



Embedded BMC IPMI

USER'S Guide

Revision 1.0a

---

The information in this User's Manual 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, 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](http://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, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

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](http://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.

---

Appendix A and Appendix B included in this user's guide are used with permission from AMI. AMI is the legal owner of these documents. Supermicro has not verified the accuracy of the contents and assumes no responsibility with regard to any errors or omissions in these documents.

---

Manual Revision 1.0a

Release Date: April 16, 2009

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 © 2009 by Super Micro Computer, Inc.

All rights reserved.

**Printed in the United States of America**

## Preface

### About this User's Guide

This user guide is written for system integrators, PC technicians and knowledgeable PC users who intend to configure the IPMI settings supported by the Nuvoton WPCM450 BMC Controller embedded in Supermicro's motherboards. It provides detailed information on how to configure the IPMI settings provided by the Nuvoton WPCM450 chip.



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

### User's Guide Organization

**Chapter 1** provides an overview on the Nuvoton WPCM450 Controller chip. It also introduces the IPMI, its features and functionality.

**Chapter 2** provides detailed instructions on how to configure the IPMI settings supported by the embedded WPCM450 Controller.

**Chapter 3** provides the answers to frequently asked questions.

### Conventions Used in the User's Guide

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



**Warning:** Important information given to prevent erroneous RAID configuration and to ensure proper system setup.



**Note:** Additional Information given to ensure correct RAID 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](mailto:marketing@supermicro.com) (General Information)  
[support@supermicro.com](mailto:support@supermicro.com) (Technical Support)

Web Site: [www.supermicro.com](http://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](mailto:sales@supermicro.nl) (General Information)  
[support@supermicro.nl](mailto:support@supermicro.nl) (Technical Support)  
[rma@supermicro.nl](mailto:rma@supermicro.nl) (Customer Support)

### Asia-Pacific

Address: Super Micro Computer, Inc.  
4F, No. 232-1, Liancheng Rd.  
Chung-Ho 235, Taipei County  
Taiwan, R.O.C.

Tel: +886-(2) 8226-3990

Fax: +886-(2) 8226-3991

Web Site: [www.supermicro.com.tw](http://www.supermicro.com.tw)

Technical Support:

Email: [support@supermicro.com.tw](mailto:support@supermicro.com.tw)

Tel: 886-2-8228-1366, ext.132 or 139

## Notes

## Table of Contents

<b>Preface.....</b>	<b>3</b>
About this User's Guide .....	3
User's Guide Organization .....	3
Conventions Used in the User's Guide.....	3
Contacting Supermicro.....	4
<b>Chapter 1 Introduction.....</b>	<b>1</b>
1-1 An Overview of the Nuvoton WPCM 450 BMC Controller .....	1-1
WPCM450 DDR2 Memory Interface.....	1-1
WPCM450 PCI System Interface.....	1-1
Other Features Supported by the WPCM BMC Controller.....	1-1
1-2 WPCM450 Block Diagram .....	1-3
1-3 A Brief Introduction to the IPMI.....	1-3
1-4 An Important Note to the User.....	1-4
<b>Chapter 2 Configuring BMC the IPMI Settings.....</b>	<b>1</b>
2-1 Configuring the IP/MAC Addresses .....	2-1
Using the IPMICFG Utility to set the IP/MAC Addresses .....	2-1
Using the BIOS Settings to set the IP/MAC Addresses .....	2-2
Accessing the BMC.....	2-2
Using the Internet Browser .....	2-3
2-2 Using IE* to Access the BMC IPMI Settings from Your Computer.....	2-4
2.2.1 To Log In .....	2-4
2.2.2 The IPMI Main Page .....	2-5
2.3 Server Health .....	2-7
2.4 Configuration .....	2-12
2.5 Remote Control - the Main Menu .....	2-23
2.6 Maintenance.....	2-37
2.7 Miscellaneous .....	2-39
2.8 Language .....	2-40
<b>Chapter 3 Frequently Asked Questions.....</b>	<b>1</b>
3-1 Frequently Asked Questions .....	3-1
<b>Appendix A AMI Flash Tools Usage Guide.....</b>	<b>1</b>
<b>Appendix B AMI VMCLI Usage Guide .....</b>	<b>1</b>

# Chapter 1

## Introduction

### 1-1 An Overview of the Nuvoton WPCM450 BMC Controller

The Nuvoton WPCM450 Controller, a Baseboard Management Controller (BMC), supports the 2D/VGA-compatible Graphics Core with support of PCI interface, multi-media virtualization, and Keyboard/Video/Mouse Redirection (KVMR) modules. The WPCM450 Controller is ideal for server management platforms.

The WPCM450 interfaces with the host system via a PCI interface to communicate with the Graphics core. It supports USB 2.0 and 1.1 for remote keyboard/mouse/virtual media emulation. It also provides LPC interface to control Super IO functions. The WPCM450 is connected to the network via an external Ethernet PHY module or shared NCSI connections.

The WPCM450 communicates with onboard components via six SMBus interfaces, Platform Environment Control Interface (PECI) buses, and General Purpose I/O ports.

#### WPCM450 DDR2 Memory Interface

The WPCM450 supports a 16-bit DDR2 memory module with a speed of up to 220 MHz. The motherboard supports 128 MB memory that is shared between the BMC and onboard graphics card. For best signal integrity, the WPCM450 provides point-to-point connection.

#### WPCM450 PCI System Interface

The WPCM450 provides 32-bit, 33 MHz 3.3V PCI interface, which is compliant with the PCI Local Bus Specification Rev. 2.3. The PCI system interface connects to the onboard PCI Bridge and is used by the graphics controller.

#### Other Features Supported by the WPCM BMC Controller

The WPCM450 supports the following features:

- IPMI 2.0
- Serial over LAN
- KVM over LAN

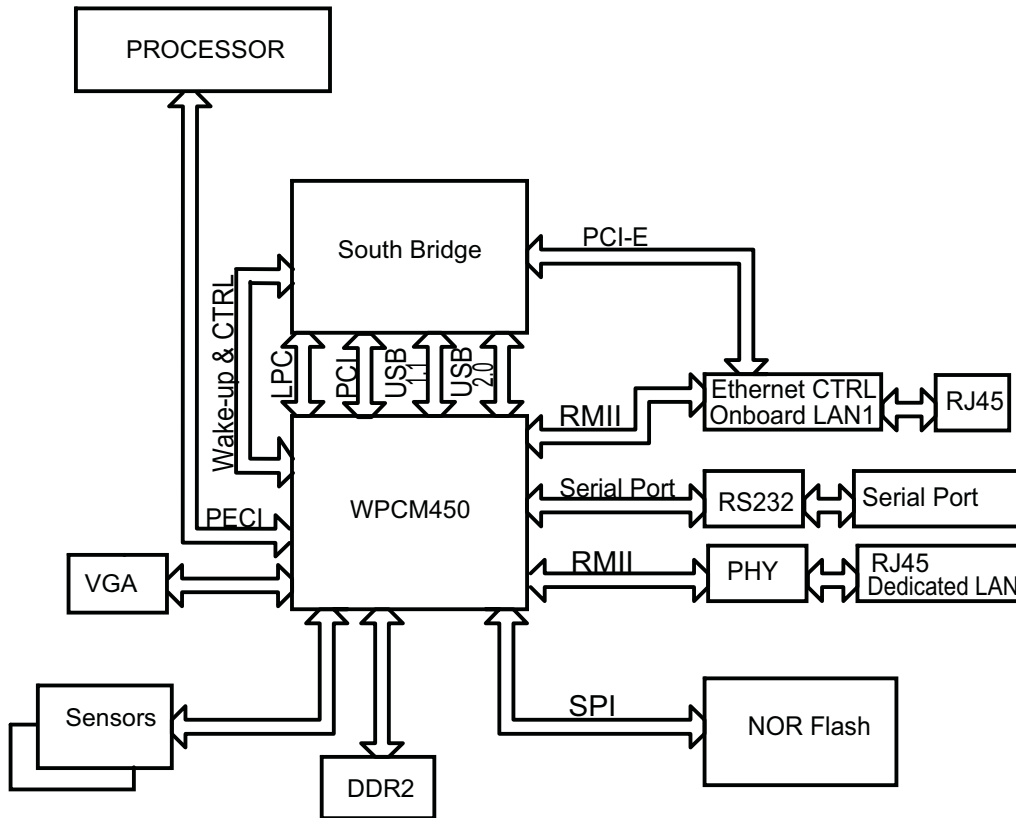
- LAN Alerting-SNMP Trap
- Event Log
- X-Bus parallel interface for I/O expansion
- Multiple ADC inputs, Analog and Digital Video outputs
- Two serial ports (optional)
- DDR2 SDRAM memory for frame-buffer, firmware support and data storage
- SPI Flash Host BIOS and firmware bootstrap program supported
- Reduced Media Independent Interface (RMII)
- OS (Operating System) Independency
- Provides remote Hardware Health Monitoring via IPMI. Key features include the following:
  - Temperature monitoring
  - Fan speed monitoring
  - Voltage monitoring
  - Power status monitoring, chassis intrusion monitoring
  - Remote power control to power-on, power-off or reboot a system
  - Remote access to text-based, graphic-based system information, including BIOS configurations and OS operation information (KVM)
  - Remote management of utility/software applications
- Provides Network Management Security via remote access/console redirection. Key features include:
  - User authentication enhancement
  - Encryption support enhancement, allowing for password configuration security to protect sensitive data transferring via Serial over LAN
- Supports the following Management tools: IPMIView, CLI (Command Line Interface)
- RMCP+ protocol supported



## 1-2 WPCM450 Block Diagram

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

## 1-3 A Brief Introduction to the IPMI



The Intelligent Platform Management Interface (IPMI) Specification defines a set of common interfaces to a computer system that provides remote access to multiple users from different locations for networking. It also allows a system administrator to monitor system health and to manage the computer events remotely.

IPMI operates independently of the operating system. When used in conjunction with the IPMIView, an IPMI-compliant management application software loaded into a PC, the WPCM450 BMC Controller, embedded onto a server board, provides serial link connections between the South Bridge and other onboard system components, allowing for network interfacing via remote access. With WPCM450 Controller and the IPMIView software, the Supermicro motherboard allows an administrator to access, monitor, diagnose and manage a computer system from a remote site. It also provides remote access to multiple users from different locations for system maintenance and management.

## **1-4 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 BMC the IPMI Settings

With the Nuvoton WPCM450 BMC Controller chip built in, the Supermicro motherboard allows the user to access, monitor, manage and interface with systems in remote locations. The necessary utilities for accessing and configuring the IPMI settings are included on the bootable CDs that came with your motherboard. This section provides detailed information on how to configure the IPMI settings.

#### 2-1 Configuring the IP/MAC Addresses



**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 firmware.

#### Using the IPMICFG Utility to Set the IP/MAC Addresses

1. Run the ipmicfg utility from the bootable CD that came with your shipment.
2. Follow the instructions given in the Readme.txt file to configure Gateway IP/ Netmask IP addresses, to enable/disable DHCP and to configure other IPMI settings.

IPMICFG Version 1.10 (Build 080711) Copyright 2008 Super Micro Computer, Inc.  
Usage: IPMICFG Parameters (Example: IPMICFG -m 192.168.1.123)

-m	Shows IP and MAC
-m IP	Sets IP (format: ###.###.###.###)
-a MAC	Sets MAC (format: ##:##:##:##:##:##)
-k	Shows Subnet Mask
-k Mask	Sets Subnet Mask (format: ###.###.###.###)
-dhcp	Gets the DHCP status
-dhcp on	Enables the DHCP
-dhcp off	Disables the DHCP
-g	Shows Gateway IP
-g IP	Sets Gateway IP (format: ###.###.###.###)
-r	BMC color reset
-garp on	Enables the Gratuitous ARP
-garp off	Disables the Gratuitous ARP

-fd	Resets to the factory defaults
-ver	Gets the firmware revision
-vlan	Gets VLAN status
-vlan on (VLANtag)	Enables the VLAN and sets the VLAN tag (If VLAN tag is not given, it uses previously saved value.)
-vlan off	Disables the VLAN
-raw	Sends a RAW IPMI request and print the response. Format: NetFn LUN Cmd [Data1...Data]

## Using the BIOS Settings to set the IP/MAC Addresses

1. Go to the BIOS by pressing the <Del> key during system boot.
2. Select IPMI from the Advanced Menu.
3. Select LAN Configuration from the IPMI submenu.
4. Click on the item - IP Address Source. Select the option Static and hit <Enter>. The onboard BIOS will automatically set the IP Address, MAC Address, Gateway, and Subnet Mask.
5. Once the IP, MAC Addresses, Gateway and Subnet Mask are set, click on the item Update LAN Settings. Select Yes and hit <Enter> to update IPMI LAN settings.
6. Go to the Exit menu. Select Save Changes & Exit and hit <Enter> to save changes and exit the BIOS.

