AST2300 iBMC
Configuration Guide

Version 1.0a

Notice
Information contained in this document is furnished by MiTAC International Corporation and has been reviewed for accuracy and reliability prior to printing. MiTAC assumes no liability whatsoever, and disclaims any express or implied warranty, relating to sale and/or use of TYAN® products including liability or warranties relating to fitness for a particular purpose or merchantability. MiTAC retains the right to make changes to product descriptions and/or specifications at any time, without notice. In no event will MiTAC be held liable for any direct or indirect, incidental or consequential damage, loss of use, loss of data or other malady resulting from errors or inaccuracies of information contained in this document.

Contents

1. IPMI OS Drivers and Open Source Software

AST2300 firmware is full compliant with IPMI 2.0 specification. So users could use standard IPMI driver comes from operation system distribution.

1.1 Windows IPMI Driver

AST2300 supports Intel reference driver, you can get it from

http://www.intel.com/design/servers/ipmi/tools.htm

From Windows Server 2003 R2, Microsoft also provide in box IPMI driver. You can use it also.

1.2 Open IPMI Driver on Linux

AST2300 supports the Open IPMI driver in Linux Kernel. Use the following commands to load IPMI drivers.

“modprobe ipmi_devintf”

“modprobe ipmi_si”

If you use old version Linux Kernel, you need to replace module “ipmi_si” with “ipmi_kcs”

Note that TYAN motherboard BIOS encodes IPMI Base IO address at 0xCA2 in its DMI table IPMI entry, any generic OS IPMI drivers should have no problem to support it.

1.3 IPMI Tool and Other Open Source Software

AST2300 supports open source software IPMI Tool, you can also use other ones like Open IPMI, IPMI Utility. Note that for IPMI Tool SOL session, user needs to use BIOS setup menu to configure “Remote Serial Console Redirect” to use COMA, and set baud rate to 38.4K, 8 bits, no parity, and Xon/Xoff handshaking.

NOTE

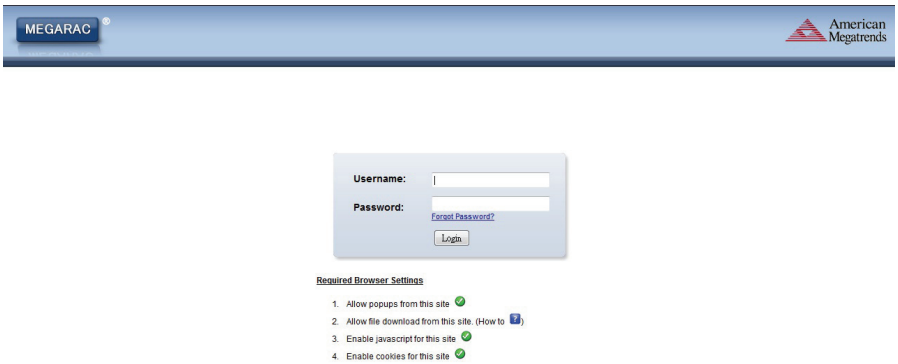
2. SP-X WEB GUI

2.1 MegaRAC® GUI Overview

The MegaRAC® SP-X SoC (System-on-Chips) has an AMI generic, user-friendly Graphics User Interface (GUI) called the **MegaRAC® 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.

2.2 User Name and Password

Initial access of MegaRAC SP-X prompts you to enter the User Name and Password. A screenshot of the login screen is given below.



Default User Name and Password

The default user name and password are as follows:

Username: root

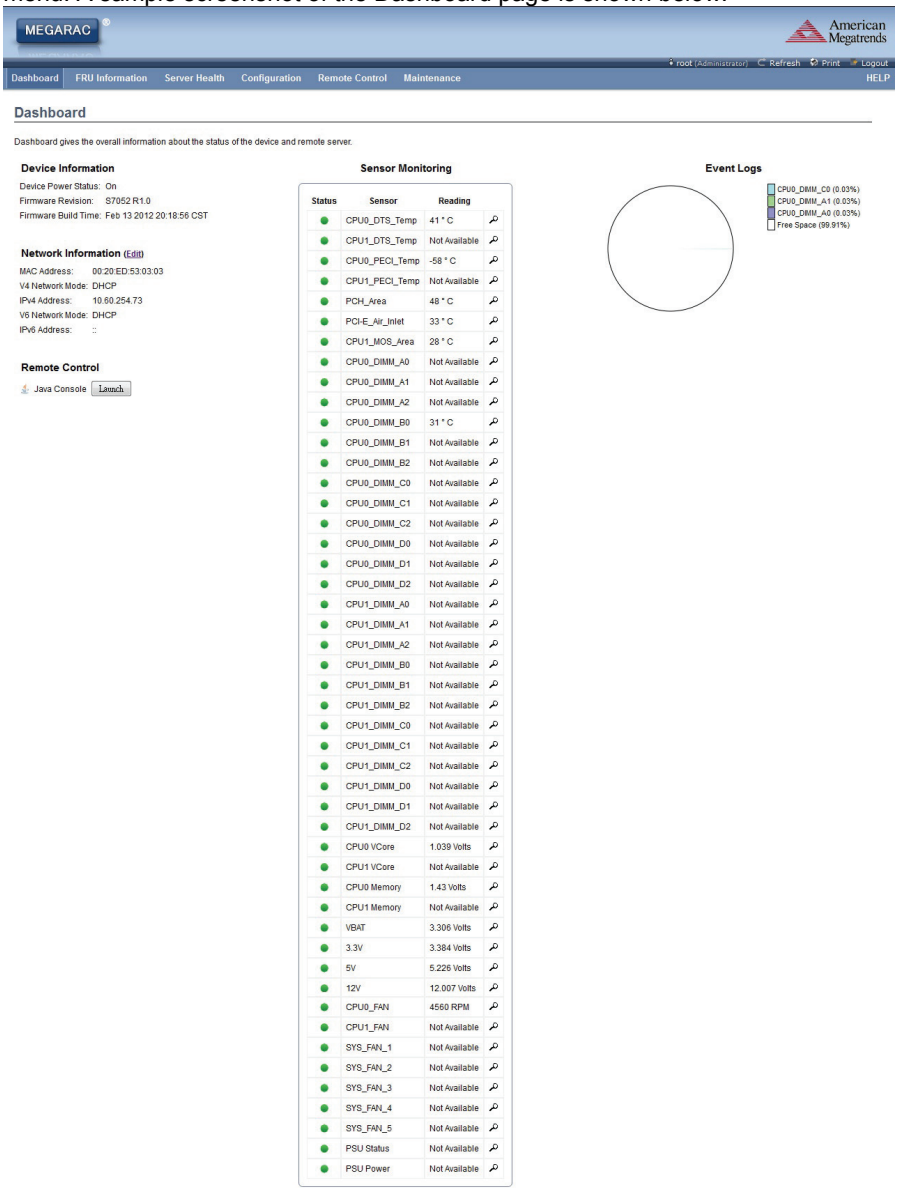
Password: superuser

NOTE:

- The default user name and password are in lower-case characters.
- When you log in using the user name and password, you get full administrative rights. It is advised to change your password once you login.

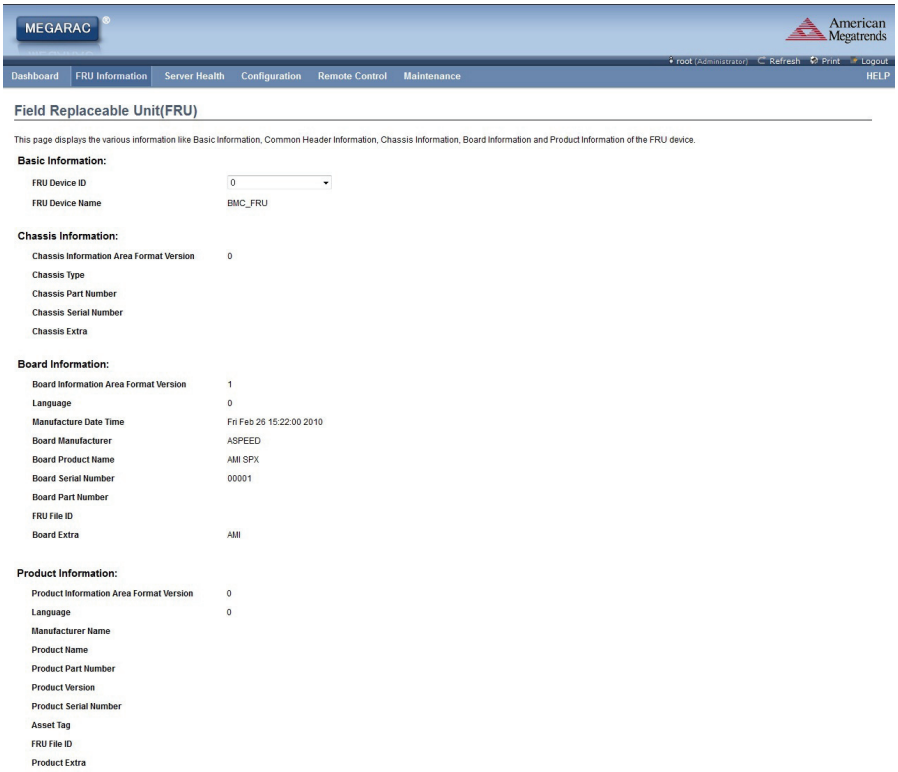
2.3 Dashboard

In MegaRAC GUI, the Dashboard page gives the overall information about the status of a device. To open the Dashboard page, click **Dashboard** from the main menu. A sample screenshot of the Dashboard page is shown below.



2.4 FRU Information

In MegaRAC GUI, the FRU Information Page displays the BMC FRU file information. The information displayed in this page is Basic Information, Common Header Information, Chassis Information, Board Information and Product Information of the FRU device.
To open the FRU Information, click **FRU Information** from the top menu. Select a FRU Device ID from the Basic Information section to view the details of the selected device. A screenshot of FRU Information Page is given below.

