

SUPER  [®]

SMT IPMI

User's Guide

Revision 2.3

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: Handling of lead solder materials used in this product may expose you to lead, a chemical known to the State of California to cause birth defects and other reproductive harm.

Manual Revision 2.3

Release Date: Nov. 19, 2014

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.


Copyright © 2014 by Super Micro Computer, Inc.
All rights reserved.

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 Nuvoton WPCM450/ASpeed AST2400 BMC Controller embedded in Supermicro's motherboards. It provides detailed information on how to configure the IPMI settings supported by the WPCM450/AST2400 controller.

 **Note:** Nuvoton Technology is a subsidiary of Winbond Corp.

User's Guide Organization

Chapter 1 provides an overview on the Nuvoton WPCM450/ASpeed AST2400 controller. It also introduces the features and the functionality of IPMI.


Chapter 2 provides detailed instructions on how to configure the IPMI settings supported by the WPCM450/AST2400 controller.

Chapter 3 provides the answers to frequently asked questions.

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

Notes

Table of Contents

Preface	3
About this User's Guide	3
User's Guide Organization	3
Conventions Used in This User's Guide	3
Contacting Supermicro	4
Chapter 1 Introduction	1-1
1.1 Overview of the Nuvoton WPCM 450/ASpeed AST 2400 BMC Controller	1-1
1.2 Supermicro IPMI Features	1-3
1.3 Introduction to the IPMI Platform	1-4
1.4 Motherboards Supported	1-4
1.5 An Important Note to the User.....	1-5
Chapter 2 Configuring the IPMI Settings	2-1
2.1 Configuring BIOS	2-1
2.2 Configuring the IP/MAC Addresses for Remote Servers.....	2-4
2.3 Connecting to the Remote Server	2-6
Using the IPMIView to Connect to the Remote Server	2-6
Using the Browser to Connect to the Remote Server	2-6
2.4 Accessing the Remote Server via Console Redirection Using the Browser..	2-7
2.5 IPMI Main Screen	2-8
2.6 Server Health	2-10
2.6.1 Sensor Readings	2-11
2.6.2 Event Log.....	2-13
2.6.3 Storage Monitoring.....	2-16
2.6.4 Multi Node.....	2-17
2.6.5 Power Consumption.....	2-19
2.6.6 Power Source	2-20
2.7 Configuration	2-22
2.7.1 Configuring the Alert Settings	2-24
2.7.2 Configuring Date and Time Settings.....	2-27
2.7.3 Configuring Lightweight Directory Access Protocol (LDAP) Settings..	2-28
2.7.4 Active Directory Settings.....	2-29
2.7.5 Configuring the RADIUS Settings.....	2-32
2.7.6 Configuring the Mouse Mode Settings	2-33
2.7.7 Configuring Network Settings	2-34
2.7.8 Configuring Dynamic DNS (Domain Name System) Settings.....	2-36
2.7.9 Configuring the SMTP Settings	2-37

2.7.10	Configuring the SSL (Secure Sockets Layer) Certification.....	2-38
2.7.11	Configuring User Settings	2-39
2.7.12	Configuring Port Settings	2-43
2.7.13	Configuring IP Access Control	2-44
2.7.14	Configuring SNMP Settings	2-46
2.7.15	Configuring Fan Settings	2-47
2.7.16	Configuring the Web Session Settings.....	2-48
2.8	Remote Control	2-49
2.8.1	Console Redirection.....	2-50
2.8.2	Power Control	2-77
2.8.3	Launch SOL	2-78
2.9	Virtual Media	2-80
2.9.1	Uploading Floppy Images	2-81
2.9.2	Uploading CD-ROM Images	2-82
2.10	Maintenance.....	2-83
2.10.1	Firmware Update	2-84
2.10.2	Unit Reset	2-86
2.10.3	IKVM Reset.....	2-87
2.10.4	Factory Default.....	2-88
2.10.5	IPMI Configuration	2-89
2.10.6	System Event Log.....	2-90
2.10.7	BIOS Upload	2-91
2.10.8	LCMC Update	2-92
2.11	Miscellaneous.....	2-93
2.11.1	POST Snooping	2-94
2.11.2	SMC RAKP.....	2-95
2.11.3	UID Control	2-96
Chapter 3 Frequently Asked Questions.....		3-1
3.1	Frequently Asked Questions	3-1
Appendix A Flash Tools		A-1
A.1	Overview	A-1
A.2	Reference.....	A-1
A.3	Using Aten Flash Tools in the DOS Environment.....	A-1
	Firmware Updating via KCS Channels	A-2
	Dumping Firmware from the BMC via KCS channels	A-3
A.4	Windows/Linux Version of Flash Tools	A-4
Appendix B Introduction to SMASH		B-1
B.1	Overview	B-1
B.2	An Important Note to the User.....	B-2

B.3	Using SMASH	B-3
B.4	Initiating the SMASH Protocol	B-3
B.5	SMASH-CLP Main Screen	B-4
B.6	Using SMASH for System Management.....	B-4
B.7	Definitions of Command Verbs	B-5
B.8	SMASH Commands	B-7
B.9	Standard Command Options.....	B-8
B.10	Target Addressing	B-9
	Terms Used in the Target Addressing Diagram	B-9
	Appendix C RADIUS Setup Guidelines.....	C-1

Chapter 1

Introduction

1.1 Overview of the Nuvoton WPCM 450/ASpeed AST 2400 BMC Controller

The Nuvoton WPCM450/ASpeed AST 2400 Baseboard Management Controller (BMC) supports PCI-based 2D/VGA Graphics cores via PCI interfaces, multimedia virtualization, and Keyboard/Video/Mouse Redirection (KVMR). The WPCM450/AST2400 controller is ideal for networking management.

The WPCM450/AST2400 interfaces with the host system via PCI connections to communicate with the graphics core. It supports USB 2.0 and 3.0 for remote KVM emulation. It also provides LPC interface support to control Super IO functions. The BMC is connected to the network via an external Ethernet PHY module or shared NCSI connections.

The WPCM450/AST2400 communicates with onboard components via the SMBus interface, PECE (Platform Environment Control Interface) buses, and General Purpose I/O ports.

WPCM450/AST2400 DDR2/DDR3 Memory Interface

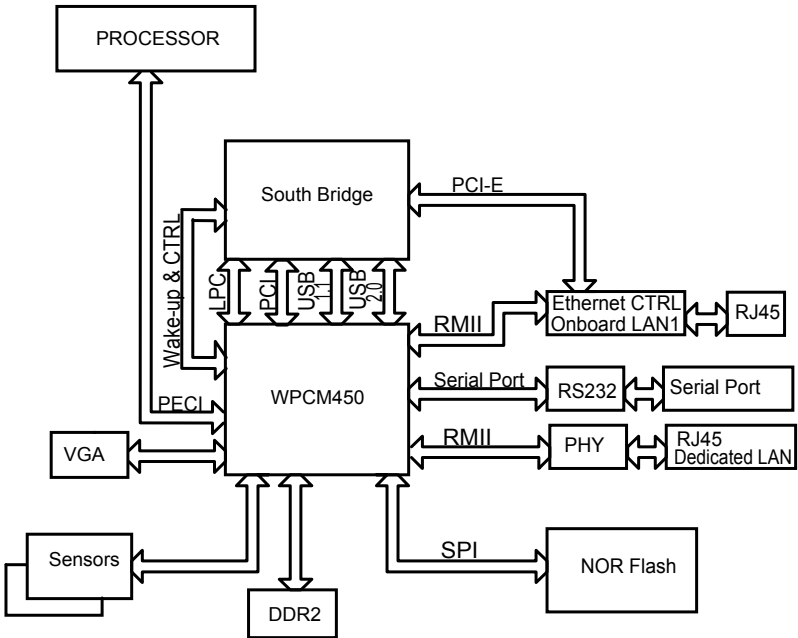
The WPCM450/AST2400 controller supports DDR2/DDR3 memory with a speed of up to 220 MHz. The motherboard supports 128 MB of memory which is shared between the BMC and onboard graphics card. For best signal integrity, the WPCM450/AST2400 provides point-to-point connections.

WPCM450/AST2400 PCI System Interface

The WPCM450/AST2400 provides a 32-bit, 33 MHz 3.3V PCI interface, which is compliant with PCI Local Bus Specification Rev. 3.0. The PCI system interface connects to the onboard PCI Bridge and is used by the graphics controller.

WPCM450 Block Diagram

The following diagram represents a typical system setup for the WPCM450 controller.



1.2 Supermicro IPMI Features

1. Basic hardware information
2. Remote KVM (graphics) console
3. Virtual media and ISO images
4. Remote server power control
5. Remote Serial Over LAN (text console)
6. Event log support
7. Automatic notification and alerts (SNMP and email)
8. Hardware monitoring
9. Monitoring of multiple nodes
10. Overall health display on the main page
11. Out-of-band management through shared or dedicated LAN
12. Option to change LAN connection interface at runtime
13. VLAN
14. RMCP/RMCP+ protocols supported
15. SMASH/CLP
16. Secure command line interface (SSH) and Telnet
17. WSMAN and WS-CIM
18. RADIUS authentication support
19. Secure browser interface (SSL support)
20. Lightweight Directory Access Protocol (LDAP) support
21. DCMI 1.0 support
22. Backup and restoration of the configuration file
23. Factory defaults from web support
24. Video quality settings
25. Record video and play
26. Server data/information
27. Preview of the remote screen on the main page
28. Firmware updates through browser and OS
29. OS-independent

1.3 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 WPCM450/AST2400 BMC Controller will connect the South Bridge to other onboard components, providing remote network interface via serial links. With the WPCM450/AST2400 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.

1.4 Motherboards Supported

This version of SMT IPMI is supported by the motherboards listed in the table below. If your motherboard is not included in the table, please refer to the motherboard product page on our website at www.supermicro.com and download the right BMC/IPMI user's guide for your motherboard.

Intel Dual-Processor Motherboards supported (-F models only)	Intel Single-Processor Motherboards supported (-F models only)	AMD Motherboards supported (for -F models only)
X8DTL-3F/-6F/iF	X7SPA/E-HF/-D525	H8DGG-QF
X8DTN+-F	X7SPT-DF-D525	H8DGT-HF/-HIBQF/-HLF/-HLIBQF
X8DTU-6F+/6TF+/LN4F+/TF	X8Si6-F	H8DGU-F/-LN4F+
X9DBU-6F/iF	X8SiA-F	H8SGL-F
X9DR6/i-F	X8SiE-F/-LN4F	H8SCM-F
X9DRT-H6F	X9SIL-F/-LN4F	H8DCL-6F/-iF
X9DRG-QF+	X9SRE-F	H8DCT-F/-HIBQF/-HLN4F/-IBQF
	X9SRW-F	H8DG6-F
	X9SCL-F	H8DGi-F
	X9SCM-F	
	X9SRE-F	
	X9SRW-F	
	X9SCL-LN4F	
	X9SCL-F	
	X9SCM-F	
	X9SRE-F	
	X9SRW-F	

1.5 An Important Note to the User

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.

Chapter 2

Configuring the IPMI Settings

With the Nuvoton WPCM450/ASpeed AST2400 BMC Controller and the IPMIView firmware built in, Supermicro motherboards allow the user to access, monitor, manage, and interface with multiple systems in different remote locations. The necessary firmware for accessing and configuring the IPMI settings are available on the 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 BIOS

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

A. Entering and Using the BIOS

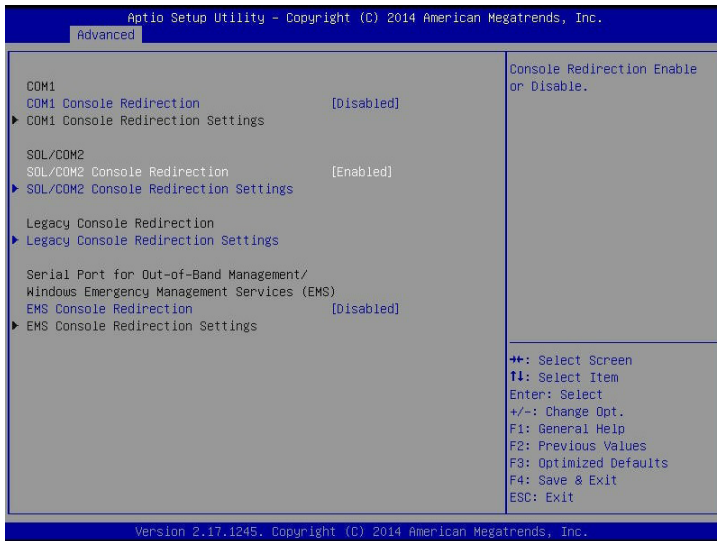
1. Boot up your system. During bootup, you will enter a bootup screen. When you see this screen, press the key. The BIOS setup screen will appear.
2. To navigate, use your arrow keys and press <Enter>. To go back to previous screens, press <Esc>.

B. Enabling COM Port for SOL (IPMI)

1. Select the *Advanced* tab at the top of the main BIOS screen.
2. From the list that appears, select *Serial Port Console Redirection*.
3. Make sure that the COM port for SOL (COM2 or COM3) is set to *[Enabled]*. If not, select the item and press <Enter>. Select *Enabled* and press <Enter>.

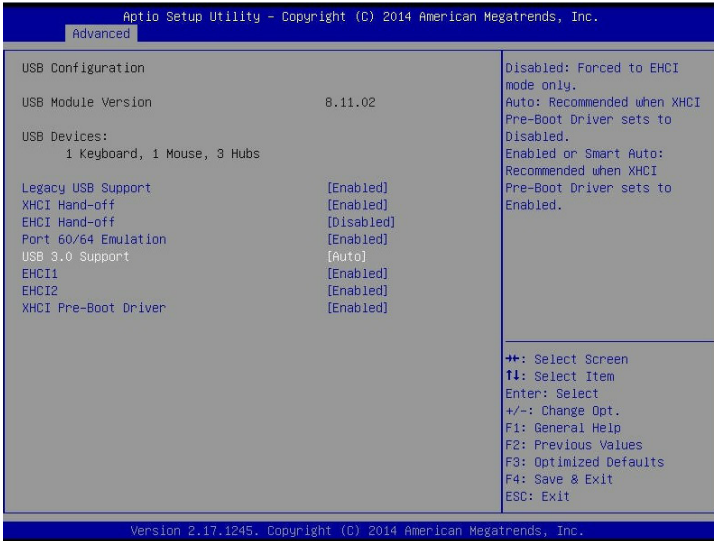


Note: For the IPMI to work properly, the BIOS will set the console redirection on this port by default.



C. Enabling All Onboard USB Ports

1. Select the *Advanced* tab at the top of the main BIOS screen.
2. From the list that appears, select *Chipset Configuration* and press <Enter>.
3. Select *South Bridge* and press <Enter>. The screen as shown below will appear.

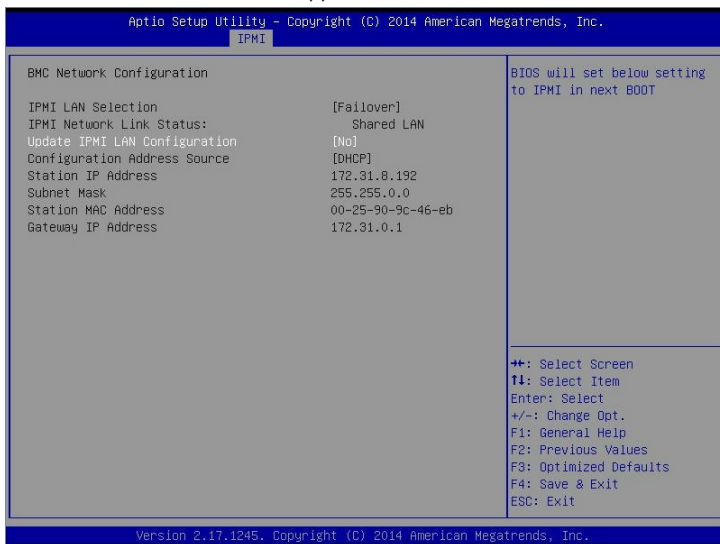


4. Check that the "USB 3.0 Support" item is set to *[Enabled]*. If not, select the item and press <Enter>. Select *Enabled* and press <Enter>. (This is required for KVM to work properly.)

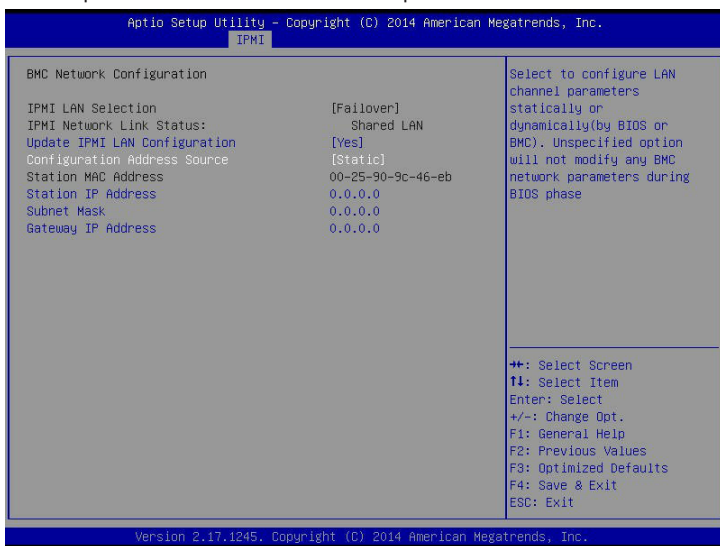


D. Configuring IP Address Using BIOS

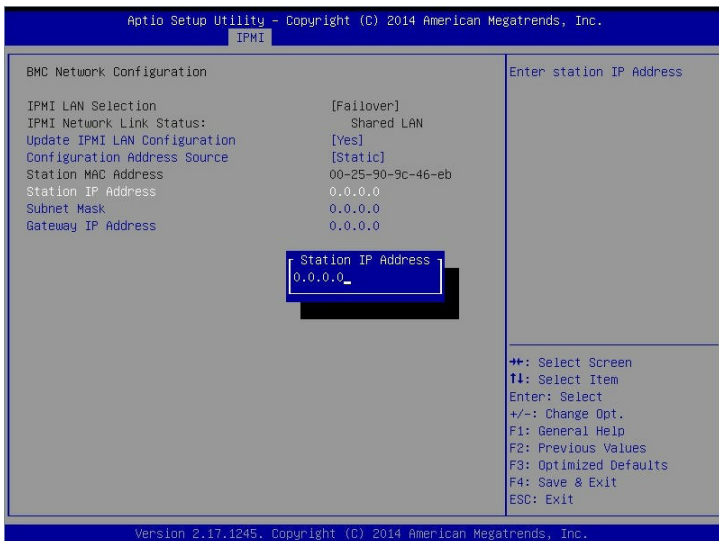
1. Select the *IPMI* tab at the top of the main BIOS screen.
2. From the list, select *BMC Network Configuration* and press <Enter>. The screen as shown below will appear.



3. Check that the "Update IPMI LAN Configuration" is set to *[Yes]*. If not, select the item and press <Enter>. Select *Yes* and press <Enter>.
4. To manually configure the IP address, select *Configuration Address Source* and press <Enter>. Select *Static* and press <Enter>.



5. Once the "Configuration Address Source" is set to *Static*, the "Station IP Address," "Subnet Mask," and "Gateway IP Address" fields should now be set to 0.0.0.0 and activated for changing (as in the screen shown on the previous page). Select each of the three items and enter an appropriate value. Press <Enter> when you are done.



2.2 Configuring the IP Address 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 BIOS Setup utility.

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

1. Run the ipmicfg utility. (You can get this from the Supermicro website, <http://www.supermicro.com/>, or from Supermicro's FTP site, <ftp://ftp.supermicro.com/utility/IPMICFG/>.)
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.
Release Date: Nov. 05, 2014

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
-clrint	Clear chassis intrusion
-fd	Reset IPMI to the factory default
-fdl	Reset IPMI to the factory default (Clean LAN)
-fde	Reset IPMI to the factory default (Clean FRU & 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	OEM power command for ME
-nm oemgettemp	OEM temp. command for ME
-nm pstate	Get max. allowed CPU P-state
-nm tstate	Get max. allowed CPU T-state
-nmcputemp	Get CPU/memory temperature
-nm hostcpudata	Get host CPU data
-pminfo	Power-supply PMBus health
-psfrinfo	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
-fru 3s	Update FRY 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 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 IPMIView utility.

Using the Browser 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 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.

 **Notes:**

1. The default network setting is "Failover," which allows the IPMI to connect to the network through a shared LAN port (onboard LAN Port 1) or through the IPMI-dedicated LAN port. If the IPMI must be connected through a specific port, please change the LAN configuration settings 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 are enabled in the system BIOS by default. The COM port for IPMI is marked with * in the BIOS. It is usually

2.4 Accessing the Remote Server via Console Redirection Using the Browser

To Log In to the Remote Console

Once you are connected to the remote server via IPMI Console Redirection, the following IPMI login screen will display.


The image shows a login form titled "Please Login" with the SUPERMICO logo above it. The form contains two input fields: "Username" and "Password", and a "login" button below them.

 **Please Login**


Username


Password

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

 **Note:** The manufacturer's 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 purposes.

2. Enter your password in the *Password* field and click <Login>.
3. The homepage 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

The IPMI main screen displays as shown below.

