CIARA

a Hypertec Group company

Speed | Performance | Passion for Innovation

ASMB7-iKVM

Server Management Board
User's guide

Table of contents

Preface

About this guide

This user's guide contains the information you need when installing and configuring the server management board.

How this guide is organized

This guide contains the following parts:

- **Chapter 1: Product introduction**

This chapter describes the server management board features and the new technologies it supports.

- **Chapter 2: Configuration**

This chapter provides instructions on how to install the board to the server system and install the utilities that the board supports.

- **Chapter 3: Web-based user interface (ASMB7-iKVM only)**

This chapter tells you how to use the web-based user interface that the server management board supports.

- **Chapter 4: Troubleshooting**

This chapter provides support to troubleshoot generic issues

Safety Information

Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- If the power supply is broken, do not try to fix it by yourself. Contact a CIARA qualified service provider.

Operation safety

- Before adding/removing components, carefully read all the manuals that came with the package.
- Before using the product, ensure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter technical problems with the product, contact a CIARA qualified service provider.

Chapter 1
Technical specifications

1.1 ASMB7-iKVM specifications summary

Chipset	Aspeed 2300
Internal RAM	224 MB for system 32 MB for video
Internal ROM	32 MB
Timers	32-bit Watchdog Timer
Main features	IPMI 2.0-compliant and supports KVM over LAN Web-based user interface (remote management) Virtual media Network Bonding support
Form factor	22 mm x 17 mm

1.2 Features

1. IPMI 2.0

- System interface (KCS)
- LAN interface (support RMCP+)
- System Event Log (SEL)
- Sensor Data Record (SDR)
- Field Replaceable Unit (FRU)
- Remote Power on/off, reboot
- Serial Over LAN (SOL)
- Authentication Type: RAKP-HMAC-SHA1
- Encryption (AES)
- Platform Event Filtering (PEF)
- Platform Event Trap (PET)
- Watchdog Timer

2. Private I2C Bus

- Auto Monitoring sensors (temperature, voltage, fan speed and logging events)

3. PMBus

- Support Power supply for PMBus device

4. PSMI

- Support Power supply for PSMI bus device 16GB (4 x 4GB)

5. Web-based GUI

- Monitor Sensor, show SDR, SEL, FRU, configure BMC, LAN
- Support SSL (HTTPS)
- Multiple user permission level
- Upgrade BMC firmware

6. Update Firmware

- DOS Tool
- Web GUI (Windows® XP/Vista/2003/2008, RHEL5.2, SLES10SP2)

7. Notification

- PET
- SNMP Trap
- e-Mail

8. KVM over Internet

- Web-based remote console

9. Remote Update BIOS

- Use remote floppy to update BIOS

10. Remote Storage (Virtual Media)

- Support two remote storage for USB/CD-ROM/DVD and image

11. Remote Install OS

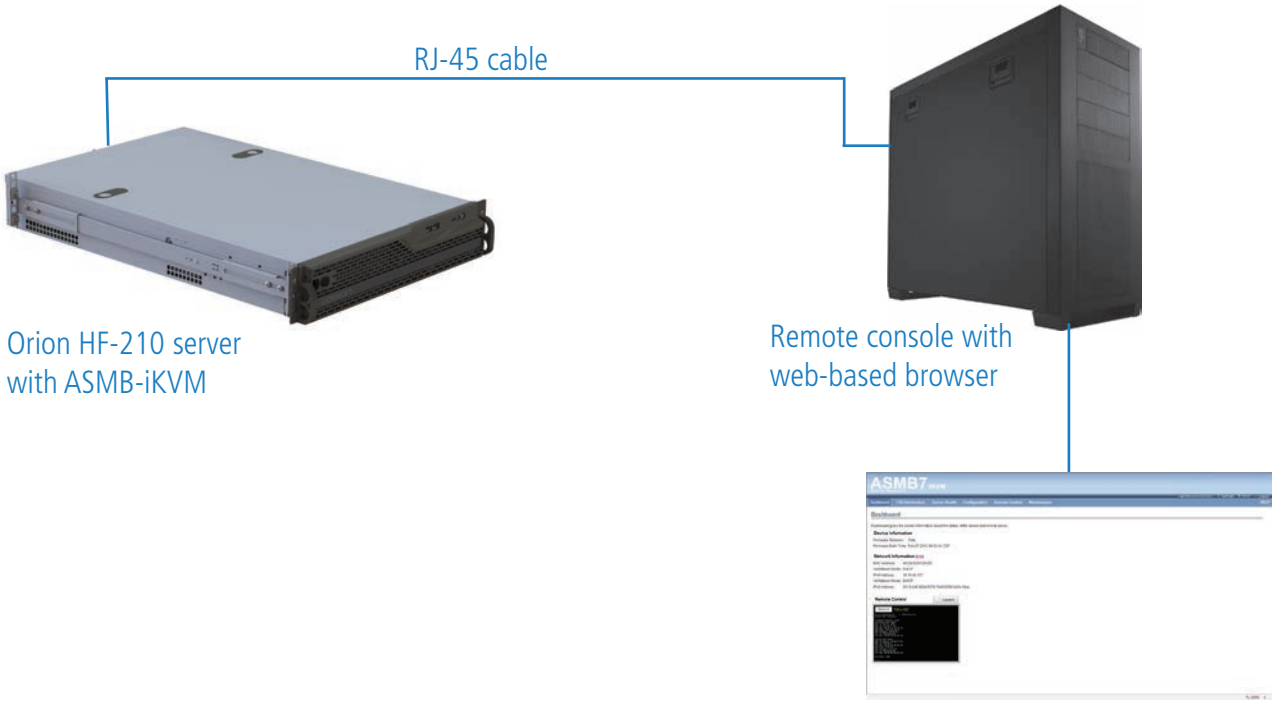
- Use remote storage to remote install OS

Chapter 2
Setup

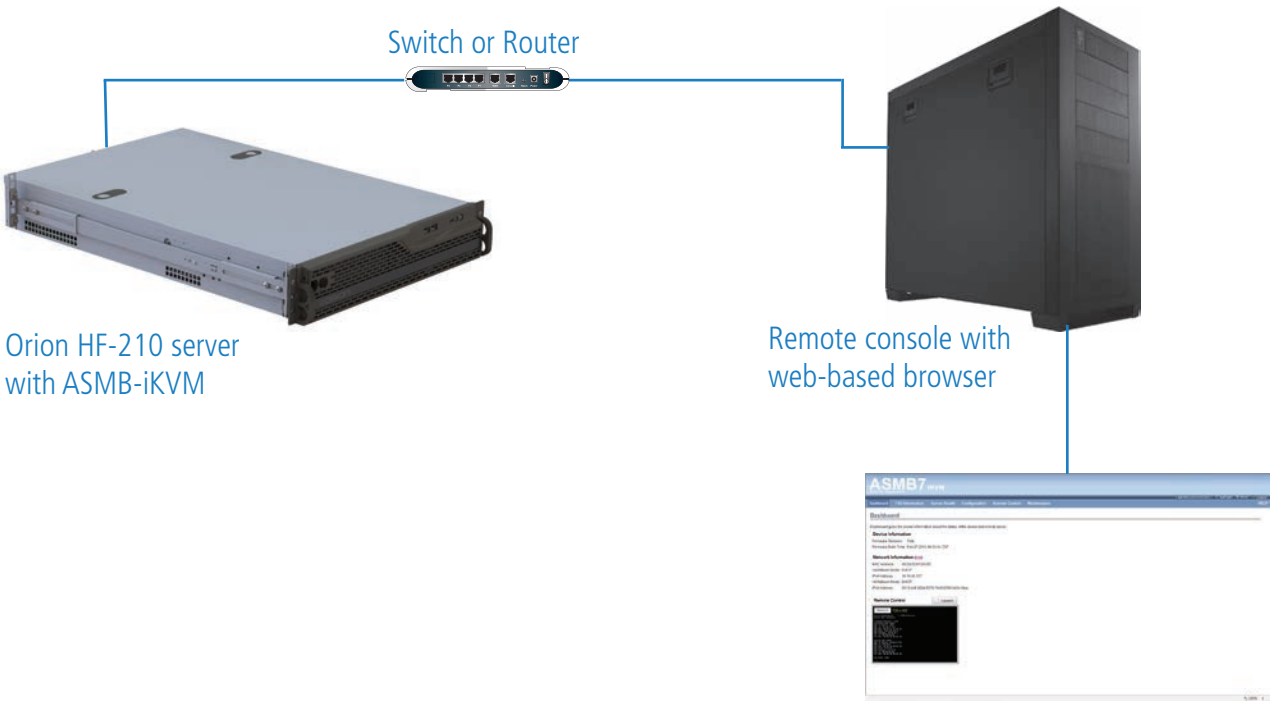
2.1 Network Setup

The ASMB7-iKVM server management board installed on the remote server connects to a local/central server via direct LAN connection or through a network hub. Below are the supported server management configurations.

Direct LAN connection



LAN connection through a network hub



2.2 BIOS Configuration

You need to adjust the settings in the BIOS setup of the remote server for correct configuration and connection to the central server.

2.3 Running the BIOS BMC configuration

To configure the BMC in the BIOS

1. Restart the remote server, then press <Del> during POST to enter the BIOS setup.
2. Go to the Server Mgmt menu, then select the BMC network configuration sub-menu. Use this sub-menu to configure the BMC settings
3. When finished, press <F10> to save your changes and exit the BIOS setup.

2.4 BMC Network configuration

Allows you to set the BMC LAN Parameter settings.

Configuration Source [Previous State]

Allows you to select the IP address source type. Set the LAN channel parameters statically or dynamically.

* The following items are available when you set Configuration Source to [Static].

Station IP Address

Allows you to set the BMC IP address.

Subnet Mask

Allows you to set the BMC subnet mask. We recommend that you use the same Subnet Mask you have specified on the operating system network for the used network card.

Gateway IP Address

Allows you to set the Gateway IP address.

2.5 System Event Log (SEL)

Allows you to view all the events in the BMC event log. It will take a maximum of 15 seconds to read all the BMC SEL records.

Sel components [Disabled]

Allows you to enable or disable all features of system event log during booting.

* The following items become configurable when you set SEL Components to [Enabled].

Erase SEL [No]

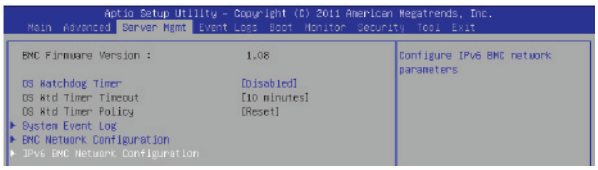
Allows you to select how to erase SEL. Configuration options: [No] - [Yes, On next reset] - [Yes, On every reset]

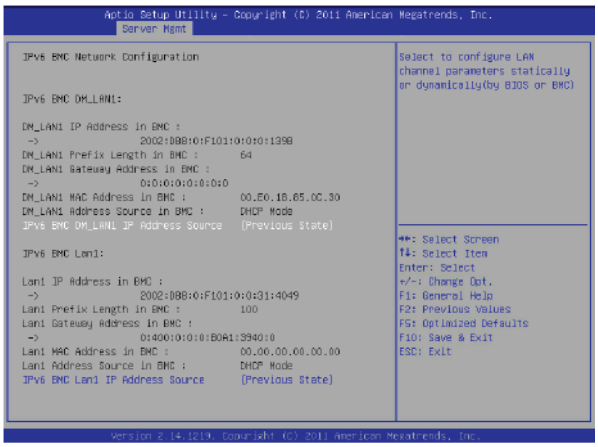
When SEL is full [Do Nothing]

Allows you to select what to do to a full SEL. Configuration options: [Do Nothing] - [Erase Immediately]

2.6 IPv6 BMC Network Configuration

Displays the LAN channel parameters and allows you to configure the IPv6 BMC LAN settings.





IPv6 BMC DM_LAN1 IP Address Source [Previous State]

Allows you to select the IP address source type and set the LAN channel parameters statically or dynamically. Configuration options: [Previous State] - [Static] - [Dynamic-Obtained by BMC running DHCP]

* The following items are available when you set IPv6 BMC DM_LAN1 IP Address Source to [Static].

IPv6 BMC DM_LAN1 IP Address

Allows you to set the IPv6 BMC DM_LAN1 IP address.

IPv6 BMC DM_LAN1 IP Prefix Length

Allows you to set the IPv6 BMC DM_LAN1 IP Prefix length.

IPv6 BMC DM_LAN1 Default Gateway

Allows you to set the IPv6 BMC DM_LAN1 Gateway IP address.

IPv6 BMC Lan1 IP Address Source [Previous State]

Allows you to select the IP address source type and set the LAN channel parameters statically or dynamically. Configuration options: [Previous State] - [Static] - [Dynamic-Obtained by BMC running DHCP]

* The following items are available when you set IPv6 BMC Lan1 IP Address Source to [Static].

IPv6 BMC Lan1 IP Address

Allows you to set the IPv6 BMC Lan1 IP address.

IPv6 BMC Lan1 IP Prefix Length

Allows you to set the IPv6 BMC Lan1 IP Prefix length.

IPv6 BMC Lan1 Default Gateway

Allows you to set the IPv6 BMC Lan1 Gateway IP address.

Chapter 3
Web-based User Interface

The web-based user interface allows you to easily monitor the remote server's hardware information including temperatures, fan rotations, voltages, and power. This application also lets you instantly power on/off or reset the remote server.

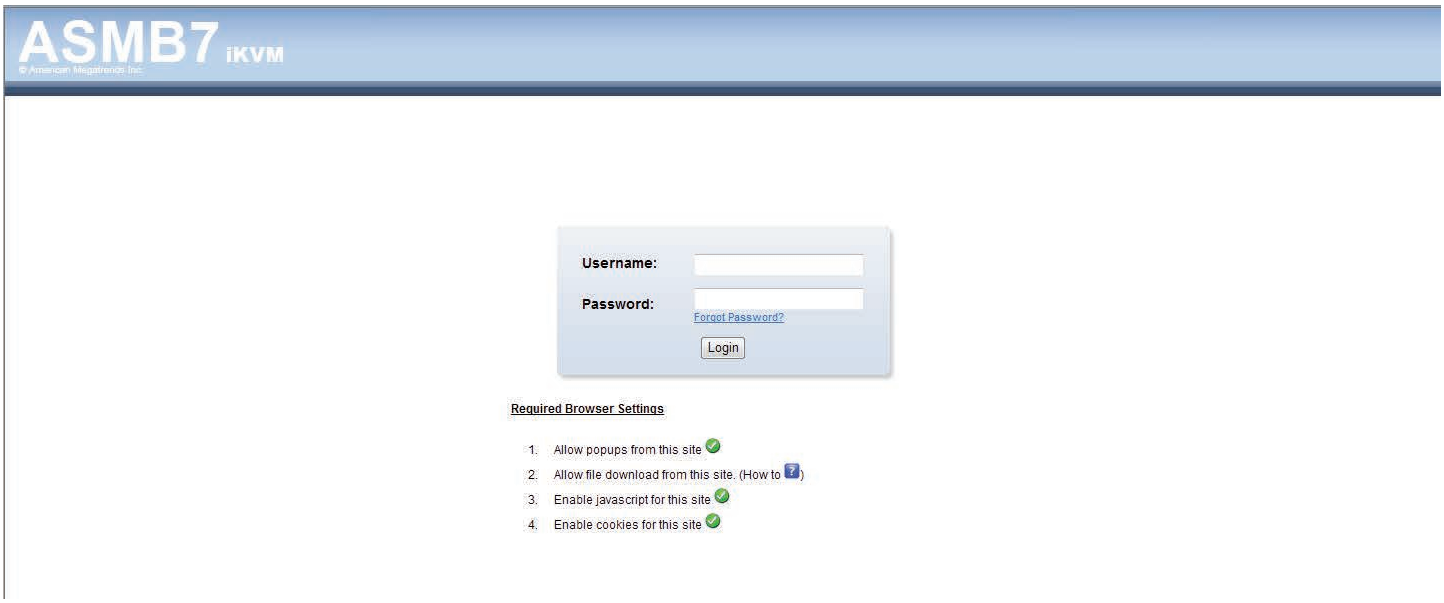
To enter the Web-based user interface:

1. Enter the BIOS Setup during POST.
2. Go to the Advanced Menu > Runtime Error Logging > CPU II0 Bridge Configuration > Launch Storage OpROM, then press <Enter>.
3. Set Launch Storage OpROM to [Enabled].
4. Go to the Server Mgmt Menu > BMC network configuration > Configuration Address source, then press <Enter>.
5. Enter the IP Address in BMC, Subnet Mask in BMC and Gateway Address in BMC.
6. Press <F10> to save your changes and exit the BIOS Setup.

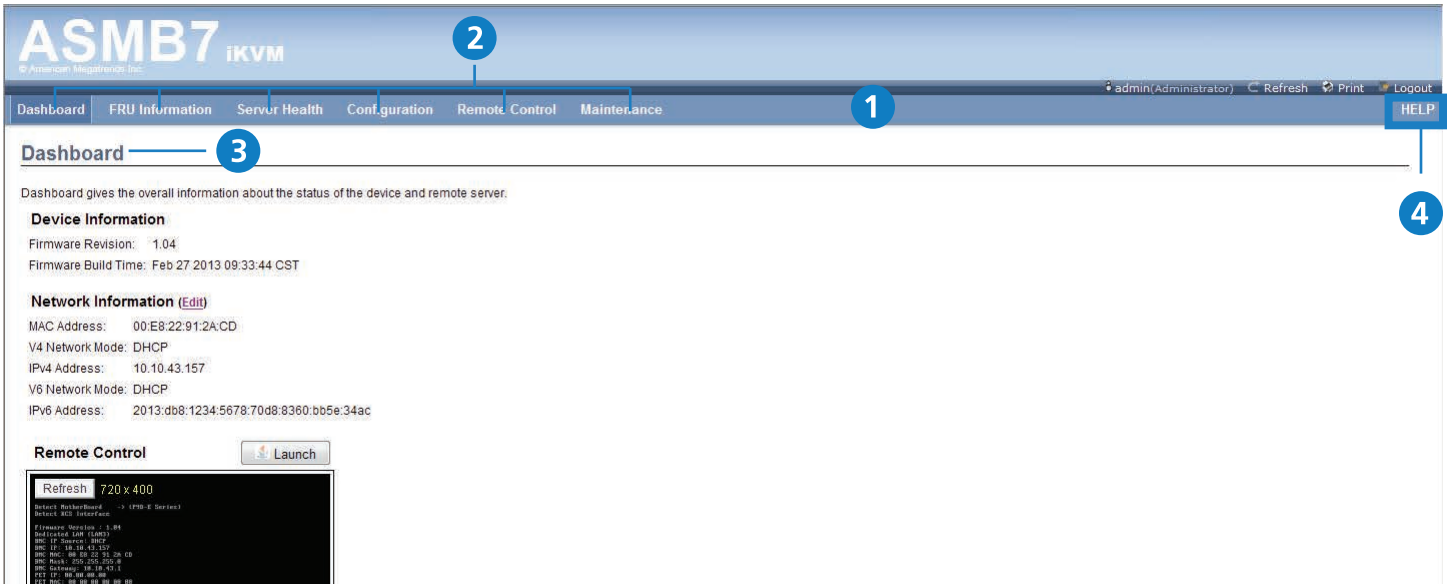
* You should install JRE on remote console first before using web-based management. You can find JRE from the folder JAVA of the ASMB7-iKVM support CD. You can also download JRE from http://www.oracle.com/technetwork/java/javase/downloads/index.html

Logging the Utility

1. Ensure that the LAN cable of the computer is connected to the LAN port of the remote server.
2. Open the web browser and type in the same IP address as the one in the remote server.
3. The below screen appears. Enter the default user name (admin) and password (admin). Then click Login.



