SUPER®

X9 SMT IPMI

User's Guide

Revision 1.0

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, and makes no commitment to update or to keep current the information in this manual, or to notify any person or organization of the updates. **Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.**

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software and documentation, is the property of Supermicro and/or its licensors, and is supplied only under a license. Any use or reproduction of this product is not allowed, except as expressly permitted by the terms of said license.

IN NO EVENT WILL SUPER MICRO COMPUTER, INC. BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, SPECULATIVE OR CONSEQUENTIAL DAMAGES ARISING FROM THE USE OR INABILITY TO USE THIS PRODUCT OR DOCUMENTATION, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN PARTICULAR, SUPER MICRO COMPUTER, INC. SHALL NOT HAVE LIABILITY FOR ANY HARDWARE, SOFTWARE, OR DATA STORED OR USED WITH THE PRODUCT, INCLUDING THE COSTS OF REPAIRING, REPLACING, INTEGRATING, INSTALLING OR RECOVERING SUCH HARDWARE, SOFTWARE, OR DATA.

Any disputes arising between manufacturer and customer shall be governed by the laws of Santa Clara County in the State of California, USA. The State of California, County of Santa Clara shall be the exclusive venue for the resolution of any such disputes. Supermicro's total liability for all claims will not exceed the price paid for the hardware product.

FCC Statement: Refer to Supermicro's web site for FCC Compliance Information.

California Best Management Practices Regulations for Perchlorate Materials: This Perchlorate warning applies only to products containing CR (Manganese Dioxide) Lithium coin cells. “Perchlorate Material-special handling may apply. See www.dtsc.ca.gov/hazardouswaste/perchlorate”.

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

Manual Revision 1.0

Release Date: January. 16, 2013

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 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 and to prevent bodily injury.

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

Contacting Supermicro

Headquarters

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

Europe

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

Asia-Pacific

Address: Super Micro Computer, Inc.
4F, No. 232-1, Liancheng Rd
New Taipei City 235
Taiwan
Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3991
Web Site: www.supermicro.com.tw
Technical Support:
Email: support@supermicro.com.tw
Tel: +886-(2)-8226-3990

Notes

Table of Contents

Preface

Chapter 1 Introduction 1-1

1.1 Overview of the Nuvoton WPCM450 BMC Controller 1-1

WPCM450 DDR2 Memory Interface 1-1

WPCM450 PCI System Interface 1-1

Supermicro IPMI Features 1-2

1.2 WPCM450 Block Diagram 1-3

1.3 Introduction to the IPMI Platform 1-3

1.4 Motherboards Supported 1-4

1.5 An Important Note to the User 1-4

Chapter 2 Configuring the IPMI Settings 2-1

2.1 Configuring BIOS 2-1

2.2 Configuring IP Addresses Using the IPMICFG Utility 2-4

2.3 Connecting to the Remote Server 2-6

Using the IPMIView to Connect to the Remote Server 2-6

Using the Browser to Connect to the Remote Server 2-6

2.4 Accessing the Remote Server Using the Browser 2-7

To Log In to the IPMI Web GUI 2-7

2.5 IPMI Main Screen 2-8

2.6 System 2-9

2.7 Server Health 2-10

2.7.1 Sensor Readings 2-11

2.7.2 Event Log 2-13

2.8 Configuration 2-14

2.8.1 Configuring the Alerts Settings 2-16

2.8.2 Configuring Date and Time Settings 2-18

2.8.3 Configuring LDAP (Light-Weight Directory Access Protocol) Settings 2-19

2.8.4 Active Directory Settings 2-20

2.8.5 Configuring the RADIUS Settings 2-22

2.8.6 Configuring the Mouse Mode Settings 2-23

2.8.7 Configuring Network Settings 2-24

2.8.8 Configuring Dynamic DNS (Domain Name System) Settings 2-26

2.8.9 Configuring the Remote Session Settings 2-27

2.8.10 Configuring the SMTP Settings 2-28

2.8.11 Configuring the SSL (Secure Sockets Layer) Certification 2-29

2.8.12 Configuring Users Settings 2-30
2.8.13 Configuring Port Settings 2-32
2.8.14 IP Access Control 2-33
2.8.15 Configuring Fan Settings 2-35
2.9 Remote Control 2-36
2.9.1 Launching Console Redirection 2-37
2.9.2 Remote Control - Server Power Control 2-55
2.9.3 Remote Control > Launch SOL 2-56
2.10 Virtual Media 2-58
2.10.1 Configuring USB Floppy & Flash Device Settings 2-59
2.10.2 Configuring CD ROM Image File Settings 2-60
2.11 Maintenance 2-61
2.11.1 Maintenance > Firmware Update 2-62
2.11.2 Maintenance > Unit Reset 2-65
2.11.3 Maintenance > IKVM Reset 2-66
2.11.4 Maintenance > Factory Default 2-67
2.11.5 Maintenance > IPMI Configuration 2-68
2.12 Miscellaneous > POST Snooping 2-69
2.12.1 Miscellaneous > UID Control 2-70
Chapter 3 Frequently Asked Questions 3-1
3.1 Frequently Asked Questions 3-1
Appendix A Flash Tools A-1
A-1 Overview A-1
A-2 Reference A-1
A-3 Using SMT Flash Tools in the DOS Environment A-1
Firmware Updating via KCS Channels A-2
Dumping Firmware from the BMC via KCS channels A-3
A-4 Windows/Linux Version of Flash Tools A-4
Appendix B Introduction to SMASH B-1
B-1 Overview B-1
How SMASH works B-1
SMASH Compliance Information B-2
B-2 An Important Note to the User B-2
B-3 Using SMASH B-3
B-4 Initiating the SMASH Protocol B-3
To Initiate SMASH Automatically B-3
B-5 SMASH-CLP Main Screen B-4
B-6 Using SMASH for System Management B-4
B-7 Definitions of Command Verbs B-5

B-8 SMASH Commands B-7
B-9 Standard Command Options..B-8
B-10 Target Addressing B-9
Terms Used in the Target Addressing Diagram B-9
Appendix C RADIUS Setup Guidelines.. C-1

Chapter 1

Introduction

1.1 Overview of the Nuvoton 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 motherboard 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

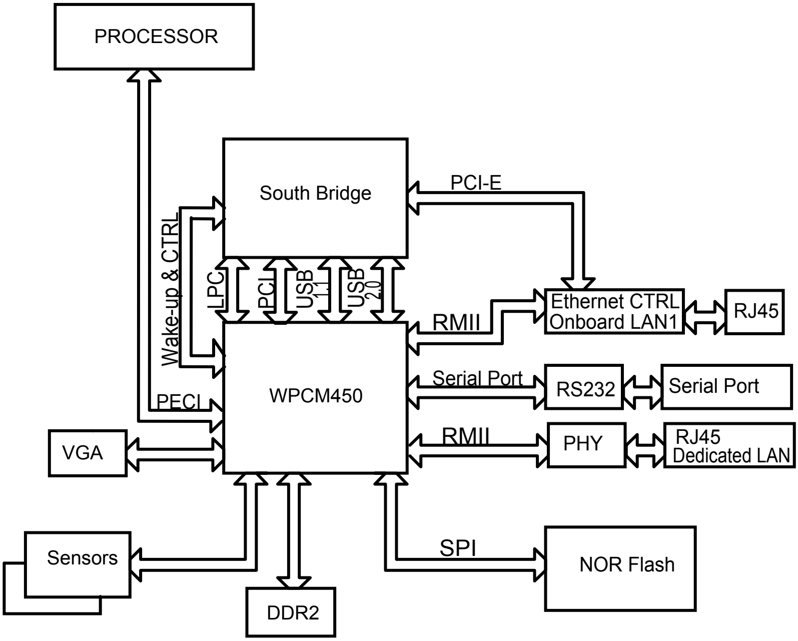
The WPCM450 provides 32-bit, 33 MHz 3.3V PCI interface, which is compliant with PCI Local Bus Specification Rev. 2.3. The PCI system interface connects to the onboard PCI Bridge and is used by the graphics controller.

Supermicro IPMI Features

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

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 motherboard, 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 Supermicro motherboard allows the user to access, monitor, diagnose, and manage a remote server via Console Redirection. It also provides remote access to multiple users from different locations for system maintenance and management.

1.4 Motherboards Supported

This version of X9 SMT IPMI is supported by the motherboards listed in the table below. If your motherboard is not included in the table, please refer to the motherboard product page on our website at www.supermicro.com and download the right BMC/IPMI user's guide for your motherboard.

Intel Dual-Processor Motherboards supported (-F models only)	Intel Single-Processor Motherboards supported (-F models only)
X9DBU-3F/iF	X9SCA-F
X9DR3/i-F/LN4F	X9SCD-F
X9DRT-HF/HIBFF/HIBQF	X9SCi-LN4F
X9DRG-QF/HF/HTF	X9SCL-F
X9DAX-iF	X9SCL+-F
X9DBL-3F/iF	X9SCM-F/IIF
X9DRL-3F/iF	X9SRE/I-F
X9DR7-LN4F	X9SRW-F
X9DR7-LN4F-JBOD	X9SPU-F
X9DRE-LN4F	X9SRD-F
X9DR7/E-TF+	X9SRG-F
X9DRD-EF/7LN4F	X9SRL-F
X9DRD-iF	X9SRH-7F / 7TF
X9DRFF (-7)	
X9DRFR	
X9DRG-HF/HTF	
X9DRH-7F/7TF/iF/iTF	
X9DRi-F	
X9DRT-F/IBFF/IBQF	
X9DRT-HF/HIBFF/HIBQF/	
X9SRT-H6F/H6IBFF/H6IBQF	
X9DRW-3LN4F+/3TF+/7TPF	
X9DRX+-F	
X9QR7-TF+	
X9QRi-F+	

1.5 An Important Note to the User

The graphics shown in this user's guide were based on the latest information available at the time of publishing of this guide. The IPMI screens shown on your computer may or may not look exactly like the screen shown in this user's guide.

Chapter 2

Configuring the IPMI Settings

With the Nuvoton WPCM450 BMC Controller and the IPMIView firmware built in, Supermicro motherboards allow the user to access, monitor, manage and interface with multiple systems in different remote locations. The necessary firmware for accessing and configuring the IPMI settings are available on Supermicro website at http://www.supermicro.com/products/nfo/ipmi.cfm. This section provides detailed information on how to configure the IPMI settings.

2.1 Configuring BIOS

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

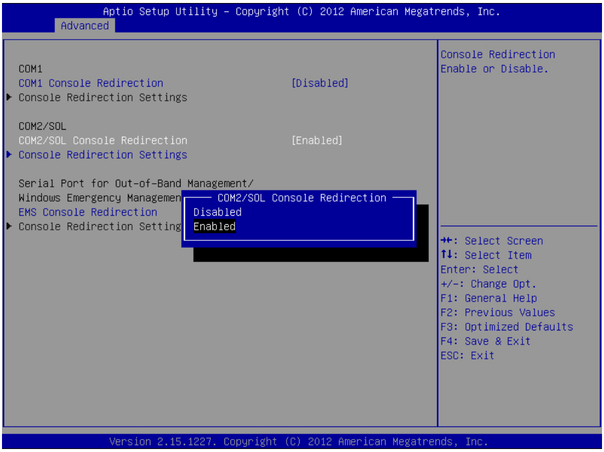
Enabling COM Port for SOL (IPMI)

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 *Serial Port Console Redirection* and press <Enter>.

4. Make sure that the COM port for SOL (COM2 or COM3) is set to enabled. If not, select the port for SOL, press <Enter>, and select **Enabled**. (For IPMI to work properly, the BIOS sets console redirection on this port by default.)



```
          Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
      Advanced

  COM1                                                  | Console Redirection
  COM1 Console Redirection               [Disabled]     | Enable or Disable.
▶ Console Redirection Settings                          |
                                                        |
  COM2/SOL                                              |
  COM2/SOL Console Redirection           [Enabled]      |
▶ Console Redirection Settings                          |
                                                        |
  Serial Port for Out-of-Band Management/               |
  Windows Emergency Managemen┌─ COM2/SOL Console Redirection ─┐
  EMS Console Redirection    │ Disabled                        │
▶ Console Redirection Setting│ Enabled                         │
                             └─────────────────────────────────┘
                                                        | →←: Select Screen
                                                        | ↑↓: Select Item
                                                        | Enter: Select
                                                        | +/-: Change Opt.
                                                        | F1: General Help
                                                        | F2: Previous Values
                                                        | F3: Optimized Defaults
                                                        | F4: Save & Exit
                                                        | ESC: Exit

          Version 2.15.1227. Copyright (C) 2012 American Megatrends, Inc.
```

Enabling All Onboard USB ports

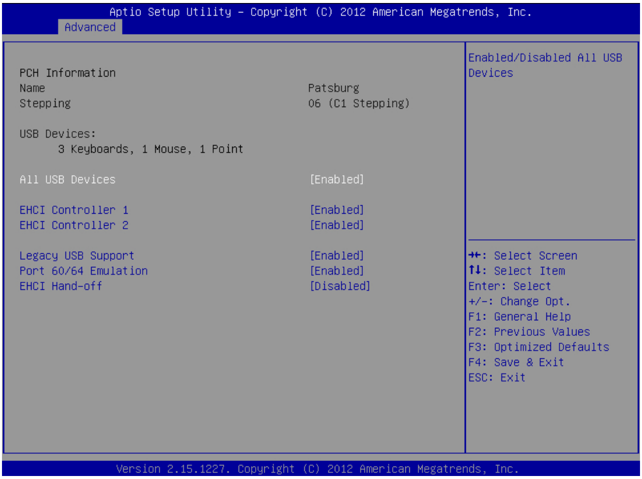
1. Press the <Del> key at bootup to enter the BIOS Setup utility.

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

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

4. Select *South Bridge* and press <Enter>.

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



```
                 Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
         Advanced

                                                                        Enabled/Disabled All USB
  PCH Information                                                       Devices
  Name                                          Patsburg
  Stepping                                      06 (C1 Stepping)

  USB Devices:
        3 Keyboards, 1 Mouse, 1 Point

  All USB Devices                               [Enabled]

  EHCI Controller 1                             [Enabled]
  EHCI Controller 2                             [Enabled]

  Legacy USB Support                            [Enabled]               →←: Select Screen
  Port 60/64 Emulation                          [Enabled]               ↑↓: Select Item
  EHCI Hand-off                                 [Disabled]              Enter: Select
                                                                        +/-: Change Opt.
                                                                        F1: General Help
                                                                        F2: Previous Values
                                                                        F3: Optimized Defaults
                                                                        F4: Save & Exit
                                                                        ESC: Exit

                 Versio 2.15.1227. Copyright (C) 2012 American Megatrends, Inc.
```

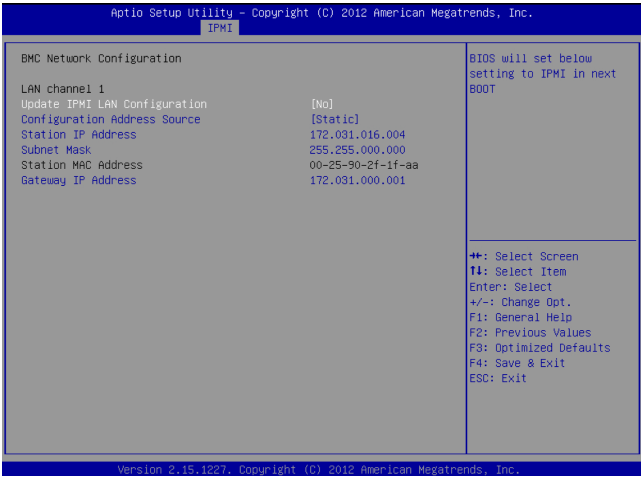
Configuring the IPMI Address Using the BIOS

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>*.*

4. From the BMC Network Configuration submenu, select *Configuration Address Source* and set it to **Static** to manually set the subnet Mask and Gateway IP address.



```
Aptio Setup Utility - Copyright (C) 2012 American Megatrends, Inc.
IPMI

BMC Network Configuration                                    BIOS will set below
                                                             setting to IPMI in next
LAN channel 1                                                BOOT
Update IPMI LAN Configuration            [No]
Configuration Address Source             [Static]
Station IP Address                       172.031.016.004
Subnet Mask                              255.255.000.000
Station MAC Address                      00-25-90-2f-1f-aa
Gateway IP Address                       172.031.000.001

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

Version 2.15.1227. Copyright (C) 2012 American Megatrends, Inc.
```

2.2 Configuring IP Addresses Using the IPMICFG Utility

1. Go to www.supermicro.com/support and click on **Supermicro FTP Site** (right side of the page).

2. ACCEPT the license agreement and go to **utility > IPMICFG**.

3. Save a copy of the IPMICFG utility file to a bootable USB flash drive.

4. Boot the system into the USB flash drive and run the IPMICFG utility.

5. Type IPMICFG and press <Enter> for a list of commands (provided below).

IPMICFG Version 1.02 (Build 120820) Copyright 2012 Super Micro Computer, Inc.
Usage: IPMICFG Params (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 cold reset
-garp on	Enables the Gratuitous ARP
-garp off	Disables the Gratuitous ARP
-fd	Resets to the factory defaults
-fde	Reset to the facctory default. (Clean FRU & LAN)
-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
selftest	Checking and reporting on the basic health of BMC.
-raw	Sends a RAW IPMI request and print the response. Format: NetFn LUN Cmd [Data1...DataN].
-fru info	Shows FRU inventory area info
-fru list	Shows all FRU values

-fru cthelp	Shows chassis type code
-fru help	Shows FRU Write help
-fru <Field>	Shows FRU field value
-fru <Field> <Value>	Writes FRU
-fru backup <File>	Backs up FRU to file
-fru restore <File>	Restores FRU from file
-fru ver [<V1> <V2>]	Retrieves and sets FRU version (V1, V2)
-sel info	Shows SEL info
-sel list	Shows SEL records
-sel del	Deletes all SEL records
-sel raw	Show SEL raw data
-sdr	Shows SDR records and reading
-sdr del <SDR ID>	Deletes SDR record
-sdr ver [<V1><v2>]	Retrieves and sets SDR version (V1, V2)
-nm nmsdr	Display NM SDR
-nm seltime	Get SEL time
-nm deviceid	Get ME Device ID
-nm reset	Reboots ME
-nm reset2default	Force ME reset to Default
-nm updatemode	Force ME to Update Mode
-nm selftest	Get Self Test Results
-nm listimagesinfo	List ME Images information
-nm oemgetpower	OEM Power command for ME
-nm oemgettemp	OEM Temp. command for ME
-nm pstate	Get Max allowed CPU P-State
-nm tstate	Get Max allowed CPU T-State
-nm cpumemtemp	Get CPU/Memory temperature
-nm hostcpudata	Get host CPU data
-nm hostcpudata	Get host CPU data
-fan	Get Fan Mode
-fan <mode>	Set Fan Mode
-pminfo	Power supply PMBus health
-psfruinfo	Power supply FRU health
-user list	List user privilege information
-user help	Show user privilege code
-user del <user id>	Delete user
-user level	Modify user privilege

2.3 Connecting to the Remote Server

Using the IPMIView to Connect to the Remote Server

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

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

3. Go to File > New > System. Enter the System Name, IP Address of IPMI/BMC, and the Description in the appropriate fields, and press <Enter>.

