IPMI

Intelligent Platform Management Interface

User's Guide

Revision 1.1

The information in this user's guide has been carefully reviewed and is believed to be accurate. The vendor 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 web site 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: Refer to Supermicro's web site for FCC Compliance Information.

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.

Manual Revision 1.1

Release Date: October 23, 2019

Printed in the United States of America

Preface

About this User's Guide

This user's guide is written for system integrators, IT professionals, and knowledgeable end users who intend to configure the IPMI settings supported by the ASpeed AST2400/AST2500 Baseboard Management Controller embedded in Supermicro motherboards. It provides detailed information on how to configure the IPMI settings supported by the AST2400/AST2500 controller.

User's Guide Organization

Chapter 1 provides an overview on the ASpeed AST2400/AST2500 controller. It also introduces the features and the functionalities of IPMI.

Chapter 2 provides detailed instructions on how to configure the IPMI settings supported by the AST2400/AST2500 controller.

Chapter 3 provides the answers to frequently asked questions.

An Important Note to the User

For documents concerning utility support such as Redfish, SMCIPMITool, SUM, SSM, IPMICFG, SPM, SuperDoctor, BIOS, RSD, 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 IPMI screens shown on your computer may or may not look exactly like the screen shown in this user's guide.

Conventions Used in This User's Guide

Pay special attention to the following symbols for proper IPMI configuration.

Warning: Important information given to avoid IPMI configuration errors.

Note: Additional information given to ensure correct IPMI configuration setup.

Contacting Supermicro

Headquarters

Address:	Super Micro Computer, Inc. 980 Rock Ave. San Jose, CA 95131 U.S.A.
Tel:	+1 (408) 503-8000
Fax:	+1 (408) 503-8008
Email:	marketing@supermicro.com (General Information) support@supermicro.com (Technical Support)
Website:	www.supermicro.com

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	sales@supermicro.nl (General Information) support@supermicro.nl (Technical Support) rma@supermicro.nl (Customer Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	support@supermicro.com.tw
Website:	www.supermicro.com.tw

Table of Contents

Chapter 1

Introduction

1-1 Introduction to the IPMI Platform

The Intelligent Platform Management Interface (IPMI) 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.

IPMI operates independently from the operating system. When used with an IPMI Management utility installed on the motherboard, the ASpeed AST2400/AST2500 BMC Controller will connect the PCH to other onboard components, providing remote network interface via serial links. With the AST2400/AST2500 controller and the IPMI firmware built in, the Supermicro motherboard allows the user 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 AST2400/2500 BMC Controller

The ASpeed AST2400 Baseboard Management Controller (BMC) is designed to interface with the host system via PCI-Express connections to communicate with the graphics core for X10 series motherboards. Designed for the X11 series, the AST2500 connects with the host system via PCI-Express Gen2 x1 bus to communicate with the graphics core. Both AST2400 and 2500 support a 64-bit 2D Graphics Accelerator with 32 bit memory sandpace and 16-bit I/O space.

The AST2400 provides a 2.5GHz PCI-Express interface. The AST2500 supports PCI-Express 2.0, which is compliant with PCI-Express Base Spec. Revision 2.0. The PCI-E bus controller connects to the VGA Controller that allows for direct communication with the 2D Graphics Engine, SPI Host Controller, and P2A Bridge.

The ASpeed AST2400 and 2500 support USB 1.1 and 2.0 for remote KVM emulation and provide LPC interface support to control Super IO functions. Both ASpeed AST2400 and 2500 include Keyboard/Video/Mouse Redirection (KVMR). The BMC is connected to the network via an external Ethernet PHY module or a shared NCSI connection.

A. AST2400 DDR2/DDR3 Memory Interface

The AST2400 controller supports DDR2/DDR3 SDRAM memory with a speed of up to 400MHz and 512 MB of memory. It includes an external 16-bit DDR2/DDR3 SDRAM data bus width and an internal 64-bit DRAM data bus width. The following DDR2 DRAM types are supported: 32MBx16, 64Mbx16, 128MBx16, and 256MBx16. The AST2400 controller also supports Error-Correction Check (ECC) with no extra external memory cost when ECC is enabled.

B. AST2500 DDR3L/DDR4 Memory Interface

The AST2500 controller supports DDR3L/DDR4 SDRAM memory with a speed of up to 800MHz and 1GB of memory. It includes an external 16-bit DDR3L/DDR4 SDRAM data bus width and an internal 128-bit DRAM data bus width. Types of DDR3L DRAM supported by the controller include: 64MBx16, 128MBx16, 256MBx16, and 512MBx16 (stack die). The DDR4 DRAM types supported: are 128MBx16, 256MBx16, and 512MBx16. The AST2500 controller also supports Error-Correction Check (ECC) with no extra external memory cost when ECC is enabled.

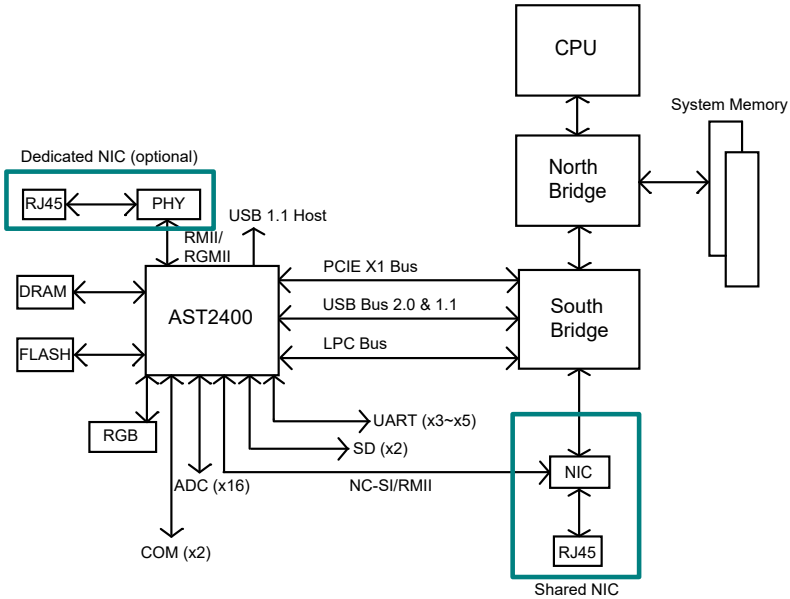
1-3 Supermicro IPMI Features

1. Remote KVM (graphics) console
2. Virtual Media and ISO images
3. Remote server power control
4. Remote Serial over LAN (text console)
5. Event Log support
6. Automatic Notification and Alerts (SNMP and email)
7. Hardware Monitoring
8. Overall health display on the main page
9. Out of band management through shared or dedicated LAN
10. Option to change LAN connection interface at Runtime
11. VLAN
12. RMCP & RMCP+ protocols supported
13. SMASH/CLP
14. Secure command line interface (SSH) and Telnet
15. WSMAN and WS-CIM

16. RADIUS authentication support
17. Secure browser interface (Secure socket layer - SSL support)
18. Lightweight Directory Access Protocol (LDAP) supported
19. DCMI 1.0 support
20. Backup and restore the configuration file
21. Factory defaults from web support
22. Video quality settings
23. Record video and play
24. Server data/information
25. Preview of the remote screen on the main page
26. Update Firmware through browser and OS
27. OS-independent

AST2400 Block Diagram

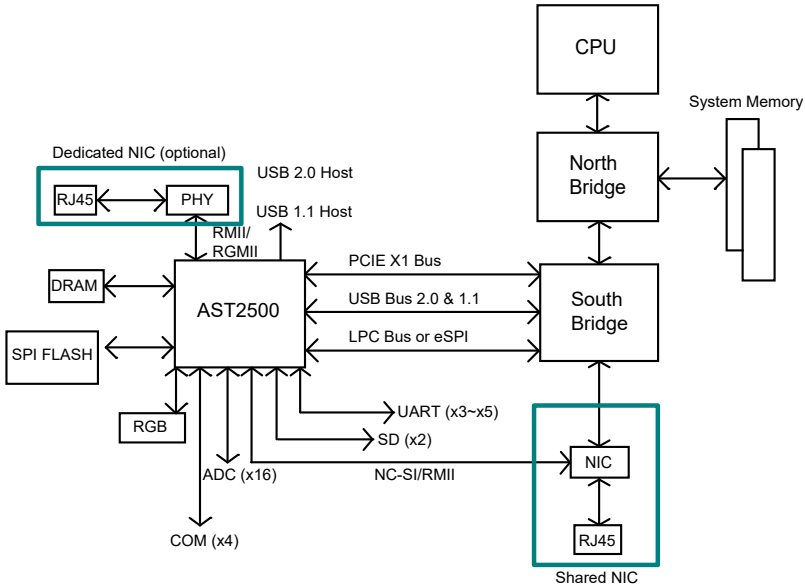
The following diagram represents a typical system setup for the AST2400 controller.



Note: This block diagram is for the X10 series motherboards.

AST2500 Block Diagram

The following diagram represents a typical system setup for the AST2500 controller.



Note: This block diagram is for the X11 series motherboards.

1-4 Software Licenses Available

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

- SFT-OOB-LIC: Basic Out of Band Management
  It covers features such as UEFI BIOS/BMC firmware update and configuration, Mounting ISO images, asset info, and many more.
- SFT-SPM-LIC: Advanced Power Management
  It can be used for SPM tool (Supermicro Power Manager).
- SFT-DCMS-Single: System Management Suite
  It covers above two license SKU and all enterprise features such as Raid Management, Advanced Redfish APIs, NIC FW management, and many more.
- SFT-DCMS-SVC-KEY: Call-Home Support

Please refer following comparison chart for more info:

Features	Standard Package	SFT-OOB-LIC	SFT-DCMS-Single
Feature Updates and Support	Based on HW Warranty	No Updates	3 Years
Software Integration and Customization**			✓
Call Home through SSM**			✓
Restful APIs through SSM			✓
Unified Hardware Management through SSM			✓
SNMP and SMTP Alerts through SSM			✓
Remote Power Management/Monitoring through SPM			✓
24/7 Health and Power Management			✓
VMware vCenter and SCOM Plugins for SSM			✓
Storage Management (3108 Only)			✓*
OS Deployment (RHEL, CentOS, SLES, Ubuntu, VMWare ESXi)			✓
Compatible with Nagios plug-ins			✓
Disable CPU core function through SPM			✓
Policies of Nodes Management			✓
System Information Monitoring			✓
Service Monitoring : FTP / HTTP / SMTP			✓
OpenStack Plugin for SSM (Roadmap)			✓
OS Deployment for Windows (Roadmap)			✓
RAID Provisioning for 3008 (Roadmap)			✓

Features	Standard Package	SFT-OOB-LIC	SFT-DCMS-Single
Out-of-Band System Checks (System Utilization, Asset Information)		✓	✓
OOB/In-band BIOS Management		✓	✓
OOB/In-band BMC Management		✓	✓*
Getting/Clearing Event Log (scripted)		✓	✓*
TPM Provisioning		✓	✓
Mount/Unmounts ISO images from SAMBA/HTTP (scripted)		✓	✓*
Remote Screenshot Capture		✓	✓
Remote Keyboard Operation		✓	✓
Syslog		✓	✓*
Changing system boot order		✓	✓*
Configuring Mousemode, Fanmode, Radius, AD through APIs		✓	✓*
CIM Management		✓	✓

Features	Standard Package	SFT-OOB-LIC	SFT-DCMS-Single
KVM/JAVA	✓	✓	✓
KVM/HTML5 support	✓	✓	✓*
In-band BIOS updates	✓	✓	✓
BMC FW updates	✓	✓	✓
LDAP/Active Directory	✓	✓*	✓*
Virtual Media	✓	✓	✓*
SNMP and SMTP Alerts through BMC	✓	✓*	✓*
SMASH and CLP Support	✓	✓	✓
VLAN Support	✓	✓	✓*
Event Log	✓	✓*	✓*
SOL	✓	✓	✓
Remote Power Control	✓	✓*	✓*
Hardware Health Monitoring	✓	✓*	✓*
HTTPS	✓	✓*	✓*
Multiple User Profiles	✓	✓*	✓*
IPv6 and IPv4	✓	✓	✓*

(*) Avaliable through Redfish APIs.

(**) Additional SKU is required.

Note: License will be deactivated when IPMI MAC address is changed.

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, RSD, 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 your motherboard supports IPMI.

Chapter 2

Configuring the IPMI Settings

With the ASpeed AST2400/ASpeed AST2500 BMC Controller and the IPMI firmware built in, Supermicro motherboards allow the user to access, monitor, manage and interface with multiple systems from different remote locations. The necessary firmware for accessing and configuring the IPMI settings are available on Supermicro website at http://www.supermicro.com/products/nfo/ipmi.cfm. This section provides detailed information on how to configure the IPMI settings.

2-1 Configuring UEFI BIOS

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

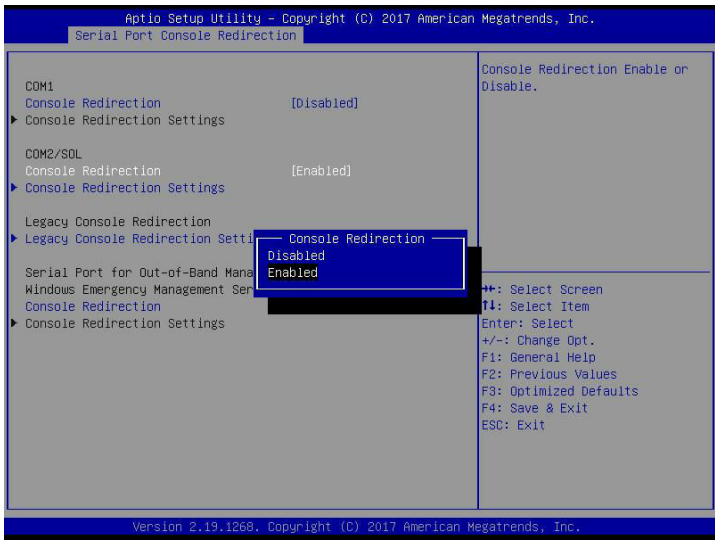
A. Entering and Using the UEFI BIOS

1. During the system bootup, press the <Del> key to enter the UEFI BIOS.

2. To navigate in the UEFI BIOS, use your arrow keys and press <Enter>. To go back to previous screens, press <Esc>.

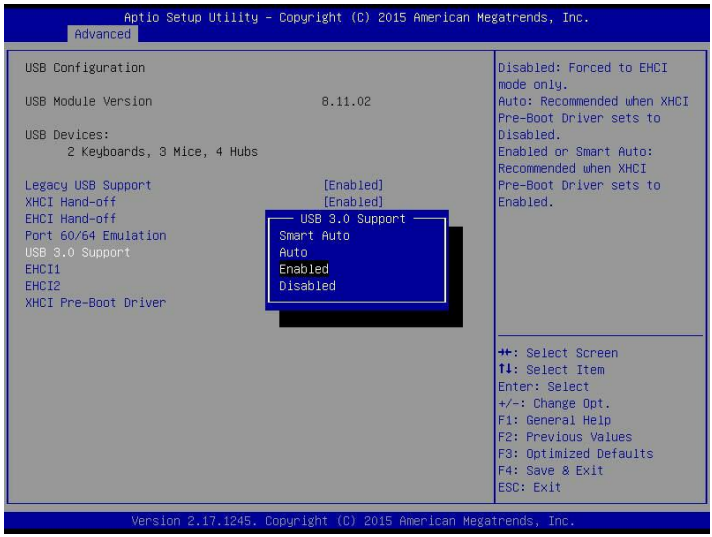
B. Enabling the COM port for SOL (IPMI)

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].



C. Enabling All Onboard USB Ports

1. Select the *Advanced* tab.
2. Select *Chipset Configuration* and press <Enter>.
3. Select *South Bridge* and press <Enter>.
4. Highlight *USB 3.0 Support,* press <Enter> and select [Enabled].

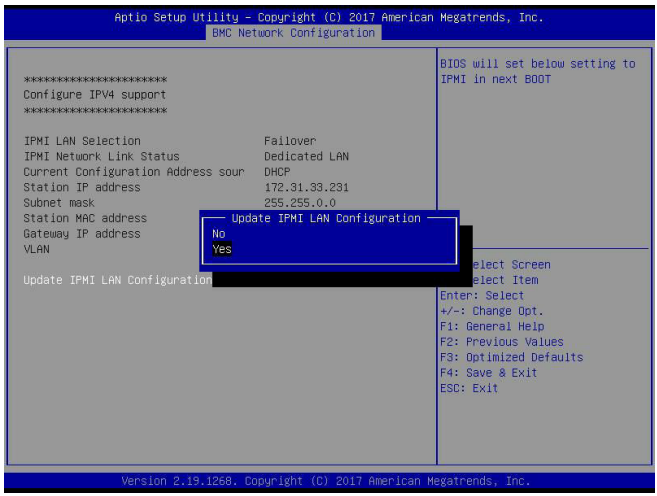


D. Configuring IP Address Using the UEFI BIOS

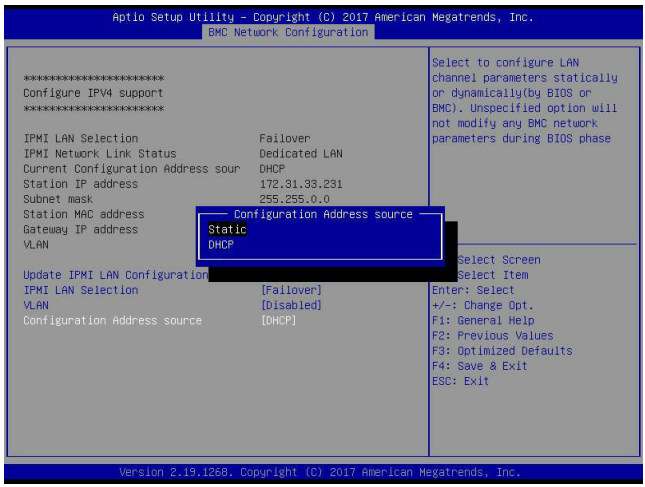
1. Select the *IPMI* tab.

2. Select *BMC Network Configuration and* press <Enter>.

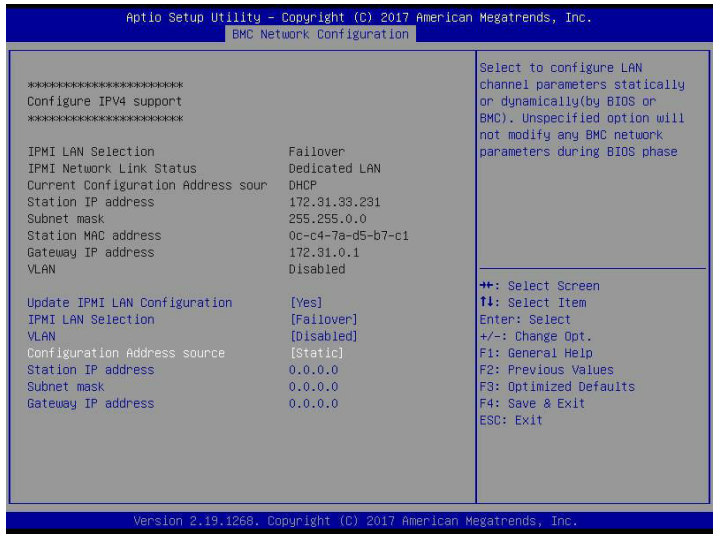
3. Highlight *Update IPMI LAN Configuration,* press <*Enter*> and select [Yes].



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



5.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.



E. Connectiong to IPMI Using the UEFI BIOS

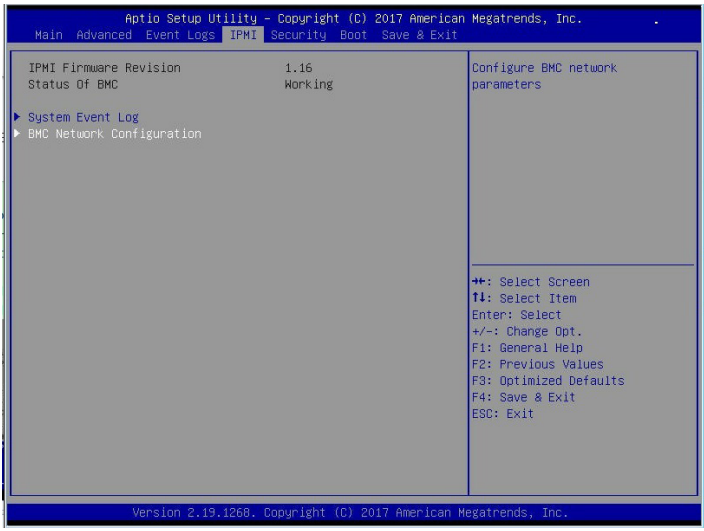
1. Plug Cat 5 cable into Linux Laptop.

2. Plug the other end of the cable into IPMI / SHARED port.

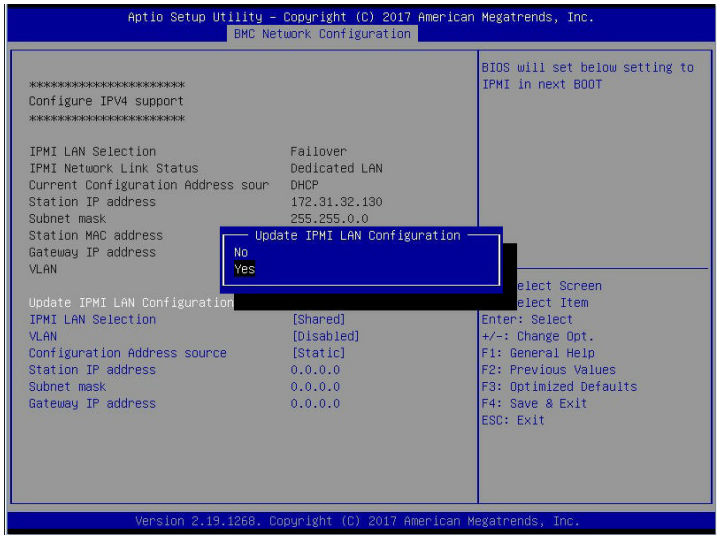
3. In Linux Laptop, configure Network settings for Static IP, and assign IP, such as 192.168.0.3, and subnet, such as 255.255.0.0. (Gateway IP does not matter since there's no router/switch in between.)

4. In the Superserver ending, boot it up, and press DEL key to enter into UEFI BIOS setup.

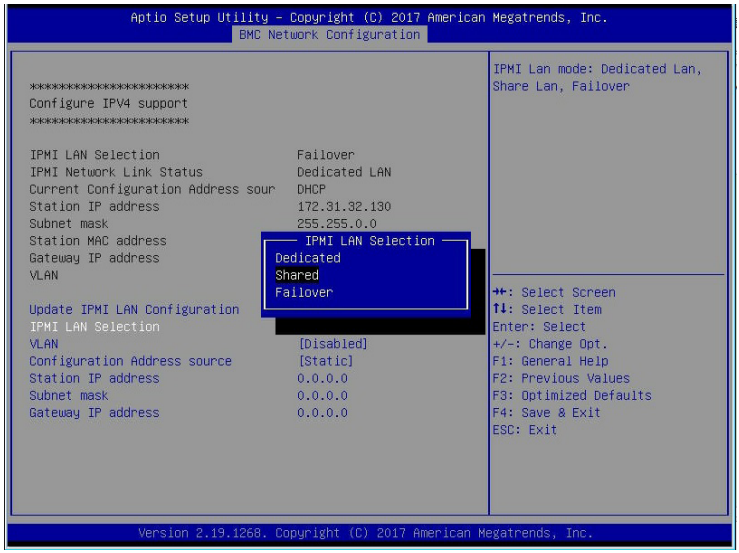
5. Use arrow key to navigate to <IPMI>, and select <BMC Network Configuration>.