The screenshot shows the IPMI main screen with the following elements:

- Top Bar:** Includes the SUPERMICRO logo, Host Identification (Server: 172.031.008.155, User: ADMIN (Administrator)), and a language menu (Normal, Refresh, Logout, English).
- Navigation Menu:** System, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, Miscellaneous, Help.
- System Summary (6):**
 - Firmware Revision: 01.70
 - Firmware Build Time: 10/03/2014
 - BIOS Version: 1.0a
 - BIOS Build Time: 08/29/2014
 - IP address: 172.031.008.155
 - BMC MAC address: 00.25.90.9c.47.a6
 - System LAN1 MAC address: 00.25.90.9c.5f.90
 - System LAN2 MAC address: 00.25.90.9c.5f.91
 - System LAN3 MAC address: 00.25.90.9c.5f.92
 - System LAN4 MAC address: 00.25.90.9c.5f.93
- Remote Console Preview:** A terminal window showing a boot menu with options like 'Enter a selection by key option:' and 'Power Control via IPMI'.
- Power Control via IPMI (7):** A section indicating 'Host is currently on' and buttons for 'Power On', 'Power Down', and 'Reset'.

Copyright © 2014 Super Micro Computer, Inc.

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

1. *The top bar.* The menu bar on the top displays the headings *System Information*, *Server Health*, *Configuration*, *Remote Control*, *Virtual Media*, *Maintenance*, *Miscellaneous*, and *Help*. Click a heading on the menu bar to access the individual items and configure their settings.



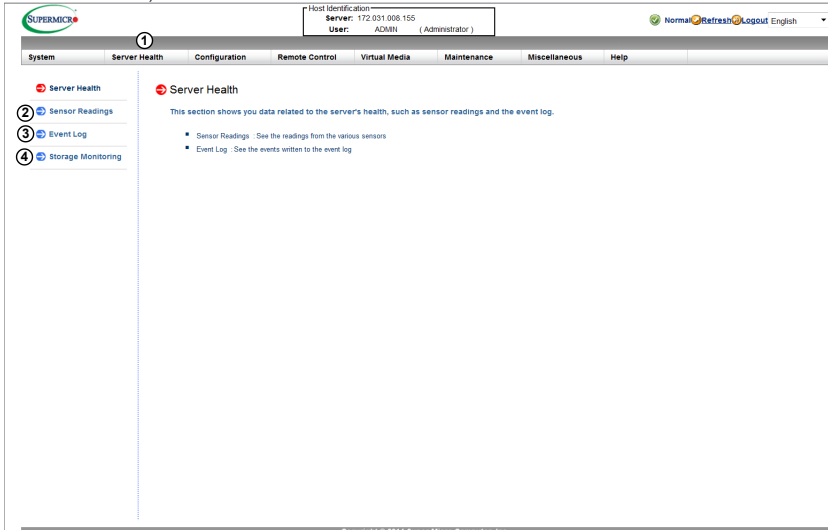
Note: The *Help* header on every page displays guidelines on how to use the features. Click the *Help* header, and a frame will display on the right with this additional information.

2. *The System sidebar.* This sidebar 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 this information.
5. *Language Select.* From the pull-down menu, select a language. At present, the options are the following:
 - *English*
 - *Japanese*

6. *Summary*. This section provides the following information:
 - *Firmware Revision*
 - *Firmware Build Time*
 - *BIOS Version*
 - *BIOS Build Time*
 - *IP Address*
 - *BMC MAC Address*
 - *System LAN MAC Address* (all available LANs)
 - *Remote Console Preview*, a display of the remote system (host machine) console running at the specified IP address
7. *Power Control via IPMI*. This section provides options for powering on and off the host system.
 - *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.

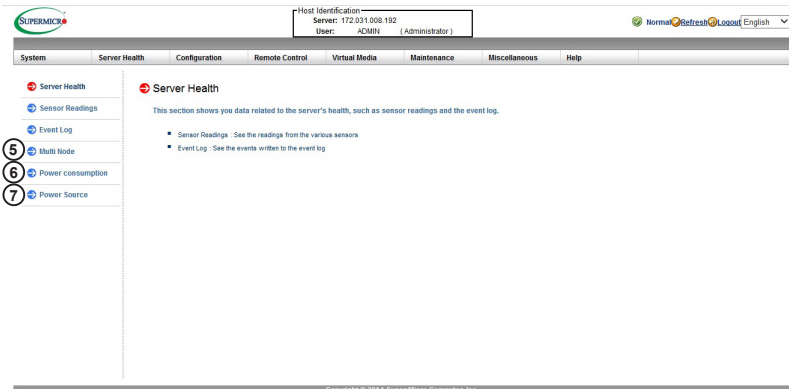
2.6 Server Health

This feature allows the user to set server health settings. To access server health information, follow the instructions below.



1. To access the Server Health main page, click on the *Server Health* header in the top bar. The individual features accessible from here are the following:
2. Sensor Readings
3. Event Log
4. Storage Monitoring (available for systems with RAID)

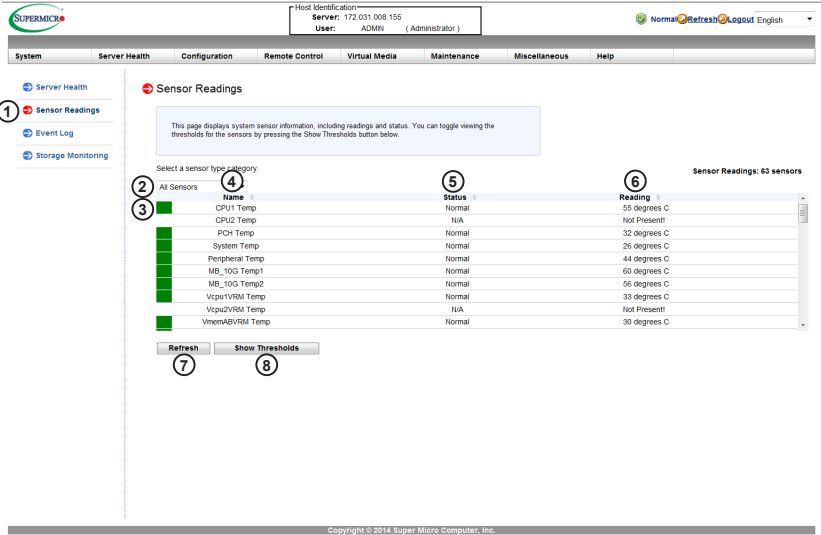
If you are working on a multi-node system, your Server Health screen and sidebar will look different. See the screenshot below and the list of additional features.



5. Multi Node
6. Power consumption
7. Power Source

2.6.1 Sensor Readings

This page displays sensor readings for the remote console. Click the arrows next to each header to rearrange the items from minimum to maximum or vice versa.



- To enter the screen shown above, click on the "Sensor Readings" item in the *Server Health* sidebar.
- From the pull-down menu, select a sensor type. The options are the following:
 - All Sensors
 - Temperature Sensors
 - Voltage Sensors
 - Fan Sensors
 - Power Supply
- A sensor color that is displayed in front of a sensor indicates the status of the sensor.
 - Green indicates that the sensor reading is normal. The system is functioning normally.
 - Amber indicates an alert on the sensor reading. Attention is needed to ensure that the system is functioning properly.
 - Red indicates that one or more sensors have reached the critical state. Immediate action is needed to resolve the problem.

4. **Name.** This column displays the names of the sensors that are currently active in system monitoring, including system temperature, CPU temperature, fan speeds, CPU core voltages, +3.3Vcc, and +12V voltage monitoring.
5. **Status.** This column indicates the status of each sensor reading. If no component is found in the specified slot, the status will read *N/A*.
6. **Reading.** This column indicates the reading of each sensor. If no component is found in the specified slot, the status will read *Not Present!*
7. **Refresh.** Click this item to refresh the page.
8. **Show Thresholds.** Click this item to display sensor thresholds. The screen as shown below will appear.

Host Identification: Server: 172.231.240.192 User: ADMIN (Administrator)

Normal Refresh Logout English

System Server Health Configuration Remote Control Virtual Media Maintenance Miscellaneous Help

Server Health Sensor Readings Event Log Multi Node Power consumption Power Source

Sensor Readings

This page displays system sensor information, including readings and status. You can toggle viewing the thresholds for the sensors by pressing the Show Thresholds button below.

Select a sensor type category: All Sensors

Name	Status	Reading	Low NR	Low CT	High CT	High NR
CPU12 Temp	Normal	79 degrees C	0	0	93	N/A
CPU1 Temp	Normal	45 degrees C	0	0	93	N/A
PCH1 Temp	Normal	60 degrees C	-11	-8	95	100
System Temp	Normal	26 degrees C	-9	-7	85	90
FanSpeed1 Temp	Normal	54 degrees C	-9	-7	85	90
Vpos1V5RM Temp	Normal	62 degrees C	-9	-7	100	105
Vpos2V5RM Temp	Normal	33 degrees C	-9	-7	100	105
Vmem14V5RM Temp	Normal	46 degrees C	-9	-7	100	105

Refresh Hide Thresholds

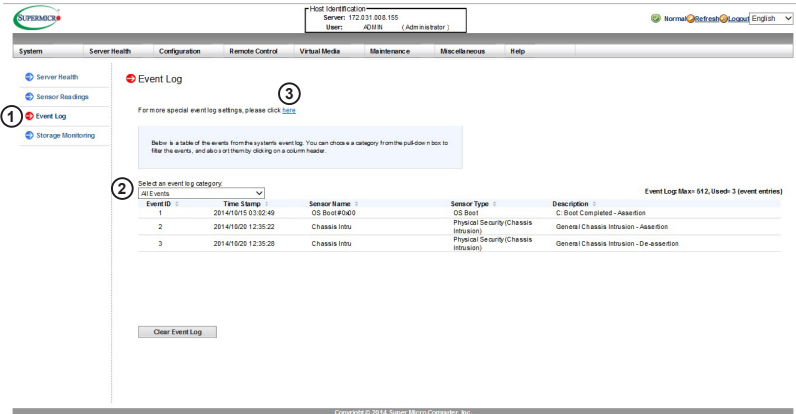
Sensor Readings: 48 sensors

Copyright © 2014 Super Micro Computer, Inc.

- **Low NR (Low Non-Recoverable).** This is the low threshold of a non-recoverable item. Any item with a reading below this point cannot be recovered.
- **Low CT (Low Critical Threshold).** This is the low threshold of a critical item. Any item with a reading below this threshold is in a critical state.
- **High CT (High Critical Threshold).** This is the high threshold of a critical item. Any item with a reading above this threshold is in a critical state.
- **High NR (High Non-Recoverable).** This is the high threshold of a non-recoverable item. Any item with a reading above this point cannot be recovered.

2.6.2 Event Log

This page displays a record of critical system monitoring events. The event log indicates the time when a critical condition occurred and when the condition was resolved. You can choose a specific event category from the pull-down menu to display events included in this category.



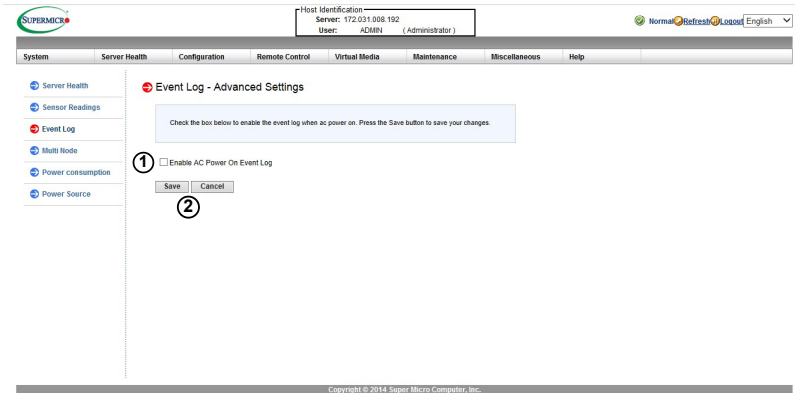
- To enter the screen shown above, click on the "Event Log" item in the *Server Health* sidebar.
- From the pull-down menu, select an event category. The following event categories are listed:
 - Sensor-Specific Events*. These event logs are generated by the BMC if the sensor's reading reaches its threshold.
 - BIOS Generated Events*. These event logs are generated by the 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 of the above event logs.
- You can enable the AC power-on event to be logged as well. Click the *here* link to go to the options page.

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

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/Shutdown	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)

2.6.2a Event Log - Advanced Settings

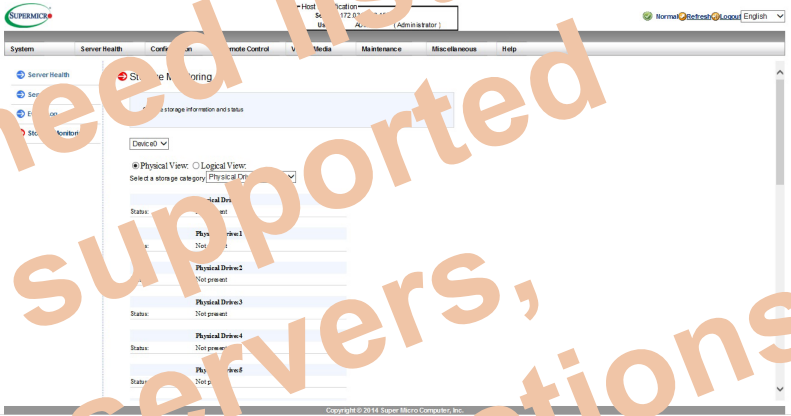
After clicking the link as described on page 2-16, the page shown below will display. From here, you can enable or disable the option to record AC power-on events in the log.



1. To enable recording of AC power-on events, check the box. To disable, uncheck the box.
2. Click *Save* to save the new setting, or click *Cancel* to return to the event log (described on pages 2-16 and 2-17) without saving.

2.6.3 Storage Monitoring

This feature, available on systems with RAID supported (LSI 2108, 2208, or 3108 storage controllers either onboard or as add-on cards), lists all storage bays whether or not they have been filled by physical drives. There are two view options, physical view and logical view.



2.6.4 Multi Node

This page displays real-time information relating to the entire system, the chassis, and all individual nodes. Such information may include power consumption, input current, serial numbers, CPU temperatures, node temperatures, and node IP addresses.

Multi Node Monitoring

The page displays power information of multi node

1 Multi Node

2 Power Supply

Power Consumption:	283 W
Input Current:	1.657 A

3 Chassis Information

Maximum Number of Nodes:	2
LCMC Firmware Version:	1.00
User Defined System Name:	twmproct10
System Part No.:	N/A
System Serial No.:	N/A
Chassis Part No.:	N/A
Chassis Serial No.:	N/A
BP Model Name:	N/A
BP Serial No.:	N/A
BP Revision:	205.H

4 Node A

Status:	Present
Power Status:	On
Power:	0 W
Current:	0 A
CPU1 Temp:	38 °C
CPU2 Temp:	47 °C
System Temp:	27 °C
Board Part Number:	N/A
Board Serial Number:	N/A
IP Address:	172.31.41.8

Node B (current node)

Status:	Present
Power Status:	On
Power:	0 W
Current:	0 A
CPU1 Temp:	39 °C
CPU2 Temp:	43 °C
System Temp:	27 °C
Board Part Number:	N/A
Board Serial Number:	N/A
IP Address:	172.31.42.4

Copyright © 2014 Super Micro Computer, Inc.

- To enter the screen shown above, click on the "Multi Node" item in the *Server Health* sidebar.
- The *Power Supply* section lists the power consumption and input current of the system in real-time.
- The *Chassis Information* section lists chassis information, including the maximum possible number of nodes; backplane location, model, serial number, revision number; and system and chassis part and serial numbers.



Note: If you are accessing a multi-node system, you may not be able to see all chassis information unless you have the LCMC enabled.

- Each node in the system is given its own section, which lists the following information:
 - Status*, indicating whether the node is detected as present or absent in the system

- *Power Status*, indicating whether the node is powered on or off
- *Power*, indicating the power usage of the node
- *Current*, indicating the input current of the node
- *CPU Temp*, indicating the CPU temperature. If the node incorporates more than one CPU, the temperatures will be listed for all CPUs
- *System Temp*, indicating the temperature of the node
- *Board Part Number*, indicating the model name of the motherboard used in the node
- *Board Serial Number*, indicating the serial number of the motherboard used in the node
- *IP Address*, indicating the IP address of that particular node. Click on this item to access the IPMI for that node. (You will need to log in.) The node you are currently accessing via IPMI is highlighted in blue.

2.6.5 Power Consumption

This page tracks the power usage over the system over time.

1. Power consumption

2. Estimate remaining BBP run time: 0 sec (No Battery in the system)

3. The Highest and lowest peak: 0 (1 = All Current Power Consumption)

Peak name	Value	Time
The Highest Peak (W)	0	
The Lowest Peak (W)	0	2014/10/23 19:2

4. Power consumption graph and history

Power Statistics	Last Hour	Time	Past 24 Hr	Time	Past 7 days	Time
Average (W)	0	None	0	None	0	None
Minimum (W)	0	2014/10/23 19:3	0	2014/10/23 06:4	0	2014/10/23 11:4
Maximum (W)	0	0	0	0	0	0

Last Hour Last Day Last Week

X:Time (min), Y:Power Consumption (Watt)

- To enter the screen shown above, click on the "Power consumption" item in the *Server Health* sidebar.
- The "Estimate remaining BBP run time" section indicates the expected amount of time left until the backup battery, if one is detected, runs out of power.
- The "highest and lowest peak" section displays three measurements:
 - Current power consumption, in watts
 - Highest recorded power consumption, in watts, along with its date and time
 - Lowest recorded power consumption, in watts, along with its date and time
- The "Power consumption graph and history" section graphs the power consumption of the system over time within the last hour, last day, and last week. In addition, it lists in a chart the average, minimum, and maximum power values over the last hour, last day ("Past 24 Hr"), and last week ("Past 7 days").

Clicking on the headings in the chart ("Power Statistics," "Last Hour," "Past 24 Hr," "Past 7 days," "Time") will rearrange the chart with either the minimum value or the maximum power or time value at the top.

2.6.6 Power Source

This feature displays detailed real-time power source information.

The screenshot shows the BMC/IPMI web interface. The top navigation bar includes 'System', 'Server Health', 'Configuration', 'Remote Control', 'Virtual Media', 'Maintenance', 'Miscellaneous', and 'Help'. The left sidebar has 'Power Source' selected. The main content area is titled 'Power Source Monitoring' and contains the following sections:

BBP Setting

- Auto Discharge Timer 0: Enable Disable in Days (Default is 30, max is 63days)
- Manual Discharge 0: Enable Disable
- Auto Discharge Timer 1: Enable Disable in Days (Default is 30, max is 63days)
- Manual Discharge 1: Enable Disable
- Auto Discharge Timer 2: Enable Disable in Days (Default is 30, max is 63days)
- Manual Discharge 2: Enable Disable
- Auto Discharge Timer 3: Enable Disable in Days (Default is 30, max is 63days)
- Manual Discharge 3: Enable Disable
- Timeout Value for graceful shutdown: Enable Disable 0 (Seconds)
- Editable remaining BBP run time: 0 sec

Slot 1 Status

Status	Power Supply OK
AC Input Voltage	115.00
AC Input Current	1.484 (A)
DC 12V Output Voltage	12.10V
DC 12V Output Current	12 (A)
Temperature 1	31 C / 87.8 F
Temperature 2	38 C / 100.4 F
Fan 1	8330 RPM
Fan 2	8280 RPM
DC 12V Output Power	144 (W)
AC Input Power	172 (W)
PWS Serial Number	

Slot 3 Status

Status	Not present
AC Input Voltage	0 (V)
AC Input Current	0 (A)
DC 12V Output Voltage	0 (V)
DC 12V Output Current	0 (A)
Temperature 1	0 C / 32 F
Temperature 2	0 C / 32 F
Fan 1	0 RPM
Fan 2	0 RPM
DC 12V Output Power	0 (W)
AC Input Power	0 (W)
PWS Serial Number	

Slot 4 Status

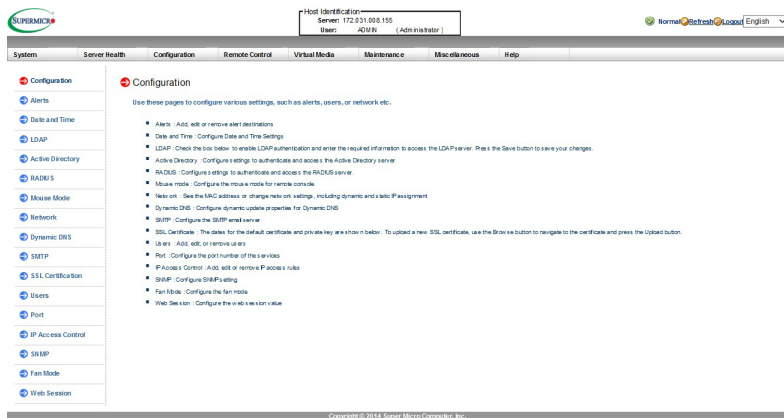
Status	Not present
AC Input Voltage	0 (V)
AC Input Current	0 (A)
DC 12V Output Voltage	0 (V)
DC 12V Output Current	0 (A)
Temperature 1	0 C / 32 F
Temperature 2	0 C / 32 F
Fan 1	0 RPM
Fan 2	0 RPM
DC 12V Output Power	0 (W)
AC Input Power	0 (W)
PWS Serial Number	

- To enter the screen shown above, click on the "Power Source" item in the *Server Health* sidebar.
- This feature allows you to manage discharging of the backup battery, if one has been installed. You can set up to three separate discharges by clicking *Enable* next to the corresponding item, either manual or auto (with a time setting of a maximum 63 days in the future).
- Each node slot in the system is given its own section detailing power information for that node. The following items are listed:
 - Status*, indicating the status of the power supply unit
 - AC Input Voltage*, indicating the current AC input voltage

- *AC Input Current*, indicating the current AC input current
- *DC 12V Output Voltage*, indicating the current DC output voltage (of a 12V DC power supply), in volts
- *DC 12V Output Current*, indicating the current DC output current (of a 12V DC power supply), in amps
- *Temperature*, indicating the current temperature of the power supply. If the node includes redundant power supplies, the temperatures of both power supplies will be listed.
- *Fan*, indicating the speed of all fans installed for that node
- *DC 12V Output Power*, indicating the current DC output power (of a 12V DC power supply), in watts
- *AC Input Power*, indicating the current AC input power, in watts
- *PWS Serial Number*, indicating the serial number of the installed power supply

2.7 Configuration

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



1. Click the *Configuration* header on the top bar. The screen shown above will appear. You will be able to access the following features from this page:

- *Alerts*. Use this feature to configure alert destination settings.
- *Date and Time*. Use this feature to configure the date and time and set up access to an NTP server.
- *LDAP*. Use this feature to configure LDAP (Lightweight Directory Access Protocol) settings for authentication and access to the LDAP server.
- *Active Directory*. Use this feature to configure the settings for authentication and access to the Active Directory server.
- *RADIUS*. Use this feature to configure the settings for authentication and access to the RADIUS server.
- *Mouse Mode*. Use this feature to configure the mouse mode for the remote console.
- *Network*. Use this feature to configure network settings.
- *Dynamic DNS*. Use this feature to configure the settings and access to the Dynamic DNS server.
- *SMTP*. Use this feature to configure the settings for authentication and access to the SMTP email server.
- *SSL Certification*. Use this feature to configure settings for SSL certification.

