Lenovo.

ThinkServer Management Module User Guide



Note: Before using the information and the product it supports, be sure to read and understand "<u>Appendix A Notices</u>".

First Edition (November 2017)

© Copyright Lenovo 2017.

LIMITED AND RESTRICTED RIGHTS NOTICE: If data or software is delivered pursuant a General Services Administration "GSA" contract, use, reproduction, or disclosure is subject to restrictions set forth in Contract No. GS-35F-05925.

Date	Version	Description
August-15-2016	v0.1	Preliminary draft
August-30-2016	v0.2	Add List of Figures and List of Tables Add System and Audit Log feature in "The Server Health Group displays". Change all IMM to TMM. Modify Chapter 5.
September-23-2016	v0.3	Modify Chapter 5.
October-04-2016	v0.4	Modify Chapter 5.
October-14-2016	v0.5	Modify Chapter 5.
October-20-2016	<i>v0.6</i>	Modify Chapter 5.
October-27-2016	v0.7	Modify Chapter 5.
Nomember-2-2016	v0.8	Modify Chapter 5.
Nomember-10-2016	v0.9	Modify Chapter 5.
Nomember-17-2016	v1.0	Modify Chapter 5.
Nomember-24-2016	v1.1	Add a note in Chapter 3. Modify Chapter 5.
December-9-2016	v1.2	Modify Chapter 5.
December-16-2016	v1.3	Modify Chapter 5.
December-22-2016	v1.4	Modify Chapter 5.
December-30-2016	v1.5	Modify Chapter 5 (FRU Information).
January-06-2017	v1.6	Modify Chapter 5 (Interfaces, NTP, PAM Order).

January-13-2017	v1.7	Modify Chapter 5 (System Firewall, Remote Session, Services, SNMP, SSL, Users).
January-20-2017	v1.8	Modify Chapter 5 (Dashboard, PAM Order, PEF, SSL, Users, Java SOL, Recorded Video, Restore Configuration, Firmware Update, BIOS Update).
February-17-2017	v1.9	Modify Chapter 5 (Dashboard).
March-10-2017	v2.0	Modify a note in Chapter 3.
March-17-2017	v2.1	Add a note in Chapter 3.
May-05-2017	v2.2	Add a note in Chapter 5 (Console Redirection). Modify Chapter 5 (Users).
June-19-2017	v2.3	Remove a note in Chapter 5 (Console Redirection). Remove a note in Chapter 5 (SSL).
Nomember-13-2017	v2.4	Update the First Edition date.

Contents

Chapter 1. Introduction	10
Terminology	10
Safety information	11
Chapter 2. Overview of the Lenovo TMM	12
Features of the TMM	12
Chapter 3. Configuring of the TMM	13
System requirements	13
Chapter 4. TMM Quick Start	14
Connecting to the TMM	14
Logging on	14
Navigation	14
Refresh	15
Print	15
Logout	15
Help	15
Chapter 5. TMM Web Console Options	16
Log in and access control	16
Forgot password	16
Required Browser Settings	17
Dashboard	17
Device Information	18
Network Information	18
Power Supply Information	18
Location LED Status	19
Remote Control	19
Remote Control Screenshot	19
Sensor Monitoring	19
Event Logs	19
Menu Bar	19
System	20
Inventory	20

FRU Information	21
Location	23
Server Health	23
Sensor Reading	23
Event Log	26
System and Audit Log	27
BSOD Screen	28
Configuration Group	29
Active Directory	30
DNS	33
Event Log	34
Images Redirection	35
LDAP/E-Directory	37
Mouse Mode	38
Network	39
NTP	41
PAM Order	42
PEF	42
RADIUS	52
Remote Session	54
Services	54
Interfaces	57
SMTP	58
SNMP	59
SSL	60
System Firewall	63
Users	65
Virtual Media	69
Cipher Suites	70
Remote Control	70
Console Redirection	71
Server Power Control	79
Java SOL	80

Auto Video Recording8	1
Triggers Configuration8	1
Recorded Video8	2
Maintenance Group8	4
Preserve Configuration8	4
Restore Configuration8	5
Firmware Update8	5
Firmware Update8	6
BIOS Update8	7
Protocol Configuration8	8
Chapter 6. User Privilege9	0
Appendix A. Notices9	1
Trademarks9	3

List of Figures

FIGURE 1. LOGON PAGE	16
FIGURE 2. FORGOT PASSWORD DIALOG	17
Figure 3. Dashboard	18
FIGURE 4. MENU BAR	20
FIGURE 5. SYSTEM - MENU	20
FIGURE 6. INVENTORY	21
FIGURE 7. FRU INFORMATION	22
FIGURE 8. LOCATION	23
Figure 9. Server Health - Menu	23
Figure 10. Sensor Reading Page	24
FIGURE 11. LIVE WIDGET	25
FIGURE 12. THRESHOLD SETTINGS	25
FIGURE 13. EVENT LOG PAGE	26
FIGURE 14. SYSTEM LOG	28
FIGURE 15. AUDIT LOG	28
FIGURE 16. BSOD SCREEN	29
FIGURE 17. CONFIGURATION CROUP MENU	30
FIGURE 18. ACTIVE DIRECTORY SETTINGS	
FIGURE 19. ADD ROLE GROUP	
FIGURE 20. Advanced Active Directory Settings	
FIGURE 21. DNS SERVER SETTINGS PAGE	
Figure 22. System Event Log Page	
FIGURE 23. IMAGES REDIRECTION PAGE	
FIGURE 24. ADVANCED MEDIA SETTINGS PAGE	
FIGURE 25. I DAP/E-DIRECTORY SETTINGS PAGE	
FIGURE 26. ADVANCED LDAP/E-DIRECTORY SETTINGS PAGE	
FIGURE 27 MOUSE MODE SETTINGS PAGE	39
FIGURE 28 NETWORK SETTINGS PAGE	40
FIGURE 29 NTP SETTINGS PAGE	41
FIGURE 30 PAM ORDER PAGE	42
FIGURE 30 PFE MANAGEMENT – EVENT FILTER PAGE	43
FIGURE 32 PEF MANAGEMENT – MODIFY EVENT FILTER PAGE	45 44
FIGURE 32. PEF MANAGEMENT – MODELLE EVENT HELENT AGE	46
FIGURE 32 PEF MANAGEMENT – A BET POLICY PAGE	
FIGURE 35, PEF MANAGEMENT – MODIEV ALERT POLICY ENTRY PAGE	
FIGURE 36 PEE MANAGEMENT - MODILY FALLERY OLD'E ERTRY PAGE	40 ــــــــــــــــــــــــــــــــــــ
FIGURE 37 PEF MANAGEMENT – JAN DESTINATION PAGE	
FIGURE 37.1 ET MANAGEMENT – DAN DESTINATION FAGE	51
FIGURE 30. TEL MANAGEMENT - MODILI EAN DESTINATION ENTRY PAGE	
FIGURE 35.1 ET MANAGEMENT ADD LAN DESTINATION ENTRY FAGE	
FIGURE 40. RADIUS SETTINGS FACE	54
FIGURE 41. RADIOS ACTIONIZATION FAGE	+55
FIGURE 42. REMOTE SESSION FAGE	
FIGURE 43. SERVICES FAGE	
FIGURE 45. INICOLIFY SERVICE FAGE	
	סכ הם
TIGURE 43. JUL CERTIFICATE CONFIGURATION - OPLOAD JUL PAGE	00
FIGURE DU. DDL CERTIFICATE CONFIGURATION - GENERATE DDL PAGE	
FIGURE 51. CERTIFICATE CUNFIGURATION - VIEW SSL PAGE	
FIGURE 52. SYSTEM FIREWALL PAGE	

FIGURE 53. ADVANCED FIREWALL PAGE	63
FIGURE 54. ADD NEW RULE FOR IP PAGE	64
FIGURE 55. SYSTEM FIREWALL PAGE	65
FIGURE 56. ADD NEW RULE FOR PORT PAGE	65
FIGURE 57. USER MANAGEMENT PAGE	66
FIGURE 58. ADD NEW USER PAGE	67
FIGURE 59. MODIFY USER PAGE	68
FIGURE 60. VIRTUAL MEDIA PAGE	70
FIGURE 61. CIPHER SUITES PAGE	70
FIGURE 62. REMOTE CONTROL PAGE	71
FIGURE 63. CONSOLE REDIRECTION PAGE	71
FIGURE 64. IPMI COMMAND DIALOG	75
FIGURE 65. VIRTUAL MEDIA	76
FIGURE 66. VIDEO RECORD SETTINGS PAGE	78
FIGURE 67. POWER CONTROL AND STATUS PAGE	80
FIGURE 68. JAVA SOL PAGE	80
FIGURE 69. JAVA SOL PAGE	81
FIGURE 70. AUTO VIDEO RECORDING MENU	81
FIGURE 71. RECORD VIDEO	82
FIGURE 72. ADVANCED REMOTE VIDEO SETTINGS	83
FIGURE 73. PRESERVE CONFIGURATION	84
FIGURE 74. RESTORE CONFIGURATION	85
FIGURE 75. FIRMWARE UPDATE MENU	86
FIGURE 76. FIRMWARE UPDATE	86
FIGURE 77. FIRMWARE UPDATE PROCESS	87
FIGURE 78. UPLOAD BMC IMAGE PAGE	87
FIGURE 79. BIOS UPDATE	88
FIGURE 80. START UPDATING BIOS PAGE	88
FIGURE 81. UPLOAD BIOS IMAGE PAGE	88
FIGURE 82. IMAGE TRANSFER PROTOCOL	89

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 TS460, 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
ТММ	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 \rightarrow Network Settings \rightarrow 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.

Table 1. IPMI	2.0Configuration	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.

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

Table 2	2. Pro	perties	on	the	тмм	dashb	oard:
Tubic I		perties	011	unc		uusiib	ouru.

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 until enter the correct Username/Password. 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. 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)

ThinkServer Management Module	Lenovo.
Username: Password: Forgot Password?	
Login Required Browser Settings	

Figure 1. Logon 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.

Username:	lenovo
Password:	Forgot Password?
	Login

Required Browser Settings

- Allow popups from this site
- 2. Allow file download from this site. (How to 2)
- Enable javascript for this site
 Enable cookies for this site
- It is recommended not to use Refresh, Back and Forward options of the browser.

網頁訊息	X
?	Click OK if you want to continue resetting the User's password.
	確定 取消

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

After logging in, the TMM presents a Dashboard page showing overall server status. 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.

