

Gigabyte Management Console User's Guide

(For ASPEED AST 1250 Chipset)

Version: 1.0

Table of Contents

Using Your Gigabyte Management Console	2
Gigabyte Management Console Key Features and Functions.....	3
Initial Setup	4
Configuring the Management Network.....	4
Software Install	5
Prerequisites on remote management PC.....	5
Install Java Tool.....	5
Gigabyte Management Console Network Configuration.....	6
Using the Web UI.....	8
Gigabyte Management Console Overview	9
Enter Gigabyte Management Console	10
Properties	10
Configuration	11
Network.....	11
Network Security	12
Security	13
Users	14
Services	15
Time Setting	16
Language.....	17
Sessions.....	18
LDAP	19
Firmware Updates	20
Utilities.....	21
FAN Profiles	22
Server Information	23
Sensor Monitor.....	23
Power Control	24
Power Consumption.....	25
System Event Log	26
Event Management	27
Platform Event	27
Trap Settings	28
Email Settings	29
Node Information	30
Node Status	30
Node MAC Address	31

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 server 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.

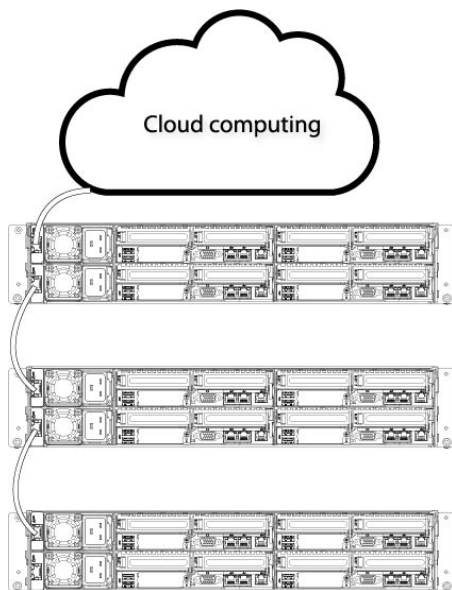
Select the redundant network connection method for a more reliable connection to the management network. This type of network connection changes the default CMC setting before connecting to the network switch.

To use this configuration, make sure your top LAN switch supports spanning tree protocol.

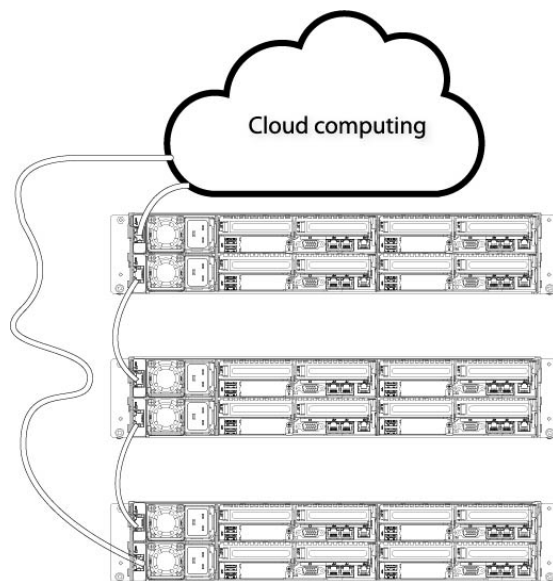
Standard Shipping Configuration: with one hub and one CMC LAN port.

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.

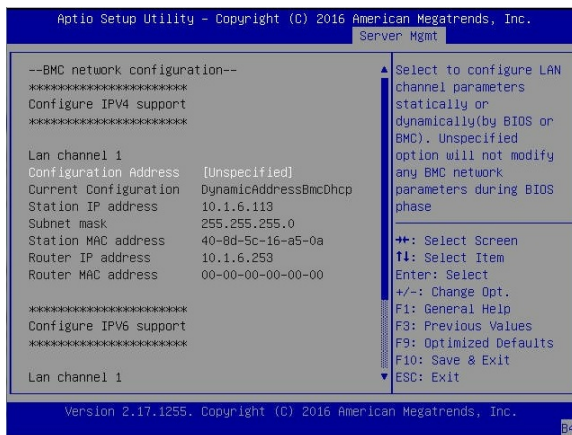
Gigabyte Management Console Network Configuration

Please follow the instruction to enable the console redirection function.

