Gigabyte Management Console User's Guide

(For ASPEED AST 1250 Chipset)

Version: 1.0

Table of Contents

Using Your Gigabyte Management Console

The Gigabyte Management Console has a user-friendly Graphics User Interface (GUI) called the Gigabyte 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 Gigabyte Management Console GUI's various functions. Each function is described in detail.

Gigabyte 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.

Initial Setup

Configuring the Management Network

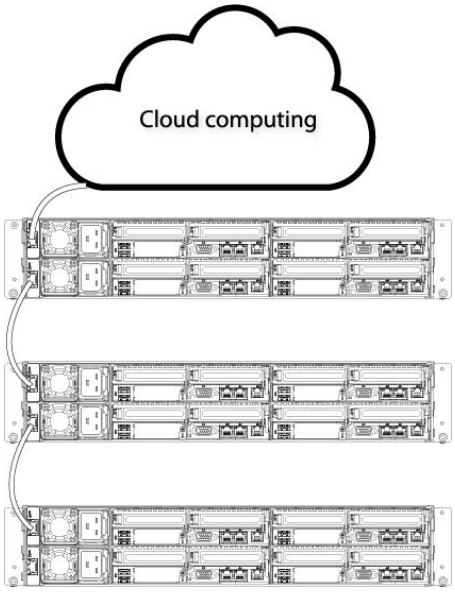
Select whether you want to use your CMC's Ethernet port for stacking (daisy-chained) or use the two CMC Ethernet ports in a redundant manner (ringed).
Stacking is best for customers who would like to take advantage of the cable consolidation feature of Multiple-Nodes. It is easy to use an in-band agent like **Gigabyte Management Console** in the rare case of a CMC port failure.

Select the redundant network connection method for a more reliable connection to the management network. This type of network connection changes the default CMC setting before connecting to the network switch.
To use this configuration, make sure your top LAN switch supports spanning tree protocol.

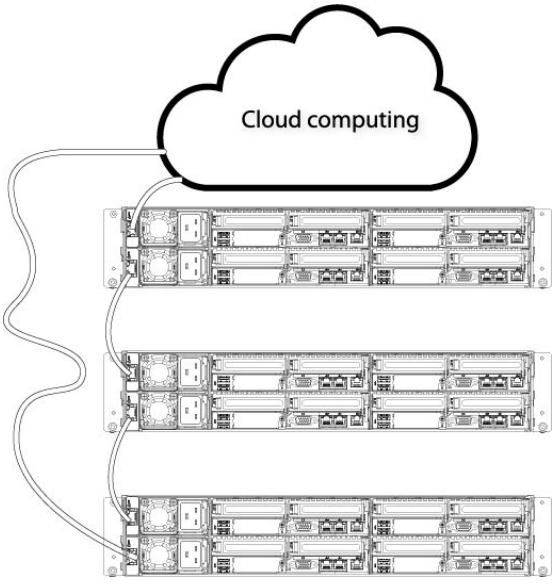
Standard Shipping Configuration: with one hub and one CMC LAN port.

Optional Configuration (Sold Separately): Add an additional hub for stacking or redundant configuration.

Stacking Configuration



Redundant Configuration



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 8 Update 25 or later version (file size: ~ 623KB)

Install Java Tool

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

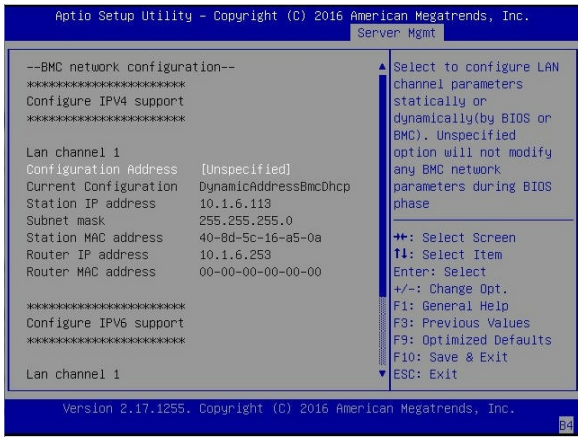
1. Go to http://www.java.com
2. Click Download on the middle of the home page.
3. Click on Agree and Start Free Download
4. Click see all Java downloads
5. Select the operating system you are using.
6. Choose the folder location. (Save the file to a known location on your computer)
7. Click Save.
8. Click Yes to replace.
9. Verify that the
   - Name of the file is **JavaSetup8u25.exe**
   - Size is approximately 623KB.
10. Close all applications including the browser.
11. Double-click on the saved file icon to start the installation process.

Gigabyte Management Console Network Configuration

Please follow the instruction to enable the console redirection function.

1. Plug the VGA port to one of the node system.
2. Boot up your node system.
3. You can gather the BMC IP address on the POST screen.

4. Or, Go to BIOS setup menu.
5. Select **Server Management**.
6. Select **BMC network Configuration**
7. Define Configuration Address source to **DynamicbmcDhcp** or **Static.**
8. Save and Exit.
9. The **BMC IP Address** will appear on the **IPv4 Address** parameter.



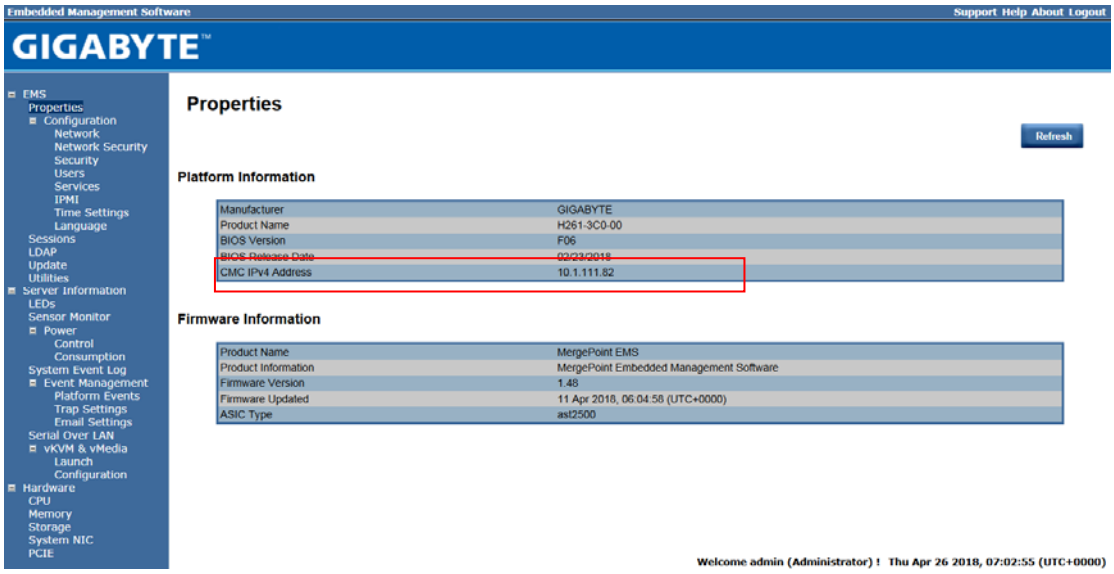
10. Save the configuration and exit BIOS setup menu.
11. Open a web browser and type in your identified IP.

