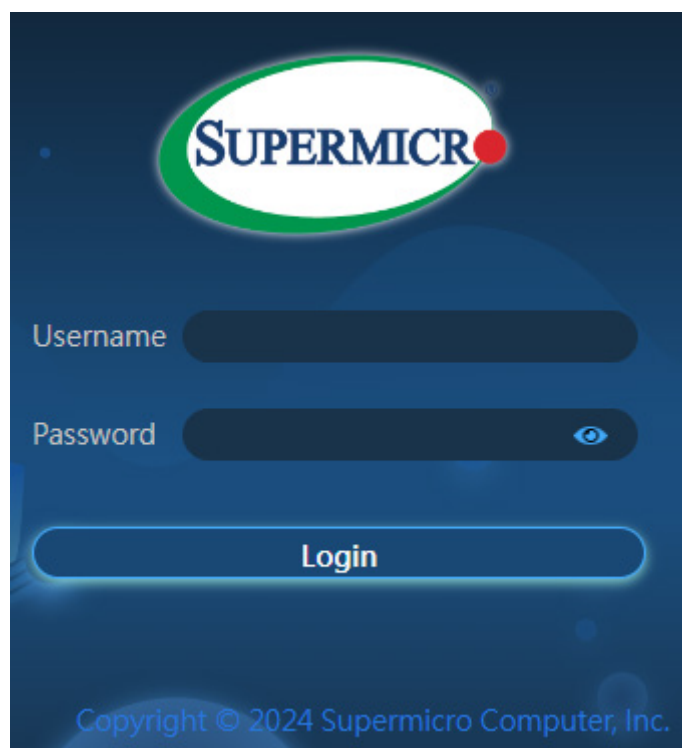
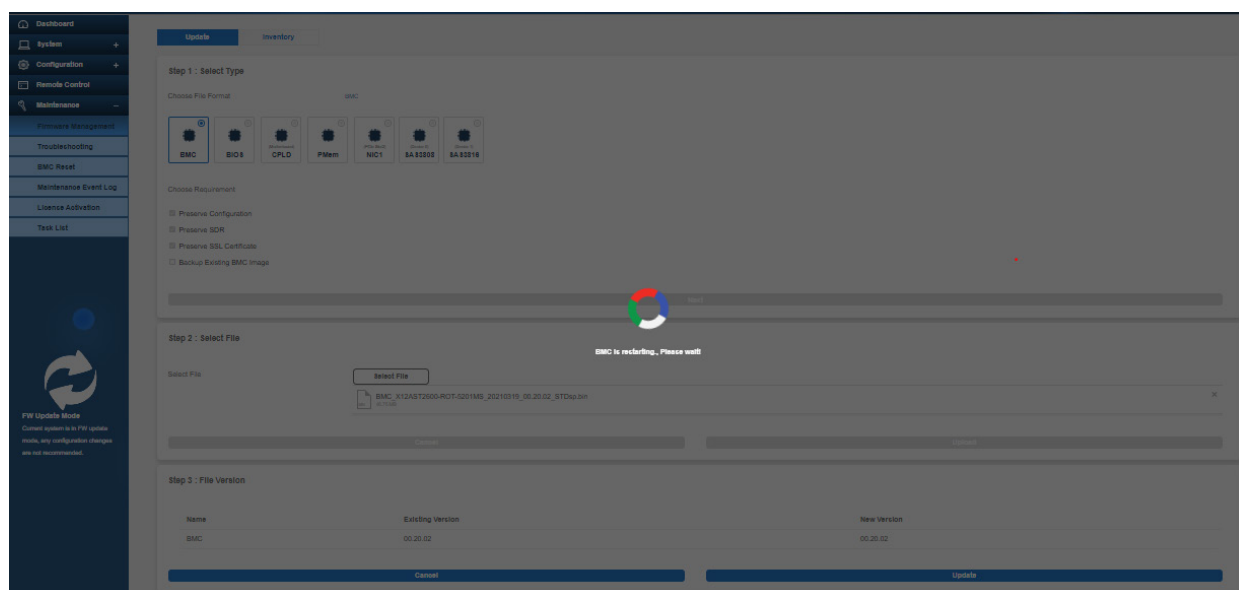
Upload

Step 3 : File Version

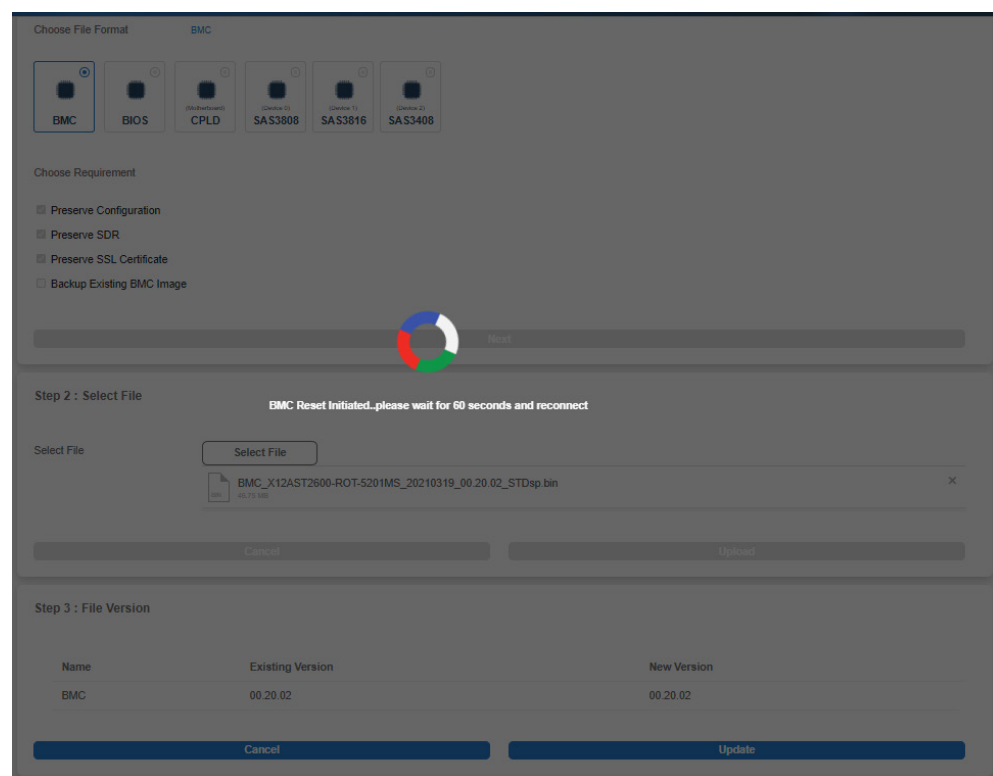
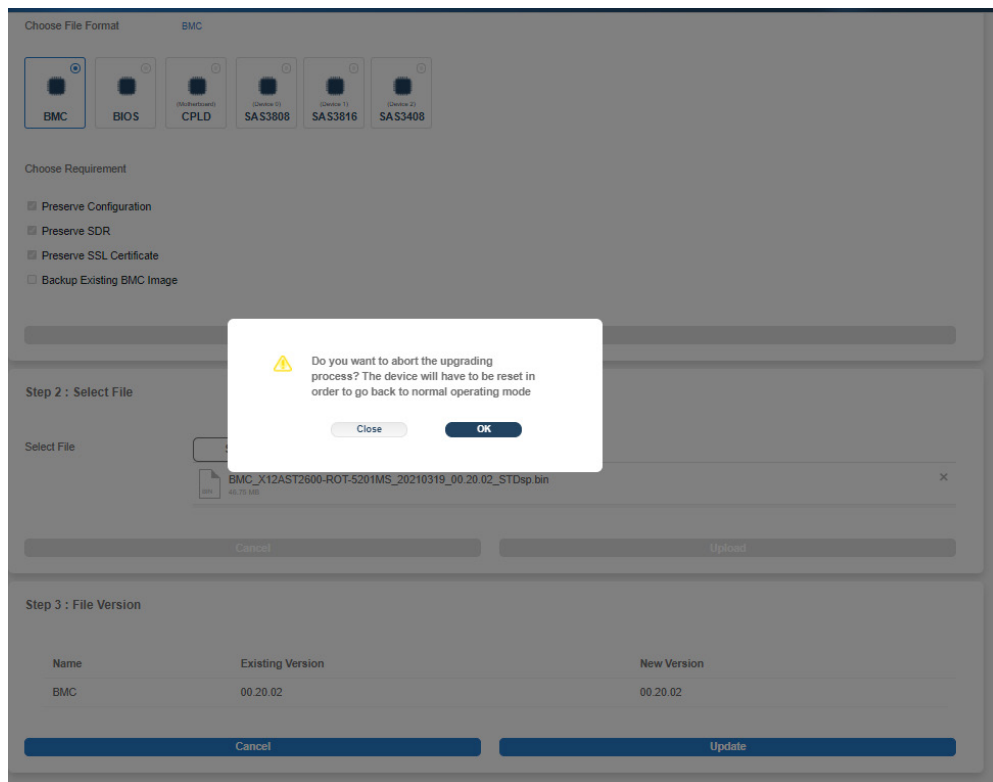
Name	Existing Version	New Version
BMC	00.20.02	00.20.02

Cancel

Update



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!”*



How BIOS Firmware is Updated

Update Inventory

Step 1 : Select Type

Choose File Format BMC

☒ BMC ☐ BIOS ☐ (Motherboard) CPLD1 ☐ (Backplane A) CPLD ☐ (Backplane B) CPLD

Choose Requirement

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

Next

Update Inventory

Step 1 : Select Type

Choose File Format BIOS

☐ BMC ☒ BIOS ☐ (Motherboard) CPLD1 ☐ (Backplane A) CPLD ☐ (Backplane B) CPLD

Choose Update Time

☒ Next-boot Update ☐ Immediate Update

Choose Requirement

- ☒ Preserve SMBIOS
- ☐ Backup Existing BIOS Image
- ☒ Preserve OA
- ☒ Preserve BIOS Setup Configuration
- ☒ Preserve BIOS Setup Password
- ☒ Preserve BIOS Secure Boot Keys
- ☒ Preserve BIOS Boot Options Configuration

Next

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

(Wharfoord) CPLD1

(Backplane A) CPLD

(Backplane B) CPLD

Choose Update Time

Next-boot Update

Immediate Update

Choose Requirement

Preserve SMBIOS

Backup Existing BIOS Image

Preserve OA

Preserve BIOS Setup Configuration

Preserve BIOS Setup Password

Preserve BIOS Secure Boot Keys

Preserve BIOS Boot Options Configuration

Next

Step 2 : Select File

Select File

Select File

Cancel

Upload

Step 2 : Select File

Select File

Select File

Cancel

Upload

Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 01/25/2024 Ver 1.6b	BIOS Date: 04/25/2024 Ver 1.9

Abort Update

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD (Multibootable)

PMem

SAS3808 (Device ID)

SAS3816 (Device ID)

Choose Requirement

☐ Preserve NVRAM

☒ Preserve SMBIOS

☐ Backup Existing BIOS Image

Next

Step 2 : Select File

Select File

Select File

BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin

32.00 MB

X

Cancel

Upload

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD (Multibootable)

PMem

SAS3808 (Device ID)

SAS3816 (Device ID)

Choose Requirement

☐ Preserve NVRAM

☒ Preserve SMBIOS

☐ Backup Existing BIOS Image

Please power off the system before executing BIOS update.

Close

Power Off

Next

Step 2 : Select File

Select File

Select File

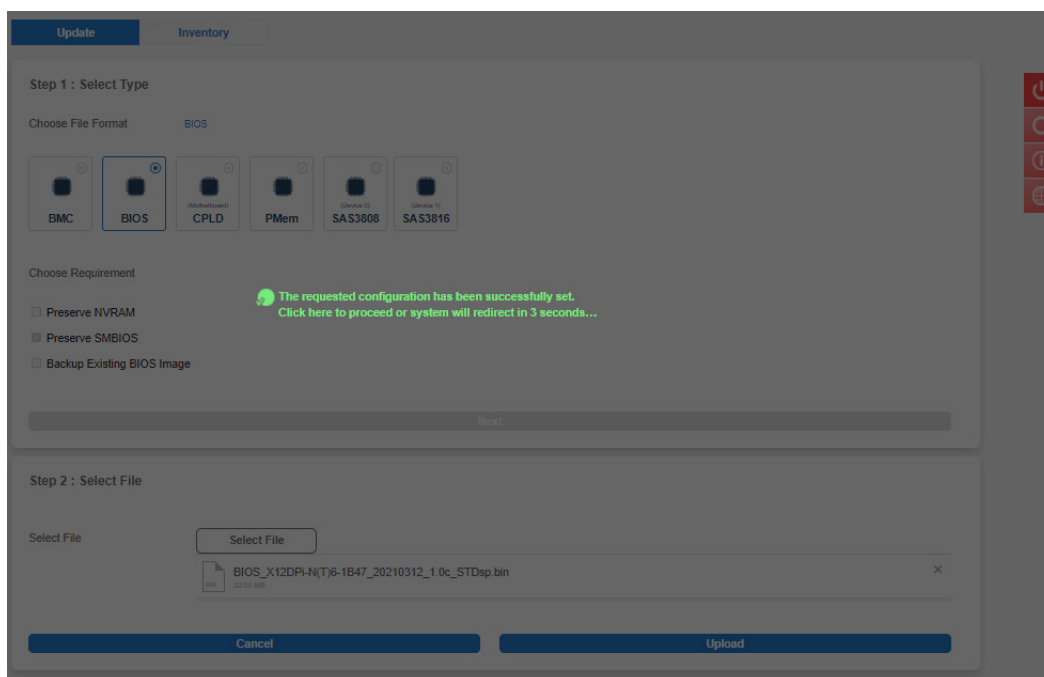
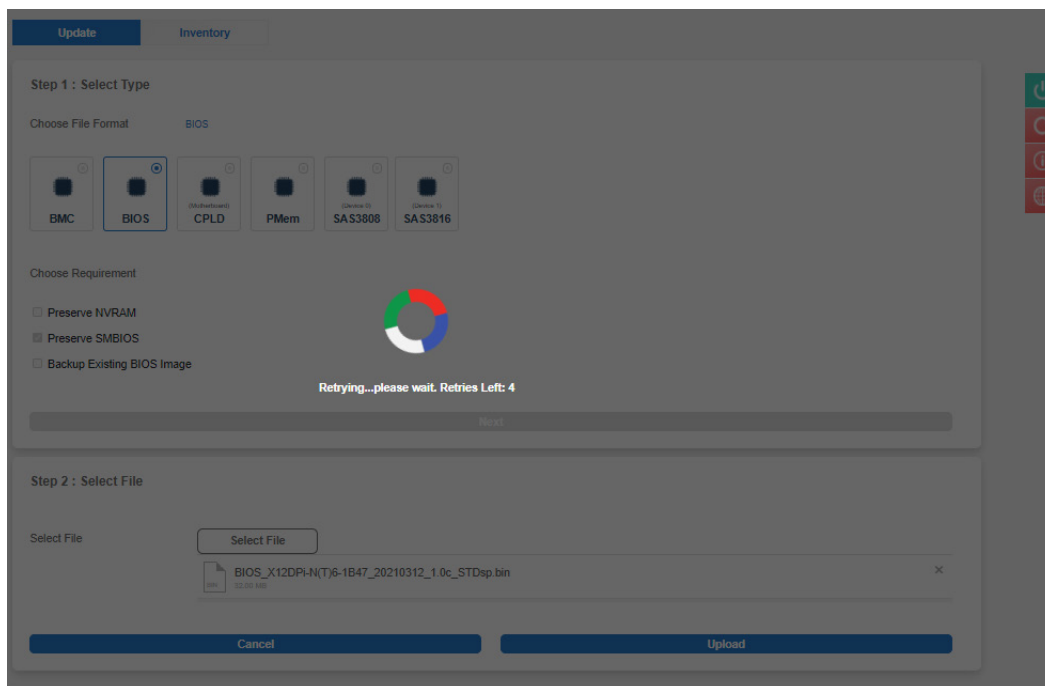
BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin

32.00 MB

X

Cancel

Upload



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

The screenshot shows the 'Update' tab in the BMC settings. Under 'Step 1: Select Type', the 'BIOS' option is selected. Below this, there are checkboxes for 'Preserve NVRAM', 'Preserve SMBIOS', and 'Backup Existing BIOS Image'. A red error message is displayed: 'Please select an image file. Click here to return.' At the bottom, there are 'Cancel' and 'Upload' buttons.

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

The screenshot shows the 'Update' tab in the BMC settings. Under 'Step 1: Select Type', the 'BIOS' option is selected. Below this, there are checkboxes for 'Preserve NVRAM', 'Preserve SMBIOS', and 'Backup Existing BIOS Image'. A progress bar shows 'Upgrade Progress: 0%'. Under 'Step 2: Select File', a file named 'BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin' is selected. At the bottom, there are 'Cancel' and 'Update' buttons.