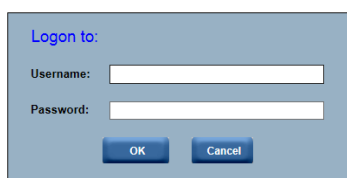
1. Plug the VGA port to one of the node system.
2. Boot up your node system.
3. You can gather the BMC IP address on the POST screen.



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.

A screenshot of a login dialog box with a light blue background. It features a "Logon to:" label at the top left. Below it are two input fields: "Username:" and "Password:". At the bottom, there are two buttons: "OK" and "Cancel".

12. Enter the following values:
Username: **admin**
Password: **password**
13. Go to the **Properties** page.
14. Gathering the **CMC identified IP address**.

The screenshot displays the GIGABYTE Embedded Management Software (EMS) interface. The top navigation bar includes 'Support', 'Help', 'About', and 'Logout'. The left sidebar lists various configuration categories under 'EMS', with 'Properties' selected. The main content area is titled 'Properties' and contains two sections: 'Platform Information' and 'Firmware Information'. A 'Refresh' button is located in the top right of the main area.

Platform Information

Manufacturer	GIGABYTE
Product Name	H261-3C0-00
BIOS Version	F06
BIOS Release Date	02/23/2018
CMC IPv4 Address	10.1.111.82

Firmware Information

Product Name	MergePoint EMS
Product Information	MergePoint Embedded Management Software
Firmware Version	1.48
Firmware Updated	11 Apr 2018, 06:04:56 (UTC+0000)
ASIC Type	ast2500

Welcome admin (Administrator) ! Thu Apr 26 2018, 07:02:55 (UTC+0000)

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



The image shows a login dialog box with a light blue background. At the top left, it says "Logon to:" in blue text. Below that are two input fields: "Username:" and "Password:". At the bottom, there are two buttons: "OK" and "Cancel".

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.

Embedded Management Software Support Help About Logout

Properties Refresh

Firmware Information

Product Name	MergePoint EMS
Product Information	MergePoint Embedded Management Software
Firmware Version	1.20
Firmware Updated	11 Apr 2018, 22:56:33 (UTC+0000)
ASIC Type	ast1250

CPLD Information

BFB CPLD 0 Version	R18
BFB CPLD 1 Version	R18
BFB CPLD 2 Version	R18
BFB CPLD 3 Version	R18

Welcome admin (Administrator) ! Thu Apr 12 2018, 09:31:51 (UTC+0000)

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.

The screenshot shows the 'Network' configuration page in the Embedded Management Software. The page has a blue header with 'Embedded Management Software' on the left and 'Support Help About Logout' on the right. A navigation menu on the left lists various settings categories. The main content area is titled 'Network' and includes a 'General Settings' section with a warning icon and text: 'To change the Network settings may change IP address settings. Each change to settings may cause a loss in connectivity and the termination of all sessions. Changes may not take effect immediately.' Below this are input fields for 'Mode' (set to 'Dedicated'), 'Host Name' (set to 'EMS'), 'DNS Domain Name' (set to 'AvotDomain'), 'Global DNS' (radio buttons for 'Enabled' and 'Disabled'), and 'Global Dynamic DNS' (radio buttons for 'Enabled', 'Disabled', and 'By Interface'). There are 'Apply Changes' and 'Refresh' buttons. Below the settings is a 'Network Interface Configuration' table with columns: Name, IF Enabled, IPv4 Enabled, IPv4 Address, IPv6 Enabled, and IPv6 Address. The table shows one entry for 'eth1' with 'IF Enabled', 'IPv4 Enabled', 'IPv4 Address' (10.1.111.95), 'IPv6 Enabled' (Disabled), and 'IPv6 Address' (::0). At the bottom right, a footer message reads: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 09:37:35 (UTC+0000)'.

