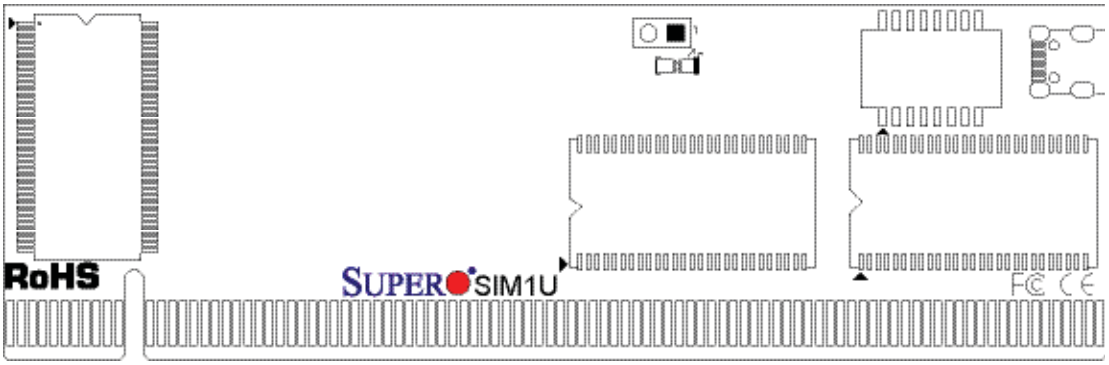
SUPERMICRO®

SUPERMICRO® AOC-SIM1U/SIM1U+

Add-On Card



USER'S GUIDE

Rev. 1.1a

The information in this User's Guide has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this user's guide, or to notify any person or organization of the updates.

Please Note: For the most up-to-date version of this user's guide, please see our web site at www.supermicro.com.

SUPERMICRO COMPUTER reserves the right to make changes to the product described in this user's guide at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

IN NO EVENT WILL SUPERMICRO COMPUTER BE LIABLE FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, 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, THE VENDOR 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.

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.

User's guide Revision: Rev. 1.1a

Release Date: July 16 , 2012

Printed in the United States of America

Table of Contents

Chapter 1
Introduction

This user's guide is written for system integrators, PC technicians and knowledgeable PC users who intend to integrate Supermicro's unique IPMI 2.0 Management Utility with support of KVM-over-LAN () into their systems. It provides detailed information for the application and use of the AOC-SIM1U/SIM1U+ that supports remote access for system monitoring, diagnosis and management. With the most advanced technologies built-in, the AOC-SIM1U/SIM1U+ offers a complete, efficient, and cost-effective remote server management.
(**Note:** KVM-over-LAN is only for the AOC-SIM1U+ only.)

1.1 Overview

The AOC-SIM1U/SIM1U+ is a highly efficient, highly compatible and easy-to-use IPMI card that allows the user to take advantage of the BMC, a baseboard management controller installed on a server motherboard and the IPMIView, an IPMI-compliant management application software loaded in a PC, to provide serial links between the main processor and other system components, allowing for network interfacing via remote access. With an independent Raritan KIRA100 processor built-in, the AOC-SIM1U/SIM1U+ provides the user with a solution to ease the complex and expensive systems, allowing an administrator to access, monitor, diagnose and manage network interfacing anywhere, anytime.

1.2 IPMI Version 2.0

The AOC-SIM1U/SIM1U+ supports the functionality of IPMI Version 2.0. The key features include the following:

- Supports IPMI 2.0 over LAN
- Supports Serial over LAN
- Supports Virtual Media over LAN
- Supports KVM over LAN (For the AOC-SIM1U+ only)
- Supports LAN Alerting-SNMP Trap
- Supports Event Log
- Offers OS (Operating System) Independency
- Provides remote Hardware Health Monitoring via IPMI. Key features include the following:
    - Temperature monitoring
    - Fan speed monitoring
    - Voltage monitoring
    - Power status monitoring, chassis intrusion monitoring
    - Remote power control to power-on, power-off or reboot a system

- Remote access to text-based, graphic-based system information, including BIOS configurations and OS operation information (KVM)
- Remote management of utility/software applications

- Provides Network Management Security via remote access/console redirection. Key features include:
  - User authentication enhancement
  - Encryption support enhancement, allowing for password configuration security to protect sensitive data transferring via Serial over LAN
- Supports the following Management tools: IPMIView, CLI (Command Line Interface) and Webengine
- Supports RMCP & RMCP protocols

1.3. Product Features

(a) The AOC-SIM1U/SIM1U+ Series: (IPMI 2.0 with a Dedicated LAN)

- Slim size (4.6" W x 1.3" H) (116.84 mm W x 25.41 mm H)
- Supports IPMI over LAN
- Supports 1U and above
- Supports dedicated LAN

1.4 Checklist

If your shipping package came with missing or damaged parts, please contact Supermicro's Tech. Support. Please refer to the following checklist when contacting us.

i. AOC-SIM1U/SIM1U+

ii. Bracket: One bracket (SKT-0240L, including the AOC-USB2RJ45 Add-On Card, the CBL-0165L Cable, Full and Low Profile I/O Brackets.) (**The SKT-0240L is included in the SIM1U+ shipping package only.)**

iii. CDR-SIMIPMI: One Installation CD

iv. White Box with Correct Barcode Label (showing AOC-SIM1U/SIM1U+).

1.5 An Important Note to the User

The graphics shown in this user's guide were based on the latest PCB Revision available at the time of publishing of this guide. The SIM1U/SIM1U+ card you've received may or may not look exactly the same as the graphics shown in this user's guide.

1.6 Contacting Supermicro

Headquarters

Address: SuperMicro 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 Informaion)
support@supermicro.com (Technical Support)
Web Site: www.supermicro.com

Europe

Address: SuperMicro 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: SuperMicro, Taiwan
4F, No. 232-1 Liancheng Road
Chung-Ho Dist., New Taipei City 235
Taiwan, R.O.C.
Tel: +886-(2) 8226-3990
Fax: +886-(2) 8226-3991
Web Site: www.supermicro.com.tw
Email: support@supermicro.com.tw (Technical Support)
Tel: +886-(2) 8226-5990 (Technical Support)

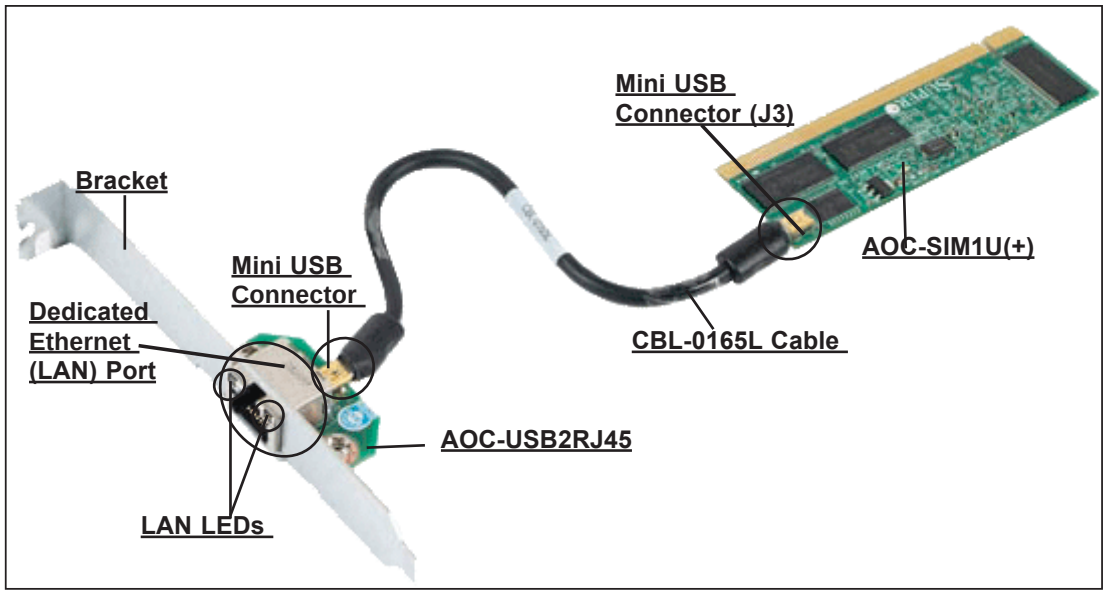
Chapter 2
Technical Specifications and Hardware Installation

2.1 Configuring the AOC-SIM1U/SIM1U+ and the AOC-USB2RJ45 Add-On Cards

The AOC-SIM1U/SIM1U+ Add-On Card is connected to a Dedicated LAN Ethernet port located on the AOC-USB2RJ45 Add-On Card via an SMC Proprietary cable (CBL-0165L) for External LAN access. One end of the CBL-0165L cable is connected to the mini USB connector (J3) located on the AOC-SIM1U(+) card and the other end to that of the AOC-USB2RJ45 card. There are two LEDs located on the LAN port to indicate network links and activities. Refer to the picture below for the configuration.

***Note 1:** You can also use LAN1 on the motherboard if you do not need the dedicated LAN support. However, dedicated LAN is recommended for better graphic support when the KVM feature is used.

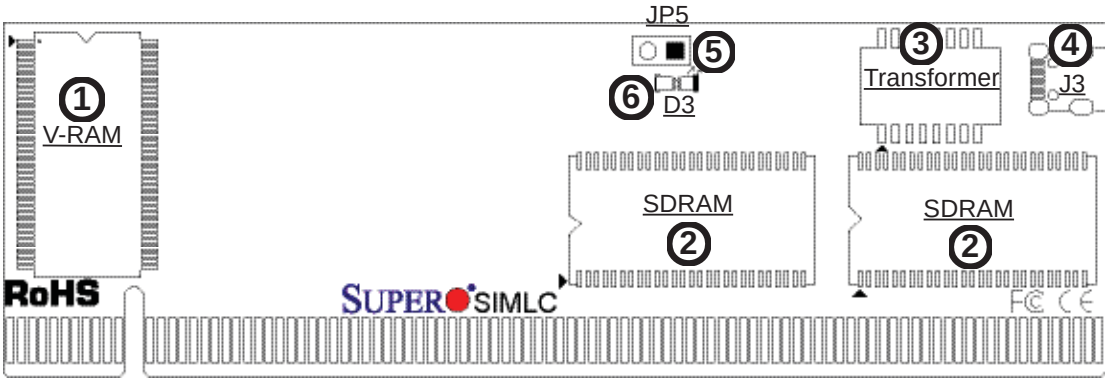
***Note 2**: The SKT-0240L is included in the SIM1U+ shipping package only.



The SKT-0240L (*Note 2 above)

2.2 AOC-SIM1U/SIM1U+ Connector and Jumper Locations

Front View



(***Note**: "■", "◗", or "▌" indicates Pin 1.)

2.2.1 Front Components on the AOC-SIM1U(+)

1. V-RAM (64Mb/166MHz)
2. SDRAM (128Mb/133MHz)
3. Transformer
4. J3: Mini USB 9-pin Connector **(*Note)**
5. JP5: Kira 100 Processor Reset **(*Note)**
6. D3: Standby Power LED Indicator

2.2.2 The Dedicated LAN LED Indicators on the AOC-USB2RJ45

8. Dedicated LAN LED Indicators **(*Note)**

(***Note**: See Pages 2-3, 2-4 for details)

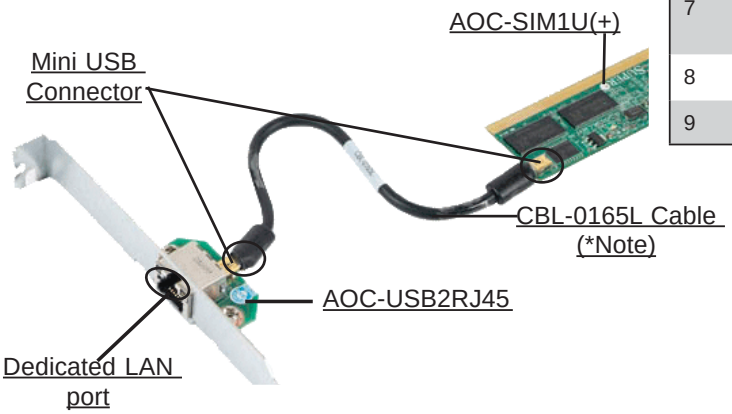
2.2.3 Front Connector and LED Indicators

#4. J3: Mini USB Connector

There is a mini USB connector (J3) located on the AOC-SIM1U/SIM1U+ and another mini USB connector is located on the AOC-USB2RJ45. Use Cable CBL-0165L to connect the two mini USB connectors on both add-on cards for external LAN access. Refer to Page 2-1 for details. See the table at right for the pin definitions.

Mini USB Pin Definitions (J3)

Pin#	Definition
1	Eth-TX_H
2	Eth-TX_L
3	Phy-100
4	Eth-RX_L
5	Eth-RX_H
6	Phy-ACT
7	Dedicated LAN-Detected
8	3V-duall
9	Ground



The SKT-0240L (*Note below)

#5. JP5: RISC CPU Reset

JP5 is used to reset the Kira 100 Processor, NIC, and R.T. Close Pin 1 and Pin 2 to enable this function.After a reset or AC power-on, the AOC-SIM1U(+) will automatically detect if a cable (CBL-0165L) is connected. If a cable is not detected, the AOC-SIM1U(+) will transfer the "Remote Control" Function to LAN1 on the motherboard. If a cable is detected, the AOC-SIM1U(+) will use the dedicated LAN attached to it via the mini USB connector to manage motherboard activities via Remote Console. See the table on the right for jumper settings.

RISC CPU Reset

Setting	Description
Open	Disabled (*Default)
Close	Enabled

***Note**: The SKT-0240L is included in the SIM1U+ shipping package only.

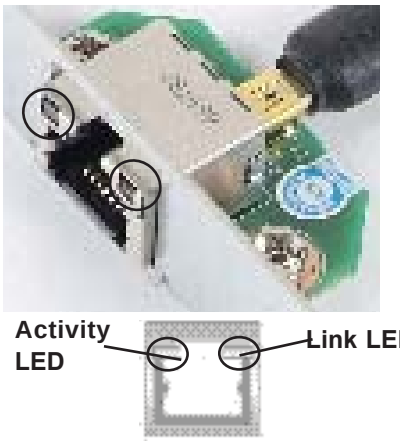
#7. D3: Standby Power LED Indicator

When this LED is on, the standby power is on. Be sure to remove power cables before installing or removing components.

2.2.4 Dedicated LAN LED Indicators

#8. Dedicated LAN LED Indicators

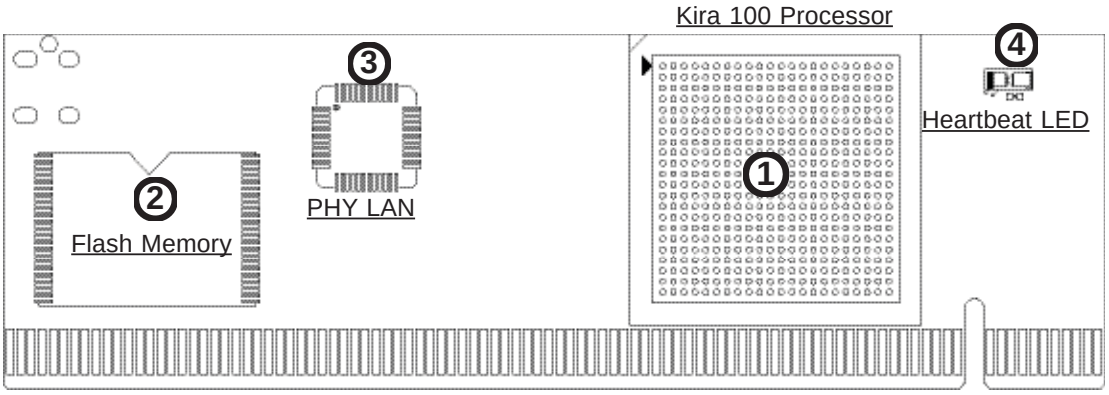
There are two LAN LED Indicators located on the (Dedicated) LAN port on the AOC-USB2RJ45 Add-On Card. The green LED indicates activity, while the power LED may be green or off to indicate the speed of the Ethernet connection. See the tables on the right for more information.



GLAN Activity Indicator		
Color	Status	Definition
Amber	Flashing	Active

GLAN Link Indicator	
LED Color	Definition
Off	No Connection or 10 Mbps
Green	100 Mbps

Rear View



2.2.5 Rear Components on the AOC-SIM1U(+)

Rear Side Components

1. Raritan's Kira 100 RISC System on Chip
2. Flash Memory
3. PHY LAN
4. Heartbeat LED

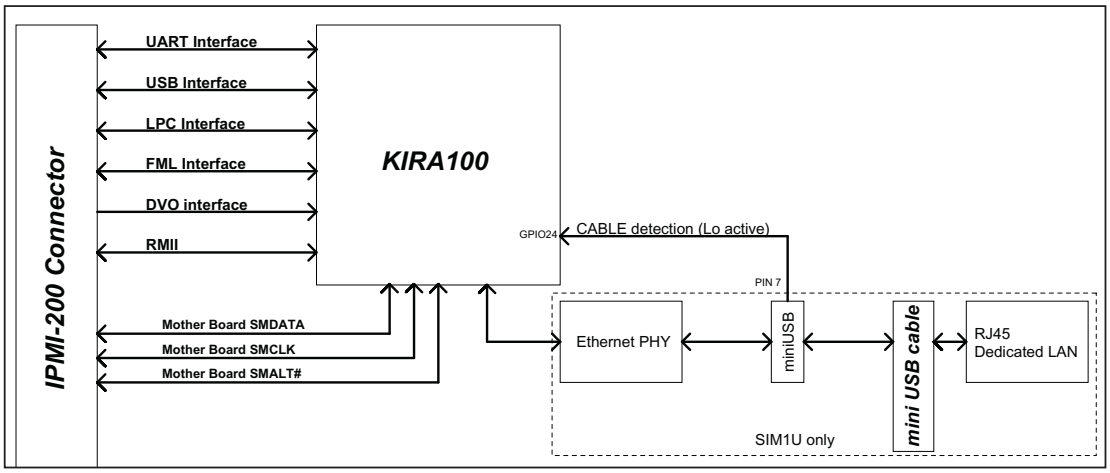
2.2.6 Rear Side LED Indicators

#4 Heartbeat LED Indicator

Heartbeat LED, located on the rear side of the AOC-SIM1U(+) card, indicates the functionality and activity of the add-on card. Heartbeat LED blinks when the AOC-SIM1U(+) is active. However, when the Linux OS and the drivers are being loaded after each AC power-on or reset, Heartbeat LED is off for about a minute. Then, Heartbeat LED will be on again to indicate that the AOC-SIM1U(+) is active. See the table on the right for details.

Heartbeat LED	
On (Blinking)	SIM1U(+): active
Off (for 1 minute)	Loading Firmware
Off (Continuously)	SIM1U is not active

2.3 Block Diagram



2.4 Installing the AOC-SIM1U/SIM1U+

2.4.1 Safety Guidelines

To avoid personal injury and property damage, please carefully follow all the safety steps listed below when installing the AOC-SIM1U(+) into your system.

ESD Safety Guidelines

Electro-Static Discharge (ESD) can damage electronic components. To prevent damage to your system, it is important to handle it very carefully. The following measures are generally sufficient to protect your equipment from ESD.

- Use a grounded wrist strap designed to prevent static discharge.
- Touch a grounded metal object before removing a component from the antistatic bag.
- Handle the add-on card by its edges only; do not touch its components, peripheral chips, memory modules or gold contacts.
- When handling chips or modules, avoid touching their pins.
- Put the card and peripherals back into their antistatic bags when not in use.

General Safety Guidelines

- Always disconnect power cables before installing or removing any components from the computer.
- Disconnect the power cable before removing any cable from the add-on card.
- Make sure that the SIM1U(+) add-on card is securely seated in the SIM1U slot to prevent damage to the system due to power shortage. For SIM1U slot locations, please refer to Section 2.4.2.

SMC Motherboards with SIM1U(+) support

The following Supermicro's motherboards support the AOC-SIM1U(+).

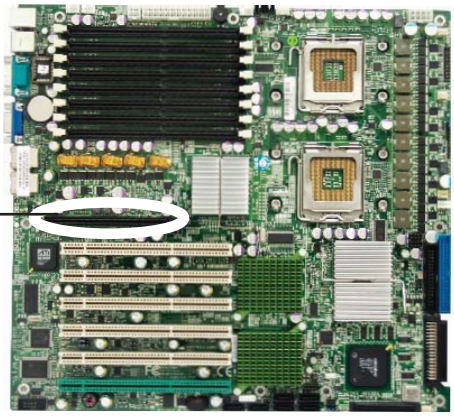
1. The X7DB8/X7DBE/X7DB8+/X7DBE+/X7DB8-X/X7DBE-X/X7DB3 Series
2. The X7DA8/X7DAE/X7DVA-8/X7DVA-E/X7DVL-3/i Series (*Note)
3. The X7DVL-E Series
4. The PDSM4+/PDSME+ Series

(***Note**: KVM-over-LAN is not supported by the X7DA8/X7DAE/X7DVL-3/i.)

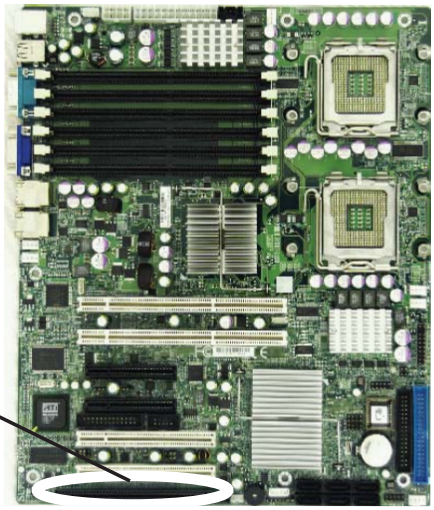
2.4.2 SIM1U Slot Locations

To properly use the AOC-SIM1U(+), be sure to install it in the right slot. Refer to the MB layouts below for SIM1U slot locations.

1. The X7DB8/X7DBE/X7DB8+/X7DBE+/X7DB8-X/X7DBE-X/X7DB3 Series and
2. The X7DA8/X7DAE/X7DVA-8/X7DVA-E/X7DVL-3/i Series (*Note)



3. The X7DVL-E



4. The PDSM4+/PDSME+ Series

(***Note**: KVM-over-LAN is not supported by the X7DA8/X7DAE/X7DVL-3/i.)

Chapter 3
Software Application and Usage

With an independent I/O processor embedded in Raritan's Kira 100 RISC System Chip, the AOC-SIM1U/SIM1U+ Add-On Card allows the user to access, monitor, manage and interface with systems that are in remote locations via LAN. (See the note on Page 3-2.) The necessary utilities for the access and configuration of the add-on card are included on the Supermicro bootable CDs that came with your card. This section provides information on the configuration and the access of the IPMI card on the network.

