IPMIView
User's Guide

Version 2.7

Table of Contents

1. Overview

IPMIView is a management software program based on the IPMI specification Reversion 1.5 - 2.0. IPMIView sends IPMI messages to and from the BMC (Base Management Card) on a host system at a remote location. IPMI messages are encapsulated in the RMCP (Remote Management Control Protocol) packets called "datagrams." This method is also referred to as "IPMI-over-LAN."

According to the Distributed Management Task Force (DMTF) Specification, RMCP is used for system management in a pre-OS or an OS-absent environment. RMCP is a simple request-response protocol that can be delivered using the UDP (User Datagram Protocol) datagrams. IPMI-over-LAN uses version 1 of the RMCP protocol and packet format. An RMCP packet is transmitted via an IP (Internet Protocol) networking, which will allow system managers to manage their IPMI-enabled systems over the Internet. In a private LAN network, this is a basic feature. IPMI uses the same UDP port number (623 in decimal) as the ASF (Alert Standard Forum) protocol. If the managed system is protected by a firewall, UDP port 623 must be opened.

In Supermicro's IPMI solution, a BMC (Baseboard Management Controller) shares the LAN1 NIC on the mainboard. (If there are more than one LAN Ports on the mainboard, LAN1 is the one closest to the Keyboard/Mouse Port.) The NIC will re-route the IPMI packet to the BMC instead of forwarding it to the upper layer of the network protocol stacks as other protocol packets do.

IPMIView V2.0 covers Supermicro's BMCs for both IPMI v1.5 and IPMI v2.0. However, due to design changes, some functions may not be available for IPMI v1.5, while others, might no longer be available for IPMI v2.0. IPMIView will automatically hide any functions that are not available based on the BMC version used in the system.

2. System Management

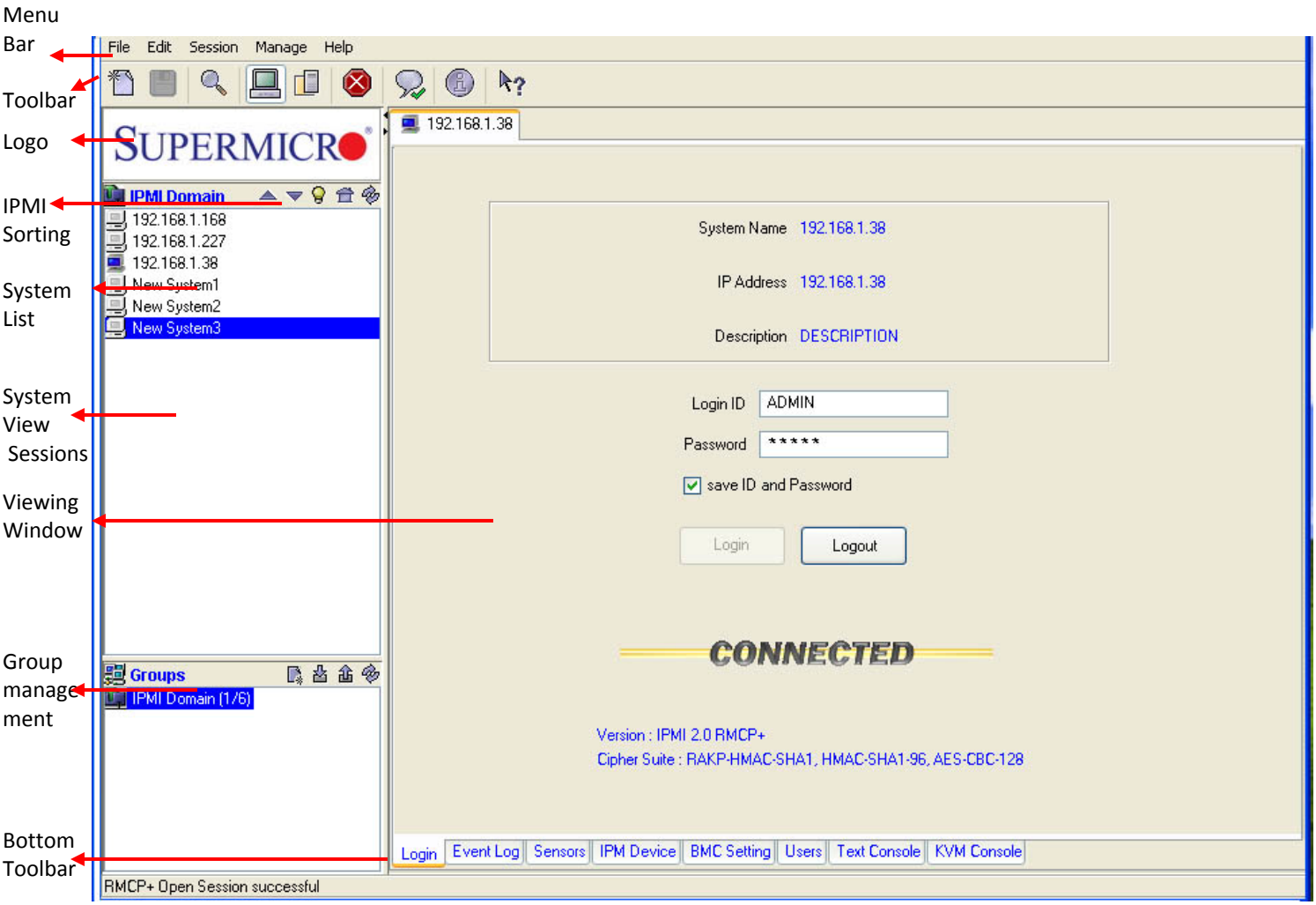


Figure 2-1

As shown in Figure 2-1, there are several components in the IPMIView window (Figure 2-2):

1) Menu Bar: contains functions that allow you to add/delete systems or groups and save configurations.
2) Toolbar: contains functions that allow you to execute commands quickly. Click the icons on the toolbar to add a new system, save the current configuration settings, to discover IPMI devices, to access group management, to discontinue the IPMIView section and to access the help menus. See Figure 2-2 for details.
3) Logo: Click the Logo icon to visit Supermicro's website.
4) IPMI Sorting: This allows you to sort devices in an ascending/descending order via the online format, or in the original sequence.
5) System List: This lists the computers managed by the BMC Controller.
6) Group management: This allows the user to manage system groups, including creating/adding new accounts, deleting accounts and update group information.
7) Group List: It lists computer groups managed by the BMC for better management.
8) Viewing Window: This shows detailed information including Login, IPMI Device, Event Log, Sensors, BMC Settings, and the status of the IPMIView firmware.
9) System View Sessions: IPMIView can manage up to 20 systems at any given time. The systems that are currently managed by the BMC are indicated in the System View window.

10) Bottom Toolbar: This toolbar contains function tabs that allow you to execute commands quickly. The tabs allow you to access the following submenus: Login, Event Log, Sensors, IPMI Device, BMC Setting, Users, Text Console, KVM Console.

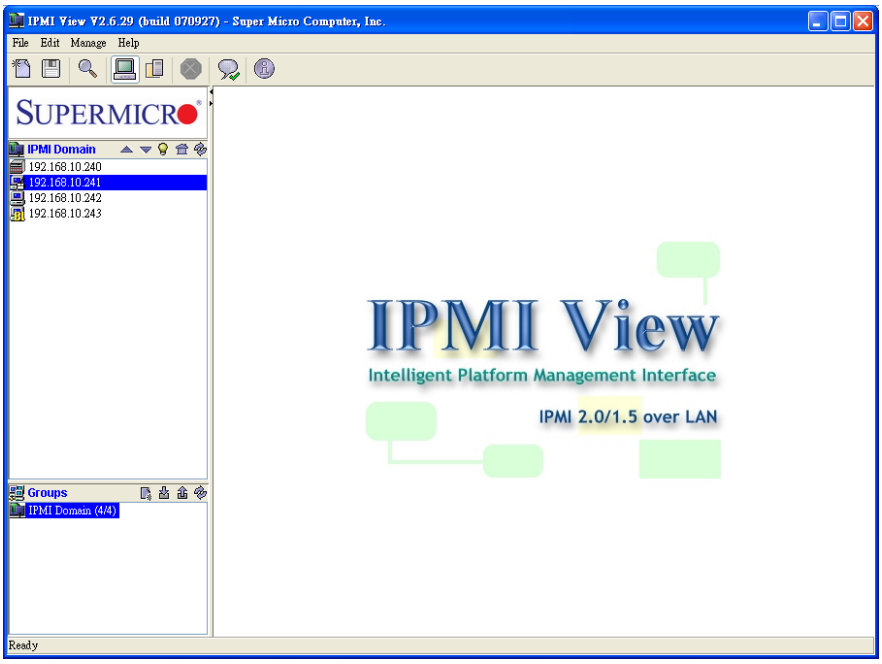


Figure 2-2

- **ToolBar (Top)**

The toolbar provides you with direct access to the features that are used frequently (as shown in Figure 2-3). You are able to switch between server- and group- management. The following toolbar shows the items that are currently available for user configuration under the BMC management.

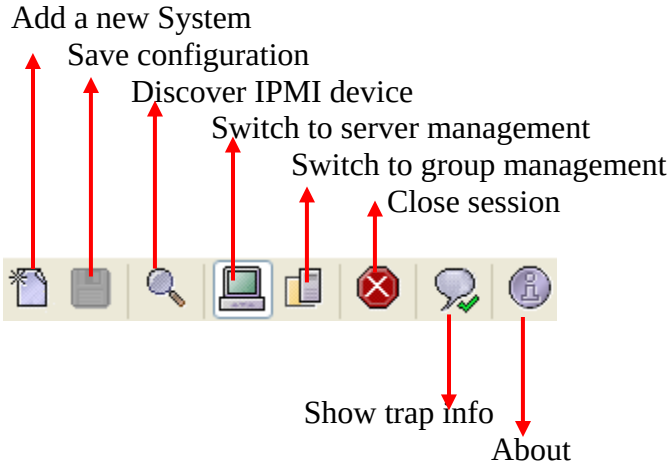


Figure 2-3

- **Adding a new system**

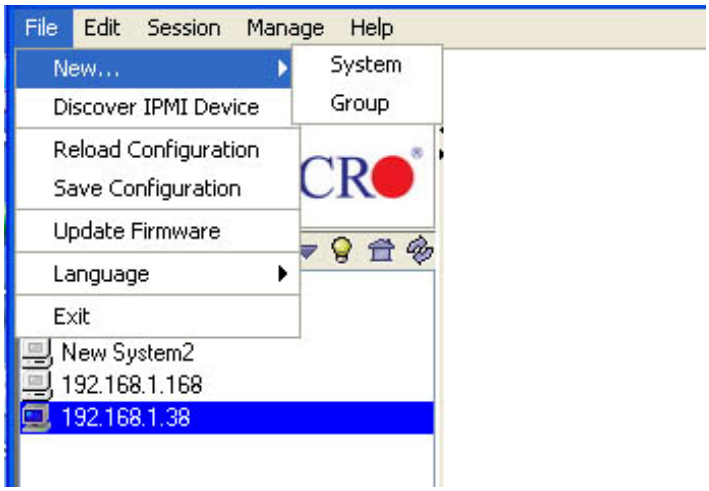


Figure 2-4

Click <File>"New>System" to add a new system to the IPMI connection (as shown in Figure 2-4). An "Add a new system…" dialog box will display as shown in Figure 2-5.

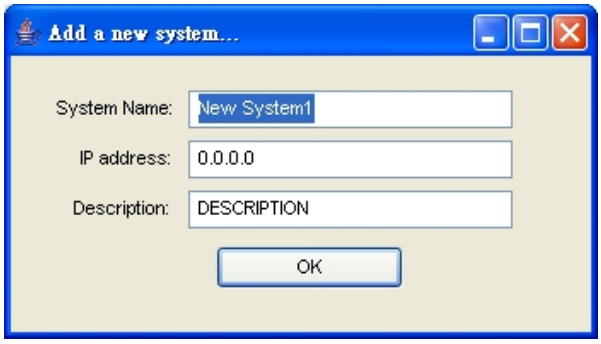


Figure 2-5

In the "Add a new system" dialog box, enter the System Name for the system to be managed by the BMC, its IP address, and its description. Then click <OK>.

- **Adding a new group**

For better system management, the manager may group systems in different groups. A system may be included in multiple groups. The default group is the "IPMI Domain." All systems under the BMC management belong to the IPMI Domain even if they are also grouped into other groups.

Click the menu: <File>"New…>Group" to add a new group to the IPMI connection.
An "Add a new group" dialog box will display as shown in Figure 2-6.

Figure 2-6

In the “Add a new group” dialog box, enter the Group Name and its description. Then click <OK.>

- **Discover IPMI Device**

  IPMIView offers a feature that will detect all devices or systems currently connected to the network. The user may specify a Network IP address range, and the network Mask, then click <Detect> or <Start> to search any IPMI devices or systems that are connected to the IPMI 1.5 or IPMI 2.0 connections as shown in Figure 2-7. Click <Exit> to discontinue this process.

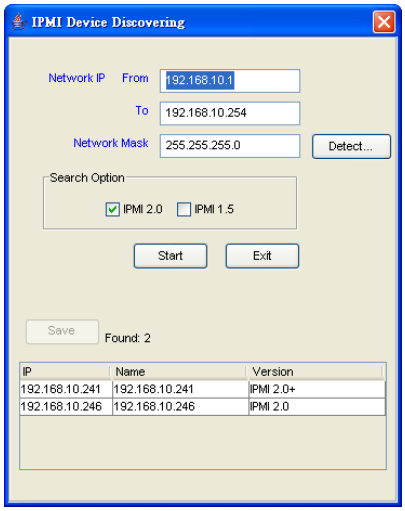


Figure 2-7

- **Reload Configuration**

  From the pull-down menu, click <File>”Reload Configuration” to load the configuration settings that were previously saved.

- **Save Configuration**

  From the pull-down menu, click <File> “Save Configuration” to save the current configuration settings.

- **Update Firmware**

  From the pull-down menu, click <File> “Update Firmware,” and select the system you wish to update from the IPMI Domain list on the left side of the window. A Confirmation dialogue box will appear. Click <OK> to update the IPMI Firmware. Click <Cancel> to discontinue this process.
  From the pull-down menu, click “File>Save Configuration” to save the current IPMIView configuration settings.

- **Language**

  From the pull-down menu, click <File> “Language” to activate a Language submenu. From the submenu, you can select Chinese (Taiwan), Chinese (China) or English (USA) as your IPMI language setting.

- **Exit**

  From the pull-down menu, click <File> “Exit” or press <Alt-F4> to exit IPMIView.

- **Modify System**

  Select a system in the System Window you want to modify and click <Edit> “Modify System” to modify it from the pull-down menu as shown in Figure 2-8.

  You can also right click on a system in the System Window and select “Modify” in the pop-up menu to modify it.

- **Modify Group**

  Select a group in the Group Window you want to modify and click “Edit>Modify…>Group” from the pull-down menu shown in Figure 2-8 to modify it.

  You can also right click a group in the Group Window and select ”Modify” in the pop-up menu to modify it.

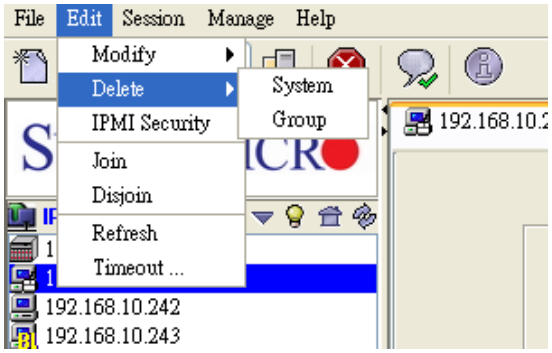


Figure 2-8

- **Delete System**

  Select a system in the System Window you want to delete and click <Edit> ”Delete System” from the pull-down menu as shown in Figure 2-8 to delete it.

  You can also right click on a system in the System Window, and select “Delete” in the pop-up menu to delete it.

- **Delete Group**

  Select a group in the System Window you want to delete and click <Edit> ”Delete Group” from the pull-down menu to delete it as shown in Figure 2-8.

  You can also right click a group in the System Window, and select “Delete” in the pop-up menu to delete it.

- **IPMI Security**

  From the pull-down menu, click <Edit>”IPMI Security” to activate the IPMI Security dialogue box. Check Auto Detection for IPMIView to automatically check the current IPMI status. Check the Advanced User box to select the following protocols as shown in Figure 2-9.

  - Hardware: BMCB, Firmware:IPMI 1.5:
  - Hardware: BMC2, Firmware:IPMI 2.0 (non-RMCP+):
  - Hardware: BMC2, Firmware:IPMI 2.0 (Standard RMCP+).

  Check the Encryption box to use encryption supported by the IPMI 2.0 Standard RMCP+. All packets transmitted from IPMIView to the BMC system management will be encrypted.

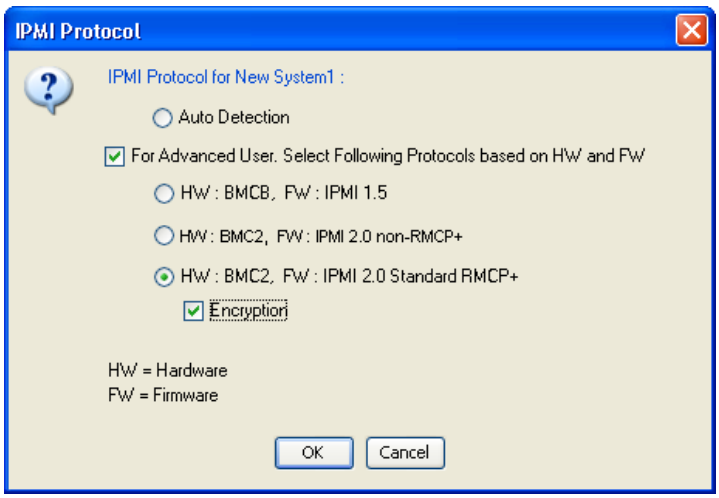


Figure 2-9

- **Join a group**

  Select a group in the Group window, a system in the System Window, and click <Edit “Join” from the pull-down menu to include (to join) this system into the group as shown in Figure 2-8.

- **Disjoin a System or a Group**

  Double click the group from which you want to disjoin a system. The systems that are included in the group will appear in the System Window. Then, select the system you want to disjoin from the group, and click <Edit> “Disjoin” from the pull-down menu shown in Figure 2-8. You can also select a group from the Groups list and click <Edit> “Disjoin” to remove it from the IPMI groups.

You can also right click the selected system, and select “Disjoin” in the pop-up menu to remove it from the group.

- **Refresh**

  Double click the group from which you want to disjoin a system. The systems that are included in the group will appear in the System Window. Select the system you want to refresh, and click <Edit> “Refresh” from the pull-down menu to refresh the system as shown in Figure 2-8.

- **Timeout**

  The timeout setting is shown in Figure 2-10. Timeout is the period for IPMIView to wait for a response after sending a command to a managed system. If a response is not received from the managed system in the timeout period, IPMIView will resend the command to managed system again. You may specify the timeout value (in seconds) to get a quicker response from the managed system. You can also specify the number of times that IPMIView will resend the command.

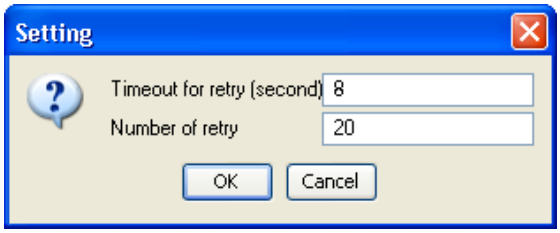


Figure 2-10

- **Section**

  IPMIView will display the IP address(es) currently connected to the network when you click <Section> from the toolbar. You can disconnect the IPMI connection from a system currently connected to the network by clicking “Closing. (the IP Address) “.

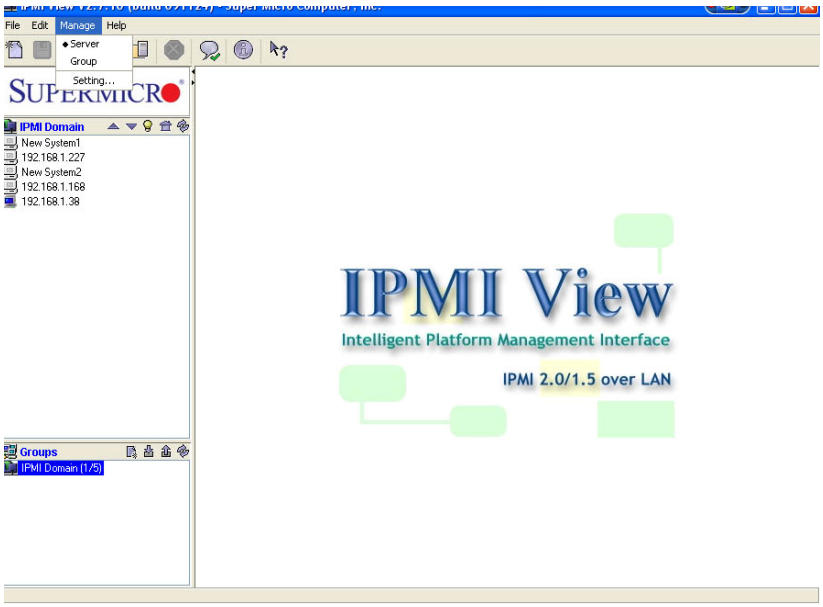


Figure 2-11

- **IPMIView Management**

  IPMIView allows you to manage your server or your network group by selecting <Manage> "Server/Group" from the pull-down menu as shown in Figure 2-11.

  In addition, you can also configure Group Login Settings by selecting "Setting" from a pull-down menu under the <Manage> tab. A dialog box will appear, prompting you for the Login ID and Password. Once enter the values in these fields, click <OK> to access the page and configure the settings. Please note that this feature is available for the system administrator only.

- **Help**

  Select <About> to display the information on the systems connected to the network.

3. Login

- **Login**

Click the <Login> tab on the bottom toolbar as shown in Figure 3-1. A login screen along with some information about the managed system will appear in the Viewing Window. Enter the login ID and password, and click the <Login> button to log in. When login is successful, the connection information will be shown at the bottom. The Login button is grayed (disabled), and the Logout button as well as other available management functions will be enabled. as shown in Figure 3-2.

