BMC

Delphinus Serverboard
User's Manual

UM_Delphinus BMC_v1.1_042522

Table of Contents

Document Release History

Release Date	Version	Update Content
December, 2021	1	Manual release to public.
April, 2022	1	System alert setting update.

Preface

Copyright

Trademarks

Changes

The material in this document is for information purposes only and is subject to change without notice.

Warning

1. A shielded-type power cord is required in order to meet FCC emission limits and also to prevent interference to the nearby radio and television reception. It is essential that only the supplied power cord be used.
2. Use only shielded cables to connect I/O devices to this equipment.
3. You are cautioned that changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

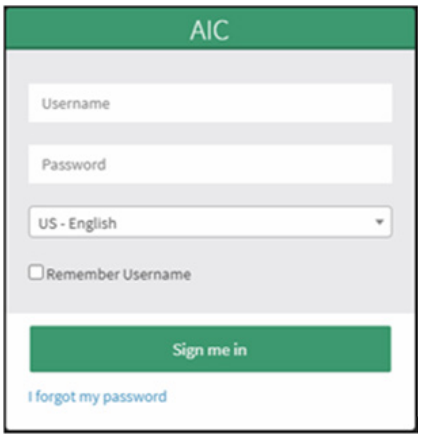
Disclaimer

AIC® shall not be liable for technical or editorial errors or omissions contained herein. The information provided is provided "as is" without warranty of any kind. To the extent permitted by law, neither AIC® or its affiliates, subcontractors or suppliers will be liable for incidental, special or consequential damages including downtime cost; lost profits; damages relating to the procurement of substitute products or services; or damages for loss of data, or software restoration. The information in this document is subject to change without notice.

Chapter 1. Login Information

1.1 User Name and Password

Initial access prompts you to enter the User Name and Password. A sample screenshot of the login screen is given below.



The fields are explained as follows:

Username: Enter your username in this field.

Password: Enter your password in this field.

Language Selection: Language selection drop-down will be populated based on supported languages in Web UI as a part of multi language support feature. Drop-down option value will be selected based on the browser language. For example, if browser language is configured with Simplified Chinese language (ZH-CN), then option value will be auto selected as China. Default language will be selected as US-English if the browser configured language not supported by Web UI. Entire Web UI pages language strings will be displayed based on selected language from drop-down.

Remember Username: Check this option to remember your login Username. 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.

Sign me in: After entering the required credentials, click the Sign me in to login.

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

Connect to your BMC web page.

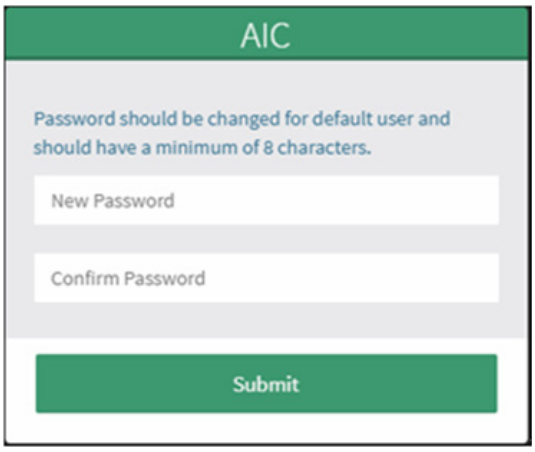
Type the default account and password.

Account: admin

Password: admin

1.2 Need for Password Change

It is mandatory to change the password for the default user at first successful login due to California Law SB-327 security fix. If the authentication is successful, then Web UI will prompt a new page which will ask to change the user password. Once the password is changed, login page will be reloaded. Enter the username and modified password to Login. A sample screenshot is given below.



Default User's password can be changed using any of the following method.

- IPMI Tool
- Web UI

> **NOTE**
> The last password used cannot be used to reset the password.

1.3 Required Browser Settings:

Allow file download from this site: For Internet Explorer, choose Tools → Internet Options → Security Tab, based on device setup, select among Internet, Local intranet, trusted sites and restricted sites. Click Custom level. In the Security Settings - Zone dialog opened, under settings, find Downloads option, Enable File download option. Click OK to the entire dialog boxes.

For all Other Browsers, accept file download when prompted.

Enable javascript for this site: The icon indicates whether the javascript setting is enabled in browser.

Enable cookies for this site: The icon indicates whether the cookies setting are enabled in browser.

> **NOTE**
> Cookies must be enabled in order to access the website.

1.4 Default User Name and Password

Username: admin

Password: admin

NOTE

The default user name and password are in lower-case characters. When you log in using the user name and password, you get full administrative rights. It is advised to change your password once you login.

Duplicate user names shouldn't exist across various authentication methods like AD, LDAP, RADIUS or IPMI since the privilege of one Authentication method is overwritten by another authentication method when login and hence the correct privilege cannot be returned properly. Duplicate user names shouldn't be existed across different channels in IPMI.

If any changes occurred for RADIUS in authentication order, then the User ID's of logged in users using other authentication services will be shown as RADIUS User ID. So, it is recommended to keep RADIUS as last in PAM Order.

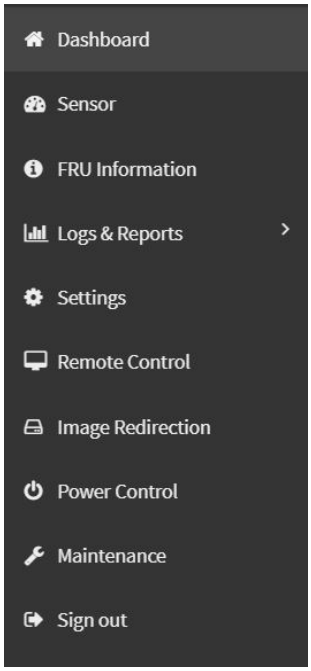
NOTE:
Once you login to the application, it is recommended not to use the following options.
- Refresh button of the browser
- Refresh menu of the browser
- Back and Forward options of the browser
- F5 on the keyboard
- Backspace on the keyboard

1.5 Menu Bar

The menu bar displays the following.

Firmware Information will be displayed with the latest version, date and time details. Power Control Status will be displayed as Host Online. To change the Power Control Status, click Host Online link.

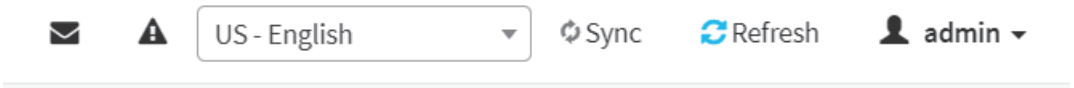
- Dashboard
- Sensor
- FRU Information
- Logs & Report
- Settings
- Remote Control
- Image Redirection
- Power Control
- Maintenance
- Sign out



1.6 Quick Button and Logged-in User

The user information and quick buttons are located at the top right. A screenshot of the logged-in user information is shown below.

User Information
The logged-in user information shows the logged-in user, his/her privilege and the four quick buttons allowing you to perform the following functions.



Logged-in user and its privilege level
This option shows the logged-in user name and privilege. There are five kinds of privileges.

User: Only valid commands are allowed.

Operator: All BMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.

Administrator: All BMC commands are allowed.

No Access: Login access denied.

OEM: All OEM commands are allowed.

Message: Click the icon to view the event log alert messages. On clicking the messages, it will navigate to the Logs and Reports page.

Language Selection: Change the language to view the language strings in different languages.

Refresh: Click the Refresh icon or pressing key F5 to reload the current page.

Sync: Click the Sync icon to synchronize with Latest Sensor and Event Log updates.

Signout: Click the Sign out icon to log out.

Notification: Click to view the notification received.

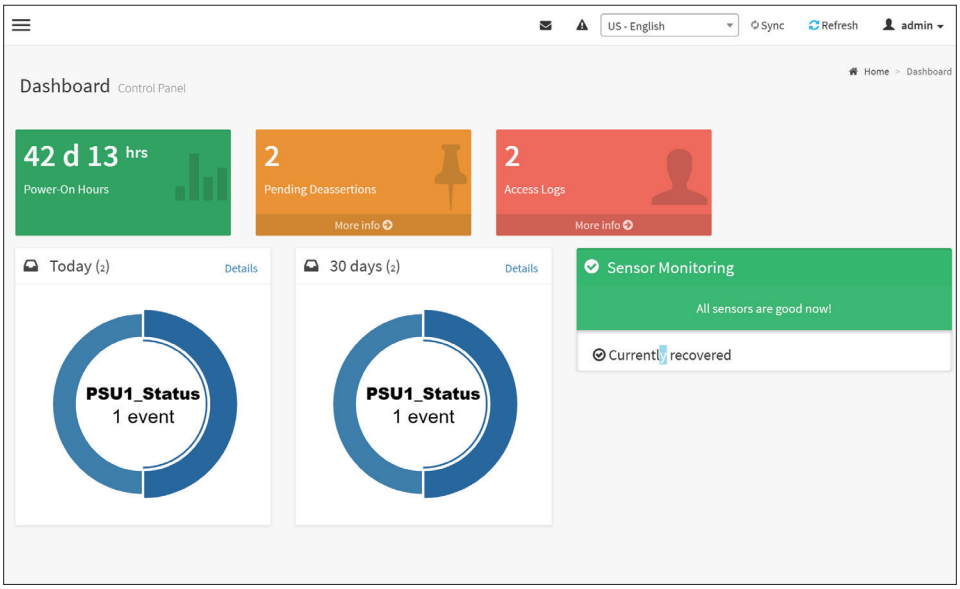
Quick Search: Quick Search is a short-cut for the available menu and sub-menu pages. It displays available search queries. Click US - English (Quick Search) field, and type search terms of the lists in the menu bar. As you type, the suggestions will be displayed in a drop-down list below the Quick Search field as a navigational links of the menu and sub-menu. On selecting your search term from the drop-down list, it will directly go to the specific page which you have searched.

Help

Help - The Help icon ( ) is Located at the top right of each page. Click this help icon to view more detailed field descriptions.

Chapter 2. Dashboard

The Dashboard page gives the overall information about the status of a device.
To open the Dashboard page, click Dashboard from the menu bar. A sample screenshot of the Dashboard page is shown below.



A brief description of the Dashboard page is given below.

Language Selection
Change the language to view the language strings in different languages.

BMC Power-On Hours
BMC Power-On Hours will keep on accumulated and will be reset to zero when you flash a new image.

Pending Deassertions
It lists all the asserted events which are waiting for deassert state. To know about the pending events details, click the More info link. This navigates to the Event Log page and display all the asserted events that are waiting for deassertion.

Access Logs
A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed. If you click on the More info link, you can view the Audit Log page.

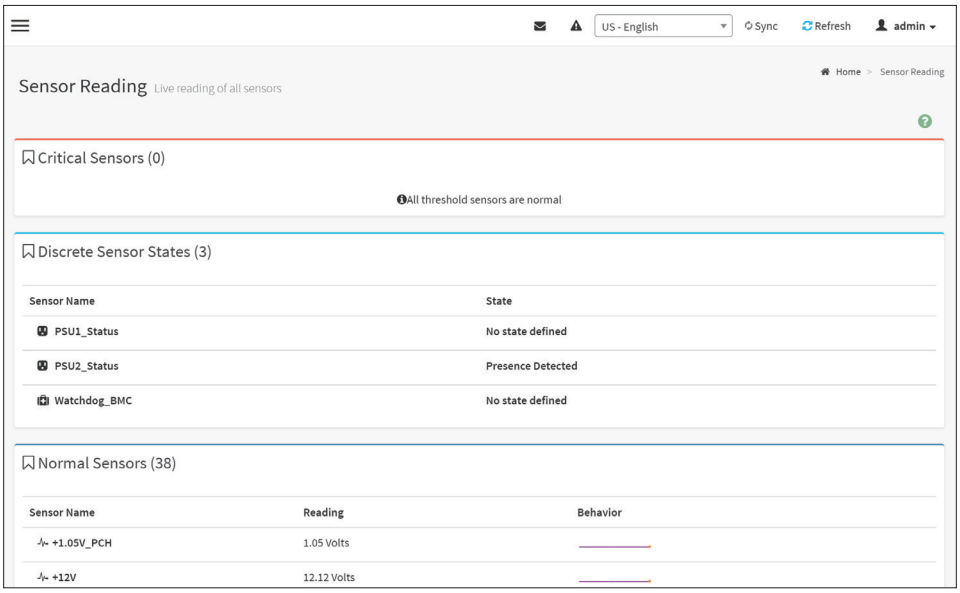
Today & 30 Days (Event Logs)
This page displays the list of event logs occurred by the different sensors on this device. Click Details link on Today and 30 days to view the event logs for Today and 30 days respectively.

Sensor Monitoring
It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

Chapter 3. Sensor

The Sensor Reading page displays all the sensor related information.

To open the Sensor Reading page, click Sensor from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events. A screenshot of Sensor Reading page is given below.

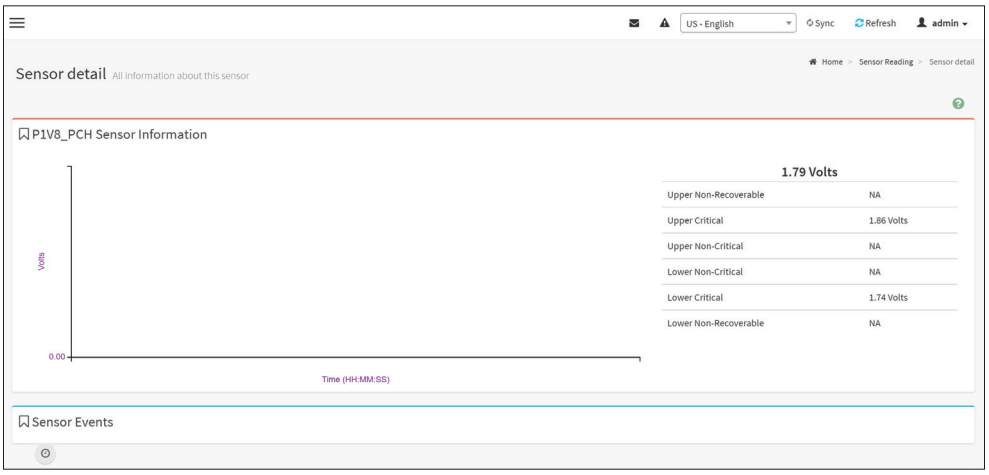


Sensor Reading Page

The Sensor Reading page contains the following information.
In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behaviour will be appeared, else you can choose the sensor type that you want to display from the list. Some examples for sensors are Temperature Sensors, Fan Sensors, Watchdog Sensors and Voltage Sensors etc.

Sensor detail

Select a particular Sensor from the Critical Sensor or Normal Sensor lists. The Sensor Information as Live Widget and Thresholds for the selected sensor will be displayed as shown below.



NOTE
Widgets are little gadgets, which provide real time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget. The session will not expire, until the widgets gets a live data of the last widget that is kept opened.

For the selected sensor, this widget gives a dynamic representation of the readings for the sensor. Thresholds are of six types:
• Lower Non-Recoverable (LNR)
• Lower Critical (LC)
• Lower Non-Critical (LNC)
• Upper Non-Recoverable (UNR)
• Upper Critical (UC)
• Upper Non-Critical (UNC)

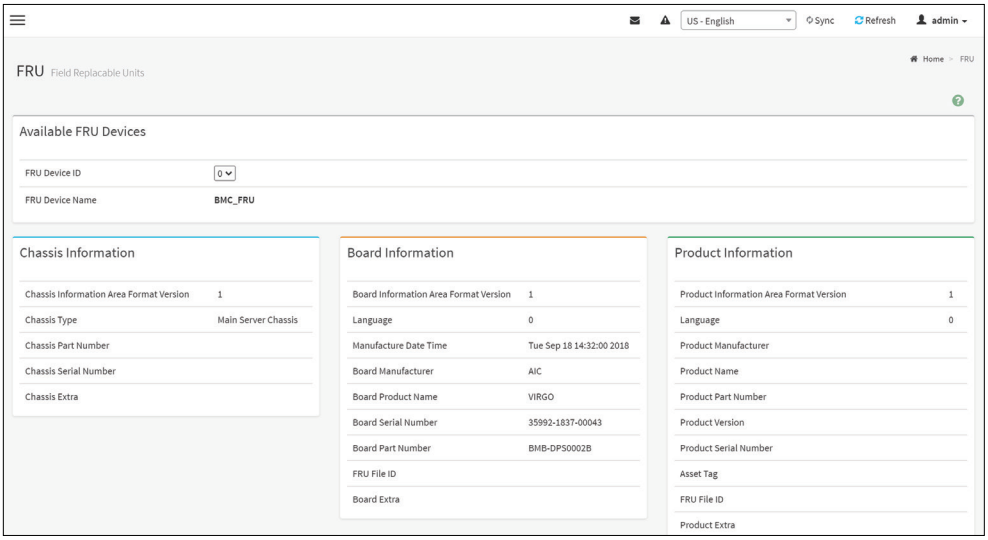
The threshold states could be Lower Non-critical - going low, Lower Non-critical - going high, Lower Critical - going low, Lower Critical - going high, Lower Non-recoverable - going low, Lower Non-recoverable - going high, Upper Non-critical - going low, Upper Non-critical - going high,Upper Critical - going low, Upper Critical - going high, Upper Non-recoverable - going low, Upper Non-recoverable - going high.

View this Event Log
You can click here to view the Logs & Reports for the selected sensor.

Chapter 4. FRU Information

FRU Information page displays the BMC's FRU device information. FRU page shows information like Basic Information, Chassis Information, Board Information and Product Information ofthe FRU device.

To open the FRU Information page, click FRU Information from the menu bar. Select a FRU Device ID from the FRU Information section to view the details of the selected device. A screenshot of FRU Information page is given below.



FRU Information Page

The following fields are displayed here for selected device.

Available FRU Devices

- FRU device ID - Select the device ID from the drop down list
- FRU Device Name - The device name of the selected FRU device.

Chassis Information

- Chassis Information Area Format Version
- Chassis Type
- Chassis Part Number
- Chassis Serial Number
- Chassis Extra

Board Information

- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

Product Information

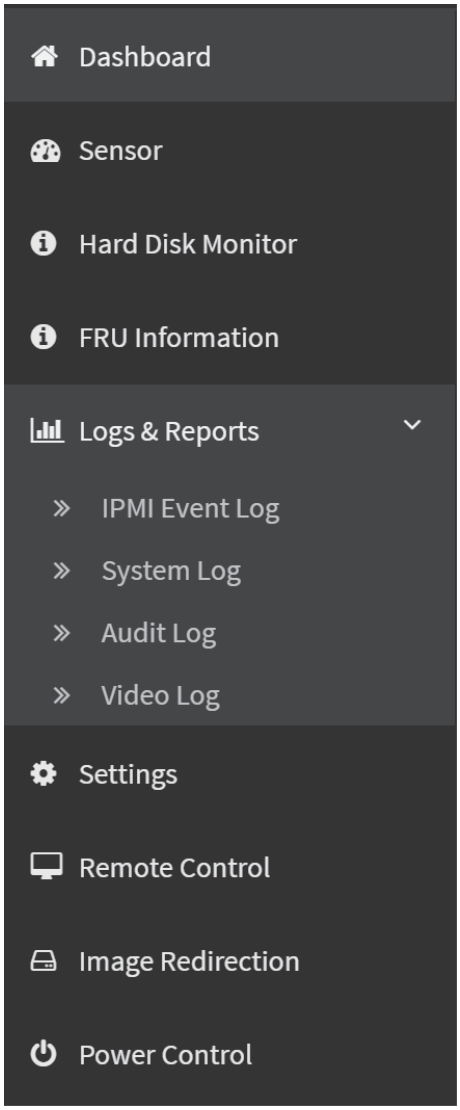
- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Serial Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

Chapter 5. Logs & Reports

The Logs & Reports page displays the following information.

- IPMI Event Log
- System Log
- Audit Log
- Video Log

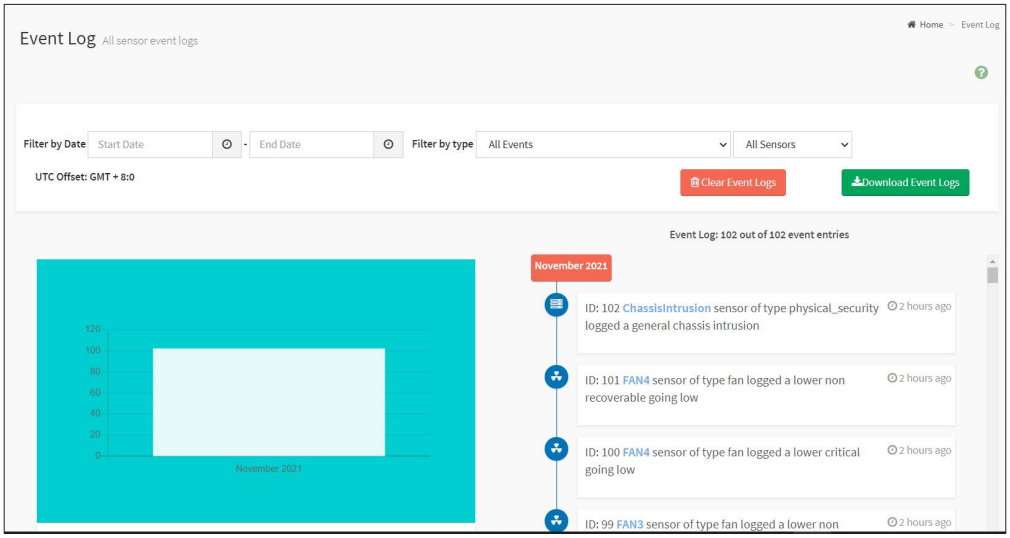
A screenshot displaying the menu items under Logs & Reports is shown below.



5.1 IPMI Event Log

This page displays the list of event logs occurred by the different sensors on this device. Double click on a record to see the details of that entry. You can use the sensor type or sensor name filter options to view those specific events or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click Logs & Reports → Event Log from the menu bar. A sample screenshot of Event Log page is shown below.



The Event Log page consists of the following Fields.

Filter By Date: Filtering can be done by selecting Start Date and End Date using Calender.

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

Filter By Type: The category could be either All Events, System Event Records, OEM Event Records, BIOS Generated Events, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console Software Events, Terminal Mode Remote Console software Events.

> **NOTE**
> Once the Filter By Date and Filter type are selected, the list of events will be displayed with the Event ID, Time Stamp, Sensor Type, Sensor Name and Description.

UTC Offset: Displays the current UTC Offset value based on which event Time Stamps will be updated. Navigational arrows can be used to selectively access different pages of the Event Log.

Event Log Statistics: Displays the statistical graph for the selected date.

Clear Event Logs: To delete all the event logs.

Download Event Logs: To download the event logs.

Download Interpreted Event Logs: To download the interpreted event logs.

Procedure:

1. From the Filter By Date field, select the time period by Start Date and End Date using Calendar for the event categories. The events will be displayed according to the selected date.
2. From the Filter By Type field, select the Type of the event and Sensor name to view the events for the date. The events will be displayed based on the selected time period.
3. To clear all events from the list, click Clear All Event Logs.
4. To download the event logs, click Download Event Logs.

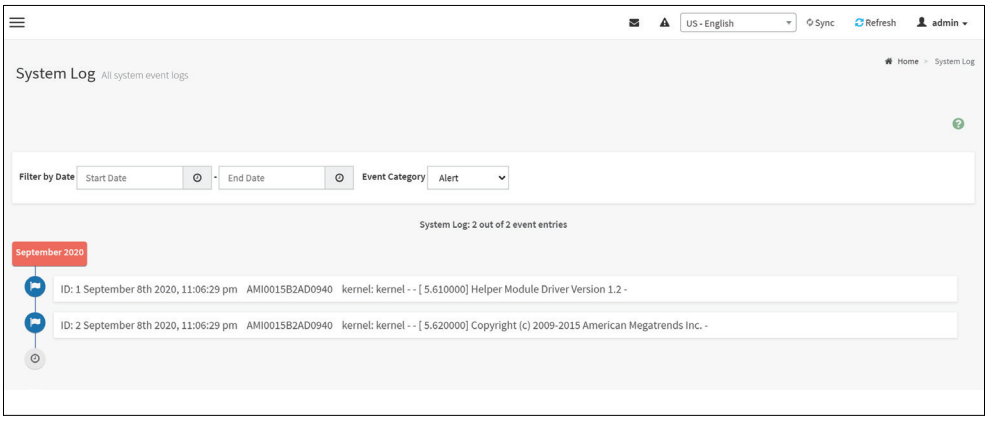
> **NOTE**
> When Clear All Event Logs action is performed, there might be some events present even after clearing those events are generated after performing clear operation which can be verified using its time stamp.

5.2 System Log

System Log page will display all the system events occurred in this device that has been already configured.

> **NOTE**
> Logs have to be configured under Settings → Log Settings in order to display any entries.

To open the Event Log page, click Logs & Reports → System Log from the menu bar. A sample screenshot of System Log page is shown below.



Procedure

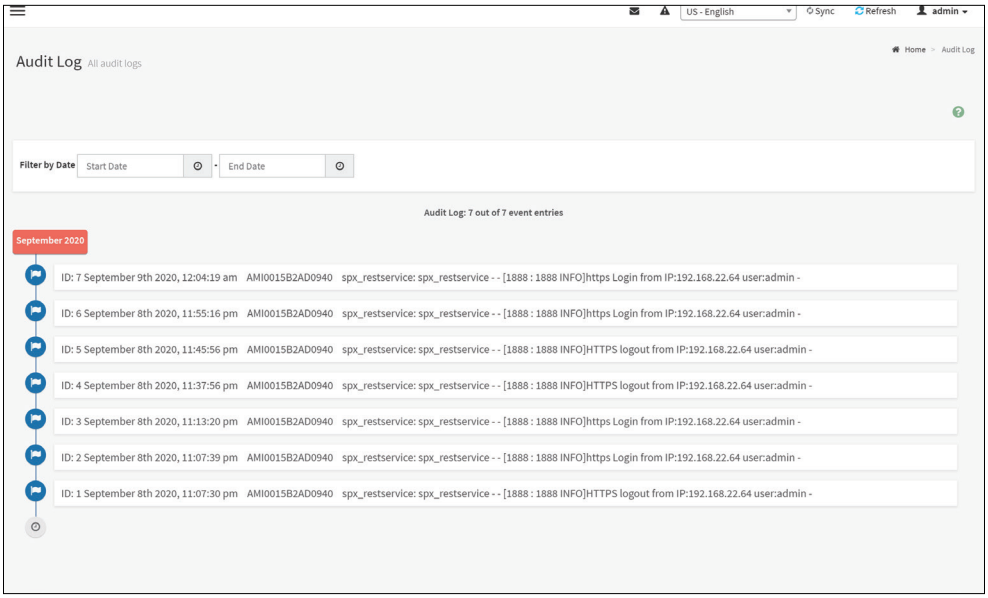
To view System Log, click the System Log tab to view all system events. Entries can be filtered based on Filter By Date (Start Date and End Date) and Event Category like Alert, Critical, Error, Notification, Warning, Debug, Emergency and Information.

5.3 Audit Log

Audit Log page will display all the system events occurred in this device that has been already configured.

> **NOTE**
> Logs have to be configured under Settings→ Log Settings→ Advanced Log Settings in order to display any entries.

To open the Event Log page, click Logs & Reports → Audit Log from the menu bar. A sample screenshot of Audit Log page is shown below.



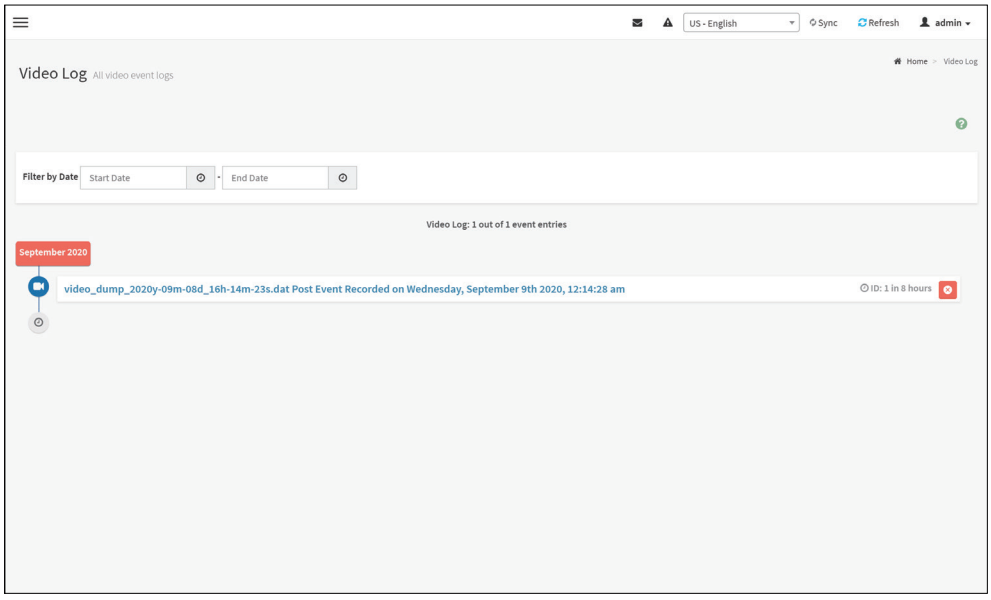
Procedure
To view Audit Log, click the Audit Log tab to view all audit events for this device.

5.4 Video Log

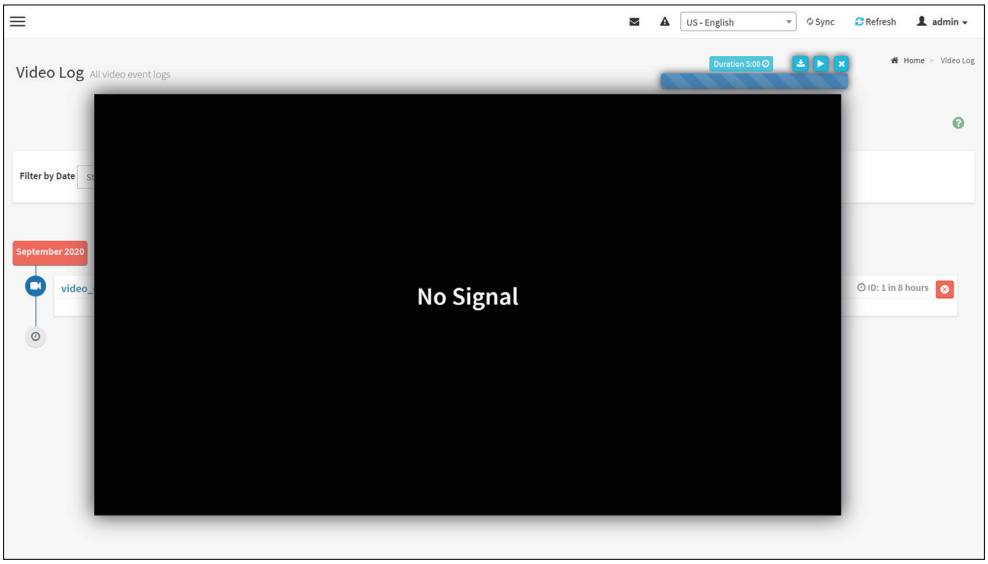
To open the Video Log page, click Logs & Reports → Video Log from the menu bar. A sample screenshot of Video Log page is shown below.

> **NOTE**
> Video Trigger Settings should be enabled, to display the Video Log page. Video Trigger Settings can be configured under Settings → Video Recording → Auto Video Settings → Video Trigger Settings.

Procedure
The video data may not be proper if the browser zoom in/out settings are changed during video playback.



1. Click on the Video Log entry to view the Video. A sample screenshot of Video Log - Video page is shown below.

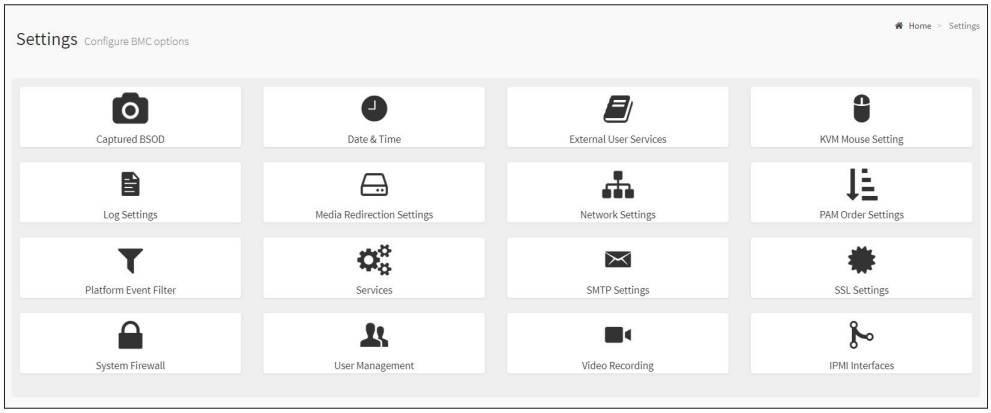


2. You can Download (), Play/Pause () and Delete () the video by clicking the respective icons.

> **NOTE**
> Video will be allowed to play/download only if file size is lesser than 40MB. Browsers have various memory restrictions, due to this browser cannot store and process data greater than 40MB (approximately). If file size is greater than 40MB, user will be notified with a message to use Java player Application.

Chapter 6. Settings

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

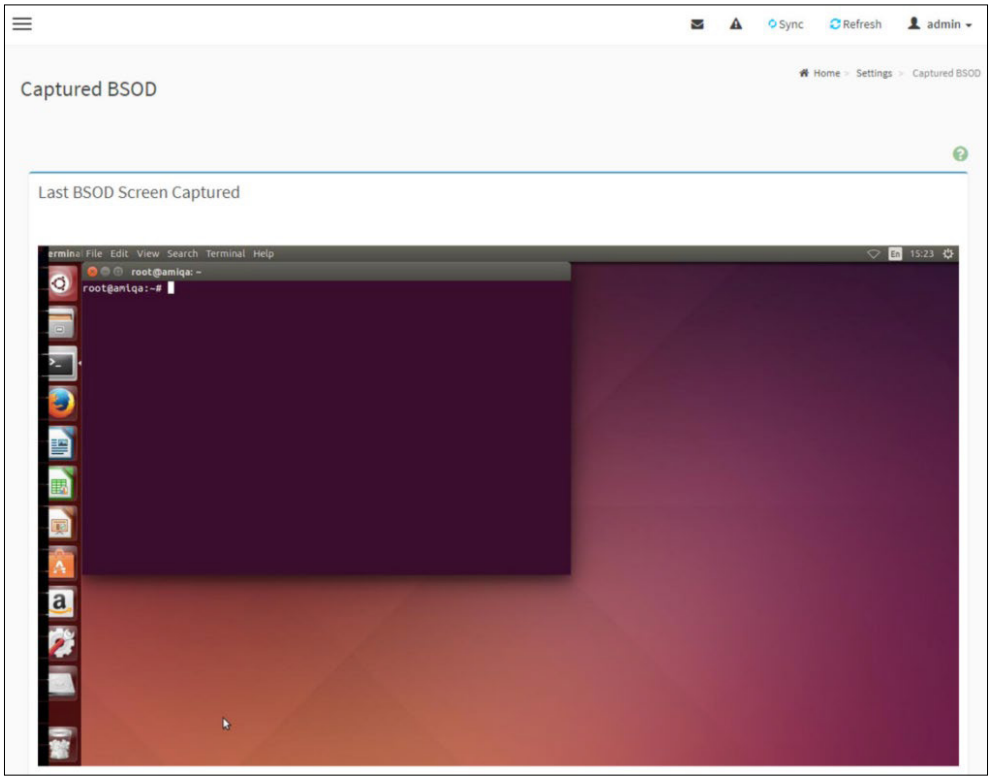


Configuration Group Menu
A detailed description of the Configuration menu is given below.

6.1 Captured BSOD

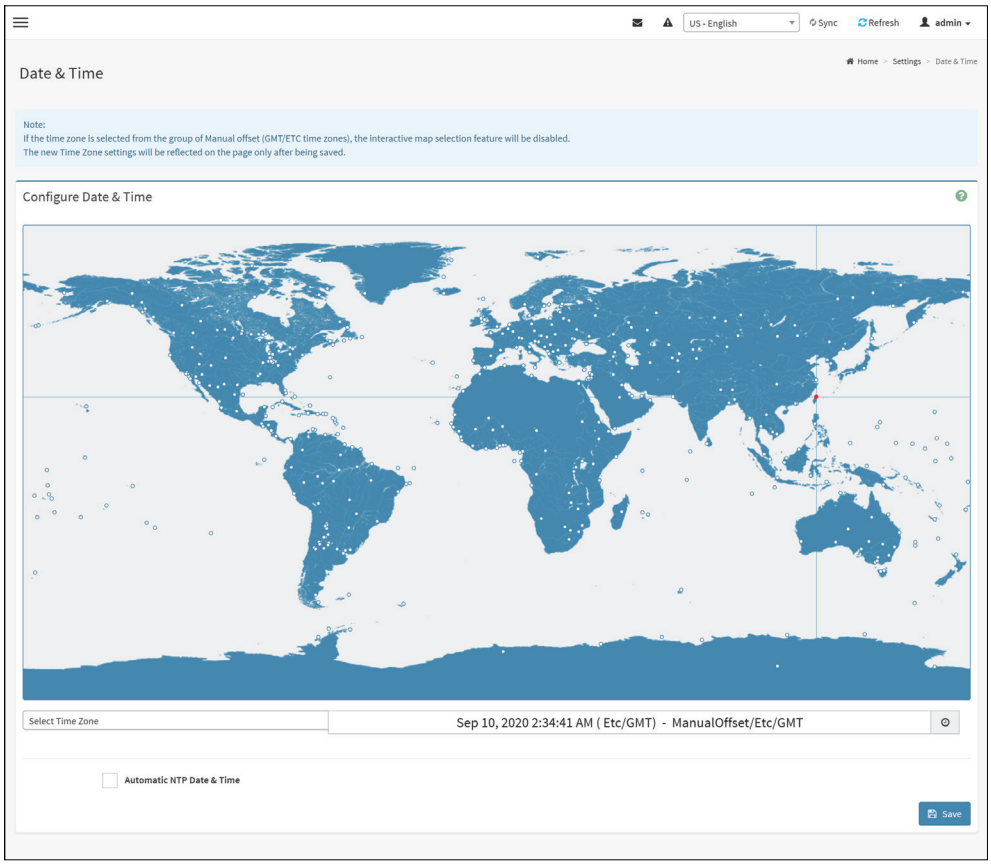
This page displays a snapshot of the blue screen captured if the host system crashed since last reboot. A screenshot of Captured BSOD is shown below.