12. Enter the following values:

    Username: **admin**

    Password: **password**

13. Go to the **Properties** page.
14. Gathering the **CMC identified IP address**.



Using the CMC Web UI

The CMC firmware features an embedded web server, enabling users to connect to the CMC 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 ~ 12

• Mozilla® Firefox® 2.0 or later

Linux:

Mozilla Firefox 2.0 or later

Gigabyte 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:
   Username: **admin**
   Password: **password**

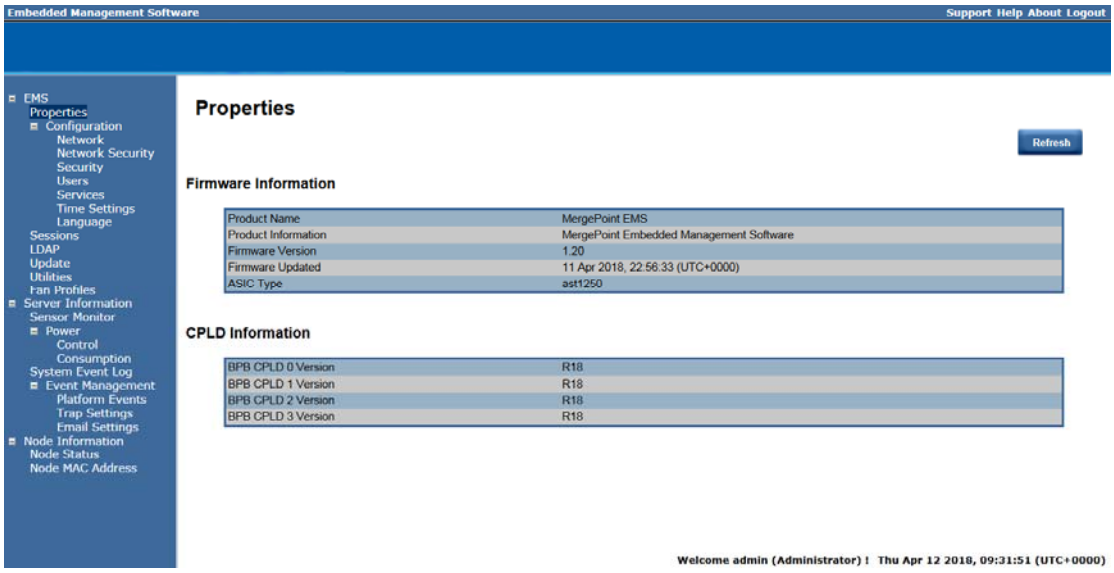
When you log in using the root user name and password, you have full administrative powers. It is advised that once you log in, you change the root password.

Enter Gigabyte Management Console

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

Properties

Properties displays the firmware version of current remote client system.



Configuration

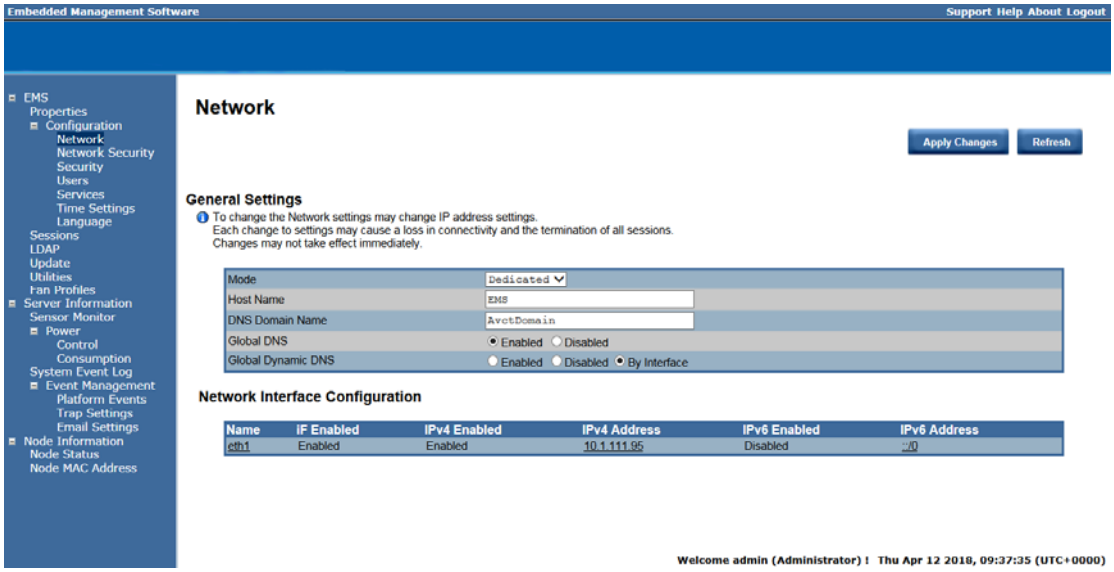
Network

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

1. Dedicate Mode

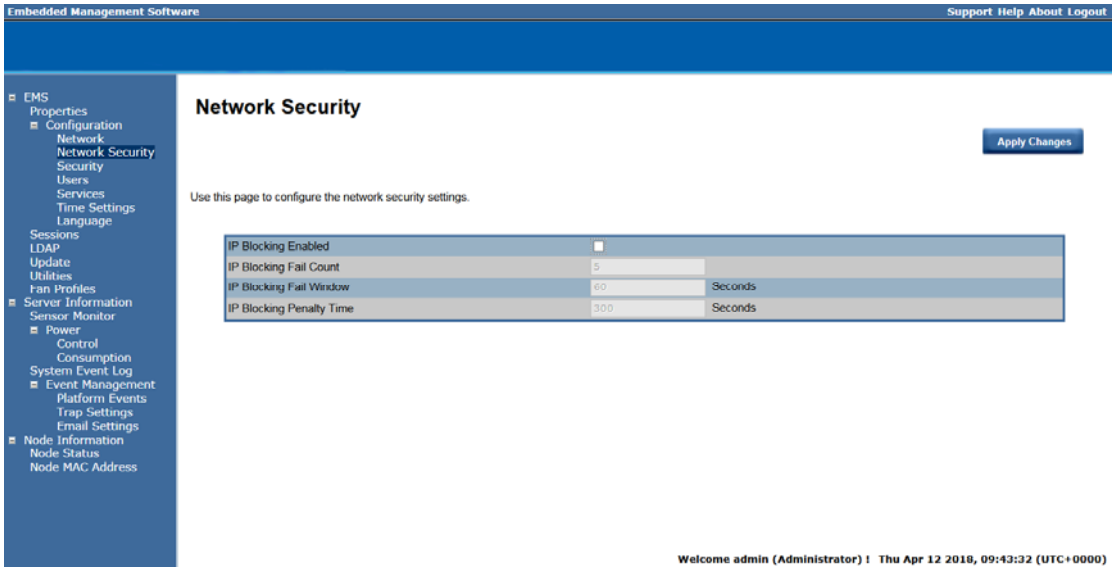
When set to Dedicate Mode, you can configure the CMC related settings through the CMC port.

