



BMC

Baseboard Management Controller

USER'S MANUAL

Revision 1.0a

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 1.0a

Release Date: March 25, 2022

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

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

Printed in the United States of America

Preface

About This Manual

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

User's Guide Organization

Chapter 1 provides an overview of the ASPEED AST2600 controller. It also introduces the features and 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, please refer to our website at <https://www.supermicro.com/products/nfo/IPMI.cfm> 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 the user's computer may or may not look exactly like the screen shown in this user's guide.

Conventions Used in the Manual

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



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



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



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



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

Contacting Supermicro

Headquarters

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

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

Email: marketing@supermicro.com (General Information)
support@supermicro.com (Technical Support)

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@supermicro.nl (General Information)
support@supermicro.nl (Technical Support)
rma@supermicro.nl (Customer 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: support@supermicro.com.tw

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 Applicable or Supported Platforms.....	16
1.6 Special Notes for Motherboard and Firmware Support	17

Chapter 2 Configuring the BMC Settings

2.1 Configuring UEFI BIOS	18
2.2 Configuring the IP/MAC Addresses for Remote Servers	29
2.3 Connecting to the Remote Server.....	30
2.4 Accessing the Remote Server Using the Browser.....	31
2.5 BMC Dashboard.....	32
2.6 System.....	37
2.7 Configuration	66
2.8 Remote Control	102
2.9 Maintenance	137

Chapter 3 Frequently Asked Questions

Chapter 4 UEFI BIOS

4.1 Introduction.....	179
4.2 Main Setup	180
4.3 Advanced Setup Configurations.....	182
4.4 Event Logs	212
4.5 IPMI	214
4.6 Security.....	217
4.7 Boot	223
4.8 Save & Exit.....	226

Appendix A Firmware Update via WEB GUI and SUM

A.1 Overview.....	228
A.2 Updating Firmware Using BMC WEB GUI.....	229
A.3 Updating Firmware Using SUM.....	237

Appendix B Introduction to SMASH

B.1 Overview.....	241
B.2 An Important Note to the User.....	242
B.3 Using SMASH	242
B.4 Initiating the SMASH Protocol.....	243
B.5 SMASH-CLP Main Screen	244
B.6 Using SMASH for System Management.....	245
B.7 Definitions of Commands Verbs.....	246
B.8 SMASH Commands	248
B.9 Standard Command Options.....	249
B.10 Target Addressing	250

Appendix C RADIUS Configuration

C.1 Overview.....	252
C.2 Configuring a User Account in Ubuntu.....	252
C.3 Configuring Client Account in Ubuntu	253
C.4 Starting the RADIUS Server Ubuntu.....	253
C.5 Adding Roles in Windows	254

Appendix D Unique Password for BMC

D.1 Overview.....	259
D.2 Notice and Shipping Label Identifier	260
D.3 Label Specifications	262
D.4 Restore Factory Default	268
D.5 Change All Unique Passwords Using Script.....	268
D.6 Frequently Asked Questions	269

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 the users to access, monitor, diagnose, and manage a remote server via Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

1.2 Overview of the ASPEED AST2600 BMC

The ASPEED AST2600 BMC is designed to interface with the host system via PCI-Express connections to communicate with the graphics core for the X12 and H12 series motherboards. Designed for the X12 series, the AST2600 connects with the host system via PCI-Express Gen2 x1 bus to communicate with the graphics core. It supports a 64-bit 2D Graphics Accelerator with 32-bit memory and 16-bit I/O space.

Additionally, AST2600 supports USB 1.1 and 2.0 for remote KVM emulation and 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 DDR4 Memory Interface

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

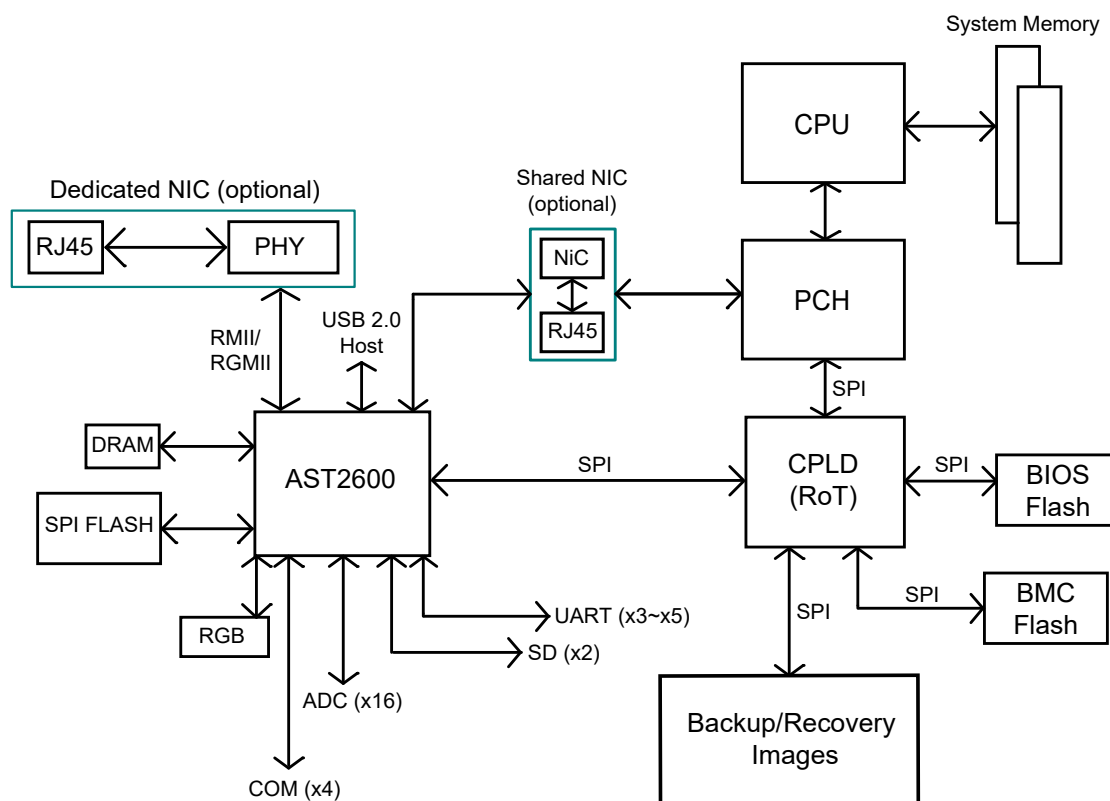
1.3 Supermicro BMC Features

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

- Update Firmware through browser and OS
- OS-indentation
- KCS Privilege Control
- Unique pre-programmed password
- Redfish

AST2600 Block Diagram

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



Note: This block diagram is for the X12 and H12 series motherboards.

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-SPM-LIC: Advanced Power Management

It can be used as an SPM (Supermicro Power Manager) tool.

- 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.

- SFT-DCMS-SVC-KEY: SSM Call-Home Support

Please 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) support- ed with OOB license)	✓	✓	✓
Shared NIC (LOM, LAN1 with automatic failover)	✓	✓	✓
Dedicated NIC	✓	✓	✓
VLAN tagging	✓	✓	✓
IPv4	✓	✓	✓
IPv6	✓	✓	✓

DHCP	✓	✓	✓
Dynamic DNS	✓	✓	✓
KCS	✓	✓	✓
LAN over USB	✓	✓	✓
Unique pre-programmed default password	✓	✓	✓
HW Root of Trust	✓	✓	✓
Signed BMC/BIOS images	✓	✓	✓
Host secure communication (LAN over USB)	✓	✓	✓
User account management and Role-based authority (User, Operator, Administrator)	✓	✓	✓
SSL Redirection	✓	✓	✓
SSL Encryption (HTTPS)	✓	✓	✓
IP Access Control	✓	✓	✓
SNMPv3.0	✓	✓	✓
AD / LDAP		✓	✓
RADIUS	✓	✓	✓
PK authentication (for SSH)	✓	✓	✓
KCS Control	✓	✓	✓
Port Configuration	✓	✓	✓
UEFI Secure Boot			✓
System Lock down			✓
TEE-OS	✓	✓	✓
BIOS/BMC automatic recovery (ROT)			✓
Disk secure erase of internal storage devices (For Broadcom controller connected drives)			✓
Power control	✓	✓	✓
Boot configuration	✓	✓	✓
Serial-over-LAN	✓	✓	✓
Virtual Media	✓	✓	✓
Virtual Console	✓	✓	✓
HTML5 access to Virtual Console	✓	✓	✓
HTML5 VM			✓
Virtual Console collaboration (3 users)	✓	✓	✓
Remote Keyboard Operation	✓	✓	✓

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

Remote configuration (Mousemode, Fanmode, Radius, AD, NTP, 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 Applicable or Supported Platforms

This BMC server and firmware applies to X12 and H12 platforms. Supported platforms include the following.

- X12DPi-N(T)6
- X12DPU-6
- X12DDW-A6
- X12DPT-B6
- X12DPG-QT6
- X12DPFR-AN6
- X12DGO-6
- X12DPD-A6M25
- X12DPG-OA6
- B12DPT-6
- X12DAi-N6
- X12DHM
- X12SPi-TF
- X12SPW-F/TF
- X12SPO-F/NTF
- X12SPM-LN4F/LN6TF/TF
- X12SPL-F/LN4F
- X12SPA-TF
- H12DSG-O-CPU
- H12SSW-iNR/NTR
- H12SSL-i/C/CT/NT
- H12DSG-Q-CPU6

- H12SSFR-AN6
- H12SSFF-AN6
- M12SWA-TF
- H12DGO-6
- H12SSW-AN6
- H12DSi-6/NT6
- H12SSG-6
- BH12SSi-M25
- H12DSU-iN
- H12SSW-iN/NT
- H12DST-B
- H12SST-PS

1.6 Special Notes for Motherboard and Firmware Support

For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI BIOS, TAS, and IPMIView, please refer to our website at <https://www.supermicro.com/products/nfo/IPMI.cfm> for details.

Please 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 the users 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 <http://www.supermicro.com/products/nfo/ipmi.cfm>. This section provides detailed information on how to configure BMC settings.



Note: Some features might not be available if the users are using an X12 motherboard as a few newer features are not supported by this generation.

2.1 Configuring UEFI BIOS

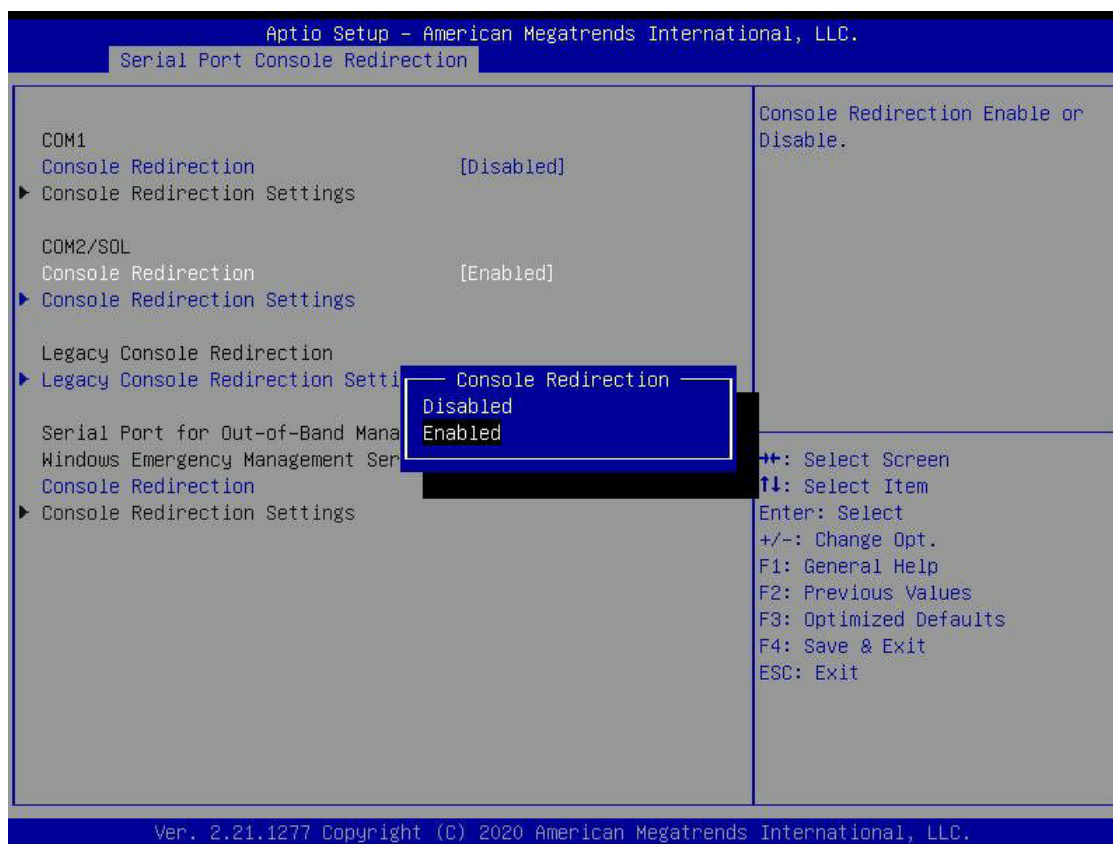
Before configuring the BMC, follow the instructions below to configure the system UEFI BIOS settings.

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>.

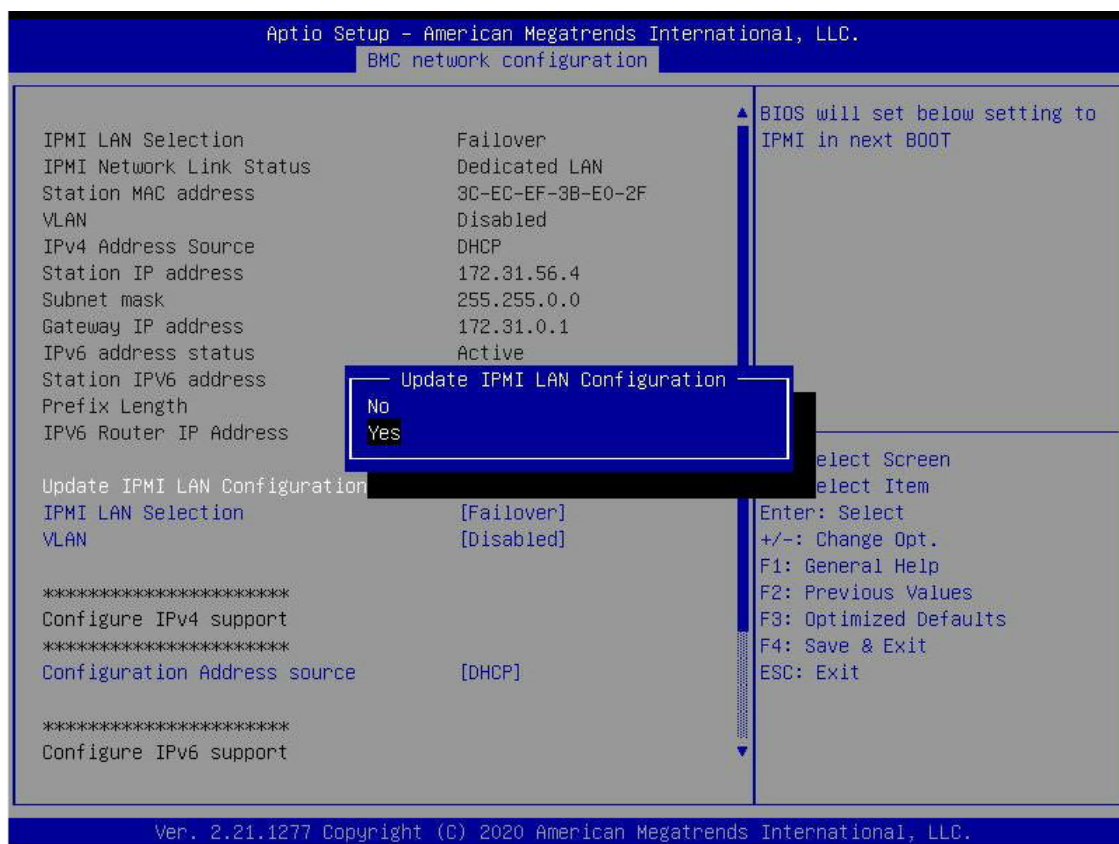
Enabling the COM port for SOL (BMC)

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].

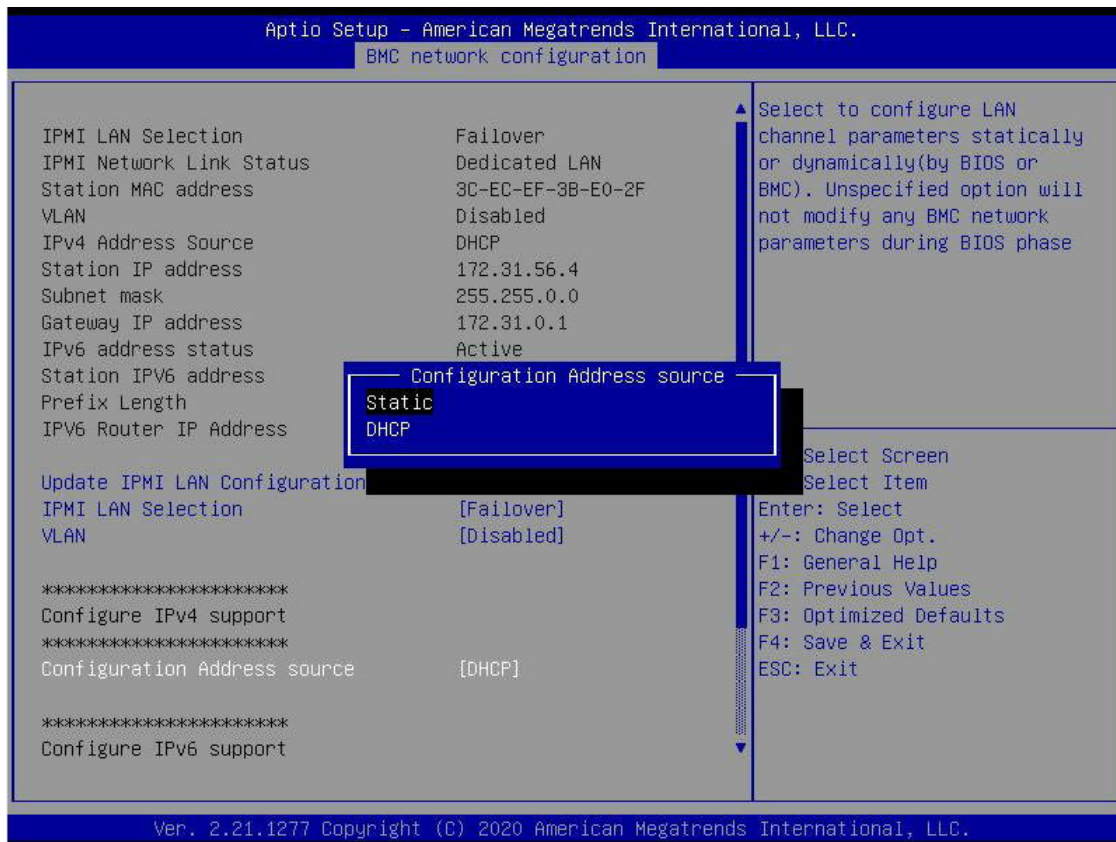


Configuring IP Address Using the UEFI BIOS

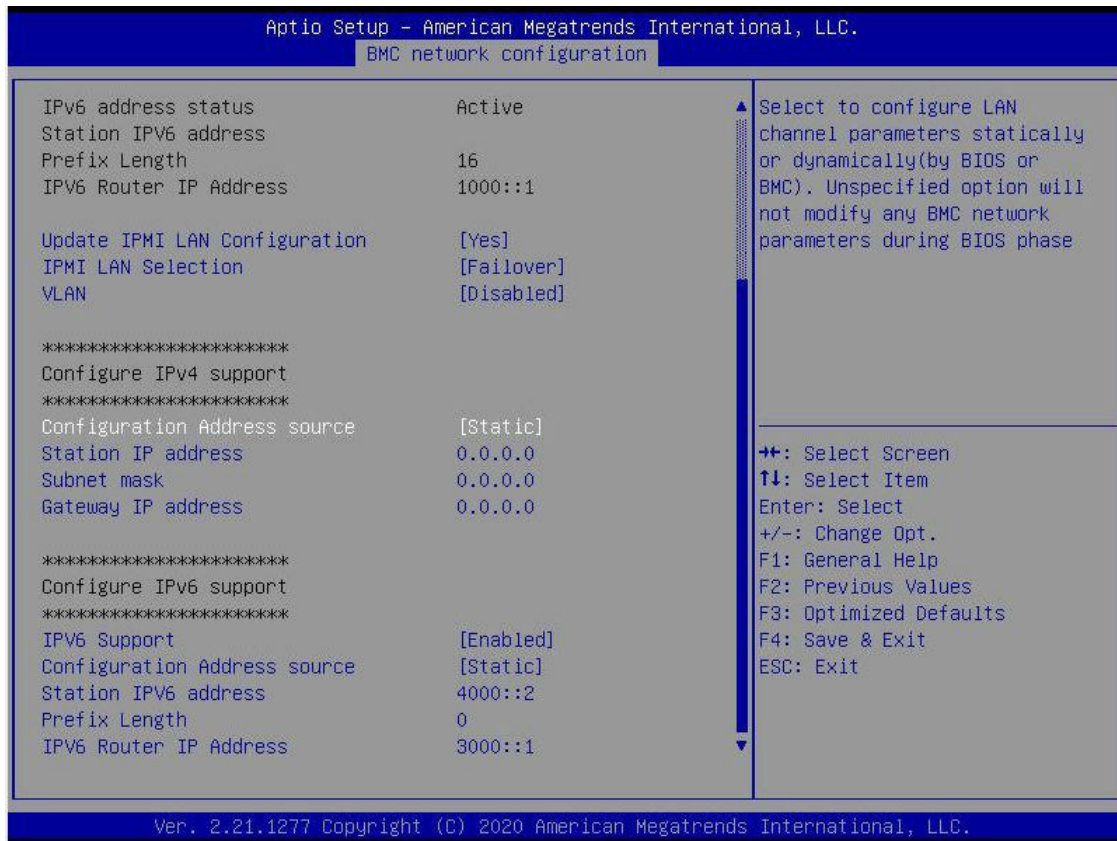
1. Select the *Server Management* tab.
2. Select *BMC Network Configuration* and press <Enter>.
3. Highlight *Update IPMI LAN Configuration*, press <Enter> and select [Yes].



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



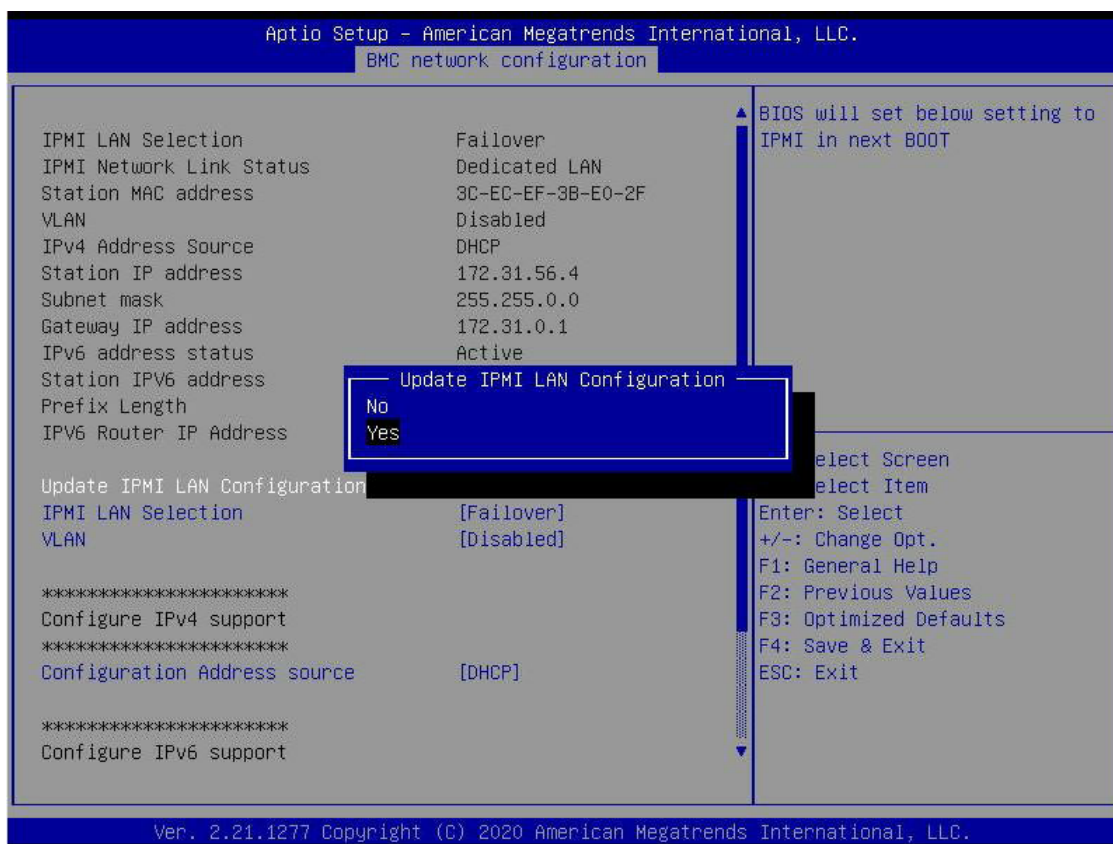
- Once the Configuration Address Source is set to [Static], the Station IP Address, Subnet Mask, and Gateway IP Address fields will display 0.0.0.0, which indicates that these fields are ready for the users to change to new values. Select each of the three items and enter the values. Press <Enter> when finished.



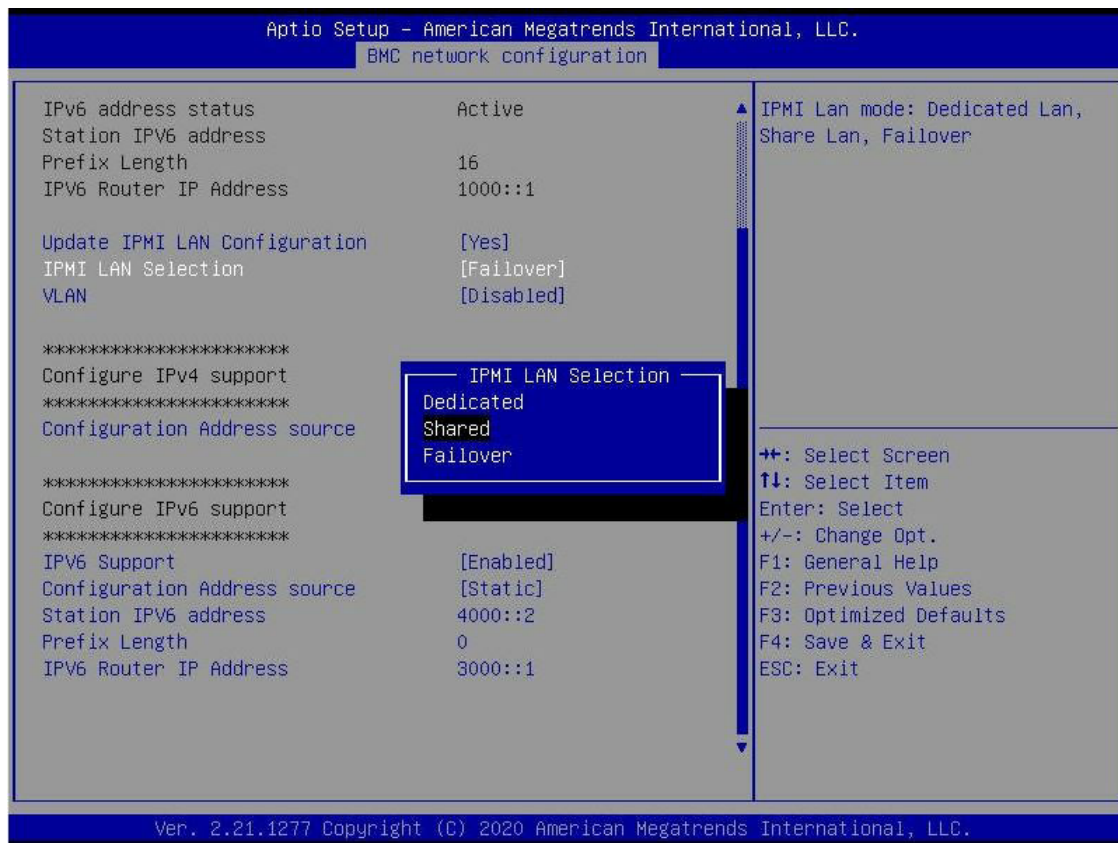
Connecting to BMC Using the UEFI BIOS

1. Plug Cat 5 cable into Linux Laptop.
2. Plug the other end of the cable into the IPMI / SHARED port.
3. In Linux Laptop, configure Network settings for Static IP, and assign IP (such as 192.168.0.4) and subnet. Gateway IP does not matter since there's no router/switch in between.
4. Launch Superserver ending and press DEL key to enter into UEFI BIOS setup.
5. Use the arrow key to navigate to *Server Management*.
6. Select *BMC Network Configuration*.

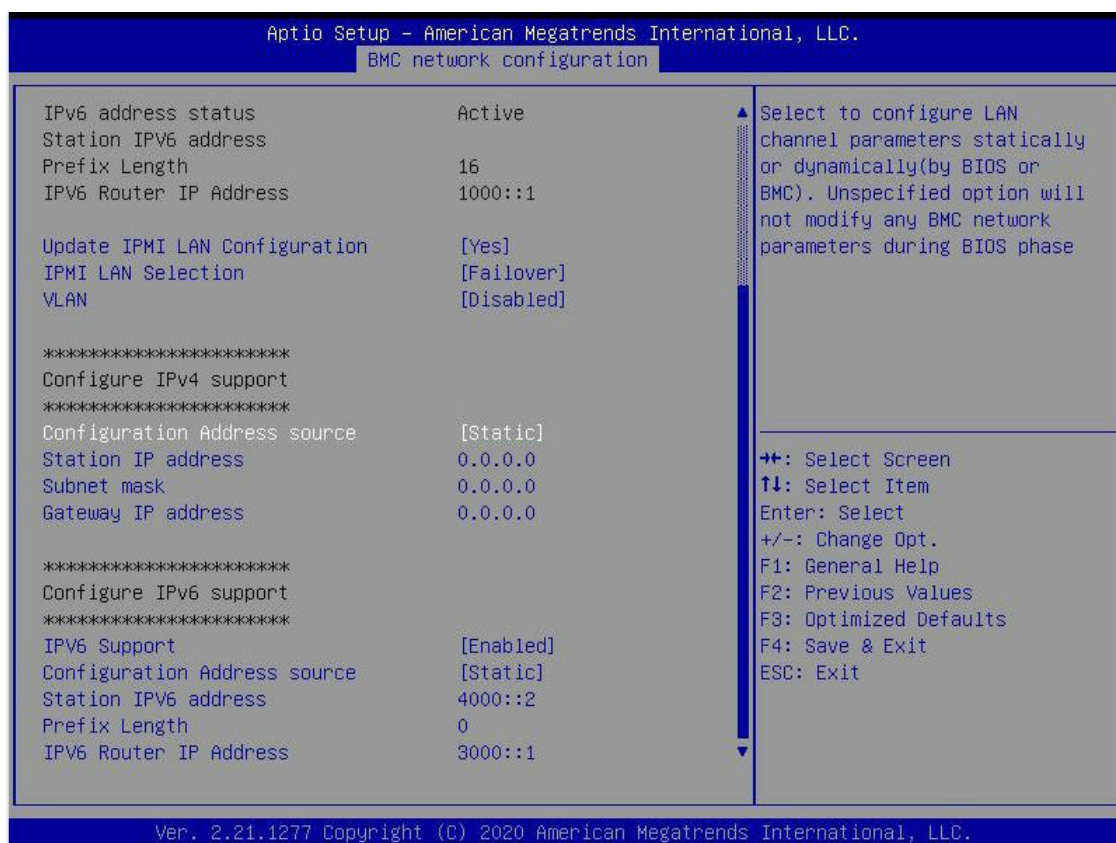


7. Select *Update IPMI LAN Configuration* and select [Yes].

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

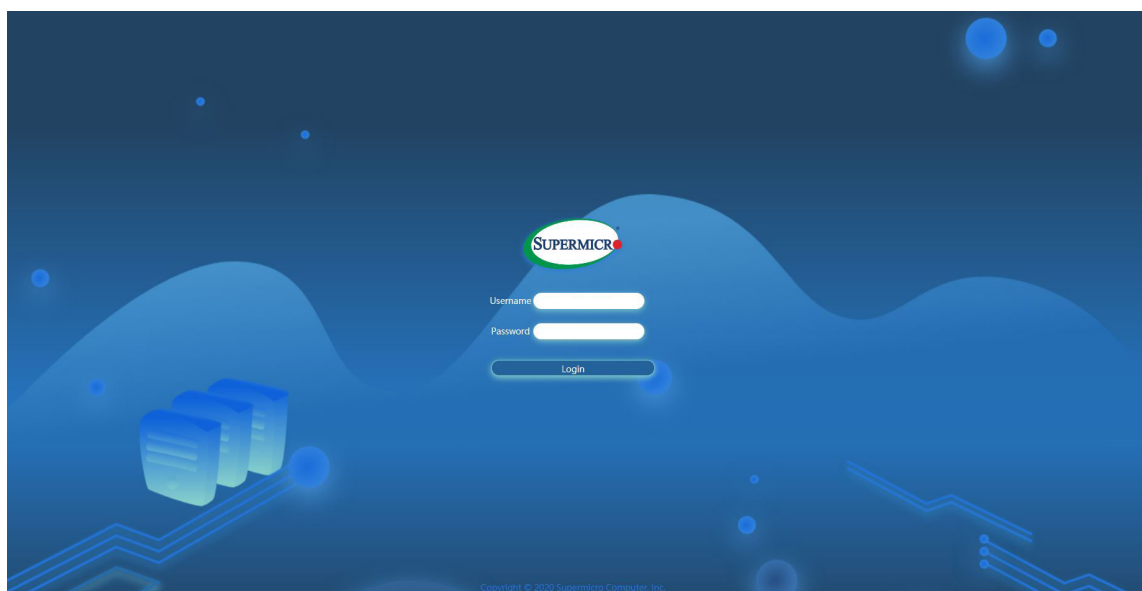


9. Navigate to *Configuration Address Source* and select [Static]. Then the users can assign an IP (such as 192.168.0.4) and subnet.

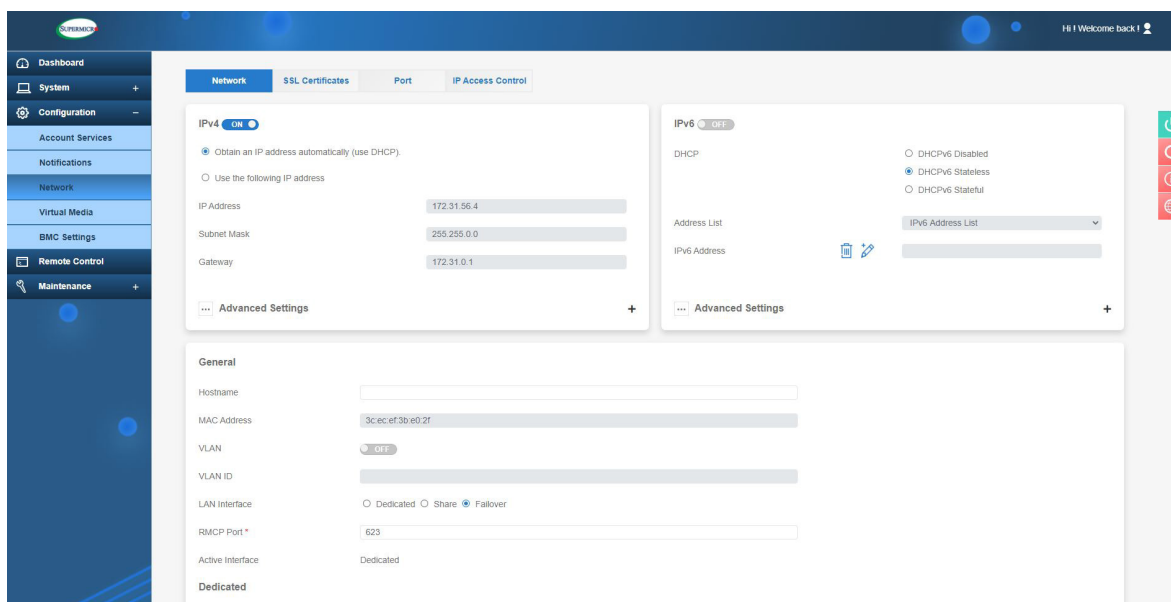


Now that both Laptop and the BMC are on the same subnet. With the static IP connected, they should be able to communicate. To establish the connection, please follow the steps below.

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



- After logging in, go over to <Network> under <Configuration>. Users can then see all the IPV6 info to configure.



2.2 Configuring the IP/MAC Addresses for Remote Servers



Note: The DHCP (Dynamic Host Configuration Protocol) is on by default. To change the manufacturer default setting, please use the ipmicfg utility or the UEFI BIOS Setup utility.

1. Run the ipmicfg utility. The users can get this from the Supermicro website at www.supermicro.com.
2. Follow the instructions given in the readme.txt file to configure Gateway IP/Netmask IP addresses, enable/disable DHCP, and configure other BMC settings.

IPMICFG Version 1.20.3 © 2020 Super Micro Computer, Inc.

Usage: IPMICFG Parameters

-m	Show IP and MAC
-m IP	Set IP (format: ###.###.###.###)
-a MAC	Set MAC (format: #:#:#:#:#::#)
-k	Show Subnet Mask
-k Mask	Set Subnet Mask (format: ###.###.###.###)
-dhcp	Get the DHCP status
-dhcp on	Enable the DHCP
-dhcp off	Disable the DHCP
-g	Show Gateway IP
-g IP	Set Gateway IP (format: ###.###.###.###)
-r	BMC cold reset option: -d Detected BMC device for BMC reset
-garp on	Enable the Gratuitous ARP
-garp off	Disable the Gratuitous ARP
-fd	Reset to the factory default option: -d Detected BMC for BMC reset
-fdl	Reset to the factory default (Clean LAN) option: -d Detected BMC for BMC reset
-fde	Reset to the factory default (Clean FRU and LAN) option: -d Detected BMC for BMC reset
-ver	Get Firmware revision
-vlan	Get VLAN status
-vlan on <vlan tag>	Enable the VLAN and set the VLAN tag. If VLANtag is not given it uses previously saved values.

2.3 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 the users wants 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.

Using IPMIView to Connect to the Remote Server

1. Connect a LAN cable to the onboard LAN1 port or the dedicated BMC LAN port.
2. Choose a computer that is connected to the same network and open the IPMIView utility.
3. Go to File>New>System. Enter the System Name, IP Address of LAN1 (or the dedicated LAN) and the Description in the appropriate fields, and press <Enter>.
4. Select the system from the BMC Domain. Enter the Login ID and Password in the appropriate fields to log in to the IPMIView with utility.



Note 1: The default network setting is "Failover", which will allow the BMC to connect to the network through a shared LAN port (onboard LAN Port 1 or 0) or through the BMC Dedicated LAN Port. If the BMC must be connected through a specific port, please change the LAN configuration setting under the Network Settings.

Note 2: For the BMC to work properly, please enable all onboard USB ports and the COM port designated for SOL (BMC) on the motherboard. All USB ports and the COM port for BMC (marked with "**") are **enabled** in the system UEFI BIOS by default. It is usually listed as COM1 or COM2 in the UEFI BIOS. Refer to Section 2-1 Configuring UEFI BIOS for more information.

2.4 Accessing the Remote Server Using the Browser

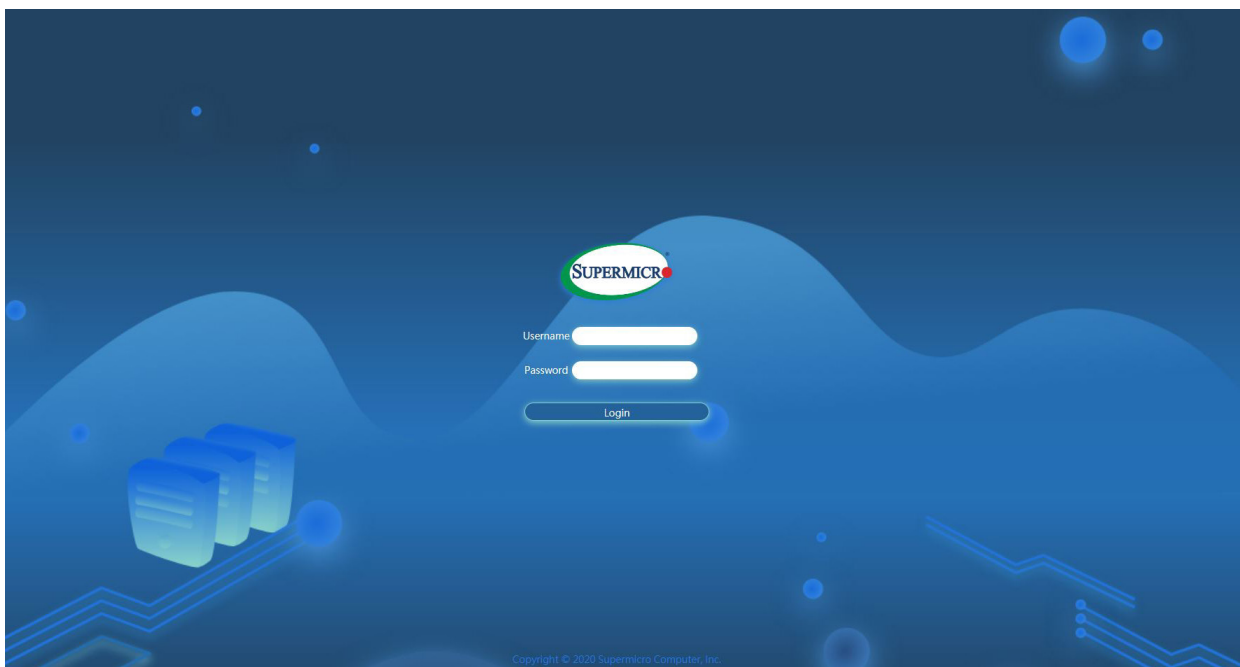
To Log In to the Remote Console

Users can login with local BMC user credentials or as a user from Active Directory, LDAP, or RADIUS. They will be able to navigate pages based on assigned user privilege. Once the users are connected to the remote server via browser, the following BMC login screen will display.



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

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



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

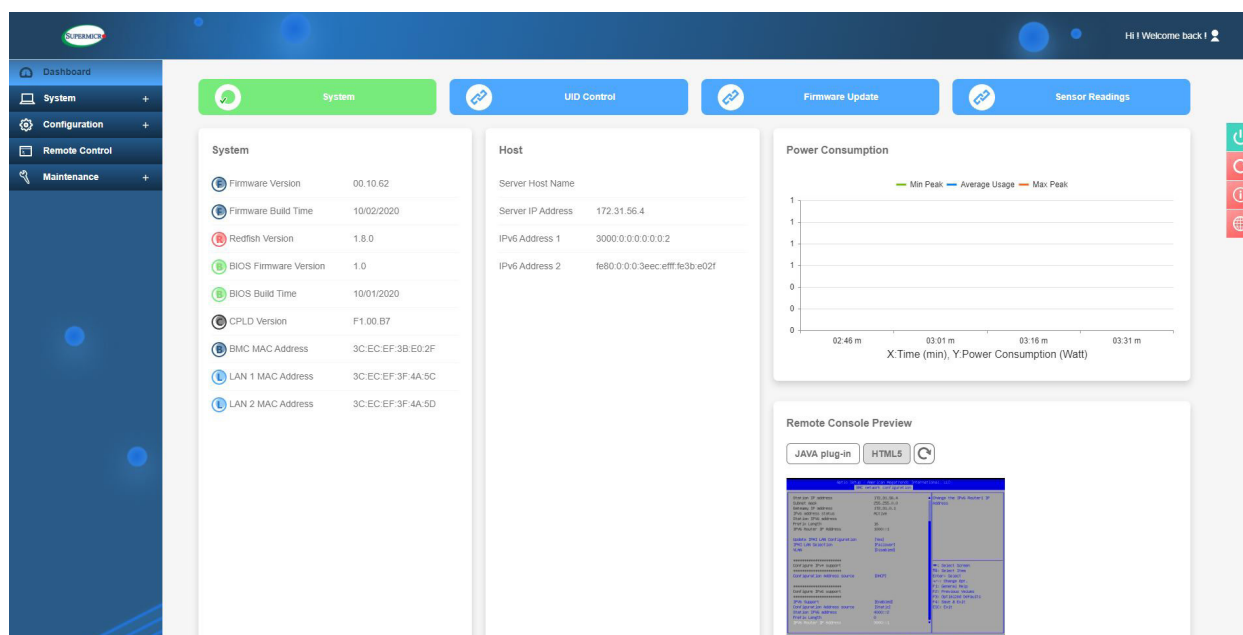


Note 1: To use the IPMIView utility for Console Redirection, please refer to the IPMI-View User's Guide for instructions.