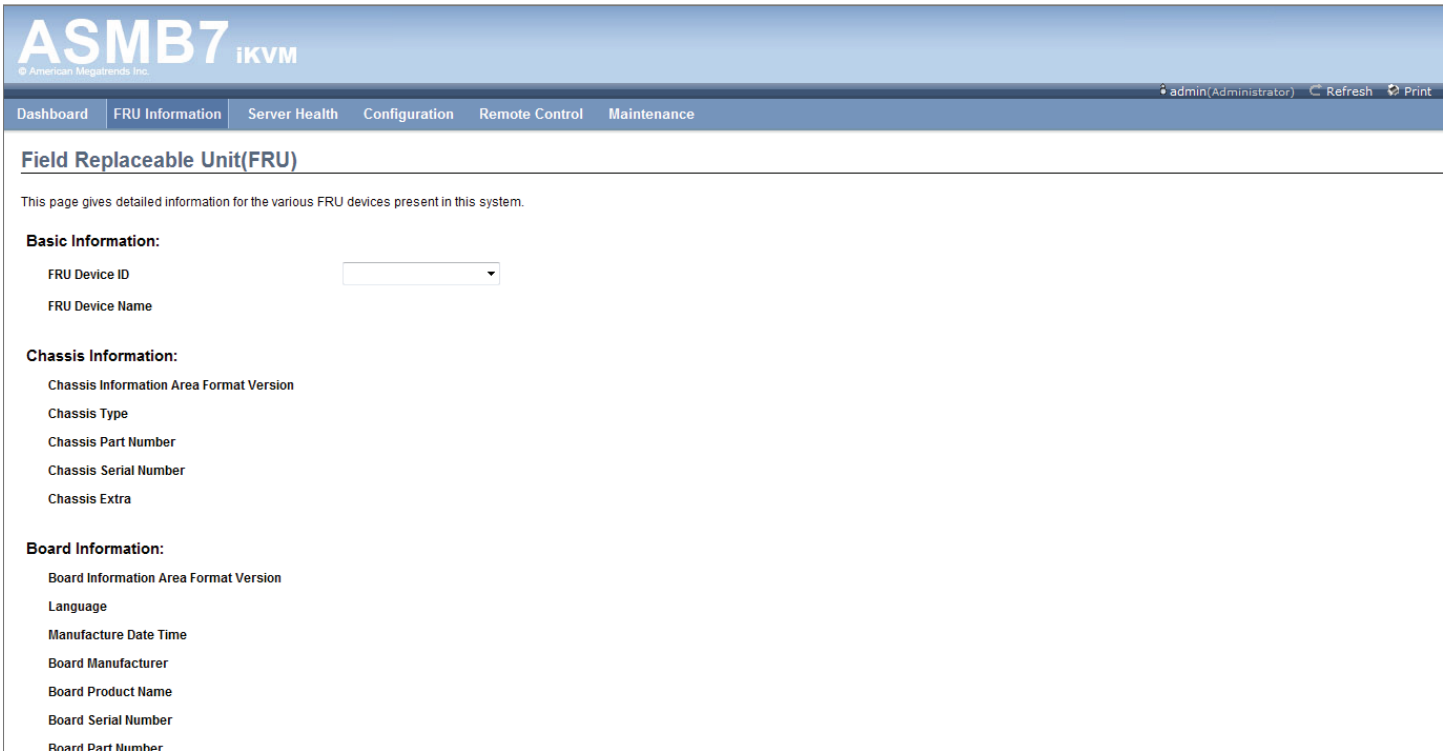
The web-based graphics user interface displays when you login in the utility successfully.



1. **Menu bar:** Click a menu to display available function lists.
2. **Function list:** Click each function key to start using its specific functions
3. **Function title:** Displays the function title.
4. **Help menu:** Click to display the brief description of the selected function.

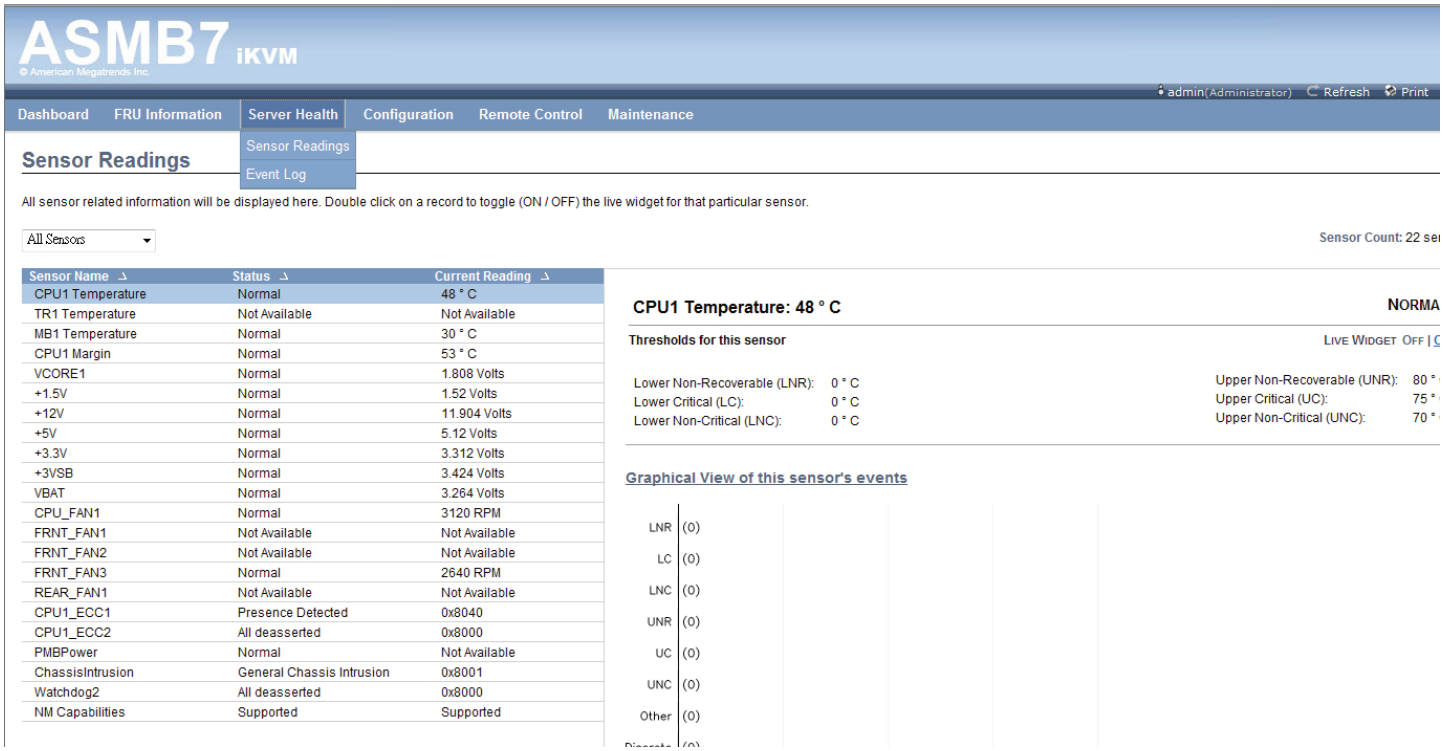
3.1 FRU Information

This section contains detailed information for various FRU devices present in this system.

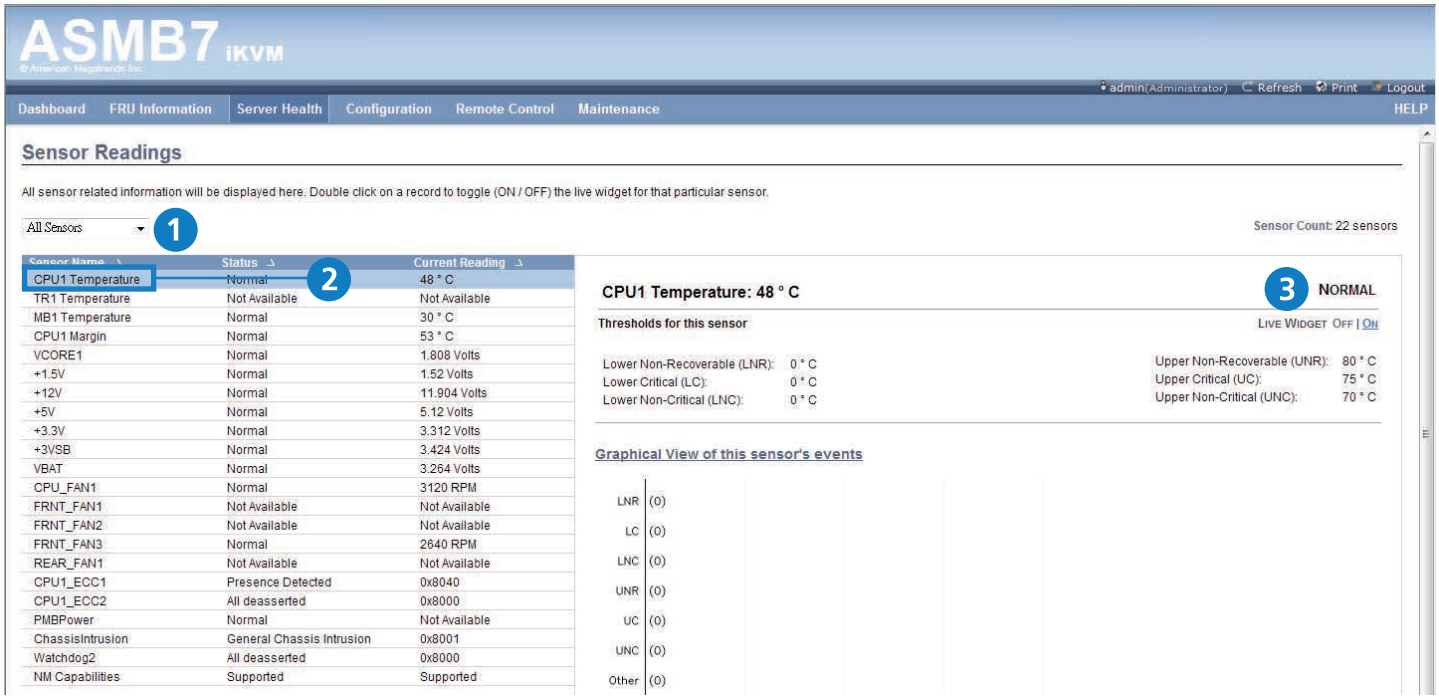


3.2 Server Health

This section contains the data related to the server health, such as the Sensor Readings, Event log and System and Audit Log. Click each function key to start using its specific function.



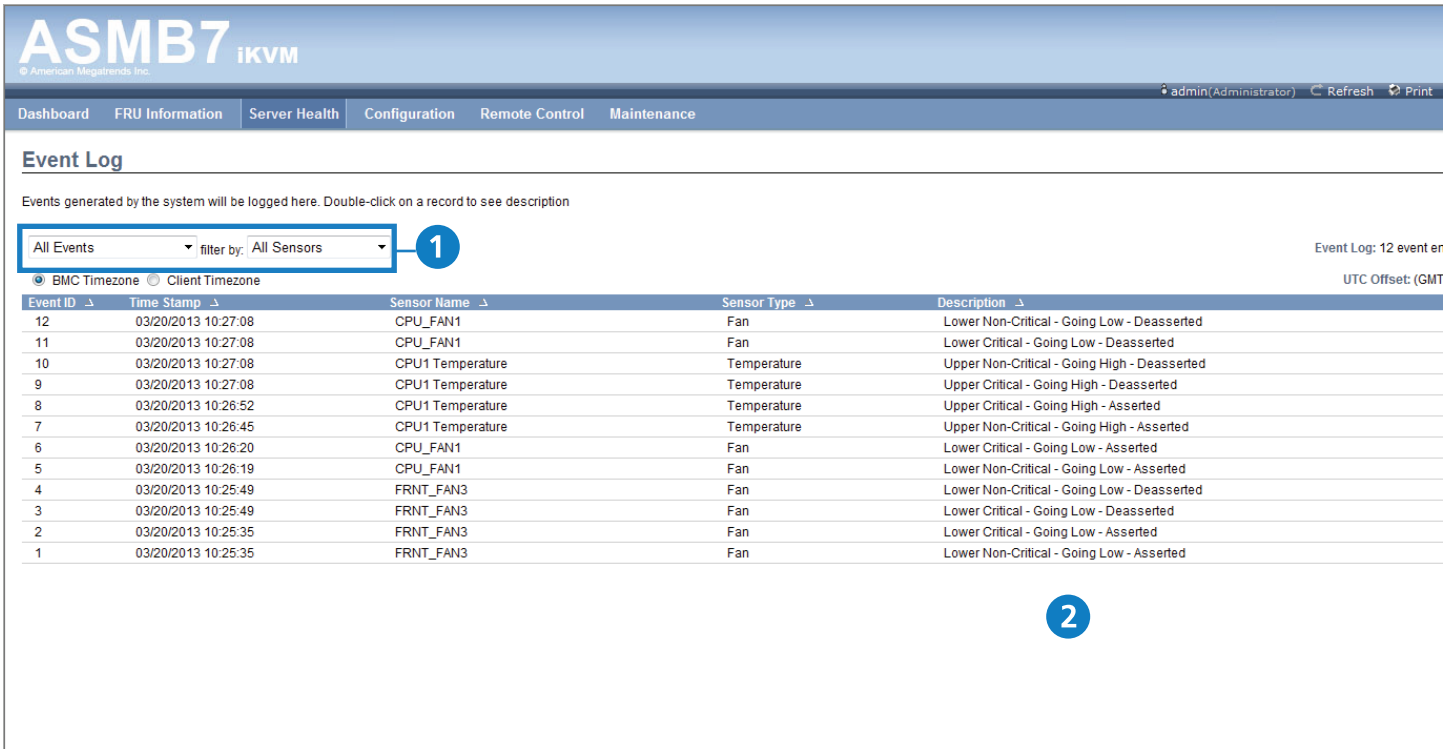
Sensor Readings (with thresholds)



1. **Select a sensor type category:** Allows you to select the type of sensor readings to be displayed in the list.
2. **Status List:** Show the type of sensor readings list that you selected in the drop-down list.
3. **Live Widget:** Click to enable or disable the Live Widget function.

Event Log

The Event Log page displays a table of system event log.



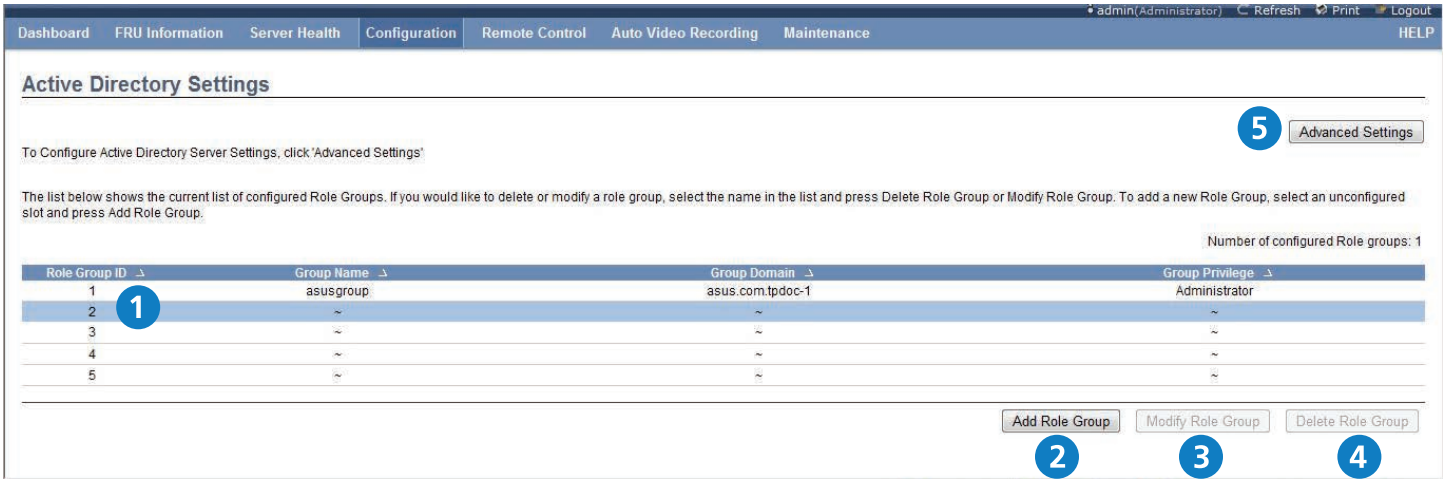
1. Select an event log category: Allows you to select the type of events to be displayed in the list.
2. Clear Event Log: Click to clear the event log.

3.3 Configuration

This section allows you to configure the system settings. Click each function key to start using its specific function.

Active Directory

An active directory does a variety of functions including the ability to provide the information on objects, helps organize these objects for easy retrieval and access, allows access by users and administrators, and allows the administrators to set security up for the directory. To open 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.

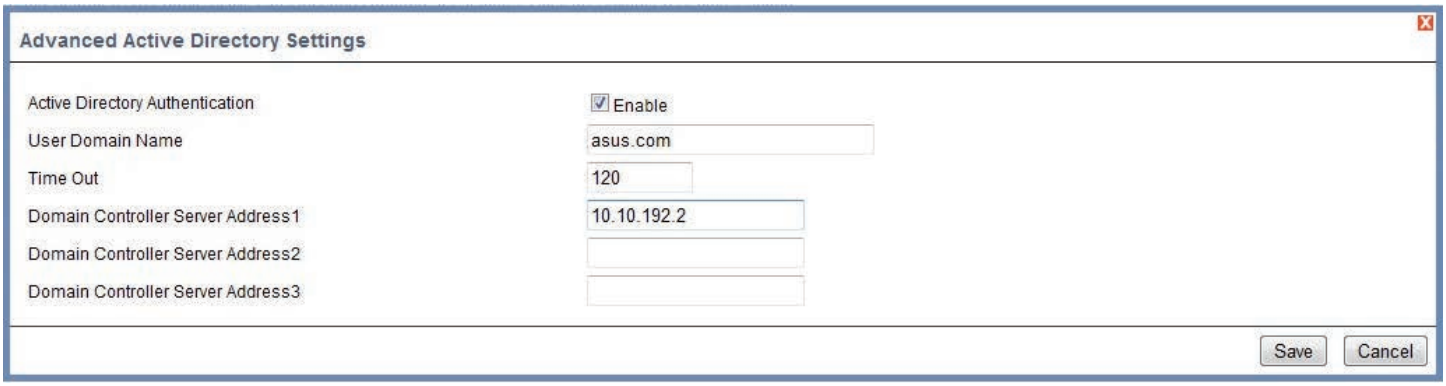


1. **Role Group ID**: The name that identifies the role group in the Active Directory. Role Group Name is a string of 255 alpha-numeric characters. Special symbols hyphen and underscore are allowed.
2. **Add Role Group**: To add a new role group to the device.
3. **Modify Role Group**: To modify that role group. Alternatively, double click on the configured slot.
4. **Delete Role Group**: To delete an existing Role Group.
5. **Advanced Settings**: This option is used to configure Active Directory Advanced Settings. Options are Enable Active Directory Authentication, User Domain name, Time Out and up to three Domain Controller Server Addresses.

Procedure:

Entering the details in Advanced Active Directory Settings Page

1. Click on Advanced Settings to open the Advanced Active Directory Settings Page.



2. In the Active Directory Settings Page, enter the following details.
3. Active Directory Authentication: To enable/disable Active Directory, check or uncheck the Enable checkbox respectively.

* If you have enabled Active Directory Authentication, enter the required information to access the Active Directory server.

4. Specify the Domain Name for the user in the User Domain Name field. e.g. yourdomain.com
5. Specify the time (in seconds) to wait for Active Directory queries to complete in the Time Out field

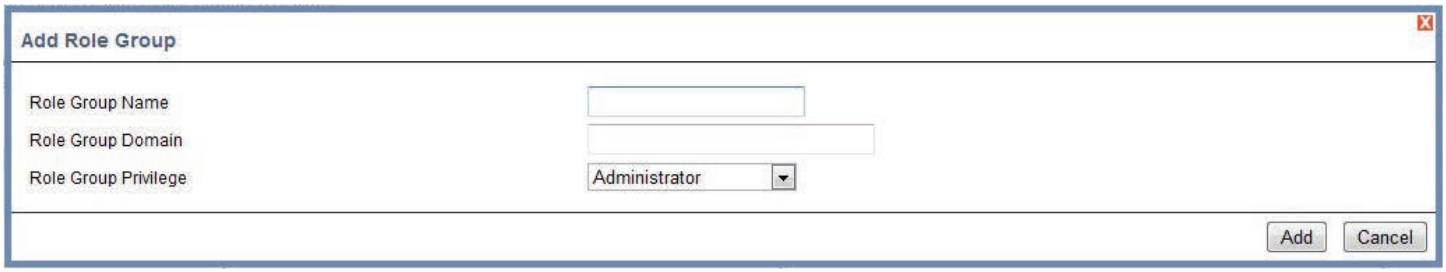
* Default Time Out value: 120 seconds. Allowed values range from 15 to 300 seconds.