Using the IPMICFG Utility to Configure IP/MAC Addresses and other IPMI Network Settings

1. Run the ipmicfg utility from the bootable CD that came with your shipment.

2. Refer to the table below to configure the IP/MAC addresses.

Board	IPMI	MAC	IP	Communication through
X7 Series	SIM1U	IPMI Card	Available IP/DHCP	Dedicated LAN
				LAN1 on MB
H8 DDR2 Memory	SIM1U	IPMI Card	Available IP/DHCP	Dedicated LAN
				LAN1 on MB
H8QM3/i-x (**Note 2** below)	SIM1U	IPMI Card	Available IP/DHCP	Dedicated LAN
		LAN1	LAN1	LAN1 on MB

3. Follow the instructions given in the Readme.txt file to configure Gateway IP/Net-mask IP addresses, to enable/disable DHCP and to configure other IPMI settings.

Note 1: The Readme.txt file is included in the CD that came with your shipment. A copy of the Readme.txt file, dated 07/05/2007, is also included below.

IPMICFG Version 1.04 Copyright 2007 SuperMicro Computer Inc.

Usage: IPMICFG Parameters (Example: IPMICFG -m 192.168.1.123)

-m	Show IP and MAC
-m IP	Set IP (format: ###.###.###.###)
-a MAC	Set MAC (format: ##:##:##:##:##:##)
-k	Show Subnet Mask
-k Mask	Set Subnet Mask (format: ###.###.###.###)
-dhcp on	Enable the DHCP
-dhcp off	Disable the DHCP
-g	Show Gateway IP
-g IP	Set Gateway IP (format: ###.###.###.###)

Note 2: For the H8QM3/i-2(+), the AOC-SIM1U(+) IPMI card has to flash the firm-ware bin from \Firmware\H8Qxx-x in the driver CD. If the AOC-SIM1U(+) IPMI card communicates through the onboard LAN1 on the H8QM3/i-2(+), you can only use the IPMIView Utility to access the AOC-SIM1U(+) IPMI card.

To Access the SIM1U/SIM1U+ Card from a Computer

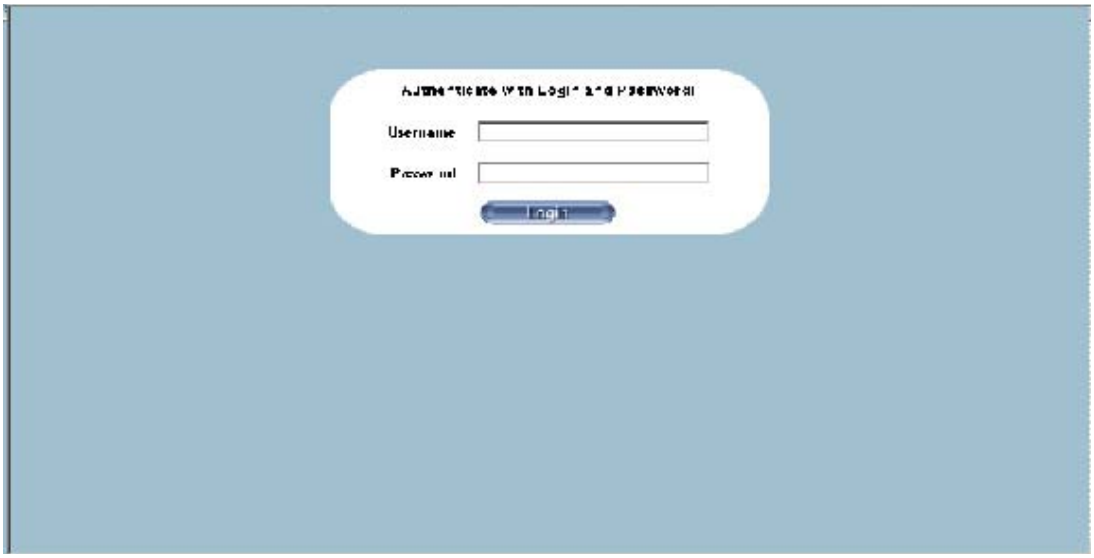
1. Choose a computer that is connected to the same network and open the browser.

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

3. Once the connection is made, the Log In screen as shown below displays.

To Log In

Once you are connected to the remote server, the following Log In screen displays.



1. Type in your Username in the "Username" box.

2. Type in your Password in the "Password" box and click on "Login."

(**Note**: The default username is ADMIN. The default password is ADMIN.)

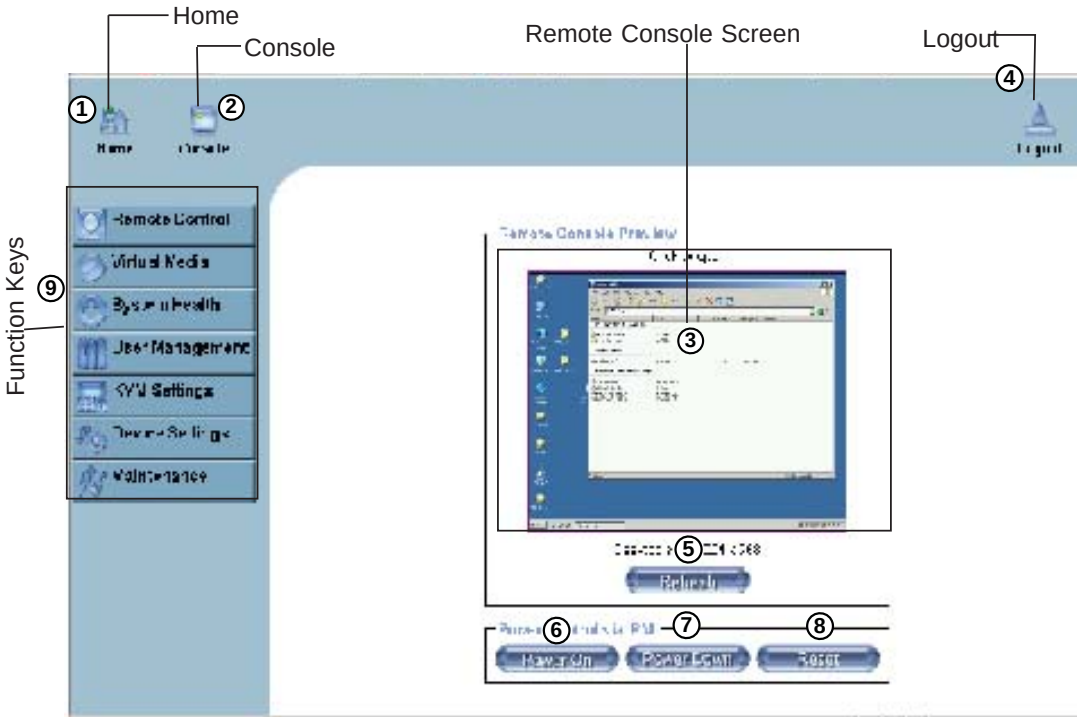
3. The Home Page will display as follows:

Note: KVM-over-LAN is available on the AOC-SIM1U+ only. All features and options related to the functionality of KVM-over-LAN are supported by the AOC-SIM1U+ only. In addition, KVM-over-LAN is not supported by the following motherboards:

1. X7DA8/X7DAE

2. X7DVL-3/X7DVL-i.

3.1 Home Page



3.1.1 Buttons from the Home Page

① **Home**: Click this icon to return to the Home Page.

② **Console**: Click this icon to go to the Remote Console Screen.

③ **Remote Console Screen**: Displayed in the window is Remote Console Screen. Click on this window to go to the Remote Console Screen.

④ **Logout**: Click on this icon to log out.

⑤ **Refresh**: Click on this icon to refresh the screen of the remote console preview.

⑥ **Power On**: Click on this icon to power on the system of the remote host.

⑦ **Power Down**: Click on this icon to power down the system of the remote host.

⑧ **Reset**: Click on this icon to reset the remote host.

3.1.2 Function Keys from the Home Page

⑨  Click on these function keys to use the functions as specified below.

1. Remote Control: Click on this icon for remote access and management of Video Console Redirection.

2. Virtual Media: Click on this icon to use virtual remote media devices.

3. System Health: Click on this icon to view and manage health monitoring for remote systems

4. User Management: Click on this icon for User Management.

5. KVM Settings: Click on this icon to configure keyboard, Video and mouse settings.

6. Device Settings: Click on this icon to configure device settings.

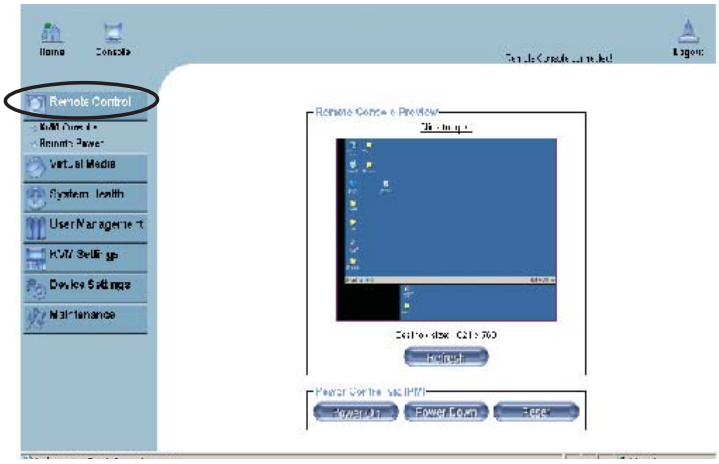
7. Maintenance: Click on this icon to access, diagnose and manage hardware devices

(**Note**: Please see the next page for details on the functions specified above.)

3.2 Functions Listed on the Home Page

3.2.1. Remote Control

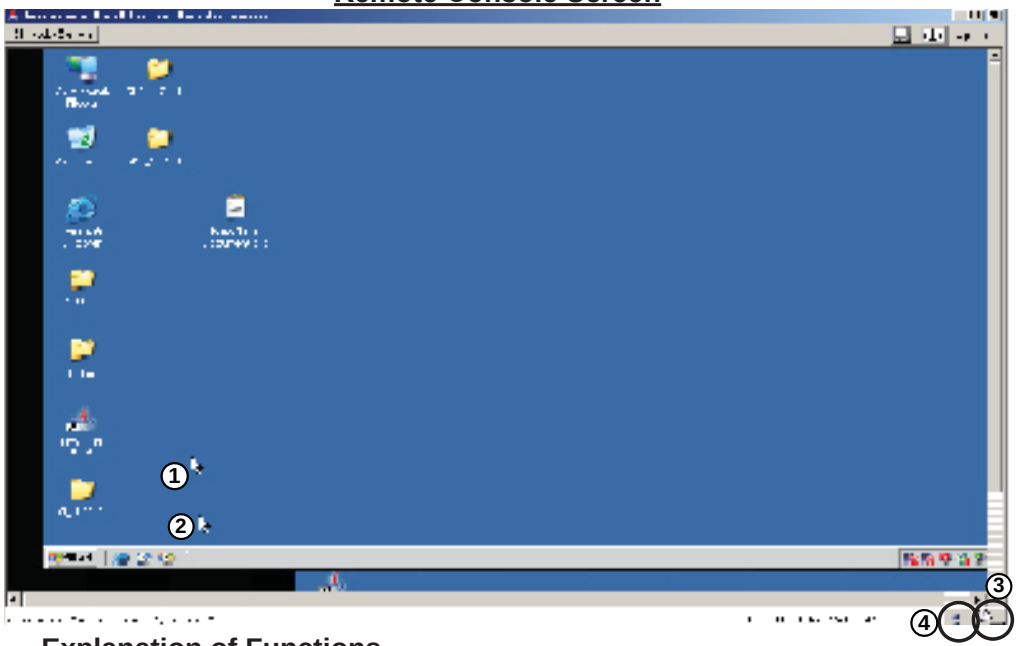
Click on the icon of Remote Control to activate its submenus-KVM Console and Remote Power as listed below.



a. KVM Console

Click on this item to configure keyboard, mouse or video settings for the remote host.

Remote Console Screen



Explanation of Functions

①  In the Single/Synchronized Mouse Mode, this cursor indicates the system that is currently active. For the Double Mouse mode, this is the cursor for the remote host.

②  This second mouse cursor only appears in the Double Mouse Mode. This cursor represents the local mouse.

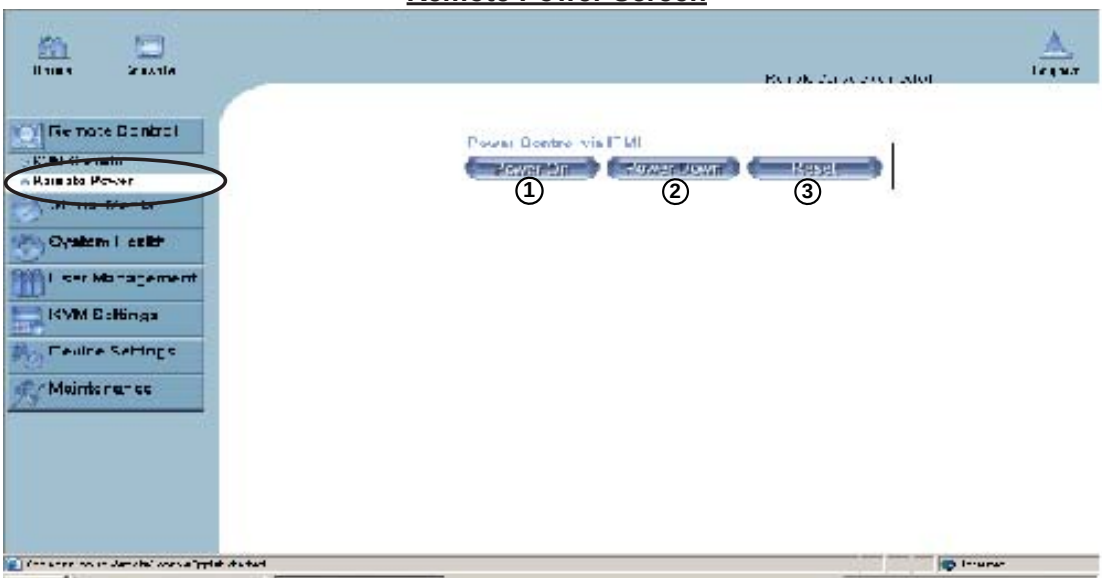
③  This icon indicates the availability of Keyboard and Mouse.

④  This icon indicates the number of networks (users) that are connected via Console Redirection. (The number of figure icons indicates the number of users connected.)

b. Remote Power

Click on this item to configure the power settings for Remote Console as shown below.

Remote Power Screen



Explanation of Functions

① 

Power On: Click on this icon to power on the remote host.

② 

Power Down: Click on this icon to power down the remote host.

③ 

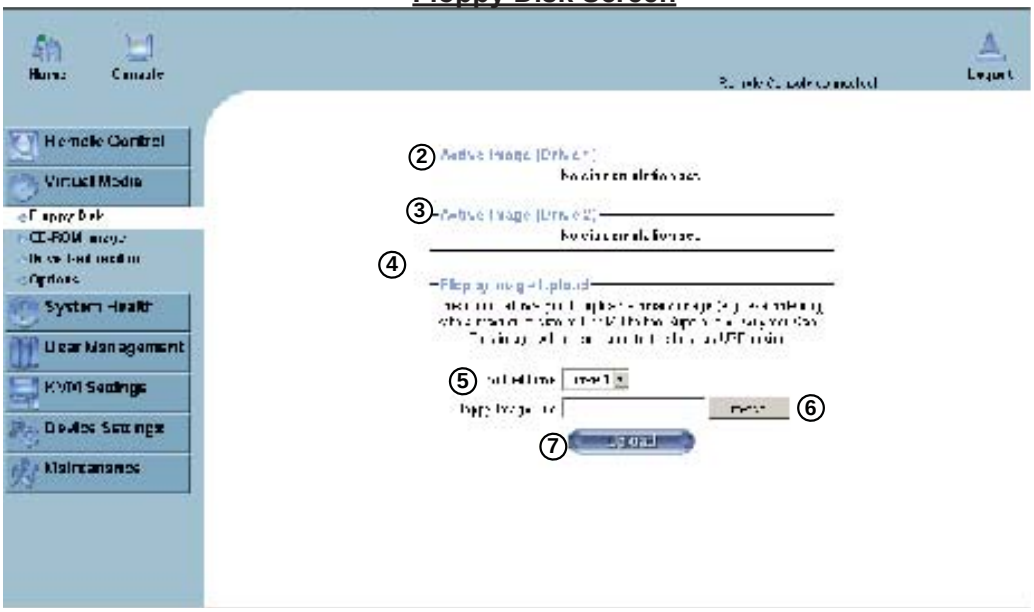
Reset: Click on this icon to reset the remote host.

3.2.2. Virtual Media

Click on the Virtual Media icon on the Home Page to activate its submenus-Floppy Disk, CD-ROM, Drive Redirection and Options as listed below.

a. Floppy disk

Floppy Disk Screen



Explanation of Functions

① 

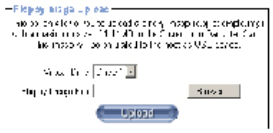
Floppy Disk: Click on this function key to upload the data stored in the local floppy disk image to the remote host.

② 

Active Image (Drive1): This window displays the data that has been uploaded to Drive 1 of the remote host.

③ 

Active Image (Drive2): This window displays the data that has been uploaded to Drive 2 of the remote host.

④ 

Floppy Image Upload: This option allows the user to upload the floppy image as "floppy" located in the remote host. The floppy image uploaded shall be in the binary format with a maximum size of 1.44MB. It will be loaded to the Supermicro SIMLP card and will be emulated to the host as a USB device.

⑤ 

Virtual Drive: Select a drive in the remote host as a destination drive for you to upload your image data.

⑥ 

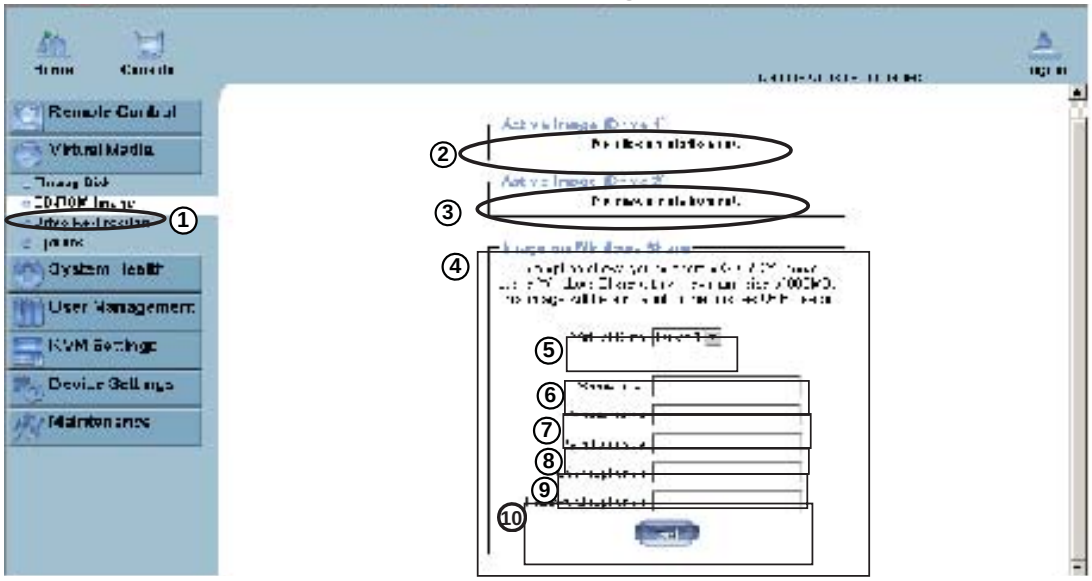
Floppy Image File: Click on "Browse" to preview and select the files that you wish to upload to the host drive selected.

⑦ 

Upload: Once the correct file name appears in the box, click Upload to upload the floppy image to the drive specified in the remote host.

b. CD-ROM Image

CD-ROM Image Screen



Explanation of Functions

① 

CD-ROM image: Click on this function key to share data stored in your local CD-ROM drive with other users in the remote host through the Windows Share application via USB.

② 

Active Image (Drive1): This window displays the file name of the data currently active in host Drive 1.

③ 

Active Image (Drive2): This window displays the file name of the data currently active in host Drive 2.

④ 

Image on Windows Share: This option allows the user to configure Windows Share settings. It allows you to decide how you want to share the CD-ROMISO Image file with users in the remote host.

⑤ 

Virtual Drive: Specify the drive that you want to share your data with in the remote host.

⑥ 

Share Host: Key in the IP Address or the name of the system you wish to share data with via Windows Share.

⑦ 

Share Name: Key in the name of the system you wish to share data with in the remote host.

⑧ 

Path to Image: Key in the location of source files that you wish to share via Windows Share.

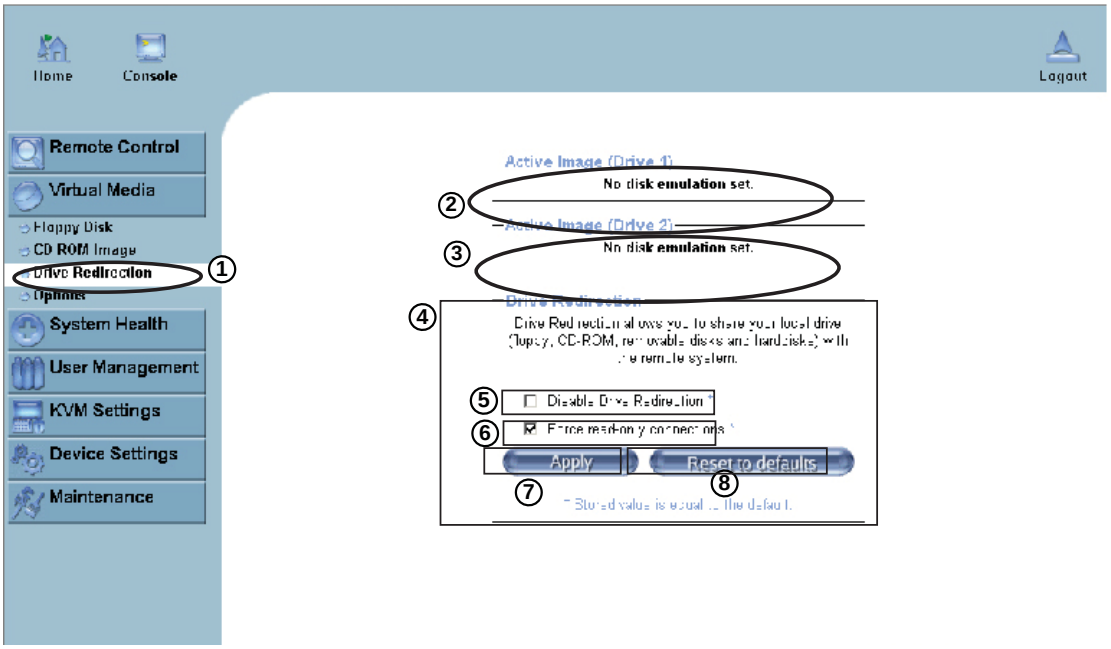
⑨ 

⑩

User/Password (Optional): Key in the Username and password for the person to access the data that you want to share and click "Set" to enter your selections.

c. Drive Redirection

Drive Redirection Screen



Explanation of Functions

① **Drive Redirection**: Click on this function key to make local drives accessible for other users via console redirection. This function allows you to share your local drives (Floppy, CD-ROM and HDDs) with users in the remote systems.

