**HX2560 M1/**
**HX2560 M2**

CA92344-0332-02

# IPMI User's Guide

FUJITSU

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.

Fujitsu Limited 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 Fujitsu Limited 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 FUJITSU LIMITED 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, FUJITSU LIMITED 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.

FCC Statement: This equipment has been tested and found to comply with the limits for a Class A digital device pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the manufacturer's instruction manual, may cause harmful interference with radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case you will be required to correct the interference at your own expense.

Manual Revision 2.0
Release Date: August 16, 2013

# 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 serverboards. It provides detailed information on how to configure the IPMI settings supported by the WPCM450 Controller.

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

## User's Guide Organization

**Chapter 1** provides an overview on the Nuvoton WPCM450 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 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.

## Notes

# Table of Contents

# Notes

# Chapter 1

# Introduction

## 1.1 Overview of the Nuvoton WPCM450 BMC Controller

The Nuvoton WPCM450, a Baseboard Management Controller (BMC), supports PCI-based 2D/VGA Graphics cores via PCI interfaces, multi-media virtualization, and Keyboard/Video/Mouse Redirection (KVMR). The WPCM450 Controller is ideal for networking management.

The WPCM450 interfaces with the host system via PCI connections to communicate with the Graphics core. It supports USB 2.0 and 1.1 for remote KVM emulation. It also provides LPC interface support 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 SMBus interface, PECI (Platform Environment Control Interface) buses, and General Purpose I/O ports.

### WPCM450 DDR2 Memory Interface

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

### WPCM450 PCI System Interface

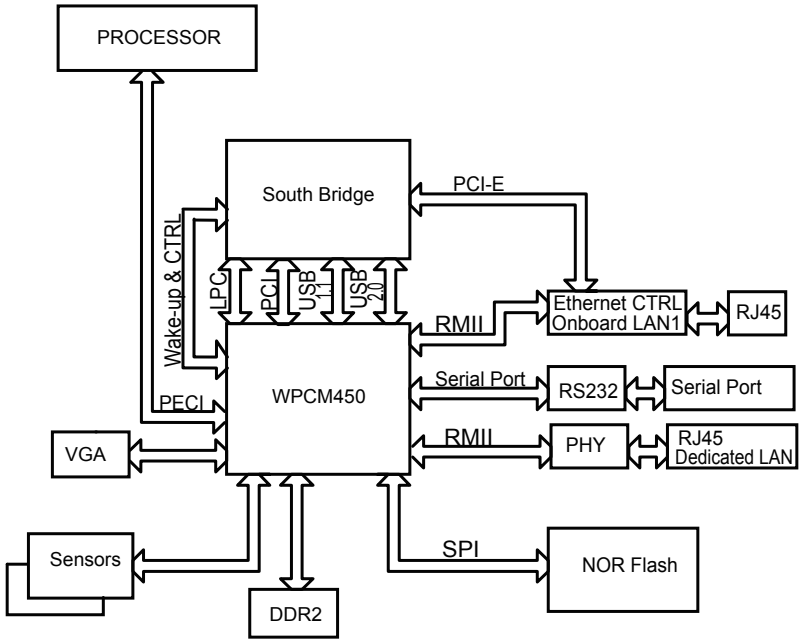
The WPCM450 provides 32-bit, 33 MHz 3.3V PCI interface, which is compliant with PCI Local Bus Specification Rev. 2.3. The PCI system interface connects to the onboard PCI Bridge and is used by the graphics controller.

## IPMI Features

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

## 1.2 WPCM450 Block Diagram

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




## 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 serverboard, the WPCM450 BMC Controller will connect the South Bridge to other onboard components, providing remote network interface via serial links. With the WPCM450 Controller and the IPMI firmware built in, the serverboard 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 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

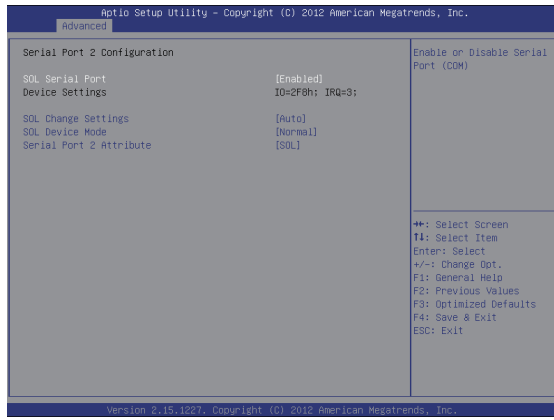
With the Nuvoton WPCM450 BMC Controller, serverboard allow the user to access, monitor, manage and interface with multiple systems in different remote locations.

## 2.1 Configuring BIOS

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

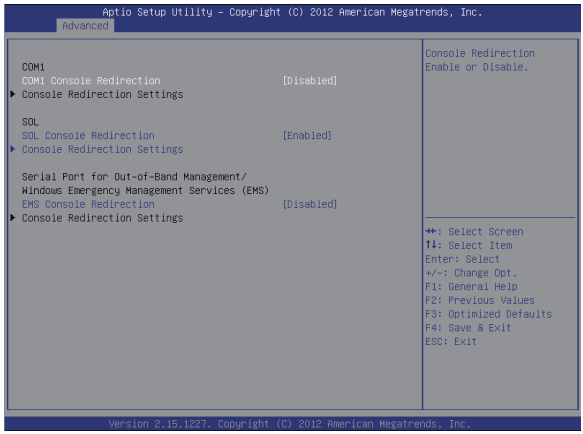
### *Enabling COM Port for SOL (IPMI)*

1. Press the <Del> key at bootup to enter the BIOS Setup utility.
2. Select *Advanced* and press <Enter> to enter the Advanced menu.
3. From the Advanced menu, select *Super IO Configuration* and press <Enter>.
4. From the Super IO Configuration menu, select *Serial Port 2 Configuration* and press <Enter>.
5. Make sure that *SOL Serial Port* is enabled. If not, Select *SOL Serial Port* and press <Enabled>.
6. Make sure that *Serial Port* 2 *Attribute* is <SOL>. If not, Select *Serial Port* 2 *Attribute* and press <SOL>.



7. Back to the Advanced menu. Then select *Serial Port Console Redirection* and press <Enter>.

8. Make sure that *SOL Console Redirection* is <Enabled>. If not, Select *SOL Console Redirection* and press <Enabled>.




### *B. Enabling All Onboard USB ports*

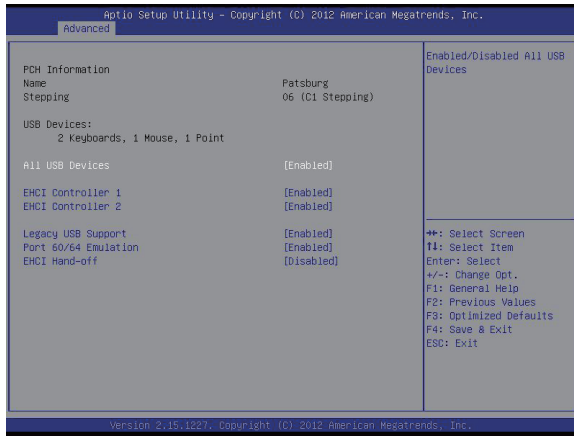
1. Press the <Del> key at bootup to enter the BIOS Setup utility.

2. Select *Advanced* and press <Enter> to enter the Advanced menu.

3. Select *Chipset Configuration* and press <Enter>.

4. From the Chipset Configuration submenu, select *South Bridge* and press <Enter>.

5. Make sure that all *All USB Devices* are enabled. If not, Select *All USB Devices* and press <Enabled>. (This is required for KVM to work properly.)

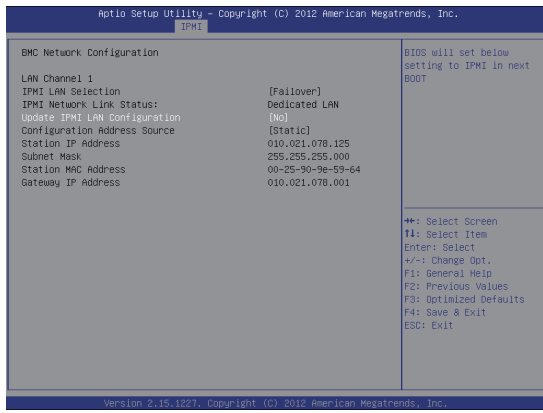



### *C. Configuring IP and MAC Addresses using BIOS*

1. Press the <Del> key at bootup to enter the BIOS Setup utility.

2. Select *IPMI* and press <Enter> to enter the IPMI menu.

3. From the IPMI menu, select *BMC Network Configuration* and press <Enter> to set IP and MAC addresses.



## 2.2 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.


1. Enter your Username in the *Username* fields.

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

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

3. The Home Page will display as shown on the next page.

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

## 2.3 IPMI Main Screen

The IPMI Main screen displays the following information.


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

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

2. The Options Window: This window displays IPMI submenu items. Click an item in this window to configure the setting.

3. The Main Display Area: This area displays the contents of the particular section. Click an item in this area to configure the setting.

4. System Health Status: This icon displays the health status of the server.

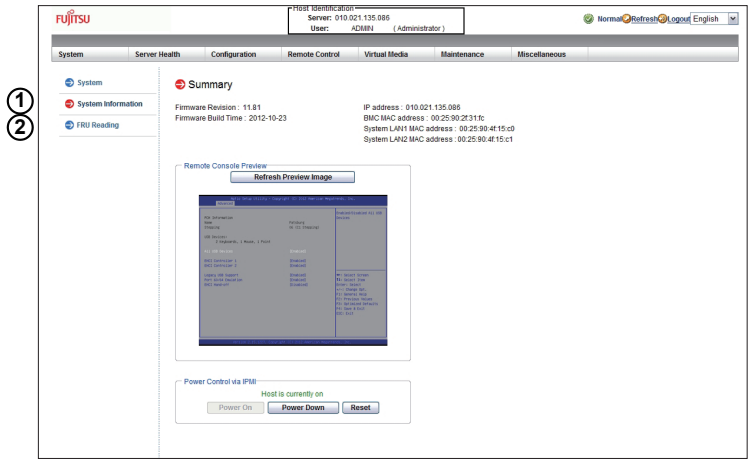
   - Green: It indicates that the server is normal.
   - Orange: At least an alert has occurred. Take proper actions to ensure system health.
   - Red: At least one critical condition has occurred. Immediate attention is required to resolve the critical condition for the server to function normally.

5. Language Select: From the pull-down menu, select a language.

   - English
   - Japanese

## 2.4 System Status

Once you've logged into the remote server, the IPMI Main scree will display.




1. System Information: This item displays the following firmware information.

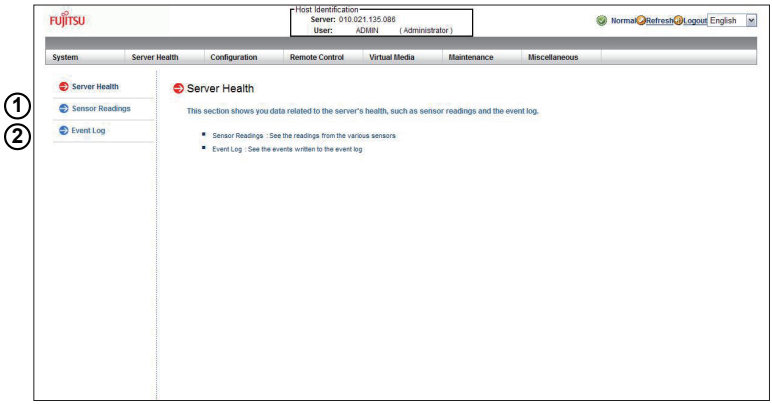
   - Firmware Revision
   - Firmware Build Time
   - IP Address
   - MAC Address
   - Preview Screen
   - Power Control: This feature allows the user to launch the remote console by clicking a preview screen.

2. FRU Reading: Click this item to display the following BMC FRU (Field Replaceable Unit) information.

   - FRU Device ID
   - Chassis Information
   - Board Information
   - Product Information

## 2.5 Server Health

This feature allows the user to set *Server Health* settings. To access *Server Health* information, follow the instructions below.

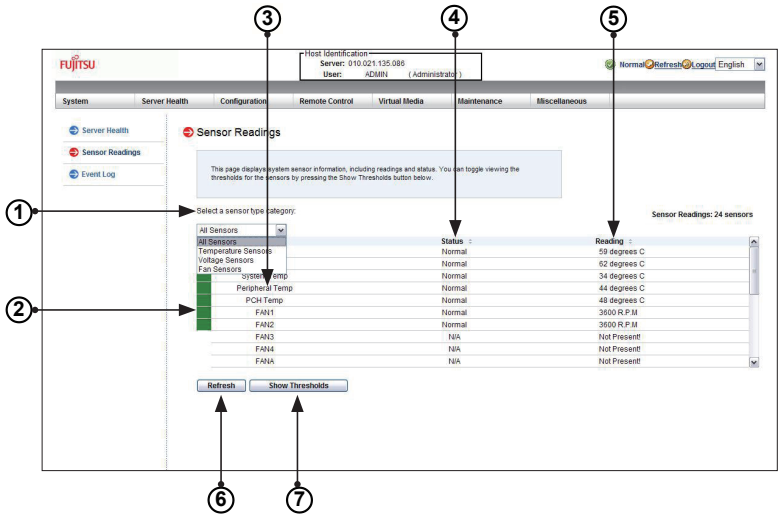



1. Click <Sensor Readings> to access information on sensor readings as shown on the next page.

2. Click <Event Log> to access event logs.

### 2.5.1 Sensor Readings

This page displays sensor readings for the remote console.




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

   - All Sensors
   - Temperature Sensors
   - Voltage Sensors
   - Fan Sensors
   - Physical Secrity
   - Power Supply
   - OEM Reserved:

2. A senor color that is displayed in front of an sensor indicates the status of the sensor.

    - Green: It indicates that the sensor reading is normal. The system functions normally.
    - Amber: There is an alert on the sensor reading. Attention is needed to ensure that the system is functioning properly.
    - Red: One or more sensors have reached the critical state. Immediate action is needed to resolve the problem.