6. Configure IP addresses in **Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3**.
7. Click Save to save the entered settings and return to Active Directory Settings Page.
8. Click Cancel to cancel the entry and return to Active Directory Settings Page.

To add a new Role Group:

1. In the Active Directory Settings Page, select a blank row and click **Add Role Group** to open the Add Role Group Page as shown in the screenshot below.
2. In the **Role Group Name** field, enter the name that identifies the role group in the Active Directory.

* Role Group Name is a string of 255 alpha-numeric characters, hyphens and underscores are allowed.



3. In the **Role Group Domain** field, enter the domain where the role group is located.

* Domain Name is a string of 255 alpha-numeric characters, hyphens, underscores and dots are allowed.

4. From the **Role Group Privilege** menu, select the level of privilege to assign to this role group.
5. Click **Add** to save the new role group and return to the Role Group List.
6. Click **Cancel** to cancel the settings and return to the Role Group List.

To Modify Role Group

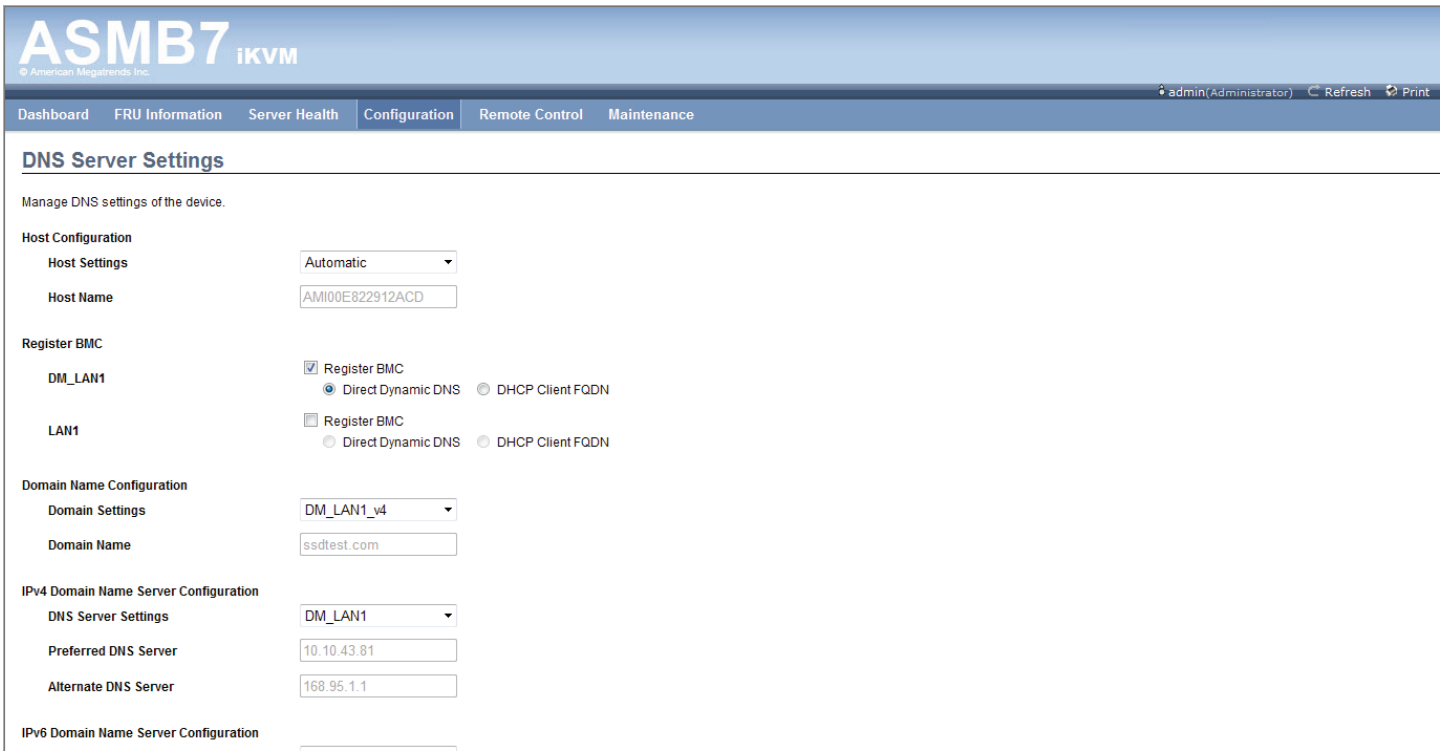
1. In the Advanced Directory Settings Page, select the row that you wish to modify and click **Modify Role Group**.
2. Make the necessary changes and click **Save**.

To Delete a Role Group

In the Advanced Directory Settings Page, select the row that you wish to delete and click **Delete Role Group**.

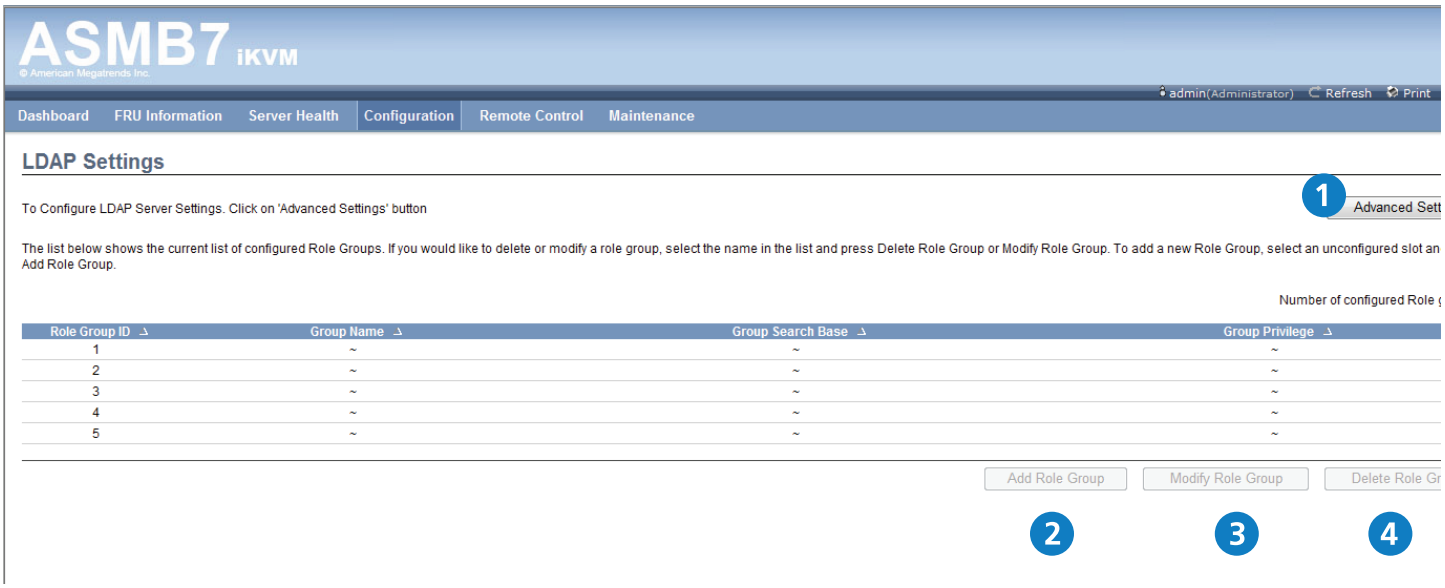
DNS

The page allows you to manage DNS settings of the device.



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. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate MegaRAC® card users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism,when using the MegaRAC card. Since your existing LDAP server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access..
To open LDAP Settings page, click **Configuration > LDAP** from the main menu. A sample screenshot of LDAP Settings Page is shown in the screenshot below.

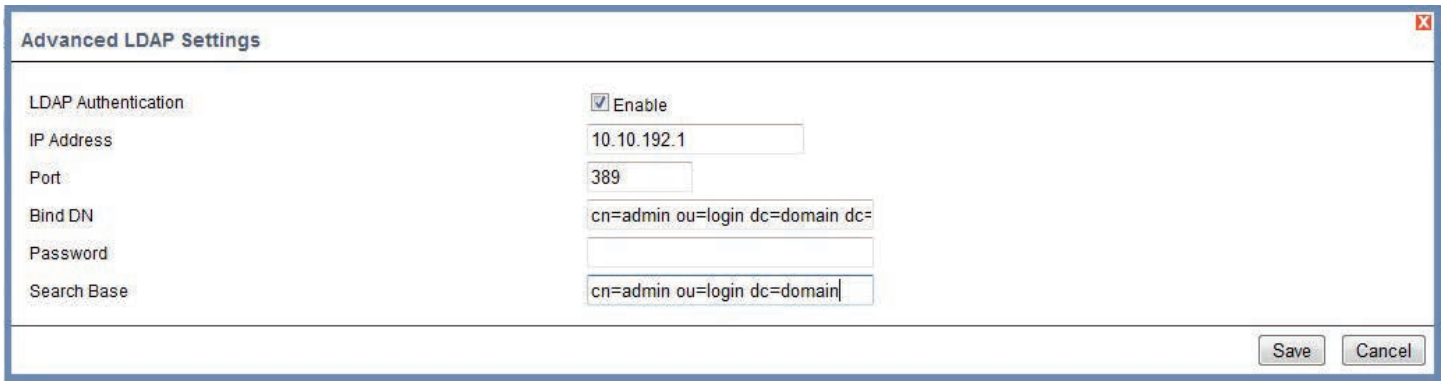


1. **Advanced Settings:** To configure LDAP Advanced Settings. Options are Enable LDAP Authentication, IP Address, Port and Search base.
2. **Add Role Group:** To add a new role group to the device. Alternatively, double click on a free slot to add a role group.
3. **Modify Role Group:** To modify the particular role group.
4. **Delete Role Group:** To be delete a role group from the list.

Procedure

Entering the details in Advanced LDAP Settings Page

1. In the LDAP Settings Page, click Advanced Settings. A sample screenshot of LDAP Settings page is given below.



2. To enable/disable LDAP Authentication, check or uncheck the Enable checkbox respectively.

* During login prompt, use username to login as an LDAP Group member.

3. Enter the IP address of LDAP Server in the IP Address field.

* 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.

* Supports IPv4 Address format and IPv6 Address format.

4. Specify the LDAP Port in the Port field.

* Default Port is 389. For Secure connection, default port is 636.

5. Enter the Search Base. The Search Base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.
6. Click Save to save the settings.
7. Click Cancel to cancel the modified changes.

To add a new Role Group

1. In the LDAP Settings Page, select a blank row and click **Add Role Group** to open the Add Role group Page.

2 In the **Role Group Name** field, enter the name that identifies the role group

3. In the **Role Group Search Base** field, enter the path from where the role group is located to Base DN.

* Search Base is a string of 255 alpha-numeric characters.

* Special symbols hyphen, underscore and dot are allowed.

4. In the **Role Group Privilege** field, enter the level of privilege to assign to this role group.
5. Click **Add** to save the new role group and return to the Role Group List.
6. Click Cancel to cancel the settings and return to the Role Group List.

To Modify Role Group

1. In the LDAP Settings Page, select the row that you wish to modify and click **Modify Role Group**.
2. Make the necessary changes and click **Save**.

To Delete a Role Group

In the LDAP Settings Page, select the row that you wish to delete and click **Delete Role Group**.

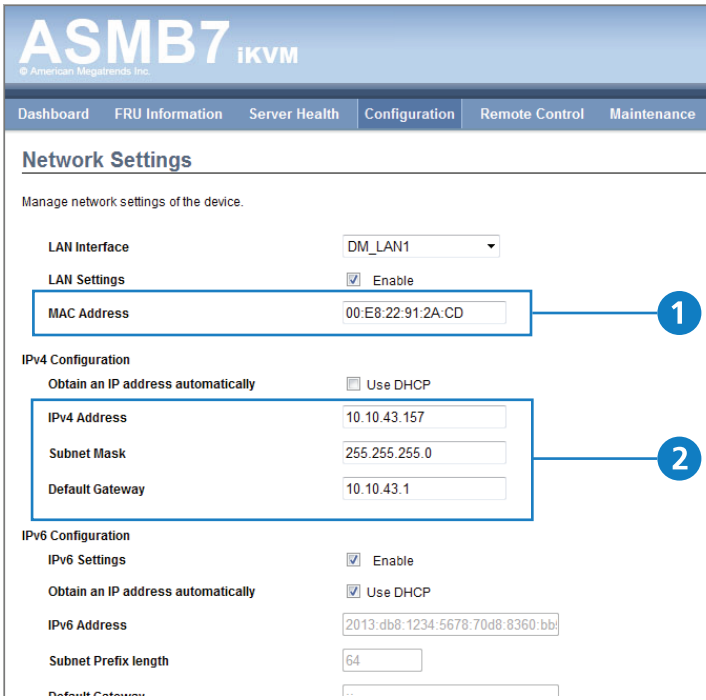
Mouse Mode

The Mouse Mode page allows you to select the mouse mode.

1. **Save:** Select the desired mouse mode, and then click Save to apply the setting.

Network

The Network page allows you to configure the network settings.



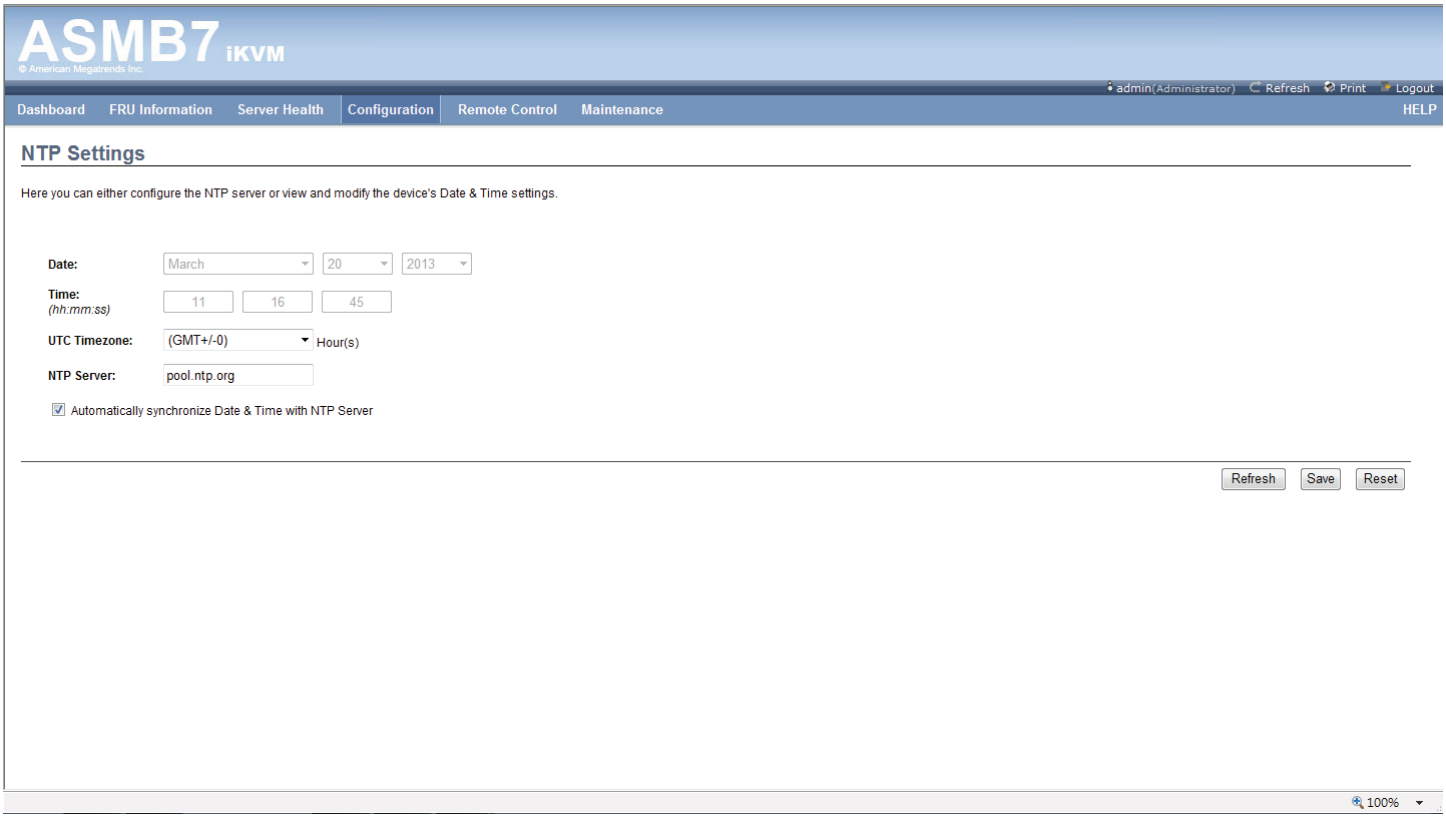
1. **MAC Address:** Select whether to obtain the IP address automatically or manually configure one.
2. **IP Address, Subnet Mask, Default Gateway:** If you configure a static IP, enter the requested address, subnet mask and gateway in the given field.

Network Bond

This page allows you to enable or disable network bonding feature and configure the default interfaces.

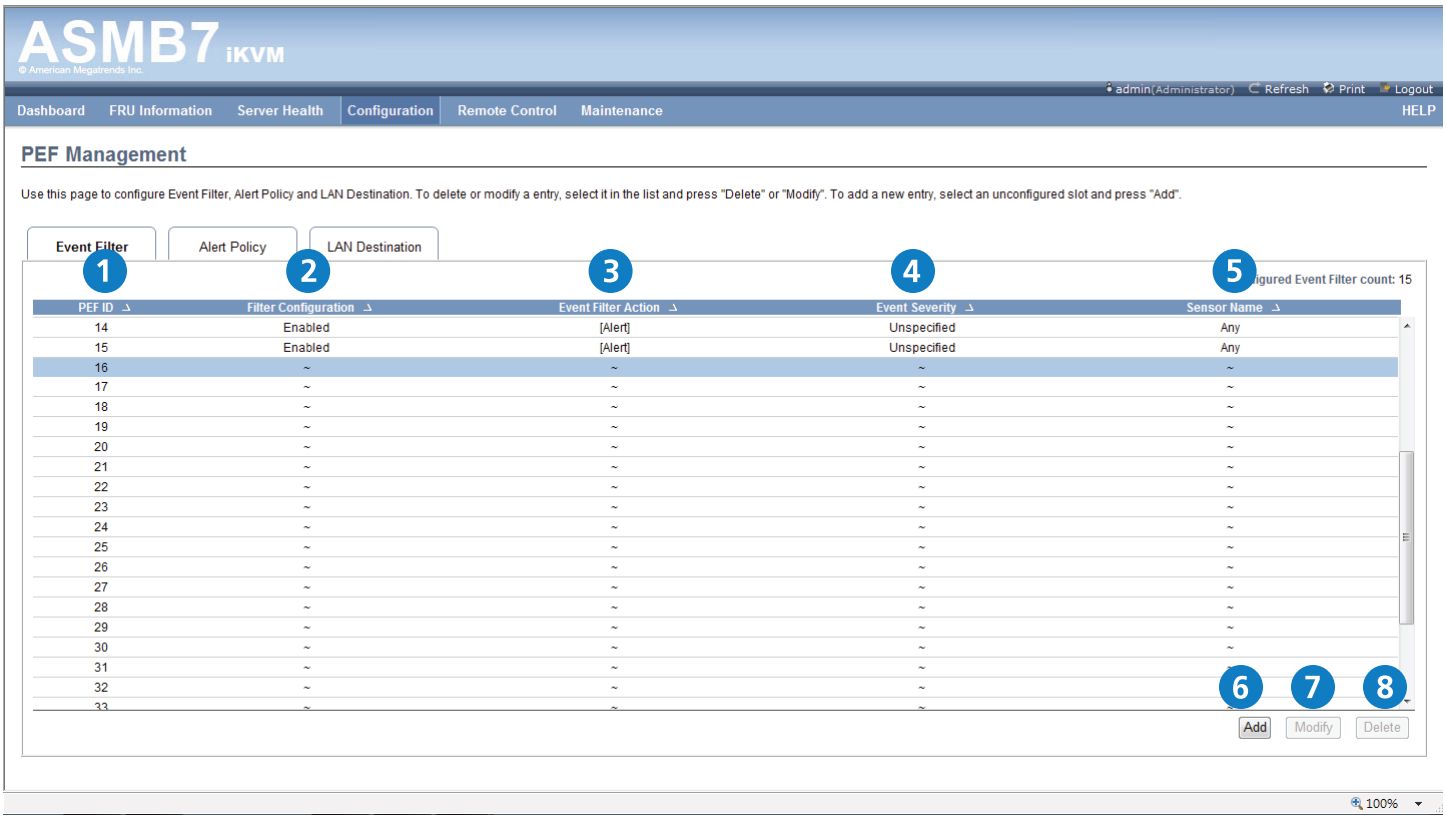
NTP

This page allows you to configure the NTP server or view and modify the device's Date and Time settings.



