



# **IPMI View User Guide**

**Version 2.0**

**Copyright © 2003-2004 Super Micro Computer, Inc., All rights reserved.**

## **IPMI View 2.0 (IPMI Over LAN)**

### **I. Overview:**

IPMI View is management software based on IPMI specification version 1.5 - 2.0. IPMI View sends IPMI messages to and from the BMC (Base Management Card) on a remotely managed system. IPMI messages are encapsulated in RMCP (Remote Management Control Protocol) packets called “datagrams”. This method is also referred to as “IPMI over LAN”.

The Distributed Management Task Force (DMTF) has defined RMCP for supporting pre-OS and OS-absent management. RMCP is a simple request-response protocol that can be delivered using UDP (User Datagram Protocol) datagrams. IPMI-over-LAN uses version 1 of the RMCP protocol and packet format. An RMCP packet is transmitted via IP (Internet Protocol) networking. Thus, system managers may manage their IPMI-enabled system over the Internet. (Of course, in a private LAN this is a basic feature.) IPMI uses the same UDP port number (623 in decimal) with 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 shares the LAN1 NIC on the mainboard. The NIC will re-route the IPMI packet to the BMC instead of forwarding it to the upper layer network protocol stacks (as other protocol packets do).

IPMI View V2.0 covers Supermicro’s BMCs for both IPMI v1.5 and IPMI v2.0. However, according to design changes, some functions added to IPMI v2.0 are not available in IPMI v1.5, and some functions are no longer available in IPMI v2.0 implementation. IPMI View will automatically hide any function that is not available to the BMC version being used.

## II. System Management:

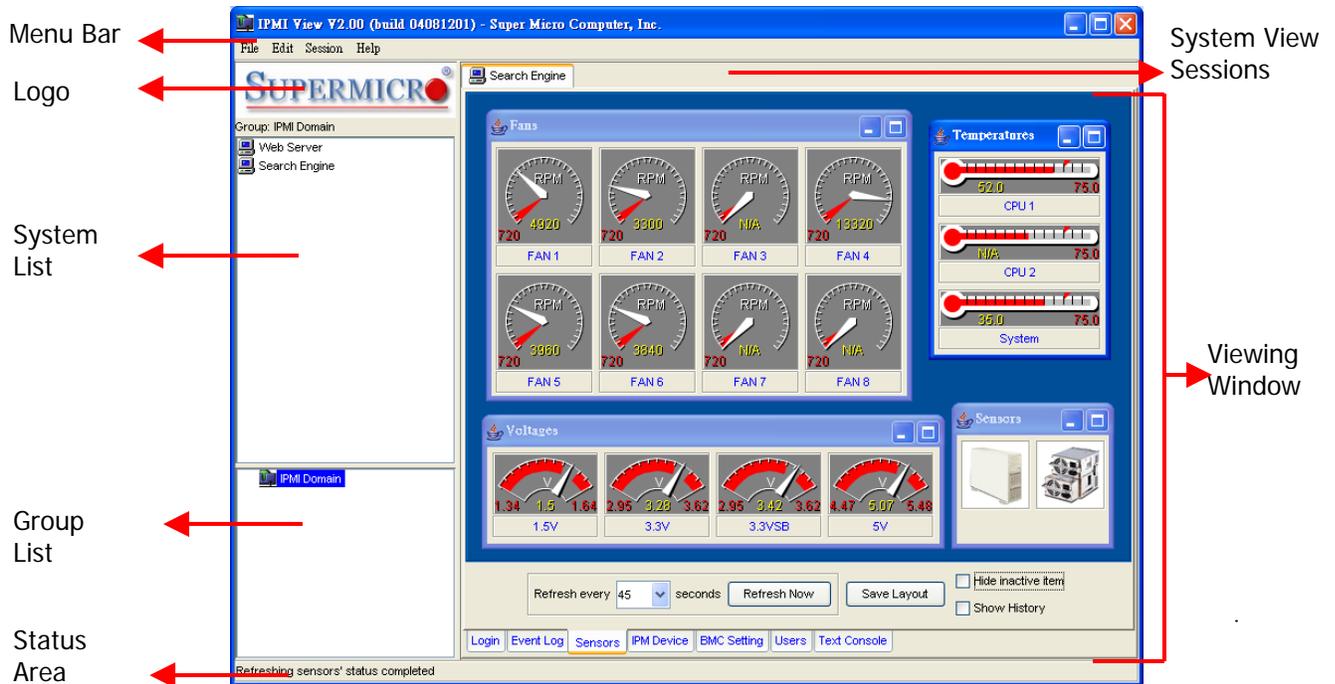


Figure 2-1

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

- 1) **Menu Bar:** contains functions allowing you to add/delete systems or groups and save configurations.
- 2) **System List:** lists the computers managed with a BMC card.
- 3) **Group List:** lists managed computer groups for more convenient management.
- 4) **Viewing Window:** shows detailed information including Login, IPMI Device, Event Log, Sensors, BMC Setting and Text Console.
- 5) **Status Area:** shows messages regarding current status.
- 6) **System View Sessions:** IPMI View may manage up to 20 systems at the same time. The current managed system is indicated in the System View window.
- 7) **Logo:** Press Logo to visit Supermicro's web site.