3. Name of the Sensor: 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.

4. Status: This column indicates the status of each sensor reading.

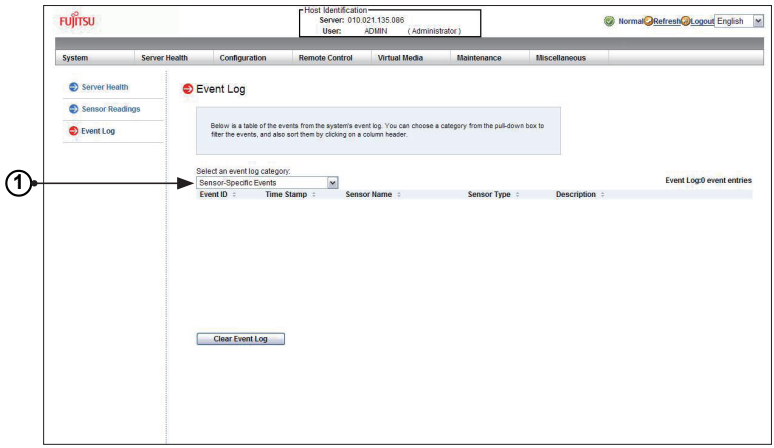
5. Reading: This column indicates the reading of each sensor.

6. Refresh: Click this item to refresh the page.

7. Show Thresholds: Click this item to display senor thresholds.

## 2.5.2 Event Log

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




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

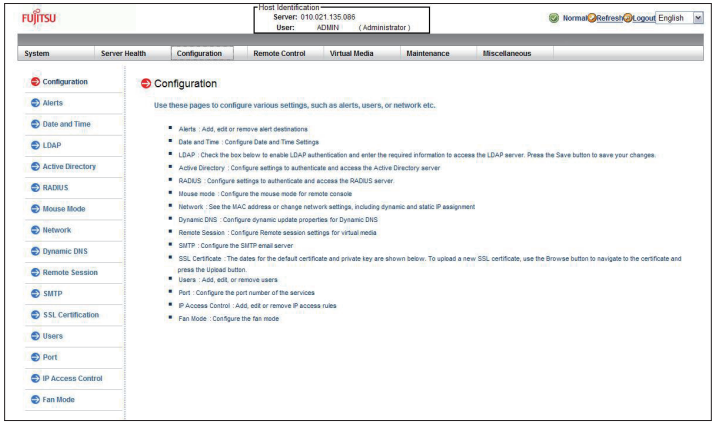
   - Sensor-Specific Events: These event logs are generated by the BMC if the sensor's reading reaches the threshold.
   - BIOS-Generated Events: These event logs are generated by the BIOS and logged to the BMC.
   - System Management Software Events: These events logs are generated by the OS, application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

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

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

## 2.6 Configuration

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



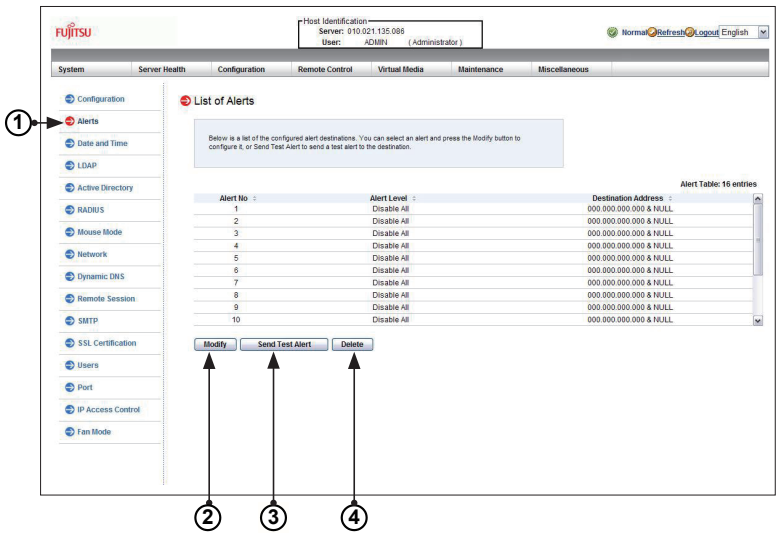

This section allows the user to configure the following settings.

- Alerts: Use this item to configure alert destination settings.
- Date & Time
- LDAP: Use this item to configure LDAP (Lightweight Directory Access Protocol) settings for authentication and access to the LDAP server.
- Active Directory: Use this item to configure the settings for authentication and access to the Active Directory server.
- RADIUS: Use this item to configure the settings for authentication and access to the Radius server.
- Mouse mode
- Network
- Dynamic DNS
- Remote Session
- SMTP
- SSL Certificate

- Users
- Port
- IP Access Control
- Fan Mode

### 2.6.1 Configuring the Alerts Settings

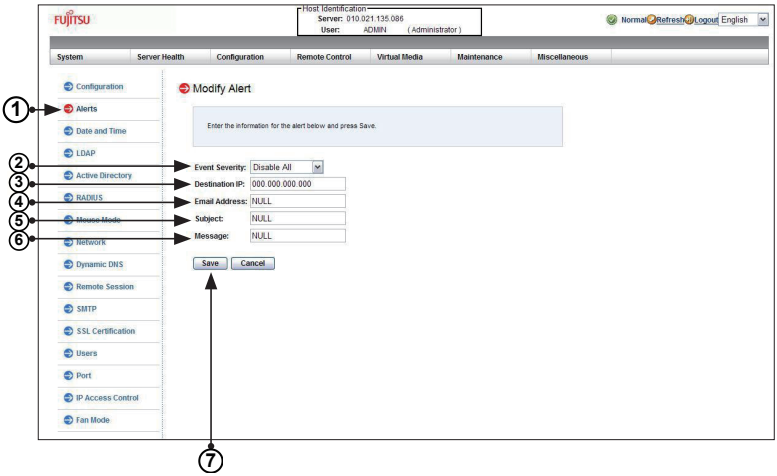
This feature allows the user to configure *Alert* settings. When you click the <Alerts> icon in the menu bar, the following screen will display.




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

1. Click <Alerts> to activate the alert submenu.
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.

*To Setup an Alert*




Follow the steps below to setup an alert.

1. Select *Alerts* from the window on the left.

2. Select *Alert Severity*.

3. Enter the SNMP Trap receiver IP address to use SNMP. For further guidance on typical inquiries relating to SNMP, see the table below.

| *Item* | *Answer* |
|---|---|
| SNMP version number | SNMP version 2. |
| The IPMI item you need to configure so the SNMP manager can receive the SNMP trap | The alert LAN destination address (see #3 under 2.6.1) 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 section 2.6.10)

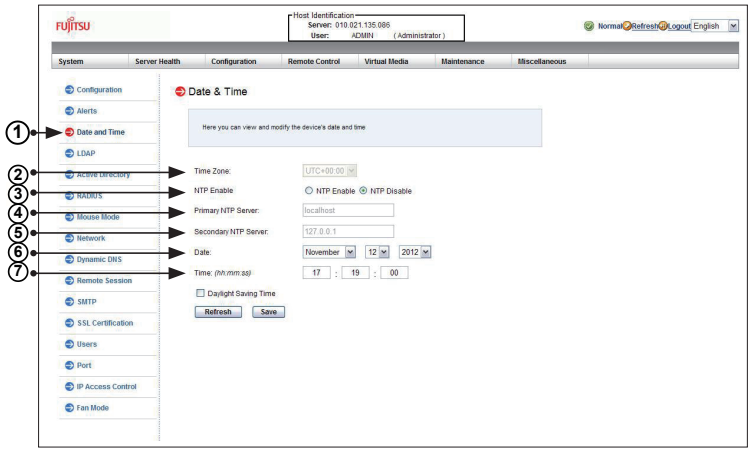
5. Enter the subject line of the alert.

6. Enter a message for the alert.

7. Click <Save> to save the settings.

## 2.6.2 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. When you click the <Time and Date> icon in the Options window, the following screen will display.




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

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

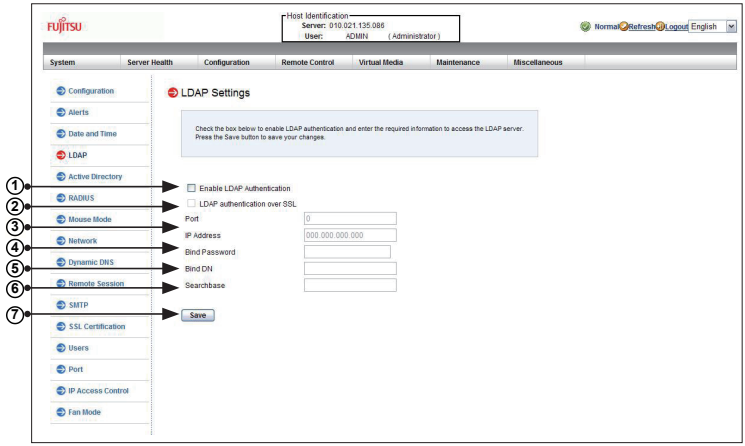
1. Click *Date/Time* on the left to set the date/time settings.
2. Select the time zone.
3. Check this item for NTP settings.
4. Enter the IP address for the primary NTP server.
5. Enter the IP address for the secondary NTP server.
6. Enter the date.
7. Enter the time in hh/mm/ss format.

Click *Refresh* to change the date/time settings.

Click *Save* to save the entries.

### 2.6.3 Configuring Light-Weight Directory Access Protocol (LDAP) Settings

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




Follow the steps below to configure the LDAP settings.

1. Check the enable box to enable *LDAP Authentication and LDAP Authentication over SSL* support.

2. Enter a port number for the LDAP server.

3. Enter an IP Address for the LDAP server.

4. Enter a Bind Password for the LDAP server.

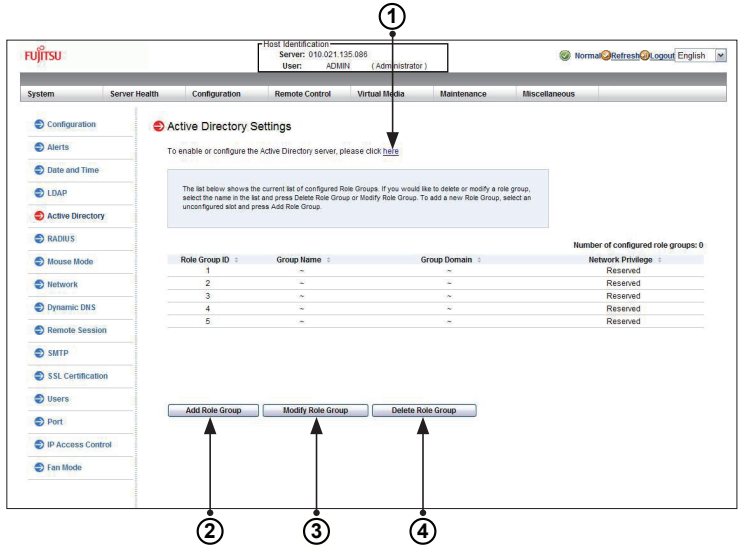
5. Enter a Bind DN value in the field. (The bind DN is the user or the LDAP server that is permitted to do search in the LDAP directory within a defined search base.)

6. Enter a SearchBase value in the field. (The SearchBase is the directory that allows the external user to search data.)

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

## 2.6.4 Active Directory Settings

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




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

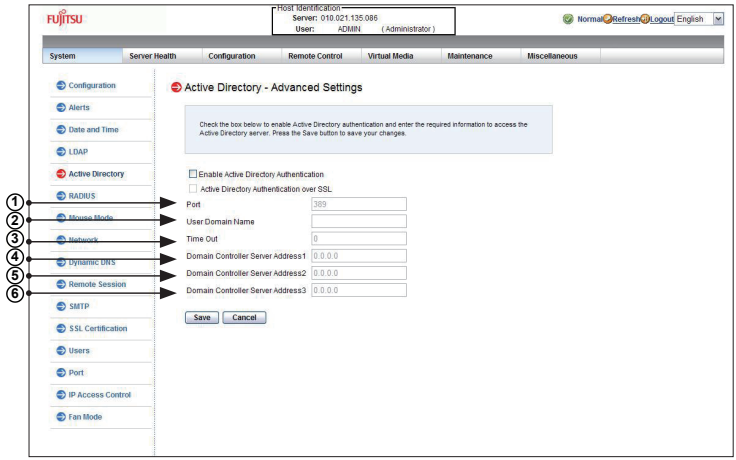
2. Select a group and click <Add> to add a role group.

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

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

### *Configuring the Active Directory Settings*

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

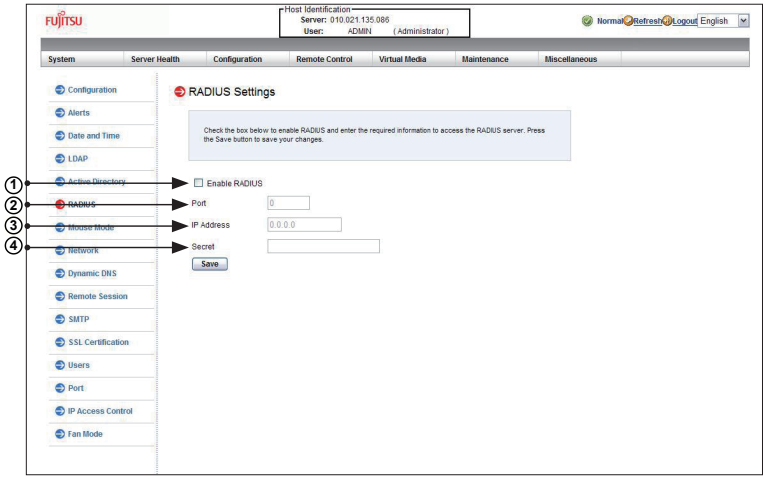



1. Check the <Enable> box to enable *Active Directory* authentication support. Then, Enter the values in the fields below.
2. Enter User Domain Name in the field.
3. Enter Time Out value in the field to set the time limit for a user to stay logging-in.
4. Enter <Controller Server Address1>.
5. Enter <Controller Server Address2>.
6. Enter <Controller Server Address3>.

After entering the information, click <Save> to save the settings.