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

2.5 BMC Dashboard

The BMC Dashboard provides an overview of the system overview, host information, power consumption, and system health. It also has quick links to access 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 the users will also be able to access Storage from here. This page will be displayed as shown below.



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



Information includes:

- User
- Role
- Server
- Logout

The following WebGUIs indicate different purposes.



: Power Control



: Refresh



: Help



: Language

Power Options

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

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



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

Refresh

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

Help

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

Language

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

- English
- Simplified Chinese
- Japanese

The BMC Main displays the following information.

Quick Links

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

- System: Users can navigate to the System page.
- Storage: Users can navigate to the Storage page if a storage component is connected.
- UID Control: Users can navigate to the UID Control page to turn on or off LED blinking to identify the server.
- Firmware Update: Users can navigate to Firmware Management page to update firmware.
- Sensor Readings: Users can navigate to Sensor Readings page.

System Health

This section contains the overall system health status notifications. Users 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

Users can find an overall storage component health status notification in this section if a storage component is connected. Click on the health status to get more details about 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 the respective storage component(s) installed.

System

This section displays a brief summary of the system components such as FW version, FW Build Time, Redfish Version, BIOS FW Version, BIOS Build Time, CPLD Version, BMC MAC Address, and LAN MAC Addresses.



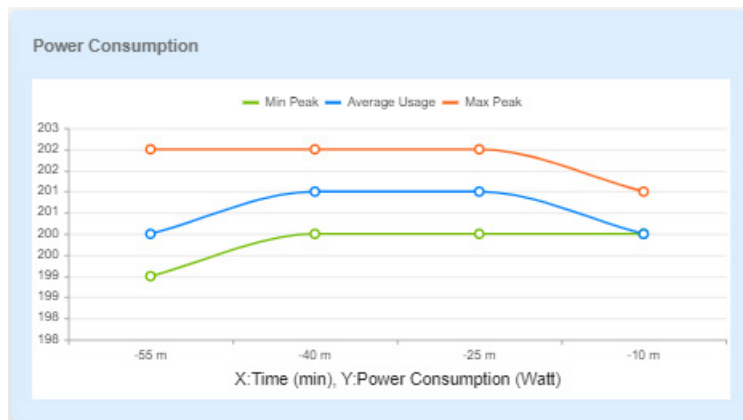
Note: In special motherboards without onboard LANs, AOC NIC information is displayed in place of onboard LANs. In addition, no System LAN interfaces will be shown if LAN interfaces are not detected.

Host

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

Power Consumption

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



Remote Console Preview

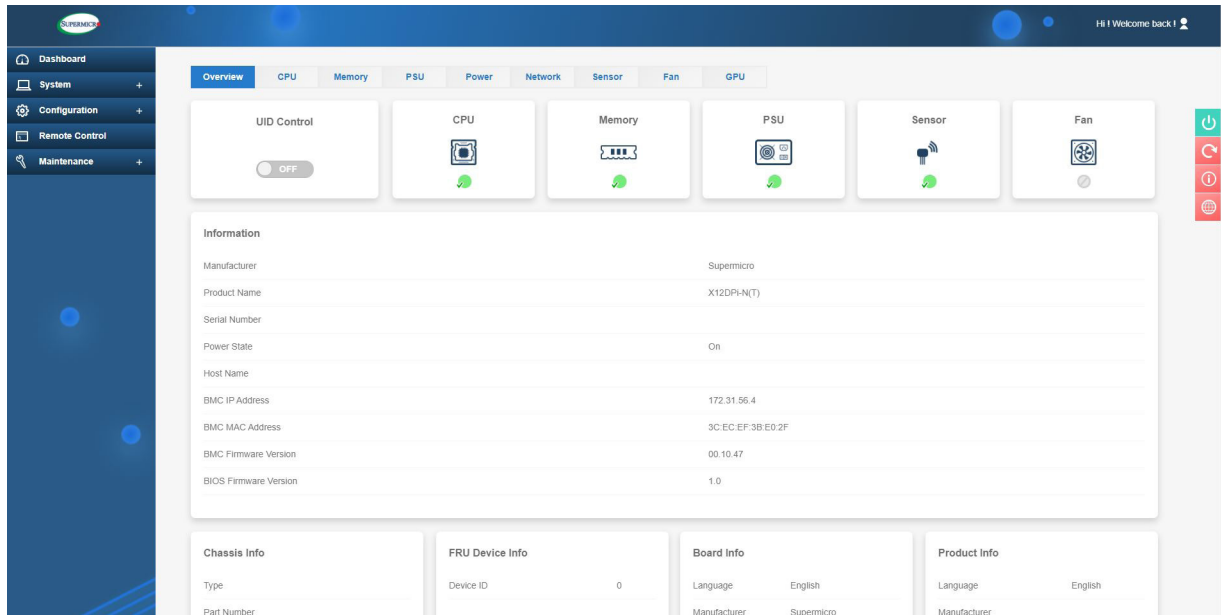
This section displays the preview of the remote console state. Click on settings to change the Virtual console settings. The page will automatically continue on its own or the users can use their mouse to click to continue. Users can choose HTML5 or Java plug-in for their preferred virtual console option.

Recent Logs

This section displays the latest health event log entries.

2.6 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).



2.6.1 Component Info

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



Note: Not all information of components under the Help Page are available for all types of servers. The Help Page is the General Guide for most system servers. See individual server manual for particular information.

Overview

- **UID Control:** Users can use this to turn on or off the UID for the users to identify the server.
- **Health Status Summary:** Users can use this to check the health status for each installed component. Users can click on the individual health status icons to view details about the component.
 - **CPU** – This displays 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 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 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 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: Users can check detailed system information.
 - Manufacturer – Manufacturer name
 - Product Part Number – Product part number of the product
 - Serial Number – Serial number of the product
 - Power State – System power status
 - Host Name – Host name of the system
 - BMC IP Address – IP address of the BMC host
 - BMC MAC Address – MAC address of the BMC
 - BMC Firmware Version – BMC Firmware version
 - BIOS Firmware Version – BIOS Firmware version
- FRU Reading: Users can configure the FRU settings by using SMCIPMITool utility and check detailed FRU information.
 - Chassis Info

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

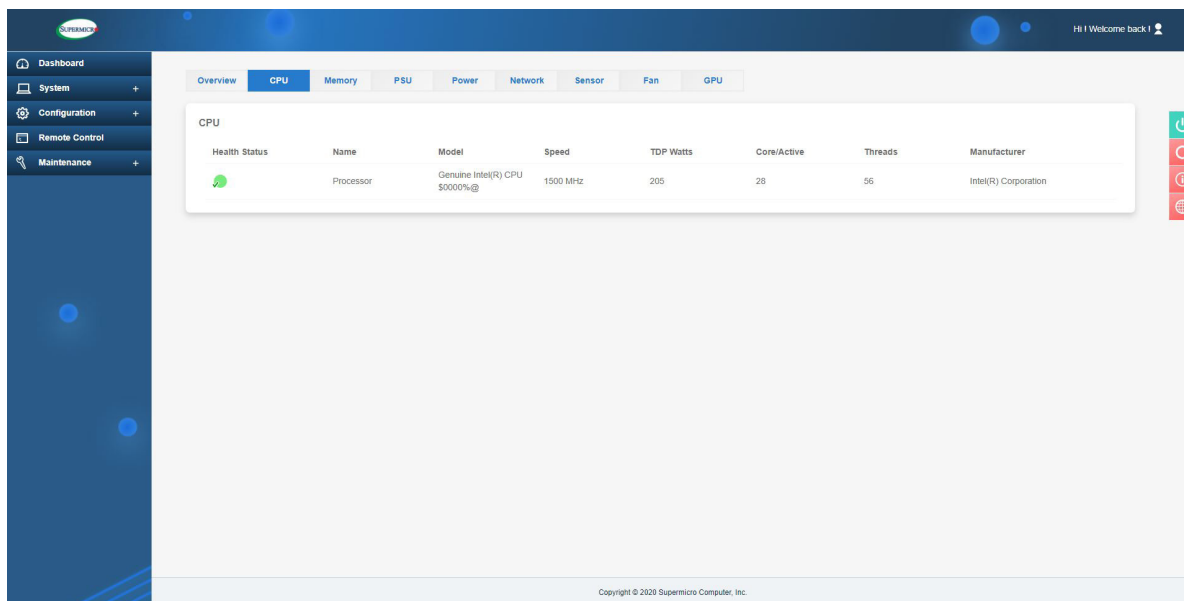
On Multi-Node System, the following information will display for chassis info.

- 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
- Device ID: Users can view the system Device ID.
- Board Info: Users can check 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: Users can check detailed product information.
 - Language – Product supported language
 - Manufacturer – Manufacturer details
 - Product Name – Product details
 - Part Number – Product part number
 - Version – Product version
 - Serial Number – Product serial number
 - Asset Tag – Product asset tag

CPU

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

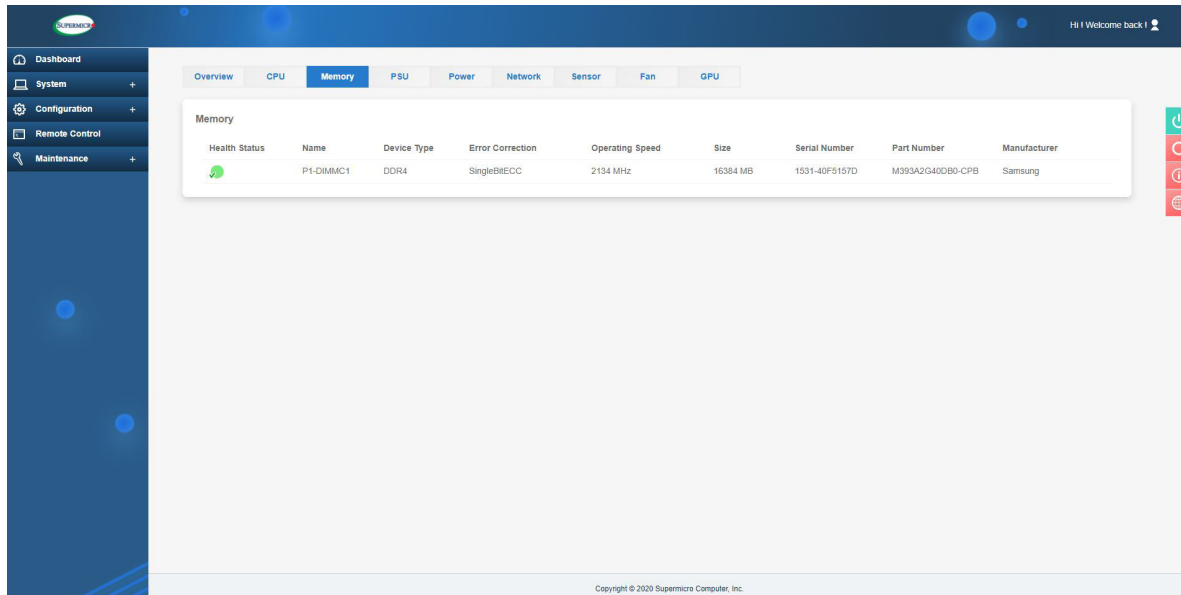


This page displays the following information.

- Health Status: Users can view the health status of the CPU (Normal, Warning, or Critical)
- Name: Users can view the name of the processor.
- Model: Users can view information about the processor model.
- Speed: Users can view the speed (in MHz) of the processor.
- TDP Watts: Users can view the supported values for TDP (Thermal Design Power).
- Cores / Active: Users can view the total cores of the processor or whether the processor is active or inactive.
- Threads: Users can view the total number threads.
- Manufacturer: Users can view the processor manufacturer info.

Memory

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



The screenshot shows the BMC interface with the 'Memory' tab selected. The table displays the following information for a single memory device:

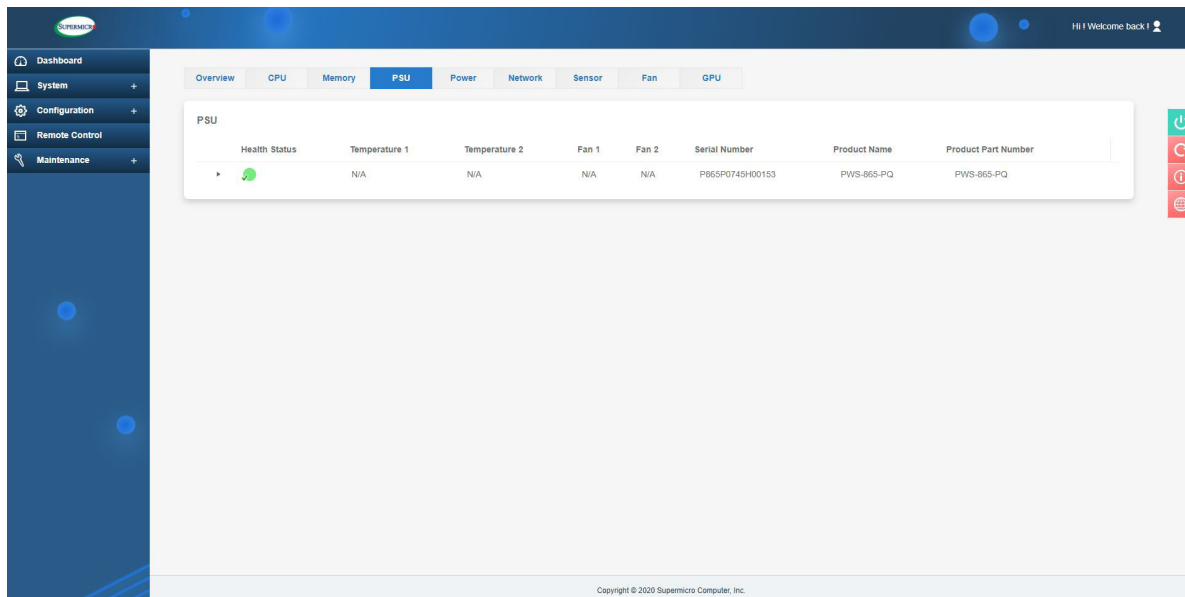
Health Status	Name	Device Type	Error Correction	Operating Speed	Size	Serial Number	Part Number	Manufacturer
Normal	P1-DIMM1	DDR4	SingleBitECC	2134 MHz	16384 MB	1531-40F5157D	M393A2G40CB0-CPB	Samsung

This page displays the following information.

- **Status:** Users can view the health status of the DIMM (Normal, Warning, or Critical).
- **Name:** Users can view the memory device name.
- **Device Type:** Users can view the memory device type defined by SMBIOS (e.g. DDR4, DDR5, RDIMM, LRDIMM, or DCPMM).
- **Error Correction:** Users 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:** Users can view operating speed of memory in MHz as reported by the memory device. Memory devices that operate at their bus speed shall report the operating speed in MHz (bus speed).
- **Size:** Users can view the size of the memory region in mebibytes (MiB).
- **Serial Number:** Users can view the product serial number of the memory device.
- **Part Number:** Users can view the product part number of the memory device.
- **Manufacturer:** Users can view the manufacturer info of the memory device.

PSU

This tab shows power supply unit information.



This page displays the following information.

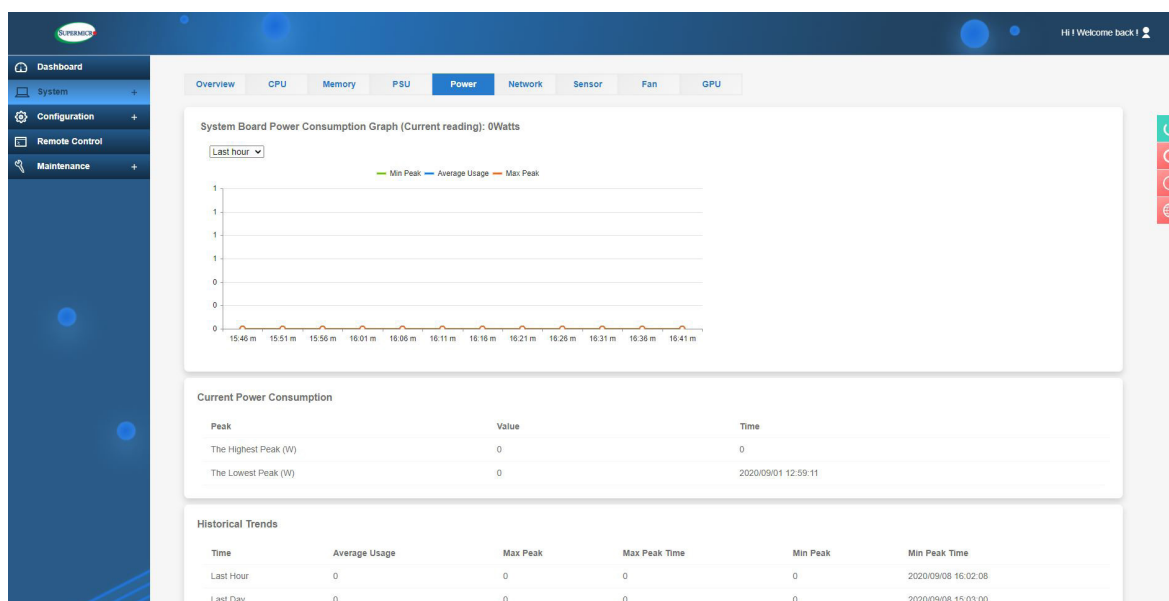
- Health Status: Users can view the health status of the CPU (Normal, Warning, or Critical).
- Temperature 1: Users can view the temperature reading of the PSU.
- Temperature 2: Users can view the temperature reading of the PSU (if present).
- Fan 1: Users can view the FAN reading of the PSU.
- Fan 2: Users can view the FAN reading of the PSU (if present).
- Serial Number: Users can view the serial number of the PSU.
- Product Name: Users can view the name of the PSU.
- Product Part Number: Users can view the part number of the PSU.

Users 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)

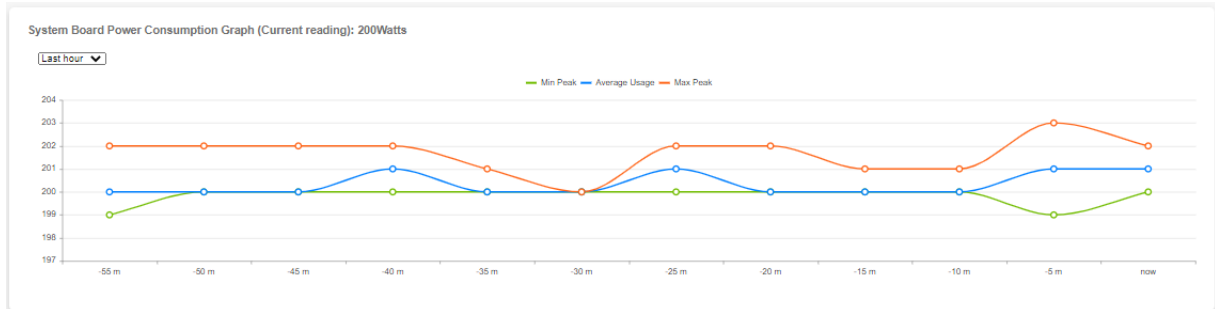
Power

The tab displays system board power consumption information.



This page displays the following information.

- **System Board Power Consumption Graph:** Users can view the system power consumption value (in Watt) with time. Users can check readings for last hour/days/week.



- **Power Consumption Since Power On:** Users 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)	302	2021/08/13 03:49:42
The Lowest Peak (W)	0	2021/08/11 19:00:05

- Historical Trend: Users 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

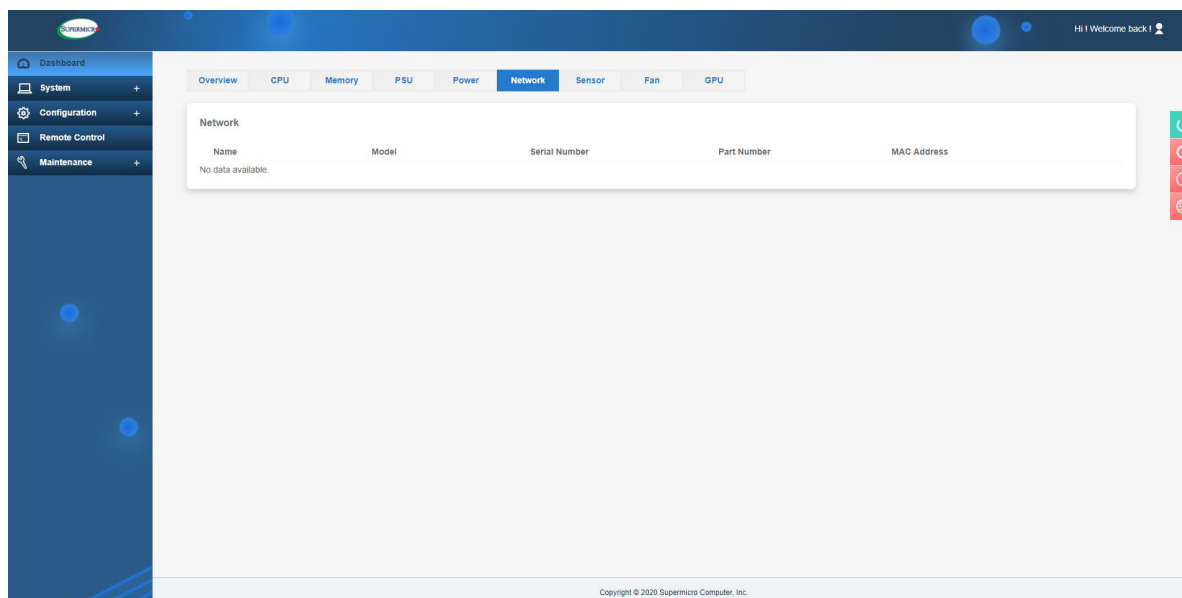
Historical Trends					
Duration	Average Usage	Max Peak	Max Peak Time	Min Peak	Min Peak Time
Last hour	200	203	2021/08/17 23:56:39	199	2021/08/17 23:54:41
Last day	199	241	2021/08/17 17:51:50	197	2021/08/17 16:09:33
Last week	198	302	2021/08/13 03:49:42	0	2021/08/11 14:43:30

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

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

Network AOC

Health Status	Model	Temperature	Location	Serial Number
▼ 	AOC-2UR68G4-4XTS	39	SXB 3 slot 0	OA20AS003306
Port 1 MAC Address 3C:EC:EF:1F:32:9A Link Status  Port 2 MAC Address 3C:EC:EF:1F:32:9B Link Status  Port 3 MAC Address 3C:EC:EF:1F:32:9C Link Status  Port 4 MAC Address 3C:EC:EF:1F:32:9D Link Status 				
▼ 	AOC-S100G-b2C	43	SXB 1 slot 2	OA19CS040217
Port 1 MAC Address AC:1F:6B:CF:39:DA Port 2 MAC Address AC:1F:6B:CF:39:DB				

Overview CPU Memory **Network AOC** Sensor

Network AOC

Health Status	Model	Temperature	Location
▶ 	AOC-A100G-b2CM	58	Unknown Slot 1
▶ 	AOC-AG-i2M	Unsupported	Unknown Slot 1

Network AOC

Health Status	Model	Temperature	Location	Serial Number
▼ 	AOC-AH25G-m2S2TM	55	AIOM slot 1	OA205S026565
Port 1 MAC Address 3C:EC:EF:4F:09:2C FW Version 14.26.4012 Port 2 MAC Address 3C:EC:EF:4F:09:2D FW Version 14.26.4012 Port 1 MAC Address 3C:EC:EF:1B:E2:F8 FW Version 14.26.4012 Port 2 MAC Address 3C:EC:EF:1B:E2:F9 FW Version 14.26.4012				

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

Network AOC

Health Status	Model	Temperature	Location	Serial Number
▼ 	AOC-AG-i2M	Unsupported	AIOM slot 1	OA212S012160
Port 1 MAC Address 3C:EC:EF:57:9C:4C Port 2 MAC Address 3C:EC:EF:57:9C:4D				

The following naming rule for Physical LAN is used by BMC to pass onto SSM. X and Y are numerical indexes (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 reading, and threshold value.

Severity	Name	Reading	Type
✓	CPU1 Temp	51	Temperature
⊘	CPU2 Temp	N/A	Temperature
✓	PCH Temp	29	Temperature
✓	System Temp	26	Temperature
✓	Peripheral Temp	31	Temperature
✓	VRMCpu1 Temp	61	Temperature
✓	VRMCpu1IO Temp	64	Temperature
⊘	VRMCpu2 Temp	N/A	Temperature
⊘	VRMCpu2IO Temp	N/A	Temperature
✓	VRMP1ABCD Temp	55	Temperature
✓	VRMP1EFGH Temp	37	Temperature
⊘	VRMP2ABCD Temp	N/A	Temperature

The sensor table displays the following information.

- Health: Users can view the sensor status and 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: Users can view the sensor names of currently available sensors from the system.
- Reading: Users can view the value of the current sensors' reading.
- Type: Users can view the sensor type, which is categorized in the following list.
 - Temperature Sensors
 - Voltage Sensors
 - Physical Security
 - Batter (aka Power Supply)

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

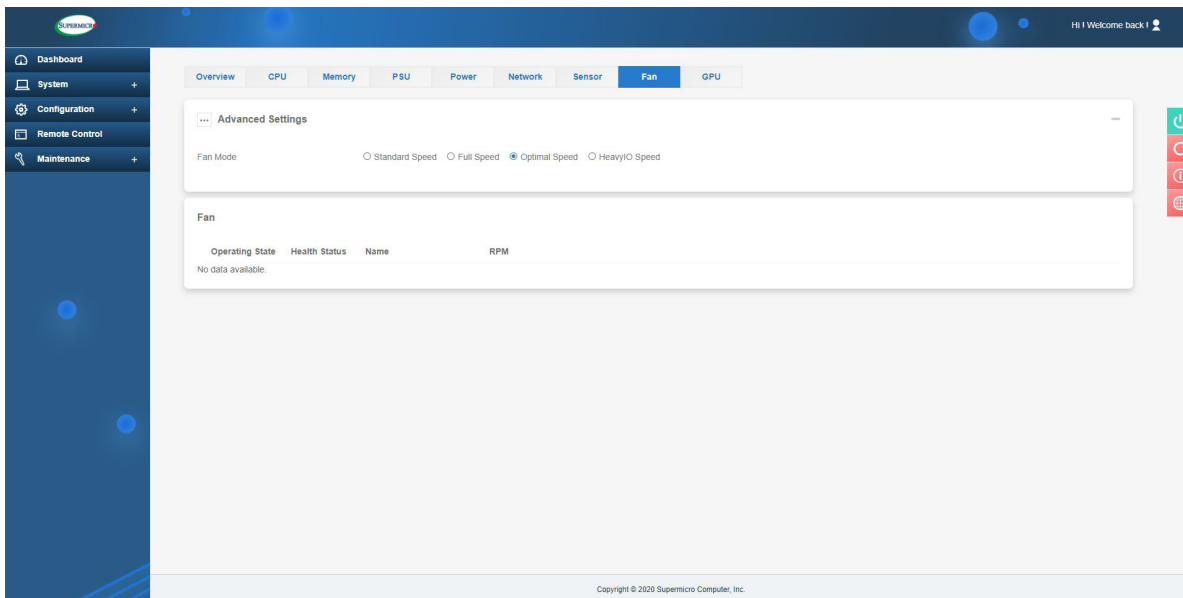


Note: If components are not installed then static sensor values will display N/A.

- Sensor Type Categories: By default, [All Sensors] categories are selected. Users can filter sensors by following categories.
 - Temperature Sensors
 - Voltage Sensors
 - VBAT Status
 - Physical Security
- Export to Excel: Users can export sensor reading in Excel format.
- Intrusion Reset: Users can use this button to reset chassis intrusion.

Fans

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

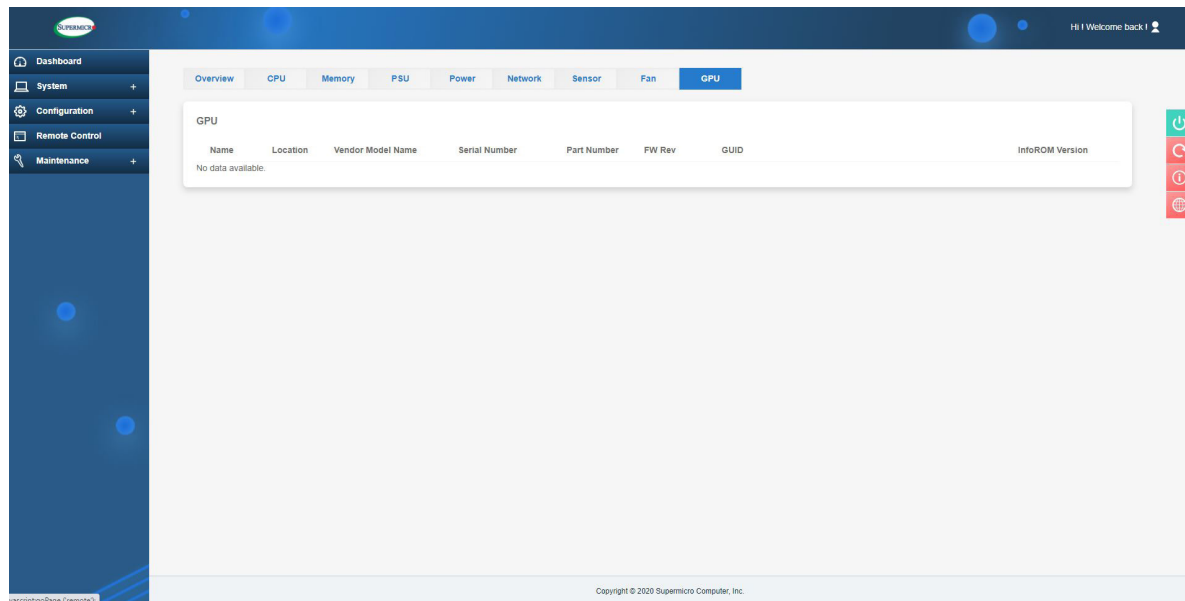


This page displays the following information.

- Status: Users can view the fan health status.
- Name: Users can view the indicated the System Fan Number.
- RPM: Users can view the indicated revolution per minute for each fan.
- Advanced Settings: Users can configure the following Fan Mode settings.
 - Standard Speed – The standard fan speed setting for power savings.
 - Full Speed – The full speed setting for optimal system performance.
 - Optimal Speed – The optimal fan speed setting, which will adjust the fan speed by balancing the needs between system performance and power savings.
 - Heavy IO Speed – The heavy I/O fan speed setting, which will boost cooling to the add-on card zone.

GPU

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



This page displays the following information.

- Name: Users can view the name of the attached GPU device.
- Location: Users can view the add-on device slot location.
- Vendor Model Name: Users can view the vendor and model names of the attached GPU device.
- Serial Number: Users can view the serial number of the GPU device.
- Part Number: Users can view the part number of the GPU device.
- Firmware Revision: Users can view the firmware revision info for GPU device.
- GUID: Users can view the GPU GUID info.
- InfoROM Version: Users can view the InfoROM version number of the GPU device.

AIP

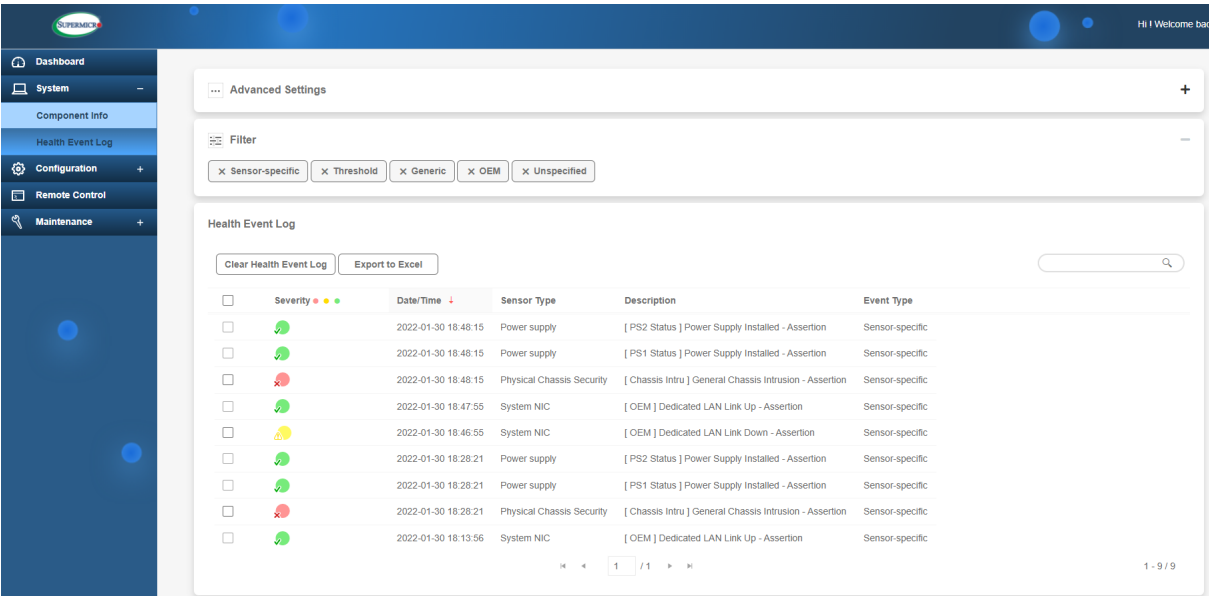
For HaBaNa system, the AIP (Advanced Integrated Peripheral) tab will be in place of GPU tab. Therefore, the following tab will be displayed instead. This tab provides following details about each installed AIP (HaBaNa Gaudi) units in the system.

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

2.6.2 Health Event Log

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

 **Note:** By default, all event types will be selected so that users can view all events. Users 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 512.



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

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

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

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

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

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

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

Users can apply the following administrator options.

- Export to Excel: Users can use this option to export the current event log to an Excel file.
- Clear Health Event Log: Users can use this to select all rows to clear the recorded event log.
- Mark as Acknowledged: Users can acknowledge warning/critical events. Select a log entry that the users wants to acknowledge and click on Mark as Acknowledged.
- Clear Acknowledgements: Users can clear all acknowledgements and click on Clear Acknowledgement.

Multi Node

Use this page to view details about the current node as well as other nodes in the server. Under System Tab, users 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”, users can see the number of nodes and whether the node is present or not. Users can also view the power status of a particular node. Detailed information for a particular node can be viewed when users select the node. Users can view Status, Power State, DC Output Power, DC Output Current, CPUs, System Temperature, Part Number, Board Serial Number, IP Address, BIOS Version, CPLD Version, BMC Version and BMC MAC Address of the node in interest. For H12 Multi Node systems, users can also view POST CODE as well as Max Power. This page will not be available for non-multi-node servers.



Note 1: Under User Privilege, users are limited to View Only mode. However, users under User Privilege can automatically log into another BMC window by clicking on a WHITE arrow on current node in Logical Front View Node frame of Multi Node page or by clicking on the IP Address in the Node frame to open up the current node into either new web browser tab or new web browser window.

Note 2: Users are limited to View Only mode if they are under User Privilege, which includes the IP Address of the accessing node.

2.6.3 Storage Monitoring

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

 **Note 1:** If users do not have a storage device installed in their 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).

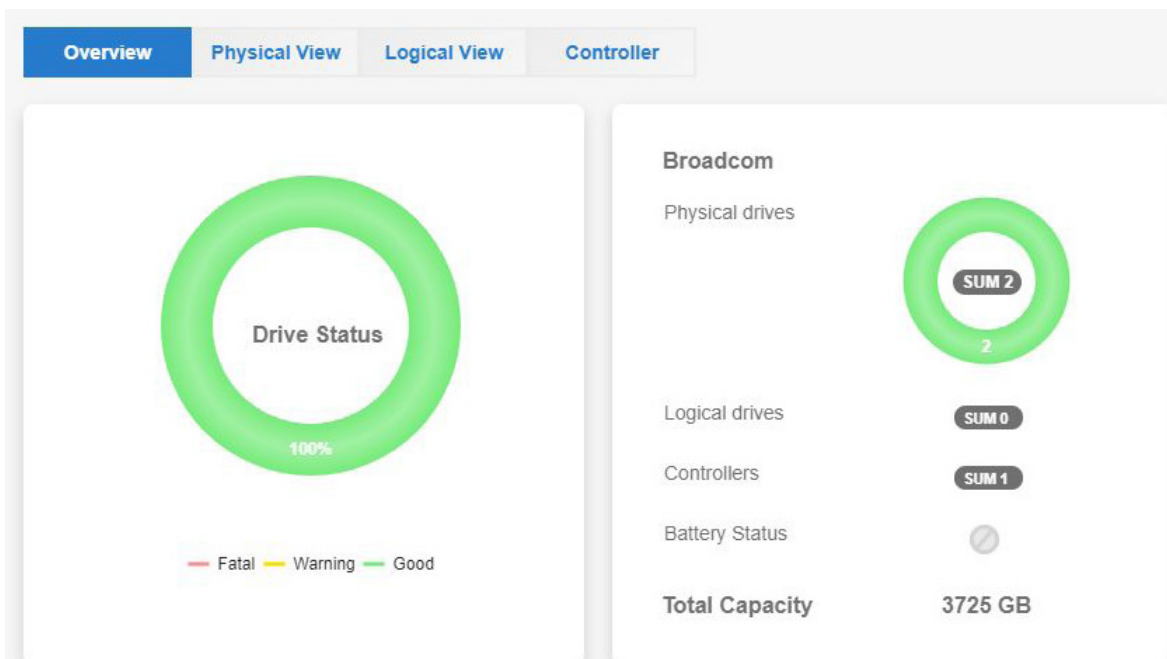
Note 2: BMC only supports (monitors) Supermicro RAID controller.

Overview

This page shows the Drive Status, the sum of physical drives, logical drives, and controllers, battery status, and total capacity of all physical drives. Drive status provides health overview of all connected disks.

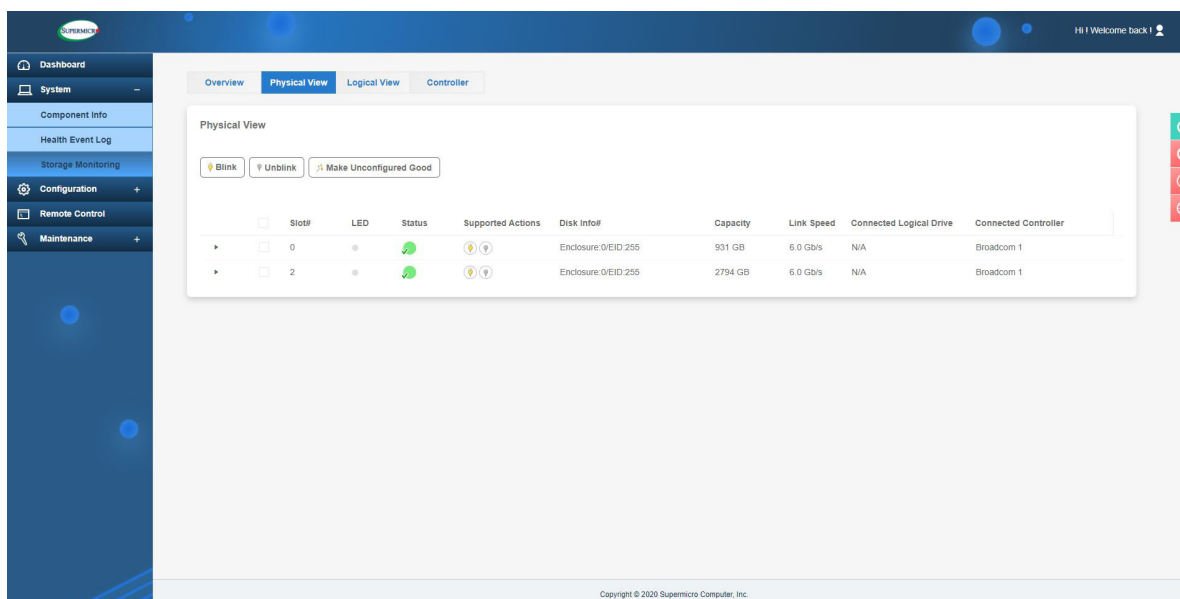
-  This symbol indicates the health of all the storage component is good.
-  This symbol indicates the storage component needs attention and could fail.
-  This symbol indicates the storage component health is critical.

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



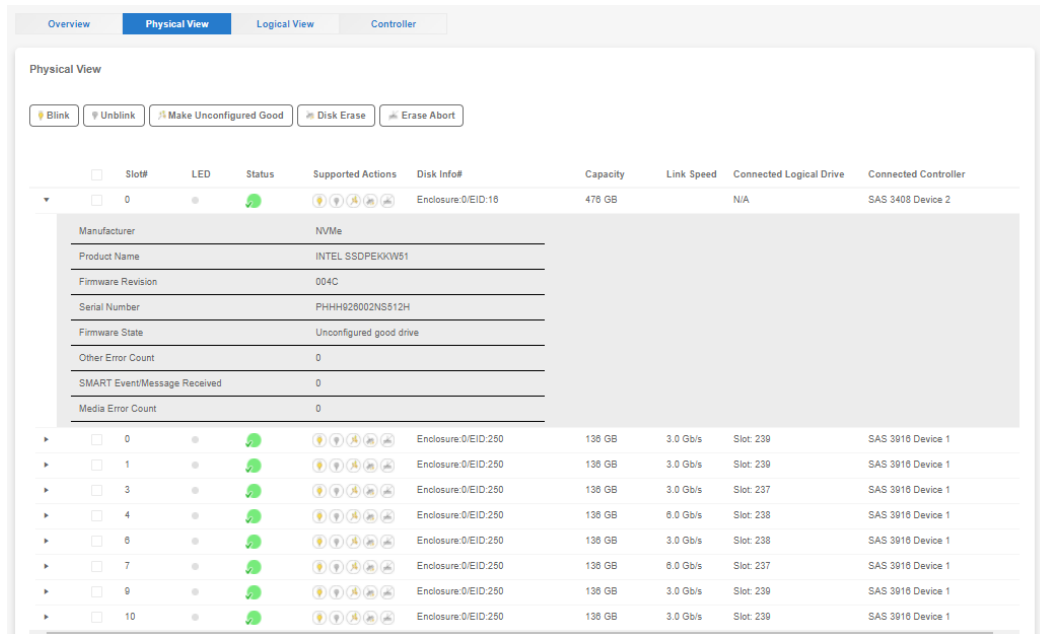
Physical View

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.



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

- Slot Number: Users can view the connected physical disk's slot number.
- Status: Users can view the indicated the 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: Users can view the indicated what actions are supported based on HDD type.
- Diskinfo: Users can view the available disk info.
- Capacity: Users can view the capacity of the physical disk (Gb).
- Link Speed: Users can view the link speed of the physical disk (b/s).
- Connected Logical Drive: Users can view the connected logical drive info (if any).
- Connected Controller: Users can view the connected controller info (if any).



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

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



Note: The following table provides details on which storage controller is supported. In the X12 series, BMC users can select more than one NVMe drive at a time. Therefore, the Eject and Insert buttons would appear whether VMD is enabled or disabled. If there is only a SATA drive connected to the Broadcom storage controller, then neither Eject nor Insert buttons would appear.

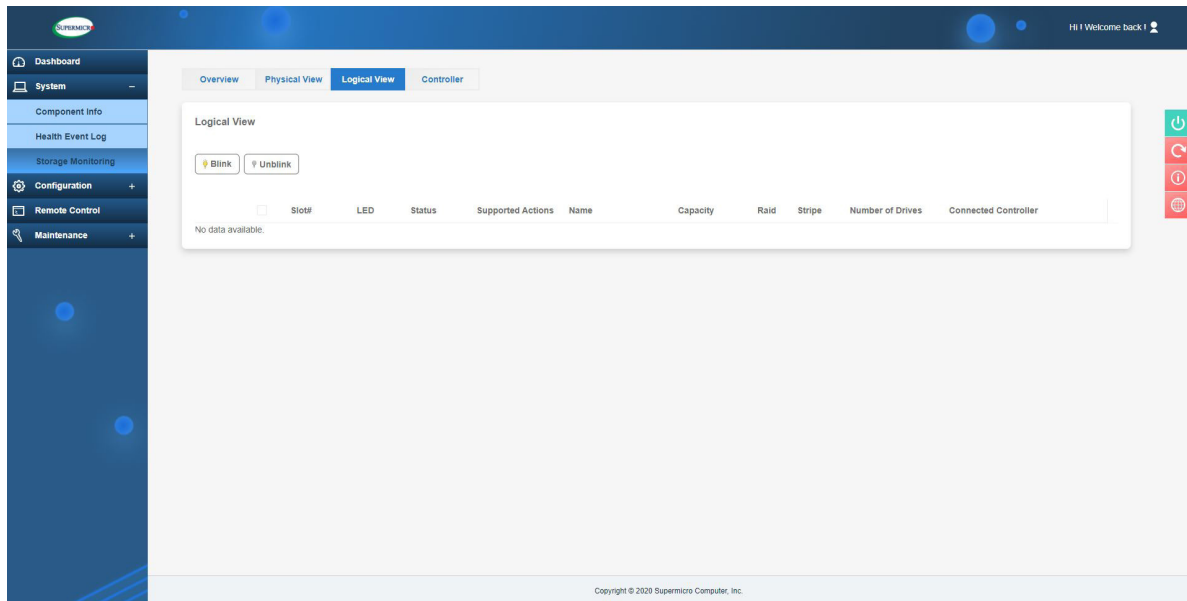
Users can also view the following HDD detailed information by clicking the arrow pointer next to a particular HDD (NVMe or SATA).

