



SSE-T7132 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: July 31, 2023

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 © 2023 by Super Micro Computer, Inc.
All rights reserved.

Printed in the United States of America

Preface

About This Manual

The Super Micro Computer SSE-T7132 is Supermicro's next-generation 400Gbps Open Networking Switch SSE-T7132. It is designed to provide high density and superior performance as a professional data center switch with a robust 50 Gbps PAM4 SERDES that lowers the cost per bit and enable higher scale I/O such as 200 GbE and 400 GbE while maintaining backward compatibility with 10/25G NRZ. SSE-T7132 delivers exceptional forwarding performance for today's networking applications such as High Performance Computing Clusters, Cloud computing and most of the data center applications. With the ability to use it as a single SKU over various network layers such as Data Center Spine, leaf, ToR and DCI applications, SSE-T7132 provides easy of management and thus less burden to users.

User's Guide Organization

Chapter 1 provides an overview of the ASPEED AST2600 controller. It also introduces the features and the functionalities of SSE-T7132 BMC.

Chapter 2 provides detailed instructions on how to configure the SSE-T7132 BMC settings supported by the AST2600 controller.

Chapter 3 provides the answers to frequently asked questions.

Chapter 4 provides detailed instructions to setup the UEFI BIOS Setup utility.

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 your computer may or may not look exactly like the screen shown in this user's guide.

Conventions Used in the Manual

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



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



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



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



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

Contacting Supermicro

Headquarters

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

Tel: +1 (408) 503-8000

Fax: +1 (408) 503-8008

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

Website: www.supermicro.com

Europe

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

Tel: +31 (0) 73-6400390

Fax: +31 (0) 73-6416525

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

Website: www.supermicro.nl

Asia-Pacific

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

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3992

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

Website: www.supermicro.com.tw

Table of Contents

Chapter 1 Introduction

1.1 Introduction to the SSE-T7132 BMC Platform	8
1.2 Overview of the ASPEED AST2600 BMC	8
1.3 Supermicro SSE-T7132 BMC Features	9
1.4 Applicable or Supported Platforms	11
1.5 Special Notes for Motherboard and Firmware Support	11

Chapter 2 Configuring the BMC Settings

2.1 Configuring UEFI BIOS	12
2.2 Configuring the IP/MAC Addresses for Remote Servers	23
2.3 Connecting to the Remote Server	24
2.4 Accessing the Remote Server Using the Browser	25
2.5 BMC Dashboard	26
2.6 System	30
2.7 Configuration	44
2.8 Remote Control	78
2.9 Maintenance	113

Chapter 3 Frequently Asked Questions

Chapter 4 UEFI BIOS

4.1 Introduction	145
4.2 Main Setup	146
4.3 Advanced Setup Configurations	148
4.4 Security	155
4.5 Boot	156
4.6 Save & Exit	159

Appendix A Firmware Update via WEB GUI

A.1 Overview	161
A.2 Updating Firmware Using BMC WEB GUI	162

Appendix B Introduction to SMASH

B.1 Overview	170
B.2 An Important Note to the User	171
B.3 Using SMASH	171
B.4 Initiating the SMASH Protocol	172
B.5 SMASH-CLP Main Screen	173

B.6 Using SMASH for System Management.....	174
B.7 Definitions of Commands Verbs.....	175
B.8 SMASH Commands	177
B.9 Standard Command Options.....	178
B.10 Target Addressing	179
<i>Appendix CRADIUS Configuration</i>	
C.1 Overview.....	180
C.2 Configuring a User Account in Ubuntu.....	180
C.3 Configuring Client Account in Ubuntu	181
C.4 Starting the RADIUS Server Ubuntu.....	181
C.5 Adding Roles in Windows	182
<i>Appendix D Unique Password for BMC</i>	
D.1 Overview.....	186
D.2 Restore Factory Default	187
D.3 Change All Unique Passwords Using Script.....	187
D.4 Frequently Asked Questions	188

Chapter 1

Introduction

1.1 Introduction to the SSE-T7132 BMC Platform

The SSE-T7132 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.

SSE-T7132 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 SSE-T7132 BMC firmware built in, the Supermicro motherboard allows you to access, monitor, diagnose, and manage a remote server via Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

1.2 Overview of the ASPEED AST2600 BMC

The ASPEED AST2600 BMC connects with the host system via PCIeexpress Gen2 x1 bus to communicate with the graphics core. It supports a 64-bit 2D Graphics Accelerator with 32-bit memory and 16-bit I/O space.

Additionally, AST2600 supports USB 1.1 and 2.0 for remote KVM emulation and provide LPC interface support to control Super IO functions. ASPEED AST2600 include Keyboard/Video/Mouse Redirection (KVMR). The SSE-T7132 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 SSE-T7132 BMC Features

- Remote KVM (graphics) console
- Virtual Media and ISO images
- Remote server power control
- Remote Serial over LAN (text console)
- Event Log support
- Automatic Notification and Alerts (SNMP and email)
- Hardware Monitoring
- Overall health display on the main page
- Out of band management through shared or dedicated LAN
- Option to change LAN connection interface at Runtime
- VLAN
- RMCP and RMCP+ protocols supported
- SMASH/CLP
- Secure command line interface (SSH) and Telnet
- RADIUS authentication support
- Secure browser interface (Secure socket layer - SSL support)
- 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

1.4 Applicable or Supported Platforms

This BMC server and firmware applies to High-performance SONiC Open Networking aggregation switch. Supported platforms include the following.

- SSE-T7132S
- SSE-T7132SR
- SSE-T7132D
- SSE-T7132DR

1.5 Special Notes for Motherboard and Firmware Support

For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, UEFI BIOS, TAS, and IPMIView, please refer to our website at <https://www.supermicro.com/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 you to access, monitor, manage, and interface with multiple systems from different remote locations. The necessary firmware for accessing and configuring the SSE-T7132 BMC settings is available on the Supermicro website at <http://www.supermicro.com/products/nfo/ipmi.cfm>. This section provides detailed information on how to configure BMC settings.

2.1 Configuring UEFI BIOS

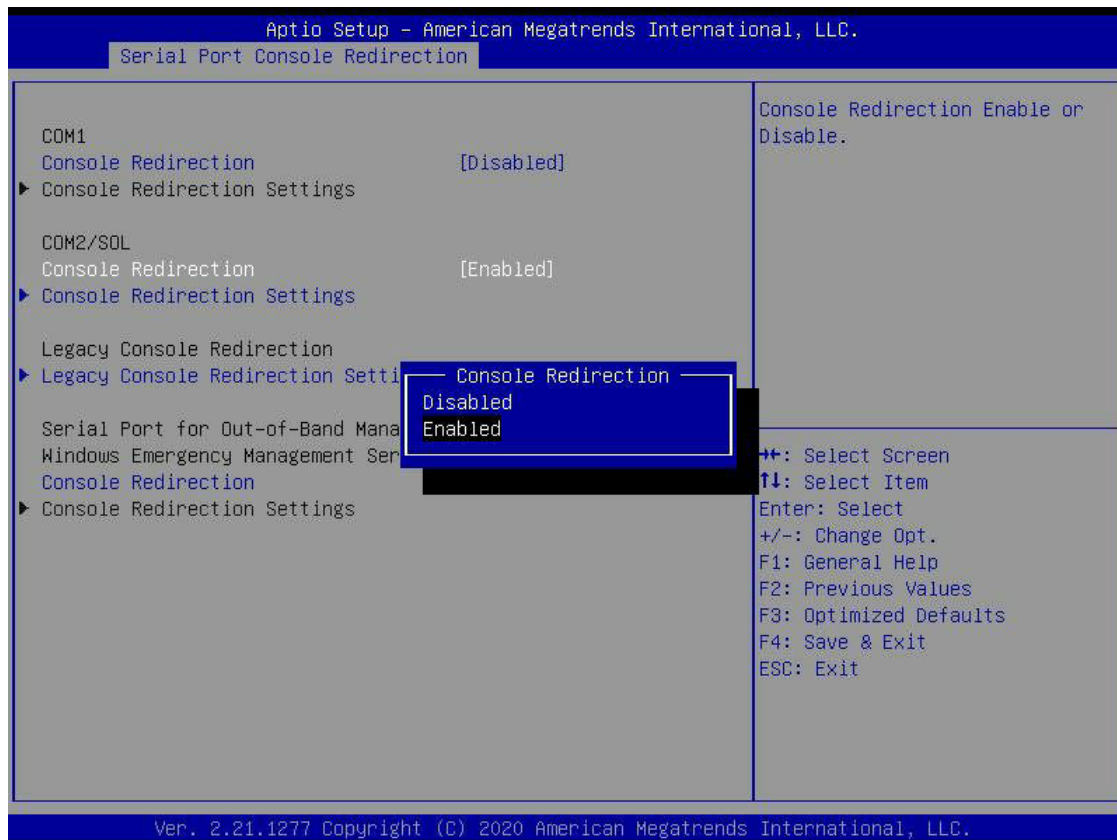
Before configuring the BMC, follow the instructions below to configure the system UEFI BIOS settings.

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>.

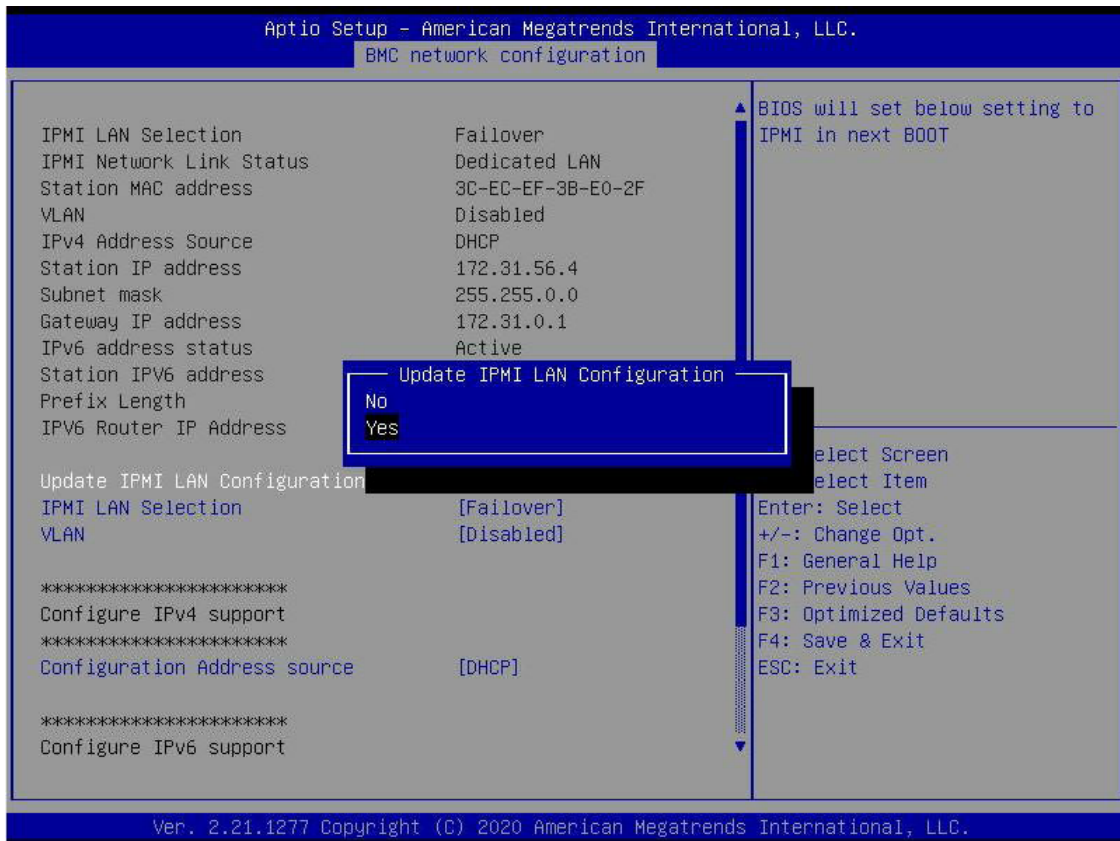
Enabling the COM port for SOL (BMC)

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].

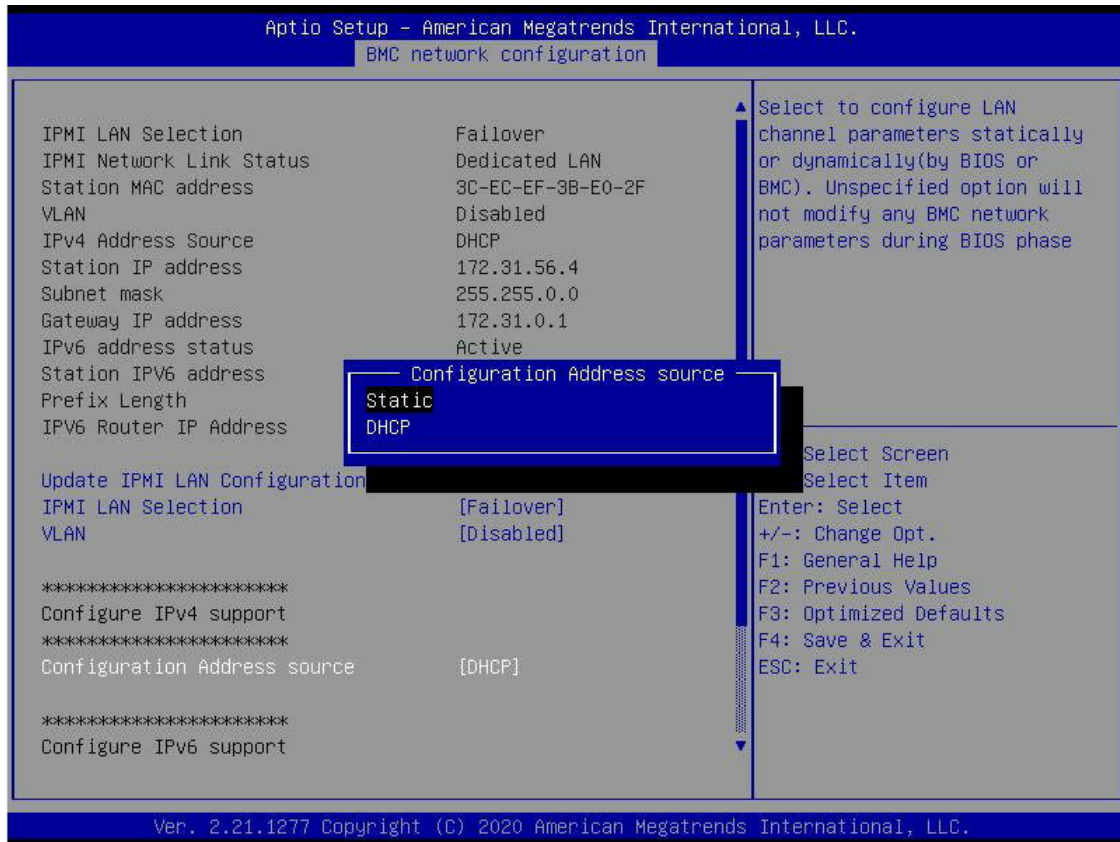


Configuring IP Address Using the UEFI BIOS

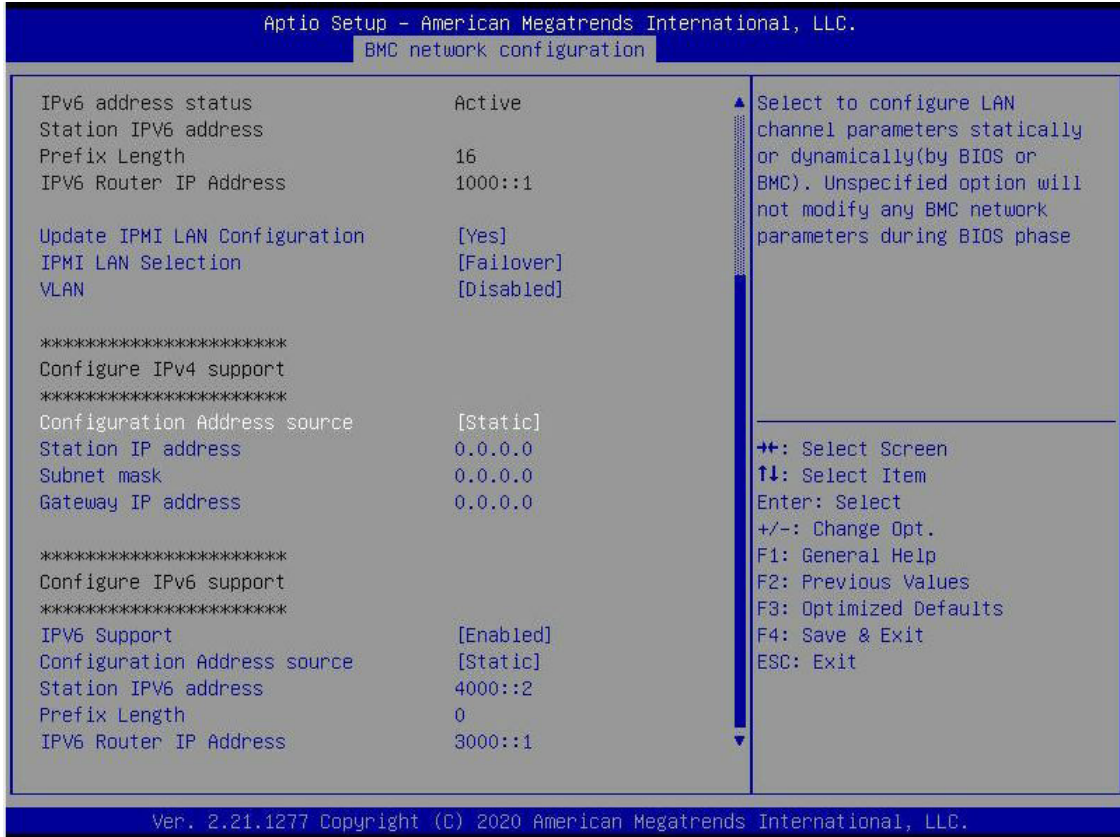
1. Select the *Server Management* tab.
2. Select *BMC Network Configuration* and press <Enter>.
3. Select *Update IPMI LAN Configuration*, and then press <Enter> and select [Yes].



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

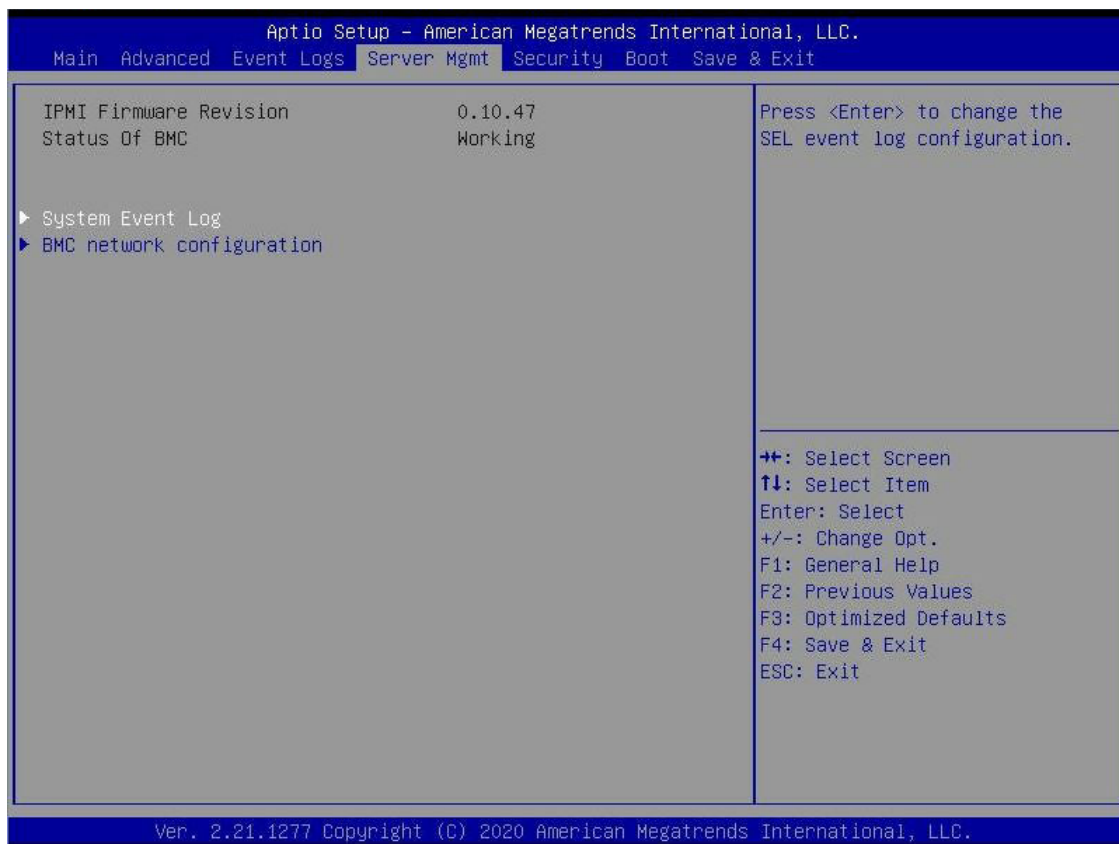


- Once the Configuration Address Source is set to [Static], the Station IP Address, Subnet Mask, and Gateway IP Address fields will display 0.0.0.0, which indicates that these fields are ready for you to change to new values. Select each of the three items and enter the values. Press <Enter> when finished.

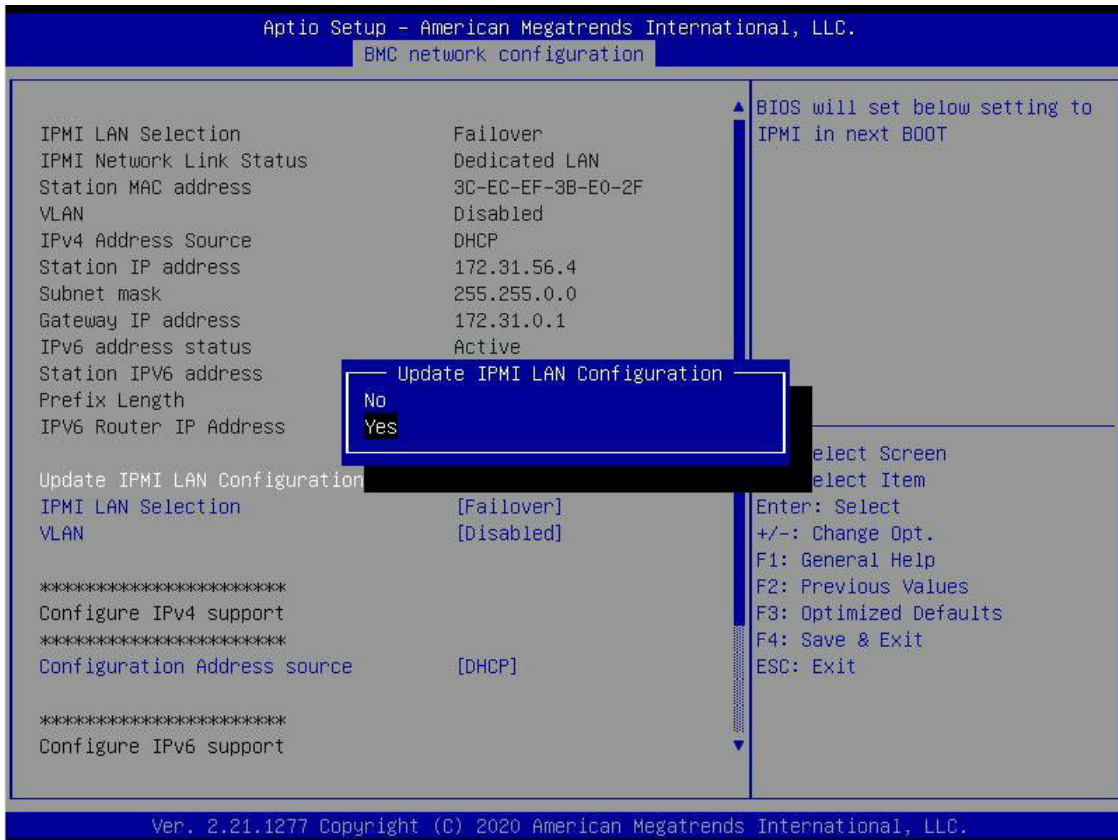


Connecting to BMC Using the UEFI BIOS

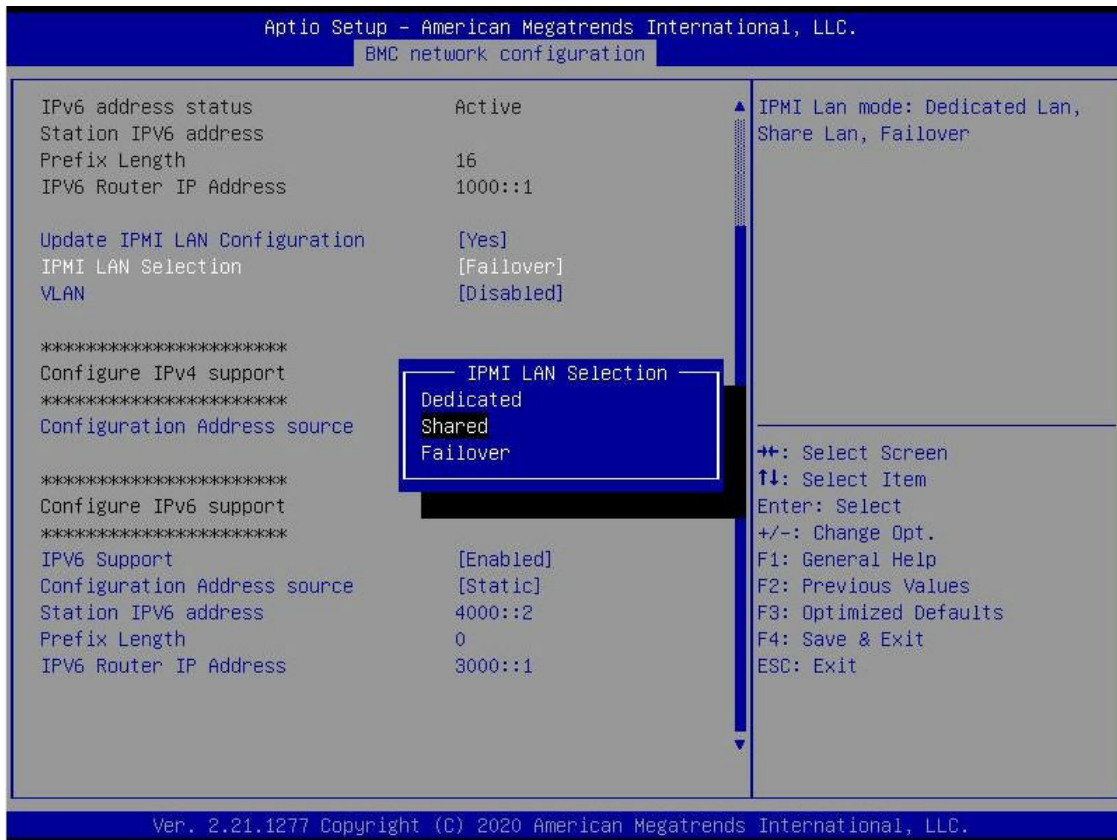
1. Plug Cat 5 cable into Linux Laptop.
2. Plug the other end of the cable into the IPMI / SHARED port.
3. In Linux Laptop, configure Network settings for Static IP, and assign IP (such as 192.168.0.4) and subnet. Gateway IP does not matter since there's no router/switch in between.
4. Launch Superserver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



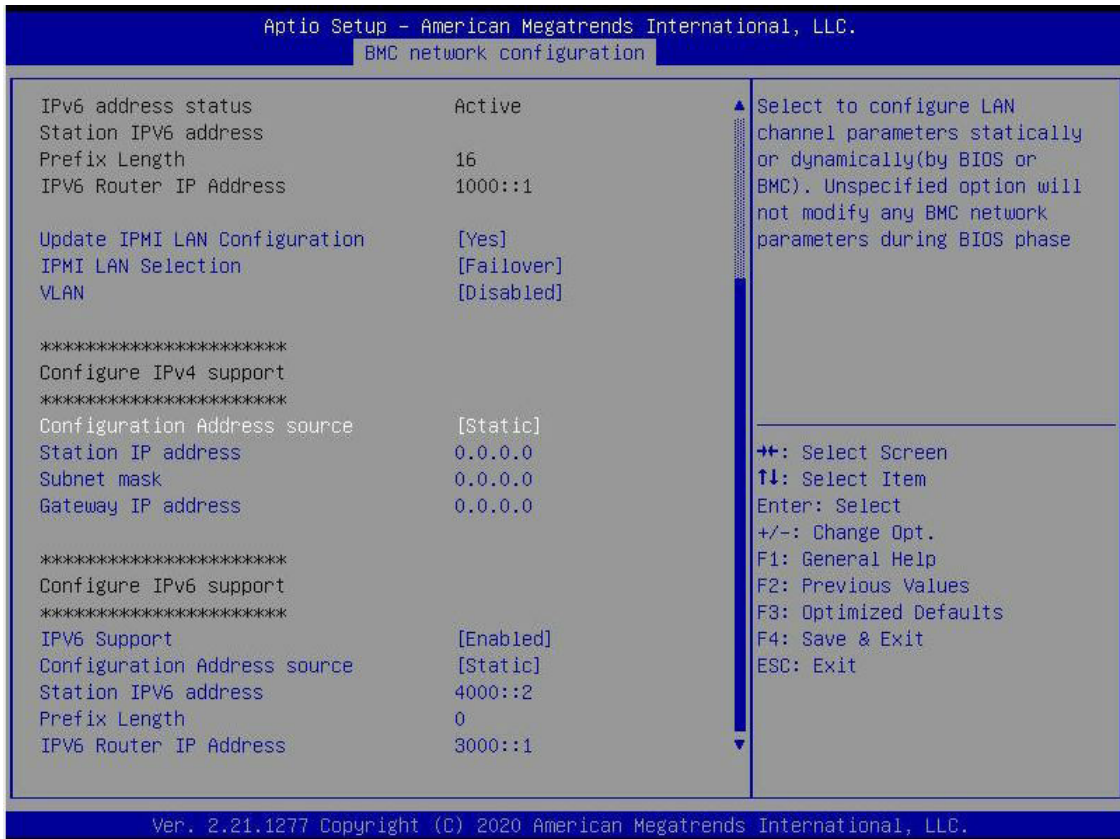
7. Select *Update IPMI LAN Configuration* and select [Yes].



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

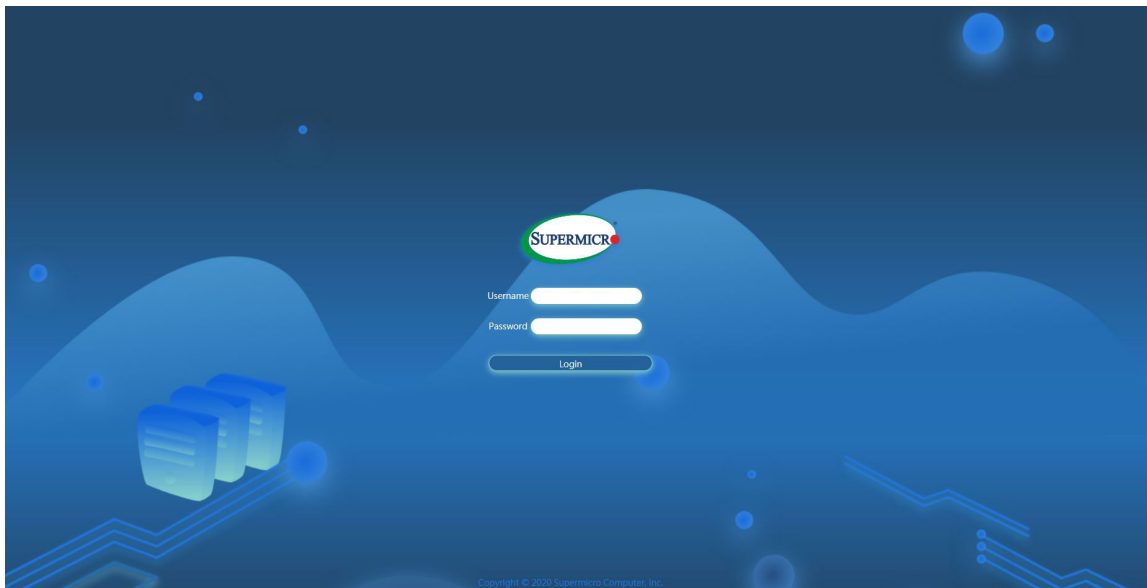


- Navigate to *Configuration Address Source* and select [Static]. Then you can assign an IP (such as 192.168.0.4) and subnet.

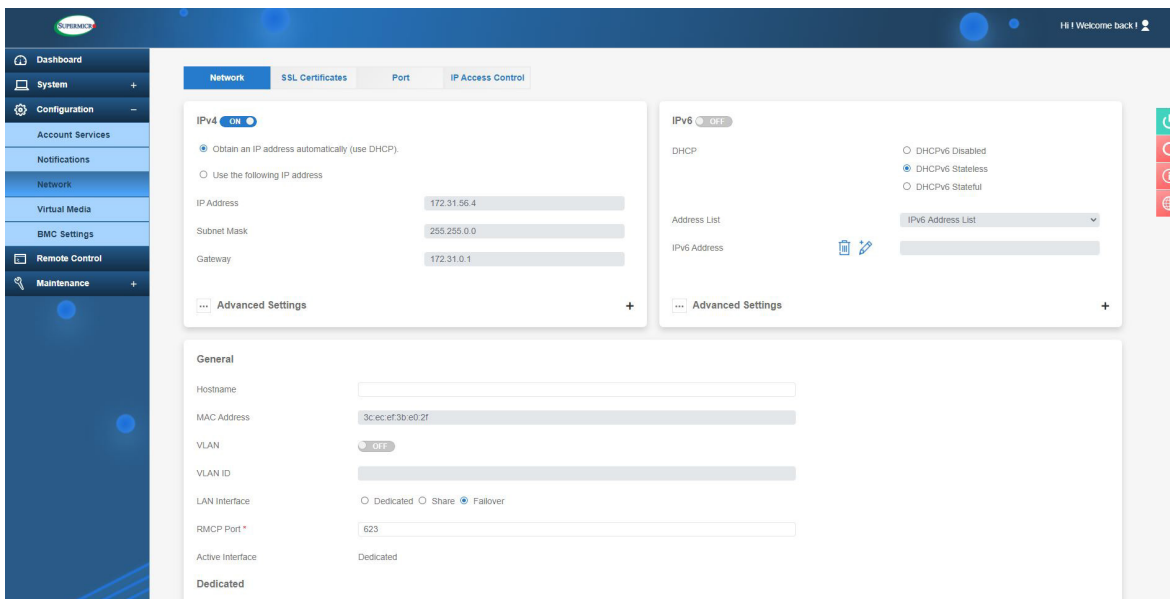


Now that both Laptop and the SSE-T7132 BMC are on the same subnet. With the static IP connected, you should be able to communicate. To establish the connection, please follow the steps below.


1. Keep the terminal of the 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 user name, ADMIN, and a BMC unique password. Please refer to Appendix D on how to retrieve the BMC unique password.



4. After logging in, go over to <Network> under <Configuration>. You can then see all the 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's default setting, please use the IPMICFG utility or the UEFI BIOS Setup utility.

1. Run the IPMICFG utility. You 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 VLAN tag 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 you want to connect, enter the IP address in the address bar of the browser.
4. Once the connection is made, the Login screen as shown on the next page will display.

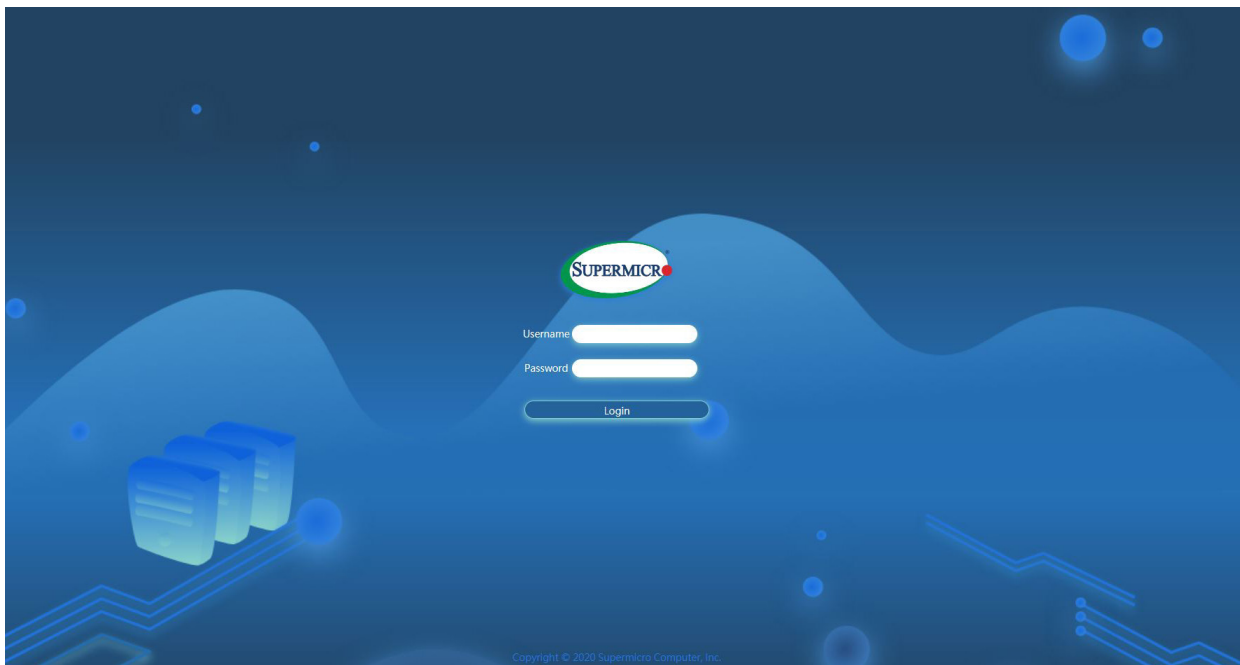
2.4 Accessing the Remote Server Using the Browser

To Log In to the Remote Console


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

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

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



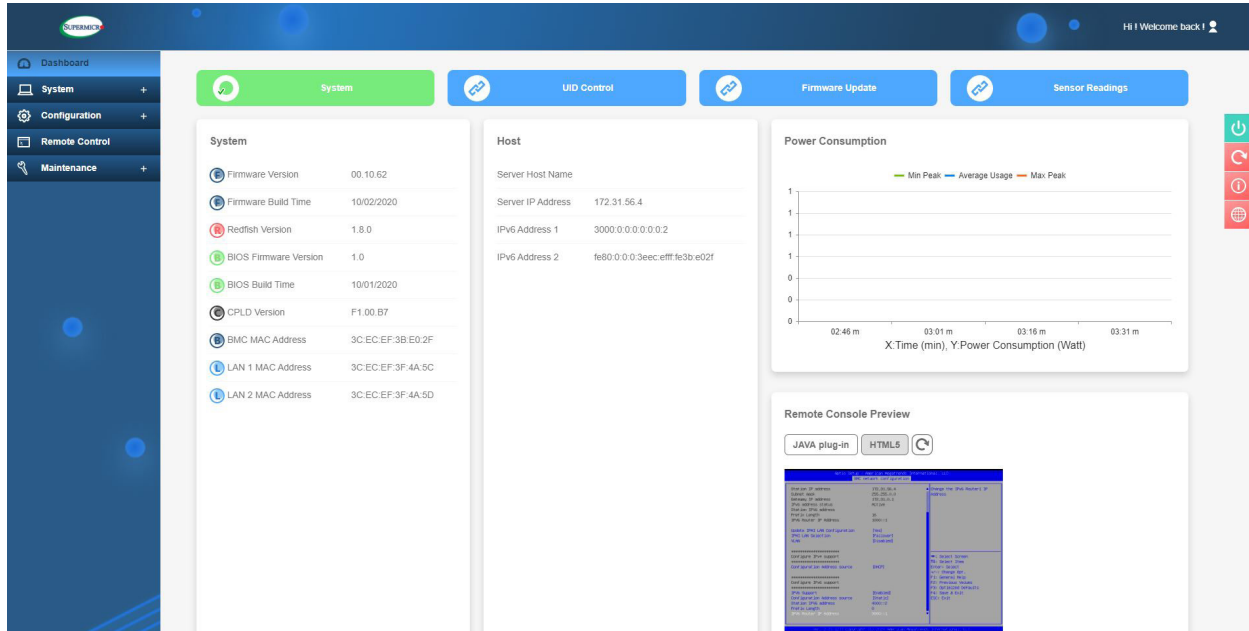
1. Enter the user name in the *User name* box.
2. Enter the password in the *Password* box and click on <Login>.
3. The home page will display as shown on the next page.

