User Guide

ThinkStation BMC remote management console

Second Edition (June 2025)

Contents

About this guide

Before starting your tour, please read the following information:

- Use this information to understand the notices that are used in this document.

  Note: These notices provide important tips, guidance, or advice.

  Warning: These notices provide information or advice that might help you avoid inconvenient or problem situations.

  Attention: These notices indicate potential damage to programs, devices, or data. An attention notice is placed just before the instruction or situation in which damage might occur.
- Illustrations and user interface instructions in this documentation might look different from your product.
- Documentation content is subject to change without notice. To get the latest documentation, go to https://support.lenovo.com/docs/bmc_web_guide

Chapter 1. Introduction

This document explains how to configure the BMC (baseboard management controller) card settings on the ThinkStation® BMC remote management console. The BMC remote management console works with UEFI (Unified Extensible Firmware Interface) BIOS (Basic Input/ Output System) to provide systems-management capability for ThinkStation computers.

The BMC remote management console is a new generation management controller for ThinkStation computers. It consolidates the service processor functionality, video controller, and remote presence capabilities into the BMC card installed on the ThinkStation computer system board. It provides the following functions:

- Choice of a dedicated or shared Ethernet connection for systems management (based on system support)
- Support for HTML5
- Remote configuration using BMC remote management console
- Capability for applications and tools to access the BMC management console either locally or remotely
- Enhanced remote-presence capabilities

Web browser requirements

ThinkStation BMC remote management console web interface supports one of the following web browsers:

- Chrome latest version
- Edge
- Firefox
- Safari (on MAC)

BMC management console standard level features

The following is a list of BMC management console standard level features:

- Monitor your computer
- Basic configurations
- Advanced configurations

BMC startup

It takes about 2-3 minutes for BMC to start up. During the startup period, different products might have different prompts. You can refer to each product's *User Guide* for details.

Note: If you install the BMC card by yourself, make sure it is compatible with your ThinkStation and follow the installation instructions provided in each product's *User Guide*. Additionally, you need to update the BIOS and EC firmware on your ThinkStation to the latest versions.

Chapter 2. Access the BMC remote management console web interface

This chapter describes the setting up network connection and login procedures.

Log in to the BMC remote management console web interface

1. Ensure that the BMC card is correctly installed in your ThinkStation computer, and the Ethernet cable is connected to the Ethernet connector on the BMC card.
2. Ensure that the management computer and host computers are in the same local area network.
3. Obtain the dynamic MAC IP address (eg: `10.176.7.`*xxx*) from either host BIOS or router port management interface.
4. Open the Web browser on the management computer and enter the login address (eg: `https://10.176.7.`*xxx*`/#login`) to enter the remote management console login interface.
5. For initial access, input your username (default: `admin`) and password (default: `admin` or `PASSWORD!@`) , and click **Sign me in** to enter the remote management console Web interface.

   Warning: Once you log in to the application, it is recommended not to use the following options:

   - Refresh button of the Web browser
   - Refresh menu of the Web browser
   - Back and Forward options of the Web browser
   - F5 on the keyboard
   - Backspace on the keyboard

   Notes:

   - Username must be a combination of 1 to 16 alpha-numeric characters and start with an alphabetical character. It is case-sensitive and special characters like '-'(hyphen), '_'(underscore), and '@'(at sign) are allowed.
   - When you log in using the username and password, you obtain full administrative rights. Password change is required after the first log in. The new password must have a minimum of 10 characters and contain characters from three of the following four categories:
     - English uppercase characters A-Z
     - English lowercase characters a-z
     - Digits 0-9
     - Special characters (!, $, #, %, etc.)
   - One-time password (OTP) mechanism is used to generate a temporary password. Click **Forgot Password** in the log-in page to generate OTP that will be sent to the previously configured e-mail ID. This temporary password will be valid for only 5 minutes.
   - Do not use the same usernames for various authentication methods like AD, LDAP, RADIUS, or IPMI since the privilege of one authentication method is overwritten by another authentication method when you log in and hence the correct privilege cannot be returned properly.
   - Do not use the same usernames for various channels in IPMI.
6. Set the Web browser to accept file download when prompted. Ensure that JavaScript and cookies are enabled for the login address.

Web interface introduction

After logging in successfully, the user information and quick buttons are displayed at the top and the configurable menu is displayed on the left of the interface. The table below provides the name of each quick button and its corresponding description:

Quick button name	Description
Message	Click to view the event log alert messages. Click the message to go to the Logs and Reports page.
Notification	Click to view the notification received.
Language	Click the drop-down list box to choose the language you prefer.
BIOS	Click to view the AMI Remote BIOS Setup. The required username and password are the same with those of the BMC Login.
Sync	Click to synchronize with the latest Sensor and Event Log updates.
Refresh	Click to reload the current page.
User	There are five kinds of privileges. • **Administrator**: All BMC commands are allowed. • **Operator**: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces. • **User**: Only valid commands are allowed. • **No Access**: Login access denied.
Sign out	Click to log out of the ThinkStation BMC GUI.
Help	Click the **Help** icon on each menu page to view more detailed descriptions.

The table below provides the name of each menu and its corresponding description:

Menu name	Description
Dashboard	Provide the overall information about the status of a device.
Sensor	Provide the relevant information of all sensors.
System Inventory	Provide the components' inventories of the device, including the details of system, processor, memory controller, baseboard, power, thermal, PCIE function and storage.
FRU Information	Provide the BMC's FRU device information.
Logs & Reports	• IPMI Event Log • Audit Log • Video Log • SOL Log • Captured BSOD • Capture Log • HW Diagnostic Log (Available for some ThinkStation products)

Menu name	Description
Views	• View SSL certificate • Existing Firewall Settings • Existing IP Rules • Existing Port Rules
Settings	• Date & Time • Active Directory • LDAP/E-Directory • RADIUS Settings • Log Settings • PAM Order Settings • Event Filters • Alert Policies • LAN Destinations • Services • SMTP Settings • SSL Settings • Security IP/User Block • Add Firewall Settings • Add New IP Rule • Add New Port Rule • User Management • IPMI Interfaces • Web Interface
Network Settings	• Network IP Settings • Network Bond Configuration • Network Link Configuration • DNS Configuration • Sideband Interface (NC-SI)
Video Recording	• Auto Video Trigger Settings • Auto Video Remote Storage • Auto Pre-event Video Recordings • SOL Trigger Settings • SOL Log Settings • SOL Configurations
Remote Control	• KVM Mouse Setting • Remote Session • Remote Control

Menu name	Description
Image Redirection	• Media Redirection General Settings • VMedia Instance Settings • Active Redirections • Local Images • Remote Images
Power Control	View and control the power of your computer.
Maintenance	• Backup Configuration • BMC Recovery • Firmware Image Location • Firmware Information • Firmware Update • Preserve Configuration • Restore Configuration • Restore Factory Defaults • System Administrator

Chapter 3. Monitor your computer

BMC helps you to view and monitor information for the computers that you are accessing.

Dashboard

The Dashboard page provides the overall information about the status of a device.

Function	Description
Firmware Information	Display the version and build time of the BMC firmware.
Network Information	Display the network details of the device. Click **Edit** to configure the network.
Remote Control	Click **Launch JViewer** to download a jviewer.jnlp file. Then, you can launch the Remote Control page by clicking the **jviewer.jnlp**. **Note:** Before you use this function, a JRE is needed to be installed and configured. Moreover, the BMC's IP is needed to add to the **Security' Exception Site List** in Java Control Panel to avoid the application being blocked by java security.
Sensor Monitoring	Display the sensors' information of the device. Click 🔍 to check the sensor details.
Event Log	Display the event logs of the device logged by BMC.

Sensor

The Sensor page provides the relevant information of all sensors. This page shows the live readings for all the available sensors with details like sensor name, status, current reading and behavior. Click on any sensor to show more information, including thresholds and a graphical representation of all associated events.

Sensor state	Description
Critical	Select a sensor from the critical sensors list to view more details such as sensor information and sensor events. Click **Change Thresholds** to configure threshold settings. **Notes:** • The threshold settings will be enabled only for administrator or operator privilege users. For other users, the threshold settings option will be disabled, and they can't access to perform this action. • The threshold value can only be changed if it has an initiate value. You cannot change a threshold value if its initial value is set to NA. • The modified threshold value will be restored to the default value after a BMC reset.
Normal	Select a sensor from the normal sensors list to view more details such as sensor information and sensor events. Click **Change Thresholds** to configure threshold settings. **Notes:** • The threshold settings will be enabled only for administrator or operator privilege users. For other users, the threshold settings option will be disabled, and they can't access to perform this action. • The threshold value can only be changed if it has an initiate value. You cannot change a threshold value if its initial value is set to NA. • The modified threshold value will be restored to the default value after a BMC reset.
Disabled	A list of disabled sensors is displayed.
Discrete Sensor States	Click **System Event Log** to view all the event entries for the selected sensor in a reverse chronological order. **Notes:** The typical state value of **System Event Log** is as follows: • 0x8000: Normal • 0x8004: SEL Log Area Reset/Cleared • 0x8010: SEL Full • 0x8020: SEL Almost Full, this event represents the SEL has reached a point of being 75% or more full.

System Inventory

The System Inventory page provides the inventory information of the host machine, including the details of System, Processor, Memory Controller, Baseboard, Power, Thermal, PCIE Function and Storage. Select any component to view the details of the component.

FRU Information

The FRU (Field Replaceable Unit) Information page displays product information for the BMC's FRU devices.

Field	Description
Available FRU Devices	Select a FRU Device ID from the drop-down list box to view the details of the device.
Product Information	Product information in details.

Chapter 4. Basic configurations

Logs and Reports

The Logs & Reports page enables you to view various event logs statistics and use different filter options to view those specific events. You also can clear or download the event logs.

Log type	Description
IPMI Event Log	Display the list of events incurred by different sensors on this device. Click on a record to see the details of that entry. Click the statistical graph to view the number of events by date. You can use the date range, sensor type, or sensor name filter options to view those specific events.
Audit Log	Display audit events for this device (if configured). **Note:** For configuration, go to **Settings → Log Settings → Advanced Log Settings**.
Video Log	Display available recorded video files (if the options have been configured). **Notes:** • For configuration, go to **Video Recording → Auto Video Trigger Settings**. • You can play or download the video only if file size is lesser than 40 MB. Browsers have various memory restrictions, due to this browser cannot store and process data greater than 40MB (approximately). If file size is greater than 40 MB, user will be notified with a message to use Java player Application.
SOL Log	Display the list of available recorded video files. **Notes:** • For configuration, go to **Video Recording → SOL Trigger Settings**. • By default, video files will be stored in the local path of the BMC. If the remote video support is enabled, then the video files will be stored only in the remote path, and not within the BMC.
Captured BSOD	Display a snapshot of the blue screen captured if the host system crashed since the last reboot. **Note:** KVM service should be enabled to display the BSOD screen. For KVM Service configuration, go to **Settings → Services → KVM**.
Captured Log	Download the logs captured by the BMC.
HW Diagnostic Log	Show and download the hardware diagnostic logs if host supports this feature.