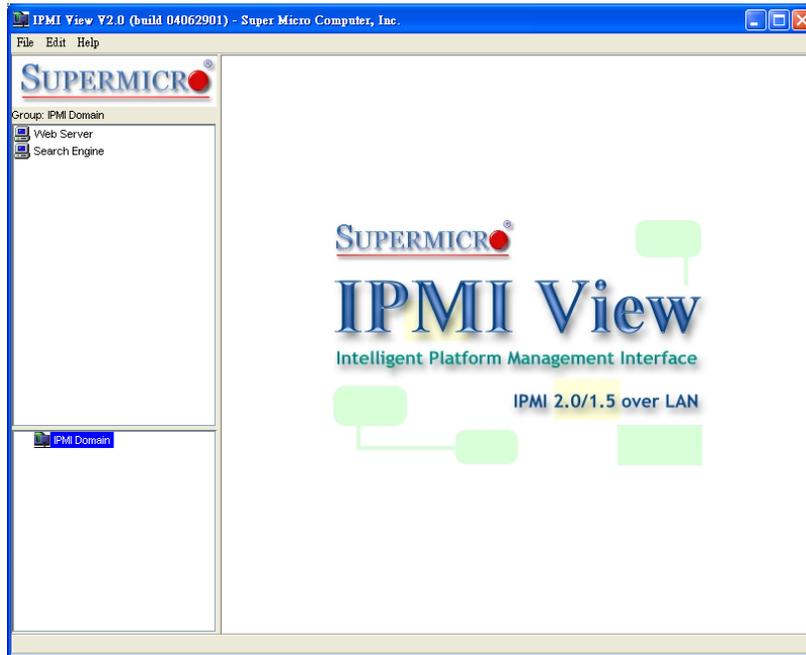


Figure 2-2

- Adding a new system to IPMI View

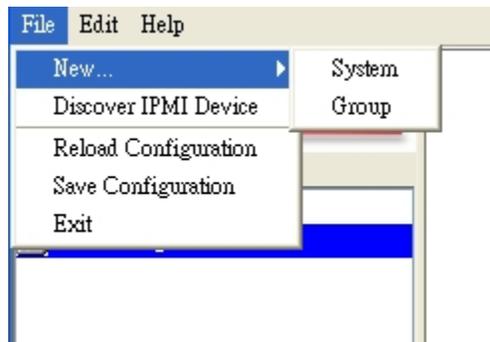


Figure 2-3

As shown in Figure 2-3, click “File>New...>System” to add a new system to IPMI View. An “Add a new system...” dialog box will pop up as shown in Figure 2-4.

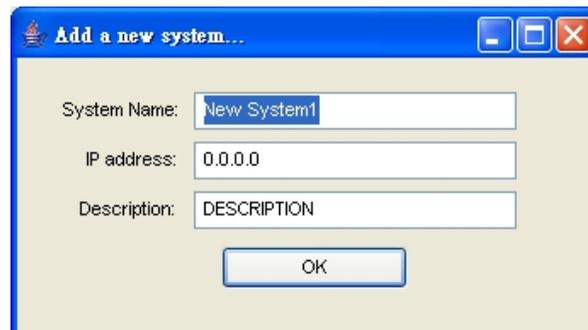


Figure 2-4

In the “Add a new system” dialog box, type in the desired System Name for the managed system and the correct IP address, as well as a description. Then click OK.

- **Adding a new group to IPMI View**

To maintain systems easier, the manager may categorize managed systems into different groups. A system may be included in multiple groups. The default group is IPMI Domain. All managed systems belong to IPMI Domain even if they join other groups.

In Figure 2-3, click menu “File>New...>Group” to add a new group to IPMI View. An “Add a new group” dialog will pop up as shown in Figure 2-5.



Figure 2-5

In the “Add a new group” dialog box, type in the desired Group Name and description. Then click OK.

- **Discover New Systems in a Specified Network**

IPMI View includes a function that allows the user to collect candidate system information in order to build their information into a System List (see Figure 2-6). User may specify the IP range to search any possible system that has either IPMI 1.5 or IPMI 2.0 capability. After the candidate system information is collected, the user may add systems into a System List by IP addresses, or by a given Prefix name.

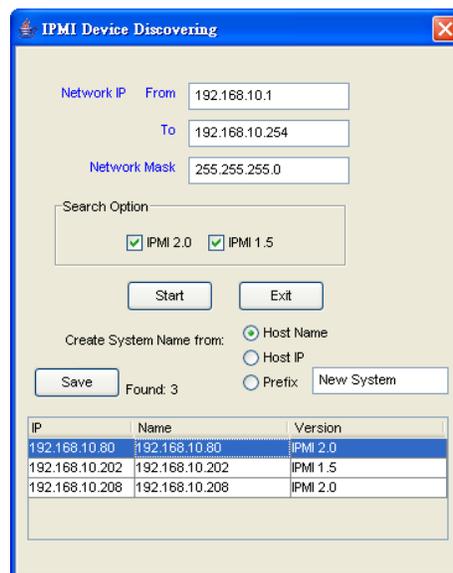


Figure 2-6

- **Reload Configuration**

From the pull-down menu, click “File>Reload Configuration” to load the previous saved configuration.

- **Save Configuration**

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

- **Exit IPMI View**

From the pull-down menu, click “File>Exit” or press Alt-F4 when the IPMI View is running to exit IPMI View. Remember to save your configuration before exiting.