> **NOTE**
> KVM service should be enabled to display the BSOD screen. KVM Service can be configured under Settings → Services → KVM.



6.2 Date and Time

This field is used to set the date and time on the BMC. A sample screenshot of Date & Time is shown as below.



The Date & Time section consists of the following fields.

Configure Date & Time: Displays Timezone 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 Date & Time: To automatically synchronize Date and Time with the NTP Server.

- **Primary NTP Server**: To configure a primary NTP server to use when automatically setting the date and time.
- **Secondary NTP Server**: To configure a secondary NTP server to use when automatically setting the date and time.

Save: To save the settings.

> **NOTE**
> If the timezone is selected as Manual Offset, the map selection will be disabled. The Time Zone settings will be reflected only after saving the settings.

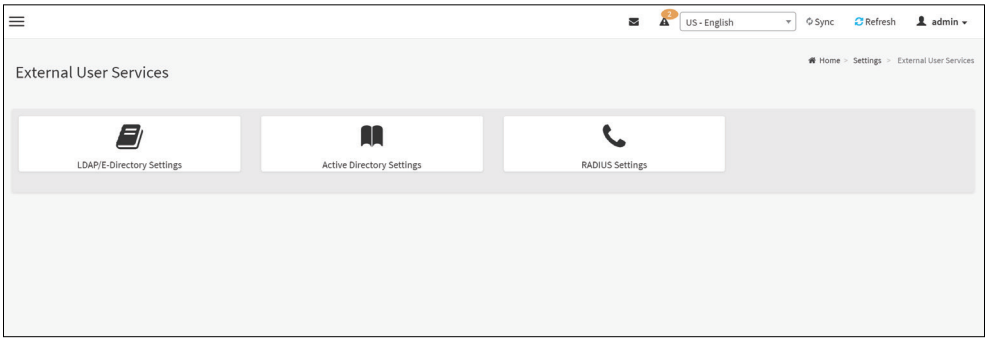
6.3 External User services

6.3.1 LDAP/E-Directory Settings

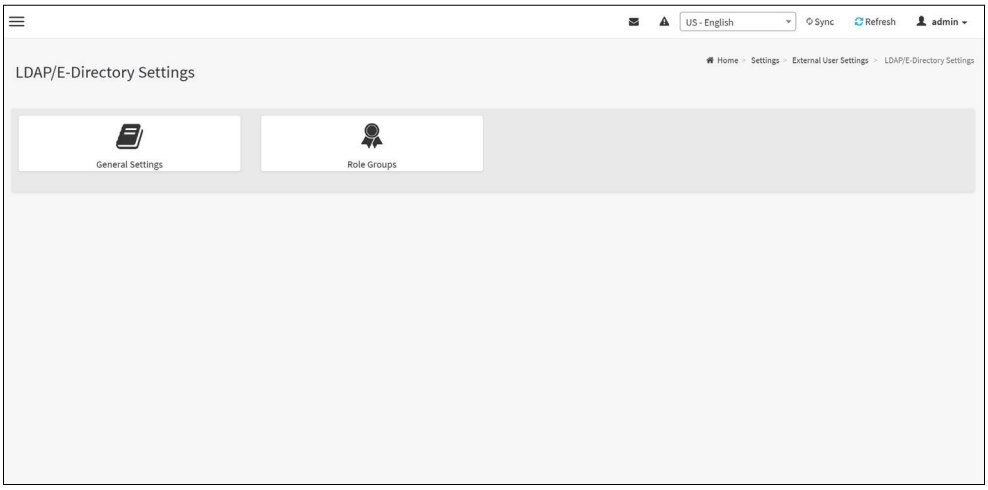
The Lightweight Directory Access Protocol (LDAP)/E-Directory Settings is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

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

To open External User Services page, click Settings → External User Services from the menu bar. A sample screenshot of External User Services page is shown below.



To open LDAP/E-DIRECTORY Settings page, click Settings → External User Services → LDAP/E Directory Settings from the menu bar. A sample screenshot of External User Services page is shown below.



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

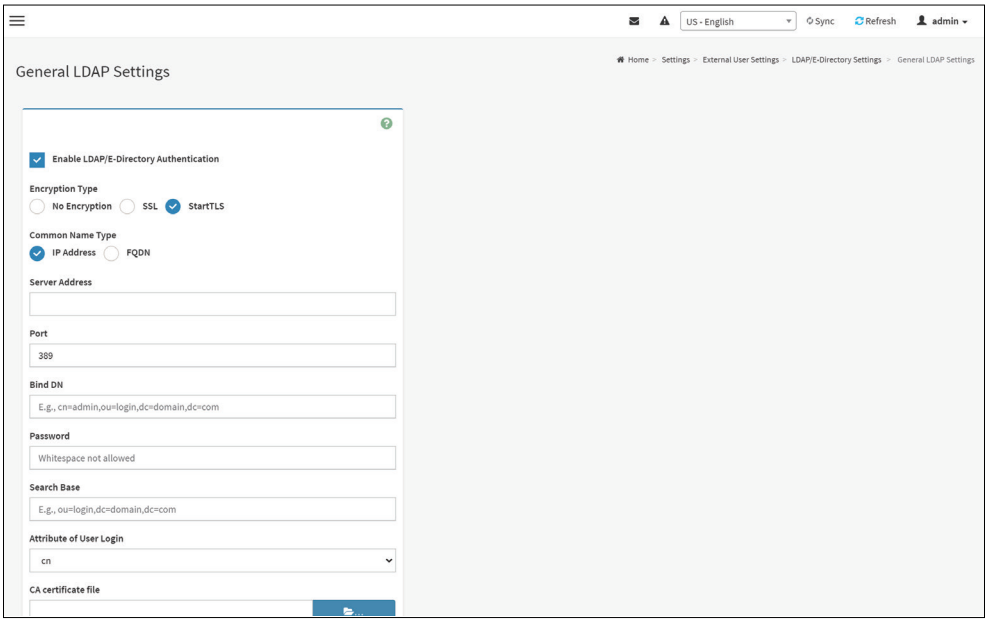
General Settings: To configure LDAP/E-Directory Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port and Search base.

Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Procedure

Entering the details in General LDAP/E-Directory Settings page

1. In the LDAP/E-Directory Settings page, click General Settings. A sample screenshot of General LDAP Settings page is given below.



2. Click Enable LDAP/E-Directory Authentication, to enable LDAP/E-Directory Settings.

> **NOTE**
> During login prompt, use username to login as an Idap Group member.

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

> **NOTE**
> Configure proper port number when SSL is enabled.

4. Select the Commoon Name Type as IP Address.
5. Enter the IP Address of LDAP server in the server address field.

> **NOTE**
> IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'. Each number ranges from 0 to 255. First number must not be 0. Supports IPv4 format and IPv6 format. Configure FDQN address when using StartTLS with FDQN.

6. Specify the LDAP Port in the port field.

> **NOTE**
> Default port is 389. For SSL connections, default port is 636. The port value ranges from 1 to 65535.

7. Specify the Bind DN that is used during bind operation, which authenticates the client to the server.

> **NOTE**
> Bind DN is a string of 4 to 64 alpha-numeric characters. It must start with an alphabetical character. Special symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to (=), are allowed.
> Example: cn=manager, ou=login, dc=domain, dc=com

8. Enter the password in the password field.

> **NOTE**
> Password must be at least 1 character long. White space is not allowed. This field will not be allowed for more than 48 characters.

9. Enter the search base. The search base tells the LDAP server which part of the external directory tree to search. The search base may be something of equivalent to the organization, group of external directory.

> **NOTE**
> Search base is a string of 4 to 63 alpha-numeric characters. It must start with an alphabetical character. Special symbols like dots (.), comma(,), hyphen(-), underscore(_), 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**
> It only supports cn or uid.

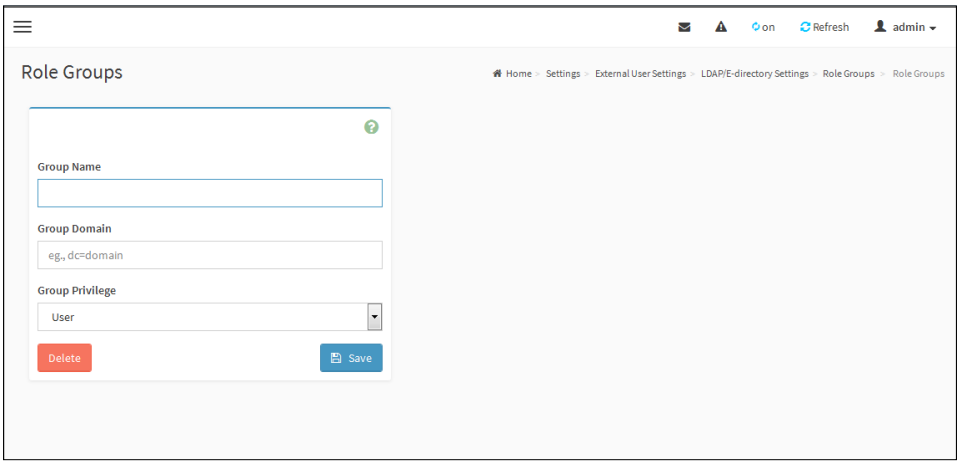
11. Select CA Certificate File from the Browse field to identify the certificate of the trusted CA certs.
12. Select the Certificate File to find the client certificate filename.
13. Select Private Key to find the client private key filename.

> **NOTE**
> All the 3 files are required, when StartTLS is enabled.

14. Click Save to save the settings.

To add a new Role Group

1. In the LDAP/E-Directory Settings page, click Role Groups and select a blank row.
2. Click Add Role Group or alternatively double click on the blank row to open the Add Role group page as shown in the screenshot below.



3. In the Group Name field, enter the name that identifies the role group.

> **NOTE**
> Role Group Name is a string of 255 alpha-numeric characters.
> Special symbols hyphen and underscore are allowed.

4. In the Group Domain field. Enter the Role Group Domain where the role group is located.

> **NOTE**
> - Domain Name is a string of 4 to 64 alpha-numeric characters.
> - It must start with an alphabetical character.
> - Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
> - Example: cn=manager,ou=login, dc=domain,dc=com

5. In the Group Privilege field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
6. Select the required options or both
   • KVM Access
   • VMedia Access
7. Click Save to save the new role group and return to the Role Group List.

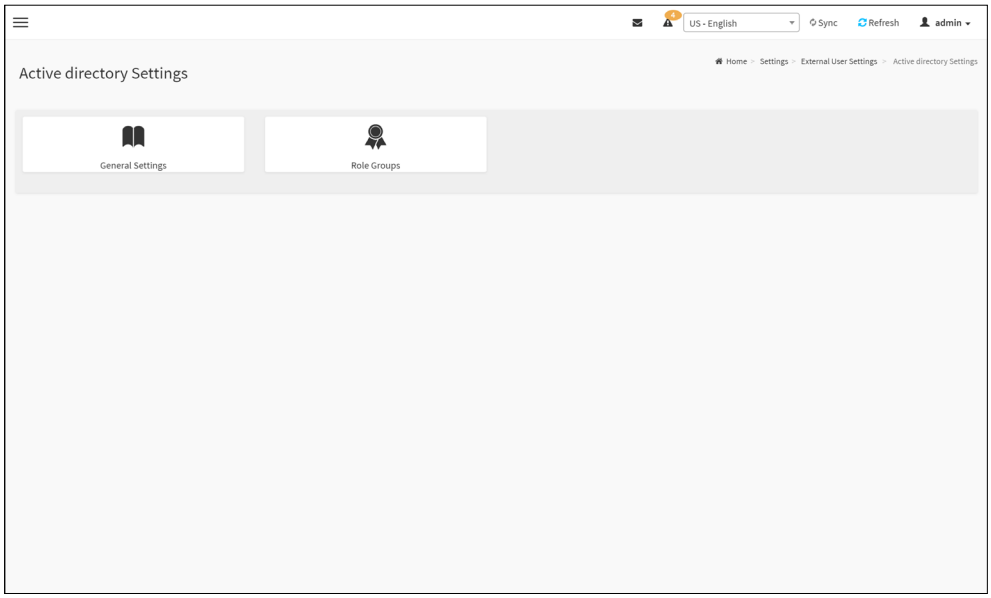
6.3.2 Active Directory Settings

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.

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. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group.

> **NOTE**
> To view the page, you must be at least a User and to modify or add a group, you must be an Administrator.

To open Active Directory Settings page, click Settings → External User Settings → Active Directory from the menu bar. A sample screenshot of Active Directory Settings page is shown below.

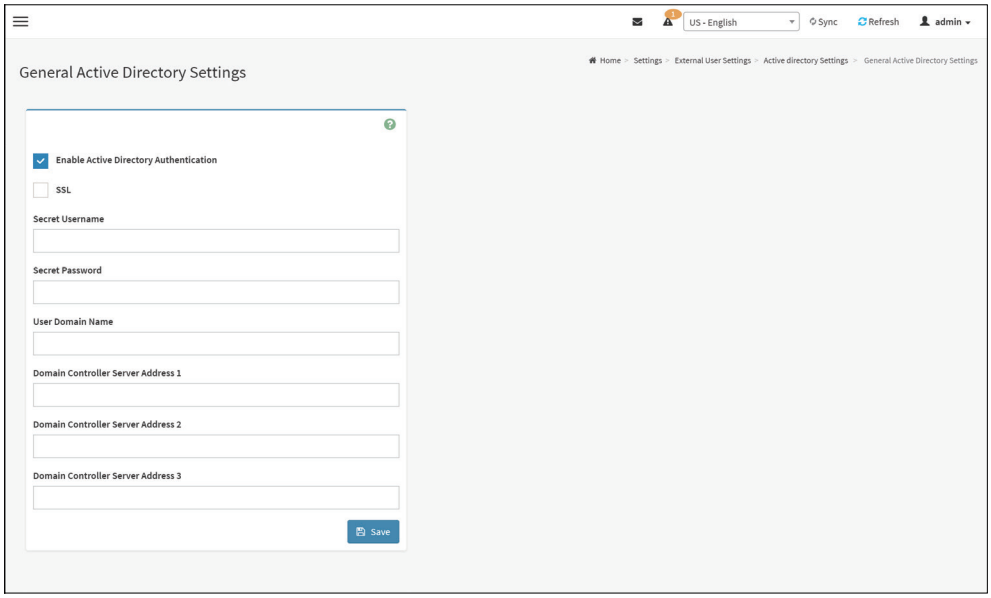


The fields of Active Directory page are explained below.

General Settings: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.

Role Groups: To add a new role group to the device. Alternatively, double click on a free slot to add a role group.

Procedure:
Entering the details in General Active Directory Settings page
1. Click on General Settings to open the General Active Directory Settings page.



2. In Active Directory Setting page, check or uncheck Authentication respectively.

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

3. Specify the secret user name and password in the Secret User Name and Secret Password respectively.

> **NOTE**
> - Secret username/password for AD is not mandatory. When secret username & password is empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So it is recommended to keep AD in the last location in PAM order.
> - User Name is a string of 1 to 64 alpha-numeric characters.
> - It must start with an alphabetical character.
> - It is case-sensitive.
> - Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.
> - Password must be at least 6 character long and will not allow more than 127 characters.
> - White space is not allowed.

4. Specify the Domain Name for the user in the User Domain field. E.g. MyDomain.com

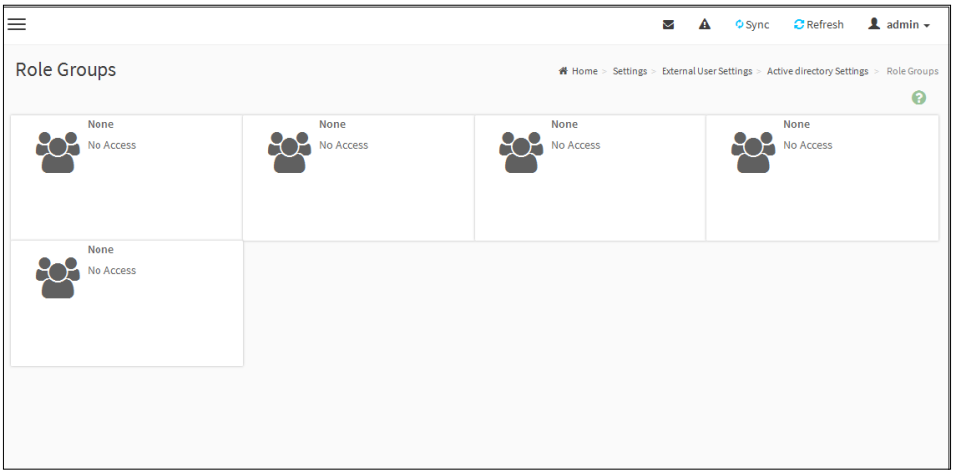
5. Configure IP addresses in Domain Controller Server Address1, Domain Controller Server Address2 and Domain Controller Server Address3

> **NOTE**
> IP address of Active Directory server: At least one Domain Controller Server Address must be configured.
> - IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
> - Each number ranges from 0 to 255.
> - First number must not be 0.
> - Domain Controller Server Addresses will supports IPv4 Address format and IPv6 Address format.

6. Click Save to save the entered settings and return to Active Directory Settings page.

Role Groups

To open Role Group page, click Settings → External User Settings → Active Directory → Role Groups from the menu bar. A sample screenshot of Role Groups page is shown below.



The fields of Role Group page are explained below.

Role Group Name: The name that identifies the role group in the Active Directory.

> **NOTE**
> Role Group Name is a string of 64 alpha-numeric characters.
> Special symbols hyphen and underscore are allowed.

Group Name: This name identifies the role group in Active Directory.

> **NOTE**
> Role Group Name is a string of 64 alpha-numeric characters. Special symbols hyphen and underscore are allowed.

Group Domain: The domain where the role group is located.

> **NOTE**
> Domain Name is a string of 255 alpha-numeric characters. Special symbols hyphen, underscore and dot are allowed.

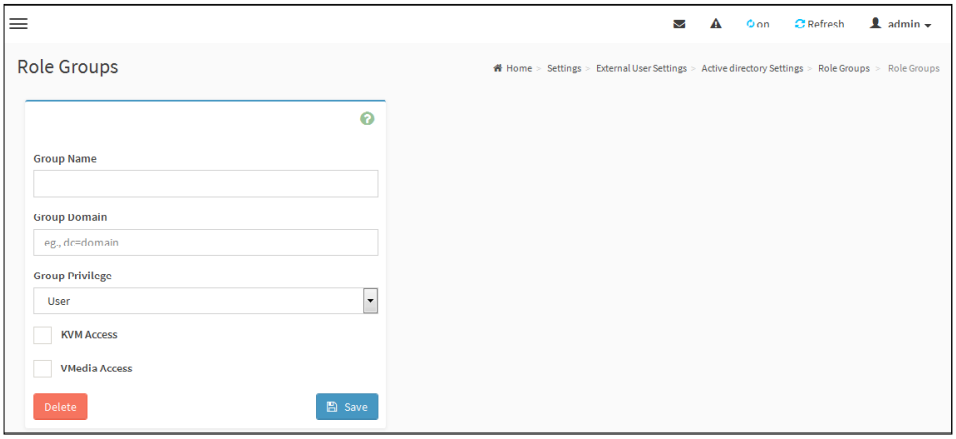
Group Privilege: The level of privilege to assign to this role group.

KVM Access: To provide access to KVM for AD authenticated role group user.

VMedia Access: To provide access to VMedia for AD authenticated role group user.

To add a new Role Group

1. In the Active Directory Settings page, select a Role Group and click Add Role Group or alternatively double click on the blank row to open the Add Role group page as shown in the screenshot below.



2. In the Group Name field, enter the name that identifies the role group in the Active Directory.

> **NOTE**
> - Role Group Name is a string of 64 alpha-numeric characters.
> - Special symbols hyphen and underscore are allowed.

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

> **NOTE**
> - Domain Name is a string of 255 alpha-numeric characters.
> - Special symbols hyphen, underscore and dot are allowed.

4. In the Group Privilege field, enter the level of privilege to assign to this role group.
5. Select the required options
   - KVM Access
   - VMedia Access
6. Click Save to add the new role group and return to the Role Group List.

To Delete a Role Group

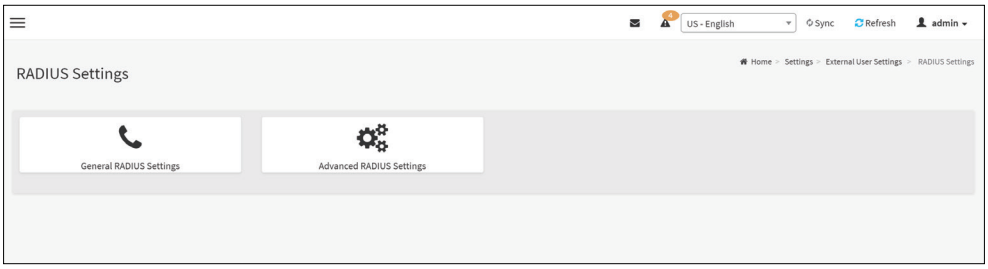
1. In the Role Groups page, select the row that you wish to delete.
2. Click Delete Role Group.

6.3.3 RADIUS Settings

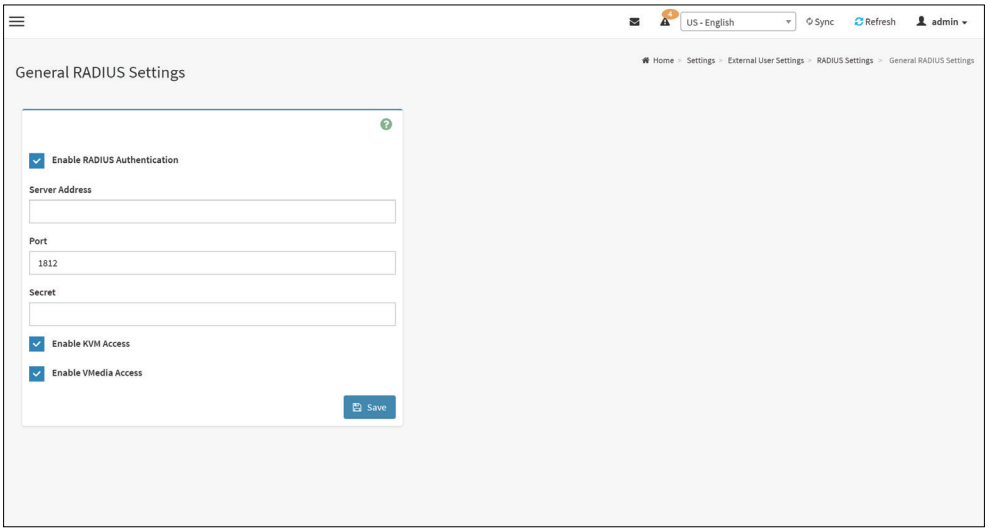
RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.

This page is used to set the RADIUS Authentication.

To open RADIUS Settings page, click Settings → External User Settings → RADIUS Settings from the menu bar. A sample screenshot of RADIUS Settings page is shown below.



General RADIUS Settings



The fields of General RADIUS Settings page are explained below.

Enable RADIUS Authentication: Option to enable/disable RADIUS authentication.

Server Address: The IP address of RADIUS server.

> **NOTE**
> - IP Address (Both IPv4 and IPv6 format).
> - FQDN (Fully Qualified Domain Name) format.

Port: The RADIUS Port number.

> **NOTE**
> - Default Port is 1812.
> - Port value ranges from 1 to 65535.

Secret: The Authentication Secret for RADIUS server.

> **NOTE**
> - This field will not allow more than 31 characters.
> - Secret must be at least 4 characters long.
> - White space is not allowed.

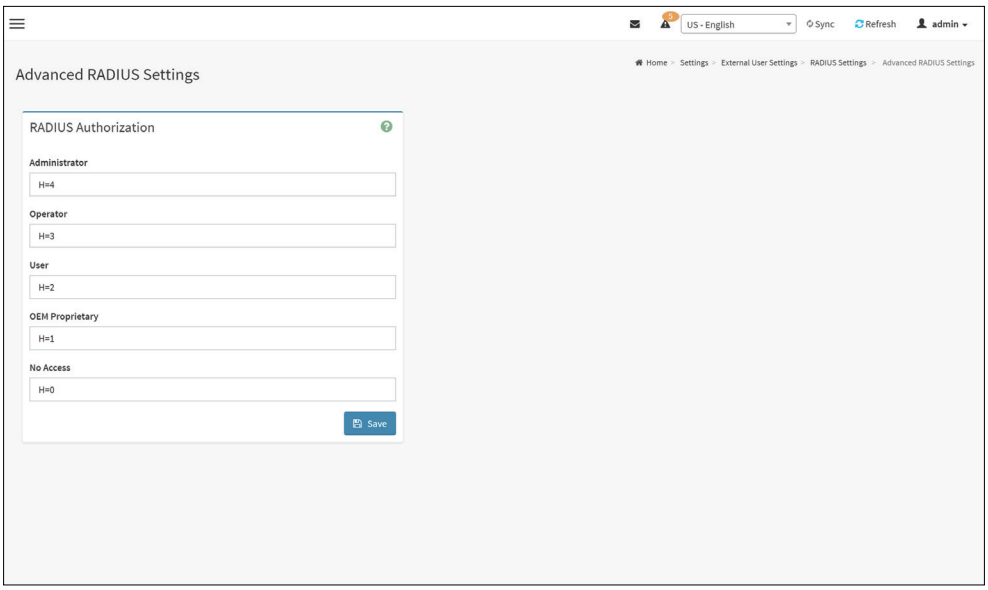
Enable KVM Access: This field provides access to KVM for RADIUS authenticated users.

Enable VMedia Access: This field provides access to VMedia for RADIUS authenticated users.

Save: To save the settings.

Procedure

1. Enable the RADIUS Authentication check box to authenticate the RADIUS.
2. Click Advanced RADIUS Settings. This opens the Radius Authorization window as shown below.



For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in Server side.

Example:1
testadmin Auth-Type :=PAP,Cleartext-Password:=”admin”
Auth-Type :=PAP, Vendor-Specific=”H=4”

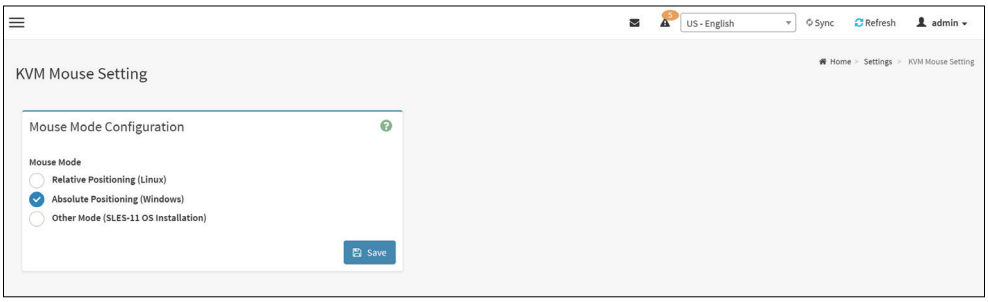
Example:2
testoperator Auth-Type := PAP,Cleartext-Password := “operator”
Auth-Type :=PAP, Vendor-Specific=”H=3”
If you change the Vendor-Specific value in server then you should change the same values in this page.

3. Click Save to save the changes made.

6.4 KVM Mouse Settings

Redirection Console handles mouse emulation from local window to remote screen in either of three methods. User has to be an Administrator to configure this option. To view the Supported Operating Systems for Mouse Mode, click Mouse Mode.

To open KVM Mouse setting page, click Settings → KVM Mouse Setting from the menu bar. A sample screenshot of KVM Mouse Settings page is shown below.



The fields of KVM Mouse Settings page are explained below.

Mouse Mode Settings Page
The fields of KVM Mouse Settings page are explained below.

Relative Positioning (Linux): Relative mode sends the calculated relative mouse position displacement to the server. Relative mouse mode will not be supported in H5Viewer, as the latest Linux operating systems follow absolute mouse mode implementation.

Absolute Positioning (Windows): The absolute position of the local mouse is sent to the server.

Other Mode (SLES-11 OS Installation): To have the calculated displacement from the local mouse in the center position sent to the server.

Save: To save the changes made.

Procedure

1. Choose either of the following as your requirement:
   - Set mode to Absolute

     NOTE
     Applicable for all Windows versions, versions above RHEL6, and versions above FC14.

   - Set mode to Relative

     NOTE
     Applicable for all Linux versions, versions less than RHEL6, and versions less than FC14.

   - Set Mode to Other Mode

     NOTE
     Recommended for SLES-11 OS Installation

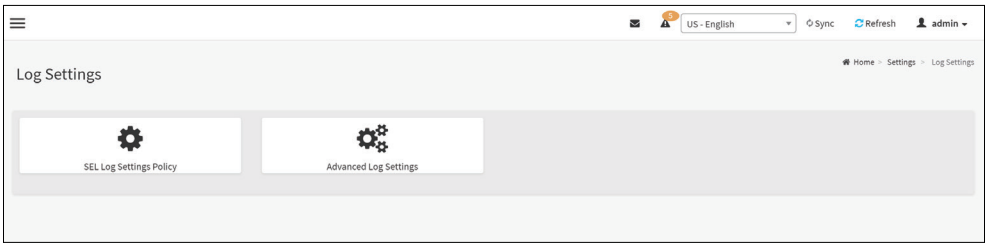
2. Click Save button to save the changes made.

NOTE
If the client and host mouse position is not in sync, then check the release note of the Host OS to verify any additional configuration to be needed in the Host.

6.5 Log Settings

System and Audit log page displays a list of system logs and audit logs occurred in this device.

To open Log Settings page, click Settings → Log Settings from the menu bar. A sample screenshot of Log Settings page is shown below.

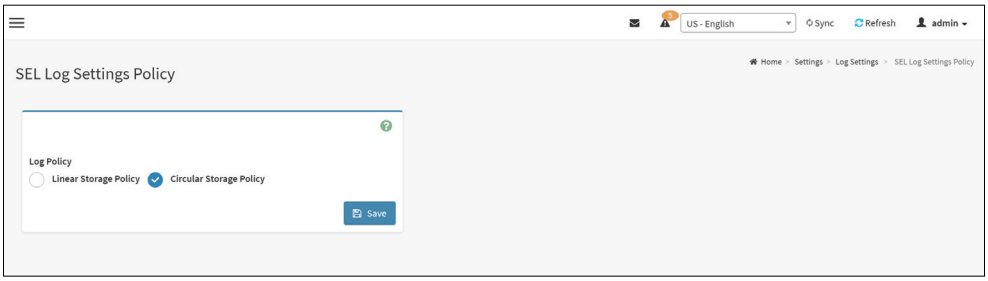


System and Audit Log Settings
The fields of Log Settings page are explained below.

- SEL Log Settings Policy
- Advanced Log Settings

6.5.1 SEL Log Setting Policy

To open Log Settings page, click Settings → Log Settings → SEL Log Settings Policy from the menu bar. A sample screenshot of Log Settings Policy page is shown below.



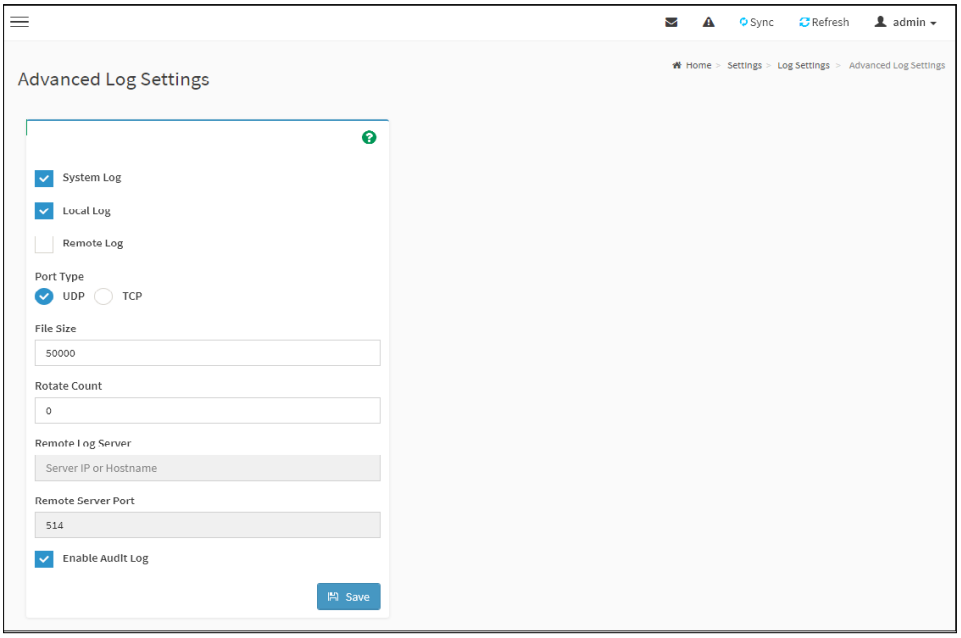
This page is used to configure the log policy for the event log. The fields are as followed.

Log Policy: This field is to enable or disable the Linear Storage Policy or Circular Storage Policy.

Save: To save the configured settings.

6.5.2 Advanced Log Settings

To open Advanced Log Settings page, click Settings → Log Settings → Advanced Log Settings from the menu bar. A sample screenshot of Advanced Log Settings Policy page is shown below.



This page is used to configure the log policy for the event log. The fields are as followed.

System Log: This field is used to enable or disable the System Log. Select System Log to view all system events. Entries can be filtered based on their classification levels. Specifies the Location for system logs, whether it should be preserved in a Local Log/ Remote Log.

Local Log: Select Local Log to save the logs locally (BMC).

Rotate Count: To back up the log information in back up files.

> **NOTE**
> Values supported are 0 and 1.

Remote Log: Select Remote Log to save the logs in a remote machine.

> **NOTE**
> - You can select either Local Log/Remote Log or both Logs as per the requirement.
> - Either one of the Log selection is mandatory.
> - Local file resides at /var/log/

Remote Log Server: This field is to specify the Remote server address to log the system events.

> **NOTE**
> Server address will support the following.
> - IPv4 address format
> - FQDN (Fully Qualified Domain Name) format
> - Maximum allowed size is 64 bytes

Port Type: Port Type is supported with the enable of Remote Log. You can select either UDP/TCP as per the requirement.

File Size: This field is to specify the size of the file in bytes if the selected log type is local.

> **NOTE**
> Size ranges from 3 to 65535. Log files are rotated when they grow bigger than size bytes mentioned, with regards for the last rotation time interval (1 minute).

Remote Server Port: This field is to specify the Remote Server port address to log the system events.

> **NOTE**
> Remote Log Server and Remote Server Port options will be available only when Remote Log is enabled.

Enable Audit Log: To enable or disable the audit log.

Save: To save the changes.

Procedure

1. In the System Log field, enable or disable the option.
2. Select the Log type: Local Log or Remote Log.
3. If Local log is selected, enter the file size in the File Size field and rotate count in the Rotate Count field.

> **NOTE**
> If Remote log is selected, the fields file size and rotate count need not be mentioned.

4. If remote log is selected, specify the Server Address of the remote server where the system events are logged.
5. In the Audit Log field, check or uncheck the Enable option as desired.
6. Click Save to save the changes.