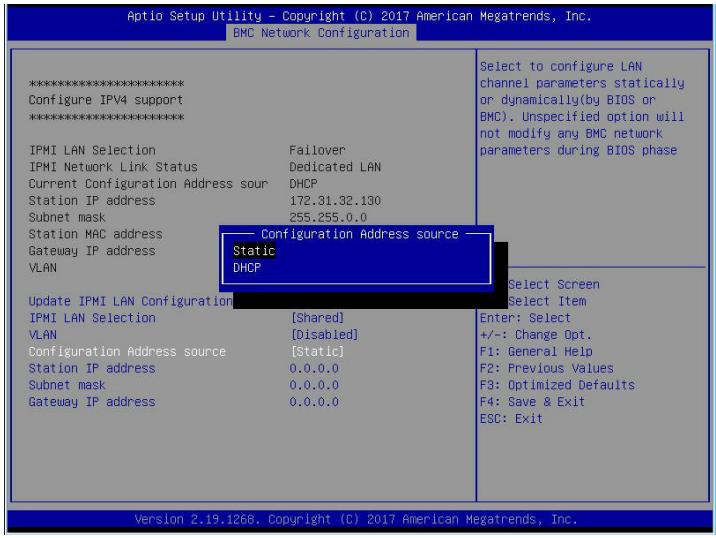
6. Highlight <Update IPMI LAN Configuration> and select <Yes>.



7. Navigate to <IPMI LAN Selection>, and you will see three options as shown below. Select <Shared>.



8. Highligh <Configuration Address source> and select <Static>. Then you can assign an IP such as 192.168.0.3, and subnet 255.255.0.0.



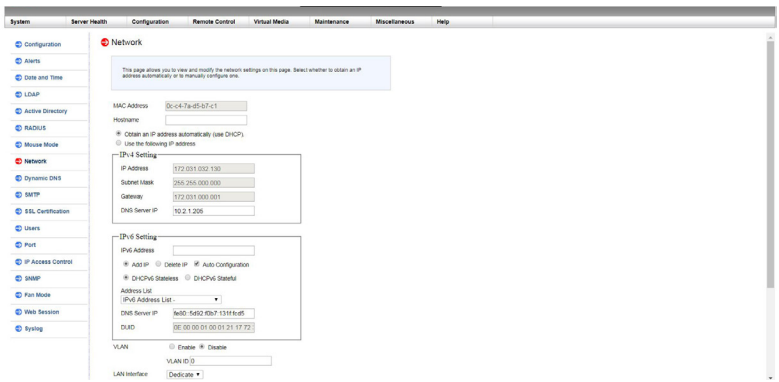
Now you have both Laptop and the IPMI on the same subnet. With the static IP connected, they should be able to communicate. To establish the connection, please follow the steps below:

1. Keep the terminal of the Linux laptop. Ping the IPMI IP, 192.168.0.4, and make sure it's pingable.

2. If it is pingable, open a web browser on the laptop. Enter the IP in URL bar and you will see a login screen.

3. Enter the username, ADMIN, and the password, ADMIN.

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



2-2 Configuring the IP/MAC Addresses for Remote Servers

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

Using the IPMICFG Utility to Set the IP Addresses for Remote Servers

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 IPMI settings.

IPMICFG Version 1.20.3 © 2014 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: ###.###.###.###)
-garp on	Enable the Gratuitous ARP
-garp off	Disable the Gratuitous ARP
-fd	Reset to the factory default
-fdl	Reset IPMI to the factory default (CLEAN LAN)
-fde	Reset to the factory default (clear FRU and LAN)
-ver	Get Firmware revision
-vlan	Get VLAN status
-vlan on [VLANtag]	Enable the VLAN and set the VLAN tag. If VLANtag is not given it uses previously saved value.
-vlan off	Disable the VLAN

-raw	Send a RAW IPMI request and print response.
-fan	Get fan mode
-fan <mode>	Set fan mode
-nm nmsdr	Display NM SDR
-nm seltime	Get SEL time
-nm deviceid	Get ME device ID
-nm reset	Reboot ME
-nm reset2default	Force ME reset to default
-nm updatemode	Force ME to update mode
-nm selftest	Get self-test results
-nm listimagesinfo	List ME image information
-nm oemgetpower	OEN power command for ME
-nm oemgettemp	OEM temp. commance for ME
-nm pstate	Get max. allowed CPU P-state
-nm tstate	Get max. allowed CPU T-state
-nmcpumemtemp	Get CPU/memory temperature
-nm hostcpudata	Get host CPU data
-pminfo	Power-supply PMBus health
-psfruinfo	Power-supply FRU health
-psbbpinfo	Battery backup power status
-autodischarge <module><day>	Set auto discharge by days
-discharge <module>	Manually discharge battery
-user list	List user privilege information
-user help	Show user privilege code
-user add <user id> <username> <password> <privilege>	Add user
-user del <user id>	Delete user
-user level <user id> <privilege>	Update user privilege
-user setpwd <user id> <password>	Update user password
-conf upload <file> <option>	Upload IPMI configuration from binary file
-conf download <file>	Download IPMI configuration to binary file

-conf tupload <file> <option>	Upload IPMI configuration from text file
-conf tdownload <file>	Download IPMI configuration to text file
-sdr	Show SDR records and reading
-sdr del <SDR ID>	Delete SDR record
-sdr ver [<V1> <V2>]	Get/Set SDR version (V1 V2 are BCD format)
-sel info	Show SEL info
-sel list	Show SEL records
-sel raw	Show SEL raw data
-sel del	Delete all SEL records
-fru info	Show FRU inventory area Info
-fru list	Show all FRU values
-fru help	Show help of FRU Write
-fru cthelp	Show chassis type code
-fru <Field>	Show FRU field value
-fru <Field> <Value>	Write FRU
-fru 1m	Update FRU product manufacturer from DMITable
-fru 1p	Update FRU product name from DMITable
-fru 1s	Update FRU product S/N from DMITable
-fru 2m	Update FRU board manufacturer from DMITable
-fru 2p	Update FRU board product name from DMITable
-fru 2s	Update FRU board S/N from DMITable(sdc.exe needed)
-fru 3s	Update FRU chassis S/N from DMITable
-fru backup <file>	Backup FRU to bin file
-fru restore <file>	Restore FRU from bin file
-fru tbackup <file>	Backup FRU to text file
-fru trestore <file>	Restore FRU from text file
-fru ver <V1> <V2>	Get/Set FRU version (V1, V2 are BCD format)
-fru dmi <$1> <$2> <$3> <$4> <$5> <$6> <$7> <$8> <$9> <$10> <$11> <$12> <$13> <$14>	$1 Product manufacturer name $2 Product name $3 Product part number $4 Product version $5 Product serial number $6 Product asset tag $7 Board manufacturing date/time $8 Board manufacturer name $9 Board product name $10 Board part number $11 Board serial number $12 Chassis type $13 Chassis part number $14 Chassis serial number

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 IPMI LAN port.

2. Choose a computer that is connected to the same network and open the browser.

3. Enter the IP address of each server that you want to connect to in the address bar of your browser.

4. Once the connection is made, the Login screen as shown on the next page will display.

Using IPMIView to Connect to the Remote Server

1. Connect a LAN cable to the onboard LAN1 port or the dedicated IPMI LAN port.

2. Choose a computer that is connected to the same network and open the IPMIView utility.

3. Go to File>New>System. Enter the System Name, IP Address of LAN1 (or the dedicated LAN, and the Description in the appropriate fields, and press <Enter>.

4. Select the system from the IPMI Domain. Enter the Login ID and Password in the appropriate fields to log in to the IPMIVie with utility.

Notes:

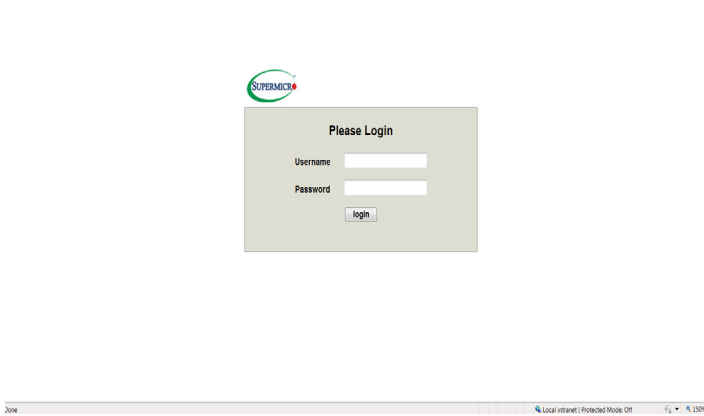
1. The default network setting is "Failover", which will allow the IPMI to connect to the network through a shared LAN port (onboard LAN Port 1 or 0) or through the IPMI Dedicated LAN Port. If the IPMI must be connected through a specific port, please change the LAN configuration setting under the Network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

2. For the IPMI to work properly, please enable all onboard USB ports and the COM port designated for SOL (IPMI) on the motherboard. All USB ports and the COM port for IPMI (marked with "*") are **enabled** in the system UEFI BIOS by default. It is usually listed as COM2 or COM3 in the UEFI BIOS. Refer to Section 2-1 Configuring UEFI BIOS for more information.

2-4 Accessing the Remote Server Using the Browser

To Log In to the Remote Console

Once you are connected to the remote server via browser, the following IPMI Login screen will display.



1. Enter your username in the *Username* box.

Note: The manufacturer default username and password are ADMIN/ADMIN. Once you have logged into the BMC using the manufacturer default password, be sure to change your password for security purpose.

2. Enter your password in the *Password* box and click on <Login>.

3. The home page will display as shown on the next page.

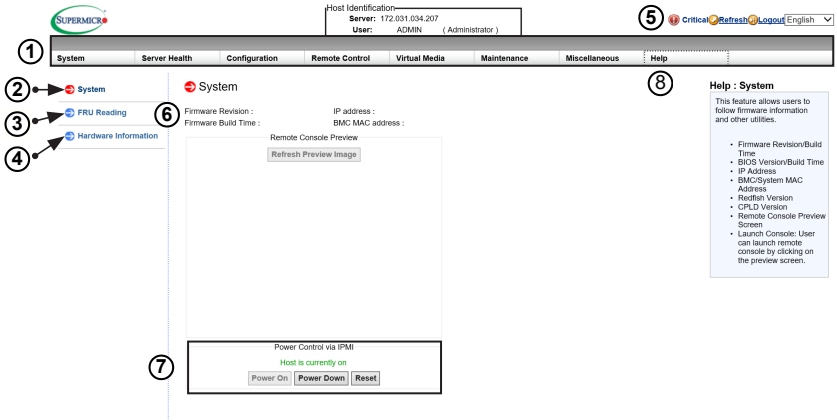
Note 1: To use the IPMIView utility for Console Redirection, please refer to the IPMIView User's Guide for instructions.

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

2-5 IPMI Main Screen

For X10 or Newer versions of Motherboards

The IPMI Main screen displays the following information.



Note: The following webGUIs indicate different purposes:

: System Normal

: Refresh Page

: Logout

The IPMI Main screen displays system information, including the following:

1. The Menu bar: The menu bar on the top displays System Information, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, Miscellaneous, and Help. Click an item on the menu bar to access an IPMI feature and configure its settings.

2. The System window: This window displays the System submenu items. Click an item in this window to configure the following settings.

3. FRU Reading: This page details the FRU (Field Replaceable Unit) information. Click on "FRU Reading" to display this information.

4. Hardware Information: This page shows the hardware architecture. Click on "Hardware Information" to display the following information:

- System
  - Manufacturer
  - Product Name
  - Serial No.
- UEFI BIOS
- CPU
  - CPU1
  - CPU2
- DIMM
  - Shows the slots that are occupied by DIMM modules

  (e.g. P1-DIMMA1, , P1-DIMMB1, P2-DIMMA1, P2-DIMMB1)
- Power Supply
  - System Power Supply #1
  - System Power Supply #2

5. Language Select: From the pull-down menu, select a language.
   - English
   - Japanese
   - Simplified Chinese
6. Summary: This field provides the following information:
   - Firmware Revision
   - Firmware Build Time
   - UEFI BIOS Version
   - UEFI BIOS Build Time

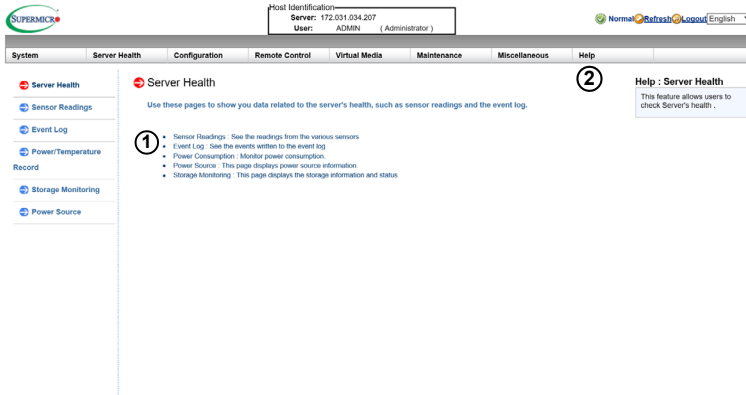
- Redfish Version
- CPLD Version
- IP Address
- BMC MAC Address
- System LAN 1 MAC Address
- System LAN 2 MAC Address
- Remote Console Preview - a display of the remote system (the host machine) running at the specified IP address

7. Power Control via IPMI: This field provides options for powering on and off the host sytem.
   - Power On: Click this button to power on the host system.
   - Power Down: Click this button to power off the host system.
   - Reset: Click this button to reset the host system.
8. Click on the <Help> tab to display the Help menu. The menu displays the following information:
   - Firmware Revision/Buiild Time
   - UEFI BIOS Version/Build Time
   - IP Address
   - BMC/System MAC Address
   - Remote Console Preview Screen
   - Launch Console: This feature allows the user to launch a remote console by clicking on the preview screen
   - Power Control: This feature allows the user to monitor and change the system power state via IPMI.

2-6 Server Health

For X10 or Newer versions of Motherboards

This feature allows the user to set the *Server Health* settings. When you click on *Server Health* in the Options window, the following screen will display:



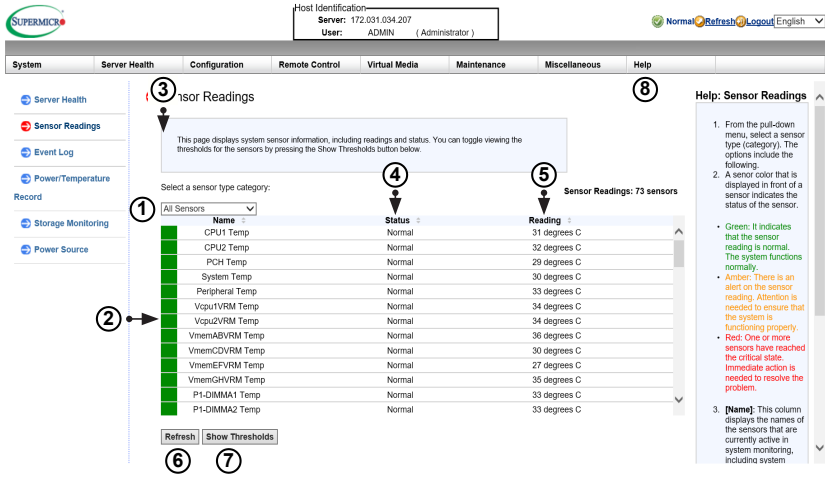
1. This section shows data related to the server's health, such as sensor readings and the event logs.
   - Displays sensor readings from the various sensors
   - Displays events to be written onto the event log
   - Displays power consumption.
   - Power Source : This page displays power source information.
2. Click on the <Help> tab to display the Help menu. The menu displays information relating to the server's health.

2-6-1 Sensor Readings

For X10 or Newer versions of Motherboards

This feature allows the user to set *Server Health* settings. When you click on *Server Health* in the Options window, the following screen will display:

1. Click <Sensor Readings> to access information on sensor readings as shown on the next page.



This page displays system sensor readings for the remote console. When you click on *Sensor Readings* in the Options window, the following screen will display:

1. From the pull-down menu, select a sensor type (category). The options include the following:

   - All Sensors
   - Temperature Sensors
   - Voltage Sensors
   - Fan Sensors
   - Physical Security

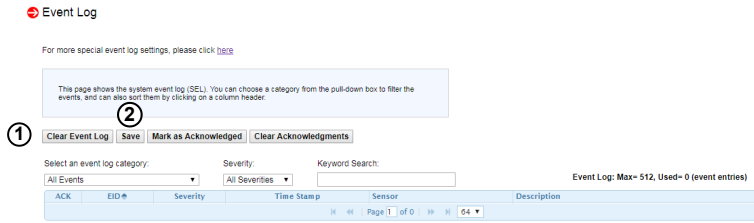
- Power Supply
- Battery

2. The color on the left of the sensor name indicates the status of that sensor.
   - Green: It indicates that the sensor reading is normal. The system functions normally.
   - Red: One or more sensors have reached the critical state. An immediate action is needed to resolve the problem.
   - No Color: There is no sensor reading.
3. Name: This column displays the names of the sensors that are currently active in system monitoring, inclu ding system temperature, CPU temperature, fan speeds, CPU core voltages, +3.3Vcc, and +12V voltage monitoring.
4. Status: This column indicates the status of each sensor reading.
5. Reading: This column indicates the reading of each sensor.
6. Refresh: Click this item to refresh the page.
7. Show Thresholds: Click this item to display senor thresholds.
8. Click on the <Help> tab to display the Help menu. The menu displays the following information:
   - An explanation of the green and red sensors.
   - An explanation of each column on the page.
   - The functions of each button on the page.

2-6-2 Event Log

For X10 or Newer versions of Motherboards

This page displays a record of critical system monitoring events. The event log indicates the time when a critical condition had occurred and when this condition was resolved. You can choose a specific event category from the pull-down menu to display events included in this category. When you click on *Event Log* in the Options window, the following screen will display:

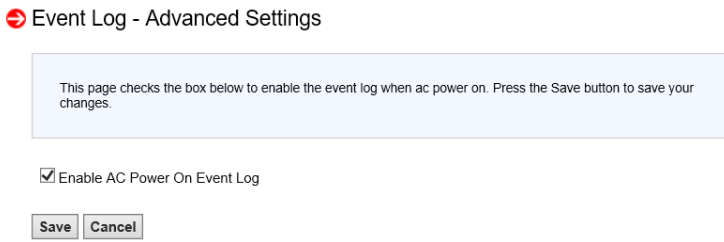


1. Event Log Category: From the pull-down menu, select an event category to display.

   - Sensor-Specific Events: These event logs are generated by the BMC if the sensor's reading reaches the threshold.
   - UEFI BIOS-Generated Events: These event logs are generated by the UEFI BIOS and logged to the BMC.
   - System Management Software Events: These events logs are generated by the OS, application software, etc., and logged to the BMC.
   - All Events: This category includes all the above event logs.

Sensor Type	Event
OS Boot	A: boot completed
	C: boot completed
	PXE boot completed
	Diagnostic boot completed
	CD-ROM boot completed
	ROM boot completed
	Boot completed - boot device not specified
OS Stop/Shut-down	Stop during OS load/initialization, Unexpected error during system startup, Stopped waiting for input or power cycle/reset
	Run-time stop (a.k.a 'core dump', 'blue screen')
	OS graceful stop (system powered up, but normal OS operation has shut down and system is awaiting reset pushbutton, power cycle or other external input)

In addition to the events listed on the previous page, it is normal to see boot-up and shutdown events generated by the installed system software (OS). The table below lists examples of these types of events



2. Click on <here> to see more special event log settings. You will see the an option to enable AC Power On Event Log. Check the box to enable the option and click on <Save>.

3. Click on the <Help> tab to display the Help menu. The menu displays information for the following features:

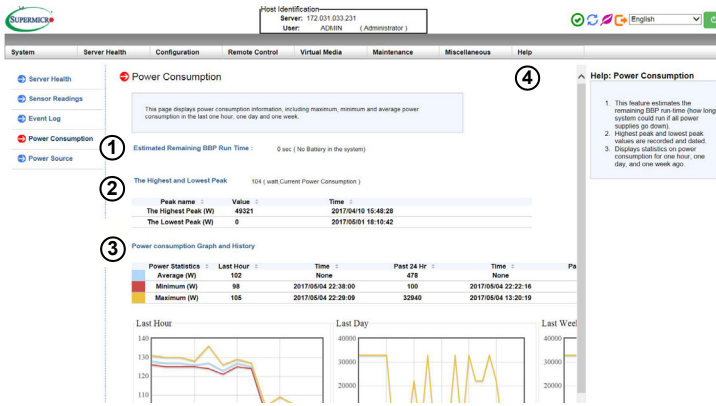
   - [Sensor-Specific Events]
   - [UEFI BIOS-Generated Events]
   - [System Mangement Software Events]
   - [All Events]

2-6-3 Power Consumption

For X10 or Newer versions of Motherboards

This page displays the Maximum, Minimum, and Average power consumption in the last hour, day, and week. When you click on *Power Consumption* in the Options window, the following screen will display:

Note: The Power Consumption feature is not available on all systems.



1. Estimate remaining BBP run time: Displays the battery backup power run time.

2. The highest and lowest peak: Displays the highest and lowest peak of power consumption.

3. Power consumption graph and history: Displays the average, minimum, and maximum power consumption of the past hour and week.

4. Click on the <Help> tab to display the Help menu. The menu displays the following information:

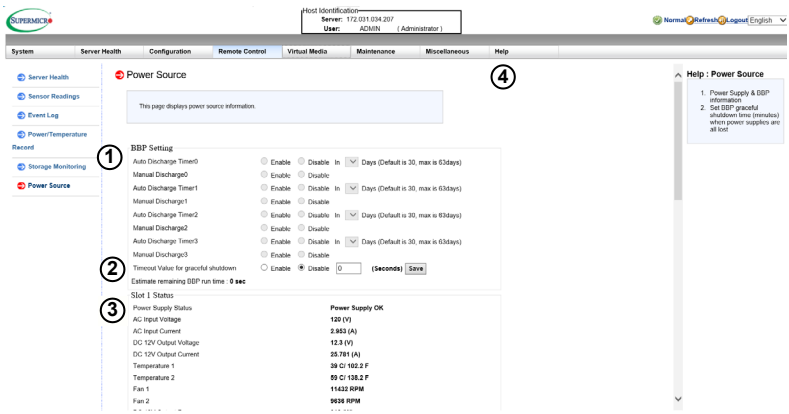
   - This feature estimates the remaining BBP run-time (how long system could run if all power supplies go down).
   - Highest peak and lowest peak values are recorded and dated.
   - Displays statistics on power consumption for one hour, one day, and one week ago.

2-6-4 Power Source

For X10 or Newer versions of Motherboards

This page displays the power source information. When you click on *Power Source* in the Options window, the following screen will display:

Note: The Power Source feature is not available on all systems.



1. BBP Setting: Displays the battery backup power settings. You can enable or disable the graceful shutdown and specify the timeout value (in seconds).

2. Timeout Value for graceful shutdown: This feature allows you to enable or disable a graceful shutdown. Specify the timeout value in seconds.

3. Slot 1 Status: Displays the following information for the indicated slot:

   - Status
   - AC Input Voltage
   - AC Input Current
   - DC 12V Output Voltage
   - DC 12V Output Current

- Temperature 1
- Temperature 2
- Fan 1
- Fan 2
- DC 12V Output Power
- AC Input Power
- PWS Serial Number

4. Click on the <Help> tab to display the Help menu. The menu displays details on the power source settings:

2-6-5 Storage Monitoring

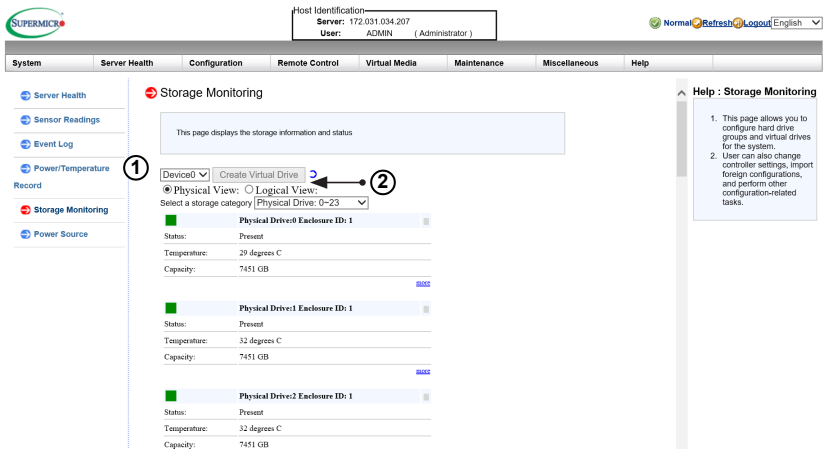
For X10 or Newer versions of Motherboards

This page displays the storage information and status. When you click on *Storage Monitoring* in the Options window, the following screen will display:

Note 1: The Storage Monitoring feature is not available on all systems. License key is required to activate RAID management features, but license key is not required to view Storage Monitoring.