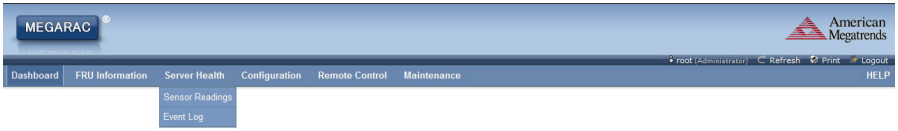


2.5 Server Health Group

The Server Health Group consists of two items.

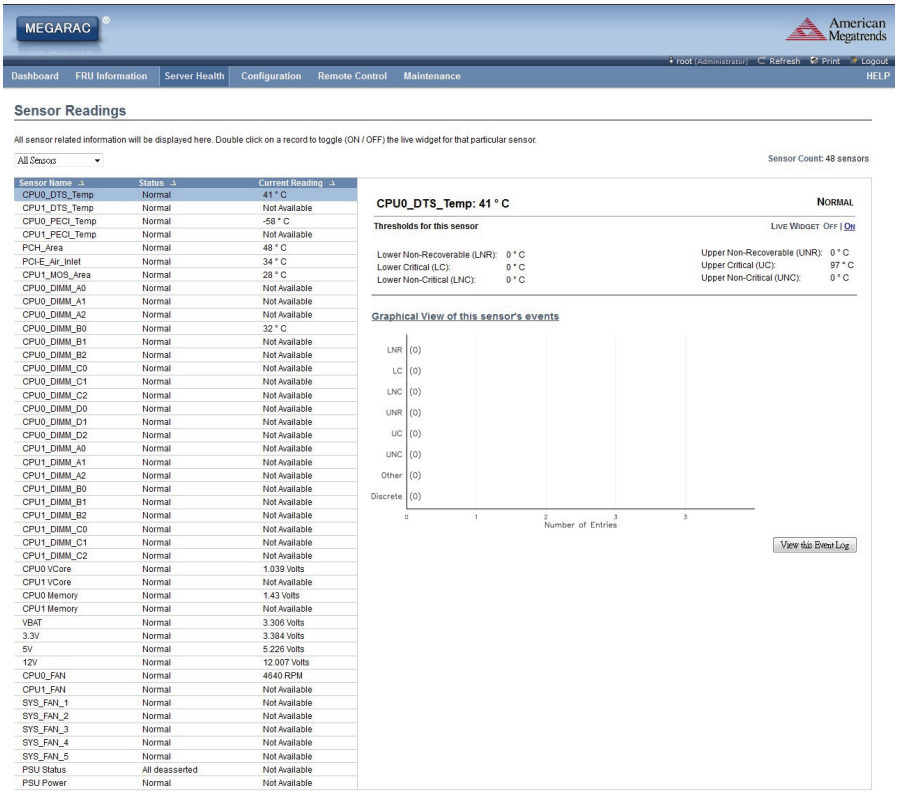
- Sensor Readings
- Event Log

A screenshot displaying the menu items under the Server Health is shown below.



2.5.1 Sensor Readings

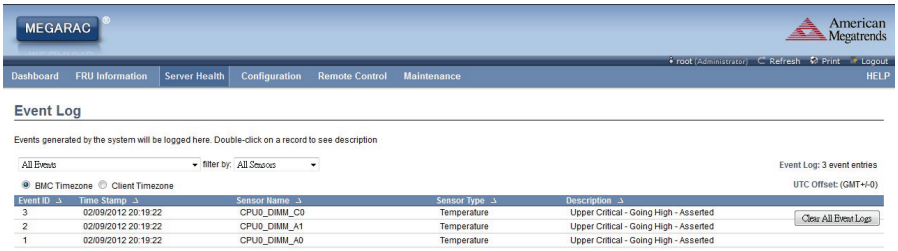
In MegaRAC GUI, the Sensor Readings Page displays all the sensor related information.
To open the Sensor Readings Page, click **Server Health → Sensor Readings** from the top menu. Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Readings Page is given below.



2.5.2 Event Log

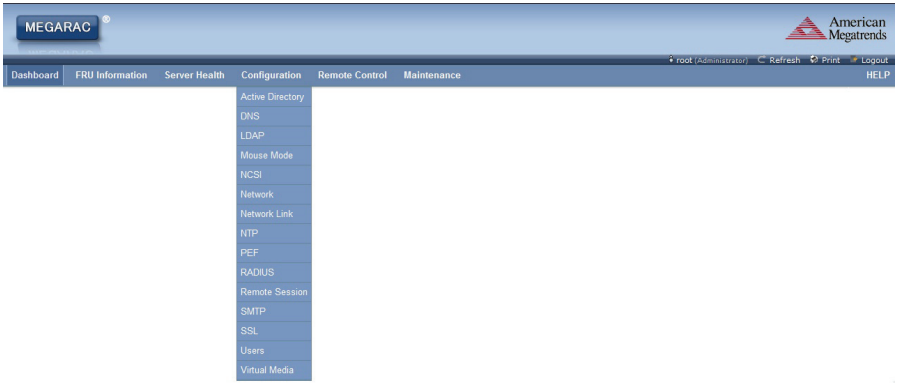
In MegaRAC GUI, this page displays the list of event logs occurred by the different sensors on this device. Double click on a record to see the details of that entry. You can use the sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click **Server Health → Event Log** from the top menu. A sample screenshot of Event Log Page is shown below.



2.6 Configuration Group

This group of pages allows you to access various configuration settings. A detailed description of each configuration group is given ahead. A screenshot of Configuration Group Page is shown below.

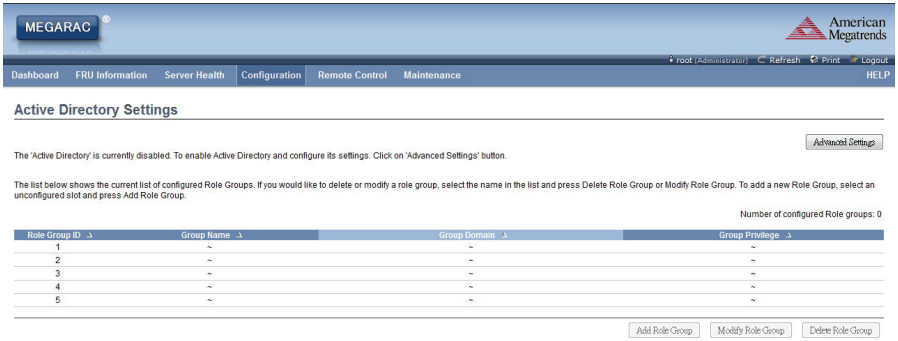


2.6.1 Active Directory

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. An active directory (sometimes referred to as an AD) does a variety of functions including the ability to provide information on objects, helps organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.

This page allows you to configure Active Directory Server Settings.

To open the Active Directory Settings Page, click **Configuration → Active Directory** from the main menu. A sample screenshot of Active Directory Settings Page is shown in the screenshot below.

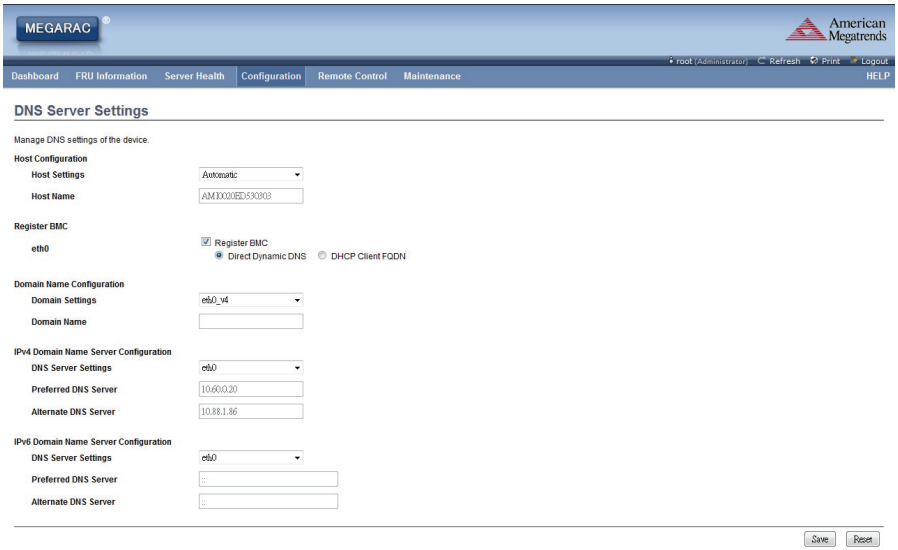


2.6.2 DNS

The **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

In MegaRAC GUI, the DNS Server Settings page is used to manage the DNS settings of a device.

To open the DNS Server Settings Page, click **Configuration → DNS** from the main menu. A sample screenshot of DNS Server Settings Page is sown in the screenshot below.



2.6.3 LDAP

The **Lightweight Directory Access Protocol (LDAP**) is an application protocol for querying and modifying data of directory services implemented in internet Protocol (IP) networks.

To open the LDAP Settings Page, click **Configuration → LDAP** from the main menu. A sample screenshot of LDAP Settings Page is shown in the screenshot below.

2.6.4 Mouse Mode

In MegaRAC GUI, Redirection Console handles mouse emulation from local window to remote screen in either of two methods. User has to be an Administrator to configure this option.

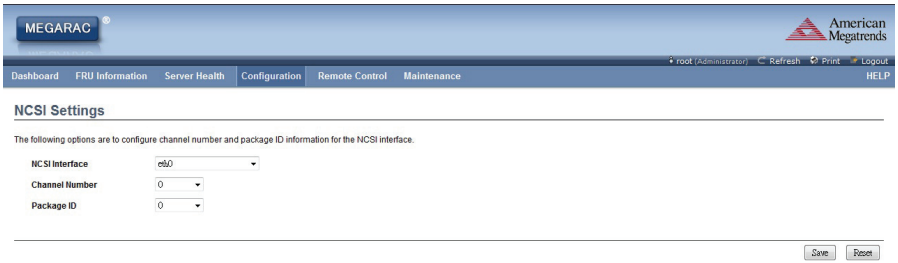
To open the Mouse Mode Page, click **Configuration → Mouse Mode** from the main menu. A sample screenshot of Mouse Mode Settings page is shown in the screenshot below.