- *Users.* Use this feature to manage the users.
- *Port.* Use this feature to configure the ports.
- *IP Access Control.* Use this feature to set IP access rules.
- *SNMP.* Use this feature to manage SNMPv2 and SNMPv3 settings.
- *Fan Mode.* Use this feature to set the fan speeds.
- *Web Session.* Use this feature to set a session timeout value.

2.7.1 Configuring the Alert Settings

This feature allows the user to configure alert settings.

Host Identification: Server: 172.231.0.0/8.115
User: ADMIN (Administrator)

System Server Health Configuration Remote Control Virtual Media Maintenance Miscellaneous Help

1 List of Alerts

Before is a list of the configured alert destinations. You can select an alert and press the Modify button to configure it, or Send Test Alert to send a test alert to the destination.

Alert No	Alert Level	Destination Address
1	Disable All	000.000.000.000 & NULL
2	Disable All	000.000.000.000 & NULL
3	Disable All	000.000.000.000 & NULL
4	Disable All	000.000.000.000 & NULL
5	Disable All	000.000.000.000 & NULL
6	Disable All	000.000.000.000 & NULL
7	Disable All	000.000.000.000 & NULL
8	Disable All	000.000.000.000 & NULL
9	Disable All	000.000.000.000 & NULL
10	Disable All	000.000.000.000 & NULL

Alert Table: 10 entries

2 3 4

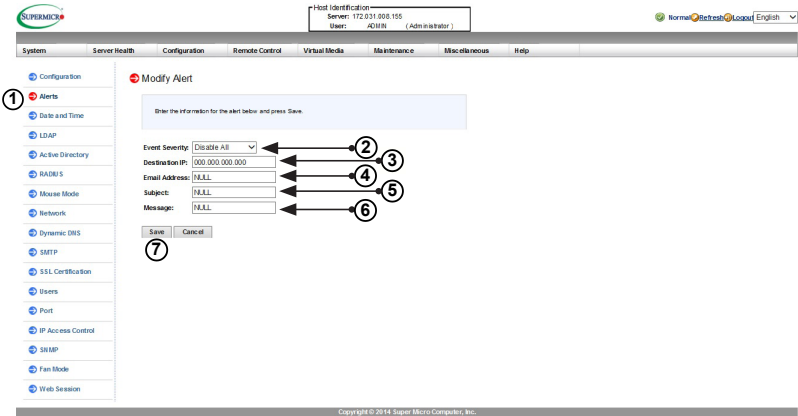
Modify Send Test Alert Delete

Copyright © 2014 Super Micro Computer, Inc.

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

1. To enter the screen shown above, click on the "Alerts" item in the Configuration sidebar.
2. Click *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 *Delete* to delete an alert.

2.7.1a Alerts - Modify Alert



1. From the Alerts page (as described in the previous page), select an alert and click *Modify*. The screen shown above will appear.
2. Select the event severity. The listed options are as follows:
 - *Disable All*. This is the default setting, disabling all alerts.
 - *Informational*. This is used to provide notifications in the case of system events that are not harmful.
 - *Warning*. This is used to provide notifications in the case of potentially dangerous system conditions.
 - *Critical*. This is used to provide notifications in the case of dangerous system conditions.
 - *Non-recoverable*. This is used to provide notifications in the case of dangerous system conditions from which the system cannot recover.
3. Enter the SNMP Trap receiver (IPMI View) IP address to use the SNMP. For further guidance on typical inquiries related to the SNMP, see the table below on the next page.

<i>Item</i>	<i>Answer</i>
SNMP version number	SNMP version 2 or 3.
MIB community name	A community name is not required since SNMP version 2 only uses traps.
MIB file location	Go to http://www.supermicro.com/products/nfo/IPMI.cfm and click "IPMI MIB (SMT)" (right-hand side of the page).
The IPMI item you need to configure so 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?	Detailed queries are not possible because event mapping is based only on sensor type, event type, and sensor offset.
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.

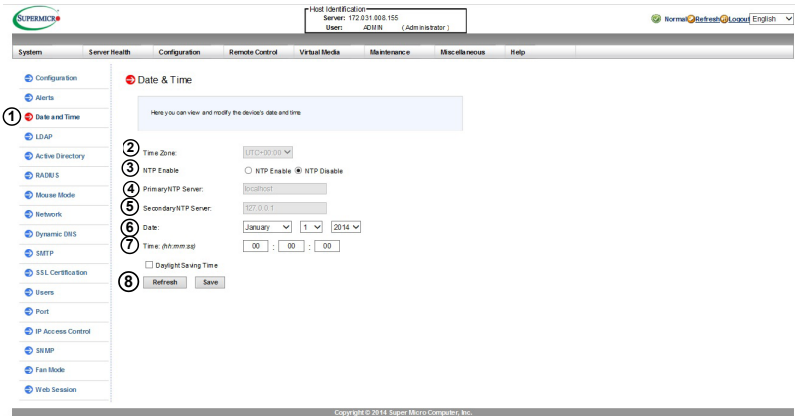
4. Enter the email address to send the alert to, then configure the SMTP settings (see page 2-40).
5. Enter the subject line of the alert.
6. Enter a message for the alert.
7. Click **Save** to save the settings.

2.7.2 Configuring Date and Time Settings

This feature allows the user to configure the time and date settings for the host server and the client computer.

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

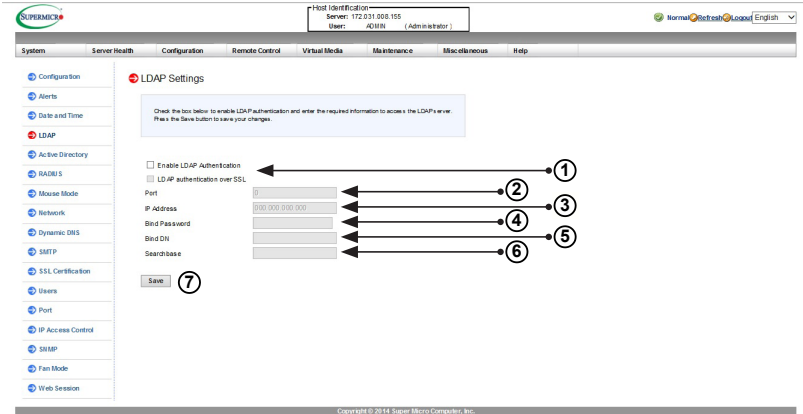
Note: Time zone is enabled when *NTP* is selected. The options are UTC -12:00 hr. ~ +12:00 hr.



1. To enter the screen shown above, click on the "Date and Time" item in the *Configuration* sidebar.
2. Select the time zone.
3. Click the *NTP Enable* radio button to enable 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 *Refresh* to refresh the date/time, or click *Save* to save the new settings.

2.7.3 Configuring Lightweight Directory Access Protocol (LDAP) Settings

This feature allows the user to configure the Lightweight Directory Access Protocol (LDAP) settings.



Follow the steps below to configure the LDAP settings.

1. Check the respective *Enable* box to enable LDAP authentication. If you want to configure LDAP authentication over SSL, check its respective box. Upon checking the latter box, the value 636 will appear in the "Port" field.
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 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. After entering the information in the fields, click *Save* to save the new settings.

2.7.4 Active Directory Settings

This page displays a list of role groups and their group IDs, group names, group domains, and network privilege settings.

Host Identification: Server: 172.201.90.155
User: ADMIN (Administrator)

System Server Health Configuration Remote Control Virtual Media Maintenance Miscellaneous Help

Configuration Alerts Date and Time LDAP Active Directory RAID5 Move Mode Network Dynamic DNS SMTP SSL Certification Users Port IP Access Control SNMP Fan Mode Web Session

Active Directory Settings

To enable or configure the Active Directory server, please click [here](#) ①

This list below shows the current list of configured Role Groups. If you wish this to delete or modify a role group, select the name in the list and press Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured role and press Add Role Group.

Role Group ID	Group Name	Group Domain	Network Privilege
1	-	-	Reserved
2	-	-	Reserved
3	-	-	Reserved
4	-	-	Reserved
5	-	-	Reserved

Number of configured role groups: 0

Add Role Group ② Modify Role Group ③ Delete Role Group ④

Copyright © 2014 Super Micro Computer, Inc.

1. Click *here* to enable or configure the active directory server. See page 2-34 for instructions on enabling or configuring the active directory.
2. Select a group and click *Add Role Group* to add the role group. You will be taken to the *Add New Role Group* screen described in the next page.
3. Select a group and click *Modify Role Group* to modify the role group. You will be taken to the *Add New Role Group* screen as described in the next page.
4. Select a group and click *Delete Role Group* to delete the role group.

2.7.4a Active Directory Settings - Add New Role Group

This page displays a list of role groups and their group IDs, group names, group domains, and network privilege settings. When you click *Add New Role Group* or *Modify New Role Group* from the *Active Directory Settings* page, you will be directed to this screen shown below.

The screenshot shows the 'Add New Role Group' page in the BMC/IPMI configuration utility. At the top, there is a 'Host Identification' box showing 'Server: 172.31.0.8.155' and 'User: Administrator'. Below this is a navigation bar with tabs for System, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, Miscellaneous, and Help. A left sidebar contains various configuration categories, with 'Active Directory' selected. The main content area is titled 'Add New Role Group' and contains a form with the following fields:

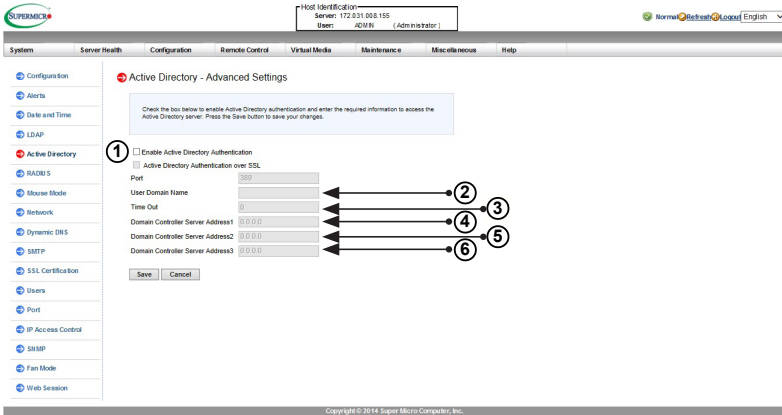
- Role Group Name:
- Role Group Domain:
- Role Group Privilege:

Below the form are 'Add' and 'Cancel' buttons. The 'Add' button is circled with the number 4. Arrows point to the input fields with circled numbers 1, 2, and 3, corresponding to the numbered list below.

1. Enter the role group name.
2. Enter the role group domain.
3. Select the role group privilege from the pulldown menu. The options are listed as follows:
 - Administrator
 - Operator
 - User
 - No Access
4. Click *Add* to save your settings, or click *Cancel* to return to the *Active Directory Settings* page without saving.

2.7.4b Active Directory Settings - Advanced Settings

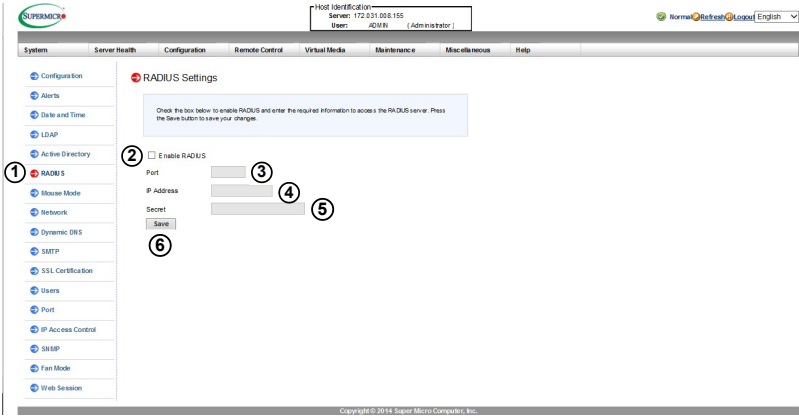
This feature allows the user to configure the advanced active directory settings. When you click [here](#) from the *Active Directory* page described on page 2-32, the following screen will display.



1. Check the respective *Enable* box to enable active directory authentication. If you want to configure LDAP authentication over SSL, check its respective box. Upon checking the latter box, the value 636 will appear in the "Port" field.
2. Enter the user domain name.
3. Enter time-out value in the field to set the time limit for a user to stay logged in.
4. Enter the controller server address 1.
5. Enter the controller server address 2.
6. Enter the controller server address 3.
7. After entering the information in the fields, click *Save* to save the new settings, or click *Cancel* to return to the *Active Directory Settings* page without saving.

2.7.5 Configuring the RADIUS Settings

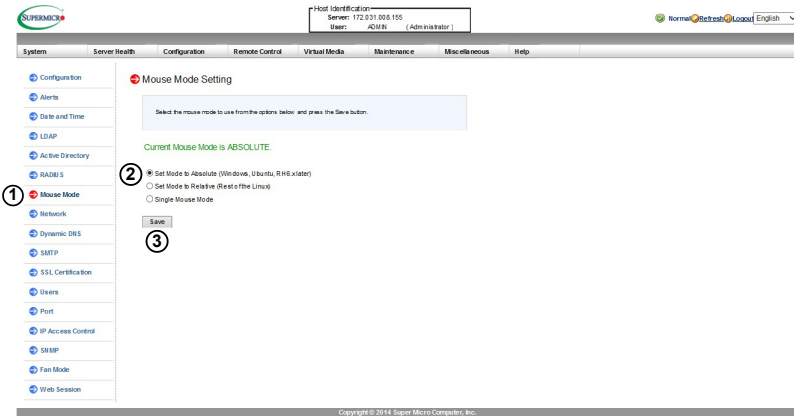
This feature allows the user to configure RADIUS settings.



1. To enter the screen shown above, click on the "RADIUS" item in the *Configuration* sidebar.
2. Check the *Enable RADIUS* box to enable RADIUS support. Enter the information in the fields below to configure RADIUS settings.
3. Enter the port number for the RADIUS server.
4. Enter the IP address of the RADIUS server.
5. Enter a password for the user to access the RADIUS server
6. After entering the information in the fields, click *Save* to save the new settings.

2.7.6 Configuring the Mouse Mode Settings

This feature allows the user to configure the mouse mode settings used in the remote console.



1. To enter the screen shown above, click on the "Mouse Mode" item in the *Configuration* sidebar.
2. This item displays the current mouse mode. To select a mouse mode, click the appropriate radio button as shown below.
 - Check the *Absolute* radio button to set the mouse mode to absolute mode for the Windows OS. (This is the default setting.)
 - Check the *Relative* radio button to set the mouse mode to relative mode for the Linux/Unix OS.
 - Check the *Single Mouse Mode* radio button to use single mouse mode.
3. After entering the information, click *Save* to save the settings.



Note: The IPMI is an OS-independent platform, and 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.

2.7.7 Configuring Network Settings

This feature allows you to configure the network settings.

The screenshot displays the 'Network Settings' configuration page. The sidebar on the left contains a 'Network' link, which is highlighted with a red circle and the number 1. The main content area is titled 'Network Settings' and contains several sections:

- MAC Address:** A text input field containing '00:05:50:9c:4f:a8', highlighted with a red circle and the number 2.
- Hostname:** An empty text input field.
- IP Configuration:** Two radio buttons: 'Obtain an IP address automatically (use DHCP)' (selected) and 'Use the following IP address'.
- IPv4 Setting:** A section highlighted with a red circle and the number 3, containing:
 - IP Address:** '172.31.008.115' (highlighted with a red circle and the number 4)
 - Subnet Mask:** '255.255.000.000'
 - Gateway:** '172.31.000.001'
 - DNS Server IP:** '66.120.31.175'
- IPv6 Setting:** A section containing:
 - IPv6 Address:** An empty text input field.
 - Options:** 'Add IP' (selected) and 'Delete IP' (unselected); 'IPv6 C configuration' (checked).
 - Mode:** 'DHCPv6 Stateless' (selected) and 'DHCPv6 Stateful' (unselected).
 - Address List:** A dropdown menu showing 'IPv6 Address List -'.
 - DNS Server IP:** An empty text input field.
- DUID:** A text input field containing '0E:00:00:31:00:00:00:00'.
- VLAN:** Radio buttons for 'enable' (unselected) and 'disable' (selected), highlighted with a red circle and the number 5. A 'VLAN ID' field is empty.
- LAN Interface:** A dropdown menu set to 'Dedicate', highlighted with a red circle and the number 6.
- RMCP Port:** A text input field containing '823', highlighted with a red circle and the number 7.
- Network Link Status:** A table showing the status of the network link.

Active Interface	Dedicated
Dedicated	
List	Auto Negotiation
Status	Connected
Speed	1G
Duplex	Full Duplex
Store	
Status	Disabled
Speed	Unknown
Duplex	Unknown

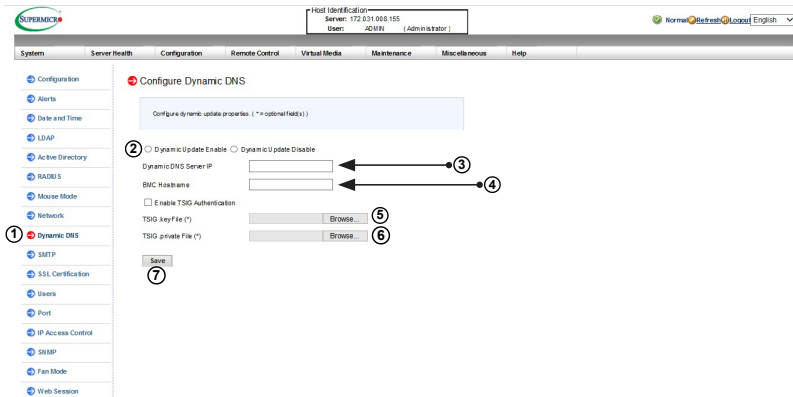
A 'Save' button is located at the bottom of the configuration area. The footer of the page reads 'Copyright © 2014 Super Micro Computer, Inc.'.

- To enter the screen shown above, click on the "Network" item in the *Configuration* sidebar.
- Enter the MAC address for the network server. You can also check the first radio button to obtain an IP address automatically by using DHCP (Dynamic Host Configuration Protocol) or check the second radio button to set up the IP address by manually entering the information in the fields below.
- IPv4 Setting. To set the IP address using the IPv4 format, enter the relevant information in the following fields.
 - IP address
 - Subnet mask
 - (Default) Gateway
 - DNS server IP

4. IPv6 Setting: To set the IP address using the IPv6 format, enter an IPv6 address in the field. Enter a DNS server IP and DUID (unit ID) in the boxes below.
5. VLAN: Check *enable* to enable Virtual LAN support, and enter the VLAN ID in the field.
6. 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 the 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 *Dedicated* to configure the IPMI to connect through the IPMI-dedicated LAN port at all times.
 - Select *Share* to configure the IPMI to connect through the LAN port on the board.
7. RMCP Port: This feature allows the user to select the desired RMCP (Remote Management Control Protocol) port based on his configuration. The default port is 623.
8. Network Link Status: This section details the status of the IPMI network as configured. The following items are listed:
 - *Dedicated*
 - Link
 - Status
 - Speed
 - Duplex
 - *Share*
 - Status
 - Speed
 - Duplex
9. Click *Save* to save the new settings.

