Supermicro IPMIView

User's Guide

Revision 2.21.1

The information in this USER'S GUIDE has been carefully reviewed and is believed to be accurate. The vendor assumes no responsibility for any inaccuracies that may be contained in this document, makes no commitment to update or to keep current the information in this manual, or to notify any person organization of the updates. Please Note: For the most up-to-date version of this manual, please see our web site at www.supermicro.com.

Super Micro Computer, Inc. ("Supermicro") reserves the right to make changes to the product described in this manual at any time and without notice. This product, including software, if any, and documentation may not, in whole or in part, be copied, photocopied, reproduced, translated or reduced to any medium or machine without prior written consent.

DISCLAIMER OF WARRANTY ON SOFTWARE AND MATERIALS. You expressly acknowledge and agree that use of the Software and Materials is at your sole risk. FURTHERMORE, SUPER MICRO COMPUTER INC. DOES NOT WARRANT OR MAKE ANY REPRESENTATIONS REGARDING THE USE OR THE RESULTS OF THE USE OF THE SOFTWARE OR MATERIALS IN TERMS OF THEIR CORRECTNESS, ACCURACY, RELIABILITY, OR OTHERWISE. NO ORAL OR WRITTEN INFORMATION OR ADVICE GIVEN BY SUPER MICRO COMPUTER INC. OR SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE SHALL CREATE A WARRANTY OR IN ANY WAY INCREASE THE SCOPE OF THIS WARRANTY. SHOULD THE SOFTWARE AND/OR MATERIALS PROVE DEFECTIVE, YOU (AND NOT SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE) ASSUME THE ENTIRE COST OF ALL NECESSARY SERVICE, REPAIR, OR CORRECTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES INCLUDING NEGLIGENCE, SHALL SUPER MICRO COMPUTER INC. BE LIABLE FOR ANY INCIDENTAL, SPECIAL, OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OR INABILITY TO USE THE SOFTWARE OR MATERIALS, EVEN IF SUPER MICRO COMPUTER INC. OR A SUPER MICRO COMPUTER INC. AUTHORIZED REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

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

Manual Revision: 2.21.1
Release Date: 2023/05/25

Unless you request and receive written permission from Super Micro Computer, Inc., you may not copy any part of this document.

Information in this document is subject to change without notice. Other products and companies referred to herein are trademarks or registered trademarks of their respective companies or mark holders.

Copyright © 2023 by Super Micro Computer, Inc.
All rights reserved.
Printed in the United States of America

Document Revision History

Date	Revision	Description
2016/02/24	2.11.0	Added document revision history.
2016/10/18	2.13.0	Added details to the sensor section.
2018/02/12	2.14.0	Added the BMC support list to *Appendix G*.
2018/08/30	2.15.0	Add Q&A to *Appendix G*.
2019/11/18	2.17.0	Added Maintenance event log.
2020/01/12	2.19.0	Added IPv6 configurations to the BMC Settings. Added the Next Boot option. Added *Appendix G*, *Appendix H* and *Appendix K*. Moved the Q & A section to *Appendix I*.
2021/01/21	2.20.0	Added sensor text view in Chapter 5 Updated UI for user management in Chapter 8
2022/09/21	2.21.0	Added RAKP related information to Chapter 3 and Chapter 7. Added the DateTime feature to Chapter 7. Added the device information to Chapter 6. Added the descriptions of Stunnel properties to Appendix I.
2023/05/25	2.21.1	Added the BMC warm reset to Chapter 6. Added the IPMIView Software Update to Chapter 14.

Contents

1 Overview 6

2 System Management 7

3 Login 16

4 Event Log 20

5 Sensors 22

5.1 Graphic View 22

5.1.1 Discharging Battery 23

5.2 Text view 24

6 IPMI Devices 25

7 BMC Settings 28

8 Users 32

8.1 Users Account 32

8.1.1 Advanced Setting 34

8.2 FRU Information 35

9 Text Console Redirection (SOL- Serial-Over-LAN) 36

10 KVM Console (KVM-Over-IP for Video Redirection) 39

11 Virtual Media 51

11.1 SIM Module 51

11.2 SIM (WA) Module 55

12 Group Management 56

13 Trap Receiver 69

14 IPMIView Software Update 79

Appendix A: SIM Firmware Update 81

Appendix B: SIM(W) KVM Console and Virtual Media 84

Appendix C: SIM (WA) iKVM Console and Virtual Media 88

Appendix D: SIM (W) Firmware Update 92

Appendix E: SIM (WA) Firmware Update 96

Appendix F: ASPEED X10 Firmware Update 99

Appendix G: ASPEED X12 Firmware Update 101

Appendix H: Updating ASPEED X12 BIOS 103
Appendix I: Node Product Key Functions 105
Appendix J: Stunnel Properties 106
Appendix K: Q&A 107
Q: Why can't I save a configuration/open KVM window on Windows platform? 107
Q: How can I enable automatic log monitoring in IPMIView? 107
Q: Why does a permission error appear when I install Supermicro on Windows? 108
Q: Why can't I launch IPMIView after installation? 108
Q: Why does my Trap Receiver icon become ? 108
Appendix L: Supported BMC List 109
Appendix M: Third-Party Software 110
Contacting Supermicro 111

1 Overview

IPMIView (IPMI-Over-LAN) 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 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 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) network, which allows 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

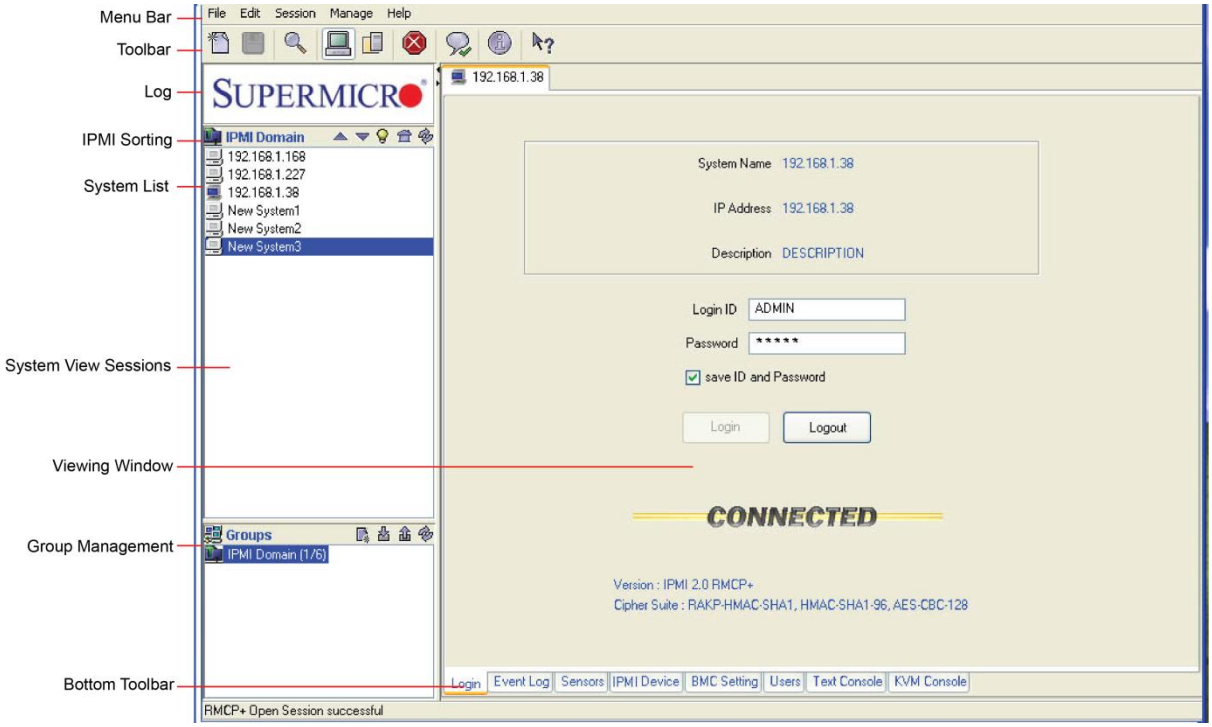


Figure 2-1

- **Menu Bar:** contains functions that allow you to add/delete systems or groups and save configurations.
- **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.
- **Logo:** Click the Logo icon to visit Supermicro's website.
- **IPMI Sorting:** This allows you to sort devices in ascending/descending order via the online format, or in their original sequence.
- **System List:** This lists the computers managed by the BMC Controller.
- **Group Management:** This allows the user to manage system groups, including creating/adding new accounts, deleting accounts and updating group information.
- **Group List:** This lists the computer groups managed by the BMC for better management.

- **Viewing Window:** This shows detailed information including Login, IPMI Device, Event Log, Sensors, BMC Settings, and the status of the IPMIView firmware.
- **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.
- **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, and KVM Console.

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

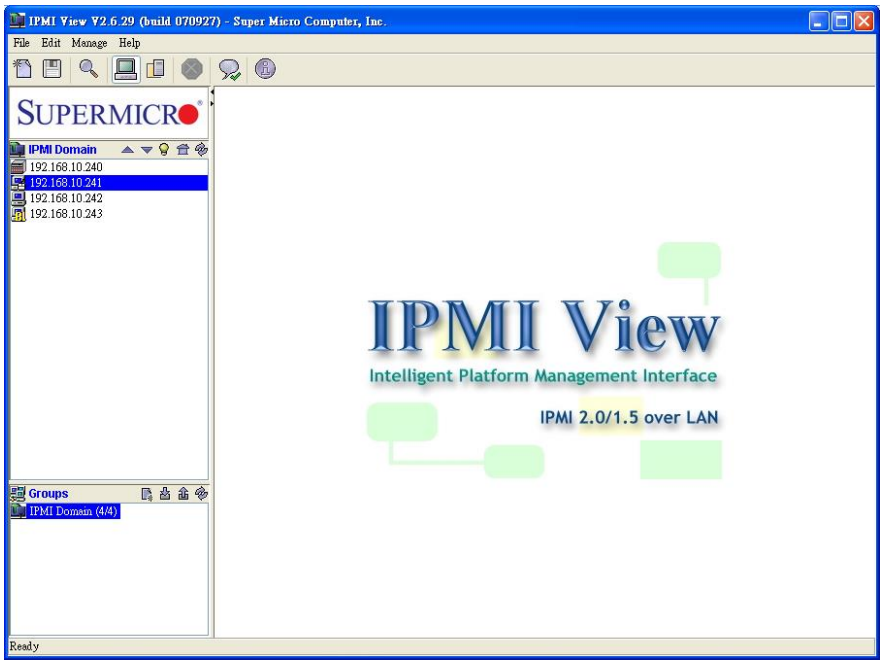


Figure 2-2

- **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 BMC management.

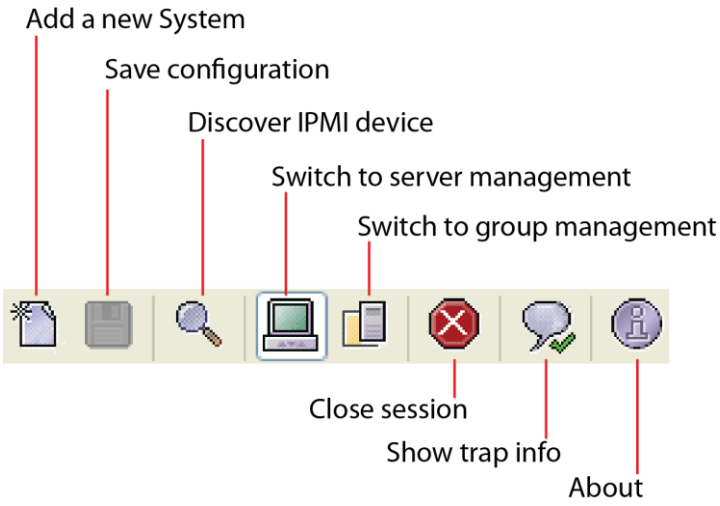


Figure 2-3

- **Adding a new system**

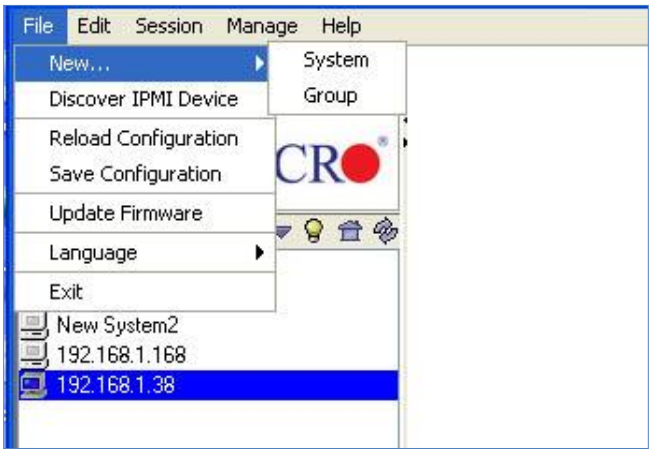


Figure 2-4

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

Click **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 network Mask, then click **Detect** or **Start** to search for 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.

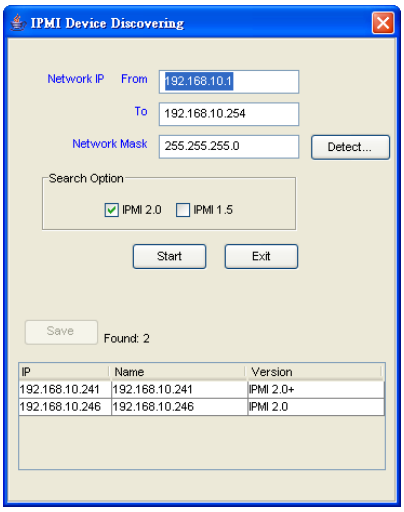


Figure 2-7

- **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 (Traditional), Chinese (Simplified) or English as your IPMI language setting.

Note: There may be Chinese display issues in some Linux systems that lack Chinese fonts for JVM. You can install Chinese fonts, e.g., SimSun.ttf, and then type the following commands: `mkfontscale`, `mkfontdir` and `fc-cache -fv` at the font path to fix the issue.

- **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.

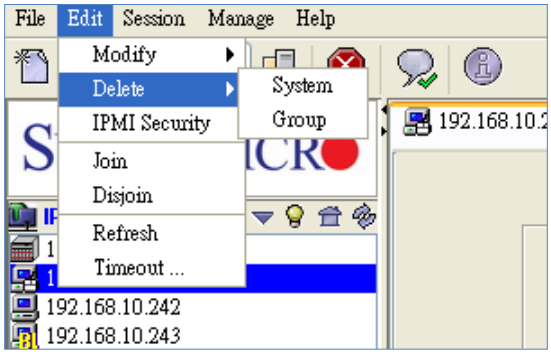


Figure 2-8

- **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 **For 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 **Encryptor** 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.

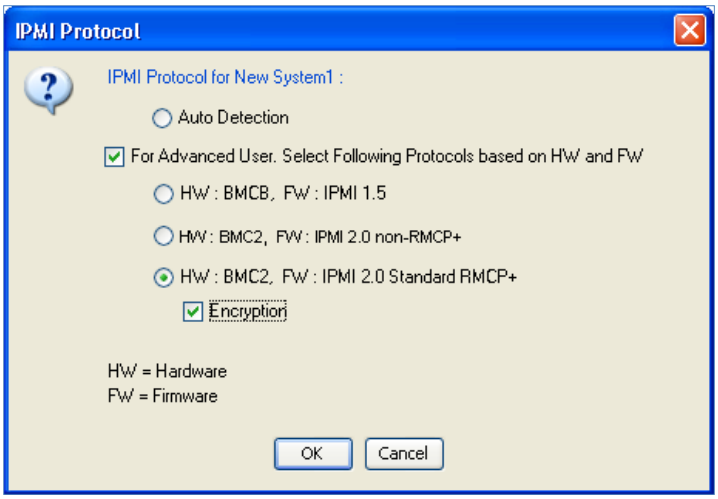


Figure 2-9

- **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.

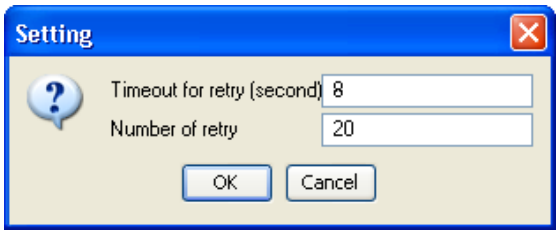


Figure 2-10

- **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).

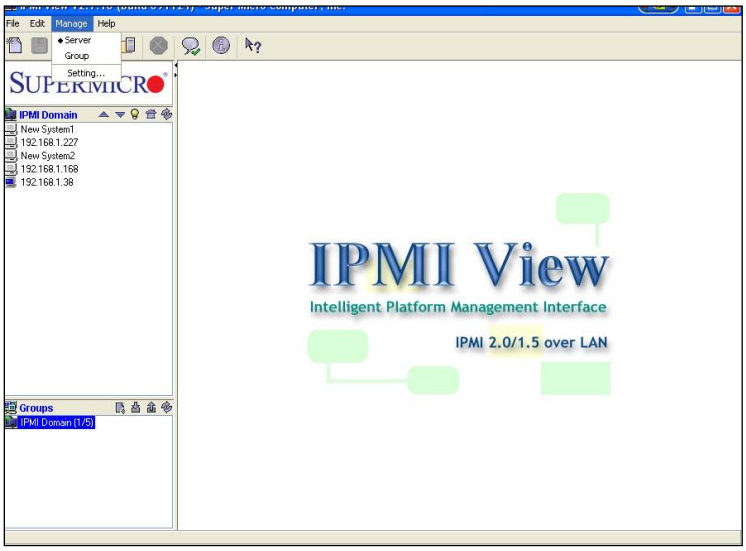


Figure 2-11

- **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.

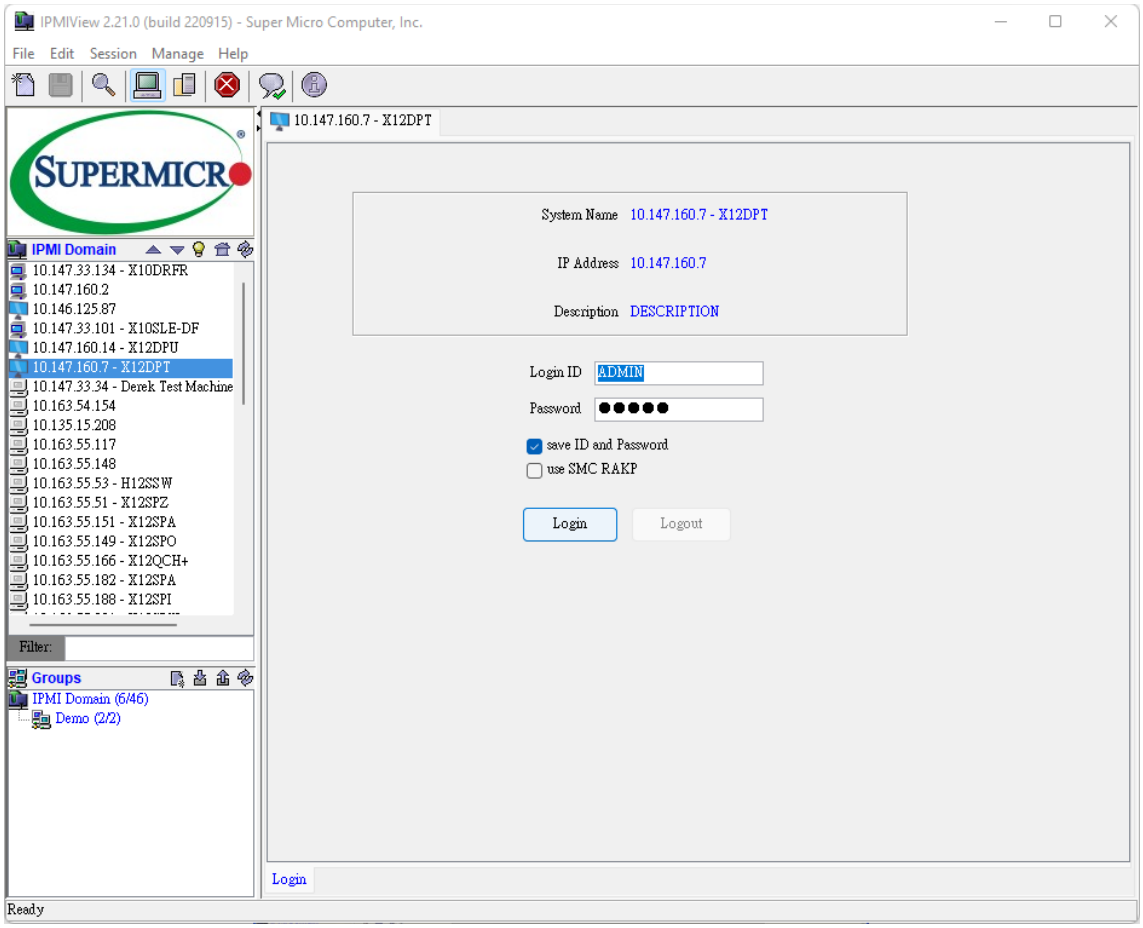


Figure 3-1

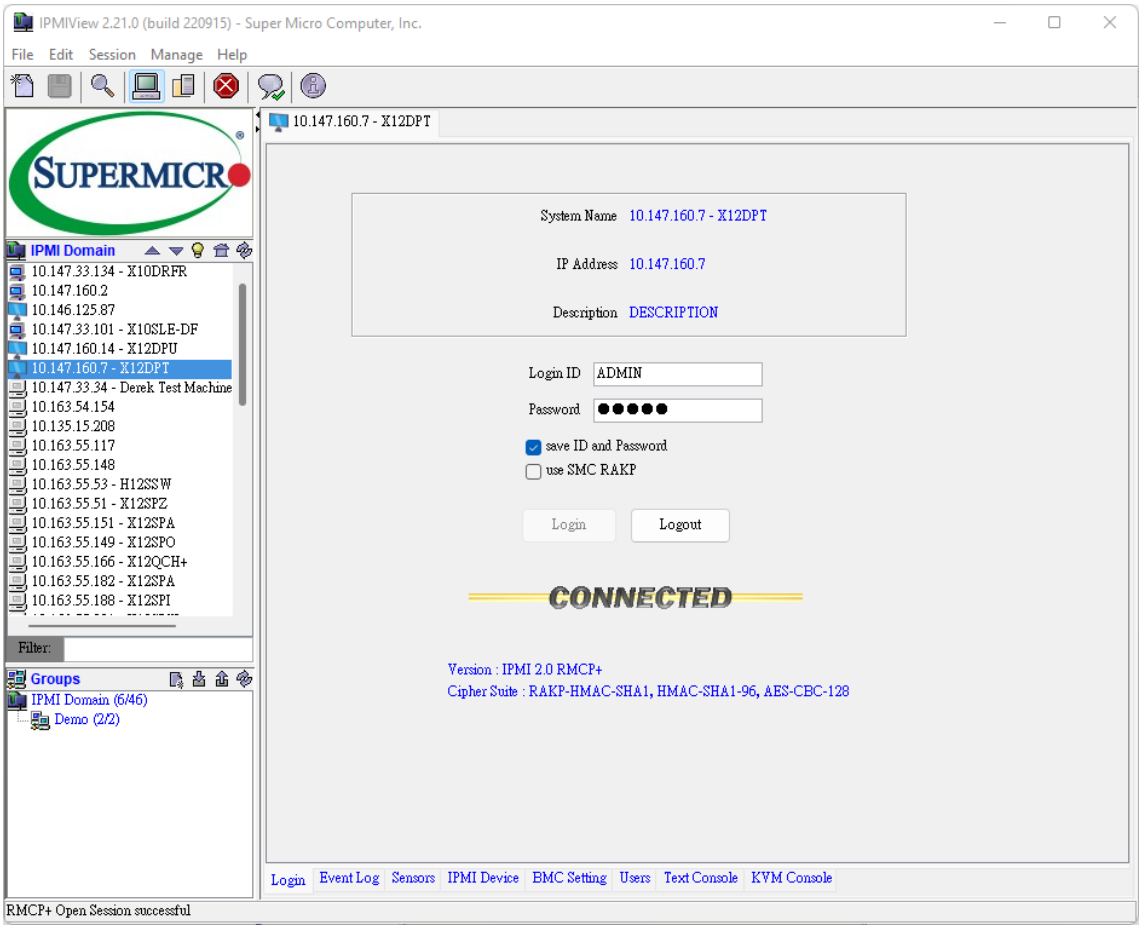


Figure 3-2

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).

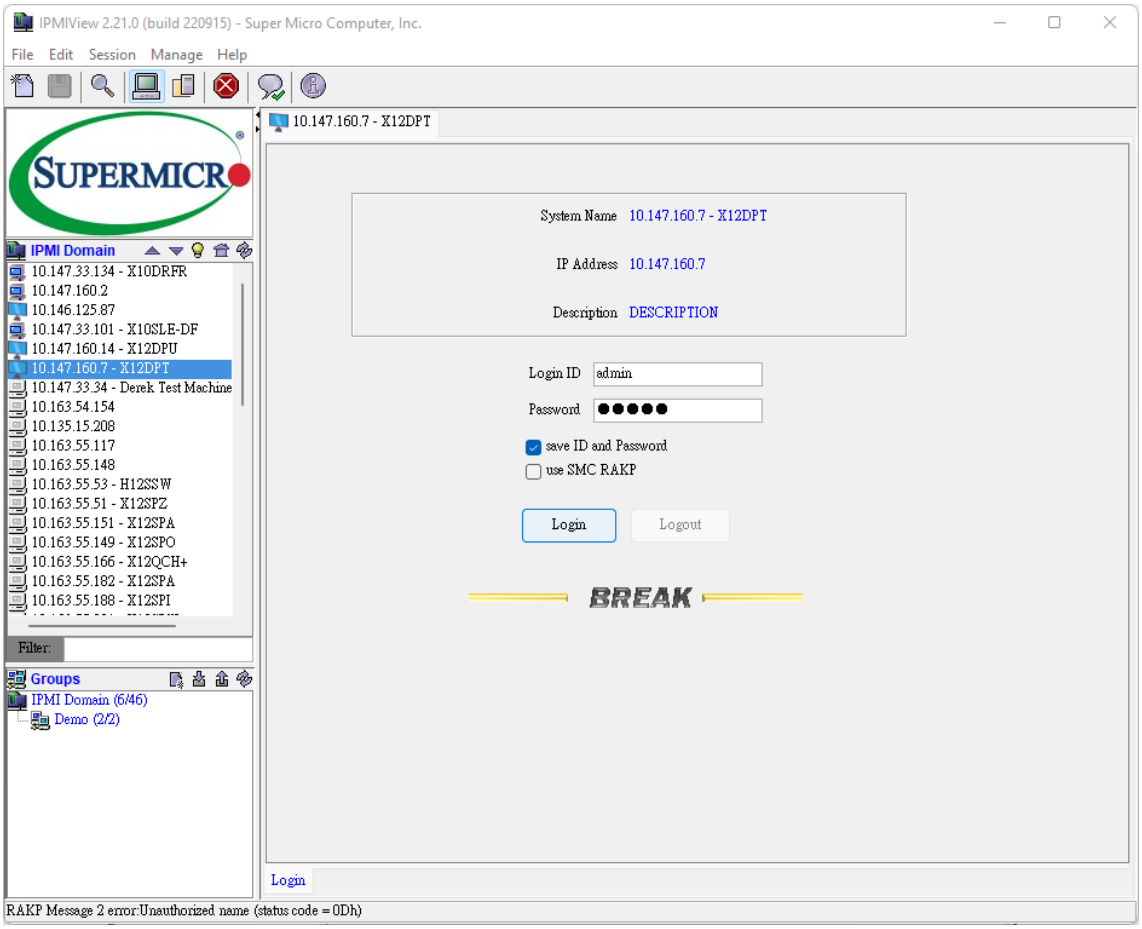


Figure 3-3

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.

Note: SMC RAKP should be enabled in IPMIView only if the connection to BMC has already enabled SMC RAKP, otherwise the connection will fail.

- **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 and KVM Console.

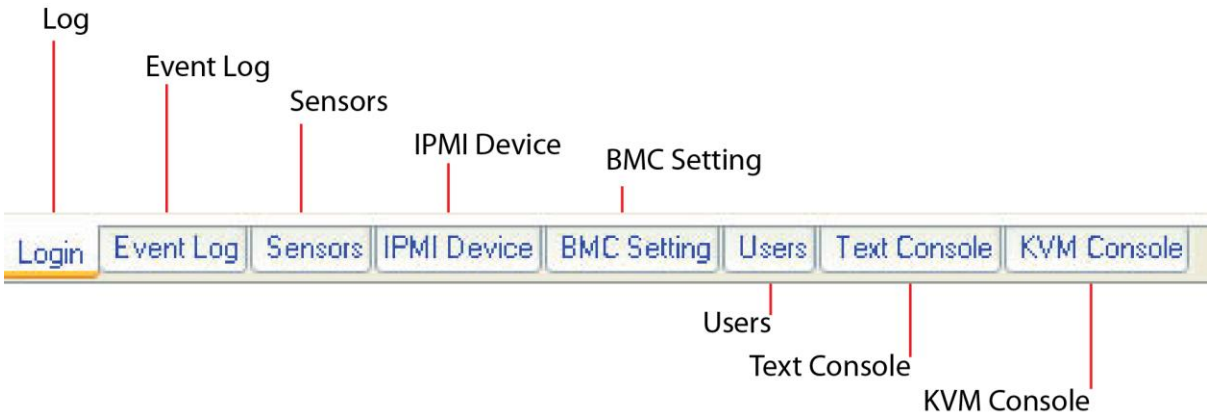


Figure 3-4

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.

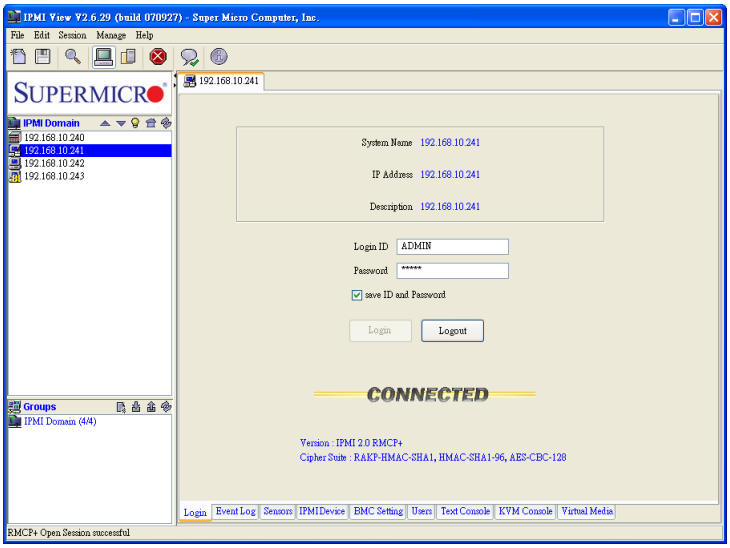


Figure 4-1

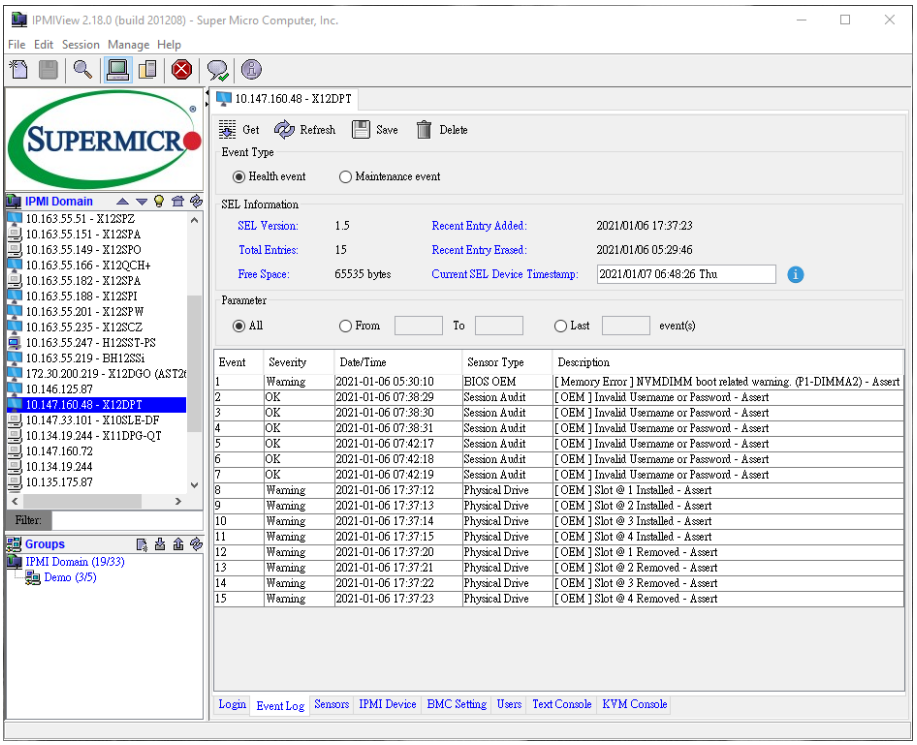


Figure 4-2

- **Get:** Click this button to retrieve event logs.
- **Refresh:** Click this button to refresh SEL information.
- **Save:** Click this button to save table event logs to a file.
- **Delete:** Click this button to delete event logs.
- **Health event:** Select this radio button to display the health event log.
- **Maintenance event:** Select this radio button to display the maintenance event log..
- **All:** Click this radio button to show all events.
- **From:** Click this radio box to select a range of health events.
- **Current SEL Device Timestamp:** This item displays the timestamp of the current SEL device.