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.

Embedded Management Software Support Help About Logout

Network Security Apply Changes

Use this page to configure the network security settings.

IP Blocking Enabled	<input type="checkbox"/>	
IP Blocking Fail Count	5	
IP Blocking Fail Window	60	Seconds
IP Blocking Penalty Time	300	Seconds

Welcome admin (Administrator) ! Thu Apr 12 2018, 09:43:32 (UTC+0000)

Security

The Security page shows the current certificate status.

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

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

Embedded Management Software Support Help About Logout

EMS
Properties
 Configuration
 Network
 Network Security
 Security
 Users
 Services
 Time Settings
 Language
Sessions
LDAP
Update
Utilities
Fan Profiles
Server Information
 Sensor Monitor
 Power
 Control
 Consumption
System Event Log
 Event Management
 Platform Events
 Trap Settings
 Email Settings
Node Information
 Node Status
 Node MAC Address

Security

[Generate Certificate](#) [Upload Certificate](#)

Current Certificate:

```
Serial Number      : D04477A404A37178
Subject Information:
Country Code (CC)  : US
State (S)          : FL
Locality (L)       : Sunrise
Organization (O)   : Avocent
Organizational Unit (OU) : AES8
Common Name (CN)   : avocent.com

Issuer Information:
Country Code (CC)  : US
State (S)          : FL
Locality (L)       : Sunrise
Organization (O)   : Avocent
Organizational Unit (OU) : AES8
Common Name (CN)   : avocent.com

Valid From         : 09 Mar 2017, 06:10:15 (UTC+0000)
Valid To           : 07 Mar 2027, 06:10:15 (UTC+0000)
```

Welcome admin (Administrator) ! Thu Apr 12 2018, 09:44:12 (UTC+0000)

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.

Embedded Management Software Support Help About Logout

Users [Apply Changes](#) [Refresh](#)

To configure a particular user, click the User ID. If Password policy check is enabled, password strength checking will be enabled while updating user configuration.

Password Policy Check Enable

User ID	State	User Name	User Role	IPMI LAN Privilege	IPMI Serial Privilege
1	Disabled		None	Administrator	Administrator
2	Enabled	admin	Administrator	Administrator	Administrator
3	Disabled		None	Administrator	Administrator
4	Disabled		None	None	None
5	Disabled		None	None	None
6	Disabled		None	None	None
7	Disabled		None	None	None
8	Disabled		None	None	None
9	Disabled		None	None	None
10	Disabled		None	None	None
11	Disabled		None	None	None
12	Disabled		None	None	None
13	Disabled		None	None	None
14	Disabled		None	None	None
15	Disabled		None	None	None
16	Disabled		None	None	None

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:06:50 (UTC+0000)

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**.

The screenshot shows the configuration page for 'Services' in the Embedded Management Software. The page has a blue header with 'Embedded Management Software' on the left and 'Support Help About Logout' on the right. A left sidebar contains a tree view of configuration options, with 'Services' selected. The main content area is titled 'Services' and contains a 'Web Server' configuration table. The table has five rows: 'HTTP Port Number' with a value of 80, 'HTTPS Port Number' with a value of 443, 'Timeout' with a value of 1800 and the unit 'seconds', 'Max Sessions' with a value of 32, and 'Active Sessions' with a value of 1. An 'Apply Changes' button is located in the top right corner of the configuration area. At the bottom right of the page, there is a status message: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:07:50 (UTC+0000)'.

Web Server	
HTTP Port Number	80
HTTPS Port Number	443
Timeout	1800 seconds
Max Sessions	32
Active Sessions	1

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**.