Note: When server OS is Redhat 6.x, please select the absolute mouse mode

2.6.5 NCSI

In MegaRAC GUI, this page is used to configure Network Controller Sideband Interface (NCSI) configuration settings.

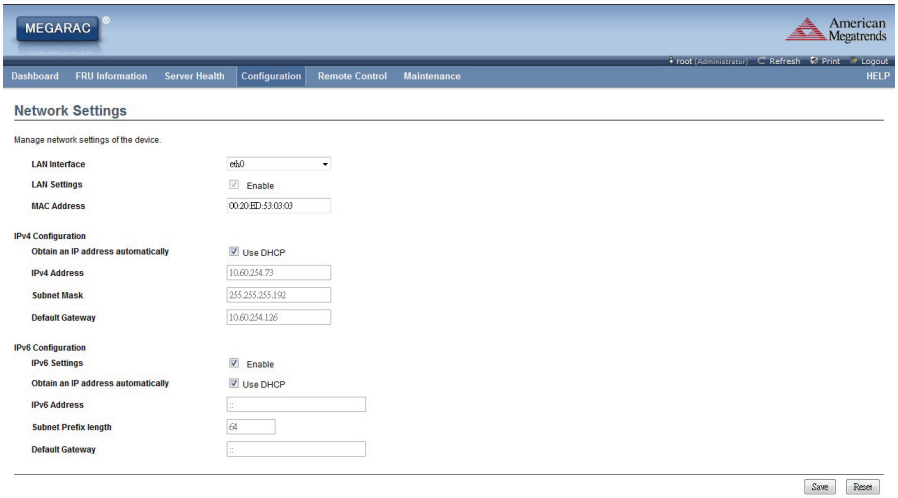
To open the NCSI Page, click **Configuration → NCSI** from the main menu. A sample screenshot of NCSI Settings Page is shown in the screenshot below.



2.6.6 Network

In MegaRAC GUI, the Network Settings Page is used to configure the network settings for the available LAN channels.

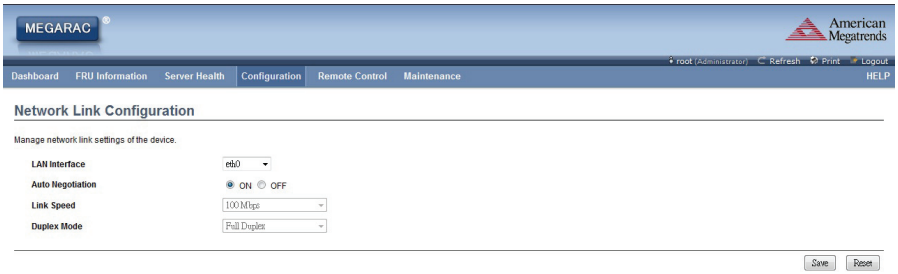
To open the Network Settings Page, click **Configuration → Network** from the main menu. A sample screenshot of Network Settings Page is shown in the screenshot below.



2.6.7 Network Link

In MegaRAC GUI, this page is used to configure network link configuration for available network interfaces.

To open the Network Link Page, click **Configuration → Network Link** from the main menu. A sample screenshot of Network Link Configuration Page is shown in the screenshot below.

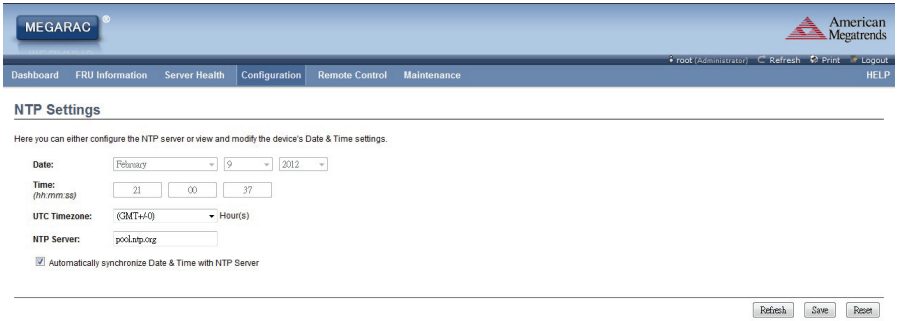


2.6.8 NTP Settings

The **Network Time Protocol (NTP)** is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is designed particularly to resist the effects of variable latency by using a jitter buffer.

In MegaRAC GUI, this page displays the device current date and time settings. It can be used to configure either Data & Time or NTP server settings for the device.

To open the NTP Settings Page, click **Configuration → NTP** from the main menu. A sample screenshot of NTP Settings Page is shown in the screenshot below.



2.6.9 PEF

Platform Event Filtering (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that is receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

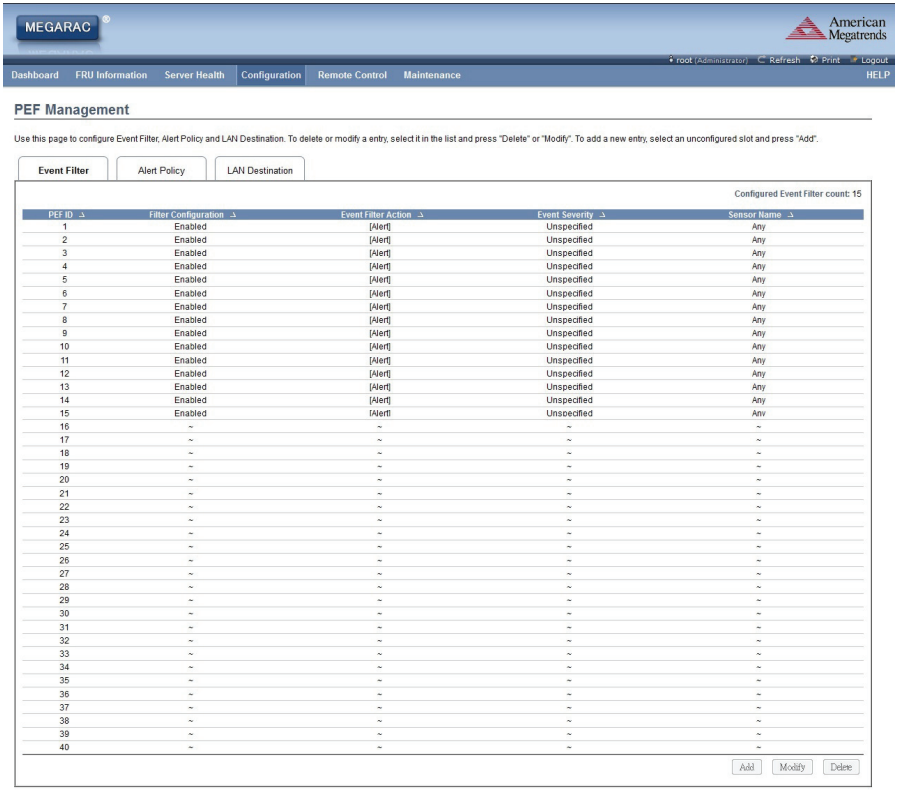
In MegaRAC GUI, the PEF Management is used to configure the following:

- Event Filter
- Alert Policy
- LAN Destination

To open the PEF Management Settings Page, click **Configuration → PEF** from the main menu. A sample screenshot of PEF Management Page is shown in the screenshot below.

Event Filter Table

A PEF implementation is recommended to provide at least 16 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use - so this ratio of pre-configured entries to run-time configurable entries can be reallocated if necessary.



The fields of PEF Management – Event Filter Tab are explained below.

This page contains the list of configured PEF's.

PEF ID: This field displays the ID for the newly configured PEF entry (readonly).

Filter configuration: Check box to enable the PEF settings.

Event Filter Action: Check box to enable PEF Alert action. This is a mandatory field.

Event Severity: To choose any one of the Event severity from the list.

Sensor Name: To choose the particular sensor from the sensor list.

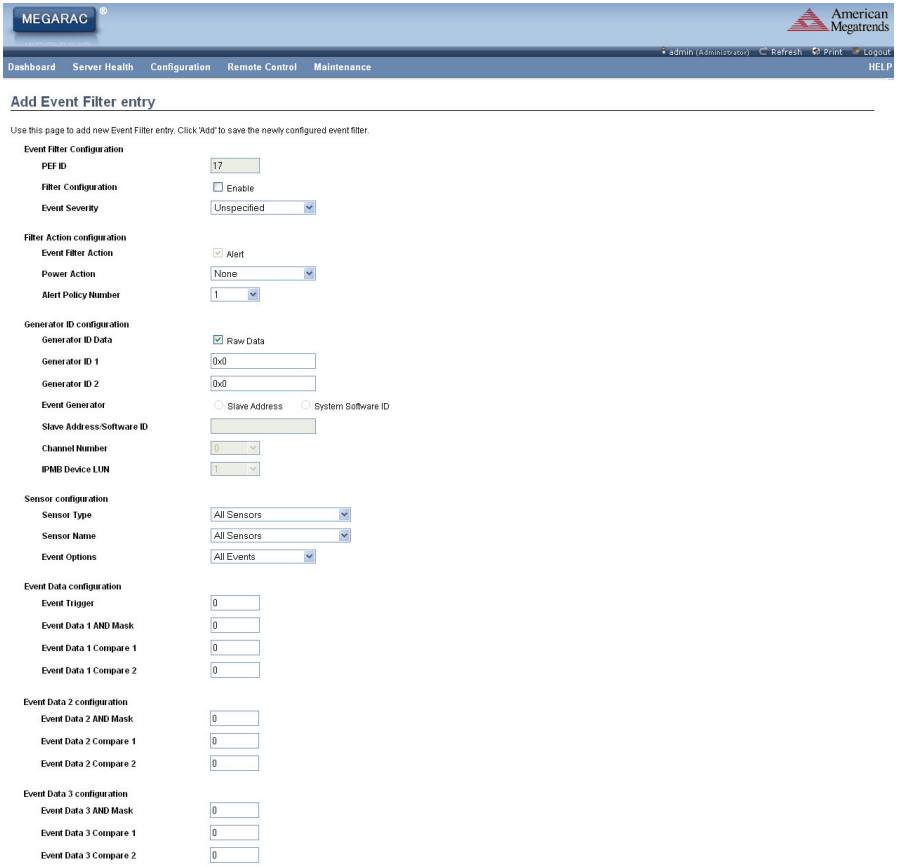
Add: To add the new event filter entry and return to Event filter list.