 **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 you will also be able to access Storage from here. This page will be displayed as shown below.



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



Information includes:

- User
- Role
- Server
- Logout

The following WebGUIs indicate different purposes.



: Power Control



: Refresh



: Help



: Language

Power Options

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

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



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

Refresh

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

Help

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

Language

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

- English
- Simplified Chinese
- Japanese

The BMC Main displays the following information.

Quick Links

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

- System: You can navigate to the System page.
- UID Control: You can navigate to the UID Control page to turn on or off the LED blinking to identify the server.
- Firmware Update: You can navigate to the Firmware Management page to update the firmware.
- Sensor Readings: You can navigate to the Sensor Readings page.

System Health

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



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




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



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

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.

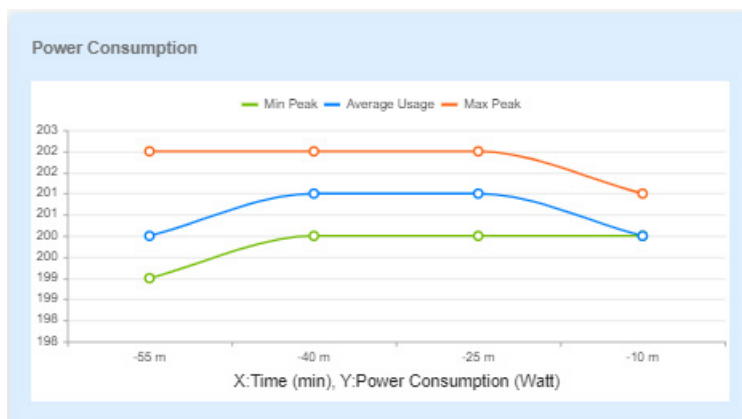
 **Note:** In special motherboards without onboard LANs, AOC NIC information is displayed in place of onboard LANs. In addition, no System LAN interfaces will be shown if LAN interfaces are not detected.

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 the Power page for more details about power consumption.



Remote Console Preview

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

Recent Logs

This section displays the latest health event log entries.

2.6 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).

The screenshot displays the BMC System page interface. On the left is a navigation sidebar with options: Dashboard, System, Configuration, Remote Control, and Maintenance. The main content area has a top navigation bar with tabs: Overview (selected), CPU, Memory, PSU, Power, Network, Sensor, Fan, and GPU. Below the tabs are six component health cards: UID Control (OFF), CPU, Memory, PSU, Sensor, and Fan, each with a green health indicator. A large 'Information' table follows, listing system details. At the bottom, there are four smaller tables: Chassis Info, FRU Device Info, Board Info, and Product Info.

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

Chassis Info	
Type	
Part Number	


FRU Device Info	
Device ID	0

Board Info	
Language	English
Manufacturer	Supernovo

Product Info	
Language	English
Manufacturer	

2.6.1 Component Info

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

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

Overview

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

- Memory – This displays the overall health status of installed memory components in the system. Issues that are occurred in memory modules should not affect Sensor Health monitoring.
- PSU – This displays the overall health status of installed Power Supply Units in the system. Issues that are occurred in PSU units should not affect Sensor Health monitoring.
- Sensor – This displays the overall health status of the sensors present in the system.
- Fan – This displays the overall health status of installed fans in the system. Issues that are occurred in FAN units should not affect Sensor Health monitoring.

- Information: You can check detailed system information.
 - Manufacturer – Manufacturer name
 - Product Part Number – Product part number of the product
 - Serial Number – Serial number of the product
 - Power State – System power status
 - Host Name – Host name of the system
 - BMC IP Address – IP address of the BMC host
 - BMC MAC Address – MAC address of the BMC
 - BMC Firmware Version – BMC Firmware version
 - BIOS Firmware Version – BIOS Firmware version

- Board Info: You 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: You 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.

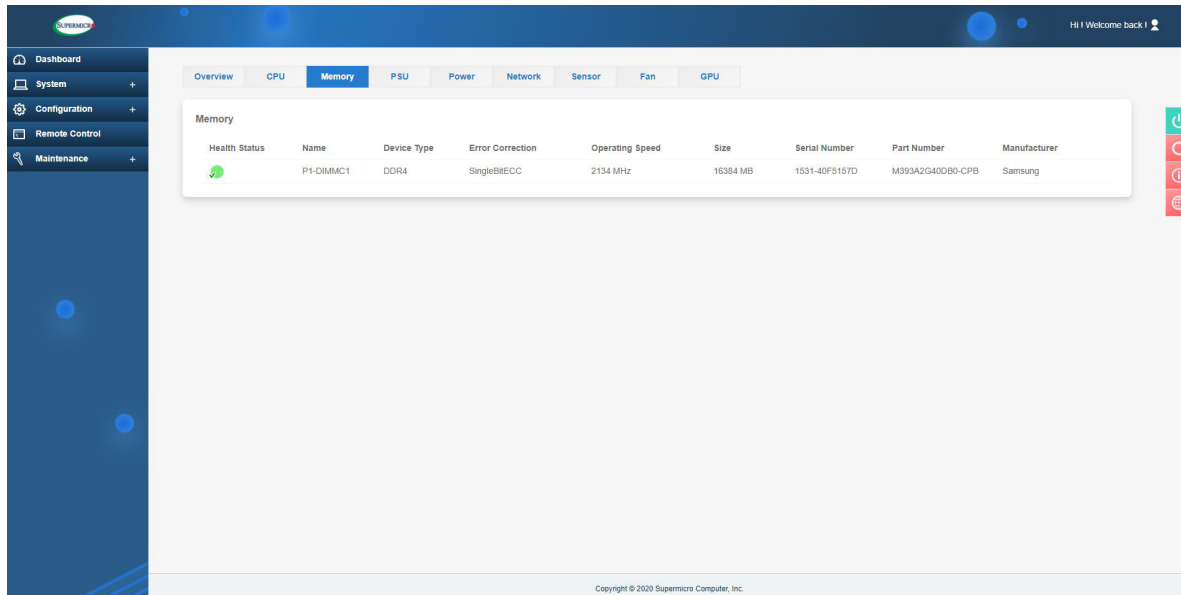
Health Status	Name	Model	Speed	TDP Watts	Core/Active	Threads	Manufacturer
	Processor	Genuine Intel(R) CPU 50000%@	1500 MHz	205	28	56	Intel(R) Corporation

This page displays the following information.

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

Memory

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

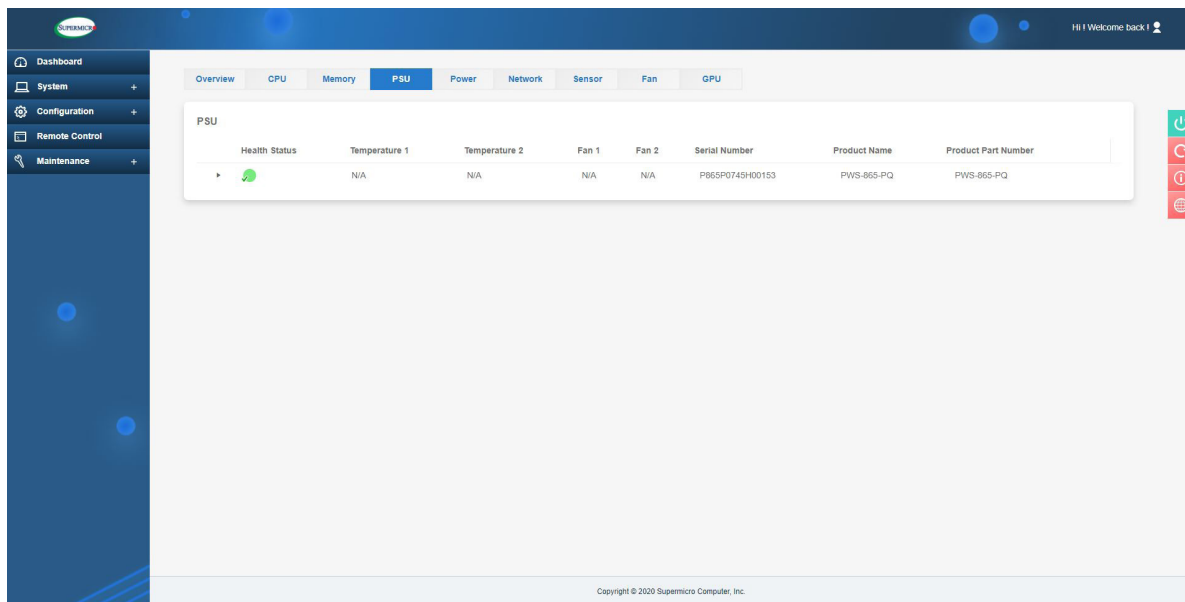


This page displays the following information.

- **Status:** You can view the health status of the DIMM (Normal, Warning, or Critical).
- **Name:** You can view the memory device name.
- **Device Type:** You can view the memory device type defined by SMBIOS (i.e. DDR4, DDR5, RDIMM, LRDIMM, or DCPMM).
- **Error Correction:** You can view the supported error correction info defined by SMBIOS.
 - **AddressParity:** Address parity errors can be corrected.
 - **MultiBitECC:** Multibit data errors can be corrected by ECC.
 - **SingleBitECC:** Single-bit data errors can be corrected by ECC.
- **Operating Speed:** You can view the operating speed of memory in MHz as reported by the memory device. Memory devices that operate at your bus speed shall report the operating speed in MHz (bus speed).
- **Size:** You can view the size of the memory region in mebibytes (MiB).
- **Serial Number:** You can view the product serial number of the memory device.
- **Part Number:** You can view the product part number of the memory device.
- **Manufacturer:** You can view the manufacturer info of the memory device.

PSU

This tab shows power supply unit information.



This page displays the following information.

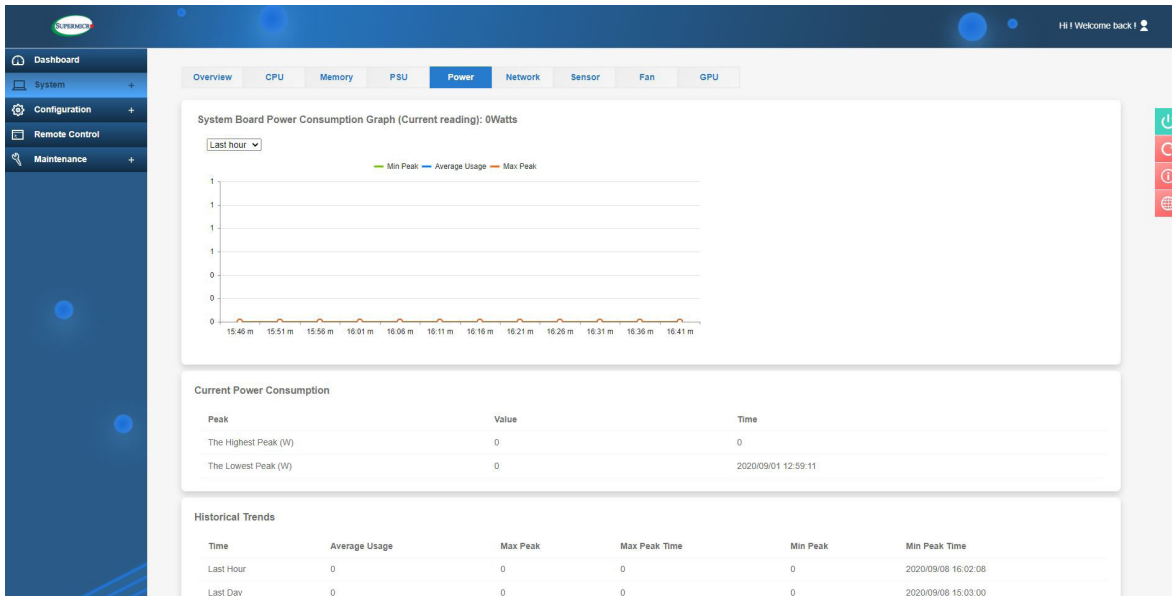
- Health Status: You can view the health status of the PSU (Normal, Warning, or Critical).
- Temperature 1: You can view the temperature reading of the PSU.
- Temperature 2: You can view the temperature reading of the PSU (if present).
- Fan 1: You can view the FAN reading of the PSU.
- Fan 2: You can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

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

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

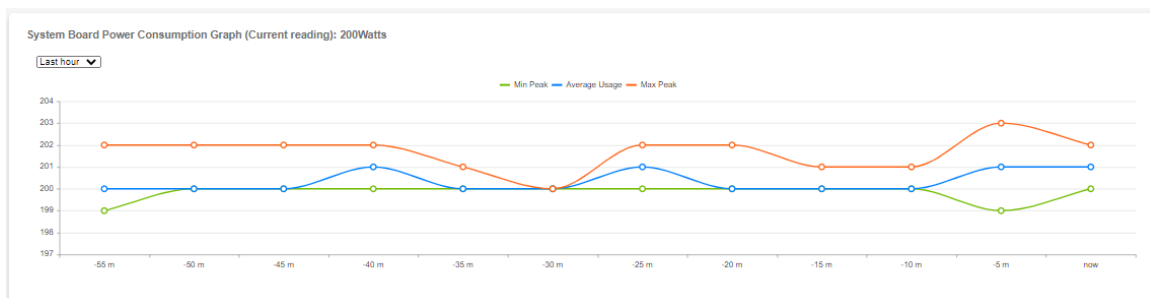
Power

The tab displays system board power consumption information.



This page displays the following information.

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



- Power Consumption Since Powered On: You can view the power consumption during the 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 Trends: You can view past data on power consumption.
 - Duration – 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

Sensor

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

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

The sensor table displays the following information.

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

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

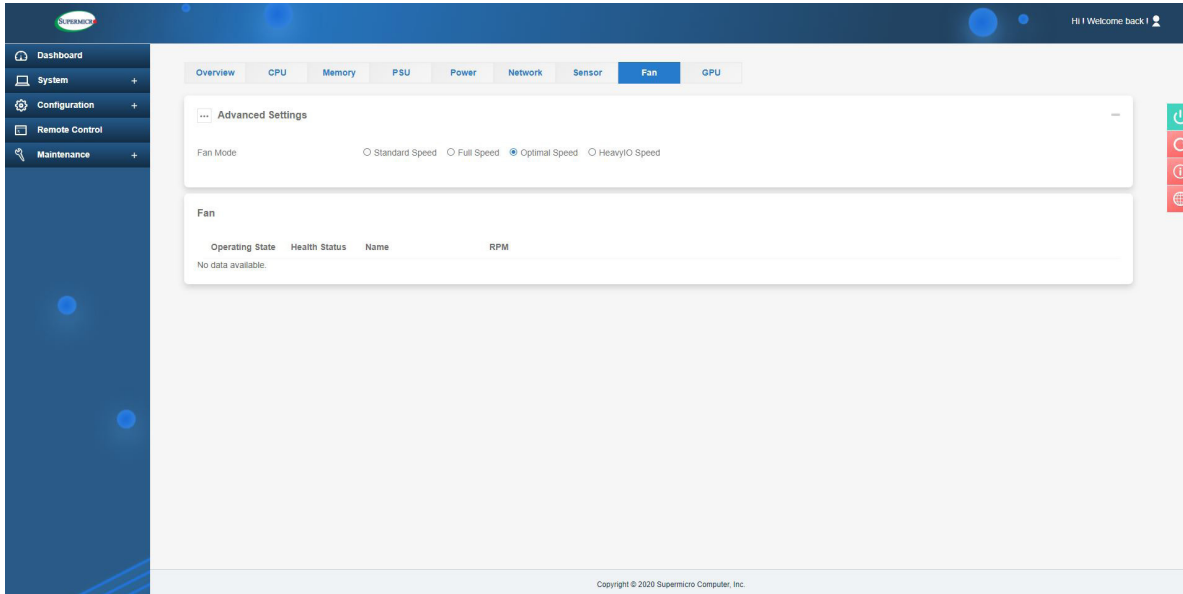


Note: If components are not installed then static sensor values will display N/A.

- Sensor Type Categories: By default, [All Sensors] categories are selected. You can filter sensors by following categories.
 - Voltage
 - Temperature
 - Physical
 - Battery
 - Drive Slot
- Export to Excel: You can export sensor readings in Excel format.

Fans

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




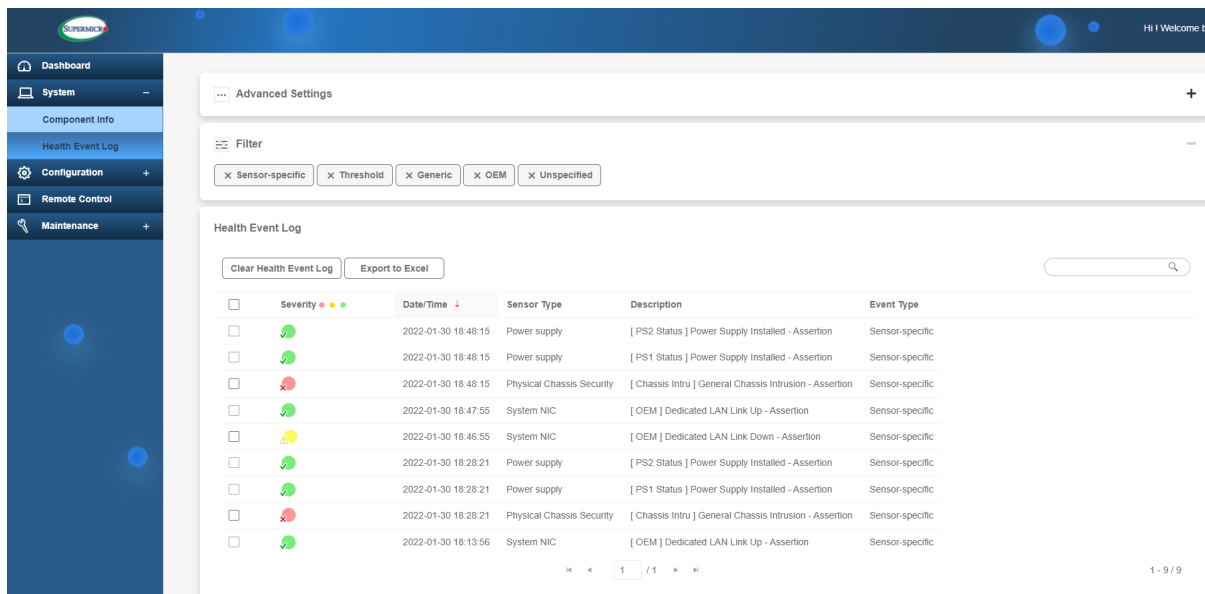
This page displays the following information.

- Operating State: Green is operating.
- Health Status: You can view the fan's health status.
- Name: You can view the indicated System Fan Number.
- RPM: You can view the indicated revolution per minute for each fan.
- Advanced Settings: You 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 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.

2.6.2 Health Event Log

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

 **Note:** By default, all event types will be selected so that you can view all events. You can apply filters for event selection based on event types (Supported event types: Sensor-Specific, Threshold, Generic, OEM, Unspecified). Currently, the number of Health Event logs is limited to 512.





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

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

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

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

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

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

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

You can apply the following administrator options.

- Export to Excel: You can use this option to export the current event log to an Excel file.
- Clear Health Event Log: You can use this to select all rows to clear the recorded event log.

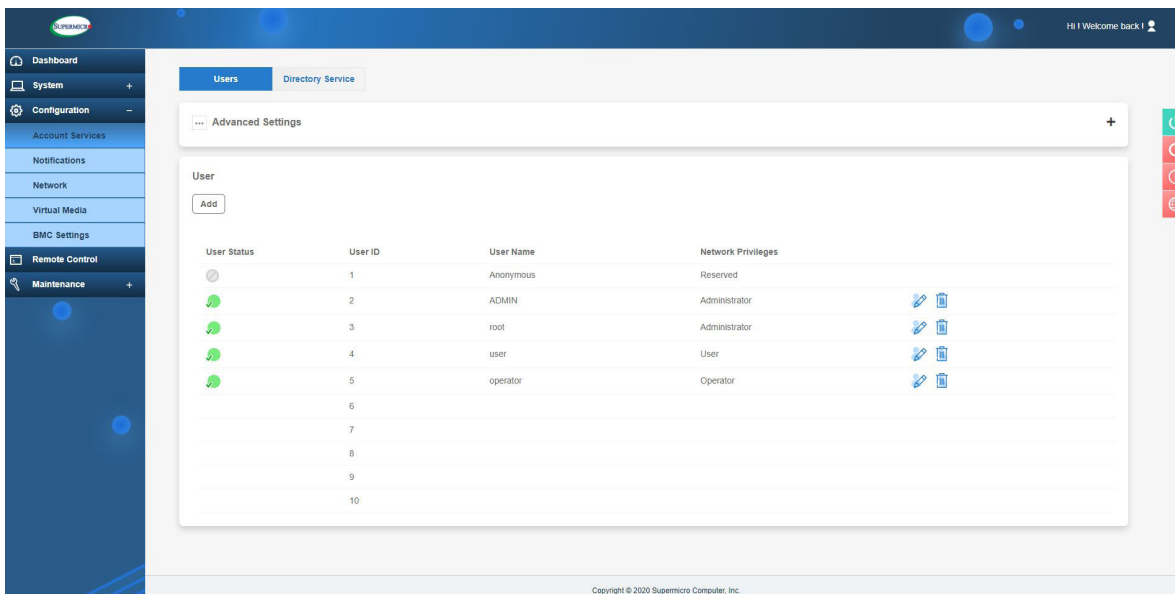
2.7 Configuration

This page allows you 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.



The screenshot shows the BMC User Management interface. On the left is a navigation menu with options like Dashboard, System, Configuration, Account Services, Notifications, Network, Virtual Media, BMC Settings, Remote Control, and Maintenance. The main content area is titled 'Users' and contains an 'Advanced Settings' section with an 'Add' button. Below this is a table of users with the following data:

User Status	User ID	User Name	Network Privileges
⊘	1	Anonymous	Reserved
●	2	ADMIN	Administrator
●	3	root	Administrator
●	4	user	User
●	5	operator	Operator
	6		
	7		
	8		
	9		
	10		

Each row in the table has edit and delete icons on the right side. The footer of the interface reads 'Copyright © 2020 Supermicro Computer, Inc.'

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

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

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

- Network Privilege: You can view one of the following types of privilege levels assigned to users.
 - Administrator
 - Operator
 - User
- Account Type
- Password Requirements
 - Password requires the length of 8 to 19 characters.
 - Password cannot be the reverse of the user name.
 - 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: You can click on the pencil icon to modify settings for the selected current user. When prompted, enter user name, password, and the network privilege level.
- Delete User: You can click on the trash can icon to delete the 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

You can perform the following actions to configure advanced settings.

- **Failed Login Lockout Control:** You 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. You can enable either LDAP, Active Directory, or RADIUS services. Please enable one directory service at a time.



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

The screenshot displays the 'Directory Service' configuration page in the BMC web interface. The left sidebar contains navigation options: Dashboard, System, Configuration, Account Services, Notifications, Network, Virtual Media, BMC Settings, Remote Control, and Maintenance. The main content area is titled 'Directory Service' and features a 'Setting' section with a dropdown menu to 'Select one directory service to enable'. Below this are three rows: LDAP, Active Directory, and RADIUS, each with an 'OFF' toggle and a '+' button. A yellow warning box says 'Please enable one directory service at a time!'. The footer shows 'Copyright © 2020 Supersica Computer, Inc.'

LDAP (Lightweight Directory Access Protocol)

This page allows you 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, your group IDs, group names, domains, and network privilege settings.

- Enable: You can enable LDAP authentication to allow you to access BMC.

 Enable LDAP authentication

 Disable LDAP authentication



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

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

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

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

Active Directory

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

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

 Enable AD authentication

 Disable AD authentication



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

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

RADIUS

This page allows you to view and configure RADIUS authentication.

- Enable: You can enable RADIUS authentication.

ON Enable RADIUS authentication

OFF Disable RADIUS authentication

- Secret Password: You can enter a secret password to access the RADIUS server.
- Server Address: You can add or edit the RADIUS server address.
 - IP or Domain – Enter the server IP or domain name.
 - Port – 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 (i.e. English letters and numbers) when entering data into the designated field. You will encounter expected errors when using Full-Width characters.

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

Alerts table will display the following information.

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

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

- Trap Community – You can fill in the info for traps.



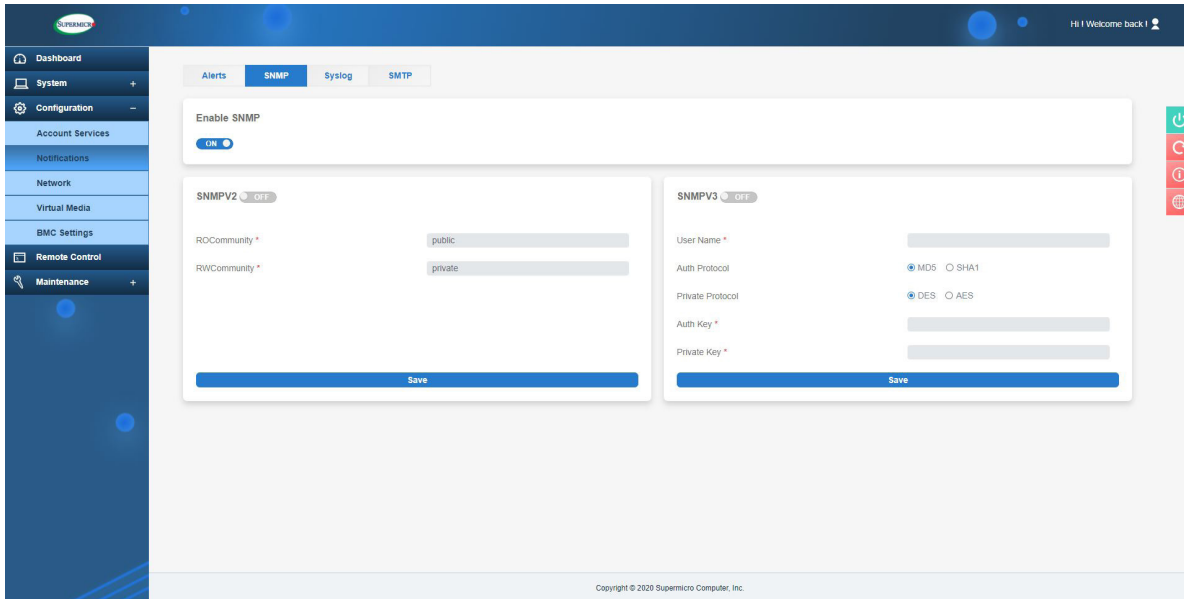
Note: This field is only displayed when SNMPv1 is selected.

- Delete: You can delete the respective alert.

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

SNMP

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



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

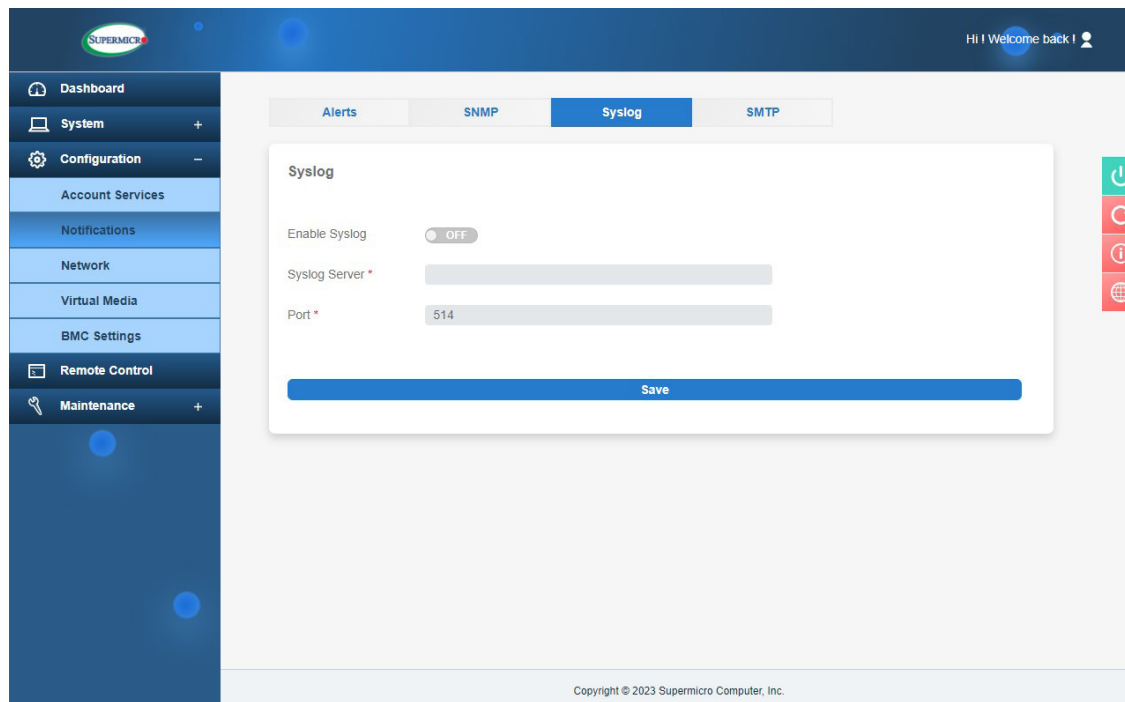
- Private Protocol – Encryption protocols. You can select one of the following private protocols.
 - None
 - DES
 - AES
 - Account.
3. Click the [Save]. The IPMI firmware will remember the settings and await your decision to start or stop the SNMP daemon.
 4. If you want to change the SNMP port number, 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**, you 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**.

Syslog

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

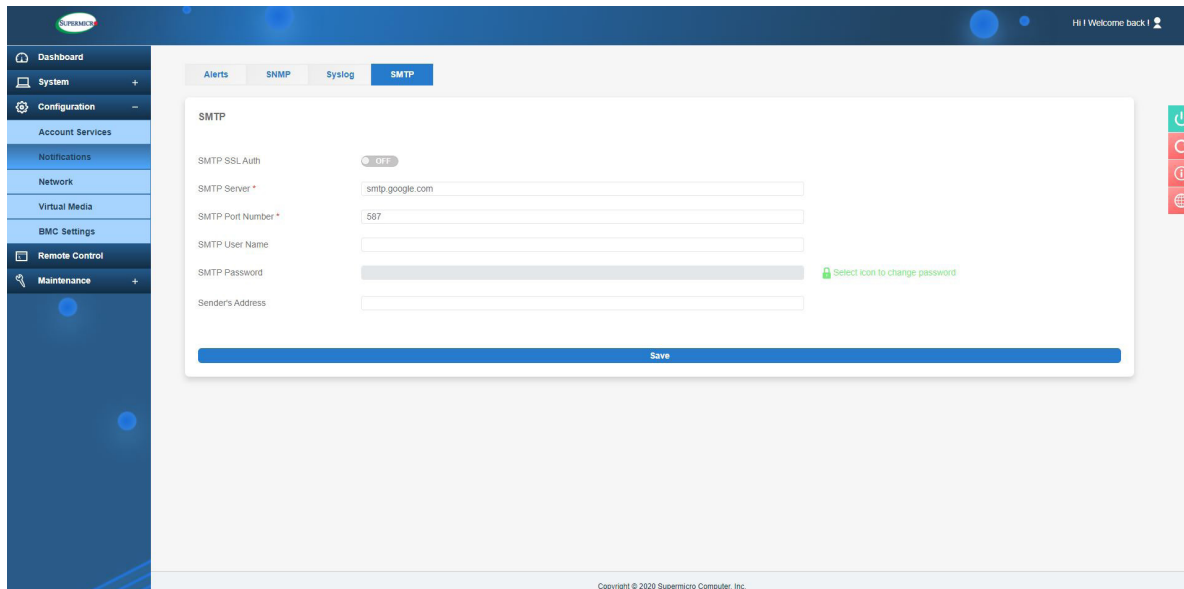


To configure the syslog settings, refer to the following steps.

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

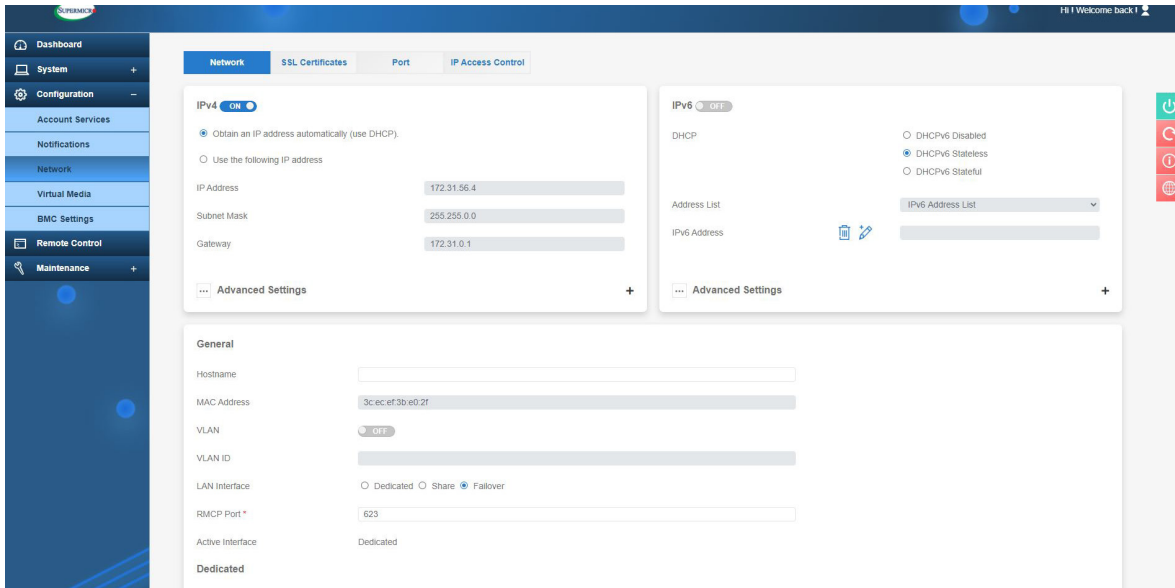


To configure SMTP settings, refer to the following steps.

1. Enable SMTP SSL Auth. Once enabled, you can configure the following information.
 - Server Address – You need to enter the address for the SMTP mail server to configure SMTP.
 - Port Number – You need to enter a SMTP port number.
 - Connection Protocol – You can choose one of the available protocols to set up SMTP authentication.
 - Authentication: You can choose one of the available Authentication methods to set up SMTP.
 - User Name – You have the option to enter the user name for the SMTP mail server (optional).
 - Password – You need to enter the password for the SMTP mail server.
 - Sender's Address – You 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: You can enable/disable the IPv4 network connection for BMC.
- Obtain an IP address automatically (use DHCP): You can select this option to configure an IPv4 address automatically by DHCP (Dynamic Host Configuration Protocol).
- Use the following IP address: You can select this option to set up a static IP address by entering the following details.
 - IP Address – Manual IPv4 address of BMC
 - Subnet Mask – IPv4 Subnet Mask Value
 - Gateway – IPv4 Gateway address

IPv4 Advanced Settings

DNS Server IP, DNS Server2 IP: You can enter a DNS Server IP to retrieve the hostname from DNS.

IPv6

- ON: You can enable/disable the IPv6 network connection for BMC.
- Disable: You can choose this option to disable the 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:
- Gateway IP:

You can take the following actions:

- Add – 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.



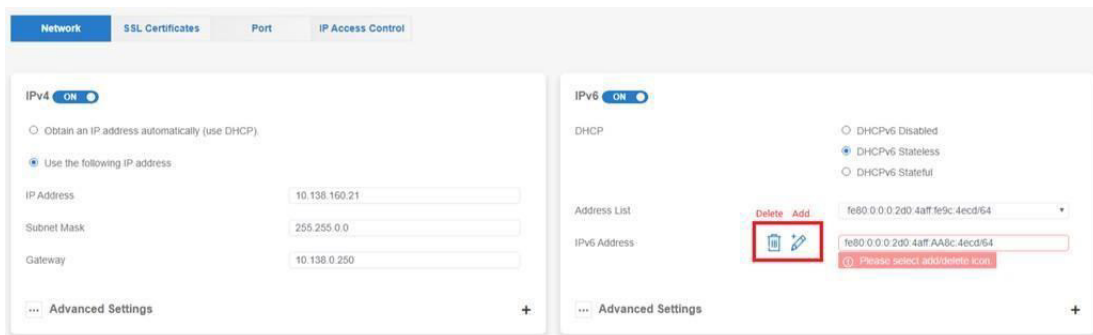
Note: Only Static IPv6 Address can be deleted.

- 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: You can select auto-configuration on or off.
- DNS Server IP: You can assign a DNS server IP address in the IPv6 form.
- DUID: You can use the Unit ID to get the DHCP IP from the DHCP server. The DUID includes client network information (address, lease time, and DNS server info). This is READ ONLY.
- Enable Static Route: When enabled, the route rules listed in Static Route List will be applied to the IPv6 routing table.
- Static Route List: You can view the static route list.