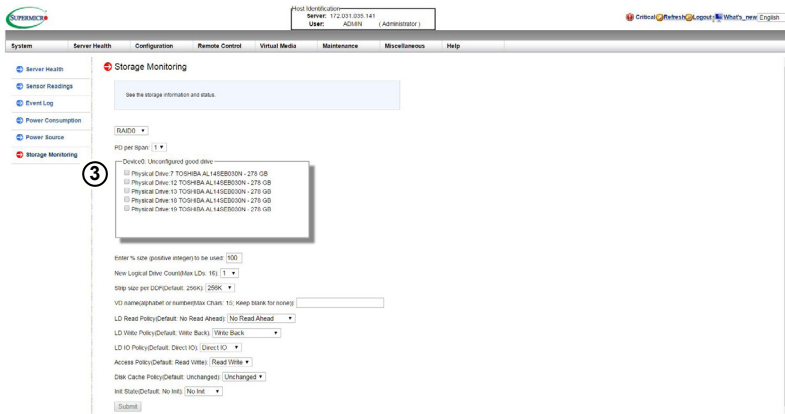
Note 2: BMC MAC address cannot be changed. If changed, prior license keys will be lost.

Note 3: The Storage Monitoring feature is only available for LSI 3108 controllers, not the onboard Intel controllers.

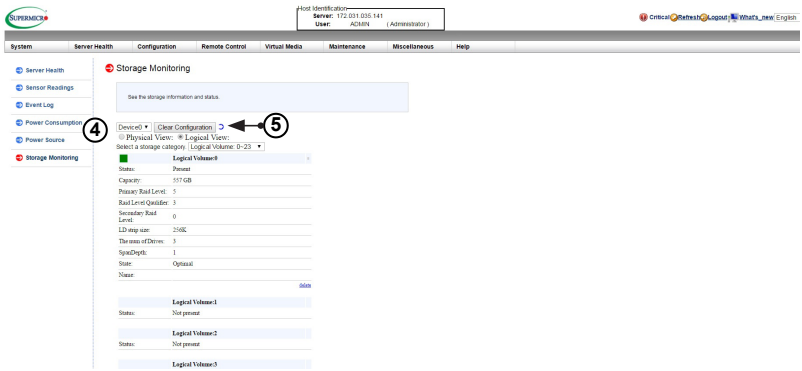


1. Click on <Physical View> and select the <Physical Drive> from the drop-down menu to view the drive numbers and their status.

2. If you have clicked on <Physical View>, click on <Create Virtual Drive> to create new RAID.

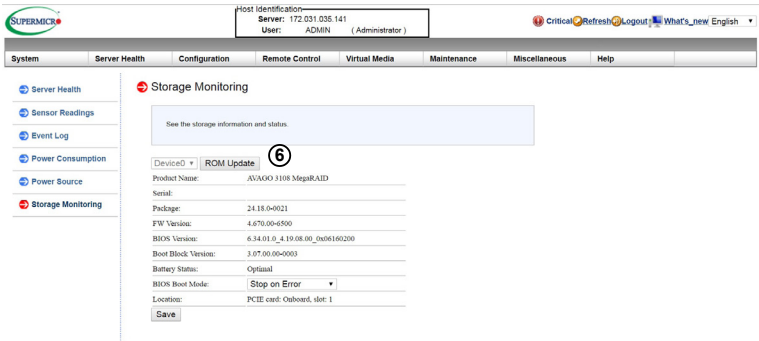


3. Select the Drives and click on <Submit> from the screen above to create new RAID.

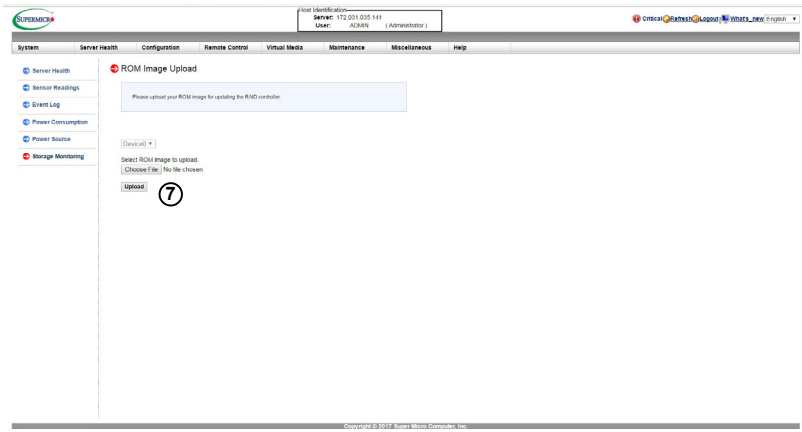


4. If you have clicked on <Logical View>, you can click on <Clear Configuration> to clear configuration or check the status of the current RAID.

5. When you click on on the previous page to update firmware, the following screen will diaplay as shown below.



6. Click on <ROM Update> to update firmware on controller and the following screen will display:

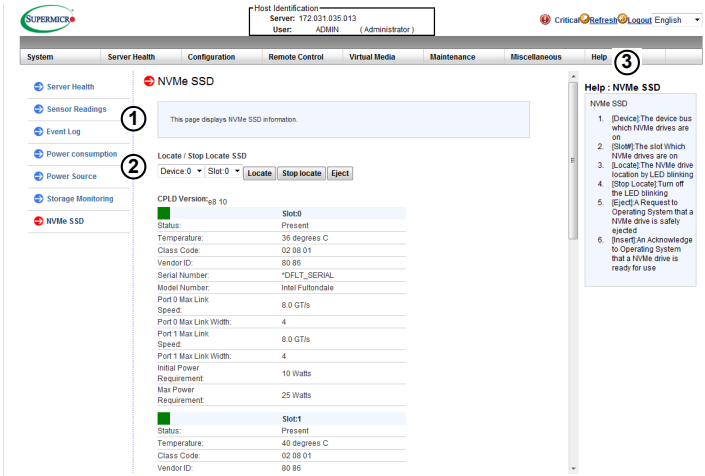


7. Click on <Choose File> and <Upload> to select and upload ROM image.

2-6-6 NVMe SSD

This page displays the NVMe SSD information and status. When you click on *NVMe SSD* in the Options window, the following screen will display:

Note: The NVMe SSD feature is not available on all systems.



1. Select the device from the drop-down menu and its location from the drop-down menu that displays the slot number. After you have selected a device and its location, click on <Locate>, <Stop Locate>, or <Eject>.

2. Displays information on the selected device and slot.

3. Click on the <Help> tab to display the Help menu. The menu displays the following information:

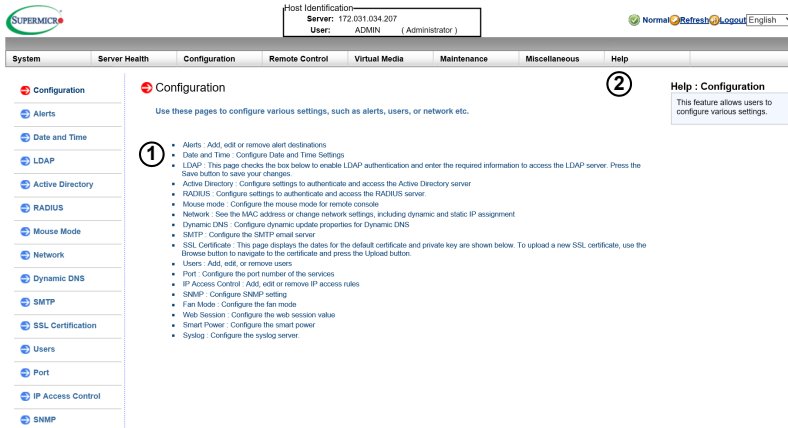
   - [Device]: This feature displays the device bus which NVMe drives are on.
   - [Slot]: This feature displays the slot which the NVMe drives are on.
   - [Locate]: This feature displays the NVMe drive location by the LED blinking.
   - [Stop]: This feature turn off the LED blinking.
   - [Eject]: This feature allows the user to enter a request to the operating system that an NVMe drive is safely ejected.
   - [Insert]: This feature displays acknowledgement to the operating system that an NVMe drive is ready for use.

2-7 Configuration

For X10 or Newer versions of Motherboards

This feature allows the user to configure various network settings. When you click on *Configuration* in the menu bar, the following screen will display:

Note: Configuration settings will vary by system.



1. This section allows the user to configure the following settings.

   - Alerts: Use this item to configure alert destination settings.
   - Date & Time
   - LDAP: Use this item to configure LDAP (Lightweight Directory Access Protocol) settings for authentication and access to the LDAP server.
   - Active Directory: Use this item to configure the settings for authentication and access to the Active Directory server.
   - Radius: Use this item to configure the settings for authentication and access to the Radius server.
   - Mouse Mode
   - Network

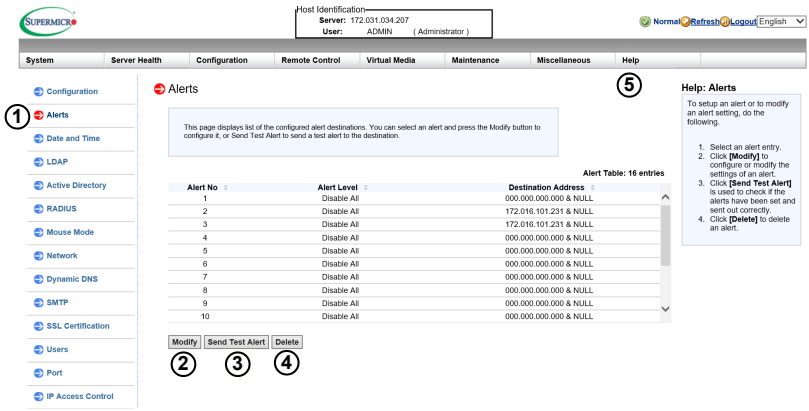
- Dynamic DNS
- SMTP
- SSL Certification
- Users
- Port
- IP Access Control
- SNMP
- Fan Mode
- Web Session
- Syslog

2. Click on the <Help> tab to display the Help menu for the *Configuration* screen.

2-7-1 Alerts

For X10 or Newer versions of Motherboards

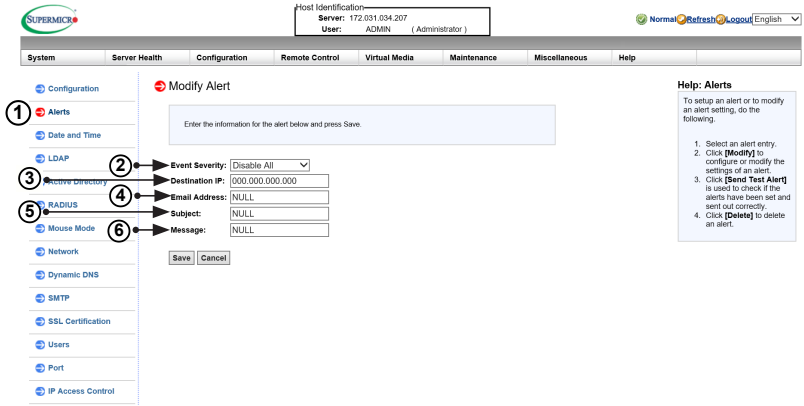
This feature allows the user to configure *Alert* settings. When you click on *Alerts* in the menu bar, the following screen will display:



To setup an alert or to modify an alert setting, do the following.

1. Click on <Alerts> to activate the alert submenu.
2. Click on <Modify> to configure or modify the settings of an alert.
3. *Send Test Alert* is used to check if the alerts have been set and sent out correctly.
4. Click on <Delete> to delete an alert.
5. Click on the <Help> tab to display the Help menu. This menu shows you how to set up or modify an alert.

To Setup an Alert



Follow the steps below to setup an alert.

1. Select *Alerts* from the window on the left. Highlight the alert and select *Modify*.

2. Select *Event Severity*.

3. Enter the destination IP address to use SNMP. For further guidance on typical inquiries relating to SNMP, see the table on the next page.

Item	*Answer*
SNMP version number	SNMP version 2 and 3.
MIB community name	A community name is not required since SNMP version 1 only uses traps.
MIB file location	Go to http://www.supermicro.com/products/nfo/IPMI.cfm and click on “IPMI MIB” (right-hand side of the page).
The IPMI item you need to configure so that the SNMP manager can receive the SNMP trap	The alert LAN destination address (see #4 under 2.4.1) must be set to the same IP in as the SNMP manager.
Can I query for detailed information on the MIB "Event" trap items?	Users can use SNMP tools to query information from BMC.
A list of trap items generated for my platform	No standard list of event traps exist because the PEF (Platform Event Filter) table is OEM customizable.

4. Enter the email address you wish the send the alert to, then configure the SMTP settings (see section 2.8.10)

5. Enter the subject line of the alert.

6. Enter a message for the alert.

After completing the steps above, Click on <Save> to save the settings.

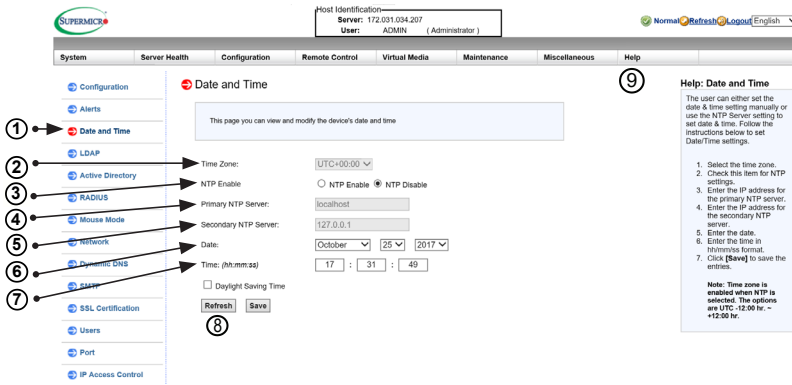
2-7-2 Date and Time

For X10 or Newer versions of Motherboards

This feature allows the user to configure the time and date settings for the host server and the client computer. When you click on *Time and Date* in the Options window, the following screen will display:

The user can either set the date & time setting manually or use the *NTP Server* setting to set date & time. Follow the instructions below to set Date/Time settings.

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

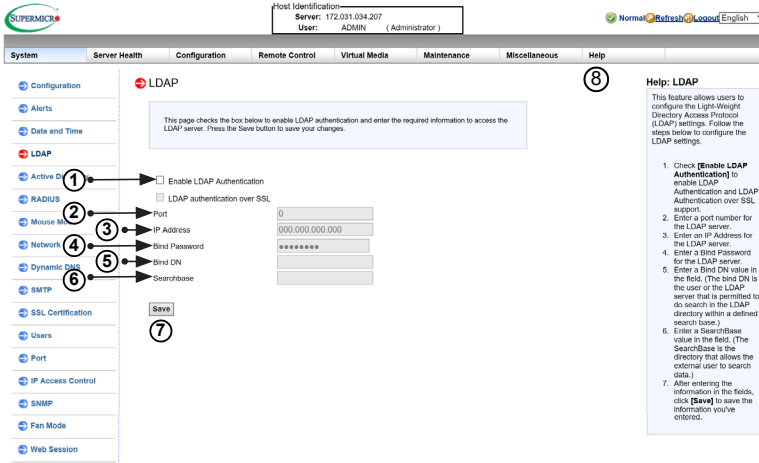


1. Click on *Date/Time* on the left to set the date/time settings.
2. Select the time zone.
3. Check this item for NTP settings.
4. Enter the IP address for the primary NTP server.
5. Enter the IP address for the secondary NTP server.
6. Enter the date.
7. Enter the time in hh/mm/ss format.
8. Click on <Refresh> to change the date/time settings. Click on <Save> to save the settings.
9. Click on the <Help> tab to display the Help menu. This menu includes instructions on how to modify the date and time.

2-7-3 LDAP

For X10 or Newer versions of Motherboards

This feature allows the user to configure the *Light-Weight Directory Access Protocol* (LDAP) settings. When you click on *LDAP* in the Options window, the following screen will display:



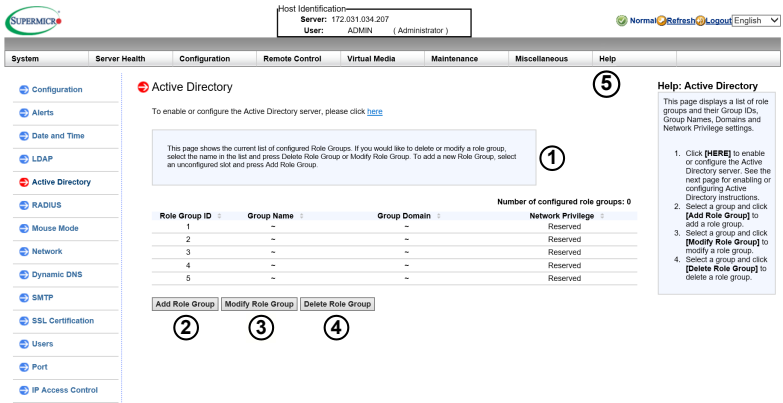
Follow the steps below to configure the LDAP settings.

1. Check the enable box to enable *LDAP Authentication and LDAP Authentication over SSL* support.
2. Enter a port number for the LDAP server.
3. Enter an IP Address for the LDAP server.
4. Enter a Bind Password for the LDAP server.
5. Enter a Bind DN value in the field. (The bind DN is the user or the LDAP server that is permitted to do search in the LDAP directory within a defined search base.)
6. Enter a SearchBase value in the field. (The SearchBase is the directory that allows the external user to search data.)
7. Click on <Save> to save the settings.
8. Click on the <Help> tab to display the Help menu. This menu provides an explanation of all the options displayed on the page.

2-7-4 Active Directory

For X10 or Newer versions of Motherboards

This page displays a list of role groups and their Group IDs, Group Names, Domains, and Network Privilege settings. When you click on *Active Directory* in the Options window, the following screen will display:



1. Click on <here> to enable or configure the Active Directory server. See the next page for enabling or configuring Active Directory instructions.

2. Select a group and click on <Add Role Group> to add a role group.

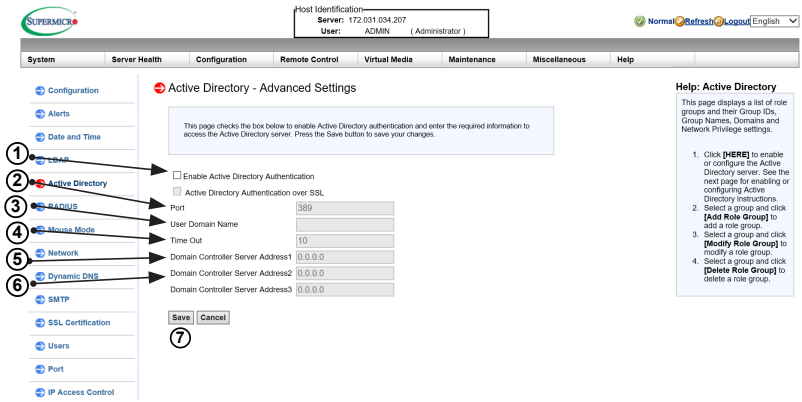
3. Select a group and click on <Modify Role Group> to modify a role group.

4. Select a group and click on <Delete Role Group> to delete a role group.

5. Click on the <Help> tab to display the Help menu. This menu provides instructions on how to add, modify, and delete a role group.

Configuring the Active Directory Settings

This feature allows the user to configure the *Advanced Active Directory* settings. When you click *Here* on the screen shown on the previous page, the following screen will display:



1. Check the <Enable> box to enable *Active Directory* authentication support. Then, Enter the values in the fields below.

2. Enter <User Domain Name>.

3. Enter Time Out value in the field to set the time limit for a user to stay logging-in.

4. Enter <Controller Server Address1>.

5. Enter <Controller Server Address2>.

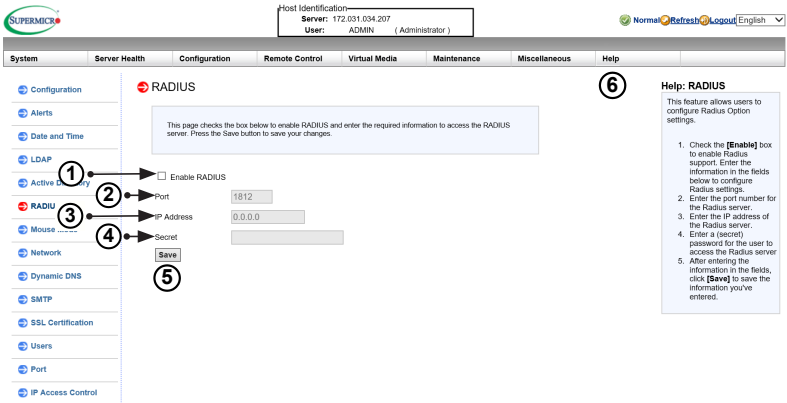
6. Enter <Controller Server Address3>.

7. Click on <Save> to save the settings.

2-7-5 RADIUS

For X10 or Newer versions of Motherboards

This feature allows the user to configure *Radius Option* settings. When you click on *Radius* in the Options Window, the following screen will display:



1. Check the <Enable> box to enable *Radius* support. Enter the information in the fields below to configure *Radius* settings.

2. Enter the port number for the Radius server.

3. Enter the IP address of the Radius server.

4. Enter a secret (password) for the user to access the Radius server.

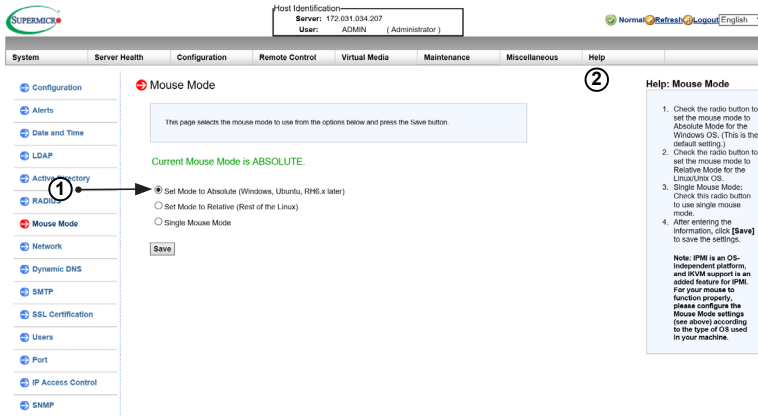
5. Click on <Save> to save the settings.

6. Click on the <Help> tab to display the Help menu. The menu includes instructions on how to configure the RADIUS settings.

2-7-6 Mouse Mode

For X10 or Newer versions of Motherboards

This feature allows the user to configure the *Mouse Mode* settings. When you click on *Mouse Mode* in the Options Window, the following screen will display.



1. This item displays the current Mouse Mode setting. To select a Mouse Mode setting, click on a mode shown below.

   - Set Mode to Absolute (Windows, Ubuntu, RH6.x later). This is the default setting.
   - Set Mode to Relative (other brands of Linux).
   - Single Mouse Mode: Check this to use single mouse mode.
   - Click on <Save> to save the settings.