Views

The Views page enables you to view the following information:

View content	Description
View SSL Certificate	View the basic information about the uploaded SSL certificate in readable format. • Certificate Version • Serial Number • Signature Algorithm • Public Key • Issuer Common Name (CN) • Issuer Organization(O) • Issuer Organization Unit (OU) • Issuer City or Locality(L) • Issuer State or Province (ST) • Issuer Country(C) • Issuer E-mail Address • Valid From • Valid Till
Existing Firewall Settings	Click the **Existing Firewall Settings** block to view the existing firewall settings details. If no firewall settings exist, click **Settings → Add Firewall Settings** to add a new firewall setting.
Existing IP Rules	Click the **Existing IP Rules** block to view the existing IP rules details. If no IP rules exist, click **Settings → Add New IP Rule** to add a new IP rule.
Existing Port Rules	Click the **Existing Port Rules** block to view the existing port rules details. If no port rules exist, click **Settings → Add New Port Rule** to add a new port rule. • **Port Single (or) Range Start**: To configure the port or range of port Addresses. • **Port Range End**: To configure the port or range of port addresses. • **Protocol**: This field specifies the protocols for the configured port or port ranges. • **Network Type**: This field specifies the affected network type for the particular port or port ranges. • **Enable Timeout**: To enable or disable firewall rules with timeout. • **Start Date**: The respective firewall rule effect will start from this time. • **Start Time**: The respective firewall rule will start from this time. • **End Date**: The respective firewall rule effect will end on this date. • **End Time**: The respective firewall rule will end at this time. • **Rule**: To indicate **Allow** or **Block** status. • **Delete**: To delete the entry to the firewall rules list.

Settings

The Settings page enables you to access various configuration settings.

Date & Time

Set the date and time on the BMC.

Settings name	Description
Configure Date & Time	Display time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.
Select Time Zone	Set the date and time on the BMC. **Note:** If the time zone is selected as **Manual Offset**, the map selection will be disabled. The time zone settings will be reflected only after saving the settings.
Automatic NTP Date & Time	Automatically synchronize date and time with the NTP Server. • **Primary NTP Server**: To configure a primary NTP server to use when automatically setting the date and time. • **Secondary NTP Server**: To configure a secondary NTP server to use when automatically setting the date and time. **Note:** The secondary NTP server is an optional field. If the primary NTP server is not working, then try the secondary NTP Server.
Automatic PTP Date & Time	Automatically synchronize date and time with the PTP Server.

Active Directory

Store information and data about networks and domains. 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.

Settings name	Description
Active Directory General Settings	To configure Active Directory General Settings: 1. Click **Active Directory General Settings** to open the Active Directory General Settings page. 2. Check or clear the **Enable Active directory Authentication** check box to enable or disable Active Directory Authentication respectively. 3. Specify the Secret username and password in the **Secret Username** and **Secret Password** fields respectively. **Notes:** • Secret username or password for AD is not mandatory. When secret username or password is empty, authentication fails will be always treated as invalid password error. For invalid password error, PAM will not try other authentication methods. It is recommended to keep AD in the last location in PAM order. • Username is a string of 1 to 64 alphanumeric characters. It must be case sensitive and start with an alphabetical character. Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed. • Password must be at least 6 characters long and no longer than 127 characters. Space is not allowed. 4. Specify the Domain Name for the user in the **User Domain Name** field. For example, `MyDomain.com`. 5. Configure IP addresses in **Domain Controller Server Address1**, **Domain Controller Server Address2**, and **Domain Controller Server Address3**. **Notes:** At least one Domain Controller Server Address must be configured. • IP Address is made of 4 numbers separated by dots as in "`xxx.xxx.xxx.xxx`". • Each number ranges from 0 to 255. • First number must not be 0. • Domain Controller Server Addresses will support IPv4 Address format and IPv6 Address format. 6. Click **Save** to save your settings and return to the Active Directory Settings page.
Active Directory Role Groups	Display any configured role groups and the available slots. You can modify, add or delete role groups. Group domain can be the AD domain or a trusted domain. Group name should correspond to the name of an actual AD group. **Notes:** • To view the page, you must be at least a user. • To modify or add a group, you must be an administrator. To add a new role group: 1. Select a role group and click on the blank area to open the Role Groups page.

Settings name	Description
	2. Enter the group name, group domain, and group privilege in corresponding fields. **Notes:** • Role group name is a string of 64 alpha-numeric characters. Special symbols such as hyphen and underscore are allowed. • Domain name is a string of 255 alpha-numeric characters. Special symbols such as hyphen, underscore, and dot are allowed. 3. Select **KVM Access** or **VMedia Access**. 4. Click **Save** to add the new role group and return to the **Role Group** list.

Note: For security reasons, the password policy of Active Directory needs to comply with the password rules of the BMC web.

LDAP/E-Directory

LDAP is an Internet protocol that ThinkStation BMC card can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate ThinkStation BMC card users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the ThinkStation BMC card. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

Settings name	Description
LDAP/E-Directory General Settings	To configure LDAP/E-Directory General Settings: 1. Click **Settings → LDAP/E-Directory → LDAP/E-Directory General Settings** to open the LDAP/E-Directory Settings page. 2. Check **Enable LDAP/E-Directory Authentication** to enable LDAP/E-Directory Settings. **Note:** During login prompt, use username to log in as an LDAP group member. 3. Select the encryption type for LDAP/E-Directory from the **Encryption Type**. **Note:** Configure proper port number when SSL is enabled. 4. Select the **Common Name Type** as **IP Address**. 5. Enter the IP address of LDAP server in the **Server Address** field. **Notes:** • IP Address is made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'. • Each number ranges from 0 to 255 and the first number must not be 0. • IPv4 and IPv6 address format is supported. • Configure FQDN address when using **StartTLS** with FQDN. 6. Specify the LDAP Port in the **Port** field. **Note:** The default port is 389. For SSL connections, the default port is 636. The port value ranges from 1 to 65535. 7. Specify the **Bind DN** that is used during bind operation, which authenticates the client to the server. **Notes:** • Bind DN is a string of 4 to 64 alpha-numeric characters, and it must start with an alphabetical character. • Special symbols like dot (.), comma (,), hyphen (-), underscore (_), and equal-to (=) are allowed. For example: `cn=manager`, `ou=login`, `dc=domain`, `dc=com`. 8. Enter the password in the **Password** field. **Notes:** • Password must be at least 1 character long and space is not allowed. • This field will not allow more than 48 characters. 9. Enter the **Search Base**. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directories. **Notes:** • Search base is a string of 4 to 63 alpha-numeric characters, and it must start with an alphabetical character. • Special symbols like dot (.), comma (,), hyphen (-), underscore (_), and equal-to (=) are allowed. For example: `ou=login`, `dc=domain`, `dc=com`.

Settings name	Description
	10. Select **Attribute of User Login** to find the LDAP/E-Directory server which attribute should be used to identify the user. **Note:** It only supports **cn** or **uid**. 11. Select **CA Certificate File** from the field to identify the certificate of the trusted CA certs. 12. Select the **Certificate File** to find the client certificate filename. 13. Select **Private Key** to find the client private key filename. **Note:** All the 3 files are required when **StartTLS** is enabled. 14. Click **Save** to save the settings.
LDAP/E-Directory Role Groups	To add a new role group: 1. Select a role group and click on the blank area to open the Role Groups page. 2. Enter the group name, group domain, and group privilege in corresponding fields. **Notes:** • Role group name is a string of 255 alpha-numeric characters. Special symbols such as hyphen and underscore are allowed. • Role group domain name is a string of 4 to 64 alpha-numeric characters, and it must start with an alphabetical character. • Special symbols like dot (.), comma (,), hyphen (-), underscore (_), and equal-to (=) are allowed. For example: `cn=manager`, `ou=login`, `dc=domain`, `dc=com`. 3. Select **KVM Access** or **VMedia Access**, or both. 4. Click **Save** to add the new role group and return to the **Role Group** list.

Note: For security reasons, the password policy of LDAP/E-Directory needs to comply with the password rules of the BMC web.

RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities. This menu is used to set the RADIUS Authentication.

Settings name	Description
RADIUS General Settings	To configure Radius: 1. Check **Enable RADIUS Authentication** to authenticate the RADIUS. 2. Enter the IP address of RADIUS server in **Server Address**. **Notes:** • IP Address (Both IPv4 and IPv6 format). • FQDN (Fully Qualified Domain Name) format. 3. Enter the RADIUS port number in **Port**. **Note:** The default port is 1812 and port value ranges from 1 to 65535. 4. Enter the authentication secret of RADIUS server in **Secret**. **Notes:** • This field will not allow more than 31 characters. • Secret must be at least 4 characters long and space is not allowed. 5. Select **KVM Access**, **VMedia Access**, or both. 6. Click **Save** to save the RADIUS General Settings.

RADIUS Advanced Settings	To configure the Radius Authorization:
	1. Check **Enable RADIUS Authentication** to enable the RADIUS to authenticate.
	2. Click **RADIUS Advanced Settings** to open the Radius Authorization window. For authorization purpose, configure the Radius user with Vendor Specific Attribute in Server side.
	Example 1:
	`test admin Auth-Type := PAP`
	`Cleartext-Password:=”admin”`
	`Auth-Type := PAP`
	`Vendor-Specific = “H=4”`
	Example 2:
	`test operator Auth-Type := PAP`
	`Cleartext-Password:=“operator”`
	`Auth-Type := PAP`
	`Vendor-Specific = “H=3”`
	If you change the Vendor-Specific value in server then you should change the same values in this page.
	3. Click **Save** to save the configurations.

Note: For security reasons, the password policy of RADIUS needs to comply with the password rules of the BMC web.

Log Settings

Display a list of system logs and audit logs occurred in this device.

Settings name	Description
SEL Log Settings Policy	To configure the log policy for the event log: • **Log Policy**: To enable or disable the **Linear Storage Policy** or **Circular Storage Policy**. • **Save**: To save the configured settings.
Advanced Log Settings	To configure the advanced log: 1. In the **Audit Log** field, check or clear the **Enable** option as desired. 2. Click **Save** to save the configurations.

PAM Order Settings

Configure the PAM ordering for user authentication into the BMC.

To configure PAM ordering:

1. Select the required PAM module and click and drag the required PAM module. It can be moved UP or DOWN to change its arrangement order.
2. Click **Save** to save the configurations.