Modify: To modify the existing entries.

Cancel: To cancel the modification and return to Event filter list.

Procedure:

1. Click the **Event Filter** Tab to configure the event filters in the available slots
2. To Add an Event Filter entry, select a free slot and click **Add** to open the Add event Filter entry Page. A sample screenshot of Add Event Filter Page is seen in the screenshot below.



3. In the Event Filter Configuration section,
   - PEF ID displays the ID for configured PEF entry (read-only).
   - In filter configuration, check the box to enable the PEF settings.
   - In Event Severity, select any one of the Event severity from the list.

4. In the Filter Action configuration section,
   - Event Filter Action is a mandatory field and checked by default, which enable PEF Alert action (read-only).
   - Select any one of the Power action either Power down, Power reset or Power cycle from the drop down list
   - Choose any one of the configured alert policy number from the drop down list.

   NOTE: Alert Policy has to be configured - under Configuration → PEF → Alert Policy.

5. In the Generator ID configuration section,
   - Check Generator ID Data option to fill the Generator ID with raw data.
   - Generator ID 1 field is used to give raw generator ID1 data value.
   - Generator ID 2 field is used to give raw generator ID2 data value.

   NOTE: In RAW data field, to specify hexadecimal value prefix with '0x'.

   - In the Event Generator section, choose the event generator as Slave Address - if event was generated from IPMB. Otherwise as System Software ID - if event was generated from system software.
   - In the Slave Address/Software ID field, specify corresponding I^2C Slave Address or System Software ID.
   - Choose the particular channel number that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
   - Choose the corresponding IPMB device LUN if event generated by IPMB.

6. In the Sensor configuration section,
   - Select the s type of sensor that will trigger the event filter action.
   - In the sensor name field, choose the particular sensor from the sensor list.
   - Choose event option to be either All Events or Sensor Specific Events.

7. In the Event Data configuration section,
   - Event Trigger field is used to give Event/Reading type value.

   NOTE: Value ranges from 1 to 255.

   - Event Data 1 AND Mask field is used to indicate wildcarded or compared bits.

   NOTE: Value ranges from 0 to 255.

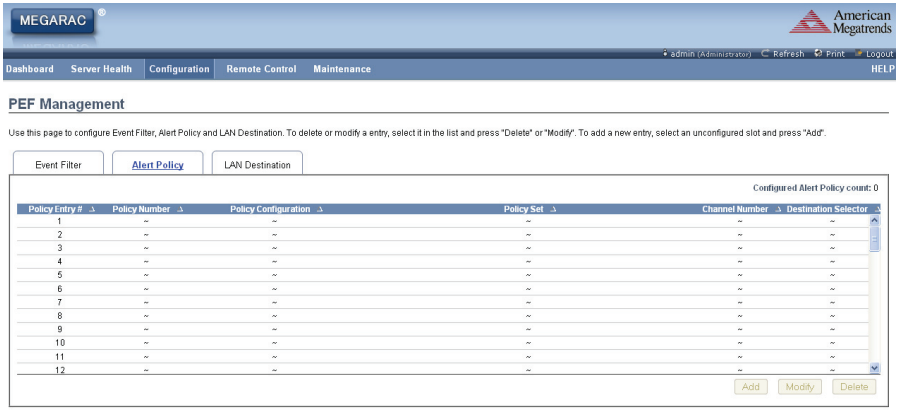
   - Event Data 1 Compare 1 & Event Data 1 Compare 2 field is used to indicate whether each bit position's comparison is an exact comparison or not.

NOTE: Value ranges from 0 to 255.

8. In the Event Data 2 configuration section,
   - Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.
   - Event Data 2 Compare 1 & Event Data 2 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
9. In the Event Data 3 configuration section,
   - Event Data 3 AND Mask field is similar to Event Data 1 AND Mask.
   - Event Data 3 Compare 1 & Event Data 3 Compare 2 fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
10. Click **Modify** to accept the modification and return to Event filter list.
11. Click **Reset** to reset the modification done.
12. Click on **Cancel** to cancel the modification and return to Event filter list.
13. In the Event filter list, click **Modify** to modify the existing filter.
14. In the Event filter list, click **Delete** to delete the existing filter.

Alert Policy Tab

This page is used to configure the Alert Policy and LAN destination. You can add, delete or modify an entry in this page.



PEF Management – Alert Policy

The fields of PEF Management – Alert Policy Tab are explained below.

Policy Entry #: Displays Policy entry number for the newly configured entry (read-only).

Policy Number: Displays the Policy number of the configuration.

Policy Configuration: To enable or disable the policy settings.

Policy Set: To choose any one of the Policy set values from the list.

0 - Always send alert to this destination.
1 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.
2 - If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.
3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.
4 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.

Channel Number: To choose a particular channel from the available channel list.

Destination Selector: To choose a particular destination from the configured destination list.

NOTE: LAN Destination has to be configured - under **Configuration → PEF → LAN Destination**.

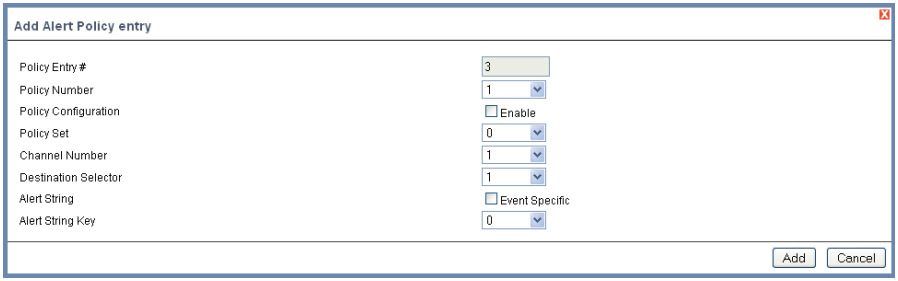
Add: To save the new alert policy and return to Alert Policy list.

Modify: To modify the existing entries.

Cancel: To cancel the modification and return to Alert Policy list.

Procedure:

1. In the Alert Policy Tab, select the slot for which you have to configure the Alert policy. That is, In the **Event Filter Entry Page,** if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click **Add** to open the **Add Alert Policy Entry Page** as shown in the screenshot below.



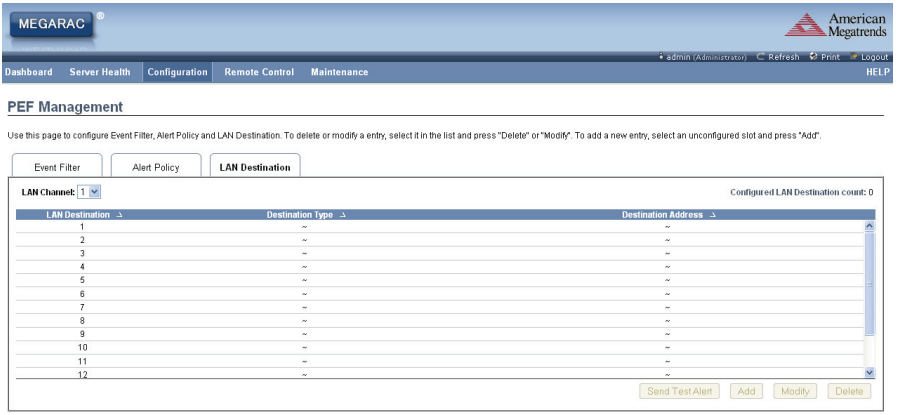
3. **Policy Entry #** is a read only field.
4. Select the **Policy Number** from the list.
5. In the **Policy Configuration** field, check **Enable** if you wish to enable the policy settings.
6. In the **Policy Set** field, choose any of the Policy set from the list.
7. In the **Channel Number field**, choose particular channel from the available channel list.
8. In the **Destination Selector field**, choose particular destination from the configured destination list.

   NOTE: LAN Destination has to be configured under **Configuration → PEF → LAN Destination**. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destination tab.

9. In the **Alert String** field, enable the check box if the Alert policy entry is Event Specific.
10. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.
11. Click **Add** to save the new alert policy and return to Alert Policy list.
12. Click **Cancel** to cancel the modification and return to Alert Policy list.
13. In the Alert Policy list, to modify a configuration, select the slot to be modified and click **Modify.**
14. In the **Modify Alert Policy Entry Page**, make the necessary changes and click **Modify**.
15. In the Alert Policy list, to delete a configuration, select the slot and click **Delete**.

PEF Management LAN Destination Page

This page is used to configure the Event filter, Alert Policy and LAN destination. A sample screenshot of PEF Management LAN Destination Page is given below.



PEF Management LAN Destination

The fields of PEF Management – LAN Destination Tab are explained below.

LAN Destination: Displays Destination number for the newly configured entry (read only).

Destination Type: Destination type can be either an SNMP Trap or an Email alert. For Email alerts, the 3 fields - destination Email address, subject and body of the message needs to be filled. The SMTP server information also has to be added - under Configuration->SMTP. For SNMP Trap, only the destination IP address has to be filled.