## Accessing the BMC

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 System Name, IP Address of LAN1 or the dedicated LAN, 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 Internet Browser

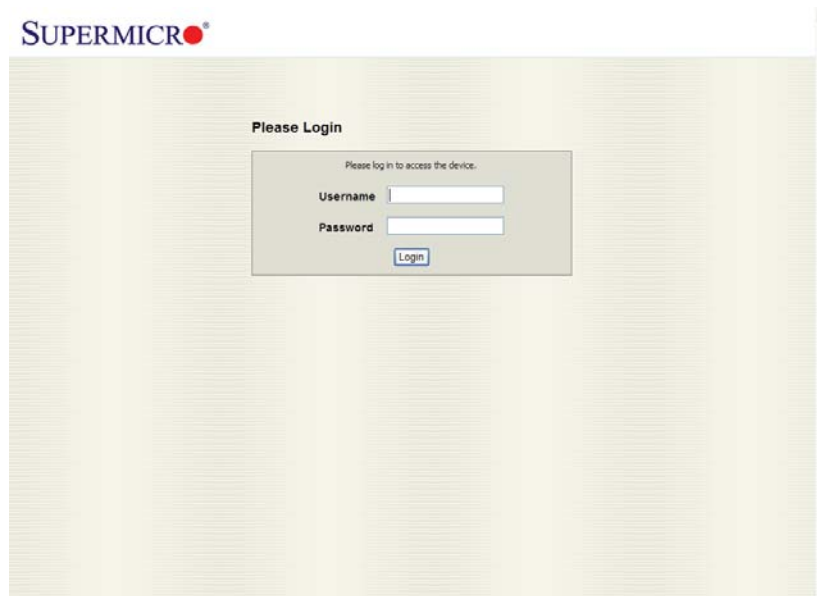
1. Connect a LAN cable to the onboard LAN1 port or the dedicated IPMI LAN port.
2. Choose a computer that is connected to the same network and open the browser.
3. Enter the IP address of each server that you want to connect to in the address bar in your browser.
4. Once the connection is made, the Log-In screen as shown on the next page will display.

### Notes:

1. If you wish to use the IPMI-dedicated LAN port for your network connections, be sure to connect an RJ45 cable to your dedicated LAN port before you activate the BMC (at first power-on or cold reset). Otherwise, the BMC will look for a shared LAN port to connect to if the IPMI-dedicated LAN cable is not detected upon BMC activation.
2. However, should you decide to use the IPMI-dedicated LAN port for a network connection, please perform a BMC cold reset or power cycle reset in order for the dedicated LAN to be detected.


## 2-2 Using IE\* to Access the BMC IPMI Settings from Your Computer

### 2.2.1 To Log In



Once you are connected to the remote server, the following screen will display.

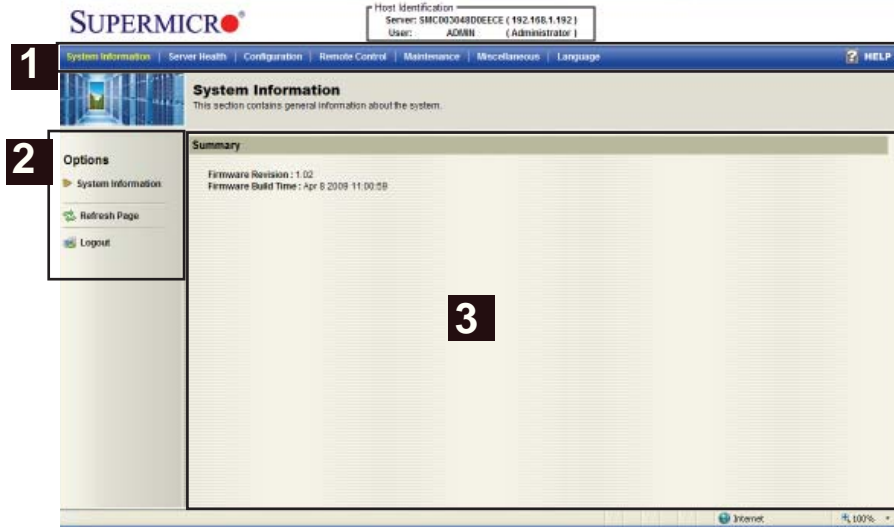
1. Enter your Username in the "Username" box.
2. Enter your Password in the "Password" box and click "Login."
3. The Home Page will display as follows.

 **Note 1:** To use the IPMIView Utility to access the BMC IPMI settings, please refer to the IPMIView User's Guide for instructions.

**Note 2:** The manufacturer default username and password are ADMIN. Once you have logged into the BMC using the manufacturer default password, be sure to change your password for security purpose.

## 2.2.2 The IPMI Main Page

Once you are logged in the IPMI utility, the IPMI Main page will display.



The IPMI Main page contains a submenu bar (Top), the Options window (Left), and the main display area (Right).

### 1. Submenu Bar (Marked 1 on the top)

The submenu bar on the top lists the following submenus:

Submenu Bar #1 (Top)	
<b>System Information</b>	This submenu displays system information.
<b>Server Health</b>	This submenu displays server health monitoring status.
<b>Configuration</b>	This submenu allows the user to configure the IPMI settings.
<b>Remote Control</b>	This submenu allows the user to launch KVM Console and perform power control & Management.
<b>Maintenance</b>	This submenu allows the user to update firmware and reset the unit.
<b>Miscellaneous</b>	This submenu allows the user to post snooping codes and to launch the SOL console.
<b>Language</b>	This submenu allows the user to select a language setting. (Currently, only English is available.)
<b>? Help</b>	Click this item to find an answer when you have a question.

## **2. Options window (#2)**

The Options window on the left side allows the user to navigate through different options, including the following:

<b>Options window #2 (Left)</b>	
<b>Refresh Page</b>	Click this icon to refresh the page.
<b>Logout</b>	Click this icon to logout from the IPMI utility.

## **3. The Main Display Area (#3)**

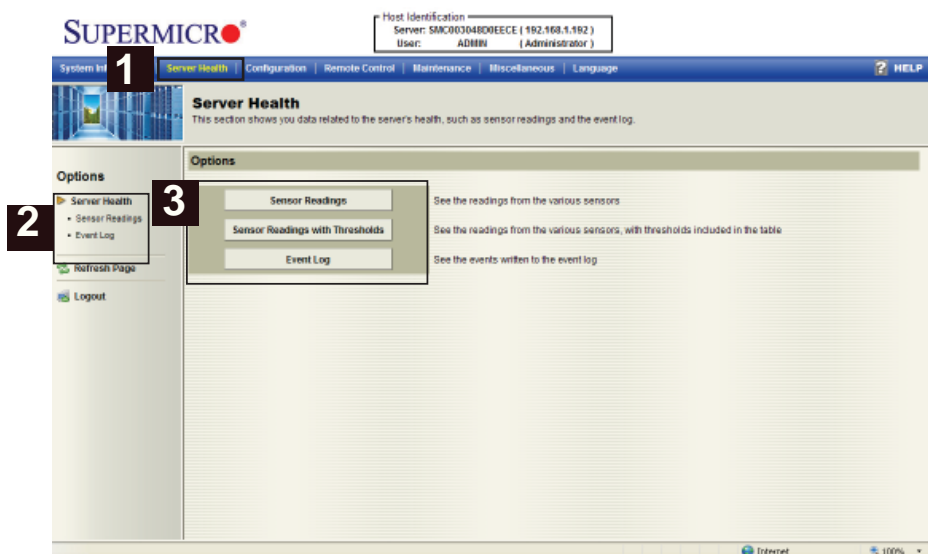
This area displays the items included in a submenu. The items included on the Main page are as follows.

<b>Main Display Area #3 (Right)</b>	
<b>Device Power Status</b>	This item displays the status of the device: On or Off.
<b>Firmware Revision</b>	This item displays the firmware revision#.
<b>Firmware Built Time</b>	This item displays time and date when the firmware was built.



## 2.3 Server Health

This feature allows the user to set Server Health Settings. When you click on the Server Health icon (#1) on the submenu bar, the following screen will display:



The Server Health submenu (#1) contains Sensor Readings, Sensor Readings with Thresholds, and Event Log. When clicking an item in the Options window on the left (#2), or on the Main Display area (#3), a pop-up menu will appear to display the category of sensor types (#4).



### ***2.3.1. The Categories of Sensor Types (#4)***

The Sensor Type Category includes the following:

- **All Sensors:** This item displays the readings for all sensors
- **Temperature Sensors:** This item displays the system temperature.
- **Voltage Sensors:** This item displays the following items: CPU voltage, CPU Core, voltage, DIMM (memory) voltage, +3.3v, +12v, +5V, -12v.
- **Fan Sensors:** This item displays the status of onboard fans.
- **Physical Security/(Chassis Intrusion):** This item displays the status of chassis intrusion.
- **Power Supply:**
  - **(PS Status OK):** This item displays Power Supply Failure status.
  - **OEM Reserved:** This item reserved for OEM use.

### ***2. Refresh (#5)***

Click on this bottom to refresh this page.

### ***3. Show Thresholds (#6)***

Click on this bottom to display the thresholds of selected sensor- reading items.

### ***4. Intrusion Reset (#7)***

Click on this bottom to reset the chassis intrusion settings.



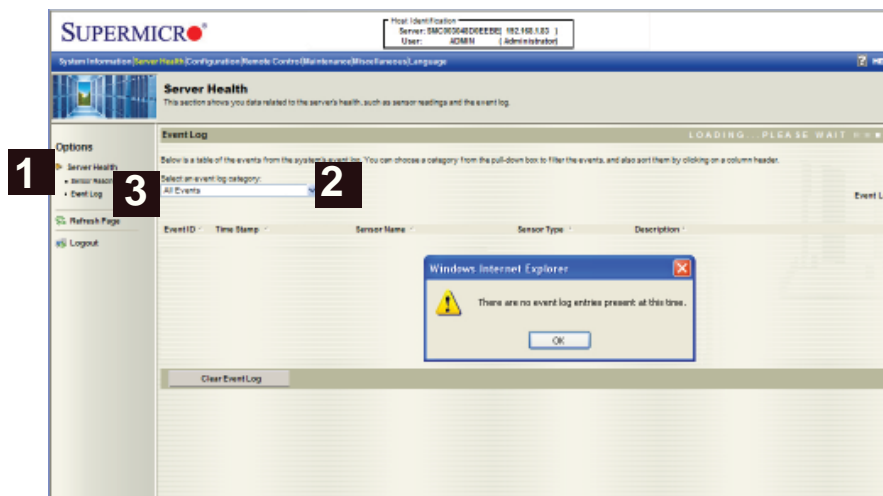
### 2.3.1 Sensor Readings Display-All Sensors

When you select All Sensors (#1) from the Sensor Type Category pop-up submenu, the sensor readings for the following items will be displayed as shown below:

- **CPU Temperature:** This item displays the status of the CPU temperature.
- **System Temperature:** This item displays the status of the system temperature.
- **CPU Vcore:** This item displays the status of the CPU core voltage.
- **+12V:** This item displays the status of the +12V power supply .
- **+3.3V:** This item displays the status of the onboard 3.3V power supply.
- **DIMM :** This item displays the status of DIMM modules.
- **+5V:** This item displays the status of the onboard +5V power supply.
- **-12V:** This item displays the status of the onboard -12V power supply.
- **+3VSB:** This item displays the status of the onboard +3.3VSB power supply.
- **-12V:** This item displays the status of the onboard -12V power supply.
- **Fan1~Fan5:** This item displays the status and the RPM reading of each on-board fan.
- **(Chassis) Intrusion:** This item displays the status of chassis intrusion to indicate the security setting of the system.
- **PS Failure:** This item indicates whether a power failure has occurred.

### 2.3.2. Event Log

This feature allows the user to configure Event Log settings. When you select Event Log (1) in Options Window and click on the item Event Log Category (2), the following event log categories will display in a pull-down submenu (3) as shown in the screen below.