Name	Existing Version	New Version
BIOS	BIOS Date: 01/27/2021 Ver 1.0b	BIOS Date: 03/12/2021 Ver 1.0c

UpdateInventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD (Microcontroller)

PMem

SAS3808 (Device ID)

SAS3816 (Device ID)

Choose Requirement

☐ Preserve NVRAM
 ☒ Preserve SMBIOS
 ☐ Backup Existing BIOS Image

Upgrade Progress : 16%

Step 2 : Select File

Select File

BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin

22.3M 100

Cancel

Upload

Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 01/27/2021 Ver 1.0b	BIOS Date: 03/12/2021 Ver 1.0c

Cancel

Update

UpdateInventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD (Microcontroller)

PMem

SAS3808 (Device ID)

SAS3816 (Device ID)

Choose Requirement

☐ Preserve NVRAM
 ☒ Preserve SMBIOS
 ☐ Backup Existing BIOS Image

Upload Firmware : 40%

Step 2 : Select File

Select File

BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin

22.3M 100

Cancel

Upload

170

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

Refurbished CPLD1

Refurbished CPLD

Refurbished CPLD

Choose Update Time

Next-boot Update

Immediate Update

Choose Requirement

☒ Preserve SMBIOS

☐ Backup Existing BIOS Image

☒ Preserve DA

☒ Preserve BIOS Setup Configuration

☒ Preserve BIOS Setup Password

☒ Preserve BIOS Secure Boot Keys

☒ Preserve BIOS Boot Options Configuration

Next

Step 2 : Select File

Select File

Select File

Cancel

Upload

Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 01/25/2024 Ver 1.0a	BIOS Date: 04/25/2024 Ver 1.0

Next

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

Refurbished CPLD

PMem

SAS3808

SAS3816

Choose Requirement

☐ Preserve NVRAM

☒ Preserve SMBIOS

☐ Backup Existing BIOS Image

Upgrade Progress : 0%

Next

Step 2 : Select File

Select File

Select File

BIOS_X12DPL-N(T)6-1B47_20210312_1.0c_STDsp.bin

Cancel

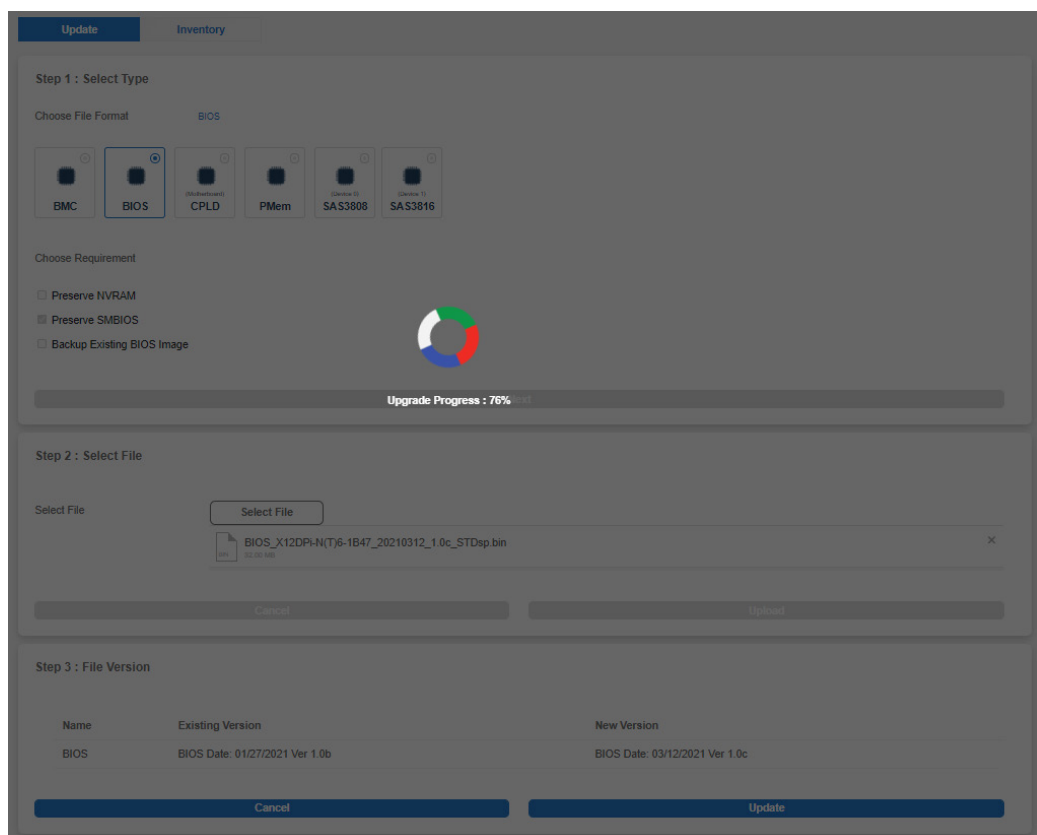
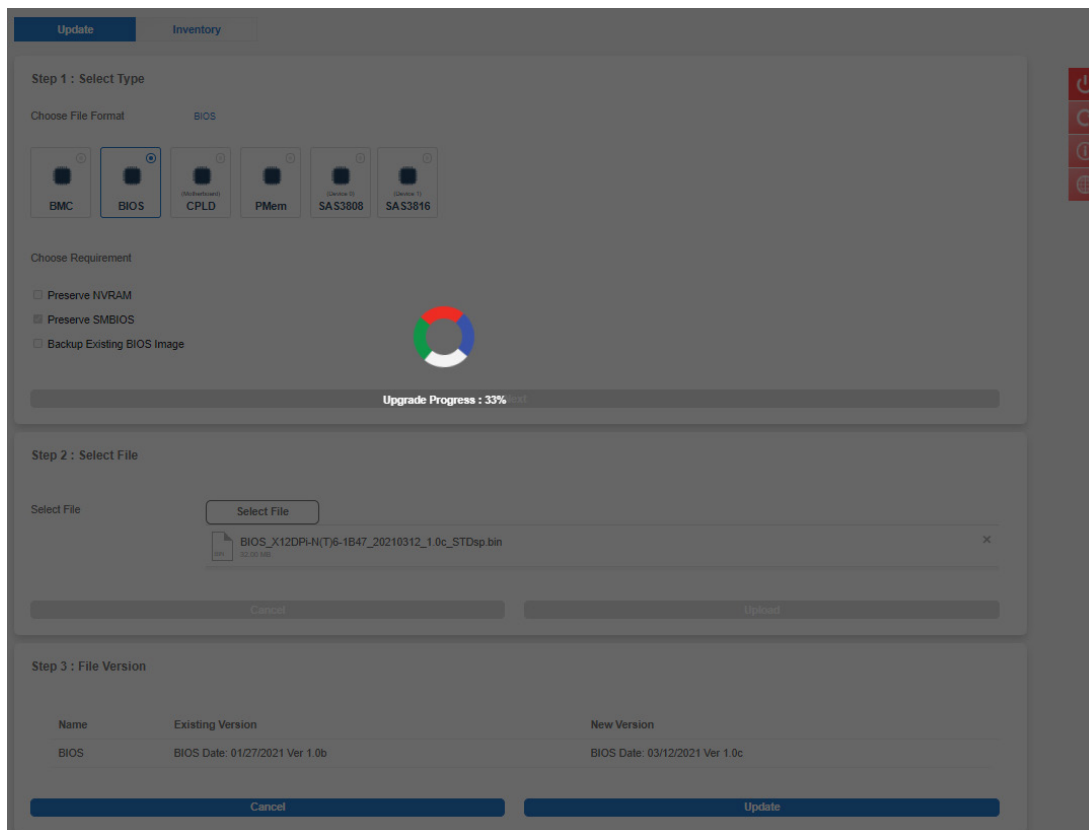
Upload

Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 01/27/2021 Ver 1.0b	BIOS Date: 03/12/2021 Ver 1.0c

Cancel

Update



Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD

PMem

SAS3808

SAS3816

Choose Requirement

☐ Preserve NVRAM

☐ Preserve SMBIOS

☐ Backup Existing BIOS Image

Upgrade Progress : 100%

Step 2 : Select File

Select File

BIOS_X12DPH-N(T)6-1B47_20210312_1.0c_STDsp bin

Cancel

Upload

Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 01/27/2021 Ver 1.0b	BIOS Date: 03/12/2021 Ver 1.0c

Cancel

Update

Dashboard

System

Configuration

Remote Control

Maintenance

Firmware Management

Troubleshooting

BMC Reset

Maintenance Event Log

License Activation

Task List

FW Update Mode

Current system is in FW update mode, any configuration changes are not recommended.

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD

PMem

SAS3808

SAS3816

Choose Requirement

☐ Preserve NVRAM

☐ Preserve SMBIOS

☐ Backup Existing BIOS Image

Upgrade Progress : 100%

Step 2 : Select File

Select File

BIOS_X12DPH-N(T)6-1B47_20210312_1.0c_STDsp bin

Cancel


Upload

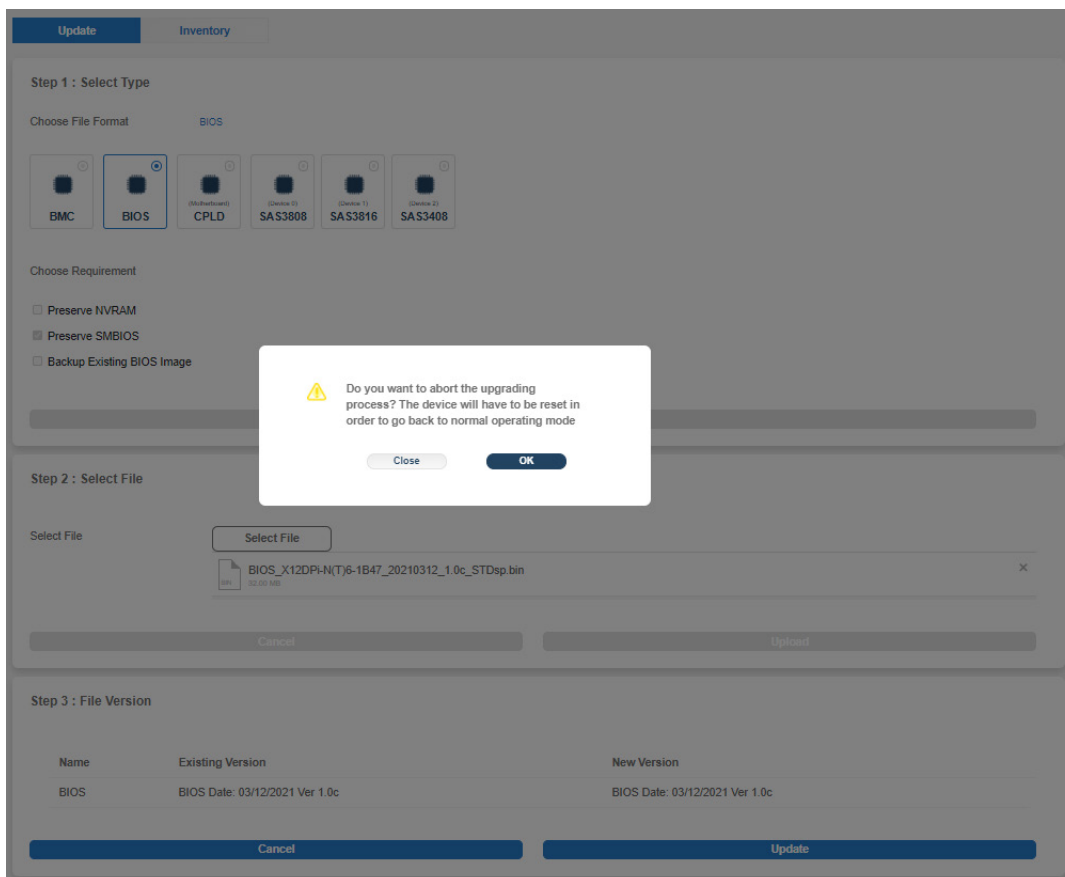
Step 3 : File Version

Name	Existing Version	New Version
BIOS	BIOS Date: 01/27/2021 Ver 1.0b	BIOS Date: 03/12/2021 Ver 1.0c

Cancel

Update

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



The screenshot displays the BIOS update utility interface. At the top, there are tabs for 'Update' and 'Inventory'. The main area is divided into three steps:

- Step 1 : Select Type**
 - Choose File Format:** A row of icons for different components: BMC, BIOS (selected), CPLD, Device 0, Device 1, and Device 2.
 - Choose Requirement:** Three checkboxes: 'Preserve NVRAM' (unchecked), 'Preserve SMBIOS' (checked), and 'Backup Existing BIOS Image' (unchecked).
- Step 2 : Select File**
 - Select File:** A file selection area showing a file named 'BIOS_X12DPi-N(T)6-1B47_20210312_1.0c_STDsp.bin' (52.00 KB).
 - Buttons for 'Cancel' and 'Upload' are visible at the bottom of this section.
- Step 3 : File Version**
 - A table comparing the existing and new BIOS versions:

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

At the bottom of the interface, there are 'Cancel' and 'Update' buttons.

Warning Dialog Box: A modal dialog box is displayed in the center of the screen with a yellow warning icon. The text inside reads: "Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode". It has 'Close' and 'OK' buttons.

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD

SA S3808

SA S3816

SA S3408

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

Upload

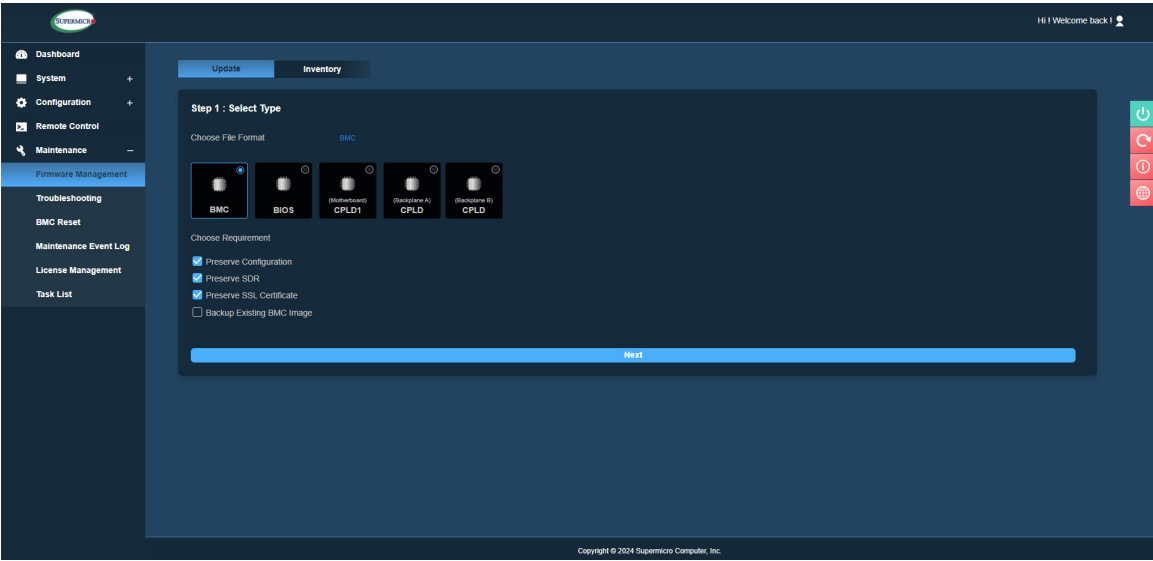
Step 3 : File Version

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

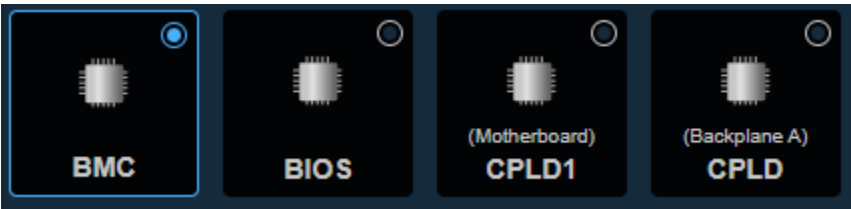


One CPLD MB

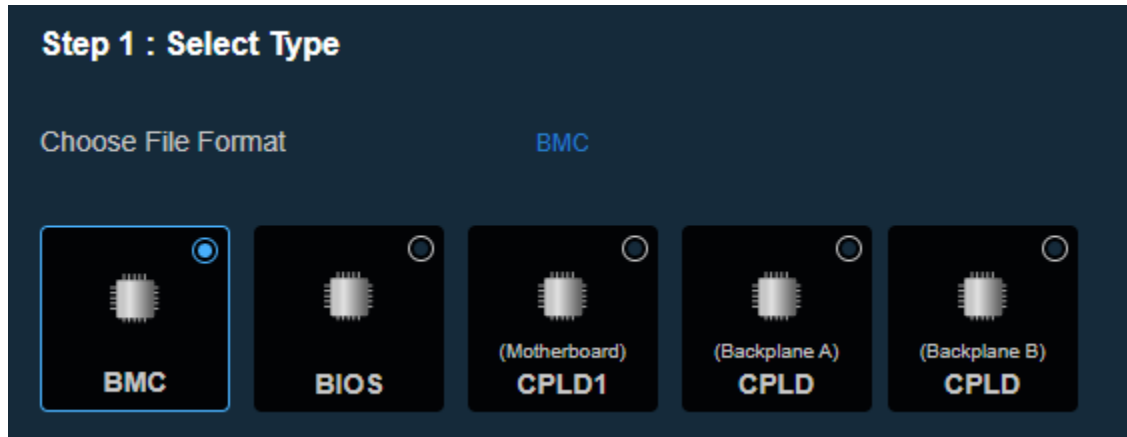


2 CPLD MB

Since some motherboards have two CPLDs, currently BMC Web UI will display as follows. Motherboard and CPLD will start at one as index. Until further announcement, future changes will be modified to reflect changes from Redfish API. Some of the supported motherboards with two CPLDs are: X13DGU, X13DEG-OAD, H13DSG-O-CPU, and H13DSG-O-CPU-D.

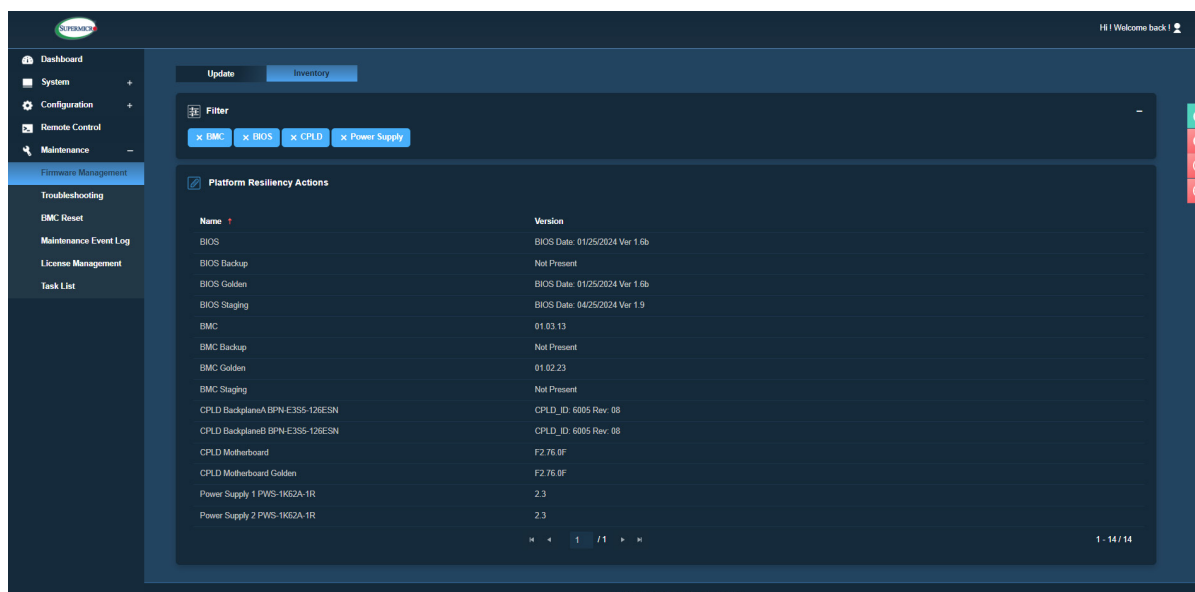


For Backplane, currently BMC Web UI will display as follows. Backplane and CPLD will start at 1 as index. Until further announcement, future changes will be modified to reflect changes from Redfish API.



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.