Notes:

- It is recommended not to keep the same username for different PAM modules.
- If Authentication fails, the reason of failure could be invalid user or invalid password.
- If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So it is always treated as invalid username error and PAM will try other authentication methods.
- If AD contains secret username and password as empty, Authentication failures will be always treated as invalid password error. For invalid password error, PAM will not try other authentication methods. So, it is recommended to keep AD in the last location in PAM order.
- Whenever the configuration is modified, the web server will be restarted automatically. Logged-in session will be logged out.

Event Filters

Platform Event Filter (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. This menu contains pre-configured 40 events with PEF IDs.

To configure event filters:

1. Click the **Event Filters** section to configure the event filters in the available slots.
2. To add an event filter entry, select a free section to open the event filter entry page.

Settings name	Description
Enable this filter	Check this option to enable the PEF settings.
Event Severity to trigger	Select any one of the Event severities from the list.
Event Filter Action Alert	It is checked by default. This action enables PEF Alert action (read only).
Power Action	Select any option from the drop-down list box.

Settings name	Description
Alert Policy Group Number	Choose any one of the configured group numbers from the drop-down list box. **Note:** Alert Policy must be configured under **Settings → Alert Policy**.
Raw Data	Check this option to fill the Generator ID with raw data.
Generator ID 1	Used to give raw generator ID1 data value.
Generator ID 2	Used to give raw generator ID2 data value. **Note:** In **RAW Data** field, specify hexadecimal value prefix with '0x'.
Generator Type	Choose the event generator as Slave Address if event was generated from IPMB. Otherwise as System Software ID if event was generated from system software.
Slave Address/Software ID	Specify corresponding I2C Slave Address or System Software ID.
Channel Number	Choose the particular **Channel Number** that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
IPMB Device LUN	Choose the corresponding **IPMB Device LUN** if events generated by IPMB.
Sensor Type	Select the **Sensor Type** of sensor that will trigger the event filter action.
Sensor name	Choose the particular sensor from the sensor list.
Event Options	Choose **Event Options** to be either All Events or Sensor Specific Events.
Event Trigger	Used to give Event/Reading type value. **Note:** Value ranges from 1 to 255.
Event Data 1 AND Mask	Used to indicate wildcarded or compared bits. **Note:** Value ranges from 0 to 255.
Event Data 1 Compare 1 and Event Data 1 Compare 2	Used to indicate whether each bit position's comparison is an exact comparison or not. **Note:** Value ranges from 0 to 255.
Event Data 2 AND Mask	Similar to Event Data 1 AND Mask.
Event Data 2 Compare 1 and Event Data 2 Compare 2	Similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
Event Data 3 AND Mask	Similar to Event Data 1 AND Mask.
Event Data 3 Compare 1 and Event Data 3 Compare 2	Similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

3. Click **Save** to save the configurations and return to event filter list.
4. Click **Delete** to delete the existing filter.

Alert Policies

Configure the alert policy for the PEF configuration. You can add, delete or modify an entry in this page.

To configure alert policies:

1. Click the slot for which you must configure the alert policy. For example, if you have chosen Alert Policy Group Number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy page.
2. Select **Policy Group Number** from the drop-down list box.
3. Check **Enable this alert** to enable the policy settings.
4. Select any of the **Policy Action** from the drop-down list box.
5. Select a particular **LAN Channel** from the available channel list.
6. In the **Destination Selector** field, select a particular destination from the configured destination list.

   Note: LAN Destination must be configured under **Settings → LAN Destinations**. That is, if you select the number 4 for destination selector in Alert Policy Entry page, then you must configure the 4th slot (LAN Destination Number 4) in the LAN Destinations page.
7. Check **Event Specific Alert String**, if the Alert policy entry is Event Specific.
8. In the **Alert String Key** field, select any one value that is used to look up the Alert String to send for this Alert Policy entry.

   Note: Using Web UI, Alert strings cannot be configured but option for Event Specific alert strings can be enabled or disabled. There is an option to select only the alert string keys, but alert strings must be configured using IPMI Command (Set PEF Config Parameter as “Alert String”).
9. Click **Save** to save the new alert policy and return to Alert Policy list.
10. Click **Delete** to delete a configuration.

LAN Destinations

Used to configure the LAN Destination.

To configure LAN Destinations:

1. Select the number of slots to be configured. This should be the same number of slot that you have selected in the **Alert Policies → Destination Selector** field. That is, if you have selected the Destination Selector as 4, then you have to configure the 4th slot of LAN Destination page.
2. Select the slot for which you want to configure to open the LAN Destination entry.
3. In the **LAN Channel Number** field, the LAN Channel Number for the selected slot is displayed and this is a read only field.
4. In the **LAN Destination** field, the destination for the newly configured entry is displayed and this is a read only field.
5. In the **Destination Type** field, select the one of the types.
6. In the **SNMP Destination Address** field, enter the destination address.

   Note: If Destination type is E-mail Alert, then provide the e-mail address that will receive the e-mail.
7. If the destination type is Email alert, select the **BMC Username** from the list of users.

   Note: E-mail address should be configured under **Settings → User Management**.
8. In the **Email Subject** field, enter the subject.
9. In the **Email Message** field, enter the message.
10. Click **Save** to save the new LAN destination and return to LAN destination list.
11. Click ✉ in the LAN Destinations page to send sample alert to configured destination.

    Note: Test alert can be sent only with SMTP configuration is enabled. SMTP support can be enabled under **Settings → SMTP Settings**.

Services

Display the basic information about services running in the BMC. Only Administrator can modify the service.

Settings name	Description
Services	Display service name of the selected slot (read-only).
Status	Display the current status of the service, either active or inactive state.
Interfaces	Show the interface in which service is running.
Secure Port	Used to configure secure port number for the service. • Web default port is 443 • KVM default port is 443 • CD Media default port is 443 • HD Media default port is 443 • SSH default port is 22 **Note:** Telnet default port is 23 and does not support secure port. If single port feature is enabled, KVM, CD Media and HD Media ports cannot be edited. Port value ranges from 1 to 65535.
Timeout	Display the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value. **Notes:** • Web timeout value ranges from 300 to 1800 seconds. • KVM timeout value ranges from 300 to 1800 seconds. • SSH and Telnet timeout value ranges from 60 to 1800 seconds. • SSH and telnet service will be using the same timeout value. If you configure SSH timeout value, it will be applied to telnet service also and vice versa. • If KVM is launched, then the web session timeout will not take effect.
Maximum Sessions	Display the maximum number of allowed sessions for the service.
Active Sessions	View the current active sessions for the service.

To view the active sessions, click ≡ to view the details about the active sessions for the service in the Active Session page. Select a slot and click to terminate the particular session of the service.

Settings name	Description
Session ID	Display the ID of the active sessions.
Session Type	Display the type of the active sessions.
User ID	Display the ID of the user.
Username	Display the name of the user.
Client IP	Displays the IP addresses that are already configured for the active sessions.
Privilege	Display the access privilege of the user.

To modify the existing services:

1. Select a slot and click to modify the configuration of the service.

Note: Whenever the configuration is modified, the service will be restarted automatically. User must close the existing opened session for the service if needed.

2. The Service Configuration page is displayed. **Service Name** is a read only field.
3. Activate the current state by checking **Active**.

   Note: **Interfaces**, **Secure port**, **Timeout** and **Maximum Sessions** will not be active unless the current state is active.
4. Select any one of the available interfaces from the **Interface Name** drop-down list box.
5. Enter the Secure Port Number in the **Secure Port** field.
6. Enter the timeout value in the **Timeout** field.

   Note: The values in the **Maximum Sessions** field cannot be modified.
7. Click **Save** to save the changes and click **Cancel** to exit.

SMTP Settings

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks. Using ThinkStation BMC GUI, you can configure the SMTP settings of the device.

To configure SMTP settings:

1. Select the **LAN Interface** from the drop-down list box.
2. Enter the **Sender Email ID** in the specified field.
3. Check **Primary SMTP Support** to enable SMTP support for the BMC.
4. Enter the Machine Name of the SMTP Server in the **Primary Server Name** field.

   Note: Machine Name is a string of maximum 15 alpha-numeric characters. Space and special characters are not allowed.
5. Enter IP address of the SMTP Server in the **Primary Server IP** field. It is a mandatory field.
6. Enter the **Primary SMTP Port** in the specified field.
7. Enter the **Primary Secure SMTP Port** in the specified field.
8. Check **Primary SMTP Authentication** if you want to authenticate SMTP Server.
9. Enter your **Primary Username** and **Primary Password** in the respective fields.
10. Check **Primary SMTP SSLTLS Enable** to send data through secure Port.

    Note: If this option is selected, STARTTLS option and Normal Port will be hidden.
11. Check **Secondary SMTP Support** to enable Secondary SMTP support for the BMC.
12. Enter the **Secondary Server Name**, **Secondary Server IP**, **Secondary SMTP Port**, and **Secure Port** values in the respective fields.
13. Check **SMTP Server Authentication** if you want to authenticate SMTP Server.
14. Enter your **Secondary Username** and **Password** in the respective fields.
15. Check **Secondary SMTP SSLTLS** to send data through secure Port.

    Note: If this option is selected, STARTTLS option and Normal Port will be hidden.
16. Click **Save** to save the entered details.

SSL Settings

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.

Configure SSL certificate into the ThinkStation BMC so that the device can be accessed in a secured mode.

To Configure SSL certificate:

1. Generate SSL Certificate.

Settings name	Description
Common Name (CN)	Common name for which certificate is to be generated. • Maximum length of 64 characters. • It is a combined string of alpha-numeric characters. • Special characters '#' and '$' are not allowed.
Organization (O)	Organization name for which the certificate is to be generated. • Maximum length of 64 characters. • It is a combined string of alpha-numeric characters. • Special characters '#' and '$' are not allowed.
Organization Unit (OU)	Over all organization section unit name for which certificate is to be generated. • Maximum length of 64 characters. • It is a combined string of alpha-numeric characters. • Special characters '#' and '$' are not allowed.
City or Locality (L)	City or Locality of the organization (mandatory). • Maximum length of 128 characters. • It is a combined string of alpha-numeric characters. • Special characters '#' and '$' are not allowed.
State or Province (ST)	State or Province of the organization (mandatory). • Maximum length of 64 characters. • It is a combined string of alpha-numeric characters. • Special characters '#' and '$' are not allowed.
Country (C)	Country code of the organization (mandatory). • Only two characters are allowed. • Special characters are not allowed.
Email Address	E-mail address of the organization (mandatory)
Valid for	Validity of the certificate (Value ranges from 1 to 3650 days).
Key Length	The key length bit value of the certificate
Save	Click to generate the new SSL certificate. **Note:** HTTPs service will get restarted to use the newly generated SSL certificate.