4. Select the system from the IPMI Domain. Enter the Login ID and Password in the appropriate fields to log in to the IPMIView utility. The default ID and password is ADMIN / ADMIN.

Using the Browser to Connect to the Remote Server

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

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

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

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

Notes:

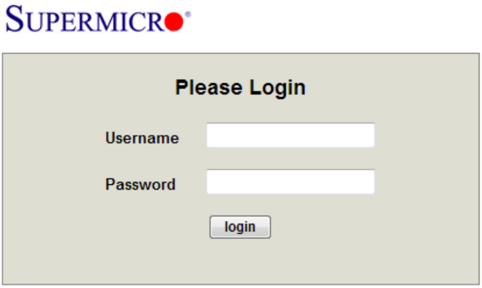
1. The default network setting is "Failover", which will allow the IPMI to connect to the network through a shared LAN port (first onboard LAN port) or through the IPMI Dedicated LAN Port. If the IPMI must be connected through a specific port, please change the LAN configuration setting under the Network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

2. For IPMI to work properly, enable all onboard USB ports and the COM port designated for SOL (IPMI) on the motherboard. All USB ports and the COM port for IPMI are set to Enabled in the system BIOS by default. Refer to Section 2.1 Configuring BIOS for more information.

2.4 Accessing the Remote Server Using the Browser

To Log In to the IPMI Web GUI

Once you are connected to the remote server's web GUI with a browser, the following IPMI Login screen will display.



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

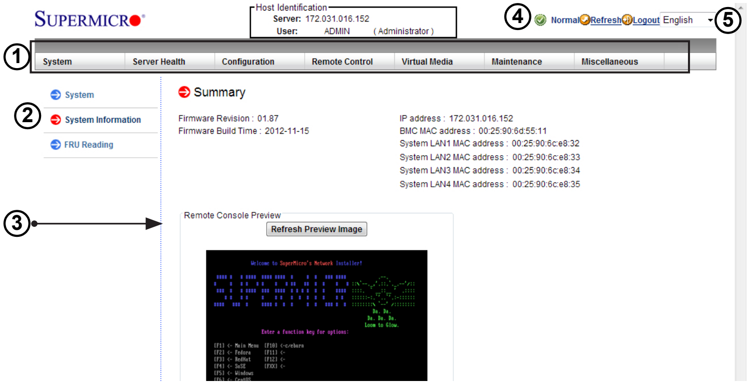
Note: The manufacturer default username and password are ADMIN/ADMIN. Once you have logged into the BMC using the manufacturer default password, be sure to change your password for security purpose.

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

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

2.5 IPMI Main Screen

The IPMI Main screen displays the following information.



Host Identification
Server: 172.031.016.152
User: ADMIN (Administrator)

Summary

Firmware Revision : 01.87
Firmware Build Time : 2012-11-15

IP address : 172.031.016.152
BMC MAC address : 00:25:90:6d:55:11
System LAN1 MAC address : 00:25:90:6c:e8:32
System LAN2 MAC address : 00:25:90:6c:e8:33
System LAN3 MAC address : 00:25:90:6c:e8:34
System LAN4 MAC address : 00:25:90:6c:e8:35

```
Welcome to SuperMicro's Network Installer!

Da. Da.
Da. Da. Da.
Loom to Glow.

Enter a function key for options:

[F1] <- Main Menu  [F10] <-c/eburn
[F2] <- Fedora     [F11] <-
[F3] <- RedHat     [F12] <-
[F4] <- SuSE       [FXX] <-
[F5] <- Windows
[F6] <- CentOS
```

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

1. Menu Bar: The menu bar on the top displays System, 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. Submenu: This window displays IPMI submenu items. Click an item in this window to configure the setting.

3. 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: Indicates that the server is normal.

   - Orange: At least one 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.

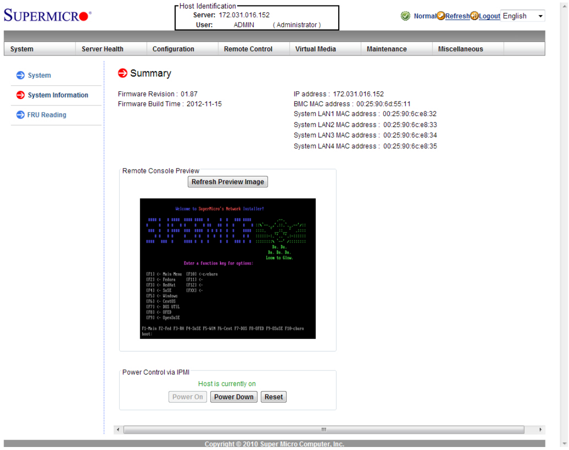
5. Language Select: From the pull-down menu, select a language.

   - English

   - Japanese

2.6 System

The Summary screen (shown below) is displayed when you first log into the remote server. From this location, you can view system information or FRU information.



Host Identification
Server: 172.031.016.152
User: ADMIN (Administrator)

Firmware Revision : 01.87
Firmware Build Time : 2012-11-15

IP address : 172.031.016.152
BMC MAC address : 00:25:90:6d:55:11
System LAN1 MAC address : 00:25:90:6c:e8:32
System LAN2 MAC address : 00:25:90:6c:e8:33
System LAN3 MAC address : 00:25:90:6c:e8:34
System LAN4 MAC address : 00:25:90:6c:e8:35

Remote Console Preview

```
          Welcome to SuperMicro's Network Installer!

                                              Da. Da.
                                            Da. Da. Da.
                                           Loom to Glow.
              Enter a function key for options:

 [F1] <- Main Menu  [F10] <-c/eburn
 [F2] <- Fedora     [F11] <-
 [F3] <- RedHat     [F12] <-
 [F4] <- SuSE       [FXX] <-
 [F5] <- Windows
 [F6] <- CentOS
 [F7] <- DOS UTIL
 [F8] <- OFED
 [F9] <- OpenSuSE

F1-Main F2-Fed F3-RH F4-SuSE F5-WIN F6-Cent F7-DOS F8-OFED F9-OSuSE F10-cburn
boot:
```

Power Control via IPMI

Host is currently on

Copyright © 2010 Super Micro Computer, Inc.

System Information: This submenu displays the following firmware information.

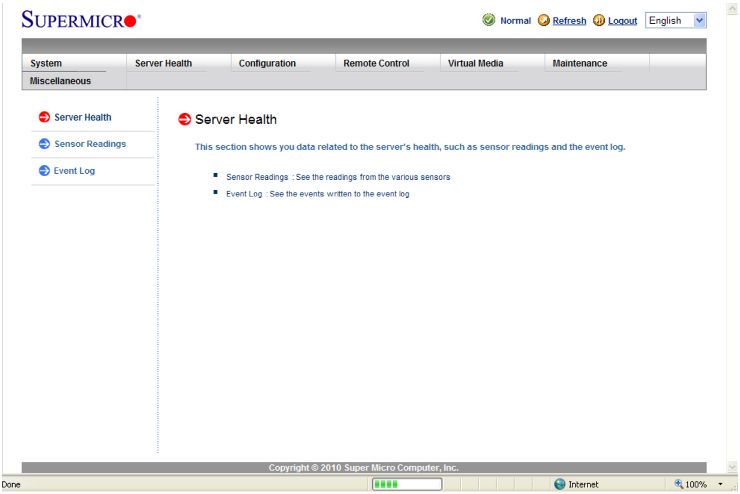
- Firmware Revision
- Firmware Build Time
- IP Address
- BMC MAC Address and System LAN MAC addresses
- Preview Screen: This feature allows the user to launch the remote console by clicking on the preview screen
- Power Control: Select from a limited set of power control functions.

FRU Reading: Click this submenu to display the following BMC FRU (Field Replaceable Unit) information. You can also configure the FRU settings by using the Supermicro IPMIView or ipmicfg utility.

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

2.7 Server Health

This feature allows you to view sensor readings and event logs. Click *Server Health* in the main menu to display the screen shown below.



Server Health

This section shows you data related to the server's health, such as sensor readings and the event log.

- Sensor Readings : See the readings from the various sensors
- Event Log : See the events written to the event log

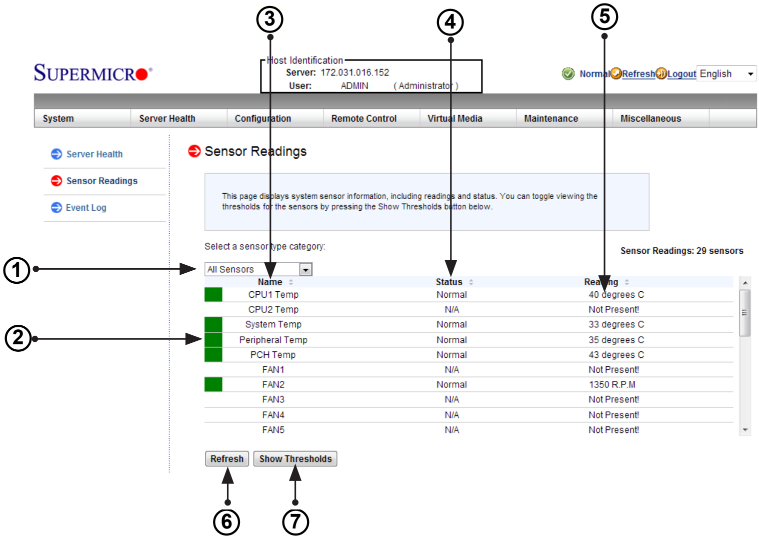
The following submenu items are available under Server Health:

1. Sensor Readings: Click this submenu to view sensor information (see next page).

2. Event Log: Click this submenu to access event logs.

2.7.1 Sensor Readings

This page displays sensor readings for the remote console.



Host Identification
Server: 172.031.016.152
User: ADMIN (Administrator)

Sensor Readings

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

Select a sensor type category:

All Sensors

Sensor Readings: 29 sensors

	Name	Status	Reading
🟩	CPU1 Temp	Normal	40 degrees C
	CPU2 Temp	N/A	Not Present!
🟩	System Temp	Normal	33 degrees C
🟩	Peripheral Temp	Normal	35 degrees C
🟩	PCH Temp	Normal	43 degrees C
	FAN1	N/A	Not Present!
🟩	FAN2	Normal	1350 R.P.M
	FAN3	N/A	Not Present!
	FAN4	N/A	Not Present!
	FAN5	N/A	Not Present!

1. From the pull-down menu, select a sensor type (category). The options include the following.
   - All Sensors
   - Temperature Sensors
   - Voltage Sensors
   - Fan Sensors
   - Physical Security/(Chassis Intrusion)
   - Power Supply
2. The color displayed in front of a sensor indicates the status of the sensor.
   - Green: Indicates that the sensor reading is normal and the system is functioning normally.
   - Amber: Indicates that there is an alert. Attention is needed to ensure that the system is functioning properly.
   - Red: Indicates that one or more sensors have reached the critical state. Immediate action is needed to resolve the problem.

3. Name of the Sensor: This column displays the names of the sensors that are currently active.

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

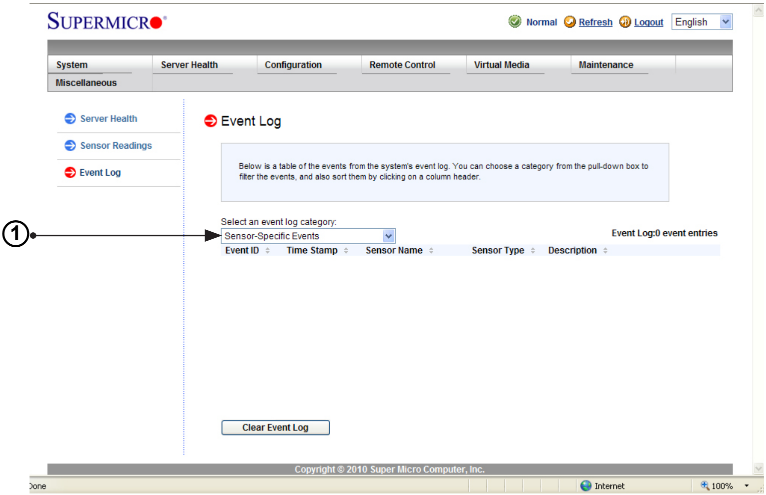
5. Reading: This column indicates the reading of each sensor.

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

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

2.7.2 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.



Below is a table of the events from the system's event log. You can choose a category from the pull-down box to filter the events, and also sort them by clicking on a column header.

Select an event log category: Sensor-Specific Events

Event Log:0 event entries

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.

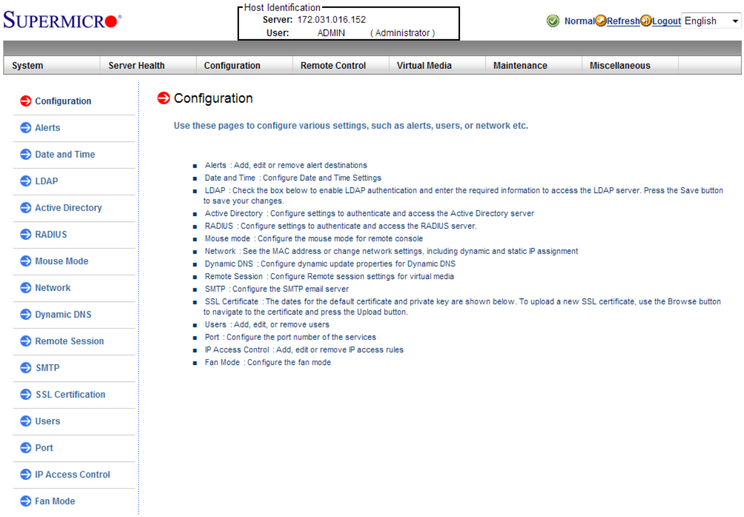
- All Events: This category includes all the above event logs.

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/Shutdown	Stop during OS load/initialization, Unexpected error during system startup, Stopped waiting for input or power cycle/reset
	Run-time stop (a.k.a 'core dump', 'blue screen')
	OS graceful stop (system powered up, but normal OS operation has shut down and system is awaiting reset pushbutton, power cycle or other external input)

2.8 Configuration

This feature allows you to configure various network settings. Click the *Configuration* button in the menu bar to display the following screen.



Host Identification
Server: 172.031.016.152
User: ADMIN (Administrator)

Configuration

Use these pages to configure various settings, such as alerts, users, or network etc.