② **Active Image (Drive1)**: This window displays the file name of the data currently active in host Drive 1.

③ **Active Image (Drive2)**: This window displays the file name of the data currently active in host Drive 2.

④ **Drive Redirection**: Use this window to configure Drive Redirection settings.

⑤ **Disable Drive Redirection**: Check the box to disable Drive Redirection. Once this function is disabled, local drives will not be accessible for other users in remote host.

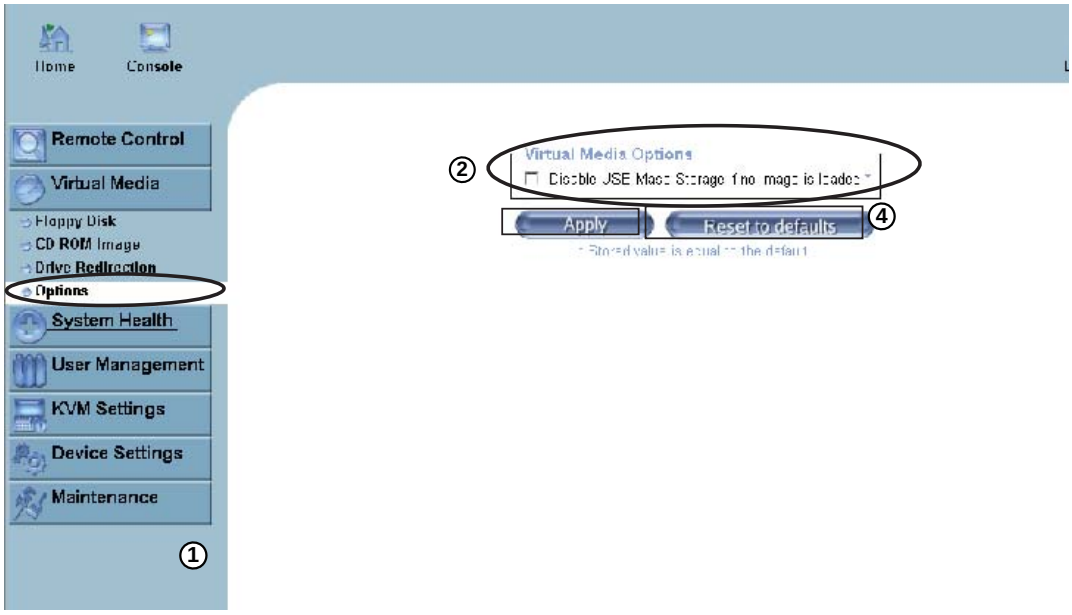
⑥ **Force Read Only**: Check this box to allow the data stored in local drives to be read in a remote system, but it cannot be overwritten to ensure data integrity and system security.

⑦ **Apply**: Once you've configured your settings, click "Apply" to enter your settings.

⑧ **Reset Default**: You can also key in your own setting values and re-set these values as "default" by clicking on this icon to reset the defaults.

d. Virtual Media Options

Virtual Media Options Screen



Explanation of Functions

① 

Options: Click on this function key to activate the Virtual Media sub-menu.

② 

Virtual Media Options: Use this option to disable or enable USB MASS storage in the remote host. Check this box to disable the function of Virtual Media Options to prevent data stored in a local drive from being accessed, or uploaded by the user in the remote host. The default setting is "enabled."

③ 

Apply: Once you've checked the box, click "Apply" to enter this value.

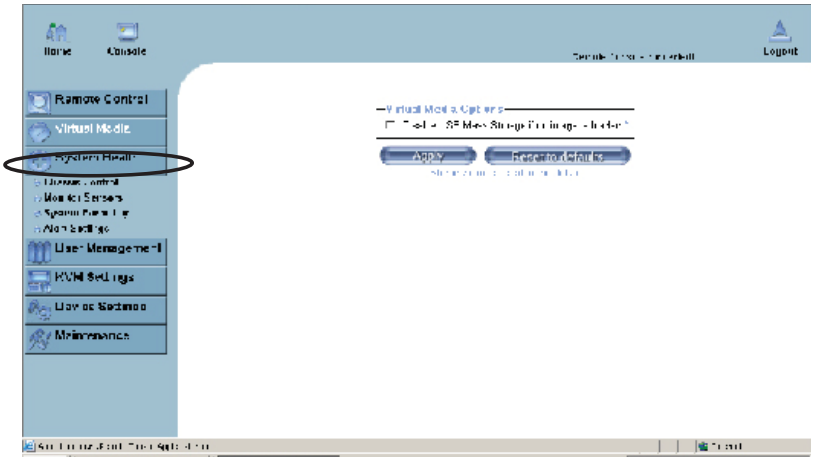
④ 

Reset to Defaults: If you want to set "Disabled" as the default setting for the item-Virtual Media Options, click on this icon.

3.2.3. System Health

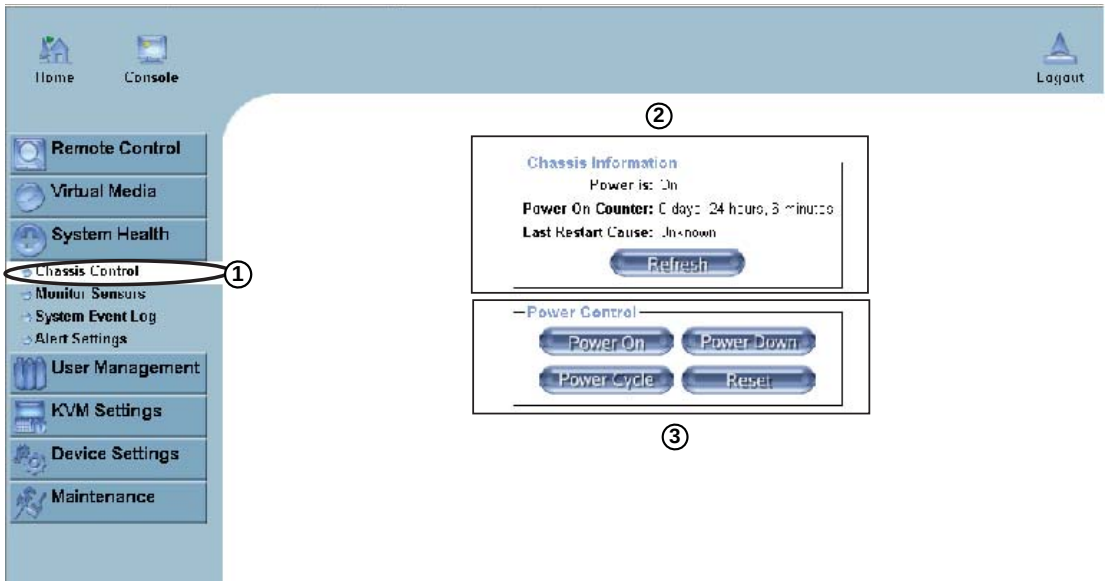
Click on the System Health icon on the Home Page to activate its submenus: Chassis Control, Monitor Sensor, System Event Log and Alert settings as listed below.

System Health Screen



a. Chassis Control

Chassis Control Screen



① **Chassis Control**

Chassis Control: Click on this function key to access Health Monitoring information on the remote chassis. The items monitored include 1. Chassis Information 2. Power Control.

② **Chassis Information:**

The following remote chassis information is included:

Power Is: This indicates if the system is on or off for the remote host.

Power On Counter: If power is on, then the counter indicates the length of time the power has been turned on.

Last Restart Cause: This item states the reason why the host system is restarted if the system has been turned off.

Refresh: Click the Refresh button to update "Chassis Information" as shown in Window 2.

③ Power Control

The following Power Control items are included:

Refresh: Click on this icon to refresh the screen of the remote host.

Power On: Click on this icon to power on the system for the remote host.

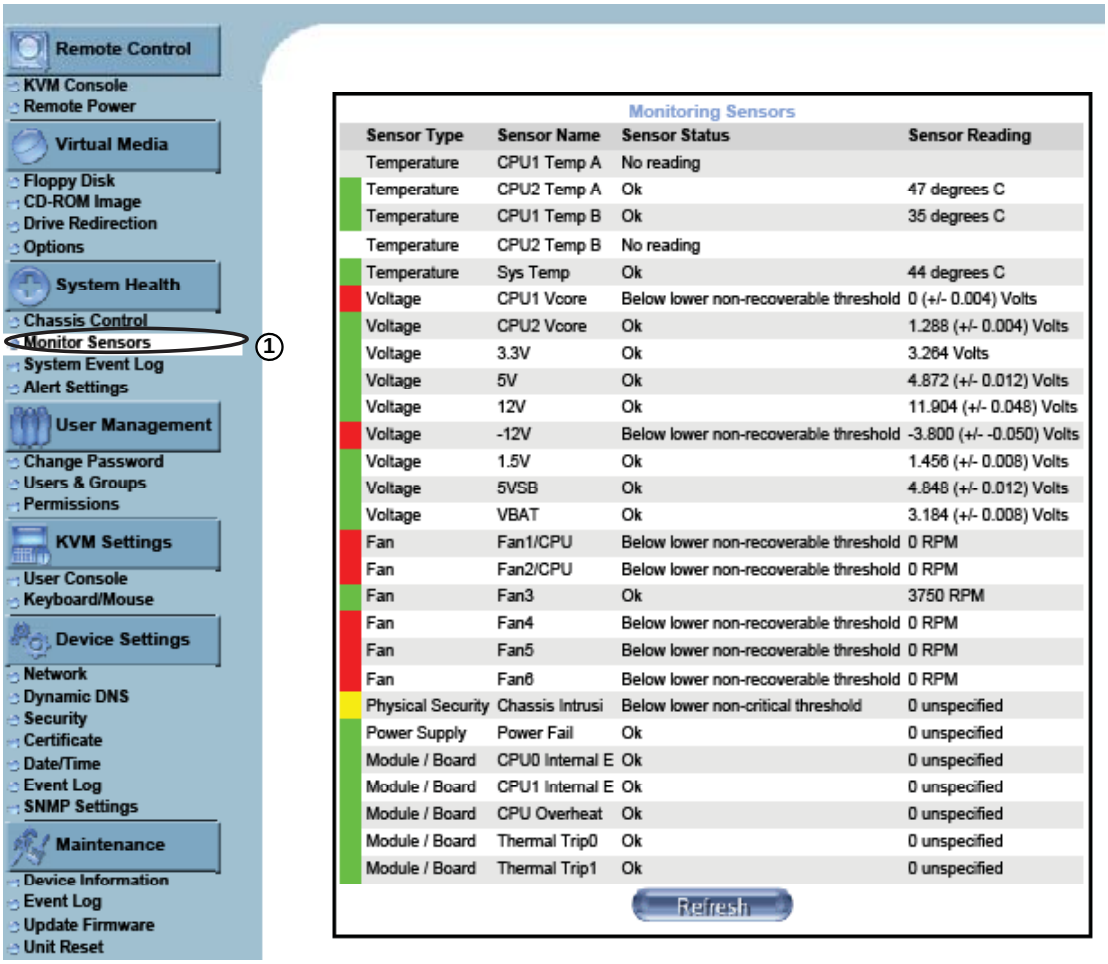
Power Down: Click on this icon to power down the system for the remote host.

Power Cycle: Click on this icon to power down the system for the remote host and turn it back on later.

Reset: Click on this icon to reset the remote console.

b. Monitor Sensors

Monitor Sensors Screen



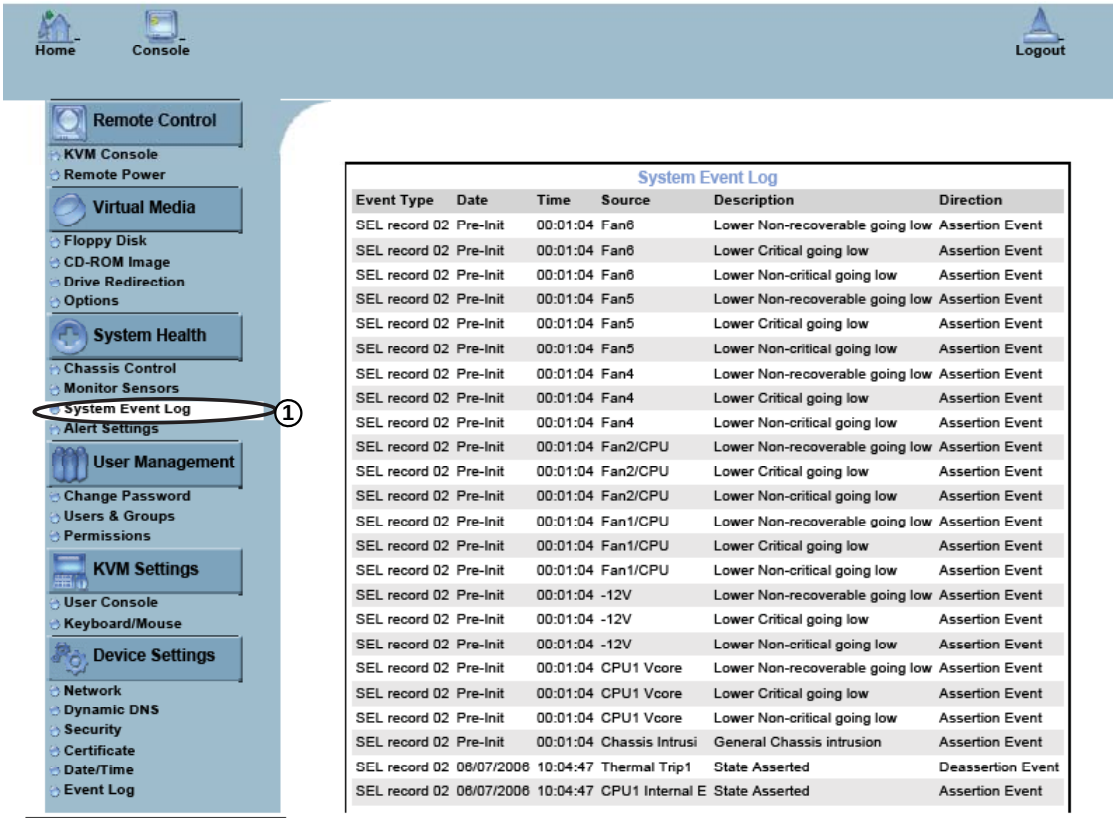
Sensor Type	Sensor Name	Sensor Status	Sensor Reading
Temperature	CPU1 Temp A	No reading	
Temperature	CPU2 Temp A	Ok	47 degrees C
Temperature	CPU1 Temp B	Ok	35 degrees C
Temperature	CPU2 Temp B	No reading	
Temperature	Sys Temp	Ok	44 degrees C
Voltage	CPU1 Vcore	Below lower non-recoverable threshold	0 (+/- 0.004) Volts
Voltage	CPU2 Vcore	Ok	1.288 (+/- 0.004) Volts
Voltage	3.3V	Ok	3.264 Volts
Voltage	5V	Ok	4.872 (+/- 0.012) Volts
Voltage	12V	Ok	11.904 (+/- 0.048) Volts
Voltage	-12V	Below lower non-recoverable threshold	-3.800 (+/- -0.050) Volts
Voltage	1.5V	Ok	1.456 (+/- 0.008) Volts
Voltage	5VSB	Ok	4.848 (+/- 0.012) Volts
Voltage	VBAT	Ok	3.184 (+/- 0.008) Volts
Fan	Fan1/CPU	Below lower non-recoverable threshold	0 RPM
Fan	Fan2/CPU	Below lower non-recoverable threshold	0 RPM
Fan	Fan3	Ok	3750 RPM
Fan	Fan4	Below lower non-recoverable threshold	0 RPM
Fan	Fan5	Below lower non-recoverable threshold	0 RPM
Fan	Fan6	Below lower non-recoverable threshold	0 RPM
Physical Security	Chassis Intrusi	Below lower non-critical threshold	0 unspecified
Power Supply	Power Fail	Ok	0 unspecified
Module / Board	CPU0 Internal E	Ok	0 unspecified
Module / Board	CPU1 Internal E	Ok	0 unspecified
Module / Board	CPU Overheat	Ok	0 unspecified
Module / Board	Thermal Trip0	Ok	0 unspecified
Module / Board	Thermal Trip1	Ok	0 unspecified

① **Monitoring Sensor**: Click on this function key to display the following Health Monitoring Information shown in the following table:

Health Monitoring Sensor Information on the Remote Host		
Temperature Monitoring	CPU1 Temperature (Temp A, Temp B)	Temp A: CPU1 Core1 Temperature, Temp B: CPU1 Core2 Temperature,
	CPU2 Temperature (Temp A, Temp B)	Temp A: CPU2 Core1 Temperature, Temp B: CPU2 Core2 Temperature,
	System Temperature	
Voltage Monitoring	CPU1 VCore	CPU1 Vcore: CPU1 Core Voltage
	CPU2 VCore	CPU2 Vcore: CPU2 Core Voltage
	3.3V	
	5V, 5VSB	5VSB: 5V Standby
	+12V, -12V	
	1.5V	
	VBAT	VBAT: Battery Voltage
Fan Control	Fan1/CPU Fan	
	Fan2/CPU Fan	
	Fan 3 – Fan 6	System Fans/Chassis Fans
Physical Security	Chassis Intrusion	
Module/Board CPU0 Internal E.		
Module/Board CPU1 Internal E.		
Module/Board CPU Overheat		When the CPU temperature exceeds this preset temperature, the overheat LED or alert will be triggered, the CPUs will slow down, the CPU fans will be in the full speed mode.
Module/Board Thermal Trip		When the system temperature exceeds this preset temperature, the overheat LED or alert will be triggered, and the cooling fans will be in the full speed mode to prevent system overheat.

c. System Event Log

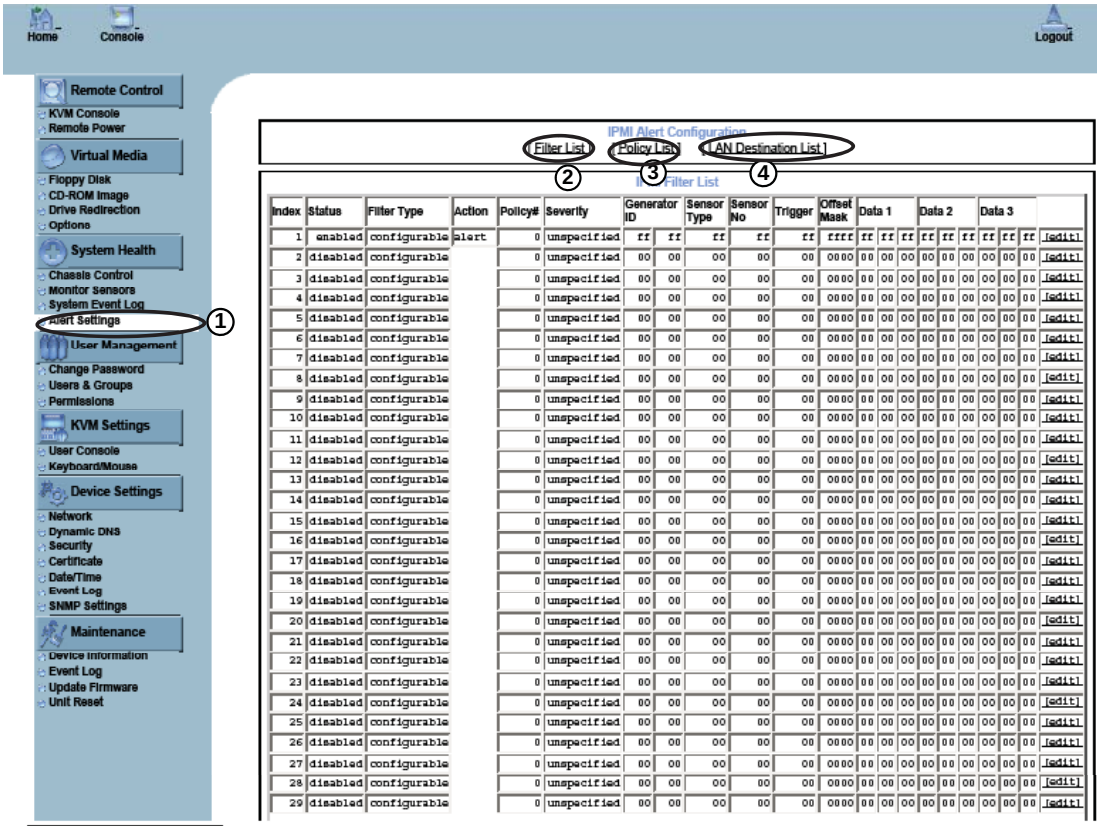
System Event Log Screen



① **System Event Log**: Click on this function key to display the System Health Event Log for the remote host system.

d. Alert Settings

Alert Settings Screen



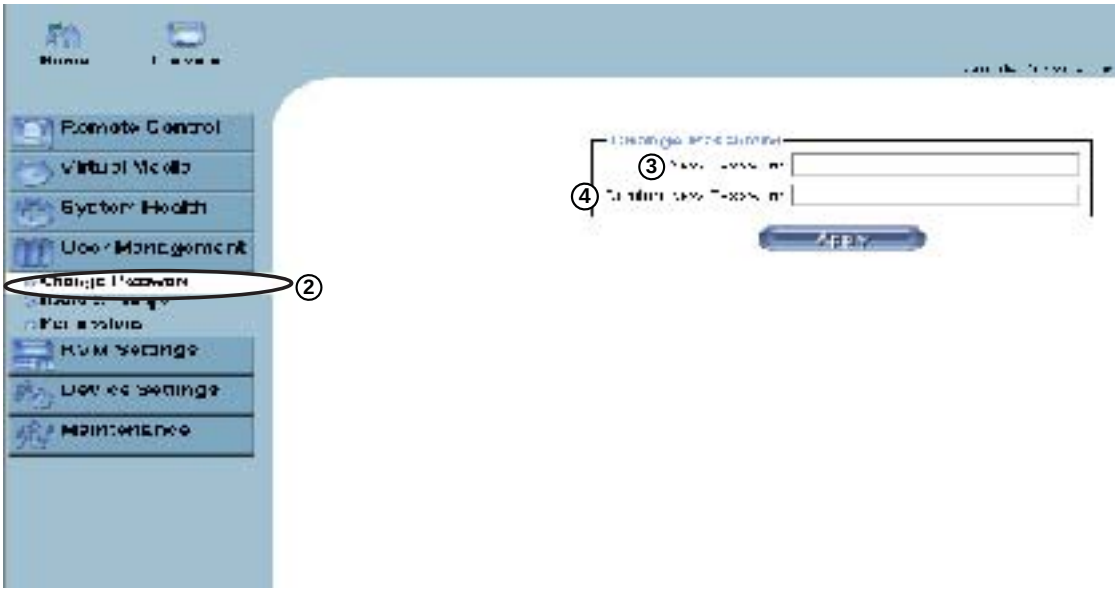
① **Alert Settings**: Click on this function key to activate the alert settings submenu for the remote host system. The items monitored include: 1. Filter List, 2. Policy List and 3. LAN Destination List

3.2.4. User Management

Click on the User Management icon on the Home Page to activate its submenus: Change Password, Users & Group and Permissions as listed below.