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

Table for Supported Controller(s)			
	Blink	Unblink	Make Unconfigured Good
Broadcom	Supported	Supported	Supported
Marvell	<i>Not supported</i>		
NVMe	Supported	Supported	<i>Not supported</i>

Table for Supported Controller(s)				
	Eject	Insert	Disk Erase	Erase Abort
Broadcom	<i>Not supported</i>	<i>Not supported</i>	Supported only for Broadcom 3108 controller	Supported only for Broadcom 3108 controller
Marvell	<i>Not supported</i>			
NVMe	<i>Not supported if NVMe in VMD mode</i>	<i>Not supported if NVMe in VMD mode</i>	<i>Not supported</i>	<i>Not supported</i>

Logical View



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

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

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

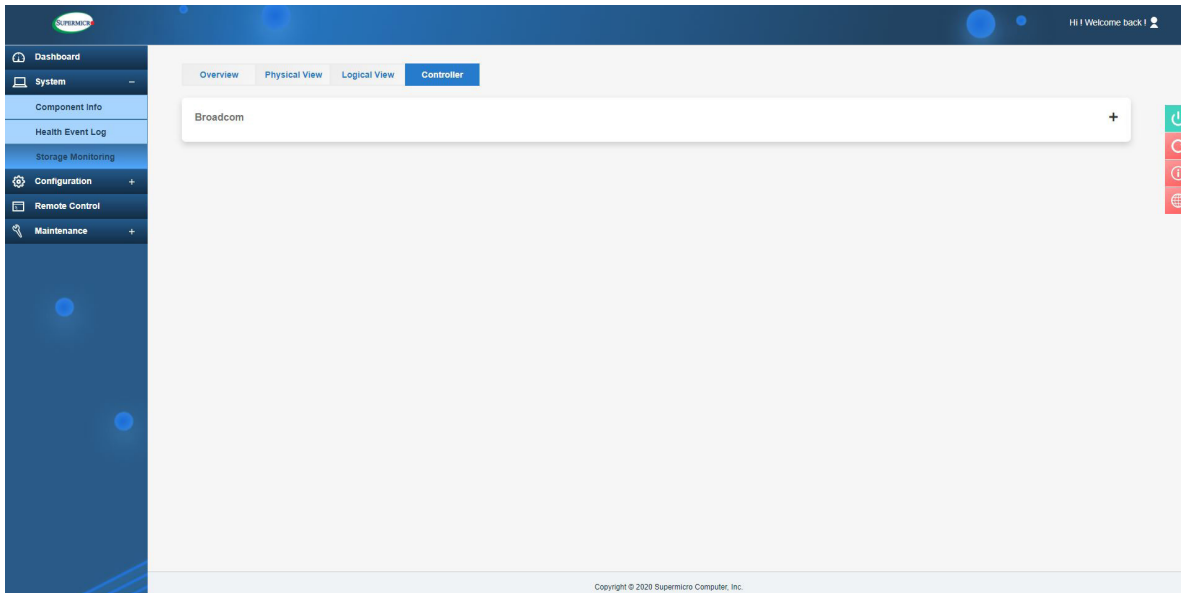
- Blink: Users can use this action to locate a virtual disk.
- Un-blink: Users can use this action to stop the Blink action.
- Delete: Users can use this action to delete a virtual disk.

The screenshot displays the 'Logical View' tab of a system management interface. At the top, there are four tabs: 'Overview', 'Physical View', 'Logical View' (which is selected), and 'Controller'. Below the tabs, there are three buttons: 'Blink' (with a yellow lightbulb icon), 'Unblink' (with a grey lightbulb icon), and 'Delete' (with a trash can icon). The main area contains a table with the following columns: Slot#, LED, Status, Supported Actions, Name, Capacity, Raid, Stripe, Number of Drives, and Connected Controller. Two rows of data are shown, each with a dropdown arrow to its left. The first row is for 'vd2' (Slot# 238, Capacity 272 GB, Raid 0, Stripe 256K, Number of Drives 2) and the second row is for 'vds' (Slot# 239, Capacity 272 GB, Raid 1, Stripe 256K, Number of Drives 4). Both rows show 'Optimal' status and 'SAS 3916 Device 1' as the connected controller. Below each row, there is a detailed view of the RAID configuration, including 'Second Raid Level', 'Raid Level Qualifier', and 'Span Depth'.

	Slot#	LED	Status	Supported Actions	Name	Capacity	Raid	Stripe	Number of Drives	Connected Controller
▼	238	●	Optimal	[Blink] [Unblink] [Delete]	vd2	272 GB	0	256K	2	SAS 3916 Device 1
Second Raid Level: 0 Raid Level Qualifier: 0 Span Depth: 1										
▼	239	●	Optimal	[Blink] [Unblink] [Delete]	vds	272 GB	1	256K	4	SAS 3916 Device 1
Second Raid Level: 0 Raid Level Qualifier: 0 Span Depth: 1										

Controller

This page shows the information about the connected controllers to the system. To view these details, select a controller and click on the expandable button. It allows users to create RAID and apply changes to controller actions. BMC supports all RAID levels from the available RAID levels of the manufacturers. For example, if AOC-S3916L-H16IR (-32DD) supports RAID 0, 1, 5, 6, 10, 50, and 60, then BMC will also provide the same RAID levels.



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

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

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

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

Create RAID

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

- **Create:** Users can 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]:** Users can use this cation to select or add logical drive to the existing group.

Controller Actions

Users can perform the following controller actions.



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

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

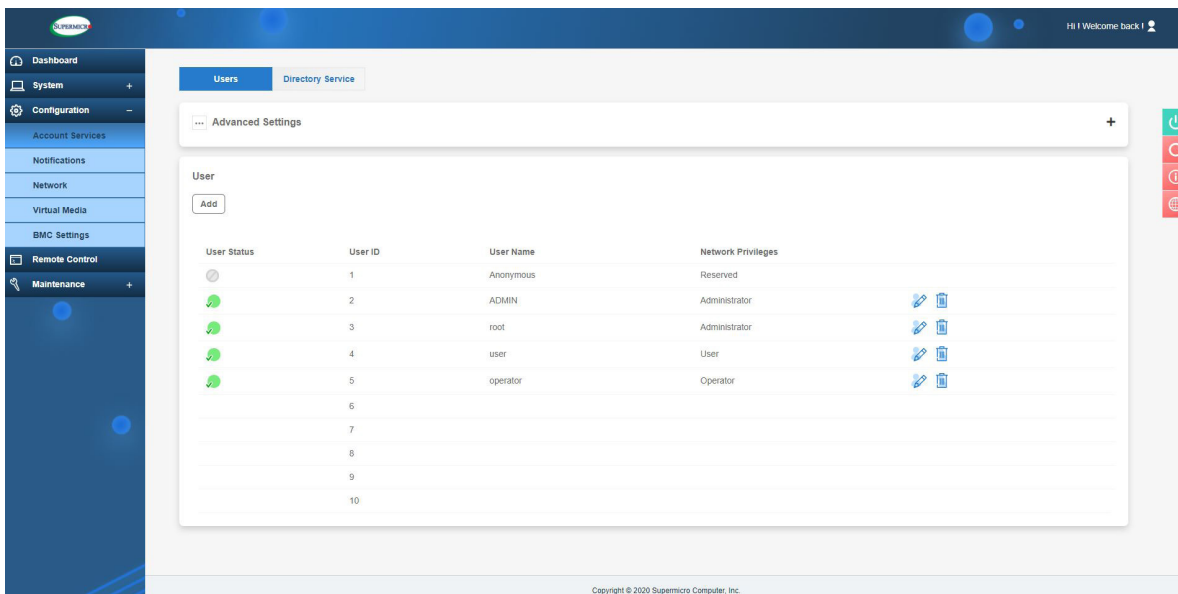
2.7 Configuration

This page allows users to perform various configuration settings such as user account management, directory services, alert notifications, network, virtual media, and BMC settings. Network setting values should be integer values and not negative values. Please refer to the pages below for additional information.

2.7.1 Account Services

Users

This feature is used to monitor and configure settings for users. The display lists current user information, including User ID, User Name, and Network Privilege settings. Administrators can also modify user access levels and privileges.



- **Add New User:** Users can click [Add] to add a new user. When prompted, enter username, password, and the network privilege level.

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

- **User Status:** Users can view whether the user login is enabled, disabled, or locked.
- **User ID:** Users can view the ID number used to identify the configured users.
- **User Name:** Users can view the username of the user.

- Network Privilege: Users can view one of the following types of privilege level assigned to the users.
 - Administrator
 - Operator
 - User
- Actions: Administrators can perform edit, delete, enable, or unlock user action for each user.
- Password Requirements
 - Password requires length of 8 to 19 characters.
 - Password cannot be the reversed of the username.
 - Password must include characters from at least three of the listed character classes. Allowed character classes include the following.
 - a through z
 - A through Z
 - 0 through 9
 - Special characters
 - Password can be previewed with the eye-icon button to view password.
- Modify User: Users can click on the pencil icon to modify settings for selected current user. When prompted, enter username, password, and the network privilege level.
- Delete User: Users can click on the trash can icon to delete selected user. Administrator(s) can delete user accounts that are not in use. Administrator user(s) cannot delete any user account(s) that are being logged on. A prompt will be issued to alert the administrator if such action is attempted.



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

Advanced Settings

Users can perform the following actions to configure advanced settings.

- **Failed Login Lockout Control:** Users can view whether the User Account is locked or unlocked 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 1 to 5 attempts. If the value is zero (00h), there is no limit on the number of failed attempts.
- **Failed Login Counter Reset:** The count of consecutive failed login attempts will be reset after this interval without a failed login attempt. If set to “Never”, Failed Login Lockout Controls will be disabled. The counter is also reset upon successful login.
- **Account Lockout Duration:** The amount of time the users will be locked out (unable to login) after Failed Login Attempt Lockout Threshold failed login attempts. If set to “Never”, Failed Login Lockout Controls will be disabled.

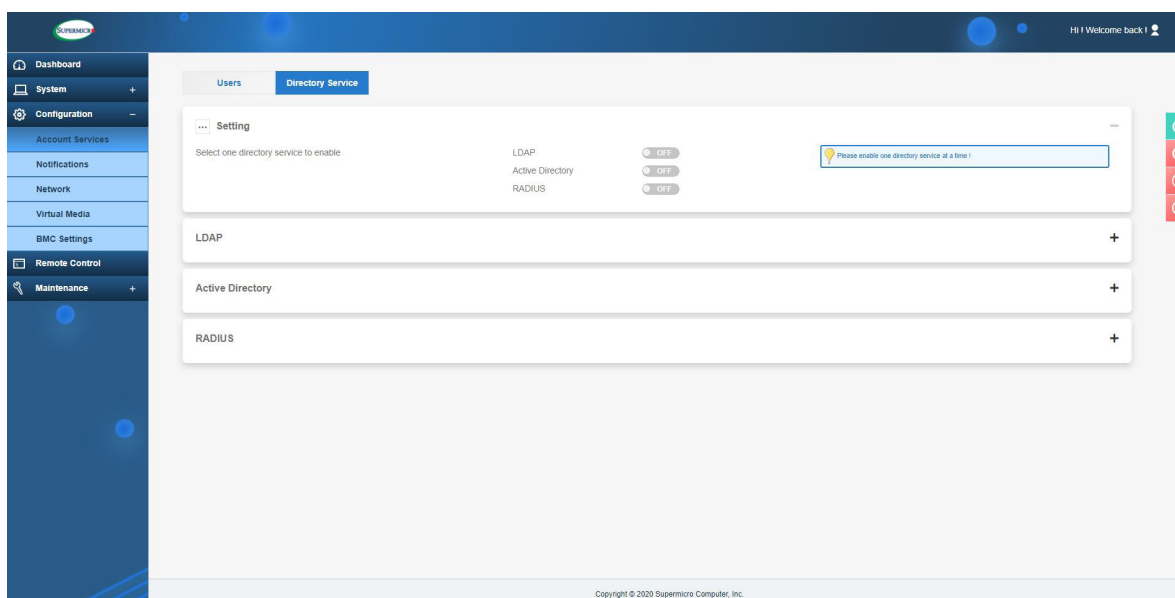
Directory Services

Settings

Use this page to configure directory services. Users can enable either LDAP, Active Directory, or RADIUS services. Please enable one directory service at a time.



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



LDAP (Lightweight Directory Access Protocol)

This page allows users to view and configure the LDAP (Lightweight Directory Access Protocol) authentication. LDAP users can log in to BMC WebUI or access Redfish API. It displays a list of role groups, their group IDs, group names, domains, and network privilege settings.

- Enable: Users can enable LDAP authentication to allow domain users to access BMC.



Enable LDAP authentication



Disable LDAP authentication



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

- Bind DN: The bind DN (Distinguished Name) is the username or the LDAP server that is permitted to search in the LDAP directory within a defined search base. For example: cn=admin,dc=example,dc=com.
- Bind Password: Users can enter the bind password for LDAP server authentication.
- Username Attribute: Users can enter the username login attribute.
- Groups Attribute: Users can enter the group membership attribute.
- Server Address: Users can enter up to three addresses for the LDAP server. Click on [+ Add new record] to add server address.
 - Prefix – Users can select to use LDAP or SSL LDAP (ldap:// or ldaps://).
 - IP or Domain – Users can enter the server IP or domain name.
 - Port – Users can enter the port number of the server. Default port number for LDAP is 389 and LDAPS is 636. Users can [Update], [Cancel], edit, or delete given settings.
- Search Base: Search base is the distinguished name used to search an external LDAP service. Click on [+ Add new record] to add search base values. Users can enter up to 3 search base values as well as edit or delete current settings.
- Rules: Users can enter up to five rules. Click on [+ Add new record] to add rules and enter the following fields.
 - Role – Users can select the privilege level for that user or role group (Administrator, Operator, or User).
 - Remote User – Users can enter the LDAP username.

- Remote Group – Users can enter the name of the LDAP group folder. For example: cn=PowerUsers,ou=Groups,dc=example,dc=org.

Users can [Update] or [Cancel] given settings, as well as edit or delete current settings.

Active Directory

This page allows users to view and configure Active Directory authentication. Active directory users can also login to BMC UI and Redfish API.

- Enable: Users can enable Active Directory authentication to allow domain users access to BMC.



Enable AD authentication



Disable AD authentication



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

- Server Address: Users can enter up to three addresses for the LDAP server. Click on [+ Add new record] to add server address.
 - Prefix – Users can select to use LDAP or SSL LDAP (ldap:// or ldaps://).
 - IP or Domain – Users can enter the server IP or domain name.
 - Port – Users can enter the port number for the server. Default port number for LDAP is 389 and LDAPS is 636. Users can [Update] and [Cancel] as well as edit or delete given settings.
- Rules: Users can enter up to five rules. Click on [+ Add new record] to add rules and enter the following fields..
 - Roles – Users can select privilege level for that user or role group (Administrator/Operator/User).
 - Remote User – Users can enter the LDAP username.
 - Remote Group – Users can enter the name of the LDAP group folder. Users can [Update] and [Cancel] as well as edit or delete given settings.

RADIUS

This page allows users to view and configure RADIUS authentication.

- **Enable:** Users can enable RADIUS authentication.



Enable RADIUS authentication



Disable RADIUS authentication

- **Bind Password:** Users can enter a bind password for the users to access the RADIUS server.
- **Server Address:** Users can add or edit RADIUS server address.
 - **IP or Domain** – Users can enter the server IP or domain name.
 - **Port** – Users can enter the port number of the server.

2.7.2 Notifications

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

Alerts

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



Note: Please use Half-Width characters (e.g. English letters and numbers) when entering data into the textbox. Users will encounter expected errors when using Full-Width characters.

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

Alerts table will display the following information.

- No.: Users can view the number of alert entries.
- Enable: Users can enable/disable alerts.
- Protocol: Users can view the supported protocol for alert transmissions (e.g. Redfish, SMTP, SNMPv1).
- Destination: Users can view the destination address where the alerts will be sent.

- Event Types: Users can view the configured event types for respective alerts. Supported event types include the following.
 - Alert
 - ResourceAdded
 - ResourceRemoved
 - ResourceUpdated
 - StatusChange
- Modify: Users can select an alert entry to configure alerts.
- Modify Alert: Users can configure the alert using the following options.
 - Enable – Users can select to enable/disable alert.
 - Protocol – Users can select protocol type and fill respective info (Redfish, SMTP, SNMPv1).
 - Severity – Users can select event severity info/warning/critical. This field is displayed only when SMTP/SNMPv1 selected.
 - Event Type – Users can select one or more supported event types.
 - Alert
 - ResourceAdded
 - ResourceRemoved
 - ResourceUpdated
 - StatusChange
 - Destination Address – Users can select an address where alerts will be sent.
 - Message – Users can view the context string that is stored with the event destination subscription.



Note: Users must fill in the Message field for the required SMTP and Redfish protocols.

- Subject – Users can add subject info if any.



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

- Trap Community – Users can fill info for traps.



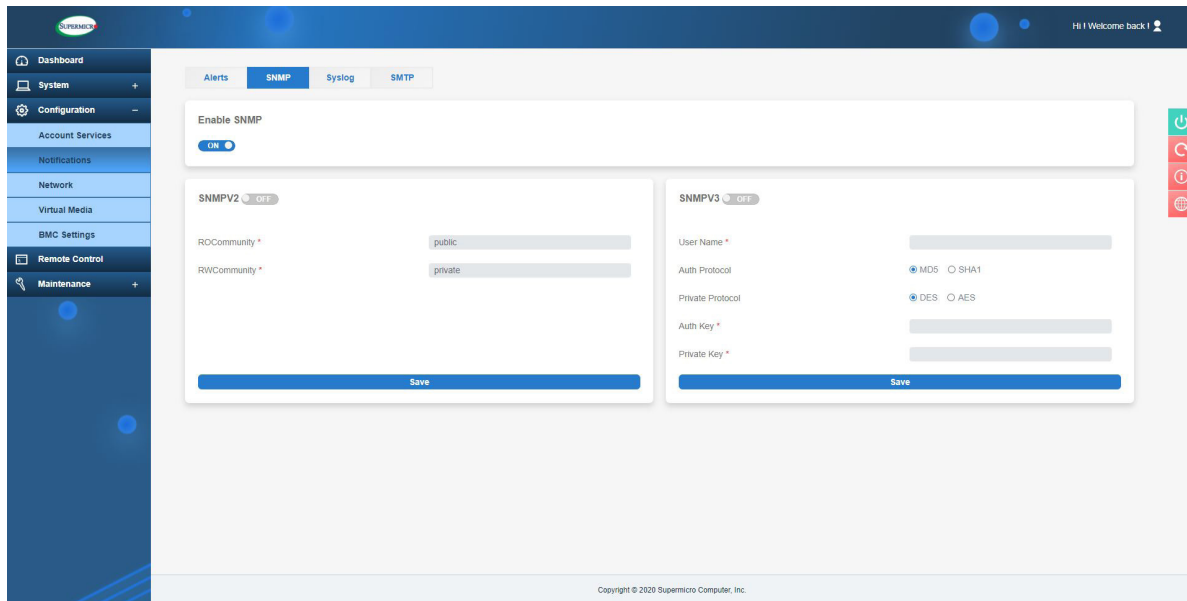
Note: This field is only displays when SNMPv1 is selected.

- Delete: Users can delete respective alert.

Users 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. Users can choose either SNMPv2 or SNMPv3 as the protocol for communicating with the SNMP client program.



To configure SNMP settings, refer to the following steps.

1. Enable SNMP.

2. Choose the SNMP version. The default version enabled is SNMPv1.

- If SNMPV2 is enabled, users can name one or more Communities by inputting Read-Only Community String and Read-Write Community String. They can also make changes if needed.
- If SNMPV3 is enabled, please input the following fields.
 - Auth Protocol – Preferred authentications. Users can select one of the following protocols.
 - MD5
 - SHA1
 - Account.

- Private Protocol – Encryption protocols. Users can select one of the following private protocols.
 - None
 - DES
 - AES
 - Account.
3. Click the [Save]. The IPMI firmware will remember the settings and await the user's decision to start or stop the SNMP daemon.
 4. If the users want to change the SNMP port number, please go to the Port page.



Note: By default, all SNMP settings are disabled and all SNMP buttons are set to **OFF**. Once SNMP setting is **ON**, users can turn **ON** SNMPv2 or SNMPv3 using the **ON/OFF** buttons. Once SNMP is turned **OFF**, no traps will be sent out even though buttons for SNMPv2 and SNMPv3 are set to **ON**.

Alerts

SNMP

Syslog

SMTP

Enable SNMP ☐ OFF

SNMPv2 ☐ OFF

Hide Community Strings ☐ OFF

Add

Name	Community String	Access Mode
------	------------------	-------------

SNMPv3 ☐ OFF

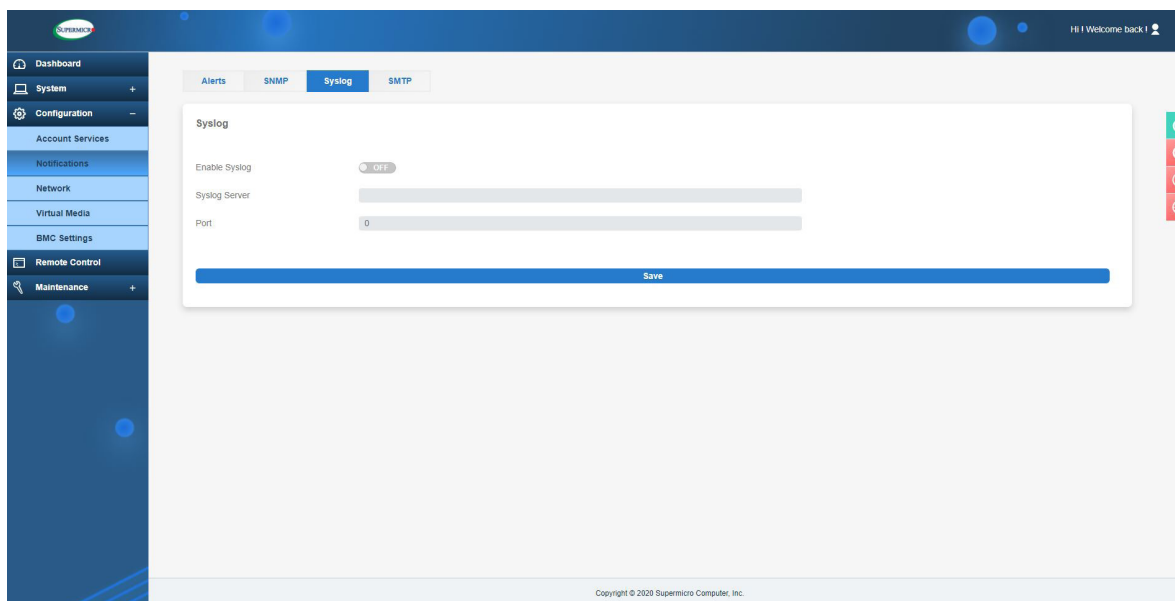
Auth Protocol ☐ MD5 ☐ SHA1 ☐ Account

Private Protocol ☐ None ☐ DES ☐ AES ☐ Account

Save

Syslog

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

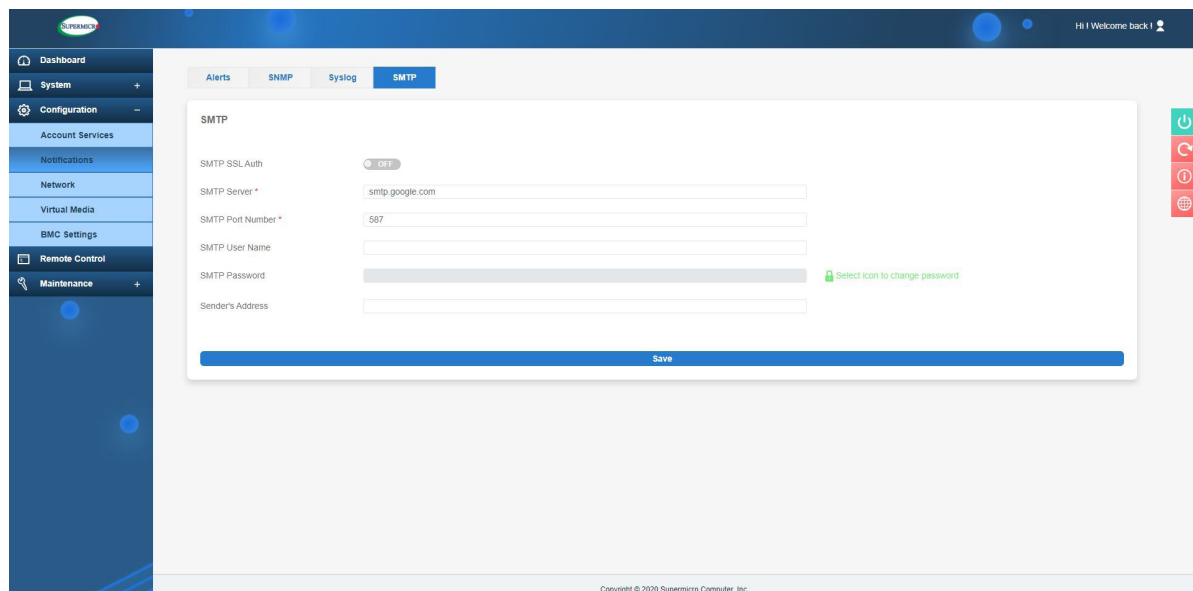


To configure the syslog settings, refer to the following steps.

1. Select [Enable Syslog].
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 users to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network.

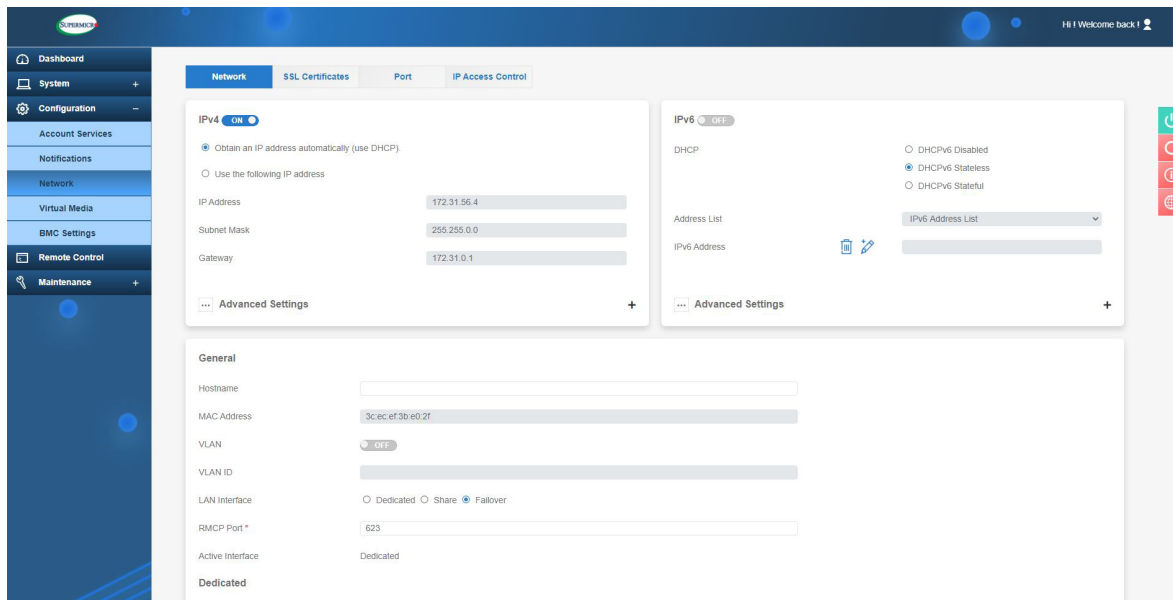


To configure SMTP settings, refer to the following steps.

1. Enable SMTP SSL Auth. Once enabled, users can configure the following information.
 - Server Address – Users need to enter the address for the SMTP mail server to configure SMTP.
 - Port Number – Users need to enter a SMTP port number.
 - Connection Protocol – Users can choose one of available protocols to set up SMTP authentication.
 - User Authentication: Users can choose one of available Authentication methods to set up SMTP.
 - User Name – Users have the option to enter the user name for SMTP mail server (optional).
 - Password – Users need to enter the user password for the SMTP mail server.
 - Sender's Address – Users have the option to add Sender's address.
2. After entering the information above, click [Save] and finish.

2.7.3 Network

Use this page to configure BMC network settings, such as IPv4, IPv6, SSL certification, ports, IP access control, and SSDP.



IPv4

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

IPv4 Advanced Settings

DNS Server IP: Users can enter DNS Server IP to retrieve hostname from DNS.

IPv6

- ON: Users can enable/disable IPv6 network connection for BMC.
 - Disable: Users can choose this option to disable DHCPv6 connection.
 - DHCPv6 Stateless: When selected, BMC will NOT apply the prefix/IPv6 address from the DHCPv6 server.
 - DHCPv6 Stateful: When selected, BMC will apply the prefix/IPv6 address from the DHCPv6 server.
 - Address List: The drop-down lists all the possible IPv6 address(es) on the BMC network interface that is currently available. Link-local address is also included.
 - IPv6 Address: Users can take the following actions.
 - Add – Users can add static IPv6 address. Please note that the prefix length is required.
 - Delete IP – When selected, the IP address in IPv6 Address field will be deleted.
-  **Note:** Only Static IPv6 Address can be deleted.
- Auto configuration – When checked, BMC will calculate a stateless auto configuration address based on the prefix information from the RA.

IPv6 Advanced Settings

- Auto Configuration: Users can select auto configuration on or off.
- DNS Server IP: Users can assign a DNS server IP address in IPv6 form.
- DUID: Users can use the Unit ID to get the DHCP IP from the DHCP server. The DUID includes client network information (address, lease time, and DNS serve info). This is READ ONLY.
- Enable Static Route: When enabled, the route rules listed in Static Route List will be applied into the IPv6 routing table.
- Static Route List: Users can view the static route list.
- Prefix to Route: Users can input the prefix to route in this field. While there is an IPv6 packet whose destination address fits the Prefix to Route, the packet will be destined via

the specific router which is defined in the Router Address field. Please note that the prefix length is required.

- **Delete this Route:** Users can delete route rules selected on the Static Route List drop down list.
- **Router Address:** Users can input the router address in this field. While there is an IPv6 packet whose destination address fits the Prefix to Route, the packet will be destined via the specific router which is defined in the Router Address field.

The screenshot shows the BMC Network configuration interface. The 'Network' tab is selected, and the 'IP Access Control' sub-tab is active. The IPv4 section is on the left, and the IPv6 section is on the right. In the IPv6 section, the 'DHCP' dropdown is set to 'DHCPv6 Stateless'. Below it, the 'Address List' dropdown is open, showing a list of IPv6 addresses. A red box highlights the 'Delete' and 'Add' icons in the Address List.

Additional Reference Steps to Add/Delete IPv6 Address

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

1. Select add icon.

The screenshot shows the BMC Network configuration interface with a confirmation dialog box overlaid. The dialog box asks 'Are you sure you want to MODIFY Network parameter(s)?' and has 'Close' and 'Save' buttons. The background shows the IPv6 configuration page with the 'Address List' dropdown open.

2. Input the address to be configured.

The screenshot shows the BMC Network configuration interface with the IPv6 configuration page. The 'Address List' dropdown is open, and the address 'fe80:0:0:2d0:4aff:fe9c:4ecc/64' is selected. The dropdown menu also shows the option 'IPv6 Address List -'.

3. Save.

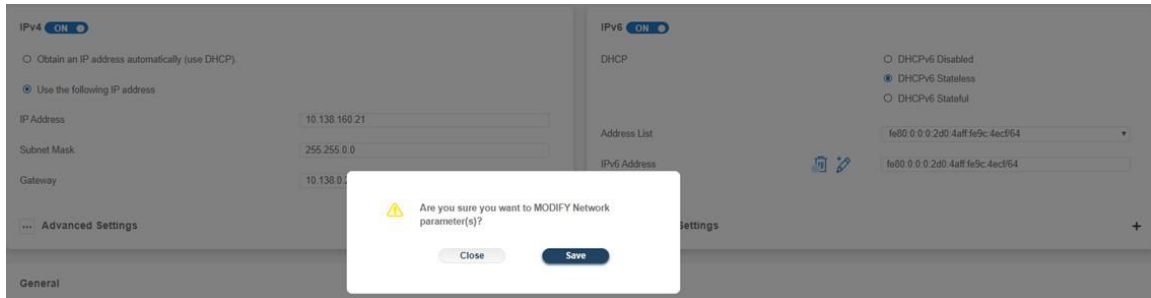
The updated address will appear on Address List.

Enter



The screenshot shows the IPv6 configuration interface. At the top, the 'IPv6' toggle is set to 'ON'. Under the 'DHCP' section, 'DHCPv6 Stateless' is selected with a radio button. Below this, the 'Address List' section shows a single entry: 'fe80:0:0:2d0:4aff:fe9c:4ecf/64'. To the left of this entry is an 'IPv6 Address' field with a trash icon and an edit icon. At the bottom left, there is an 'Advanced Settings' link with a plus icon on the right.

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



The screenshot shows the IPv6 configuration interface with a confirmation dialog box in the center. The dialog box has a yellow warning icon and the text: 'Are you sure you want to MODIFY Network parameter(s)?'. It has two buttons: 'Close' and 'Save'. The background interface shows the 'IPv6' toggle is 'ON', 'DHCPv6 Stateless' is selected, and the 'Address List' contains the same entry as the previous screenshot.

1. Select add icon.



The screenshot shows the IPv6 configuration interface. The 'IPv6' toggle is 'ON', and 'DHCPv6 Stateless' is selected. The 'Address List' section shows the same entry as before. To the left of the entry is an 'IPv6 Address' field with a trash icon and an edit icon. At the bottom left, there is an 'Advanced Settings' link with a plus icon on the right.

2. Input the address to be configured.
3. Save.

The updated address will appear on Address List.

General

In this section, users can use and view the following features.

- Hostname: Users can enter a name for the server as server identification.
- MAC Address: Users can view the MAC Address of BMC.
- VLAN: Users can enable/disable Virtual LAN support.
 - VLAN ID – Users can enter the VLAN ID.
- LAN Interface: Users can select the type of the LAN interface.
 - Failover
 - Dedicated
 - Shared
- Shared LAN: Users can select one of the LAN modes.
 - Auto
 - Onboard
 - AIOM
 - AOC

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

Failover - AOC	Failover between "Shared - AOC" and "Dedicated"
Shared - Onboard	Onboard Shared LAN
Failover - Onboard	Failover between "Shared - Onboard" and "Dedicated"

- RMCP Port: Users can select the desired RMCP (Remote Mail Checking Protocol) port based on their configuration. The default port is 623.
- Active Interface: Users can view the current type of LAN interface selected.
- Link: Users can select one of the following link speeds.
 - Auto negotiation
 - 10M half-duplex
 - 10M full duplex
 - 100M half-duplex
 - 100M full duplex



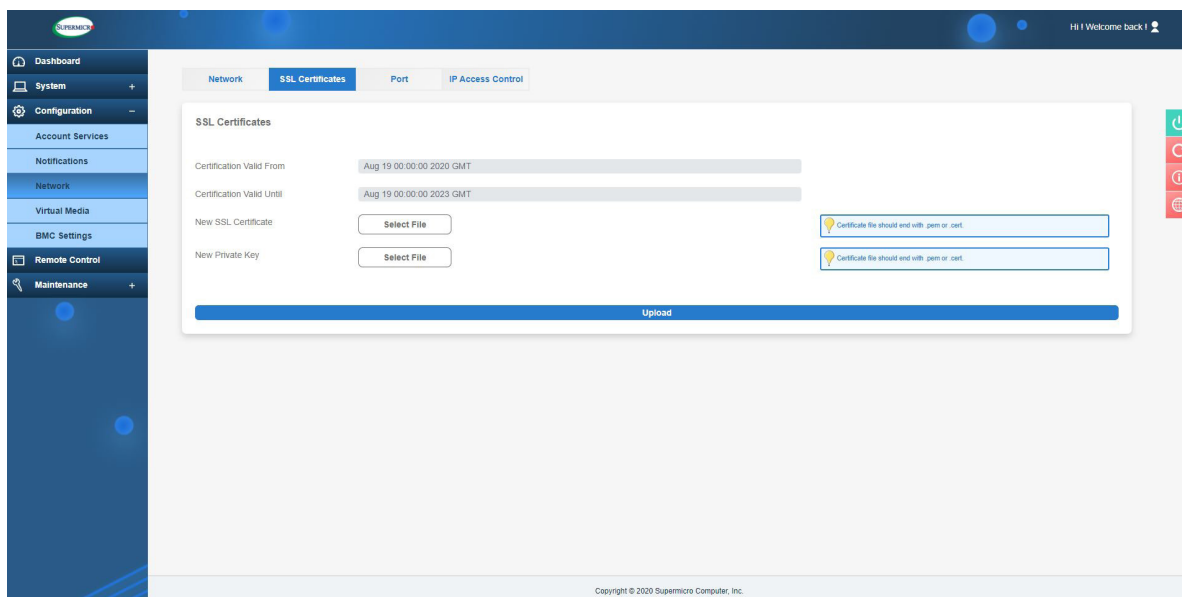
Note: Link options are only enabled when the LAN Interface is in Dedicated mode.

- Status: Users can view the status of the BMC link.
- Speed: Users can view the indicated the speed of the system link connection.
- Duplex: Users can view whether the BMC link is a full or half duplex.

SSL Certificates

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

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



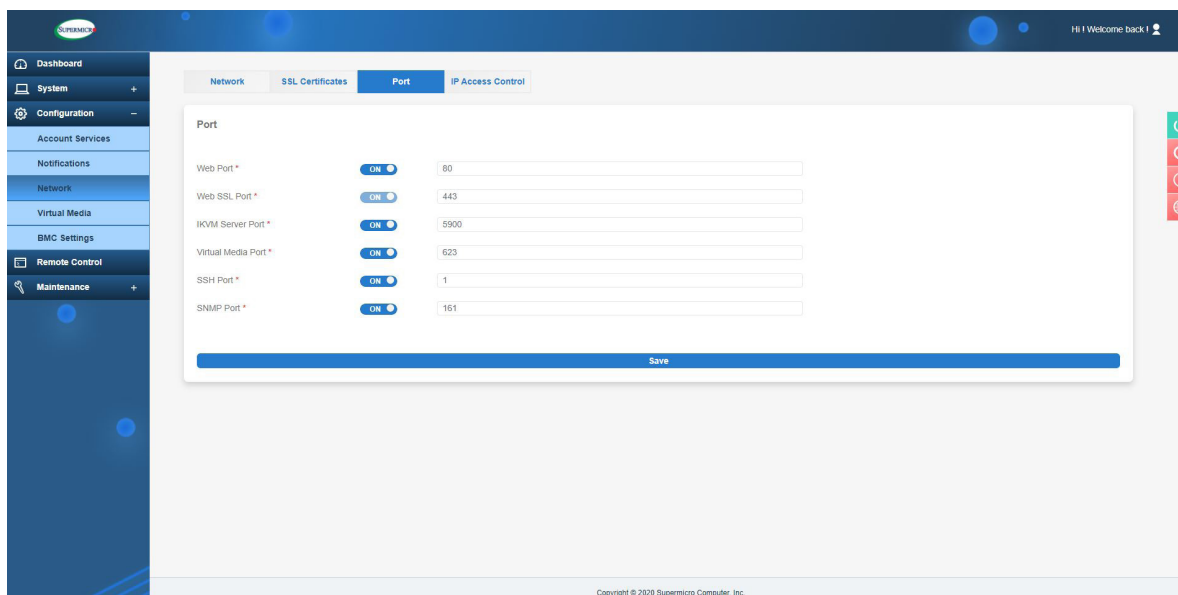
Users can click [Upload] to upload the certificate and the private key to the server. Once uploaded, the BMC will reset itself for the new certificate to take effect.



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

Port

This tab provides the following ports along with the associated standard port numbers. Most ports can be modified by users. The following ports are ON or OFF by default.



Users can turn on/off the following port options to enable/disable each port and enter its respective port number.

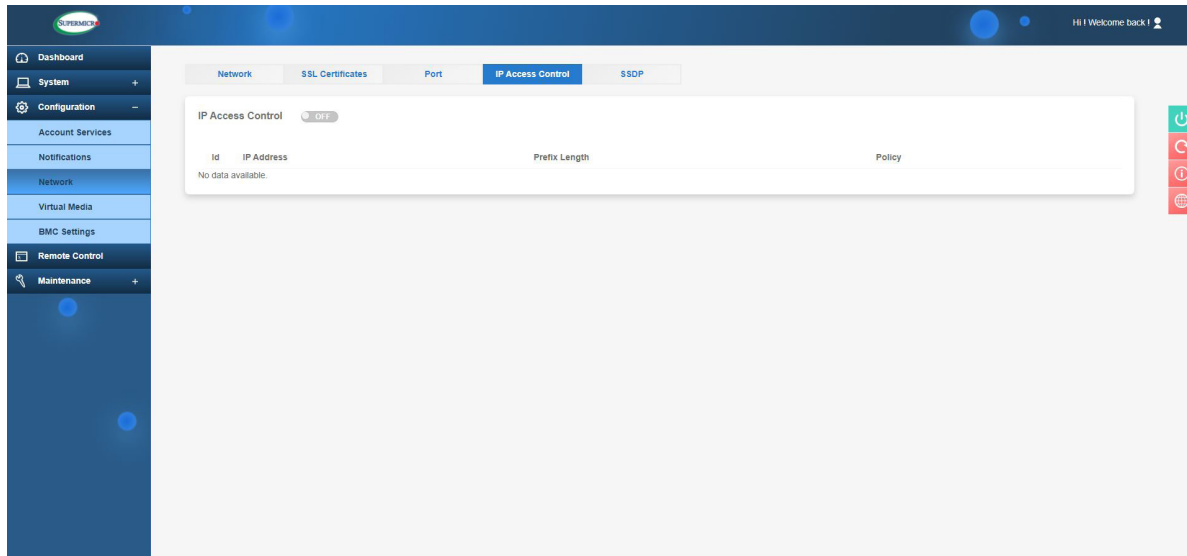
- Web Port: ON (80)
- Web SSL Port: ON (443)
- IKVM Server Port: ON (5900)
- Virtual Media Port: ON (623)
- SSH Port: ON (22)
- SNMP Port: OFF (161)

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

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

IP Access Control

Use this page to configure IP access control policy. Users can set up to 10 rules on this page. Please note that the default policy is OFF (disabled) and default rule is ACCEPT. Users can set up rules for either IPV4 or IPV6 IP addresses.



The access control list will include the following information.

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

Users can adjust the following options.

- [Enable IP Access Control button]: Users can click enable or disable IP access control features.
- [Add button]: Users can select to add a new rule to the list.
- [Modify / Edit button]: Users can select a policy and click to change its rule.
- [Delete button]: Users can select to delete an existing policy.

For the same IP addresses with the same prefixes, the following rules apply.

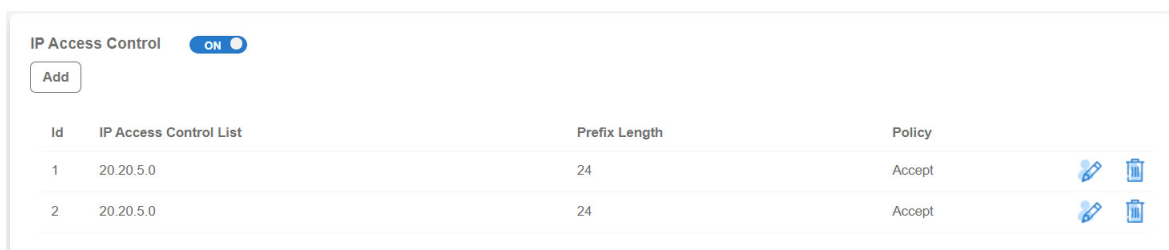
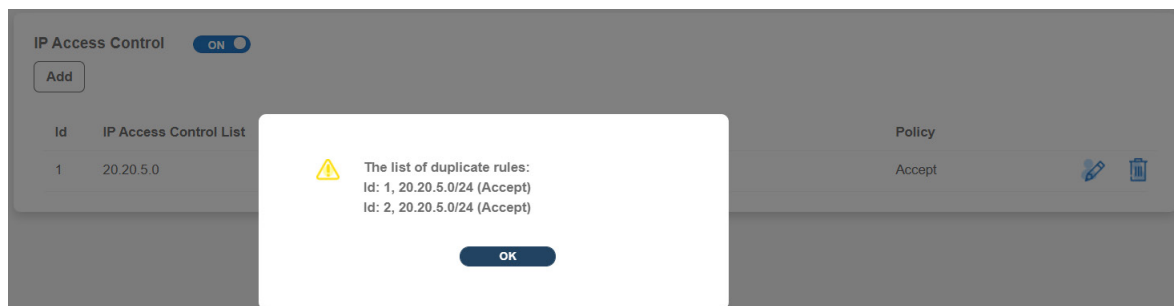
- BMC / Web UI will follow ID order.
- BMC always follows ID #1 when users set the same or different policy (ACCEPT/DROP) for the same IP Address with the same prefix. See below example for details.

