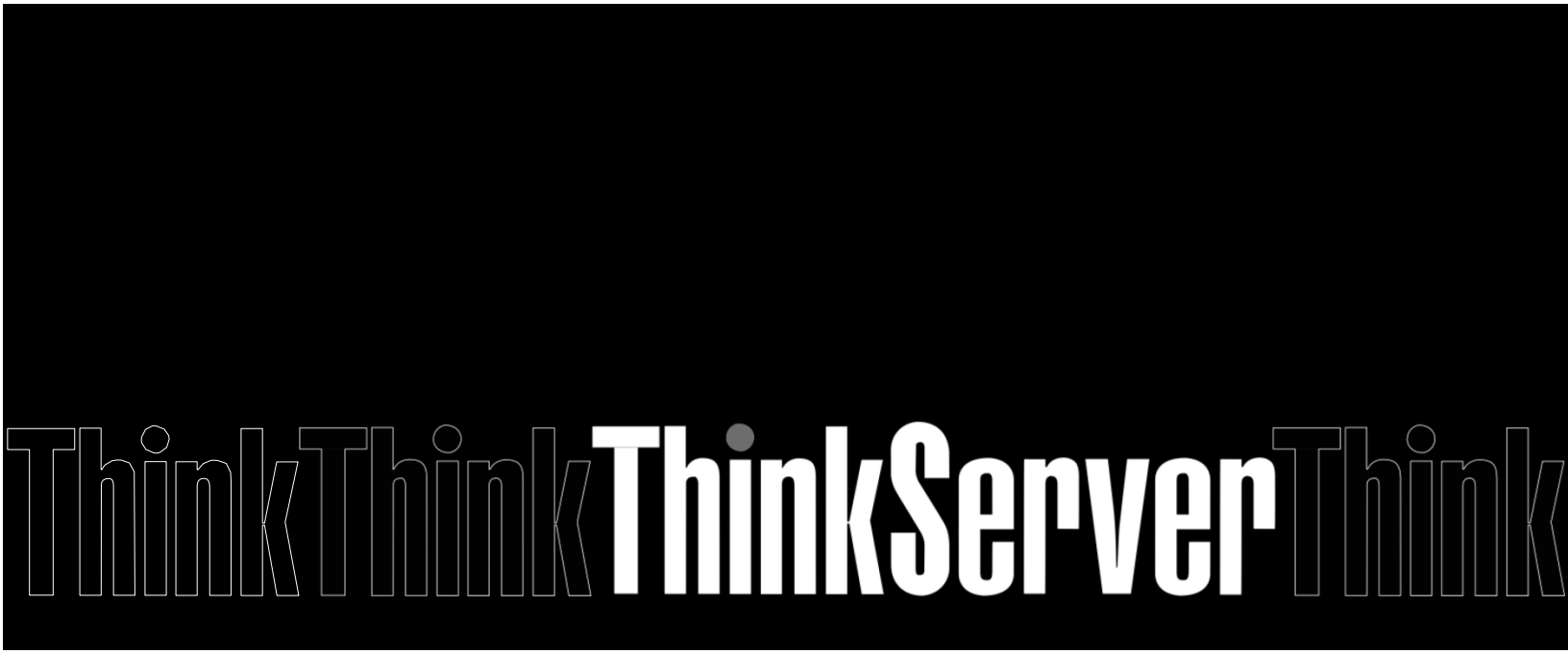
Lenovo

ThinkServer Management Module User Guide



NOTE: Before using the information and the product it supports, be sure to read and understand "Appendix A Notices".

First Edition (June 2016)

Date	Version	Description
June-08-2016	*v0.1*	*Preliminary draft*
July-01-2016	*v0.2*	*1. Modify Logo* *2. Modify "Contents", chapter 4, chapter 5*
July-15-2016	*v0.3*	*1. Modify chapter 5*
July-26-2016	*v0.4*	*1. Modify chapter 5* *2. Add chapter 6*
August-04-2016	*v0.5*	*1. Modify chapter 5*
August-25-2016	*v0.6*	*1. Modify chapter 5*
September-22-2016	*v0.7*	*1. Modify chapter 5*
October-06-2016	*v0.8*	*1. Modify chapter 5*
October-20-2016	*v0.9*	*1. Modify chapter 5* *2. Modify chapter 6*
October-27-2016	*v1.0*	*1. Modify chapter 5*
November-04-2016	*v1.1*	*1. Modify chapter 5*
November-11-2016	*v1.2*	*1. Modify chapter 5*
November-17-2016	*v1.3*	*1. Modify chapter 5*
November-18-2016	*v1.4*	*1. Modify chapter 3* *2. Modify chapter 5*
December-02-2016	*v1.5*	*1. Modify chapter 5*
December-09-2016	*v1.6*	*1. Modify chapter 5 (Image Redirection)*
December-16-2016	*v1.7*	*1. Modify chapter 5*

December-22-2016	*v1.8*	*1. Modify chapter 5*
December-30-2016	*v1.9*	*1. Modify chapter 5(FRU Information)*
January-06-2017	*v2.0*	*1. Modify chapter 5(Interfaces, NTP)*
January-13-2017	*v2.1*	*1. Modify Chapter 5 (System Firewall, Remote Session, Services, SNMP, SSL, Users)*
January-20-2017	*v2.2*	*1. Modify Chapter 5 (System Firewall, Users, Recorded Video, Firmware Update, BIOS Update)*
February-17-2017	*v2.3*	*1. Modify Chapter 5 (Dashboard)*
March-10-2017	*v2.4*	*1. Modify a note in Chapter 3.*
March-17-2017	*v2.5*	*1. Add a note in Chapter 3.*
May-05-2017	*v2.6*	*1. Add a note in Chapter 5 (Console Redirection).* *2. Modify Chapter 5 (Users).*

Contents

Chapter 1. Introduction

Welcome to “Lenovo ThinkServer Management Module (TMM)” User Guide. For simplicity, in the next sections, the term “TMM” will refer to “Lenovo ThinkServer Management Module”.

This User Guide describes how to use the TMM on RS160, the overview of the module features and how to set up and operate the module.

The User Guide is for system administrators responsible for configuring, upgrading, and maintaining the TMM. As a system administrator once you are familiar with the User Guide, you can access the TMM remotely from any location to respond to emergencies. If further assistance is required, please, proceed to the Lenovo support web site.

Some screenshots in this document may be not same as the actual TMM UI, they’re only for reference.

Terminology

The following table lists the terms that are used in this document and its corresponding descriptions.

Abbreviation	Definition
AD	Active Directory
BIOS	Basic Input Output System
BMC	Baseboard Management Controller
CPLD	Complex Programmable Logic Device
DCMI	Data Center Manageability Interface
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual-Inline-Memory-Modules
DNS	Domain Name Service
FRU	Field Replaceable Unit
FQDN	Fully Qualified Domain Name
IP	Internet Protocol
IPMI	Intelligent Platform Management Interface
KVM	Keyboard, Video, and Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Controller

ME/NM	Node Manager
NCSI	Network Communication Services Interface
NFS	Network File System
NIC	Network Interface Controller
Nsupdate	Direct Dynamic DNS
NTP	Network Time Protocol
PEF	Platform Event Filter
POST	Power On Self Test
PSU	Power Supply Unit
RAID	Redundant Arrays of independent Disks
RADIUS	Remote Authentication Dial In User Service
SEL	System Event Log
SMASH	Systems Management Architecture for Server Hardware
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOL	Serial Over LAN
SSH	Secure Shell
SSL	Secure Sockets Layer
TCP/IP	Transfer Control Protocol/Internet Protocol
TDM	ThinkServer Deployment Manager
TMM	ThinkServer Management Module
TSIG	Transaction Signature
USB	Universal Serial Bus
VLAN	Virtual Local Area Network

Safety information

WARNING

With reference to either the Guide or other documents, you should always pay particular attention to safety information before operating the ThinkServer. To ensure full compliance with the existing certification and licensing, you must follow the installation instructions in the Guide.

Power on/off: the power button does not disable TMM power. To disable the TMM, you must disconnect the AC power cord from the power outlet. When opening the chassis to install or remove the parts, you should make sure the AC power cord has been disconnected.

Chapter 2. Overview of the Lenovo TMM

This topic describes the features of the TMM. The TMM has an embedded operating system that is integrated in the ThinkServer. Independent of the server operating system, the embedded operating system can provide a whole set of complete, stable and effective solutions for the server. As a system administrator, you can manage the server remotely through the network and view system event log messages.

Features of the TMM

The TMM is accessed through a network connection and if a remote KVM is installed, the user can remotely connect to an operating system, Embedded with remote access and related control software.

Key features of the TMM are as follows:

- Embedded Web UI - Remote power on/off, system health, system information, alert notification and event log.
- Security - open source SSL
- Compatible with IPMI V2.0
- KVM - allow remote viewing and configuring in the POST and the BIOS setup utility
- Supports Platform deployment management
- Supports SNMP using both IPv4 and IPv6.
- Supports the NTP client.
- Supports USB redirection/ Remote Media (Virtual Media).
- Supports Extended SEL.
- Supports LDAP and LDAPS.
- Support Email alert for log notification via SMTP.
- Supports TMM and BIOS.
- Supports SMASH

Chapter 3. Configuring of the TMM

This topic describes how to use the server configuration utility to configure the TMM. When first installed, the TMM by default will search the DHCP server on the network to automatically assign an IP address, subnet mask and gateway. It is recommended that users manually set a fixed IP address in the BIOS.

To set an IP address, do the following:

1. Press F1 as soon as you see the Lenovo logo screen.
2. From the BIOS setup menu, select Server management →Network Settings →Configuration Address Source.
3. From the Configuration option, you can choose Static or DHCP to set the IP address.
4. When you finish the configuration, save the settings.

Table1.IPMI 2.0 Configuration submenu

Configuration Address Source	**Static**	Static IP configuration. IP and the subnet mask can be set manually
	DHCP	Dynamic IP configuration. System can obtain IP automatically

System requirements

Supported Browsers:

- Chrome
- Firefox
- Internet Explorer

To use the Virtual Console, you must also have the Java Run-Time Environment (JRE) properly installed and working, including the Java plugin for your preferred Web browser. Depending on the JRE version installed, you may need to lower your Java security to run the Virtual Console.

Note: There is another window will appear if you choose allow pop-up which is used to confirm the exception site when use Firefox.

Note: There is a pop-up in login page when use Firefox if you choose allow pop-up. It's caused by Firefox so please don't use and turn off.

Note: The preview box of remote console is dependent on NPAPI (technology required for Java applets) plugin. If the browser does not support NPAPI plugin, the preview box will be not available.

Supported Java :

- Java 1.8.0_77 for KVM/VM

Chapter 4. TMM Quick Start

Connecting to the TMM

The TMM has an embedded Web server and an application with multiple standard interfaces. This topic describes these interfaces and their usages. You can use the TCP/IP protocol to access these interfaces.

For more information about the initial settings, see Chapter 3 “Configuring of the TMM” on page 7. The default user name and password are as follows:

- Username = lenovo
- Password = len0vO

The TMM is accessible through standard Java-enabled Web browsers with HTTPS, and accessing the TMM via the HTTPS protocol, the browser may prompt you to trust and install the security digital certification. Just follow the prompts to import and confirm the certification.

Logging on

To log on to the TMM, please do following:

1. Enter the IP address assigned by the TMM into the Web browser.
   For example:
   http://10.99.87.131/
   For secure connection, refer to the following example: https://10.99.87.131/
   The web browser will then be directed to the logon page of the TMM.
2. On the logon page of the TMM, enter the user name and password. For example:
   - Username = lenovo
   - Password = len0vO
3. Click **Sign in** to view the home page of the TMM.

Navigation

When you have successfully logged on to the TMM, the TMM dashboard is displayed. You can select the left or right arrows to navigate between dashboard pages. The information and tasks found on each dashboard page is listed in the following table.

Table 2 . Properties on the TMM dashboard

	Comments
Dashboard	This dashboard contains the following information: • **Device Information** • **Network Information** • **Location LED status** • **Remote Control Preview Box** • **Sensor Monitoring** • **Event Log summary**

Refresh

You can reload current page at any time by clicking on the "Refresh".

Print

You can print current page at any time by clicking on the "Print".

Logout

You can print current page at any time by clicking on the "Logout".

Help

You can view the help page at any time by clicking on the "Help".

Chapter 5. TMM Web Console Options

This topic describes the TMM web console. You can check the status of sensors presented by the ThinkServer, view the installed hardware components, grant access to other users, and configure TMM settings. This section presents all available features and the possible operations for each one.

Log in and access control

In order to login TMM, you must provide both a valid Username and a Password, both fields are mandatory and should be filled properly, if the field is invalid, the TMM login is not allowed.

The TMM supports local users as well as Active Directory and LDAP. You may need to ask your system administrator about credentials to log in.

NOTE: To log in to the TMM web interface, you must provide both a valid Username and a Password. Both fields are mandatory and should be filled properly. If three failed login attempts, the account will be locked out 30 minutes. For Active Directory and LDAP services, the Username field doesn't require the domain before the username itself (for example, domainABC\userXYZ).

By default, the TMM will try to authenticate the provided credentials in the following order:

1. Locally
2. LDAP (if enabled)
3. Active Directory (if enabled)

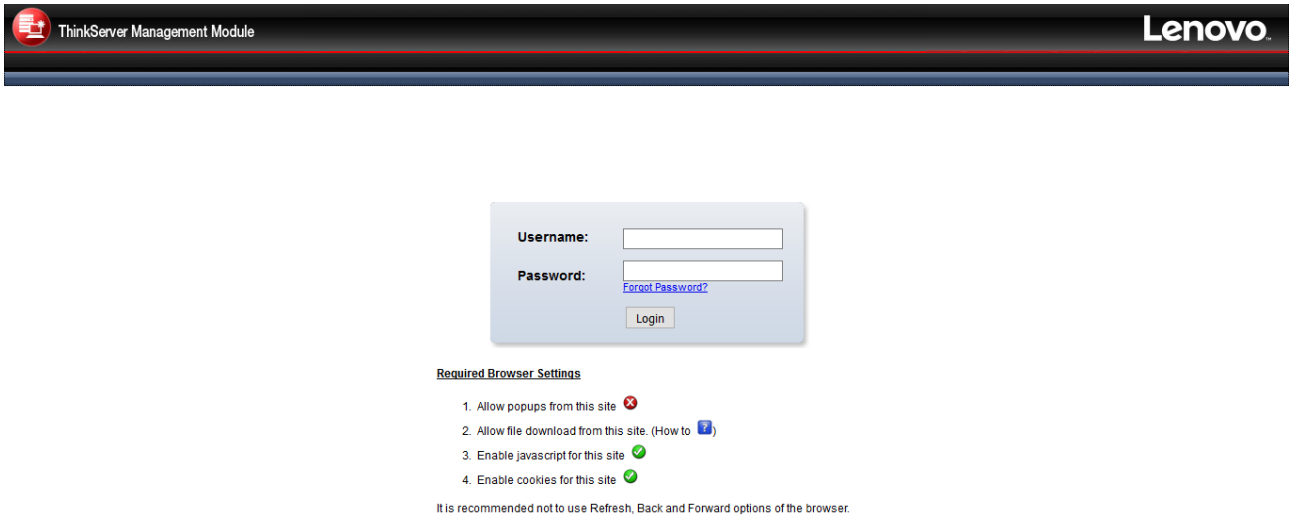


Figure 1. Login page

Forgot password

The “Forgot password” mechanism can generate a new one using this link, and enter the username to click on " Forgot password?". This will send the newly generated password to configured Email-ID for this user.

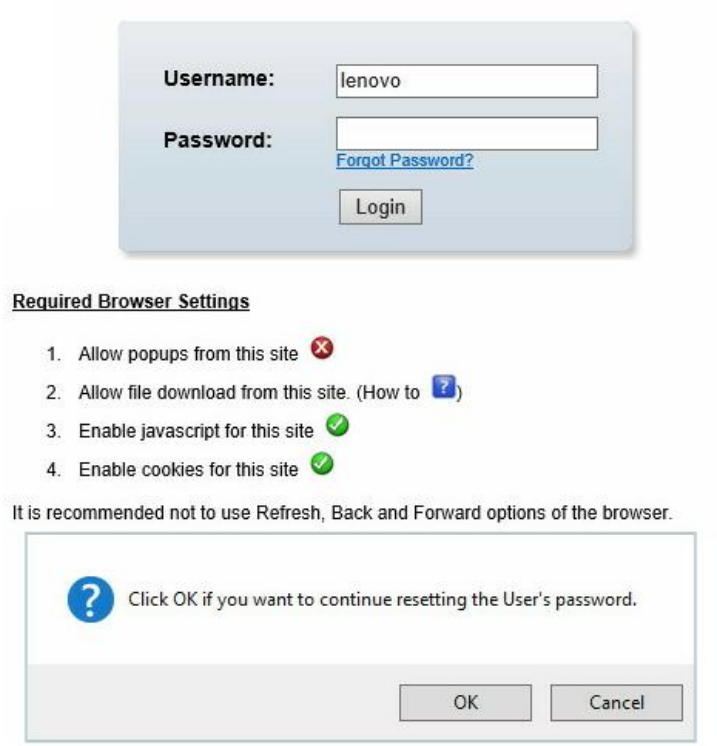


Figure 2. Forgot Password dialog

Required Browser Settings

Allow pop-ups from this site: The icon indicates whether the browser allows popup for this site or not.
Allow file download from this site: For Internet Explorer, Choose Tools ->Internet Options ->Security Tab, based on device setup, select among Internet, Local intranet, trusted sites and restricted sites. Click Custom level.... In the Security Settings - Zone dialog opened, under settings, find Downloads option, Enable File download option. Click OK to the entire dialog boxes.
For all Other Browsers, accept file download when prompted.
Enable javascript for this site: The icon indicates whether the javascript setting is enabled in browser.
Enable cookies for this site: The icon indicates whether the cookies setting are enabled in browser
NOTE: Cookies must be enabled in order to access the website.

Dashboard

Dashboard displays the overall information about the device status. Launch the remote console redirection window from this page. To launch it, you must have Administrator privilege or KVM privilege.
After logging in, the TMM presents a Dashboard page showing overall server status.

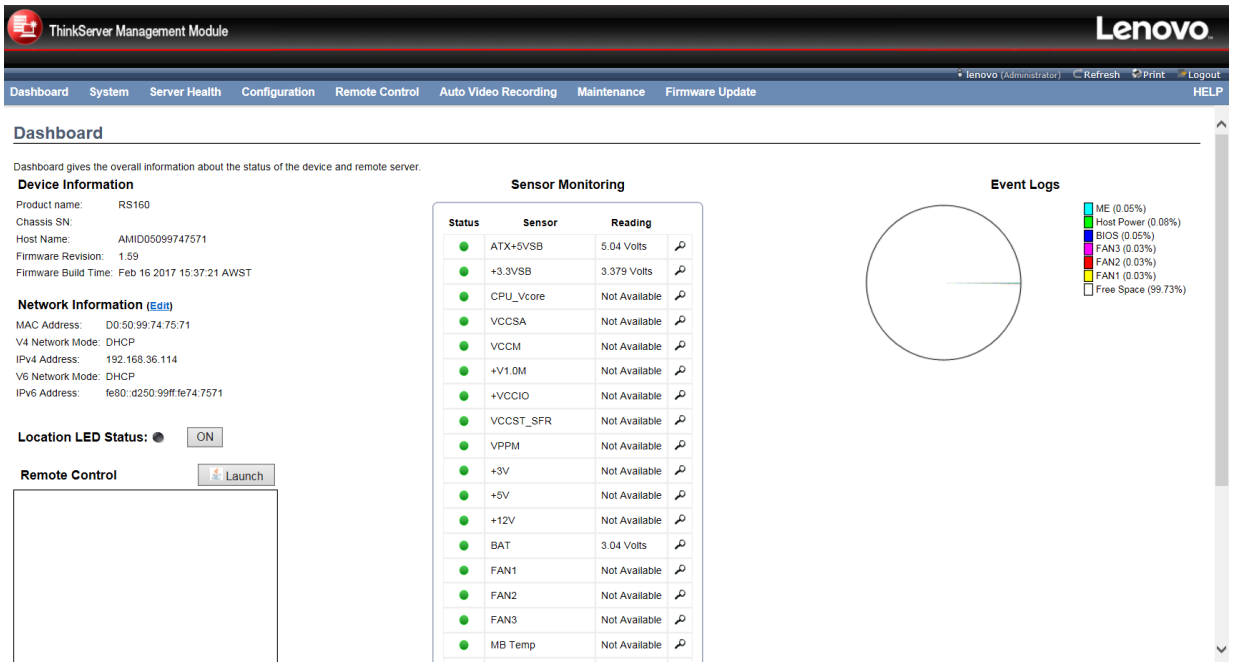


Figure 3. Dashboard

A brief descript of the Dashboard page is given below.

Device Information

Displays the Firmware Revision and Firmware Build Time (Date and Time).

Network Information

Shows network settings for the device. Click on the link Edit to view the Network Settings Page.

Location LED Status

Display the current status of the Location LED. Click the ON/OFF button to control the Location LED.

Remote Control

Start remote redirection of the host by launching the console from this page. Clicking on ' Launch' button of 'Remote Control' will cause the jviewer.jnlp file to be downloaded. Once the file is downloaded and launched, a Java redirection window will be displayed.

Remote Console Screenshot

It will show the screenshot of the remote server using java application. Click on 'Refresh' button to reload the screenshot.

Sensor Monitoring

It lists all available sensors on the device, with information such as status, name, reading, and status icon, as well as a link to that sensor's page. Current reading will be displayed for Analog sensor whereas event state will be displayed for discrete sensor in Reading field.
There are 3 possible states for a Sensor:

- Green dot denotes a Normal state.

- Yellow exclamation mark denotes a Warning state.

- Red x denotes a Critical state.

The magnifying glass allows access to the Sensor details page for that sensor.

Event Logs

A graphical representation of all events incurred by the various sensors and occupied/available space in logs. If you click on the color-coded rectangle in the Legend for the chart, you can view a list of those specific events only.

NOTE: If the log doesn't belong to device SDR, it will be classified as group "Others". You can find available space of event log in group "Free Space".

Menu Bar

The Menu bar displays the following.

- Dashboard
- System
- Server Health
- Configuration
- Remote Control
- Auto Video Recording
- Maintenance
- Firmware Update

A screenshot of the menu bar is shown below.

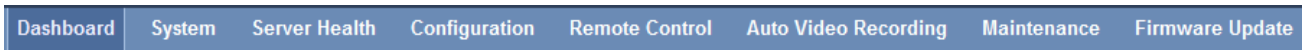


Figure 4. Menu Bar

System

The System Group displays the following information

- Inventory
- FRU information

A screenshot displaying the menu items under System is shown below.

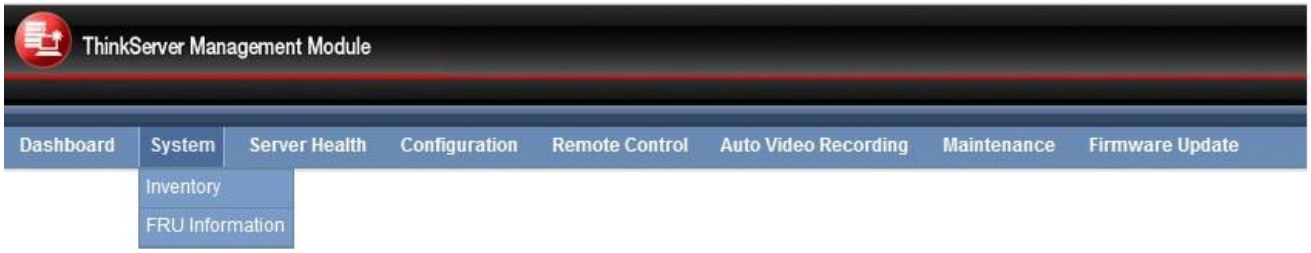


Figure 5. System - Menu

Inventory

This page displays the inventory information.

- **BIOS Information**: It displays the BIOS Information.
  - BIOS Vendor
  - BIOS Version
  - BIOS Build Date

- **CPU Information**: It displays the CPU Information.
  - CPU Model
  - CPU Signature
  - CPU Core Count
  - CPU Thread Count
  - Base CPU Speed
  - Max CPU Speed
  - Min CPU Speed
  - L1 iCache
  - L1 dCache
  - L2 Cache
  - L3 Cache
- **Memory Information**: It displays the memory information.
  - Total Memory Installed
  - Memory Select: User can select the memory to show below information.
    - DDR4 Slot
    - Capacity
    - Type
    - Type Detail
    - Rank
    - Configured Speed
    - Voltage
    - Manufacturer
    - Part Number
    - Serial Number
- **Storage Information**: It displays the storage information.
  - Storage Select: User can select the device to show below information.
    - HDD Port
    - Port speed
    - Device Model
    - Device Revision
    - Serial Number
- **Network Information**: It displays the onboard network information.
  - Port Count
  - Port Select
  - MAC Address

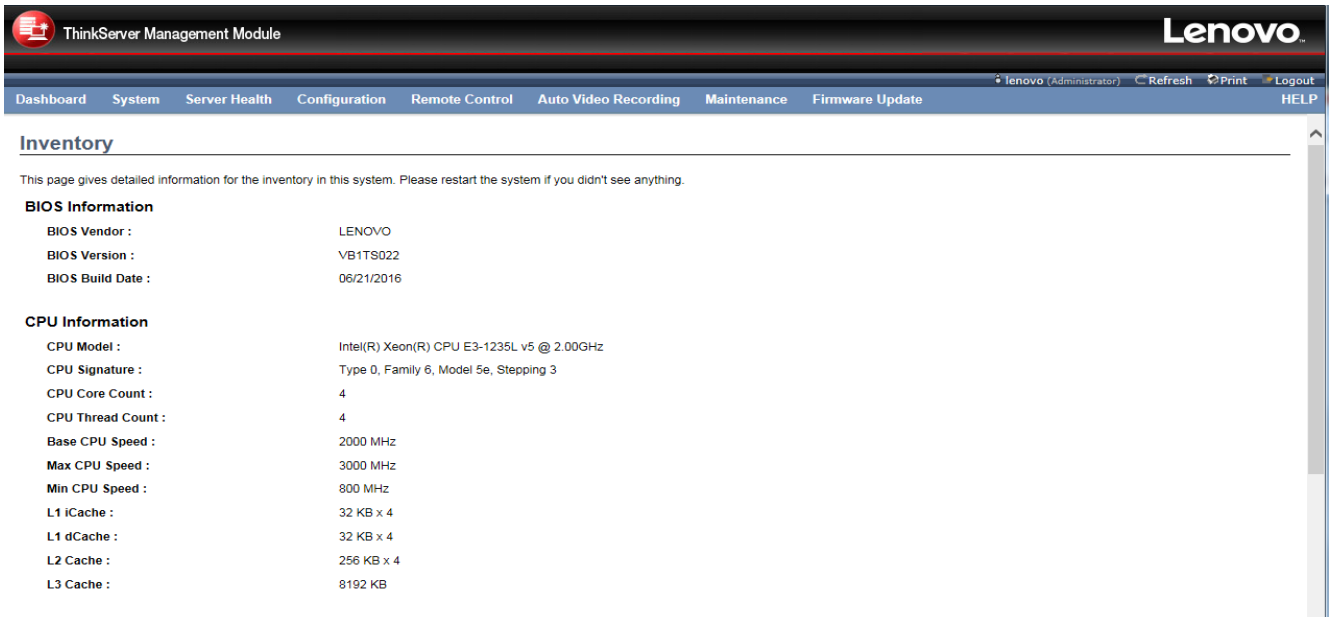


Figure 6. Inventory

FRU Information

This page displays the BMC FRU file information. On selecting any particular FRU Device ID its corresponding FRU information will be displayed.

To open the FRU Information Page, click **FRU Information** from the menu bar. 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.

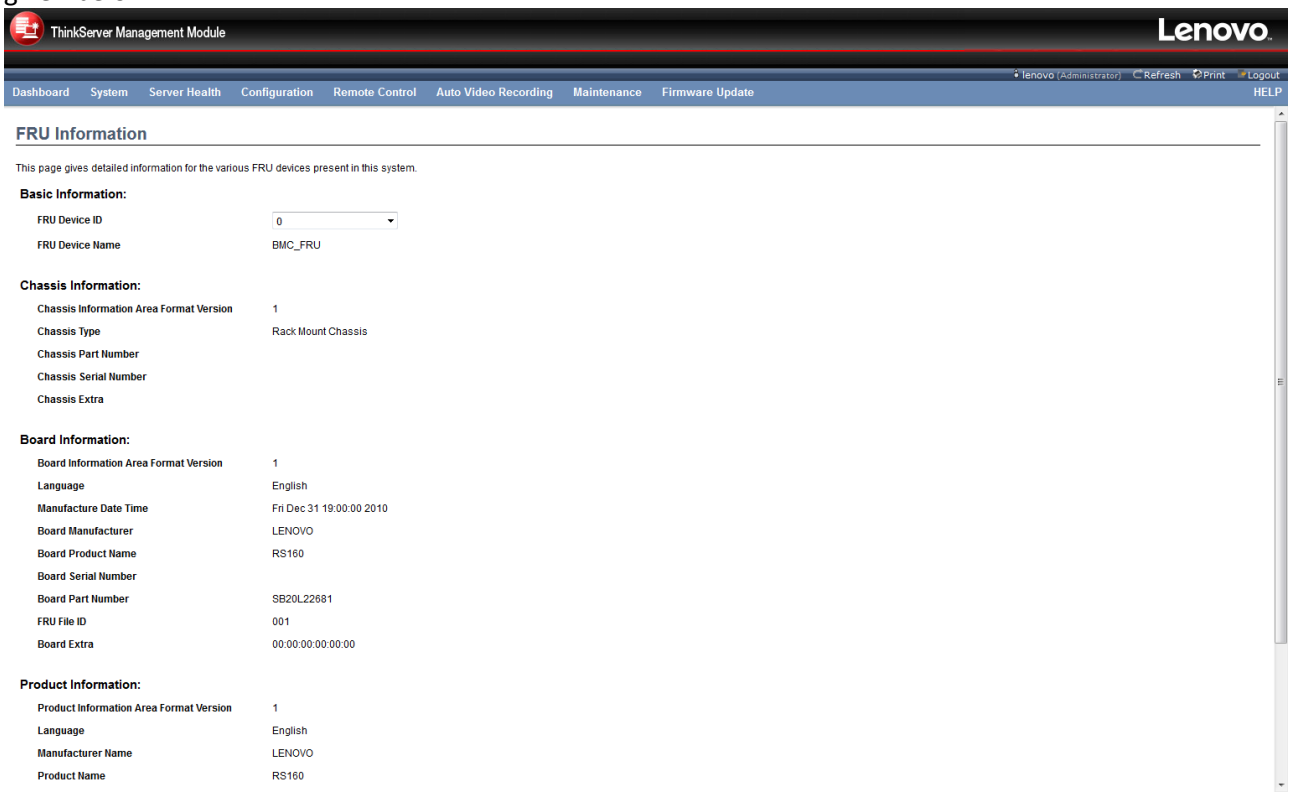


Figure 7. FRU information

- **Basic Information:** It displays the FRU Device Name for the selected FRU Device ID. This page displays the Chassis, Board, and Product details (if available) for the items shown in each field.
- **Chassis Information:** It displays the FRU Chassis Area.
  - Chassis Information Area Format Version
  - Chassis Type
  - Chassis Part Number
  - Chassis Serial Number
  - Chassis Extra
- **Board Information:** It displays the FRU Board Area.
  - Board Information Area Format Version
  - Language
  - Manufacture Date Time
  - Board Manufacturer
  - Board Product Name
  - Board Serial Number
  - Board Part Number
  - FRU File ID
  - Board Extra
- **Product Information:** It displays the FRU Product Area.
  - Product Information Area Format Version
  - Language
  - Manufacturer Name
  - Product Name
  - Product Part Number
  - Product Version
  - Product Serial Number
  - Asset Tag
  - FRU File ID
  - UUID

NOTE: UUID will be displayed in Product Extra if you get FRU data by ipmitool, the data could not be displayed normally because it's defined as hex data(FRU data is displayed as ASCII in ipmitool).