ThinkServer Management Module			Lenov
hboard System Server Health Configuration Remote Contr	ol Auto Video Recording Maintenance	e Firmware Update	i lenovo (Administrator) CRefresh VPrint 👘
ashboard			
board gives the overall information about the status of the device and remote serv vice Information	er. Sensor Monitoring		Event Logs
duct name: TS460			ME (0.11%)
ssis SN:	Status Sensor Re	eading	Host Power (0.49%)
Name: AMID05099322332 vare Revision: 1.59	 ATX+5VSB 4.92 	Volts 🔎	FAN2 (0.22%) FAN1 (0.16%)
ware Build Time: Feb 17 2017 11:47:43 AWST	 +3.3VSB 3.41 	9 Volts 🔎	REAR_FAN (0.16%) PSU2 AC lost (0.16%)
work Information (Edit)	CPU_Vcore Not	Available 🖌	PSU2 Presence (0.16%) PSU1 Presence (0.16%)
Address: D0:50:99:32:23:32	VCCSA Not.	Available 🔎	Others (0.36%)
etwork Mode: DHCP	VCCM Not	Available 🔎	ChassisIntr_BIOS (0.03%)
Address: 192.168.36.134	+V1.0M Not	Available 🖉	PSU1 AC lost (0.03%)
etwork Mode: DHCP Address: fe80::d250:99ff:fe32:2332	AVCCIO Not	Available D	
	NOCET SER		
ver Supply Information: PSU1 V	VCCST_SFR Not	Available 🗡	
dor Name: AcBel dor Part Number: ESD062-EL0G	VPPM Not	Available D	
dor Assembly Revision: S2	● +3V Not	Available 🔎	
ation of Manufacture: DG	 +5V Not. 	Available 🔎	
e: 20140809 vdor Serial Number: 1079	● +12V Not	Available 🔎	
hange PWR mode	 BAT 3.06 	Volts 🔎	
3	CPU_FAN Not.	Available 🔎	
cation LED Status: ON	REAR_FAN Not.	Available 🔎	
mate Control	FAN1 Not	Available 🔎	
Launch	FAN2 Not	Available 🔊	
	MB Temp		
	Orad Olde Terre Note	Augilable 0	
	 Card Side Temp Not a 	Avaliable M	
	CPU1 Temp Not	Available 🖌	

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).

- Product name: TS460
- Chassis SN:
- Hostname:
- Firmware Revision:
- Firmware Build Time:

Network Information

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

- MAC Address:
- V4 Network Mode:
- IPv4 Address:
- V6 Network Mode:
- IPv6 Address:

Power Supply Information

Display the information of the selected Power Supply. Click the menu to select PSU1 or PSU2.

- Vendor Name:
- Vendor Part Number:
- Vendor Assembly Revision:
- Location of Manufacture:

- Date:
- Vendor Serial Number:

Change PWR mode

Click 'Change PWR mode' to switch the power mode form Normal mode to Redundancy mode or back to Normal mode from Redundancy mode.

NOTE:

There are no "Power Supply Information" and "Change PWR mode" when install power supply without PMBus.

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. If you click the \sim icon, the sensor page for that particular sensor will displayed.

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.

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

Figure 4. Menu Bar

System

The System Group displays the following information

- Inventory
- FRU information
- Location

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

ThinkServer Management Module												
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update					
	Inventory											
	FRU Information											
	Location											



A detailed description of System is given below

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

ThinkServer Management N	Nodule	Lenovo
ashboard System Server He	ealth Configuration Remote Control Auto Video Recording Maintenance Firmware Update	¥lenovo (Administrator) ⊂ Refresh ©Print ■Logo HEI
nventory		
his page gives detailed information for	r the inventory in this system. Please restart the system if you didn't see anything.	
BIOS Information		
BIOS Vendor :	LENOVO	
BIOS Version :	VB1TS003	
BIOS Build Date :	07/15/2016	
CPU Information		
CPU Model :	Intel(R) Xeon(R) CPU E3-1240 v5 @ 3.50GHz	
CPU Signature :	Type 0, Family 6, Model 5e, Stepping 3	
CPU Core Count :	4	
CPU Thread Count :	8	
Base CPU Speed :	3500 MHz	
Max CPU Speed :	3900 MHz	
Min CPU Speed :	800 MHz	
L1 iCache :	32 KB × 4	
L1 dCache :	32 KB × 4	
L2 Cache :	256 KB × 4	
L3 Cache :	8192 KB	

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.

ThinkServer Management	Module							Leno	VO.
Dashbaard Sustam Conver	Health	Configuration	Demote Centrel	Auto Video Decordina	Maintenance	Cirmuna co Undoto	lenovo (Administrator)	CRefresh 🖗 Print	Logout
Dashboard System Server	neaith	Configuration	Remote Control	Auto video Recording	maintenance	Firmware Opdate			nelP
FRU Information									
This page gives detailed information f	for the vario	us FRU devices pre	esent in this system.						
Basic Information:									
FRU Device ID		0	•						
FRU Device Name		BMC FRU							
		-							
Chassis Information:									
Chassis Information Area Forma	at Version	1							
Chassis Type		Tower							
Chassis Part Number									=
Chassis Serial Number									
Chassis Extra									
Board Information:									
Board Information Area Format	Version	1							
Language		English							
Manufacture Date Time		Sat Jan 1 0	8:00:00 2011						
Board Manufacturer		LENOVO							
Board Product Name		TS460							
Board Serial Number									
Board Part Number		SB20M0798	34						
FRU File ID		001							
Board Extra		00:00:00:00	0:00:00						
Product Information:									
Product Information Area Forma	at Version	1							
Language		English							
Manufacturer Name		LENOVO							

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).

Location

This page displays the system location information. It can be used to configure location setting for the system.

Think	ThinkServer Management Module										L	eno	VO.
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update			lenovo (Administrato	or) CRefrest	n 🔗 Print	Logout HELP
Locatio	n												
This page is u	used to config	gure the location info	rmation.										
Loaction	n												
												Save	Reset



- Save: Click 'Save' to save the new location information configuration.
- **Reset:** Click 'Reset' to reset the modified changes.

Server Health

The Server Health Group displays the following information.

- Sensor Readings
- Event Log
- System and Audit Log
- BSOD Screen

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

	ThinkServer Management Module											
Dashbo	pard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update				
			Sensor Readings	;								
			Event Log									
			System and Aud	lit Log								
			BSOD Screen									

Figure 9. Server Health - Menu

A detailed description of Server Health Group is given below

Sensor Reading

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.

NOTE: When use the fix power, it is normal that PSU1 pin, PSU2 pin and PWR Consumption show Normal. 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.

ThinkServer	r Management Module								1	enovo.
Dashboard Syst	tem Server Health Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Upd	ate			Ienovo (Administrator) ⊂ Refre	sh ⊗Print ≫Logout HELP
Sensor Rea	dings									
All sensor related inf	ormation will be displayed here. Double click o	on a record to toggle (ON	I / OFF) the live widget for that	particular sensor.						
All Sensors	•								Sensor	Count: 35 sensors
Sensor Name 🗳	Status 🛆	Current Read	د ding							
ATX+5VSB	Normal	4.89 Volts	471		0.1/-1/-					Normal
+3.3VSB	Normal	3.399 Volts	AI)	+5738: 4.8	9 Volts					Norman
CPU_Vcore	Normal	1.15 Volts	Threst	olds for this sen	sor				Live V	Vidget Off On
VCCSA	Normal	1.079 Volts								
VCCM	Normal	1.209 Volts	Lowe	r Non-Recoverable	e (LNR): 4.23 Volts				Upper Non-Recoverable (UN	R): 5.61 Volts
+V1.0M	Normal	1.02 Volts	Lowe	r Critical (LC):	4.71 Volts				Upper Critical (UC):	5.55 Volts
+VCCIO	Normal	0.969 Volts	Lowe	r Non-Critical (LN	C): 0 Volts				Upper Non-Critical (UNC):	0 Volts
VCCST_SFR	Normal	1.01 Volts							Thursd	hald Cattings
VPPM	Normal	2.48 Volts							Thres	noid Settings
+3V	Normal	3.28 Volts								
+5V	Normal	5.009 Volts	Graph	nical View of th	nis sensor's eve	nts				
+12V	Upper Non-Recoverable	13.5 VOItS								
BAI	Normal	3.179 VOIts								
CPU_FAN	Normal	1200 RPM	LN	(0)						E
REAR_FAN	Lower Non-Childai	0 RPM		(0)						
FANT	Lower Non-Childan	0 RPM								
FANZ	Lower Non-Childai	0 RPM	LN	C (0)						
Mb remp Cord Side Temp	Normal	35 C	UN	R (0)						
Card Side Temp	Normal	31 0								
CPUT temp	Normal	44 0	U	C (0)						
Chassislet DVO	Normal	43 0	UN	0						
Inlet Temp	Air deassened	UX0000		- (-)						
Rel 14 Braganca	Normal Brossnes Detected	INOL AVAILABLE	Othe	r (0)						
PSUI Pin	Normal	0.8001	Discret	. (0)						
PRU1 AC lost	All dependented	0.4000	0.001.01	(0)					_	
PSU 12 Presence	Presence Detected	0x8000				Number of Entrice		9		
PSI I2 Pin	Normal	40 Watts				Number of Entrie	69			
PSU2 AC Inst	hatrassed IIA	0x8000							View t	his Event Log
PWR Consumption	Normal	40 Watte								
PSILRedundancy	hetresseeb IIA	0v8000								
CPU1 Power	Normal	13 Watts								
CPU1 THERMTRIP	All deasserted	0x8000								
CPU CATERR BMC	All deasserted	0x8000								
SEL Status	All deasserted	0x8000								
	ra dodoonto d	0.0000								

Figure 10. 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 11. 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.

Threshold Settings : +3.3VSB		X
Lower Non-Recoverable (LNR):		
Lower Critical (LC):		
Lower Non-Critical (LNC):	Not settable	
Upper Non-Recoverable (UNR):		
Upper Critical (UC):		
Upper Non-Critical (UNC):	Not settable	
		Save Cancel

Figure 12. 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", "Unknown PSU Redundancy".

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.