PEF

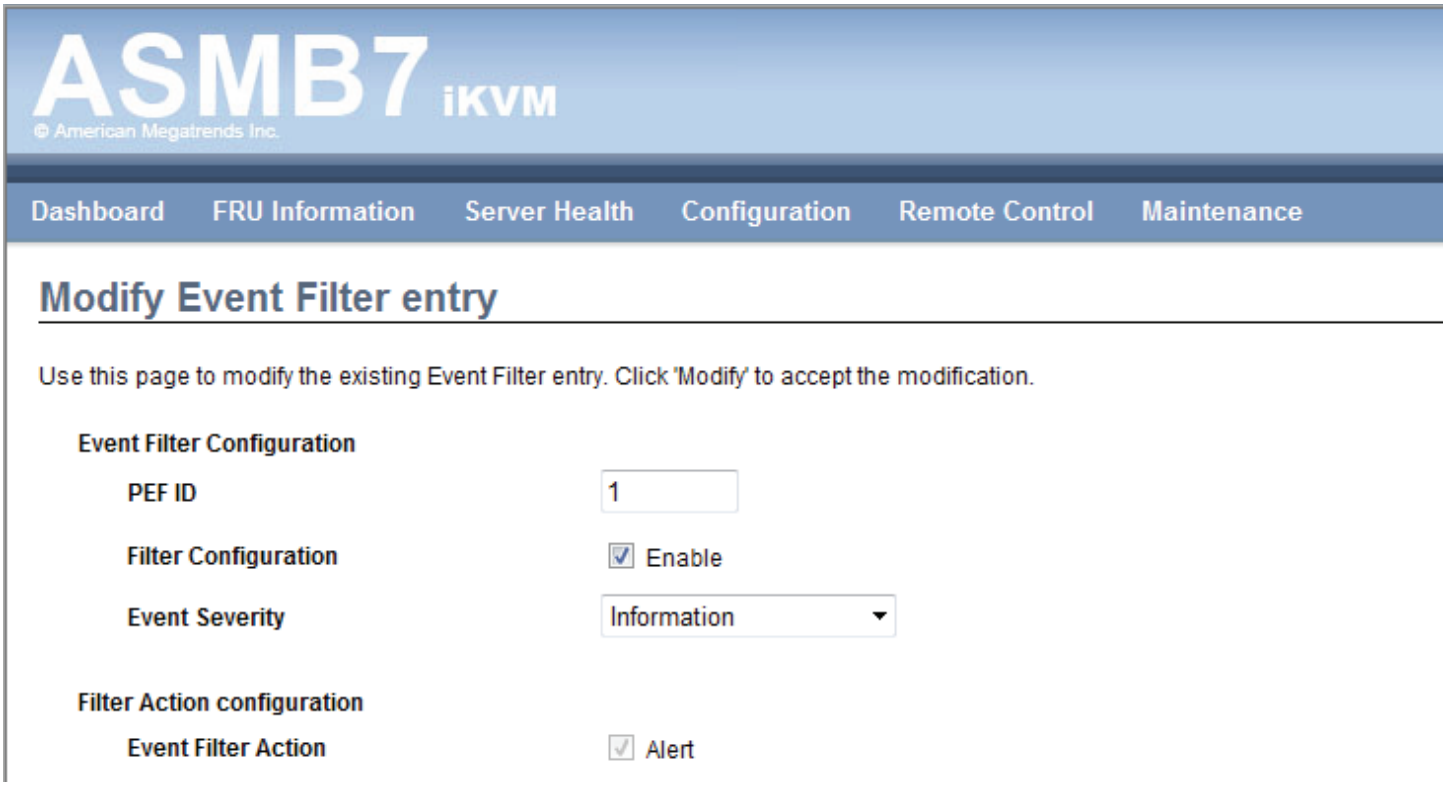
Platform Event Filtering (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert. A PEF implementation 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 event, such as over-temperature, power system failure, fan failure events, etc.
To open PEF Management Settings page, click **Configuration > PEF** from the main menu. A sample screenshot of PEF Management Settings Page is shown in the screenshot below.



1. **PEF ID:** This field displays the ID for the newly configured PEF entry (read only).
2. **Filter configuration:** Check box to enable the PEF settings.
3. **Event Filter Action:** Check box to enable PEF Alert action. This is a mandatory field.
4. **Event Severity:** To choose any one of the Event severity from the list.
5. **Sensor Name:** To choose the particular sensor from the sensor list.
6. **Add:** To add the new event filter entry and return to Event filter list.
7. **Modify:** To modify the existing entries.
8. **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 in seen 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 setting.
   - 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 enables 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.

* 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.

* In RAW data field, to specify hexadecimal value prefix with '0x'

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.

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

1. **Policy Entry #:** Displays Policy entry number for the newly configured entry (read-only).
2. **Policy Number:** Displays the Policy number of the configuration.
3. **Policy Configuration:** To enable or disable the policy settings.
4. **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.

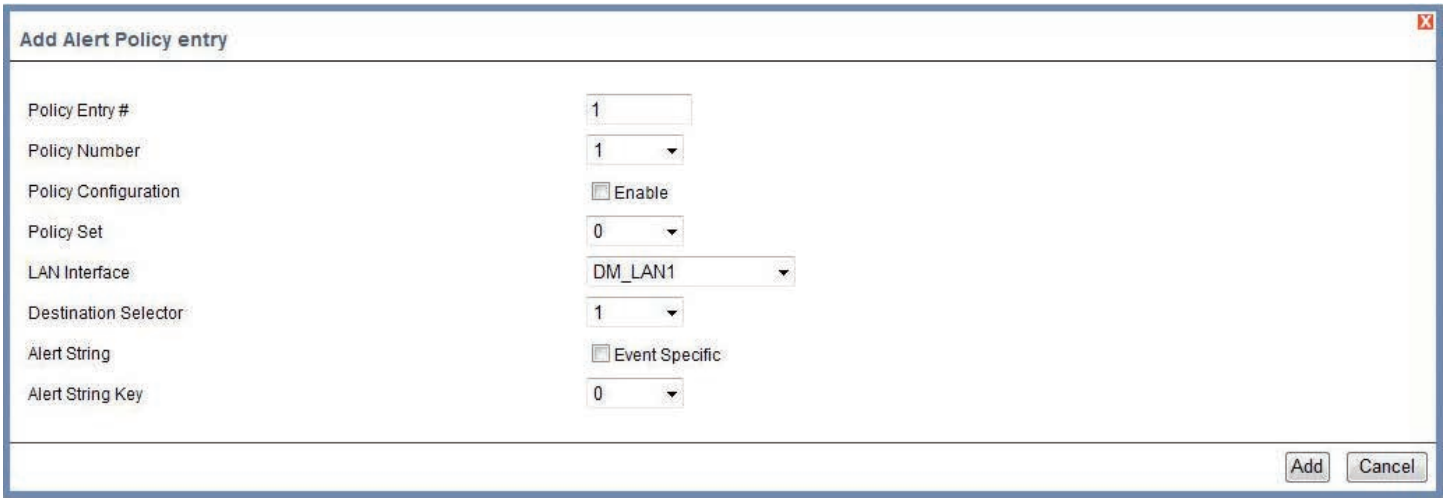
   3 - If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.

   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.
5. **Channel Number:** To choose a particular channel from the available channel list.
6. **Destination Selector:** To choose a particular destination from the configured destination list.

* LAN Destination has to be configured under Configuration->PEF->LAN Destination.

7. **Add**: To save the new alert policy and return to Alert Policy list.
8. **Modify**: To modify the existing entries.
9. **Cancel**: To cancel the modification and return to Alert Policy list.

Procedure:



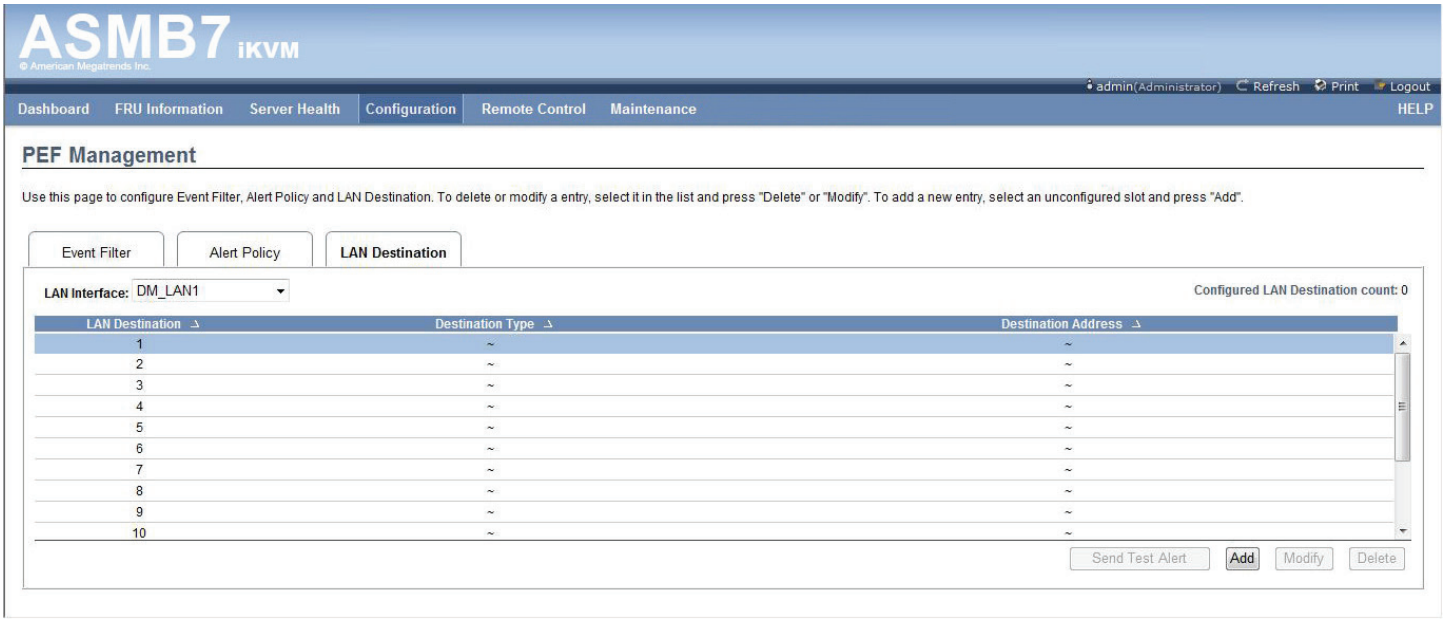
1. In the Alert Policy tab, select the slot for which you have to configure the Alert policy. That is, in the **Event Filter Entry Page**, if you have chosen Alert Policy number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy tab.
2. Select the slot and click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

* 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.



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

1. **LAN Destination:** Displays Destination number for the newly configured entry (read-only).
2. **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 - need 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.
3. **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:

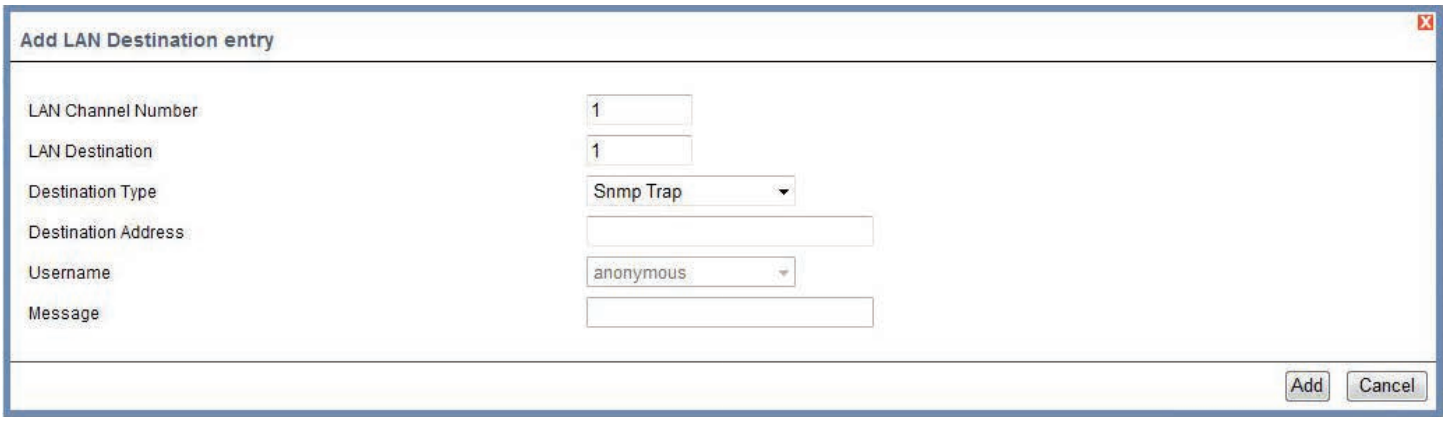
   - IPv4 address format.

   - IPv6 address format.

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

4. **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.
5. **Add:** To save the new LAN destination and return to LAN destination list.
6. **Cancel:** To cancel the modification and return to LAN destination list.

Procedure:



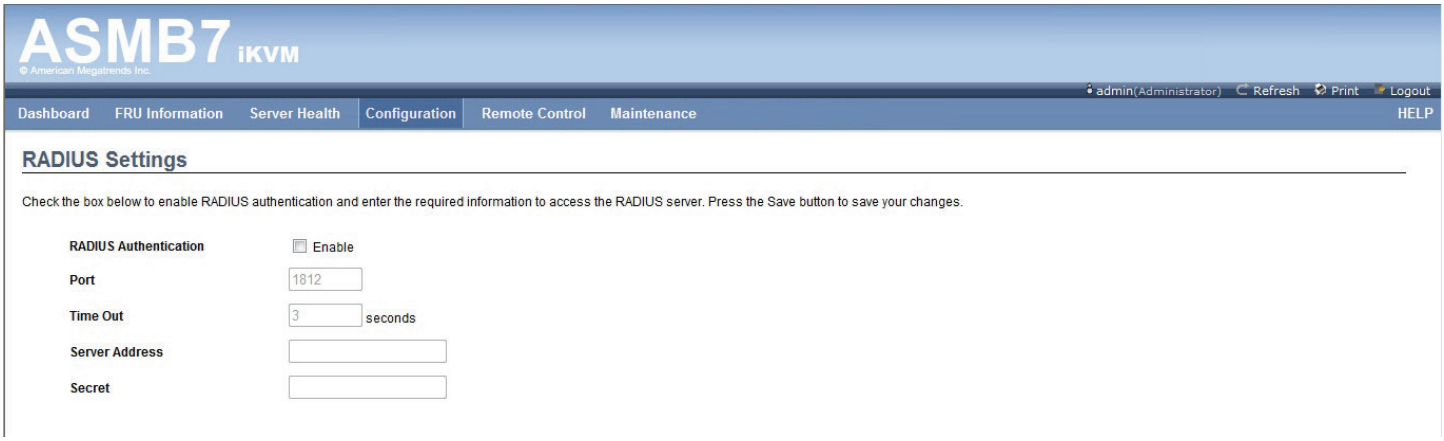
1. In the LAN Destination Tab, choose the slot to be configured. This should be the same slot that you have selected in the Alert Policy Entry- Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policy Entry page of Alert Policy Tab, then you have to configure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

RADIUS

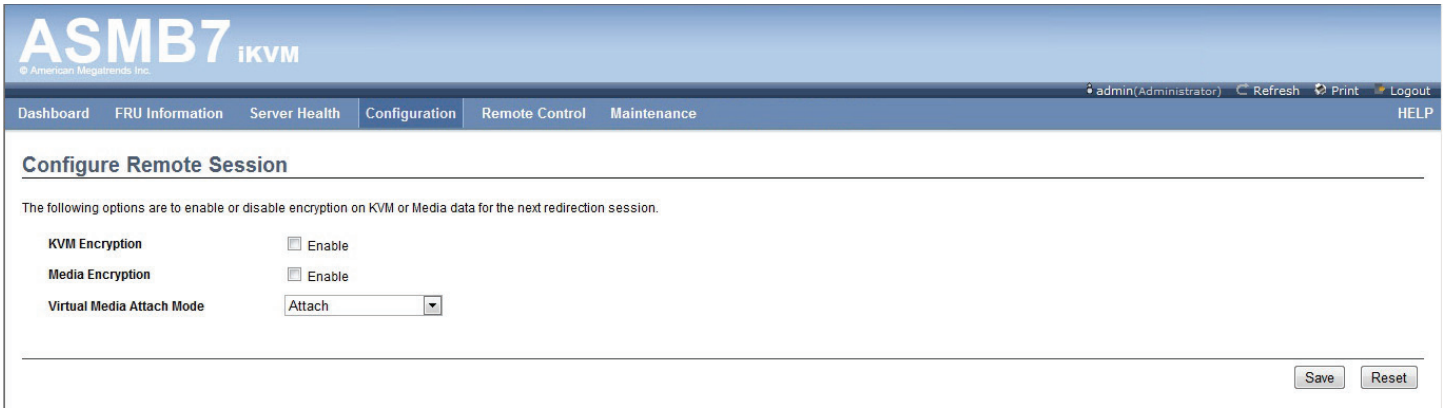
This page is used to enable or disable RADIUS authentication and enter the required information to access the RADIUS server.



Remote Session

The Remote Session page allows you to enable or disable encryption on KVM or data during the redirection session.

1. **KVM Encryption:** Enable/Disable encryption on KVM data for the next redirection session.
2. **Media Encryption:** Enable/Disable encryption on Media data for the next redirection session.



3. **Virtual Media Attach Mode:** Two types of VM attach mode are available:

- Attach - Immediately attaches Virtual Media to the server upon bootup. (The option is for local F/W Update usage).
- Auto Attach - Attaches Virtual Media to the server only when a virtual media session is started.