Destination Address: If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format
- IPv6 address format

If Destination type is Email Alert, then give the email address that will receive the email.

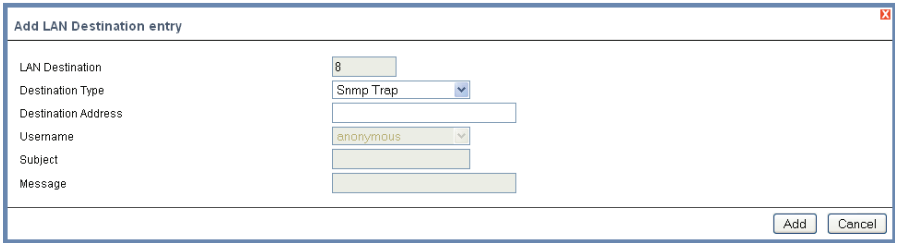
Subject & Message: These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address in case of any severity events with a subject specified in subject field and will contain the message field's content as the email body.

Add: To save the new LAN destination and return to LAN destination list.

Cancel: To cancel the modification and return to LAN destination list.

Procedure:

1. In the **LAN Destination Tab**, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of Alert Policy Tab, then you have to configure the 4th slot of LAN Destination Page.
2. Select the slot and click **Add**. This opens the **Add LAN Destination entry.**



Add LAN Destination Entry Page

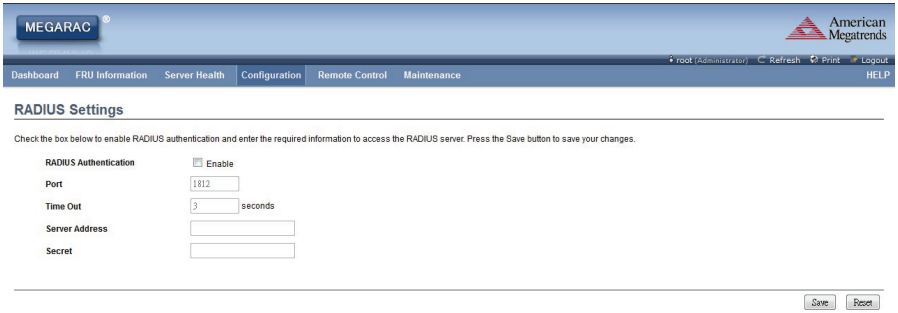
3. In the **LAN Destination** field, the destination for the newly configured entry is displayed and this is a read only field.
4. In the **Destination Type** field, select the one of the types.
5. In the **Destination Address** field, enter the destination address.
   NOTE: If Destination type is Email Alert, then give the email address that will receive the email.
6. Select the **User Name** from the list of users.
7. In the **Subject** field, enter the subject.
8. In the **Message** field, enter the message.
9. Click **Add** to save the new LAN destination and return to LAN destination list.
10. Click **Cancel** to cancel the modification and return to LAN destination list.
11. In the LAN Destination Tab, to modify a configuration, select the row to be modified and click **Modify**.
12. In the **Modify LAN Destination Entry** page, make the necessary changes and click **Modify**.
13. In the LAN Destination Tab, to delete a configuration, select the slot and click **Delete**.

2.6.10 RADIUS

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

In MegaRAC GUI, this page is used to set the RADIUS Authentication.

To open the RADIUS Settings Page, click **Configuration → RADIUS** from the main menu. A sample screenshot of RADIUS Settings Page is shown in the screenshot below.



RADIUS Settings Page

The fields of RADIUS Settings Page are explained below.

RADIUS Authentication: Option to enable RADIUS authentication.

Port: The RADIUS Port number.

Note:

- Default Port is 1812.

Time Out: The Time out value in seconds.

Note:

- Default Timeout value is 3seconds.
- Timeout value ranges from 3 to 300.

Server Address: The IP address of RADIUS server.

Note:

- IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".

- Each Number ranges from 0 to 255.
- First Number must not be 0.

Secret: The Authentication Secret for RADIUS server.

Note:

-This field will not allow more than 31 characters.
- Secret must be at least 4 characters long.
- White space is not allowed.

Save: To save the settings.

Reset: To reset the modified changes.

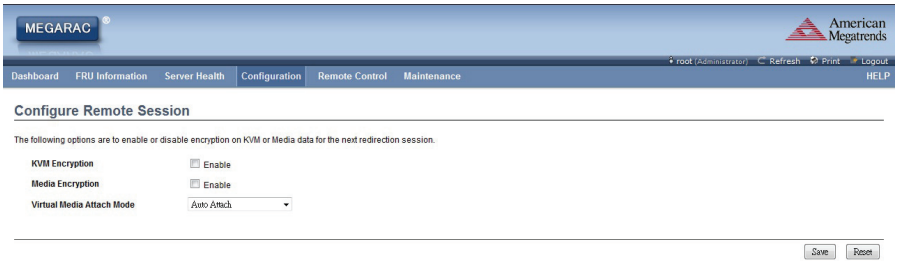
Procedure

1. Enable the **RADIUS Authentication** checkbox to authenticate the RADIUS.
2. Enter the port number in the **Port Number** field.
3. Enter the time out value in seconds in the **Time out** field.
4. Enter the address of the server in the **Server Address** field.
5. Enter the authentication secret for RADIUS Server in the **Secret** field.
6. Click **Save** to save the entered details.
7. Click **Reset** to reset the entered details.

2.6.11 Remote Session

In MegaRAC GUI, use this page to configure virtual media configuration settings for the next redirection session. Encryption is disabled by default.

To open the Configure Remote Session Page, click **Configuration → Remote Session** from the main menu. A sample screenshot of Configure Remote Session Page is shown in the screenshot below.

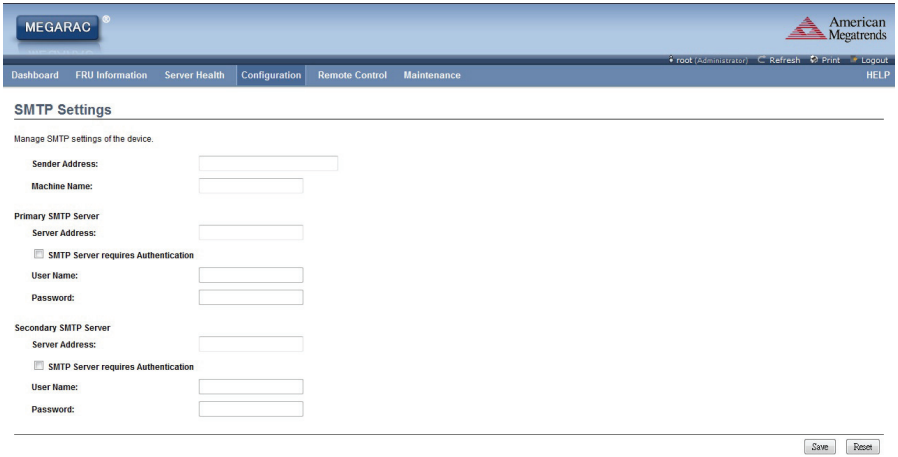


2.6.12 SMTP

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.

Using the MegaRAC GUI, you can configure the SMTP settings of the device.

To open the SMTP Settings Page, click **Configuration → SMTP** from the main menu. A sample screenshot of SMTP Settings Page is shown in the screenshot below.



SMTP Settings Page

SMTP Server IP: The IP address of the SMTP Server.

Note:

- IPv4 Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- IPv6 Address made of 8 numbers separated by colon ":" or double colon "::". Eg: 2004::2010
- Each field ranges from 0 to FFFF.

Sender Address: The email address of the sender valid on the SMTP Server.

Machine Name: Name of the SMTP Server.

- Machine Name is a string of maximum 15 alpha-numeric characters.
- Space and special characters are not allowed.

SMTP Server requires Authentication: Option to enable SMTP Authentication.

Note: Server Authentication Types supported are:
- CRAM-MD5
- LOGIN
- PLAIN

If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, "Authentication type is not supported by SMTP Server"

Username: Username using which you wish to access SMTP Accounts.

Note:
- User Name can be of length 4 to 15 alpha-numeric characters.
- It must start with an alphabet.
- Special characters ','(comma), ':'(colon), ';'(semicolon), ' '(space) and '\'(backslash) are not allowed.

Password: Password for the SMTP User Account.

Note: This field will not allow more than 19 characters.
- Password must be at least 4 characters long.
- White space is not allowed.

Save: To save the entries.

Reset: To reset the entries.

Procedure

1. Enter the SMTP Server IP in the field given.
2. Enter your email address in the Sender Address field.
3. Enter the IPMI machine name in the Machine Name field.
4. Enable the check box SMTP Server requires Authentication if you want to authenticate SMTP Server.
5. Enter your User name in the given field.
6. Enter your Password in the given field.
7. Click Save to save the entered details.
8. Click Reset to update the entered details.

2.6.13 SSL

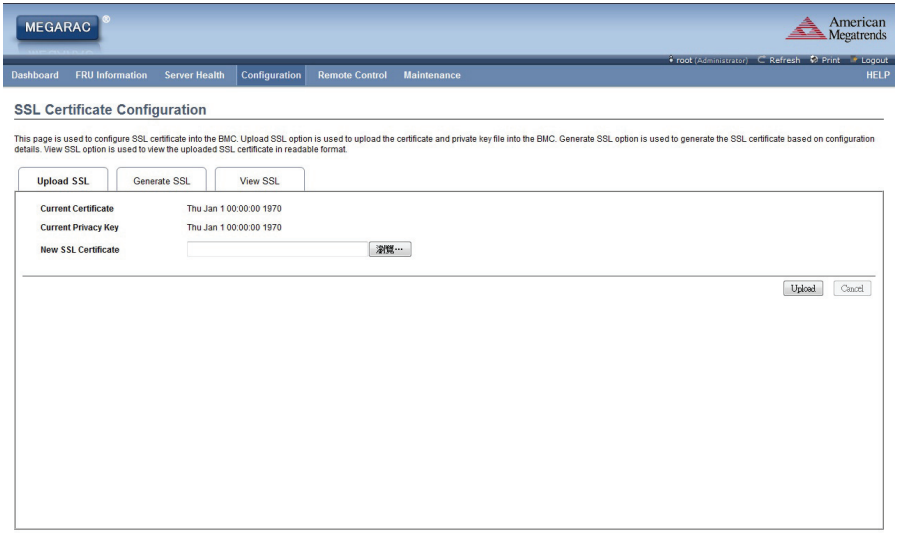
The **Secure Socket Layer (SSL)** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

Using the MegaRAC GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open the SSL Certificate Configuration Page, click **Configuration → SSL** from the main menu. There are three tabs in this page.