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



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

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

- 88NR2241
- PMem
- NIC AOC
- Capsule BIOS (X13/H13 and later motherboard)
- Capsule MCU (X13/H13 and later motherboard)
- Capsule ME (X13/H13 and later motherboard)
- CPLD Backplane (A number will be appended at the end of 'CPLD Backplane' if there are multiple backplane CPLDs)
- CPLD Motherboard (A number will be appended at the end of 'CPLD Motherboard' if there are multiple motherboard CPLDs.)
- CPLD Motherboard Golden (X13/H13 and later MB)
- Motherboard EC
- Multi-node EC
- NIC AOC
- Power Supply (A number will be appended at the end of 'Power Supply' if there are multiple Power Supplies)
- CPLD1 Backplane1
- PMem
- Storage AOC (Broadcom, Marvell)



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

Sample of Inventory Page

Filter

✕ BMC

✕ BIOS

✕ CPLD

✕ Power Supply

☒ Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 01/25/2024 Ver 1.6b
BIOS Backup	Not Present
BIOS Golden	BIOS Date: 01/25/2024 Ver 1.6b
BIOS Staging	BIOS Date: 04/25/2024 Ver 1.9
BMC	01.03.13
BMC Backup	Not Present
BMC Golden	01.02.23
BMC Staging	Not Present
CPLD BackplaneA BPN-E3S5-126ESN	CPLD_ID: 6005 Rev: 08
CPLD BackplaneB BPN-E3S5-126ESN	CPLD_ID: 6005 Rev: 08
CPLD Motherboard	F2.76.0F
CPLD Motherboard Golden	F2.76.0F
Power Supply 1 PWS-1K62A-1R	2.3
Power Supply 2 PWS-1K62A-1R	2.3

⏮

1

⏭

1 - 14 / 14

Update

Inventory

Filter

+ BMC

✕ BIOS

✕ CPLD

✕ Power Supply

☒ Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 01/25/2024 Ver 1.6b
BIOS Backup	Not Present
BIOS Golden	BIOS Date: 01/25/2024 Ver 1.6b
BIOS Staging	BIOS Date: 04/25/2024 Ver 1.9
CPLD BackplaneA BPN-E3S5-126ESN	CPLD_ID: 6005 Rev: 08
CPLD BackplaneB BPN-E3S5-126ESN	CPLD_ID: 6005 Rev: 08
CPLD Motherboard	F2.76.0F
CPLD Motherboard Golden	F2.76.0F
Power Supply 1 PWS-1K62A-1R	2.3
Power Supply 2 PWS-1K62A-1R	2.3

⏮

1

⏭

1 - 10 / 10

Platform Resiliency Actions

This page allows you with administrator privileges to manage Platform Firmware Resiliency options. Only BMC and BIOS images are available in the Platform Resiliency Actions page. Click on the Editor button (✎) next to **Platform Resiliency Actions** to perform 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, then the administrator can manually recover BMC or BIOS from the backup image. You can select the current BMC/BIOS image and click on [Recover].



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

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



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

- **Generate Evidence:** When BMC or BIOS is recovered manually or automatically from the last known good image or golden image, the active image will be stored in the evidence region where you can download evidence. If evidence is available, the Generate Evidence button will be enabled. Generate Evidence options 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. Make sure to download evidence before initiating firmware update.

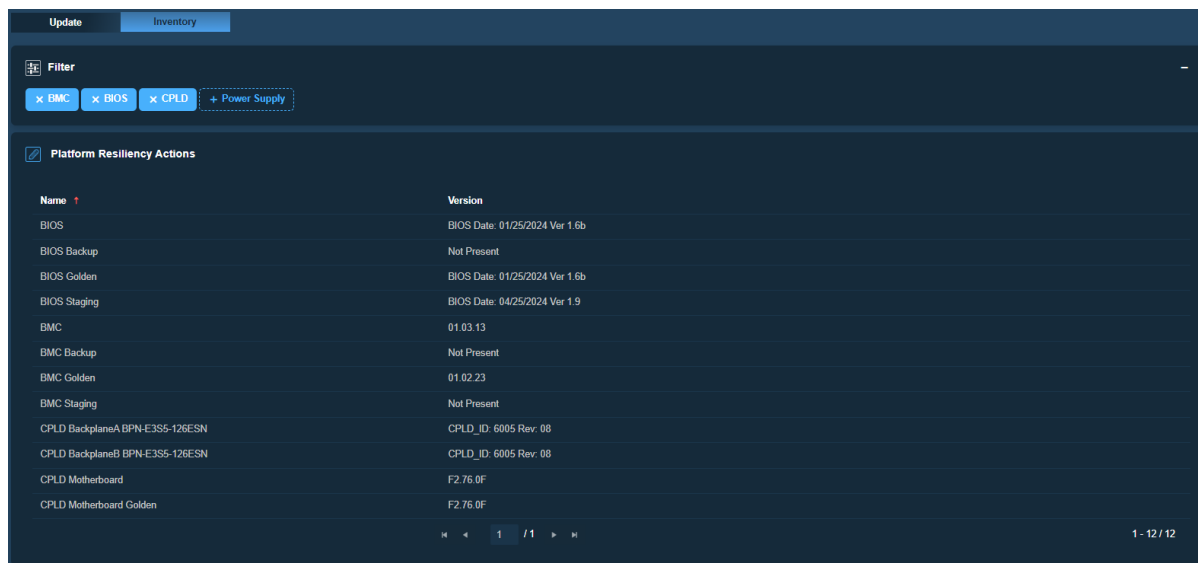
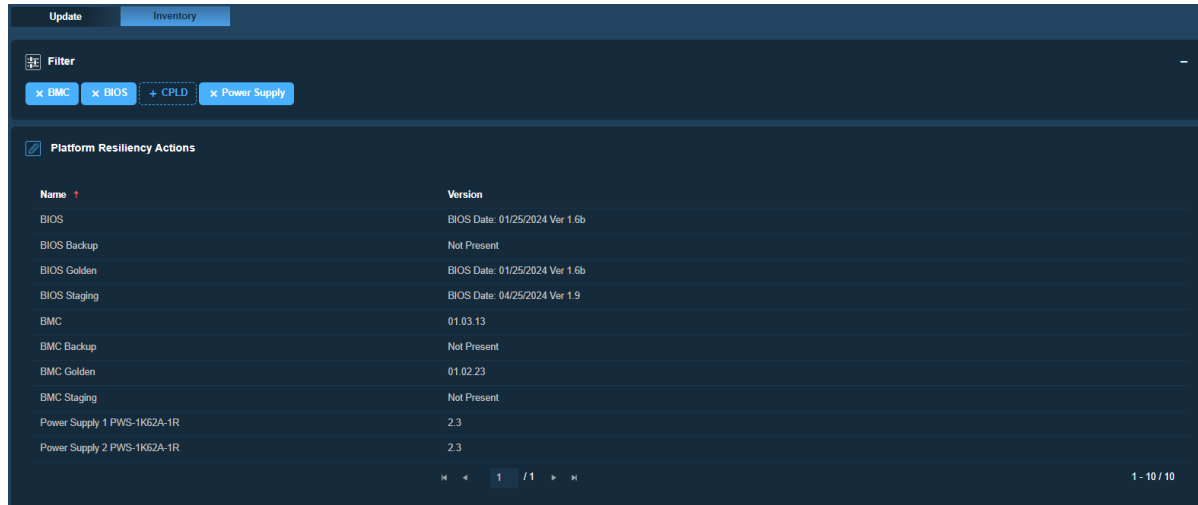
- **Download Evidence:** Once a compressed evidence file is generated, the Download Evidence button will be enabled. Click to download the evidence.




Note 1: Compressed evidence file 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.

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) are to be greyed out.

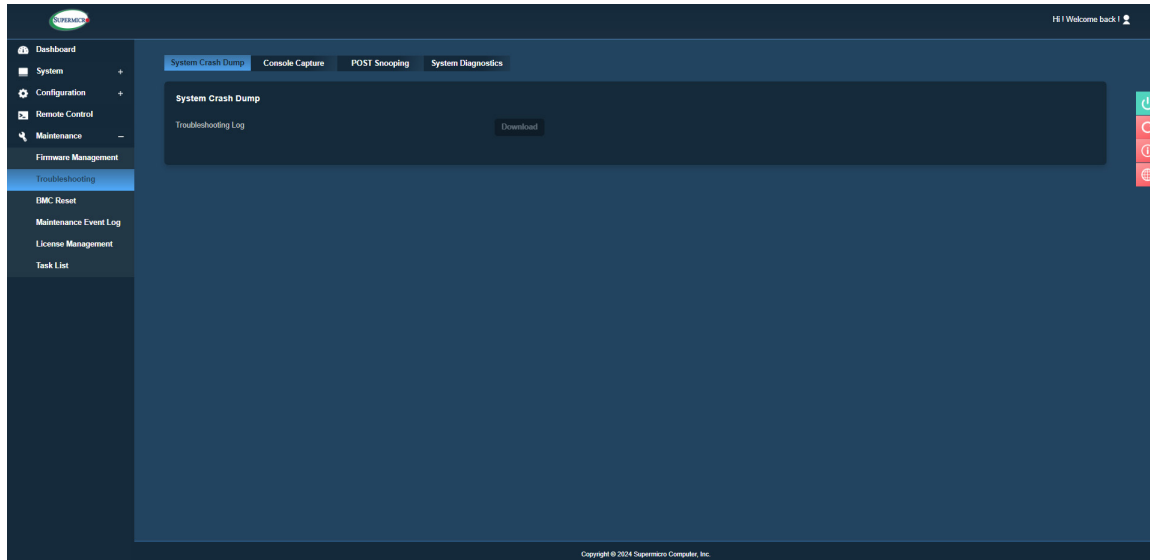


 **Note:** Starting from X13, staging areas will be cleaned out after firmware updates. Hence the Staging areas will be **Not Present** after BMC, BIOS, or other firmware update processes are completed. If you enter wrong file type or bad image for new firmware, a prompt message *“Please upload a valid file!”* will show to ask users to reenter a valid file.

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 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.

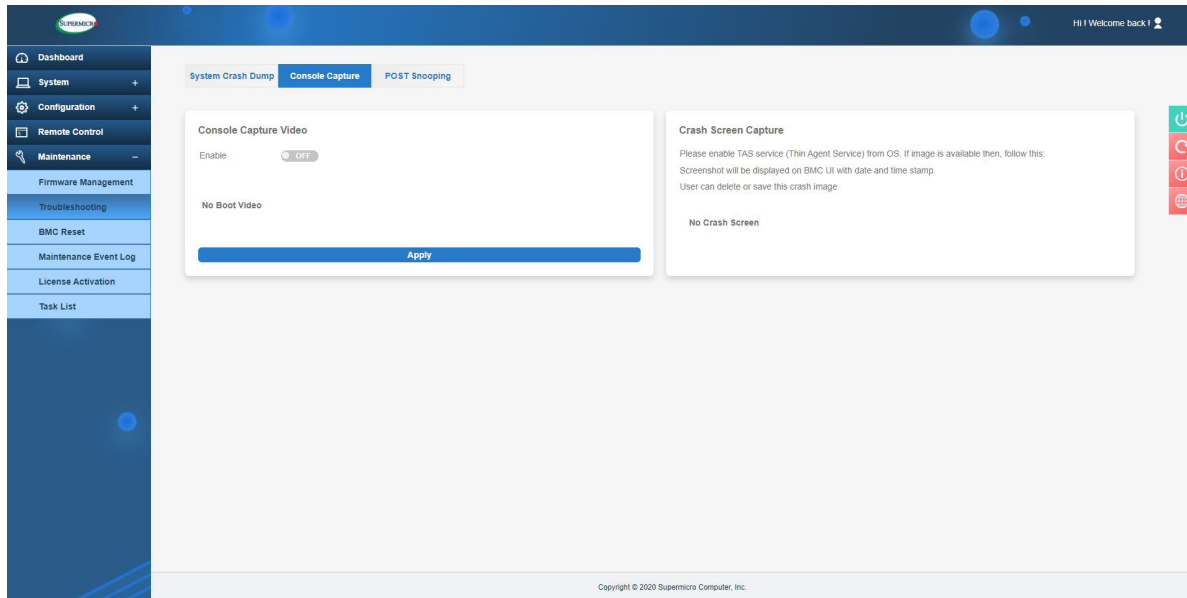


Note: Upon clicking [Generate], the system will remove previous error logs or dump available files and regenerate a new dump file.

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

Console Capture

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



Console Capture

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

Console Capture Video

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 option. By default, it will be disabled.
- **Record until buffer is full:** You can record video of the console until the buffer is full. Video will be saved as AVI format and the maximum buffer size is 7-8 MB (approximately 4 mins. time calculated based on video size).
- **Record until POST ends:** You can record video till POST ends or record till timeout value (approximately 4 minutes). BMC will receive POST completion information from BIOS and record video until that time or if any delay is introduced then BMC will record video until timeout period of approximately 4 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 video from here.
- AC Cycle/Factory Reset: Upon reset, all videos will be deleted.

Crash Screen Capture

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



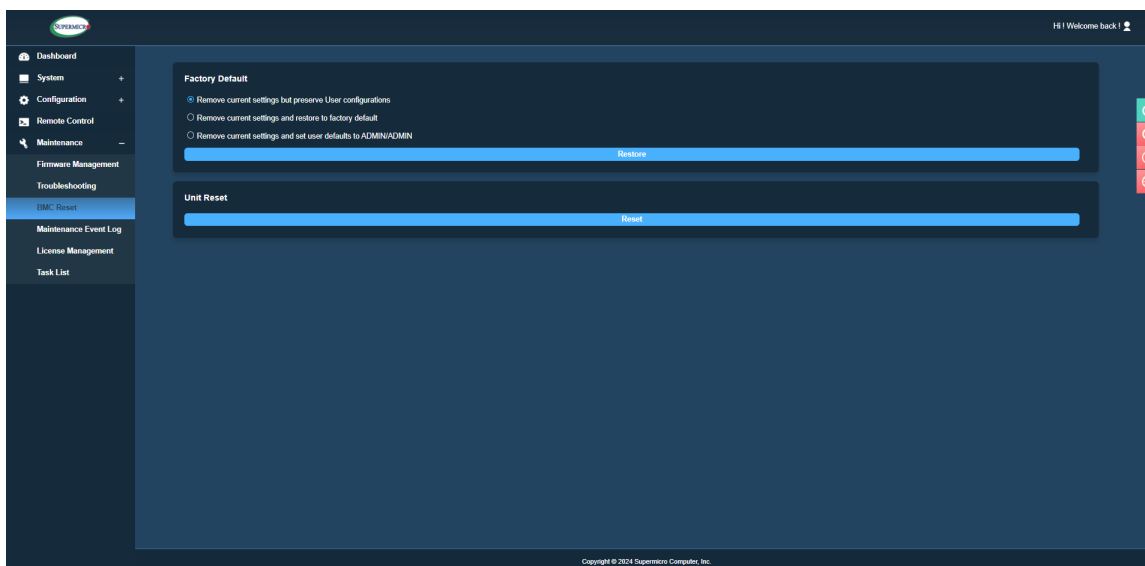
Note: The table shows the supported and unsupported server platforms (non-workstations) for System Crash Dump, Console Capture Video, and Crash Screen Capture features. We will enable the functions when they are supported. Due to time constraint, Console Capture Video and Crash Screen Capture on Intel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

Supported and Unsupported Server Platforms (Non-Workstation)			
	System Crash Dump	Console Capture Video	Crash Screen Capture
Whitley Non-Workstation Platforms (Intel ICE Lake)	Supported	Supported	Supported
Purley Platforms Non-Workstation (Intel Sky Lake)	Supported	Not Yet Supported	Not Yet Supported
MicroCloud Non-Workstation (Intel Rocket Lake)	<i>Unsupported</i>	<i>Unsupported</i>	<i>Unsupported</i>
IoT Solutions (Intel Atom based MB)	<i>Unsupported</i>	<i>Unsupported</i>	<i>Unsupported</i>
AMD H13_AST2600 Non-Workstation Platforms (RoT and non-RoT)	Supported (download only)	Supported	Supported
AMD H12_AST2600 Non-Workstation Platforms (RoT and non-RoT)	Supported (download only)	Supported	Supported
AMD H12_AST2500 Non-Workstation Platforms (RoT and non-RoT)	Supported (download only)	<i>Unsupported</i>	<i>Unsupported</i>
AMD H11_AST2500 (Non-Workstation)	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 following options to restore BMC to the factory default settings. This feature includes the following options:

- Remove current settings but preserve user configurations: You can restore all configurations to factory default and preserve all user configurations.
- Remove current settings and restore to factory default: You can restore all the configuration to factory default. This option will remove all users and reset ADMIN user password to factory default password.
- Remove current settings and set user defaults to ADMIN/ADMIN: You can restore all the configuration to factory default. This option will remove all users and reset ADMIN user password to ADMIN.
- If BMC is reset, only LAN link related should be reported to SEL. (For example: [LAN-0005] Dedicated LAN link Up.)



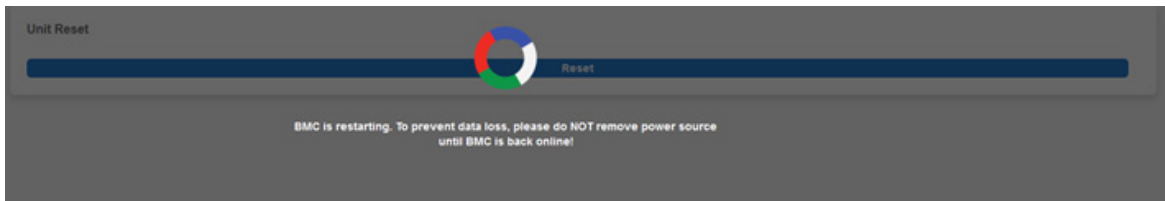
Note: Factory default password is the unique password for X12 and next generation platforms. There will be a prompt saying “BMC is resetting to default. To prevent data loss, please do NOT remove power source until BMC is back online!”

Unit Reset

This feature allows you to reset an IPMI device.




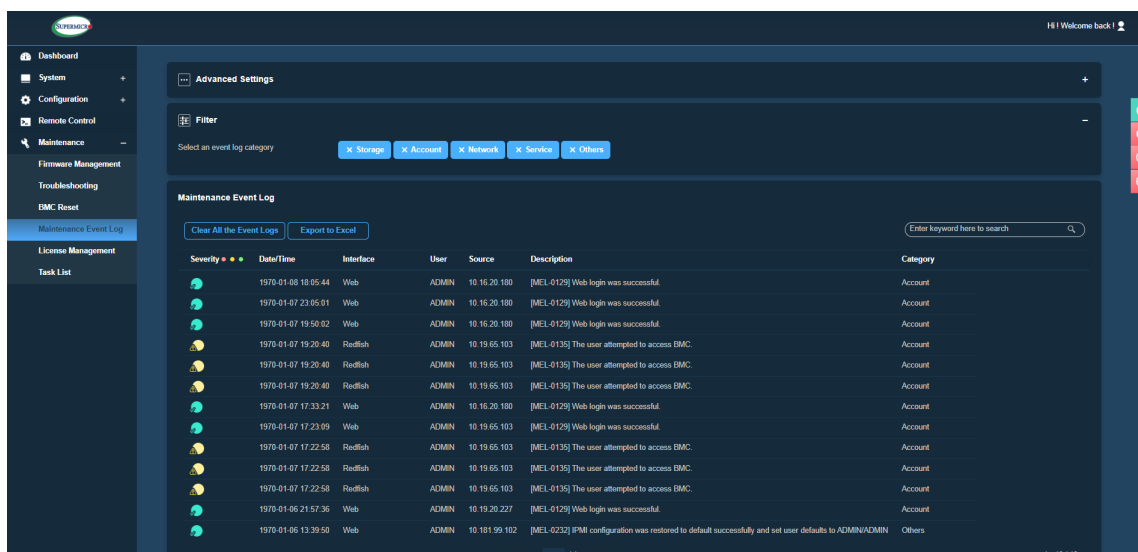
Note: You will get a prompt that *“BMC is restarting. To prevent data loss, please do NOT remove power source until BMC is back online!”*



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).



