Management Console
User's Guide
(AST 2500 Chipset)

Version: 1.2

Table of Contents

Using Your Management Console

The Management Console has a user-friendly Graphics User Interface (GUI) called the Management Console GUI. It is designed to be easy to use. It has a low learning curve because it uses a standard Internet browser. You can expect to be up and running in less than five minutes. This chapter allows you to become familiar with the Management Console GUI's various functions. Each function is described in detail.

Management Console Key Features and Functions

- Support IPMI v2.0
- Out-of-band monitoring and control for sever management over LAN.
- FRU information report includes main board part number, product name, and manufacturer, etc.)
- Health status/Hardware monitoring report.
- Events log, view, and clear.
- Event notification via PET (Platform Event Trap).
- Platform Event Filtering (PEF) to take selected action for selected events.
- Chassis management includes power control and status report, front panel buttons and LEDs control.
- Support multi-session user, and alert destination for LAN channel.

Software Install

Prerequisites on remote management PC

Before installing Java tool, please check your system for the following required configuration requirements:

- Supported Browsers:
  - Internet Explorer 8 - 11
  - Google chrome Version 29.0.1547.66m
  - Firefox 2.0
- JAVA Recommended Version 6.45 or Below (file size: ~ 16691KB)

Install Java Tool

Please follow the instruction to install Java in Windows operating system.

1. Go to http://www.java.com
2. Click Download on the middle of the home page.
3. Click on Agree and Start Free Download
4. Click see all Java downloads
5. Choose the folder location. (Save the file to a known location on your computer)
6. Click Save.
7. Click Yes to replace.
8. Verify that the
   - Name of the file is jre-6u45-windows-i586.exe
   - Size is approximately 16691KB.
9. Close all applications including the browser.
10. Double-click on the saved file icon to start the installation process.

Management Console Network Configuration

Please follow the instruction to enable the console redirection function.
You can gather the IP address.

Using the Web UI

The BMC firmware features an embedded web server, enabling users to connect to the BMC using an Internet browser (Microsoft® Internet Explorer™).

The web server shall support 4 concurrent connections

Web-based GUI is supported on the following browsers:

Microsoft Windows:

• Internet Explorer 8 ~ 11

• Mozilla® Firefox® 2.0 or later

Linux:

Mozilla Firefox 2.0 or later

Management Console Overview

1. Open a web browser and type in your identified IP. The IP address can be found using your DHCP server.
2. A dialog box prompts you to enter Username and Password.
3. Enter the following values:

Account 1	Username: **admin**	Password: **password**
Account 2	Username: **ADMIN**	Password: **ADMIN**

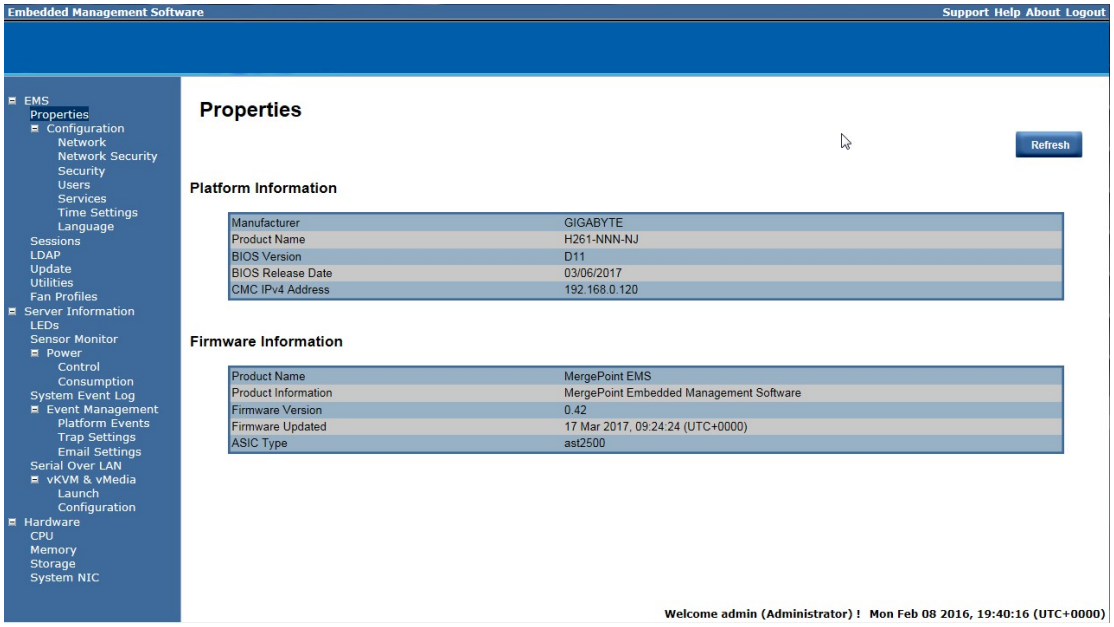
When you log in using the root user name and password, you have full administrative powers. It is advised that once you log in, you change the root password.

Enter Management Console

After you successfully log into your Management Console, the Remote Management Console GUI appears.

Properties

Properties displays the firmware version of current remote client system.



Configuration

Network

You can view and modify the network settings on this screen. Select the Network **Mode** from the drop-down list.

1. Dedicate Mode

When set to Dedicate Mode, you can configure the BMC related settings through the BMC port.

2. Shared Mode**

When set to Shared Mode, you can configure the BMC related settings through the NIC2 port. (Shared NIC Mode)

NOTE: Function available on selected models.

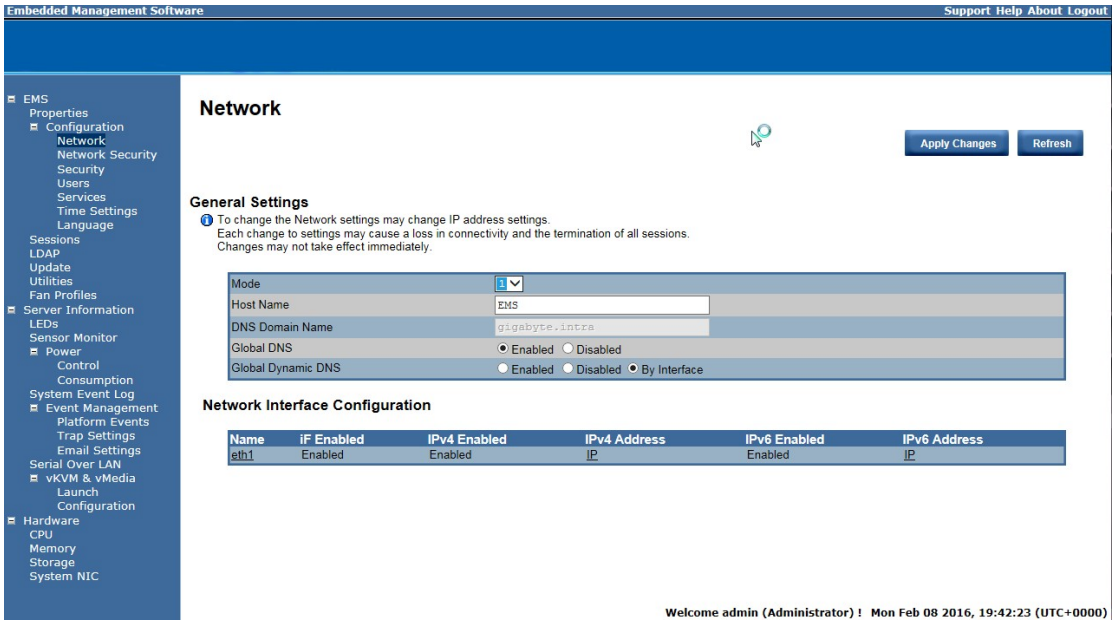
3. Failover Mode

When set to Failover Mode, you can configure the BMC related settings through the BMC or NIC2 port. (Backup Mode)

When you finish configuration, click **Apply Change**.