2.7.8 Configuring Dynamic DNS (Domain Name System) Settings

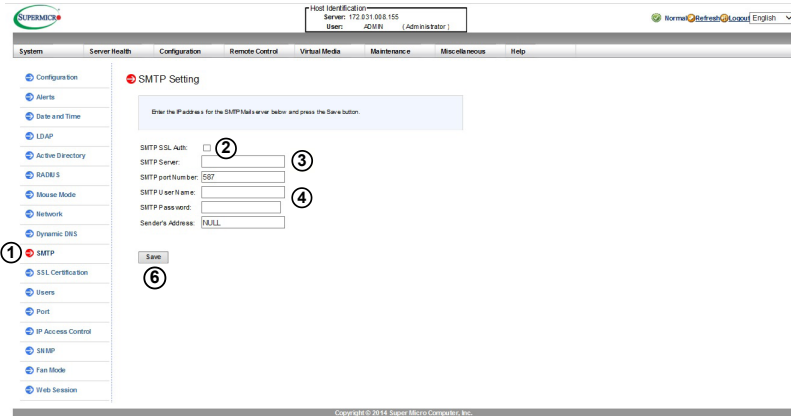
This feature allows you to configure dynamic DNS settings.




1. To enter the screen shown above, click on the "Dynamic DNS" item in the *Configuration* sidebar. Note that you cannot change any of the dynamic DNS settings without first setting up an NTP server. (See page 2-30.)
2. Click the *Dynamic Update Enable* radio button to enable Dynamic DNS update support. Dynamic update is disabled by default.
3. Enter the IP address of your Dynamic DNS (Domain Name System) server.
4. Enter the name of the BMC (Baseboard Management Controller) host server.
5. Check the box to enable TSIG Authentication support, and browse the files to select the *TSIG.key* file. This item is optional.
6. Browse the files to select the *TSIG.private* file. This item is optional.
7. Click *Save* to save the new settings.

2.7.9 Configuring the SMTP Settings

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




1. To enter the screen shown above, click on the "SMTP" item in the *Configuration* sidebar.
2. Check the box to enable SMTP SSL authentication support.
 **Note:** SHA2 and RSA 2048-bit SSL are supported.
3. Enter the IP address for the SMTP (Simple Mail Transfer Protocol) mail server. The SMTP port number will be displayed.
4. Enter a username and password for your SMTP mail server. These items are optional. The status of the sender's address will be displayed.
5. Click Save to save the new settings.

2.7.10 Configuring the SSL (Secure Sockets Layer) Certification

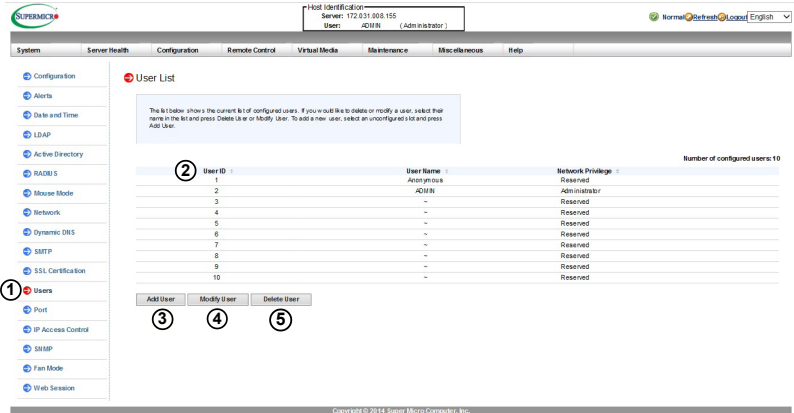
This feature displays the default certificate and private keys. It also allows the user to upload a new SSL certificate.

The screenshot shows the BMC/IPMI web interface. At the top, there is a header with the Supermicro logo, user information (User: ADMIN, Administrator), and language settings (English). Below the header is a navigation menu with tabs: System, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, Miscellaneous, and Help. The 'Configuration' tab is active, and the 'SSL Upload' page is displayed. On the left sidebar, 'SSL Certification' is selected and marked with a circled '1'. The main content area has a title 'SSL Upload' and a message box: 'The data for the default certificate and private key are shown below. To update a new SSL certificate, use the Browse button to navigate to the certificate and press the Upload button.' Below this, there is a table showing certificate details: 'Certification Valid From' (Thursday, October 02, 2014 5:00:00 PM), 'Certification Valid Until' (Monday, October 02, 2017 5:00:00 PM), 'New SSL Certificate' (with a 'Browse...' button marked 2), and 'New Private Key' (with a 'Browse...' button marked 3). At the bottom of the form is an 'Upload' button marked 4.

1. To enter the screen shown above, click on the "SSL Certification" item in the *Configuration* sidebar.
 2. To enter a new SSL Certificate, enter a new certificate in the field. You can also browse the computer to select a new certificate.
-  **Note:** SHA2 and RSA 2048-bit SSL are supported.
3. Enter a new private key in the field, if desired. You can also browse the computer to select a new key.
 4. After entering the new SSL certificate or/and new private key, click *Upload* to upload the certificate and private key to the server.

2.7.11 Configuring User Settings

This page displays information on the current users. It also allows you to add, delete or modify user information.



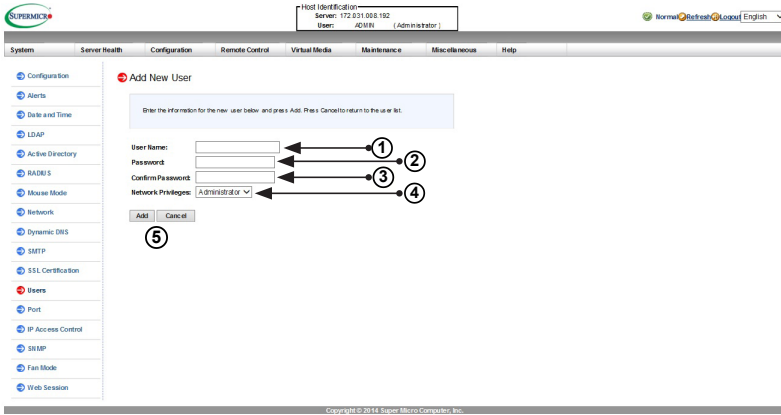
1. To enter the screen shown above, click on the "Users" item in the *Configuration* sidebar.
2. This item lists current user information, including user ID, username, and network privilege settings. Network privilege settings are shown below.

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
Remote Session	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
SDR Update	View Only	View Only	Full Access
Logout	Full Access	Full Access	Full Access

3. To add a new user to the network, click *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 *Modify User*. When prompted, use the arrow keys to select a user from the users list to modify the user information.
5. To delete a user from the network, click *Delete User*. When prompted, use the arrow keys to select a user from the users list to delete it from the list.

2.7.11a User Settings - Add New User

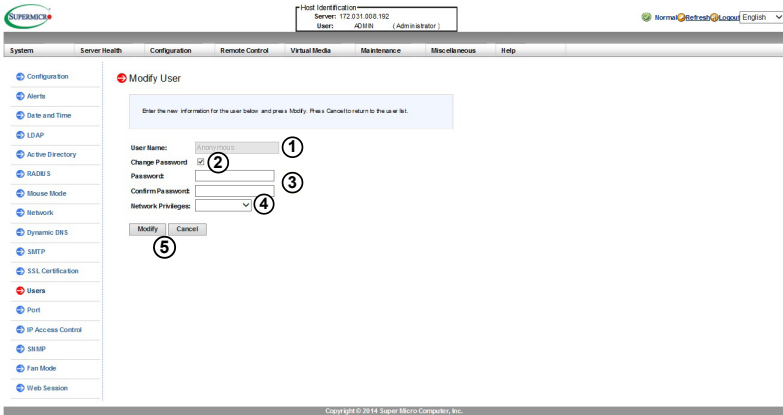
When you click on the *Add User* button as described in section 2.7.11, the following screen will appear.



1. Enter a username.
2. Enter a password.
3. Re-enter the same password.
4. Define the new user's network privileges. The options are the following. Refer to the table on page 2-42 for the list of access privileges.
 - Administrator
 - Operator
 - User
 - No Access
5. Click *Add* to add the new user, or click *Cancel* to return to the User List page without saving.

2.7.11b User Settings - Modify User

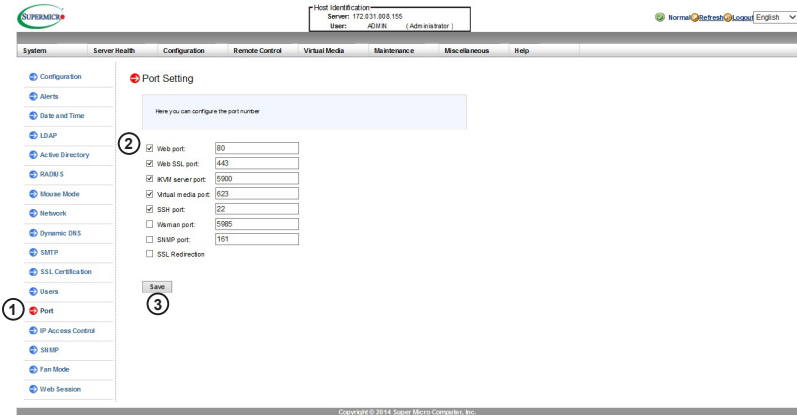
When you select a user and click *Modify User* as described on page 2-42, the following screen will appear.



1. Enter a new username.
2. If you want to change the password, check the *Change Password* box. The password fields will activate.
3. If you want to change the password, enter a new password and confirm.
4. If you want to change the network privileges, select a new setting from the pull-down menu.
5. Click *Modify* to save the changes, or click *Cancel* to return to the User List screen without saving.

2.7.12 Configuring Port Settings

This page allows you to configure port settings for the ports listed on this page.



1. To enter the screen shown above, click on the "Port" item in the *Configuration* sidebar.
2. From this page, you can change the port number of the following ports. Check the boxes next to the respective ports to enable.
 - Web port
 - Web SSL port
 - IKVM server port
 - Virtual media port
 - SSH port
 - Wsman port
 - SNMP Port
 - SSL Redirection - check this box to enable
3. After configuring the port settings, click **Save** to save the settings.

2.7.13 Configuring IP Access Control

This page displays an IP access table and allows you to add, modify and delete an IP access rule, IP address/mask setting, or an IP access policy.



Note: This submenu is applicable to X9 and newer motherboards only.

Host Identification
Server: 172.237.260.110
User: ADMIN (Administrator)

System Server Health Configuration Remote Control Virtual Media Maintenance Miscellaneous Help

Configuration Alerts Date and Time LDAP Active Directory RADIUS Moore Mode Network Dynamic DNS SMTP SSL Certification Users Port

1 IP Access Control

2 Enable IP Access Control

Behe & Places: control table. You can select an Places rule and press the liberty button to configure your Places's policy.

Default Policy: ACCEPT

3 Rule No.	4 IP Address/Mask	5 Policy	6 Number of Access Rules: 10 entries
1	NULL	NULL	
2	NULL	NULL	
3	NULL	NULL	
4	NULL	NULL	
5	NULL	NULL	
6	NULL	NULL	
7	NULL	NULL	
8	NULL	NULL	
9	NULL	NULL	
10	NULL	NULL	

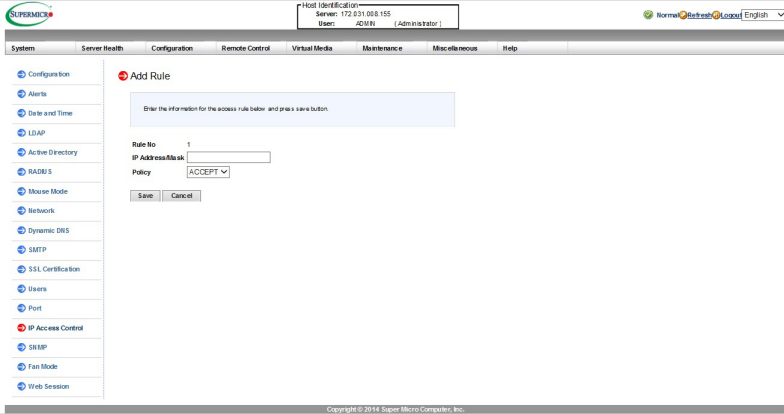
7 Add **8** Modify **9** Delete

Copyright © 2014 Super Micro Computer, Inc.

- To enter the screen shown above, click on the "IP Access Control" item in the *Configuration* sidebar.
- Check this box to enable control of IP access. A message will pop up, reading, "Do you want to enable IP access control?" Click *OK*. The page will reload, and the three buttons at the bottom will activate.
- Rule Number*. This column lists the designated number of the access control rule.
- IP Address/Mask*. This column displays IP address/mask settings.
- Policy*. This column displays the status of an IP access policy.
- Number of Access Rules*. This displays the maximum number of IP access rules you can set for the system.
- Click the *Add* button to add a new rule.
- Click the *Modify* button to modify the rule.
- To delete a rule, select the rule and click the *Delete* button.

2.7.13a IP Access Control - Add New Rule

When you click the *Add* button as described on the previous page, the following screen will appear.



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.
3. When you are done, click *Save* to save the changes, or click *Cancel* to return to the IP Access Control page without saving.

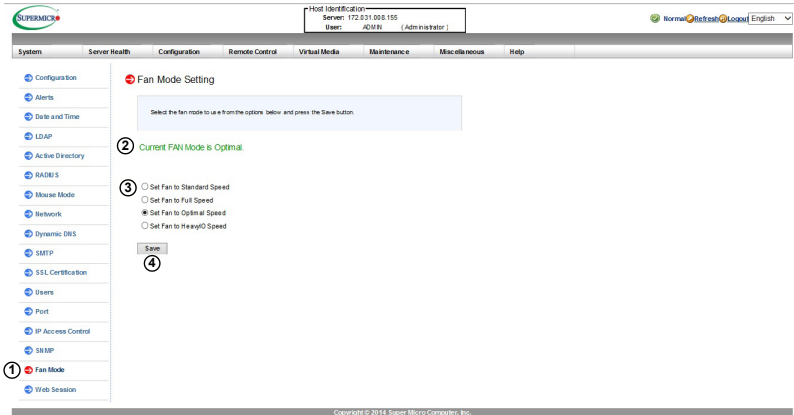
2.7.14 Configuring SNMP Settings

This page allows you to configure SNMP settings.

1. Check the *Enable SNMP* box to modify SNMP settings. Certain fields on the page will activate.
2. Click the *SNMPV2* radio button to modify v2 settings; the relevant SNMPV2 fields will activate.
 - Enter either (or both) the ROCommunity (Read-Only Community) name or the RWCommunity (Read-Write Community) name. If you enter both, do not specify the same names.
3. Click the *SNMPV3* radio button to modify v3 settings; the relevant SNMPV3 fields will activate.
 - Enter a username.
 - Specify the authentication protocol, either MD5 or SHA-1.
 - Specify the privacy (encryption) protocol, either DES or AES.
 - Enter the authentication protocol key. It should be over 8 characters long.
 - Enter the privacy protocol key. It should be over 8 characters long.
4. Once you are done configuring your settings, click *Save*.


2.7.15 Configuring Fan Settings

This page allows you to configure fan mode settings.



1. To enter the screen shown above, click on the "Fan Mode" item in the *Configuration* sidebar.
2. This item displays the current fan mode setting.
3. The following options are listed. Check the corresponding radio button to enable the setting.

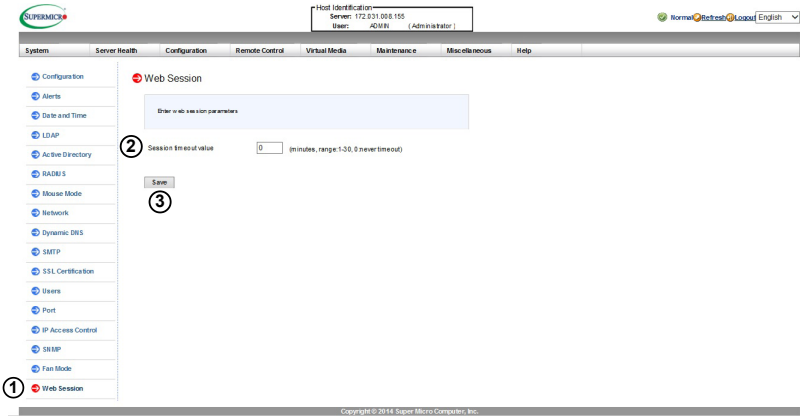
- *Standard speed*, for standard power efficiency
- *Full speed*, for maximum system performance
- *Optimal speed* or *PUE2 speed*, for most efficient cooling under normal use
- *Heavy IO speed*, for running the system at maximum I/O (maximizing cooling around PCI-E add-on cards)

 **Note:** Heavy IO mode is used in X10 motherboards with dual cooling zones. PUE Optimal mode is used in certain X10 motherboards with single cooling zones to consume the least amount of power possible.

4. Click **Save** to save the new setting.

2.7.16 Configuring the Web Session Settings

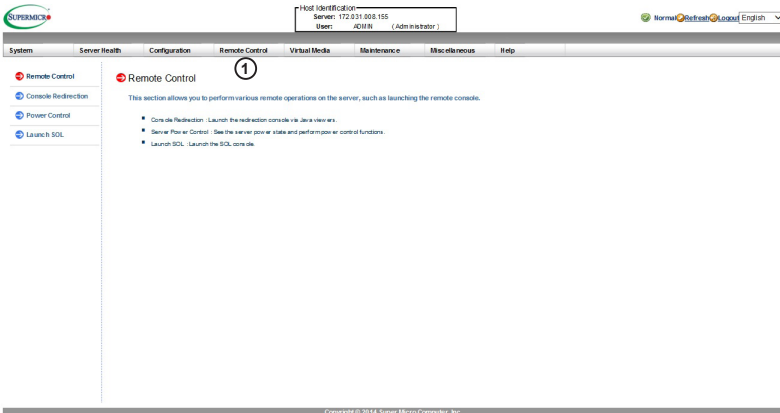
This feature allows the user to configure the web session timeout value.



1. To enter the screen shown above, click the "Web Session" item in the *Configuration* sidebar.
2. Input the length of time, in minutes, you would like the web session to remain before timing out. The default is 0, which means that the web session will never time out.
3. Click *Save* to save the new setting.

2.8 Remote Control

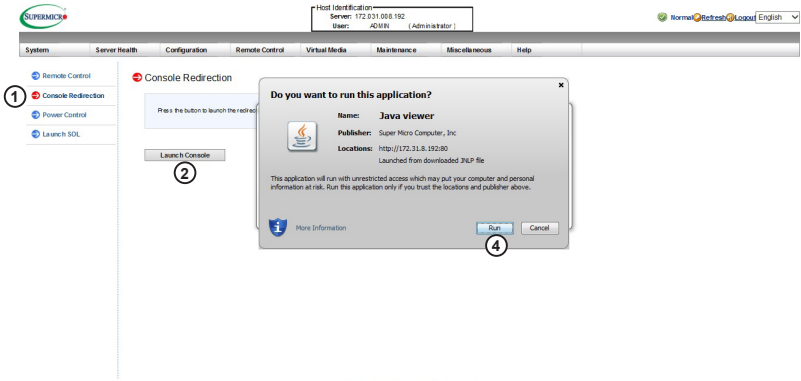
This section allows the user to carry out activities and perform operations on a remote server via remote access.



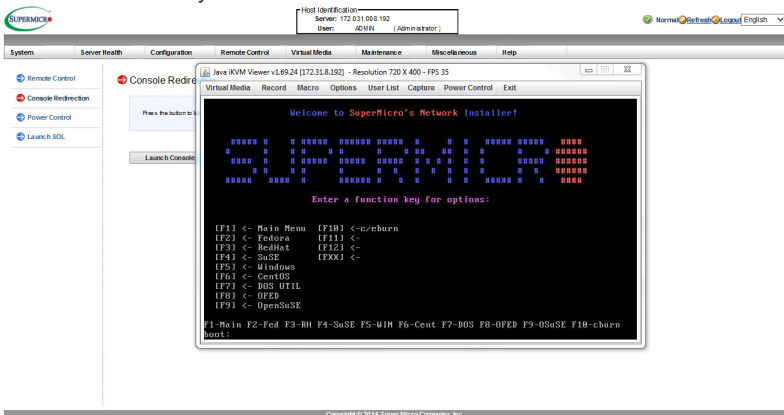
1. To access the screen shown above, click on the *Remote Control* header in the top bar. The following features can be accessed in the sidebar:
 - *Console Redirection* launches the remote console and configure the settings of the remote server. For more details on console redirection, please refer to *Launching Console Redirection* on 2-50.
 - *Power Control* displays and configures the power settings of the remote console, including the following settings.
 - *Launch SOL* launches the SOL (Serial Over LAN) console to manage the remote server.

2.8.1 Console Redirection

This feature allows you to launch console redirection via IKVM (keyboard, video/monitor, mouse) support.