## 2.6.5 Configuring the RADIUS Settings

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




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

2. Enter the port number for the Radius server.

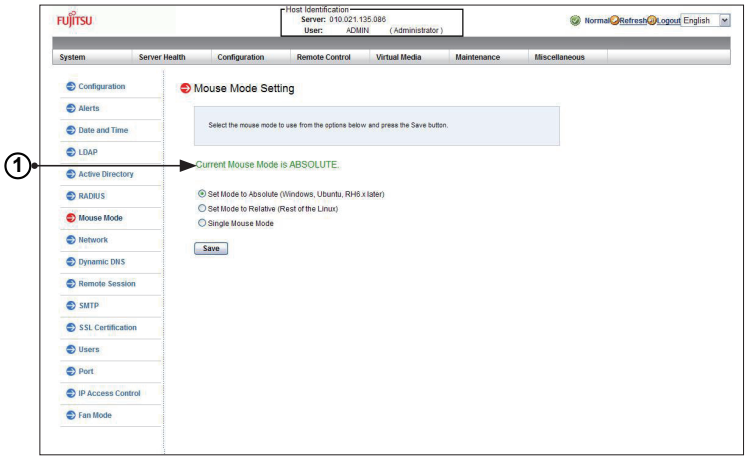
3. Enter the IP address of the Radius server.

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

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

## 2.6.6 Configuring the Mouse Mode Settings

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



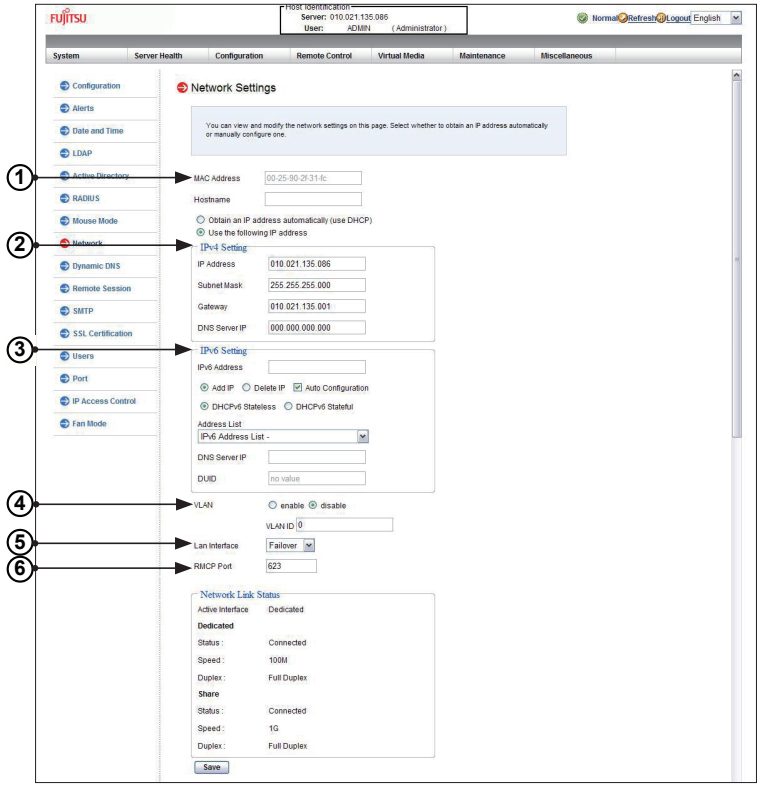

1. This item displays the current Mouse Mode setting. To select a proper Mouse Mode setting, click the proper radio button as shown below.

   - Check the radio button to set the mouse mode to *Absolute Mode* for the Windows OS. (This is the default setting.)
   - Check the radio button to set the mouse mode to *Relative Mode* for the Linux/ Unix OS.
   - Single Mouse Mode: Check this radio button to use single mouse mode.
   - After entering the information, click "Save" to save the settings.

   **Note**: 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.

## 2.6.7 Configuring Network Settings

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




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

1. 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 setup the IP address by manually entering the information in the fields below. (**Note**: DHCP is the default setting.)

2. To set the IP address using the IPv4 format, enter proper information in the following fields.

   - IP address

- Subnet Mask
- (Default) Gateway
- DNS Server IP

3. 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.

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

5. LAN Interface

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

- The default setting is Failover, which will allow IPMI to be connected from either the shared LAN port (LAN1/0) or the dedicated IPMI LAN port. Precedence is given to the Dedicated LAN port over the shared LAN port.
- Select <Dedicated LAN> for IPMI to connect through the IPMI Dedicated LAN port at all time.
- Select *Shared LAN* for IPMI to connect through the LAN port on the board.

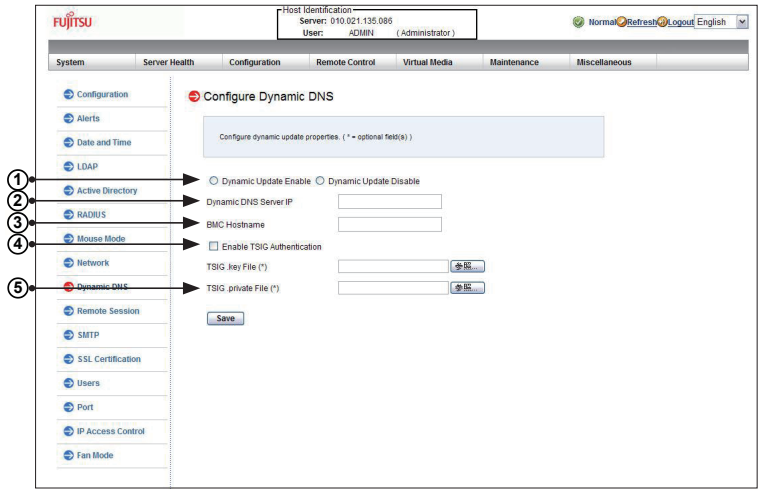
6. RMCP Port

This feature allows the user to select the desired RMCP (Remote Mail Checking Protocol) port based on his configuration. The default port is 623.

After entering all fields above, click <Save> to save the Network settings.

## 2.6.8 Configuring Dynamic DNS (Domain Name System) Settings

This feature allows you to configure DNS settings. When you click the Dynamic DNS icon in the Options Window, the following screen will display.




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

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

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

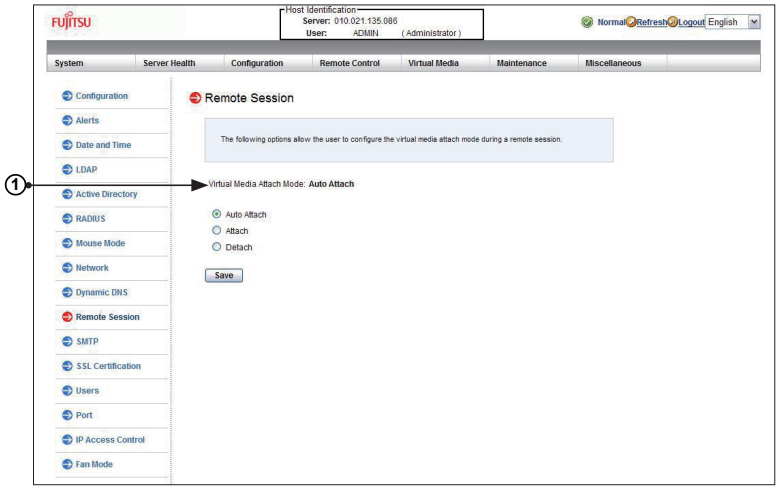
4. Check the box to enable TSIG Authentication support, and browse the files to select the *TSIG.key* file. (This item is optional.)

5. Browse the files to select the *TSIG.private* file. (This item is optional.)

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

### 2.6.9 Configuring the Remote Session Settings

This feature allows the user to enable or disable encryption support on IKVM, or to select the Virtual Media Attach mode for console redirection. When you click the Remote Session in the menu bar, the following screen displays.



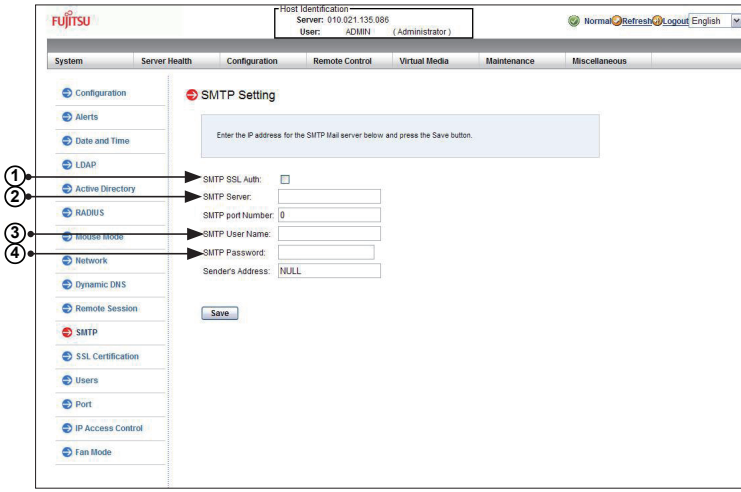

1. This item displays the current Virtual Media Attached mode. To change the Virtual Media Attached mode, select the desired setting from the list below.

   - 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 the BIOS when a device or an ISO image is connected through the virtual media wizard.
   - Attach: Select this mode to activate a virtual media and make it available for remote access. A virtual device will always be seen in the system BIOS even when it is not active.
   - Detach: Select this mode to disable virtual media for remote access.

After making selection, click <Save> to save the settings.

## 2.6.10 Configuring the SMTP Settings

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




To configure SMTP settings, follow the instructions below.

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

   **Note:** SHA2 and RSA 2048 bit SSL supported.

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

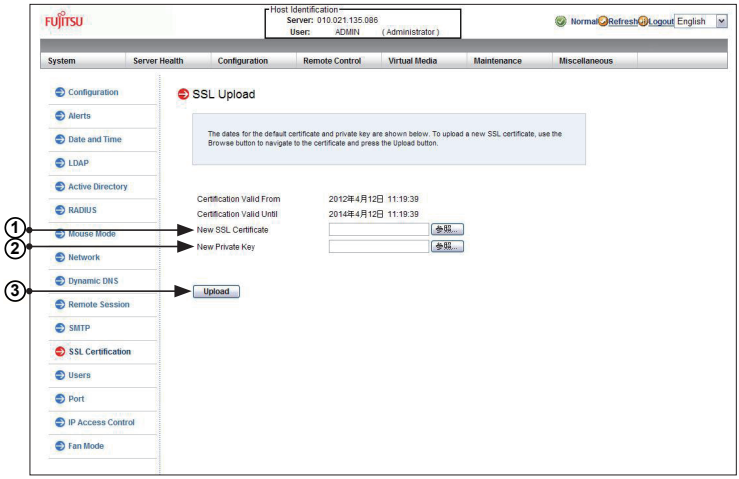
3. Enter the user name for your SMTP Mail server. (Optional)

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

After entering the information above, click <Save> to save the settings.

## 2.6.11 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. When you click the <SSL> icon in the Options window, the following screen will display.




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

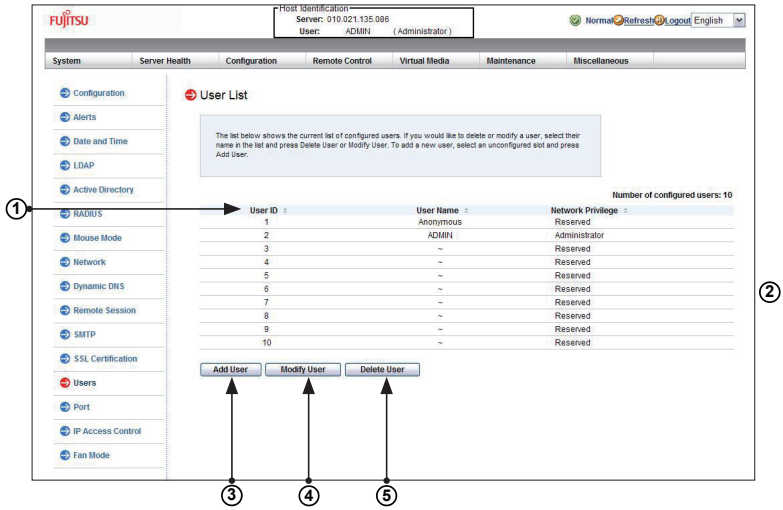
   **Note:** SHA2 and RSA 2048 bit SSL supported.

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

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

## 2.6.12 Configuring Users Settings

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




1. This item lists current user information, including User ID, User name 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 |

2. This item displays the number of the users that are set up for the network. The maximum of 10 user profiles can be made.

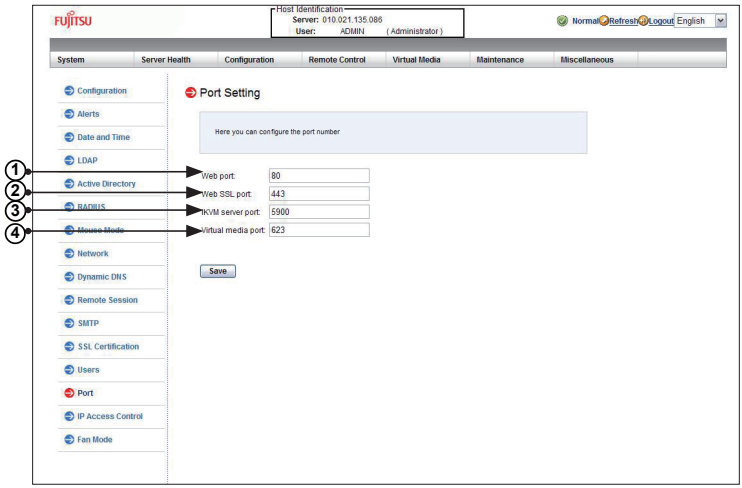
3. To add a new user to the network, click <Add User>. When prompted, select an empty slot from the users list to add an user.

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

### 2.6.13 Configuring Port Settings

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




1. Web Port: Enter the desired web port number.

2. Web SSL Port: Enter the Web SSL port number.

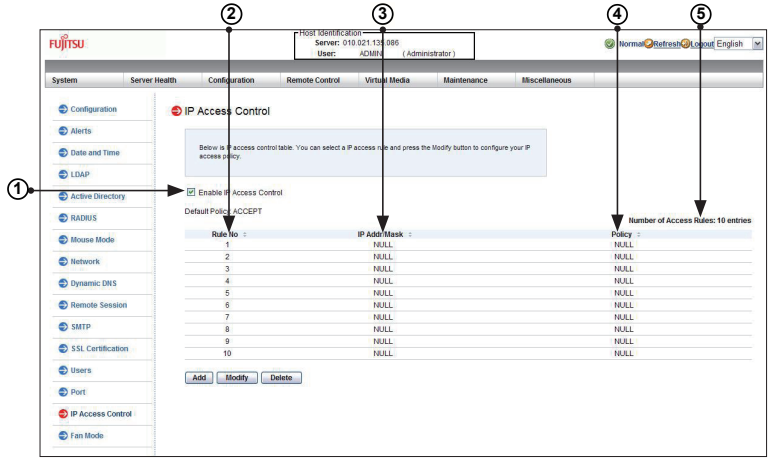
3. IKVM Port: Enter the desired IKVM port number.