The screenshot displays the 'Time Settings' page in the Embedded Management Software (EMS) interface. The page is titled 'Time Settings' and includes a navigation menu on the left with options like EMS, Properties, Configuration, Network, Network Security, Security, Users, Services, Time Settings, Language, Sessions, LDAP, Update, Utilities, Fan Profiles, Server Information, Sensor Monitor, Power, Control, Consumption, System Event Log, Event Management, Platform Events, Trap Settings, Email Settings, Node Information, Node Status, and Node MAC Address. The main content area is divided into two sections: 'Network Time Protocol' and 'Time Zone Setting'. The 'Network Time Protocol' section includes a dropdown for 'Operation Mode' (set to 'Disabled'), three text input fields for 'NTP Server 1', 'NTP Server 2', and 'NTP Server 3', a text input for 'Requested Mode's Update Frequency (minutes)' (set to '3'), and radio buttons for 'Time Synchronization Method' (set to 'Step Mode'). The 'Time Zone Setting' section includes a message: 'The Client Time Zone can be changed from modify the time zone of client operating system.' Below this, there are radio buttons for 'Use Server or Client Time Zone' (set to 'Server Time Zone') and a text input for 'Server Time Zone' (set to 'UTC'). There are also buttons for 'Sync Time Now', 'Apply Changes', and 'Refresh' at the top right of the page. The footer of the page reads: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:08:51 (UTC+0000)'.

Language

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

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

The screenshot shows the 'Language' configuration page in the Embedded Management Software (EMS) web interface. The page has a blue header with 'Embedded Management Software' on the left and 'Support Help About Logout' on the right. A left-hand navigation menu lists various configuration categories, with 'Language' highlighted. The main content area is titled 'Language' and contains a description: 'This page provides the language display setting for WebGUI, Virtual KVM Viewer, and Virtual Media Session.' Below the description is a dropdown menu labeled 'Language' with 'English' selected. To the right of the dropdown are two buttons: 'Apply Changes' and 'Refresh'. At the bottom right of the page, a status message reads: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:10:03 (UTC+0000)'.

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.

Embedded Management Software Support Help About Logout

Sessions [Session Log](#) [Refresh](#)

Use this page to view information about the active sessions. Additionally, privileged users can click on the trash can icon to kill an active session.

Session ID	User Name	IP Address	Session Type	Kill
1	admin	10.1.2.48	GUI	N/A

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:10:42 (UTC+0000)

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.

The screenshot displays the 'LDAP Configuration Page' within the Embedded Management Software interface. The page includes a navigation menu on the left and a main configuration area. The configuration area contains several sections:

- LDAP Configuration:** Includes a search bar for LDAP servers and a note: "Before uploading certificate, any change to Certificate File Path should be saved." Below this is a 'File Path' field with an 'Upload Certificate' button.
- Server Information:** A table of configuration options with checkboxes and dropdown menus.

Configuration Option	Value / Status
Enable Encryption for LDAP client	<input checked="" type="checkbox"/>
Validate Server Certificate at Binding	<input checked="" type="checkbox"/>
Certificate File Path	/etc/openssl/certs/ldap.pem
Use DNS to find servers	<input checked="" type="checkbox"/>
Utdomain source	Use Domain from Login
Domain Name for DNS SRV request	
Service Name	ldap
Domain Controller 1's Port	389
Domain Controller 2's Port	389
Domain Controller 3's Port	389
Base Domain Name	
UID Search Object value	sAMAccountName
Group Filter	
Binding Method	Use Login Credentials
Client ID used with CC binding	
Client Password used with CC binding	
Group ID Attribute	smbnetDE
Attribute to query permission in group	

At the bottom right of the page, the status bar reads: "Welcome admin (Administrator) | Thu Apr 12 2018, 10:11:23 (UTC+0000)".

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.