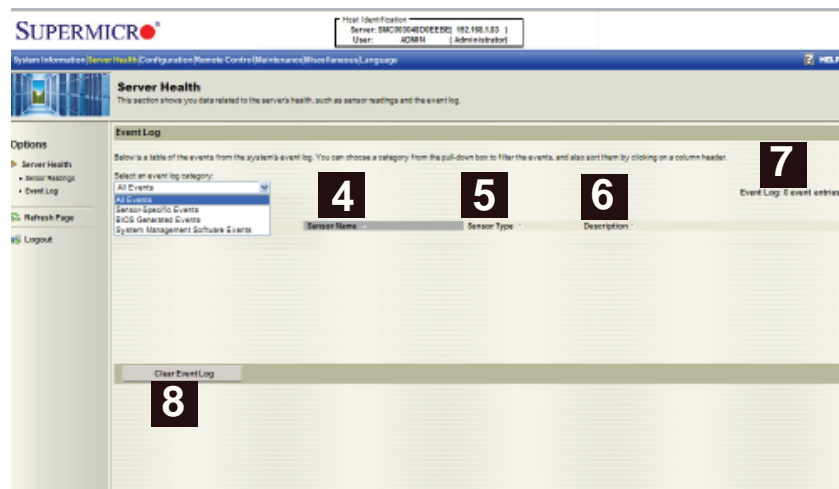


**Sensor-Specific Events:** This item displays the event log for sensor-specific events.

**BIOS-Generated Events:** This item displays the event log for BIOS-generated events.

**System Management Software Events:** This item displays the event log for system management software events.

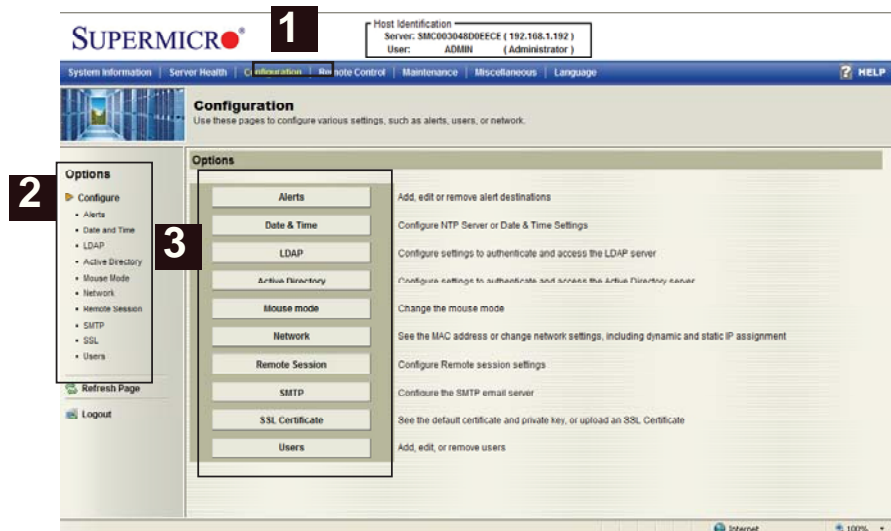
After you have selected an event log category, a screen will appear to show the status of the event log as shown below.



- 4. Sensor Name:** This item indicates the name of the sensor (device) to which the event occurred.
- 5. Sensor Type:** This item indicates the type of the event.
- 6. Description:** This item provides a brief description of the event.
- 7. Event Log:** This item indicates the number of events included on the event log.
- 8. Clear Event Log:** Click the button to clear the event log.

## 2.4 Configuration

This feature allows the user to configure various network settings. When you click on the Configuration icon (#1) on the submenu bar, the following screen will display:



The Configuration submenu includes the items shown in the Options window on the left (2) or in the Main Display area on the right (3).

Select an item on the list to configure the settings for the item selected.

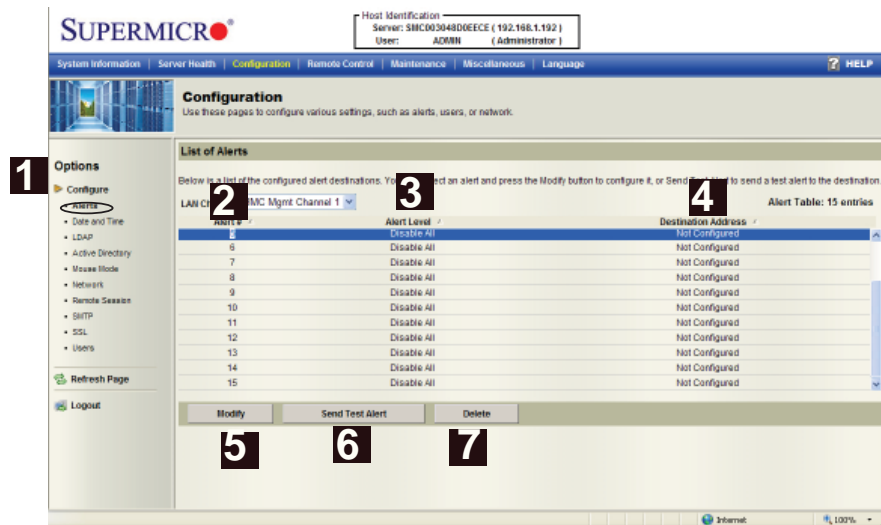
- Alert
- Date & Time
- LDAP
- Active Directory
- Mouse mode
- Network
- Remote Session
- SMTP
- SSL Certificate
- Users



**Note:** To set up an email alert, please enter the IP address of your mail server in the SMTP (Simple Mail Transfer Protocol.)

### 2.4.1 Configuration - Alerts

This feature allows the user to configure Alert settings. When you click on the Alerts icon in the Options window (1), the following screen will display.



**1. Alerts:** Click this item to add, to modify, to delete or to define the setting of an alert.

**2. Alert#:** This item lists Alert item numbers.

**3. Alert Level:** This item indicates the alert level for each alert.

**4. Destination Address:** This item indicates the target address of an alert.

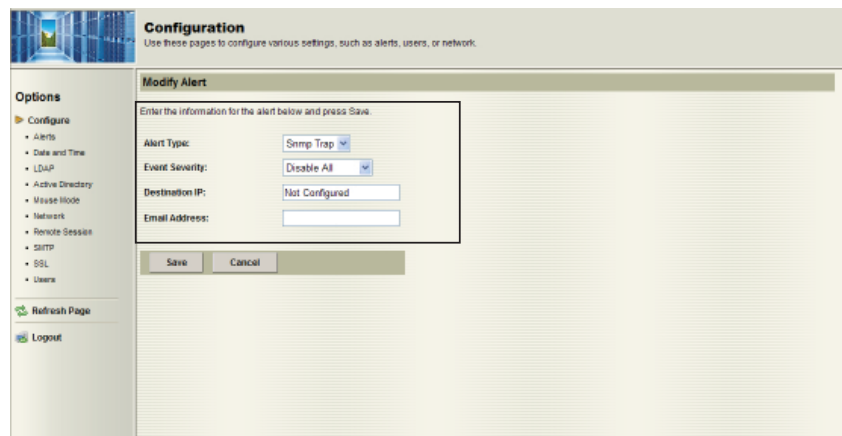
**5. Modify:** Click on the Modify icon to configure or modify a selected alert.

**6. Send Test Alert:** Click on this icon to send a configured alert to its destination (the target address) for testing.

**7. Delete:** Click on this icon to delete an alert.

#### Modifying Alerts

When you select an item (2) and click on Modify (5), the Modify Alert submenu will display as shown below.



To modify an alert, enter the information needed for the following items:

- **Alert Type:** This item allows you to specify the alert type. You can select Snmp Type or Email from the pop-up menu.
- **Event Severity:** This item allows you to decide how to classify or label an alert according to the seriousness of the alert. You can choose an item from the pop-up menu to categorize the alert: Disable All, Informational, Warning, Critical or Non-recoverable.
- **Destination IP:** This item allows you to specify the IP address of the server that you want to send your alert to.
- **Email Address:** This item allows you to specify the e-mail address that you want to send your alert to.

After entering the information in the fields, press <Save> to save the information you've entered or press <Cancel> to cancel it.



**Note:** To set up an email alert, please enter the IP address of your mail server in the SMTP (Simple Mail Transfer Protocol.)



### 2.4.2 Configuration - Time and Date Settings

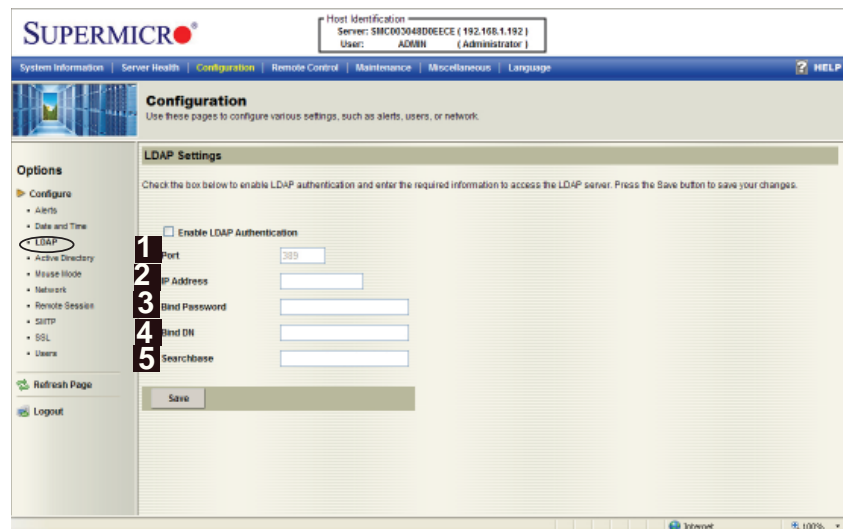
This feature allows the user to configure time and date settings for the host server and client computer. When you click on the Time and Date icon in the Options window (1), the following screen will display.



1. **Time and Date:** Click on this item to configure the Time and Date settings.
2. **Date:** Enter month, date and year in this row.
3. **Time:** Enter hour, minute and second in the (*hh:mm:ss*) format.
4. **NTP Server:** Enter the name of the NTP server in this field.
5. **Enabling Synchronizing:** Check this box to enable synchronization of time and date of the client computer with the NTP server.
6. **Refresh:** Click this button to refresh the page.
7. **Save:** Click on this icon to save any changes done to the Time and Date settings.

### 2.4.3 Configuration - Light-Weight Directory Access Protocol (LDAP) Settings

This feature allows the user to configure Light-Weight Directory Access Protocol (LDAP) settings. When you click on the LDAP icon in the Options window (1), the following screen will display.



Examples and Explanations of the LDAP settings are shown below:

1. **Port: 389**-This item indicates the LDAP server port number.
2. **IP Address: xx.xx.xx.xx**- This item indicates the LDAP server IP address
3. **Bind Password: Secret**- This item indicates the LDAP server password
4. **Bind DN: cn=manager, dc=administrator, dc=com**-The bind DN is the user or the LDAP server that is permitted to do search in the LDAP directory within a defined search base.
5. **SearchBase: dc=administrator, dc=com**-The research base shows the client which port in the external directory tree to search.

After entering the information in the fields, click Save to save the information you've just entered.

### 2.4.4 Configuration - Active Directory Settings

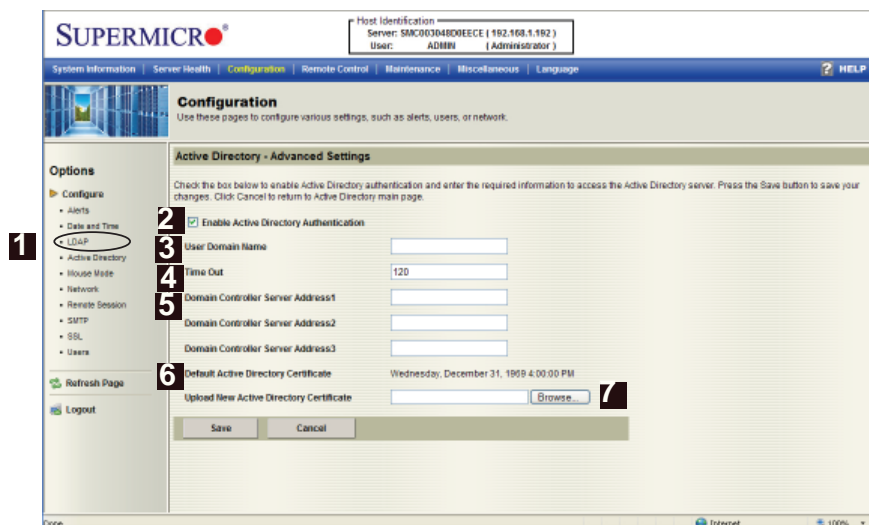
This feature allows the user to configure Active Directory settings. When you click on the Active Directory icon in the Options window (1), the following screen will display.



1. **Active Directory:** Click on this item to configure Active Directory settings.
2. If Active Directory is currently disabled, click <Here> to enable it.
3. **Number of Configured Role Group:** This item displays the number of configured role groups.
4. **Role Group ID:** This item displays the role group ID.
5. **Group Name:** This item displays the name of the role group.
6. **Group Domain:** This item displays the domain of the role group.
7. **Group Privilege:** This item displays the user privilege of the role group.

### 2.4.4.a Configuration - Active Directory - Advanced Settings

This feature allows the user to configure Active Directory-Advanced settings. When you click on the Active Directory icon in the Options window (1) and checked the Enable box indicated on the previous page, the following screen will display.



**1. Active Directory:** Click on this item and check the Enable box on the previous page to configure Active Directory settings.

**2.** Check the Enable box to enable Active Directory Authentication.

**3. User Domain Name:** This item allows the user to enter the user domain name.

**4. Time Out:** This item displays the Time-out settings.

**5. Domain Controller Server Addresses 1~3:** These items allow the user to enter the IP addresses for the Domain Controller Servers 1~3.

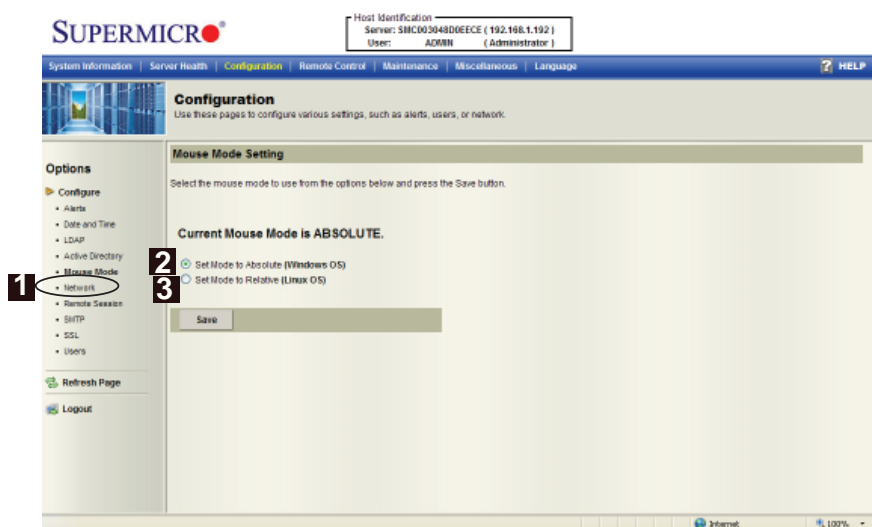
**6. Default Active Directory Certificate:** This item displays the information of the default active directory certificate.