- **Upload SSL** option is used to upload the certificate and private key file into the BMC.
- **Generate SSL** option is used to generate the SSL certificate based on configuration details.
- **View SSL** option is used to view the uploaded SSL certificate in readable format.

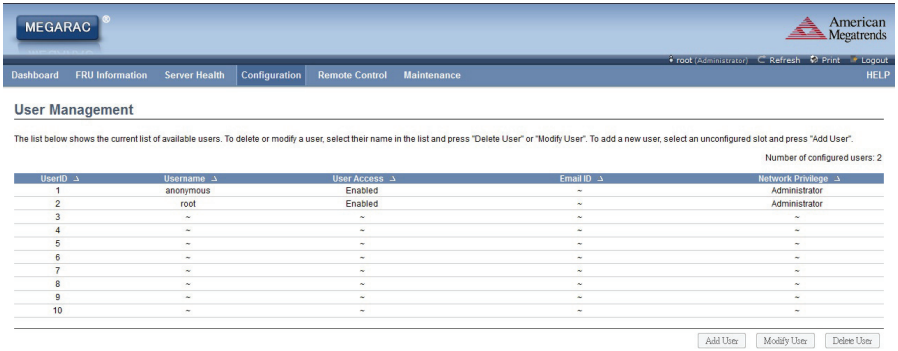
A sample screenshot of SSL Certificate Configuration Page is shown in the screenshot below.



2.6.14 User Management

In MegaRAC GUI, the User Management Page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open the User Management Page, click **Configuration → Users** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.



User Management

The fields of User Management Page are explained below.

User ID: Displays the ID number of the user.
Note: The list contains a maximum of ten users only.

User Name: Displays the name of the user.

Email ID: Displays email address of the user.

Network Privilege: Displays the network access privilege of the user.

Add User: To add a new user.

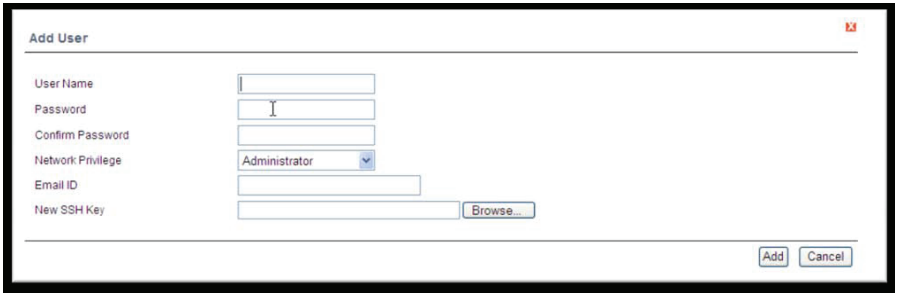
Modify User: To modify an existing user.

Delete User: To delete an existing user
Note: The Free slots are denoted by "~" in all columns for the slot.

Procedure

Add a new user:

1. To add a new user, select a free slot and click **Add User**. This opens the Add User screen as shown in the screenshot below.



Add User Page

2. Enter the name of the user in the **User Name** field.
   Note:
   - User Name is a string of 4 to 16 alpha-numeric characters.
   - It must start with an alphabetical character.
   - It is case-sensitive.
   - Special characters ','(comma), '.'(period), ':'(colon), ';'(semicolon), ' '(space), '/'(slash), '\'(backslash), '('(left bracket) and ')'(right bracket) are not allowed.

3. In the **Password** and **Confirm Password** fields, enter and confirm your new password.

4. Note:
   - Password must be at least 8 characters long.
   - White space is not allowed.
   - This field will not allow more than 20 characters.

5. In the **Network Privilege** field, enter the network privilege assigned to the user which could be Administrator, Operator, User or No Access.

6. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.
   Note: SMTP Server must be configured to send emails.

7. In the **New SSK Key** field, click Browse and select the SSH key file
   Note: SSH key file should be of pub type.

8. Click **Add** to save the new user and return to the users list.

9. Click **Cancel** to cancel the modification and return to the users list.

Modify an existing User

10. Select an existing user from the list and click **Modify User**. This opens the Add User screen as shown in the screenshot below.

Modify User Page

11. Edit the required fields.
12. To change the password, enable the **Change Password** option.
13. After editing the changes, click **Modify** to return to the users list page.

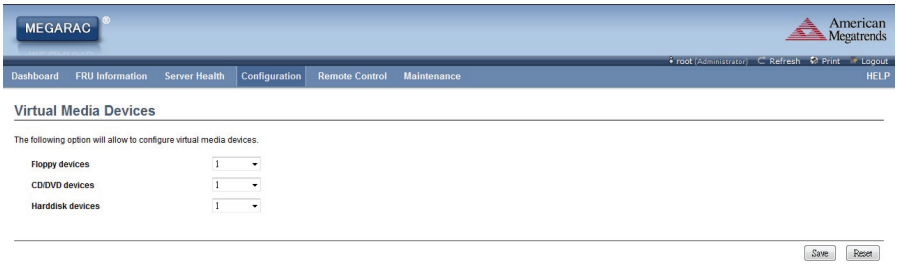
Delete an existing User

14. To delete an existing user, select the user from the list and click **Delete User**.

2.6.15 Virtual Media

In MegaRAC GUI, this page is used to configure Virtual Media Devices settings. If you change the configuration of the Virtual Media Devices in this page, it show the appropriate device in the JViewer Vmedia dialog. For example, if you select two floppy devices in Configure Virtual Media Page, then in JViewer Vmedia, you can view two floppy device panel.

To open the Virtual Media Devices Page, click **Configuration → Virtual Media** from the main menu. A sample screenshot of Virtual Media Devices Page is shown in the screenshot below.



2.7 Remote Control

The Remote Control consists of the following menu items.

- Console Redirection
- Server Power Control
- Other Control

A sample screenshot of the Remote Control menu is given below.

2.7.1 Console Redirection

The remote console application, which is started using the WebGUI, allows you to control your server's operating system remotely, using the screen, mouse, and keyboard, and to redirect local CD/DVD, Floppy diskette and hard disk/USB thumb drives as if they were connected directly to the server.

List of Supported Client Operating System

winxp
w2k3 - 32 bit
w2k3 - 64 bit
RHEL 4 - 32 bit
RHEL 4 - 64 bit
RHEL 5.4 - 32 bit
RHEL 5.4 - 64 bit
RHEL 6.0 - 64 bit
RHEL 6.0 - 32 bit
Ubuntu 9.10 LTS - 32
Ubuntu 9.10 LTS - 64
Ubuntu 8.10 -32
Ubuntu 8.10 -64
OpenSuse 11.2 -32
OpenSuse 11.2 -64
FC 9 - 32
FC 9 - 64
FC 10 - 32
FC 10 - 64
FC 12 - 32
FC 12 - 64
FC 13 - 32
FC 13 – 64
FC 14 - 32
FC 14 - 64
MAC -32
MAC-64

List of Supported Host OS

RHEL 5
RHEL 6
w2k3
w2k8
RHEL 4
OpenSuse 11.2
OpenSuse 10.x
Ubuntu 8.10
Ubuntu 9.10
Ubuntu 11.04

Browser Settings
For launching the KVM, pop-up block should be disabled. For Internet Explorer, enable the download file options from the settings.

Java Console
This is an OS independent plug-in which can be used in Windows as well as Linux with the help of JRE. JRE should be installed in the client's system. You can install JRE from the following link.
http://www.java.com/en/download/manual.jsp

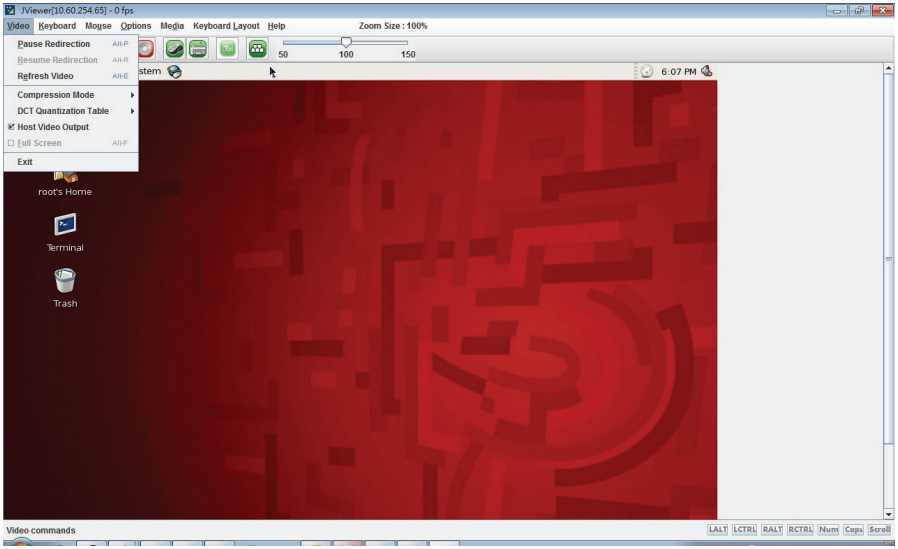
The Console Redirection main menu consists of the following menu items.