The screenshot shows the 'Firmware Update' page in the Embedded Management Software (EMS) interface. The page has a blue header with 'Embedded Management Software' on the left and 'Support Help About Logout' on the right. A left sidebar contains a navigation menu with categories like EMS, Properties, Configuration, Network, Security, Users, Services, Time Settings, Language, Sessions, LDAP, Update, Utilities, Fan Profiles, Server Information, Sensor Monitor, Power, Control, Consumption, System Event Log, Event Management, Platform Events, Trap Settings, Email Settings, Node Information, Node Status, and Node MAC Address. The main content area is titled 'Firmware Update' and features an 'Upload' section. Below the title, there is an information icon and a warning message: 'Select an image file and click upload. The upload process will terminate all other sessions including Virtual KVM Viewer and Virtual Media Session. After the upload process is started, any attempt to refresh, logout or navigate away from the update page will restart the system.' Below this message is a form with a 'Firmware Type' dropdown menu set to 'BMC', a 'File Path' input field with a 'Browse...' button, and an 'Upload' button. At the bottom right of the page, there is a status bar that reads 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:14:16 (UTC+0000)'.

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**.

The screenshot displays the 'Utilities' page in the Embedded Management Software interface. The page is titled 'Utilities' and contains four main sections:

- Reboot**: Click 'Reboot' button to reboot Embedded Management Software. A blue 'Reboot' button is present.
- Factory Default**: Click 'Factory Default' button to reset Embedded Management Software to default. A blue 'Factory Default' button is present.
- Backup Configuration**: Click 'Backup' button to Backup Configuration. A blue 'Backup' button is present.
- Restore Configuration**: Select a restore file to upload, Then Click 'Restore' button to restore configuration. Below this instruction is a text input field labeled 'File Path' with a 'Browse ...' button and a 'Restore' button.

The left sidebar shows a navigation menu with the following items: EMS, Properties, Configuration, Network, Network Security, Security, Users, Services, Time Settings, Language, Sessions, LDAP, Update, Utilities, Fan Profiles, Server Information, Sensor Monitor, Power, Control, Consumption, System Event Log, Event Management, Platform Events, Trap Settings, Email Settings, Node Information, Node Status, and Node MAC Address. The top right corner of the page has links for Support, Help, About, and Logout. The bottom right corner displays the user information: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:15:07 (UTC+0000)'.

Fan Profiles

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

Embedded Management Software Support Help About Logout

Fan Profiles

[Import](#) [Export](#) [Add](#) [Refresh](#)

ID	Profile Name	Status	Action
1	default	Run	Copy View Stop

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:36:25 (UTC+0000)

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.

Sensor Monitor

Auto Refresh Interval: Never Auto-Refresh

Sensor Type: Temperatures

Display Type: All Sensors Active Sensors

Probe List

Status	Probe Name	Reading	Lower Non-Critical	Upper Non-Critical	Lower Critical	Upper Critical	Lower Non-Recoverable	Upper Non-Recoverable
🔄	ND01_CPU_Temp	Unavailable	N/A	85 °C	N/A	90 °C	N/A	N/A
🟢	ND02_CPU_Temp	58 °C	N/A	98 °C	N/A	100 °C	N/A	N/A
🔄	ND03_CPU_Temp	Unavailable	N/A	85 °C	N/A	90 °C	N/A	N/A
🔄	ND04_CPU_Temp	Unavailable	N/A	85 °C	N/A	90 °C	N/A	N/A
🔄	ND01_GPU_DTS	Unavailable	3 °C	N/A	0 °C	N/A	N/A	N/A
🔄	ND02_GPU_DTS	Unavailable	3 °C	N/A	0 °C	N/A	N/A	N/A
🔄	ND03_GPU_DTS	Unavailable	3 °C	N/A	0 °C	N/A	N/A	N/A
🔄	ND04_GPU_DTS	Unavailable	3 °C	N/A	0 °C	N/A	N/A	N/A
🔄	ND01_PCH_Temp	Unavailable	N/A	84 °C	N/A	88 °C	N/A	N/A
🟢	ND02_PCH_Temp	47 °C	N/A	84 °C	N/A	88 °C	N/A	N/A
🔄	ND03_PCH_Temp	Unavailable	N/A	84 °C	N/A	88 °C	N/A	N/A
🔄	ND04_PCH_Temp	Unavailable	N/A	84 °C	N/A	88 °C	N/A	N/A
🔄	ND01_DIMM_Temp	Unavailable	N/A	84 °C	N/A	87 °C	N/A	N/A
🟢	ND02_DIMM_Temp	31 °C	N/A	84 °C	N/A	87 °C	N/A	N/A
🔄	ND03_DIMM_Temp	Unavailable	N/A	84 °C	N/A	87 °C	N/A	N/A
🔄	ND04_DIMM_Temp	Unavailable	N/A	84 °C	N/A	87 °C	N/A	N/A
🟢	Inlet_Temp2+	24 °C	N/A	N/A	N/A	N/A	N/A	N/A
🟢	Inlet_Temp1+	23 °C	N/A	N/A	N/A	N/A	N/A	N/A