2. Upload SSL Certificate. This option is used to upload the certificate and private key file into the BMC.

Settings name	Description
Current Certificate	Current certificate and uploaded date or time will be displayed (read-only).
New Certificate	Certificate file should be of pem type.
Current Private Key	Current Private key information will be displayed (read-only).
New Private Key	Private key file should be of pem type.
Upload	To upload the SSL certificate and privacy key into the BMC. **Note:** After successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

Note: If you'd like to use your own security certificate, you can upload your private key and certificate here. Private key and certificate must be in PEM format.

Security IP/User Block

To enable or disable the Security IP/User Block function.

Add Firewall Settings

Only administrators can add or delete a firewall.

To Add Firewall Settings:

1. Select **IPv4**, **IPv6**, or **Both** from the **Block All** drop-down list box to block the incoming IPs and ports you prefer.

   Note: Blocking All IPv4 will also block all Redfish requests from the BIOS, which may extend the system boot time.
2. Check **Flush All** to flush all the system firewall rules.
3. Check **Timeout** to enable firewall rules with timeout.
4. Enter **Start Time** to start the respective firewall rule effect from this time.
5. Enter **End Time** to end the respective firewall rule effect from this time.

   Note: The time should be in the "dd-mm-yy:hh-mm" format.
6. Click **Save** to save your configuration.

   Notes:

   - The parameters should be set as you needed. Otherwise, the interface might be blocked unexpectedly.
   - The timeout setting relies on the BMC's system time. Ensure the BMC's system time is properly synchronized to avoid issues.

Add New IP Rule

The firewall IP rule can be set for an IP or range of IP Addresses

To add an IP rule:

1. Enter an IP address or a range of IP addresses in the **IP Single or IP Range Start** field.

   Notes:

- IP Address will support IPv4 Address format only.
- IPv4 Address is made of 4 numbers separated by dots as in `xxx.xxx.xxx.xxx`.
- Each number ranges from 0 to 255.
- The first number must not be 0.
- IPv6 Address is made of 8 groups of 4 Hexadecimal digits separated by colon as in `xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx`.

2. Enter IP range end value in the **IP Range End** field.
3. Check **Timeout** to enable firewall rules with timeout.
4. Enter **Start Date** to start the respective firewall rule effect from this date.
5. Enter **End Date** to end the respective firewall rule effect from this date.
6. Enter **Start Time** to start the respective firewall rule effect from this time.
7. Enter **End Time** to end the respective firewall rule effect from this time.

   Note: The time should be in the dd-mm-yy:hh-mm format.
8. Select **Block** or **Allow** from the **Rule** drop-down list box.
9. Click **Save** to save your configuration.

Notes:

- If there are conflicting rules, the most recently defined rule takes precedence.
- The timeout setting relies on the BMC's system time. Ensure the BMC's system time is properly synchronized to avoid issues.

Add New Port Rule

The firewall Port rule can be set for a Port number or range of Port numbers.

To Add New Port Rule:

1. Enter the port number or a range of port numbers in the **Port Single** (or) **Range Start** field.

   Note: Port value ranges from 1 to 65535.
2. Enter the end value in the **Port Range End** field.
3. Select either **TCP**, **UDP**, or **Both** from the **Protocol** drop-down list box.
4. Select **IPv4** or **IPv6** or **Both** from the **Network Type** drop-down list box.
5. Check **Enable Timeout** to enable firewall rules with timeout.
6. Enter **Start Date** to start the respective firewall rule effect from this time.
7. Enter **Start Time** to start the respective firewall rule effect from this date.
8. Enter **End Date** to end the respective firewall rule effect on this date.
9. Enter **End Time** to end the respective firewall rule effect at this time.

   Note: The time should be in the YYYY/MM/DD:hh-mm format.
10. Select **Block** or **Allow** from the **Rule** drop-down list box.
11. Click **Save** to save your configuration.

Notes:

- If there are conflicting rules, the most recently defined rule takes precedence.

- The timeout setting relies on the BMC's system time. Ensure the BMC's system time is properly synchronized to avoid issues.

User Management

View the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To add a new user:

1. Select a free section and click on the blank area to open the Add User screen.
2. Enter the name of the user in the **Username** field.

   Notes:

   - Username is combined a string of 1 to 16 alpha-numeric characters.
   - It must start with an alphabetical character.
   - It is case-sensitive.
   - Special characters like '-'(hyphen), '_'(underscore), and '@'(at sign) are allowed. For 20 Bytes password, LAN session will not be established.
3. Select a password size from the **Password Size** drop-down list box for the new password.
4. In the **Password** and **Confirm Password** fields, enter and confirm your new password.

   Notes:

   - Password should be the combination of alphabets, numbers, symbol and upper-case characters. White space is not allowed.
   - This field will not allow more than 16/20 characters based on Password size field value.
   - This field will not allow the below mentioned characters.
   - The password should be a string, if you try to set password using "ipmitool user set password".

Hex	Char	Hex	Char
00	NUL '\0'	11	DC1 (device control 1)
01	SOH (start of heading)	12	DC2 (device control 2)
02	STX (start of text)	13	DC3 (device control 3)
03	ETX (end of text)	14	DC4 (device control 4)
04	EOT (end of transmission)	15	NAK (negative ack.)
05	ENQ (enquiry)	16	SYN (synchronous idle)
06	ACK (acknowledge)	17	ETB (end of trans. blk)
07	BEL '\a' (bell)	18	CAN (cancel)
08	BS '\b' (backspace)	19	EM (end of medium)
09	HT '\t' (horizontal tab)	1A	SUB (substitute)
0A	LF '\n' (new line)	1B	ESC (escape)
0B	VT '\v' (vertical tab)	1C	FS (file separator)
0C	FF '\f' (form feed)	1D	GS (group separator)
0D	CR '\r' (carriage ret)	1E	RS (record separator)

Hex	Char	Hex	Char
0E	SO (shift out)	1F	US (unit separator)
0F	SI (shift in)	20	SPACE
10	DLE (data link escape)	7F	DEL

5. Enable or Disable the **Enable User Access** Privilege.

   Notes:

   - Enabling User Access will intern assign the IPMI messaging privilege to user.
   - 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.

6. In the **Privilege** field, enter the privilege assigned to the user which could be Administrator, Operator, User or None. By default, the channel privileges will be displayed based on the channel availability.

   Note: The Callback privilege will only be displayed in the **Privilege** field if it's assigned through other interfaces. It cannot be set directly in the Web UI like other privileges.

7. Check **KVM Access** to assign the KVM privilege for the user.
8. Check **VMedia Access** assign the VMedia privilege for the user.

   Notes:

   - It is recommended that the privileges support to KVM and VMedia should be provided only to the ADMIN user and shouldn't be provided to USER and OPERATOR privilege level users. The administrator can provide the privilege support to user and operator privilege level users at their own risk.
   - VMedia Privilege only restricts initiating / starting media redirection. If a device is already being redirected and attached to the host, then in host it will be visible as normal device. Hence it will be accessible to all the KVM sessions. Which includes 'KVM Privilege only' sessions as well.

9. Check **SNMP Access** to enable SNMP access for the user.

   Note: Password field is mandatory if SNMP Status is enabled.

10. Choose the SNMP Access level option for user from the **SNMP Access level** (SHA or MD5) drop-down list box. Either it can be Read Only or Read Write.
11. Choose the **SNMP Authentication Protocol** (SHA or MD5) to use for SNMP settings from the drop-down list box.

    Note: Password field is mandatory if Authentication protocol is changed.

12. Choose the Encryption algorithm to use for SNMP settings from the **SNMP Privacy protocol** (AES or DES) drop-down list box.
13. Select an e-mail format from the **Email Format** drop-down list box:

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

14. In the **Email ID** field, enter the e-mail ID of the user. If the user forgets the password, the new password will be mailed to the configured e-mail address.

    Note: SMTP Server must be configured to send e-mails.

15. In the **Upload SSH Key** field, click Browse and select the SSH key file.

Note: SSH key file should be of pub type.

16. Click **Save** to save the new user and return to the users list.

To modify a user:

1. Click the active user tab to open a user screen.
2. Check **Change Password** if you wish to change the existing Password.
3. Follow the steps (3 to 15) of **Procedure to add a new User**.
4. Click **Save** to save the changes and return to the users list.
5. Click **Delete** to delete the user.

Important: There are certain reserved users which cannot be added as BMC Users. The list of reserved users are as below:

- sysadmin
- daemon
- sshd
- ntp
- root

IPMI Interfaces

Used to configure the IPMI Interfaces. You can enable or disable the IPMI Over LAN function in this page. And if 'IPMI Over LAN' is disabled, it means IPMI communication will not work over LAN interface.

Web Interface

Used to configure the HTTP Interface. You can enable or disable the HTTP function in this page. If **Access through HTTP** is enabled, users can access the BMC web interface via the HTTP protocol.

Warning: Use HTTPS for secure communication. HTTP is not encrypted and may expose sensitive data.

Power Control

Allow you to view and control the power of your computer. Select an action and click **Perform Action** to proceed with the selected action. During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after a few minutes.

Settings name	Description
Power Off	Immediately power off the computer.
Power On	Power on the computer.
Power Cycle	First power off, and then reboot the system (cold boot).
Hard Reset	Reboot the system without powering off (warm boot).
ACPI Shutdown	Initiate operating system shutdown prior to the shutdown.
Perform Action	Click to perform the selected operation.

Chapter 5. Advanced configurations

Network Settings

The Network Settings page is used to configure the network settings for the available LAN channels.

Network IP Settings

To configure Network IP:

1. Check **Enable LAN** to enable LAN support for the selected interface.
2. Select a LAN interface to be configured in the **LAN Interface** field.
3. Check **Enable IPv4** to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, enter the IPv4 Address, IPv4 Subnet and IPv4 Gateway in respective fields.

   Notes:

   - IP address is made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
   - Each number ranges from 0 to 255.
   - The first number must not be 0.
6. In IPv6 configuration, if you wish to enable the IPv6 settings, check **Enable IPv6**.
7. If the IPv6 setting is enabled, enable or disable the option **Enable IPv6 DHCP**.
8. If the field is disabled, enter the **IPv6 Address**, **Subnet Prefix length** (Value ranges from 0 to 128), **IPv6 Gateway** and **IPv6 Index** in respective fields.

   Note: If core feature IPV6_COMPLIANCE is enabled, the IPV6 default Gateway field will not be displayed.
9. In VLAN configuration, if you wish to enable the VLAN settings, check **Enable LAN**.
10. Enter the **VLAN ID** in the specified field (Value ranges from 2 to 4094).
11. Enter the **VLAN Priority** in the specified field (Value ranges from 0 to 7).
12. Click **Save** to save the entries.

Network Bond Configuration

This setting is used to configure the network bonding for the network interface. At least two network interfaces are required to enable Network bonding for the device.

The **Enable Bonding** option is enabled. You can disable the option if needed.