Severity	Date/Time	Interface	User	Source	Description	Category
Info	1970-01-08 18:05:44	Web	ADMIN	10.16.20.100	[MEL-0129] Web login was successful	Account
Info	1970-01-07 23:05:01	Web	ADMIN	10.16.20.100	[MEL-0129] Web login was successful	Account
Info	1970-01-07 19:50:02	Web	ADMIN	10.16.20.100	[MEL-0129] Web login was successful	Account
Warning	1970-01-07 19:20:40	Redfish	ADMIN	10.19.65.103	[MEL-0135] The user attempted to access BMC	Account
Warning	1970-01-07 19:20:40	Redfish	ADMIN	10.19.65.103	[MEL-0135] The user attempted to access BMC	Account
Warning	1970-01-07 19:20:40	Redfish	ADMIN	10.19.65.103	[MEL-0135] The user attempted to access BMC	Account
Info	1970-01-07 17:33:21	Web	ADMIN	10.16.20.100	[MEL-0129] Web login was successful	Account
Info	1970-01-07 17:23:09	Web	ADMIN	10.19.65.103	[MEL-0129] Web login was successful	Account
Warning	1970-01-07 17:22:58	Redfish	ADMIN	10.19.65.103	[MEL-0135] The user attempted to access BMC	Account
Warning	1970-01-07 17:22:58	Redfish	ADMIN	10.19.65.103	[MEL-0135] The user attempted to access BMC	Account
Warning	1970-01-07 17:22:58	Redfish	ADMIN	10.19.65.103	[MEL-0135] The user attempted to access BMC	Account
Info	1970-01-06 21:57:36	Web	ADMIN	10.19.20.227	[MEL-0129] Web login was successful	Account
Info	1970-01-06 13:39:50	Web	ADMIN	10.101.99.102	[MEL-0232] IPMI configuration was restored to default successfully and set user defaults to ADMIN/ADMIN	Others

The Maintenance Event Log table displays 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 type of the event (e.g., Storage, Account, Network, Service, or others).
- Keyword Search: You can search keyword related events.

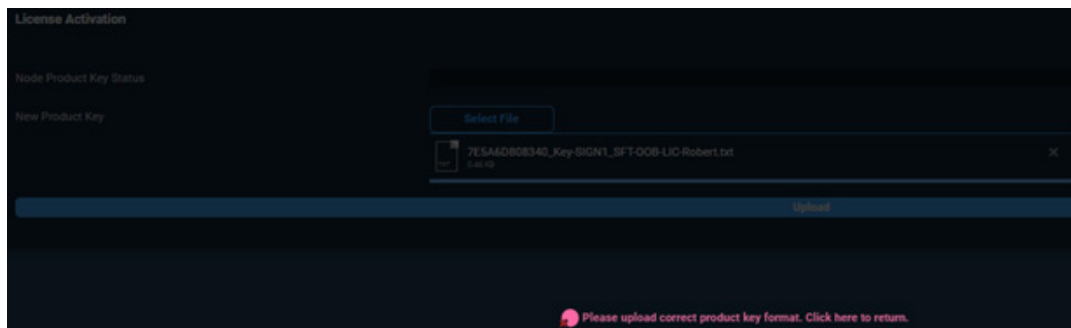
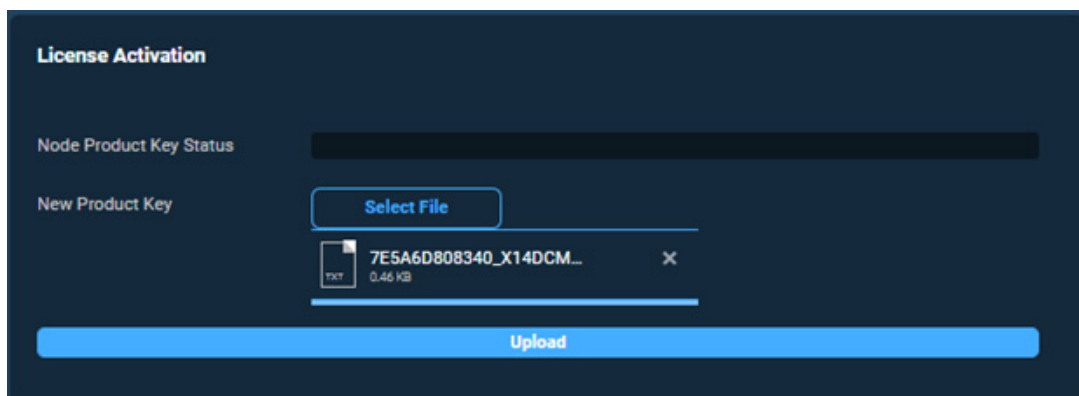
Administrators can perform one of the following operations for the event logs.

- 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**, you must 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 Management

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

Intel SDSi licenses (such as SGX, QAT, DLB, DSA, IAX, and VROC) are also available for review. The Capability Activation Payload (CAP) contains specific Intel SDSi-enabled CPU features that are being enabled, with a maximum provision of 40 CAPs per CPU. You can then activate CAPs on one or more CPUs based on the license paid for activation.



License Activation

Node Product Key **SFT-DCMS-SINGLE**
Status

New Product Key [Select File](#)

[Upload](#)

Filter

Intel SGX License ☒ SGX ☒ QAT ☒ DLB ☒ DSA ☒ IAX ☒ VROC

CPU 1

CAP No.	SGX	QAT	DLB	DSA	IAX	VROC
No data available						

CPU 2

CAP No.	SGX	QAT	DLB	DSA	IAX	VROC
No data available						

Filter

Intel SGX License ☒ SGX ☒ QAT ☒ DLB ☒ DSA ☒ IAX ☒ VROC

CPU 1

CAP No.	SGX	QAT	DLB	DSA	IAX	VROC
016c3086d90222c						
018eb777800516c3						
01f72970b0ca1580						
019633006e7a30e						
010b515a3e3c2782						
01fe06990d0ca9c						
01088009f2490						

CPU 2

CAP No.	SGX	QAT	DLB	DSA	IAX	VROC
No data available						

You can adjust the following settings to configure this feature.

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

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

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

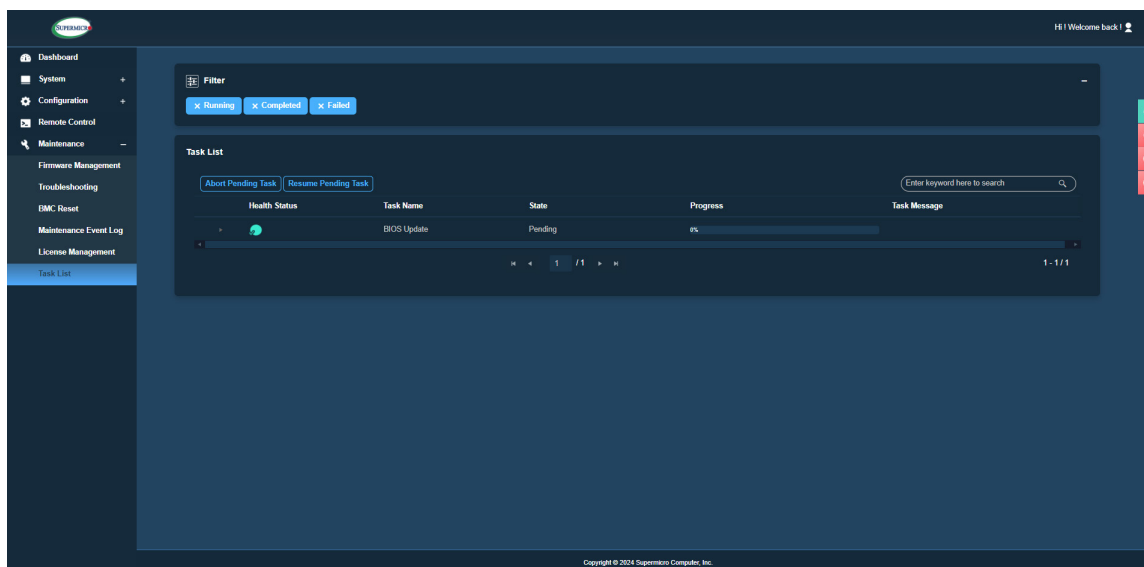
If you upload a product key with a valid format but an invalid license, a prompt message will appear stating, *"Product key is invalid. Click here to return."* Additionally, a log will be generated.

2.8.6. Task List

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



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



You can search 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 type.
- State: You can view current state values (Running, Completed, or Failed).
- Create Time: You can view the timestamp for task beginning.
- Progress: You can view the progress of current running task(s).
- Total Duration: You can view the total time taken to finish current task(s).
- Completed Time: You can view the task completion time stamp.

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



Note: Only Administrative users can cancel pending tasks. The trash can icon will be disabled under Operator and User privileges.

<i>UI Task Filter</i>	<i>Task List State</i>
Running	New
	Starting
	Running
	Suspended
	Interrupted
	Pending
	Stopping
	Service
	Cancelling
Completed	Completed
	Killed
	Cancelled
Failed	Exception

Chapter 3

Frequently Asked Questions

Question: How do I flash the BMC firmware?

Answer:

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

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

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

HTTP: 80 (TCP)

HTTPS: 443 (TCP)

BMC: 623 (UDP)

Remote console: 5900 (TCP)

Virtual media: 623 (TCP)

SMASH: 22 (TCP)

WS-MAN: 8889 (TCP)

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

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

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

Answer: It is not a normal condition. Make sure that there is no other device accessing the I²C bus. If another device accesses the I²C bus frequently, it might cause a collision with the BMC when this device accesses the I²C bus. When you see this error, uninstall lm_sensors in Linux.

Chapter 4

UEFI BIOS

4.1 Introduction

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



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

Starting the Setup Utility

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

The Main BIOS screen has two main frames. The left frame displays all the options that can be configured. Greyed-out options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it. Settings printed in **Bold** are the default values.



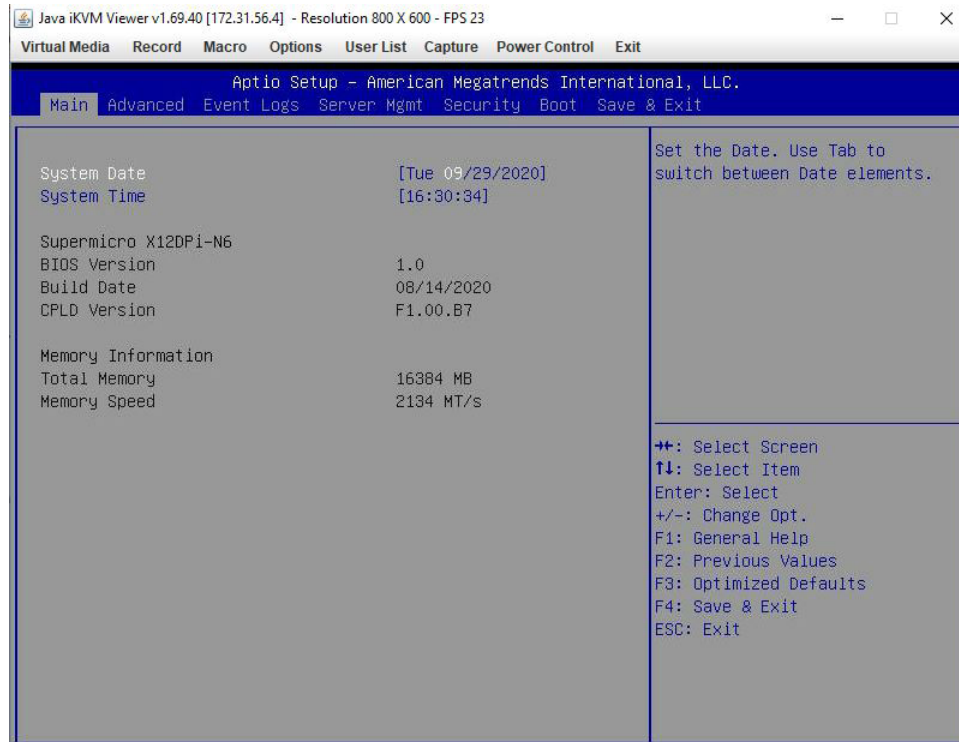
Note: BIOS has default text messages built in. We retain the option to include, omit, or change any of these text messages. Settings printed in **Bold** are the default values.

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

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

4.2 Main Setup

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



System Date/System Time

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



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

Supermicro BMC IPMI

BIOS Version

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

Build Date

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

CPLD Version

This item displays the Complex Programmable Logic Device version.

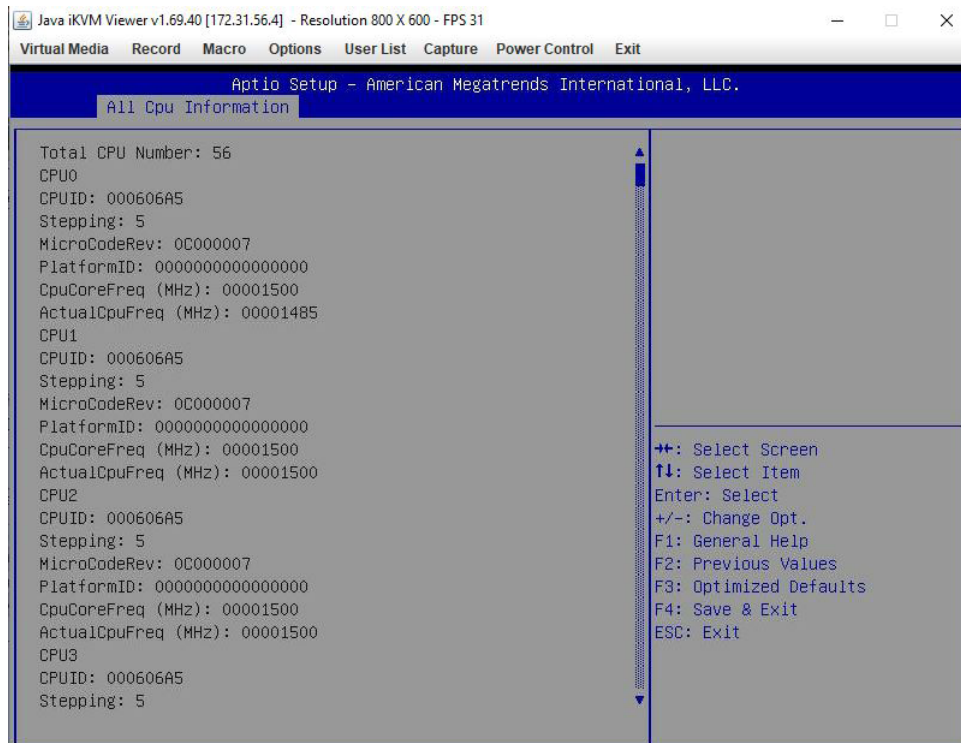
Memory Information

Total Memory

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

4.3 Advanced Setup Configurations

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



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

► Boot Feature

Quiet Boot

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

Option ROM Messages

Use this feature to set the display mode for the Option ROM. Select Keep Current to display the current AddOn ROM setting. Select Force BIOS to use the Option ROM display set by the system BIOS. The options are **Force BIOS** and Keep Current.

Bootup NumLock State

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

Wait For "F1" If Error

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

INT19 (Interrupt 19) Trap Response

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

Re-try Boot

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

Install Windows 7 USB Support

Enable this feature to use the USB keyboard and mouse during the Windows 7 installation since the native XHCI driver support is unavailable. Use a SATA optical drive as a USB drive, and USB CD/DVD drives are not supported. Disable this feature after the XHCI driver has been installed in Windows. The options are **Disabled** and Enabled.

Port 61h Bit-4 Emulation

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

Power Configuration

Watch Dog Function

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

Restore on AC Power Loss

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

Power Button Function

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

►CPU Configuration

The following CPU information will display:

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

Hyper-Threading (ALL) (Available when supported by the CPU)

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

Cores Enabled

Set a numerical value to enable the number of cores in the CPU. Refer to Intel's website for more information. Enter **0** to enable all cores.

Monitor/Mwait

Select Enable to use the CPU monitor instructions for address-range monitoring and advanced power management to enhance processor performance. The options are **Auto**, Enable, and Disable.

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

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

Intel Virtualization Technology

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

PPIN Control

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

Hardware Prefetcher (Available when supported by the CPU)

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

Adjacent Cache Prefetch (Available when supported by the CPU)

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

DCU Streamer Prefetcher (Available when supported by the CPU)

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

DCU IP Prefetcher (Available when supported by the CPU)

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

LLC Prefetch

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

Extended APIC

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

AES-NI

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

► Advanced Power Management Configuration

Power Technology

Select Energy Efficiency to support power-saving mode. Select Custom to customize system power settings. Select Disable to disable power-saving settings. The options are Disable, **Energy Efficient**, and Custom.

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

Power Performance Tuning

This feature allows you to select whether the BIOS or Operating System chooses energy performance bias tuning. The options are **OS Controls EPB** or BIOS Controls EPB.

**If the item above is set to BIOS Controls EPB, the following item will be displayed:*

ENERGY_PERF_BIAS CFG mode

The Energy Performance BIAS (EPB) feature allows you to configure CPU power and performance settings. Select Maximum Performance to set the highest performance. Select Performance to optimize performance over energy efficiency. Select Balanced Performance to prioritize performance optimization while conserving energy. Select Balanced Power to prioritize energy conservation while maintaining good performance. Select Power to optimize energy efficiency over performance. The options are Maximum Performance, Performance, **Balanced Performance**, Balanced Power, and Power.

► CPU P State Control

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

SpeedStep (Pstates)

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

EIST PSD Funtion

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

Turbo Mode

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

► Hardware PM State Control

Hardware P-States

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

► CPU C State Control

Autonomous Core C-State

Enabling this setting allows the hardware to autonomously choose to enter a C-state based on power consumption and clock speed. The options are **Disable** and Enable.

CPU C6 Report

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

Enhanced Halt State (C1E)

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

► Package C State Control

Package C State

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

► CPU T State Control

Software Controlled T-States

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

► Chipset Configuration

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

► North Bridge

This feature allows you to configure the following North Bridge settings.

► UPI Configuration

The following UPI information will display:

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

Degrade Precedence

Use this feature to set degrade precedence when system settings are in conflict. Select Topology Precedence to degrade Features. Select Feature Precedence to degrade Topology. The options are **Topology Precedence** and Feature Precedence.

Link L0p Enable

Select Enable for the QPI to enter the L0p state for power saving. The options are Disable, Enable, and **Auto**.

Link L1 Enable

Select Enable for the QPI to enter the L1 state for power saving. The options are Disable, Enable, and **Auto**.

IO Directory Cache (IODC)

IO Directory Cache is an 8-entry cache that stores the directory state of remote IIO writes and memory lookups, and saves directory updates. Use this feature to lower cache to cache (C2C) transfer latencies. The options are Disable, **Auto**, Enable for Remote Invltom Hybrid Push, Invltom AllocFlow, Enable for Remote Invltom Hybrid AllocNonAlloc, and Enable for Remote Invltom and Remote WViLF.

SNC

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

XPT Prefetch

This feature makes a copy to the memory controller of a read request being sent to LLC. The options are **Disable** and Enable.

KTI Prefetch

KTI Prefetch enables memory read to start early on a DDR bus. The options are Disable and **Enable**.

Local/Remote Threshold

This feature allows you to set the threshold for the Interrupt Request (IRQ) signal. The options are Disable, **Auto**, Low, Medium, and High.

Stale AtoS

Use this feature to optimize the A to S directory. The options are Disable, Enable, and **Auto**.

LLC Dead Line Alloc

Select Enable to optimally fill dead lines in LLC. The options are Disable, **Enable**, and Auto.

Isoc Mode

Isochronous (Isoc) mode allows time-sensitive processes to be given priority. The options are Disable, Enable, and **Auto**.