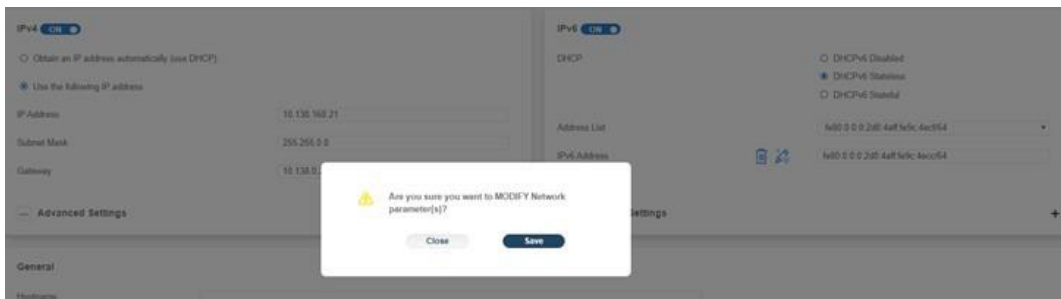
- **Prefix to Route:** You can input the prefix to route in this field. While there is an IPv6 packet whose destination address fits the Prefix to Route, the packet will be destined via the specific router which is defined in the Router Address field. Please note that the prefix length is required.
-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



Additional Reference Steps to Add/Delete IPv6 Address

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

1. Select add icon.

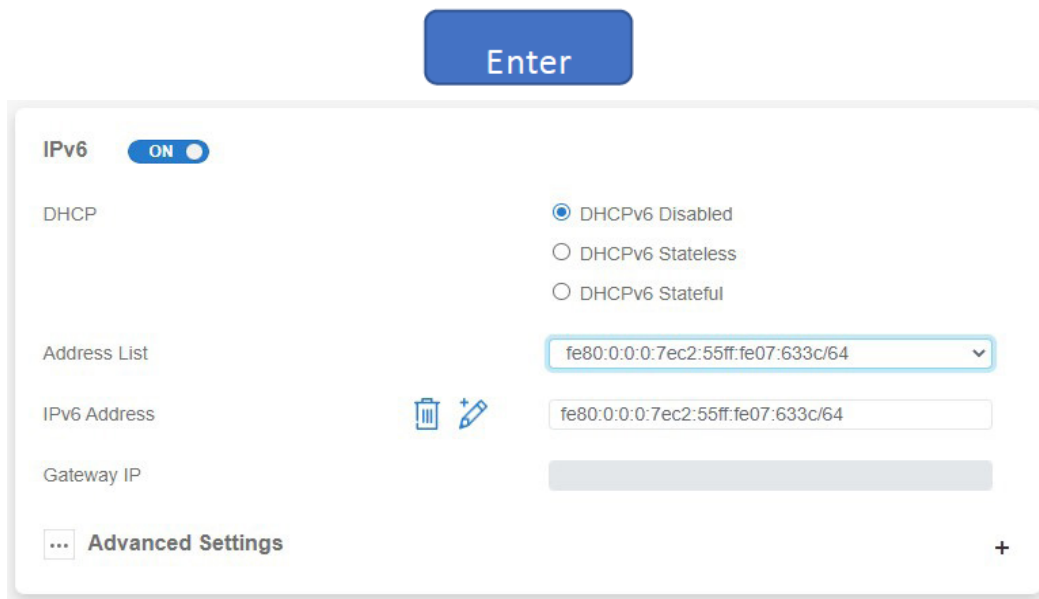


2. Input the address to be configured.

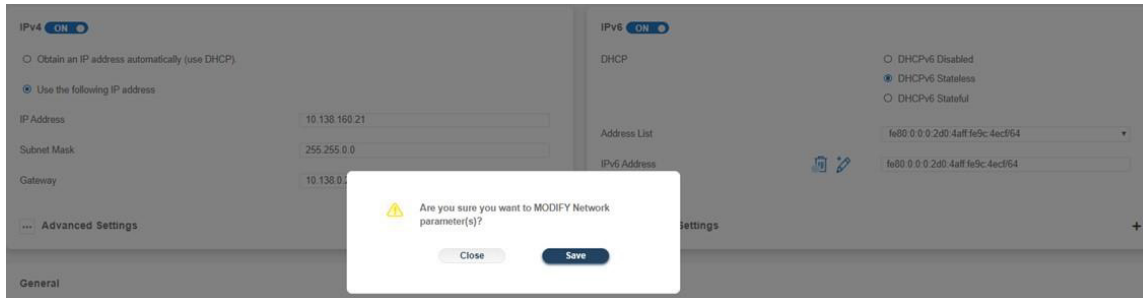


3. Save.

The updated address will appear on Address List.



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



1. Select add icon.



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

The updated address will appear on Address List.

General

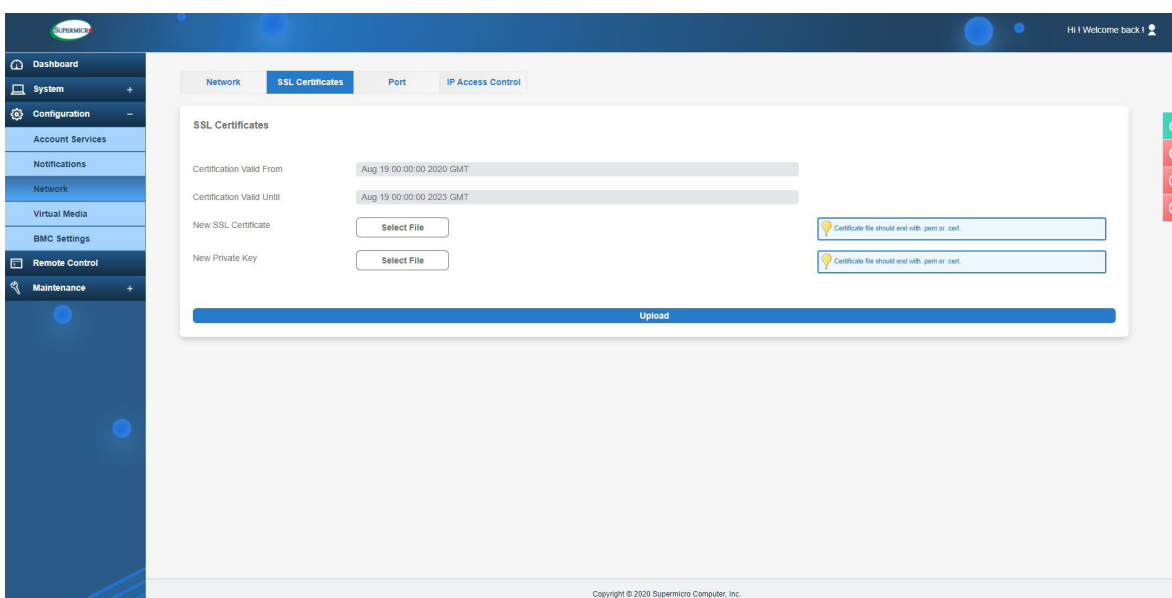
In this section, you can use and view the following features.

- Hostname: You can enter a name for the server as server identification.
- MAC Address: You can view the MAC Address of BMC.
- VLAN: You can enable/disable Virtual LAN support.
 - VLAN ID – Enter the VLAN ID.
- LAN Interface: You can select the type of LAN interface.
 - Shared
- RMCP Port: You can select the desired RMCP (Remote Mail Checking Protocol) port based on your configuration. The default port is 623.
- Active Interface: You can view the current type of LAN interface selected.
- Status: You can view the status of the BMC link.
- Speed: You can view the indicated speed of the system link connection.
- Duplex: You can view whether the BMC link is a full or half duplex.

SSL Certificates

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

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



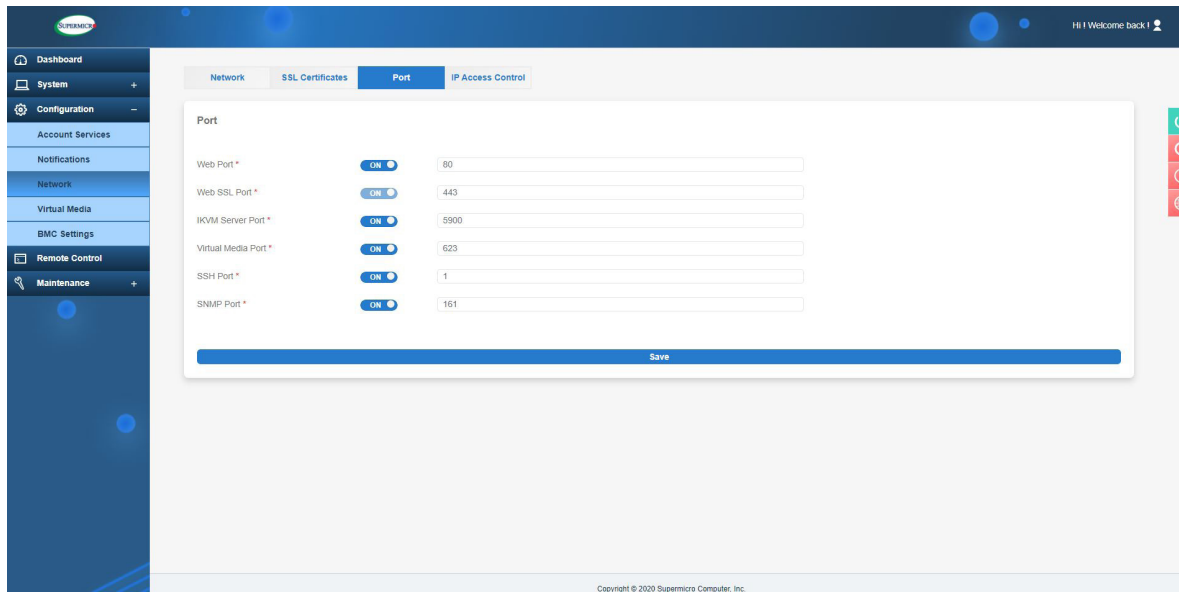
You can click [Upload] to upload the certificate and the private key to the server. Once uploaded, the BMC will reset itself for the new certificate to take effect.



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

Port


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



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

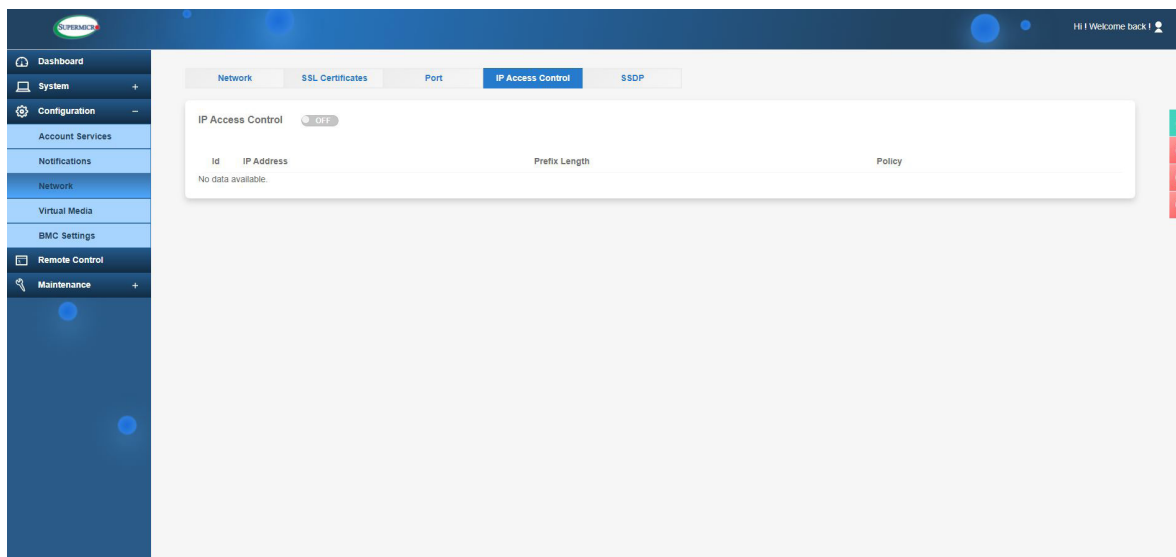
- Web Port: ON (80)
- Web SSL Port: ON (443)
- IKVM Server Port: ON (5900)
- Virtual Media Port: ON (623)
- SSH Port: ON (22)
- SNMP Port: OFF (161)

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



The access control list will include the following information.

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

You can adjust the following options.

- [Enable IP Access Control button]: You can click enable or disable IP access control features.
- [Add button]: You can select to add a new rule to the list.
- [Modify / Edit button]: You can select a policy and click to change its rule.
- [Delete button]: You 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 you set the same or different policy (ACCEPT/DROP) for the same IP Address with the same prefix. See the 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.

- You can still set the IP policy, but there will be a pop-up notification when the Save button is clicked.

The screenshot shows the IP Access Control interface with a warning message. The warning message reads: "The list of duplicate rules: Id: 1, 20.20.5.0/24 (Accept) Id: 2, 20.20.5.0/24 (Accept)". The interface includes an "Add" button, a table with columns "Id", "IP Access Control List", "Prefix Length", and "Policy", and a "Save" button.

Id	IP Access Control List	Prefix Length	Policy
1	20.20.5.0	24	Accept

The screenshot shows the IP Access Control interface with two duplicate rules. The interface includes an "Add" button, a table with columns "Id", "IP Access Control List", "Prefix Length", and "Policy", and a "Save" button.

Id	IP Access Control List	Prefix Length	Policy
1	20.20.5.0	24	Accept
2	20.20.5.0	24	Accept

Web UI follows ID #1

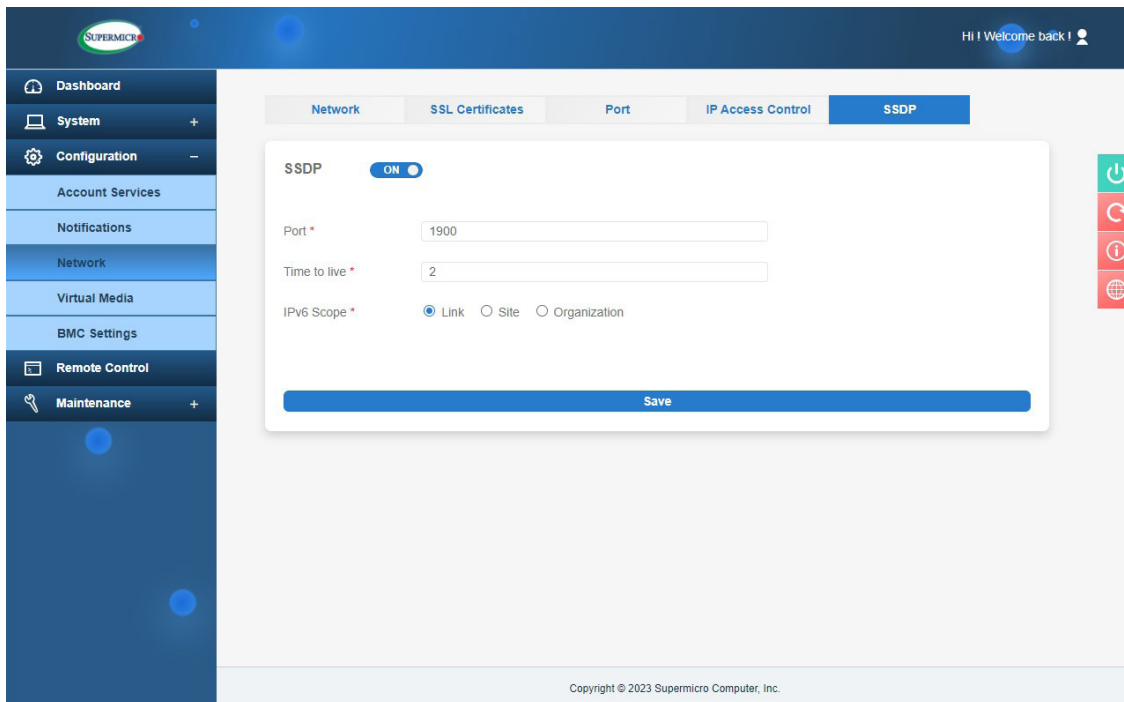


Id	IP Address	Prefix Length	Policy
1	20.20.5.0	24	Accept
2	20.20.0.0	16	Accept
3	20.0.0.0	8	Drop

The ID number notifies you when the IP access control is already set after you 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 your local network.



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

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

2.7.4 Virtual Media

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

Status

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

Floppy Disk

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

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

The screenshot displays the BMC Virtual Media interface. On the left is a navigation menu with options: Dashboard, System, Configuration, Account Services, Notifications, Network, Virtual Media (highlighted), BMC Settings, Remote Control, and Maintenance. The main content area is divided into three sections:

- Status:** A table with columns 'No', 'Health Status', and 'Connected Via'. It lists three devices: Device 1, Device 2, and Device 3.
- Floppy Disk:** A section for uploading a floppy image. It includes a 'Floppy Image File *' label, a 'Select File' button, and an 'Upload' button at the bottom.
- Virtual CD-ROM:** A section for mounting a virtual CD-ROM. It includes fields for 'Share Host *', 'Path to Image *', 'Users', and 'Password' (with a 'Select icon to change password' link). An 'Mount' button is at the bottom.

At the bottom of the interface, there is a copyright notice: 'Copyright © 2020 Supermicro Computer, Inc.'

Virtual CD-ROM

- **Share Host:** The host server for your console redirection. Share Host will only accept alphanumeric characters, dash, and periods (i.e. a-z, A-Z, 0-9, – and .) for the URL domain part. Moreover, the domain part will only accept http:// or https:// at the beginning of the string (i.e. HTTP+ IP Address, HTTPS + IP Address). Port numbers can be used after the IP Address as an option. For example: http(s):/192.188.8.8:443 for IPv4 Address and http(s)://[2021::8888:443].
- **Path to Image:** The path of the CD-ROM image file will only accept 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 you cannot use /, \, ^, and \\. Path must be started with / or * character and ends with “.iso” file extension.

- **Users:** If you have access to the CD-ROM image files, you will only be able to input the following accepted 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
 - ^

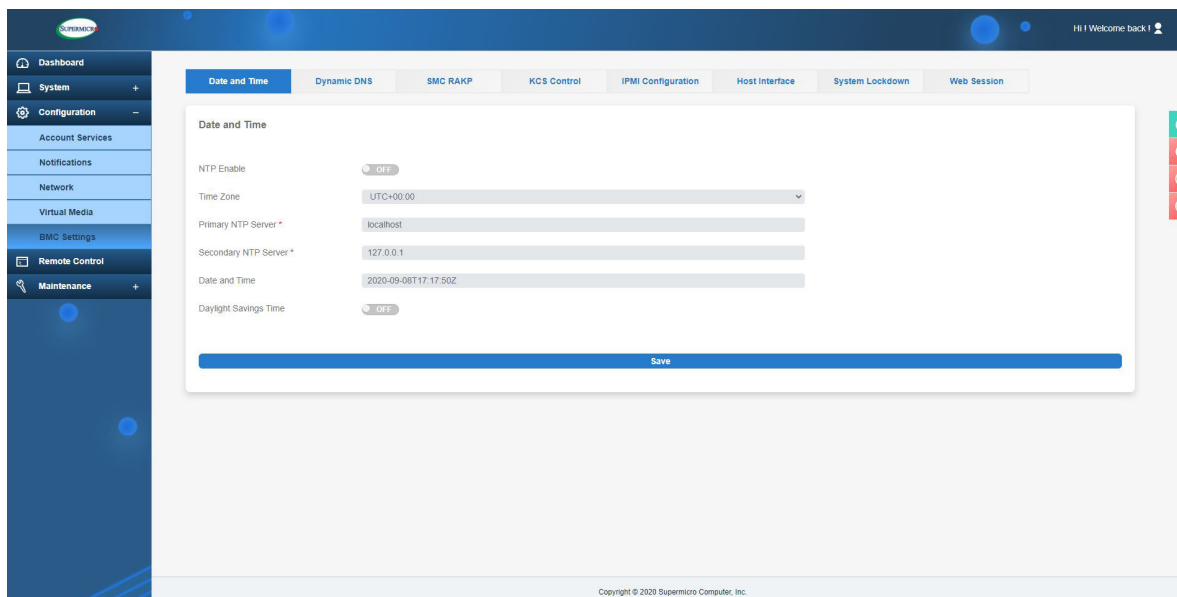


Note: CD-ROM mounting supports HTTP, HTTPS, Samba, and the Windows CIFS method.

2.7.5 BMC Settings


Date and Time

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




You can adjust the following fields.

- **NTP Enable:** You can enable or disable NTP server settings. If NTP is disabled, the system time is used to set the date and time. If NTP is enabled, the NTP server is used to set the date and time. However, before BMC successfully gets the date and time from 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, they will sync with system time (from BIOS) upon a system reboot when NTP is then set to disable.

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

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

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

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

Dynamic DNS

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



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

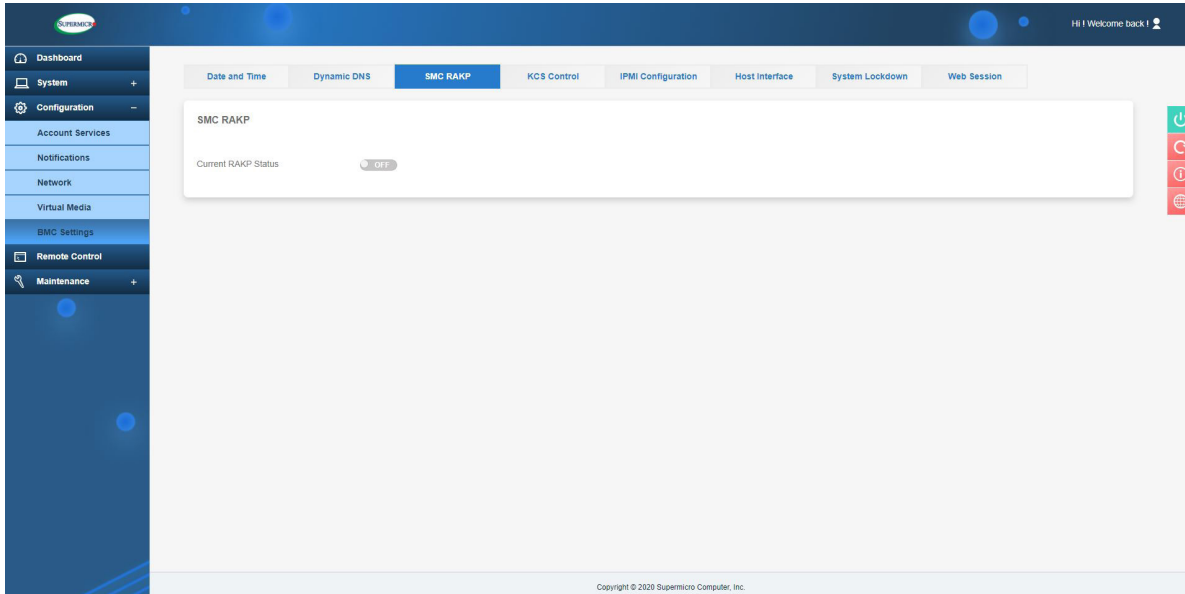
- Dynamic Update Enable: You can enable/disable Dynamic DNS (Domain Name System) update support.
- Dynamic DNS Server Address: You can view the server address of your Dynamic DNS server.
- BMC Hostname: You can name the BMC (Baseboard Management Controller) Host Server.
- Enable TSIG Authentication: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



Note: Fields with * are optional.

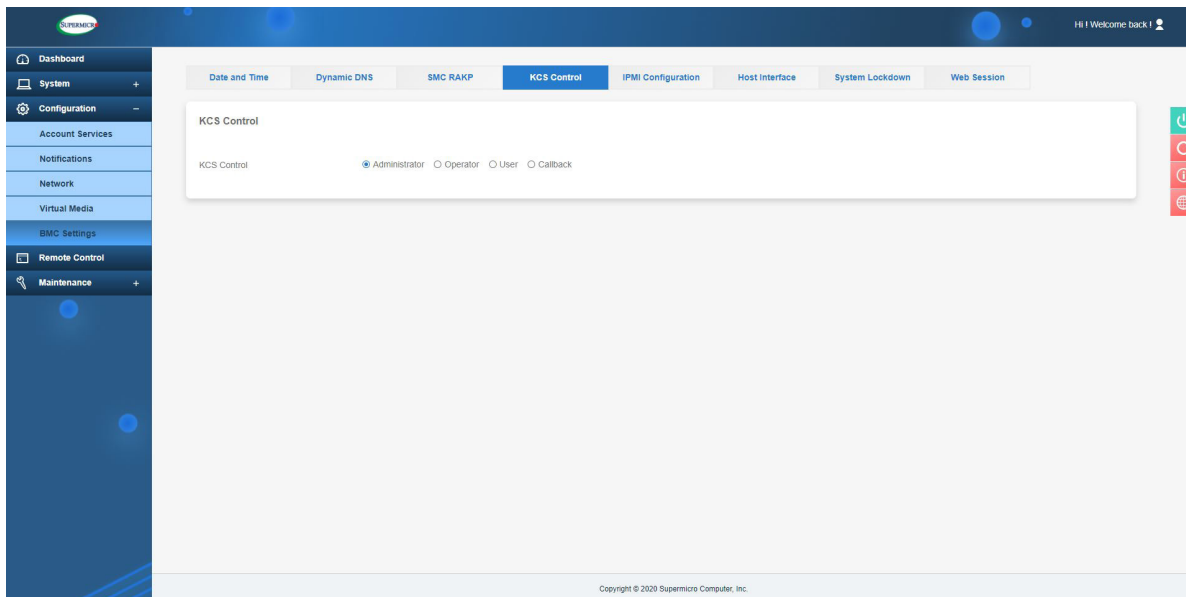
SMC RAKP

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



KCS Control

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




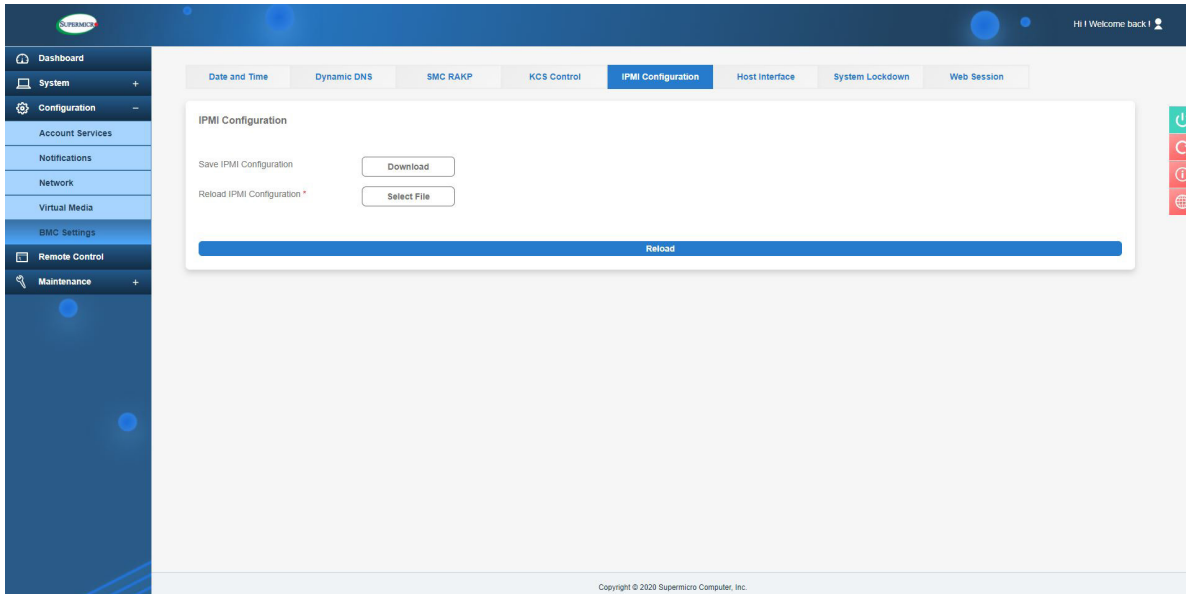
You can select one of the following options to determine who is allowed what supported privilege.

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

IPMI Configuration

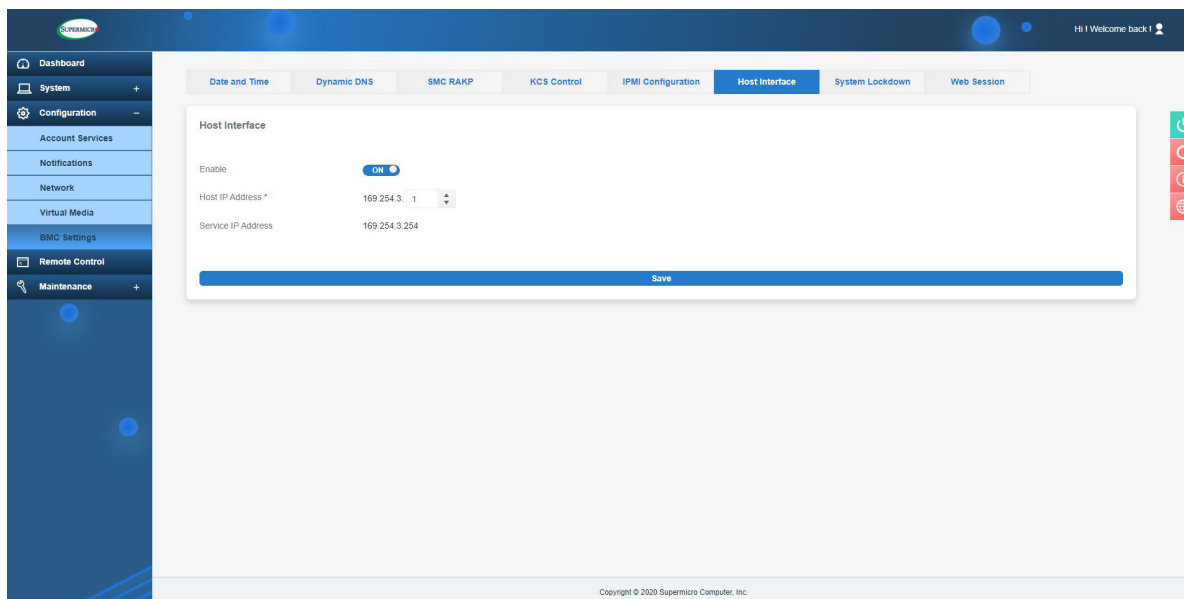
You can use this page to save or restore IPMI configuration settings.

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



Host Interface

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



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

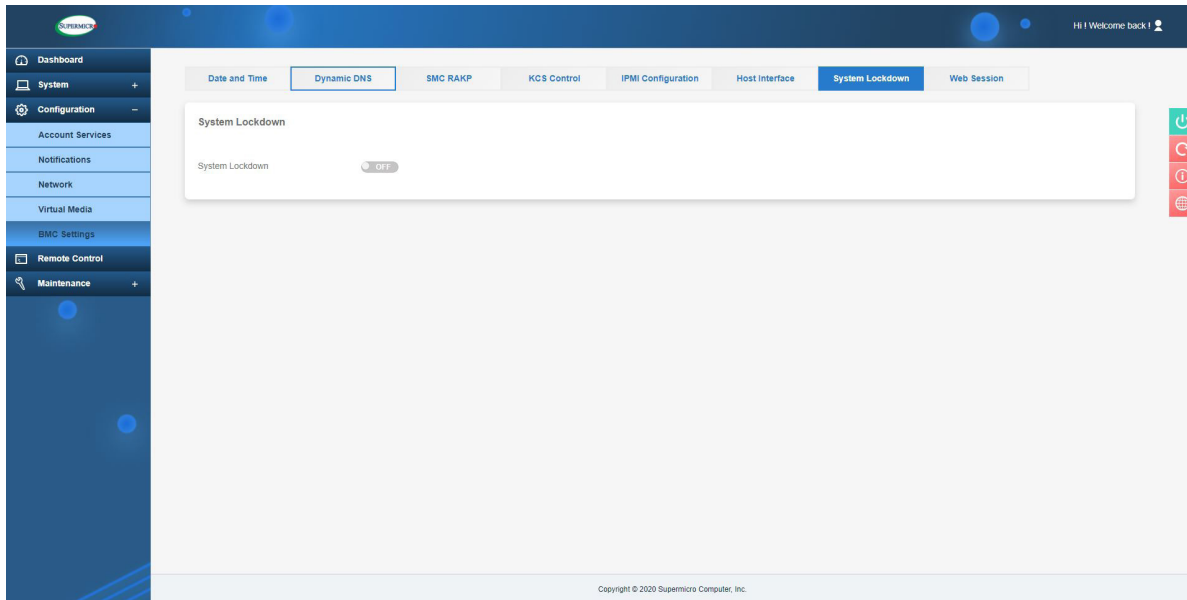
- Enable: You can enable/disable this service.
- Host IP Address: You can set up a host IP address that is assigned to the host OS.
- Service IP Address: You can view the management host interface service IP. This is READ ONLY.

System Lockdown

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



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

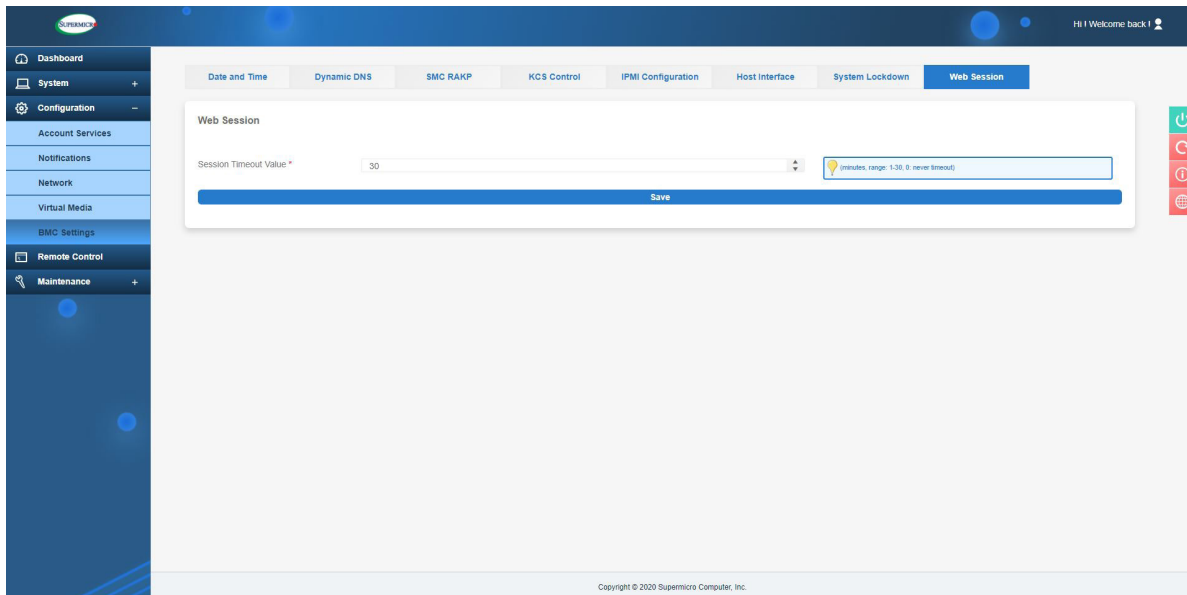


The following features will be functional during the system lockdown.

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

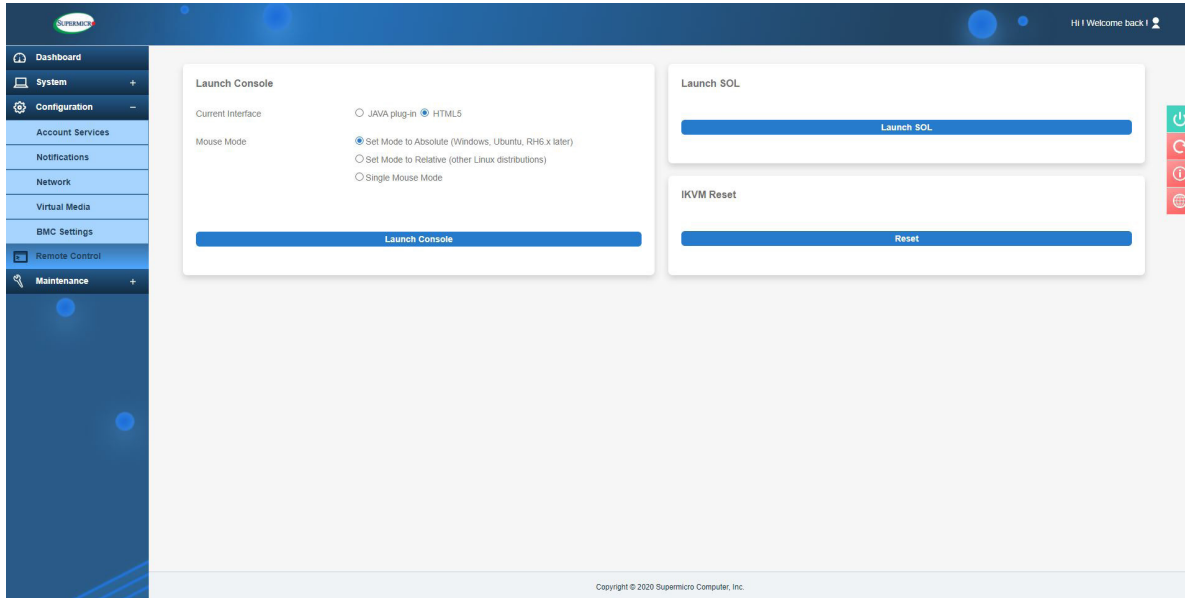
Web Session

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



2.8 Remote Control

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



Launch Console


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

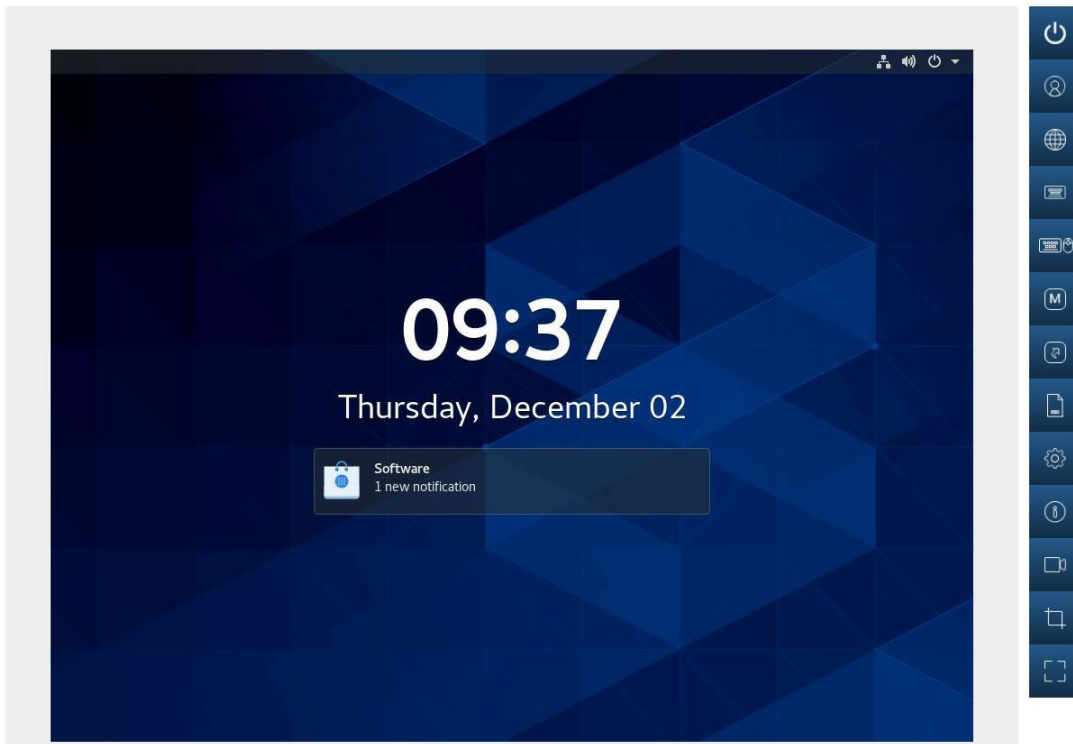
To launch a remote console via Java or Active X (for Internet Explorer), refer to the following steps.