🔁 Thi	nkServer Management Module			Lenovo
Dashboard	System Server Health	Configuration Remote Control A	uto Video Recording Maintenance Firmware Update	🕴 lenovo (Administrator) 🤇 Refresh 較 Print 🔷 Logot HEL
Event	Log			
Events gen	erated by the system will be logged t	here. Double-click on a record to see the descrip	tion.	
All Even	IS	✓ filter by: All Sensors	\checkmark	Event Log: 7 event entries, 1 page(s)
BMC	Timezone 🔿 Client Timezone UT(C Offset: (GMT-04:00)		<< < 1 > >>
Event ID	د Time Stamp د	Sensor Type 🗅	Description	
7	06/30/2016 01:25:24	Fan	FAN3: Lower Non-Critical - Going Low - Deasserted	
6	06/30/2016 01:25:23	Fan	FAN2: Lower Non-Critical - Going Low - Deasserted	
5	06/30/2016 01:25:20	Fan	FAN2: Lower Non-Critical - Going Low - Asserted	
4	06/30/2016 01:25:18	Fan	FAN3: Lower Non-Critical - Going Low - Asserted	
3	06/30/2016 00:24:25	System Event	Timestamp Clock Synch - Asserted	
2	06/30/2016 00:24:28	System Event	Timestamp Clock Synch - Asserted	
1	06/16/2016 19:12:10	Event Logging disabled	SEL_Status: Log Area Reset/Cleared - Asserted	
-				
				Save Event Logs Clear All Event Logs

Figure 13. EventLog 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.
- **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.
- Save Event Logs: Clicking this button will pop-up a Save dialog to save all existing records.

NOTE: There are some event log "Bugcheck code OEM Event Record" which asserted by OS after system BSOD.

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.

Fuent	Depard Turne	Generator ID1+		
Event	Record Type	[7:1] <i>•</i>	[0]	
BIOS Generated Events.		0x00 - 0x0F _*		
SMI Handler Events]	0x10 - 0x1F _*]	
System Management Software Events.]	0x20 – 0x2F₀	16	
System Software - OEM Events	0x00 – 0xBF₀	0x30 – 0x3F _e	TDo	
Remote Console software Events.]	0x40 − 0x46]	
Terminal Mode Remote Console software Events]	0x47₽		
System Event Records.		others _€		
OEM Event Records _e	0xC0 – 0xFF₽	₽Q		

NOTE1: About the "Record Type" & "Generator ID", you can refer to the IPMI 2.0 spec for details. **NOTE2:** For sensor type: 'OS Stop/Shutdown', IPMITOOL will show 'OS Critical Stop'. **NOTE3:** For sensor type: 'Base OS Boot/Installation Status', IPMITOOL will show 'OS BootBase'.

System and Audit Log

This page displays logs of system and audit events for this device (if the options have been configured). If configured, these logs will display all the system and audit events that occurred in this device. **NOTE:** Logs have to be configured under 'Configuration -> System and Audit Log' in order to display any entries.

- Filter by : Choose the option 'Filter by' to filter event.
- **System Log :** Click the System Log tab to view all system events. Entries can be filtered based on their classification levels.
- Audit Log : Click the Audit Log tab to view all audit events for this device.

ThinkServer Management Module

Lenovo

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

System and Audit Log

System Log	Audit Log			UTC Offset: (GMT+08:
er by: Alert	27			This Filter: 2 event entrie
Event ID 🔺	Time Stamp △	HostName ->	Description A	
1	Nov 9 17:55:20	AMID05099E02366	kernel: [15.540000] Helper Module Driver Version 1.2	
2	Nov 9 17:55:20	AMID05099E02366	kernel: [15.540000] Copyright (c) 2009-2015 American Megatrends Inc.	

Figure 14. System Log

ThinkServer Management Module						Lenovo	0.		
	_							🕯 lenovo (Administrator) 🛛 CRefresh 🚳 Print 👘 Li	ogout
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		HELP

System and Audit Log

This page displays logs of system and audit events for this device (if the options have been configured).

System Log	Audit Log			UTC Offset: (GMT+08:0
				This Filter: 6 event entries
Event ID 🗳	Time Stamp	HostName 🗅	Description 📣	
1	Nov 9 17:56:31	AMID05099E02366	lighttpd[2129]; [2129 : 2129 INFO]https Login from IP:192.168.36.38 user:lenovo	
2	Nov 9 18:24:09	AMID05099E02366	lighttpd[2129]: [2129 : 2129 INFO]https Login from IP:192.168.36.67 user:lenovo	
3	Nov 9 18:28:09	AMID05099E02366	lighttpd[2129]: [2129 : 2129 INFO]HTTPS logout from IP:192.168.36.67 user:lenovo	
4	Nov 9 18:28:31	AMID05099E02366	lighttpd[2129]: [2129 : 2129 INFO]https Login from IP:192.168.36.67 user:lenovo	
5	Nov 9 18:40:57	AMID05099E02366	lighttpd[2129]: [2129 : 2129 INFO]HTTPS logout from IP:192.168.36.38 user:lenovo	
6	Nov 9 19:07:30	AMID05099E02366	lighttpd[2129]; [2129 : 2129 INFO]HTTPS logout from IP:192.168.36.67 user:lenovo	

Figure 15. Audit Log

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 page is shown below.



Figure 16. 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.

Think	Server Man	agement Module				_	
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update
			Active Directory				
			DNS				
			Event Log				
			Images Redirection				
			LDAP/E-Directory				
			Mouse Mode				
			Network				
			NTP				
			PAM Order				
			PEF				
			RADIUS				
			Remote Session				
			Services				
			Interfaces				
			SMTP				
			SNMP				
			SSL				
			System Firewall				
			Users				
			Virtual Media				
			Cipher Suites				
				_			

Figure 17. 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.

E Think	Server Man	agement Module							Leno	VO.
								lenovo (Administrator)	🗆 Refresh 🛛 🕏 Print	Logout
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update			HELP
Active D)irectory	/							Advanced 5	Settings

The 'Active Directory' is currently disabled. To enable Active Directory and configure its settings. Click on 'Advanced Settings' button, first,

The list below shows the current list of configured Role Groups. If you would like to delete or modify a role group, select the name from the list and click Delete Role Group or Modify Role Group. To add a new Role Group, select an unconfigured slot and click Add Role Group.

Role Group ID 🔺	Group Name 🔺	Group Domain 🗳	Group Privilege 🗳
1	~	~	~
2	~	~	~
3	~	~	~
4	~	~	~
5	~	~	~

Add Role Group Modify Role Group Delete Role Group

Number of configured Role groups: 0



- 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.

Add Role Group	X
Role Group Name Role Group Domain Role Group Privilege Extended Privileges	Administrator VMedia
	Add Cancel

Figure 19. Add Role Group

- **Group Name:** Enter the Role Group Name. This name identifies the role group in Active Directory.
 - Role Group Name is a string of 64 alpha-numeric characters.
 - Special symbols hyphen and underscore are allowed.
- **Group Domain:** Enter the Role Group Domain. This is the domain where the role group is located.
 - Domain Name is a string of 255 alpha-numeric characters.
 - Special symbols hyphen, underscore and dot are allowed.

- **Group Privilege:** Enter the Role Group Privilege. This is the level of privilege to be assigned for this role group.
- **Extended Privileges:** This field used to assign the KVM and VMedia privilege for this role group.
- **NOTE:** The KVM and VMedia privilege will enable(disable) automatic when User Privilege is administrator(other).

Add: Click 'Add' to save the new role group and return to the Role Group list.

Cancel: Click 'Cancel' to cancel the modification and return to the Role Group list.

Advanced Active Directory

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.

Advanced Active Directory Settings			X
Active Directory Authentication	Enable		
Secret Username]	
Secret Password]	
User Domain Name			
Domain Controller Server Address1]	
Domain Controller Server Address2			
Domain Controller Server Address3]	
		_	
			Save Cancel

Figure 20. 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".
 - 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.

ThinkServer Management Module	,	Lenovo.
Dashboard System Server Health	kenovo (Administrator) C Re Configuration Remote Control Auto Video Recording Maintenance Firmware Update	fresh SPrint Logout HELP
DNS Manage DNS settings of the device. Domain Name Service Configuration		
DNS Service Multicast DNS mDNS Settings	 Enable Enable 	
Host Configuration Host Settings Host Name	Automatic - AMID05099E02366	
Register BMC bond0	Register BMC Nsupdate DHCP Client FQDN Hostname	
TSIG Configuration TSIG Authentication Current TSIG Private File New TSIG Private File	■ Enable Not Available 瀏覽 未選擇檔案。	
Domain Name Configuration Domain Settings Domain Name	IPMI_LAN_v4 -	

Figure 21. DNS ServerSettingsPage

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.

Think	Server Man	nagement Module						Lenovo
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	♦ lenovo (Administrator) ⊂ Refresh ♥Print ● Logo HE
Event Lo	og							
his page is us	sed to configu	ure the System Event	log information .					
Current	Event Log Po	olicy : LINEAR						
Enat	ble Linear Eve	ent Log Policy						
Enat	ble Circular E	vent Log Policy						
								Save Res

Figure 22. 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.

1 Think	Server Mana	agement Module						Lenovo
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	● lenovo (Administrator) ⊂ Refresh ♀Print ■ Logout HELF
Images	Redirec	tion						
Remote Media	is used to m	ount the images from	remote system and	perform redirection. Ren	note Media is currently disable	d. To configure Remo	te Media Settings. Click on 'Advanced Settings' butto	Advanced Settings
								Number of Available Media Types: 0
# Δ	Me	edia Type ⊃		Image Na	د me		Redirection Status ム	Connected Server Session 🕒
					Dat	a Not Available		
								Start Redirection



- 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.**

Advanced Media Settings		X
Remote Media		
Remote Media Support Enable Media Types	Enable CD/DVD Floppy Harddisk All	
		Save Cancel

Figure 24. 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.
- **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.
- Enable Media Types: Selected 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

Think	Server Man	agement Module							Lenovo
								Ienovo (Administrator) CR	efresh 🕏 Print 📑 Logout
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		HELP
LDAP/E-Direct LDAP/E-Direct The list below Add Role Grou	-Directo tory is current shows the cu	IV disabled. To enable	e LDAP/E-Directory a Role Groups. If you v	nd configure its settings would like to delete or n	s. Click on 'Advanced Settings' nodify a role group, select the r	button, first. name from the list an	l click Delete Role Group	r or Modify Role Group. To add a new Role Group, select an ur Number	Advanced Settings inconfigured slot and click of configured Role groups: 0
Role Gro	up ID 🔺		Group Name 🔺			Group Search Bas	eΔ	Group Privilege	
1			~			~		~	
2			~			~		~	
3			~			~		~	
4			~			~		~	
5			~			~		~	
								Add Role Group Modify Role Group	Delete Role Group

Figure 25. 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 Settings

Use this page to configure advanced LDAP/E-Directory configuration.