4. Virtual Media Port: Enter the desired virtual media port number.

After configuring the port settings, click <Save> to save the settings.

## 2.6.14 IP Access Control

This page displays an IP Access Control table, which will allow you to add, modify and delete an IP Access rule, an IP Address/Mask setting or an IP access policy.



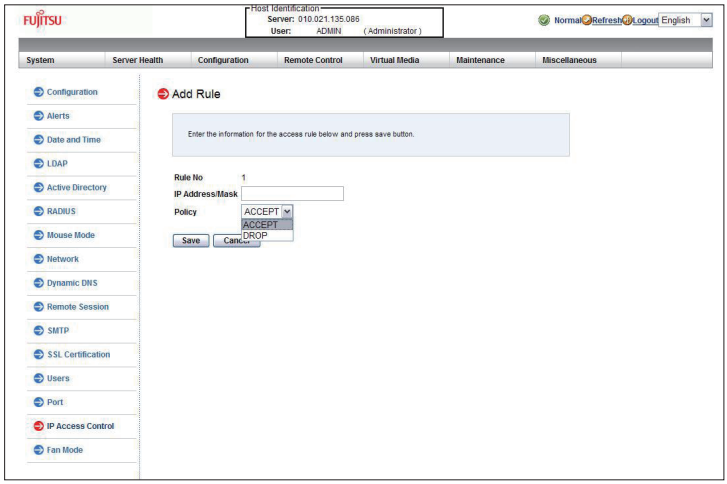

1. Check this box to configure IP Access Control settings. (The default setting is **Accept**.)

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

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

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

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




*Modifying IP Access Rules*

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

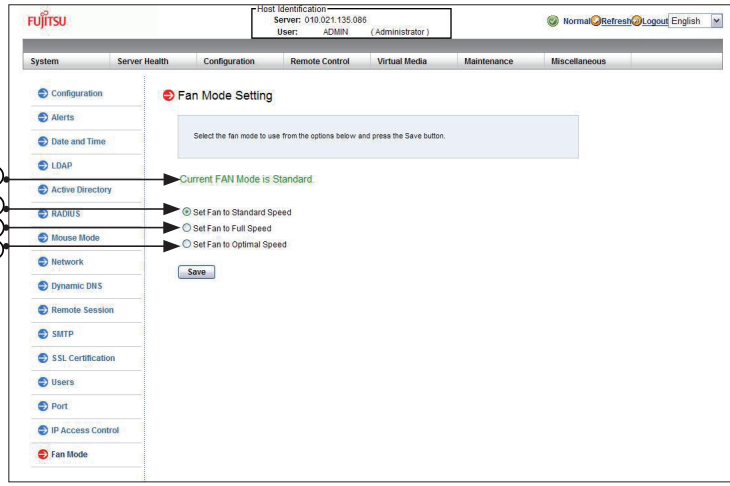
To modify a rule, enter the information needed for the following items:

- 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.

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

## 2.6.15 Configuring Fan Settings

This page allows you to configure fan mode settings. When you click the <Fan Mode> icon in the Options window, the following screen will display.




1. This item displays the current fan mode setting.

2. Check this radio button to use the standard fan speed setting for power-saving.

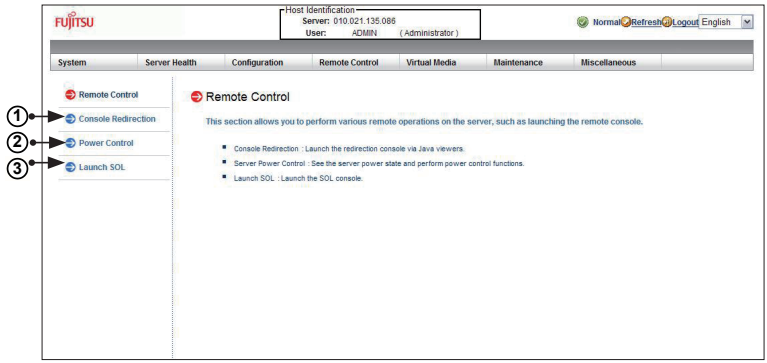
3. Check this button to use the full speed setting for optimal system performance.

4. Check this button to use the optimal fan speed setting which will adjust the fan speed by balancing the needs between system performance and power saving.

After configuring the fan speed setting, click <Save> to save the entry.

## 2.7 Remote Control

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




To launch remote console or to change to power settings of the remote console, follow the instructions below.

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

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

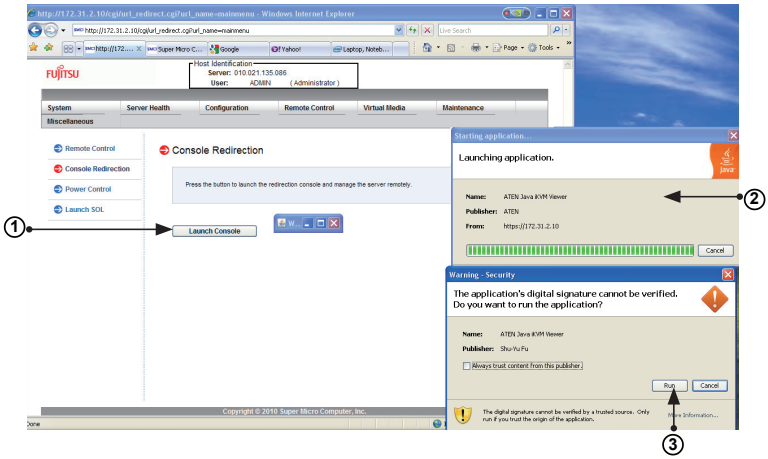
   - Reset Server
   - Power Off Server-Immediately
   - Power Off Server-Orderly Shutdown
   - Power On Server
   - Power Cycle Server

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

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

### 2.7.1 Launching Console Redirection

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



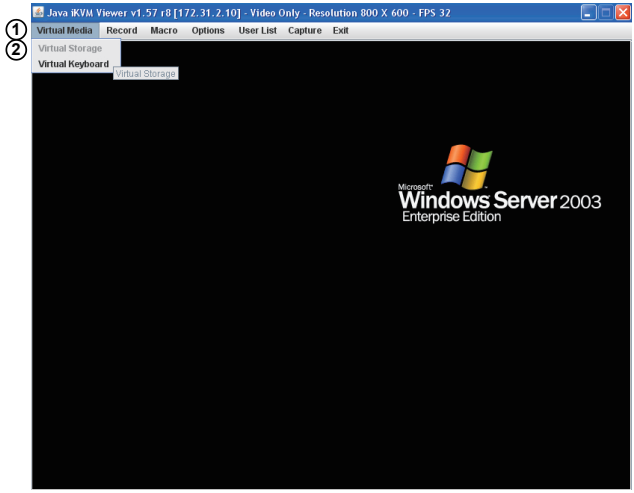

1. Click <Launch Console> on the Console Redirection screen to launch the remote console via Java or Active X (for the Internet Explorer). If it is blocked by the IE due to security reasons, click on the top of the menu bar and select <Download File>.

2. A screen will display to indicate that Java is launching.

3. When the warning screen as shown above displays, click <Run> to launch the remote console.

### *2.7.1.1 Console Redirection - Virtual Device*

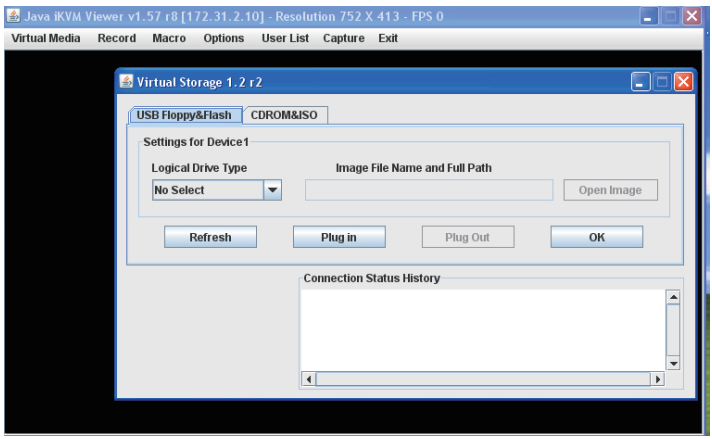
This feature allows you to configure Virtual Device settings for your console redirection. When you click the <Virtual Device> icon in the Menu bar, the video settings of the remote console will display as shown below.




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. When you click on this item, the screen as shown below displays.

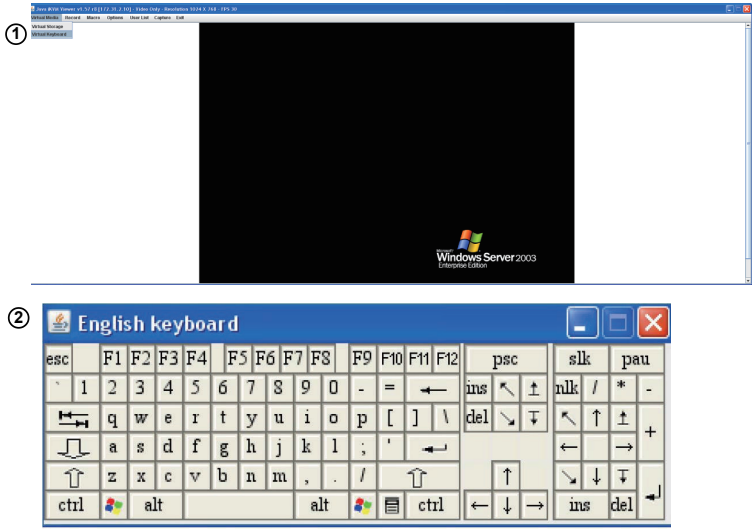
You can connect Floppy, USB Flash, CD-ROM, DVD ROM or ISO images using this feature.



### *Virtual Keyboard*

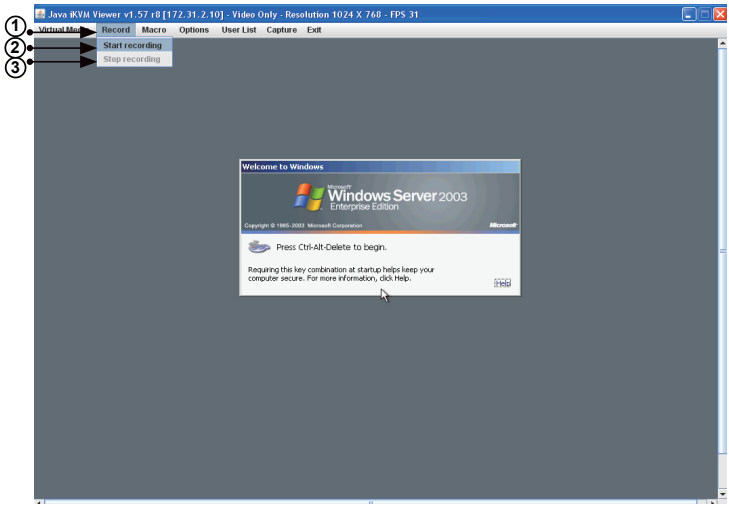
1. Click the <Virtual Keyboard> to use the onscreen Keyboard.

2. The screen above shows the Virtual Keyboard in English. Click a key on the keyboard for your BMC connection.



### *2.7.1.2. Console Redirection - Recording*

This feature allows you to record media displays for your console redirection. When you click the Record icon in the Menu bar, Record settings will be shown below.



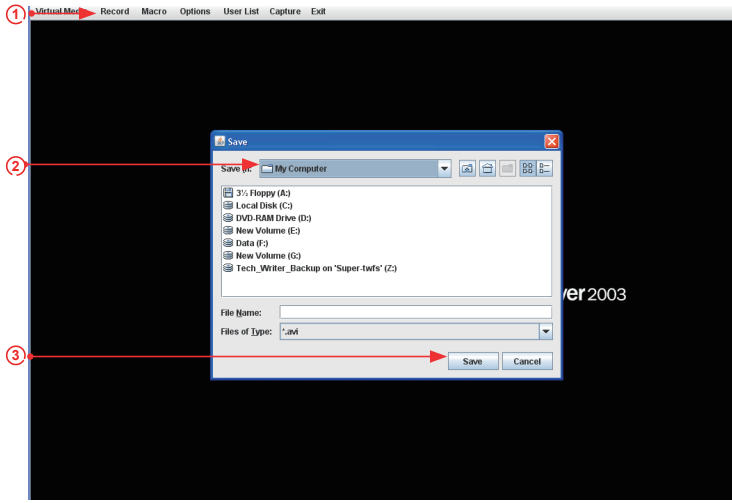

1. Click <Record> to use the recording features for your remote server. The features include the following.

2. Click <Start Recording> to start video recording from your remote server.

3. Click <Stop Recording> to stop video recording from your remote server.

### *2.7.1.3. Console Redirection - Recording*

This feature allows you to record the media displays. Click <Record> in the Menu bar to enable virtual media recording support.