► Memory Configuration

Enforce POR

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

PPR Type

Use this feature to set the Post Package Repair type. The options are **Auto**, Hard PPR, Soft PPR, and PPR Disable.

Memory Frequency

Use this feature to set the maximum memory frequency for onboard memory modules. The options are **Auto**, 1866, 2000, 2133, 2400, 2666, and 2933.

Data Scrambling for DDR4

Use this feature to enable or disable data scrambling for DDR4 memory. The options are **Auto**, Disable, and Enable.

tCCD_L Relaxation

If this feature is enable, SPD (Serial Presence Detect) will override TCCD_L ("Column to Column Delay-Long" or "Command to Command Delay-Long" on the column side). If this feature is set to Disable, TCCD_L will be enforced based on the memory frequency. The options are Disable and **Auto**.

tRWSR Relaxation

Select Enable to use the same TRWSR DDR timing setting among all memory channels, in which case, the worst value among all channels will be used. Select Disable to use different values for the TRWSR DDR timing settings for different channels as trained. The options are **Disable** and Enable.

2x Refresh

Select Enable for memory 2X refresh support to enhance memory performance. The options are Enable and **Auto**.

Page Policy

Use this feature to set the page policy for onboard memory support. The options are Closed, Adaptive, and **Auto**.

IMC Interleaving

Use this feature to configure interleaving settings for the IMC (Integrated Memory Controller), which will improve memory performance. The options are 1-way Interleave, 2-way Interleave, and **Auto**.

►Memory Topology

This item displays the information of onboard memory modules as detected by the BIOS.

►Memory RAS Configuration

Static Virtual Lockstep Mode

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

Mirror Mode

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

Memory Rank Sparing

Select Enable to enable memory-sparing support for memory ranks to improve memory performance. The options are **Disable** and Enable.

Correctable Error Threshold

Use this feature to specify the threshold value for correctable memory-error logging, which sets a limit on the maximum number of events that can be logged in the memory error log at a given time. The default setting is **100**.

SDDC Plus One (Available when this feature is supported by the CPU & the feature: Intel Run Sure is set to Disable)

SDDC (Single Device Data Correction) checks and corrects single-bit or multiple-bit (4-bit max.) memory faults that affect an entire single x4 DRAM device. SDDC Plus One is the enhanced feature to SDDC. SDDC+1 will spare the faulty DRAM device out after an SDDC event has occurred. After the event, the SDDC+1 ECC mode is enabled to protect against any additional memory failure caused by a 'single-bit' error in the same memory rank. The options are **Disable** and Enable*. (The **Enable** option can be set as default when it is supported by the motherboard).

ADDDC Sparing

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

Patrol Scrub

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

Patrol Scrub Interval

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

► I/O Configuration

EV DFX Features

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

► CPU Configuration

IOU0 (I/O PCIe Br1)

This feature configures the PCIe port Bifurcation setting for a specified PCIe port. The options are x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, and **Auto**.

IOU1 (I/O PCIe Br2)

This feature configures the PCIe port Bifurcation setting for a specified PCIe port. The options are x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, and **Auto**.

IOU2 (I/O PCIe Br3)

This feature configures the PCIe port Bifurcation setting for a specified PCIe port. The options are x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, and **Auto**.

► CPU SLOT2 PCIe 3.0 X8 / CPU SLOT6 PCIe X16 / CPU SLOT4 PCIe X16 / CPU SLOT3 PCIe X8

Link Speed

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

The following information will also be displayed:

- PCIe Port Link Status
- PCIe Port Link Max
- PCIe Port Link Speed

PCIe Port Max Payload Size

Selecting **Auto** for this feature will enable the motherboard to automatically detect the maximum Transaction Layer Packet (TLP) size for the connected PCIe device, allowing for maximum I/O efficiency. Selecting 128B or 256B will designate maximum packet size of 128 or 256. The options are 128B, 256B, and **Auto**.

► IOAT Configuration

Disable TPH

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

Prioritize TPH

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

Relaxed Ordering

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

► Intel® VT for Directed I/O (VT-d)

Intel® VT for Directed I/O (VT-d)

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

ACS Control (Available if Intel VT for Directed I/O (VT-d) is enabled)

Use this feature to program Access Control Services (ACS) to the PCIe Root Port Bridges. The options are **Enable** and **Disable**.

Interrupt Remapping

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

PassThrough DMA

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

ATS

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

Posted Interrupt

Use this feature to enable VT_D Posted Interrupt. The options are **Enable** and **Disable**.

Coherency Support (Non-Isoch)

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

► Intel® VMD Technology

► Intel® VMD for Volume Management Device on CPU



Note: After you have enabled VMD on a PCIe slot of your choice, this PCIe slot will be dedicated for NVMe storage devices use only, and it will no longer support PCIe devices of other functionalities. To re-activate this slot for PCIe use, disable VMD.

VMD Config for PStack0

Intel® VMD for Volume Management Device

Select Enable to use the Intel Volume Management Device Technology for this stack. The options are **Disable** and Enable.

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

CPU SLOT2 PCIe 3.0 X8 VMD (Available when the device is detected by the system)

Select Enable to use the Intel Volume Management Device Technology for this specific root port. The options are **Disable** and Enable.

Hot Plug Capable (Available when the device is detected by the system)

Use this feature to enable hot plug support for PCIe root ports 1A~1D. The options are **Disable** and Enable.

VMD Config for PStack1

Intel® VMD for Volume Management Device

Select Enable to use the Intel Volume Management Device Technology for this stack. The options are **Disable** and Enable.

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

CPU SLOT6 PCIe 3.0 X16 VMD (Available when the device is detected by the system)

Select Enable to use the Intel Volume Management Device Technology for this specific root port. The options are **Disable** and Enable.

Hot Plug Capable (Available when the device is detected by the system)

Use this feature to enable hot plug support for PCIe root ports 2A~2D. The options are **Disable** and Enable.

VMD Config for PStack2

Intel® VMD for Volume Management Device

Select Enable to use the Intel Volume Management Device Technology for this stack. The options are **Disable** and Enable.

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

CPU SLOT4 PCIe 3.0 X16 VMD (Available when the device is detected by the system)

Select **Enable** to use the Intel Volume Management Device Technology for this specific root port. The options are **Disable** and **Enable**.

CPU SLOT3 PCIe 3.0 X8 VMD (Available when the device is detected by the system)

Select **Enable** to use the Intel Volume Management Device Technology for this specific root port. The options are **Disable** and **Enable**.

Hot Plug Capable (Available when the device is detected by the system)

Use this feature to enable hot plug support for PCIe root ports 3A~3D. The options are **Disable** and **Enable**.

PCIe Completion Timeout Disable

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

► South Bridge

The following USB information will display:

- USB Module Version
- USB Devices

Legacy USB Support

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

XHCI Hand-off

When this feature is disabled, the motherboard will not support USB 3.0. The options are **Enabled** and **Disabled**.

Port 60/64 Emulation

This feature allows legacy I/O support for USB devices like mice and keyboards. The options are **Enabled** and **Disabled**.

PCIe PLL SCC

Select Enable for PCH PCIe Spread Spectrum Clocking support, which will allow the BIOS to monitor and attempt to reduce the level of Electromagnetic Interference caused by the components whenever needed. The options are **Disable** and Enable.

►Server ME Configuration

The following General ME Configuration will display:

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

►PCH SATA Configuration

When this submenu is selected, the AMI BIOS automatically detects the presence of the SATA devices that are supported by the Intel PCH chip and displays the following features:

SATA Controller

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

Configure SATA as

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

SATA HDD Unlock

This feature allows you to remove any password-protected SATA disk drives. The options are **Enable** and Disable.

Aggressive Link Power Management

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

****If the feature "Configure SATA as" above is set to RAID, the following features will become available for configuration:***

SATA RSTe Boot Info

Select Enable to provide full int13h support for the devices attached to SATA controller. The options are Disable and **Enable**.

SATA RAID Option ROM/UEFI Driver

Select UEFI to load the EFI driver for system boot. Select Legacy to load a legacy driver for system boot. The options are Disable, EFI, and **Legacy**.

SATA Port 0 ~ Port 7

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

- Model number of drive and capacity
- Software Preserve Support

Port 0 ~ Port 7 Hot Plug

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

Port 0 ~ Port 7 Spin Up Device

On an edge detect from 0 to 1, set this feature to allow the PCH to initialize the device. The options are **Disable** and Enable.

Port 0 ~ Port 7 SATA Device Type

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

►PCH sSATA Configuration

When this submenu is selected, the AMI BIOS automatically detects the presence of the SATA devices that are supported by the Intel PCH chip and displays the following features:

sSATA Controller

This features enables or disables the onboard sSATA controller supported by the Intel PCH chip. The options are **Enable** and Disable.

Configure sSATA as

Select AHCI to configure a specified sSATA drive as an AHCI drive. Select RAID to configure a specified sSATA drive as a RAID drive. The options are **AHCI** and RAID.

SATA HDD Unlock

This feature allows you to remove any password-protected SATA disk drives. The options are Disable and **Enable**.

Aggressive Link Power Management

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

****If the feature "Configure sSATA as" above is set to RAID, the following features will become available for configuration:***

sSATA RSTe Boot Info

Select Enable to provide full int13h support for the devices attached to sSATA controller. The options are Disable and **Enable**.

sSATA RAID Option ROM/UEFI Driver

Select UEFI to load the EFI driver for system boot. Select Legacy to load a legacy driver for system boot. The options are Disable, EFI, and **Legacy**.

sSATA Port 0 ~ Port 2

This item displays the information detected on the installed sSATA drive on the particular sSATA port.

- Model number of drive and capacity
- Software Preserve Support

Port 0 ~ Port 2 Hot Plug

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

Port 0 ~ Port 2 Spin Up Device

On an edge detect from 0 to 1, set this feature to allow the PCH to initialize the device. The options are **Disable** and Enable.

Port 0 ~ Port 2 sSATA Device Type

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

►PCIe/PCI/PnP Configuration

The following information will display:

- PCI Bus Driver Version
- PCI Devices Common Settings:

Above 4G Decoding (Available if the system supports 64-bit PCI decoding)

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

SR-IOV Support

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

MMIO High Base

Use this feature to select the base memory size according to memory-address mapping for the IO hub. The options are **56T**, 40T, 24T, 16T, 4T, 2T, and 1T.

MMIO High Granularity Size

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

Maximum Read Request

Use this feature to select the Maximum Read Request size of the PCIe device, or select Auto to allow the System BIOS to determine the value. The options are **Auto**, 128 Bytes, 256 Bytes, 512 Bytes, 1024 Bytes, 2048 Bytes, and 4096 Bytes.

MMCFG Base

Use this feature to select the low base address for PCIe adapters to increase base memory. The options are 1G, 1.5G, 1.75G, **2G**, 2.25G. and 3G.

NVMe Firmware Source

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

VGA Priority

Use this feature to select VGA priority when multiple VGA devices are detected. Select Onboard to give priority to the onboard video device. Select Offboard to give priority to the graphics card. The options are **Onboard** and Offboard.

PCH SLOT1 PCIe 3.0 X4 (IN X8) OPROM

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

CPU SLOT2 PCIe 3.0 X8 OPROM

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

CPU SLOT3 PCIe 3.0 X8 OPROM

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

CPU SLOT4 PCIe 3.0 X16 OPROM

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

CPU SLOT6 PCIe 3.0 X16 OPROM

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

M.2 PCIe 3.0 X4 OPROM

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

Bus Master Enable

Select Enabled to enable the Bus Driver Master bit. The options are **Enabled** and Disabled.

Onboard LAN Device

Select Enabled to enable the Onboard LAN device. The options are **Enabled** and Disabled.

Onboard LAN1 Option ROM

Use this feature to select which firmware function to be loaded for LAN Port1 used for system boot. The options are Disabled, **Legacy**, and EFI.

Onboard LAN2 Option ROM

Use this feature to select which firmware function to be loaded for LAN Port2 used for system boot. The options are **Disabled**, Legacy, and EFI.

Onboard Video Option ROM

Use this feature to select the Onboard Video Option ROM type. The options are Disabled, **Legacy**, and EFI.

► **Network Stack Configuration**

Network Stack

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

IPv4 PXE Support

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

IPv4 HTTP Support

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

IPv6 PXE Support

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

IPv6 HTTP Support

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

PXE Boot Wait Time

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

Media Detect Count

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

► **Super IO Configuration**

The following Super IO information will display:

- Super IO Chip AST2500

► Serial Port 1 Configuration

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

Serial Port 1

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

Device Settings

This item displays the status of a specified serial part.

Change Settings

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

The options for Serial Port 1 are **Auto**, (IO=3F8h; IRQ=4;), (IO=2F8h; IRQ=3, 4;), (IO=3E8h; IRQ=4;), and (IO=2E8h; IRQ=4;).

► Serial Port 2 Configuration

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

Serial Port 2

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

Device Settings

This item displays the status of a specified serial part.

Change Settings

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

The options for Serial Port 2 are **Auto**, (IO=2F8h; IRQ=3;), (IO=3F8h; IRQ=3;), (IO=3E8h; IRQ=3;), and (IO=2E8h; IRQ=3;).

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

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

► Serial Port Console Redirection

COM1 Console Redirection

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

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

► COM1 Console Redirection Settings

Use this feature to specify how the host computer will exchange data with the remote client computer you are using.

COM1 Terminal Type

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

COM1 Bits Per Second

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

COM1 Data Bits

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

COM1 Parity

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

COM1 Stop Bits

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

COM1 Flow Control

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

COM1 VT-UTF8 Combo Key Support

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

COM1 Recorder Mode

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

COM1 Resolution 100x31

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

COM1 Legacy OS Redirection Resolution

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

COM1 Putty KeyPad

This feature selects the settings for Function Keys and KeyPad used for Putty, which is a terminal emulator designed for the Windows OS. The options are **VT100**, LINUX, XTERMR6, SC0, ESCN, and VT400.

COM1 Redirection After BIOS POST

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

SOL/COM2 Console Redirection

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

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

► SOL/COM2 Console Redirection Settings

Use this feature to specify how the host computer will exchange data with the remote client computer you are using.

COM2 Terminal Type

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

COM2 Bits Per Second

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

COM2 Data Bits

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

COM2 Parity

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

COM2 Stop Bits

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

COM2 Flow Control

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

COM2 VT-UTF8 Combo Key Support

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

COM2 Recorder Mode

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

COM2 Resolution 100x31

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

COM2 Legacy OS Redirection Resolution

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

COM2 Putty KeyPad

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

COM2 Redirection After BIOS POST

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

Legacy Console Redirection

Legacy Serial Redirection Port

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

EMS (Emergency Management Services) Console Redirection

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

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

► EMS Console Redirection Settings

This feature allows you to specify how the host computer will exchange data with the remote client computer you are using.

Out-of-Band Mgmt Port

The feature selects a serial port in a client server to be used by the Microsoft Windows Emergency Management Services (EMS) to communicate with a remote host server. The options are **COM1** and SOL/COM2.

Terminal Type

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

Bits Per Second

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

Flow Control

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

Data Bits, Parity, Stop Bits

►ACPI Settings

WHEA Support

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

High Precision Event Timer

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

► Trusted Computing

The BMC IPMI supports TPM 1.2 and 2.0. The following Trusted Platform Module (TPM) information will display if a TPM 2.0 module is detected:

- Vendor Name
- Firmware Version

Security Device Support

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

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

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

SHA-1 PCR Bank

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

SHA256 PCR Bank

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

Pending Operation

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

Platform Hierarchy

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

Storage Hierarchy

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

Endorsement Hierarchy

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

PH Randomization

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

SMCI BIOS-Based TPM Provision Support

Use feature to enable the Supermicro TPM Provision support. The options are **Disabled** and Enabled.

TXT Support

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

► HTTP Boot Configuration

HTTP BOOT Configuration

Http Boot One Time

Use feature to create the HTTP boot option. The options are **Disabled** and Enabled.

Input the description

Use feature to enable the Supermicro TPM Provision support. The options are **Disabled** and Enabled.

Boot URI

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

► TLS Authentication Configuration

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

► Server CA Configuration

► Enroll Certification

Enroll Certification Using File

Use this feature to enroll certification from a file.

Cert GUID

Use this feature to input the certification GUID.

► Commit Changes and Exit

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

► Discard Changes and Exit

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

► Delete Certification

► iSCSI Configuration

iSCSI Initiator Name

This feature allows you to enter the unique name of the iSCSI Initiator in IQN format. Once the name of the iSCSI Initiator is entered into the system, configure the proper settings for the following items.

► Add an Attempt

► Delete Attempts

► Change Attempt Order

► Driver Health

Intel® DCPMM 1.0.0 3429 Driver

This feature provides health status for the drivers and controllers.

4.4 Event Logs

Use this feature to configure Event Log settings.



► Change SMBIOS Event Log Settings

Enabling/Disabling Options

SMBIOS Event Log

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

Erasing Settings

Erase Event Log

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

When Log is Full

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

SMBIOS Event Log Standard Settings

Log System Boot Event

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

MECI

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

METW

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



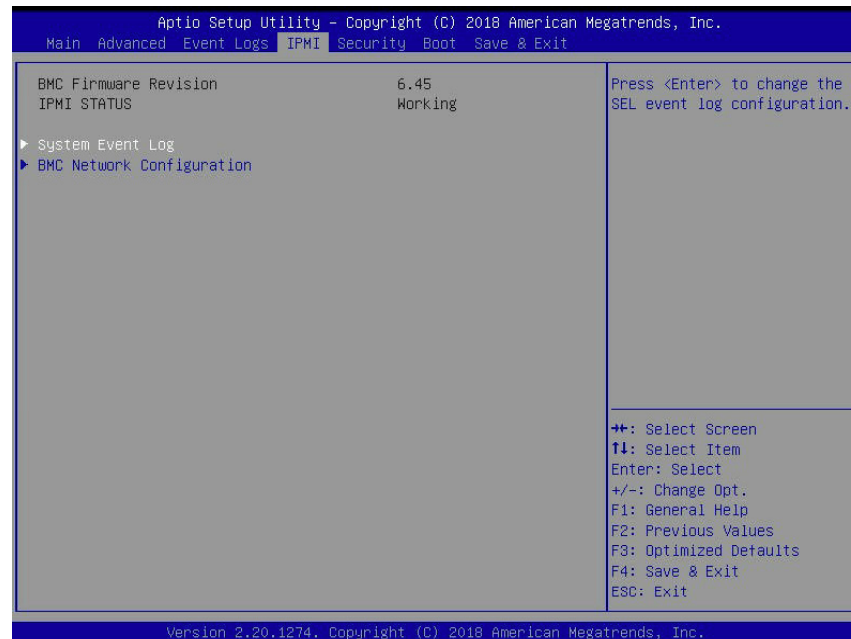
Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

►View SMBIOS Event Log

Select this submenu and press enter to see the contents of the SMBIOS event log. The following categories will be displayed: Date/Time/Error Codes/Severity.

4.5 IPMI

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



BMC Firmware Revision

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

IPMI Status (Baseboard Management Controller)

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

▶ System Event Log

Enabling/Disabling Options

SEL Components

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

Erasing Settings

Erase SEL

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

When SEL is Full

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



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

►BMC Network Configuration

BMC Network Configuration

Configure IPV4 Support

This section displays configuration features for IPV4 support.