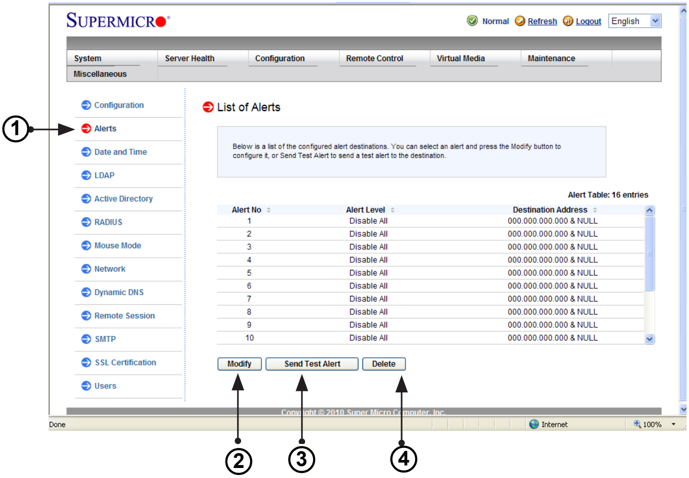
- Alerts : Add, edit or remove alert destinations
- Date and Time : Configure Date and Time Settings
- LDAP : Check the box below to enable LDAP authentication and enter the required information to access the LDAP server. Press the Save button to save your changes.
- Active Directory : Configure settings to authenticate and access the Active Directory server
- RADIUS : Configure settings to authenticate and access the RADIUS server.
- Mouse mode : Configure the mouse mode for remote console
- Network : See the MAC address or change network settings, including dynamic and static IP assignment
- Dynamic DNS : Configure dynamic update properties for Dynamic DNS
- Remote Session : Configure Remote session settings for virtual media
- SMTP : Configure the SMTP email server
- SSL Certificate : The dates for the default certificate and private key are shown below. To upload a new SSL certificate, use the Browse button to navigate to the certificate and press the Upload button.
- Users : Add, edit, or remove users
- Port : Configure the port number of the services
- IP Access Control : Add, edit or remove IP access rules
- Fan Mode : Configure the fan mode

This section allows you 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

2.8.1 Configuring the Alerts Settings

This feature allows the user to configure alert settings. When you click *Alerts* in the Configuration submenu, the following screen displays



List of Alerts

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

Alert Table: 16 entries

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

To modify an existing alert setting, do the following (refer to above image):

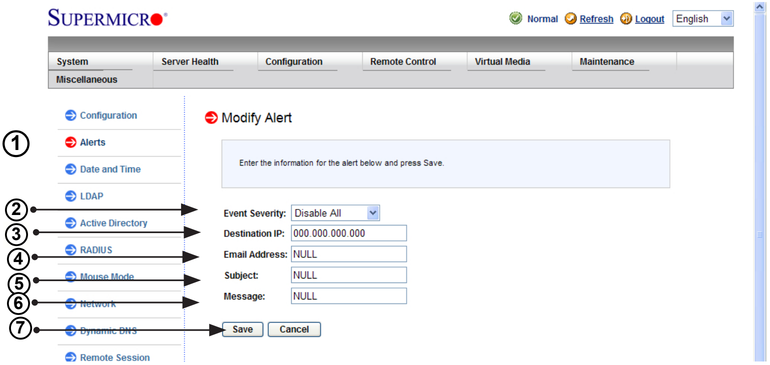
1. Click **Alerts** to activate the alert submenu.

2. Click **Modify** to configure or modify the settings of an alert.

3. Click **Send Test Alert** to check if the alerts have been set and sent out correctly.

4. Click **Delete** to delete an alert.

Creating an Alert



Modify Alert

Enter the information for the alert below and press Save.

Event Severity: Disable All
Destination IP: 000.000.000.000
Email Address: NULL
Subject: NULL
Message: NULL

Follow the steps below to setup an alert (refer to the image at bottom of page 2-16):

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

2. Select the event severity level from the pull-down list.

3. Enter the SNMP Trap receiver (i.e. IPMI View) 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.
MIB community name	A community name is not required since SNMP version 2 only uses traps.
MIB file location	Go to http://www.supermicro.com/products/nfo/IPMI.cfm and click “IPMI MIB (SMT)” (right-hand side of the page).
The IPMI item you need to configure so the SNMP manager can receive the SNMP trap	The alert LAN destination address (see #4 under 2.4.1) must be set to the same IP in as the SNMP manager.
Can I query for detailed information on the MIB "Event" trap items?	Detailed queries are not possible because event mapping is based only on sensor type, event type, and sensor offset.
A list of trap items generated for my platform	No standard list of event traps exist because the PEF (Platform Event Filter) table is OEM customizable.

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

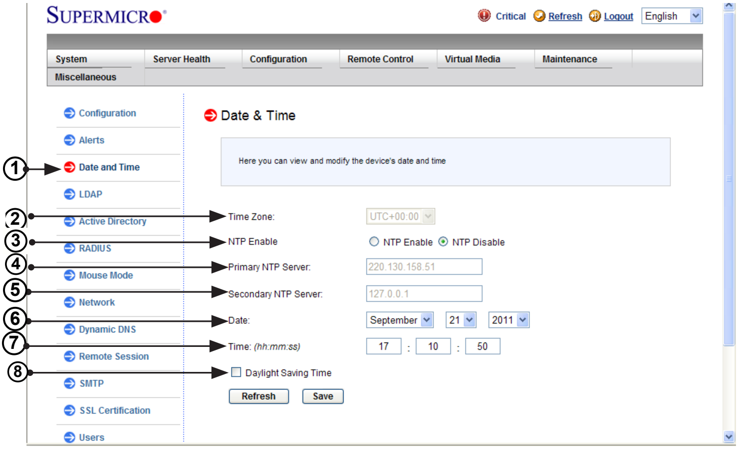
5. Enter the subject line of the alert.

6. Enter a message for the alert.

7. Click **Save** to save the settings.

2.8.2 Configuring Date and Time Settings

This feature allows you to configure the time and date settings for the host server and the client computer. In the Configuration submenu, select *Date and Time* to display the screen shown below.



Date & Time

Here you can view and modify the device's date and time

Time Zone: UTC+00:00

NTP Enable ○ NTP Enable ● NTP Disable

Primary NTP Server: 220.130.158.51

Secondary NTP Server: 127.0.0.1

Date: September 21 2011

Time: *(hh:mm:ss)* 17 : 10 : 50

□ Daylight Saving Time

You can either set the date and time manually or use the NTP server to set date and time. Follow the instructions below to set date and time settings.

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

1. Click **Date and Time** on the left to set the date and time settings.

2. Select the time zone (available if NTP is enabled).

3. Check this item to use NTP settings.

4. Enter the IP address for the primary NTP server.

5. Enter the IP address for the secondary NTP server.

6. Enter the date.

7. Enter the time in hh/mm/ss format.

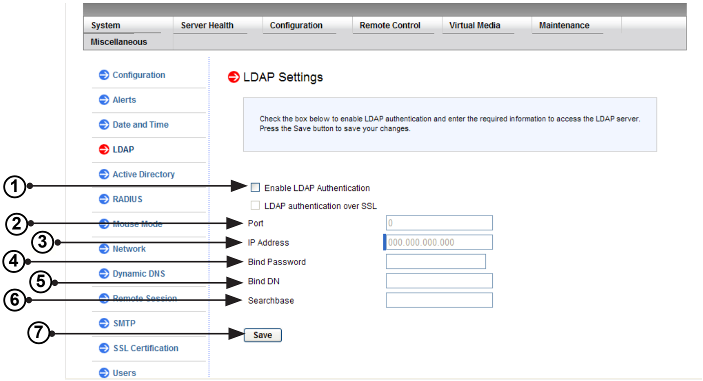
8. Check this box for the time to automatically adjust during daylight savng time.

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

Click **Save** to save the entries.

2.8.3 Configuring LDAP (Light-Weight Directory Access Protocol) Settings

This feature allows you to configure the LDAP settings. In the Configuration submenu, select LDAP to display the screen shown below.



LDAP Settings

Check the box below to enable LDAP authentication and enter the required information to access the LDAP server. Press the Save button to save your changes.

□ Enable LDAP Authentication

□ LDAP authentication over SSL

Port: 0

IP Address: 000.000.000.000

Bind Password:

Bind DN:

Searchbase:

Follow the steps below to configure the LDAP settings.

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

2. Enter a port number of the LDAP server.

3. Enter an IP Address of the LDAP server.

4. Enter a Bind Password of the LDAP server.

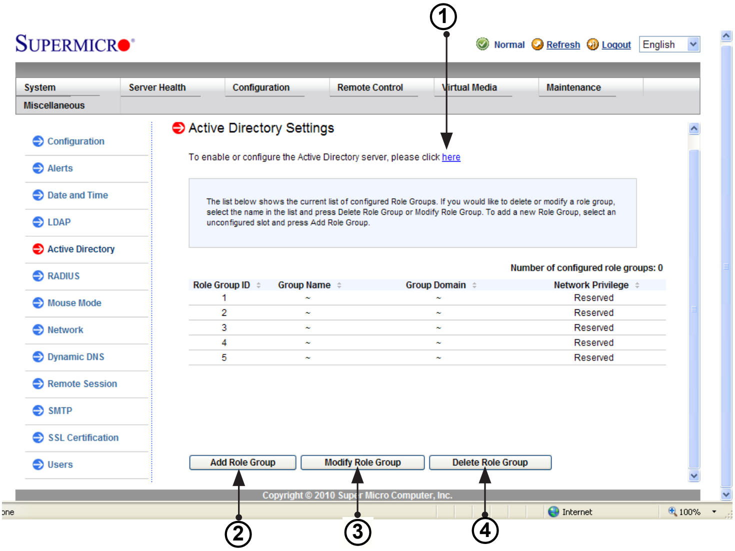
5. Enter a Bind DN value in the field. The bind DN is the user or the LDAP server that is permitted to do search in the LDAP directory within a defined search base.

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 settings.

2.8.4 Active Directory Settings

This page displays a list of role groups and their Group IDs, Group Names, Domains and Network Privilege settings. In the Configuration submenu, select *Active Directory* to display the screen shown below.



Active Directory Settings

To enable or configure the Active Directory server, please click here

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

Number of configured role groups: 0

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

1. To enable or configure the Active Directory server, click the **here** hyperlink (see next page for instructions on enabling or configuring the Active Directory).

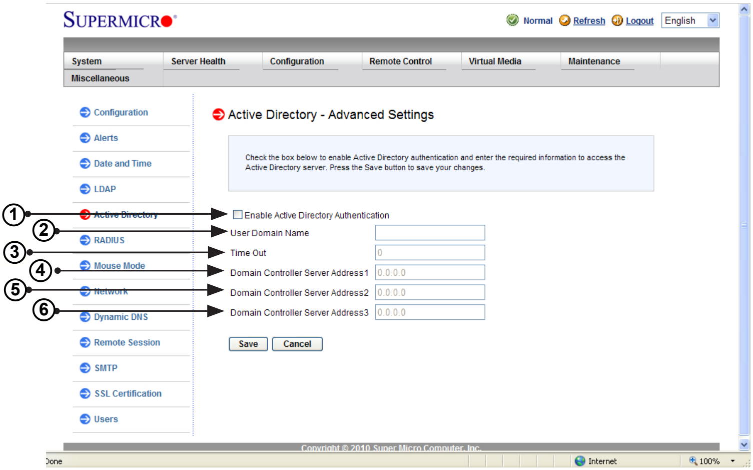
2. Select a group and click **Add** to add a role group.

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. Click the here hyperlink (see #1 on previous page) display the Advanced Settings page for the active directory (shown below).



Active Directory - Advanced Settings

Check the box below to enable Active Directory authentication and enter the required information to access the Active Directory server. Press the Save button to save your changes.

☐ Enable Active Directory Authentication

User Domain Name	
Time Out	0
Domain Controller Server Address1	0.0.0.0
Domain Controller Server Address2	0.0.0.0
Domain Controller Server Address3	0.0.0.0

1. Check the Enable box to enable Active Directory authentication support. Once enabled, you can enter 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 logged-in.

4. Enter Controller Server Address1.

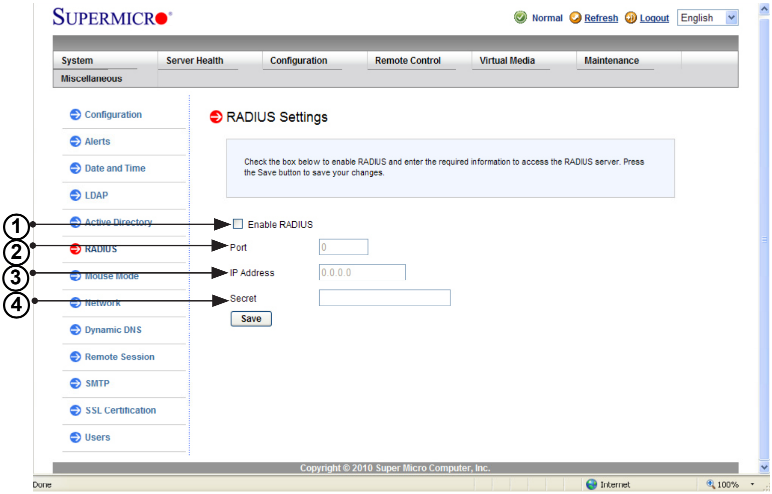
5. Enter Controller Server Address2.

6. Enter Controller Server Address3.

After entering the information, click **Save** to save the settings.

2.8.5 Configuring the RADIUS Settings

This feature allows you to configure RADIUS settings. In the Configuration sub-menu, select RADIUS to display the screen shown below.



RADIUS Settings

Check the box below to enable RADIUS and enter the required information to access the RADIUS server. Press the Save button to save your changes.

□ Enable RADIUS

Port: 0

IP Address: 0.0.0.0

Secret:

Save

Copyright © 2010 Super Micro Computer, Inc.

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 of the RADIUS server.

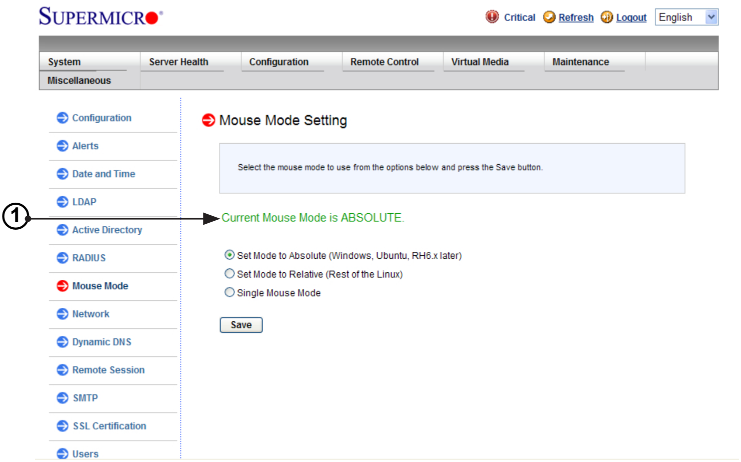
3. Enter the IP address of the RADIUS server.

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.

2.8.6 Configuring the Mouse Mode Settings

This feature allows you to configure the mouse mode settings. In the Configuration submenu, select *Mouse Mode* to display the screen shown below.



Mouse Mode Setting

Select the mouse mode to use from the options below and press the Save button.

Current Mouse Mode is ABSOLUTE.

◉ Set Mode to Absolute (Windows, Ubuntu, RH6.x later)
○ Set Mode to Relative (Rest of the Linux)
○ Single Mouse Mode

Save

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

    - Set the mouse mode to *Absolute* for the Windows OS. (This is the default setting.)

    - Set the mouse mode to *Relative* for the Linux/Unix OS.

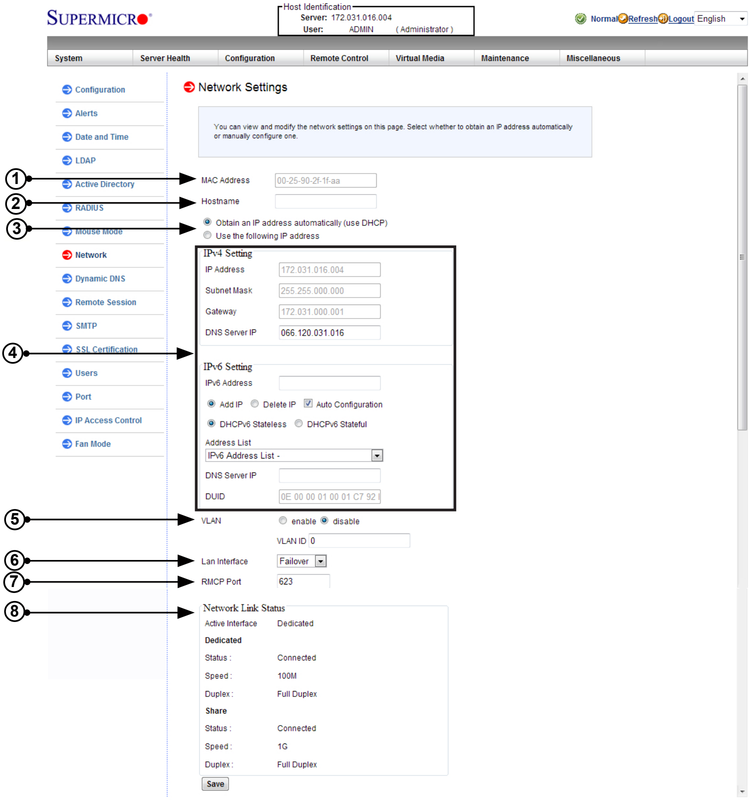
    - Set the mouse mode to Single for use with LSI's WebBIOS GUI.

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.

2.8.7 Configuring Network Settings

This feature allows you to configure the network settings. In the Configuration submenu, select *Network* to display the screen shown below.



Host Identification
Server: 172.031.016.004
User: ADMIN (Administrator)

Network Settings

You can view and modify the network settings on this page. Select whether to obtain an IP address automatically or manually configure one.

MAC Address 00-25-90-2f-1f-aa

Hostname

● Obtain an IP address automatically (use DHCP)

○ Use the following IP address

IPv4 Setting

IP Address 172.031.016.004

Subnet Mask 255.255.000.000

Gateway 172.031.000.001

DNS Server IP 066.120.031.016

IPv6 Setting

IPv6 Address

● Add IP ○ Delete IP ☑ Auto Configuration

● DHCPv6 Stateless ○ DHCPv6 Stateful

Address List
IPv6 Address List -

DNS Server IP

DUID 0E 00 00 01 00 01 C7 92 I

VLAN ○ enable ● disable

VLAN ID 0

Lan Interface Failover

RMCP Port 623

Network Link Status

Active Interface Dedicated

Dedicated

Status : Connected

Speed : 100M

Duplex : Full Duplex

Share

Status : Connected

Speed : 1G

Duplex : Full Duplex

Enter information into the following fields to configure network settings:

1. **MAC Address**: This field displays the MAC address for the network server.

2. **Host Name**: Enter a hostname for the network server (optional).

3. 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.)