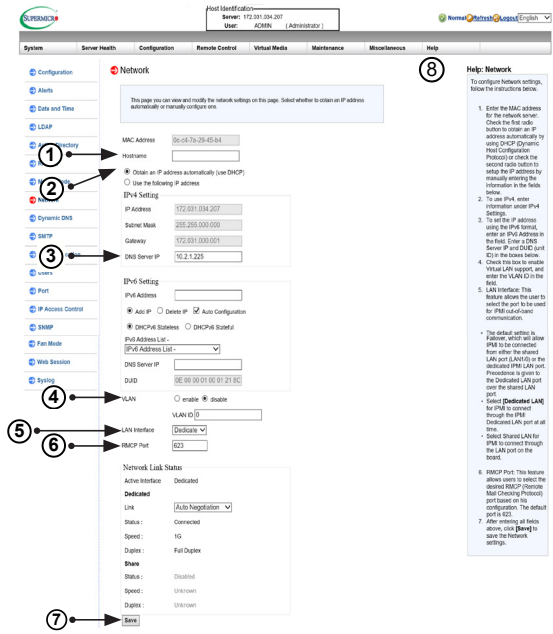
   Note: IPMI is an OS-independent platform. IKVM support is an added feature for IPMI. For your mouse to function properly, please configure the Mouse Mode settings (see above) according to the type of OS used in your machine.

2. Click on the <Help> tab to display the Help menu. The menu provides an explanation of the mouse modes.

2-7-7 Network

For X10 or Newer versions of Motherboards

This feature allows you to configure the network settings. When you click on *Network* in the Options Window, the following screen will display.



To configure *Network* settings, follow the instructions below.

1. Select *Obtain an IP automatically* (use DHCP) or *Use the following IP address* to manually configure one.

2. If you select *Use the following IP address,* enter information into the following IPv4 Setting fields:

   - IP address
   - Subnet Mask
   - Gateway
   - DNS Server IP

3. To set the IP address using the IPv6 format, enter an address in the field. Enter a DNS Server IP and DUID (unit ID) in the boxes.

4. Check this box to enable Virtual LAN support and enter the VLAN ID in the field.

5. LAN Interface: This feature allows the user to select the port to be used for IPMI out-of-band communication.

   - The default setting is Failover, which will allow IPMI to be connected from either the shared LAN port (LAN1/0) or the dedicated IPMI LAN port. Precedence is given to the Dedicated LAN port over the shared LAN port.

   - Select <Dedicate> for IPMI to connect through the IPMI Dedicated LAN port at all time.

   - Select <*Share*> for IPMI to connect through the LAN port on the board.

6. RMCP Port: This feature allows the user to select the desired RMCP (Remote Management Control Protocol) port. The default port is 623.

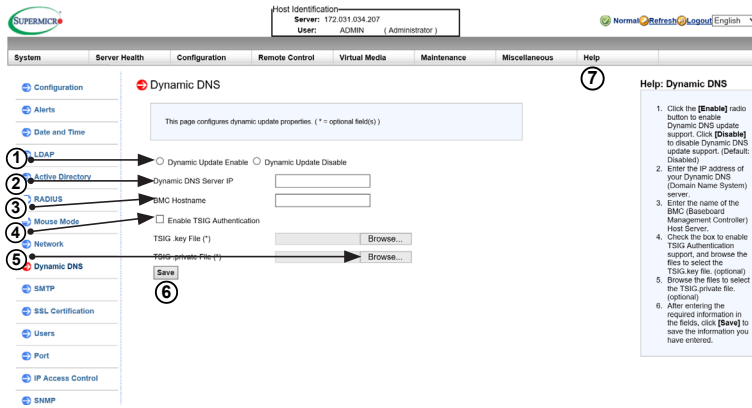
7. Click <Save> to save the settings.

8. Click the <Help> tab to display the Help menu. The menu inlcudes instructions on how to configure the Network settings.

2-7-8 Dynamic DNS

For X10 or Newer versions of Motherboards

This feature allows you to configure DNS (Dynamic Name System) settings. When you click *Dynamic DNS* in the Options Window, the following screen will display.



1. Click <Dynamic Update Enable> to enable DNS support. Click <Dynamic Update Disable> to disable Dynamic DNS update support. (**Default**: Disable)

2. Enter the IP address of your Dynamic DNS (Domain Name System) server.

3. Enter the name of the BMC (Baseboard Management Controller) Host Server.

4. Check the box to enable TSIG Authentication support, and browse the files to select the *TSIG.key* file. (This item is optional.)

5. Click <Browse> to locate the *TSIG.private* file. (This item is optional.)

6. Click <Save> to save the information you have entered.

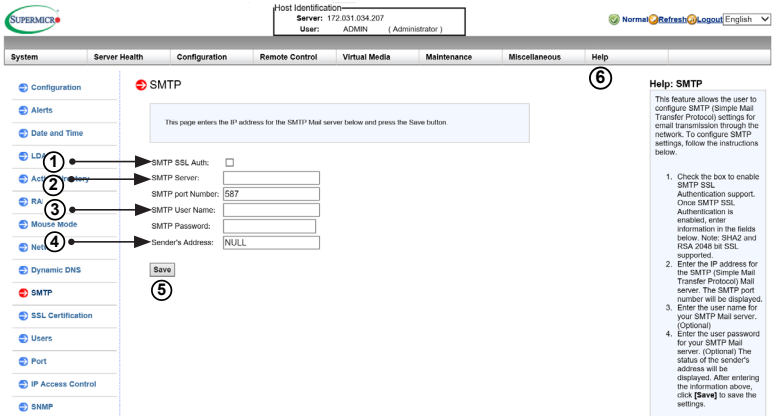
7. Click the <Help> tab to display the Help menu. The menu inlcudes instructions on how to configure the Dynamic DNS settings.

2-7-9 SMTP

For X10 or Newer versions of Motherboards

This feature allows the user to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network. When you click on *SMTP* in the Options window, the following screen will display.

To configure SMTP settings, follow the instructions below.



1. Check the box to enable SMTP SSL Authentication support. Once SMTP SSL Authentication is enabled, enter information in the fields below.

   Note: SHA2 and RSA 2048 bit SSL supported.

2. Enter the IP address for the SMTP (Simple Mail Transfer Protocol) Mail server. The SMTP port number will be displayed.

3. Enter the user name for your SMTP Mail server. (Optional)

4. Enter the user password for your SMTP Mail server. The status of the sender's address will be displayed. (Optional)

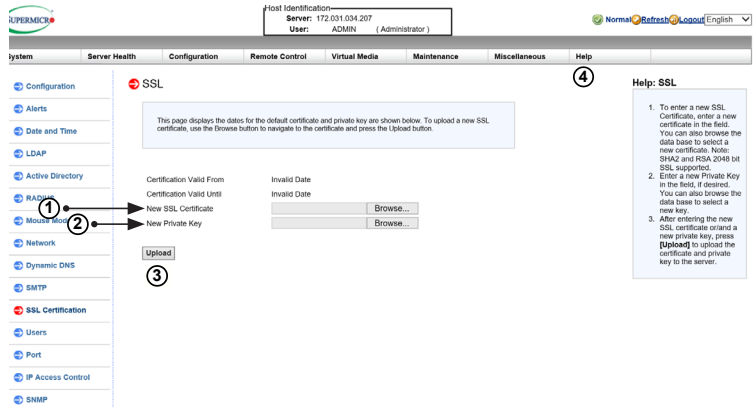
5. Click <Save> to save the settings.

6. Click the <Help> tab to display the Help menu. The menu inlcudes instructions on how to configure the SMTP settings.

2-7-10 SSL Certification

For X10 or Newer versions of Motherboards

This feature displays the default certificate and private keys. It also allows the user to upload a new SSL (Secure Sockets Layer) certificate. When you click on *SSL* in the Options window, the following screen will display:



1. To enter a new SSL Certificate, enter a new certificate in the field. You can also browse the data base to select a new certificate.

   Note: SHA2 and RSA 2048 bit SSL supported.

2. Enter a new Private Key in the field, if desired. You can also browse the data base to select a new key.

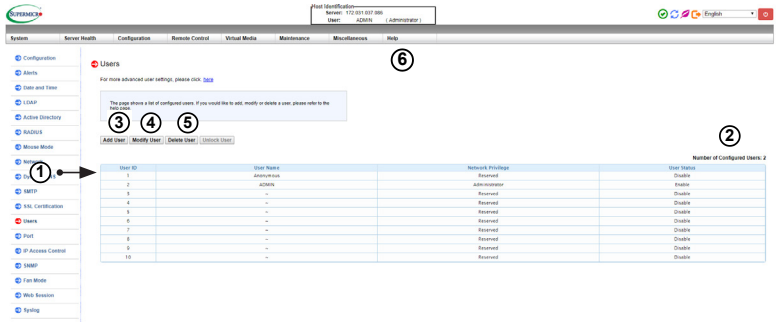
3. After entering the new SSL certificate and/or new private key, click <Upload> to upload the certificate and/or private key to the server.

4. Click the <Help> tab to display the Help menu. The menu includes instructions on how to set up a new SSL certificate and private key.

2-7-11 Users

For X10 or Newer versions of Motherboards

This page displays information on the current users. It also allows you to add, delete, or modify user information. When you click on *Users* in the Options window, the following screen will display:



1. This item lists current user information. This includes User ID, User name, and Network Privilege settings (shown below).

Function	User	Operator	Administrator
System Information	Full Access	Full Access	Full Access
Chassis Locator Control	View Only	Full Access	Full Access
FRU Reading	Full Access	Full Access	Full Access
Sensor Readings	Full Access	Full Access	Full Access
Event Log	View Only	Full Access	Full Access
Alert	No	View Only	Full Access
LDAP	No	View Only	Full Access
Mouse Mode	No	Full Access	Full Access
Network	No	View Only	Full Access
SMTP	No	View Only	Full Access
SSL	No	View Only	Full Access
Users	No	View Only	Full Access
Event Action	No	View Only	Full Access
Power Control	View Only	Full Access	Full Access
KVM	View Only	Full Access	Full Access
F/W Update	View Only	View Only	Full Access
Logout	Full Access	Full Access	Full Access

2. This item displays the number of the users that are set up for the network. The maximum number of profiles that can be made is ten.

3. To add a new user to the network, click on <Add User>. When prompted, select an empty slot from the users list to add an user.

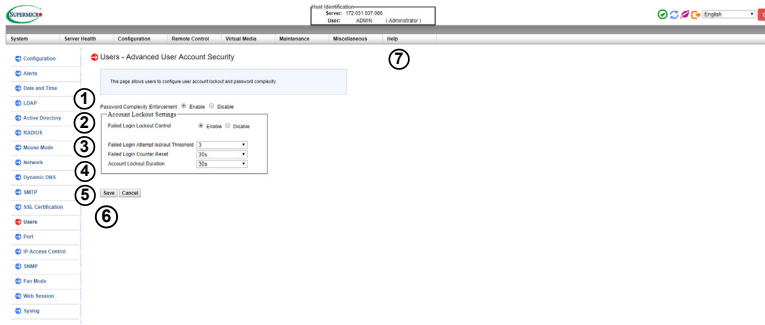
4. To modify the information or the status of a user, click on <Modify User>. When prompted, select a user from the users list to modify the user information.

5. To delete a user from the network, click on <Delete User>. When prompted, select a user from the users list to delete it from the list.

6. Click on the <Help> tab to display the Help menu. The menu displays an explanation of the columns displayed on the page and how to add, modify, and delete a user.

Account Security

This feature is used to configure user account security. System Administrator can configure security settings using Web GUI or Redfish.



Unlock User: If the user is locked out after failed login attempts, the administrator may use this feature to unlock the user.

1. Password Complexity Enforcement: The default is <Enable>, which enforces the password complexity requirements while the user is creating a password. Each password must adhere to the requirements listed below.
    - Must be 8 to 20 characters
    - Cannot be reverse of username
    - Must include characters from at least three of the listed character classes
        - A - Z
        - a - z
        - 0 - 9
        - Special characters

2. Failed Login Lockout Control: The default is <Enable> and allows failed login settings adjustment. Click <Disable> to disallow.

Authentication Failure Lockout Controls: The default is <Enable> to lock account after excessive failed login attempts. Configure fields below to control authentication failure lockout.

3. Failed Login Attempt Lockout Threshold: This item allows the user to adjust the number of times a password may be attempted before the user is locked out. The options range from 1 to 5. The default is 3.

4. Failed Login Counter Reset: Use this option to adjust the amount of time before the user may attempt to input a password after failing.

5. Account Lockout Duration: Use this item to adjust the amount of time the user is locked out after passing failed login attempt lockout threshold.

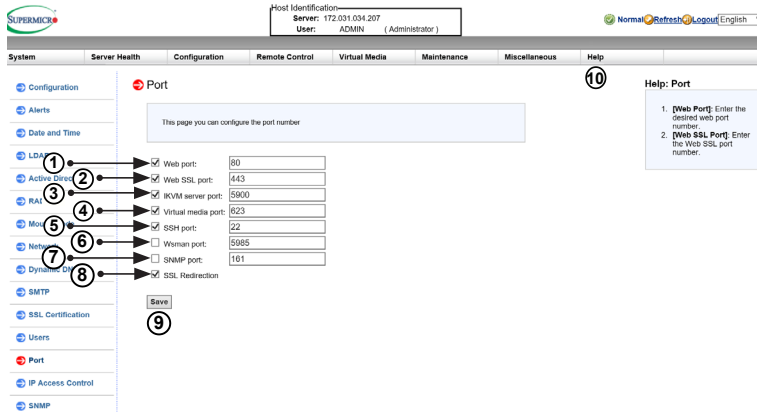
6. After the required information is entered, click <Save> to save the information you've entered or click <Cancel> to cancel it.

7. Click on the <Help> tab to display the Help menu. The menu displays an explanation of the items displayed on the page.

2-7-12 Port

For X10 or Newer versions of Motherboards

This page allows you to configure port settings. When you click on *Port* in the Options window, the following screen will display.



Check the box next to the port to configure the settings. Uncheck the box to disable the port.

1. Web port: Enter the web port number.
2. Web SSL port: Enter the Web SSL port number.
3. IKVM server port: Enter the IKVM port number.
4. Virtual media port: Enter the virtual media port number.
5. SSH port: Enter the SSH (Secure Shell) port number
6. Wsman port: Enter the WS-Management port number.
7. SNMP port: Enter the Simple Network Management Protocol port number.

8. SSL Redirection: Check the box to allow the IPMI webUI to redirect http to https automatically.

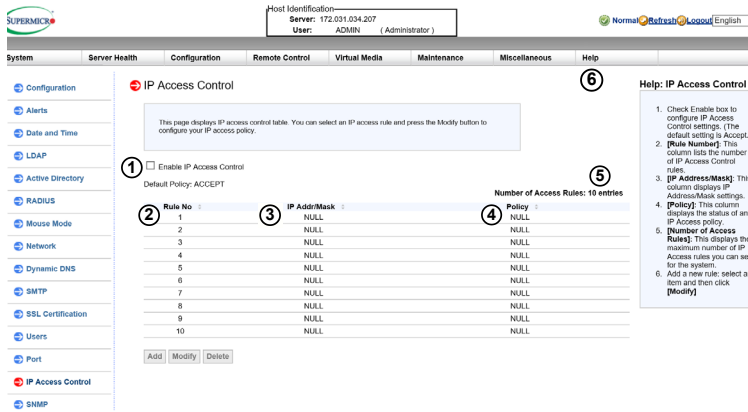
9. Click <Save> to save the settings.

10. Click the <Help> tab to display the Help menu. The menu inlcudes port setting information.

2-7-13 IP Access Control

For X10 or Newer versions of Motherboards

This page displays an IP Access Control table with the IP Address/Mask setting and the IP Access Policy. Enabling the IP Access Control will allow you to add, modify, and delete an IP Access rule.



1. Check this box to configure IP Access Control settings. When prompted, "Do you want to enable IP access control," click <OK>.

2. Rule Number: This column lists the number of IP Access Control rules.

3. IP Address/Mask: This column displays IP Address/Mask settings.

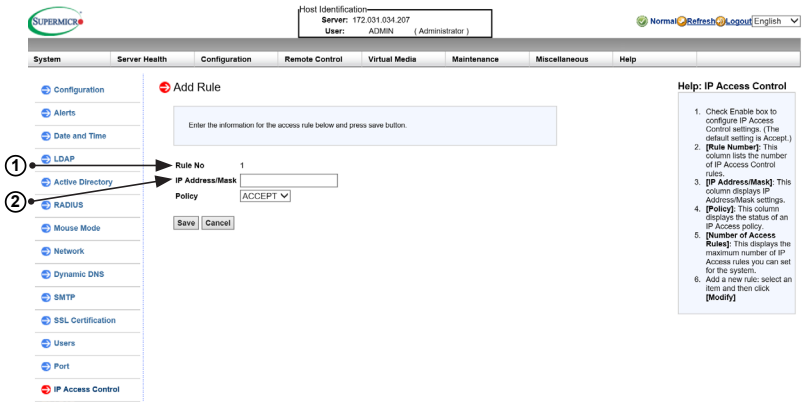
4. Policy: This column displays the status of an IP Access policy.

5. Number of Access Rules: This displays the maximum number of IP Access rules you can set for the system.

6. Click on the <Help> tab to display the Help menu. The menu includes an explanation of all the columns displayed on the page.

Modifying IP Access Rules

When you select an item and click on *Modify*, the Add Rule submenu will display as shown below.



To modify a rule, enter the information needed for the following items:

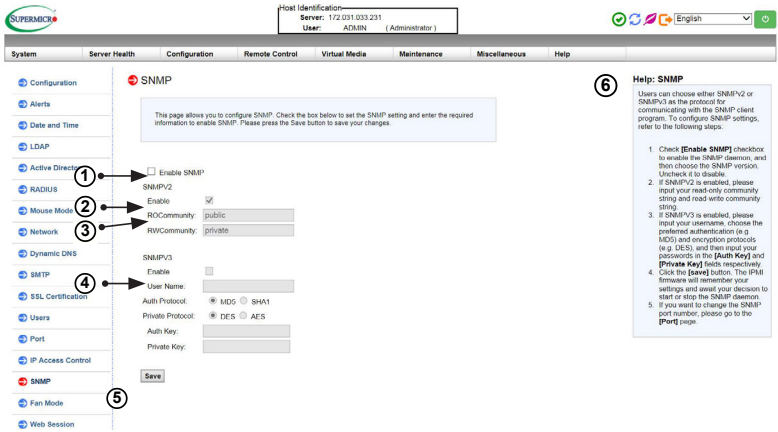
1. IP Address/Mask: This item allows you to grant access to a specific IP address or a range of IP addresses. For example, if you wanted to specify a range of IP addresses from 192.168.0.1 to 192.168.0.126, you would enter 192.168.0.1/25.

2. Policy: Select <Accept> to allow access for the IP address(es) entered above. Select Drop to deny access.

2-7-14 SNMP

For X10 or Newer versions of Motherboards

This feature allows the user to configure the SNMP (Simple Network Management Protocol). When you click on *SNMP* in the Options window, the following screen will display:



1. Check the box to enable the SNMP. Once it is enabled, enter information in the fields below.

2. SNMP Version: Select SNMPV2 or SNMPV3.

3. SNMPV2: If this options is selected, enter a password for ROCommunity and RWCommunity.

4. SNMPV3: If this option is selected, enter information in the fields below:

   - Enter a username
   - Select the Authentication Protocol
   - Select the Private Protocol

- Enter the Authentication Key
- Enter the Private key

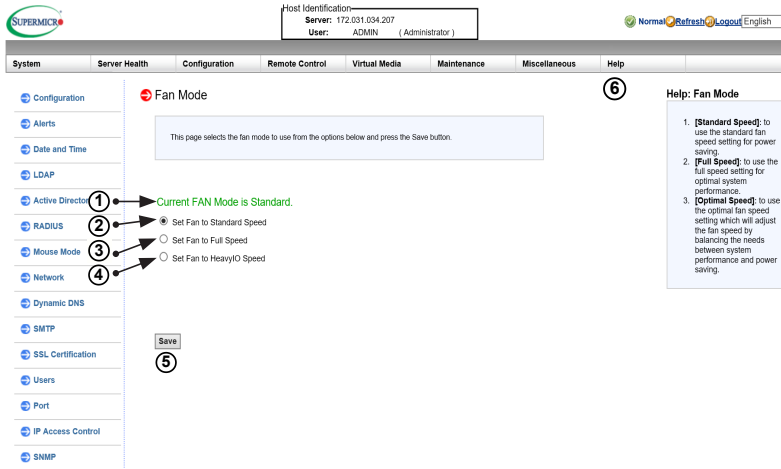
5. Click <Save> to save the settings.
6. Click the <Help> tab to display the Help menu. The menu includes an explanation of all the options on this page.

2-7-15 Fan Mode

For X10 or Newer versions of Motherboards

This page allows you to configure fan mode settings. When you click on *Fan Mode* in the Options window, the following screen will display:

Note: Fan mode settings will vary by system.

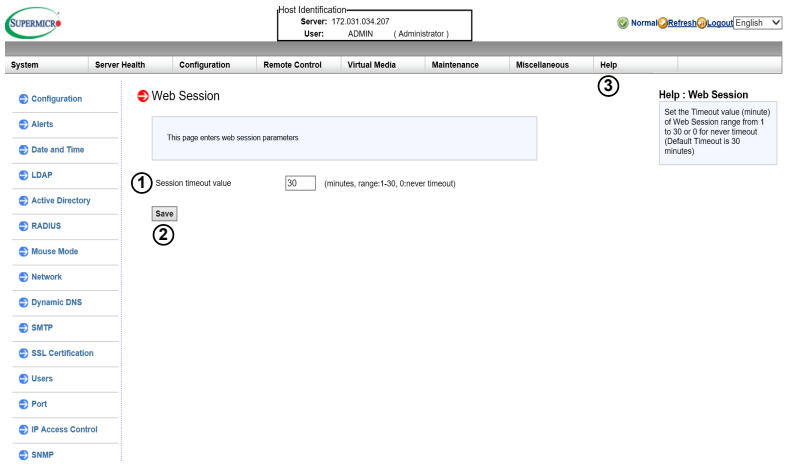


1. This item displays the current fan mode setting.
2. Select this option for the standard fan speed setting.
3. Select this option for the full speed setting.
4. Select this option for the Heavy IO speed.
5. Click <Save> to save the settings.
6. Click the <Help> tab to display the Help menu. The menu includes an explanation of the fan modes.

2-7-16 Web Session

For X10 or Newer versions of Motherboards

This page allows you to configure web session parameters. When you click on *Web Session* in the Options window, the following screen will display:



1. Enter the session timeout value. Values are in minutes and range from 1-30.
2. Click <Save> to save the settings.
3. Click the <Help> tab to display the Help menu. The menu defines the web session parameters.

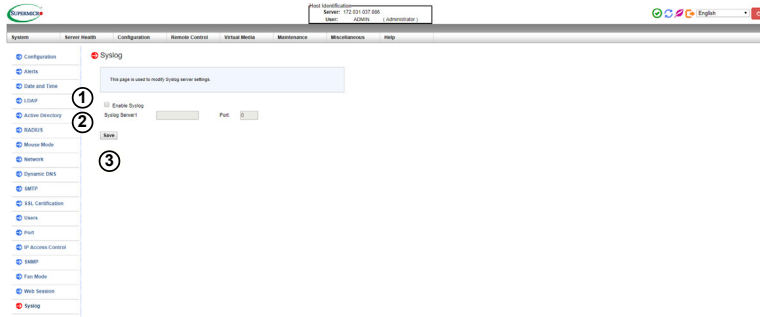
2-7-17 System Log

For X10 or Newer versions of Motherboards

This page allows you to configure Syslog setting. When you click on *Syslog* in the Options window, the following screen will display:

Note 1: SFT-OOB-LIC license is required for the feature.

Note 2: All Health Event Log and Maintenance Event Log information is available to the syslog server for X11 or newer versions of motherboards.