IPMI LAN Selection

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

IPMI Network Link Status

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

Update IPMI LAN Configuration

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

****If the item above is set to Yes, the following item will become available for configuration:***

Configuration Address Source

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

****If the item above is set to Static, the following items will become available for configuration:***

Station IP Address

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

Subnet Mask

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

Station MAC Address

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

Gateway IP Address

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

VLAN

This item displays the virtual LAN settings. The options are **Disable** and Enable.

Configure IPV6 Support

This section displays configuration features for IPV6 support.

IPV6 address status**IPV6 Support**

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

Configuration Address Source

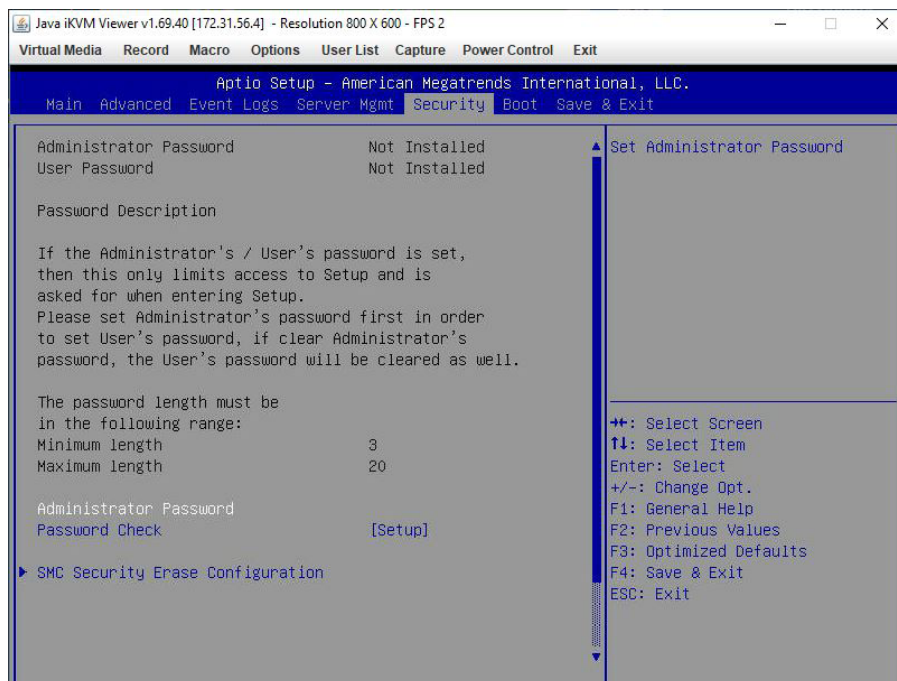
This feature allows you to select the source of the IP address for this computer. If Static is selected, you will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration Protocol) server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

****If the item above is set to Static, the following items will become available for configuration:***

- Station IPV6 Address
- Prefix Length
- IPV6 Router1 IP Address

4.6 Security

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



Administrator Password

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

User Password

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

Password Check

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

► Secure Boot

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

- System Mode
- Vendor Keys
- Secure Boot

Secure Boot

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

Secure Boot Mode

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

CSM Support

Select Enabled to support the EFI Compatibility Support Module (CSM), which provides compatibility support for traditional legacy BIOS for system boot. The options are **Enabled** and Disabled.

► Key Management

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

Provision Factory Default Keys

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

► Restore Factory Keys

Force System to User Mode. Install factory default Secure Boot key databases. The options are **Yes** and No.

► Reset to Setup Mode

This feature deletes all Secure Boot key databases from NVRAM. The options are **Yes** and No.

► Export Secure Boot variables

This feature allows you to copy NVRAM content of Secure boot variables to files in a root folder on a file system device. The options are **Yes** and No.

► Enroll EFI Image

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

Device Guard Ready

► Remove 'UEFI CA' from DB

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

► Restore DB defaults

Select Yes to restore the DB defaults.

Secure Boot Variable

► Platform Key (PK)

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

Details

Review details on current settings of the platform keys.

Export

This feature allows you to export Platform Keys to an available file system.

Update

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

Delete

Select Yes to confirm deletion of the Platform Key from NVRAM.

► Key Exchange Key

Details

Review details on current settings of the Key Exchange Keys.

Export

This feature allows you to export Key Exchange Keys to an available file system.

Update

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

Append

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

Delete

Select Yes to delete the Key Exchange Keys. Select No to delete only a certificate from the key database. The options are Yes and No.

► Authorized Signatures

Details

Review details on current settings of Authorized Signatures.

Export

This feature allows you to export Authorized Signatures to an available file system.

Update

Select Yes to load the factory default DB.' Select No to load the DB from a external file. The options are Yes and No.

Append

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

Delete

Select Yes to delete the Authorized Signatures key database. Select No to delete only a certificate from the key database. The options are Yes and No.

► Forbidden Signatures

Details

Review details on current settings of the Forbidden Signatures.

Export

This feature allows you to export Forbidden Signatures to an available file system.

Update

Select Yes to load the DBX factory default 'dbx.' Select No to load it from an external file. The options are Yes and No.

Append

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

Delete

Select Yes to delete the Forbidden Signatures key database. Select No to delete only a certificate from the key database. The options are Yes and No.

► Authorized TimeStamps

Details

Review details on current settings of the Authorized TimeStamps.

Export

This feature allows you to export Authorized TimeStamps to an available file system.

Update

Select Yes to load the DBT from the manufacturer's defaults. Select No to load the DBT from a file. The options are Yes and No.

Append

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

Delete

Select Yes to delete the Authorized TimeStamps key database. Select No to delete only a certificate from the key database. The options are Yes and No.

► OsRecovery Signature

This item uploads and installs an OsRecovery Signature. You may insert a factory default key or load from a file. The file formats accepted are:

- 1) Public Key Certificate
 - a. EFI Signature List
 - b. EFI CERT X509 (DER Encoded)
 - c. EFI CERT RSA2048 (bin)
 - d. EFI SERT SHA256 (bin)
- 2) EFI Time Based Authenticated Variable

When prompted, select **Yes** to load Factory Defaults or **No** to load from a file.

Details

Review details on current settings of the OsRecovery Signature.

Export

This feature allows you to export an OsRecovery Signature to an available file system.

Set New

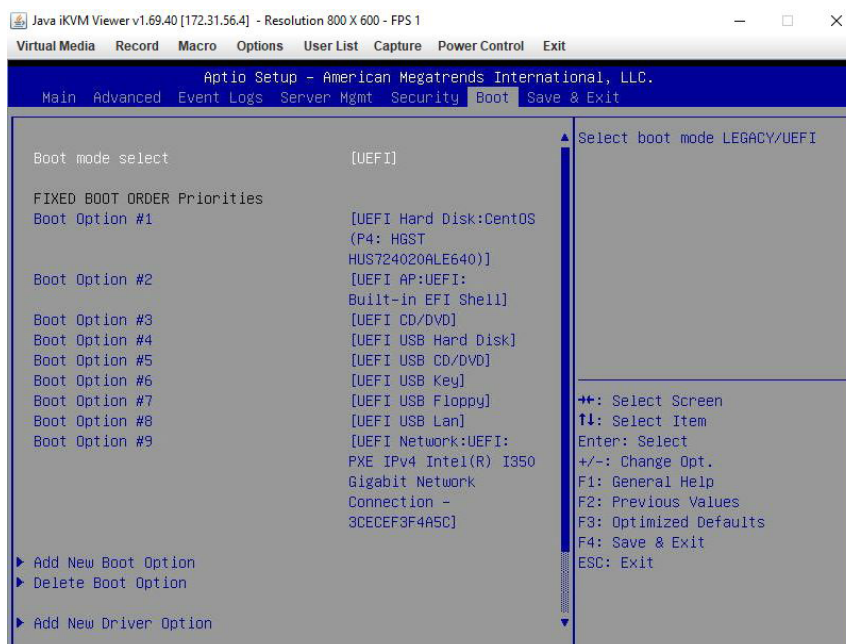
Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file. The options are Yes and No.

Append

This item uploads and adds an OsRecovery Signature into the Key Management. You may insert a factory default key or load from a file. When prompted, select **Yes** to load Factory Defaults or **No** to load from a file.

4.7 Boot

Use this feature to configure Boot settings.



Boot Mode Select

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

Legacy to EFI Support

Select Enabled to boot EFI OS support after Legacy boot order has failed. The options are **Disabled** and Enabled.

Fixed Boot Order Priorities

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

****If the item "Boot Mode Select" above is set to Legacy, UEFI, or Dual, the following items will be displayed:***

- Legacy/UEFI/Dual Boot Option #1
- Legacy/UEFI/Dual Boot Option #2
- Legacy/UEFI/Dual Boot Option #3
- Legacy/UEFI/Dual Boot Option #4
- Legacy/UEFI/Dual Boot Option #5

- Legacy/UEFI/Dual Boot Option #6
- Legacy/UEFI/Dual Boot Option #7
- Legacy/UEFI/Dual Boot Option #8
- UEFI/Dual Boot Option #9
- Dual Boot Option #10
- Dual Boot Option #11
- Dual Boot Option #12
- Dual Boot Option #13
- Dual Boot Option #14
- Dual Boot Option #15
- Dual Boot Option #16
- Dual Boot Option #17

► Delete Boot Option

This feature allows you to select a boot device to delete from the boot priority list.

Delete Boot Option

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

► UEFI Application Boot Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

► Network Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

****If any storage media is detected, the following items will become available for configuration:***

► Add New Boot Option

This feature allows you to add a new boot option to the boot priority features for the system.

Add Boot Option

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

Path for Boot Option

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

Boot Option File Path

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

Create

Use this item to set the name and the file path of the new boot option.

► UEFI USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

► USB Key Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

► UEFI Hard Disk Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

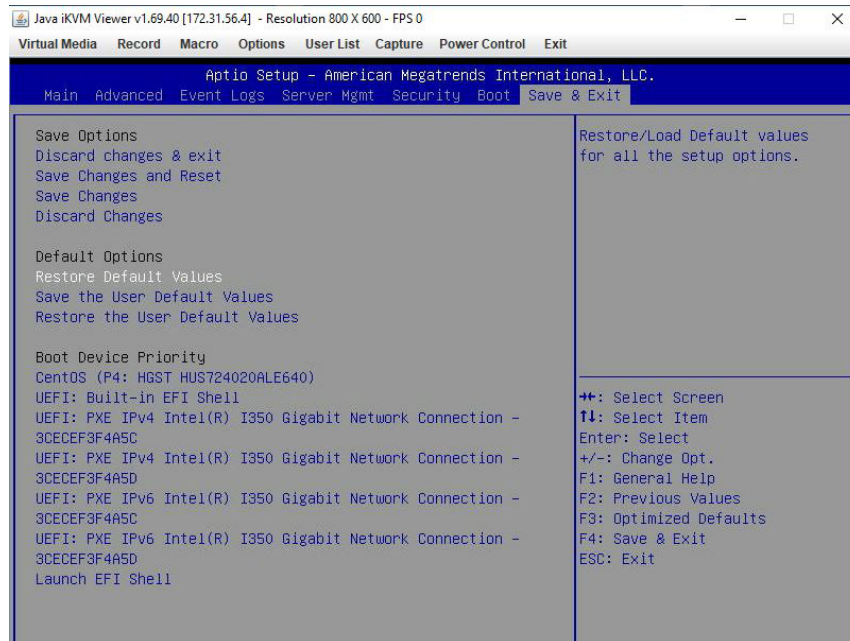
► Hard Disk Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

4.8 Save & Exit

Select the **Save & Exit** tab from the BIOS setup screen to configure the settings below:



Save Options

Discard Changes and Exit

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

Save Changes and Reset

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

Save Changes

When you have completed the system configuration changes, select this option to leave the BIOS setup utility and reboot the computer for the new system configuration parameters to take effect. Select Save Changes from the Save & Exit menu and press <Enter>.

Discard Changes

Select this option and press <Enter> to discard all the changes and return to the AMI BIOS utility program.

Default Options

Restore Optimized Defaults

To set this feature, select Restore Defaults from the Save & Exit menu and press <Enter>. These are factory settings designed for maximum system stability, but not for maximum performance.

Save As User Defaults

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

Restore User Defaults

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

Boot Override

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

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 and H13 series motherboards using BMC WEB GUI or SUM (Supermicro® Update Manager).



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

A.2 Updating Firmware Using BMC WEB GUI

In order to keep the system working properly, follow the steps 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.

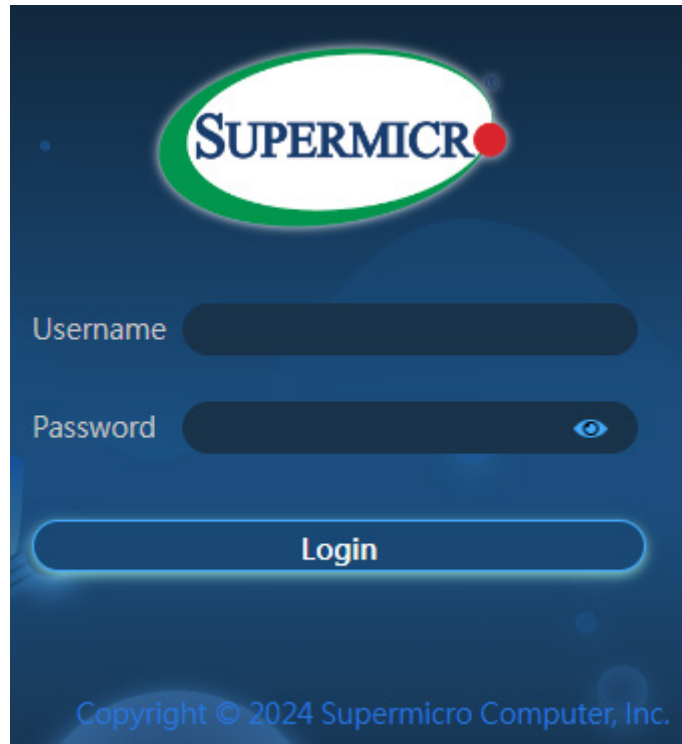


Figure 1: BMC Firmware Web User Login



Note: 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.

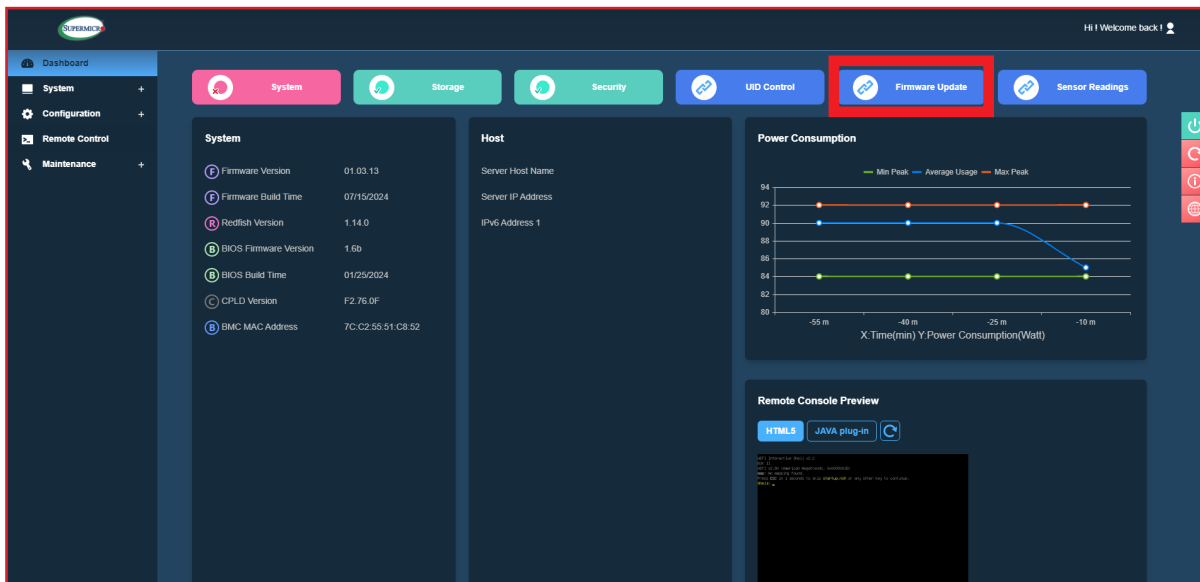


Figure 2: BMC Firmware Update Dashboard

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

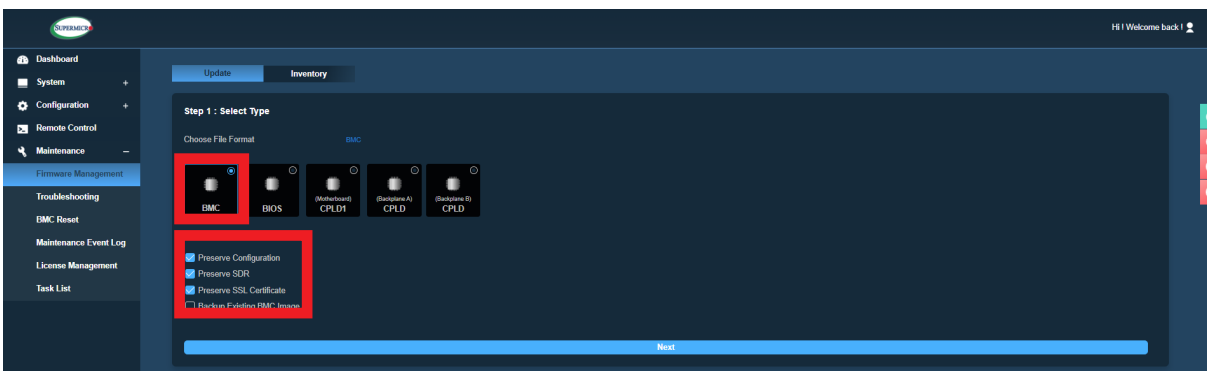


Figure 3: BMC Firmware Update Default Setting

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

The screenshot displays a two-step process for selecting and uploading a new BMC firmware file.

Step 1 : Select Type

Under "Choose File Format", the "BMC" option is selected. Other options like "BIOS", "(Motherboard) CPLD1", "(Backplane A) CPLD", and "(Backplane B) CPLD" are present but their selection controls are grayed out. A red dashed arrow points from a text box to these grayed-out options.

A text box in the upper right corner states: "Configurations are reserved for BMC firmware update and the selections are grayed out."

Under "Choose Requirement", the following options are checked with blue checkmarks:

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

A "Next" button is located at the bottom of Step 1.

Step 2 : Select File

Under "Select File", a "Select File" button is highlighted with a red rectangle. Below it are "Cancel" and "Upload" buttons.

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 "Backup existing image" option to backup existing BMC or BIOS image. The backup image will be used for auto-recovery in case of a firmware integrity check fails at any time. You can also manually recover BMC or BIOS from the backup image. Go to the inventory page to manually recover BMC or BIOS. 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.