To configure Network bonding:

1. Select the bond interface from the **Bond Interface** drop-down list box.

   Note: The bond interface can be selected only if the **Enable Bonding** option is enabled.
2. Check **Auto Configuration** to enable the auto configuration.

   Notes:

   - The Link Speed and Duplex Mode will be active only when **Auto Configuration** is disabled.

- Use **Auto Configuration** by default. Use other modes based on network settings.

3. Select the link speed from the **Link Speed** drop-down list box.

   Note: Link speed of 1000 Mbps is not applicable when **Auto Configuration** is disabled.

4. Select either **Full duplex** or **Half duplex** from the **Duplex Mode** drop-down list box
5. Click **Save** to save the configuration.

Network Link Configuration

This setting is used to configure the network link configuration for available network interfaces.

To configure network link:

1. Select the LAN interface from the **LAN Interface** drop-down list box.
2. Check or clear **Auto Negotiation**.

   Notes:

   - The Link Speed and Duplex Mode will be active only when **Auto Negotiation** is disabled.
   - Use **Auto Negotiation** by default. Use other modes based on network settings.

3. Select the link speed from the **Link Speed** drop-down list box.

   Note: Link speed of 1000 Mbps is not applicable when **Auto Negotiation** is disabled.

4. Select either **Full duplex** or **Half duplex** from the **Duplex Mode** drop-down list box.
5. Click **Save** to save the configuration.

DNS Configuration

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 configurations are used to manage the DNS settings of a device.

To configure DNS:

1. Check **DNS Enabled** to enable all DNS services.
2. Select either **Automatic** or **Manual** for the **Host Name Setting** option.

   Note: If you select **Automatic**, you need not to enter the host name and if you select **Manual**, you need to enter the host name.

3. Enter the host name in the **Host Name** field if you have selected **Manual**.
4. In the **BMC Registration Settings** section, choose the BMC's network interface to register with DNS settings.
   a. Check **Register BMC** to register with DNS settings.
   b. Select the **Registration method**.
      - Select **Nsupdate** to register with DNS server using nsupdate application.
      - Select **DHCP Client FQDN** to register with DNS Server using DHCP option 81.
      - Select **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.

5. Check **Both** to modify TSIG authentication for both interfaces (eth0&1).
6. In **Eth 0&1 TSIG Configuration**, Check **TSIG Authentication Enabled** to enable or disable TSIG authentication while registering DNS via nsupdate.
   - The current file name will be displayed in **Current TSIG Private file info** field.
   - To view a new one, click **New TSIG private file** to browse and navigate to the TSIG private file.
7. In the Domain Settings section,
   - Select the domain settings (**Automatic** or **Manual**).
   - Enter the **Domain Name** in the given field if the option **Manual** is selected in domain settings field.
8. In **Domain Name Server Setting**,
   - Select the **DNS Name Server Setting**.
   - Select the IP Priority, either **IPv4** or **IPv6**.
   - Enter the DNS server address.
9. In **DNS Server1**, **DNS Server2**, and **DNS Server3** fields, enter the server addresses to be configured for the BMC.
10. Click **Save** to save the entries.

Sideband Interface (NC-SI)

To configure NC-SI settings:

1. Select either **Auto Failover Mode** or **Manual Switch Mode** for **NCSI Mode** type.

   Notes:

   - If you select **Auto Failover Mode**, the NCSI Interface will be configured automatically.
   - If you select **Manual Switch Mode** you are only allowed to configure NCSI interface, channel number, and package ID.
2. Select a particular interface name for which to configure NCSI settings from the **NCSI Interface** drop-down list box.
3. Select the package ID to be configured for the selected interface name from the **Package ID** drop-down list box.
4. Select the channel number to be configured for the selected interface name from the **Channel Number** drop-down list box.
5. Click **Save** to save the current changes.

Video Recording

The Network Settings page is used to configure the Video Recording. The first 3 options are used to configure the events that will trigger auto video recording function of the KVM server. And the last 3 options are used to configure and record the SOL log events.

Auto Video Trigger Settings

To configure auto video trigger:

1. Select the events to be enabled from the event list.

   Notes:

- KVM service should be enabled to perform auto-video recording.
- The **Date** field and **Time** field should be set in advance to the system date and time if Date and Time Event is checked.
- Disable or enable pre-event recording selection for newly modified configuration in **Auto Pre-Event Video Recordings** to take effect.
- Pre-Event video recording will not occur when active KVM session or Post-Event video recording is in progress.

2. Click **Save** to save the changes.

Auto Video Remote Storage

To enable or disable Remote Video support, check or uncheck the**Record Video to Remote Server** checkbox. By default, video files will be stored in the local path of the BMC. If the remote video support is enabled, then the video files will be stored only in the remote path, and not within the BMC.

To record video to remote server:

1. Check **Record Video to Remote Server** to enable the remote video support.

   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.

2. Enter **Maximum Dumps**, **Maximum Duration (Second)**, and **Maximum Size (MB)** of the video in respective fields.

   Note: The maximum dumps should be in the range from 1 to 100. The maximum duration of the video should be in the range from 1 to 3600 seconds. The maximum size of the video should be in the range from 1 to 500 MB. The recorded video file should meet either the size constraint or duration constraint, according to the configured settings, depending on which constraint is met first.

3. Enter the **Server Address**.

   Notes: The server address will support the following:

   - IP Address (Both IPv4 and IPv6 format).
   - FQDN (Fully qualified domain name) format.

4. Enter the source path in **Path in Server** field.
5. Select the **Share Type** (NFS or CIFS). If you select **CIFS**, enter the **Username**, **Password** and **Domain Name** in respective fields.
6. Click **Save** to save the settings.

Auto Pre-Event Video Recordings

Used to configure the Pre-Event video recording options. Pre-Event video recording is disabled by default. To enable the Pre-Event video recording, go to the Auto Video Trigger Settings page.

To configure Pre-Event video recording:

1. Select quality (very low, low, average, normal, or high) from the **Video Quality** drop-down list box.
2. Select modes (high, normal, low, or no) from the **Compression Mode** drop-down list box.
3. Select frames per second (1-4) from the **Frames Per Second** drop-down list box.
4. Select second (10-60) from the **Video Duration** drop-down list box.
5. Click **Save** to save the changes made on the Pre-Event Video Recording.

Pre-Event

Pre-Event video recording files will be named as per event captured. For example, if any video is recorded for crash event, the recorded file will be named as `pre_crash_video_x.dat`, where *x* is file count, similarly if it is recorded for reset event it will be named as `pre_reset_video_x.dat`.

Post-Event

Post-Event video recording files will be named as `video_dump_<Hostname>_%y%m%d%H%M%S.dat`.

File count and duration for Pre and Post Event Recordings are as shown in the below table.

Items	Auto Video Recording (Post Event)	Post Event) Pre-Event Video Recording (only for crash or reset event)
Time Limits	• 20 seconds or 5.5MB video allowed if local storage. • 3600 seconds or 500MB video recording allowed if remote storage (remote path).	Default value is 10 seconds but can be configured up to 60 seconds.
Video File Count	• local storage: 2 (After 2, if video recording starts, the older video file among the two files will be replaced with the new video) • remote storage: maximum configured dump value of video files for remote storage.	1 if local storage or 3 if remote storage. (Once the maximum file count is reached, will delete the old video file to store the new file.)

Notes:

- The recorded video duration may vary by up to ±5 seconds.
- If the video resolution changes during auto-video recording, the system will generate separate video files for each resolution segment. Video file will be downloaded with name `video_d-m-Y_H-M-S_part`*N*`.avi`. *N* indicates the sequence number of the segmented file.
- Multiple video files will be generated only for HTML video download option. In case of Java video download application, single video file will be downloaded even when resolution changes occurs. The behavior difference between HTML video download option and Java video download application is due to browser memory constrain.
- During rapid shutdown sequences (e.g., BIOS/DOS boot), the system may not capture post-power-off screen recordings due to insufficient time.
- If recording fails, the video file will be unavailable for download or playback.

SOL Trigger Settings

Used to configure which event on the page will trigger the SOL log.

To configure SOL Trigger:

1. Check the events to be enabled to configure which event will trigger the SOL log option to start.

   Note: The **Date** and **Time** field should be set in advance to the system date and time if **Date and Time Event** is checked.

2. Click **Save** to save the changes.

SOL Log Settings

To configure recorded video files:

1. Enter the log size in the **Log Size (KB)** field. The value supports a maximum length of 10 digits.
2. Enter the log file count in the **Log File Count** field. The Maximum number of log files count is 1.
3. Check **Record Video to Remote Server** to enable the remote video support.

   Note: The **Server Address**, **Source Path**, and **Share Type** options will be enabled only if the **Remote Video Support** option is enabled.
4. Enter the server address in the **Server Address** filed and the source path in the **Path in server** filed.

   Notes: Server address will support the following:

   - IP Address (Both IPv4 and IPv6 format)
   - FQDN (Fully qualified domain name) format
5. Select **NFS** or **CIFS** for the **Share Type** option. If you select **CIFS**, Enter the username, password and domain name in respective fields.
6. Click **Save** to save the settings.

Notes:

- If the proper SOC specific video driver is installed in the host, only video changes will be captured during the video recording process.
- The host cursor data, in this case, will not be a part of the video changes, and hence the host cursor will not be available in the recorded video file (DAT file).

SOL Configurations

Used to configure the Baud rate between the BMC card and the host. You can select the Volatile Bit Rate and the Non-Volatile Bit Rate from the drop-down list box according to your device configuration.

Remote Control

KVM Mouse Settings

The Redirection Console handles mouse emulation from the local window to the remote screen using any of three methods. Only an Administrator user has the rights to configure this option.

To configure the Mouse mode:

1. Select either of the following as your requirement:
   - Relative Positioning (Linux)

     Note: Applicable for all Linux versions, versions less than RHEL6, and versions less than FC14.
   - Absolute Positioning (Windows)

     Note: Applicable for all Windows versions, versions above RHEL6, and versions above FC14.
   - Other Mode

     Note: Recommended for SLES-11 OS Installation.
2. Click **Save** to save the changes made.

Note: If the client and host mouse position is not in sync, then check the release notes of the host operating system to verify any additional configuration to be needed in the Host.

Remote Session

Used to configure remote session settings.

To configure remote session:

1. Select **JViewer/H5Viewer** for the **KVM Client Type** option.
2. Select the keyboard language from the **Keyboard Language** drop-down list box.
3. Select the virtual media attach mode from the **Virtual Media Attach Mode** drop-down list box.
4. Enter a value in the **Retry Count** field to set the number of attempts for retrying the redirection session.
5. Enter a value in the **Retry Time Interval (Seconds)** field to give time interval for each attempt.
6. Check **Server Monitor OFF Feature Status** to enable the local monitor on/off command during runtime.
7. Check **Automatically OFF Server Monitor, When KVM Launches** to automatically lock the local monitor during H5Viewer launch.
8. Click **Save** to save the current changes.