User Management Screen

a. Change Password



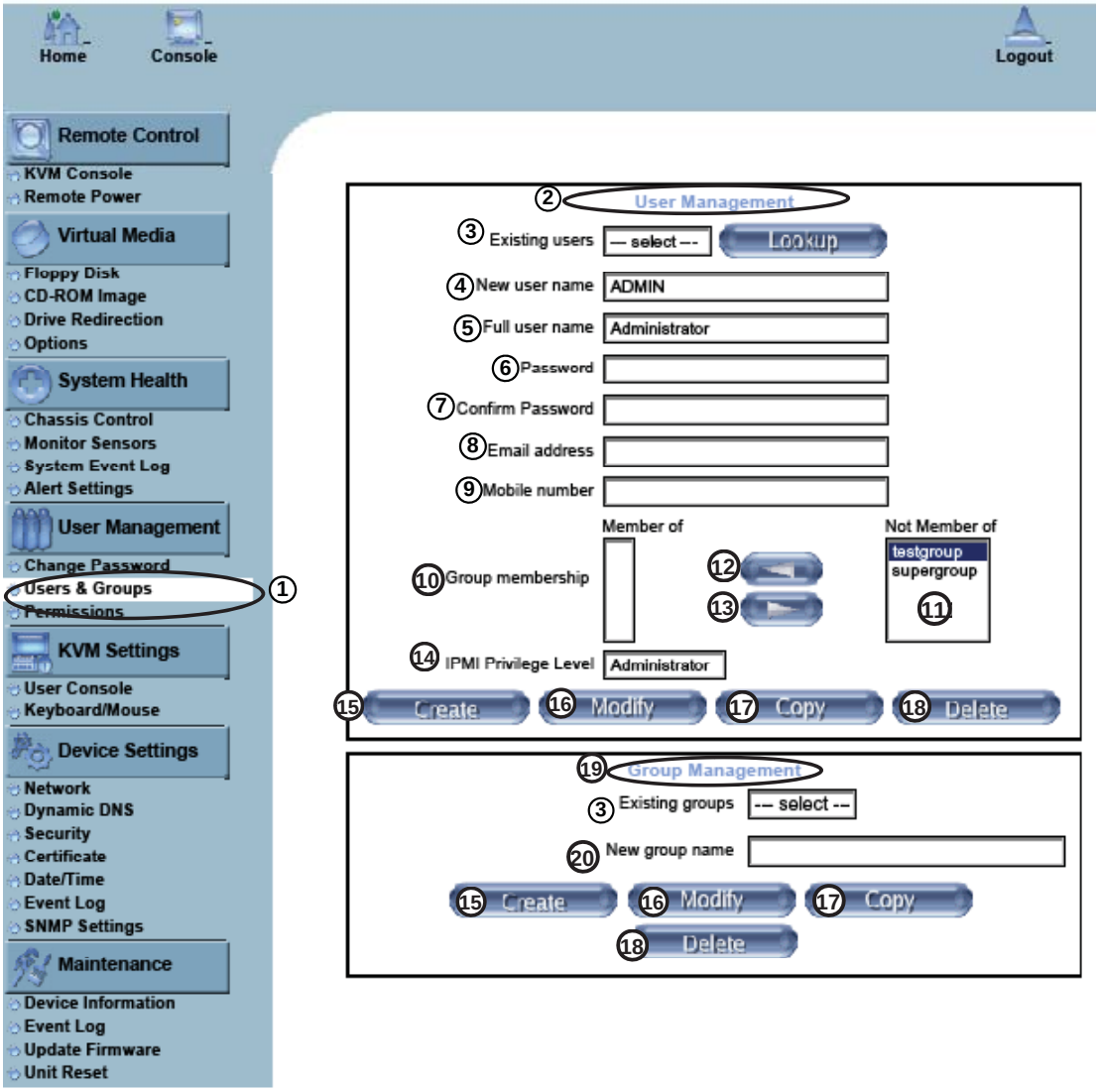
① **User Management:** Click on this icon to activate the User Management submenu. Once this submenu displays, you can access the New Password fields.

② **Change Password:** Click on this function key to access the New Password and Confirm New Password fields.

③ **New Password:** Key in your new password in the blank.

④ **Confirm New Password:** Key in your new password in the blank again and click "Apply" to confirm it.

b. Users & Groups-User Management and Group Management



① **Users & Groups:** Click on this icon to activate the Users & Groups submenu.

② **User Management:** This window displays the user's information.

③ **Existing users:** Select an existing user for information updates. Once a user is selected, click on the "Lookup" icon on right to view user information.

④ **New user name:** Key in new user name in this field.

⑤ **Full user name:** Key in full user name in this field.

⑥ ⑦ **Password and Confirm Password:** Type the user's password in the field and then type the password again in the next field to confirm it. The password must be 4 characters or longer.

⑧ **Email Address:** Key in the user's email address in the field. (Optional)

⑨ **Mobile Phone:** Key in the user's mobile phone number in the field. (Optional)

⑩ **Group Membership:** This field indicates the group that the user belongs to. To select a group, click on the group name on the "Not Member Of" window to select it as shown in Window ⑪, then click on the backwards arrow shown on ⑫ to enter the group name in the Group Membership field as shown in ⑩. Reverse the procedure to remove the user from a group.

⑭ **IPMI Privilege Level:** Click on the arrow key on the right to activate the Privilege Selection menu. The IPMI Privilege Level contains five categories: No Access, User, Operator, Administrator and OEM.

⑮ **Create:** Click on this button to enter a new user's or group information in the User/ Group Management fields.

⑯ **Modify:** Click on this button to modify a user's or group information in the User/ Group Management fields.

⑰ **Copy:** Click on this button to copy a user's or group information in the User/Group Management fields.

Copy User

Choose an Existing User from the selection box. Enter a new user name in the field "New User Name." Click on the "Copy" button and a new user with the name you've typed in will be created. The properties of the selected user will be copied to the new user.

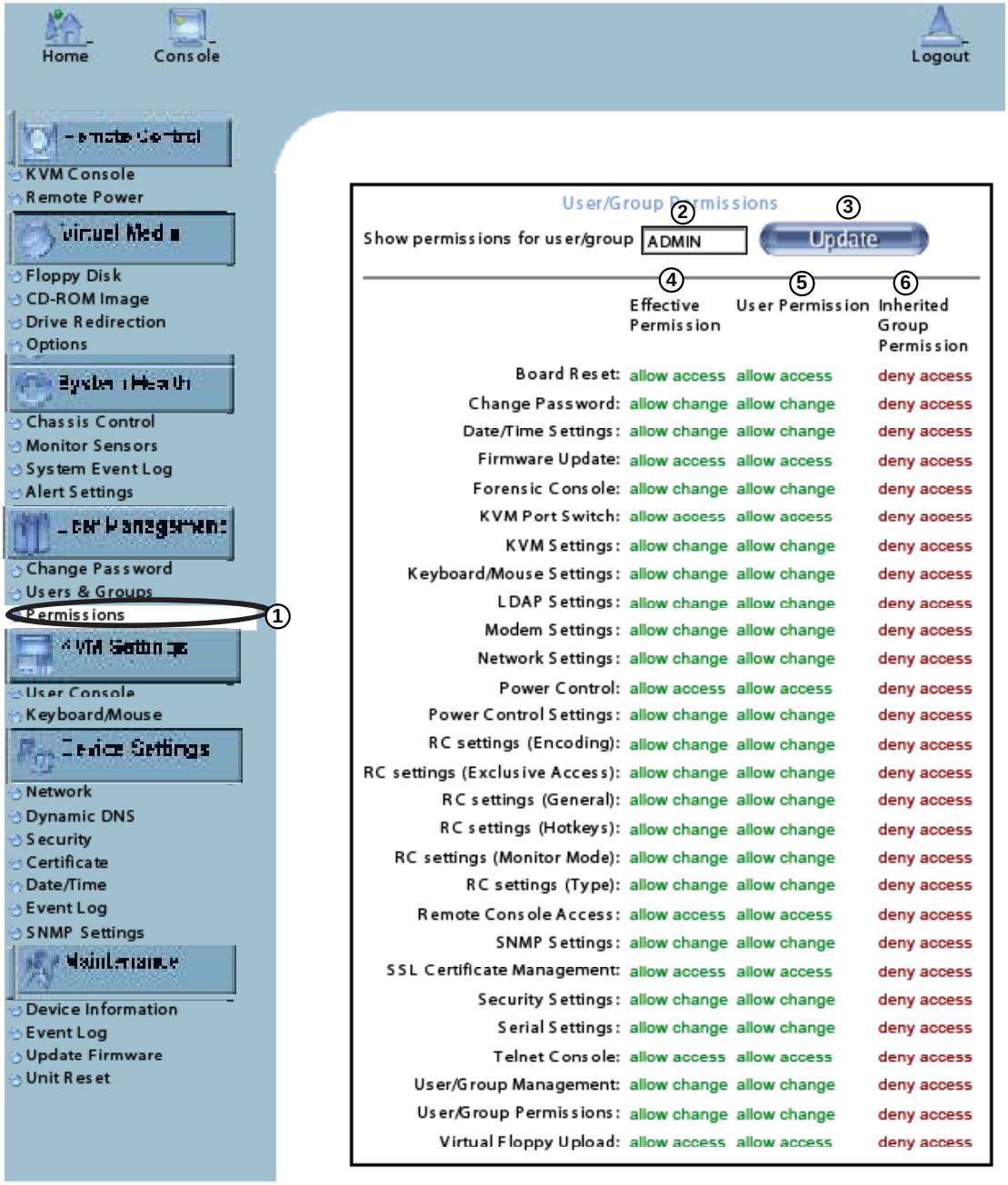
Copy Group

Choose an Existing group from the selection box. Enter a new group name in the field "New Group Name." Click on the "Copy" button and a new group with the name you've typed in will be created. The properties of the selected group will be copied to the new group.

⑱ **Delete:** Click on this button to delete a user's or group information in the User/Group Management fields.

⑲ **Group Management:** This window allows you to enter group information for better user management.

c. Permissions



① **Permissions:** Click on this icon to activate the User/Group Permissions submenu.

② **Show Permissions for User/Group:** click on the arrow on the right to activate the user/group permissions selection menu.

③ **Update:** Click this icon to update permissions information.

④ **Effective Permissions:** This field indicates the actual permissions a user/group has.

⑤ **User Permissions:** This field indicates the actual permissions a user has.

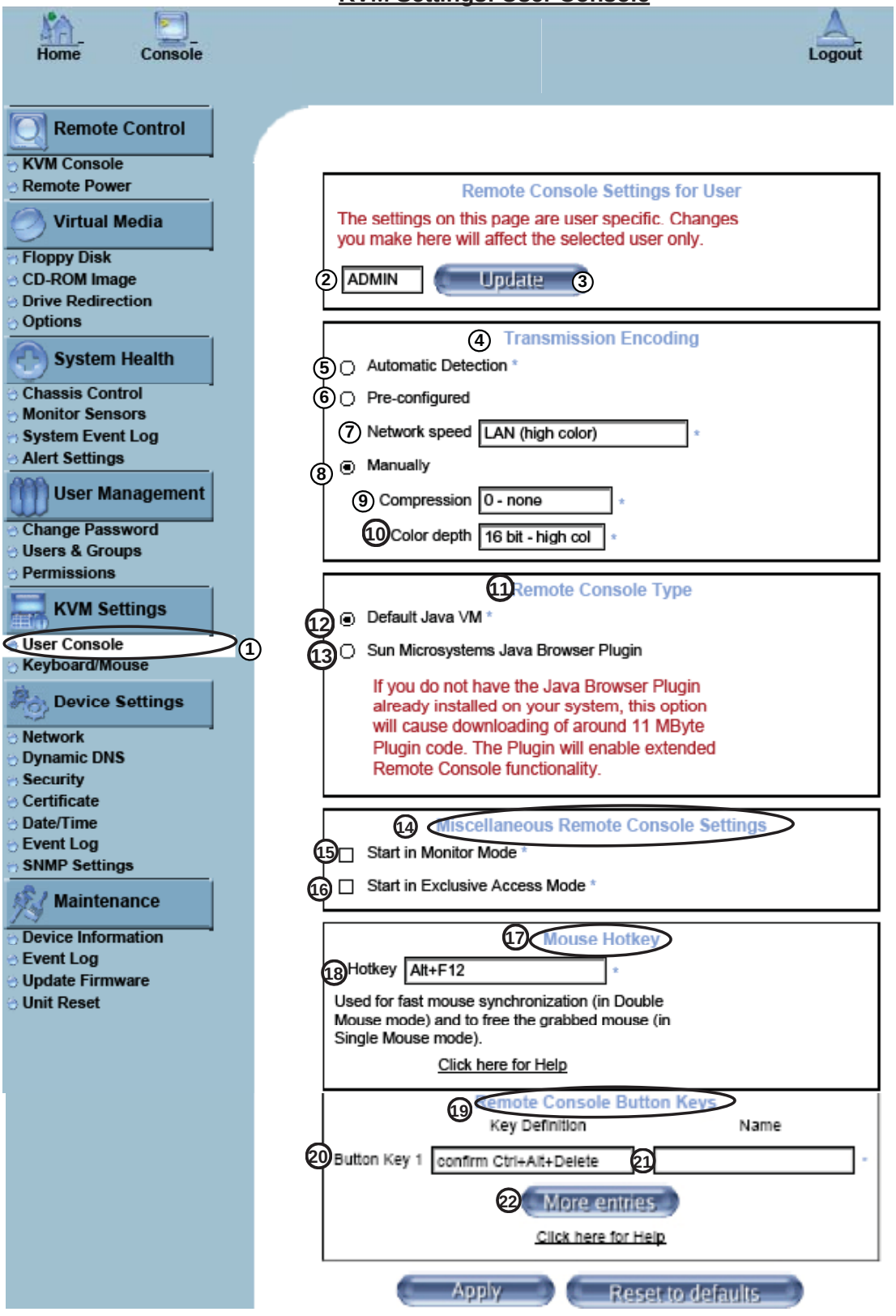
⑥ **Inherited Group Permission:** This field indicates the permissions a user has due to the fact that he or she belongs to a certain group.

3.2.5. KVM Settings

Click on the KVM Settings icon on the Home Page to activate its submenus: User Console and Keyboard/Mouse as listed below.

a. User Console

KVM Settings: User Console



a. User Console

1. User Console: Click on this icon to activate the User Console submenu.

2. User Selection: This field allows you to decide which group the user belongs to. Click on the arrow on the right to activate the selection menu and highlight the name of the group to select it.

3. Update: Once you've selected the group name, click on Update to save the selections.

4. Transmission Encoding: This field allows the user to decide how (the video) data is transmitted between the local system and the remote host.

5. Automatic Detection: Select this option to allow the OS to automatically detect the networking configuration settings such as the bandwidth of the connection line, and transmit data accordingly. (You can only select one item from #5, #6 and #8.)

6. Pre-configured: This item allows the user to select the data transmission setting from a pre-defined options list. The pre-configured settings will provide the best result because the compression and color depth settings will be adjusted for optimization based on the network speed indicated. (You can only select one item from #5, #6 and #8.)

7. Network speed: Once you've selected the pre-configured option above, you then can select a desired network speed setting from the selection menu by clicking on the arrow on the right.

8. Manually: You can select a desired network speed setting from the selection menu by clicking on the arrow on the right. This item allows the user to adjust both compression and color depth settings individually. (You can only select one item from #5, #6 and #8.)

9. Compression: Data signal transmission is compressed to save bandwidth. High compression rates will slow down network interfacing and shall not be used when several users are connected to the network.

10. Color Depth: Click on the arrow on the right to select either 16 bit-high colors or 8 bit-256 colors. The standard color depth is 16 bit-high color. This setting is recommended for compression level 0. For typical desktop interfaces, the setting of 8 bit-256 colors is recommended for faster data transmission.

11. Remote Console Type: This field allows the user to decide which Remote Console Viewer to use.

12. Default Java VM (JVM): Select this option to use the default Java Virtual Machine of your web browser. This can be the Microsoft JVM for Internet Explorer or the Sun JVM depending on the configuration of your browser.

13. Sun Microsystems Java Browser Plugin: Select this option when the JVM used to run the code for the Remote Console is a Java Applet. If you use this function for the first time and the appropriate Java plugin is not yet installed in your system, you may download and install it automatically. To download and install it, you need to check "yes" in the dialogs. Downloading Sun's JVM will allow you to use a stable and identical JVM across different platforms. (Note: If your internet connection is slow, please pre-install the JVM on your administration machine.)

14. Miscellaneous Remote Console Settings: This window allows you to specify the following Remote Console Settings.

15. Start in Monitor Mode: Check this box to enable the Start in Monitor Mode which will allow data to be displayed in the remote monitor as soon as Remote Console is activated. (The data displayed in the remote monitor is ready-only.)

16. Start in Exclusive Access Mode: Check this box to enable the exclusive access mode immediately at Remote Console startup, which will force all other users connected to the network to close. No other users can open the Remote Console until you disable this function or log off.

17. Mouse Hotkey: This option allows you to use a hotkey combination to specify the mouse synchronization mode or the single mouse mode.

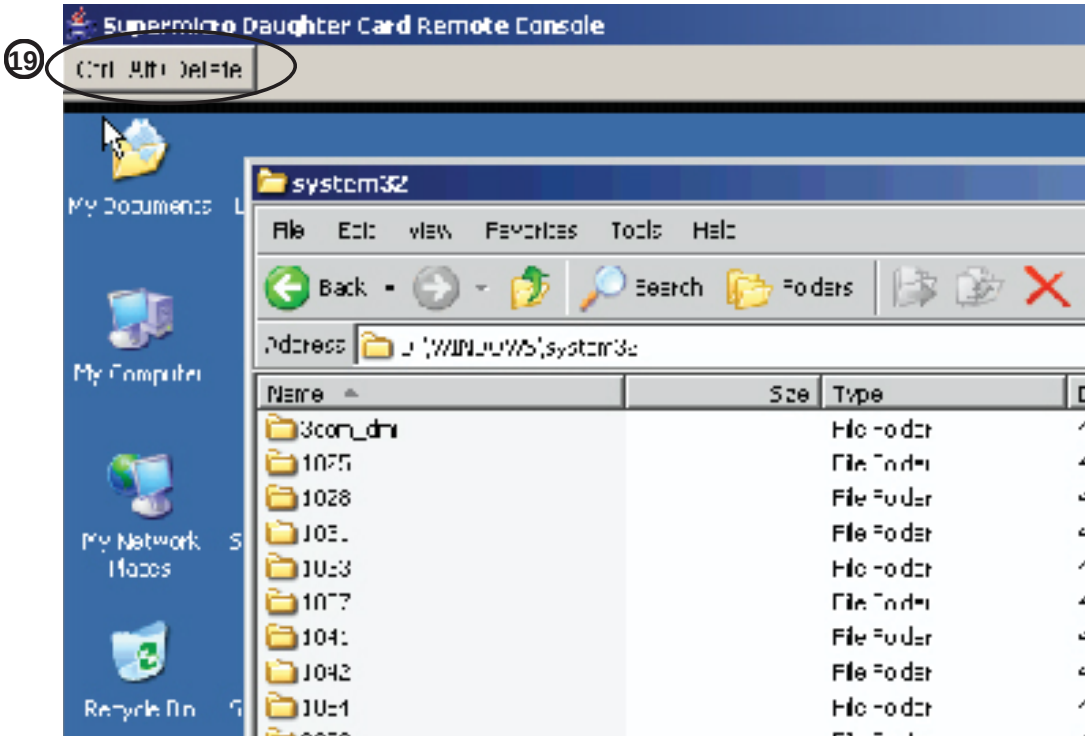
18. Hotkey: Enter a hotkey combination in the box to specify the mouse synchronization mode or the single mouse mode.

19. Remote Console Button Keys: This window allows the user to define button keys for the remote host. The button keys allow simulating keystrokes on a remote host or issuing commands to a remote system. The button keys are needed when you have a missing key or when you want to prevent interference caused to the local system. After a remote console button key is set, it will appear on the right upper corner of the remote monitor screen as shown in the graphics below. (For details instructions in creating button keys, please click on the link-"Click here for Help.")

20 Button Keys: Enter the syntax of a button key in the box. (For detailed instructions in creating button keys, please click on the link-"Click here for Help.")