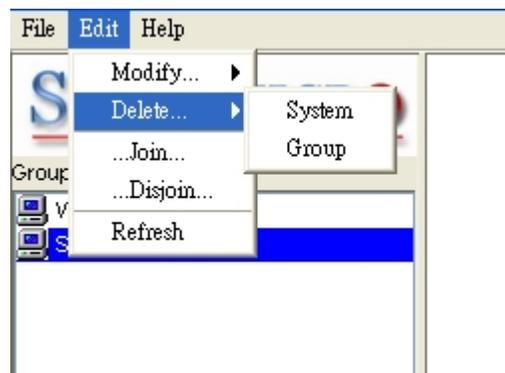


Figure 2-7

- **Modify System**

Select a system in the System Window you want to modify and then click “Edit>Modify...>System” from the pull-down menu shown in Figure 2-7 to modify it.

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

- **Delete System**

Select a system in the System Window you want to delete and then click “Edit>Delete...>System” from the pull-down menu shown in Figure 2-7 to delete it.

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

- **Modify Group**

Select a group in the Group Window you want to modify and then click “Edit>Modify...>Group” from the pull-down menu shown in Figure 2-7 to modify it.

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

- **Delete Group**

Select a group in the Group Window you want to delete and then click "Edit>Delete...>Group" from the pull-down menu shown in Figure 2-7 to delete it.

You can also right click on a group in the Group Window and then select "Delete" in the pop-up menu to delete it.

- **Join a group**

Select a group in the Group window and select a system in the System Window, then click "Edit>...Join..." from the pull-down menu shown in Figure 2-7 to have the selected system join the desired group.

- **Disjoin a group**

Double click the group you want to disjoin a system from. The members of that group will appear in the System Window. Then, select the system you want to disjoin and click "Edit>...Disjoin..." from the pull-down menu shown in Figure 2-7.

You can also right click the selected system to disjoin the system from the group and then select "Disjoin" in the pop-up menu to delete it.

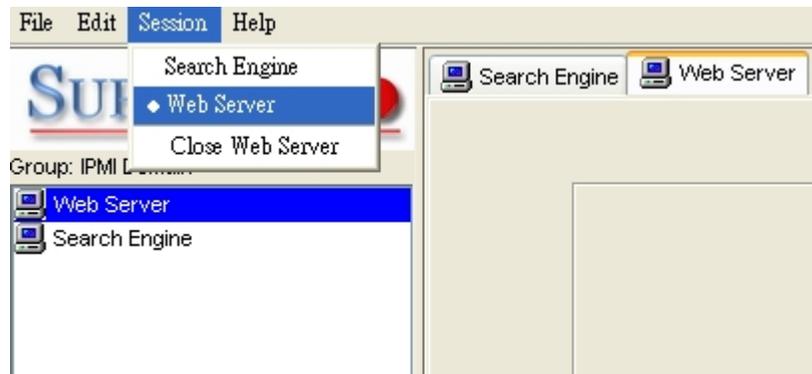


Figure 2-8

- **Selecting an IPMI View management session**

When more than one system is managed by IPMI View at the same time, you can select which opened management session you want to control by double clicking on system's name in the System Window or by selecting "Session<<System name>>" in the pull-down menu, where <<System name>> denotes the name of the target system you want to control (as shown in Figure 2-8).

- **Closing IPMI View management session**

To close the opened IPMI View management session, select the IPMI View management session you want to close as the current IPMI View management session and then click “Session>Close <<System name>>” in the pull-down menu, where <<System name>> denotes the name of the system you want to close (as shown in Figure 2-8).

Or - right click on the system in the System Window you want to close and select “Close Session” in the pop-up menu to close it.

When closing a session, a session will not be closed until 1) replies have been received for all outstanding packets or 2) all outstanding packets have timed out.

### III. Login

- Login

In Figure 3-1, double click the system in the System Window you want to manage. A login screen along with some information about the managed system will appear in the Viewing Window. Type in the login ID and password and click the Login button to log in. When a login is successful, the Login button is grayed (i.e. disabled) and the Logout button is enabled as well as the availability of other management functions, as shown in Figure 3-2.