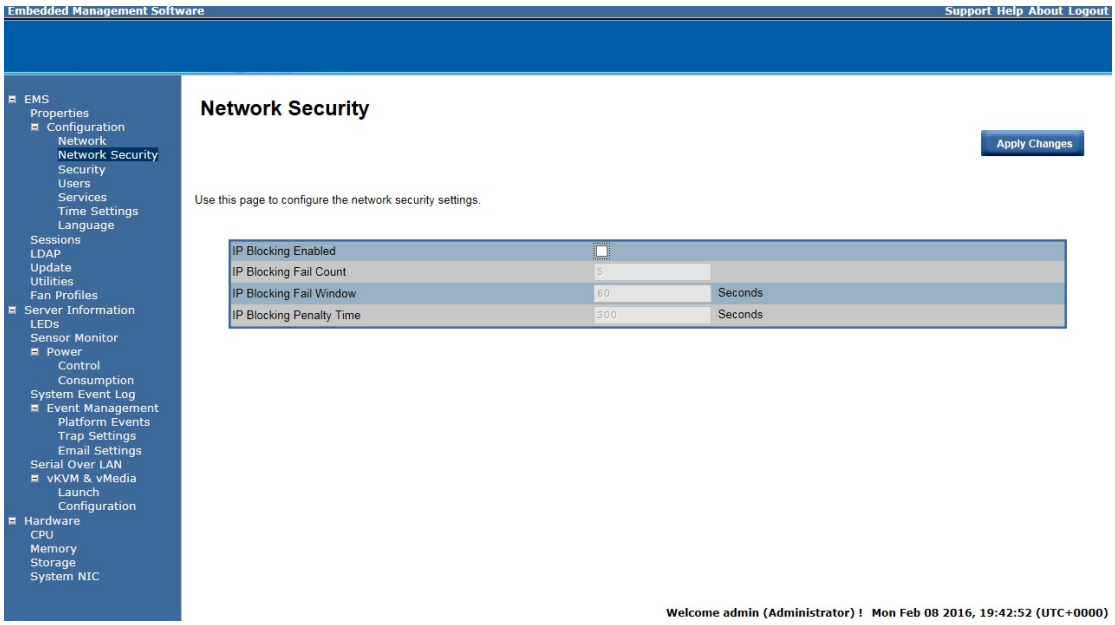
Please note that the changes may not take effect immediately, click "Refresh" to take effect of changes.

NOTE: Function available on selected models.



Network Security

You can configure the network security settings on this screen. Check the **IP Blocking Enabled** box and input the desire value of **IP Blocking Fail Count**, **IP Blocking Fail Window**, and **IP Blocking Penalty Time**. After you finish the configuration, click **Apply Change** to save the settings.



Security

The Security page shows the current certificate status.

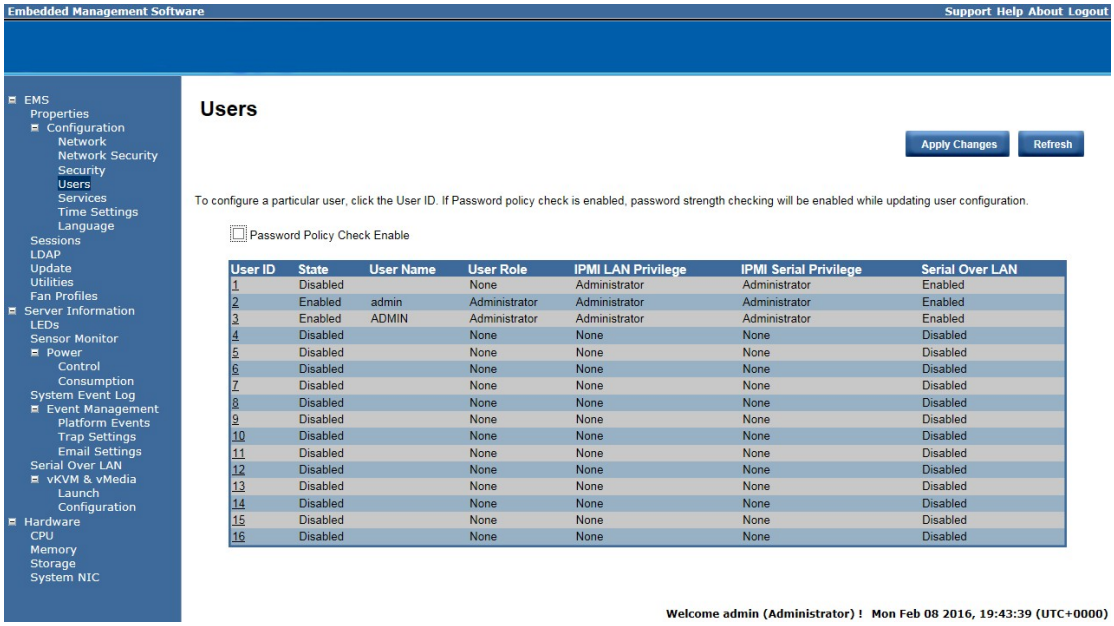
To generate a new certificate, click **Generate Certificate**.

To upload a certificate, click **Upload Certificate**.

Users

To configure a specific user, click the Users ID. To display new user information, click **Refresh**.

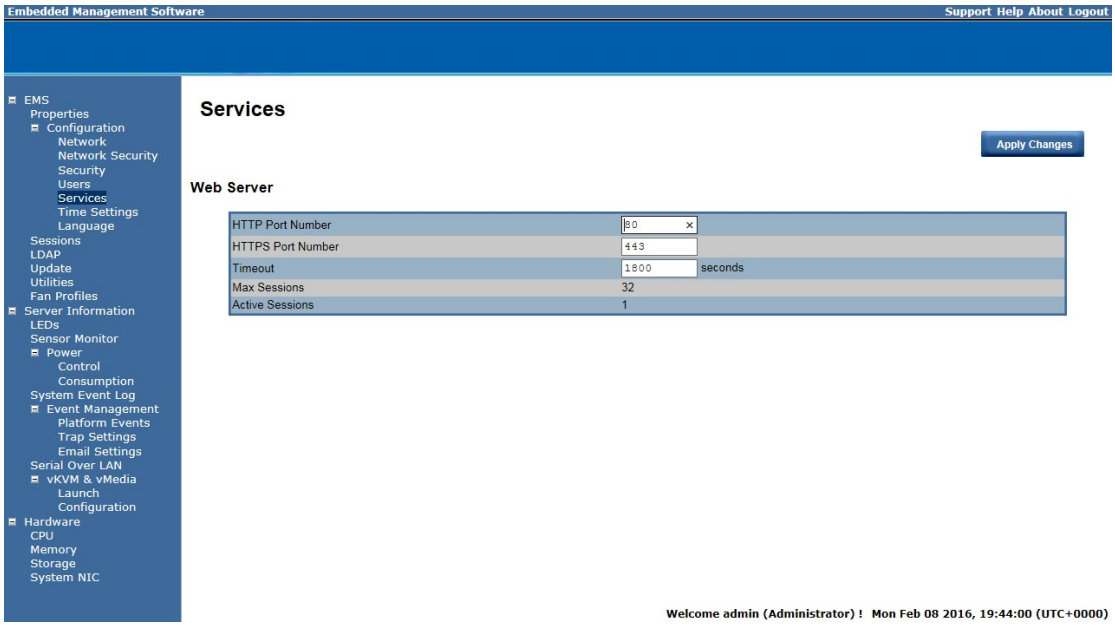
NOTE: BMC convention for enabling an ‘anonymous’ login is to configure the entry for User ID 1 with a null username (all zero’s) and a null password (all zero’s). Applications may then present this to the user as an anonymous login.



Services

You can configure the web server parameters (such as, HTTP Port Number, HTTPS Port Number, and Timeout) on a remote computer. By default, the timeout is 1800 seconds.

When you finish the configuration, click **Apply Changes**.



Time Setting

This page provides the mechanism to configure the Network Time acquisition method. With Administrator or Operator privilege level, you can modify configuration settings and click the Apply Changes button to execute the settings, as well as click the Sync Time Now button (when in Requested Mode) to request an immediate clock set.