Remote Control

Used to define the system and browser requirements for Remote Control are given below.

Launch H5Viewer

System Requirements:

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be lag in video, keyboard, and mouse functionality. Supported Browsers:
- Chrome latest version.
- IE11 and above.
- Firefox (with limited support).

Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations.

To start or stop KVM:

1. Click **Launch H5Viewer** to open the Remote KVM page.
2. To stop the H5Viewer video redirection, click **Stop KVM**.

To Start or stop Media:

1. Click **Browse File** to select CD Image.
2. Click **Start Media** to redirect the selected CD image file to the Host.

   Note: To use KVM CD/DVD media redirection, make sure that the **Remote KVM CD/DVD device instances** are not set to **0**. For specific settings, refer to “VMedia Instance Settings” on page 46.
3. To stop the CD Image redirection, click **Stop Media**. A detailed description of the menu items is as below:

Settings name	Description
Video	• **Pause Video**: This option is used for pausing Console Redirection. • **Resume Video**: 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. • **Host Display**: The display of the host. • **Display on**: If you enable this option, the display will be shown on the screen in the server screen. If you disable this option, the display will be shown on the screen in Console Redirection only. • **Display off**: 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. • **Capture Screen**: This option helps to take the screenshot of the host screen and save it in the client's system.
Mouse	• **Show Client Cursor**: This menu item can be used to show or hide the local mouse cursor on the remote client system. • **Mouse Mode**: This option handles mouse emulation from local window to remote screen using either of the two methods. Only an Administrator user 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. **Note:** Client cursor will be hidden always. If you want to enable, use Alt+C to access the menu.
Options	• **Zoom** – **Normal**: By default this option is selected. – **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%. • **Bandwidth**: This option helps to choose the bandwidth between BMC and the host. • **Block Privilege Request**: To enable or disable the access privilege of the user. • ***Compression Mode**: This option helps to compress the Video data transfer to the specific mode. • ***DTC Quantization Table**: This option helps to choose the video quality from 0 to 7, and 0 means best quality. **Note:** *Specific to AST SOC.

Settings name	Description
Keyboard	• **Keyboard Layout**: 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. List of Host Physical Keyboard languages supported in SPX H5Viewer. – English U.S. – German. – Japanese. • **Send Keys**: This option is used to key items. This menu contains the following sub menu items. – **Hold Down** – **Right Ctrl Key**: This menu item can be used to act as the right-side <CTRL> key when in Console Redirection. – **Right Alt Key**: This menu item can be used to act as the right-side <ALT> key when in Console Redirection. – **Right Windows Key**: This menu item can be used to act as the right-side <WIN> key when in Console Redirection. – **Left Ctrl Key**: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection. – **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. – **Press and Release** – **Ctrl+Alt+Del**: This menu item can be used to act as if you depressed the <CTRL>, <ALT>, and <DEL> keys down simultaneously on the server that you are redirecting. – **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. – **Context Menu Key**: This menu item can be used to act as the context menu key, when in Console Redirection. – **Print Screen Key**: This menu item can be used to act as the print screen 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. **Add Hot Keys**: This menu is used to enable macros. Click **Add** to macros.

Settings name	Description
Video Record	**Record Video**: This option is to start recording the screen. **Stop Recording**: This option is used to stop the recording. **Record Settings**: This option is used to set video record duration and video compression value. Video record duration value should be in the range of 1 to 1800 seconds. Video Compression value should be in the range of 0.1 (Low image quality) to 0.9. (High image quality). **Normalized video resolution to 1024 x 768**: Host video will be scaled to 1024 x 768 in the recorded video file. Enabling this option improves video recording performance of client side in H5Viewer. Disable this option to record video at same resolution as host video. The host video capture depends on client system performance. If this option is disabled, recorded video file may have inconsistency. (i.e., Recorded video file duration may not be the same as configured value). **Notes:** • The Maximum video file size allowed is around 40MB. If the video file size reaches its max size limit, the recorded file will be downloaded, and the recording will be in progress until the configured video recording time is reached. The video file is saved as video_date-month-year_hr-min-sec_partno in client-side video recording. • User must take care of saving the video files in different browsers. • When H5viewer focus is lost and if video recording is in progress, the recording will be stopped with a notification message and the recorded video file will be discarded. • Due to browser limitation, set timeout/set interval will be delayed from specified time of interval when browser window loses focus, hence video server will not send the video packets to H5viewer and so the video recording will be stopped.
Power	The power options are 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 perform Power OFF Immediately. • **Orderly Shutdown**: To Power OFF the sever in proper order. • **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 display the active users and their system IP address. Active KVM Session can be terminated when there are multiple KVM session from master [FULL Privilege KVM Session].
Help	Click this option to get more information About H5Viewer. The KVM Remote Console utility version and plugin version will be displayed.

The upper right of H5Viewer window displays all the quick buttons which allow you to perform the below functions.

Quick Buttons	Description
	This quick button shows or hides notifications dropdown menu, which contain the list of notifications displayed by H5Viewer.
	This quick button shows the current zoom value in percentage.
	This quick button is used to display the current host monitor status. If icon is in green, then host monitor is unlocked. If the icon is in red, host monitor is locked. By clicking the button host monitor status can be toggled.
	This quick button is used to display the current server power status. If the icon is in green color, the server status is powered on. If the icon is in red color, the server status is powered off. Click the button to toggle immediate power off / power on the host.

Status bar buttons:

Keyboard LED Sync

When the H5Viewer is launched, the keyboard locks status and LEDs denoting the lock status of the host machine, should be in sync with the client machine. That is, if the **Num/Caps/Scroll lock** is enabled or disabled in the client machine, the same should be updated in the host machine as well.

Notes:

- Due to web browser related security concerns this feature has following limitations.
- Host LED status will be synced with client LED status, only if user presses any key in client keyboard when H5Viewer window is in focus.
- Client keyboard LED status cannot be updated.
- This functionality is not available in safari web browser.

Control keys

This option provides the same functionality of **Send Keys → Hold Down** menu item. Select any of the menu item, it will highlight the corresponding status bar button in green color. Similarly, by clicking the buttons will toggle the selection status of the corresponding menu item.

H5Viewer browser limitations

This section describes the H5Viewer limitations of different browsers.

- **All browsers:**
  - To use secure H5Viewer sessions, adding an SSL certificate to the browser is mandatory.
  - H5Viewer video record length (client-side video recording length set by a user) will differ from the downloaded video file duration. The recorded video duration depends on the browser, and the amount of host video update.
  - Keyboard LED sync will not work when the host is the Linux text console.
  - Clearing H5Viewer sessions will take some time when a user abruptly closes the H5Viewer window.

  - If any dialog (like File Choose, Confirmation dialog, etc) in H5Viewer is kept open and not closed, then the background functionalities of threads might get affected leading to H5Viewer reconnect or connection close.
- **Google Chrome**: Upon launching, the H5Viewer window will not be resized to the client resolution.
- **Firefox**: Only the Japanese QWERTY input method will work. The Japanese hiragana or katakana input method will not work.
- **Safari**:
  - Keyboard LED sync will not work.
  - To use secure H5Viewer sessions, adding an SSL certificate to the browser is mandatory.

Launch JViewer

This is an OS-independent plug-in which can be used in Windows as well as Linux with the help of Java Runtime Environment (JRE). JRE should be installed in the client's system.

Note: It is recommended to use openJDK 8 or any later LTS version. IcedTea-Web launch applications may work inconsistently when JDK 11 or a later version is used. The Web launch dialog may freeze and become unresponsive.

Procedure to launch JViewer:

1. Download the .jnlp file from the BMC.
2. Open the .jnlp file using the appropriate JRE version (Javaws).

   When the downloading is done, it opens the console redirection window.

A detailed explanation of the menu items are given below:

Settings name	Description
Video	• 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. • DTC Quantization Table: This option helps to choose the video quality. • 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. • Low Bandwidth Mode: This option is used to control the video packet dataflow in the network. • 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	• Hold Right Ctrl Key: This menu item can be used to act as the right-side <CTRL> key in console redirection. • Hold Right Alt Key: This menu item can be used to act as the right-side <ALT> key in console redirection. • Hold Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key in console redirection. • Hold Left Alt Key: This menu item can be used to act as the left-side <ALT> key in console redirection. • Left Windows Key: This menu item can be used to act as the left-side <WIN> key 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 in console redirection. You can also decide how the key should be pressed: Hold Down or Press and Release. • Ctrl+Alt+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT>, and <DEL>keys down simultaneously on the server that you are redirecting. • Context menu: This menu item can be used to act as the context menu key 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 keys directly to host from the physical keyboard.

Settings name	Description
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. Use the '+' or '-' key to change the threshold settings until both the cursors go out of sync. Detect the first reading on which cursors go out of sync. Once this is detected, use 'ALT-T' to save the threshold value. • **Show Host Cursor**: This option is used to enable or disable the visibility of the host cursor. Specific video drivers should be installed in the host for this feature to work. **Note:** Remote KVM supports mouse move, and left and right button clicks only. • **Mouse Mode**: This option handles mouse emulation from local window to remote screen using any of the following methods. Only administrators have 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 and accessing mouse in the UEFI screen. **Notes:** – Users are advised to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issues in absolute mouse mode. – The client cursor will be hidden always. If you want to enable it, use Alt+C to access the menu. – You can see client and host cursors in JViewer if the mouse is moved faster or in circle. Mouse sync will depend on many factors like network, client machine video packet receiving and rendering, and BMC CPU utilization. In normal use cases, you will have better mouse sync, compared to heavy video or stress testing scenarios. High resolution and media redirection (copy) will have direct impacts on video rendering because the client or host cursor can be viewed while moving the cursor.
Options	• **Bandwidth**: 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

Settings name	Description
	• **Keyboard/Mouse Encryption**: This option allows you to encrypt keyboard inputs and mouse movements sent between the connections. • **Zoom**: – **Zoom In**: This option is used for increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%. – **Zoom Out**: This option is used for decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%. **Note:** This option is available only when you launch the Java console. • **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 the 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. Therefore, the client and host mouse cursors might not be in perfect sync. • **Fit to Host Resolution**: If the host screen resolution is smaller than the client screen resolution, choose this option to resize the JViewer frame to the host resolution. **Note:** This option can be configured from PRJ in MDS. • **Send IPMI Command**: This option opens the **IPMI Command Dialog**. Enter the raw IPMI command in the **Hexadecimal** field as a hexadecimal value and click **Send**. The response will then be displayed. • **GUI Languages**: Choose the desired GUI language. • **Request Full Permission**: Partially permitted sessions can use this option to request the full permission from the existing fully permitted session. **Note:** This menu option is available only for partially privileged sessions and full permission sessions will not have this option in the menu. • **Block Privilege Request**: Fully privileged sessions can use this option to block incoming requests from partially privileged sessions by setting an auto response as either Allow only Video or Deny Access. **Notes:** This menu option is available only for full permission sessions and partially privileged sessions will not have this option in the menu. Either of the options can only be selected. Both options cannot be selected together. To disable **Block Privilege Request**, none of the options should be selected in the menu. – If **Allow only Video** is selected, the slave session will be notified as `KVM Master Session blocked incoming request` and it will always receive `Video Only` (partial permission). – If **Deny Access** is selected, the slave session will be notified as `KVM Master Session blocked incoming request` and the incoming KVM session will be closed.