Advanced LDAP/E-Directory Settings	×
LDAP/E-Directory Authentication	
Encrypted Type	No Encrypted \sim
Common Name Type	IP Address 🗸
Server Address	
Port	389
Bind DN	
Password	
Search Base	
Attribute of User Login	cn v
	Save Cancel

Figure 26. 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'.
 - 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 6 to 63 alpha-numeric characters.
 - The string should start with 'cn' or 'uid.'
 - start with cn: the string length should be 6 (ex cn=air).
 - start with uid: the string length should be 7 (ex uid=air).
 - It must start with an alphabetical character. ex: cn=1r will be illegal.
 - Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
 - The end of string can not be ','.
 - 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 63 alpha-numeric characters.
 - start with cn: the string length should be 6 (ex cn=air).
 - start with uid: the string length should be 7 (ex uid=air).
 - start with ou: the string length should be 5 (ex ou=a1).
 - start with dc: the string length should be 5 (ex dc=a1).
 - start with o: the string length should be 4 (ex o=au).
 - It must start with an alphabetical character. ex: cn=1r will be illegal.
 - Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
 - Example: ou=login,dc=domain,dc=com
 - The end of string cannot be ','.
- 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.
 - 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 27. 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.

Think	Server Man	agement Module							Leno	VO.
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	• lenovo (Administrator) ⊂ Refresh 🐶Print	Logout HELP
Network	(
Manage networ	rk settings of t	he device.								
MAC Add	ress		D0:50:99:	E0:23:66						
IPv4 Configura	ation									
IPv4 Setti	ings		Enab	le						
Obtain an	IP address	automatically	Use DI	HCP						
IPv4 Addr	ress		192.168.3	36.91						
Subnet M	lask		255.255.2	255.0						
Default G	ateway		192.168.3	36.1						
IPv6 Configura	ation									
IPv6 Setti	ings		Enab	le						
Obtain an	n IP address a	automatically	🗵 Use DI	HCP						
IPv6 Addr	ress		fe80::d25	50:99ff:fee0:2366						
Subnet P	refix length		0							
VLAN Configu	ration									
VLAN Set	ttings		Enab	le						
VLAN ID			0							
VLAN Prie	ority		0							

Figure 28. 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.

ThinkServer Manage	ement Module							Lenovo
Dashboard System S	erver Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 lenovo (Administrator) 🤇	Refresh ≌Logou HEL
NTP								
Here you can either configure t	ne NTP server or vie	w and modify the	device's Date & Time se	attings.				
Date:	November	- 10	- 2016	T				
Time: (hh:mm:ss)	11	26	26					
Timezone:	GMT+8		•					
Primary NTP Server:	pool.ntp.org							
Secondary NTP Server:	time.nist.gov							
Automatically synchro	nize Date & Time wi	th NTP Server						
							Refresh	Save Reset



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, and open PAM Ordering page, click **Configuration > PAM Order** from the menu bar. A sample screenshot of PAM Ordering Page is shown below.

Think	Server Mana	agement Module						Lei	novo.
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 Tenovo (Administrator) C Refresh 🕏	Print Logout HELP
PAM Or	der								
This page is u	sed to configu	ire the PAM Ordering	for the user authen	tication.					
	IPMI								
	LDAP	^							
Act	ive Directory	· •							
	RADIUS								

Save Reset



- **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. Loggedin session will be logged out.
- **Reset**: Click 'Reset' to reset the modified changes.

PEF

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

In TMM GUI, the PEF Management is used to configure the following

- Event Filter
- Alert Policy
- LAN Destination

To open PEF Management Settings page, click **Configurations > PEF** from the menu bar. Each tab is explained

below.

Event Filter Tab

A PEF implementation is recommended to provide at least 15 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over- temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 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.

ThinkServe	er Management Module						Lenovo
hboard Sys	stem Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 lenovo (Administrator) 🤇 Refresh 🗇 Print 🛸 L
F							
this page to co	nfigure Event Filter, Alert Po	blicy and LAN Destina	ation. To delete or modi	fy an entry, select it in the list a	nd click "Delete" or "M	odify". To add a new entry, select an unconfigured slo	ot and click "Add".
Event Filter	Alert Policy	LAN Dest	nation				
							Configured Event Filter count:
PEF ID	△ Filt	er Configuration 🔺		Event Filter Actio	n 🛆	Event Severity 🛆	Sensor Name 🛆
1		Disabled		[Alert]		Unspecified	Any
2		Disabled		[Alert]		Unspecified	Any
3		Disabled		[Alert]		Unspecified	Any
4		Disabled		[Alert]		Unspecified	Any
5		Disabled		[Alert]		Unspecified	Any
6		Disabled		[Alert]		Unspecified	Any
7		Disabled		[Alert]		Unspecified	Any
8		Disabled		[Alert]		Unspecified	Any
9		Disabled		(Alert)		Unspecified	Any
10		Disabled		[Alert]		Unspecified	Any
11		Disabled		[Alert]		Unspecified	Any
12		Disabled		[Alert]		Unspecified	Any
13		Disabled		(Alert)		Unspecified	Any
14		Disabled		(Alert)		Unspecified	Any
15		Disabled		[Alert]		Unspecified	Any
16		~		~		~	~
17		~		~		~	~
18		~		~		~	~
19		~		~		~	~
20		~		~		~	~
21		~		~		~	~
22		~		~		~	~
23		~		~		~	~
24		~		~		~	~
25		~		~		~	~
25		~		~		~	~ Add Modify Dele

Figure 31. PEF Management – Event Filter page

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.

- 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.
- 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:

- 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.

🗾 Think	Server Man	agement Module								Lend	ovo
ashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	€ lenovo	(Administrator)	CRefresh 🔗Prin	nt PLog Hi
'EF											
						click "Delete" or "Mo		nconfigured slot and click "Ad			
					,,,		,		N		
Event	Filter	Modify Event F	ilter entry								
		Event Filter Conf	iguration						*	red Event Filter o	count: 15
	D A	PEE ID	iguration		1					Δ	
	2	Filter Configuration	n		I Cashia				=		
	3	Event Severity			Linepacified	-					
		Eilter Action conf	Iguration		Unspecified	-					
	3	Fuent Filter Action	iguration								
7		Event Filler Action			Alert						
	3	Power Action			None	·					
	0	Alert Policy Numbe	er		1 •						
1	1	Generator ID con	inguration								
	2	Generator ID Data	1		Raw Data						
	4	Generator ID 1			0xFF						
	5	Generator ID 2			0xFF				-		
	6				_			Maulif.	Consel		
								Modify	Cancel	Modify	

Figure 32. PEF Management – Modify Event Filter page

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

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 I²C 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.
- **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 Entry:

- 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.

Add Event Filter entry	
	A
Event Filter Configuration	
PEFID	16
Filter Configuration	Enable
Event Severity	Unspecified •
Filter Action configuration	
Event Filter Action	☑ Alert
Power Action	None
Alert Policy Number	1 •
Generator ID configuration	
Generator ID Data	🗹 Raw Data
Generator ID 1	0x0
Generator ID 2	0×0
Event Generator	Slave type Software type
Slave Address/Software ID	
Channel Number	
IPMB Device LUN	1 •
Sensor configuration	
Sensor Type	All Sensors
Sensor Name	Voltage_5
Event Options	Sensor Events
	Lower Non-Critical : 🔲 Going Low 🔲 Going High
	Lower Critical : Going Low Going High
Sensor Events	Lower Non-Recoverable : Going Low Going High
	Upper Non-Critical : Going Low Going High
	Upper Chucai : Going Low Going High
Event Data configuration	
Event Trigger	0
Event Data 1 AND Mask	0
Event Data 1 Compare 1	0
Event Data 1 Compare 2	0
Event Data 2 configuration	
Event Data 2 AND Mask	0
Event Data 2 Compare 1	0
Event Data 2 Compare 2	0
Event Data 3 configuration	
Event Data 3 AND Mask	0
Event Data 3 Compare 1	0
Event Data 3 Compare 2	
	•
	[Add] [Cancel

Figure 33. PEF Management – Add Event Filter Entry Pag

Use this form to add a new Event Filter entry.

For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.

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 I²C 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.
- 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 Tab

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

🔁 Think	Server Man	agement Module						Lenovo.
								🕯 lenovo (Administrator) 🤇 Refresh 🔗 Print 🛸 Logout
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	HELP

PEF

Use this page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify a entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add"

Event Filter	Alert Policy	LAN Destination			
		· · · ·		Config	gured Alert Policy count: 15
Policy Entry # 🔺	Policy Number 🔺	Policy Configuration 🗳	Policy Set 🗳	Channel Number 🔺	Destination Selector 🔺 🔺
1	1	Disabled	Always send alert to this destination	1	0
2	2	Disabled	Always send alert to this destination	1	0
3	3	Disabled	Always send alert to this destination	1	0
4	4	Disabled	Always send alert to this destination	1	0
5	5	Disabled	Always send alert to this destination	1	0
6	6	Disabled	Always send alert to this destination	1	0
7	7	Disabled	Always send alert to this destination	1	0
8	8	Disabled	Always send alert to this destination	1	0
9	9	Disabled	Always send alert to this destination	1	0
10	10	Disabled	Always send alert to this destination	1	0
11	11	Disabled	Always send alert to this destination	1	0
12	12	Disabled	Always send alert to this destination	1	0
13	13	Disabled	Always send alert to this destination	1	0
14	14	Disabled	Always send alert to this destination	1	0
15	15	Disabled	Always send alert to this destination	1	0
16	~	ner .	~	~	~ .
				Add	Modify Delete



Modify Alert Policy Entry:

- 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.