Server Health Group

The Server Health Group displays the following information.

- Sensor Readings
- Event Log
- BSOD Screen

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

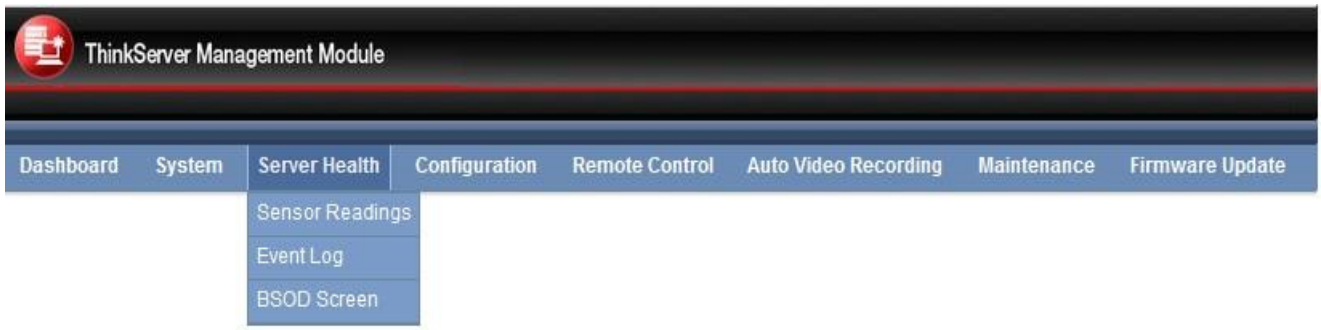


Figure 8. Server Health - Menu

A detailed description of Server Health Group is given below

Sensor Readings

A list of sensor readings will be displayed here. Current reading will be displayed for Analog sensor whereas event state will be displayed for discrete sensor. Click on a record to show more information about that particular sensor, including thresholds and a graphical representation of all associated asserted events. Double click on a record to toggle (ON / OFF) the live widget for that particular sensor.

NOTE: N/A represents Not Applicable.

To open the Sensor readings page, click Server **Health > Sensor Readings** from the menu. Click on any sensor 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

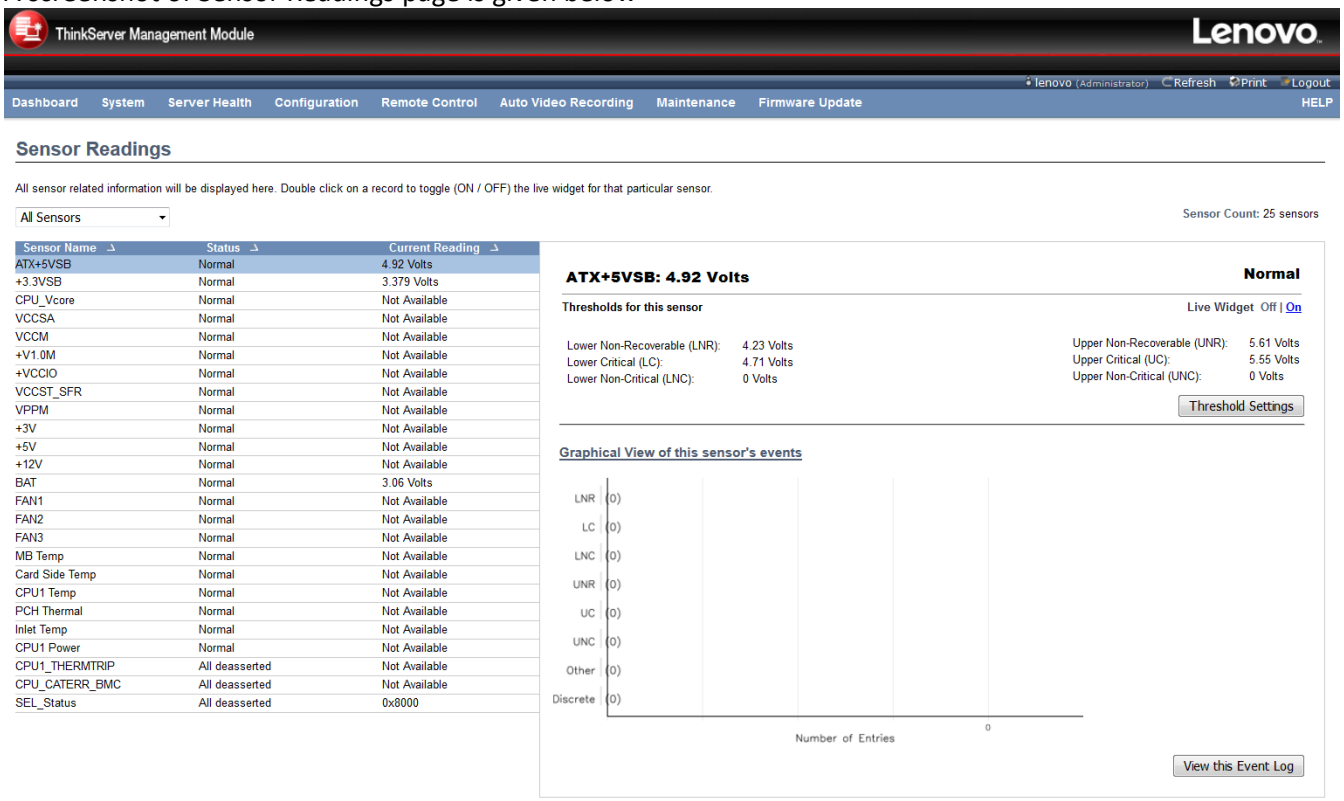


Figure 9. Sensor Reading Page

- **Threshold Settings**: Click this option to configure Threshold Settings. Options are
  - Lower Non-Recoverable (LNR)

- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

- **Live Widget:** Turn On or Off the live widget for this sensor. This widget gives a dynamic representation of the readings for the sensor.
- **View this Event Log:** Click this button to view the event log page for the selected sensor.

Sensor Type (drop down menu)

This drop down menu allows you to select the type of sensor. If you select All Sensors, all the available sensors with details like Sensor Name, Status and Current Reading will be appeared, else you can choose the sensor type that you want to display in the list. Some examples for sensors are Temperature Sensors, Fan Sensors, Watchdog Sensors and Voltage Sensors etc.

Live Widget

For the selected sensor, you can click ON or OFF to turn the widget appear or disappear. This widget gives a dynamic representation of the readings for the sensor. You can also double click on a record to toggle (ON / OFF) the live widget for that particular sensor. Given below is a sample screenshot when the widget is on.

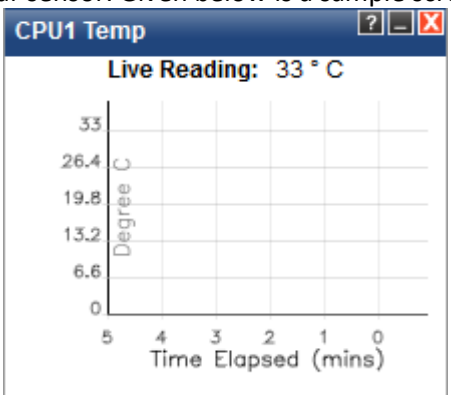


Figure 10. Live Widget

Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget.

Since widgets require getting live data, as long as a widget is kept open, the session will not expire.

- **Minimize/Restore**: Minimize button causes the graph to be hidden, but the live reading will continue to be displayed. Please note the graph will still be up-to-date when restored. Restore toggles the widget to its normal size.
- **Close**: User can close the widget at any time. Sensor history monitored until then will be lost on the client side. but any events will still be logged on the server.

Threshold Settings

The threshold settings can be configured by clicking this button. A sample screenshot is given below.

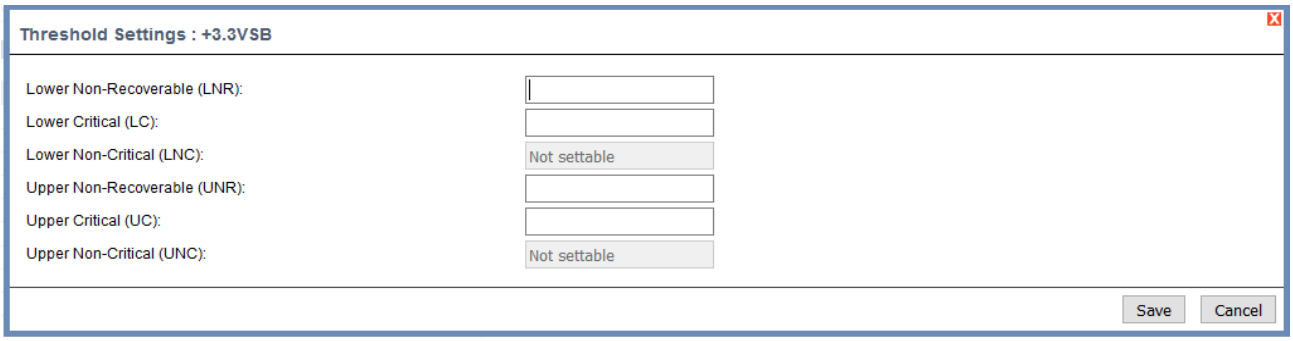


Figure 11. Threshold Settings

Use this page to configure threshold settings configuration.

- **Lower Non-Recoverable (LNR):** Set lower non-recoverable threshold.
- **Lower Critical (LC):** Set lower critical threshold.
- **Lower Non-Critical (LNC):** Set lower non-critical threshold.
- **Upper Non-Recoverable (UNR):** Set upper non-recoverable threshold.
- **Upper Critical (UC):** Set upper critical threshold.
- **Upper Non-Critical (UNC):** Set upper non-critical threshold.
- **Save:** Save the settings. All data in the text box will be converted into IPMI data type, for more information, please refer to IPMI SPEC. 2.0, chapter 36, Sensor Types and Data Conversion.
- **Cancel:** Cancel the modified changes.

View this Event Log

You can click "**View this Event Log**" to view the Event Log for the selected sensor.
NOTE: Some sensor type is **OEM define**, you will see that “Unknown” when you get sensor status by ipmitool. etc. “Unknown CPU_CATERR_BMC”

Event Log

This page displays the list of events incurred by different sensors on this device. Double click on a record to see the details of that entry. 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 menu bar. A sample screenshot of Event Log page is shown below.

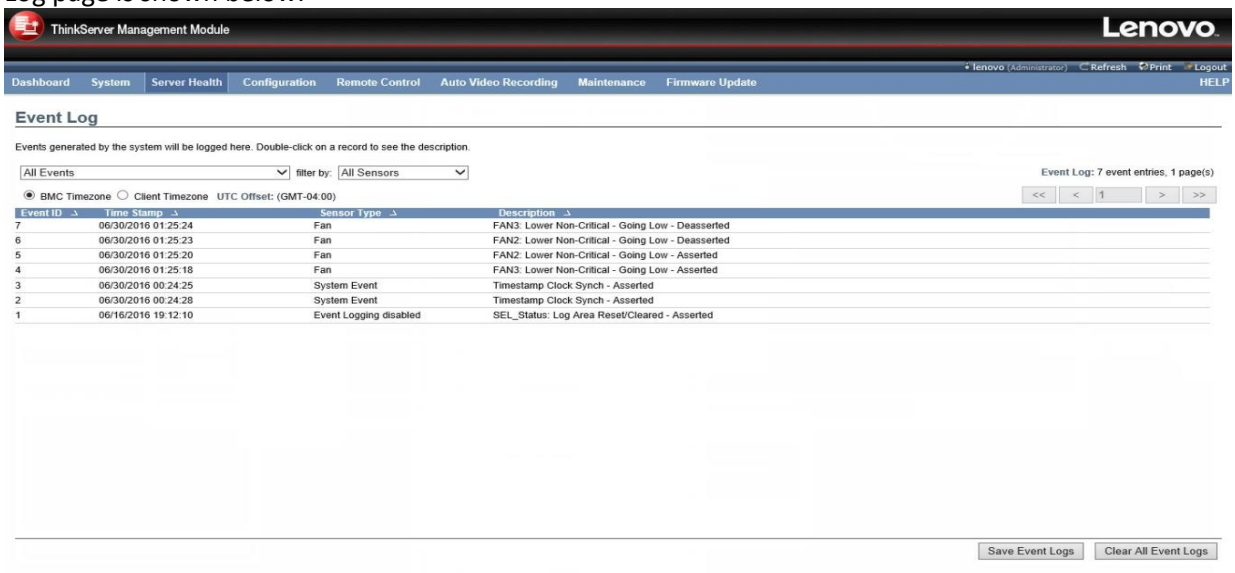


Figure 12. Event Log Page

You can use the sensor type or sensor name filter options to view those specific events logged in the device.

- **Event log Category**: The group of Sensor type, you can filter event log by sensor type.

All Events, System Event Records, OEM Event Records, BIOS Generated Events, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console software Events, Terminal Mode Remote Console software Events, follow the table below for more information.

Event	Record Type	Generator ID1	
		[7:1]	[0]
BIOS Generated Events	0x00 – 0xBF	0x00 – 0x0F	1b
SMI Handler Events		0x10 – 0x1F	
System Management Software Events		0x20 – 0x2F	
System Software - OEM Events		0x30 – 0x3F	
Remote Console software Events		0x40 – 0x46	
Terminal Mode Remote Console software Events		0x47	
System Event Records		others	
OEM Event Records	0xC0 – 0xFF		

NOTE: About the “Record Type” & “Generator ID”, you can refer to the IPMI 2.0 spec for details.

- **Filter By**: The group of Sensor name, you can filter event log by sensor name.
- **BMC Time zone**: Check this option to display the event log entries logged with the BMC Time zone value.
- **Client Time zone**: Check this option to display the event log entries logged with the Client (user's) Time zone value.
- **UTC Offset**: Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.
- **Event ID**: Displays the ID number of event.
- **Time Stamp**: Displays the timestamp of event.
- **Sensor Type**: Displays the sensor type of event.
- **Description**: Displays more information include which sensor name that generated the event.
- **Clear All Event Logs**: Clear All Event Logs option will delete all existing records for all sensors.
  NOTE: There are some event log “Bugcheck code OEM Event Record” which asserted by OS after system BSOD.
- **Save Event Logs**: Clicking this button will pop-up a Save dialog to save all existing records.

BSOD Screen

This page displays the snapshot of the blue screen captured if the host system crashed since last reboot.
To open the BSOD Screen page, click **Server Health > BSOD Screen** from the menu bar. A sample screenshot of BSOD Screen is shown below.

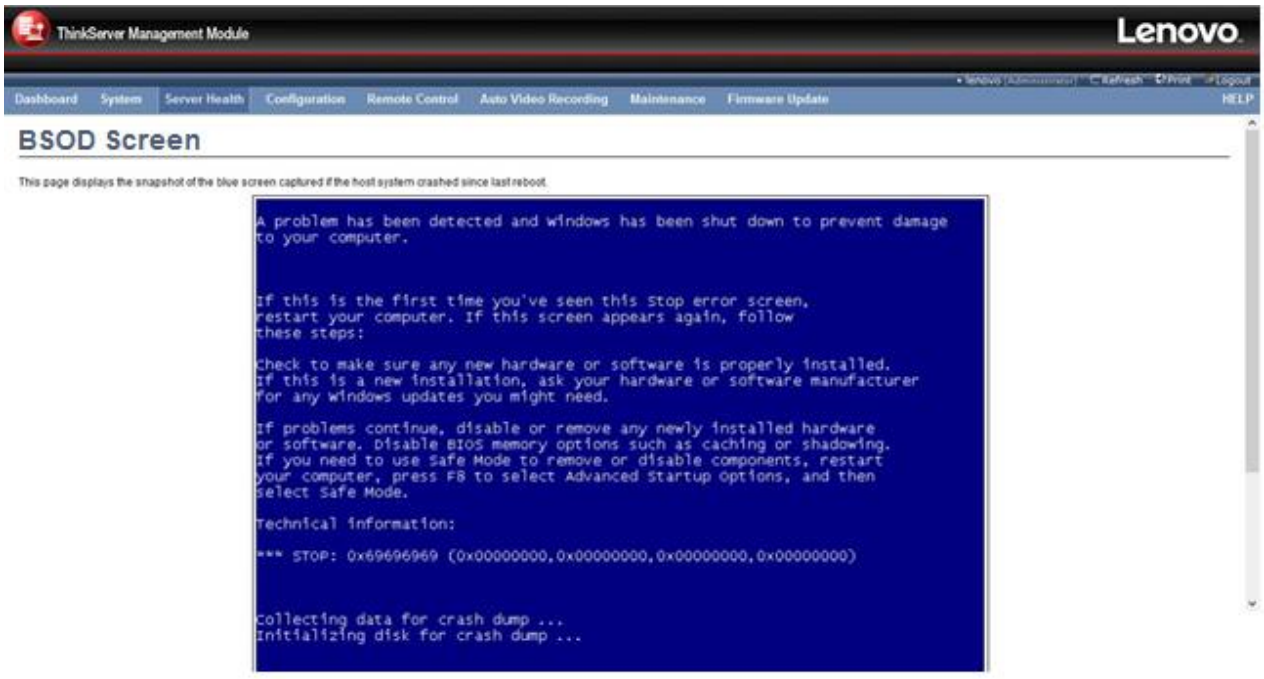


Figure 13. BSOD Screen

NOTE:

- KVM service should be enabled, to display the BSOD screen. KVM Service can be configured under Configuration-> Services->KVM.

Configuration Group

This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.

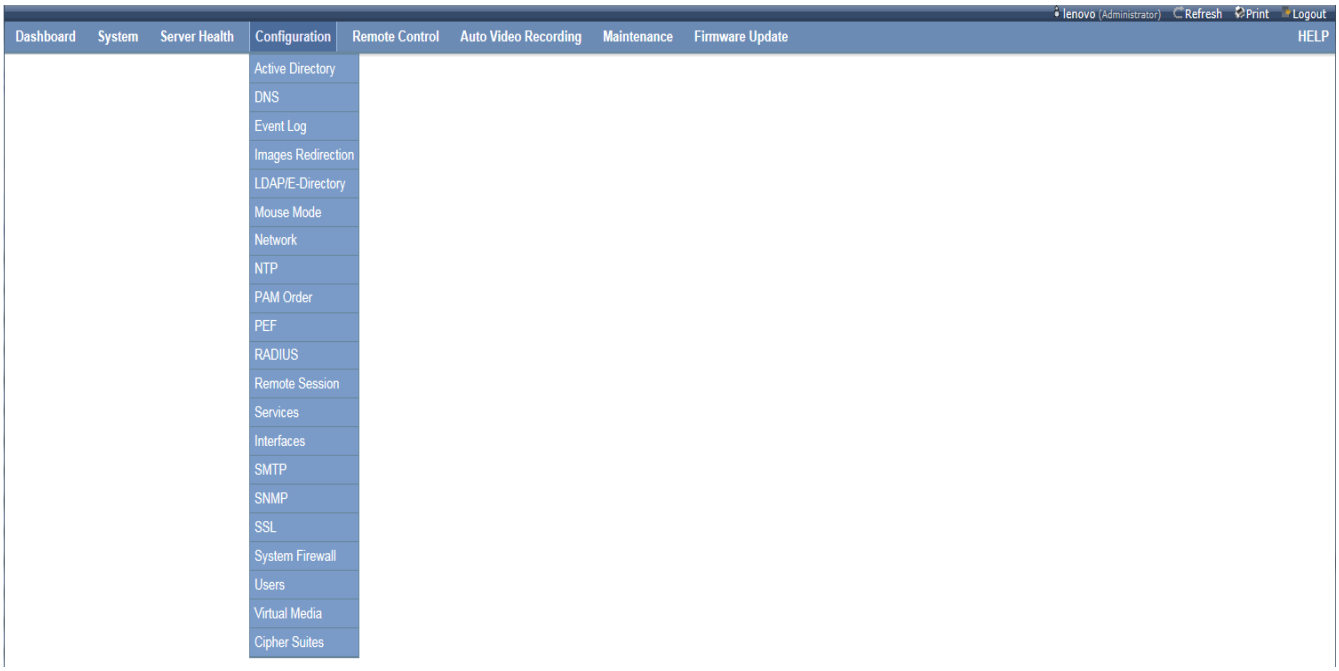


Figure 14. Configuration Croup Menu

A detailed description of the Configuration menu is given below.

Active Directory

The displayed table shows any configured Role Groups and the available slots. You can modify, add or delete role groups from here. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group. To view the page, you must be at least a User. To modify or add a group, you must be an Administrator(or OEM Proprietary).

NOTE: Free slots are denoted by "~" in all columns for the slot.

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 AD) does a variety of functions including the ability to provide information on objects. It also helps to 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.

The Active Directory Settings page, click **Configuration > Active Directory** from the menu bar. A sample screenshot of Active Directory Settings page is shown below.

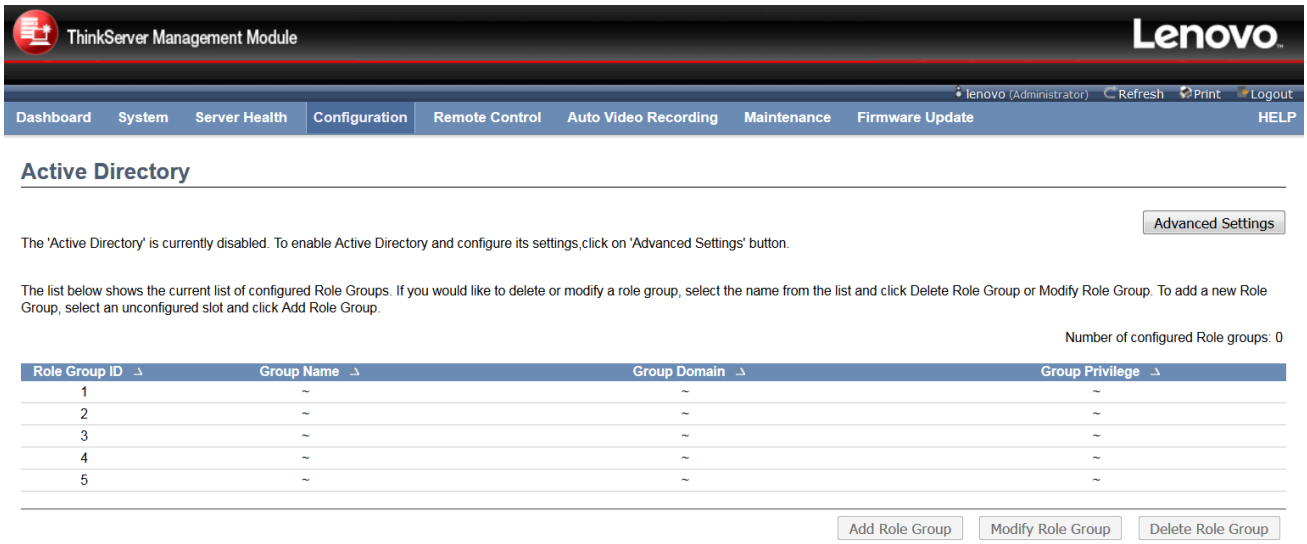


Figure 15. Active Directory Settings

- **Advanced Settings**: Click this option to configure the Active Directory Settings. Options are Enable Active Directory Authentication, User Domain name, Time Out and up to three Domain Controller Server Addresses.
- **Add Role Group**: Select a free slot and click 'Add Role Group' to add a new role group to the device. Alternatively, double click on a free slot to add a role group.
- **Modify Role Group**: Select a configured slot and click 'Modify Role Group' to modify that role group. Alternatively, double click on the configured slot.
- **Delete Role Group**: Select the desired role group to be deleted and click 'Delete Role Group'.
- **Role Group ID:** The number of role group.
- **Group Name:** Role Group Name. This name identifies the role group in Active Directory.
- **Group Domain:** This is the domain where the role group is located.
- **Group Privilege:** This is the level of privilege to be assigned for this role group.

Advanced Setting

This page is used to configure the Active Directory Advanced Settings Trusted domains are supported as well.

The Active Directory Settings page, click **Configuration > Active Directory > Advanced Settings**.

A sample screenshot of Active Directory Settings page is shown below.

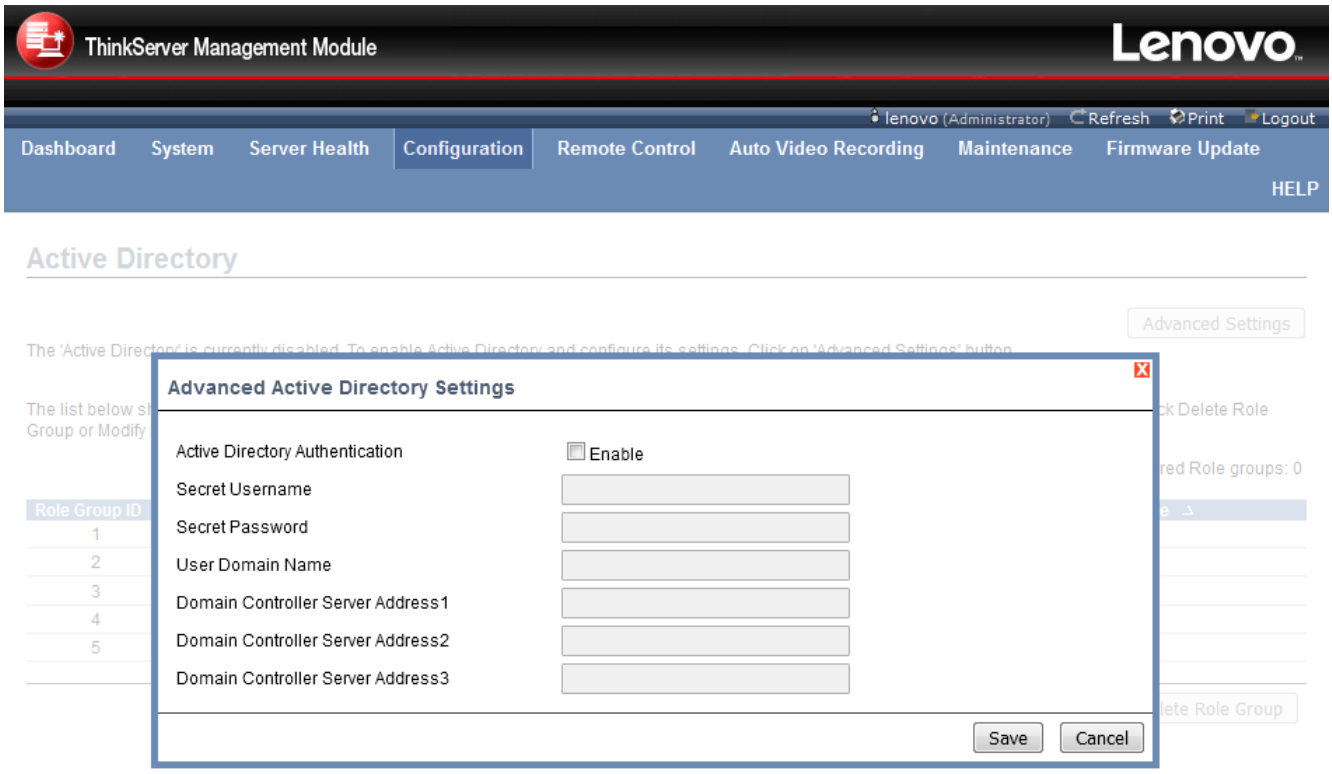


Figure 16. Advanced Active Directory Settings

- **Active Directory Authentication:** To enable or disable Active Directory, check or uncheck the 'Active Directory Authentication' checkbox respectively.
  If you have enabled the Active Directory Authentication, then enter the required information to access the Active Directory server.
- **Secret Username:** Specify the Username of the Active Directory Server.
  - User Name is a string of 1 to 64 alpha-numeric characters.
  - It must start with an alphabetical character.
  - It is case-sensitive.
  - Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterick, question mark, double quotes, space are not allowed.

  NOTE: If Secret Username and Password are not needed, both can stay empty.
- **Secret Password:** Specify the Password of the Active Directory Server.
  - Password must be at least 6 character long.
  - White space is not allowed.

  NOTE: This field will not allow more than 127 characters.
- **User Domain Name:** Specify the Domain Name for the user. e.g. MyDomain.com
- **Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3:** Enter the IP address of Active Directory server. At least one Domain Controller Server Address must be configured.
  - 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.

  Domain Controller Server Addresses will support the following:
  - IPv4 Address format.

- IPv6 Address format.

- **Save:** Click 'Save' to save the settings.
- **Cancel:** Click 'Cancel' to cancel the modifications and return to the Active Directory page.

DNS

This page is used to configure the Host name and Domain Name Server configuration of the device.
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. The DNS Server settings page is used to manage the DNS settings of a device.
The DNS Server Settings page, click **Configuration > DNS** from the menu bar. A sample screenshot of DNS Server Settings page is shown below

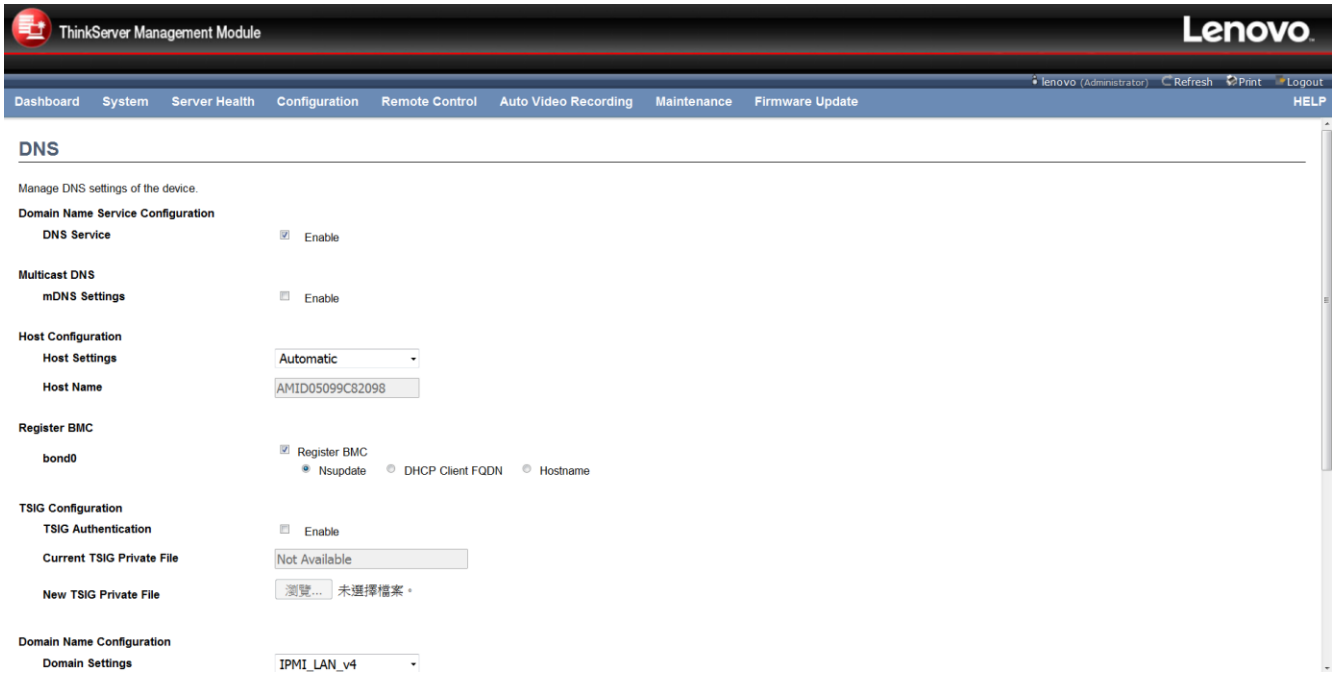


Figure 17. DNS Server Settings Page

Domain Name Service Configuration

- **DNS Service:** Check this box to enable all the DNS Service configurations.

Multicast DNS

- **mDNS Settings:** Check this box to enable/disable the mDNS Support Configurations.

Host Configuration

- **Host Settings:** Choose either Automatic or Manual settings.
- **Host Name:** It displays hostname of the device if Auto was selected above. If the Host setting is chosen as Manual, then specify the hostname of the device.
  - Value ranges from 1 to 63 alpha-numeric characters.
  - Special characters '-'(hyphen) and '_'(underscore) are allowed.
  - It must not start or end with a '-'(hyphen).