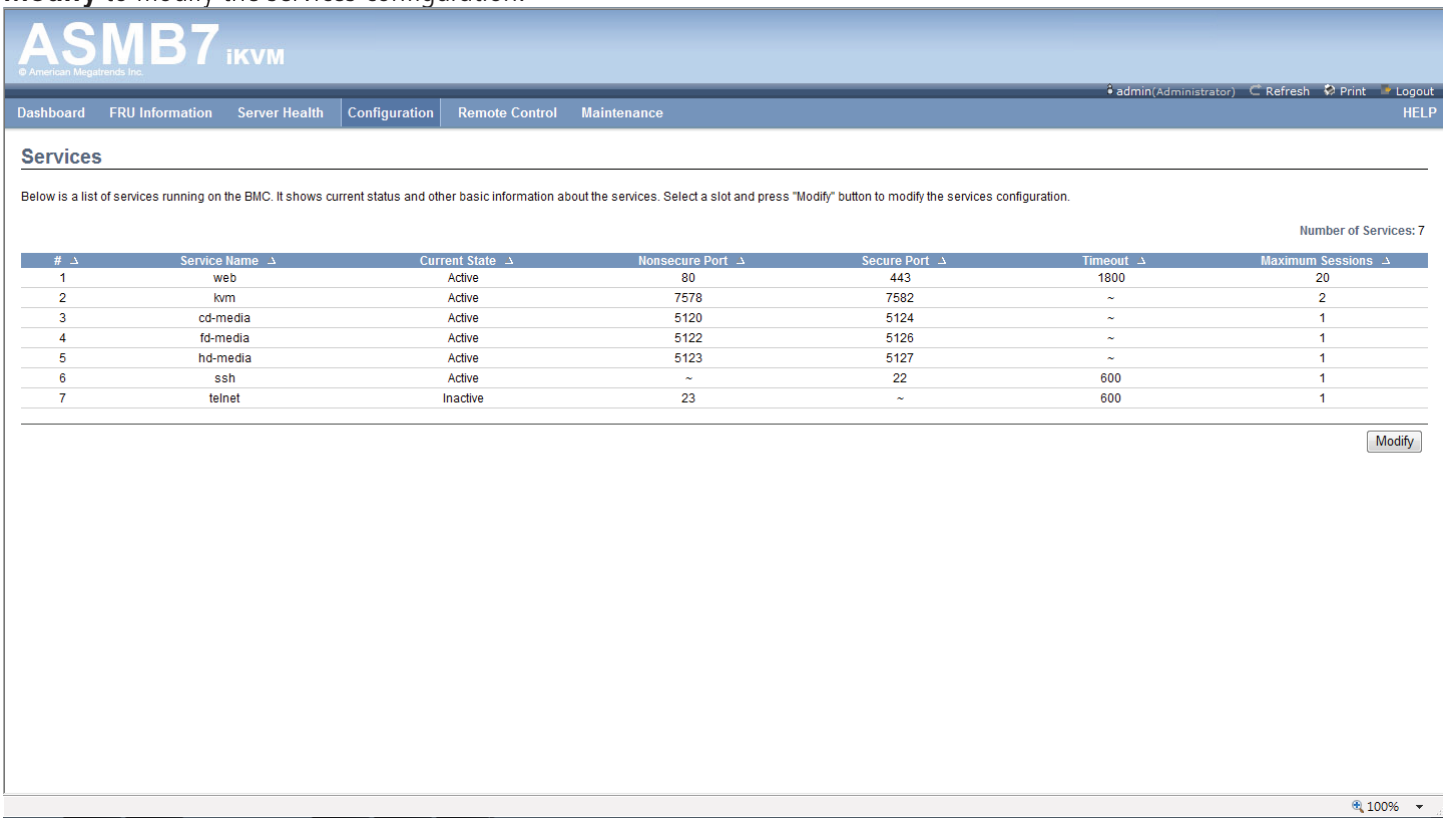
4. **Save:** To save the current changes.

* It will automatically close the existing remote redirection either KVM or Virtual media sessions, if any.

5. **Reset:** To reset the modified changes.

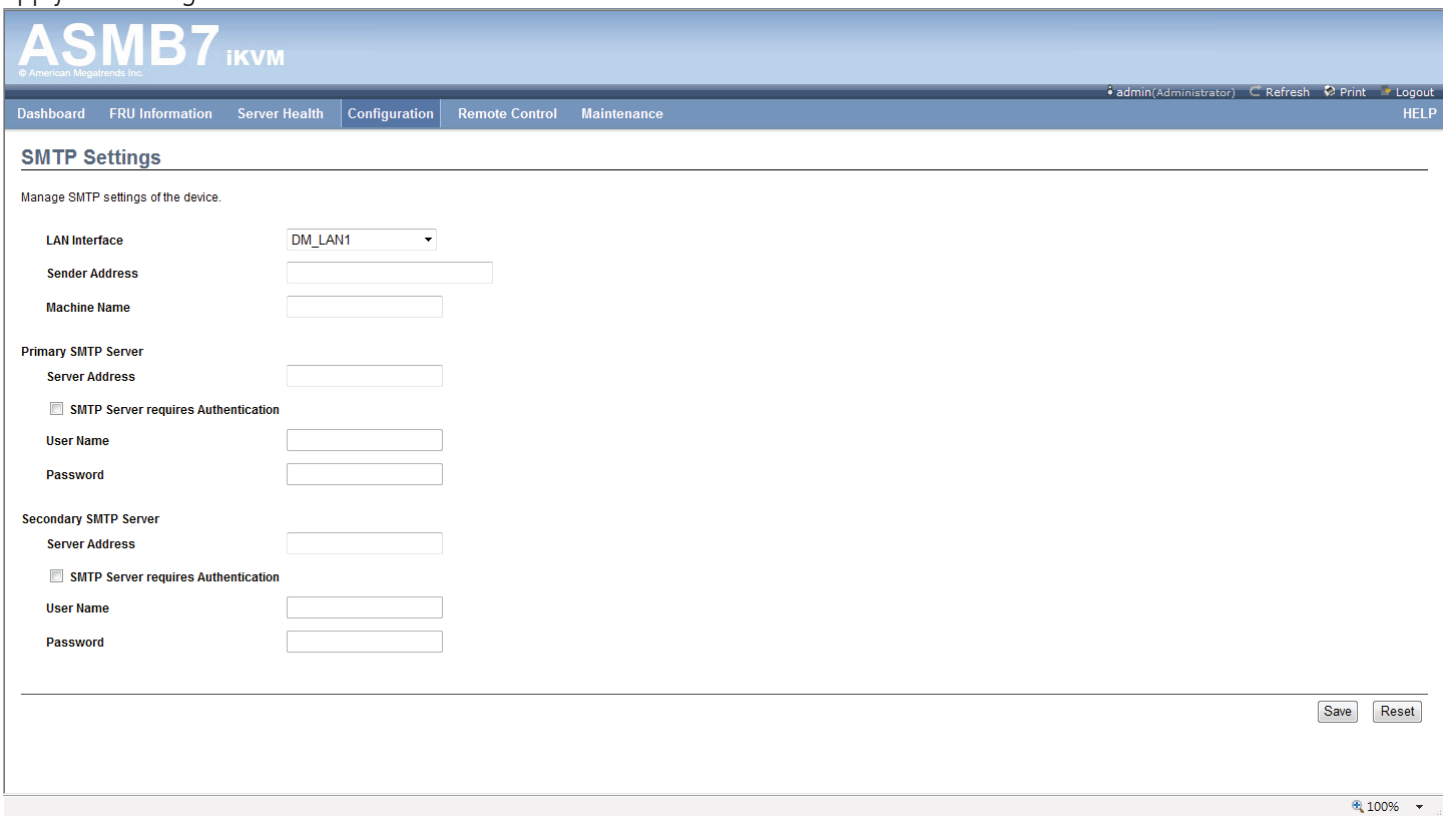
Services

This page lists services running on the BMC. It shows current status and other basic information about the services. Press **Modify** to modify the services configuration.



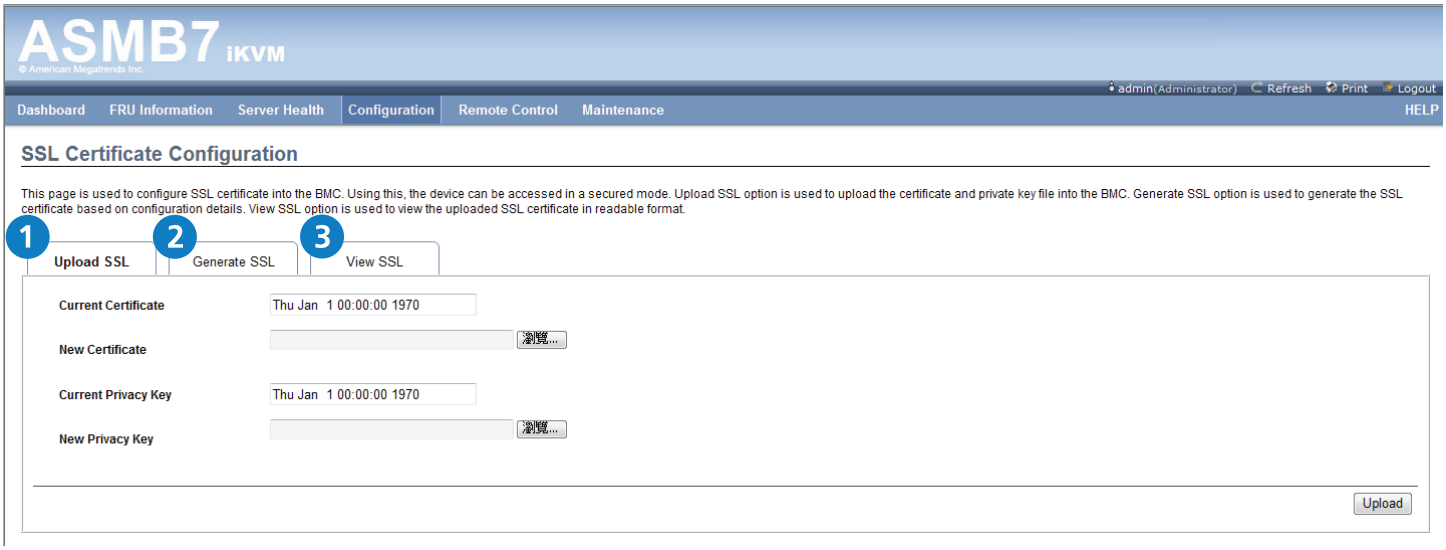
SMTP

The SMTP page allows you to configure SMTP mail server. Enter the IP address of the mail server, and then click **Save** to apply the settings.

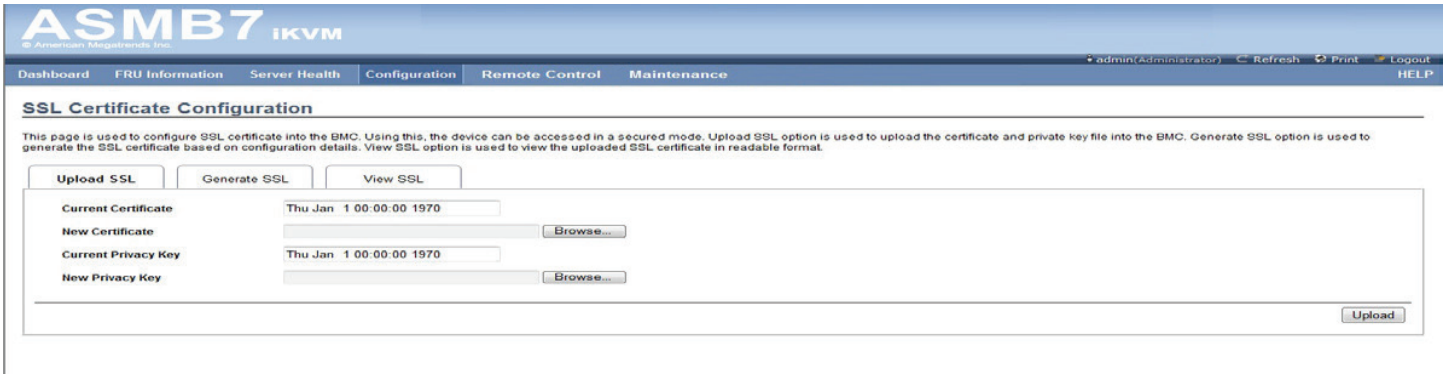


SSL

The Secure Socket Layer 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. To open SSL Certificate Configuration page, click Configuration > SSL from the main menu. There are three tabs in this page.



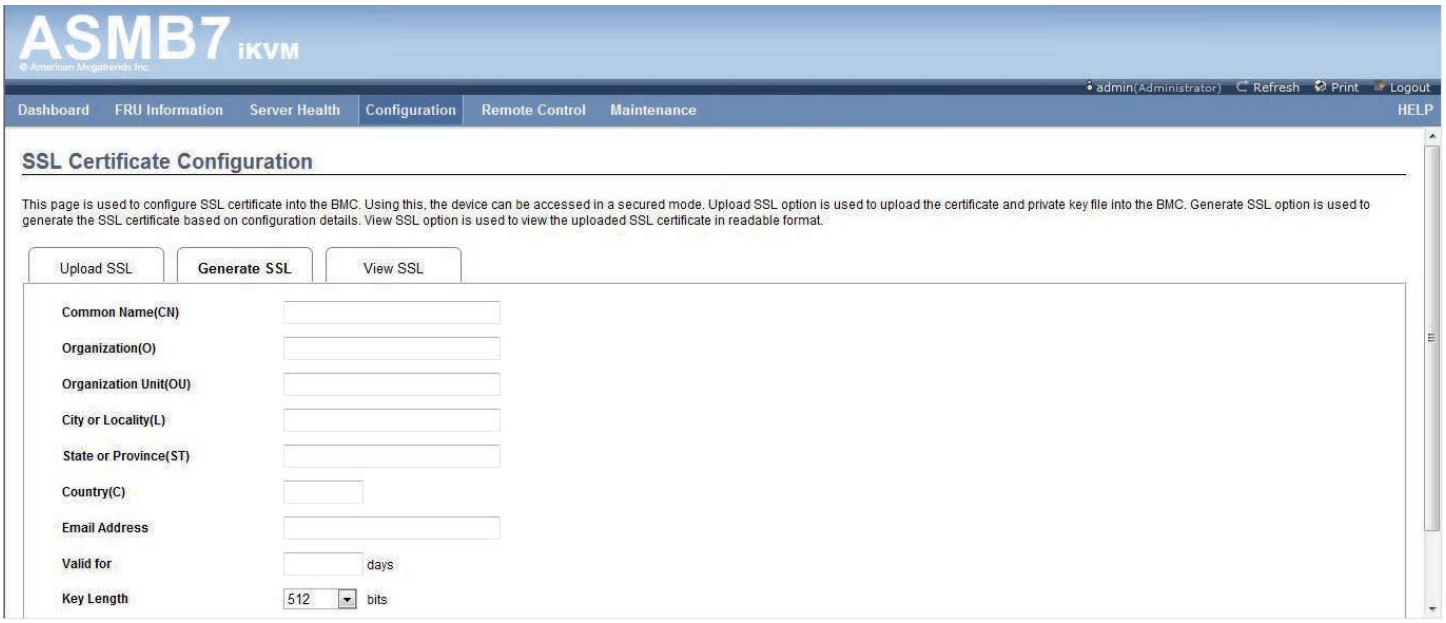
1. Upload SSL option is used to upload the certificate and private key file into the BMC.
2. Generate SSL option is used to generate the SSL certificate based on configuration details.
3. View SSL option is used to view the uploaded SSL certificate in readable format.



The fields of SSL Certificate Configuration – Upload SSL tab are explained below.

1. **Current Certificate:** Current certificate information will be displayed (read only).
2. **New Certificate:** Certificate file should be of pem type.
3. **Current Privacy Key:** Current privacy key information will be displayed (read-only).
4. **New Privacy Key:** Privacy key file should be of pem type.
5. **Upload:** To upload the SSL certificate and privacy key into the BMC

* Upon successful upload, HTTPS service will get restarted to use the newly uploaded SSL certificate



The fields of SSL Certificate Configuration – Generate SSL tab are explained below.

1. **Common Name(CN):** Common name for which certificate is to be generated

- Maximum length of 64 characters.
- Special characters '#' and '$' are not allowed.

2. **Organization(O):** Organization name for which the certificate is to be generated.

- Maximum length of 64 characters.

- Special characters '#' and '$' are not allowed.

3. **Organization Unit(OU):** Overall organization section unit name for which certificate is to be generated

- Maximum length of 64 characters.

- Special characters '#' and '$' are not allowed.

4. **City or Locality(L):** City or Locality of the organization (mandatory).

- Maximum length of 64 characters.

- Special characters '#' and '$' are not allowed.

5. **State or Province(ST):** State or Province of the organization (mandatory).

- Maximum length of 64 characters.

- Special characters '#' and '$' are not allowed.

6. **Country(C):** Country code of the organization (mandatory).

- Only two characters are allowed.

- Special characters are not allowed.

7. **Email Address:** Email Address of the organization (mandatory).

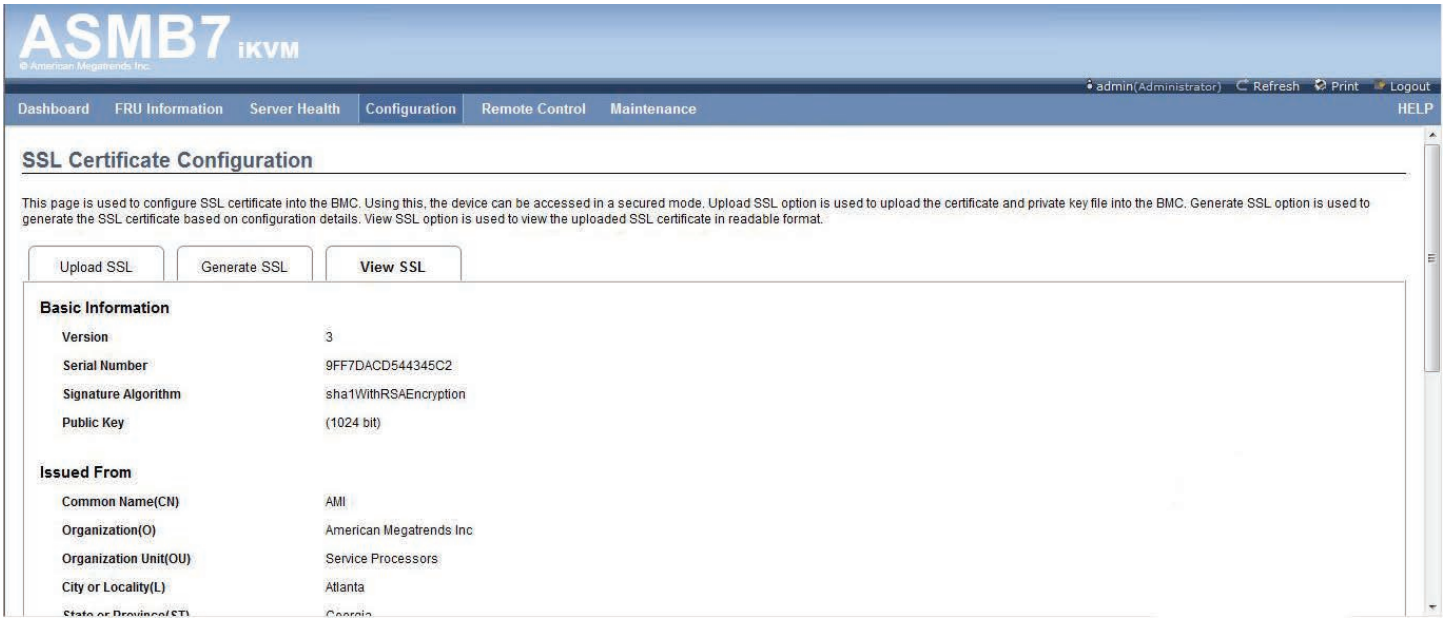
8. **Valid for:** Validity of the certificate

- Value ranges from 1 to 3650 days.

9. **Key Length:** The key length bit value of the certificate

10. **Generate:** To generate the new SSL certificate

* HTTPS service will get restarted, to use the newly generated SSL certificate



The fields of SSL Certificate Configuration – View SSL tab are explained below.

1. **Basic Information:** This section displays the basic information about the uploaded SSL certificate. It displays the following fields

- Version
- Serial Number
- Signature Algorithm
- Public Key

2. **Issued From:** This section describes the following Certificate Issuer information

- Common Name(CN)
- Organization(O)
- Organization Unit(OU)
- City or Locality(L)
- State or Province(ST)
- Country(C)
- Email Address

3. **Validity Information:** This section displays the validity period of the uploaded certificate

- Valid From
- Valid To

4. **Issued To:** This section display the information about the certificate issue.