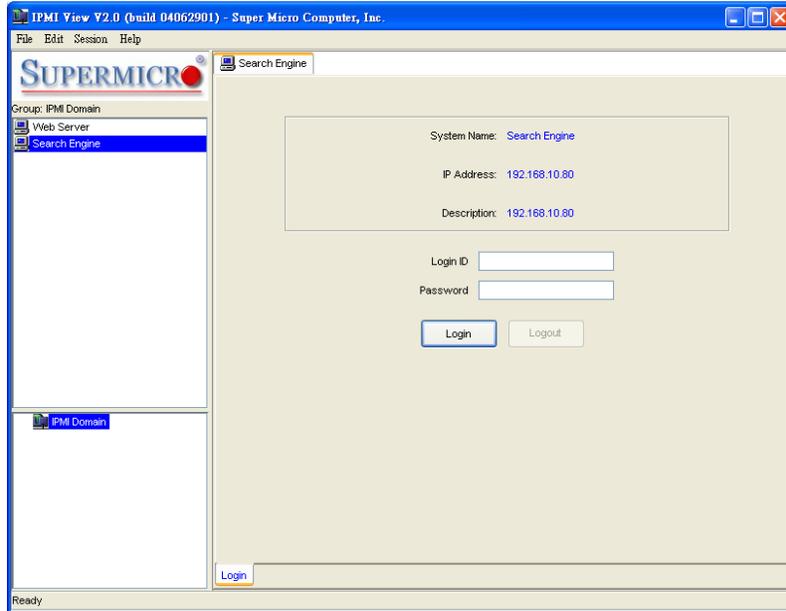


Figure 3-1

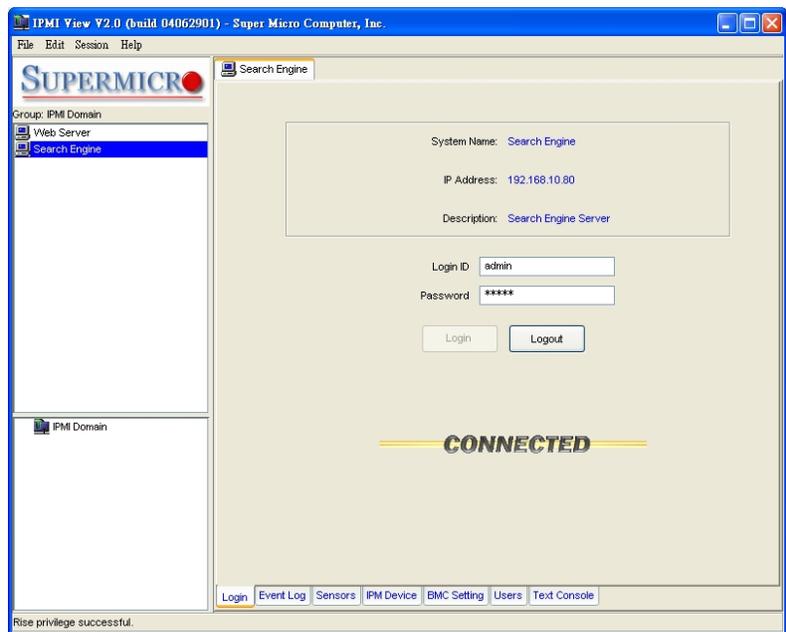


Figure 3-2

The default Login ID is “ADMIN”, which has the default password of “ADMIN”. Both the Login ID and Password are case-sensitive.

In the IPMI design, an MD5 algorithm will encrypt the password when it’s transmitted through the network. Once the password is confirmed, IPMI View will show a CONNECTED symbol, and all available function pages will be shown as seen in Figure 3-2. If the password is invalid, it will show a message 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).

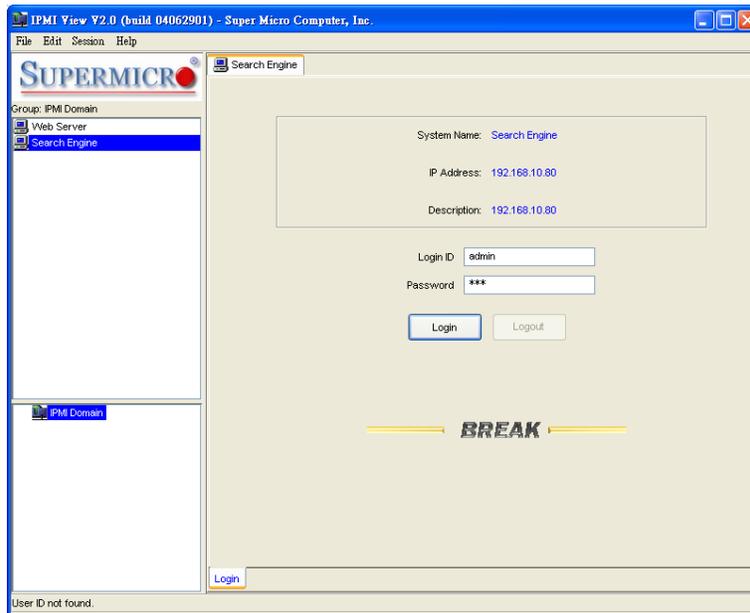


Figure 3-3

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

## IV. IPM Device



Figure 4-1

Clicking the IPM Device tab of the IPMI View management session in the Viewing Window (shown in Figure 4-1) will display some information and functions of the system's BMC firmware.

- **Device Information**

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

- **ACPI System Power State**

This shows the managed system's power state. If the managed system is in a power-off state, the green light will be off. This status will update 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/power-cycle within a specified time (the default 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 managed system's monitor and start a count down. This pop-up notice window gives the user who is working on the system a chance to save any working files. However, remote login users or service users (for example Web site visitors) will not see this notice.

**Graceful Shutdown:** same as the shutdown function in Windows. The managed system will enter an S5 state.

**Graceful Reboot:** same as the reboot function in Windows.

**Graceful Power Cycle:** this function is a combination of the Graceful Shutdown and Power Up functions.

The Power Cycle function will shut down the managed system for a few seconds and then power up the system. Graceful power control will send an event to the System Event Log (next section). If no more memory space is left for the incoming event, graceful power control will not function.

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

This function is used to forcibly control the power state of the managed system's chassis. When the BMC receives a chassis power control command, it will have direct control over the power button or reset button of a system.

**Reset:** this is the same as pressing the Reset button on a managed system's chassis to reset the managed system.

**Power Down:** this is the same as pressing the Power button on a managed system's chassis to remove power from the managed system.

