

Lenovo

Lenovo ThinkSystem System Manager User Guide



Fifth Edition (December 2020)

© Copyright Lenovo 2019, 2020.

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

Contents

Chapter 1. Introduction	1
BMC features	1
Chapter 2. Accessing the BMC through TSM	5
Obtaining the BMC IP address	5
Logging in to TSM	5
Menu bar	7
Quick buttons on the TSM main interface	8
Chapter 3. Dashboard	11
Chapter 4. System Inventory	13
Chapter 5. Utilization	15
Chapter 6. Logs & Reports	17
IPMI Event Log	17
Audit Log	17
Chapter 7. Settings	19
Captured BSOD.	19
Date & Time	19
External User Services	20
LDAP/E-Directory Settings.	20
Active Directory Settings	22
RADIUS Settings	24
KVM Mouse Settings.	25
Remote Log Settings.	26
Media Redirection Settings	26
General Settings.	26
VMedia Instance Settings	27
Remote Session.	28
Active Redirections	28
Network Settings	29
Network IP Settings	29
Network Bond Configuration	30
Network Link Configuration	30
DNS Configuration	31
Sideband Interface (NC-SI)	32
PAM Order Settings	33
Platform Event Filters	33
Event Filters	33
Alert Policies	35
LAN Destinations	35
Services.	36
Modifying the configurations of a service	38

Viewing or terminating active sessions for a service	38
SMTP Settings	38
SSL Settings	40
Generate CSR	40
Download CSR	41
Import Signed Certificate	41
Generate SSL Certificate	41
View SSL Certificate	42
Download SSL Certificate	42
System Firewall	42
General Firewall Settings	42
IP Address Firewall Rules	43
Port Firewall Rules	44
User Management.	44
System Location	47
Account Lockout Policy.	47
SNMP Trap Version	47
Power Supply Setting	47
IPMI Configuration.	47
Chapter 8. Remote Control	49
Launch H5Viewer	49
Procedure to start/stop KVM	49
Procedure to start/stop media	49
Video	50
Mouse	50
Options	50
Keyboard	51
Send Keys	51
Hot Keys.	51
Video Record	52
Power.	52
Active Users	52
Help	53
Quick buttons.	53
Status bar buttons	53
Keyboard LED sync	53
KVM sharing	54
Launch JViewer.	55
Procedure to launch JViewer	55
Video	55
Keyboard	56
Mouse	56
Options	57
Media	59
Keyboard Layout	61

Video Record	62	Restore Factory Defaults	73
Power	62	Chapter 12. Sign Out	75
Active Users	63	Chapter 13. Flash tool	77
Help	63	Chapter 14. Standalone	
Quick buttons.	63	application	79
Keyboard LED sync	64	Launching from Windows	79
Serial over LAN	64	Launching from Linux	79
Chapter 9. Image Redirection.	67	Launching from a GUI-based environment	82
Remote Media	67	Chapter 15. KVM OS and browser	
Chapter 10. Power Control	69	compatibility	85
Chapter 11. Maintenance	71	H5Viewer browser limitations	85
Backup BMC Configuration	71	Appendix A. Notices.	87
BMC Firmware Information	71	Trademarks	88
Download Service Data.	71		
Firmware Update	72		
Restore BMC Configuration	72		

Chapter 1. Introduction

The Lenovo baseboard management controller (BMC) is a service processor that provides the Intelligent Platform Management Interface (IPMI), H/W monitor, iKVM, VM, and Web-server functionality into a single chip on the server system board.

BMC features

BMC has the following features:

IPMI message interface support

- Keyboard controller style (KCS) interface
- Intelligent platform management bus (IPMB)
- LAN
- USB

Media redirection

- Simultaneous CD or DVD redirection
- Efficient USB 2.0-based CD/DVD redirection speed at the maximum of around 20XCD. Note that the speed varies depending on the method of communication (SSL or non-SSL). Refer to the VMedia performance analysis matrix for further information.
- Support for USB key
- Completely secured (authenticated or encrypted) remote KVM or VMedia

IPMI 2.0-based management

- BMC stack with a full IPMI 2.0 implementation
- Customizable sensor management
- IPMI thread management
- Support for reusing the space upon a SEL entry deletion
- LAN channel mapping via MDS
- Support for setting override using PDK hook

Event log and alerting

- Read log events
- Sensor readings
- SNMP traps
- E-mail alerts

Sophisticated user management

- IPMI-based user management
- Added security with SSL (HTTPS)
- Multiple user permission levels
- Multiple user profiles

LDAP support

- Direct LDAP support from the device
- Support for Open LDAP (Generic LDAP)

Remote server power control

- Server's power status report
- Support for remote server reset, power-on, power-off, and power cycle

SSH-based serial over LAN (SOL)

- Power control of the server
- Support for all DMTF profiles
- Complete command support
- Customizable parser for easy update to future modifications in grammar
- Dynamic target discovery
- Firmware update
- Role-based authentication and authorization
- Output filtering
- OEM command and target

Web-based configuration

- Full configuration using the Web UI
- Fail-safe firmware upgrade
- English as the currently supported language for the Web interface
- Extended node manager support

KVM/Media redirection support

- Low bandwidth video capture support (Pilot SoC)
- Auto video recording based on the event trigger
- Auto video recording prior to critical event (crash/reset) trigger
- Auto Recorded Video saved in the Remote share support
- Standalone Java client support for recorded video playback
- Auto resizing of the KVM/JViewer window to fit the client resolution (via a standalone Java client)
- Privilege support for KVM and VMedia
- IPMI Raw command support (via a standalone Java client)
- Single JAR for standalone App
- Keyboard mapping in KVM to send the correct codes as per host
- KVM localization using menu option in the client at runtime (via a standalone Java client)
- Recorded videos to be downloaded and playable in AVI format
- RMedia configuration using IPMI commands
- BSOD capture/view support
- HID sharing support to allow more than two concurrent sessions
- Power save mode support

KVM/Media redirection H5Viewer support

- Keyboard mapping in KVM to send the correct codes as per host
- Recorded videos to be downloaded and playable in AVI format
- HID sharing support to allow more than two concurrent sessions

Security support

- Encrypted password for AD/LDAP server authentication
- Web port for KVM/Media redirection

Multi-language support for Web and KVM

- Web pages are loaded based on the browser language settings.
- H5Viewer GUI language settings can be loaded based on the browser language settings (English and Simplified Chinese).

Miscellaneous

- Memory test support in u-boot
- Section-based flashing support via Web
- Support for auto reboot in case of abrupt cancellation during YAFU-based firmware update

Chapter 2. Accessing the BMC through TSM

BMC has a Web-based interface called the Lenovo ThinkSystem System Manager (TSM). Before accessing your BMC through TSM, you need to specify how the BMC will connect to the network.

Obtaining the BMC IP address

By default, the BMC will automatically search the DHCP server on the network to obtain an assigned IP address.

To view the IP address, perform the following steps:

1. Connect an Ethernet cable from the network to the BMC management Ethernet connector. If the management connector is unavailable, you can connect the server to the network through one of the Ethernet connectors on the OCP NIC adapter.
2. Attach a monitor to the server.
3. Power on the server.

The BMC IP address is displayed on the welcome page.

Alternatively, you can also set a static IP address by using Setup Utility:

1. Start the server. When you see **<F1> System Setup**, press F1 to open Setup Utility.
2. Go to **Server Mgmt → BMC network configuration**. Specify a static IP address for the BMC.

Logging in to TSM

After acquiring the BMC IP address, you can log in to TSM over your network to manage the BMC.

To log in to TSM, perform the following steps:

- Step 1. Enter the BMC IP address in the Web browser.
The login page is displayed.

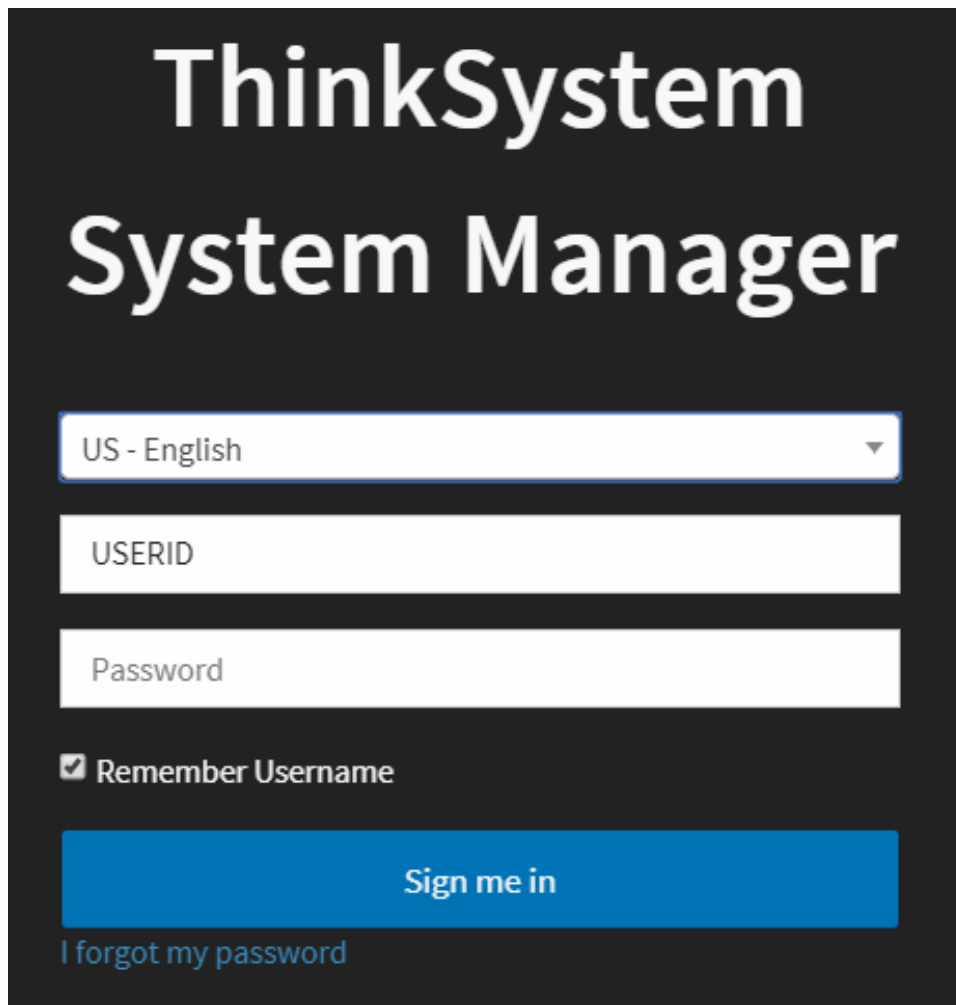


Figure 1. TSM login page

Note: TSM is accessible through standard Java-enabled Web browsers with HTTPS. For secure connection, TSM only supports HTTPS access. For example, enter `https://xx.xxx.xx.xxx` in the Web browser.

Step 2. On the login page, select the language, and enter the user name and password.

The fields are explained as follows:

- **US - English:** default language. You can switch to simplified Chinese or Japanese from the selection box.
- **Username:** Enter your user name in this field.
- **Password:** Enter your password in this field.

Notes: The default user name and password for TSM are:

- User name: USERID
- Password: PASSWORD (with a zero, not the letter O)
- **Remember Username:** Check this option to remember your login user name. If you select this option, the browser will save your credentials internally in its memory, and when you open that site the next time, it will auto-fill **Username** for you.

- **I forgot my password:** If you forget your password, you can generate a new password using this link.

Step 3. After entering the required credentials, click **Sign me in**.

Step 4. Optional: If you are logging in to TSM for the first time, change your password on the displayed page, and then click **Submit**.

**ThinkSystem
System Manager**

Enter a strong password consisting of at least one upper case letter, alpha-numeric characters, and special characters.

NOTE: Password field is mandatory and should have a minimum of 8 characters when SNMP status is enabled.

If enable Passwod Complex in Global Setting. Please follow the below rules:

- 1.No other characters (in particular, spaces or white-space characters) are allowed .
- 2.Must contain at least one letter.
- 3.Must contain at least one number.
- 4.contain at least 2 of the following :
 - An upper-case letter
 - A lower-case letter
 - A special character
- 5.Passwords may have no more than 2 consecutive instances of the same character.
- 6.Passwords must not be a repeat or reverse of the associated user ID.
- 7.Passwords must be a minimum of 8 and maximum of 20 characters long.
- 8.BMC prevent the same password.

New Password

Confirm Password

Submit

Figure 2. TSM password change page

Menu bar

The TSM menu bar displays the following information.

- **Firmware Information:** displays the latest version, date, and time details.

- **Host Online:** displays the power control status. To change the power control status, click the **Host Online** link.
- **Dashboard:** provides overall information about the status of the device.
- **System Inventory:** lists hardware used in the device.
- **Utilization:** describes the current and historical power consumption.
- **Logs & Reports:** provides logs and reports about the device, including:
 - **IPMI Event Log**
 - **Audit Log**
- **Settings:** allows you to access various configuration settings, such as system firewall, networking settings, and SSL settings.
- **Remote Control:** enables you to launch the H5Viewer or JViewer, and activate SOL.
- **Image Redirection:** supports to configure images into the BMC for redirection.
- **Power Control:** allows you to view and control the power of the device.
- **Maintenance:** provides available maintenance tasks for the device.
- **Sign out:** allows you to log out from TSM.

Quick buttons on the TSM main interface

The quick buttons and user information are located on the upper side of the TSM main interface.

Notes: Once you log in to the TSM WebUI, you are recommended not to use the following options:

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

Table 1. Quick buttons on the TSM main interface







Button	Description
	After you click this icon, the current page will be expanded to hide the left menu bar. To display the left menu bar, click this icon again.
	Click this icon to check the notifications received.
	Toggle between English and simplified Chinese to display.
 Refresh	Click this icon or press F5 to reload the current page.

Table 1. Quick buttons on the TSM main interface (continued)

Button	Description
 USERID ▾	<p>After your click this icon, user information will be displayed.</p> <ul style="list-style-type: none"> • Profile: The User Management Configuration page is displayed, where you can change the user configuration. • Sign out: To log out from TSM, click OK in the dialog box that is displayed. Alternatively, log out from TSM by using the Sign out function on the menu bar.
	<p>Click this icon in the upper right corner of a section or page to view its description.</p>

Chapter 3. Dashboard

Click **Dashboard** from the menu bar. The Dashboard page is displayed.

The Dashboard page gives the overall information about the status of the device.

System Health

This section displays the health status and quantity of the following components:

- Processor (CPU)
- Memory
- Local storage
- PCI adapter
- Power supply
- Fan
- System board
- Others

A green indicator shows that the hardware component is normal. If any of the hardware components is not operating normally, it will be marked by a red critical icon.

Click the name or quantity information of a component. You can enter the System Inventory page for more details.

System Information

This section provides a summary of common system information, including the date and time, product model, BMC version, and serial number.