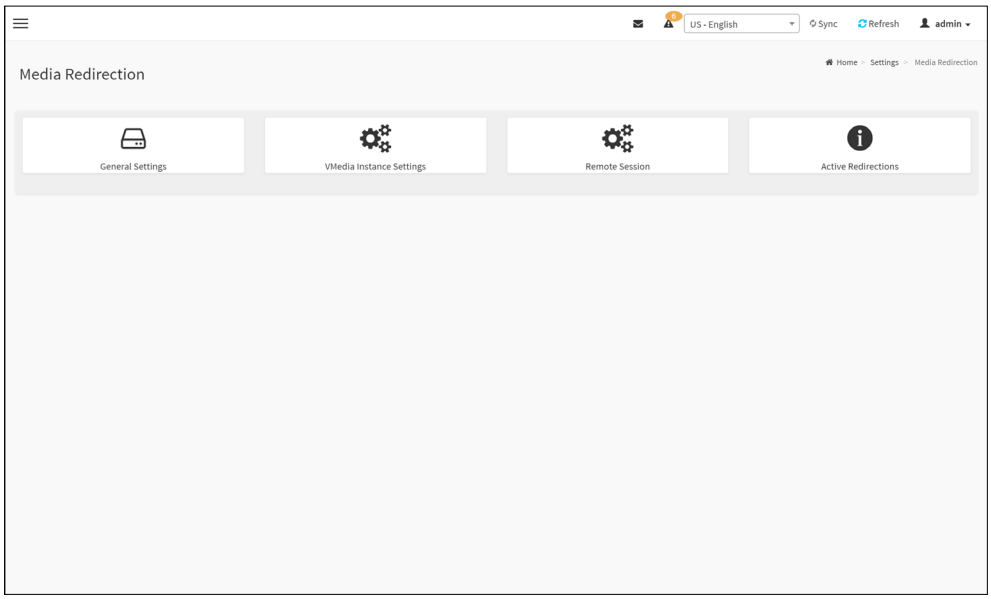
Steps to configure the remote server to enable syslogging

> **NOTE**
> This example uses FC13 as the remote machine to log syslog. On FC machine, disable the following lines for UDP in /etc/rsyslog.conf.

1. MODLOAD imudp
2. UDPSERVER 514

6.6 Media Redirection Settings

This page is used to configure the media into BMC for redirection. To open Media Redirection page, click Settings → Media Redirection Settings from the menu bar. A sample screenshot of Media Redirection page is shown below.



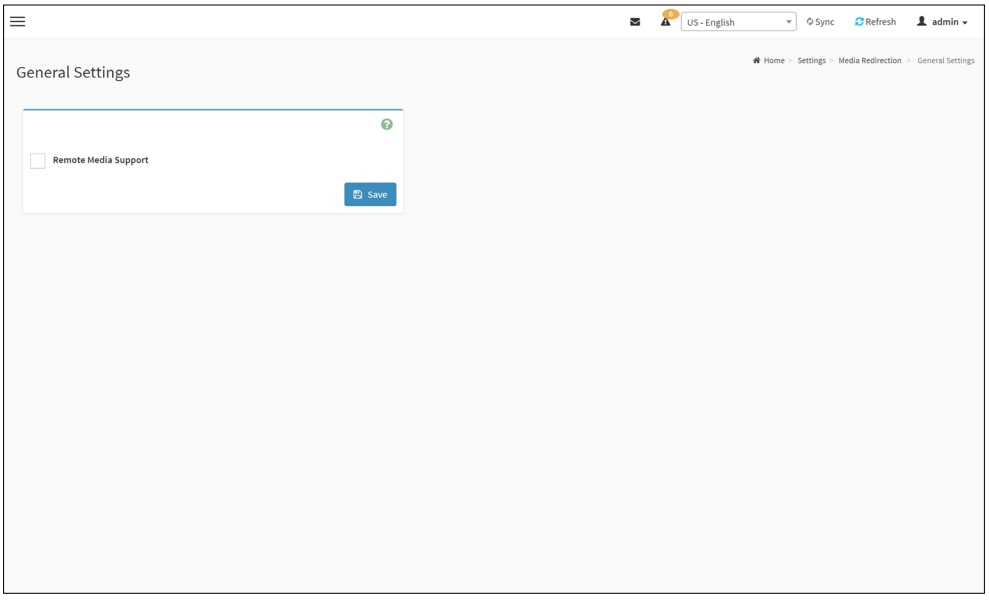
The fields of Media Redirection page are explained below.

- General Settings
- VMedia Instance Settings
- Remote Session
- Active Redirections

6.6.1 General Settings

This option is used to configure General Media Settings.

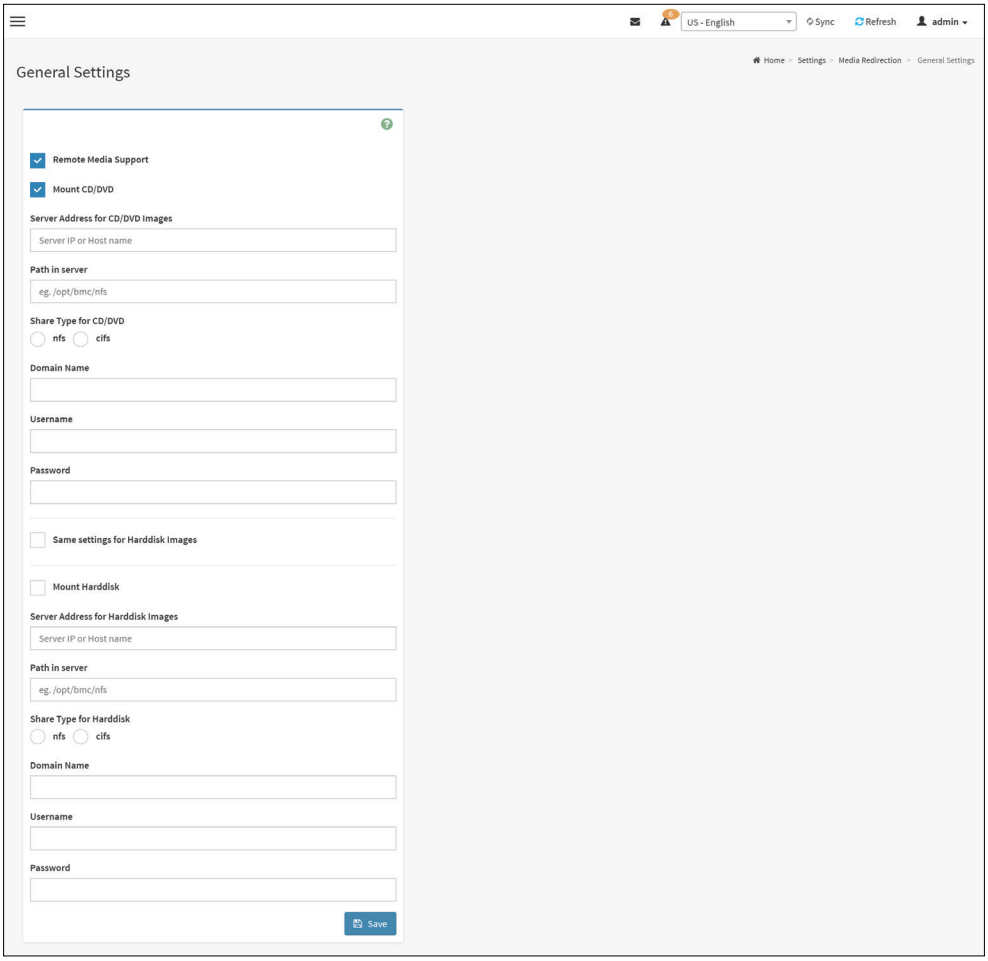
To open General Media Settings section, click Settings → Media Redirection Settings → General Settings.



Remote Media Support: To enable or disable Remote Media support, check/uncheck the Enable check box.
If it is selected, then the following Remote Media types will be displayed.

- Mount CD/DVD
- Mount Hard disk

On selecting the individual media types, its respective configurations will be displayed. You can configure different settings for different Remote Media types. A sample screenshot of General Settings page is shown below.



Same settings for Harddisk Images: Enable/Disable to select same media type data configurations for all the Remote media types.

Mount Harddisk: Enable/Disable to Mount Harddisk.

Server Address for Harddisk Images: Address of the server where the Remote media images are stored.

Path in server: Source path to the Remote media images.

> **NOTE**
> Path must be alpha-numeric and the following special characters are only allowed: '/'(backward slash), '\'(forward slash), '-'(hyphen) , '_'(underscore) , '.'(dot), ':'(colon).

Share Type for Harddisk: To Select Share Type for Harddisk either NFS or CIFS.

Domain Name, Username, and Password: If share Type is Samba(CIFS), then enter user credentials to authenticate on the server.

> **NOTE**
> If RMedia Reconnect Feature is enabled, the below Retry fields will be displayed to config¬ure the retry interval and count.

Retry Interval: Enter the retry interval to reconnect RMedia.

Retry Count: Enter the retry count to reconnect RMedia.

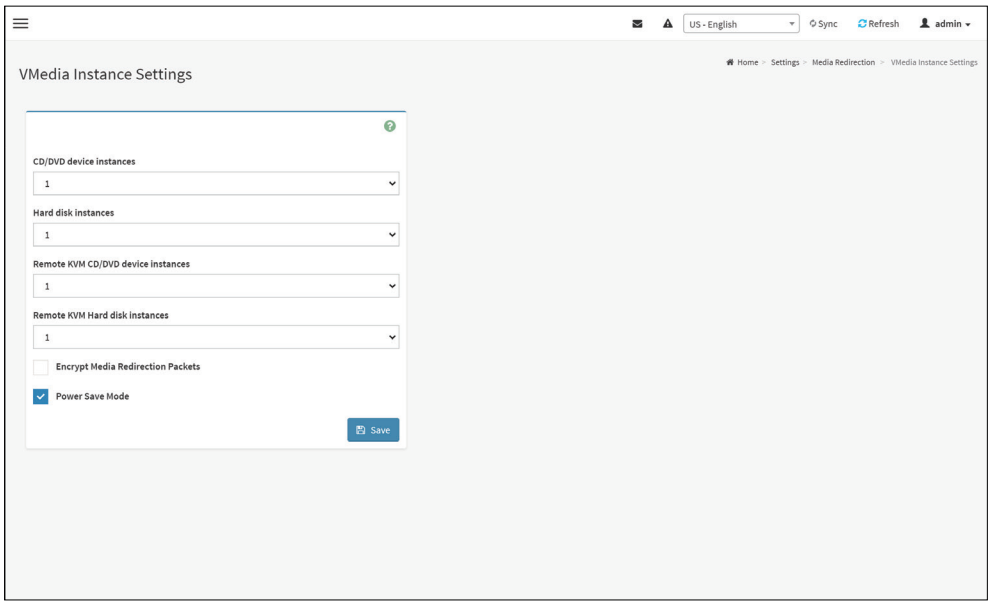
Save: To save the settings.

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

6.6.2 VMedia Instance Settings

This page is used to configure Virtual Media device settings. To open VMedia Instance Settings page, click Settings → Media Redirection Settings → VMedia Instance Settings from the menu bar.

A sample screenshot of VMedia Instance Settings page is shown below.



The following fields are displayed in this page.

CD/DVD device instances: The number of CD/DVD devices supported for Virtual Media redirection.

Harddisk instances: The number of harddisk devices supported for Virtual Media redirection.

Remote KVM Floppy devices instances: The number of floppy devices supported for KVM Virtual Media redirection.

Remote KVM CD/DVD device instances: The number of CD/DVD devices supported for Virtual Media redirection.

Remote KVM Hard disk instances: The number of Hard disk devices supported for Virtual Media redirection.

Emulate SD Media as USB disk to Host: To emulate SD Media on BMC as a USB device to Host Server.

Power Save Mode: To enable or disable the virtual USB devices visibility in the host. If this option is enabled, Virtual media devices will be connected to the Host machine only at the instance launching KVM session. If this option is disabled, Virtual media devices will remain connected to the host machine all the time irrespective of KVM session status.

Save: To save the configured settings.

> **NOTE**
> Virtual Media configuration changes will restart all the media services. So configuration changes be blocked when any active media redirection is present.

Procedure

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

> **NOTE**
> Maximum of four devices can be added in CD/DVD and Hard disk drives.

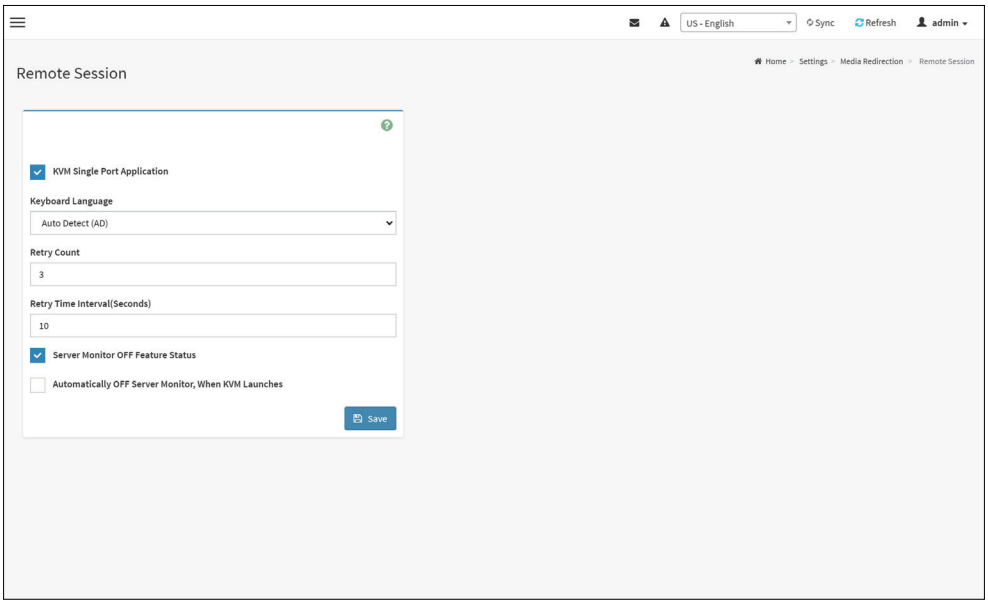
2. Select the Emulate SD Media as USB disk to Host option to enable/disable the SD card support in the host.
3. Check the Power Save Mode option to enable/disable the Virtual USB devices visibility in the host.
4. Click Save to save the changes made else click Reset to reset the previously saved values.

> **NOTE**
> If there are two device panels for each device, and when you click the Connect button, then the redirected device panel will be disabled.
>
> Unmounting device will make the driver disconnect device when using Auto Attach. Hence, when unmounting one USB key, the other USB key will be disconnected and then reconnected.

6.6.3 Remote Session

This page is used to configure virtual media configuration settings for the next redirection session. “KVM Single Port Application” is enabled by default. While disabling, “KVM Single Port Application” and “Encrypt H5Viewer KVM packets” are disabled by default.

To open Remote Session page, click Settings → Media Redirection Settings → Remote Session from the menu bar. A sample screenshot of Remote Session page is shown below.



The fields of Configure Remote Session page are explained below.

KVM Single Port Application: To Enable/Disable single port support by runtime, On changing this configuration, KVM and VMedia Sessions will be restarted. If this support is enabled, KVM session will not use its dedicated port whereas both Web and KVM sessions will be established only via Web Port. If this support is disabled, KVM and Web sessions will use their own dedicated ports respectively.

Enable KVM Encryption: To Enable/Disable Enable KVM Encryption for the next redirection session. If KVM Encryption is enabled, the KVM session will use the Secure port which has been configured in Settings → Services page.

> **NOTE**
> If “Allow Non-Secure communication for KVM/Media” in the PRJ option is enabled, then KVM/Media can use non-secure communication. i.e. The KVM or Media Encryption will be able to disable.

If KVM Encryption is disabled, the KVM session will use the Non-Secure port which has been configured in Settings → Services page

> **NOTE**
> This option is disabled if Single Port is enabled.

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 reconnect attempts. The KVM client will wait for a time interval equal to this value, after making a reconnect 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: To enable/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: To enable/disable Automatically OFF Server Monitor, When KVM Launches.

Save: To save the current changes.

> **NOTE**
> It will automatically close the existing remote redirection either KVM or Virtual media sessions on Single Port enable/Disable or KVM Encryption Enable/ Disable.

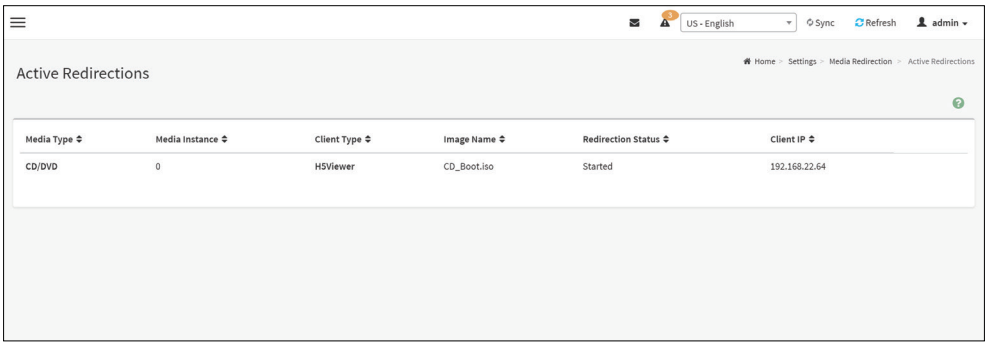
Procedure

1. Check or uncheck the KVM Single Port Application option to enable Single Port Application support in BMC.
2. Check or uncheck Enable KVM Encryption option to enable/disable KVM Encryption for the next redirection session.
3. Choose the Keyboard Language from the list of keyboard supported languages.
4. Enter a value in the Retry Count field to set the number of attempts for retrying the redirection session.
5. Enter a value in the Retry Time Interval(Seconds) field to give time interval for each attempts.
6. Check the Server Monitor OFF Feature Status check box to enable Local Monitor ON/ OFF command during runtime.
7. Check the Automatically OFF Server Monitor, When KVM Launches check box to automatically Lock the local monitor during H5Viewer launch.
8. Click Save to save the current changes.

6.6.4 Active Redirections

This page is used to display the active redirected media, which are redirected via JViewer/VMAPP/H5Viewer/LMedia/RMedia/VMCLI. Information like Media type, Media Instance, Client Type, Image Name, Redirection status, Client IP will be displayed.

To open Active Redirections page, click Settings → Media Redirection Settings → Active Redirections from the menu bar. A sample screenshot of Active Redirections page is shown below.



The following fields are displayed in this page.

Media Type: The type Media devices (CD/DVD) supported for Active Redirections.

Media instances: The number of Media devices supported for Active Redirections.

Client Type: The type Media devices (CD/DVD) supported for Active Redirections.

Image Name: The name of Media devices supported image for Active Redirections.

Redirection Status: The status Media for Active Redirections.

Client IP: The IP of the connected Media devices (CD/DVD) supported for Active Redirections.

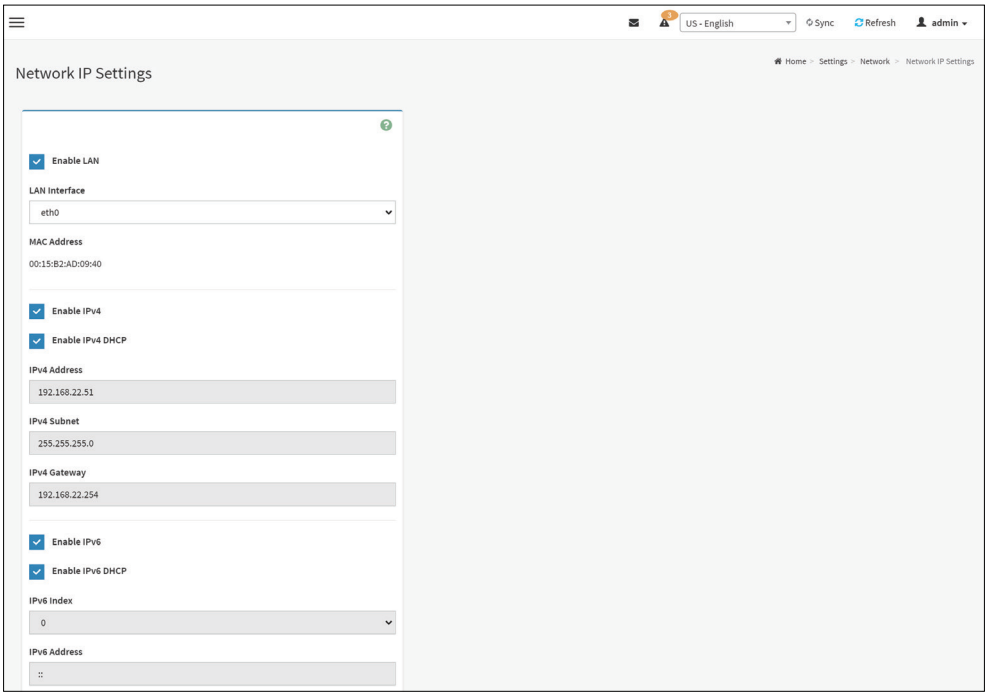
> **NOTE**
> Local/Remote Media connection will use loopback socket for communication. So '~' symbol will be displayed for loopback ip(127.0.0.1 (or) ::1) in media session information page.

6.7 Network Settings

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

6.7.1 Network IP Settings

To open Network Settings page, click Settings → Network Settings → Network IP Settings from the menu bar. A sample screenshot of Network IP Settings page is shown below.



The fields of Network IP Settings page are explained below.

Enable LAN: To enable or disable the LAN Settings.

LAN Interface: Lists the LAN interfaces.

MAC Address: This field displays the MAC Address of the device. This is a read only field.

Enable IPv 4: This option is to enable/disable the IPv4 settings in the device.

Enable IPv4 DHCP: This option is to enable IPv4 DHCP support for the selected interface.

IPv4 Address, IPv4 Subnet Mask , and IPv4 Default Gateway: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device.

> **NOTE**
> - IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
> - Each Number ranges from 0 to 255.
> - First Number must not be 0.

Enable IPv6: To Enable/Disable the IPv6 configuration settings.

Enable IPv6 DHCP: To Enable/Disable the IPv6 settings in the device. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).

IPv6 Index: To specify a static IPv6 Index to be configured to the device. Eg: 0

IPv6 Address: To specify a static IPv6 address to be configured to the device. Eg: 2004::2010

Subnet Prefix length: To specify the subnet prefix length for the IPv6 settings.

> **NOTE**
> Value ranges from 0 to 128.

IPv6 Gateway: Specify v6 default gateway for the IPv6 settings.

> **NOTE**
> If core feature IPV6_COMPLIANCE and SUPPORT_IPMIIPV6_LAN_PARAM_ONLY are enabled, the IPv6 default Gateway field will not be displayed.

Enable VLAN: To enable/disable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.

> **NOTE**
> Value ranges from 2 to 4094.

VLAN Priority: The priority for VLAN configuration.

> **NOTE**
> - Value ranges from 0 to 7.
> - 7 is the highest priority for VLAN.

Save: To save the entries.

Procedure

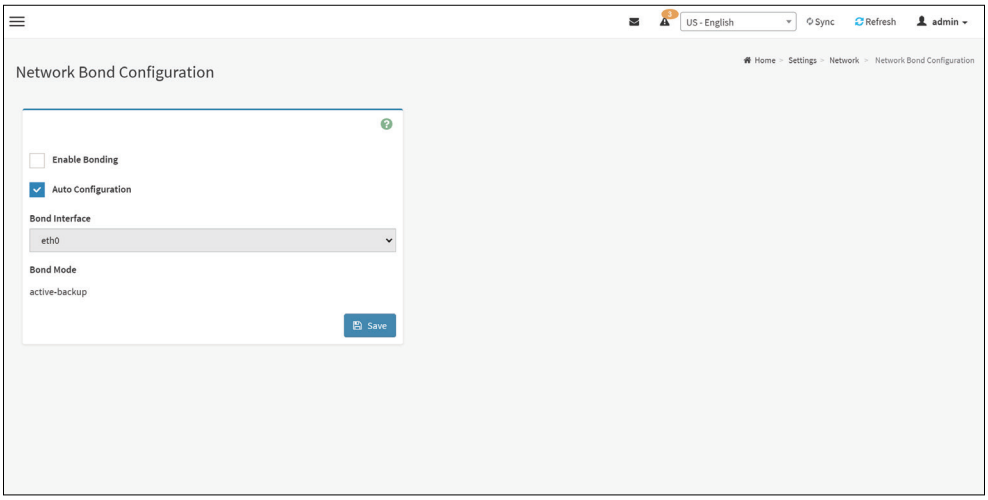
1. Check Enable LAN to enable LAN support for the selected interface..
2. Select the LAN Interface to be configured.
3. Check Enable IPv4 to enable IPv4 support for the selected interface.
4. Check Enable IPv4 DHCP to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, enter the IPv4 Address , IPv4 Subnet Mask and IPv4 Default Gateway in the respective fields.
6. In IPv6 Configuration, if you wish to enable the IPv6 settings, check Enable IPv6.
7. If the IPv6 setting is enabled, enable or disable the option Enable IPv6 DHCP.
8. If the field is disabled, enter the IPv6 Address, Subnet Prefix length and IPv6 Index in the given field.
9. In VLAN Configuration, if you wish to enable the VLAN settings, check Enable LAN.
10. Enter the VLAN ID in the specified field.
11. Enter the VLAN Priority in the specified field.
12. Click Save to save the entries.

6.7.2 Network Bond Configuration

This page is used to configure the network bonding configuration for the network interfaces.

> **NOTE**
> Minimum of two network interfaces required to enable Network bonding for the device.

To open Network Settings page, click Settings → Network Settings → Network Bond from the menu bar. A sample screenshot of Network Bonding page is shown below.



The fields of Network Bond Configuration page are explained below.

Enable Bonding: To enable or disable network bonding for network interfaces.

Auto Configuration: To configure the interfaces in service configuration automatically.

> **NOTE**
> If Auto configuration is disabled, then interfaces in services can be configured via IPMI command.

If Auto configuration is enabled, then all the services will be restarted automatically.

Bond Mode: This field displays the Network bonding mode.

> **NOTE**
> This field cannot be configured.

Save: To save the current changes.

Procedure:

> **NOTE**
> The Eable Bonding option is enabled. You can disable the option if needed.

1. Select the Bond Interface from the drop-down list.

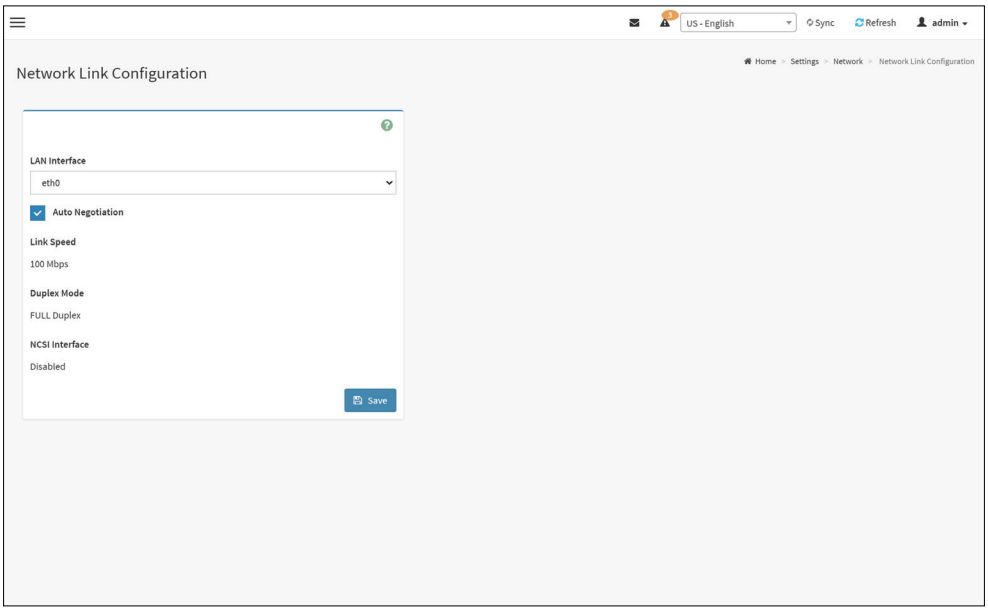
> **NOTE**
> The Bond Interface can be selected only if the Enable Bonding option is enabled.

2. Check the Auto Configuration option to enable the auto configuration.
3. Click Save to save the configuration.

6.7.3 Network Link

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

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



The fields of Network Link Configuration page are explained below.

LAN Interface: Select the required network interface from the list to which the Link speed and duplex mode 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.

Link Speed: Link speed will list all the supported capabilities of the network interface. It can be 10/100/1000 Mbps.

> **NOTE**
> Link speed of 1000 Mbps is not applicable, when Auto Negotiation is OFF.

Duplex Mode: Duplex Mode could be either Half Duplex or Full Duplex.

Save: To save the settings.

Procedure:

1. Select the LAN Interface from the drop down list.
2. Select either Enable or Disable for Auto Negotiation.

> **NOTE**
> The Link Speed and Duplex Mode will be active only when Auto Negotiation is OFF.

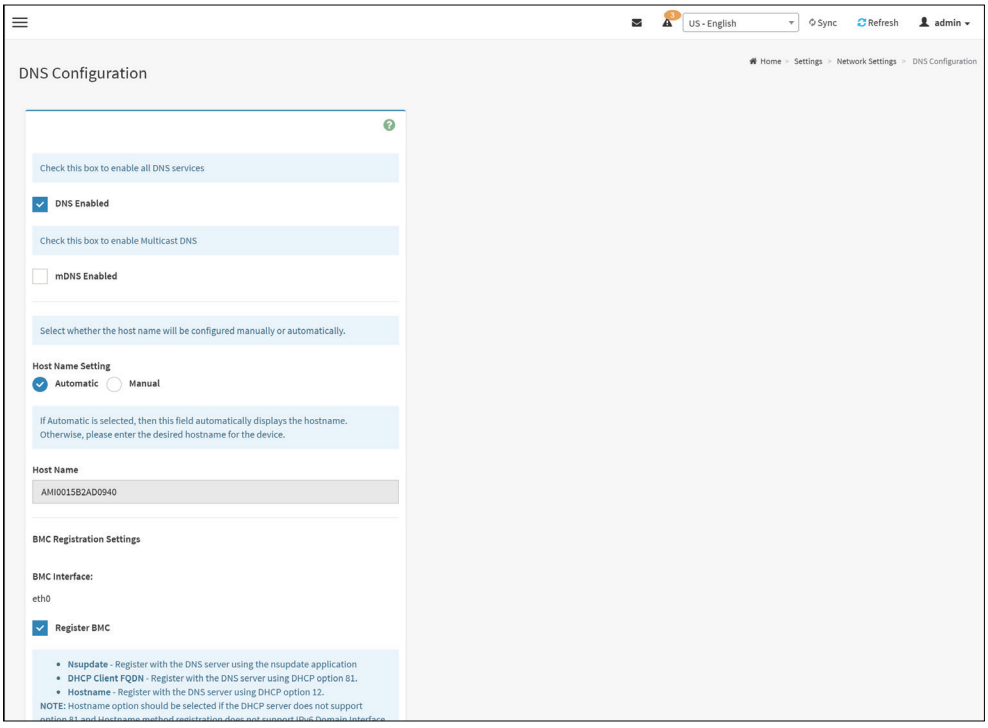
3. Select the Link Speed from the drop-down list.
4. Select the Duplex Mode either Full duplex or Half duplex.
5. Click Save to save the configuration.

6.7.4 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 Server settings page is used to manage the DNS settings of a device.

To open DNS Server Settings page, click Settings → Network Settings → DNS Configuration from the menu bar. A sample screenshot of DNS Configuration page is shown below.



The fields of DNS Configuration page are explained below.

Domain Name Service Configuration

DNS Enabled: To enable/disable all the DNS Service Configurations. mDNS Enable: To enable/disable the mDNS Support Configurations.

Host Name Settings: Choose either Automatic or Manual settings.

Host Name: It displays host name of the device. If the Host setting is chosen as Manual, then specify the host name of the device.

> **NOTE**
> - Value ranges from 1 to 64 alpha-numeric characters.
> - Special characters '-'(hyphen) and '_'(underscore) are allowed.
> - It must not start or end with a '-'(hyphen). IE browsers won't work correctly if any part of the host name contain underscore (_) character.

BMC Registration Settings

BMC Interface: Options to register the BMC are through an Interface.

Register BMC: To register BMC through registration method.

Registration Method
Options to register the BMC are through NS Update or DHCP Client FQDN or Hostname.

TSIG Authentication Enabled:
Both: Check this option to modify TSIG authentication for both interfaces.
Eth 0&1:

- **TSIG Authentication Enabled**: Check this box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.
- **Current TSIG Private File**: The information of Current TSIG private file along with its uploaded date/time will be displayed (readonly).
- **New TSIG Private File**: Browse and navigate to the TSIG private file.

> **NOTE**
> TSIG file should be of private type.

Domain Setting: Select whether the domain interface will be configured manually or automatically.

- **Automatic** - If you Select Automatic, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
- **Manual** - If the Domain setting is chosen as Manual, then 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 Name Server Setting

Automatic - If you select Automatic “DNS Interface” option should be explained.

Manual - Specify the DNS (Domain Name System) server address to be configured for the BMC.

IP Priority:

- If IP Priority is IPv4, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server.
- If IP Priority is IPv6, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.

> **NOTE**
> This is not applicable for Manual configuration.

DNS Server 1, 2 & 3
To specify the DNS (Domain Name System) server address to be configured for the BMC.

> **NOTE**
> - IPv4 Addresses should be given in dotted decimal representation.
> - IPv6 Addresses are supported and must be global unicast addresses..

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

Save: To save the entered changes.

Procedure:

1. In Domain Name Service Configuration, Enable DNS Service.
   - Check the option DNS Enabled to enable all the DNS Service Configurations.
2. Choose the Host Name Setting either Automatic or Manual.

> **NOTE**
> If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.

3. Enter the Host Name in the given field if you have chosen Manual Configuration.
4. Under Register BMC, choose the BMC’s network port to register with DNS settings.
   - Check Register BMC option to register with DNS settings.
   - **Nsupdate** - Choose Nsupdate option to register with DNS server using nsupdate application.
   - **DHCP Client FQDN** - Choose DHCP Client FQDN option to register with DNS Server using DHCP option 81.
   - **Hostname** - Choose Hostname option to register with DNS server using DHCP option.

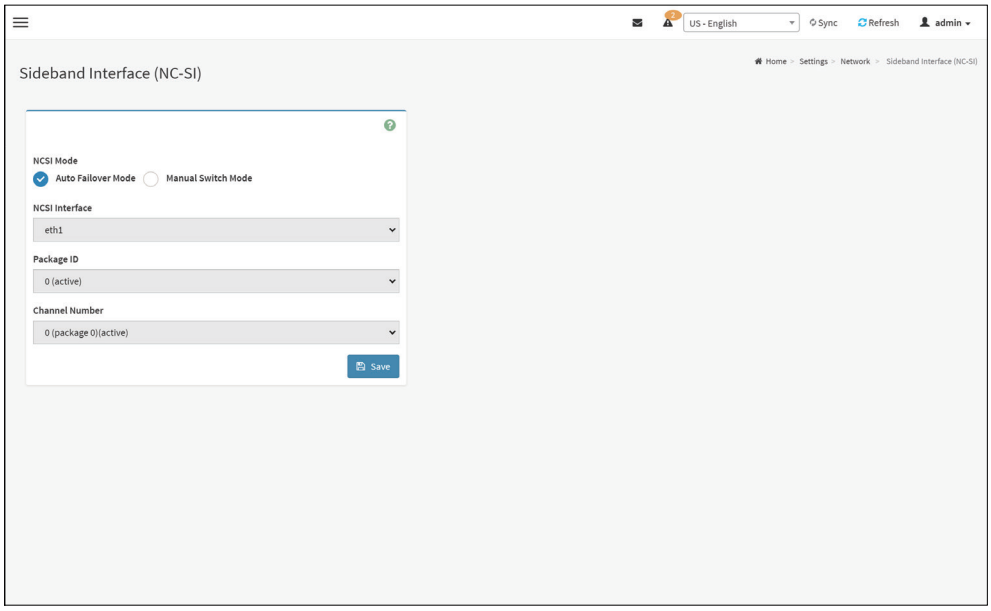
> **NOTE**
> Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.

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

6.7.5 NC-SI Configuration

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

To open NCSI page, click Settings → Network Settings → NC-SI Configuration from the menu bar. A sample screenshot of NCSI page is shown below.



The following fields are displayed in this page.

NCSI Mode: To Select the NCSI Mode either Auto Failover Mode or Manual Switch mode.

NCSI Interface: It lists the interface name in list box.

Channel Number: Lists the channel number of the selected interface.

Package ID: Lists the package id of the selected interface.

Save: To save the current changes.

Procedure

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

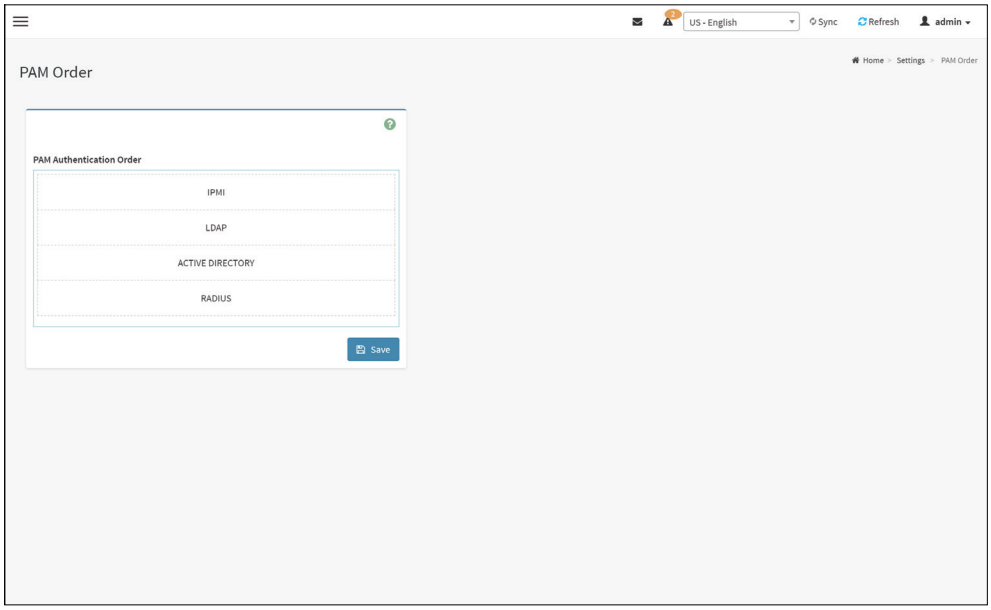
> **NOTE**
> - If you select Auto Failover Mode, the NCSI Interface will be configured automatically.
> - If you select Manual Switch Mode only you are allowed to configure NCSI Interface, Channel number and Package ID.