Operation Mode

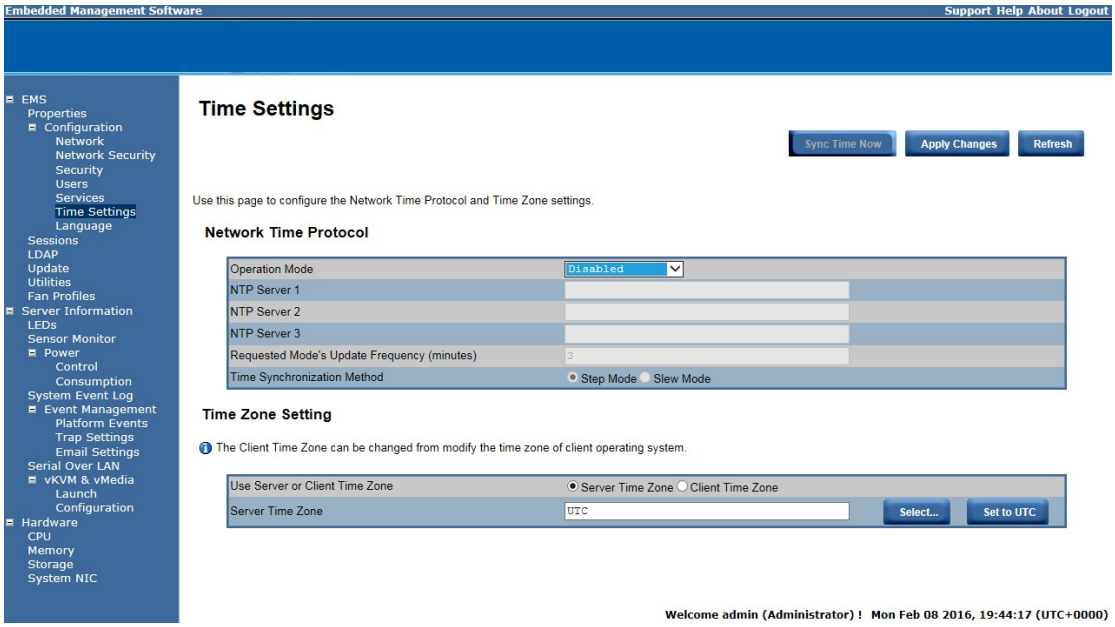
Configures the NTP Mode. You can Disable NTP, set **Requested Mode**, or **Daemon Mode** in this parameter.

In **Requested Mode**, you can request an immediate clock synchronization with the NTP server; request will be sent when click the Sync Time Now button.

The **Daemon Mode** runs NTP daemon which sends a NTP request at approximately 5 minute intervals. Multiple NTP servers may be specified to provide redundancy.

Time Synchronization Method

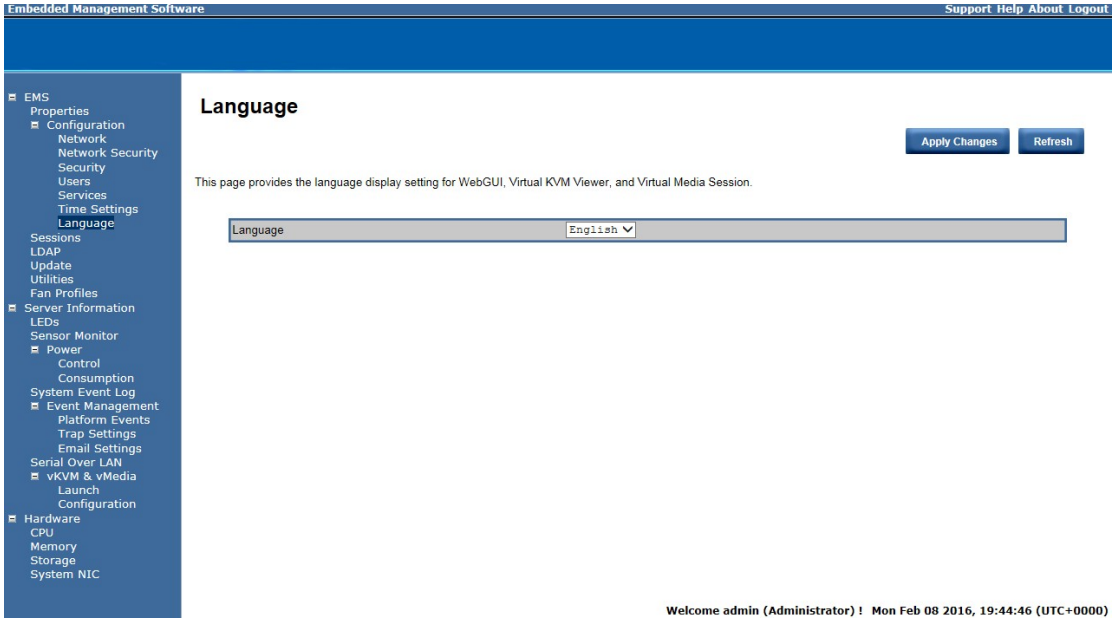
Specifies the synchronization method for Requested Mode. Select **Slew mode** when you want to adjust the time smoothly over time if there are time sensitive applications in place. Select **Step mode** to aggressively change the time using settimeofday() system call.



Language

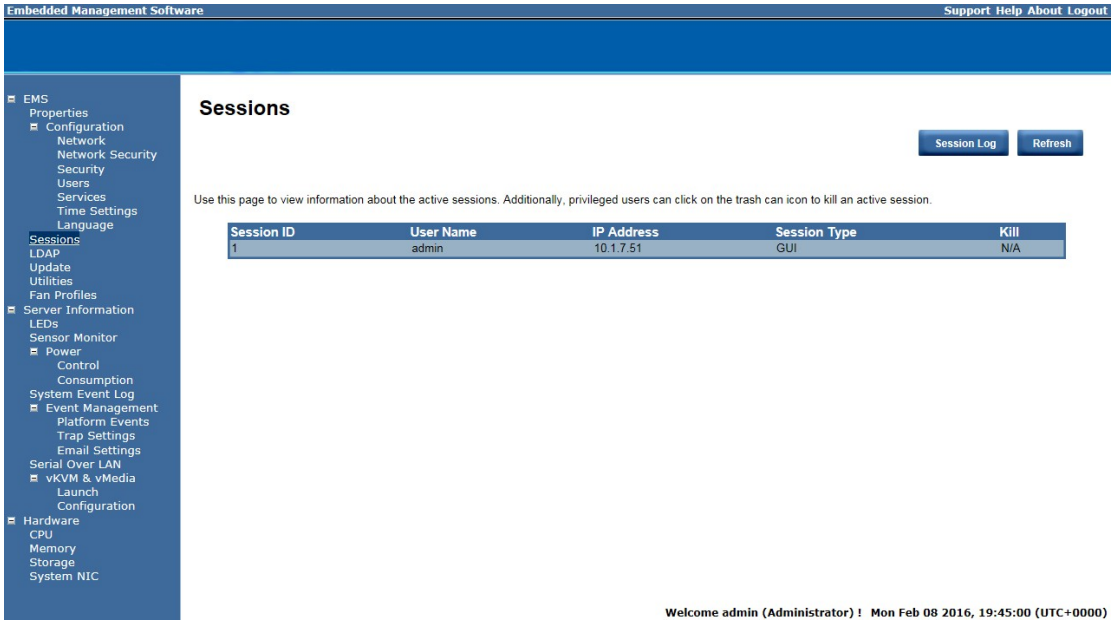
This page allow users to choose preferred language when using the WebUI.

When you finish the configuration, click **Apply Change**.



Sessions

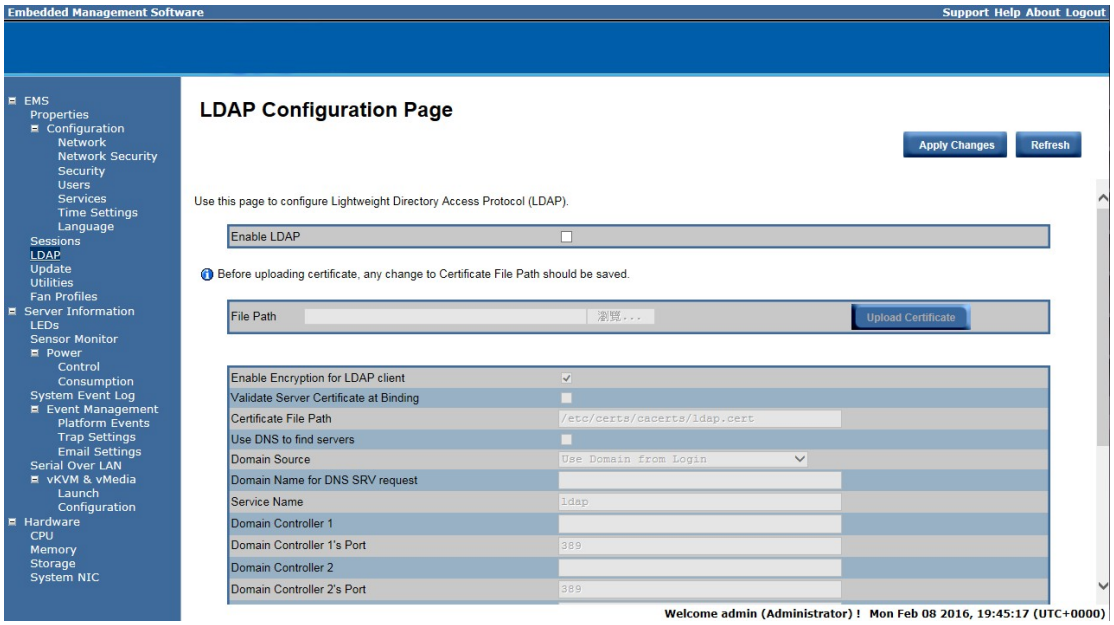
This screen displays information on Active Sessions. Additionally, the trash can icon provides the delete function for privileged users. Click Session log to view the session log. Click **Refresh** to refresh the Sessions status.