Welcome admin (Administrator) | Thu Apr 12 2018, 10:36:52 (UTC+0000)

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**.

The screenshot shows the 'Power Control' page in the Embedded Management Software. The page has a blue header with 'Embedded Management Software' on the left and 'Support Help About Logout' on the right. A left sidebar contains a navigation menu with categories like EMS, Properties, Configuration, Network, Security, Users, Services, Time Settings, Language, Sessions, LDAP, Update, Utilities, Fan Profiles, Server Information, Sensor Monitor, Power, Control, Consumption, System Event Log, Event Management, Platform Events, Trap Settings, Email Settings, Node Information, Node Status, and Node MAC Address. The main content area is titled 'Power Control' and contains two buttons: 'Apply Changes' and 'Refresh'. Below the buttons is a text instruction: 'In this page, you can view your server's power status and click Refresh to refresh the screen. To perform a power control operation, select the operation you wish to perform and click Apply Changes.' There are two sections: 'Power Status' showing 'ON' and 'Power Control Operations' with radio buttons for 'Power On System' and 'Power Off System'. At the bottom right, a status message reads: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:37:39 (UTC+0000)'.

Power Consumption

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

Embedded Management Software Support Help About Logout

Power Consumption [Show Graph](#) [Refresh](#)

Power Reading

Current Power Consumption	196 W 669 BTU/hr
Max Power Consumption	203 W 693 BTU/hr
Min Power Consumption	0 W 0 BTU/hr
Average Power Consumption	202 W 689 BTU/hr

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:38:01 (UTC+0000)

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.

Embedded Management Software Support Help About Logout

- EMS
- Properties
- Configuration
- Network
- Network Security
- Security
- Users
- Services
- Time Settings
- Language
- Sessions
- LDAP
- Update
- Utilities
- Fan Profiles
- Server Information
- Sensor Monitor
- Power
- Control
- Consumption
- System Event Log
- Event Management
- Platform Events
- Trap Settings
- Email Settings
- Node Information
- Node Status
- Node MAC Address