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

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

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


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



Mouse Mode

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

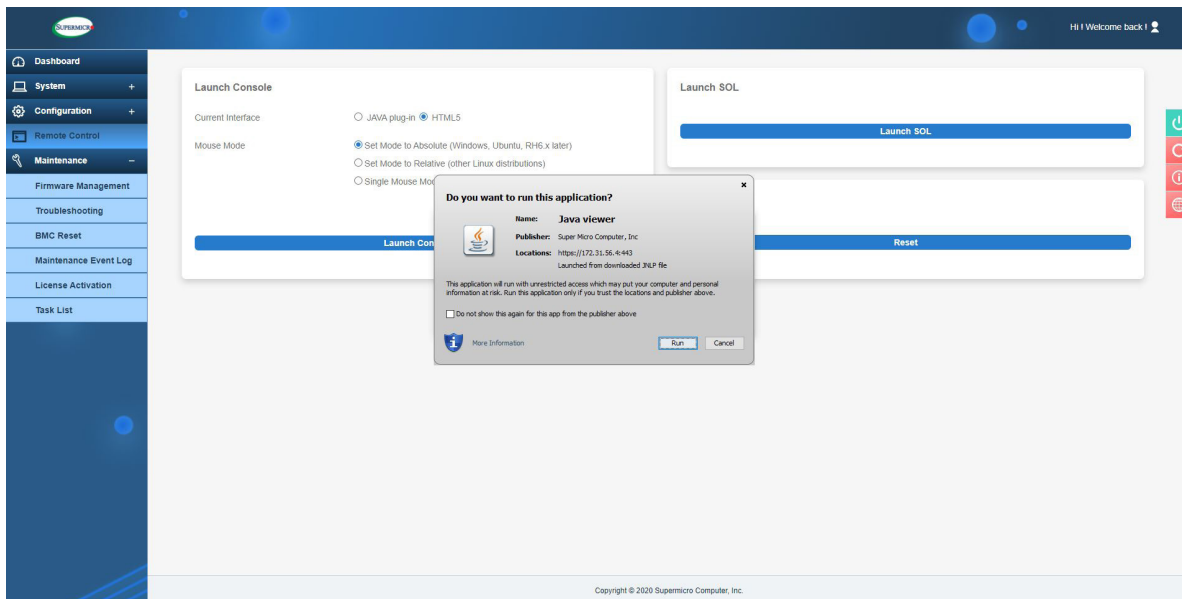
- Select Absolute Mode for Windows, Ubuntu, and RH6.x later.
- Select Relative Mode for other Linux/Unix distributions.
- Select Single Mouse Mode to use single mouse mode.

 **Note:** IPMI is an OS-independent platform and iKVM support is an add-on feature of 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

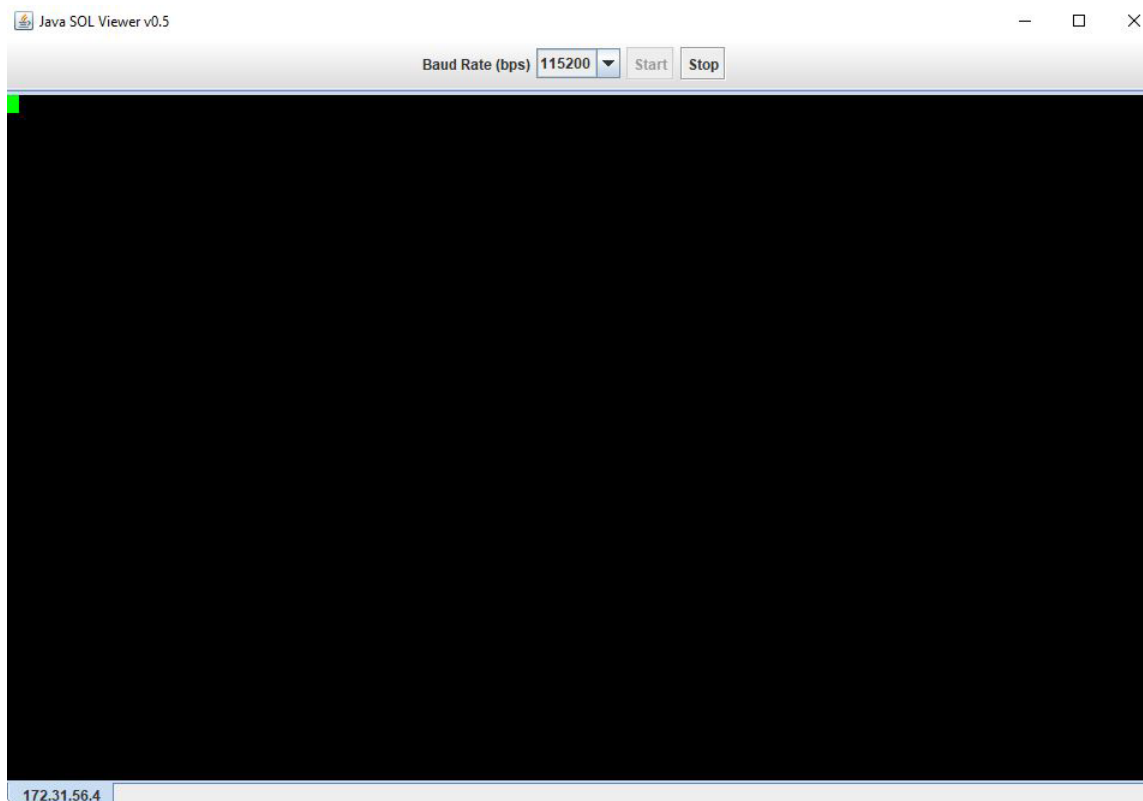
This page allows you to launch a remote console using SOL (Serial over LAN), which provides serial port connections over LAN to access a host server via console redirection. It also allows the system administrator to monitor and manage servers from a remote site. In order to connect the console through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

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



To launch the 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 you have reached the Java SOL viewer, the following options are available.

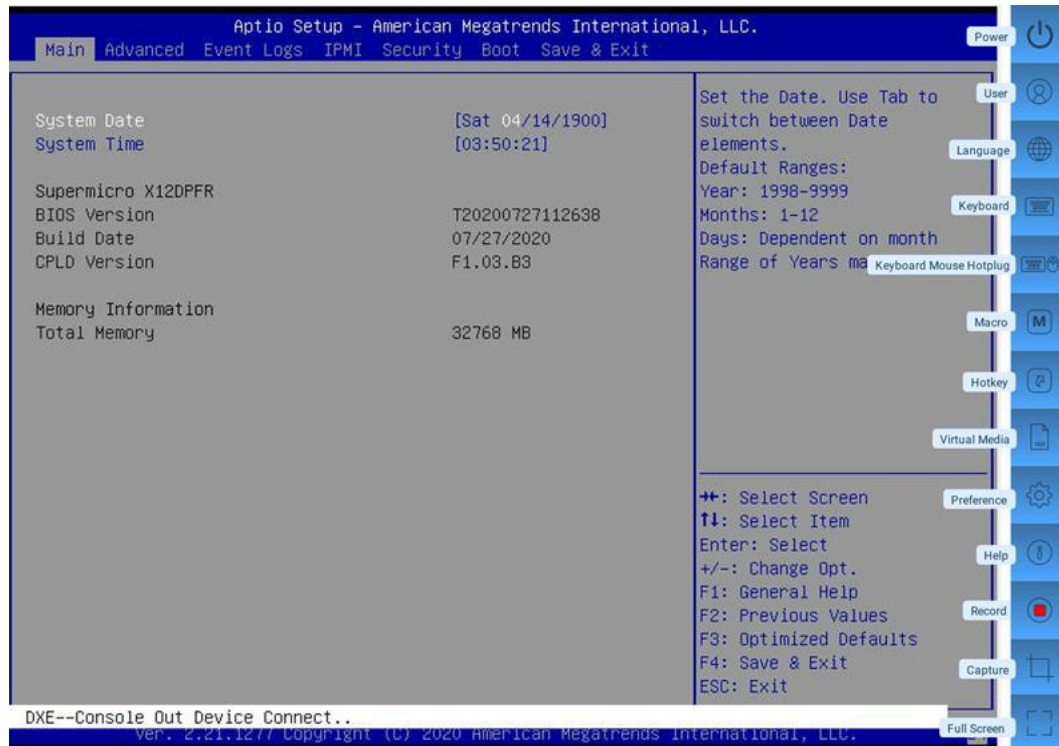
- Baud rate (bps): You can select one of the following SOL transfer rates from the pull-down menu. Make sure that the baud rate selected matches the baud rate set in the UEFI BIOS.
 - 9600 bps (bits per second)
 - 19200 bps
 - 38400 bps
 - 57600 bps
 - 115200 bps
- Start: You can start the session after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

iKVM Reset

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

2.8.1 Console Redirection

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



Click [Help] for further assistance if needed.

2.8.1a Console Redirection – Power

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

Power Control

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



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

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

2.8.1b 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 you to configure the language setting and select one of the following support languages.

Language Setting

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

Close

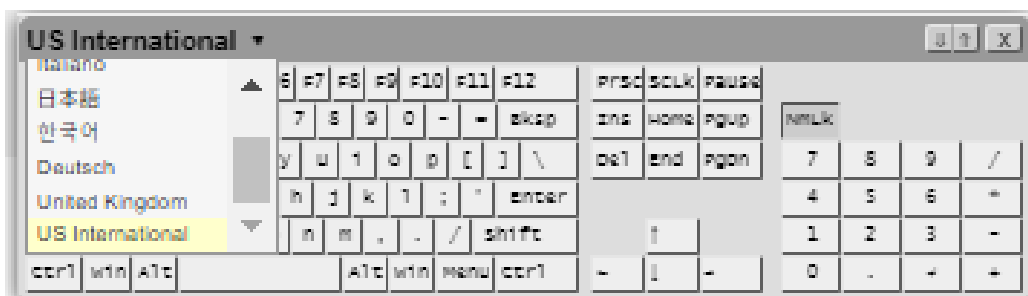
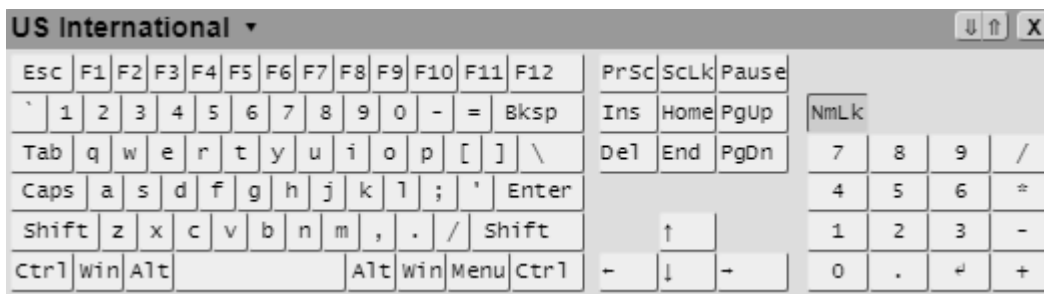
Apply

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

2.8.1d Console Redirection – Keyboard

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

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




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



Note: JAVA-iKVM virtual keyboard's language will be using a US-international virtual keyboard regardless of whether any of the supported languages are set. Please also note that due to language differences in size and shape, the sizes of supported virtual keyboards will be varied. Thus, will not be the same.

2.8.1e Console Redirection – Keyboard Mouse Hotplug

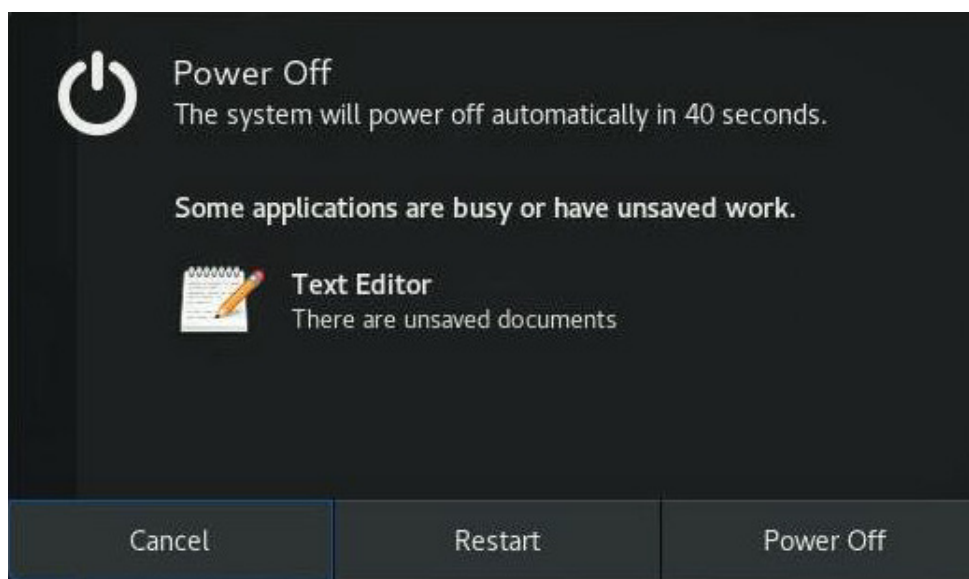
This option allows you to hot-plug the server-side Keyboard and Mouse devices using the Hotplug icon.

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

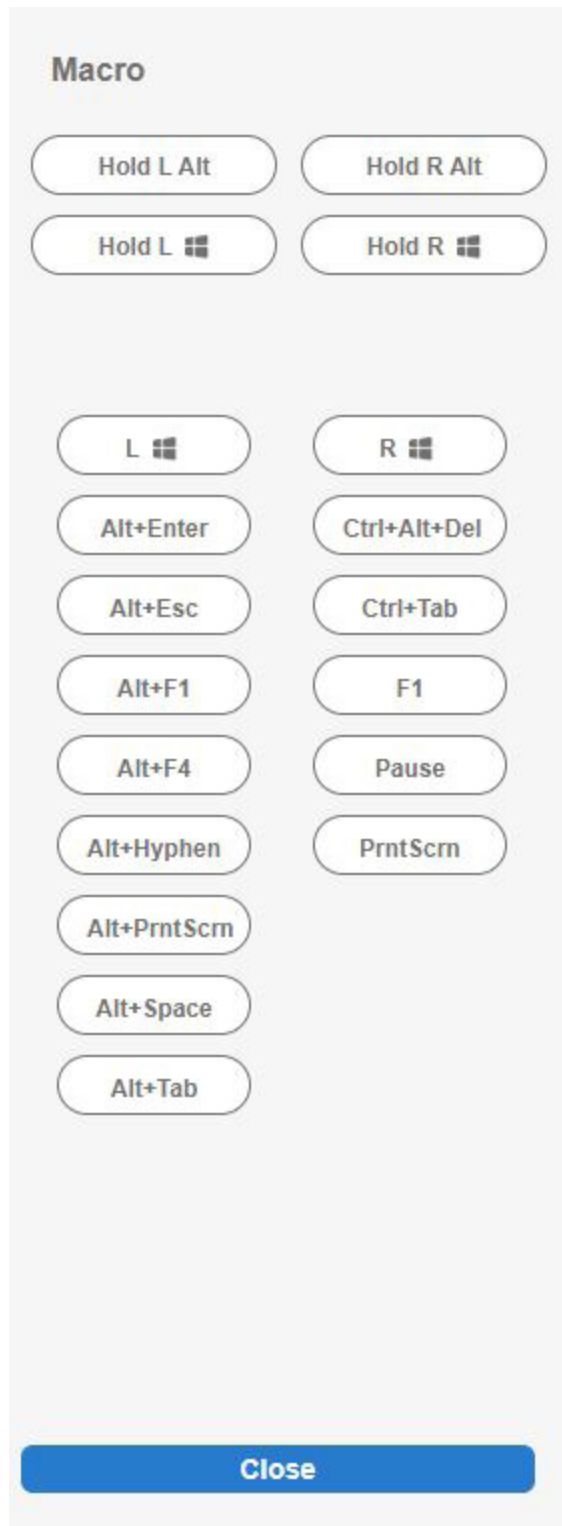
2.8.1f Console Redirection – Macro

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

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



Example of pressing *Ctrl+Alt+Del*




Macro UI

2.8.1g Console Redirection – Hotkey

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

Hotkey Settings

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

Close

Default











The following display options are available.


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

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

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











Hotkey Settings


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

 Please enter a valid shortcut.

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

Hotkey Settings

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

 New shortcut key has been assigned successfully!


[Close](#)

[Default](#)


2.8.1h Console Redirection – Virtual Media


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

● Device 1 ○ Device 2 ○ Device 3

 No disk emulation set.

Select Device Type

 ISO Image

 IMG/IMA Image

Select File

Display Input Video Stream Control Record

Display Scale

60% 70% 80% 90% 100%

Image Quality

Low Medium High

2.8.1i Console Redirection – Preference

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

Console Redirection – Display

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

Display	Input	Video Stream Control	Record
Display Scale			
<input type="radio"/> 60% <input type="radio"/> 70% <input type="radio"/> 80% <input type="radio"/> 90% <input checked="" type="radio"/> 100%			
Image Quality			
<input type="radio"/> Low <input checked="" type="radio"/> Medium <input type="radio"/> High			
Close			

Console Redirection – Input

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

Display	Input	Video Stream Control	Record
Mouse Settings			
<input checked="" type="radio"/> Absolute Mouse (Windows, Ubuntu, RHEL 6.x and later)			
<input type="radio"/> Relative Mouse (Other Linux distributions)			
<input type="radio"/> Single Mouse			
Close			

Console Redirection – Video Stream Control

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

Display
Input
Video Stream Control
Record

LAN Flow Control

256K Cable/DSL(Default)

T1

T2

Close

Console Redirection – Record

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



Note: Video Recording only works with the Chrome browser.

Display
Input
Video Stream Control
Record

Recording Time

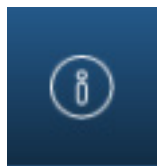
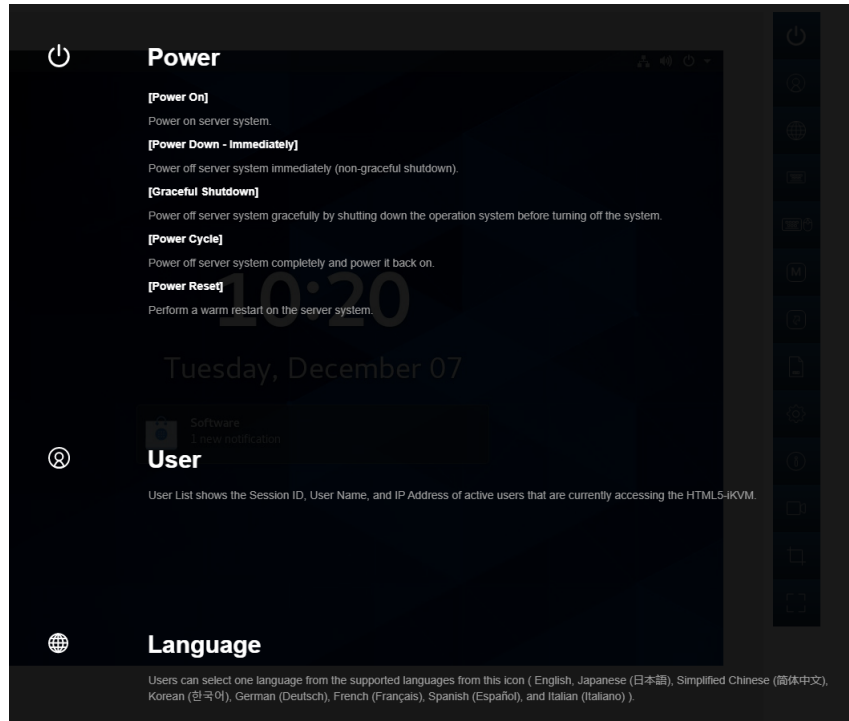
ON Enable auto stop after minute(s)

New settings will take effect in next recording.

Close

2.8.1j Console Redirection – Help

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



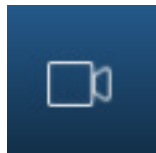
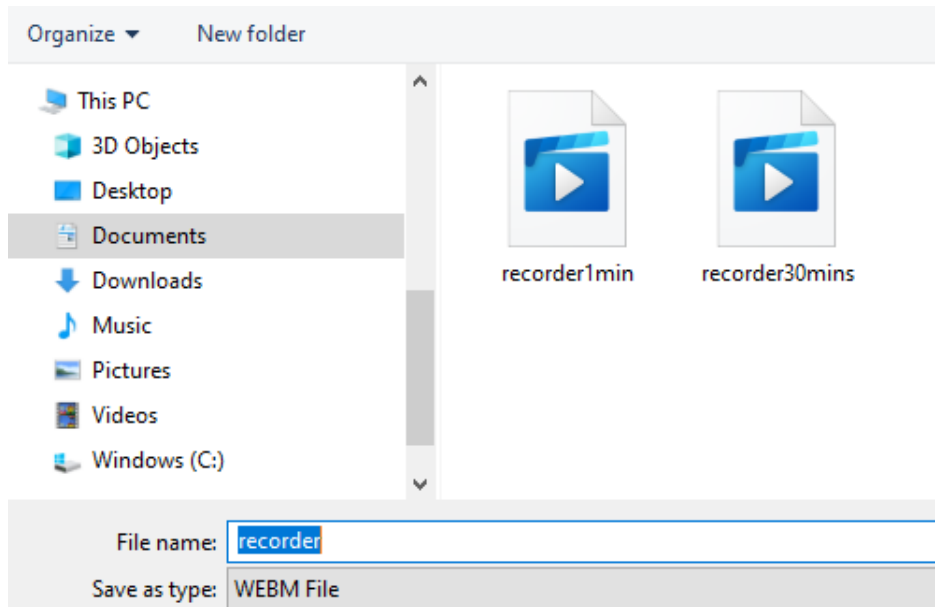
Help Icon

2.8.1k Console Redirection – Record

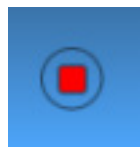
Use this feature to record Video during BIOS booting. After you press the Record button and then the Stop button, the recording will be available to be saved as shown below.



Note: Video recording only works with the Chrome browser.



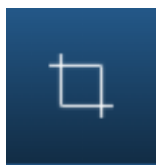
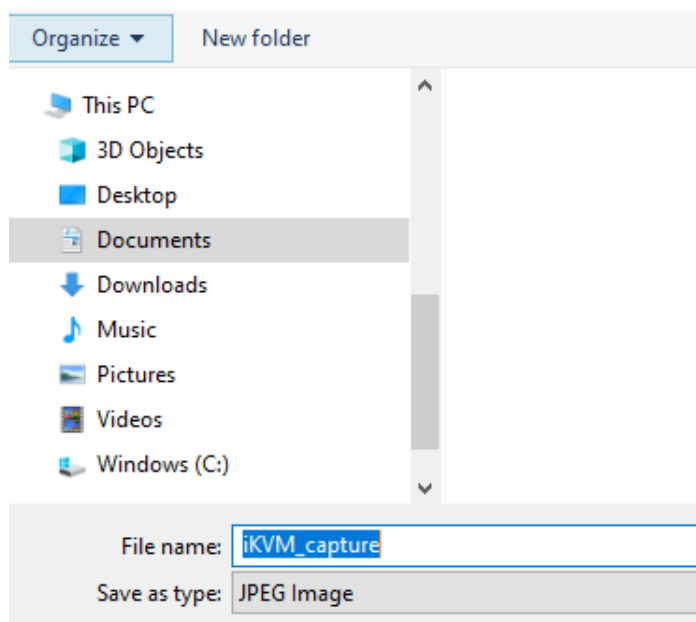
Record Icon



Stop (Recording) Icon

2.8.1l Console Redirection – Capture

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



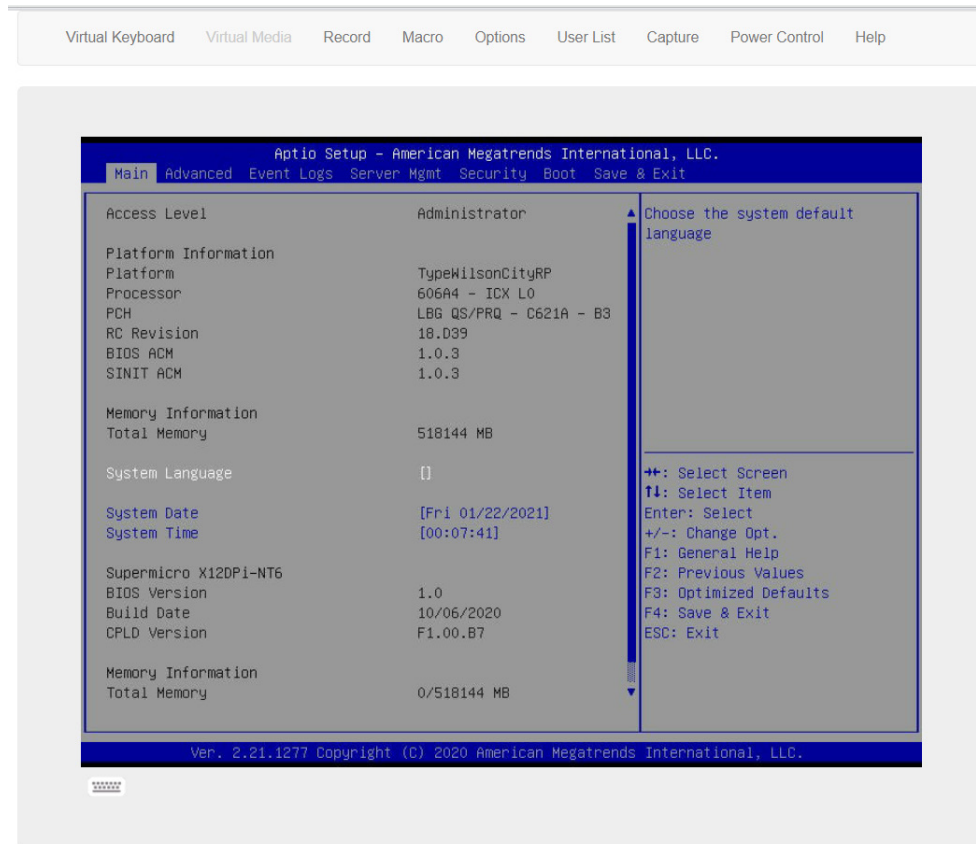
Capture Icon

2.8.1m Console Redirection – Full-Screen

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

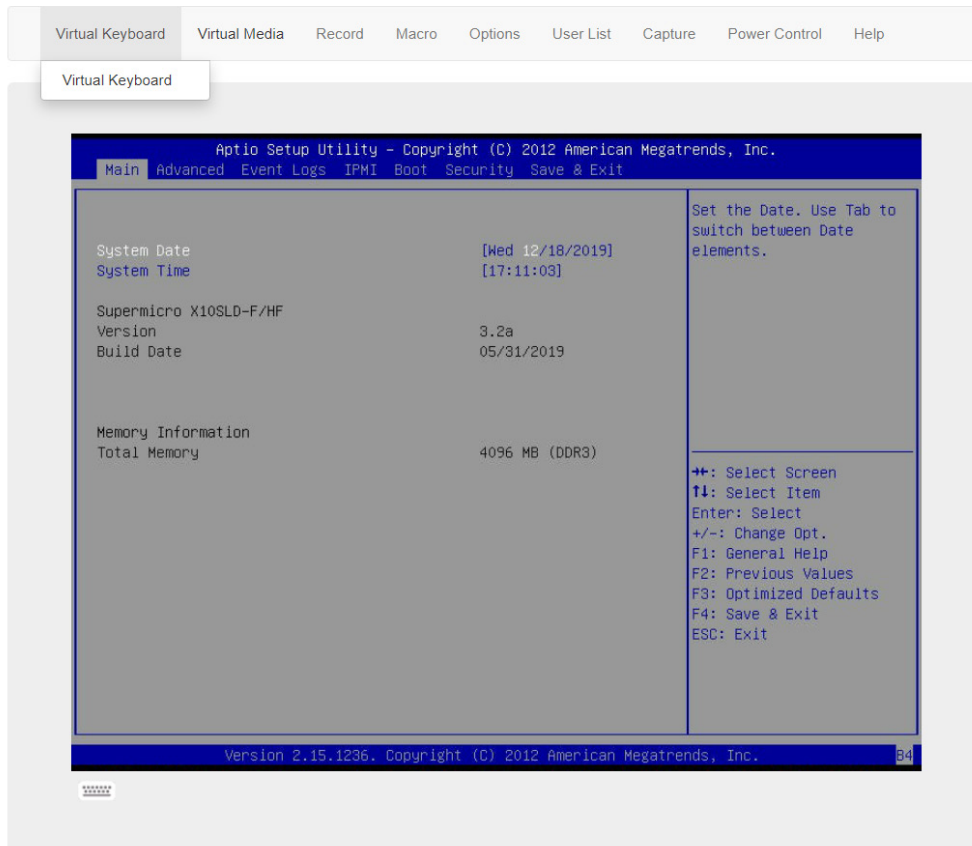
2.8.2 iKVM/HTML5

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

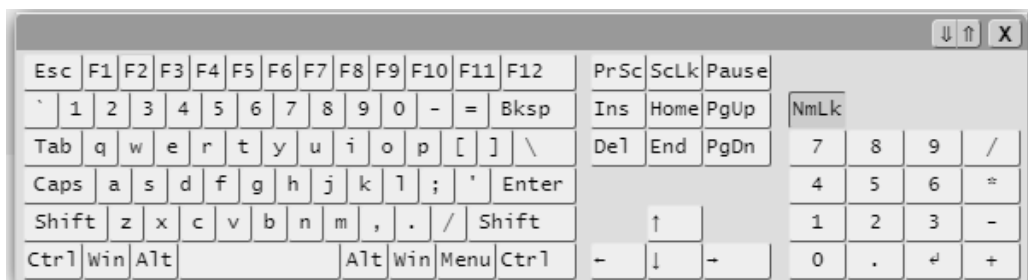


2.8.2a iKVM/HTML5 – Virtual Keyboard

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



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



2.8.2b iKVM/HTML5 – Virtual Media

This feature allows you to upload and share images via the SSE-T7132 BMC (Baseboard Management Controller). These images will be emulated to the host server as USB applications. You need to first activate a Super Micro Software License to enable this feature.

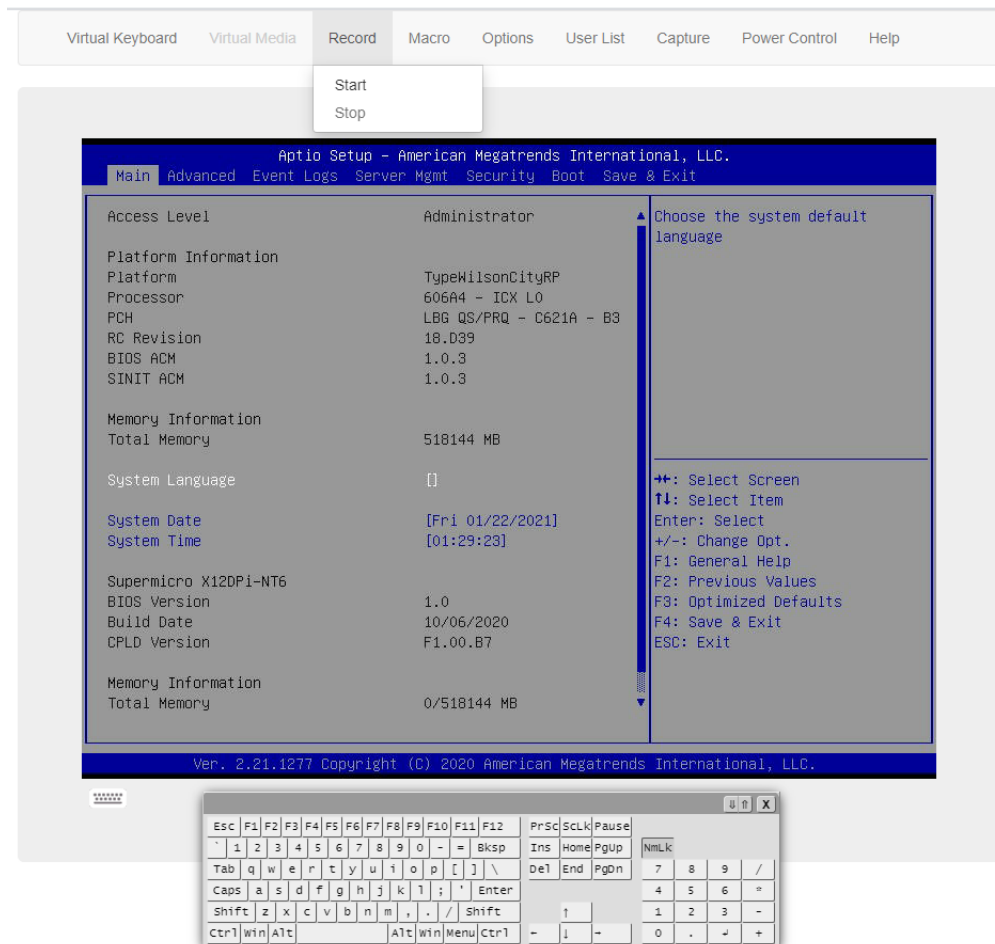
2.8.2c iKVM/HTML5 – Record

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

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



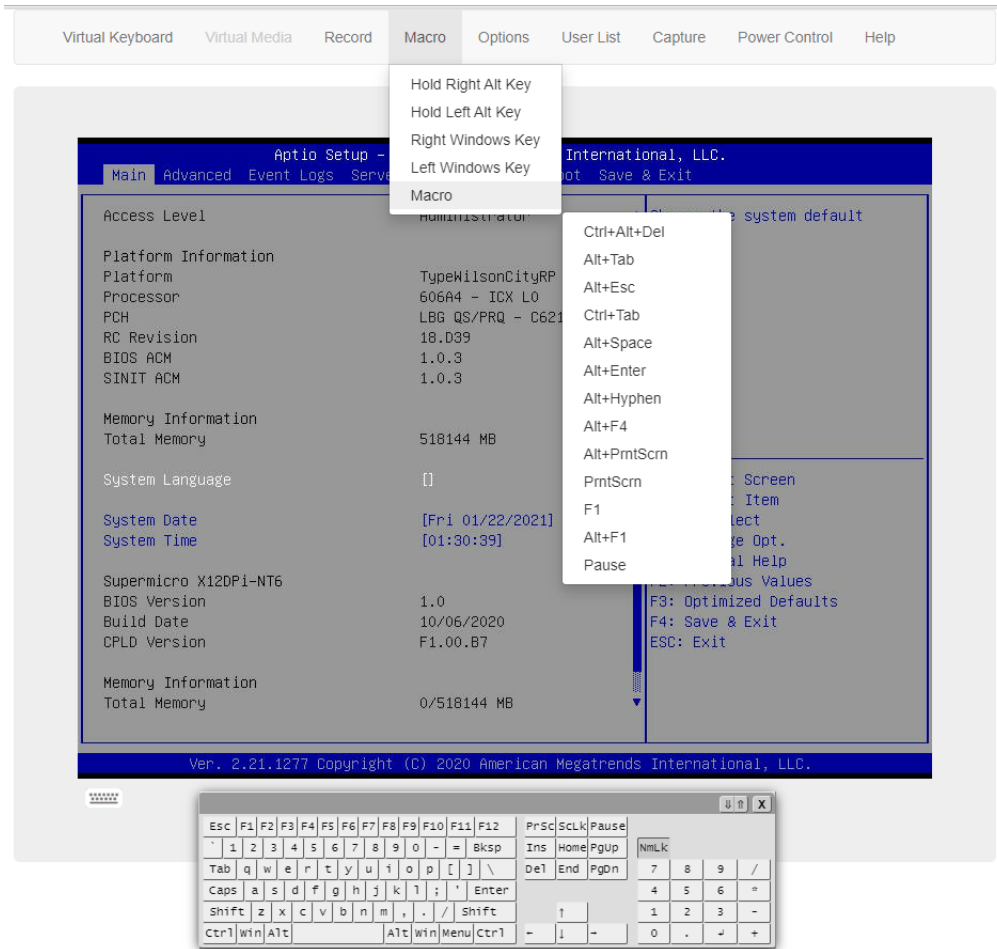
Note: This new HTML5 implementation is currently only supported by the Chrome browser.



2.8.2d iKVM/HTML5 – Macro

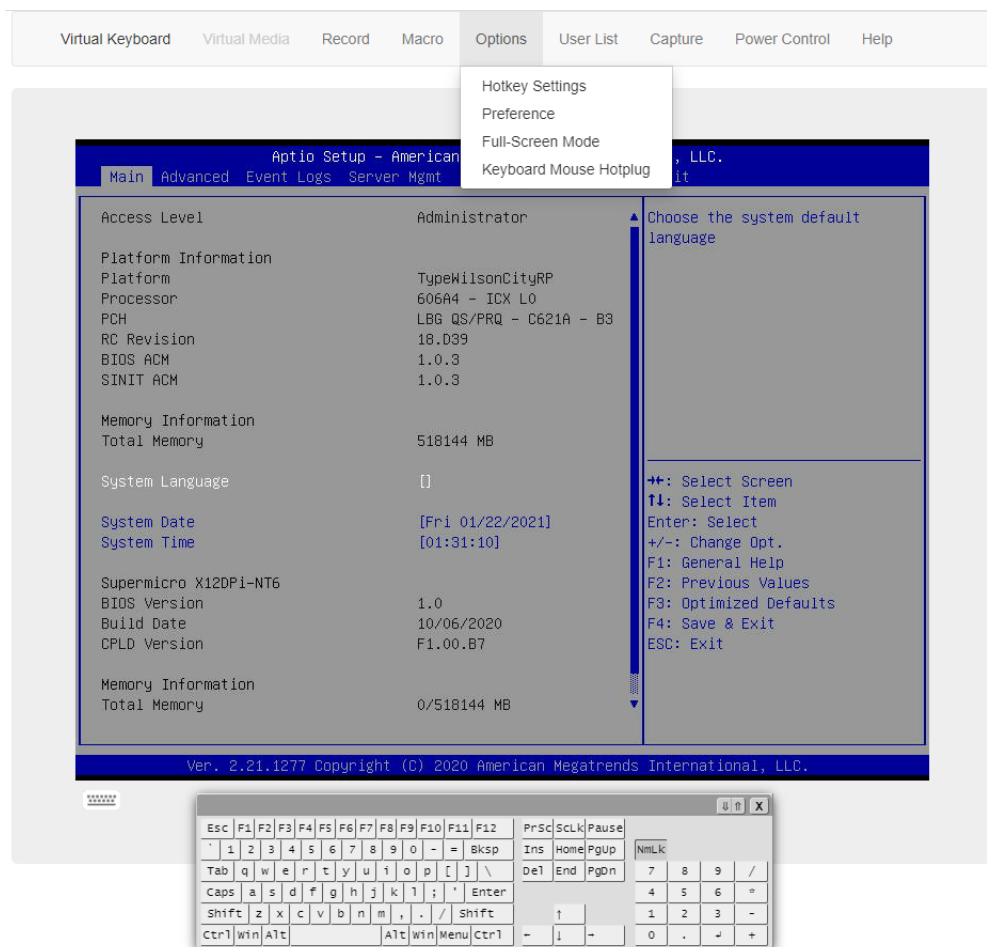
This feature allows you quick access to combo keys.

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



2.8.2e iKVM/HTML5 – Options

This feature provides hotkeys for the following functions.