LDAP

LDAP screen allows download user list of LDAP server then create Management Console user account from this list directly.

Check the box below to enable LDAP authentication and enter the required information to access the LDAP server. Click **Apply Changes** to save your changes.



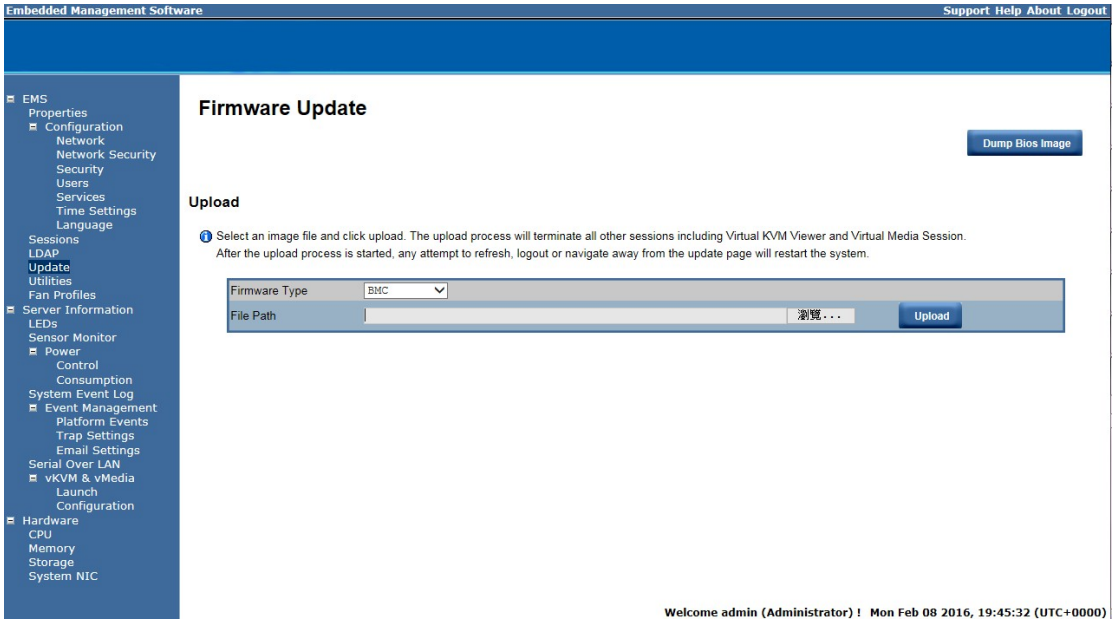
Updates

The firmware can be updated remotely.

To update firmware, follow the instruction below:

1. Select Update Type.
2. Select the file on your local system by using **Browse**.

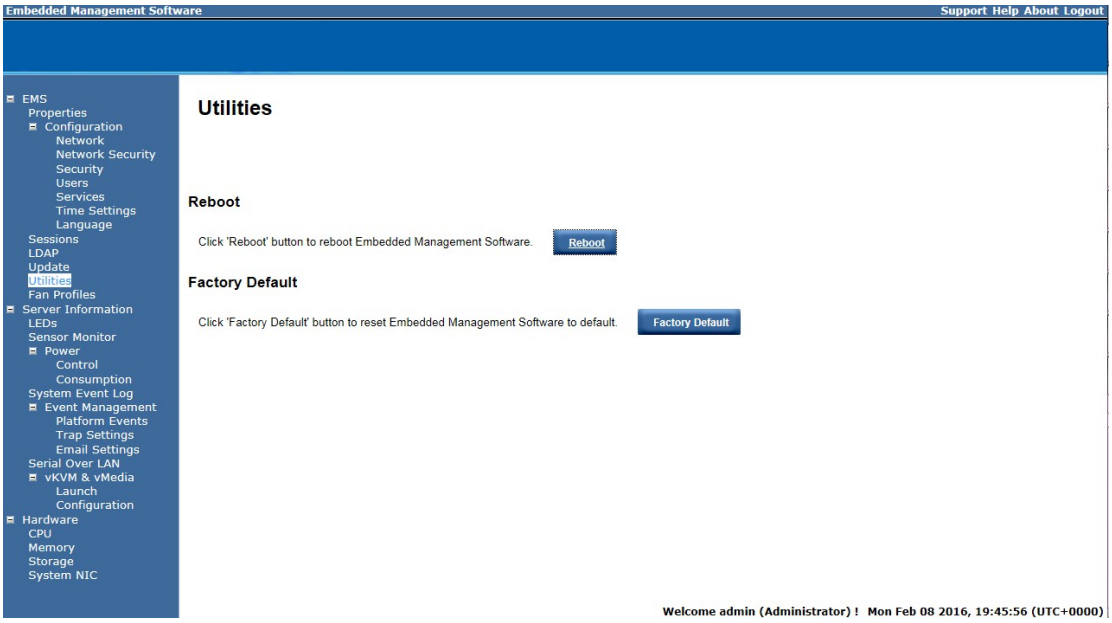
Click **Upload** to update to the new version of firmware.



Utilities

Utilities provides BMC reboot and Factory default restore functions.

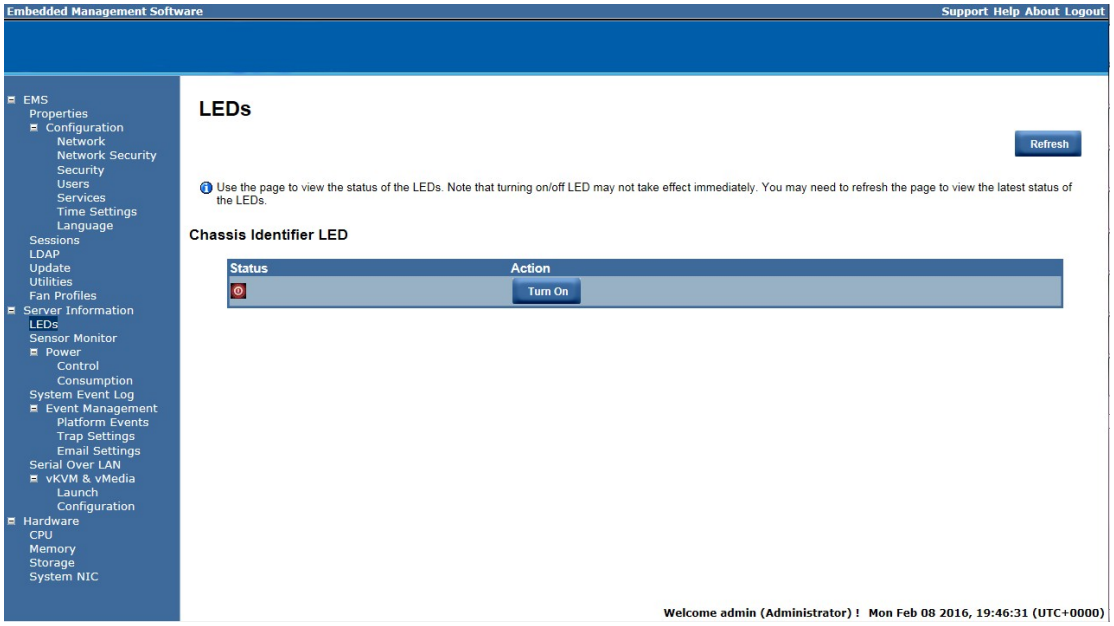
1. To reboot system, click **Reboot**.
2. To restore factory default, click **Factory Default**.
3. To Adjust the PWM offset for the system fans, enter offset values and click **Submit**.
4. To update Logo, select the file on your local system using **Browse** and click **Update**.