**Power Up:** this is the same as pressing the Power button on a managed system's chassis to turn on the power of the managed system.

**Power Cycle:** this function is a combination of the Power Down and Power Up functions.

The Power Cycle function will shutdown the managed system for a few seconds and then power up the system.

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

Clicking the Cold Reset button allows you to reset the BMC. After confirming to reset the BMC, the session will break immediately. The user has to close this session manually. This function is rarely used, only in events such as when a malfunction is suspected.

## V. System Event Log

The screenshot shows the 'System Event Log' interface. At the top, it displays 'SEL Version: 1.5', 'Total Entries: 132', 'Free Space: 6080 bytes', 'Recent Entry Added: 07/01/2004 11:47:15', and 'Recent Entry Erased: 06/29/2004 14:40:13'. Below this is an 'Export Entries' section with radio buttons for 'All' (selected) and 'From' (with input fields for '1' and '132'), and 'Get' and 'Export' buttons. A table of events is shown with columns: Event, Type, Timestamp, Sensor Type, Sensor, and Event Type. The table contains 9 rows of system events. Below the table is a 'Clear All Entries' button. At the bottom, there is a 'Current SEL Device Timestamp' field with the value '07/01/2004 16:00:24 Thu' and a 'Set Timestamp' button, and a 'Refresh' button. A navigation bar at the very bottom includes tabs for 'Login', 'Event Log' (selected), 'Sensors', 'IPM Device', 'BMC Setting', 'Users', and 'Text Console'.

Event	Type	Timestamp	Sensor Type	Sensor	Event Type
1	System Event	06/29/2004 14...	Fan	Fan4	Assertion: Lower Non...
2	System Event	06/29/2004 14...	Fan	Fan4	Assertion: Lower Critic...
3	System Event	06/29/2004 14...	Fan	Fan4	Assertion: Lower Non...
4	System Event	06/29/2004 14...	Fan	CPU2	Assertion: Lower Non...
5	System Event	06/29/2004 14...	Fan	CPU2	Assertion: Lower Critic...
6	System Event	06/29/2004 14...	Fan	CPU2	Assertion: Lower Non...
7	System Event	06/29/2004 14...	Fan	CPU2	Assertion: Lower Non...
8	System Event	06/29/2004 14...	Fan	CPU2	Assertion: Lower Critic...
9	System Event	06/29/2004 14...	Fan	CPU2	Assertion: Lower Non...

Figure 5-1

Clicking on the Event Log tab of the IPMI View management session in the Viewing Window (shown in Figure 5-1) gives you detailed information on the System Event Log for the BMC. It shows the System Event Log version, number of log entries, free space for the System Event Log and the times of recently added and recently erased System Event Logs.

- **Get System Event Log**

In the Get Entries group on the upper left side of the Event Log tab in the Viewing Window, you can decide how many logs you want to get from the BMC. Click the From button and type in the first and last numbers of the logs you wish to view, or click the All button to get all the logs from the BMC. The logs retrieved from the BMC will be listed as a table in the central part of the Viewing Window. Please refer to the IPMI specifications version 2.0 for detailed descriptions of each field. Some helpful fields:

**Timestamp:** the time the event happened.

**Sensor Type:** this could be health sensors or a system event.

**Event Type:** the event description.

Because the BMC communicates with the NIC on the mainboard via a slow channel, requesting only the events you need to see is recommended. Choosing "all" to get hundreds of event entries will result in a very long delay.

- **Clear System Event Log**

Clicking the Clear All Entries button clears the logged system events on the BMC. The total event log space is 16 KB. When all this space is used, any incoming event will be lost. The user has to clear the system event log manually as needed.

- **Time stamp of System Event Log and Time Zone**

To set the time stamp of the BMC on the managed system, type in the time in the Current SEL Device Timestamp field. Then click the Set Timestamp button to update the BMC.

Timestamp and Time Zone reflect the managed system's local time.  
(Time Zone setting is only available for IPMI 1.5)