Power Status/Control

This section provides a series of power-on or power-off options.

- **Power Switch:** Power on or off the server.
- **FP Switch:** Enable or disable the front panel.
- **Remote Console Control:** Access the operating system of the server.
- **NMI Button:** Trigger a non-maskable interrupt (NMI) event.

Network Information

This section provides a summary of the BMC management network and system network MAC addresses.

Temperature


This section provides the temperature reading and status (normal, warning, or critical) of key thermal components.

Chapter 4. System Inventory

Click **System Inventory** from the menu bar. The System Inventory page is displayed.

The System Inventory page displays information about the system hardware inventory and detailed information of active DIMM, PCIe, CPU, and other components.

Notes:

- Click  in the upper right corner of a hardware section to view the detailed information of the hardware.
- For the HDD, detailed information is available for drives (NVMe or SATA) that are connected from JSL1-9, and M2 on JSL8. There is no detailed information when the HDD is connected from a Switch, Retimer, and HBA/RAID card.

Chapter 5. Utilization

Click **Utilization** from the menu bar. The Utilization page is displayed.

The Utilization page displays the current output power consumption and historical power consumption in the past 1, 6, 12, or 24 hours. In addition, temperature, voltage, and fan speed detected by different sensors are displayed.

Pie chart for current output power consumption

- The center of the pie chart is the total available power.
- Different colors represent different power consumption categories. When you place the mouse cursor over a certain color, only this color and its legend are not grey. In addition, a tip is displayed, showing the percentage of power consumed by the category this color represents.

Line chart for historical power consumption

- Power consumption categories available in the selection box correspond to those depicted in the left pie chart, except for spare power.
- You can view the maximum, average, and minimum power consumption of the selected category in the past 1, 6, 12, or 24 hours.
- When you place the mouse cursor over the line chart, a tip is displayed, showing the maximum, average, and minimum power consumption of the selected category at the specific time point.

Temperature, voltage, and fan speed reading tables

In these tables, you can view the sensor status, reading, and different thresholds set for these sensors.

Chapter 6. Logs & Reports

The Logs & Reports page displays the following information:

- “IPMI Event Log” on page 17
- “Audit Log” on page 17

IPMI Event Log

Click **Logs & Reports** → **IPMI Event Log** from the menu bar. The IPMI Event Log page is displayed.

The IPMI Event Log page displays a list of event logs occurred on different sensors on this device. By default, all sensor events are listed, with the severity, common ID, sensor name, sensor type, description, status, and event time displayed. To view specific events, you can specify the time range, or specify the event type and sensor name to filter the events.

Fields on the IPMI Event Log page

This page consists of the following fields:

- **Filter by Date:** Filtering can be done by selecting **Start Date** and **End Date** using the calendar. The events will be displayed according to the selected date.

Notes:

- Date should be in MM/DD/YYYY format.
- By default, all log time will be displayed in BMC time zone.

- **Filter by type:** Select a specific event type and sensor name to view corresponding events in the selected time period.

Notes:

- Once **Filter By Date** and **Filter by type** are selected, the list of events will be displayed with the event ID, time stamp, severity, common ID, sensor type, sensor name, status, and description.
- For events not generated by the BMC, **Severity** and **Common ID** are displayed as **N/A**; for events generated by the BMC, the event severity and message ID are displayed.
- **UTC Offset:** Display the current UTC offset value based on which event time stamps will be updated.
- **Clear Event Logs:** Delete all the event logs.
- **Download Event Logs:** Download the event logs.

Note: The maximum number of IPMI event log records is about 3000. When the event logs are full, the new log entry will automatically overwrite the oldest one.

Audit Log

Click **Logs & Reports** → **Audit Log** from the menu bar. The Audit Log page is displayed.

The Audit Log page displays all the audit events occurring in this device. Entries can be filtered based on **Filter By Date (Start Date and End Date)**.

Note: The maximum number of audit log records is 300. When the audit logs are full, the new log entry will automatically overwrite the oldest one.

Chapter 7. Settings

Click **Settings** from the menu bar. The Settings page is displayed.

The Settings page allows you to access various configuration settings.

Captured BSOD

This section displays a snapshot of the blue screen captured at the time if the host system crashed since the last reboot.

To open the Captured BSOD page, click **Settings → Captured BSOD**.

Note: The KVM service should be enabled to display the BSOD screen. The KVM service can be configured under **Settings → Services → KVM**.

Date & Time

This section is used to set the date and time on the BMC.

To open the Date & Time page, click **Settings → Date & Time**.

The Date & Time section consists of the following fields:

- **Configure Date & Time:** This pane displays the 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:** This field is used to set the date and time on the BMC.
- **Automatic NTP Date & Time:** Select this option to automatically synchronize date and time with the NTP Server.
 - **Primary NTP Server:** Configure a primary NTP server to use when automatically setting the date and time.
 - **Secondary NTP Server:** Configure a secondary NTP server to use when automatically setting the date and time.
- **Save:** Saving the settings.

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 you save the settings.

Procedure

1. Select the time zone location either using the drop-down list box or the map.
2. Enable **Automatic NTP Date & Time** to enable or disable the use of NTP servers to automatically set the date and time.
 - In the **Primary NTP Server** and **Secondary NTP Server** fields, specify the NTP servers of the device respectively.

Note: **Secondary NTP server** is an optional field. If the **Primary NTP Server** is not working fine, then the **Secondary NTP Server** will be tried.
3. Click **Save** to save the settings.

External User Services

LDAP/E-Directory Settings

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

On the TSM GUI, LDAP is an Internet protocol that the BMC 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 BMC 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 BMC. Since your existing LDAP server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user- or group-based policies to control access.

To open the LDAP/E-Directory Settings page, click **Settings** → **External User Services** → **LDAP/E-Directory Settings**.

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

- **General Settings:** Configure LDAP/E-Directory settings, including whether to enable LDAP/E-Directory authentication, encryption type, and server address.
- **Role Groups:** Modify the configuration of a configured role group, click a free slot to add a role group, or delete a role group.

Configuring general LDAP settings

1. On the LDAP/E-Directory Settings page, click **General Settings**.
2. Select or clear the check box of **Enable LDAP/E-Directory Authentication** to enable or disable LDAP/E-Directory authentication.

Note: All the other fields can be set only after **Enable LDAP/E-Directory Authentication** is selected.

3. Select the encryption type for LDAP/E-Directory from the **Encryption Type**.

Note: Configure a proper port number if SSL is enabled.

4. Select the **Common Name Type** as **IP Address**.
5. Enter the IP address of LDAP/E-Directory server in the **Server Address** field.

Notes:

- IPv4 and IPv6 address formats are supported.
- Configure a fully qualified domain name (FQDN) address when using StartTLS with FQDN.

6. Specify the LDAP/E-Directory port in the **Port** field.

Notes:

- The default port number is 389. For SSL connections, the default port number is 636.
- The value of **Port** ranges from 1 to 65535.
- Port 80 is blocked for TCP and UDP protocols.

7. Specify the **Binding Method** that is used during bind operations.

Notes:

- **Pre-configured Credential** can keep Bind DN and password used to authenticate the client to the server.
 - **Login Credential** requires the client to input Bind DN and password during runtime.
8. Enter the password in the **Password** field, which is also used in the bind authentication operation between the client and server.

Notes:

- A password must contain 1 to 48 characters.
 - White space is not allowed.
9. Enter the **Search Base**. The search base allows the LDAP/E-Directory server to find which part of the external directory tree is to be searched. This search base may be equivalent to the organization or the group of the external directory.

Notes:

- **Search Base** is a string of 4 to 64 alpha-numeric characters that must start with an alphabetical character.
 - Special symbols such as dot (.), comma (,), hyphen (-), underscore (_), and equal-to (=) are allowed.
 - Example: ou=login,dc=domain,dc=com
10. Select **Attribute of User Login** to find the LDAP/E-Directory server which attribute should be used to identify the user.

Note: Only **cn** or **uid** is supported.

11. Select the **CA Certificate File** that contains 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 of the 3 files are required when **StartTLS** is enabled.


14. Click **Save** to save the settings.

Adding, deleting, or modifying a role group

1. On the LDAP/E-Directory Settings page, click **Role Groups**.

The Role Groups page is displayed.

Note: Free or unconfigured slots are denoted by the word 'None'.

2. Select the role group you want to delete or modify, or select a free slot to add a role group.
 - To delete a role group from the list, click  in the upper right corner.
 - To modify a role group, click its name.
 - To add a role group, click a free slot.
3. On the role group configuration page, modify the existing configurations or define configurations for a new role group.

The role group configurations are described as follows:

- **Group Name:** Enter the role group name. This name identifies the role group in LDAP/E-Directory.
 - A group name is a string of 64 alpha-numeric characters.
 - Special symbols hyphen (-) and underscore (_) are allowed.
- **Group Domain:** Enter the role group domain. This is the domain where the role group is located.

- A domain name is a string of 4 to 64 alpha-numeric characters that must start with an alphabetical character.
 - Special symbols like dot (.), comma (,), hyphen (-), underscore (_), and equal-to (=) are allowed.
 - Example: cn=manager,ou=login,dc=domain,dc=com
 - **Group Privilege:** Enter the role group privilege. This is the level of privilege to be assigned for this role group.
- Note:** OEM permissions are the same as administrator permissions.
- **KVM Access:** Select or clear this check box to enable or disable KVM access.
 - **VMedia Access:** Select or clear this check box to enable or disable VMedia access.

4. Click **Save**.

Active Directory Settings

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

In TSM application, Active Directory allows you to configure the Active Directory server settings. The displayed table shows any configured role groups and the available slots. You can modify, add, or delete role groups from here. A group domain can be the AD domain or a trusted domain. A group name should correspond to the name of an actual AD group.

To open the Active directory Settings page, click **Settings → External User Services → Active Directory Settings**.

Notes:

- To view the page, you must be at least a user.
- To modify or add a group, you must be an administrator.

The fields of the Active directory Settings page are explained below.

- **General Settings:** Configure general active directory settings, including whether to enable active directory authentication, secret username, secret password, and user domain name.
- **Role Groups:** Modify the configuration of a configured role group, click a free slot to add a role group, or delete a role group.

Configuring general active directory settings

1. On the Active directory Settings page, click **General Settings**.

The General Active Directory Settings page is displayed.

2. Select or clear the check box of **Enable Active Directory Authentication** to enable or disable active directory authentication.

Note: If you have enabled active directory authentication, enter the required information to access the Active Directory server.

3. Specify the user name of an administrator of the Active Directory server.

Notes:

- **Username** is a case-sensitive string of 1 to 64 alpha-numeric characters that must start with an alphabetical character.
 - Special characters and spaces are not allowed.
 - If **Secret Username** and **Secret Password** are not needed, both fields can remain blank. However, this will affect the ability to reorder the PAM sequence.
4. Specify the password of the administrator.

Notes:

- **Password** is a string of 6 to 127 characters.
 - White space is not allowed.
5. Specify the **User Domain Name** field, for example, MyDomain.com.
 6. 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.
 - IPv4 and IPv6 address formats are supported.
7. Click **Save** to save the settings.

Adding, modifying, or deleting a role group

1. On the Active directory Settings page, click **Role Groups**.

The Role Groups page is displayed.

Note: Free or unconfigured slots are denoted by the word 'None'.

2. Select the role group you want to delete or modify, or select a free slot to add a role group.
 - To delete a role group from the list, click  in the upper right corner.
 - To modify a role group, click its name.
 - To add a role group, click a free slot.
3. On the role group configuration page, modify the existing configurations or define configurations for a new role group.

The role group configurations are described as follows:

- **Group Name:** Enter the role group name. This name identifies the role group in Active Directory.
 - A group name is a string of 64 alpha-numeric characters.
 - Special symbols hyphen (-) and underscore (_) are allowed.
 - **Group Domain:** Enter the role group domain. This is the domain where the role group is located.
 - A domain name is a string of 255 alpha-numeric characters.
 - Special symbols hyphen (-), underscore (_), and dot (.) are allowed.
 - **Group Privilege:** Enter the role group privilege. This is the level of privilege to be assigned for this role group.
 - **KVM Access:** This field provides access to KVM for AD authenticated role group users
 - **VMedia Access:** This field provides access to VMedia for AD authenticated role group users.
4. Click **Save**.

RADIUS Settings

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

On the TSM GUI, the RADIUS Settings page is used to set the RADIUS authentication

To open the RADIUS Settings page, click **Settings → External User Services → RADIUS Settings**.

The fields of the RADIUS Settings page are explained below.

- **General RADIUS Settings:** Configure general RADIUS settings, including whether to enable RADIUS authentication, server address, port number, and secret.
- **Advanced RADIUS Settings:** Configure advanced RADIUS authorization settings, including the administrator, operator, user, and OEM proprietary.

Configuring general RADIUS settings

1. On the RADIUS Settings page, click **General RADIUS Settings**.

The General RADIUS Settings page is displayed.

2. Select or clear the check box of **Enable RADIUS Authentication** to enable or disable RADIUS authentication.

Note: All the other fields can be set only after **Enable RADIUS Authentication** is selected.

3. Specify the RADIUS server address.

Note: IPv4, IPv6, and FQDN address formats are supported.

4. Specify the RADIUS port number.

Notes:

- The default port number is 1812.
- The value of **Port** ranges from 1 to 65535.
- Port 80 is blocked for TCP and UDP protocols.

5. Specify the RADIUS server secret.

Notes:

- A secret must contain 4 to 32 characters.
- White space is not allowed.

6. Select or clear the check box of **Enable KVM Access** to enable or disable KVM access. This option provides access to KVM for RADIUS authenticated users.

7. Select or clear the check box of **Enable VMedia Access** to enable or disable VMedia access. This option provides access to VMedia for RADIUS authenticated users.

8. Click **Save** to save the settings.

Configuring advanced RADIUS settings

1. On the RADIUS Settings page, click **Advanced RADIUS Settings**.

The Advanced RADIUS Settings page is displayed.

2. For authorization purposes, configure vendor-specific attributes for the RADIUS users on the server.

Example:

- Add vendor-specific attributes:

```
cd/usr/share/freeradius
vim dictionary.adtest
(Add the content below)

# dictionary.adtest

VENDOR ADTest 58

# Standard attribute

BEGIN-VENDOR ADTest

ATTRIBUTE ADTest-group 1 string

END-VENDOR ADTest

vim dictionary
(Add this line)

$INCLUDE dictionary.adtest
```

- Add users:

```
vim users
(Add the content below)

"RadiusTest1" Cleartext-Password := "000000"

Service-Type = Administrative-User,

Auth-Type := System,

ADTest-group := "H=4"
```

Note: These fields will not allow more than 127 characters. '#' is not allowed.

3. Click **Save** to save the settings.

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 view the supported operating systems for mouse modes, see “Supported operating systems for mouse modes” on page 26.

To open the KVM Mouse Settings page, click **Settings → KVM Mouse Settings**.

The fields of the KVM Mouse Settings page are explained below.