  NOTE: IE browsers won't work correctly if any part of the hostname contain underscore (_) character.

Register BMC

Choose the BMC's network port to register with DNS settings. Check the option 'Register BMC' to register with DNS settings.

- **Nsupdate:** Choose the option 'Nsupdate' to register with DNS server using nsupdate application.
- **DHCP Client FQDN:** Choose the option 'DHCP Client FQDN' to register with DNS Server using DHCP option 81.
- **Hostname:** Choose the option 'Hostname' to register with DNS server using DHCP option 12.
  NOTE: Hostname option should be selected if the DHCP client FQDN option is not supported by DHCP server.

TSIG Configuration

- **TSIG Authentication:** Check this option to enable TSIG authentication while registering DNS via Nsupdate.
- **Current TSIG Private File:** The information as Current TSIG private and uploaded date/time will be displayed (readonly).
- **New TSIG Private File:** Browse and navigate to the TSIG private file.
  - TSIG file should be of private type

Domain Name Configuration

- **Domain Settings:** It lists the option for domain interface as Manual, v4 or v6 for multiLAN channels.
- **Domain Name:** It displays the domain name of the device if Auto was selected. If the Domain setting is chosen as Manual, then specify the domain name of the device.

Domain Name Server Configuration

- **DNS:** It lists the option for DNS interface, Manual and available LAN interfaces.
- **IP Priority:** If IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server. If IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.
  NOTE: This is not applicable for Manual configuration.
- **DNS Server 1, 2 & 3:** Specify the DNS (Domain Name System) server address to be configured for the BMC.
  - 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.

  DNS Server Address will support the following:
  - IPv4 Address format.
  - IPv6 Address format.

  NOTE: Only Global IPv6 Addresses are allowed.
- **Save**: Click 'Save' to save any changes made. You will be logged out of current UI session and will need to log back in.
- **Reset**: Reset the modified changes.

Event Log

This page is used to configure the System Event log behavior. Linear SEL type will store the System Event log linearly up to its SEL Repository size and SEL will be discarded if the SEL Repository is full. Circular SEL type will store the System Event log linearly up to its SEL Repository size and override the SEL entry if the SEL Repository is full.

To open System Event log page, click **Configuration > Event Log** from the menu bar. A sample screenshot of System Event log page is shown below.

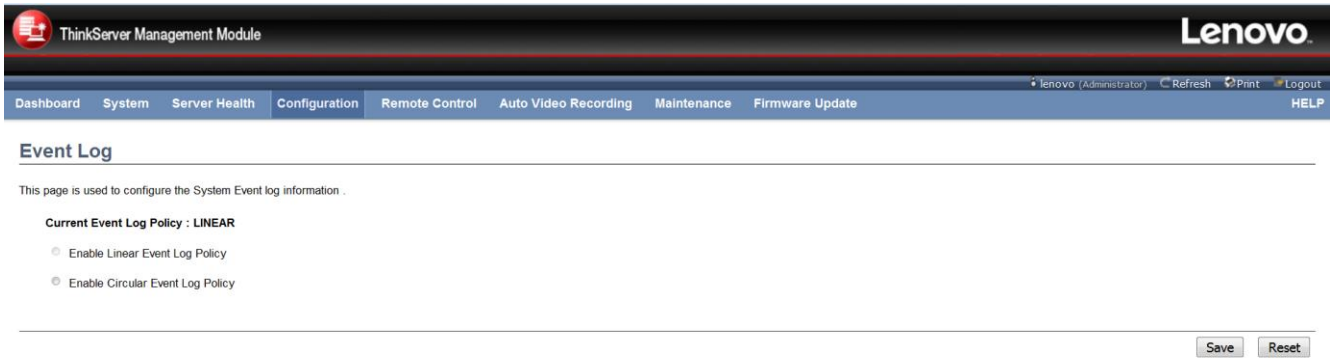


Figure 18. System Event Log Page

- **Current Event Log Policy**: It will display the configured Event Log Policy.
- **Linear Event Log Policy**: Check this option to enable the Linear System Event Log Policy for Event Log.
- **Circular Event Log Policy**: Check this option to enable the Circular System Event Log Policy for Event Log.
- **Save**: Click 'Save' to save the configured settings.
- **Reset**: Click 'Reset' to reset the modified changes.

Images Redirection

The displayed table shows configured images on BMC. You can start/stop redirection from here to remote media.
Any number image can be configured for each image type.
To configure the image, you need to enable Remote Media support using 'Advanced Settings'.
To start/stop redirection, you must have Administrator Privileges.
NOTE: Free slots are denoted by "~".
To open Images Redirection page, click **Configuration > Images Redirection** from the menu bar. A sample screenshot of Images Redirection page is shown below.

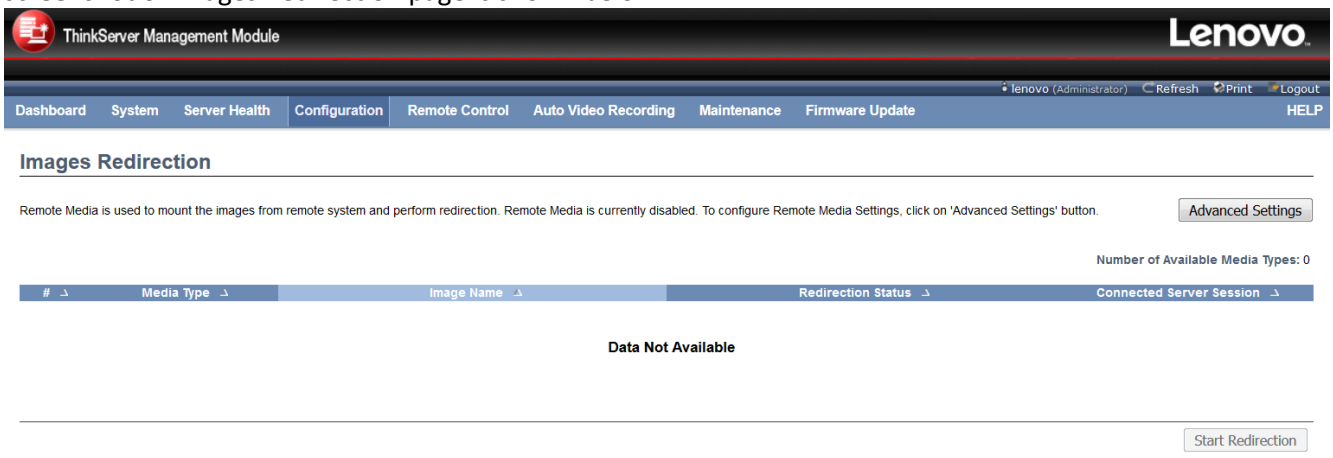


Figure 19. Images Redirection Page

- **Advanced Settings:** Click this option to configure the Remote Media Settings. Options are Enable/Disable Remote Media Support, Server Address, Source Path, Share Type, Username, Password and Domain Name.
- **#:** The serial number.
- **Media Type:** Show the media type which type of media is supported.
- **Image Name:** Show the image name of the image.

- **Redirection Status:** Show the Redirection Status.
- **Connected Server Session:** Show the connected server session.
- **Start/Stop Redirection:** Select a configured slot and click 'Start Redirection' to start the remote media redirection. It is a toggle button. If the image is successfully redirected, then click 'Stop Redirection' button to stop the remote media redirection.

Advanced Setting

This form is used to configure the Advanced Media settings.
To open Advanced Media Settings section, click **Configuration > Images Redirection > Advanced Settings**.

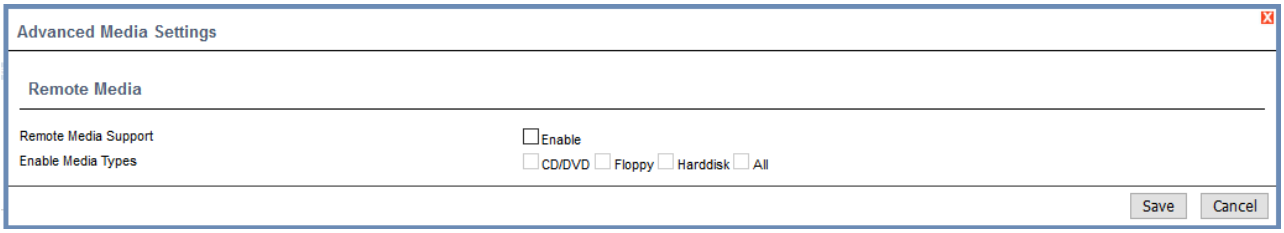


Figure 20. Advanced Media Settings Page

- **Remote Media Support**: To enable or disable Remote Media support, check or uncheck the 'Enable' checkbox respectively. Based on Remote Media support enabled/disabled, following remote media types will be enabled/disabled.
- **Enable Media Types:** Selected remote media types.
- **CD/DVD, Floppy, Harddisk, All**: Based on selected remote media types, the following fields will be visible. If **All** option selected, all the entered configurations will be common for all remote media types. On selecting individual remote media types will visible the three configuration rows. User can configure different settings for different remote media types by enabling corresponding media type. If **All** option used then the entered media type data only will update and the configurations will be same for rest of remote media types.
- **Server Address**: Address of the server where the remote media images are stored.
- **Source Path**: Source path to the remote media images.
- **Share Type**: Share Type of the remote media server either NFS or Samba(CIFS).
- **Username, Password and Domain Name**: If share Type is Samba(CIFS), then enter user credentials to authenticate on the server.
  NOTE: Domain Name field is optional.
- **Save**: Click 'Save' to save the settings.
- **Cancel**: Click 'Cancel' to cancel the modifications and return to Image list.

LDAP/E-Directory

The **Lightweight Directory Access Protocol (LDAP)/E-Directory Settings** is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.
In TMM GUI, LDAP is an Internet protocol that TMM can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate TMM 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 TMM. 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/E-DIRECTORY Settings page, click **Configuration > LDAP/E-Directory** from the menu bar. A sample screenshot of LDAP/E-Directory Settings page is shown below.

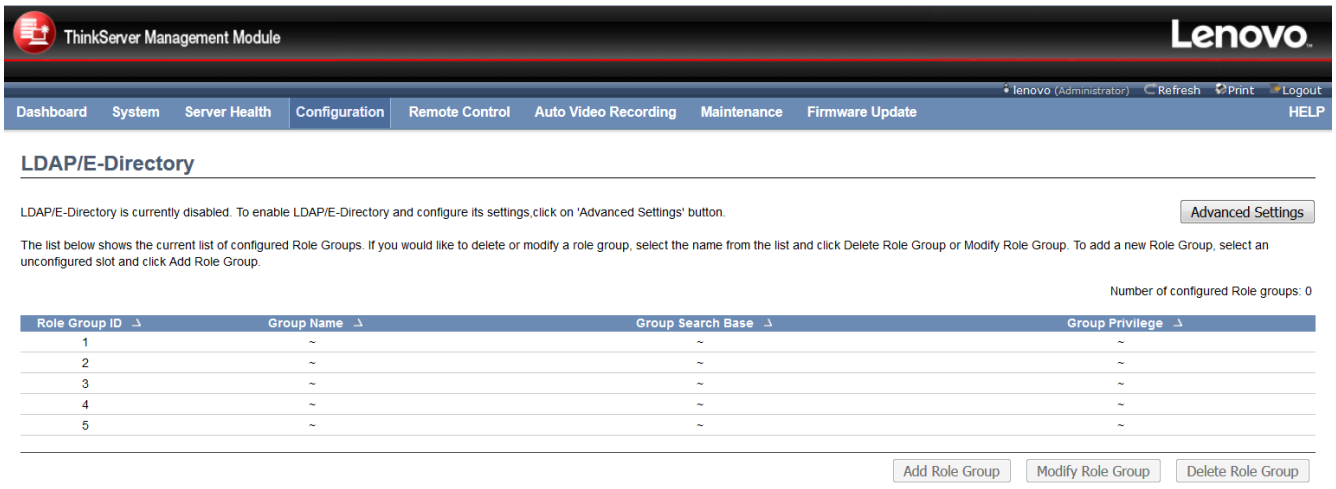


Figure 21. LDAP/E-Directory Settings Page

Displayed table shows any configured Role Groups and available slots. You can modify or add/delete role groups from here.
Group Search Base can be any path from where Group is located to Base DN. Group Name should correspond to the name of an actual LDAP/E-Directory group. To view the page, user must at least be a User.
To modify or add a group, user must be an Administrator(or OEM Proprietary).
NOTE: Free slots are denoted by "~" in all columns for the slot.

The fields of LDAP/E-Directory Settings Page are explained below.

- **Advanced Settings:** Click this option to configure LDAP/E-Directory Advanced Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port, Bind DN, Password and Search Base.
- **Add Role Group:** Select a free slot and click 'Add Role Group' to add a new role group to the device. Alternatively, double click on a free slot to add a role group.
- **Modify Role Group:** Select a configured slot and click 'Modify Role Group' to modify that role group. Alternatively, double click on the configured slot.
- **Delete Role Group:** Select the desired role group to be deleted and click 'Delete Role Group'.
- **Role Group ID:** The number of role group.
- **Group Name:** The Role Group Name. This name identifies the role group in LDAP/E-Directory.
- **Group Search Base:** Any path from where the role group is located to Base DN.
- **Group Privilege:** This is the level of privilege to be assigned for this role group.

Advanced Setting

Use this page to configure advanced LDAP/E-Directory configuration.
In the LDAP/E-Directory Settings Page, click Advanced Settings.
A sample screenshot of Advanced LDAP/E-Directory Settings page is given below.

Figure 22. Advanced LDAP/E-Directory Settings Page

- **LDAP/E-Directory Authentication**: Check the box below to enable LDAP/E-Directory authentication.
- **Encrypted Type**: Select the encryption type for LDAP/E-Directory.
  NOTE: Configure proper port number, when SSL enabled.
- **Common Name Type:** Server Address Configuration. Using IP as Server address.
- **Server Address**: The IP address of LDAP/E-Directory server
  - 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.

  LDAP/E-Directory Server Address will support the following:
  - IPv4 Address format.
  - IPv6 Address format.

  NOTE: Configure FQDN address, when using StartTLS with FQDN.
- **Port**: Specify the LDAP/E-Directory Port.
  - Default Port is 389.
  - For SSL connections, default port is 636.
  - Port value ranges from 1 to 65535.
- **Bind DN**: The Bind DN is used in bind operation, which authenticates the client to the server.
  - Bind DN is a string of 4 to 63 alpha-numeric characters.
  - It must start with an alphabetical character.
  - Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
  - Example: cn=manager, ou=login, dc=domain, dc=com
- **Password**: The Bind password is used in bind operation, which authenticates the client to the server.
  - Password must be at least 1 character long.
  - White space is not allowed.

  NOTE: This field will not allow more than 48 characters.
- **Search Base:** The Search Base tells the LDAP/E-Directory server which part of the external directory tree to search. The search Base may be something equivalent to the organization, group of external directory.
  - Searchbase is a string of 4 to 64 alpha-numeric characters.
  - It must start with an alphabetical character.
  - Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
  - Example: ou=login, dc=domain, dc=com
- **Attribute of User Login**: The attribute of user login field tells the LDAP/E-Directory server which attribute should be used to identify the user[1].
  - Only support cn or uid

  NOTE: All of the 3 files are required when StartTLS enabled.
- **Save:** Save the settings.
- **Cancel:** Cancel the modified changes.

Mouse Mode

The Redirection Console handles mouse emulation from local window to remote screen using either of the three methods. Only 'Administrator' has the right to configure this option.

- Relative Mouse mode
- Absolute Mouse mode
- Other Mouse mode

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

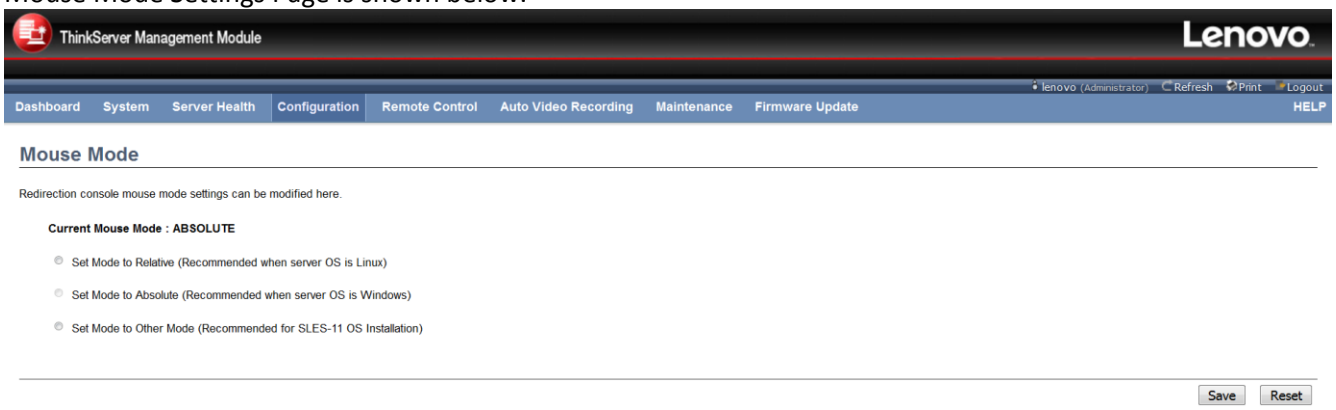


Figure 23. Mouse Mode Settings Page

The fields of Mouse Mode Settings page are explained below.

- **Relative Mouse mode:** The Relative mode sends the calculated relative mouse position displacement to the server. To select this mode select the "Set mode to Relative" option.
- **Absolute Mouse mode:** The absolute position of the local mouse is sent to the server. To select this mode, select the "Set mode to Absolute" option. Recommended for Windows or latter Linux releases.
- **Other Mouse mode:** Select Other Mode to have the calculated displacement from the local mouse in the center position, sent to the server. Use this mode for SLES 11 Linux OS installation.
- **Save**: Click 'Save' to save any changes made.
- **Reset**: Click 'Reset' to reset the modified changes.

Network

This page is used to configure the network settings for available LAN channels.

To open Network Settings page, click **Configuration > Network** from the menu bar. A sample screenshot of Network Settings Page is shown below.

Suggestion:

Using Access Control Lists (ACLs) or isolated networks to limit access to ThinkServer RS160 IPMI management interfaces.

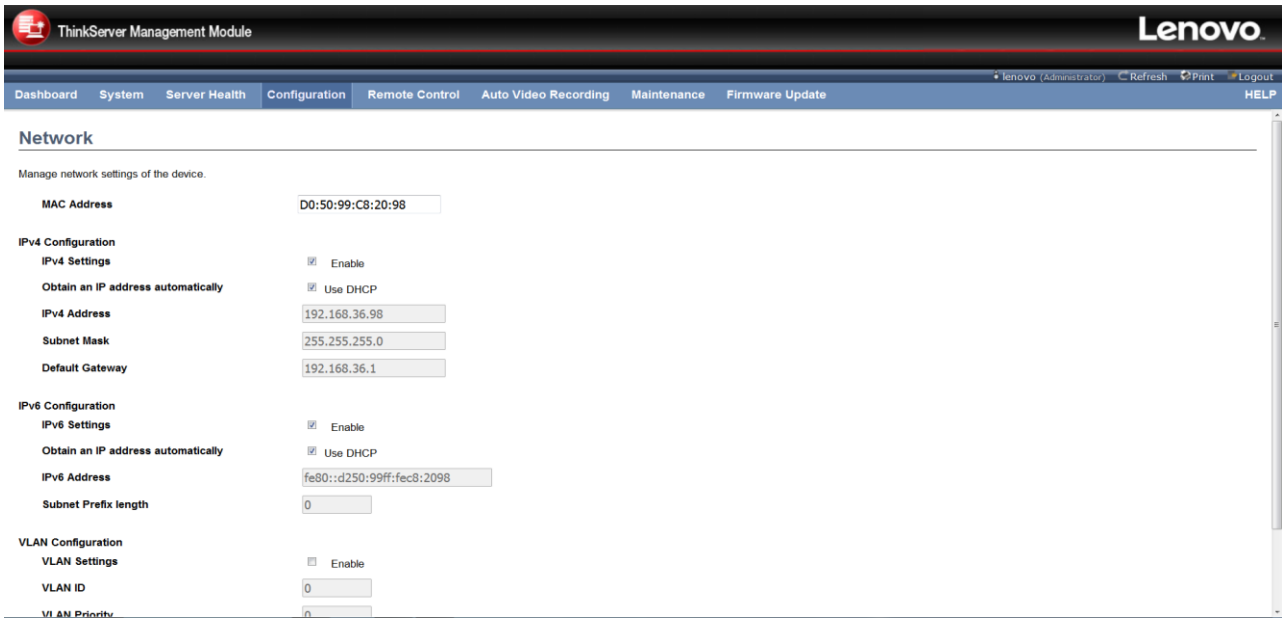


Figure 24. Network Settings Page

The fields of Network Settings page are explained below.

- **MAC Address:** This field displays the MAC address of the selected interface (read only).
- **IPv4 Configuration**: It lists the IPv4 configuration settings.
- **IPv4 Settings**: Check this option to enable IPv4 support for the selected interface.
- **Obtain an IP address automatically**: Enable 'Use DHCP' to dynamically configure IPv4 address using Dynamic Host Configuration Protocol (DHCP).
- **IPv4 Address, Subnet Mask, Default Gateway**: If DHCP is disabled, specify a static IPv4 address, Subnet Mask and Default Gateway to be configured for the selected interface.
  - IP Address consists of 4 sets of numbers separated by dots as in "xxx.xxx.xxx.xxx".
  - Each set ranges from 0 to 255.
  - First Number must not be 0.
- **IPv6 Configuration**: It lists the IPv6 configuration settings.
- **IPv6 Settings**: Check this option to enable IPv6 support for the selected interface.
- **Obtain an IP address automatically**: Enable 'Use DHCP' to dynamically configure IPv6 address using Dynamic Host Configuration v6 Protocol (DHCPv6).
- **IPv6 Address**: Specify a static IPv6 address to be configured for the selected interface.
- **Subnet Prefix length**: Specify the subnet prefix length for the IPv6 settings.
  - Value ranges from 0 to 128.
- **VLAN Configuration**: It lists the VLAN configuration settings.
- **VLAN Settings**: Check this option to enable VLAN support for the selected interface.
- **VLAN ID**: Specify the Identification for VLAN configuration.
  - Value ranges from 2 to 4094.

  NOTE: VLAN ID cannot be changed without resetting the VLAN configuration. VLAN ID 0, 1, 4095 are reserved VLAN ID's.
- **VLAN Priority**: Specify the priority for VLAN configuration.
  - Value ranges from 0 to 7.

  NOTE: 7 is the highest priority for VLAN.
- **Save:** Click 'Save' to save any changes made. You will be prompted to log out of current UI session and log back in at the new IP address.

- **Reset:** Click 'Reset' to reset the modified changes.

NTP

This page displays the device's current Date & Time Settings. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.
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.
To open NTP Settings page, click **Configuration > NTP** from the menu bar. A sample screenshot of NTP Settings Page is shown below.

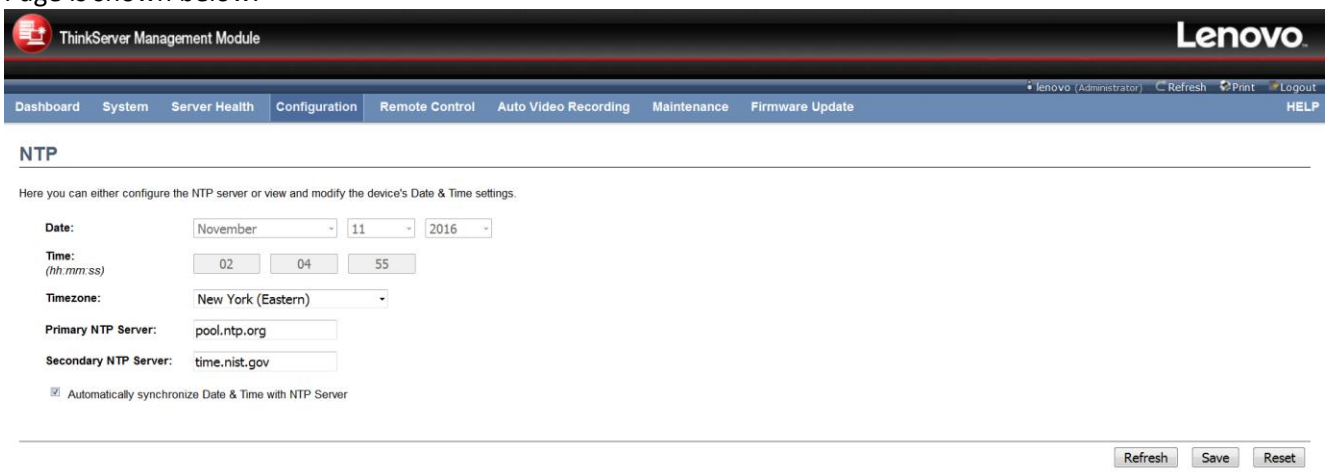


Figure 25. NTP Settings page

The fields of Configuration – NTP are explained below.

- **Date**: Specify the current Date for the device.
- **Time**: Specify the current Time for the device.
  NOTE: As a year 2038 problem exists, the acceptable date range is from 01-01-2005 to 01-18-2038.
- **Primary NTP Server & Secondary NTP Server:** Specify the NTP Servers for the device. NTP Server fields will support the following:
  - IP Address (Both IPv4 and IPv6 format).
  - FQDN (Fully qualified domain name) format.
  - FQDN Value ranges from 1 to 128 alpha-numeric characters.

  NOTE: Secondary NTP server is optional field. If the Primary NTP server is not working fine, then the Secondary NTP Server will be tried.
- **Timezone:** Timezone list contains the UTC offset along with the locations and Manual UTC offset for NTP server, which can be used to display the exact local time.
- **Automatically synchronize Date & Time with NTP Server**: Check this option to automatically synchronize Date and Time with the NTP Server once every 12 hours.
  NOTE: BIOS will check BMC time when reboot system. If BIOS and BMC time difference is greater than 2 seconds, BIOS will update BMC time.
- **Refresh**: Click 'Refresh' to reload the current date & time settings.
- **Save**: Click 'Save' to save any changes made.
- **Reset**: Click 'Reset' to reset the modified changes.

NOTE: If User uncheck 'Automatically synchronize Date & Time with NTP Server', then User can modify time & timezone manually. The current Time will not be modified automatically when user change the timezone.

PAM Order

This page is used to configure the PAM order for user authentication into the BMC.
To open PAM Order page, click **Configuration > PAM Order** from the menu bar. A sample screenshot of PAM Ordering Page is shown below.

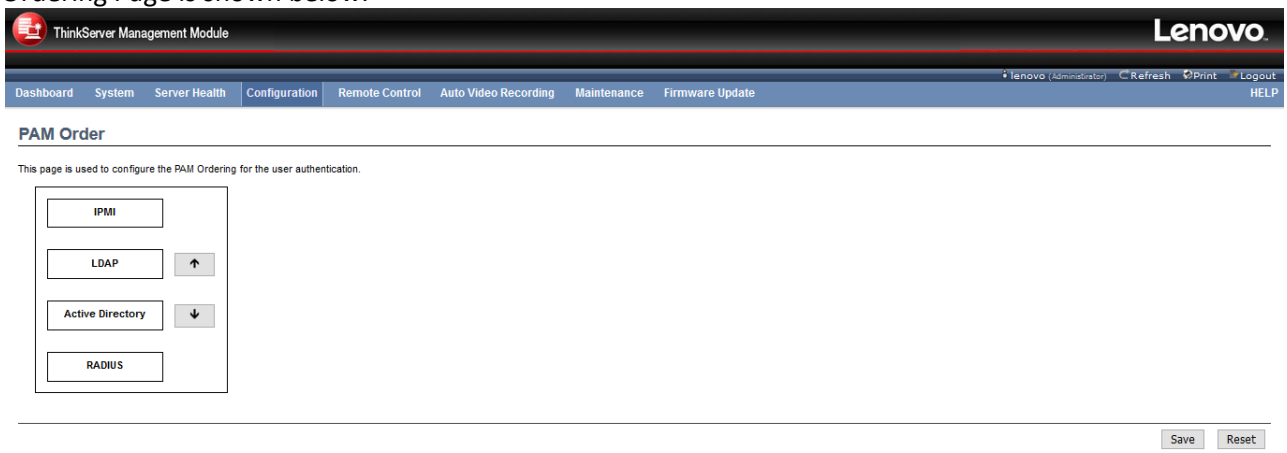


Figure 26. PAM Ordering Page

- **PAM Module**: It shows the list of available PAM modules supported in the BMC.
- **IPMI:** The PAM Module of IPMI.
- **LDAP:** The PAM Module of LDAP.
- **Active Directory:** The PAM Module of Active Directory.
- **RADIUS:** The PAM Module of RADIUS.
- **Move Up**: Click on the required PAM module, it will be selected. Click on 'Move Up' option to move the selected PAM module one step before the existing PAM module.
- **Move Down**: Click on the required PAM module, it will be selected. Click on 'Move Down' option to move the selected PAM module one step after the existing PAM module.
- **Save**: Click 'Save' to save any changes made.
  NOTE: Whenever the configuration is modified, the web server will be restarted automatically. Logged-in session will be logged out.
- **Reset**: Click 'Reset' to reset the modified changes.

PEF

This page is used to configure Event Filter, Alert Policy and LAN Destination for alerts. To view the page, user must at least be an Operator. To modify or add a PEF, user must be an Administrator(or OEM Proprietary).
NOTE: Free slots are denoted by '~' in all columns of the particular slot.
For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.
To open PEF Management Settings page, click **Configurations > PEF** from the menu bar. Each tab is explained below.

- **Event Filter:** Click the Event Filter tab to show any configured Event filters and available slots. You can modify or add new event filter entry from here. By default, 15 event filter entries are configured among the 40 available slots.
  - PEF ID: Displays ID for the configured PEF entry.
  - Filter Configuration: Displays the PEF entry setting is enabled or disabled.
  - Event Filter Action: This is a mandatory field and is checked by default. This action enables PEF Alert

action.
- Event Severity: Displays the PEF entry setting of event severity.
- Sensor Name: Displays the PEF entry setting of sensor name.

- **Alert Policy:** Click the Alert policy tab to show any configured Alert policies and available slots. You can modify or add new alert policy entry from here. A maximum of 60 slots are available.
  - Policy Entry #: Displays the Policy Entry number.
  - Policy Number: Displays the Policy Number that was configured in Event filter table.
  - Policy Configuration: Displays the Policy setting is enabled or disabled.
  - Policy Set: Displays the Policy Set value.
  - Channel Number: Displays the Policy setting of channel number.
  - Destination Selector: Displays the Policy setting of destination selector.
- **LAN Destination:** Click the LAN Destination tab to show any configured LAN destinations and available slots. You can modify or add new LAN destination entry from here. A maximum of 15 slots are available.
  - LAN Destination: Displays the LAN Destination number.
  - Destination Type: Displays the Destination Type.
  - Destination Address: Displays the Destination Address.

Event Filter

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 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. A sample screenshot of Event Filter page is given below.