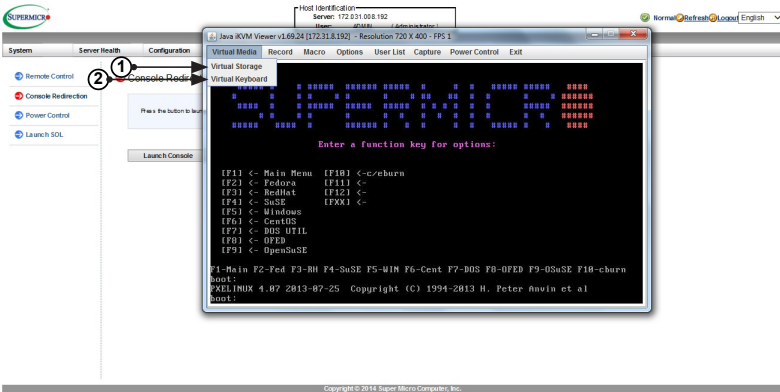


1. To enter the screen shown above, click on the "Console Redirection" item in the *Remote Control* sidebar.
2. Click *Launch Console* to launch the remote console via Java (for Internet Explorer). If it is blocked by the IE due to security reasons, click on the top of the menu bar and select "Download File."
3. A screen will display to indicate that Java is launching. If you see a window pop up informing you that the connection or application is untrusted, trust the application and click *Continue*.
4. When the warning screen as shown above displays, click *Run* to launch the remote console.
5. The main screen should appear as shown below. Note that your screen may not look exactly like the one below.



2.8.1a Console Redirection - Virtual Device

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

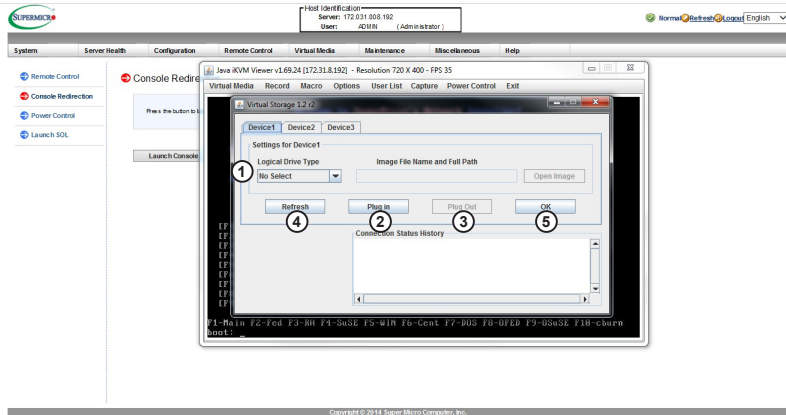


1. Click *Virtual Media* to configure virtual device settings of a server at a remote site via Console Redirection.
2. Click *Virtual Storage* to select a device you want to connect to the remote server as a virtual device.

You can connect Floppy, USB Flash, CD-ROM, DVD ROM or ISO images using this feature.

Virtual Storage

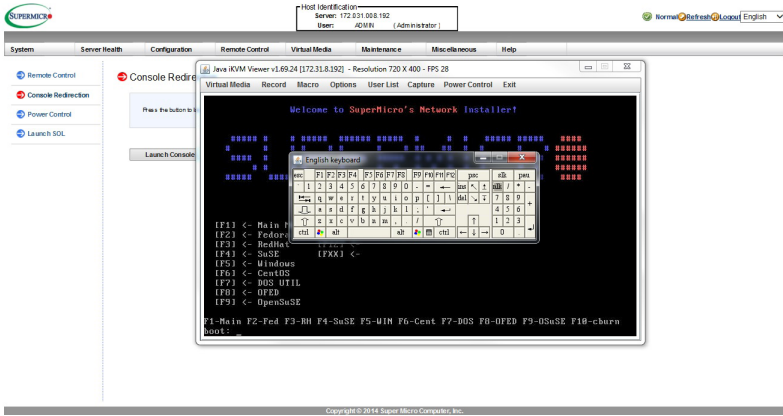
When you click the *Virtual Storage* item as described on the previous page, the following screen will appear. You are able to use up to three devices for virtual storage.



1. Select the logical drive type from the dropdown menu. The options are as follows:
 - *Upload IMA*. Select to browse for and upload an IMA file.
 - *ISO File*. Select to browse for and upload an ISO file.
 - *Web ISO*. Select to mount a Web ISO. The file will be mounted from the web interface. To specify the file location, set the image path on the CD-ROM Image page in the IPMI. (See page 2-85.)
 - *C: SATA HD*. Select to mount from the local computer you are using to access the IPMI.
2. Click *Plug in* to mount the selected drive.
3. Click *Plug out* to unmount the selected drive.
4. Click *Refresh* to refresh the connection status.
5. Click *OK* to save the changes and exit the window.

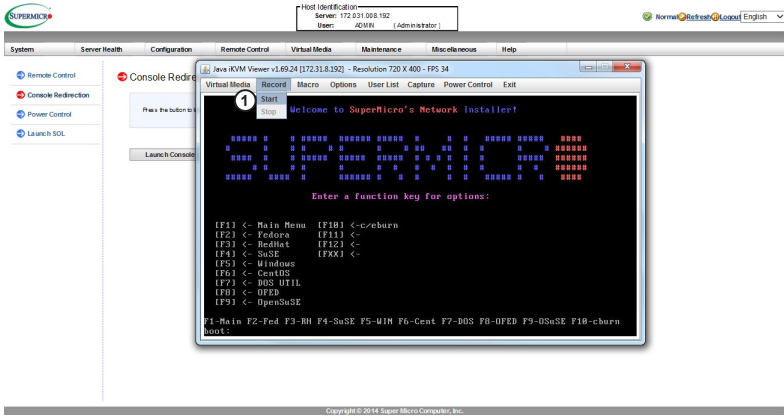
Virtual Keyboard

When you click the *Virtual Keyboard* item under the Virtual Media menu, the virtual keyboard will pop up.



2.8.1b Console Redirection - Recording

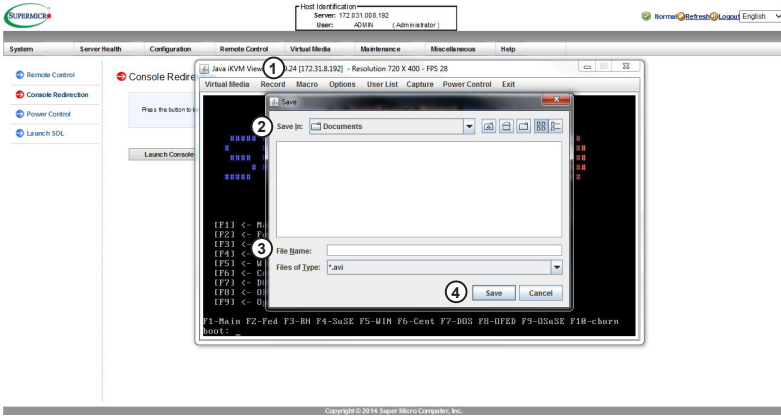
This feature allows you to record media displays for your console redirection.



1. Click *Start* to start video recording from your remote server. Click *Stop* to stop video recording from your remote server.

Recording

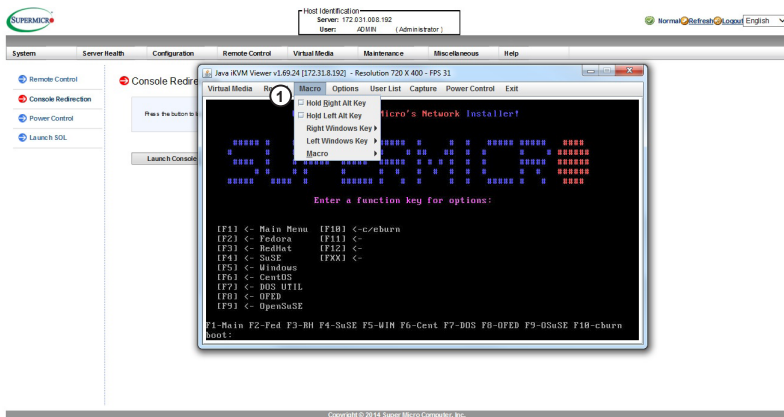
This feature allows you to record the media displays.



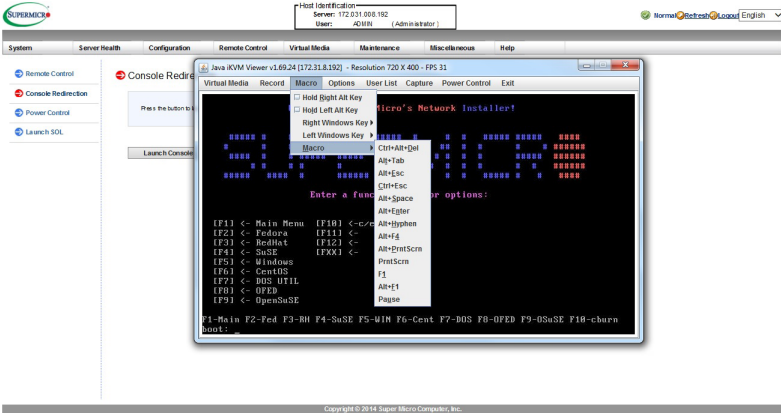
1. Click *Start* from the Record menu (as described in the previous page) to start recording. The window shown above will pop up.
2. Browse for and select the location where you want to save the recording.
3. Enter a file name.
4. Click *Save* to save the settings and begin recording, or click *Cancel* to exit the window without recording. The recording process will continue until you click *Stop* under the Record menu.

2.8.1c Console Redirection - Macro

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



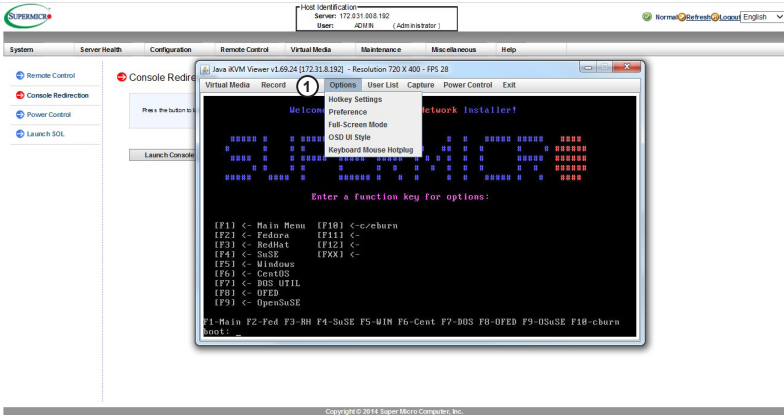
1. Click *Macro* to configure the Macro settings for your remote server. The features include the following:
 - *Hold Right Alt Key*. This item performs the same function as holding down the right <Alt> key.
 - *Hold Left Alt Key*. This item performs the same function as holding down the left <Alt> key.
 - *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*.
 - *Macro*. Click this item to activate a pull-down submenu. The Macro submenu includes the following items as listed on the next page.



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

2.8.1d Console Redirection - Options

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

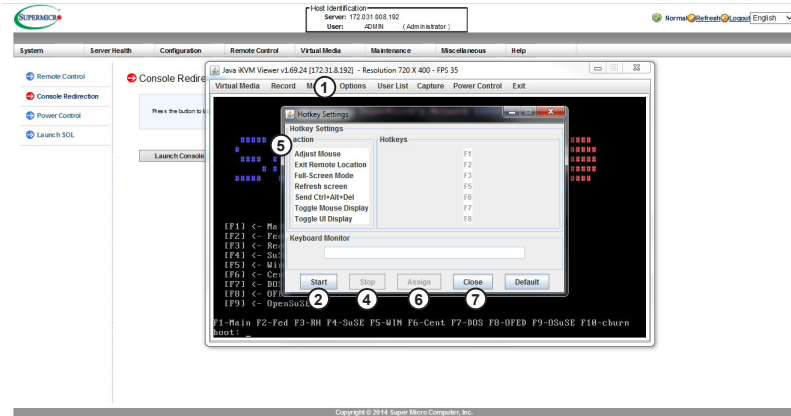


1. Click *Options* to activate the pull-down menu to configure options settings. The options menu allows you to configure the following settings.

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

Options - Hotkey Settings

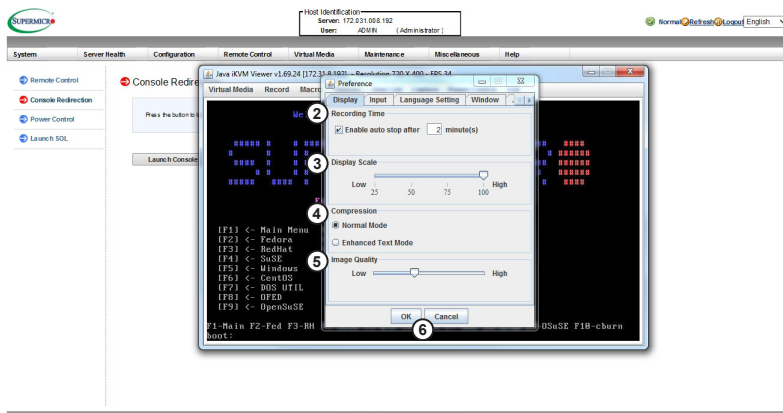
This feature allows you to configure hotkey settings for your console redirection.



1. To assign a hotkey for an action, click *Hotkey Settings* under the *Options* menu. A *Hotkey Settings* window will pop up.
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)

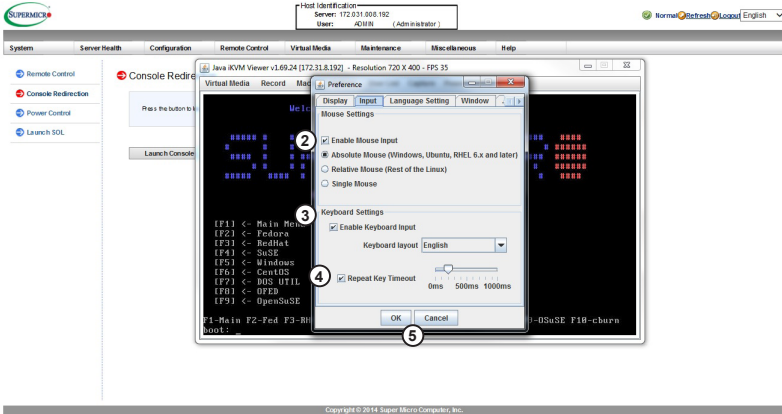
This feature allows you to configure video recording settings for your remote console.



1. Click *Preference* under the Options menu. A window will pop up. The first tab is *Display*.
2. The *Recording Time* section refers to video recording. (To learn more about video recording, see page 2-57.) 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; select *Low* for lighter network traffic.
6. Click *OK* to save the new settings, or click *Cancel* to exit the Preference window without saving.

Options - Preference (Input)

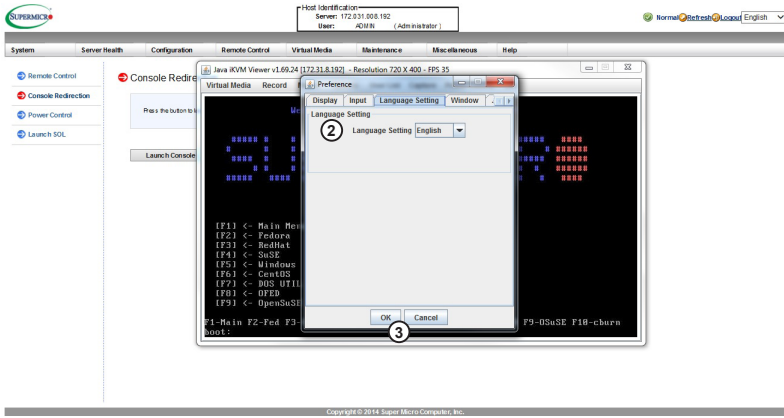
This feature allows you to configure input settings for your remote console.



1. Click *Preference* under the Options menu. A window will pop up. 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 the Windows OS
 - 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 *Save* to save the new settings or click *<Cancel>* to exit the Preference window without saving.

Options - Preference (Language Setting)

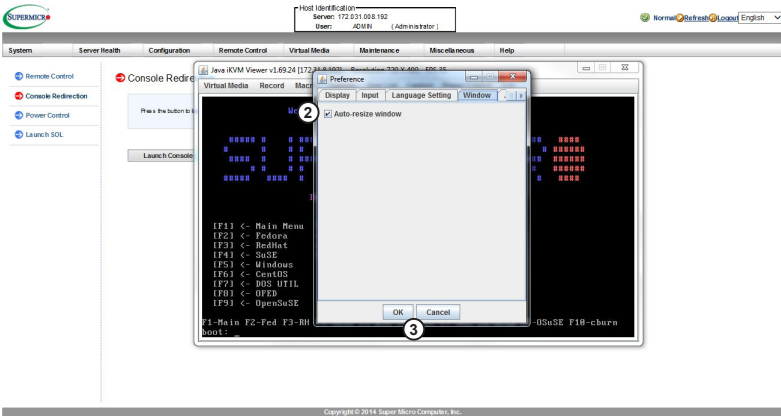
This feature allows you to configure language settings for your remote console.



1. Click *Preference* under the Options menu. A window will pop up. 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 *OK* to save the changes and exit the window, or click *Cancel* to exit without saving.

Options - Preference (Window)

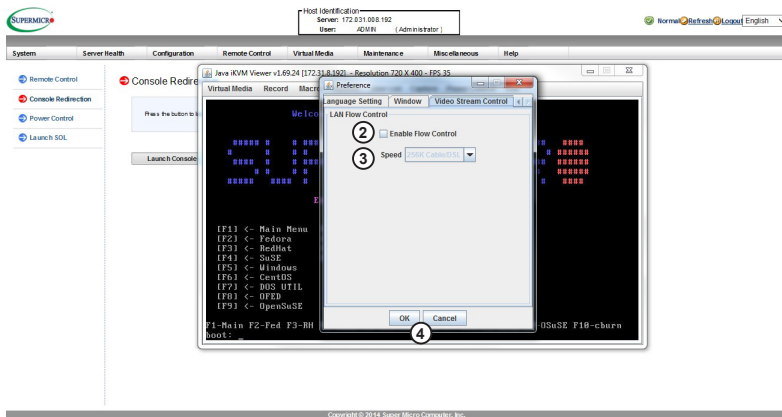
This feature allows you to configure window settings for your remote console.



1. Click *Preference* under the *Options* menu. A window will pop up. 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, or click *Cancel* to exit without saving.

Options - Preference (Video Stream Control)

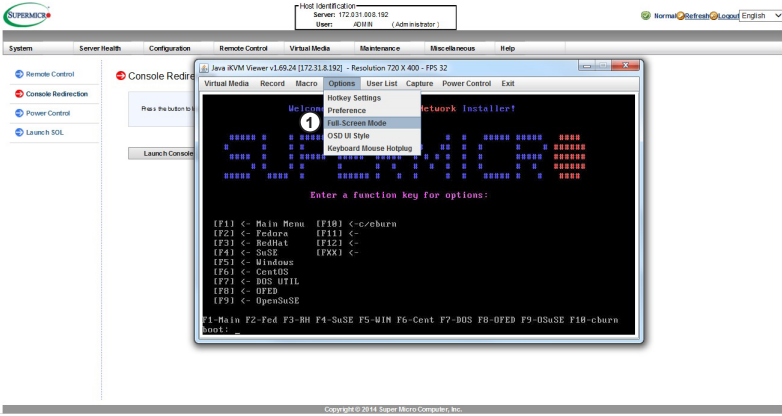
This feature allows you to configure window settings for your remote console.



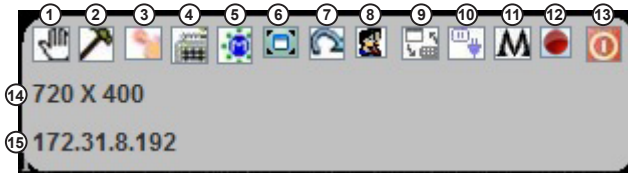
1. Click *Preference* under the Options menu. A window will pop up. The last tab is *Video Stream Control*.
2. Check the *Enable Flow Control* box to enable support for video stream control.
3. Select the speed from the pull-down menu. The options are as follows:
 - 256K Cable/DSL
 - T1
 - T2
4. Click *OK* to save the change and exit the window, or click *Cancel* to exit without saving.

Options - Full Screen Mode

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

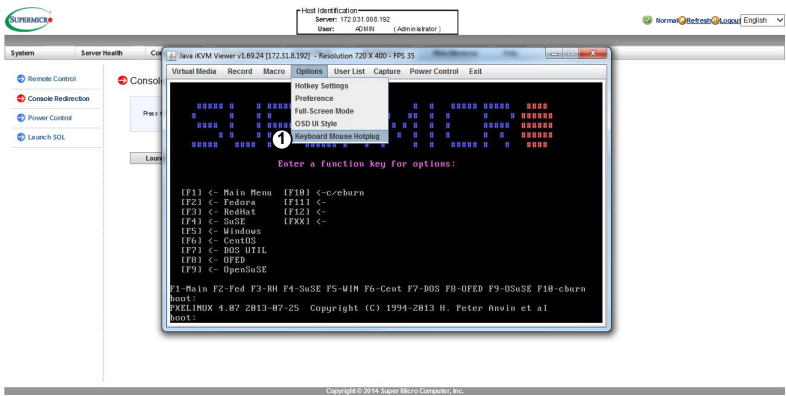


1. Click *Full-Screen Mode* under the Options menu.
2. To leave the full-screen display, click *Leave Full-Screen Mode* under the Options menu.