  To learn about the rules, hover on the information icon .

5 Sensors

There are two sensor display modes supported with IPMIView 2.20.0 and later versions. Click the right-top combo box to switch between two modes as shown in Figure 5-1. The Graphic view is the default display mode. Alternatively, users can still switch to text view if preferred.

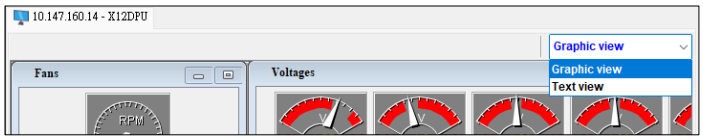


Figure 5-1

5.1 Graphic View

This feature displays the status of each sensor used to monitor system health, as shown in Figure 5-2.

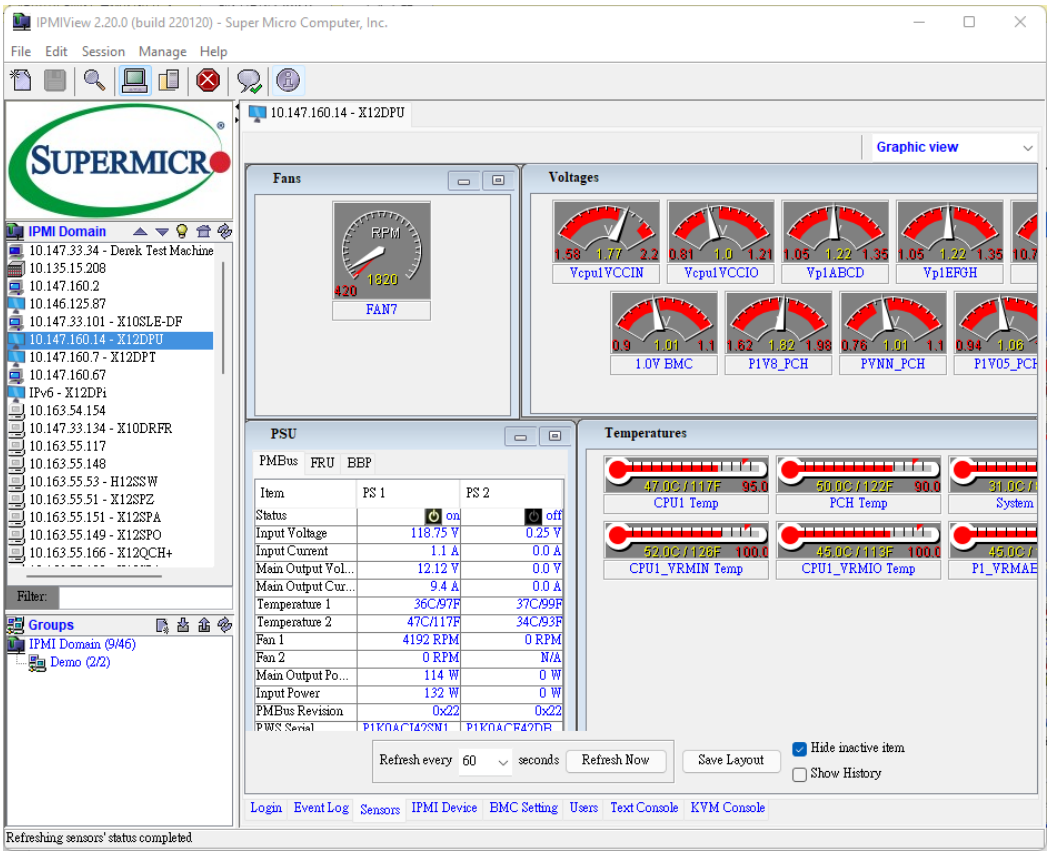


Figure 5-2

- **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.
- **PSU:** This window includes three tabs: PMBus, FRU, BBP (Battery Backup Power). Click each tab to view the information.
- **Refresh Every X seconds:** Enter the number of seconds for the system to refresh.
- **Refresh Now:** Click this button to refresh the Sensors page immediately.
- **Save Layout:** Click this button 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.

Some sensors (e.g., discrete sensors) are not available on certain motherboards, but they are still displayed in IPMIView.

5.1.1 Discharging Battery

1. The battery can be automatically or manually discharged. In the PSU dialog box (see Figure 5-3), click the **BBP** tab.

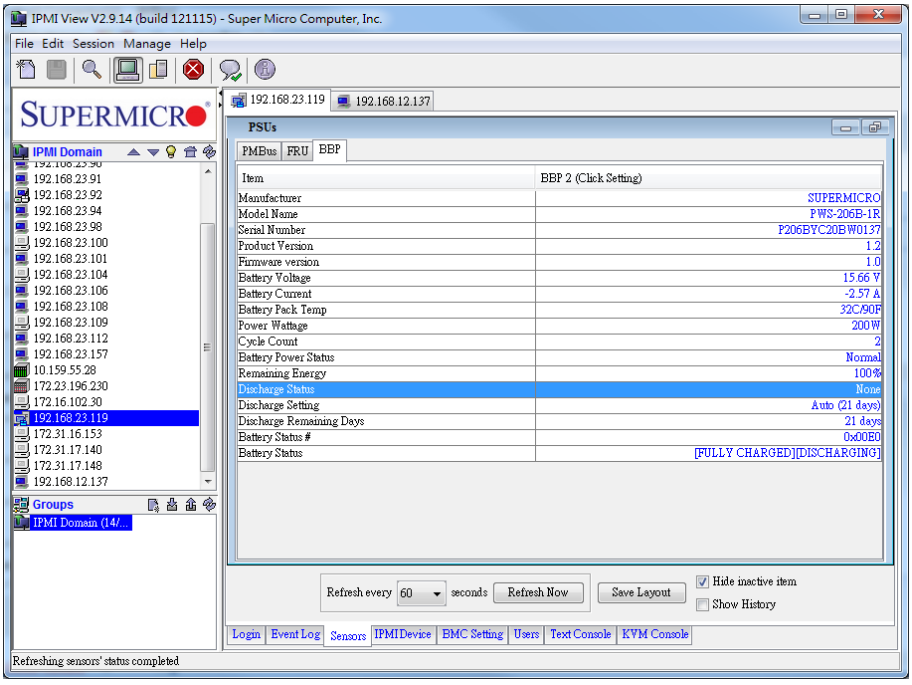


Figure 5-3

2. Click the top right field BBP2. A dialog box appears.

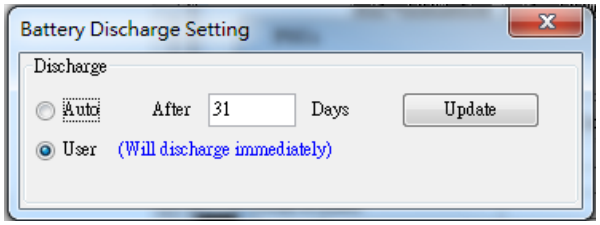


Figure 5-4

3. Select **Auto** and type desired number of days for the battery to discharge automatically, or select **User** to manually discharge the battery. Click **Update** to start.

5.2 Text view

This feature displays the status of each sensor in text list as shown in Figure 5-5.

Plus and minus button can be clicked to fold/unfold sensors by sensor type.

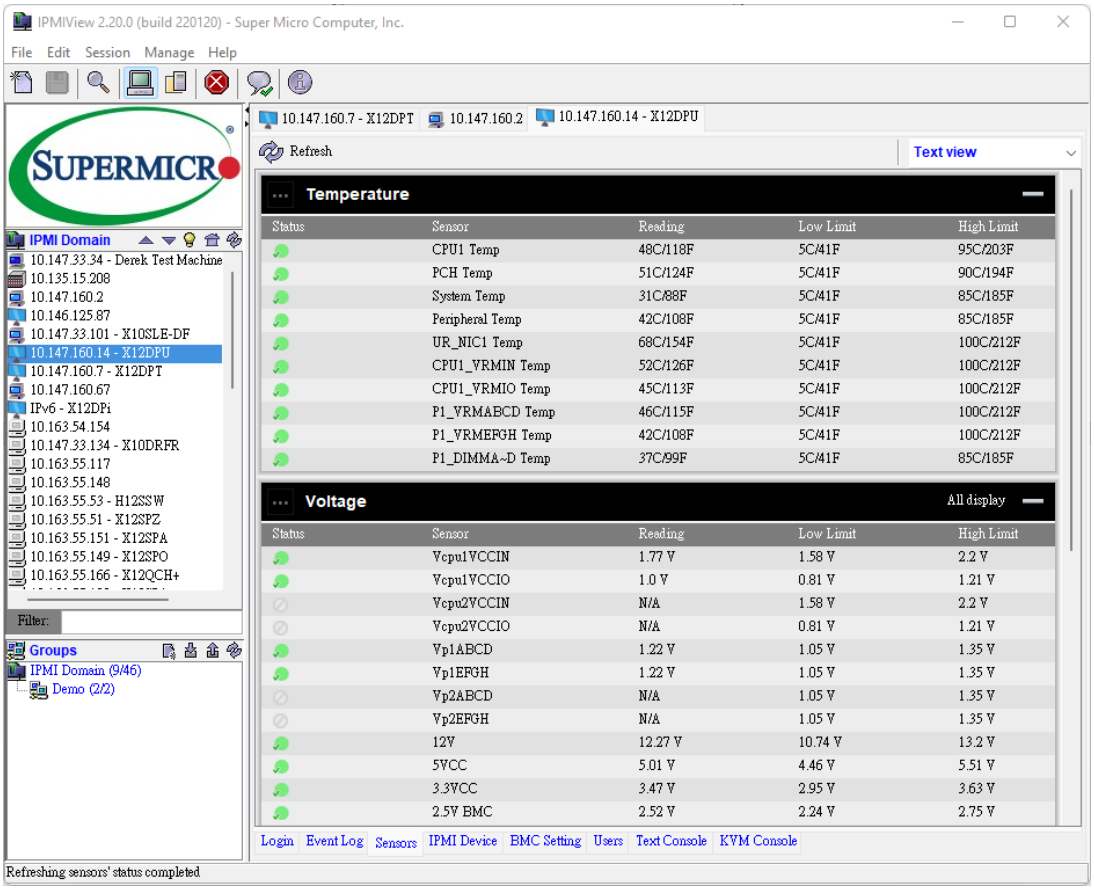


Figure 5-5

6 IPMI Devices

Click the IPMI Device tab of the IPMIView management session in the Viewing Window (shown in Figure 6-1 and 6-2) to display the UID, fan, boot, power information and functionality of the BMC firmware installed in the system.

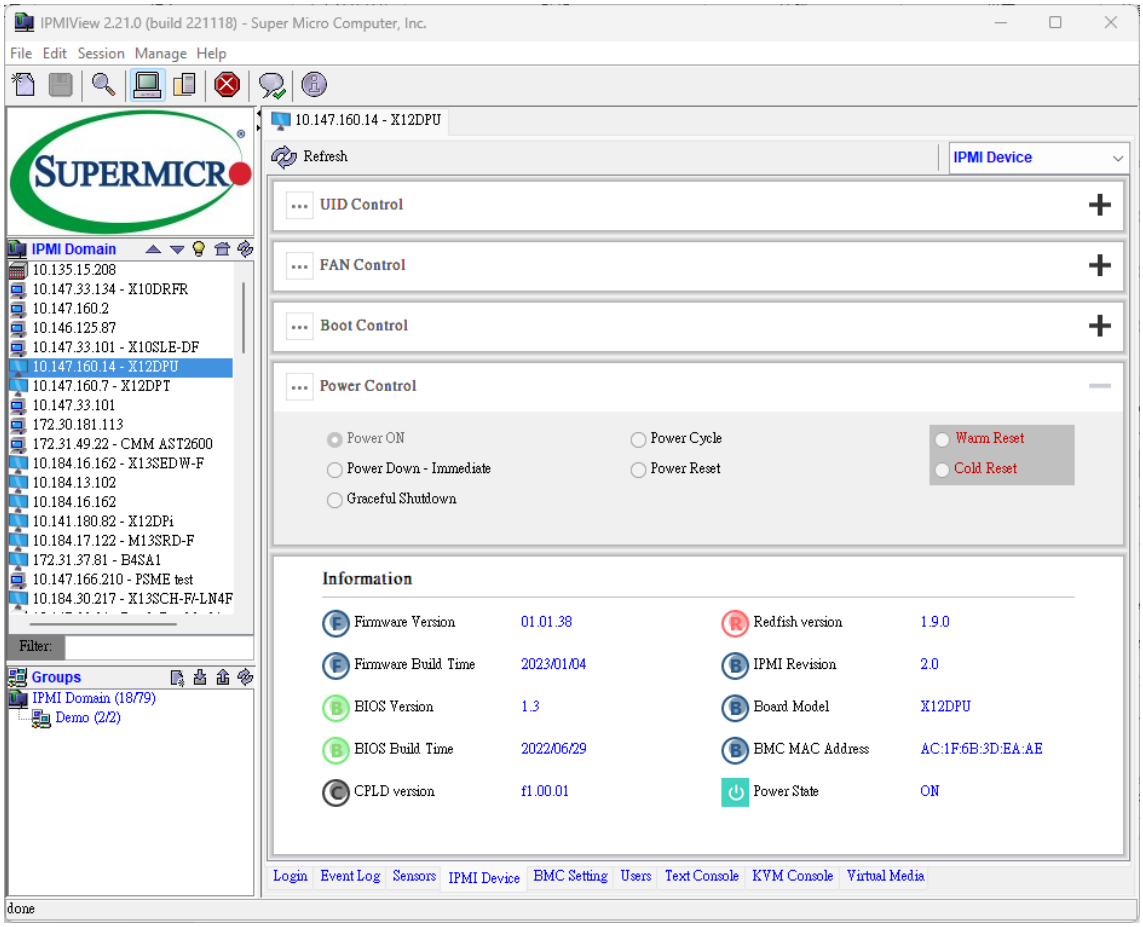


Figure 6-1

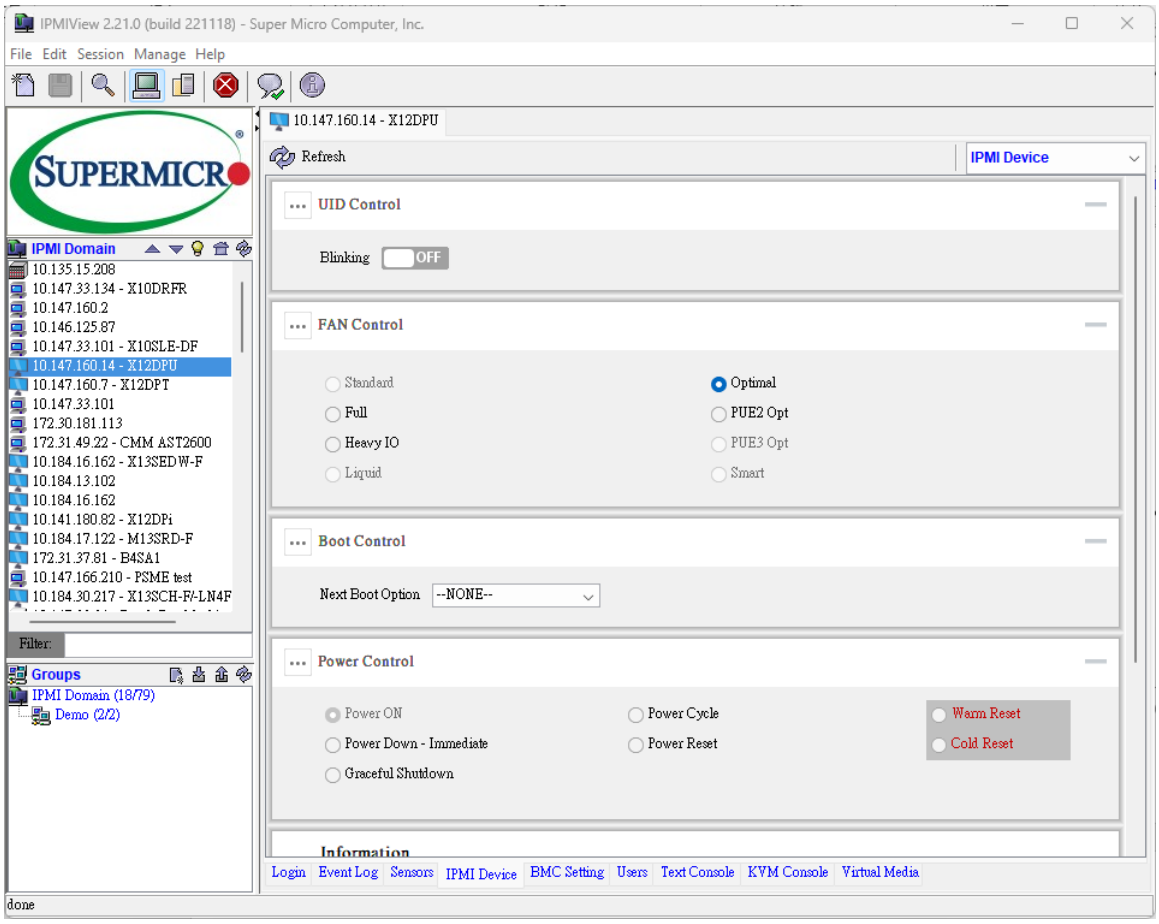


Figure 6-2

- **UID (Unit Identifier) Control (Administrator only)**
  - **Blink UID LED:** Click the switch button for the UID LED to blink when the unit in question is identified.
- **Fan Control (Administrator only)**

  Select the desired fan speed mode. The setting will be applied immediately. Note that available speed options vary.
- **Boot Control (Administrator and Operator only)**

  Select the boot device in the Next Boot pull-down menu. The setting will be applied immediately.
- **Power Control**
  - **Power ON (Administrator and Operator only):** This feature will power on a managed system.
  - **Power Down – Immediate (Administrator and Operator only):** This feature will power off a managed system.

- **Graceful Shutdown (Administrator and Operator only)**: This feature has the same function as "shutdown" in Windows. Using this feature will cause the managed system to enter the S5 state. A graceful shutdown will inform the OS running on the managed system to shut down within a specified time. When the OS running on the managed system receives a graceful shutdown request, it will start to shut down the system.
- **Power Cycle (Administrator and Operator only):** This feature will turn off the power to a managed system for a few seconds and then turn it on again.
- **Power Reset (Administrator and Operator only):** This feature resets a managed system.
- **Warm Reset (Administrator only):** A warm reset allows the current settings of interrupt enables, thresholds, etc. unchanged while communications interfaces are reset. Selecting the **Warm Reset** radio button allows you to reset the BMC. Click Yes to warm reset the BMC and the session will be terminated immediately. You may try a Warm Reset if the system hangs.

- **Cold Reset (Administrator only)**: A cold reset allows the BMC to restore to the default settings of interrupt enables, event message generation, sensor scanning, threshold values, and other "power up default" state. Selecting the **Cold Reset** radio button to reset the BMC. After confirming the reset of the BMC, the session will be terminated immediately. This feature is rarely used, for example when you suspect a system malfunction.

- **Device Information**

  This panel shows all the FW revisions of the BMC, BIOS, CPLD, Redfish and IPMI. Board model information and power state information are also provided here.

7 BMC Settings (Available for the Administrator only)

Click the BMC Setting tab of the IPMIView management session in the Viewing Window (as shown in Figure 7-1, 7-2, 7-3 and 7-4) to display detailed information on the Network, SNMP trap, SMC RAKP and Date-Time configuration in sub-tab respectively.

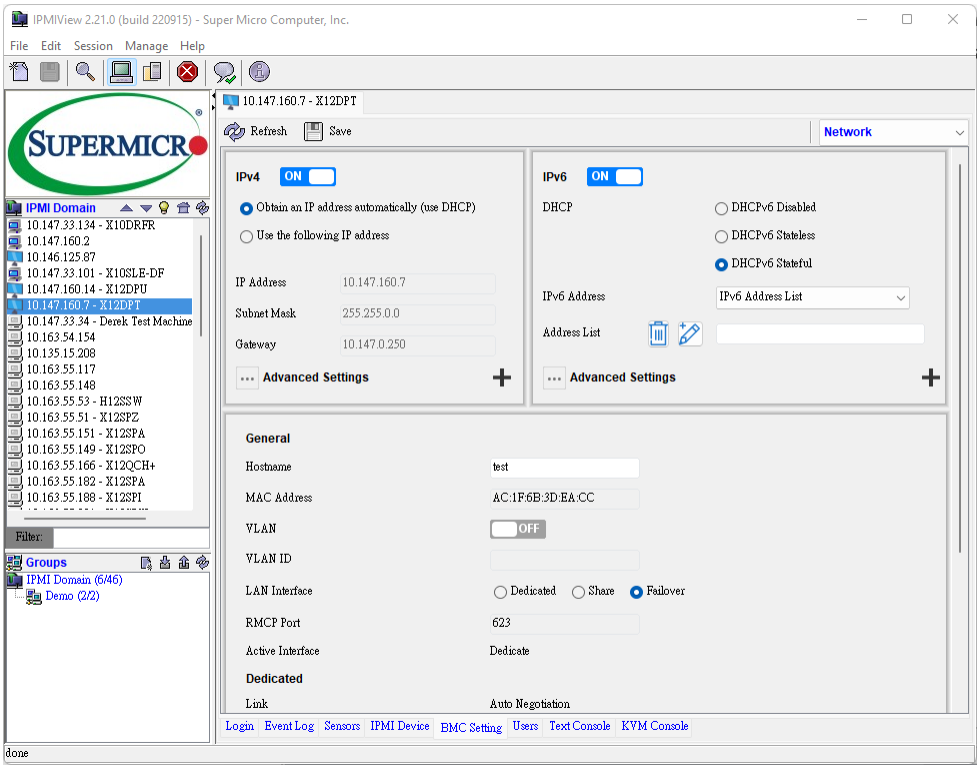


Figure 7-1

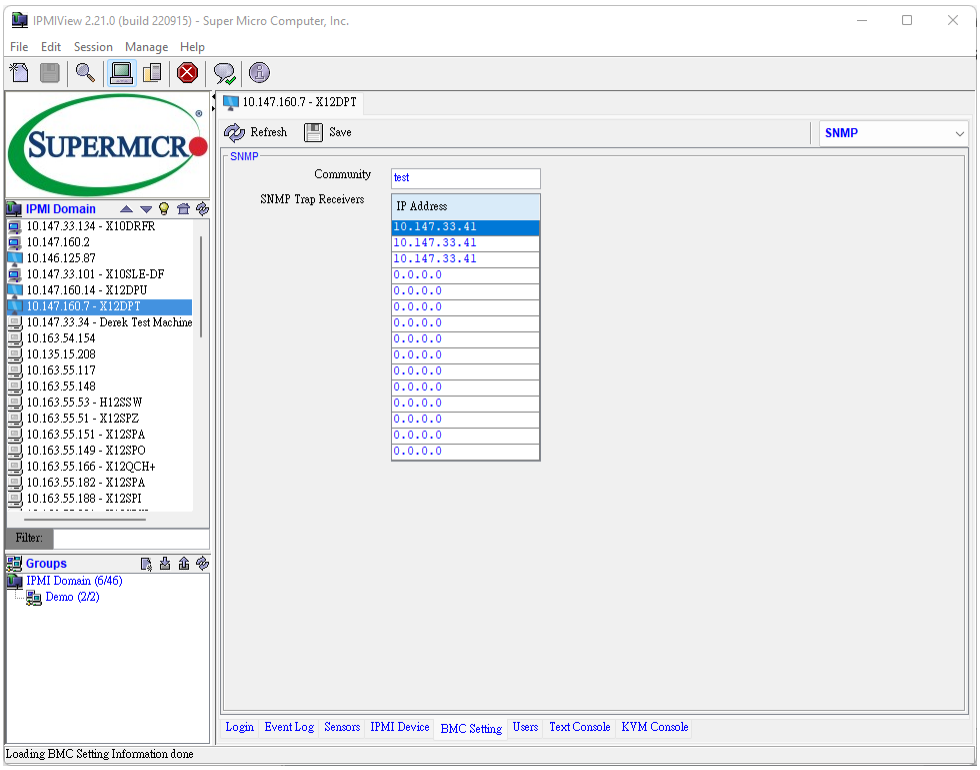


Figure 7-2

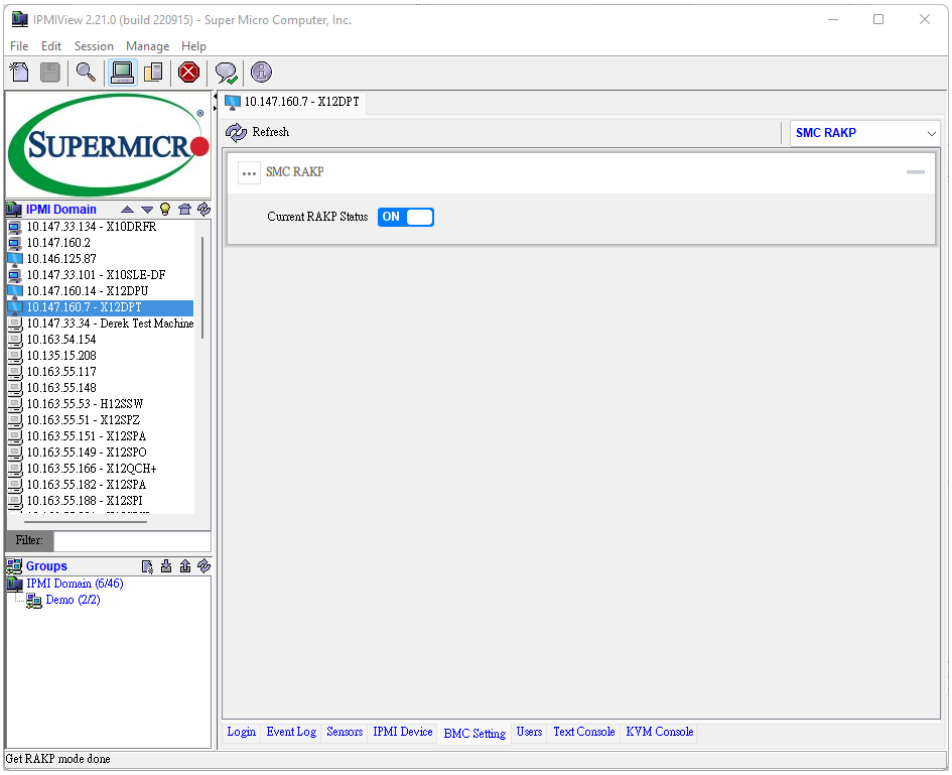


Figure 7-3

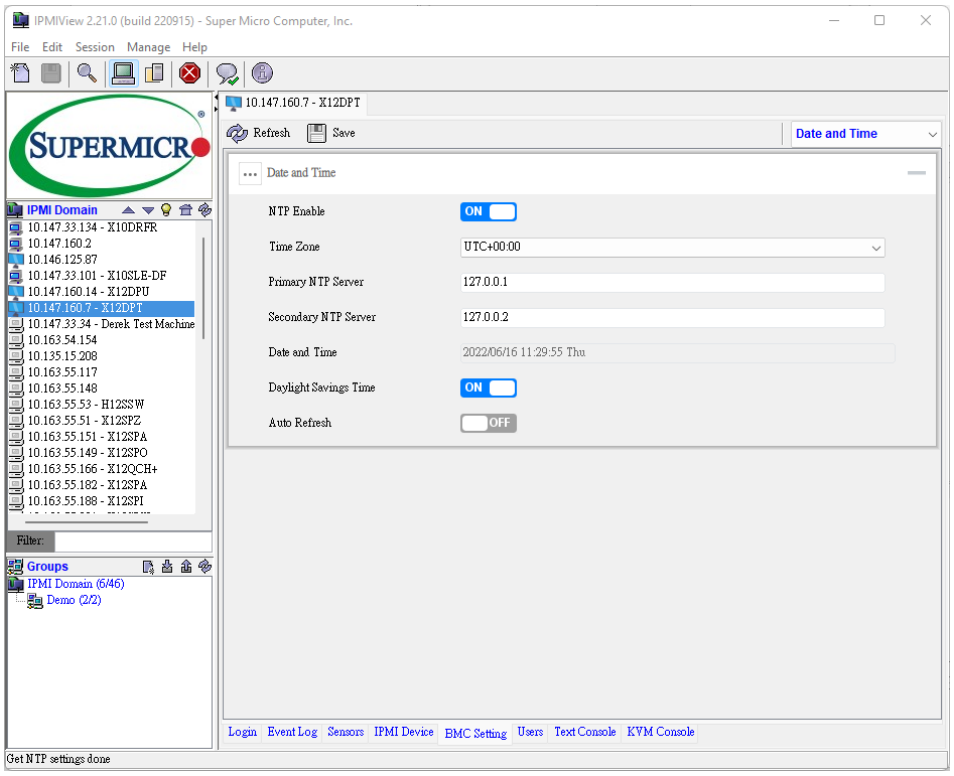


Figure 7-4

- **Network Configuration**

This feature displays the IP address, the LAN MAC, the Gateway IP, the Gateway MAC, LAN interface, a router's IP address, and the Subnet Mask of the BMC and allows you to modify these settings.

To configure the VLAN Tag setting, you can enable the VLAN (Virtual LAN) Tag setting by clicking the checkbox of Enable VLAN Tagging on the right and entering the value in the VLAN Tag field.

Note: Please make sure both MAC addresses of LAN and gateway for the BMC are correct before clicking the **Save** button. Be especially careful when you enter the MAC address of LAN. If the entered address is incorrect, the connection between IPMIView and the system will no longer be established.

- **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 **Save** 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 **Save**.

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.

Note: SNMP trap can display SNMPv1 and SNMPv3 protocol. If the protocol is unsupported, the trap list will display with "N/A".

- **SMC RAKP**

Clicking this button allows you to enable SMC RAKP mode. A confirmation dialogue box will appear. After clicking OK button, the session will be terminated immediately.