Web UI follows ID #1

Id	IP Address	Prefix Length	Policy
1	20.20.5.0	24	Accept
2	20.20.0.0	16	Accept
3	20.0.0.0	8	Drop

These 3 IPs are set as 20.20.5.0 but with different prefixes.

- Users can still set the IP policy but BMC will pop up a notification to users when Save button is clicked by users.



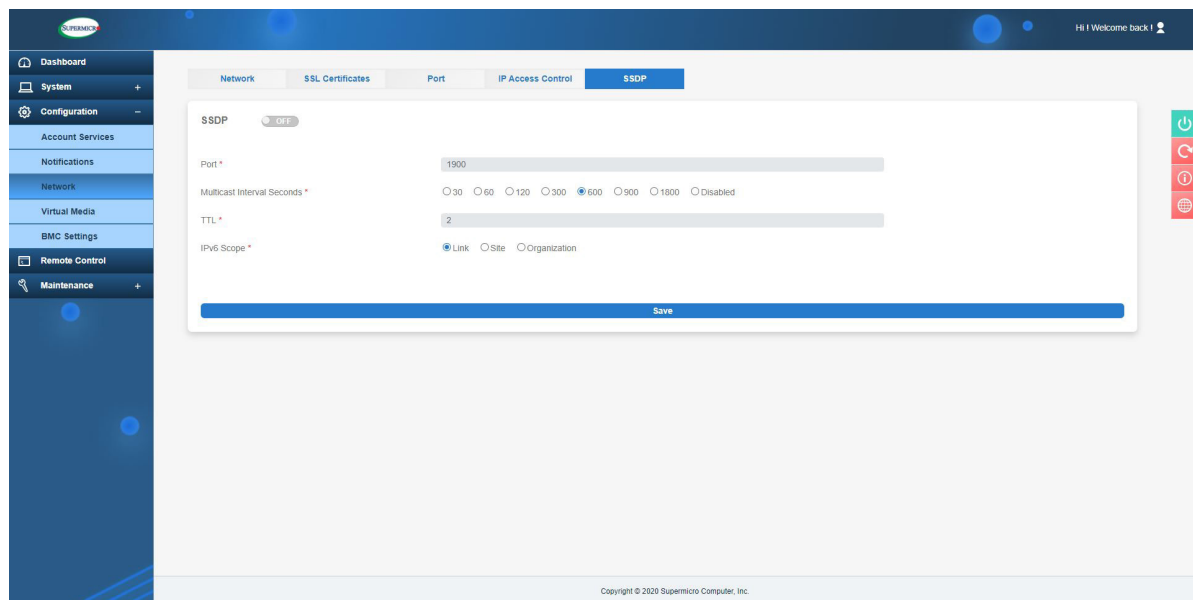
Web UI follows ID #1

Id	IP Address	Prefix Length	Policy
1	20.20.5.0	24	Accept
2	20.20.0.0	16	Accept
3	20.0.0.0	8	Drop

The ID number notifies users when the IP access control is already set for %IP_ADDR after they click the save button. In the example shown above, the notification is that the IP access control is already set for 20.20.5.0.

SSDP (Simple Service Discovery Protocol)

Use this page for broadcast and discovery of network services on the user's local network.



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

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

2.7.4 Virtual Media

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

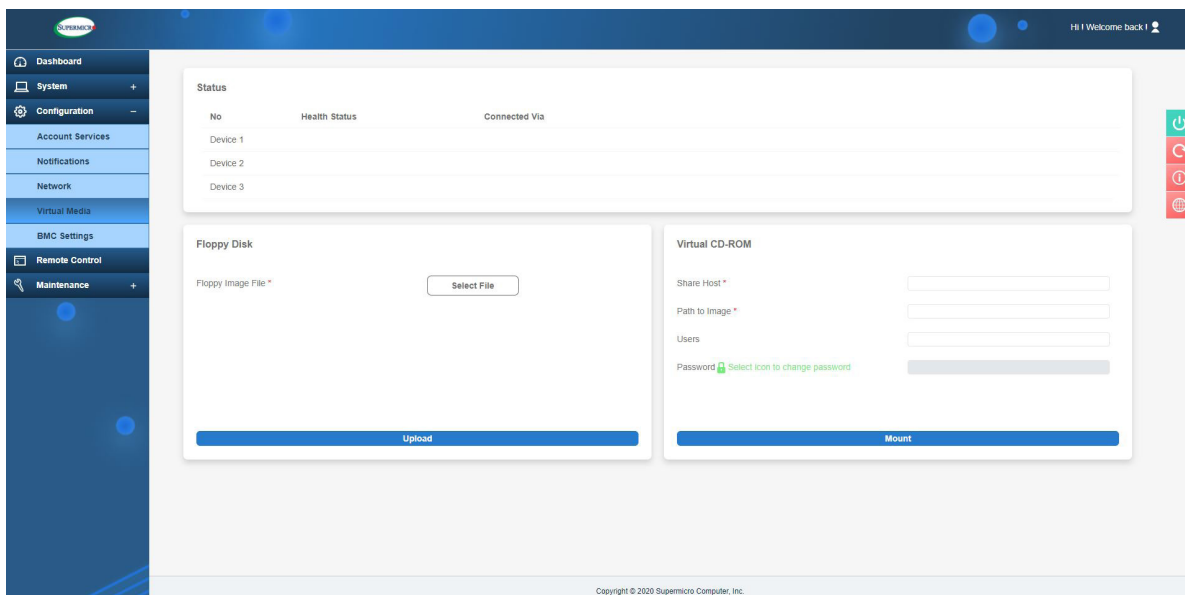
Status

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

Floppy Disk

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

1. Choose File: Users can upload a floppy image. The allowed file type is img files.
2. Upload: Users can click on [Upload] to upload the image file to the server.



Virtual CD-ROM

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

Moreover, the domain part will only accept http:// or https:// at the beginning, (HTTP+ IP Address, HTTPS + IP Address, and only IP Address). Port numbers can be used after IP Address as an option.



Note: HTTPS service will not be supported.

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

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

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

- Password: The feature will only accept the following character classes. All other special characters, including space and tab, will be rejected.
 - a through z
 - A through Z
 - 0 through 9
 - ^

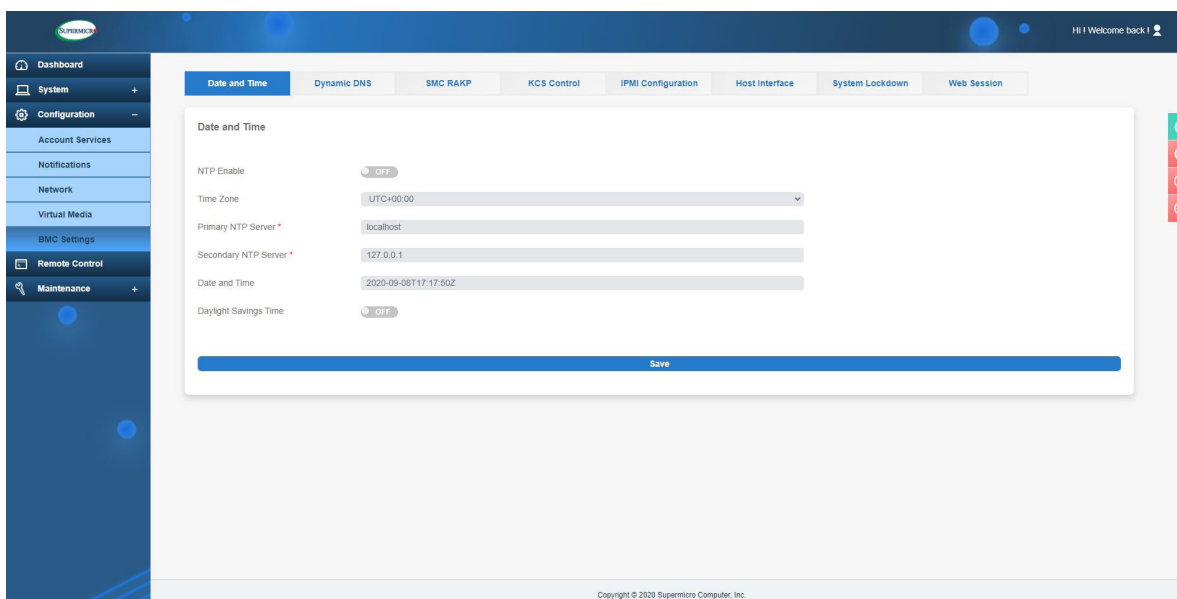


Note: CD-ROM mounting supports HTTP, HTTPS, Samba, and the Windows CIFS method.

2.7.5 BMC Settings

Date and Time

Users 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.



Users can adjust the following fields.

- **NTP Enable:** Users can enable or disable NTP server settings. If NTP is disabled, the system time is used to set date and time. 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 (i.e. from BIOS). If NTP is 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 users.

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



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

- **Primary NTP Server:** Users can enter primary NTP server info.

- Secondary NTP Server: Users can enter secondary NTP server info (optional).
- Date/Time: Users can view the time in HH:MM:SS format.
- Daylight Savings Time: Users can turn ON this field for applying Daylight Savings Time.

Dynamic DNS

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



Note: NTP service should be enabled prior to Dynamic DNS (Domain Name System) configuration.

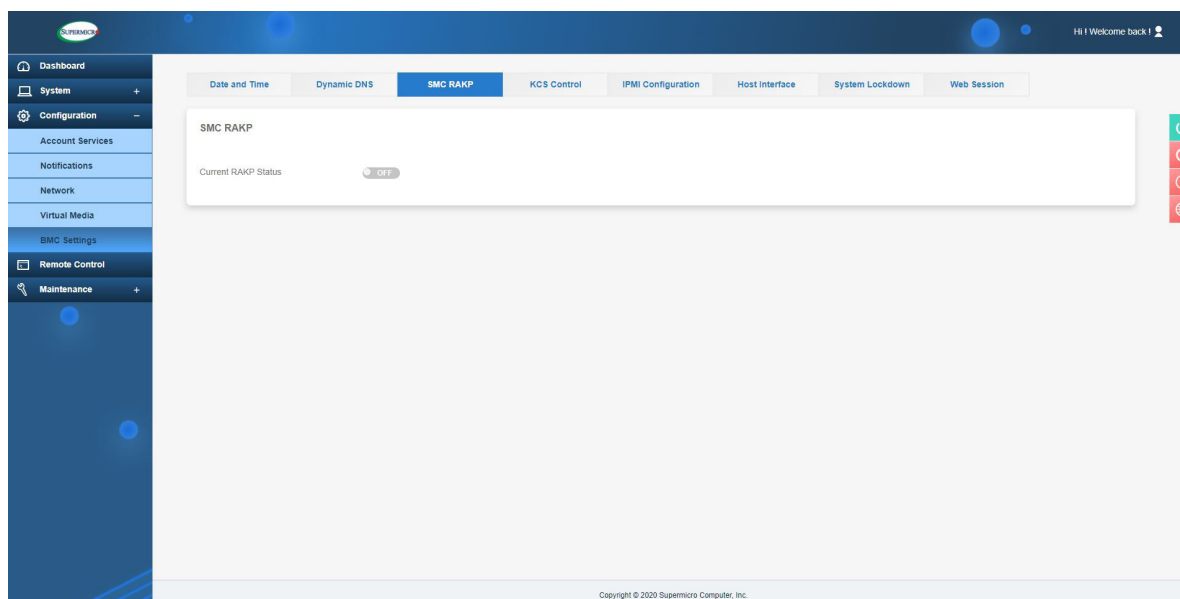
- Dynamic Update Enable: Users can enable/disable Dynamic DNS (Domain Name System) update support.
- Dynamic DNS Server Address: Users can view the server address of the user's Dynamic DNS server.
- BMC Hostname: Users can name of the BMC (Baseboard Management Controller) Host Server.
- TSIG Authentication: Users can enable TSIG (Transaction Signature) authentication support and upload TSIG.key files.



Note: Fields with * are optional.

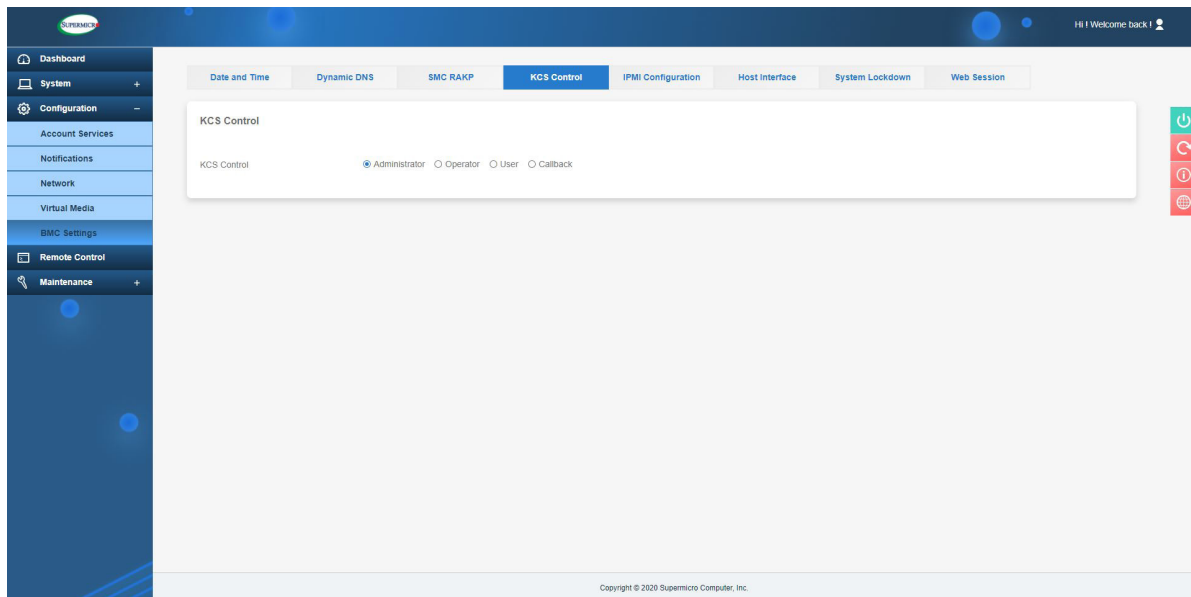
SMC RAKP

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



KCS Control

This feature allows users to secure their environment by configuring appropriate privileges to access KCS interface.



Users can select one of the following options to determine who is allowed what supported privilege.

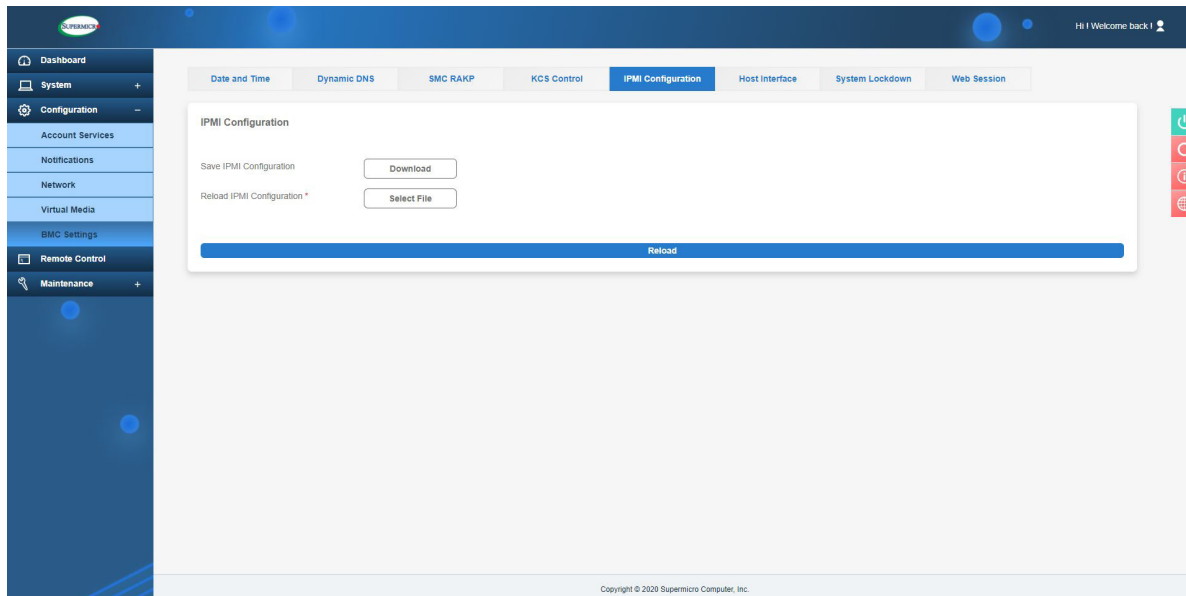
- Administrator: Any users accessing KCS interface will be able to do all the operations that an administrator user can do.
- Operator: Any users accessing KCS interface will be able to do all the operations that a user with Operator privilege can do.
- User: Any users accessing KCS interface will be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

IPMI Configuration

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

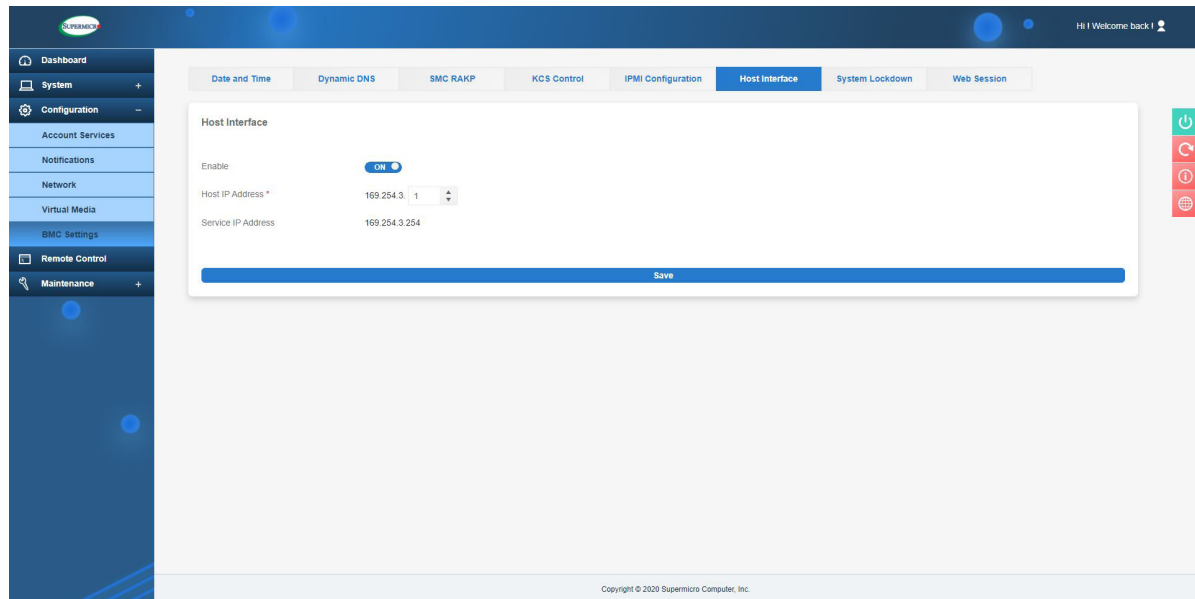


Note: The saved IPMI Configuration option will download the IPMI configuration .bin file.



Host Interface

Host interface (HI) provides a Ethernet over USB solution, which has the the ability to connect ethernet devices via USB.



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

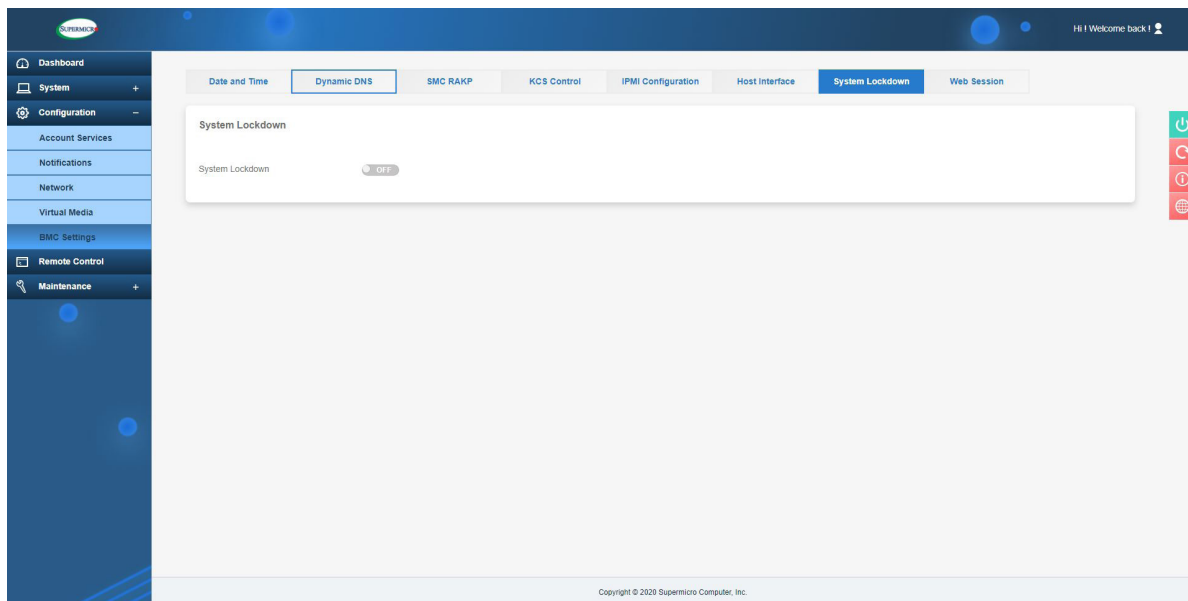
- Enable: Users can enable/disable this service.
- Host IP Address: Users can set up a host IP address that is assigned to the host OS.
- Service IP Address: Users can view the management host interface service IP. This is READ ONLY.

System Lockdown

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



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

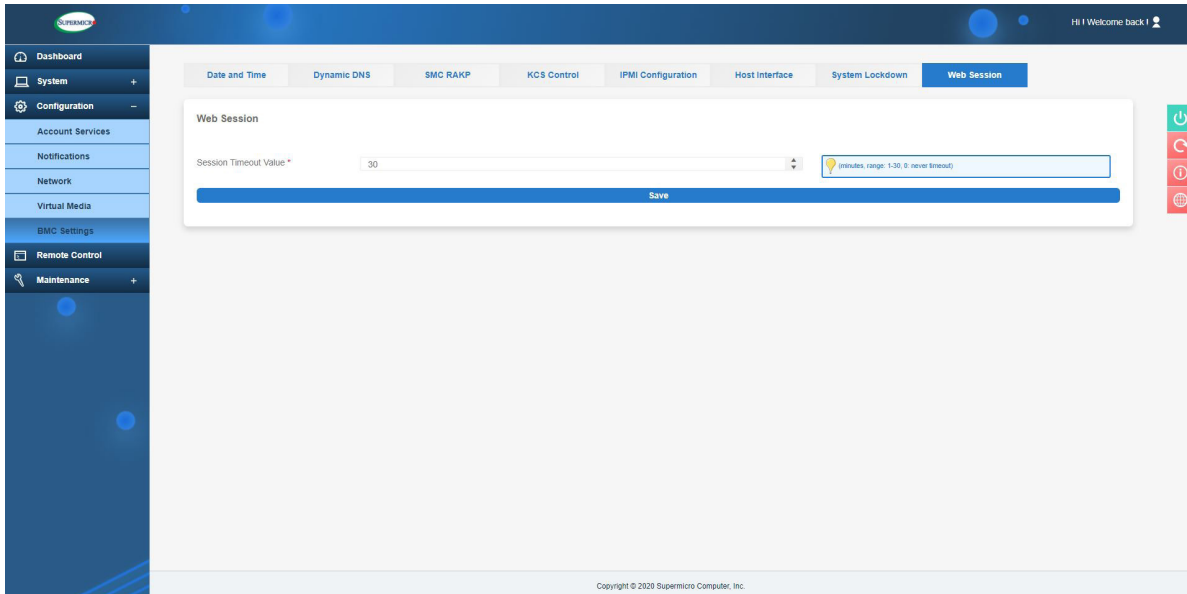


The following features will be functional during system lockdown.

- System power operations
 - Power on
 - Power off
 - Reset
- Identify operations (Chassis identify)
- IPMI configuration download
- Maintenance events download
- UID control

Web Session

Users 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 0 minutes.



Smart Power

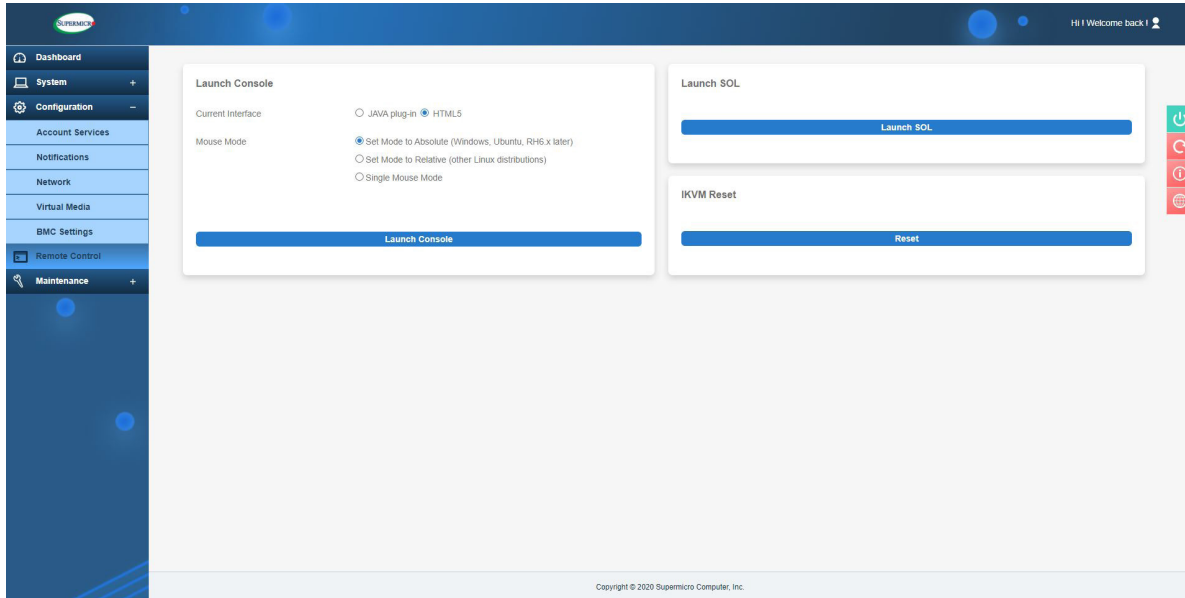
Currently, users can turn on or enable Smart Power Option for the “Big Twin” and “H12DST-B” systems on this page. Additional supported systems will be added accordingly. The feature will involve Power Supply, BMC, and CPLD. Smart Power will be activated when a PMBUS alert happens.

Alerts will be sent to “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 is reset or b) there is a lost or additional power supply to the system. In those cases, IPMI/BMC will find out the power supply and set the CPU power limit.

2.8 Remote Control

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



Launch Console

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



Note: Java Console is the default selection for X12 and H12 platforms. Once a remote console session is connected, switching between JAVA and HTML5 is not allowed.

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

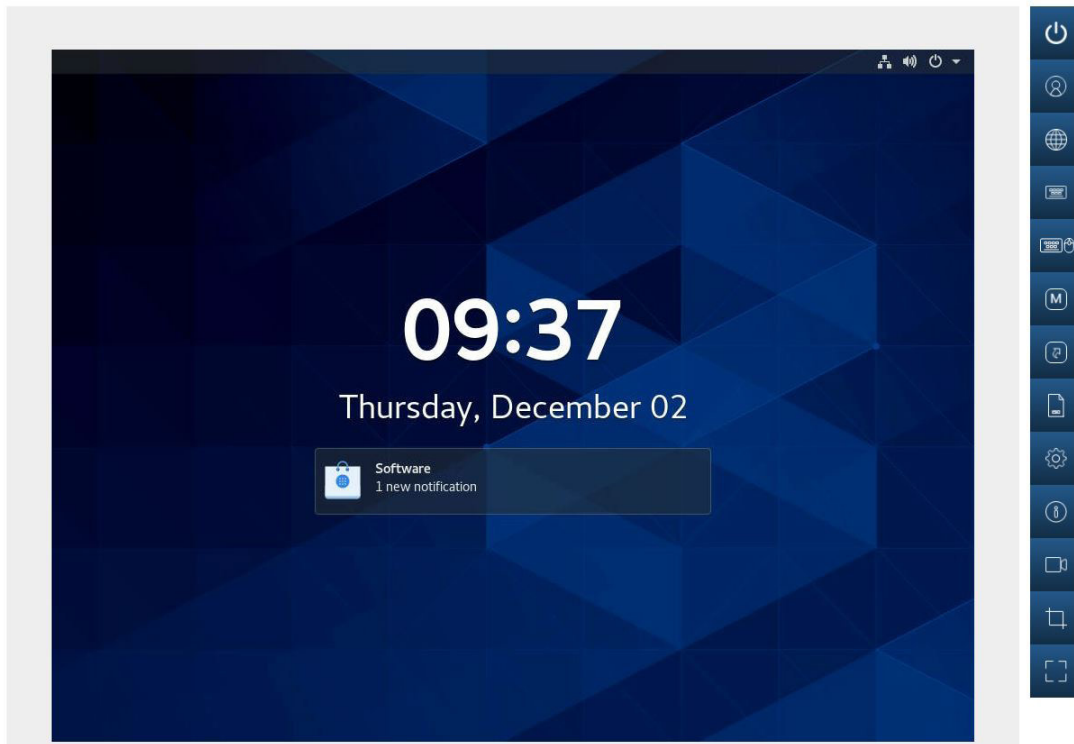
1. Select JAVA plug-in interface option.
2. Click on [Launch Console] to launch Console Redirection or KVM Console.

To launch a HTML5 remote console, refer to the following steps. A console in a new browser window will automatically pop up.

1. Select the HTML5 option.
2. Click on [Launch Console] to launch Console Redirection or KVM Console.



Note: Video recording only works with Chrome browser.



Mouse Mode

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

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

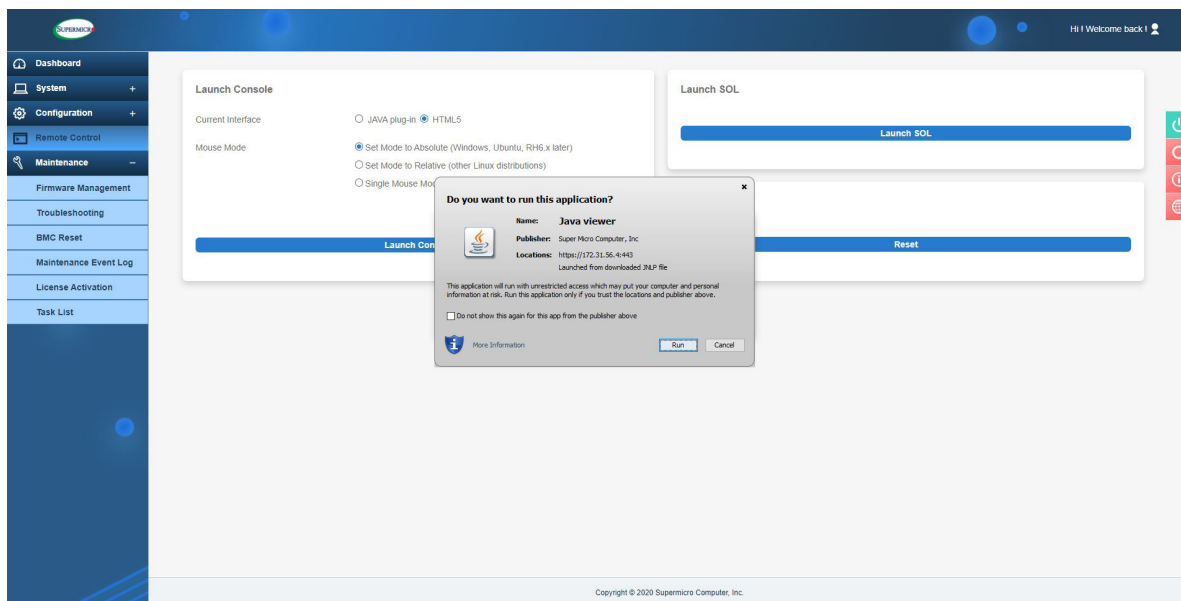


Note: IPMI is an OS-independent platform and iKVM support is an add-on feature of IPMI. For the mouse to function properly, please configure the Mouse Mode settings (see above) according to the type of OS used in the system.

Launch SOL

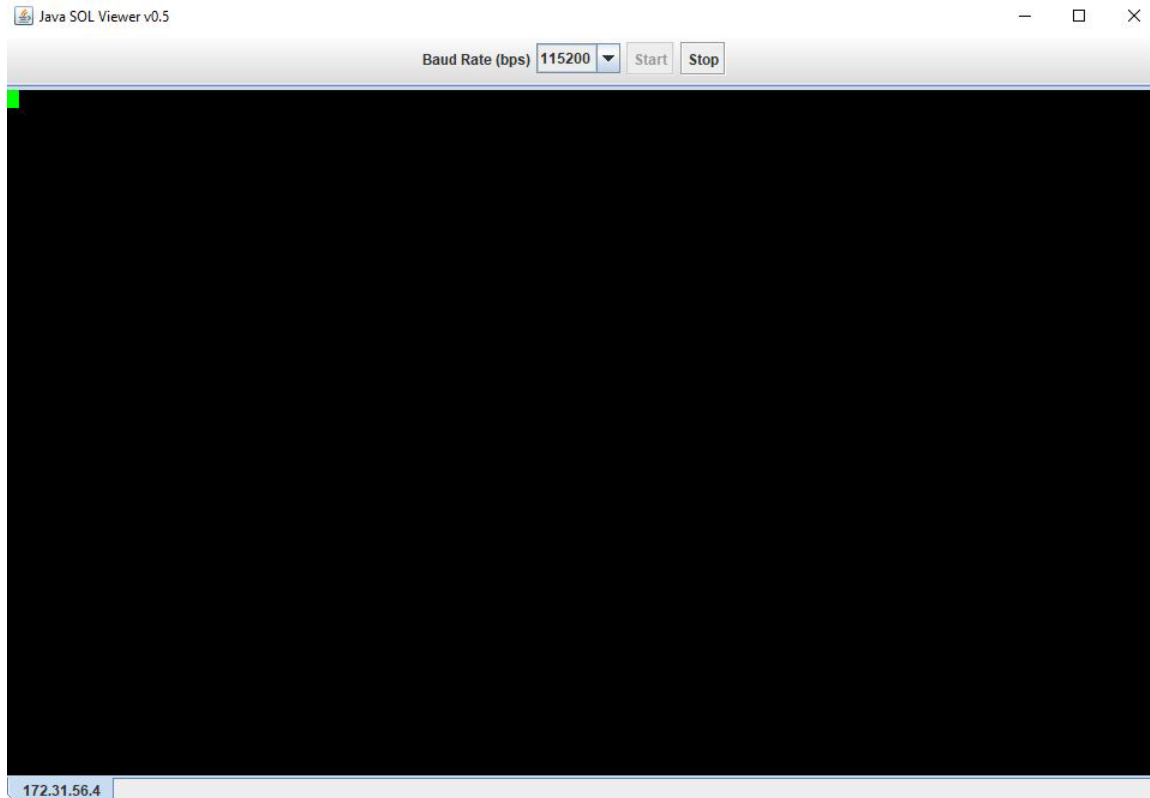
This page allows users to launch a remote console using SOL (Serial over LAN), which provides serial port connections over LAN to access a host server via console redirection. It also allows the system administrator to monitor and manage servers from a remote site. In order to connect the console through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

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



To launch console using SOL, please refer to the following steps.

1. Click [Launch SOL].
2. In the dialog box that asks "Do you want to keep launch?" click [Run]. A warning may pop up.
3. Click [launch] to download.
4. The SOL Viewer screen will appear as shown above.



Once the user has reached the Java SOL viewer, the following options are available.

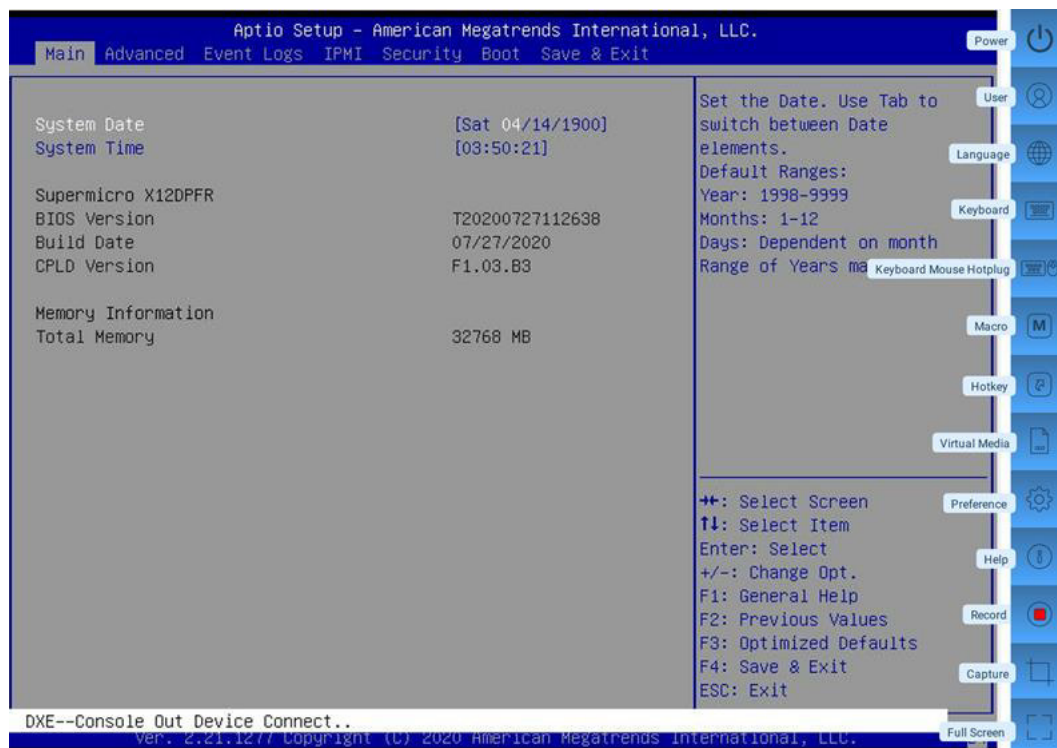
- Baud rate (bps): Users can select one of the following SOL transfer rates from the pull-down menu. Make sure that the baud rate selected matches the baud rate set in the UEFI BIOS.
 - 9600 bps (bits per second)
 - 19200 bps
 - 38400 bps
 - 57600 bps
 - 115200 bps
- Start: Users can start the session after selecting a baud rate. Once the session has started, SOL commands can be imputed through the command-line interface.
- Stop: Users can stop the SOL connection.

iKVM Reset

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

2.8.1 Console Redirection

This feature allows the user 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.

2.8.1a Console Redirection – Power

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

Power Control

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

Close

Apply

Once the user has reached the window shown above, the following options are available.

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

2.8.1b 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

2.8.1c Console Redirection – Language

This feature allows users 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

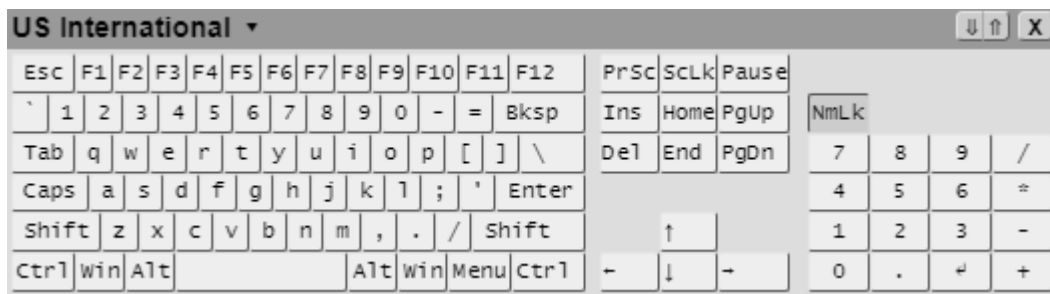
[Close](#)[Apply](#)

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

2.8.1d Console Redirection – Keyboard

This feature allows users to access the virtual keyboard and provides an alternative input mechanism for users unable to use a physical keyboard. Users 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. Please also note that due to language differences in size and shape, the sizes of supported virtual keyboards will be varied. Thus, will not be the same.

2.8.1e Console Redirection – Keyboard Mouse Hotplug

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

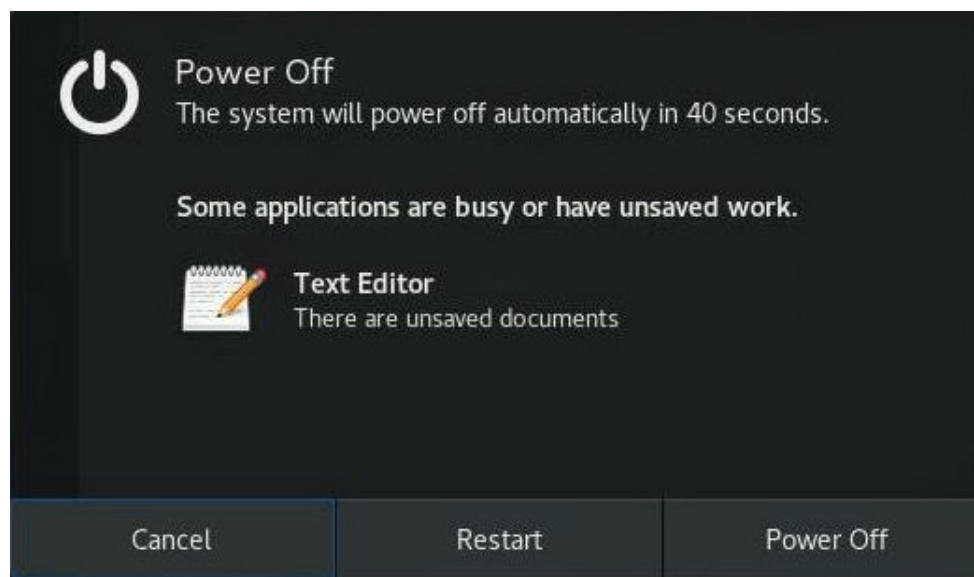


Note: The action of this function is on the server side, not the client's side. Server side is the server on which BMC is installed.

2.8.1f Console Redirection – Macro

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

Hold L Alt	Hold R Alt
Hold L 	Hold R 
L 	R 
Alt+Enter	Ctrl+Alt+Del
Alt+Esc	Ctrl+Tab
Alt+F1	F1
Alt+F4	Pause
Alt+Hyphen	PrntScrn
Alt+PrntScrn	
Alt+Space	
Alt+Tab	

Close

Macro UI

2.8.1g Console Redirection – Hotkey

Hotkey settings allow users to define their 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: Users can switch between mouse modes.
- Exit Remote Location: Users can exit/close iKVM.
- Refresh Screen: Users can recapture one frame of the screen.
- Send Ctrl+Alt+Del: Users can restart the Host OS.
- Toggle Mouse Display: Users can hide or unhide the mouse cursor.

The hotkeys for the display options can be modified to the users' preferences. Users can choose 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 users 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	Ctrl+Shift+	 
Send Ctrl+Alt+Del	Ctrl+Shift+F5	 
Toggle Mouse Display	Ctrl+Shift+F6	 

 Please enter a valid shortcut.