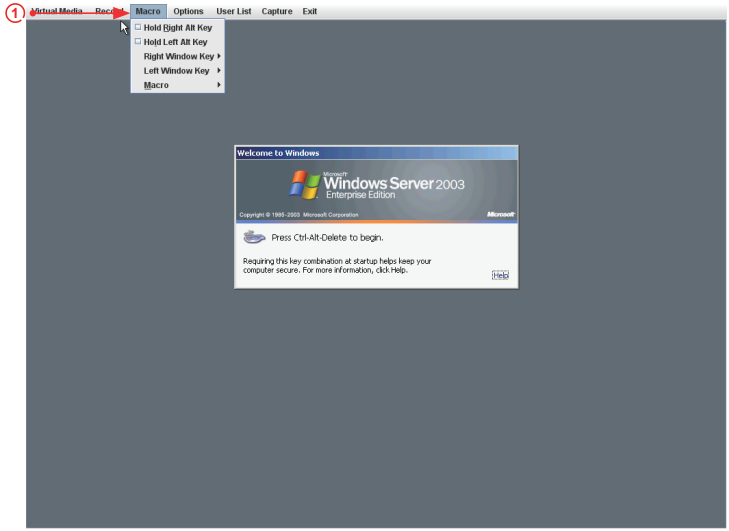

1. Click <Record> to enable media recording support. Click <Start Recording> to start recording.

2. From the pull-down menu, select the location where you want to save the recording.

3. Enter the filename and click <Save> to save the recording.

### *2.7.1.4. Console Redirection - Macro*

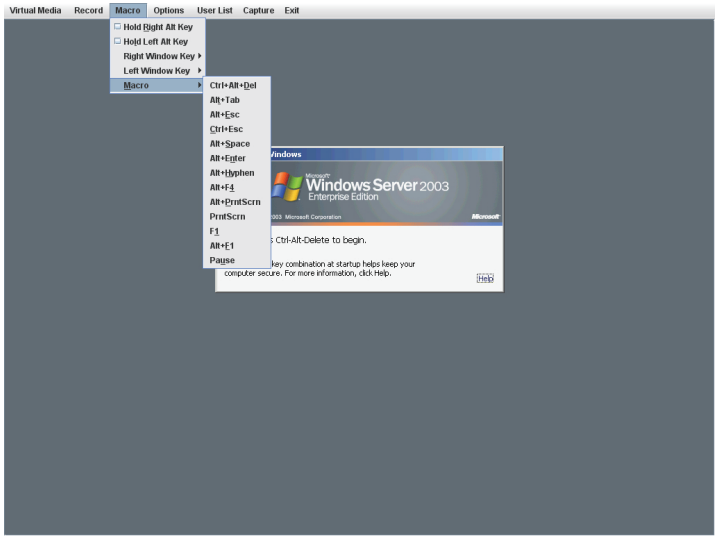
This feature allows you to configure Macro settings for your console redirection. When you click the <Macro> icon in the Menu bar, the macro settings screen will display as shown below.




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. Right click this item to select <Hold Down> or <Press & Release> for the Right Windows key.
- **Left Windows Key:** This item performs the same function as pressing the <Left Windows> key. Right click this item to select <Press Down> or <Press & Release> for the <Left Windows> key.
- **Macro:** Click this item to activate a pull-down submenu. The Macro Hotkey submenu includes the following items as shown on the next page.

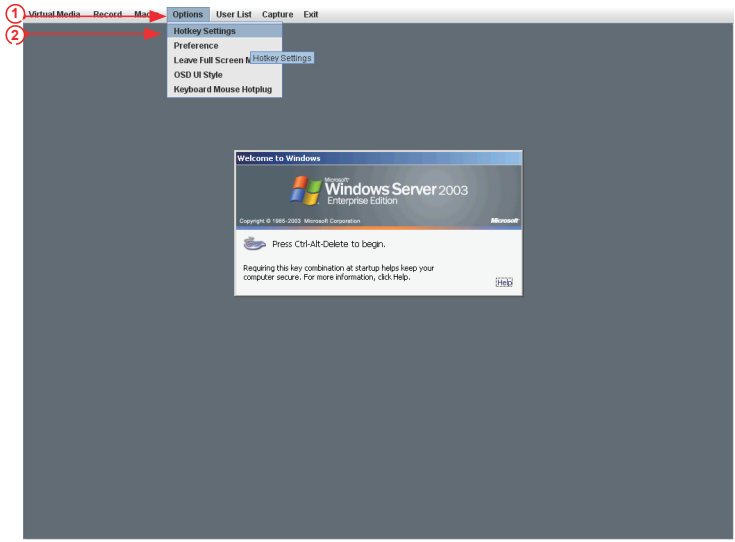
Click <Macro Hotkeys> to display the Macro Hotkey pop-up submenu. The hot keys include the following:




- CTRL + ALT + Del
- ALT + Tab
- ALT + Esc
- Ctrl + Esc
- ALT + Space
- ALT + Enter
- ALT + Hyphen
- ALT + F4
- ALT + Prnt Scrn
- Prnt Scrn
- F1
- Alt + F1
- Pause

### *2.7.1.5 Console Redirection - Options*

This feature allows you to configure *Options* settings for your console redirection. When you click the <Options> icon in the Menu bar, the Options menu will display as shown below.



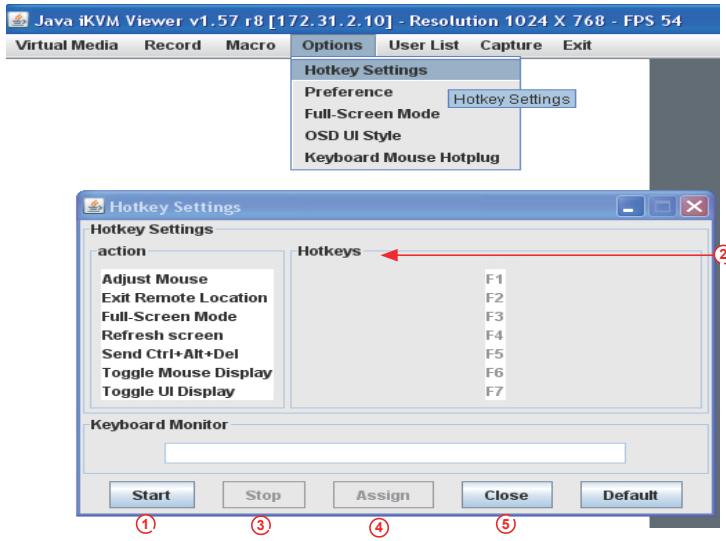

1. Click <Options> to activate the pull-down menu to configure *Options* settings.

2. The options menu allows you to configure the following settings.

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

### *2.7.1.5.1 Console Redirection - Options: Hotkey Settings*

This feature allows you to configure Hotkey settings for your console redirection. When you click the <Options-Hotkey> icon in the Menu bar, the Hotkey menu will display as shown below.

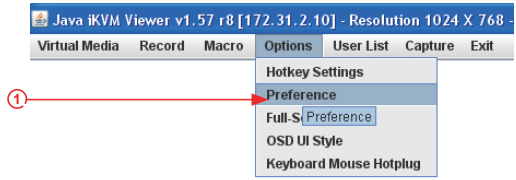


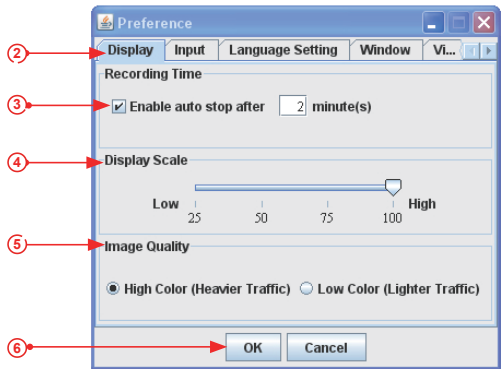

To assign a hotkey for an action, follow the steps below.

1. Click <Start>.
2. Enter the hotkey of your choice (-it can be a single word or a combination).
3. Click <Stop>.
4. Select an item from the action list and click <Assign>.
5. Click <Close> to exit.

### *2.7.1.5.2. Console Redirection - Options: Preference (-Display)*

This feature allows you to configure Video Recording Preference settings for your console redirection. When you click the <Preference> icon in the Menu bar, the Preference menu will display as shown below.




To configure the preference settings for video recording, please follow the instructions below.

1. Click <Preference> to invoke the Preference submenu which includes Display, Input, Language Setting, Window and Video Stream Control settings.

2. Click <Display> to configure Video Display features.

3. Check this box to enable Auto Stop support, which will allow the video recording to be automatically turned off after recording of certain period of time. After <Enable auto stop> is checked, enter the number of minutes upon which your video recording will be automatically turned-off.

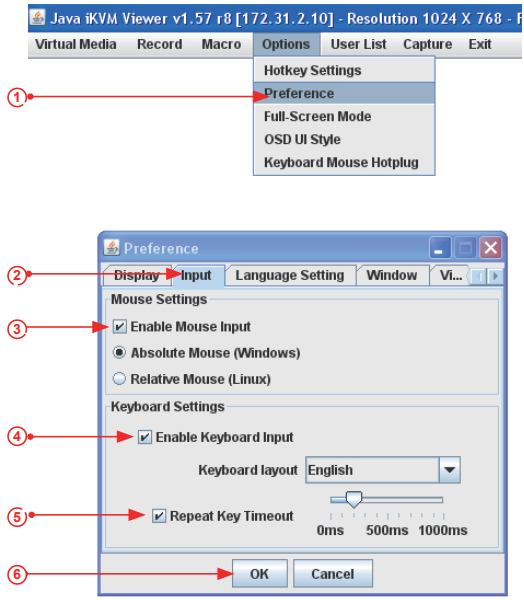
4. Use the slider on the Display Scale to set the appropriate scale setting for your video display from Low (25) to High (100).

5. To ensure the best image quality, select <High Color> for heavier network traffic connections; select <Low Color> for lighter network traffic.

6. Click <OK> to save the recording preference settings or click <Cancel> to cancel the selection.

### *2.7.1.5.3. Console Redirection - Options: Preference (-Input)*

This feature allows you to configure Video Recording input settings for your console redirection. Click <Input> in the menu bar to activate the Input submenu.




To configure Video Input settings, follow the instructions below.

1. Click <Preference> to invoke the Options submenu.

2. From the Options submenu, click <Input> to invoke the *Input* page to configure mouse and keyboard settings.

3. Check <Enable Mouse Input> to enable mouse support so that you can use the mouse as an input device. Once mouse support is enabled, set a proper mode for your console redirection.

   - Select *Absolute Mode* if you have the Windows OS
   - Select *Relative Mouse* for the Linux OS.

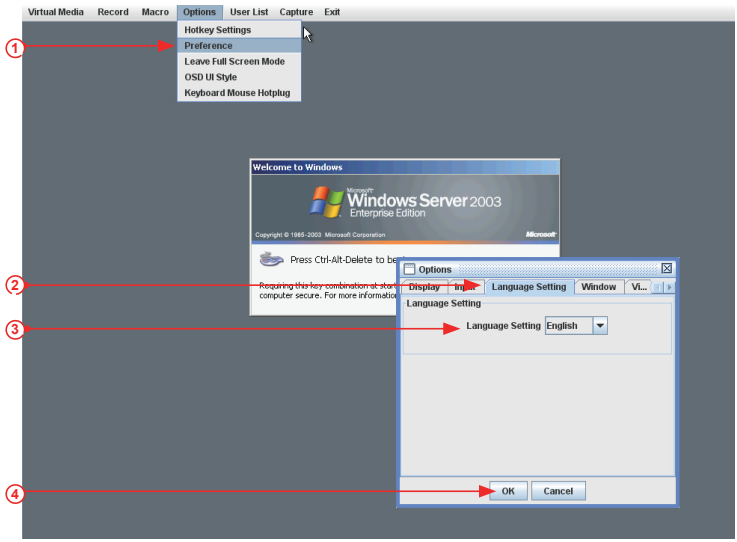
4. Select *Enable Keyboard Input* to enable keyboard support so that you can use soft keyboard as an input device. From the *Keyboard layout* pull-down menu, select the right language setting for your soft keyboard.

5. Use the slider on the *Repeat Key Timeout* scale to select the appropriate timeout settings for repeat keystrokes from 0ms to 1000ms (micro-second).

6. Click <Save> to save the keyboard setting or click <Cancel> to cancel it.

### *2.7.1.5.4. Console Redirection - Options: Preference (-Language Settings)*

This feature allows you to configure Language settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.




To select the correct language setting for your console, follow the steps below.

1. Select *Options* from the Menu bar. From the pull-down menu, select *Preference*.

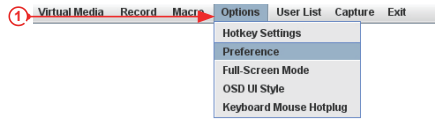
2. Click <Language Setting>.

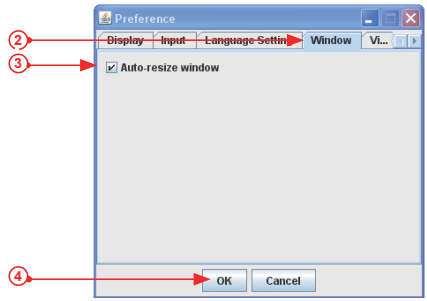
3. From the Language Setting pop-up menu, select the language you want to use for your console redirection. The language options include English, Chinese (Traditional), Japanese, German, French, Spanish, Korean, and Italian.

4. Once you have selected a language setting, click <OK> to use the language.

### *2.7.1.5.5. Console Redirection - Options: Preference (-Window)*

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.




To select the correct Window settings for your console redirection, follow the instructions below.

1. Select *Options* from the Menu bar. From the pull-down menu, select Preference.

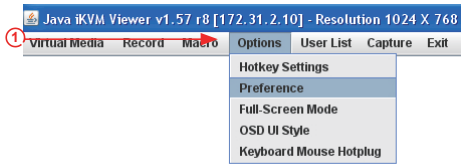
2. Click <Window>.

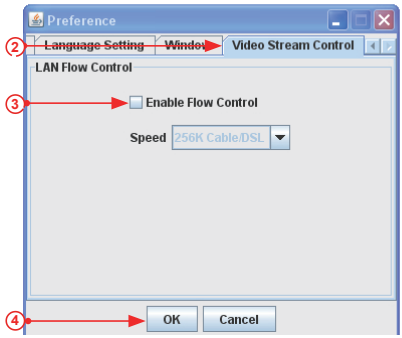
3. Check <Auto Re-size Window> for the system to reset the size of your display window. (If you do not wish your display window to be re-sized automatically, leave the box blank.)

4. Click <OK> to save the window settings.

### *2.7.1.5.6. Console Redirection - Options: Preference (-Video Stream Control)*

This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the Preference menu.



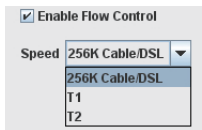




To select the correct Video Stream Control settings for your console redirection, follow the instructions below.

1. Select <Options> from the Menu bar. From the pull-down menu, select *Preference*.

2. Click <Video Stream Control>.

3. Check <Enable Flow Control> to provide support for video flow control. Once the Flow Control support is enabled, select the proper speed for video streaming from the pull-down menu. The speed settings listed below.