Click **Apply Change** to save the settings.



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.

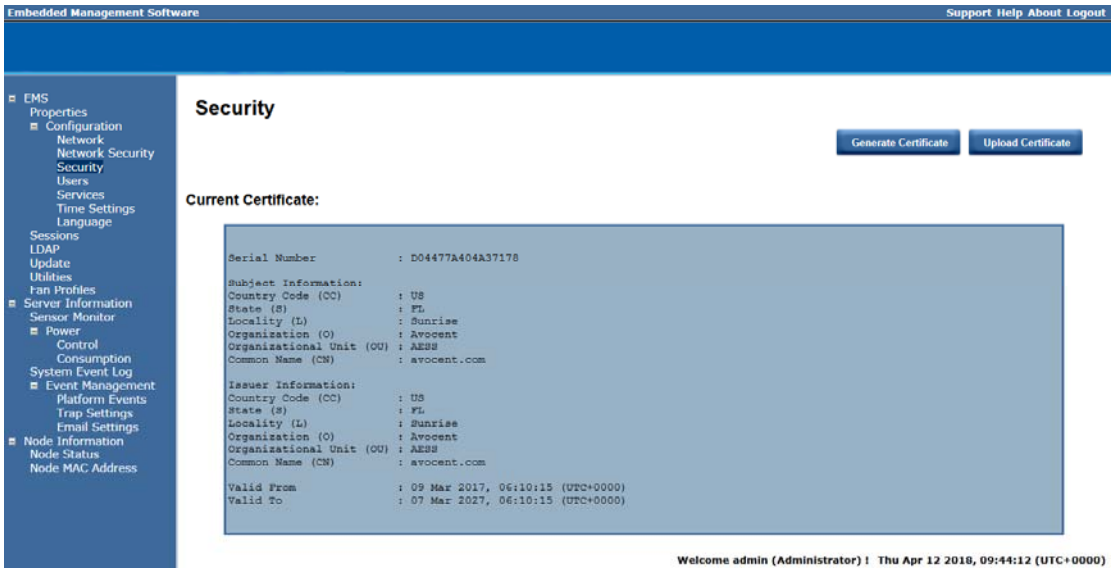


Security

The Security page shows the current certificate status.

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

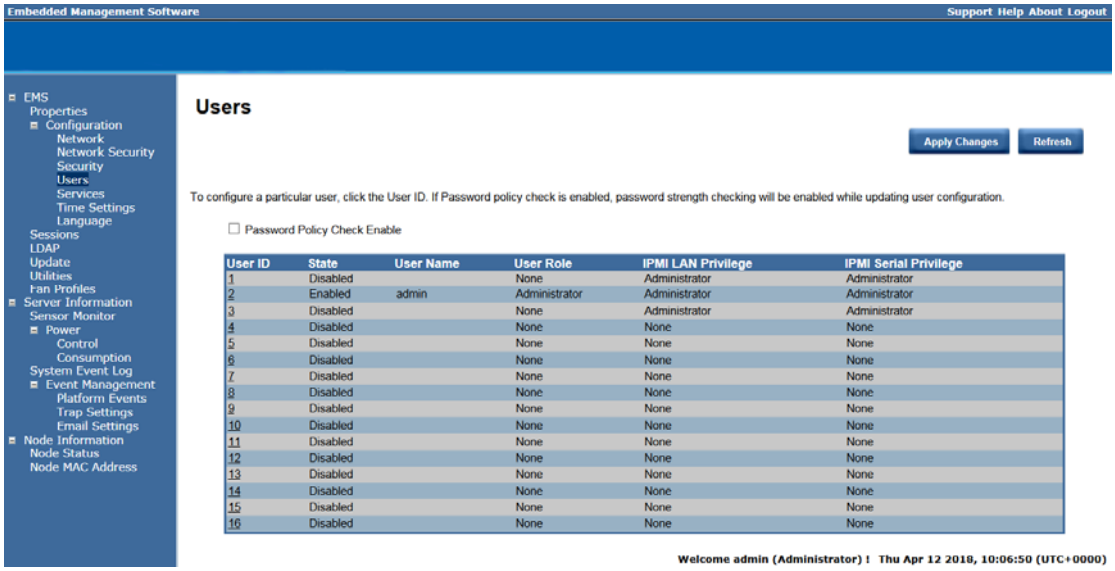
To upload a certificate, click **Upload Certificate**.



Users

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

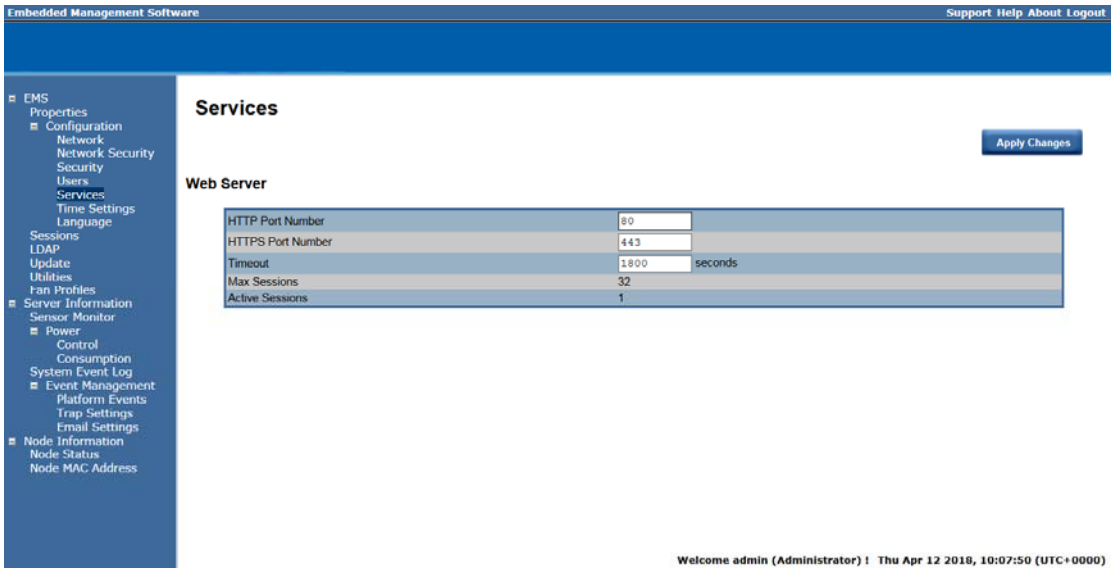
NOTE: CMC convention for enabling an ‘anonymous’ login is to configure the entry for User ID 1 with a null username (all zero’s) and a null password (all zero’s). Applications may then present this to the user as an anonymous login.