- **Relative Positioning (Linux):** Relative mode sends the calculated relative mouse position displacement to the server.
- **Absolute Positioning (Windows):** The absolute position of the local mouse is sent to the server. This mode is recommended for Windows or later Linux releases.
- **Other Mode (SLES-11 OS Installation):** This option sends the calculated displacement from the local mouse in the center position to the server.
- **Save:** Save the configuration.

Supported operating systems for mouse modes

Table 2. Supported operating systems for mouse modes

Host OS	Mouse Mode
Windows server 2016	Absolute
Windows server 2016 R2	Absolute
RSLES server 12.1	Absolute
SLES server 11.4	Absolute
RHEL 7.3	Absolute
Ubuntu server 16.04	Absolute
Ubuntu server 14.04	Absolute

Remote Log Settings

This section allows you to configure the function of saving logs in a remote machine.

To open the Remote Log Settings page, click **Settings → Remote Log Settings**.

The fields of the Remote Log Settings page are explained below.

- **Remote Log:** Check this option to enable the function of saving logs in a remote machine.
- **Port Type:** This field is available if **Remote Log** is enabled. **UDP** and **TCP** port types are supported.
- **Remote Log Server:** This field specifies the address of the remote server to log system events, which supports the IP address (IPv4 or IPv6) and FQDN formats.
- **Remote Server Port:** This field specifies the port to log system events.

Note: If the port number is set to 0, the default port will be used, which is port 514.

Media Redirection Settings

This section is used to configure the media into BMC for redirection.

To open the Media Redirection page, click **Settings → Media Redirection Settings**.

The fields of the Media Redirection page are explained below.

- “General Settings” on page 26
- “VMedia Instance Settings” on page 27
- “Remote Session” on page 28
- “Active Redirections” on page 28

General Settings

This section is used to configure general media settings.

To open the General Settings page, click **Settings → Media Redirection Settings → General Settings**.

On the General Settings page, the following check box is displayed:

Remote Media Support: Select or clear this check box to enable or disable remote media support.

If it is selected, the following remote media types will be displayed:

- CD/DVD
- Hard disk

On selecting the individual media types, its respective configurations will be displayed. You can configure different settings for different remote media types. Alternatively, the same configurations can be applied to both media types by using the check box of **Same settings for Harddisk Images**.

The following page shows the configurations for different media types.

The fields of the General Settings page are explained below.

- **Same settings for Harddisk Images:** If this check box is selected, the server information entered for the CD/DVD media type will be applied to the hard disk media type as well.
- **Server Address for Harddisk Images:** Address of the server where remote media images are to be stored. IPv4, IPv6, and FQDN address formats are supported.
- **Path in server:** Source path to the remote media images.

Note: A path must be alpha-numeric and only the following special characters are allowed: backward slash (\), forward slash (/), hyphen (-), underscore (_), dot (.), and colon (:).

- **Share Type for Harddisk:** Select **nfs** or **cifs**.
- **Domain Name, Username, and Password:** If the share type is Samba (CIFS), enter user credentials to authenticate on the server.
- **Retry Interval:** Enter the retry interval to reconnect RMedia. The value ranges from 15 (default) to 30.
- **Retry Count:** Enter the retry count to reconnect RMedia. The value ranges from 3 (default) to 6.
- **Save:** Save the settings.

Note: For RMedia share types, we support the following NFS and CIFS mount protocols, for mounting remote image share paths to the BMC.

Protocol	Versions
NFS	NFSv2, NFSv3, NFSv4
CIFS	SMBv1, SMBv2.1

VMedia Instance Settings

This section is used to configure virtual media device settings.

To open the VMedia Instance Settings page, click **Settings → Media Redirection Settings → VMedia Instance Settings**.

The fields of the VMedia Instance Settings page are explained below.

- **Remote CD/DVD device instances:** Number of CD/DVD devices supported for virtual media redirection.
- **Remote Hard disk instances:** Number of hard disk devices supported for virtual media redirection.
- **Remote KVM CD/DVD device instances:** Number of remote KVM CD/DVD devices supported for virtual media redirection.
- **Remote KVM Hard disk instances:** Number of remote KVM hard disk devices supported for virtual media redirection.
- **Power Save Mode:** Select this check box to enable power save mode for the BMC.

- **Save:** Save the settings.

Remote Session

This section is used to configure remote session settings.

To open the Remote Session page, click **Settings → Media Redirection Settings → Remote Session**.

The fields of the Remote Session page are explained below.

- **KVM Single Port Application:** This option is used to enable or disable single port support by runtime. On changing this configuration, KVM and media sessions will be stopped, and the respective video and media server will be restarted. If this support is enabled, the KVM session will not use its dedicated port whereas both Web and KVM sessions will be established only via the Web port.
- **Keyboard Language:** This option is used to select the keyboard supported languages.
- **Retry Count:** This value specifies the number of attempts the KVM client will make to reconnect the KVM session. The retry count value ranges from 1 to 20.
- **Retry Time Interval(Seconds):** This value specifies the time duration between two consecutive reconnection attempts. The KVM client will wait for a time interval equal to this value, after making a reconnection attempt, before trying to connect again. The retry interval value is mentioned in seconds and it ranges between 5 to 30 seconds.
- **Server Monitor OFF Feature Status:** This option is used to enable or disable Server Monitor OFF.
 - If this option is enabled, you can lock or unlock the local host monitor from the remote KVM window.
 - If this option is disabled, you cannot lock or unlock the local host monitor from the remote KVM window.
- **Automatically OFF Server Monitor, When KVM Launches:** This option is available only when **Server Monitor OFF Feature Status** is enabled. You can use this option to enable or disable Automatically OFF Server Monitor when KVM launches.
- **Save:** Save the settings.

Note: Upon clicking **Save** after enabling or disabling **KVM Single Port Application**, the opened remote KVM viewer will automatically close.

Active Redirections

This section is used to display the active redirected media, which are redirected via JViewer, VMAPP, H5Viewer, LMedia, RMedia, or VMCLI. Information like **Media Type**, **Media Instance**, **Client Type**, **Image Name**, **Redirection Status**, and **Client IP** will be displayed.

To open the Active Redirections page, click **Settings → Media Redirection Settings → Active Redirections**.

The fields of the Active Redirections page are explained below.

- **Media Type:** type of media
- **Media Instance:** number of media devices
- **Client Type:** type of media devices
- **Image Name:** name of the image supported by media devices
- **Redirection Status:** media status
- **Client IP:** IP address of the connected media devices

Note: Local or remote media connections will use the loopback socket for communication. Therefore, a tilde (~) will be displayed for a loopback IP (127.0.0.1 (or) ::1) on the media session information page.

Network Settings

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

To open the Network Settings page, click **Settings → Network Settings**.

The fields of the Network settings page are explained below.

- “Network IP Settings” on page 29
- “Network Bond Configuration” on page 30
- “Network Link Configuration” on page 30
- “DNS Configuration” on page 31
- “Sideband Interface (NC-SI)” on page 32

Network IP Settings

This section is used to configure network IP settings.

To open the Network IP Settings page, click **Settings → Network Settings → Network IP Settings**.

The fields of the Network IP Settings page are explained below.

- **Enable LAN:** This option is used to enable or disable LAN support for the interface configured below.
- **LAN Interface:** This option is used to select the LAN interface to be configured.
- **MAC Address:** This field displays the read-only MAC address of the selected interface.
- **Enable IPv4:** This option is used to enable or disable IPv4 support for the selected interface.
- **IPv4 Method:** Choose a method you want to use among **Static IP address**, **DHCP**, and **First DHCP, then static IP address**.
 - If **Static IP address** is selected, configure static **IPv4 Address**, **IPv4 Subnet**, and **IPv4 Gateway**.

Notes:

- An IP address consists 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.
- If **DHCP** is selected, current IPv4 address, IPv4 subnet, and IPv4 gateway are displayed.
- If **First DHCP, then static IP address** is selected, current IPv4 address, IPv4 subnet, and IPv4 gateway are displayed. You can also configure **IPv4 Address**, **IPv4 Subnet**, and **IPv4 Gateway** if necessary.
- **Enable IPv6:** This option is used to enable or disable IPv6 support for the selected interface.
- **Enable IPv6 DHCP:** If this option is enabled, an IPv6 address is dynamically configured using DHCP.
- **IPv6 Index, IPv6 Address, Subnet Prefix Length, and IPv6 Gateway:** These fields need to be manually configured when **Enable IPv6 DHCP** is disabled.

Notes:

- **IPv6 Index:** Configure a static IPv6 index for the device, for example, 0.
- **IPv6 Address:** Configure a static IPv6 address for the device, for example, 2004::2010.

- **Subnet Prefix Length:** Specify the subnet prefix length for the IPv6 settings. The value ranges from 0 to 128.
- **IPv6 Gateway:** Specify an IPv6 gateway for the selected interface.
- **Enable VLAN:** This option is used to enable or disable VLAN support for the selected interface.
- **VLAN ID and VLAN Priority:** These fields need to be manually configured when **Enable VLAN** is enabled.

Notes:

- **VLAN ID:** The value ranges from 1 to 4094, and 0 and 4095 are reserved IDs. **VLAN ID** cannot be changed without resetting the VLAN configuration.
- **VLAN Priority:** The value ranges from 0 to 7.
- **Save:** Save the settings.

Network Bond Configuration

This section is used to configure the network bonding settings for the network interfaces.

To open the Network Bond Configuration page, click **Settings → Network Settings → Network Bond Configuration**.

The fields of the Network Bond Configuration page are explained below.

- **Enable Bonding:** This option is used to enable or disable bonding for the network interfaces.
- Note:** If VLAN is enabled for either slave interface, then bonding cannot be enabled. VLAN can be disabled under **Settings → Network Settings → Network IP Settings**.
- **Auto Configuration:** This option is used to enable or disable automatic interface configuration.

Notes:

- If this option is enabled, all the services will restart automatically.
 - If this option is disabled, the interfaces in service can be configured via IPMI commands.
 - **Bond Interface:** This option is used to configure bonding for the network interfaces.
- Note:** A minimum of two network interfaces is required to enable network bonding for the device.
- **Bond Mode:** This field displays the network bonding mode and cannot be configured.
 - **Save:** Save the settings.

Network Link Configuration

This section is used to configure the network link settings for available network interfaces.

To open the Network Link Configuration page, click **Settings → Network Settings → Network Link Configuration**.

The fields of the Network Link Configuration page are explained below.

- **LAN Interface:** Select the required network interface from the list for which the link speed and duplex mode are to be configured.
- **Auto Negotiation:** This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link.

Note: The **Link Speed** and **Duplex Mode** will be active only when **Auto Negotiation** is disabled.

- **Link Speed:** Link speed options depend on the network interface capabilities, which can be 10, 100, or 1000 Mbps.

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

- **Duplex Mode:** This field could be either **Half Duplex** or **Full Duplex**.
- **NCSI Interface:** The NCSI interface status could be either **Enabled** or **Disabled** for the selected LAN interface.
- **Save:** Save the settings.

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 Configuration page is used to manage the DNS settings of the device.

To open the DNS Configuration page, click **Settings** → **Network Settings** → **DNS Configuration**.

The fields of the DNS Configuration page are explained below.

Domain Name Service Configuration

- **DNS Enabled:** Enable or disable all the DNS service configurations.
- **mDNS Enable:** Enable or disable multicast DNS.
- **Host Name Settings:** Choose either **Automatic** or **Manual** settings.
- **Host Name:** It displays the host name of the device.
 - If the host name setting is chosen as **Automatic**, the host name is automatically displayed.
 - If the host name setting is chosen as **Manual**, specify the host name of the device.

Note: A host name consists of 1 to 64 alpha-numeric characters and must not start or end with a hyphen (-). Special characters hyphens (-) and underscores (_) are allowed. IE browsers won't work correctly if any part of the host name contains underscores (_).

BMC Registration Settings

- **BMC Interface:** Options to register the BMC through the interfaces **share** and **dedicated**.
- **Register BMC:** Register BMC through a registration method.
- **Registration method:**
 - **Nsupdate:** Register with the DNS server using the nsupdate application.
 - **DHCP Client FQDN:** Register with the DNS server using DHCP option 81.
 - **Hostname:** Register with the DNS server using DHCP option 12.

Note: The **Hostname** method should be selected if the DHCP server does not support option 81, and the **Hostname** method does not support an IPv6 domain interface.

TSIG Configuration

- **Both:** Select this check box to modify TSIG authentication for both interfaces.
- **share & dedicated TSIG Configuration**

- **TSIG Authentication Enabled:** Select this check box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.
 - **Current TSIG Private File:** Display the information of the current TSIG private file along with its uploaded date and time, which is read-only.
 - **New TSIG Private File:** Browse and navigate to the TSIG private file.
 - **Domain Setting:** Select whether the domain interface will be configured manually or automatically.
 - **Automatic:** If you select **Automatic**, specify the domain interface. The domain name cannot be configured as it will be done automatically.
 - **Manual:** If you select **Manual**, specify the domain name of the device.
- Note:** If you select **Automatic**, it displays the **Domain Interface** option. If you select **Manual**, it displays **Domain name**.
- **Domain Interface or Domain name:** Specify the domain interface or domain name of the device.

Domain Name Server Setting

- **Automatic:** If you select **Automatic**, specify the DNS interface to be used.
- **Manual:** If you select **Manual**, specify the DNS server address to be configured for the BMC.
- **IP Priority:**
 - **IPv4:** 2 IPv4 DNS servers and 1 IPv6 DNS server can be used.
 - **IPv6:** 1 IPv4 DNS server and 2 IPv6 DNS servers can be used
- **DNS Server 1, 2, & 3:**

Specify the DNS server address to be configured for the BMC.

Notes:

- IPv4 and IPv6 address formats are supported.
- IPv4 addresses should be given in dotted decimal representation.
- IPv6 addresses are supported and must be global unicast addresses.
- **Save:** Save the settings.

Sideband Interface (NC-SI)

This section is used to configure Network Controller Sideband Interface (NCSI) settings.

To open the Sideband Interface (NC-SI) page, click **Settings → Network Settings → Sideband Interface (NC-SI)**.

The fields of the Sideband Interface (NC-SI) page are explained below.

- **NCSI Mode:**
 - If you select **Auto Failover Mode**, the NCSI interface and other settings will be configured automatically.
 - If you select **Manual Switch Mode**, you are allowed to configure the below settings.
- **NCSI Interface:** Select the NCSI interface for which you need to configure NCSI settings.
- **Package ID:** Select the package ID to be configured for the selected interface.
- **Channel Number:** Select the channel number to be configured for the selected interface.
- **Save:** Save the settings.

PAM Order Settings

This section is used to configure the PAM ordering for user authentication into the BMC.

To open the PAM Order page, click **Settings → PAM Order Settings**.

A list of PAM modules supported in the BMC is displayed.

Procedure

- Step 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.
- Step 2. Click **Save** to save any changes.