Note: Under administrator privileges, new settings will apply to the login tab.
Please refer to Figure 3-1 and the Q&A Appendix for more information.

- **Date and Time**

This feature displays NTP status, time zone, primary NTP server, secondary NTP server, current date-time and daylight savings time of the BMC. It allows you to modify these settings other than date-time.

8 Users

IPMIView supports user account and FRU information sub-page in user tab of the IPMIView management session from 2.20.0 version. Click the right-top combo box to switch sub-page as shown in Figure 8-1.

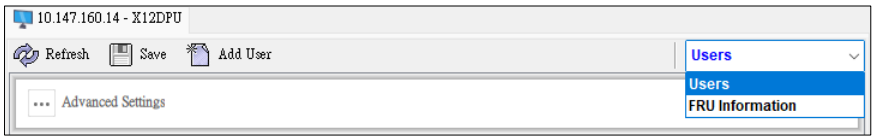


Figure 8-1

8.1 Users Account

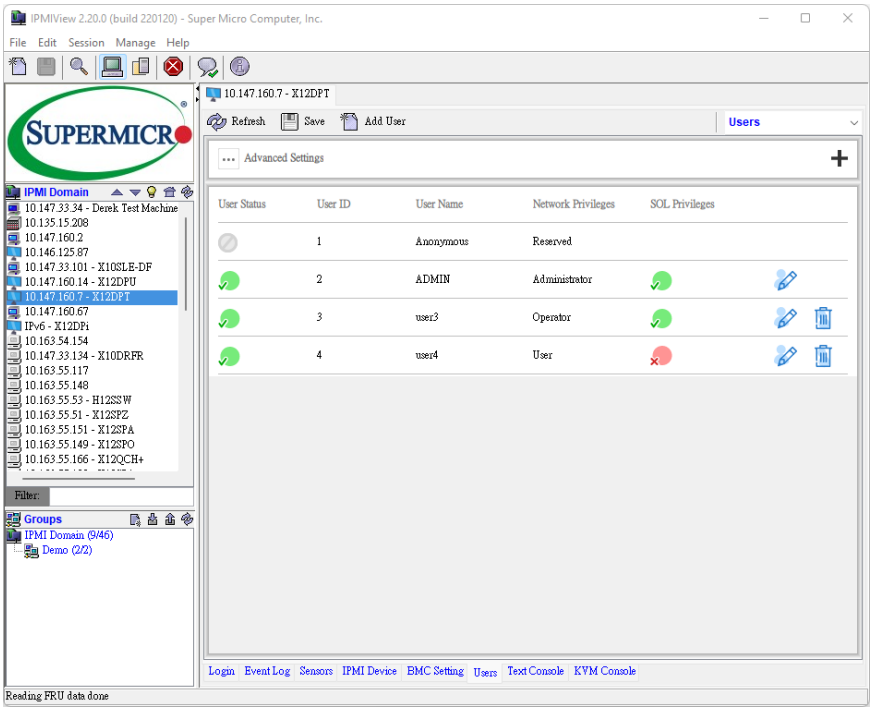


Figure 8-2

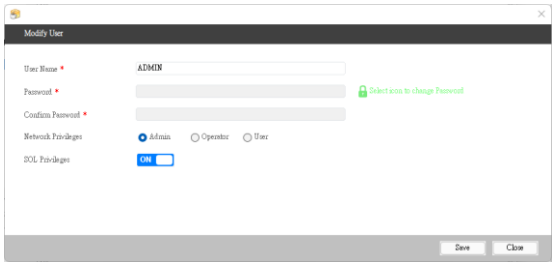


Figure 8-3

Click the Users tab of the IPMIView management session in the Viewing Window (as shown in Figure 8-2 and Figure 8-3) to display detailed information on the Users management, advanced settings.

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 network privilege and SOL privilege settings by clicking the appropriate button.
  - **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 three 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. Choose network privilege radio button to change the privilege level setting for a user.

Group Privilege Levels

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 disable the channel over which the Administrator is communicating.

8.1.1 Advanced Setting

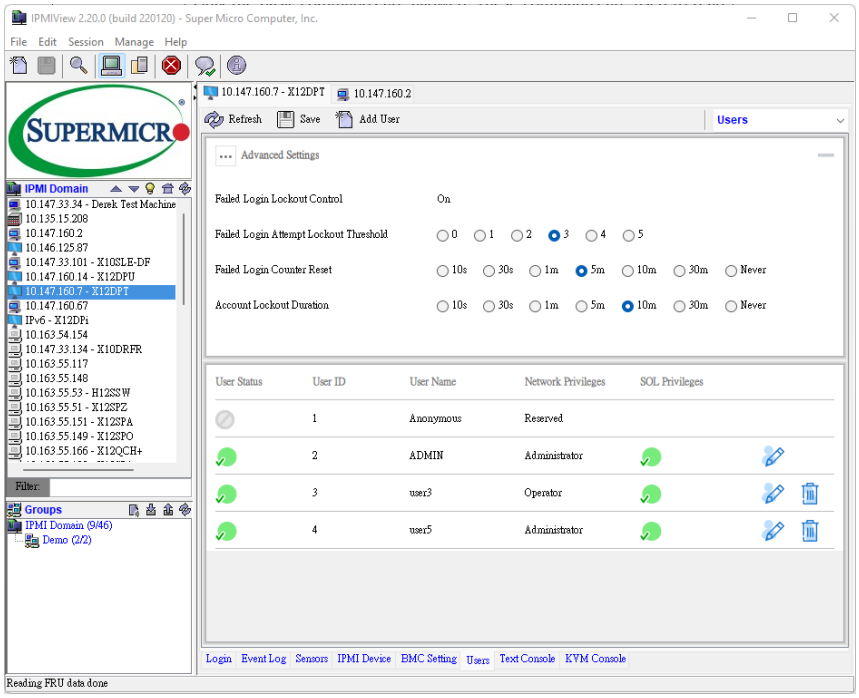


Figure 8-4

Click the Users tab of the IPMIView management session in the Viewing Window (as shown in Figure 8-4) and Advanced Settings title bar to expand detailed settings.

IPMIView allows you to change failed login attempt lockout threshold, failed login counter reset and account lockout duration settings by clicking the appropriate radio button.

Notes:

- It is supported by X12 and later platforms.
- Failed Login Counter Reset value cannot be greater than Account Lockout Duration.

8.2 FRU Information

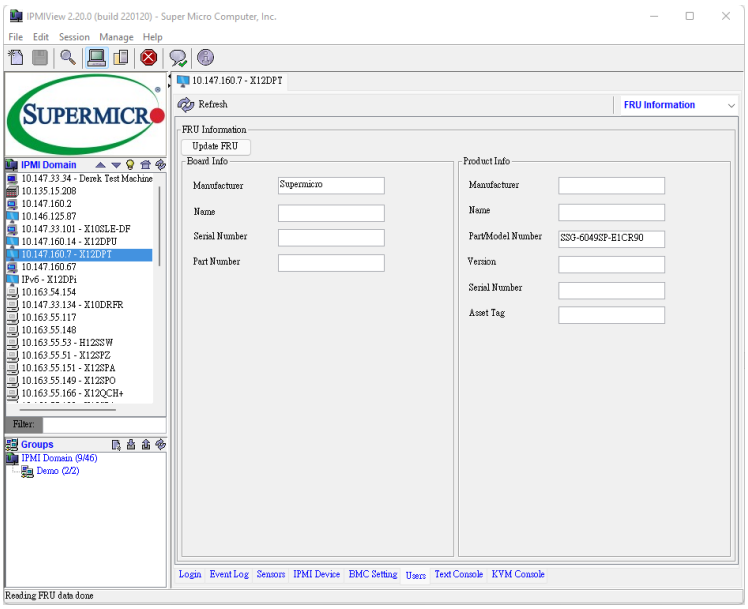


Figure 8-4

Click the Users tab of the IPMIView management session in the Viewing Window (see Figure 8-4) and right-top combobox to display FRU information.

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

This provides useful information on the board and the product, including the serial number, part number, and the motherboard components. Click the **Update FRU** tab to update the 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. In some RoT systems, FRU data is considered as critical data. When an FRU entry is updated, it will be further backed up to flash. Due to the backup, writing FRU data to system on RoT platforms may take much longer than on other platforms.

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

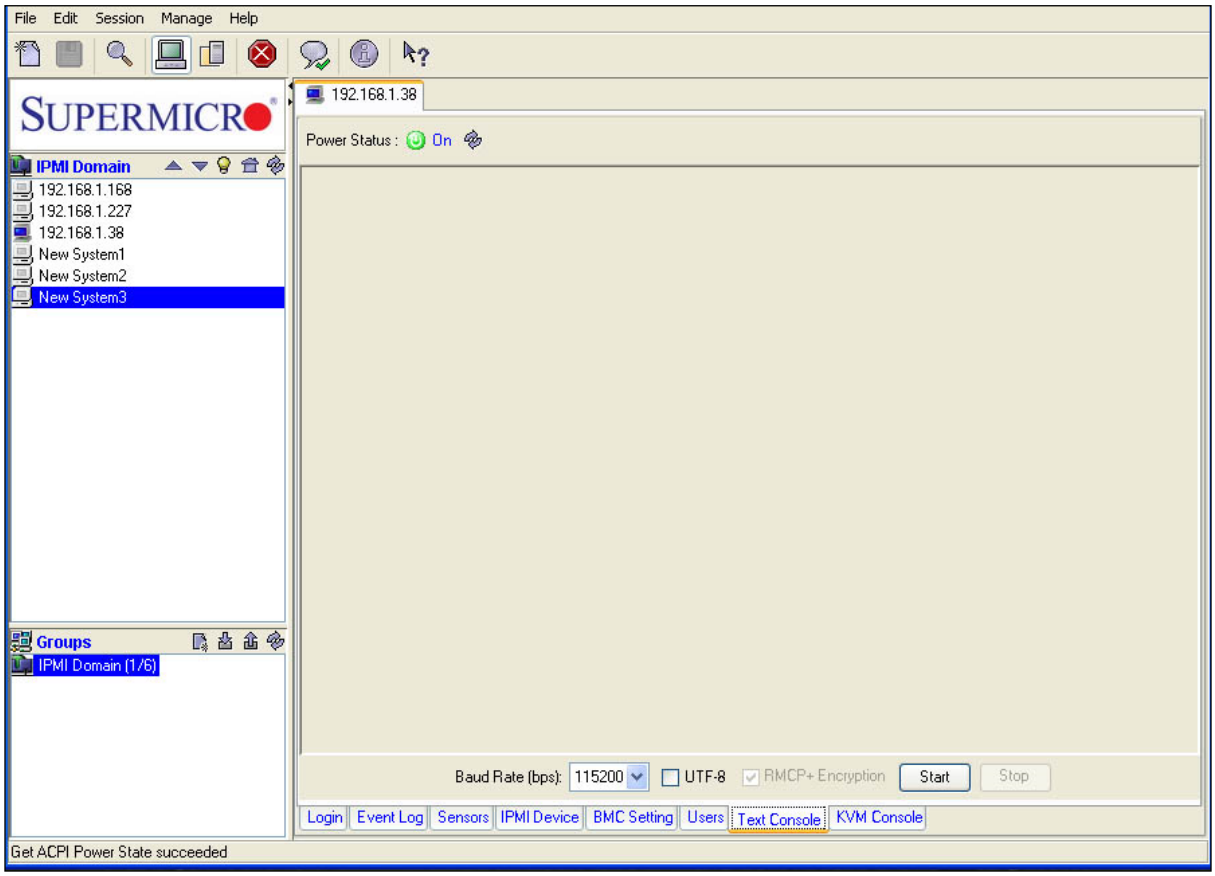


Figure 9-1

Click the **Text Console** tab on the bottom toolbox (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. To enable SAC, follow these steps:

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.

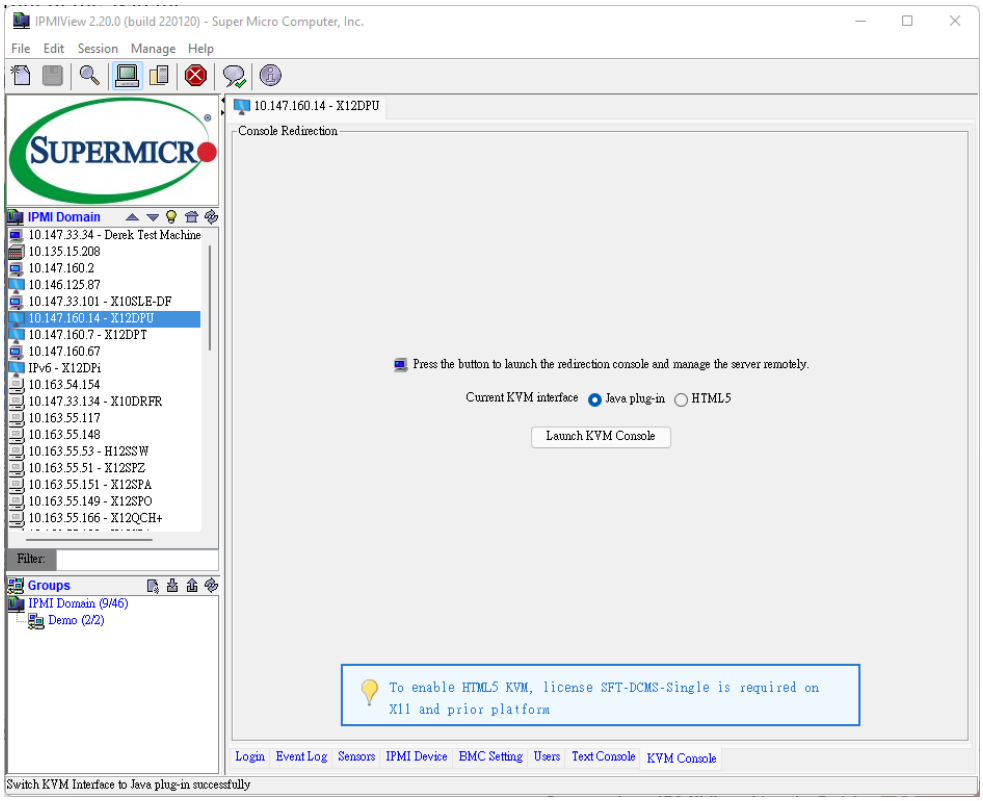
You will see the BIOS POST, the boot loader, and the Linux OS messages and prompts.

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. KVM Console will be disconnected if the user performs a FW update or BIOS update. Administrative privileges are required (Linux: sudo, Windows: Run as administrator) to perform the virtual storage mounting function.

IPMIView supports Java plug-in and HTML5 version of KVM since 2.20. An example below shows Java plug-in version of KVM first.

Select Java plug-in radio button to switch to Java KVM interface, and then click the **Launch KVM Console** tab to launch KVM console redirection. For product X10 and later, an iKVM console will pop out. Figure 10-1-1 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.



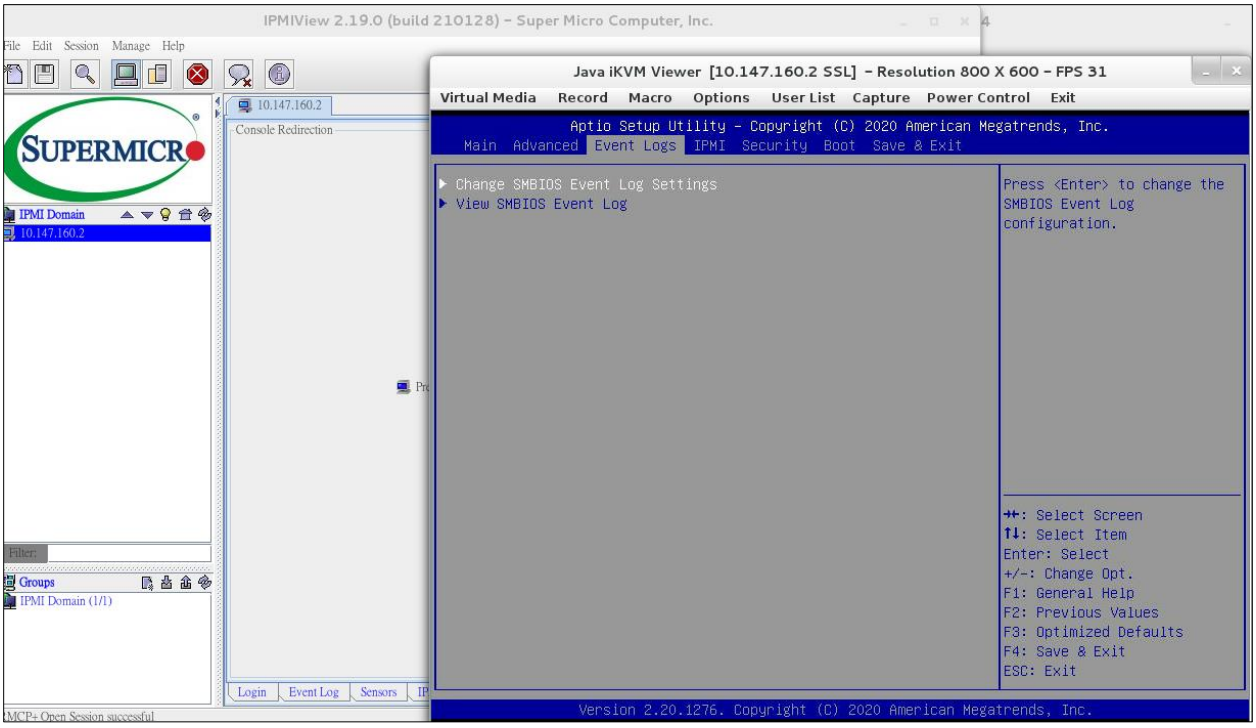
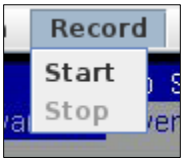


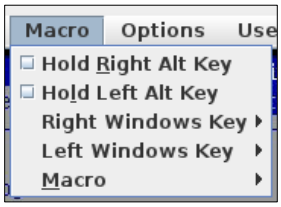
Figure 10-1-1

- **Virtual Media:** To mount a virtual storage or to open virtual keyboard.

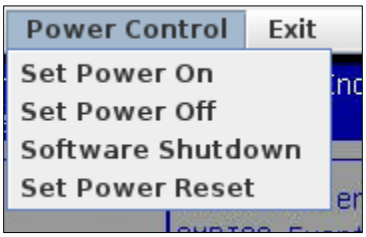
- **Record:** This function is to start/stop the record screen.



- **Marco:** Marco and hotkey settings.

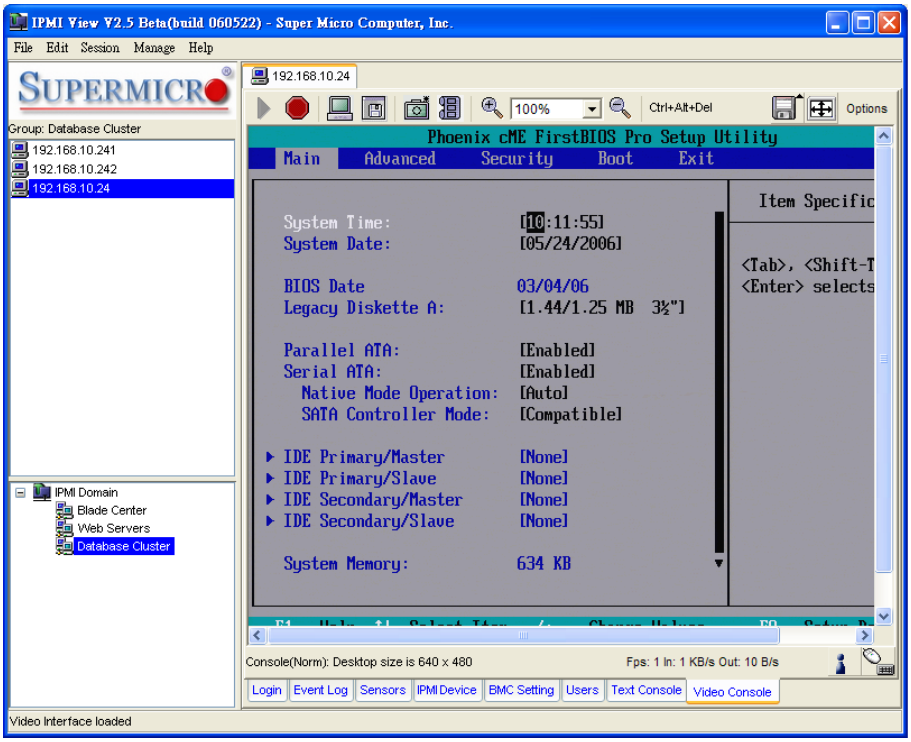


- **Power control:** To perform power control of this system.



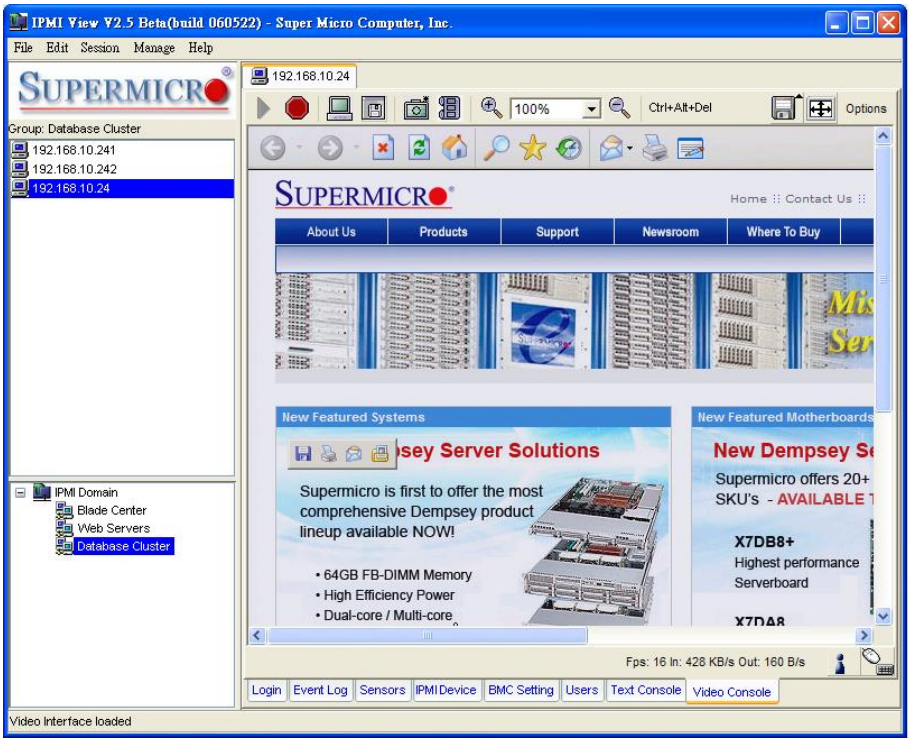
Due to platform characteristics, there are a little difference in UI for earlier Supermicro product like X9.

For these kinds of platforms, a “Video Console” tab will show up instead of “KVM Console.”



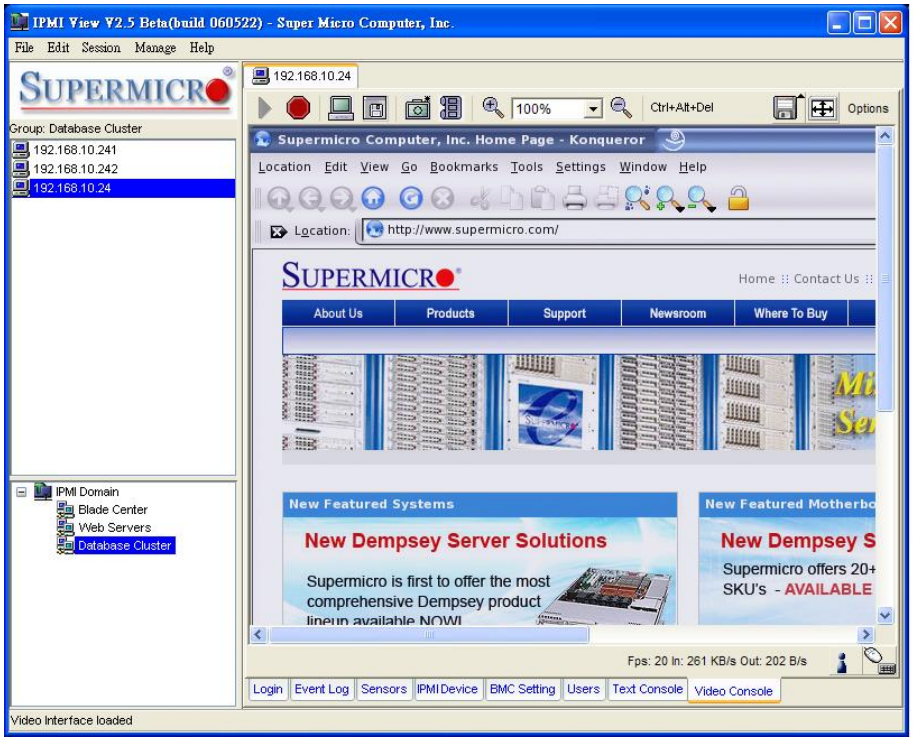
BIOS Screen

Figure 10-1-2



Windows XP

Figure 10-1-3



Linux X Window

Figure 10-1-4

Toolbar

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

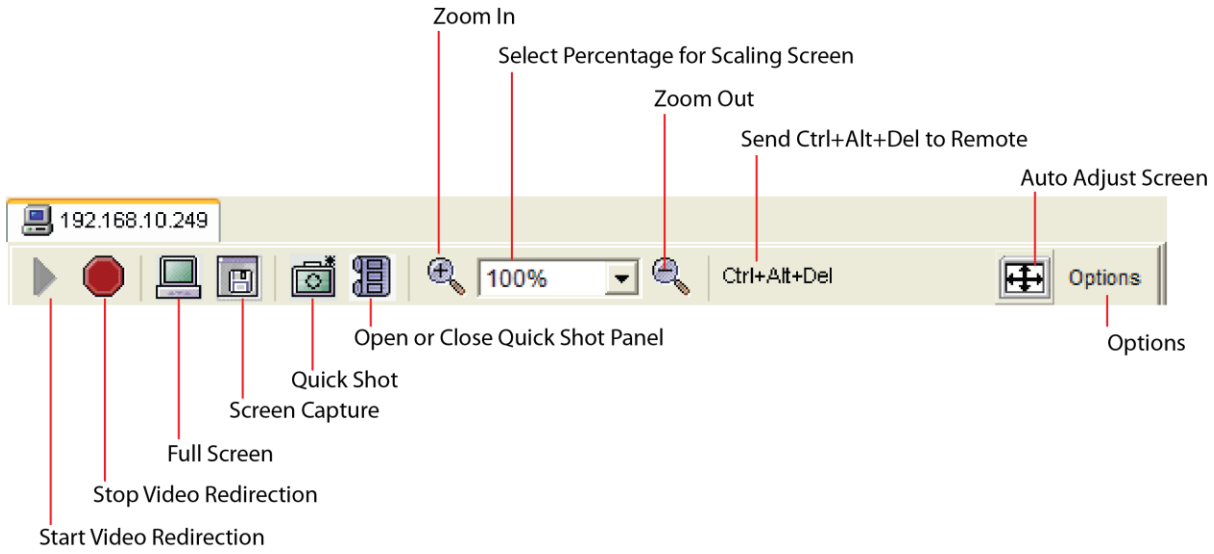


Figure 10-2 Video Console Toolbar

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 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.

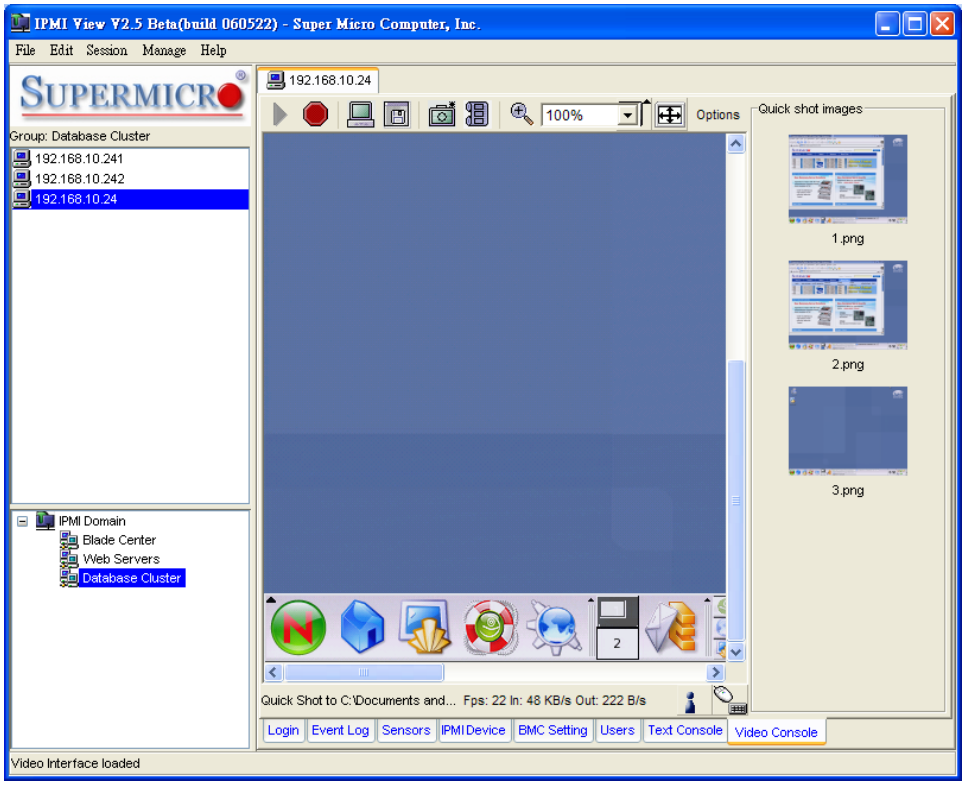


Figure 10-4

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.

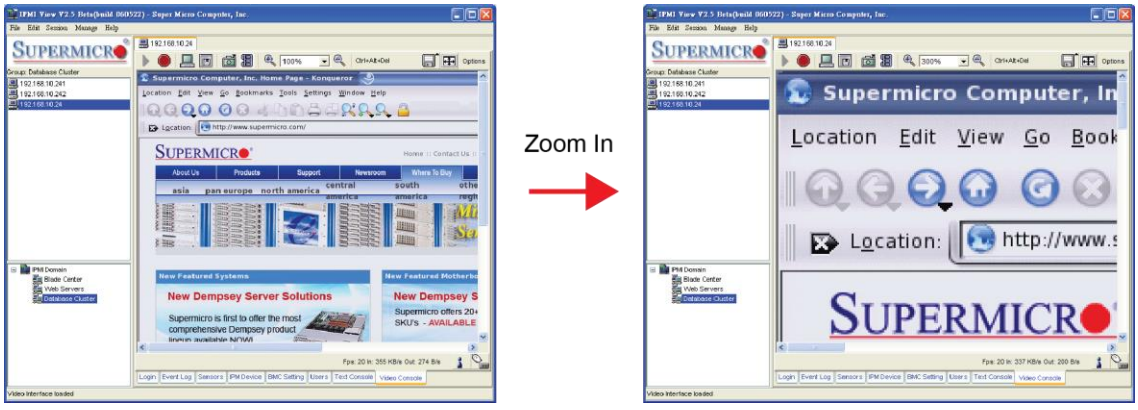


Figure 10-5

Zoom Out:

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

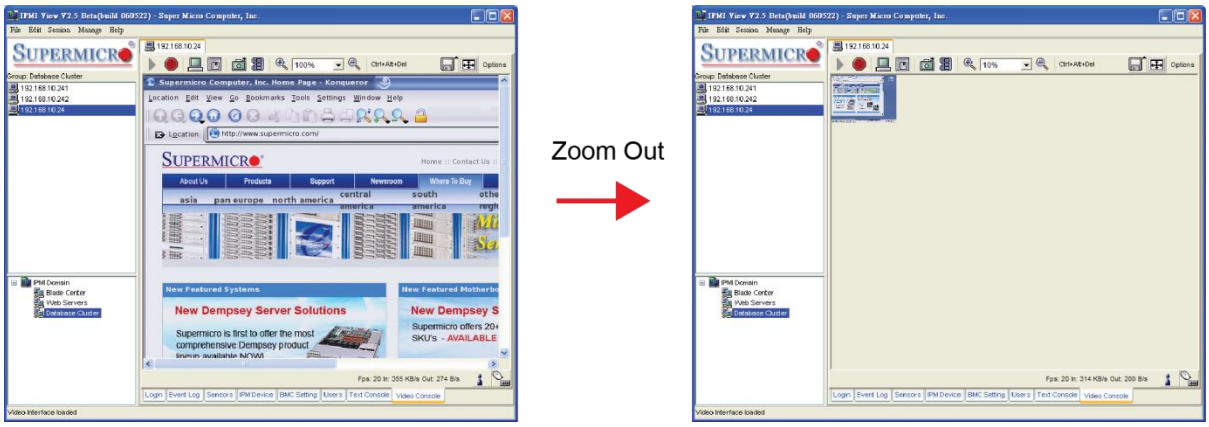


Figure 10-6

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. Click 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.