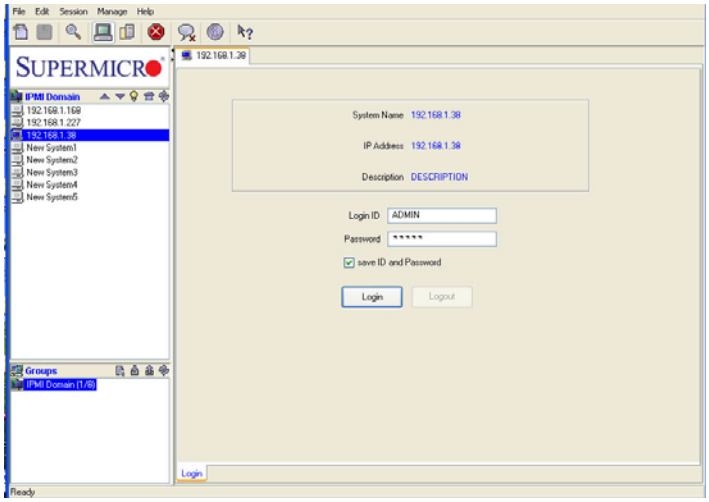


Figure 3-1

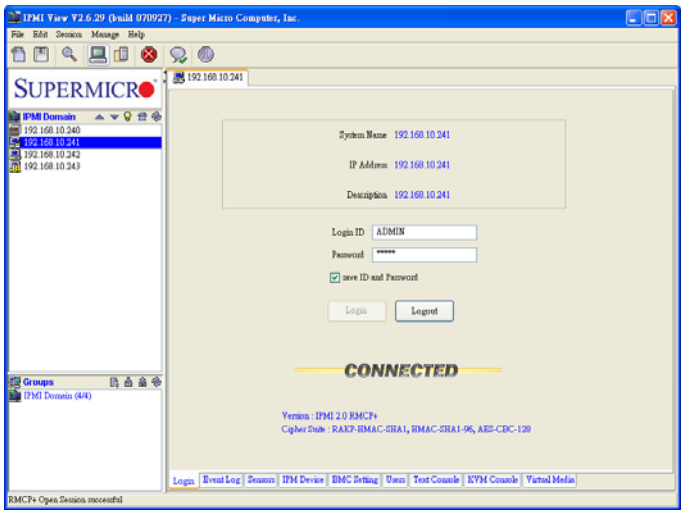


Figure 3-2

The default Login ID and password are “ADMIN”. Both are case-sensitive.

In IPMIView, an MD5 algorithm will encrypt the password when it is transmitted through the network. (If you are connecting to the IPMI 2.0 RMCP+, all the data will be transmitted by an encrypted algorithm.) Once the password is confirmed, IPMIView will show a CONNECTED symbol, and all available function pages will be shown as in Figure 3-2. If the password is invalid, a message will be displayed in the Status Area that reads, “Unable to activate a session, please check ID and Password.” and a Break symbol will be shown (see Figure 3-3).

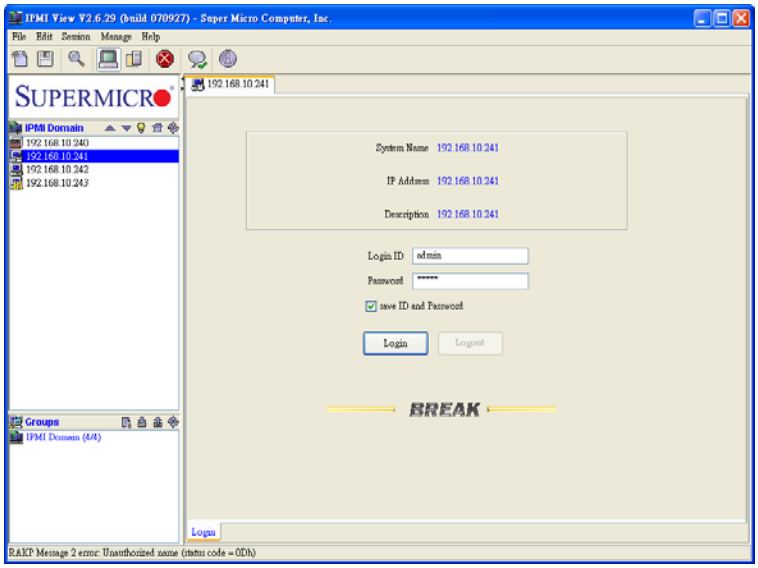


Figure 3-3

In order to reduce overhead on the managed system, all pages will not be refreshed automatically. The user must refresh the pages manually as needed.

After logging in, the IPMIView main window will display as shown in Figure 3-2. A tool bar will display on the bottom of the screen for your convenience.

- **Bottom ToolBar**

  As shown in Figure 2-4 below, this toolbar contains function tabs to allow you to execute commands quickly. The tabs allow you to access the following submenus: Login, Event Log, Sensors, IPMI Device, BMC Setting, Users, Text Console, KVM Console.

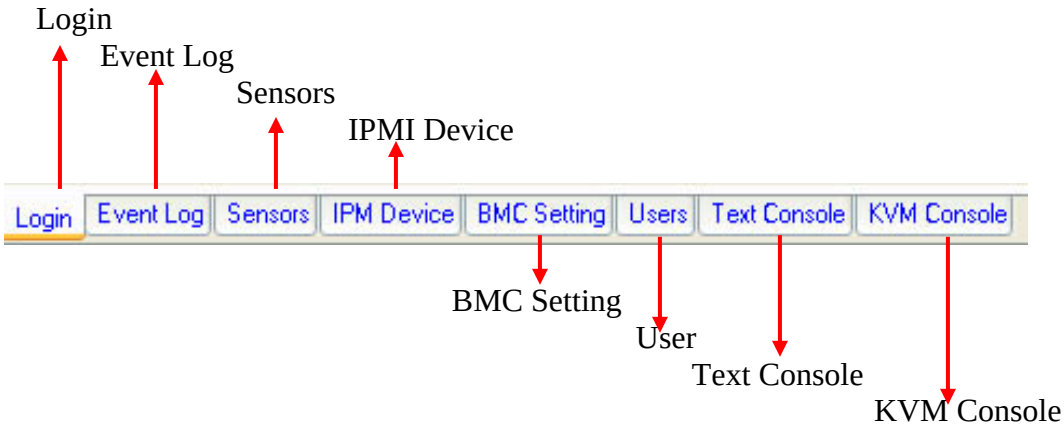


Figure 3-4

4. Event Log

After you have logged into a system, the screen as shown in Figure 4-1 will display. Click the <Event Log> tab on the bottom toolbar to activate the Event Log screen as shown in Figure 4-2.

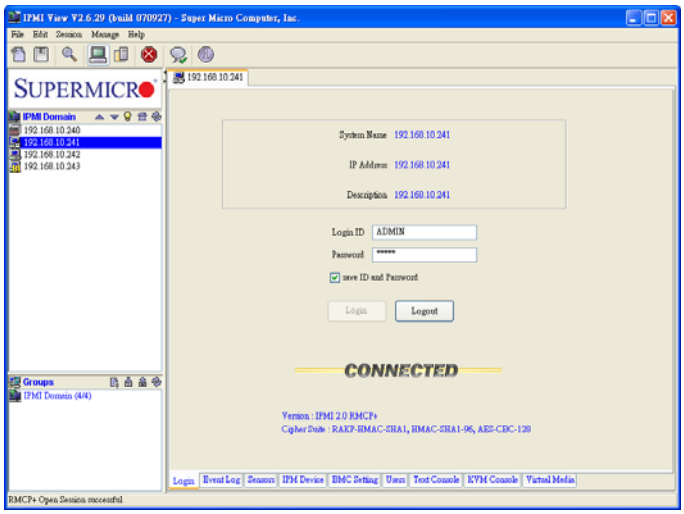


Figure 4-1

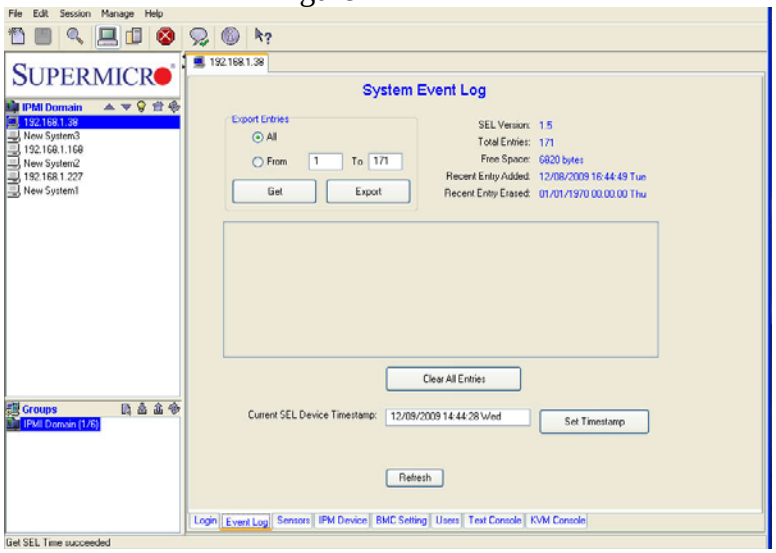


Figure 4-2

- **System Event Log**
  - **All**: Click this radio button to select all events.
  - **From…to**: Click this radio box to select a portion of events.
  - **Get**: Click this tab to get the event logs.
  - **Export**: Click this tab to export event logs to a file.
  - **Clear All Entries**: Click this tab to clear all event log entries.
  - **Current SEL Device Timestamp**: This item displays the timestamp of the current SEL device.
  - **Set Timestamp**: Click this tab to set the timestamp for the system selected.
  - **Refresh**: Click this tab to refresh this page.

5. Sensors

This feature displays the status of each sensor used to monitor system health as shown on Figure 5-1.

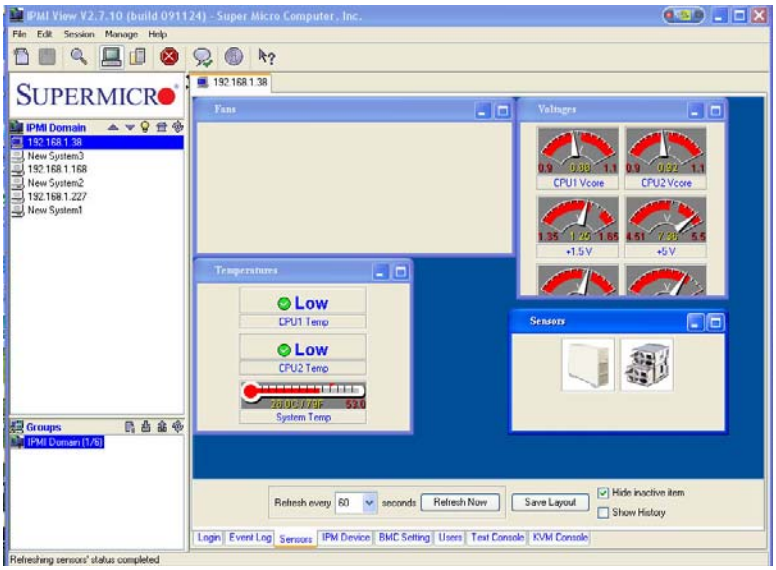


Figure 5-1

- **Fans**: This window displays fan status.
- **Voltages**: This window displays voltage readings for various devices.
- **Temperatures**: This window displays temperature readings for various devices.
- **Sensors**: This window displays the devices being monitored.
- **Refresh Every X seconds**: Enter the number of seconds for the system to refresh.
- **Refresh Now**: Click this tab to refresh the Sensors page immediately.
- **Save Layout**: Click this tab to save the current layout setting.
- **Hide inactive item**: Check this box to hide inactive items.
- **Show History**: Check this box to display the sensor records.

6. IPM Devices

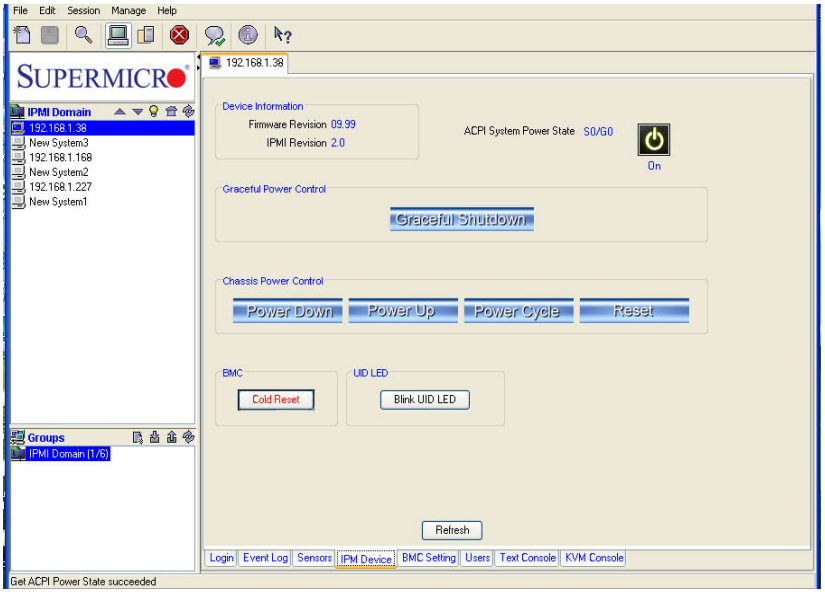


Figure 6-1

Click the IPM Device tab of the IPMIView management session in the Viewing Window (shown in Figure 6-1) to display the information and functionality of the BMC firmware installed in the system.

- **Device Information**

  This shows the revision levels of the BMC and IPMI firmware.

- **ACPI System Power State**

  This shows the power state of the managed system. If the managed system is in a power-off state, the green light will be off. It will be updated automatically every five seconds.

- **Graceful Power Control (Administrator and Operator only)**

  Graceful power control will inform the OS running on the managed system to shutdown, reboot and reset the power-cycle within a specified time. (The default setting is 30 seconds). When the OS running on the managed system receives a graceful power control request, it will generate a pop-up window on the monitor of the managed system, and start to count-down. This pop-up notice window will give the user working on the system an opportunity to save any working files. However, remote login users or service users (e.g. Web site visitors) will not see this notice.

  Graceful Shutdown: This feature has the same function as “shutdown” in the Windows. Using this feature will cause the managed system to enter the S5 state.

  Power On Icon: Click on the Power-On Icon to power on or power off the device.

- **Chassis Power Control (Available for the Administrator and Operator only)**

  This feature is used to manually control the power state of the chassis of a managed system. When the BMC receives the power control command from the chassis, it will have direct control over the power button or the reset button of a system.

  Power Down: This feature will power off a managed system as it would when the Power-Down button of the chassis is pressed.

  Power Up: This feature will turn on the power of a managed system as it would when the Power-Up button of the chassis is pressed.

  Power Cycle: This feature will turn off the power of a managed system for a few seconds and then turn on the power of the system again.

  Reset: This feature resets a managed system as it would when the Reset button of the chassis is pressed.

- **BMC Cold Reset (for the Administrator only)**

  Clicking the Cold Reset button allows you to reset the BMC. After confirming the reset of the BMC, the session will be terminated immediately. The user has to close this session manually. This feature is rarely used. It is only used for an event when you suspect a system malfunction for example.

- **UID (Unit Identifier) LED**

  Blink UID LED: Click this table for the UID LED to blink when the unit in question is identified.

- **Refresh**

  Click this tab to refresh this page.

7. BMC Settings (Available for the Administrator only)

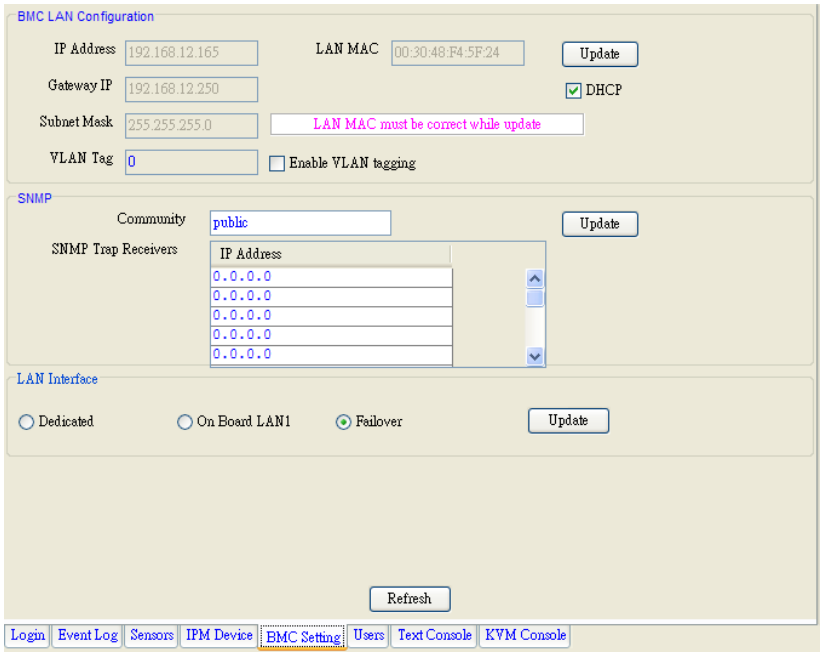


Figure 7-1

Click the BMC Setting tab of the IPMIView management session in the Viewing Window (as shown in Figure 7-1) to display detailed information on the BMC LAN Configuration, SNMP trap configuration and the serial port status.

- **BMC LAN Configuration**

  This feature displays the IP address, the LAN MAC, the Gateway IP, the Gateway MAC and the Subnet Mask of the BMC and allows you to modify these settings. NOTE: please make sure that the MAC address of the LAN and the gateway for the BMC are correct before updating it by clicking the <Update> button. Be careful to enter the correct values especially for the LAN MAC. If you enter the wrong LAN MAC, IPMIView will not be able to connect to that system any more.

  If you accidentally enter a wrong LAN MAC value, you may use the IPnMAC.exe command in the IPMI Solution/Utility subfolder on this CD to update it. To activate IPnMAC.exe.,which is a DOS command, you must first boot your managed system to DOS, and then execute IPnMAC.exe on the managed system. You can also enable the VLAN (Virtual LAN) Tag setting by clicking on the “Enable VLAN Tagging” box on the right and enter the value on the VLAN Tag field to configure VLAN Tag setting.

- **SNMP**

  This displays the SNMP trap configuration of the system that needs to receive the SNMP traps generated by the BMC to allow you to modify the settings. To change the configuration on the BMC, enter the SNMP community name in the Community text field, and enter the IP address as well as the MAC address in the SNMP Trap Receivers table in the SNMP group. Then, click the <Update> button.

The SNMP Trap may have multiple destinations. When any critical error occurs, an SNMP trap packet will be sent to all receivers in the list. To remove an SNMP receiver, you may change both IP and MAC addresses to 0.0.0.0 and 00:00:00:00:00:00 respectively. Then, click <Update>.

For a system to receive the SNMP traps, you must install and run an SNMP trap receiver program. The managed system will send out an SNMP trap packet to all receivers when an event occurs. If an SNMP trap receiver is not running, the trap packet is discarded, and cannot be queued anywhere.

- **RS232 / MODEM (available for IPMI 1.5 only)**

  This displays the configuration of the RS232 interface on the BMC. It is used to initialize the RS232 port and the installed modem, if any. The RS232 port is the box-header (Figure 7-2) on the BMC, and a dedicated serial port.

  Baud Rate: It is the baud rate for serial connections, which will not affect paging settings.

  Modem Init String: This is the modem initialization string for serial link connections, which will not affect paging settings.

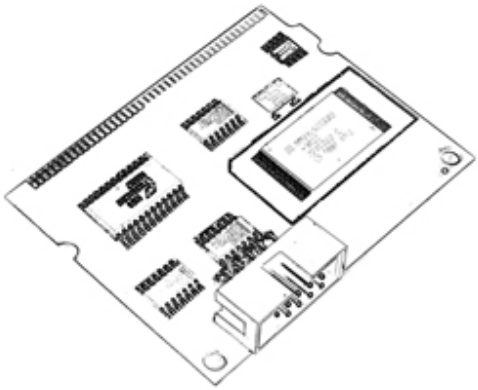


Figure 7-2

- **LAN Interface**

  - **Dedicated**: Click this radio box to use the IPMI-Dedicated LAN as the default LAN connection.
  - **Onboard LAN1**: Click this radio box to use the onboard LAN port 1 as the default LAN connection.

  - **Failover**: Click this radio box to enable Failover support.

  - **Update**: Click this tab to update LAN connection status.

  - **Refresh**: Click this tab to refresh the page.

8. Users

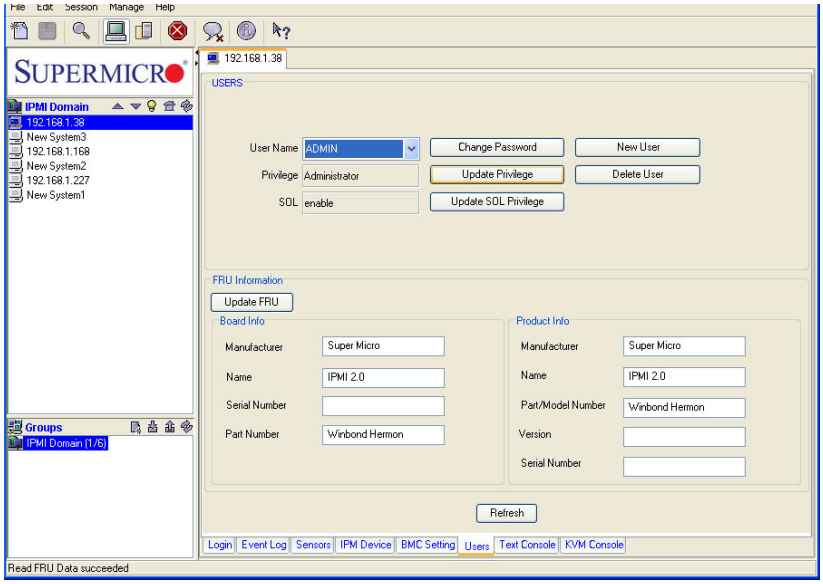


Figure 8-1 (For IPMI 2.0)

Figure 8-2 (For IPMI 1.5)

Click the Users tab of the IPMIView management session in the Viewing Window (as shown in Figure 8-1 and 8-2) to display detailed information on the Users management, and paging severity thresholds for IPMI 1.5.

We strongly recommend that you change the password immediately for security reasons.

- **USERS**

User Name

IPMIView allows you to add or delete a user, to change a user's password, to set and update user privilege settings by clicking the appropriate tabs.

Privilege

This feature allows you to set and update privilege level for a user or delete a user from the list. There are six privilege levels, Callback, User, Operator, Administrator, OEM, and No Access. Only the first four privileges are supported. Privilege Levels determine which IPMI commands a user can execute over a channel. Privilege Limits set the maximum privilege level that a user is allowed to operate at. A user is granted certain privileges for each channel, and the user can operate at a privilege level that is granted. Click the "Update Privilege" to change the privilege level setting for a user.