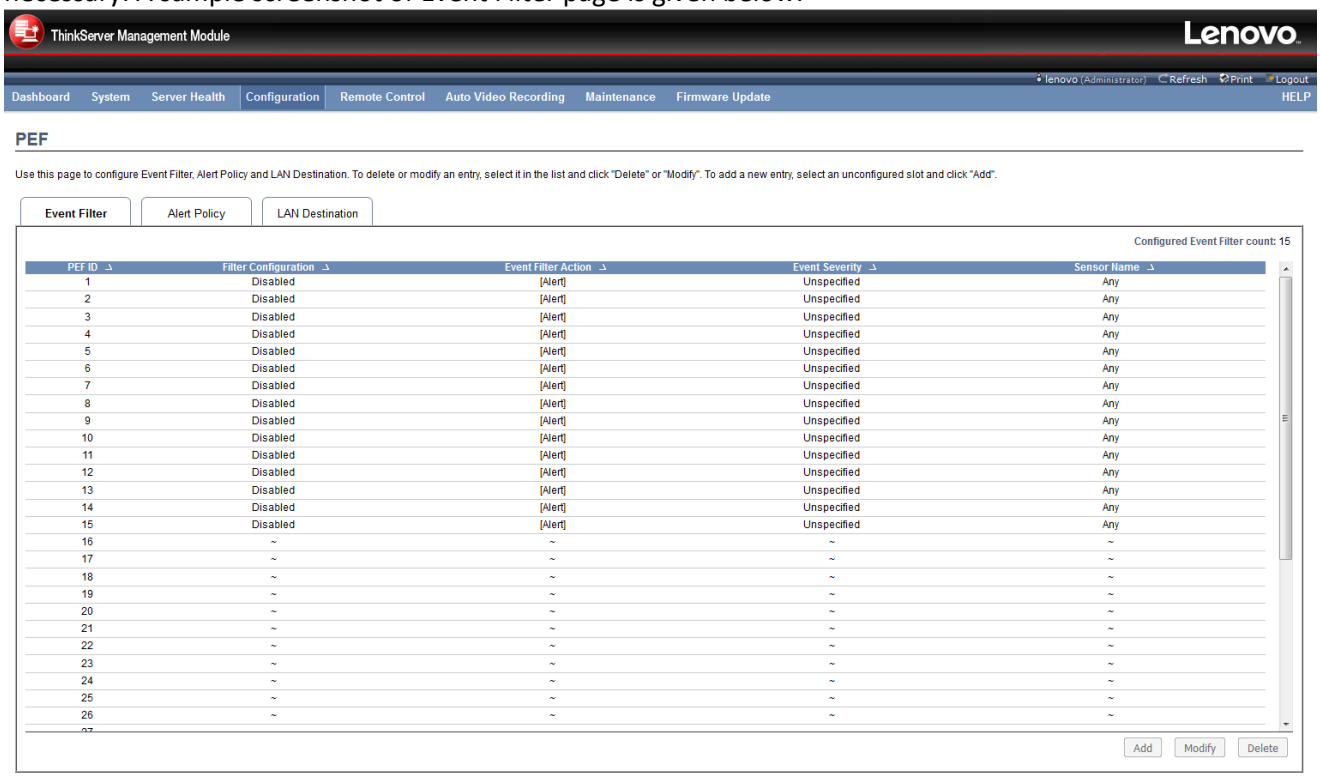


Figure 27. PEF Management – Event Filter page

The fields of PEF Management – Event Filter Tab are explained below. This page contains the list of configured

PEF's

- **Add:** Select a free slot and click 'Add' to add a new entry to the device. Alternatively, double click on a free slot.
- **Modify:** Select a configured slot and click 'Modify' to modify the selected entry. Alternatively, double click on the configured slot.
- **Delete:** Select the configured slot to be deleted and click 'Delete'.

Modify Event Filter Entry:

This form is used to modify the existing Event Filter entry. For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.

- Click the **Event Filter** Tab to configure the event filters in the available slots
- To modify the selected entry, select a configured slot and click **Modify** or alternatively double click the configured slot to open the Modify event Filter entry Page. A sample screenshot of Modify Event Filter Page is shown below.

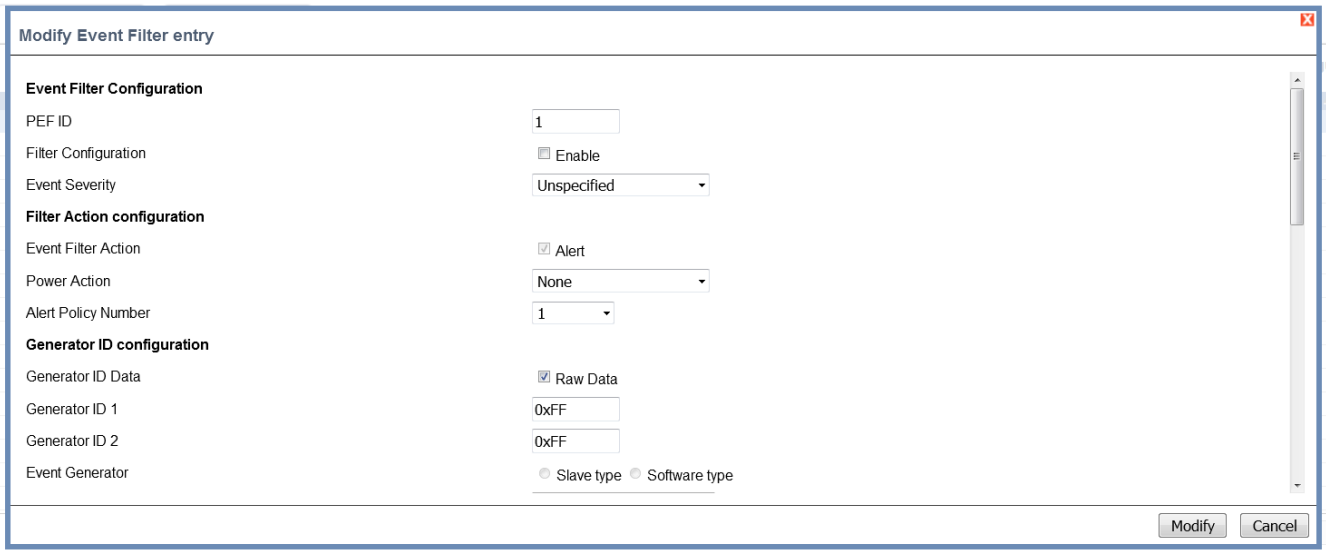


Figure 28. PEF Management – Modify Event Filter page

Event Filter Configuration

- **PEF ID:** Displays ID for the configured PEF entry(readonly).
- **Filter Configuration:** Check the option 'Enable' to enable the PEF settings.
- **Event Severity:** Choose any one of the Event Severity from the dropdown list.

Filter Action configuration

- **Event Filter Action:** This is a mandatory field and is checked by default. This action enables PEF Alert action (readonly).
- **Power Action:** Choose Power action to be either Power down, Power reset or Power cycle from the dropdown list.
- **Alert Policy Number:** Choose configured alert policy number from the dropdown list.
  NOTE: Alert Policy can be configured under Configuration->PEF->Alert Policy.

Generator ID configuration

- **Generator ID Data:** Enable this option to enter the Generator ID with raw data.
- **Generator ID 1:** Enter the raw generator ID1 data value.
- **Generator ID 2:** Enter the raw generator ID2 data value.
  NOTE: In the RAW data field, to specify hexadecimal value prefix the value with '0x'.
- **Event Generator:** Choose the event generator as Slave Address - if event is generated from IPMB else

Choose System Software ID - if event is generated from system software.

- **Slave Address/Software ID:** Specify corresponding I^2C Slave Address or System Software ID.
- **Channel Number:** Choose the particular channel number through which the event message is received over. Choose '0' if the event message is received via the system interface, primary IPMB, or internally generated by the BMC.
- **IPMB Device LUN:** Choose the corresponding IPMB device LUN if event generated by IPMB.

Sensor configuration

- **Sensor Type:** The type of sensor that will trigger the event filter action.
- **Sensor Name:** Choose the particular sensor from the sensor list.
- **Event Options:** Choose event option to be either All events or Sensor specific events.

Event Data configuration

- **Event Trigger:** This field is used to give Event/Reading type value.
  - Value ranges from 1 to 255
- **Event Data 1 AND Mask:** This field is used to indicate wildcarded or compared bits.
  - Value ranges from 0 to 255.
- **Event Data 1 Compare 1 & Event Data 1 Compare 2:** This field is used to indicate whether each bit position's comparison is an exact comparison or not.
  - Value ranges from 0 to 255.

Event Data 2 configuration

- **Event Data 2 AND Mask:** This field is similar to Event Data 1 AND Mask.
- **Event Data 2 Compare 1 & Event Data 2 Compare 2:** These fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

Event Data 3 configuration

- **Event Data 3 AND Mask:** This field is similar to Event Data 1 AND Mask.
- **Event Data 3 Compare 1 & Event Data 3 Compare 2:** These fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

- **Modify:** Click 'Modify' to accept the modification and return to Event filter list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to Event filter list.

Add Event Filter:

Use this form to add a new Event Filter entry. For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.

- Click the **Event Filter** Tab to configure the event filters in the available slots
- To Add an Event Filter entry, select a free slot and click **Add** or alternatively double click the empty slot to open the Add event Filter entry Page.

A sample screenshot of Add Event Filter Page is shown below.

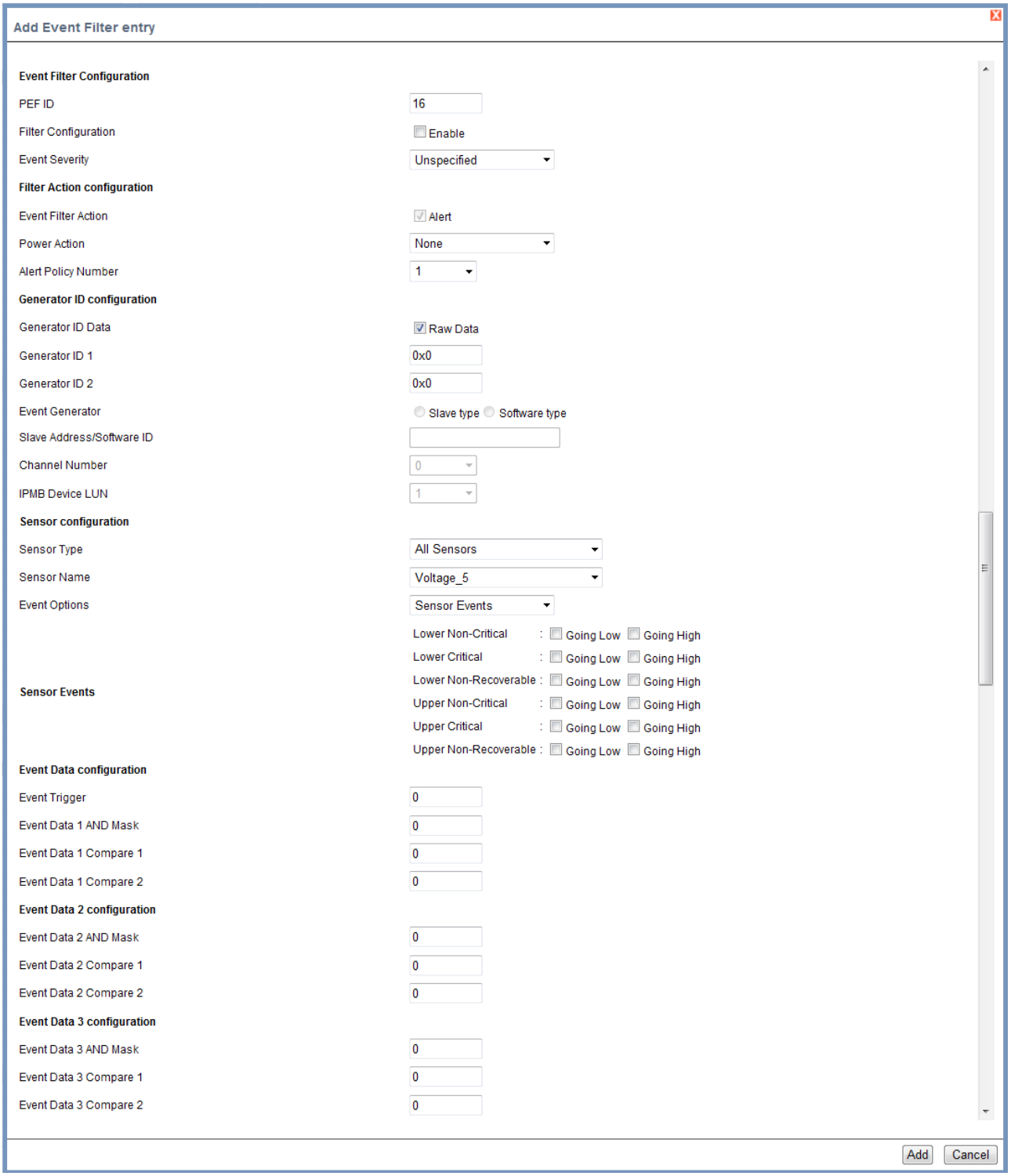


Figure 29. PEF Management – Add Event Filter Entry Page

Event Filter Configuration

- **PEF ID:** Displays ID for the newly configured PEF entry (readonly).
- **Filter Configuration:** Check the option 'Enable' to enable the PEF settings.
- **Event Severity:** Choose any one of the Event Severity from the dropdown list.

Filter Action configuration

- **Event Filter Action:** This is a mandatory field and is checked by default. This action enables PEF Alert action (readonly).
- **Power Action:** Choose Power action to be either Power down, Power reset or Power cycle from the dropdown list.
- **Alert Policy Number:** Choose configured alert policy number from the dropdown list.
  NOTE: Alert Policy can be configured under Configuration->PEF->Alert Policy.

Generator ID configuration

- **Generator ID Data:** Enable this option to enter the Generator ID with raw data.
- **Generator ID 1:** Enter the raw generator ID1 data value.
- **Generator ID 2:** Enter the raw generator ID2 data value.
  NOTE: In the RAW data field, to specify hexadecimal value prefix the value with '0x'.
- **Event Generator:** Choose the event generator as Slave Address - if event is generated from IPMB else Choose System Software ID - if event is generated from system software.
- **Slave Address/Software ID:** Specify corresponding I^2C Slave Address or System Software ID.
- **Channel Number:** Choose the particular channel number through which the event message is received over. Choose '0' if the event message is received via the system interface, primary IPMB, or internally generated by the BMC.
- **IPMB Device LUN:** Choose the corresponding IPMB device LUN if event generated by IPMB.

Sensor configuration

- **Sensor Type:** The type of sensor that will trigger the event filter action.
- **Sensor Name:** Choose the particular sensor from the sensor list.
- **Event Options:** Choose event option to be either All events or Sensor specific events.
- **Sensor Events:** The list of all the possible events for the selected sensors.

Event Data configuration

- **Event Trigger:** This field is used to give Event/Reading type value.
  - Value ranges from 1 to 255
- **Event Data 1 AND Mask:** This field is used to indicate wildcarded or compared bits.
  - Value ranges from 0 to 255.
- **Event Data 1 Compare 1 & Event Data 1 Compare 2:** This field is used to indicate whether each bit position's comparison is an exact comparison or not.
  - Value ranges from 0 to 255.

Event Data 2 configuration

- **Event Data 2 AND Mask:** This field is similar to Event Data 1 AND Mask.
- **Event Data 2 Compare 1 & Event Data 2 Compare 2:** These fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

Event Data 3 configuration

- **Event Data 3 AND Mask:** This field is similar to Event Data 1 AND Mask.
- **Event Data 3 Compare 1 & Event Data 3 Compare 2:** These fields are similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

- **Add**: Click on 'Add' to save the new event filter entry and return to Event filter list.
- **Cancel**: Click 'Cancel' to cancel the modification and return to Event filter list.

Alert Policy

This page is used to configure the Alert Policy for the PEF configuration. You can add, delete or modify an entry in this page. A sample screenshot of Alert Policy page is given below.

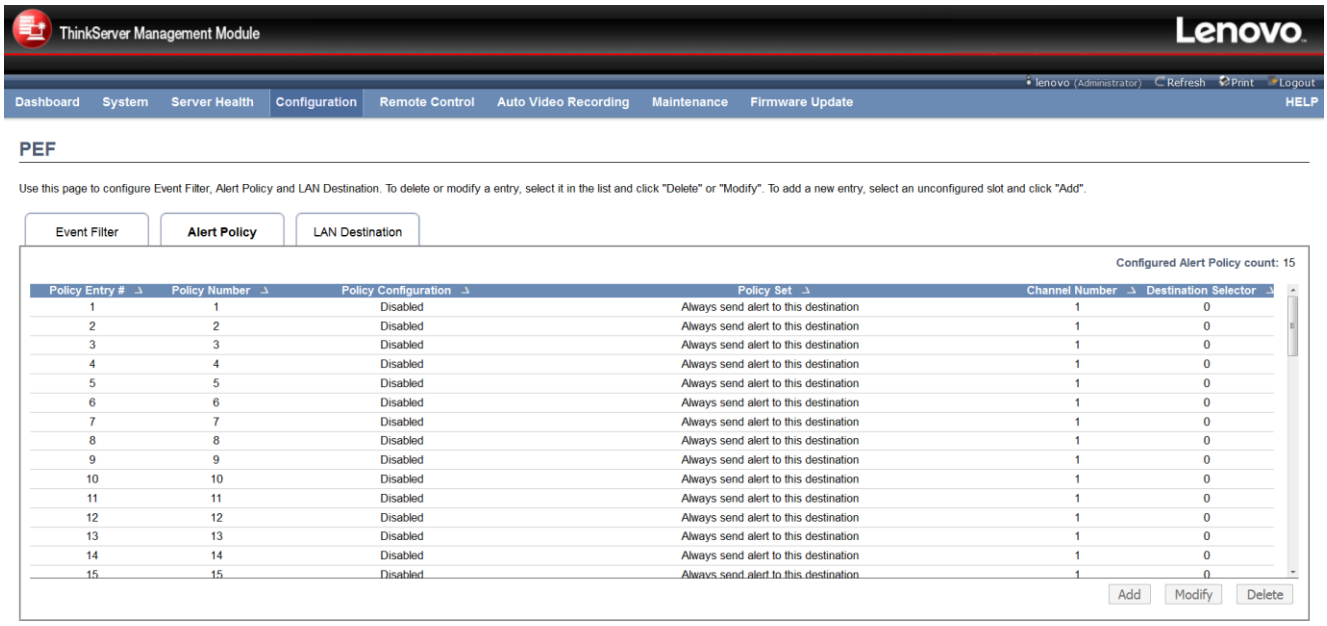


Figure 30. PEF Management – Alert Policy Page

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

- **Add:** Select a free slot and click 'Add' to add a new entry to the device. Alternatively, double click on a free slot.
- **Modify:** Select a configured slot and click 'Modify' to modify the selected entry. Alternatively, double click on the configured slot.
- **Delete:** Select the configured slot to be deleted and click 'Delete'.

Modify Alert Policy Entry:

This form is used to modify the existing Alert Policy entry. For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.

- 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.
- Select the slot and click **Modify** or alternatively double click on the configured slot to open the **Modify Alert Policy Entry Page** as shown in the screenshot below.

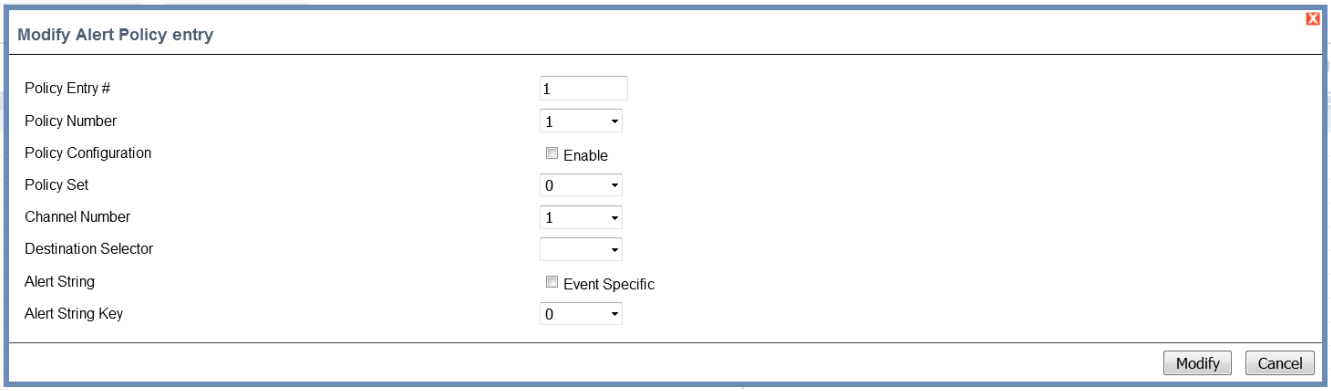


Figure 31. PEF Management – Modify Alert Policy Page

- **Policy Entry #:** This field displays Policy entry number of the selected slot (readonly).
- **Policy Number:** Choose the policy number that was configured in Event filter table.
- **Policy Configuration:** Check the option 'Enable' to enable the policy settings.
- **Policy Set:** 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:** Choose a particular channel from the available channel list.
- **Destination Selector:** Choose a particular destination from the configured destination list.
  NOTE: LAN Destination have to be configured - under Configuration->PEF->LAN Destination.
- **Alert String:** Check the box to specify an event-specific Alert String.
- **Alert String Key:** Choose from a set of values, all linked to strings kept in the PEF configuration parameters, to specify which string is to be sent for this Alert Policy entry.
- **Modify:** Click 'Modify' to accept the modification and return to Alert Policy list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to Alert Policy list.

Add Alert Policy Entry:

This form is used to add a new Alert Policy entry. For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.

- 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.
- Select the slot and click **Add** or alternatively double click on the empty slot to open the **Add Alert Policy Entry Page** as shown in the screenshot below.

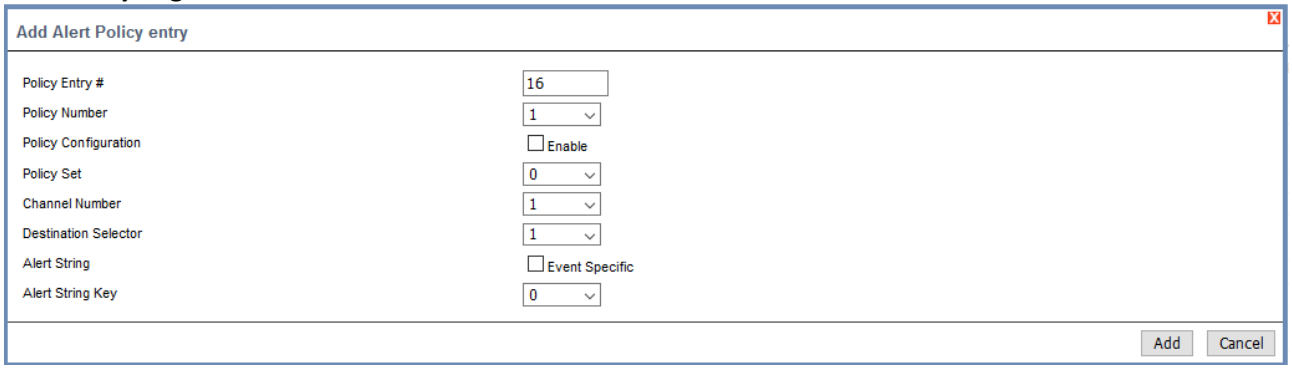


Figure 32. PEF Management – Add Alert Policy Entry Page

- **Policy Entry #:** This field displays Policy entry number of the selected slot (readonly).
- **Policy Number:** Choose the policy number that was configured in Event filter table.
- **Policy Configuration:** Check the option 'Enable' to enable the policy settings.
- **Policy Set:** 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:** Choose a particular channel from the available channel list.
- **Destination Selector:** Choose a particular destination from the configured destination list.
  NOTE: LAN Destination have to be configured - under Configuration->PEF->LAN Destination.
- **Alert String:** Check the box to specify an event-specific Alert String.
- **Alert String Key:** Choose from a set of values, all linked to strings kept in the PEF configuration parameters, to specify which string is to be sent for this Alert Policy entry.
- **Add:** Click 'Add' to save the new alert policy and return to Alert Policy list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to Alert Policy list.

LAN Destination

This page is used to configure the LAN destination of PEF configuration. A sample screenshot of LAN Destination page is given below.

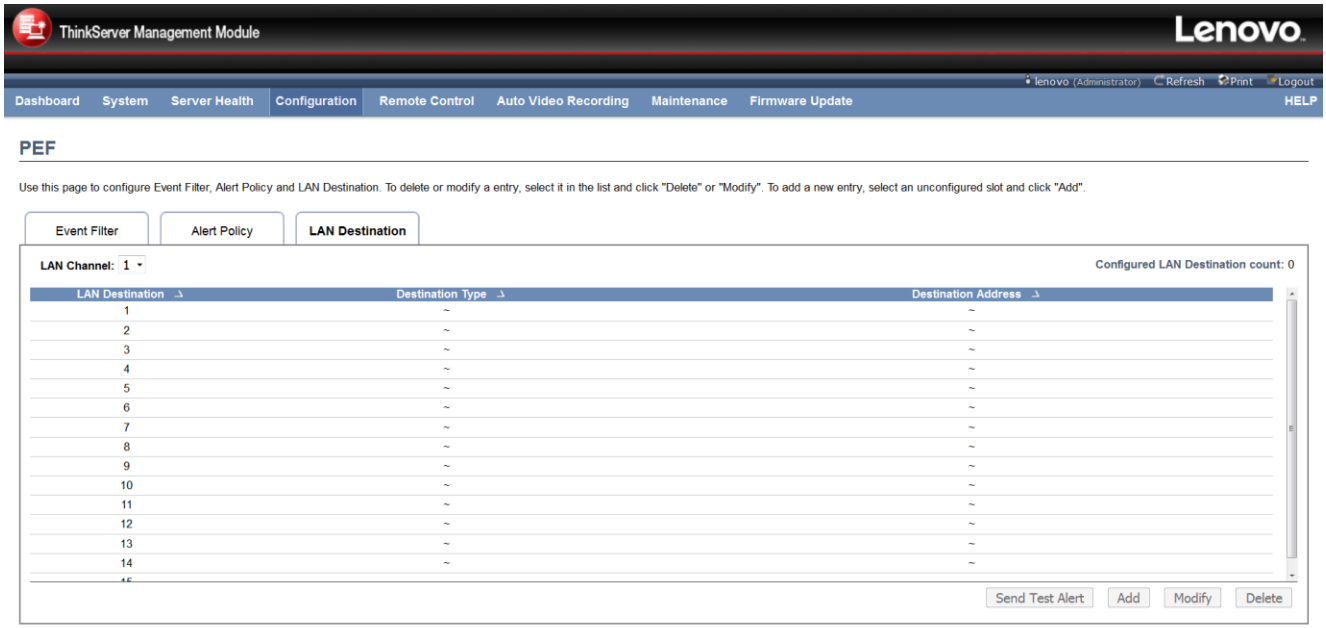


Figure 33. PEF Management – LAN Destination Page

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

- **LAN Channel:** Select the LAN Channel from the list to be configured.
- **Send Test Alert:** Select a configured slot in LAN Destination tab and click 'Send Test Alert' to send sample alert to configured destination.
  NOTE: Test alert can be sent only when SMTP configuration is enabled. SMTP support can be enabled under Configuration->SMTP. Also make sure that SMTP server address and port numbers are configured properly.
- **Add:** Select a free slot and click 'Add' to add a new entry to the device. Alternatively, double click on a free slot.
- **Modify:** Select a configured slot and click 'Modify' to modify the selected entry. Alternatively, double click

on the configured slot.

- **Delete:** Select the configured slot to be deleted and click 'Delete'.

Modify LAN Destination entry:

This form is used to modify the existing LAN destination entry.

- 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
- Select the slot and click **Modify** or alternatively double click on the configured slot. This opens the **Modify LAN Destination entry.**

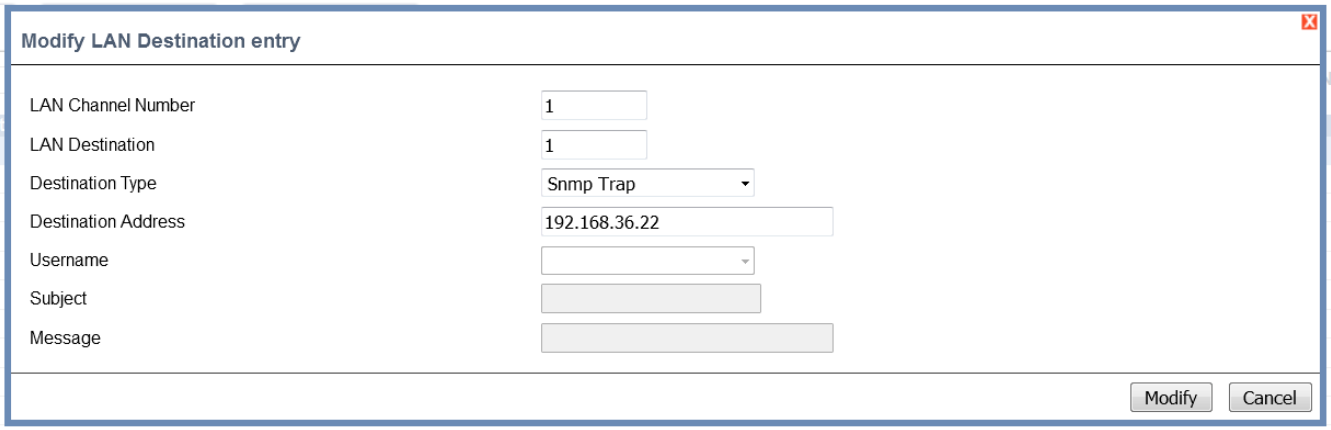


Figure 34. PEF Management – Modify LAN Destination Entry Page

- **LAN Channel Number:** Displays LAN Channel Number of the selected slot (readonly).
- **LAN Destination:** Displays Destination number of the selected slot (readonly).
- **Destination Type:** The destination type can be either an SNMP Trap or an Email alert. For SNMP Trap, destination IP address has to be filled. For Email alert, 3 fields Username, subject and body of the message have to be filled. The SMTP server information also has to be added under **Configuration->SMTP.**
- **Destination Address:** If Destination type is SNMP Trap, then give the IP address of the system that will receive the alert. Destination address will support the following:
  - IPv4 address format.
  - IPv6 address format.
- **Username:** If Destination type is Email Alert, then choose the user to whom the email alert has to be sent. **NOTE:** Email address for the user has to be configured under Configuration->Users.
- **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 of the user 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.
  NOTE: These fields are not applicable for 'AMI-Format' email users.
- **Modify:** Click 'Modify' to accept the modification and return to LAN destination list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to LAN destination list.

Add LAN Destination entry:

Use this form to add a new LAN destination entry.

- 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

- Select the slot and click **Add** or alternatively double click on the empty slot. This opens the **Add LAN Destination entry**.

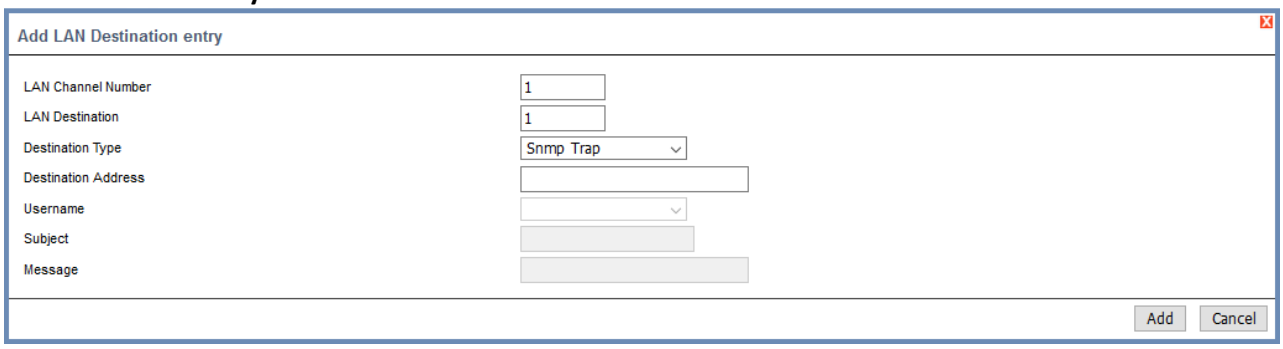


Figure 35. PEF Management – Add LAN Destination Entry Page

- **LAN Channel Number:** Displays LAN Channel Number of the selected slot (readonly).
- **LAN Destination:** Displays Destination number of the selected slot (readonly).
- **Destination Type:** The destination type can be either an SNMP Trap or an Email alert. For SNMP Trap, destination IP address has to be filled. For Email alert, 3 fields Username, subject and body of the message have to be filled. The SMTP server information also has to be added under Configuration->SMTP.
- **Destination Address:** If Destination type is SNMP Trap, then give the IP address of the system that will receive the alert. Destination address will support the following:
  - IPv4 address format.
  - IPv6 address format.
- **Username:** If Destination type is Email Alert, then choose the user to whom the email alert has to be sent. **NOTE:** Email address for the user has to be configured under Configuration->Users.
- **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 of the user 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. **NOTE:** These fields are not applicable for 'AMI-Format' email users.
- **Add:** Click on 'Add' to save the new LAN destination and return to LAN destination list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to LAN destination list.