Server Information

LEDs

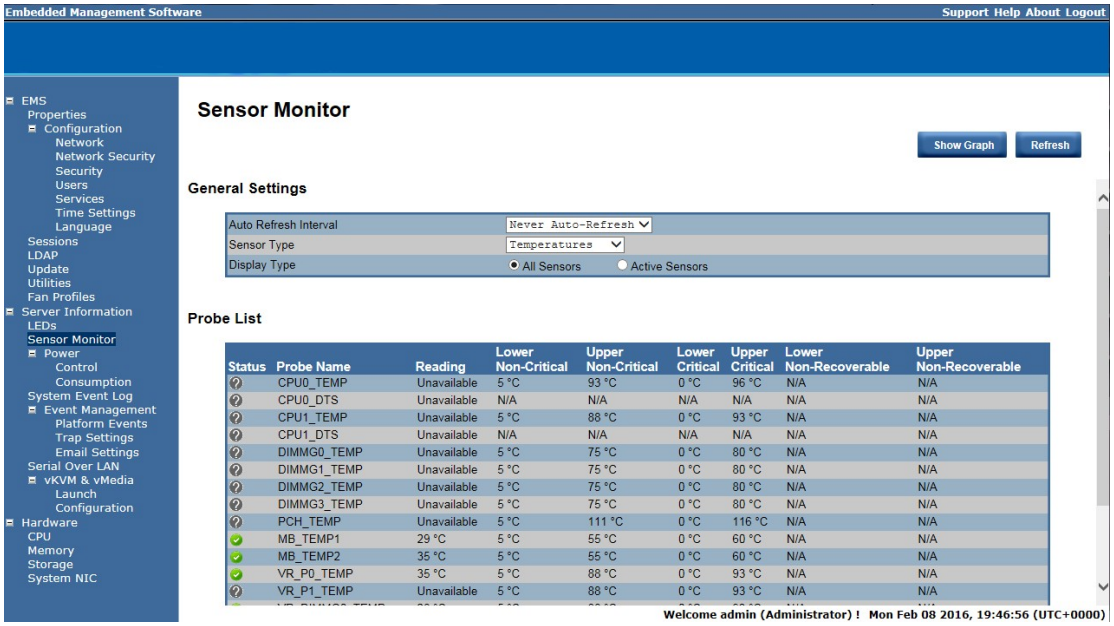
Click **Turn On** to light on the front panel ID indication LED remotely.



Sensor Monitor

The Sensor monitor provides general configuration for related system hardware monitoring.

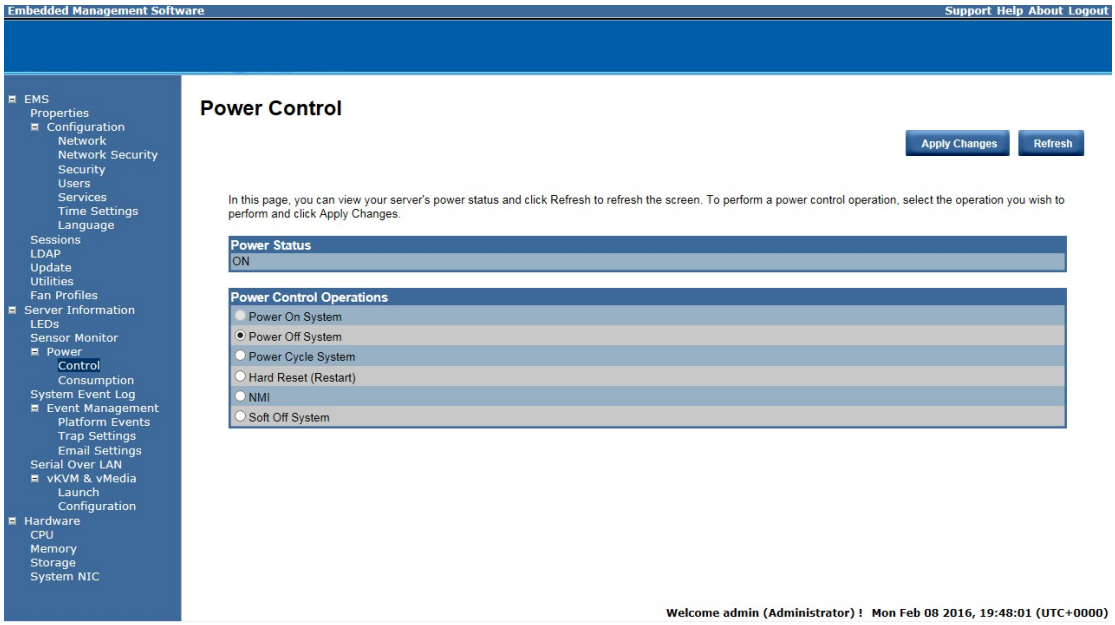
To view the Probe list, click **Show Graph**. And click **Refresh** to update current probe list.



Power Control

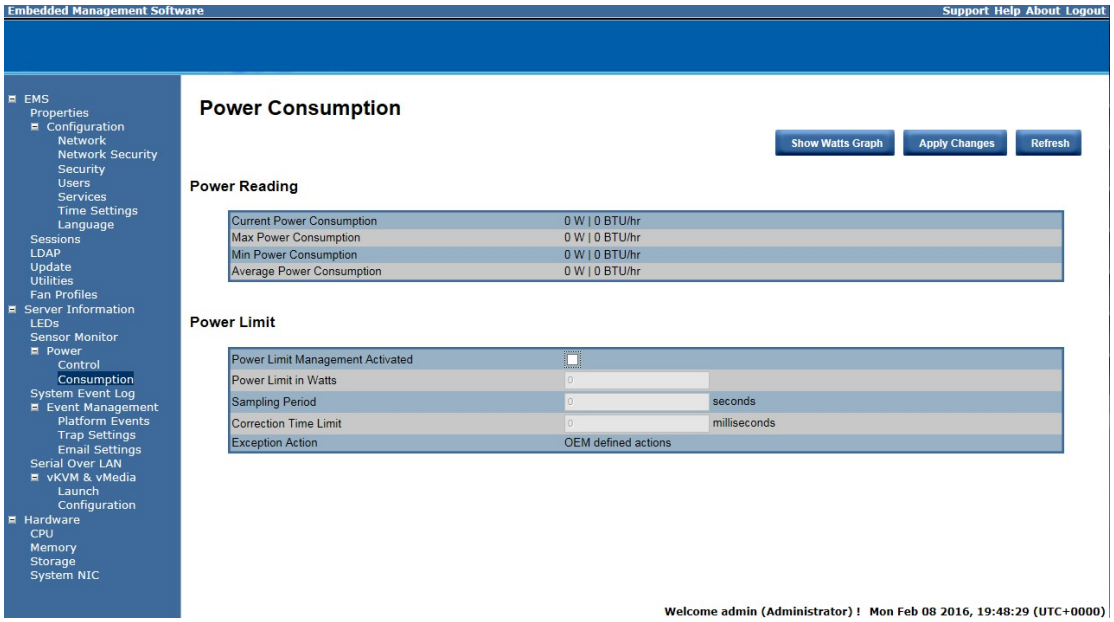
The Power Control allows you to power on/off/cycle, Hard Reset/NMI/Soft Off System the remote host system. Additionally you can see the remote power status.

To perform the power control operation, select the operation and click **Apply Changes**.



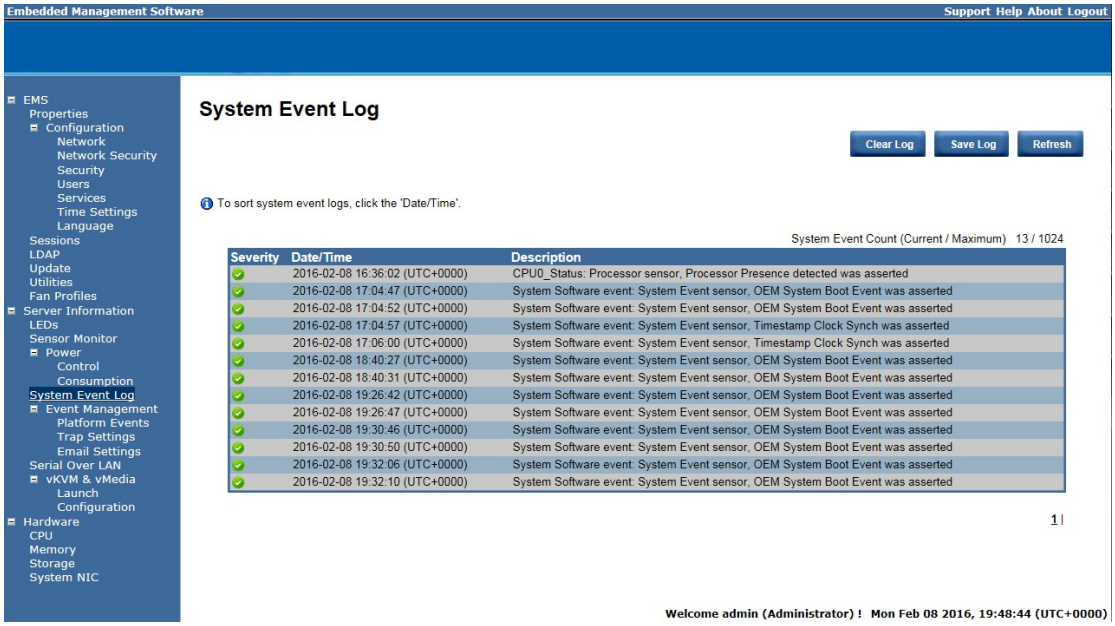
Power Consumption

This section allows user to configure the power policies for the system.