Group Privilege Levels

Callback	This may be the lowest privilege level. Only those commands that are used to initiate a Callback are allowed. (Available for IPMI 1.5 only.)
User	Only the basic commands are allowed. These commands are used to read and retrieve data, to modify BMC configuration settings, or to write data to the BMC or other controllers. Actions such as resets, power on/off, and watchdog activation are not allowed.
Operator	All BMC commands are allowed, except for commands that can modify out-of-band interface settings. For example, the Operator is not allowed to disable individual channels or change a user's access privileges.
Administrator	All BMC commands are allowed, including modifying commands. An Administrator is allowed to execute configuration commands that disables the channel over which the Administrator is communicating.

SOL (Serial-Over-LAN)

This feature allows the user to configure SOL settings. Click "Enable" to enable SOL support. Click "Update SOL Privilege" to update a user's SOL privilege level.

Click Paging Setting to set the parameters for an individual user (Figure 8-3). There are two types of paging services: Numeric paging and alphanumeric paging. To use a paging service, a modem must be connected to the RS232 connector on the BMC (Figure 7-2).

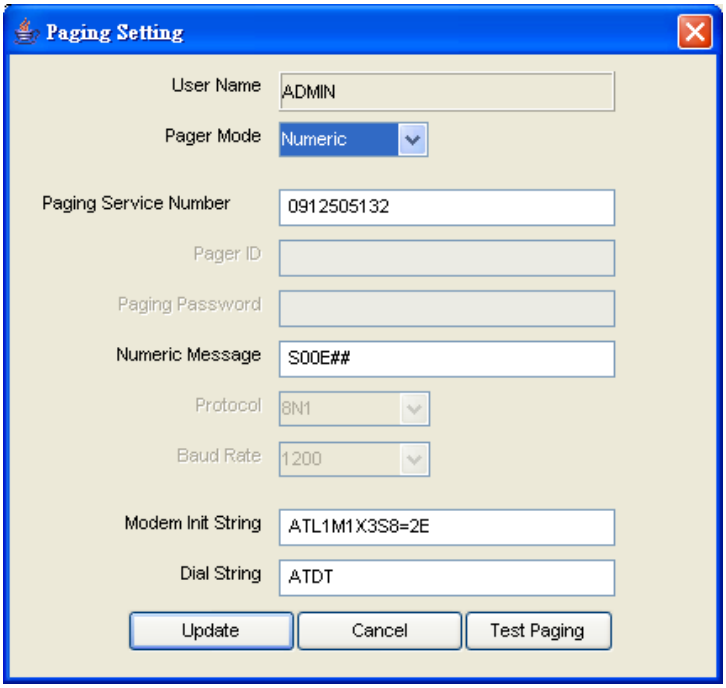


Figure 8-3

- **FRU (for IPMI 2.0 only)**

  This provides useful information on the board and the product, including the serial number, part number, and the components of the motherboard. Click the "Update FRU" tab to update board information and product information, including information on the manufacturer, the name of firmware, the serial number/ the part number of the motherboard, and the part/model number of the BMC firmware, the version and the serial of the IPMI/BMC firmware.

- **PAGING/SEVERITY (for IPMI 1.5 only)**

  Use paging severity settings to determine when a user will be notified of an entry of the system event log (SEL).

  The following settings are available for each group:

None	When this setting is selected, user notification for this group is disabled.
Warning	When this setting is selected, the RMC will notify the user when SEL entries for the group exceed the warning thresholds.
Critical	When this setting is selected, the RMC will notify the user when SEL entries for the group exceed the critical thresholds.
All	When this is selected, the RMC will notify the user of all entries of the SEL events for the group.

  All warning and critical thresholds are predefined by Supermicro based on hardware design.

9. Text Console Redirection (SOL- Serial-Over-LAN)

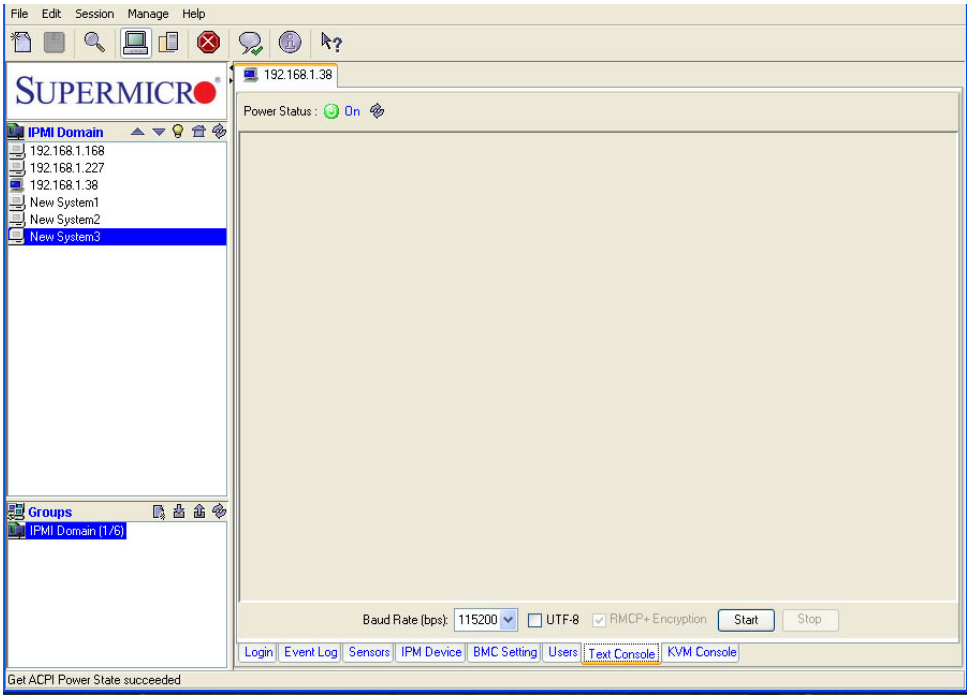


Figure 9-1

Click the <Text Console> tab on the bottom tool box (shown in Figure 9-1) to enable Text Console Redirection support, which will allow you to control a remote system from a text mode console. Click the <Start> button to start the text console redirection. Click the <Stop> button to stop the text console.

- BMC for IPMI 1.5

  Console Redirection is not supported by the IPMI specification V1.5. Supermicro provides this useful feature for a manager to control the managed system from a remote location. When a managed system is booting up during the POST routine, and no other software application are available for you so that you can gain control over console redirection, IPMIView provides you with this valuable feature. Console Redirection will redirect the monitor of a managed system for IPMIView use and allows you to send the key codes to the managed system.

  When a managed system changes its video mode from Text Mode to Graphics Mode, a termination notice will be sent to IPMIView to terminate the console redirection. Text Console Redirection only works with the text mode.

  Important Note: Console Redirection can cast a very heavy load on a managed system. It will redirect the whole monitor to the manager's system, and it will slow down the managed system significantly. We suggest that you use this function only when you absolutely need it. For other applications, a proper console redirection software application (pcAnywhere, Symantec Corporation) or a remote login protocol (telnet) is recommended. When you finish your remote operation, click <Stop> to terminate console redirection to take the load off the managed system.

- BMC for IPMI 2.0

Serial-Over-LAN (SOL) was designed to support Text Console Redirection based on the IPMI specification V2.0. This function performs better in IPMI 2.0 than in IPMI 1.5. The Text mode console is supported by the Windows 2003, even when the OS is running. To support Text Console Redirection on the Windows 2003, Special Administration Console (SAC) must be enabled. The following instructions are used to enable the SAC:

1. Enable Console Redirection in the BIOS, and set it to COM 2 (or COM B)
2. Modify boot.ini in C:\. Boot.ini is a hidden file. An example of boot.ini is listed below.

```
[boot loader]
redirect=com2
redirectbaudrate=19200
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /fastdetect
/redirect
```

To enable Text Console Redirection support on a Linux Platform:

1. Host A with the IPMI BMC installed (for the Linux Platform):

a) BIOS POST:

(i) Enable "Console Redirection" in BIOS Setup.
For example, COM2 / 19.2Kbps / 8N1

(ii) Disable "Enable Console Redirection after POST" in the BIOS setup.

b) Boot Loader:

(i) For GRUB,
add the following TWO lines into /boot/grub/grub.conf, but
comment out "splashimage=(hd0,0)/grub/splash.xpm.gz"
serial --unit=1 --speed=19200 --word=8 --parity=no --stop=1
terminal --timeout=10 serial console
#splashimage=(hd0,0)/grub/splash.xpm.gz

(ii) Then add "serial console=ttyS1,19200n8" to the end of kernel /vmlinuz in /boot/grub/grub.conf.

For example:
kernel /vmlinuz-2.6.5-1.358smp ro root=LABEL=/ rhgb quiet serial console=ttyS1,19200n8

This will result in all boot messages being output to the console ttyS1, but you will not see All these boot messages on the local console until the login message prompts.

c) LINUX OS:

(i) Add the following line into /etc/inittab.
s0:2345:respawn:/sbin/agetty ttyS1 19200

(ii) Edit /etc/securetty and add ttyS1

2. Host B with IPMIView installed:

a) Install and run IPMIView.
b) Log in Host A with the IPMI BMC installed as Admin.
c) Start Console Redirection in IPMIView immediately after the Host A reboots.

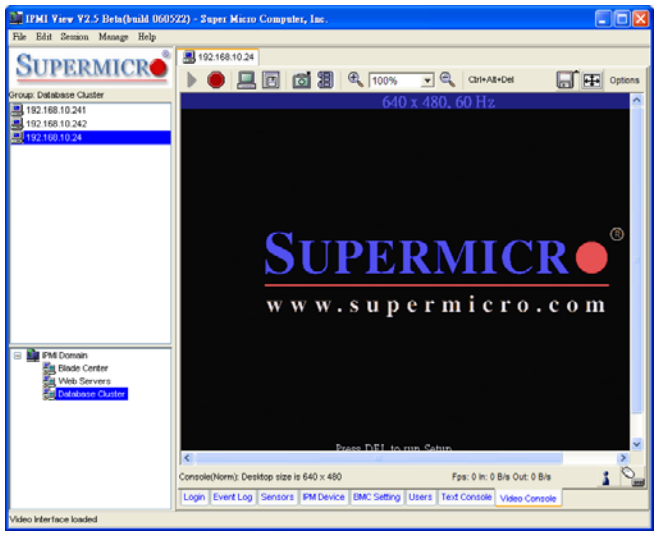
You will see the BIOS POST, the boot loader, and the Linux OS messages and prompts.

10. KVM Console (KVM-Over-IP for Video Redirection)

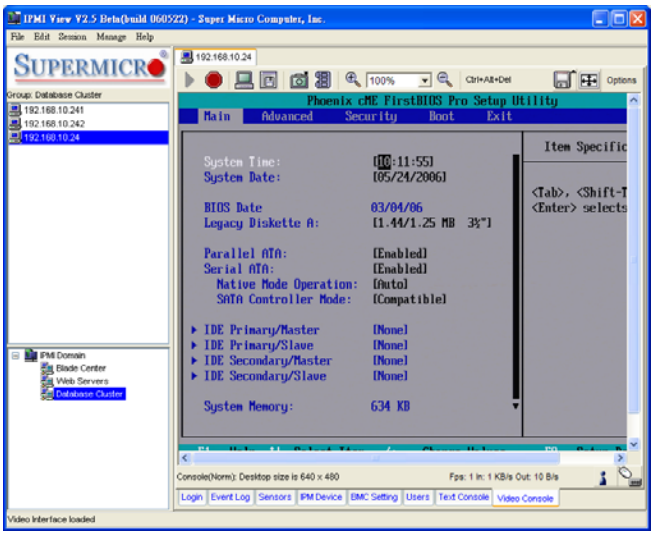
KVM Console Redirection is a new feature included in the Supermicro Intelligent Management (SIM) Module. If Video Console Redirection support is enabled, the remote screen will be redirected to IPMIView. BIOS POST, BIOS settings, DOS, Windows or Linux OS screens can all be redirected to IPMIView.

Click the <Launch KVM Console> tab to launch KVM console redirection.

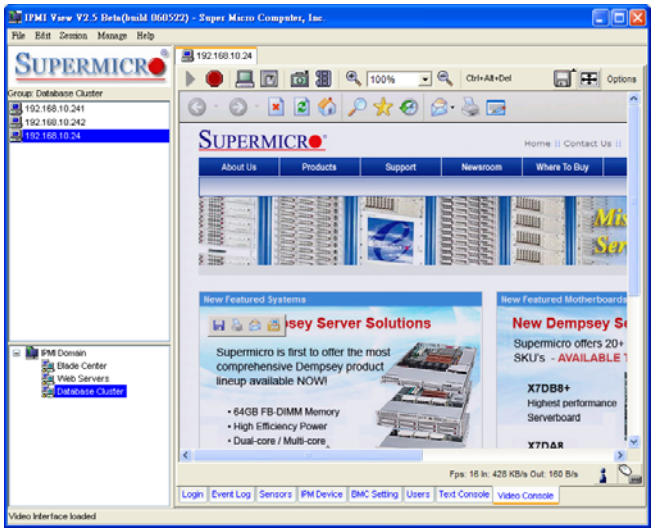
Figure 10-1 shows sample screenshots of Video Console redirection. The screen of a remote managed system will be redirected to IPMIView. You will see the screen of the remote system just as if you were sitting in front of the system.



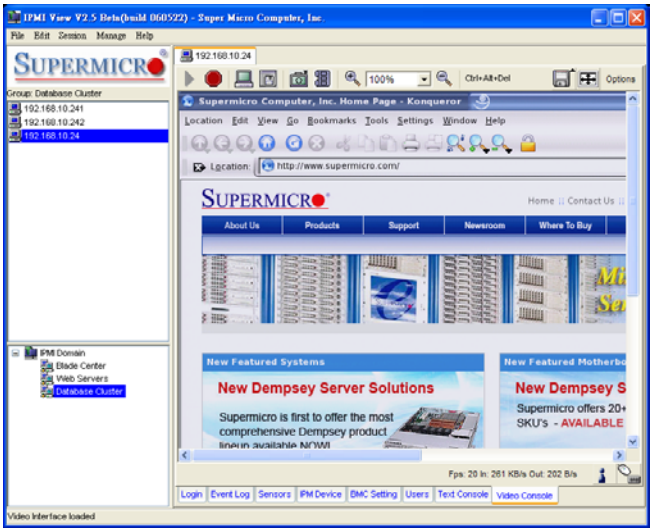
System Boot Up



BIOS Screen



Windows XP



Linux X Window

Figure 10-1

Toolbar

There are several tool buttons that can be used for video console as shown in Figure 10-2.

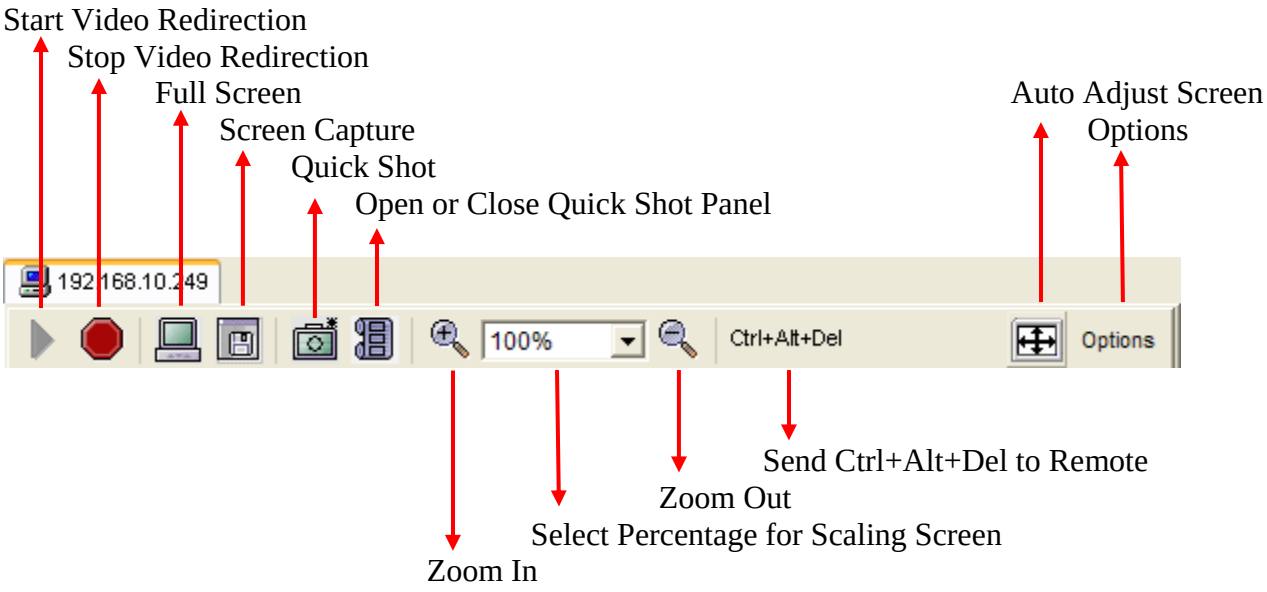


Figure 10-2 Video Console Toolbar

- Start Video Redirection

This button is used to start video redirection. IPMIView will automatically start the video redirection when you click the Video console tab.

- Stop Video Redirection

This button is used to stop video redirection. To stop video redirection, press this button again to stop it. Please note that the drive redirection will continue to work when it is enabled.

- Full Screen

This button is used to maximize the size of the remote video screen on the local computer display. You may press <alt + enter> to return back to the original mode. Please refer to Figure 10-3.

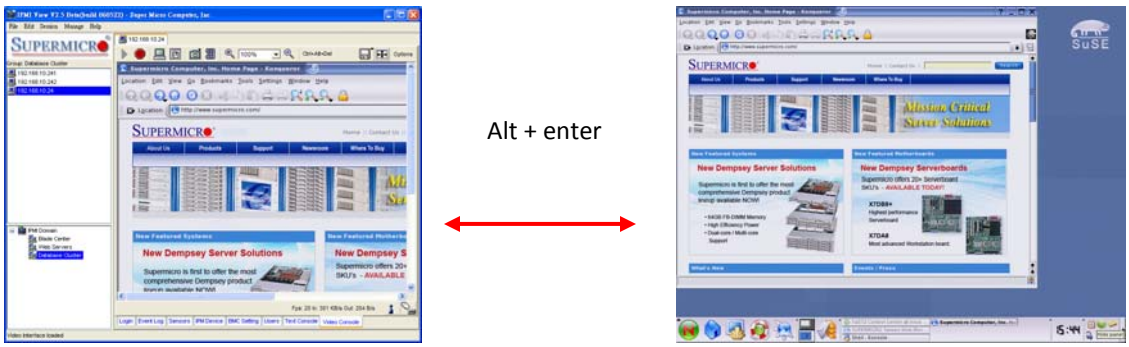


Figure 10-3

-  Screen Capture

This button is used to capture the screenshots of the remote managed systems. You will see a file-save dialog box with a preview image. Select the directory and filename to save it. The file format can be PNG or JPG.

-  Quick Shot

This button is used to capture quick screenshots. You will need to first specify a directory where you want to store quick shot images. You will see the quick shot images in the quick shot panel. Please refer to Figure 10-4.

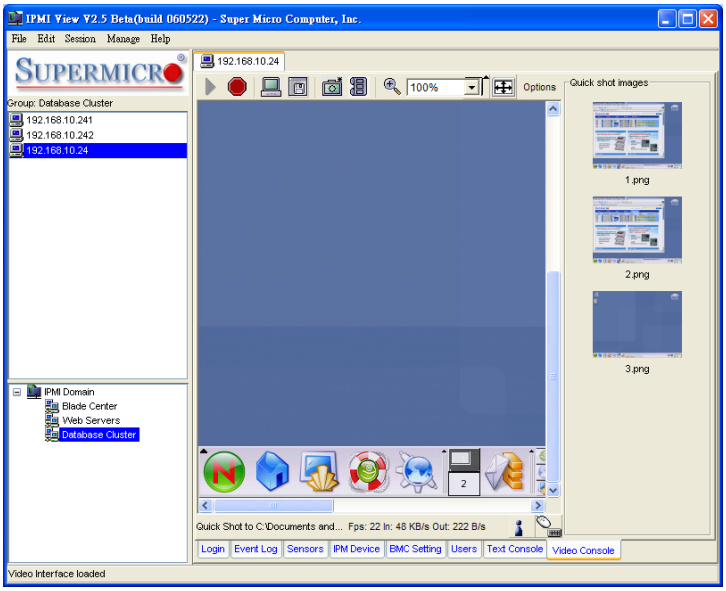


Figure 10-4 Quick Shot

-  Open or Close a Quick Shot Panel

This button is a switch used for opening or closing the quick shot panel. Double click the image in this panel to show a full-size window for viewing.

-  Zoom In

This button is used for zooming in the screen (up to 300%). Please refer to Figure 10-5.

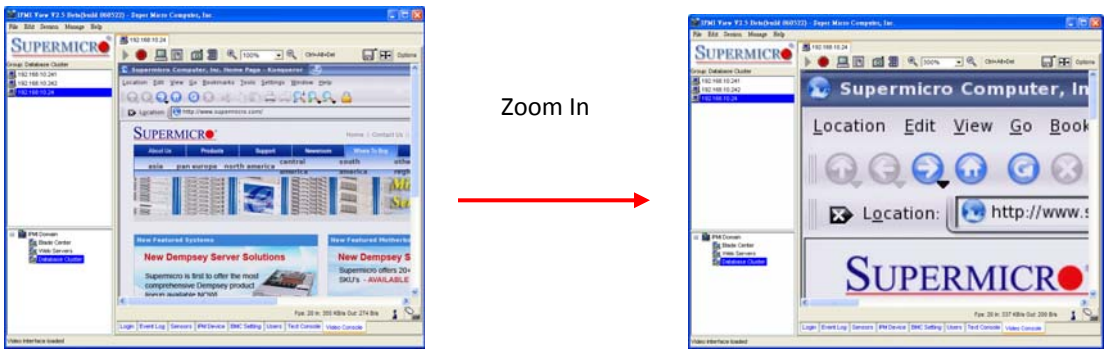


Figure 10-5

-  Zoom Out

This button is used for zooming out. The maximum zoom out percentage is 10%. Please refer to Figure 10-6.