2. Choose the particular NCSI Interface to which you need to configure NCSI settings.
3. Choose the Channel Number to be configured for the selected Interface name.
4. Choose the Package ID to be configured for the selected Interface name.
5. Click Save to save the current changes.

6.8 PAM Order Settings

This page is used to configure the PAM ordering for user authentication in to the BMC.

To open PAM Ordering page, click Settings → PAM Order Settings from the menu bar. A sample screenshot of PAM Order page is shown below.



PAM Module: It shows the list of available PAM modules supported in BMC.

> **NOTE**
> If AD contains secret username & password as empty, Authentication fails will be always treated as Invalid Password error. For Invalid Password error PAM will not try other Authentication Methods. So it is recommended to keep AD in the last location in PAM order.

Procedure

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

> **NOTE**
> Whenever the configuration is modified, the web server will be restarted automatically. Logged-in session will be logged out.

6.9 Platform Event Filter

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.

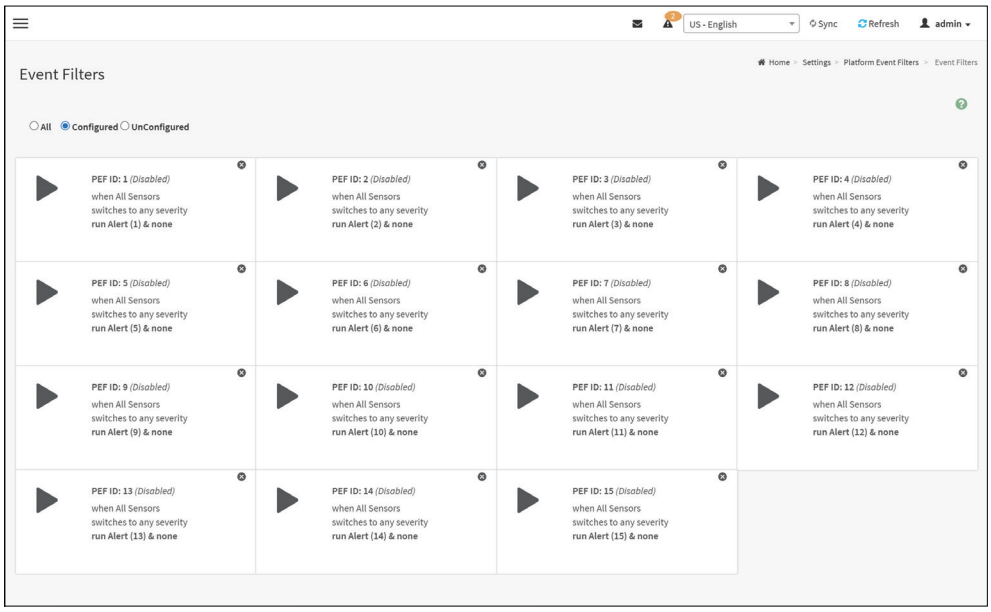
The PEF Management is used to configure the following

- Event Filters
- Alert Policies
- LAN Destinations

To open PEF Management Settings page, click Settings → Platform Event Filter the menu bar. Each tab is explained below.

6.9.1 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, fan failure events, etc. Remaining entries can be made available for 'OEM' or System Management Software configured events. Note that individual entries can be tagged as being reserved for system use - so this ratio of preconfigured entries to run-time configurable entries can be reallocated if necessary.

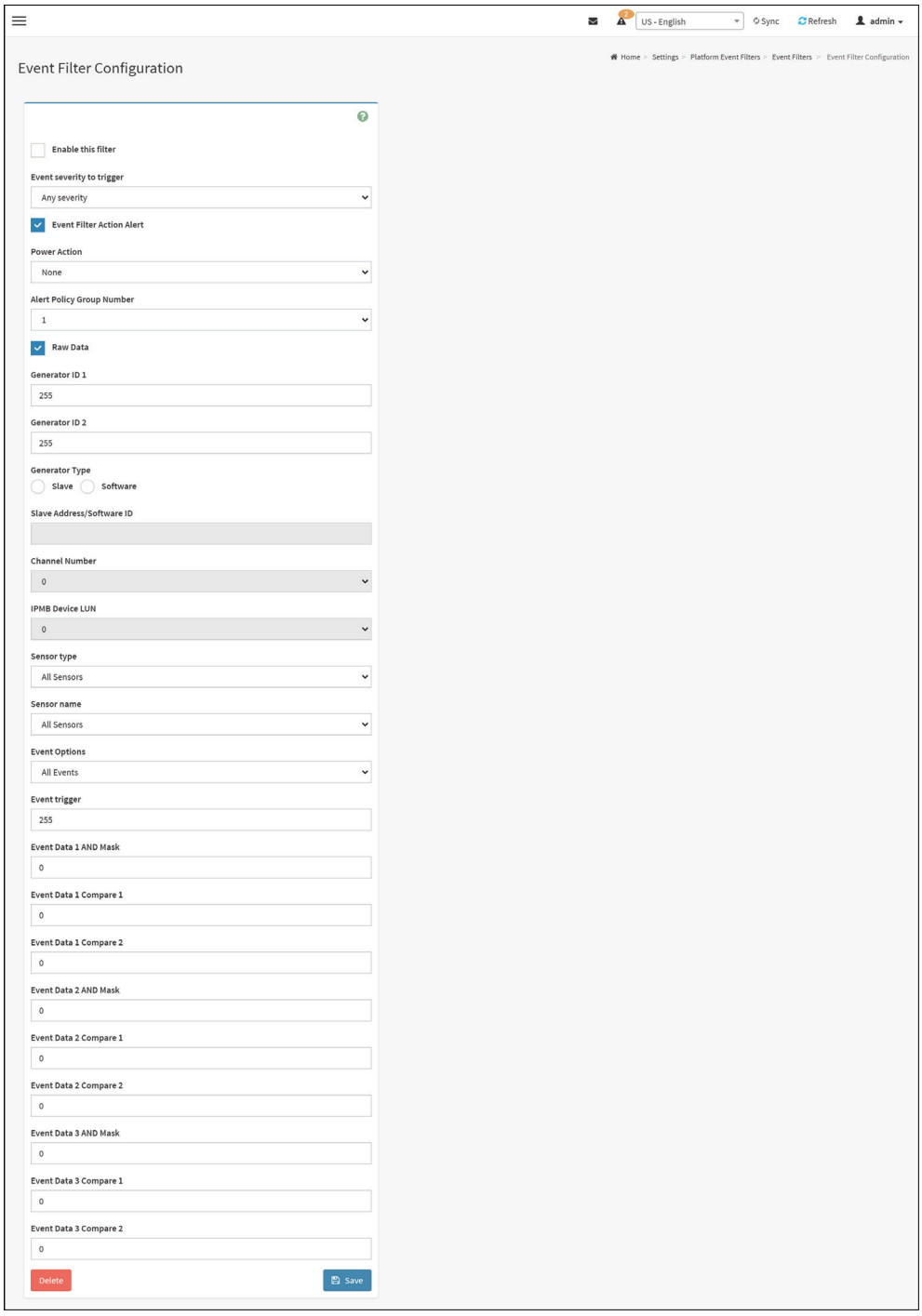


Platform Event Filters

The fields of Platform Event Filters Tab are explained below. This page contains Pre-configured 40 Events with PEF IDs. Click Delete icon (x) on the top right corner to directly delete an item from the list.

Procedure:

1. Click the Event Filters section to configure the event filters in the available slots.
2. To Add an Event Filter entry, select a free section to open the Event Filter entry page.
   A sample screenshot of Event Filter Configuration page is shown below.



Event Filter Configuration

In the Event Filter Configuration section,

- In Enable this filter, check this option to enable the PEF settings.
- In Event Security to trigger, select any one of the Event security from the list.
- **Event Filter Action Alert**: It is checked by default. This action enables PEF Alert action (readonly).
- Select any one of the Power Action either Power down, Power reset or Power cycle from the drop down list.
- Choose any one of the configured Alert Policy Group Number from the drop down list.

> **NOTE**
> Alert Policy has to be configured - under Settings → PEF → Alert Policy.

- Check Raw Data option to fill the Generator ID with raw data.
- Generator ID 1 field is used to give raw generator ID1 data value.
- Generator ID 2 field is used to give raw generator ID2 data value.

> **NOTE**
> In RAW data field, specify hexadecimal value prefix with '0x'.

- In the Event Generator section, choose the event generator as Slave Address - if event was generated from IPMB. Otherwise as System Software ID - if event was generated from system software.
- In the Slave Address/Software ID field, specify corresponding I2C Slave Address or System Software ID.
- Choose the particular Channel Number that event message was received over. Or choose '0' if the event message was received via the system interface, primary IPMB, or internally generated by the BMC.
- Choose the corresponding IPMB Device LUN if event generated by IPMB.
- Select the Sensor Type of sensor that will trigger the event filter action.
- In the Sensor Name field, choose the particular sensor from the sensor list.
- Choose Event Option to be either All Events or Sensor Specific Events.
- Event Trigger field is used to give Event/Reading type value.

> **NOTE**
> Value ranges from 1 to 255.

- Event Data 1 AND Mask field is used to indicate wildcarded or compared bits.

> **NOTE**
> Value ranges from 0 to 255.

- Event Data 1 Compare 1 & Event Data 1 Compare 2 fields are used to indicate whether each bit position's comparison is an exact comparison or not.

> **NOTE**
> Value ranges from 0 to 255.

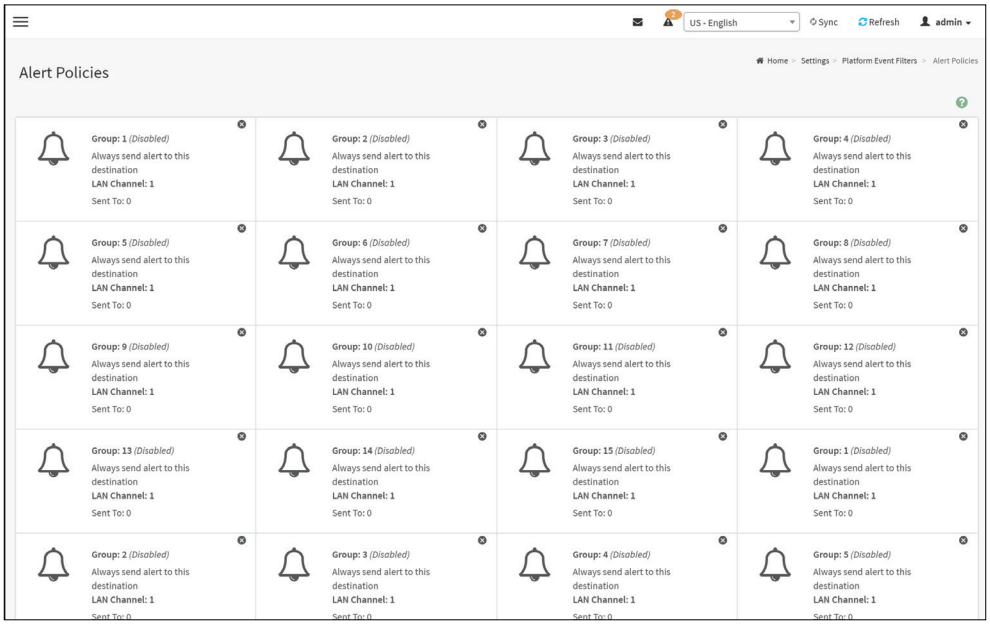
- Event Data 2 AND Mask field is similar to Event Data 1 AND Mask.

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

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

6.9.2 Alert Policies

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



The fields of Platform Event Filter – Alert Policies section are explained below.

Policy Group Number: Displays the Policy number of the configuration.

Enable this alert: To enable or disable the policy settings.

Policy Action: To choose any one of the Policy set values (0-5) 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: To choose a particular channel from the available channel list.

Destination Selector: To choose a particular destination from the configured destination list.

> **NOTE**
> LAN Destination has to be configured under Settings → Platform Event Filters → LAN Destinations.

Event Specific Alert String: To specify an event-specific Alert String.

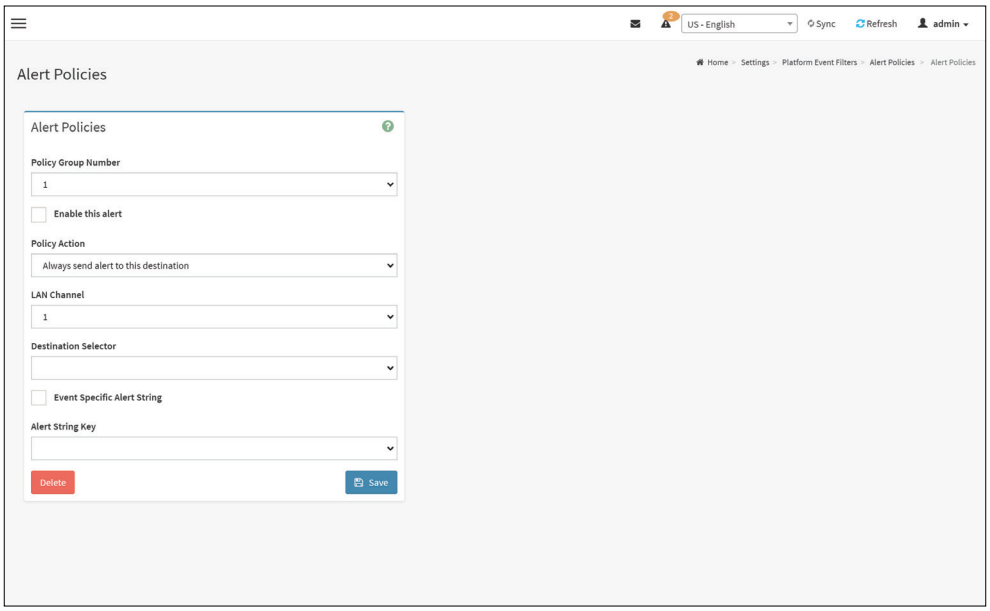
Alert String Key: To specify which string is to be sent for this Alert Policy entry.

Save: To save the Alert Policies entries.

Delete: To delete the selected configured Alert Policy.

Procedure:

1. In the Alert Policies Section, select the slot for which you have to configure the Alert policy. That is, In the Alert Policies page, if you have chosen Alert Policy Group Number as 4, you have to configure the 4th slot (the slot with Policy Number 4) in the Alert Policy Tab.
2. Select the slot and click on the empty slot to open the Alert Policies page as shown in the screenshot below.



3. Select Policy Group Number from the drop-down list.
4. Check Enable this alert to enable the policy settings.
5. Choose any of the Policy Action from the list.
6. Choose particular LAN Channel from the available channel list.

7. In the Destination Selector, choose particular destination from the configured destination list.

> **NOTE**
> LAN Destination has to be configured under Settings → Platform Event Filters → LAN Destinations. That is if you select the number 4 for destination selector in Alert Policy Entry page, then you have to configure the 4th slot (LAN Destination Number 4) in the LAN Destinations tab.

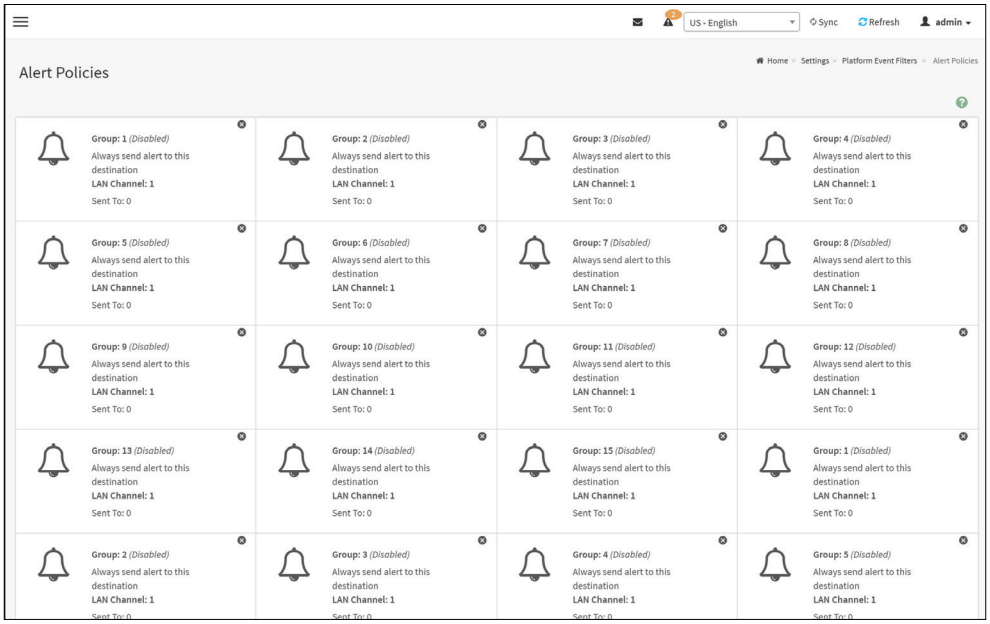
8. Enable Event Specific Alert String, if the Alert policy entry is Event Specific.
9. In the Alert String Key field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

> **NOTE**
> Using Web UI, Alert strings cannot be configured but option for Event Specific alert strings can be enabled/disabled. There is an option to select only the alert string keys, but alert strings has to be configured using IPMI Command (Set PEF Config Parameter “Alert String”). # and ; symbols are not supported for PEF Alert string.

10. Click Save to save the new alert policy and return to Alert Policy list.
11. Click Delete to delete a configuration.

6.9.3 LAN Destinations

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



The fields of Platform Event Filters – LAN Destinations are explained below.

Select any empty slot to configure LAN Destinations.

Select the LAN Channel: To select the LAN Channel number.

LAN Channel: Displays LAN Channel Number for the selected slot (read-only).

LAN Destination: Displays ID for setting Destination Selector of Alert Policy (readonly). alerts, the four fields - SNMP Destination Address, BMC User Name, Email subject and Email message needs to be filled. The SMTP server information also has to be added - under Settings → SMTP Settings. For SNMP Trap, only the SNMP Destination Address has to be filled.

SNMP Destination Address: If Destination type is SNMP Trap, then enter the IP address of the system that will receive the alert. Destination address will support the following:

- IPv4 address format.
- IPv6 address format.

BMC User Name: If Destination type is Email Alert, then choose the user to whom the email alert has to be sent. Email address for the user has to be configured under Settings → Users Management.

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

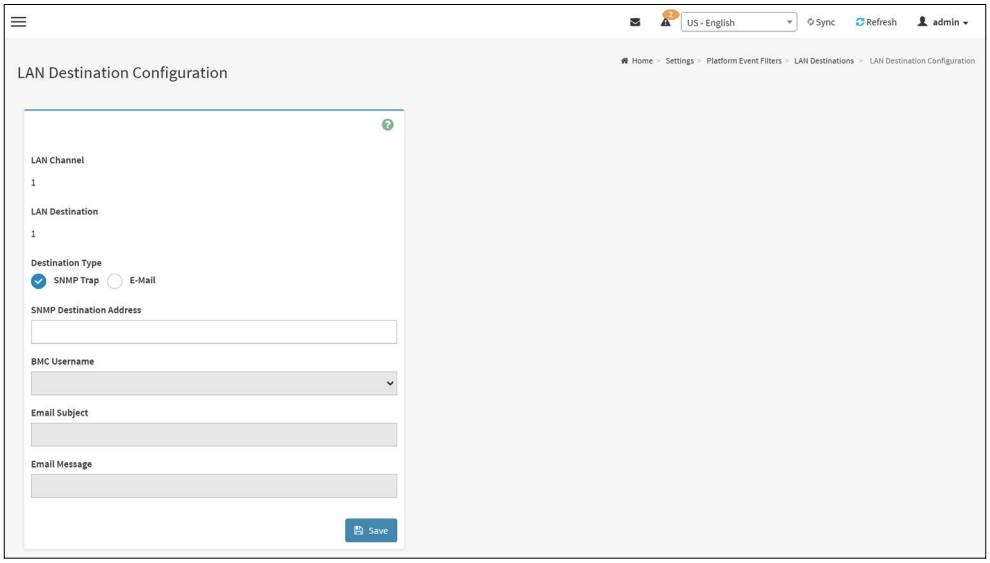
> **NOTE**
> User should be configured under Settings → Users Management

Save: To add a new entry to the device. Alternatively, double click on a free slot.

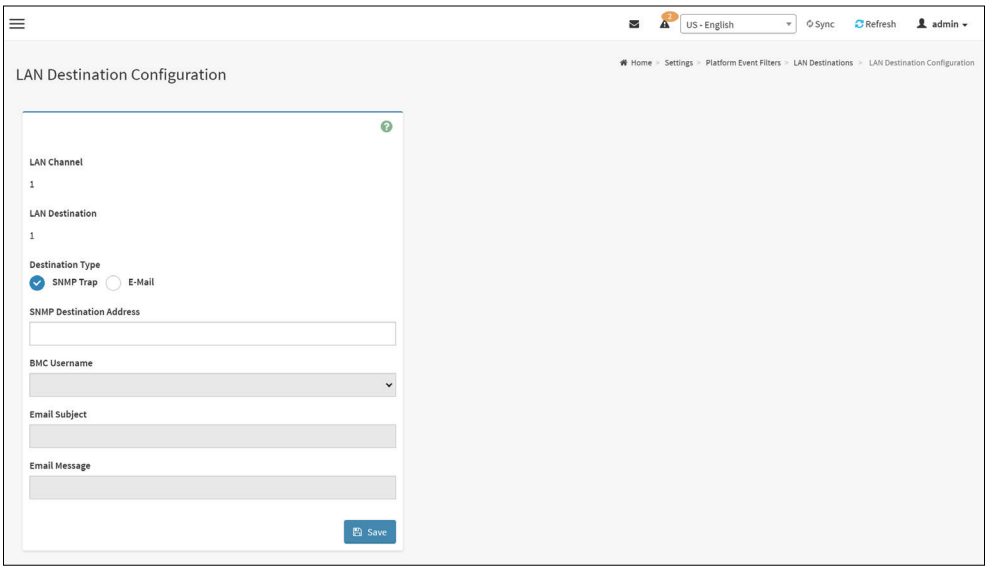
Delete: To delete the selected configured LAN Destination.

Procedure:

1. In the LAN Destinations section, choose the number of slots to be configured. This should be the same number of slot that you have selected in the Alert Policies - Destination Selector field. That is if you have chosen the Destination Selector as 4 in the Alert Policies page of Alert Policies tab, then you have to configure the 4th slot of LAN Destination page.



2. Select the slot and click on the empty slot. This opens the LAN Destination entry.



3. In the LAN Channel Number field, the LAN Channel Number for the selected slot is displayed and this is a read only field.
4. In the LAN Destination field, the destination for the newly configured entry is displayed and this is a read only field.
5. In the Destination Type field, select the one of the types.
6. In the SNMP Destination Address field, enter the destination address.

> **NOTE**
> If Destination type is E-mail Alert, then give the e-mail address that will receive the e-mail.

7. If the destination type is Email alert, select the BMC User Name from the list of users.

> **NOTE**
> E-mail address should be configured under Settings → User Management.

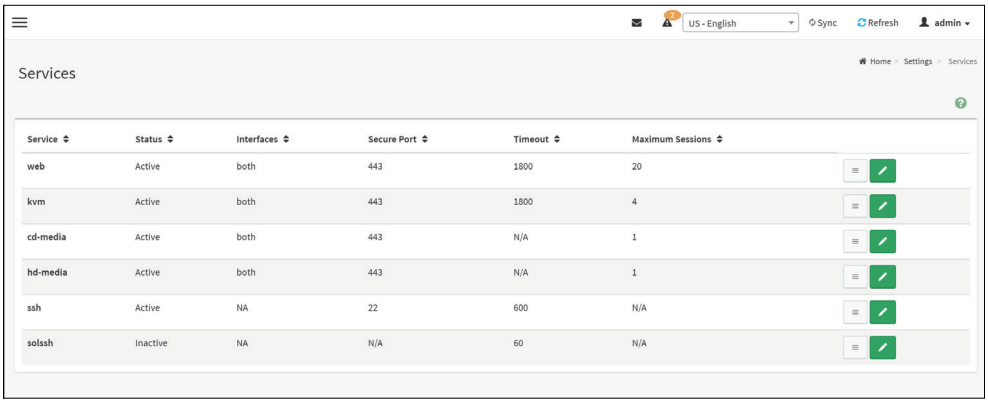
8. In the Email Subject field, enter the subject.
9. In the Email Message field, enter the message.
10. Click Save to save the new LAN destination and return to LAN destination list.
11. Click Delete to delete a configuration.
12. Click Send Test Alert to send sample alert to configured destination.

> **NOTE**
> Test alert can sent only with enabled SMTP configuration. SMTP support can be enabled under Settings → SMTP Settings.

6.10 Service

This page displays the basic information about services running in the BMC. Only Administrator can modify the service.

To open Services page, click Settings → Services from the menu bar. A sample screenshot of Services page is shown below.



The fields of Services page are explained below.

Services: Displays service name of the selected slot (read-only).

Status: Displays the current status of the service, either active or inactive state.

Interfaces: It shows the interface in which service is running.

Nonsecure Port: This port is used to configure non secure port number for the service.

- Web default port is 80
- KVM default port is 7578
- CD Media default port is 5120
- HD Media default port is 5123
- Telnet default port is 23
- SOLSSH default port is 52123

> **NOTE**
> SSH service will not support Non-secure port. If Single port feature is enabled, KVM, CD Media and HD Media ports cannot be edited. Port value ranges from 1 to 65535. “ALLOW_NON_SECURE_COMMUNICATION” feature (if applicable) and port 80 will be disabled by default due to the security reasons. Hence, use _https://<ip address> (port 443) instead of _http://<ip address> (port80).

Secure Port: Used to configure secure port number for the service.

- Web default port is 443
- KVM default port is 7582
- CD Media default port is 5124
- HD Media default port is 5127
- SSH default port is 22

> **NOTE**
> Telnet service and SOLSSH will not support secure port. If single port feature is enabled, KVM, CD Media, FD Media and HD Media ports cannot be edited.Port value ranges from 1 to 65535.

Port listening status on various feature settings:

	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 (EO)	7578 (LP) 7582 (EO)	7578 (EO)	7578 (LP) 7582 (EO)
Cdserver	5120 (LP)	5120 (EO)	5120 (EO)	5120 (LP) 5124 (EO)	5120 (LP) 5124 (EO)
Hdserver	5123 (LP)	5123 (EO)	5123 (EO)	5123 (LP) 5127 (EO)	5123 (LP) 5127 (EO)

NOTE
LP – Loopback, EO – Exposed Outside.
The adviser will always be listening to loopback as well as kvm configured interface 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 interface as mentioned in the above table. So that the lmedia/rmedia and H5Viewer/JViewer client can connect to the media servers.

Timeout: Displays the session timeout value of the service. For web, SSH and telnet service, user can configure the session timeout value.

NOTE
- Web timeout value ranges from 300 to 1800 seconds.
- KVM timeout value ranges from 300 to 1800 seconds.
- SSH and Telnet timeout value ranges from 60 to 1800 seconds.
- SSH and Telnet timeout value ranges from 60 to 1800 seconds.
- SSH and telnet service will be using the same timeout value. If you configure SSH timeout value, it will be applied to telnet service also and vice versa.
- If KVM is launched then the web session timeout will not take effect.

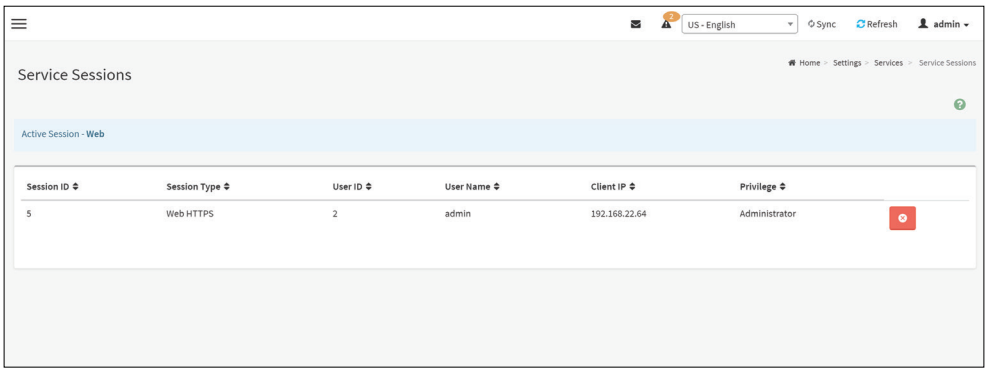
Maximum Sessions: Displays the maximum number of allowed sessions for the service.

Active Sessions: To view the current active sessions for the service.

To view the Active Sessions:

Procedure:

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



3. Session Type: Displays the type of the active sessions.
4. User: Displays the name of the user.
5. Client IP: Displays the IP addresses that are already configured for the active sessions.
6. Privilege: Displays the access privilege of the user.
7. Select a slot and click Terminate icon ( ) to terminate the particular session of the service.

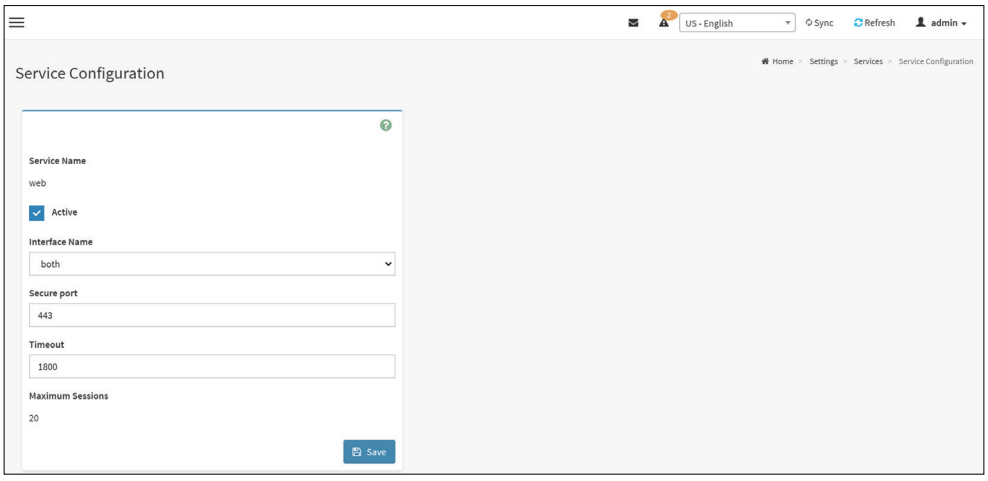
To modify the existing services:

Procedure

1. Select a slot and click Edit icon ( ) to modify the configuration of the service.

> **NOTE**
> Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the Service Configuration screen as shown in the screenshot below.



3. Service Name is a read only field.
4. Activate the Current State by enabling the Active check box.

> **NOTE**
> Interfaces, Nonsecure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

5. Choose any one of the available interfaces from the Interface Name drop-down list.
6. Enter the Nonsecure port number in the Non-secure Port field.
7. Enter the Secure Port Number in the Secure Port field.
8. Enter the timeout value in the Timeout field.

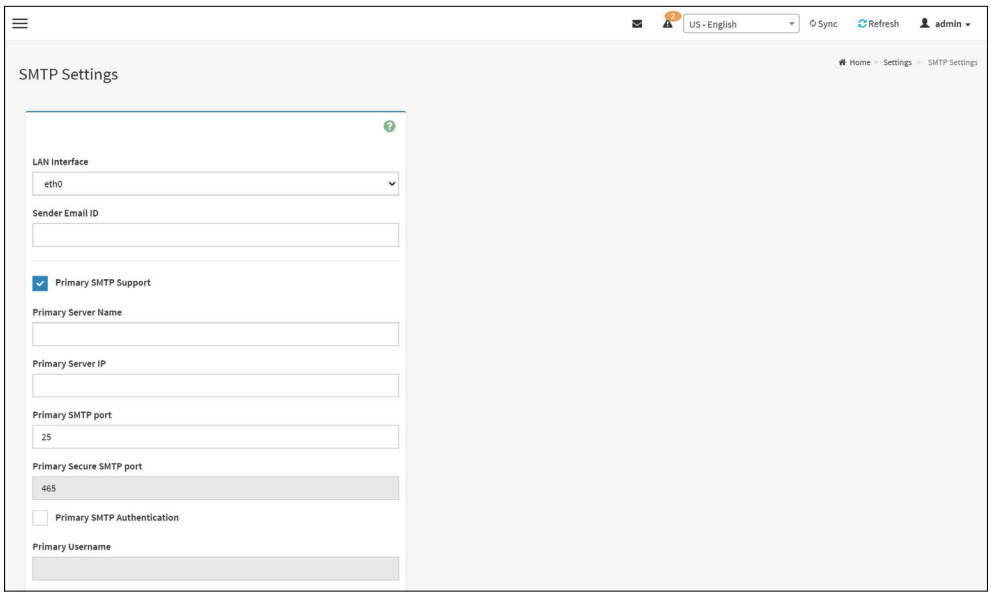
> **NOTE**
> The values in the Maximum Sessions field cannot be modified.

9. Click Save to save the entered changes else click Cancel to exit.

6.11 SMTP Settings

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

To open SMTP Settings page, click Settings → SMTP Settings from the menu bar. A sample screenshot of SMTP Settings page is shown below.



The fields of SMTP Settings page are explained below.

LAN Interface: Displays the list of LAN channels available

Sender Email ID: A valid 'Sender Address' to indicate the BMC, whenever e-mail is sent.

Primary Server Name: The 'Machine Name' of the BMC, from where the e-mail is sent.

> **NOTE**
> - Machine Name is a string of maximum 15 alpha-numeric characters.
> - Space, special characters are not allowed.

Primary SMTP Support: To enable/disable SMTP support for the BMC.

Primary SMTP Port: To specify the SMTP Normal Port.

Primary Secure SMTP Port: To specify the SMTP Secure Port.

> **NOTE**
> For Primary SMTP Port - Default Port is 25, and the Port value ranges from 1 to 65535.
> For Primary Secure SMTP Port - Default Port is 465, and the Port value ranges from 1 to 65535.

Primary Server IP: The IP address of the SMTP Server. It is a mandatory field.

> **NOTE**
> - IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
> - Each Number ranges from 0 to 255.
> - First Number must not be 0.
> - Supports IPv4 Address format and IPv6 Address format.

Primary SMTP Authentication: To enable/disable SMTP Authentication.

> **NOTE**
> SMTP Server Authentication Types supported are:
> - CRAM-MD5
> - LOGIN
> - PLAIN
> If the SMTP server does not support any one of the above authentication types, the user will get an error message stating, Authentication type is not supported by SMTP Server.

Primary Username: Enter username to access SMTP Accounts.

> **NOTE**
> - User Name can be of length 4 to 64 alpha-numeric characters, dot(.), dash(-), and underline(_).
> - It must start with an alphabet.
> - Other Special Charactres are not allowed.

Primary Password: Enter password for the SMTP User Account.

> **NOTE**
> - Password must be at least 4 characters long.
> - White space is not allowed.
> - This field will not allow more than 64 characters.

Primary SMTP STARTTLS Enable: To enable STARTTLS support for the SMTP Client.
Upload SMTP CA Certificate File: File that contains the certificate of the trusted CA certs.

- CACERT key file should be of pem type,
- **Upload SMTP Certificate File**: Client certificate filename. CERT key file should be of pem type.
- **Upload SMTP Private Key**: Client private key filename. SMTP key file should be of pem type.

> **NOTE**
> To enable STARTTLS support, the respective 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 Primary SMTP Support.

Save: To save the new SMTP server configuration.

Procedure

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

> **NOTE**
> - Machine Name is a string of maximum 15 alpha-numeric characters.
> - Space, special characters are not allowed.

5. Enter IP address of the SMTP Server in the Primary Server IP field. It is a mandatory field.
6. Enter the Primary SMTP Port in the specified field.
7. Enter the Primary Secure SMTP Port in the specified field.
8. Enable the check box Primary SMTP Authentication if you want to authenticate SMTP Server.
9. Enter your Primary User name and Primary Password in the respective fields.
10. Enable the check box Primary SMTP SSLTLS Enable to send data through secure Port.

> **NOTE**
> If this option is selected, STARTTLS option and Normal Port will be hidden.

11. Check the Secondary SMTP Support option to enable Secondary SMTP support for the BMC.
12. Enter the Secondary Server Name, Secondary Server IP, Secondary SMTP Port and Secure Port values in the respective fields.
13. Enable the check box SMTP Server Authentication if you want to authenticate SMTP Server.
14. Enter your Secondary User name and Password in the respective fields.
15. Enable the check box Secondary SMTP SSLTLS to send data through secure Port.