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout

A detailed explanation of these menu items are given below.

2.7.1.1 Video

This menu contains the following sub menu items.
Pause redirection: This option is used for pausing Console Redirection.
Resume Redirection: This option is used to resume the Console Redirection when the session is paused.
Refresh Video: This option can be used to update the display shown in the Console Redirection window.
Turn Off Host display: If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.
Full Screen: This option is used to view the Console Redirection in full screen mode (Maximize). This menu is enabled only when both the client and host resolution are same.
Exit: This option is used to exit the console redirection screen



2.7.1.2 Keyboard

This menu contains the following sub menu items.

Hold Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.

Hold Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

Hold Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

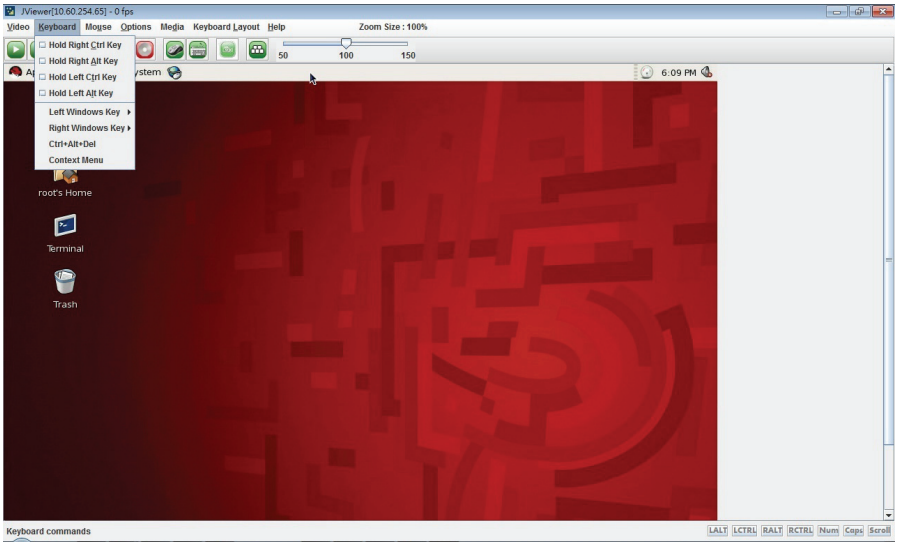
Hold Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Alt+Ctrl+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.

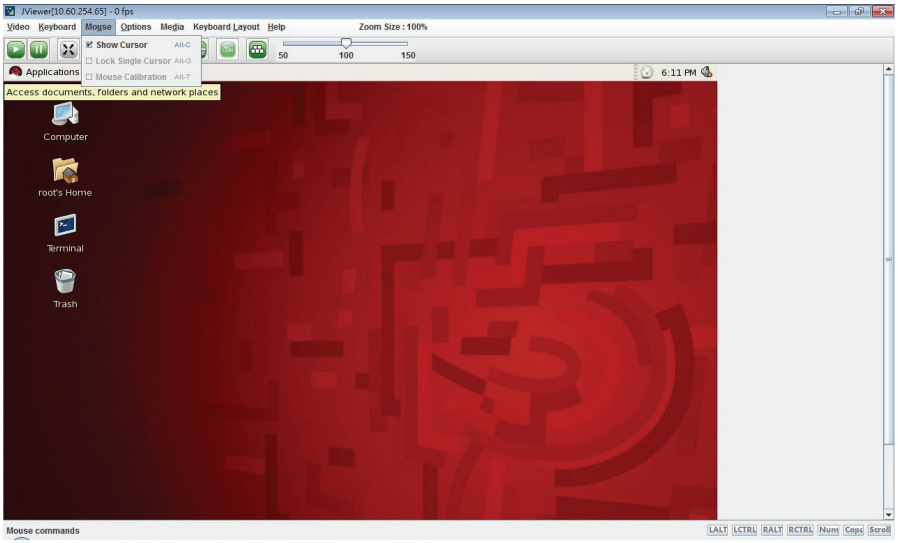
Context menu: This menu item can be used to act as the context menu key, when in Console Redirection.



2.7.1.3 Mouse

Show Cursor: This menu item can be used to show or hide the local mouse cursor on the remote client system.

Lock Single Cursor: This menu item can be used when mouse mode is relative mode.



2.7.1.4 Options

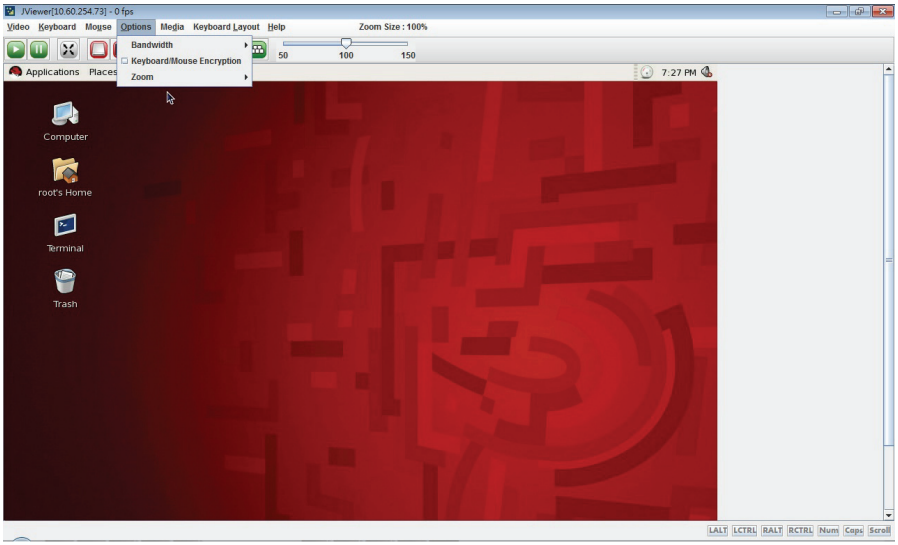
Band width: The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following:

- Auto Detect - This option is used to detect client system keyboard layout automatically and send the key event to the host based on the Layout detected.
- 256 Kbps
- 512 Kbps
- 1 Mbps
- 10 Mbps

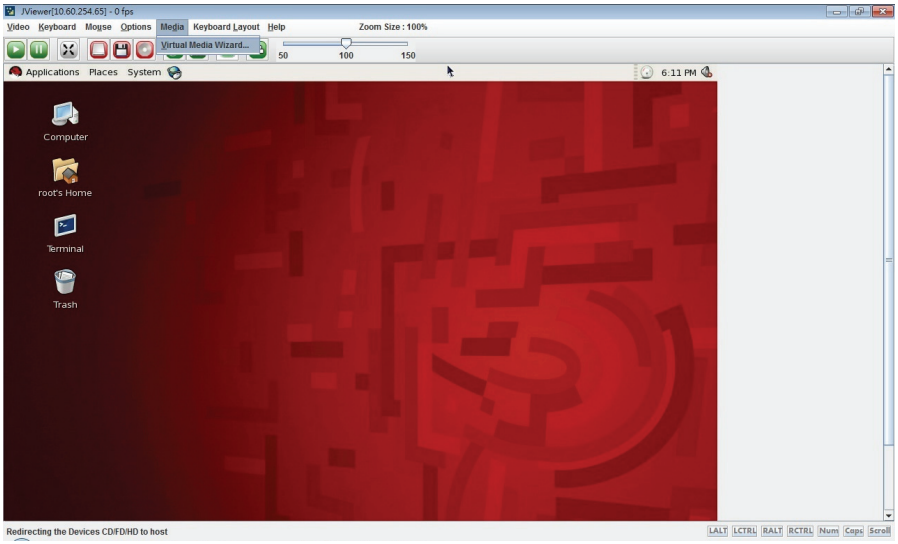
Keyboard/Mouse Encryption: This option allows you to encrypt keyboard inputs and mouse movements sent between the connections.

Zoom:
Note: When the mouse is relative, the mouse synchronization will be executed if the zoom size reaches 100%.

- Zoom In – For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%
- Zoom Out – For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%

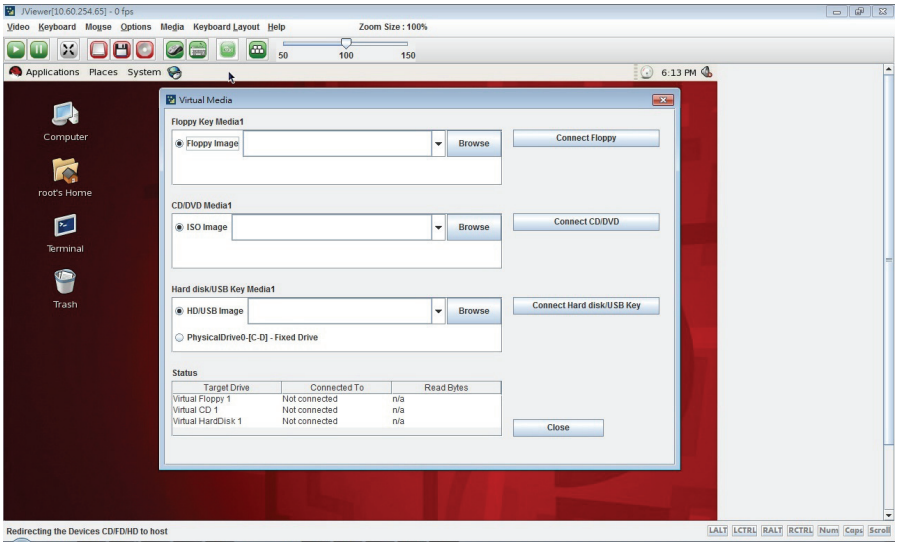


2.7.1.5 Media



Virtual Media Wizard

To add or modify a media, select and click **Virtual Media Wizard**, which pops out a box named “Virtual Media” where you can configure the media. A sample screenshot of Virtual Media Page is given below.