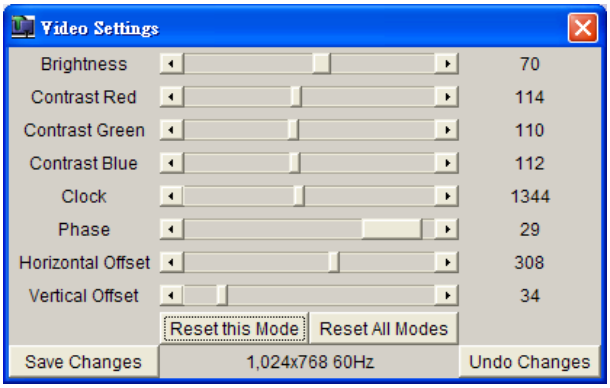


Figure 10-8 Video Settings

- **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.

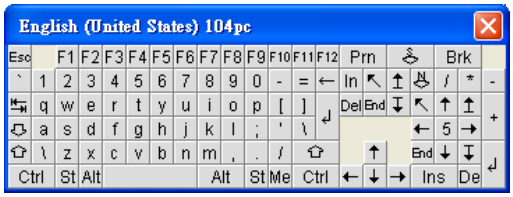


Figure 10-9 Soft Keyboard

- **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.

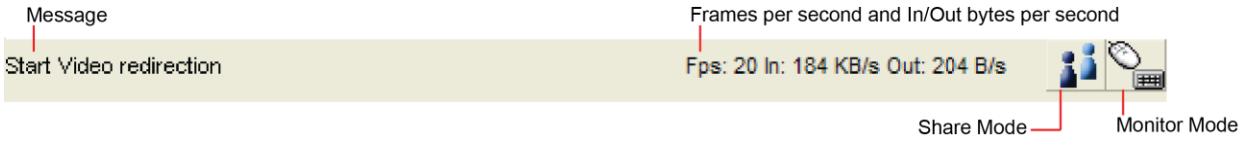


Figure 10-10

Start Video redirection **Message:**

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

Fps: 20 In: 184 KB/s Out: 204 B/s

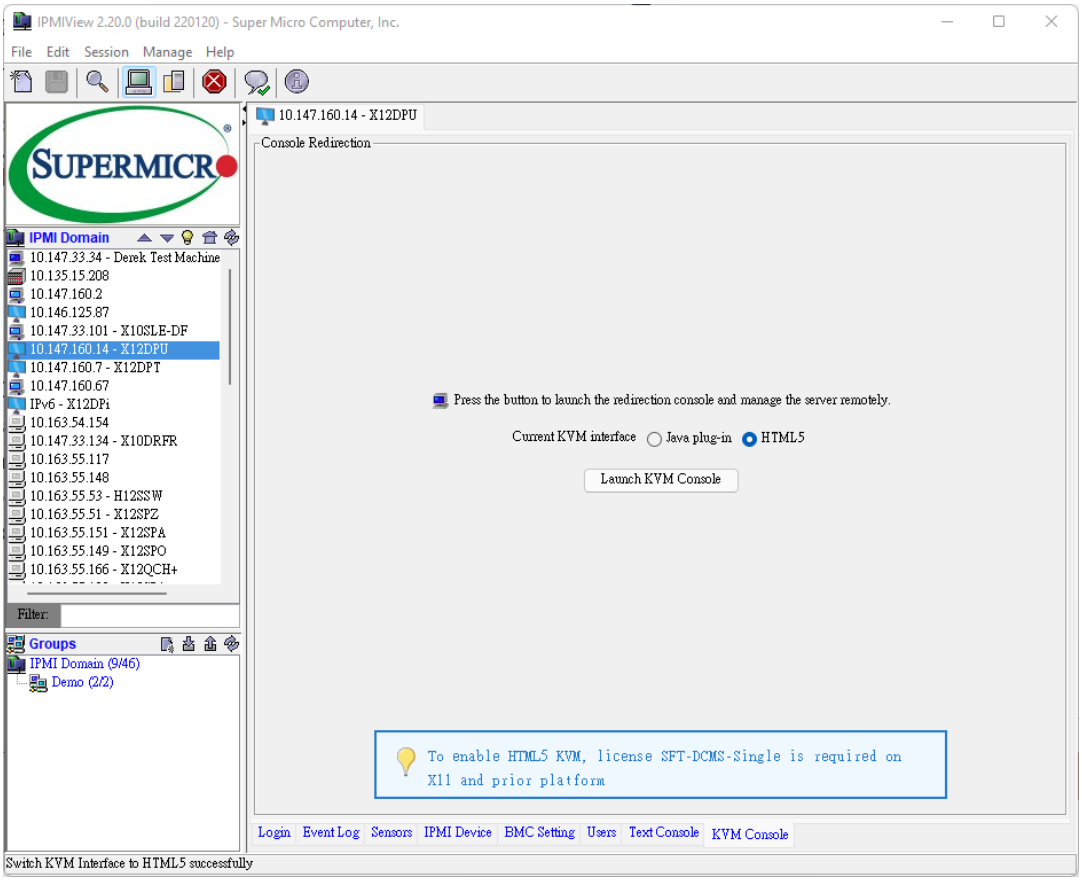
This section indicates the number of the frames displayed per second, and Input (Kbytes per second)/ Output (bytes per second).

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.



Click HTML5 radio button to switch to HTML5 KVM interface, and then Click the **Launch KVM Console** tab to launch HTLM5 KVM console redirection. Figure 10-11 shows sample screenshot of a warning message appears when a new connection to the BMC is established for the first time. Click the **Continue to "BMC IP address" (unsafe)** link to proceed. For product X10 and later, an HTML5 KVM console will pop out by default browser. Figure 10-12 shows sample screenshots of HTML5 KVM Console redirection.

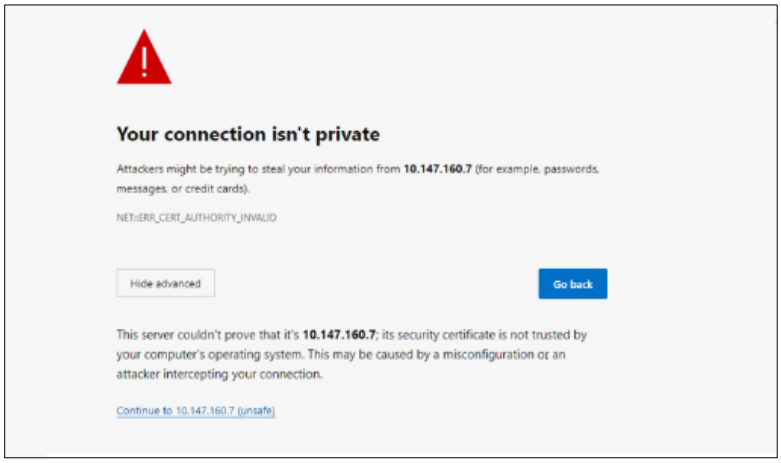


Figure 10-11

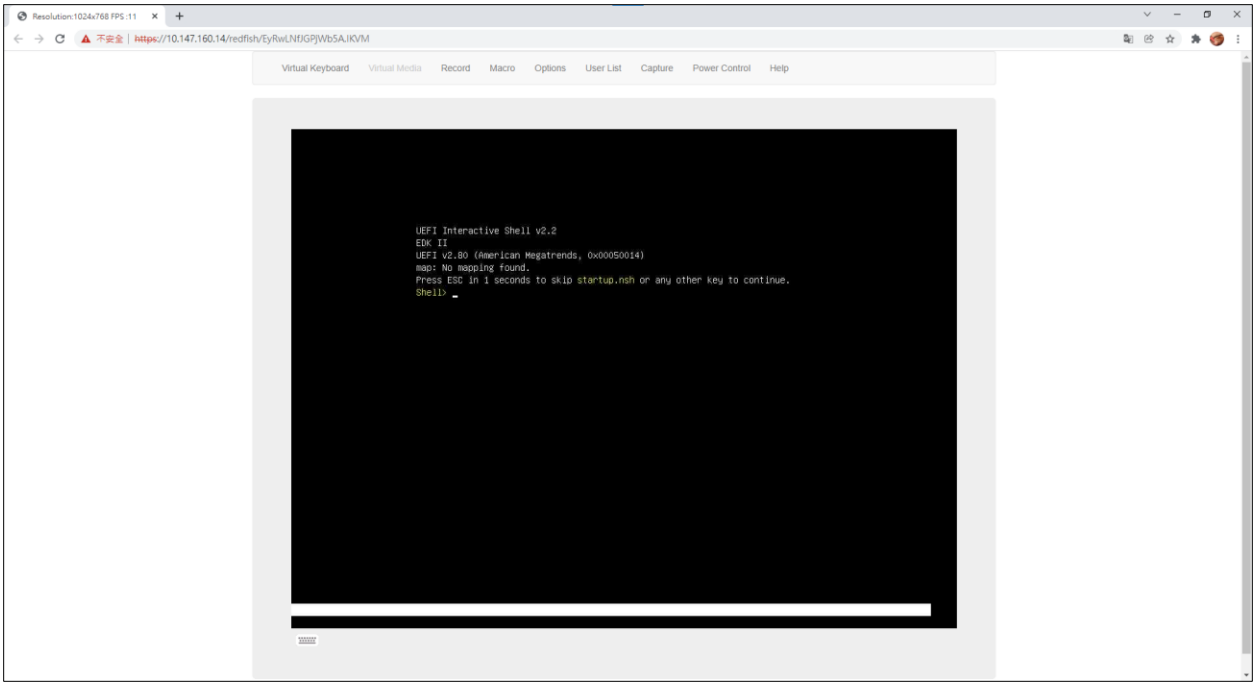


Figure 10-12

Note: HTML5 KVM requires a SFT-DCMS-Single license on X10 and X11 generations of motherboards.

11 Virtual Media

IPMIView provides virtual media functions for different generations of motherboards. The older one is Supermicro Intelligent Management (SIM) Module and the later one is SIM (WA) Modules, which is applied on the ASPEED AST2400 and later BMC. IPMIView will automatically show up on the virtual media tab if the device is supported. However please note that this function requires a license. You need to enable either SFT-OOB-LIC or SFT-DCMS-Single on the target device.

11.1 SIM Module

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.

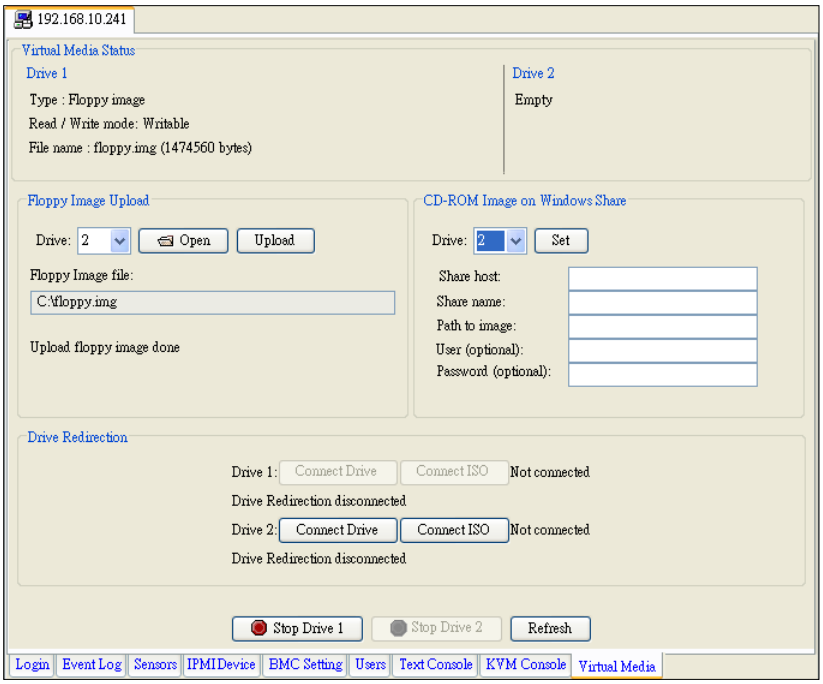

192.168.10.241
Virtual Media Status
Drive 1
Type : Floppy image
Read / Write mode: Writable
File name : floppy.img (1474560 bytes)
Drive 2
Empty
Floppy Image Upload
Drive: 2
Open
Upload
Floppy Image file:
C:\floppy.img
Upload floppy image done
CD-ROM Image on Windows Share
Drive: 2
Set
Share host:
Share name:
Path to image:
User (optional):
Password (optional):
Drive Redirection
Drive 1: Connect Drive Connect ISO Not connected
Drive Redirection disconnected
Drive 2: Connect Drive Connect ISO Not connected
Drive Redirection disconnected
Stop Drive 1
Stop Drive 2
Refresh
Login
Event Log
Sensors
IPMI Device
BMC Setting
Users
Text Console
KVM Console
Virtual Media

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.

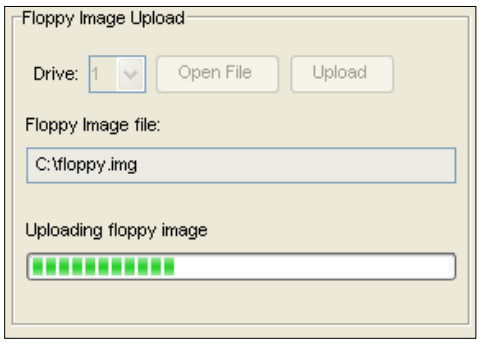


Figure 11-2

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 name 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.

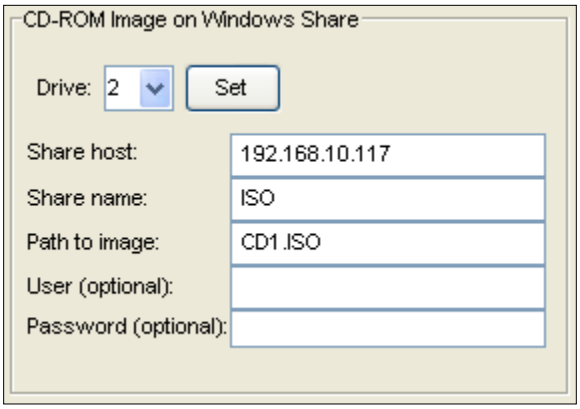


Figure 11-3

Drive Redirection

As shown in Figure 11-4, Drive Redirection supports both local drive and the ISO file. When you click the **Connect Drive** button, a dialog box (Figure 11-5) will show up.

- **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.

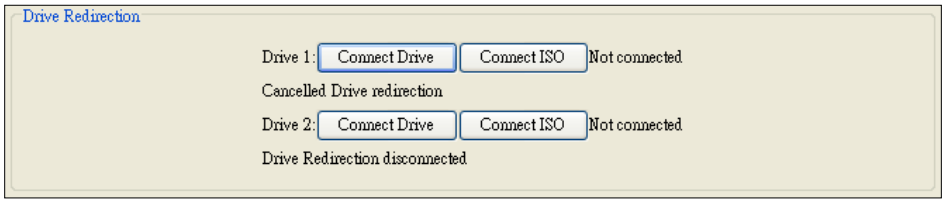


Figure 11-4

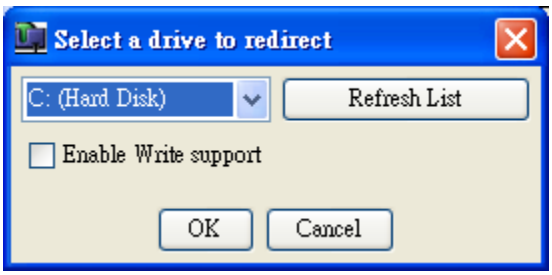


Figure 11-5

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

11.2 SIM (WA) Module

The SIM (WA) Module provide a CD-ROM image feature that allows users to share data via “Windows Share” (Windows) or "Samba" (Linux).

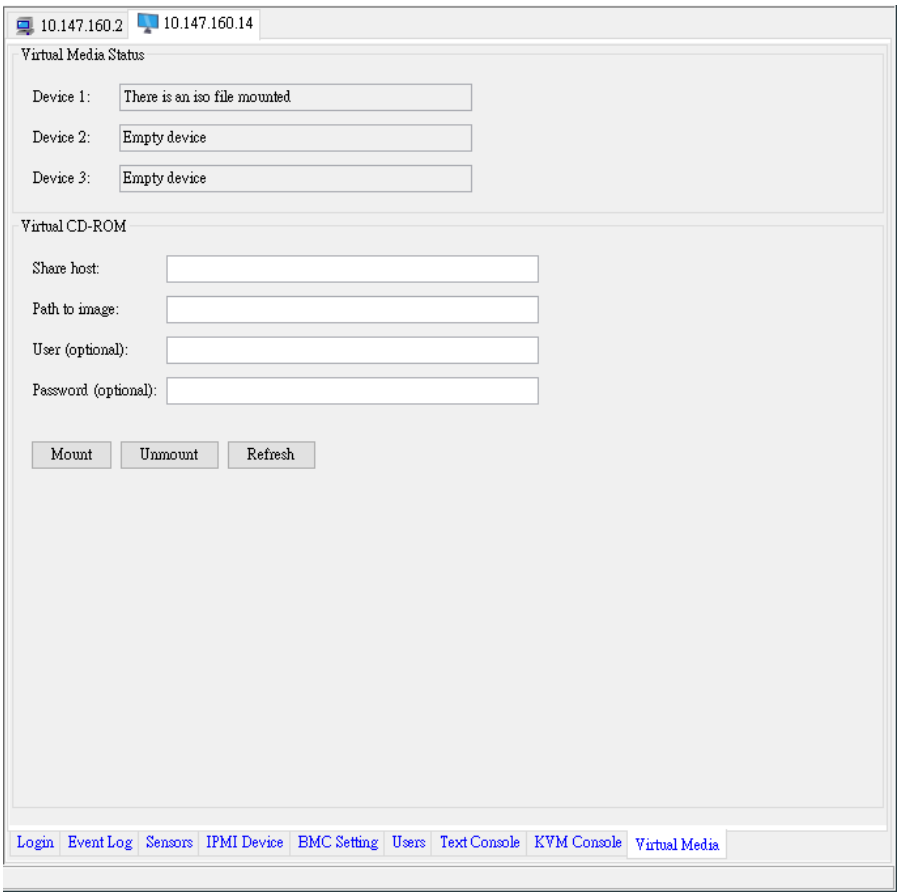


Figure 11-7

- **Virtual Media Status:** Displays the current virtual device status.
- **Virtual CD-ROM**: Allows users to configure Windows-Share or Samba settings. You can decide how to mount the data stored in your shared folder to the target device.
  - **Share Host**: Enter the IP address or the name of the system where the source data is located.
  - **Path to Image**: Enter the location of the source file on the share-host.
  - **User/Password (Optional)**: Enter the username and password for the share-host if needed.
  - **Mount**: Click the **Mount** button to connect the source, which will automatically refresh after mounting.
  - **Unmount**: Click the **Unmount** button to disconnect the source, which will automatically refresh after unmounting
  - **Refresh**: Click the **Refresh** button to update the virtual media status.

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 the **Manage Group** button to show the Group Management screen. 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.

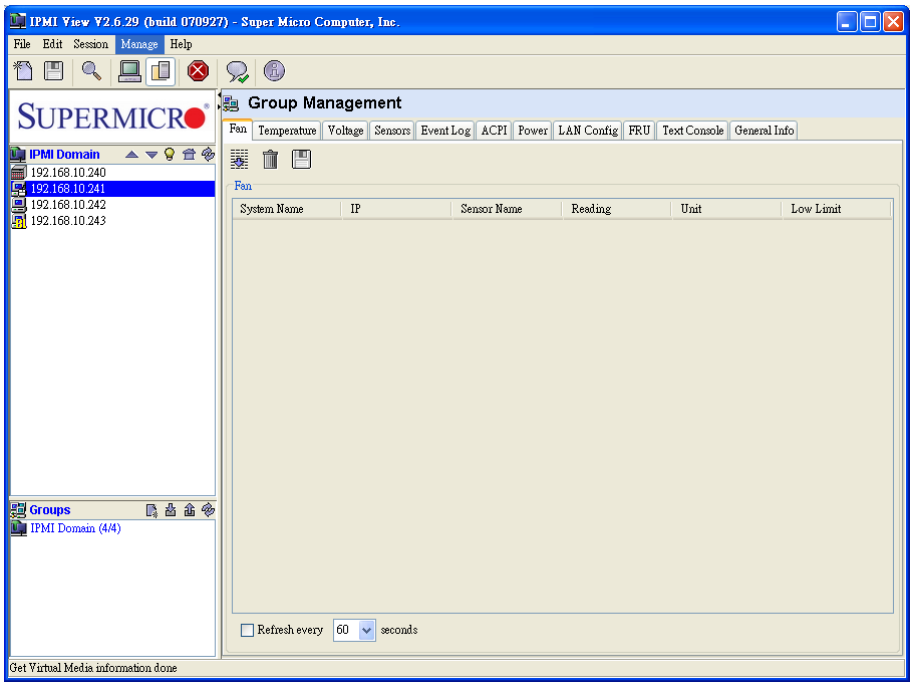


Figure 12-1

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 allows servers to be grouped in the following categories:

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

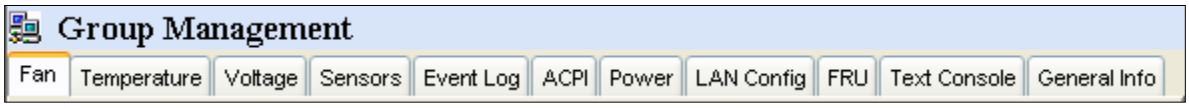


Figure 12-3

Fans

After you've selected multiple servers and clicked the **Fan** tab, a window will display as shown in Figure 12-4. You can press **<Ctrl+Click>**, **<Shift+Click>** or dragging 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.

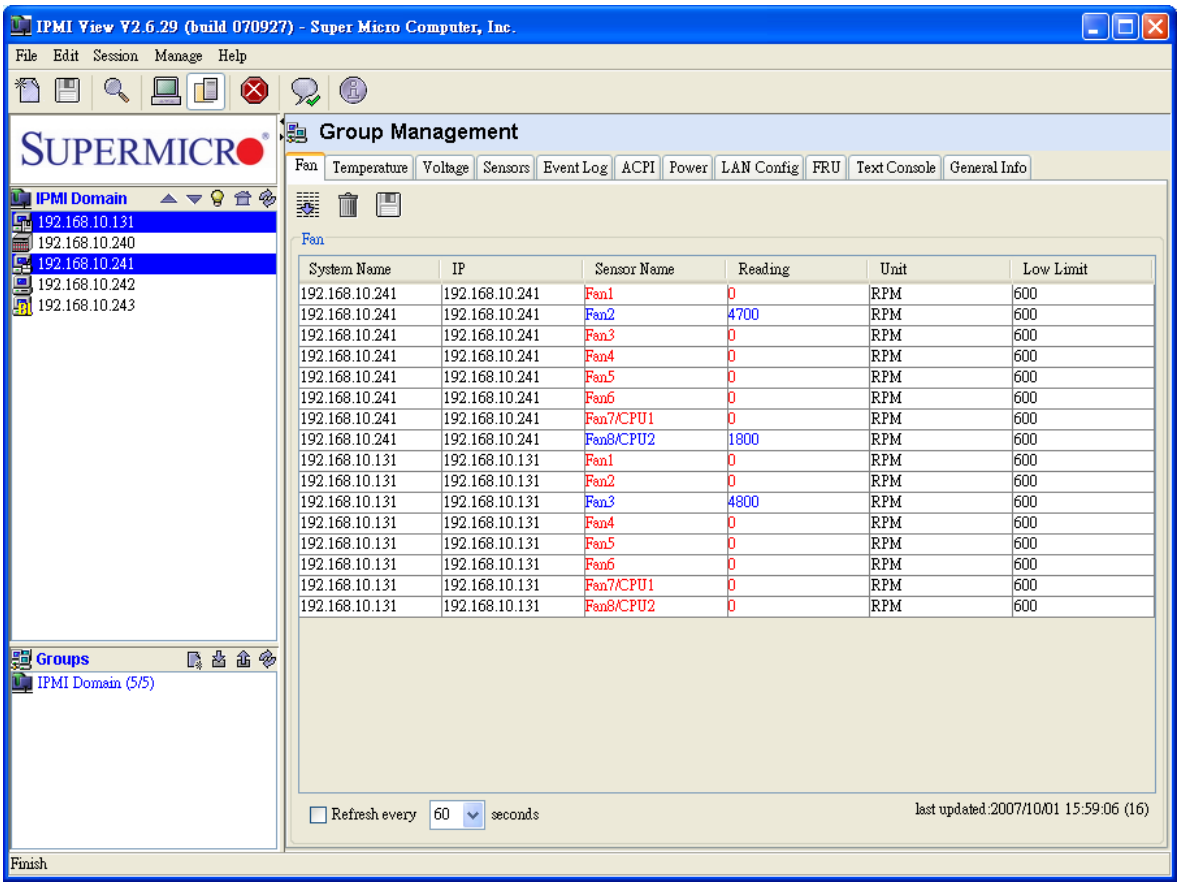


Figure 12-4

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.

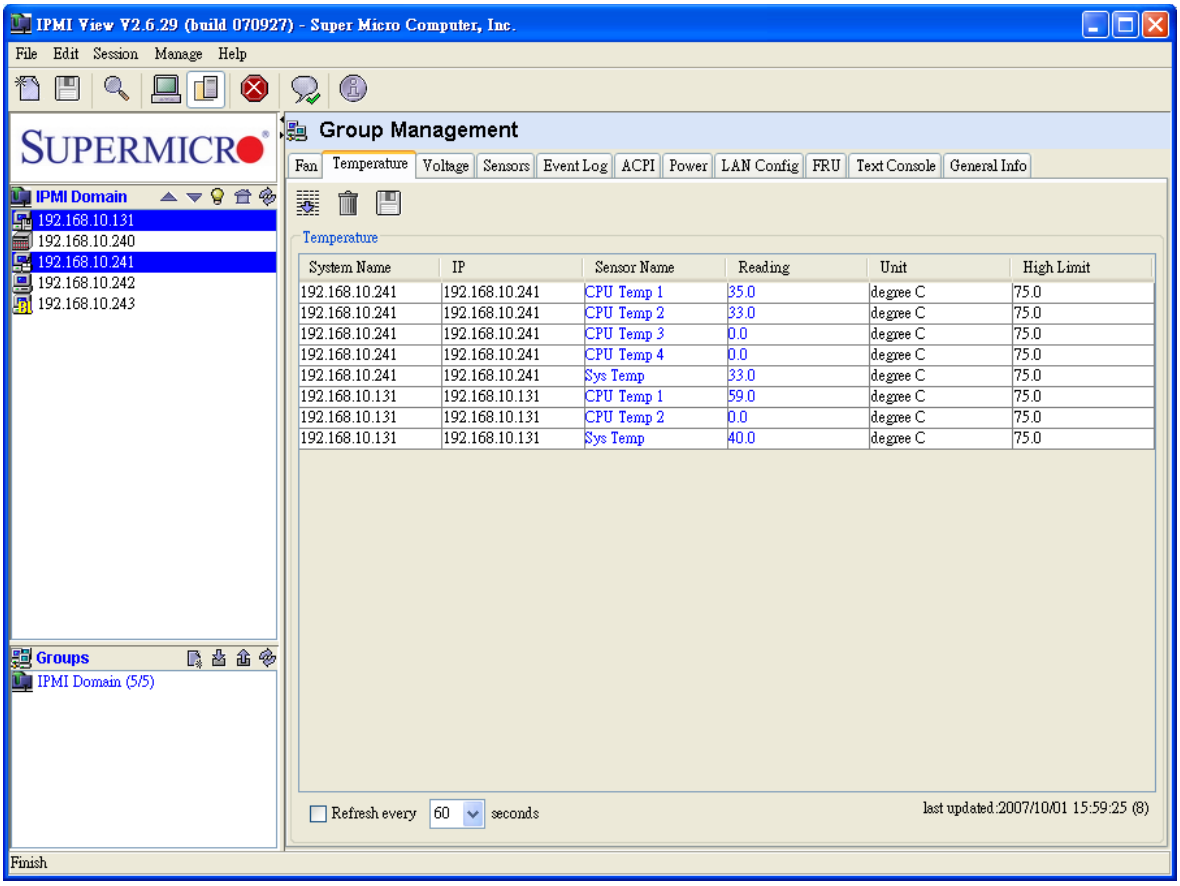


Figure 12-5

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.

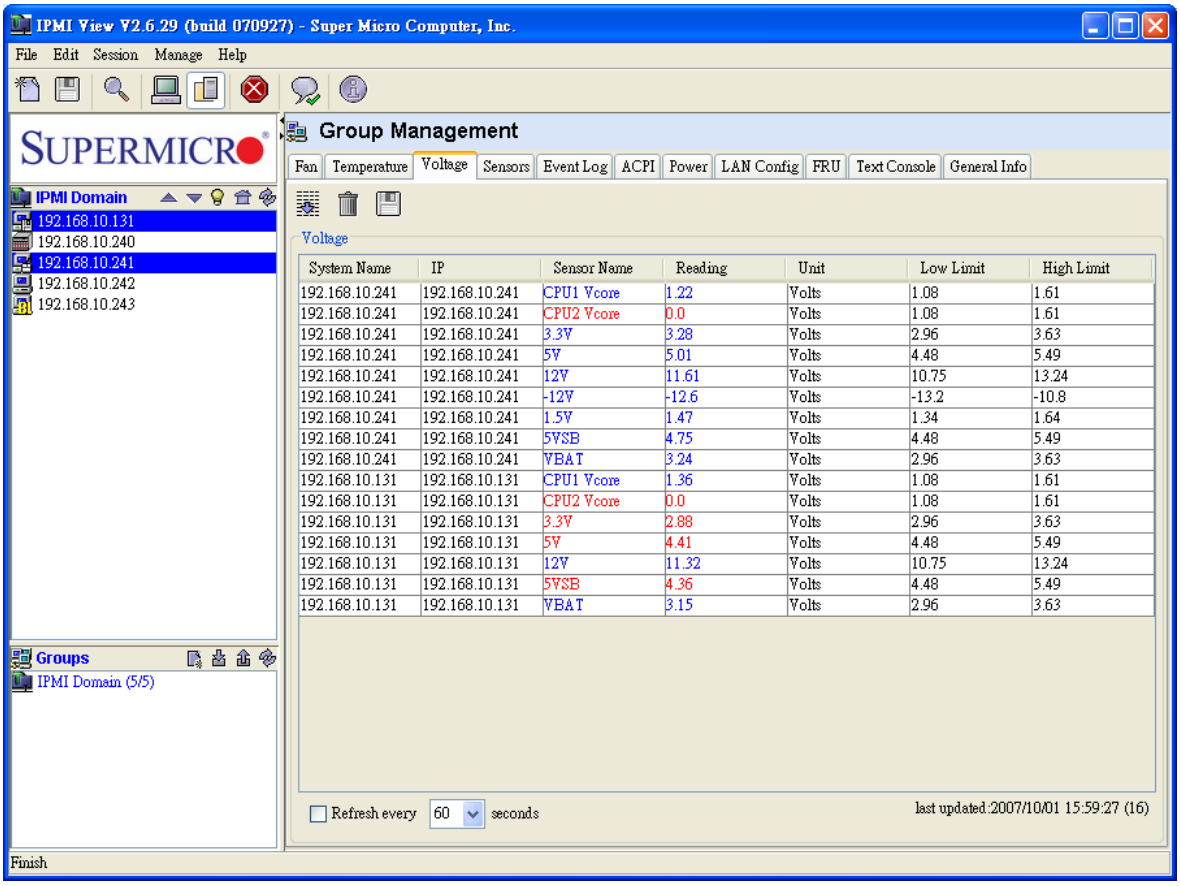


Figure 12-6

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.