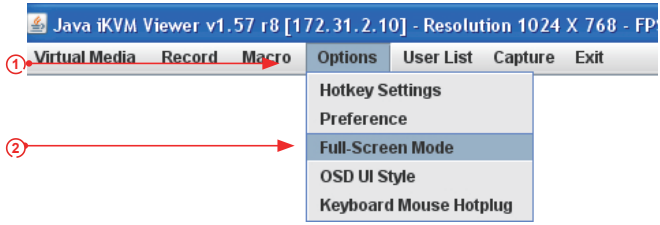



   - 256K Cable/DSL
   - T1
   - T2

4. Click <OK> to save the Video Stream Control setting.

### *2.7.1.5.7. Console Redirection - Options: Full Screen Mode*

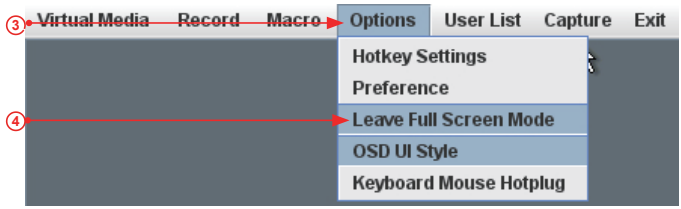
This feature allows you to configure Window settings for your console redirection. Click <Options> in the Menu bar to activate the submenu. From the pull-down menu, select *Full Screen Mode*.




- To Use a Full Screen Display

To set a full screen display for your console redirection, follow the instructions below.

1. Select <Options> from the menu bar to activate the submenu.
2. Select <Full Screen Mode> from the pull-down menu. Then, press <Enter>. A full-screen display will appear.

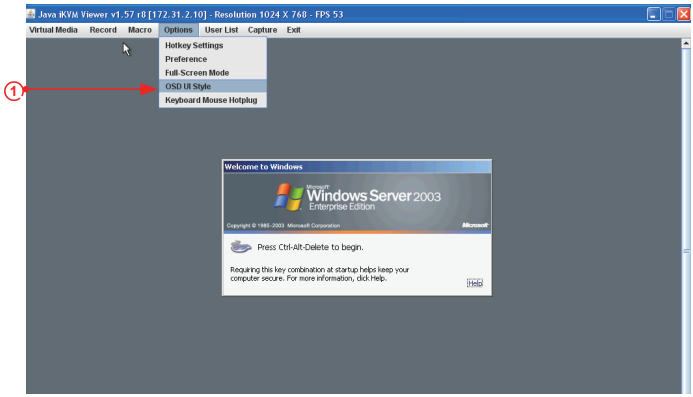



- To Leave the Full Screen Display

3. To leave the full screen display, click <Options> to activate its submenu.
4. From the pull-down submenu, select <Leave Full Screen> and press <Enter>.

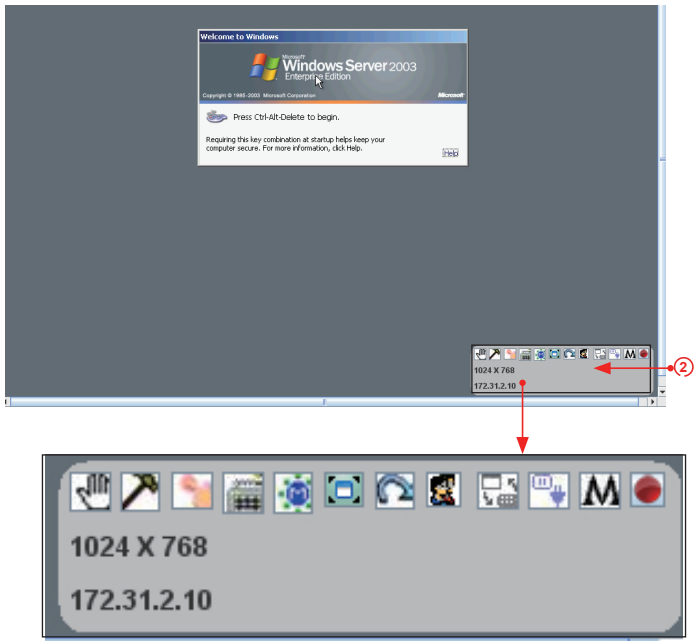
### *2.7.1.5.8 Console Redirection - Options: OSD UI Style*

This feature allows you to configure OSD (On-screen Display) UI (User-Interface) Style settings for your console redirection. To configure the OSD UI settings, follow the steps below.




1. From the Options pull-down menu, click <OSD UI Style> to display the OSD UI Style screen as shown below. This screen provides shortcuts to the main features provided by the firmware for your console redirection.

2. Click an <OSD UI_Style> icon to change the settings listed on the next page.




*The OSD UI Style Screen Close-up*


*The OSD UI Style Screen Close-up*

1. **Move OSD UI Screen:** Click this icon to move the OSD UI Screen to a new location on the display.

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

3. **Virtual Media:** Click this item to access the Virtual Media submenu and configure the settings.

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

5. **Preferences submenu:** Click this item to access the References submenu as indicated in the previous sections.

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

7. **Exit Remote Console:** Click this item to exit from the remote connection.

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

9. **Change Toolbar Display:** Click this item to change the toolbar display format.

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

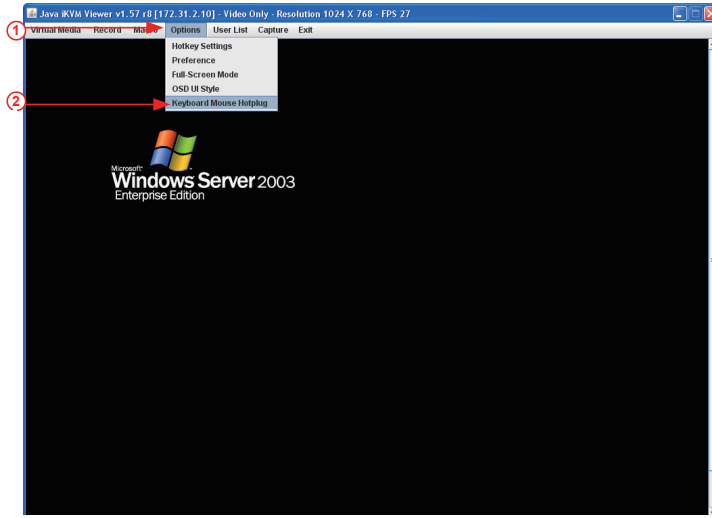
11. **Macro:** Click this item to enable Macro support and use Macro features.

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

13. **Image Size:** This item displays the image size in pixel.

14. **IP Address:** This item displays the IP Address of IPMI.

### *2.7.1.5.9 Console Redirection - Keyboard/Mouse Hotplug*

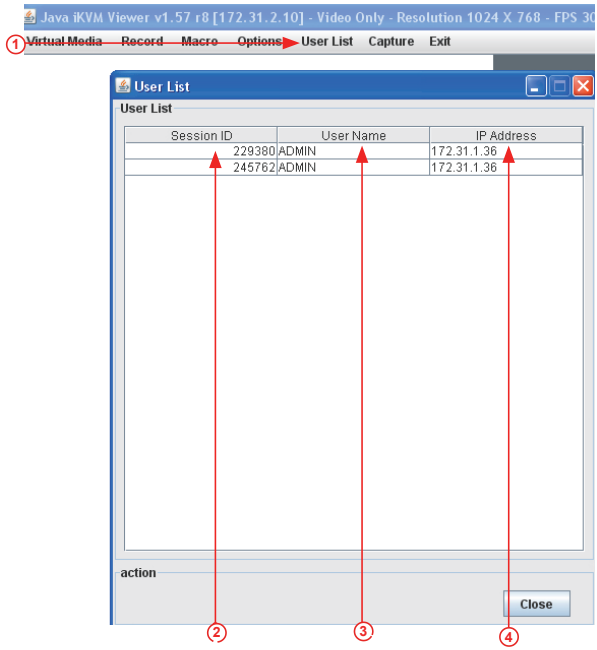



1. Click <Options> on the menu bar to invoke the pull-down submenu.

2. Click <Keyboard/Mouse Hotplug> from the pull-down menu to enable keyboard/ mouse hotplug support for your console redirection.

### *2.7.1.6 Console Redirection - User List*

This feature allows you to access the user list. To configure User List settings, follow the instructions below.




1. From the menu bar, click <User List> to display the User List screen as shown above.

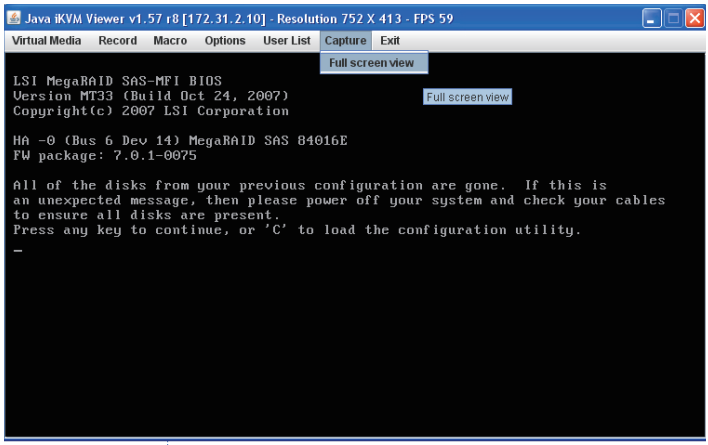
2. **Session ID:** This item displays the current session ID#.

3. **User Name:** This item displays the name(s) of the user(s).

4. **IP Address:** This item displays the IP Address of the client server.

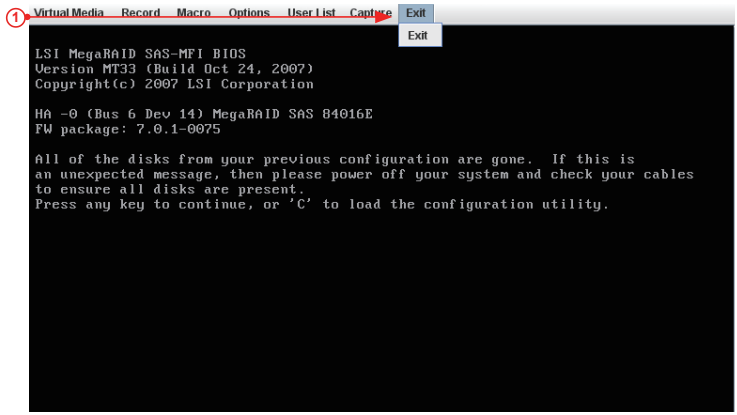
### *2.7.1.7 Console Redirection - Capture*

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

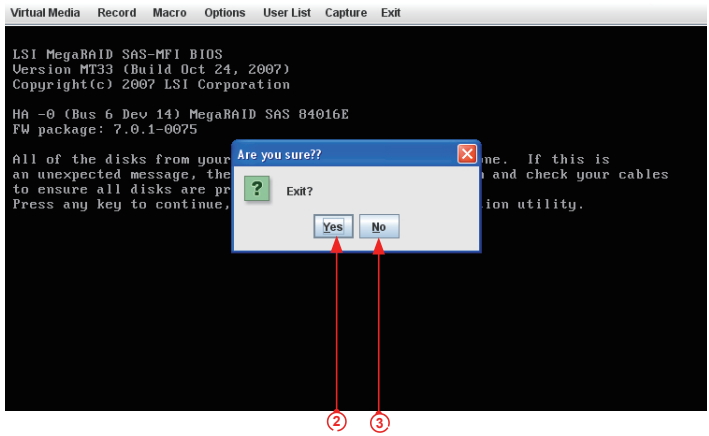



1. Click "Capture" in the Menu bar. The Capture submenu will display as shown above
2. From the pull-down menu, select "Full Screen" video display for your remote console.

### *2.7.1.8 Console Redirection - Exit*




1. To exit from Console Redirection, click <Exit>.

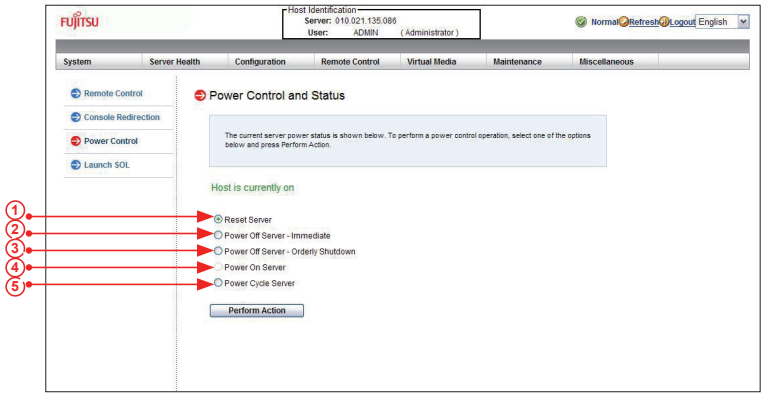



2. At the prompt- "Are you sure?", click <Yes> to exit from remote redirection.

3. Click <No> to return to the current session.

### 2.7.2 Remote Control - Server Power Control

This feature allows the user to check power state and perform remote power control.




1. Click <Reset Server> and press <Perform Action> to reset the host server.

2. Click <Power Off Server - Immediately> and press <Perform Action> to power off the remote server immediately.

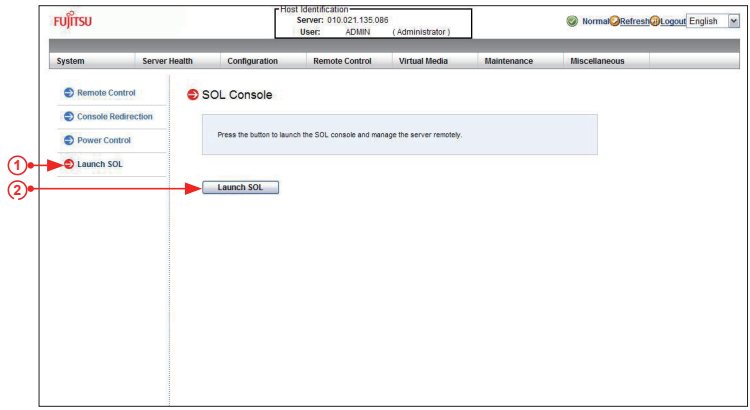
3. Click <Power Off Server - Orderly Shutdown> and press <Perform Action> to power off and shutdown the remote server orderly.