1. Check the box to enable Syslog. Once it is enabled, enter the information in the fields below.

2. Enter the IP address number of Syslog Server 1 and the port number in the field

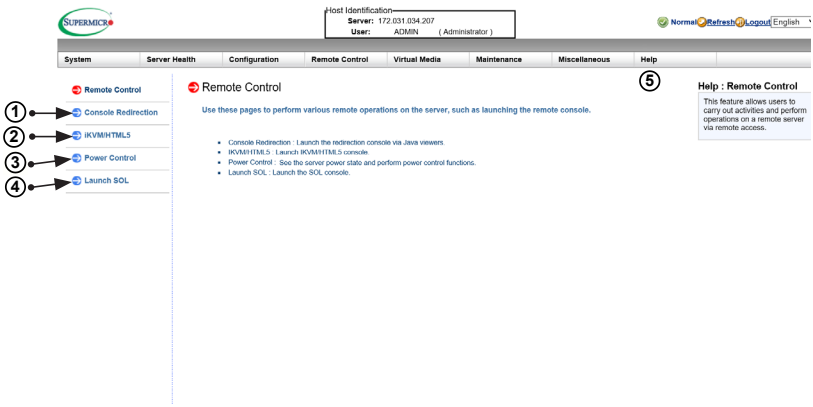
3. Click <Save> to save the settings

2-8 Remote Control

For X10 or Newer versions of Motherboards

This section allows the user to carry out activities and perform operations on a remote server via remote access. When you click *Remote Control* in the Options window, the following screen will display:

Note: Settings will vary by system.



1. Click *Console Redirection* to launch Console Redirection and configure the settings of the remote server. For more details on Console Redirection, please refer to "Launching Console Redirection" on the next page.

2. Click IKVM/HTML5 to to launch the remote console.

3. Click *Power Control* to display and configure the power settings of the remote console, including the following settings.

   - Reset Server
   - Power Off Server-Immediate

- Power Off Server-Orderly Shutdown
- Power On Server
- Power Cycle Server

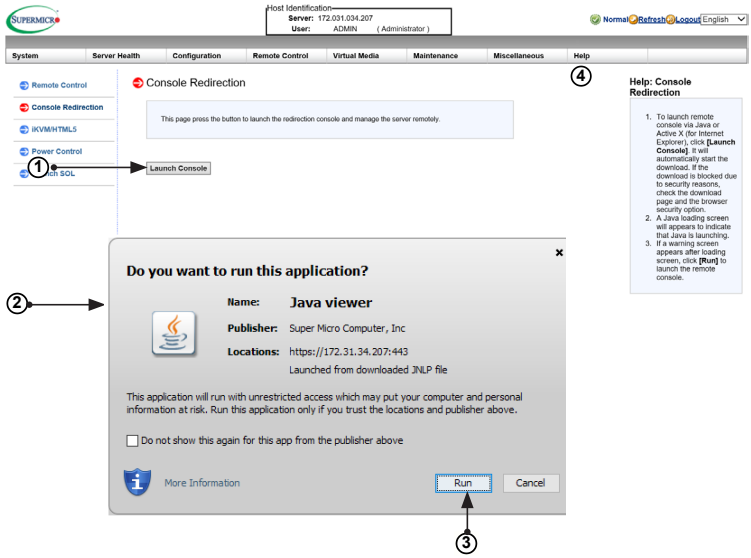
Once you have clicked the desired power setting, click "Perform Action" to change the power setting of the server.

4. Click *Launch SOL* to launch SOL (Serial Over LAN) console and manage the remote server.

5. Click <Help> to display the Help menu for the *Remote Control* page.

2-8-1 Launch Console Redirection

This feature allows you to launch Console Redirection via IKVM (keyboard, video/monitor, mouse) support. When you click *Console Redirection* in the Options window, the following screen will display:



1. Click <Launch Console> on the Console Redirection screen to launch the remote console via Java. You need to have Java installed in your system to launch the console.

2. A dialog box will display to indicate that Java is launching

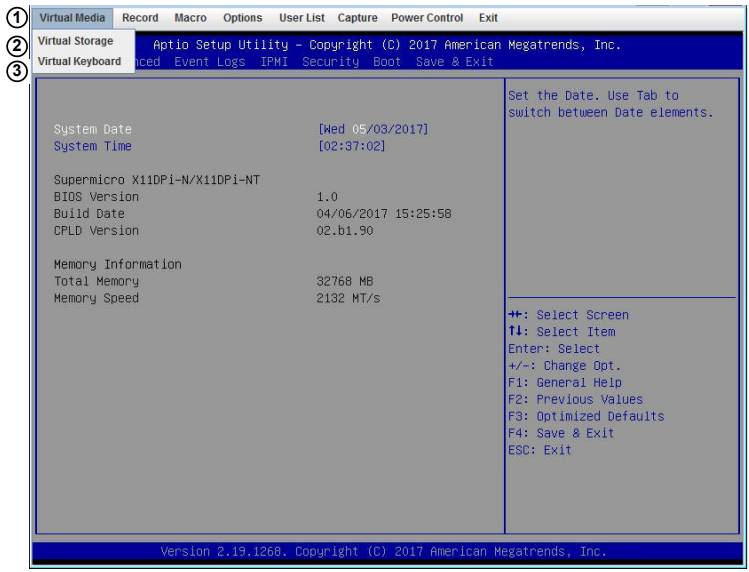
3. Click <Run> to launch the remote console. The main screen like the one below will appear. Note that your screen may not look exactly like the one below.

4. Click <Help> to display the Help menu for the *Console Redirection* page.

2-8-1a Console Redirection - Virtual Device

For X10 or Newer versions of Motherboards

This feature allows you to configure virtual device settings for your console redirection.



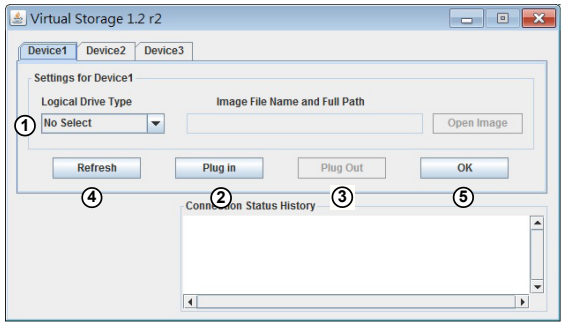
1. Click *Virtual Media* to configure virtual device settings of a server at a remote site via Console Redirection.

2. Click *Virtual Storage* to select a device you want to connect to the remote server as a virtual device.

3. Click *Virtual Keyboard* to launch the virtual keyboard.

Virtual Storage

When you click on *Virtual Storage* as described on the previous page, the following screen will appear. You are able to use up to three devices for virtual storage.



1. Select the logical drive type from the dropdown menu. The options are as follows:

   - *Upload IMA*: Select this feature to browse for an IMA file and upload it to the system.
   - *ISO File*: Select this feature to browse for an ISO file and upload it to the system.
   - *Web ISO*: Select this feature to select a Web ISO and mount it from the web page. The file will be mounted from the web interface. To specify the file location, set the image path on the CD-ROM Im- age page in the IPMI.
   - HD image: Use this feature to select a virtual HD image and install it into the system.
   - *C: SATA HD*: Use this feature to select a SATA HD from the local computer you are using to access the IPMI.
   - D: *SATA HD:* Use this feature to select a SATA HD from the local computer you are using to access the IPMI.

2. Click on <Plug in> to mount the selected drive.

3. Click on <Plug out> to unmount the selected drive.

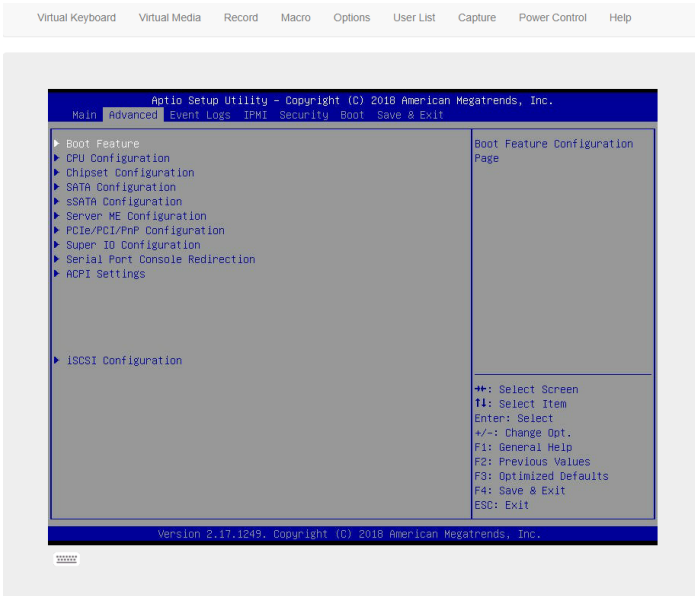
Virtual Keyboard

When you click on *Virtual Keyboard* in the Virtual Media menu, the virtual keyboard will appear.

2-8-1b HTML5

For X10 or Newer versions of Motherboards

This feature allows you to launch HTML5 via iKVM (keyboard, video/monitor, mouse) support. When you click *iKVM/HTML5* in the Options window, the following screen will display:



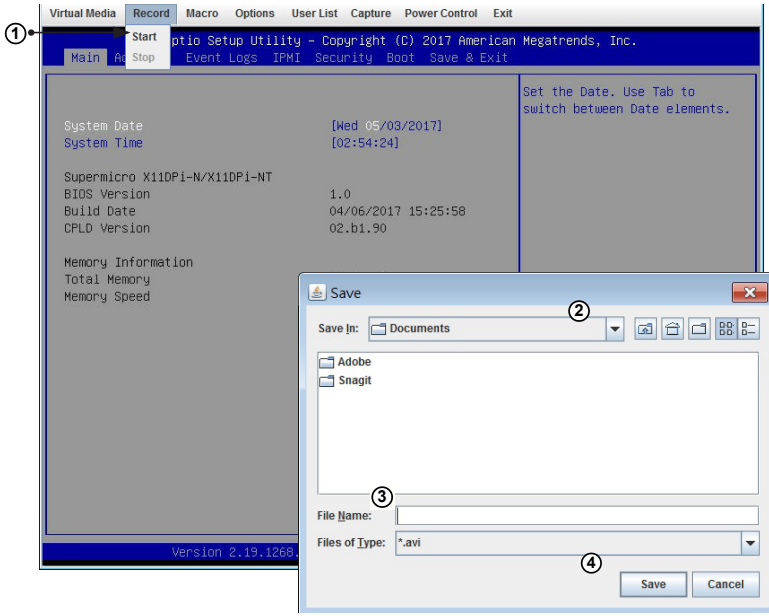
1. Click <iKVM/HTML5> to launch the remote console.

2. Click <Help> to display the Help menu for the *iKVM/HTML5* page.

2-8-1c Console Redirection - Record

For X10 or Newer versions of Motherboards

This feature allows you to record media displayed for your console redirection.



1. Click on *Start* from the Record menu to start recording. The window shown above will appear.

2. Then select the location to save the recording.

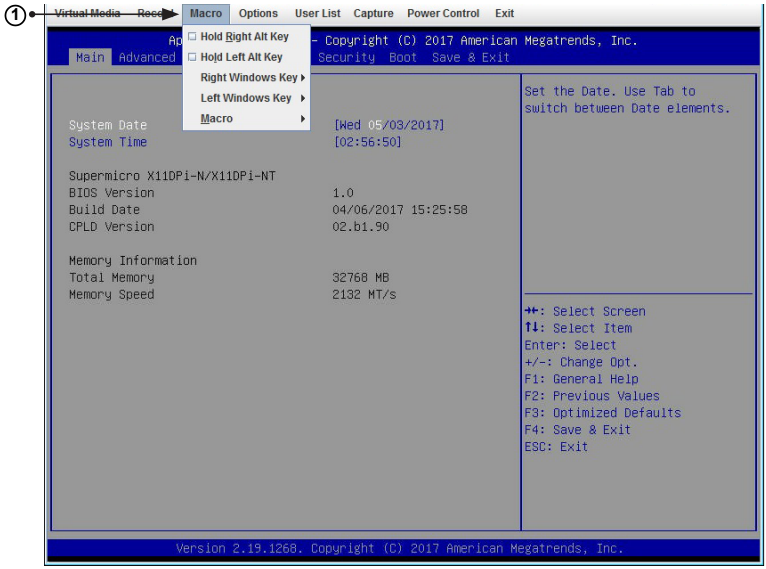
3. Enter a file name.

4. Click <Save> to save the settings and begin recording. If you want to exit the window without recording, click <Cancel>. The recording process will continue until you click on *Stop* under the Record menu.

2-8-1d Console Redirection - Macro

For X10 or Newer versions of Motherboards

This feature allows you to configure Macro settings for your console redirection.



1. Click *Macro* to configure the Macro settings for your remote server. The features include the following:

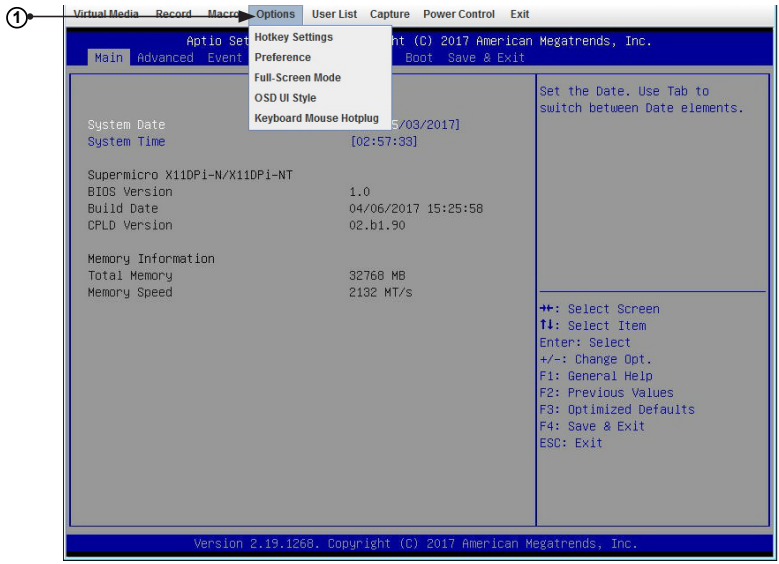
   - *Hold Right Alt Key:* This item performs the same function as holding down the right <Alt> key.
   - *Hold Left Alt Key*: This item performs the same function as holding down the left <Alt> key.
   - *Right Windows Key*: This item performs the same function as you pressing the right <Windows> key. 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*.

- Alt+Esc
- Ctrl+Esc
- Alt+Space
- Alt+Enter
- Alt+Hyphen
- Alt+F4
- Alt+PrntScrn
- PrntScrn
- F1
- Alt+F1
- Pause

2-8-1e Console Redirection - Options

For X10 or Newer versions of Motherboards

This feature allows you to configure Options settings for your console redirection.

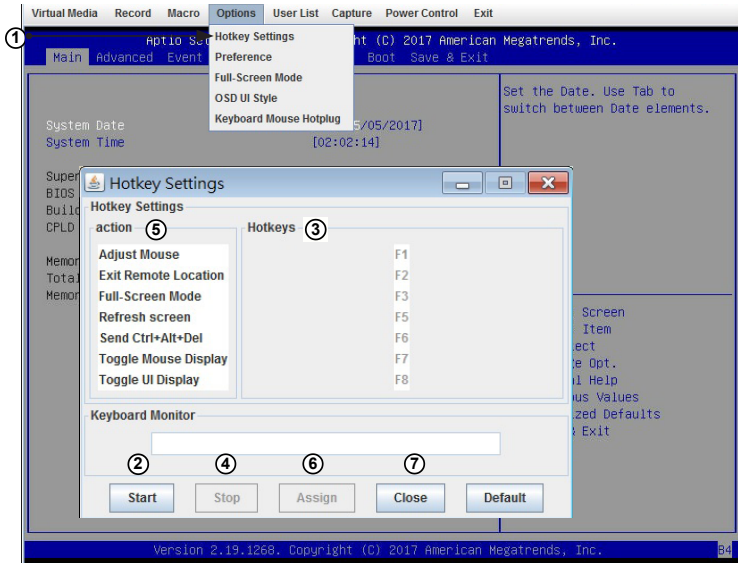


1. Click on *Options* to activate the pull-down menu to configure options settings. The options menu allows you to configure the following settines:

   - HotKey
   - Preference
   - Full-Screen Mode
   - OSD UI Style
   - Keyboard Mouse Hotplug

Options - Hotkey Settings

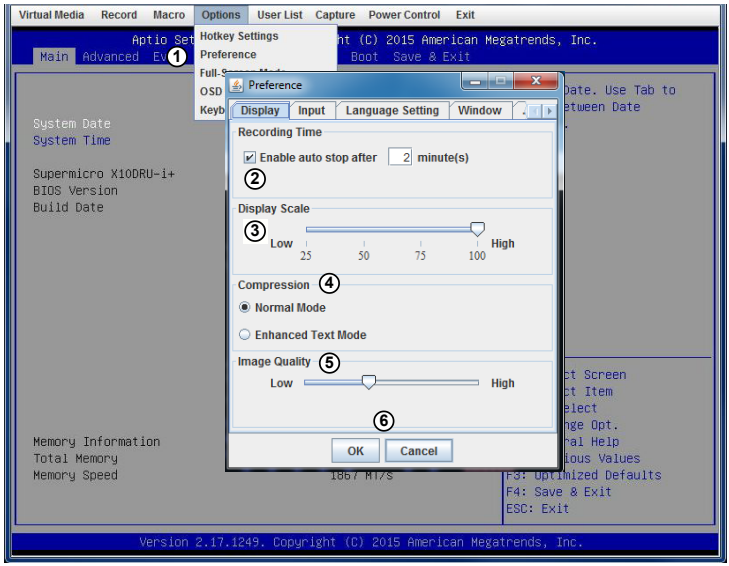
This feature allows you to configure the hotkey settings for your console redirection.



1. To assign a hotkey for an action, click *Hotkey Settings* under the Options menu. A Hotkey Settings window will appear.
2. Click <Start>
3. Enter the hotkey of your choice. It can be a single word or a combination.
4. Click <Stop>
5. Select an item from the action list.
6. Click <Assign>
7. Click <Close> to exit the window.

Options - Preference (Display)

This feature allows you to configure video recording settings for your remote console.



1. Click *Preference* under the Options menu. The *Preference* settings box will display. The first tab is *Display*.

2. The *Recording Time* section refers to video recording. If you want to automatically stop recording after a preset time, check the box, then input the number of minutes that should pass before the recording should automatically stop.

3. Use the slider on the Display Scale to set the appropriate scale setting for your display from Low (25) to High (100).

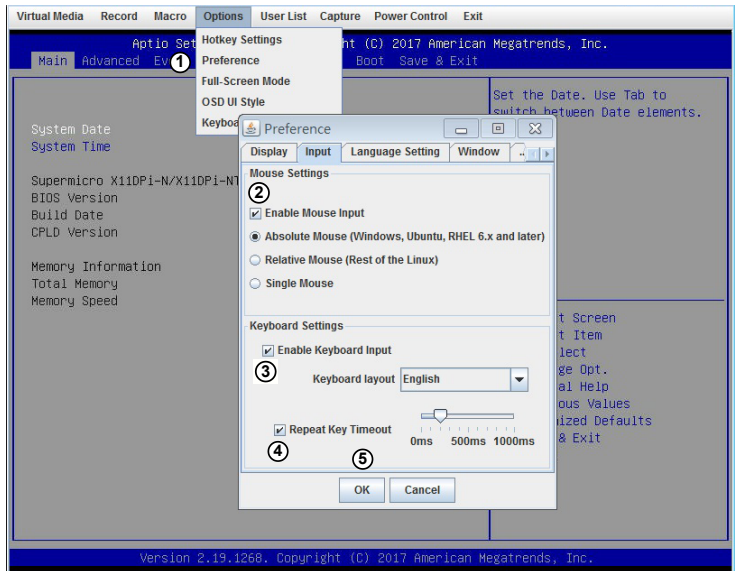
4. You can change the compression options under the *Compression* section.

5. You can adjust the image quality settings in accordance with varying degrees of network traffic. To ensure the best image quality, select *High* for heavier network traffic connections and select *Low* for lighter network traffic.

6. Click on <OK> to save the new settings. To exit the Preference window without saving, click <Cancel>.

Options - Preference (Input)

This feature allows you to configure input settings for your remote console.



1. When you click Preference under the Options menu, the Preference settings box will display. The second tab is *Input*.

2. Check the *Enable Mouse Input* box to enable mouse support so that you can use the mouse as an input device. Once mouse support is enabled, you need to set a proper mouse mode for your remote console. Check the corresponding radio button from the list below.

   - Select Absolute Mode if you have Windows, Ubuntu, and RHEL 6.x.
   - Select Relative Mouse for the Linux OS.
   - Single Mouse

3. Check the *Enable Keyboard Input* box to enable keyboard support so that you can use a soft keyboard as an input device. From the *Keyboard Layout* pull-down menu, select the right language setting for your soft keyboard. The language options are the following:

   - English

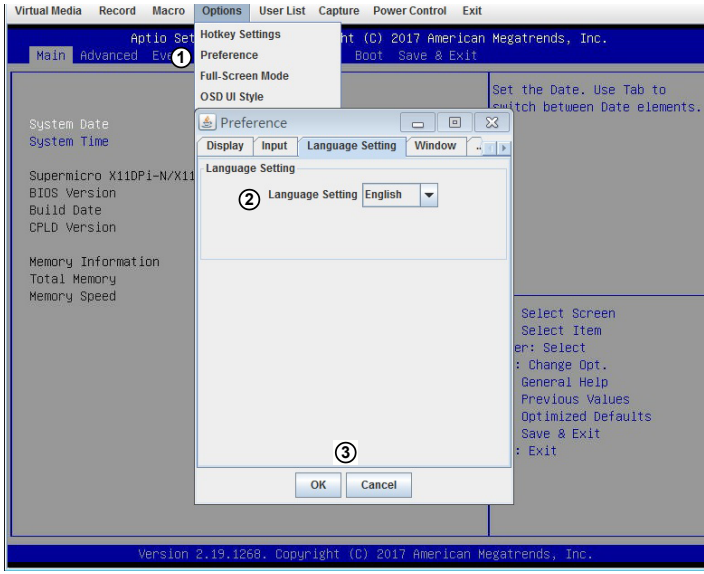
- Chinese (traditional)
- Japanese
- Germany
- French
- Spanish
- Korean
- Italian
- United Kingdom
- Swiss

4. To timeout repeated keystrokes, check the *Repeat Key Timeout* box, and use the slider on the scale to select the appropriate timeout settings for repeat keystrokes from 0ms to 1000ms (microseconds).

5. Click <OK> to save the new settings or click on <Cancel> to exit the *Preference* window without saving.

Options - Preference (Language Setting)

This feature allows you to configure language settings for your remote console.



1. When you click *Preference* under the Options menu, the *Preference* settings box will display. The third tab is *Language Setting*.

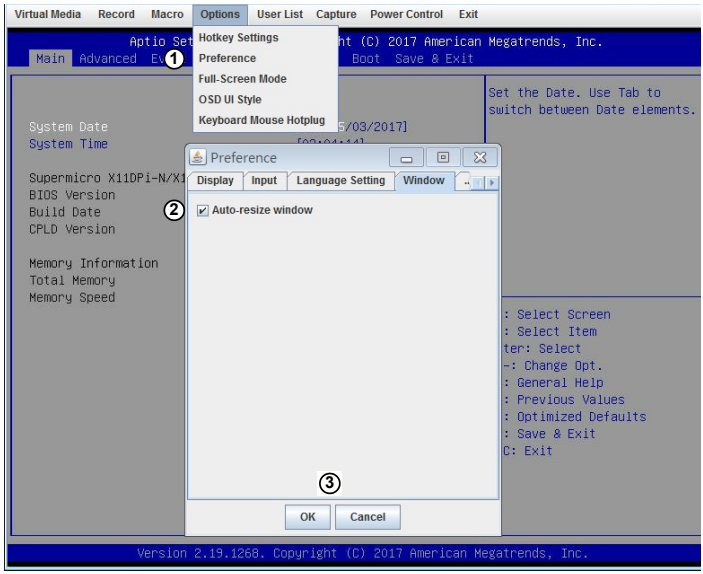
2. From the pull-down menu, select the language you want to use for your remote console. The language options are the following:

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

3. Click on <OK> to save the changes and exit the window. To exit without saving, click <Cancel>.

Options - Preference (Window)

This feature allows you to configure language settings for your remote console.