RADIUS

To enable/disable RADIUS, check or uncheck the RADIUS Authentication Enable checkbox respectively.
NOTE: Generic Free RADIUS alone is supported.
RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities, and open RADIUS Settings page, click **Configuration > RADIUS** from the menu bar. A sample screenshot of RADIUS Settings Page is shown below.

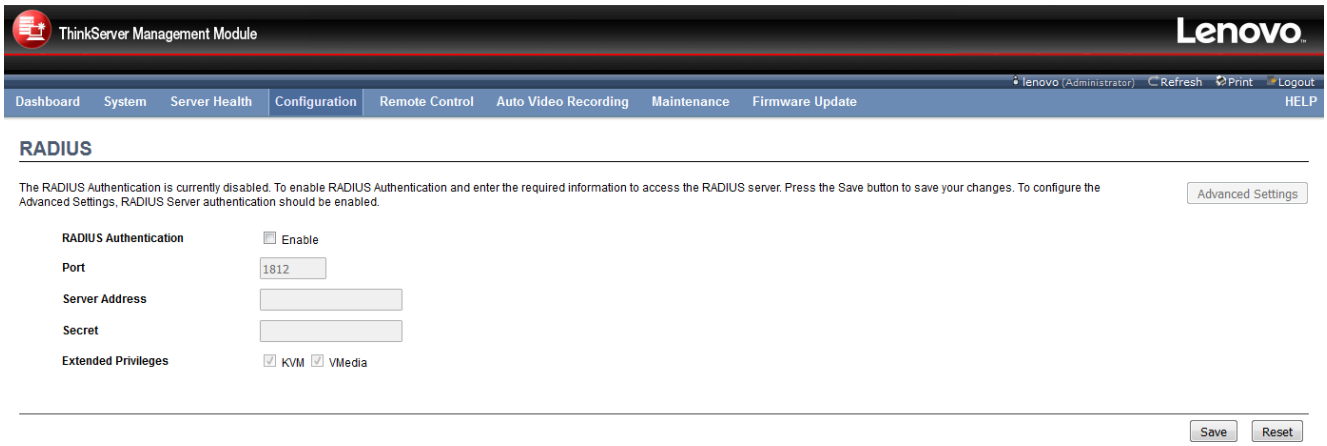


Figure 36. RADIUS Settings Page

The fields of RADIUS Settings Page are explained below.

- **RADIUS Authentication**: Check the option 'Enable' to enable RADIUS authentication.
- **Port**: Specify the RADIUS Port.
  - Default Port is 1812.
  - Port value ranges from 1 to 65535.
- **Server Address**: Enter the 'Server address' of RADIUS server. Server address will support the following:
  - IP Address (Both IPv4 and IPv6 format).
  - FQDN (Fully qualified domain name) format.
- **Secret**: Enter the 'Authentication Secret' for RADIUS server
  - Secret must be at least 4 characters long.
  - White space is not allowed.

  NOTE: This field will not allow more than 31 characters.
- **Extended Privileges:** This field is used to assign KVM and VMedia privilege for the user.
  NOTE: The KVM and VMedia privilege will enable(disable) automatic when User Privilege is administrator(other).
- **Advanced Settings:** Click 'Advanced Settings' to Radius User Authorization.
- **Save**: Click 'Save' to save the settings.
- **Reset**: Click 'Reset' to reset the modified changes.

Advanced Settings

Use this page to Configure Advanced Radius Authorization Setting.

- Enable the **RADIUS Authentication** check box to authenticate the RADIUS.
- Click **Advanced Settings**, this opens the Radius Authorization window as shown below.

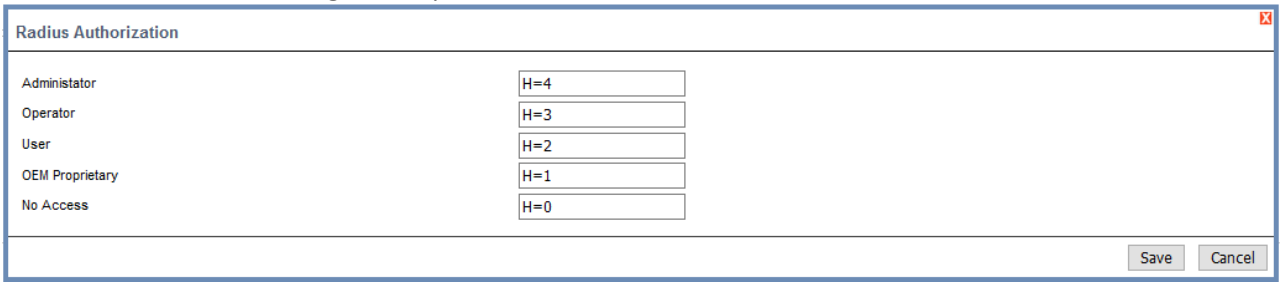


Figure 37. RADIUS Authorization Page

- **Administrator:** Setting Administrator with Vendor Specific Attribute in Server side.

- **Operator:** Setting Operator with Vendor Specific Attribute in Server side.
- **User:** Setting User with Vendor Specific Attribute in Server side.
- **OEM Proprietary:** Setting OEM Proprietary with Vendor Specific Attribute in Server side.
- **No Access:** Setting No Access with Vendor Specific Attribute in Server side.
  NOTE: This fields will not allow more than 127 characters. '#' is not allowed.
- **Save:** Click 'Save' to save the settings.
- **Cancel:** Click 'Cancel' to cancel the modified changes.

Remote Session

This page is used to configure virtual media settings for the next redirection session. “Single Port Application” is enabled by default. While disabling “Single Port Application” KVM and Media Encryption are disabled by default, and open Remote Session page, click **Configuration > Remote Session** from the menu bar. A sample screenshot of Remote Session Page is shown below.

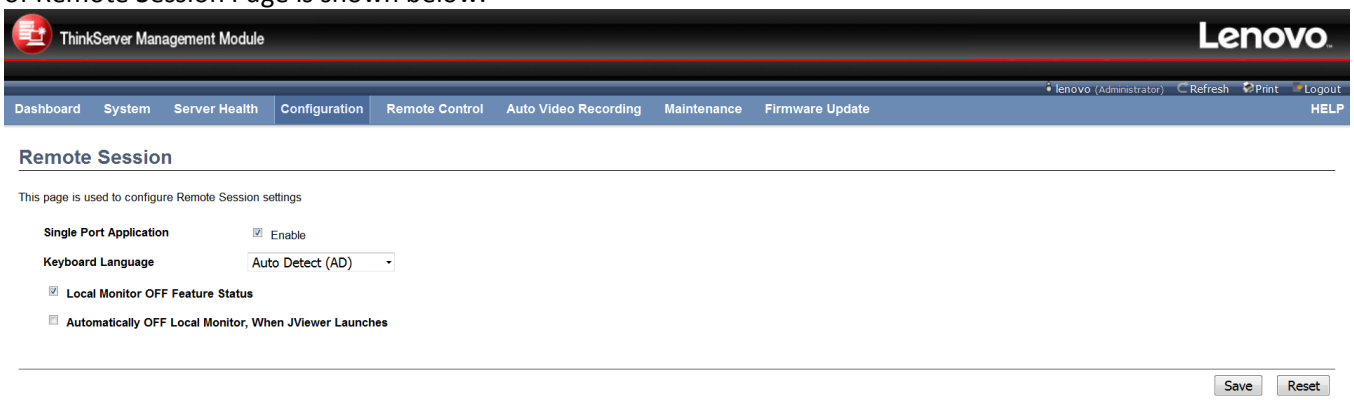


Figure 38. Remote Session Page

The fields of Configure Remote Session Page are explained below.

- **Single Port Application**: This select box is used to enable the single port application support at runtime.
- **KVM Encryption**: Enable/Disable encryption on KVM data for the next redirection session.
  NOTE: It will automatically close existing remote redirection either KVM or Virtual media sessions, if any.
- **Keyboard Language**: This select box is used to select the keyboard supported language.
- **Local Monitor OFF Feature Status**: Check this box to enable Local Monitor ON/OFF command.
- **Automatically OFF Local Monitor, When JViewer Launches**: Check this box to automatically Lock the local monitor, When JViewer launches.
- **Save**: Click 'Save' to save the current changes.
- **Reset:** Click 'Reset' to reset the modified changes.

Services

This page displays basic information about services running in the BMC. To modify a service, user must be an Administrator(or OEM Proprietary). And open Services page, click **Configuration > Services** from the menu bar. A sample screenshot of Services Page is shown below.

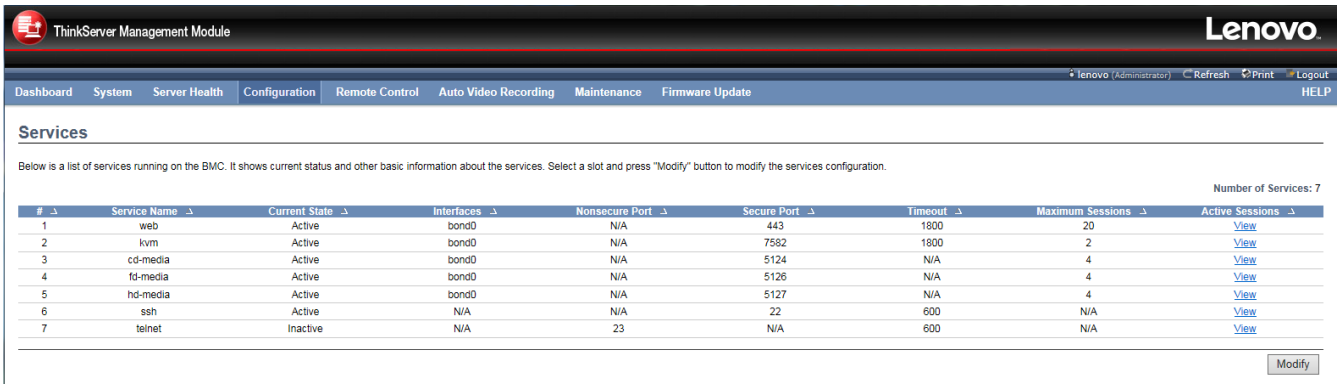


Figure 39. Services Page

The fields of Services Page are explained below.

- **# :** The number of service.
- **Service Name**: Displays service name of the selected slot (read-only).
- **Current State**: Displays the current status of the service, either active or inactive state.
- **Interfaces**: It shows the interface in which service is running.
- **Nonsecure Port**: This port is used to configure nonsecure port number for the service.
- **Secure Port**: Used to configure secure port number for the service.
- **Timeout**: Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.
- **Maximum Sessions**: Displays the maximum number of allowed sessions for the service.
- **Active Sessions**: To view the current active sessions for the service.
- **Modify**: Select a slot and click 'Modify' to modify the configuration of the service. Alternatively, double click on the slot.
  NOTE: Whenever the configuration is modified, the service will be restarted automatically. The changes will be available only when the user closes the opened sessions.

Active Session:

This page displays basic information about the Active sessions, which are present in BMC from various services. To Terminate the session, user must be an Administrator(or OEM Proprietary).

- Click **View** to view the details about the active sessions for the service.
- This opens the **Active Session** screen (for example - Web Service screen) as shown in the screenshot below.

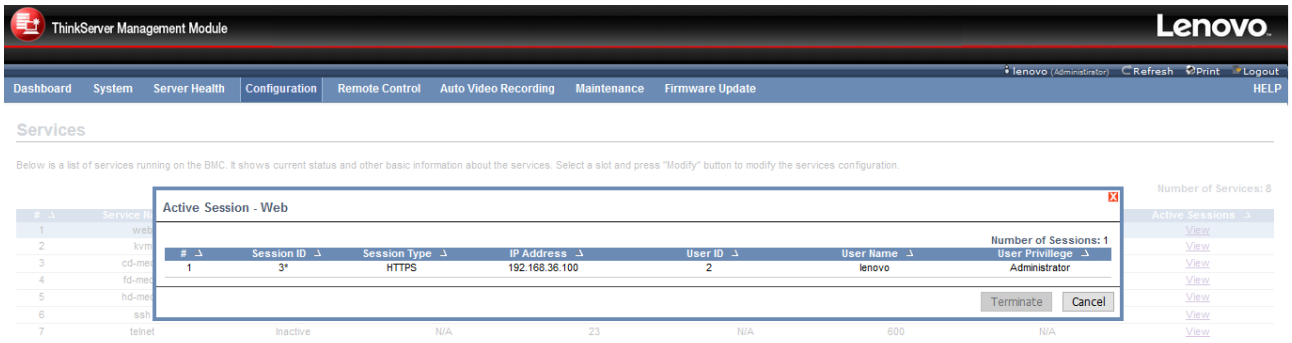


Figure 40. Active Session Page

- **#:** The serial number.
- **Session ID**: Displays the ID number of the active sessions.

- **Session Type**: Displays the type of the active sessions.
- **IP Address**: Displays the IP addresses that are already configured for the active sessions.
- **User ID**: Displays the ID number of the user.
- **User Name**: Displays the name of the user.
- **User Privilege**: Displays the access privilege of the user.
- **Terminate**: Select a slot and click 'Terminate' to terminate the particular session of the service.
- **Cancel:** Click 'Cancel' to cancel the modification and return to Services list.

  NOTE: The default user id's for various PAM Module users are,
  - Active Directory User is 30
  - LDAP/E-Directory User is 20
  - RADIUS User is 40

Modify Service:

Use this form to modify the configuration of the services running in the BMC.

- Select a slot and click **Modify** to modify the configuration of the service. Alternatively, double click on the slot.
- This opens the **Modify Service** screen as shown in the screenshot below.

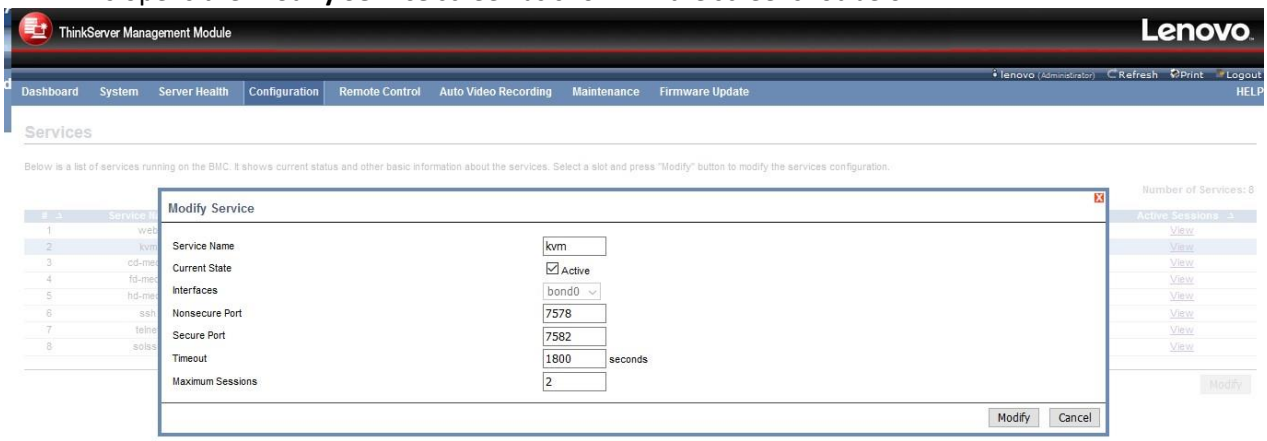


Figure 41. Modify Service Page

- **Service Name:** Displays service name of the selected slot (readonly).
- **Current State:** Displays the current status of the service, either active or inactive. Check this box to start the inactive service.
- **Interface:** It shows the interface on which service is running. The user can choose any one of the available interfaces.

  NOTE:
  - Service mapping to disabled interfaces will not work. Status of Interface can be checked/enabled, under Configuration -> Network -> LAN Settings.
  - KVM and Media Interfaces are read-only, when single port is enabled.
- **Nonsecure Port:** Used to configure nonsecure port number for the service.
  - Telnet default port is 23.
  - Port value ranges from 1 to 65535.

  NOTE: Web/KVM/CD/FD/HD/SSH service will not support a nonsecure port.
- **Secure Port:** Used to configure secure port number for the service.
  - Web default port is 443.
  - KVM default port is 7582.

- CD Media default port is 5124.
- FD Media default port is 5126.
- HD Media default port is 5127.
- SSH default port is 22.
- Port value ranges from 1 to 65535.

NOTE: Telnet service will not support a secure port.

- **Timeout:** Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.
  - Web and KVM timeout value ranges from 300 to 1800 seconds.
  - Web timeout would be ignored if there exists any alive KVM session.
  - SSH and Telnet timeout value ranges from 60 to 1800 seconds.
  - SSH and telnet timeout value should be in multiples of 60 seconds.

  NOTE: SSH and telnet service will be using the same timeout value. If the user configures the SSH timeout value, that will be applied to the telnet service also, and vice versa.
- **Maximum Sessions:** Displays the maximum number of allowed sessions for the service.
- **Modify:** Click on 'Modify' to save the configuration for the service and return to Services list.
  NOTE: Already opened sessions for the service will be affected and service will be restarted.
- **Cancel**: Click 'Cancel' to cancel the modification and return to Services list.

Interfaces

Use this page to configure the interface settings. A sample screenshot of Interfaces Settings Page is shown below.

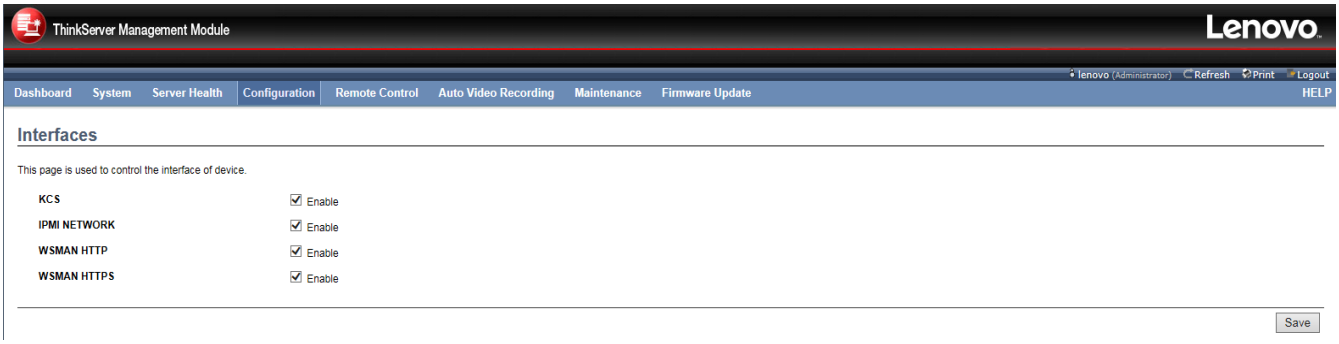


Figure 42. Interfaces Page

The fields of Interfaces Settings Page are explained below.

- **KCS**: Check the option 'Enable' to enable KCS.
- **IPMI NETWORK**: Check the option 'Enable' to enable IPMI Network.
  NOTE: When you disable this option, the device will create the firewall automatically, that's mean you can find the port of IPMI Network setting in page "System Firewall".
- **WSMAN HTTP**: Check the option 'Enable' to enable WSMAN HTTP.
  NOTE: When you disable this option, the device will create the firewall automatically, that's mean you can find the port of WSMAN HTTP setting in page "System Firewall".
- **WSMAN HTTPS**: Check the option 'Enable' to enable WSMAN HTTPS.
  NOTE: When you disable this option, the device will create the firewall automatically, that's mean you can find the port of WSMAN HTTP setting in page "System Firewall".
- **Save**: Click 'Save' to save any changes made.

SMTP

This page is used to configure the SMTP settings.

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

To open SMTP Settings page, click **Configuration > SMTP** from the menu bar.

A sample screenshot of SMTP Settings Page is shown below.

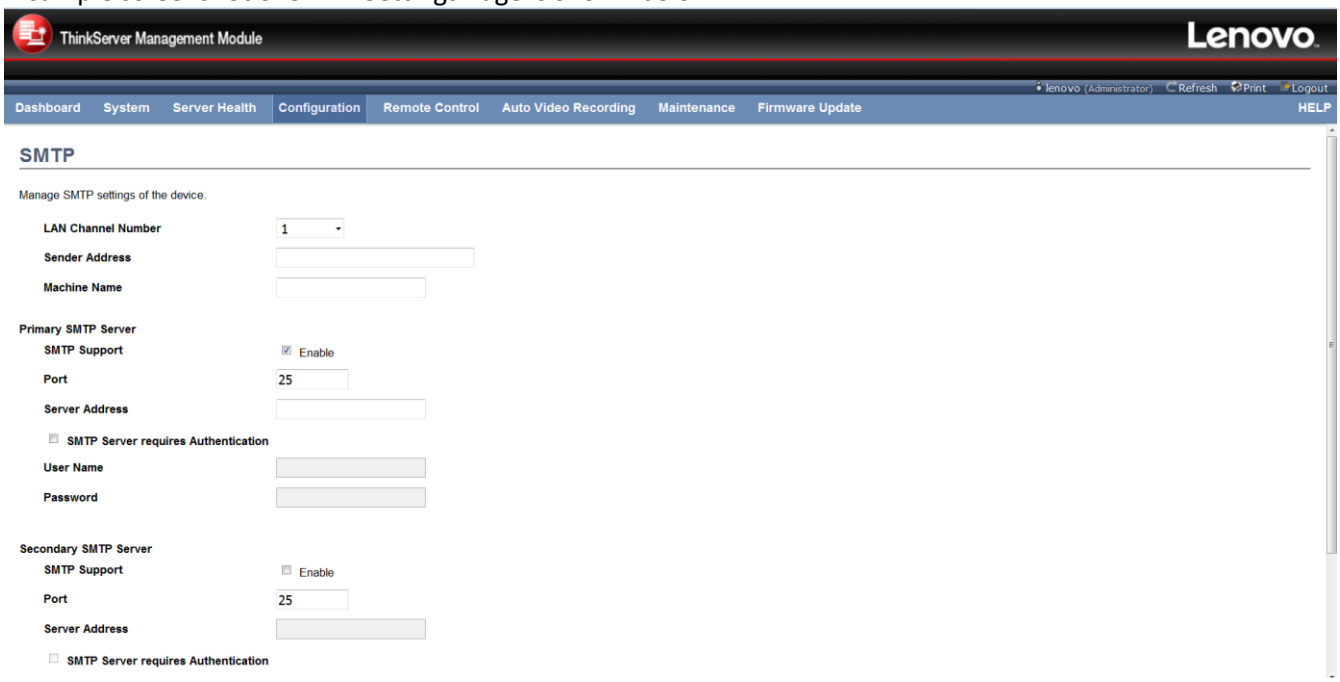


Figure 43. SMTP Page

The fields of SMTP Settings Page are explained below.

- **LAN Channel Number**: Select the LAN channel to which the SMTP information needs to be configured.
- **Sender Address**: Enter the 'Sender Address' valid on the SMTP Server.
- **Machine Name**: Enter the 'Machine Name' of the SMTP Server.
  - Machine Name is a string of maximum 15 alpha-numeric characters.
  - Space, special characters are not allowed.
- **Primary SMTP Server**: It lists the Primary SMTP Server configuration.
- **SMTP Support**: Check this option to enable SMTP support for the BMC.
- **Port**: Specify the SMTP Port.
  - Default Port is 25.
  - Port value ranges from 1 to 65535.
- **Server Address**: Enter the 'IP address' of the SMTP Server. It is a mandatory 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.

  Server address will support the following:
  - IPv4 Address format.
  - IPv6 Address format.
- **SMTP Server requires Authentication**: Check the option 'Enable' to enable SMTP Authentication.

Note: SMTP 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".*

- **User Name**: Enter username to access SMTP Accounts.
  - User Name can be of length 4 to 64 alpha-numeric characters, dot(.), dash(-), and underline(_).
  - It must start with an alphabet.
  - Other Special Characters are not allowed.
- **Password**: Enter the password for the SMTP User Account.
  - Password must be at least 4 characters long.
  - White space is not allowed.

  NOTE: This field will not allow more than 64 characters.
- **Secondary SMTP Server**: It lists the Secondary SMTP Server configuration. It is a optional field.
  If the Primary SMTP server is not working fine, then it tries with Secondary SMTP Server configuration.
- **Save:** Click 'Save' to save the new SMTP server configuration.
- **Reset**: Click 'Reset' to reset the modified changes.

SNMP

Use the page to configure the SNMP settings.

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for collecting and organizing information about managed devices on IP networks and for modifying that information to change device behavior.

To open SNMP Settings page, click **Configuration > SNMP** from the menu bar. A sample screenshot of SNMP Settings Page is shown below.

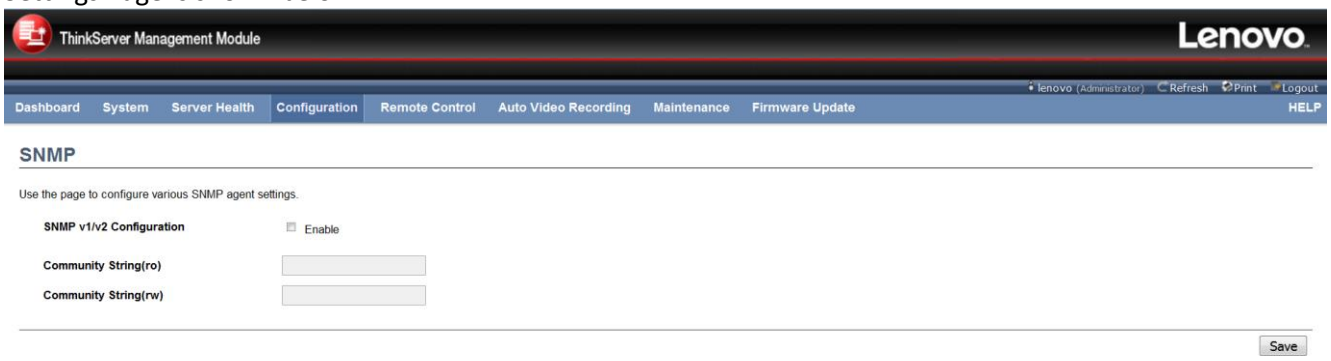


Figure 44. SNMP Page

The fields of SNMP Settings Page are explained below.

- **SNMP**: Check the option 'Enable' to enable SNMP.
- **SNMP v1/v2 Configuration**: Check the option 'Enable' to enable SNMP & SNMPv1 & SNMPv2c features.
- **Community String**: Community string is match in both SNMPv1 and SNMPv2c.
  - **Community String(ro)**: Community string for read-only access.
  - **Community String(rw)**: Community string for read-write access.
- **Save:** Click on 'Save' to save the SNMP configuration.

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 menu bar. There are three tabs in this page.
NOTE: This page provides a simple method to generate SSL certificate and it was not issued by a trusted Certificate Authority, you can upload a trusted certificate by yourself, if necessary.

- **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.

Upload SSL Tab

This page is used to upload a new SSL certificate and private key.
NOTE: Please check the current BMC time in NTP under Configuration menu while uploading the SSL certificate.
A sample screenshot of SSL Certificate Configuration – Upload SSL Page is shown below.

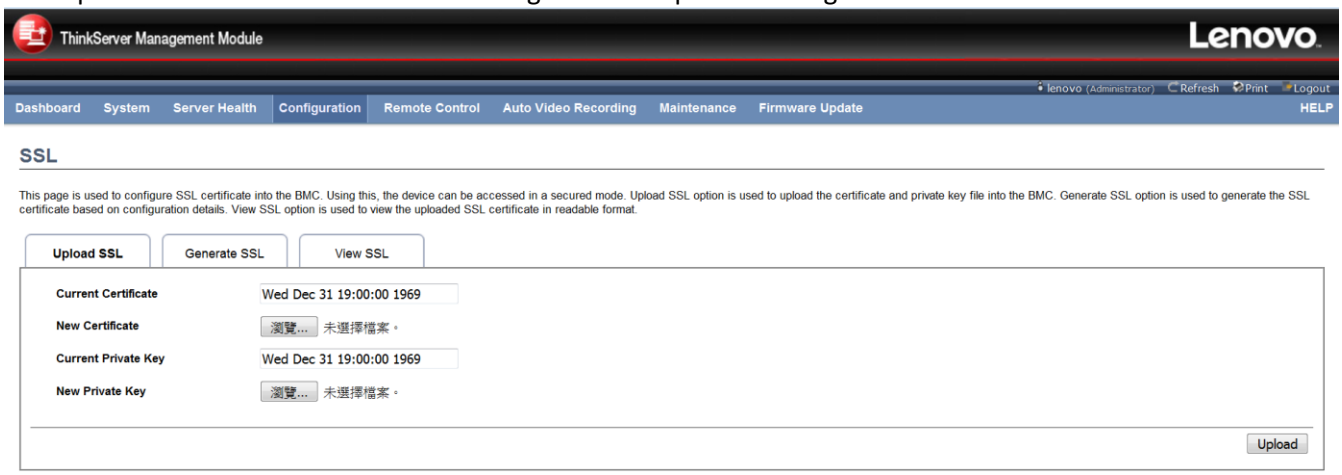


Figure 45. SSL Certificate Configuration – Upload SSL Page

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

- **Current Certificate**: The information as Current certificate and uploaded date/time will be displayed (read-only).
- **New Certificate**: Browse and navigate to the certificate file.
  - Certificate file should be of pem type
- **Current Private Key**: The information as current private key and uploaded date/time will be displayed (read-only).
- **New Private Key**: Browse and navigate to the private key file.
  - Private key file should be of the type pem
- **Upload**: Click 'upload' to upload the SSL certificate and private key into the BMC.
  NOTE: Upon successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

Generate SSL Tab

This tab is used to generate the SSL certificate using the configuration.
A sample screenshot of SSL Certificate Configuration – Generate SSL Page is shown below.

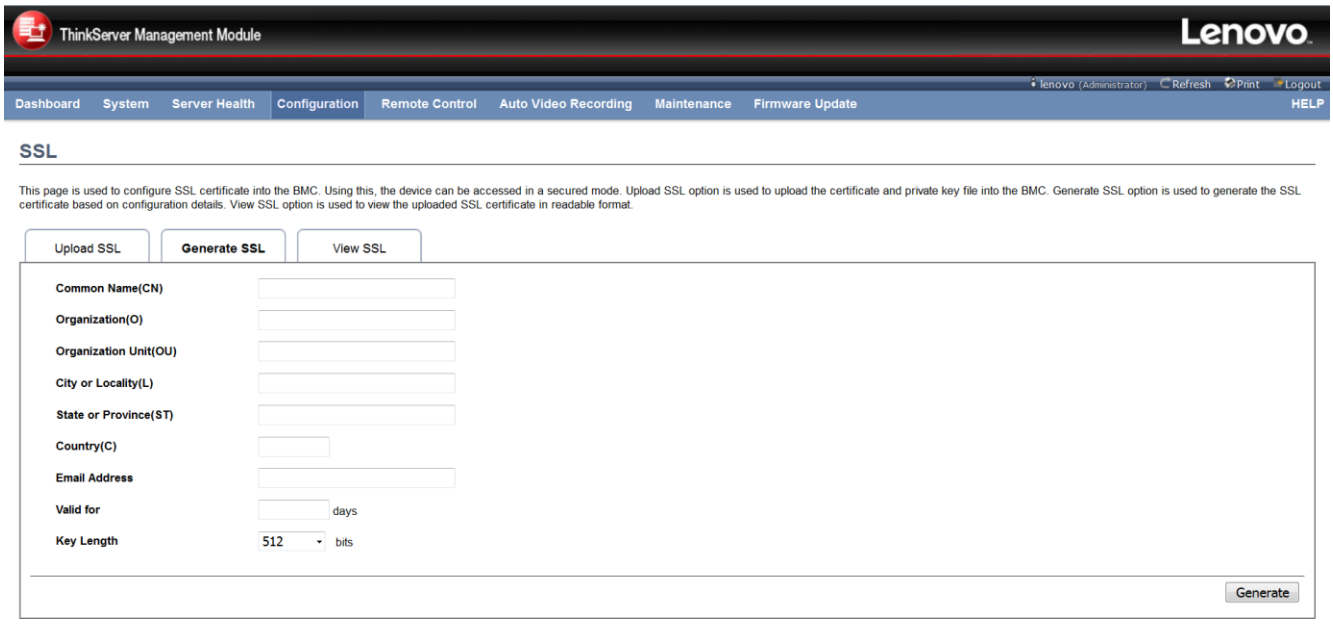


Figure 46. SSL Certificate Configuration – Generate SSL Page

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

- **Common Name(CN):** Common name for which the certificate is to be generated.
  - Maximum length of 64 characters.
  - It is a string of alpha-numeric characters.
  - Special characters '#' and '$' are not allowed.
- **Organization(O):** Organization name for which certificate to be generated.
  - Maximum length of 64 characters.
  - It is a string of alpha-numeric characters.
  - Special characters '#' and '$' are not allowed.
- **Organization Unit(OU)**: Over all organization section unit name for which certificate to be generated.
  - Maximum length of 64 characters.
  - It is a string of alpha-numeric characters.
  - Special characters '#' and '$' are not allowed.
- **City or Locality(L)**: City or Locality has to be given.
  - Maximum length of 64 characters.
  - It is a string of alpha-numeric characters.
  - Special characters '#' and '$' are not allowed.
- **State or Province(ST)**: State or Province has to be given.
  - Maximum length of 64 characters.
  - It is a string of alpha-numeric characters.
  - Special characters '#' and '$' are not allowed.
- **Country(C)**: Country code has to be given.
  - Only two characters are allowed.
  - Special characters are not allowed.
- **Email Address**: Email Address of the organization has to be given.
- **Valid for**: Number of days the certificate to be validated.
  - Value ranges from 1 to 3650 days.
- **Key Length**: Choose the key length bit value of the certificate.