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.

Network Time Protocol

Operation Mode

Configures the Operation 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.

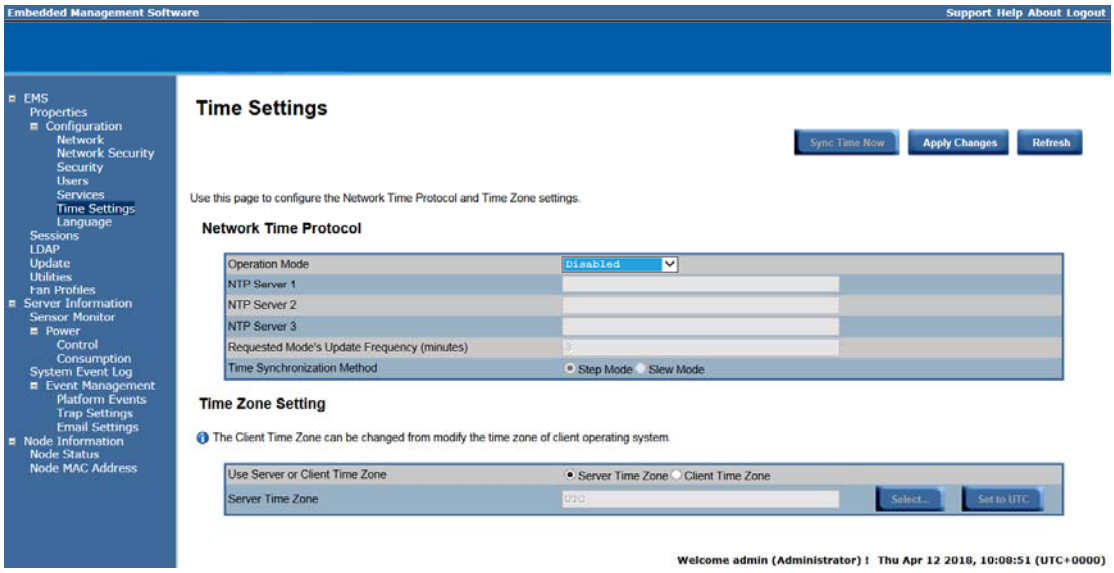
Time Synchronization Method

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.

Time Zone Setting

Configure the client time zone in this parameter.

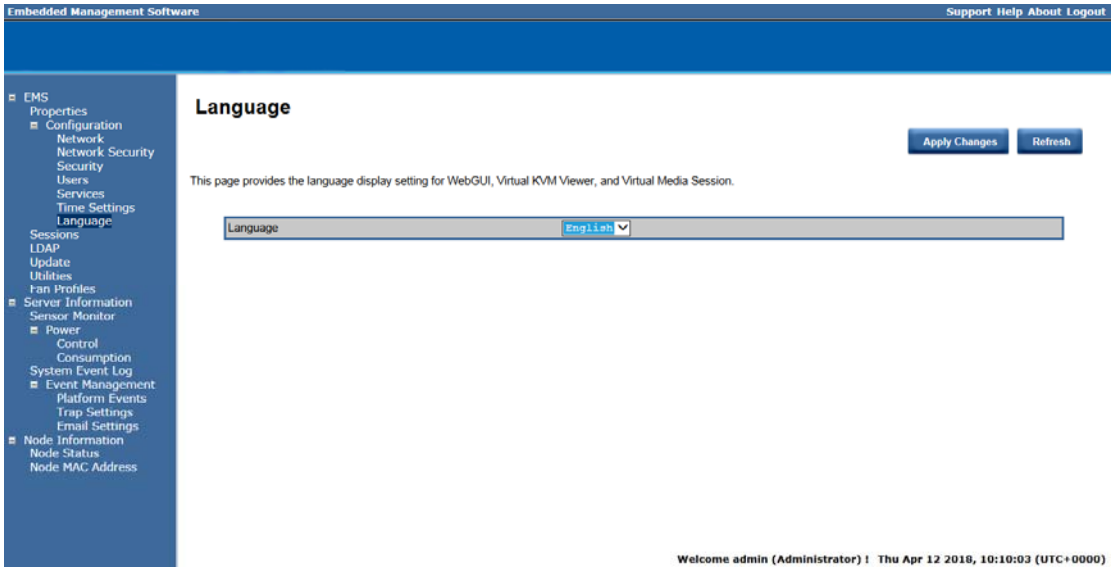
When you finish the configuration, click **Apply Changes**.



Language

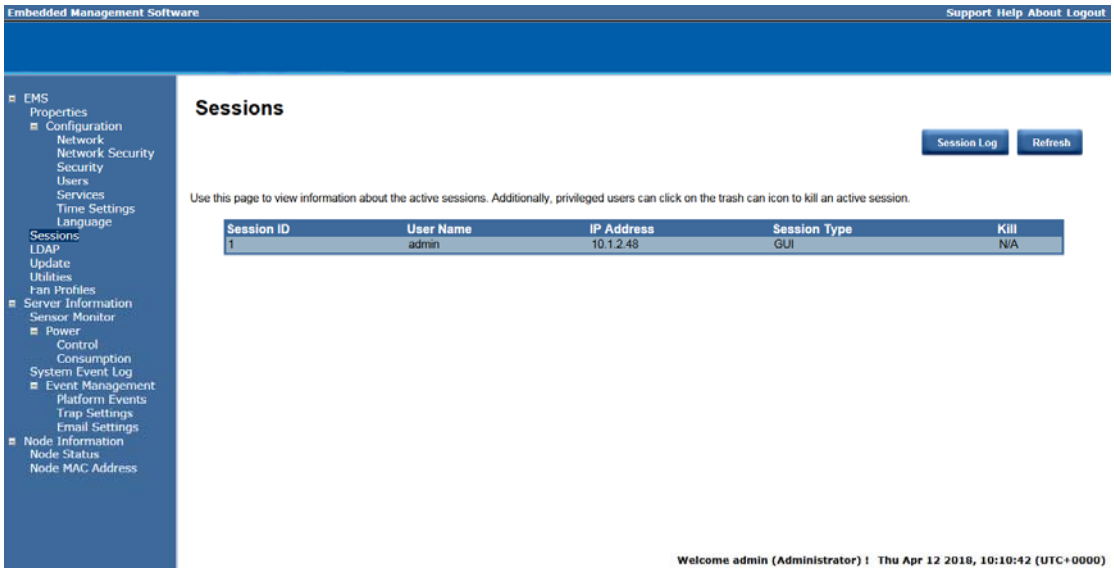
This page allow users to choose preferred language when using the WebUI.