4. Click <Power On Server> and press <Perform Action> to power on the remote server.

5. Click <Power - Cycle Server> and press <Perform Action> to reset the power cycle of the remote server.

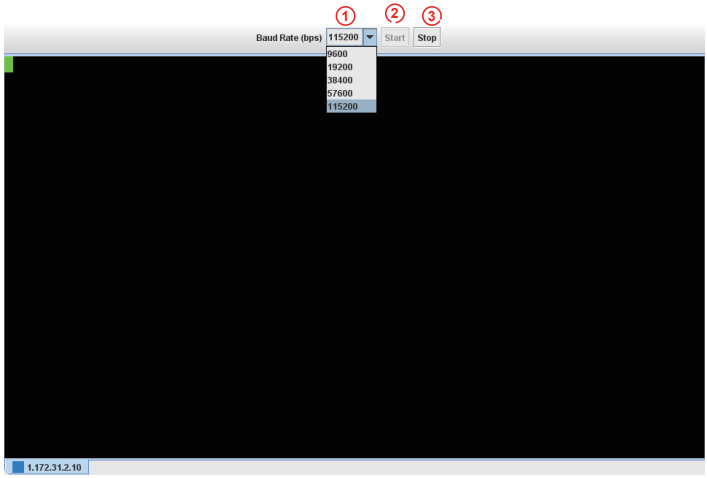
### 2.7.3 Remote Control-Launch SOL

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. To launch SOL, follow the instructions below.




1. Click <Launch SOL> in the left Options window to enable SOL (Serial Over LAN) support.

2. Click the <Launch SOL> button to launch SOL. After SOL is launched, the following screen will display as shown on the next page.




**Launching SOL**

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.

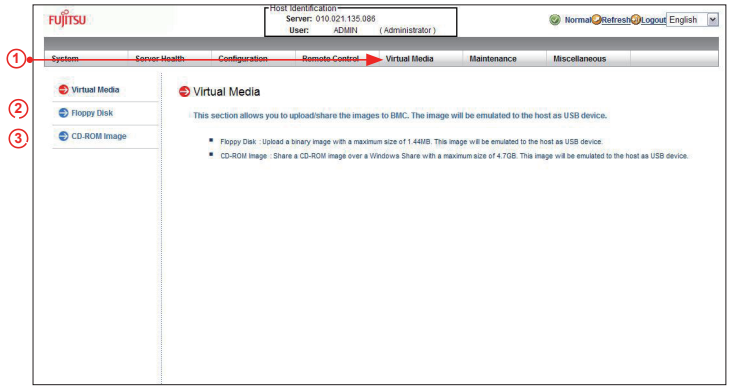
   - 9600 bps (bit-per-second)
   - 19200 bps
   - 38400 bps
   - 57600 bps
   - 115200 bps
   - Manufacture Default.

2. Once you've selected the Baud rate, press <Start> to start the session.

3. You can also press <Stop> to stop SOL connection.

## 2.8 Virtual Media

This feature allows you to upload and share images via the BMC (Baseboard Management Controller). These images will be emulated to the host server as USB applications. To follow the Virtual Media settings, follow the instructions below.



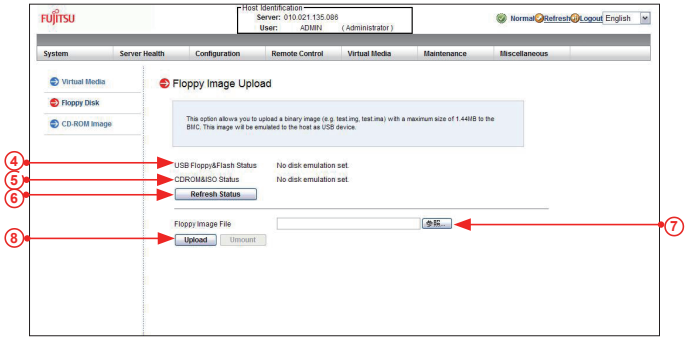

1. Click <Virtual Media> to configure virtual media settings for your remote console, including Floppy Disk and CD-ROM image settings.

2. Click <Floppy Disk> on the Options Window to configure the floppy disk settings for your console redirection. The Floppy Disk screen will display as shown on the next page.

3. Click <CD-ROM Image> to configure CD-ROM image settings for your console redirection. When you click on this item, the screen on Page 2-59 displays.

### 2.8.1 Configuring USB Floppy & Flash Device Settings

To configure CD ROM image files for sharing, follow the instructions below.




4. *USB Floppy & Flash Status* displays the status of a USB floppy or a flash device.

5. *CDROM & ISO Status* displays the status of a CDROM or an ISO device.

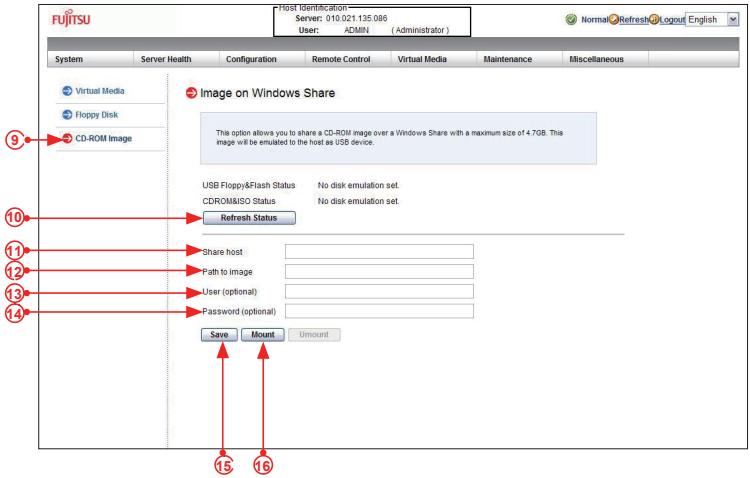
6. Click <Refresh Status> to refresh the USB floppy or the flash device.

7. Click <Browse> to select an image file from your data base for your console redirection.

8. After you've selected your image file, click <Upload> to upload your image file to the server.

## 2.8.2 Configuring CD ROM Image File Settings

To configure CD ROM image files for sharing, follow the instructions below.




9. Click <CD-ROM Image File> to invoke the <Image on Windows Share> screen as shown above. The following items will display.

- *USB Floppy & Flash Status* indicates the status of a USB floppy or a flash device.
- *CD ROM & ISO Status* indicates the status of a CD-ROM or an ISO device.

10. Click <Refresh Status> to refresh *USB Floppy/Flash* and *CD ROM/ISO* devices.

11. Enter the *Share Host* server for your console redirection.

12. In the *Path to Image* field, enter the path to the CD-ROM image file for sharing.

13. In the *Users (Optional)* field, specify the users that have access to the CD-ROM image files. (This item is optional).

14. In the *Password (Optional)* field, enter your user password. (Optional.)

15. To *mount* an image file, follow the steps below.

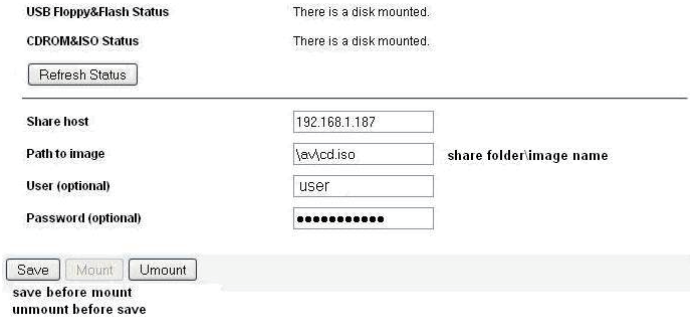
    1. Click <Save>.

    2. Click <Mount>.

3. To *unmount* an image file, follow the steps below.

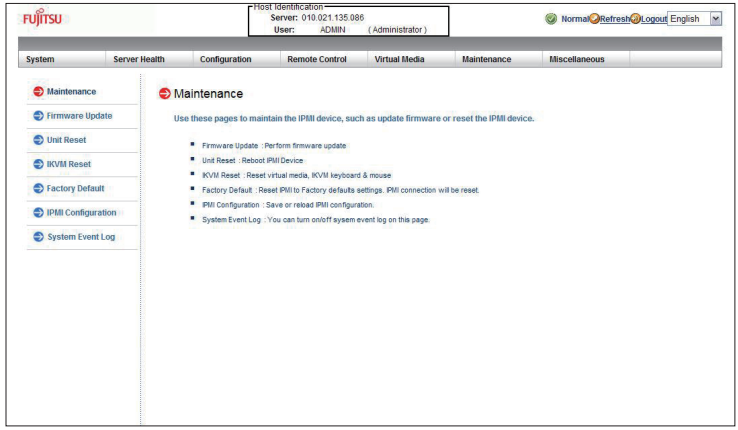
   1. Click <Unmount>.

   2. Click <Save>.



## 2.9 Maintenance

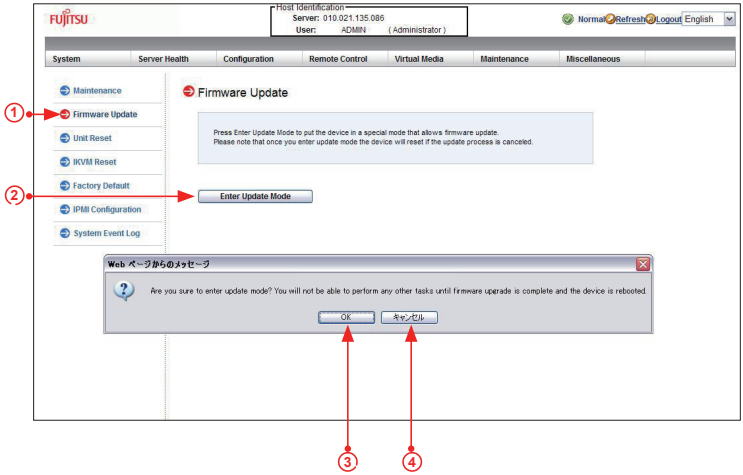
Use this feature to manage and configure IPMI device settings.




Click the <Maintenance> icon in the menu bar to invoke the *Maintenance* main screen as shown above. The *Maintenance* menu includes the following items.

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

### 2.9.1 Maintenance - Firmware Update




**Firmware Update**

To update IPMI Firmware, follow the instructions below.

1. Click <Firmware Update> in the Options Window.

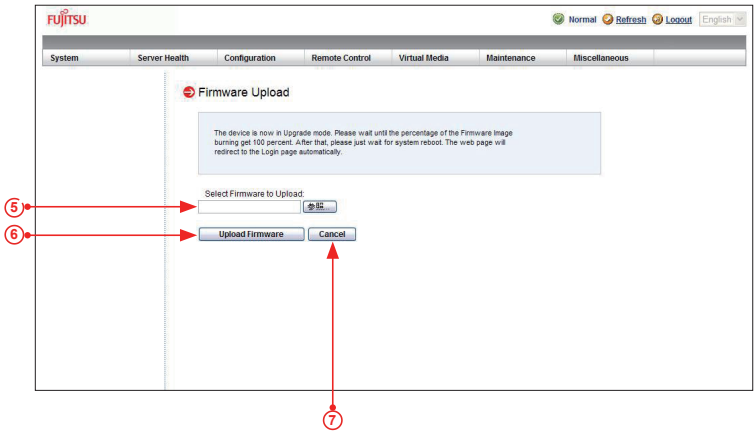
2. Click <Enter Update Mode> to enter the update mode. A warning message will display.

   **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. Once you've clicked OK to update the firmware, the *Firmware Upload* screen will display as shown on the next page.

4. Click <Cancel> to cancel firmware updates.

Once you have clicked <OK> to update the IPMI Firmware, the following Firmware Upload screen will display as shown below.




5. Enter the name of the firmware you wish to upload. You can also select a firmware from the pull-down menu to upload.

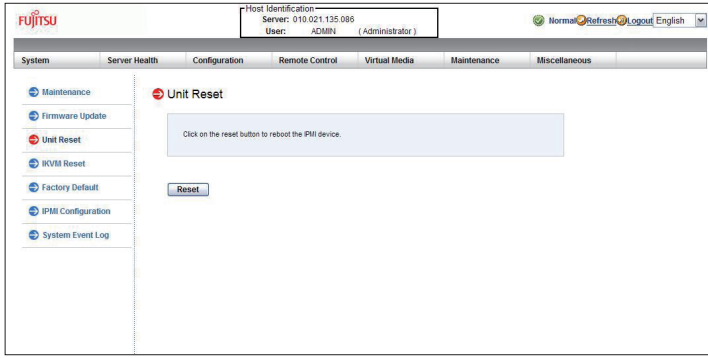
6. Click <Upload Firmware> to upload the selected firmware to the host server.

> **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.

7. Click <Cancel> to abort firmware uploading.

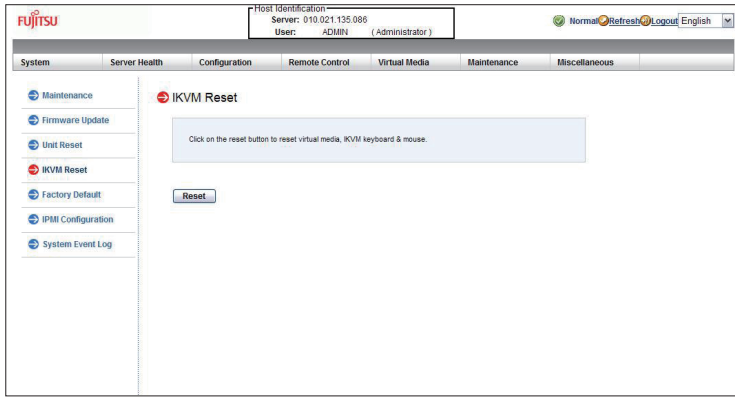
### 2.9.2 Maintenance - Unit Reset

Use this feature to reset the IPMI device.



### 2.9.3 Maintenance - IKVM Reset

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




To reset these devices, follow the instructions below.