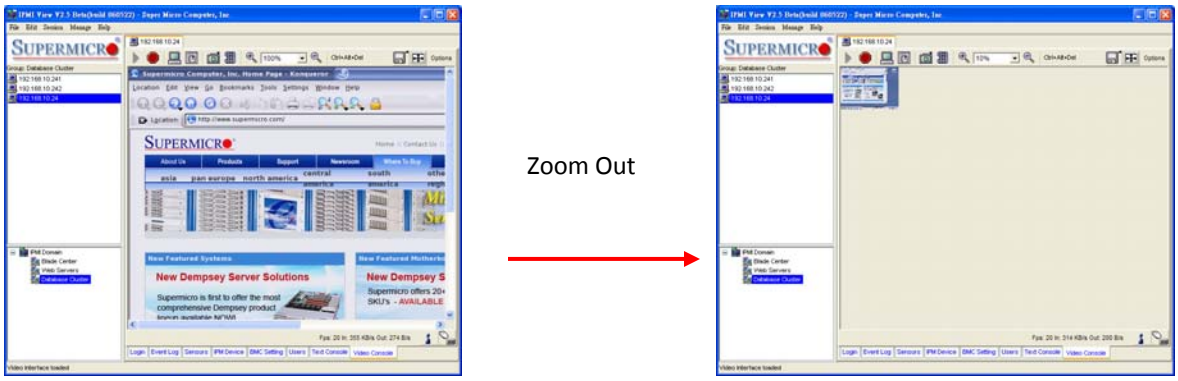
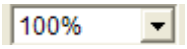
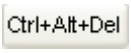


Figure 10-6

-  Select percentage for Scaling Screen

This combo box allows you to select the setting of screen scaling, either 10%, 25%, 50%, 75%, 100%, 200%, 250% or 300%. An additional selection allows you to scale to fit with the IPMIView window size.

-  Send Ctrl + Alt + Del to Remote

This button is used to send the <Ctrl + Alt + Del key >combination to the remote system. It is useful when the remote system is running in the BIOS, DOS or Windows environment.

-  Auto Adjust Screen

This button is used to adjust the screen automatically. Press this button if it's difficult for you to see the whole screen.

-  Options

You can select more options here. The list of options is listed below.

  - Monitor Only: Use this feature to display the remote screen only. The keyboard and mouse will be disabled.
  - Readability Filter: This item uses algorithm to improve screen display. This will allow you to see the text content easier when you scale the screen.
  - Local Cursor: Use this to change local cursor settings.
  - Chat Window: This feature allows the user to chat with each other via the IPMI connection. Please refer to Figure 10-7.

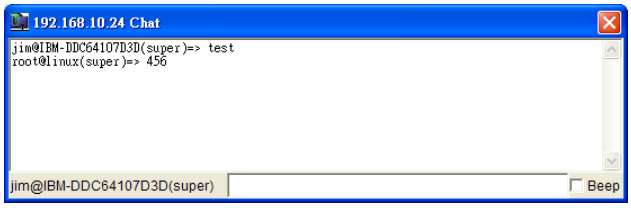


Figure 10-7 Chat Window

- Video Settings: This feature allows you to configure the advanced video settings. Please refer to Figure 10-8.

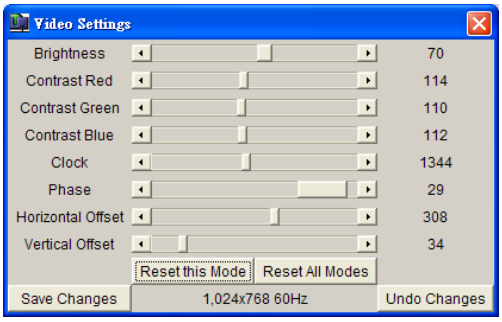


Figure 10-8 Video Settings

- Refresh Video: This feature allows you to refresh the video screen.
- Soft Keyboard: A virtual keyboard is provided for easy input. It also provides localized keyboard mapping. Please refer to Figure 10-9.

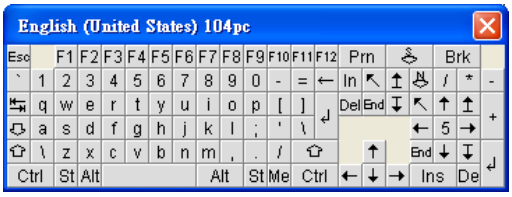


Figure 10-9 Soft Keyboard

- Local Keyboard: This feature allows you to set local keyboard mapping settings.
- Encoding: This feature supports encoding for the video screen. The options for encoding are "Predefined", "Compression" and "Color Depth".

Status Bar

Figure 10-10 displays the status bar for the video redirection.

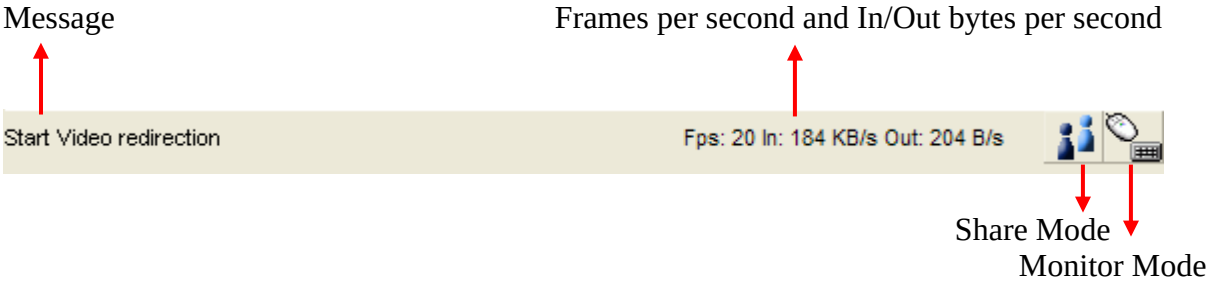
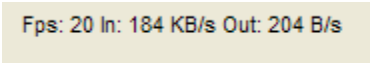


Figure 10-10

- 

Message

This section displays tool tip information and the video redirection status.

- 

This section indicates the number of the frames displayed per second, and Input (Kbytes per second)/ Output (bytes per second).

-  Share Mode

This icon indicates the status of screen-sharing on the remote system. If there is only one user using the video redirection of a remote system, the icon will look like  .If two or more users using the video redirection of the same remote system, the icon will look like  .

-  Monitor Mode

This icon displays the status of monitor mode. When the display looks like  , it indicates that you can use the local keyboard and the mouse to control the remote screen. When the display looks like  , it indicates that the local keyboard and the mouse are not available. If you select the option “monitor only”, the keyboard and mouse will be disabled.

11. Virtual Media

The Supermicro Intelligent Management (SIM) Module provides a Virtual Media feature, which includes a Virtual USB Floppy, a CD-ROM image and Drive Redirection.

Figure 11-1 shows the Virtual Media GUI. The Virtual Media Status section displays the current virtual device status. There are two virtual drives available.

Floppy Image Upload allows the user to upload a floppy image as "floppy" located at 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 SIM card and emulated to the host as a USB device.

The CD-ROM Image on the “Windows Share” allows the user to configure Windows-Share settings. It allows you to decide how you want to share the data stored in your shared folder with the users on the remote host system.

Drive Redirection makes local drives accessible to other users via console redirection. This function allows you to share your local drives (floppy, CD-ROM and HDDs) with users on remote systems.

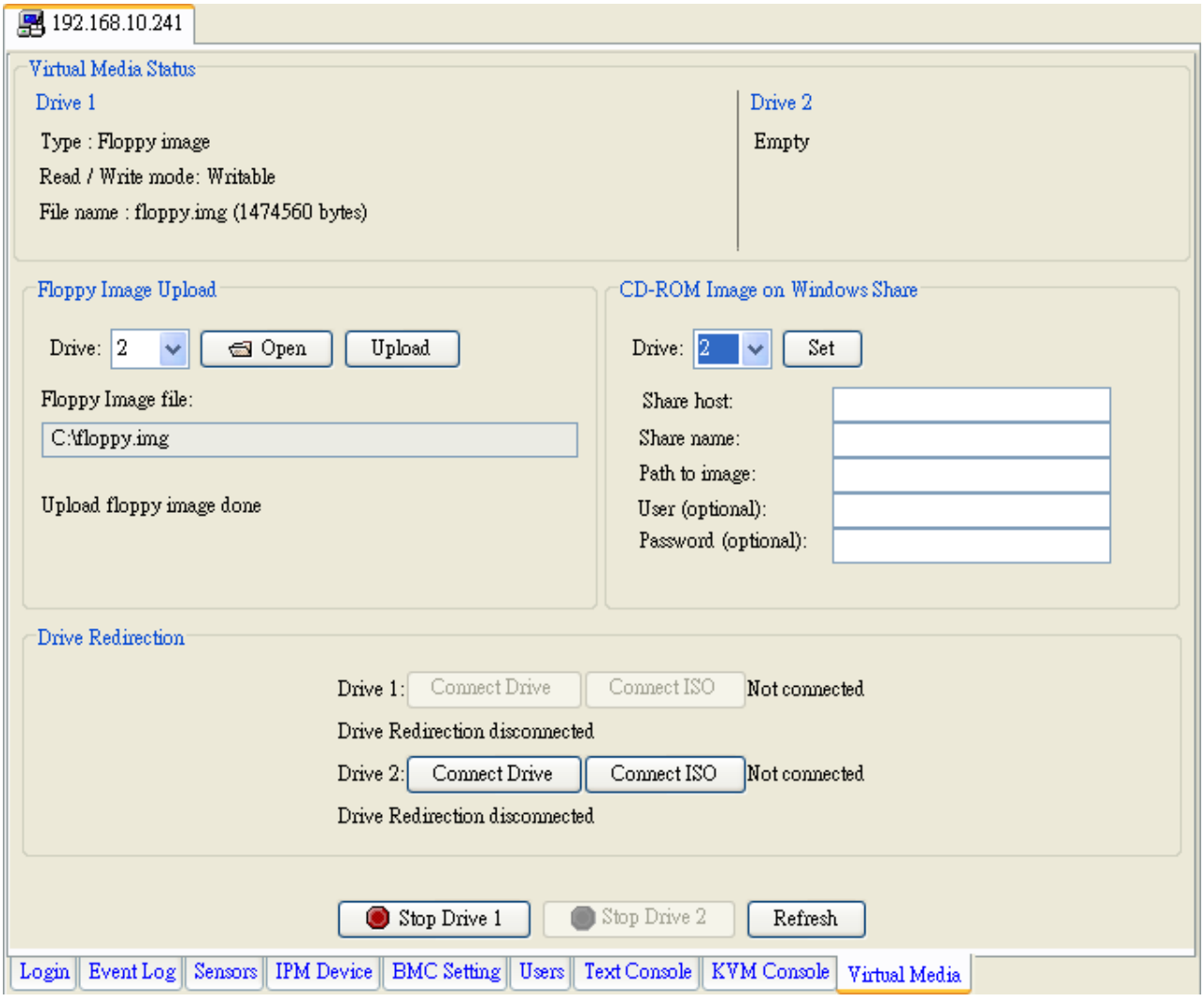


Figure 11-1

● Floppy Image Upload

As shown in Figure 11-2, click <Open File> to select the file that you wish to upload to a specific host drive of your choice. Click <Upload> to upload the floppy image. Please wait for the uploading process to complete. The virtual floppy will be activated after the floppy image is uploaded.

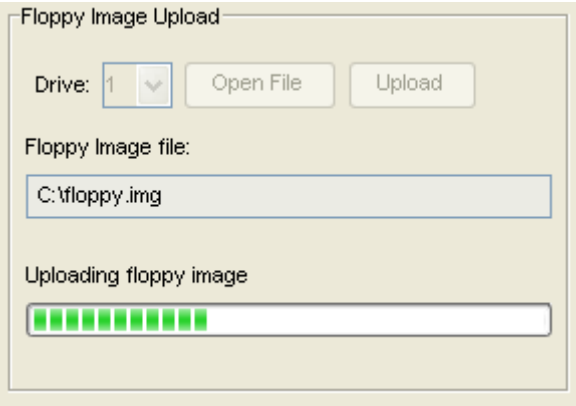


Figure 11-2

● CD-ROM Image on Windows Share

Please refer to Figure 11-3 for the following items.
Drive: Specify the drive that you want the remote host to share.
Share Host: Enter the IP Address or the name of the system you wish to share data with via “Windows Share”.
Share Name: Enter the name of the shared data in the remote host.
Path to Image: Enter the location of the source file that you wish to share via “Windows Share”.
User/Password (Optional): Enter the user and password for the person to access the data that you want to share, and click the <Set> button to enter your selections as shown in Figure 11-3.

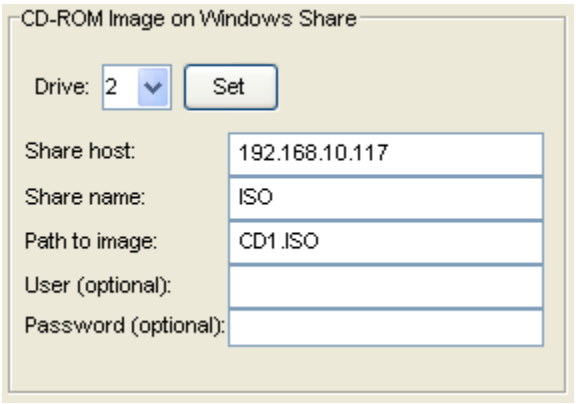


Figure 11-3

● Drive Redirection

As shown in Figure 11-4, Drive Redirection supports both local drive and the ISO file. When you click the <Connect Drive>, a dialog will show up as figure 11-5.

Local Drive List: This 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.

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

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. Select the drive and click "OK" to start direct redirection.

The second type of drive redirection is "Connect ISO". You may redirect the ISO file directly from your file system. Click this button and select an ISO file to start this function.

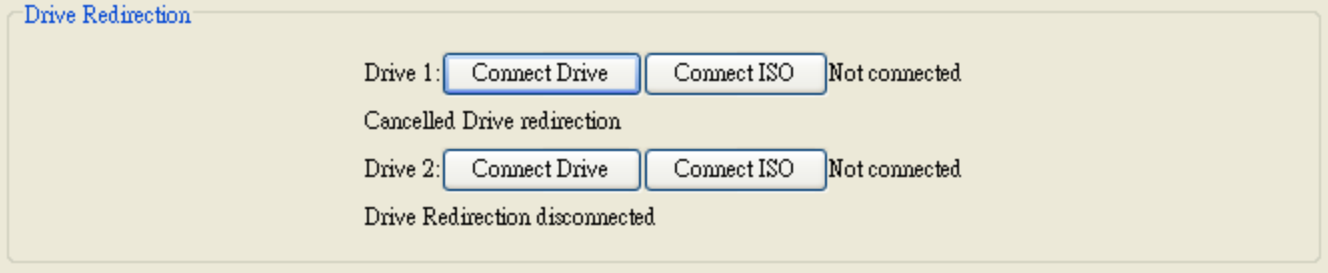


Figure 11-4

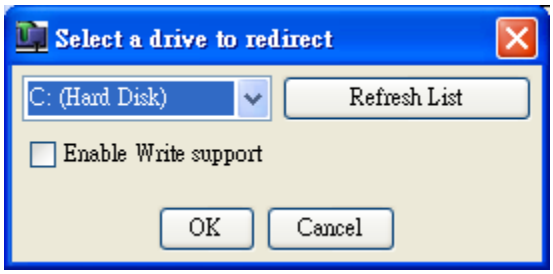


Figure 11-5

- **Stop Active Drives**

As shown in Figure 11-6, click <Stop Drive 1> to disable Drive 1 and Click "Stop Drive 2" to disable Drive 2. The <Refresh> button is used for refreshing the Virtual Media settings. If you want to stop or change the type of a virtual drive, you first need to stop it.

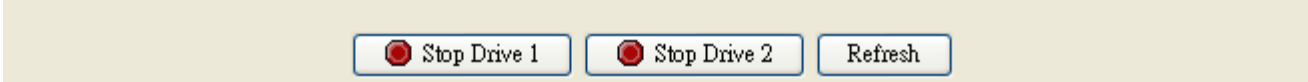


Figure 11-6

12. Group Management

Group management is a way to manage multiple servers at the same time. For example, you can query the fan sensor readings from multiple servers and note their differences. Also, you can simultaneously power on or off multiple servers at the same time. As shown in Figure 12-1, click <Manage Group> to show group management. In group management, you can select multiple servers from the host group on the left and manage them with the functions provided. You may re-arrange groups of servers in the group list to make server group management easier.

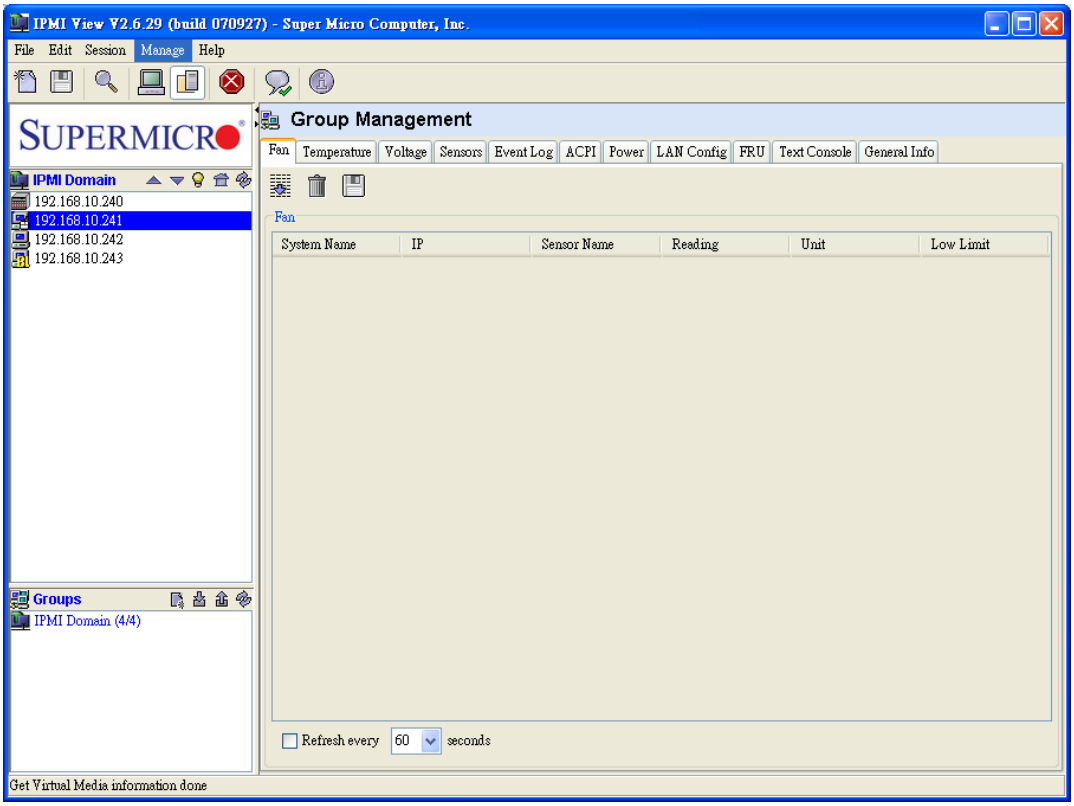


Figure 12-1

In the group management, a Login ID and password are required. Click <Manage > Setting to set the login information. Please note that IPMIView will use this account to login to multiple servers. (Figure 12-2)

Figure 12-2

IPMIView provides various tools for group management. As shown in Figure 12-3, group management can be grouped to the following categories.

- ✧ Fans
- ✧ Temperature
- ✧ Voltages
- ✧ Sensors
- ✧ Event Log
- ✧ ACPI
- ✧ Power
- ✧ LAN Configuration
- ✧ FRU
- ✧ Text Console
- ✧ General Information

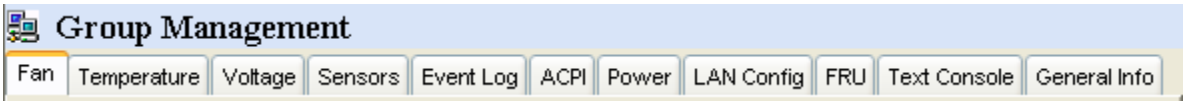


Figure 12-3

- **Fans**

After you've selected multiple servers and clicked the <Fan> tab, a window will display as shown in Figure 12-4. You can use <Ctrl+Click>, <Shift+Click> or draggin your mouse to select servers. Click the <Query> button for IPMIView to collect the fan readings from the selected servers. The information listed in the table shows the fan status of the selected servers. If a fan reading is colored in red, the fan may be broken, not installed, or the reading is below the lower limit. When this occurs, the Administrator should take precautionary measures to ensure that the system functions properly.

You may refresh the fan status by checking the Re-flash checkbox. IPMIView will refresh the fan status based on a preset schedule. Please note that IPMIView will not refresh if you switch to another tab.

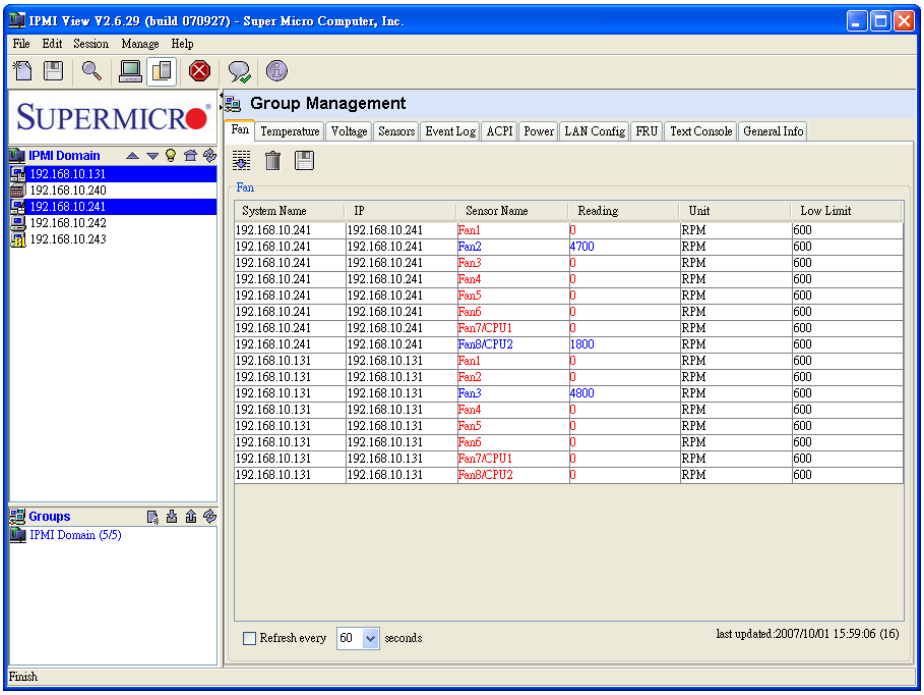


Figure 12-4

- **Temperatures**

The screen shown in Figure 12-5 indicates that multiple servers have been selected, and the Temperature tab is pressed. Clicking the <Query> button allows IPMIView to collect the temperature readings from the selected servers. The information listed in the table shows the temperature settings of the selected servers.