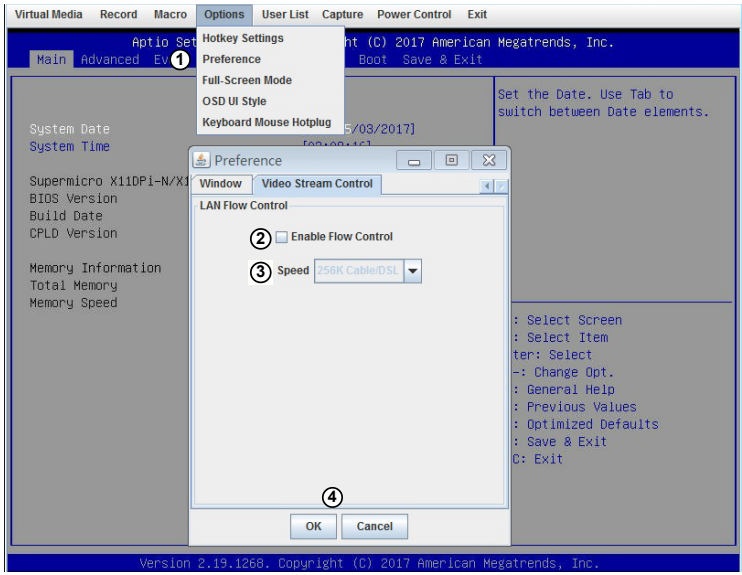
1. When you click *Preference* under the Options menu, the *Preference* settings box will display. The fourth tab is *Window*.

2. Check *Auto-resize window* to reset the size of your display window.

3. Click <OK> to save the change and exit the window. To exit without saving, click <Cancel> .

Options - Preference (Video Stream Control)

This feature allows you to configure window settings for your remote console.



1. When you click *Preference* under the Options menu, the *Preference* settings box will display. The last tab is *Video Stream Control*.

2. Check the *Enable Flow Control* box to enable support for video stream control.

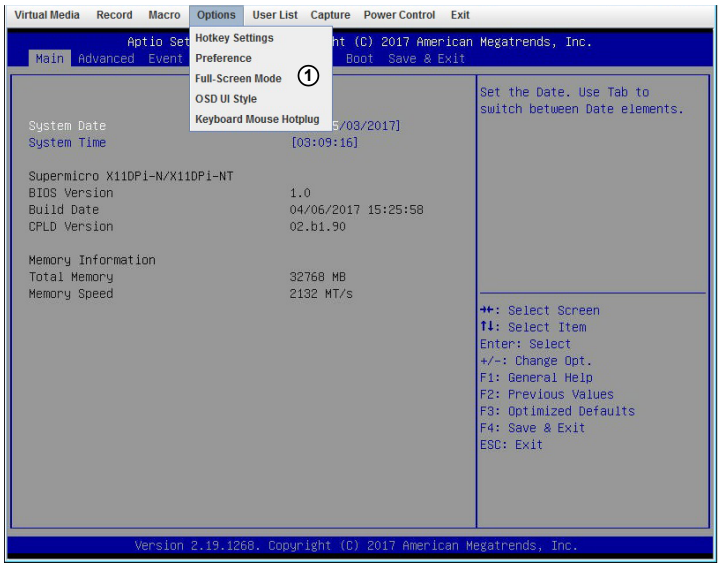
3. Select the speed from the pull-down menu. The options are as follows:

   - 256K Cable/DSL
   - T1
   - T2

4. Click <OK> to save the change and exit the window. To exit without saving, click <Cancel>.

Options - Full Screen Mode

This feature allows you to configure window settings for your remote console.

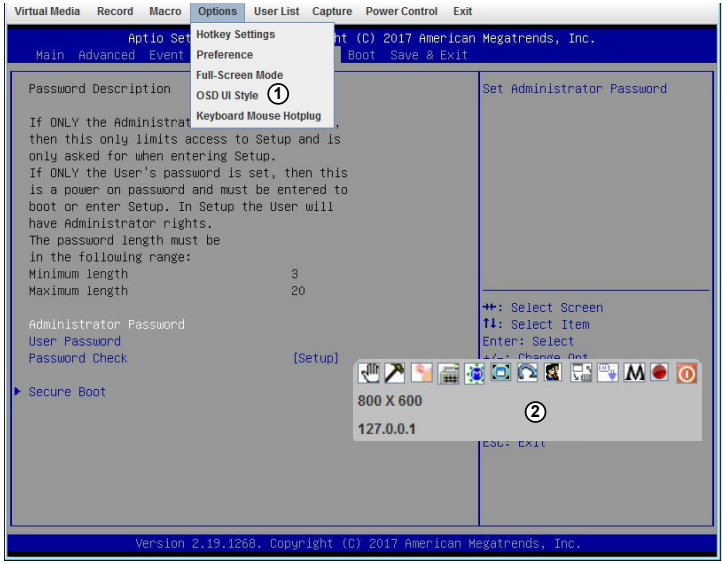


1. Click *Full Screen Mode* under the Options menu.

2. To leave the full-screen display, click *Leave Full-Screen Mode* under the Options menu.

Options - OSD UI Style

This feature allows you to configure OSD (On-Screen Display) UI (User Interface) style settings for your remote console.



1. Click on *OSD UI Style* under the Options menu.

2. A gray box with shortcut icons will appear. They are shortcuts to the main features provided by the firmware for your console redirection. Click on an icon to activate its function. See the next page for the list of icons and their functions.

1. **Move OSD:** Click and drag this icon to move the OSD UI pop-up screen to a new location on the display

2. **Hotkey Settings:** Click this icon to access the Hotkeys submenu and configure the settings.

3. **Virtual Storage:** Click this item to access the Virtual Media submenu andconfigure the settings.

4. **Virtual Keyboard:** Click this item to access the Virtual Keyboard submenu and use your virtual (soft) keyboard.

5. **Preference:** Click this item to access the Preferences window.

6. **Full-Screen Mode:** Click this item to change the size of your display window to the full screen mode.

7. **Exit:** Click this item to exit from the remote console.

8. **Show User List:** Click this item to display the user list.

9. **Menubar UI Style:** Click this item to change the toolbar display format.

10. **Keyboard Mouse Hotplug:** Click this item to hotplug keyboard and mouse.

11. **Macro:** Click this item to enable Macro support and use Macro features.

12. **Record:** Click this item to access the Video Recording submenu and to use video recording.

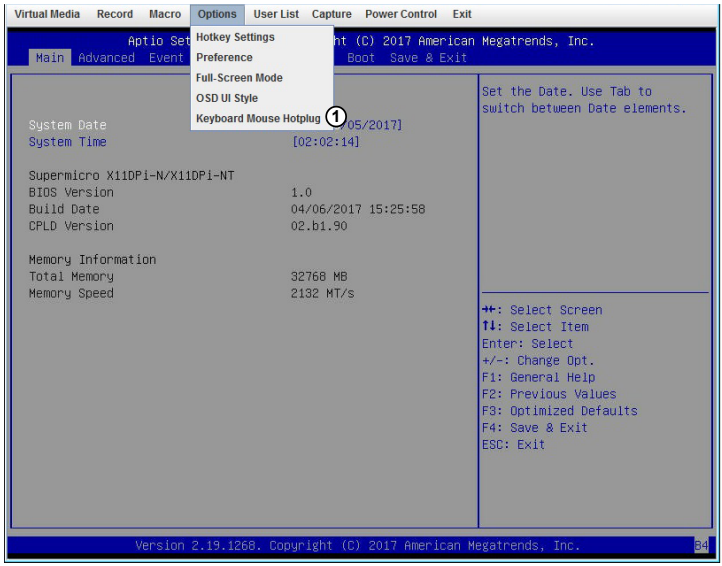
13. **Set power on-off:** Click this item to turn the system off.

14. **Resolution:** This item displays the remote console resolution in pixels.

15. **IP Address:** This item displays the IP address of the IPMI.

Options - Keyboard Mouse Hotplug

This feature allows you to enable keyboard/mouse hotplug support for your remote console.

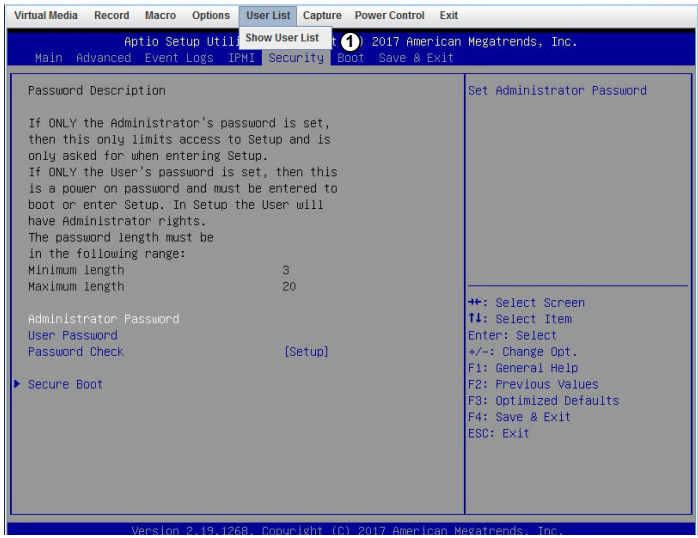


1. Click *Keyboard Mouse Hotplug* under the *Options* menu.

2-8-1f Console Redirection - User List

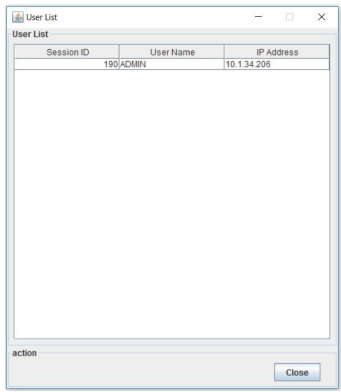
For X10 or Newer versions of Motherboards

This feature allows you to access the user list.



1. Click on *Show User List* under the Options to show the user list. A pop-up window will appear and show the following information:

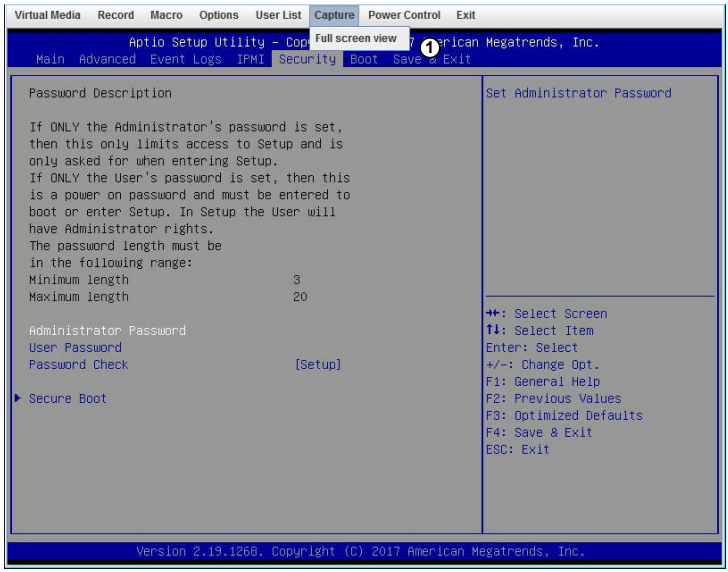
   - *Session ID:* This item displays the current session ID number.
   - *User Name:* This item displays the name of each user.
   - *IP Address:* This item displays the IP address of the client server.



2-8-1g Console Redirection - Capture

For X10 or Newer versions of Motherboards

This feature allows you to capture the screen displayed on your remote console.

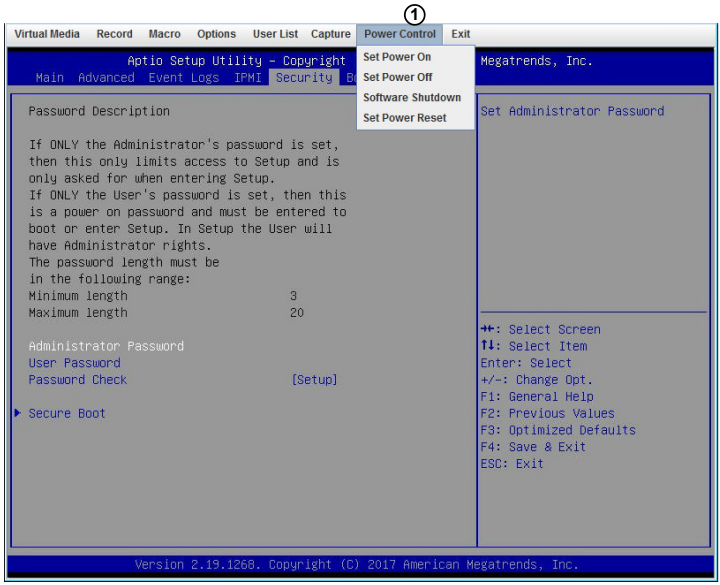


1. Click *Full screen view* under the *Capture* menu.

2-8-1h Console Redirection - Power Control

For X10 or Newer versions of Motherboards

Under the Power Control menu, you can manage the power state of the system.

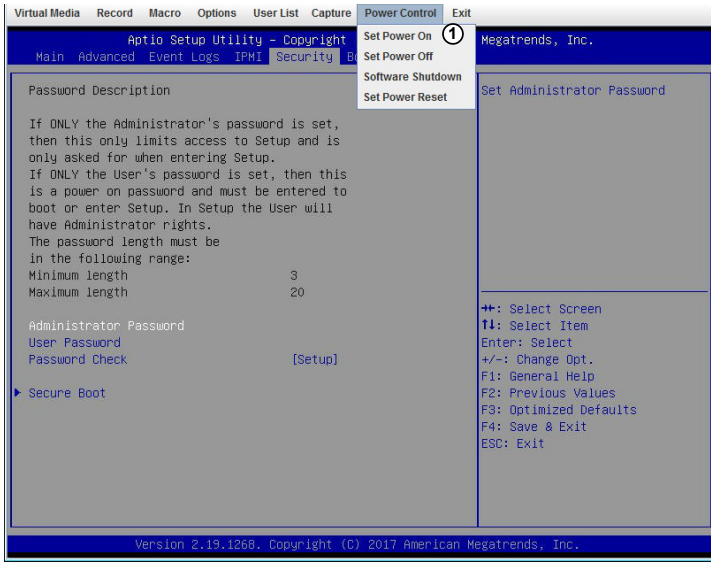


1. The power control features are the following:

   - *Set Power On:* This feature allows you to turn the system on.
   - *Set Power Off:* This feature allows you to turn the system off.
   - *Software Shutdown:* This feature allows you to perform a graceful shutdown of the system.
   - *Set Power Reset*: This feature allows you to reset the system.

Power Control - Set Power On

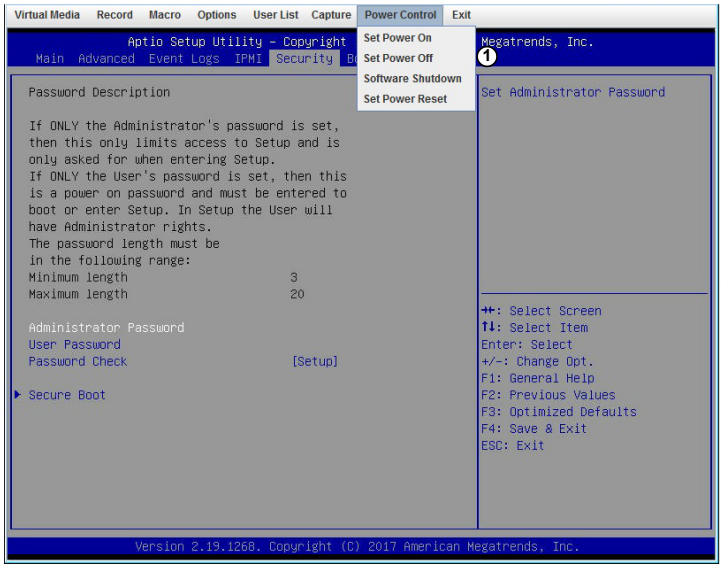
The *Set Power On* option allows you to power on the system if the system is off.



1. Click the *Set Power On* option under the *Power Control* menu.

Power Control - Set Power Off

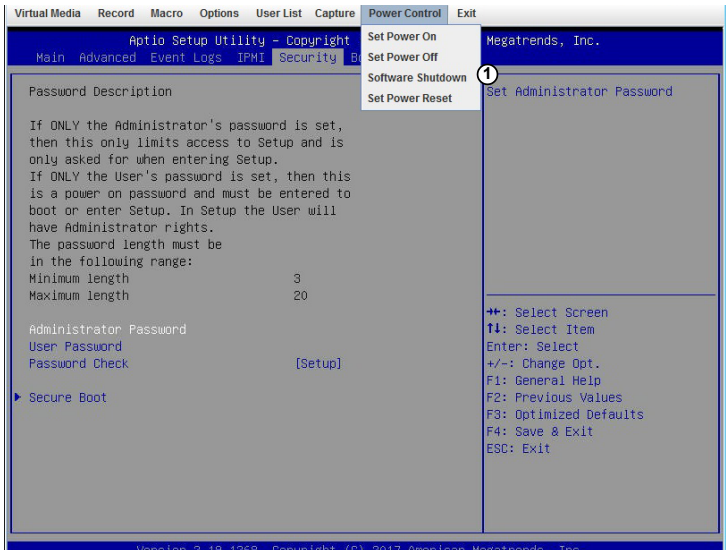
The *Set Power On* option allows you to power off the system if the system is on.



1. Click the *Set Power Off* option under the *Power Control* menu.

Power Control - Software Shutdown

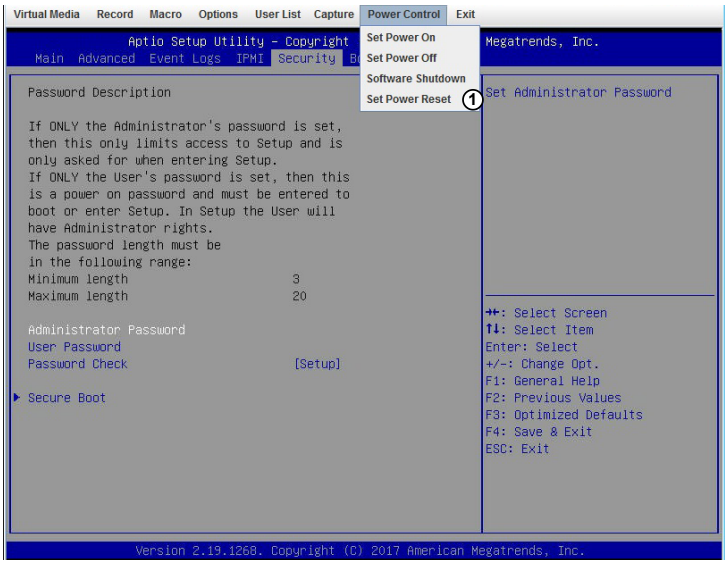
The *Software Shutdown* option allows you to perform a graceful shutdown of the operating system.



1. Click the *Software Shutdown* option under the *Power Control* menu.

Power Control - Set Power Reset

The *Set Power On* option allows you to reset the system.

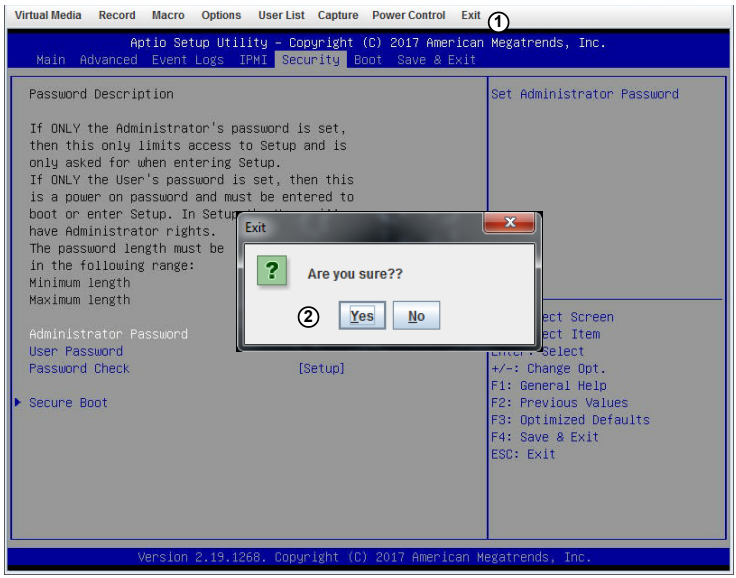


1. Click the *Set Power Reset* option under the *Power Control* menu.

2-8-1i Console Redirection - Exit

For X10 or Newer versions of Motherboards

Under the Power Control menu, you can manage the power state of the system.



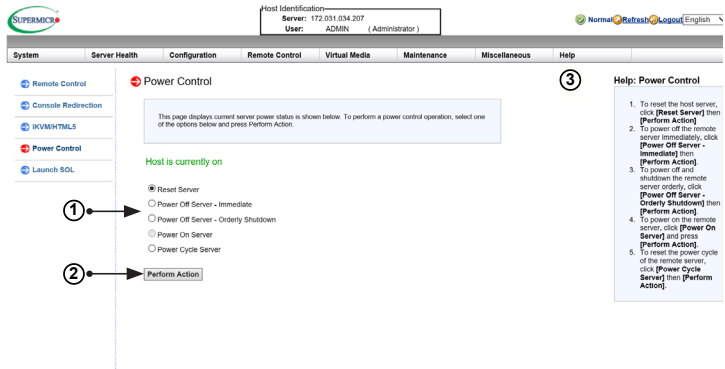
1. To exit the Console Redirection, click on *Exit* under the *Exit* menu.

2. Click on <Yes> in the Exit dialog box to exit.

2-8-2 Power Control

For X10 or Newer versions of Motherboards

This feature allows the user to check the power state and manage the system. When you click on *Power Control* in the Options window, the following screen will display.



1. To enter the screen shown above, click the "Power Control" item in the Remote Control sidebar. The following options are listed:

   - Click on *Reset Server* to reset the host server.
   - Click on *Power Off Server - Immediate* to power off the remote server immediately.
   - Click on *Power Off Server - Orderly Shutdown* to power off and shutdown the remote server in an orderly fashion.
   - Click *Power On Server* to power on the remote server.
   - Click *Power Cycle Server* to power cycle the remote server.

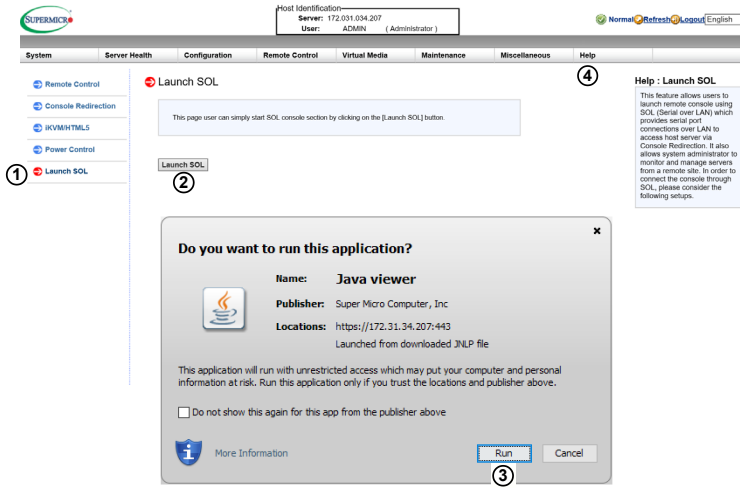
2. Click <Perform Action> after choosing an option to commence

3. Click the <Help> tab to display the Help menu. The menu includes an explanation of all the power modes.

2-8-3 Launch SOL

For X10 or Newer versions of Motherboards

This feature allows you to launch the remote console by using SOL (Serial over LAN). This feature provides serial port connections over LAN to allow the user to access a host server via console redirection. It also allows a system administrator to monitor and manage a server from a remote site.