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



Sessions

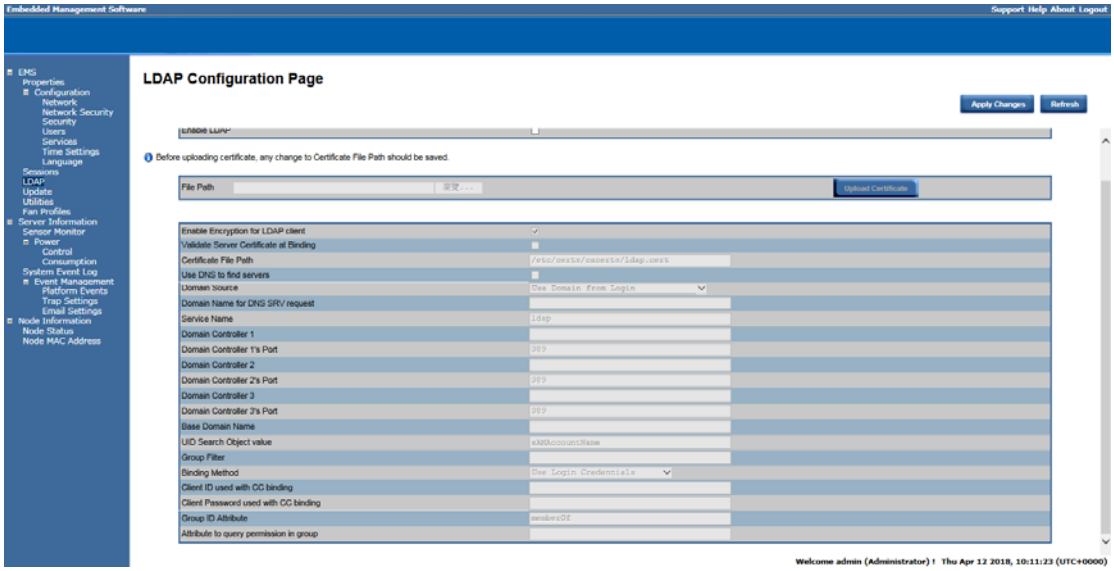
This screen displays information on Active Sessions. Additionally, the trash can icon provides the delete function for privileged users. Click Session log to view the session log. Click **Refresh** to refresh the Sessions status.



LDAP

LDAP screen allows download user list of LDAP server then create Gigabyte 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.



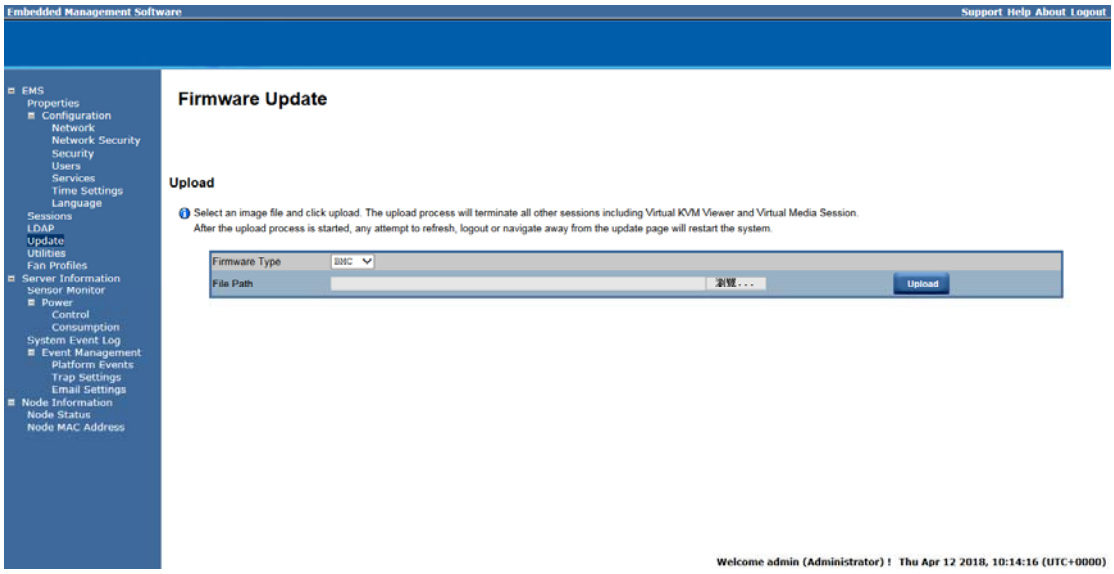
Firmware Updates

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**.

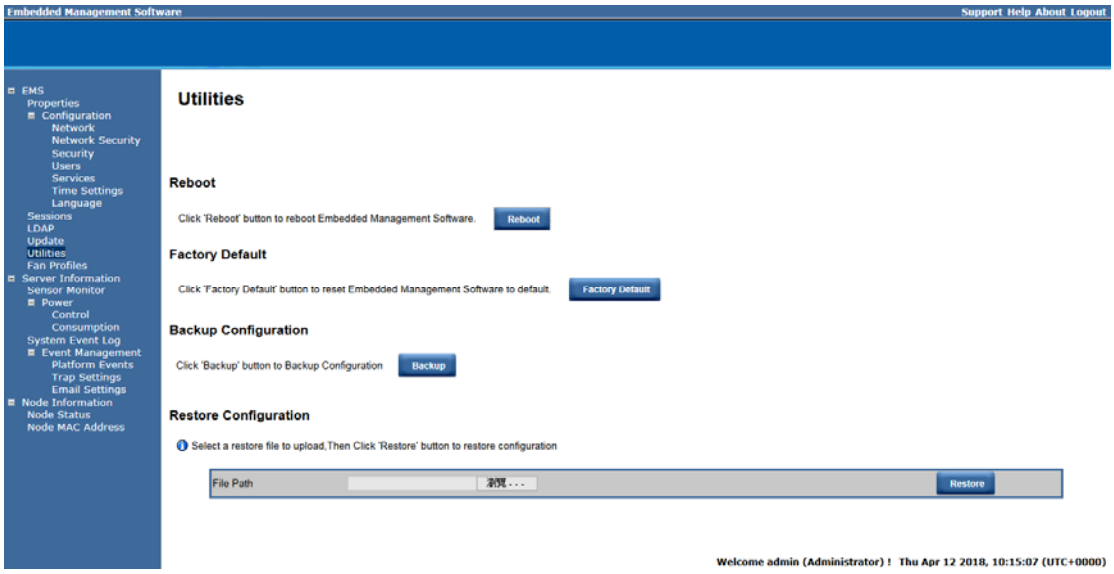
Click **Upload** to update to the new version of firmware.