Settings name	Description
Media	• The virtual media application will allow you to redirect different media to the host system. The application supports CD/DVD, hard disk/USB devices, as well as image files. **Notes:** – If there are two device panels for each device, when you click **Connect**, the redirected device panel will be disabled. – Unmounting a device will make the driver disconnect the device when using **Auto Attach**. Hence, when unmounting one USB key, the other USB key will be disconnected and then reconnected. • The virtual media application can be launched as a standalone application from the StandAlone connection dialog. It can also be launched from the JViewer, using the Virtual Media menu. When launched from JViewer, this application will work like a child dialog of the JViewer. Each of the supported devices is listed in a separate tab. Each tab in the application is described below. – **CD/DVD**: This tab can be used to start or stop the redirection of a physical DVD/CD-ROM drive and DVD/CD image file of ISO/ NRG file format. – **Hard Disk/USB**: This tab can be used to start or stop the redirection of a hard disk/USB key image and USB key image such as img/ima. **Notes:** – For redirecting hard disk drives, you should have the administrator privilege (root user in the case of Linux clients). – For Windows 7 and above, the Web browser from which the KVM redirection will be initiated, should be launched using the **Run as Administrator** option. If there are multiple instances of the Web browser open simultaneously, ensure that all the instances are launched using the **Run as Administrator** option. – For a Windows client, if the logical drive of the physical drive is dismounted, the logical device is redirected with read/write permission. Else it is redirected with read permission only. The USB/hard disk drive can be redirected as a whole physical drive or individual logical drives. – For a MAC client, external USB hard disk redirection is only supported. The external hard disk drives should be unmounted from the client before being redirected. – For a Linux client, fixed hard drive is redirected only as read mode. It does not support write mode. The USB/hard disk drive will be redirected as a whole physical drive. – For hard disk image redirection, only the file extension is validated. The hard disk/USB key device or image will be redirected to the host as it is. The BMC will not validate the hard disk medium, and the host OS will take care of this. This is applicable for all the media redirection client applications. – If the feature **Redirect Devices Always in READ and WRITE Mode** is enabled, the internal hard disk drives in the client

Settings name	Description
	machine will not be listed. This information will be displayed in the status bar of the virtual media application. – If files with hidden attribute are visible in the file open dialog, the file can be opened and redirected. – If the file is not visible in the file open dialog, the user shall mention the path of the image file in the file name field of the file open dialog and then open the image. – TSM stack media redirection supports only basic hard disk redirection. – **Connection Status**: This tab provides a collective view of the redirection status of various virtual media devices. **Note:** VMedia privilege only restricts initiating or starting media redirection. If a device is already being redirected and attached to the host, then it will be visible as a normal device in the host. Hence, it will be accessible to all the KVM sessions, including sessions for KVM privilege only as well.
Keyboard Layout	• **Auto Detect**: This option is used to detect keyboard layout automatically. If the client and host keyboard layouts are the 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, you can choose the host language layout in the menu and thereby can directly use the physical keyboard. • **Physical Keyboard**: This feature is fully compatible when the host and client have 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 a Windows host, the Windows option should be selected. Similarly, when working with a Linux host, the 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. • **Soft Keyboard**: This option allows you to select the keyboard layout. It will show the dialog as similar to the 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. **Notes:** – Different Linux systems follow different keyboard layouts. Therefore, the soft keyboard displayed uses the standard windows keyboard layout irrespective of the host OS. – Soft keyboard is applicable only for the JViewer application, not for other applications in the client system.
Video Record	• **Start Record**: This option is to start recording the screen. • **Stop Record**: This option is used to stop the recording. • **Settings**: This option is used to set the settings for video recording. **Notes:** Before you start recording, you have to enter the settings.

Settings name	Description
	1. Click **Video Record → Settings**. The settings page is displayed. 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 of **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	• **Reset Server**: To reboot the system without powering off (warm boot). • **Immediate shutdown**: To perform power-off immediately. • **Orderly shutdown**: To power off the server in a proper order. • **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 display the active users and their system IP addresses.
Help	**JViewer**: displays the copyright and version information.

The lower right of console redirection windows displays all the quick buttons. These quick buttons allow you to perform the below functions by clicking them.

Note: This option is available only when you launch the Java console.

Button	Description
	This quick button is used to play the console redirection after being paused.
	This quick button can be used for pausing console redirection.
	This quick button is used to view the console redirection in full screen mode. **Note:** Set your client system resolution same as the host system resolution so that you can view the server in full screen.
	This quick button is used to show or hide the soft keyboard.
	Drag this quick button to zoom in or out.
	This quick button is used to record the video.

Button	Description
 	These 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 switch to Active Users.
	This quick button will work like a toggle button. • If the icon is in green, the server status is powered on. Clicking the button will trigger an immediate shutdown action in the host. • If the icon is in red, the server status is powered off. Click the button to power on the host.
	This quick button displays the available hot keys.

Keyboard LED sync

When the JViewer is launched, the keyboard lock status and LEDs denoting the lock status of the host machine, should be in sync with those in the client machine. That is, if the Num, Caps, or Scroll lock is enabled or disabled in the client machine, the same should be updated in the host machine as well. The host keyboard LED status will be synchronized with the client keyboard, the lock indicators in the JViewer status bar, and the JViewer soft keyboard. The client keyboard's LED status before launching JViewer, or before the JViewer gains focus, will be set back to the client when the focus is lost from the JViewer, or when the JViewer is closed.

Notes:

- For Macintosh® OS X clients, the client keyboard LED sync will not work as the OS does not allow user applications to alter the keyboard LED status. However, the keyboard lock indicators on the JViewer status bar, and the JViewer soft keyboard lock status will sync with the host keyboard LED status.
- In the case of latest Linux distributions used as the host, the keyboard LED sync will not work if the lock status is changed using the host physical keyboard directly. However, the sync will work if the LED status is changed using the on-screen keyboard available in the host OS.
- Opening a child dialog in JViewer will cause the focus shift out of JViewer. The client keyboard's LED status before launching JViewer, or the JViewer gains focus, will be set back to the client in this case.

Serial Over LAN

One of the powerful tools in IPMI is SOL, which provides serial line access over the management LAN. The BMC does this by redirecting information destined for the serial port over to the LAN. With SOL console redirection, system administrators can remotely view the text-based console on their remote machines from anywhere and perform any task that does not require a GUI.

To activate SOL Support, follow the below procedures:

1. Click **Remote Control** from the Menu Bar.
2. Click **Activate** to activate SOL. Columns and Rows can be configured separately by changing the input field.
3. Click **Deactivate** to deactivate SOL.

Image Redirection

This page is used to configure the images into BMC for redirection. This can be done either by uploading an image into BMC, **Local Media** or by mounting the image from the remote system, **Remote Media**.

Note: VMedia privilege only restricts initiating or starting media redirection. If a device is already redirected and attached to the host, then in host it will be visible as normal device. Hence it will be accessible to all the KVM sessions, which includes **KVM Privilege only** sessions as well.

Media Redirection General Settings

General Settings	Description
Local Media Support	Enable or disable Local Media support.
Remote Media Support	Enable or disable Remote Media support. If it is selected, the following remote media types will be displayed. • Mount CD/DVD* • Mount Hard disk **Note:** *If the share type is HTTP or HTTPS, the checked status of the option “Mount CD/DVD” cannot be kept after refreshing, but it will not affect the functionality

On selecting the individual media types, its respective configurations will be displayed. You can configure different settings for different remote media types.

Settings	Description
Share Type for CD/DVD	Share Type of the remote media server, NFS, Samba (CIFS), HTTPS, and HTTP are supported. **Notes:** Remote media HTTP/HTTPS support limitations are as follows: • Only CD Image redirection is supported. • Only one CD/DVD Instance is supported.
Same settings for Harddisk Images	Enable or disable to select same media type data configurations for all the remote media types.
Mount Harddisk	Enable or disable to mount hard disk.
Server Address for Harddisk Images	Address of the server where the remote media images are stored.
Path in server	Source path to the Remote media images.
Share Type for Harddisk	Select share type for hard disk either NFS or CIFS.
Domain Name, Username, and Password	If share type is Samba (CIFS), then enter user credentials to authenticate on the server.
Save	Save the settings.

VMedia Instance Settings

To configure VMedia Instance:

1. Select the number of **CD/DVD devices**, **Hard disk devices** and **Remote KVM CD/DVD and Hard disk Devices** from respective drop-down list boxes.

Note: Maximum of four devices can be added in CD/DVD and hard disk drives.

2. Check **Power Save Mode** to enable or disable the virtual USB devices visibility in the host.
3. Click **Save** to save the changes made.

Note: Virtual media configuration changes will restart all the media services. So, configuration changes will be blocked when any active media redirection is present.

Active Redirections

Used to display the active redirected media, which are redirected via JViewer/VMAPP/ H5Viewer/LMedia/ RMedia/VMCLI. Information like media type, media instance, client type, image name, redirection status, client IP will be displayed.

Settings	Description
Media Type	The type of media devices (CD/DVD) supported for active redirections
Media Instance	The number of media devices supported for active redirections
Client Type	The type of media devices (CD/DVD) supported for active redirections
Image Name	The name of media devices supported image for active redirections
Redirection Status	The status media for active redirections
Client IP	The IP of the connected media devices (CD/DVD) supported for active redirections

Note: Local or remote media connection will use loopback socket for communication. So "~" symbol will be displayed for loopback IP (`127.0.0.1` (`or`) `::1`) in media session information page.

Local Images

This page displays the list of available images in the local media on BMC. You can replace or add new images from here.

To configure the image, you need to enable Local Media support under **Image Redirection → Media Redirection General Settings**. Once you enable this option, the user can add the images and the added images will be redirected to the host machine.