Aboard System Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update Firmware Update <td< th=""><th></th><th>server Man</th><th>agement Module</th><th></th><th></th><th></th><th></th><th></th><th></th><th>Lenovo</th></td<>		server Man	agement Module							Lenovo
Bystem Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update EF Image: Second gene Event Filter, Aert Policy and LAN Destination. To delete or modify a entry, select it in the list and clek "Delete" or "Modify". To add a new entry, select an unconfigured slot and clek "Add". Image: Second gene Event Filter, Aert Policy entry Policy Entry #	_								lenovo (Administrato	r) 🕻 Refresh 🐶Print 📕Le
Policy Entry # 4 Policy Entry # 4 Policy Configuration 6 Policy Set of String 0 4 Policy Set of 0 0 3 Policy Configuration 4 Policy Set of 0 0 3 Policy Set of 0 0 3 Policy Set of 0 0 0 0 1 Policy Set of 0 0 0 0 0 0 0 0 0 0 0 0 1 Policy Configuration 0 0 1 0 0 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 <t< th=""><th>hboard</th><th>System</th><th>Server Health</th><th>Configuration</th><th>Remote Control</th><th>Auto Video Record</th><th>ng Maintenan</th><th>e Firmware Update</th><th></th><th></th></t<>	hboard	System	Server Health	Configuration	Remote Control	Auto Video Record	ng Maintenan	e Firmware Update		
his page to configure Event Filter, Alert Policy and LAN Destination. To delete or modify a entry, select it in the list and click "Delete" or "Modify". To add a new entry, select an unconfigured slot and click "Add". Vent Filter Modify Alert Policy entry Policy Entry # 4 1 Policy Entry # Policy Configuration 6 2 Policy Configuration 3 Polsy Self 0 0 3 O self 4 0 4 0 6 0 7 Destination Selector 7 Alert String 4 0 10 1 11 Disabled 12 1 13 Disabled 14 14 Disabled Alert String Always send alert to this destination 14 14 15 Disabled										
Event Filter Modify Alert Policy entry Image: Control of the cont	this page to	o configure E	event Filter, Alert Polic	y and LAN Destination	on. To delete or modify	a entry, select it in the list	and click "Delete" or	"Modify". To add a new entry, select an u	inconfigured slot and click "Add".	
Policy Entry # 4 Policy Entry # 4 Policy Entry # 4 Policy Configuration Enable Policy Set 0 Policy Set 0 Channel Number 1 Sector 0 Get Altert Policy Configuration Enable Destination Selector 0 Get Altert Policy Entry # 4 Policy Set 0 Destination Selector 0 Red Event Specific Altert String Key 0 Internet String Key 0	Event F	Filter								X
Policy Entry # 4 1 Policy Entry # 4 1 Policy Number 4 2 Policy Onfiguration Enable 0 0 4 O 5 Channel Number 1 6 Destination Selector 0 7 Destination Selector 0 8 Alert String Event Specific 0 9 Alert String Key 0 0 11 Image: Cancel	LTOITT		Modify Alert Po	olicy entry						urad Alart Pollov count: 1
Policy Luny 2 - 0 Policy Number 4 0 2 Policy Configuration Enable 0 4 Policy Set 0 0 5 Channel Number 1 0 5 Channel Number 1 0 6 Destination Selector 0 7 O 0 8 Alert String Event Specific 0 9 Alert String Key 0 0 10 0 0 11 0 0 12 13 Disabled Aways send alert to this destination 1 14 14 Disabled Aways send alert to this destination 1 15 15 Disabled Aways send alert to this destination 1			Policy Entry #			4				and Alert Folicy Count.
2 Policy Configuration Enable 0 3 Policy Set 0 0 5 Channel Number 1 0 6 Destination Selector - 0 7 Destination Selector - 0 8 Alort String Event Specific 0 9 Alert String Key 0 0 11 Modify Cancel 12 13 Disabled Always send alert to this destination 1 14 14 Disabled Always send alert to this destination 1 15 15 Disabled Always send alert to this destination 1		nuy # 🗅	Policy Number			4	•			
3 For any province of the second of the se			Policy Configuration	on		Enable	,			0
4 Policy Sea 0 5 Channel Number 1 6 Destination Selector 0 7 Destination Selector 0 8 Alert String Event Specific 0 10 Alert String Key 0 0 11 1 0 0 12 13 Disabled Always send alert to this destination 1 14 14 Disabled Always send alert to this destination 1 16 5 Disabled Always send alert to this destination 1			Policy Cot				-			0
Channel Number 1 Channel Number 1 Destination Selector 0 Alert String Event Specific 0 Alert String Key 0 0 10 Modify Cancel 11 Modify Cancel 13 13 Disabled Always send alert to this destination 1 14 14 Disabled Always send alert to this destination 1 15 15 Disabled Always send alert to this destination 1			Policy Set			0	•			0
7 Destination Selector 0 7 Aleft String Event Specific 0 9 Aleft String Key 0 0 10 0 0 0 11 Image: Selector Specific 0 12 Modify Cancel 0 13 Disabled Always send alert to this destination 1 14 14 Disabled Always send alert to this destination 1 15 15 Disabled Always send alert to this destination 1			Channel Number			1	•			0
8 Alert String Event Specific 0 9 Alert String Key 0			Destination Select	or			-			0
9 Alert String Key 0 0 0 10			Alert String			Event	Specific			0
10 0 11 Modify Cancel 0 12 10 0 0 13 13 Disabled Aways send alert to this destination 1 0 14 14 Disabled Aways send alert to this destination 1 0 15 15 Disabled Aways send alert to this destination 1 0	9		Alert String Key			0	•			0
11 Modify Cancel 0 12 0 <)								0
12 0 13 13 Disabled Always send alert to this destination 1 0 14 14 Disabled Always send alert to this destination 1 0 15 15 Disabled Always send alert to this destination 1 0 16 - - - - - -									Modify Cancel	
13 13 Disabled Aways send alert to this destination 1 0 14 14 Disabled Aways send alert to this destination 1 0 15 15 Disabled Aways send alert to this destination 1 0 16 ~ ~ ~ ~ ~		2	10		Distant and					0
14 14 14 1 0 15 15 Disabled Aways send alor to its destination 1 0 16 ~ ~ ~ ~ ~			13						1	
			14						1	

Figure 35. PEF Management – Modify Alert Policy Entry Page

This form is used to modify the existing Alert Policy entry.

For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.

- **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:

- 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.

Add Alert Policy entry	
Policy Entry #	16
Policy Number	1 ~
Policy Configuration	Enable
Policy Set	0 ~
Channel Number	1 ~
Destination Selector	1 ~
Alert String	Event Specific
Alert String Key	0 ~
	Add Cancel

Figure 36. PEF Management – Add Alert Policy Entry Page

This form is used to add a new Alert Policy entry.

- For more information, refer Platform Event Filtering (PEF) section in IPMI Specification.
- **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 Tab

14 15

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

🔁 Think	Server Man	agement Module							Lenovo
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	lenovo (/	Administrator) ⊂Refresh �Print ≥Logout HELP
PEF	to configure E	unat Eiltar, Alart Dalia	w and LAN Destination	an To dalata ar modify	a antru coloct it in the list and	oliok "Doloto" or "Ma	difu". To odd o now ontou o	aleat as unconfigured old and allow "Add	
Event	Filter	Alert Policy	LAN Dest	ination	a enay, select it in the list and	CICK Delete of MC	uny . To aut a new entry, s	elect all anconingured sict and click Aud	
LAN Cha	nnel: 1 ·	n A		Destination Typ	د e			Destination Address →	Configured LAN Destination count: 1
	1			Snmp Trap				192.168.36.111	
	2			~				~	
	3			~				~	
	4			~				~	
	5			~				~	
	6			~				~	
	7			~				~	
	8			~				~	
	9			~				~	
	10			~				~	
	11			~				~	
	12			~				~	

Figure 37. 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.

Send Test Alert

Add Modify Delete

- 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.**

Think	Server Man	agement Module							Lenovo
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🗘 lenovo (Administ	rator) ⊂Refresh �Print →Logout HELP
PEF									
Use this page	to configure E	vent Filter, Alert Polic	cy and LAN Destinati	on. To delete or modify	a entry, select it in the list and (click "Delete" or "Mo	dify". To add a new entry, s	select an unconfigured slot and click "Add".	
Event	Filter	Modify LAN De	stination entry						×
LAN Char	nnel: <u>1 -</u>	LAN Channel Nurr	nber		1				LAN Destination count: 1
	1 0	LAN Destination			1				
	3	Destination Type Destination Addre	ss		Snmp Trap 192.168.36.1	-			
	4	Username				Ŧ			
	6 7	Subject Message							
	8 9							Modify	acel
	10 11			~				~	
	12 13								
	14 15								

Figure 38. PEF Management – Modify LAN Destination Entry Page

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

- 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:

- 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.

Add LAN Destination entry	
LAN Channel Number LAN Destination	
Destination Type	Snmp Trap v
Destination Address	
Username	v
Subject	
Message	
	Add Cancel

Figure 39. PEF Management – Add LAN Destination Entry Page

Use this form to add a new LAN destination entry.

- 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.

Think	Server Man	agement Module							Lenovo
								ê lenovo (Administra	ator) CRefresh SPrint Logout
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		HELP
RADIUS									
The RADIUS / Advanced Set	Authenticatior tings, RADIU	n is currently disable S Server authenticat	d. To enable RADIUS ion should be enable	Authentication and er d.	ter the required information to	access the RADIUS	S server. Press the Save butto	on to save your changes. To configure the	Advanced Settings
RADI	US Authentic	ation	Enable						
Port			1812						
Serve	er Address								
Secr	et								
Exter	nded Privileg	es	🗹 KVM 🗹 VMedia						
									Save Reset

Figure 40. 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 configuration setting:

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.

Radius Authorization		X
Administator	H=4	
Operator	H=3	
User	H=2	
OEM Proprietary	H=1	
No Access	H=0	
	Save C	Cancel

Figure 41. 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.

Think	Server Man	agement Module		Leno	VO.					
Dashboard	System	Server Health	Configuration	Rem	ote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 lenovo (Administrator) 🔍 Refresh 🚯 Print	Logout HELP
Remote	Sessio	n								
This page is u	sed to configu	re Remote Session	ettings							
Single Po	ort Applicatio	n 🗵	Enable							
Keyboar	d Language	Au	to Detect (AD)	•						
V Loca	I Monitor OF	F Feature Status								
Auto	matically OF	F Local Monitor, W	nen JViewer Launch	nes						
									Save	Reset



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.