Utilities

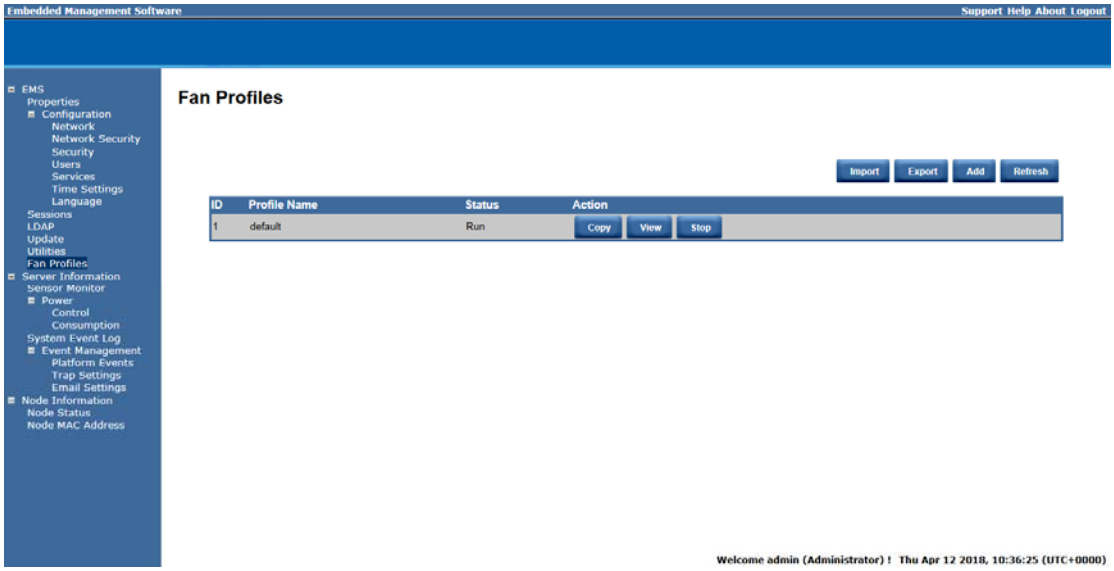
Utilities provides CMC reboot and Factory default restore functions.

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**.



Fan Profiles

Fan Profiles provides user to configure the system fan control policy.

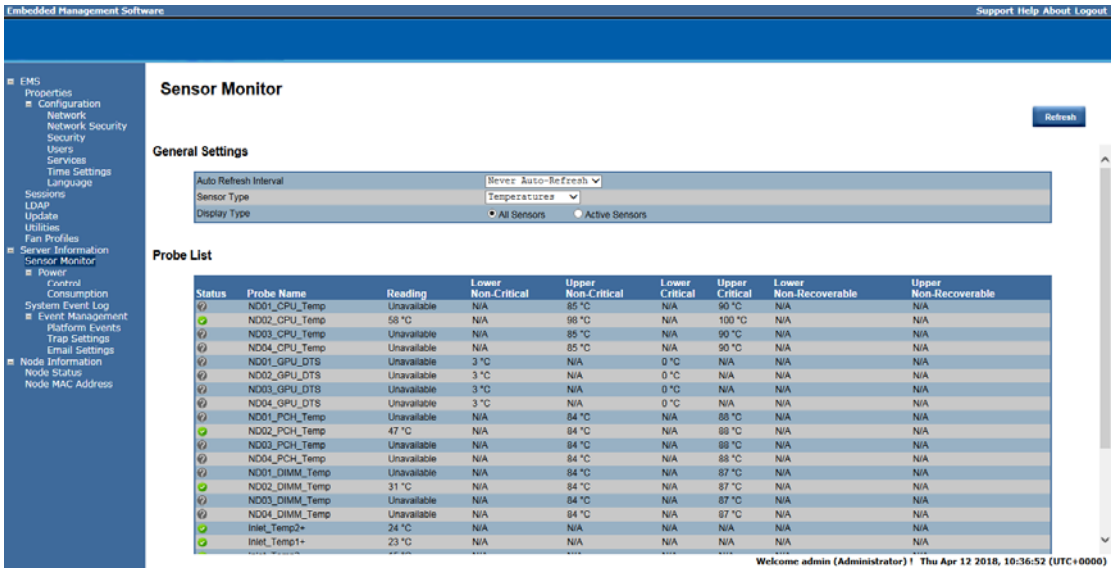


Server Information

Sensor Monitor

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

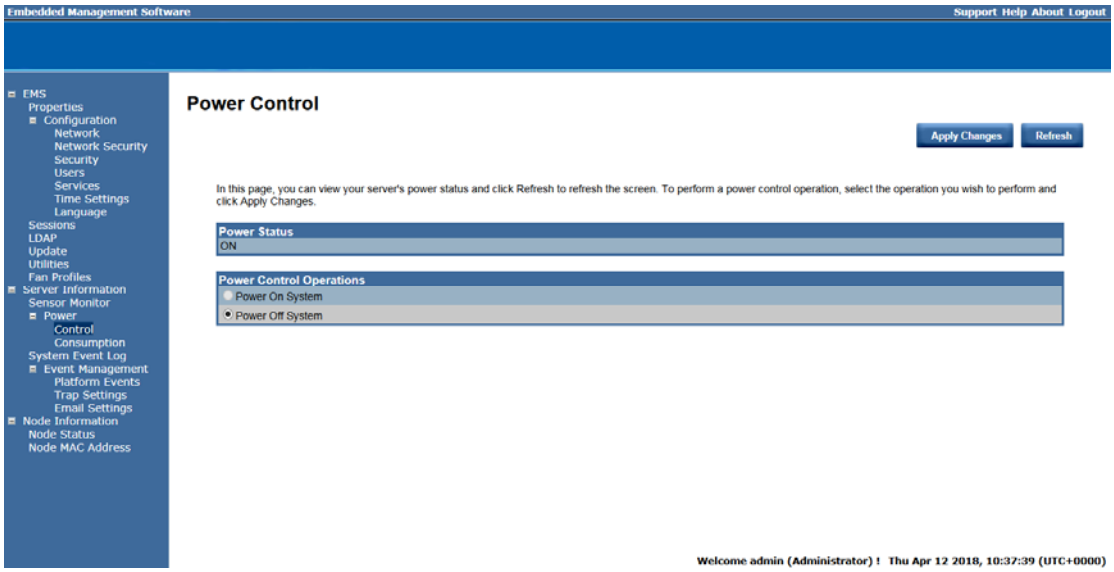
To view the Probe list, click **Show Graph**. And click **Refresh** to update current probe list.