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. For more about hotkey settings, see page 2-62.
3. **Virtual Storage:** Click this item to access the Virtual Media submenu and configure the settings. For more about virtual storage, see page 2-55.
4. **Virtual Keyboard:** Click this item to access the Virtual Keyboard submenu and use your virtual (soft) keyboard. For more about the virtual keyboard, see page 2-56.
5. **Preference:** Click this item to access the Preferences window. For more about this window, see pages 2-63 through 2-67.
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. For more about the user list, see page 2-72.
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. For more about keyboard-mouse hotplug, see page 2-71.
11. **Macro:** Click this item to enable Macro support and use Macro features. For more about Macro support, see pages 2-59 and 2-60.
12. **Record:** Click this item to access the Video Recording submenu and to use video recording. For more about recording, see pages 2-57 and 2-58.
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.

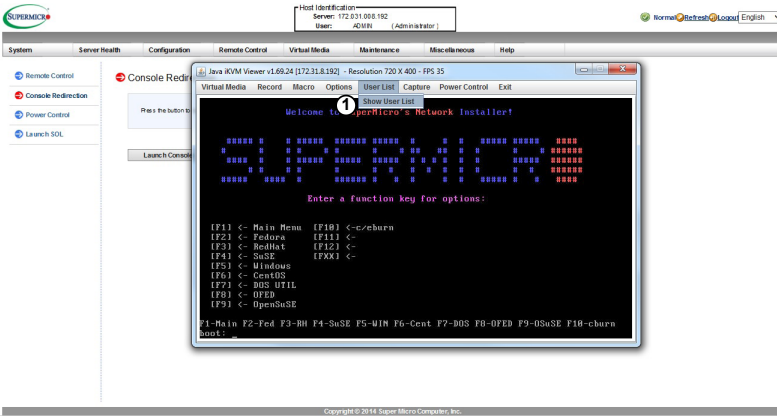
Options - Keyboard Mouse Hotplug



1. Click *Keyboard/Mouse Hotplug* under the *Options* menu to enable keyboard/mouse hotplug support for your remote console.

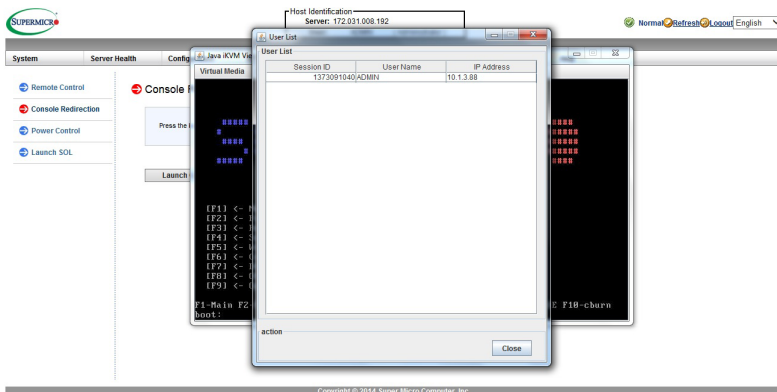
2.8.1e Console Redirection - User List

This feature allows you to access the user list.



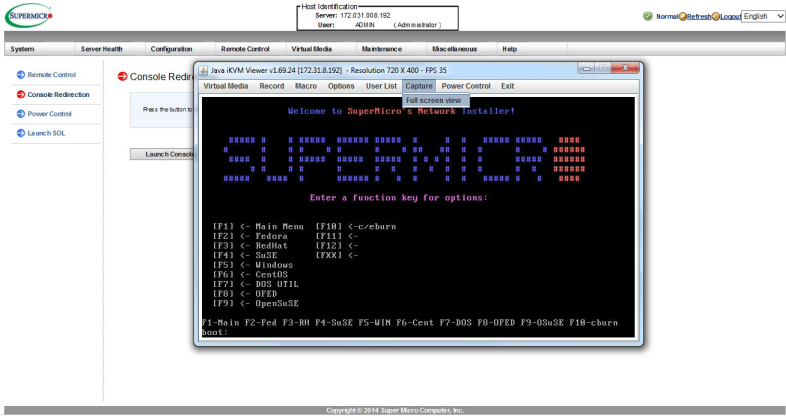
1. Click *Show User List* under the User List menu. A window will pop up displaying the following three columns:

- *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.



2.8.1f Console Redirection - Capture

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



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

2.8.1g Console Redirection - Power Control

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

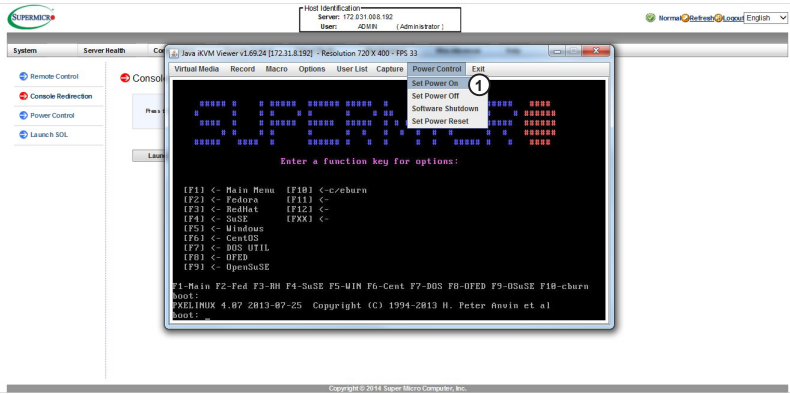


1. The power control features are the following:

- *Set Power On*. Allows you to turn the system on if it is off.
- *Set Power Off*. Allows you to turn the system off.
- *Software Shutdown*. Allows you to perform a graceful shutdown of the system.
- *Set Power Reset*. Allows you to reset the system.

Power Control - Set Power On

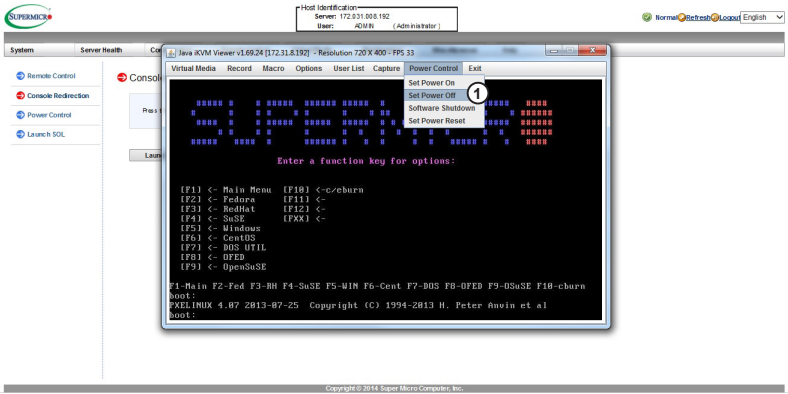
The "Set Power On" option allows you to power on the system if the system is off.



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

Power Control - Set Power Off

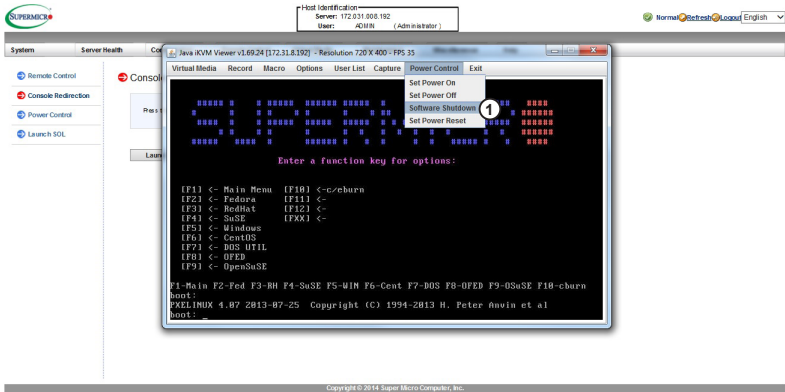
The "Set Power Off" option allows you to power off the system if the system is on.



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

Power Control - Software Shutdown

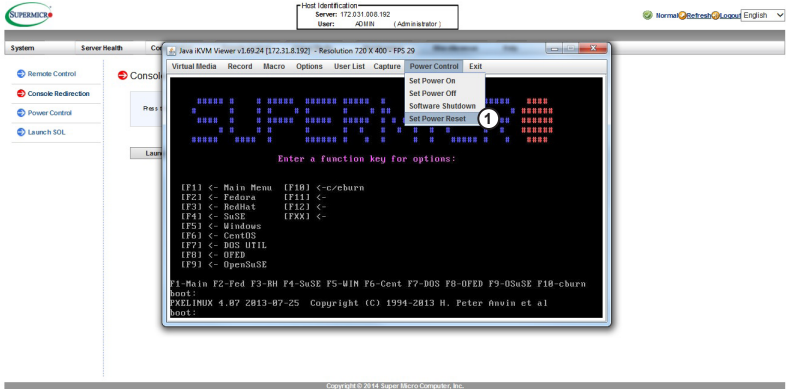
The "Software Shutdown" option allows you to perform a graceful shutdown of the operating system.



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

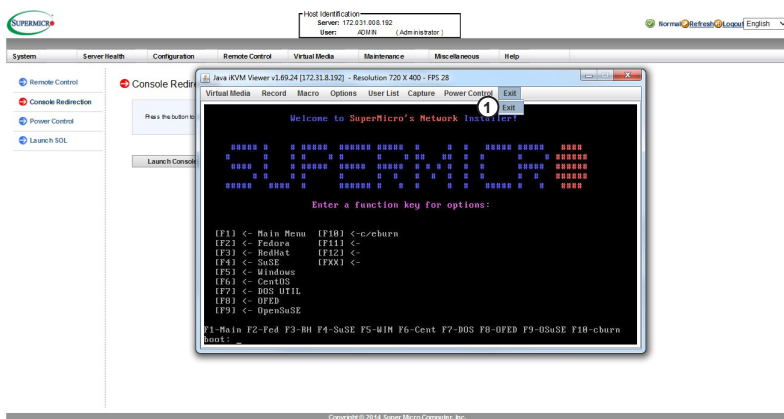
Power Control - Set Power Reset

The "Set Power Reset" option allows you to reset the system.

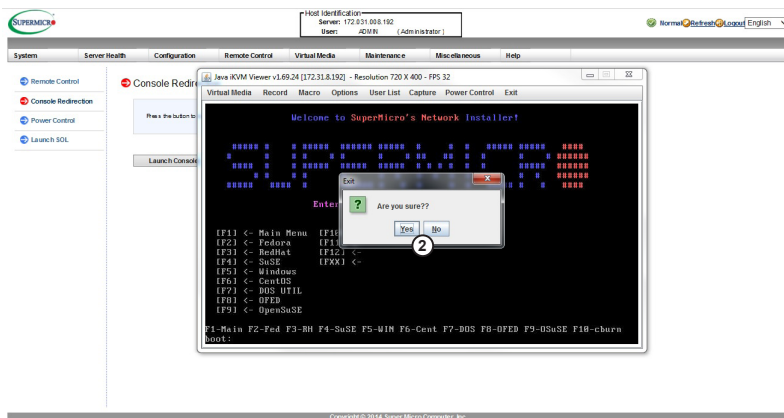


1. Click the "Set Power Reset" option under the Power Control menu.

2.8.1h Console Redirection - Exit



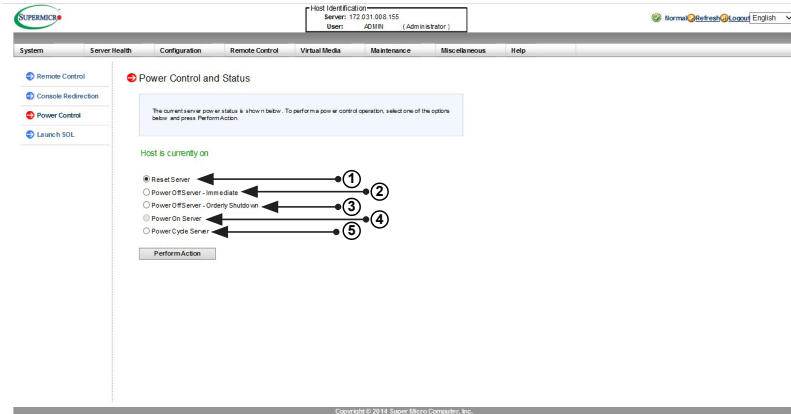
1. To exit from Console Redirection, click *Exit* under the Exit menu.



2. At the prompt that reads, "Are you sure??" click *Yes* to exit from the remote console. Otherwise, click *No* to return to the remote console.

2.8.2 Power Control

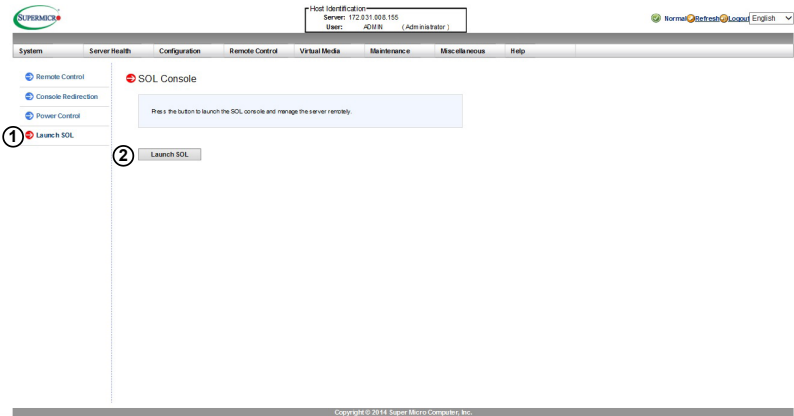
This feature allows the user to check the power state and manage the system power status.



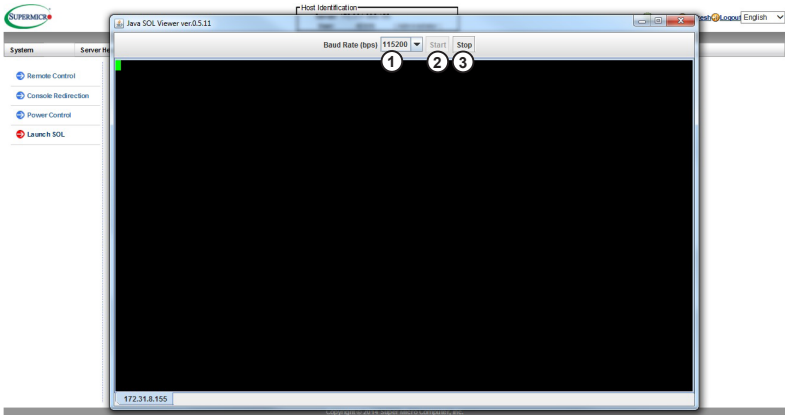
1. To enter the screen shown above, click on the "Power Control" item in the *Remote Control* sidebar. The following options are listed:
 - Click *Reset Server* to reset the host server.
 - Click *Power Off Server - Immediate* to power off the remote server immediately.
 - Click *Power Off Server - Orderly 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.

2.8.3 Launch SOL

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.



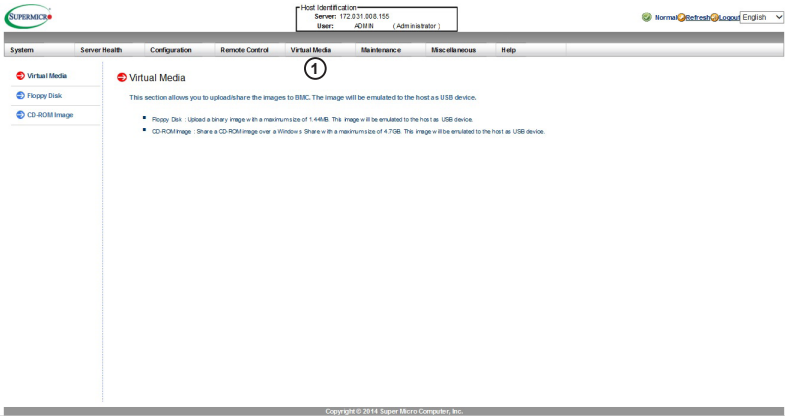
1. To enter the screen shown above, click on the "Launch SOL" item in the *Remote Control* sidebar.
2. To launch SOL, click the *Launch SOL* button. A window will pop up as shown on the next page.



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 BIOS.
 - 9600 bps (bits per second)
 - 19200 bps
 - 38400 bps
 - 57600 bps
 - 115200 bps
2. Once you've selected the baud rate, press *Start* to start the session. Once you have started the session, you can input SOL commands through the command-line interface.
3. You can also press *Stop* to stop SOL connection.

2.9 Virtual Media

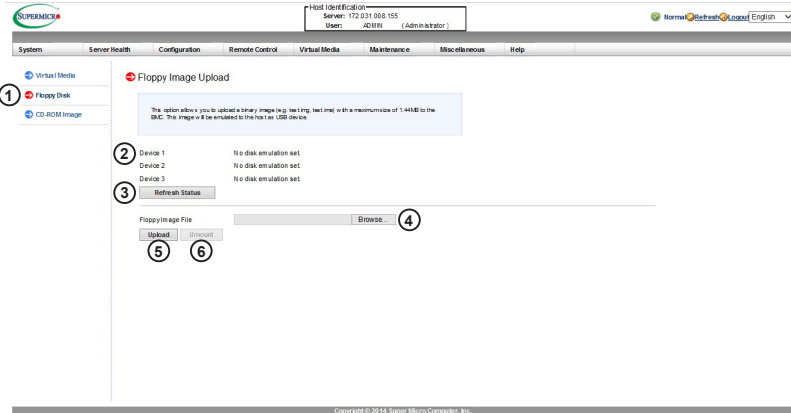
This feature allows you to upload and share images via the BMC (Baseboard Management Controller). These images will be emulated to the host server as USB devices.



1. Click the *Virtual Media* header on the top bar to configure virtual media settings for your remote console, including floppy disk and CD-ROM image settings. The following features can be accessed from this page:
 - *Floppy Disk*, which allows you to upload floppy images to the BMC
 - *CD-ROM Image*, which allows you to upload CD-ROM images to the BMC

2.9.1 Uploading Floppy Images

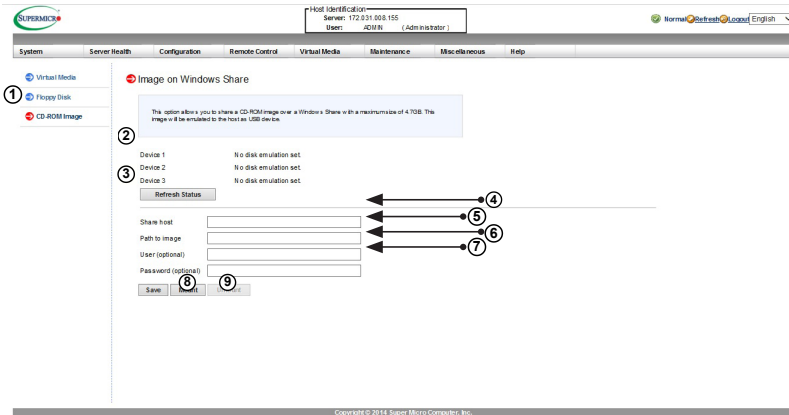
This page allows you to upload floppy image files to share to the BMC. The maximum image size is 1.44 MB.



1. To enter the screen shown above, click on the "Floppy Disk" item in the *Virtual Media* sidebar.
2. A list of devices will display, which shows the status of up to three flash devices.
3. Click *Refresh Status* to refresh the status of the devices.
4. Click *Browse* and select an image file from your computer to upload to the BMC.
5. After you've selected your image file, click *Upload* to upload your image file to the server.
6. To unmount the floppy image from the BMC, select *Unmount*.

2.9.2 Uploading CD-ROM Images

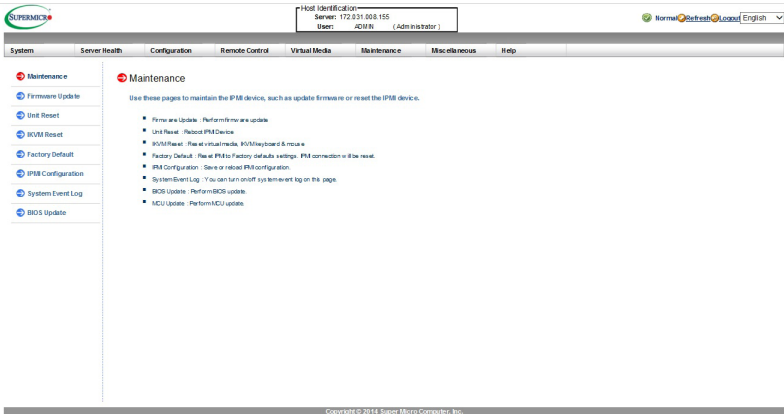
This page allows you to upload CD-ROM image files to share to the BMC. Here, you can upload ISO images and configure their settings. The maximum image size is 4.7 GB.



1. To enter the screen shown above, click on the "CD-ROM Image" item in the *Virtual Media* sidebar.
2. A list of devices will display, which shows the status of up to three flash devices.
3. Click *Refresh Status* to refresh the status of the devices.
4. Enter the IP address of the share host server.
5. In the *Path to image* field, enter the path to the CD-ROM image file for sharing.
6. In the *User (optional)* field, specify the users that have access to the CD-ROM image files. This item is optional.
7. In the *Password (optional)* field, enter your user password. This item is optional.
8. To mount an image file, follow the steps below in sequence.
 - Click *Save*.
 - Click *Mount*.
9. To unmount an image file, follow the steps below in sequence.
 - Click *Unmount*.
 - Click *Save*.