Close

Default

If users 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

2.8.1h Console Redirection – Virtual Media

This feature allows users to upload and share images via the BMC (Baseboard Management Controller). These images will be emulated to the host server as USB applications. Users 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

2.8.1i Console Redirection – Preference

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

Console Redirection – Display

Users 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, users can select low, medium, or high quality depending on the bandwidth of their 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 users 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

Users can select one of the three options depending on the speed of their network. The 256K Cable/DSL is preselected while T1 (1.5 Mbps) and T2 (6.3 Mbps) are options for users who 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. Users can use turn on/off recording time in this tab. A preset two minutes recording time is enabled by default. Users 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

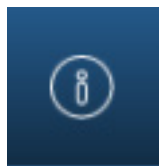
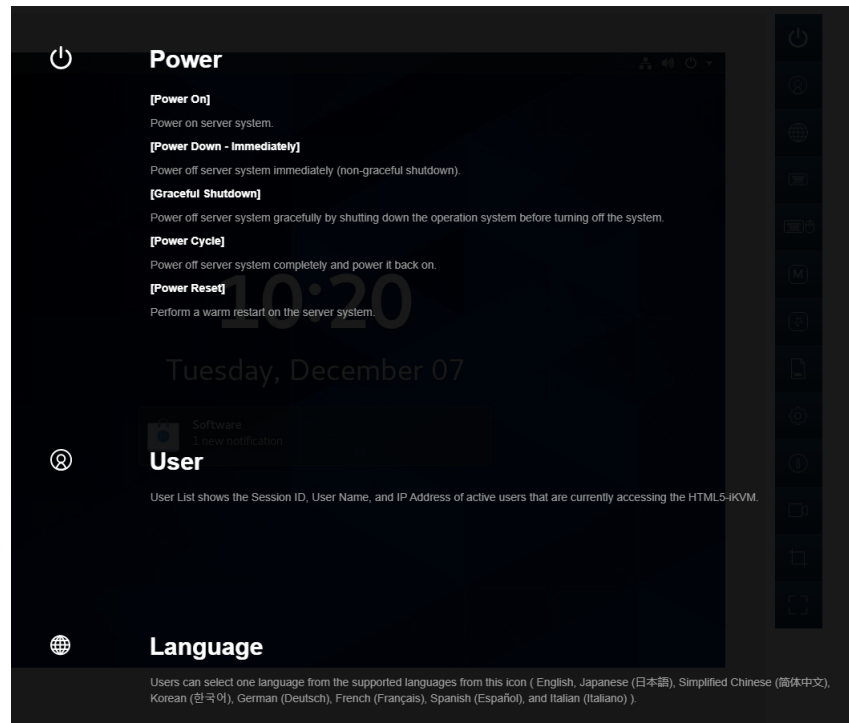
ON ☒ Enable auto stop after minute(s)

New settings will take effect in next recording.

Close

2.8.1j Console Redirection – Help

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



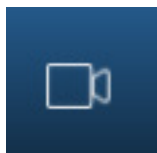
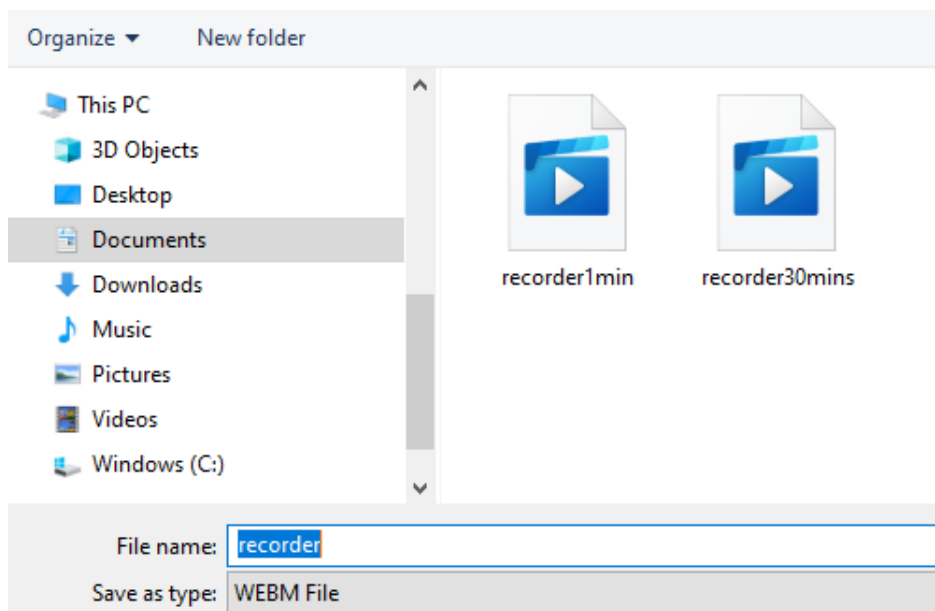
Help Icon

2.8.1k Console Redirection – Record

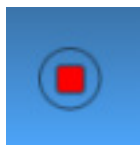
Use this feature to record Video during BIOS booting. After users press the Record button then the Stop button, the recording will be available to be saved as shown below.



Note: Video recording only works with the Chrome browser.



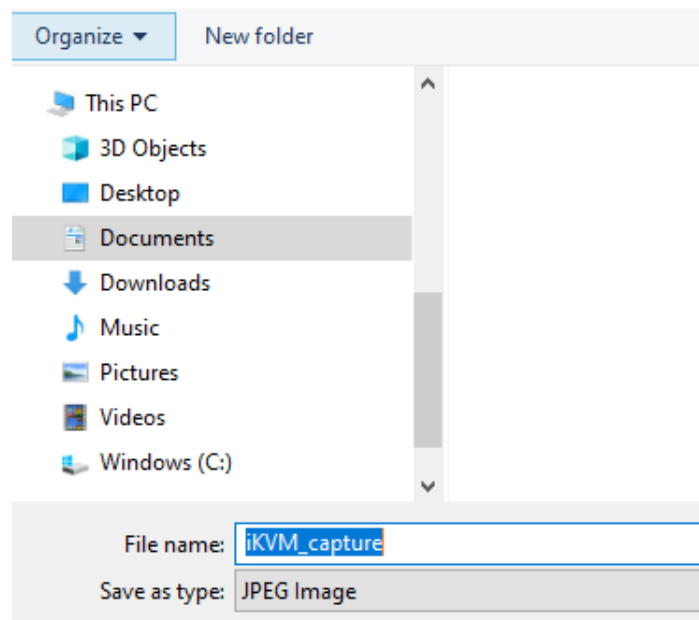
Record Icon



Stop (Recording) Icon

2.8.1I Console Redirection – Capture

Capture allows the user to save an image of the current screen. After users press the Capture button, a JPEG image will be available to be saved as shown below.



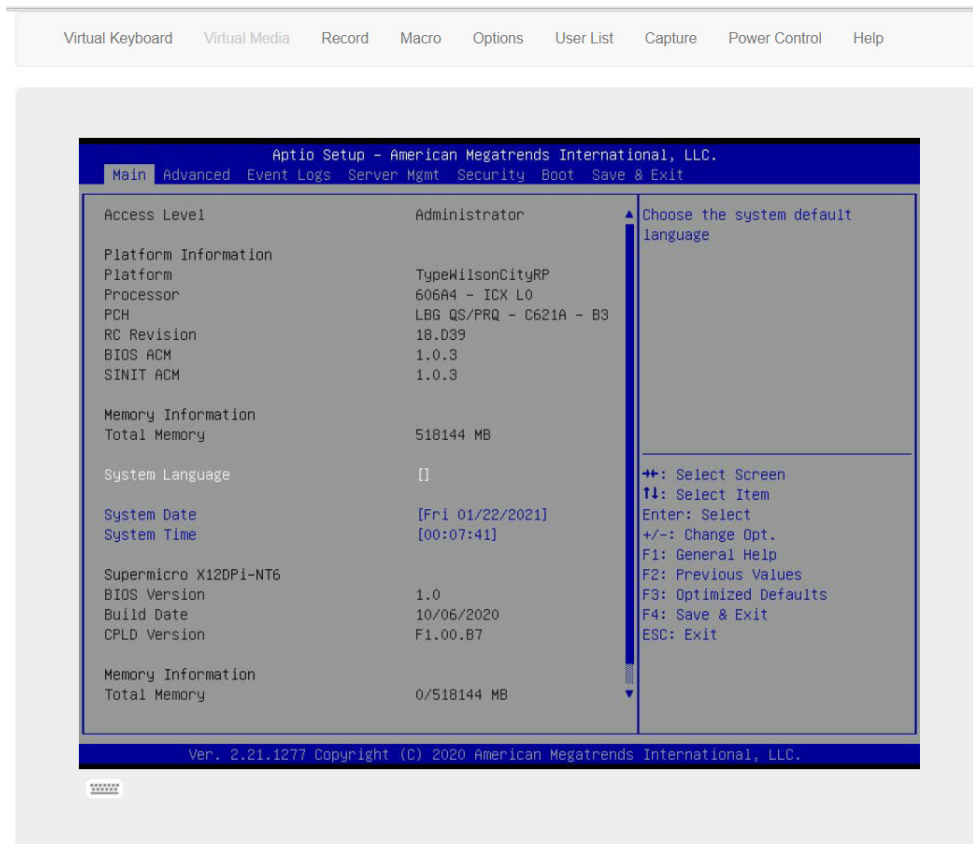
Capture Icon

2.8.1I Console Redirection – Full-Screen

This feature allows users to expand the HTML5-iKVM screen to the maximum display of the monitor screen.

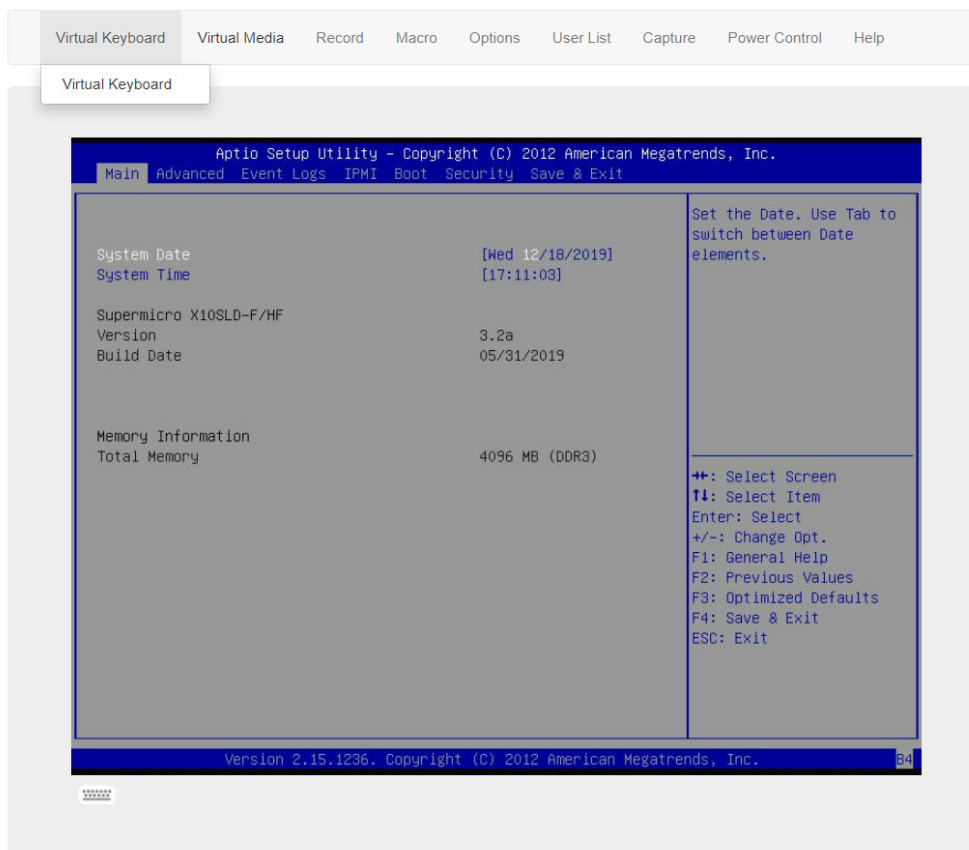
2.8.2 iKVM/HTML5

This feature allows the user 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.

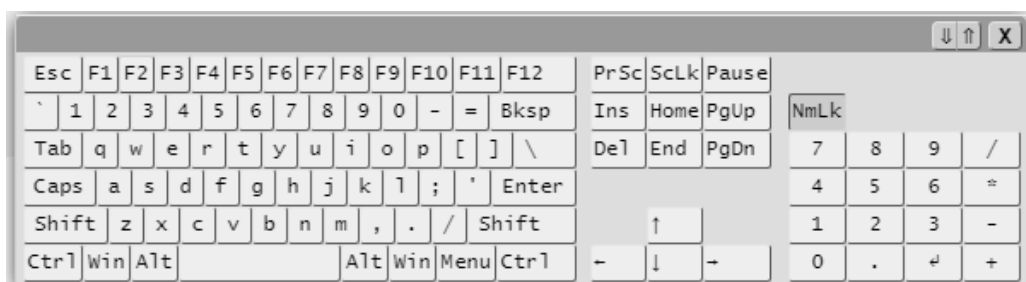


2.8.2a iKVM/HTML5 – Virtual Keyboard

The virtual keyboard provides an alternative input mechanism for users who 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.



2.8.2b iKVM/HTML5 – Virtual Media

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

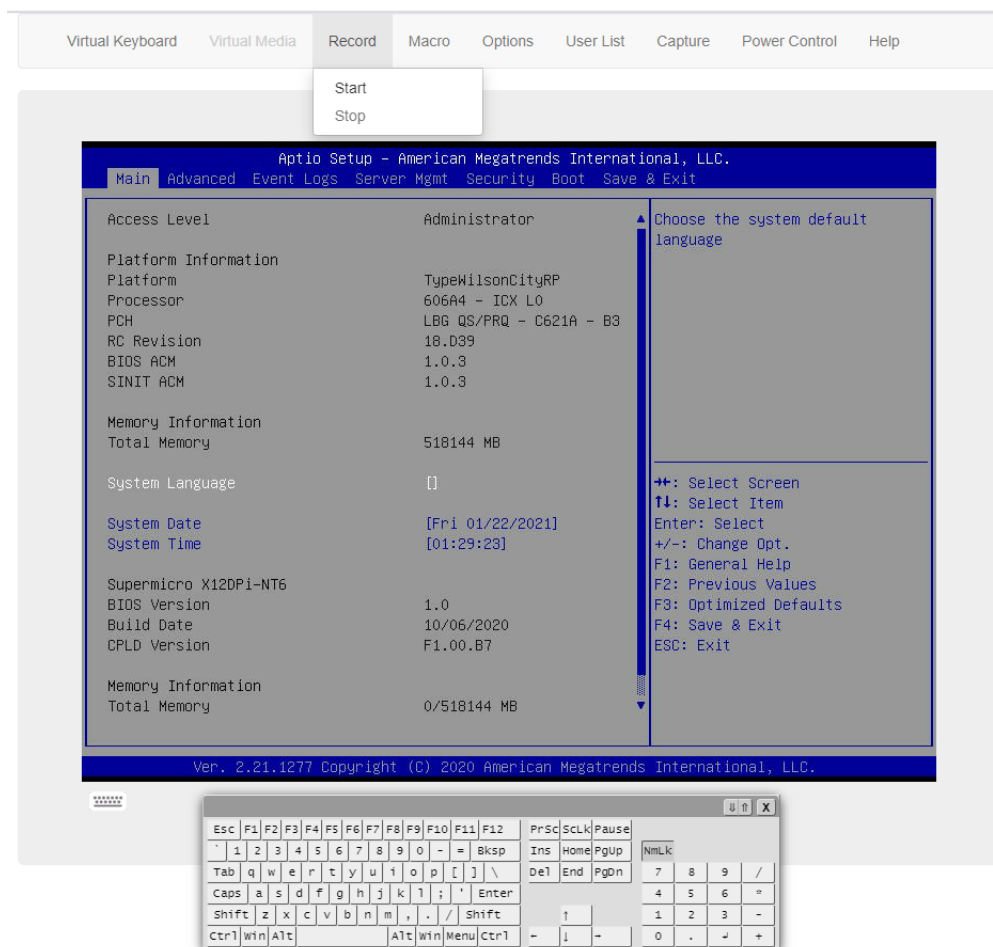
2.8.2c iKVM/HTML5 – Record

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

- **Start:** Users 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:** Users can use this submenu to manually stop the recording process. Recorded videos will be automatically saved onto the user's drive.



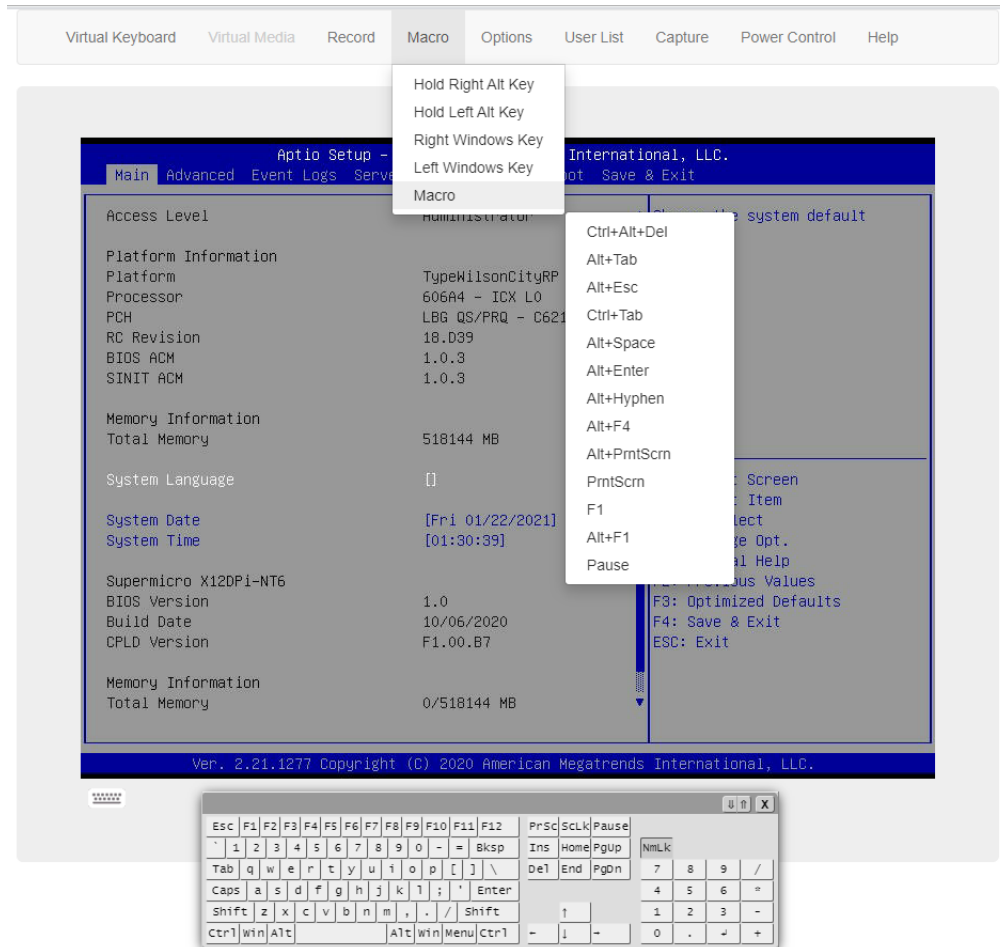
Note: This new HTML5 implementation is currently only supported by the Chrome browser.



2.8.2d iKVM/HTML5 – Macro

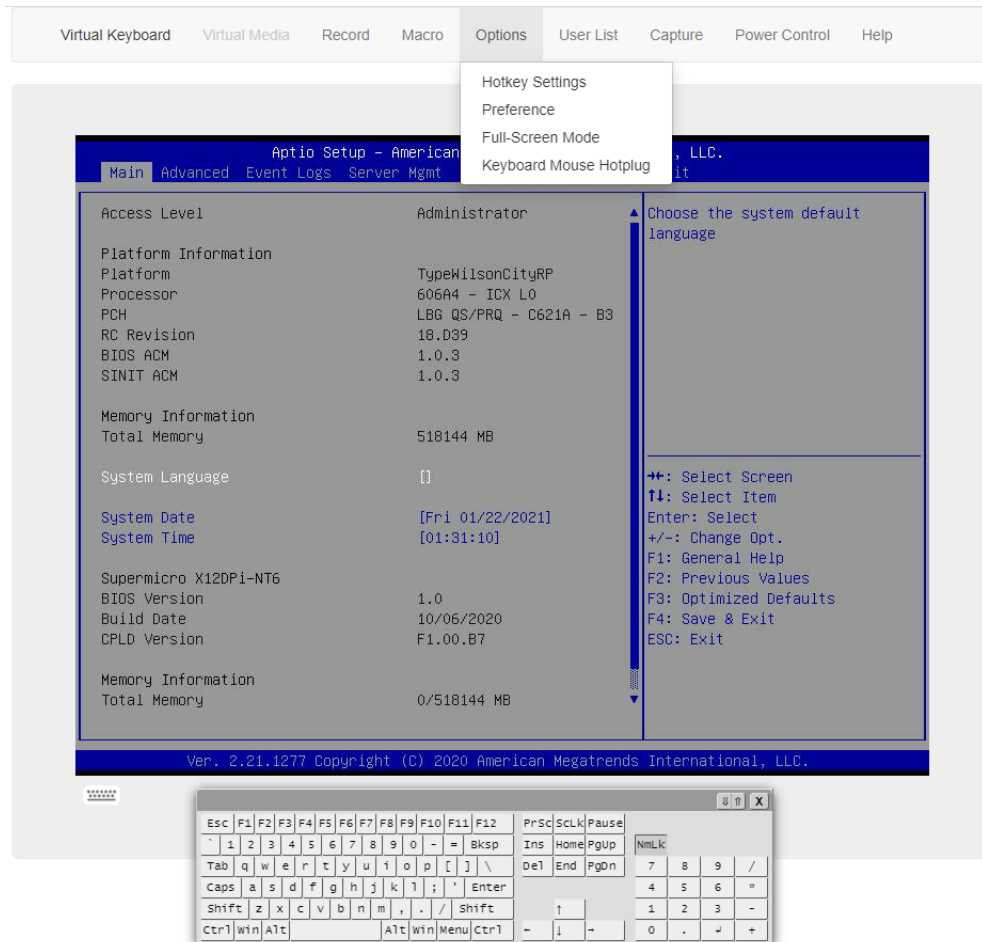
This feature allows users quick access to combo keys.

- 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: Users 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



2.8.2e 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 user preference. However, the adjustable key after Ctrl+Shift is limited to function keys F2 to F12 and numbers 0 to 9. Preference allows the users to adjust Display, Input, Language Setting, and Video Stream Control properties.

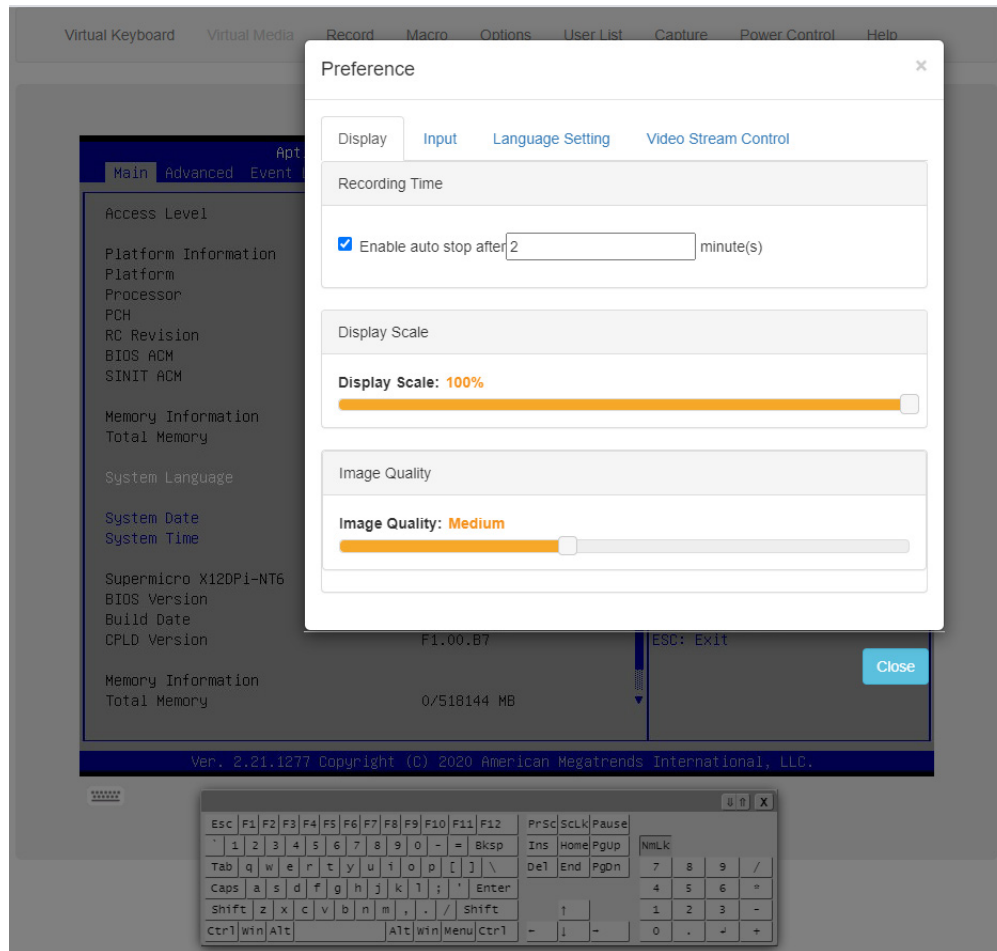
Hotkey Settings

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

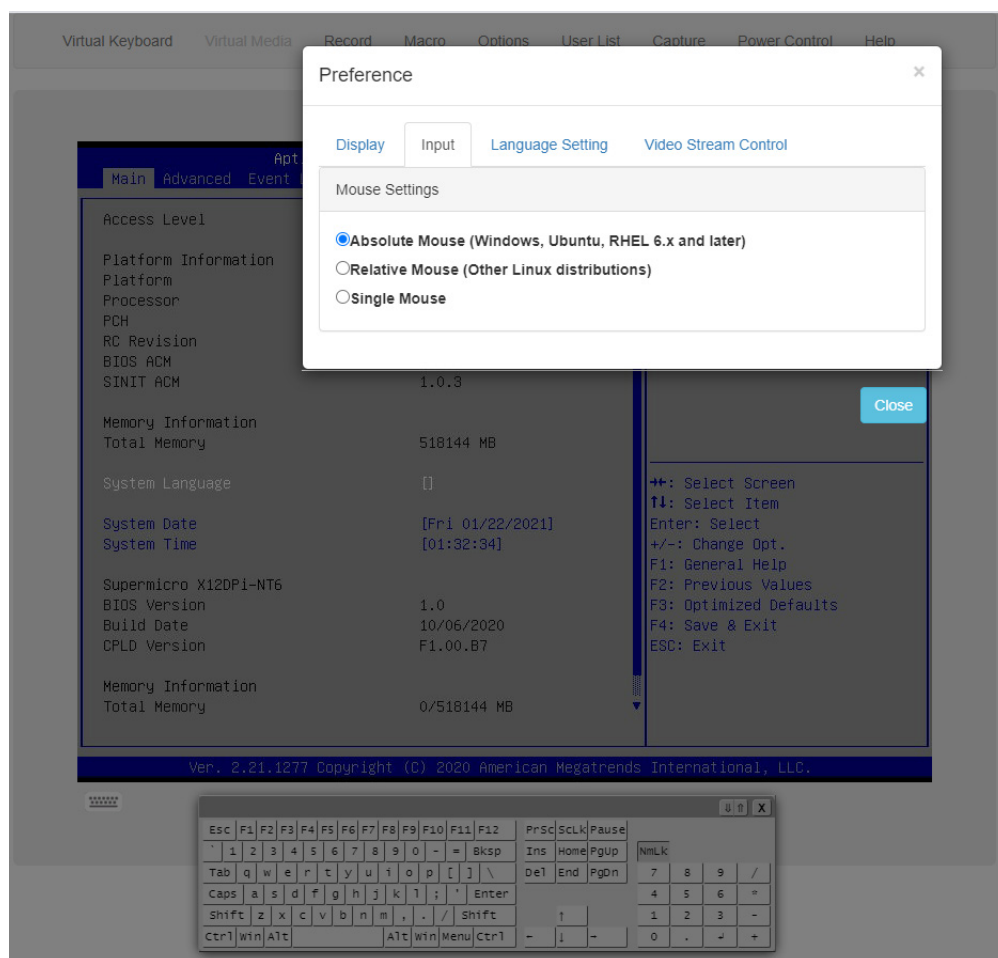
This feature enables auto-stop after n (default: 2) minutes. Adjust the maximum duration of video recordings.



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

Preference – Input

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



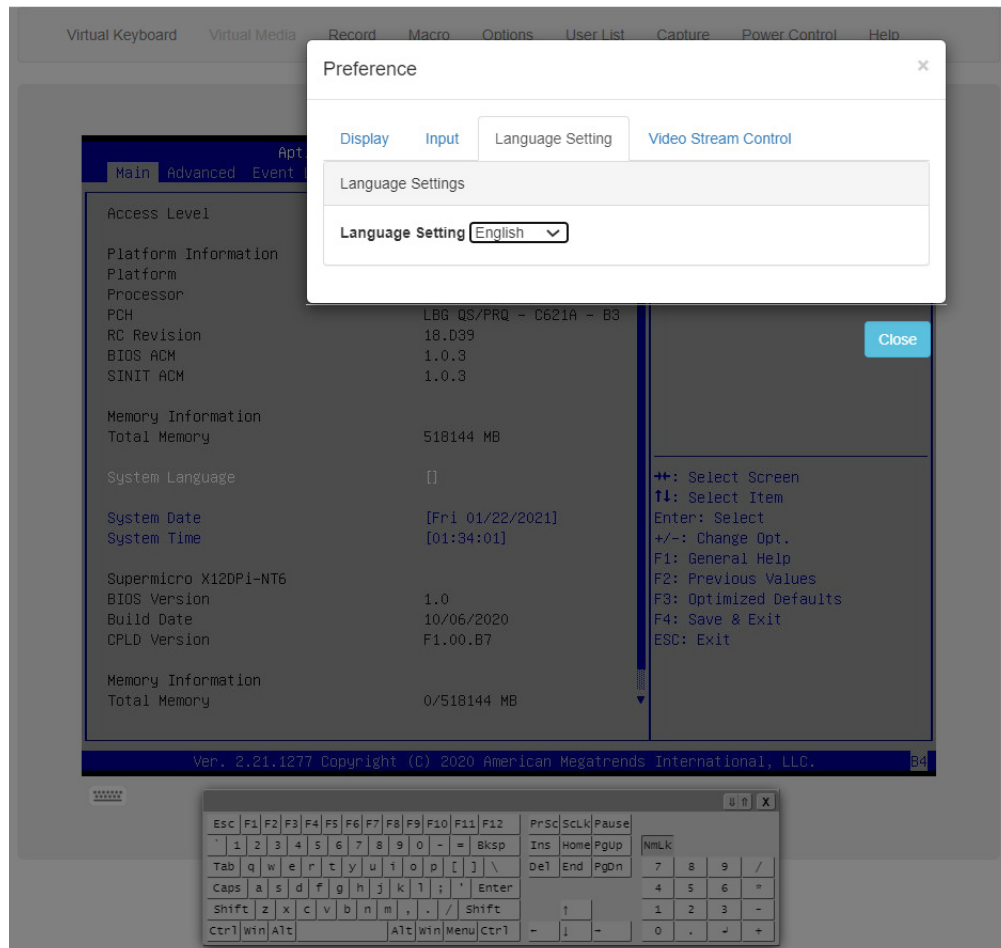
- Absolute Mouse
- Relative Mouse
- Single Mouse



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

Preference – Language Setting

This feature allows users to select one of the following languages to be used by the iKVM/HTML5 interface.

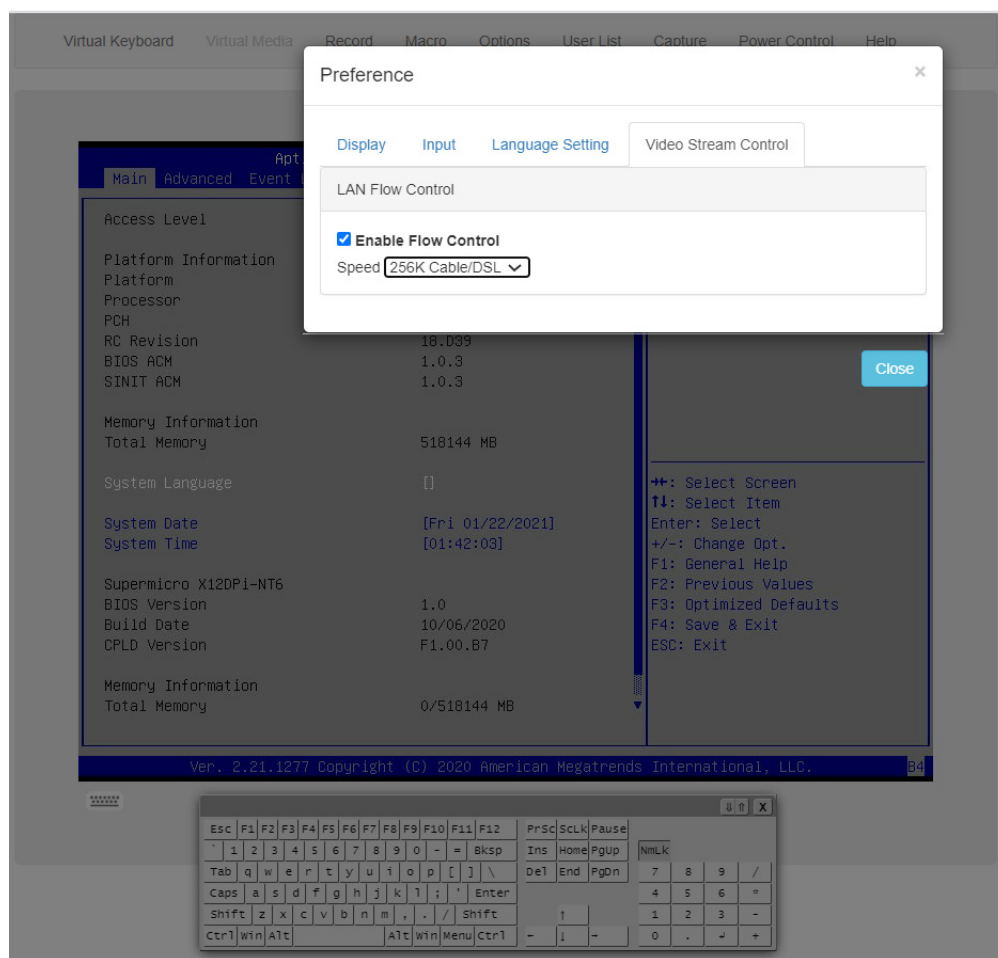


- English
- Japanese
- German
- French
- Spanish
- Italian

Preference – Video Stream Control

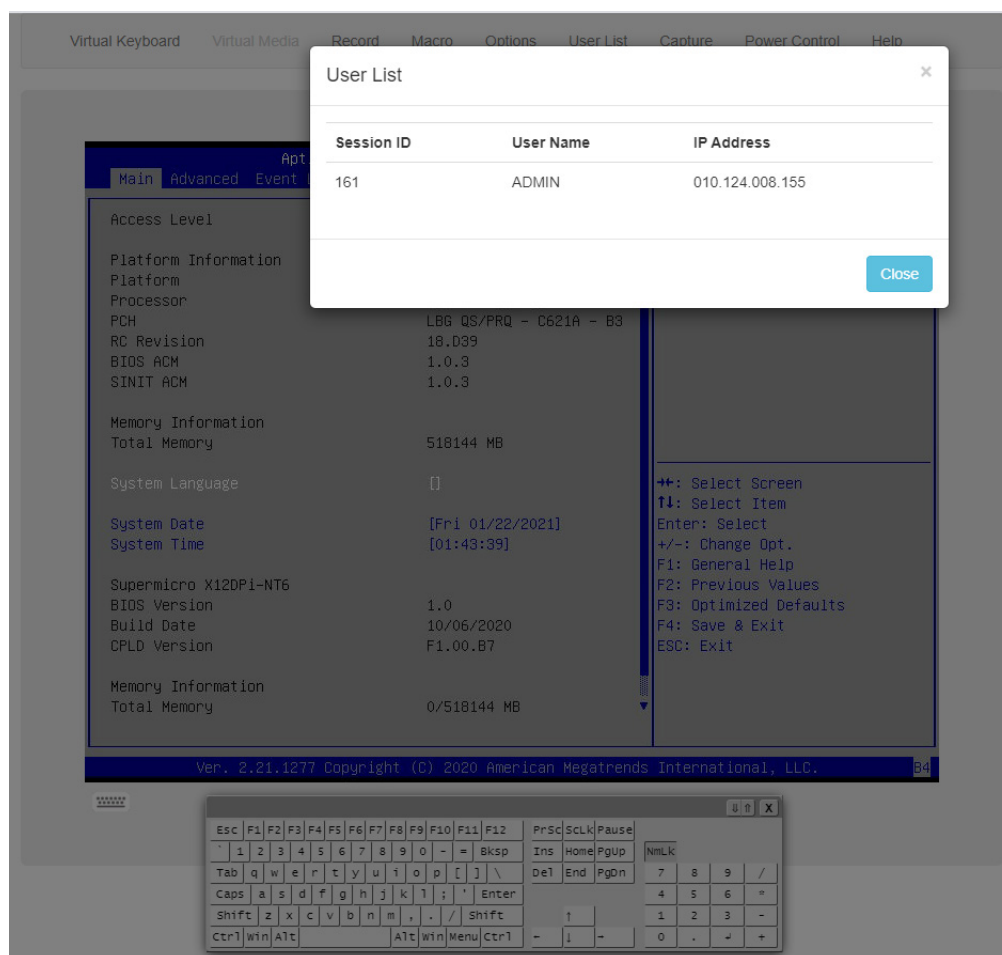
This feature allows users to enable video flow control for LAN Quality of Service (QoS) by selecting one of the following options.

- 256K Cable/DSL
- T1
- T2



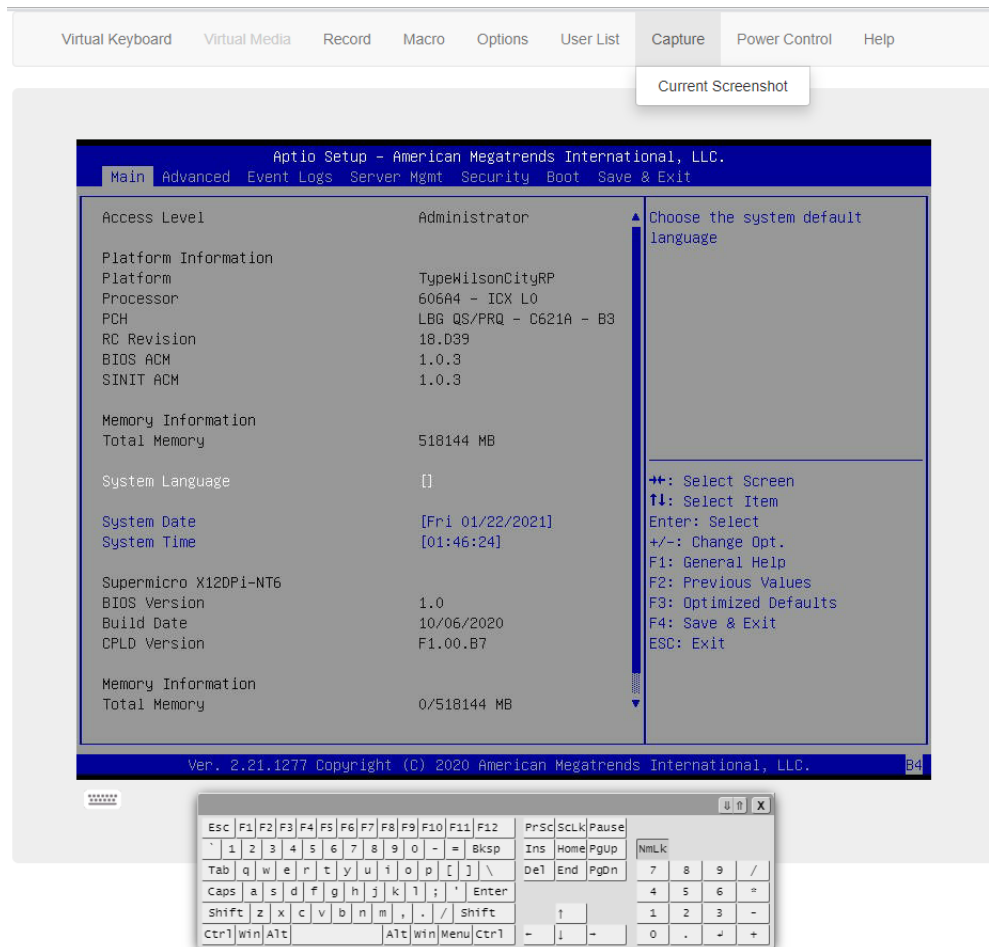
2.8.2f iKVM/HTML5 – User List

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.



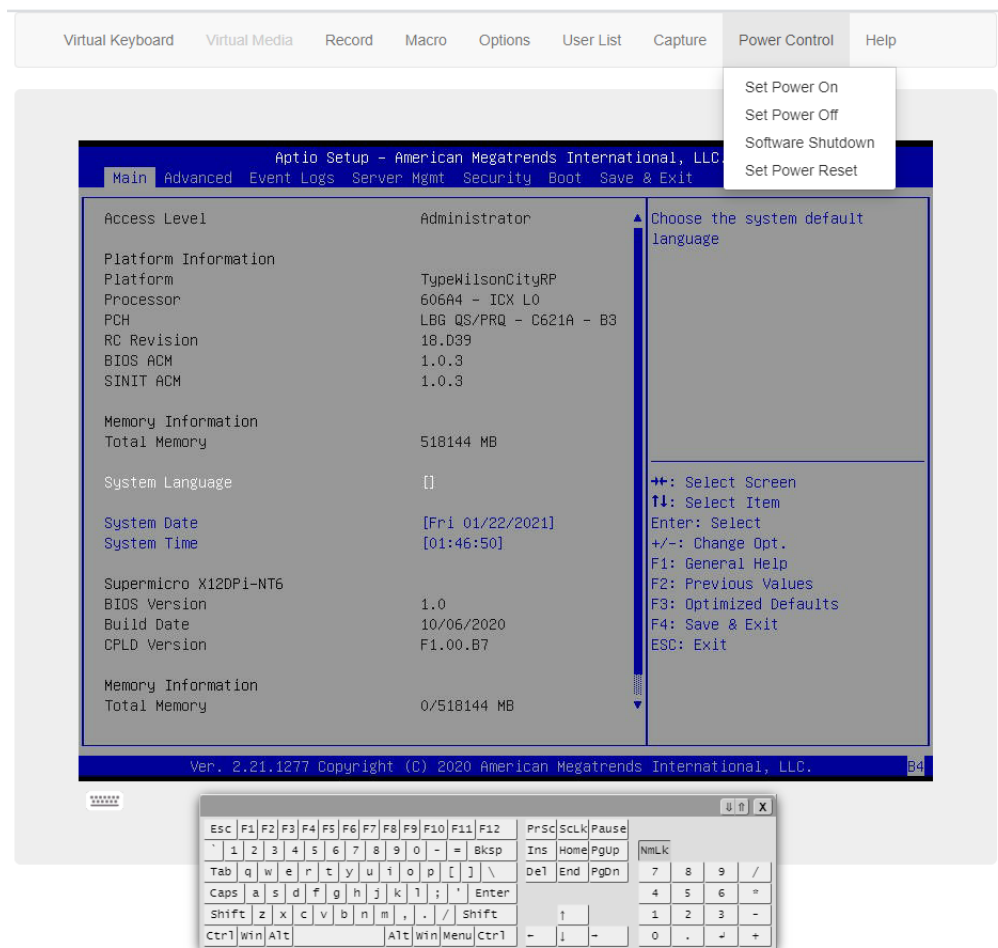
2.8.2g iKVM/HTML5 – Capture

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



2.8.2h iKVM/HTML5 – Power Control

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



2.9 Maintenance

This page allows users 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 512.

2.9.1. Firmware Management

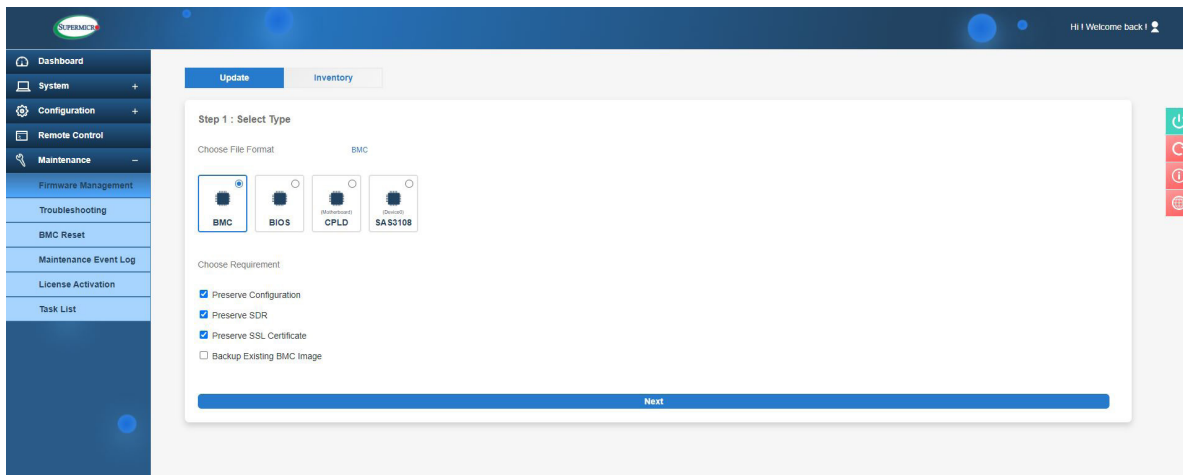
Firmware management page allows administrators to update firmware for BMC, BIOS, Motherboard CPLD, BackPlane CPLD, network AOC, or storage AOC as well as manage Platform Firmware Resiliency (PFR) options.