Power Control

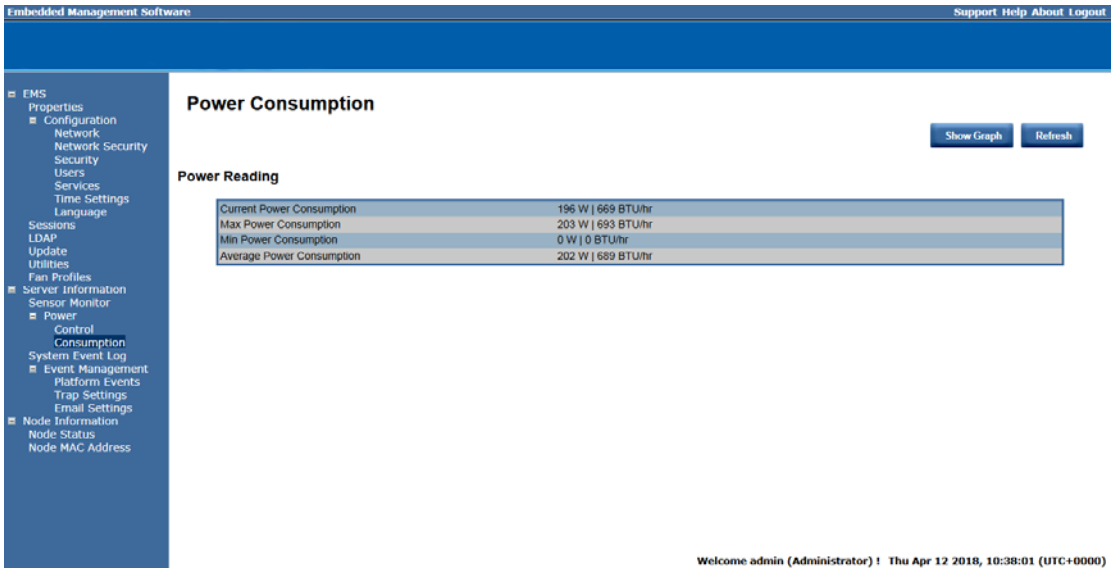
The Power Control allows you to power on/off/cycle the remote host system. Additionally you can see the remote power status.

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



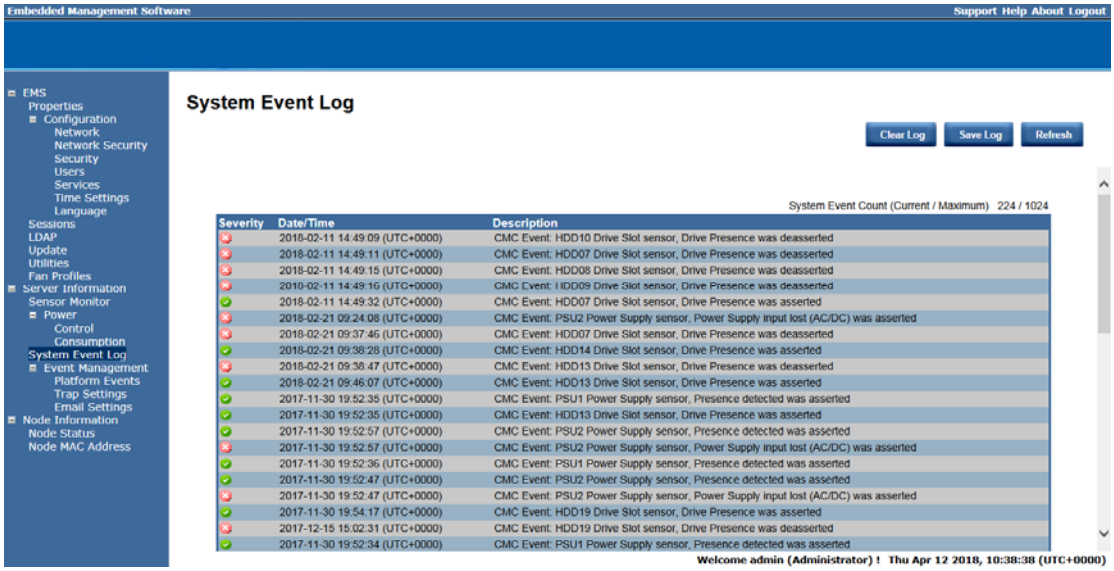
Power Consumption

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.



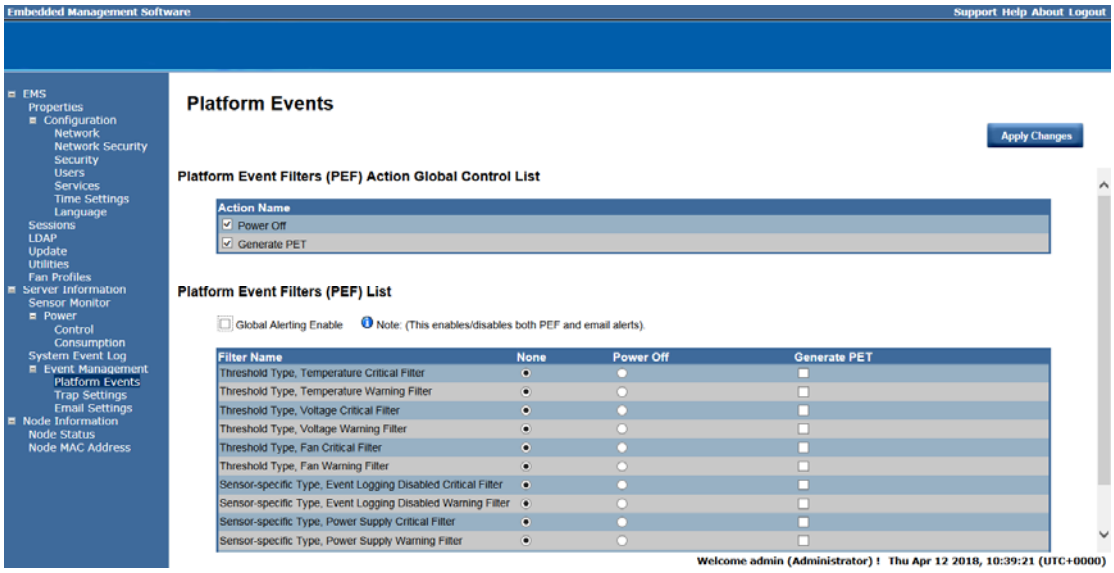
Event Management

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**.