- Adjust Mouse
- Exit Remote Location
- Full-Screen Mode
- Refresh screen
- Send Ctrl+Alt+Del
- Toggle Mouse Display
- Toggle UI Display

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

Hotkey Settings

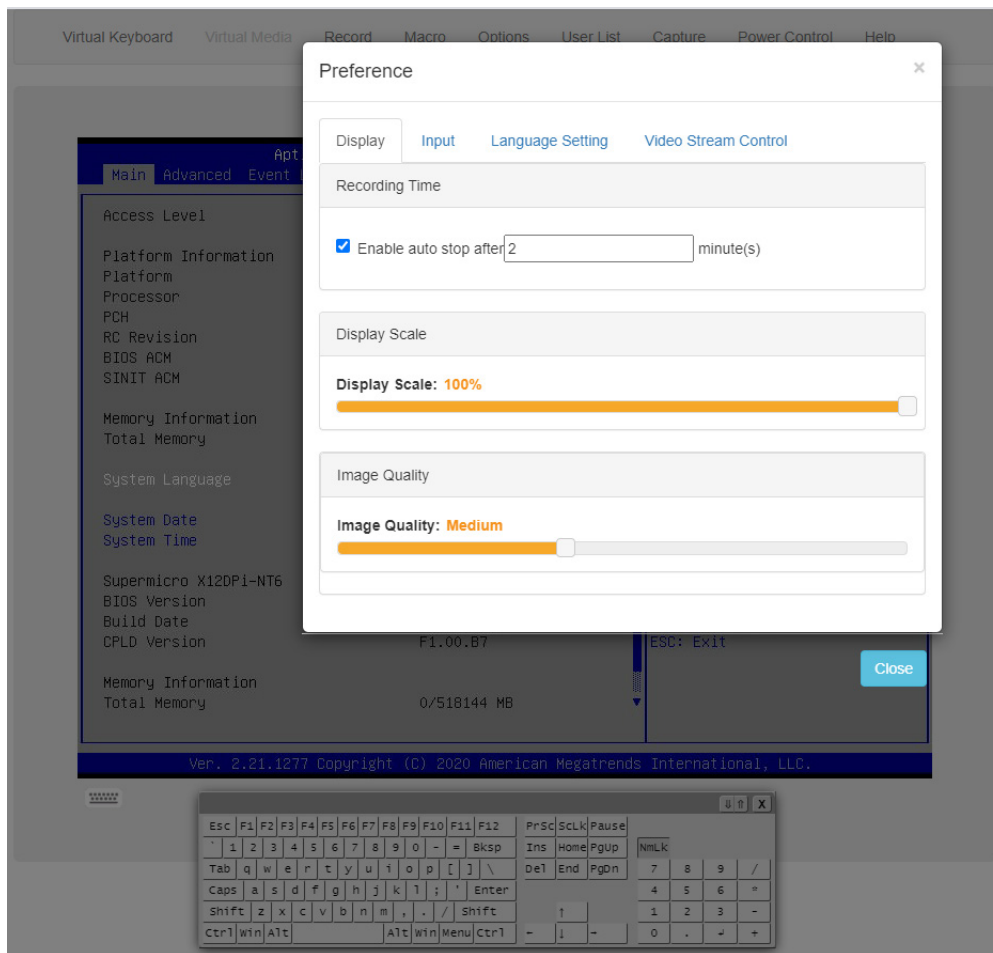
Display	Hotkeys	
Adjust Mouse	Ctrl+Shift+F2	 
Exit Remote Location	Ctrl+Shift+F3	 
Refresh Screen	Ctrl+Shift+F4	 
Send Ctrl+Alt+Del	Ctrl+Shift+F5	 
Toggle Mouse Display	Ctrl+Shift+F6	 

Close

Default

Preference – Display

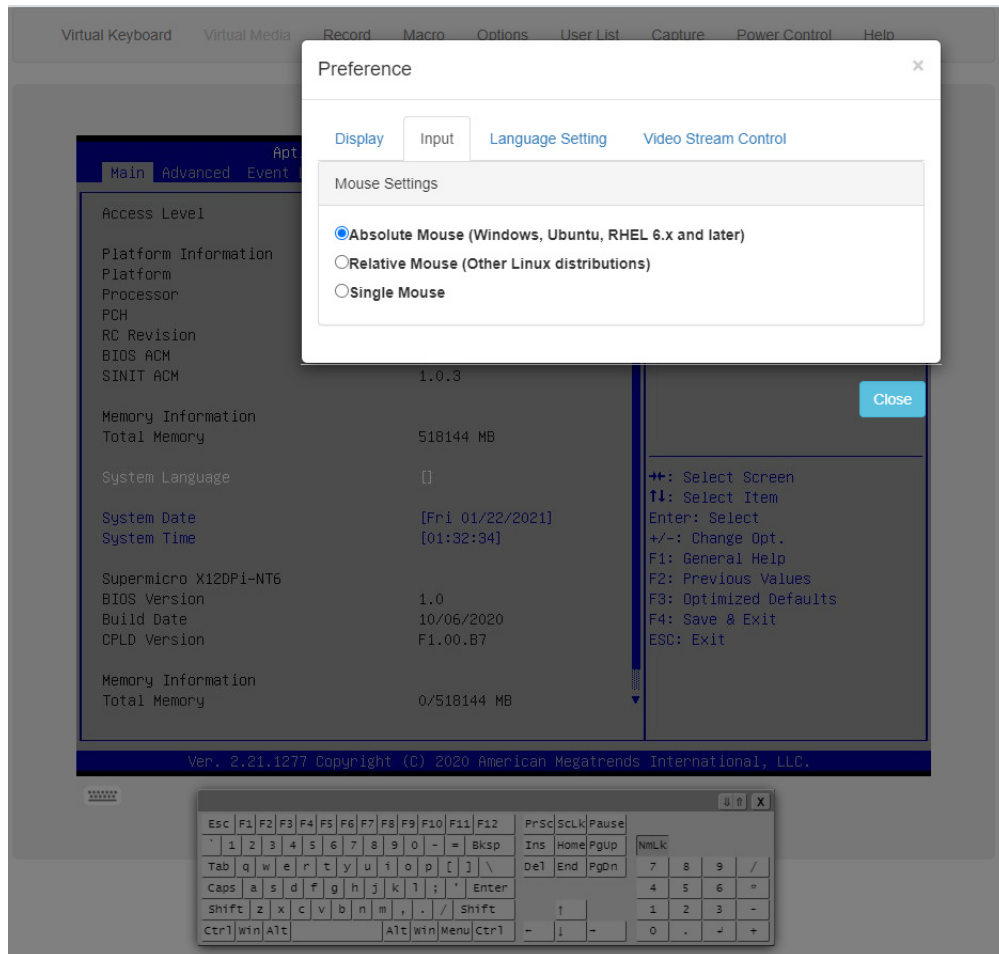
This feature enables auto-stop after n (default: 2) minutes. Adjust the maximum duration of video recordings.



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

Preference – Input

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



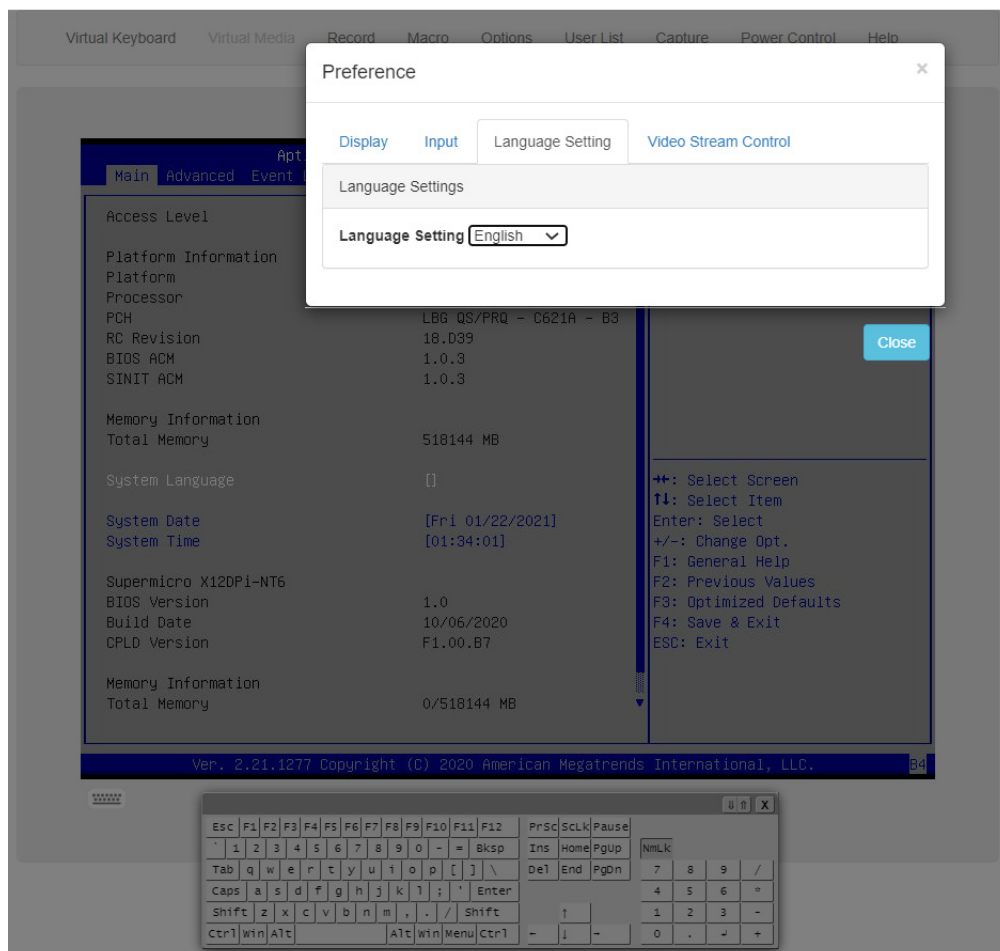
- Absolute Mouse
- Relative Mouse
- Single Mouse



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

Preference – Language Setting

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

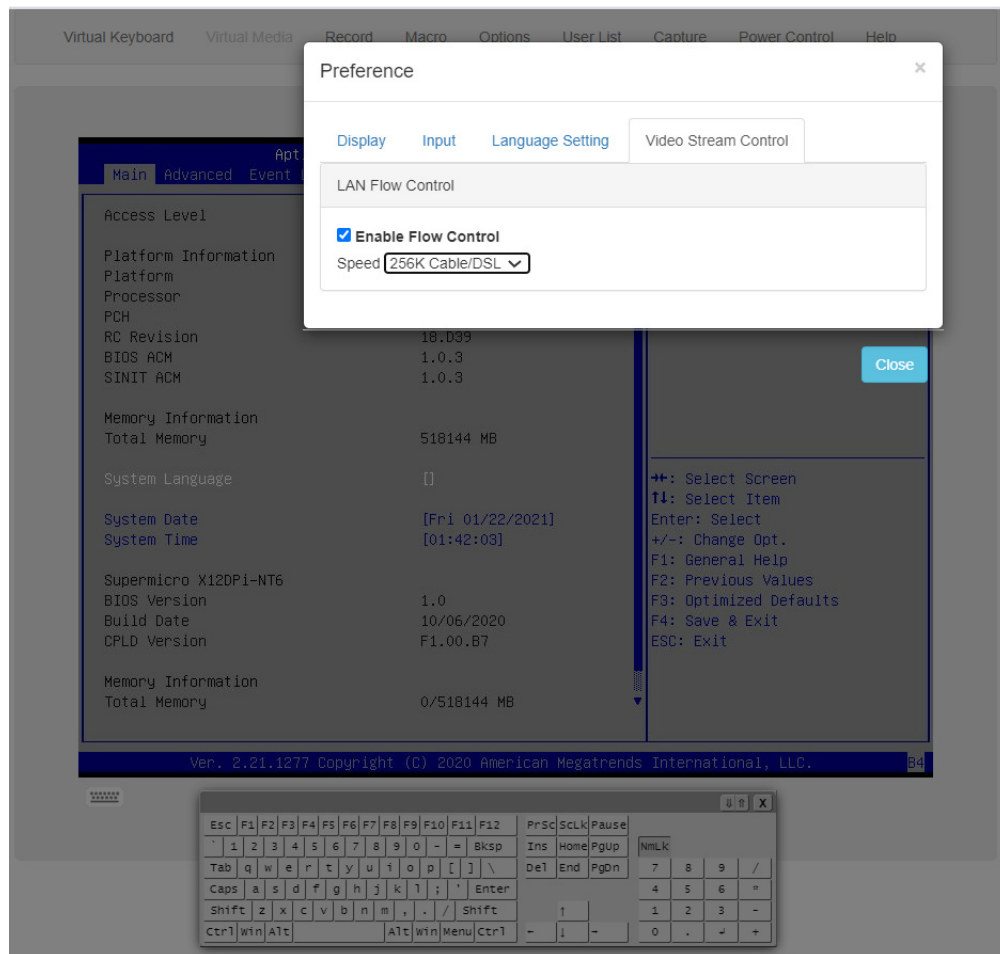


- English
- Japanese
- German
- French
- Spanish
- Italian

Preference – Video Stream Control

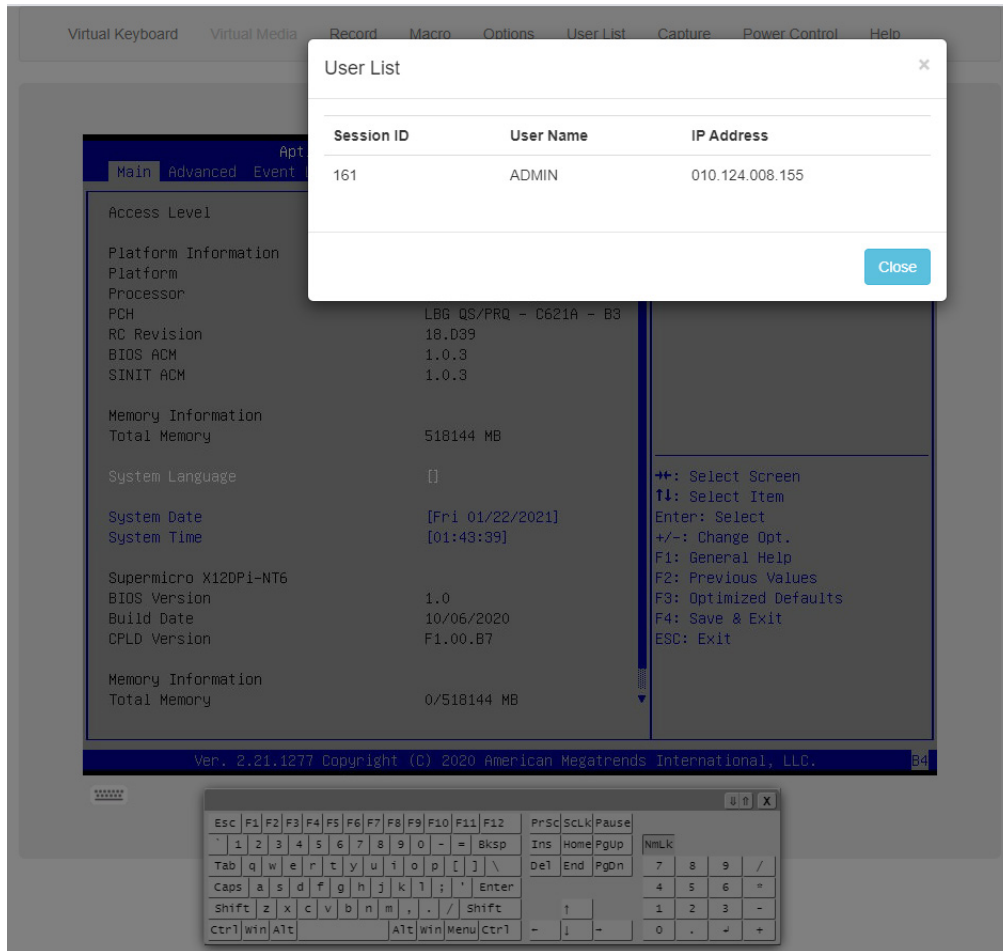
This feature allows you to enable video flow control for LAN Quality of Service (QoS) by selecting one of the following options.

- 256K Cable/DSL
- T1
- T2



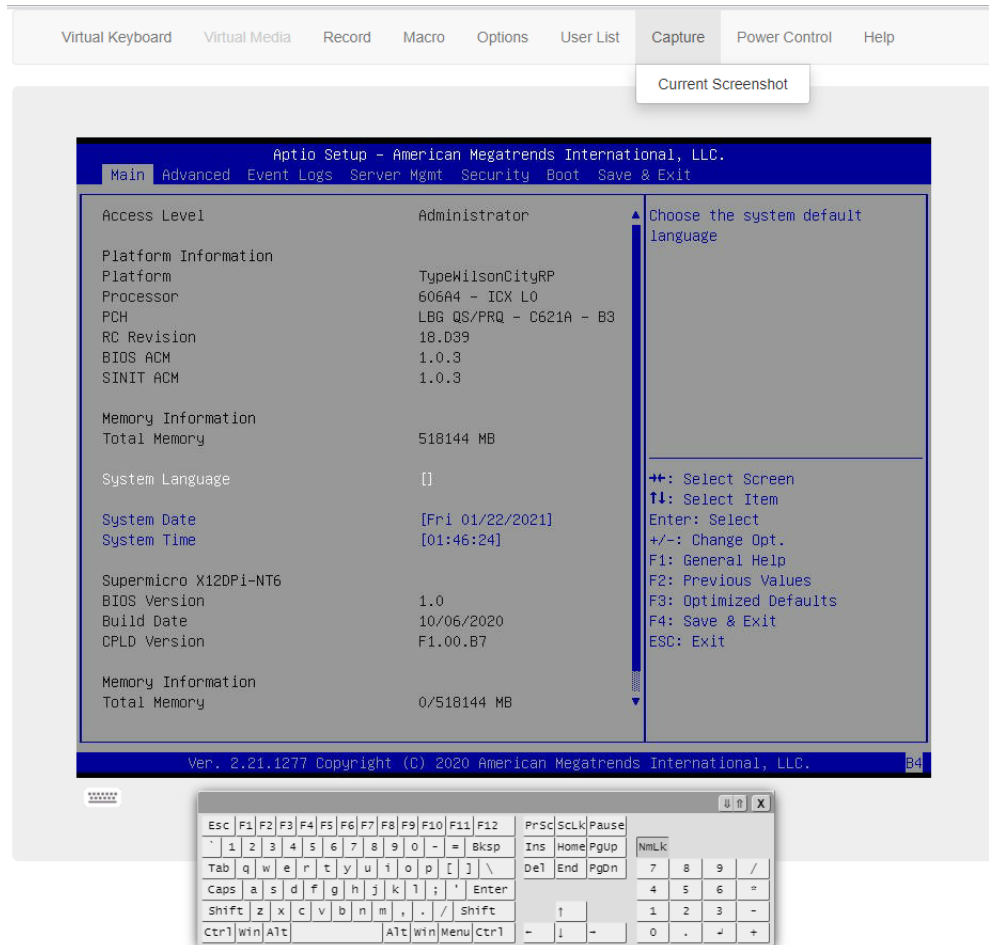
2.8.2f iKVM/HTML5 – User List

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.



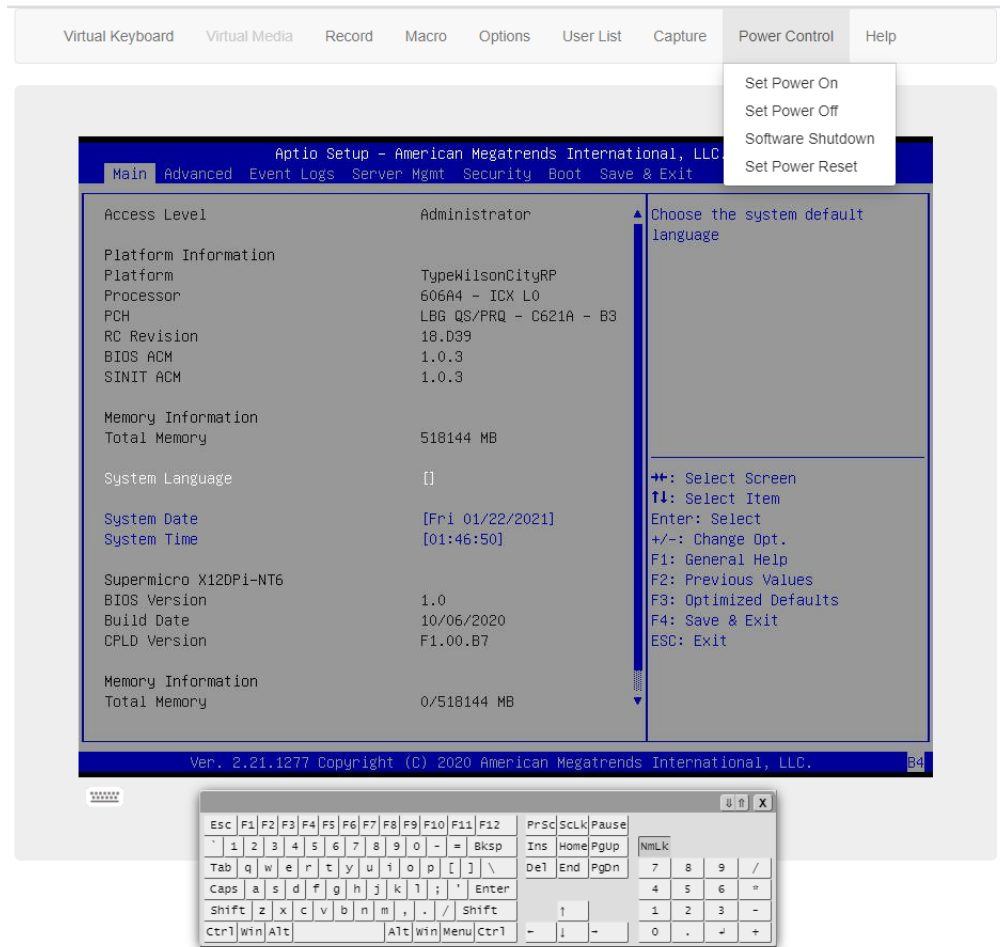
2.8.2g iKVM/HTML5 – Capture

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



2.8.2h iKVM/HTML5 – Power Control

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



2.9 Maintenance

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



Note: Currently, the number of Maintenance Event Log entries is limited to 512.

2.9.1. Firmware Management

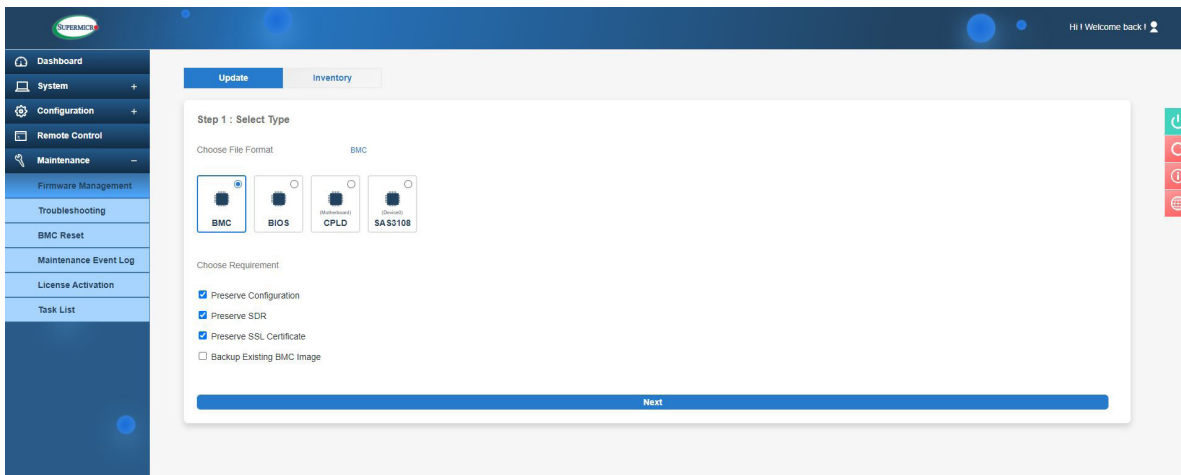
The firmware management page allows the administrator to update firmware for BMC, BIOS, Motherboard CPLD, Backplane CPLD, network AOC, or storage AOC as well as to manage Platform Firmware Resiliency (PFR) options.



Note: Systems are required to power down all HOSTs from single-node or multi-node systems prior to Motherboard CPLD, Backplane CPLD, LCMC PDB CPLD, and BIOS firmware updates. They are required to reboot after firmware updates for network AOC and/or storage AOC. Lastly, BMC may be required to reset after the motherboard CPLD firmware update, especially in multi-node systems (i.e. GrandTwin).

Update

This page allows you to update component firmware if you have administrator privileges.



To update component firmware, please refer to the following steps.

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

4. Update the firmware by clicking the “Update” button. Once the firmware is in update mode, the device will be reset and the server will reboot even if you cancel the firmware updating process. If you cancel the firmware updating process, there will be an alert message asking, “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 saying, “BMC is restarting to continue the BMC firmware update process. To prevent data loss, please Do Not Remove the power source until BMC is back online!” upon confirmation.



Note: Web Browser / BMC UI of secondary UI (viewing web browser) needs to refresh to renew the BMC connection since viewing the web browser has stopped sending requests after the firmware 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 the power source until BMC is back online!”

BMC update supports the following preserve configuration options.

- Preserve configuration
- Preserve SDR
- Preserve SSL certificate

How BMC Firmware is Updated

Update Inventory

Step 1 : Select Type

Choose File Format **BMC**

BMC BIOS CPLD (Motherboard) PMem SAS3808 (Device 0) NIC1 (PCIe Slot2) SAS3816 (Device 1)

Choose Requirement

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

Next

Update Inventory

Step 1 : Select Type

Choose File Format **BMC**

BMC BIOS CPLD (Motherboard) PMem NIC1 (PCIe Slot2) SAS3808 (Device 0) SAS3816 (Device 1)

Choose Requirement

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

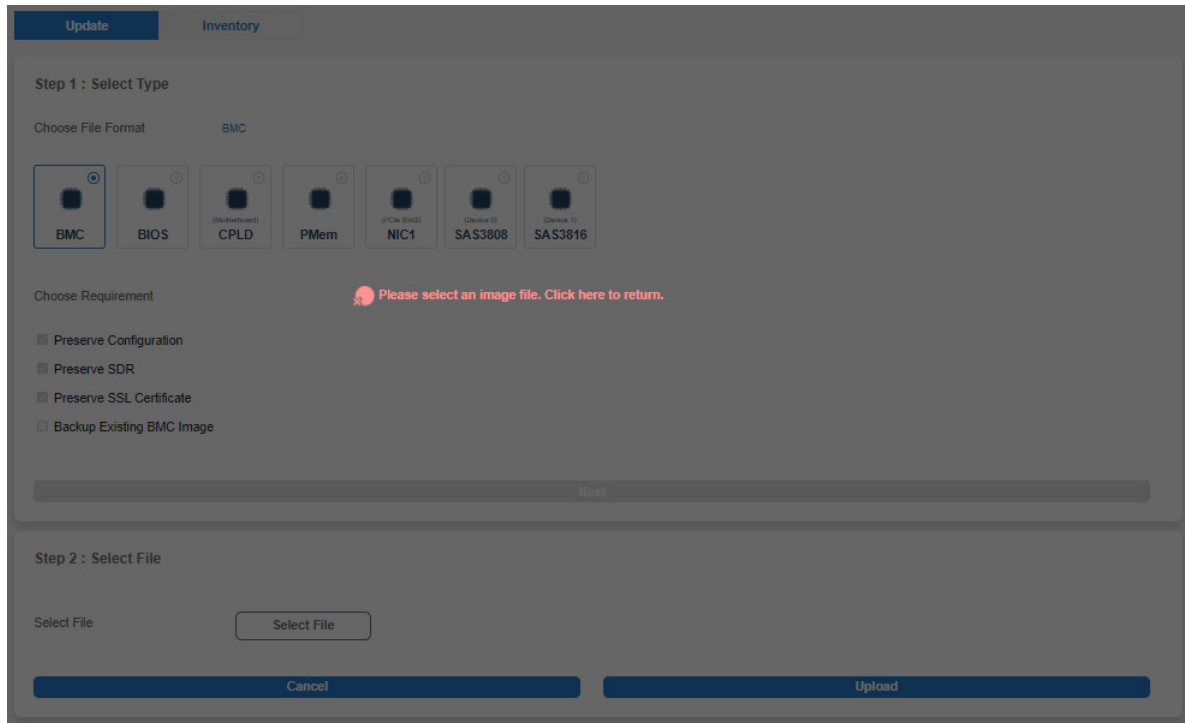
Next

Step 2 : Select File

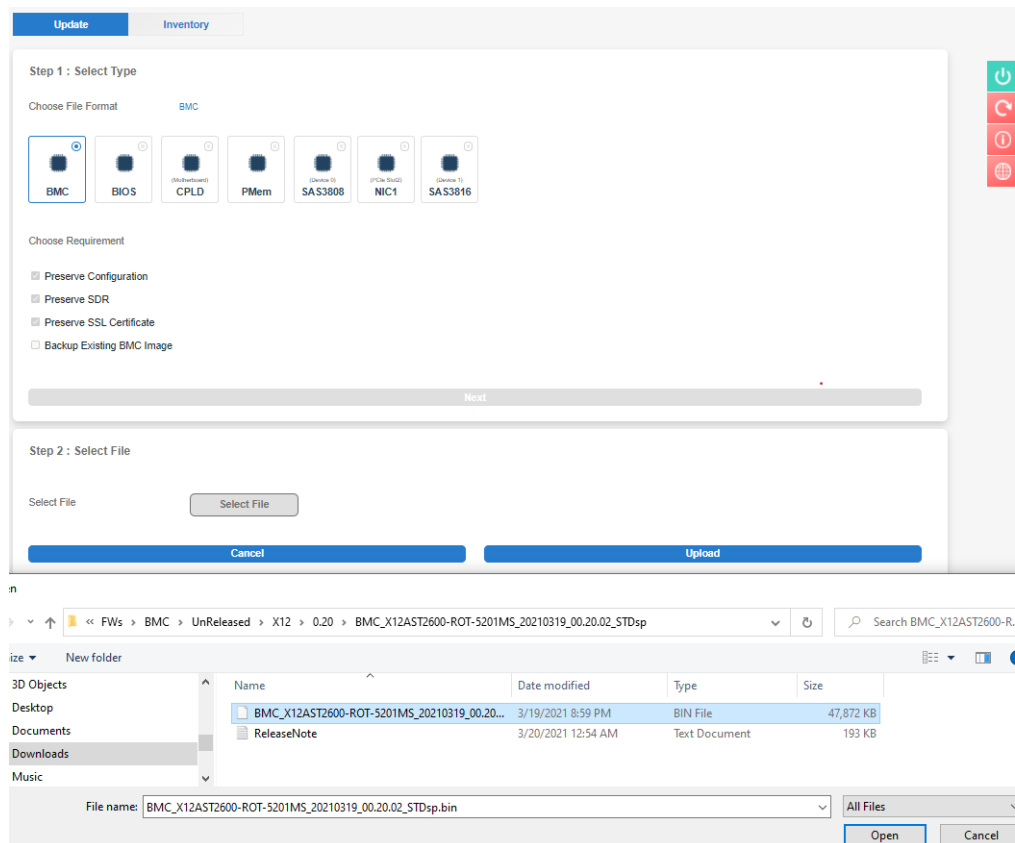
Select File

Cancel Upload

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



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



Update
Inventory

Step 1 : Select Type

Choose File Format BMC

BMC

BIOS

CPLD
(Microprocessor)

PMem

NIC1
(PCIe Slot2)

SAS3808
(Device 0)

SAS3816
(Device 1)

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

×

Cancel
Upload

Update
Inventory

Step 1 : Select Type

Choose File Format BMC

BMC

BIOS

CPLD
(Microprocessor)

PMem

NIC1
(PCIe Slot2)

SAS3808
(Device 0)

SAS3816
(Device 1)

Choose Requirement

●
●
●
●

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

Next

Step 2 : Select File

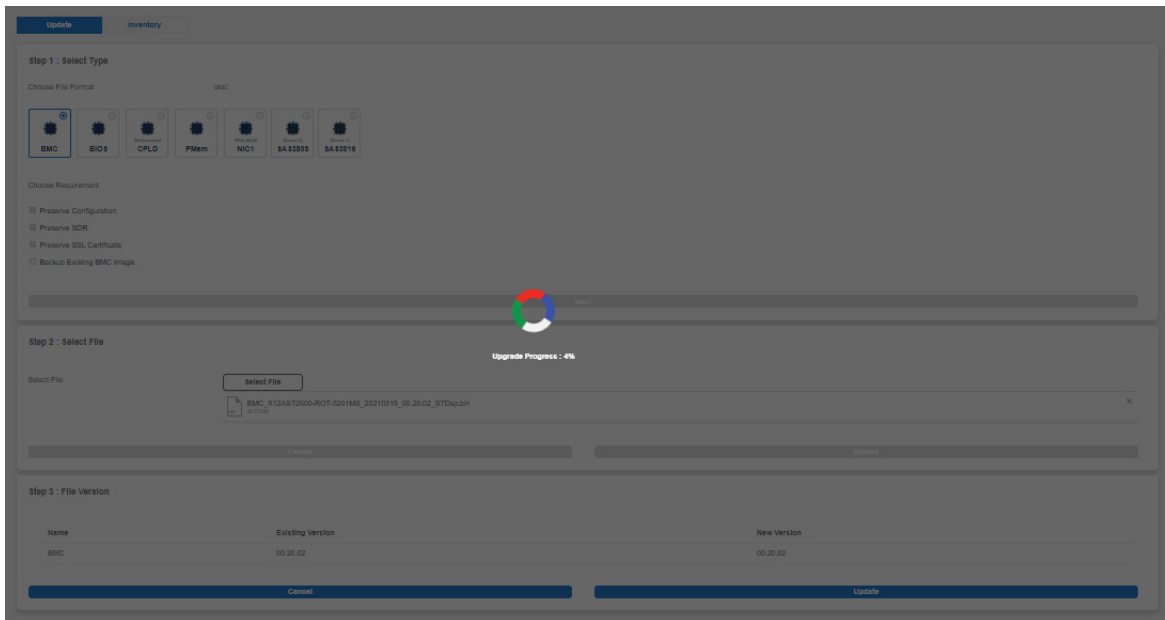
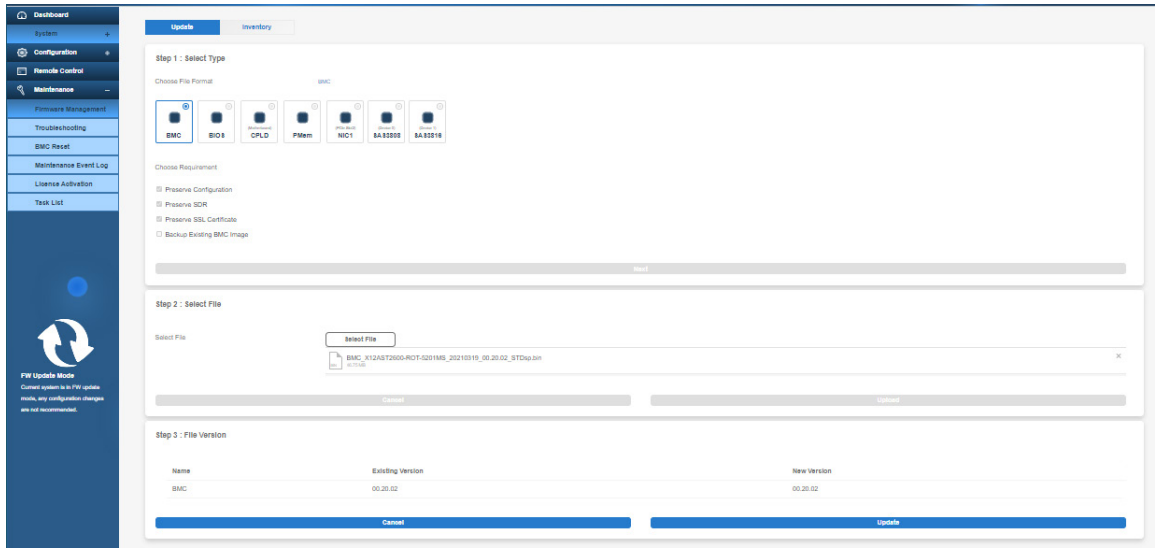
Select File

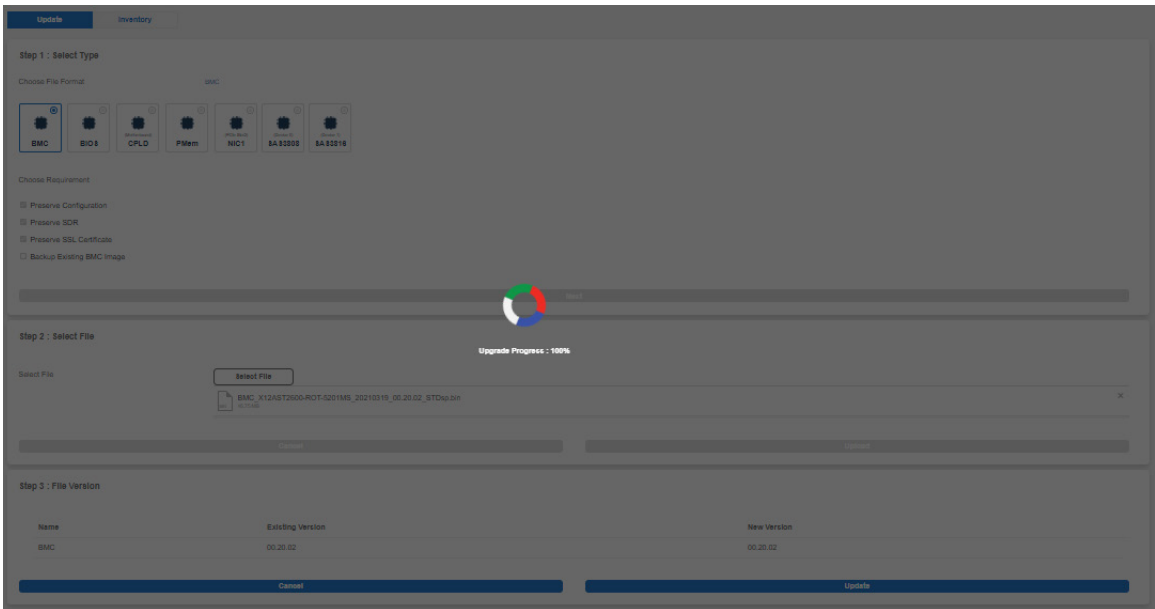
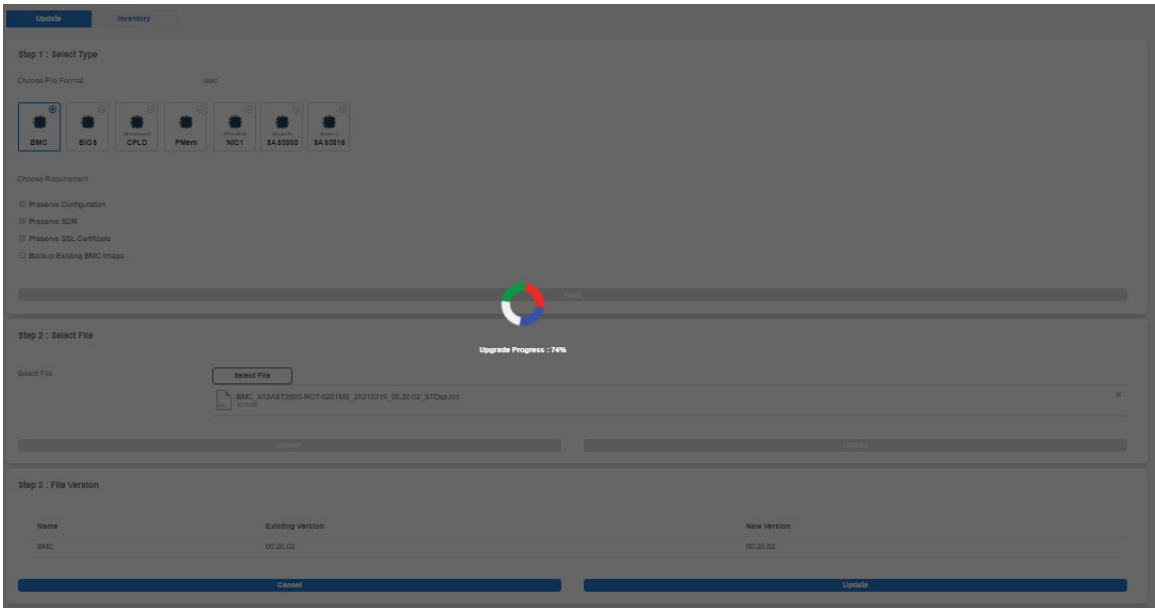
Select File