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

Update

This page allows users with Administrator privileges to update component firmware.



To update firmware, please 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 users click “Upload” button without a firmware image, a message will inform users “Please select an image file. Click here to return.”

4. Update the firmware by clicking the “Update” button. Users 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 the user cancels the firmware updating. If users cancel the firmware updating process, there will be an alert message that pops up to ask users “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!” See images below for details.

 **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!”

BMC update supports the following preserve configuration options.

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

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

- Preserve SMBIOS
- Backup existing BIOS image

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

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

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

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

How BMC Firmware is Updated

The image displays two sequential screenshots of the BMC firmware update web interface.

Top Screenshot (Step 1: Select Type):

- Update** and **Inventory** tabs are at the top.
- Step 1 : Select Type** is the current step.
- Choose File Format:** A row of icons with radio buttons. **BMC** is selected. Other options are BIOS, CPLD (Motherboard), PMem, SAS3808 (Device 0), NIC1 (PCIe Slot2), SAS3808 (Device 0), and SAS3816 (Device 1).
- Choose Requirement:** Four checkboxes are shown: ☒ Preserve Configuration, ☒ Preserve SDR, ☒ Preserve SSL Certificate, and ☐ Backup Existing BMC Image.
- A blue **Next** button is at the bottom.

Bottom Screenshot (Step 2: Select File):

- Update** and **Inventory** tabs are at the top.
- Step 1 : Select Type** is the current step.
- Choose File Format:** A row of icons with radio buttons. **BMC** is selected. Other options are BIOS, CPLD (Motherboard), PMem, NIC1 (PCIe Slot2), SAS3808 (Device 0), and SAS3816 (Device 1).
- Choose Requirement:** Four checkboxes are shown: ☐ Preserve Configuration, ☐ Preserve SDR, ☐ Preserve SSL Certificate, and ☐ Backup Existing BMC Image.
- A greyed-out **Next** button is at the bottom.
- Step 2 : Select File** is the current step.
- Select File:** A text label and a **Select File** button.
- At the bottom are two blue buttons: **Cancel** and **Upload**.

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

The screenshot shows the BMC Update interface. At the top, there are tabs for 'Update' and 'Inventory'. The main area is divided into two steps:

Step 1 : Select Type

Choose File Format: BMC

Choose Requirement:

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

Buttons: Next, Cancel, Upload

Step 2 : Select File

Select File: Select File

Buttons: Cancel, Upload

If users continue on with BMC update, BMC will provide timely percentage of completion. See images below for details.

The screenshot shows the BMC Update interface with a file selection dialog open. The dialog displays the file 'BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp' selected.

File name: BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp.bin

Buttons: Open, Cancel

Name	Date modified	Type	Size
BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp	3/19/2021 8:59 PM	BIN File	47,872 KB
ReleaseNote	3/20/2021 12:54 AM	Text Document	193 KB

UpdateInventory

Step 1 : Select Type

Choose File Format

BMC

BMC

BIOS

(Motherboard)CPLD

PMem

(PCIe Slot2)NIC1

(Device 0)SAS3808

(Device 1)SAS3816

Choose Requirement

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

Next

Step 2 : Select File

Select File

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

(Motherboard)CPLD

PMem

(PCIe Slot2)NIC1

(Device 0)SAS3808

(Device 1)SAS3816

Choose Requirement

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

Next

Step 2 : Select File

Select File

Select File

BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp.bin

46.75 MB

×

Cancel

Upload

142

Dashboard

System

Configuration

Remote Control

Maintenance

Firmware Management

Troubleshooting

BMC Reset

Maintenance Event Log

Licence Activation

Task List

FW Update Mode

Current system is in FW update mode, any configuration changes will not be implemented.

UpdateInventory

Step 1 : Select Type

Choose File Format: BMC

BMC

BIO

CPLD

PMem

NIC1

SA-E1000

SA-E1016

Choose Requirement

☐ Preserve Configuration

☐ Preserve SDR

☐ Preserve SSL Certificate

☐ Backup Existing BMC Image

Next

Step 2 : Select File

Select File

BMC_X12AST2000-RCOT-0201MS_20210319_00.20.02_STDip.bin

X

CancelUpload

Step 3 : File Version

Name	Existing Version	New Version
BMC	00.20.02	00.20.02

CancelUpdate

UpdateInventory

Step 1 : Select Type

Choose File Format: BMC

BMC

BIO

CPLD

PMem

NIC1

SA-E1000

SA-E1016

Choose Requirement

☐ Preserve Configuration

☐ Preserve SDR

☐ Preserve SSL Certificate

☐ Backup Existing BMC Image

Next

Step 2 : Select File

Upgrade Progress : 4%

Select File

BMC_X12AST2000-RCOT-0201MS_20210319_00.20.02_STDip.bin

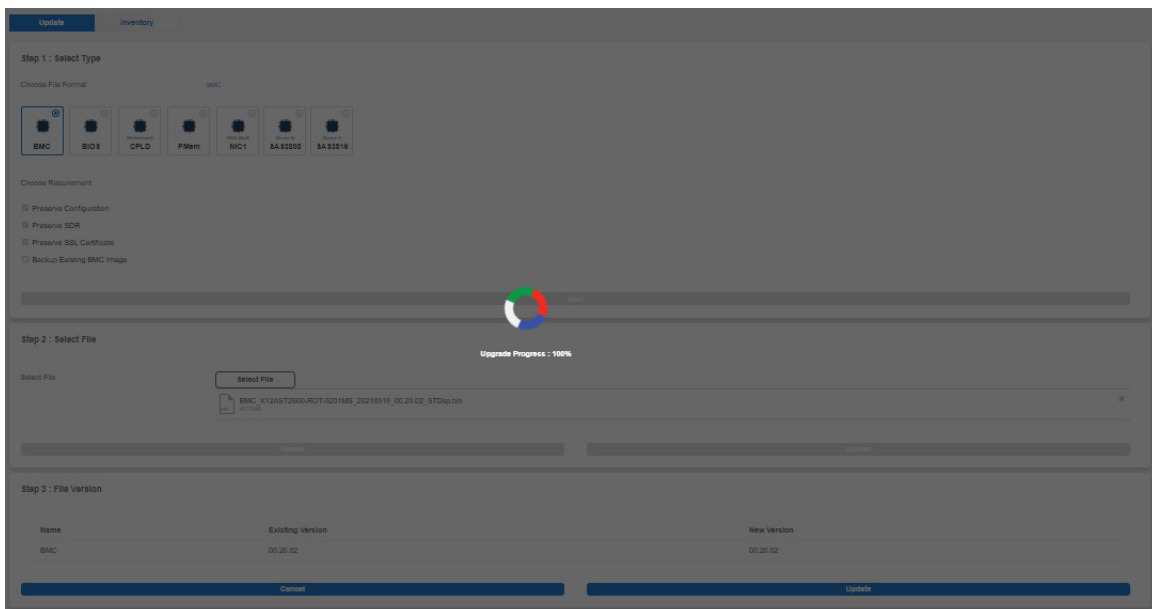
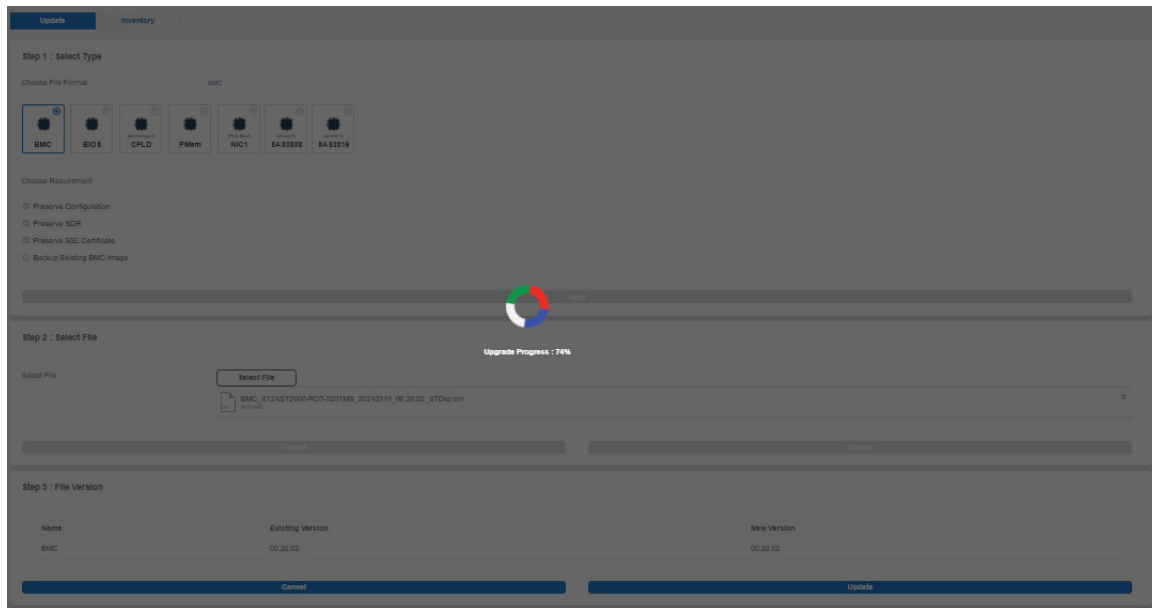
X

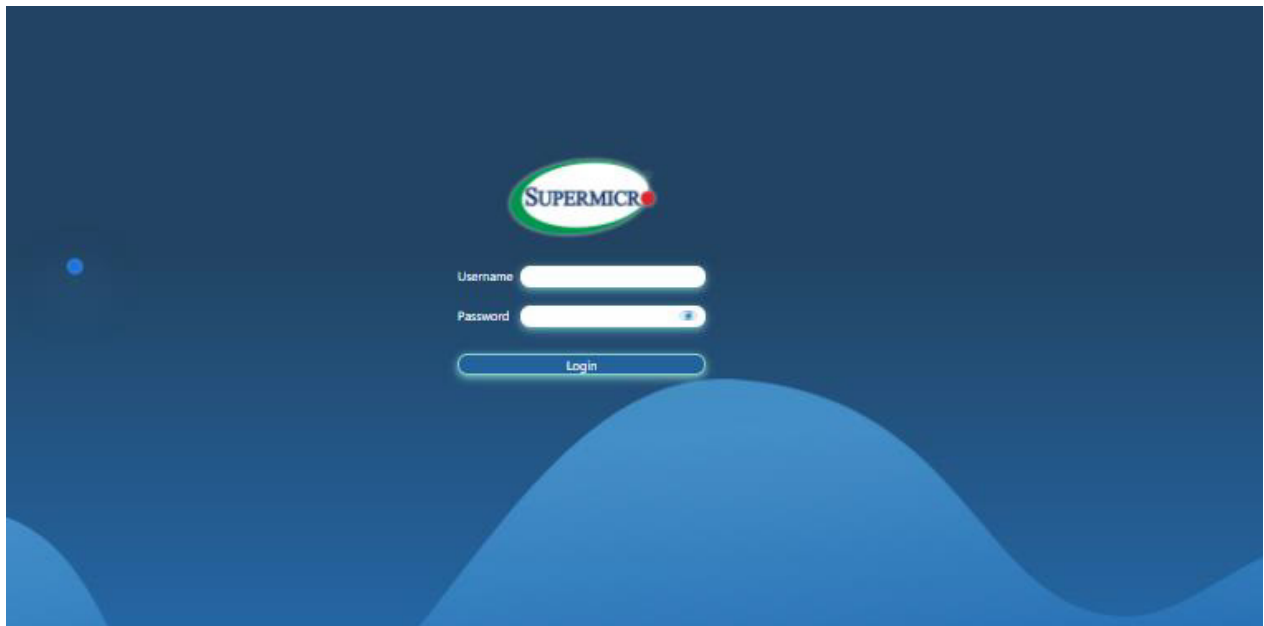
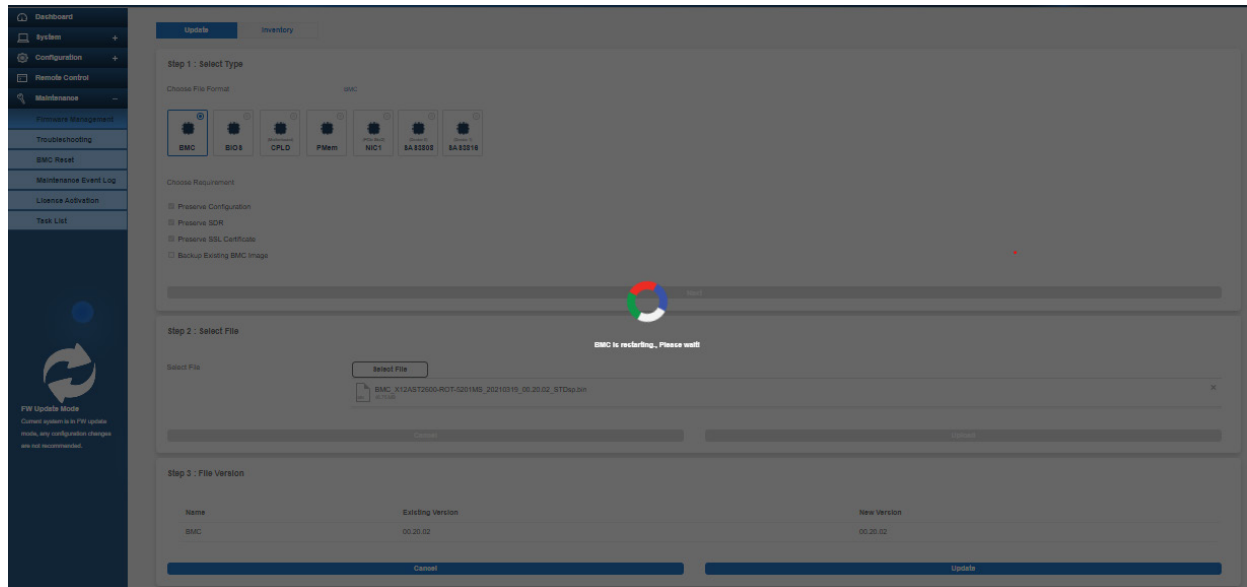
CancelUpload

Step 3 : File Version

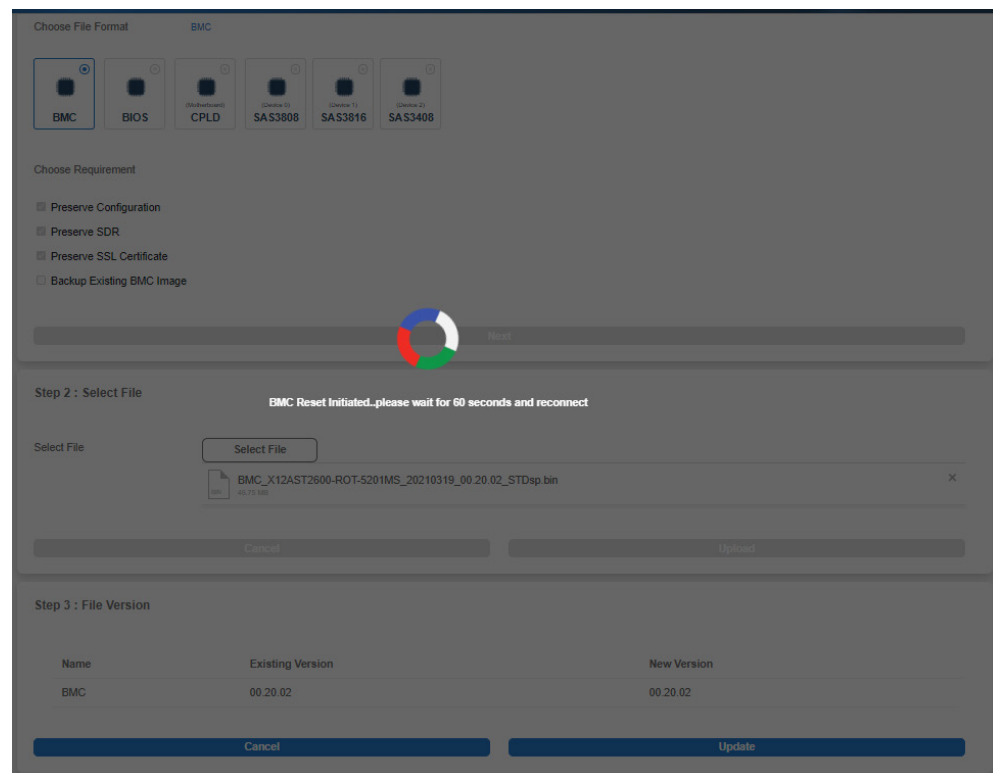
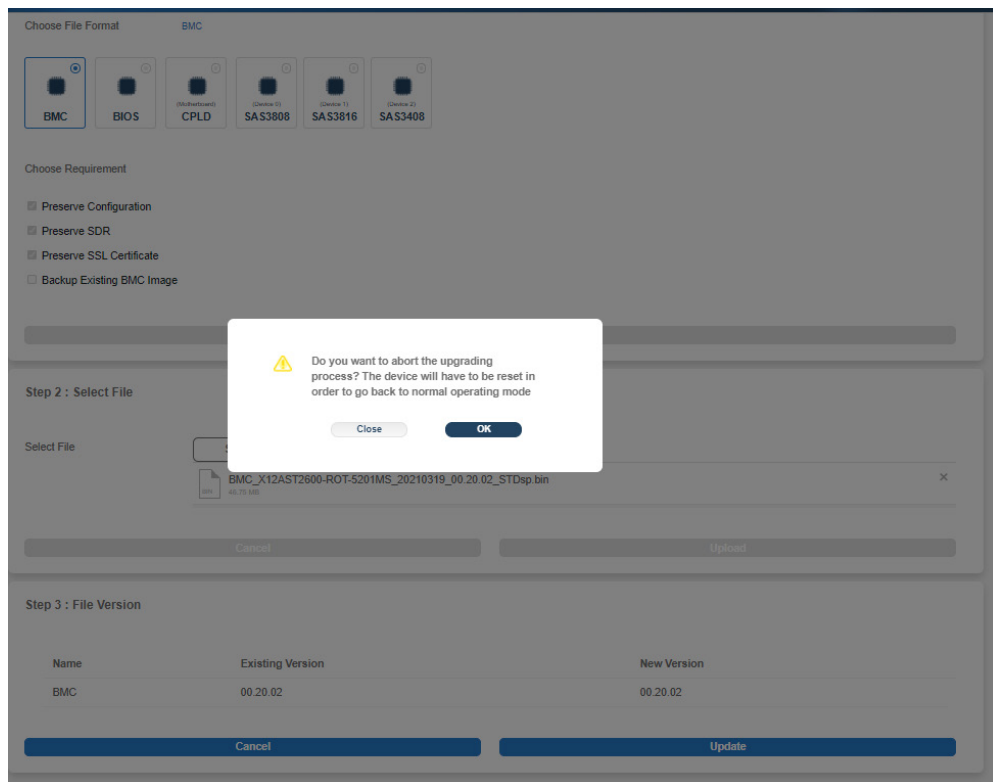
Name	Existing Version	New Version
BMC	00.20.02	00.20.02

CancelUpdate

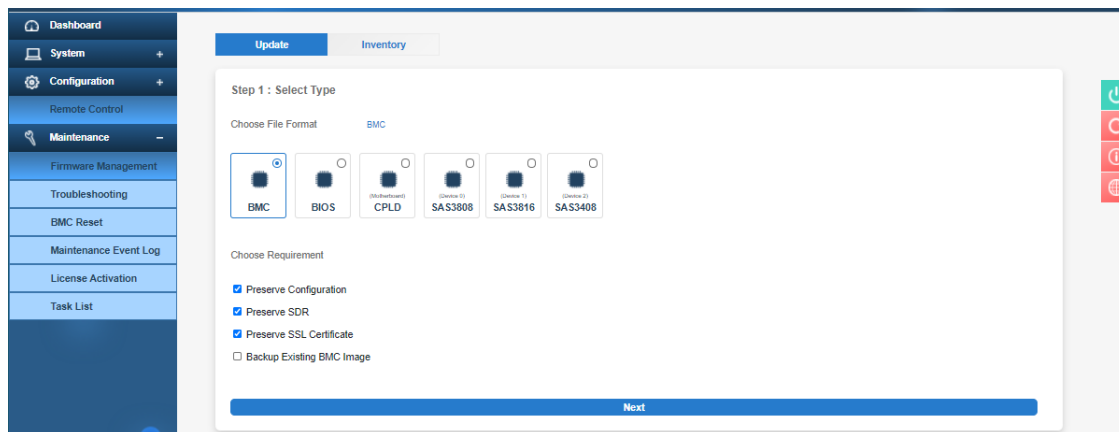




Note: If users cancel the BMC updating process, there will be an alert message pops up to ask users “Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode.” BMC is then reset with the message “BMC is restarting. To prevent data loss,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



How BIOS Firmware is Updated



UpdateInventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD (Motherboard)

SAS3808 (Device 0)

SAS3816 (Device 1)

SAS3408 (Device 2)

Choose Requirement

☐ Preserve NVRAM
 ☒ Preserve SMBIOS
 ☐ Backup Existing BIOS Image

Next

Step 2 : Select File

Select File

Select File

Cancel

Upload

BIOS_X12DPi-N(T)6-1B47_20201228_1.0a_STDsd.bin1/20/2021 6:35 PMBIN File32,768 KB

BIOS_X12DPi-N(T)6-1B47_20201228_1.0a_STDsp.bin1/20/2021 6:35 PMBIN File32,768 KB

BIOS_X12DPi-N(T)6-1B47_20210312_1.0c_STDsp.bin3/15/2021 7:22 PMBIN File32,768 KB

File name: BIOS_X12DPi-N(T)6-1B47_20210312_1.0c_STDsp.bin

All Files

Open

Cancel

BMCBIOSCPLDPMemSAS3808SAS3816

Choose Requirement

☐ Preserve NVRAM
 ☒ Preserve SMBIOS
 ☐ Backup Existing BIOS Image

Next

Step 2 : Select File

Select File

Select File

Cancel

Upload

148

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

(Multiboot) CPLD

PMem

(Device 1) SAS3808

(Device 1) SAS3816

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

×

Cancel

Upload

Update

Inventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

(Multiboot) CPLD

PMem

(Device 1) SAS3808

(Device 1) SAS3816

Choose Requirement

☐ Preserve NVRAM

☒ Preserve SMBIOS

☐ Backup Existing BIOS Image

Please power off the system before executing BIOS update.

Close

Power Off

Step 2 : Select File

Select File

Select File

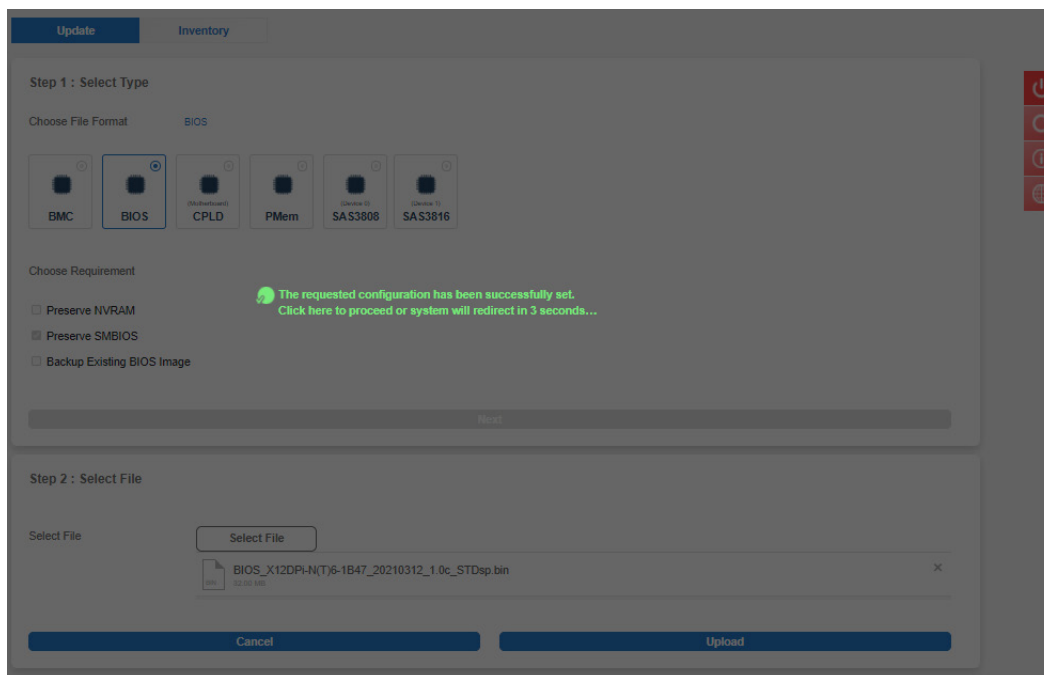
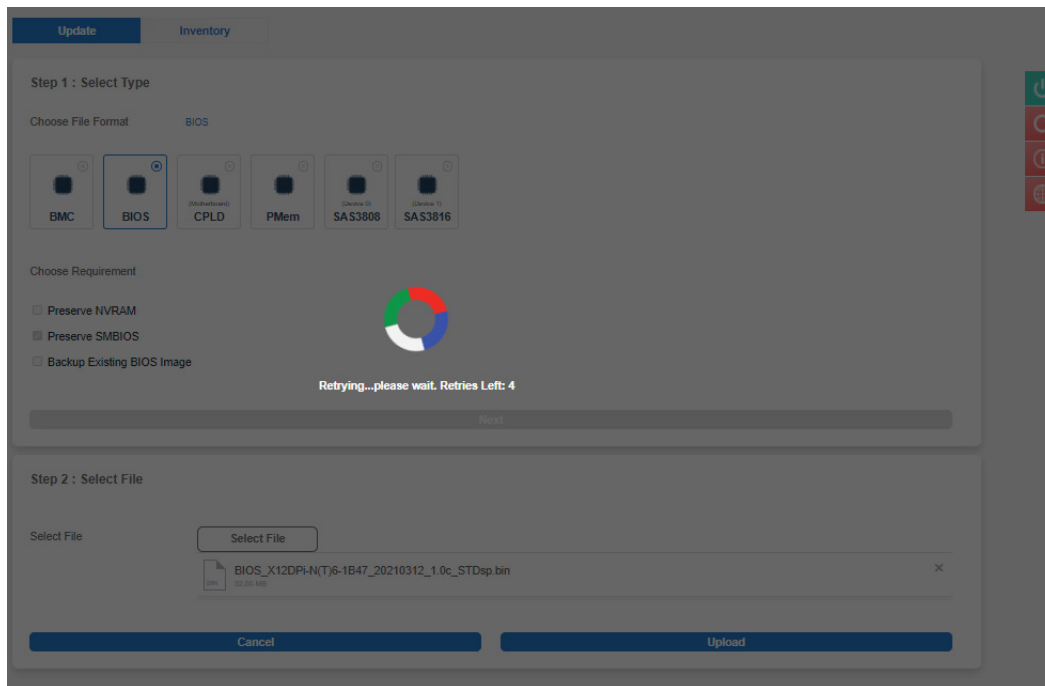
BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin

32.00 MB

×

Cancel

Upload



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

The screenshot shows the BMC Update interface with the 'Update' tab selected. Under 'Step 1: Select Type', the 'BIOS' option is chosen. Below, under 'Choose Requirement', there are three checkboxes: 'Preserve NVRAM', 'Preserve SMBIOS', and 'Backup Existing BIOS Image'. A red error message is displayed: 'Please select an image file. Click here to return.' The 'Next' button is disabled. Below this is 'Step 2: Select File' with a 'Select File' button. At the bottom are 'Cancel' and 'Upload' buttons.

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

The screenshot shows the BMC Update interface during the BIOS update process. A progress bar indicates 'Upgrade Progress : 0%'. The file 'BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin' is selected. The interface shows Step 3: File Version with a table comparing existing and new BIOS versions.

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

At the bottom are 'Cancel' and 'Update' buttons.

UpdateInventory

Step 1 : Select Type

Choose File Format

BIOS

BMC

BIOS

CPLD (Watchdog)

PMem

Device ID: SAS3808

Device ID: SAS3816

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 (Watchdog)

PMem

Device ID: SAS3808

Device ID: SAS3816

Choose Requirement

☐ Preserve NVRAM
 ☒ Preserve SMBIOS
 ☐ Backup Existing BIOS Image

Upload Firmware : 40%

Step 2 : Select File

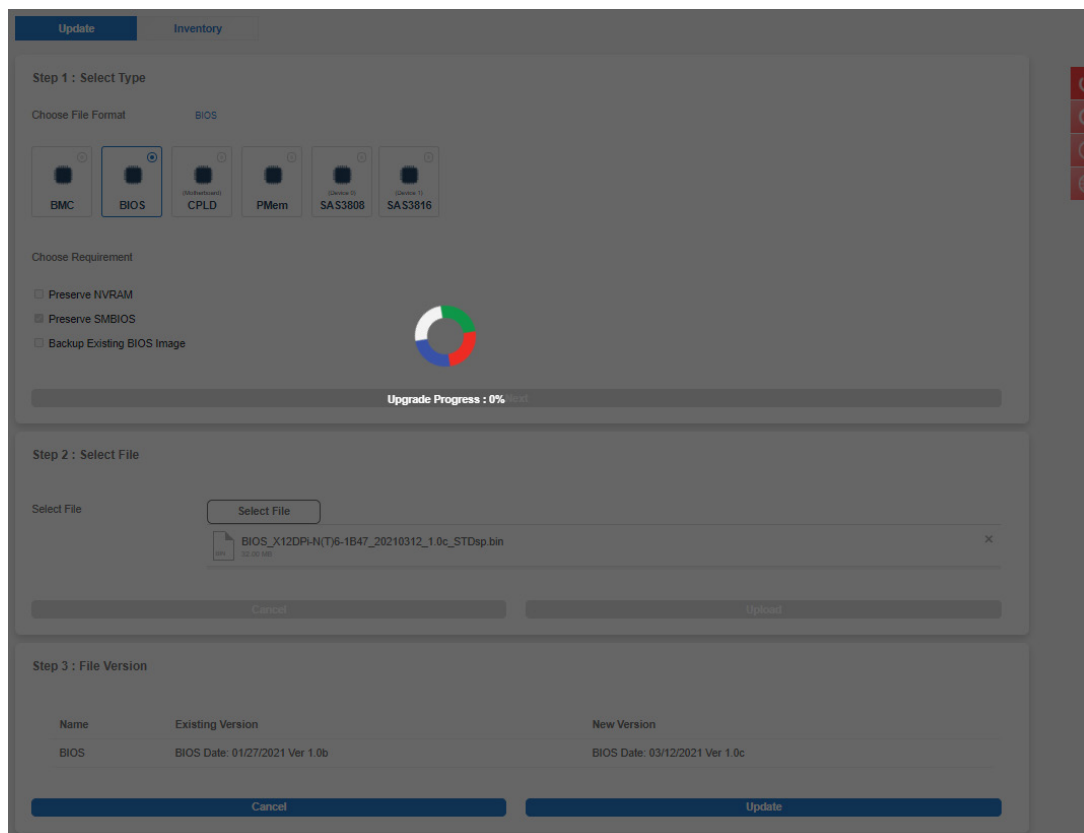
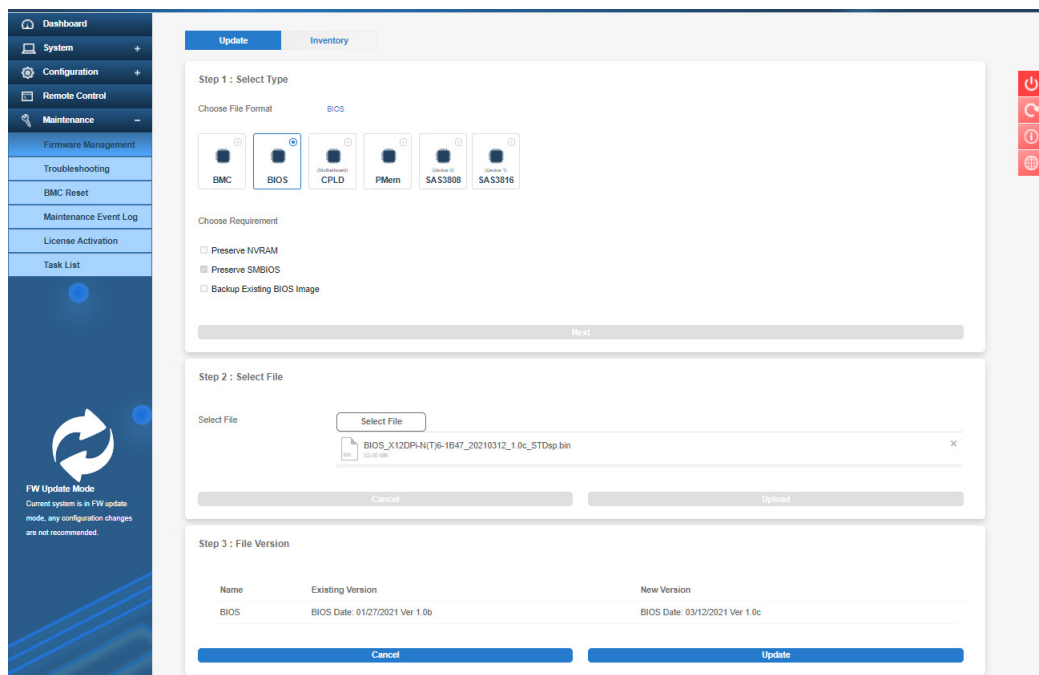
Select File

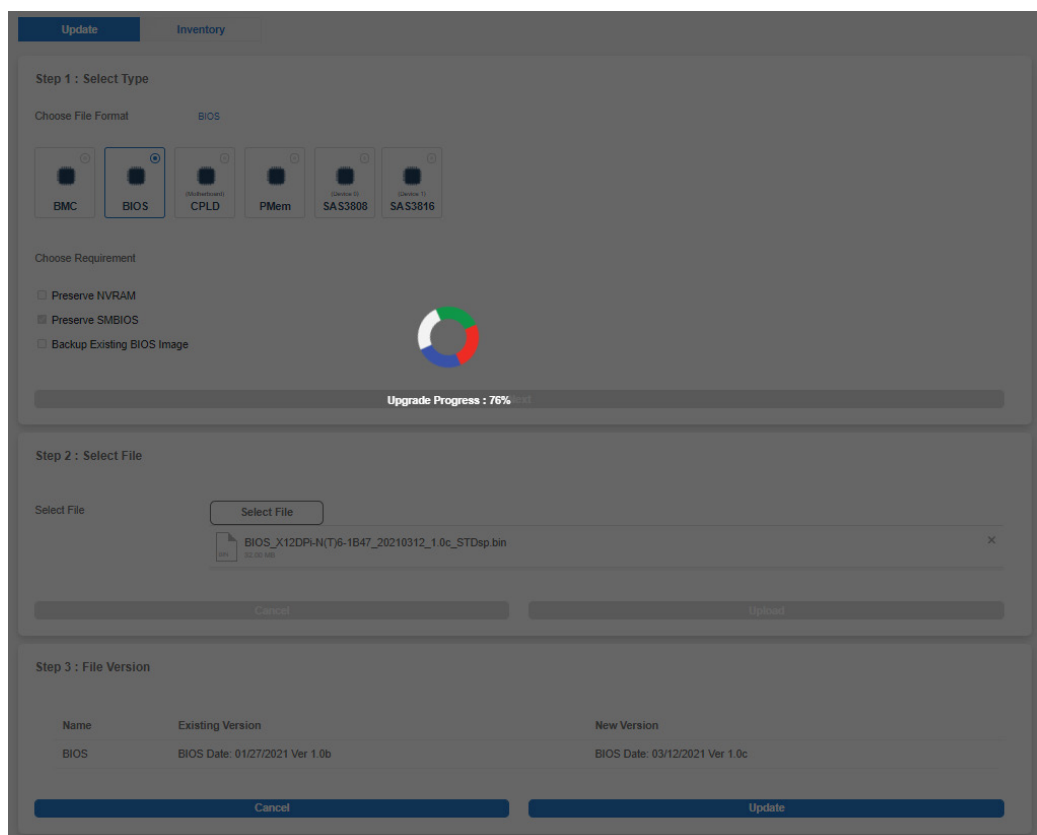
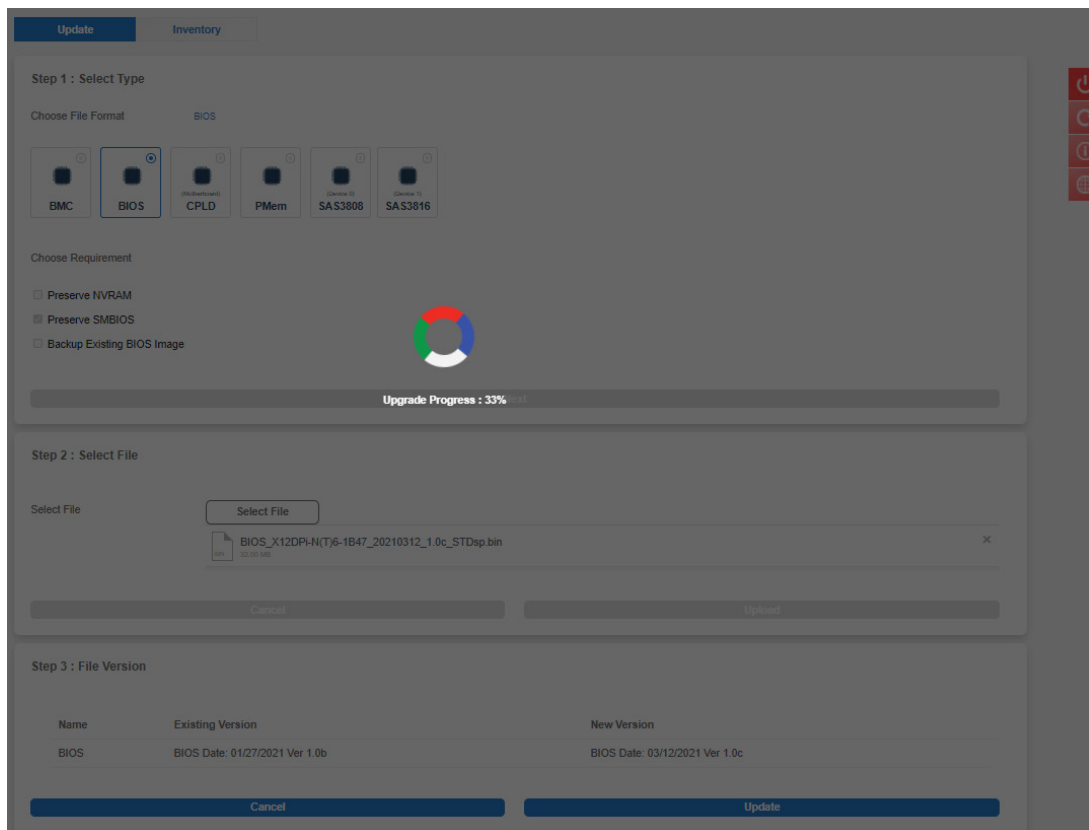
BIOS_X12DPI-N(T)6-1B47_20210312_1.0c_STDsp.bin

22.3M 100

Cancel

Upload





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

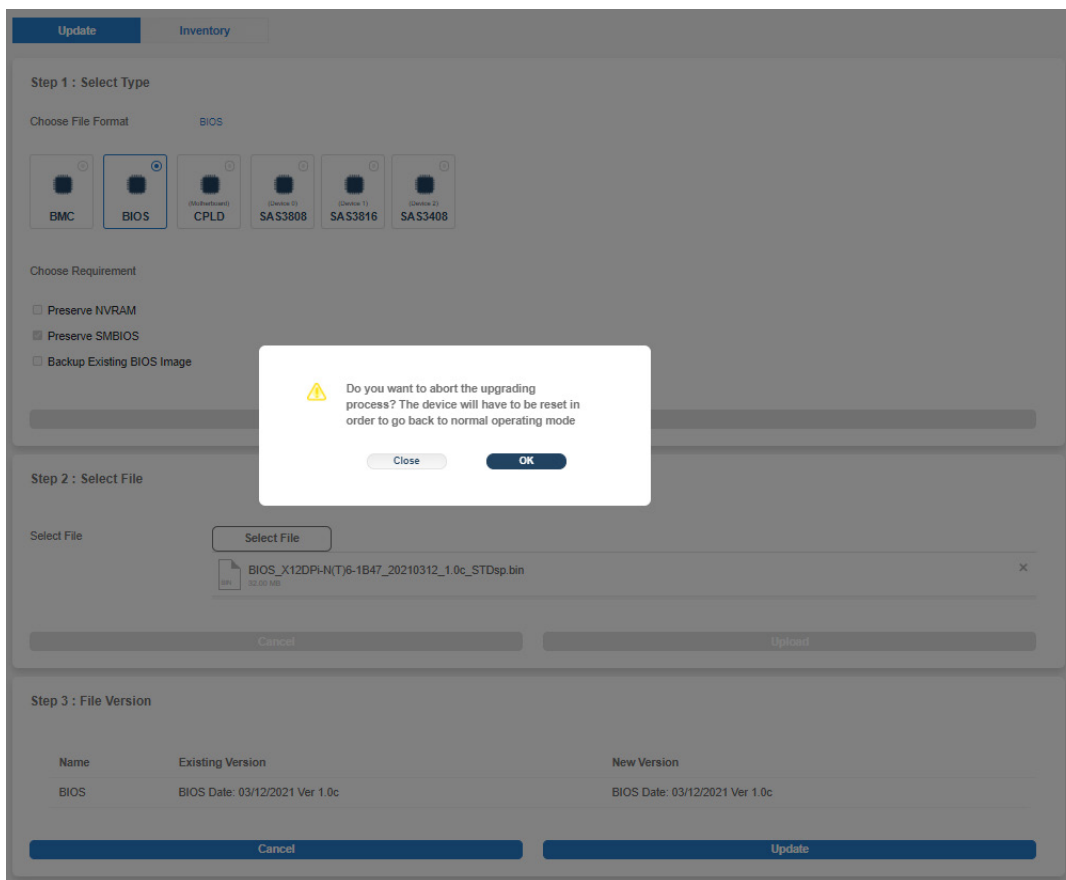
Step 3 : File Version

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 users cancel the BIOS updating process, there will be an alert message that pops up to ask users “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. See images below for details.



The screenshot displays the BIOS update interface with a confirmation dialog box in the center. The dialog box contains a yellow warning icon and the text: "Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode". Below the text are "Close" and "OK" buttons.

Update | Inventory

Step 1 : Select Type

Choose File Format: BIOS

Choose Requirement:

- ☐ Preserve NVRAM
- ☒ Preserve SMBIOS
- ☐ Backup Existing BIOS Image

Step 2 : Select File

Select File

BIOS_X12DP1-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

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

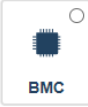
Update

BIOS Update Page for Tatlow Platforms

Update Inventory

Step 1 : Select Type

Choose File Format BIOS


BMC


BIOS

Choose Requirement

☒ Preserve SMBIOS

☒ Preserve OA

☒ Preserve BIOS Setup Configuration

☒ Preserve BIOS Setup password

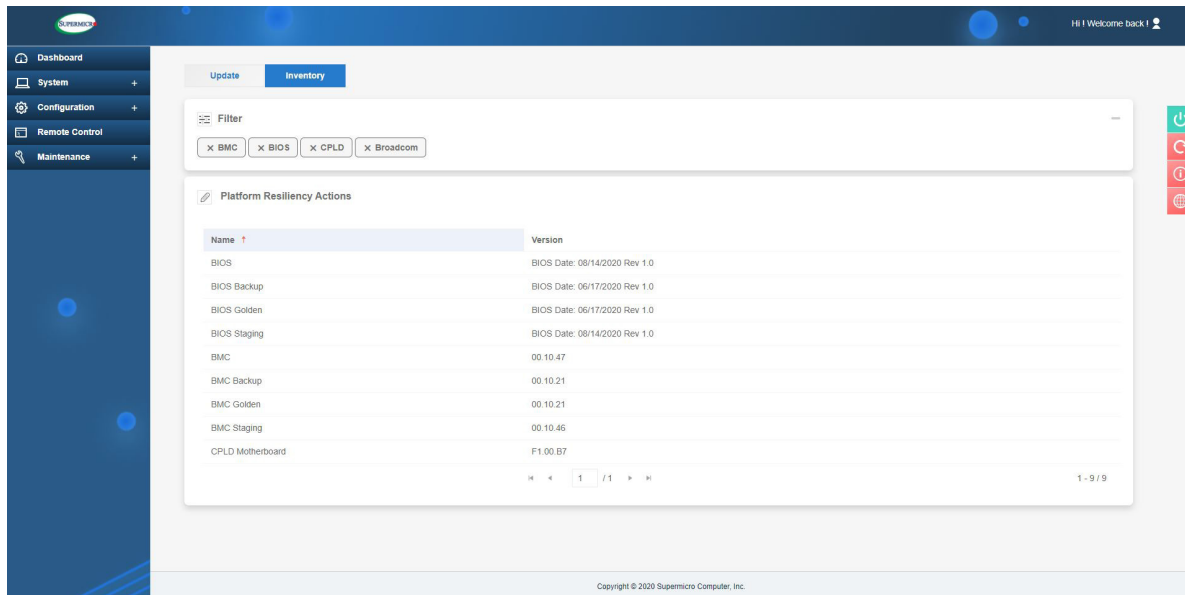
☒ Preserve BIOS Secure Boot Keys

☒ Preserve BIOS Boot Options Configuration

Next

Inventory

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



Users 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:** Users can view active BMC firmware.
- **BMC Backup:** Users can backup the active image during BMC FW update. This image will be used by CPLD to recover the BMC firmware if the active image is compromised or if the users wanted to manually recover BMC from the backup image.
- **BMC Golden:** Otherwise referring to the BMC factory firmware image. This golden image will be used as a second option for recovery by CPLD. During automatic or manual recovery operation, if the backup image fails the integrity check, the golden image will be used for recovery by CPLD.
- **BMC Staging:** Active images are placed in this staging region for evidence during firmware updates, when new firmware images are placed in this staging region, and during firmware recovery (Manual or Automatic). The active images may then be recovered from Backup or Golden image.