- **Generate**: Click this option to generate the new SSL certificate.
  NOTE:
  - Upon successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.
  - HTTPs session will not work in some browsers for 512 bits of RSA Key, please check the official website of browser for details.

View SSL Tab

This tab is used to view the uploaded SSL certificate in user readable format.
A sample screenshot of SSL Certificate Configuration – View SSL Page is shown below.

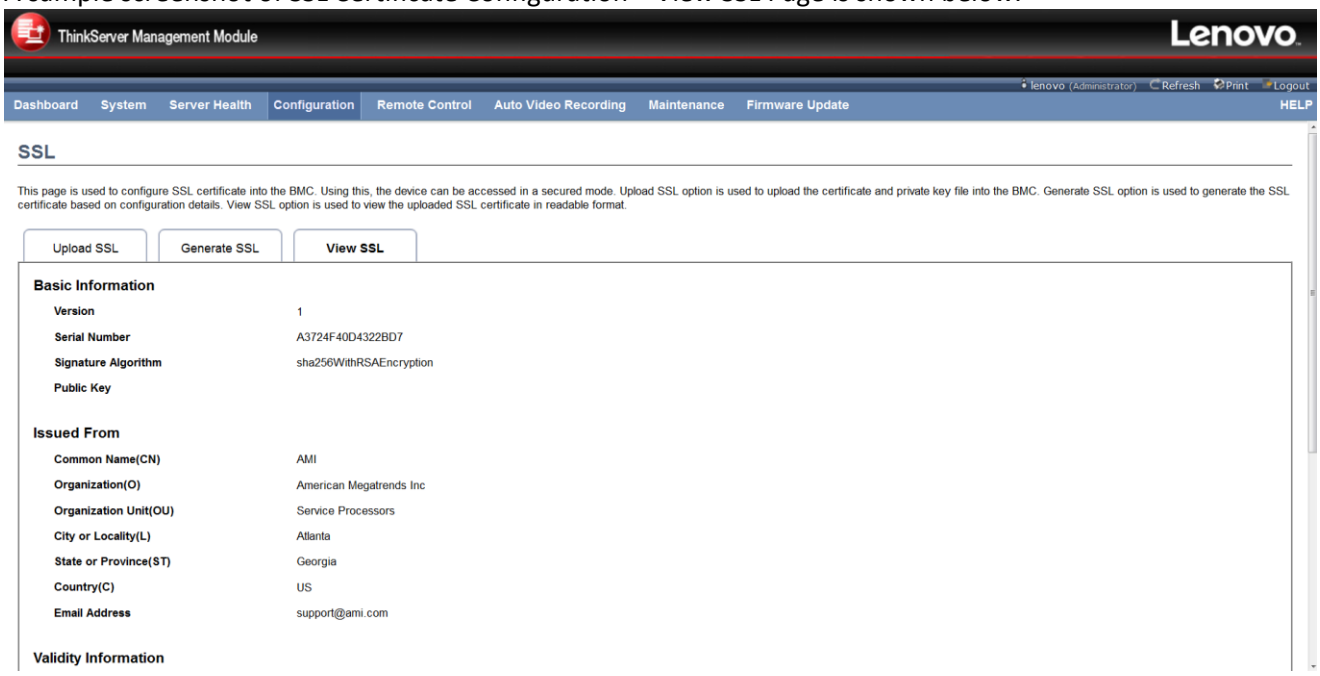


Figure 47. Certificate Configuration – View SSL Page

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

- **Basic Information**: It displays the basic information about the uploaded SSL certificate.It displays the following fields.
  - Version
  - Serial Number
  - Signature Algorithm
  - Public Key
- **Issued From**: This contains the information about the Certificate Issuer.
  - Common Name(CN)
  - Organization(O)
  - Organization Unit(OU)
  - City or Locality(L)
  - State or Province(ST)
  - Country(C)
  - Email Address
- **Validity Information**: It displays the validity period of the uploaded certificate.
  - Valid From
  - Valid To

- **Issued To**: It displays about the information to whom the certificate is issued.
  - Common Name(CN)
  - Organization(O)
  - Organization Unit(OU)
  - City or Locality(L)
  - State or Province(ST)
  - Country(C)
  - Email Address

System Firewall

This page is used to configure System Firewall support. To view the page, user must at least be an Operator.
To add or delete a firewall, user must be an Administrator(or OEM Proprietary).
The firewall rule can be set for an IP or range of IP Addresses or Port numbers. And open System Firewall page, click **Configuration > System Firewall** from the menu bar.

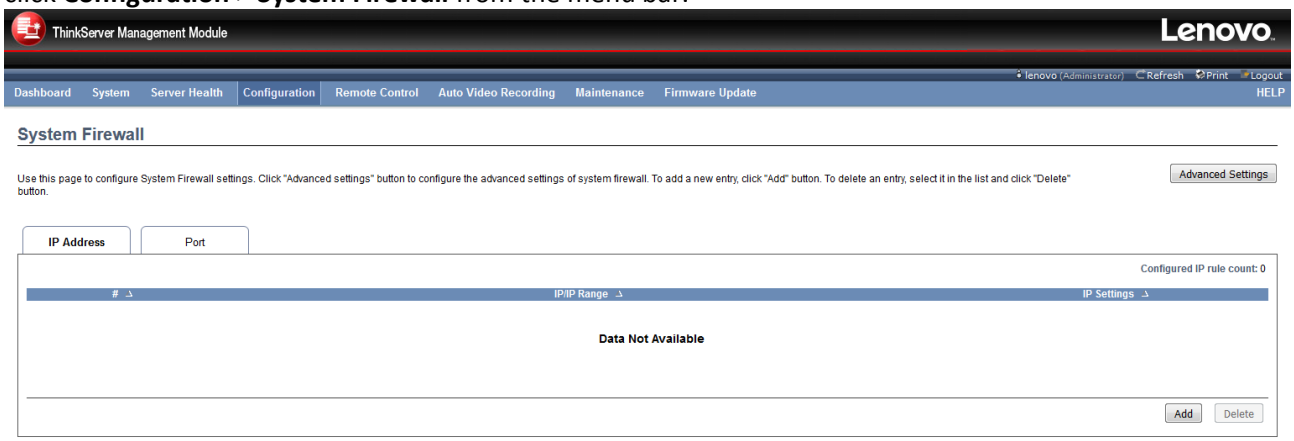


Figure 48. System Firewall Page

- **Advanced Settings**: Click this option to configure the Advanced Firewall Settings. Options are Block all and Flush all.
- **#**: The serial number.
- **IP/IP Range**: This field is used to show the IP Address or Range of IP Addresses that are already configured.
- **IP Settings**: This column indicates the current setting of the listed IP Address or Range of IP Addresses rules (Allow or Block).
- **Add**: Click 'Add' to add a new entry to the firewall rules list.
- **Delete**: Select the configured slot to be deleted and click 'Delete'.

Advanced Settings

This form is used to configure Advanced System Firewall settings.

- Click on the **Advanced Settings** button. This opens the Advanced Firewall Settings window as shown below.

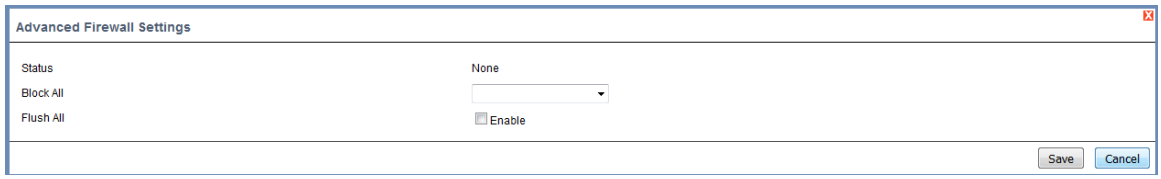


Figure 49. Advanced Firewall Page

- **Status:** Displays the type that will block.
- **Block All:** This option will block all incoming IPs and Ports.
- **Flush All:** This is used to flush all the system firewall rules.
- **Save:** Click 'Save' to save a configured entry.
- **Cancel:** Click 'Cancel' to cancel the modification to the existing settings.

Set system firewall for an IP or a range of IP Addresses:

This form is used to add a new IP Address or Range of IP Address rule settings.
Click Add button is shown below.

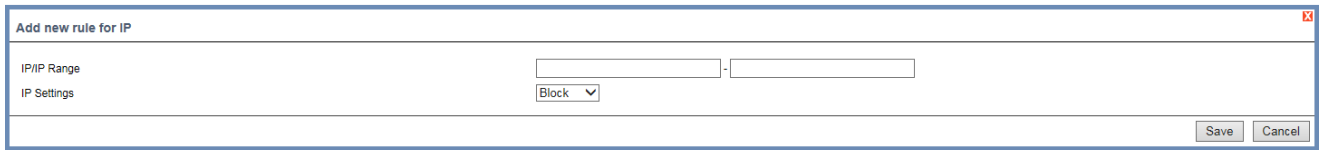


Figure 50. Add New Rule for IP Page

- **IP/IP Range:** This field is used to configure the IP Address or Range of IP Addresses.
  IP Address will support IPv4 and IPv6 Address formats:
  - 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 groups of 4 Hexadecimal digits separated by colon as in xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.
  - Hexadecimal digits are expressed as lower-case letters.
- **IP Settings:** IP Settings are used to determine the rule whether block or allow from the configured IP or IP Range.
- **Save:** Click 'Save' to save a configured entry
- **Cancel:** Click 'Cancel' to cancel the modification to the existing settings.

To set system firewall for a single port or range of Port numbers:

This page is used to configure System Firewall support. To view the page, user must at least be an Operator.
To add or delete a firewall, user must be an Administrator(or OEM Proprietary).
Click the Port tab. A sample screenshot of Port tab is shown below.

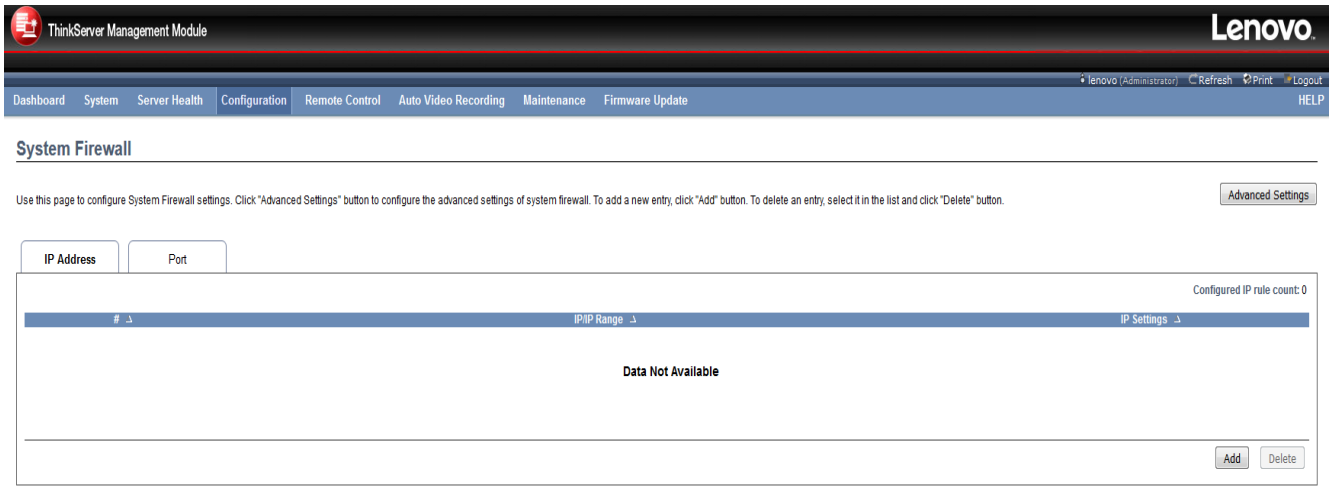


Figure 51. System Firewall Page

The fields of System Firewall - **Port** tab are explained below.

- **Advanced Settings:** Click this option to configure the Advanced Firewall Settings. Options are Block all and Flush all.
- **#**: The serial number.
- **Protocol:** This field specifies the affected protocol for the particular Port or Port Ranges.
- **Network Type**: This field specifies the affected network type for the particular Port or Port Ranges.
- **Port/Port Range:** This field is used to show the configured Port Address or Range of Ports.
- **Port Settings**: This column indicates the current setting of the listed Port or Range of Port rules (Allow or Block).
- **Add:** Click 'Add' to add a new entry to the firewall rules list.
- **Delete:** Select the configured slot to be deleted and click 'Delete'.

Add New Rule for Port:

This form is used to add a new Port or Range of Port rule settings.
To Click Add button is shown below.

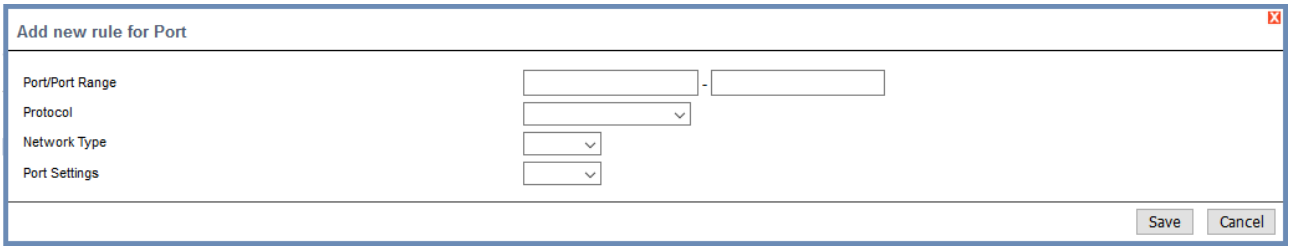


Figure 52. Add New Rule for Port Page

- **Port/Port Range:** This field is used to configured the Port or Range of Port Addresses.
  - Port value ranges from 1 to 65535.
- **Protocol:** This field is used to select the protocol. It may be TCP or UDP or Both.
- **Network Type:** This field is used to select the network type. It may be IPv4 or IPv6 or Both.
- **Port Settings:** Port Settings are used to determine the rule whether block or allow from the configured Port or Port Range.
- **Save:** Click 'Save' to save a configured entry.
- **Cancel:** Click 'Cancel' to cancel the modification to the existing settings.

Users

The displayed table shows any configured Users and available slots. You can modify or add new users from here. A maximum of 10 slots are available and include the default of admin. To view the page, you must have Operator privileges. To modify or add a user, You must have Administrator privileges.

NOTE: Free slots are denoted by "~" in all columns for the slot.

And open User Management page, click **Configuration > Users** from the menu bar. A sample screenshot of User Management Page is shown below.

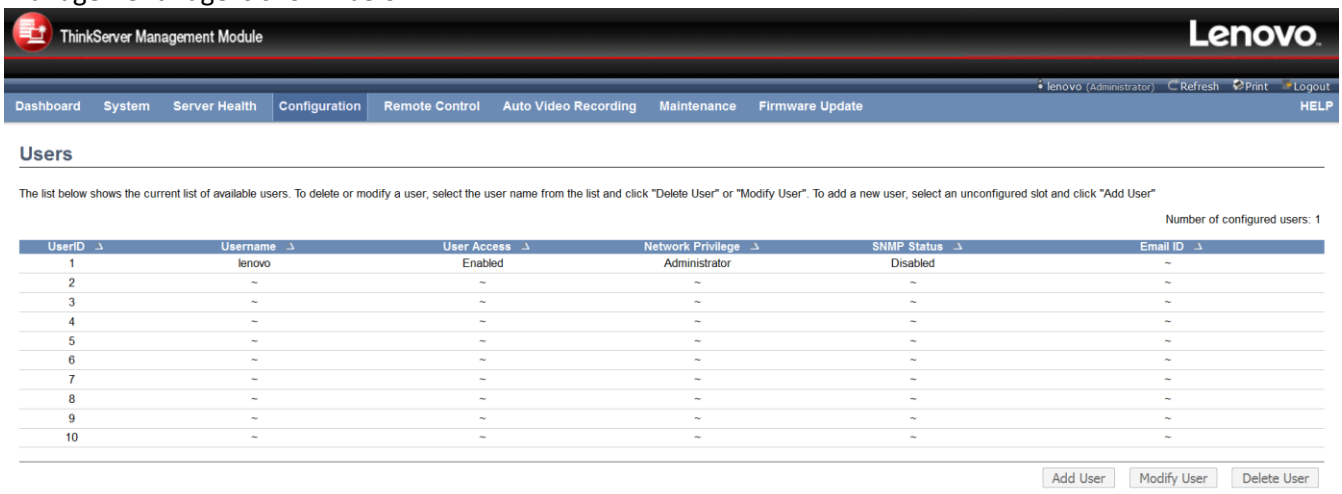


Figure 53. User Management Page

The fields of User Management Page are explained below.

- **UserID:** The number of user.
- **Username:** The name of user.
- **User Access:** Displays that enable/disable user access.
- **Network Privilege:** The level of network privilege to be assigned to this user. 5 levels are available: Administrator, Operator, User, OEM Proprietary and No Access.
- **SNMP Status:** Displays that enable/disable SNMP access for the user.
- **Email ID:** The email ID for the user.
- **Add User**: Select a free slot and click 'Add User' to add a new user to the device. Alternatively, double click on a free slot to add a user.
- **Modify User**: Select a configured slot and click 'Modify User' to modify the selected user. Alternatively, double click on the configured slot.
- **Delete User**: Select the user to be deleted and click 'Delete User'.

Add a new user:

Use this form to add a new user.

- To add a new user, select a free slot and click **Add User** or alternatively double click on the empty slot. This opens the Add User screen as shown in the screenshot below.

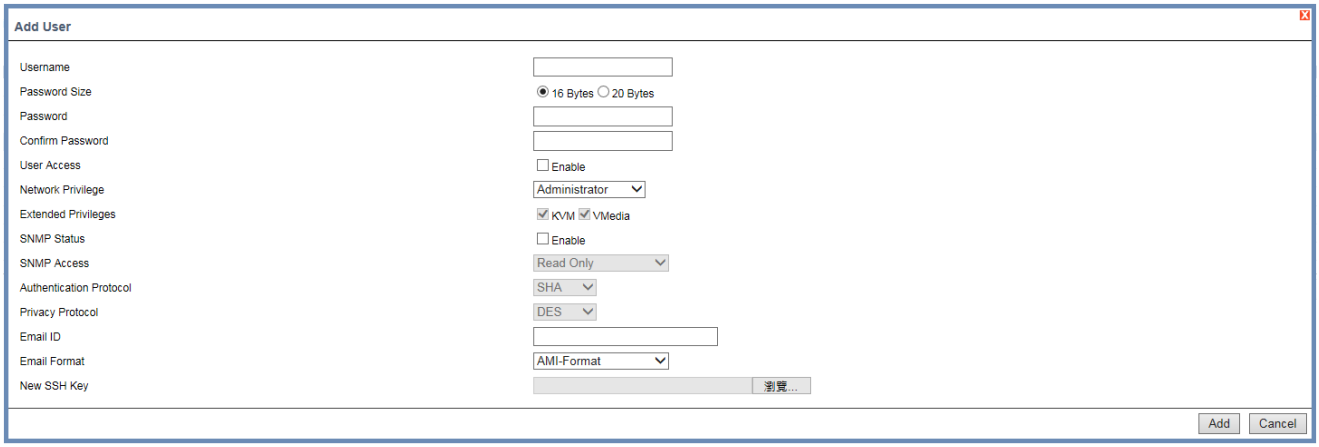


Figure 54. Add new User Page

- **Username:** Enter the name of the new user.
  - Username is a string of 1 to 16 alpha-numeric characters.
  - It must start with an alphabetical character.
  - It is case-sensitive.
  - Special characters '-'(hyphen), '_'(underscore), '@'(at sign), '.'(point) are allowed.
- **Password Size:** Either 16 Bytes or 20 Bytes password size can be chosen. Default option is 16 Bytes.
  If '16 Bytes' option is chosen, maximum password size is 16 characters. If '20 Bytes' option is chosen, maximum password size is 20 characters.
  NOTE: For 20 Bytes password, lan session will not be established.
- **Password, Confirm Password:** Enter and confirm the new password here.
  - Password must be at least 1 character long.
  - White space is not allowed.

  NOTE: This field will not allow more than 16/20 characters based on Password size field value.
- **User Access:** Enabling user access check box will intern assign the IPMI messaging privilege to user.
  NOTE: It is recommended that the IPMI messaging option should be enabled for the user to enable the **User Access** option, While creating User through IPMI.
- **Network Privilege:** Select the level of network privilege to be assigned to this user. 5 levels are available: Administrator, Operator, User, OEM Proprietary and No Access.
- **Extended Privileges:** This field is used to display the KVM and VMedia privilege for the user.
  NOTE: The KVM and VMedia privilege will enable (disable) automatic when Network Privilege is administrator(other).
- **SNMP Status:** Check the box to enable SNMP access for the user.
  NOTE1: Please enable SNMP in page 'SNMP'.
  NOTE2: Password field is mandatory and should at least be 8 characters long when SNMP Status is enabled.
  For 'anonymous' user, SNMP access is disabled as the username and password length is null.
- **SNMP Access:** Choose the SNMP Access level option for user. It can be either Read Only or Read Write.
- **Authentication Protocol:** Choose an Authentication Protocol for SNMP settings.
  NOTE: Password field is mandatory, if Authentication protocol is changed.
- **Privacy Protocol:** Choose the Encryption algorithm to use for SNMP settings.
- **Email ID:** Enter the email ID for the user. If user forgets the password, new password will be mailed to the configured email ID.
  NOTE: SMTP Server must be configured to send the email.
- **Email Format:** Specify the format for the email. This format will be used, while sending the email. Two

type of formats are available:

- AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content shows sensor information, ex: Sensor type and Description.
- FixedSubject-Format: This format displays the message according to user's setting. You must set the subject and message for email alert.

- **New SSH Key:** Use Browse button to navigate to the public SSH key file.
  - SSH key file should be of pub type.
- **Add:** Click 'Add' to save the new user and return to the Users list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to the Users list.

Modify an existing User

Use this form to modify the existing user's password and permission.

- Select an existing user from the list and click **Modify User** or alternatively double click on the configured slot. This opens the Modify User screen as shown in the screenshot below.

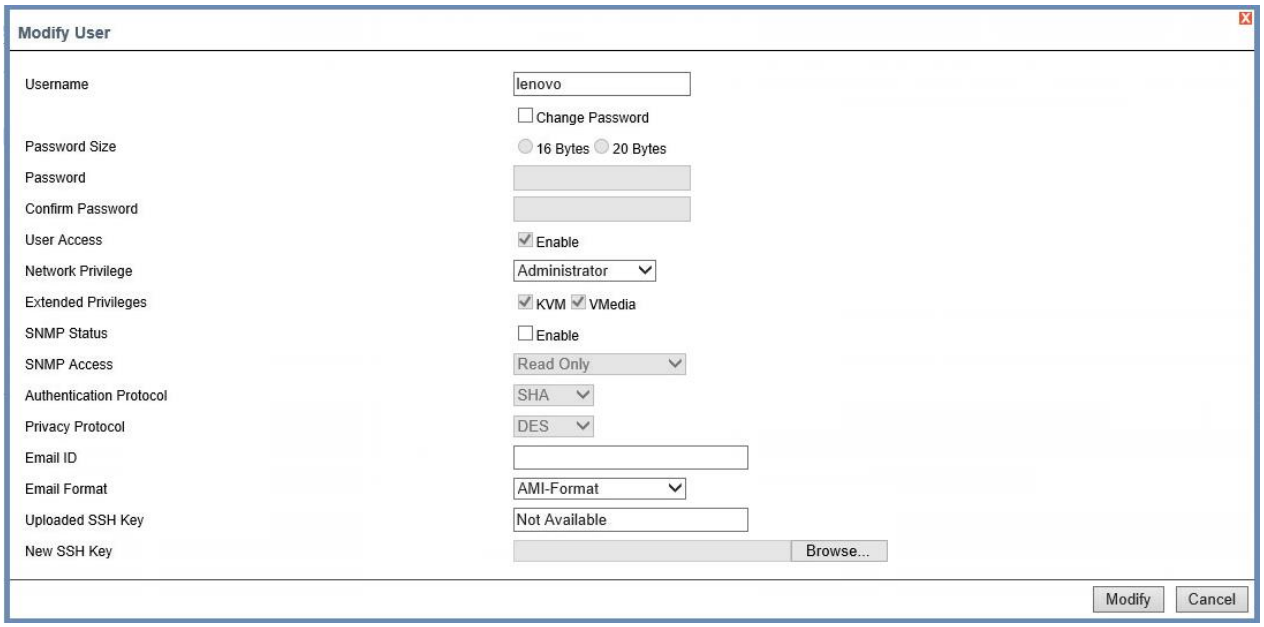


Figure 55. Modify User Page

- **Username:** Modify the existing user.
  - Username is a string of 1 to 16 alpha-numeric characters.
  - It must start with an alphabetical character.
  - It is case-sensitive.
  - Special characters '-'(hyphen), '_'(underscore), '@'(at sign), '.'(point) are allowed.
- **Password Size:** Either 16 Bytes or 20 Bytes password size can be chosen. Default option is 16 Bytes. If '16 Bytes' option is chosen, maximum password size is 16 characters. If '20 Bytes' option is chosen, maximum password size is 20 characters.
  NOTE: For 20 Bytes password, lan session will not be established.
- **Password, Confirm Password:** Enter and confirm the new password here.
  - Password must be at least 1 character long.
  - White space is not allowed.

  NOTE: This field will not allow more than 16/20 characters based on Password size field value.
- **User Access:** Enabling user access check box will intern assign the IPMI messaging privilege to user.

NOTE: It is recommended that the IPMI messaging option should be enabled for the user to enable the **User Access** option, While creating User through IPMI.

- **Network Privilege:** Select the level of network privilege to be assigned to this user. 5 levels are available: Administrator, Operator, User, OEM Proprietary and No Access.
- **Extended Privileges:** This field is used to display the KVM and VMedia privilege for the user.
  NOTE: The KVM and VMedia privilege will enable (disable) automatic when Network Privilege is administrator(other).
- **SNMP Status:** Check the box to enable SNMP access for the user.
  NOTE1: Please enable SNMP in page 'SNMP'.
  NOTE2: Password field is mandatory and should at least be 8 characters long when SNMP Status is enabled.
  For 'anonymous' user, SNMP access is disabled as the username and password length is null.
- **SNMP Access:** Choose the SNMP Access level option for user. It can be either Read Only or Read Write.
- **Authentication Protocol:** Choose an Authentication Protocol for SNMP settings.
  NOTE: Password field is mandatory, if Authentication protocol is changed.
- **Privacy Protocol:** Choose the Encryption algorithm to use for SNMP settings.
- **Email ID:** Enter the email ID for the user. If user forgets the password, new password will be mailed to the configured email ID.
  NOTE: SMTP Server must be configured to send the email.
- **Email Format:** Specify the format for the email. This format will be used, while sending the email. Two type of formats are available:
  - AMI-Format: The subject of this mail format is 'Alert from (your Hostname)'. The mail content shows sensor information, ex: Sensor type and Description.
  - FixedSubject-Format: This format displays the message according to user's setting. You must set the subject and message for email alert.
- **Uploaded SSH Key:** The uploaded SSH key information will be displayed (read only).
- **New SSH Key:** Use Browse button to navigate to the public SSH key file.
  - SSH key file should be of pub type.
- **Modify:** Click 'Modify' to accept the modification and return to Users list.
- **Cancel:** Click 'Cancel' to cancel the modification and return to the Users list.

Virtual Media

Use this page to configure Virtual Media device settings. If you change the configuration of the virtual media in this page, it will show the appropriate devices in the JViewer Vmedia Wizard. For example, if you select two floppy devices in Configure -> Virtual Media page, then in Jviewer -> VMedia Wizard, you can view two floppy devices available for redirection, open Virtual Media page, click **Configuration > Virtual Media** from the menu bar. A sample screenshot of Virtual Media Page is shown below.

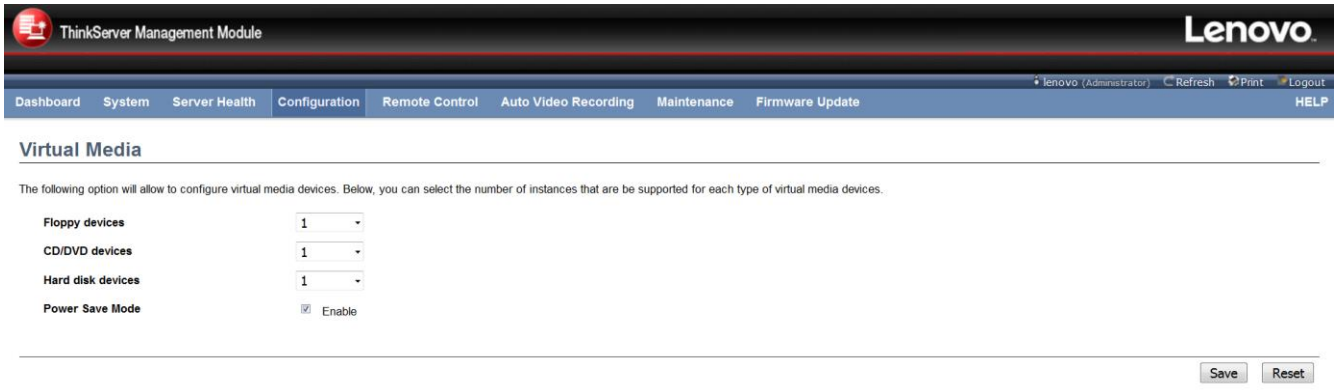


Figure 56. Virtual Media Page

The following fields are displayed in this page.

- **Floppy devices**: Select the number of floppy devices that are to be supported for Virtual Media redirection.
- **CD/DVD devices**: Select the number of CD/DVD devices that are to be supported for Virtual Media redirection.
- **Hard disk devices**: Select the number of Hard disk devices to be supported for Virtual Media redirection.
- **Power Save Mode:** Enable/Disable virtual USB devices visibility in the host.
- **Save:** Click 'Save' to save the configured settings.
- **Reset:** Click 'Reset' to reset the previously-saved values.

Cipher Suites

Use this page to configure the cipher suite.

To open Cipher Suites Settings page, click **Configuration > Cipher Suites** from the menu bar. A sample screenshot of Cipher Suite Page is shown below.