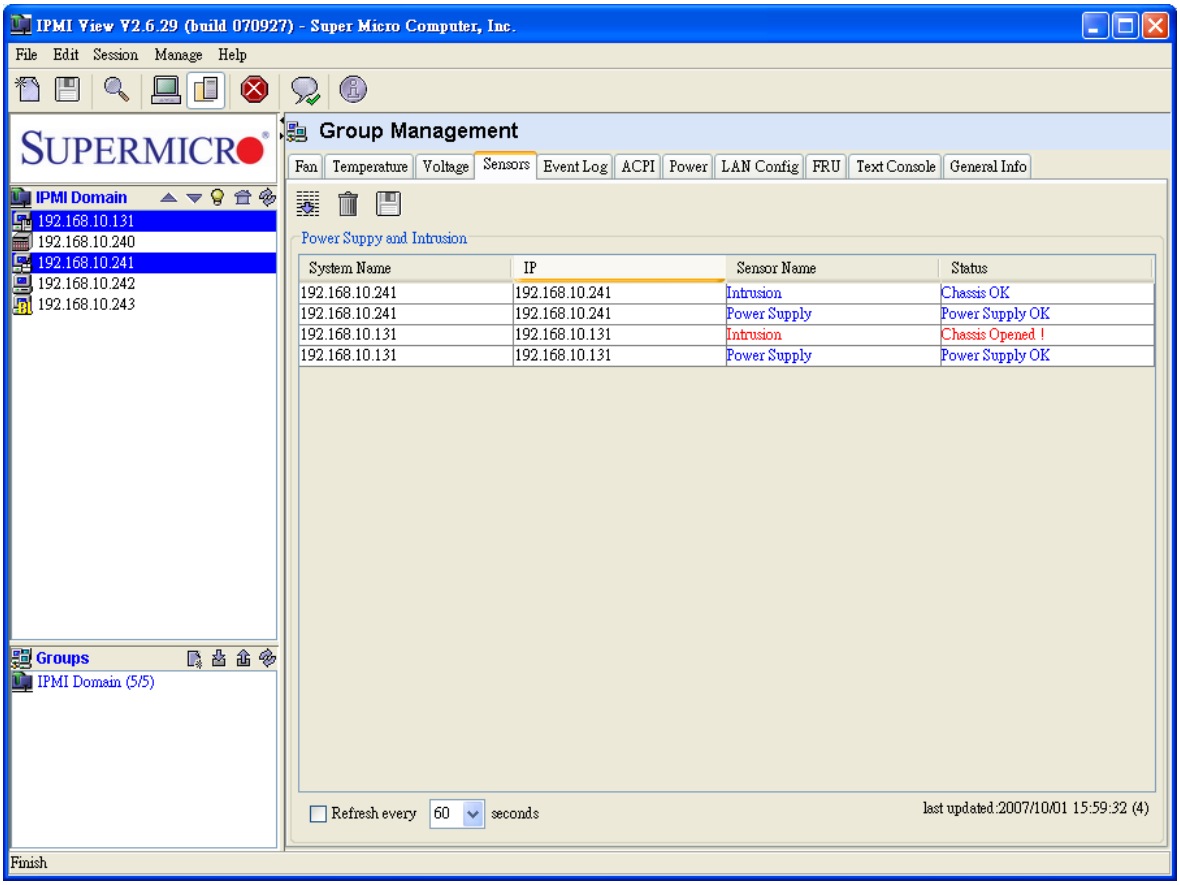


Figure 12-7

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.

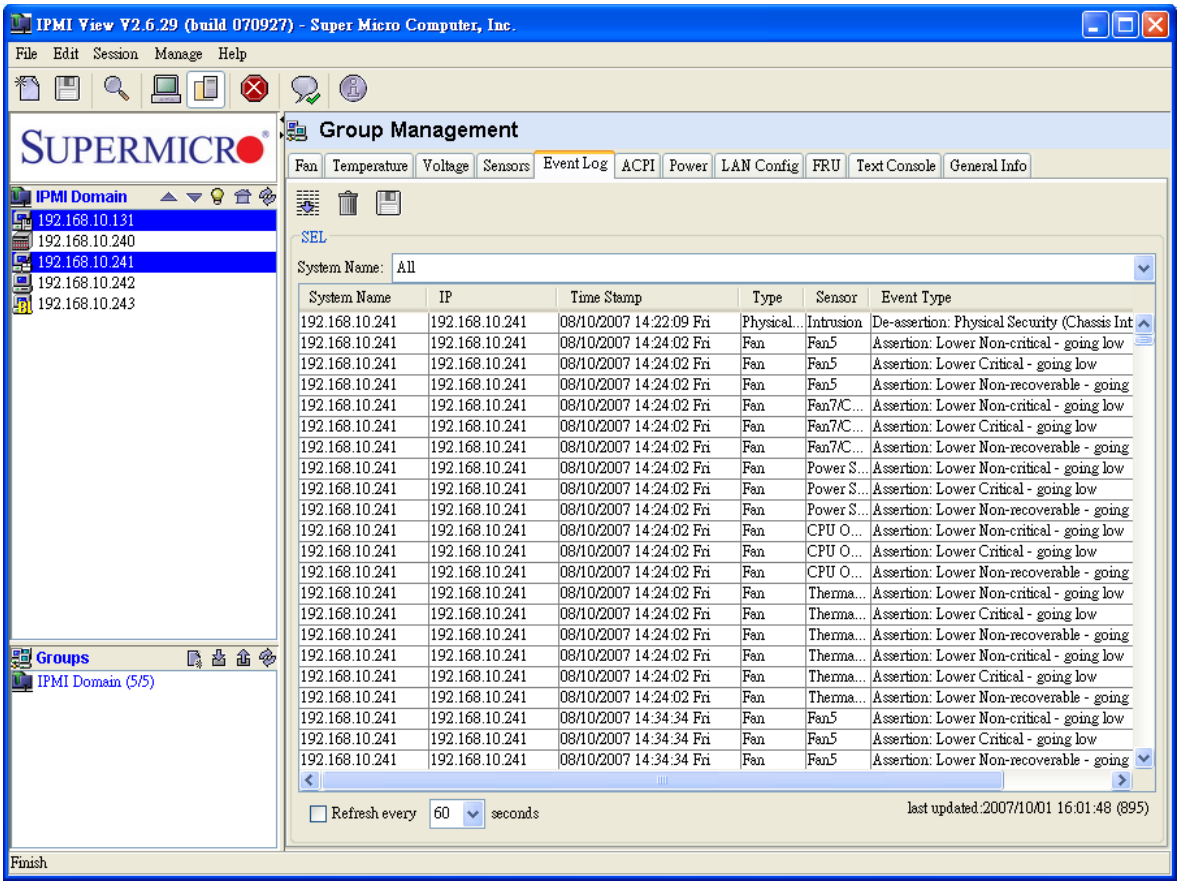


Figure 12-8

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.

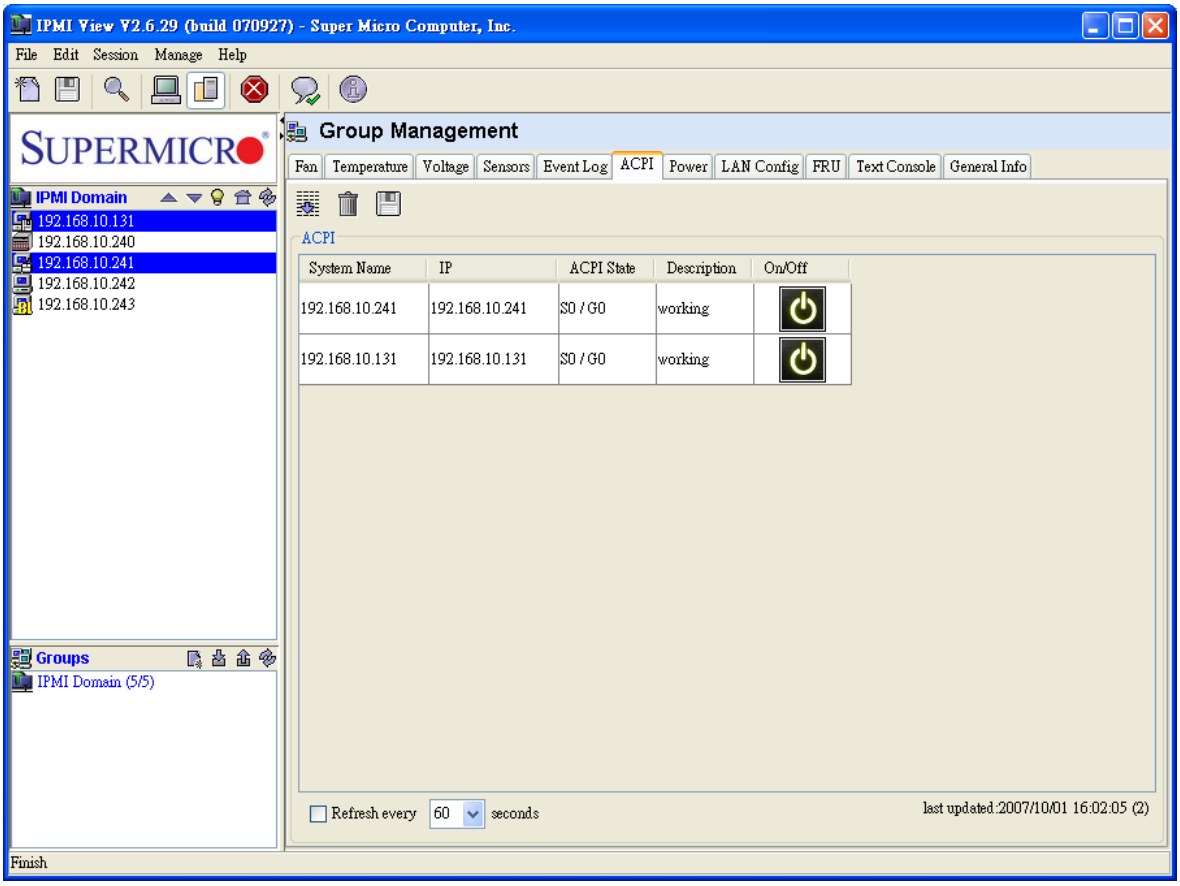


Figure 12-9

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.

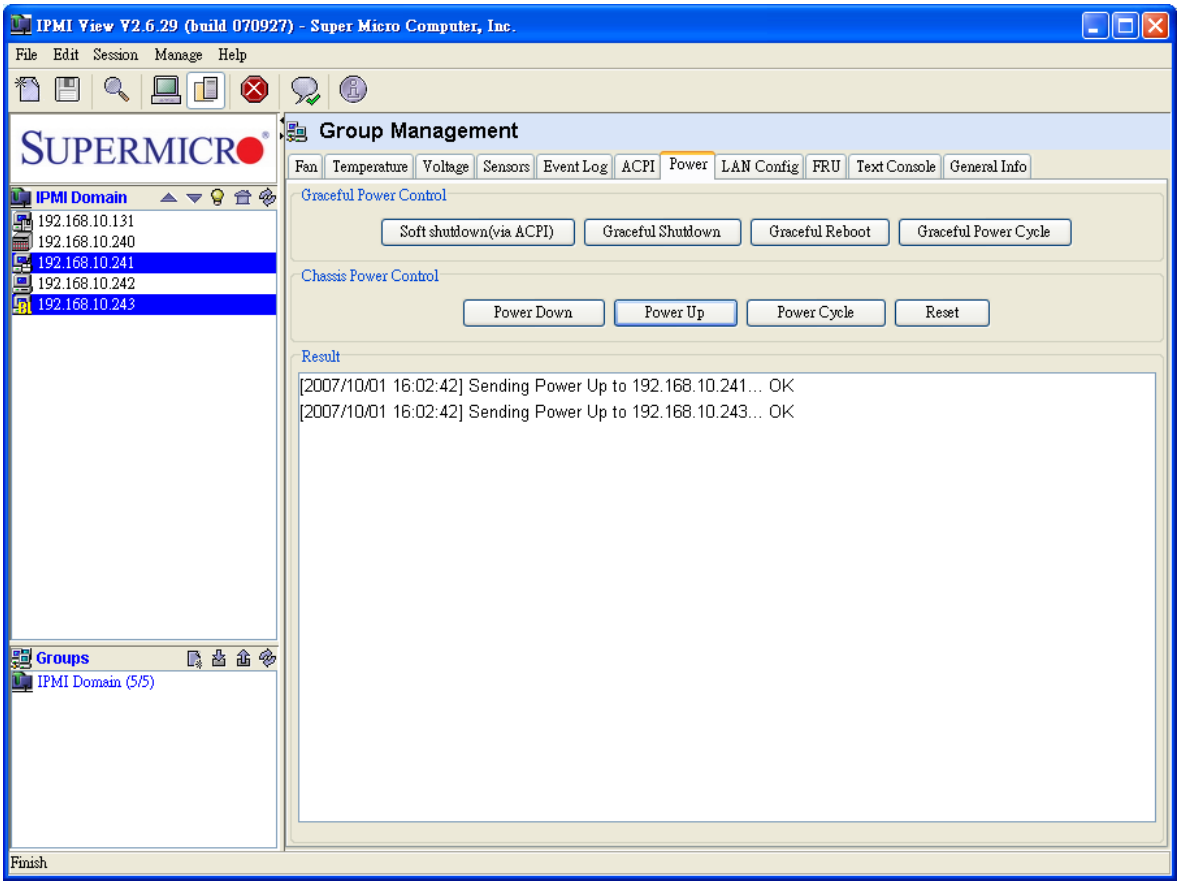


Figure 12-10

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.

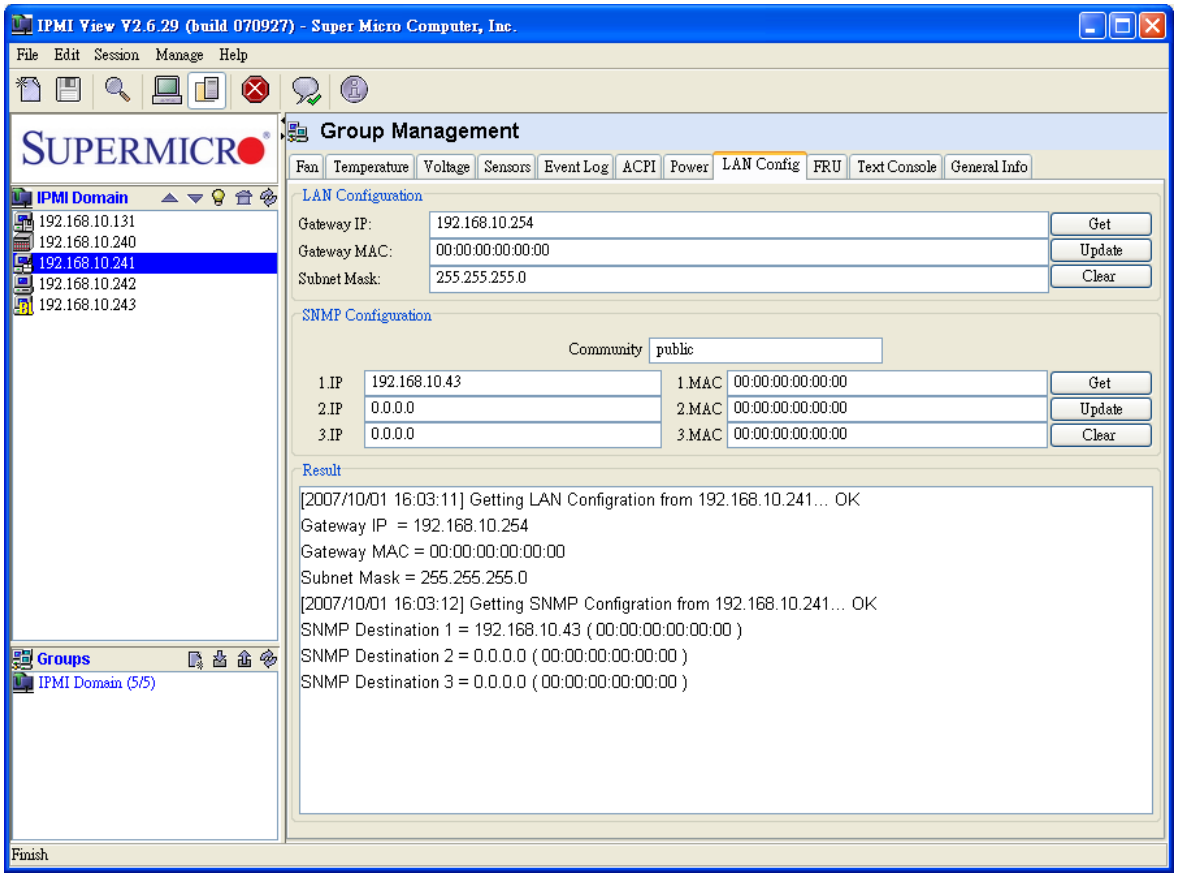


Figure 12-11

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.

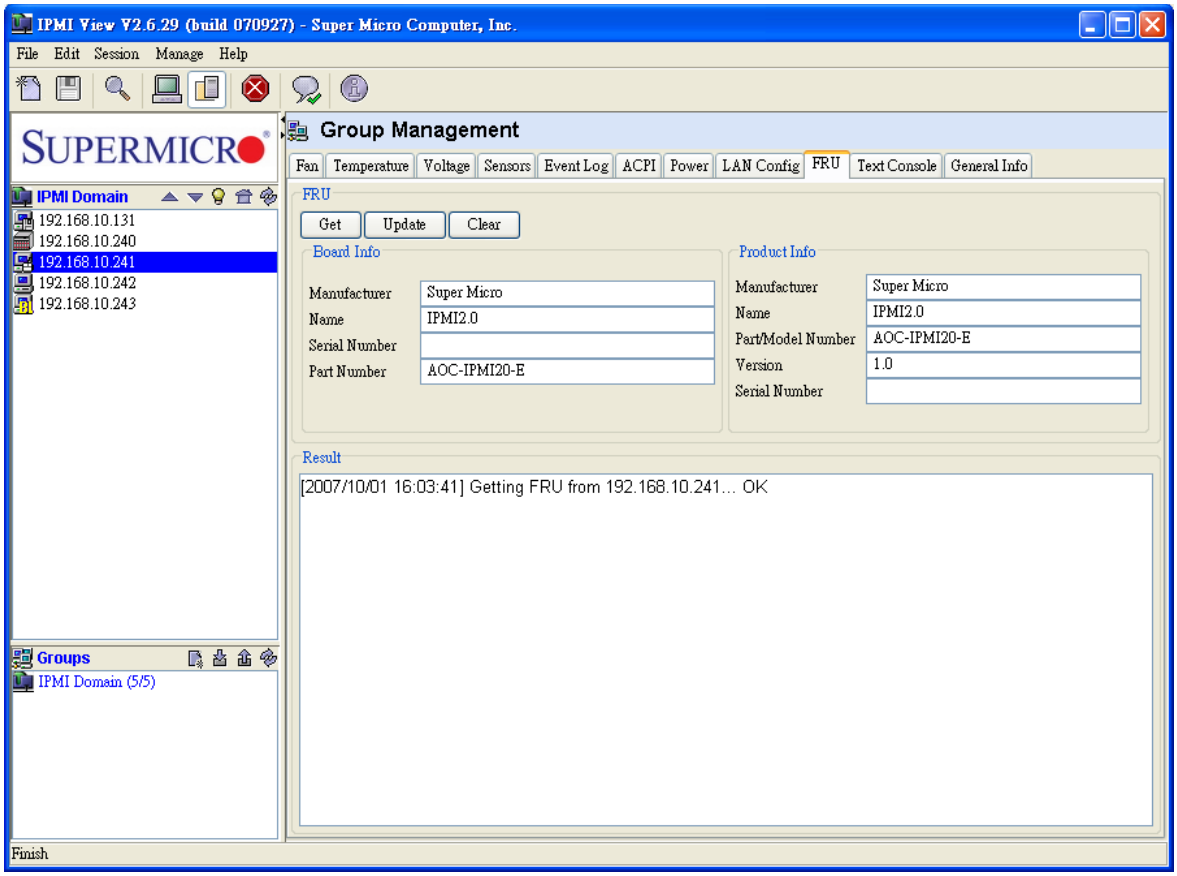


Figure 12-12

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.

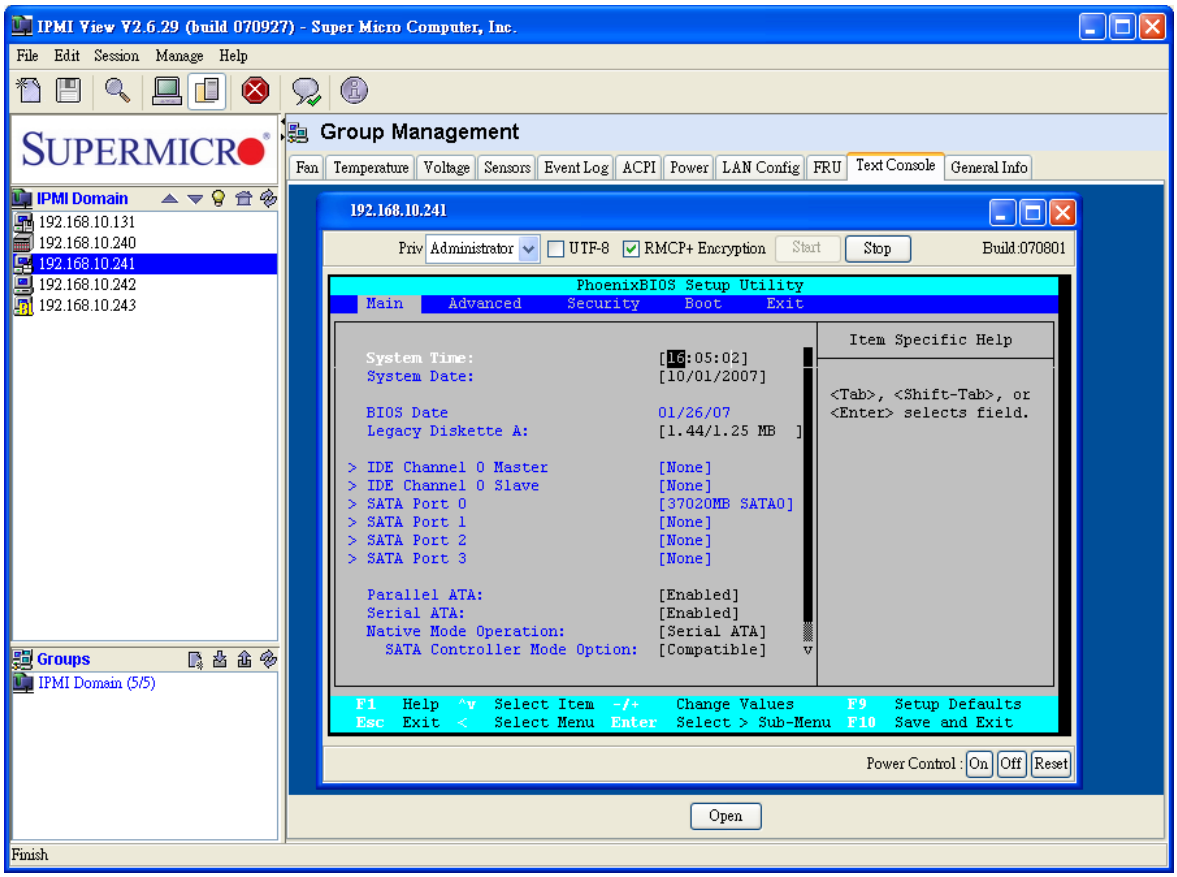


Figure 12-13

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.

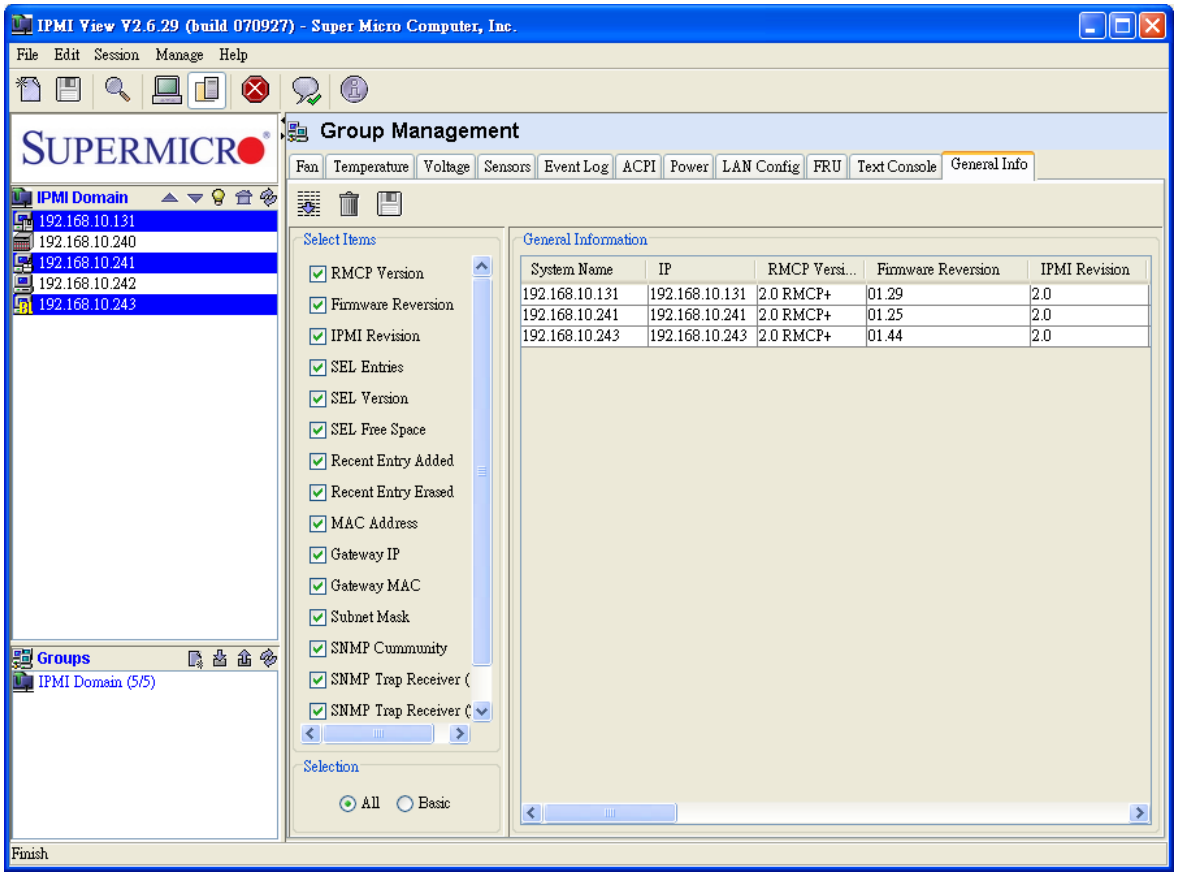


Figure 12-14

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 SNMPv1/v3 traps to the destinations set in the BMC. The Trap Receiver is executed on the destination site and receives the SNMPv1/v3 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 SNMPv1/v3 destination.

As shown in Figure 13-1, there are several components to the IPMI Trap Receiver.

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

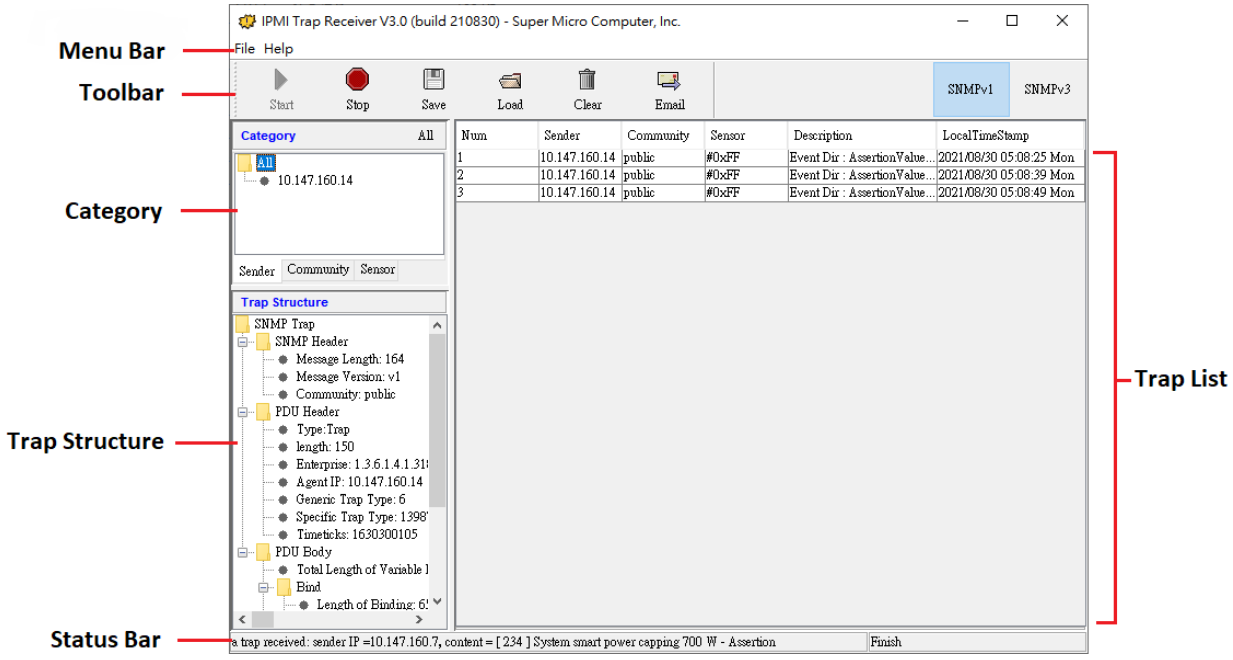


Figure 13-1

Menu Bar

As shown in Figure 13-2 and 13-3, click **File> Preferences** to set the SNMPv3 Trap User Table. This user table configuration is used to decrypt SNMPv3 traps by Trap Receiver. In the User Table, a Username, Authentication model, Authentication password, Privacy protocol and Privacy password are required. If you want to add or remove the configuration of SNMPv3 trap, you first need to click "**+**" or "**-**" buttons. If you want to load other properties file or change file path, you need click the folder path. Click **OK** to save the current SNMPv3 Trap configuration settings.