- BIOS: Users can view active BIOS firmware.
- BIOS Backup: Users can backup the active image during BMC BIOS update. This image will be used by CPLD to recover the BMC BIOS if the active image is compromised or if the users wanted to manually recover BMC from the backup image.
- BIOS Golden: Otherwise referring to the BIOS factory firmware image. This golden image will be used as a second option for recovery by CPLD. During automatic or manual recovery operation, if the backup image fails the integrity check, the golden image will be used for recovery by CPLD.
- BIOS Staging: Active images are placed in this staging region for evidence during BIOS updates, when new BIOS images are placed in this staging region, and during BIOS recovery (Manual or Automatic). The active images may then be recovered from Backup or Golden image.
- BMC ME: Users can view the active BIOS ME version.
- Broadcom: Users can view the Broadcom controller firmware version.
- Marvell: Users can view the Marvell controller firmware version.
- CPLD Backplane: Otherwise referring to the backplane CPLD version. If multiple CPLD backplane, then append [num] at the end.
- CPLD Motherboard: Users can view the motherboard CPLD version.
- Multi-node EC: Users can view the micro controller firmware version.
- Power Supply: Otherwise referring to the power supply firmware version. if multiple PSU, then append [num] at the end.



Note: Staging Firmware – RoT stores firmware in a temporary staging area for back-up, recovery, or evidence. To be consistent, the word “Ver” is used after the FW date for BIOS.

Name	Version
====	=====
88NR2241 Device 0	
BIOS	1.0.0.9447
BIOS Backup	BIOS Date: 03/12/2021 Ver 1.0c
BIOS Golden	BIOS Date: 03/12/2021 Ver 1.0c
BIOS Staging	BIOS Date: 10/06/2020 Ver 1.0
BMC	BIOS Date: 03/12/2021 Ver 1.0c
BMC Backup	01.00.15
BMC Golden	Not Present
BMC Staging	00.10.85
CPLD Motherboard	01.00.15
PowerSupply1	F1.00.B7
PowerSupply2	1.4
SAS3808 Device 1	1.4
SAS3816 Device 0	16.00.08.00
SAS3916 Device 2	16.00.02.00
NIC1_ SXB1 Slot2	5.130.02-3170
NIC2_AOC-2UR68G4-i4XTS SXB3 Slot0	N:01400000O:010A1500T:00000000
	01C3

Samples of Inventory Page

UpdateInventory

Filter

X BMC

X BIOS

X CPLD

Platform Resiliency Actions

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

1

/ 1

1 - 9 / 9

UpdateInventory

Add Filter

X BMC

X BIOS

X CPLD

X EC

Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 01/12/2021 Rev 1.0a
BIOS Backup	BIOS Date: 01/12/2021 Rev 1.0a
BIOS Golden	BIOS Date: 01/12/2021 Rev 1.0a
BIOS ME	4.4.3.283
BIOS Staging	BIOS Date: 01/12/2021 Rev 1.0a
BMC	55.04.10 dbgs
BMC Backup	55.04.10 dbgs
BMC Golden	Not Present
BMC Staging	55.04.10 dbgs
CPLD Backplane0	N/A
CPLD Motherboard	10.0d.50

Page 1

of 1

1 - 11 of 11 items

Update

Inventory

Add Filter

+

Platform Resiliency Actions

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

⏪ ⏩ Page 1 of 1

1 - 12 of 12 items

Update

Inventory

Filter

X BMC

X BIOS

X CPLD

X SAS

Platform Resiliency Actions

Name ↑	Version
BIOS	BIOS Date: 12/17/2020 Ver 1.0a
BIOS Backup	BIOS Date: 06/18/2020 Ver 1.00
BIOS Golden	BIOS Date: 06/18/2020 Ver 1.00
BIOS Staging	BIOS Date: 12/17/2020 Ver 1.0a
BMC	00.10.83
BMC Backup	00.10.77
BMC Golden	00.10.24
BMC Staging	00.10.83
CPLD Motherboard	F1.00 BE
SAS3108 Device 0	4.880.00-8485

⏪ ⏩ 1 / 1

1 - 10 / 10

UpdateInventory

Filter

X BMCX BIOSX CPLDX SAS

Platform Resiliency Actions

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

1

/ 1

1 - 10 / 10

Platform Resiliency Actions

This page allows users 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, the administrator can manually recover BMC or BIOS from the backup image. Users can select the current BMC/BIOS image and click on [Recover].



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

- **Update:** Users can update the current active image as a golden template. If recommended by Supermicro or if the administrator prefers that the current image be used as a golden template, then use this option to update the golden image with the active image. Options include Golden BMC and Golden BIOS. Once finished, click on [Update].
- **Generate Evidence:** When BMC or BIOS is recovered manually or automatically from the last known good image or golden image, the active image will be stored in the evidence region where users 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. Users 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, users can not generate other evidence or update other firmware.

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

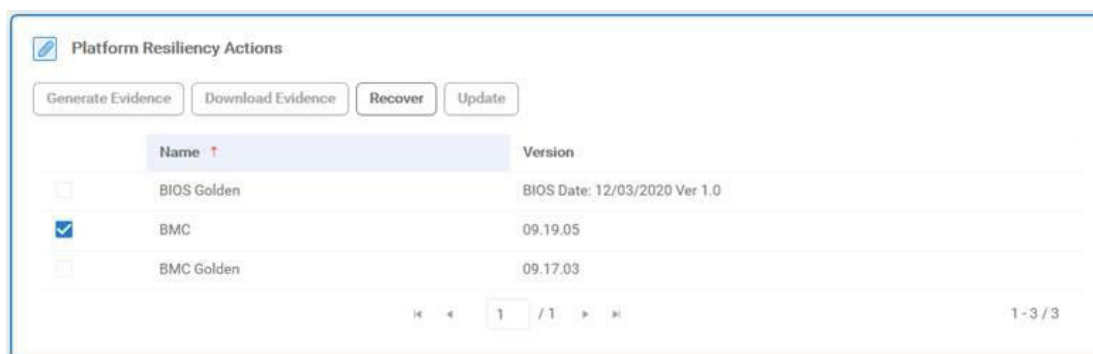
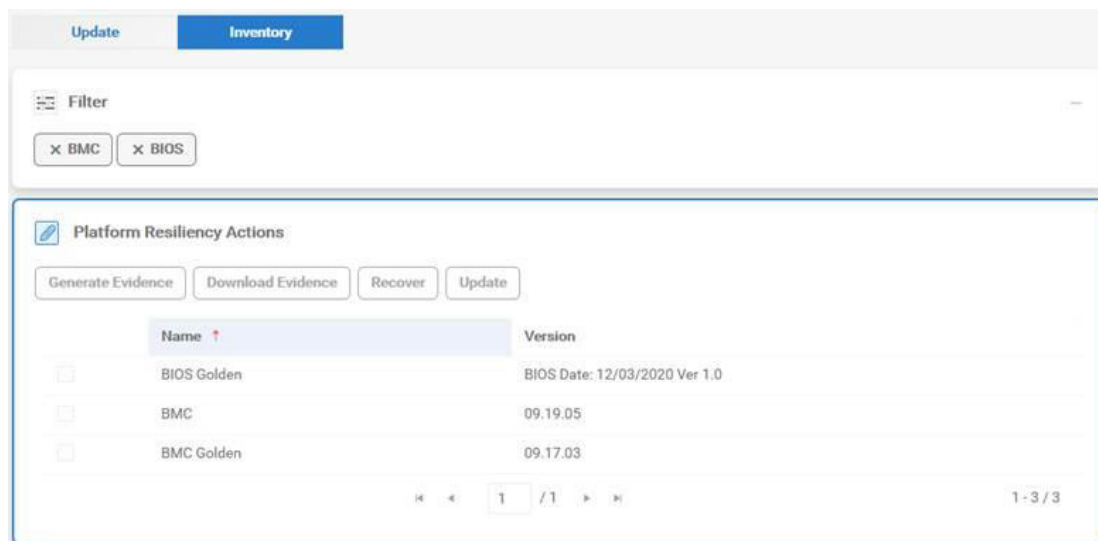
- **Download Evidence:** Once a compressed evidence file is generated, the Download Evidence button will be enabled. Click to download the evidence.



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

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

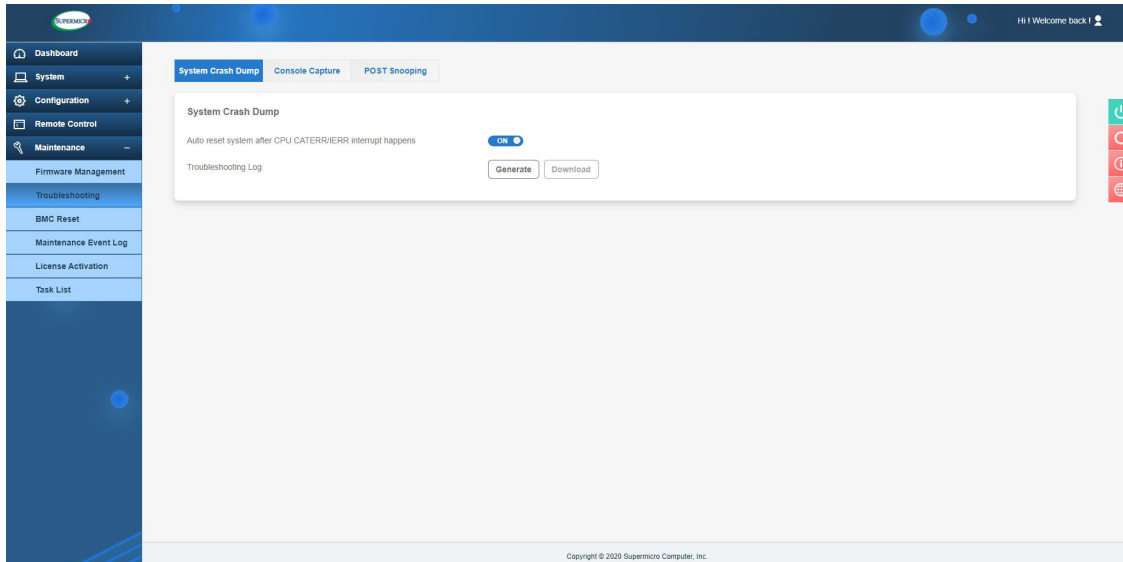
Below images are snapshots of Inventory page. When one of the action buttons is selected, unavailable or non-applicable action buttons (i.e. Generate Evidence, Download Evidence, Recover and Update buttons) are to be greyed out.



2.9.2. Troubleshooting

System Crash Dump

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



Users can adjust the following options.

- Auto reset system after CPU CATERR/IERR interrupt happens: Users can use the check box allows users to reset options 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: Users can generate a new crash dump.

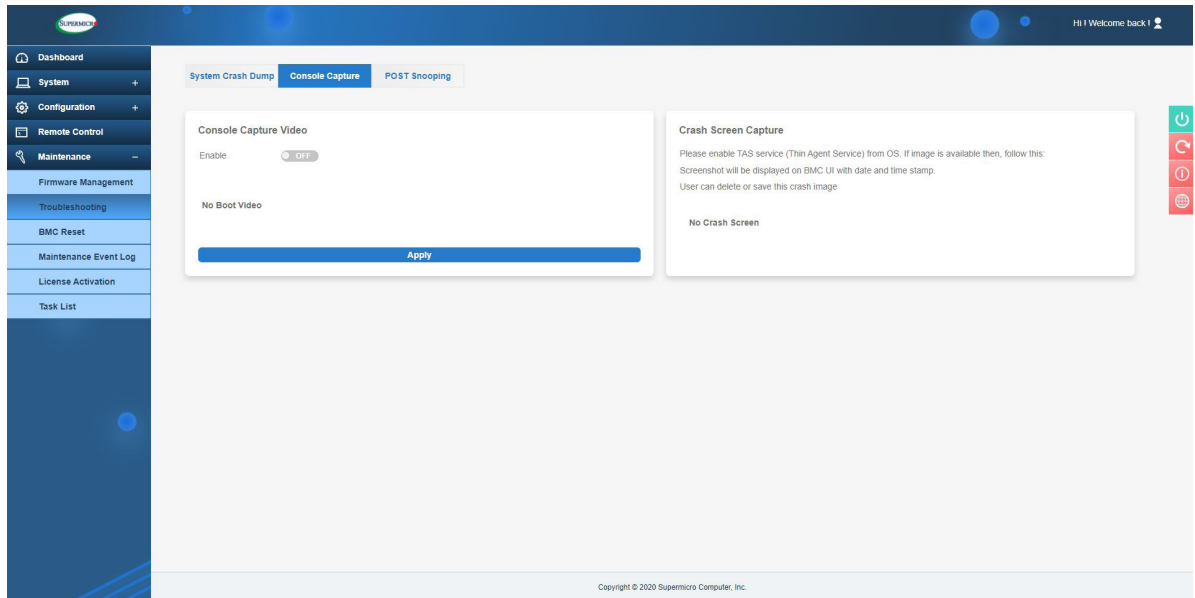


Note: Upon clicking [Generate], the system will remove previous error logs or dump available files and regenerate a new dump file.

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

Console Capture

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



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

- Disable/Enable: Users can enable or disable option. By default, it will be disabled.
- Record until buffer is full: Users can record video of the Console until the buffer is full. Video will be saved as AVI format and the maximum buffer size is 32 MB (approximate time calculated based on video size).
- Record until POST ends: Users can record video until POST ends or record until timeout value. BMC will receive POST completion information from BIOS and record video until that time. If any delay is introduced, then BMC will record video until a timeout period of approximately **eight minutes**.
- Apply: Users can record all videos with the title and time stamp. It will also allow users to delete a specific video.
- Download: Users can play and download video from here.
- AC Cycle/Factory Reset: Users can delete all videos.

The Crash Screen Capture feature allows users to capture the crash screen. Users have to enable Thin Agent Service (TAS) 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 users can delete or save the crash image.



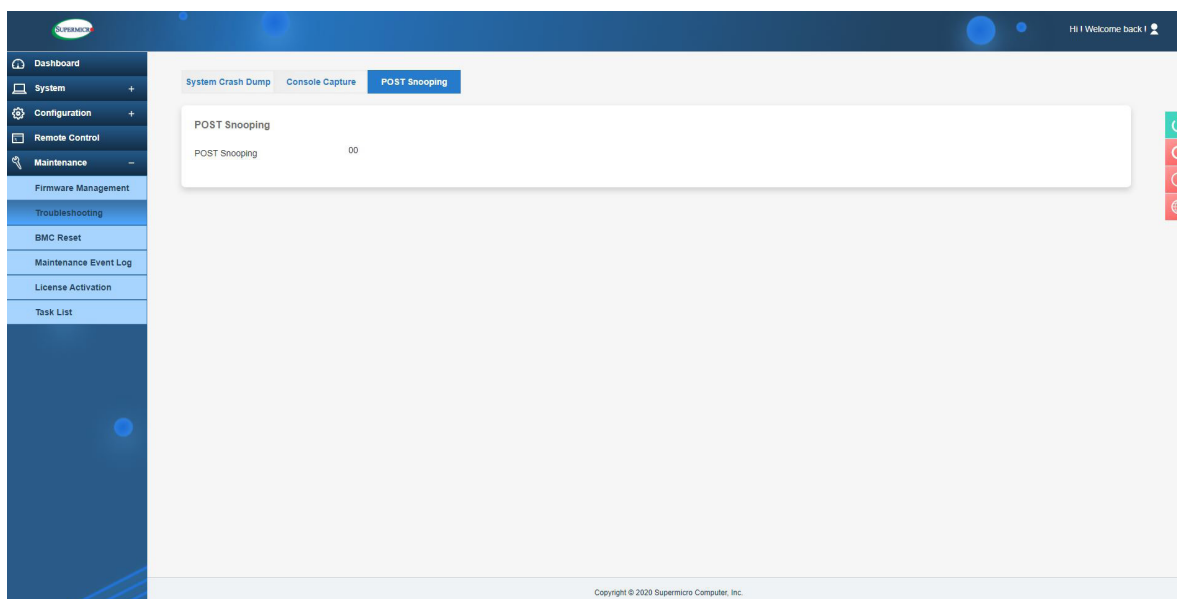
Note 1: Table below shows the supported and unsupported server platforms for System Crash Dump, Console Capture Video, and Crash Screen Capture features. We will enable the functions when they are supported. Due to time constraint, Console Capture Video and Crash Screen Capture on Intel Platforms with AST2500 are not supported at this time.

Note 2: All workstations platforms are not supported.

Supported and Unsupported Server Platforms (Non-Workstation)			
	System Crash Dump	Console Capture Video	Crash Screen Capture
Whitley Platforms (Intel ICE Lake)	Supported	Supported	Supported
Purley Platforms (Intel Sky Lake)	Supported	Not Yet Supported	Not Yet Supported
MicroCloud (Intel Rocket Lake)	<i>Unsupported</i>	<i>Unsupported</i>	<i>Unsupported</i>
Desktop Platforms (Intel Comet Lake, Parker Ridge, Snow Ridge, etc.)	<i>Unsupported</i>	<i>Unsupported</i>	<i>Unsupported</i>
AMD H12_AST2600 platforms (RoT and non-RoT)	Supported (download only)	Supported	Supported
AMD H12_AST2500 platforms (RoT and non-RoT)	Supported (download only)	<i>Unsupported</i>	<i>Unsupported</i>
AMD H11_AST2500	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.

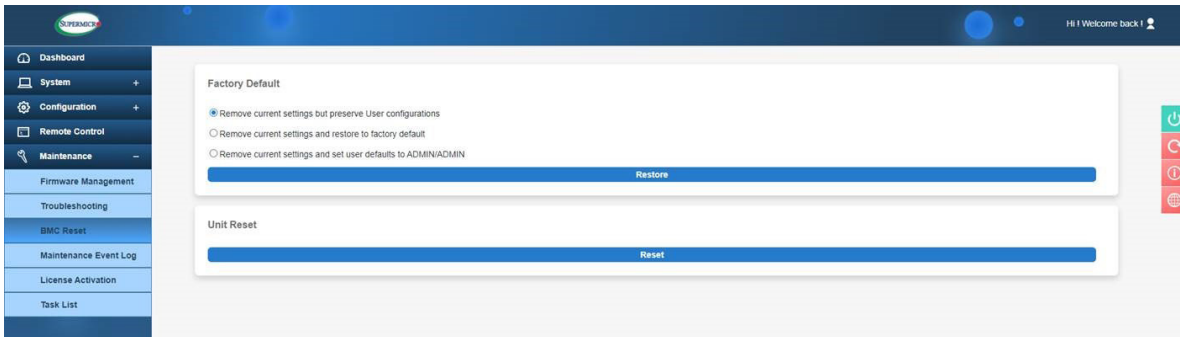


2.9.3. BMC Reset

Factory Default

This page displays the factory default options and the unit reset feature.

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



The Factory Default feature allows users to restore IPMI to the factory default settings. Options include the following.

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

Unit Reset

This feature allows users to reset an IPMI device.

 **Note:** There will be a prompt to users “BMC is restarting. To prevent data loss, please do NOT remove power source until BMC is back online!”

2.9.4. Maintenance Event Log

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



Note: By default, all event categories are selected so that users can view all events. Users 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	2020-10-03 16:02:58	DRTM	ADMIN/ADMIN	Localhost	ID 0x00 - TEE FW Start (0000.00.17)	service
Info	2020-10-03 16:02:59	DRTM	ADMIN/ADMIN	Localhost	ID 0x01 - SMC1_TEE_SERVICE (STS) Start	service
Info	2020-10-03 16:03:00	DRTM	ADMIN/ADMIN	Localhost	ID 0x02 - Security Functions Start (TA0)	service
Info	2020-10-03 16:03:01	DRTM	ADMIN/ADMIN	Localhost	ID 0x02 - Security Functions Start (TA0)	service
Info	2020-10-03 16:03:02	DRTM	ADMIN/ADMIN	Localhost	ID 0x02 - Security Functions Start (TA3)	service
Info	2020-10-03 16:03:43	DRTM	ADMIN/ADMIN	Localhost	ID 0x02 - Security Functions Start (TA1)	service
Info	2020-10-03 16:03:44	DRTM	ADMIN/ADMIN	Localhost	ID 0x02 - Security Functions Start (TA2)	service
Info	2020-10-03 16:05:02	Redfish	ADMIN/ADMIN	10.124.8.53	Redfish session was created successfully.	account
Info	2020-10-03 16:05:02	Web	ADMIN/ADMIN	10.124.8.53	Web login was successful.	account
Info	2020-10-03 16:05:48	Web	ADMIN/ADMIN	10.124.8.53	Hostname was configured to NULL successfully.	network
Warning	2020-10-03 16:05:48	Web	ADMIN/ADMIN	10.124.8.53	IPv6 DNS server 10.2.1.225 was deleted unsuccessfully.	network
Info	2020-10-03 16:05:48	Web	ADMIN/ADMIN	10.124.8.53	IPv6 address 1000:0000:0000:0000:0000:0000:0000:0002:54 was added successfully.	network

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

- **Severity:** Users 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:** Users can view the time stamp of the event occurrence.
- **Interface:** Users can view the interface that triggered the event (e.g. RMCP, Redfish, Web).
- **User:** Users can view the name of the user that triggered the event (e.g. ADMIN, N/A, BIOS).
- **Source:** Users can view the source that triggered the event.
- **Description:** Users can view the basic description of the event.

- Category: Users can view the event category based on type of the event (e.g. Storage, Account, Network, Service, or others).
- Keyword Search: Users can search keyword related events.

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

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

2.9.5. License Activation

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



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

Users can adjust the following settings to configure this feature.

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

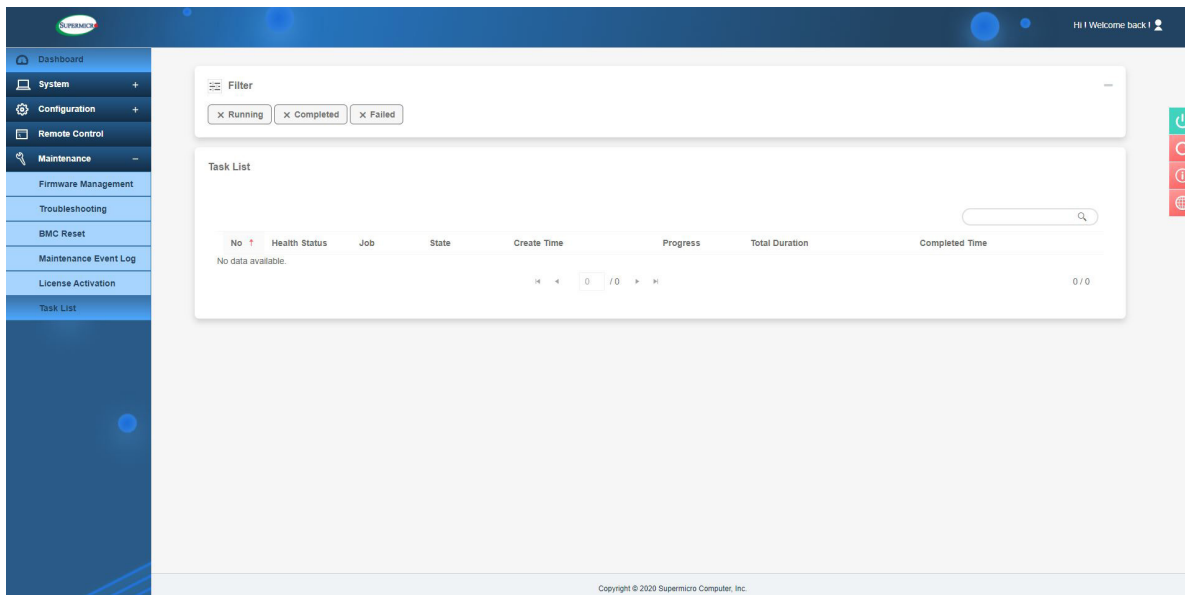
Virtual Media (BM) License						
	SMBV2	SMBV3	CIFS	SAMBA	HTTP	HTTPS
Current X11 License			FREE	FREE	OOB	
Current X12 License	OOB		OOB	OOB	OOB	
Proposal X12 License	FREE	FREE	FREE	FREE	OOB	OOB

2.9.6. 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. Storage controller disks can erase task progress.



The following information is presented in the table for review.

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

Users can filter tasks to view based on task status (Running, Completed, or Failed). The following table shows corresponding Redfish State to Filter criteria.

<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, please open the following ports:

HTTP: 80 (TCP)

HTTPS: 443 (TCP)

BMC: 623 (UDP)

Remote console: 5900 (TCP)

Virtual media: 623 (TCP)

SMASH: 22 (TCP)

WS-MAN: 8889 (TCP)

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

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

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

Answer: It is not a normal condition. Make sure that there is no other device accessing the 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, please 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. Please 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. "Grayed-out" options cannot be configured. The right frame displays the key legend. Above the key legend is an area reserved for a text message. When an option is selected in the left frame, it is highlighted in white. Often a text message will accompany it. 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 the users first enter the AMI BIOS setup utility, they will enter the Main setup screen. They can always return to the Main setup screen by selecting the Main tab on the top of the screen. The Main BIOS setup screen is shown below and 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

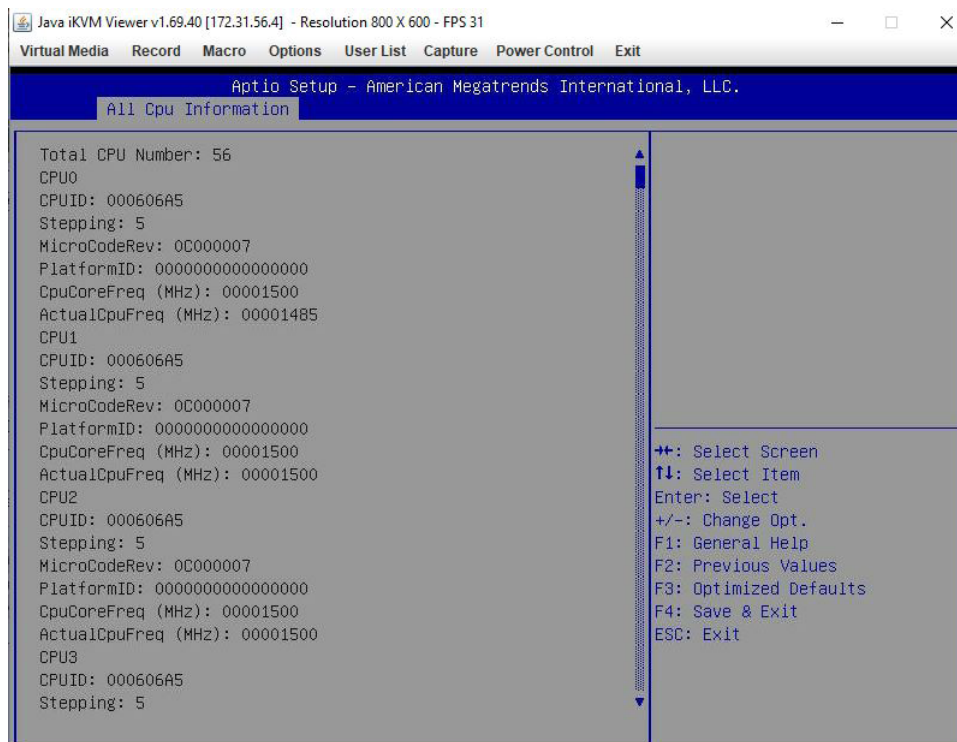
This item displays the Complex Programmable Logic Device version.

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 the users 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 the users 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. Please 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 the users 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 the users 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 the users 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 the users 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 the users 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 the users 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 the users 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 Pci-e 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 the users 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 option "Enable" 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 the users 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**.

► IIO 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 (IIO PCIe Br1)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, and **Auto**.

IOU1 (IIO PCIe Br2)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, and **Auto**.

IOU2 (IIO PCIe Br3)

This feature configures the PCI-E port Bifurcation setting for a PCI-E port specified by the user. The options are x4x4x4x4, x4x4x8, x8x4x4, x8x8, x16, and **Auto**.

► CPU SLOT2 PCI-E 3.0 X8 / CPU SLOT6 PCI-E X16 / CPU SLOT4 PCI-E X16 / CPU SLOT3 PCI-E X8

Link Speed

Use this feature to select the link speed for the PCI-E port specified by the user. 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:

- PCI-E Port Link Status
- PCI-E Port Link Max
- PCI-E Port Link Speed

PCI-E 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 PCI-E 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 PCI-e 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 the users have enabled VMD on a PCI-E slot of their choice, this PCI-E slot will be dedicated for NVMe storage devices use only, and it will no longer support PCI-E devices of other functionalities. To re-activate this slot for PCI-E use, please 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 PCI-E 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 PCI-E 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 PCI-E 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 PCI-E 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**.

PCI-E Completion Timeout Disable

Use this feature to enable PCI-E 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 PCI-E 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 SATA drive specified by the users as an AHCI drive. Select RAID to configure a SATA drive specified by the users as a RAID drive. The options are **AHCI** and RAID.

SATA HDD Unlock

This feature allows the users 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 the users 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 SATA port specified by the users 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 an sSATA drive specified by the users as an AHCI drive. Select RAID to configure an sSATA drive specified by the users as a RAID drive. The options are **AHCI** and RAID.

SATA HDD Unlock

This feature allows the users 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 the users 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 SATA port specified by the users 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 PCI-Express 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 PCI-E 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 PCI-E 3.0 X8 OPROM

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

CPU SLOT3 PCI-E 3.0 X8 OPROM

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

CPU SLOT4 PCI-E 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 PCI-E 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 PCI-E 3.0 X4 OPROM

Use this feature to select which firmware type to be loaded for the add-on card in this slot. The options are Disabled, **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 the users 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 serial port specified by the user.

Change Settings

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

The options 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 the users 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 serial port specified by the user.

Change Settings

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

The options 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 serial port specified by the user. 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 client computer, which is the remote computer used by the user.

COM1 Terminal Type

This feature allows the users 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 the users 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 client computer, which is the remote computer used by the user.

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 the users 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 COM port selected by the users 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 the users to specify how the host computer will exchange data with the client computer, which is the remote computer used by the user.

Out-of-Band Mgmt Port

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



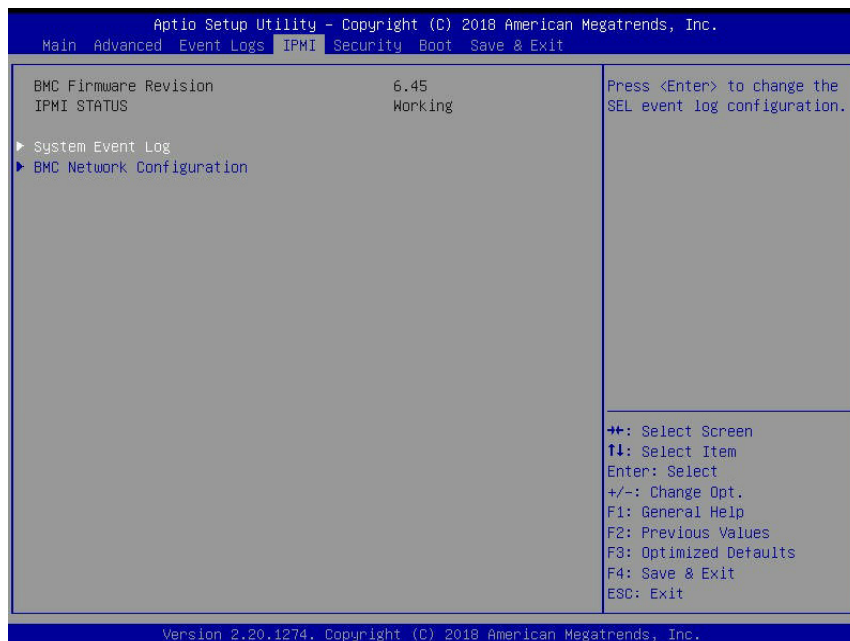
Note: After making changes on a setting, be sure to reboot the system for the changes to take effect.

►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 the users 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 the users to select the source of the IP address for this computer. If Static is selected, the users 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

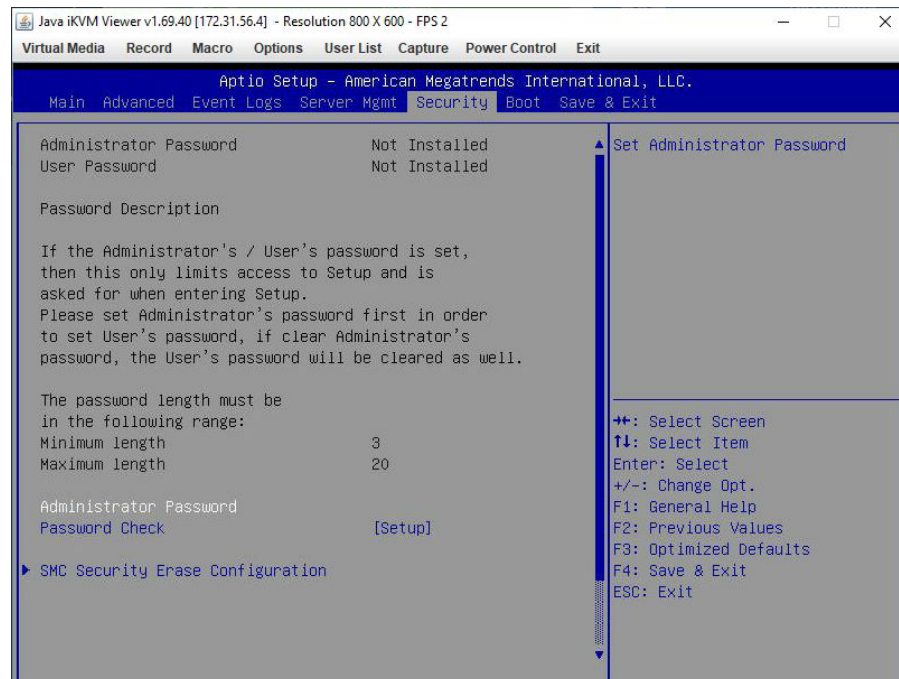
This feature allows the users to select the source of the IP address for this computer. If Static is selected, the users will need to know the IP address of this computer and enter it to the system manually in the field. If DHCP is selected, the BIOS will search for a DHCP (Dynamic Host Configuration 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 the users 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 the users 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 the users 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 the users 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 the users to configure the settings of the platform keys.

Details

Review details on current settings of the platform keys.

Export

This feature allows the users 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 the users 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 the users 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 the users 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 the users 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. The users 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 the users to export an OsRecovery Signature to an available file system.

Set New

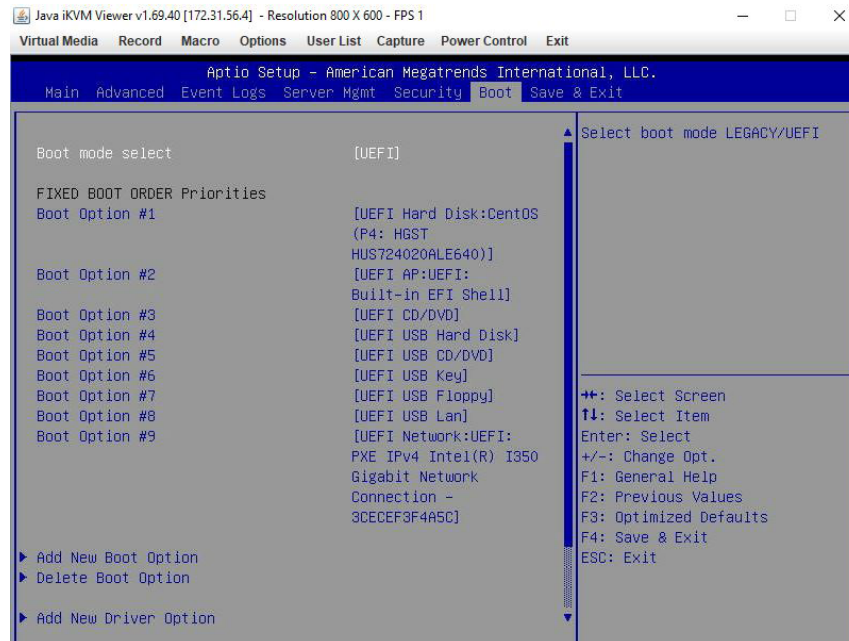
Select Yes to load the DBR from the manufacturer's defaults. Select No to load the DBR from a file. The options are Yes and No.

Append

This item uploads and adds an OsRecovery Signature into the Key Management. The users 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 the users 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 the users 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

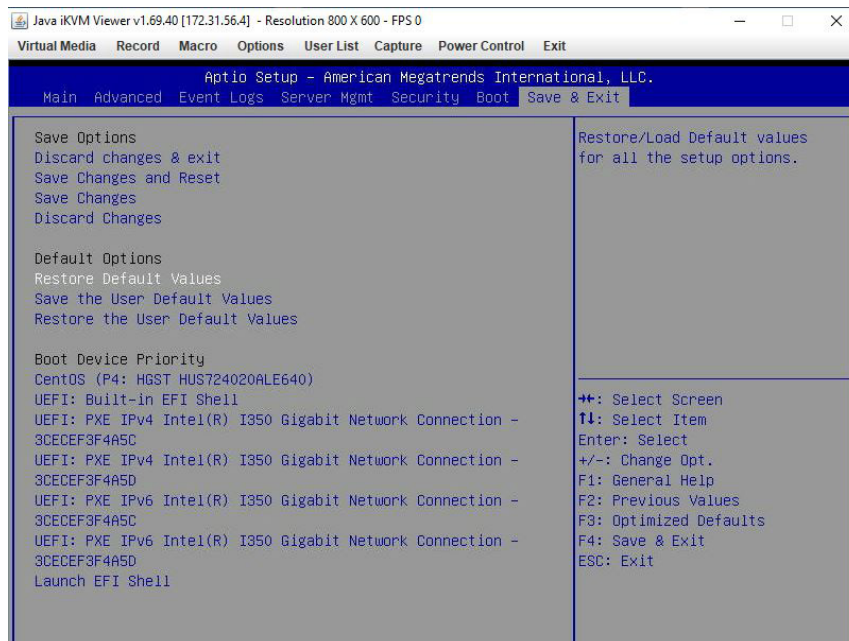
► Hard Disk Drive BBS Priorities

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 the users 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 the users 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 X12 and H12 series motherboards using BMC WEB GUI or SUM (Supermicro® Update Manager).



Note: For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI UEFI BIOS, RSD/SCC, TAS, and IPMIView, please refer to our website at <https://www.supermicro.com/products/nfo/IPMI.cfm> for details.

A.2 Updating Firmware Using BMC WEB GUI

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

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

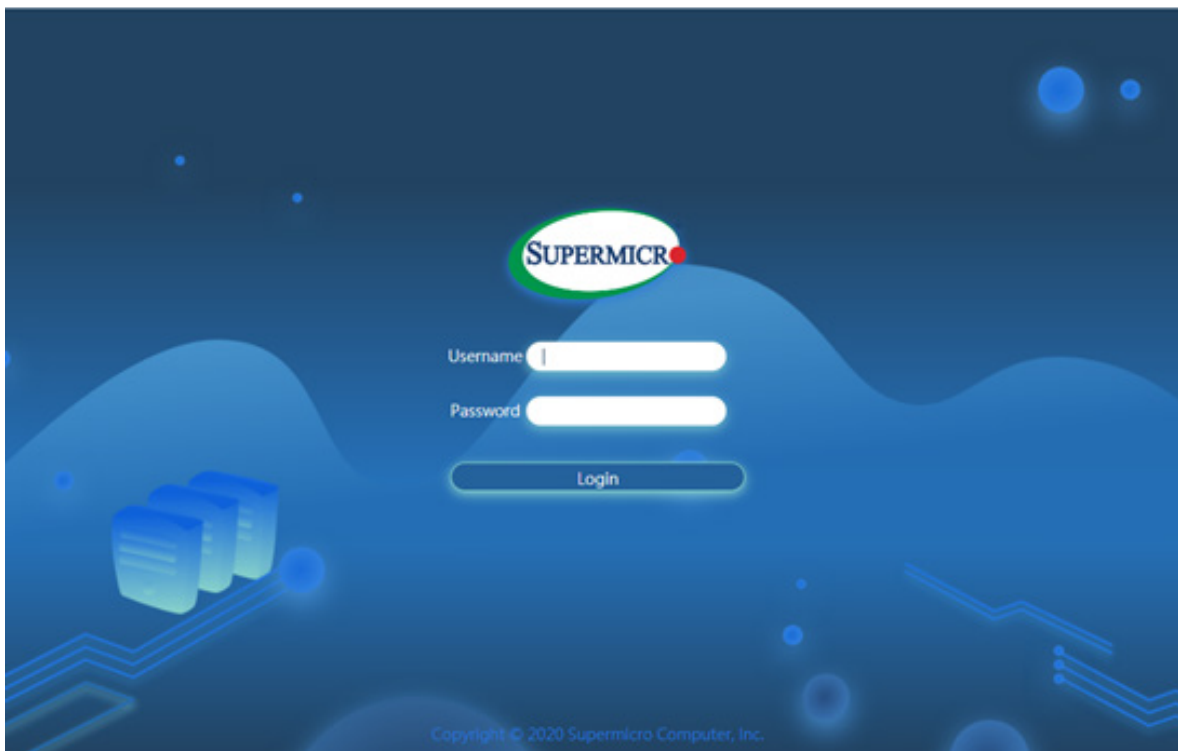


Figure 1: BMC Firmware Web User Login



Note: Please contact Supermicro sales or FAE if the users do not know their username or password.