**7. Upload New Default Active Directory Certificate:** Click <Browse> to select and upload the new default active directory certificate.

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

### 2.4.5 Configuration - The Mouse Mode Setting

This feature allows the user to configure mouse mode settings. When you click on the Mouse Mode icon in the Options window (1), the following screen will display.



1. **Mouse Mode:** Click on this icon to configure the mouse mode setting.
2. **Set Mode to Absolute:** Check the radio button to use the Absolute mode for the Windows OS. (This is the default setting.)
3. **Set Mode to Relative:** Check the radio button to use the Relative mode for the Linux/Unix OS.



**Note:** IPMI is an OS-independent platform, and KVM support is an added feature for IPMI. For your mouse to function properly, please configure the Mouse Mode settings (above) according to your OS type.

## 2.4.6 Configuration - Network Settings

This feature allows you to configure network settings. When you click on the Network icon in the Options window (1), the following screen will display.

**1. Network:** This item allows you to view or modify network settings.

**2. MAC Address:** Enter the MAC address for networking in the box.

Check the first radio button to obtain an IP address automatically by using DHCP (Dynamic Host Configuration Protocol).

Check the second radio button to use the IP address entered below.

**3. IP address:** If the second radio button above is checked, please enter your IP address in the box.

**4. Subnet Mask:** Enter the address for the subnet mask of your network.

**5. Default Gateway:** Enter the IP address for the default gateway of your network.

**6. Primary DNS Server:** Enter the IP address of your primary domain name server.

**7. Secondary DNS Server:** Enter the IP address of your secondary domain name server.

**8. Enable VLAN:** Check this box to enable Virtual LAN support

**9. VLAN Tag:** This item allows you to use VLAN Tagging or Frame Tagging to encapsulate specific data, so it can be transparently transmitted through multiple platforms without information leakage.

After entering the required information in the fields, click <Save> to save the information you have entered.

### 2.4.7 Configuration - Remote Session

This feature allows the user to configure remote session settings. When clicking on the Remote Session in the Options window (1), the following screen displays.



**2. Virtual Media Attach Mode:** Click the pull-down menu to display the following virtual media attach modes:

- **Attach:** Select this mode to activate a virtual media in order to make it available for remote access. A virtual device will always be seen in the system BIOS even when it is not active.
- **Auto Attach (Default):** Select this mode to automatically enable virtual media support and make it available for remote access. Virtual devices will only be shown in the operating systems and BIOS when a device or an ISO image is connected through the virtual media wizard.
- **Detach:** Select this mode to disable virtual media for remote access.

**3. Floppy Emulation:** Click the pull-down menu to see the following:

- **Off (Default):** Select this item to disable floppy emulation when you wish to connect the USB Flash drive via virtual media redirection.
- **On:** Select this item to enable floppy emulation when you wish to connect a floppy drive or floppy ISO image through virtual media redirection.



**Warning:** Be sure to close all Java sessions before changing floppy emulation to avoid unexpected errors.

## 2.4.8 Configuration - SMTP Settings

This feature allows the user to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network. When you click on the SMTP icon in the Options window (1), the following screen will display.



- 1. SMTP:** Check this item to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission across the IP network.
- 2. Mail Server IP:** Enter the SMTP Mail Server IP address for your network in the box.
- 3. Save:** Click on this icon to save any changes to the SMTP setting.



### 2.4.9 Configuration - SSL Upload Settings

This feature allows the user to configure upload settings for encrypted data to transmit across the internet by using the Secure Sockets Layer (SSL) protocol. When you click on the SSL Upload icon in the Options window (1), the following screen will display.



1. **SSL:** Check this item to configure SSL Upload settings for the encrypted data to securely transmit through the internet.
2. **Default Certificate:** This item allows the user to enter the default certificate information. Once entered, it will display the default certificate information.
3. **Default Private Key:** This item allows the user to enter the default private key information. Once entered, it will display the default private key information.
4. **New SSL Certificate:** This item allows the user to enter the new SSL Certificate information.
5. **Upload:** Click on this button to upload encrypted data to the network for transmission.

## 2.4.10 Configuration - Users Settings

This feature allows you to change users settings. When you click on the Users icon in the Options window (1), the following screen will display.



**1. Users:** Select this item to configure the user settings. The current users list is displayed. To delete or to modify a user setting, select the name and press <Delete User> or <Modify User>.

**2. UserID:** This item displays the ID# of a user.

**3. User Name:** Use this item to enter and display a user name.

**4. Network Privileges:** Use this item to set the network access privileges for a user.

- Privileges for an Administrator: An administrator has full power in accessing, controlling and managing the network, including creating accounts for users and changing network configuration settings.
- Privileges for an Operator: An operator has limited access to the network in order to perform tasks that have been pre-assigned or approved by the Administrator. He/she is not allowed to issue commands or modify network settings, for example.

**5. Number of configured users:** This item displays the number of the users that are set up for the network. The maximum of 16 user profiles can be made.

**6. Add User:** Click on this icon to add a new user to the network. When prompted, select an empty slot from the users list to add an user.

**7. Modify User:** Click on this icon to modify the information or the status of a user. When prompted, using the arrow keys, select a user from the users list to modify the user information.

**8. Delete User:** Click on this icon to delete a user from the network. When prompted, using the arrow keys, select a user from the users list to delete it from the list.

## 2.5 Remote Control - the Main Menu

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



The Remote Access Main Menu includes the following items:

1. **Remote Control:** Click on this icon to configure Remote Control settings.
2. **(Launch) Remote Console:** Click this button to launch Remote Console.
3. **(Launch) SOL:** Click this button to enable Serial\_Over\_LAN support.
4. **(Server) Power Control:** Click this button to display server power state and to configure server power settings.
5. **Refresh:** Click this button to refresh the page.
6. **LogOut:** Click this button to log out from the remote console.

## 2.5.1 Remote Console

This feature allows you to perform various activities on the server. When you click on the Remote Console icon in the Options window (1) to activate Remote Console settings, the following screen will display.

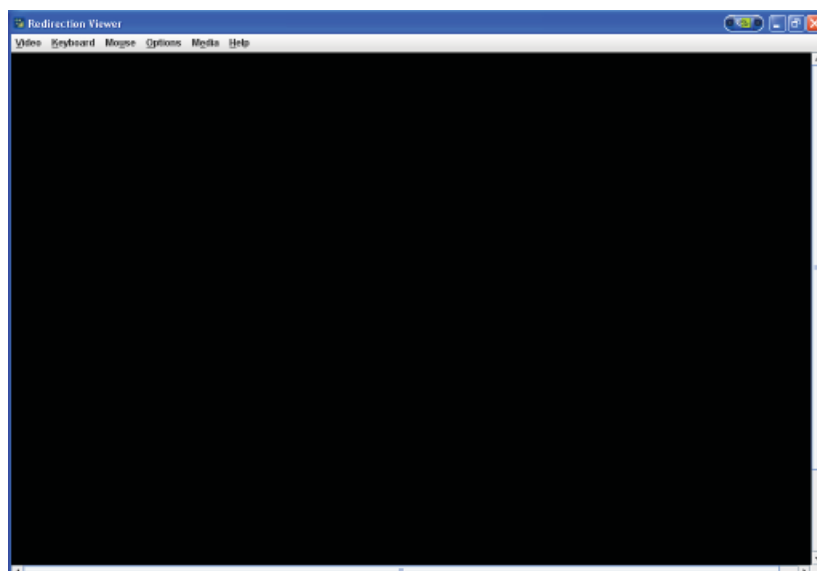


**1. Remote Console:** Check this item to enable the remote console and manage the server from a remote site via Java or ActiveX (for Internet Explorer).

**2. Launch Console:** Click this button to launch the remote console via the Java script.

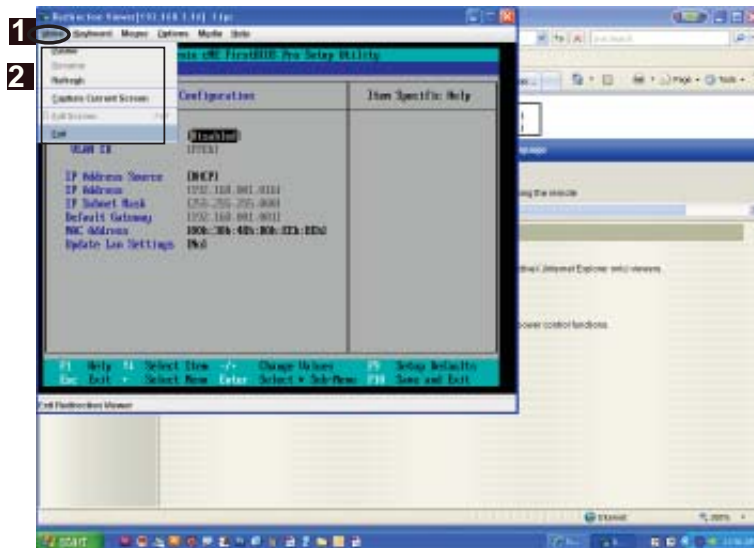
**3. Java Starting:** Upon launching the remote console, a screen displays, indicating that Java is starting.

Once the process is completed, a screen will display as shown below.



### 2.5.1.1 Remote Console - Video

This feature allows you to configure video settings for your remote console. When you click on the Video icon in the Menu bar (1), the video settings of the remote console will display as shown below.



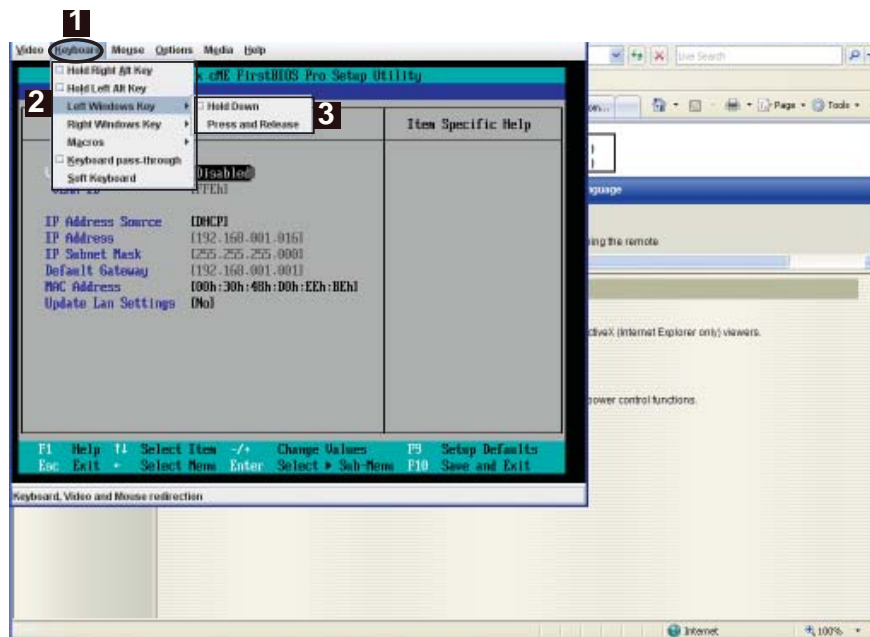
**1. Video:** Click this item to configure and manage the video settings of a server on a remote site via the Remote Console.

**2. Video Options:** The pull-down submenu contains the options listed below.

- **Pause:** Click this item to freeze the screen.
- **Resume:** Click this item to re-activate a frozen screen.
- **Refresh:** Click this item to refresh the system.
- **Capture Current Screen:** Click this item to capture the current screen display.
- **Full Screen:** Click this item to use the full screen mode.
- **Exit:** Click this item to exit the Remote Console.

### 2.5.1.2 Remote Console - Keyboard

This feature allows you to configure keyboard settings for your remote console. When you click on the Keyboard item in the Menu bar (1), the keyboard settings of the remote console will display as shown below.