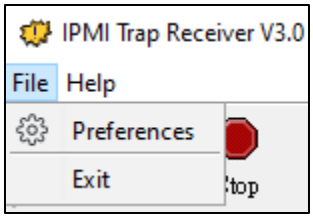


Figure 13-2

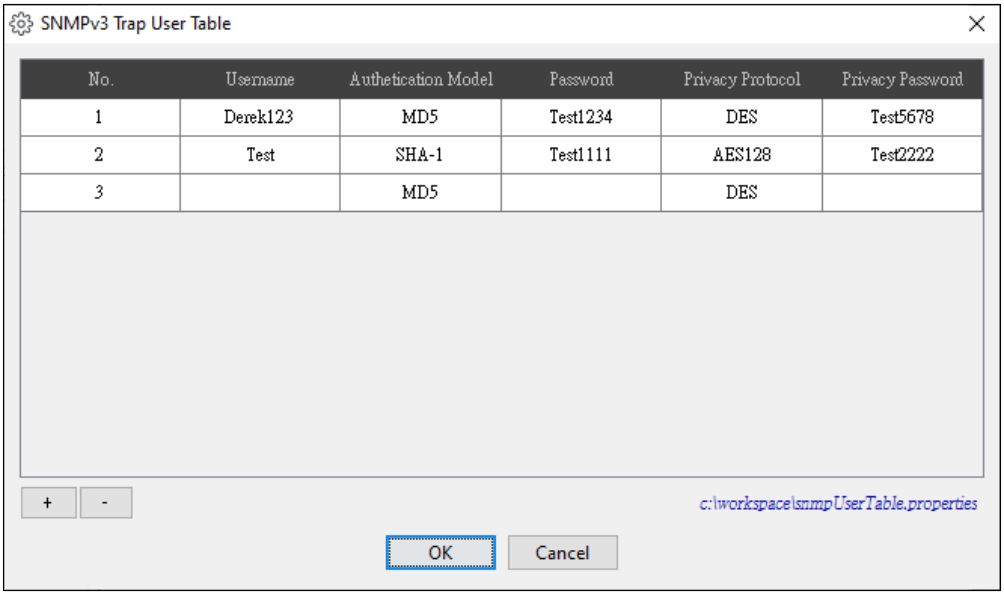


Figure 13-3

Tool Bar functions

The tool bar provides the following features as shown in Figure 13-4.

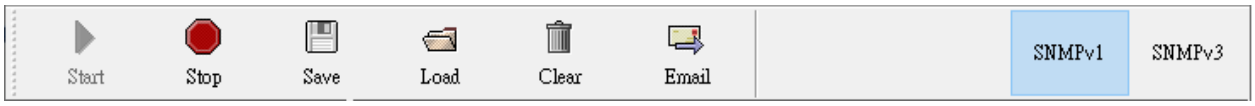


Figure 13-4

- **Start:** starts the Trap Receiver.
- **Stop:** stops the Trap Receiver.
- **Save:** saves the SNMPv1 or v3 traps received into a file by selected file extension (see Figure 13-5).
- **Load:** loads a saved SNMPv1 or v3 trap file into the Trap Receiver by selected file extension (see Figure 13-6).
- **Clear:** clears all the SNMPv1/v3 traps in the trap list.
- **Email:** displays an "Email-Alert Settings" dialog box (see Figure 13-7). 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.
- **SNMPv1:** Displays SNMPv1 traps in Trap List.
- **SNMPv3:** Displays SNMPv3 traps in Trap List.

Note: For some mail servers, the Enable TLS checkbox should be clicked so that emails can be sent.

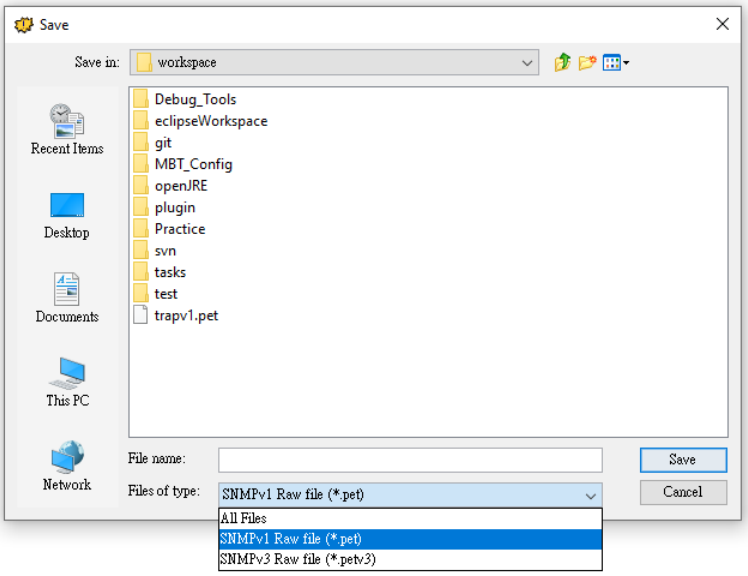


Figure 13-5

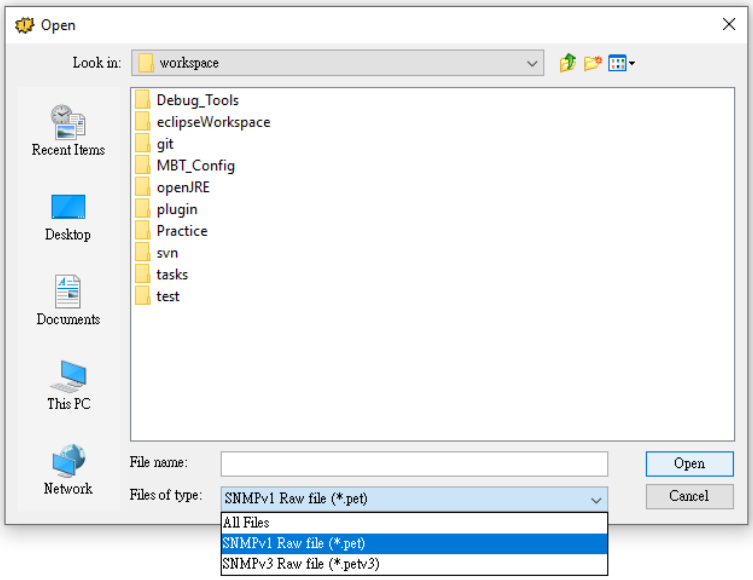


Figure 13-6

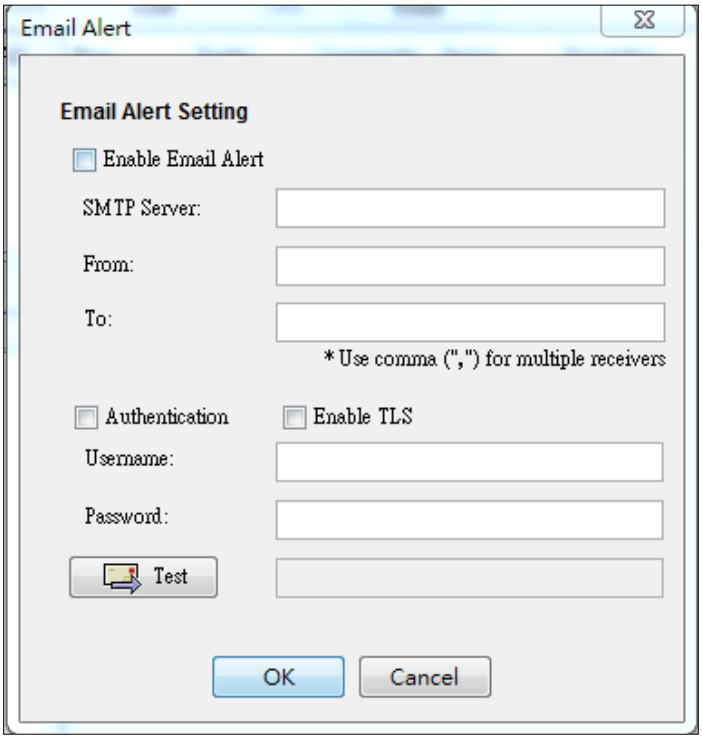


Figure 13-7

Category

There are three SNMPv1 categories including: Sender, Community and Sensor as shown in Figure 13-8. 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.

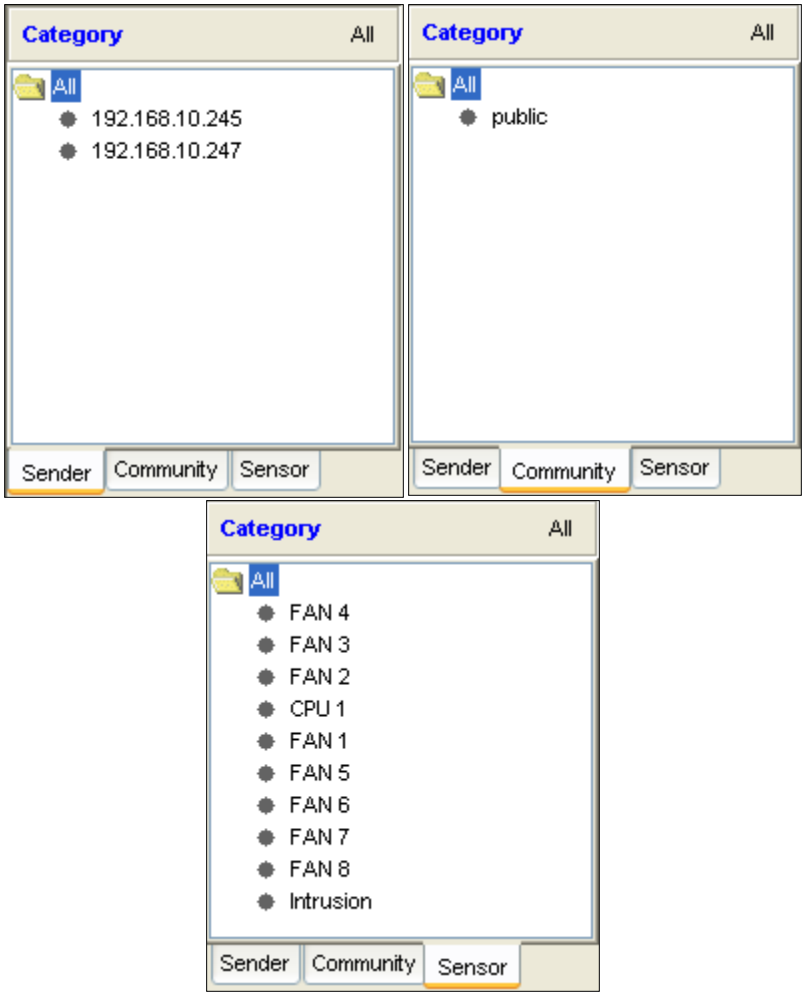


Figure 13-8

There are four SNMPv3 categories including: Sender, Sensor Name, Sensor Type and Username as shown in Figure 13-9. The Sender page lists all sender IP addresses. The Sensor Name page lists all Sensor Name from the traps. The Sensor Type page lists all sensor types from the traps. The Username page lists all username 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.

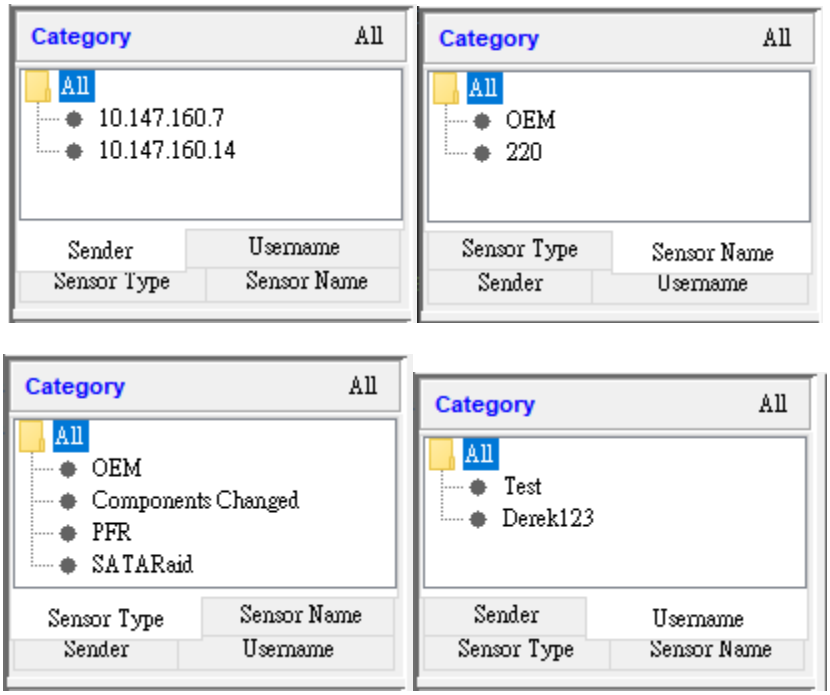
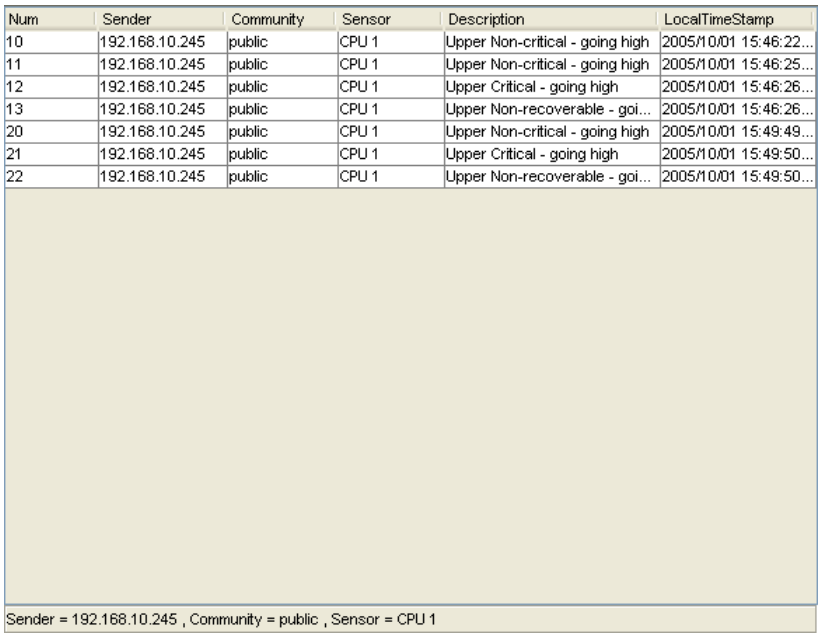


Figure 13-9

Once a category has been selected, the filter condition will be displayed at the bottom of the “trap” list. See Figure 13-10 for reference. As displayed in Figure 13-10, 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 13-10

Trap Structure

The Trap Structure displays detailed information for the selected item in the trap list.

SNMPv1 Information includes the “SNMP Header,” “PDU Header”, “PDU Body”, “Bind” and “PET” data as shown in Figure 13-11.

SNMPv3 Information includes the “SNMP Header”, “Decrypted ScopedPDU”, “PDU Header”, “PDU Body” and “Bind” data as shown in Figure 13-12.

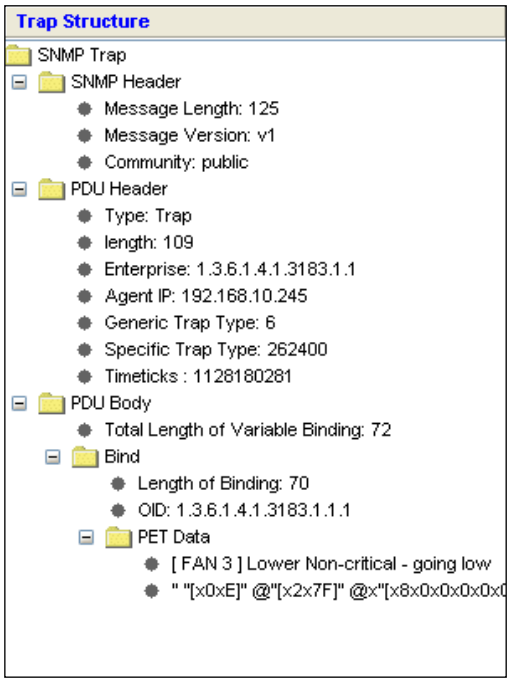


Figure 13-11

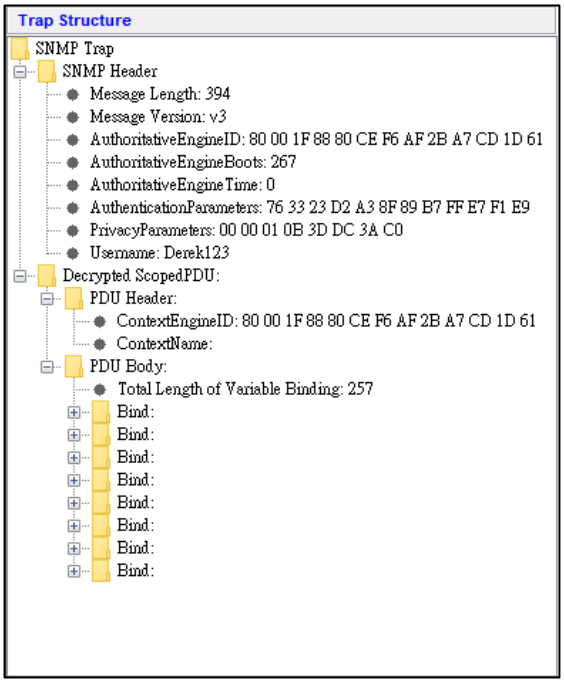


Figure 13-12

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 Figures 13-13 and 13-14

The SNMPv1 email will include the following information.

```
A SNMP trap received
Sender:10.147.160.14 (community:public )
Sensor:#0xFF
Description:Event Dir : Assertion
Value: Device @ 0 CPLD @ 3 Slot @ 5 Ejected
Time:2021/08/31 05:30:56 Tue
```

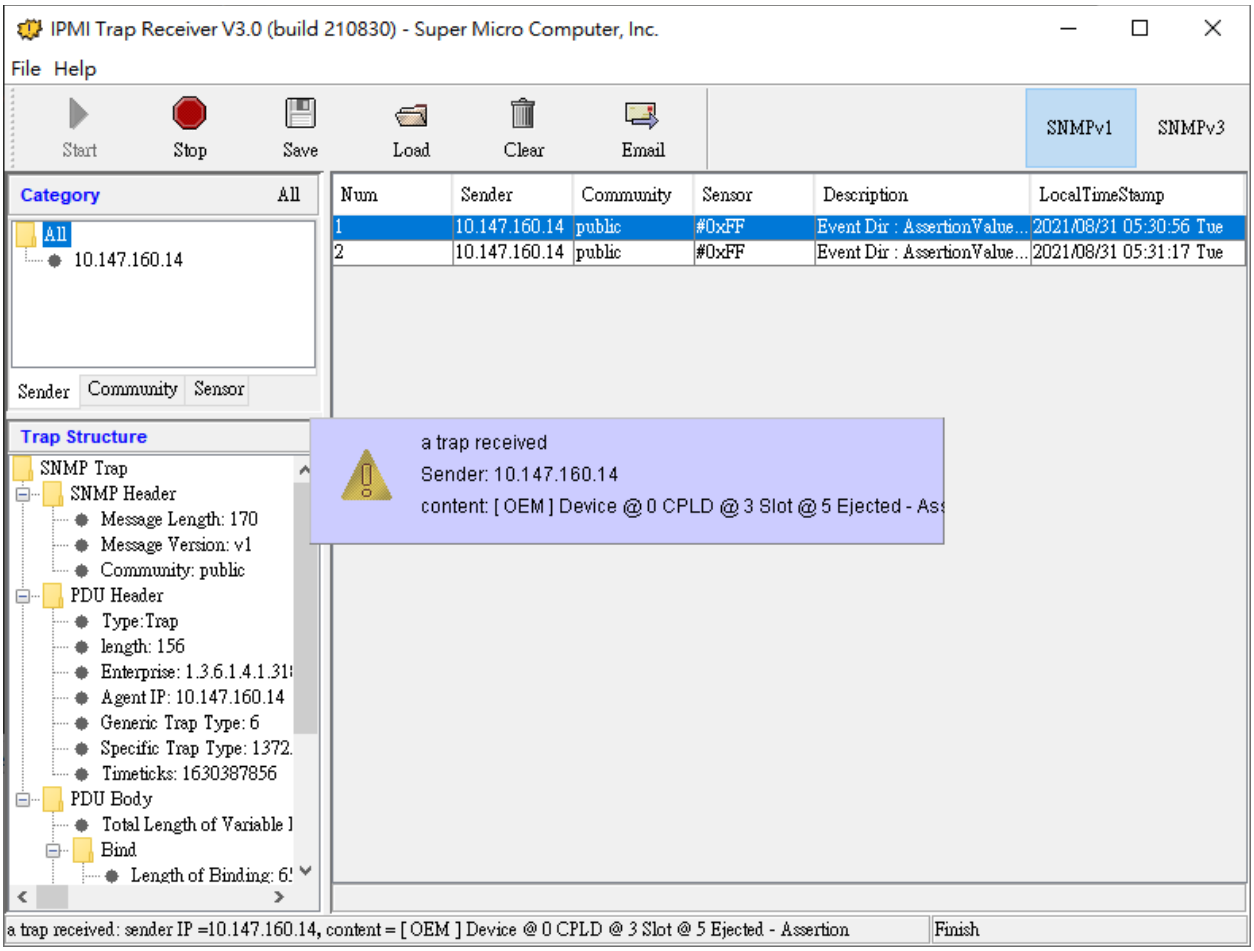


Figure 13-13

The SNMPv3 email will include the following information.

```
A SNMPv3 trap received
Sender:10.147.160.14 (Username:Derek123 )
Time: 2021/08/30 15:09:56 Mon
Sensor Type:NVMe
Sensor Name:OEM
Description:Device @ 0 CPLD @ 3 Slot @ 5 Ejected – Assertion
```

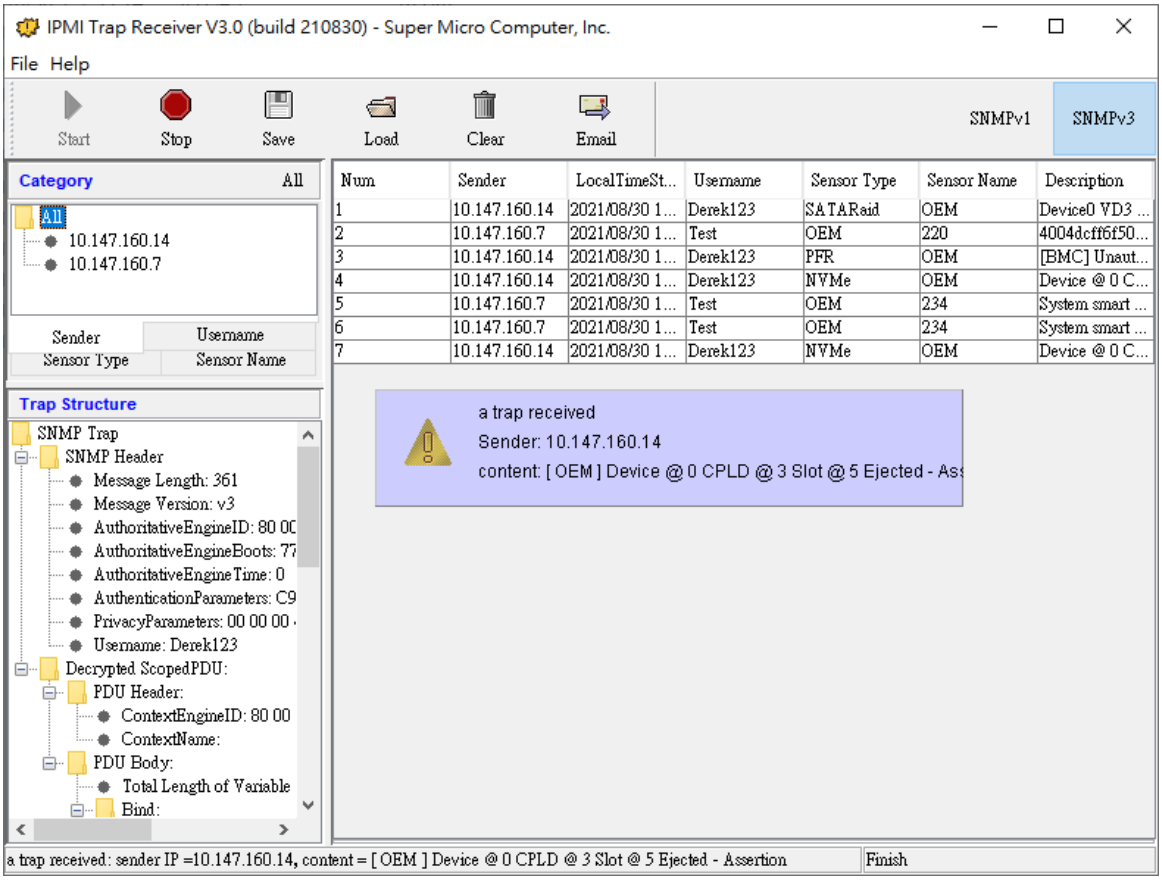


Figure 13-14

14 IPMIView Software Update

To check the latest version of IPMIView, follow these steps.

1. Click **Help** on the menu bar and then select **Check for updates** in the pull-down menu (see Figure 14-1). This will allow IPMIView to check the Supermicro website for a new version.

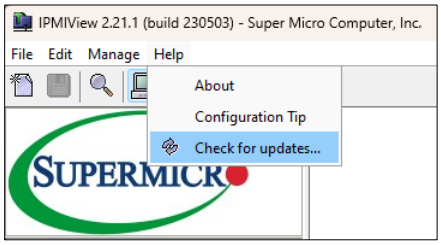


Figure 14-1

2. As shown in Figure 14-2, click **Download** to start downloading the file to update if a new revision is available.

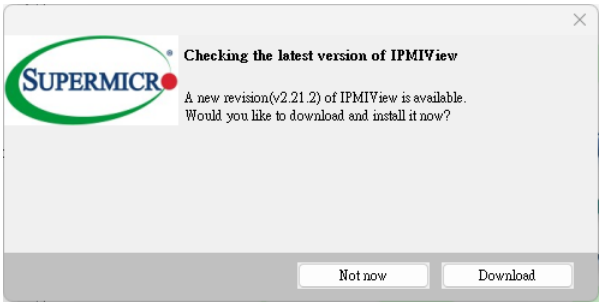


Figure 14-2

3. When the download is complete, click **Open** to launch the installation. The IPMIView application will be closed once you click **Yes** to continue.

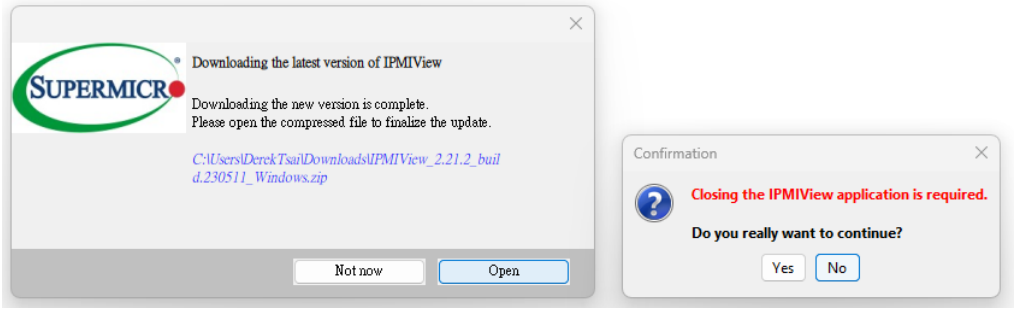


Figure 14-3

4. Afterwards, note that executing the update file on Windows is different from Linux.
   - On Windows: The .exe file is automatically executed to start the installer wizard.

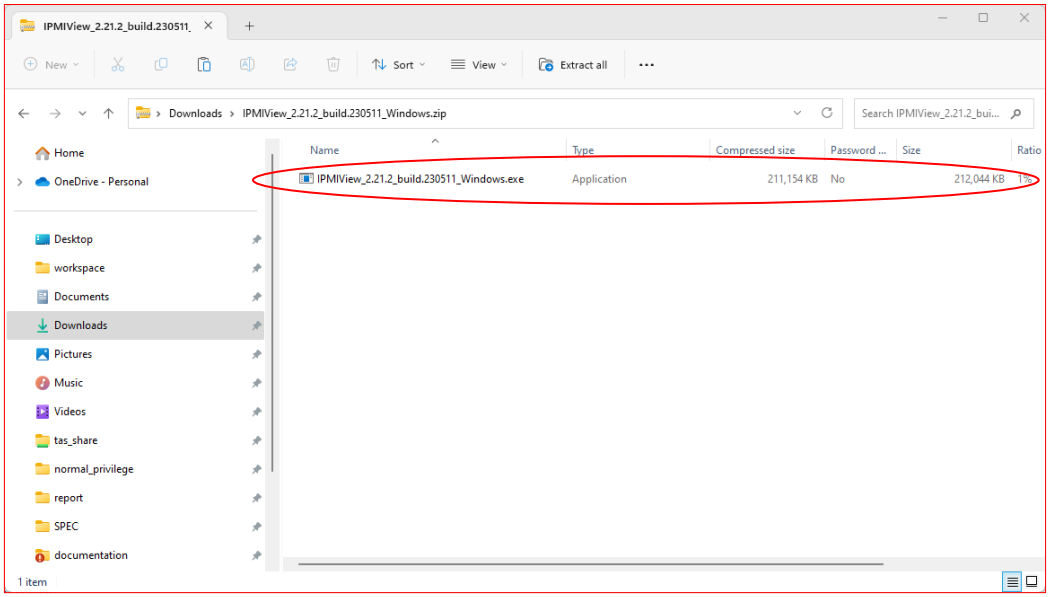


Figure 14-4

   - On Linux: Extract and execute the file to continue the installation.

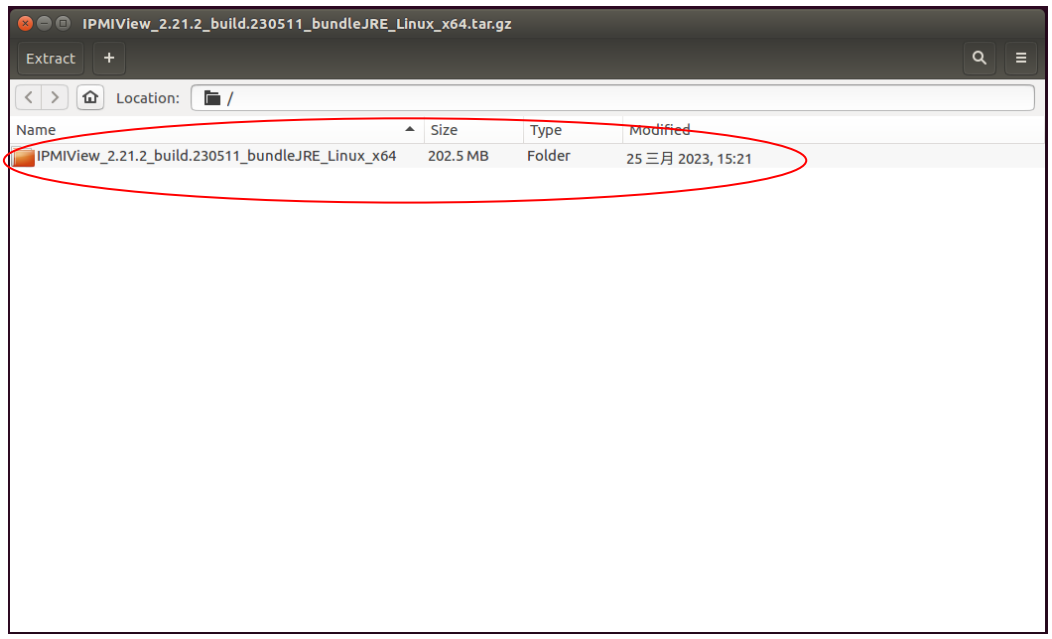


Figure 14-5

Appendix A: SIM Firmware Update

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

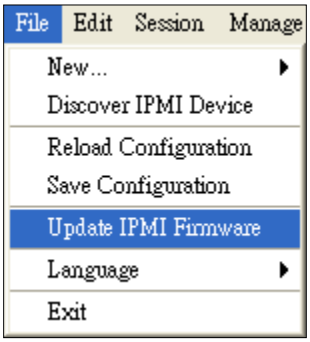


Figure A-1

- Click the **Open** button to select the firmware you desire and then click **Start** to continue.