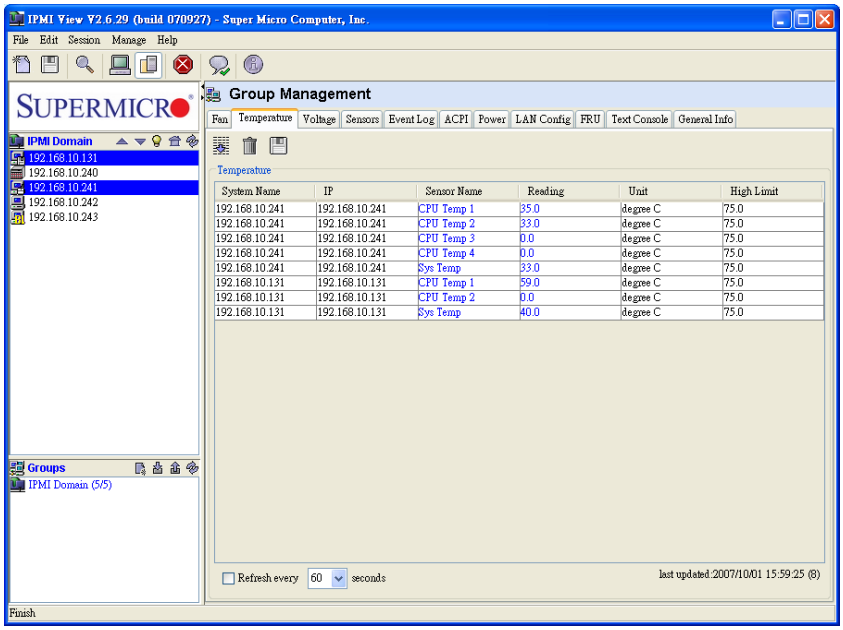


Figure 12-5

- **Voltages**

After selecting multiple servers and < Voltages> settings, you will see the display as shown in Figure 12-6. Clicking the <Query> tab will allow IPMIView to collect the voltage readings from the selected servers. The information listed in the table shows the voltage status of the selected servers.

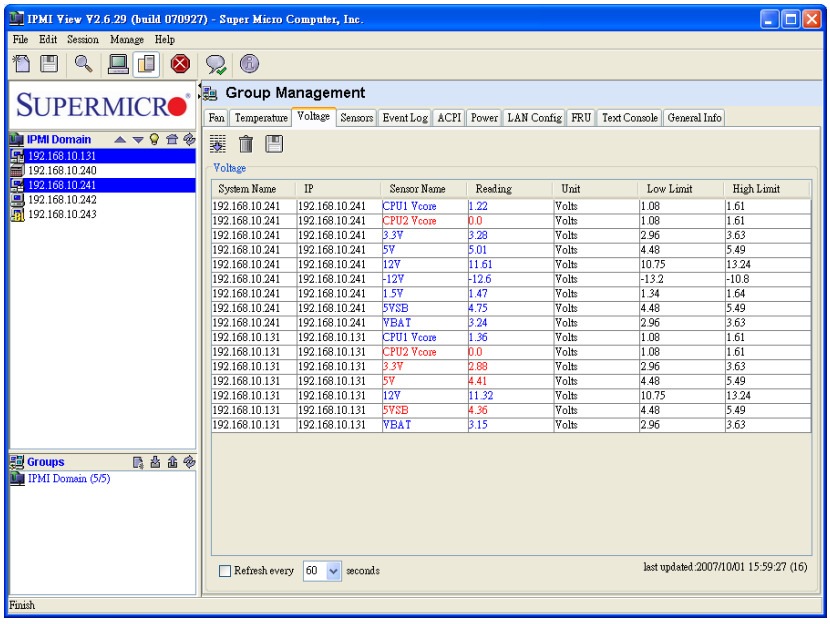


Figure 12-6

- **Sensors**

After selecting multiple servers and clicking the <Sensors> tab, you will see the window as shown in Figure 12-7. Click the <Query> button for IPMIView to collect the sensor readings from the selected servers. The information listed in the table shows the sensor status of the selected servers. The window here shows the chassis status and power supply status. If the chassis is opened or a power supply has failed, the reading will be in red.

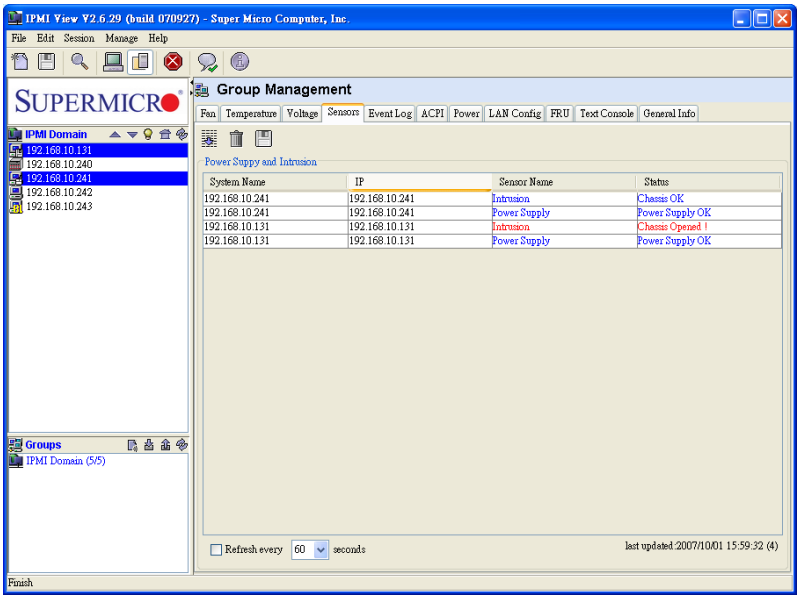


Figure 12-7

- **Event log**

After selecting multiple servers and clicking the <Event Log> tab, you will see a display as shown in Figure 12-8. Click the <Query> button for IPMIView to collect the event logs from the selected servers. The table below displays the event log of the selected servers. Select the <Host combo> box to filter the event log data in the table.

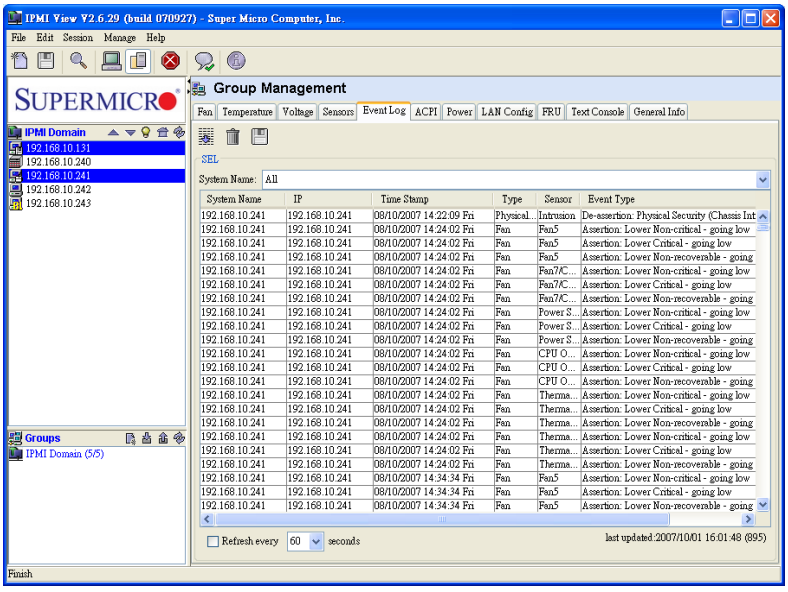


Figure 12-8

- **ACPI**

After selecting multiple servers and clicking the <ACPI> tab, you will see a display as shown in Figure 12-9. Click the "Query" button for IPMIView to collect the ACPI state from the selected servers. The table displays the ACPI state of the selected servers.

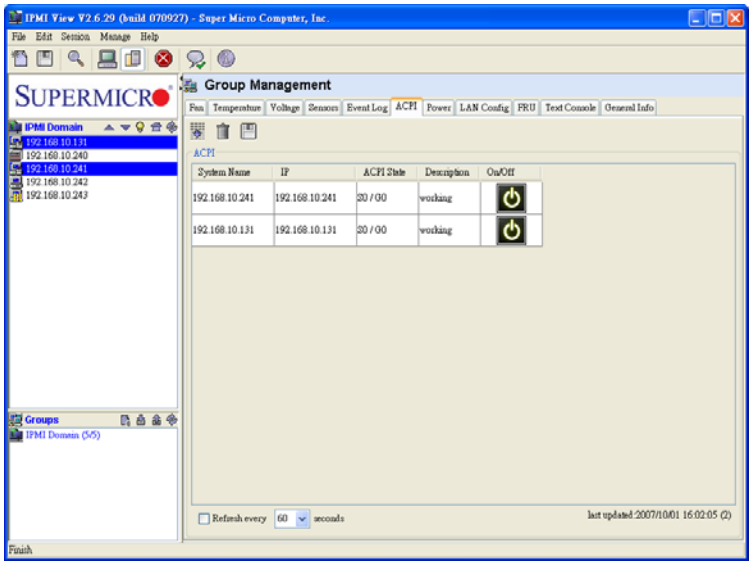


Figure 12-9

- **Power**

After selecting multiple servers and clicking the <Power> tab, you will see a display as shown in Figure 12-10. Click one of the power <Control> buttons to send a command to the selected server. The text area will show the result.

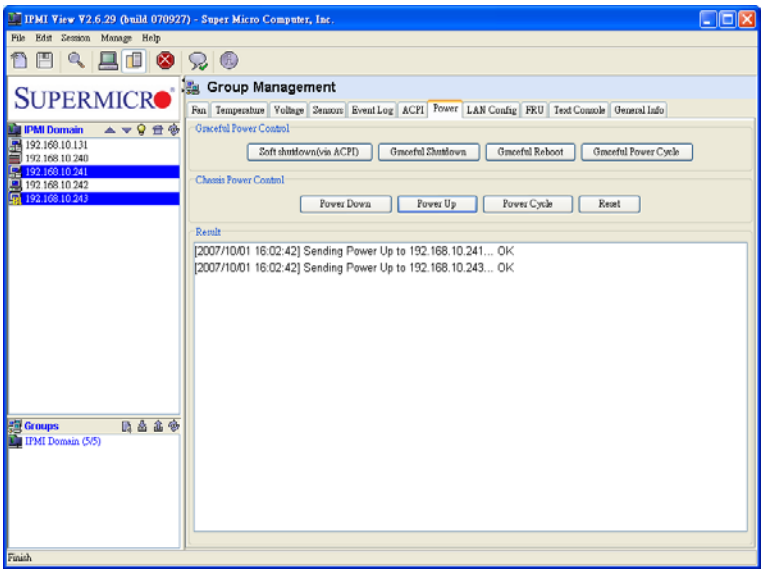


Figure 12-10

- **LAN Configuration**

After selecting a single server and clicking the <LAN Config > tab, you will see a display as shown in Figure 12-11. Click <Query> to get the information needed from a single server and copy it to other servers for data-sharing. The text area will show the results of the query and provide updates. The <Clear> button is used to clear the text field only; it will not clear the actual LAN configuration from the server.

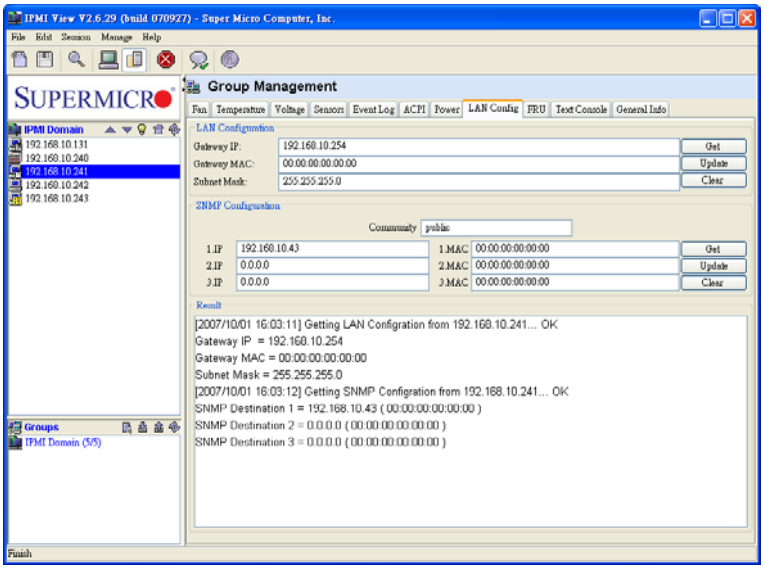


Figure 12-11

- **FRU**

After selecting a single server and clicking the <FRU> tab, you will see a display as shown in Figure 12-12. Click the <Query> button for IPMIView to get the FRU information from a single server, and copy it to other servers for data-sharing. The text area will show the results of a query and provide updates. The <clear> button is used to clear the text field only; it will not clear the actual FRU data from the server.

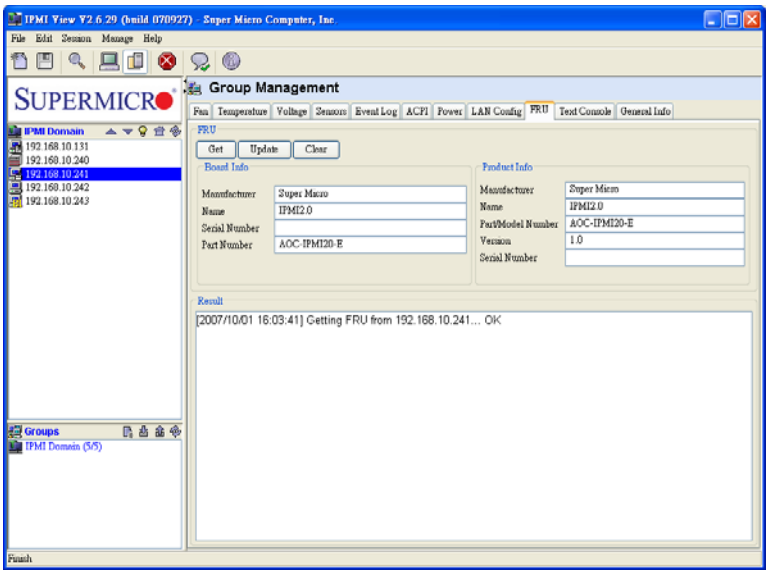


Figure 12-12

- **Text Console**

After selecting a single server and clicking the <Text Console> tab, you will see a display as shown in Figure 12-13. Click the <Open> button for IPMIView to create an internal text console window for the selected server. Click <Start> to start the text console redirection. The power control buttons displayed on the status bar provides power on, power off and reset commands, allowing you to easily power on or power off a remote server. The <Encode> checkbox is for RMCP+ encoding. Check it to enable packet encoding between the IPMIView and a server.

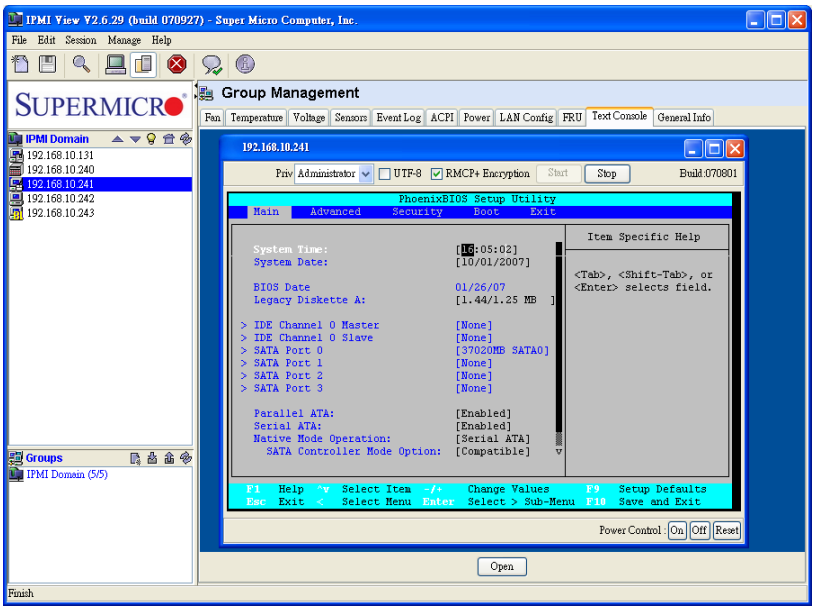


Figure 12-13

- **General Information**

After selecting multiple servers and clicking the <General Info> tab, you will see a display as shown in Figure 12-14. Select the fields you want to query from the servers, and click the <Query> button to allow IPMIView to collect the information from the selected servers.

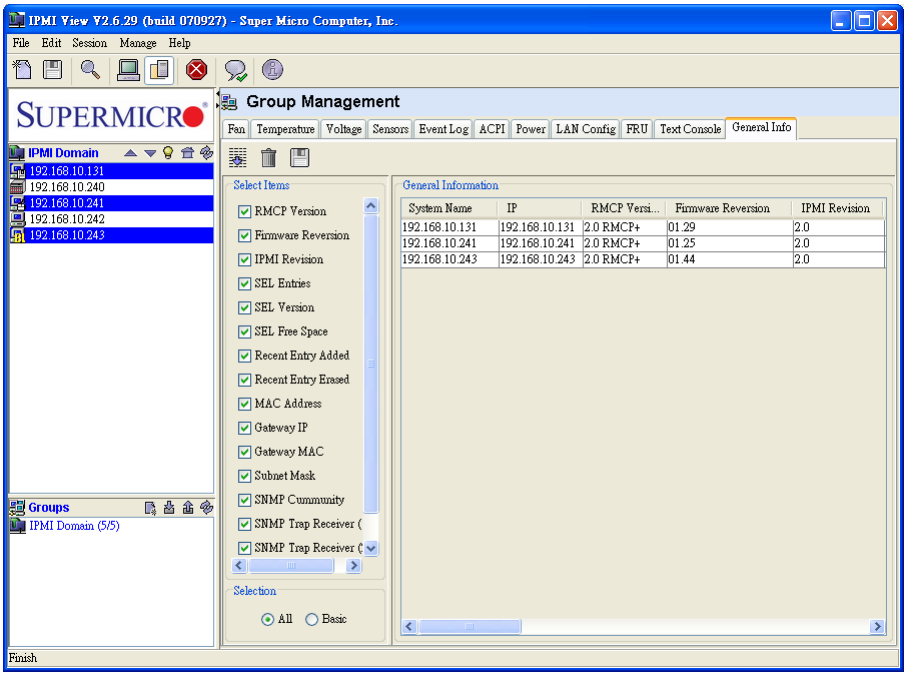


Figure 12-14

13. Trap Receiver

The Trap Receiver is a utility used for receiving traps from the BMC. In the event of a sensor error or a sensor reading that exceeds a threshold, the BMC will send SNMP traps to the destinations set in the BMC. The Trap Receiver is executed on the destination site and receives the SNMP trap from multiple senders (BMCs). If you select a category, you can see all the traps in that category. Furthermore, when you click a trap in the trap list, you can see its details in the <Trap Structure> window. Please refer to the BMC Setting page in IPMIView to set the SNMP destination.

As shown in Figure 12-1, there are several components to the IPMI Trap Receiver.

1) Menu Bar: contains pull-down menus for exiting the programs, getting help, etc.
2) Tool Bar: contains all IPMI Trap Receiver features.
3) Category: categorizes the traps by the sender, community and sensor.
4) Trap Structure: It is a tree structure that displays traps in detail.
5) Status Bar: shows messages regarding the current status of related components.
6) Trap List: shows detailed information for traps received.

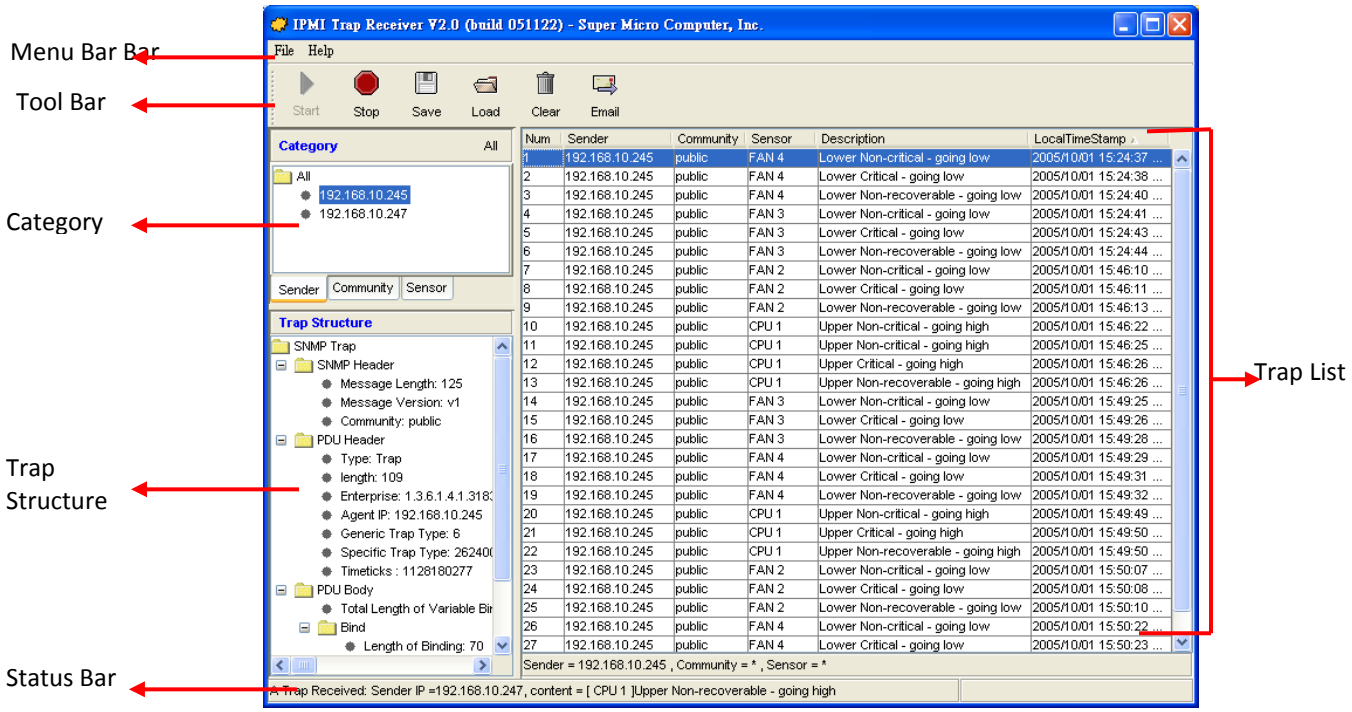


Figure 12-1

- Tool Bar functions

The tool bar provides the following features as shown in Figure 12-2.