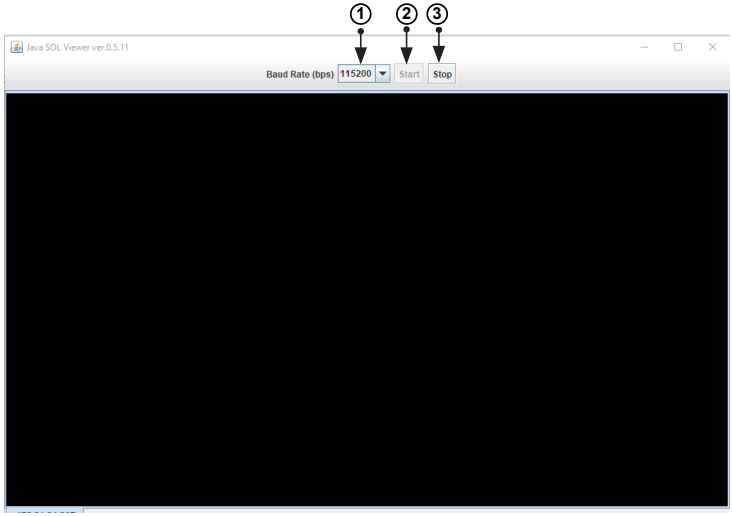


1. To enter the screen shown above, click *Launch SOL* in the left column.

2. Click the <Launch SOL> button to launch SOL.

3. In the dialog box that asks "Do you want to run this application?" click <Run>. The SOL Viewer screen will appear as shown on the next page.

4. Click the <Help> tab to display the Help menu. The menu includes an explanation of the SOL Console.



1. You can select a baud rate (bps) from the pull-down menu as your SOL transfer rate. The options are listed below. Make sure that the baud rate selected here matches the baud rate set in the UEFI BIOS.

   - 9600 bps (bits per second)
   - 19200 bps
   - 38400 bps
   - 57600 bps
   - 115200 bps

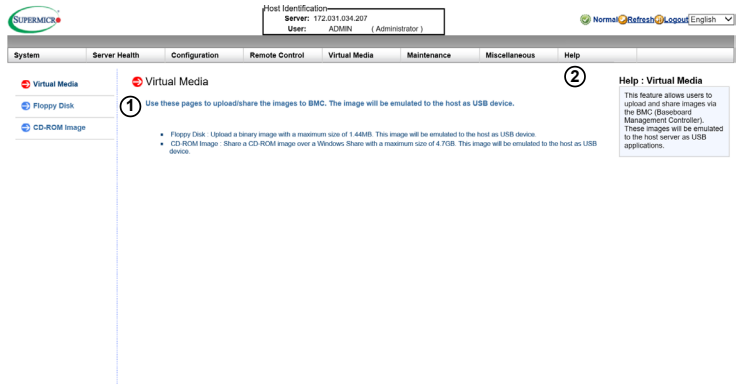
2. Once you have selected the baud rate, click <Start> to start the session. Once you have started the session, you can input SOL commands through the command-line interface.

3. Click <Stop> to stop the SOL connection.

2-9 Virtual Media

For X10 or Newer versions of Motherboards

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. When you click *Virtual Media* in the Options window, the following screen will display:



1. This section shows information related to virtual media, such as the Floppy Disk and the CD-ROM Image.

   - Floppy Disk: Upload a binary image with a maximum size of 1.44MB. This image will be emulated to the host as a USB device.

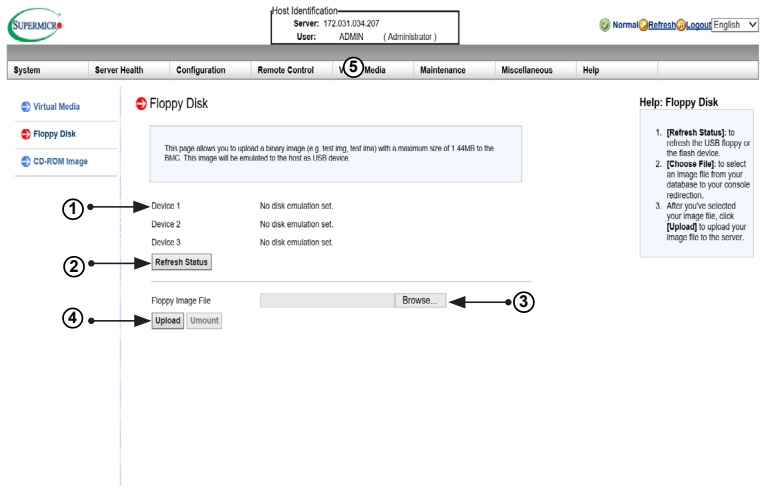
   - CD-ROM Image: Share a CD-ROM image over Windows Share with a maximum size of 4.7GB. This image will be emulated to the host as a USB device.

2. Click the <Help> tab to display the Help menu for the *Virtual Media* page.

2-9-1 Floppy Disk

For X10 or Newer versions of Motherboards

This feature allows you to configure the Floppy Disk image files for sharing. When you click *Floppy Disk* in the Options window, the following screen will display:



1. Dislpays a list of devices and their status (e.g. Device 1, Device 2, Device 3).

2. Click <Refresh Status> to refresh the Floppy Disk.

3. Click <Browse> to select an image file from a specified location for your console redirection.

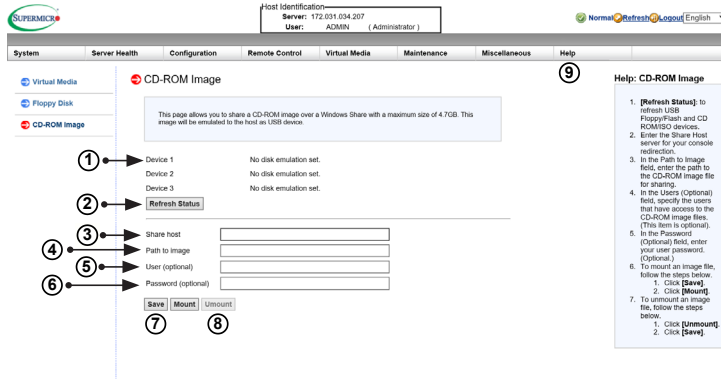
4. After you have selected your image file, click <Upload> to upload your image file to the server.

5. Click the <Help> tab to display the Help menu. The menu explains the function of each button on the page.

2-9-2 CD-ROM Image

For X10 or Newer versions of Motherboards

This feature allows you to configure CD-ROM image files for sharing. When you click *CD-ROM Image* in the Options window, the following screen will display:

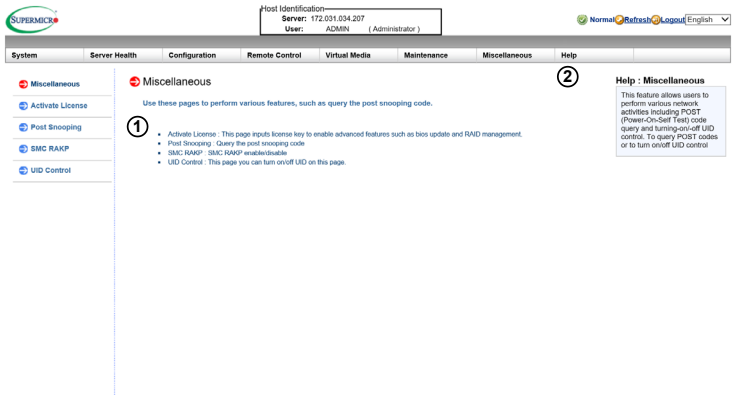


1. Dislpays a list of devices and their status (e.g. Device 1, Device 2, Device 3).
2. Click <Refresh Status> to refresh *USB Floppy/Flash* and *CD ROM/ISO* devices.
3. Enter the *Share Host* server for your console redirection.
4. In the *Path to Image* field, enter the path to the CD-ROM image file for sharing.
5. In the *Users (Optional)* field, specify the users that have access to the CD-ROM image files. (This item is optional).
6. In the *Password (Optional)* field, enter your user password. (Optional)
7. To *mount* an image file, click <Save> and then <Mount>.
8. To *unmount* an image file, click <Unmount> and then <Save>.
9. Click the <Help> tab to display the Help menu. The menu inlcudes instructions on how to share a CD-ROM image.

2-10 Maintenance

For X10 or Newer versions of Motherboards

Use this feature to manage and configure IPMI device settings. When you click *Maintenance* in the Options window, the following screen will display:



1. This screen displays the following items:

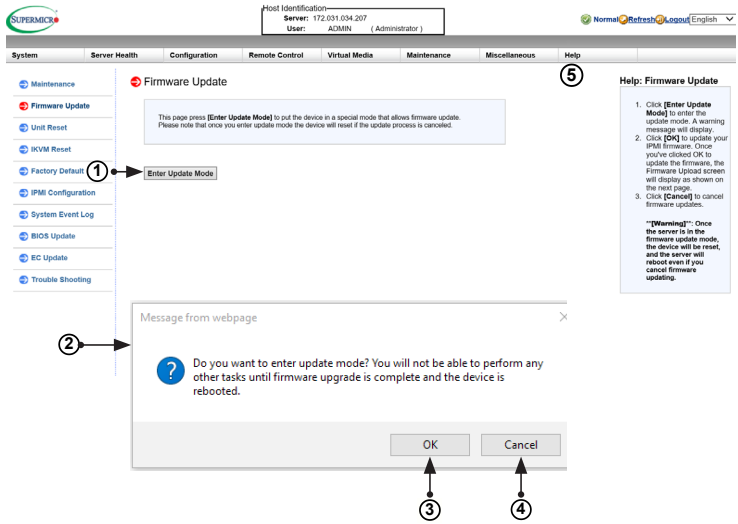
   - Firmware Update: Click this item to update the remote server's BMC firmware. The Firmware Update screen is shown in the next section.
   - Unit Reset: Click this item to reboot the BMC (IPMI) controller.
   - IKVM Reset: Click this item to reset the IKVM setting.
   - Factory Default: Click this item to restore IPMI to the factory default settings.
   - IPMI Configuration: Click this item to save IPMI configuration settings to a file or to load IPMI configuration settings from a file.
   - System Event Log: Click this this item to turn on or off the system event log.
   - UEFI BIOS Update: Click this item to update the UEFI BIOS.

2. Click the <Help> tab to display the Help menu for the *Maintenance* page.

2-10-1 Firmware Update

For X10 or Newer versions of Motherboards

Use this feature to update the IPMI firmware. When you click *Firmware Update* in the Options window, the following screen will display:



To update IPMI Firmware, follow the instructions below.

1. Click <Enter Update Mode>.

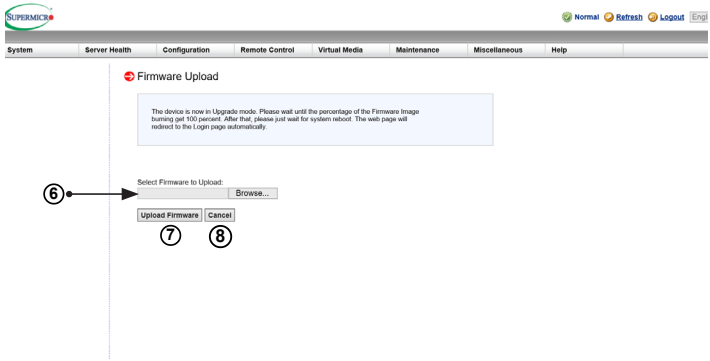
2. A dialog box will appear. It will ask: "Do you want to enter update mode?" Click <OK> to proceed with the update.

3. Click <OK> to update your IPMI firmware. After you click <OK> to update the firmware, the *Firmware Upload* screen will display as shown on the next page.

4. Click <Cancel> to cancel firmware updates.

5. Click the <Help> tab to display the Help menu. The menu includes instructions on how to update the firmware.

After you click <OK> to update the IPMI Firmware, the following Firmware Upload screen will display as shown below.



6. Enter the name of the firmware you wish to upload. You can also select a firmware specified location by clicking <Choose File>.

7. Click <Upload Firmware> to upload the selected firmware to the host server.

   Warning: To properly update your firmware, do not interrupt the process. The system will reboot after the firmware update is complete.

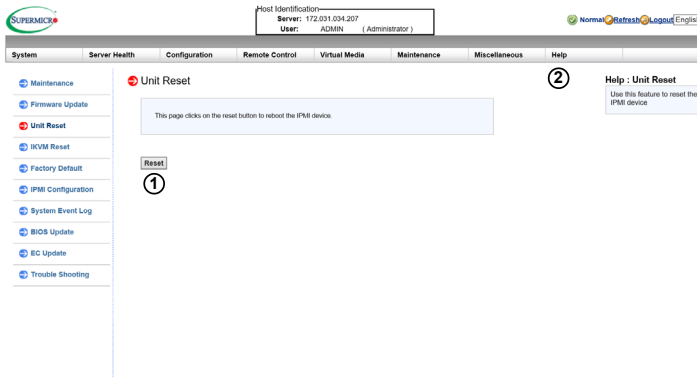
8. Click <Cancel> to abort firmware uploading.

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

2-10-2 Unit Reset

For X10 or Newer versions of Motherboards

Use this feature to reset the IPMI device. When you click *Unit Reset* in the Options window, the following screen will display:



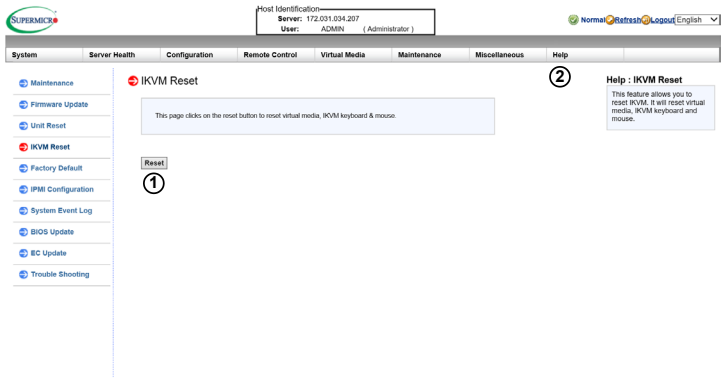
1. Click <Reset> to reset the IPMI device.

2. Click the <Help> tab to display the Help menu for the *Unit Reset* page.

2-10-3 IKVM Reset

For X10 or Newer versions of Motherboards

This feature allows you to reset IKVM. It will reset virtual media, as well as the IKVM keyboard and mouse. When you click *IKVM Reset* in the Options window, the following screen will display:



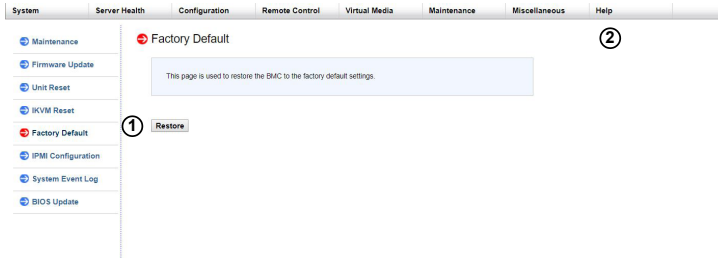
1. Click <Reset> to reset virtual media, as well as the IKVM keyboard and mouse.

2. Click the <Help> tab to display the Help menu for the *IKVM Reset* page.

2-10-4 Factory Default

For X10 or Newer versions of Motherboards

This feature allows the user to restore IPMI to factory default settings. When you click *Factory Default* in the Options window, the following screen will display:



1. Click <Restore> to reset the IPMI to factory default settings. The IPMI connection will reset.

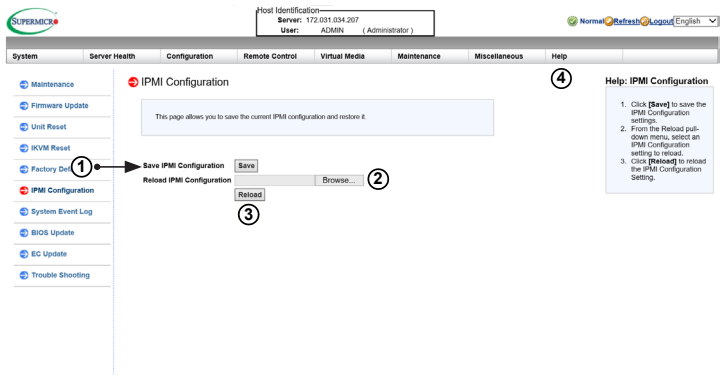
2. Click the <Help> tab to display the Help menu for the *Factory Default* page.

2-10-5 IPMI Configuration

For X10 or Newer versions of Motherboards

This feature allows the user to save IPMI configuration settings and restore it. When you click *IPMI Configuration* in the Options window, the following screen will display:

1. Click <Save> to save the current IPMI configuration.



2. Click <Choose file> to select a configuration from specified location to reload.

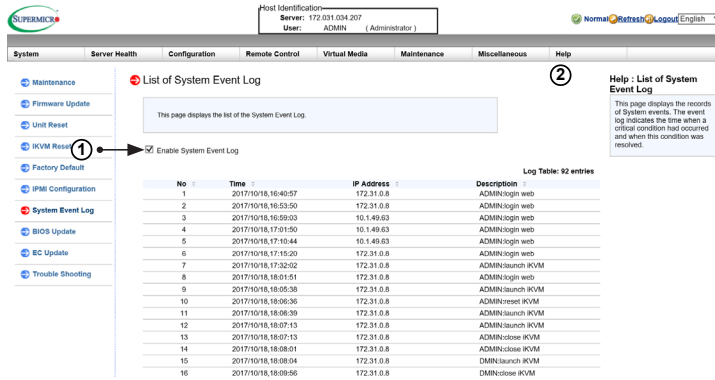
3. Click <Reload> to save the IPMI Configuration settings.

4. Click the <Help> tab to display the Help menu. The menu includes instructions on how to configure the IPMI configuration.

2-10-6 System Event Log

For X10 or Newer versions of Motherboards

This feature displays a list of the system event log. When you click *System Event Log* in the Options window, the following screen will display:

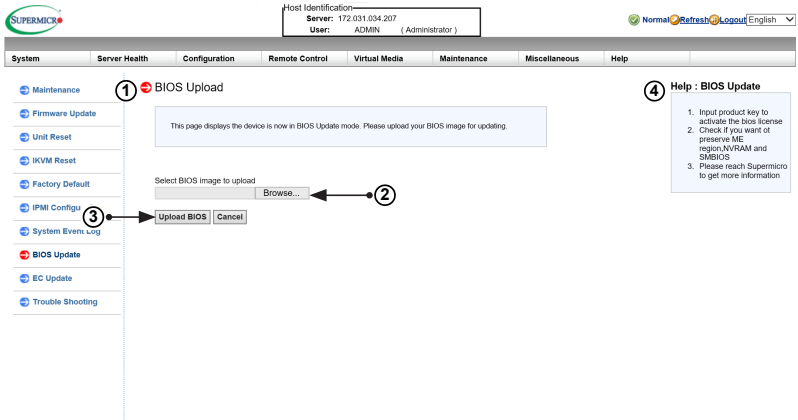


1. Check the <Enable System Event Log> box to display the records of system events.

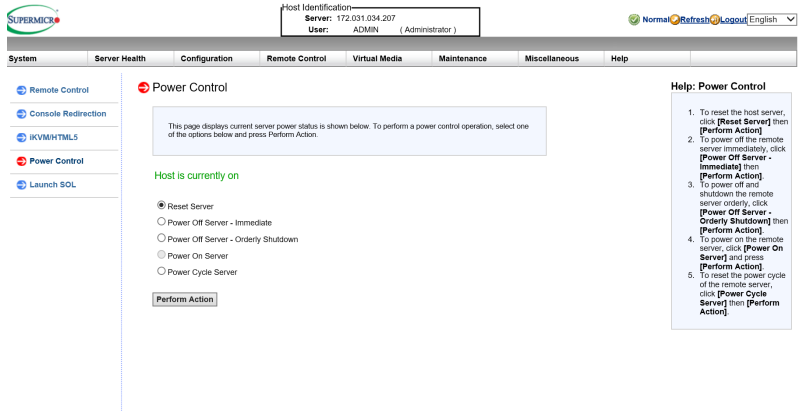
2. Click the <Help> tab to display the Help menu for the *System Event Log* page.

2-10-7 UEFI BIOS Update

This feature allows the user to update the UEFI BIOS. When you click *UEFI BIOS Update* in the Options window, the following screen will display:



Click <OK>, and you will be redirected to the following page to power down the system.



Note: For the UEFI BIOS update to take effect, please reboot the system.

To update UEFI BIOS, follow the instructions below:

1. Check node product key status. If key status is inactive, enter product key to activate the UEFI BIOS license.
2. Click <Choose File> to select a UEFI BIOS image to upload.
3. Click <Upload UEFI BIOS> to begin updating process.
4. Check the following options if you want to make any preservation:
   - ME region (Management)
   - NVRAM (Non-volatile Random-Access Memory)
   - SMUEFI BIOS (System Management UEFI BIOS)
5. Click <Start Upgrade> to initiate the process.

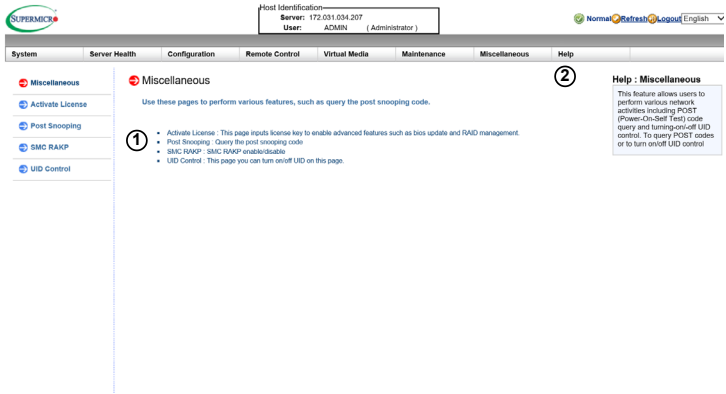
   Warning: Once the server is in update mode, UEFI BIOS will reset in order to go back to normal operating mode even if you abort the update process.

Note: All of the X9 generation UP (single processor) motherboards do not have this feature, except X9 DP.

UEFI BIOS Fea-	Support
OOB Flash UEFI	N
OOB Update Setting	N
OOB Change SMUEFI	N
InBand Flash UEFI	N
InBand Update Setting	N
InBand Change SMUEFI	N
InBand SMI E7h support	N

2-11 Miscellaenous

This screen displays various features that the user can perform. When you click *Miscellaneous* in the Options window, the following screen will display:



1. This screen displays the following information:

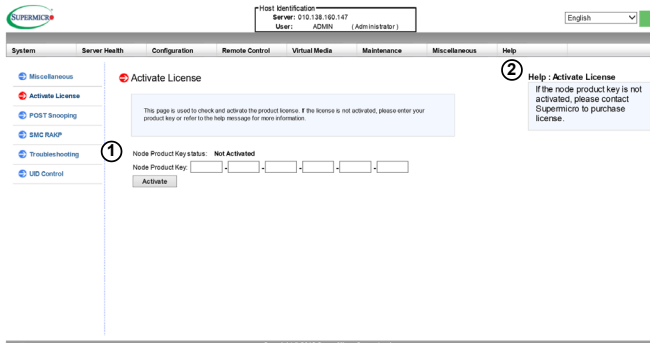
   - Activate License: Input license key to enable advanced features such as UEFI BIOS update and RAID management.
   - Post Snooping: Query the post snooping code.
   - SMC RAKP: SMC RAKP enable/disable.
   - UID Control: Turn on or off the UID on this page.