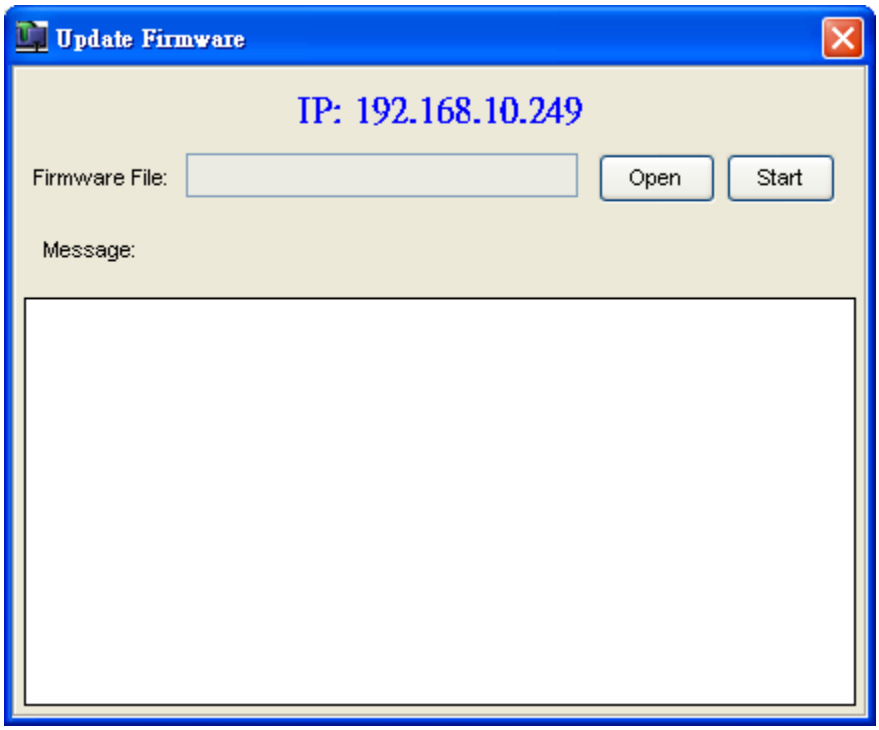


Figure A-2

- 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

- A firmware information dialog will appear. It shows detailed information on the current and new firmware. Click **Yes** to continue.

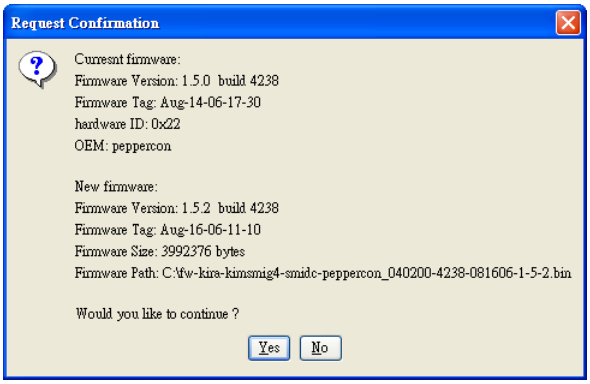


Figure A-4

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

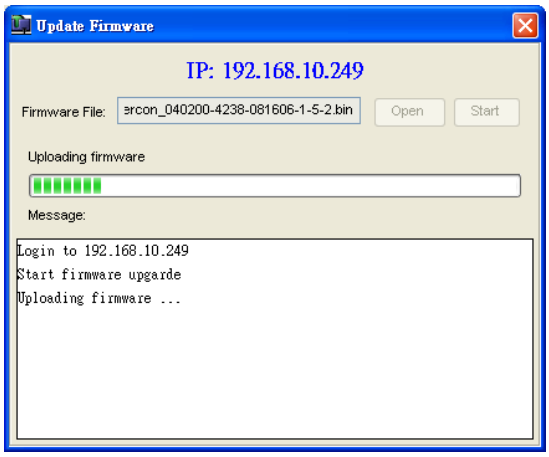


Figure A-5

- 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.

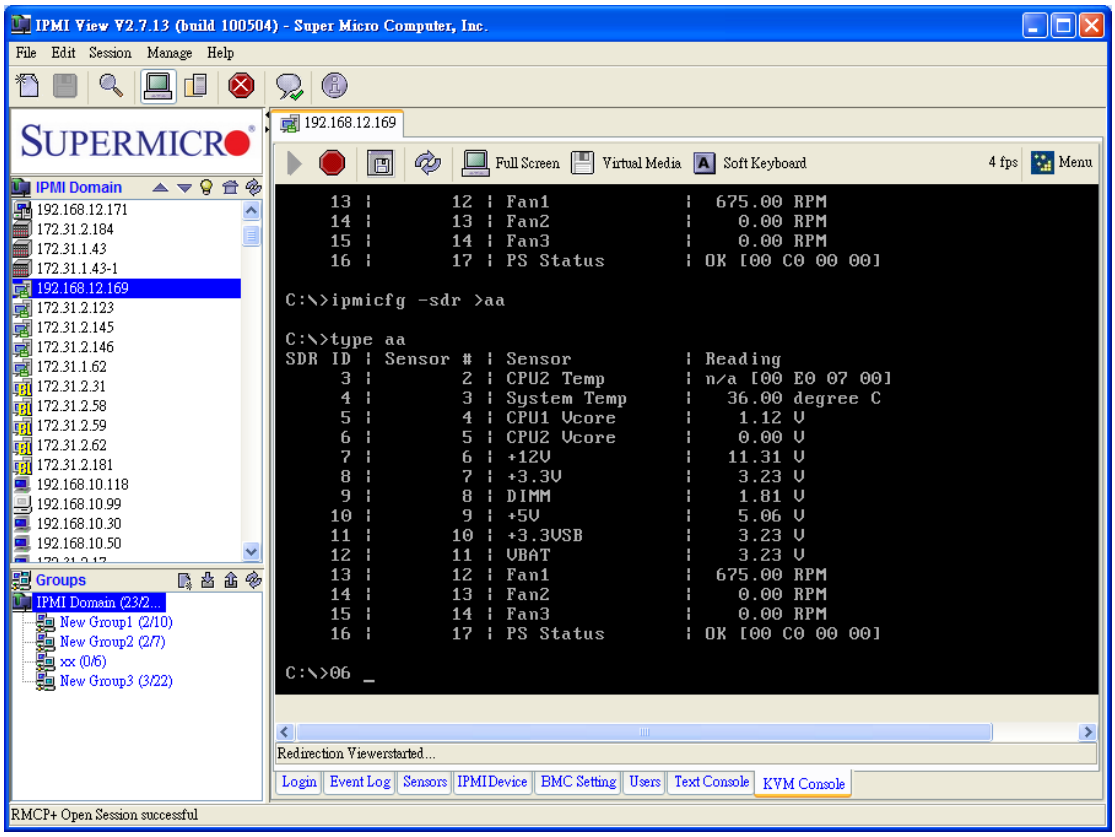


Figure B-1 SIM(W) KVM Console Main Screen

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.

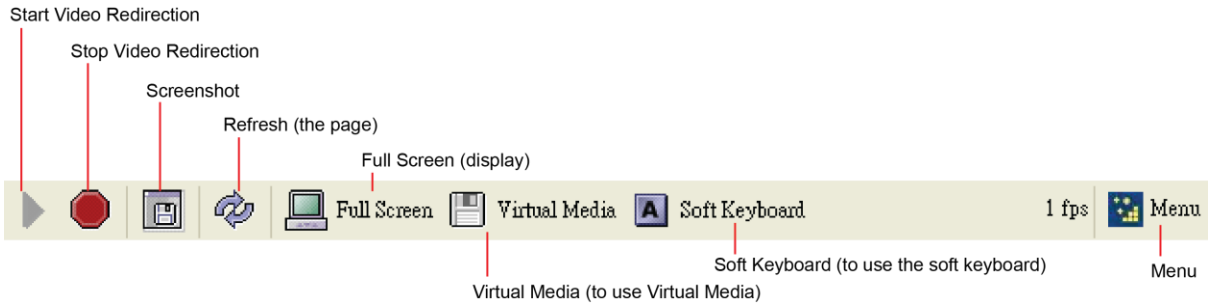


Figure B-2 SIM(W) KVM Console Toolbar

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.

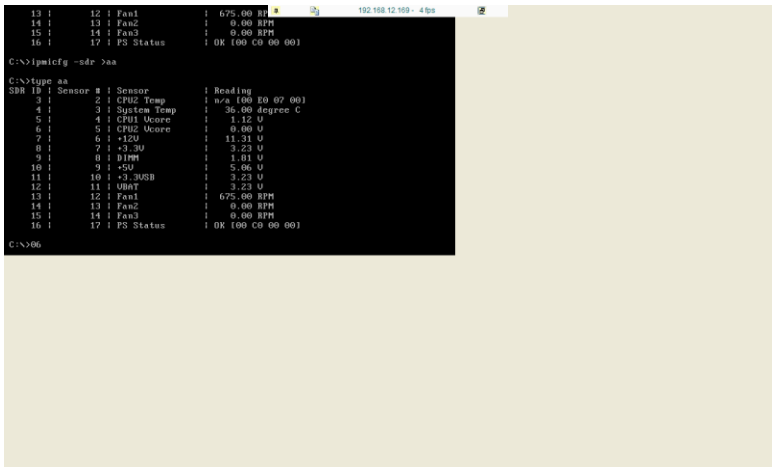


Figure B-3 Full Screen

Virtual Media:

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

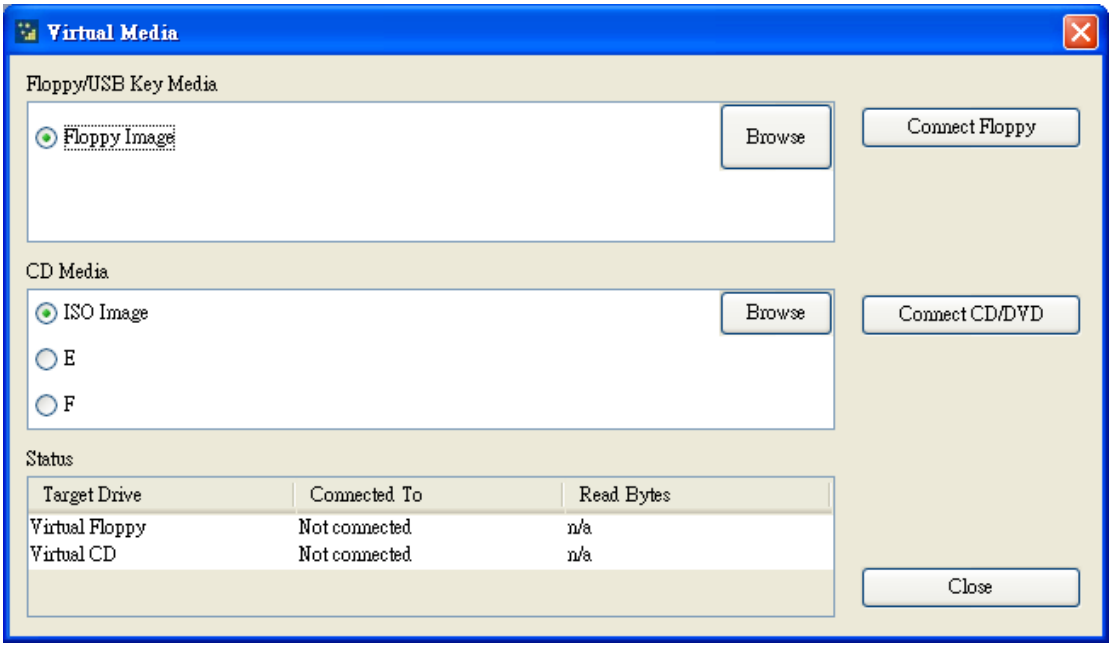


Figure B-4 Virtual Media

- **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.

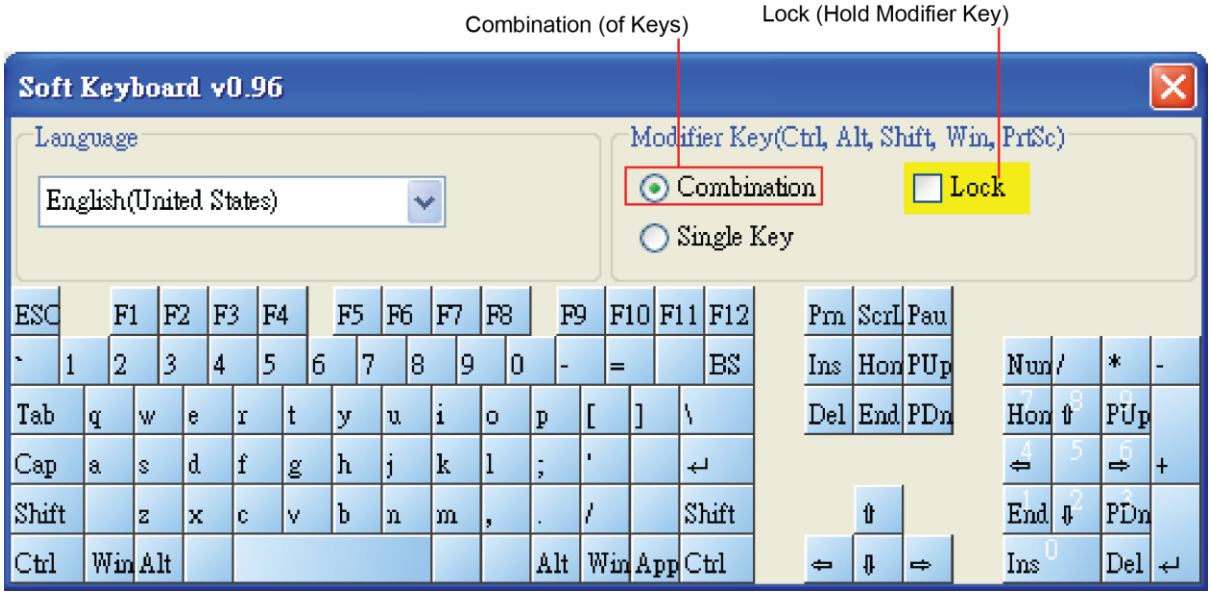


Figure B-5 Soft Keyboard

- **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

Click **Launch KVM Console** to open SIM(WA) iKVM Window as in Figure C-1.

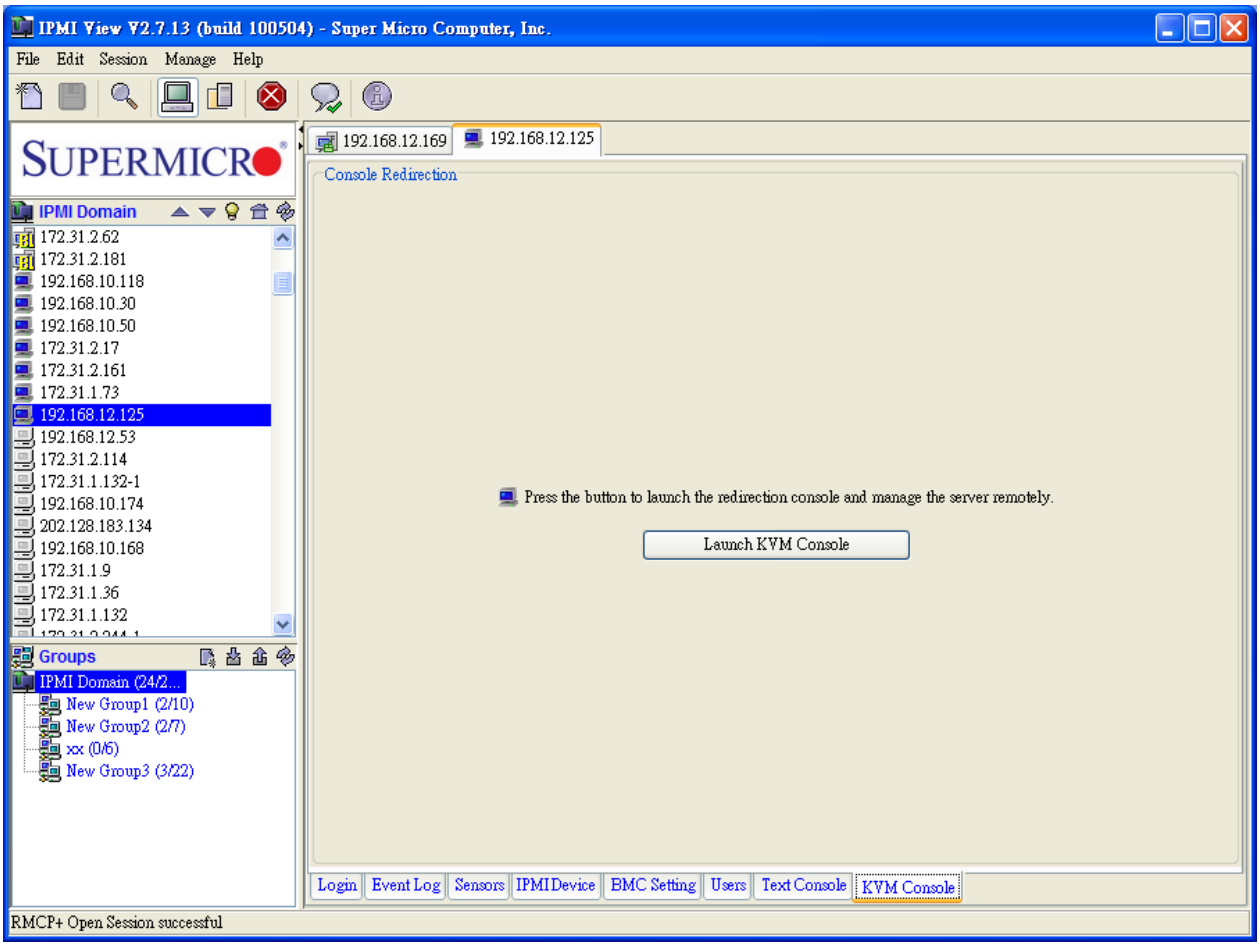


Figure C-1 SIM(WA) iKVM Window

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.

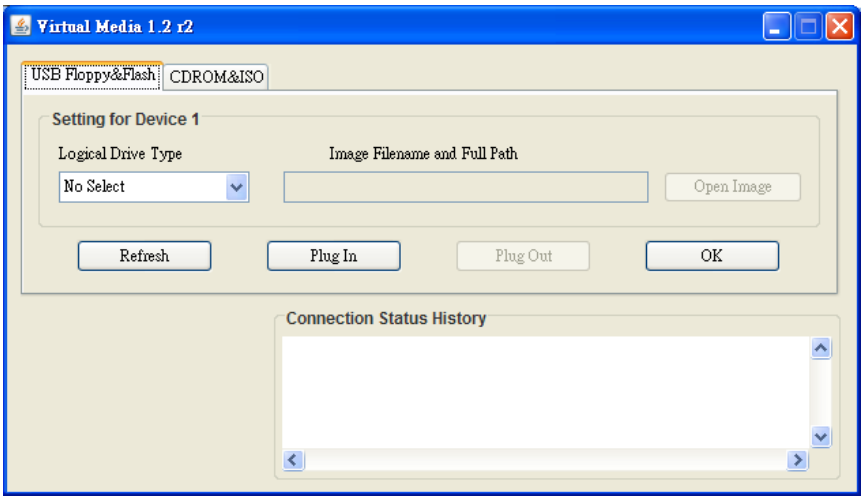


Figure C-3 Virtual Media (USB Floppy & Flash)

- **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.

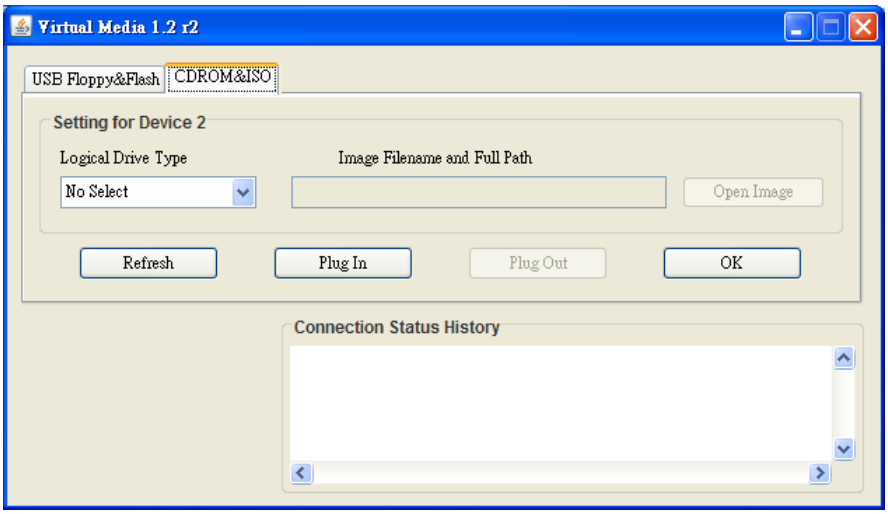


Figure C-4 Virtual Media (CDROM & ISO)

- **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

1. To re-flash SIM(W) Firmware, select an SIM(W) device, click **File** on the menu bar and then select Update **firmware** in the pull-down menu. A dialog box appears.

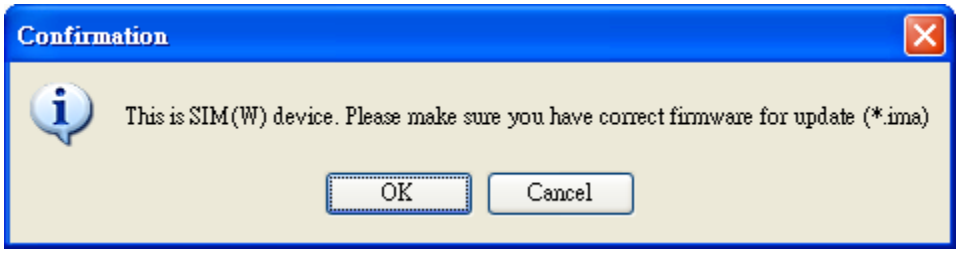


Figure D-1 SIM(W) Firmware Re-flash

2. Make sure that you select the correct firmware for update, and click **OK**. This dialog box appears.

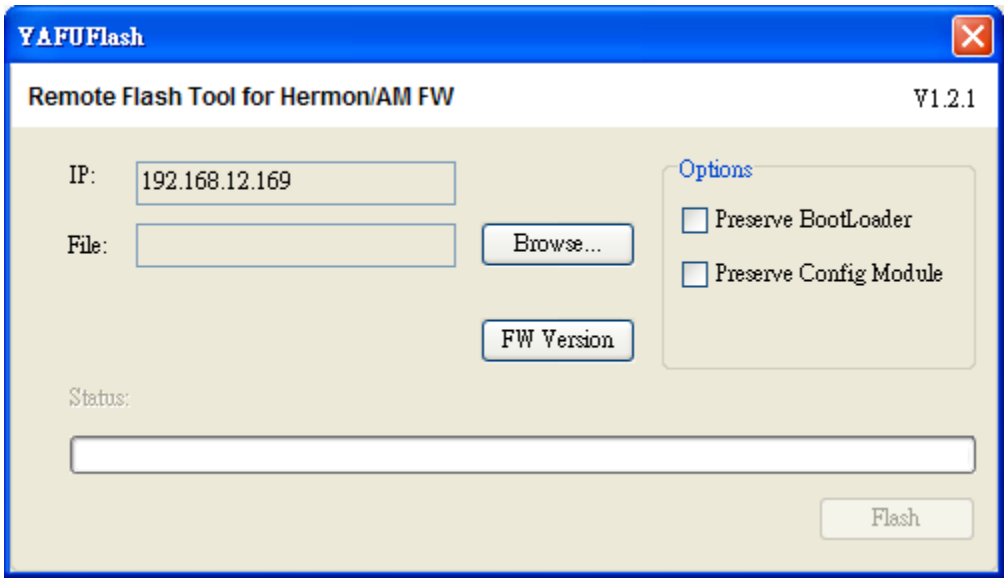


Figure D-2 YAFU Flash

3. The selected firmware is checked for validation before remote flashing starts.

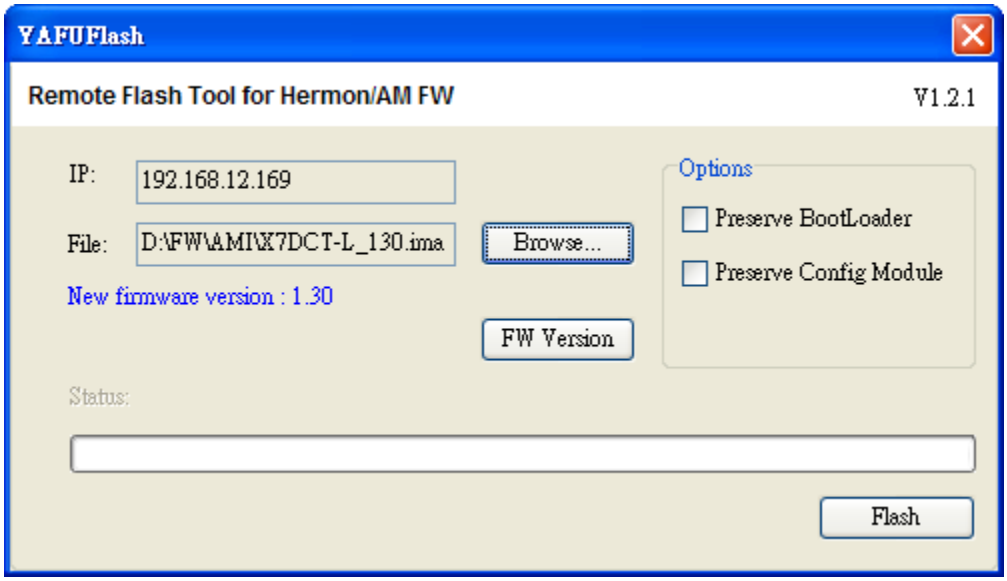


Figure D-3 YAFU Flash

- **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.

4. Click **FW Version**. Remote Flashing can only be performed by an Administrator. If you are an administrator, enter your ID and your password in the dialog box below. Then click **OK**.

Figure D-4 ID and Password (Administrator)

5. After you check the firmware versions and click **Flash**, firmware flashing will start. See the figures below.

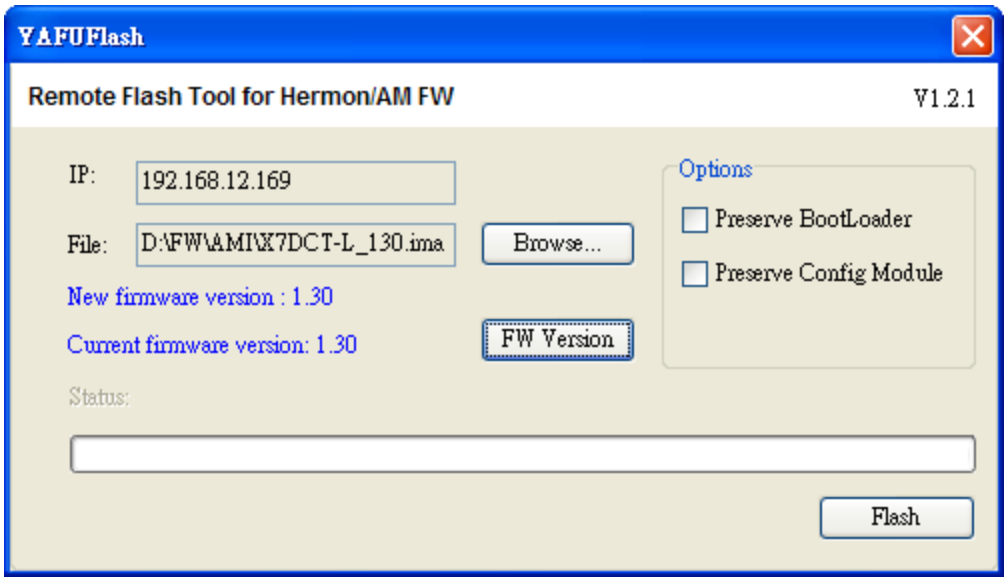


Figure D-5 Display of Current Firmware Version

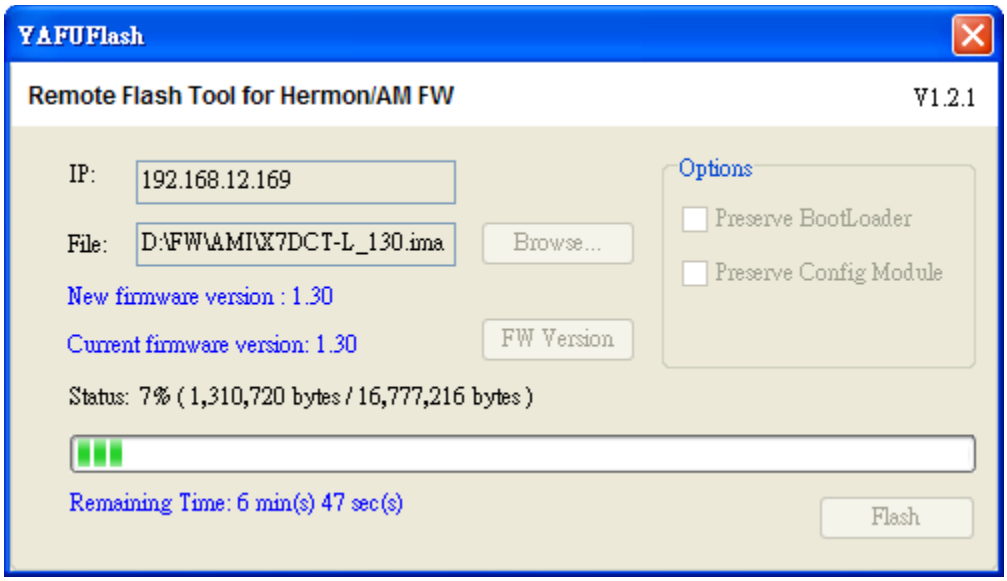


Figure D-6 Remote Flash #1

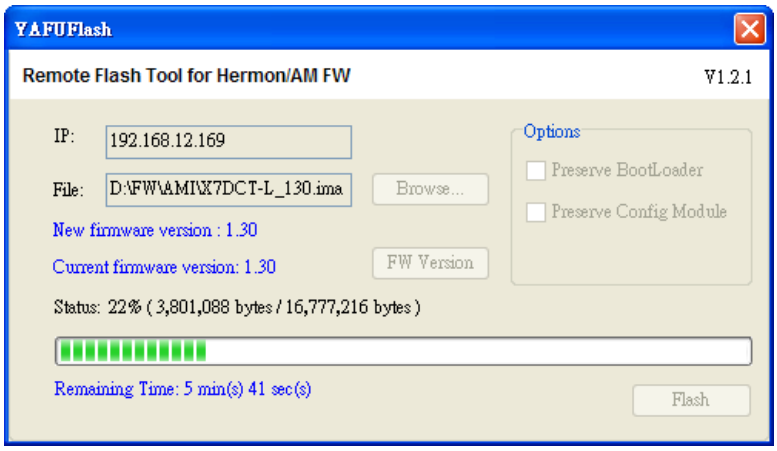


Figure D-7 Remote Flash Screen #2

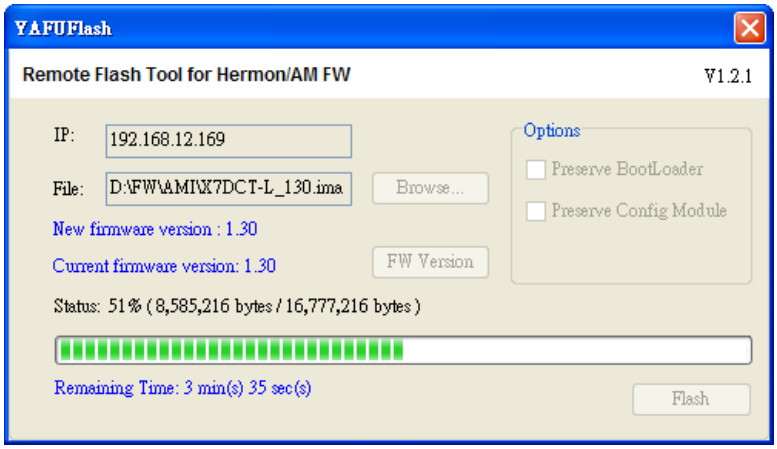


Figure D-8 Remote Flash Screen #3

6. When the flashing is complete, the status field displays “Finished.” Click **Finish** to exit this dialog box.

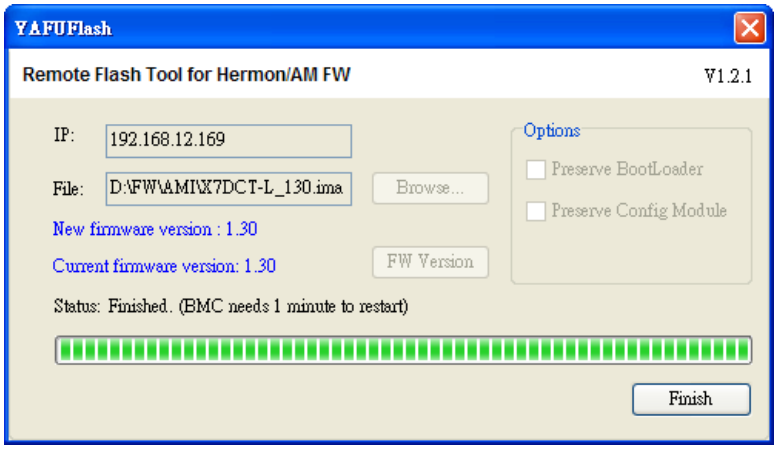


Figure D-9 Remote Flash Screen #4

Appendix E: SIM (WA) Firmware Update

1. To re-flash SIM(WA) Firmware, select an SIM(WA) device, click **File** on the menu bar and then select **Update firmware** in the pull-down menu. A dialog box appears.