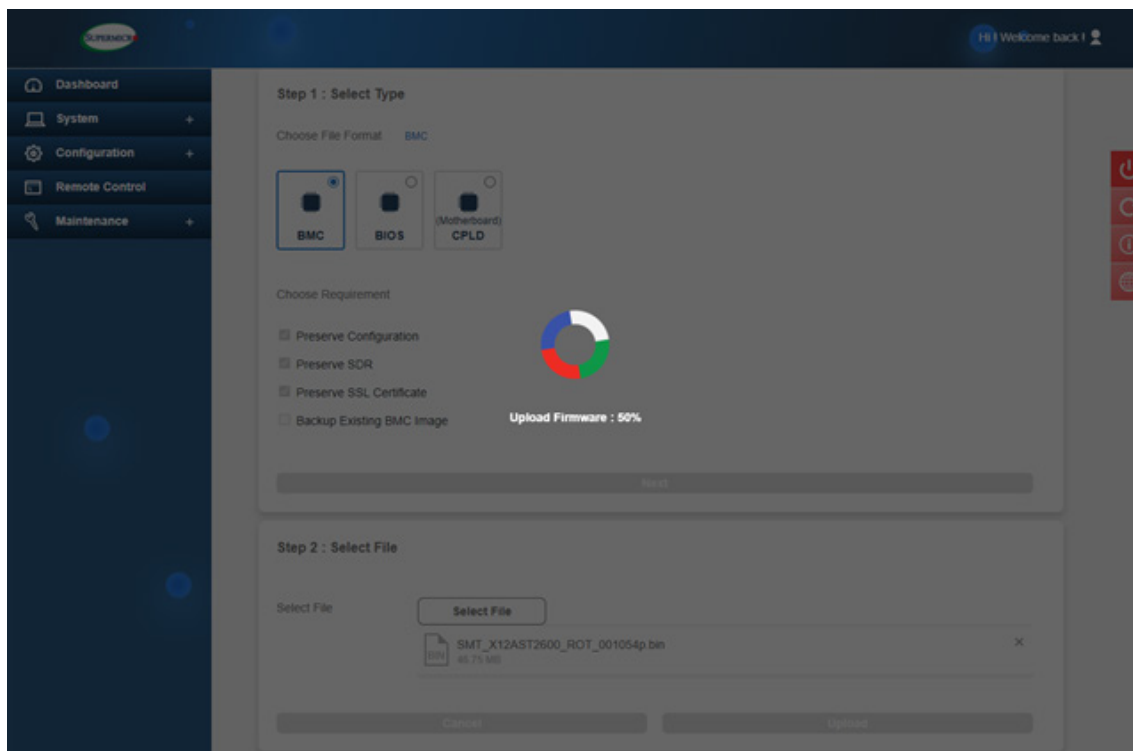


Figure 5: New BMC Firmware Uploading

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

The screenshot displays the BMC Firmware Update web interface. On the left is a navigation menu with 'Dashboard', 'System', 'Configuration', 'Remote Control', and 'Maintenance'. A 'FW Update Mode' banner indicates that configuration changes are not recommended during the update. The main content area has tabs for 'BMC', 'BIOS', and 'CPLD'. Under 'BMC', there are checkboxes for 'Preserve Configuration', 'Preserve SDR', 'Preserve SSL Certificate', and 'Backup Existing BMC Image'. A 'Next' button is below these options. 'Step 2: Select File' shows a file named 'SMT_X12AST2600_ROT_001054p.bin' (45.75 MB) selected, with 'Cancel' and 'Upload' buttons. 'Step 3: File Version' contains a table comparing the existing and new firmware versions. The 'New Version' field is highlighted with a red box, showing '00.10.54'. Below the table are 'Cancel' and 'Update' buttons, with the 'Update' button also highlighted with a red box.

Name	Existing Version	New Version
BMC	00.10.53	00.10.54

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.

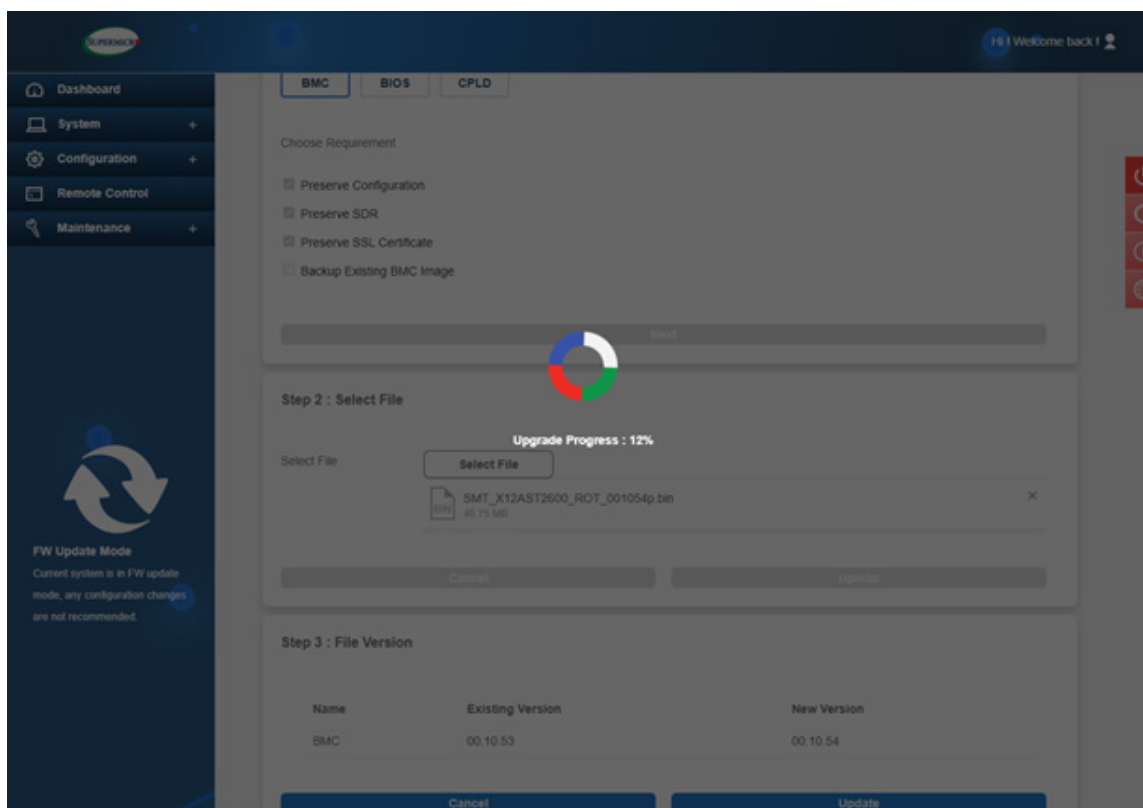


Figure 7: BMC Firmware Updating in Progress

8. BMC will reboot after the firmware is completely updated. 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.

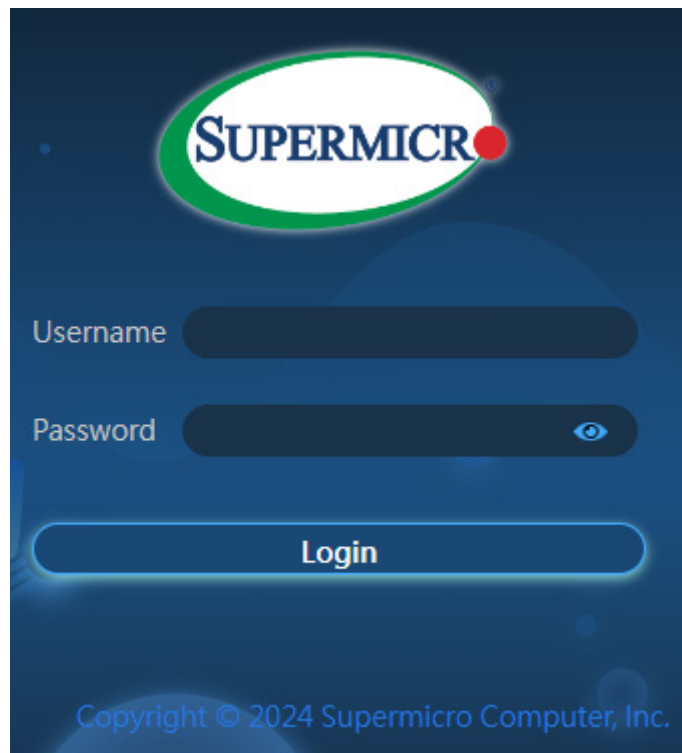


Figure 8: BMC Firmware Web User Login

A.3 Updating Firmware Using SUM

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

Step 1: Installing SUM

To install SUM in Linux/FreeBSD OS, follow 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 updating will be displayed as shown below. DO NOT interrupt the process until it is complete. BMC will reboot after the firmware is completely updated. Wait for BMC to complete the system reboot. For an example, refer to 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>
```



```
SUM_HOME]# ./sum -I Redfish_HI -u ADMIN -p XXXXXX -c UpdateBmc --file
SMCI_BMC.rom
```

[illegible]

Figure 10: Output of BMC Local Update in SUM

Appendix B

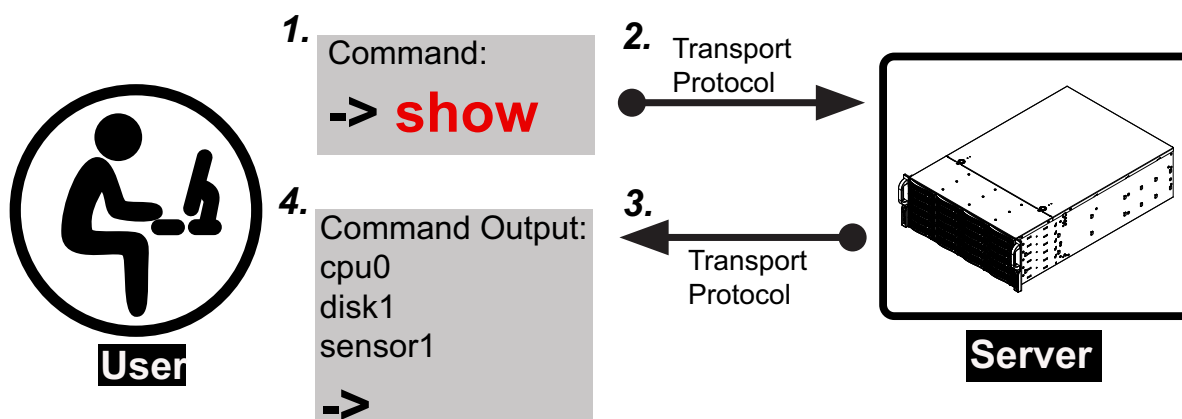
Introduction to SMASH

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 the IT professionals to effectively manage multi-system clusters, minimize power consumption, and achieve system management efficiency.



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, 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

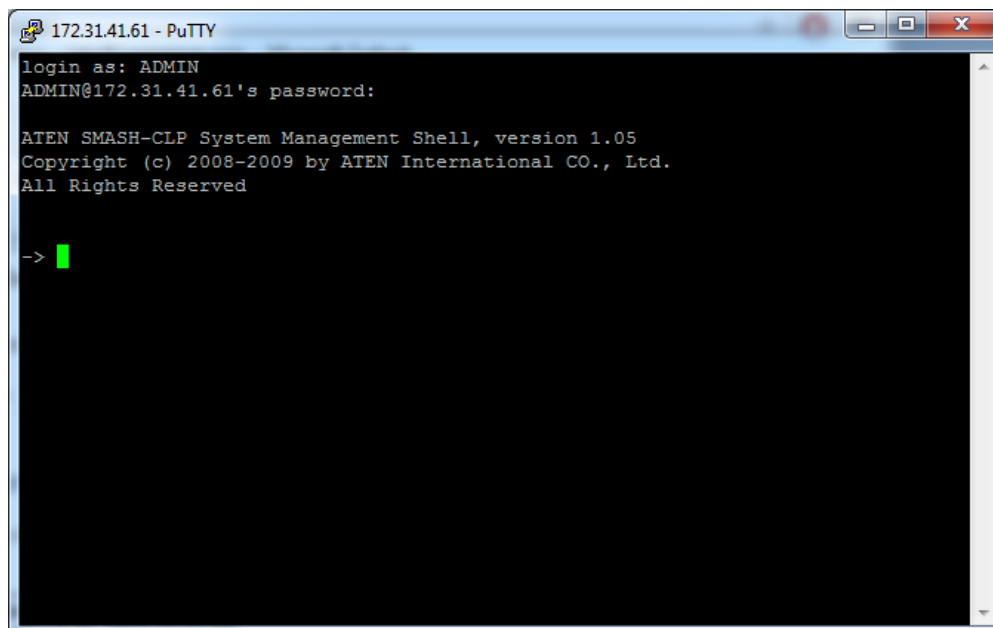
1. Use 'ssh<BMC ip address>'.
2. Enter the password.

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 logged in the SSL network, the SMASH Command Line Protocol Main screen will display as shown below.

A screenshot of a PuTTY terminal window titled "172.31.41.61 - PuTTY". The terminal displays the following text: "login as: ADMIN", "ADMIN@172.31.41.61's password:", "ATEN SMASH-CLP System Management Shell, version 1.05", "Copyright (c) 2008-2009 by ATEN International CO., Ltd.", "All Rights Reserved", and a prompt "-> " followed by a green cursor. The terminal has a black background and white text.

```
172.31.41.61 - PuTTY
login as: ADMIN
ADMIN@172.31.41.61's password:
ATEN SMASH-CLP System Management Shell, version 1.05
Copyright (c) 2008-2009 by ATEN International CO., Ltd.
All Rights Reserved
-> 
```

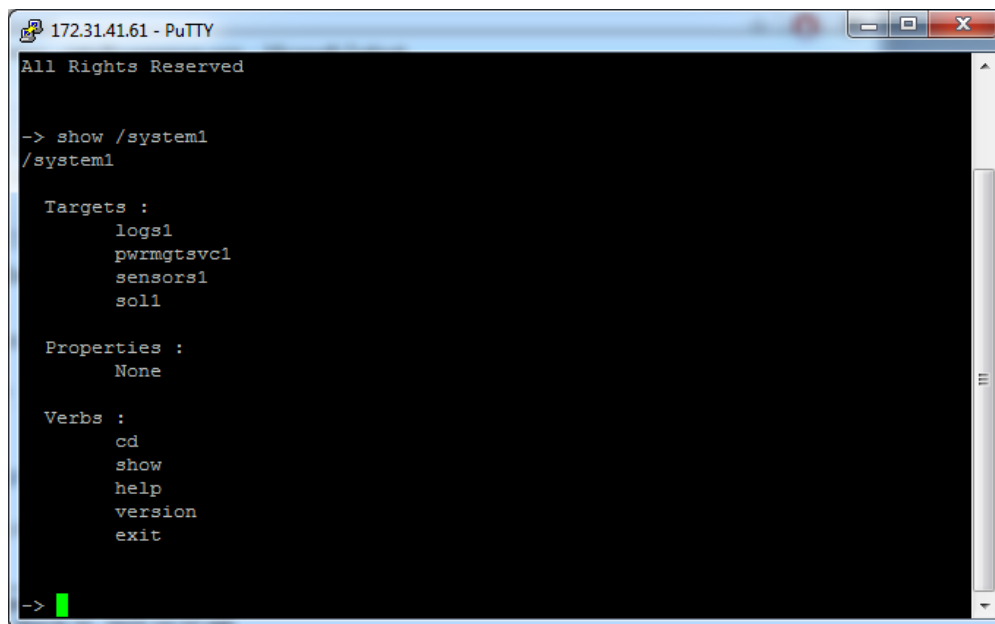
SMASH-CLP Main Screen

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 are 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

-> █
```

Using SMASH for System Management

B.7 Definitions of Commands Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow you to issue commands to a target system to perform certain tasks. For example, the verbs supported by the *admin* target group include: *cd*, *help*, *load*, *dump*, *create*, *delete*, *exit*, *version*, *show*, etc.

- ***cd***

The command verb *cd* is used to navigate to a specific target address using the SSL protocol. For example, issuing the command *cd/admin1* will direct you to the target *admin* (AdminDomain).

- ***show***

The command verb *show* is used to display the properties and the contents of a target, a group of targets, a sub-groups of the target(s). Properties, contents, supported operations related to the target, the group of targets or their sub-targets will be displayed.

- ***exit***

The command verb *exit* is used when you want to exit from a SMASH session or close a session.

- ***help***

The command verb *help* is used when you want to get helpful hints or information on a context-specific 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, to stop a process, or to change an operation state from a higher level to a lower level.

- ***reset***

The command verb *reset* is used to enable or to disable the power control of or the processes of the machine.

- ***delete***

The command verb *delete* is used to delete or to 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

SMASH Commands

B.9 Standard Command Options

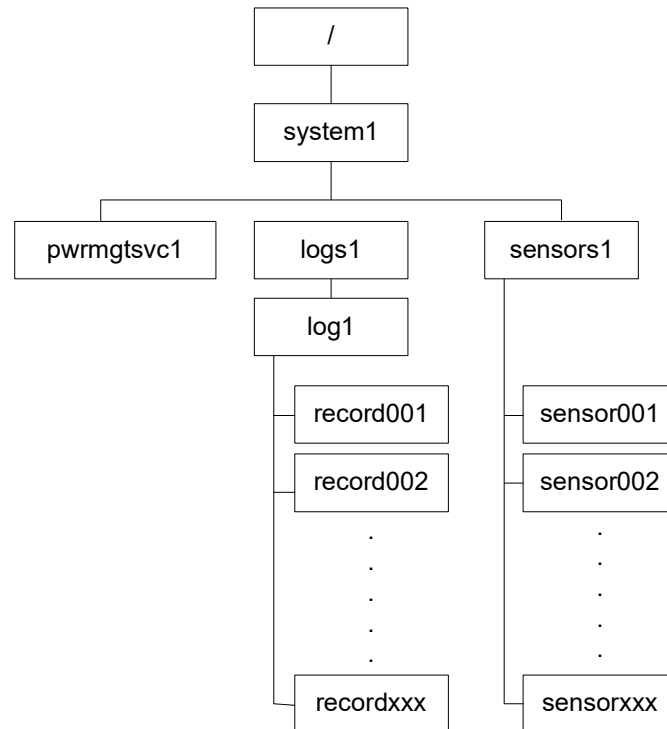
The following table lists the standard command options.

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													

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.



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, use the unique password provided by Supermicro to log in. Afterward, the unique password can be changed to the customer's chosen username and password for subsequent logins.

For more information regarding BMC passwords, visit our website at <http://www.supermicro.com/bmcpassword>.

C.2 Notice and Shipping Label Identifier

Every server that has a BMC unique password will include a notice in the plastic wrap on the top side of the plastic wrap as well as an identifier on its shipping label.