Note: Whenever the configuration is modified, the Web server will be restarted automatically. The logged-in session will be logged out.

Platform 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.

To open the Platform Event Filters page, click **Settings → Platform Event Filters**.

The fields of the Platform Event Filters page are explained below.

- “Event Filters” on page 33
- “Alert Policies” on page 35
- “LAN Destinations” on page 35

Event Filters

A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, and fan failure events. Remaining entries can be made available for events configured through OEM or system management software. Note that individual entries can be tagged as being reserved for system use, so this ratio of pre-configured entries to runtime configurable entries can be reallocated if necessary.


To open the Event Filters page, click **Settings → Platform Event Filters → Event Filters**.

By default, 15 event filter entries are configured among the 40 available slots.

- Select **All** to view available configured and unconfigured slots.
- Select **Configured** or **Unconfigured** to view available configured or unconfigured slots.

Supported operations on event filters

Event Filters allows you to delete, modify, or add event filter entries.

- To delete an event filter entry from the list, click  in the upper right corner.
- To modify a configured event filter entry, click the entry to enter the Event Filter Configuration page and then modify its configurations.

- To add an event filter entry, select a free slot to open the Event Filter Configuration page and then set its configurations.

Event Filter Configuration

The Event Filter Configuration page includes the following configurations.

- **Enable this filter:** Select this check box to enable the PEF settings.
- **Event Severity to trigger:** Select any one of the event severities from the list.
- **Event Filter Action Alert:** This option is enabled by default, which means to enable the PEF alert action.
- **Power Action:** Select a desired power action.
- **Alert Policy Group Number:** Configure the number of alert policies.

Note: Alert policies can be configured under **Settings → Platform Event Filters → Alert Policies**.

- **Raw Data:** Select this check box to fill the **Generator ID** with raw data.
- The **Generator ID 1** field is used to give raw generator ID1 data value.
- The **Generator ID 2** field is used to give raw generator ID2 data value.

Note: In the raw data fields, prefix the value with '0x' to specify a hexadecimal value.

- **Generator Type:**
 - Select **Slave** if events were generated from IPMB.
 - Select **Software** if events were generated from system software.
- **Slave Address/Software ID:** Specify the corresponding I2C slave address or system software ID.
- Select the particular **Channel Number** that event messages were received over. Alternatively, select **0** if the event messages were received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding **IPMB Device LUN** if events were generated by IPMB.
- Select the **Sensor type** of sensors that will trigger the event filter action.
- **Sensor name:** Select the particular sensor from the sensor list.
- Choose **Event Options** to be either all events or sensor-specific events.
- The **Event trigger** field is used to give Event/Reading type value, ranging from 0 to 255.
- The **Event Data 1 AND Mask** field is used to indicate wildcarded or compared bits, ranging from 0 to 255.
- The **Event Data 1 Compare 1** and **Event Data 1 Compare 2** fields are used to indicate whether each bit position's comparison is an exact comparison or not. Both values range 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

Click **Save** to save the changes and return to the event filter list.

Click **Delete** to delete the existing filter.

Alert Policies


This section is used to configure alert policies for the PEF configuration. You can add, delete, or modify an entry on this page.

To open the Alert Policies page, click **Settings → Platform Event Filters → Alert Policies**.

By default, all configured alert policies and available slots are displayed, and a maximum of 60 slots are available.

Supported operations on alert policies

Alert Policies allows you to delete, modify, or add alert policies.

- To delete an alert policy from the list, click  in the upper right corner.
- To modify a configured alert policy, click the policy to enter the alert policy configuration page and then modify its configurations.
- To add an alert policy, select a free slot to open the alert policy configuration page and then set its configurations.

Alert policy configuration

The alert policy configuration page includes the following configurations.

- **Policy Group Number:** Select a policy number that was configured in the event filter table.
- **Enable this alert:** Select this check box to enable the policy settings.
- **Policy Action:** Select any one of the policy set values (0–4) from the list.
 - 0: Always send alert to this destination.
 - 1: If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set.
 - 2: If alert to previous destination was successful, do not send alert to this destination. Do not process any more entries in this policy set.
 - 3: If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different channel.
 - 4: If alert to previous destination was successful, do not send alert to this destination. Proceed to next entry in this policy set that is to a different destination type.
- **LAN Channel:** Select a particular channel from the available channel list.
- **Destination Selector:** Select a particular destination from the configured destination list.

Note: LAN destinations have to be configured under **Settings → Platform Event Filters → LAN Destinations**.

- **Event Specific Alert String:** Specify an event-specific alert string.
- **Alert String Key:** Specify which string is to be sent for this alert policy entry.

Click **Save** to save the changes and return to the alert policy list.

Click **Delete** to delete the alert policy.

LAN Destinations



This section is used to configure the LAN destinations of PEF configuration.

To open the LAN Destinations page, click **Settings → Platform Event Filters → LAN Destinations**.

By default, all LAN destination slots are displayed, and a maximum of 15 slots are available.

Supported operations on LAN destinations

LAN Destinations allows you to modify, add, or delete LAN destinations.

- To delete a configured LAN destination, click  in the upper right corner.
- To modify a configured LAN destination, click the entry to enter the LAN Destination Configuration page and then modify its configurations.
- To add a LAN destination, select a free slot to open the LAN Destination Configuration page and then set its configurations.
- Click  to send sample alerts to the configured destination. Note that test alerts can be sent only with enabled SMTP configuration. This can be done under **Settings → SMTP Settings**. Make sure that the SMTP server address and port numbers are configured properly.

LAN Destination Configuration

The LAN Destination Configuration page includes the following configurations.

- **LAN Channel:** Displays the LAN channel number for the selected slot, which is read-only.
- **LAN Destination:** Displays the destination number of the selected slot, which is read-only.
- **Destination Type:** Destination type can be either an **SNMP Trap** or an **E-mail** alert.
- **SNMP Destination Address:** If **Destination Type** is **SNMP Trap**, then provide the IP address of the system that will receive the alert. IPv4 and IPv6 address formats are supported.
- **BMC User Name:** If **Destination Type** is **E-Mail**, then choose the user to whom the e-mail alert has to be sent.

Note: The e-mail address for the user has to be configured under **Settings → User Management**.

- **Email Subject** and **Email Message:** These fields must be configured if e-mail alert is chosen as the destination type. An e-mail will be sent to the configured e-mail address of the user in case of any severity events with a subject specified in subject field and will contain the message field's content as the e-mail body. These fields are not applicable for AMI-Format e-mail users.

Click **Save** to save the changes and return to the LAN destination list.



Click **Delete** to delete the LAN destination.

Services

This section lists services running on the BMC and provides the current status and other basic information about each service. Only an administrator user can modify a service.

To open the Services page, click **Settings → Services**.

Notes:

- Click  to modify the service configuration.
- Click  to view or terminate the connected session for this service.

The fields of the Services page are explained below.

- **Service:** service name of the selected slot, which is read-only.
- **Status:** current status of the service, either active or inactive.
- **Interfaces:** interface on which the service is running.

Notes:

- Services mapping to disabled interfaces will not work.
- Media and KVM interfaces are read-only when the single port is enabled. To change the interfaces, disable the feature of **KVM Single Port Application**.
- **Secure Port:** secure port for the service. Port value ranges from 1 to 65535. Default port configurations for different services are as follows:
 - Web: 443
 - KVM: 7582
 - CD media: 5124
 - HD media: 5127
 - SSH: 22

Notes:

- Port 80 is blocked for TCP and UDP protocols. To view the port listening status on various feature settings, see “Port listening status on various feature settings” on page 37.
- Media and KVM interfaces are read-only when the single port is enabled. To change the interfaces, disable the feature of **KVM Single Port Application**.
- **Timeout:** session timeout value of the service.
 - Web and KVM timeout value ranges from 300 to 1800 seconds.
 - Web timeout will be ignored if there is any ongoing KVM session.
 - SSH timeout value ranges from 60 to 1800 seconds.
 - Timeout value should be in multiples of 60 seconds.
- **Maximum Sessions:** maximum number of allowed sessions for the service.

Port listening status on various feature settings

Table 3. Port listening status on various feature settings

Server	Single port enabled	Single port disabled	Only KVM encryption enabled	Only Media encryption enabled	Both KVM and Media encryption enabled
Adviser (video server)	7578 (LP)	7578 (LP) 7578 (EO)	7578 (LP) 7582 (EO)	7578 (LP) 7578 (EO)	7578 (LP) 7582 (EO)
Cdserver	5120 (LP)	5120 (LP) 5120 (EO)	5120 (LP) 5120 (EO)	5120 (LP) 5124 (EO)	5120 (LP) 5124 (EO)
Hdserver	5123 (LP)	5123 (LP) 5123 (EO)	5123 (LP) 5123 (EO)	5123 (LP) 5127 (EO)	5123 (LP) 5127 (EO)


Notes:

- **LP** indicates loopback and **EO** indicates exposed outside.

- The adviser will always be listening to loopback as well as KVM-configured interfaces as mentioned in the above table, so that the H5Viewer client can connect to the video server.
- The media servers will be listening to loopback as well as configured interfaces as mentioned in the above table, so that the LMedia/RMedia and H5Viewer/JViewer client can connect to the media servers.

Modifying the configurations of a service

To modify the configurations of a service, perform the following steps:

Step 1. On the Settings page, click  in the same row as the service for which you want to modify its configurations.
The Service Configuration page is displayed.


Step 2. Modify the service configurations as required.

Note: **Service Name** and **Maximum Sessions** cannot be modified.

Step 3. Click **Save** to save the changes.

Viewing or terminating active sessions for a service

To view or terminate the active sessions for a service, perform the following steps:


Step 1. On the Settings page, click  in the same row as the service for which you want to view or terminate its active sessions.
The Service Sessions page is displayed, which displays the information about active sessions.

- **Session ID** and **Session Type:** ID and type of the active session.
- **User ID** and **User Name:** ID and name of the user.

Notes: The default user ID ranges for the supported PAM modules are as follows:

- LDAP/E-Directory user: 2000–2999
- Active Directory user: 3000–3999
- RADIUS user: 4000–4999

- **Client IP:** IP address already configured for the active session.
- **Privilege:** access privilege of the user.

Step 2. Select a slot and click  to terminate the particular session of the service.

SMTP Settings

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

This section allows you to configure the SMTP settings of the device.

To open the SMTP Settings page, click **Settings** → **SMTP Settings**.

The fields of the SMTP Settings page are explained below.

- **LAN Interface:** Select the LAN interface to be configured.

- **Sender Email ID:** Enter a valid sender e-mail ID on the SMTP Server. Maximum allowed size for an e-mail ID is 64 bytes, which includes user name and domain name.
- **Primary SMTP Support:** Enable or disable SMTP support for the BMC.
- **Primary Server Name:** Enter the “Machine Name” of the SMTP server. This field is for information purpose only.
 - Machine Name is a string of maximum 25 alpha-numeric characters.
 - Spaces and special characters are not allowed.
- **Primary Server IP:** Enter the server address for the SMTP Server
 - An IP address consists 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.
 - IPv4, IPv6, and host name formats are supported.
- **Primary SMTP port:** The default port is 25 and the port value ranges from 1 to 65535.
- **Primary Secure SMTP port:** The default port is 465 and the port value ranges from 1 to 65535.
- **Primary SMTP Authentication:** Enable or disable SMTP authentication.

Notes: Supported SMTP server authentication types include:

- CRAM-MD5
- LOGIN
- PLAIN

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

- **Primary Username:** Enter the user name required to access SMTP accounts.
 - A user name is string of 4 to 64 alpha-numeric characters that must start with an alphabetical character.
 - Special characters like dot (.), at sign (@), hyphen (-), and underscore (_) are supported. Others are not allowed.
- **Primary Password:** Enter the password for the SMTP user.
 - A password must be 4 to 64 characters long.
 - White space is not allowed.
- **Primary SMTP SSLTLS Enable:** Enable or disable the SMTP SSLTLS protocol.
- **Primary SMTP STARTTLS Enable:** This option is available only when **Primary SMTP SSLTLS Enable** is not selected.
 - **Upload SMTP CA Certificate File:** file that contains the certificate of the trusted CA certs. The CACERT key file should be of pem type.
 - **Upload SMTP Certificate File:** Client certificate filename. The CERT key file should be of pem type.
 - **Upload SMTP Private Key:** Client private key filename. The SMTP key file should be of pem type.

Note: To enable STARTTLS support, the primary SMTP support option should be enabled.

- **Secondary SMTP Support:** It lists the secondary SMTP server configuration. It is an optional field. If the primary SMTP server is not working fine, then it tries with secondary SMTP server configuration.

Note: Options of **Secondary SMTP Support** are same as those of **Primary SMTP Support**.

- **Save:** Save the settings.

SSL Settings

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

This section is used to configure an SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open the SSL Settings page, click **Settings** → **SSL Settings**.

The SSL Settings page includes the following tabs:

- “Generate CSR” on page 40: used to generate a certificate signing request (CSR).
- “Download CSR” on page 41: used to download a generated CSR.
- “Import Signed Certificate” on page 41: used to import a signed certificate.
- “Generate SSL Certificate” on page 41: used to generate an SSL certificate based on configuration details.
- “View SSL Certificate” on page 42: used to view an uploaded SSL certificate in readable format.
- “Download SSL Certificate” on page 42: used to download a generated SSL certificate.

Generate CSR

The fields of the Generate CSR page are explained below.

- To download a CSR, click the **Download CSR** link.
- **Common Name (CN)**: common name for which the certificate is to be generated.
 - It contains a maximum of 64 alpha-numeric characters.
 - Special characters ‘#’ and ‘\$’ are not allowed.
- **Organization (O)**: name of the organization for which the certificate is to be generated.
 - It contains a maximum of 64 alpha-numeric characters.
 - Special characters ‘#’ and ‘\$’ are not allowed.
- **Organization Unit (OU)**: section or unit of the organization for which certificate is to be generated.
 - It contains a maximum of 64 alpha-numeric characters.
 - Special characters ‘#’ and ‘\$’ are not allowed.
- **City or Locality (L)**: city or locality of the organization.
 - It contains a maximum of 128 alpha-numeric characters.
 - Special characters ‘#’ and ‘\$’ are not allowed.
- **State or Province (ST)**: state or province of the organization.
 - It contains a maximum of 128 alpha-numeric characters.
 - Special characters ‘#’ and ‘\$’ are not allowed.
- **Country (C)**: country code of the organization.
 - Only two characters are allowed.
 - Special characters are not allowed.
- **Email Address**: e-mail address of the organization.

- **Valid for:** requested validity days for the certificate, ranging from 1 to 3650 days.
- **Key Length:** key length bit value of the certificate.
- **Save:** Generate the new CSR.

Download CSR

Note: Clicking the **Download** button allows you to obtain the service data for your system. Normally you would do this only at the request of support personnel.

Procedure

- Step 1. Specify the CSR download type, which can be **PEM** or **DER**.
- Step 2. Click **Download**.