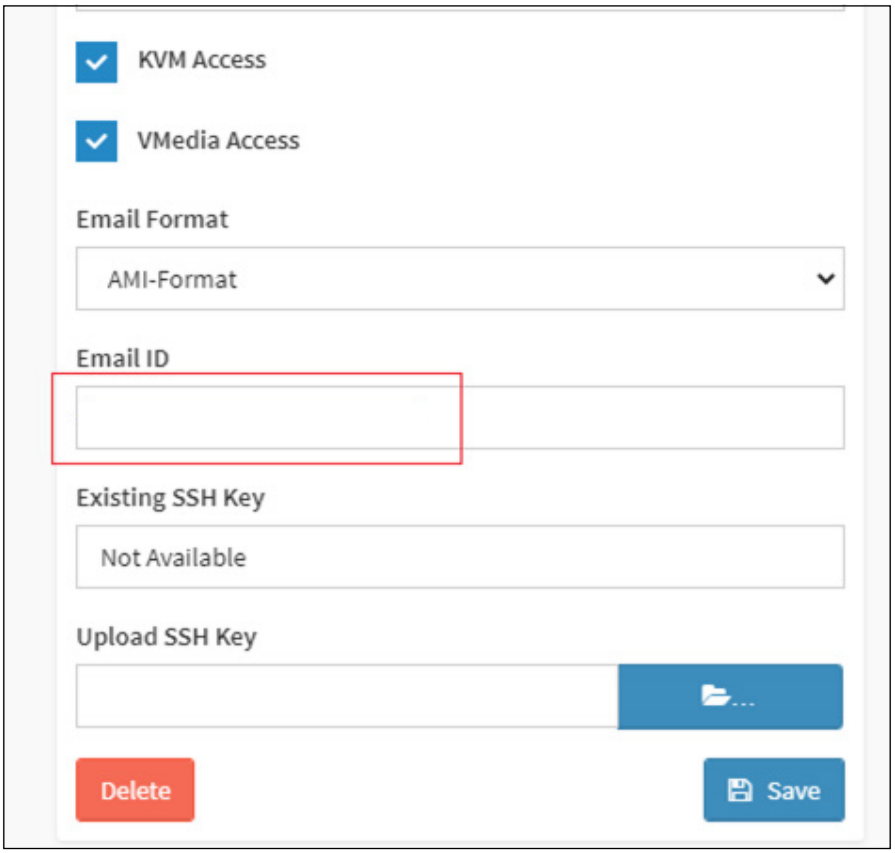
> **NOTE**
> If this option is selected, STARTTLS option and Normal Port will be hidden.

16. Click Save to save the entered details.

6.11.1 System Alert setting

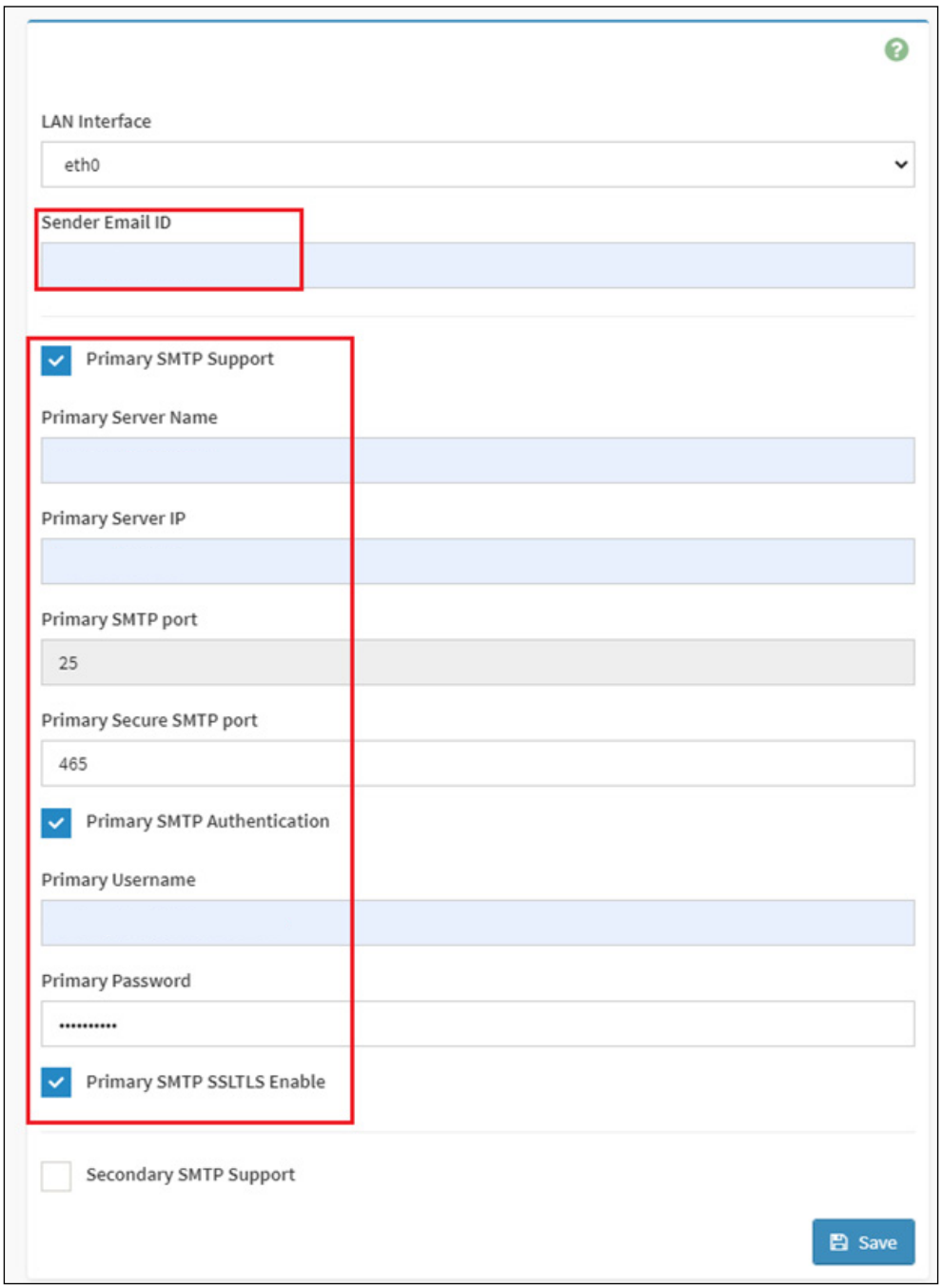
1. User Management Configuration Email ID for recipient's email address.

admin (recipient email address)



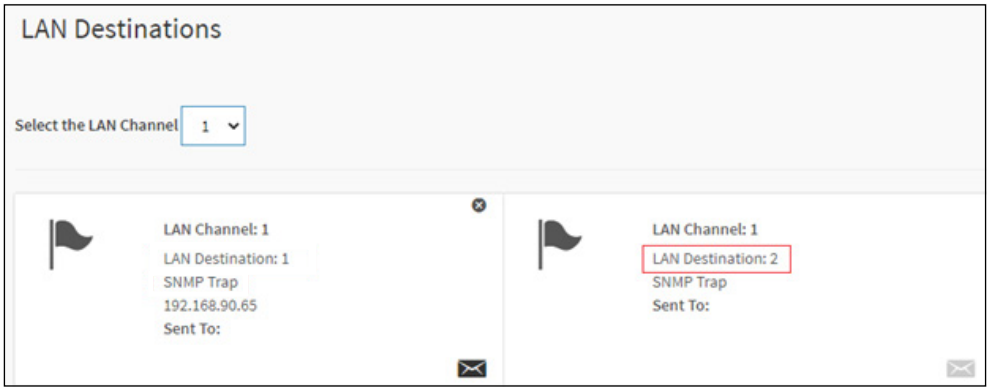
2. Settings - SMTP settings
   - Sender Email ID
   - Primary Server Name
   - Primary Server IP
   - Primary Username
   - Primary Password

   Please check with the email administrator.

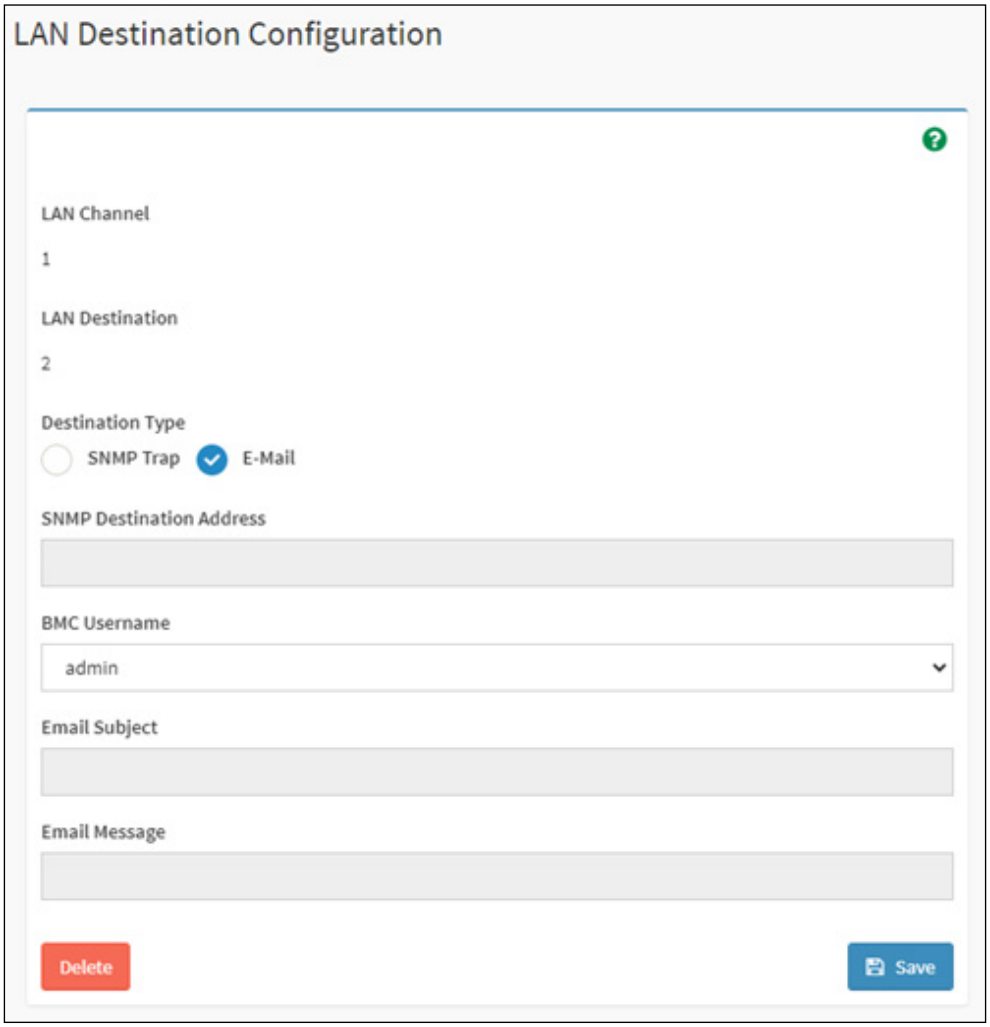


3. Settings - LAM Destinations

   Platform Event Filters- > LAN Destinations - > LAN Destination: 2

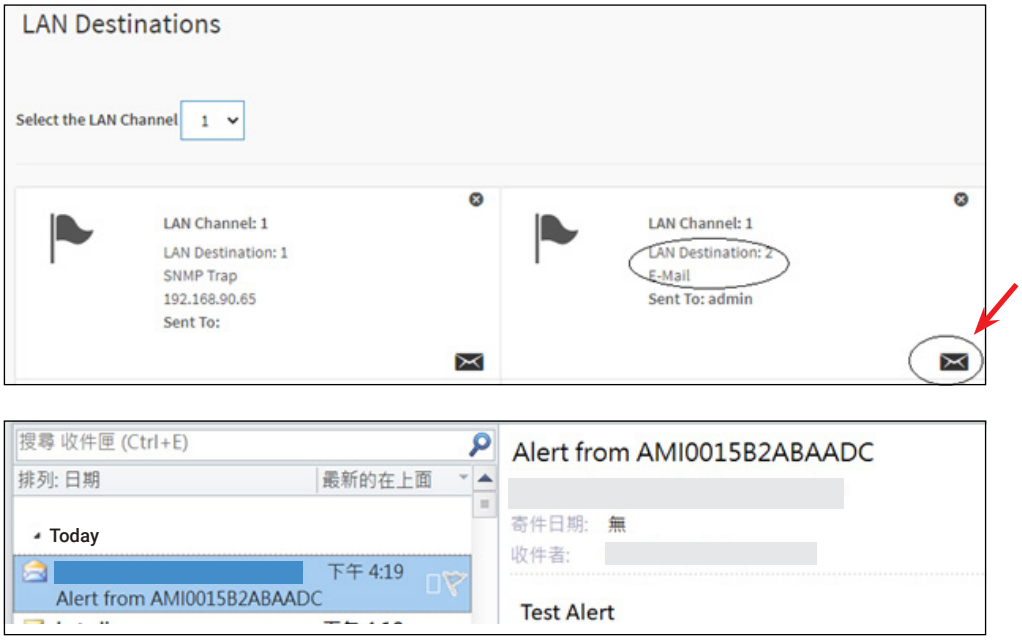


① LAN Destination Configuration:
Choose user and change the Destination Type to E-mail.



② Send a test mail

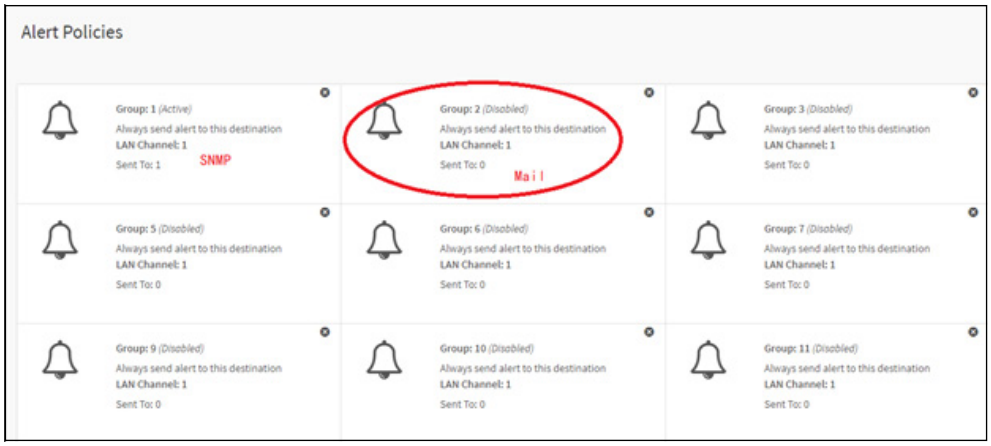
Platform Event Filters -> LAN Destination: 2 >> Send a Test Alert
System will send a test mail to the email address you set in step one.



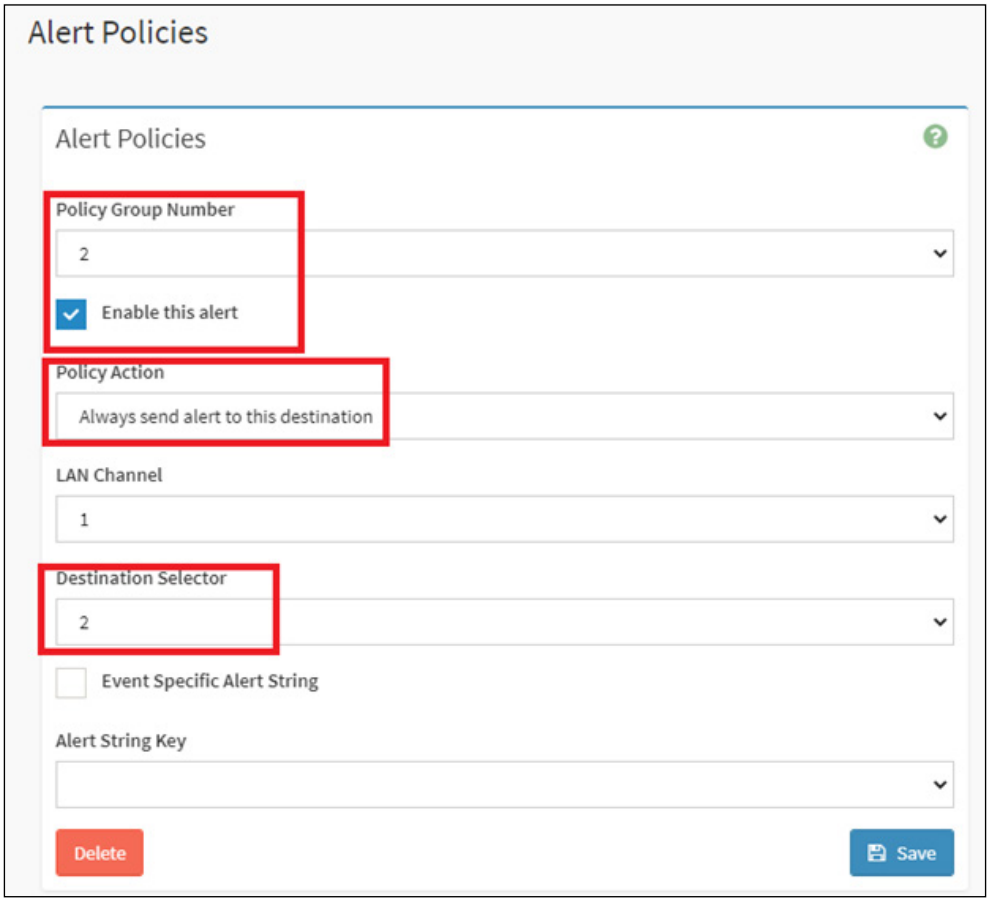
A sample of Test Alert mail

4. Settings - Alert Policies

Platform Event Filters -> Alert Policies >> Enable the alert



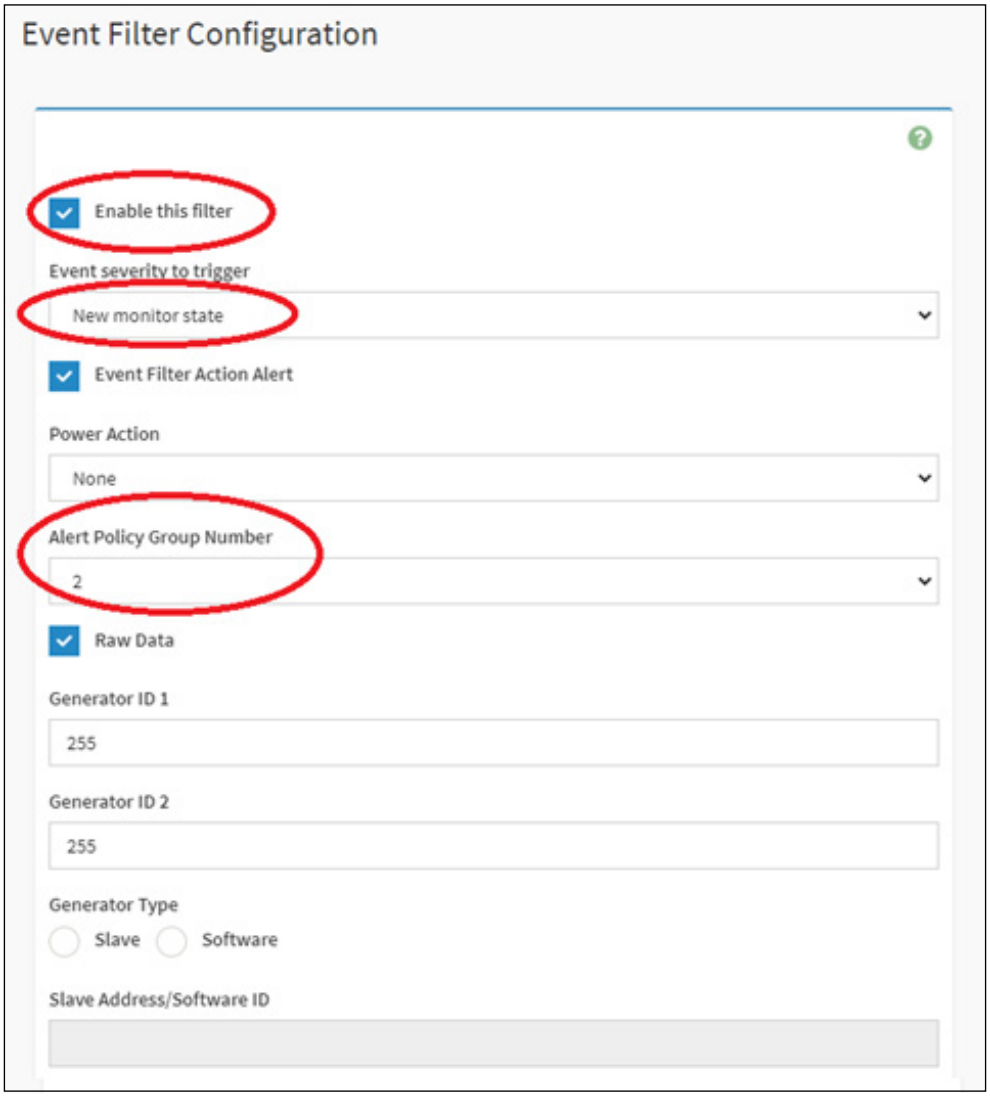
- Policy Group Number
  (Enable this alert)
- Policy Action
- Destination Selector



Alert Policies Settings

You can also set the events that you want to get the alerts on.
Platform Event Filter -> Event Filters >> Enable the alert

Event Fliters



- Enable this filter
- Event severity to trigger -> New monitor state
- Alert Policy Group Number

Remember to click Save to save the entered details.

6.12 SSL Settings

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

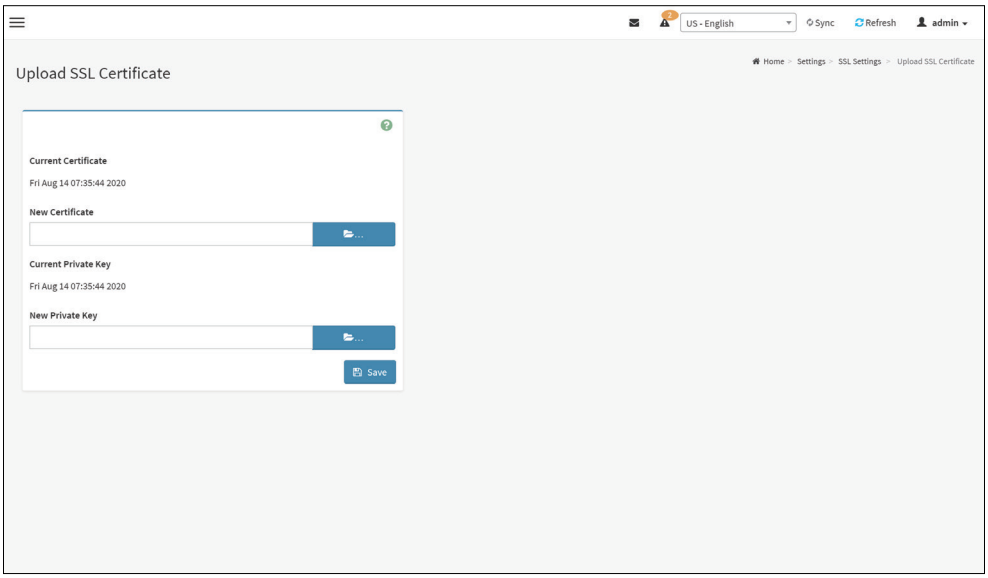
Configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open SSL Certificate Configuration page, click Settings → SSL Settings from the menu bar. There are three tabs in this page.

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

6.12.1 Upload SSL Certificate

A sample screenshot of Upload SSL Certificate page is shown below.



The fields of SSL Settings – Upload SSL Settings tab are explained below.

Current Certificate: Current certificate and uploaded date/time will be displayed (read-only).

New Certificate: Certificate file should be of pem type

Current Private Key: Current Private key information will be displayed (read-only).

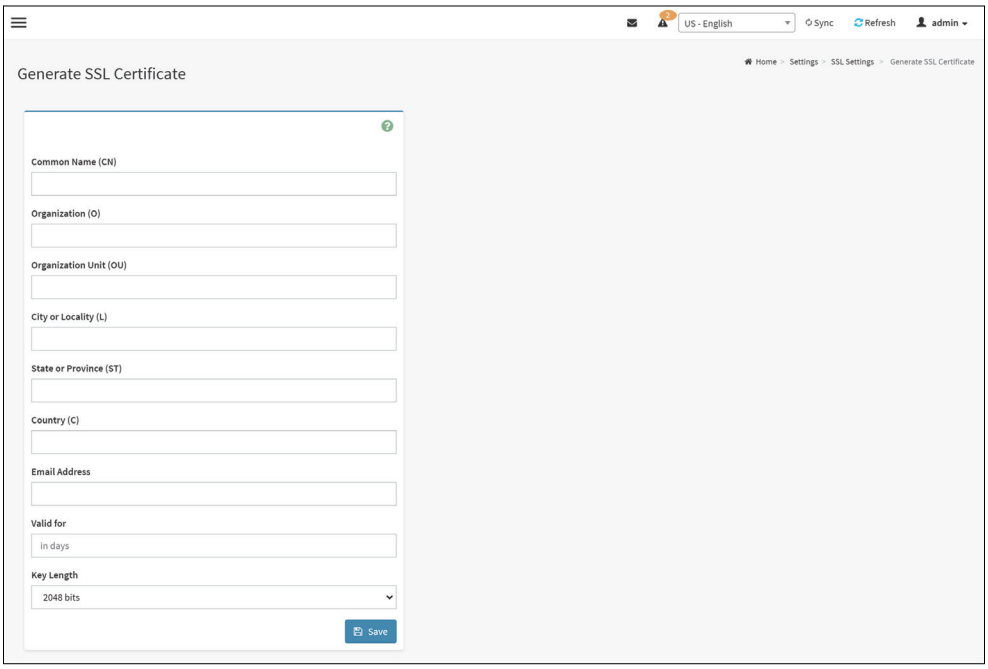
New Private Key: Private key file should be of pem type

Upload: To upload the SSL certificate and privacy key into the BMC.

> **NOTE**
> After successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

6.12.2 Generate SSL Certificate

A sample screenshot of Generate SSL Certificate page is shown below.



The fields of SSL Settings – Generate SSL Certificate are explained below.

Common Name(CN): Common name for which certificate is to be generated.
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization(O): Organization name for which the certificate is to be generated.
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization Unit(OU): Over all organization section unit name for which certificate is to be generated.
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

City or Locality(L): City or Locality of the organization (mandatory).
- Maximum length of 128 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

State or Province(ST): State or Province of the organization (mandatory).
- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Country(C): Country code of the organization (mandatory).
- Only two characters are allowed.
- Special characters are not allowed.

Email Address: E-mail Address of the organization (mandatory).

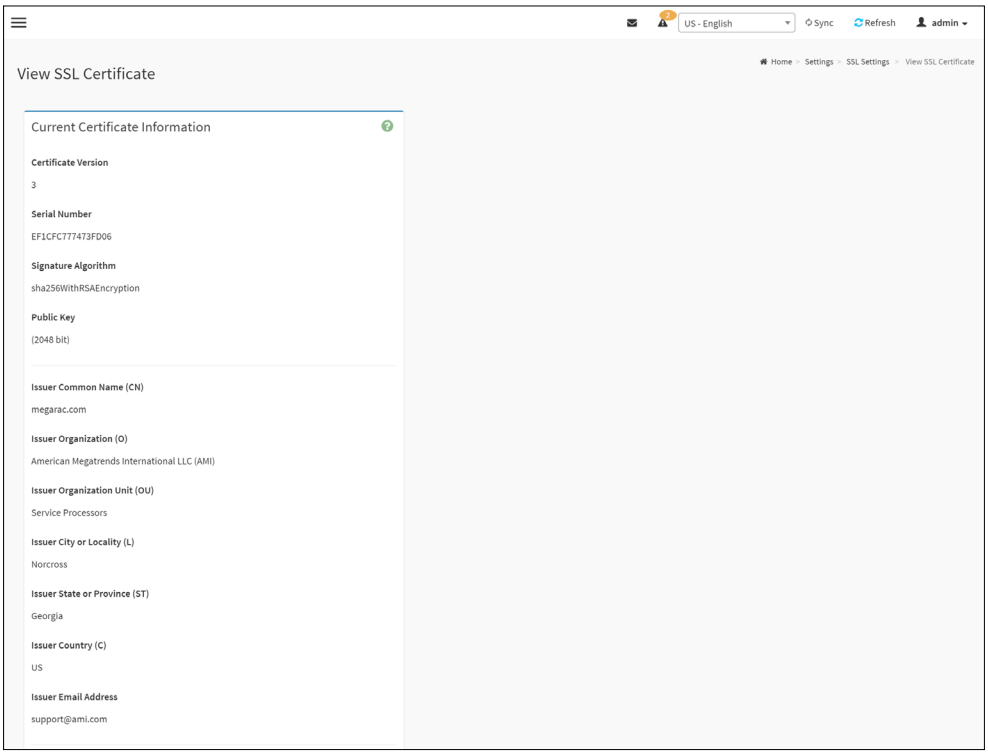
Valid for: Validity of the certificate.
- Value ranges from 1 to 3650 days.

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

Save: To generate the new SSL certificate.

> **NOTE**
> HTTPs service will get restarted, to use the newly generated SSL certificate.

6.12.3 View SSL Certificate



The fields of SSL Settings – View SSL Certificate are explained below.

Basic Information: This section displays the basic information about the uploaded SSL certificate. It displays the following fields.
- Version Serial Number
- Signature Algorithm
- Public Key
- Issuer Common Name(CN)
- Issuer Organization(O)
- Issuer Organization Unit(OU)
- Issuer City or Locality(L)
- Issuer State or Province(ST)
- Issuer Country(C)
- Issuer E-mail Address
- Valid From
- Valid Till

Procedure

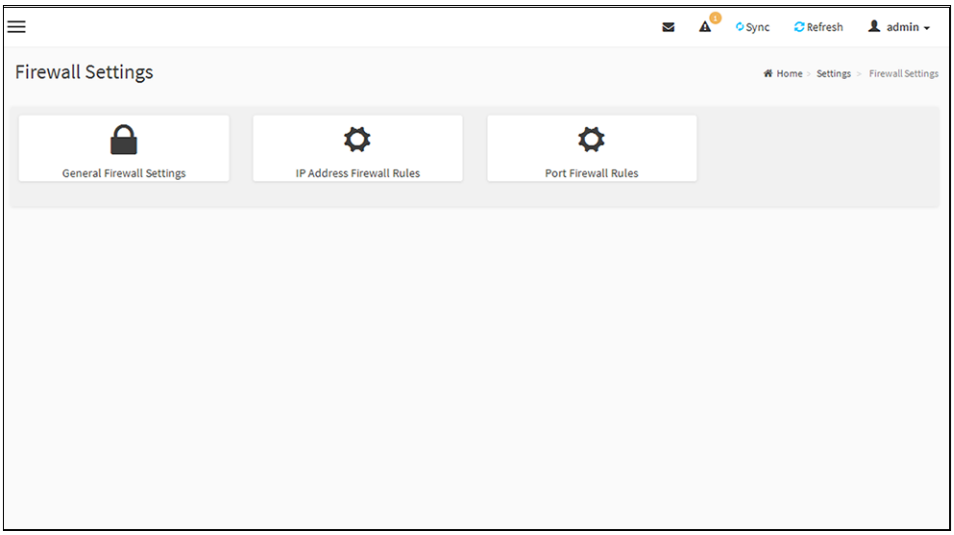
1. Click the Upload SSL Certificate tab, Browse the New Certificate and New Private key.
2. Click Upload to upload the new certificate and private key.
3. In Generate SSL Certificate, enter the following details in the respective fields.
   - The Common Name for which the certificate is to be generated.
   - The Organization for which the certificate is to be generated.
   - The Organization Unit name for which certificate to be generated.
   - The City or Locality of the organization
   - The State or Province of the organization
   - The Country of the organization
   - The Email address of the organization.
   - The number of days the certificate will be valid in the Valid For field.
4. Choose the Key Length bit value of the certificate
5. Click Save to generate the certificate.
6. Click View SSL Certificate tab to view the uploaded SSL certificate in user readable format.

NOTE
- Once you Upload/Generate the certificates, only HTTPs service will get restarted.
- You can now access your Generic MegaRAC® SP securely using the following format in your IP Address field from your Internet browser: https://<your MegaRAC® SP's IP address here>
- For example, if your MegaRAC® SP's IP address is 192.168.0.30, enter the following: https://192.168.0.30
- Please note the <s> after <http>.You must accept the certificate before you are able to access your Generic MegaRAC® SP.

6.13 System Firewall

The System Firewall page 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 System Firewall page, click Settings → System Firewall from the menu bar.

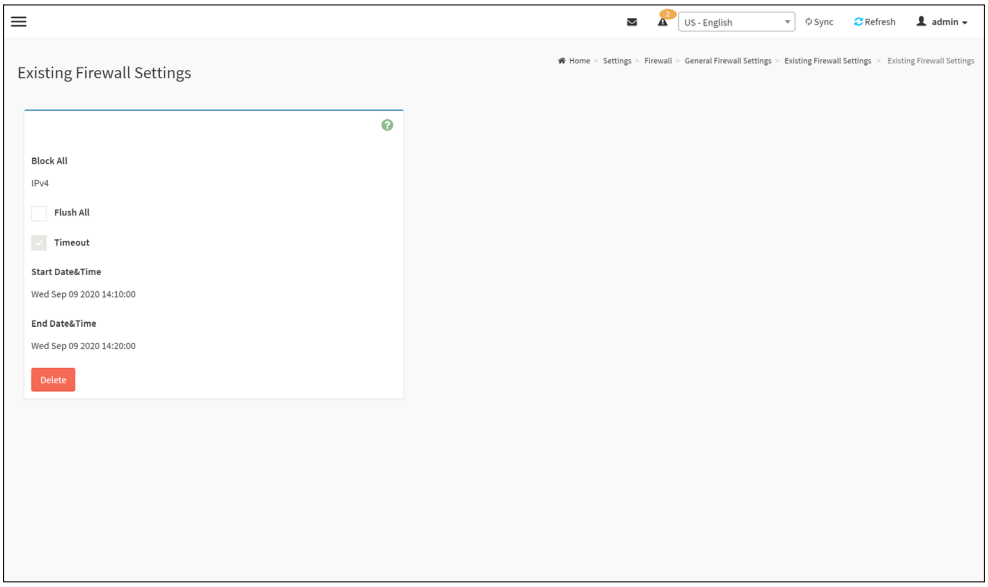


6.13.1 General Firewall Settings

Click General Firewall Settings page. The fields of Firewall Settings tab are explained below.

Existing Firewall Settings

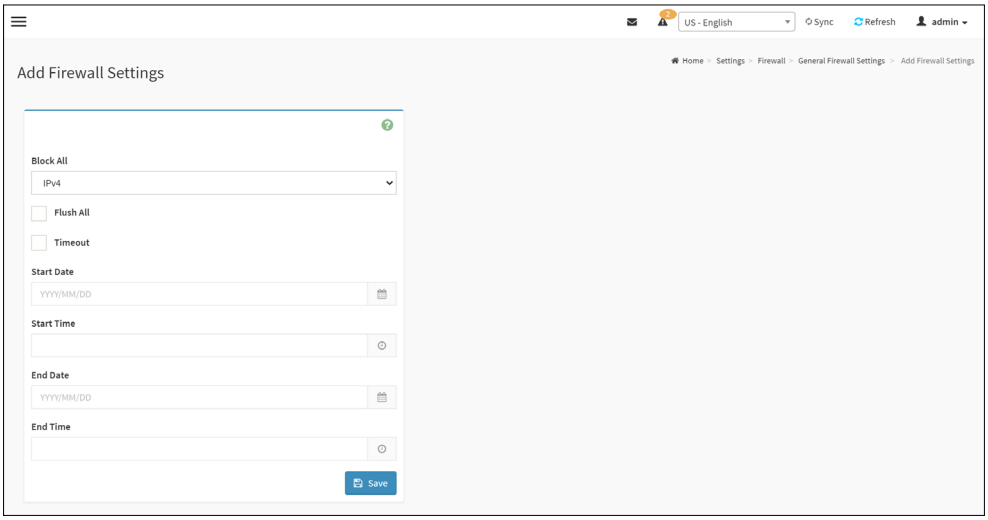
1. Click General Firewall Settings → Existing Firewall Settings icon. A blank page will be opened if you did not add anything in “Add Firewall settings”. If there is no Firewall Settings Exists, add a new Firewall settings by clicking link Add Firewall Settings page. A sample screenshot of Existing Firewall Settings page is shown below.



2. Select Block All to block all the incoming IP's and Port's.
3. Select Flush All to flush all the system firewall rules.
4. Select Timeout to enable or disable firewall rules with timeout.

Add Firewall Settings

1. Click General Firewall Settings → Add Firewall Settings. This opens the Existing Firewall Settings page as shown below.



2. Select Block All to block all the incoming IP's and Port's.
3. Select Flush All to flush all the system firewall rules.
4. Select Timeout to enable or disable firewall rules with timeout.
5. Enter Start Time to start the respective firewall rule effect from this time.
6. Enter End Time to end the respective firewall rule effect from this time.

> **NOTE**
> The time should be in the dd-mm-yy:hh-mm formart.