System Event Log

It records the event when sensor has an abnormal state. When the log matches the pre-defined alert, the system sends out the notification automatically, if it is pre-configured.

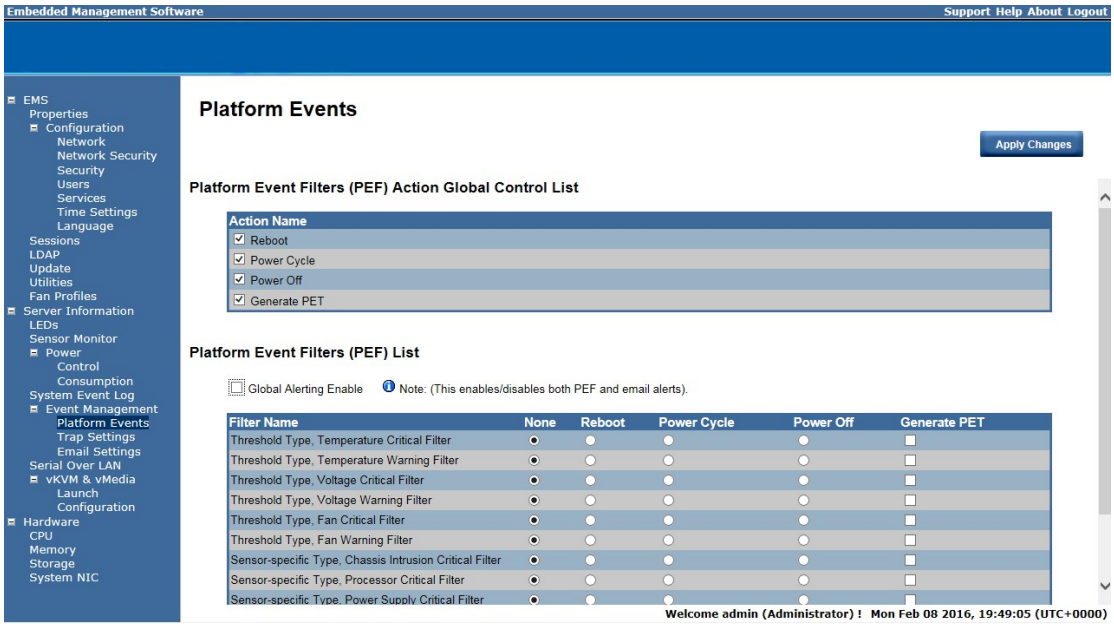


Platform Event

A platform event filter (PEF) can trigger an action and generate an alert when a critical hardware-related event occurs. For each PEF, you can choose the action to be taken when a platform event occurs.

You can also choose to generate and send an alert when a platform event occurs. In the Platform Events screen, you can enable the generation of platform event alerts globally by clicking Global Alerting Enable.

When you finish the configuration, click **Apply Changes**.



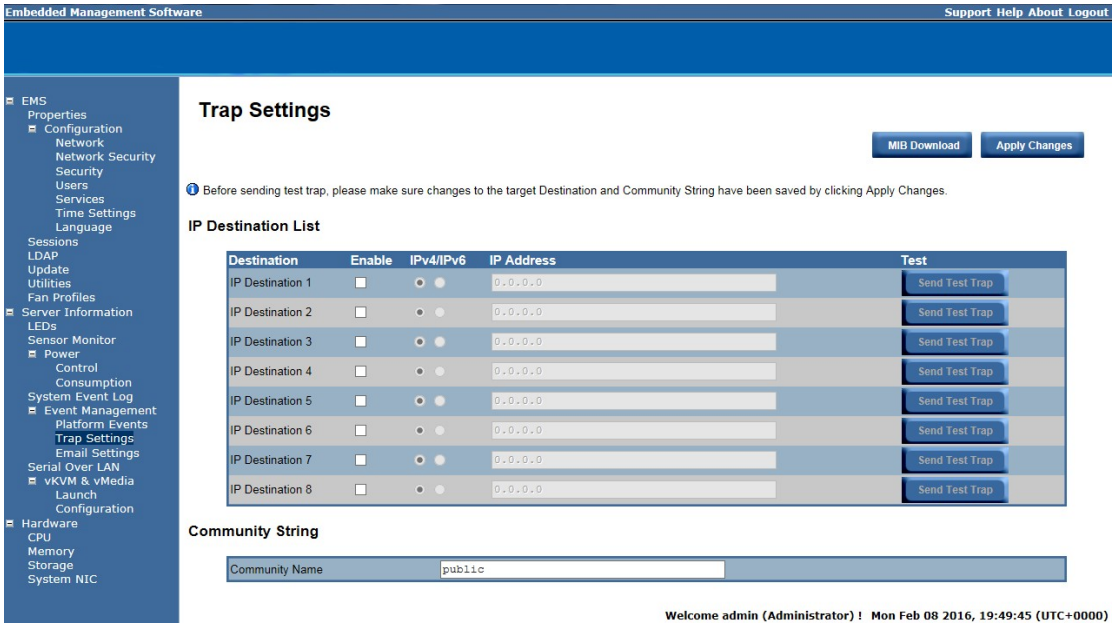
Trap Settings

In the Trap Settings, user can set the IPv4 and Ipv6 Destination List.

IPv6 and IPv4 are two completely separate protocols. IPv6 is not backwards compatible with IPv4, and IPv4 hosts and routers will not be able to deal directly with IPv6 traffic.

IPv6 has a significantly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits.

When you finish the configuration, click **Apply Changes**.



Email Settings

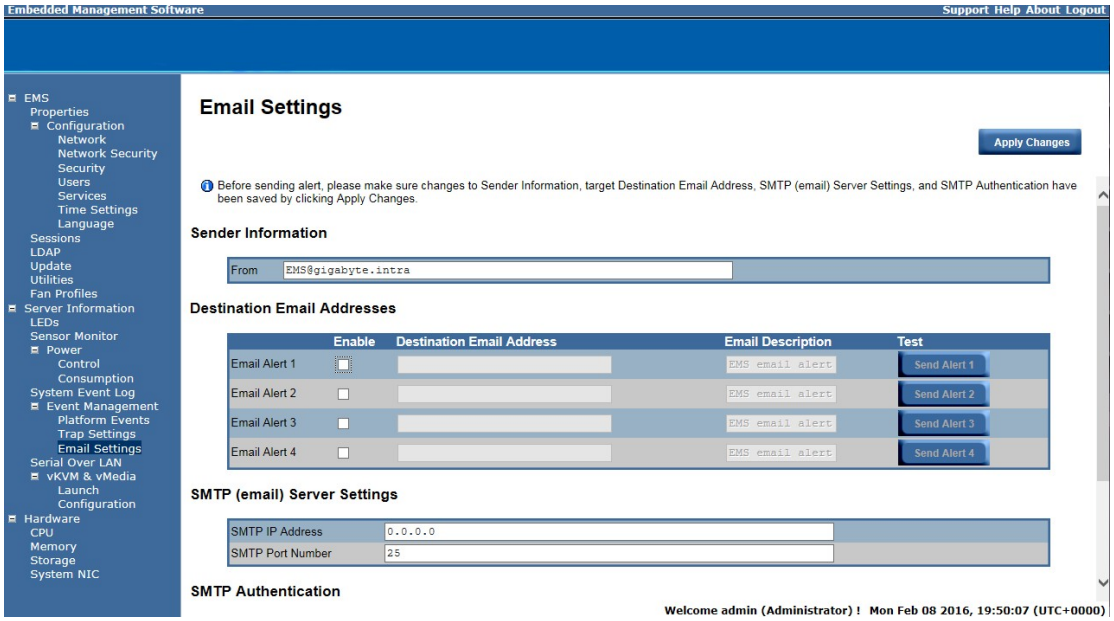
If you want the alert to be sent by email, you can configure to specify the e-mail address, subject and message in the Email Settings. After you finish the configuration, click Apply Change to save the settings.

SMTP

Set E-mail (SMTP) server IP address for sending alert notification to user.