Import Signed Certificate

Note: The certificate being imported must have been created from the CSR most recently created.

Procedure

- Step 1. Click **Choose File** and choose a new signed certificate (in DER format).
Alternatively, paste the file content in the blank area.
- Step 2. Click **Upload**.

Generate SSL Certificate

The fields of the Generate SSL Certificate page are explained below.

- **Common Name (CN):** common name for which the certificate is to be generated.
 - It contains a maximum of 64 alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- **Organization (O):** name of the organization for which the certificate is to be generated.
 - It contains a maximum of 64 alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- **Organization Unit (OU):** section or unit of the organization for which certificate is to be generated.
 - It contains a maximum of 64 alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- **City or Locality (L):** city or locality of the organization.
 - It contains a maximum of 128 alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- **State or Province (ST):** state or province of the organization.
 - It contains a maximum of 128 alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- **Country (C):** country code of the organization.
 - Only two characters are allowed.
 - Special characters are not allowed.
- **Email Address:** e-mail address of the organization.
- **Valid for:** requested validity days for the certificate, ranging from 1 to 3650 days.

- **Key Length:** key length bit value of the certificate.
- **Save:** Generate the new SSL certificate.

View SSL Certificate

Current Certificate Information: displays the information about the uploaded SSL certificate.

- Basic Information
- Issued From
- Validity Information
- Issued To

Download SSL Certificate

Note: Clicking the **Download** button allows you to obtain the service data for your system. Normally you would do this only at the request of support personnel.

Procedure

Step 1. Specify the download type, which can be **PEM** or **DER**.

Step 2. Click **Download**.

System Firewall

This section allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP addresses or port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

To open the System Firewall page, click **Settings → System Firewall**.

The fields of the System Firewall page are explained below.

- “General Firewall Settings” on page 42
- “IP Address Firewall Rules” on page 43
- “Port Firewall Rules” on page 44

General Firewall Settings

Click **System Firewall → General Firewall Settings**.

The General Firewall Settings page is displayed, including the following:

- “Existing Firewall Settings” on page 42
- “Add Firewall Settings” on page 43

Existing Firewall Settings

A blank page will be opened if you did not add anything in Add Firewall Settings. If there are no firewall settings, add firewall settings by clicking the **Add Firewall Settings** link.

After you have configured firewall settings, all the configured firewall settings will be displayed on the Existing Firewall Settings page. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

Note: Click  in the upper right corner to delete an item.

Add Firewall Settings

To add firewall settings, perform the following steps:

1. Click **General Firewall Settings → Add Firewall Settings**.

The Add Firewall Settings page is displayed.

2. Select **Block All** to block all the incoming IP addresses and ports.
3. Select **Flush All** to flush all the system firewall rules (read-only). After you select this check box, the other fields cannot be configured. Then click **Save** to save the settings.
4. Select **Timeout** to enable firewall rules with timeout.
5. Enter **Start Date** and **Start Time** to start the respective firewall rule effect from this time.
6. Enter **End Date** and **End Time** to end the respective firewall rule effect from this time.
7. Click **Save** to save the settings.

IP Address Firewall Rules

Click **System Firewall → IP Address Firewall Rules**.


The IP Firewall Rules page is displayed, including the following:

- “Existing IP Rules” on page 43
- “Add New IP Rule” on page 43

Existing IP Rules

A blank page will be opened if you did not add anything in Add IP Rule. If there is no IP rule, add an IP rule by clicking the **Add IP Rule** link.

After you have configured IP rules, all the configured IP rules will be displayed on the Existing IP Rules page. To view this page, you must at least be an operator. Only administrators can add or delete an IP rule.

Note: Click  in the upper right corner to delete an item.

Add New IP Rule

To add an IP rule, perform the following steps:

1. Click **IP Address Firewall Settings → Add New IP Rule**.

The Add IP Rule page is displayed.

2. Enter an IP address or the start value of a range of IP addresses in the **IP Single (or) Range Start** field.

Notes:

- An IP address consists 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.
3. (Optional) Enter the end value of the IP range in the **IP Range End** field.
 4. Select **Enable Timeout** to enable firewall rules with timeout.
 5. Enter **Start Date** and **Start Time** to start the respective firewall rule effect from this date and time.
 6. Enter **End Date** and **End Time** to end the respective firewall rule effect from this date and time.
 7. Determine the rule to **Block** or **Allow**.
 8. Click **Save** to save the settings.

Port Firewall Rules

Click **System Firewall → Port Firewall Rules**.


The Port Firewall Rules page is displayed, including the following:

- “Existing Port Rules” on page 44
- “Add New Port Rule” on page 44

Existing Port Rules

A blank page will be opened if you did not add anything in Add Port Rule. If there is no port rule, add a port rule by clicking the **Add Port Rule** link.

After you have configured port rules, all the configured port rules will be displayed on the Existing Port Rules page. To view this page, you must at least be an operator. Only administrators can add or delete a port rule.

Note: Click  in the upper right corner to delete an item.

Add New Port Rule

To add a port rule, perform the following steps:

1. Click **Port Firewall Rules → Add New Port Rule**.

The Add Port Rule page is displayed.

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

Notes:

- The port number ranges from 1 to 65535.
- Port 80 is blocked for TCP and UDP protocols.

3. (Optional) Enter the end value of the port range in the **Port Range End** field.
4. Specify the **Protocol** for the configured port or port range.
5. Specify the affected **Network Type** for the particular port or port ranges.
6. Select **Enable Timeout** to enable firewall rules with timeout.
7. Enter **Start Date** and **Start Time** to start the respective firewall rule effect from this date and time.
8. Enter **End Date** and **End Time** to end the respective firewall rule effect from this date and time.
9. Determine the rule to **Block** or **Allow**.
10. Click **Save** to save the rule.

User Management

This section allows you to view the current list of user slots for the server.


To open the User Management page, click **Settings → User Management**.

By default, currently configured users for each LAN channel are displayed, and a maximum of 15 users are available, including the default administrator and anonymous users. Each slot displays the channel ID, user ID, user name, access privilege, and network privilege of the user.

Note: By default, the complex password policy is enabled under **Global Setting**. To change the setting, click **Global Setting**, disable **Password Complex**, and then click **Save**.

Supported operations on users

User Management allows you to view, delete, modify, or add users.

- To view this page, you must have operator privileges.
- To delete a user from the list, click  in the upper right corner.
- To modify a user, click the user slot to enter the User Management Configuration page and then modify its configurations.
- To add a user, select a free slot to open the User Management Configuration page and then set its configurations.

Notes:

- It is advised that the anonymous user's privilege and password should be modified immediately as a security measure.
- To modify or add a user, you must have administrator privileges.

User Management Configuration

The User Management Configuration page includes the following configurations.

- **Username:** Enter the name of the user.
 - A user name is a case-sensitive string of 1 to 16 alpha-numeric characters that must start with an alphabetical character.
 - Special characters like hyphen (-), underscore (_), and at sign (@) are supported.
- **Change Password:** Select this check box to enable password changing. When adding a new user, this option is not displayed, and you can directly set the password.
- **Password Size:** Select the preferred size for the password.
- **Password** and **Confirm Password:** Enter and confirm your password, which must consist of at least one upper case letter, alpha-numeric characters, and special characters.

Notes:

- The **Password** field is mandatory and should have a minimum of 8 characters when the SNMP status is enabled.
- This field will not allow more than 16 or 20 characters based on the value of the **Password** size.
- If **Password Complex** is enabled under **Global Setting**, follow the rules below:
 1. No other characters, in particular, spaces or white-space characters, are allowed.
 2. At least one letter must be contained.
 3. At least one number must be contained.
 4. At least two of the following types must be contained:
 - An upper-case letter
 - A lower-case letter
 - A special character
 5. A password may have no more than 2 consecutive instances of the same character.
 6. A password must not be the same as an associated user ID or the user ID in a reverse order.
 7. A password must contain a minimum of 8 and a maximum of 20 characters.
 8. BMC prevents duplicated passwords.

- **Enable User Access:** Check the boxes to enable network access for the user. Upon enabling, the corresponding IPMI messaging privilege will be assigned to the user.

Note: It is recommended that the IPMI messaging option should be enabled as well if user is created through IPMI.

- **Privilege(Channel 1) and Privilege(Channel 8):** Select the privilege assigned to the user which could be **Administrator, Operator, User, OEM, or None.**
- **KVM Access:** Select this check box to assign the KVM privilege for the user.
- **VMedia Access:** Select this check box to assign the VMedia privilege for the user.

Note: The term VMedia represents H5Viewer, JViewer, VMapp, and VMCLI clients.

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 Admin user can provide the privilege support to User and Operator privilege level users at their own risk.

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.

While modifying the KVM and VMedia access by logged in User, it will prompt you with the alert message to log out the current session to reflect the changes.

- **SNMP Access:** Select this check box to enable SNMP access for the user.
 - **SNMP Access level:** Select the SNMP access level for the user.
 - **SNMP Authentication Protocol:** Select an SNMP authentication protocol for the user.

Note: The **Password** field is mandatory whenever the authentication protocol is changed.
 - **SNMP Privacy Protocol:** Select the encryption algorithm to be used for the SNMP settings.
- **Email Format:** Specify the format for sending e-mail. Two types of formats are available:
 - **AMI-Format:** The subject of this mail format is **Alert from (your Hostname)**. The mail content includes sensor information such as sensor type and description.
 - **FixedSubject-Format:** This format displays the specific subject and message configured for e-mail alerts for the specified user.
- **Email ID:** Enter the e-mail ID for the user. If the user forgets the password, a new password will be mailed to this e-mail ID.

Notes:

- The SMTP server must also be configured for this option.
- The maximum allowed size for **Email ID** is 64 bytes, including user name and domain name.
- **Existing SSH Key:** If available, the uploaded SSH key information will be displayed, which is read-only.
- **Upload SSH Key:** Click **Browse** and select the SSH key file.

Note: SSH key file should be of pub type.

Click **Save** to save the changes and return to the user list.

Click **Delete** to delete the existing user.

System Location

This section allows you to provide the information that identifies the system to operation and support personnel.

To open the System Location page, click **Settings → System Location**.

On the System Location page, specify the contact number, rack name, and location information about the system, and then click **Save** to save the configuration.

Account Lockout Policy

This section allows you to configure the account lockout policy.

To open the Account Lockout Policy page, click **Settings → Account Lockout Policy**.

The fields of the Account Lockout Policy page are explained below.

- **Enable Lockout Policy:** Select this check box to enable the account lockout policy.
- **Attempt Times:** Specify the number of incorrect attempts before the account is locked out.
- **Reset Time (Min):** Enter a value between 0 and 10922. The value **0** indicates that the account resets till the BMC goes through a power cycle.
- **Lockout Time (Min):** Enter a value between 30 and 10922, or 0. The value **0** indicates that the account lockout terminates till the BMC goes through a power cycle.
- Click **Account Lockout Policy** to save the policy.

SNMP Trap Version

This section allows you to configure the SNMP trap version.

To open the SNMPTrap Version page, click **Settings → SNMPTrap Version**.

- **SNMPTrap Version:** Select **SNMPTrap V1** or **SNMPTrap V3** as required.
- Click **Save** to save the configuration.

Power Supply Setting

This section provides power supply unit (PSU) redundancy configuration.

To open the PSU Redundant page, click **Settings → PSU Redundant**.

As shown on the page, there are two PSUs available.

- To immediately disable PSU redundancy, select **Non-redundant**.
- To enable PSU redundancy, select **Redundant(N+N)**.
- Click **Perform Action** to save the configuration.

IPMI Configuration

This section provides IPMI configuration.

To open the IPMI Configuration page, click **Settings → IPMI Configuration**.

- To immediately enable IPMI LAN (IPv4), select **Enable IPMI LAN (IPv4)**.
- To immediately enable IPMI LAN (IPv6), select **Enable IPMI LAN (IPv6)**.
- Click **Save** to save the configuration.

Note: The default settings for the IPMI configuration vary depending on customers' configuration.

Chapter 8. Remote Control

Click **Remote Control** from the menu bar. The Remote Control page is displayed.

The Remote Control page allows you to implement remote control on the device. The various options of remote control are given below.

- “**H5Viewer**” on page 49
- “**JViewer**” on page 55
- “**Serial Over LAN**” on page 64

The system and browser requirements for remote control are given below.

System Requirements

- Client machine with 8 GB RAM.
- If the client machine has 4 GB RAM or lower, there will be lag in video/keyboard/mouse/media redirection 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.

In Microsoft Windows operating systems, IPv4 addresses are valid location identifiers in Uniform Naming Convention (UNC) path names. However, the colon (:) is an invalid character in a UNC path name. Thus, the use of IPv6 addresses is also invalid in UNC names.

For this reason, in the IE browser, IPv6 addresses should be given in the format of literal IPv6 addresses in UNC path names.

Example:

For Web, **2001-db8-85a3-8d3-1319-8a2e-370-7348.ipv6-literal.net:85**, where IP is **2001:db8:85a3:8d3:1319:8a2e:370:7348** and port is **85**.

Launch H5Viewer

On the Remote Control page, click **Launch H5Viewer**.

The remote KVM page is displayed.

Procedure to start/stop KVM

- Step 1. Click **Launch H5Viewer** to open the remote control KVM page.
- Step 2. To stop the H5Viewer video redirection, click **Stop KVM** in the upper left corner.

Procedure to start/stop media

- Step 1. Click **Browse File** in the upper right corner to select a CD image.

Step 2. Click **Start Media** to redirect the selected CD image file to the host.

Step 3. To stop the CD Image redirection, click **Stop Media**.

A detailed description of the menu items is given below.

Video

This menu contains the following sub menu items:

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:

- **Display ON:** If you disable this option, that is, enable **Display OFF**, the display will be shown on the screen in console redirection.
- **Display OFF:** If you enable this option, the server display will be blank but you can view the screen in console redirection.

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 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 Mmode:** 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: 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.

Options

Zoom:

- **Normal:** By default this option is selected.
- **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%.

Block Privilege Request: This option is used to enable or disable the access privilege of the user, which can be **Partial Permission** or **No Permission**.

Bandwidth: This option determines the bandwidth. You can select **Auto Detect**, **256 Kbps**, **512 Kbps**, **1 Mbps**, **10 Mbps**, or **100 Mbps**.

Compression mode: This option helps to compress the video data transfer to the specific mode.

Video quality list: This list allows you to choose a video quality.

Keyboard

Keyboard Layout: 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.

Send Keys

This option is used to key items. This menu contains the following sub menu items:

- Hold Down
- Press and Release

Hold Down

- **Right Ctrl Key:** This menu item can be used to act as the right-side <CTRL> key in console redirection.
- **Right Alt Key:** This menu item can be used to act as the right-side <ALT> key in console redirection.
- **Right Windows Key:** This menu item can be used to act as the right-side <WIN> key in console redirection.
- **Left Ctrl Key:** This menu item can be used to act as the left-side <CTRL> key in console redirection.
- **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**.