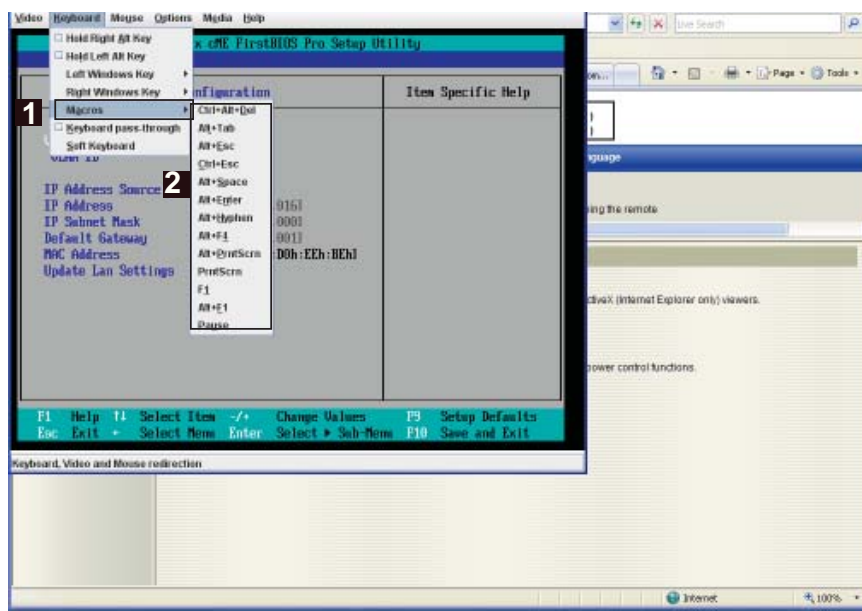


**1. Keyboard:** Click this item to configure and manage the keyboard settings of a server on a remote site via the Remote Console.

**2. Options:** The pull-down submenu contains the options listed below.

- **Hold Right Alt Key:** Check this item to emulate right alt key press.
- **Hold Left Alt Key:** Check this item to emulate left alt key press.
- **Left Window Key:** Click on this item to display the Left Window Key submenu as follows:
  - **3. Hold down:** Check this item to emulate left window key press.
  - **3. Press and Release:** Click on this option to press and release the left window key.
- **Right Window Key:** Click on this item to display the Right Window Key submenu as follows:
  - **3. Hold down:** Check this item to emulate right window key press.
  - **3. Press and Release:** Click on this option to press and release the right window key.

- **Macros:** Click this item (1) to display and to use the Macros hot keys listed in its pull-down submenu as shown in the screen below.

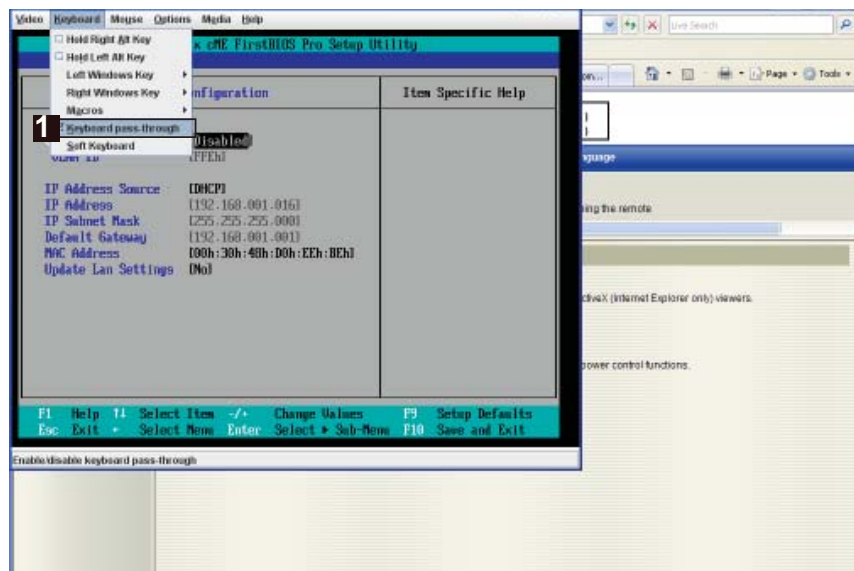


- Ctrl+Alt+Del
- Alt+Tab
- Alt+Esc
- Ctrl+Esc
- Alt+Space
- Alt+Enter
- Alt+Hyphen
- Alt+F4
- Alt+PrintScrn (Print Screen)
- PrintScrn
- F1
- Pause

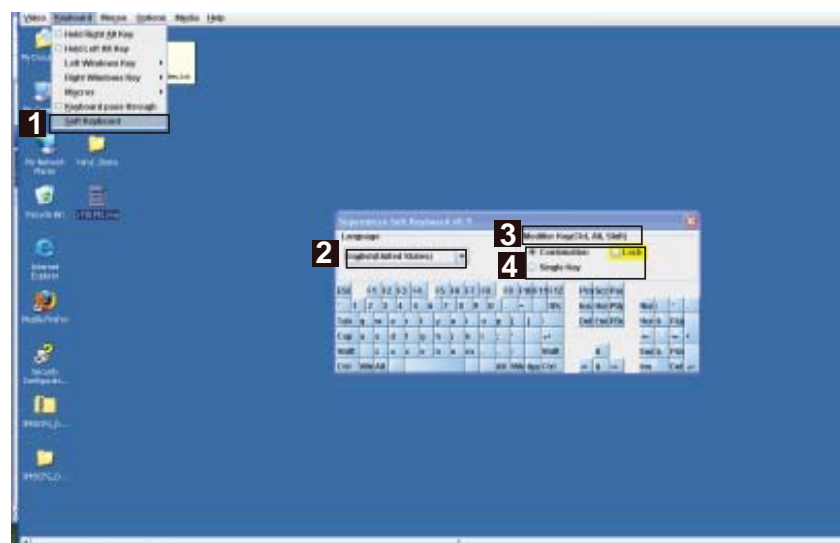
- **Keyboard pass-through:** Click this item (1) to use your local keyboard for the remote console.



**Note:** This feature-"Keyboard Pass-through" provides full keyboard support. It will send all keys, including special key combinations to the host server.



1. **Soft Keyboard:** Select the item Soft Keyboard (1) to use soft keyboard for the remote console as shown below.

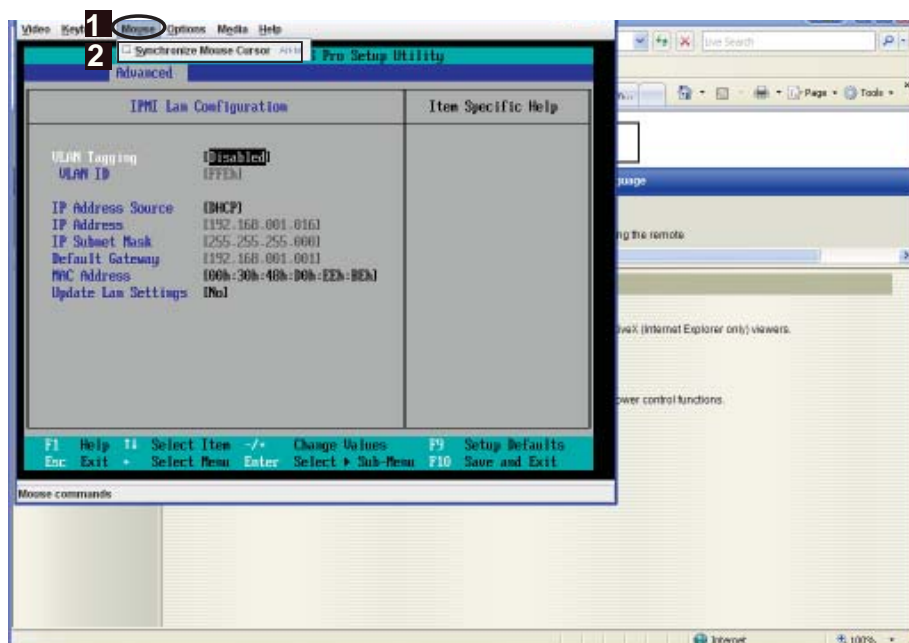


2. **Language:** From the pull down menu, select the following language settings: English (United States), English (United Kingdom), Japanese, and Germany.
3. **Modifier Key (CTRL, Alt, Shift)** - Select the keys: <Ctrl>, <Alt>, and <Shift> to work as a special key combination or as a single key. Check the box in front of "Lock" to lock the key combination.



### 2.5.1.3 Remote Console - Mouse

This feature allows you to configure the mouse settings for your remote console. When you click on Mouse in the Menu bar (1), the Mouse settings of the remote console will display as shown below.

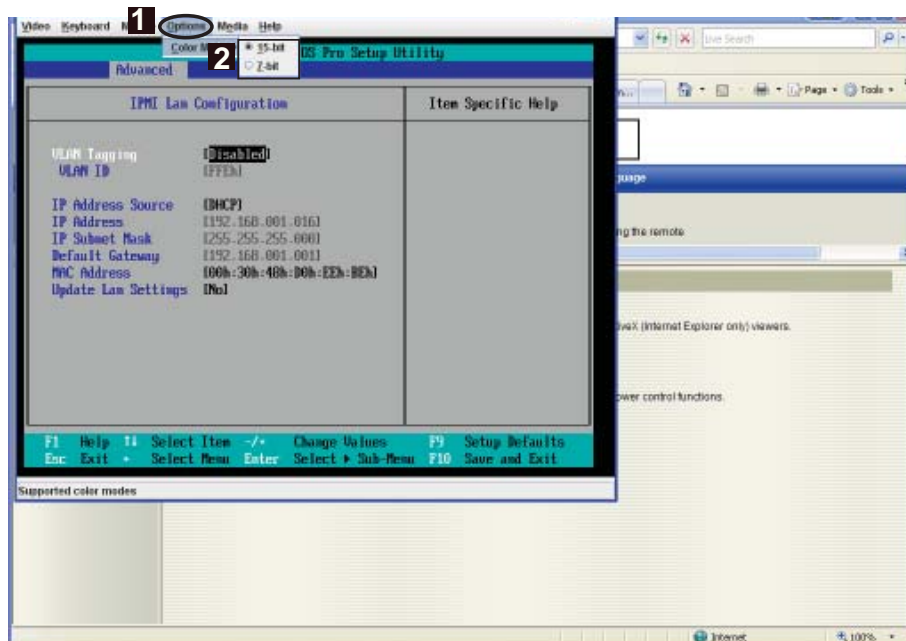


The pull-down submenu contains the option listed below.

**Synchronize Mouse Cursor** Alt+M (2): Click this item (or press <Alt> and <M> keys simultaneously) to synchronize your local mouse cursor and the mouse cursor of your remote console.

### 2.5.1.4 Remote Console - Options

This feature allows you configure color modes for your remote console. When you click on Options in the Menu bar (1), the (Color mode) Options settings of the remote console will display as shown below.



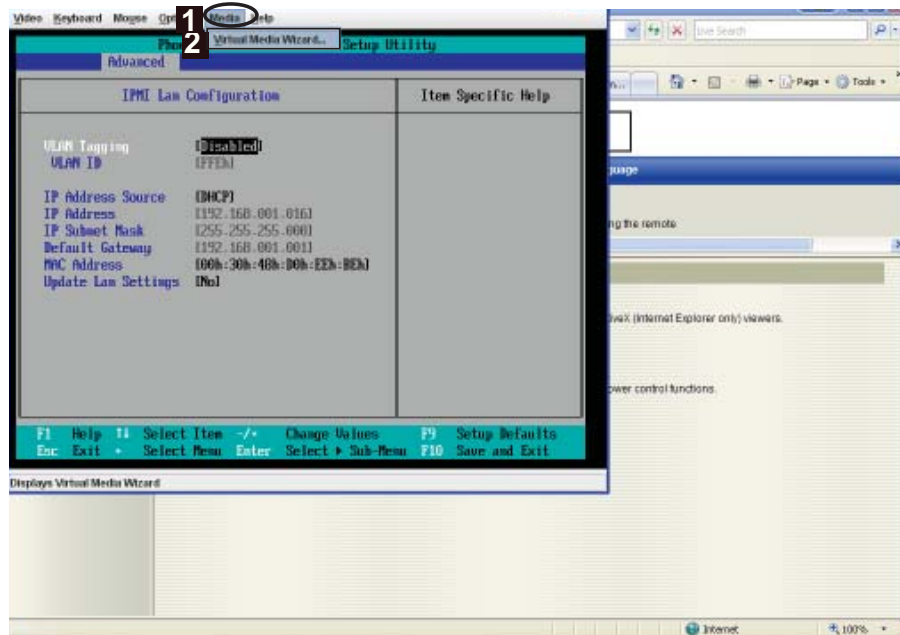
The pull-down submenu displays the option listed below.