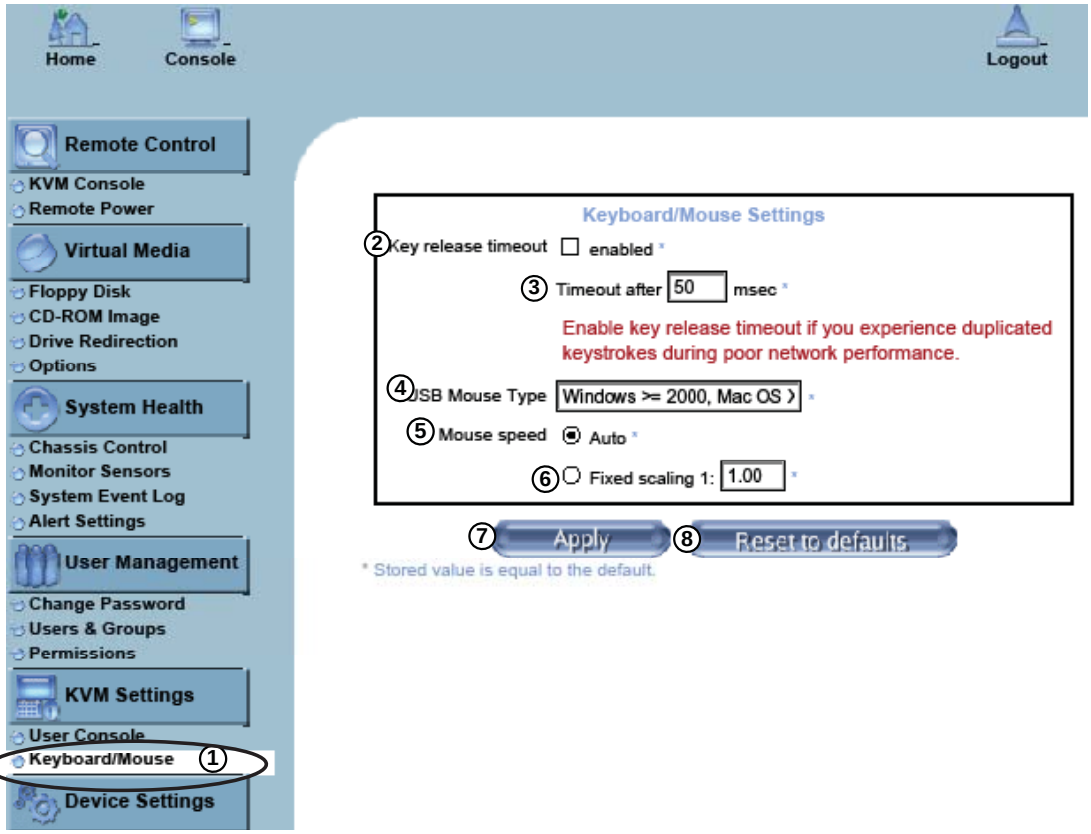
21 Name: Key in the name of a button key in the box. (For details instructions in creating button keys, please click on the link-"Click here for Help.")

22 More Entries: Click on this icon to create more Button Keys.



b. Keyboard/Mouse

KVM Settings: Keyboard/Mouse



1. Keyboard/Mouse: Click on this function key to configure the following Keyboard/ Mouse Settings.

2. Key Release Timeout: Check this box to enable the function of "Key Release Timeout," which will set the time limit for a key to be pressed by the user.

3. Timeout after_____msec: If the "Key Release Timeout" indicated above has been enabled, click on the arrow on the right to activate a selection menu to select the timeout setting for the item above.

4. USB Mouse Type: For the USB Mouse to function properly, please select the correct OS for your system from the selection menu by clicking on the arrow on the right.

5. Mouse Speed-Auto: Check the selection to allow your system to automatically set your mouse speed.

6. Fixed Scaling: You can also check the "Fixed Scaling" box and manually key in your selection.

7. Apply: Click on this icon to enter your selections.

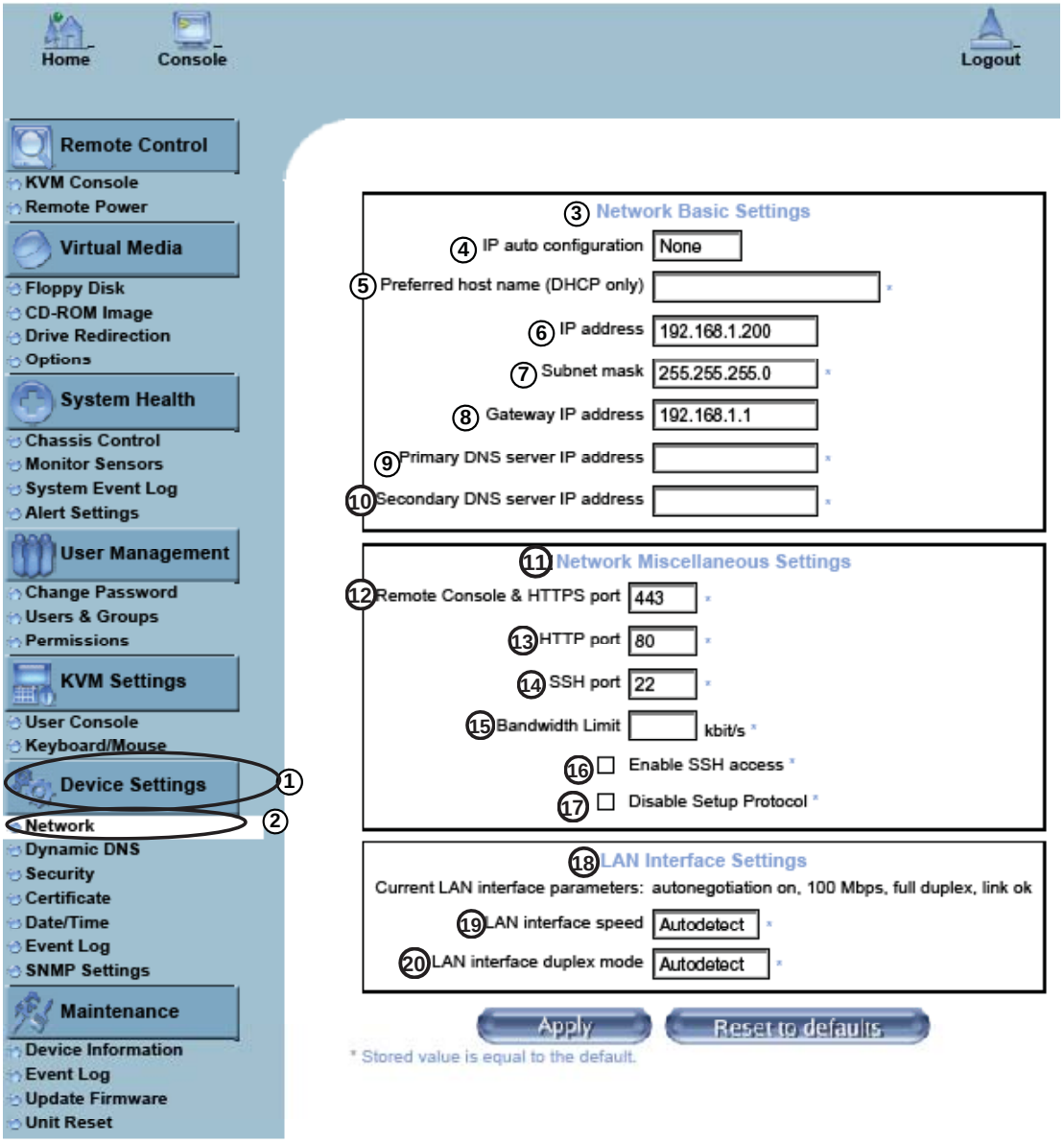
8. Reset to defaults: You can also cancel your selections and use the default values pre-set by the manufacturer by clicking on this icon.

3.2.6. Device Settings

Click on the Device Settings icon on the Home Page to activate its submenus: Network, Dynamic DNS, Security, Certificate, Date/Time, Event Log and SNMP Settings as listed below.

a. Network

Device Settings: Network



a. Network

1. Device Settings: Click on the Device Settings icon to activate its submenus: Network, Dynamic DNS, Security, Certificate, Date/Time, Event Log and SNMP Settings.

2. Network: Click on this function key to activate the Network submenu to configure the following settings: Network Basic Settings, Network Miscellaneous Settings and LAN Interface Settings.

3. Network Basic Settings: This window allows you to configure basic settings for your network.

4. IP Auto Configuration: Click on the box to activate the selection menu and select a desired item from the list. The options are None, DHCP, and BOODP.

5. Preferred Host Name (DHCP only): Enter a Preferred Host Name in the box.

6. IP Address: Enter the IP Address for the remote host in the box.

7. Subnet Mask: Enter the net mask of the local network in the box.

8. Gateway IP Address: Enter the local network router's IP address in this box for the accessibility of the users that are not connected to the local network.

9. Primary DNS Server IP Address: Enter the IP Address of the Primary Domain Name Server in the box.

10. Secondary DNS Server IP Address: Enter the IP Address of the Secondary Domain Name Server in the box. It will be used when the Primary DNS Server cannot be contacted.

11. Network Miscellaneous Setting: This field allows the user to configure the following Network Miscellaneous settings as listed below:

12. Remote Console & HTTPS Port: Enter the port numbers the remote host and the HTTP server are listening. If a number is not entered in the box, the default value will be used.

13. HTTP Port: Enter the port number the HTTP server is listening. If a number is not entered in the box, the default value will be used.

14. SSH Port: Enter the port number the SSH server is listening. If a number is not entered in the box, the default value will be used.

15. Bandwidth Limit: Enter the maximum bandwidth value for network interfacing. The value should be in Kbits per second.

16. Enable SSH Access: Click this box to enable SSH Access.

17. Disable Setup Protocol: Check this box to disable the function of Setup Protocol for the SIMLP card.

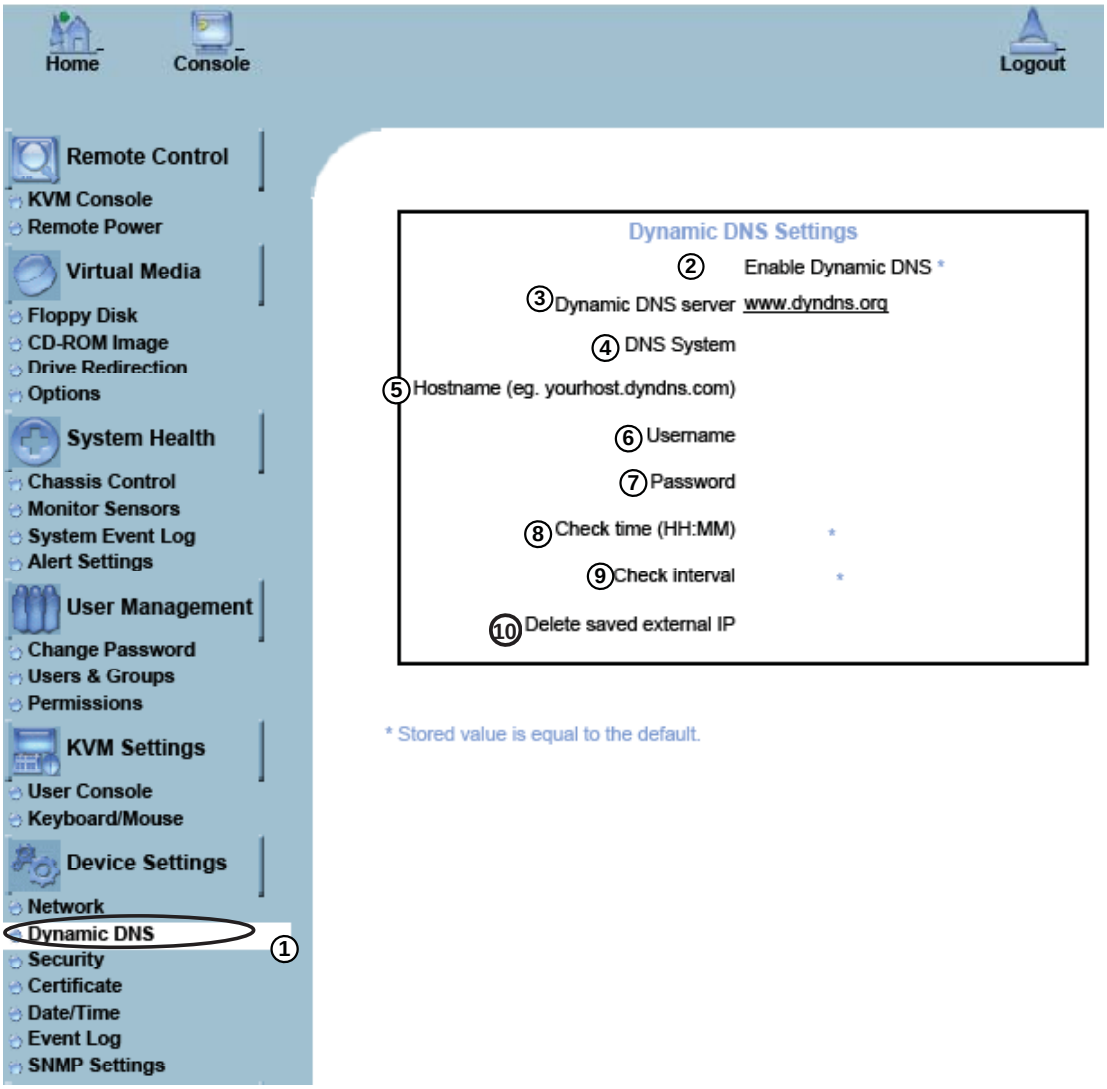
18. LAN Interface Setting: This field allows the user to configure the following LAN Interface settings as listed below:

19. LAN Interface Speed: Click on the arrow on the right to activate the selection menu and select a desired speed. The options are: Auto-detect, 10 Mega bits per second or 100 Mega bits per second. If Auto-detect is selected, LAN Interface Speed will be set at the optimized speed based on the system configurations detected by the OS.

19. LAN Interface Duplex Mode: Click on the arrow on the right to activate the selection menu to select a desired LAN Interface Duplex Mode. The options are: Auto-detect, Half Duplex and Full Duplex. If Auto-detect is selected, the LAN Interface Duplex Mode will be set to the optimized setting based on the system configurations detected by the OS.

b. Dynamic DNS

Device Settings: Dynamic DNS



b. Dynamic DNS

1. Dynamic DNS: Click on this function key to activate its submenu and configure the following Dynamic DNS (-Domain Name Server) settings as listed below.

2. Enable Dynamic DNS: Check this box to enable the Dynamic DNS service.

3. Dynamic DNS Server www.dyndns.org: Click this link to access the DynDNS web site. This is the server name where the DDNS Service is registered.

4. DNS System: Dynamic DNS (Item#2 above) is enabled, you can select from the options: Custom or Dynamic from the selection menu. Select "Custom" to use your own system as the DNS server. Select Dynamic to use the pre-configured Dynamic DNS as your server.

5. Hostname: Enter the name you want to use for the remote host server.

6/7. Username/Password: Enter the username and the password for the remote host user.

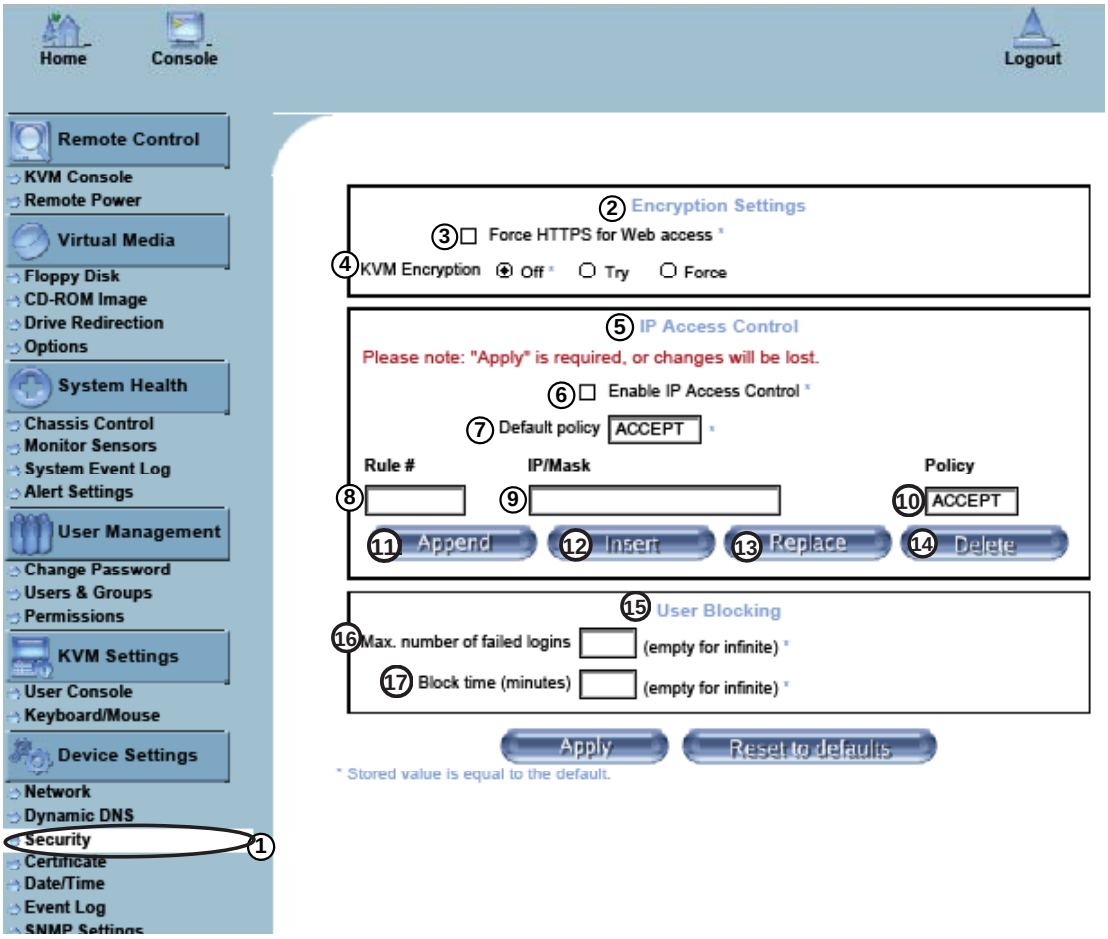
8. Check time (HH:MM): Enter the time the SIMLP card first registers with the DNS server in the HH:MM Format. (e.g. 07:25, 19:30)

9. Check Interval: Enter the interval for the IPMI to report to the Dynamic DNS again.

10. Delete Saved External IP Address: Click on the Delete Icon to delete the IP Address for an external system that has been previous entered and saved.

c. Security

Device Settings: Security



c. Security

1. Security: Click on this function key to activate its submenu and configure the following Security settings as listed below.

2. Encryption Settings: This window allows you to configure encryption settings.

3. Force HTTPS for Web Access: Check this box to enable the function-Force HTTPS for Web Access. If enabled, you will need to use an HTTPS connection to access to the web.

4. KVM Encryption: This option allows you to configure the encryption of the RFB protocol. RFB is used by the remote host to transmit video data displayed in the host monitor to the local administrator machine, and transmit keyboard and mouse data from the local administrator machine back to the remote host.

If set to "Off," no encryption will be used. If set to "Try," the applet (-JVM of the remote host) will attempt to make an encrypted connection. In this case, when a connection cannot be established, an unencrypted connection will be used. If set to "Force," the applet will make an encrypted connection. In this case, an error will be reported if no connection is made.

5. IP Access Control: This section allows you to configure the IP Access Control settings listed below.

6. Enable IP Access Control: Check this box to enable the function of IP Access Control. This function is used to limit user access to the network by identifying them by their IP addresses. (This function is available to the LAN interface only.)

7. Default Policy: When item#6 (-IP Access Control) set to "enabled," you can select either "accept" or "drop", allowing access or denying access according to pre-defined rules. (**Note**: If this option is set to "drop," and you do not have a set of rules that will accept the internet connection, then the internet connection over LAN is impossible. In this case, you need to change your security settings via modem or by disabling the IP Access Control.)

8. Rule#: Enter a rule number in the box for a command (or commands) that will be used by the IP Access Control.

9. IP/Mask: Enter the IP Address or an IP Address Range for which the command(s) will be applied.

10. Policy: This item instructs the IPMI what to do with the matching packages.

(**Note:** The sequence or the order of the rules is important. The rules are checked in the ascending order until a rule matches. All rules below the matching one will be ignored. The default policy applies if no matching rules are found.)

11. Append: Select this option to add IP Address/Mask, rules or commands to the existing ones.

12. Insert: Select this option to insert IP Address/Mask, rules or commands to the existing ones.

13. Replace: Select this option to replace an old IP Address/Mask, rule or command with a new one.

14. Delete: Select this option to delete (a part of) an existing IP Address/Mask, rule or command.

15. User Blocking: This window allows you to set the conditions how a user is blocked.

16. Max. Number of Failed Logins: Enter the maximum number of failed attempts or failed logins allowed for a user. If the number of failed logins or attempts exceeds this maximum number allowed, the user will be blocked from system.

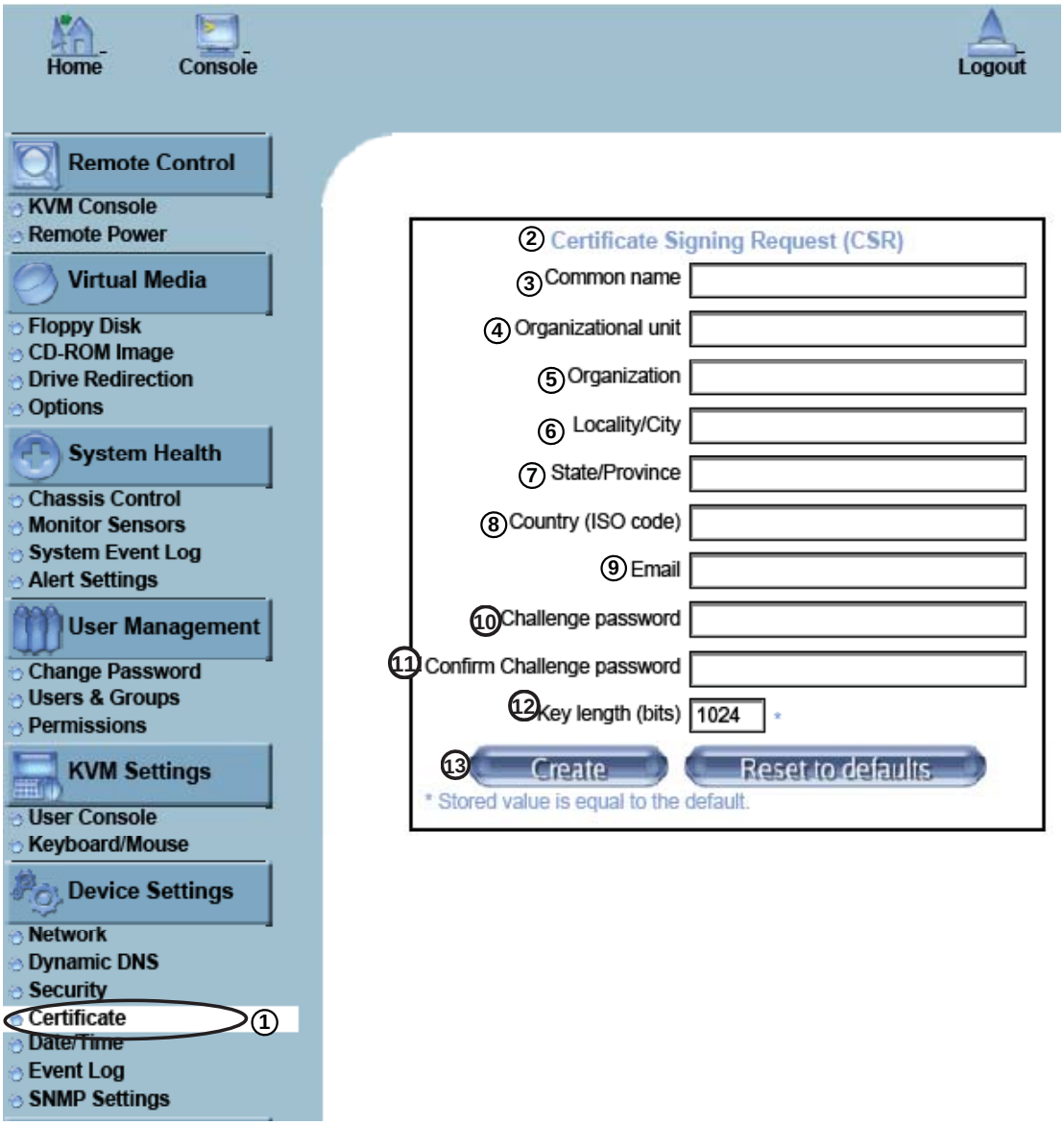
(**Note:** If this box is left empty, the user is allowed to try to login to the server infinitely. For network security, this is not recommended.)