Press and Release

- **Ctrl+Alt+Del:** This menu item can be used to act as if you depressed the <CTRL>, <ALT>, and keys down simultaneously on the server that you are redirecting.
- **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.
- **Context Menu Key:** This menu item can be used to act as the context menu key in console redirection.
- **Print Screen Key:** This menu item can be used to act as the print screen 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.

- **Add Hot Keys:** This menu is used to enable macros. Click **Add** to macros.

Video Record

This menu contains the following sub menu items:

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 Length** should be in the range of 1 to 1800 seconds. **Video Compression** 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 client-side video recording performance in H5Viewer.
- Disable this option to record video at the same resolution as host video. The host video capture depends on client system performance. If this option is disabled, the recorded video file may have inconsistency. (for example, recorded video file duration may not be the same as the configured value).

Note: The maximum video file size allowed is around 40 MB. If the video file size reaches its maximum size limit, the recorded file is downloaded and 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.

Users have to 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 limitations, the set timeout or set interval will be delayed from specified time of interval when the browser window loses focus. Hence, the 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 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 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.

Active KVM Session can be terminated when there are multiple KVM Session From Master [FULL Privilege KVM Session].


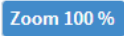


Help

Click this option to get more information about H5Viewer. The KVM remote console utility version and plugin version will be displayed.

Quick buttons

The upper right of the H5Viewer window displays all the quick buttons. These quick buttons allow you to perform the below functions by clicking them.

Table 4. Quick buttons in the H5Viewer window

Button	Description
	This quick button will show or hide the notification drop-down menu, which contains the list of notifications displayed by H5Viewer.
	It shows the current zoom value in percentage.
	This quick button is used to display the current host monitor status. <ul style="list-style-type: none">• If the icon is in green, the host monitor is unlocked.• If the icon is in red, the host monitor is locked. By clicking the button, the host monitor status can be toggled.
	This quick button is used to display the current server power status. <ul style="list-style-type: none">• If the icon is in green, the server status is powered on.• If the icon is in red, the server status is powered off. Click the button to toggle between immediate host power-off and power-on.

Status bar buttons



Figure 3. Status bar buttons

Some of these buttons provide the same functionality of the menu items under **Send Keys → Hold Down**. Select any of the menu items, and the corresponding status bar button will be highlighted in green color. Similarly by clicking the buttons will toggle the selection status of the corresponding menu item.

Keyboard LED sync

When the H5Viewer 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.

Notes: Due to Web browser-related security concerns, this feature has the following limitations:

- Host LED status will be synced with client LED status, only if the user presses any key in the client keyboard when the H5Viewer window is in focus.
- Client keyboard LED status cannot be updated.

This functionality is not available in the safari Web browser.

- In some Linux hosts, with text mode, CapsLock LED status will not be updated properly.
In such cases, the H5Viewer CapsLock synchronization functionality will not work properly.
- Example: Typing letters in H5Viewer (after pressing CapsLock) will toggle between lower to upper case inside the host.

KVM sharing

TSM stack supports multiple KVM redirection sessions, with only one full-permission JViewer or H5Viewer session at a time. With full permission in JViewer or H5Viewer, the user can control the KVM redirection, while the other JViewer or H5Viewer users can only view the video redirected from the server without intervention.

When the first user launches JViewer or H5Viewer, the user will get full permission to control the host during KVM redirection. When another JViewer or H5Viewer session is launched, the video server will send a KVM sharing permission request packet to the current session, for the new requesting session.

Once the requesting session is authenticated, a packet containing the information such as the client IP or host name and user name of the newly authenticated or logged in user, will be sent to the current session.

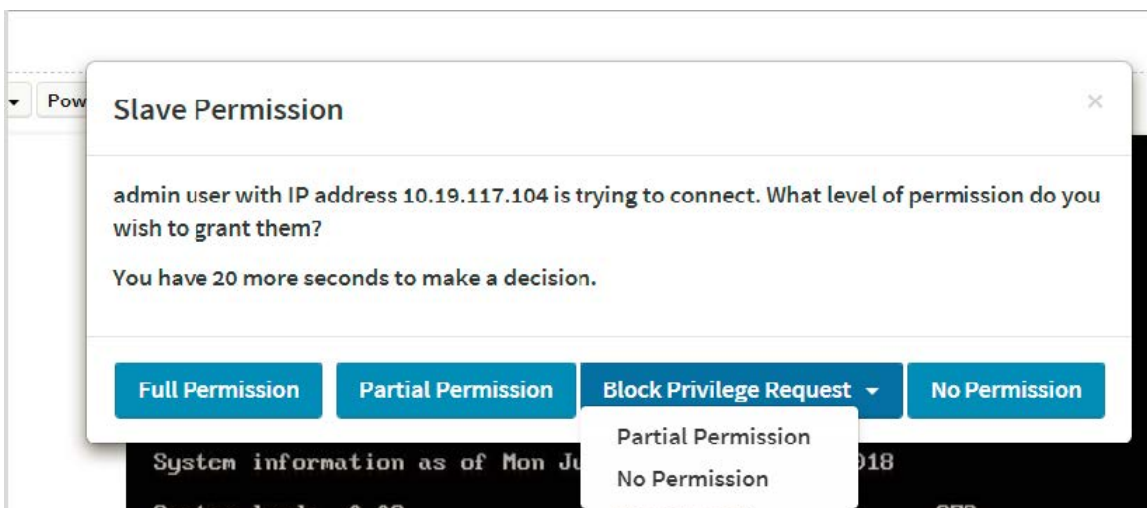


Figure 4. KVM sharing page

Clicking the button in the dialog box will trigger the specified action:

- **Full Permission:** When this button is clicked, the requesting session will receive full access permission, and the current (full permission) session will have a partial KVM access permission only.
- **Partial Permission:** When this button is clicked, the requesting session will receive partial permission and can only view server display (video only).
- **Block Privilege Request:**
 - **Partial Permission:** Once this option is selected, both the newly requesting session and active partially privileged session will get partial permission as auto response and can only view server display. Further requests will be served by the auto response mechanism.
 - **No Permission:** Once this option is selected, both the newly requesting session and active partially privileged session access will be denied as auto response. Further requests will be served by the auto response mechanism.

- **No Permission:** When this button is clicked, the requesting session access will be denied.

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. Visit https://icedtea.classpath.org/wiki/IcedTea-Web#Filing_bugs for further information.

In some earlier versions of JRE 1.7, TLS v1 protocol will be enabled by default. Users need to manually enable TLS v1.2 protocol support from the Java configuration panel for proper JViewer functionality.

Procedure to launch JViewer

Step 1. Download the .jnlp file from the BMC.

Step 2. Open the .jnlp file using the appropriate JRE version (Javaws).
When the downloading is done, it opens the console redirection window.

The console redirection menu bar consists of the following menu items:

- Video
- Keyboard
- Mouse
- Options
- Media
- Keyboard Layout
- Video Record
- Power
- Active Users
- Help

A detailed description of the menu items is given below.

Video

This menu contains the following sub menu items:

Pause redirection: This option is used for pausing console redirection.

Resume Redirection: This option is used to resume the console redirection when the session is paused.

Refresh Video: This option can be used to update the display shown in the console redirection window.

Capture Screen: This option helps to take the screenshot of the host screen and save it in the client's system.

Compression mode: This option helps to compress the video data transfer to the specific mode.

Video quality list: This list allows you to choose a 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

This menu contains the following sub menu items:

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

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.

Note: 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.

To view the supported operating systems for mouse modes, see “Supported operating systems for mouse modes” on page 26.

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

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

Zoom:

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

- **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%.

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.

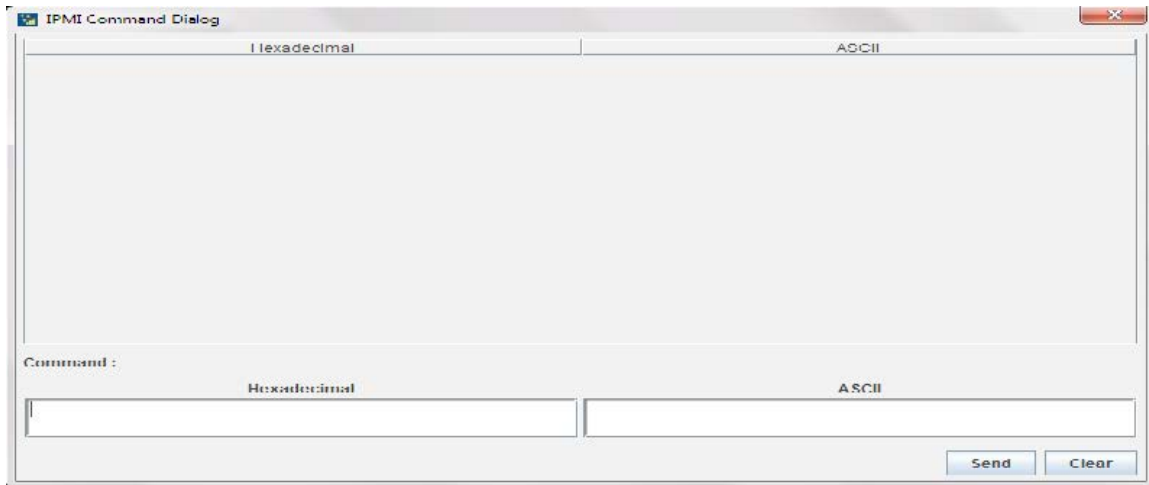


Figure 5. IPMI Command Dialog

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**.

Note: 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.

Media

Virtual media application:

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.

A sample screenshot of virtual media application is given below.

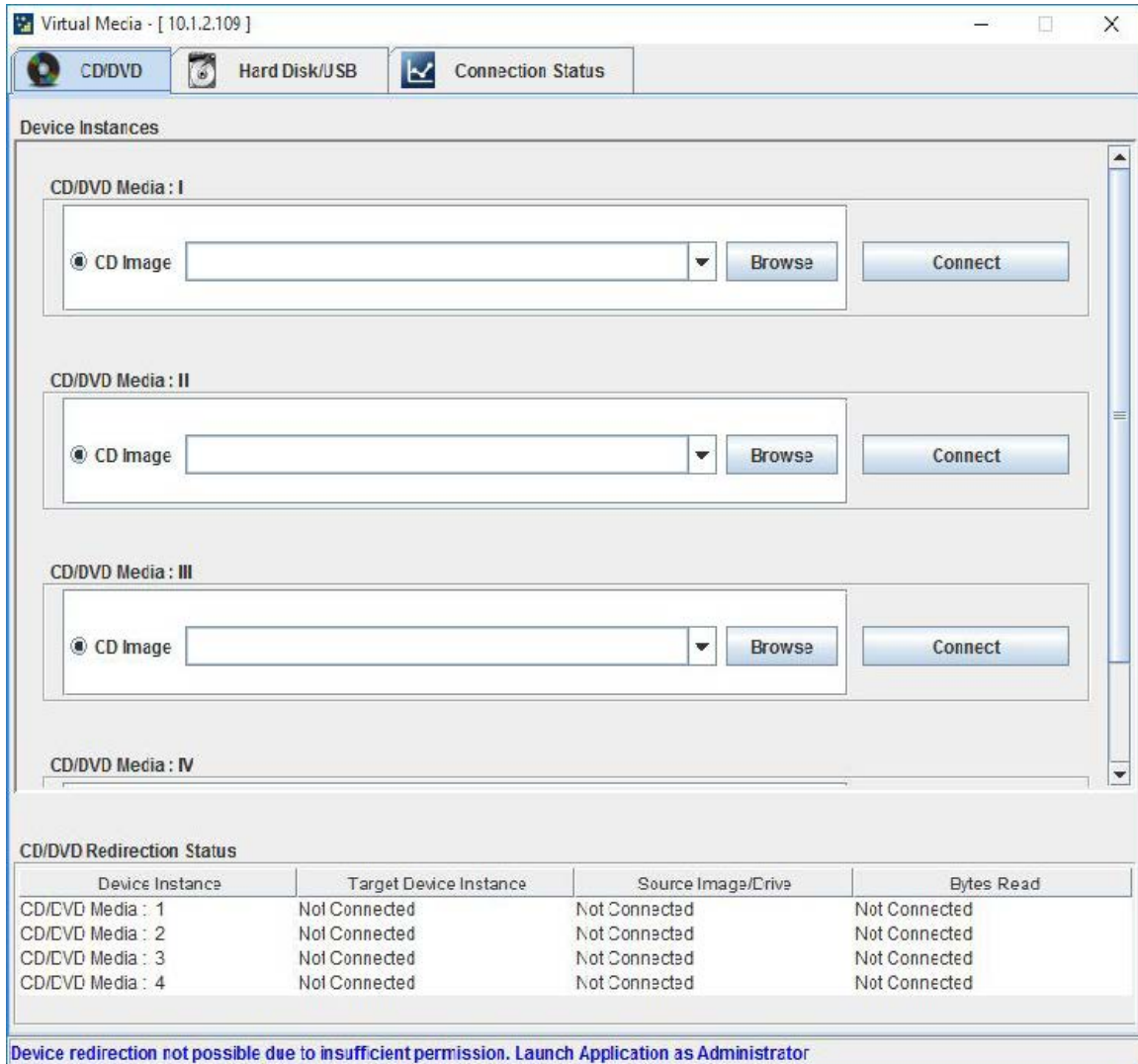


Figure 6. Virtual Media

Note: 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.

Note: 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 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.