**Color Mode (2):** Click this item to choose the color mode of your remote console from the pull-down submenu:

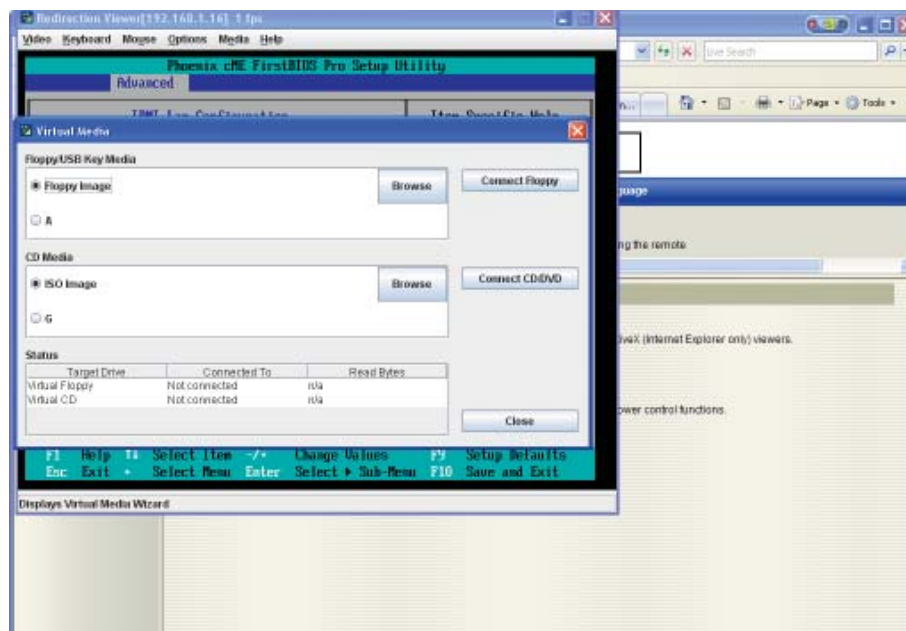
- 15-bit
- 7-bit

### 2.5.1.5 Remote Console - Media

This feature allows you to configure media virtualization settings for your remote console. When you click on Media in the Menu bar (1), the Media settings of the remote console will display as shown below.



**Virtual Media Wizard (2):** Click on this item on the pull-down submenu to launch the Virtual Media Wizard, which allows you to configure Virtual Media settings as shown below.



## Virtual Media

**1 Floppy/USB Key Media**

☒ Floppy Image Browse

☐ A

**2 Connect Floppy**

**3 CD Media**

☒ ISO Image Browse

☐ G

**4 Connect CD/DVD**

**5 Status**

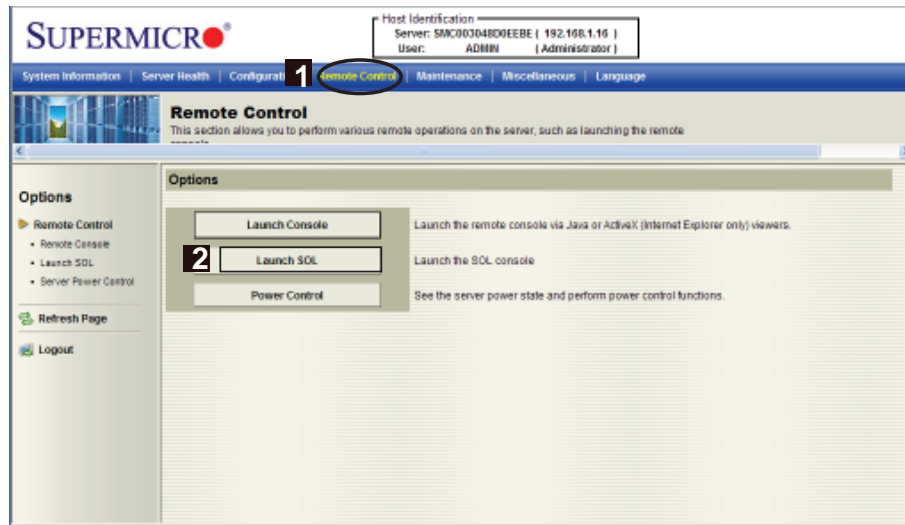
Target Drive	Connected To	Read Bytes
Virtual Floppy	Not connected	n/a
Virtual CD	Not connected	n/a

Close

1. Floppy/USB Key Media: This item allows the user to configure the Floppy/USB Key Media settings. You can choose from the following items:
  - Floppy Image
  - A (Disk Drive A of the remote console)
  - Browse: Click Browse to select the location of the Floppy ISO image.
2. Connect Floppy: After selecting the Virtual Media for your Remote Console, click on the Connect Floppy icon to connect to the remote console via the Floppy drive you chose.
3. CD Media: This item allows the user to configure CD Media settings. You can choose from the following items:
  - ISO Image
  - <Drive letter> (CD/DVD Drive)
  - Browse: Click Browse to select the location of the CD/DVD ISO image.
4. Connect CD/DVD: After selecting the Virtual Media for your Remote Console, click Connect CD/DVD to connect to the remote console via the CD/DVD you chose.
5. Status: This window displays the status of the target drive of the remote console.

### 2.5.3 Remote Control-Launch SOL

This feature allows you to launch the remote console by using Serial\_over\_LAN. When you click on the Remote Control icon in the Menu bar (1) to activate the Remote Control settings, the Remote Control Main Page will display.



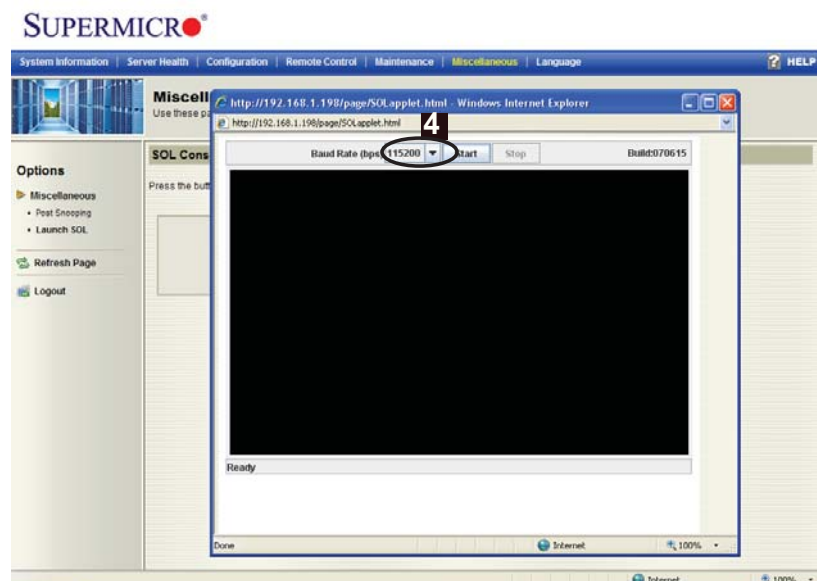
#### Launching SOL

1. **Launch SOL:** Click on this item in the left Options window to activate SOL (Serial Over LAN) support, which provides serial port connections over LAN and allows 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.
2. **The Launch SOL Button:** Click on this button to launch SOL. The following screen displays to indicate the progress of SOL launching as shown on the next page.

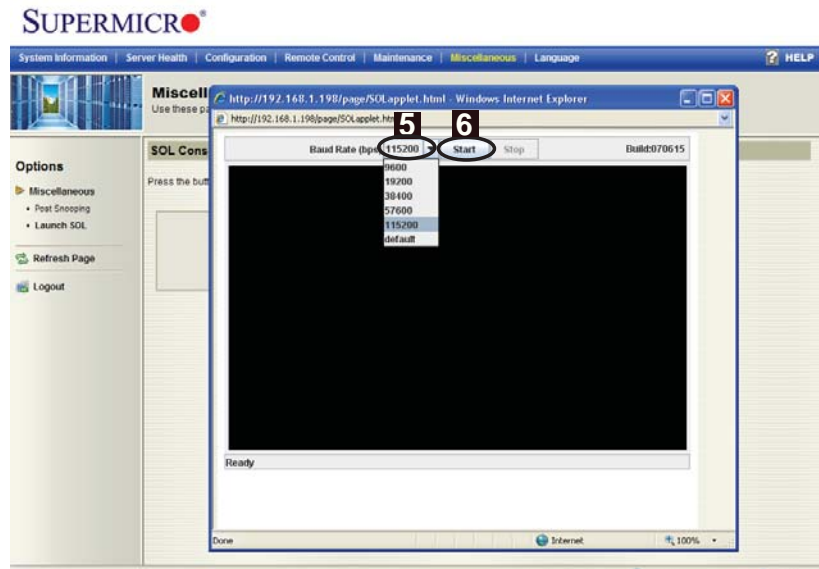


### Launching SOL

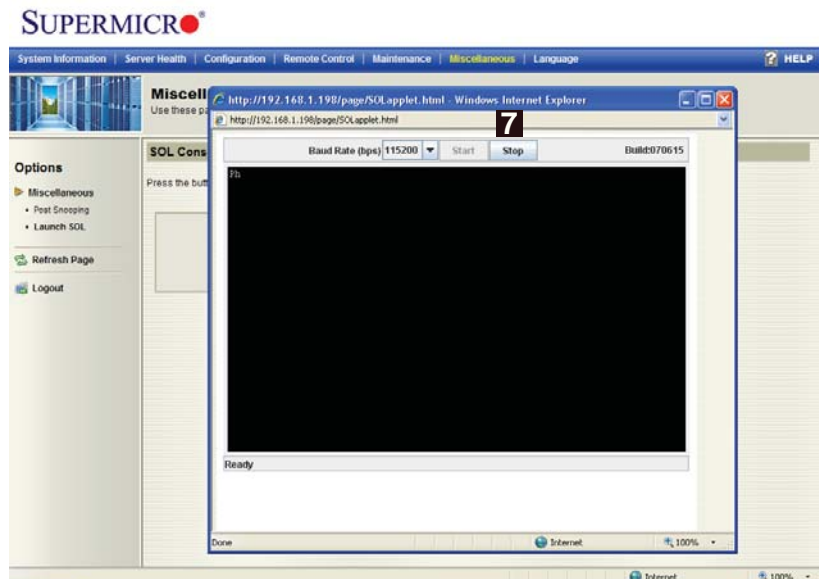
1. **Security Warning:** Once you've launched SOL, a security warning will appear, indicating that the application's digital signature cannot be verified
2. **Always trust content from this publisher:** Click on this item to give full access to this publisher, eliminating further security warnings.
3. Click Run to continue with SOL launching. Click Cancel to cancel SOL launching. If you continue with SOL launching, the following screen will appear.



4. Click on the ▼ to pull down the Baud Rate submenu, which will allow you to select the Baud Rate for serial line transfer.



5. Baud Rate (bps): You can select a Baud rate from the list as your SOL transfer rate. The options are: 9600 bps (bit-per-second), 19200 bps, 38400 bps, 57600 bps, 115200 bps, and default. Make sure that the Baud Rate selected here matches the Baud Rate set in the BIOS.
6. Once you've selected the Baud rate, press <Start> to start the session.



7. You can also press <Stop> to abort the SOL session.



### 2.5.3 Server Power Control

This feature allows you to configure power management settings for your remote console. When you click on the Remote Control icon in the Menu bar (1) to activate the Remote Control settings, the Remote Control Main Page will display.



Click Server Power Control in the left Options Window (2) to display the Power Control submenu as shown above.

#### Power Control and Status

**3. Power Control and Status:** This submenu indicates the status and the current power control settings of the host server (the remote console). The status of the remote server are displayed as below:

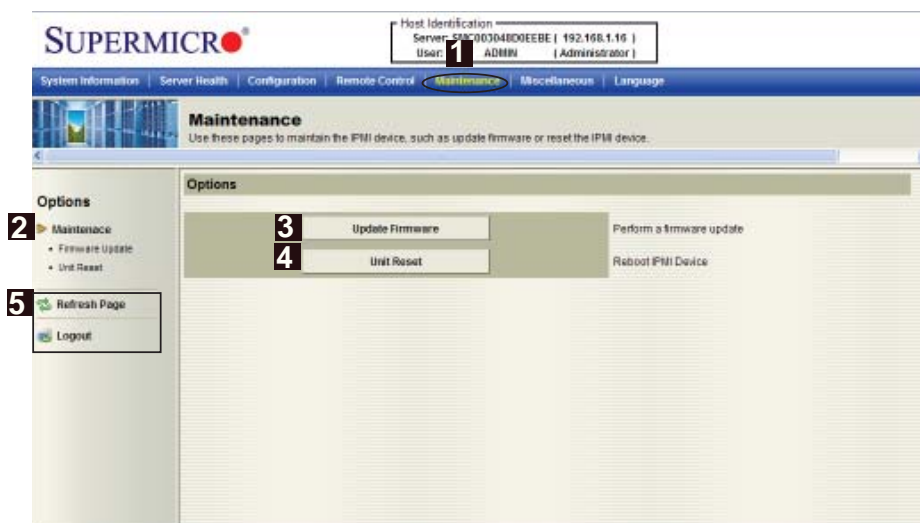
- **Reset Server:** Click on this radio button to reset the power control settings for the remote server.
- **Power Off Server - Immediately:** Click on this radio button to immediately power off the remote server.
- **Power Off Server - Orderly Shutdown:** Click on this radio button to power off and shut down the remote server in an orderly manner.
- **Power On Server:** Click on this radio button to power on the remote server.
- **Power Cycle Server:** Click on this radio button to power cycle the remote server.

**4. Perform Action:** After selecting a power setting from the list above, click on this item to execute the command and perform the action.



## 2.6 Maintenance

Use this feature to manage and configure IPMI devices. When you click on the Maintenance icon (1) in the Menu bar, the Maintenance Main page will display.