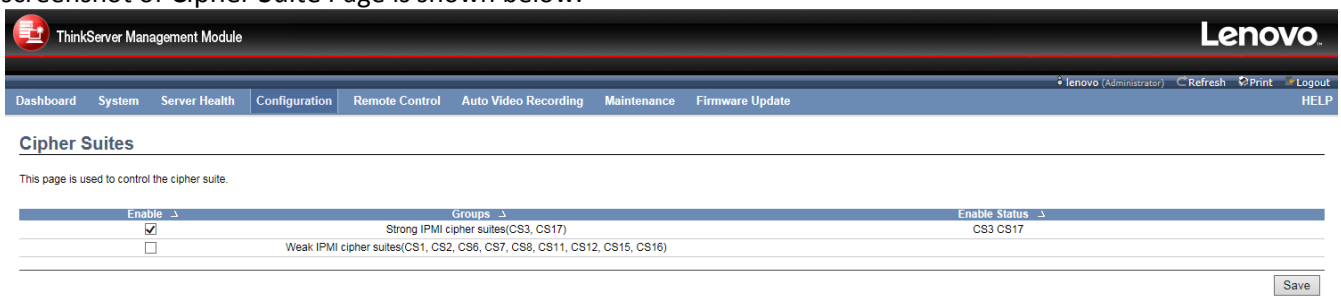


Figure 57. Cipher Suites Page

The fields of Cipher Suite Page are explained below.

- **Enable:** Check the option to enable Group.
- **Groups:** Displays the details of Group.
- **Enable Status:** Displays the status of Group.
- **Save:** Click on 'Save' to save the configuration.

Remote Control

The Remote Control consists of the following menu items.

- Console Redirection
- Server Power Control
- Java SOL

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

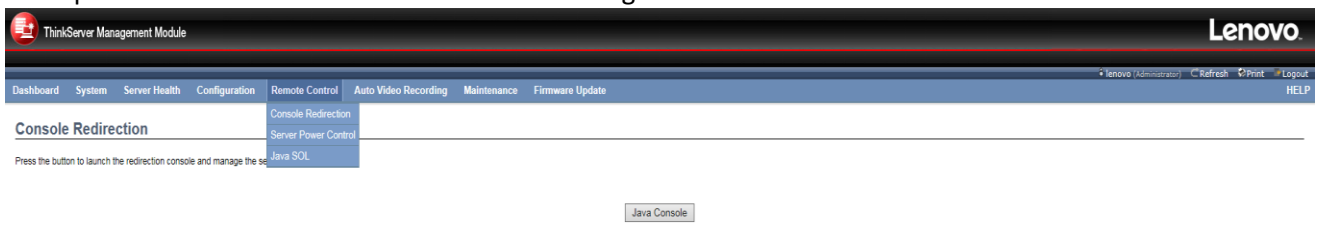


Figure 58. Remote Control Page

A detailed description of the menu items are given below.

Console Redirection

Launch the remote console redirection window from this page. To launch it, you must have Administrator privilege or KVM privilege.

NOTE: A compatible JRE must be installed in the system prior to the launch of JNLP file.

Open Console Redirection page, click **Remote Control > Console Redirection** from the menu bar. A sample screenshot of Console Redirection page is shown below.

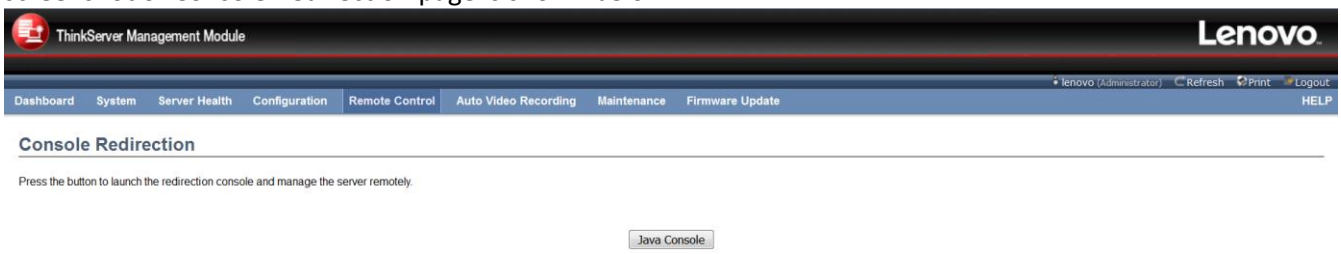


Figure 59. Console Redirection Page

- **Java Console:** Click 'Java Console' which will cause the jviewer.jnlp file to be downloaded. Once the file is downloaded and launched, a Java redirection window will be displayed.

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

In TMM GUI, 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 menu bar consists of the following menu items.

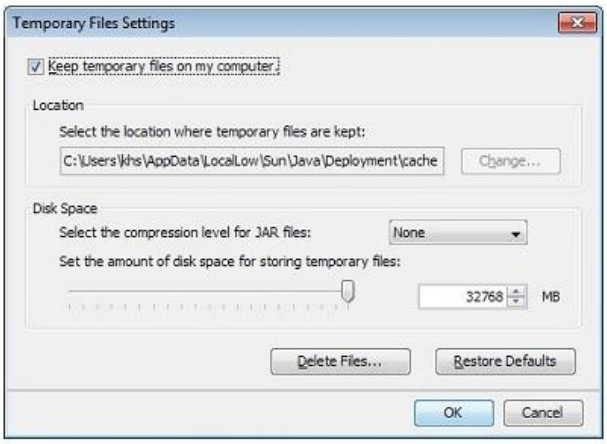
NOTE: Starting from version 8u131 of Java no longer trust algorithm of MD5-signed, the restriction will result Java Console invalid, so please use version 8u121 of Java or older.

Tips: Clear the Java cache.

Clearing the Java Plug-in cache forces the browser to load the latest versions of web pages and programs. Clear Java cache by deleting Temporary Files through the Java Control Panel. You can see more detail from the following link. *https://www.java.com/en/download/help/plugin_cache.xml*

This article applies to:

- **Platform(s):** Windows 8, Windows 7, Vista, Windows XP, Windows 10
- **Java version(s):** 7.0, 8.0
- **Delete Temporary Files through the Java Control Panel:**
  1. In the Java Control Panel, under the **General** tab, click **Settings** under the Temporary Internet Files section. The **Temporary Files Settings** dialog box appears.



2. Click **Delete Files** on the Temporary Files Settings dialog. The **Delete Files and Applications** dialog box appears.

3. Click **OK** on the **Delete Files and Applications** dialog. This deletes all the Downloaded Applications and Applets from the cache.
4. Click **OK** on the **Temporary Files Settings** dialog. If you want to delete a specific application and applet from the cache, click on View Application and View Applet options respectively.

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.
- **Capture Screen:** This option helps to take the screenshot of the host screen and save it in the client's system
- **Compression Mode :** This option helps to compress the Video data transfer to the specific mode. You can select one of the following:
  - YUV 420
  - YUV 444
  - YUV 444 + 2 colors VQ
  - YUV 444 + 4 colors VQ
- **DTC Quantization Table:** This option helps to choose the video quality. You can select one of the following:
  - 0 Best Quality
  - 1
  - 2
  - 3

- 4
- 5
- 6
- 7 Worst Quality

- **Turn ON Host Display:** If you disable this option, the server display will be blank but you can view the screen in Console Redirection. If you enable this option, the display will be back in the server screen.
- **Turn OFF Host Display/Host Video Output:** 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.

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.
- **Ctrl+Alt+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.
- **Hot Keys:** This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.
- **Full Keyboard Support:** Enable this option to provide full keyboard support. This option is used to trigger the Ctrl and Alt key directly to host from the physical keyboard.

Mouse

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

- **Mouse Mode:** This option handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right to configure this option.
  - **Absolute mouse mode**: The absolute position of the local mouse is sent to the server if this option is selected.
  - **Relative mouse mode**: The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.

- **Other mouse mode**: This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.

Options

- **Band width (Except Hornet)**: 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 the network bandwidth usage of the BMC automatically.
  - 256 Kbps
  - 512 Kbps
  - 1 Mbps
  - 10 Mbps
  - 100 Mbps
- **Keyboard/Mouse Encryption**: This option allows you to encrypt keyboard inputs and mouse movements sent between the connections.
- **Zoom**
  - **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%.
  - **Actual Size** - By default this option is selected.
  - **Fit to Client Resolution** - If the host screen resolution is greater than the client screen resolution, choose this option to fit the host screen to client screen. The host video will be scaled down and rendered in the KVM console. In this case, the host mouse cursor will appear smaller than the client mouse cursor. So the client and host mouse cursors might not be in perfect sync.
  - **Fit to Host Resolution** - If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution.
- **Send IPMI Command** - This option opens the IPMI Command dialog. Enter the raw IPMI command in Hexadecimal field as Hexadecimal value and click Send. The Response will be displayed as shown in the screenshot below.

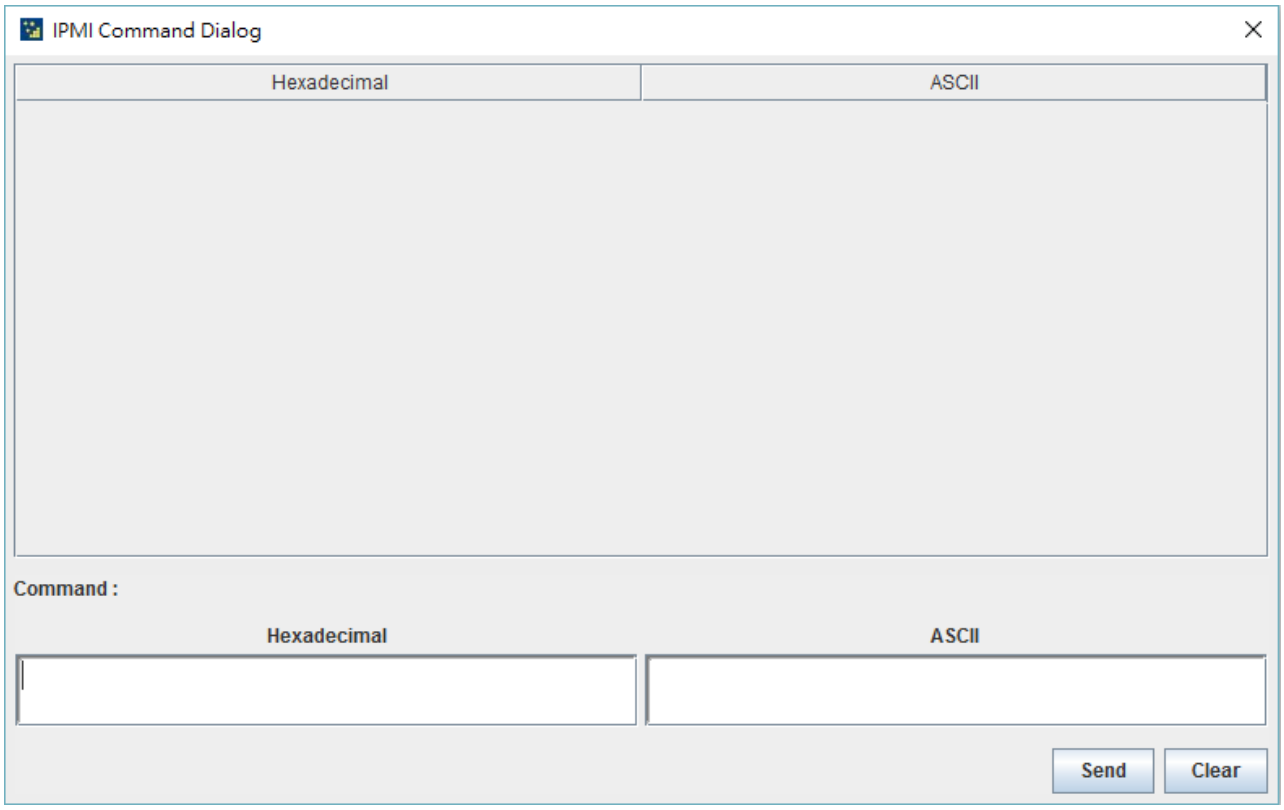


Figure 60. IPMI Command Dialog

- **GUI Languages** - Choose the desired GUI language.

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.

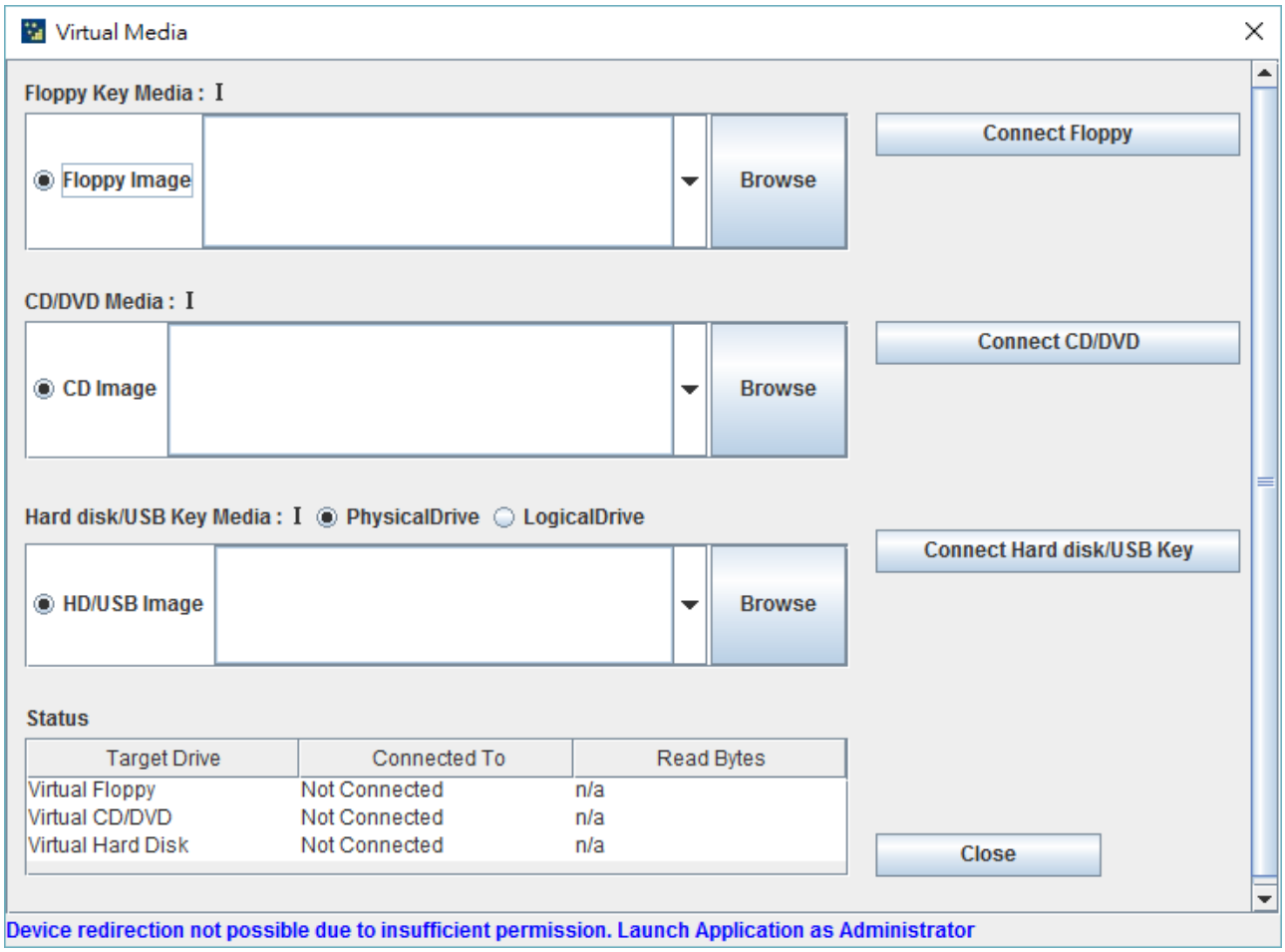


Figure 61. Virtual Media

- **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 disk/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. If the client and host keyboard layouts are same, then for all the supported physical keyboard layouts, you must select this option to avoid typo errors. If the host and client languages differ, user can choose the host language layout in the menu and thereby can directly use the physical keyboard.
- **Host Physical Keyboard**: This feature is fully compatible when host and client has the same keyboard language layout. If the client and host language layouts differ, some special characters will not be compatible.
  - **Host Platform**: This feature contains two options Windows and Linux. When working with Windows host, Windows option should be selected. Similarly when working with Linux host, Linux option should be selected. This option should be selected properly for the Physical keyboard layout cross mapping to work properly. By default, Windows will be selected.

  To list of List of Soft Physical Keyboard languages supported in TMM JViewer.
  - English –US

- English – UK
- French
- French (Belgium)
- German (Germany)
- German (Switzerland)
- Japanese
- Spanish
- Italian
- Danish
- Finnish
- Norwegian (Norway)
- Portuguese (Portugal)
- Swedish
- Dutch (Netherland)
- Dutch(Belgium)
- Turkish – F
- Turkish – Q

- **Soft Keyboard**: This option allows you to select the keyboard layout. It will show the dialog as similar to Windows On-screen keyboard. If the client and host languages are different, you can select the soft keyboard that corresponds to the host keyboard layout from the list shown in JViewer, and use it to avoid typo errors.
  To list of List of Soft Physical Keyboard languages supported in TMM JViewer.
  - English – US
  - English – UK
  - Spanish
  - French
  - German (Germany)
  - Italian
  - Danish
  - Finnish
  - German (Switzerland)
  - Norwegian (Norway)
  - Portuguese (Portugal)
  - Swedish
  - Hebrew
  - French (Belgium)
  - Dutch (Netherland)
  - Dutch(Belgium)
  - Russian (Russia)
  - Japanese (QWERTY)
  - Japanese (Hiragana)
  - Japanese (Katakana)
  - Turkish – F
  - Turkish – Q

Video Record

- **Start Record**: This option is to start recording the screen.
- **Stop Record**: This option is used to stop the recording.
- **Settings**: To set the settings for video recording,

1. Click **Video Record > Settings** to open the settings page as shown in the screenshot below.

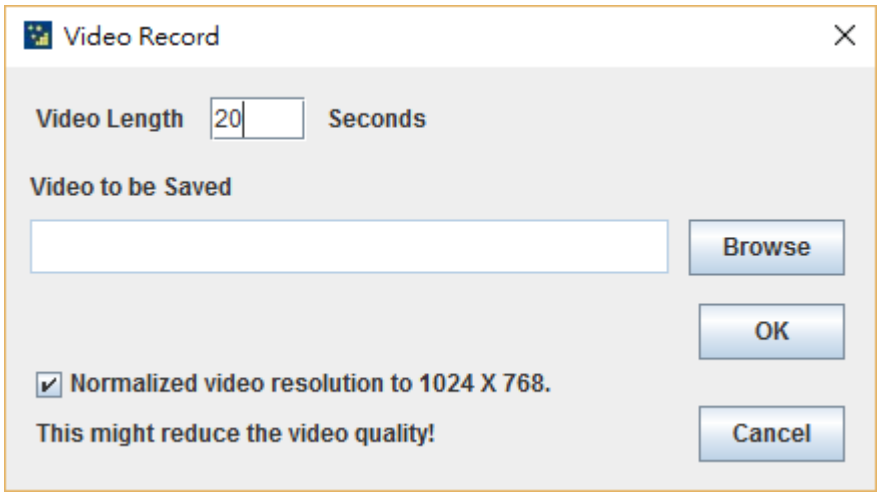


Figure 62. Video Record Settings Page

2. Enter the **Video Length** in seconds.
3. Browse and enter the location where you want the video to be saved.
4. Enable the option Normalized video resolution to 1024 X 768.
5. Click **OK** to save the entries and return to the Console Redirection screen.
6. Click **Cancel** if you don't wish to save the entries.
7. In the Console Redirection window, click **Video Record > Start Record**.
8. Record the process.
9. To stop the recording, click **Video Record > Stop Record**.

Power

The power option is to perform any power cycle operation. Click on the required option to perform the following operation.

- **Reset Server :** To reboot the system without powering off (warm boot).
- **Immediate Shutdown :** To immediately power off the server.
- **Orderly Shutdown :** To initiate operating system shutdown prior to the shutdown.
- **Power On Server :** To power on the server.
- **Power Cycle Server :** To first power off, and then reboot the system (cold boot).

Active Users

Click this option to displays the active users and their system IP address.

Help

Jviewer: Displays the copyright and version information.

Quick Buttons

The lower right of Console Redirection windows displays all the quick buttons. These quick buttons helps you to perform these functions by just clicking them.

Quick Buttons	Explanation
	This key is used to play the Console redirection after being paused.
	This key can be used for pausing Console Redirection.
	This button is used to view the Console Redirection in full screen mode. **Note**: *Set your client system resolution same to host system resolution so that you can view the server in full screen.*
	These three quick buttons will pop up a virtual media where you can configure the media.
	This quick button is used to show or hide the mouse cursor on the remote client system.
	This quick button is used to show or hide the soft keyboard.
	This quick button is used to record the video.
	This quick button displays the available hotkeys.
	Drag this to zoom in or out.
	Active Users
	This quick button is used to lock or unlock the local host display.
	This quick button will work like toggle button if icon is in green color server status is **power on** by clicking the button **immediate shutdown** action will be triggered in host If the icon is in red color server status is **power off** . Click the button to **power on** the host.

Server Power Control

This page helps you to view or perform any host power cycle operation. And open Power Control and Status page, click **Remote Control > Server Power Control** from the menu bar.

A sample screenshot of Power Control and Status page is shown below.

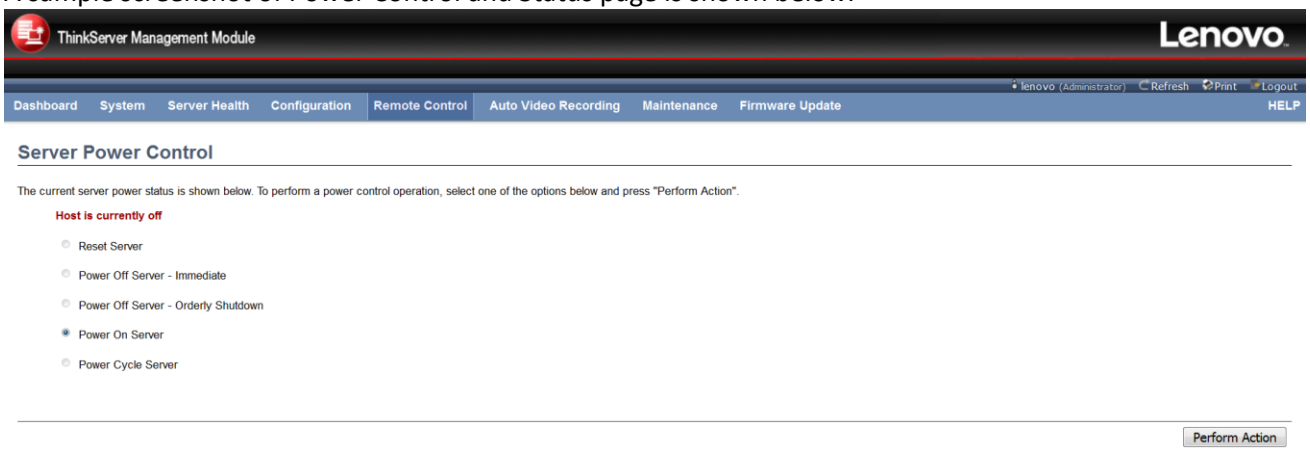


Figure 63. Power Control and Status Page

The various options of Power Control are given below.

- **Reset Server**: Select this option to reboot the system without powering off (warm boot).
- **Power Off Server – Immediate:** Select this option to immediately power off the server.
- **Power Off Server – Orderly Shutdown**: Select this option to initiate operating system shutdown prior to the shutdown.
- **Power On Server**: Select this option to power on the server.
- **Power Cycle Server**: Select this option to first power off, and then reboot the system (cold boot).
- **Perform Action:** Click 'Perform Action' to perform the selected option.

Java SOL

This page allows you to launch the Java SOL. The Java SOL is used to view the host screen using the SOL Redirection, open Java SOL page, click **Remote Control > Java SOL** from the menu bar. A sample screenshot of Java SOL page is shown below.

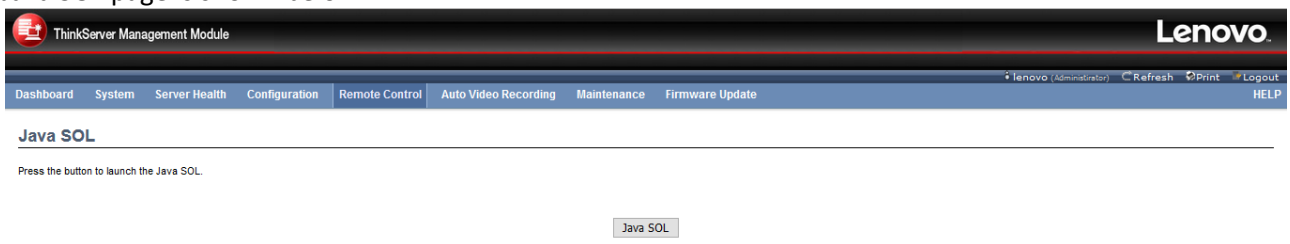


Figure 64. Java SOL Page

-

Launch the Java SOL, you must have Administrator privileges or KVM privilege.
NOTE: A compatible JRE must be installed in the system prior to the launch of JNLP file.

1. Click the Java SOL button to open the Java SOL window.

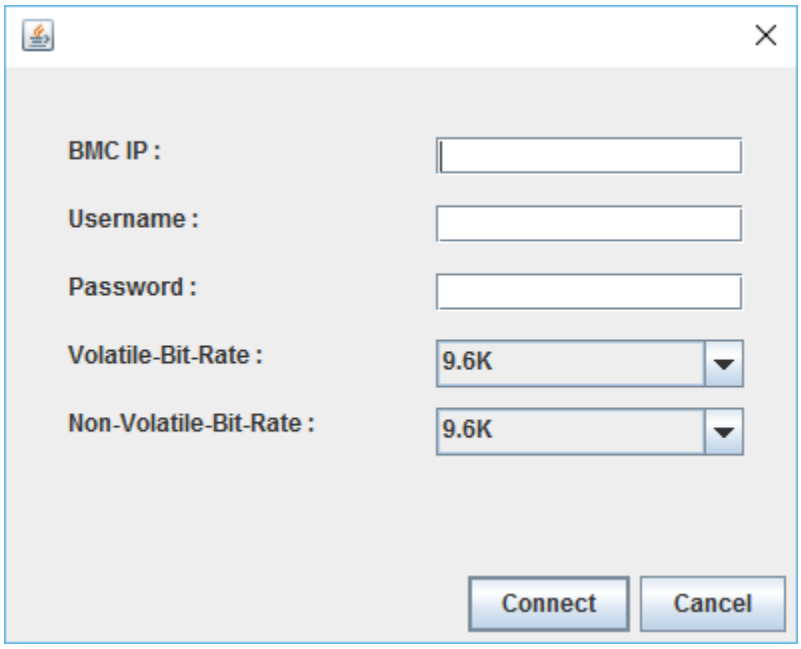


Figure 65. JAVA SOL Page

2. Enter the BMC IP address, User Name and Password in the respective fields.
3. Select the Volatile-Bit-Rate and Non-Volatile-Bit-Rate from the drop down lists.
4. Click **Connect** to open the SOL redirection.

NOTE:

- Before open the SOL, please enable SOL setting of BIOS Setup first.
- The Username/Password is the same as Web user.

Auto Video Recording

TMM can support triggers Video recording. A sample screenshot of the Auto Video Recording menu is given below including trigger configuration setting.

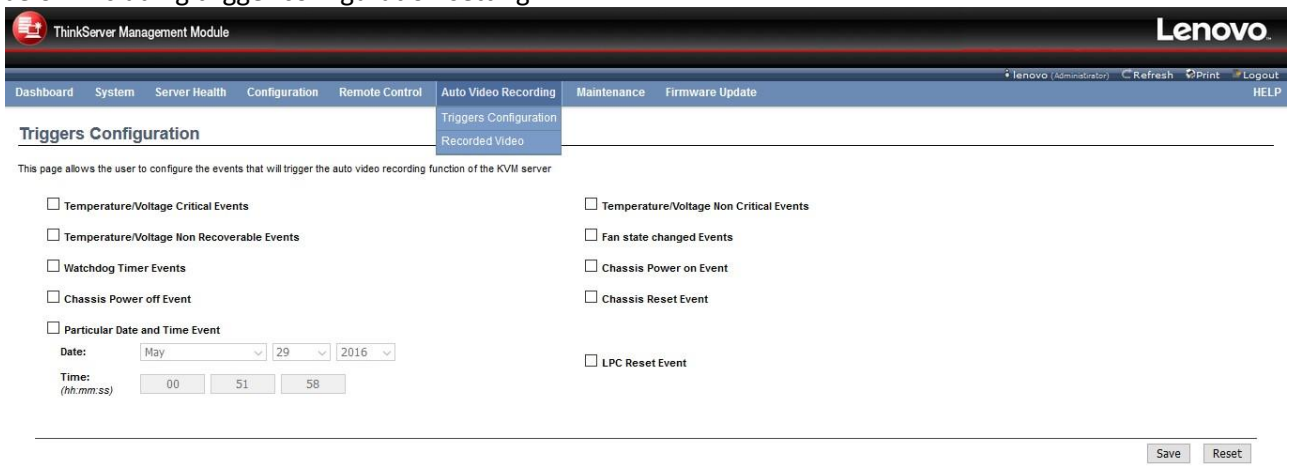


Figure 66. Auto Video Recording Menu

Triggers Configuration

Configure which event on the page will trigger the auto-video recording option to start.

To open Triggers Configuration page, click **Auto Video Recording > Triggers Configuration** from the menu bar. A

sample screenshot of Triggers Configuration page is shown below.

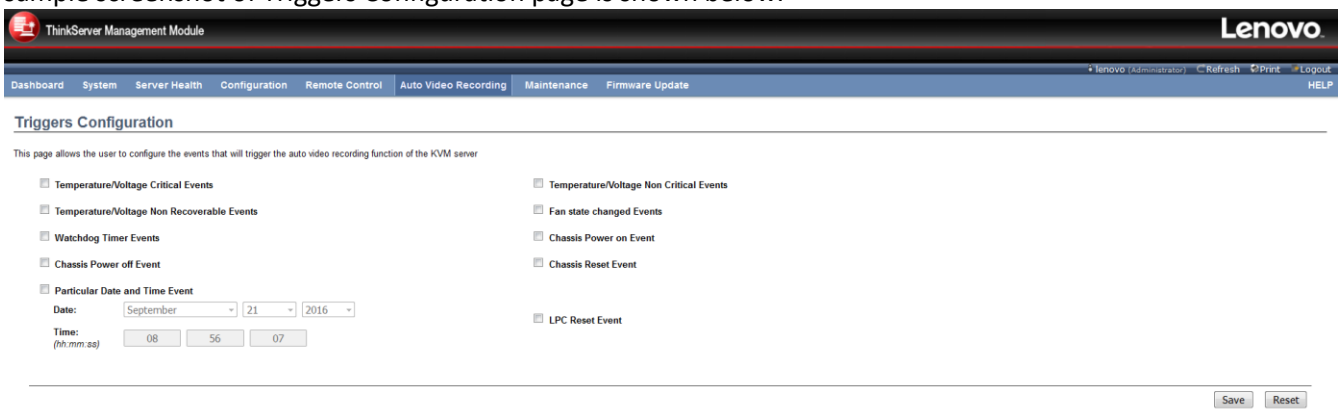


Figure 67. Triggers Configuration Page

- **Event List**: You can check/uncheck a box to add/remove the trigger for your system.
  - **Temperature/Voltage Critical Events:** trigger the recording by the critical events for Temperature/Voltage sensors.
  - **Temperature/Voltage Non Recoverable Events:** trigger the recording by the Non Recoverable events for Temperature/Voltage sensors.
  - **Temperature/Voltage Non Critical Events:** trigger the recording by the Non Critical events for Temperature/Voltage sensors.
  - **Fan state changed Events:** trigger the recording by All fan sensor events.
  - **Chassis Power off Event:** trigger the recording by system power off events (DC OFF).
  - **Chassis Power on Event:** trigger the recording by system power on events (DC ON).
  - **Chassis Reset Event:** trigger the recording by system reset events.
  - **LPC Reset Event:** trigger the recording by Host LPCRESET event.
  - **Watchdog Timer Events:** trigger the recording when watchdog timer be triggered.
  - **Particular Date and Time Event:** trigger the recording by specific date and time.