17. Block Time (Minutes): Enter the number of minutes allowed for a user to attempt to login. If the user fails to login within this time allowed, the user will be blocked from system.

(**Note:** If this box is left empty, the user is allowed to try to login to the server infinitely. For network security, this is not recommended.)

d. Certificate

Device Settings: Certificate



d. Certificate

1. Certificate: Click on this function key to activate its submenu and configure the following Certificate settings as listed below.

2. Certificate Signing Request (CSR): This window allows you to define the Certificate Signing Request (CSR) form. The IPMI uses the Secure Socket Layer (SSL) protocol for encrypted network traffic between itself and the remote host servers. When a connection is made, the IPMI has to expose its identity to a remote host by using a cryptographic certificate.

Note: SHA1 and RSA 2048 bit SSL supported.

To create a certificate that is unique to a particular IPMI card or SIMLP card, a certification authority (CA) needs to fill out the CSR form indicated in the CSR window above and click "Create" to generate it.

3. Common Name: Enter the (fully qualified domain) network name of the IPMI.

4. Organization Unit: Enter the name of the department within an organization that the IPMI belongs to.

5. Organization: Enter the name of the organization that the IPMI belongs to.

6. Locality/City: Enter the name of the city or the location where the organization is located.

7. State/Province: Enter the name of the state/province where the organization is located.

8. Country (ISO): Enter the name of the country or the ISO code where the organization is located.

9. Email: Enter the email address of a contact person that is responsible for the IPMI.

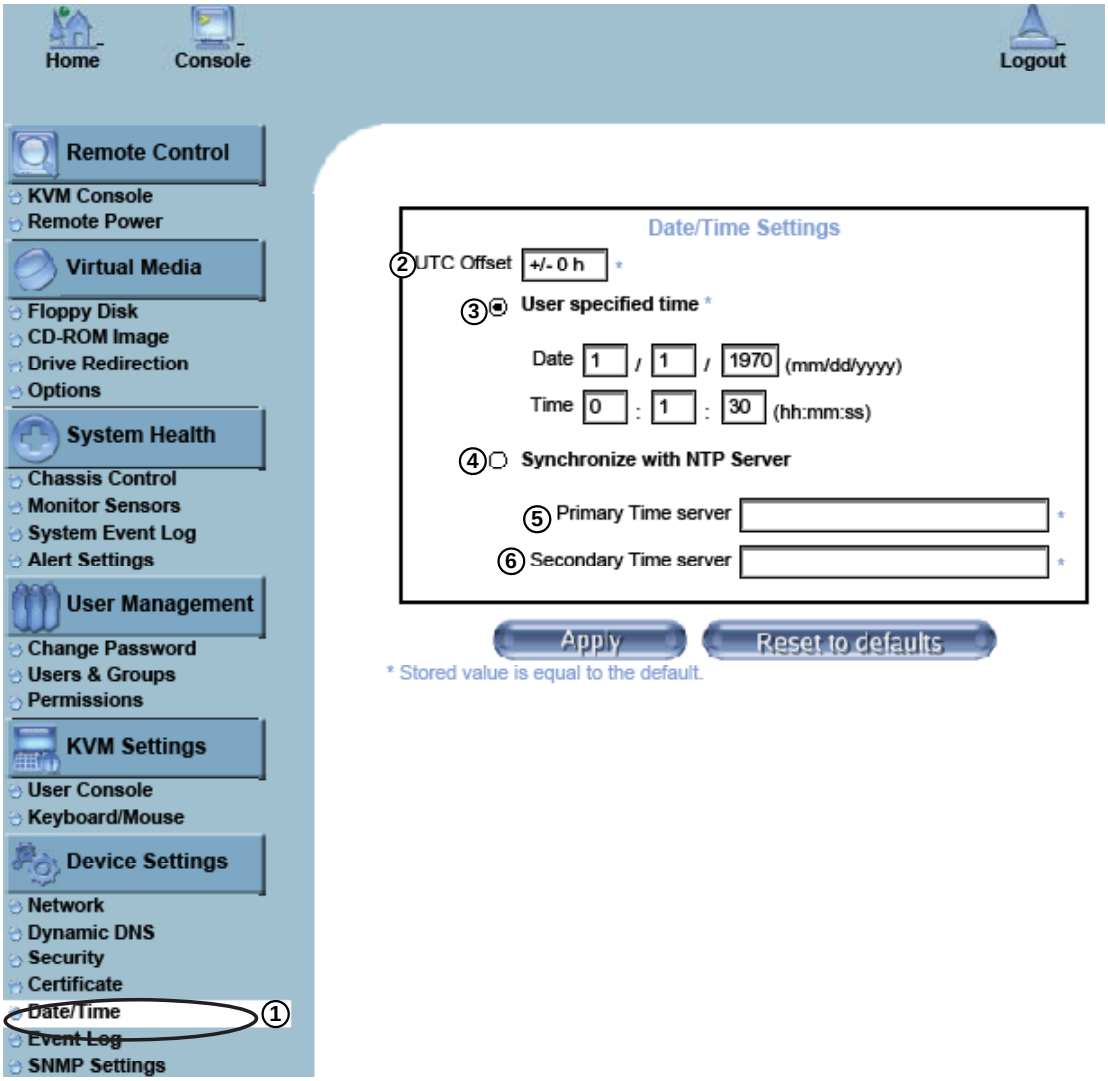
10. Challenge Password: Enter a challenge Password for the Certification Authority to authorize necessary changes to the certificate at a later time. The password shall be four characters or longer.

11. Confirm Challenge Password: Enter a challenge Password one more time to confirm it.

12. Key Length (bits): This is the length of key generated in bits.

e. Date/Time

Device Settings: Date/Time



e. Date/Time

1. Date/Time: Click on this function key to activate its submenu. This feature allows you to set the internal realtime clock for your SIMLP card.

2. UTC Offset: This window allows you to offset the UTC Timer.

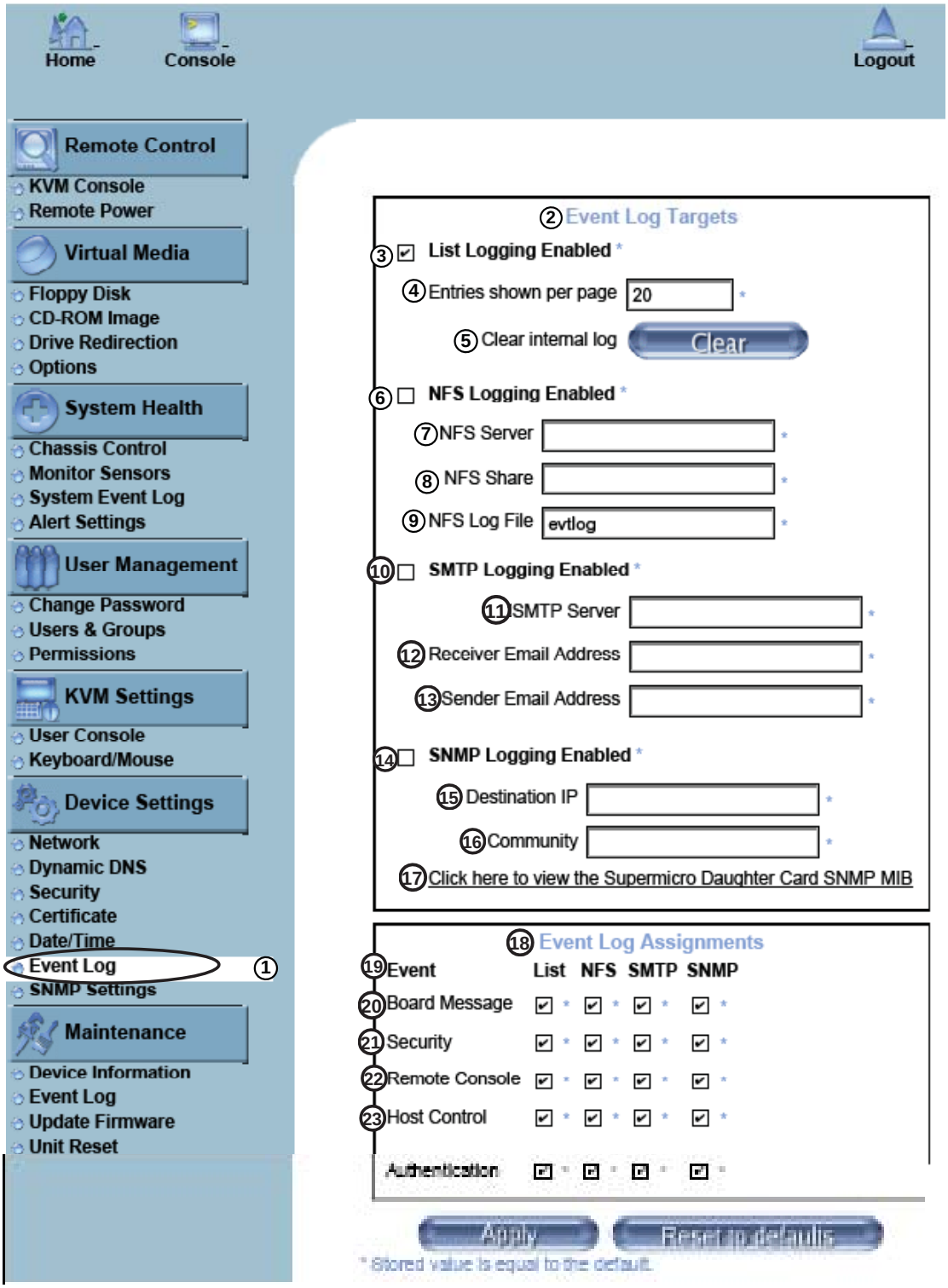
3. User Specified Time: This option allows the user to enter the time values for the SIMLP internal realtime clock.

4. Synchronize with NTP Server: Enter the IP Address for the NTP (Network Time Protocol) Server that you want your SIMLP internal realtime clock to synchronize with.

5/6. Primary Time Server/Secondary Time Server: Enter the IP Address for the primary NTP Server and the secondary NTP Server that you want your SIMLP internal realtime clock to synchronize with. (The daylight saving time cannot be automatically adjusted. Please manually set up the UTC offset twice a year for your timer to work properly.)

f. Event Log

Device Settings: Event Log



f. Event Log

1. Event Log: Click on this function key to activate its submenu. This feature allows you to set Event Log Targets and Event Log Assignment.

2. Event Log Targets: This section allows you to manually set the event log targets and settings.

3. List Logging Enabled: Check this box to activate the event-logging list. To show the event log list, click on "Event Log" on the "Maintenance" page. (The maximum number of log list entries is 1,000 events. Every entry that exceeds this limit will automatically override the oldest one in the list. If the reset button is pressed, all logging information will be saved; however, all logging data will be lost if hard reset is performed or the system loses power.)

4. Entries Shown Per Page: Enter the number of entries you want to display on a page.

5. Clear Internal Log: Click this icon to clear internal event log from the memory.

6. NFS Logging Enable: Click this box to enable NFS Logging which will create a Network File System (NFS) for the event logging data to be written into.

7. NFS Server: Enter the IP Address of the NFS Server.

8. NFS Share: Enter the path of the Network File System in which the event logging data is stored.

9. NFS Log File: Enter the filename of the Network File System in which the event logging data is stored.

10. SMTP Logging Enable: Check this box to enable the function of SMTP (Simple Mail Transfer Protocol) logging.

11. SMTP Server: Enter the IP Address for the SMTP Server.

12. Receiver Email Address: Enter the email address that the SMTP event logging data will be sent to.

13. Sender Email Address: Enter the email address from which the SMTP event logging data is sent.

14. SNMP Logging Enable: Check this box to enable the function of SNMP (Simple Network Management Protocol) logging.

15. Destination IP: Enter the IP address where the SNMP trap will be sent to.

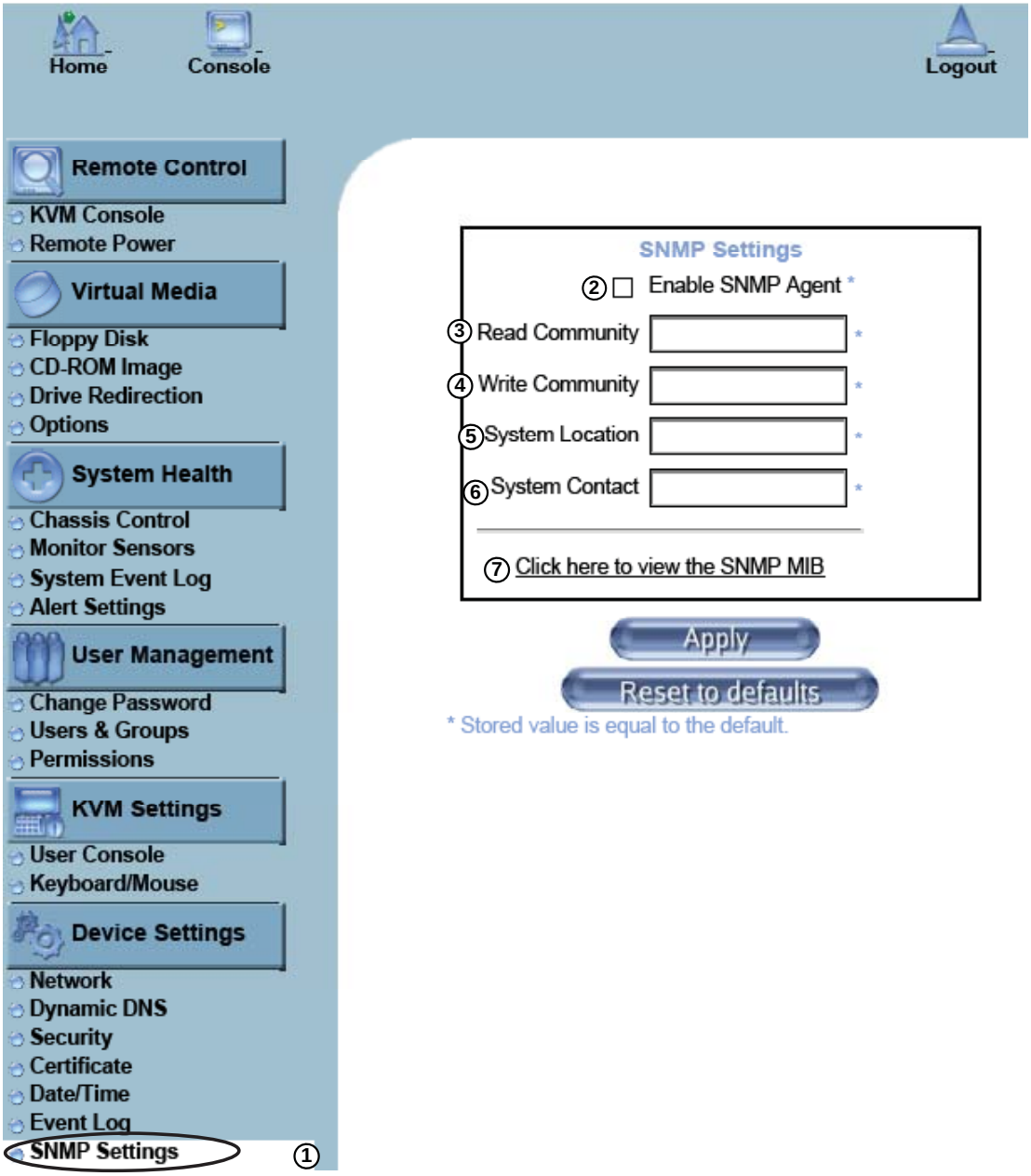
16. Community: Enter the name of the community if the receiver requires a community string.

17. Click here to view the Supermicro Daughter Card SNMP MIB: Click this link to see the SMLP card SNMP MIB.

18. Event Log Assignments: This window allows you to specify the types and the destination for the event logging.

g. SNMP Settings

Device Settings: SNMP Settings



g. SNMP Settings

1. SNMP Settings: Click on this function key to activate its submenu. This feature allows you to configure Simple Network Management Protocol settings.

2. Enable SNMP Agent: Check the box to enable the SNMP Agent and allow it to interface with your SIMLP card.

3. Read Community: Enter the name of the SNMP Community from which you will retrieve information via SNMP.

4. Write Community: Enter the name of the SNMP Community to which you can write information and issue commands via SNMP.

5. System Location: Enter the physical location of the SNMP host server. This location will be used in response to the SNMP request as "sysLocation0."

6. System Contact: Enter the name of the contact person for the SNMP host server. This value will be referred to as "sysContact0."

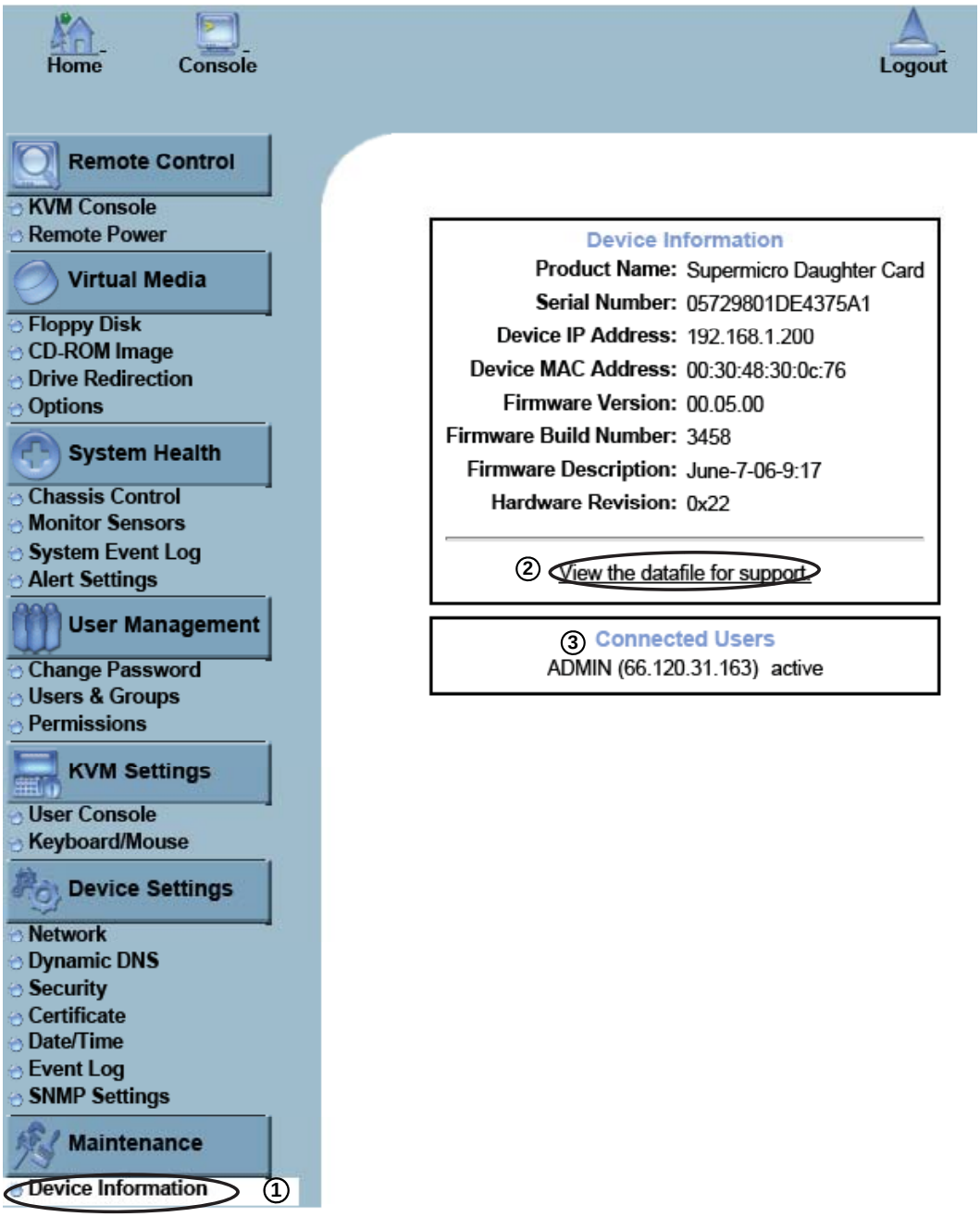
7. Click here to view the SNMP MIB: Click this link to view the SMLP card SNMP MIB file. This file may be necessary for an SNMP client to interface with the SIMLP card.