4. **IPv4 and IPv6 Setting**: To set the IP address manually using the IPv4 or IPV6 format, enter proper information in the available fields.

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

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

- The default setting is Failover, which will allow 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 first LAN port (port 0 or port1) on the board.

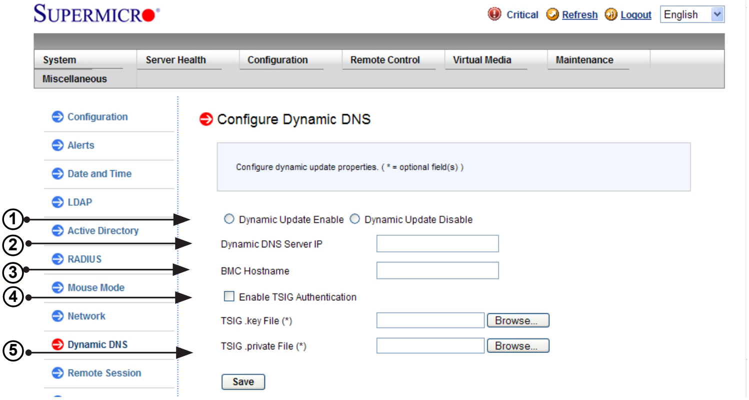
7. **RMCP Port**: This feature allows the user to select the desired RMCP (Remote Mail Checking Protocol) port based on his configuration. The default port is 623.

8. **Network Link Status**: This section displays the status, speed, and duplex type for the dedicated and shared network links.

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

2.8.8 Configuring Dynamic DNS (Domain Name System) Settings

This feature allows you to configure Dynamic DNS settings. In the Configuration submenu, select *Dynamic DNS* to display the screen shown below.



Configure Dynamic DNS

Configure dynamic update properties. (* = optional field(s))

○ Dynamic Update Enable ○ Dynamic Update Disable

Dynamic DNS Server IP

BMC Hostname

□ Enable TSIG Authentication

TSIG .key File (*)

TSIG .private File (*)

1. Select the desired radio button to enable or disable Dynamic DNS update support. The default setting is disabled.

2. Enter the IP address of your Dynamic DNS server.

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

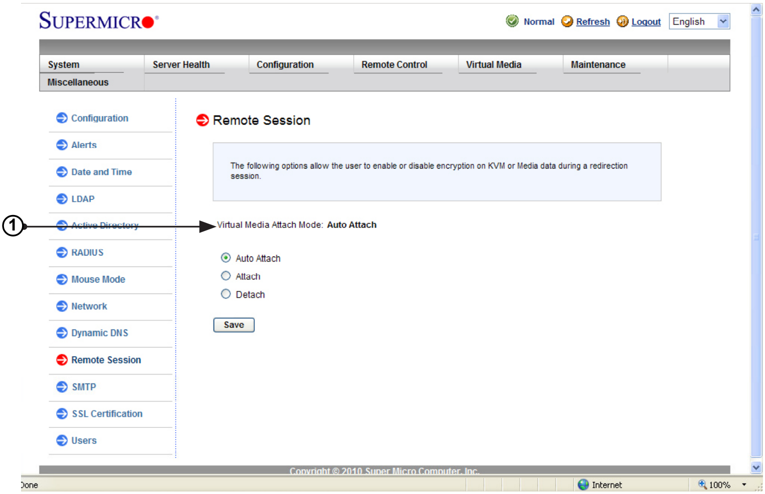
4. Check the box to enable TSIG Authentication support, and browse the files to select the TSIG.key file. (This item is optional.)

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.

2.8.9 Configuring the Remote Session Settings

This feature allows you to enable or disable encryption support on IKVM, or to select the Virtual Media Attach mode for console redirection. In the Configuration submenu, select *Remote Session* to display the screen shown below.



Remote Session

The following options allow the user to enable or disable encryption on KVM or Media data during a redirection session.

Virtual Media Attach Mode: **Auto Attach**

● Auto Attach
○ Attach
○ Detach

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.

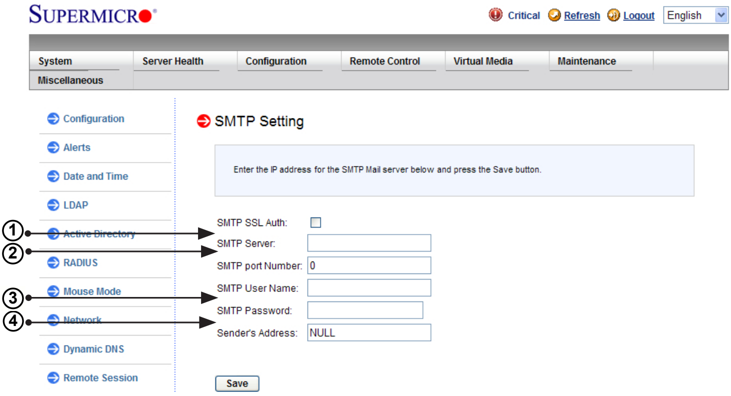
- Attach: Select this mode to activate a virtual media and make it available for remote access. A virtual device will always be seen in the system BIOS even when it is not active.

- Detach: Select this mode to disable virtual media for remote access.

After making selection, click **Save** to save the settings.

2.8.10 Configuring the SMTP Settings

This feature allows you to configure SMTP (Simple Mail Transfer Protocol) settings for email transmission through the network. In the Configuration submenu, select *SMTP* to display the screen shown below.



SMTP Setting

Enter the IP address for the SMTP Mail server below and press the Save button.

SMTP SSL Auth: □
SMTP Server:
SMTP port Number: 0
SMTP User Name:
SMTP Password:
Sender's Address: NULL

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.

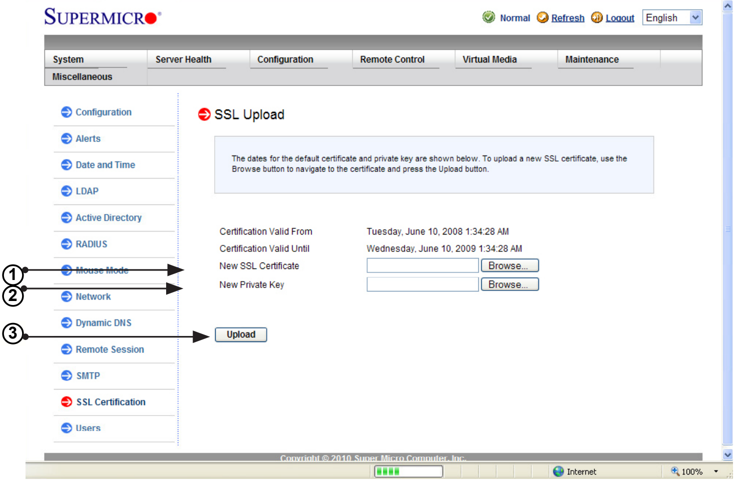
3. Enter the user name for your SMTP Mail server (optional).

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.

2.8.11 Configuring the SSL (Secure Sockets Layer) Certification

This feature displays the default certificate and private keys. It also allows you to upload a new SSL certificate. In the Configuration submenu, select *SSL* to display the screen shown below.



SSL Upload

The dates for the default certificate and private key are shown below. To upload a new SSL certificate, use the Browse button to navigate to the certificate and press the Upload button.

Certification Valid From	Tuesday, June 10, 2008 1:34:28 AM
Certification Valid Until	Wednesday, June 10, 2009 1:34:28 AM
New SSL Certificate	
New Private Key	

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

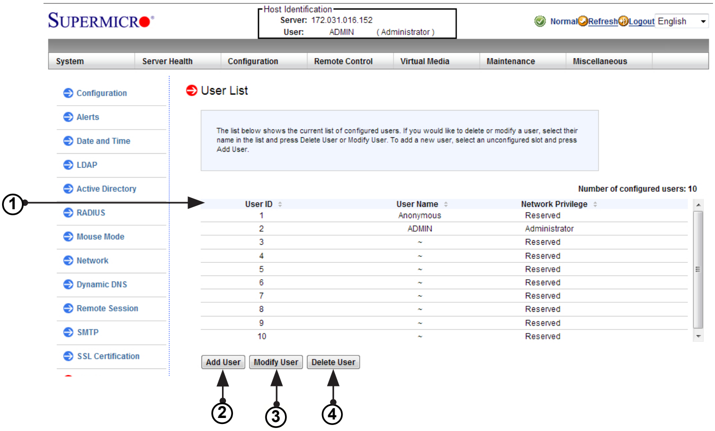
   Note: SHA2 and RSA 2048 bit SSL supported.

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

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

2.8.12 Configuring Users Settings

This page displays information on the current users. It also allows you to add, delete or modify user information. In the Configuration submenu, select *Users* to display the screen shown below.



User List

The list below shows the current list of configured users. If you would like to delete or modify a user, select their name in the list and press Delete User or Modify User. To add a new user, select an unconfigured slot and press Add User.

Number of configured users: 10

User ID	User Name	Network Privilege
1	Anonymous	Reserved
2	ADMIN	Administrator
3	~	Reserved
4	~	Reserved
5	~	Reserved
6	~	Reserved
7	~	Reserved
8	~	Reserved
9	~	Reserved
10	~	Reserved

1. This item lists current user information, including User ID, User name and Network Privilege settings. Network privilege settings are shown below. A maximum of 10 user profiles can be made.

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. 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.

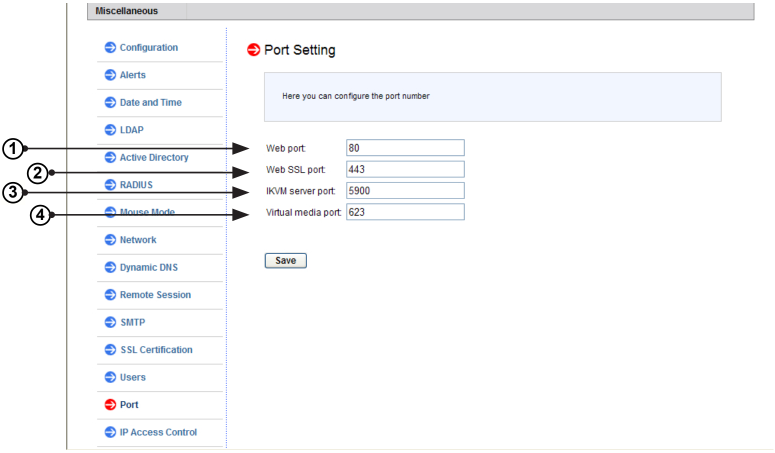
3. To modify the information or the status of a user, click **Modify User**. When prompted, using the arrow keys, select a user from the users list to modify the user information.

4. 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.

Note: The *User ID #1* (Anonymous) account cannot be deleted.

2.8.13 Configuring Port Settings

This page allows you to configure port settings. In the Configuration submenu, select *Port* to display the page as shown below.



Port Setting

Here you can configure the port number

Web port: 80

Web SSL port: 443

IKVM server port: 5900

Virtual media port: 623

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.

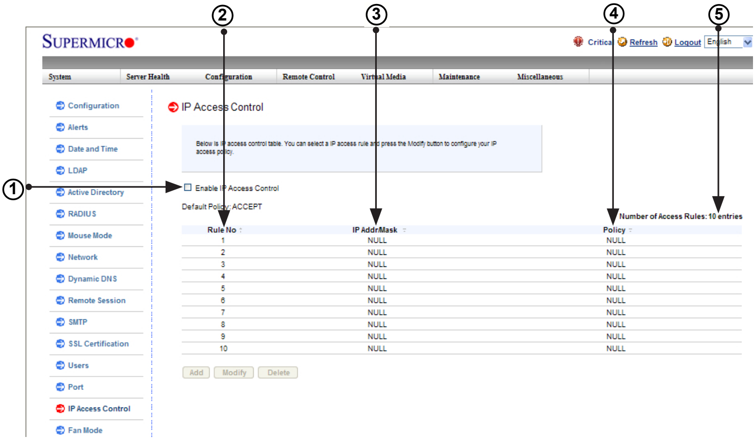
4. Virtual Media Port: Enter the desired virtual media port number.

After configuring the port settings, click **Save** to save the settings.

2.8.14 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.

Note: This submenu is applicable to X9 motherboards only.



IP Access Control

Below is IP access control table. You can select a IP access rule and press the Modify button to configure your IP access policy.

□ Enable IP Access Control

Default Policy: ACCEPT

Number of Access Rules: 10 entries

Rule No	IP Addr/Mask	Policy
1	NULL	NULL
2	NULL	NULL
3	NULL	NULL
4	NULL	NULL
5	NULL	NULL
6	NULL	NULL
7	NULL	NULL
8	NULL	NULL
9	NULL	NULL
10	NULL	NULL

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.

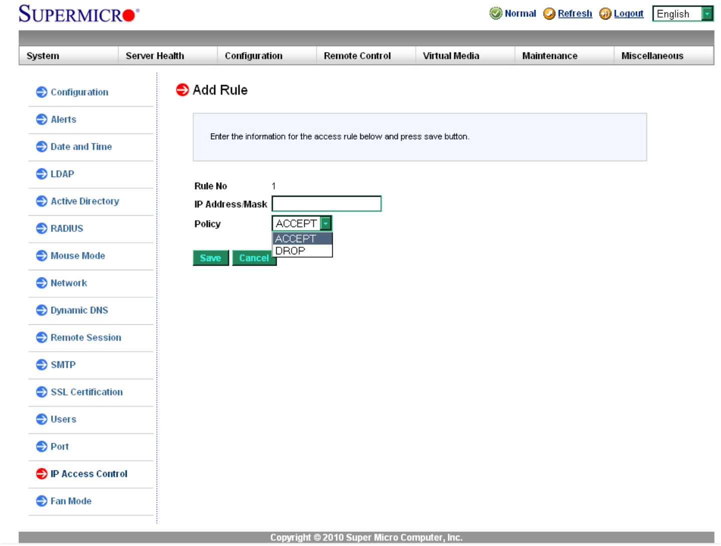
3. IP Address/Mask: This column displays IP Address/Mask settings.

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

Select an item in the IP Access Control list and click **Modify**, to display the Add Rule screen as shown below.



Add Rule

Enter the information for the access rule below and press save button.

Rule No 1

IP Address/Mask

Policy ACCEPT

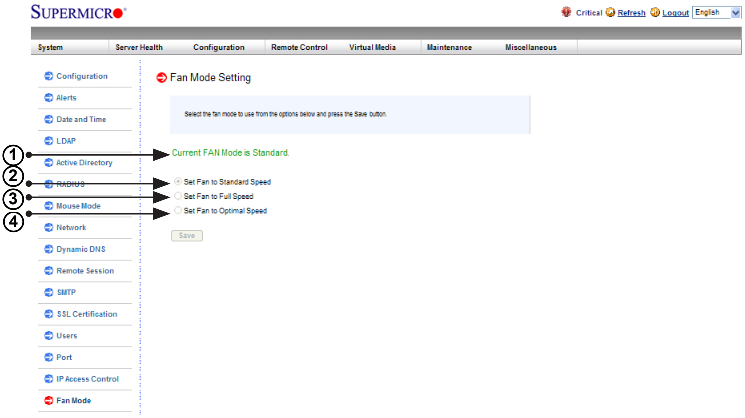
To modify a rule, enter the information needed for the following items:

- 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.

2.8.15 Configuring Fan Settings

This page allows you to configure fan mode settings. In the Configuration submenu, select *Fan Mode* to display the screen shon below.



Fan Mode Setting

Select the fan mode to use from the options below and press the Save button.

Current FAN Mode is Standard.

● Set Fan to Standard Speed
○ Set Fan to Full Speed
○ Set Fan to Optimal Speed

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.

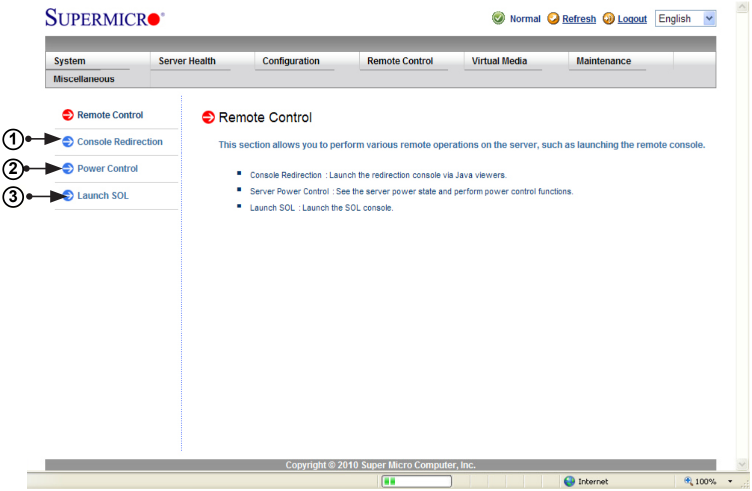
4. Check this button to use the optimal fan speed setting which will adjust the fan speed by balancing the needs between system performance and power saving.

Note: Fan mode settings will vary depending on the server board.

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

2.9 Remote Control

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



Remote Control

This section allows you to perform various remote operations on the server, such as launching the remote console.

- Console Redirection : Launch the redirection console via Java viewers.
- Server Power Control : See the server power state and perform power control functions.
- Launch SOL : Launch the SOL console.

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

1. Click *Console Redirection* to launch console redirection and configure the settings of the remote server. For more details on console redirection, refer to section 2.9.1 (next page).