Note:

For windows client, if the logical drive of the physical drive is dismount then the logical device is redirected with Read/Write Permission else it is redirected with Read permission only.

For MAC client, External USB Hard disk redirection is only supported.

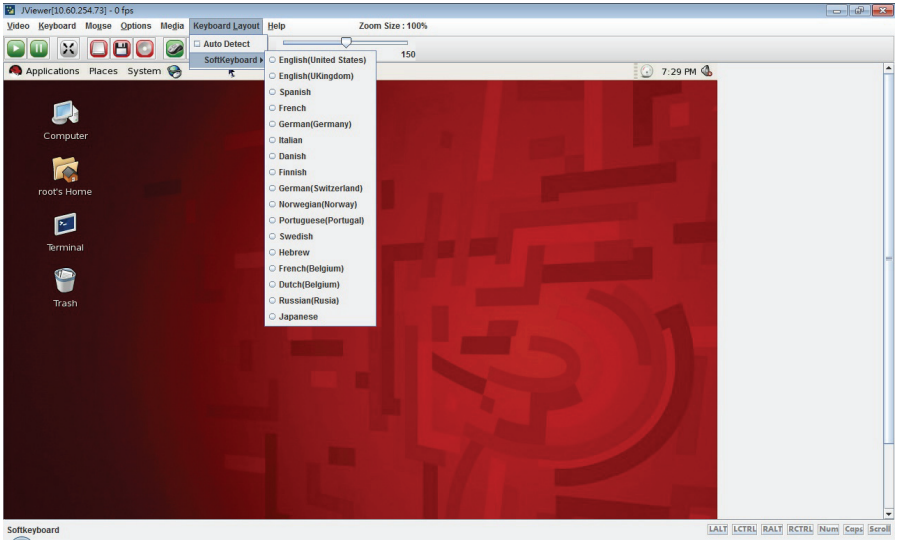
For Linux client, fixed hard drive is redirected only as Read Mode. It is not Write mode supported.

2.7.1.6 Keyboard Layout

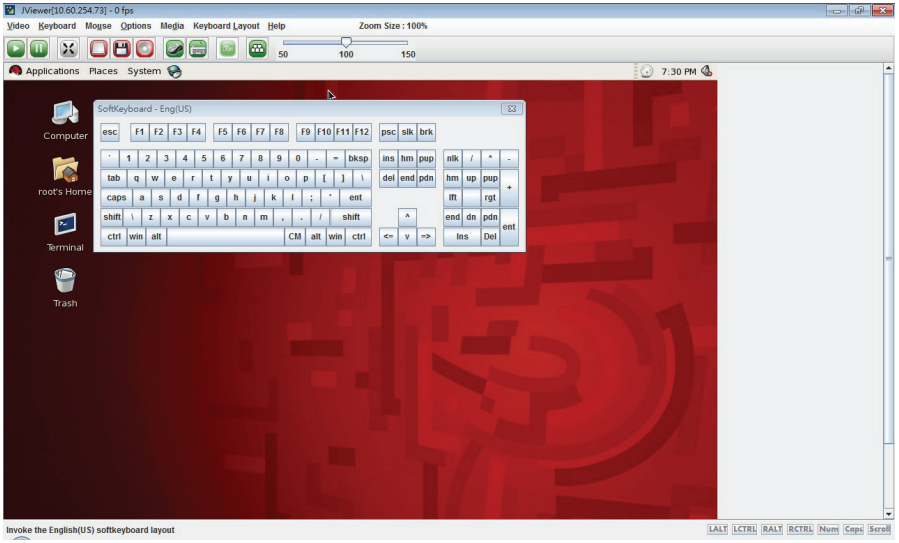
Auto Detect: This option is used to detect keyboard layout automatically. The languages supported automatically are English-US, French-France, Spanish-Spain, German-Germany, Japanese-Japan. If the client and host languages are same, then for all the languages other than English mentioned above, you must select this option to avoid typo errors.

Soft Keyboard: This option allows you to select the keyboard layout. It will show the dialog as similar to onscreen keyboard. If the client and host languages are different, then for all the languages other than English mentioned above, you must select the appropriate language in the list shown in JViewer and use the softkeyboard to avoid typo errors.

Note: Soft keyboard is applicable only for JViewer Application not for other application in the client system.



A sample screenshot of the US Keyboard is given below.



2.7.2 Server Power Control

This page allows you to view and control the power of your server.

To open the Power Control and Status Page, click **Remote Control → Server Power Control** from the main menu. A sample screenshot of Power Control and Status Page is shown in the screenshot below.

2.7.3 Other Control

Select options in the All Others Control Page to Chassis Locate LED, Clear CMOS and Local Panel Lock control.

2.8 Maintenance Group

This group of pages allows you to do maintenance tasks on the device. The menu contains of the following items:

- Firmware Update
- Restore Factory Defaults
- BIOS Update

A detailed description is give ahead.

2.8.1 Firmware Update

In MegaRAC GUI, this wizard takes you through the process of firmware upgrade. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to preserve configuration will be presented. Enable it, if you wish to preserve configured settings through the upgrade.

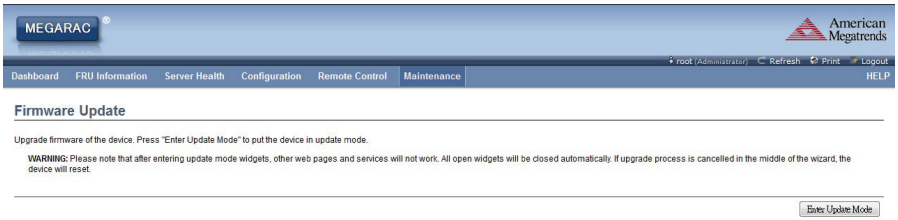
WARNING: Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically, if upgrade process is cancelled in the middle of the wizard, the device will be reset.

NOTE:

The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation.

Once you enter into Update Mode and choose to cancel the firmware flash operation, the MegaRAC card must be reset. This means that you must close the Internet browser and log back onto the MegaRAC card before you can perform any other types of operations.

To open the Firmware Update Page, click **Maintenance → Firmware Update** from the main menu. A sample screenshot of Firmware Update Page is shown in the screenshot below.

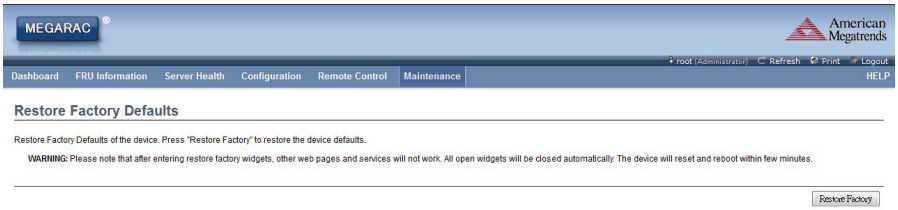


2.8.2 Restore Factory Defaults

In MegaRAC GUI, this option is used to restore the factory defaults of the device firmware.

WARNING: Please note that after entering restore factory defaults widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.

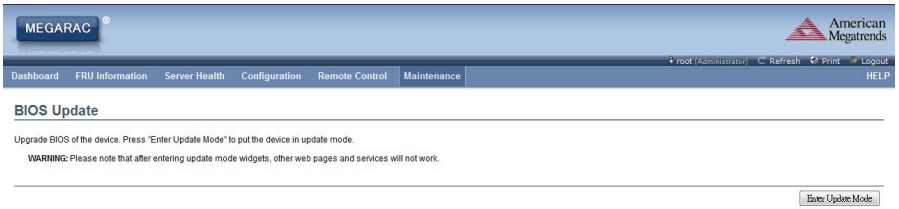
To open the Restore Factory Defaults Page, click **Maintenance → Restore Factory Defaults** from the main menu. A sample screenshot of Restore Factory Defaults Page is shown in the screenshot below.



2.8.3 BIOS Update

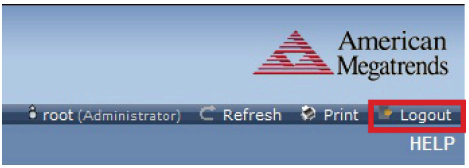
This page allows you to upgrade BIOS of the device.

To open the BIOS Update Page, click **Maintenance → BIOS Update** from the main menu. A sample screenshot of BIOS Update Page is shown in the screenshot below.

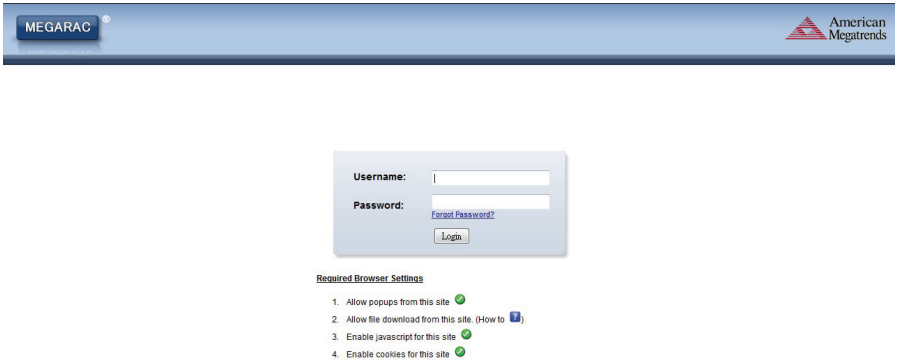


2.9 Log Out

To log out of the MegaRAC GUI, click the logout link on the top right corner of the screen.



The Log in screen will pop out.



3. BMC Port Number

This section will list a table of the BMC Port numbers.

BMC Port Number	Web Server: 80, 443
	KVM: 7578, 7582
	CD Media: 5120, 5124
	FD Media: 5123, 5127
	HD Media: 5122, 5126
	IPMI: 623
	UPnP Discovery: 1900, 50000