3.2.7 Maintenance

Click on the Maintenance icon on the Home Page to activate its submenus: Device Information, Event Log, Update Firmware and Unit Reset Settings as listed below.

a. Device Information

Maintenance: Device Information



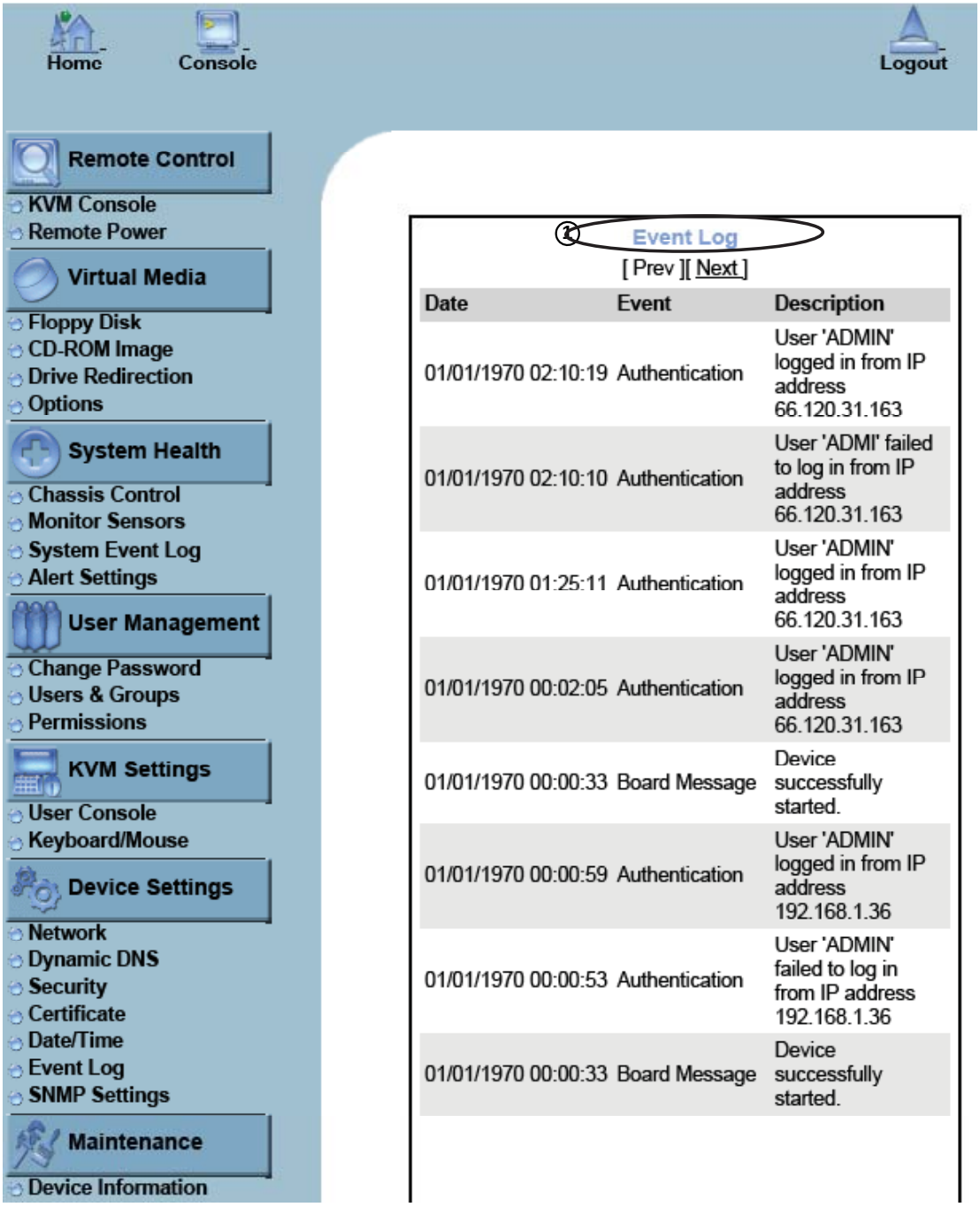
1. Device Information: Click on this function key to activate its submenu. This feature displays the information of the SIMLP card and its firmware.

2. View the Data File for Support: Click on this link to view the XML file which contains you and your product information which is needed for technical support.

2. Connect Users: List the name(s), the IP Address(es) and the status of the connect person(s).

b. Event Log

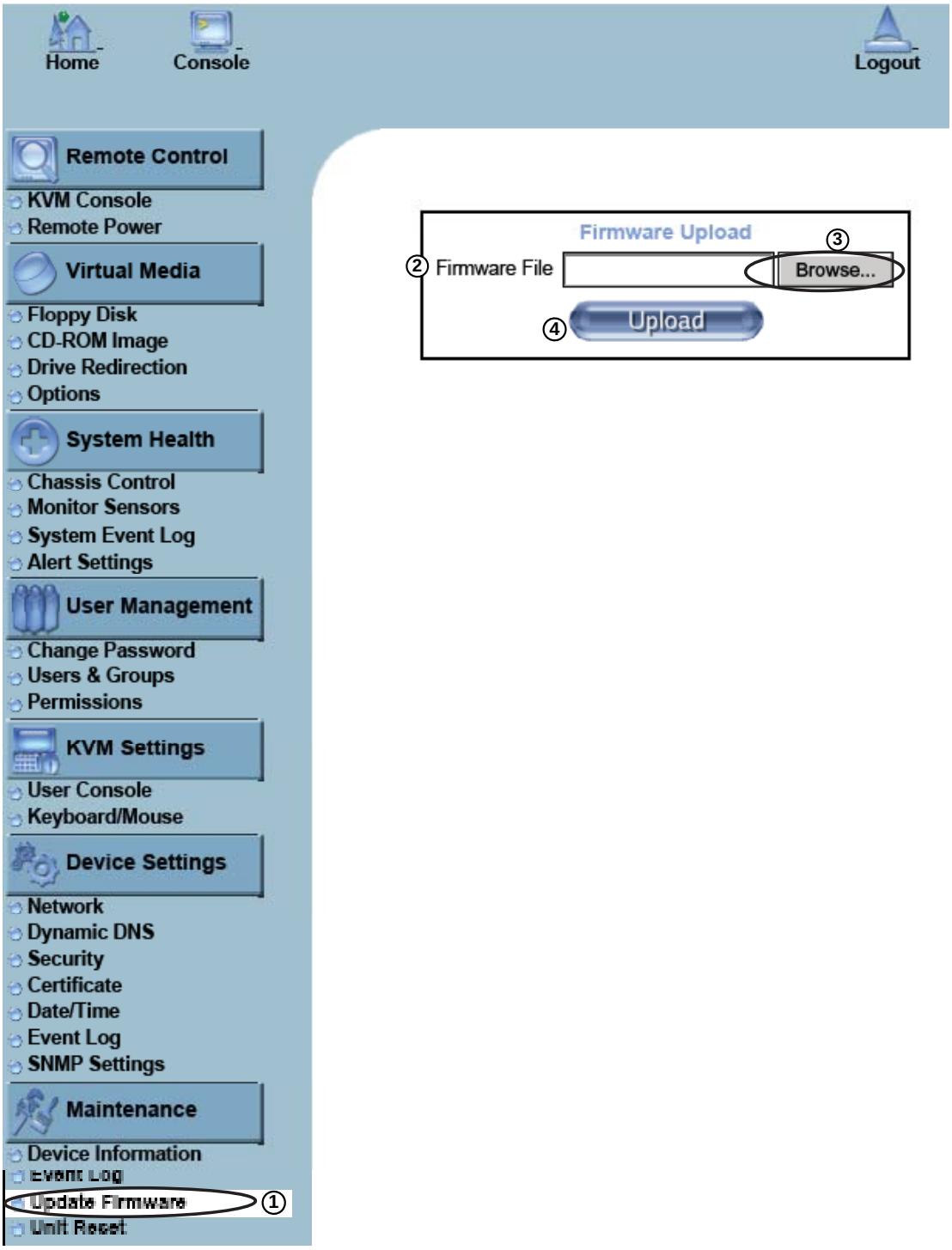
Maintenance: Event Log



1. Event Log: Click on the function key on the left to activate the Event Log submenu. Once the submenu is displayed, the Event Log List will display. **The Event Log List** contains the information of events that are recorded by the SIMLP in the order of Date/Time, Types, and the descriptions of the events including the IP address(es), person(s) and activities involved .

c. Update Firmware

Maintenance: Update Firmware



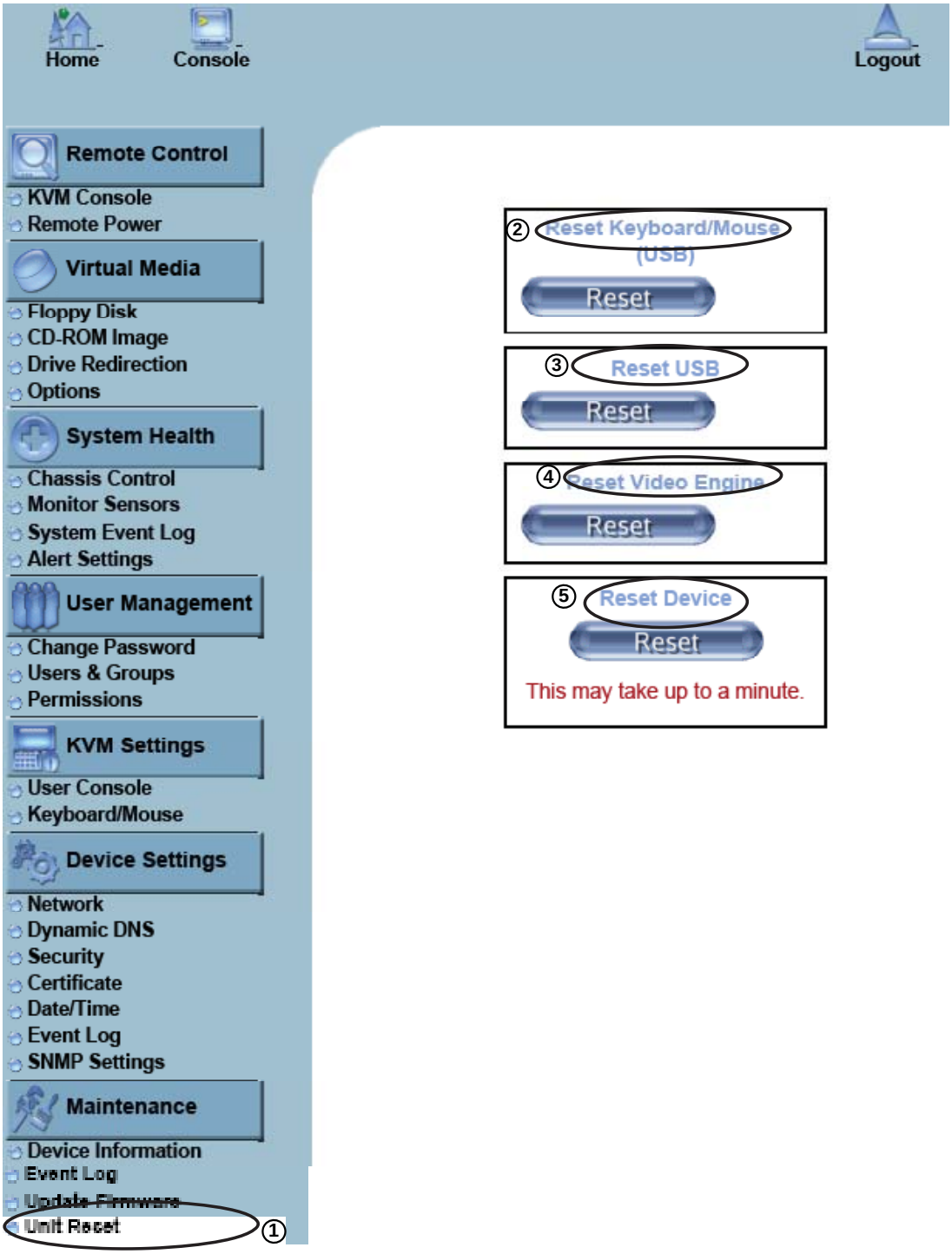
1. Update Firmware: Click on this function key to enable "Update Firmware."

2/3. Firmware File: Enter the name of the firmware you want to update or click on the "Browser" icon to select the firmware file.

4. Update: Click on the "Upload" icon to upload the firmware file to the server for the update. **(Note**: This process is not reversible once the firmware is updated, so proceed with caution. It might take a few minutes to complete the procedure.)

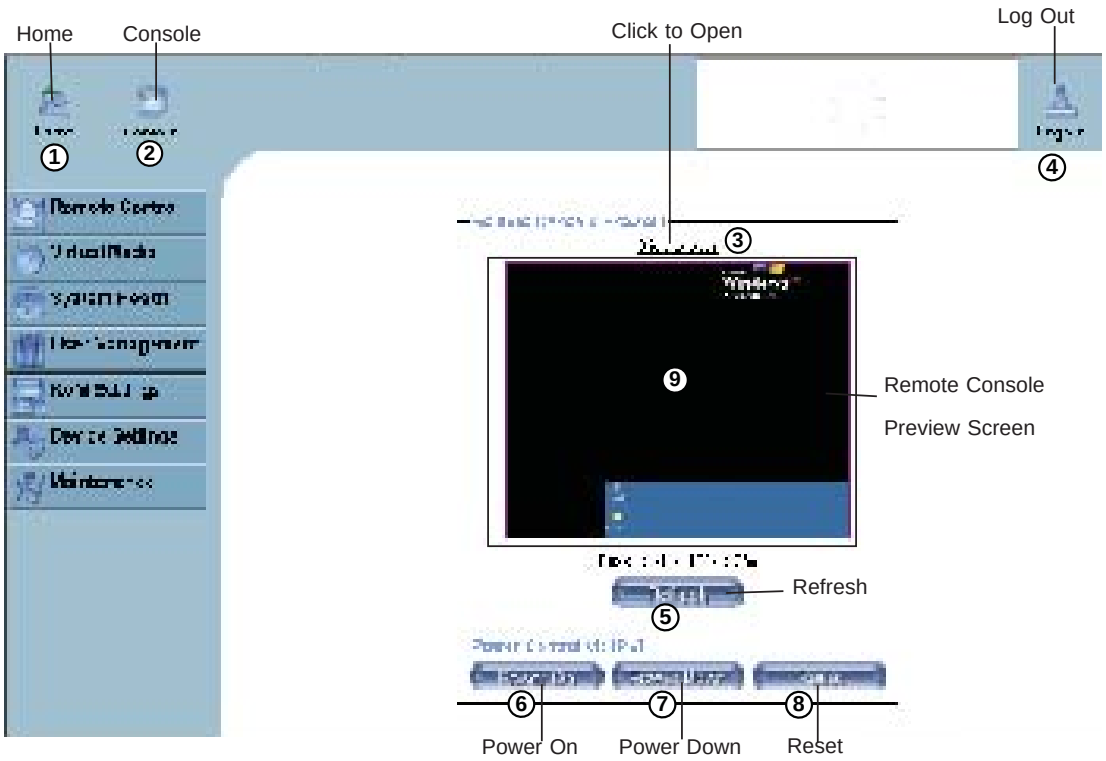
d. Unit Reset

Maintenance: Unit Reset



1. **Unit Reset:** This feature allows you to reset the following components:
2. **Reset Keyboard/Mouse:** Click the "Reset" icon to reset Keyboard/mouse.
3. **Reset USB:** Click the "Reset" icon to reset the USB module.
4. **Reset Video Engine:** Click the "Reset" icon to reset Video and its controller.
5. **Reset Device:** Click the "Reset" icon to cold reset the IPMI firmware.

3.3 Remote Console Main Page



After you have entered the correct IP address for your remote console and typed in correct user name and password, you should be connected to the remote console. When the remote console is connected, the Remote Console window displays as shown above. To go to the remote console screen, you can do one of the following:

1. Click on the console icon (marked "2") on the upper left corner, or

2. Click on the link "Click to Open" to open the remote console screen as shown on #3 above.

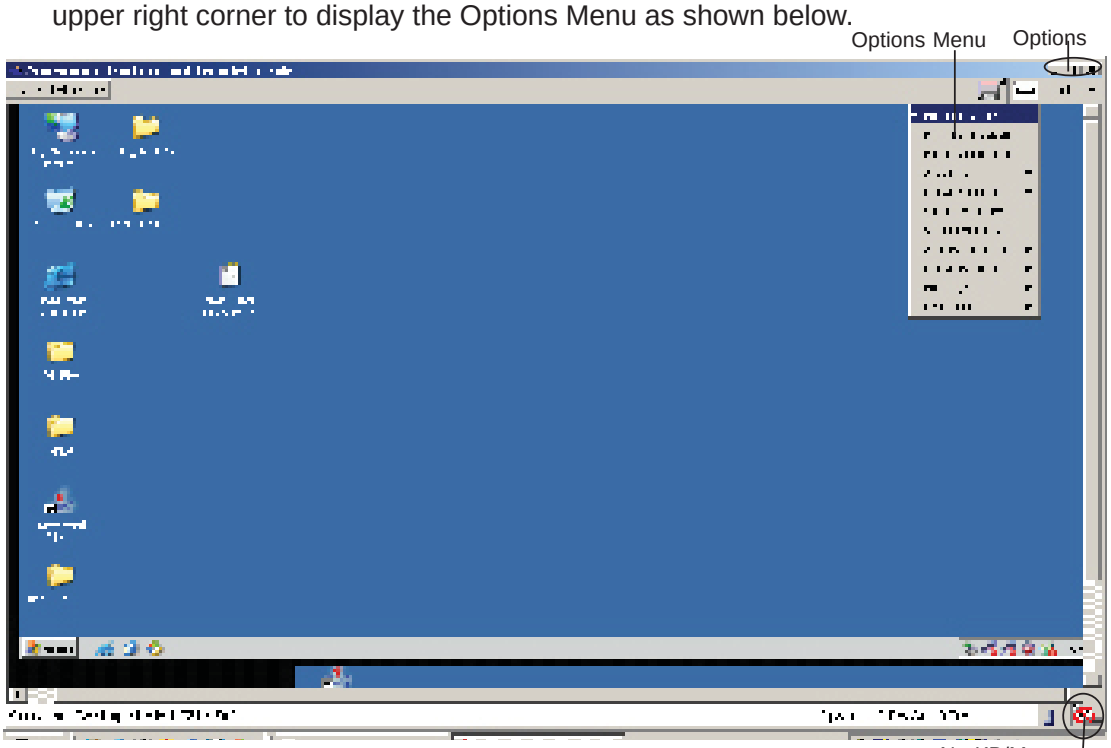
The remote console screen as shown on the next page displays.

Note: For your reference, the functions of the icons for this home page are listed below:

1. **Home**: Click this icon to return to the Home Page.
2. **Console**: Click this icon to open the remote console screen.
3. **Click to Open**: Click this link to open the remote console screen.
4. **Log-Out**: Click this icon to log out.
5. **Refresh**: Click this icon to refresh the remote console preview screen.
6. **Power On**: Click this icon to power on the remote server.
7. **Power down**: Click this icon to power down the remote server.
8. **Reset: Click this icon to reset the remote server.**
9. **Remote Console Preview Screen**: This window displays the preview of the remote console screen. Click on this window to go to the remote console screen.

3.3.1 Remote Console Options

After the remote console screen appears, click on the button "Option" on the very upper right corner to display the Options Menu as shown below.



a. Options Menu Items

The following items are included in the Options Menus:

1. Monitor Only: Click on the Monitor Only button to turn the function of "Monitor Only" on or off. If the function of "Monitor Only" is selected, the KB/Mouse icon on the lower right corner will be crossed out as shown above, and the user can only view or monitor remote console activities. Any remote console interaction is no longer available.

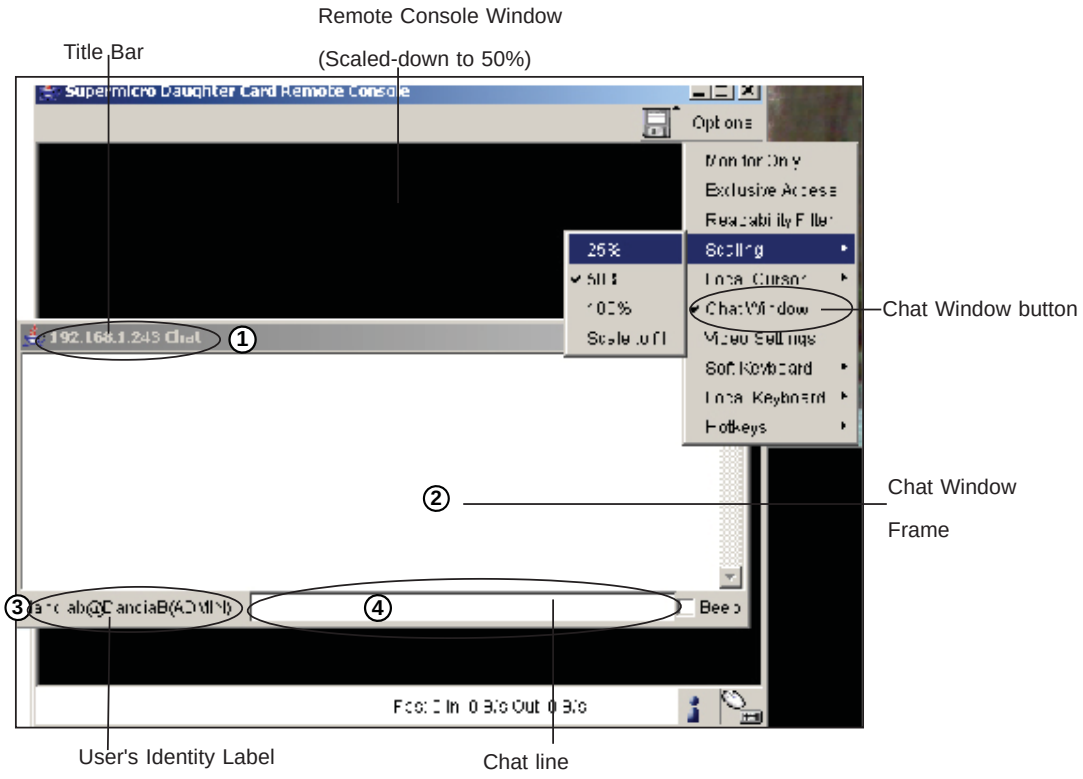
2. Exclusive Access: With an appropriate permission, a user can force other users to quit the remote console and claim the console for his or her own exclusive use by clicking on the Exclusive Access icon to select it. When this function is selected, the 2nd user icon on the lower left corner of the screen will be crossed out.

3. Readability Filter: Click on this button to turn the "Readability Filter" on or off. Turn on this function to preserve most of the screen details even when the screen image is substantially scaled down. (**Note**: This item is available for a system with a JVM 1.4 or higher.)

4. Scaling: This item allows the user to scale the remote console screen to a desired size. Click on this button to access its submenu and select a desired setting from the options listed in the submenu: 25%, 50%, 100% and Scale to Fit.

5. Local Cursor: This item allows the user to choose the desired shape for the local cursor pointer. Click on this button to access its submenu and select a desired shape from the options listed in the submenu: Transparent, Default, Big, Pixel, and Crosshair. The availability of the shapes depends on the Java Virtual Machine used.

6. Chat Window: This item allows the user to communicate with other users logged in the same remote host by clicking on the Chat Window button. The screen below shows a Chat Window displayed in a scaled down remote console screen.



For your reference, the items shown on the Chat Window screen are listed below:

1. Title Bar: This shows the IP address of the remote host you are connected to.

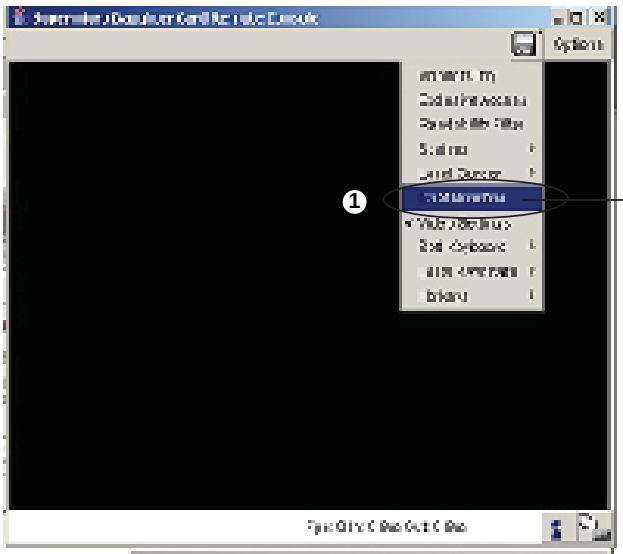
2. Chat Window Frame: This frame displays chat messages, including your own message that has been sent to other users. This is a read-only test display area.