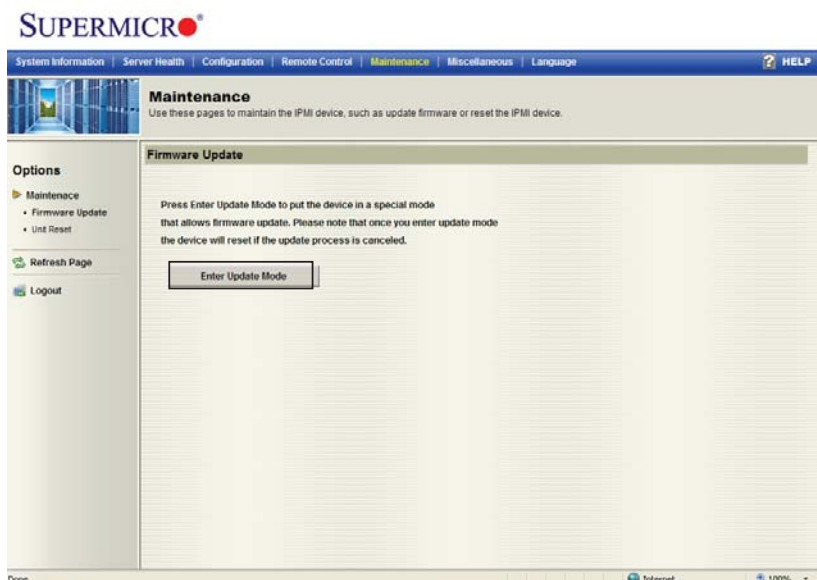


**Options:** Click on the Options window on the left (2) to use Maintenance settings. The options include the following:

- **Firmware Update (3):** Click this item to update the BMC firmware (the BIOS) of the remote server. The Firmware Update screen is shown in the next section.
- **Unit Reset (4):** Press the <Unit Reset> button to reboot the BMC (IPMI) Controller.


## 2.6.1 Maintenance - Firmware Update

When you click on the Maintenance icon in the Menu bar, the Maintenance Main page will display as below.



### Firmware Update

**Enter Update Mode:** Click on this item to enter the update mode.

 **Warning:** Once you've entered the firmware update mode, the device will be reset even if you cancel the process of firmware updating.

 **Notes:**

1. When updating firmware, you are given the option to "Preserve Configuration." Uncheck this option to load the factory default settings, and all the configuration settings will be lost.
2. If you are using the Static IP mode, it is not recommended to uncheck the option-"Preserve Configuration," since it will reset the network settings to the DHCP (Dynamic Host Configuration Protocol) mode.

## 2.7 Miscellaneous

This feature allows the user to perform network activities. Click on the Miscellaneous icon (1) in the Menu bar to display the Miscellaneous page.



### Miscellaneous

**Options:** Click on the Options window on the left (2) to use Miscellaneous settings. The options include the following:

- Post Snooping: Click on this item to query the POST (Power\_On\_Self-Test) Snooping code for BIOS LPC Port80.

## 2.8 Language

This feature allows you to configure Language Settings for your IPMI connections. Click on the Language icon (1) in the Menu bar to display the Language page as shown below.



### Language Settings

**Available Languages (2):** The Available Languages submenu displays language setting options. (Currently, English is the only language available for this utility.)

## Chapter 3

### Frequently Asked Questions

#### 3-1 Frequently Asked Questions

##### **A. Questions: How do I flash the IPMI firmware?**

##### **Answer:**

1. Log onto the web interface page of the IPMIcfg utility by typing the IP address of the system.
2. Click the Maintenance button. Browse to choose the correct file to flash the firmware.
3. Click the "Update Firmware" button to proceed with firmware flashing.

##### **B. Questions: How do I set up the IP address and MAC address for remote access?**

##### **Answer:**

1. Boot the system into DOS.
2. Run the utility-IPMICFG from DOS.
3. Follow the prompts to set up the IP address and MAC address for remote access.

You can also go to the BIOS to configure the IP address.

## 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.

# **Appendix A**

## **AMI Flash Tools Usage Guide**

Disclaimer: The following documents are used with permission from AMI. AMI is the legal owner of these documents. Supermicro has not verified the accuracy of the contents and assumes no responsibility with regard to any errors or omissions in the documents.





# Flash Tools Usage Guide

# **FLASH Tools**

## **Flash Tools:**

- 1) The Flash Tools are Command line utility programs used to upgrade Firmware using different medium like KCS, USB, and LAN.
- 2) The tools which are going to be focused in this guide are as follows,
  - a. YafuFlash
  - b. YafuKCS

## **YafuFlash:**

**Yet Another Firmware Upgrade Flash** is a tool used for flashing BMC. This utility is used for flashing in both Linux and Windows environment. Two types of medium used to flash the BMC are as follows,

- 1) Network
- 2) USB

Both mediums are applicable for Windows and Linux environment. The medium can be selected accordingly by usage.

## **YafuKCS:**

**Yet Another Firmware Upgrade Keyboard Controller Style** is a tool used for Flashing Firmware. This Utility is used for flashing in DOS environment. And particularly used in Keyboard Controller Style (KCS) interface.

## DOS flash firmware utility

**YAFUKCS** (Yet another Firmware Upgrade Flash) is a tool used for flashing BMC. This utility is used in DOS Environment. through KCS interface.

### Usage

- 1) Copy Yafukcs.exe into DOS machine
- 2) Run Yafukcs utility.
- 3) Note

### Format:

Yafukcs [OPTION] [FW\_IMAGE\_FILE]

### [OPTION]

- info Displays information about existing firmware and new firmware
- auto Option to do automatic upgrade by comparing Flash Module Header
- full Options to do full upgrade
- force-boot Option to FORCE BootLoader upgrade during full upgrade  
By default boot loader will be preserved
- c Option Preserve configuration module during full upgrade

### [FW\_IMAGE\_FILE]

Firmware image file name [rom.ima].

### Ex1:

./Yafukcs -info rom.ima

### Description:

Displays the details of both Existing Firmware and new firmware.

### Ex2:

./Yafukcs -full rom.ima

### Description:

This command starts to flash the new rom.ima to the firmware.

### Ex3:

./Yafukcs -full -force-boot rom.ima

### Description:

This command starts to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

## Windows Flash utility

- 1) Open Command Prompt and go to YafuFlash\Windows\ path.
- 2) There will be two files
  - a. Yafuflash.exe
  - b. LIBIPMI.dll
- 3) Now, run the Yafuflash.exe in the command prompt

### Format:

Yafuflash [OPTIONS] [MEDIUM] [FW\_IMAGE\_FILE]

### Note:

#### [OPTIONS]

- |              |   |
|--------------|---|
| - info       | Displays information about existing FW and new FW   |
| - auto       | Options to do auto upgrade by comparing Flash Module Header   |
| - full       | Options to do full upgrade  |
| - force-boot | Option to FORCE BootLoader upgrade during full upgrade.<br>By default boot loader will be preserved |
| - c          | Option Preserve configuration module during full upgrade  |

#### [MEDIUM]

- |            |  |
|------------|--|
| -cd        | Option to use USB medium                                 |
| - nw & -ip | Option to network medium with -ip followed by ipaddress. |

#### [FW\_IMAGE\_FILE]

Firmware image file name [rom.ima].

- 4) Examples:

### Network Medium:

**Ex1:** Yafuflash -nw -ip 155.166.132.12 -info rom.ima

#### **Description:**

This command works with network medium using the ip 155.166.132.12, which displays the details of both Existing Firmware and new firmware.

**Ex2:** Yafuflash -nw -ip 155.166.132.12 -full rom.ima

#### **Description:**

This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware.

**Ex3:** Yafuflash -nw -ip 155.166.132.12 -full -force-boot rom.ima

#### **Description:**

This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with FORCE BootLoader Upgrade.

### USB Medium:

**Ex1:** Yafuflash -cd -info rom.ima

**Description:**

This command works with USB medium which displays the details of both Existing Firmware and new firmware.

**Ex2:** Yafuflash -cd -full rom.ima

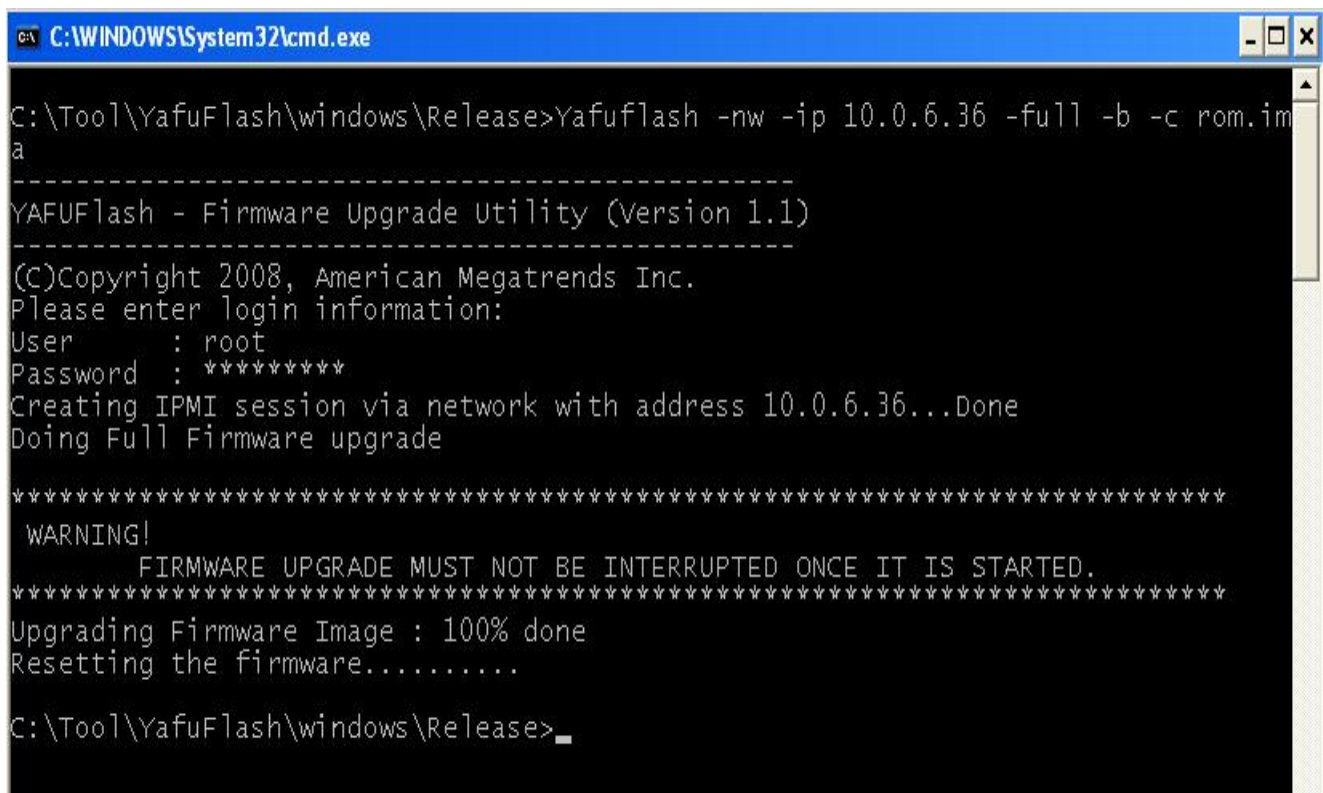
**Description:**

This command works with USB medium which start to flash the new rom.ima to the firmware.

**Ex3:** Yafuflash -cd -full -force-boot rom.ima

**Description:**

This command works with USB medium which start to flash the new rom.ima to the firmware with FORCE BootLoader Upgrade.

A screenshot of a Windows command prompt window titled "C:\WINDOWS\System32\cmd.exe". The command entered is "C:\Tool\YafuFlash\windows\Release>Yafuflash -nw -ip 10.0.6.36 -full -b -c rom.ima". The output shows the YAFUFlash utility version 1.1, copyright 2008 by American Megatrends Inc. It prompts for login information with user "root" and password "\*\*\*\*\*". It then reports "Creating IPMI session via network with address 10.0.6.36...Done" and "Doing Full Firmware upgrade". A warning message states: "WARNING! FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED." followed by "Upgrading Firmware Image : 100% done" and "Resetting the firmware.....". The prompt ends with "C:\Tool\YafuFlash\windows\Release>".

```
C:\WINDOWS\System32\cmd.exe
C:\Tool\YafuFlash\windows\Release>Yafuflash -nw -ip 10.0.6.36 -full -b -c rom.ima
a
-----
YAFUFlash - Firmware Upgrade Utility (Version 1.1)
-----
(C)Copyright 2008, American Megatrends Inc.
Please enter login information:
User       : root
Password   : *****
Creating IPMI session via network with address 10.0.6.36...Done
Doing Full Firmware upgrade

*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
*****
Upgrading Firmware Image : 100% done
Resetting the firmware.....
C:\Tool\YafuFlash\windows\Release>
```

```
C:\WINDOWS\System32\cmd.exe

C:\Tool\YafuFlash\windows\Release>Yafuflash -nw -ip 10.0.6.36 :www rom.ima
-----
YAFUFlash - Firmware Upgrade Utility (Version 1.1)
-----
(C)Copyright 2008, American Megatrends Inc.
Please enter login information:
User       : root
Password   : *****
Creating IPMI session via network with address 10.0.6.36...Done

*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
*****
Updating the module www ..... Done
Resetting the firmware.....

C:\Tool\YafuFlash\windows\Release>_
```

## Linux flash utility

1. Open Terminal and go to YafuFlash/Linux path.
2. The file libipmi.so.1 should be accessible to linux system. Usually when running an application Linux searches for the dependent libraries in the default locations like /usr/lib /lib folders.
3. Copy libipmi.so.1 to /lib or /usr/lib and run 'ldconfig'  
OR  
Copy libipmi.so.1 to some folder and issue the following command  
# LD\_LIBRARY\_PATH=<location\_of\_libipmi\_so> ./Yafuflash  
You may have to create a link to libipmi.so.1.0 (ln -sf libipmi.so.1.0 libipmi.so.1)
4. Now, run the Yafuflash.exe in the terminal

### Format:

`./Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE]`

### Note:

#### **[OPTIONS]**

- info Displays information about existing FW and new FW
- auto Options to do auto upgrade by comparing Flash Module Header
- full Options to do full upgrade
- force-boot Option to FORCE BootLoader upgrade during full upgrade  
By default boot loader will be preserved
- c Option Preserve configuration module during full upgrade

#### **[MEDIUM]**

- cd Option to use USB medium
- nw & -ip Option to network medium with -ip followed by ipaddress.