Figure 12-2

- Start: starts the Trap Receiver.

- Stop: stops the Trap Receiver.
- Save: saves the traps received into a file.
- Load: loads a saved trap file into the Trap Receiver.
- Clear: clears all the traps in the trap list.
- Email: displays an “Email-Alert Settings” dialog box (see Figure 12-3). Fill the “SMTP server”, “From (email address)” and “To (email address)” fields. The “From” and “To” addresses must be valid in the SMTP server. If the SMTP server requires authentication, please enter the username and password. Once entering needed information, click the <Test> button to verify if your email works properly.

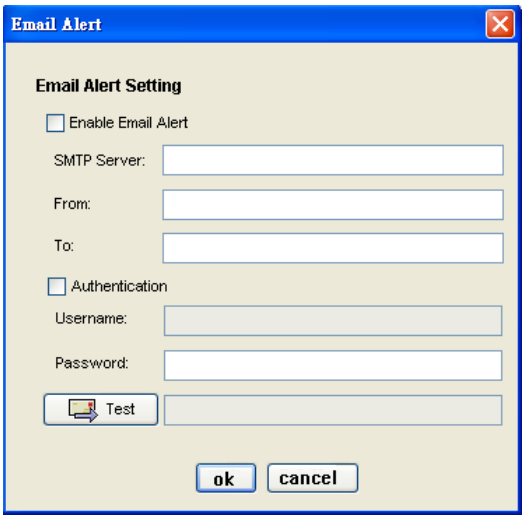


Figure 12-3

- Category

There are three categories including: Sender, Community and Sensor as shown in Figure 12-4. The Sender page lists all sender IP addresses. The Community page lists all SNMP communities. The Sensor page lists all sensor types from the traps. Clicking on each category type will act as a filter for all traps in the traps list. Click the <All> button to cancel all filters.

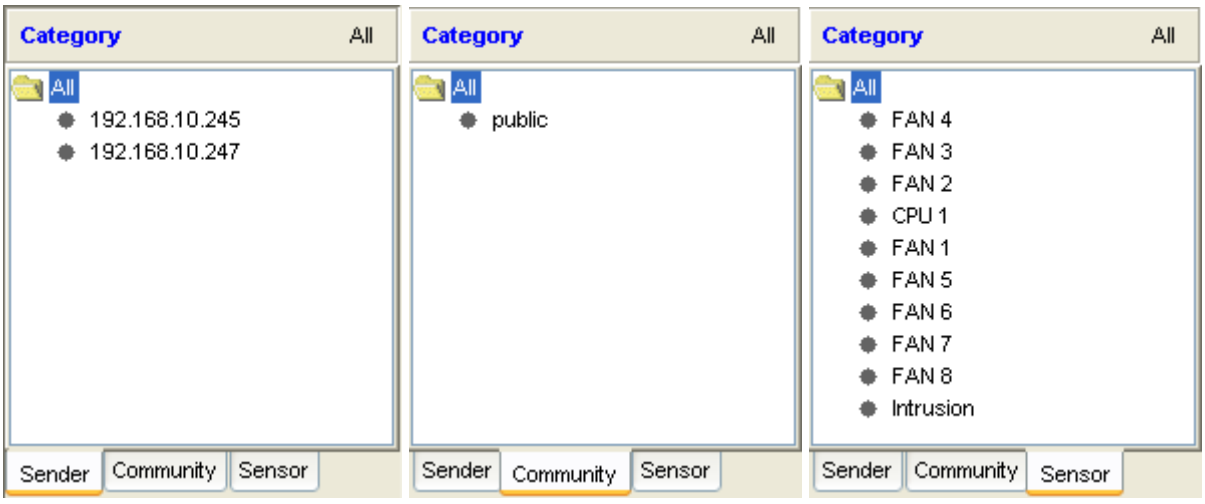
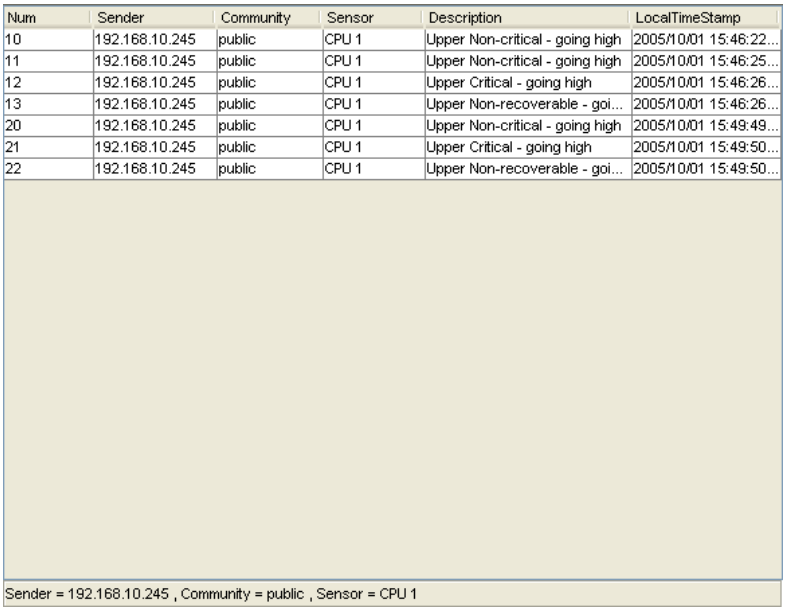


Figure 12-4

Once a category has been selected, the filter condition will be displayed at the bottom of the “trap” list. See Figure 12-5 for reference. As displayed in Figure 12-5, the filter is “Sender = 192.168.10.245,

Community = public, Sensor = CPU 1”. The trap list displays only those traps whose contents are included in each of the three filters.



Num	Sender	Community	Sensor	Description	LocalTimeStamp
10	192.168.10.245	public	CPU 1	Upper Non-critical - going high	2005/10/01 15:46:22...
11	192.168.10.245	public	CPU 1	Upper Non-critical - going high	2005/10/01 15:46:25...
12	192.168.10.245	public	CPU 1	Upper Critical - going high	2005/10/01 15:46:26...
13	192.168.10.245	public	CPU 1	Upper Non-recoverable - goi...	2005/10/01 15:46:26...
20	192.168.10.245	public	CPU 1	Upper Non-critical - going high	2005/10/01 15:49:49...
21	192.168.10.245	public	CPU 1	Upper Critical - going high	2005/10/01 15:49:50...
22	192.168.10.245	public	CPU 1	Upper Non-recoverable - goi...	2005/10/01 15:49:50...

Sender = 192.168.10.245 , Community = public , Sensor = CPU 1

Figure 12-5

- Trap Structure

The Trap Structure displays detailed information for the selected item in the trap list. Information includes the “SNMP Header”, “PDU Header”, “PDU Body”, “Bind” and “PET” data.

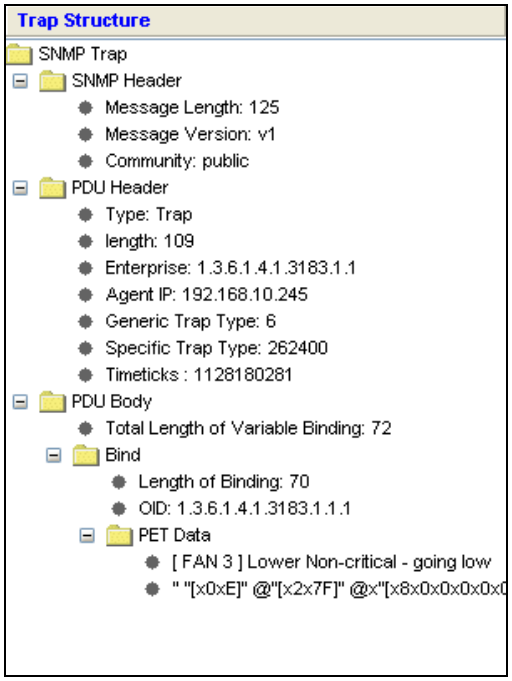


Figure 12-6

- Receiving a Trap

When the Trap Receiver receives a trap from the BMC, an alert bar will display on the screen for about 10 seconds to notify you that a trap has occurred. In addition, an email alert will be sent according to the information field in the Email Alert dialog box. Please refer to Figure 12-7.

The content of the email will include the following information.

A SNMP trap received
Sender:192.168.10.247
Sensor:FAN 2
Description:Lower Non-recoverable - going low
Time:2005/11/22 14:27:07 Tue

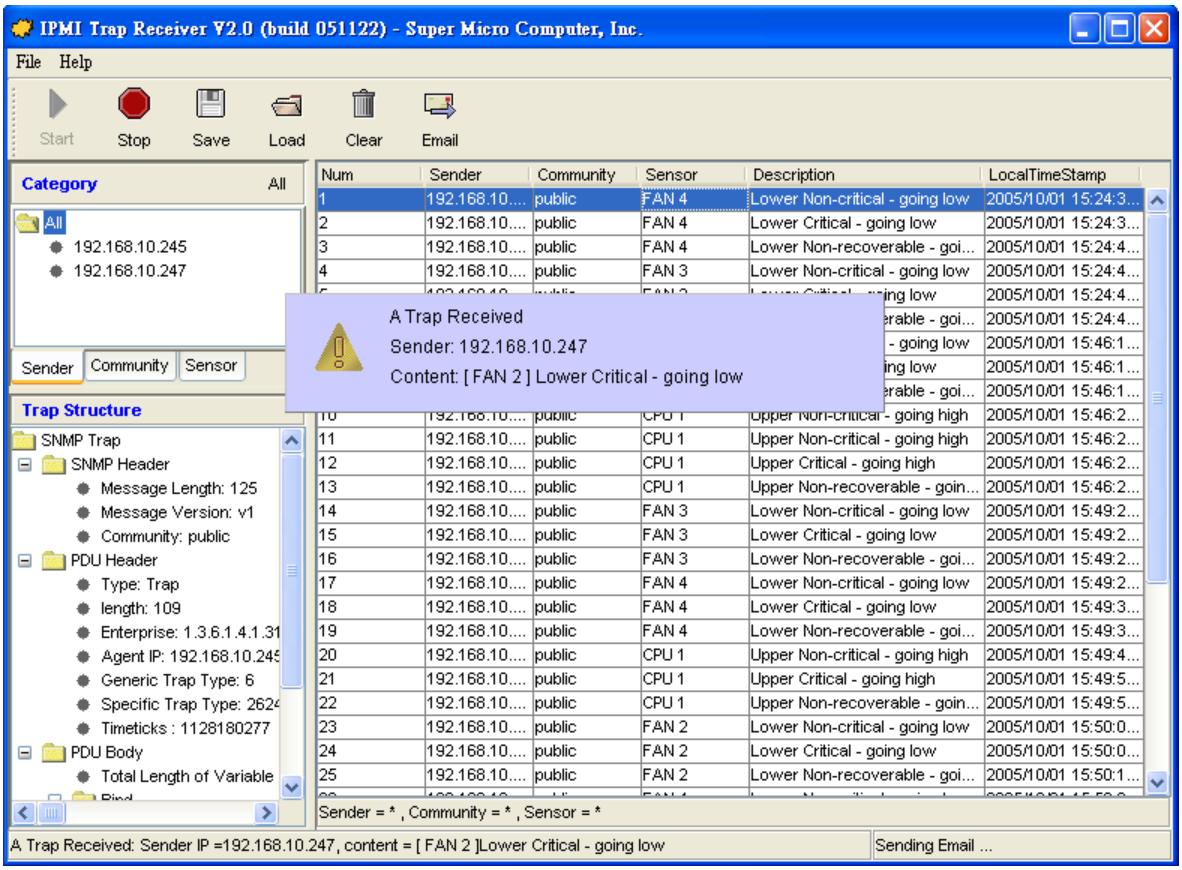


Figure 12-7

Appendix A: SIM Firmware Update

1. Select a remote system on the System list and click “File > Update IPMI Firmware” to start the firmware update.

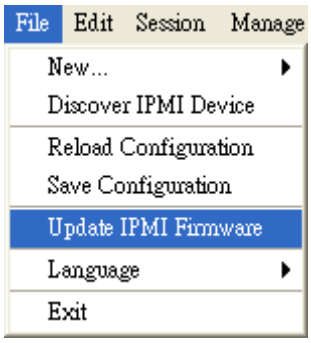


Figure A-1

2. Click the <Open> button to select the<firmware> you desire and then click <Start> to continue.

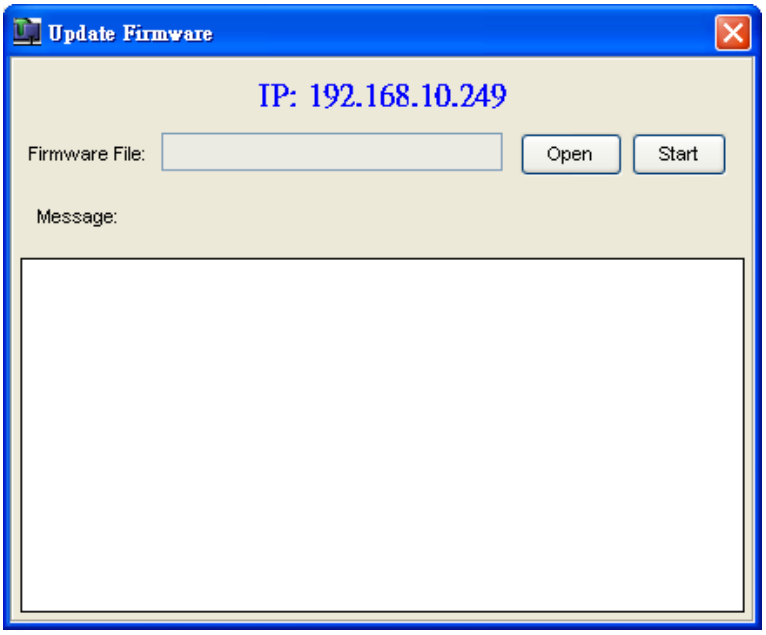


Figure A-2

3. A login dialog will appear. Please enter the Login_ID and the password. This user will be granted the privilege as an Administrator.

Figure A-3

4. A firmware information dialog will appear. It shows detailed information on the current and new firmware. Click <Yes> to continue.

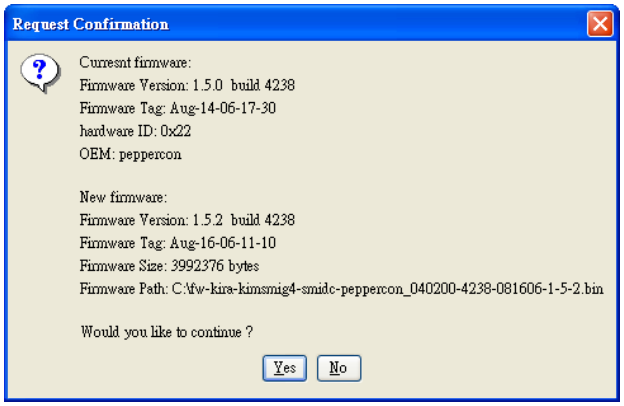


Figure A-4

5. The firmware file will start to upload. This process may take few minutes to complete.

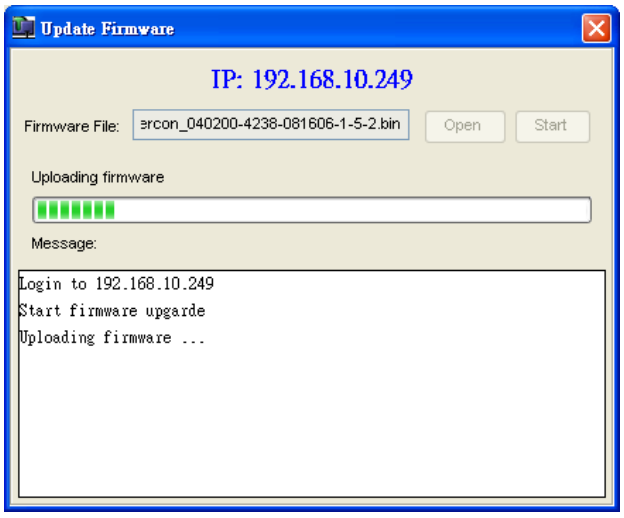


Figure A-5

6. Please wait for the firmware to upload. Once uploading is completed, the BMC will start to flash the firmware internally. This step may take about a minute. Please try to connect to the system after two minutes.

Appendix B: SIM(W) KVM Console and Virtual Media

SIM(W) KVM Console allows the user to perform console redirection via KVM (Keyboard/Video/Mouse) support as shown in Figure B-1.

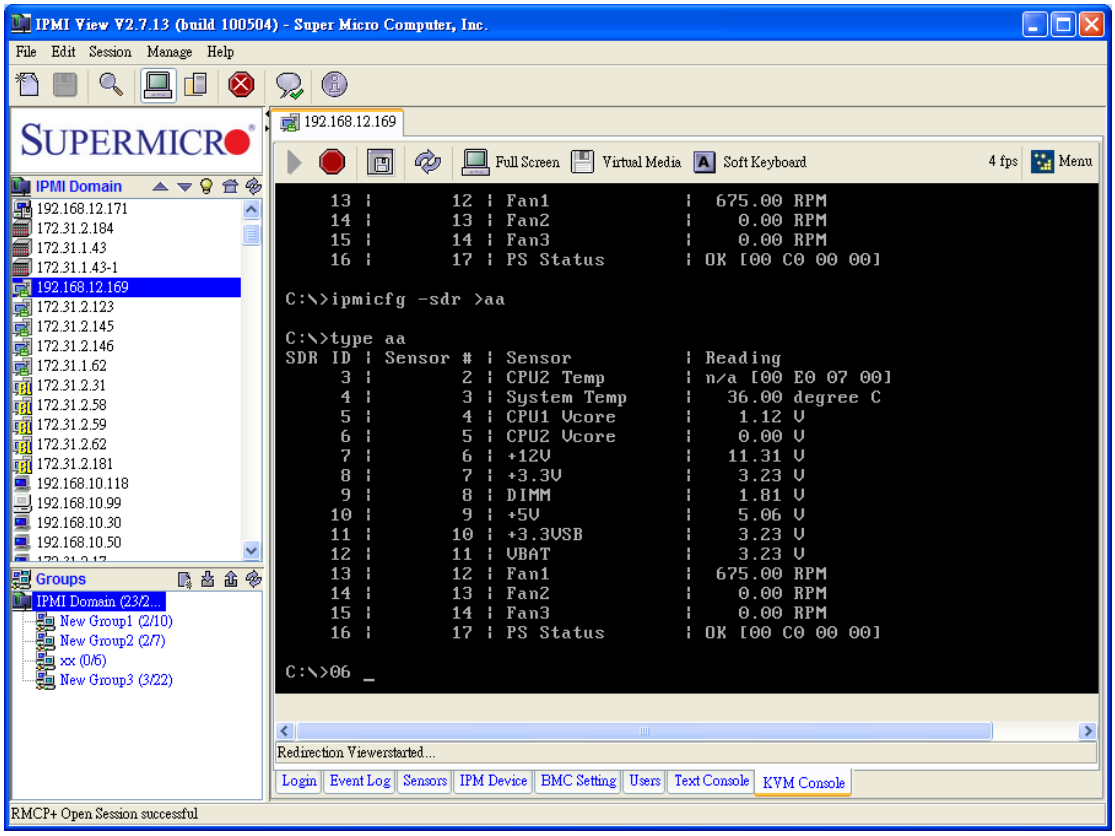


Figure B-1 SIM(W) KVM Console Main Screen

SIM(W) Console Toolbar

The SIM(W) Console Toolbar provides seven tool buttons which will allow the user to perform the following actions as shown in Figure B-2.

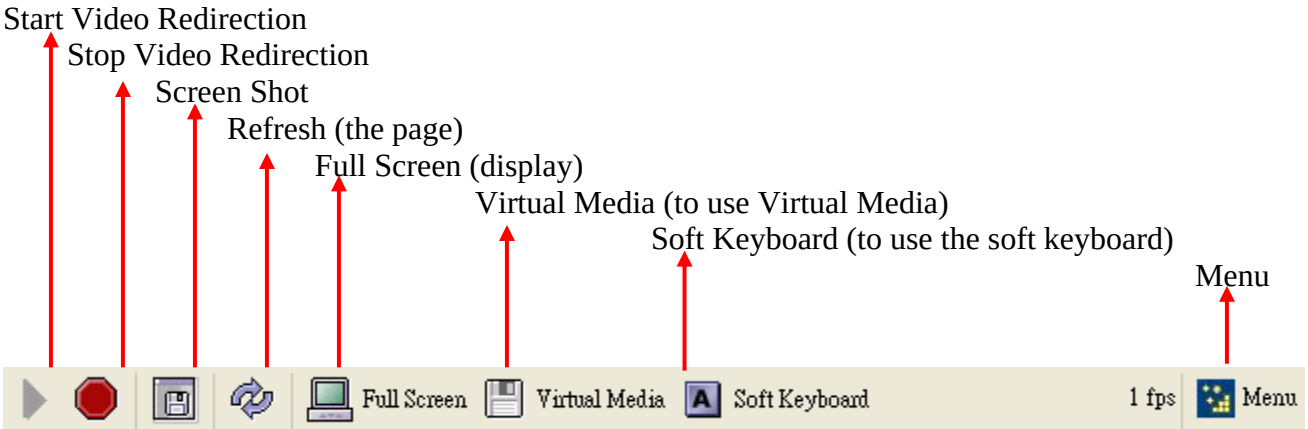


Figure B-2 SIM(W) KVM Console Toolbar

-  Start Video Redirection

Click this button to start SIM(W) KVM console redirection.

-  Stop Video Redirection

Click this button to stop video redirection. Please note that the drive redirection will continue to work when it is enabled.

-  Full Screen

Click this button to maximize the size of the remote video screen displayed on the local computer screen as shown in Figure B-3.