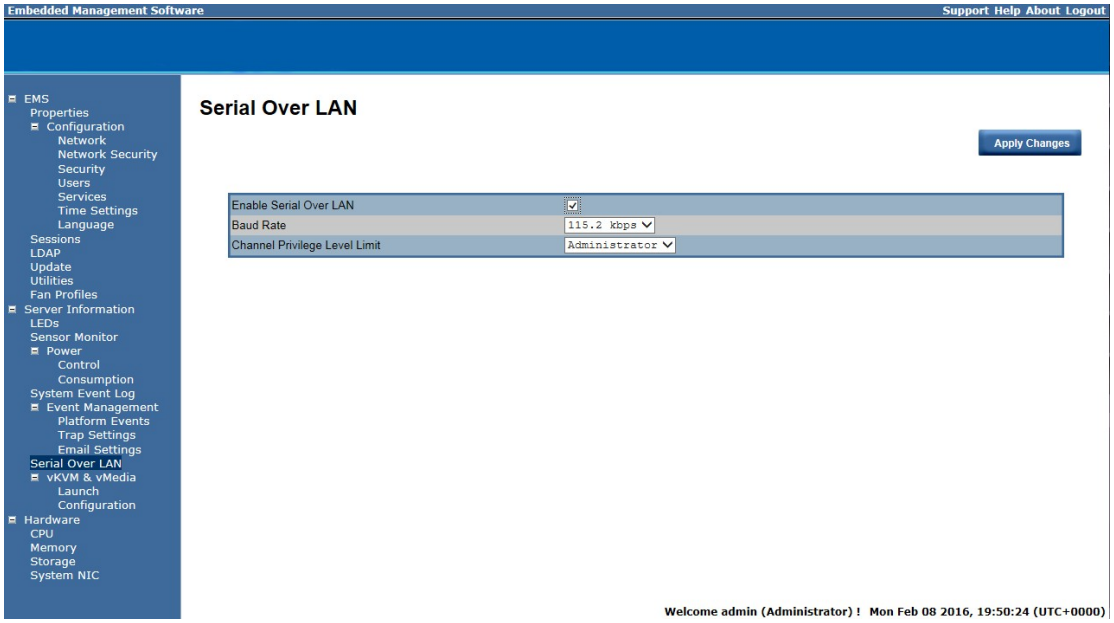
Check the SMTP Authentication **Enabled** box and enter the **SMTP IP address**, **User Name**, **Password**; select the **STARTTLS Mode** and **SASL Mode** from the drop-down list.

When you finish the configuration, click “Apply Changes”.



Serial Over LAN

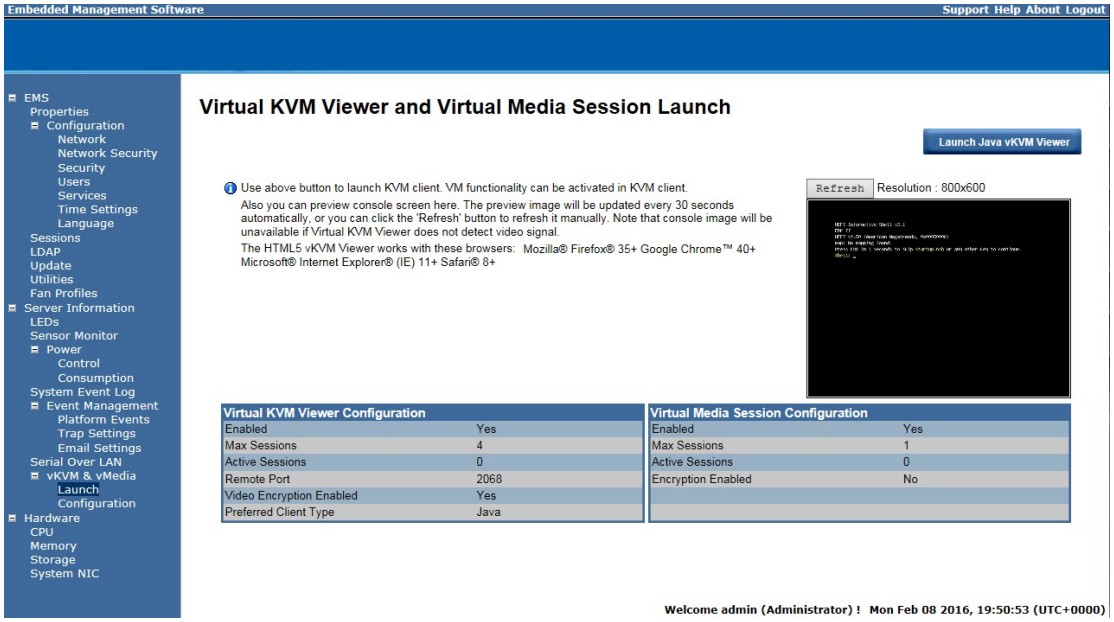
You can configure the Serial Over LAN settings on this screen. Check the **Enable Serial Over LAN** box and select the **Baud Rate** and **Channel Privilege Limit** from the drop-down list. After you finish the configuration, click **Apply Change** to save the settings.



vKVM & vMedia

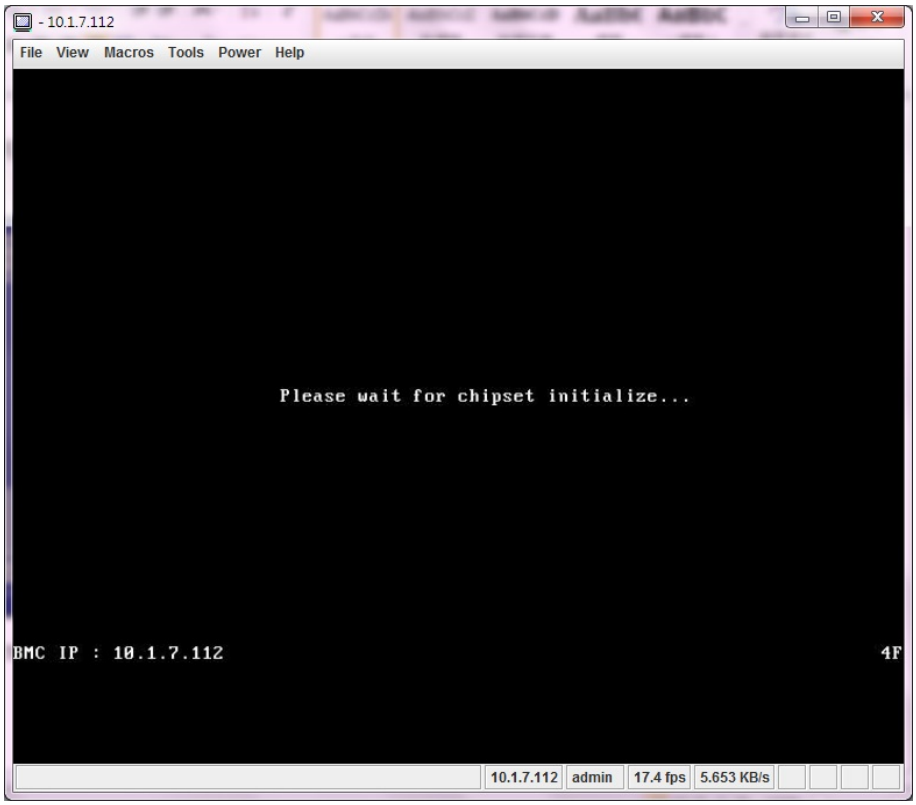
vKVM Viewer and Virtual Media Session Lanuch

This screen allows you to start a Remote Console session with the host system.



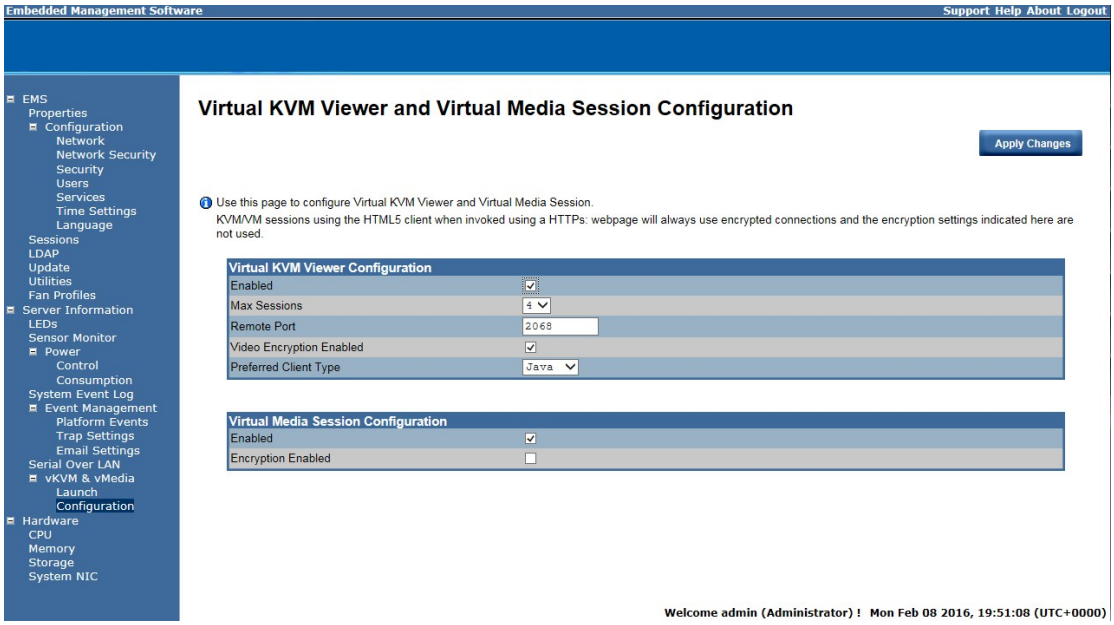
Launch Java KVM Viewer

Click **Launch Java KVM Viewer** to launch the redirection console and manage the server remotely. After clicking the button, a console appears as below:



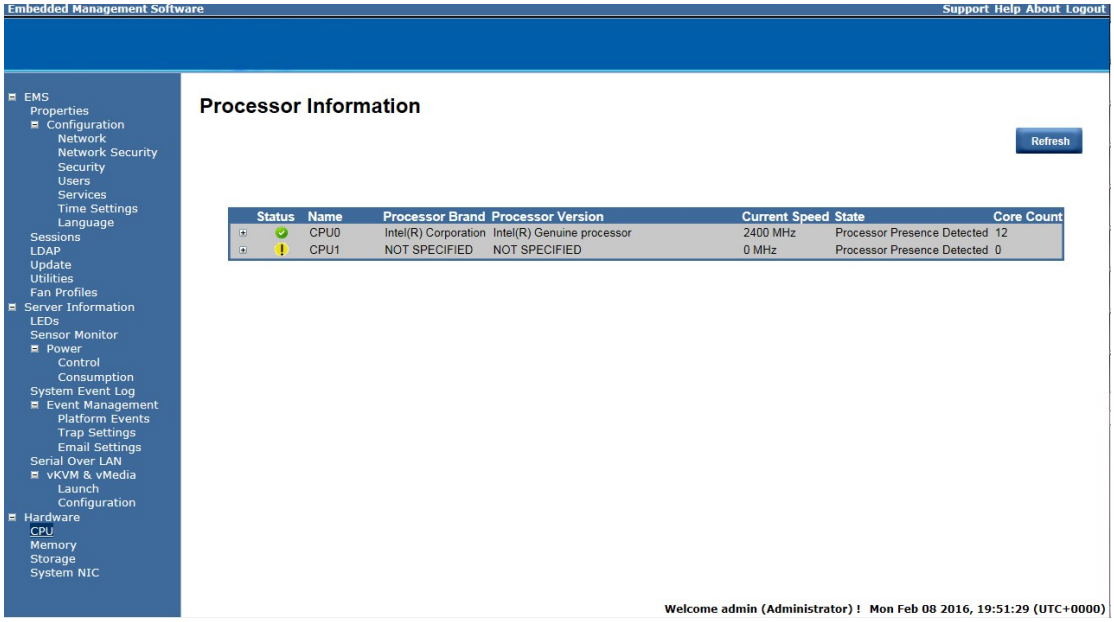
vKVM & vMedia Session Configuration

This screen allows you to configure the Remote Console settings. Check the Virtual KVM Configuration **Enabled** box or Virtual Media Configuration **Enabled** box, and select the **Max Sessions**, **Remote Port**, **Video Encryption Enabled**, and **Preference Client** from the drop-down list. After you finish the configuration, click **Apply Change** to save the settings.



System Information
Processor Information

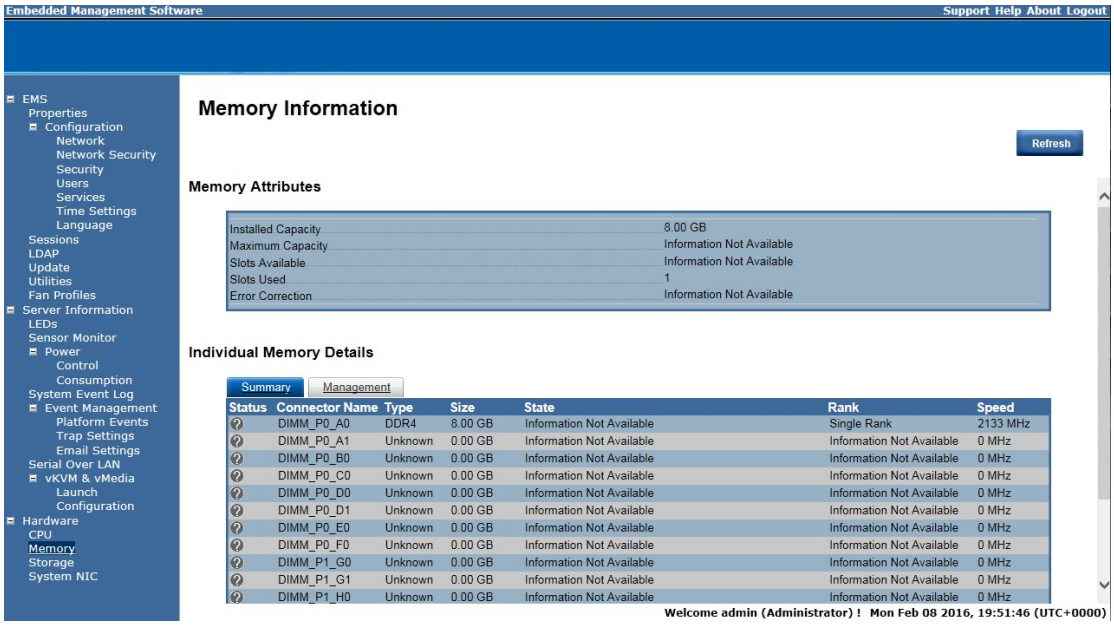
This page displays the technical specifications of the installed processor.



Memory Device Information

This page displays the technical specifications of the installed memory.

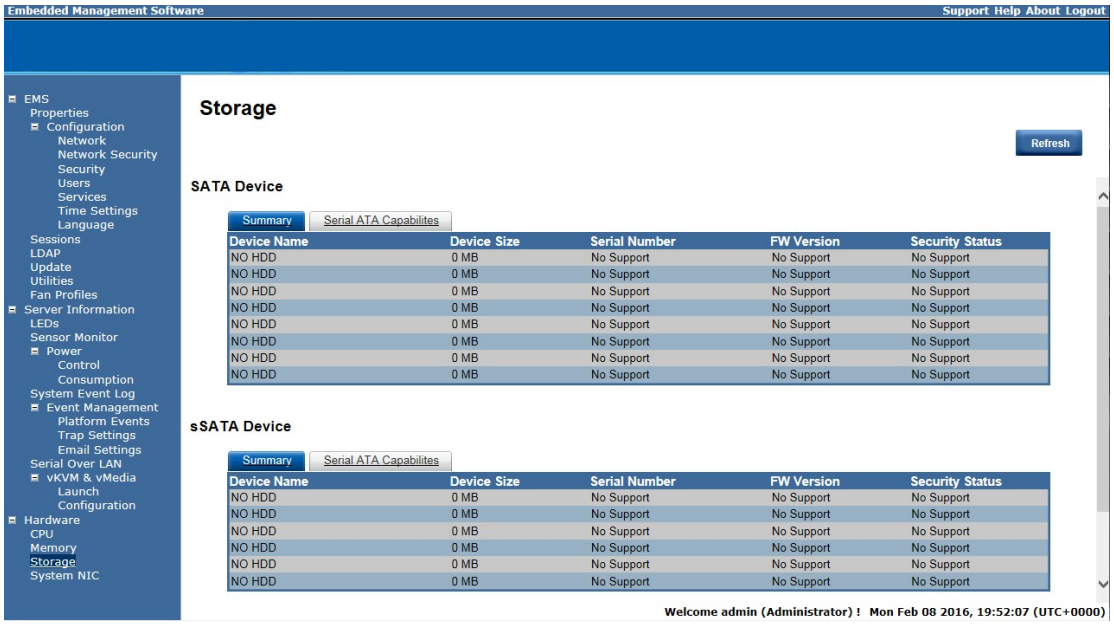
Click **Refresh** to refresh current installed memory information.



Storage Information

This page displays the connected hard disk drive and hardware health information.

Click **Refresh** to view connected hard disk drive hardware health status.



System NIC Information

This page displays the connected hard disk drive and hardware health information.

Click **Refresh** to view the onboard LAN device related information .