## VI. Sensors

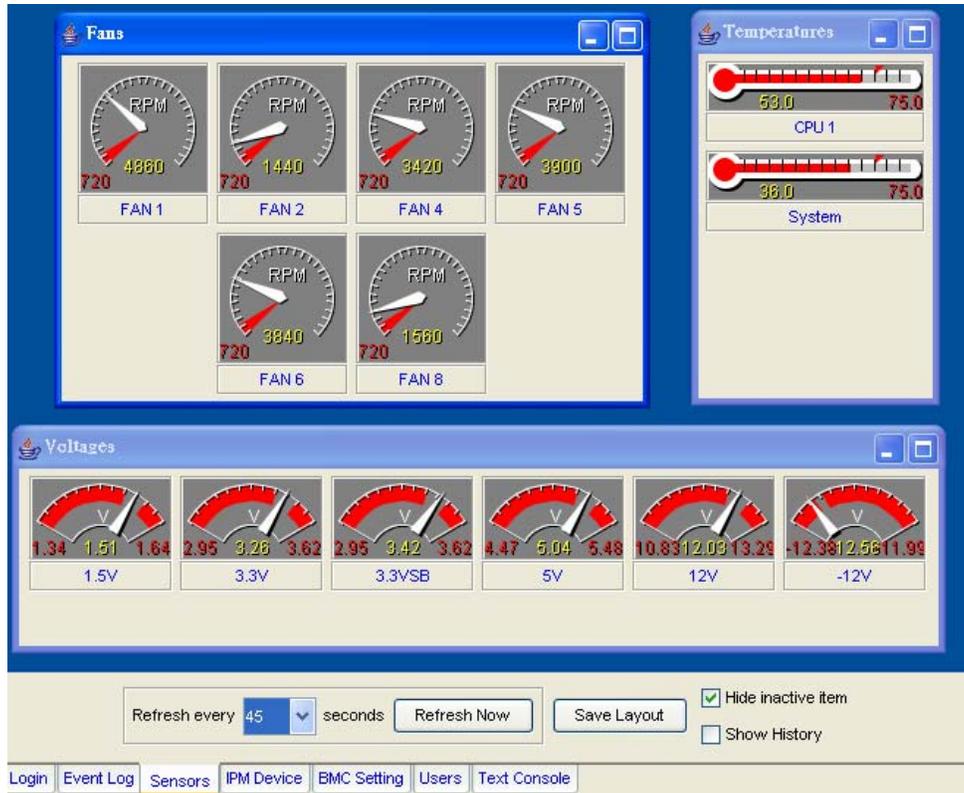


Figure 6-1

Clicking on the Sensors tab of the IPMI View management session in the Viewing Window (as shown in Figure 6-1) provides you with detailed information on the sensors monitored by the BMC. It shows the reading of supported voltages and fan speeds and temperatures monitored by the BMC. The current reading is shown in yellow numbers, the high limits/low limits in red numbers and a description for the monitoring sensors in blue text beneath the monitoring sensor figures.

Fan speeds have only a low limit, temperatures have only a high limit, and voltages have both high and low limits.

- **Refreshing monitor status**

You can configure the IPMI View to automatically refresh the monitoring status periodically by checking the Auto Refresh check box and selecting the refresh period in seconds in the seconds list. Or, click the Manual Refresh button to refresh the monitoring status every time you need an update.

- **Hide inactive item**

IPMI View gets predefined sensor information from the mainboard. Some items may be not installed for different configurations. For example, there will be no CPU fan if using a passive CPU heat sink, and only one CPU on a dual CPU mainboard that has only a single CPU installed. The first time the sensors page is shown, IPMI View will hide inactive items (the default setting) if any. A manager may change this option later by un-checking the “Hide inactive item” box, as shown in Figure 6-2.



Figure 6-2

- **Show History**

IPMI View provides a history chart for fans, temperatures and voltages. The yellow line indicates the reading correspond to sensor. A red line indicates a high or low limit. A blue line indicates the base value of 0 (zero). Check the “Show History” box to display these charts, as shown in Figure 6-3.

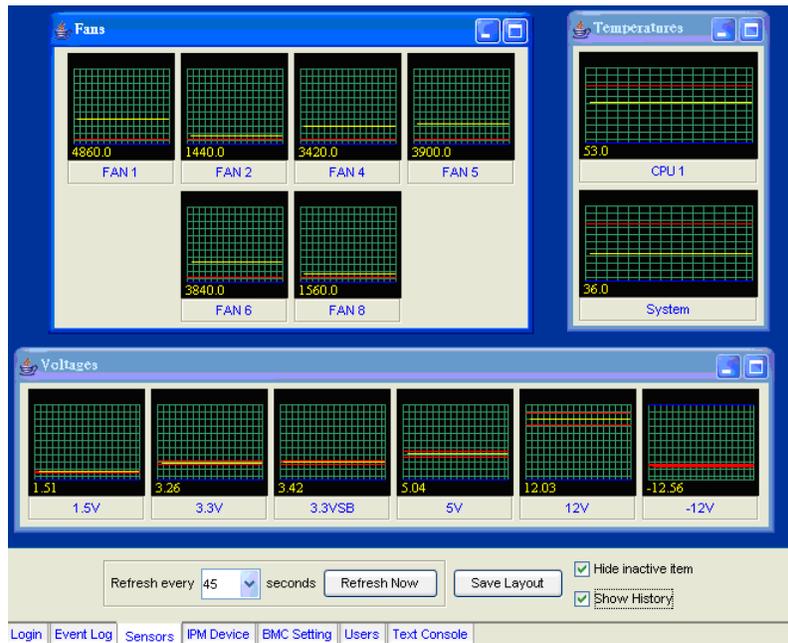


Figure 6-3

## VII. BMC Setting (Administrator only)

The screenshot shows a web-based configuration interface for BMC settings. It is divided into two main sections: BMC LAN Configuration and SNMP.

**BMC LAN Configuration:**

- IP Address: 192.168.10.80
- LAN MAC: 00:30:48:20:B8:52
- Gateway IP: 192.168.0.1
- Gateway MAC: 00:00:0C:07:AC:09
- Subnet Mask: 255.255.255.0
- A pink error message states: "LAN MAC must be correct while update"
- An "Update" button is present.

**SNMP:**

- Community: public
- SNMP Trap Receivers table:

IP Address	MAC Address
192.168.10.28	00:30:48:70:7E:C6
192.168.10.107	00:06:1B:D9:91:60

At the bottom of the interface, there is a "Refresh" button and a navigation bar with tabs: Login, Event Log, Sensors, IPM Device, **BMC Setting** (selected), Users, and Text Console.