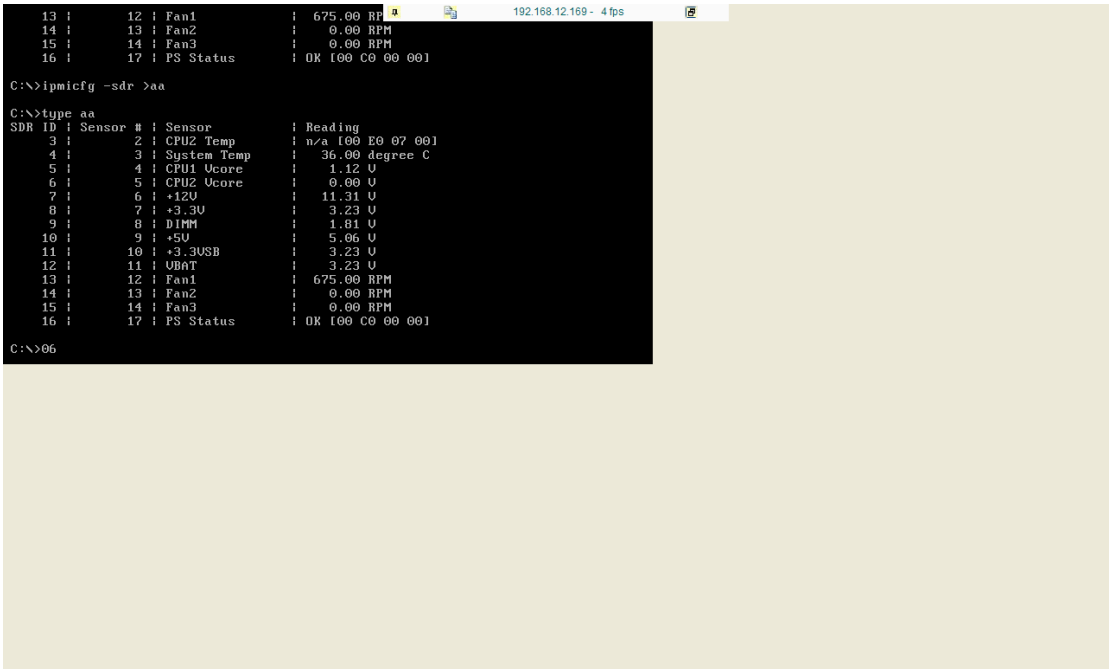


Figure B-3 Full Screen

-  Virtual Media

Click this button to enable Virtual Media support as shown in Figure B-4.

Virtual Media

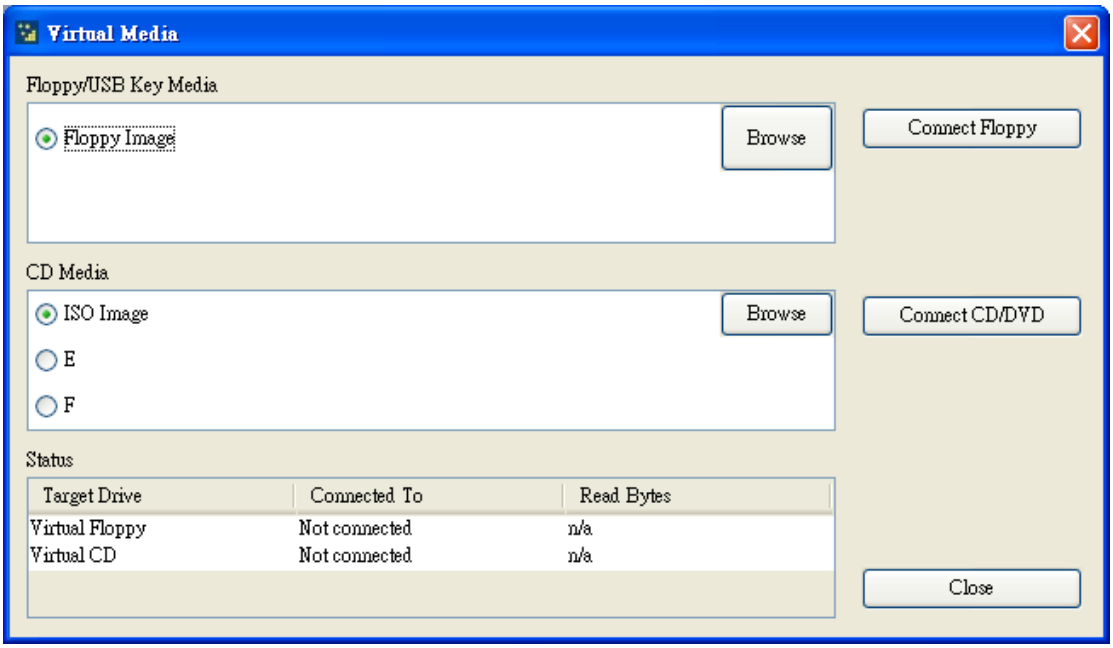


Figure B-4 Virtual Media

- Floppy/USB key Media: This feature allows the user to redirect Floppy/USB Media.
- CD Media: This feature allows the user to redirect CD/DVD or ISO image file.
- Connect Floppy: Click this button to start to redirect your Floppy Image or USB Key Media.
- Connect CD/DVD: Click this button to start to redirect your CD/DVD or ISO image file.

-  Soft Keyboard

Click this button to use the Soft Keyboard for console redirection as shown in Figure B-5.

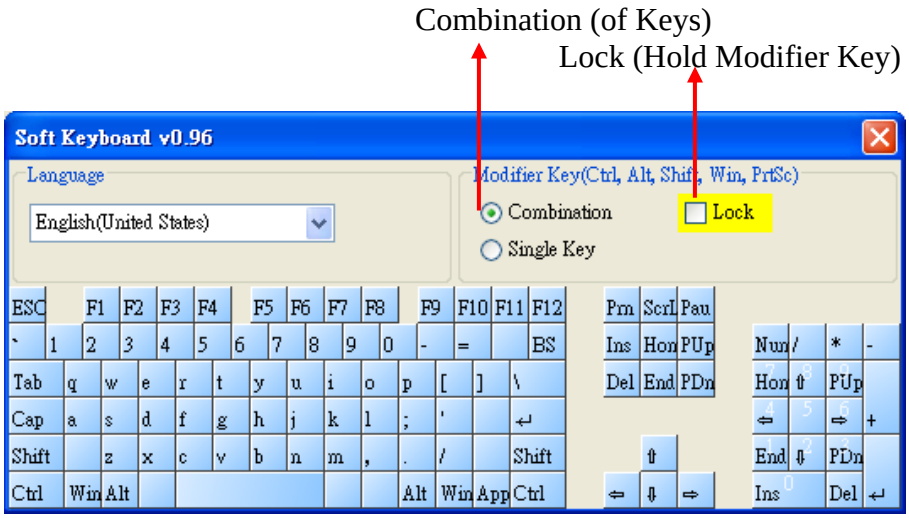


Figure B-5 Soft Keyboard

- Language: This feature allows you to select a proper language setting for your soft keyboard.
- Combination: Check this button if you want to use a combinations of modifier keys
- Single Key: Check this button if you want to use a modifier key as single key.
- Lock: Check this button to hold the modifier key you've clicked.

The menu is same as web KVM UI.

Appendix C: SIM(WA) iKVM Console and Virtual Media

Press <Launch KVM Console> to open SIM(WA) iKVM Window as in Figure C-1.

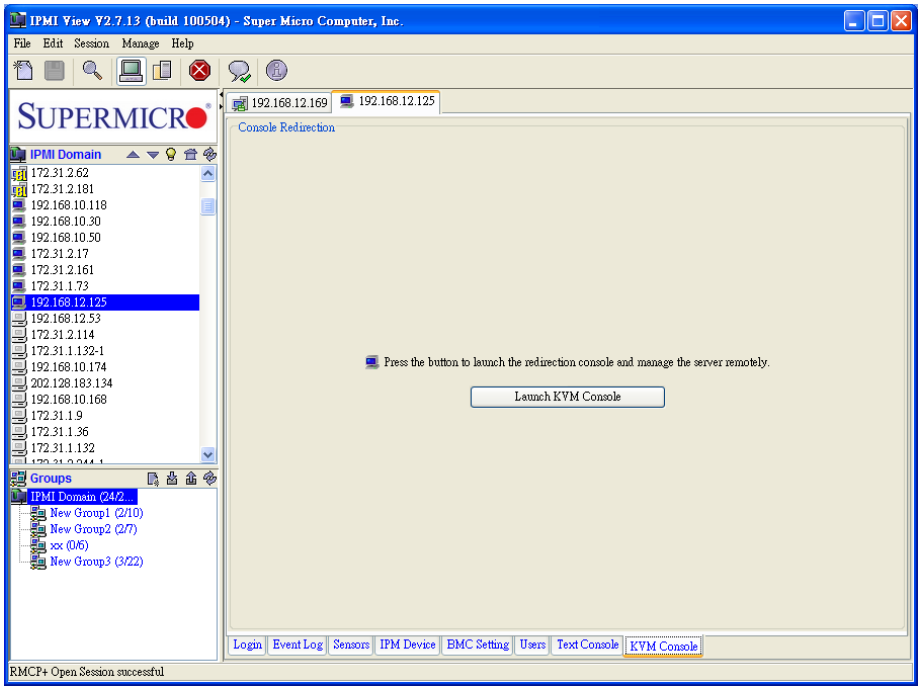


Figure C-1 SIM(WA) iKVM Window

Please note that SIM(WA) iKVM window supports same features as other versions of Web KVM as shown in Figure C-2.

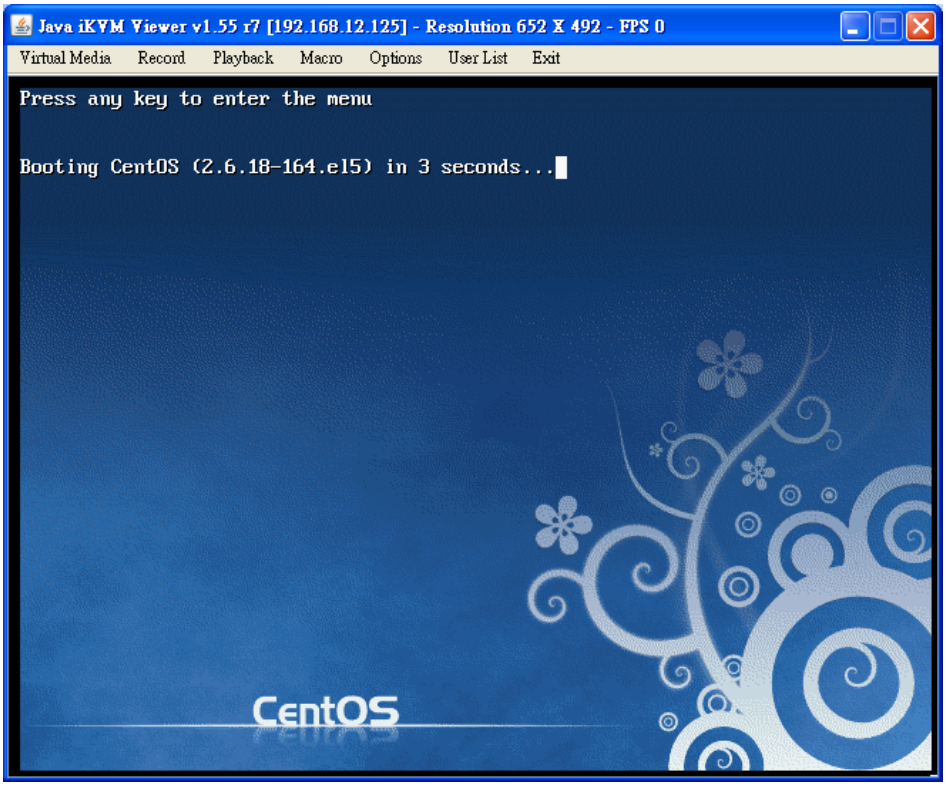


Figure C-2 iKVM Window

- Virtual Media (USB Floppy & Flash)

Click <Virtual Media> on the menu bar and then click <Virtual Storage> to display the Virtual Media (USB Floppy & Flash screen) as shown in Figure C-3.

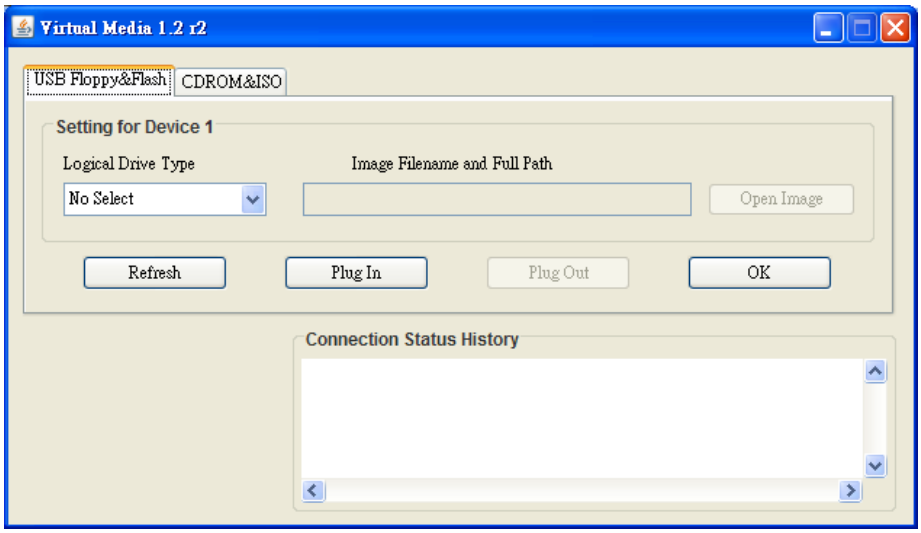


Figure C-3 Virtual Media (USB Floppy & Flash)

- Logical Drive Type: From the pull-down menu select the logical drive type.
- Image Filename and Full Path: Enter the image file name and the full path to the file. It is available only for ISO files.
- Refresh: Click this button to refresh the page.
- Plug In: Click this button to mount your logical drive as virtual media.
- Plug Out: Click this button to un-mount virtual media.
- OK: Click this button to confirm and exit.
- Connection Status History: This window displays the connection and the status of virtual media.

- Virtual Media (CDROM & ISO)

Click < CDROM & ISO > to display the Virtual Media (CDROM & ISO). as shown in Figure C-4.

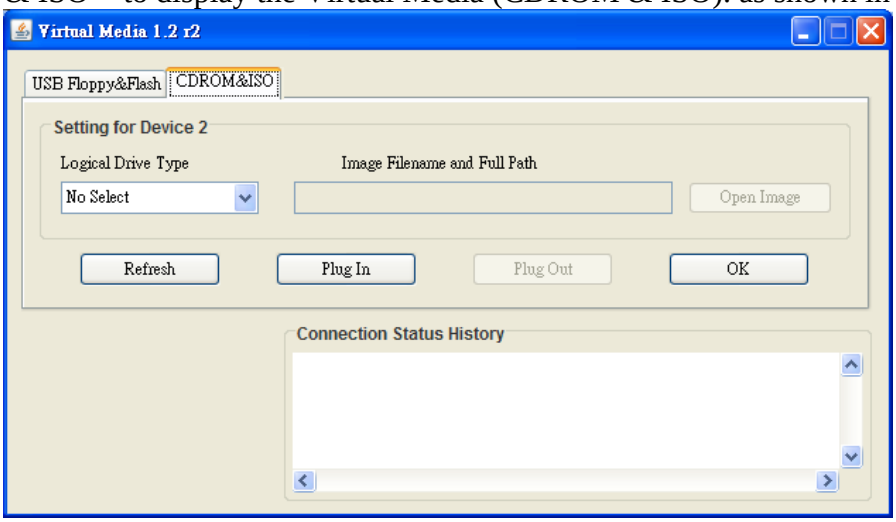


Figure C-4 Virtual Media (CDROM & ISO)

- Logical Drive Type: From the pull-down menu select the logical drive type.
- Image Filename and Full Path: Enter the image file name and the full path to the ISO file.
- Refresh: Click this button to refresh the page.
- Plug In: Click this button to mount your logical drive as virtual media.
- Plug Out: Click this button to un-mount virtual media.
- OK: Click this button to confirm and exit.
- Connection Status History: This window displays the connection and the status of Virtual Media.

- iKVM Virtual Keyboard

Virtual Keyboard provides soft keyboard support and allows the user to click a key on the soft keyboard by using the mouse when a keyboard is not available. Refer to Figure C-5 for Virtual Keyboard.

Figure C-5 Virtual Keyboard

Appendix D: SIM(W) Firmware Update

To re-flash SIM(W) Firmware, please select an SIM(W) device and <Update firmware> in the menu. Then, click <OK>. A dialog box will display as shown in Figure D-1.

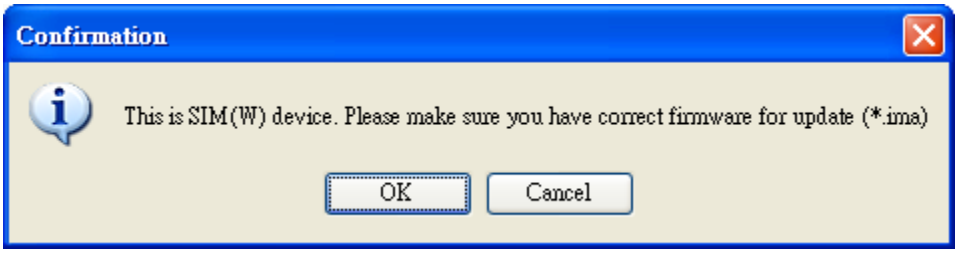


Figure D-1 SIM(W) Firmware Re-flash

YAFU Flash

1. To flash Hermon Firmware, The YAFU Flash Main screen will display as shown in Figure D-2.

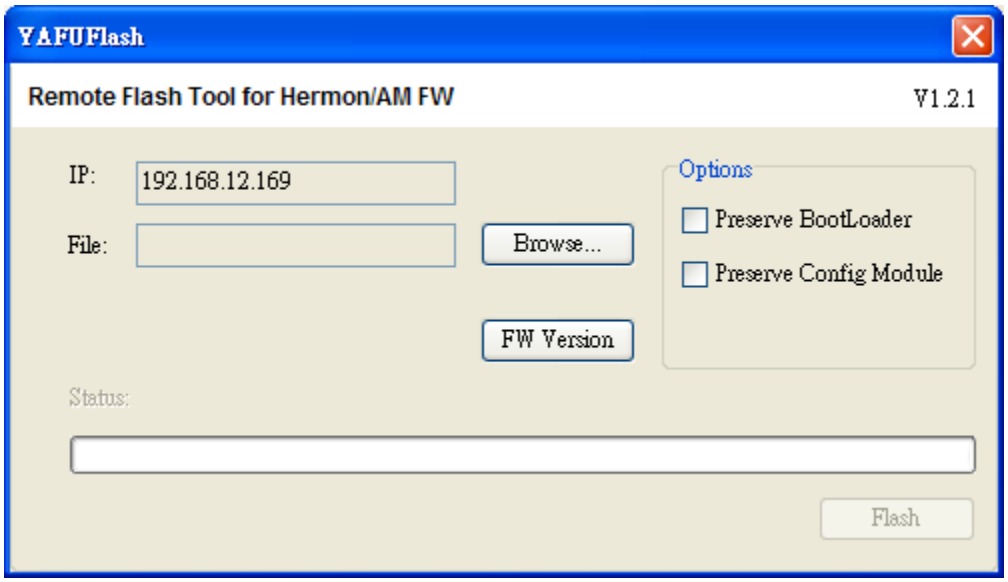


Figure D-2 YAFU Flash Main screen

2. After you've selected a firmware file for remote flashing, it will be checked if it is a valid file before remote flashing starts.

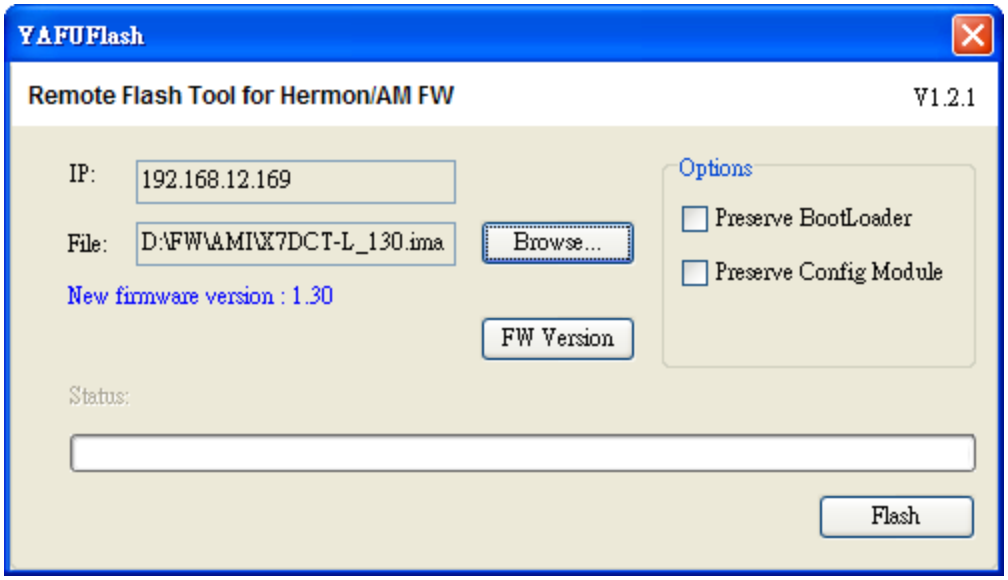


Figure D-3 YAFU Flash (2)

- IP: This item displays the IP Address of the IPMI device.
- Browse: Enter the file name or browse the data base to select a file that you want to perform remote flashing.
- Preserve BootLoader: Check this box to preserve the settings of BootLoader.
- Preserve Config Module: Check this box to preserve the settings of Configuration Module.
- Firmware Version: The new firmware version will be displayed.
- Flash: Click <Flash> to commit the file for remote flashing.

3. Remote Flashing can only be performed by an Administrator. If you are an administrator, enter your ID and your password in the screen below. Then click <OK>.

Figure D-4 ID and Password (Administrator)

4. Check the current firmware version. The current firmware version will be displayed as shown in Figure D-5.

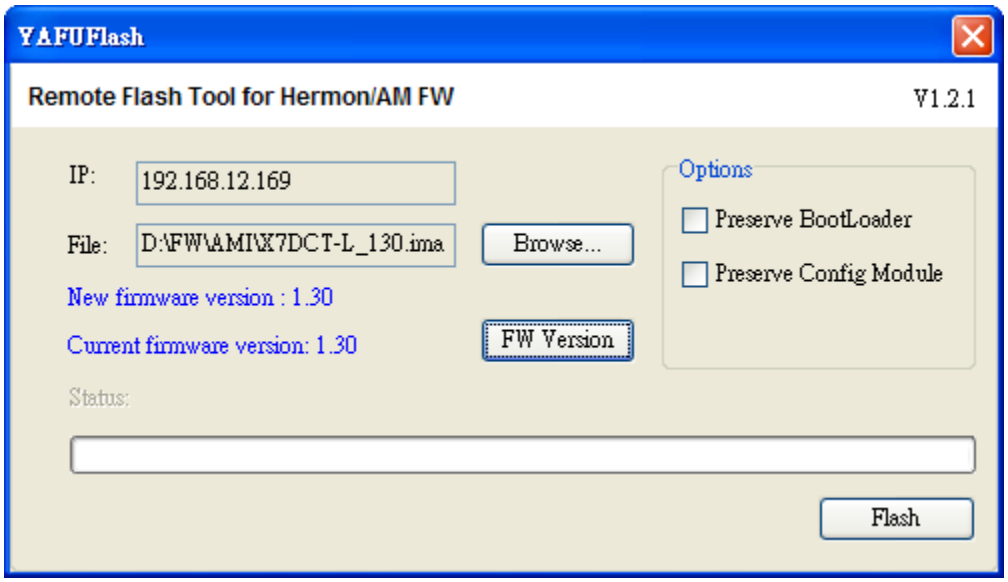


Figure D-5 Display of Current Firmware Version

5. Once you've checked the firmware versions and clicked <Flash>, YAFUFlash remote flashing will start as shown in the screens below.