🛃 Think	Server Management M	odule						Lenovo
					P 114	_	• lenovo (Administrator)	CRefresh Print Logo
Jashboard	System Server He	aith Configuration	Remote Control Auto	video Recording Maintenanc	e Firmware Opdate			HEL
Services	S							
	a				1021001000000 88 98 90000000	12 12 12		
Below is a list	of services running on the	BMC. It shows current status	s and other basic information a	bout the services. Select a slot and pr	ess "Modify" button to modify the	services configuration.		
Below is a list	of services running on the	BMC. It shows current statu	s and other basic information a	bout the services. Select a slot and pr	ess "Modify" button to modify the	services configuration.		Number of Services: 7
Below is a list # →	of services running on the Service Name →	BMC. It shows current status Current State →	s and other basic information a Interfaces अ	bout the services. Select a slot and pr Nonsecure Port 스	ess "Modify" button to modify the s	services configuration.	لد Maximum Sessions	Number of Services: 7 Active Sessions 스
Below is a list #_⊥ 1	of services running on the Service Name web	BMC. It shows current status Current State ے Active	s and other basic information a Interfaces 스 bond0	bout the services. Select a slot and pr Nonsecure Port $\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \$	ess "Modify" button to modify the s Secure Port 스 443	services configuration. Timeout → 1800	Maximum Sessions → 20	Number of Services: 7 Active Sessions 스 <u>View</u>
Below is a list # 스 1 2	of services running on the Service Name Δ web kvm	MC. It shows current statu: <u>Current State</u> Active Active	s and other basic information a Interfaces bond0 bond0	bout the services. Select a slot and pr Nonsecure Port 스 80 7578	ess "Modify" button to modify the : Secure Port → 443 7582	Timeout	Maximum Sessions → 20 2	Number of Services: 7 Active Sessions → <u>View</u> <u>View</u>
Below is a list # 1 2 3	of services running on the Service Name 스 web kvm cd-media	MC. It shows current status Current State Active Active Active	s and other basic information a Interfaces bond0 bond0 bond0	Nonsecure Port $\ \ \ \ \ \ \ \ \ \ \ \ \ $	Secure Port $\ \ \ \ \ \ \ \ \ \ \ \ \ $	services configuration. Timeout 1800 N/A	د Maximum Sessions ک 20 2 4	Number of Services: 7 Active Sessions → <u>View</u> <u>View</u> <u>View</u>
Below is a list # 스 1 2 3 4	of services running on the Service Name web kvm cd-media fd-media	MC. It shows current statu: <u>Current State</u> → Active Active Active Active	s and other basic information a Interfaces bond0 bond0 bond0 bond0 bond0 bond0	bout the services. Select a slot and pr Nonsecure Port △ 80 7578 5120 5122	ess "Modify" button to modify the : <u>Secure Port</u> △ 443 7582 5124 5126	Timeout 3 1800 1800 N/A N/A	Maximum Sessions △ 20 2 4 4	Number of Services: 7 Active Sessions <u>View</u> <u>View</u> <u>View</u> <u>View</u>
8elow is a list # → 1 2 3 4 5	of services running on the Service Name web kvm cd-media fd-media hd-media	BMC. It shows current status Current State Active Active Active Active Active Active	s and other basic information a Interfaces $\ \ \Delta$ bond0 bond0 bond0 bond0 bond0 bond0	Nonsecure Port ∆ 80 7578 5120 5122 5123 5123	Secure Port △ 443 7582 5124 5126 5127	Timeout Δ 1800 1800 N/A N/A N/A	Maximum Sessions → 20 2 4 4 4	Number of Services: 7 Active Sessions View View View View View
8elow is a list # → 1 2 3 4 5 6	of services running on the Service Name (2) Web kvm cd-media fd-media hd-media ssh	BMC. It shows current statu: Current State Active Active Active Active Active Active Active	s and other basic information a Interfaces -3 bond0 bond0 bond0 bond0 bond0 bond0 N/A	Nonsecure Port Δ 80 7578 5120 5122 5123 N/A	Secure Port (2) 443 7582 5124 5126 5127 22	Timeout -3 1800 N/A N/A N/A 600	Maximum Sessions → 20 2 4 4 4 4 N/A	Number of Services: 7 Active Sessions View View View View View View View View

Figure 43. 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).

Thinks	Server Man	agement Module								Lenovo
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update		🕯 lenovo (Administrator) С	Refresh 🕏 Print PLogout HELP
Services	5									
Below is a list	of services ru	inning on the BMC. It	shows current statu	s and other basic informa	ation about the services. Select	t a slot and press "M	odify" button to modify th	e services configura	tion.	Number of Conders 7
# A	Service N	Active Session	- Web						×	
2	web kvm								Number of Sessions: 1	
3	cd-me	# 스	Session ID 🔺	Session Type 🔺	IP Address	User II) ()	User Name 🔺	User Privillege 🔺	
4	fd-me		3*	HIPS	192.168.36.32	1		lenovo	Administrator	
5	hd-me								Terminate Cancel	
6	ssh								- Cancer	
7	telne	et	Inactive	N/A	23		N/A	600	N/A	View

Figure 44. 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.

Think	Server Mana	gement Module							Lenovo
ashboard	System	Server Health Configura	ion Remote Control	Auto Video Recording	Maintenance	Firmware Update		• lenovo (Administrator)	CRefresh Print PLo
arvice									
low is a list	of services rui	nning on the BMC. It shows curre	it status and other basic inf	formation about the services. S	elect a slot and pre	ess "Modify" button to modify the services	configuration.		
								X	Number of Service
		Modify Service							Active Sessions
1		Service Name		kv	m				View
	od-me	Current State			Active				View
4	fd-me	Interfaces		bo	ndû				View
	hd-me	Nonsecure Port		75	70				View
	teini	Segure Port		75	00				View
8	sóls	Secure Port		/5	82				View
		Timeout		18	00 second	s			
		Maximum Sessions		2					Modif
							Γ	Modify Cancel	
								Houry Calleer	

Figure 45. 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.
- Active Sessions: To view the current active 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.

1 Think	Server Man	agement Module			Lenovo			
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	→ Ienovo (Administrator) CRefresh SPrint →Logoul HELI
Interfac	es							
This page is u	sed to control	I the interface of dev	ice.					
KCS			🗹 En	able				
IPMI NET	WORK		🗹 En	able				
WSMAN	нттр		🗹 En	able				
WSMAN	HTTPS		🗹 En	able				
								Save

Figure 46. 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.

🔁 Think	Server Man	agement Module						Lenovo
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	Ienovo (Administrator) C Refresh ØPrint ■Logout HELP
CMTD								
SWIP								9
Manage SMTP	settings of the	e device.						
LAN Cha	nnel Number		1 -					
Sender A	ddress							
Machine	Name							
Primary SMTF	P Server		Fnablo					
Port			25					
Server A	ddress							
E SMT	P Server reg	iree Authentication						
User Nan	ne	mes Automucation						
Passwor	d							
. dasword								
Secondary SI	MTP Server							
SMTP Su	pport		Enable					
Port			25					
Server A	ddress							
SMT	P Server requ	ires Authentication	í .					
User Nan	ne							

Figure 47. 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.

🔁 Think	kServer Mar	nagement Module		Leno	VO.					
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 lenovo (Administra	tor) CRefresh 🕏Print	Logout HELP
SNMP										
Use the page	to configure v	arious SNMP agent s	ettings.							
SNMP v1	1/v2 Configur	ation	Enable							
Commun	nity String(ro)								
Commun	nity String(rw	()								
										Save



The fields of SNMP Settings Page are explained below.

- **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. A sample screenshot of SSL Certificate Configuration Page is shown below.

ThinkSe	erver Mana	gement Module						Lenov	D.
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 lenovo (Administrator) 🔍 Refresh 🖓 Print 🖃 t	ogout HELP
SSL									
This page is used certificate based	d to configure on configure	e SSL certificate int ation details. View S	o the BMC. Using thi SL option is used to	is, the device can be ac view the uploaded SSL	ccessed in a secured mode. Up certificate in readable format.	load SSL option is u	sed to upload the certifica	ate and private key file into the BMC. Generate SSL option is used to generate the S	iL
Upload S	SSL	Generate SSL	View S	SSL					
Current	Certificate	1	Thu Jan 1 08:00:0	00 1970					
New Cert	tificate		瀏覽 未選擇檔	當案。					
Current F	Private Key		Thu Jan 1 08:00:0	00 1970					
New Priv	ate Key		瀏覽」未選擇檔	黨案。					
								Upload	

Figure 49. SSL Certificate Configuration – Upload SSL Page

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.

- **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 Privacy 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.

Think	(Server Man	agement Module							Lenovo
									🔹 lenovo (Administrator) 📿 Refresh 🕏 Print 🔤 Logou
Dashboard	System	Server Health	Configu	ration Ren	note Control	Auto Video Recording	Maintenance	Firmware Update	HEL
SSL									
This page is u	sed to configu	re SSL certificate in	to the BMC.	Using this, the d	evice can be ac	cessed in a secured mode. Up	load SSL option is us	ed to upload the certification	ate and private key file into the BMC. Generate SSL option is used to generate the SSL
certificate bas	sed on configu	ration details. View §	SSL option is	s used to view the	e uploaded SSL	centricate in readable format.			
Upload	d SSL	Generate SSL		View SSL					
Comm	on Name(CN)	<u>ا</u>							
Organ	ization(O)								
Organi	ization Unit(C)U)							
City or	r Locality(L)								
State	or Province(S	T							
Count	ry(C)								
Email	Address								
Valid fo	or			days					
Key Le	ength		512 -	bits					
									Generate

Figure 50. SSL Certificate Configuration – Generate SSL Page

This tab is used to generate the SSL certificate using the configuration.

- **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.

ThinkServer Management Module		Lenovo
Dashboard System Server Health Co	المعادية المعامية الم Configuration Remote Control Auto Video Recording Maintenance Firmware Update	Refresh 🏶 Print 📕 Logout HELP
SSL		A
This page is used to configure SSL certificate into the certificate based on configuration details. View SSL o	he BMC. Using this, the device can be accessed in a secured mode. Upload SSL option is used to upload the certificate and private key file into the BMC. Generate SSL option is option is used to view the uploaded SSL certificate in readable format.	used to generate the SSL
Upload SSL Generate SSL	View SSL	
Basic Information		
Version	1	
Serial Number	A3724F40D4322BD7	
Signature Algorithm	she256WithRSAEncryption	
Public Key		
Issued From		
Common Name(CN)	AMI	
Organization(O)	American Megatrends Inc	
Organization Unit(OU)	Service Processors	
City or Locality(L)	Atlanta	
State or Province(ST)	Georgia	
Country(C)	US	
Email Address	support@ami.com	
Validity Information		
Valid From	Jul 15 09:45:22 2016 GMT	

Figure 51. Certificate Configuration – View SSL Page

This tab is used to view the uploaded SSL certificate in user readable format.

- **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.

🔁 Think	Server Man	agement Module						Lenovo	
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	€ lenovo Firmware Update) (Administrator) ⊂ Refresh 🔗Print 👘 Log H	jout ELP
System	Firewal	I							_
Use this page select it in the	to configure S list and click '	System Firewall settin "Delete" button.	gs. Click "Advanced	Settings" button to con	figure the advanced settings o	f system firewall. To	add a new entry, click "Add" button. To delete a	Advanced Setting	5
IP Add	ress	Port							
								Configured IP rule count: 0	
	# △				IP/IP Range 🛆			IP Settings ⊥	
					Data Not A	vailable			
								Add Delete	-

Figure 52. 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.

Advanced Firewall Settings	X
Status Biock All Flush All	None Enable
	Save Cancel

Figure 53. 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.

Add new rule for IP	×
IP/IP Range IP Settings	
	Save Cancel

Figure 54. 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.
 - 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
 - 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.