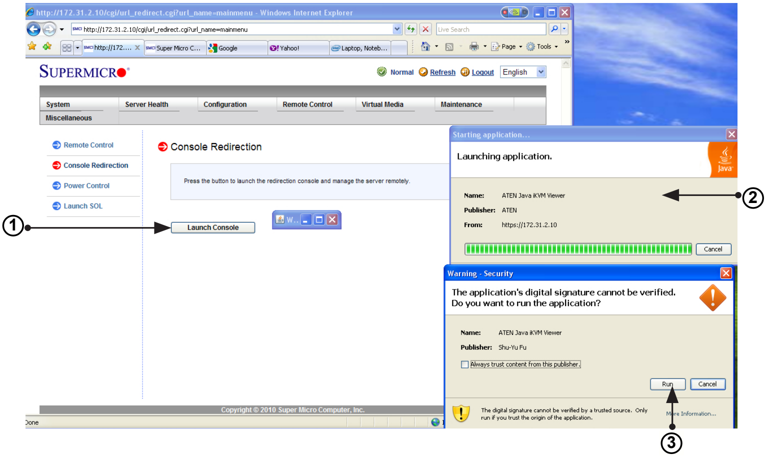
2. Click *Power Control* to display and execute the power options of the remote system, including the following:

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

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

2.9.1 Launching Console Redirection

This feature allows you to launch console redirection via IKVM (keyboard, video/monitor, mouse) support. In the Remote submenu, select *Console Redirection* to display the screen shown below.



Console Redirection

Press the button to launch the redirection console and manage the server remotely.

Launching application.

Name: ATEN Java iKVM Viewer
Publisher: ATEN
From: https://172.31.2.10

The application's digital signature cannot be verified.
Do you want to run the application?

Name: ATEN Java iKVM Viewer
Publisher: Shu-Yu Fu

□ Always trust content from this publisher.

The digital signature cannot be verified by a trusted source. Only run if you trust the origin of the application.

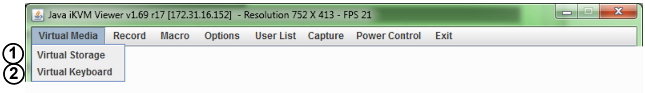
1. Click **Launch Console** on the Console Redirection screen to launch the remote console via Java or Active X (for the Internet Explorer). If it is blocked by the IE due to security reasons, click on the top of the menu bar and select **Download File**.

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

3. When the warning screen displays (as shown above), click **Run** to launch the remote console.

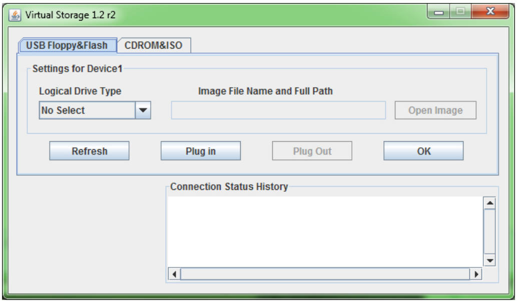
2.9.1.1 Console Redirection > Virtual Media

This feature allows you to configure virtual device settings for your console redirection. In the iKVM menu bar, select *Virtual Media* to display the submenu items as shown below.

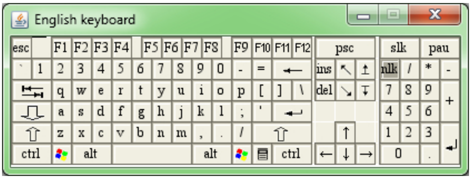


1. Click *Virtual Storage* to open the window shown below. Use the Virtual Storage window to select a device you want to connect to the remote server as a virtual device.

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

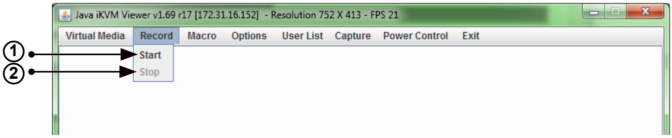


2. Click *Virtual Keyboard* to use the onscreen Keyboard shown below. Click a key on the keyboard for your BMC connection.


English keyboard
esc F1 F2 F3 F4 F5 F6 F7 F8 F9 F10 F11 F12 psc slk pau
` 1 2 3 4 5 6 7 8 9 0 - = ins nlk / * -
q w e r t y u i o p [ ] \ del 7 8 9 +
a s d f g h j k l ; ' 4 5 6
z x c v b n m , . / 1 2 3
ctrl alt alt ctrl 0 .

2.9.1.2. Console Redirection > Record

This feature allows you to record media displays for your console redirection. In the iKVM menu bar, select *Record* to disply the submenu items as shown below.



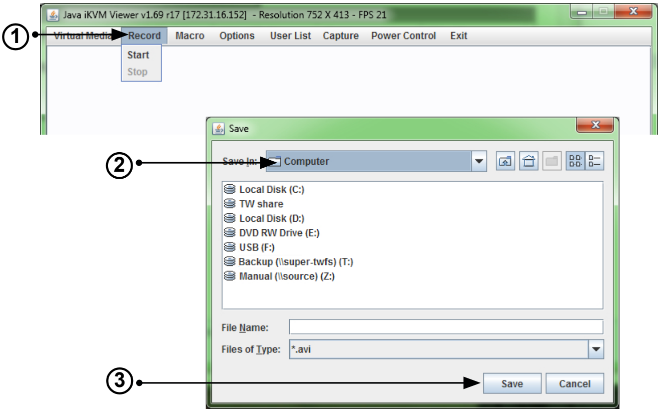
1. Click *Start* to start video recording from your remote server.

2. Click *Stop* to stop video recording from your remote server.

Note: By default, recording will stop automatically after two minutes. You can change this through the Display Preferences (see section 2.9.1.5.2)

2.9.1.3. Console Redirection > Recording Media

This feature allows you to record the media displays. Follow the instructions below to start and stop media recording.



Save In: Computer

Files of Type: *.avi

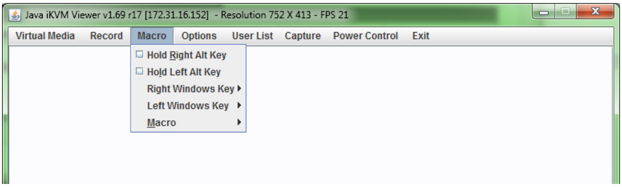
1. In the iKVM menu bar, click **Record** to display the recording options, then click **Start** to start recording.

2. From the pop-up window, select the location where you want to save the recording.

3. Enter the filename and click **Save** to save the recording.

2.9.1.4. Console Redirection > Macro

This feature allows you to configure macro settings for your console redirection. In the iKVM menu, select *Macro* to display the submenu items as shown below.



The submenu items include the following.

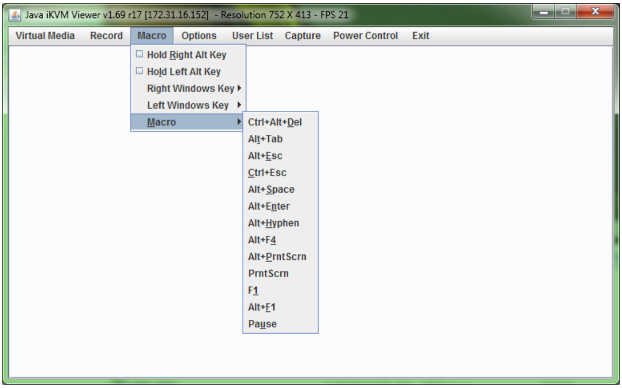
- **Hold Right ALT Key:** This item performs the same function as holding down the <Right Alt> key.

- **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 pressing the <Right Windows> key. Right click this item to select <Hold Down> or <Press & Release> for the Right Windows key.

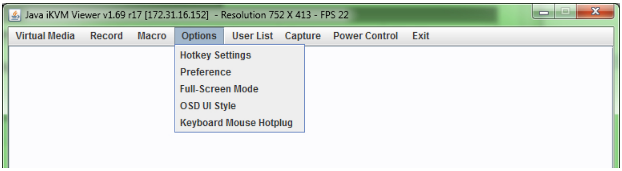
- **Left Windows Key:** This item performs the same function as pressing the <Left Windows> key. Right click this item to select <Press Down> or <Press & Release> for the <Left Windows> key.

- **Macro:** Click this item to activate the macro hotkey submenu as shown below.



2.9.1.5 Console Redirection > Options

This feature allows you to configure options settings for your console redirection. In the iKVM menu bar, select *Options* to display the submenu items as shown below.

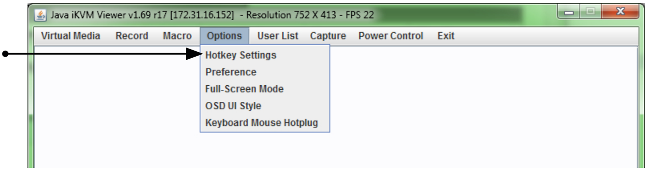


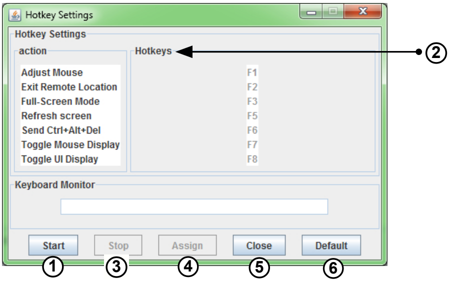
The options menu allows you to configure the following settings:

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

2.9.1.5.1 Console Redirection > Options > Hotkey Settings

This feature allows you to configure Hotkey settings for your console redirection. In the Options submenu, select Hotkey Settings to open the hotkey window as shown below.





action	Hotkeys
Adjust Mouse	F1
Exit Remote Location	F2
Full-Screen Mode	F3
Refresh screen	F5
Send Ctrl+Alt+Del	F6
Toggle Mouse Display	F7
Toggle UI Display	F8

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**.

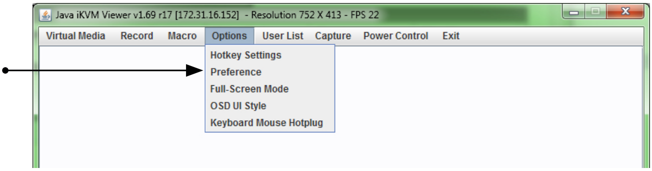
4. Select an item from the action list and click **Assign**.

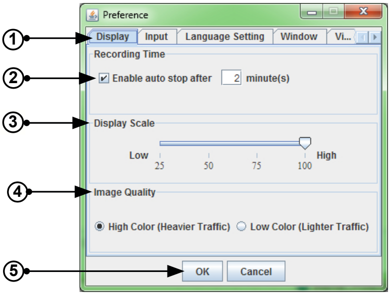
5. Click **Close** to exit.

6. Click **Default** to reset all hotkey settings to default values.

2.9.1.5.2. Console Redirection > Options > Preference > Display

This feature allows you to configure Video Recording Preference settings for your console redirection. In the iKVM menu, select *Preference* to open the preference window as shown below.





Recording Time

☑ Enable auto stop after 2 minute(s)

Display Scale

Image Quality

● High Color (Heavier Traffic) ○ Low Color (Lighter Traffic)

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

1. Click the Display tab to configure video display features.

2. 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. If enabled, enter the number of minutes upon which your video recording will automatically stop recording.

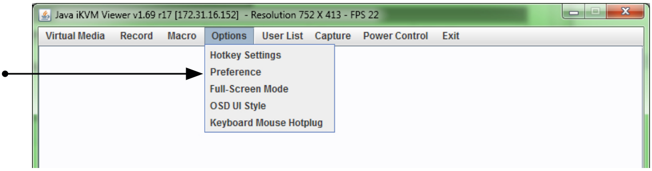
3. Use the slider on the Display Scale to set the appropriate scale setting for your video display from Low (25) to High (100).

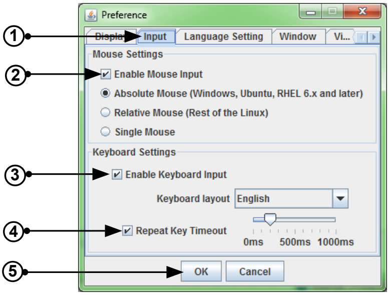
4. To ensure the best image quality, select High Color for heavier network traffic connections; select Low Color for lighter network traffic.

5. Click **OK** to save the recording preference settings or click **Cancel** to cancel the selection.

2.9.1.5.3. Console Redirection > Options> Preference >Input

This feature allows you to configure Video Recording input settings for your console redirection. In the iKVM menu bar, select Preferences to open the preference window as shown below.





Mouse Settings

☑ Enable Mouse Input

● Absolute Mouse (Windows, Ubuntu, RHEL 6.x and later)

○ Relative Mouse (Rest of the Linux)

○ Single Mouse

Keyboard Settings

☑ Enable Keyboard Input

Keyboard layout English

☑ Repeat Key Timeout 0ms 500ms 1000ms

To configure Video Input settings, follow the instructions below.

1. Click the Input tab to configure mouse and keyboard settings.

2. 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* for the Windows OS, Ubuntu, or RHEL 6.x and later.
- Select *Relative Mouse* for the Linux OS.
- Select *Single Mouse* for use with all other OS.

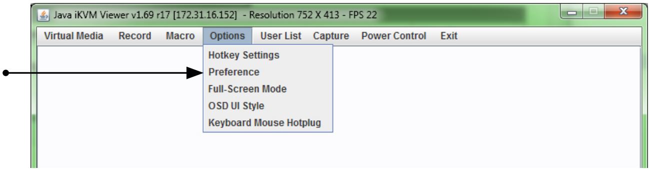
3. Select *Enable Keyboard Input* to enable keyboard support so that you can use soft keyboard as an input device. From the *Keyboard layout* pull-down menu, select the right language setting for your soft keyboard.

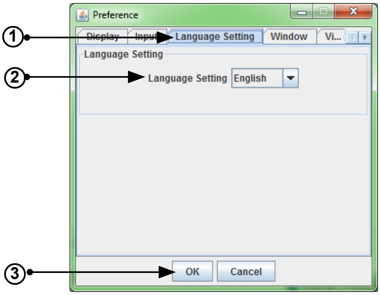
4. Use the slider on the *Repeat Key Timeout* scale to select the appropriate timeout settings for repeat keystrokes from 0ms to 1000ms (micro-second).

5. Click **Save** to save the keyboard setting or click **Cancel** to cancel it.

2.9.1.5.4. Console Redirection > Options > Preference > Language Settings

This feature allows you to configure language settings for your console redirection. In the iKVM menu bar, select Preferences to open the preference window as shown below.





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

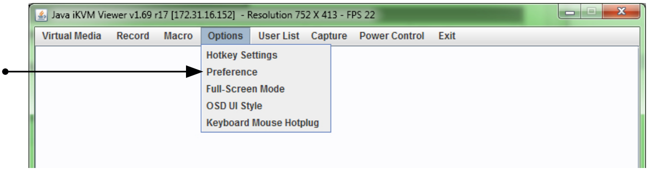
1. Click the Language Setting tab.

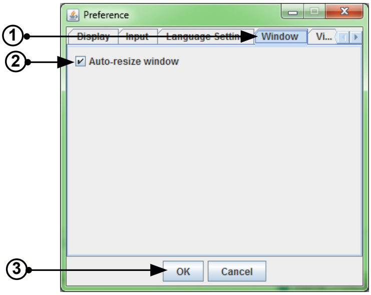
2. From the Language Setting pull-down menu, select the language you want to use for your console redirection. The language options include English, Japanese, German, French, Spanish, Korean, and Italian.

3. Once you have selected a language setting, click **OK** to use the language.

2.9.1.5.5. Console Redirection > Options > Preference > Window

This feature allows you to configure window settings for your console redirection. In the iKVM menu bar, select Preferences to open the preference window as shown below.





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

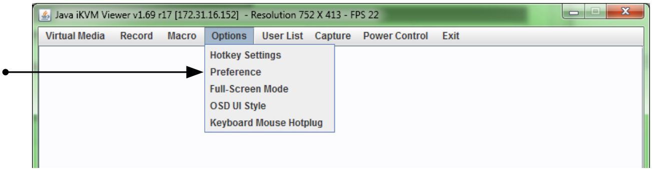
1. Click the Window tab.

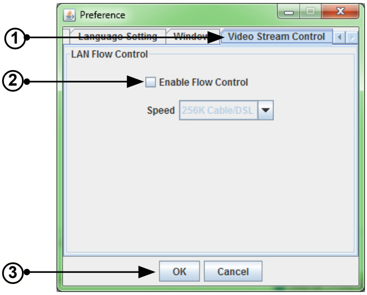
2. Check *Auto re-size window* for the system to reset the size of your display window. (If you do not wish your display window to be re-sized automatically, leave the box unchecked.)

3. Click **OK** to save the window settings.

2.9.1.5.6. Console Redirection > Options > Preference > Video Stream Control

This feature allows you to configure video stream settings for your console redirection. In the iKVM menu bar, select Preferences to open the preference window as shown below.



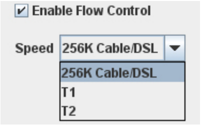


To select the correct video stream control settings for your console redirection, follow the instructions below.

1. Click the Video Stream Control tab.

2. 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



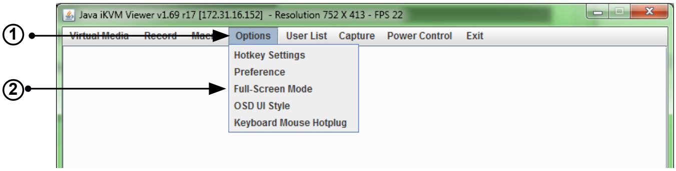
3. Click **OK** to save the Video Stream Control setting.

2.9.1.5.7. Console Redirection > Options > Full Screen Mode

This feature allows you to configure the screen settings for your console redirection. To set a full screen display for your console redirection, follow the instructions below.