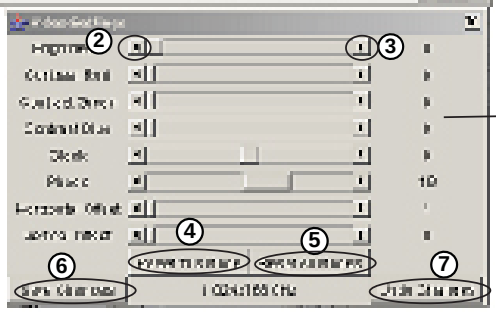
3. User's Identity Label: This line displays your own identity.

4. Chat Line: This is an edit-able text line where you can enter a new message.

Note: Once you've typed your message in the chat line box and press <Enter>, your message will be sent to remote systems and read by other users. Please review the text displayed in the chat line box before you hit the <Enter> key.

7. <u>Video Settings</u>: This item allows the user to set the monitor display settings by clicking on the Video Settings button (marked "1" below.) After you've clicked the Video Settings button, the submenu displays as shown below.





Use your cursor pointer to click on the triangles (marked 2 and 3) to adjust the setting for each of the following items:

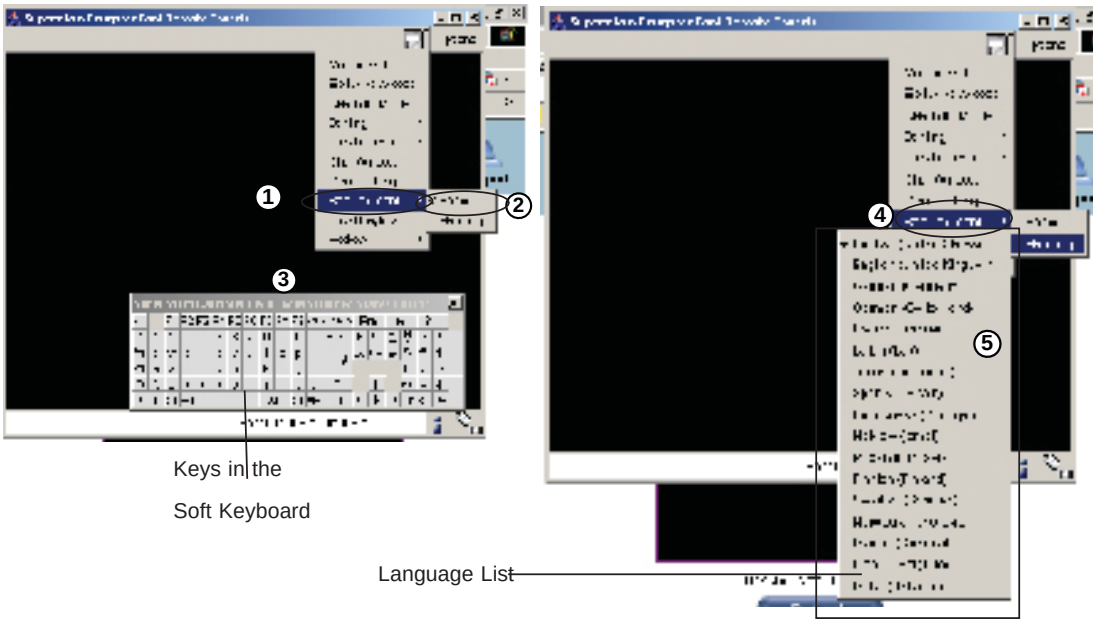
i. Brightness
ii. Contrast Red
iii. Contrast Green
iv. Contrast Blue
v. Clock
vi. Phase
vii. Horizontal Offset
viii. Vertical Offset

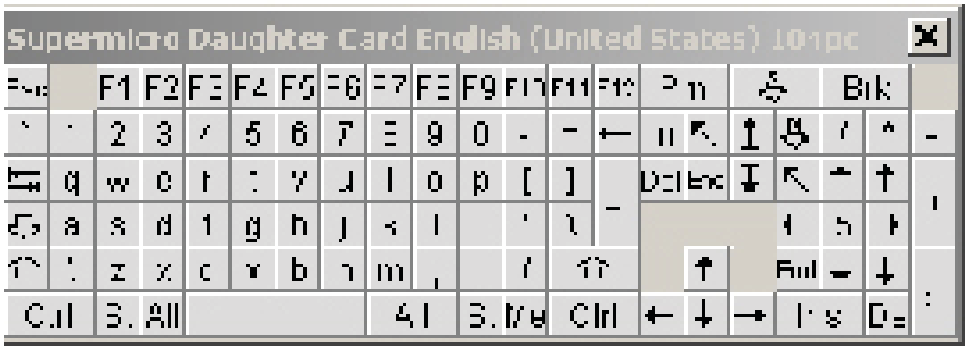
If you are not happy with the changes you have made, you can click on the "**Reset this Mode**" button (marked 4) to reset a particular item, or click on the "**Reset All Modes**" button (marked 5 above) to reset all items.

To save all changes, click on the "**Save Changes**" button (Marked 6). You can also click on the "**Undo Changes**" (Marked 7 above) to abandon the changes.

If "Save Changes" is selected, the confirmation message as shown below appears. Click "OK" to save the changes. Click "Cancel" to return to the previous menu.

8. Soft Keyboard: This item allows the user to use the soft keys that have been pre-installed in the "Soft Keyboard" of the particular language selected. After you've clicked the Soft Keyboard button, the submenu displays as shown below.





③ **Keys in English Soft Keyboard**

i Soft Keyboard: Click on this button to use the pre-installed soft keys or to select keyboard language.

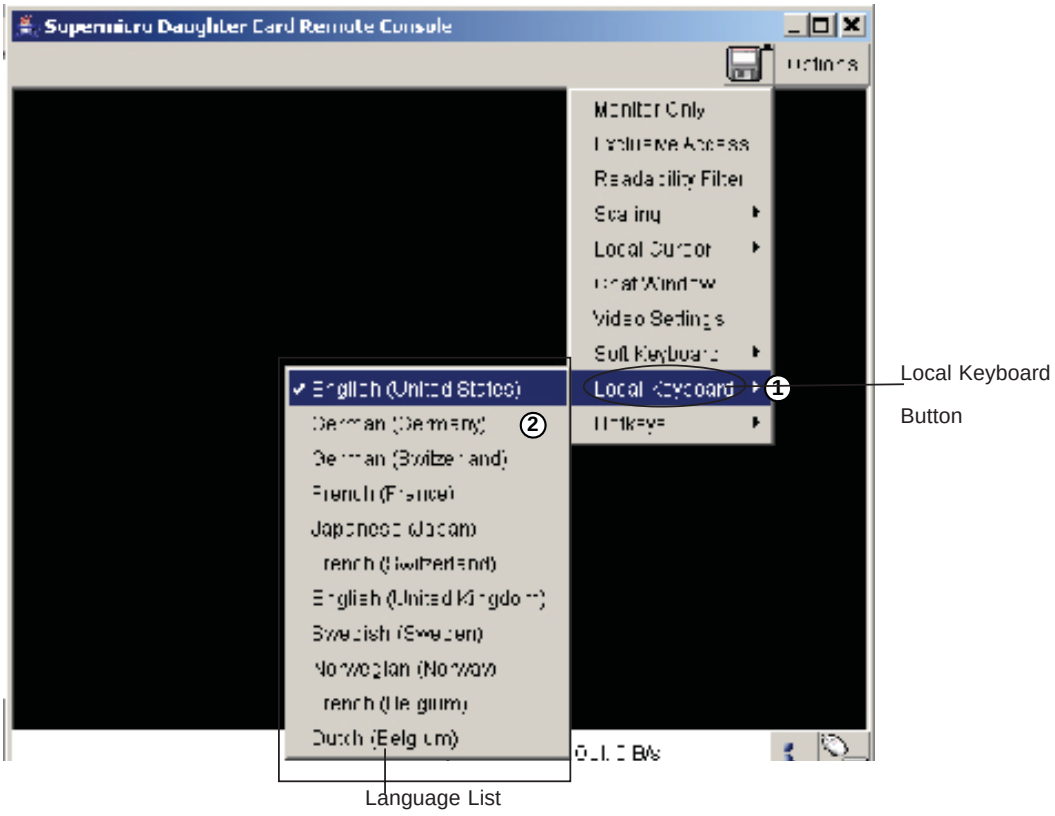
ii. Show: Click on the "Show Button" to show a soft keyboard which contains pre-installed soft keys.

iii. Soft Keyboard: When the soft keyboard displays, use your mouse cursor to select the soft key(s) you want to use.

iv. Mapping: Click on this button to display a list of major languages of the world. Select from the list the language you want the soft keyboard to be in.

v. Language List: When this language list displays, select the language you want to use by clicking on it.

9. Local Keyboard: This item allows the user to manually change the local keyboard setting for interaction with a remote host. Use this function to change the language mapping of your browser machine running the remote console host. After you have clicked Local Keyboard button, the submenu displays as shown below.

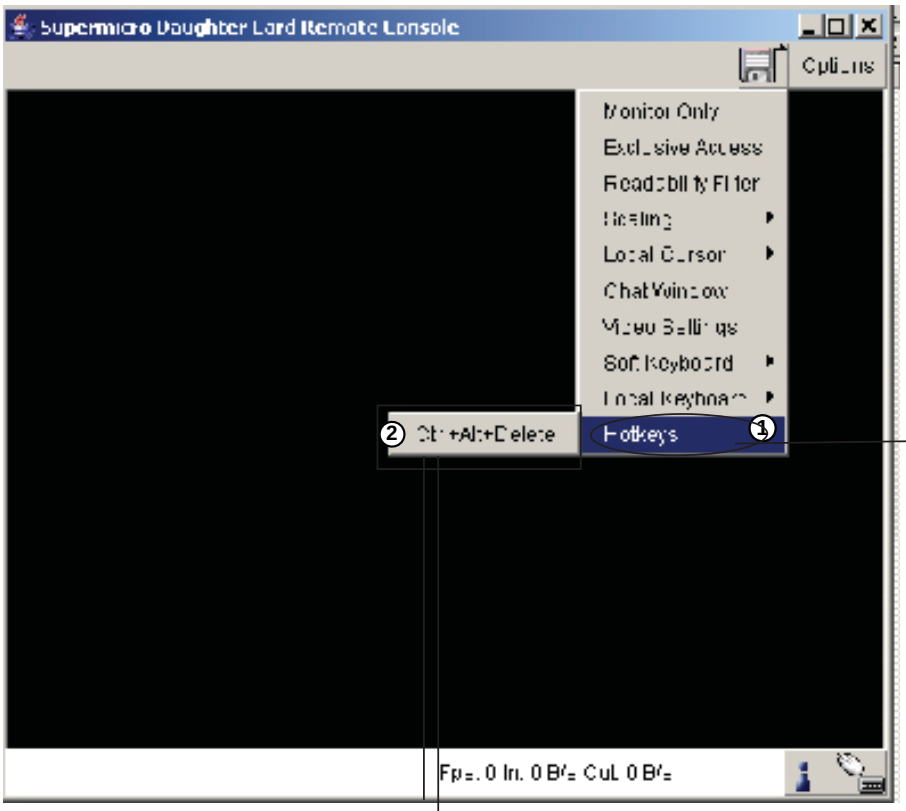


i Local Keyboard: Click on this button to manually change the local keyboard setting for remote console interaction. Use this function to change the language mapping of your browser machine running the remote console host. Click on this button to display a list of major languages in the world.

ii. Language List: When this language list displays, select the language you want to use.

10. Hot Keys: This item allows the user to select a pre-defined hot key from a hot key list. Once a hot key is selected, the command associated with the hot key will be sent to the remote console host for execution.

After you've clicked Hot Key button, the submenu displays as shown below.

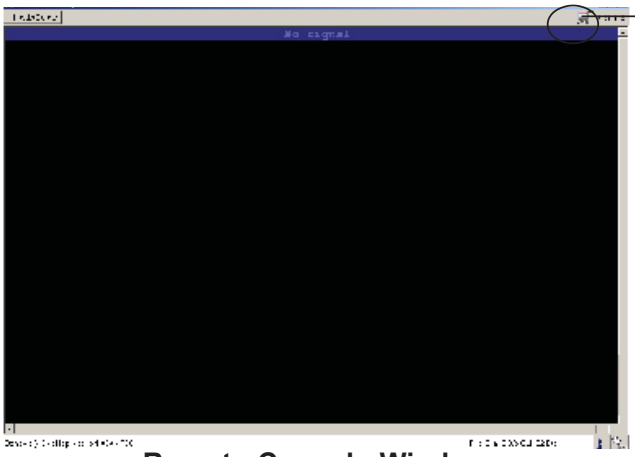


i. Hot Key Button: Click on this button to display a hot key list. This list contains the hot keys that have been pre-defined and pre-entered in the system. You can also use this function to write your own commands and add your own hot keys to the list.

ii. Hot Key List: Select from the list a hot key you wish to use. By selecting a hot key, you will send the command associated with this hot key will be sent to the remote host for execution.

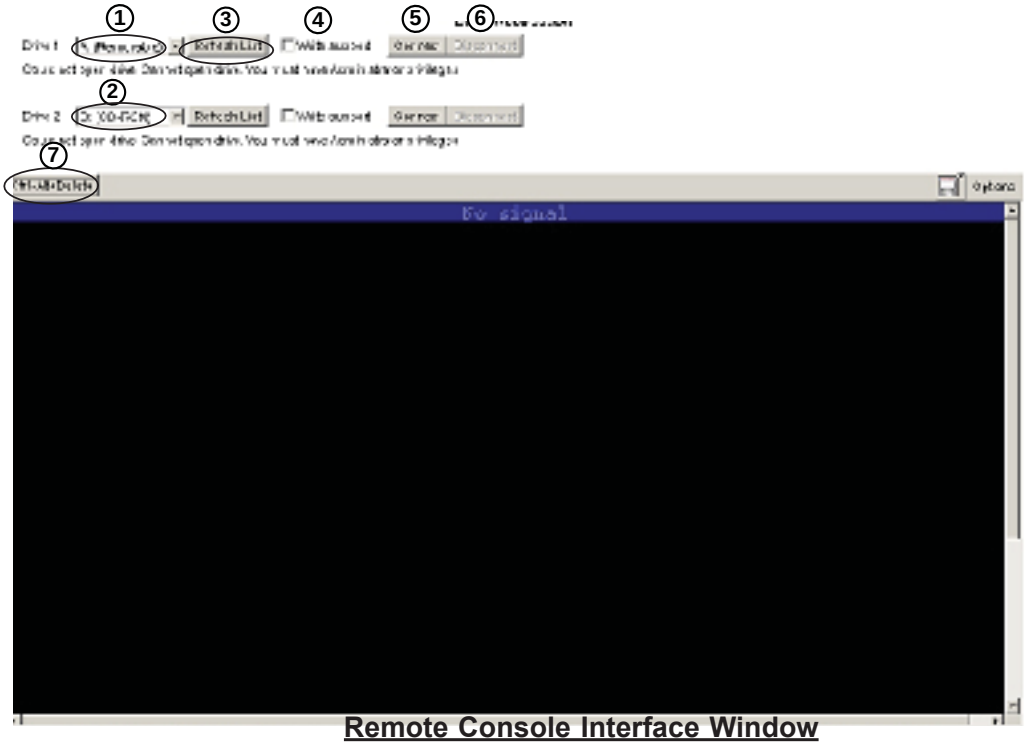
11. Remote Console Interface Window: This item allows the local host to interact with a remote server. Through the Remote Console Interface Window, the user can share files stored in the local drive with a user connected to the remote server, download data from a local drive to the remote server, issue commands to manage the remote server, or allow the remote server be controlled and managed by a local user logged in the remote server. This function provides a full spectrum of remote console interaction and management. You also need to have the Administrator Privilege to use this feature.

To access the Remote Console Interface window, you need to click the Console icon on the Remote Console window as shown below.



Remote Console Window

Once you have clicked on the Console Icon on the Remote Console window, the Remote Console Interface window displays as shown below.

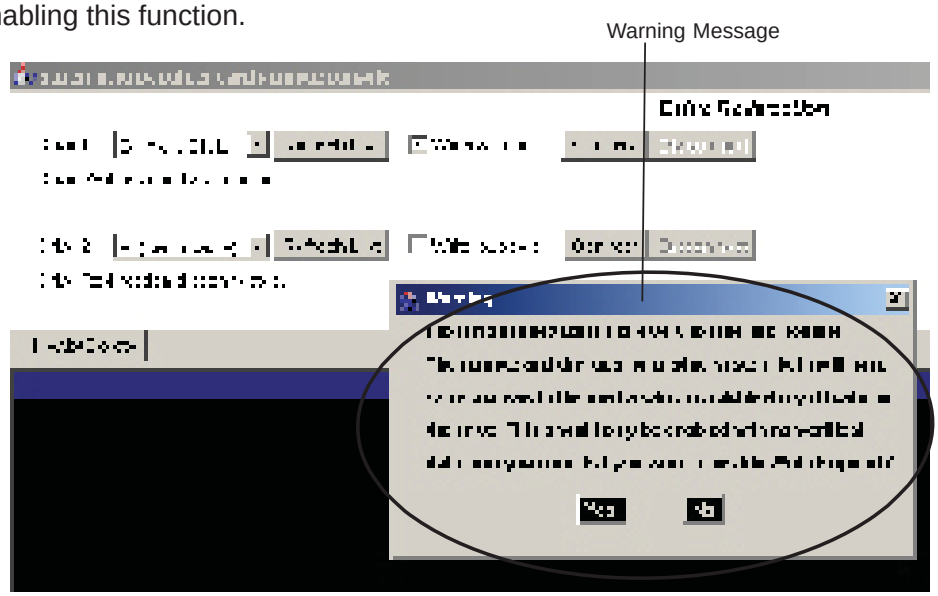


Remote Console Interface Window

i./ii. Local Drive List: The box displays a list of local drives available for remote access. Select from the list a local drive that you want to make accessible for a remote server.

iii. Refresh: Click this button to refresh the local drive list.

iv. Write Support: Check this button to allow the remote operating system to have write access to the drive that you have selected. This function allows a user to alter, overwrite, erase and destroy data stored in the drive selected. This feature should only be used with non-critical data. When "Write Support" is checked, the warning message as shown below will display. Read the warning message carefully before enabling this function.



v. Connect: Click this button to make the drive you have selected accessible for remote console interaction. Once you have clicked "connect," users logged in remote servers will have access to the local drive that you have selected.

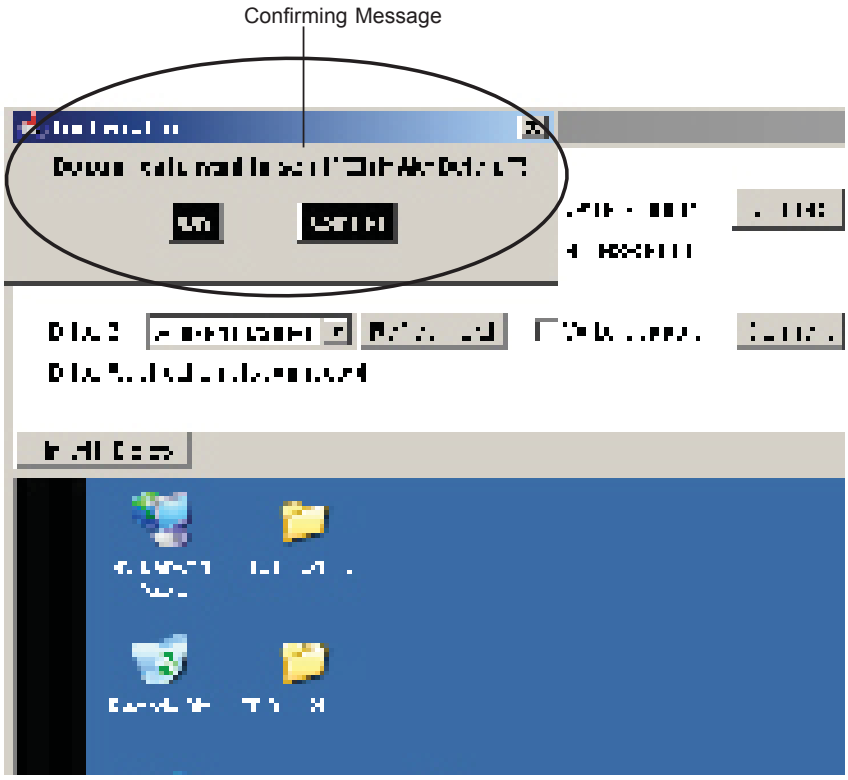
vi. Disconnect: Click this button to cancel the connection established between a local drive and a remote server. Once you click this button, the drive you have selected will not be accessible for remote console interface.

vii. Sending Commands: This functions allows the user to issue a pre-defined command to a remote server for execution.

To use this function, you need to click the hot keys displayed on the upper right corner of the screen as shown below. (**Note**: Hot keys are the commands that have been pre-defined and pre-stored in a remote consoles.)

Click Button 7 "Ctrl+Alt+Delete" as shown on Page 3-49 to send the command "Ctrl+Alt+Delete" to the remote server for execution.

Once you have clicked on the button, a message displays, asking you if you really want to send "Ctrl+Alt+Delete" as shown in the picture on the next page. Click "Yes" to confirm it or click "Cancel" to stop sending the command for remote execution.


Confirming Message

To Log Out

Return to the Home Page and click on the "Log Out" button to log out from Remote Console Interface.

Chapter 4
Frequently Asked Questions

1. Questions: How do I flash the firmware of an IPMI card such as a SIM1U card or a SIM1U+ card?

Answer:

- 1. Log on to the web interface page of the IPMI card by typing the IP address of the card.
- 2. Click on the maintenance button.
- 3. Browse to choose the correct file to flash the firmware.
- 4. Click on the "Update Firmware" button and proceed with firmware flashing.

2. Questions: How do I setup the IP address and MAC address for the AOC-SIM1U(+) Add-On card?

Answer:

- 1. Boot the system into DOS.
- 2. Run the utility-IPNMAC from DOS.
- 3. Follow the prompts to setup the IP Address and MAC address for the AOC-SIM1U(+).

Contacting Technical Support:

If you still have problems after trying out all the recommended solutions, please contact our Tech. Support @ (408)503-8000 or visit our web site @ www.supermicro.com/support/.

Notes