Figure E-1 Firmware Update

2. Make sure that you have the correct firmware for the update and click **OK**. The dialog box below appears.

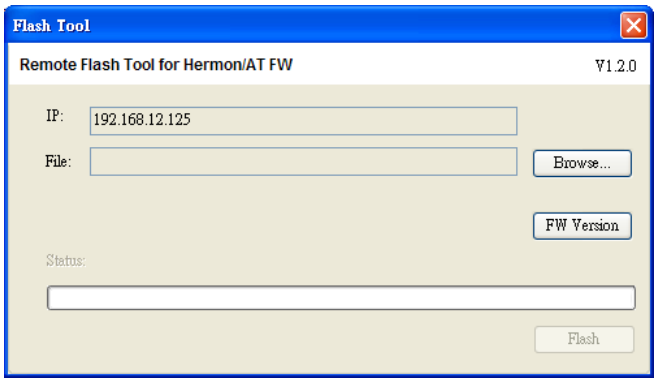


Figure E-2 Flash

3. Click **Browse** to select the desired firmware file for remote flashing. It will be checked for validation before remote flashing starts.

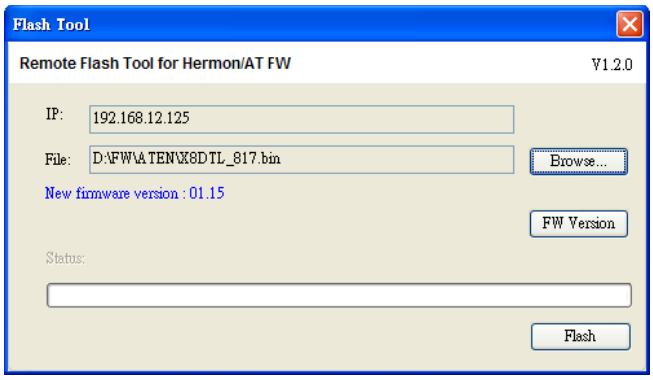


Figure E-3 Flash

4. Click **FW Version**. Remote flashing can only be performed by an administrator. If you are an administrator, enter your ID and password in the dialog box.

Figure E-4 ID/Password

5. After you check the firmware version and click **Flash**, firmware flashing will start.

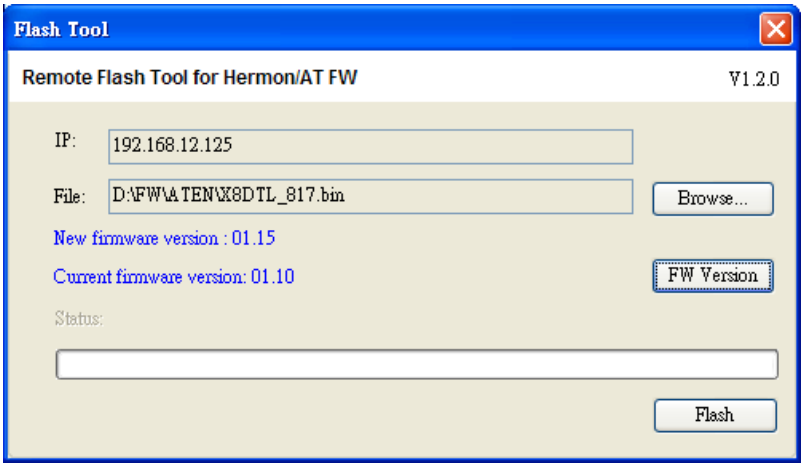


Figure E-5 Firmware Versions

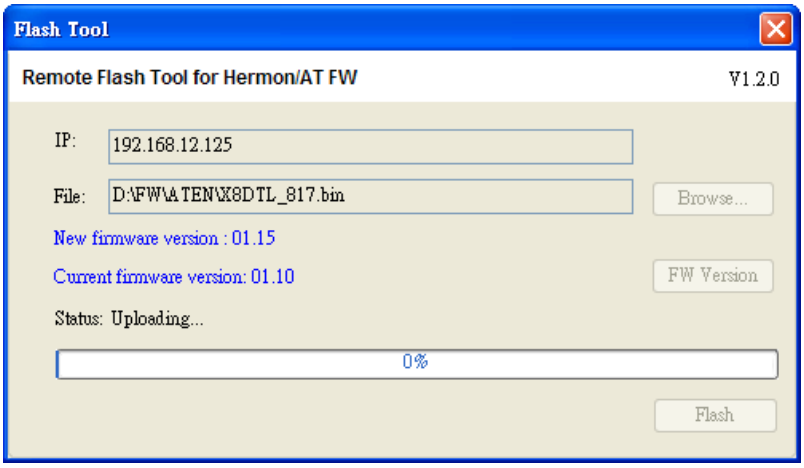


Figure E-6 Remote Flash #1

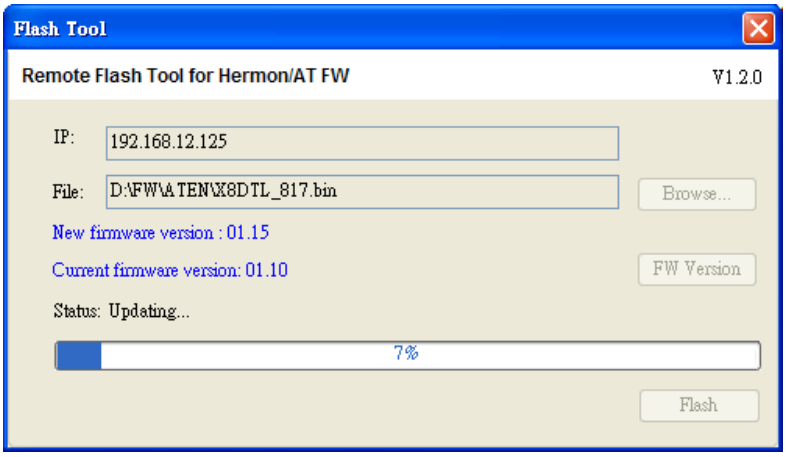


Figure E-7 Remote Flash #2

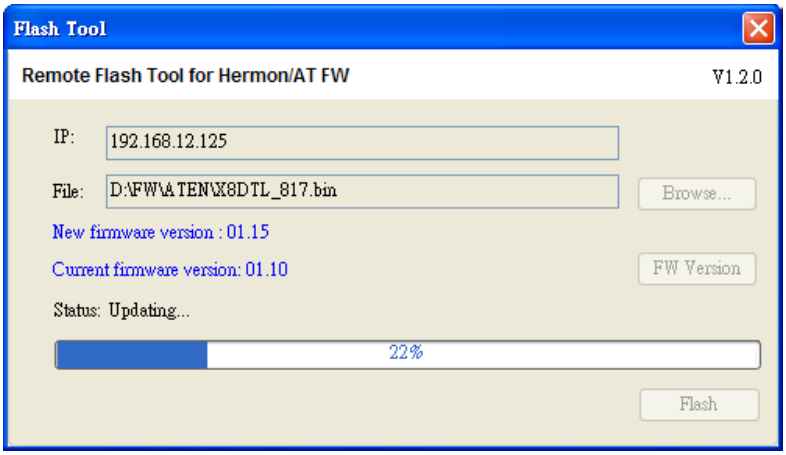


Figure E-8 Remote Flash #3

6. When the flashing is complete, the status field displays “Finished.” Click **Close** to exit this dialog box.

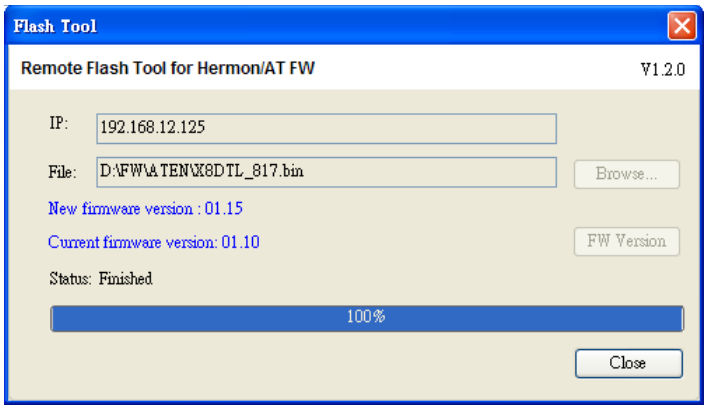


Figure E-9 Remote Flash #4

Appendix F: ASPEED X10 Firmware Update

1. To re-flash ASPEED Firmware, select an ASPEED BMC device, click **File** on the menu bar and then select **Update firmware** in the pull-down menu. The dialog box below appears.

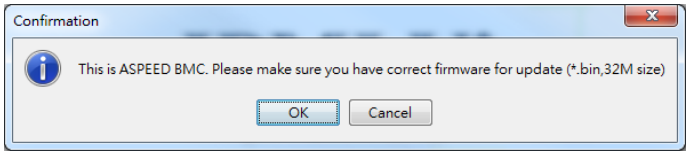


Figure F-1 Firmware Update

2. Make sure that you have the correct firmware for the update and click **OK**. The dialog box below appears.

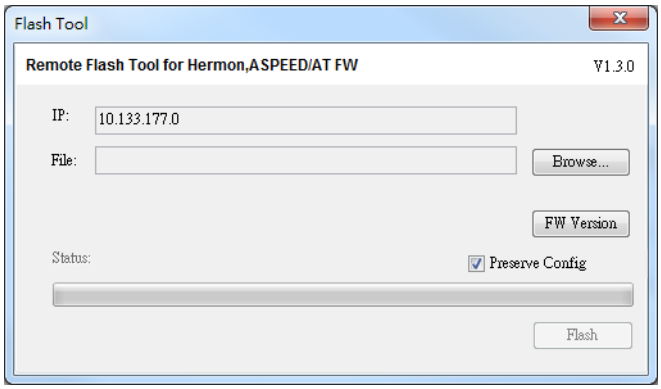


Figure F-2 Flash

3. Click **Browse** to select the desired firmware file for remote flashing. It will be checked for valication before remote flashing starts.

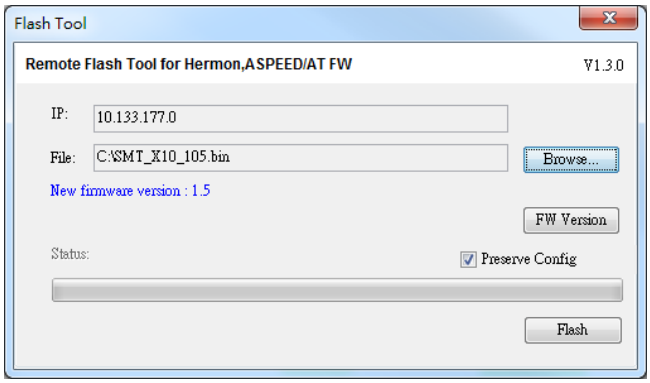


Figure F-3 Flash

4. Click **FW Version**. Remote flashing can only be performed by an administrator. If you are an administrator, enter your ID and password in the dialog box. Then click **OK**.

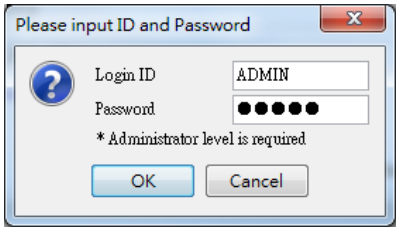


Figure F-4 ID/Password

5. After you check the firmware versions and click **Flash**, firmware flashing will start.

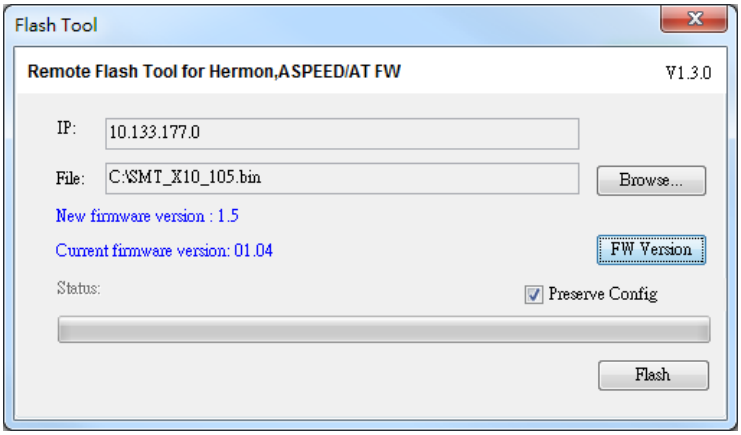


Figure F-5 Firmware Versions

6. When the flashing is complete, the status field displays “Done.” Note that it takes one minute for the BMC to restart. Click **Close** to exit this dialog box.

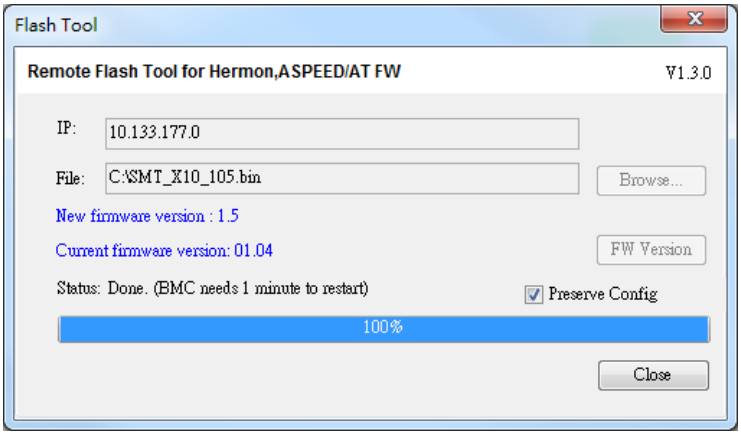


Figure F-6 Remote Flash

Appendix G: ASPEED X12 Firmware Update

1. To re-flash ASPEED firmware, select an ASPEED BMC device, click **File** on the menu bar and then select **Update Firmware** in the pull-down menu. The dialog box below appears.

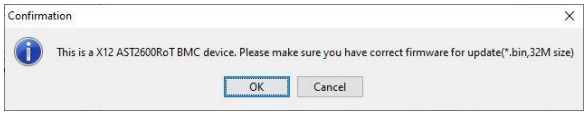


Figure G-1

2. Make sure that you have the correct firmware for the update, and click **OK**. The dialog box below appears.

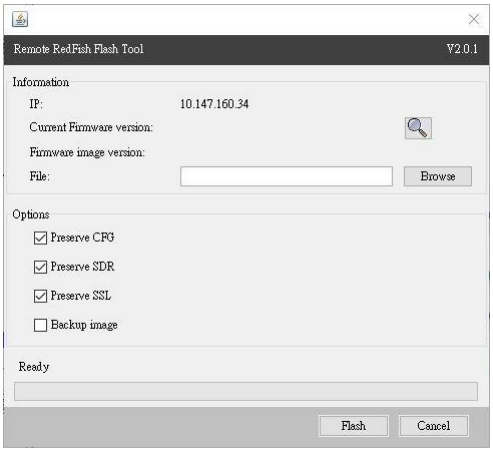


Figure G-2

3. Click **Browse** to select the desired firmware file for remote flashing. It will be checked for valication before remote flashing starts.

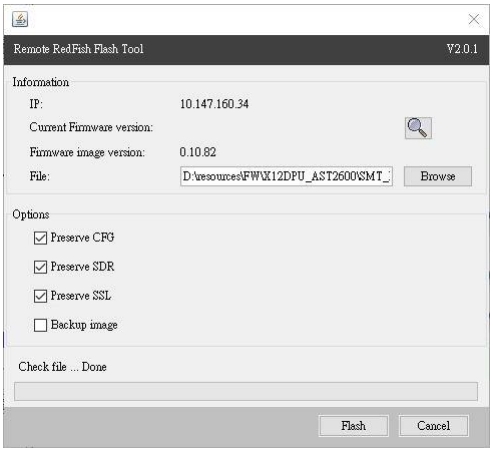


Figure G-3

4. Click the check icon . Remote flashing can only be performed by an administrator. If you are an administrator, enter your ID and password in the dialog box. Then click **OK**.

Figure G-4

5. After you check the firmware versions and click **Flash**, firmware flashing will start.

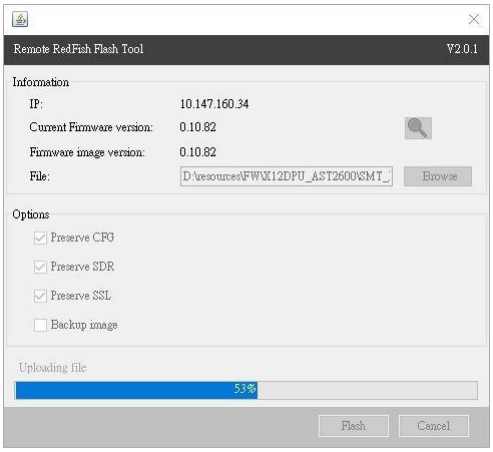


Figure G-5

6. When the flashing is complete, the status field displays “Device is ready now.” Note that it takes a few minutes for the BMC to restart. Click **Cancel** to exit this dialog box.

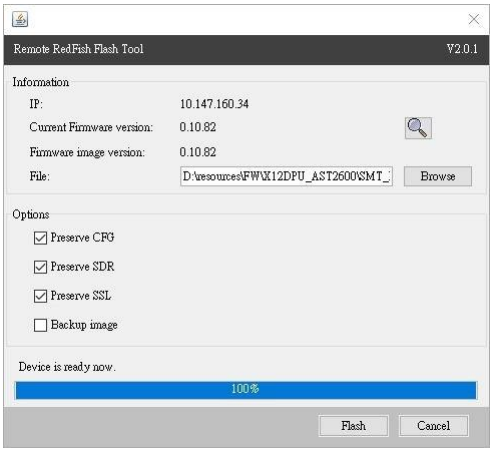


Figure G-6

Appendix H: Updating ASPEED X12 BIOS

1. To re-flash ASPEED BIOS, select an ASPEED BMC device, click **File** on the menu bar and then select **Update BIOS** in the pull-down menu. The dialog box below appears.

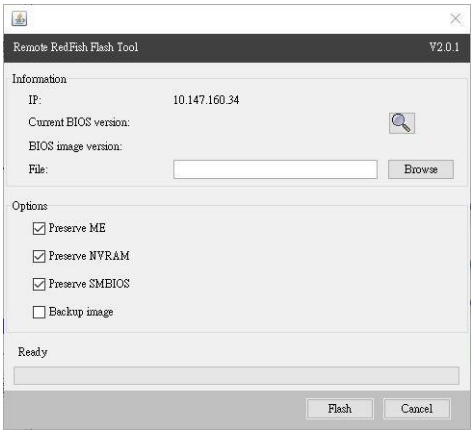


Figure H-1

2. Click the check icon . Remote flashing can only be performed by an administrator. If you are an administrator, enter your ID and password in the dialog box. Then click **OK**.

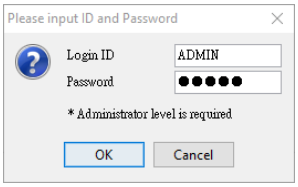


Figure H-2

3. Click **Browse** to select the desired firmware file for remote flashing. It will be checked for validation before remote flashing starts.

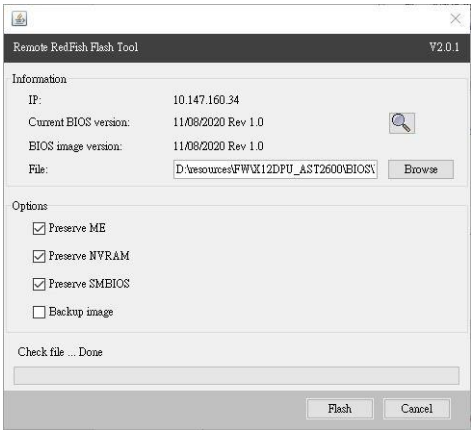


Figure H-3

4. After you select the firmware file, click **Flash**. firmware flashing will start.

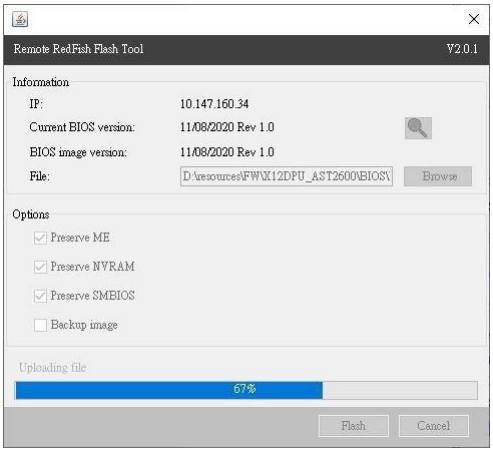


Figure H-4

5. After the flashing is complete, the status field displays “Device is ready now.” Note that it takes a few minutes for the BMC to restart. ” Click **Cancel** to exit the dialog box.

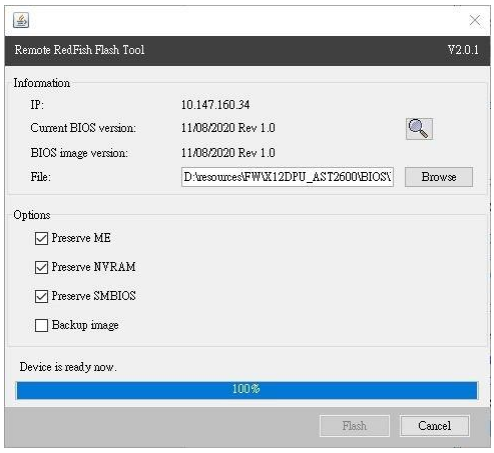


Figure H-5

Appendix I: Node Product Key Functions

The node product key, including SFT-OOB-LIC and SFT-DCMS-Single, provides the following functions:

Functions requiring SFT-OOB-LIC (or SFT-DCMS-Single):

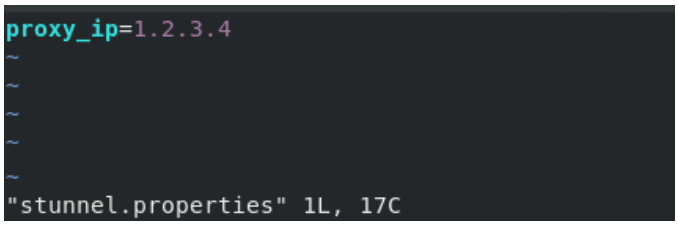
- Virtual Media

Functions requiring SFT-DCMS-Single

- KVM Console (HTML5)

Appendix J: Stunnel Properties

When using the iKVM Console, a Stunnel proxy is used to establish an encrypted connection. The first non-loopback IP address by default is used for a UNIX system. You can change your own NIC IP address by setting the “proxy_ip” in the stunnel.properties file.

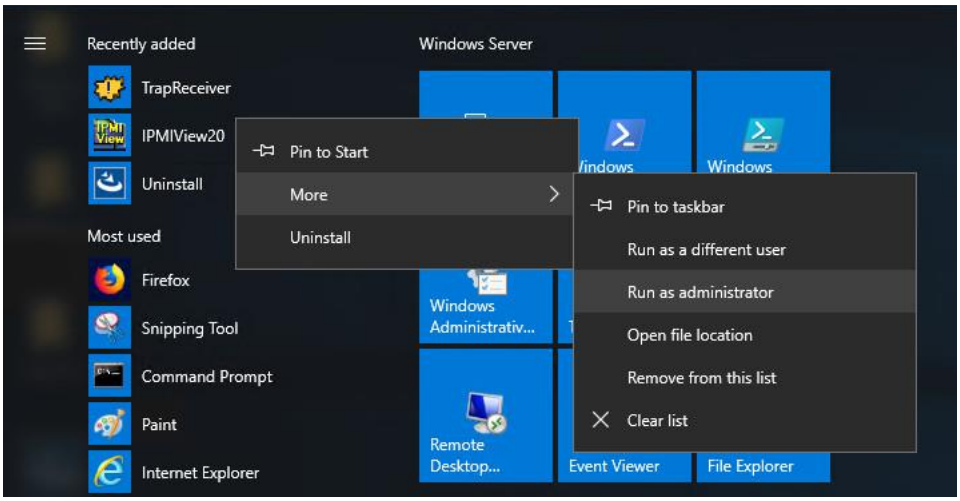


Appendix K: Q&A

Q: Why can't I save a configuration/open KVM window on Windows platform?

A: There are two ways to solve this problem:

- Running the IPMIView using the Administrator permission
  a. Right-click the IPMIView20 icon, click **More** and then click **Run as administrator**.
  b. When prompted for an administrator password or for a confirmation, type the administrator password, and click **Continue**.



- Installing the IPMIView to another location
  Select a drive other than C drive. However, when you install the IPMIView, do not install it to the default path (C:\Program Files).

Q: How can I enable automatic log monitoring in IPMIView?

A: Open a Command Prompt and change directory to the IPMIView folder and run the command "java -jar IPMIView20.jar d" to enable automatic log monitoring. A log.txt file is then created and saved in the IPMIVIew folder.

Note: The log size grows rapidly if the transaction is busy.

Q: Why does a permission error appear when I install Supermicro on Windows?

A: Please execute the installation in the **"Run as administrator"** mode because some IPMIView functions require OS write permission.

Q: Why can't I launch IPMIView after installation?

A: To start the IPMIView for the first time, please execute it as an Administrator.

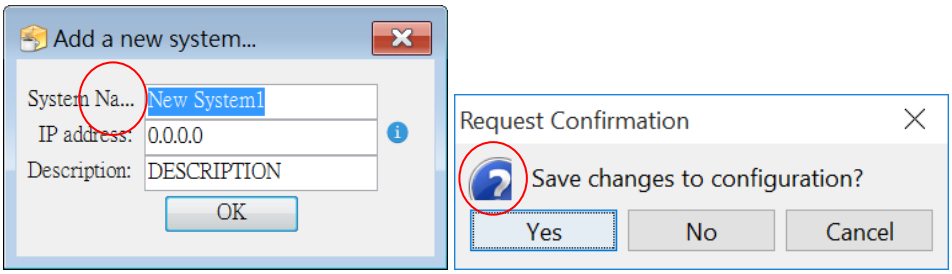
1. Right-click the IPMIView20 icon, click **More** and then click **Run as administrator**.
2. When a dialog box appears and asks for an administrator password, type the administrator password, and click **Continue**.

Q: Why does my Trap Receiver icon become ?

A: It indicates that the IPMIView cannot receive any traps. Please check your network, firewall or operating system settings.

Q: Why do texts or icons in the dialog boxes or windows appear incomplete?

A: The partially displayed dialog boxes or windows (see the exemplary figures below) result from your system's scaling settings.



To fix the problem, open **Start Menu**, select **Settings**>**System**>**Display**, and then set the scaling in the **Change the size of text, apps, and other items** field to be 100%.

Appendix L: Supported BMC List

- ASPEED AST2600 BMC on-Board (e.g. X12DPU, X12DPi boards)
- ASPEED AST2500 BMC on-Board (e.g., X11SPL-F, X11DPU, X11DGQ, B11DPT boards)
- ASPEED AST2400 BMC on-Board (e.g., X10, X11SSH-F, B10, B1 boards)
- Renesas SH7757 BMC on-Board (e.g., X9, B9 boards)
- Nuvoton WPCM450 BMC on-Board (e.g., X9 boards)
- Winbond WPCM450 BMC on-Board (e.g., X8 boards)

* KVM-over-LAN supports BMCs with ATEN solution in ASPEED AST2500 (e.g., X11, B11), AST2400 (e.g., X10, B10, B1) and WPCM450 (e.g., X9)

Appendix M: Third-Party Software

The following open source libraries are used in IPMIView package.

Library	License
AbsoluteLayout	Apache 2.0
Miglayout	BSD
Jfreechart	LGPL
Jackson	Apache 2.0
openssl	OpenSSL
run-as-root	Apache 2.0
out-process	Apache 2.0

Contacting Supermicro

Headquarters

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

Europe

Address:	Super Micro Computer B.V. Het Sterrenbeeld 28, 5215 ML 's-Hertogenbosch, The Netherlands
Tel:	+31 (0) 73-6400390
Fax:	+31 (0) 73-6416525
Email:	Sales_Europe@supermicro.com (Sales Inquiries) Support_Europe@supermicro.com (Technical Support) RMA_Europe@supermicro.com (RMA Support)
Website:	www.supermicro.nl

Asia-Pacific

Address:	Super Micro Computer, Inc. 3F, No. 150, Jian 1st Rd. Zhonghe Dist., New Taipei City 235 Taiwan (R.O.C)
Tel:	+886-(2) 8226-3990
Fax:	+886-(2) 8226-3992
Email:	Sales-Asia@supermicro.com.tw (Sales Inquiries) Support@supermicro.com.tw (Technical Support) RMA@supermicro.com.tw (RMA Support)
Website:	www.supermicro.com.tw