System Event Log

Clear Log Save Log Refresh

System Event Count (Current / Maximum) 224 / 1024

Severity	Date/Time	Description
🔴	2018-02-11 14:49:09 (UTC+0000)	CMC Event: HDD10 Drive Slot sensor, Drive Presence was deasserted
🔴	2018-02-11 14:49:11 (UTC+0000)	CMC Event: HDD07 Drive Slot sensor, Drive Presence was deasserted
🔴	2018-02-11 14:49:15 (UTC+0000)	CMC Event: HDD08 Drive Slot sensor, Drive Presence was deasserted
🔴	2018-02-11 14:49:16 (UTC+0000)	CMC Event: HDD09 Drive Slot sensor, Drive Presence was deasserted
🟢	2018-02-11 14:49:32 (UTC+0000)	CMC Event: HDD07 Drive Slot sensor, Drive Presence was asserted
🔴	2018-02-21 09:24:08 (UTC+0000)	CMC Event: PSU2 Power Supply sensor, Power Supply Input lost (AC/DC) was asserted
🔴	2018-02-21 09:37:46 (UTC+0000)	CMC Event: HDD07 Drive Slot sensor, Drive Presence was deasserted
🟢	2018-02-21 09:38:28 (UTC+0000)	CMC Event: HDD14 Drive Slot sensor, Drive Presence was asserted
🔴	2018-02-21 09:38:47 (UTC+0000)	CMC Event: HDD13 Drive Slot sensor, Drive Presence was deasserted
🟢	2018-02-21 09:46:07 (UTC+0000)	CMC Event: HDD13 Drive Slot sensor, Drive Presence was asserted
🟢	2017-11-30 19:52:35 (UTC+0000)	CMC Event: PSU1 Power Supply sensor, Presence detected was asserted
🟢	2017-11-30 19:52:35 (UTC+0000)	CMC Event: HDD13 Drive Slot sensor, Drive Presence was asserted
🟢	2017-11-30 19:52:57 (UTC+0000)	CMC Event: PSU2 Power Supply sensor, Presence detected was asserted
🔴	2017-11-30 19:52:57 (UTC+0000)	CMC Event: PSU2 Power Supply sensor, Power Supply Input lost (AC/DC) was asserted
🟢	2017-11-30 19:52:36 (UTC+0000)	CMC Event: PSU1 Power Supply sensor, Presence detected was asserted
🟢	2017-11-30 19:52:47 (UTC+0000)	CMC Event: PSU2 Power Supply sensor, Presence detected was asserted
🔴	2017-11-30 19:52:47 (UTC+0000)	CMC Event: PSU2 Power Supply sensor, Power Supply Input lost (AC/DC) was asserted
🟢	2017-11-30 19:54:17 (UTC+0000)	CMC Event: HDD19 Drive Slot sensor, Drive Presence was asserted
🔴	2017-12-15 15:02:31 (UTC+0000)	CMC Event: HDD19 Drive Slot sensor, Drive Presence was deasserted
🟢	2017-11-30 19:52:34 (UTC+0000)	CMC Event: PSU1 Power Supply sensor, Presence detected was asserted

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:38:38 (UTC+0000)

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**.

Embedded Management Software Support Help About Logout

EMS

- Properties
 - Configuration
 - Network
 - Network Security
 - Security
 - Users
 - Services
 - Time Settings
 - Language
 - Sessions
 - LDAP
 - Update
 - Utilities
 - Fan Profiles
- Server Information
 - Sensor Monitor
 - Power
 - Control
 - Consumption
 - System Event Log
 - Event Management
 - Platform Events
 - Trap Settings
 - Email Settings
 - Node Information
 - Node Status
 - Node MAC Address

Platform Events

[Apply Changes](#)

Platform Event Filters (PEF) Action Global Control List

Action Name
<input checked="" type="checkbox"/> Power Off
<input checked="" type="checkbox"/> Generate PET

Platform Event Filters (PEF) List

Global Alerting Enable Note: (This enables/disables both PEF and email alerts)

Filter Name	None	Power Off	Generate PET
Threshold Type, Temperature Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Threshold Type, Temperature Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Threshold Type, Voltage Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Threshold Type, Voltage Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Threshold Type, Fan Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Threshold Type, Fan Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Sensor-specific Type, Event Logging Disabled Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Sensor-specific Type, Event Logging Disabled Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Sensor-specific Type, Power Supply Critical Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>
Sensor-specific Type, Power Supply Warning Filter	<input type="radio"/>	<input type="radio"/>	<input type="checkbox"/>

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:39:21 (UTC+0000)

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**.

Embedded Management Software Support Help About Logout

Trap Settings MIB Download Apply Changes

Before sending test trap, please make sure changes to the target Destination and Community String have been saved by clicking Apply Changes.