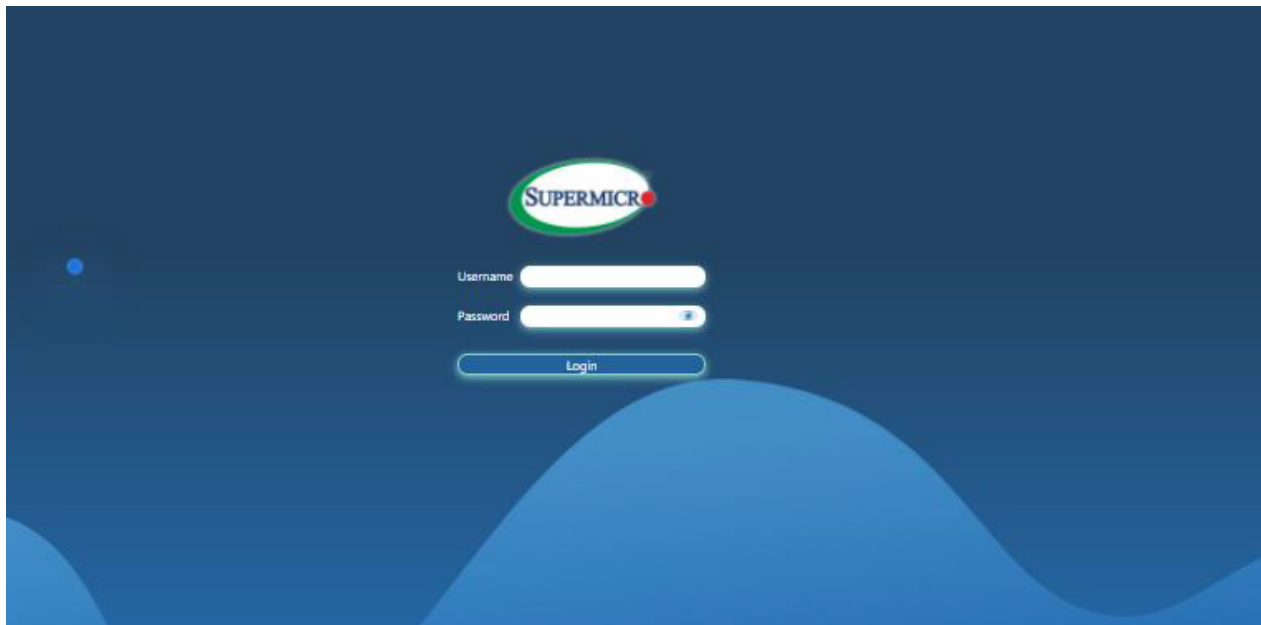
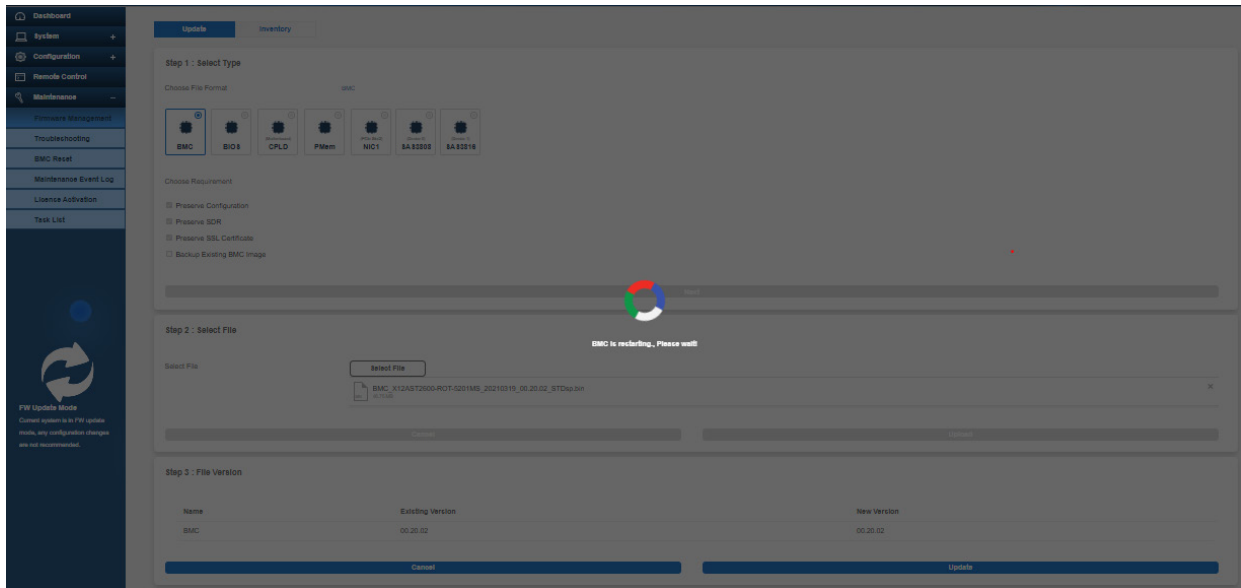
BMC_X12AST2600-ROT-5201MS_20210319_00.20.02_STDsp.bin

×

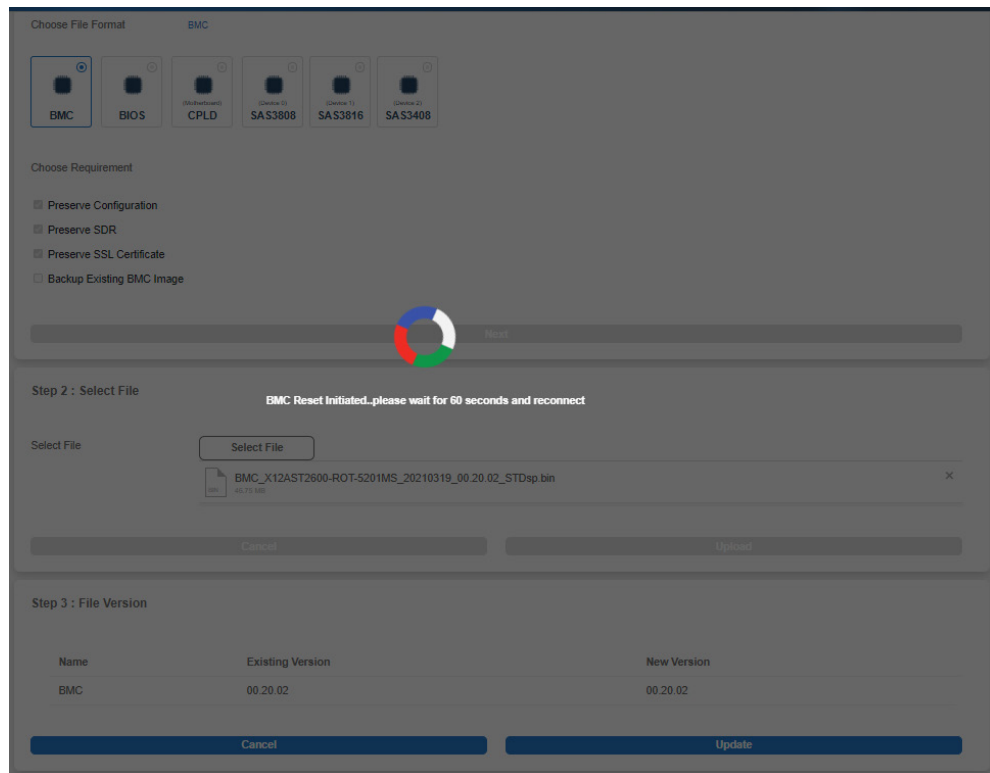
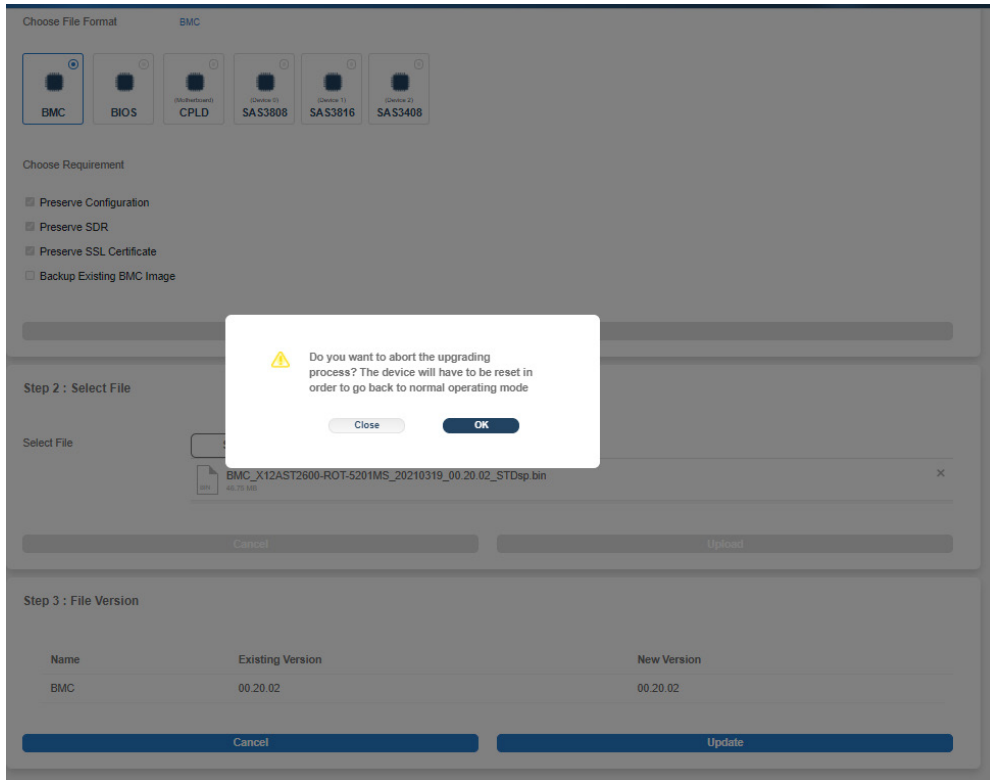
Cancel
Upload



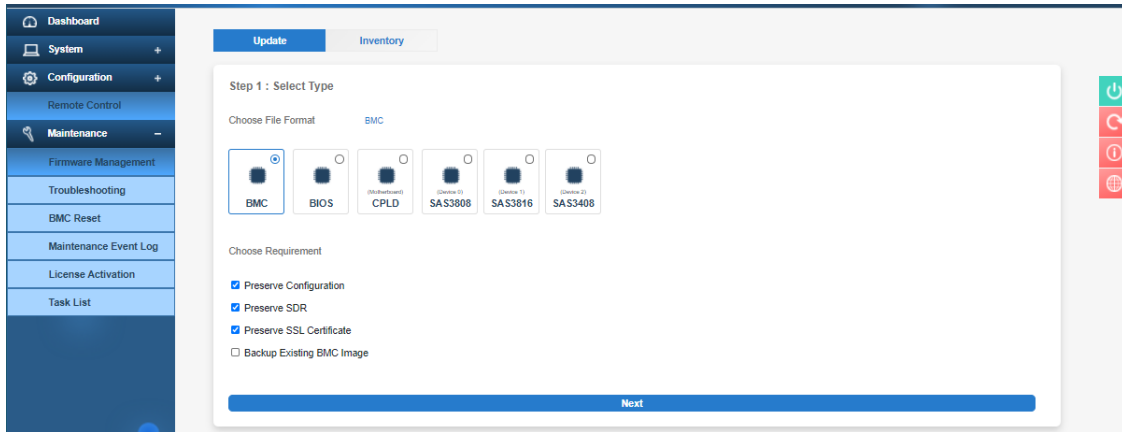


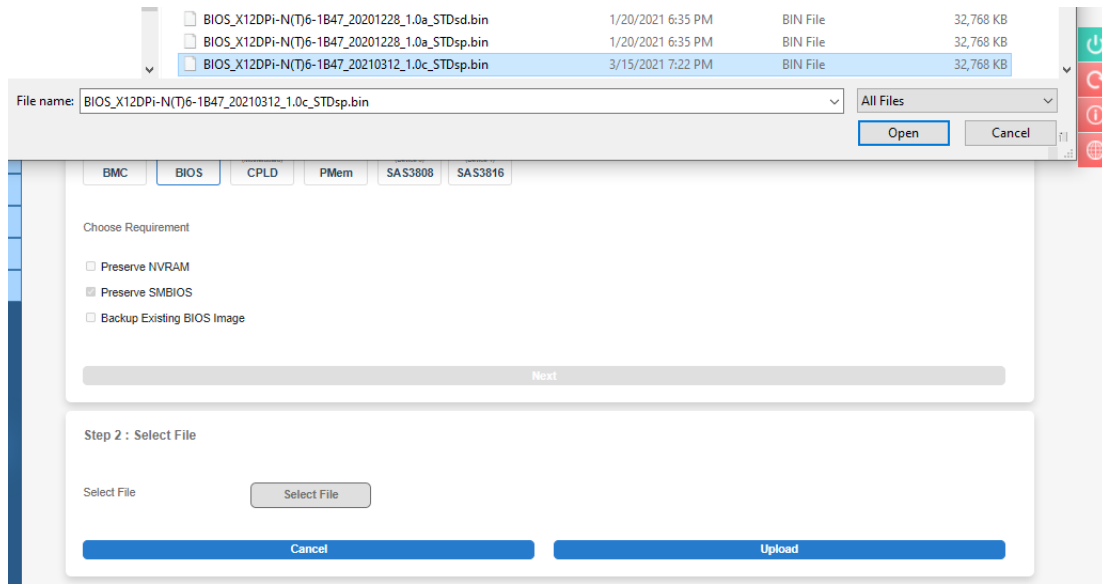
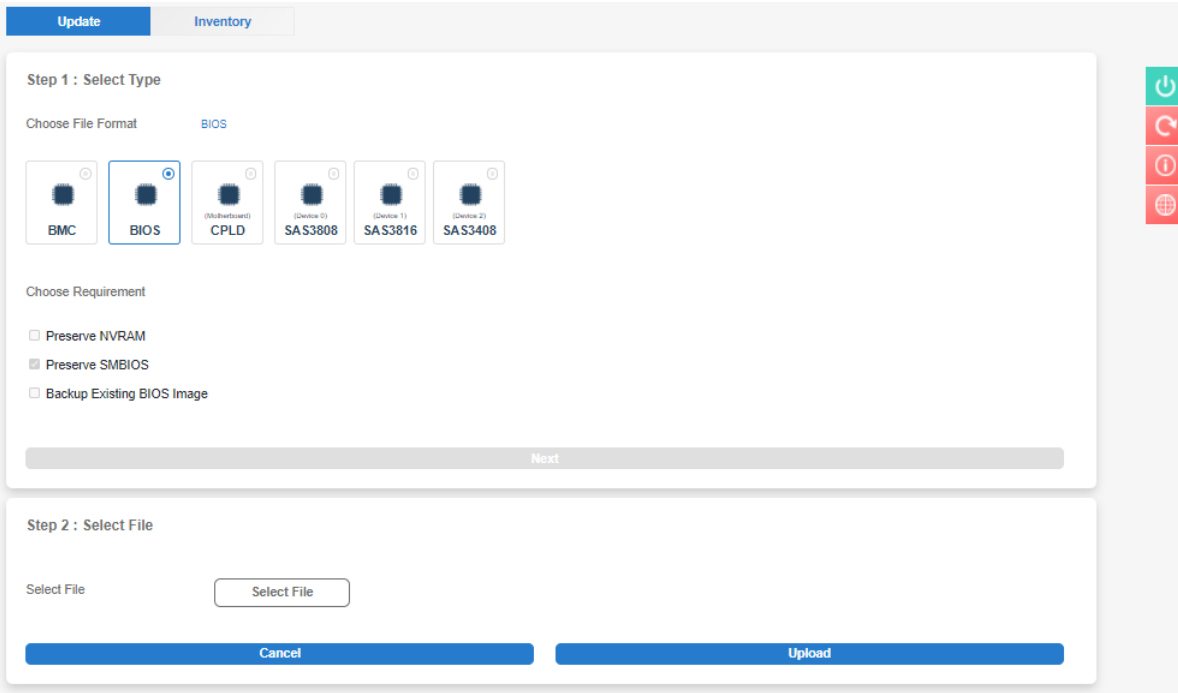


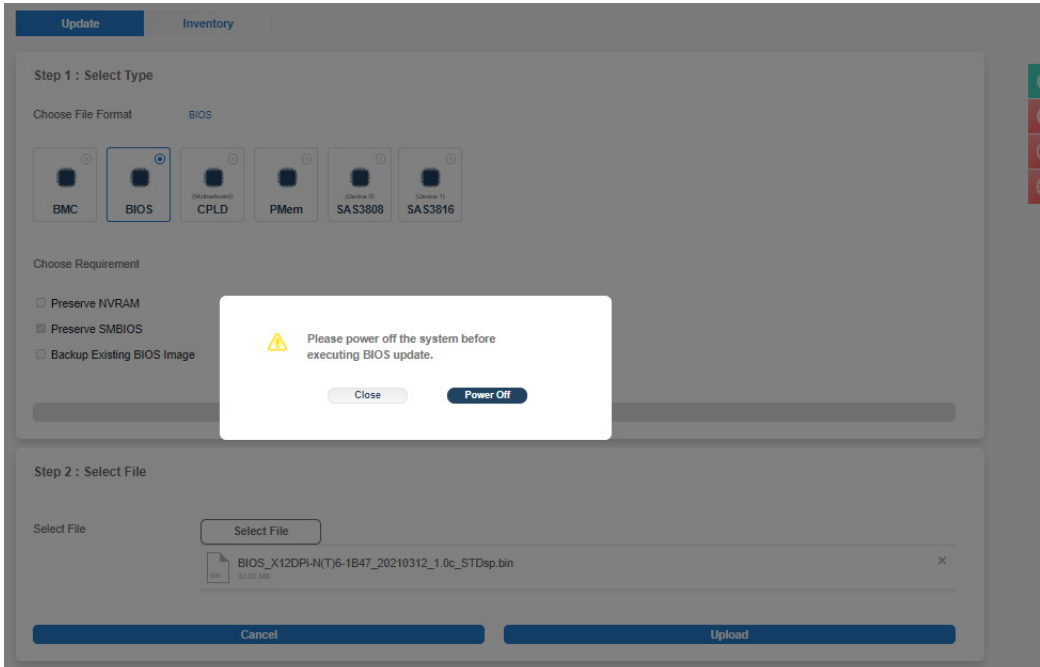
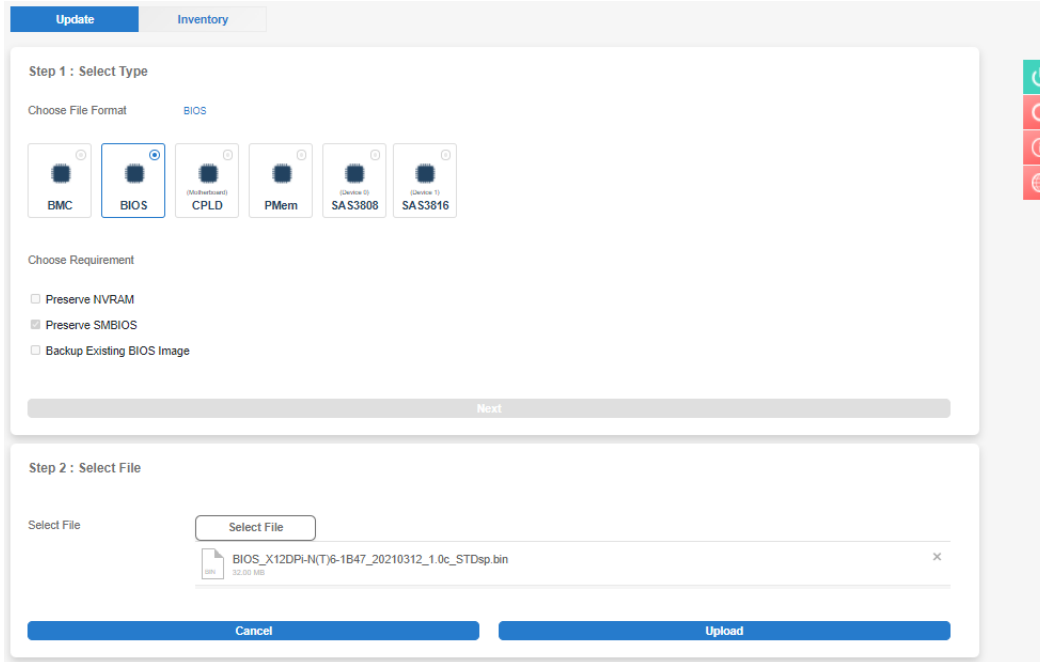
Note: If you cancel the BMC updating process, there will be an alert message pops up to ask you “Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode.” BMC is then reset with the message “BMC is restarting. To prevent data loss, please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

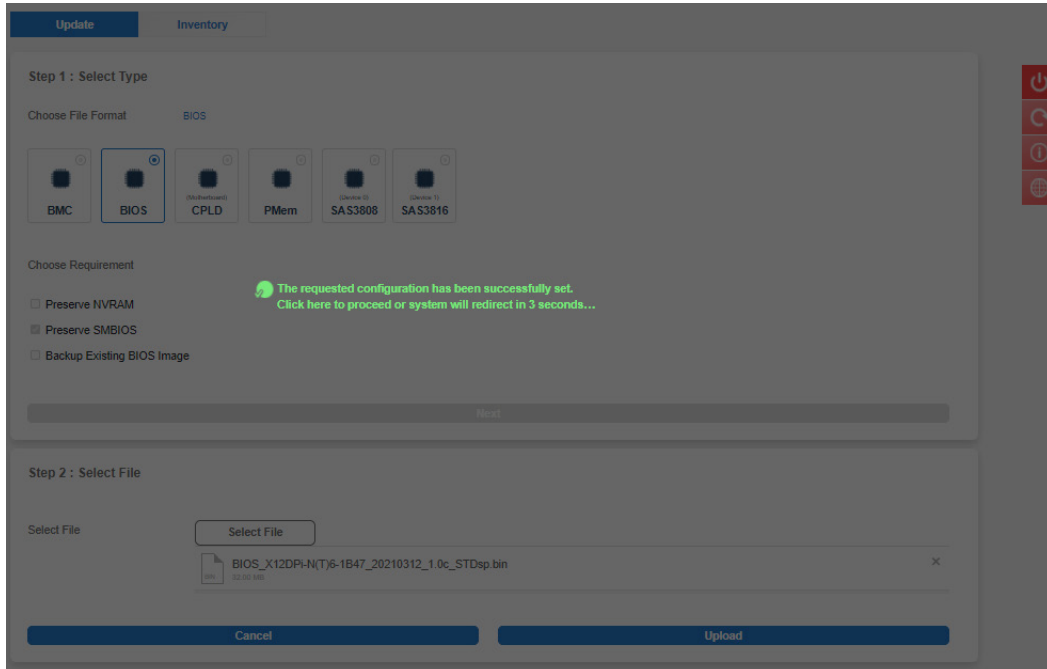
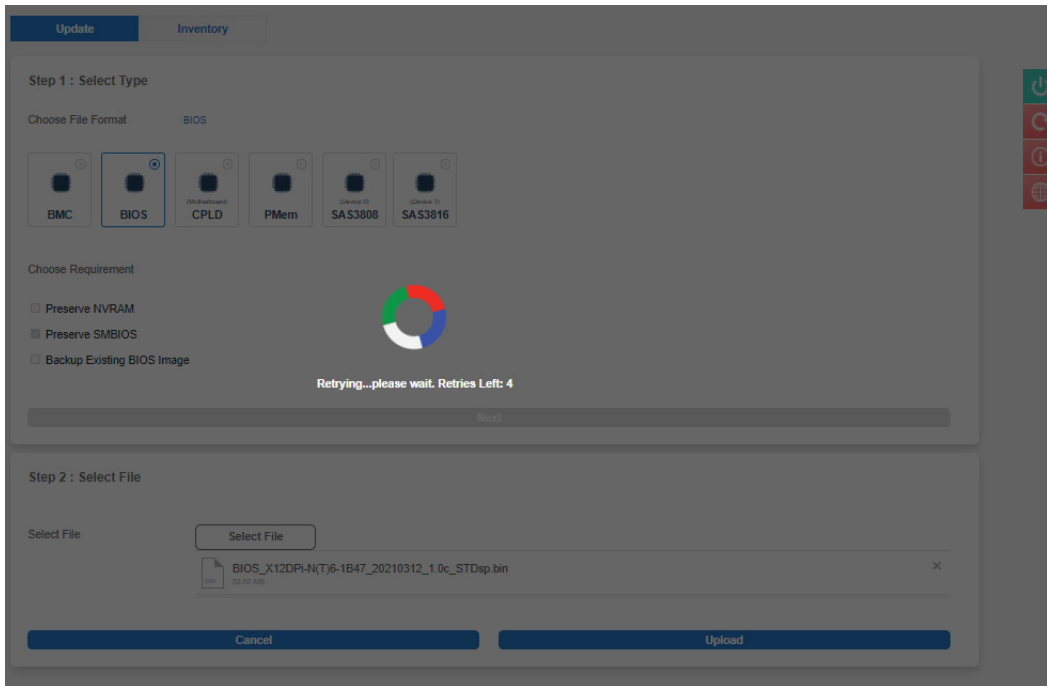


How BIOS Firmware is Updated

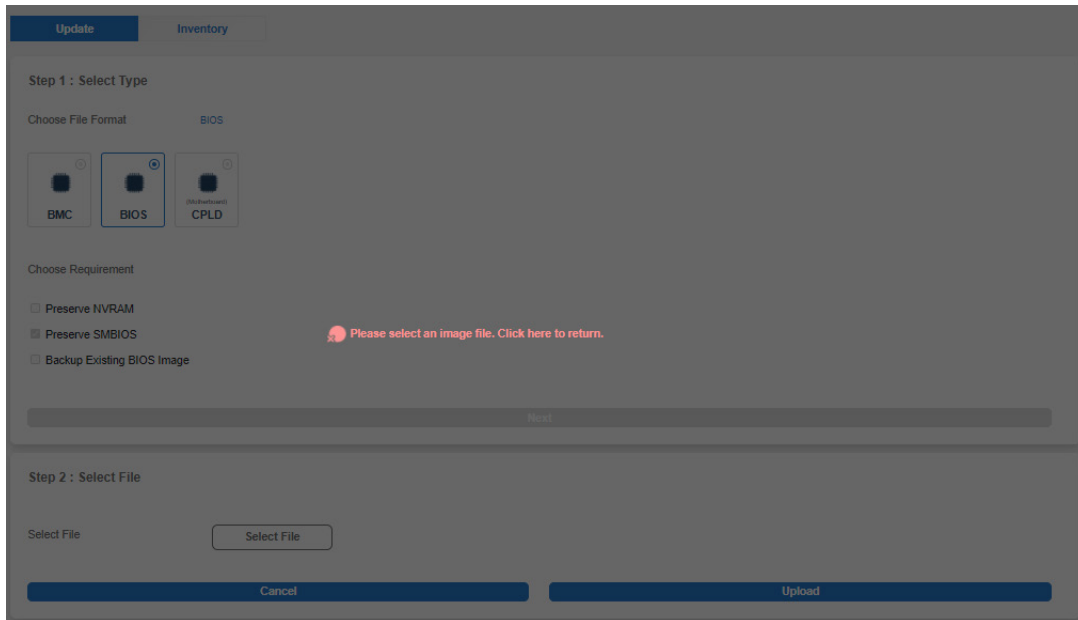




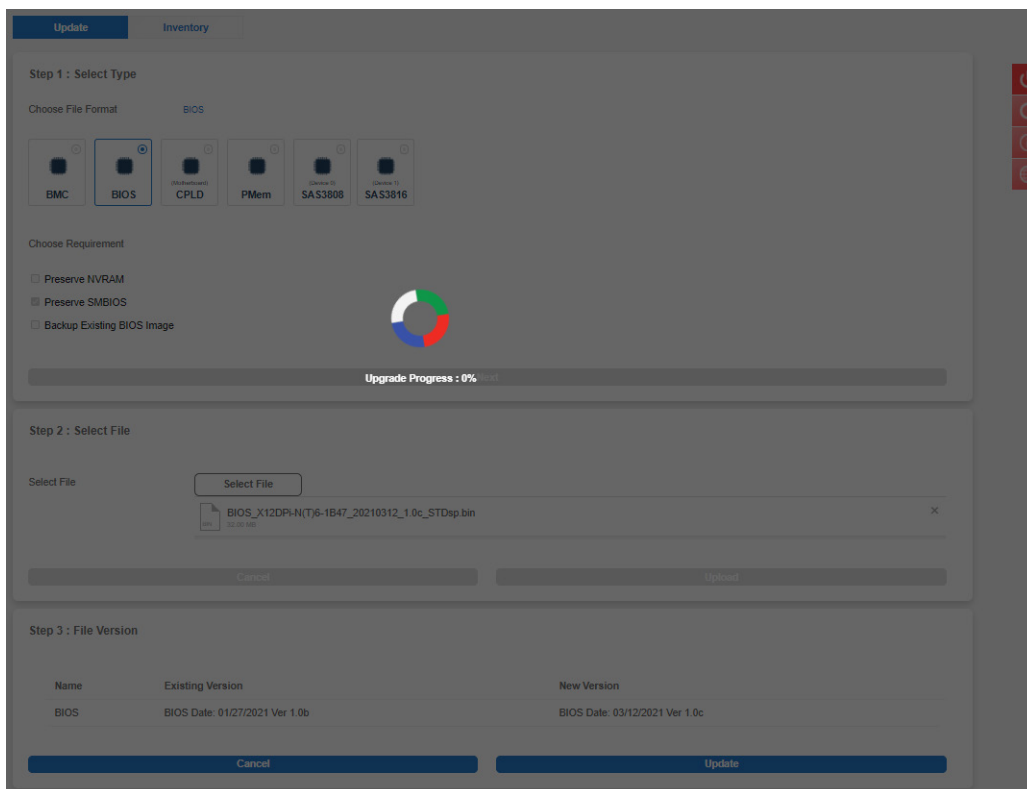


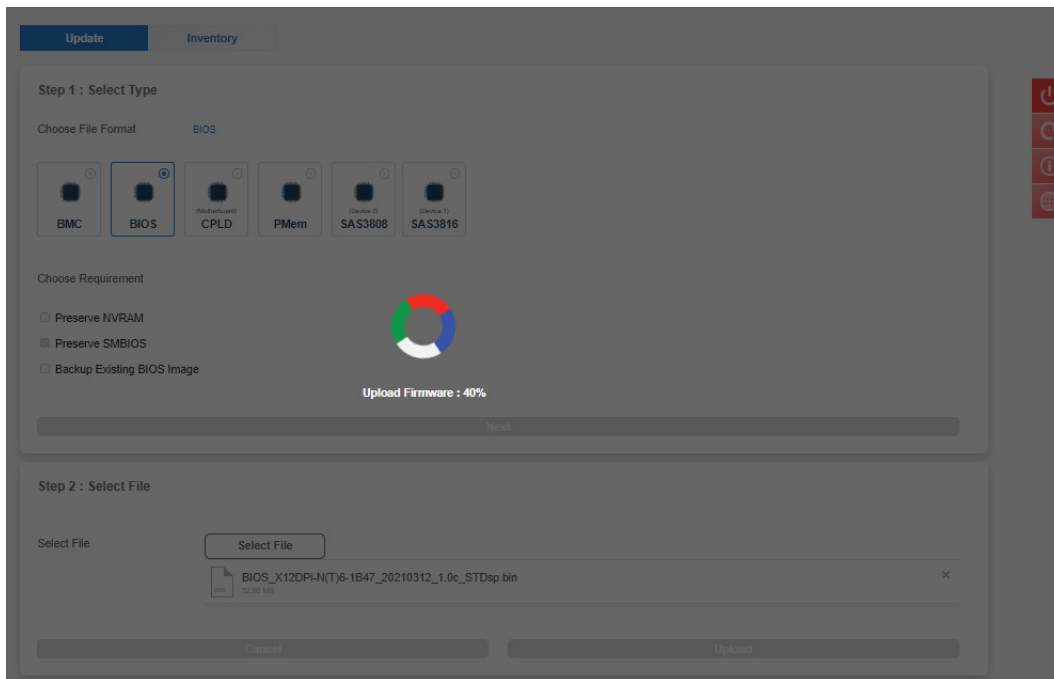
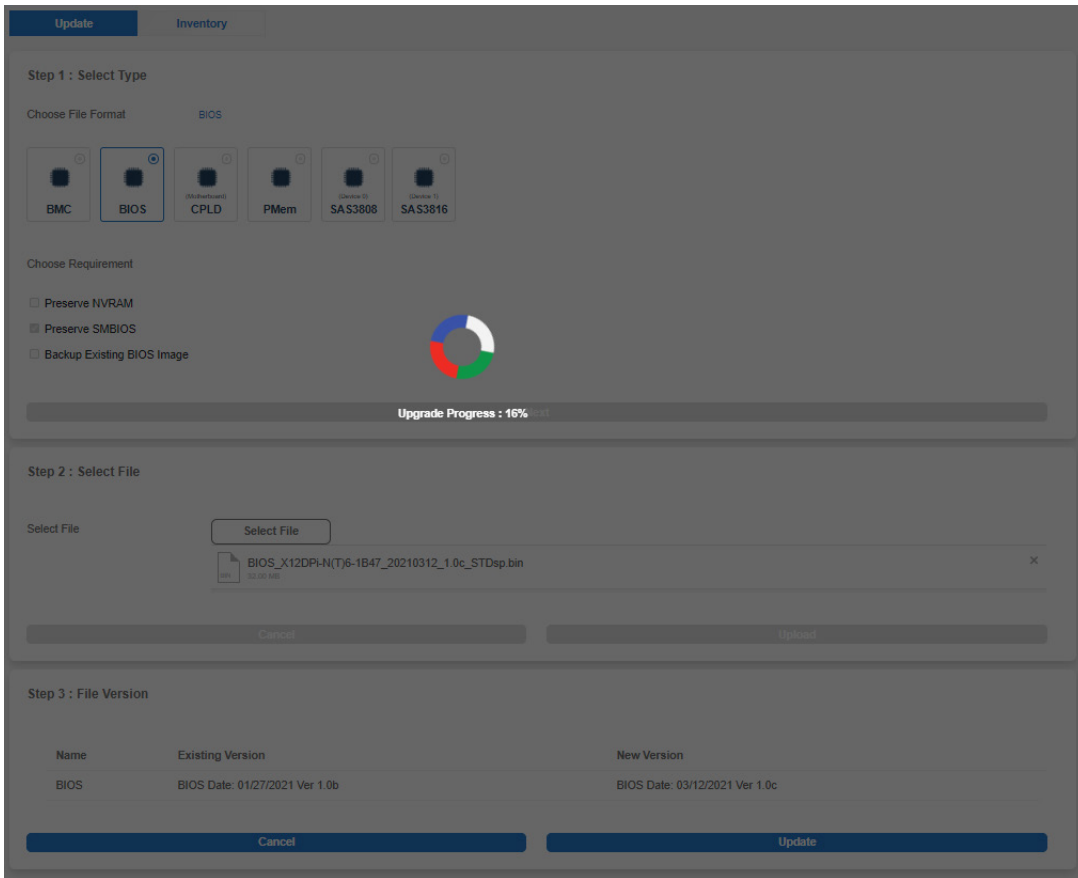


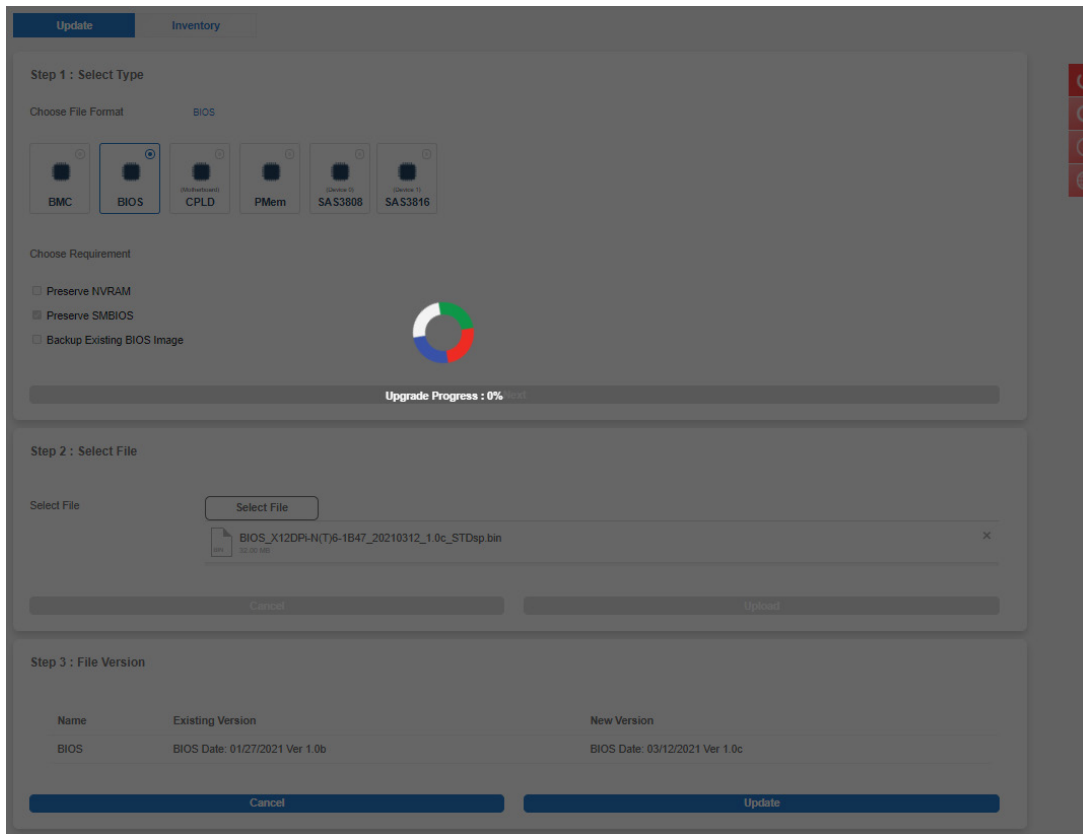
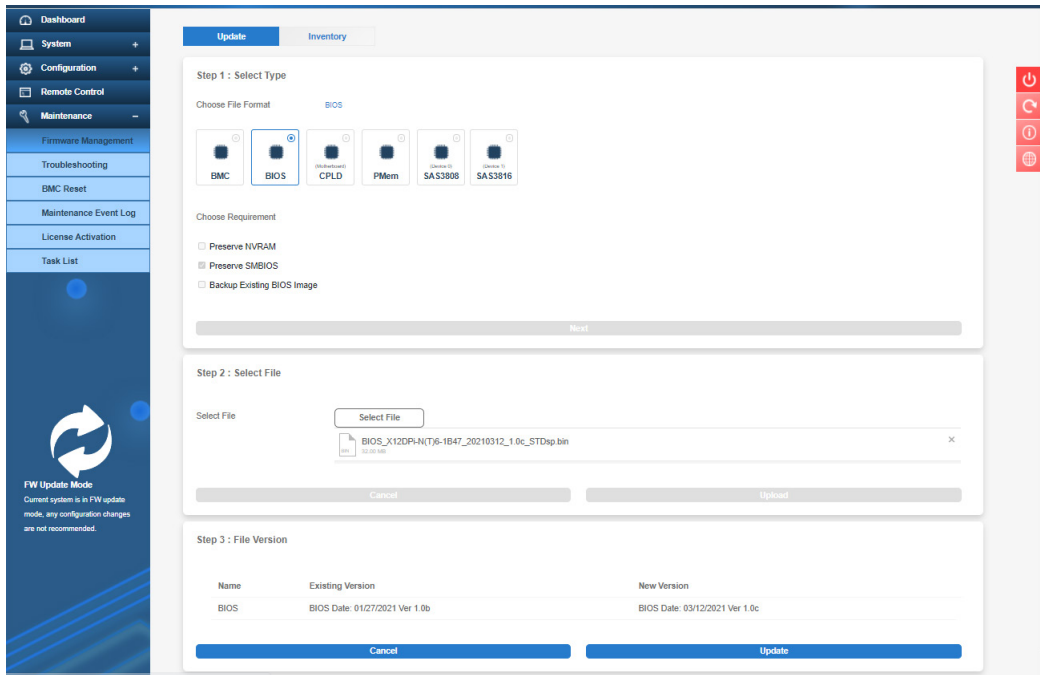
If you click the “Upload” button without a BIOS image included, a message will inform you to “Please select an image file. Click here to return.”