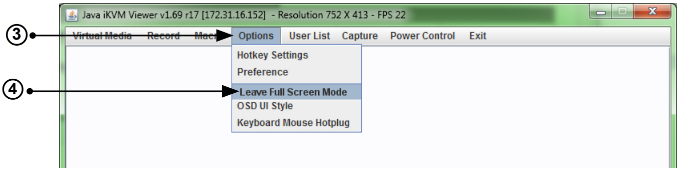
1. Select Options from the iKVM menu bar to display the submenu.

2. Select *Full Screen Mode* from the submenu. A full-screen display will appear.



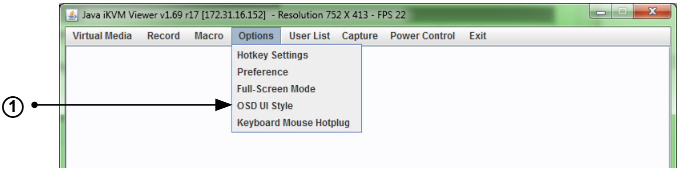
3. To leave the full screen display, click Options in the iKVM submenu.

4. From the submenu, select *Leave Full Screen* and press <Enter>.



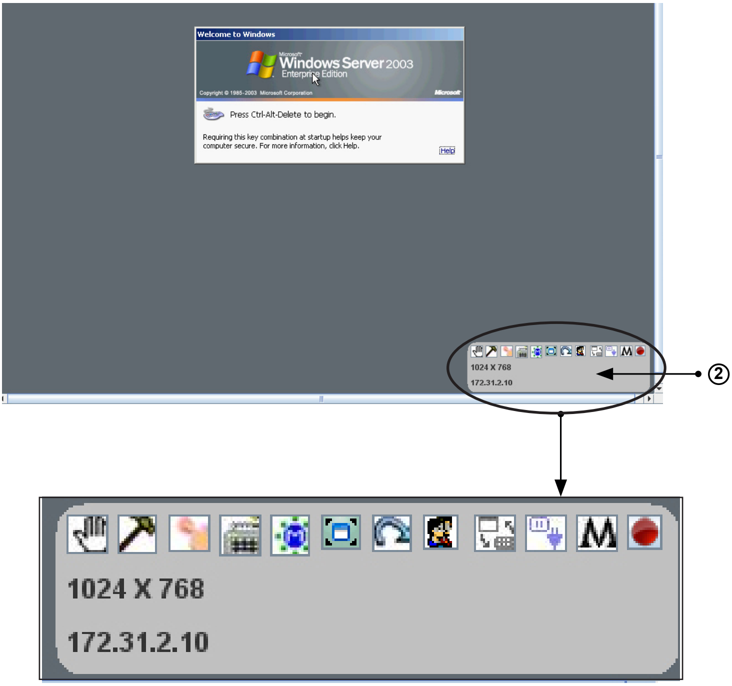
2.9.1.5.8 Console Redirection > Options > OSD UI Style

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.

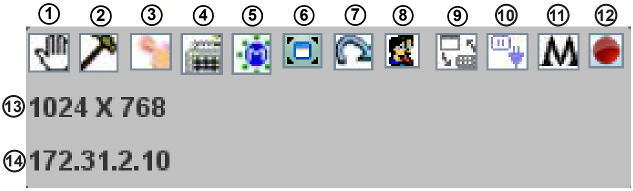


1. From the Options submenu, select *OSD UI Style* to display the OSD UI Style screen as shown below. This screen provides shortcuts to the main features provided by the firmware for your console redirection.

2. Click an OSD UI Style icon to change the settings listed on the next page.


Welcome to Windows
Microsoft Windows Server 2003 Enterprise Edition
Copyright © 1985-2003 Microsoft Corporation
Microsoft
Press Ctrl-Alt-Delete to begin.
Requiring this key combination at startup helps keep your computer secure. For more information, click Help.
Help
1024 X 768
172.31.2.10
2

The OSD UI Style Screen Close-up



1024 X 768

172.31.2.10

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.

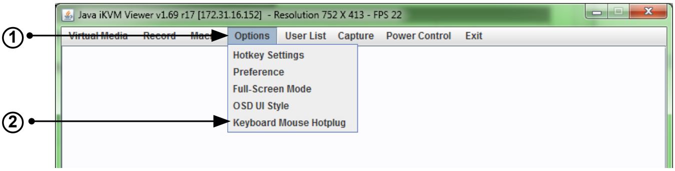
11. **Macro:** Click this item to enable Macro support and use Macro features.

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.

2.9.1.5.9 Console Redirection > Keyboard Mouse Hotplug

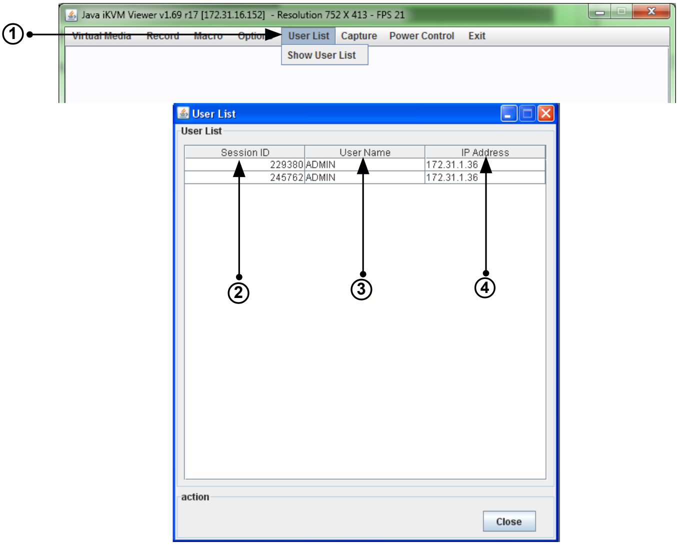


1. in the iKVM menu, select Options to display the submenu.

2. Click **Keyboard Mouse Hotplug** from the pull-down menu to simulate a keyboard/mouse hotplug on the remote console.

2.9.1.6 Console Redirection > User List

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



Session ID	User Name	IP Address
229380	ADMIN	172.31.1.36
245762	ADMIN	172.31.1.36

1. From the iKVM menu bar, click *User List* to display the screen shown above.

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

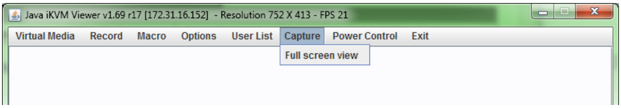
3. **User Name:** This item displays the name(s) of the user(s).

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

2.9.1.7 Console Redirection > Capture

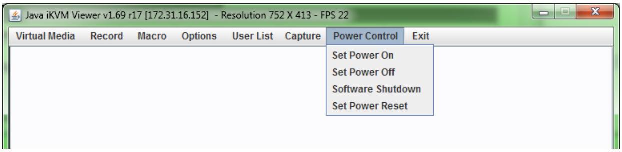
This feature allows you to capture the screen displayed on your remote console.

In the iKVM menu, click *Capture* > *Full Screen View* as shown below.



2.9.1.8 Console Redirection > Power Control

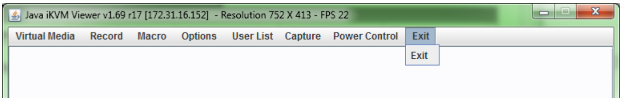
Use this feature to perform power functions using the remote console. In the iKVM menu, select *Power Control* to display the options as shown below.



The options in the Power Control submenu are described below.

- Set Power On: Powers on the server.
- Set Power Off: Powers off the server immediately.
- Software Shutdown: Powers off the server after OS shutdown functions have completed
- Set Power Reset: Reboots the server without powering off.

2.9.1.9 Console Redirection > Exit

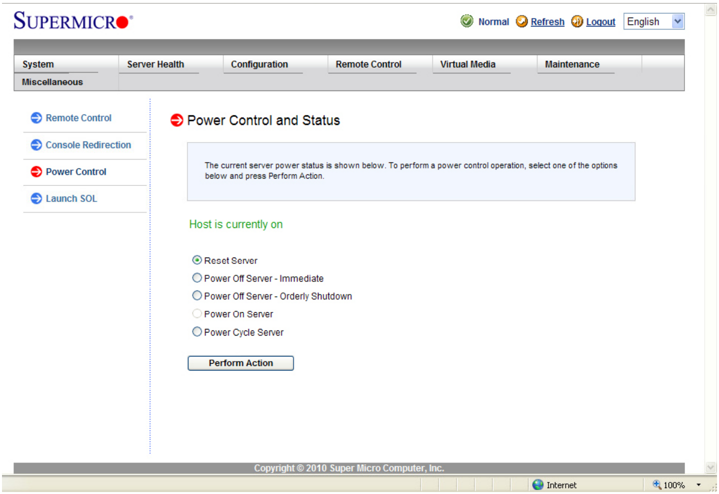

Java iKVM Viewer v1.69 r17 [172.31.16.152] - Resolution 752 X 413 - FPS 22
Virtual Media
Record
Macro
Options
User List
Capture
Power Control
Exit
Exit

To exit from Console Redirection, select Exit. At the prompt "Are you sure?", click **Yes** to exit from remote redirection or click **No** to return to the current session.

2.9.2 Remote Control - Server Power Control

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

Select from the following power options:



Power Control and Status

The current server power status is shown below. To perform a power control operation, select one of the options below and press Perform Action.

Host is currently on

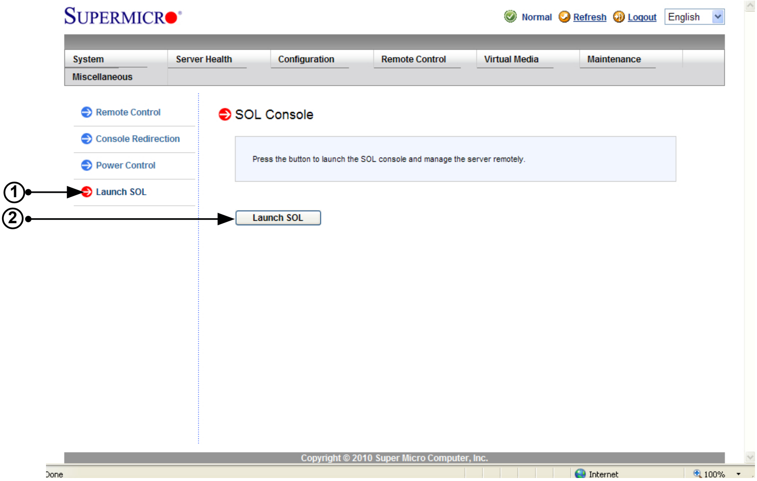
- ● Reset Server
- ○ Power Off Server - Immediate
- ○ Power Off Server - Orderly Shutdown
- ○ Power On Server
- ○ Power Cycle Server

- Reset Server: Select this optoin to reset the server.
- Power Off Server - Immediate: Select this option to shut down the server immediately.
- Power Off Server - Orderly Shutdown: Select this option to shut down the server after OS shutdown functions have completed.
- Power On Server: Select this option to power on the server. This option is only available if the server is not currently powered on .
- Power Cycle Server: Select this option to simulate an AC power cycle. The server will power off, then power on after a couple seconds.

Note: Power cycling the server via IPMI is not the same as an actual power cycle. Stanby power is still available.

2.9.3 Remote Control > Launch SOL

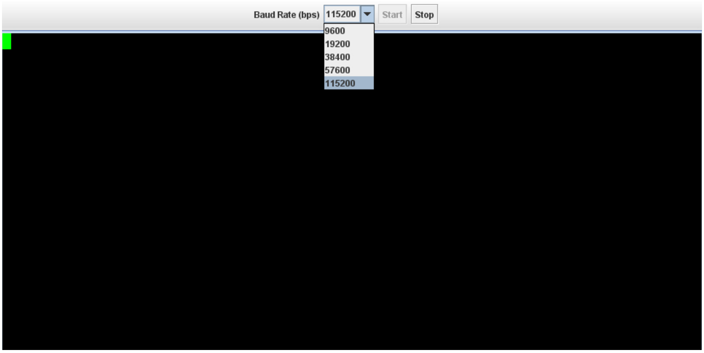
This feature allows you to launch the remote console by using SOL (Serial over LAN). This feature provides serial port connections over LAN to provide access to a host server via Console Redirection. It also allows a system administrator to monitor and manage a server from a remote site. To launch SOL, follow the instructions below.



Press the button to launch the SOL console and manage the server remotely.

1. In the Remote Control submenu, select *Launch SOL* to display the screen shown above.

2. Click **Launch SOL** to launch SOL. After SOL is launched, the following screen displays.



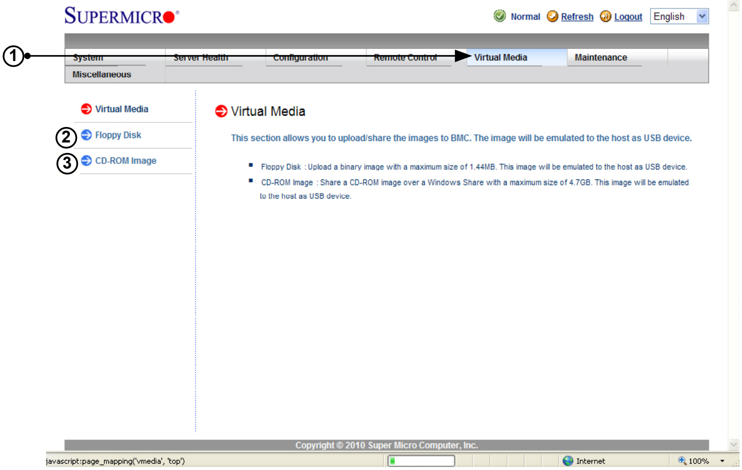
Select a Baud Rate (bps) from the pull-down menu as your SOL transfer rate. The options are listed below. Make sure that the Baud Rate selected here matches the Baud Rate set in the BIOS.

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

After selecting the Baud rate, click **Start** to start the session. Once a session has started, click **Stop** at any time to stop SOL connection.

2.10 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 configure the Virtual Media settings, follow the instructions below.



Virtual Media

This section allows you to upload/share the images to BMC. The image will be emulated to the host as USB device.

- Floppy Disk : Upload a binary image with a maximum size of 1.44MB. This image will be emulated to the host as USB device.
- CD-ROM Image : Share a CD-ROM image over a Windows Share with a maximum size of 4.7GB. This image will be emulated to the host as USB device.

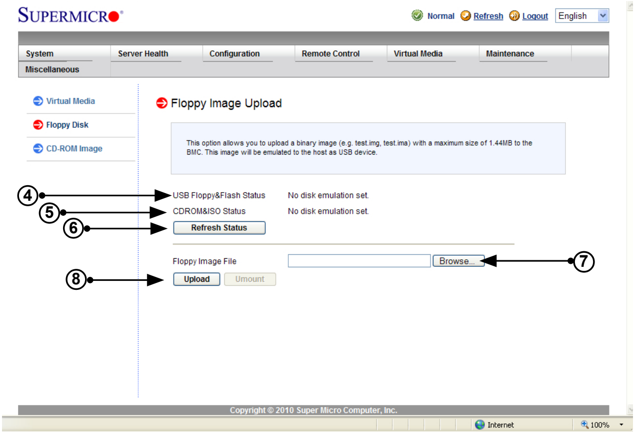
1. Select *Virtual Media* to configure virtual media settings for your remote console, including Floppy Disk and CD-ROM image settings.

2. Select *Floppy Disk* to configure the floppy disk settings for your console redirection.

3. Select CD-ROM Image to configure CD-ROM image settings for your console redirection.

2.10.1 Configuring USB Floppy & Flash Device Settings

To configure USB floppy and flash device settings, follow the instructions below.



This option allows you to upload a binary image (e.g. test.img, test.ima) with a maximum size of 1.44MB to the BMC. This image will be emulated to the host as USB device.

USB Floppy&Flash Status: No disk emulation set.

CDROM&ISO Status: No disk emulation set.

Floppy Image File

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 file system for your console redirection.

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

2.10.2 Configuring CD ROM Image File Settings

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

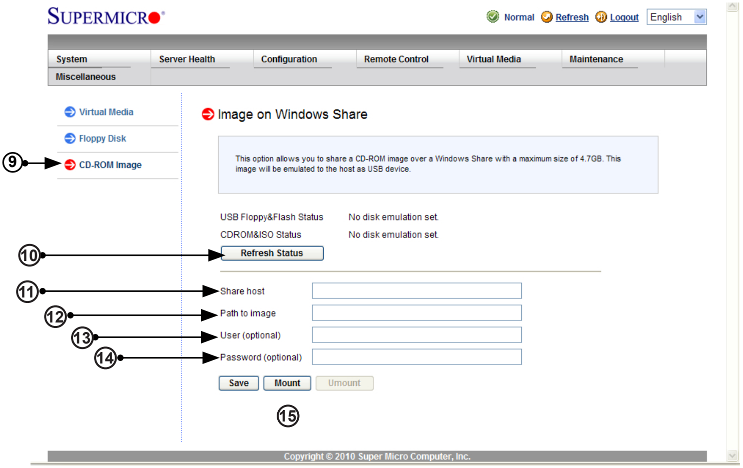


Image on Windows Share

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

USB Floppy&Flash Status No disk emulation set.
CDROM&ISO Status No disk emulation set.

Share host
Path to image
User (optional)
Password (optional)

9. In the Virtual Media submenu, select *CD-ROM Image* to display the screen shown above.

- *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. Enter the path to the CD-ROM image file for sharing.