Figure 7-1

Clicking on the BMC Setting tab of the IPMI View management session in the Viewing Window (as shown in Figure 7-1) gives you detailed information on the BMC LAN Configuration, SNMP trap configuration and serial communication port of the BMC.

In order to support the power-down state management capability under the IPMI specification, the manager has to configure the proper MAC address for each IP address. To deliver an IP packet to a receiver, the sender needs to know the receiver's MAC address or the gateway's MAC address. ARP (Address Resolution Protocol) is used to get the MAC address from the IP address. While the managed system's OS is running, the network protocol stack will take care of this function. However, when the managed system is in a power down state, this function cannot be accomplished. Therefore, each MAC address has to be configured manually.

The BMC and the OS running on a managed system may use different IP addresses for security reasons. For example, the OS may use 66.201.4.73 (which can be reached by public access) while the address for BMC may be set to 192.168.1.55, which can only be reached in a private LAN. But, LAN MAC addresses must be the exact same. If the BMC uses a private IP address, you have to make sure that the manager's system can communicate with the private IP address for the BMC on a managed system.

- **BMC LAN Configuration**

This shows the IP address, LAN MAC, Gateway IP, Gateway MAC and Subnet Mask of the BMC and allows you to modify them. 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, IPMI View 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.

- **SNMP**

This shows the SNMP trap configuration of the system needing to receive the SNMP traps generated by the BMC and allows you to modify them. To change the configuration on the BMC, type in the SNMP community name in the Community text field and the IP address and MAC address in the SNMP Trap Receivers table in the SNMP group, and 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, and then click Update.

On the system receiving the SNMP traps, an SNMP trap receiver software needs to be installed and run. The managed system will send out an SNMP trap packet to receivers at the moment the event occurs. If an SNMP trap receiver is not running, the trap packet is discarded and won't be queued anywhere.

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

This shows 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 is a dedicated serial port.

**Baud Rate:** the baud rate for serial connections (does not affect paging settings).

**Modem Init String:** the modem initialization string for serial connections (does not affect paging settings).

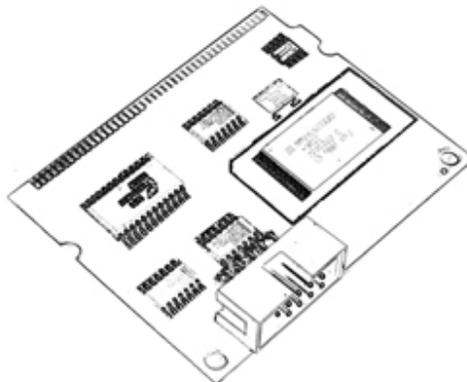


Figure 7-2

## VIII. Users

**USERS**

User Name: ADMIN

Privilege: Administrator

---

**FRU**

Board | Product

Language Code: 0 Mfg. Date/Time: 000

Board Manufacturer: Super Micro Board Product Name: IPMI2.0

Board Serial Number: Board Part Number: AOC-IPMI20-E

[Login](#)
[Event Log](#)
[Sensors](#)
[IPM Device](#)
[BMC Setting](#)
[Users](#)
[Text Console](#)

Figure 8-1 (For IPMI 2.0)

**USERS**

User Name: ADMIN

Privilege: Administrator

Paging: Enable

---

**PAGING SEVERITY**

System Power: Warning	Security: Warning
Temperature Sensors: Warning	System Status: None
Fans: Warning	Disk Drives & Controllers: Critical
Memory Errors: Critical	Network Interface: Warning
Critical H/W Errors: All	Remote Management: Critical
System Hang: Critical	Others: None
POST Errors: All	<input type="button" value="Update"/>

[Login](#)
[Event Log](#)
[Sensors](#)
[IPM Device](#)
[BMC Setting](#)
[Users](#)
[Text Console](#)

Figure 8-2 (For IPMI 1.5)

Clicking on the Users tab of the IPMI View management session in the Viewing Window (as shown in Figure 8-1 and 8-2) gives you detailed information on the Users management, and the thresholds for paging severity for IPMI 1.5.

**We strongly suggest you change passwords immediately to prevent malicious users getting control before you.**

- **USERS**

There are several buttons that allow you to add/delete a user, set user privileges, change passwords and enable/disable paging.

There are six privilege level groups, Callback, User, Operator, Administrator, OEM, and No Access. Only the first four privilege levels are implemented. Privilege Levels determine which IPMI commands a given user can execute over a given channel. Privilege Limits set the maximum privilege level that a user can operate at. A user is configured with a given maximum privilege limit for each channel. Thus, a user can operate at a privilege level that is no higher than his group privilege limit.

Group Privilege Levels

Callback	This may be considered the lowest privilege level. Only commands necessary to support initiating a Callback are allowed. (Only available for IPMI 1.5.)
User	Only 'benign' commands are allowed. These are primarily commands that read data structures and retrieve status. Commands that can be used to alter BMC configuration, write data to the BMC or other management controllers or perform system actions such as resets, power on/off, and watchdog activation are not allowed.
Operator	All BMC commands are allowed, except for configuration commands that can change the behavior of the out-of-band interfaces. For example, Operator privilege does not allow the capability to disable individual channels or change user access privileges.
Administrator	All BMC commands are allowed, including configuration commands. An Administrator can even execute configuration commands that would disable the channel that the Administrator is communicating over.