1 Think	Server Man	agement Module							Lenovo	D .
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	↓ lenovo (Administr	stor) ⊂Refresh �Print ⊮Log H	gout IELP
System	Firewal									_
Use this page button.	to configure S	System Firewall setti	ngs. Click "Advanced	I settings" button to co	nfigure the advanced settings	of system firewall.	To add a new entry, click "Add" bu	utton. To delete a entry, select it in the list and click "Delete"	Advanced Setting	IS
IP Add	ress	Port								
									Configured Port rule count: (0
	# A		Protocol	7	Network Type 🔺		Port/Port F	Range 4	Port Settings →	
	Data Not Available									
									Add Delete	ī

Figure 55. 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.
- **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.

Add new rule for Port	E
Port/Port Range	
Protocol Network Type	
Port Settings	
	Save Cancel

Figure 56. 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.

ThinkServer Management Module

Lenovo

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

Users

The list below shows the current list of available users. To delete or modify a user, select the user name from the list and click "Delete User" or "Modify User". To add a new user, select an unconfigured slot and click "Add User"

Number of configured users:		Number	of	configured	users:	1
-----------------------------	--	--------	----	------------	--------	---

UserID 🔺	Username 🔺	User Access 🔺	Network Privilege 🔺	SNMP Status 🔺	Email ID 🔺
1	lenovo	Enabled	Administrator	Disabled	~
2	~	~	~	~	~
3	~	~	~	~	~
4	~	~	~	~	~
5	~	~	~	~	~
6	~	~	~	~	~
7	~	~	**	ne -	~
8	~	~	~	~	~
9	~	~	~	~	~
10	~	~	~	~	~

Add User Modify User Delete User

Figure 57. 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.

Add User		X
Username		
Password Size	● 16 Bytes ◯ 20 Bytes	
Password		
Confirm Password		
User Access		
Network Privilege	Administrator 🗸	
Extended Privileges	KVM VMedia	
SNMP Status		
SNMP Access	Read Only 🗸	
Authentication Protocol	SHA 🗸	
Privacy Protocol	DES 🗸	
Email ID		
Email Format	AMI-Format V	
New SSH Key	Browse	
		Add Cancel

Figure 58. 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.

Modify User		
Username	lenovo	
	Change Password	
Password Size	16 Bytes 20 Bytes	
Password		
Confirm Password		
User Access	✓ Enable	
Network Privilege	Administrator 🗸	
Extended Privileges	KVM 🗹 VMedia	
SNMP Status	Enable	
SNMP Access	Read Only 🗸	
Authentication Protocol	SHA 🗸	
Privacy Protocol	DES 🗸	
Email ID		
Email Format	AMI-Format 🗸	
Uploaded SSH Key	Not Available	
New SSH Key	Browse	

Figure 59. 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.

Think	Server Man	agement Module						Lenovo.
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	∔lenovo (Administrator) ⊂ Refresh ©Print PLogout HELP
Virtual N	Media							
The following o	option will allow	w to configure virtual	media devices. Belo	w, you can select the nu	mber of instances that are be s	supported for each ty	pe of virtual media device	S
Floppy de	evices		1 -					
CD/DVD	devices		1 -					
Hard dis	k devices		1 -					
Power Sa	ave Mode		Enable					
								Save Reset

Figure 60. 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.

ThinkServer Management Module	·	Lenovo.
Dashboard System Server Health	Configuration Remote Control Auto Video Recording Maintenance	Ienove (Administrator) ⊂ Refresh ●Print = Logout Firmware Update HELF
Cipher Suites		
This page is used to control the cipher suite.		
Enable A	Groups $ ightarrow$	Enable Status ム
V	Strong IPMI cipher suites(CS3, CS17)	C\$3 C\$17
	Weak IPMI cipher suites(CS1, CS2, CS6, CS7, CS8, CS11, CS12, CS15, CS16)	
		Save

Figure 61. 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.

ThinkServer Management Module							lenovo		
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	è albert (Administrator) ⊂ Refresh 🕏 Print 🚽 Logout HELP	
				Console Redirection	1				
				Server Power Contr	ol				
				Java SOL					



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.

ThinkServer Management Module	Lenovo		
Dashboard System Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update	ilenovo (Administrator) ⊂ Refresh Print = Logout HELP		
Console Redirection			
Press the button to launch the redirection console and manage the sener remotely.			

Java Console

Figure 63. 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.

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. <u>https://www.java.com/en/download/help/plugin_cache.xml</u> 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.

ocation		
Select the location where temporary files a	re kept:	
C:\Users\khs\AppData\LocalLow\Sun\Java	\Deployment\cache	Change
Disk Space		
Select the compression level for JAR files:	None	•
Set the amount of disk space for storing te	mporary files:	
	-0	32768 💠 MB
	and a	

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

Delete Files and Applications
Delete the following files?
Trace and Log Files
Cached Applications and Applets
Installed Applications and Applets
OK Cancel

- 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 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.

🔯 IPMI Command Dialog	×
Hexadecimal	ASCII
	J
Command :	
llovadasimal	4501
hexadecimai	ASCII
	Send Clear

Figure 64. 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.

😼 Virtual Media				×
Floppy Key Media : I				
Floppy Image			Browse	Connect Floppy
CD/DVD Media : I				
CD Image			Browse	Connect CD/DVD
Hard disk/USB Key Media	I 🖲 PhysicalDrive 🔾 Log	icalDrive		=
HD/USB Image		•	Browse	Connect Hard disk/USB Key
Status				
Target Drive	Connected To	Rea	id Bytes	
Virtual Floppy	Not Connected	n/a		
Virtual CD/DVD Virtual Hard Disk	Not Connected Not Connected	n/a n/a		Close
evice redirection not possi	ble due to insufficient permis	ssion. Launch	Application as A	Administrator

Figure 65. 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.

😼 Video Record	×
Video Length 20 Seconds	
Video to be Saved	
	Browse
Vormalized video resolution to 1024 ¥ 769	ОК
This might reduce the video quality!	Cancel
the mgn reader are theo quarty.	

Figure 66. 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.
X	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.
8	This quick button is used to record the video.
	This quick button displays the available hotkeys.
50 100 150	Drag this to zoom in or out.
1	Active Users
	This quick button is used to lock or unlock the local host display.
25	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 67. 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



Java SOL

Figure 68. Java SOL Page

This page allows you to launch the Java SOL. 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.

٩	×
BMC IP :	
Username :	
Password :	
Volatile-Bit-Rate :	9.6K 🗨
Non-Volatile-Bit-Rate :	9.6К 👻
	Connect Cancel

Figure 69. 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.

ThinkServer Management Module		Lenovo
Dashboard System Server Health Configuration	Remote Control Auto Video Recording	Ienovo (Administrator) CRefresh OPrint Zlogo Maintenance Firmware Update HE
Triggers Configuration	Triggers Configuration Recorded Video	
This page allows the user to configure the events that will trigger the an	uto video recording function of the KVM server	
Temperature/Voltage Critical Events		Temperature/Voltage Non Critical Events
Temperature/Voltage Non Recoverable Events		☐ Fan state changed Events
Watchdog Timer Events		Chassis Power on Event
Chassis Power off Event		Chassis Reset Event
Particular Date and Time Event		
Date: May ~ 29 ~	2016 🗸	LPC Reset Event
Time: (hh:mm:ss) 00 51 58		

Save Reset

Figure 70. 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.

- **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 postevent 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.



Play Video Download Delete

Figure 71. 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:

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

Advanced Remote Video Settings			X
Remote Video Support	Enable		
Maximum Duration(Sec)	20		
Maximum Size(MB)	5		
Maximum Dumps	2		
Server Address			
Source Path			
Share Type	NFS ~		
Username			
Password			
Domain Name			
		Save	Cancel

Figure 72. Advanced Remote Video Settings

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.

• **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 the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/ Firmware Upgrade configuration, open Preserve Configuration page, click **Maintenance Group > Preserve Configuration** from the menu bar. A sample screenshot of Preserve Configuration page is shown below.

Think	Server Manag	gement Module							Lenovo.
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	🕯 lenovo (Administrator) – C Re	sfresh �Print ■Logout HELI
Preserve	e Configu	uration							
This page allo	ws you to seled	ct the specific confi	guration items to be	preserved in the case	s of "Restore Configuration", a	and "Firmware Upda	ate without Preserve Configuration option	۳.	
Click here to	go to <u>Firmwar</u>	<u>e Update or Resto</u>	re Configuration					Num	her of Dreserved Items: 0
#	Δ			Preser	ve Configuration Item 🗅			Preserve Status	for or reserved items. V
1					SDR				
					IDMI				
					Network				
5					NTP				
6					SNMP				
7					SSH				
8					KVM				
9					Authentication				
								Check All Uncheck All	Save Reset



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.

HinkServer Management Module		Lenovo
zebboard Svetom Sonvor Hoalth (Configuration Domete Control Auto Video Decording Maintonanco Eirmuvaro Indato	€ lenovo (Administrator) ⊂ Refresh ØPrint = Log
shourd System Server nearth C		
estore Configuration		
s page allows you to restore the default configu	rration for your device. You can select specific configuration items to be preserved by clicking "Enter Preserve Configura	tion". Upon "Restore Configuration", the selected configuration items will be preserved while all the other
figuration items will be restored to their default	values. If none are selected, all the configuration items will be restored to their default values, essentially restoring the	device configuration to its factory defaults
	trades, in fore are serviced, an are comparation terms will be restored to area default values, essentially restoring are	device configuration to its racioly defaults.
WARNING: Please note that once you enter rest	tore configuration, widgets, other web pages and services will not work. All open widgets will be closed automatically. T	The device will reset and reboot within few minutes.
WARNING: Please note that once you enter res	tore configuration, while do called a set of an and services will not work. All open widgets will be closed automatically. To be a set of a service set of the set of	The device will reset and reboot within few minutes.
JARNING: Please note that once you enter res section lists the configuration items, that will t # م	tables many and protecting with the comparation terms must be closed to the central rates, costmany forcemany in tare configuration, widgets, other web pages and services will not work. All open widgets will be closed automatically. The be preserved during restore configuration. Click "Preserve Configuration" to modify the preserve configuration items. Preserve Configuration items.	Preserve Status
VARNING: Please note that once you enter res section lists the configuration items, that will i 罪 ム	tore configuration, widgets, other web pages and services will not work. All open widgets will be closed automatically. T be preserved during restore configuration. Click "Preserve Configuration" to modify the preserve configuration items. Preserve Configuration Item SDR	Preserve Status ⊥ Preserve Status ⊥ Preserve Status ⊥
WARNING: Please note that once you enter res section lists the configuration items, that will I #1 2	tore configuration, widgets, other web pages and services will not work. All open widgets will be closed automatically. 1 be preserved during restore configuration. Click "Preserve Configuration" to modify the preserve configuration items. Preserve Configuration Item	Preserve Preserve Preserve Preserve Preserve
WARNING: Please note that once you enter res is section lists the configuration items, that will i #1 2 3	tore configuration, widgets, other web pages and services will not work. All open widgets will be closed automatically. T be preserved during restore configuration. Click "Preserve Configuration" to modify the preserve configuration items. Preserve Configuration Item	Preserve Preserve
WARNING: Please note that once you enter res is section lists the configuration items, that will it #	tore configuration, widgets, other web pages and services will not work. All open widgets will be dosed automatically " be preserved during restore configuration. Click "Preserve Configuration" to modify the preserve configuration items. Preserve Configuration Item SOR SEL IPMI SSH	Preserve Preserve Preserve Preserve Preserve Preserve Preserve Preserve

Enter Preserve Configuration Restore Configuration

Figure 74. 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,

ThinkServer Management Module	Lenovo
Dashboard System Server Health Configuration Remote Control Auto Video Recording Maintenance	• Ienovo (Administrator) ⊂ Refresh ♥Print ●Logou Firmware Update HEL
Firmware Update	Firmware Update BIOS Lindate
Upgrade firmware of the device.Press 'Enter Update Mode ' to put the device in update mode.	Protocol Configuration
The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose 'Protocol Configur Protocol Type : HTTP/HTTPs	ation' under Firmware Update menu.
WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets the firmware upgrade process is a crucial operation. Please do not power off system and keen the connection.	will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset.

Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below All configuration items below will be preserved as default during the restore configuration operation. Click * Enter Preserve Configuration * to modify the Preserve status settings.

# A	Preserve Configuration Item 🔺	Preserve Status △
1	SDR	Overwrite
2	SEL	Overwrite
3	IPMI	Overwrite
4	Network	Overwrite
5	NTP	Overwrite
6	SNMP	Overwrite
7	SSH	Overwrite
8	KVM	Overwrite
9	Authentication	Overwrite

Enter Preserve Configuration Enter Update Mode



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.

ThinkServer Management Module		Lenovo
		🕯 Jenovo (Administrator) - C.Refresh - 🐼 Print - 💽 Logou
ashboard System Server Health (Configuration Remote Control Auto Video Recording Maintenance Firmware Update	HEL
Firmware Update		
Jpgrade firmware of the device.Press ' Enter Upda	ate Mode ' to put the device in update mode.	
The protocol information to be used for firmware Protocol Type : HTTP/HTTPs	e image transfer during this update is as follows. To configure, choose 'Protocol Configuration' under Firmware	Update menu.
WARNING: Please note that after entering the upd. The firmware upgrade process is a crucial operat	ale mode, the widgets, other web pages and services will not work. All the open widgets will be automatically d ion. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as preserv	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. Will be restart. s/overwritte in the table below.
VARNING: Please note that after entering the upd. The firmware upgrade process is a crucial operat Preserve all Configuration. This will preserve I configuration items below will be preserved as o	ate mode, the widgets, other web pages and services will not work. All the open widgets will be automatically d fore. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as preserv default during the restore configuration operation. Click * Enter Preserve Configuration * to modify the Preserve S	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. Will be restart. a/overwrite in the table below. atus settings.
WARNING: Please note that after entering the upd. he firmware upgrade process is a crucial operat Preserve all Configuration. This will preserve at configuration items below will be preserved as of #	The mode, the widgets, other web pages and services will not work. All the open widgets will be automatically of tion. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as preserv detault during the restore configuration operation. Click "Enter Preserve Configuration " to modify the Preserve S Preserve Configuration fitem SDR	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset, will be restart. a/overwrite in the table below. atus settings. <u>Preserve Status </u> Overwrite
ARNING: Please note that after entering the upd the firmware upgrade process is a crucial operat Preserve all Configuration. This will preserve configuration items below will be preserved as of #1 2	tate mode, the widgets, other web pages and senices will not work. All the open widgets will be automatically of ton. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as preserv default during the restore configuration operation. Click "Enter Preserve Configuration * to modify the Preserve S Preserve Configuration film SDR SPL	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart. aloverwrite in the table below. alus settings. <u>Preserve Status</u> <u>Overwrite</u>
ARNING: Please note that after entering the upd. e firmware upgrade process is a crucial operat Preserve all Configuration. This will preserve a configuration items below will be preserved as (#	tale mode, the widgets, other web pages and services will not work. All the open widgets will be automatically d for. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as presen default during the restore configuration operation. Click * Enter Preserve Configuration * to modify the Preserve S Preserve Configuration Item SCR SEL 	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart. af/overwrite in the table below. atus settings. Preserve Status Overwrite Overwrite
ARNING: Please note that after entering the upd. he firmware upgrade process is a crucial operat Preserve all Configuration. This will preserve configuration items below will be preserved as of 1 2 3 4	late mode, the widgets, other web pages and services will not work. All the open widgets will be automatically of ion. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as presen- default during the restore configuration operation. Click " Enter Preserve Configuration * to modify the Preserve S Preserve Configuration Item SDR SEL IPINI Network	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart. s/overwrite in the table below. alus settings. Preserve Status (Constraint) Overwrite Overwrite
ARNING: Please note that after entering the upd he firmware upgrade process is a crucial operat "Preserve all Configuration. This will preserve configuration items below will be preserved as	late mode, the widgets, other web pages and senices will not work. All the open widgets will be automatically of ton. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as presen- default during the restore configuration operation. Click "Enter Preserve Configuration * to modify the Preserve S Preserve Configuration Item △ SDR SEL IPMI Network NTP	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart. aloverwrite in the table below. alus settings. Preserve Status Overwrite Overwrite Overwrite
ARNING: Please note that after entering the upd he firmware upgrade process is a crucial operat I Preserve all Configuration. This will preserve a configuration items below will be preserved as #	late mode, the widgets, other web pages and services will not work. All the open widgets will be automatically d fore. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as preserve default during the restore configuration operation. Click "Enter Preserve Configuration * to modify the Preserve Preserve Configuration Item → SDR SEL IPMI Network NTP SNMP	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart. alsoverwrite in the table below. also settings. Preserve Status Overwrite Overwrite Overwrite Overwrite
ARNING: Please note that after entering the upd he firmware upgrade process is a crucial operat or figuration. This will preserve configuration items below will be preserved as 1 2 3 4 5 6 7	late mode, the widgets, other web pages and services will not work. All the open widgets will be automatically of for. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as presen- default during the restore configuration operation. Click "Enter Preserve Configuration * to modify the Preserve S Preserve Configuration Item	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart. z/overwrite in the table below: atus settings:
VARNING: Please note that after entering the und the firmware upgrade process is a crucial operat Preserve all Configuration. This will preserve il configuration items below will be preserved as 1 2 3 4 4 5 6 7 8	late mode, the widgets, other web pages and senices will not work. All the open widgets will be automatically of ton. Please do not power off system and keep the connection. If click previous page button in process, the BMC all the configuration settings during the firmware update - irrespective of the individual items marked as presen- default during the restore configuration operation. Click "Enter Preserve Configuration * to modify the Preserve S Preserve Configuration Item	sed. If the upgradation is cancelled in the middle of the wizard, the device will be reset. will be restart.

Enter Preserve Configuration Enter Update Mode

Figure 76. 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

ThinkServer Management Module	Lenovo
Dashboard System Server Bestth Configuration Benote Control Auto Video Recording Maintenance Firmware Didate	lenovo (Administrator)
Firmware Update	
Upgrade firmware of the device.Press " Enter Update Mode " to put the device in update mode.	
The protocol information to be used for firmware image transfer during this update is as follows. To configure, choose 'Protocol Configuration' under Firmware Update menu. Protocol Type : HTTP/HTTPs	
WARNING: Please note that after entering the update mode: the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the The firmware upgrade process is a crucial operation. Please do Not power off system and keep the connection.	e middle of the wizard, the device will be reset.
© Closing all active client requests.	
Preparing device for immore upgrade.	
Verifying firmware image.	
Finshing firmware image.	

Figure 77. 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.**

Upload Firmware		
Please select the firmware image to flash		
	Browse	
		Upload Cancel

Figure 78. Upload BMC Image Page

- 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.



Start Updating BIOS



• 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

	ThinkServer Management Module	Lenovo
Dasht	ooserd System Server Health Configuration Remote Control Auto Video Recording Maintenance Firmware Update	Ienovo (Administrator) HELP
BIO	IS Update	
Upgra W.	de BIOS of the host. Press "Start Updating BIOS" to start the BIOS update procedure. ARNING: Please note that after entering update mode widgets, all open widgets will be closed automatically. Please do Not power off system and keep the connection. Preserve BIOS Configuration Microarchine Configuration Mi	Start Uredating BIOS
	Figure 80. Start Updating BIOS Page	
2. 3. 4. 5.	Closing all active client requests Preparing Device for Firmware Upgrade Uploading Firmware Image Browse and select the Firmware image to flash and click Upload.	

Upload BIOS Image	
Please select the BIOS image to flash Browse	
	Upload Cancel



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

Protocol Configuration

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

ThinkServer Management Module						Lenovo				
Dashboard	System	Server Health	Configuration	Remote Control	Auto Video Recording	Maintenance	Firmware Update	• lenovo (Administrato	r) CRefresh 🌮rin	t PLogout HELP
Protoco	I Config		vare image protocol i	nformation						
Protocol Server A	Type ddress	HTTP/HTTPs	•							
Image Na Retry Co	ame ount	0								
									Save	Reset

Figure 82. 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".
 - 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.

Chapter 6. User Privilege

		Access	Operate
Dashboard		A,O,U,OEM	А
Sustam	Inventory	A,O,U,OEM	A,O,U,OEM
System	FRU Information	A,O,U,OEM	A,O,U,OEM
	Sensor Readings	A,O,U,OEM	A,O,OEM
Server Health	Event Log	A,O,U,OEM	A,OEM
	BSOD Screen	A,OEM	A,OEM
	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
Configuration	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
	Console Redirection	A,O,U,OEM	А
Remote Control	Server Power Control	A,O,U,OEM	A,OEM
	Java SOL	A,O,U,OEM	А
Auto Video Pocording	Triggers Configuration	A,O,OEM	A,OEM
Auto video Recording	Recorded Video	A,O,U,OEM	A,OEM
Maintonanco	Preserve Configuration	A,O,U,OEM	A,OEM
	Restore Configuration	A,OEM	A,OEM
	Firmware Update	A,OEM	A,OEM
Firmware Update	BIOS Update	A,OEM	A,OEM
	Protocol Configuration	A,OEM	A,OEM

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

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.