7. Click Save to save the changes made else click Cancel to go back to the previous screen.

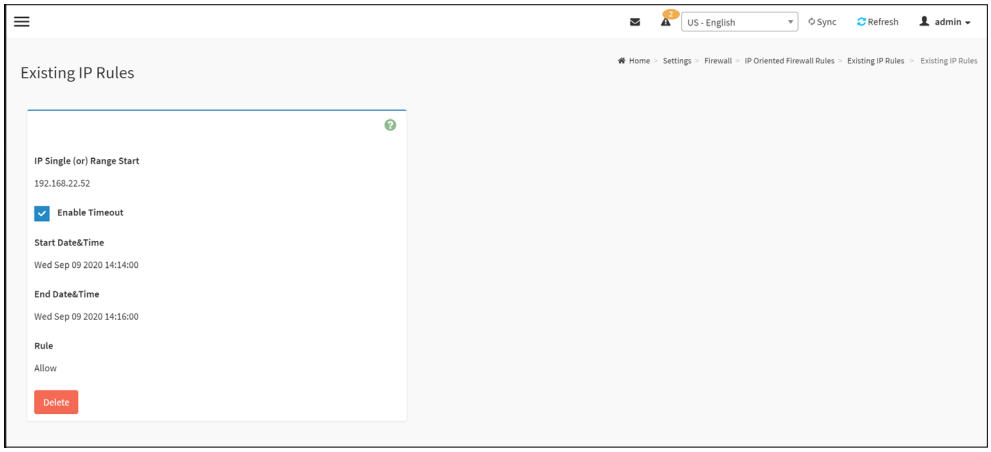
IP Address Firewall Rules

To View Existing IP Rules or a range of IP Addresses,

A blank page will be opened if you did not add anything in “Add IP Rule”. If there is no Add IP Rule Exists, add a new IP Rule by clicking link Add IP Rule page.

Procedure to Add IP Rule

1. Click Settings→ System Firewall→ IP Address Firewall Rules→ Existing IP Rules. A blank page will be opened if you did not add anything in “Add IP Rule”. If any rule is added, then the added rule will be listed in “Existing IP Rules” page.
2. Click the IP Addresses tab. A sample screenshot of IP Addresses tab is shown below.



IP Single (or) Range Start - To show the configured Port Address or Range of Ports.

Range End - To show the configured Port Address or Range of Ports.

Enable Timeout - To enable/disable Timeout.

Start Date - The respective firewall rule effect will start from this date.

Start Time - The respective firewall rule effect will start from this time.

End Date - The respective firewall rule effect will end from this date.

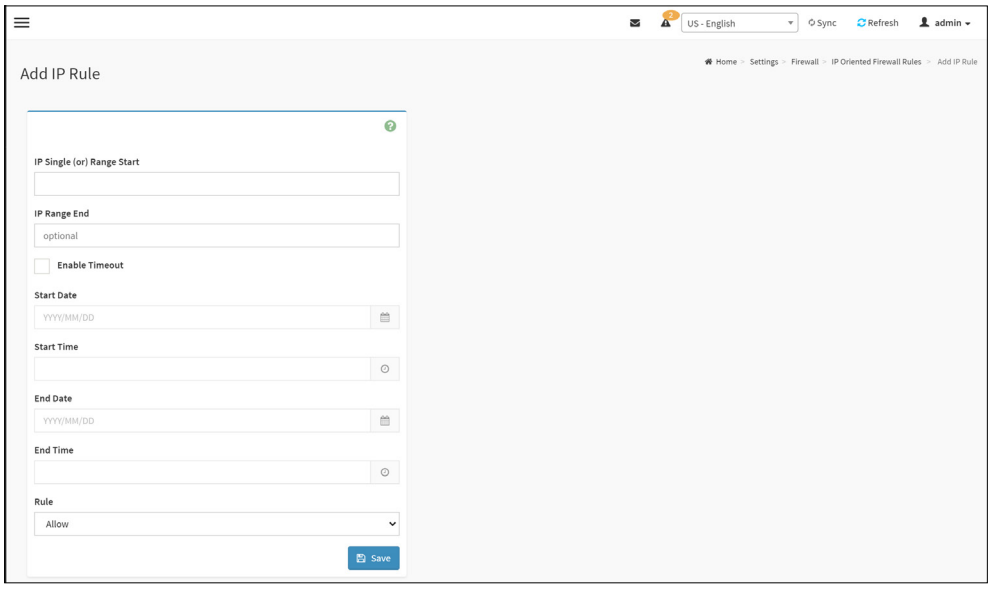
End Time - The respective firewall rule effect will end from this time.

Rule - To indicate the current setting of the listed Port or Range of Port rules (Allow or Block) status.

Delete - To delete the selected slot.

Procedure To add an IP address or range of IP adresses,

1. Click Settings→ System Firewall→ IP Address Firewall Rules→ Add New IP Rule to add a new IP or range of IP address.



2. In the Add new rule for IP page, Enter the IP address and a range of IP addresses in the IP Single or IP Range Start field.

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

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

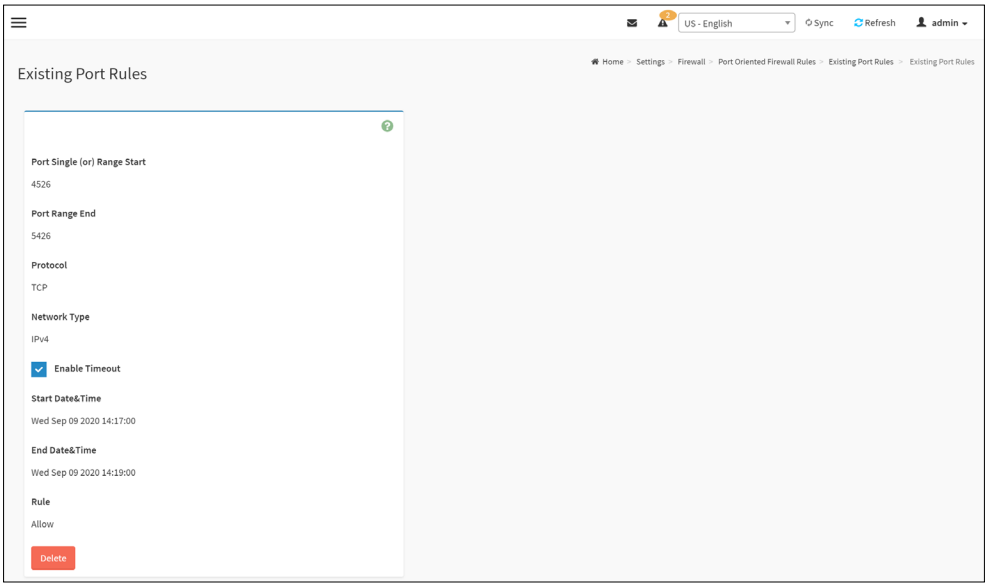
> **NOTE**
> The date and time should be in the YYYY/MM/DD and hh-mm formart respectively.

9. Determine the rule to block or accept.
10. Click Save to save the changes made.

Port Firewall Rules

To view Existing Port Rules

1. Click Settings→ System Firewall→ Port Firewall Rules→ Existing Port Rules. A blank page will be opened if you did not add anything in “Add New port Rule”. If any rule is added, then the added rule will be listed in “Existing Port Rules” page.
2. Click the Existing Port Rules. A sample screenshot of Port tab is shown below.



6.13.2 System Firewall

The fields of System Firewall - Existing Port Rules page are explained below.

Port Single (or) Range Start - To configure the Port or Range of Port Addresses.

Port Range End - To configure the Port or Range of Port Addresses.

Protocol - This field specifies the protocols for the configured Port or Port Ranges.

Network Type - This field specifies the affected network type for the particular Port or Port Ranges.

Enable Timeout - To enable or disable firewall rules with timeout.

Start Date - The respective firewall rule effect will start from this time.

Start Time - The respective firewall rule will start from this time. End Date - The respective firewall rule effect will end on this date. End Time - The respective firewall rule will end at this time.

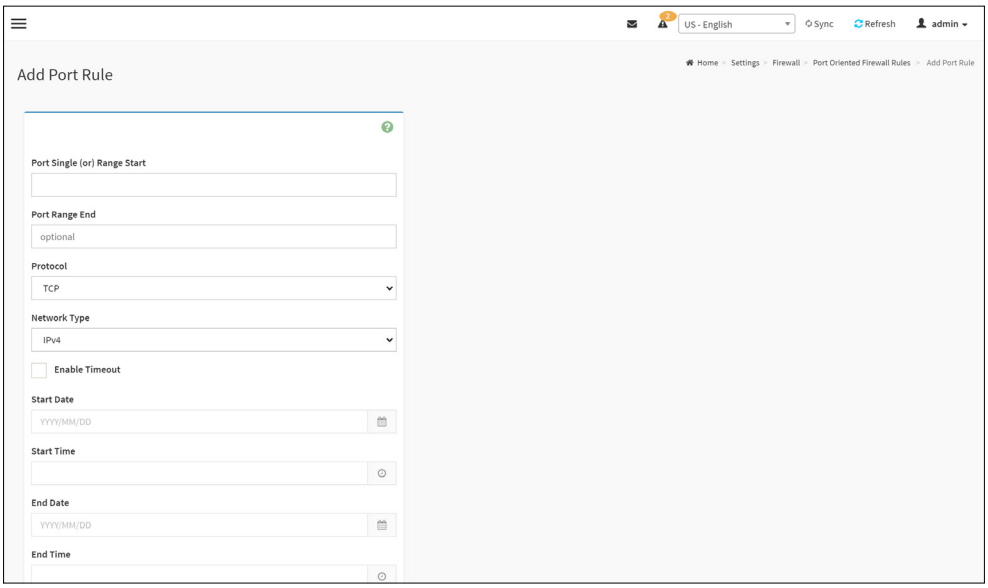
Rule - To indicate Allow or Block status.

Delete - To delete the entry to the firewall rules list.

Procedure

To Add Port/Range of ports

1. To add a new rage of Port address, click the Add button.



2. In the Add new rule for Port window, Enter the port number or a range of port numbers in the Port Single (or) Range Start field.

> **NOTE**
> Port value ranges from 1 to 65535.

3. Enter the end value in the Port Range End field.
4. Select the Protocol to be either TCP or UDP or Bot.
5. Select the Network Type. It may be IPv4 or IPv6 or Both.
6. Select Timeout to enable or disable firewall rules with timeout.
7. Enter Start Time to start the respective firewall rule effect from this time.
8. Enter Start Date to start the respective firewall rule effect from this date.
9. Enter End Date to end the respective firewall rule effect on this date.
10. Enter End Time to end the respective firewall rule effect at this time.

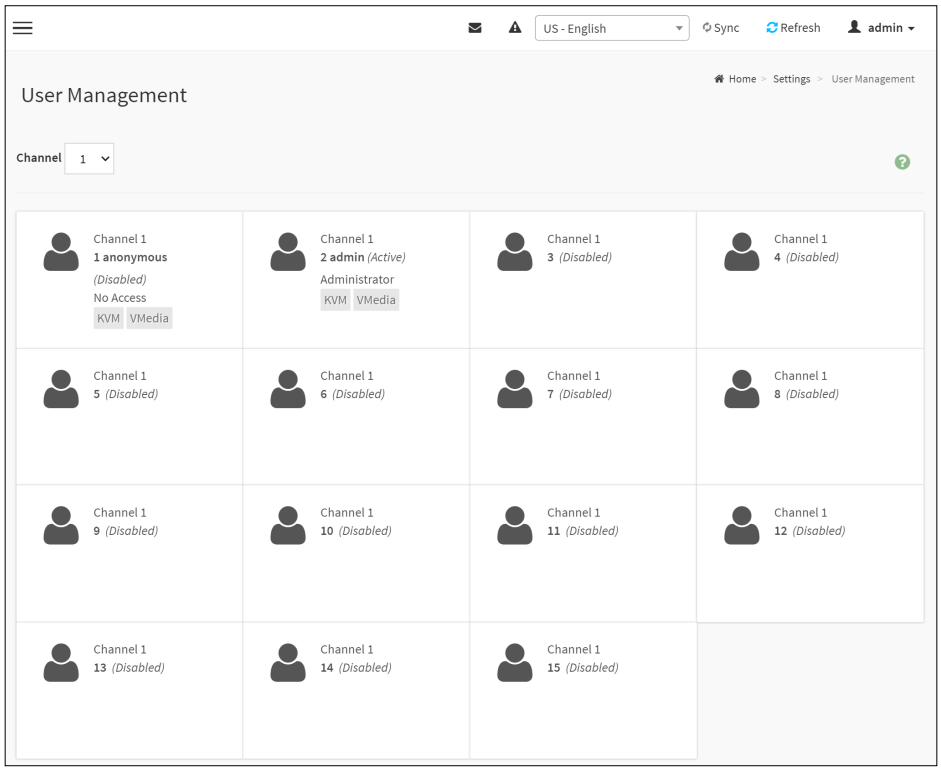
> **NOTE**
> The time should be in the YYYY/MM/DD:hh-mm format.

11. Select the Rule to determine the rule to Block or Allow.
12. Click Save to save the changes made.

6.14 User Management

The User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

To open User Management page, click Settings → User Management from the menu bar. A sample screenshot of User Management page is shown below.



Click user icon ( ) and select any free slot to add a new user from the User Management main page. Click Delete icon (x) on the top right corner to directly delete an item from the list.

> **NOTE**
> The Free slots are shown as “Disabled” in all columns for the slot.

The fields of User Management page are explained below.

User ID: Displays the ID number of the user.

> **NOTE**
> The list contains a maximum of ten users only.

User Name: Displays the name of the user.

User Access: To enable or disable the access privilege of the user.

Network Privilege: Displays the network access privilege of the user.

SNMP Status: Displays if the SNMP status for the user is enabled or Disabled.

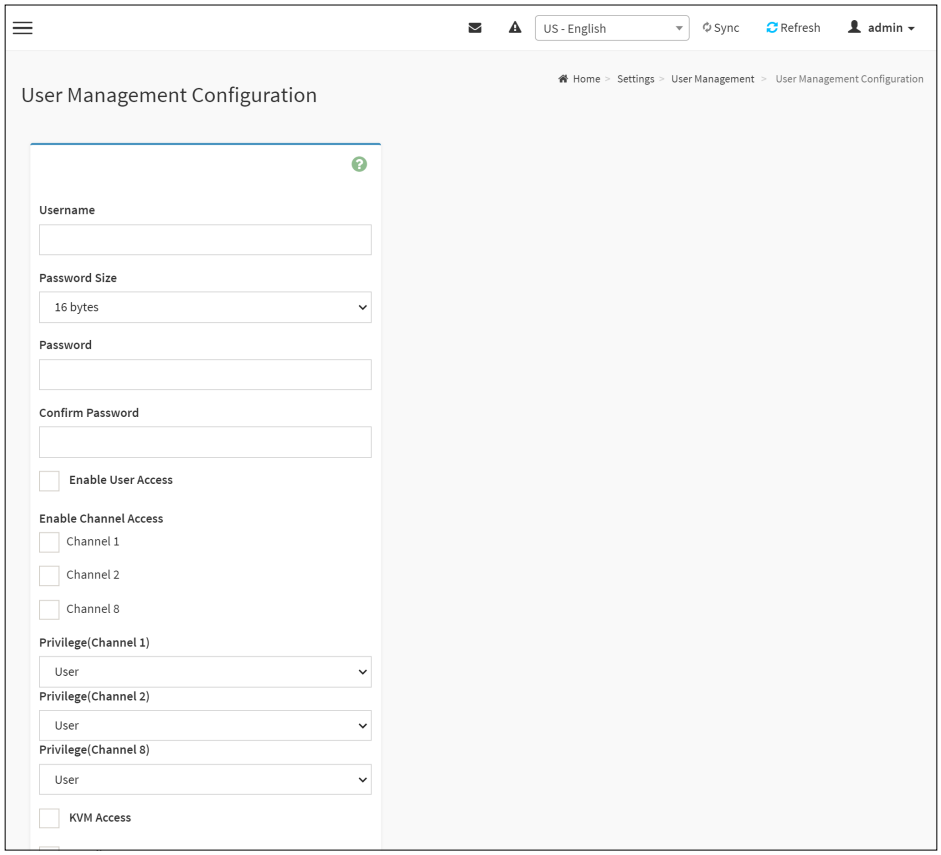
E-mail ID: Displays e-mail address of the user.

Add User: To add a new user.

Delete User: To delete an existing user.

Procedure to add a new User

1. To add a new user, select a free section and click on the empty section. This opens the Add User screen as shown in the screenshot below.



2. Enter the name of the user in the User Name field.

NOTE
- User Name is a string of 1 to 16 alpha-numeric characters.
- It must start with an alphabetical character.
- It is case-sensitive.
- Special characters '-'(hyphen), '_'(underscore), '@'(at sign) are allowed.
- For 20 Bytes password, LAN session will not be established.

3. Set Password Size for the new password.

4. In the Password and Confirm Password fields, enter and confirm your new password.

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

Hex	Char
00	NUL '\0'
01	SOH (start of heading)
02	STX (start of text)
03	ETX (end of text)
04	EOT (end of transmission)
05	ENQ (enquiry)
06	ACK (acknowledge)
07	BEL '\a' (bell)
08	BS '\b' (backspace)
09	HT '\t' (horizontal tab)
0A	LF '\n' (new line)
0B	VT '\v' (vertical tab)
0C	FF '\f ' (form feed)
0D	CR '\r' (carriage ret)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)
11	DC1 (device control 1)
12	DC2 (device control 2)
13	DC3 (device control 3)
14	DC4 (device control 4)
15	NAK (negative ack.)
16	SYN (synchronous idle)
17	ETB (end of trans. blk)
18	CAN (cancel)
19	EM (end of medium)
1A	SUB (substitute)
1B	ESC (escape)
1C	FS (file separator)
1D	GS (group separator)
1E	RS (record separator)
1F	US (unit separator)
20	SPACE
7F	DEL

5. In Enable User Access, select this option to enable the network access for the appropriate user.

NOTE
- Enabling Channel User Access will intern assign the IPMI messaging privilege to the specific Channel user.
- It is recommended that the IPMI messaging option should be enabled for the user to enable the User Access option, While creating User through IPMI.

6. In Enable Channel Access field, select the channel/channels to enable the network access for the appropriate channels."
7. In the Privilege field, select the privilege assigned to the user which could be Administrator, Operator, User, OEM or None. By default, the channel privileges will be displayed based on the channel availability.
8. Check KVM Access to assign the KVM privilege for the user.
9. Check VMedia Access 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 / starting media redirection. If a device is already being redirected and attached to the host, then in host it will be visible as normal device. Hence it will be accessible to all the KVM sessions. Which includes 'KVM Privilege only' sessions as well.

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.

10. Check the SNMP Access check box to enable SNMP access for the user.

NOTE
Password field is mandatory, if SNMP Status is enabled.

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

NOTE
Password field is mandatory, if Authentication protocol is changed.

13. Choose the Encryption algorithm to use for SNMP settings from the SNMP Privacy protocol (AES or DES) drop-down list.
14. In the Email ID field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

NOTE
SMTP Server must be configured to send emails.

Email Format: Two types of formats are available:

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

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

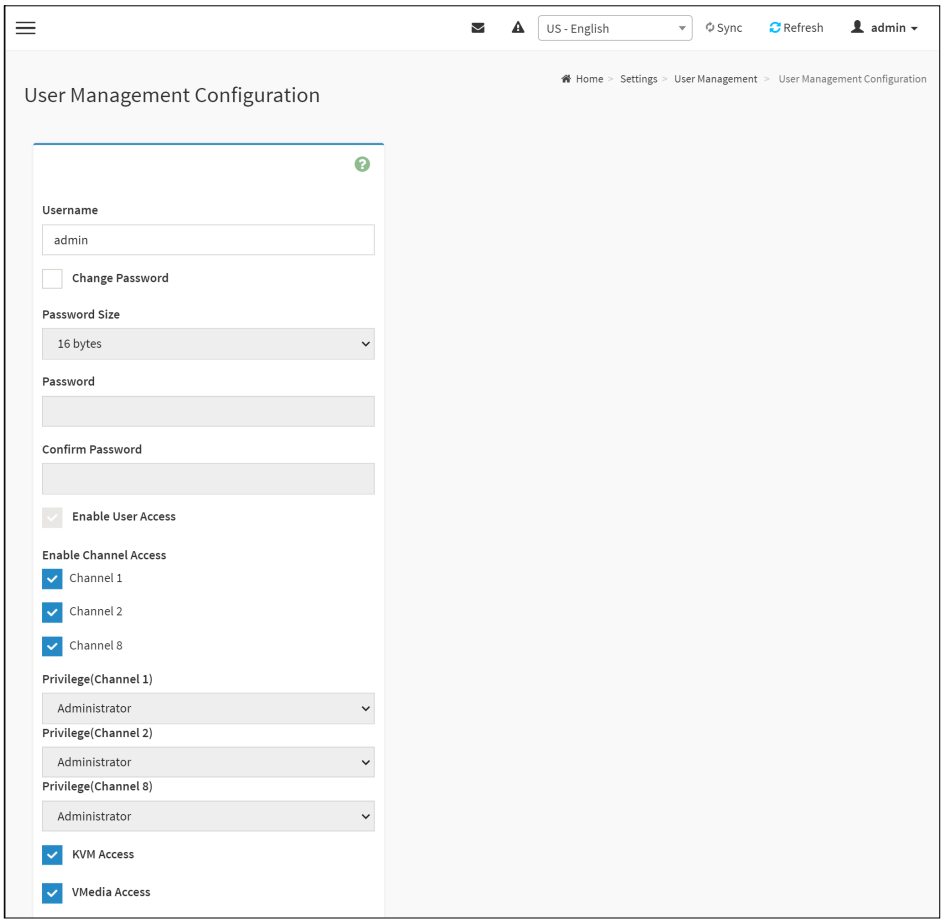
15. In the Upload SSH Key field, click Browse and select the SSH key file.

NOTE
SSH key file should be of pub type.

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

To Modify User

1. To modify the existing user, click on the active user tab. This opens a User screen as shown in the screenshot below.



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

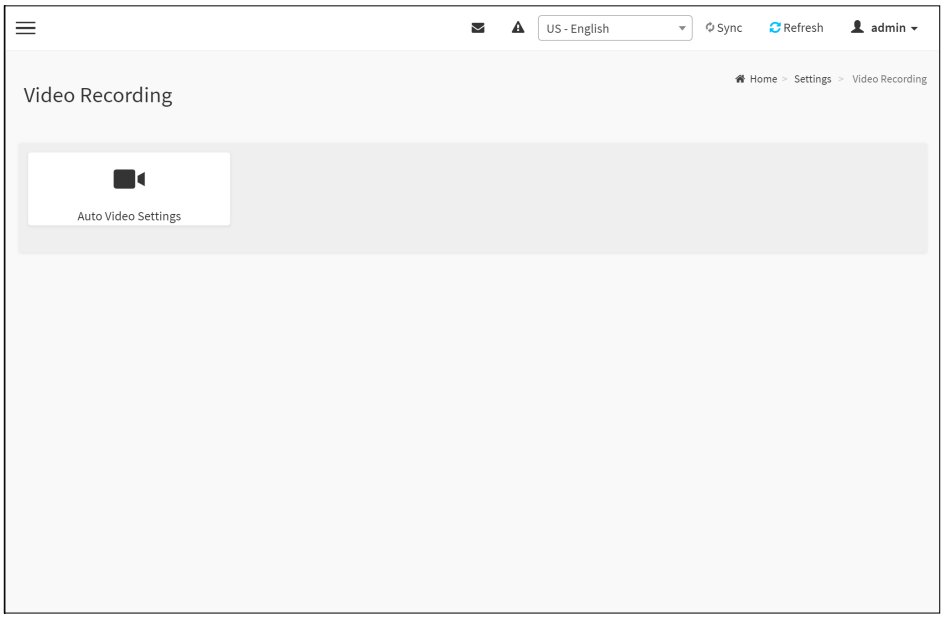
NOTE

There is a list of reserved users which cannot be added / modified as BMC users. Please Refer MEGARAC SP-X Platform Porting Guide section Changing the Configurations in PMC File → User Configurations in PMC File for the list of reserved users.

Important:
Reserved Users: There are certain reserved users which cannot be added as BMC Users. The list of reserved users are given below,
- sysadmin
- daemon
- sshd
- ntp
- root

6.15 Video Recording

The Video Recording consists of the following. A sample screenshot of the Video Recording is given below.

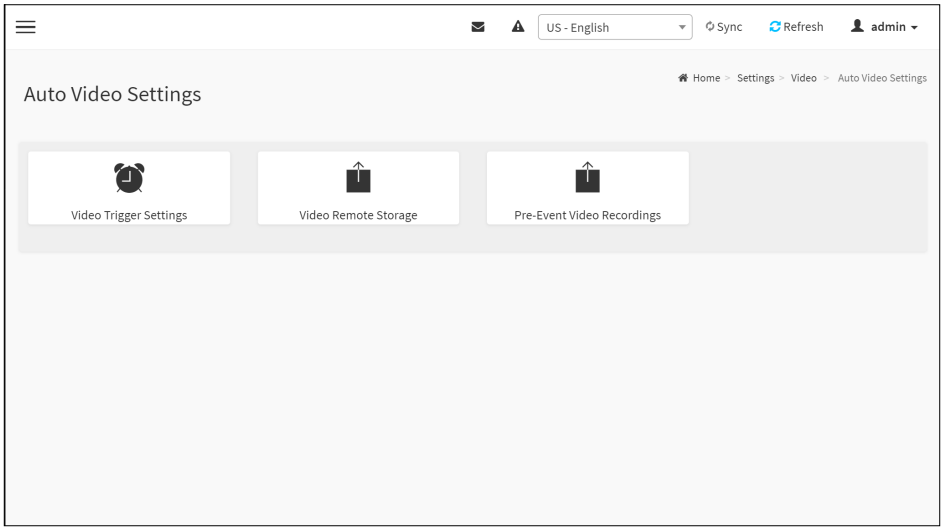


- Auto Video Settings
- Video Trigger Settings
- Video Remote Storage
- Pre-Event Video Recordings
- SOL Settings
- SOL Trigger Settings
- SOL Video Settings
- SOL Recorded Video

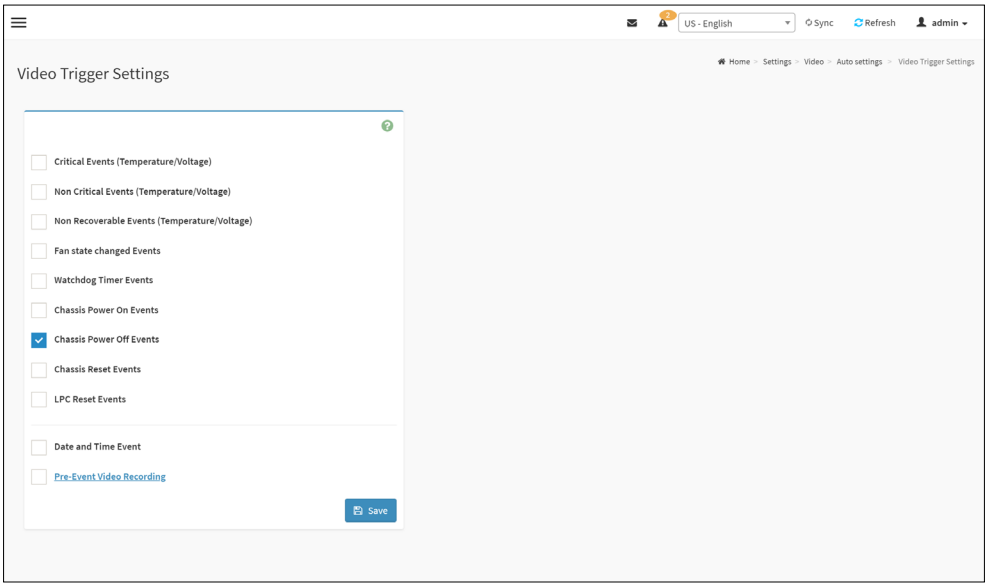
A detailed description of the menu items are given below.

6.15.1 Auto Video Settings

This page is used to configure the events that will trigger auto video recording function of the KVM server. A sample screenshot of the Video Recording is given below.



6.15.2 Video Trigger Settings



Event List: It shows the list of available events to be configured. The events are mentioned below.

- Critical Events (Temperature/Voltage)
- Non Critical Events (Temperature/Voltage)
- Non Recoverable Events (Temperature/Voltage)
- Fan state changed Events
- Watchdog Timer Events
- Chassis Power on Events
- Chassis Power off Events
- Chassis Reset Events
- LPC Reset Events
- Date and Time Event
- Pre-Event Video Recording
- Pre-crash
- Pre-reset

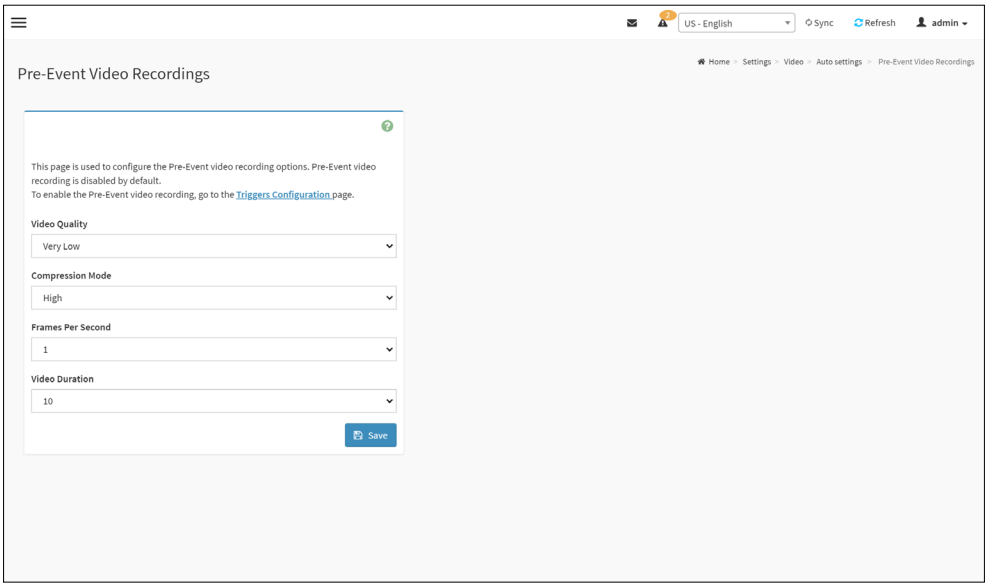
Save: To save any changes made.

Procedure:

1. Check the events to be enabled.
2. To set particular Date and Time Event, check the option Date and Time Event.
   a. Choose the month, day and year from the Date field
   b. Enter/Choose the Time in hh:mm format in the respective fields.

> **NOTE**
> KVM service should be enabled to perform auto-video recording. The date and time should be in advance to the system date and time.

3. Click Pre-Event Video Recording to edit the Pre-Event video recording configurations. A sample screenshot of Pre-Event Video Recordings page is shown as below.



a. To set video quality, select ranges (very low, low, high, average and normal) from Video Quality drop-down list.

b. To set compression mode, select modes (high, nowmal, low, no) from Compression Mode drop-down list.

c. To set number of frames per second, select frames/sec (1-4) from Frames Per Second drop- down list.

d. To set duration of video, select second (10-60) from Video Duration drop-down list.

e. Click Save to save the changes made on the Pre-Event Video Recording.

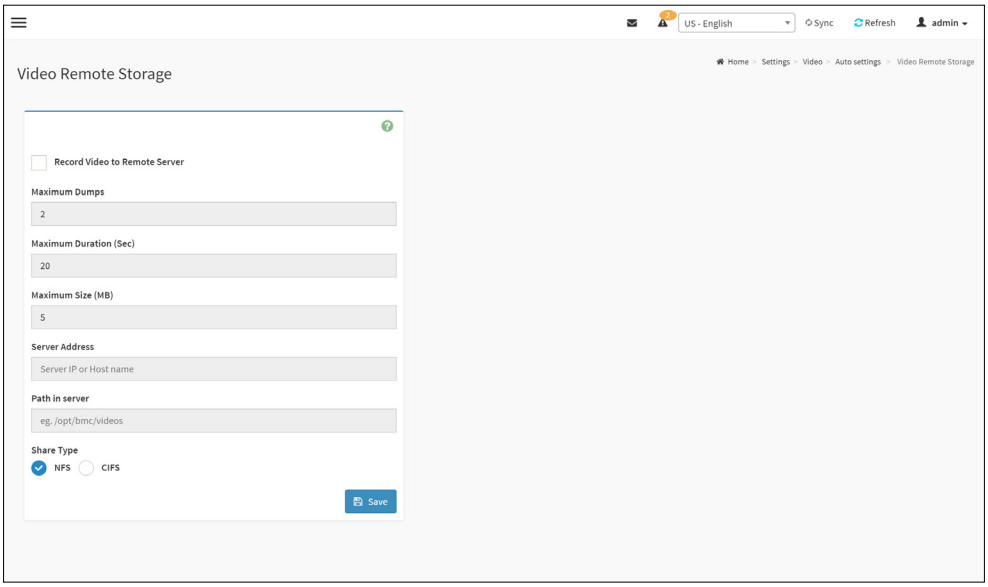
4. Select Crash Reset either Pre-crash or Pre-reset.

5. Click Save to save the changes.

NOTE
Pre-Event video recording will not occur, while active KVM session or Post-event video recording is in progress.

6.15.3 Video Remote Storage

To Video Remote Storage capture host video before critical event like crash or reset occurs, click Video Recording → Auto Video Settings → Video Remote Storage. A Sample screenshot of Video Remote Storage is as shown below.



1. Check Record Video to Remote Server to enable the Remote Video Support.

> **NOTE**
> By default, video files will be stored in local path of BMC. If remote video support is enabled, then the video files will be stored only in remote path, not within BMC.

2. Enter Maximum Duration (Sec) of the video.
3. Enter Maximum Size (MB) of the video.
4. Enter Maximum Dumps of the video.

> **NOTE**
> The Maximum Duration of the video should be in the range from 1 to 3600 seconds. The Maximum Size of the video should be in the range from 1 to 500 mb. The Maximum Dumps should be in the range from 1 to 100. The recorded video file should meet either the size con- straint or duration constraint, according to the configured settings, depending on which constraint is met first.

5. Enter the Server Address.

> **NOTE**
> Server address will support the following:
> - IP Address (Both IPv4 and IPv6 format).
> - FQDN (Fully qualified domain name) format.

6. Enter the source path in Path in Server field.

7. Select the Share Type (NFS/CIFS). If the selected share type is (CIFS), Enter the User Name, Password and Domain Name in the respective fields.

8. Click Save to save the settings.

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

Post-Event
Post-Event video recording files will be named as shown below.
video_dump_<Hostname>_%Y%m%dT%H%M%S.dat.

File Count and Duration for Pre and Post Event Recordings are as shown in the below table:

	Auto Video Recording (Post Event)	**Pre-Event Video Recording(only for Crash/reset event)**
Time Limits	20 seconds or 5.5MB video allowed if Local Storage.	Default-10sec, but can be configurable up to 60sec.
	300 seconds recording allowed if Remote Storage(Remote Path).	
Video File Count	Local Storage: 2 (After 2, if video recording starts, the oldest video file among the two files will be replaced with the new video)	1 if local storage/3 if remote storage. (Once Max file count reached, will Delete Old video file to store new file.)
	Remote Storage: maximum configured dump value of video files for Remote Storage.	

6.16 IPMI Interfaces

This page is used to configure the IPMI Interfaces. To open IPMI interfaces page, click Settings → IPMI Interfaces. A sample screenshot of IPMI Interfaces page is displayed below.

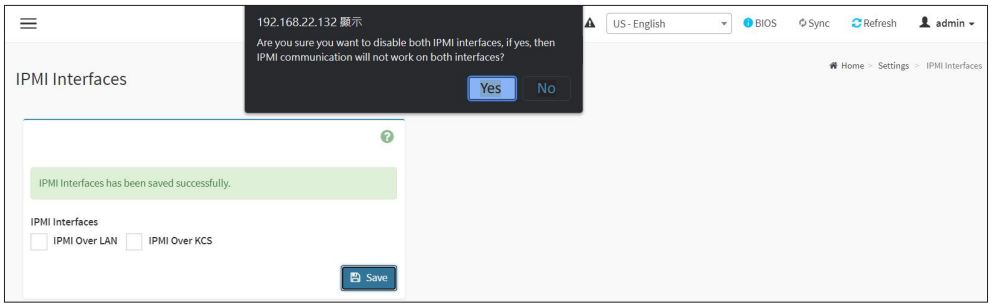
This page displays the following interfaces like IPMI Over LAN and IPMI Over KCS.

Procedure

- **IPMI Over LAN**: Check or uncheck the IPMI Over LAN interface which allows the user to perform IPMI communication over LAN.
- **IPMI Over KCS**: Check or uncheck the IPMI Over KCS interface which allows the user to perform IPMI communication over KCS.

> **NOTE**
> IPMI Communication will not be performed over LAN /KCS interface if it is disabled.

- **Save**: Click Save to save the confifigured interfaces



Chapter 7. Remote Control

The Remote Control page consists of the following options. A sample screenshot is displayed below.

- Launch H5Viewer
- Launch JViewer
- Launch Serial Over LAN

7.1 Launch H5Viewer

The system and browser requirements for Remote Control are given below.