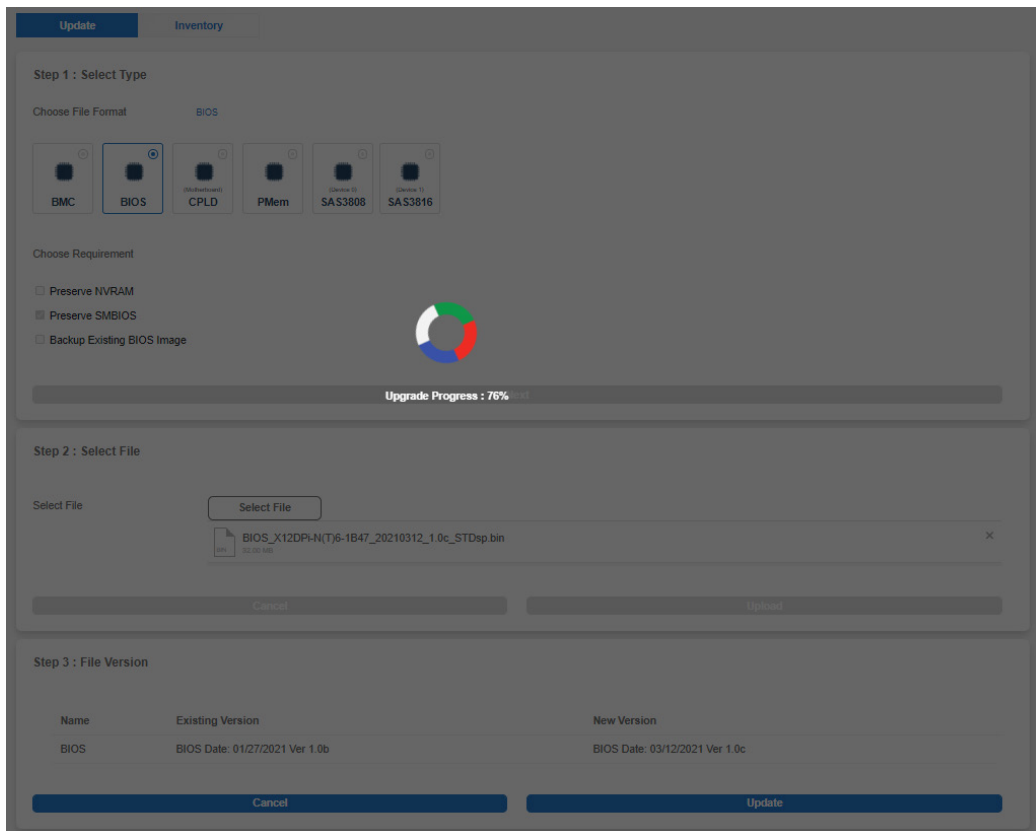
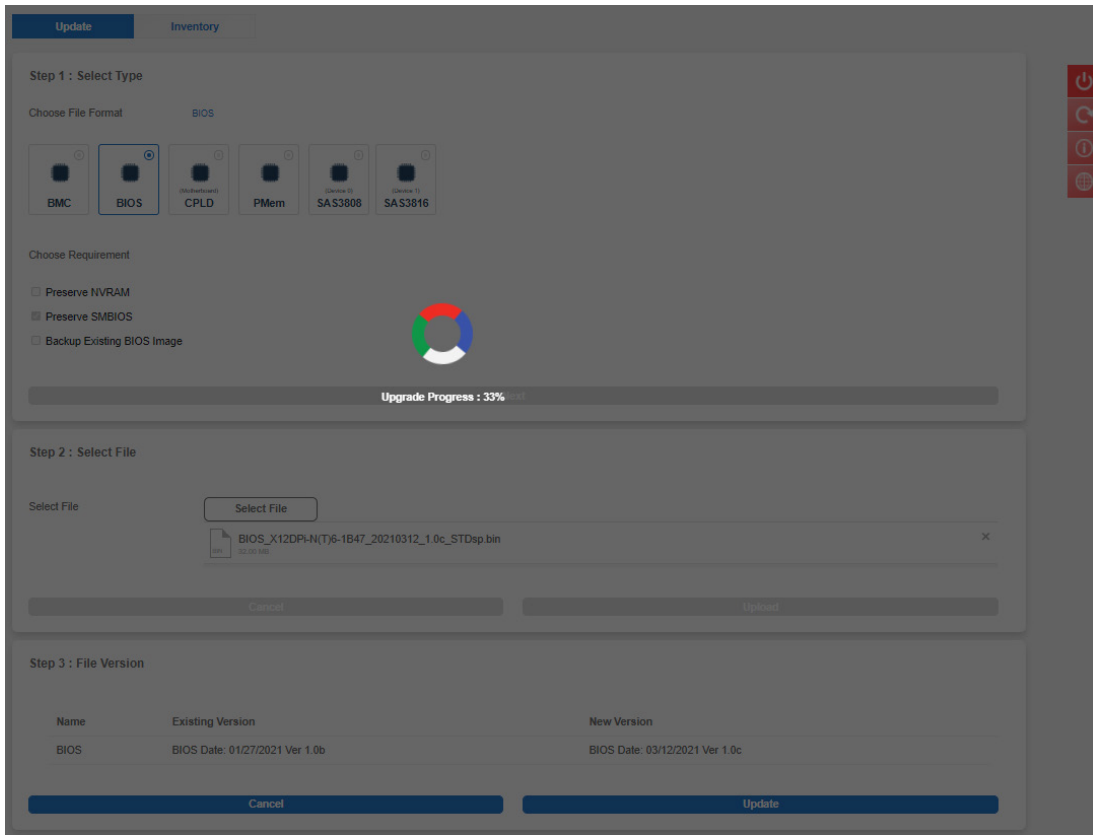


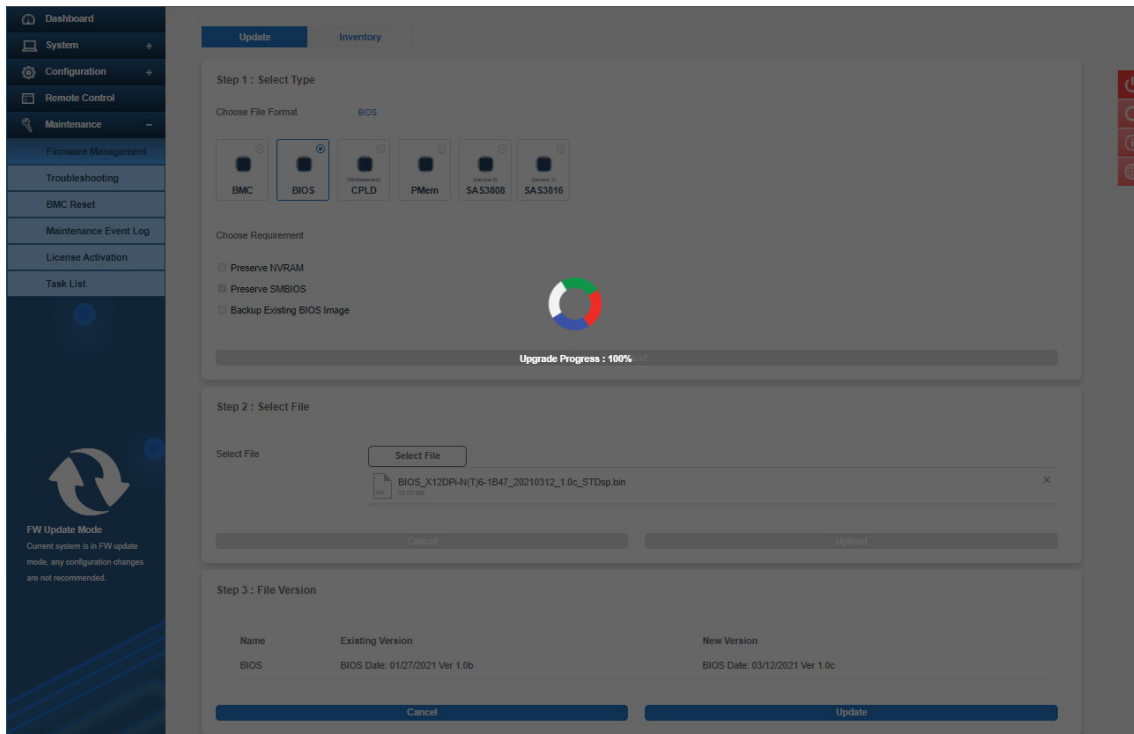
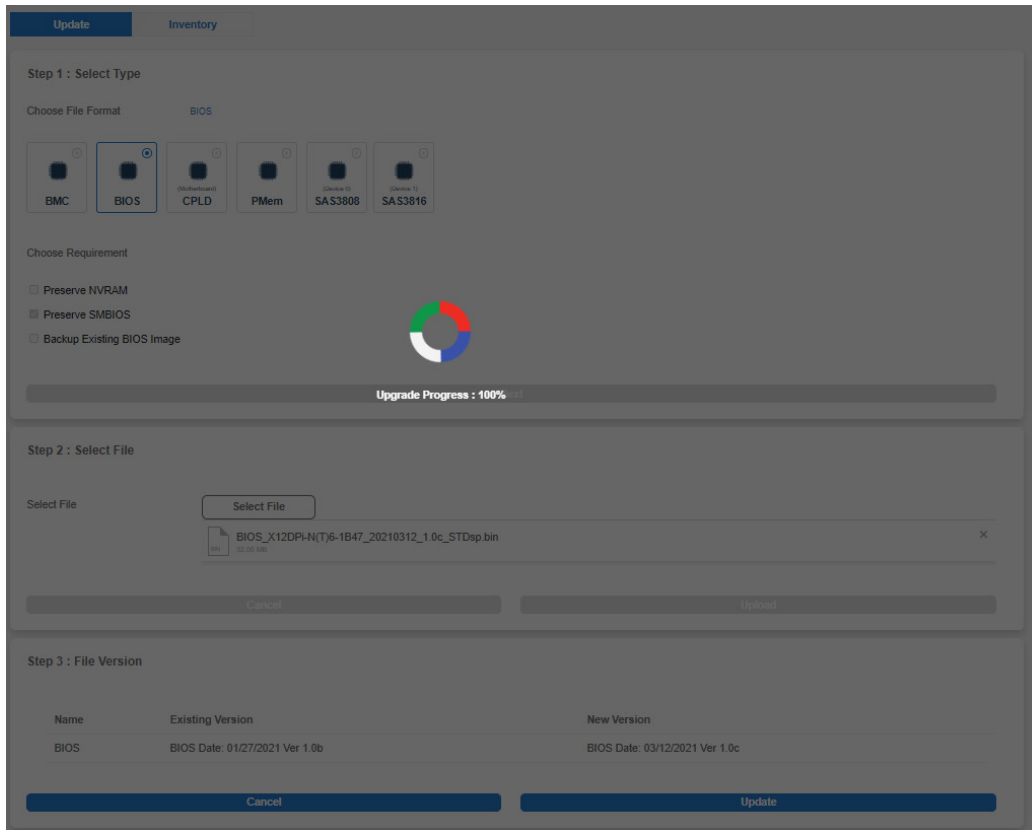
If you continue on with the BIOS update, BMC will provide a timely percentage of completion. See images below for details.



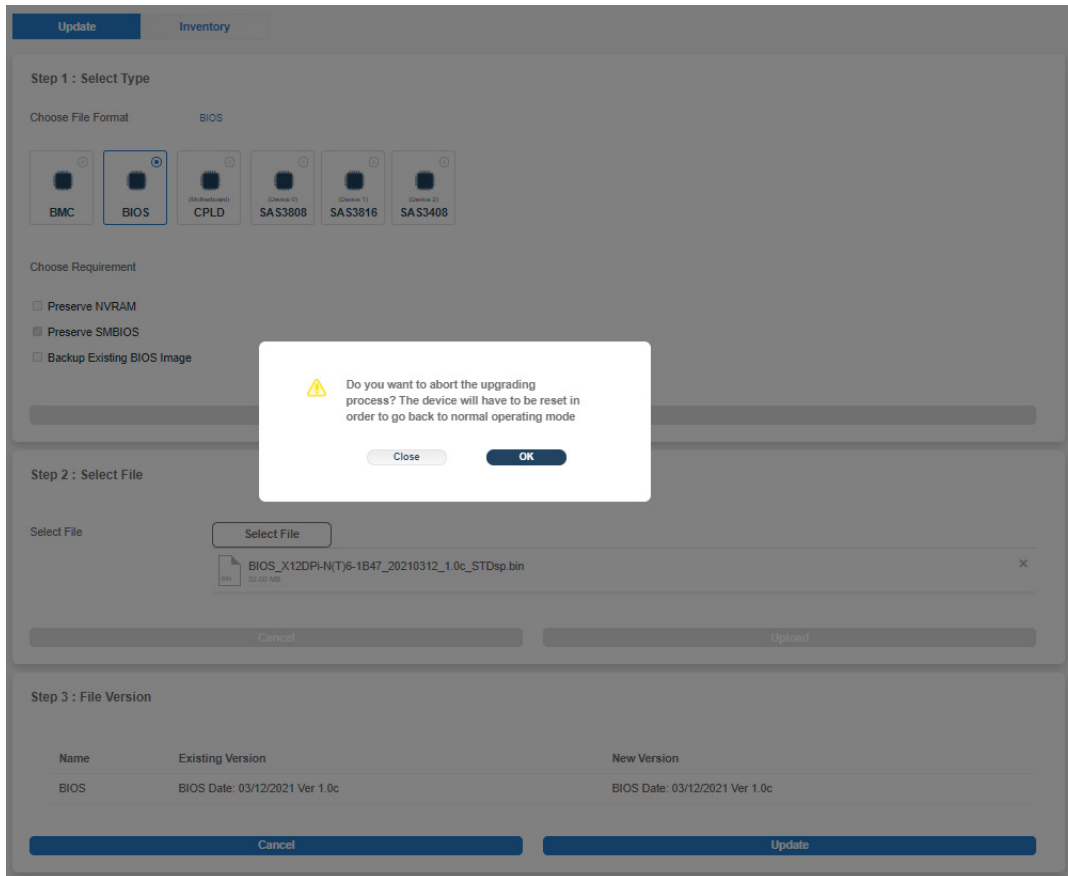








Note: If you cancel the BIOS updating process, there will be an alert message that pops up to ask you “Do you want to abort the upgrading process? The device will have to be reset in order to go back to normal operating mode.” BMC is then reset with a message “BMC Reset Initiated..please wait for 60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



Update Inventory

Step 1 : Select Type

Choose File Format BIOS

BMC BIOS CPLD (WebBoard) SAS3808 (Device 1) SAS3816 (Device 1) SAS3408 (Device 2)

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

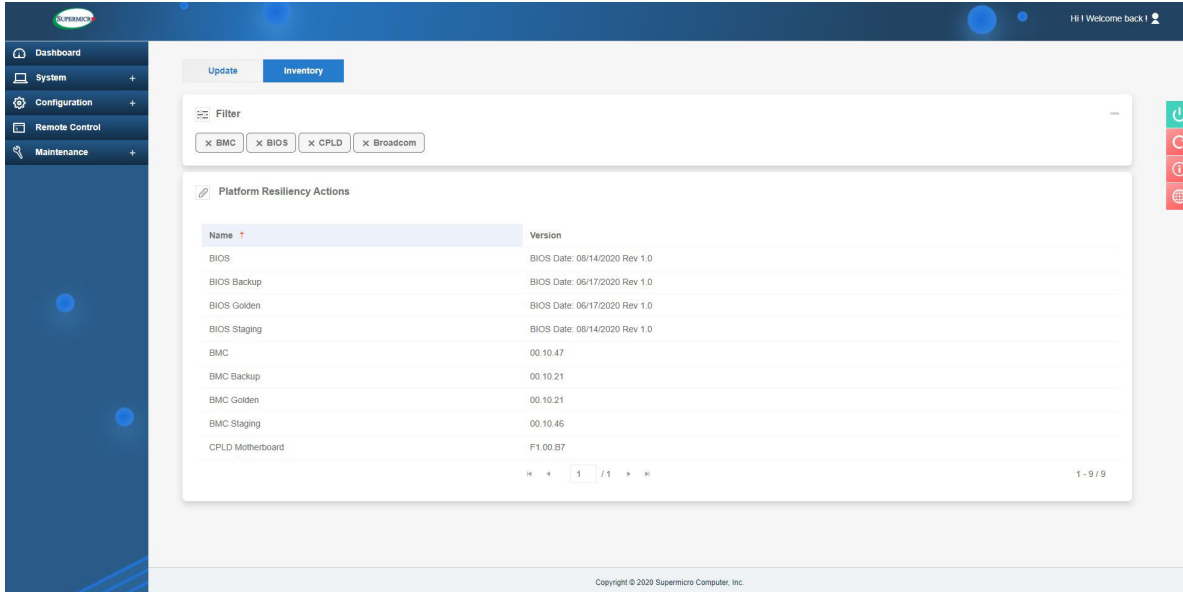
Step 3 : File Version

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

Cancel Update

Inventory

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



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

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



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

- BMC: You can view active BMC firmware.
- BIOS: You can view active BIOS firmware.
- BMC ME: You can view the active BIOS ME version.
- CPLD Motherboard: You can view the motherboard CPLD version.
- Power Supply: Otherwise refers 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.

Update **Inventory**

Filter

Platform Resiliency Actions

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

« 1 / 1 » 1 - 9 / 9

Update **Inventory**

Add Filter

Platform Resiliency Actions

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

« Page 1 of 1 » 1 - 11 of 11 Items

Update **Inventory**

Filter

x BMC x BIOS x CPLD x PowerSupply

Name ↑	Version
BIOS	BIOS Date: 04/14/2023 Ver 1.0
BIOS ME	3.0.3.214
BMC	01.00.03
CPLD CPUboard	255
CPLD1 Switchboard	9
CPLD2 Switchboard	7
PowerSupply1	1.4
PowerSupply2	1.4

1 / 1 1 - 8 / 8

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

Update **Inventory**

Filter

X BMC X BIOS X CPLD X SAS

Platform Resiliency Actions

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

1 / 1 1 - 10 / 10

2.9.2. Troubleshooting

POST Snooping

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

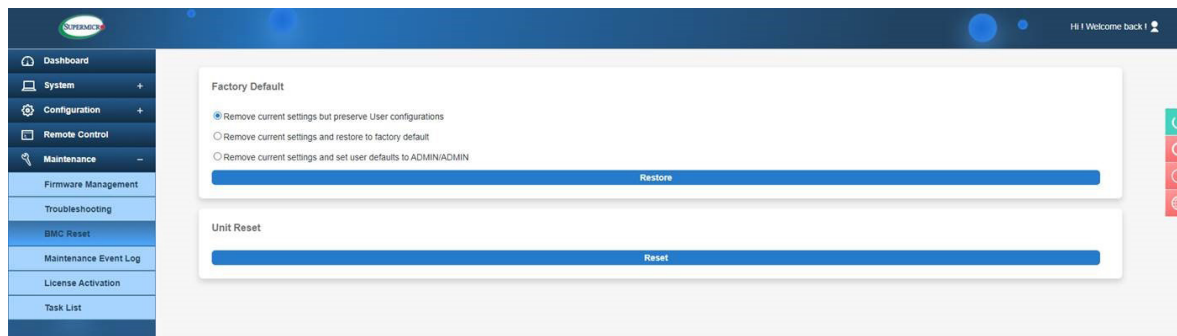
2.9.3. BMC Reset

Factory Default

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



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



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

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

Unit Reset

This feature allows you to reset an IPMI device.



Note: You will get a prompt that “BMC is restarting. To prevent data loss, please do NOT remove the 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 you can view all events. You can apply event category filters to view respective events (i.e. 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 - SMCI_TEE_SERVICE (STS) Start	service
Info	2020-10-03 16:03:00	DRTM	ADMIN(ADMIN)	Localhost	ID 0x02 - Security Functions Start (TA5)	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 1000:0000:0000:0000:0000:0000:0000:0002:64 was added successfully.	network

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

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

Info event

Warning event which needs attention

Critical event which needs immediate actions to prevent possible failure

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

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

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

- **Clear All the Event Logs:** You can select the respective event and click [Clear] to remove the maintenance event log entry. To clear “All the Event Logs”, first enable Maintenance Event Log in Advance Settings.
- **Export to Excel:** You can export the current maintenance event log to an Excel file.

2.9.5. 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 screenshot shows the BMC Task List interface. The sidebar on the left contains the following menu items: Dashboard, System, Configuration, Remote Control, Maintenance, Firmware Management, Troubleshooting, BMC Reset, Maintenance Event Log, License Activation, and Task List. The main content area features a 'Filter' section with buttons for 'X Running', 'X Completed', and 'X Failed'. Below the filter is a 'Task List' table with the following columns: Health Status, Job, State, Create Time, Progress, Total Duration, and Completed Time. The table currently displays 'No data available' and a pagination indicator '0 / 0'. The footer of the page reads 'Copyright © 2020 Supermicro Computer, Inc.'.

The following information is presented in the table for review.

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

You can filter tasks to view based on task status (Running, Completed, or Failed). The following table shows the 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 SSE-T7132 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 UEFI BIOS Setup utility. 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.



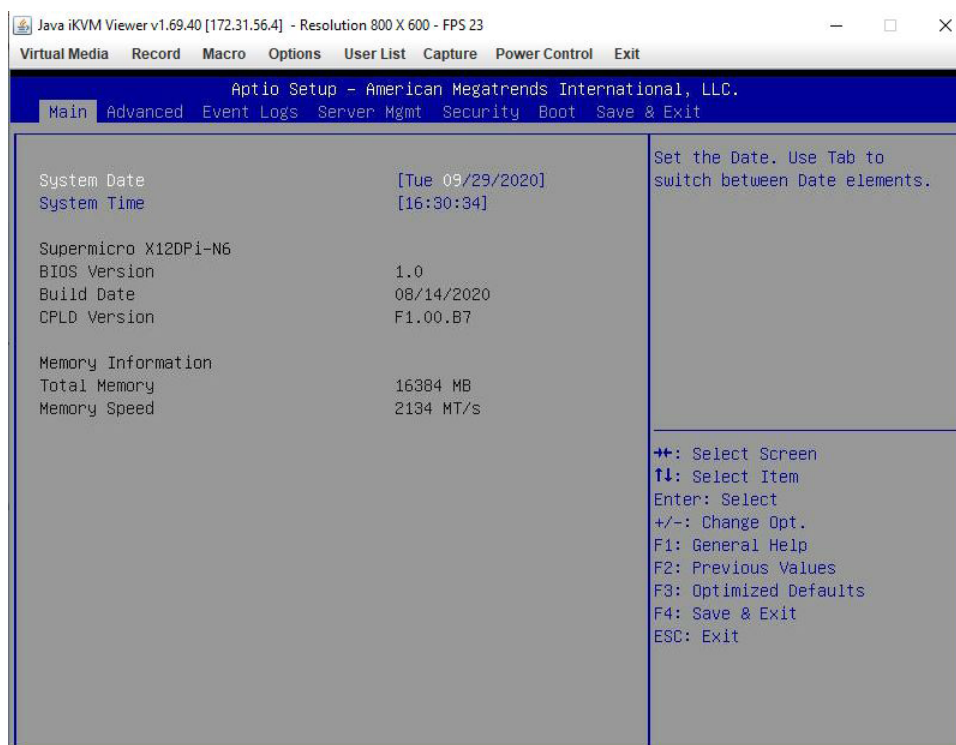
Note: BIOS has default text messages built-in. We retain the option to include, omit, or change any of these text messages. Settings printed in **Bold** are the default values.

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 you first enter the AMI BIOS setup utility, you will enter the Main setup screen. You can always return to the Main setup screen by selecting the Main tab at the top of the screen. The Main BIOS setup screen 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 the 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.

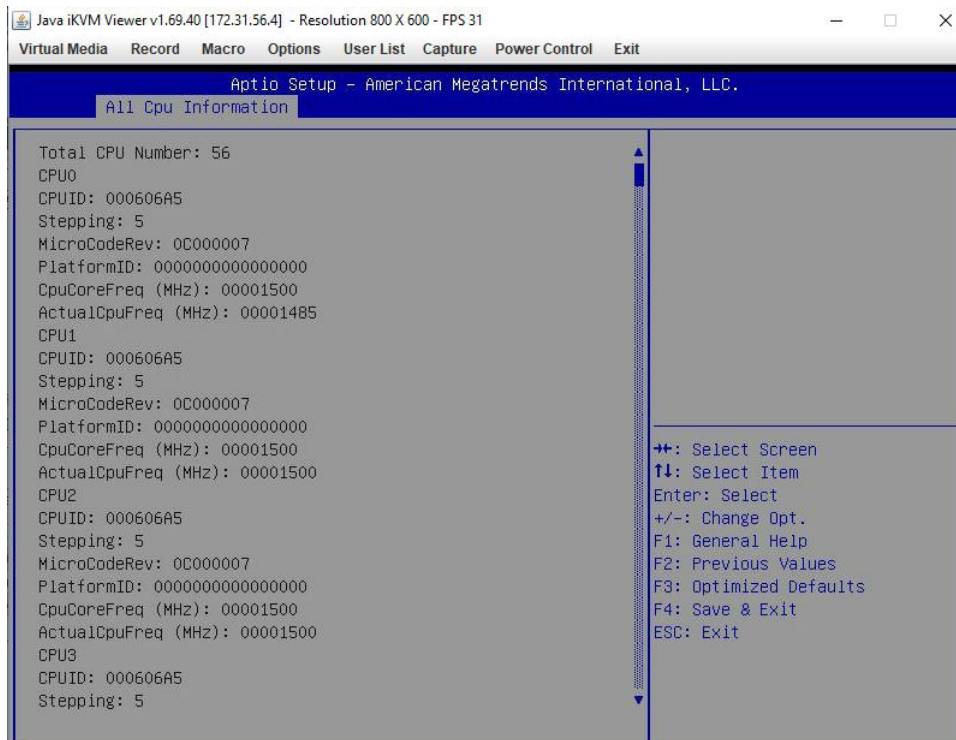
Memory Information

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:



The screenshot shows a Java iKVM Viewer window displaying the Aptio Setup utility. The window title is "Java iKVM Viewer v1.69.40 [172.31.56.4] - Resolution 800 X 600 - FPS 31". The menu bar includes "Virtual Media", "Record", "Macro", "Options", "User List", "Capture", "Power Control", and "Exit". The main window title is "Aptio Setup - American Megatrends International, LLC." and the current screen is "All Cpu Information". The screen displays the following information for 56 CPUs:

```
Total CPU Number: 56
CPU0
CPUID: 000606A5
Stepping: 5
MicroCodeRev: 0C000007
PlatformID: 0000000000000000
CpuCoreFreq (MHz): 00001500
ActualCpuFreq (MHz): 00001485
CPU1
CPUID: 000606A5
Stepping: 5
MicroCodeRev: 0C000007
PlatformID: 0000000000000000
CpuCoreFreq (MHz): 00001500
ActualCpuFreq (MHz): 00001500
CPU2
CPUID: 000606A5
Stepping: 5
MicroCodeRev: 0C000007
PlatformID: 0000000000000000
CpuCoreFreq (MHz): 00001500
ActualCpuFreq (MHz): 00001500
CPU3
CPUID: 000606A5
Stepping: 5
```

On the right side of the screen, there is a legend for navigation keys:

```
++: Select Screen
↑↓: Select Item
Enter: Select
+/-: Change Opt.
F1: General Help
F2: Previous Values
F3: Optimized Defaults
F4: Save & Exit
ESC: Exit
```



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

▶AST2600 Super IO

The following Super IO information will display:

- Super IO Chip AST2600

▶Serial Port 1 Configuration

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

Serial Port 1

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

Device Settings

This item displays the status of a specified serial part.

Change Settings

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

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

▶Serial Port 2 Configuration

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

Serial Port 2

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

Device Settings

This item displays the status of a specified serial part.

Change Settings

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

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

► Serial Port Console Redirection

COM1 Console Redirection

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

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

► COM1 Console Redirection Settings

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

COM1 Terminal Type

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

COM1 Bits Per Second

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

COM1 Data Bits

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

COM1 Parity

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

as a parity bit to be sent along with the data bits. Select Space to add a Space as a parity bit to be sent with the data bits. The options are **None**, Even, Odd, Mark, and Space.

COM1 Stop Bits

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

COM1 Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffering the 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 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 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 Console Redirection Settings

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

COM2 Terminal Type

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

COM2 Bits Per Second

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

COM2 Data Bits

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

COM2 Parity

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

COM2 Stop Bits

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

COM2 Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffering the 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 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 the redirection of Legacy OS and Legacy OPRM messages. The options are **COM1** and SOL/COM2.

EMS (Emergency Management Services) Console Redirection

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

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

► EMS Console Redirection Settings

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

Out-of-Band Mgmt Port

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

Terminal Type

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

Bits Per Second

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

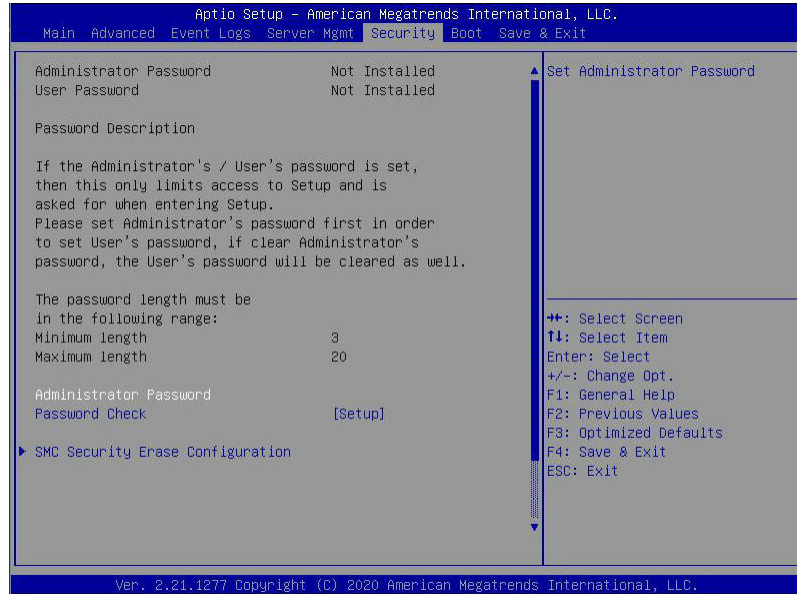
Flow Control

Use this feature to set the flow control for Console Redirection to prevent data loss caused by buffering the 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

4.4 Security

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



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.

Administrator Password

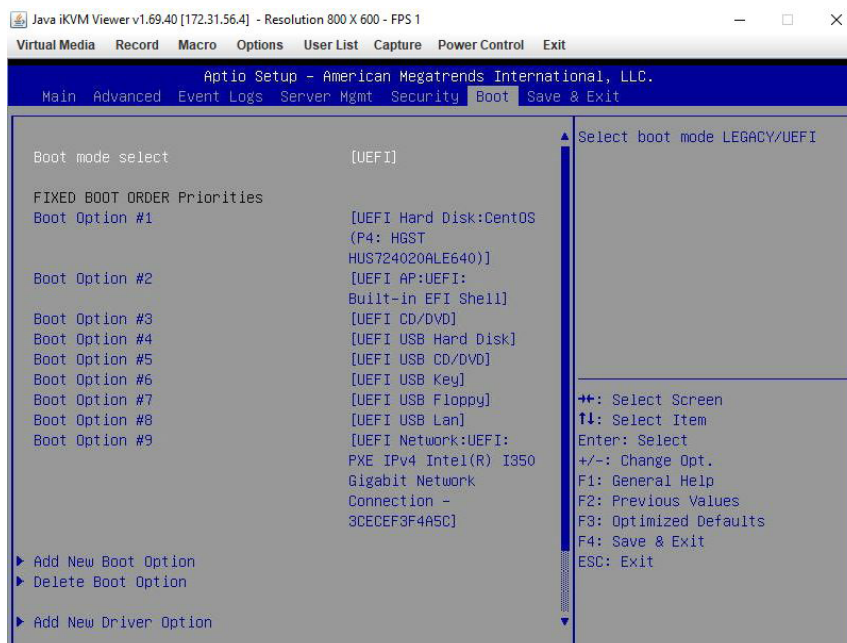
Press Enter to create a new, or change an existing, administrator password.

User Password

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

4.5 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 the Legacy boot order has failed. The options are **Disabled** and Enabled.

Fixed Boot Order Priorities

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

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

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

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

▶ Delete Boot Option

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

Delete Boot Option

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

▶ UEFI Application Boot Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

▶ Network Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

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

► Add New Boot Option

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

Add Boot Option

Use this item to specify the name of 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

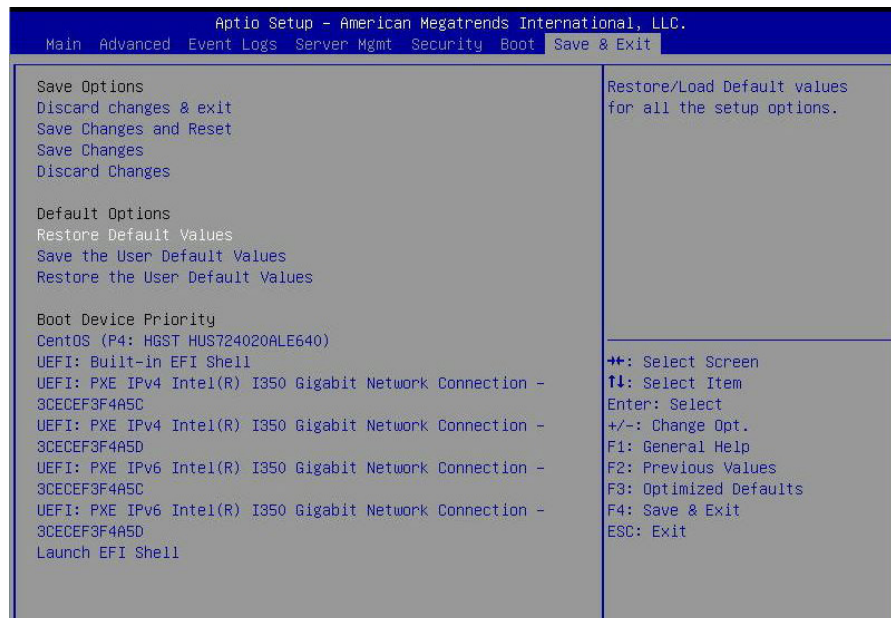
► Hard Disk Drive BBS Priorities

This feature sets the system boot order of detected devices.

- Boot Option #1

4.6 Save & Exit

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



Save Options

Discard Changes and Exit

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

Save Changes and Reset

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

Save Changes

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

Discard Changes

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

Default Options

Restore Optimized Defaults

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

Save As User Defaults

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

Restore User Defaults

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

Boot Override

Listed in this section is 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

A.1 Overview

This user's guide provides detailed information on how to update Supermicro BMC firmware on SSE-T7132 series motherboards using BMC WEB GUI.

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 following the prompts on the screen.