2.10 Maintenance

Use this menu to manage the IPMI device, including resetting and updating.



1. Click the *Maintenance* header on the top bar. The Maintenance main screen will display as shown above. The following features can be accessed from this page:

- *Firmware Update*. Click this item to update the remote server's BMC firmware.
- *Unit Reset*. Click this item to reboot the BMC (IPMI) controller.
- *KVM 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 item to enable or disable the system event log.
- *BIOS Update*. Click this item to update the BIOS remotely.
- *MCU Update*. Click this item to update the MCU remotely.

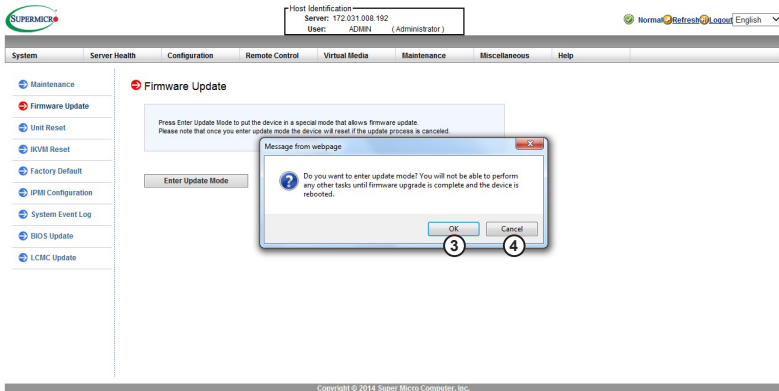
2.10.1 Firmware Update

You will be able to update the IPMI firmware from this page.



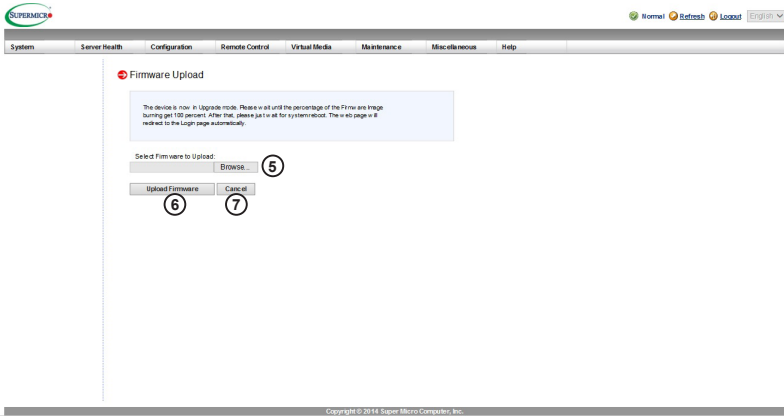
1. To enter the screen shown above, click the "Firmware Update" item in the *Maintenance* sidebar.
2. Click *Enter Update Mode* to enter the update mode. A message will pop up as shown in the image below.

STOP Warning: Once the server is in the firmware update mode, the device will be reset, and the server will reboot even if you cancel firmware updating.



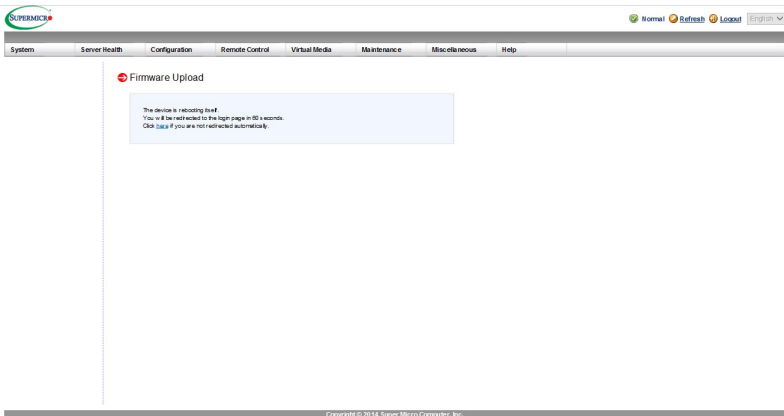
3. Click *OK* to update your IPMI firmware. The Firmware Upload screen will display as shown below.
4. If you want to cancel the firmware update, click *Cancel*. Keep in mind that by this point, the server will already be reset even if you choose to cancel.

- Browse your computer for the firmware file you wish to upload. You can also select a firmware from the pull-down menu to upload.
- Click *Upload Firmware* to upload the selected firmware to the host server.



Warning: To properly update your firmware, do not interrupt the process until the process is completed. Once it is completed, the system will automatically reboot, and you will need to login to the server again.

- If you wish to abort at this time, click *Cancel*. If you cancel, the screen below will appear. You may need to log in again to continue working with the IPMI.



2.10.2 Unit Reset

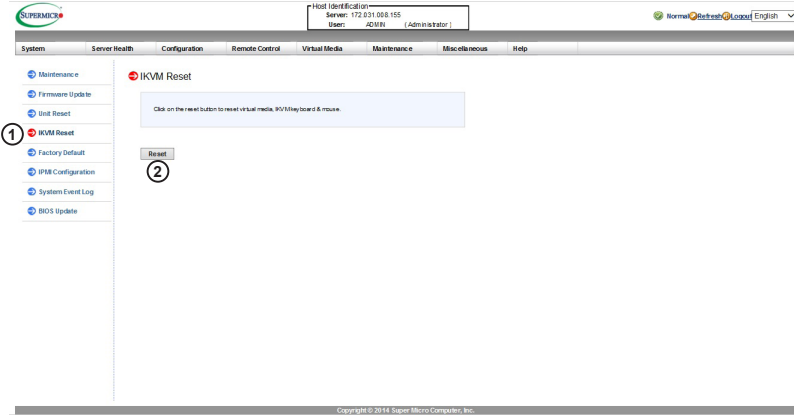
Use this feature to reset the IPMI device.



1. To enter the screen shown above, click on the "Unit Reset" item in the *Maintenance* sidebar.
2. To reset the device, click the *Reset* button.

2.10.3 IKVM Reset

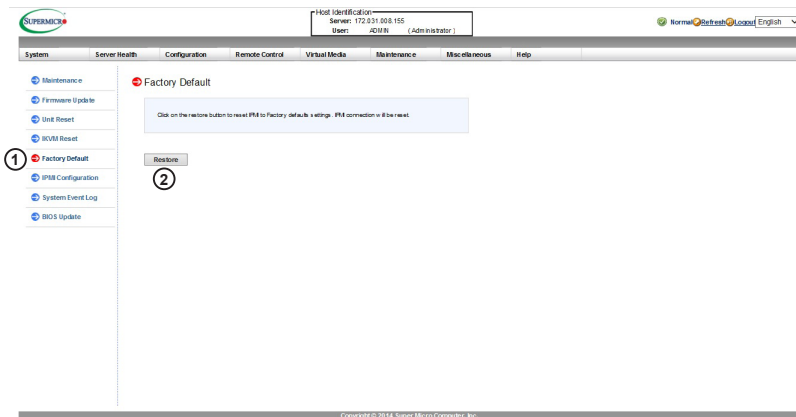
This feature allows you to reset IKVM. It will reset the virtual media, IKVM keyboard, and mouse.



1. To enter the screen shown above, click on the "IKVM Reset" item in the *Maintenance* sidebar.
2. To reset IKVM, click the *Reset* button.

2.10.4 Factory Default

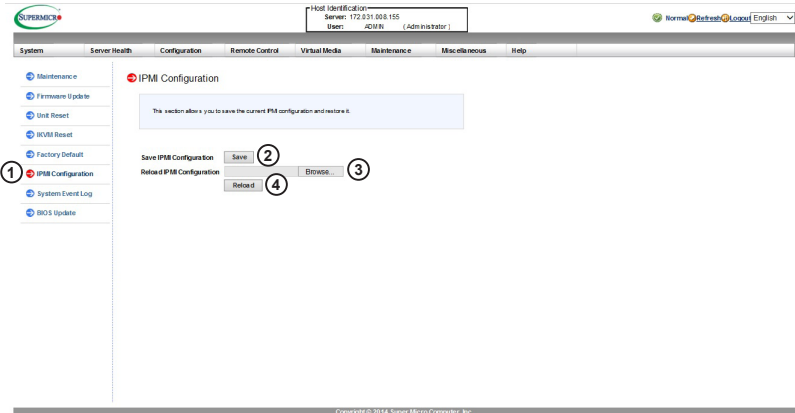
This feature allows the user to restore the IPMI to factory default settings.



1. To enter the screen shown above, click on the "Factory Default" item in the *Maintenance* sidebar.
2. To restore to factory default, click the *Restore* button.

2.10.5 IPMI Configuration

This feature allows the user to save the IPMI configuration settings in a file that can be uploaded later.



1. To enter the screen shown above, click on the "IPMI Configuration" item in the *Maintenance* sidebar.
2. Click *Save* to save the IPMI configuration settings. You may see a window pop up asking if you want to save *save_config.bin*. Click *Save*. The file will be saved into your computer in your Downloads folder or in a folder of your choice.
3. To upload an IPMI configuration file that was previously saved, click *Browse* and select the file in your computer.
4. Click *Reload* to reload the new configuration file.

2.10.6 System Event Log

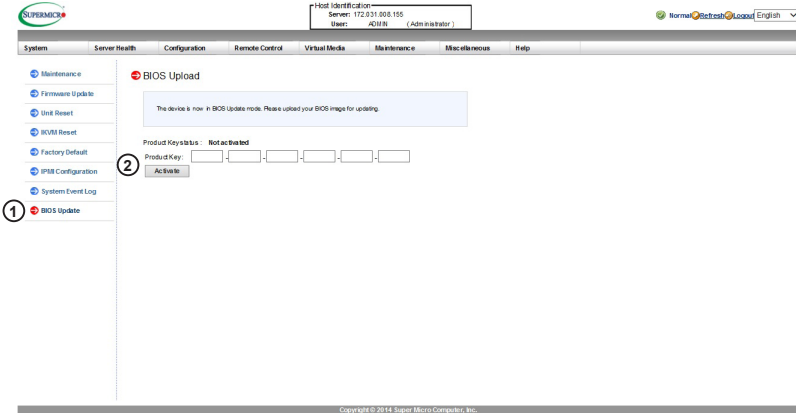
This feature allows you to enable and view the system event log.

The screenshot displays the BMC/IPMI web interface. At the top, there is a header with the SUPERMICO logo, user information (Server: 172.031.008.155, User: ADMIN, Administrator), and language settings (Normal, Dark, Light, English). Below the header is a navigation bar with tabs: System, Server Health, Configuration, Remote Control, Virtual Media, Maintenance, Miscellaneous, and Help. The left sidebar contains a 'Maintenance' menu with items: Maintenance, Firmware Update, UEFI Reset, BIOS Reset, Factory Default, IPMI Configuration, System Event Log (selected), and BIOS Update. The main content area is titled 'List of System Event Log' and contains a message: 'Below is a list of the System Event Log'. Below this message is a checkbox labeled 'Enable System Event Log' (2). Underneath the checkbox is a table with the following headers: 'No.', 'Time', 'IP Address', and 'Description'. The table is currently empty, with a note 'Log Table: 0 entries' on the right. Below the table is a 'Clear' button (4). The footer of the page reads 'Copyright © 2014 Super Micro Computer, Inc.'.

1. To enter the screen shown above, click on the "System Event Log" item in the *Maintenance* sidebar.
2. Check the *Enable System Event Log* box to enable the system event log. A window will pop up, reading, "The requested configuration has been successfully set." Click *OK*.
3. You will be able to view system events recorded in the log. Click the arrows next to each header to rearrange the events.
4. To clear the system event log, click *Clear*.

2.10.7 BIOS Upload

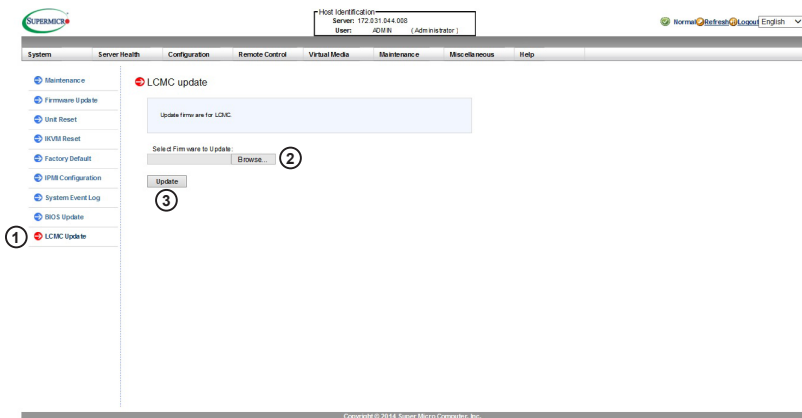
You will be able to update the BIOS image from this page. You will need to purchase a license key to continue. Use the Supermicro part number SFT-OOB-LIC.



1. To enter the screen shown above, click on the "BIOS Update" item in the *Maintenance* sidebar.
2. Enter your license key in the fields and click *Activate*. If the license key has been accepted, you will be able to upload the BIOS image from your computer.

2.10.8 LCMC Update

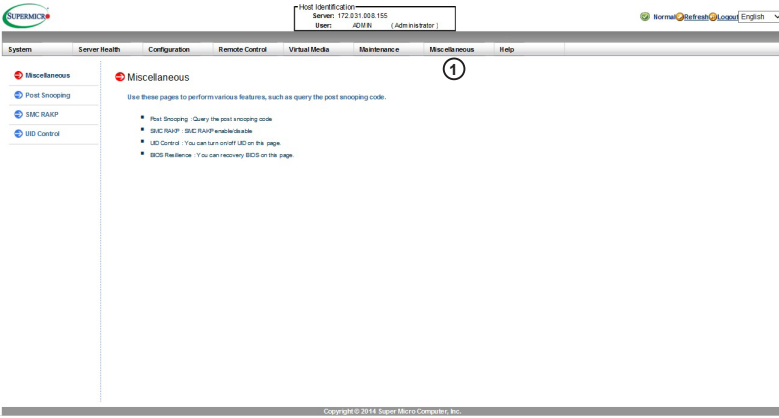
The LCMC (Lite Chassis Management Controller) is used in multi-node systems to access and manage all nodes singly and remotely rather than having to log in to access each individual node, as well as provide each node access to other nodes' statuses. If your system includes the LCMC feature, which is used in multi-node systems, you will be given the option to update the LCMC firmware from this page.



1. To enter the screen shown above, click on the "LCMC Update" item in the Maintenance sidebar. Note that your system may or may not have this feature.
2. Click *Browse* to select an LCMC file from your computer to upload.
3. Click *Update* to update the LCMC.

2.11 Miscellaneous

This feature allows the user to perform various network activities including POST (Power-On-Self Test) code query and turning on/off UID control.



1. Click the *Miscellaneous* header on the top bar. The screen shown above will appear. You will be able to access the following features from this page:

- POST Snooping
- SMC RAKP
- UID Control

2.11.1 POST Snooping

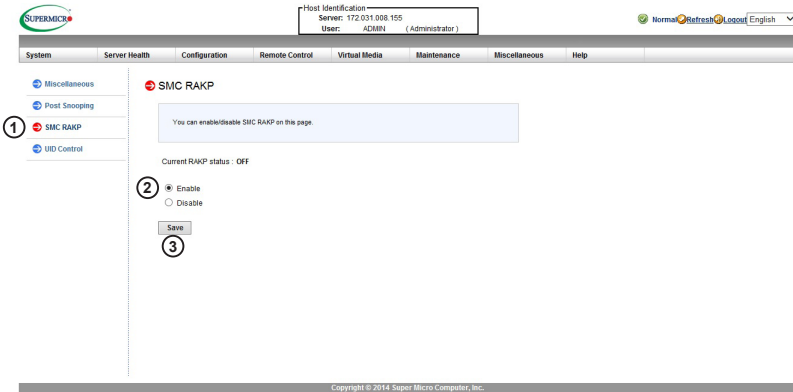
POST snooping allows you to view the current BIOS POST (Power-On Self-Test) code.




1. To access the screen shown above, click on the "Post Snooping" item in the *Miscellaneous* sidebar.
2. The POST code will display on the page.
3. Click *Refresh* to query the POST Snooping code for BIOS LPC Port80.

2.11.2 SMC RAKP

This page allows you the option of enabling or disabling the RAKP (Remote Authenticated Key exchange Protocol). By default, the RAKP is off.

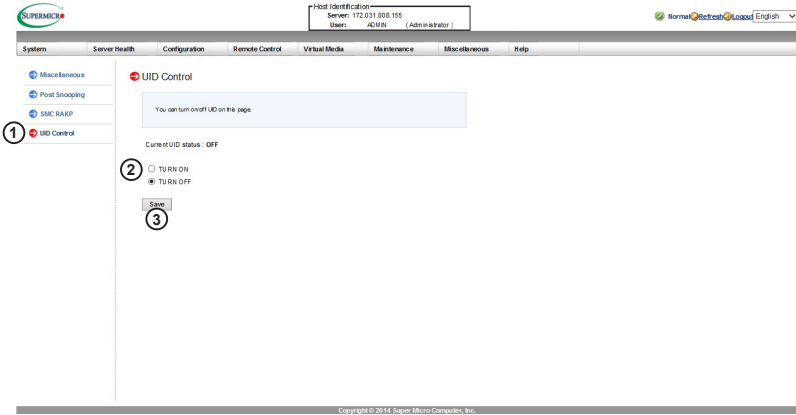


1. To enter the screen shown above, click on the "SMC RAKP" item in the *Miscellaneous* sidebar.
2. To enable the RAKP, click the *Enable* radio button. Alternatively, click *Disable* to disable the RAKP.
3. Click *Save* to save the new setting.

 **Note:** This will only work for the standard RAKP protocol, which uses standardized IPMI specifications. If you are using an OEM RAKP protocol, you will need to enable RAKP through the SMCIPMITool using the command `oem_rakp`.

2.11.3 UID Control

This feature allows the user to turn on or turn off the UID (Unit Identification) LED. When you turn on the UID, the blue UID LED at the front of the system or node chassis will light up.



1. To enter the screen shown above, click on the "UID Control" item in the *Miscellaneous* sidebar.
2. Click the *TURN ON* radio button to turn on UID control. Alternatively, click the *TURN OFF* radio button to turn off UID control.
3. Click *Save* to save the new setting.

Notes

Chapter 3

Frequently Asked Questions

3.1 Frequently Asked Questions

Q1. How do I flash the IPMI firmware?

Answer:

Method #1

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.

Method #2

- You can flash the IPMI firmware using flash tools located at [ftp://ftp.supermicro.com/utility/IPMI FW flash tools/](ftp://ftp.supermicro.com/utility/IPMI_FW_flash_tools/).
- For the latest IPMI Firmware, please refer to <http://www.supermicro.com/support/bios/firmware0/asp>.

Q2. 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)

Q3. When I update IPMI firmware through web, I got a file download pop-up,

but the firmware was not updated. Why?

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

Q4. My system seems to function properly; however, the IPMI event log indicates that my voltage and temperatures are beyond the limits. Why?

Answer: This is not a normal condition. Make sure that there is no other device accessing the I²C bus. If another device accesses the I²C bus frequently, that might cause a collision with the BMC when more than one device tries to access the I²C bus simultaneously. 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 the Aten Flash Tools. The Aten Flash Tools utility supports firmware updates and firmware dumping.

1. Firmware Updates

The Aten Flash Tools utility provides a complete solution for firmware updates. The user 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.

2. Firmware Dumping

In addition to firmware updating, Aten Flash Tools also support 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. Firmware dumping is supported by DOS, Windows, and Linux.

Section A.3 covers X9 Aten flash tools. Section A.4 covers X10 Aten flash tools.

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.3.1 Using X9 Aten Flash Tools in the DOS Environment

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

1. Enter `update.exe` and press <Enter>.
2. The information about the utility will be displayed. Follow the instructions given on the screen to configure the settings as shown in Figure 1.


```

*****
* ATEN Technology, Inc.
*****
* FUNCTION   : IPMI FIRMWARE UPDATE UTILITY
* VERSION   : 1.15
* BUILD DATE : Jan 06 2010
* USAGE     :
*             (1)Update FIRMWARE : dUpdate.exe -f filename.bin [OPTION]
*             (2)Dump FIRMWARE  : dUpdate.exe -d filename
*****
* OPTION
* -r Preserve Configuration(default is Preserve)
* n:No Preserve, reset to factory default settings
* y:Preserve, keep all of the settings
*****

```

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 the Flash Tools utility allows the user to update or dump the firmware via the KCS channels.