System Requirements

- Client machine with 8GB RAM.
- If the client machine has 4GB 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).
- Edge
- Safari (On Mac only)

> **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 illegal character in a UNC path name. Thus, the use of IPv6 addresses is also illegal in UNC names.

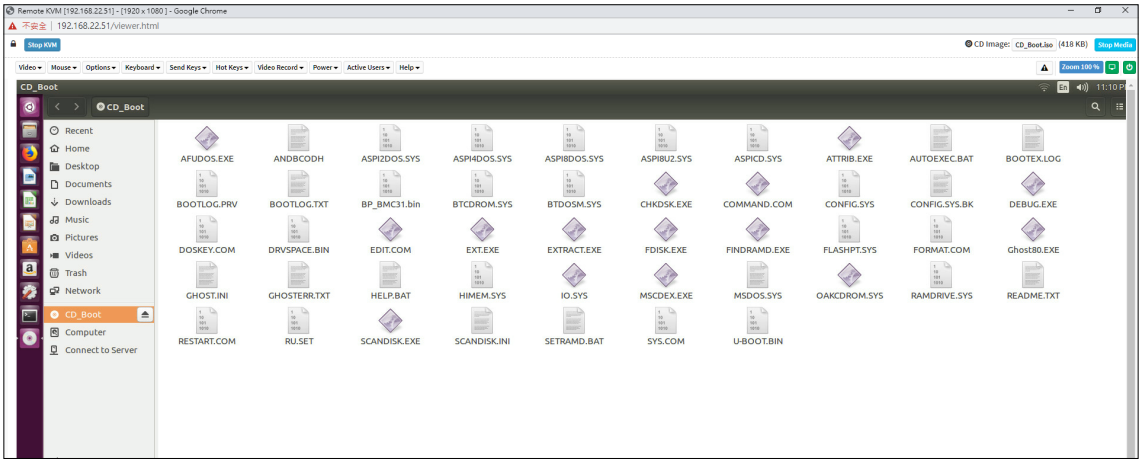
For this reason, in IE browser the IPV6 address should be given in "Literal IPv6 addresses in UNC path names" format.

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.

To open Remote Control page, click Remote Control from the menu bar.

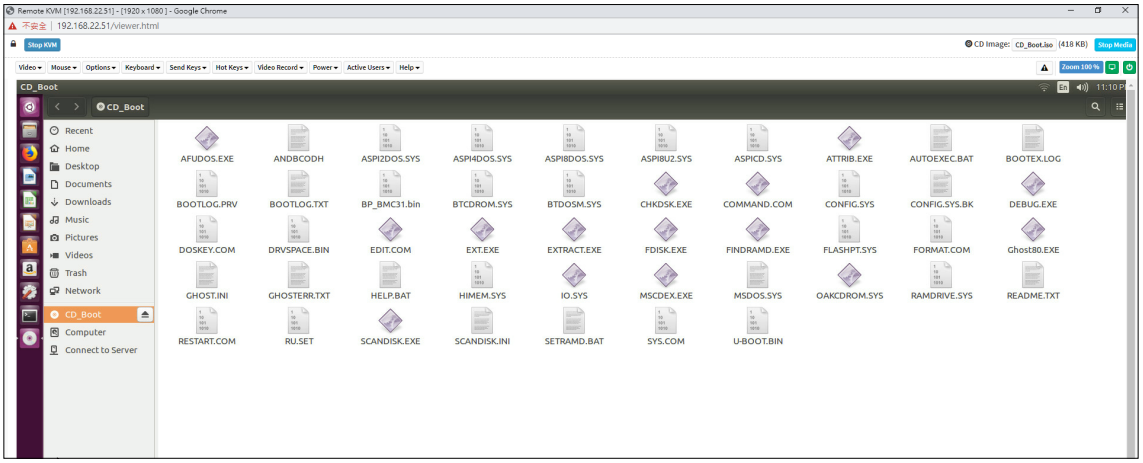
A detailed description of the menu items are given below.

Open the Remote Control page, click Launch H5Viewer. A sample screenshot of the Remote KVM page is shown below.



Procedure To Start KVM

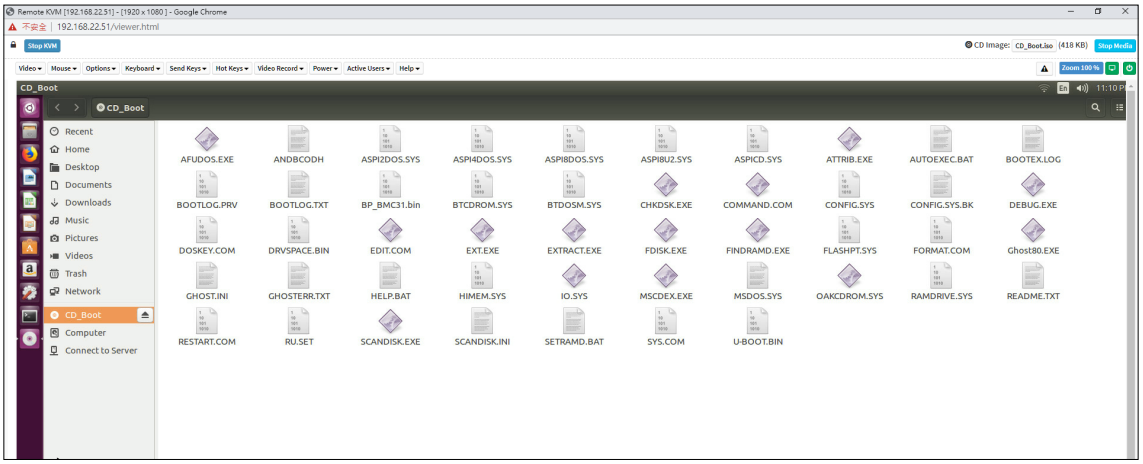
1. Click Launch H5Viewer to open the Remote Control KVM page. A sample screenshot of the Remote KVM page is shown below.



2. To stop the H5Viewer video redirection, click Stop KVM.

Procedure To Start / Stop Media

1. Click Browse to select CD Image.
2. Click Start Media to redirect the selected CD image file to the Host. A sample screenshot is as shown below.



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

A detailed description of the menu items are 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, 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. If you disable this option, the display will be back in the server screen.

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

Mouse

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

Mouse Mode: This option handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right to configure this option.

- Absolute mouse mode: The absolute position of the local mouse is sent to the server if this option is selected.
- Relative mouse mode: The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
- Other mouse mode: This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.

> **NOTE**
> AMI MegaRAC® SP-X suggests users to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse mode.

Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.

Options

Zoom:

Normal - By default this option is selected.
Zoom In - For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%
Zoom Out - For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%

Block Privilege Request: To enable or disable the access privilege of the user.

***Compression Mode**: This option helps to compress the Video data transfer to the specific mode.

***DTC Quantization Table**: This option helps to choose the video quality.

> **NOTE**
> *Specific to AST SOC.

Keyboard

Keyboard Layout: This feature is fully compatible when host and client has the same keyboard language layout. If the client and host language layouts differ, some special characters will not be compatible.

List of Host Physical Keyboard languages supported in SPX H5Viewer.

1. English U.S.
2. German.
3. Japanese.

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

- Hold Down
- Press and Release

Hold Down
This menu contains the following sub menu items.

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

Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection.

Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Press and Release

Ctrl+Alt+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection.

Context Menu Key: This menu item can be used to act as the context menu key, when in Console Redirection.

Print Screen Key: This menu item can be used to act as the print screen key, when in Console Redirection.

Hot Keys: This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.

This menu contains the following sub menu items.

•**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 record duration value should be in the range of 1 to 1800 seconds. Video Compression value should be in the range of 0.1 (Low image quality) to 0.9. (High image quality).

Normalized video resolution to 1024 X 768 (*Specific to AST SOC): 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 same resolution as host video. The host video capture depends on client system performance. If this option is disabled, recorded video file may have inconsistency. (i.e., Recorded video file duration may not be the same as configured value).

> **NOTE**
> The Maximum video file size allowed is around 40MB. If the video file size reaches its max 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.
>
> User 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 limitation, Set timeout/set interval will be delayed from specified time of interval when browser window loses focus, Hence video server will not send the video packets to H5View¬er and so the video recording will be stopped.

Power
The power options are to perform any power cycle operation. Click on the required option to perform the following operation.

Reset Server: To reboot the system without powering off (warm boot).

Immediate Shutdown: To perform Power OFF Immediately.

Orderly Shutdown: To Power OFF the sever in proper order.

Power ON Server: To Power ON the server.

Power Cycle Serve: To first power off, and then reboot the system (cold boot).

Active Users
Click this option to display the active users and their system ip address.

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

Help
Click this option to get more information About H5Viewer. The KVM Remote Console utility version and plugin version will be displayed.

Quick Buttons

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

Quick Buttons	Explanation
	This quick button will show/hide notifications dropdown menu, which will 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. If icon is in green color then host monitor is unlocked. If the icon is in red color host monitor is locked. By clicking the button host monitor status can be toggled.
	This quick button is used to display the current server power status. If the icon is in green color, the server status is powered on. If the icon is in red color, the server status is powered off. Click the button to toggle immediate power off/power on the host.

Status bar buttons

Num/Caps/Scroll lock buttons are LED status buttons that denotes the current status of Num/Caps/ Scroll lock in the host.

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

NOTE
Client Side Limitations
Due to web browser related security concerns, this feature has following limitations.
- Host LED status will be synced with client LED status, only if user presses any key in client keyboard when H5Viewer window is in focus.
- Client keyboard LED status cannot be updated from web browsers.

Host Side Limitations
- In some Linux hosts, when the host is booted into text mode, CAPS LOCK LED status will not be updated properly. CAPS LOCK LED won't turn ON/OFF while changing the CAPS lock status in the host OS.
- In such cases, H5Viewer CAPS LOCK synchronization functionality will not work properly.
- Example - Typing letters in H5Viewer (after pressing CAPS LOCK) will toggle between lower to upper case inside host.

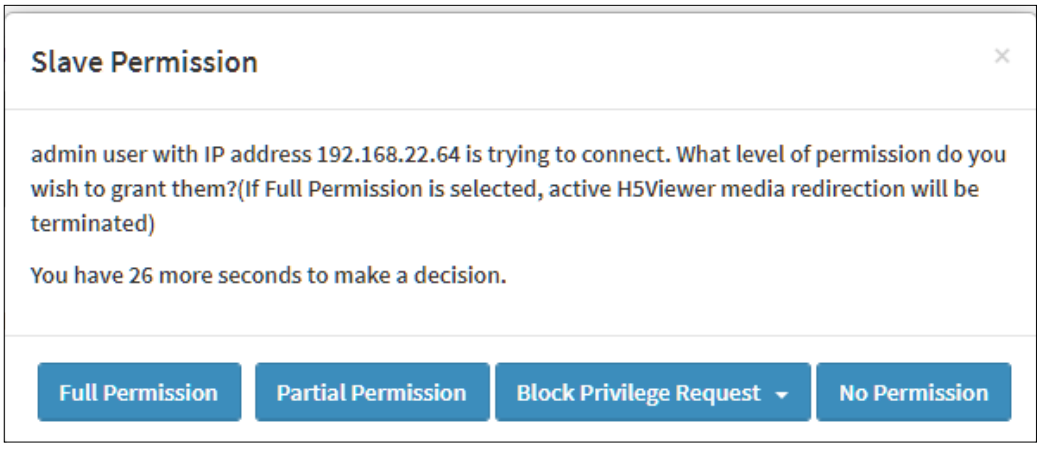
Control keys
This options provides the same functionality of Send Keys → Hold Down menu item. Select any of the menu item, it will highlight the corresponding status bar button in green color. Similarly by clicking the buttons will toggle the selection status of the corresponding menu item.

KVM Sharing
MegaRAC® SP-X stack supports "N" number of KVM Redirection sessions. Only one full permission JViewer/H5Viewer session at a time.

With Full permission in JViewer/H5Viewer, the user can control the KVM redirection, and the other JViewer/H5Viewer users can only view the video redirected from the server without intervention.

When the First user launches JViewer/H5Viewer, the user will get full permission to control the host during KVM redirection. When another JViewer/H5Viewer session is launched, the Video server will send 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/hostname and user name of the newly authenticated or logged in user, will be send to the current session. The first client shows the dialog as a shown below:



Clicking the button in the dialog box will trigger 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 newly requesting session and active partial privileged session will get partial permission as auto response and can only view server display. Further request will be served by auto response mechanism.

Block Privilege Request → No Permission: Once this option is selected, both newly requesting session and active partial privileged session access will be denied as auto response. Further request will be served by auto response mechanism.

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

7.2 Launch JViewer

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

> **NOTE**
> It is recommended to use openJDK 8 or any higher LTS version. Icedtea-Web launch application may work inconsistently when used JDK 11 or higher version. Web launch dialog may freeze and become unresponsive.
> Refer the link for further information.
> https://icedtea.classpath.org/wiki/IcedTea-Web#Filing_bugs
>
> In some earlier versions of JRE 1.7, TLS v1 protocol will be enabled by default. User needs to manually enable TLS v1.2 protocol support from Java configuration panel for proper JViewer functionality.

Procedure
To download the .jnlp file from BMC. To open the .jnlp file, use the appropriate JRE version (Javaws). When the downloading is done, it opens the Console Redirection window.
The Console Redirection menu bar consists of the following menu items.

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

A detailed explanation of these menu items are 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.

***DTC Quantization Table**: This option helps to choose the video quality.

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

> **NOTE**
> This Feature is only specific to Pilot and AST SOCs.

****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.

> **NOTE**
> * Specific to AST SOC. ** Specific to Pilot SOC.

Keyboard
This menu contains the following sub menu items.

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

Hold Right Alt Key: This menu item can be used to act as the right-side <ALT> key when in Console Redirection.

Hold Left Ctrl Key: This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.

Hold Left Alt Key: This menu item can be used to act as the left-side <ALT> key when in Console Redirection.

Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Right Windows Key: This menu item can be used to act as the right-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

Ctrl+Alt+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.

Context menu: This menu item can be used to act as the context menu key, when in Console Redirection.

Hot Keys: This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.

Full Keyboard Support: Enable this option to provide full keyboard support. This option is used to trigger the Ctrl and Alt key directly to host from the physical keyboard.

Mouse

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

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

****Show Host Cursor**: This option is used to enable or disable the visibility of the host cursor. Proper SOC specific video driver should be installed in the host for this feature to work.

> **NOTE**
> Remote KVM Supports Mouse move, left and right button clicks only.

Mouse Mode: This option handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right to configure this option.

- **Absolute mouse mode**: The absolute position of the local mouse is sent to the server if this option is selected.
- **Relative mouse mode**: The Relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
- **Other mouse mode**: This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation and accessing mouse in UEFI screen.

> **NOTE**
> AMI MegaRAC® SP-X suggests users to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse mode.
>
> Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.
>
> You can see client and host cursor in JViewer if mouse is moved faster/ in circle. Mouse sync will depend on so many factors like network, client machine video packet receive and rendering, BMC CPU utilization etc. In Normal use case scenario you will have mouse sync better compare to heavy video/stress testing. High resolution, media redirection(copy) will have directly impact in video rendering due to that client and host cursor can be viewed while moving the cursor.

To view the Supported Operating Systems for Mouse Mode, click Mouse Mode.

Options

Band width (Except Pilot SOC): 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 – For increasing the screen size. This zoom varies from 100% to 150% with an interval of 10%

Zoom Out – For decreasing the screen size. This zoom varies from 100% to 50% with an interval of 10%

Actual Size - By default this option is selected

Fit to Client Resolution - If the host screen resolution is greater than the client screen resolution, choose this option to fit the host screen to client screen. The host video will be scaled down and rendered in the KVM console. In this case, the host mouse cursor will appear smaller than the client mouse cursor. So the client and host mouse cursors might not be in perfect sync.

Fit to Host Resolution - If the host screen resolution is lesser than the client screen resolution, choose this option to resize the JViewer frame to the host resolution.

> **NOTE**
> This option can be configured from PRJ in MDS.

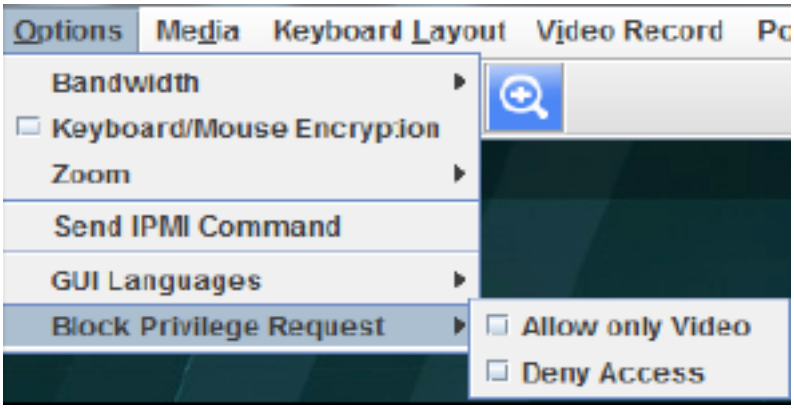
Send IPMI Command - This option opens the IPMI Command dialog. Enter the raw IPMI command in Hexadecimal field as Hexadecimal value and click Send. The Response will be displayed as shown in the screenshot below.

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 full permitted session.

> **NOTE**
> This menu option is available only for partially privileged session and Full permission sessions will not have this option in the menu.

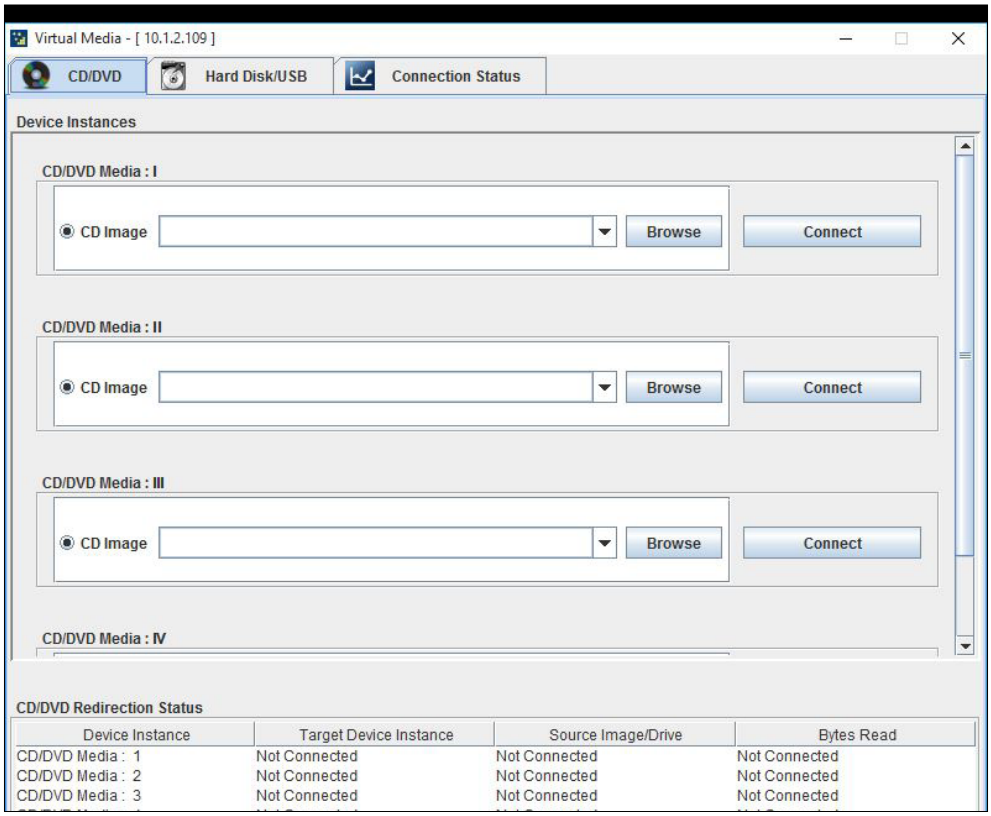
Block Privilege Request - Full privileged sessions can use this option to block incoming request from partial privileged sessions by setting an auto response as either “Allow only Video” or “Deny Access”.



> **NOTE**
> This menu option is available only for Full permission session 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, then 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, then 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.



NOTE
If there are two device panels for each device, and when you click the Connect button, then the redirected device panel will be disabled.

Unmounting device will make the driver disconnect 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.

NOTE
AST/PILOT4 SOC:- Configured number of devices will be emulated in Windows/ Linux Host.

Macintosh OS X Clients: The package XQuartz should be present in the Macintosh OS X clinet machines for the V-Media redirection to work. Otherwise it may lead to problems in loading the VMedia libraries. If the package is not already installed, download and install from the following link. https://www.xquartz.org/

Each of the supported devices is listed in a separate tab. Each tab in the application is described below.

CD/DVD Media: 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 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 “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 Windows client, if the logical drive of the physical drive is dismounted then 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 whole physical drive or individual logical drives.

For 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 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 whole physical drive.

For Hard disk image redirection, only the file extension is validated. The Harddisk/USB key device/ image will be redirected to the host as it is. The BMC will not validate the harddisk medium, 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, then 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, then the file can be opened and redirected.

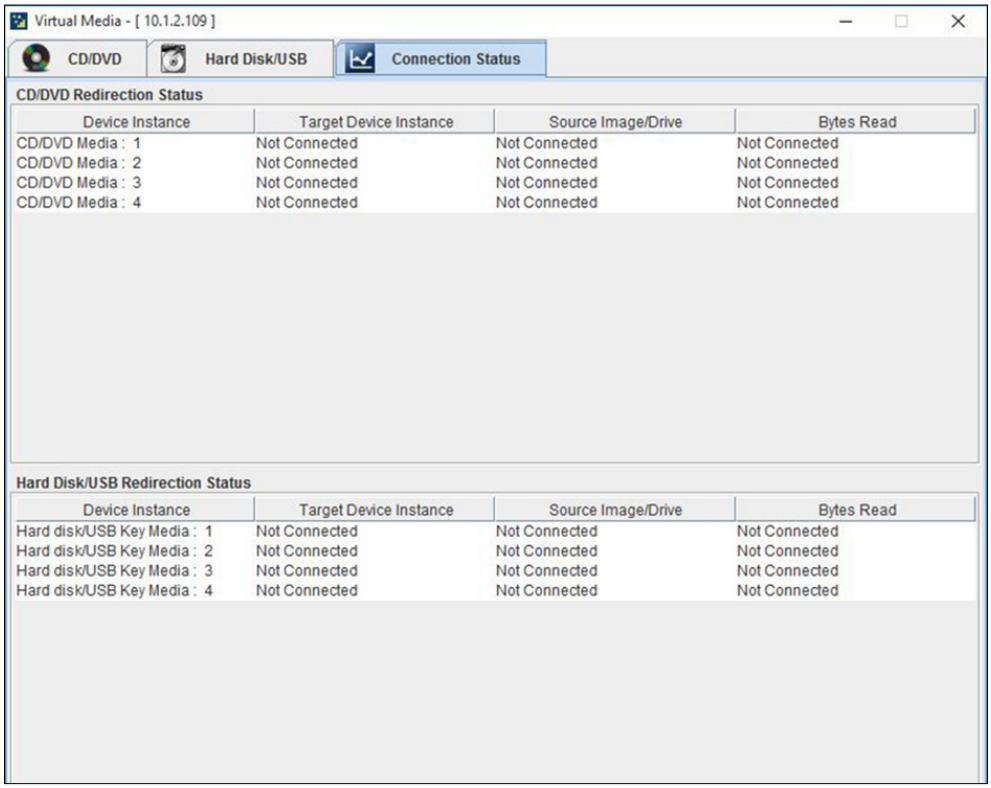
If the file is not visible in the file open dialog, the user shall mention the path of the image file in the file name field of the file open dialog and then open the image.

Continuously clicking connect/disconnect buttons without giving any delay in-between may cause failure in media redirection, since the host may take few seconds to connect/disconnect the media device.

SPX 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.

The connection status tab is shown below.



NOTE
VMedia Privilege only restricts initiating/starting media redirection. If a device is already being redirected and attached to the host, then in host it will be visible as normal device. Hence it will be accessible to all the KVM sessions. Which includes 'KVM Privilege only' sessions as well.

Keyboard Layout

Auto Detect: This option is used to detect keyboard layout automatically. If the client and host keyboard layouts are same, then for all the supported physical keyboard layouts, you must select this option to avoid typo errors. If the host and client languages differ, user can choose the host language layout in the menu and thereby can directly use the physical keyboard.

Physical Keyboard: This feature is fully compatible when host and client has the same keyboard language layout. If the client and host language layouts differ, some special characters will not be compatible.

- Host Platform: This feature contains two options Windows and Linux. When working with Windows host, Windows option should be selected. Similarly when working with Linux host, Linux option should be selected. This option should be selected properly for the Physical keyboard layout cross mapping to work properly. By default, Windows will be selected.

List of Host Physical Keyboard languages supported in SPX JViewer.

1. English –US
2. English – UK
3. French
4. French (Belgium)

5. German (Germany)
6. German (Switzerland)
7. Japanese
8. Spanish
9. Italian
10. Danish
11. Finnish
12. Norwegian (Norway)
13. Portuguese (Portugal)
14. Swedish
15. Dutch (Netherland)
16. Dutch (Belgium)
17. Turkish – F
18. Turkish – Q

Soft Keyboard: This option allows you to select the keyboard layout. It will show the dialog as similar to Windows On-screen keyboard. If the client and host languages are different, you can select the soft keyboard that corresponds to the host keyboard layout from the list shown in JViewer, and use it to avoid typo errors.

> **NOTE**
> Different Linux systems follow different keyboard layouts. So the softkeyboard displayed uses standard windows keyboard layout irrespective of the host OS.

We have list of List of Soft Physical Keyboard languages supported in SPX JViewer.

1. English –US
2. English – UK
3. Spanish
4. French
5. German (Germany)
6. Italian
7. Danish
8. Finnish
9. German (Switzerland)
10. Norwegian (Norway)
11. Portuguese (Portugal)
12. Swedish
13. Hebrew
14. French (Belgium)
15. Dutch (Netherland)
16. Dutch(Belgium)
17. Russian (Russia)
18. Japanese (QWERTY)
19. Japanese (Hiragana)
20. Japanese (Katakana)
21. Turkish – F
22. Turkish – Q

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

Video Record

Start Record: This option is to start recording the screen.

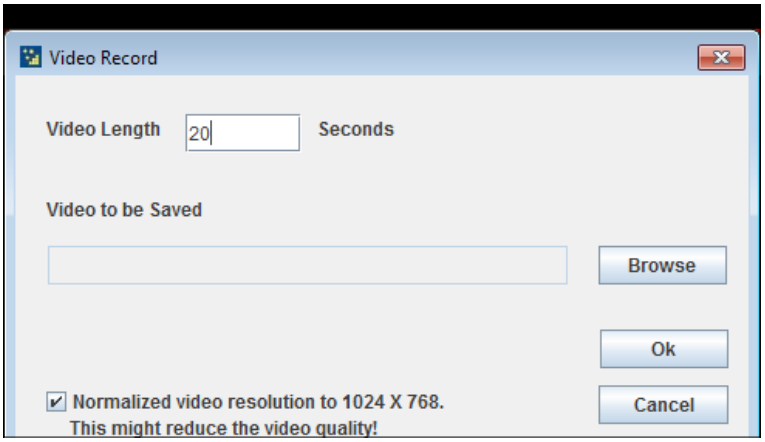
Stop Record: This option is used to stop the recording.

Settings: To set the settings for video recording.

Procedure

> **NOTE**
> Before you start recording, you have to enter the settings.

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



2. Enter the Video Length in seconds.
3. Browse and enter the location where you want the video to be saved.
4. Enable the option Normalized video resolution to 1024X768.
5. Click OK to save the entries and return to the Console Redirection screen.
6. Click Cancel if you don't wish to save the entries.
7. In the Console Redirection window, click Video Record → Start Record.
8. Record the process.
9. To stop the recording, click Video Record → Stop Record.

Power

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

Reset Server : To reboot the system without powering off (warm boot).

Immediate Shutdown : To immediately power off the server.

Orderly Shutdown : To initiate operating system shutdown prior to the shutdown.

Power On Server : To power on the server.

Power Cycle Server : To first power off, and then reboot the system (cold boot).

Active Users

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

Help

JViewer: Displays the copyright and version information.

Quick Buttons

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

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

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

Keyboard LED Sync

When the JViewer is launched from a client machine, the keyboard locks status and LEDs denoting the lock status, in the host machine should be in sync with that in the client machine. That is if the Num/Caps/Scroll lock is enabled in the host, the same should be enabled in the client machine as well.

The host keyboard LED status will be synced with the client keyboard, the lock indicators in the JViewer status bar, and the JViewer Softkeyboard.

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 Softkeyboard lock status will sync with the host keyboard LED status.

In the case of latest Linux distributions used as host, the keyboard LED sync will not work if the lock status is changed using the host physical keyboard directly. However the synch will work if the LED status is changed using the onscreen keyboard available in the host OS.

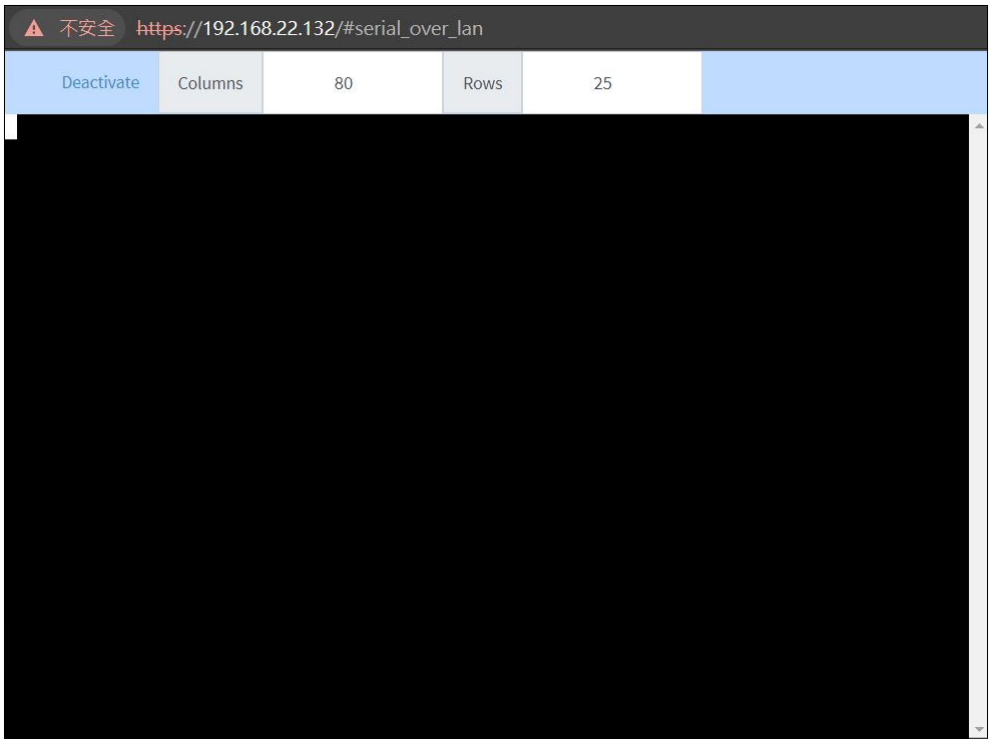
Open a child dialog in JViewer will cause the focus shift out of JViewer. The client keyboard's LED status before launching JViewer, or the JViewer gains focus, will be set back to the client in this case.

7.3 Launch Serial Over LAN

Serial Over LAN (SOL) is a mechanism that enables the input and output of the serial port for a managed system to be redirected over IP; In this feature, Serial data is transmitted to HTML5 Web UI through websocket.
To activate SOL Support, follow the below procedures.

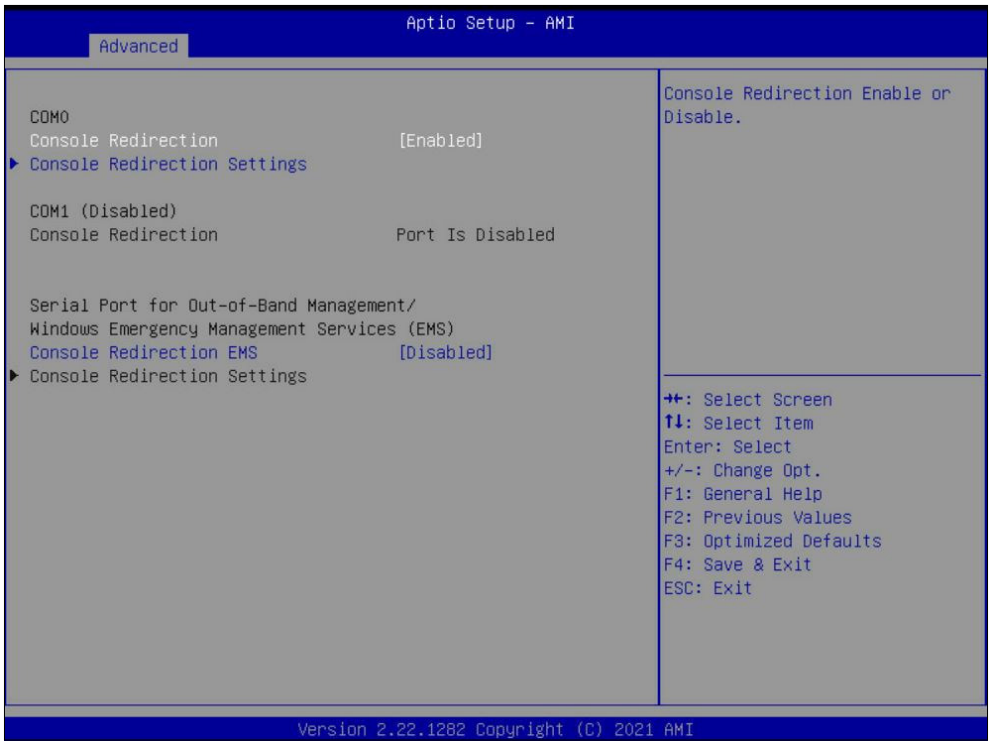
1. Click **Remote Control** from the Menu Bar. A sample screenshot of Remote Control page is shown as below.

2. Click **Activate** to activate SOL. A blank screen will appear as shown below.

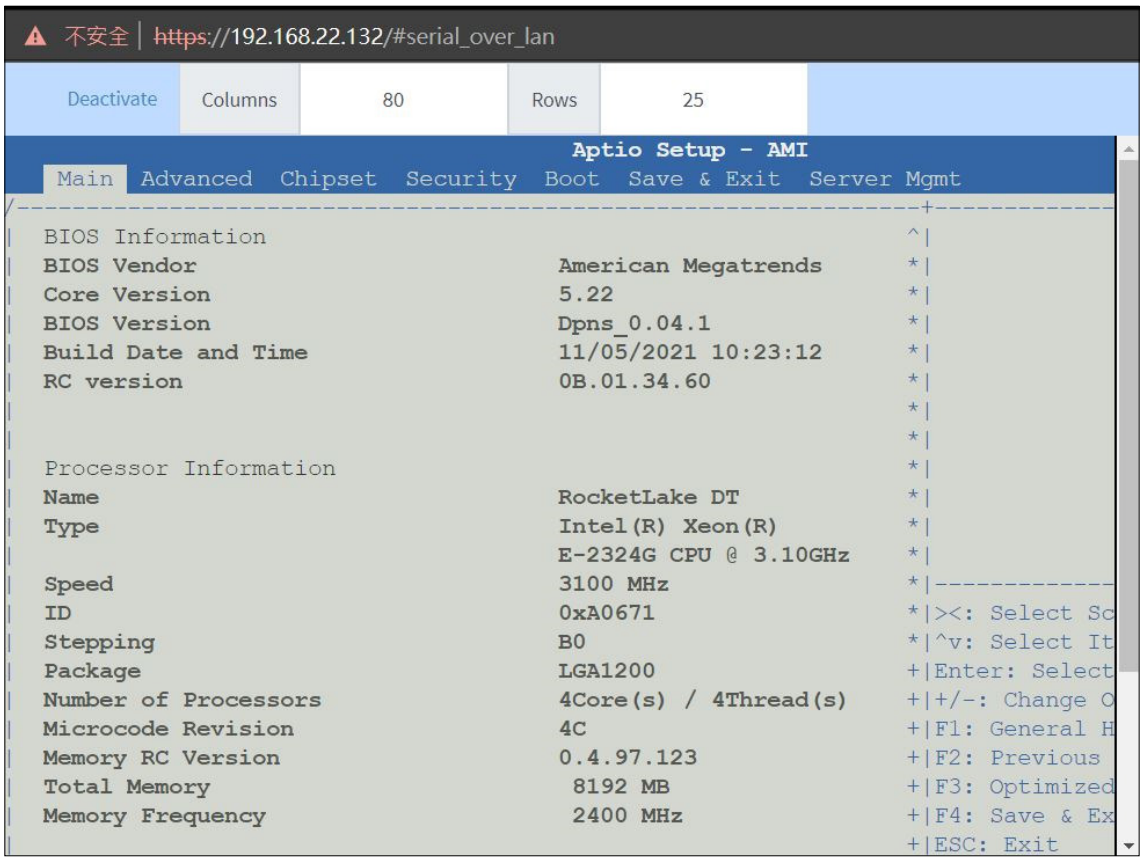


3. Enable serial port console redirection in BIOS setup page as below screenshot. Then select [Enabled] in COM0 Console Redirection. Press **F4** key to save confirmation and exit.