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)

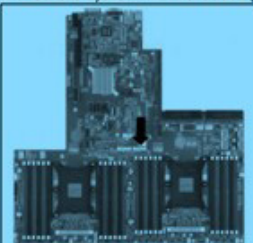


Figure 2: BMC barcode labels located on the motherboard
2. On the system service tag or chassis (label locations will vary depending on system model)



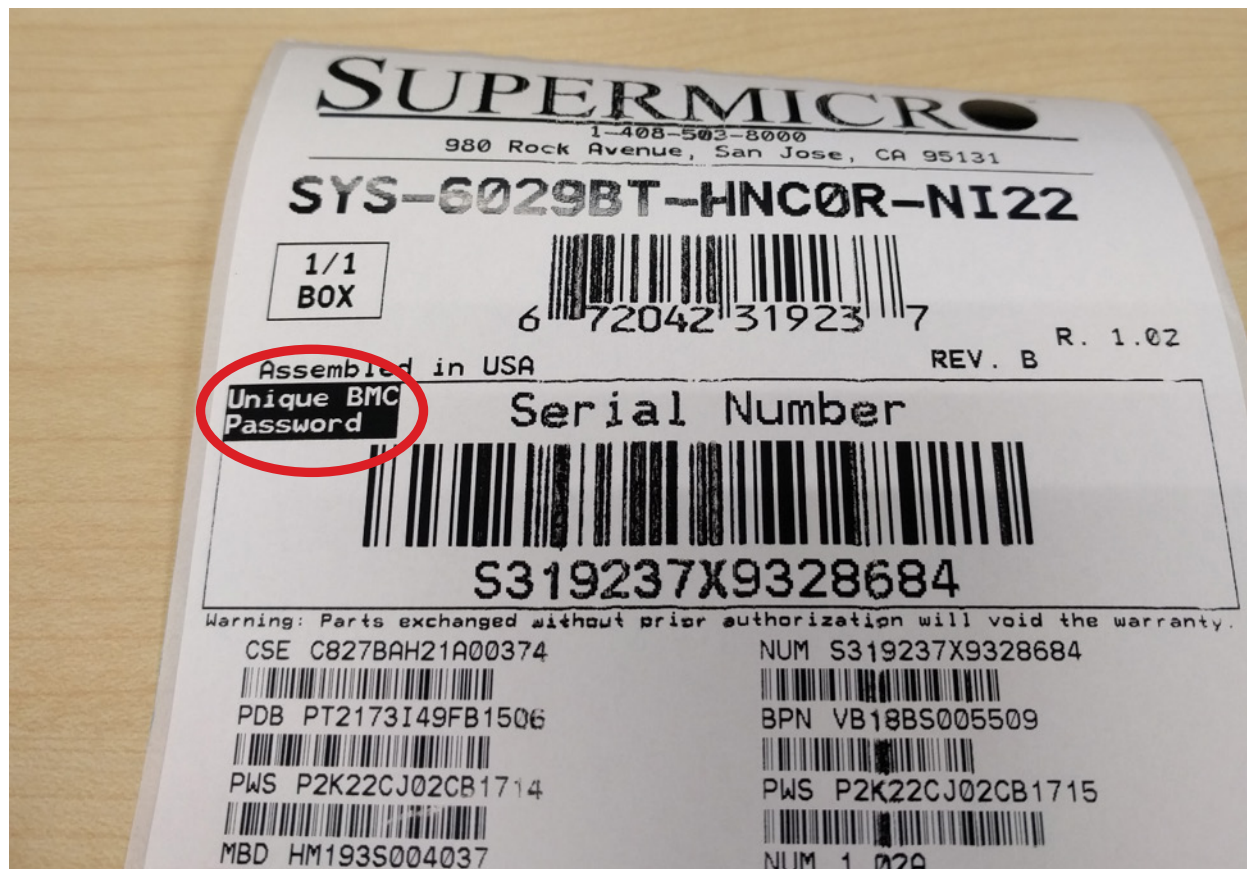



Figure 3: BMC barcode label located on the chassis service tag and chassis

For assistance or more information, contact Supermicro Technical Support online at www.supermicro.com/support

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 lower case 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.

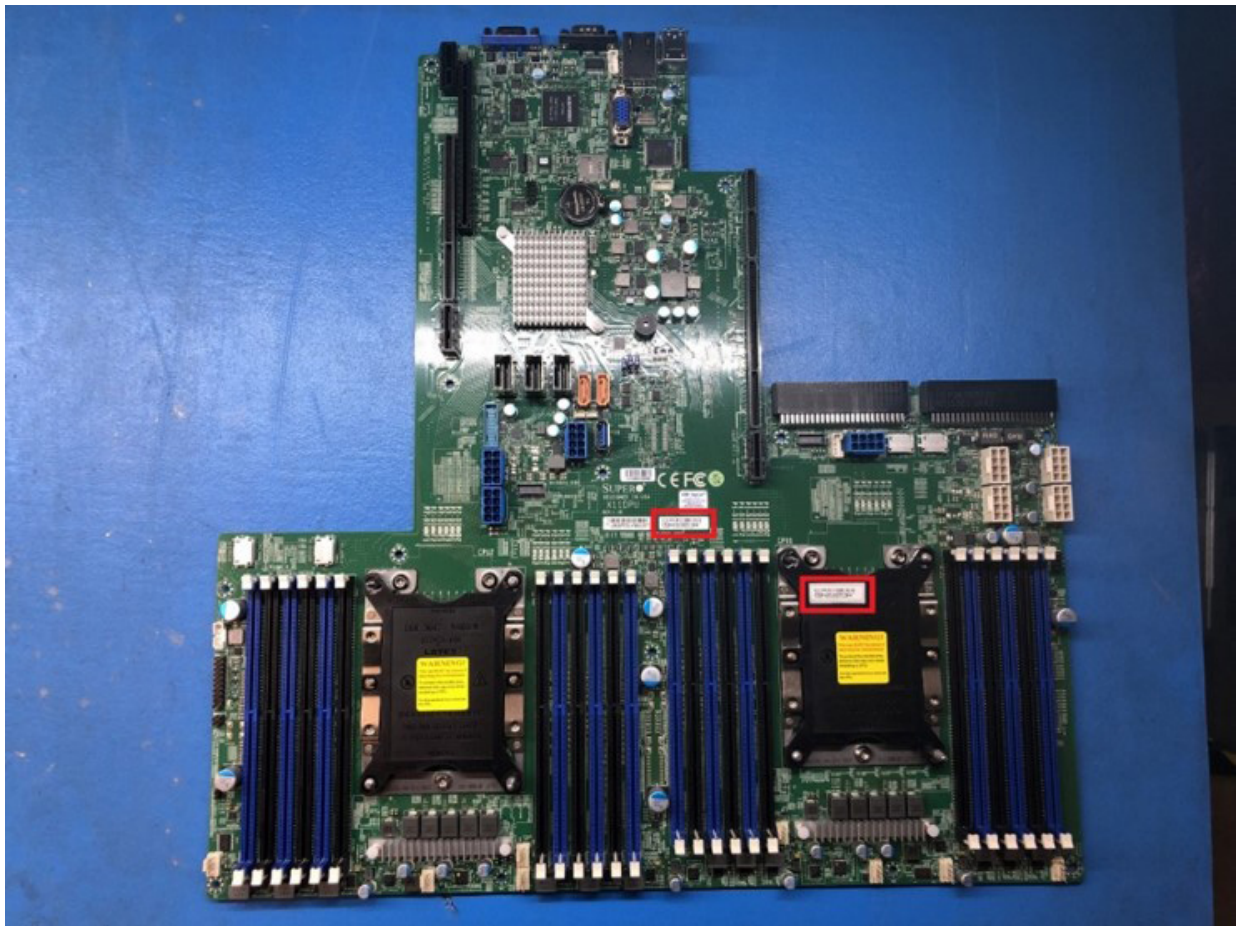
Most systems have a pull-out tag to display the BMC MAC address and the preprogrammed unique password. The rest of the systems will have the sticker on top/front of the chassis.



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



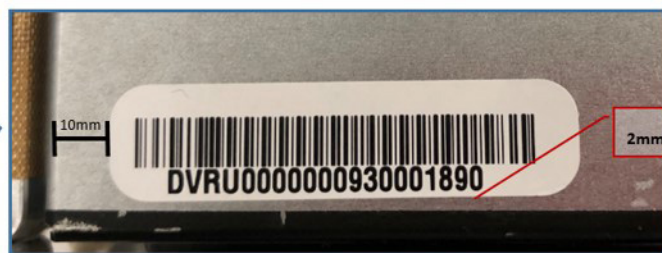
Label on the opposite side of the service tag



Label on the opposite side of the service tag



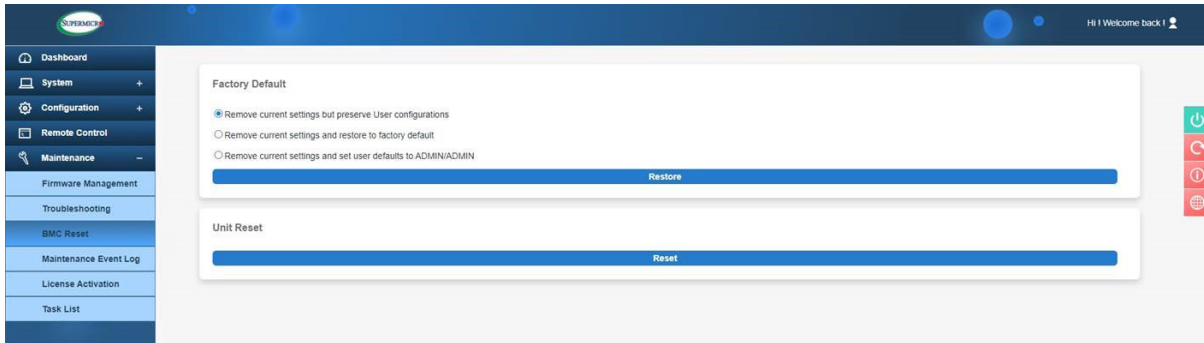
Label on the opposite side of the service tag



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 configuration to factory default. It will remove all users and reset ADMIN user password to factory default password.
- Remove current settings and set user defaults to ADMIN/ADMIN: This option will restore all the configuration to factory default. It will remove all users and reset 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 incidence, 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, 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 datacenter. How do I change all of the unique preprogrammed passwords for these systems in an efficient manner to support my operations?

Answer: Contact the systems integrator (SI) or value-added reseller (VAR) to assist you in this process.

Question: Can Supermicro apply a single unique customer-specified password for all my systems? Will this comply with SB327?

Answer: All systems from Supermicro will ship with a unique preprogrammed password. Customers will be able to change the password on each system. In order for Supermicro to comply with SB327, we are not able to use customer-specified passwords. All passwords will be unique and assigned at the time of manufacturing.

Question: When will my motherboard have this change rolled out?

Answer: Supermicro plans to have new stickers rolled out starting mid-December 2019.

Appendix D

Remote Attestation

D.1 Overview

Supermicro trusted supply chain assurance offers to verify the identity of Supermicro server that is received by the customer matches with what Supermicro has manufactured. IT administrator and security teams can confidently deploy servers in data centers after validating the servers manufactured by Supermicro and unexpected modifications have not occurred during the journey from Supermicro to datacenters.

To ensure smooth Day One operation, it is highly recommended that your systems are verified using Supermicro's system attestation process. Attestation will detect any changes in the composition of your hardware and firmware through cryptographic signing, thereby guaranteeing the state of your server, while identifying and reporting any unauthorized changes.

D.2 License Requirements

An Enterprise SFT-SDDC-SINGLE license is required to perform attestation. You may inquire about this license through your Supermicro sales representative.

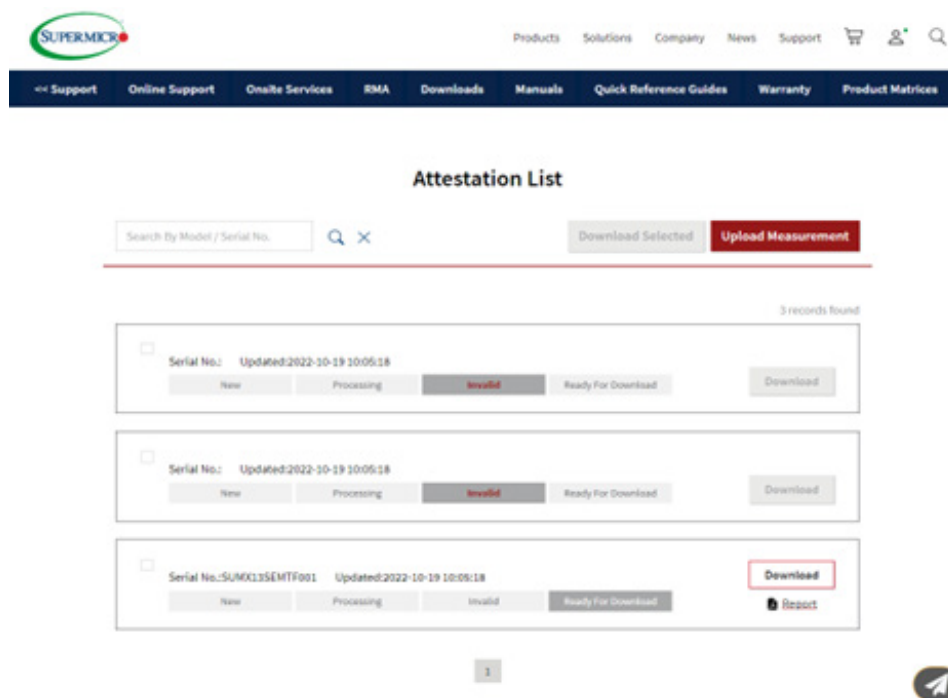
D.3 Attest Your System Using the Supermicro Website

Follow these steps to attest your system:

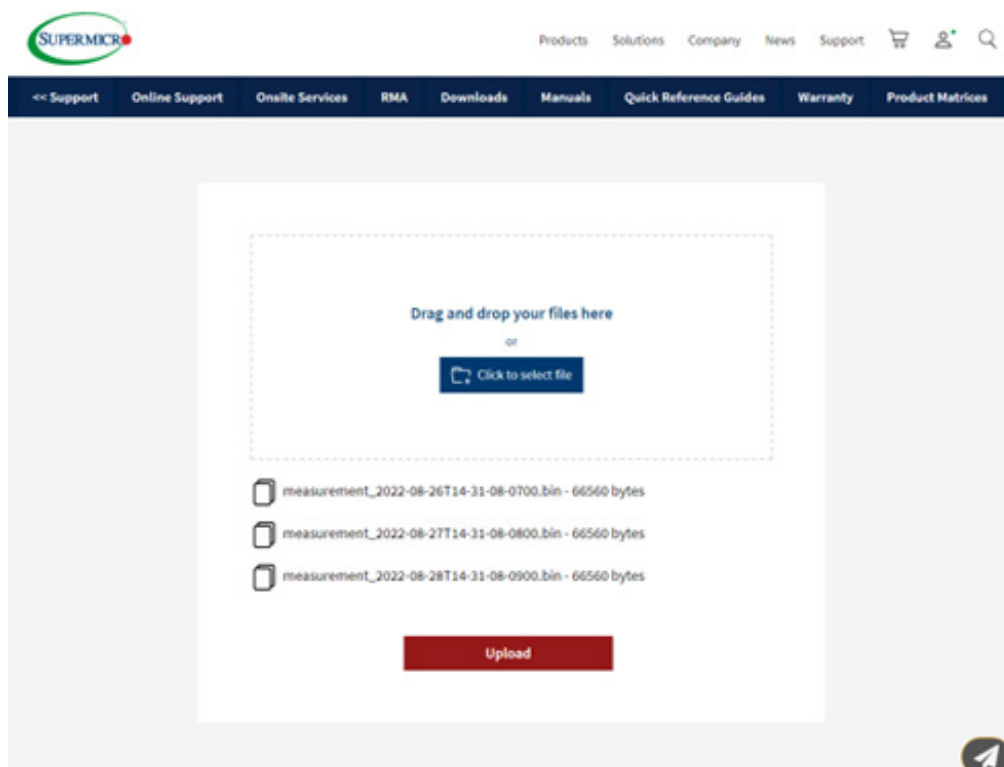
1. Run Supermicro Update Manager (SUM) to create a measurement file containing your current system configuration. Use command below to get the measurement dump from your system.

```
sum -i <BMC IP> -u <BMC_USER> -p <BMC_USER_PASSWORD> -c Attestation  
--dump --file <MEASUREMENT_FILE>
```

2. Log in to the Attestation Portal at <https://www.supermicro.com/attestation>.



3. Upload the measurement file obtained in step 1 to the Measurement Validation Server, which will compare the configuration to Supermicro's reference manifest file.



4. Download the verification report that compares the uploaded measurements with Supermicro's reference manifest. The verification report includes:

- System components
- Firmware
- FRU

See sample report below.



980 Rock Avenue
San Jose, CA 95131
USA
Phone: (408) 503-8000 Fax: (408) 503-8008

Comparison Report

Date 01/09/2023

Get All - Not Match :

No.	Uploaded Data	Reference Data
1	BIOS ME Board ID: SPS	BIOS ME Board ID: EagleStream SPS
2	BIOS ME Rollback ID	Not Found
3	Not Found	Staging BIOS ME Board ID

SMBIOS - All Match

FRU - All Match

In addition to an interactive web interface, you may also use the Attestation RESTful API to automate the process using your own script.

D.4 Attest Your System Using RESTful APIs

Bearer Authentication

Token Generation

Users need to generate bearer token from <https://www.supermicro.com/attestation> using a web browser. Tokens expire after 60 minutes.

User of Token

There should be generated token included to the API request header. **Authorization Bearer <token>**

API Calls

Refresh Tokens

To refresh the token data, take utilize the following.

Method: GET

End Point: <https://rots.supermicro.com/api/v1/attestation/refreshtoken>

Request Params: None

Sample query: <https://rots.supermicro.com/api/v1/attestation/refreshtoken>

List of Attestation Data

To query all attestation data by pagination, utilize the following.

Method: GET

End Point: <https://rots.supermicro.com/api/v1/attestation>

Request Json: (Optional)

```
{
  "pagination": {
    "offset": 20,
    "limit": 10,
    "order_by": "serial_no",
    "asc_desc": "desc"
  }
}
```

Response Json: Users need to generate bearer token from <https://www.supermicro.com/> attestation using a web browser before using these RESTful APIs.

```
{
  "data": [
    {
      "uuid": "163690ab-749e-4dd2-bbbd-41c10d8befc8",
      "upload_name": "measurement.bin",
      "serial_no": "SUMX13SEMTF001",
      "status": "Ready for Download",
      "ref_manifest_base64": "...",
      "report_log_base64": "...",
      "last_updated": "2022-10-13 19:55:40"
    }
  ],
  "pagination": {
    "offset": 20,
    "limit": 10,
    "order_by": "last_updated",
    "asc_desc": "desc"
  }
}
```

Query Attestation Data

To query individual Attestation Data by UUID or serial number, utilize the following data. You may attest an entire system and/or motherboard by using the appropriate serial number. The report is base64 encoded and must be decoded before use.

Method: GET

End Point:

<https://rots.supermicro.com/api/v1/uuid/{uuid}>

<https://rots.supermicro.com/api/v1/sn/{sn}>

Request Json: None

Response Json:

Upload Attestation Data

To upload base64-encoded measurement file to query and validate against RoTS, utilize the following.

Method: POST

End Point:

<https://rots.supermicro.com/api/v1/upload>

Request Json:

```
{
  "data": [
    {
      "upload_name": "measurement1.bin",
      "measurement_base64": "...."
    },
    {
      "upload_name": "measurement2.bin",
      "measurement_base64": "...."
    },
    {
      "upload_name": "measurement3.bin",
      "measurement_base64": "...."
    }
  ]
}
```

Response Json:

```
{
  "data": [
    {
      "upload_name": "measurement1.bin",
      "uuid": "163690ab-749e-4dd2-bbbd-41c10d8befc8",
      "status": "New",
      "last_updated": "2022-10-13 19:55:40"
    },
    {
      "upload_name": "measurement2.bin",
      "uuid": "193690ab-749e-4dd2-bbbd-41c10d8becs3",
      "status": "New",
      "last_updated": "2022-10-13 19:55:36"
    },
    {
      "upload_name": "measurement3.bin",
      "uuid": "188690ab-749e-4dd2-bbbd-41c10d8bell1",
      "status": "Processing",
      "last_updated": "2022-10-13 19:55:32"
    }
  ]
}
```

(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.