Clicking on Paging Setting allows you to set the parameters for an individual user (Figure 8-3). There are two types of paging service: 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).

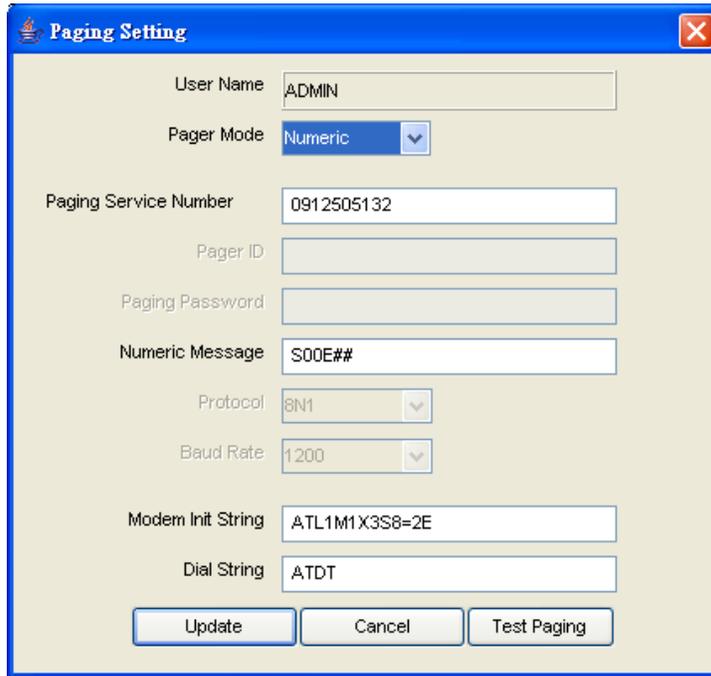


Figure 8-3

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

Here may be found useful information about the board and product, for example the serial number, part number and part name of the board and product.

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

The paging severity settings define when users will be notified of entries in the system event log (SEL).

The following settings are available for each group:

<b>None</b>	When this is selected, user notification for this group is inactive.
<b>Warning</b>	When this is selected, the RMC will notify users when SEL entries for the group exceed the warning thresholds.
<b>Critical</b>	When this is selected, the RMC will notify users when SEL entries for the group exceed the critical thresholds.
<b>All</b>	When this is selected, the RMC will notify users of all SEL entries of events for the group.

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

## IX. Text Console Redirection (SOL, Serial Over LAN)

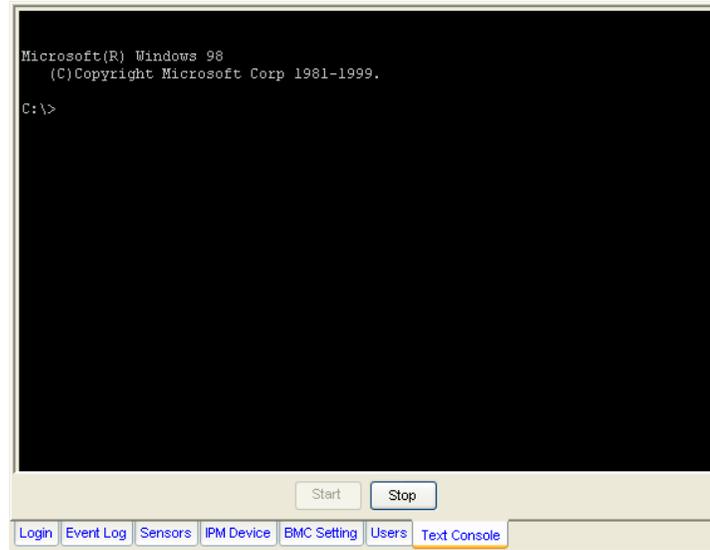


Figure 9-1

On the Text Console tab of the IPMI View management session in the Viewing Window (as shown in Figure 9-1), there is a function for you to remotely control the managed system in a text mode console. Click the Start button to start the text console redirection. During control, click the ReSynch button to synchronize the text console with the managed system if you think the screen is not shown properly. Click the Stop button to stop the text console.

- BMC for IPMI 1.5

Console Redirection is not a function in the IPMI specification V1.5. Supermicro provides this useful function for a manager to control the managed system remotely. When a managed system is booting up and in the POST routine and no other software application can give you control to redirect the console, IPMI View offers this valuable function. Console Redirection will dump a managed system's screen to IPMI View and send the key codes you entered in the managed system.

When a managed system switches its video mode from Text Mode to Graphics Mode, a terminate notice will be sent to IPMI View to terminate the console redirection. Text Console Redirection only works for text mode.

**Important:** Console Redirection puts a very heavy load on a managed system. It will dump the whole screen to the manager's system and slow down the managed system significantly. We suggest you use this function only when you need to get special control and cannot achieve it any other way. For other applications, a proper console redirection software application (pcAnywhere, Symantec Corporation) or a remote login protocol (telnet) is suggested. 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

IPMI specification V2.0 defines Serial Over LAN (SOL) to support Text Console Redirection. This implementation performs better than the one we implemented for IPMI 1.5. The Text mode console remains working on Windows 2003, even when the OS is running. To support Text Console

Redirection on Windows 2003, Special Administration Console (SAC) must be enabled. The following instruction is used to enabled SAC:

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

```
[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
```