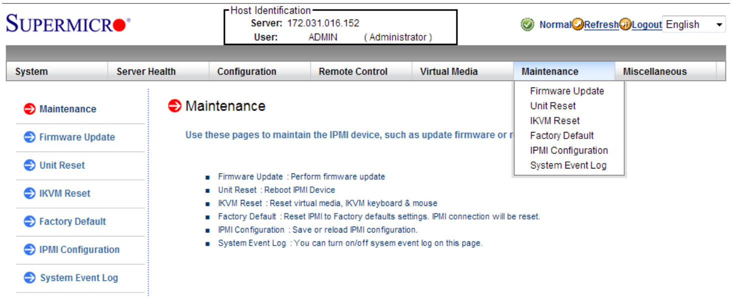
13. Specify the user that has access to the CD-ROM image files. (This item is optional).

14. Enter your user password (optional).

15. To mount or unmount an image file, click Mount or Unmount, then click the Save button.

2.11 Maintenance

Use this feature to manage and configure IPMI device settings.



Host Identification
Server: 172.031.016.152
User: ADMIN (Administrator)

Maintenance

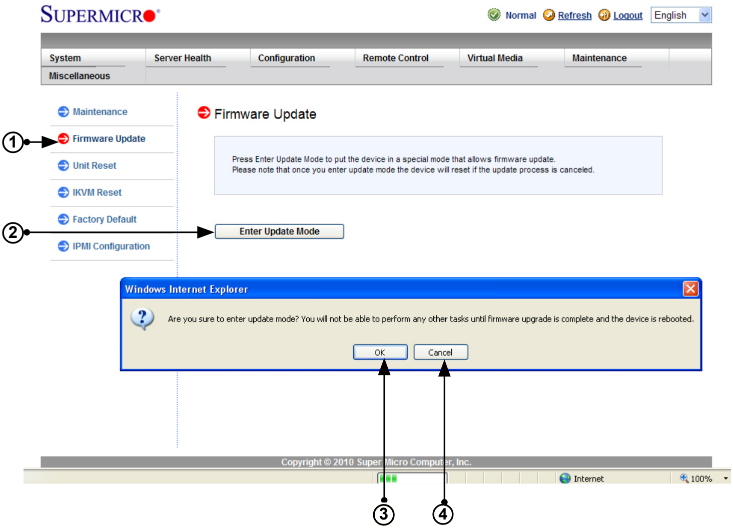
Use these pages to maintain the IPMI device, such as update firmware or r

- Firmware Update : Perform firmware update
- Unit Reset : Reboot IPMI Device
- IKVM Reset : Reset virtual media, IKVM keyboard & mouse
- Factory Default : Reset IPMI to Factory defaults settings. IPMI connection will be reset.
- IPMI Configuration : Save or reload IPMI configuration.
- System Event Log : You can turn on/off sysem event log on this page.

Select *Maintenance* in the menu bar to display 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.
- **System Event Log**: Click this item to view the system event logs.

2.11.1 Maintenance > Firmware Update



Press Enter Update Mode to put the device in a special mode that allows firmware update.
Please note that once you enter update mode the device will reset if the update process is canceled.

Are you sure to enter update mode? You will not be able to perform any other tasks until firmware upgrade is complete and the device is rebooted.

Firmware Update

To update IPMI Firmware, follow the instructions below.

1. In the Maintenance submenu, select *Firmware Update*.

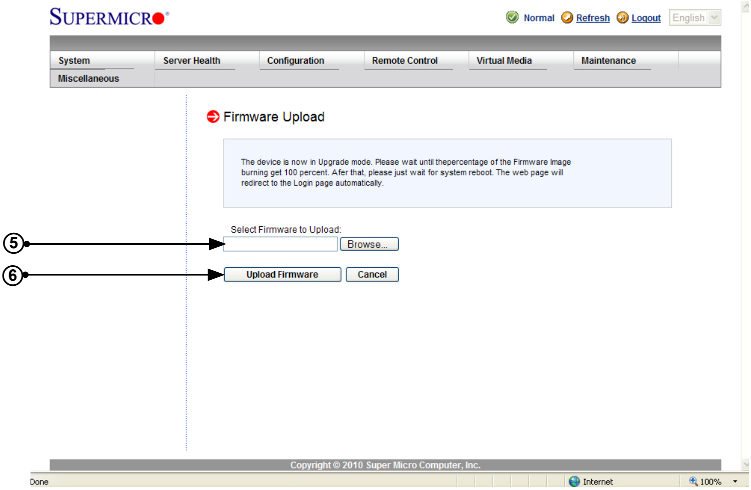
2. Click **Enter Update Mode** to enter the update mode. A warning message will display.

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.

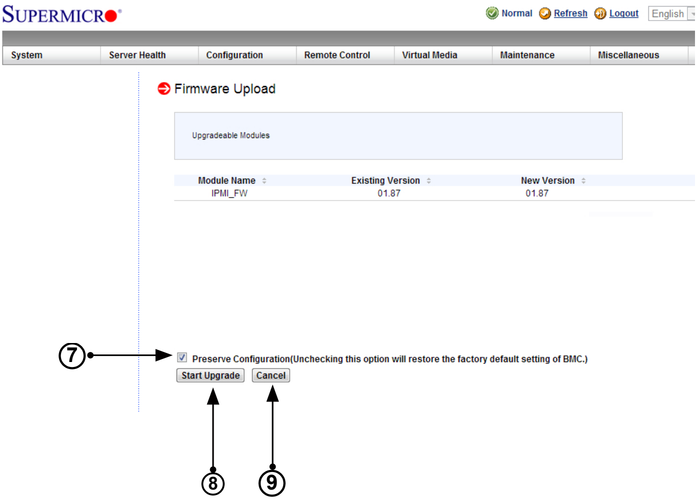
Once you have clicked OK to update the IPMI Firmware, the Firmware Upload screen displays as shown below.



The device is now in Upgrade mode. Please wait until thepercentage of the Firmware Image burning get 100 percent. Afer that, please just wait for system reboot. The web page will redirect to the Login page automatically.

5. Enter the name of the firmware you wish to upload. You can also select a firmware by clicking the **Browse** button.

6. Click **Upload Firmware** and the following screen will display.



Firmware Upload

Upgradeable Modules

Module Name	Existing Version	New Version
IPMI_FW	01.87	01.87

☑ Preserve Configuration(Unchecking this option will restore the factory default setting of BMC.)

7. If you would like to keep the current configuration, check the Preserve Configuration checkbox.

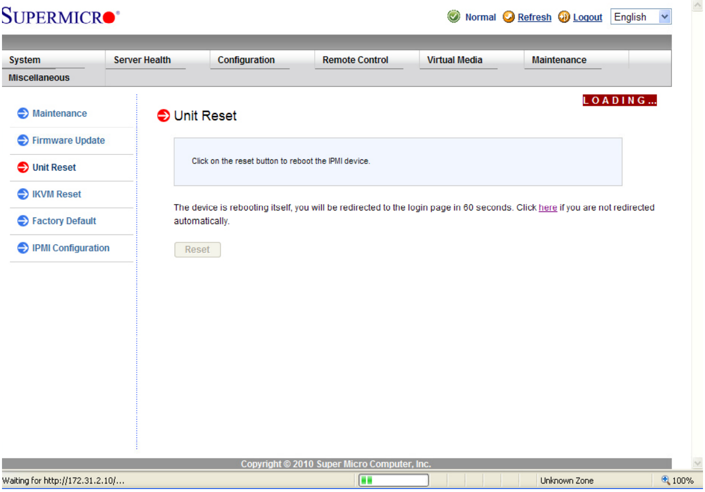
8. Click **Start Update** to begin uploading the selected firmware to the host server.

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.

9. Click **Cancel** to abort firmware uploading.

2.11.2 Maintenance > Unit Reset

Use this feature to reset the IPMI device.

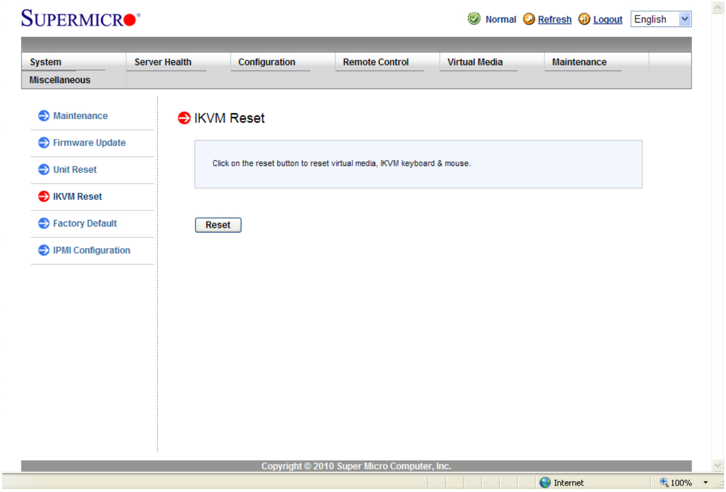


Click on the reset button to reboot the IPMI device.

The device is rebooting itself, you will be redirected to the login page in 60 seconds. Click here if you are not redirected automatically.

2.11.3 Maintenance > IKVM Reset

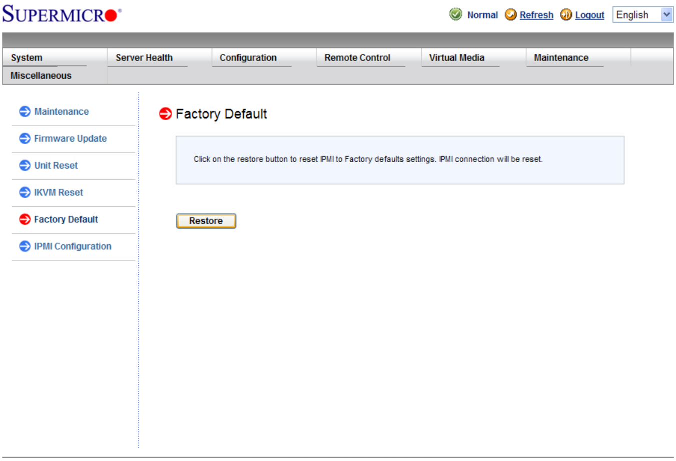
This feature allows you to reset iKVM. It will reset virtual media, iKVM keyboard and mouse.



Click on the reset button to reset virtual media, IKVM keyboard & mouse.

2.11.4 Maintenance > Factory Default

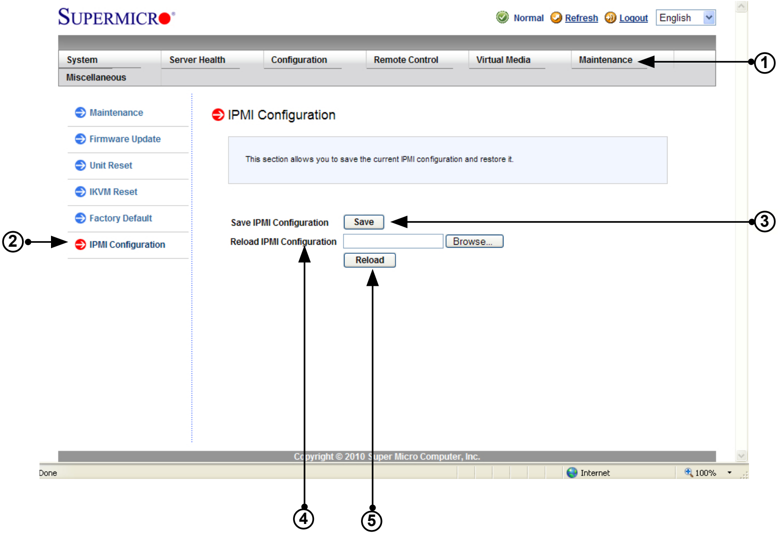
This feature allows the user to restore IPMI to factory default settings.



Click on the restore button to reset IPMI to Factory defaults settings. IPMI connection will be reset.

2.11.5 Maintenance > IPMI Configuration

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



This section allows you to save the current IPMI configuration and restore it.

1. From the top menu bar, select *Maintenance*.

2. In the Maintenance submenu, select *IPMI Configuration*.

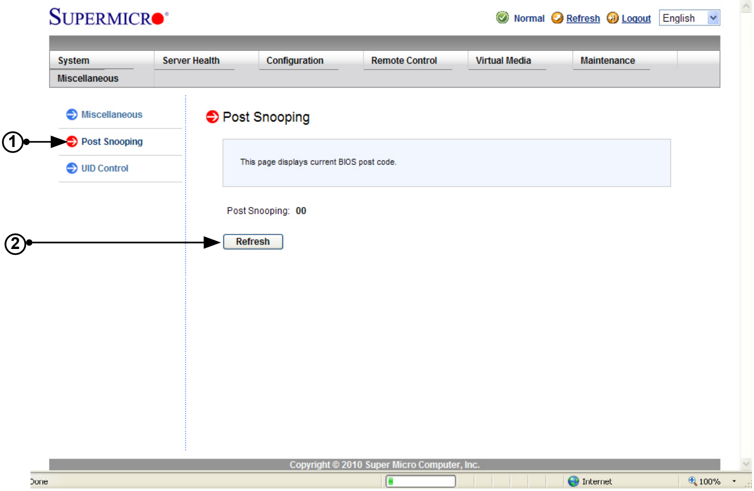
3. Click **Save** to save the IPMI Configuration settings.

4. To reload an IPMI configuration, click the **Browse** button and select an IPMI configuration.

5. Click **Reload** to reload the IPMI configuration that you seleted.

2.12 Miscellaneous > POST Snooping

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.



Post Snooping

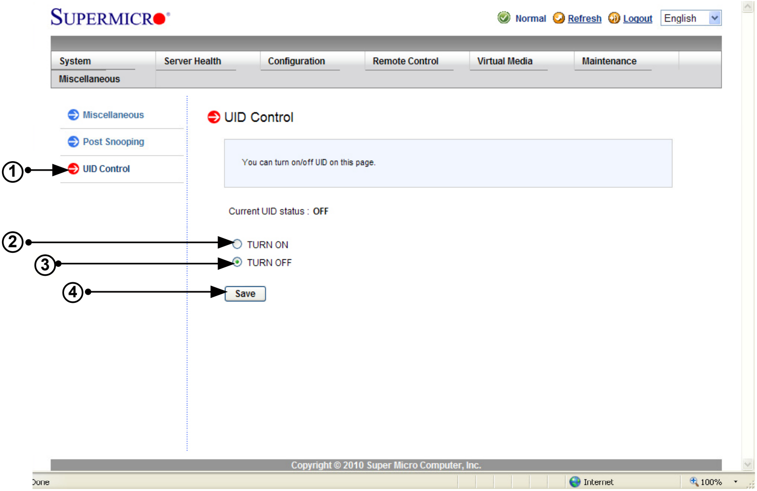
This page displays current BIOS post code.

Post Snooping: 00

1. In the Miscellaneous submenu, select *Post Snooping* to display the screen shown above.
2. Click **Refresh** to query the POST Snooping code for BIOS LPC Port80.

2.12.1 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.



UID Control

You can turn on/off UID on this page.

Current UID status : OFF

○ TURN ON

● TURN OFF

1. In the Miscellaneous submenu, select **UID Control** to display the screen shown above.

2. Select Turn On to turn on UID control.

3. Select Turn Off to turn off UID control.

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

Chapter 3

Frequently Asked Questions

3.1 Frequently Asked Questions

A. Question: How do I flash the IPMI firmware?

Answer:

Method#1

1. In the IPMI menu bar, click Maintenance. Browse the files available and select the correct file to flash the firmware.

2. Click the Update Firmware button to proceed with firmware flashing.

Method#2

- You can flash the IPMI firmware using flash tools located at: ftp://ftp.supermicro.com/utility/IPMI FW flash tools/.

- For the latest IPMI Firmware, please refer to: http://www.supermicro.com/products/nfo/ipmi.cfm

B. 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)

C. Question: When trying to update IPMI firmware through the web, I got a file download pop-up, but the firmware was not updated. Why?

Answer: This may be caused by your anti-virus software. Some anti-virus software can cause this. Disable your anti-virus software temporarily and update your firmware.

D. 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.

Appendix A

Flash Tools

A-1 Overview

This chapter provides instructions on how to use SMT Flash Tools. The SMT Flash Tools Utility supports firmware updates and firmware dumping.

1. Firmware Updates

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

2. Firmware Dumping

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

A-2 Reference

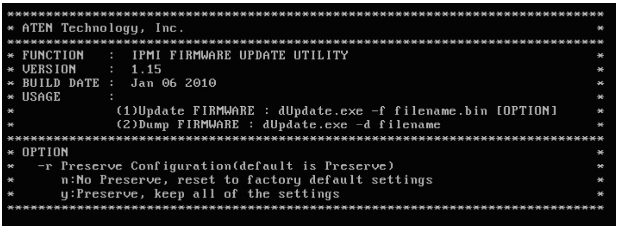
The SMT Flash Tools Utility was built in reference to the IPMI - Intelligent Platform Management Interface Specification Second Generation v2.0, Document Revision 1.0, February 12, 2004, by Intel, Hewlett-Packard, NEC, and Dell.