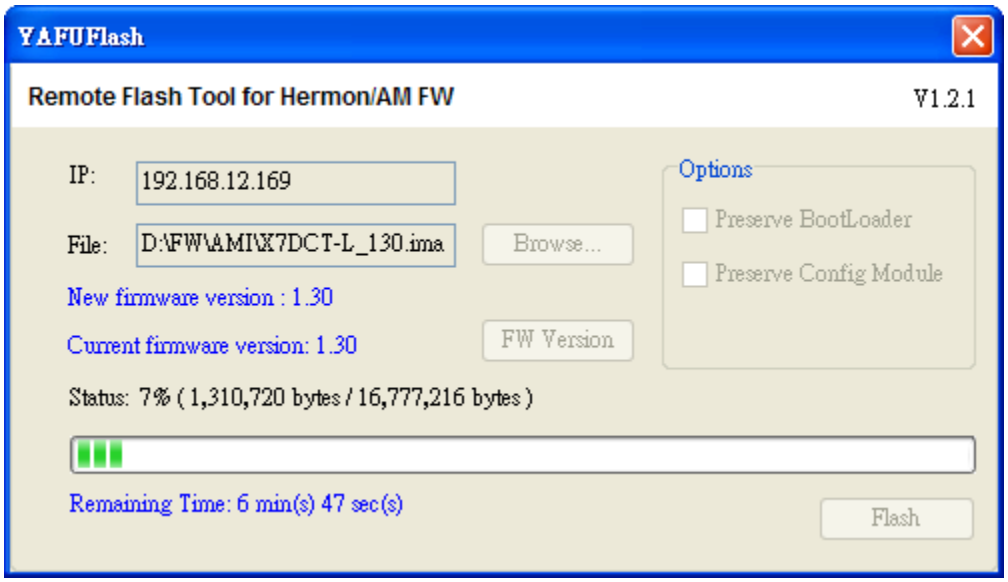


Figure D-6 Remote Flash Screen #1

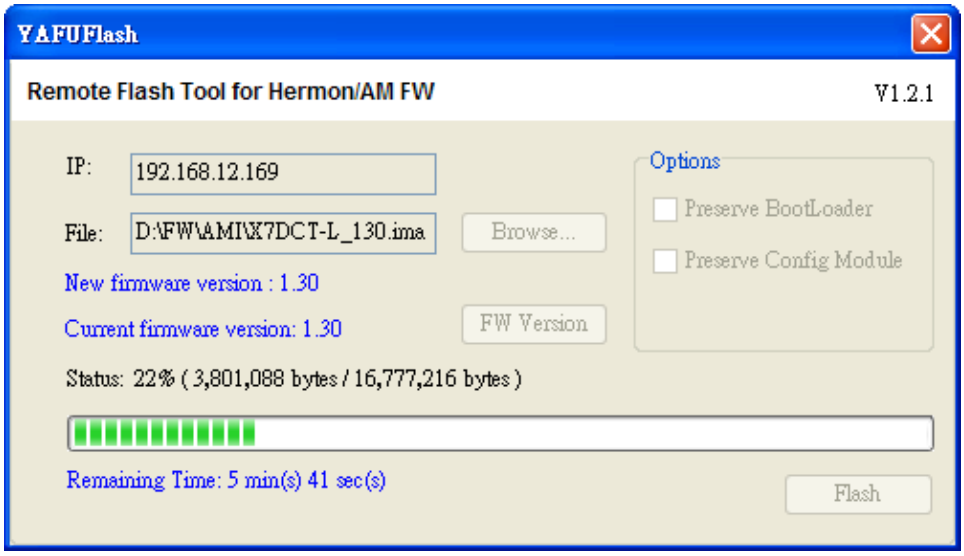


Figure D-7 Remote Flash Screen #2

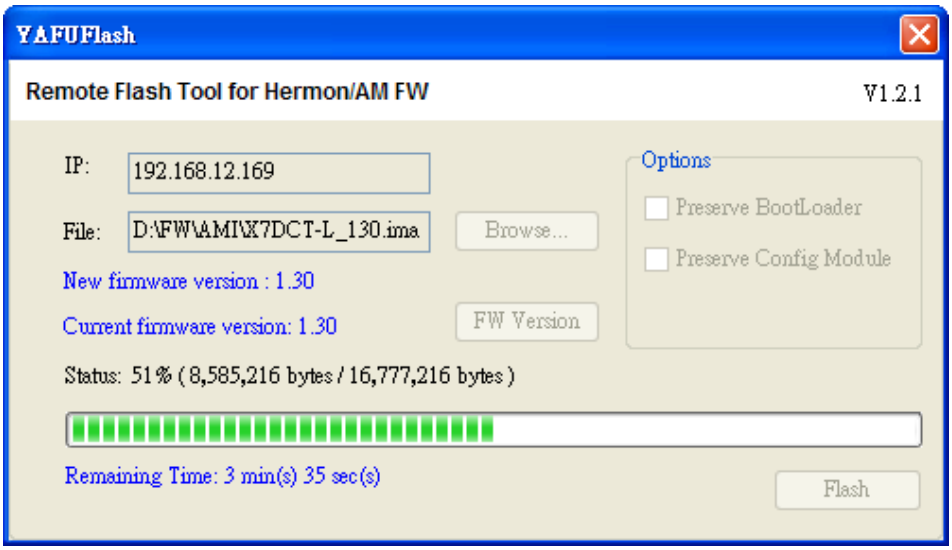


Figure D-8 Remote Flash Screen #3

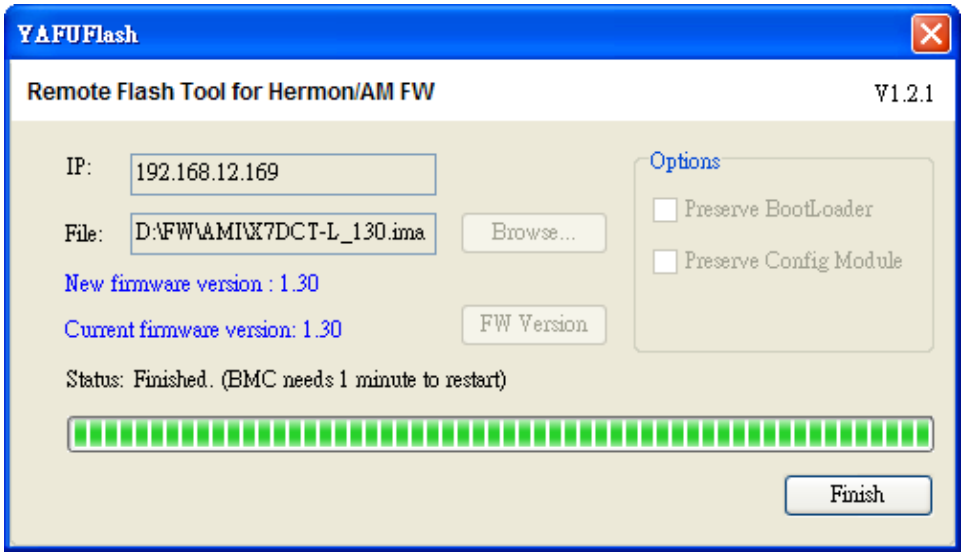


Figure D-9 Remote Flash Screen #4

Appendix E: SIM(WA) Firmware Update

1. Select an SIM(WA) device and select <Update Firmware> in the menu for SIM(WA) Firmware Re-flashing. A screen will display as shown in Figure E-1.

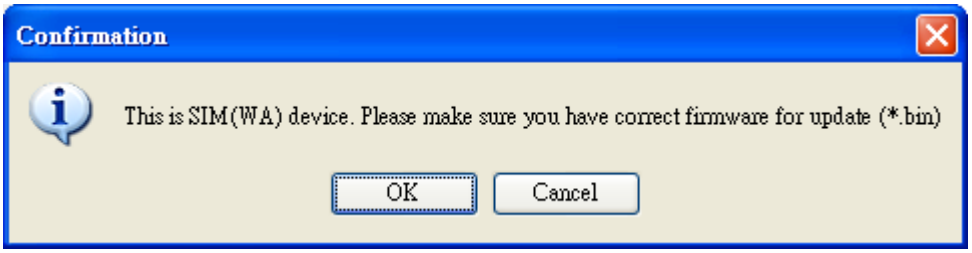


Figure E-1 Firmware Update Screen

2. Make sure that you've selected the correct firmware for update, and click <OK>. The Main Flash Screen will display as shown in Figure E-2.

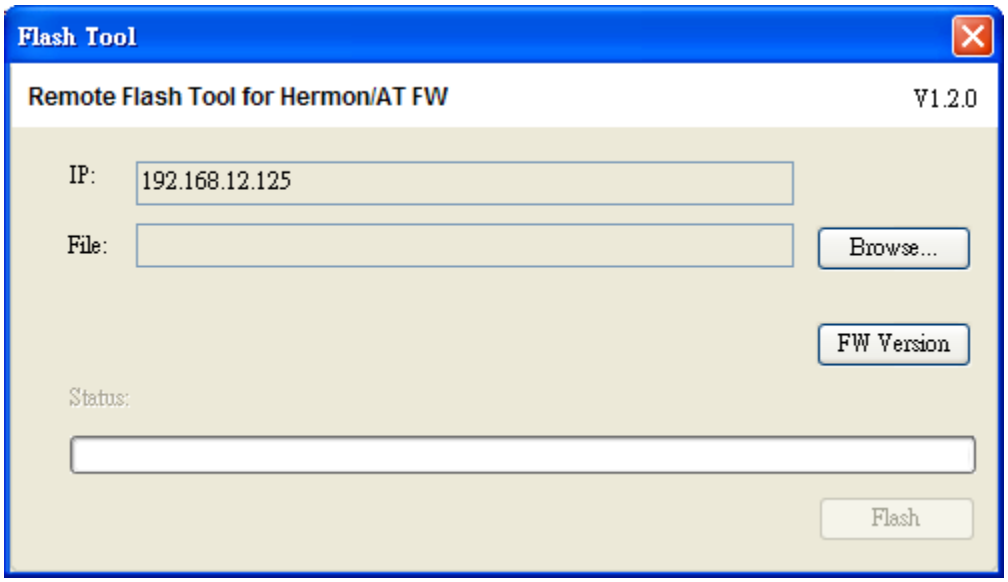


Figure E-2 Main Flash Screen

3. After you've selected a firmware file for remote flashing, it will be checked if it is a valid file before remote flashing start.

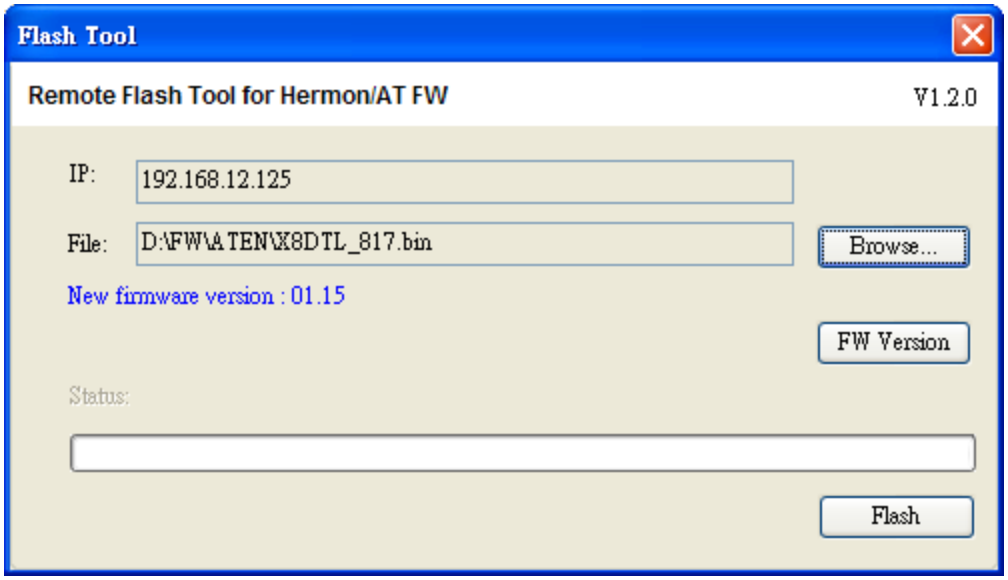


Figure E-3 Main Flash Screen

4. Remote Flashing can only be performed by an administrator. If you are an administrator, enter your ID and your password in the screen below. Then click <OK>.

Figure E-4 ID/Password Screen

5. Check new and current firmware versions. The firmware versions will be displayed as shown in Figure E-5.

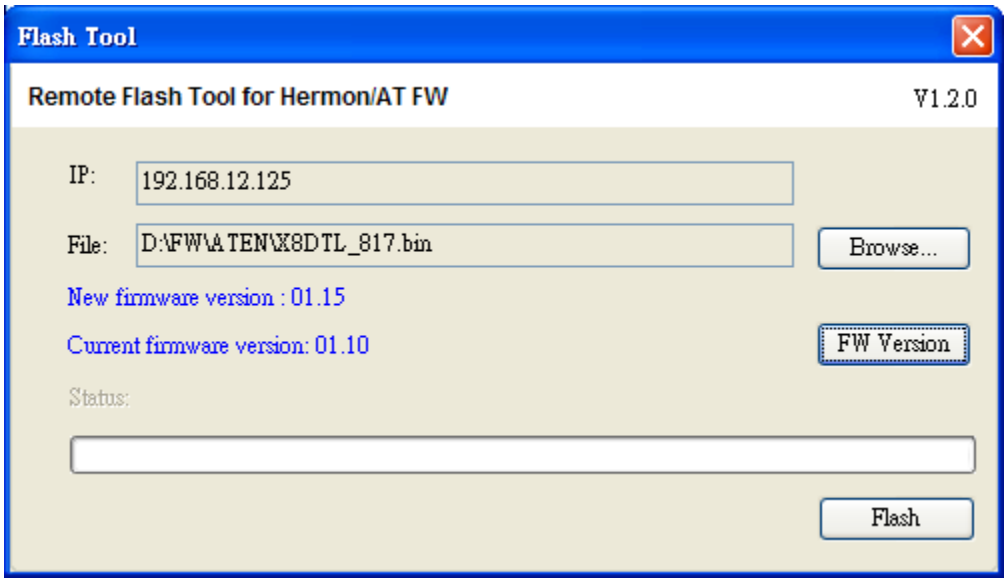


Figure E-5 Firmware Versions

6. Once you've checked the firmware versions and clicked <Flash>, firmware flashing will start as shown in the screens below.

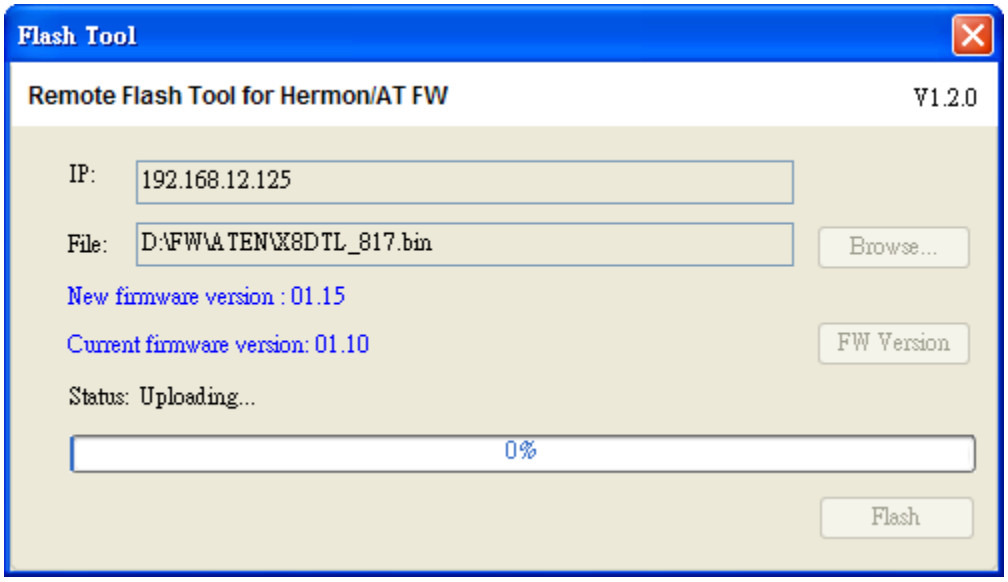


Figure E-6 Remote Flash Screen #1

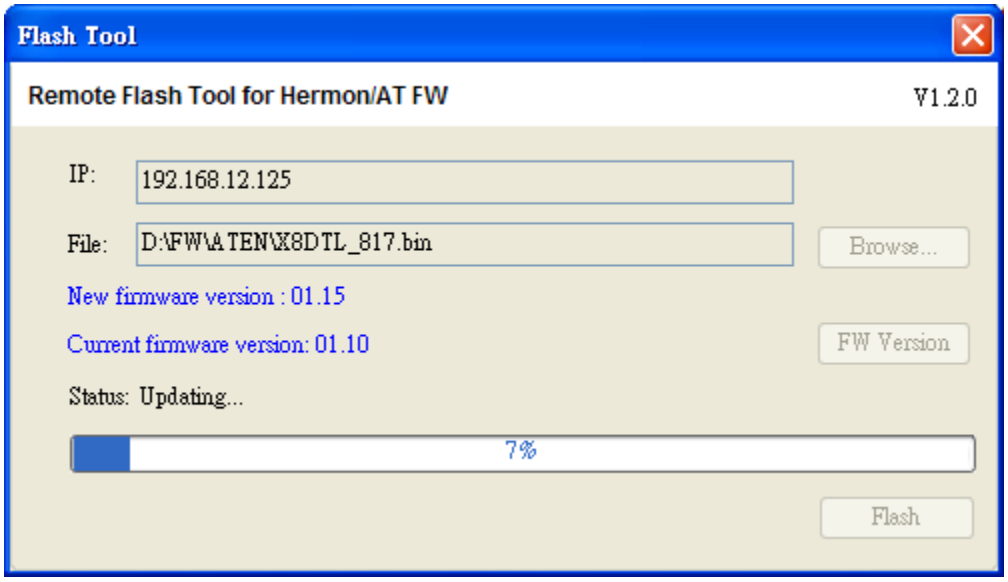


Figure E-7 Remote Flash Screen #2

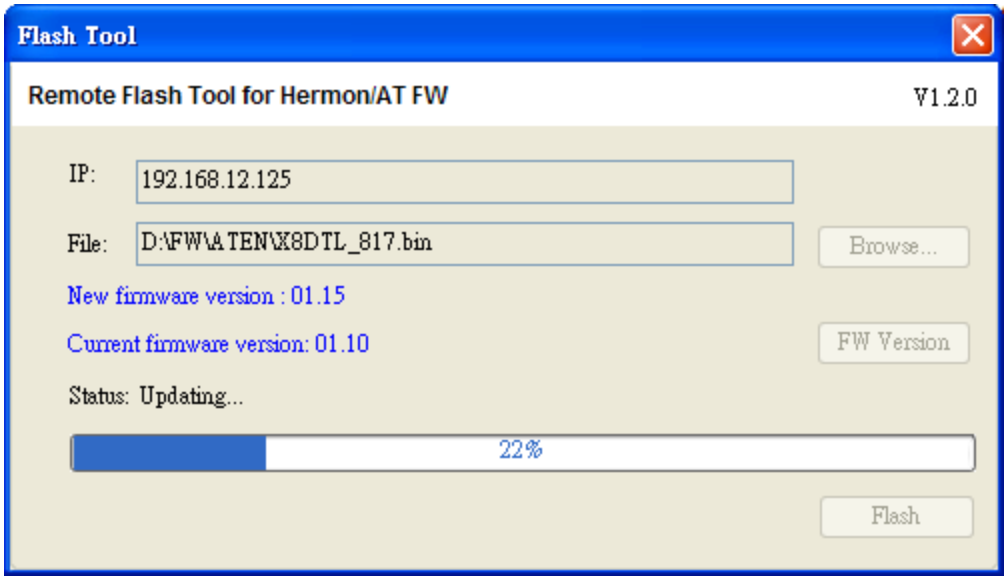


Figure E-8 Remote Flash Screen #3

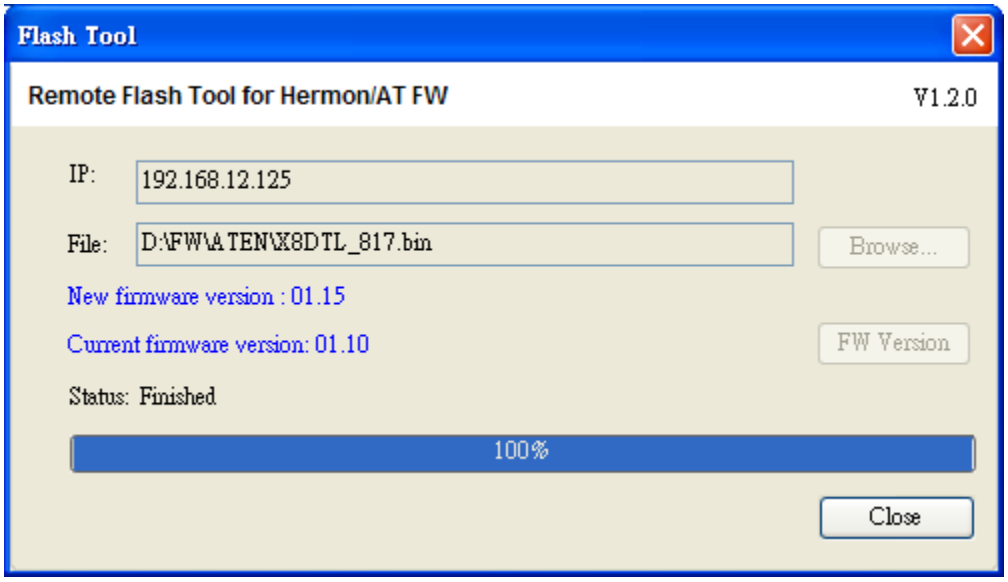


Figure E-9 Remote Flash Screen #4