- Common Name(CN)
- Organization(O)
- Organization Unit(OU)
- City or Locality(L)
- State or Province(ST)
- Country(C)
- Email Address

Procedure

1. Click the Upload SSL Tab, **Browse** the **New Certificate** and **New Privacy key**.
2. Click **Upload** to upload the new certificate and privacy key.
3. In **Generate SSL** tab, enter the following details in the respective fields:

- The **Common Name** for which the certificate is to be generated.
- The **Name of the Organization** for which the certificate is to be generated.
- The **Overall Organization Section Unit** name for which certificate to be generated.
- The **City** or **Locality** of the organization.
- The **State** or **Province** of the organization.
- The **Country** of the organization.

- The **email address** of the organization.
- The number of days the certificate will be valid in the **Valid For** field.

4. Choose the **Key Length** bit value of the certificate.
5. Click **Generate** to generate the certificate.
6. Click **View SSL** tab to view the uploaded SSL certificate in user readable format.

* Once you Upload/Generate the certificates, only HTTPS service will get restarted.

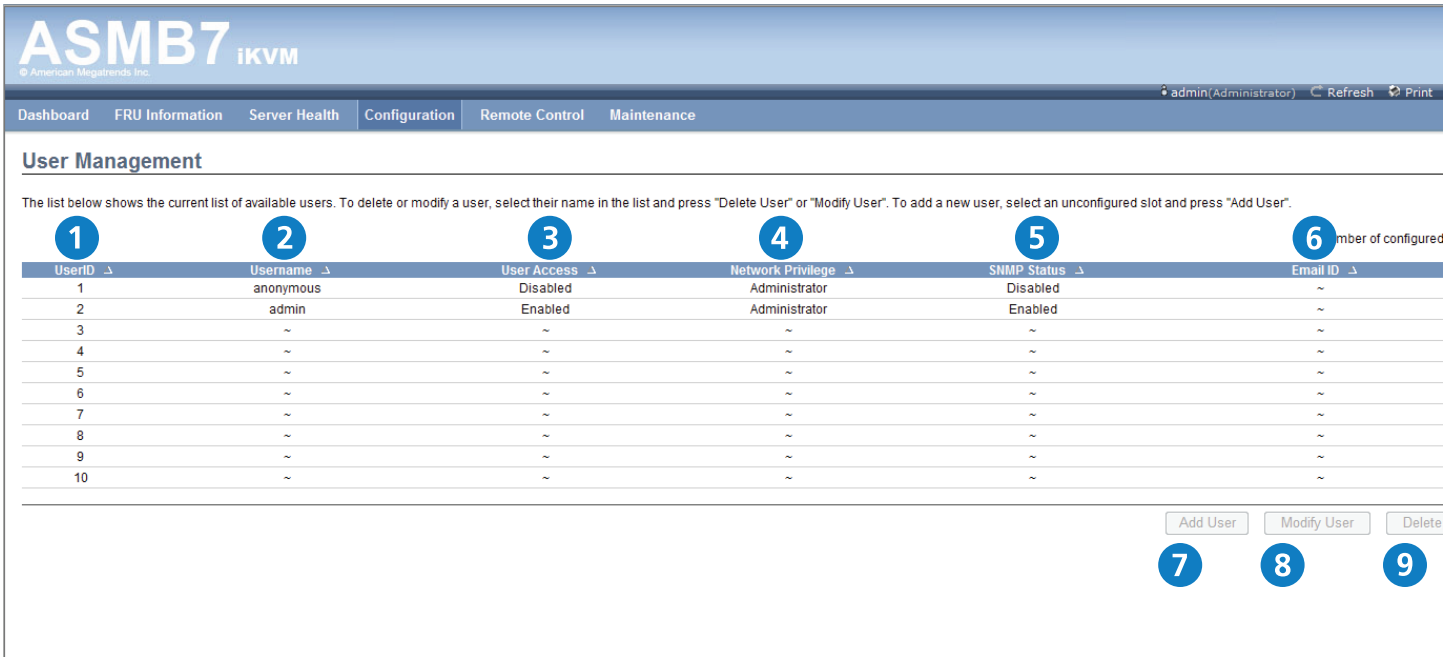
* You can now access your Generic MegaRAC® SP securely using the following format in your IP Address field from your Internet browser: https://<your MegaRAC® SP's IP address here>

* For example, if your MegaRAC® SP's IP address is 192.168.0.30, enter the following: https://192.168.0.30

* Please note the <s> after <http>.You must accept the certificate before you are able to access your Generic MegaRAC® SP

Users

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 User Management page, click **Configuration > User** from the main menu. A sample screenshot of User Management Page is shown in the screenshot below.



1. **User ID:** Displays the ID number of the user. Note: The list contains a maximum of ten users only.
2. **User Name:** Displays the name of the user.
3. **User Access:** To enable or disable the access privilege of the user.
4. **Network Privilege:** Displays the network access privilege of the user.
5. **SNMP Status:** Displays if the SNMP status for the user is enabled or disabled.
6. **Email ID:** Displays email address of the user.
7. **Add User:** To add a new user.

8. **Modify User:** To modify an existing user.
9. **Delete User:** To delete an existing user.

Add a new user:

1. To add a new user, select a free slot and click Add User.
2. Enter the name of the user in the User Name field.
3. In the Password and Confirm Password fields, enter and confirm your new password.
4. Password must be at least 8 characters long. White space is not allowed. This field will not allow more than 20 characters.
5. Enable or Disable the User Access Privilege.
6. In the Network Privilege field, enter the network privilege assigned to the user which could be Administrator, Operator, User or No Access.
7. Check the SNMP Status checkbox to enable SNMP access for the user. NOTE: Password field is mandatory, if SNMP Status is enabled.
8. Choose the SNMP Access level option for user from the SNMP Access drop-down list. Either it can be Read Only or Read Write.
9. Choose the Authentication Protocol to use for SNMP settings from the drop-down list. NOTE: Password field is mandatory, if Authentication protocol is changed.
10. Choose the Encryption algorithm to use for SNMP settings from the Privacy protocol drop-down list.
11. 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.

AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content shows sensor information, ex: Sensor type and Description.

Fixed-Subject Format: This format displays the message according to user's setting. You must set the subject and message for email alert.

12. In the **New SSK Key** field, click Browse and select the SSH key file. Note SSH key file should be of pub type.
13. Click **Add** to save the new user and return to the users list.
14. Click **Cancel** to cancel the modification and return to the users list.

Modify an existing User

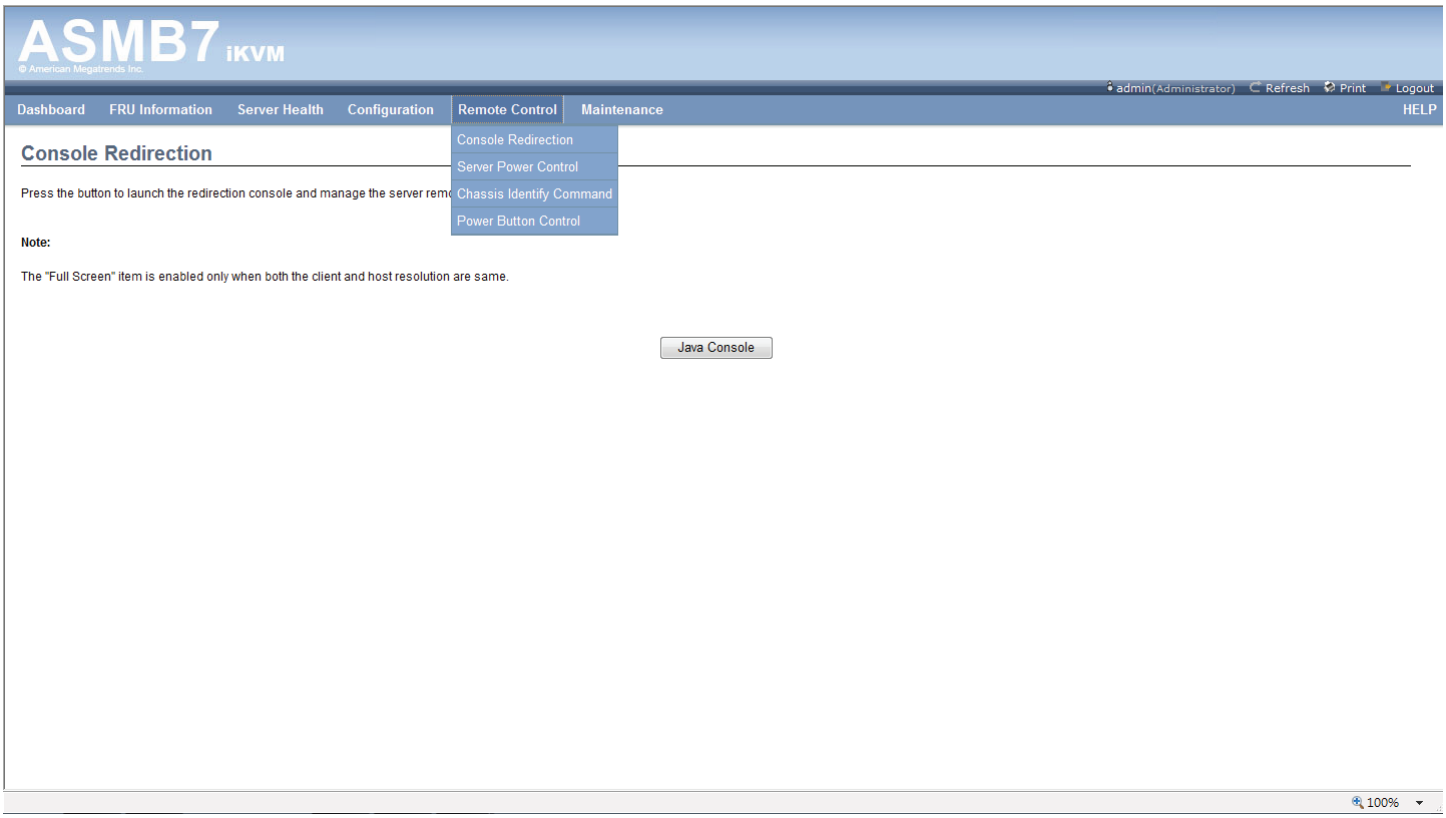
1. Select an existing user from the list and click Modify User. This opens the Add User screen.
2. Edit the required fields.
3. To change the password, enable the Change Password option.
4. After editing the changes, click Modify to return to the users list page.

Delete an existing User

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

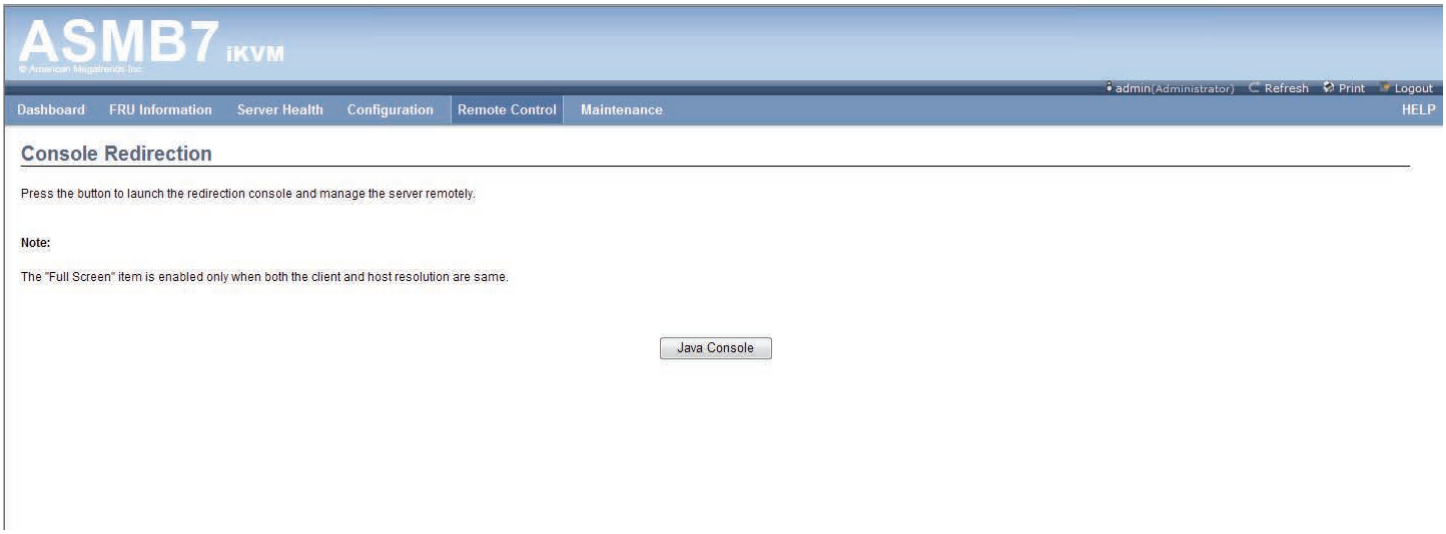
3.4 Remote Control

This section allows you to perform remote operations on the server. Click each function key to start using its specific function.



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.



Browser Settings

For launching the KVM, pop-up blocker 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 Java Console can be launched in two ways:

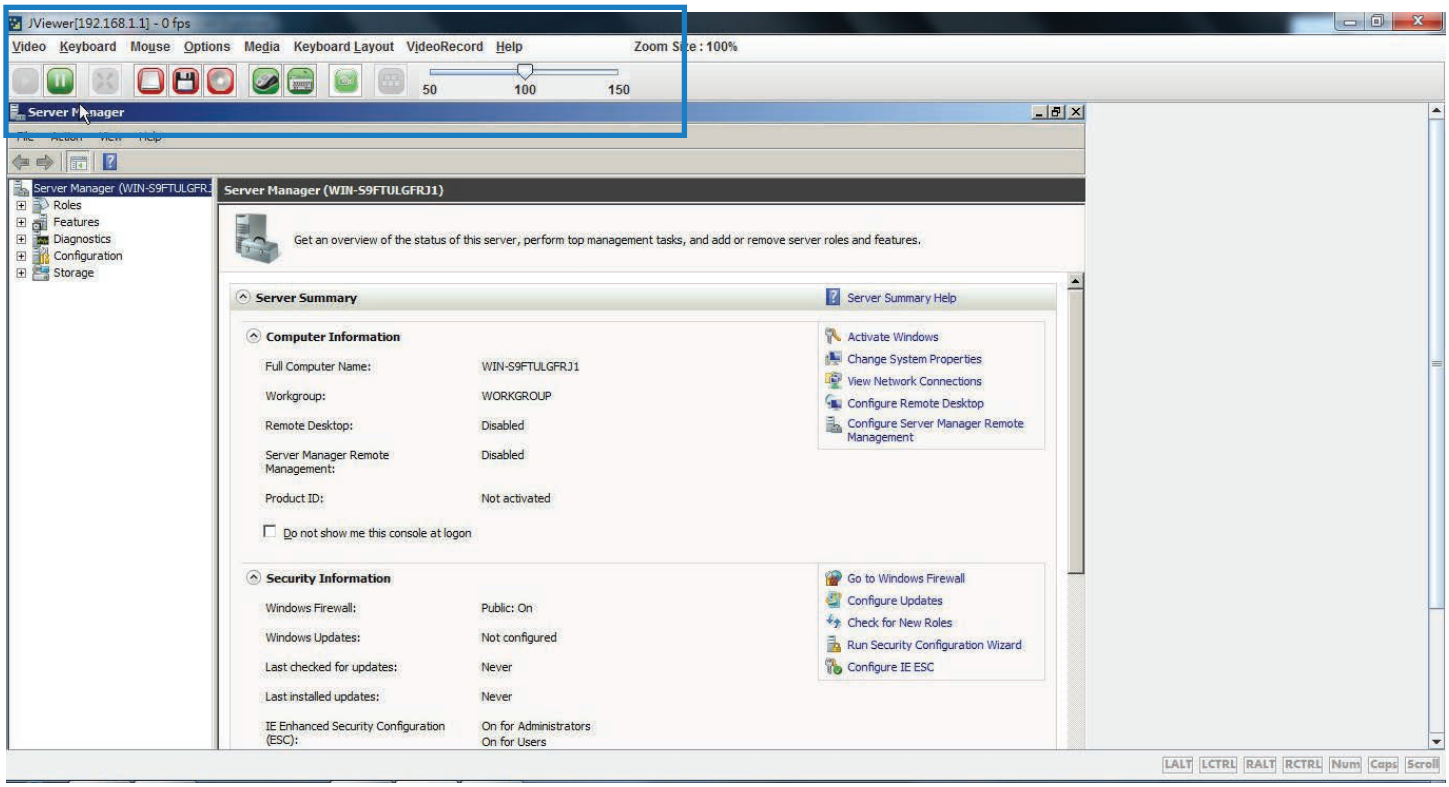
1. Open the Dashboard Page and in Remote control section, click Launch for Java Console.
2. Open **Remote Control>Console Redirection** Page and click **Java Console**. This will download the .jnlp file from BMC.

To open the **.jnlp** file, use the appropriate JRE version (Javaws) When the downloading is done, it opens the Console Redirection window.

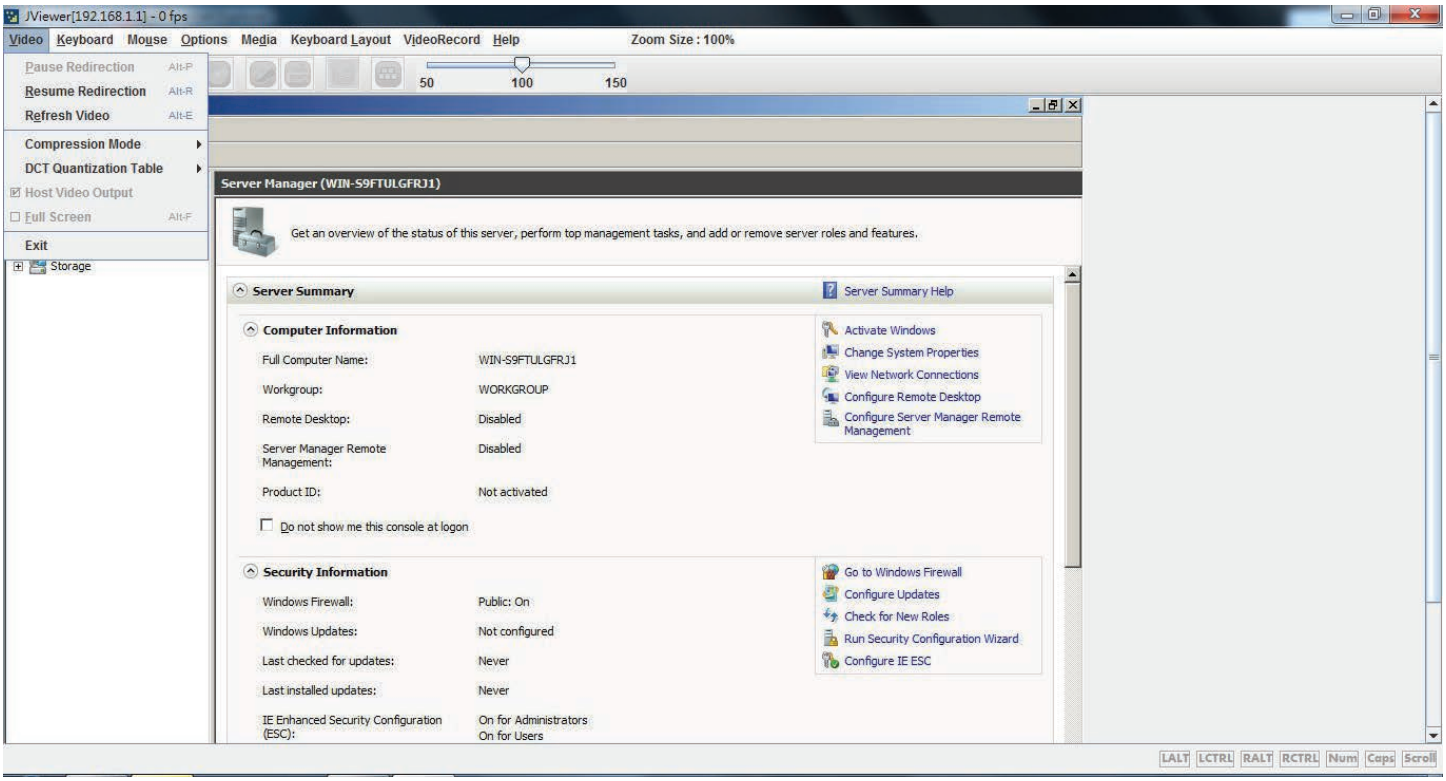
The Console Redirection main menu consists of the following menu items:

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

A detailed explanation of these menu items is given below.