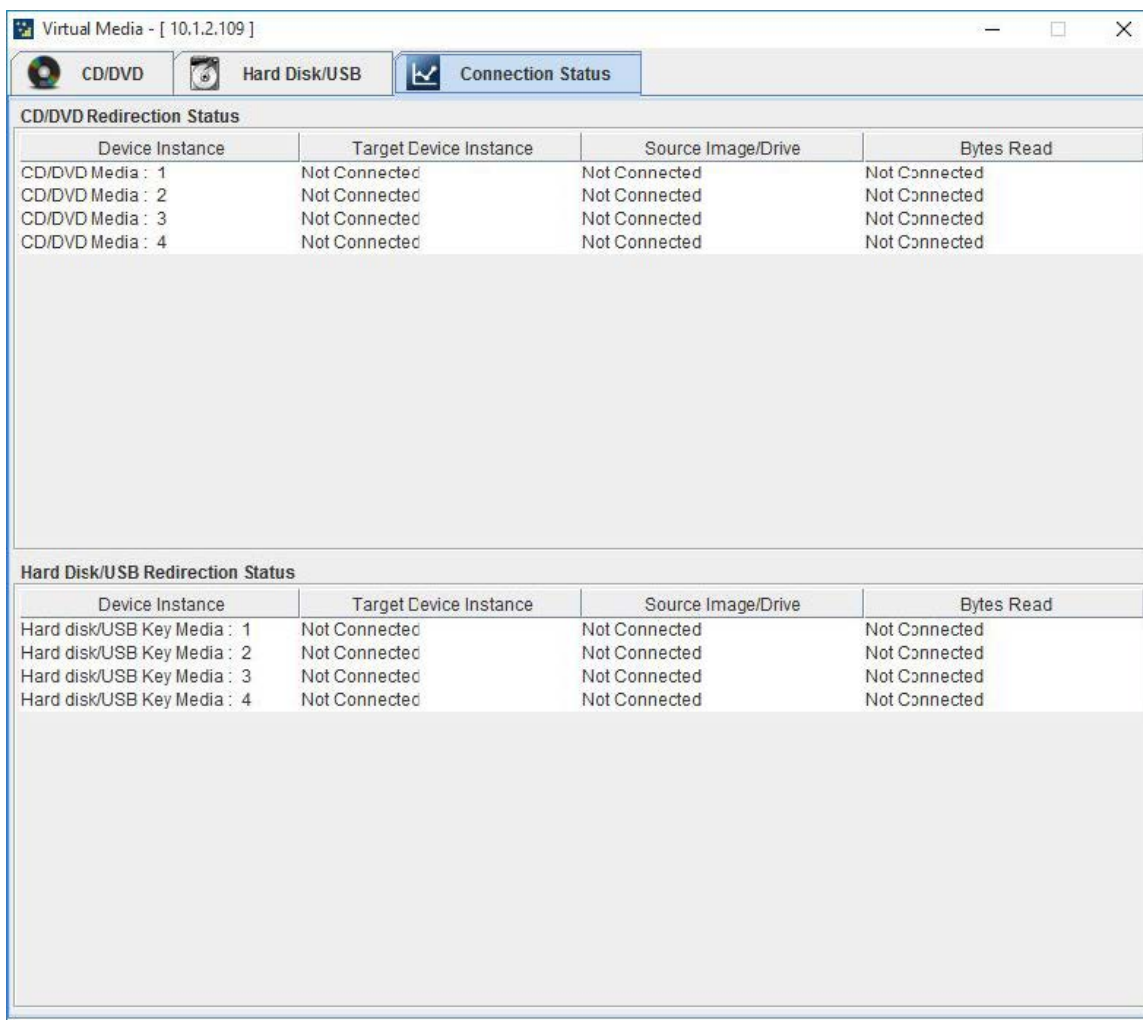


Figure 7. Connection Status tab

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.

The following host physical keyboard languages are supported in JViewer:

- English
- Simplified Chinese

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.

Note: Different Linux systems follow different keyboard layouts. Therefore, the soft keyboard displayed uses the standard windows keyboard layout irrespective of the host OS.

The following soft physical keyboard languages are supported in JViewer:

- English
- Simplified Chinese

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

Video Record

This menu contains the following sub menu items:

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.

Note: Before you start recording, you have to enter the settings.

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

The power options are to perform any power cycle operation. Click 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 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.

Quick buttons

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.

Table 5. Quick buttons in console redirection windows












Button	Description
	This key is used to play the console redirection after being paused.
	This key can be used for pausing console redirection.
	This button is used to view the console redirection in full screen mode. Note: Set your client system resolution same 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 to zoom in or out.
	This quick button is used to record the video.
	These quick buttons will pop up a virtual media where you can configure the media.

Table 5. Quick buttons in console redirection windows (continued)

Button	Description
	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. <ul style="list-style-type: none"> • 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.

Note: 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 micro-controller embedded on the server system board 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 servers from anywhere and perform any task that does not require a GUI.

Transporting serial data over IP networks using telnet, serial over IP, SOL and the likes is the way forward for server serial communications. Just as the KVM function in embedded service processors is displacing the need for external KVM appliances, so the SOL capability of BMCs and console redirection in service processors is reducing the need for serial console servers for server console management.

Chapter 9. Image Redirection

Click **Image Redirection** from the menu bar. The Image Redirection page is displayed.

The Image Redirection page is used to configure the images into BMC for redirection. This can be done by mounting the images from the remote system.

On the Image Redirection page, the **Remote Images** option is available.

Remote Media

Click **Image Redirection → Remote Images**.

The Remote Media page is displayed.

The displayed table shows remote images available to the BMC. You can start redirection or clear the images on this page.

Notes: A maximum of 4 images can be added for each image type, depending on your configuration.

To configure the images, you need to enable remote media support in **Settings → Media Redirection → General Settings**.

To start or stop redirection and to delete an image, you must have administrator privileges.

Free slots are denoted by “~”.

- Supported CD/DVD format: ISO9660, UDF (v1.02–v2.60).
- Supported CD/DVD media file type: (*.iso), (*.nrg).
- Supported HDD media file type: (*.img), (*.ima).



Field description

The image list displays the following fields:



- **Media Type:** Displays the type of media such as **CD/DVD** and **Hard disk**.
- **Media Instance:** Displays the total number of media instances.
- **Image Name:** Displays the default recovery image name on the server.
- **Redirection Status:** Displays the status of the media.
- **Connected Server Session Index:** Displays the media server session index.

Supported operations

Remote Media allows you to perform various operations on the images.

- Click  in the upper right corner of the page to view the brief description of this page.
- Click  **Refresh Image List** in the upper right corner of the list to get the latest list of images from the remote storage server.

- Click  to redirect the selected image.

- Click  to stop the remote image redirection.
- Click  to clear the selected image from the BMC.

Chapter 10. Power Control

Click **Power Control** from the menu bar. The Power Control page is displayed.

The Power Control page allows you to view and control the power of your server. The various options of Power Control are given below.

- **Power Off:** Power off the server without first shutting down the operating system.
- **Power On:** Power on the server and boot the operating system.
- **Power Cycle:** Power off the server first and then power on the server.
- **Hard Reset:** Reset the server and boot the operating system.
- **ACPI Shutdown:** Shut down the operating system and power off the server.
- **BMC Cold Reset:** Restart the TSM hardware.
- **BMC Warm Reset:** Restart the IPMI process of TSM.

Select an action and click **Perform Action** to proceed with the selected action.

Note: During the execution, you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

Chapter 11. Maintenance

Click **Maintenance** from the menu bar. The Maintenance page is displayed.

The Maintenance page allows you to do maintenance tasks on the device. The menu contains the following items:

- “Backup BMC Configuration” on page 71
- “BMC Firmware Information” on page 71
- “Download Service Data” on page 71
- “Firmware Update” on page 72
- “Restore BMC Configuration” on page 72
- “Restore Factory Defaults” on page 73

Backup BMC Configuration

This section allows you to select the specific configuration items to be backed up in case of backup configuration.

Procedure

Step 1. Click **Maintenance** → **Backup BMC Configuration**.
The Backup BMC Configuration page is displayed.

Step 2. Select **Check All** or the particular components that need to be backed up. You will be able to save the backup configuration file to a location of your choice. That saved file can be used to restore the configuration when needed.

Note: Network configurations are inter-related to IPMI, hence, by default, IPMI configurations will be selected automatically when you check the **Network & Services** box and vice versa.

Step 3. Click **Download** to download and save the configuration files backed up from the BMC to the client system.

BMC Firmware Information

This section is used to display the firmware information.

To open the Firmware Information page, click **Maintenance** → **BMC Firmware Information**.

Active Firmware:

- **Build Date:** Describes the build date of the active BMC image.
- **Build Time:** Describes the build time of the active BMC image.
- **Firmware version:** Displays the firmware version of the active BMC image.

Download Service Data

This section is used to download service data.

Note: Normally you would do this only at the request of support personnel.

Procedure

- Step 1. Click **Maintenance → Download Service Data**.
The Download Service Data page is displayed.
- Step 2. Click **Download Service Data**, and BMC starts to collect data. After collection, data will be downloaded automatically.

Firmware Update

This section enables you to perform update operations on **System Firmware**, **BP Firmware**, and **PSU Firmware**.

To open the Firmware Update page, click **Maintenance → Firmware Update**.

The following describes how to update the BMC firmware by using the HPM firmware update method. For BP firmware update and PSU firmware update, follow the steps indicated by the upgrade wizard.

Notes:

- System firmware update includes UEFI, LXPM, and BMC firmware update.
- HPM firmware update indicates BMC firmware update using an image in .hpm format.

Updating the BMC firmware

- Step 1. Click **Choose File** to select the required firmware image.

Note: While creating an HPM image with multiple components, BOOT and APP components should be placed at the end of the configuration file.

- Step 2. Click **Start firmware update** to load the firmware update information.

Note: All configuration items will be preserved by default during the restore configuration operation.

- Step 3. Click **Proceed** to update the firmware for all of the components.

Note: After entering the update mode, the widgets, other Web pages and services will not work. All the open widgets will be automatically closed. If the upgrade is cancelled in the middle of the wizard, the device will be reset.

- Step 4. The firmware update undergoes the below steps:

- Uploading the firmware image
- Flashing the image
- Resetting the image

Notes:

- 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 system firmware. The device will be reset if update is canceled. The device will also be reset upon successful completion of firmware update.
- In case of a BMC downgrade, a message may be displayed to indicate that no user settings will be retained, depending on the target version for the downgrade.

Restore BMC Configuration

This section allows you to restore the configuration files from the client system to the BMC.

Procedure

Step 1. Click **Maintenance** → **Restore BMC Configuration**.

The Restore BMC Configuration from File page is displayed.

Step 2. Use the Browse button to navigate to a previously-saved configuration file.

Step 3. Click **Save** to upload the backup file to restore the backup files.

Restore Factory Defaults

This section is used to restore the factory defaults of the device firmware.

Warning:

- After entering the restore factory widgets, other Web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.
- Restoring to factory defaults will not preserve any existing configuration data. Exercise caution when performing this operation.

To restore your device to factory defaults, directly click **Save**.

Chapter 12. Sign Out

This section instructs how to sign out from the TSM Web page.

Procedure

Step 1. Click **Sign out** from the menu bar.

A dialog box is displayed, asking you to confirm whether to log out from TSM.

10.245.38.92 says

Would you like to Sign out of this Session? If yes, click 'Ok', else click 'Cancel'.



Figure 8. Dialog box for confirming logout

Step 2. Click **OK** to log out from TSM.

Chapter 13. Flash tool

A flash tool is a command line utility program used to upgrade the firmware using different mediums such as USB and LAN. The flash tool being used is YAFUFlash.

YAFUFlash

Yet Another Firmware Upgrade Flash (YAFUFlash, 64 bit) is a tool used for flashing the BMC in both Linux and Windows environments. There are two types of mediums used to flash the BMC:

- Network (out of band mode)
- USB (inband mode)

The following provides commands for BMC firmware upgrade.

Example for network medium

```
# Yafuflash -nw -ip <BMC ip addr> -u USERID -p PASSWORD -non-interactive -fb -mmc -spi  
lnvgy_fw_bmc_ambt01p-1.6_anyos_arm.hpm(file name)
```

Example for USB medium

```
Yafuflash -cd -non-interactive -fb -mmc -spi lnvgy_fw_bmc_ambt01p-1.6_anyos_arm.hpm(file name)
```

Chapter 14. Standalone application

The JViewer application can be launched from the client system as a standalone application. For launching the application, we need to have the executable jar files available in the client machine. The jar files include JViewer.jar. The supported platforms are listed below.

- 64-bit Linux platforms
- 64-bit Mac platforms
- 64-bit Windows platforms

Note: It is recommended to use openJDK 8 or any higher LTS version.

Launching from Windows

The JViewer.jar file that includes the platform-specific media wrapper libraries should be stored in the same directory in the file system of the client machine.

Run the following commands while launching the JViewer standalone application from the command prompt or terminal of a client system:

```
java -jar JViewer.jar [-apptype StandAlone] [-hostname host IP address]
[-webport Secure web port] [-u Username] [-p Password]
[-launch Application Mode] [-lang Localization Language Code]
```

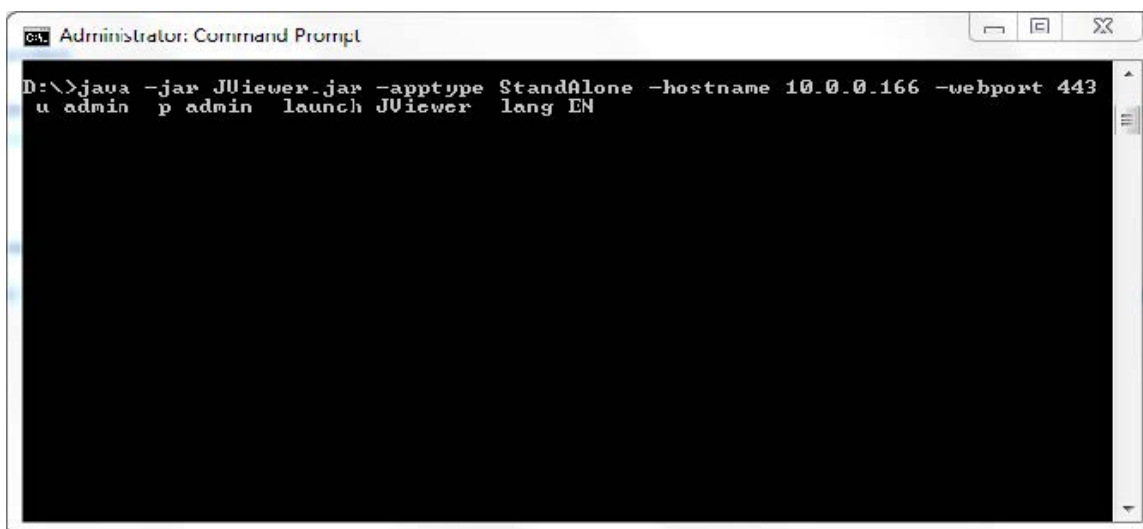
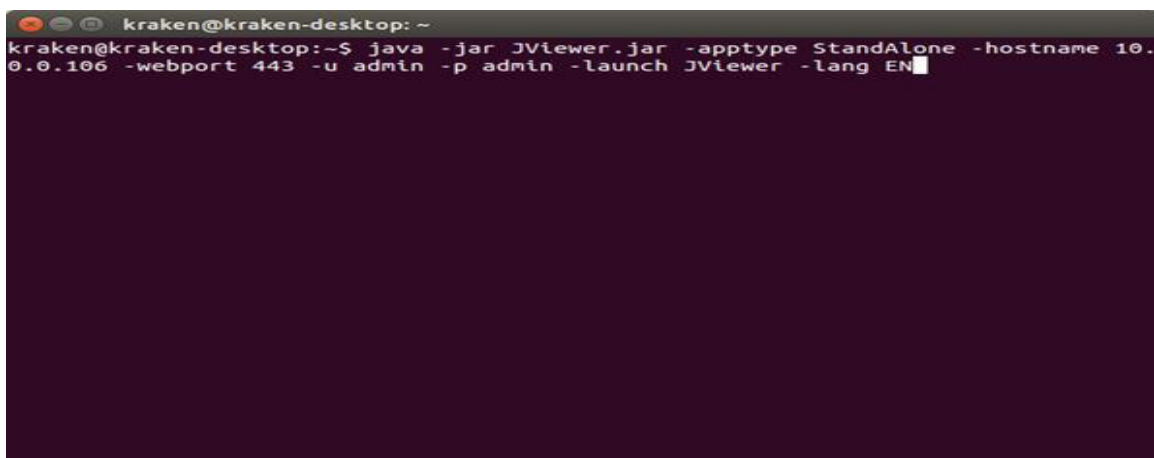


Figure 9. Launching JViewer standalone application from the Windows command prompt

Launching from Linux

Procedure

Step 1. Run the following commands on a Linux terminal:



```
kraken@kraken-desktop: ~  
kraken@kraken-desktop:~$ java -jar JViewer.jar -apptype StandAlone -hostname 10.0.0.106 -webport 443 -u admin -p admin -launch JViewer -lang EN
```

Figure 10. Launching JViewer standalone application from a Linux terminal

- -apptype: application type - StandAlone
- -hostname: host name or IP address of the BMC
- -webport: secure Web port number of the BMC
- -u: user name of the BMC Web session
- -p: password of the BMC Web session
- -launch: application mode
- -lang/localization : localization language code

Notes: It is not mandatory to specify any of these arguments while launching the application from the command prompt or terminal.