Notes:

- Support maximum 2TB microSD card.
- The microSD card is divided into at least 2 partitions and should be formatted as ext4/ext3/ext2 file system. Place the image(s) to the partition 2.
- To delete or add an image, you must have Administrator Privileges.
- More than one image can be uploaded for each image type. The allocated size for local media upload is determined by the size of partition 2. User cannot upload image size greater than 1GB. For example, if the allocated size for partition 2 is 3GB, the user can upload multiple images to fill up the 3GB size, but each upload image size should not exceed 1GB.
- Support CD/DVD format: ISO9660, UDF(v1.02~v2.60).
- Support CD/DVD media file type: (*.iso), (*.nrg).
- For your reference, the following microSD cards have been tested compatible.
  - SanDisk microSD, SDHC, 16GB
  - Kingston microSD, SDXC, 64GB

Compatible cards are not limited to the above list.

To configure local images:

Note: The **Start Redirection** button is active only for VMedia enabled users.

1. Click on the **Local Images** section.
2. Select a configured slot and click ▶ to start the local media redirection. It is a toggle button, if the image is successfully redirected, then click ■ to stop the local media redirection.

   Note: Avoid using these special characters when naming images: {} () < > & * ` | = ? ; [ ] $ - # ~ ! \ ” % / \\ : + , ’
3. To add an image, select a free slot and click to upload a new image to the device. A pop-up screen will be displayed, prompting you to select the image. Select the image and click **OK** to continue adding the image.
4. To clear an image status, select an image and click to clear image status from the device.
5. To delete an image, select a record and click to delete the selected image. A popup message will be displayed, prompting you to continue. Click **OK** to continue deleting the image.

   Note: Redirection needs to be stopped to delete the image.
6. To refresh the image lists, click to get the latest image lists.
7. To sync the image status, click to sync the latest images’ status.

Remote Images

This page displays configured images on BMC. You can configure images of the remote media server.

To configure remote images:

1. To start redirection and configure remote media images, click ▶ and make sure **Remote Media Support** is enabled.

   Note: The **Start Redirection** button is active only for VMedia enabled users.
2. Select a configured slot and click ▶ to start the remote media redirection. It is a toggle button, if the image is successfully redirected, then click ■ to stop the remote media redirection.

   Notes:

   - Redirection needs to be stopped to clear the image.
   - Avoid using these special characters when naming images: {} () < > & * ` | = ? ; [ ] $ - # ~ ! \ ” % / \\ : + , ’
3. Perform CD Redirection with Media Boost Mode.
   - Select CD media configured slot and click ▶ to start the remote media redirection.
   - This action prompts you with the message and click **OK** to redirect image with the media boost mode. Or else, click **Cancel** to stop this action.

   Notes:

   - If media boost mode is selected, the processes related to media redirection will have high priority than other processes. This will improve media performance, but other processes will have limited access to CPU cycle.
   - If CD/DVD instance is started with media boost mode, the next CD/DVD instance will be started without any pop-up message.

4. To clear an image status, select an image and click ⏏ to clear image status from the device.
5. Click **Refresh Image list** to get latest image lists from the remote storage. The latest image names list will be displayed in the **Image Name** drop-down list box.
6. Click **Sync Image Status** to get the image status from the remote storage. The latest image status will be displayed in the Redirection Status list.

Maintenance

This maintenance group allows you to do maintenance tasks on the device.

Backup Configuration

Allow you to select the specific configuration items to be backed up.

To backup configuration:

1. Check **Check All** to back up all configuration items or check the configuration that needs to be backed up.

   Note: Network configurations are inter-related to IPMI, and hence by default **IPMI** will be selected automatically when you select **Network and Services** to be backed up and vice versa.
2. Click **Download** to save the backup configuration file to the client system.

Note: During the backup process, the mechanism will parse and filter out the values of sensitive data related to passwords.

BMC Recovery

Allow you to configure BMC recovery settings. The BMC Auto-Recovery is a mechanism to flash and boot the recovery image when primary image in the SPI-ROM is corrupted or fails to boot. It will provide an additional failure over mechanism for BMC firmware.

To configure BMC recovery:

Check or clear **Force Recovery** to start auto-recovery immediately at next reboot.

1. Enter the **Boot Retry Count** value.
2. Enter the **Recovery Retry Count** value.
3. Enter the **Server Address** to store firmware image.
4. Enter the **Image Name**.

   Note: By default, the image name is mentioned as `rom.ima`.
5. Click **Save** to save the configured settings.

Notes:

- The recovery image can be loaded from microSD card (partition 1). If failed, image will be recovered from TFTP path. Recovering the BMC firmware via TFTP will erase the FRU information stored in the BMC. Ensure you back up this data before proceeding to allow for proper restoration afterward.
- The recovery image's name in microSD card is restricted to "rom.ima".
- In order to perform BMC firmware recovery via microSD, partition table should be GPT label and partition 1 should have EXT filesystem. The Recovery image "rom.ima" should be in partition 1.

Firmware Image Location

Used to configure firmware image into the BMC.

To configure Firmware image location:

1. Select the **Image Location Type** (**Web Upload during flash** or **TFTP Server**).
2. If the protocol selected is TFTP, enter the IP address of the server in the **TFTP Server Address** field.
3. Enter the TFTP image name in the **TFTP Image Name** field.
4. Enter the TFTP retry count value in the **TFTP Retry Count** field.
5. Click **Save** to save the changes.

Firmware Information

Provide the active Firmware Information.

Settings	Description
Build Date	The build date of the active BMC image
Build Time	The build time of the active BMC image
Firmware version	The Firmware version of the active BMC image

Firmware Update

Take you through the process of firmware upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to **Preserve All Configuration** is available. Enable it if you wish to preserve configured settings through the upgrade.

To update firmware:

1. Click **Browse** to select firmware image. The Firmware update undergoes the following steps:
   a. Close all active client requests.
   b. Prepare device for firmware upgrade.
   c. Click **Choose File** to select your firmware image.

      Note: A file upload pop-up will be displayed for http/https but in the case of TFTP files, the file is automatically uploaded displaying the status of upload.
   d. Click **Start firmware update** to upload the firmware image.
2. Click **Preserve all Configuration** to preserve all configurations if you prefer.
3. Click **Proceed to Flash** to start the firmware upload. A warning message will be displayed, prompting you to proceed further and click **OK** to start the firmware upload.
4. Verify Firmware image:
   - In **Section Based Firmware Update**, you can configure the firmware image for section-based flashing. Check the required sections and click **Flash to Proceed** to update the firmware.
   - If flashing is required for all images, select **Full Flash**.
   - If you select **Version Compare Flash** from web, the current and uploaded module versions, FMH location, size will be compared.
   - If the modules differ in size and location, proceed with force firmware upgrade.
   - If all the module versions are the same, restart BMC by saying all the module versions are similar.
   - If only few module versions are differed, those modules will be flashed.

Note: Only selected sections of the firmware will be updated. Other sections are skipped. Before starting flash operation, you are advised to verify the compatibility between image sections.

5. Click the **Flash to Proceed** again to flash firmware image.
6. Reset the image.

Notes:

- The Firmware Update page will be disabled, and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the BMC card's firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.
- After resetting, the device IP may be changed, and you are supposed to use the latest IP to log in.
- Interrupting the BMC firmware update process may cause the BMC inoperable. If the recovery functionality of BMC is properly configured, it may trigger a recovery mode when BMC reboot. The recovery process may take about 30 minutes.

Preserve Configuration

Allow 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 update configuration.

To preserve configuration:

1. Click **Firmware Update** or **Preserve Configuration** link to view the Firmware Update or Preserve Configuration page accordingly.
2. Select the required preserve configuration items by either checking the appropriate check boxes or by checking **Check All**.
3. Click **Save** to save the changes.

Settings	Description
SDR	This contains the sensor data record information that is used in IPMI. **Dependency Configurations** - NIL
FRU	This contains the logical field replaceable unit data that are used by IPMI. **Dependency Configurations** - SDR
SEL	This contains the system event logs that are being logged by the IPMI. **Dependency Configurations** - IPMI
IPMI	This contains the IPMI configurations, DCMI1.5 specification parameters, the keys that are used to decrypt the passwords. **Dependency Configurations** - NIL
Network	To save network settings related with IPMI (LAN IP or DHCP configuration), select **IPMI** and **Network** simultaneously. After restore configuration, the Network Configuration will be preserved successfully. **Dependency Configurations** - IPMI

Settings	Description
NTP	This contains the NTP dameon protocol configuration parameters, the auto or manual network type protocols, the time to synchronize the system clock, local time and time zone. **Dependency Configurations** - IPMI
SNMP	This contains the SNMP user configurations and SNMP users privilege levels. **Dependency Configurations** - NIL
SSH	This contains the keyword argument pairs of configurations, the private parts of the host keys, and the public parts of the host keys. **Dependency Configurations** - NIL
KVM	This contains the modes of media, the mouse mode configurations, host machine physical keyboard language layout, the parameters of video record file, the stunnel configuration, the user defined macro from the JViewer, the image name and the remote machine information. **Dependency Configurations** - NIL
Authentication	This contains the configurations related to authentication such as SSL enable, timeout, RAC domain, AD type, open LDAP role group information, PAM Order, user login information, and so on. **Dependency Configurations** - NIL
Syslog	This contains the system log configuration details to preserve different event categories such as alert, critical, error notification and so on. **Dependency Configurations** - NIL
Web	This contains the firmware image location details to update firmware configuration. **Dependency Configurations** - NIL
Extlog	It preserves Extended SEL Log events. **Dependency Configurations** - IPMI **Note:** This support is feature based. If this feature is enabled, then the **Extlog** option will be displayed in Preserve configuration.
Redfish	Redfish preserves the Redis Database file. **Dependency Configurations** - NIL **Note:** This support is feature based. If this feature is enabled, then the **Redfish** option will be displayed in Preserve configuration.

Restore Configuration

Allow you to restore the configuration files from the client system to the BMC.

To restore configuration:

1. Click **Browse** to select the configuration file that needs to be backed up and used to restore the configuration when needed.

2. Click **Save** to restore the backup files. The Restore Configuration page will be displayed.
3. Click **OK** to upload the new configuration file and restore.

Note: Reset password after restoring configuration.

Restore Factory Defaults

Used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration.

To restore factory defaults:

1. Click **Preserve Configuration** to redirect to the Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click **Restore Factory Defaults** to restore the factory defaults of the device firmware.

Notes:

- To ensure BMC's proper functionality, power cycle your computer after restoration.
- Generally, it takes within 10 minutes to restore the device firmware to factory defaults.

System Administrator

To configure the System Administrator settings:

1. Check **Enable User Access** to enable user access for system administrator.
2. Check **Change Password** to change the user password. This action enables the **Password** fields.
3. Enter the new password in the **Password** field.
4. Enter the password in the **Confirm Password** field again.
5. Click **Save** to save the changes.

Appendix A. Trademarks

Lenovo, Lenovo logo, ThinkStation, and ThinkStation logo are trademarks of Lenovo. Microsoft and Windows are trademarks of the Microsoft group of companies. All other trademarks are the property of their respective owners.


Lenovo