IP Destination List

Send Test Trap to IPv6 destinations is disabled due to the IPv6's disability of the system.

Destination	Enable	IPv4/IPv6	IP Address	Test
IP Destination 1	<input checked="" type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	10.202.21.122	Send Test Trap
IP Destination 2	<input checked="" type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	192.168.1.190	Send Test Trap
IP Destination 3	<input checked="" type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	10.1.111.132	Send Test Trap
IP Destination 4	<input checked="" type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	10.1.111.78	Send Test Trap
IP Destination 5	<input type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	0.0.0.0	Send Test Trap
IP Destination 6	<input type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	0.0.0.0	Send Test Trap
IP Destination 7	<input type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	0.0.0.0	Send Test Trap
IP Destination 8	<input type="checkbox"/>	<input type="radio"/> <input checked="" type="radio"/>	0.0.0.0	Send Test Trap

Community String

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:40:11 (UTC+0000)

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”.

The screenshot displays the 'Email Settings' configuration page in the Embedded Management Software (EMS) interface. The page is titled 'Email Settings' and includes a navigation menu on the left. The main content area is divided into several sections:

- Sender Information:** A text input field for the 'From' address, currently containing 'EMS@AvetDomain'.
- Destination Email Addresses:** A table with four rows, each representing an email alert. Each row has columns for 'Enable', 'Destination Email Address', 'Email Description', and 'Test'.
- SMTP (email) Server Settings:** A table with two rows: 'SMTP IP Address' (0.0.0.0) and 'SMTP Port Number' (25).

The 'Apply Changes' button is located in the top right corner of the configuration area. A warning message at the top of the main content area states: 'Before sending alert, please make sure changes to Sender Information, target Destination Email Address, SMTP (email) Server Settings, and SMTP Authentication have been saved by clicking Apply Changes.'

The footer of the page displays the message: 'Welcome admin (Administrator) ! Thu Apr 12 2018, 10:40:41 (UTC+0000)'.

Node Information

Node Status

This page displays the technical specifications of the connected node.

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

Embedded Management Software Support Help About Logout

- EMS
- Properties
 - Configuration
 - Network
 - Network Security
 - Security
 - Users
 - Services
 - Time Settings
 - Language
 - Sessions
 - LDAP
 - Update
 - Utilities
 - Fan Profiles
- Server Information
 - Sensor Monitor
 - Power
 - Control
 - Consumption
 - System Event Log
 - Event Management
 - Platform Events
 - Trap Settings
 - Email Settings
- Node Information
 - Node Status
 - Node MAC Address

Node Information

[Refresh](#)

Node Status

ID	Model	DC	Node	CPU	DIMM	T1	T2	Healthy	Version
Node01B	ZU4N	ON	144 Watts	61 Watts	1 Watts	59 °C	N/A	NO ALERT	1.48

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:42:12 (UTC+0000)

Node MAC Address

This page displays the connected node MAC address information.

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

Embedded Management Software Support Help About Logout

- EMS
 - Properties
 - Configuration
 - Network
 - Network Security
 - Security
 - Users
 - Services
 - Time Settings
 - Language
 - Sessions
 - LDAP
 - Update
 - Utilities
 - Fan Profiles
 - Server Information
 - Sensor Monitor
 - Power
 - Control
 - Consumption
 - System Event Log
 - Event Management
 - Platform Events
 - Trap Settings
 - Email Settings
 - Node Information
 - Node Status
 - Node MAC Address

Node Information

[Refresh](#)

Node MAC Address

ID	Model	BMC MAC Address	LAN1 MAC Address	LAN2 MAC Address	BMC IPv4 Address	BMC IPv6 Address
Node01B	ZU4N	e0d55e1e7b1c	e0d55e1e7b1a	e0d55e1e7b1b	10.1.111.119	1999::11

Welcome admin (Administrator) ! Thu Apr 12 2018, 10:42:44 (UTC+0000)