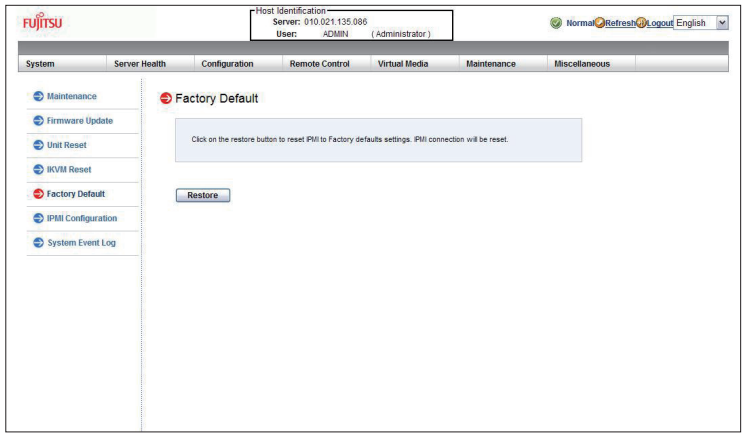
1. Click the Maintenance icon in the menu bar, the Maintenance Main page will display as shown above.

2. Click "IKVM Reset" in the Options Window to enable Unit-Reset support

3. Press the "Reset" button to reset virtual media, keyboard and mouse devices.

### 2.9.4 Maintenance - Factory Default

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



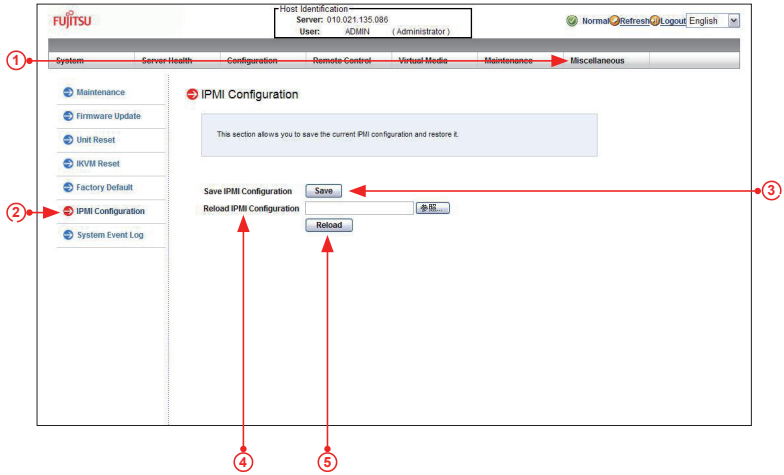

1. Click the Maintenance icon in the menu bar, the Maintenance Main page will display as shown above.

2. Click "Factory Default" in the Options Window to enable default setting support

3. Press the "Restore" button to restore the IPMI settings to the factory default settings.

## 2.9.5 Maintenance - IPMI Configuration

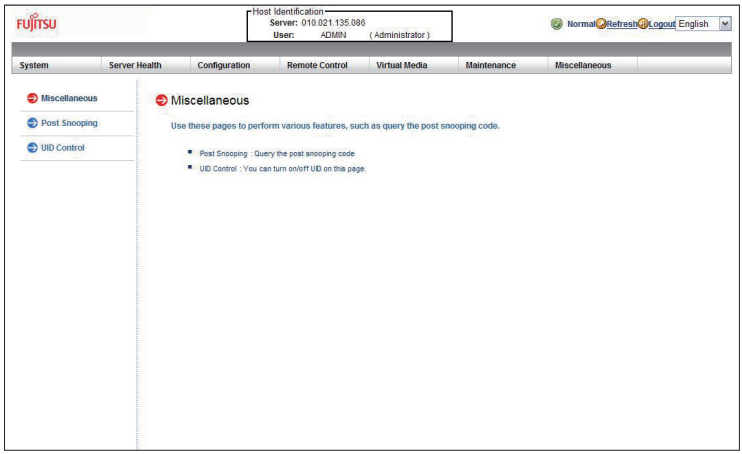
This feature allows the user to save IPMI configuration settings. To save the IPMI configuration settings, follow the instructions below.




1. From the top menu bar, select *Maintenance*.
2. Select *IPMI Configuration* on the left of the screen.
3. Click *Save* to save the IPMI Configuration settings.
4. From the Reload pull-down menu, select an IPMI Configuration setting to reload.
5. Click *Reload* to reload the IPMI Configuration Setting.

## 2.10 Miscellaneous

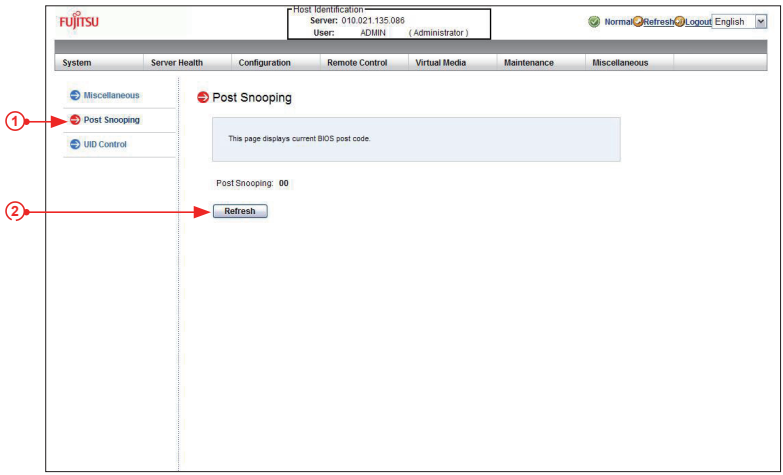
This feature allows the user to perform various network activities including POST (Power-On-Self Test) code query and turning-on/-off UID control. To query POST codes or to turn on/off UID control, follow the instructions below.




### 2.10.1 Miscellaneous - POST Snooping

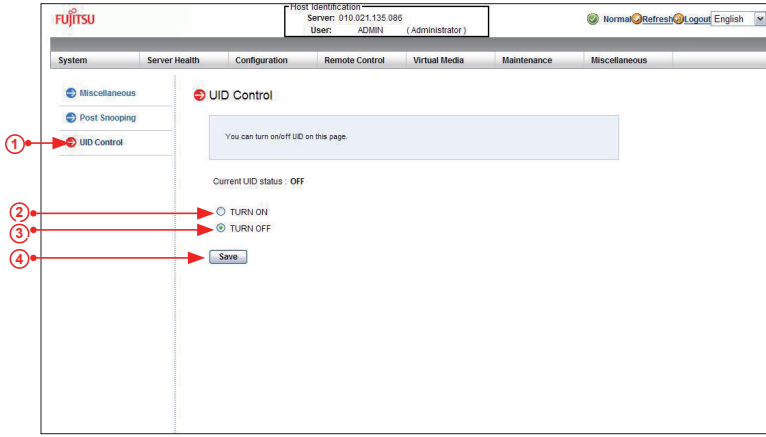
1. Click <Post Snooping> in the Options window. The *Post Snooping* screen will display as shown above.

2. Click <Refresh> to query the POST Snooping code for BIOS LPC Port80.



## 2.10.2 Miscellaneous - UID Control

This feature allows the user to turn-on or turn-off UID (Unit Identification) control. To turn on or off UID control, follow the instructions below.




1. Click <UID Control> in the *Options* window. The <UID Control> screen will display as shown above. It will also show the current UID Control status.

2. Click <Turn On> to turn on UID control.

3. Click <Turn Off> to turn off UID control.

4. Click <Save> to save the setting.

## Notes

# Chapter 3

# Frequently Asked Questions

## 3.1 Frequently Asked Questions

**A. Question: If I am using a firewall for my network connections, which ports should I open so that I can access my IPMI connection?**

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

HTTP: 80 (TCP)

HTTPS: 443 (TCP)

IPMI: 623 (UDP)

Remote console: 5900 (TCP)

Virtual media: 623 (TCP)

SMASH: 22 (TCP)

WS-MAN: 8889 (TCP)

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

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

## Notes

# Appendix A

# Introduction to SMASH

## A-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 will allow 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.

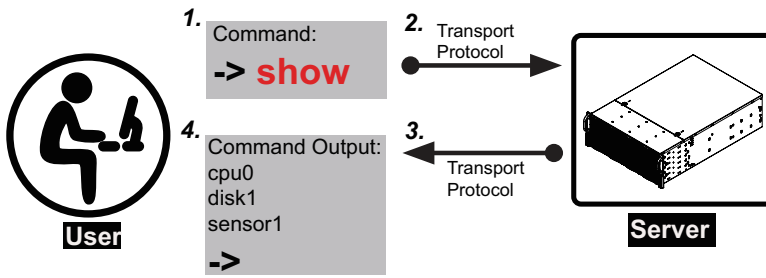



**Figure 1 SMASH-CLP User Interface**

### 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)

## A-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.

## A-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.

## A-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.

## A-5 SMASH-CLP Main Screen

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

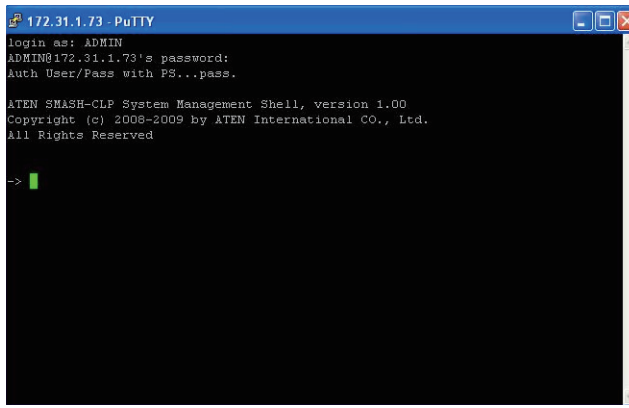



**Figure 2 SMASH-CLP Main Screen**

## A-6 Using SMASH for System Management

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

**Note:**

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

- A ***Verb*** means a *command*.
- An ***Option*** works according to the definition of a command given in Section 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.

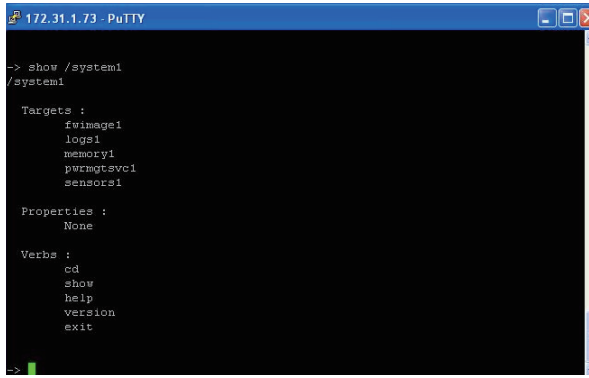



**Figure 3 Using SMASH for System Management**

## A-7 Definitions of Command Verbs

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

- ***cd***

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

- ***show***

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

- ***exit***

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

- ***help***

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

- ***Version***

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

- ***set***

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

- ***start***

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

- ***stop***

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

- ***reset***

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

- ***delete***

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

- ***load***

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

- ***dump***

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

- ***create***

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

## A-8 SMASH Commands

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

**Table 1 SMASH Commands**

## A-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**

## A-10 Target Addressing

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

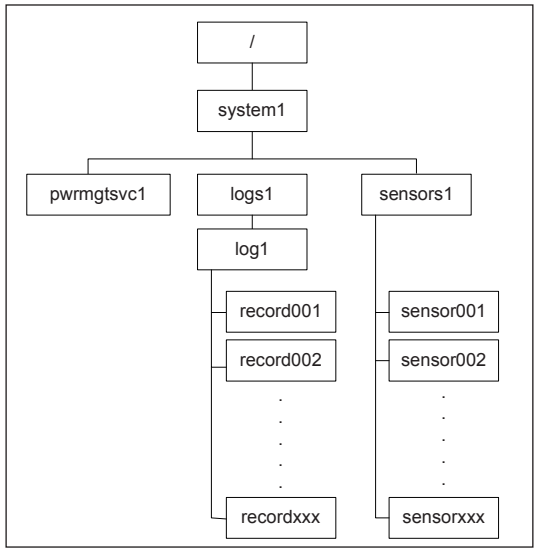



**Figure 4 Target Addressing Diagram**

### Terms Used in the Target Addressing Diagram

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

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

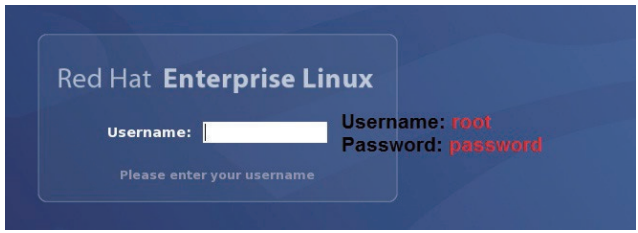
## Notes

# Appendix B

# 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

4. Configure Client information.

# vi /etc/raddb/client.conf

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

5. Configure Port information.

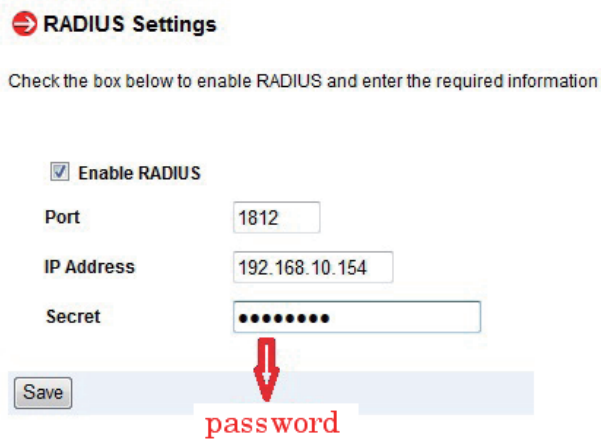
# vi /etc/raddb/radiusd.conf

```
#  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
```

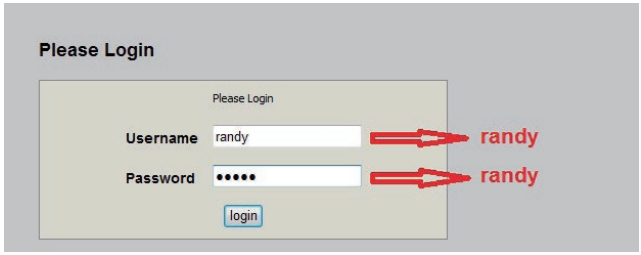
6. Start RADIUS service.

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

7. Enable RADIUS in the IPMI web page.



8. Logout ADMIN and try to login using a RADIUS account



## Notes

(continued from front)