Firmware Updating via KCS Channels

To update your firmware via KCS, 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.
3. **y/n:** Type `y` to keep all settings after the firmware is updated; otherwise, type `n` to reset all settings to factory default.

```

C:\GET>dupdate.exe -f hermon~1.bin -r y_
C:\GET>dupdate.exe -f hermon~1.bin

```

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

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

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 Figures 3, 4, and 5.

```

If the FW update fails,PLEASE TRY AGAIN
update part 0, the size is 0x6f0000 bytes
Transfer data .....164K bytes      3%

```

Figure 3: Transferring (Part 0)

```

If the FW update fails,PLEASE TRY AGAIN
update part 1, the size is 0x110000 bytes
Transfer data .....61K bytes      6%_

```

Figure 4: Transferring (Part 1)

```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....82K bytes          4%_
```

Figure 5: Transferring (Part 2)

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

```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....2304K bytes          100%

Programming Flash
Please wait...If the FW update fails. PLEASE WAIT 5 MINS AND REMOVE THE AC...
Update progress:2 %
```

Figure 6: Progress of Firmware Update

```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....2304K bytes          100%

Programming Flash
Please wait...If the FW update fails. PLEASE WAIT 5 MINS AND REMOVE THE AC...
Update progress:100 %
Update Complete,Please wait for BMC reboot, about 1 min
```

Figure 7: Updates Completed

Dumping Firmware from the BMC via KCS channels

The user can dump the firmware by typing `dupdate.exe -d [filename]`. The utility will dump the firmware into the file that the user has assigned in the previous command. In the example given in Figure 8, the utility will dump the firmware to `dump_img_`.

```
C:\GET>dupdate.exe -d dump_img_
```

Figure 8: Example of Firmware Dumping via KCS

There are two phases in firmware dumping.

- During Phase 1, the utility is waiting for the BMC to prepare the firmware for dumping. As soon as preparation is complete, the utility will enter Phase 2.
- In Phase 2, the utility gets the firmware from the BMC. The user can see the progress on the screen as shown in Figure 10.

```
*****
* ATEN Technology, Inc. *
*****
* FUNCTION   : IPMI FIRMWARE UPDATE UTILITY *
* VERSION   : 1.15 *
* BUILD DATE : Jan 06 2010 *
* USAGE     : *
*           : (1)Update FIRMWARE : dUpdate.exe -f filename.bin [OPTION] *
*           : (2)Dump FIRMWARE  : dUpdate.exe -d filename *
*****
* OPTION *
* -r Preserve Configuration(default is Preserve) *
* n:No Preserve, reset to factory default settings *
* y:Preserve, keep all of the settings *
*****
Phase1:Wait for BMC.....10%_
```

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

```

*****
* ATEEN Technology, Inc.
*****
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY
*
* VERSION : 1.15
* BUILD DATE : Jan 06 2010
* USAGE :
*
* (1)Update FIRMWARE : dUpdate.exe -f filename.bin [OPTION]
* (2)Dump FIRMWARE : dUpdate.exe -d filename
*****
* OPTION
*
* -r Preserve Configuration(default is Preserve)
* n:No Preserve, reset to factory default settings
* y:Preserve, Keep all of the settings
*****
Phase1:Wait for BMC.....100%
Phase2:Receive the flash data.....107K bytes 0%

```

Figure 10: Phase 2, Flash Tools Dumping the Firmware

A.3.2 Windows/Linux Version of X9 Flash Tools

In addition to DOS, Aten's Flash Tools utility supports the Windows and Linux platforms.

The Windows/Linux version of the 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.

The main screen of the Windows/Linux version displays information about the firmware and the instructions on how to use the utility as shown in Figure 11.

```

*****
* ATEEN Technology, Inc.
*****
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY
*
* VERSION : 1.15
* BUILD DATE : Jan 8 2010
* USAGE :
*
* (1)Update FIRMWARE : uUpdate.exe -f filename.bin [OPTION]
* (2)Dump FIRMWARE : uUpdate.exe -d filename
*****
* OPTION
*
* -i the IPMI channel, currently, kcs and lan are supported
* LAN channel specific arguments
* h remote BMC address and BMC's port, <default port is 623>
* -u IPMI user name
* -p IPMI password correlated to IPMI user name
* -r Preserve Configuration <default is Preserve>
* n:No Preserve, reset to factory default settings
* y:Preserve, keep all of the settings
*****
* EXAMPLE
*
* we like to upgrade firmware through KCS channel
* uUpdate.exe -f fw.bin -i kcs -r y
*
* we like to upgrade firmware through LAN channel with
* BMC IP address 10.11.12.13 port 623
* IPMI username is alice
* Password for alice is secret
* Preserve Configuration
* uUpdate.exe -f fw.bin -i lan -h 10.11.12.13 623 -u alice -p secret -r y
*****

```

Figure 11 Main Screen of Flash Tools (in the Windows/Linux Version)

In the Windows/Linux version of the Flash Tools utility, there are seven 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 five parameters.

3. **-h**: Type *-h* to enter the addresses of the remote BMC and the RMCP+ port. The 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 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.

To connect the IPMI via KCS, type `wUpdate.exe/Update -f [filename.bin] -l kcs -r y` as shown in Figure 12.

```
D:\>wUpdate.exe -f HERMONEUB_all.bin -i kcs -r y
D:\>wUpdate.exe -f HERMONEUB_all.bin -i kcs
```

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

```
D:\>wUpdate.exe -f HERMONEUB_all.bin -i lan 192.168.46.65 -u alice -p secret
D:\>wUpdate.exe -f HERMONEUB_all.bin -i lan -h 192.168.46.65 623 -u alice -p secret -r y
```

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

To connect the IPMI via LAN, type `wUpdate.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.

A.4 Using X10 Aten Flash Tools

This section provides instructions on how to use the X10 Aten flash tools in the DOS, Windows, and Linux environments. Except where noted, these instructions may apply to all three.

1. Enter one of the following utilities and press <Enter>. **(From here on out, we will refer to A[x]Update.exe. Replace that name with the name of the appropriate utility.)**
 - AUpdate.exe for Linux
 - AdUpdate.exe for DOS
 - AwUpdate.exe for Windows
2. The information about the utility will be displayed, as shown in Figure 1. Follow the instructions given on the screen to configure the settings.

```

*****
* ATEN Technology, Inc.
*****
* FUNCTION : IPMI FIRMWARE UPDATE UTILITY
* VERSION : 2.42
* BUILD DATE : Jul 26 2013
* USAGE :
(1)Update FIRMWARE : A\update.exe -f filename.bin [OPTION]
(2)Dump FIRMWARE : A\update.exe -d filename
(3)Restore CONFIG : A\update.exe -c -f filename.bin
(4)Backup CONFIG : A\update.exe -c -d filename.bin
*****
* OPTION
* -i the IPMI channel, currently, lan supported only
* LAN channel specific arguments
* -h remote BMC address and RMCP+ port. (default port is 623)
* -u IPMI user name
* -p IPMI password correlated to IPMI user name
* -r Preserve Configuration (default is Preserve)
* n:No Preserve, reset to factory default settings
* y:Preserve, keep all of the settings
* -c IPMI configuration backup/restore
* -f [restore.bin] Restore configurations
* -d [backup.bin] Backup configurations
*****
* EXAMPLE
* we like to upgrade firmware through LAN channel with
* - BMC IP address 10.11.12.13 port 623
* - IPMI username is usr
* - Password for alice is pud
* - Preserve Configuration
A\update.exe -f fw.bin -i lan -h 10.11.12.13 623 -u usr -p pud -r y
A\update.exe -d fwdump.bin -i lan -h 10.11.12.13 623 -u usr -p pud -r y
* we like to restore/backup IPMI config through LAN channel with
* - BMC IP address 10.11.12.13 port 623
* - IPMI username is usr
* - Password for alice is pud
* - Preserve Configuration
A\update.exe -c -f fw.bin -i lan -h 10.11.12.13 623 -u usr -p pud
A\update.exe -c -d fwdump.bin -i lan -h 10.11.12.13 623 -u usr -p pud
*****
C:\SMT_X10_169\windows>

```

Figure 1: X10 IPMI Firmware Update Utility

Firmware Updating via KCS Channels

To update your firmware via KCS, type `A[x]Update.exe -f [filename.bin] -r y`. After entering this command, a screen will display as shown in Figure 2. Make sure that the binary file and the update utility are in the same folder.

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.
3. **y/n:** Type `y` for the BMC to keep all settings after the firmware is updated; otherwise, type `n` to reset all settings to factory default.

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

```
C:\SMT_X10_169\windows>A\update.exe -f SMT_X10_169.bin
```

```
C:\SMT_X10_169\windows>A\update.exe -f SMT_X10_169.bin -r y
```

Figure 2: Examples of Firmware Updates with/without the Command to Preserve

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 Figures 3, 4, and 5.

```
If the FW update fails,PLEASE TRY AGAIN
update part 0, the size is 0x6f0000 bytes
Transfer data .....164K bytes      3%
```

Figure 3: Transferring (Part 0)

```
If the FW update fails,PLEASE TRY AGAIN
update part 1, the size is 0x110000 bytes
Transfer data .....61K bytes      6%_
```

Figure 4: Transferring (Part 1)

```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....82K bytes      4%_
```

Figure 5: Transferring (Part 2)

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

```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....2304K bytes      100%

Programming Flash
Please wait...If the FW update fails. PLEASE WAIT 5 MINS AND REMOVE THE AC...
Update progress:2 %
```

Figure 6: Progress of Firmware Update

```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000 bytes
Transfer data .....2304K bytes      100%

Programming Flash
Please wait...If the FW update fails. PLEASE WAIT 5 MINS AND REMOVE THE AC...
Update progress:100 %
Update Complete,Please wait for BMC reboot, about 1 min
```

Figure 7: Updates Completed

Dumping Firmware from the BMC via KCS channels

The user can dump the firmware by typing `A[x]update.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`.

```
C:\SMT_X10_169\windows>AvUpdate.exe -d 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.

Manage Configuration

To manage the configuration, type `-c`.

1. `-d`: Type `-d` to back up a configuration into a binary file.
2. `-f`: Type `-f` to restore a configuration from a saved binary file.

Updating the Firmware via LAN (Windows/Linux Only)

The Windows/Linux versions of the Aten flash tools utility also allows the user to update the firmware via LAN.

In the Windows/Linux version of the Flash Tools utility, there are seven 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 five parameters.
3. `-h`: Type `-h` to enter the addresses of the remote BMC and the RMCP+ port. The 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 the configuration settings you've entered. This feature is optional. (default: preserve configuration)
7. `y/n`: Type `y` for the BMC to keep all settings after updating the firmware; otherwise, type `n` to reset the settings to factory default.

To connect the IPMI via KCS, type `A[x]Update.exe -f [filename.bin] -l kcs -r y` as shown in Figure 9.

To connect the IPMI via LAN, type `A[x]Update.exe -f [filename.bin] -i lan -h 192.168.46.65 623 -u alice -p secret -r y` as shown in Figure 10.

```
C:\SMT_X10_169\windows>AwUpdate.exe -f SMT_X10_169.bin -i kcs
C:\SMT_X10_169\windows>AwUpdate.exe -f SMT_X10_169.bin -i kcs -r y
```

Figure 9: Example of KCS FW Updates with/without Preserving Configuration

```
C:\SMT_X10_169\windows>AwUpdate.exe -f SMT_X10_169.bin -i lan -h 192.168.46.65 623 -u alice -p secret
C:\SMT_X10_169\windows>AwUpdate.exe -f SMT_X10_169.bin -i lan -h 192.168.46.65 623 -u alice -p secret -r y
```

Figure 10: Example of LAN_FW_Updates with/without Preserving Configuration and RMCP+ Port

Notes

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, industry-standard protocols that allows IT professionals to simplify the task of managing multiple network systems in a data center. SMASH offers a simple, intuitive solution to manage heterogeneous servers in a web environment regardless of their differences in hardware, software, OS, or network configuration. SMASH 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. SMASH 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.

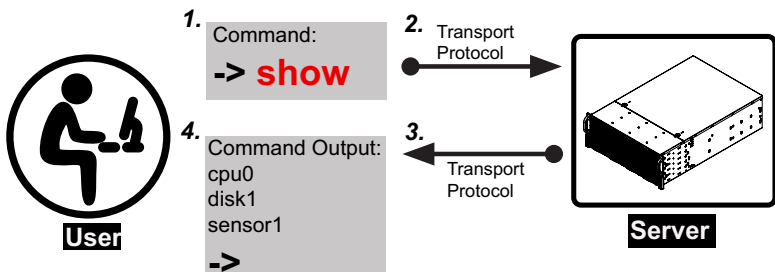


Figure 1 SMASH-CLP User Interface

SMASH Compliance Information

SMASH 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; it depends on the configuration of the system or the environment it operates in.

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

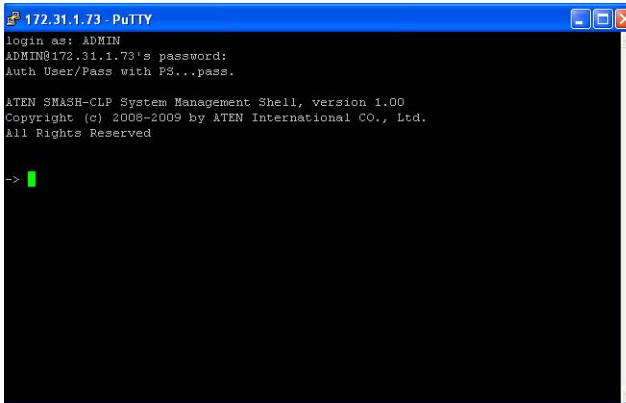
1. Use `ssh<BMC ip address>`.
2. Enter the password.

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 into the SSL network, the SMASH Command Line Protocol main screen will display as shown below.



```
172.31.1.73 - PuTTY
login as: ADMIN
ADMIN@172.31.1.73's password:
Auth User/Pass with PS...pass.

ATEN SMASH-CLP System Management Shell, version 1.00
Copyright (c) 2008-2009 by ATEN International CO., Ltd.
All Rights Reserved

-> █
```

Figure 2 SMASH-CLP Main Screen

B.6 Using SMASH for System Management

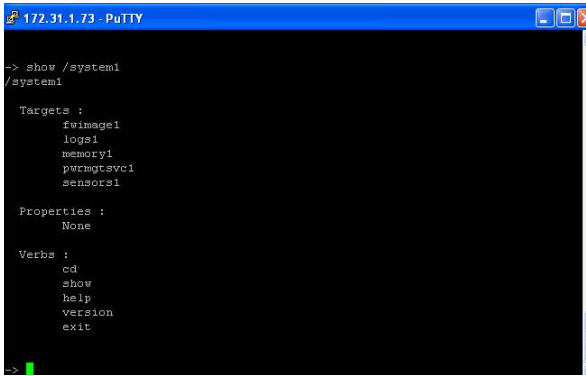
After you've familiarized yourself with the SMASH commands, you should be able to use these commands to manage your system. To properly manage your network system, be sure to follow the instructions below.



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 7: Definitions of Command Verbs.
- A **Target** is a managed device which is also referred to in the diagram of *Target Addressing* as shown in Figure 2.1.
- **Properties** are the specific attributes that you want to assign to a target machine or to get from a target machine.



```
172.31.1.73 - PuTTY
-> show /system1
/system1

Targets :
  Evinagle1
  logs1
  memory1
  permqtsvc1
  sensors1

Properties :
  None

Verbs :
  cd
  show
  help
  version
  exit
```

Figure 3 Using SMASH for System Management

B.7 Definitions of Command Verbs

Based on the DSP specifications, 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*, *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 contents of a target, a group of targets, or a subgroup 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, start a process, or change an operating state from a lower level to a higher level in a system.

- **stop**

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

- **reset**

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

- **delete**

The command verb *delete* is used to delete 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 the 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 provide the user with useful 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 and to go ahead and execute the command instead	None
-help	-h	Displays all information and documentation regarding the command verb	None
-keep <m[.s]>	-k	Sets a time period to hold and keep the Job ID and the status of a command	The amount of time set to hold a command Job ID or its status can differ.
-level <n>	-l	Instructs the Command Processor to execute the command for the current target and for all target machines within the level specified by the user	Levels should be expressed in a natural number or "all"
-Output <args>	-o	Controls the format and the content of a command output. This only supports "format=clpxml" and "format=keyword"	Many variables or factors can affect the outcome of format, language, level of detail of the output
-Source <URI>	None	Indicates the location of a source image or target	URI or SM Instance Address
-Version	-v	Displays the version of the command verb	None
-Wait	-w	Instructs the Command Processor to hold the command response or query result until all spawned jobs are completed.	None

Table 1 SMASH Commands

B.9 Standard Command Options

The following table lists the standard command options.

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

Table 2 Standard Command Options

B.10 Target Addressing

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

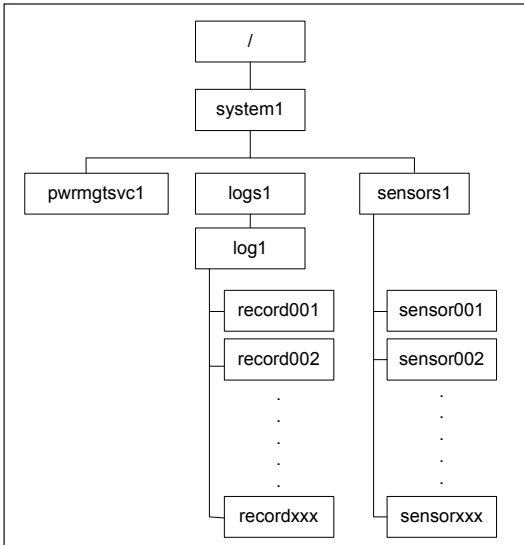


Figure 4 Target Addressing Diagram

Terms Used in the Target Addressing Diagram

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

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

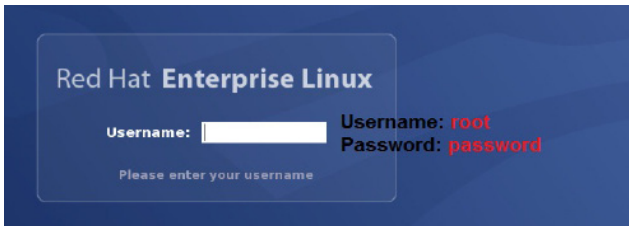
Notes

Appendix C

RADIUS Setup Guidelines

This chapter provides the RADIUS setup guidelines for IPMI firmware.

1. Start VM with RHEL4.7.VMX and boot into the OS.



2. Check the IP address of the RADIUS server.

```
[root@server postfix]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:D6:5E:27
          inet addr:192.168.10.154  Bcast:192.168.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed6:5e27/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:61045 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1708 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:5596983 (5.3 MiB)  TX bytes:151803 (148.2 KiB)
          Interrupt:193 Base address:0x2024

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2556 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2556 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:3202416 (3.0 MiB)  TX bytes:3202416 (3.0 MiB)

[root@server postfix]#
```

3. Configure User information.

vi /etc/raddb/users

```
# For ATEN "IPMI Web IKVM"
super    Auth-Type := Local, User-Password == "super"
         Vendor-Specific = "H=4, I=4",

randy    Auth-Type := Local, User-Password == "randy"
         Vendor-Specific = "H=4, I=4",

tester   Auth-Type := Local, User-Password == "tester"
         Vendor-Specific = "H=3, I=3"
```

- H=4, I=4 → Administrator (Super)
- H=3, I=3 → Operator (Randy)
- H=2, I=2 → User (Tester)
- H=1, I=1 → No Access

- Configure Client information.

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

```
# For "ATEN Web IKVM"
client 192.168.0.0/16 {
  secret = micro
  shortname = svc
}
```

- Configure Port information.

```
# vi /etc/raddb/radiusd.conf
```

```
# port: Allows you to bind FreeRADIUS to a specific port.
#
# The default port that most NAS boxes use is 1645, which is historical.
# RFC 2138 defines 1812 to be the new port. Many new servers and
# NAS boxes use 1812, which can create interoperability problems.
#
# The port is defined here to be 0 so that the server will pick up
# the machine's local configuration for the radius port, as defined
# in /etc/services.
#
# If you want to use the default RADIUS port as defined on your server,
# (usually through 'grep radius /etc/services') set this to 0 (zero).
#
# A port given on the command-line via '-p' over-rides this one.
#
# As of 1.0, you can also use the "listen" directive. See below for
# more information.
#
port = 1812
```

- Start RADIUS service.

```
[root@server postfix]#
[root@server postfix]#
[root@server postfix]# service radiusd start
Starting RADIUS server: [ OK ]
[root@server postfix]#
```

- Enable RADIUS in the IPMI web page.

RADIUS Settings

Check the box below to enable RADIUS and enter the required information!

Enable RADIUS

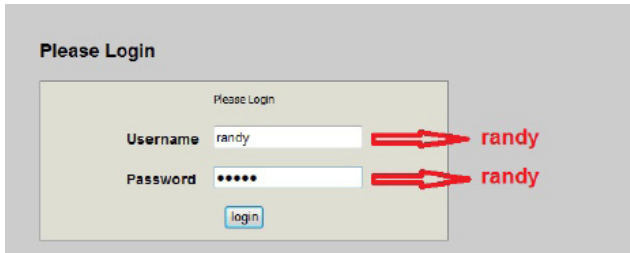
Port

IP Address

Secret


micro

8. Log out ADMIN, and log in using a RADIUS account.



The image shows a login form titled "Please Login". The form contains two input fields: "Username" and "Password". The "Username" field contains the text "randy". The "Password" field contains five dots. Below the password field is a "login" button. Two red arrows point from the text "randy" to the "Username" and "Password" fields, indicating that the password is also "randy".

Please Login

Please Login

Username

Password

randy

randy

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.