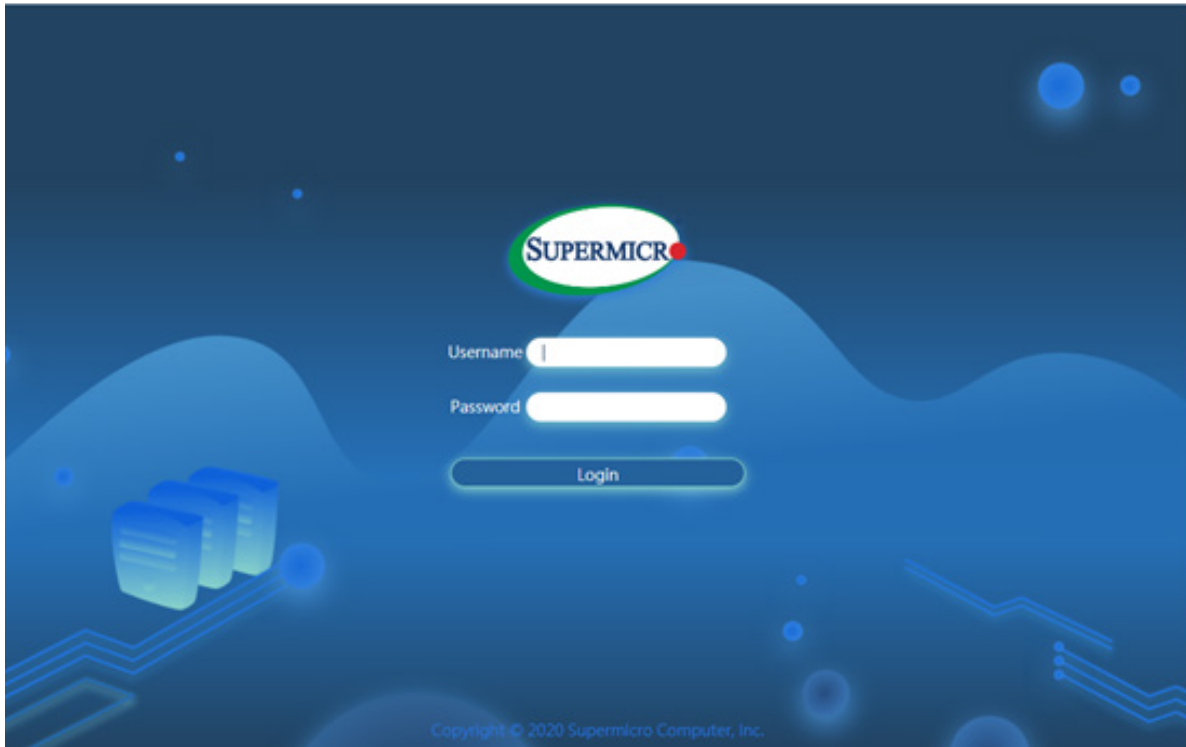


Figure 1: BMC Firmware Web User Login



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

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

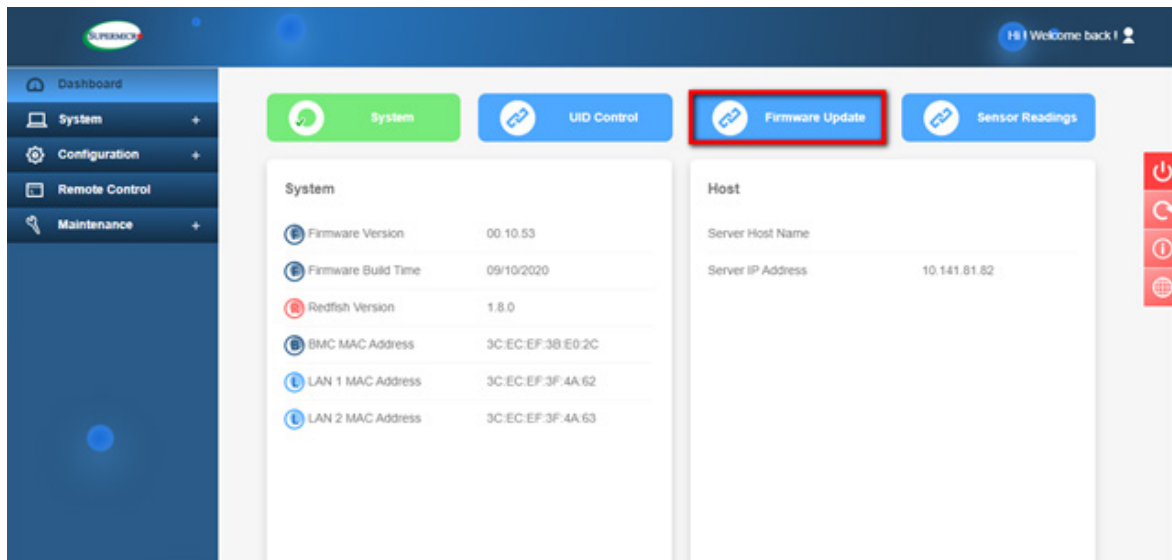


Figure 2: BMC Firmware Update Dashboard

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

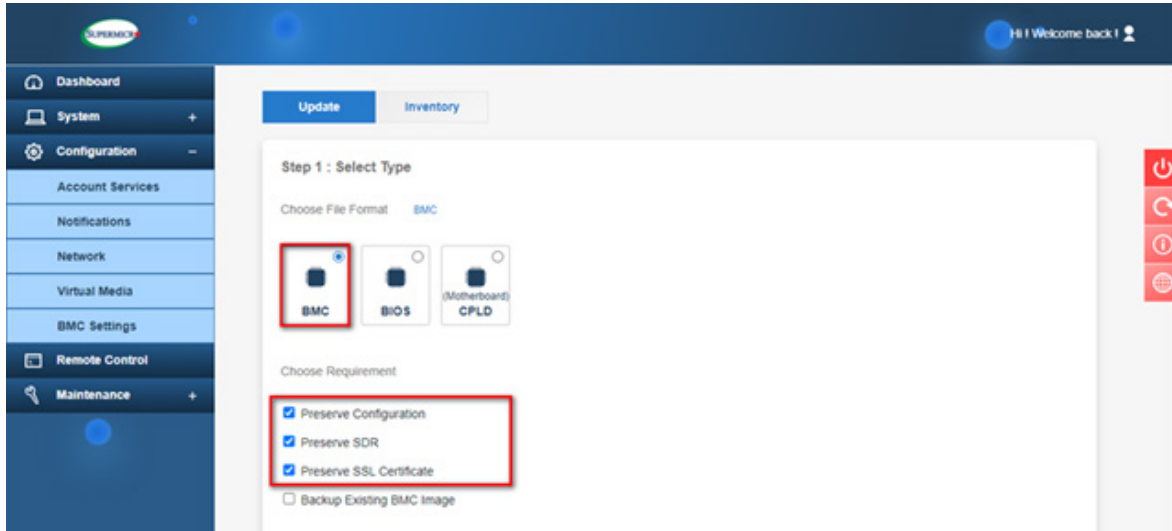


Figure 3: BMC Firmware Update Default Setting

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

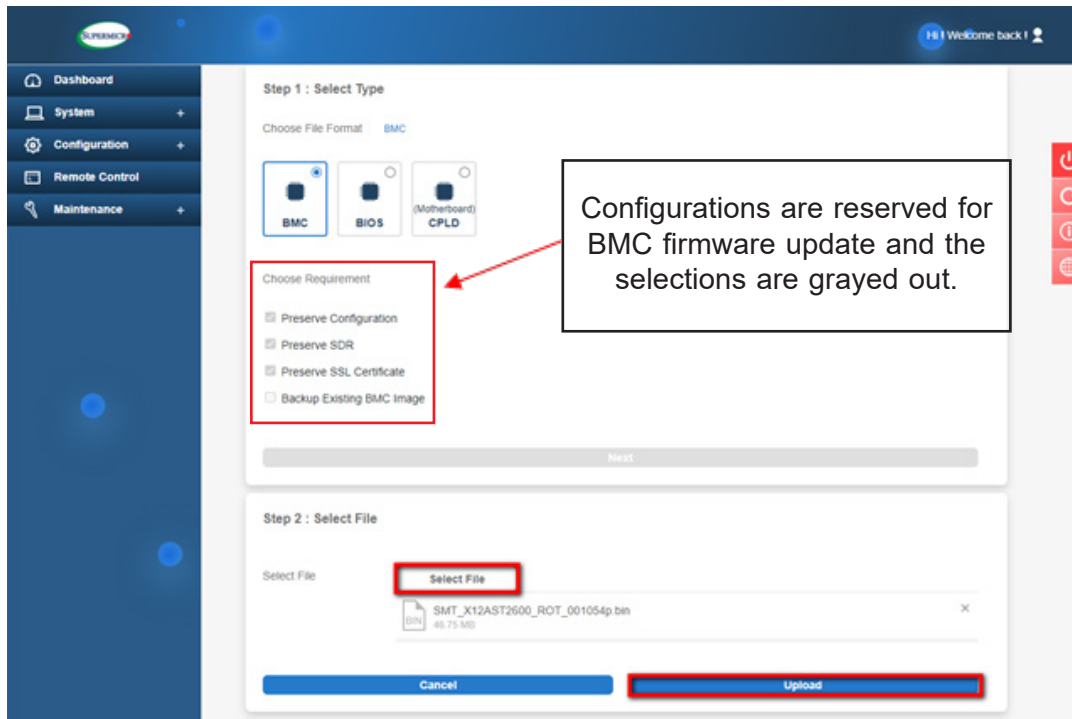



Figure 4: Select and Upload New BMC Firmware File

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

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

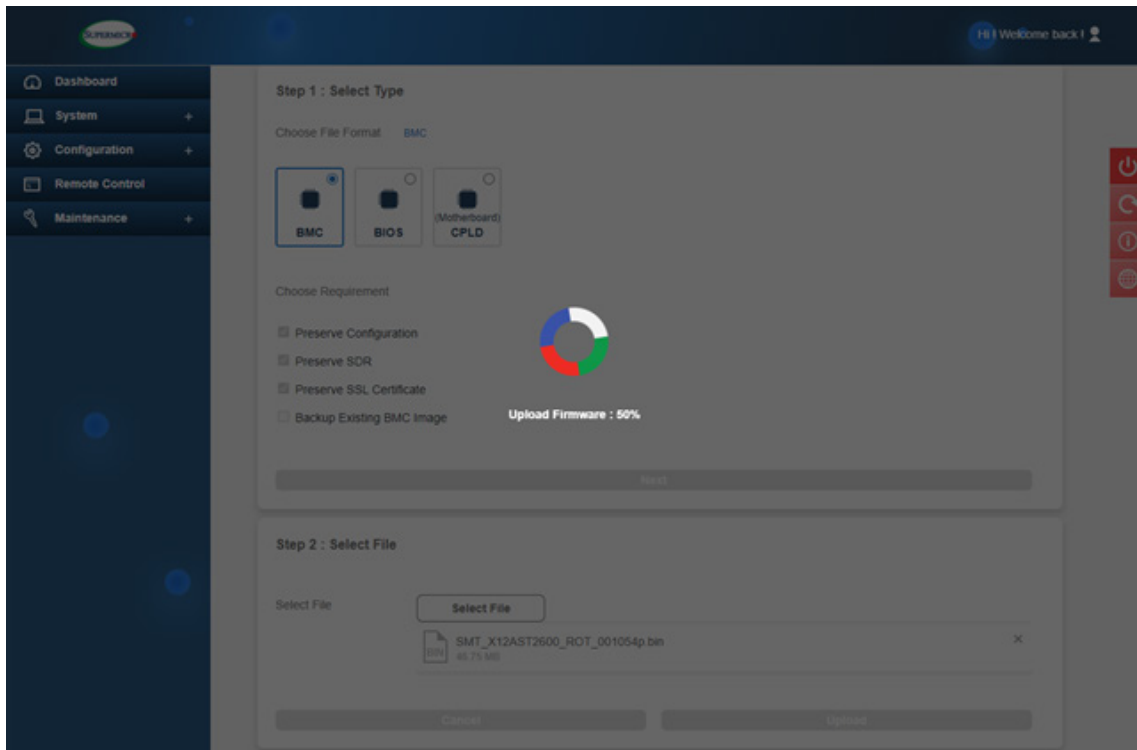


Figure 5: New BMC Firmware Uploading

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

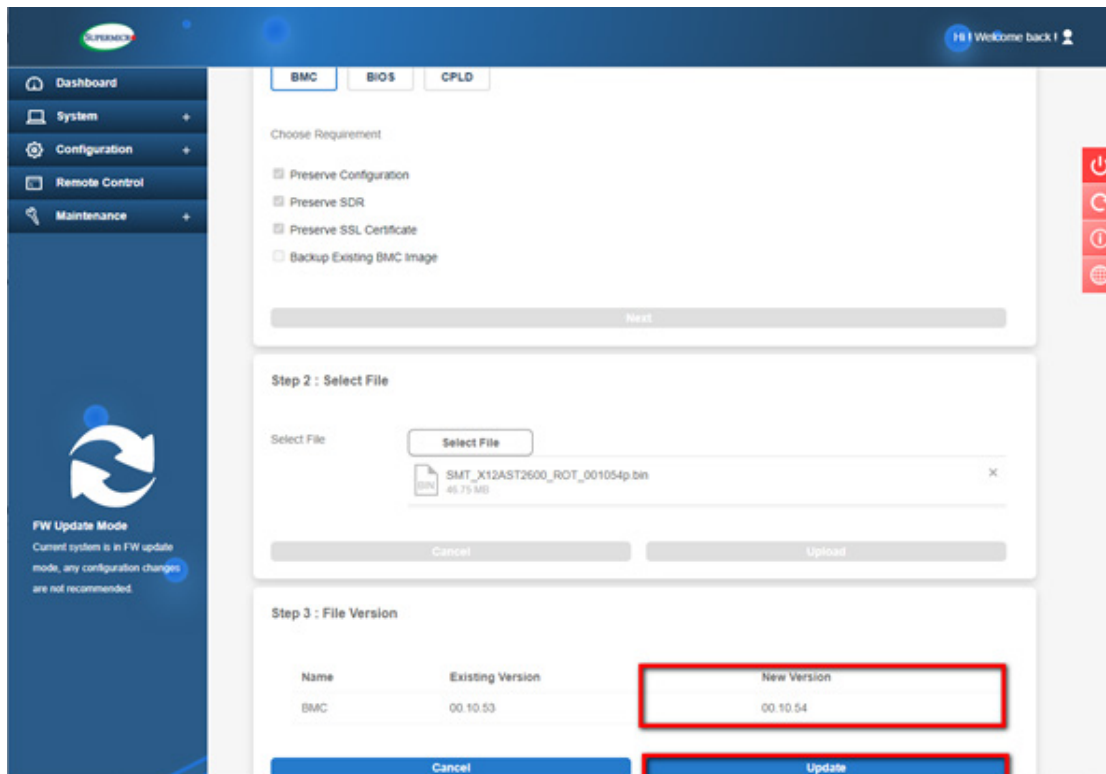


Figure 6: Verify the New BMC Firmware Version

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

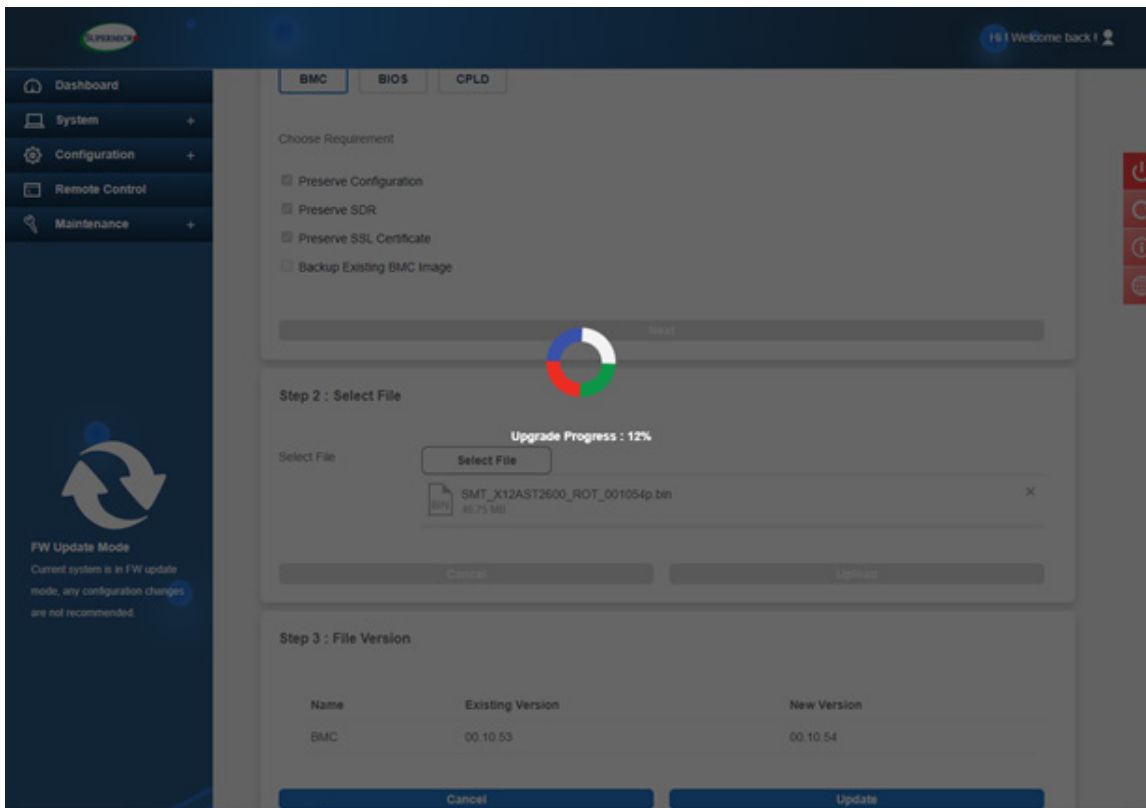


Figure 7: BMC Firmware Updating in Progress

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

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

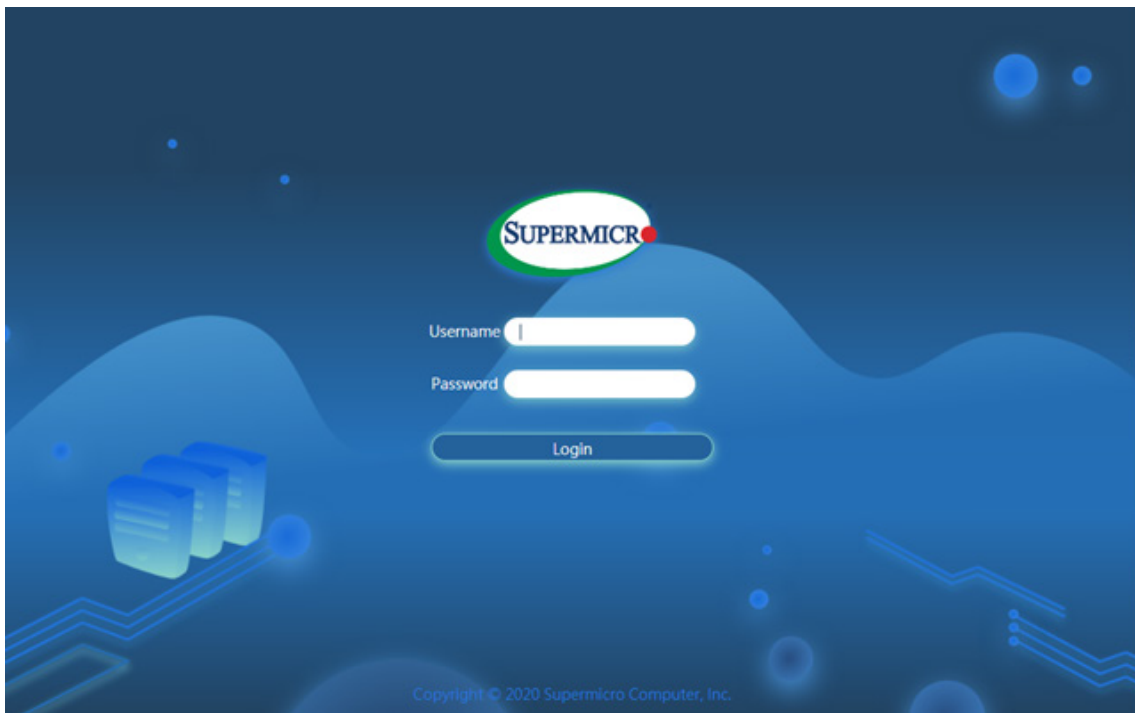


Figure 8: BMC Firmware Web User Login

Appendix B

Introduction to SMASH

B.1 Overview

The SMASH (System Management Architecture for Server Hardware) platform, developed by Distributed Management Task Force, Inc. (DMTF), delivers a host of architecture-based and industry-standard protocols that will allow IT professionals to simplify the task of managing multiple network systems in a data center. This platform offers a simple, intuitive solution to manage heterogeneous servers in a web environment regardless of differences in hardware, software, OS, or network configuration. It also provides the end-users and the ISV community with interoperable management technology for multi-vendor server platforms.

How SMASH works

SMASH simplifies typical SMASH scripts by reducing commands to simple verbs. Although designed to manage multi-servers as a whole, SMASH can address individual components in a specific machine by using the SSH command-line protocol. Even when multiple processors, add-on cards, logical devices, and cooling systems are installed in a server, SMASH can be directed at a particular component in the server. A manager can use a text console to access, monitor, and manage all servers that are connected to the same SSL connection. This platform can be programmed to periodically check all sensors in all machines or monitor a particular component in a specific server at any time. By adjusting the scope of tasks and the schedules of monitoring, SMASH allows the IT professionals to effectively manage multi-system clusters, minimize power consumption, and achieve system management efficiency.

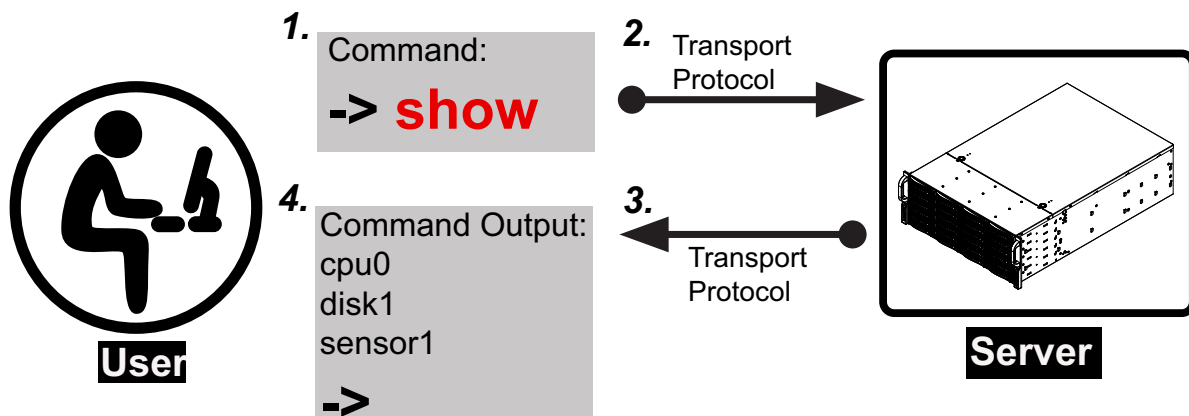


Figure 1 SMASH-CLP User Interface

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

You can initiate SMASH automatically by connecting the BMC (Baseboard Management Controller) via the Secure Shell protocol (SSH) from a client machine.

To connect from a Linux machine

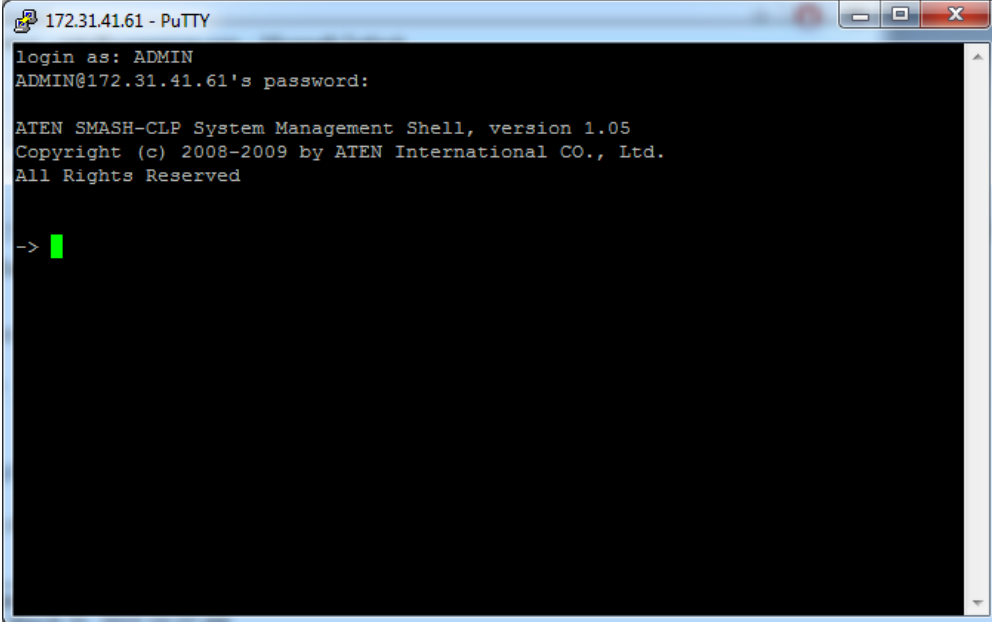
1. Use 'ssh<BMC ip address>'.
2. Enter the password.

To connect from other machines

1. Use a terminal emulator application such as *Putty*.
2. Enter the *BMC IP* address in the terminal emulator application.
3. Choose *ssh* as the connection type
4. Enter the password at the prompt.
5. If successfully logged in, the SMASH prompt will be displayed.

B.5 SMASH-CLP Main Screen

After successfully logging into the SSL network, the SMASH Command Line Protocol Main screen will display as shown below.

A screenshot of a PuTTY terminal window titled "172.31.41.61 - PuTTY". The terminal displays the following text:

```
login as: ADMIN
ADMIN@172.31.41.61's password:

ATEN SMASH-CLP System Management Shell, version 1.05
Copyright (c) 2008-2009 by ATEN International CO., Ltd.
All Rights Reserved


-> █
```

The terminal window has a black background with white text. A green cursor is visible at the end of the prompt line. The window title bar shows standard Windows window controls (minimize, maximize, close).

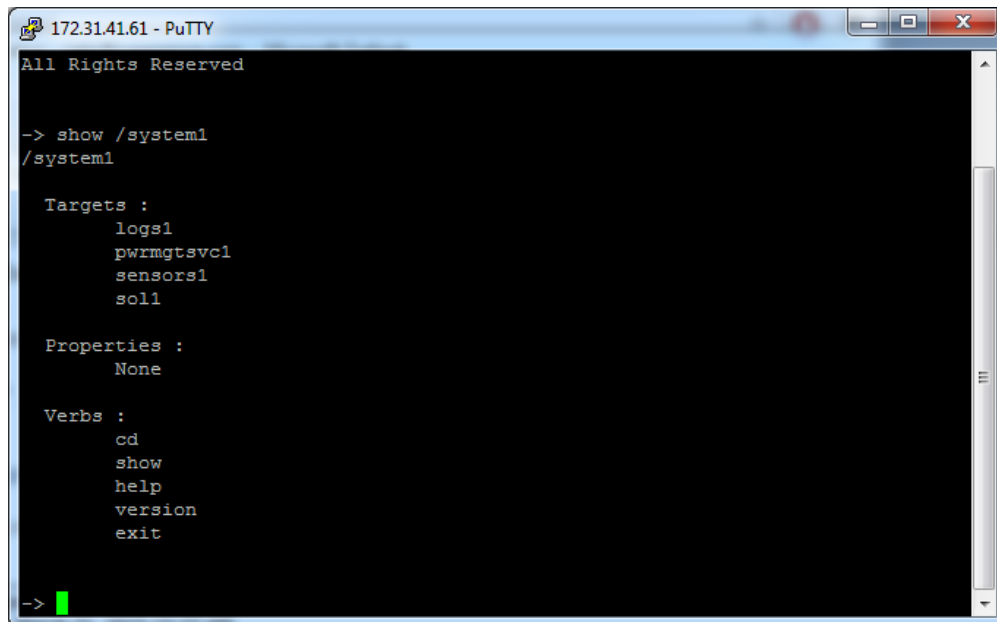
Figure 2 SMASH-CLP Main Screen

B.6 Using SMASH for System Management

After you have familiarized yourself with the SMASH commands, you will be able to use these commands to manage the system. To properly manage the network system, be sure to follow the instructions below.

 **Note:** Make sure that the format of all commands are compliant with the DMTF specification, which is "<Verb> [<option>] [<target>] [<properties>]", where:

- A **Verb** means a *command*.
- An **Option** works according to the definition of a command given in Section B-7: Definitions of Command Verbs.
- A **Target** is a managed device.
- **Properties** are the specific attributes that you want to assign to a target machine or to get from a target machine.



```
172.31.41.61 - PuTTY
All Rights Reserved

-> show /system1
/system1

Targets :
  logs1
  pwrmgtsvc1
  sensors1
  sol1

Properties :
  None

Verbs :
  cd
  show
  help
  version
  exit

-> |
```

Figure 3 Using SMASH for System Management

B.7 Definitions of Commands Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow you to issue commands to a target system to perform certain tasks. For example, the verbs supported by the *admin* target group include *cd*, *help*, *load*, *dump*, *create*, *delete*, *exit*, *version*, *show*, etc.

- ***cd***

The command verb *cd* is used to navigate to a specific target address using the SSL protocol. For example, issuing the command *cd/admin1* will direct you to the target *admin* (AdminDomain).

- ***show***

The command verb *show* is used to display the properties and the contents of a target, a group of targets, a sub-groups of the target(s). Properties, contents, and supported operations related to the target, the group of targets, or their sub-targets will be displayed.

- ***exit***

The command verb *exit* is used when you want to exit from a SMASH session or close a session.

- ***help***

The command verb *help* is used when you want to get helpful hints or information on a context-specific item. This command has the same function as the *help option* listed for the target group.

- ***Version***

Use the command verb *version* to display the CLP version used in a specific machine.

- ***set***

Use the command verb *set* to assign a set of values to the properties of a target machine.

- ***start***

The command verb *start* is used to turn on the power control, to start a process, or to change an operation state from a lower level to a higher level in a system.

- ***stop***

The command verb *stop* is used to turn off the power, stop a process, or change an operation state from a higher level to a lower level.

- ***reset***

The command verb *reset* is used to enable or disable the power control of or the processes of the machine.

- ***delete***

The command verb *delete* is used to delete or destroy an entry or a value previously entered. It can only be used in a specific target as defined according to the SAMSHCLP Standards.

- ***load***

The command verb *load* is used to move a binary image file from a URI source to the MAP. This command will achieve different results depending on the setting of a target system, and how the verb *load* is defined in the DSP specification used in the system.

- ***dump***

The command verb *dump* is used to move a binary image file from the MAP to a URI source. This command will achieve different results depending on the setting of a target system, and how the verb *dump* is defined in the DSP specification implemented in the system.

- ***create***

The command verb *create* is used to create a new address entry or a new item in the MAP. It can only be used in a specific target as defined in the SMASH profile or in MAP specifications.

B.8 SMASH Commands

The following table provides the definitions and descriptions of SMASH commands. The most useful commands are *show* and *help*, which will provide you with information on how to navigate through the SSL network connection.

Option Name	Short Form	Definition	Notes
-all	-a	Instructs a command verb to perform all tasks possible	None
-destination <URI>	None	Indicates the final location of an image or selected data	URI or SM instance address
-display	-d	Selects data that you wish to display	This can generate multiple query results
-examine	-x	Instructs the Command Processor to examine a command for syntax or semantic errors without executing it	None
-force	-f	Instructs the verb to ignore any warnings triggered by default but go ahead executing the command instead	None
-help	-h	Displays all information and documentation regarding the command verb	None
-keep <m[s]>	-k	Sets a time period to hold and keep the Job ID and the status of a command	The amount of time set to hold a command Job ID or its status can differ.
-level <n>	-l	Instructs the Command Processor to execute the command for the current target and for all target machines within the level specified by you	Levels should be expressed in a natural number or "all".
-Output <args>	-o	Controls the format and the content of a command output. This only supports "format=clpxml" and "format=keyword"	Many variables or factors can affect the outcome of format, language, and level of details of the output.
-Source <URI>	None	Indicates the location of a source image or a target	URI or SM Instance Address
-Version	-v	Displays the version of the command verb	None
-Wait	-w	Instructs the Command Processor to hold the command response or query result until all spawned jobs are completed.	None

Table 1 SMASH Commands

B.9 Standard Command Options

The following table lists the standard command options.

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

Table 2 Standard Command Options

B.10 Target Addressing

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

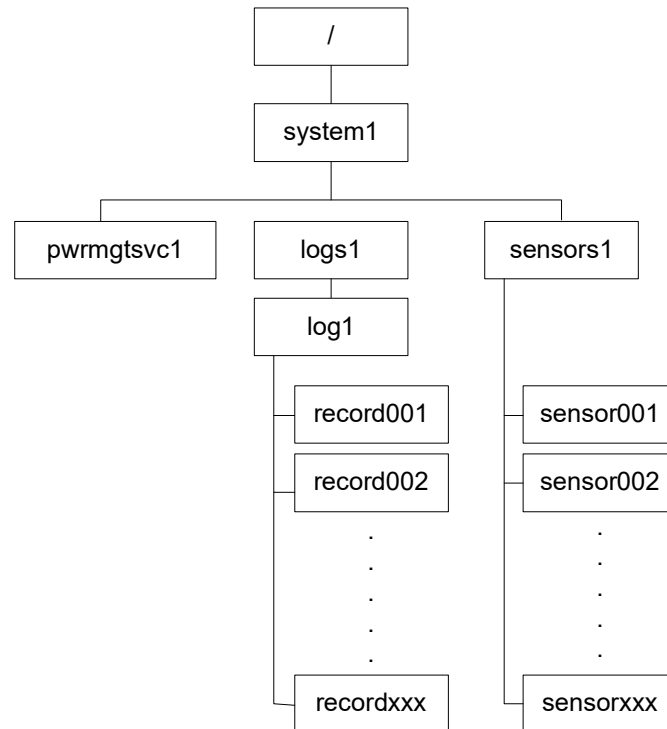


Figure 4 Target Addressing Diagram

Terms Used in the Target Addressing Diagram

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

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

Appendix C

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 you to manage remote user authentication and accounting. It authenticates users trying to establish a network connection, authorizes them to access the network, and accounts for those accessing the network. Before running RADIUS, you need 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. You 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
```

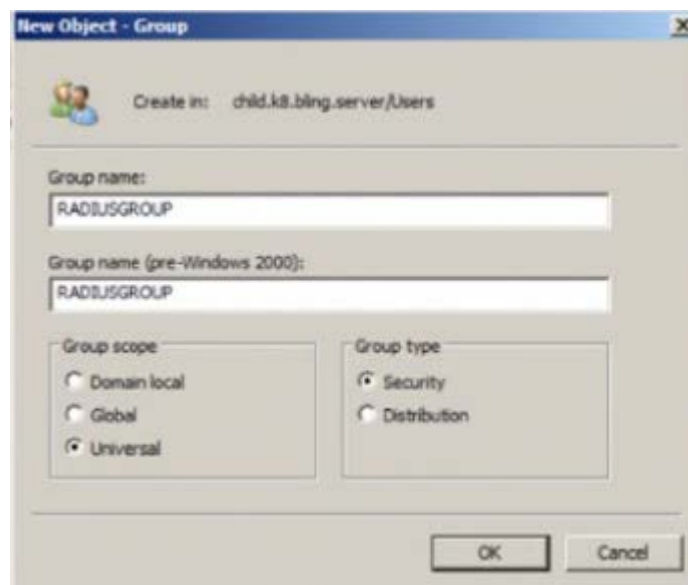
C.5 Adding Roles in Windows

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:
PME

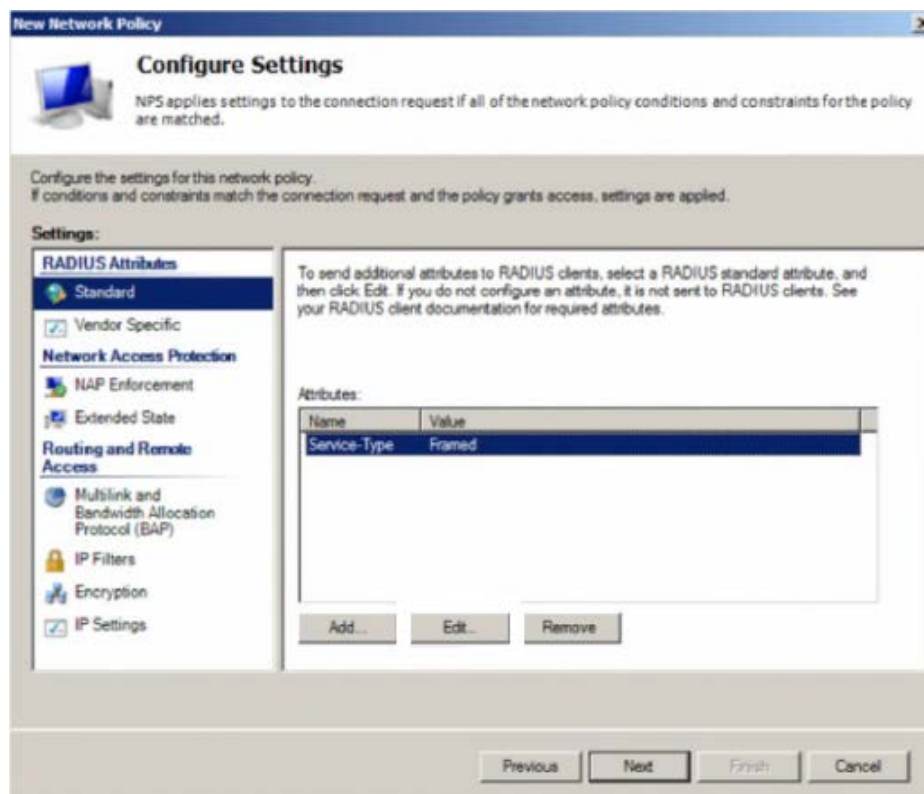
Network connection method
Select the type of network access server that sends the connection request to NPS. You can select either the network access server type or Vendor specific, but neither is required. If your network access server is an 802.1X authenticating switch or wireless access point, select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

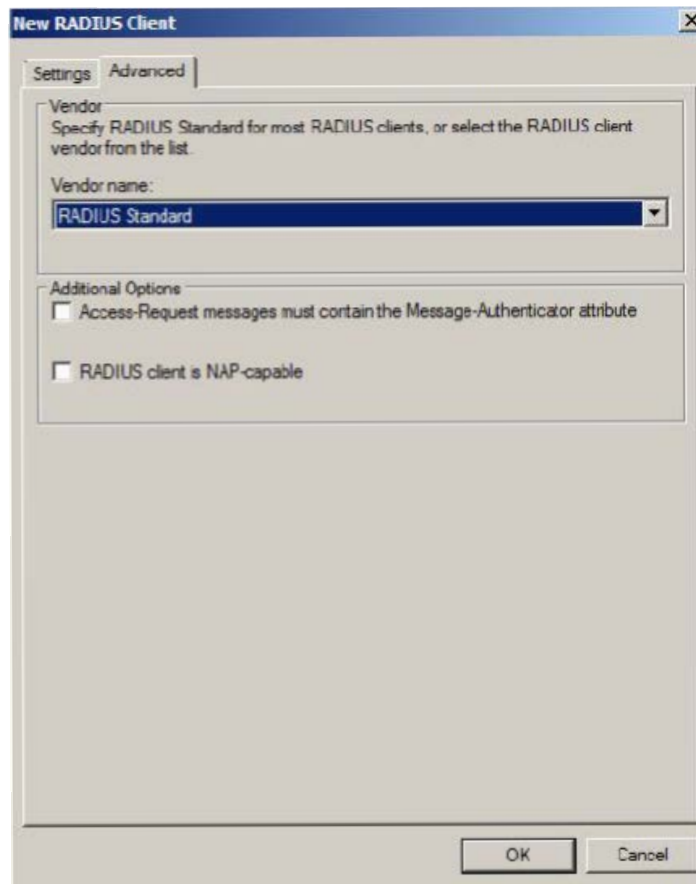


Adding a Vendor Specific

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.



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.

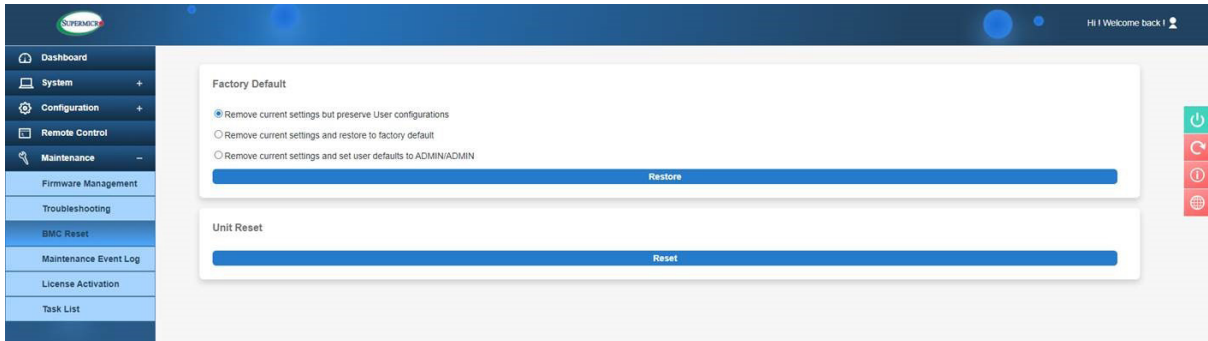
Effective as of January 1, 2020, each new Supermicro motherboard will come with two labels that contain a unique password assigned to that motherboard. One unique password label will be placed near the BMC (Baseboard Management Controller) chip and/or close to the MB serial number label. This label is 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 username and password for subsequent logins.

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

D.2 Restore Factory Default

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



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

D.3 Change All Unique Passwords Using Script

Due to possible different operating environments, you are given the option to modify the provisioning script and unique passwords.

D.4 Frequently Asked Questions

Question: What if a password sticker is lost? How do I get my unique password?

Answer: There is a minimum of two stickers on each product. One sticker will be placed on the motherboard and a second sticker will be on the server chassis. At this time, Supermicro has not encountered any instances of lost or misplaced stickers. In the rare case of such incidents, please contact the direct sales support to receive a soft copy of the password.

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

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

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

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

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

Answer: We will provide a sample script with documentation. Of course, the operating environment may change from customer to customer. It is the end user's responsibility to modify the provisioning script.

Question: Will this law affect customers in Europe and Asia where shipments are from the Netherlands or Taiwan manufacturing facilities?

Answer: Since our standard SKUs will be rendered from California, we keep the same design across our portfolio, so it gives a unified experience across all platforms.

Question: Will customers purchasing Supermicro products from an OEM vendor be subject to the preprogrammed password initiative?

Answer: Yes, customers will still receive products with a unique preprogrammed password. You will be able to change the preprogrammed password yourselves or you can work with your OEM vendor to make the necessary password updates.

Question: I am purchasing multiple systems for my data center. How do I change all of the unique preprogrammed passwords for these systems in an efficient manner to support my operations?

Answer: Please contact the systems integrator (SI) or value-added reseller (VAR) to assist you in this process.

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

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

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

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

(Disclaimer Continued)

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