2. Click the <Help> tab to display the Help menu for the Miscellaneous page.

2-11-1 Activate License

For X10 or Newer versions of Motherboards

This page displays the Node Product Key. Enter the license key to enable features such as OOB (Out of Band) UEFI BIOS update and RAID management. The license key is a paid feature and is optional. The license key part number is SFT-OOB-LIC and can be purchased from the Supermicro Sales department or a reseller. One key can be used per board.



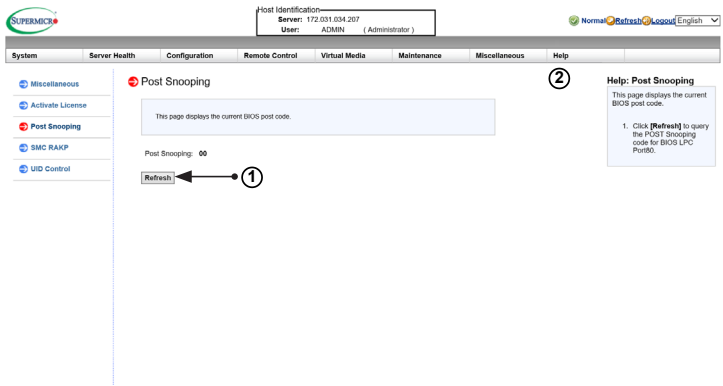
1. This feature displays the Node Product Key.

2. Click the <Help> tab to display the Help menu for the Activate License page.

2-11-2 Post Snooping

For X10 or Newer versions of Motherboards

This page displays the current UEFI BIOS code. When you click *Post Snooping* in the Options window, the following screen will display:



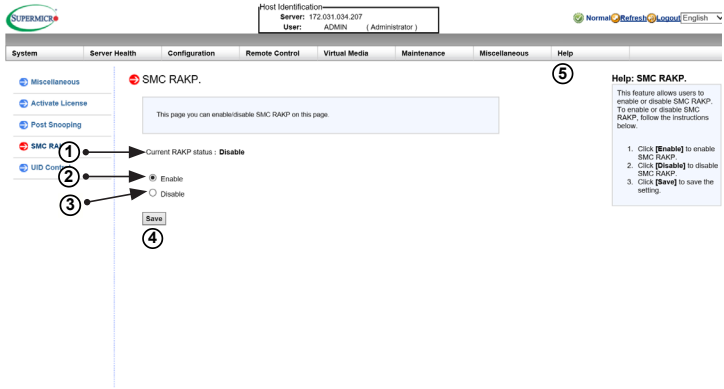
1. Displays the current UEFI BIOS code.

2. Click the <Help> tab to display the Help menu for the Post Snooping page.

2-11-3 SMC RAKP

For X10 or Newer versions of Motherboards

This feature allows the user to enable or disable the SMC RAKP (Remote Authenticated Key-Exchange Protocol). When you click *SMC RAKP* in the Options window, the following screen will display:

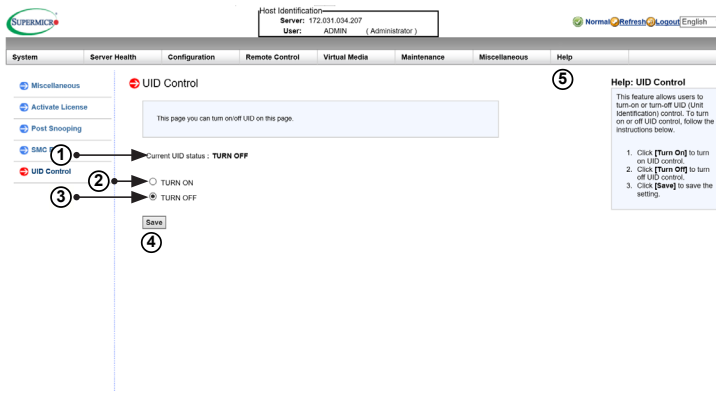


1. This feature displays the current RAKP status.
2. Click <Enable> to enable RAKP.
3. Click <Disable> to disable RAKP.
4. Click <Save> to save the changes.
5. Click the <Help> tab to display the Help menu. The menu inlcudes instructions on how to enable or disable SMC RAKP.

2-11-4 UID Control

For X10 or Newer versions of Motherboards

This feature allows the user to turn on or off the UID (Unit Identification). When you click *UID Control* in the Options window, the following screen will display:



1. This feature displays the current UID status.
2. Click <TURN ON> to turn on the Unit identification.
3. Click <TURN OFF> to turn off the Unit Identification.
4. Click <Save> to save the settings.
5. Click the <Help> tab to display the Help menu. The menu inlcudes instructions on how to turn on or off the UID.

Chapter 3

Frequently Asked Questions

3-1 Frequently Asked Questions

Question: How do I flash the IPMI 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 IPMI connection?

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

HTTP: 80 (TCP)

HTTPS: 443 (TCP)

IPMI: 623 (UDP)

Remote console: 5900 (TCP)

Virtual media: 623 (TCP)

SMASH: 22 (TCP)

WS-MAN: 8889 (TCP)

Question: When I update the IPMI 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. Some anti-virus softwares can cause this. Disable your anti-virus software temporarily and update your firmware.

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

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

Appendix A

Flash Tools

A-1 Overview

This chapter provides instructions on how to use ATEN Flash Tools, which supports firmware updates and firmware dumping.

Firmware Updates

The ATEN Flash Tools utility provides a complete solution for firmware updates. Users can flash the firmware using DOS, Windows or Linux. In addition, Windows and Linux allow the user to update the firmware via LAN or KCS.

Firmware Dumping

Firmware dumping is supported by DOS, Windows and Linux. In addition to firmware updating, ATEN Flash Tools also supports firmware dumping from the BMC (Baseboard Management Controller). You can use this feature to back up the firmware by *dumping* the current version of the firmware to an archive folder before updating to a new version. It will also allow you to flash other BMCs in the factory for mass production.

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

A-2 Reference

ATEN Flash Tools Utility was built in reference to the IPMI - Intelligent Platform Management Interface Specification Second Generation v2.0, Document Revision 1.0, February 12, 2004, by Intel, Hewlett-Packard, NEC, and Dell.

A-3 Using ATEN Flash Tools in the DOS Environment

To use the ATEN Flash Tools in DOS, follow the steps below:

1. At the command line prompt, type “cd /specify location” to change to the directory where the flash tool is located. Example: “cd /temp”

2. At the command line prompt, type "AwUpdate.exe" and press <Enter>.

3. The information about the utility will be displayed. Follow the instructions given on the screen to configure the settings as shown in Figure 1.

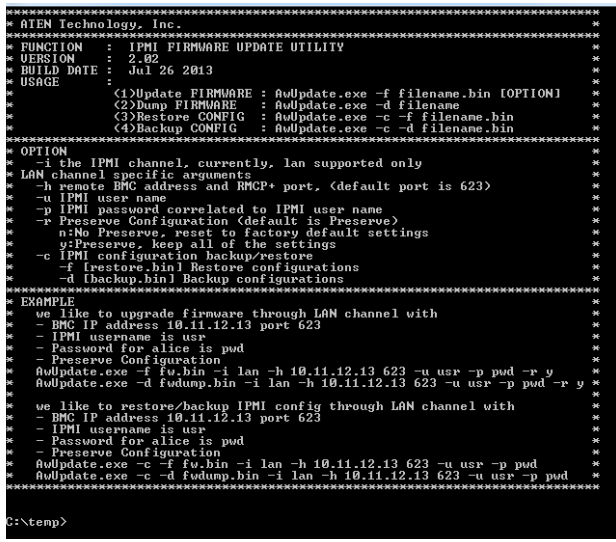


Figure 1: IPMI Firmware Updates Utility in DOS - Main Screen

The main screen of the IPMI Update Utility for DOS (above) displays the version and the built date of the utility currently used in the system. The DOS version of Flash Tools Utility allows the user to update or dump the firmware via KCS channels.

Firmware Updating via KCS Channels

To update your firmware via KCS (Keyboard Controller Style), type <dUpdate.exe –f [filename.bin] *–r y*.>. After entering this command, a screen will display as shown in Figure 2.

1. –f: Type <-f> to enter the file name of the firmware that you want to update.

2. –r: Type <-r> to preserve the configuration settings you've chosen. This feature is optional. The default setting is to "preserve" the configuration.

3. y: Type <y> for the BMC to keep all settings after the firmware is updated; otherwise, the BMC will reset all settings to factory default.

After you have entered the commands above, ATEN Flash Tools will start to update the firmware. There are two phases in firmware updating.

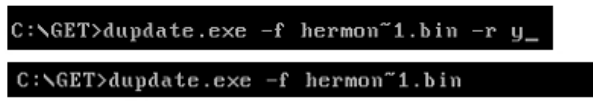


Figure 2: Examples of Firmware Updates with or without the "Preserved" Command

1. Phase 1 is to transfer the FW image file to the BMC. In this phase, Flash Tools will transfer three parts to the BMC as shown in Figure 3, Figure 4 and Figure 5.

Figure 3: Transferring (Part 0)

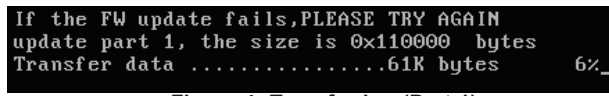


Figure 4: Transferring (Part 1)

Figure 5: Transferring (Part 2)

2. Phase 2 is to flash the new firmware. The progress of firmware updating will be displayed as shown in Figure 6. After the firmware is completely updated, the BMC will reboot. Please wait for the BMC to complete system reboot (Figure 7).

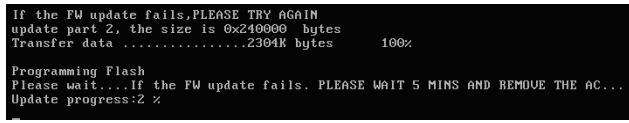


Figure 6: Progress of Firmware Updating

Figure 7: Updates Completed

Dumping Firmware from the BMC via KCS channels

The user can dump the firmware by typing <dupdate.exe –d [filename].>. Flash Tools will dump the firmware into the file that the user has assigned in the previous command. In the example given in Figure 8, Flash Tools will dump the firmware to dump_img.

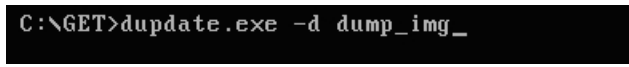


Figure 8: Example of Firmware Dumping via KCS

There are two phases in firmware dumping.

1. During Phase 1, the Flash Tools Utility is waiting for the BMC to prepare the firmware for dumping. As soon as preparation is complete, the Flash Tools Utility will enter Phase 2.

2. In Phase 2, the Flash Tools utility gets the firmware from the BMC. The user can see the progress on the screen as shown in Figure 10.

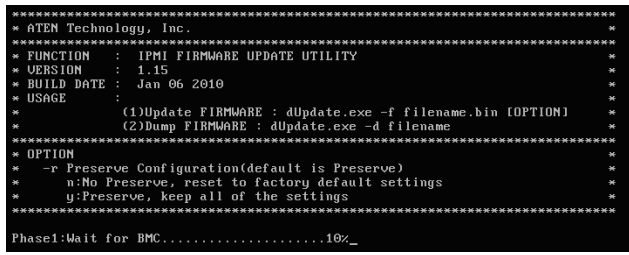


Figure 9: Phase 1- Flash Tools Waiting for the BMC to Prepare Data

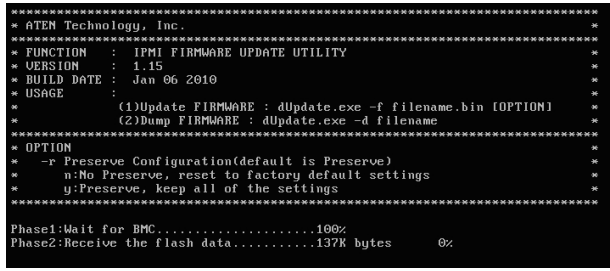


Figure 10: Flash Tools Dumping the Firmware

A-4 Using ATEN Flash Tools in Windows/Linux

In addition to DOS, ATEN's Flash Tools Utility supports Windows and Linux platforms.

The Windows/Linux version of Flash Tools Utility provides the same features supported by the DOS version. In addition, it also allows the user to update the firmware via LAN connections.

To use the ATEN Flash Tools in Windows/Linux, follow the steps below:

1. For Windows, start the Command Prompt. For Linux, start the Terminal.

2. At the command line prompt, type “cd /specify location” to change to the directory where the flash tool is located. Example: “cd /temp”

3. At the command line prompt, type "AwUpdate.exe" and press <Enter>.

4. The information about the utility will display. Follow the instructions given on the screen to configure the settings as shown in Figure 11.

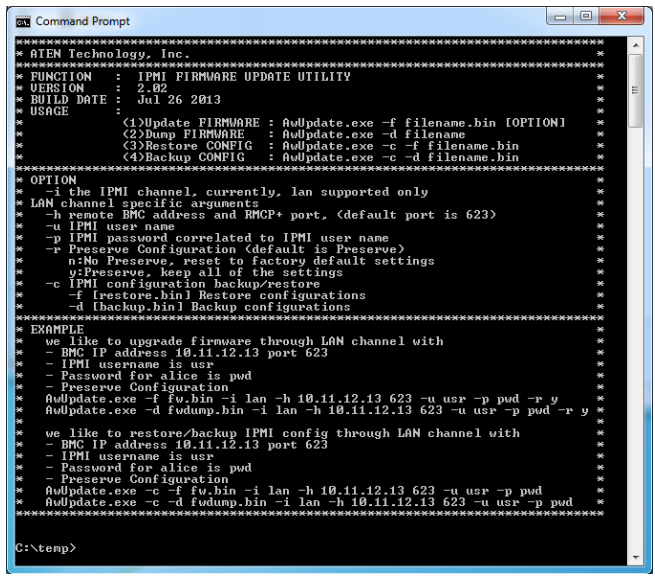


Figure 11 Main Screen of Flash Tools (Windows Version)

In the Windows/Linux version of the Flash Tools Utility, there are six parameters:

1. –f: Type <-f> to enter the filename of the firmware that you want to update

2. –i: -i indicates the IPMI channel. Currently, KCS and LAN connections are supported. If a LAN connection is used, the user needs to enter the following parameters:

3. –h: Type <-h> to enter the addresses of the remote BMC and the RMCP+ port (default port is 623).

4. –u: Type <-u> to enter the IPMI username.

5. –p: Type <-p> to enter the password for the IPMI user.

6. –r: Type <-r> to preserve (to save) the configuration settings you've entered. (This feature is optional.) (Default: preserve configuration.)

7. -y: Type <-y> for the BMC to keep all settings after updating the firmware; otherwise, the BMC will reset the settings to factory default.

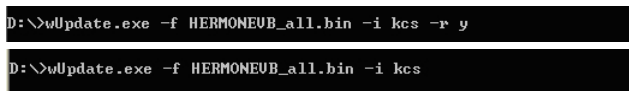


Figure 12: Example of KCS FW Updates with/without Preserving Configuration

To connect IPMI via KCS, type <wUpdate.exe/lUpdate –f [filename.bin] –I kcs –r y> as shown in Figure 12.

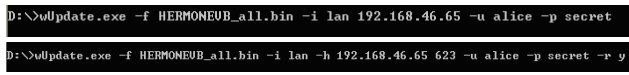


Figure 13: Example of LAN_FW_Updates with/without Preserving Configuration and RMCP+ Port

To connect IPMI via LAN, type <wUpdate.exe/lUpdatewUpdate.exe -f [filename.bin] -i lan -h 192.168.46.65 623 -u alice -p secret -r y> as shown in Figure 13.

For other settings, please refer to their counterparts in the DOS version for configuration instructions.

Appendix B

Introduction to SMASH

B-1 Overview

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

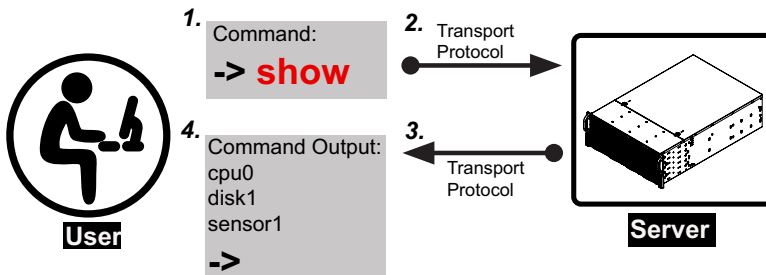


Figure 1 SMASH-CLP User Interface

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 your system management. Instructions given in this document may or may not be applicable to your 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, 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 your system management in a web-based environment. Refer to the SMASH script provided below to curtail a server management protocol for your 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. At the prompt '#", enter "SMASH" to invoke the SMASH prompt '—>'.
6. If you have successfully logged in, the SMASH prompt will display.

B-5 SMASH-CLP Main Screen

After you've successfully logged in the SSL network, the SMASH Command Line Protocol Main screen will display as shown below.

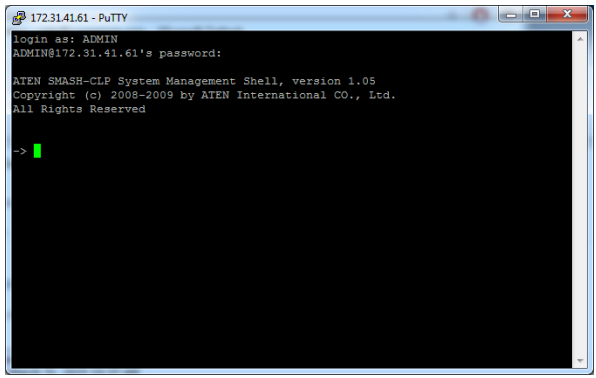


Figure 2 SMASH-CLP Main Screen

B-6 Using SMASH for System Management

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

Note: Make sure that the format of all your 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.

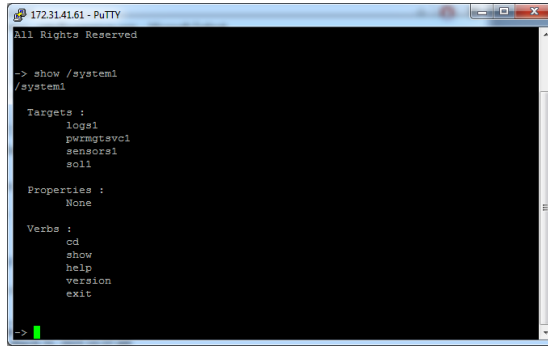


Figure 3 Using SMASH for System Management

B-7 Definitions of Command Verbs

Based on the DSP Specification, each target supports its own set of verbs. These verbs allow the user 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 and show etc.

- ***cd***

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

- ***show***

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

- ***exit***

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

- ***help***

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

- ***Version***

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

- ***set***

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

- ***start***

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

- ***stop***

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

- ***reset***

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

- ***delete***

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

- ***load***

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

- ***dump***

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

- ***create***

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

B-8 SMASH Commands

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

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

Table 1 SMASH Commands

B-9 Standard Command Options

The following table lists the standard command options.

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

Table 2 Standard Command Options

B-10 Target Addressing

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

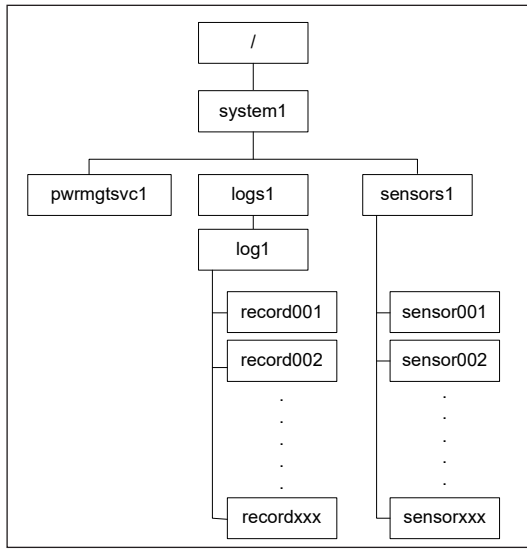


Figure 4 Target Addressing Diagram

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 senor 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.

Notes

Appendix C

RADIUS Configuration

C-1 Overview

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

RADIUS (Remote Authentication Dial In User Service) is a network protocol that allows you to manage remote user authentication and accounting. It authenticates users trying to establish a network connection, authorizes users to access the network, and accounts for users accessing the network. Before you run RADIUS, you need to cofigure 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/users
```

2. Then you will 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 the 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=1"A-2

C-3 Configuring Client Information 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/client.conf
```

Example:

client 192.123.4.5 {

secret = super

shortname = superbmc

}

C-4 Starting the RADIUS Server in 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 -X
```

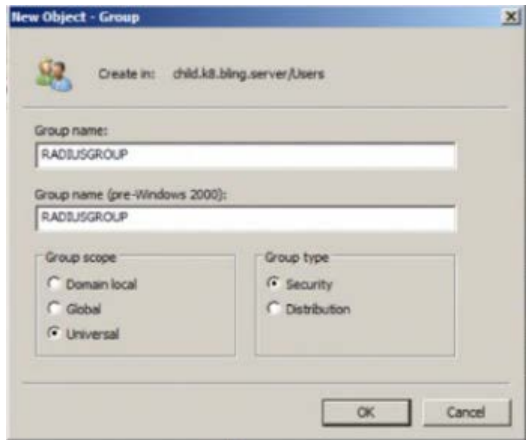
C-5 Adding Roles in Windows

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

1. Click on the <Start> button, then *Adminstrative 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 in the group name and select the group scope and type. Click on <OK> to complete to this step.

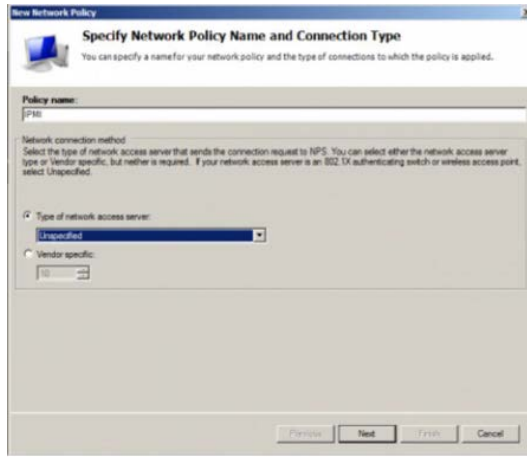


Add a New Object - User

1. To add a new object user, enter in 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*. Type in the policy name and select the type of network access server.

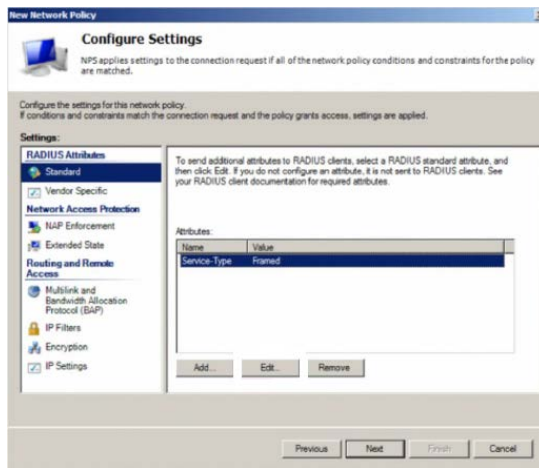


2. Click on <Next> to choose a permission.

3. Then configure Contraints and remove *Framed* protocol.

4. Edit Service-Type for login.

5. Check the *Others* option and select *Login.* Click on <OK> to complete the configuration.

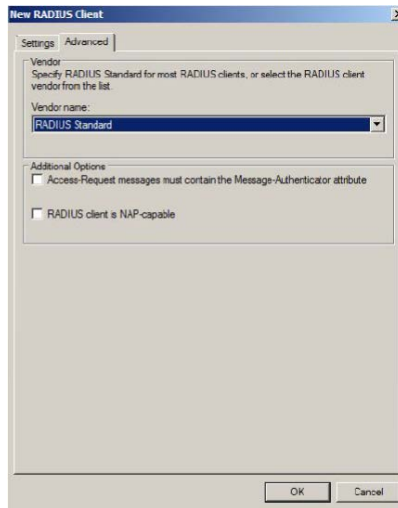


Adding a Vendor Specific

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

Configuring a New RADIUS Client

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



Notes

(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.