A-3 Using SMT Flash Tools in the DOS Environment

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

1. Enter <dupdate.exe> and press <Enter>.

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



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

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

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

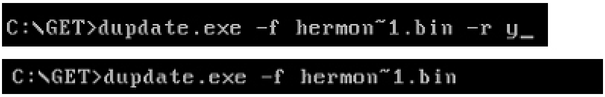
Firmware Updating via KCS Channels

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

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

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

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



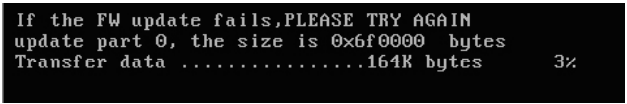
```
C:\GET>dupdate.exe -f hermon~1.bin -r y_
```

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

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

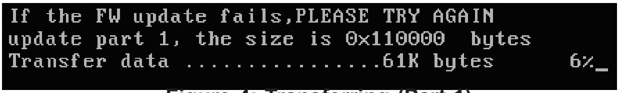
After you've entered the commands above, SMT Flash Tools will start to update the firmware. There are two phases in firmware updating.

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



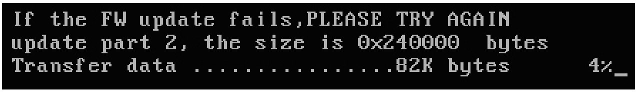
```
If the FW update fails,PLEASE TRY AGAIN
update part 0, the size is 0x6f0000  bytes
Transfer data ................164K bytes       3%
```

Figure 3: Transferring (Part 0)



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

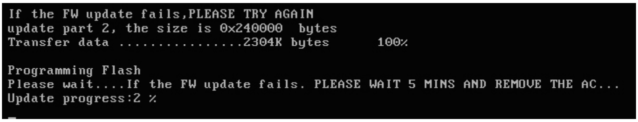
Figure 4: Transferring (Part 1)



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

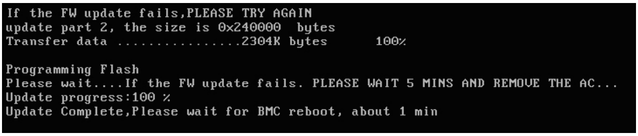
Figure 5: Transferring (Part 2)

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



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

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

Figure 6: Progress of Firmware Updating

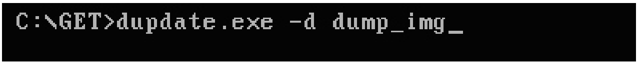


```
If the FW update fails,PLEASE TRY AGAIN
update part 2, the size is 0x240000  bytes
Transfer data ................2304K bytes      100%

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

Figure 7: Updates Completed

Dumping Firmware from the BMC via KCS channels

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



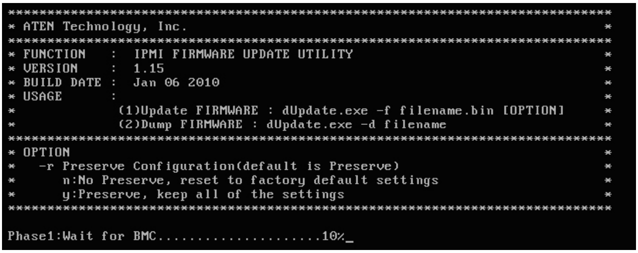
```
C:\GET>dupdate.exe -d dump_img_
```

Figure 8: Example of Firmware Dumping via KCS

There are two phases in firmware dumping.

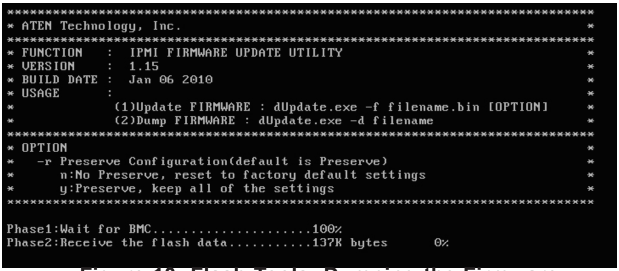
1. During Phase 1, the Flash Tools Utility is waiting for the BMC to prepare the firmware for dumping. As soon as preparation is complete, the Flash Tools Utility will enter Phase 2.

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



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

Phase1:Wait for BMC.....................10%_
```

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



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

Phase1:Wait for BMC.....................100%
Phase2:Receive the flash data...........137K bytes      0%
```

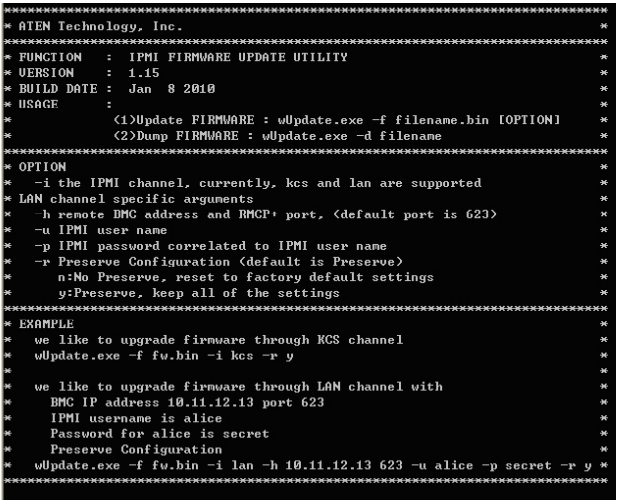
Figure 10: Flash Tools Dumping the Firmware

A-4 Windows/Linux Version of Flash Tools

In addition to DOS, SMT Flash Tools Utility supports Windows and Linux platforms.

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

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



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

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

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

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

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

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

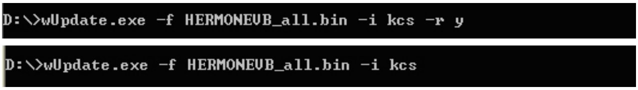
2. –u: Type <-u> to enter the IPMI username.

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

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

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

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

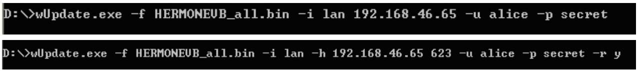


```
D:\>wUpdate.exe -f HERMONEVB_all.bin -i kcs -r y
```

```
D:\>wUpdate.exe -f HERMONEVB_all.bin -i kcs
```

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

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



```
D:\>wUpdate.exe -f HERMONEVB_all.bin -i lan 192.168.46.65 -u alice -p secret
```

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

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

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

Notes

Appendix B

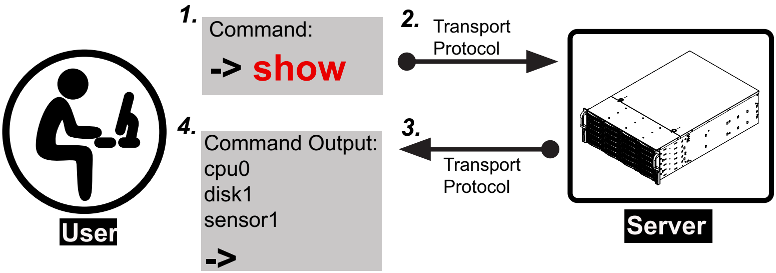
Introduction to SMASH

B-1 Overview

The SMASH (System Management Architecture for Server Hardware) platform, developed by Distributed Management Task Force, Inc. (DMTF), delivers a host of architecture-based, industry-standard protocols that 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.



1.
```
Command:
-> show
```

4.
```
Command Output:
cpu0
disk1
sensor1
->
```

Figure 1 SMASH-CLP User Interface

SMASH Compliance Information

SMASH documented in this user's guide is developed in reference to and in compliance with the SMASH Initiative Standards based on the following DMTF documents.

- System Management Architecture for Server Hardware (SMASH) Command Line Protocol (CLP) Architecture White Paper (DSP 2001)
- SM CLP Specification (DSP 0214)
- SM ME Addressing Specifications (DSP 0215)
- SM SLP to CIM Common Mapping Specification (DSP 0216)
- Common Information Model (CIM) Infrastructure Specification (DSP0004)
- The Secure Shell (SSH) Protocol Architecture (RFC4251)
- The Secure Shell (SSH) Connection Protocol (RFC4254)

B-2 An Important Note to the User

The information included in this user's guide provides a general guideline on how to use the SMASH protocol for your system management. Instructions given in this document may or may not be applicable to your system; it depends on the configuration of the system or the environment it operates in.

B-3 Using SMASH

This section provides a general guideline on how to use SMASH for your system management in a web-based environment. Refer to the SMASH script provided below to curtail a server management protocol for your systems.

Note: The instructions listed below are applicable to both Windows and Linux systems. We use the Windows platform as our default setting.

B-4 Initiating the SMASH Protocol

There are two ways of initiating the SMASH protocol.

To Initiate SMASH Automatically

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

To connect from a Linux machine

1. Use 'ssh<BMC ip address>'.

2. Enter the password.

To connect from other machines

1. Use a terminal emulator application such as *Putty*.

2. Enter the *BMC ip* address in the terminal emulator application.

3. Choose *ssh* as the connection type

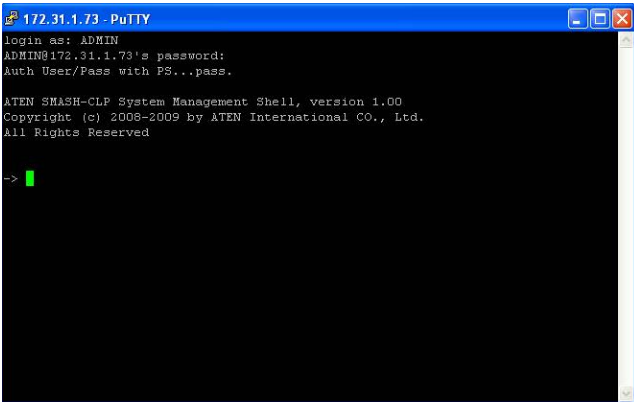
4. Enter the password at the prompt.

5. At the prompt '#", enter <SMASH> to invoke the SMASH prompt '—>'.

6. If you have successfully logged in, the SMASH prompt will display.

B-5 SMASH-CLP Main Screen

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



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

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


->
```

Figure 2 SMASH-CLP Main Screen

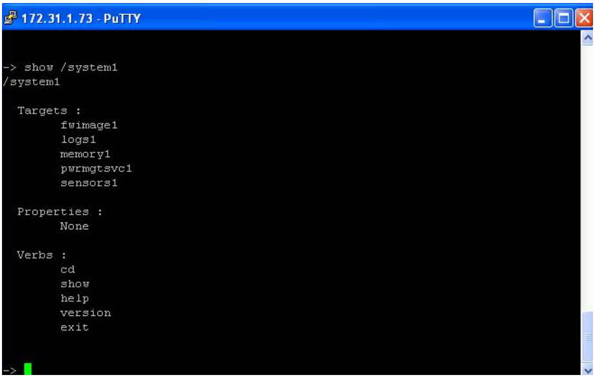
B-6 Using SMASH for System Management

After you've familiarized yourself with 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.



```
-> show /system1
/system1

  Targets :
        fwimage1
        logs1
        memory1
        pwrmgtsvc1
        sensors1

  Properties :
        None

  Verbs :
        cd
        show
        help
        version
        exit


->
```

Figure 3 Using SMASH for System Management

B-7 Definitions of Command Verbs

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

- ***cd***

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

- ***show***

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

- ***exit***

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

- ***help***

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

- ***Version***

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

- ***set***

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

- ***start***

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

- ***stop***

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

- ***reset***

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

- ***delete***

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

- ***load***

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

- ***dump***

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

- ***create***

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

B-8 SMASH Commands

The following table provides the definitions and the descriptions of SMASH commands. The most useful commands are *show* and *help*, which will provide the user with 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

B-9 Standard Command Options

The following table lists the standard command options.

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

Table 2 Standard Command Options

B-10 Target Addressing

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

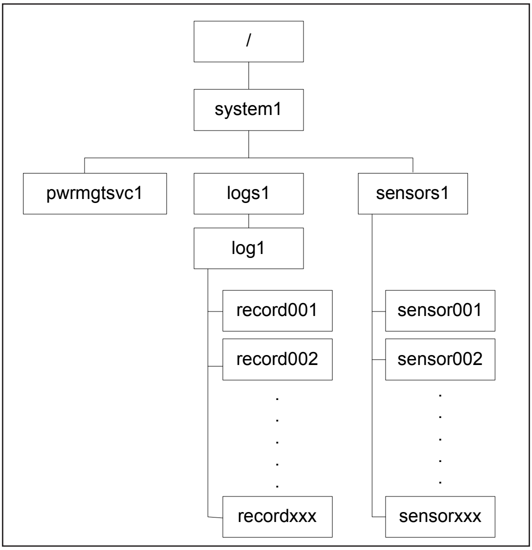


Figure 4 Target Addressing Diagram

Terms Used in the Target Addressing Diagram

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

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

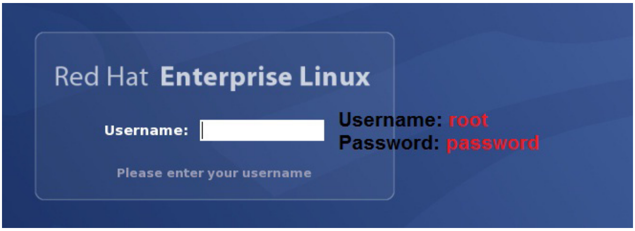
Notes

Appendix C

RADIUS Setup Guidelines

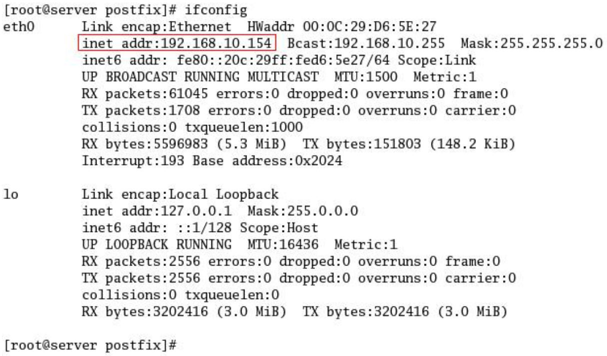
This chapter provides the Radius setup guidelines for IPMI firmware.

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



Username: root
Password: password

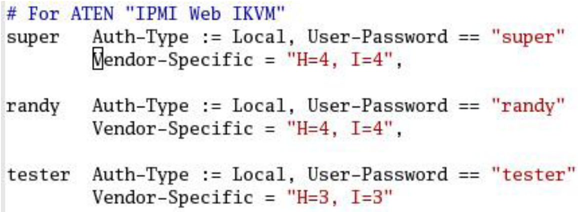
2. Check the IP address of the RADIUS server.



```
[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

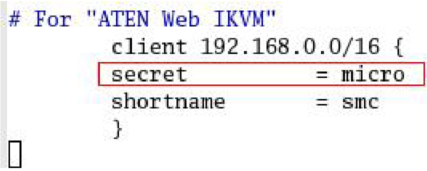


```
# For ATEN "IPMI Web IKVM"
super   Auth-Type := Local, User-Password == "super"
        Vendor-Specific = "H=4, I=4",

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.

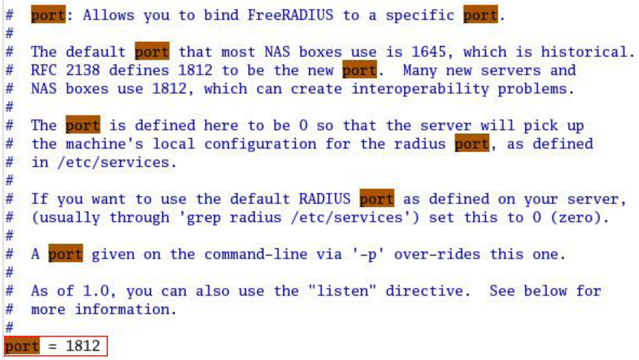
# vi /etc/raddb/client.conf



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

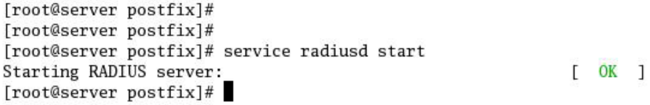
5. Configure Port information.

# vi /etc/raddb/radiusd.conf



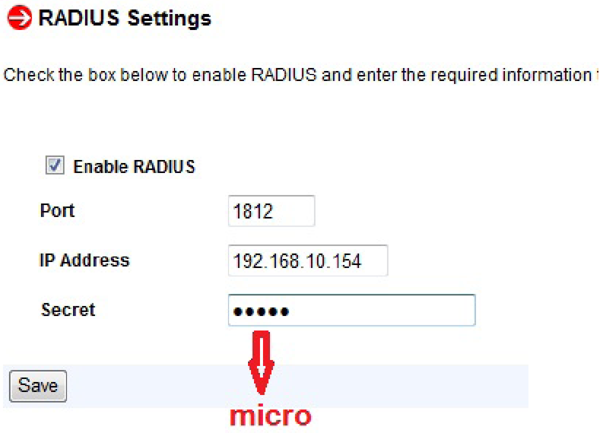
```
#  port: Allows you to bind FreeRADIUS to a specific port.
#
#  The default port that most NAS boxes use is 1645, which is historical.
#  RFC 2138 defines 1812 to be the new port.  Many new servers and
#  NAS boxes use 1812, which can create interoperability problems.
#
#  The port is defined here 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.



RADIUS Settings

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

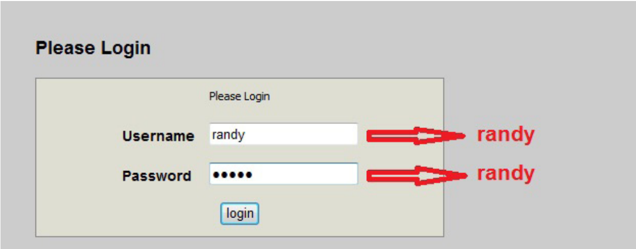
☑ Enable RADIUS

Port: 1812

IP Address: 192.168.10.154

Secret: ●●●●●

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



Please Login

Please Login

Username: randy

Password: ●●●●●

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.