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

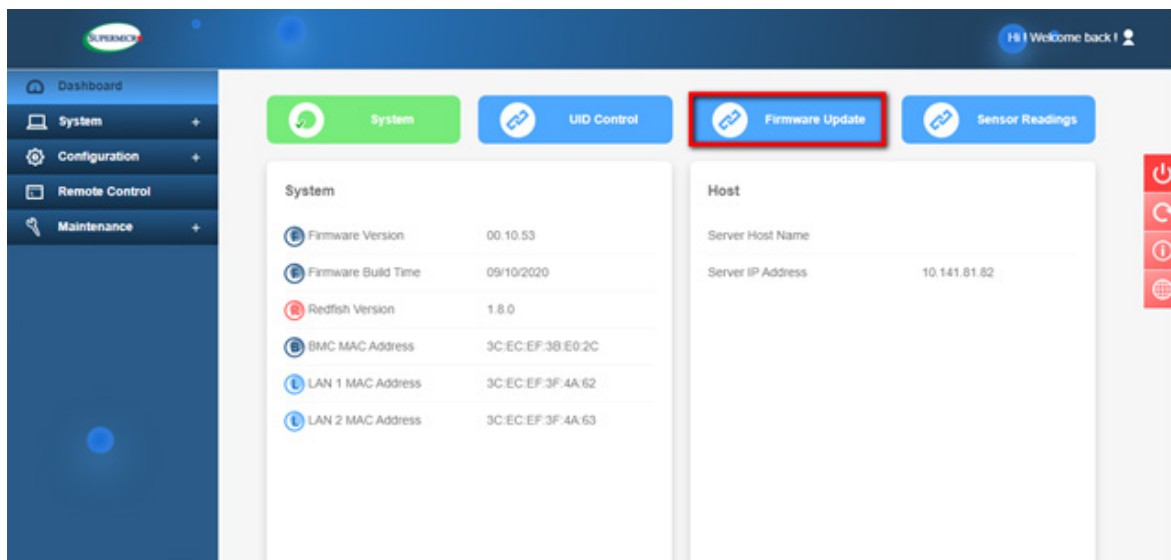


Figure 2: BMC Firmware Update Dashboard

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

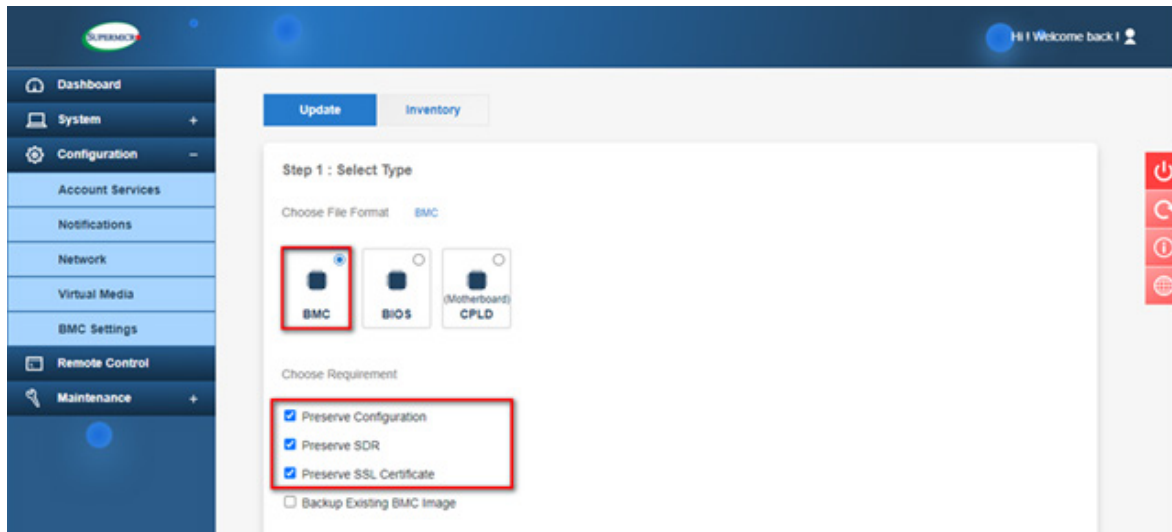


Figure 3: BMC Firmware Update Default Setting

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

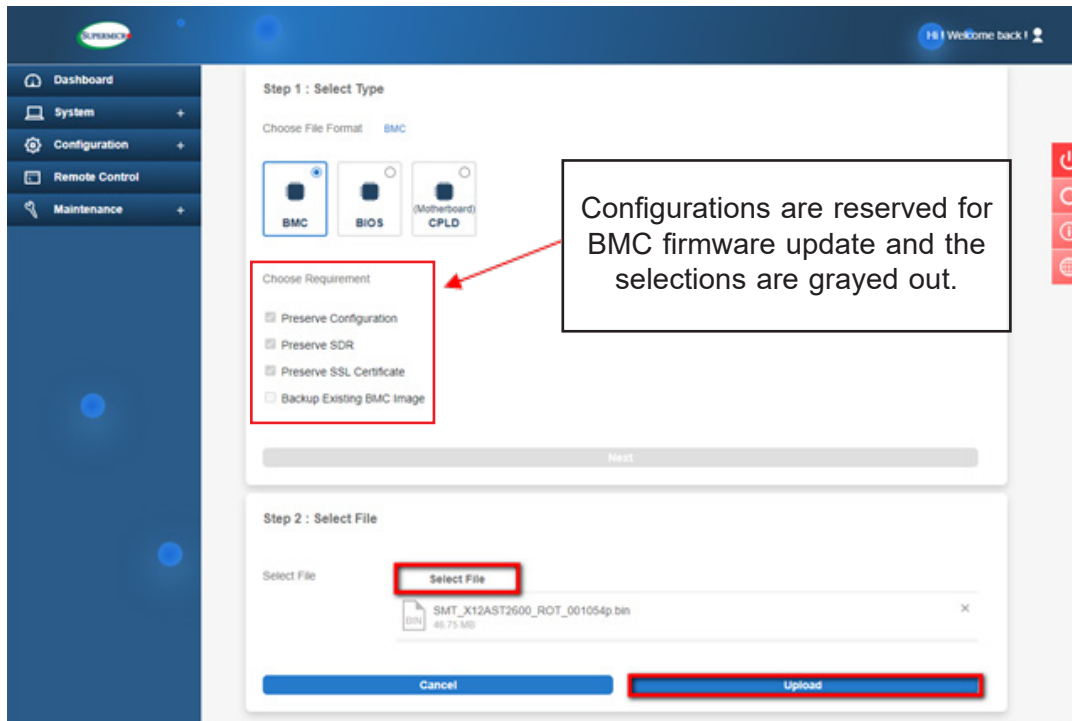


Figure 4: Select and Upload New BMC Firmware File

Note 1: By default, the firmware update process preserves the existing configuration, SDR, and SSL certificates for the new BMC firmware. The users 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. Users 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.

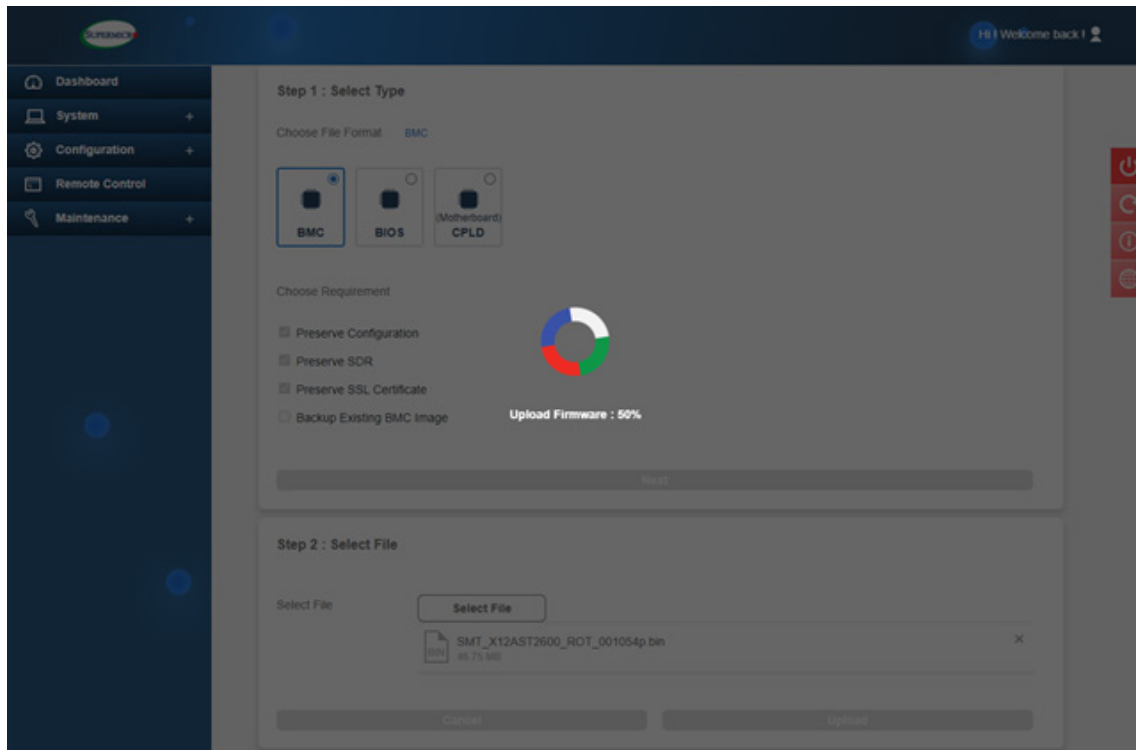


Figure 5: New BMC Firmware Uploading

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

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

Choose Requirement

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

Next

Step 2 : Select File

Select File

Select File

SMT_X12AST2600_ROT_001054p.bin
45.75 MB

Cancel Upload

Step 3 : File Version

Name	Existing Version	New Version
BMC	00.10.53	00.10.54

Cancel Update

Figure 6: Verify the New BMC Firmware Version

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

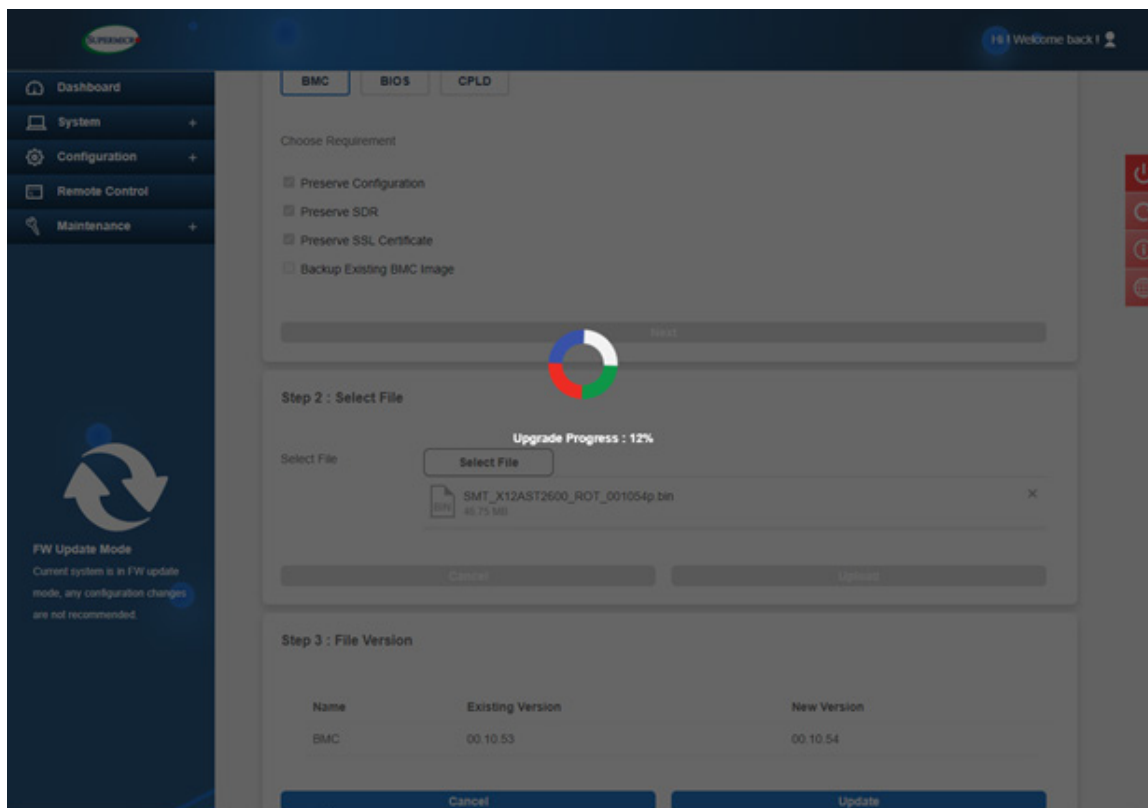


Figure 7: BMC Firmware Updating in Progress

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

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

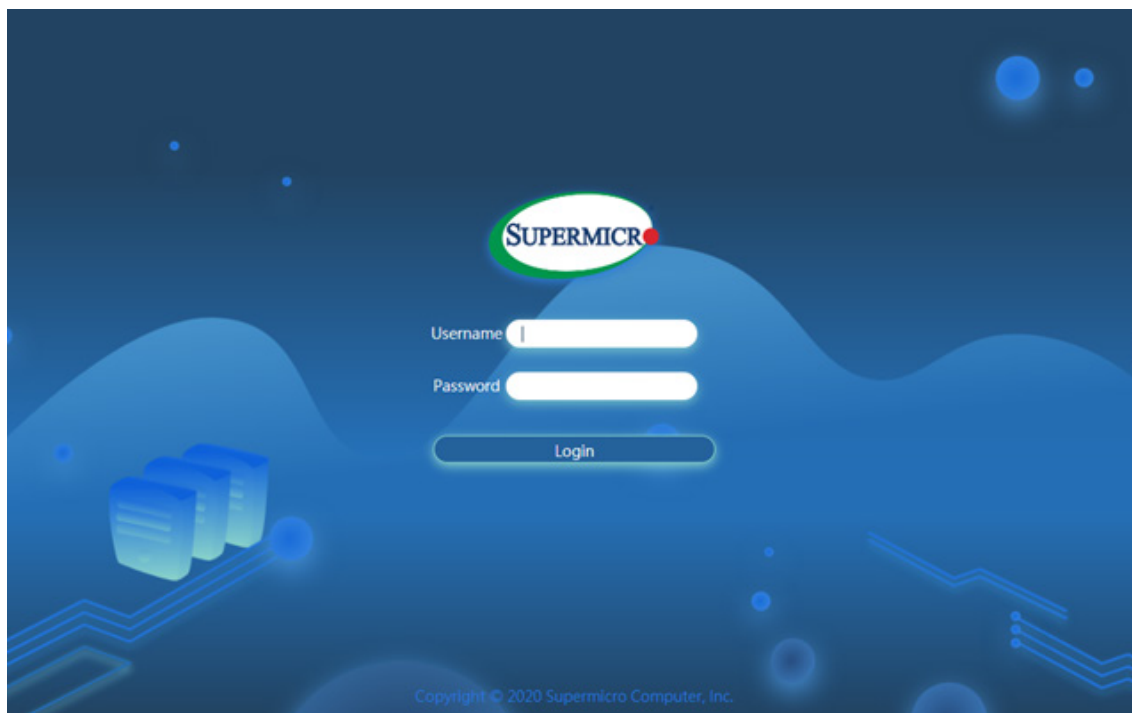


Figure 8: BMC Firmware Web User Login

A.3 Updating Firmware Using SUM

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

Step 1: Installing SUM

To install SUM in Linux/FreeBSD OS, 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. Please wait for BMC to complete the system reboot. (Figure 9)

**Notes:**

- BMC SOC will be updated after the firmware update process is completed.
- BMC configuration settings will be preserved by default for the new BMC firmware unless the `--overwrite_cfg` option is used.
- DO NOT flash BIOS and BMC firmware images at the same time.
- The `--overwrite_cfg` option overwrites the current BMC configuration using the factory default values in the given BMC image file.
- The `--overwrite_sdr` option overwrites the current BMC SDR data.
- SUM command is recommended for BMC firmware updates: `sum [[-i <IP or host name> | -I Redfish_HI] -u <username> -p <password>] -c UpdateBmc --file <filename>`

Remote Update

The users can use SUM to update BMC firmware via IPMI port.

```
[SUM_HOME]# ./sum -i 192.168.34.56 -u ADMIN -p XXXXXX -c UpdateBmc  
--file SMCI_BMC.rom
```

Local Update

The users can use SUM to update BMC firmware under Linux, Windows, or FreeBSD.

[illegible]

Figure 9: Output of BMC Remote Update in SUM

```
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 their 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.

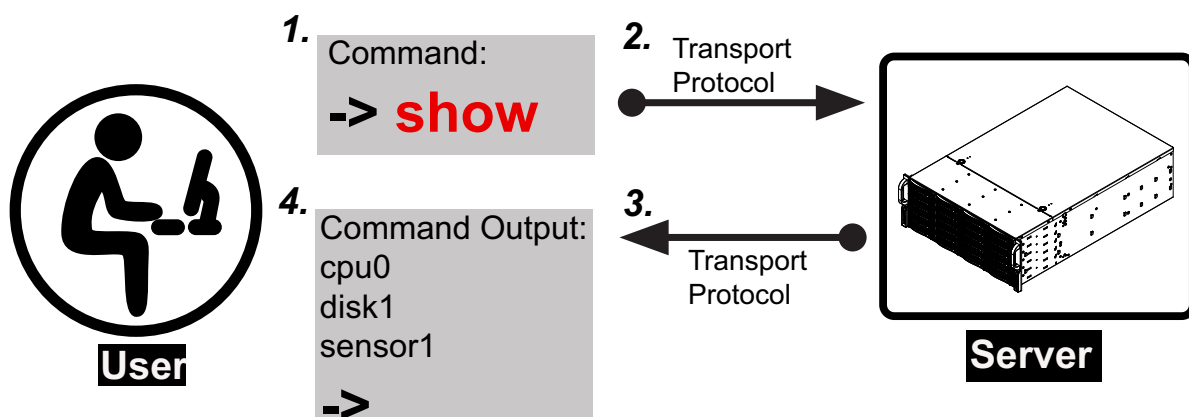


Figure 1 SMASH-CLP User Interface

SMASH Compliance Information

The SMASH platform documented in this user's guide is developed in reference to and in compliance with the SMASH Initiative Standards based on the following DMTF documents.

- System Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP) Architecture White Paper (DSP 2001)
- SM CLP Specification (DSP 0214)
- SM ME Addressing Specifications (DSP 0215)
- SM SLP to CIM Common Mapping Specification (DSP 0216)
- Common Information Model (CIM) Infrastructure Specification (DSP0004)
- The Secure Shell (SSH) Protocol Architecture (RFC4251)
- The Secure Shell (SSH) Connection Protocol (RFC4254)

B.2 An Important Note to the User

The information included in this user's guide provides a general guideline on how to use the SMASH protocol for the system management. Instructions given in this document may or may not be applicable to the system depending on the configuration of the system or the environment it operates in.

For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI BIOS, RSD/SCC, TAS, and IPMIView, please refer to our website at <https://www.supermicro.com/products/nfo/IPMI.cfm> 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

The users 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.

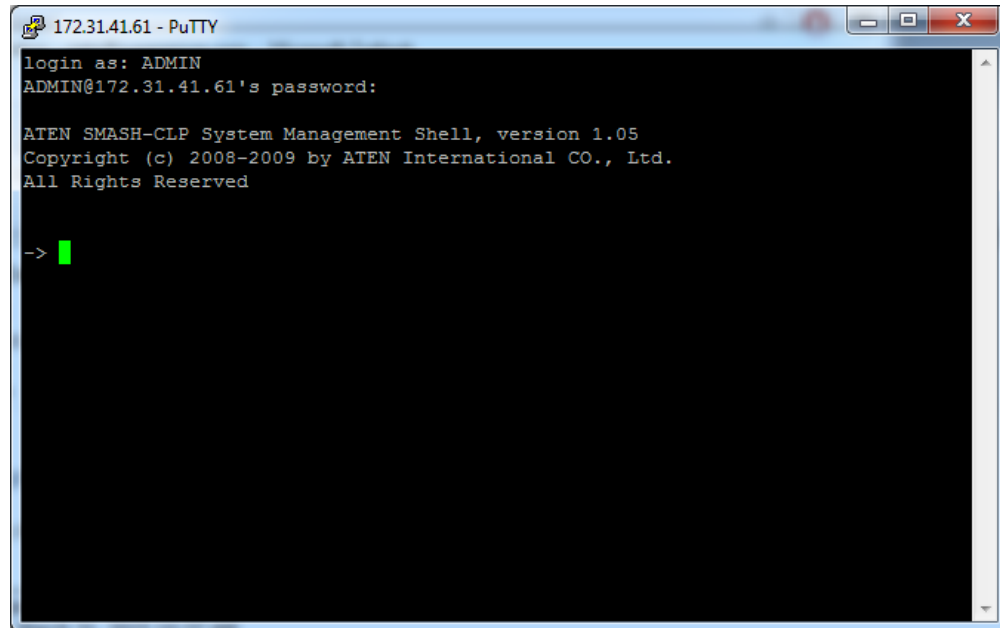


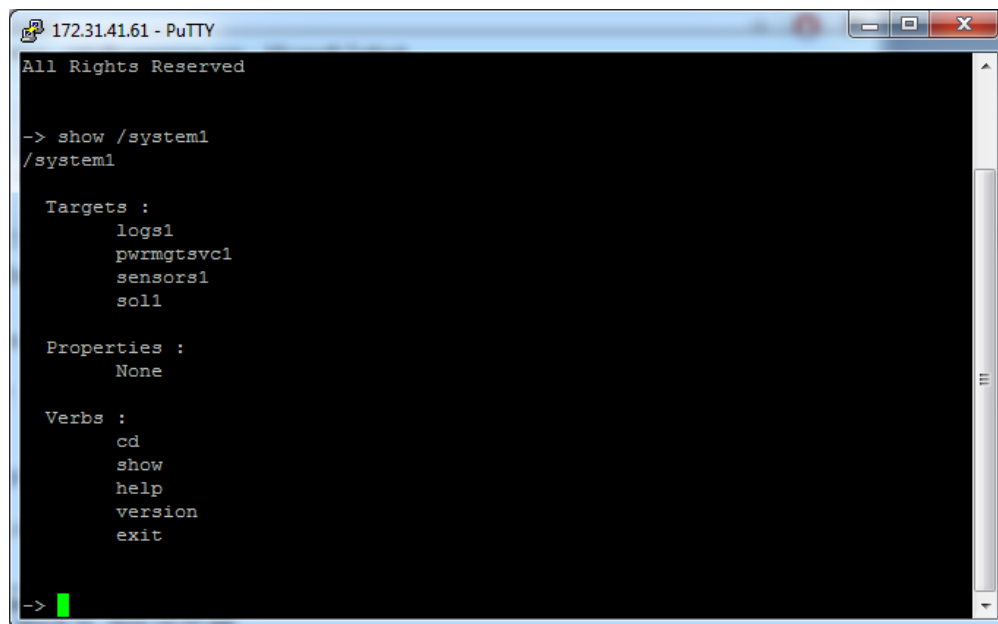
Figure 2 SMASH-CLP Main Screen

B.6 Using SMASH for System Management

After the users have familiarized themselves with the SMASH commands, they 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 the users want to assign to a target machine or to get from a target machine.



```
172.31.41.61 - PuTTY
All Rights Reserved

-> show /system1
/system1

Targets :
  logs1
  pwrmgtsvc1
  sensors1
  sol1

Properties :
  None

Verbs :
  cd
  show
  help
  version
  exit

-> █
```

Figure 3 Using SMASH for System Management

B.7 Definitions of Commands Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow the users 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 the users 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 the users want to exit from a SMASH session or close a session.

- ***help***

The command verb *help* is used when the users 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 the users 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 the users 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 the user	Levels should be expressed in a natural number or "all".
-Output <args>	-o	Controls the format and the content of a command output. This only supports "format=clpxml" and "format=keyword"	Many variables or factors can affect the outcome of format, language, level of details of the output.
-Source <URI>	None	Indicates the location of a source image or a target	URI or SM Instance Address
-Version	-v	Displays the version of the command verb	None
-Wait	-w	Instructs the Command Processor to hold the command response or query result until all spawned jobs are completed.	None

Table 1 SMASH Commands

B.9 Standard Command Options

The following table lists the standard command options.

CLP Option	CLP Verbs												
	CD	Create	delete	dump	exit	help	load	reset	set	show	start	Stop	version
all										x			
destination				x									
display										x			
examine	x	x	x	x	x	x	x	x	x	x	x	x	x
force			x	x			x	x	x	x	x	x	
help	x	x	x	x	x	x	x	x	x	x	x	x	x
keep													
level										x			
Output	x	x	x	x	x	x	x	x	x	x	x	x	x
Source							x						
Version	x	x	x	x	x	x	x	x	x	x	x	x	x
Wait													

Table 2 Standard Command Options

B.10 Target Addressing

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

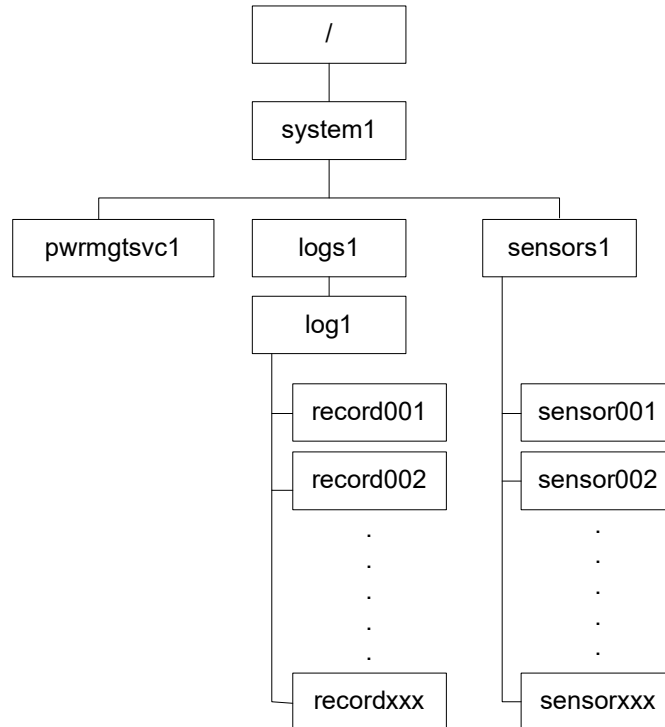


Figure 4 Target Addressing Diagram

Terms Used in the Target Addressing Diagram

This section provides the descriptions of the terms used in the Target Addressing Diagram above.

- **" / "** indicates *the root* of the system.
- **" /system1 "** includes all major *Targets*.
- **" /system1/logs1/log1 "** includes all sensor event logs.
- **" /system1/sensors1 "** contains the readings and information of all sensors.
- **" /system1/pwrmgtsvc1 "** is used for chassis control.
- **"show../logs1 "** allows the users to issue SMASH commands for the system to perform the tasks of the user's choice. For example:
 - Issuing the command **"show/system1/logs1 "** while you are in **"show../logs1 "** will allow the users to set the *Absolute* or the *Relative* target path.

Notes

Appendix C

RADIUS Configuration

C.1 Overview

This chapter provides instructions on how to configure RADIUS on Ubuntu and the Windows operating systems.

RADIUS (Remote Authentication Dial In User Service) is a network protocol that allows the users to manage remote user authentication and accounting. It authenticates users trying to establish a network connection, authorizes users to access the network, and accounts for users accessing the network. Before running RADIUS, the users needs to configure the user account and client information.

C.2 Configuring a User Account in Ubuntu

Follow the instructions below to configure a user account.

1. To add a local user and password, type the following command at the prompt and press <Enter>:

```
# vi/etc/freeradius/client.conf
```

2. Users will then be able to grant privileges to a user account. There are four types of user accounts. The list below displays the four types of accounts and vendor-specific attributes.

- radius_admin: Password: "123456"
Vendor-Specific Attributes: "H=4, I=4"
- radius_operator: Password: "654321"
Vendor-Specific Attributes: "H=3, I=3"
- radius_user: Password: "654321"
Vendor-Specific Attributes: "H=2, I=2"

- radius_callback: Password: "654321"
Vendor-Specific Attributes: "H=1, I=2"

C.3 Configuring Client Account in Ubuntu

Follow the instructions below to configure the client information.

1. To add the client IP, secret and short name, type the following command at the prompt and press <Enter>:

```
# vi /etc/freeradius/users
```

Example:

```
client 192.123.4.5 {  
secret    = super  
shortname = superbmc  
}
```

C.4 Starting the RADIUS Server Ubuntu

1. To start the server, type the following command:

```
# service radiusd start
```

2. To start the server in debugging mode, type the following command:

```
# /usr/sbin/radiusd
```

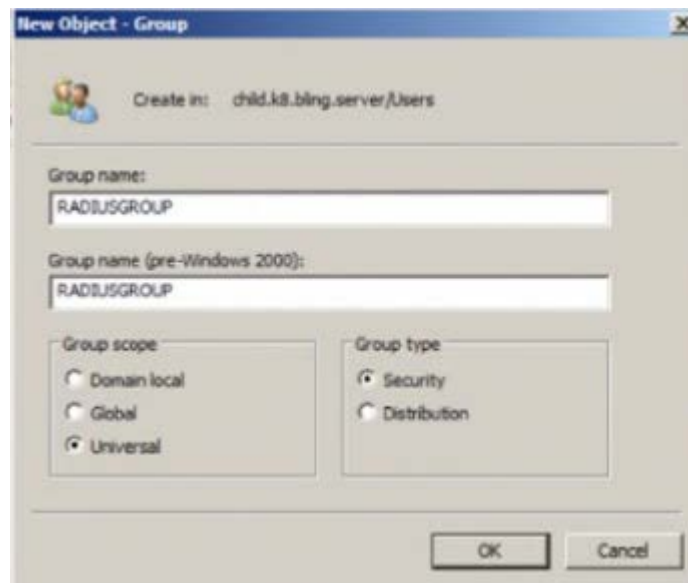
C.5 Adding Roles in Windows

Follow the instructions below to add a role in Windows Server.

1. Click on the <Start> button, then *Administrative Tools* and then *Server Manager*.
2. Under *Server Manager*, select *Add Roles*.
3. Select *Server Roles* and click on <Next>.
4. Select *Network Policy and Access Services* and click on <OK>.

Adding a New Object - Group

1. To add a new object group, enter the group name and select the group scope and type. Click on <OK> to complete this step.



Add a New Object - User

1. To add a new object user, enter the user's name and login name. Click on <Next>.

Adding a New Network Policy

1. To add a new network policy, click on *Network Policies*. Enter the policy name and select the type of network access server.

New Network Policy

Specify Network Policy Name and Connection Type

You can specify a name for your network policy and the type of connections to which the policy is applied.

Policy name:

PM

Network connection method

Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select Unspecified.

☒ **Type of network access server:**

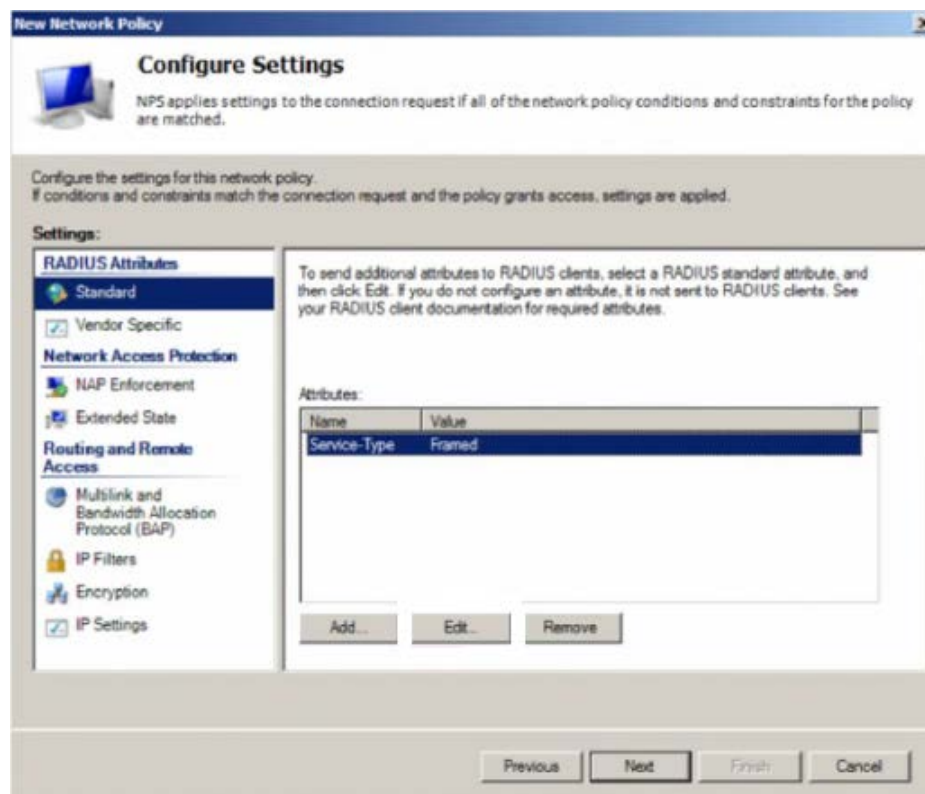
Unspecified

☐ **Vendor specific:**

10

Previous Next Finish Cancel

2. Click on <Next> to choose a permission.
3. Then configure Constraints and remove *Framed* protocol.
4. Edit Service-Type for login.
5. Check the *Others* option and select *Login*. Click <OK> to complete the configuration.

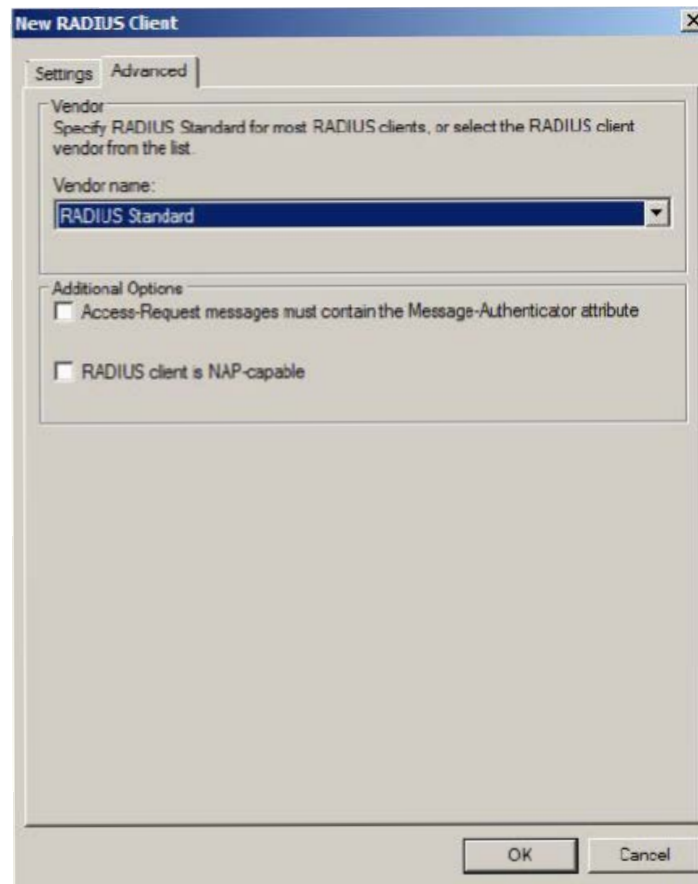


Adding a Vendor Specific

1. In the *New Network Policy* screen, select *Vendor Specific* and click <Add>.
2. Select a vendor specific attribute and click <Add>.
3. Click <Add> and configure the attribute.
4. Specify the vendor specific account and click the <Configure Attribute> button to configure the attribute. Click on <OK> to complete the configuration.

Configuring a New RADIUS Client

1. In the *New RADIUS Client* screen, select the *Settings* tab and enter information in the following fields:
 - Friendly name:
 - Address (IP or DNS):
 - Shared secret:
 - Confirm shared secret:
2. In the *Advanced* tab, select a vendor name from the drop-down menu. Select RADIUS Standard for most RADIUS clients.



Notes

Appendix D

Unique Password for BMC

D.1 Overview

Due to California Senate Bill No. 327, a common default password is required to be available in a connected device that is capable of connecting to an IP network. Supermicro will no longer use the default password “ADMIN” for new devices or systems. Instead, we will assign a unique password that is specific to each new motherboard.

Effective as of January 1, 2020, each new Supermicro motherboard will come with two labels that contain a unique password assigned to that motherboard. One unique password label will be placed near the BMC (Baseboard Management Controller) chip and/or close to the MB serial number label. This label is not to be removed. The other unique password label will be placed on the CPU1 socket cover. This label is removable and can be placed in any location, such as on the side of the chassis or a service tag.

When logging in to the BMC for the first time, please use the unique password provided by Supermicro to log in. Afterward, the unique password can be changed to the customer's chosen user name and password for subsequent logins.

For more information regarding BMC passwords, please visit our website at <http://www.supermicro.com/bmcpassword>.

D.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

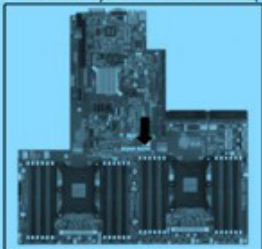
1. On the system motherboard (label locations will vary depending on motherboard model)


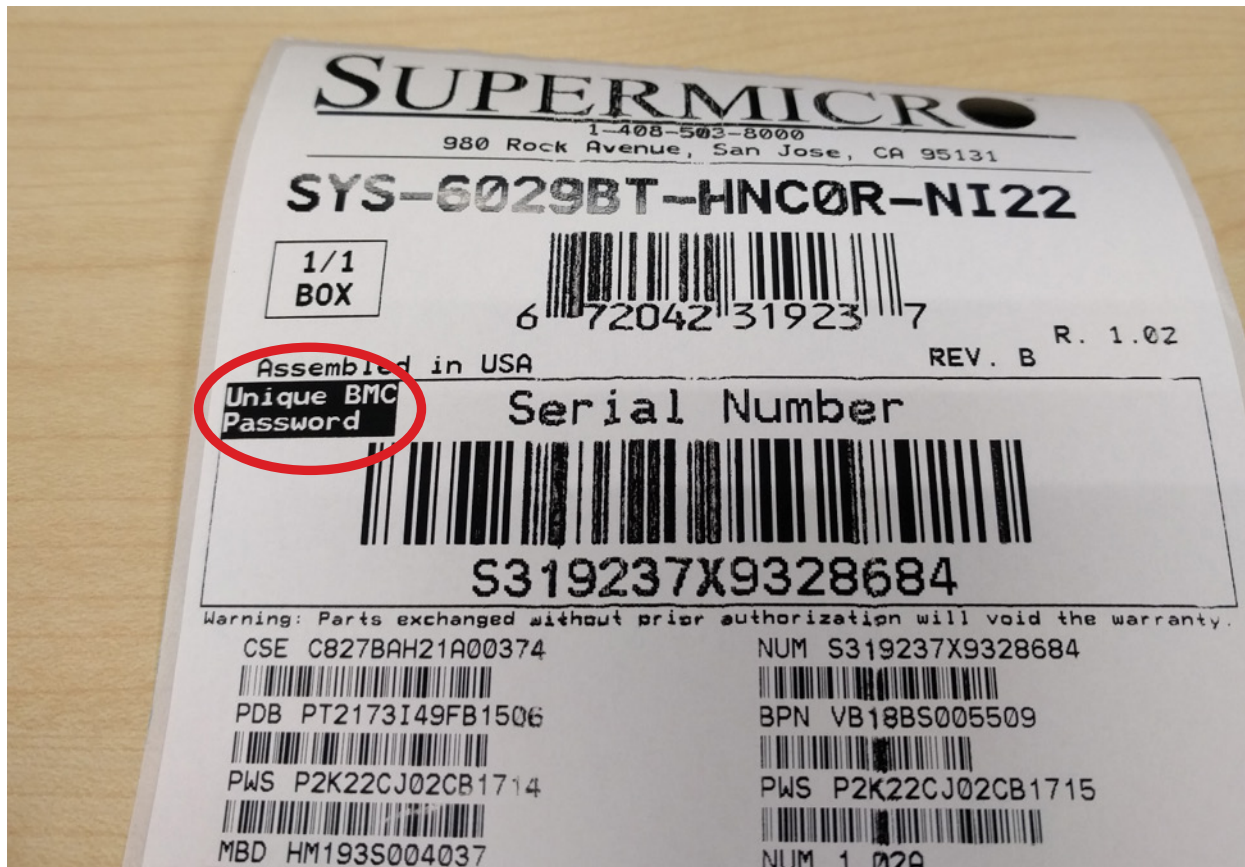
Figure 2: BMC barcode labels located on the motherboard

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

D.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.

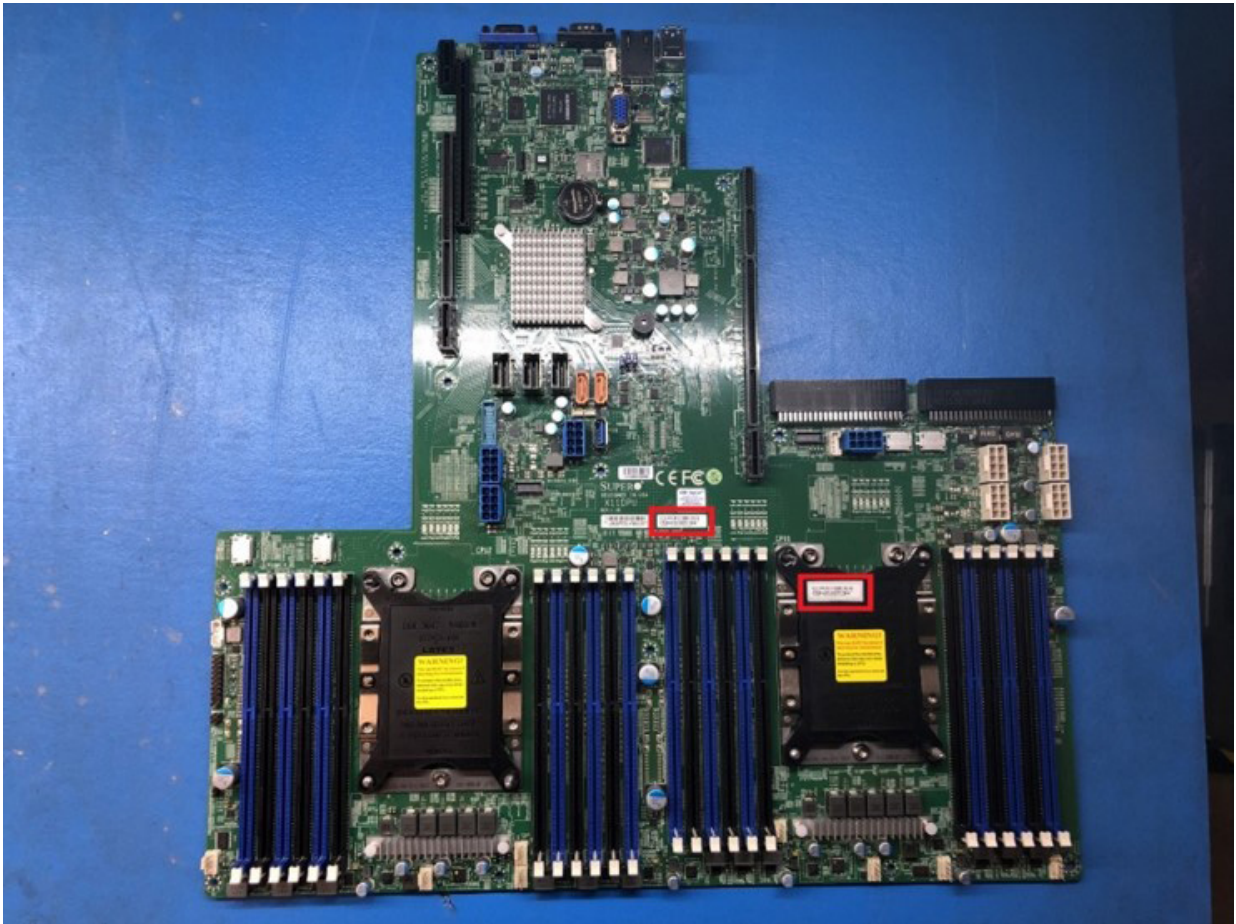
Most systems have a pull-out tag to display the BMC MAC address and the preprogrammed unique password. The rest of the systems will have the sticker on top/front of the chassis.



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



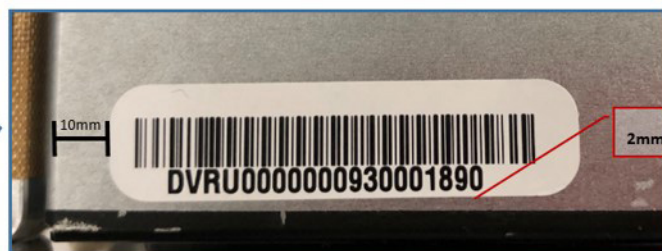
Label on the opposite side of the service tag



Label on the opposite side of the service tag



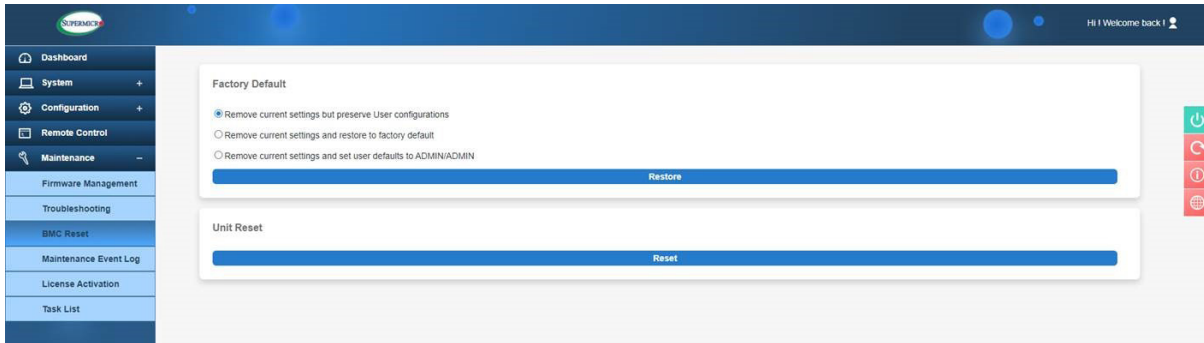
Label on the opposite side of the service tag



Label location on chassis

D.4 Restore Factory Default

Users 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.

D.5 Change All Unique Passwords Using Script

Due to possible different operating environments, the user is given the option to modify their provisioning script and unique passwords.

D.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, please contact the direct sales support to receive the soft copy of the password.

Question: What if the password stickers on the chassis and the motherboard are different?

Answer: If there is a discrepancy, use the motherboard sticker. The motherboard sticker is always correct.

Question: I purchased my products from a distributor. Can Supermicro provide me soft copies of the unique preprogrammed passwords?

Answer: At this time, we only have the ability to provide soft copies to our direct customers. These customers will need to register their products to obtain soft copies of their passwords. For direct customers, please use the Supermicro Customer Registration portal.

Question: Do you have a script that can change all unique passwords to my password?

Answer: We will provide a sample script with documentation. Of course, the operating environment may change from customer to customer. It is the end user's responsibility to modify their 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. Customers will be able to change the preprogrammed password themselves or they can work with their 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: Please contact the systems integrator (SI) or value-added reseller (VAR) to assist you in this process.

Question: Can Supermicro apply a single unique customer-specified password for all my systems? Will this comply with SB327?

Answer: All systems from Supermicro will ship with a unique preprogrammed password. Customers will be able to change the password on each system. In order for Supermicro to comply with SB327, we are not able to use customer-specified passwords. All passwords will be unique and assigned at the time of manufacturing.

Question: When will my motherboard have this change rolled out?

Answer: Supermicro plans to have new stickers rolled out starting mid-December 2019.

(Disclaimer Continued)

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