#### **[FW\_IMAGE\_FILE]**

Firmware image file name [rom.ima].

## Examples

### Network Medium:

#### **Ex1:**

`./Yafuflash -nw -ip 155.166.132.12 -info rom.ima`

#### **Description:**

This command works with network medium using the ip 155.166.132.12, which displays the details of both Existing Firmware and new firmware.

**Ex2:**

```
./Yafuflash -nw -ip 155.166.132.12 -full rom.ima
```

**Description:**

This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware.

**Ex3:**

```
./Yafuflash -nw -ip 155.166.132.12 -full -force-boot rom.ima
```

**Description:**

This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.

**USB Medium:****Ex1:**

```
./Yafuflash -cd -info rom.ima
```

**Description:**

This command works with USB medium which displays the details of both Existing Firmware and new firmware.

**Ex2:**

```
./Yafuflash -cd -full rom.ima
```

**Description:**

This command works with USB medium which start to flash the new rom.ima to the firmware.

**Ex3:**

```
./Yafuflash -cd -full -force-boot rom.ima
```

**Description:**

This command works with USB medium which start to flash the new rom.ima to the firmware with FORCE BootLoader upgrade.



```
root@localhost:/home/siva/SP/SP/pilot-ii/development/proprietary/software/YafuFlash/linux_86
[root@localhost linux_86]# ./Yafuflash -nw -ip 10.0.6.36 -full -c rom.ima
-----
YAFUFlash - Firmware Upgrade Utility (Version 1.1)
-----
(C)Copyright 2008, American Megatrends Inc.
Please enter login information:
User      : root
Password  :

Creating IPMI session via network with address 10.0.6.36...Done
Doing Full Firmware upgrade

*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
*****
Preserving Env Variables ... Done
Upgrading Firmware Image : 100% done
Setting Env variables ... Done
Resetting the firmware.....
[root@localhost linux_86]#
```

```
root@localhost:/home/siva/SP/SP/pilot-ii/development/proprietary/software/YafuFlash/linux_86
[root@localhost linux_86]# ./Yafuflash -nw -ip 10.0.6.36 :www rom.ima
-----
YAFUFlash - Firmware Upgrade Utility (Version 1.1)
-----
(C)Copyright 2008, American Megatrends Inc.
Please enter login information:
User      : root
Password  :

Creating IPMI session via network with address 10.0.6.36...Done

*****
WARNING!
FIRMWARE UPGRADE MUST NOT BE INTERRUPTED ONCE IT IS STARTED.
*****
Updating the module www ..... Done
Resetting the firmware.....
[root@localhost linux_86]#
```

## **Firmware Recovery**

If the firmware upgrade was interrupted due to any reason, when the flashing was in progress, it can be recovered using Yafukcs

### **Steps:**

1. Power cycle the system by removing the power cord.
2. Boot to DOS and flash the FW using Yafukcs.

## **Appendix B**

### **AMI VMCLI Usage Guide**



# VMCLI

## Usage Guide

# VMCLI

## VMCLI (Virtual Media Command line interface):

The Virtual Media Command Line Interface (VMCLI) is a command-line interface that provides virtual media features from the Client system to the Host.

VMCLI is used to redirect the virtual media from the Client system to the host. VMCLI comes in two versions to support Windows and Linux clients.

VMCLI can redirect the following medias

- CD/DVD ROM
- ISO image
- USB Key
- Floppy drive
- Floppy image

## In Linux

- 1) Open Terminal and go to VMCLI /Linux path.
- 2) There will be one file
  - a. VMCLI
- 3) Now, run the VMCLI in the terminal
- 4) Syntax:

```
VMCLI -r <RAC-IP> -u <RAC-USER> -p <RAC-PASSWD>  
[ -f <FLOPPY-IMG> | -f <FDDrive:\> | -c <ISO9660-IMG> -c <CDDrive:\> ] -e
```

- 5) Note:

<RAC-IP> - string of the form: 'RAC-IP[:https\_port]'  
<ISO9660-IMG> <FLOPPY-IMG> are bootable image files  
<-c <CDDrive:\> and <-c <FDDrive:\> are valid CD and floppy drives  
<RAC-USER> - RAC user ID, with 'virtual media' privilege  
<RAC-PASSWD> - RAC user password  
-e - Enable encrypted data transfer through SSL

- 6) Examples:

**Eg1:** ./VMCLI -r 10.0.3.230::443 -u root -p superuser -f /dev/sdc

Description:

This command is to redirect the floppy disk media from Client System to Host

**Eg2:** ./VMCLI -r 10.0.3.230::443 -u root -p superuser -c /dev/cdrom

**Description:**

This command is to redirect the CD/DVD media from the Client System to Host

**Eg3:** `./VMCLI -r 10.0.3.230::443 -u root -p superuser -c /dev/cdrom -f /dev/sdc`

**Description:**

This command is to redirect the USB floppy, CD/DVD media from the Client System to Host

**Eg4:** `./VMCLI -r 10.0.3.230::443 -u root -p superuser -f /tmp/myfloppy.img`

**Description:**

This command is to redirect the floppy image file from the Client System to Host

**Eg5:** `./VMCLI -r 10.0.3.230::443 -u root -p superuser -c /tmp/mydvd.img`

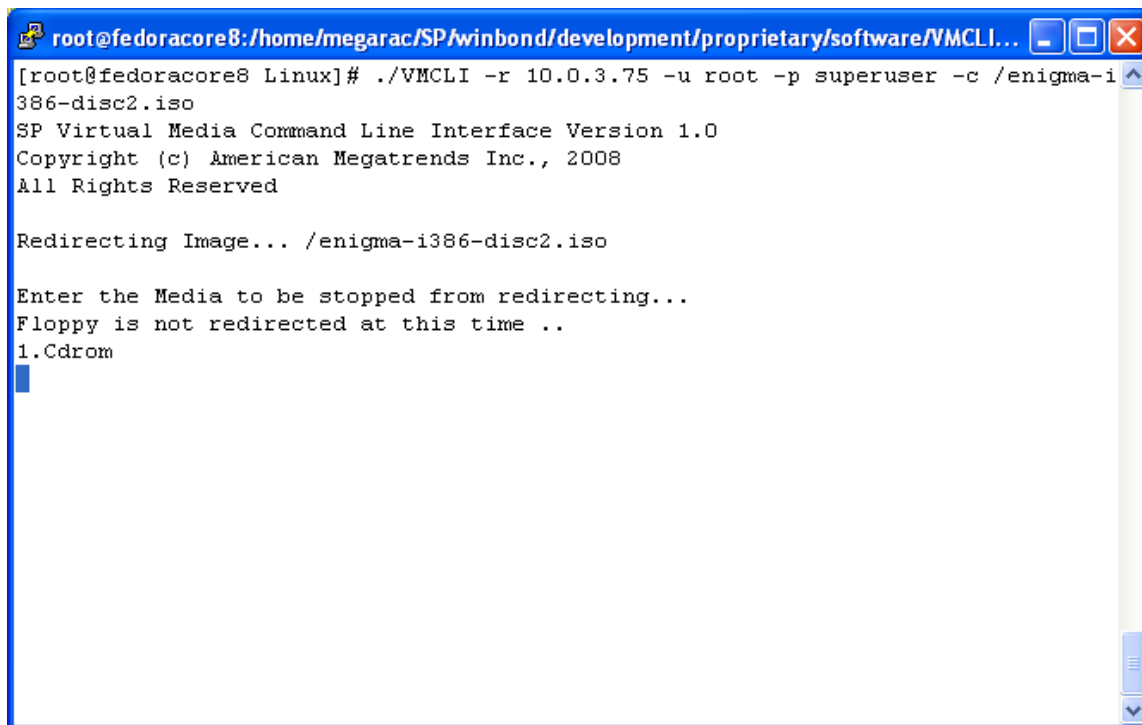
**Description:**

This command is to redirect the CD/DVD image file from the Client System to Host

**Eg6:** `./VMCLI -r 10.0.3.230::443 -u root -p superuser -f /tmp/myfloppy.img  
-c /tmp/mydvd.img`

**Description:**

This command is to redirect the floppy, CD/DVD image file from the Client System to Host



```
root@fedoracore8:/home/megarac/SP/winbond/development/proprietary/software/VMCLI...
[root@fedoracore8 Linux]# ./VMCLI -r 10.0.3.75 -u root -p superuser -c /enigma-i
386-disc2.iso
SP Virtual Media Command Line Interface Version 1.0
Copyright (c) American Megatrends Inc., 2008
All Rights Reserved

Redirecting Image... /enigma-i386-disc2.iso

Enter the Media to be stopped from redirecting...
Floppy is not redirected at this time ..
1.Cdrom
```

## **In Windows**

- 1) Open Command prompt and go to VMCLI /Windows path.
- 2) There will be one file
  - a. VMCLI.exe
- 3) Now, run the VMCLI in the Command prompt
- 4) Note: To run VMCLI in Windows, Wget utility should be installed in the system.

5) Syntax:

```
VMCLI.exe -r <RAC-IP::https_port> -u <RAC-USER> -p <RAC-PASSWD>  
[ -f <FLOPPY-IMG> | -f <FDDrive:\> | -c <ISO9660-IMG> -c <CDDrive:\> ] -e
```

6) Note:

<RAC-IP> - string of the form: 'RAC-IP[:https\_port]'  
<ISO9660-IMG> <FLOPPY-IMG> are bootable image files  
<-c <CDDrive:\> and <-c <FDDrive:\> are valid Cd and floppy drives  
<RAC-USER> - RAC user id, with 'virtual media' privilege  
<RAC-PASSWD> - RAC user password  
-e - Enable encrypted data transfer through ssl'

7) Examples:

**Eg1:** VMCLI.exe -r 10.0.3.230::443 -u root -p superuser -f a:\

Description:

This command is to redirect the floppy disk media from the Client System to Host

**Eg2:** VMCLI -r 10.0.3.230::443 -u root -p superuser -c d:\

Description:

This command is to redirect the CD/DVD media from the Client System to Host

**Eg3:** VMCLI.exe -r 10.0.3.230::443 -u root -p superuser -c d:\ -f a:\

**Description:**

This command is to redirect the floppy, CD/DVD media from the Client System to Host

**Eg4:** VMCLI.exe -r 10.0.3.230::443 -u root -p superuser -f c:\myfloppy.img

Description:

This command is to redirect the floppy image file from Client System to Host

**Eg5:** . /VMCLI.exe -r 10.0.3.230::443 -u root -p superuser -c c:\mydvd.img

**Description:**

This command is to redirect the CD/DVD image file from the Client System to Host

**Eg6:** VMCLI.exe -r 10.0.3.230::443 -u root -p superuser -f c:\myfloppy.img

-c c:\mydvd.img

**Description:**

This command is to redirect the floppy, CD/DVD image file Client System to Host

```
C:\ D:\WINDOWS\system32\cmd.exe - VMCLI.exe -r 10.0.3.75 -u root -p superuser -c e:\redhat...
D:\Documents and Settings\revanthani\Desktop>VMCLI.exe -r 10.0.3.75 -u root -p s
uperuser -c e:\redhat7.2\enigma-i386-disc1.iso
SP Virtual Media Command Line Interface Version 1.0
Copyright (c) American Megatrends Inc., 2008
All Rights Reserved

Redirecting Image... e:\redhat7.2\enigma-i386-disc1.iso

Enter the Media to be stopped from redirecting...
Floppy is not redirected at this time ..
1.Cdrom
-
```

```
C:\ D:\WINDOWS\system32\cmd.exe - VMCLI.exe -r 10.0.3.75 -u root -p superuser -f a:\
D:\Documents and Settings\revanthani\Desktop>VMCLI.exe -r 10.0.3.75 -u root -p s
uperuser -f a:\
SP Virtual Media Command Line Interface Version 1.0
Copyright (c) American Megatrends Inc., 2008
All Rights Reserved

Redirecting Floppy drive.. A

Enter the Media to be stopped from redirecting...
CD is not redirected at this time ..
1.Floppy
-
```