Video



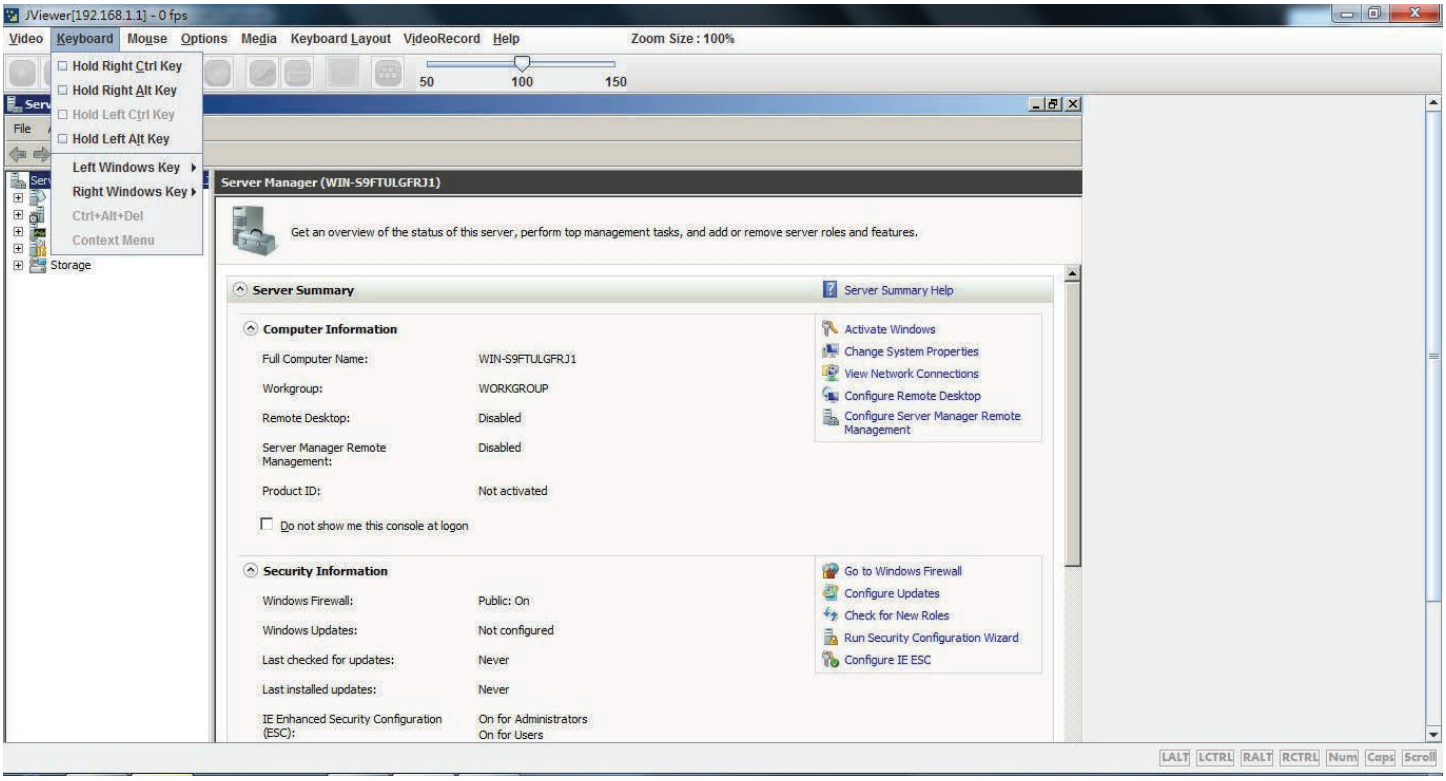
This menu contains the following sub menu items:

1. **Pause redirection:** This option is used for pausing Console Redirection.
2. **Resume Redirection:** This option is used to resume the Console Redirection when the session is paused.
3. **Refresh Video:** This option can be used to update the display shown in the Console Redirection window.
4. **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.
5. **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.
6. **Exit:** This option is used to exit the Console Redirection screen.

Keyboard

This menu contains the following sub menu items.

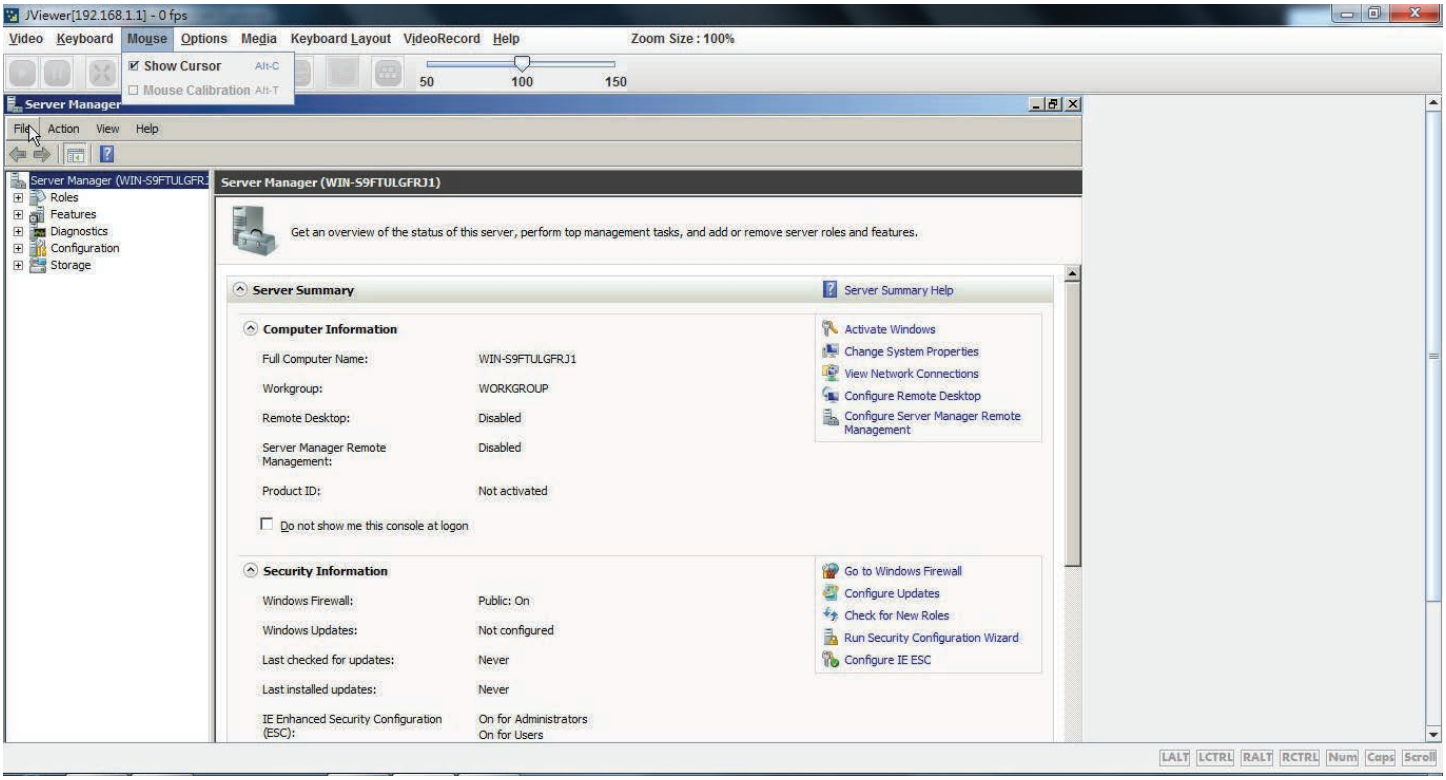
1. Hold Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.
2. Hold Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.
3. Hold Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.
4. Hold Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.
5. 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.
6. 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.
7. 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.
8. Context menu: This menu item can be used to act as the context menu key, when in Console Redirection.



Mouse

1. Show Cursor: This menu item can be used to show or hide the local mouse cursor on the remote client system.
2. Mouse Calibration: This menu item can be used only if the mouse mode is relative.

In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be synchronized in the beginning. Please use '+' or '-' keys to change the threshold settings until both the cursors go out of synch. Please detect the first reading on which cursors go out of synch. Once this is detected, use 'ALT-T' to save the threshold value.



Options

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

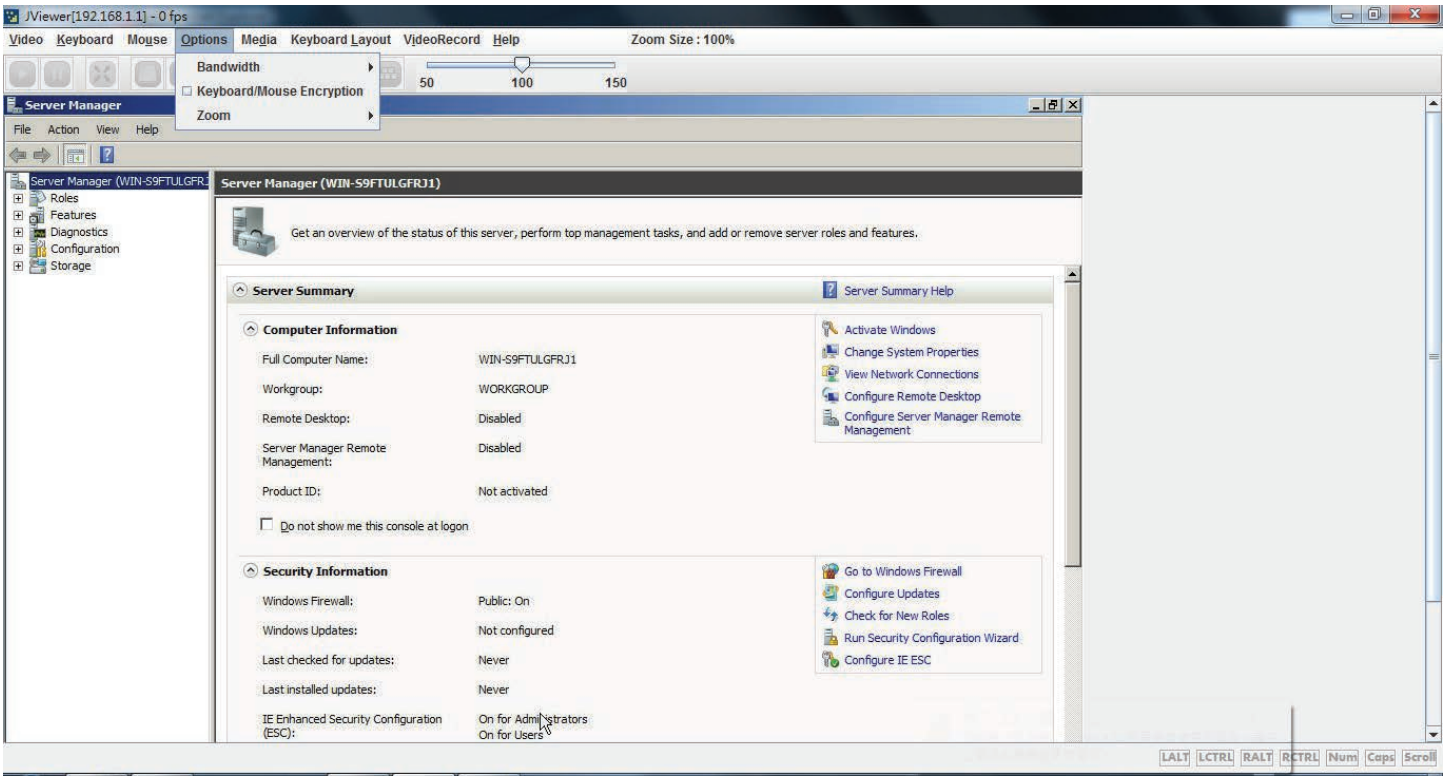
1. Auto Detect: This option is used to detect client system keyboard layout automatically and send the key event to the host based on the Layout detected.
2. 256 Kbps
3. 512 Kbps
4. 1 Mbps
5. 10 Mbps

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

Zoom:

This option is available only when you launch the Java Console.

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



Media

Virtual Media Wizard:

To add or modify a media, select and click 'Virtual Media Wizard' button, which pops out a box named "Virtual Media" where you can configure the media. A sample screenshot of Virtual media screen is given below. Virtual Media.

Floppy Key Media:

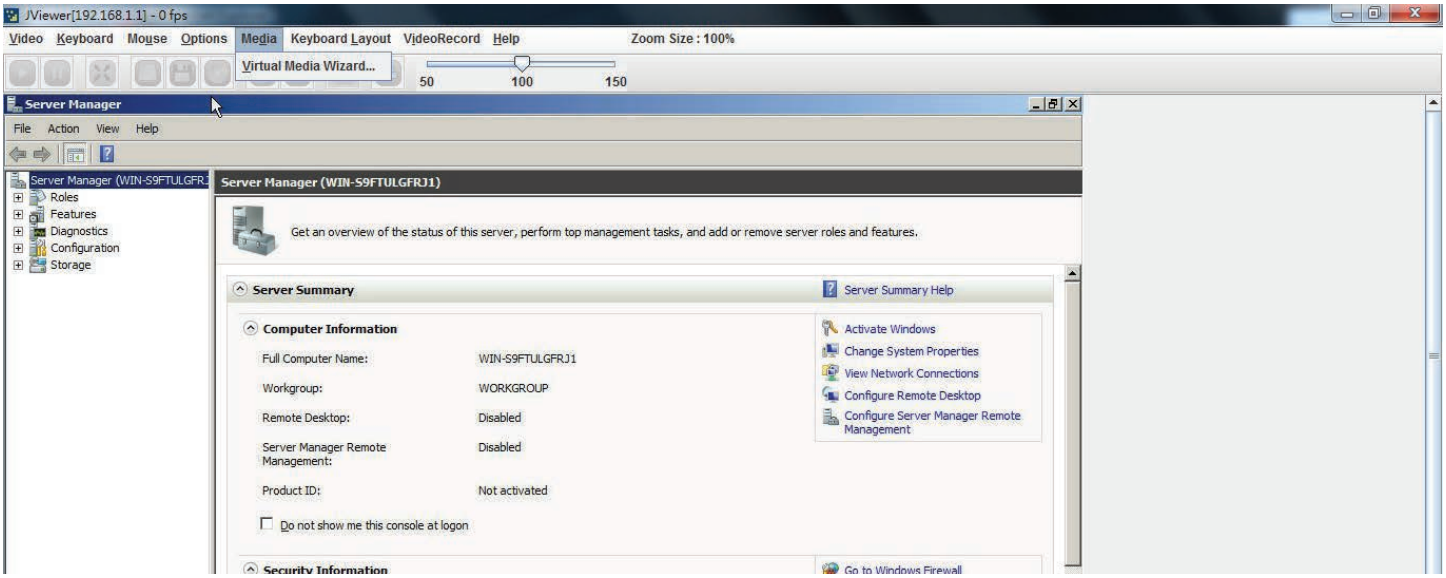
This menu item can be used to start or stop the redirection of a physical floppy drive and floppy image types such as img.

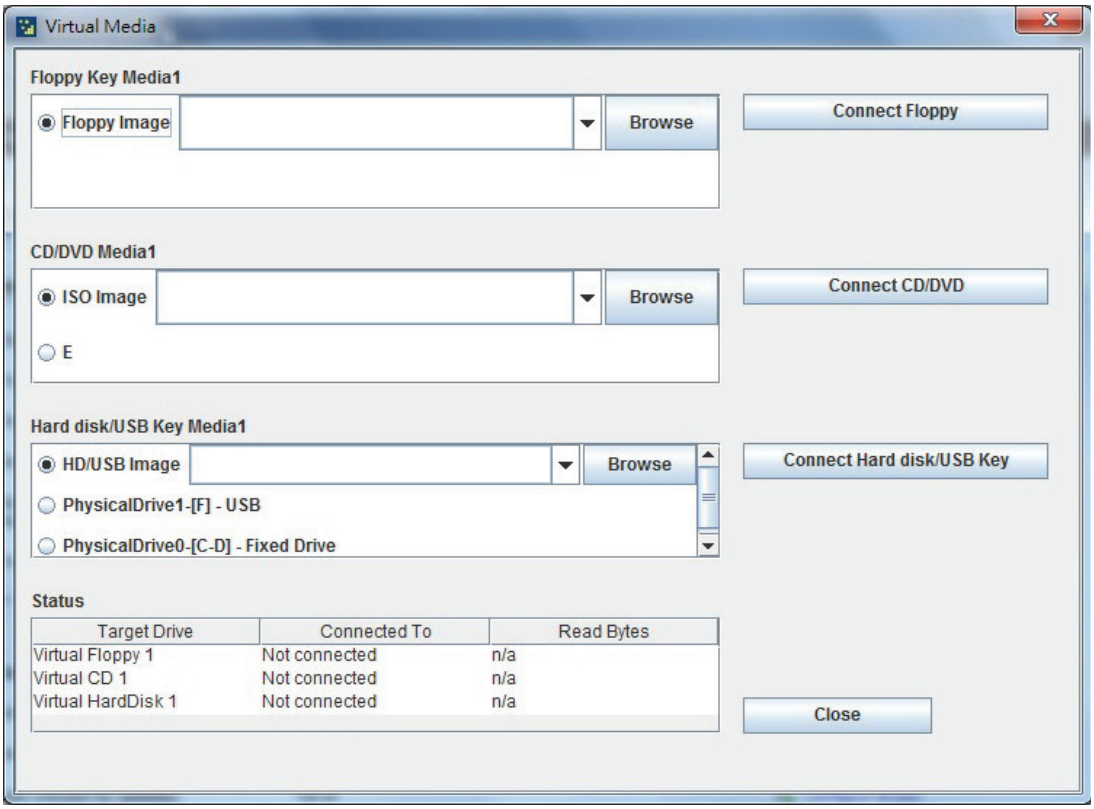
CD/DVD Media:

This menu item can be used to start or stop the redirection of a physical DVD/CD-ROM drive and cd image types such as iso.

Hard disc/USB Key Media:

This menu item can be used to start or stop the redirection of a Hard Disk/USB key image and USB key image such as img.