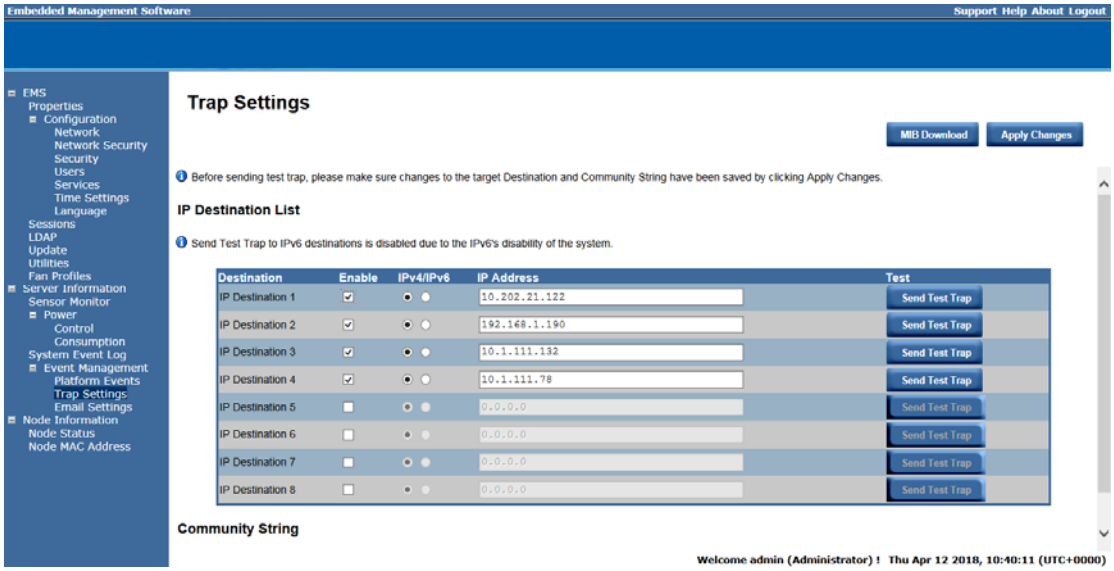
Trap Settings

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

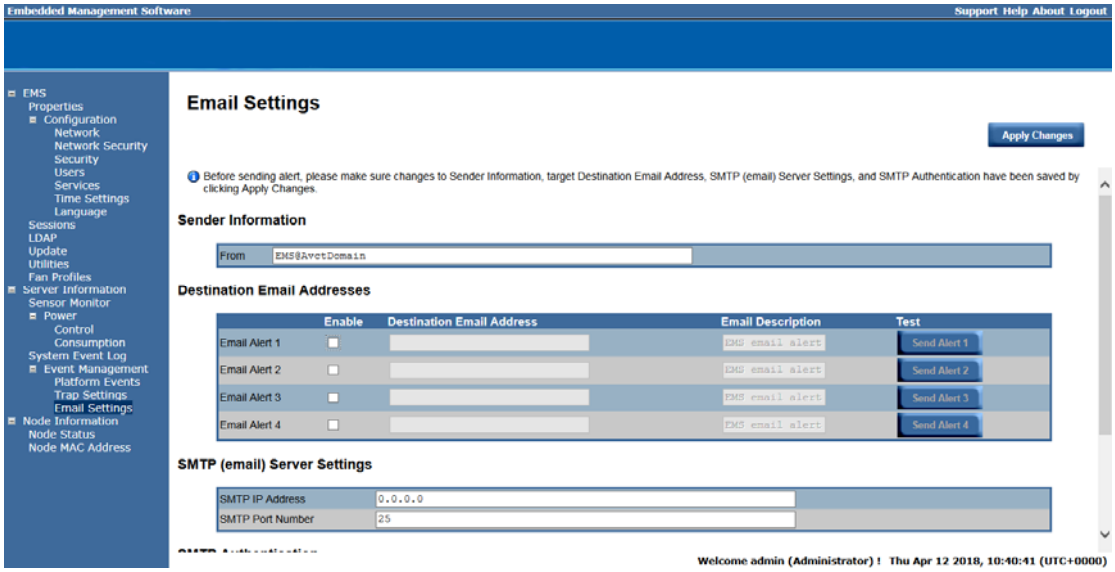
If you want the alert to be sent by email, you can configure to specify the e-mail address, subject and message in the Email Settings. After you finish the configuration, click Apply Change to save the settings.

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”.

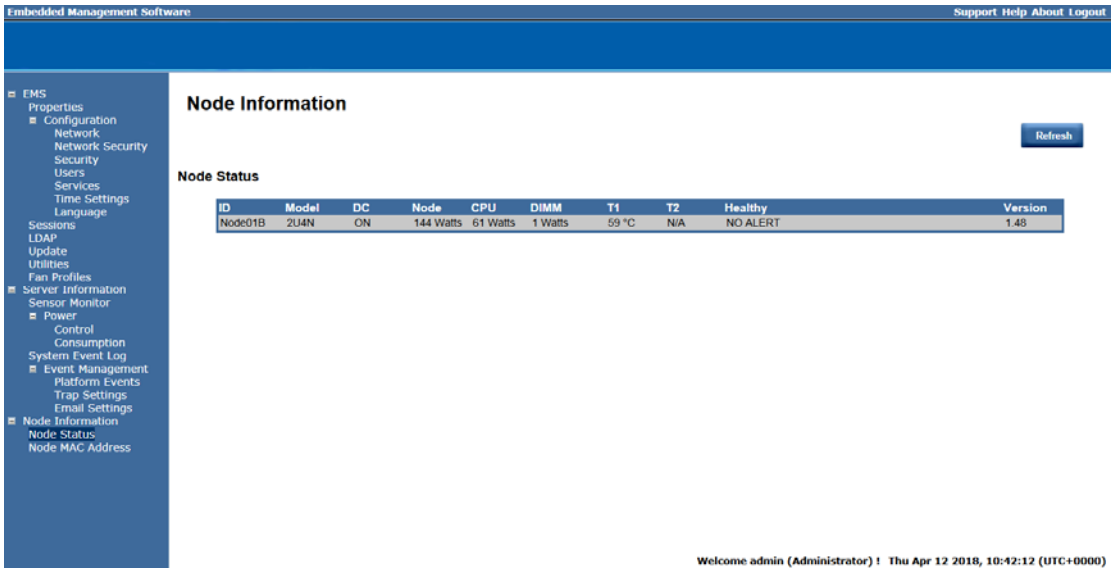


Node Information

Node Status

This page displays the technical specifications of the connected node.

Click **Refresh** to refresh current connected node information.



Node MAC Address

This page displays the connected node MAC address information.

Click **Refresh** to refresh current connected node MAC address information.