- **Save**: Click 'Save' to save any changes made.
  NOTE: KVM service should be enabled (under 'Configuration -> Services') to perform auto-video recording. The date and time should be in advance to the system date and time.
- **Reset**: Click 'Reset' to reset the modified changes.

Recorded Video

This page displays the list of available recorded video files. The various fields of Recorded Video are given below:

- **#:** The serial number.
- **File Name:** The video filename.
- **Video Type:** The Type of the video either Pre-Event or Post-Event.
- **File Information:** Day, date and time of video upload.

NOTE: If remote video support is enabled, 3 pre-event videos and maximum configured dump value of post-event videos can be recorded. If remote video support is disabled, 1 pre-event video and 2 post-event videos can be recorded.

In case of mount failure in remote share, video files will be stored in local path of BMC.

To open Video Recording page, click **Auto Video Recording > Recorded Video** from the menu bar.A sample screenshot of Recorded Video page is shown below.

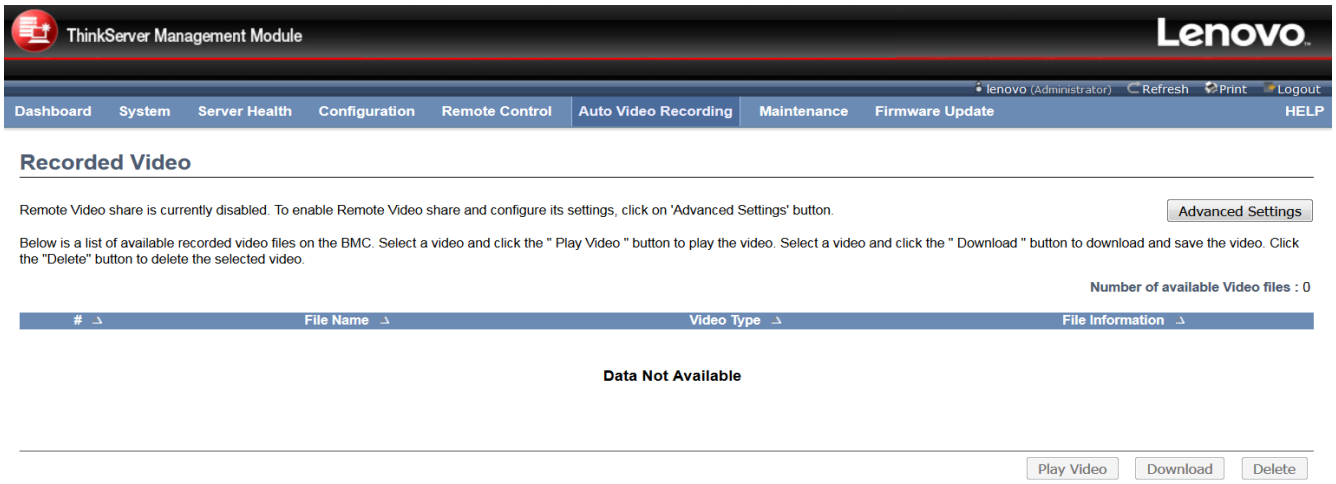


Figure 68. Record Video

- **Advanced Settings:** Click this option to configure the Remote Video Settings. Options are Enable/Disable Remote Video Support, Server Address, Source Path, Share Type, Username, Password and Domain Name.
- **Play Video:** Select a video and click the Play Video button to play the video file in Java Application.
- **Download:** Select a video and click the Download button to download and save the video file in the client machine. The video will be downloaded in (.avi) format.
- **Delete:** Click the Delete button to delete the selected video file.

Procedure for Auto Recorded Video:

This page is used to configure the Remote Video Advanced Settings. All the trusted domains are supported as well.

NOTE: Configured settings will be reflected during next video recording.

To open Advanced Remote Video Settings page, Click **Advanced Settings**.

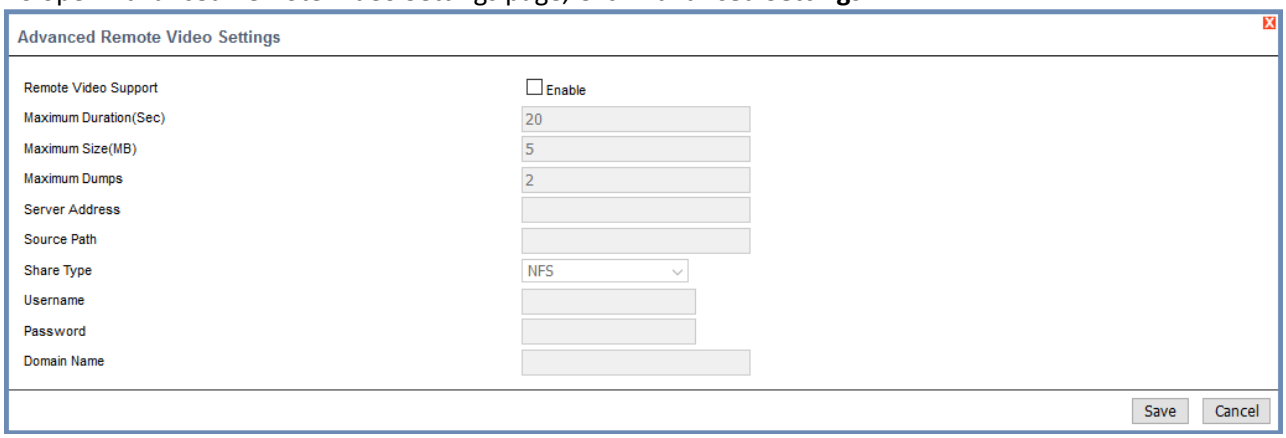


Figure 69. Advanced Remote Video Settings

- **Remote Video Support**: To enable or disable Remote Video support, check or uncheck the 'Enable' checkbox respectively.
  NOTE: By default, video files will be stored in local path of BMC. If remote video support is enabled, then the video files will be stored only in remote path, not within BMC.
- **Maximum Duration (Sec):** Maximum Duration should be in range from 1 to 3600 seconds.
- **Maximum Size (MB):** Maximum Size should be in range from 1 to 500 MB.

- **Maximum Dumps:** Maximum Dumps should be in range from 1 to 100.
- **Server Address:** Server address of the server where remote videos are to be stored. Server address will support the following:
  - IP Address (Both IPv4 and IPv6 format).
  - FQDN (Fully qualified domain name) format.
- **Source Path:** Source path to directory where the remote videos will be stored.
  - Special characters '<'(less than), '>'(greater than), ':'(colon), '*'(asterisk), '|'(vertical bar), '.'(dot), '?'(question mark) are not allowed.
- **Share Type:** Share Type of the remote video server either NFS or Samba (CIFS).
- **Username, Password and Domain Name:** If share Type is Samba(CIFS), enter the user credentials for server authentication.
  NOTE: Domain Name field is optional.
- **Save**: Click 'Save' to save any changes made.
- **Cancel**: Click 'Cancel' to cancel the modified changes.

Maintenance Group

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

- Preserve Configuration
- Restore Configuration

Preserve Configuration

This page allows you to select the specific configuration items to be preserved in the cases of "Restore Configuration", and "Firmware Update without Preserve Configuration option". Open Preserve Configuration page, click **Maintenance Group > Preserve Configuration** from the menu bar. A sample screenshot of Preserve Configuration page is shown below.

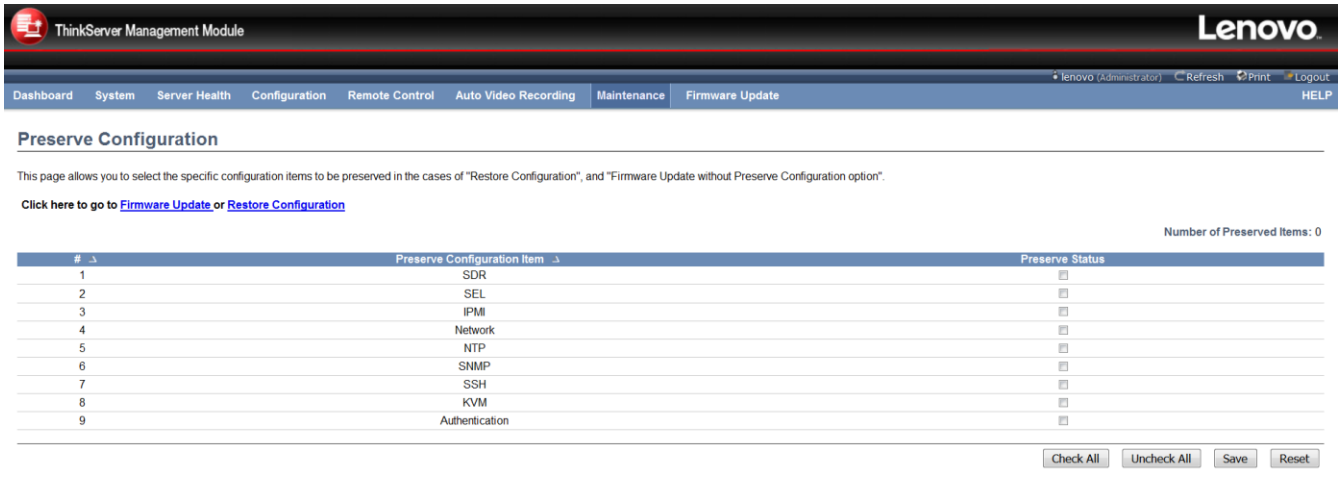


Figure 70. Preserve Configuration

Check the configuration that needs to be preserved, while the Restore Configuration is done.

- **#:** The serial number.
- **Preserve Configuration Item:** The configuration item that you can preserve/overwrite.
- **Preserve Status:** You can either check/uncheck a check box to preserve/overwrite the configuration for your system in firmware update.
- **Check All**: Click this button to check all the configuration list.
- **Uncheck All**: Click this button to uncheck all the configuration list.

- **Save**: Click 'Save' to save any changes made.
  NOTE: This configuration is used by Restore Configuration process. Please also enable option "IPMI" when you select "SEL" or "NTP" as dependency configuration.
- **Reset**: Click 'Reset' to reset the modified changes.

Files Preserved

- **SDR:** This file contains the sensor data record information that is used in IPMI.
- **SEL**: This file contains the system event logs that are being logged by the IPMI.
- **IPMI:** This file contains the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.
- **Network:** This file contains the Network configuration such hostname, interface, PHY config, NCSI config etc.
- **NTP:** This file contains the NTP configuration.
- **SNMP:** This file contains the SNMP configuration.
- **SSH:** This file contains the SSH configuration.
- **KVM:** This file contains the KVM configuration.
- **Authentication:** This file contains the Authentication configuration.

Restore Configuration

This page helps to restore the configuration of the device. Please note once you enter restore configuration, 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.

Open Restore Factory Defaults page, click **Maintenance > Restore Configuration** from the menu bar. A sample screenshot of Restore Factory Defaults Page is shown below.

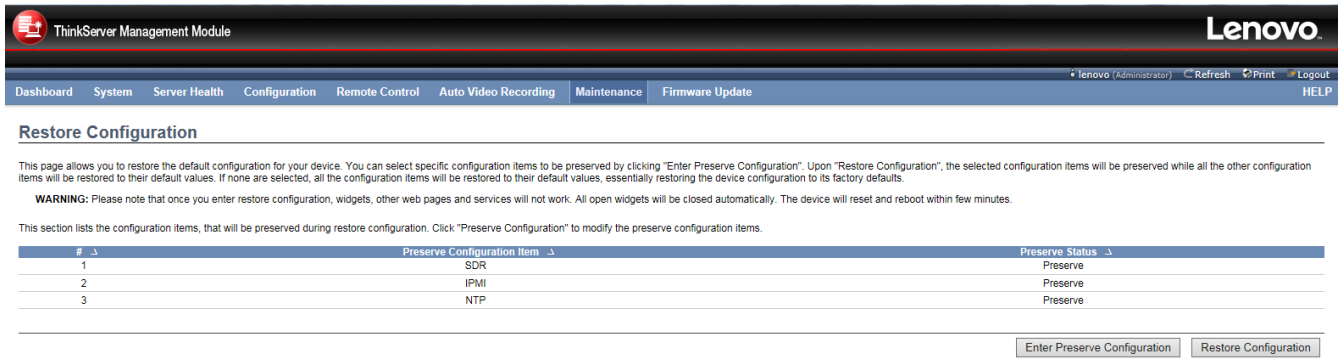


Figure 71. Restore Configuration

- **#:** The serial number.
- **Preserve Configuration Item:** Display the item that will be preserved.
- **Preserve Status:** Display the preserve status of the item.
- **Enter Preserve Configuration:** Click this to redirect to preserve configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
- **Restore Configuration:** Click this to restore the firmware with default configuration.

Firmware Update

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

- Firmware Update
- BIOS Update

- Protocol Configuration

A detailed description is given below,

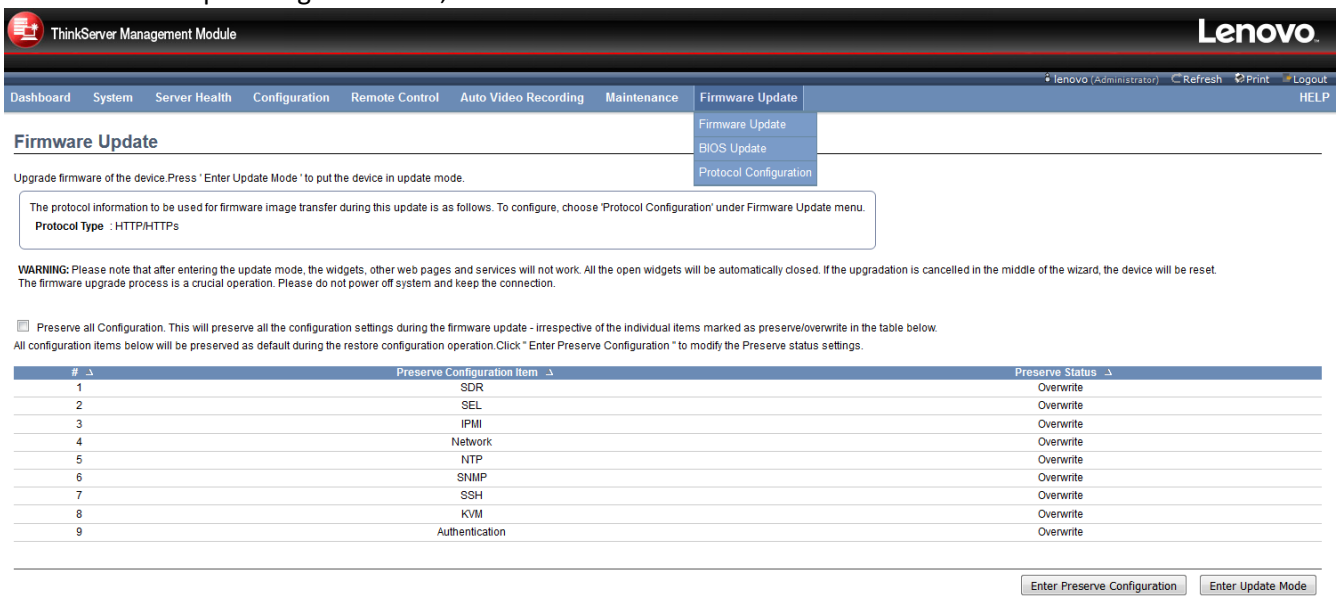


Figure 72. Firmware Update Menu

Firmware Update

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

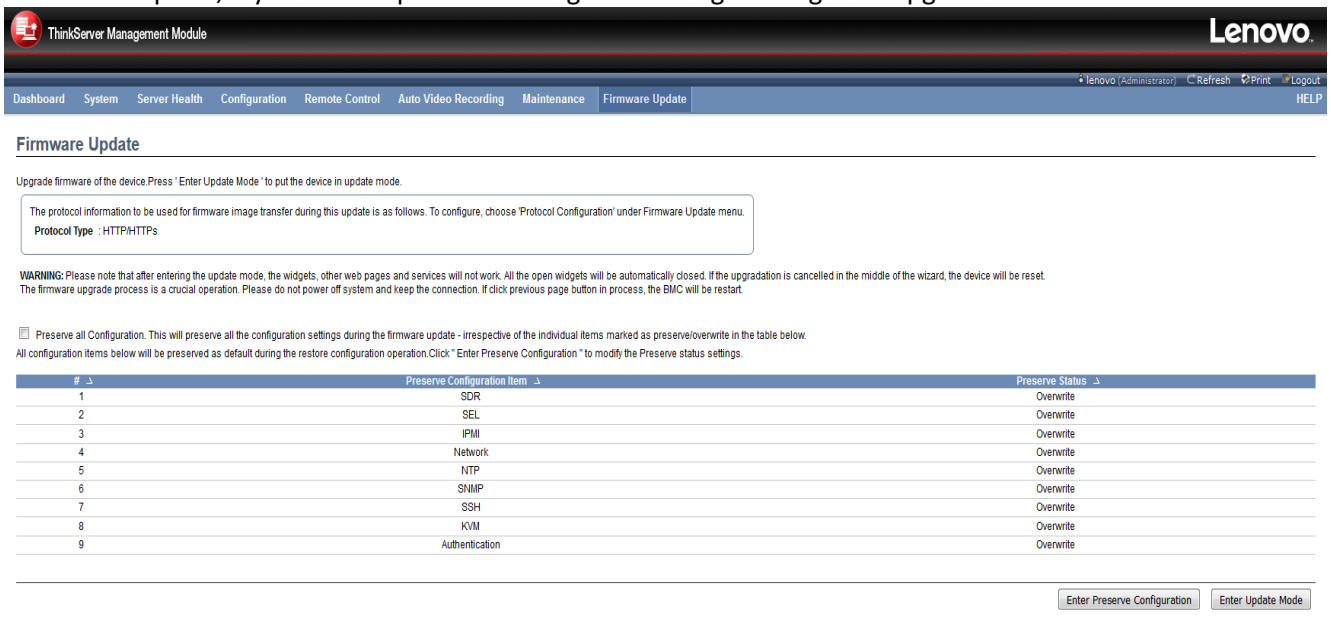


Figure 73. Firmware Update

The various are listed below.

- **#:** The serial number.
- **Preserve Configuration Item:** Display the item that will be preserved.

- **Preserve Status:** Display the preserve status of the item.
- **Enter Preserve Configuration:** Click this button to be redirected to the Preserve configuration page, where the configurations are preserved from being overwritten by the default configurations.
- **Enter Update Mode:** Click 'Enter Update Mode' to upgrade the current device firmware.

Procedure

1. Click **Enter Update Mode** to upgrade the current device firmware., and following the step is given below,
2. Closing all active client requests.

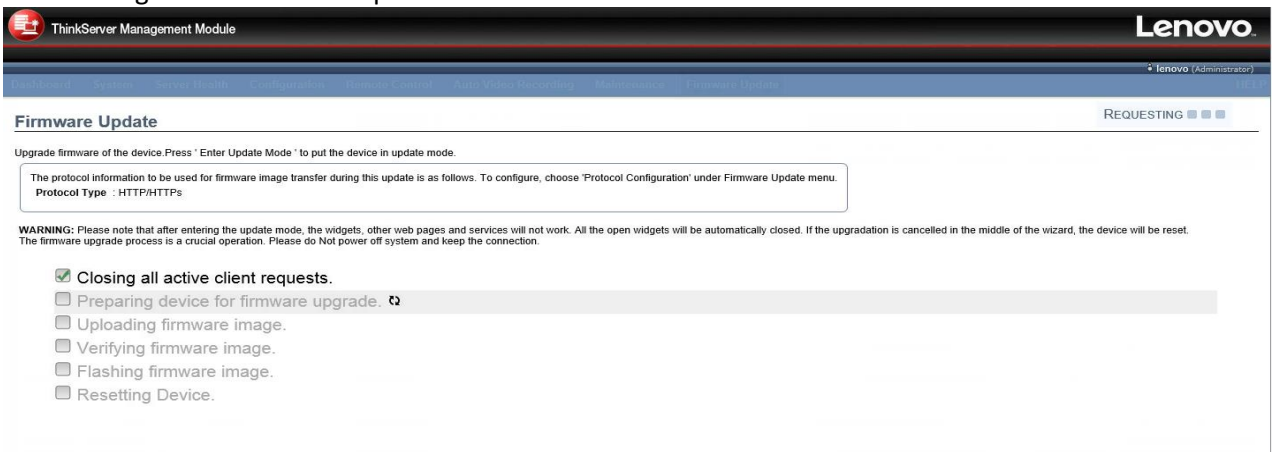
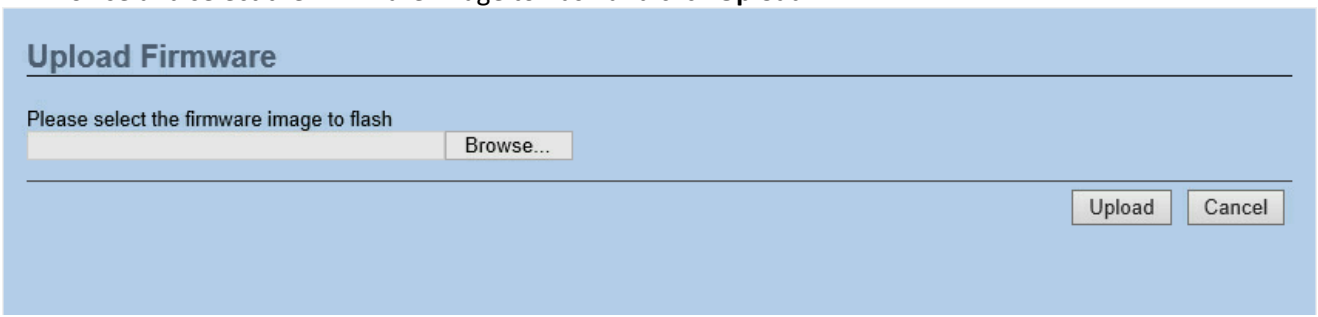


Figure 74. Firmware Update process

3. Preparing Device for Firmware Upgrade.
4. Uploading Firmware Image.
5. Browse and select the Firmware image to flash and click **Upload**.



6. Verifying Firmware Image.
7. Flashing Firmware Image.
8. Resetting Device.

BIOS Update

This wizard takes you through the process of BIOS upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled.

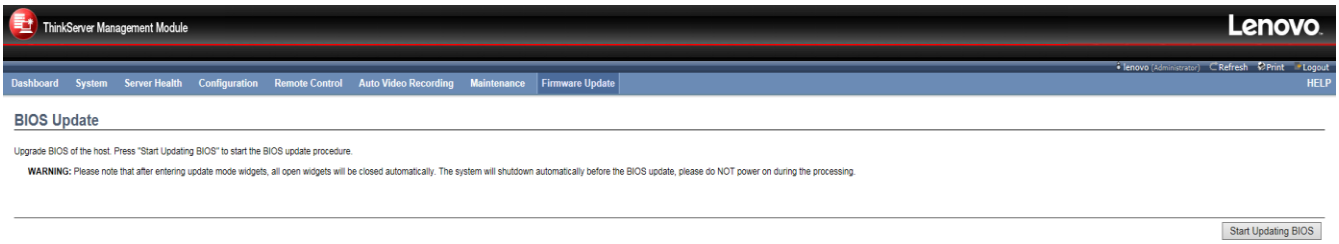


Figure 75. BIOS Update

- **Start Updating BIOS:** Click 'Start Updating BIOS' to upgrade the current device BIOS.

1. Click start Updating BIOS, a sample screenshot page is shown below

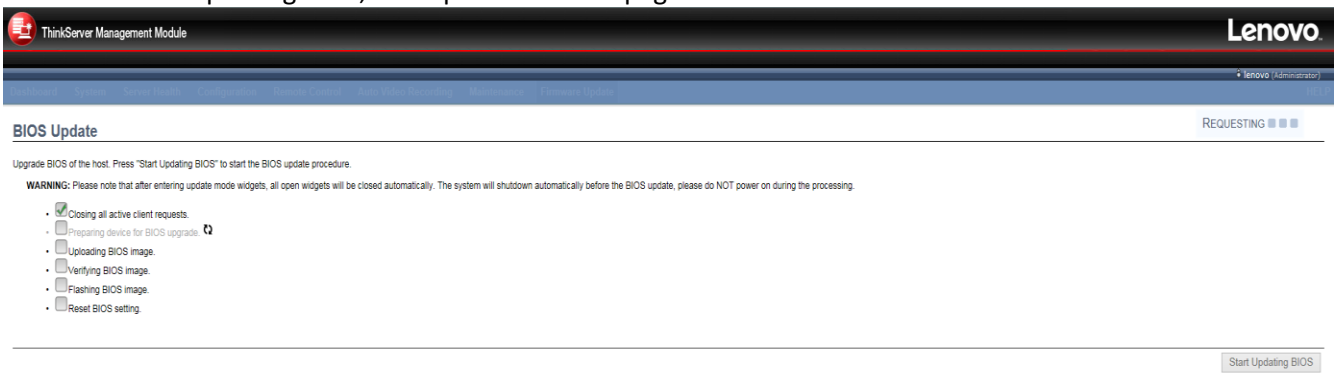


Figure 76. Start Updating BIOS Page

2. Closing all active client requests.
3. Preparing Device for Firmware Upgrade.
4. Uploading Firmware Image.
5. Browse and select the Firmware image to flash and click **Upload**.

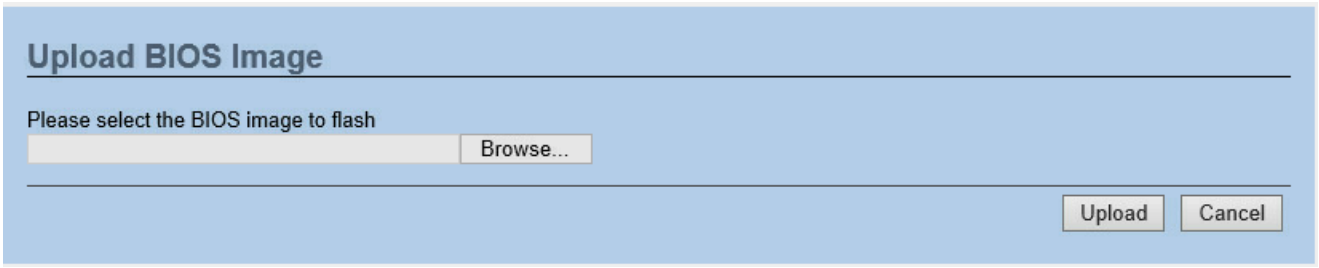


Figure 77. Upload BIOS Image Page

6. Verifying Firmware Image
7. Flashing Firmware Image
8. Resetting Device

Protocol Configuration

This page is used to configure the firmware image protocol information.

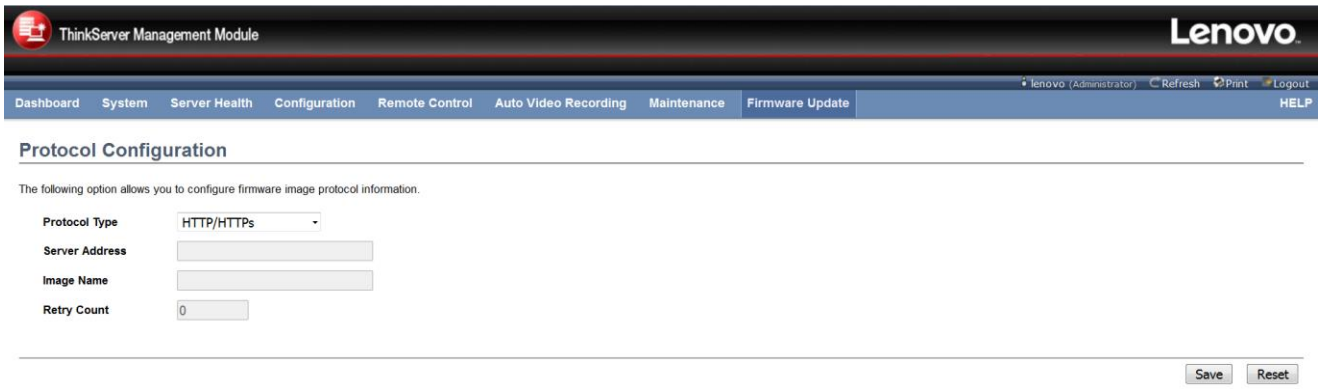


Figure 78. Image Transfer Protocol

- **Protocol Type:** Protocol to be used to transfer the firmware image into the BMC.
- **Server Address:** Address of the server where the firmware image is stored. It supports both IPv4 and IPv6.
  - 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 groups of 4 Hexadecimal digits separated by colon as in "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx".
  - Hexadecimal digits are expressed as lower-case letters.
- **Image Name:** Image filename on TFTP server.
- **Retry Count:** Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.
- **Save:** Click 'Save' to save the configured settings.
- **Reset:** Click 'Reset' to reset the modified changes.

---

1. Note that the member attribute of Group should be “member”.

Chapter 6. User Privilege

This topic describes the access privilege of the TMM Web UI.

		Access	Operate
Dashboard		A,O,U,OEM	A
System	Inventory	A,O,U,OEM	A,O,U,OEM
	FRU Information	A,O,U,OEM	A,O,U,OEM
Server Health	Sensor Readings	A,O,U,OEM	A,O,OEM
	Event Log	A,O,U,OEM	A,OEM
	BSOD Screen	A,OEM	A,OEM
Configuration	Active Directory	A,O,U,OEM	A,OEM
	DNS	A,O,OEM	A,OEM
	Event Log	A,O,U,OEM	A,OEM
	Images Redirection	A,O,U,OEM	A,OEM
	LDAP/E-Directory	A,O,U,OEM	A,OEM
	Mouse Mode	A,O,U,OEM	A,OEM
	Network	A,O,OEM	A,OEM
	NTP	A,O,U,OEM	A,OEM
	PAM Order	A,O,U,OEM	A,OEM
	PEF	A,O,OEM	A,OEM
	RADIUS	A,O,U,OEM	A,OEM
	Remote Session	A,O,U,OEM	A,OEM
	Services	A,O,U,OEM	A,OEM
	Interfaces	A,O,OEM	A,OEM
	SMTP	A,O,OEM	A,OEM
	SNMP	A,O,U,OEM	A,OEM
	SSL	A,O,U,OEM	A,OEM
	System Firewall	A,O,OEM	A,OEM
	Users	A,O,OEM	A,OEM
	Virtual Media	A,O,U,OEM	A,OEM
	Cipher Suites	A,O,OEM	A,OEM
Remote Control	Console Redirection	A,O,U,OEM	A
	Server Power Control	A,O,U,OEM	A,OEM
	Java SOL	A,O,U,OEM	A
Auto Video Recording	Triggers Configuration	A,O,OEM	A,OEM
	Recorded Video	A,O,U,OEM	A,OEM
Maintenance	Preserve Configuration	A,O,U,OEM	A,OEM
	Restore Configuration	A,OEM	A,OEM
Firmware Update	Firmware Update	A,OEM	A,OEM
	BIOS Update	A,OEM	A,OEM
	Protocol Configuration	A,OEM	A,OEM

A: Administrator
O: Operator
U: User
OEM: OEM Proprietary
N: No Access

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area. Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

Lenovo (United States), Inc. 1009
Think Place - Building One Morrisville, NC 27560 U.S.A.
Attention: Lenovo Director of Licensing

LENOVO PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT,MERCHANTABILITY OR FITNESS
FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. Lenovo may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

The products described in this document are not intended for use in implantation or other life support applications where malfunction may result in injury or death to persons. The information contained in this document does not affect or change Lenovo product specifications or warranties. Nothing in this document shall operate as an express or implied license or indemnity under the intellectual property rights of Lenovo or third parties. All information contained in this document was obtained in specific environments and is presented as an illustration. The result obtained in other operating environments may vary.

Lenovo may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any references in this publication to non-Lenovo Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this Lenovo product, and use of those Web sites is at your own risk.

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems.

Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

Lenovo, the Lenovo logo, and ThinkServer are trademarks of Lenovo in the United States, other countries, or both.
Windows is a trademark of the Microsoft group of companies.

Other company, product, or service names may be trademarks or service marks of others.