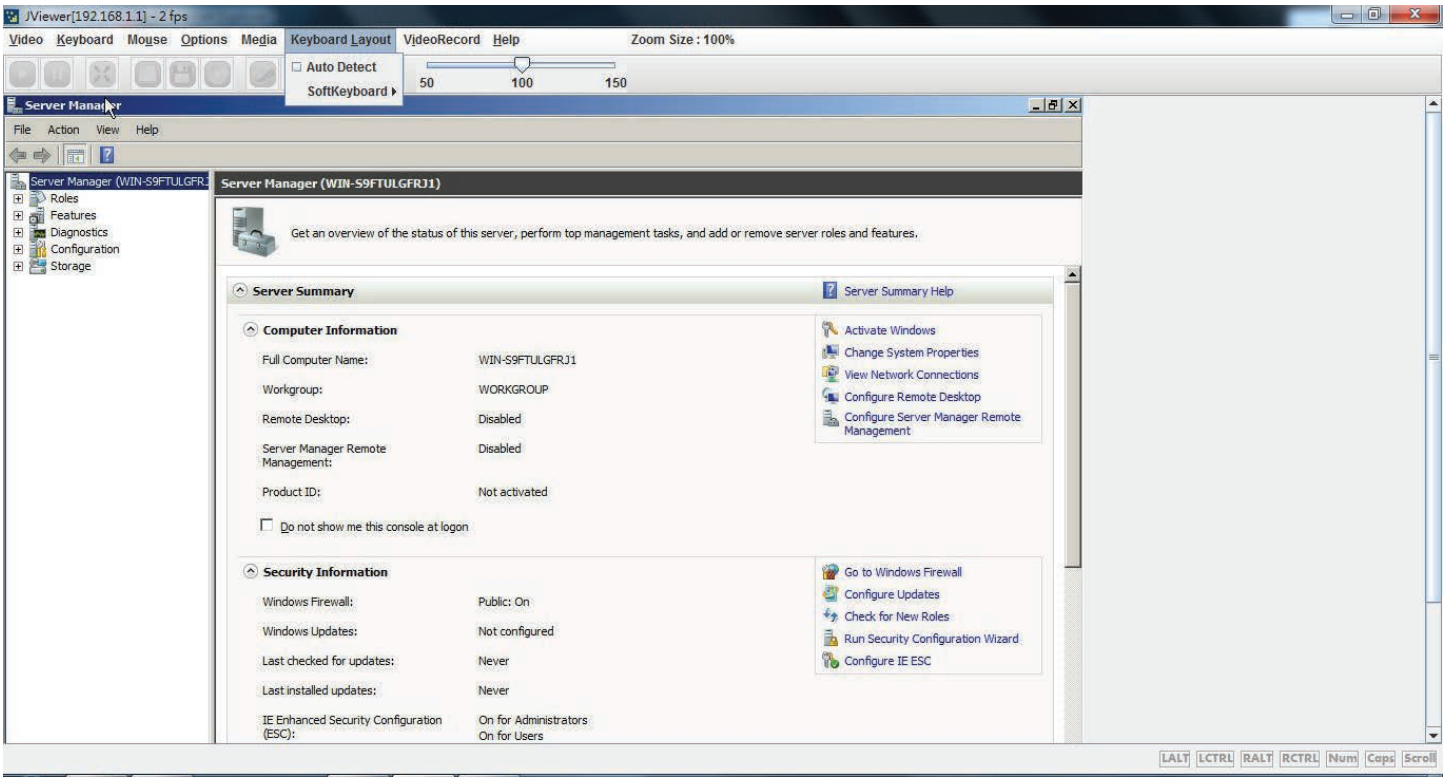




Keyboard Layout

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

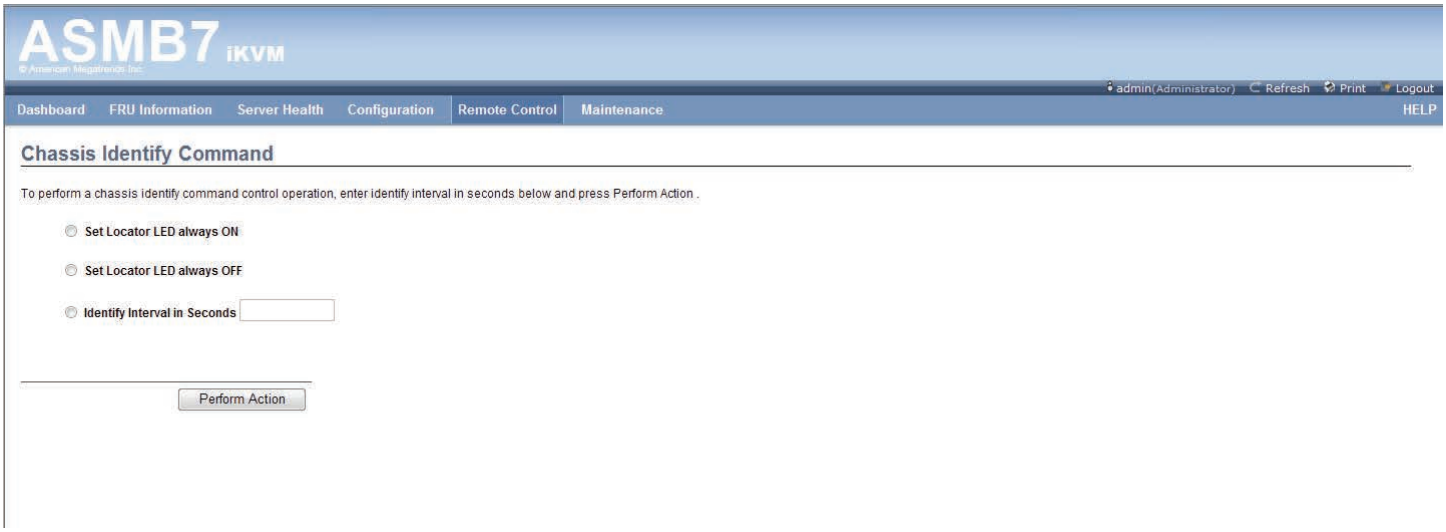


Server Power Control

The Server Power Control page displays the current server power status and allows you to change the current settings. Select the desired option, and then click **Perform Action** to execute the selected action.

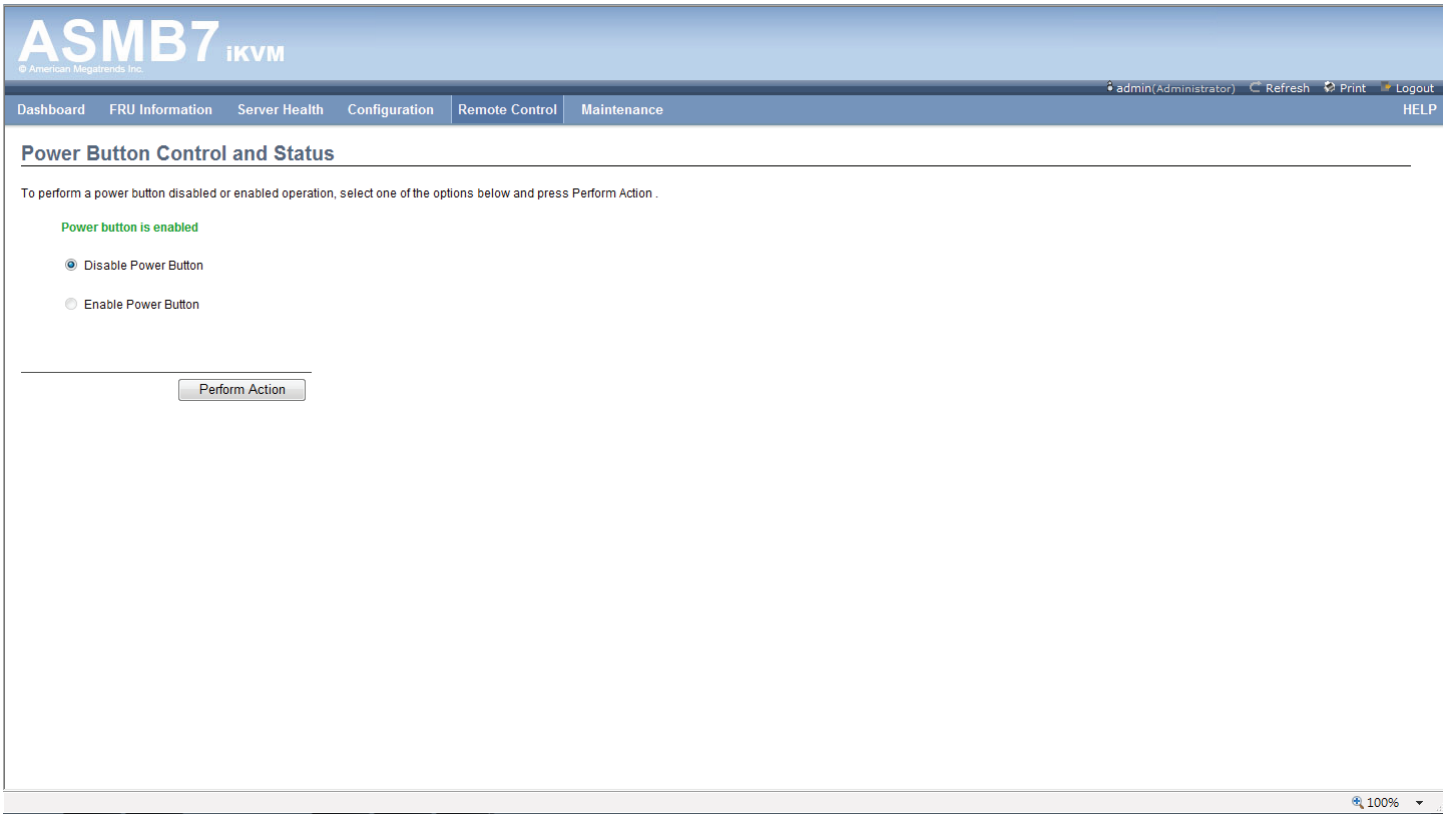
Chassis Identify Command

The Chassis Identify Command page allows you to perform a chassis identify command control operation. Enter identify interval in seconds, and then click **Perform Action** to start the command.



Power Button

The Power Button page allows you to enable or disable power button and click **Perform Action** to confirm the selection.

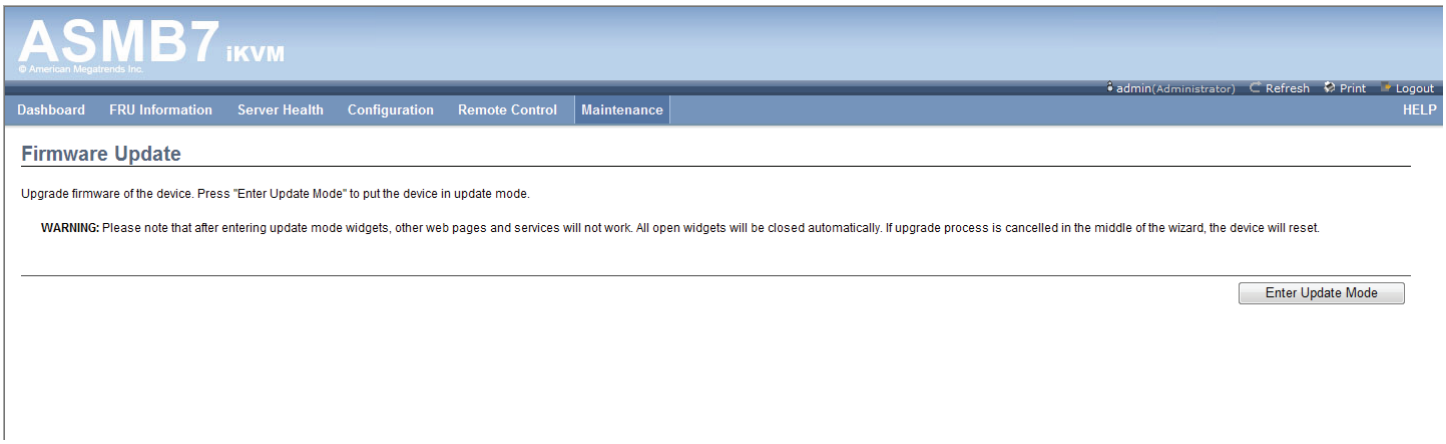


3.5 Maintenance

This section allows you to perform the firmware update for the remote server. You can also use **Restore Factory Defaults** to reset system settings.

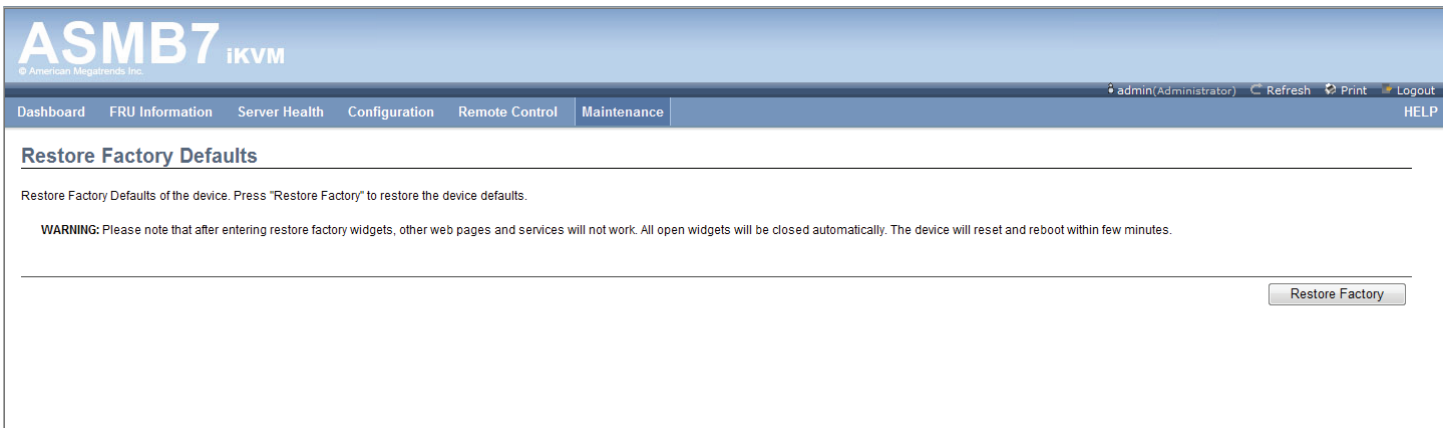
Firmware Update

This section allows you to enter the update mode, and update the firmware of ASMB7. Please note that after entering update mode widgets, other web pages and services will not work. All oopen widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will reset.



Restore Factory Default

This section allows you to restore all settings to factory default. Please click the Restore Factory to reset all settings.



Chapter 4
Troubleshooting

4.1 Troubleshooting

Problem	Solution
The local/central server cannot connect to the ASMB7-iKVM board	1. Check if the LAN cable is connected to the LAN port. 2. Make sure that the IP address of both the remote and local/central servers are on the same subnet. (Refer to chapter 2 for details.) Try "ping xx.xx.xx.xx" (remote server ip) on local/central server and make sure remote server could reply the ping request. 3. Check if the IP source is set to [DHCP]. When set to [DHCP], you'll not be able to configure the IP address.
All the SEL (System Event Log) cannot be displayed	The maximum SEL number is 900 events.
The date/time shown in SEL (System Event Log) screen is incorrect	Refer to section 4.4.9 to check if the time zone is set up correctly.
ASMB7-iKVM has network connection problems in Firewall environment	Ask MIS to add the following port numbers in Firewall: 5123 (virtual floppy) (TCP) 5120 (virtual CDROM) (TCP) 623 (IPMI) (TCP & UDP) 80 (HTTP) (TCP) 7578 (iKVM) (TCP) 443 (HTTPs) (TCP) 161 (SNMP) (UDP)
The Java redirection screen cannot be displayed normally	Click Refresh Page button to refresh the redirection screen.

* The ASMB JAVA console only works with the onboard VGA. Other add-on video cards may not properly display the ASMB JAVA console.

4.2 Sensor Table

Memory ECC

Sensor No.	Sensor Name	Sensor Type	Sensor Type code	Sensor Value or Event Type	Event Data 3
0xD1	CPU1_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03:DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0B: DIMM_C4, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x0F: DIMM_D4
0xD2	CPU1_ECC2	OEM Memory ECC Sensor (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	0xC1	Discrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_A1, 0x01: DIMM_A2, 0x02: DIMM_A3, 0x03:DIMM_A4, 0x04: DIMM_B1, 0x05: DIMM_B2, 0x06: DIMM_B3, 0x07: DIMM_B4, 0x08: DIMM_C1, 0x09: DIMM_C2, 0x0A: DIMM_C3, 0x0B: DIMM_C4, 0x0C: DIMM_D1, 0x0D: DIMM_D2, 0x0E: DIMM_D3, 0x0F: DIMM_D4
0xD3	CPU2_ECC1	Memory ECC Sensor	0x0C	Discrete(0x6F) 0x01: Correctable ECC 0x02: Uncorrectable ECC 0x40: Presence detected	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05:DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_C1, 0x15: DIMM_C2, 0x16: DIMM_C3, 0x17: DIMM_C4
0xD4	CPU2_ECC2	OEM Memory ECC Sensor (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	0xC1D	iscrete(0x6F) 0x01: Read ECC error 0x02: ECC Error occurred on a scrub 0x04: Write Parity Error 0x08: Error in Redundant memory 0x10: Sparing Error 0x20: Memory access out of Range 0x40: Address Parity Error 0x80: Byte Enable Parity	0x00: DIMM_D1, 0x01: DIMM_D2, 0x02: DIMM_D3, 0x03: DIMM_D4, 0x04: DIMM_E1, 0x05:DIMM_E2, 0x06: DIMM_E3, 0x07: DIMM_E4, 0x08: DIMM_F1, 0x09: DIMM_F2, 0x0A: DIMM_F3, 0x0B: DIMM_F4, 0x0C: DIMM_G1, 0x0D: DIMM_G2, 0x0E: DIMM_G3, 0x0F: DMM_G4, 0x10: DIMM_H1, 0x11: DIMM_H2, 0x12: DIMM_H3, 0x13: DIMM_H4, 0x14: DIMM_C1, 0x15: DIMM_C2, 0x16: DIMM_C3, 0x17: DIMM_C4

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x68	Backplane1 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x69	Backplane1 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6A	Backplane1 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6B	Backplane1 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6C	Backplane1 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6D	Backplane1 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6E	Backplane1 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x6F	Backplane1 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x78	Backplane2 HD1	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x79	Backplane2 HD2	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7A	Backplane2 HD3	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7B	Backplane2 HD4	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7C	Backplane2 HD5	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7D	Backplane2 HD6	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7E	Backplane2 HD7	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild
0x7F	Backplane2 HD8	Drive Slot	0x0D	Discrete(0x6F) 0x01: Drive Presence 0x02: Drive Fault 0x80: Rebuild

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x81	PSU1 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critital - going high
0x82	PSU1 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x83	PSU1 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x92	PSU1 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x93	PSU1 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x94	PSU1 AC	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x95	PSU1 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x96	PSU1 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x97	PSU1 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected
0x84	PSU2 Temp	Temperature	0x01	Threshold(0x01) Upper Non-Critical - going high Upper Critital - going high
0x85	PSU2 Fan1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x86	PSU2 Fan2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x9A	PSU2 Over Temp	Temperature	0x01	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9B	PSU2 FAN Low	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe
0x9C	PSU2 AC Lost	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x08: Power Supply input lost (AC/DC)
0x9D	PSU2 Slow FAN1	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9E	PSU2 Slow FAN2	FAN	0x04	Discrete(0x07) 0x01: Transition to OK 0x10: Transition to Non-Critical from more severe 0x40: Transition to Non-Recoverable
0x9F	PSU2 PWR Detect	Power Supply	0x08	Discrete(0x6F) 0x01: Presence Detected 0x02: Power Supply Failure Detected

Sensor No.	Sensor Name	Sensor Type	Sensor Type Code	Sensor Value or Event Type
0x31	CPU1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x32	CPU2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCC	TR1 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0xCD	TR2 Temperature	Temperature	0x01	Threshold(0x01) Upper Non-critical - going high Upper Critical - going high
0x34	VCORE1	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x35	VCORE2	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x36	+3.3V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x37	+5V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x38	+12V	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x39	+1.5V_ICH (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3A	+1.1V_IOH (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3B	+5VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3C	VBAT	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3D	P1VTT (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x3E	+1.5V_P1DDR3 (For Intel platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high

0x3F	P2VTT (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x40	+3.3VSB	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x41	+1.5V_P2DDR3 (For Intel DP platform only -- ASUS Z8 series server MB; -E6 server system)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	P1DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x42	+1.5V (For Intel UP platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x43	P2DDR3 (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x44	P1_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x45	P2_+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x46	P1_VDDNB (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x47	+1.8V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x48	+1.2V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x49	+1.1V (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0x4A	VTT (For AMD platform only)	Voltage	0x02	Threshold(0x01) Lower Non-critical - going low Lower Critical - going low Upper Non-critical - going high Upper Critical - going high
0xA0	CPU_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA1	CPU_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low

0xA2	FRNT_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA3	FRNT_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA4	FRNT_FAN3	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA5	FRNT_FAN4	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA6	REAR_FAN1	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA7	REAR_FAN2	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA8	FRNT_FAN5	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xA9	FRNT_FAN6	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0xAA	FRNT_FAN7	FAN	0x04	Threshold(0x01) Lower Non-critical - going low Lower Critital - going low
0x4F	Chassis Intrusion	Physical Security (Chassis Intrusion)	0x05	Discrete(0x6F) 0x01: General Chassis Intrusion 0x02: Drive Bay Intrusion