If launched from the command line with all the valid arguments mentioned above, it will be directly launched using specified mode.

If any duplicate arguments are detected, a popup will be shown to the user regarding the parameter repeated and the application will be terminated.

The valid values for the -launch option are:

- JViewer: Launches JViewer App.
- VMApp: Launches Virtual Media App.
- PlayVideo, SaveVideo: Launches Manage Video App.

Under a manage video application, the **OK** button will be disabled until the user selects a file from the table (if any).

If valid values for options -launch, and -localization or -lang are provided, the respective option will be selected in combo box and it is disabled to avoid further modification. Else it will not be disabled and left to user's choice.

Either -localization or -lang parameter is supported. If both are mentioned together, then it will be treated as duplicate parameters.

In case of PlayVideo and SaveVideo options in Manage Video App, their respective radio buttons will be selected and other options will be disabled to prevent changes. Otherwise, the options will not be disabled and left to user's desire.

Only one instance of the StandAlone App can be launched using the JViewer.jar file from the same directory. This applies for application types Remote KVM/VMedia (JViewer) and Virtual Media App. This is because the native library files extracted to the client file system cannot be shared by two instances of the application at the same time.

- Step 2. The user can specify all, some, or none of these arguments. If all the arguments are provided correctly, the application will be launched. If any of these arguments is missing, or invalid, an input dialog box will appear, and it will prompt the user to input the correct values.
- Step 3. If the -lang argument is missing, English will be selected as the default language. If the -launch argument is missing, Remote KVM/VMedia (JViewer) will be selected as the default application type.
- Step 4. After entering the correct values, select **Remote KVM/VMedia** from the **Application Type** drop-down box. Click **Launch** to connect to the BMC using JViewer StandAlone application.

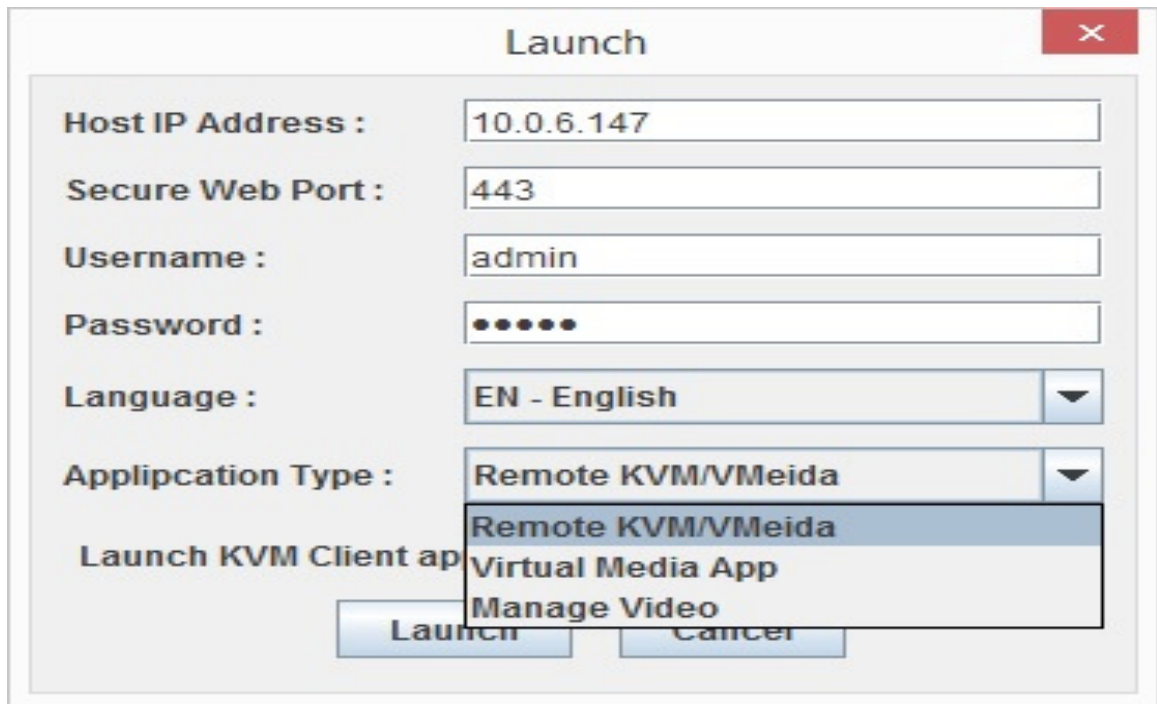


Figure 11. JViewer standalone application connection dialog

- Step 5. To launch the application as Virtual Media App, select the **Virtual Media App** option from the **Application Type** drop-down box, and click **Launch**.
- Step 6. Else select the **Manage Video** option from the **Application Type** drop-down box and click **Launch** to view the recorded video files as shown below.

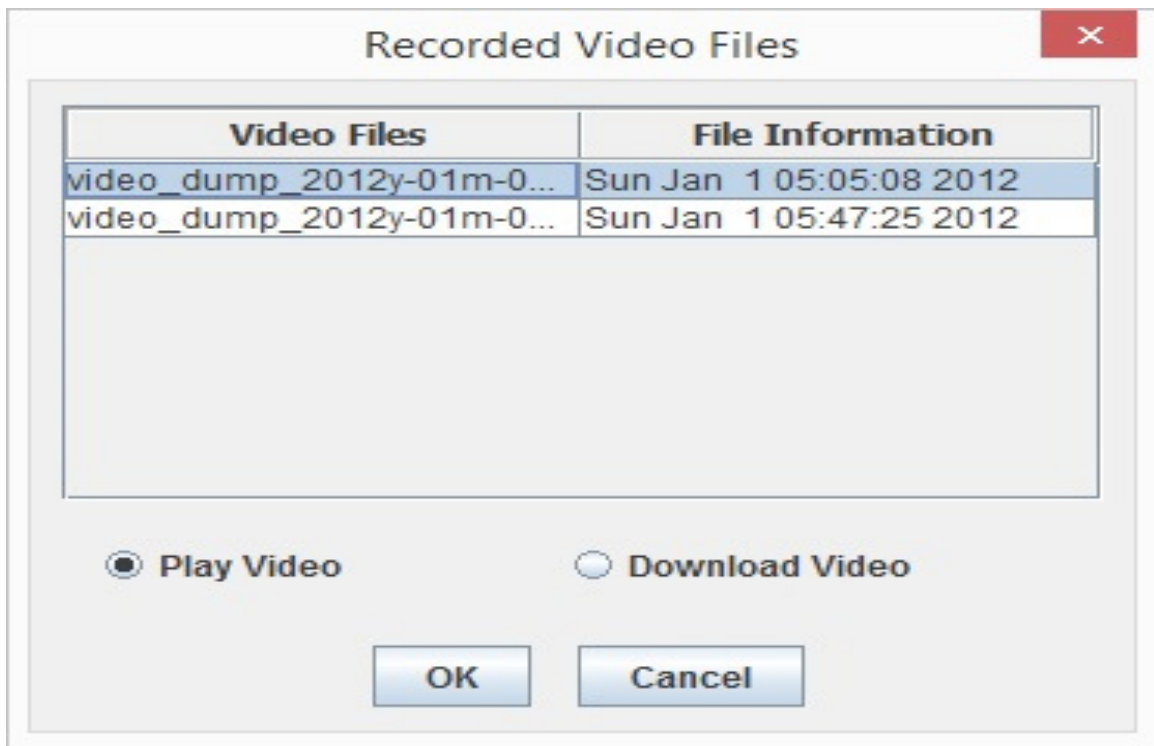


Figure 12. Recorded video files

Step 7. After selecting the required file from the lists as shown above, you can select the **Play Video** option or **Download Video** option and click **OK** to play or download the recorded videos.

Launching from a GUI-based environment

Procedure

Step 1. While launching the JViewer standalone application from a GUI-based environment, double-click the JViewer.jar file or right-click the file, and open it using the Java platform available.

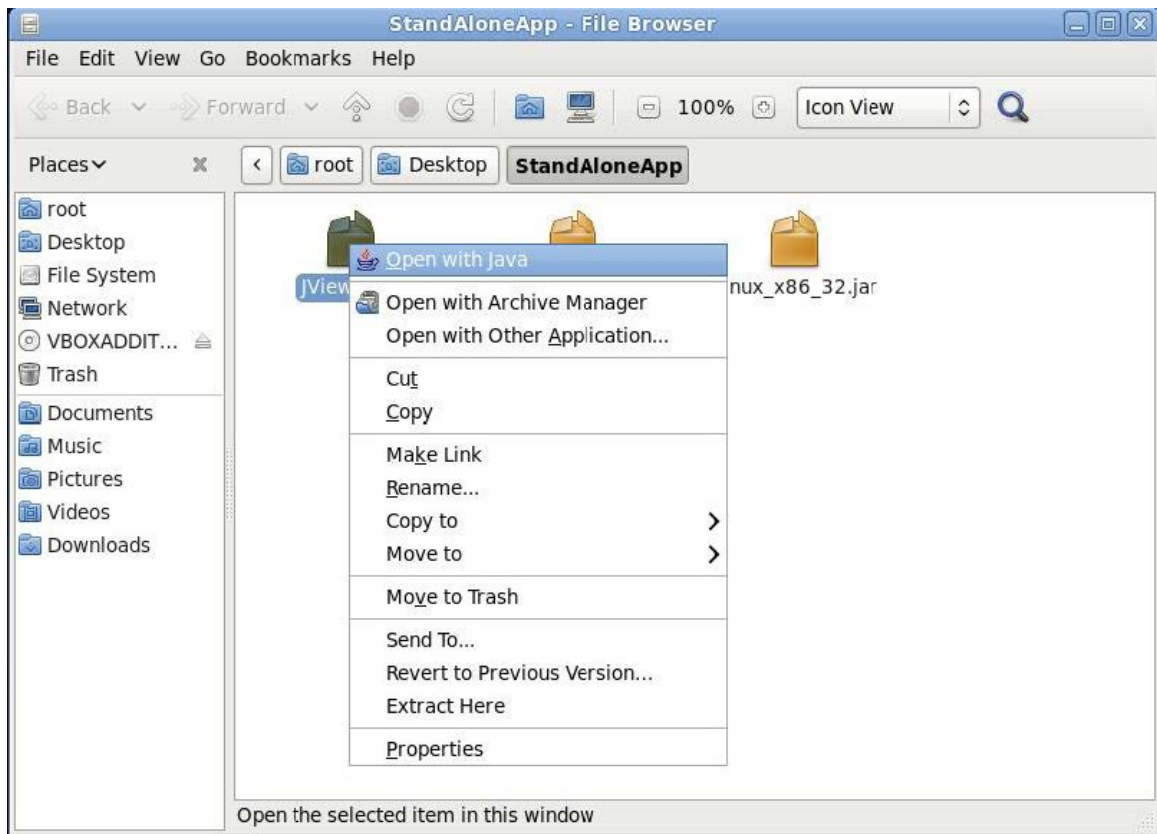


Figure 13. Launching JViewer standalone application from a GUI-based environment

Once the application is launched, an input dialog appears.

- Step 2. Specify the valid input values for host IP address, secure Web port, user name, and password in the input dialog.
A list of supported localization languages will be shown in a combo box list.
- Step 3. Select the required language from the combo box list.
Note: English will be selected by default.
- Step 4. Once all the valid inputs are entered, click **Connect** on the dialog to start KVM redirection.

Chapter 15. KVM OS and browser compatibility

This section lists out the supported KVM OS and browser compatibility.

JViewer/H5Viewer OS & Browser Compatibility		
Host OS (64 bit)	Client OS (64 bit)	Browser
Windows server 2016	Ubuntu Desktop 16.04	Firefox (on Ubuntu, Windows, Fedora)
Windows server 2012 R2	Ubuntu Desktop 14.04	Chrome (on Windows, Ubuntu, Fedora, MAC)
SLES server 12.1	Windows 10	IE (on Windows)
SLES server 11.4	Windows 8.1	Edge (on Windows 10)
RHEL 7.3	Fedora Workstation 26	Safari (on MAC)
RHEL 6.9	MAC 10.12	
Ubuntu server 16.04 (AST only)		
Ubuntu server 14.04 (AST only)		

- Media CD/DVD performance is getting worse if the test image includes redfish relative processes.
- On Pilot IV w/ SLES 12.1 and RHEL 7.3, some performance issues might happen if a valid Pilot- IV video driver is not installed. Ensure that kernel update has been executed before running these combinations.
- Users are advised to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issues in absolute mouse mode.

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.

IE:

- To use IPv6 H5Viewer sessions in the IE browser, IPv6 addresses should be mentioned in literal format.
- When using the Japanese language, a user can change the language input method only using the mouse. The keyboard input method switching will not work.
- If the CD media file choosing dialog is kept open, the background functionality of threads might get affected.

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.

Appendix A. Notices

Lenovo may not offer the products, services, or features discussed in this document in all countries. Consult your local Lenovo representative for information on the products and services currently available in your area.

Any reference to a Lenovo product, program, or service is not intended to state or imply that only that Lenovo product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any Lenovo intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any other product, program, or service.

Lenovo may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document is not an offer and does not provide a license under any patents or patent applications. You can send inquiries in writing to the following:

*Lenovo (United States), Inc.
8001 Development Drive
Morrisville, NC 27560
U.S.A.
Attention: Lenovo Director of Licensing*

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

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

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

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the result obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Trademarks

LENOVO and LENOVO logo are trademarks of Lenovo.

Intel is a trademark of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

Microsoft, Windows, and Windows Server are trademarks of the Microsoft group of companies.

Linux is a registered trademark of Linus Torvalds.

All other trademarks are the property of their respective owners. © 2020 Lenovo

Lenovo