   Page path in BIOS: Advanced → Serial Port Console Redirection



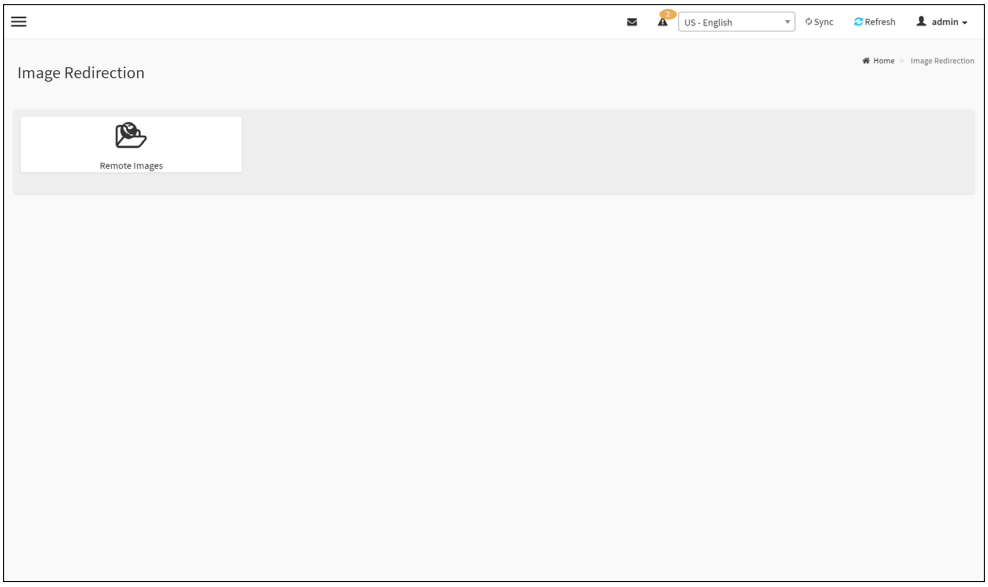
4. The serial over LAN screen will show the data from COM0.



Chapter 8. Images Redirection

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

To open Images Redirection page, click Images Redirection from the menu bar. A sample screenshot of Images Redirection page is shown below.

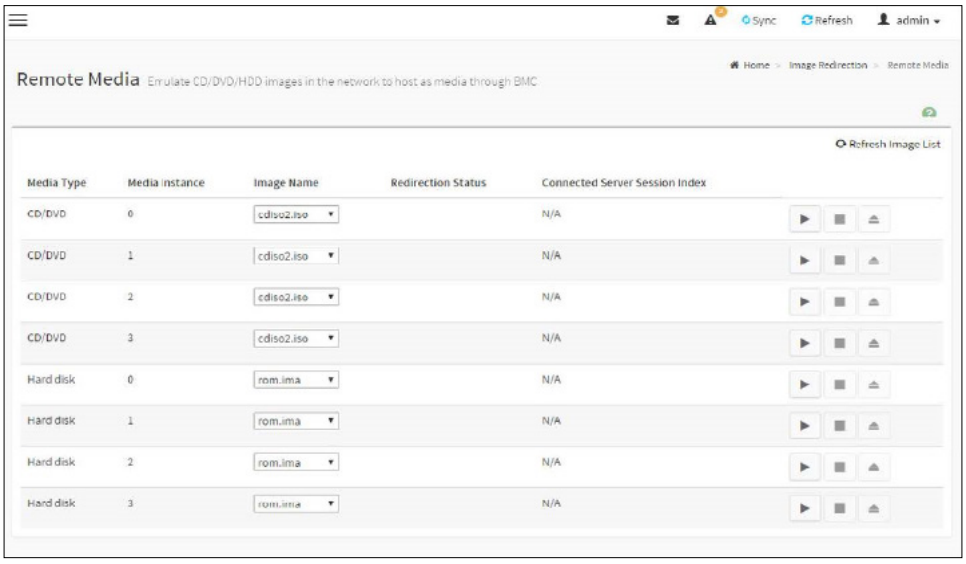


The fields of Images Redirection page are explained below.

- Remote Images

8.1 Remote Image

The displayed table shows configured images on BMC. You can configure images of the remote media server.



NOTE
More than one image can be configured for each image type. At maximum 4 images can be configurable.
To configure the image, You need to enable Remote Media support under Settings → Media Redirection → General Settings.
To start/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).

The fields of Remote Media tab are as follows:

Multiple Image support in Image Redirection

Media Type: Displays type of Media such as CD/DVD and Harddisk.

Media Instance: Displays total media instance count.

Image Name: Displays the default recovery image name on the server.

Status: Displays the status of the media.

Session Index: Displays Media Server Session Index.

Start/Stop Redirection: To start or stop Media redirection.

Pause: To Pause the Media redirection.

Refresh Image List: To get latest Image lists from the Remote Storage.

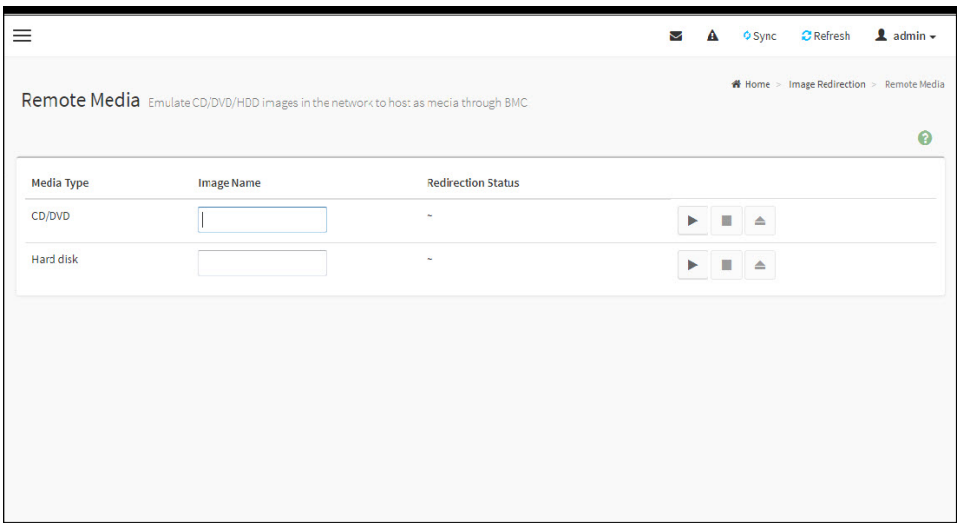
Procedure:

1. To Start/Stop Redirection and configure Remote media images, click ▶ (Start/Stop icon) and make sure Remote Media Support option is enabled.
2. Select a configured slot and click ▶ (Start/Stop icon) to start the Remote media redirection. It is a toggle button, if the image is successfully redirected, then click (Start/Stop icon) to stop the Remote media redirection. If you want to pause the Remote media Redirection, click ■ (Pause icon).

   NOTE
   Redirection needs to be stopped to clear the image.

3. To clear an image status, select an image and click (⏏) (Clear icon) to clear image status from the device.
4. Click Refresh Image list to get latest Image lists from the Remote Storage. The Latest Image Names list will be displayed in the Image Name drop-down list.

Single Image support in Image Redirection



NOTE
Only Single image can be configured for each image type.

To configure the image, You need to enable Remote Media support under Settings → Media Redirection → General Settings.

To start/stop redirection and to delete an image, you must have Administrator Privileges.

Free slots are denoted by "~".

The fields of Remote Media tab are as follows:

Media Type: Displays type of Media such as CD/DVD and Harddisk.

Image Name: Enter the default recovery image name on the server.

Redirection Status: Displays the status of the media.

Start/Stop Redirection: To start or stop Media redirection.

Pause: To Pause the Media redirection

Procedure:

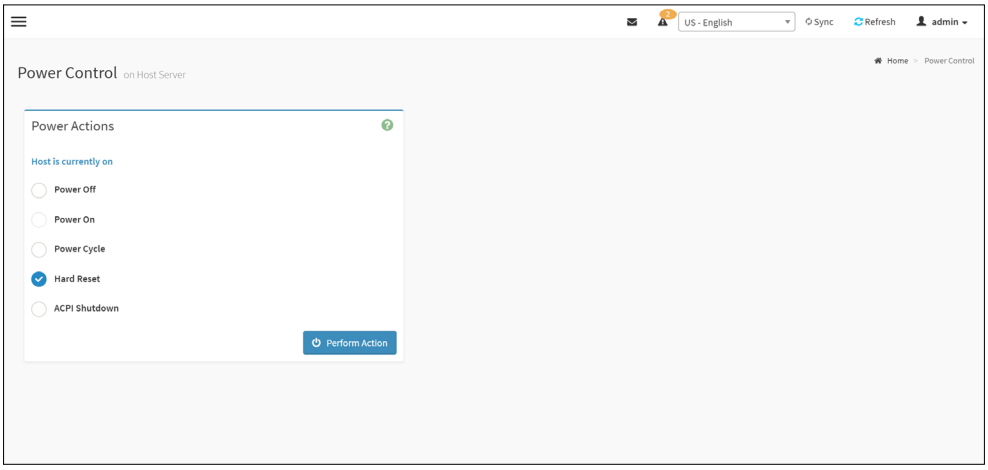
1. To Start/Stop Redirection and configure Remote media images, click ▶ (Start/Stop icon) and make sure Remote Media Support option is enabled.
2. Select a configured slot, and Enter the default recovery image name on the server in the Image Name text field.
3. Click ▶ (Start/Stop icon) to start the Remote media redirection. It is a toggle button, if the image is successfully redirected, then click ▶ (Start/Stop icon) to stop the Remote media redirection. If you want to pause the Remote media Redirection, click ■ (Pause icon).

NOTE
Redirection needs to be stopped to clear the image.

4. To clear an image status, select an image and click (⏏) (Clear icon) to clear image status from the device.

Chapter 9. Power Control

This page allows you to view and control the power of your server.
To open Power Control, click Power Control from the menu bar. A sample screenshot of Power Control is shown below.



The various options of Power Control are given below.

Power Off: To immediately power off the server.

Power On: To power on the server.

Power Cycle: This option will first power off, and then reboot the system (cold boot).

Hard Reset: This option will reboot the system without powering off (warm boot).

ACPI Shutdown: This option to initiate operating system shutdown prior to the shutdown.

Perform Action: Click this option to perform the selected operation.

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

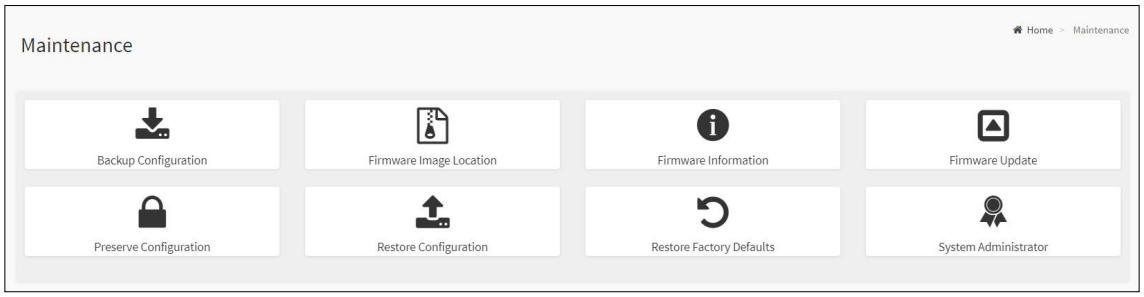
> **NOTE**
> During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

Chapter 10. Maintenance Group

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

- Backup Configuration
- Firmware Image Location
- Firmware Information
- Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- System Administrator

A sample screenshot of Maintenance page is displayed below.

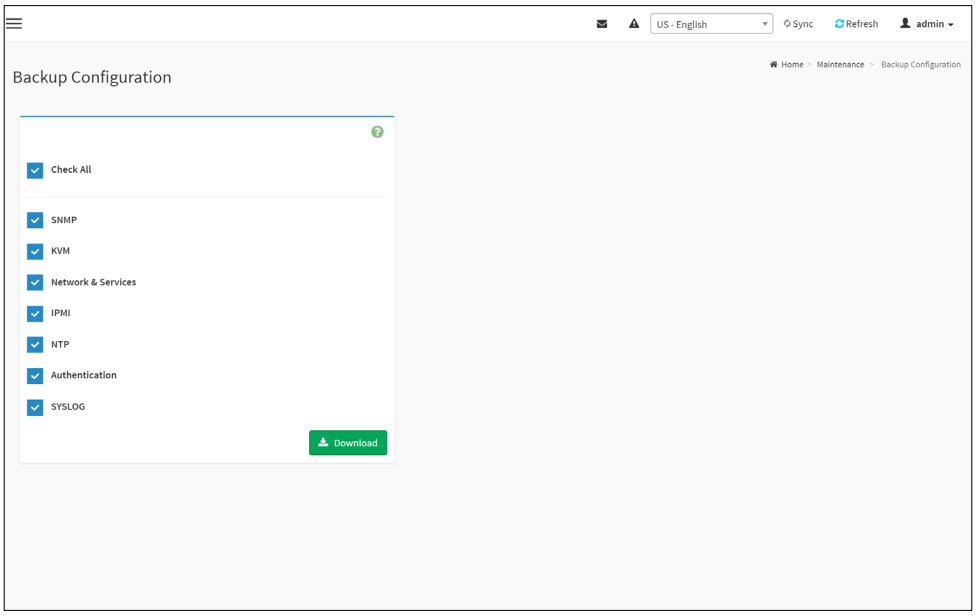


A detailed description is given below.

10.1 Backup Configuration

This page allows you to select the specific configuration items to be backup in case of “Backup Configuration”.

To open Backup Configuration page, click Maintenance → Backup Configuration from the menu bar. A sample screenshot of Backup Configuration page is shown below.



The various fields of Backup Configuration page are given below.

Check All - To select all the configuration list.

Download Config - To downlaod and save the configuration files backup from BMC to client system.

> **NOTE**
> During backup, because of security concern, the mechanism parses sensitive data to filter it out and not backup sensitive files. User has to set password again after restoring configuration by using default user in case of login failure.

Procedure for Backup Configuration:

1. Click Check All to backup all the configuration items or check the configuration that needs to be backup. The Backup Configuration page will appear as shown in the above screenshot.

> **NOTE**
> Network configurations are inter-related to IPMI, and hence by default IPMI configurations will be selected automatically when you select “Network and Services” to be backed up.

2. Click Download Config to save the backup file to the client system.
3. Click OK to perform the backup action. The Backup file will be saved in the client system.
4. Click Cancel to cancel the backup process.

> **NOTE**
> If select sd/emmc for backup conf space, has to create /confbkup folder in sd/emmc parti¬tion before backup.

TFTP server configuration
The TFTP server configuration is used for exporting the backupfile.

> **NOTE**
> Ensure that no other TFTP servers are enabled, if so remove all other servers with all con- figuration files. Login as “super” user means “root” user.

Procedure to make the default tftp server

1. Install the application which are needed.
   >apt-get install xinetd tftp tftpd
2. Edit the configuration file for TFTP.

   >vi /etc/xinetd.d/tftp

Edit the file as below:

```
service tftp
{
protocol = udp
port = 69
socket_type = dgram
wait = yes
user = nobody
server = /usr/sbin/in.tftpd
server_args = <DIR to which the file to be access>
disable = no
}
#EOF
#example:server_args = /tftpboot
```

> **NOTE**
> No arguments to be passed to the server_args other than directory.

```
########################################
```

>vi /etc/xinetd.conf

Add to the file :

```
defaults
{
# Please note that you need a log_type line to use log_on_success
and log_on_failure.
```

The default is the following :

```
# log_type = SYSLOG daemon info
}
includedir /etc/xinetd.d
########################################
```

3. Restart the server.
   >/etc/init.d/xinetd restart

4. Give permission to the file to access by all.
   >mkdir <DIR>
   >chmod -R 777 <DIR>
   >chown -R nobody <DIR>

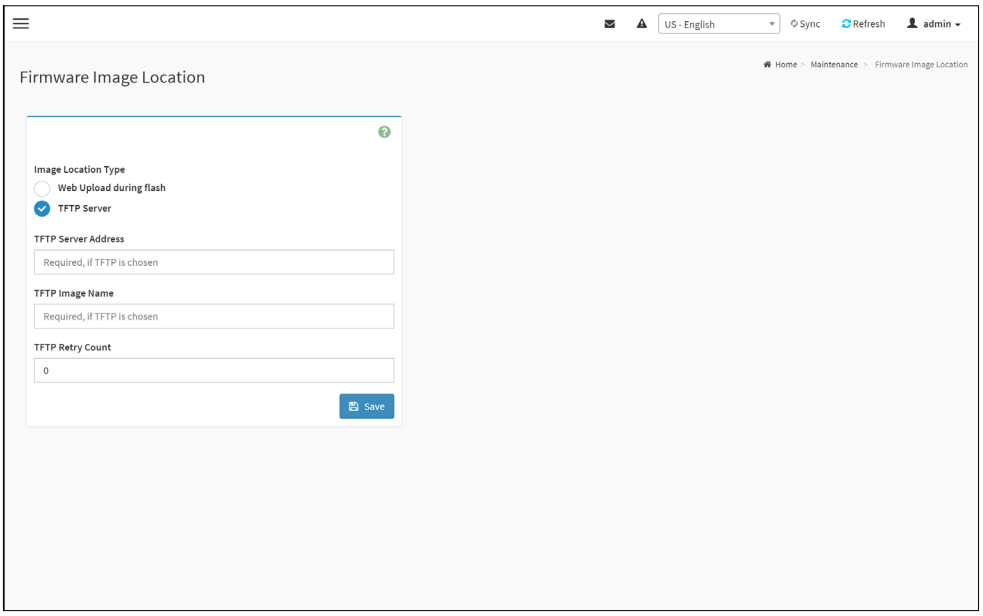
For Example:
   mkdir /tftpboot
   chmod -R 777 /tftpboot
   chown -R nobody /tftpboot

5. To receive the file you have to touch the file and give permission to access by all users
   > touch <DIR>/conf.bak
   > chmod 777 <DIR>/conf.bak

6. Even after all this step has been done and still facing error of timeout:
   a. Check with /etc/xinetd.d/tftp file and uncomment the EOF(Remove the '#' before the EOF alone).
   b. Restart the server.

10.2 Firmware Image Location

This page is used to configure firmware image into the BMC.
To open Firmware Image Location, click Maintenance → Firmware Image Location from the menu bar. A sample screenshot of Firmware Image Location page is shown below.



The various options of Image Transfer Protocol are given below.

Image Location Type: Type of location to transfer the firmware image into the BMC either Web Upload during Flash or TFTP Server.

TFTP Server Address: Address of the server where the firmware image is stored.

> **NOTE**
>
> The Server supports both IPv4 and IPv6 addresses
> - IP Address made of 4 numbers separated by dots as in “xxx.xxx.xxx.xxx”.
> - Each number ranges from 0 to 255.
> - First number must not be 0.
> - IPv6 Address made of 8 groups of 4 Hexadecimal digits separated by colon as in “xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx”.
> - Hexadecimal digits are expressed as lower-case letters.

TFTP Image Name: Full Source path with file name of the firmware image is stored on TFTP Server.

TFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.

Save: To save the configured settings.

Procedure

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

10.3 Firmware Information

This page is used to configure the Firmware Information settings.
To open System Administrator page, click Maintenance → Firmware Information from the menu bar. A sample screenshot of Firmware Information page is shown below.

The various fields of Firmware Information page are given below.

Build Date: Describes the Build Date of the active BMC image.

Build Time: Describes the Build Time of the active BMC image.

Firmware version: Describes the Firmware version of the active BMC image.

Firmware name: Describes the Firmware name of the active BMC image.
Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.

10.4 Firmware Update

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

> **NOTE**
> Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled in the middle of the wizard, the device will be reset.

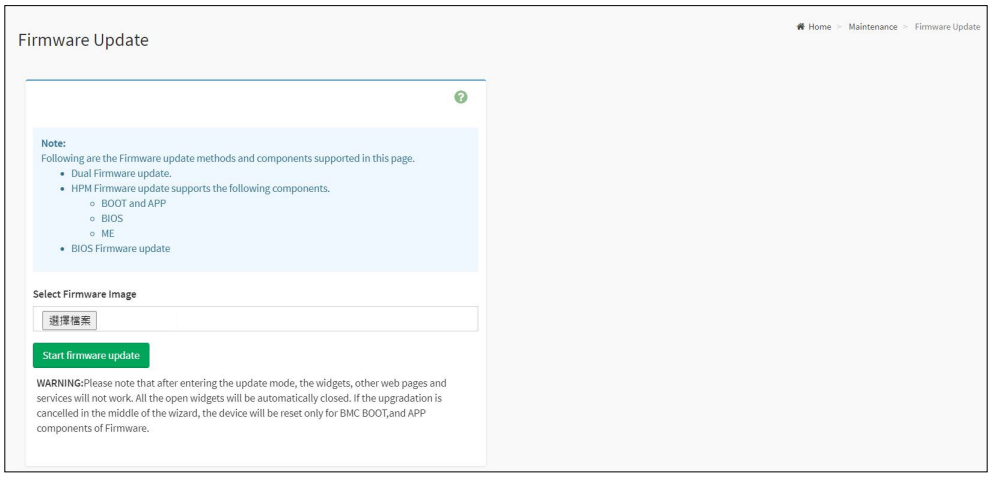
> **NOTE**
> The firmware upgrade process is a crucial operation. Make sure that the chances of a power or con¬nectivity loss are minimal when performing this operation.
> Once you enter into Update Mode and choose to cancel the firmware flash operation, the Mega¬RAC® card must be reset. This means that you must close the Internet browser and log back onto the MegaRAC® card before you can perform any other types of operations.
>
> Once Firmware upgrade using web is started, the regular IPMI command will not be allowed for safety concern if Enable IPMI Command handling during flashing support is disabled in project configuration.

To configure, choose Firmware Image Location under Maintenance. To open Firmware Update page, click Maintenance → Firmware Update from the menu bar.

Procedure
1. Click Browse to select firmware image.

> **NOTE**
> A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.

2. Click Start firmware update to load the Firmware Update information. A sample screenshot is displayed below.



> **NOTE**
> SignImage Public Key is feature based option. If encrypted Signimage feature is enabled, then support to Upload a public.pem key info option will be available.

Dual Firmware Update

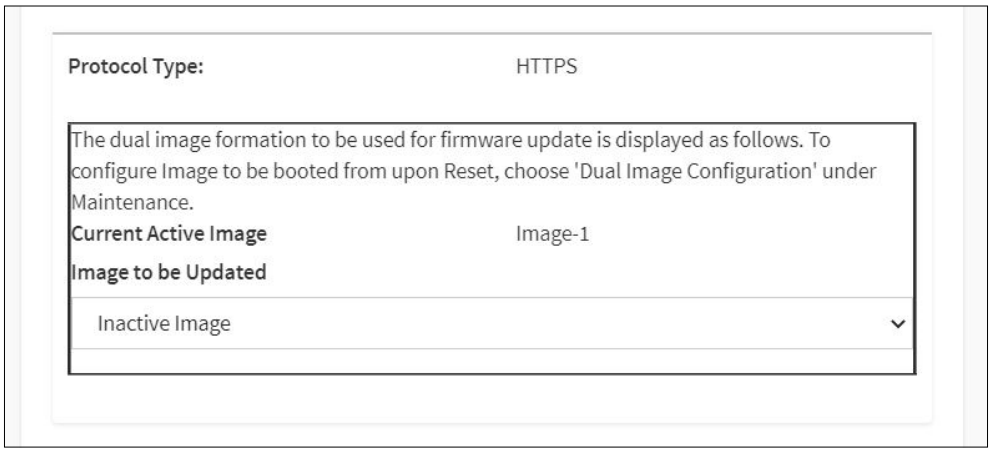
To perform Dual Firmware Update operation, click Maintenance → Firmware Update from the menu bar.

Procedure

1. Click Browse to select firmware image.

> **NOTE**
> A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.

2. Click Start firmware update to load the Firmware Update information. A sample screenshot is displayed below.

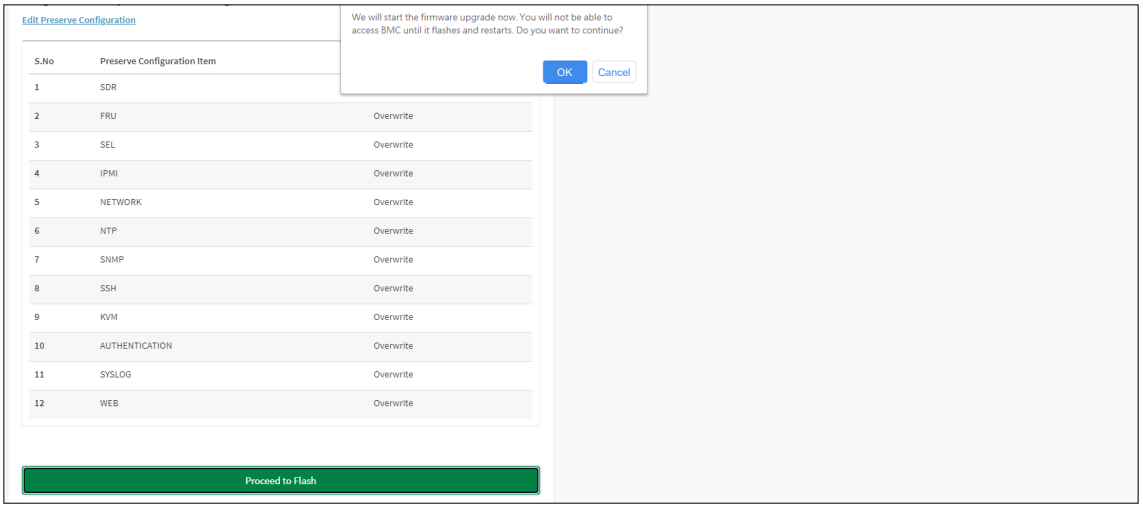


3. Select an Image (Inactive Image, Image 1, Image 2 or Both Image) from Image to be Updated drop-down list. The selected image will be getting flashed.
   - **Image to be Updated**: To update an Image (Inactive, Image 1, Image 2 or Both) to be flashed. If You select an Inactive image, the Inactive image will be flashed. If you select both images, then Both Image 1 and Image 2 will be flashed with uploaded image file.
   - **Reboot the device after update**: This option is used to reboot the device after the firmware update,
4. Click Preserve all Configuration to preserve all configuration.
   - **Preserve all Configuration**: To preserve all configuration.
   - **Edit Preserve Configuration**: To modify the Preserve status settings.

This wizard takes you through the process of AMI based firmware upgradation. The protocol information to be used for firmware image transfer during this update is as follows.

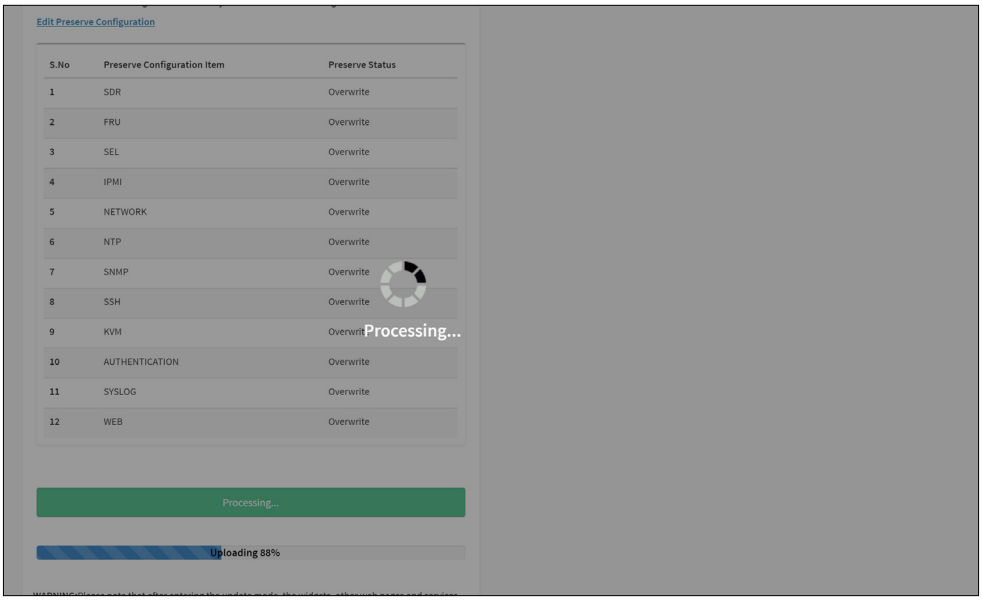
> **NOTE**
> All configuration items will be preserved/overwrite as default during the restore configuration operation.

5. Click Proceed to Flash, it will prompt you with the warning message. Click Ok to start the Firmware update.



6. The Firmware update undergoes the following steps:
   a. Closing all active client requests
   b. Preparing Device for Firmware Upgrade
   c. Uploading Firmware Image.

A sample screenshot is shown as below.



d. Verifying Firmware Image

In Section Based Firmware Update, you can configure the firmware image for section based flashing. Check the required sections and click Proceed to update the firmware.

If flashing is required for all images, select the option Full Flash .

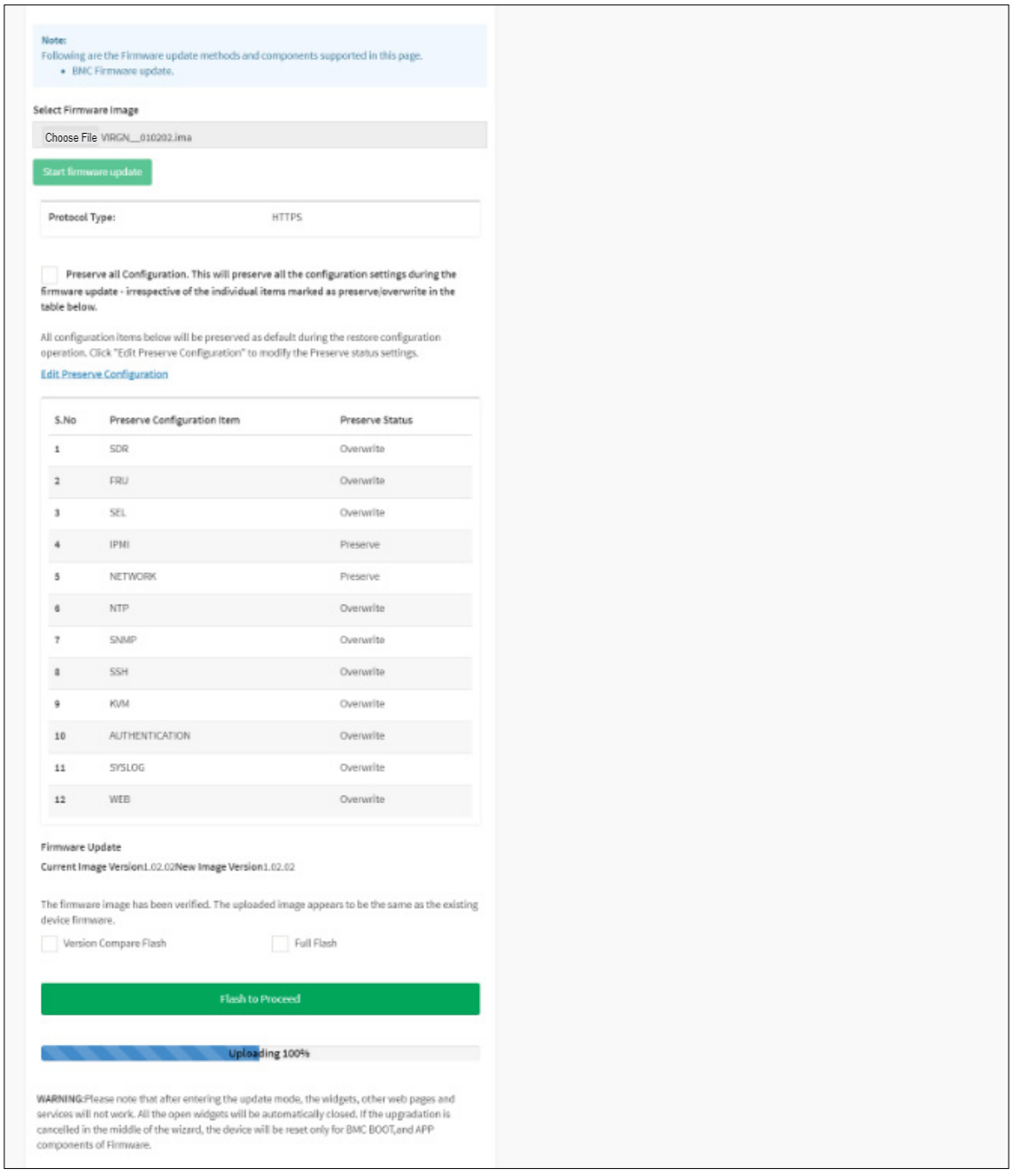
If you select Version Compare Flash option from web, the current and uploaded module versions, FMHlocation, size will be compared.

If the modules differ in size and location, proceed with force firmware upgrade.

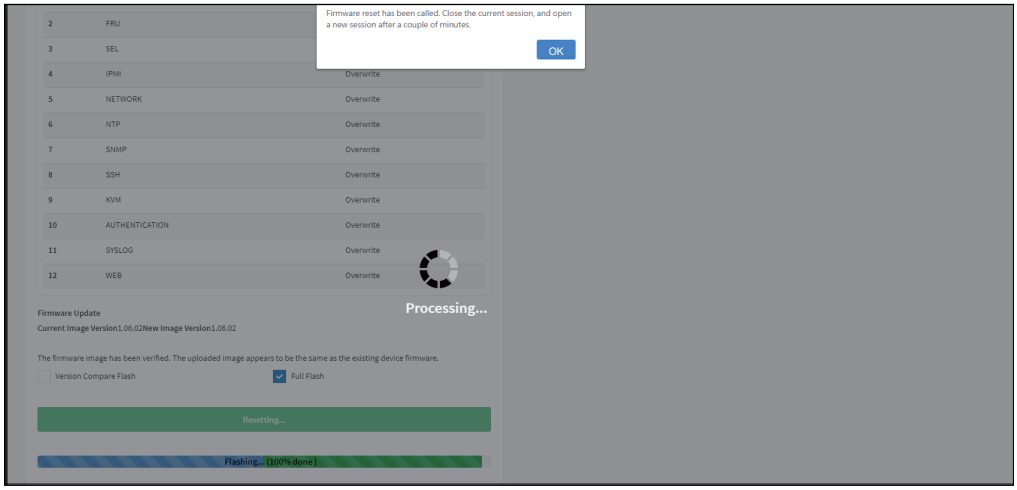
If all the module versions are same, restart BMC by saying all the module versions are similar.

If only few module versions are differ, those module will be flashed.

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



e. Flashing Firmware Image
f. Resetting the image. The sample screenshot of Firmware update is as shown below.

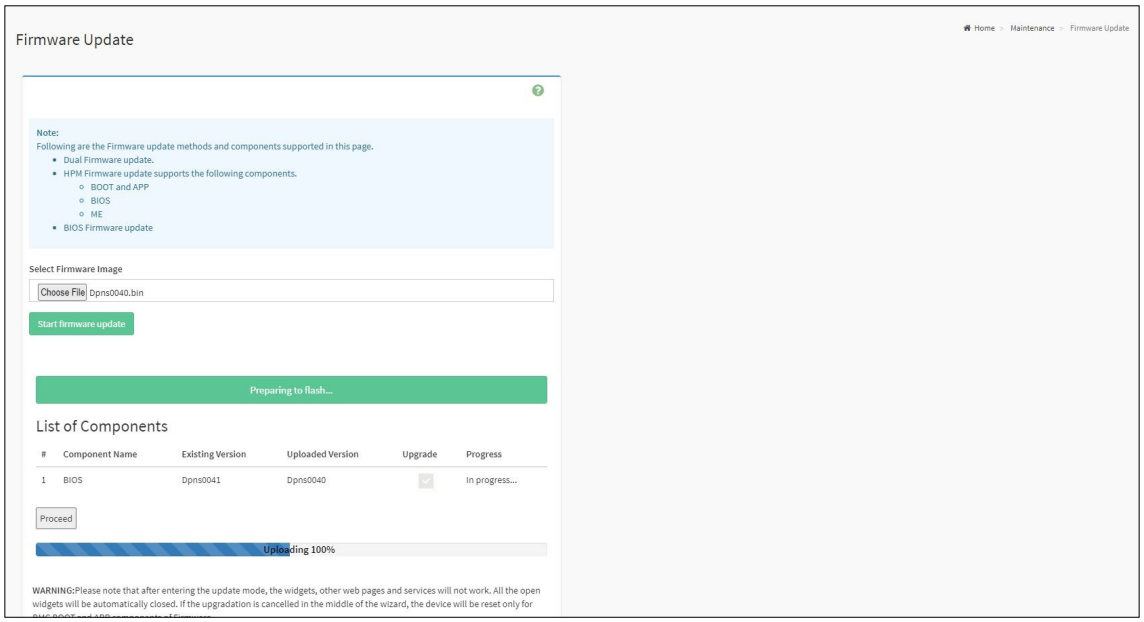


NOTE
The Firmware Update page will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the in¬structions presented in the subsequent pages to successfully update the card's firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

10.5 BIOS Firmware Update

This wizard takes you through the process of BIOS firmware upgradation.

To perform BIOS Firmware Update operation, click Maintenance → Firmware Update from the menu bar. A sample screenshot is displayed below.



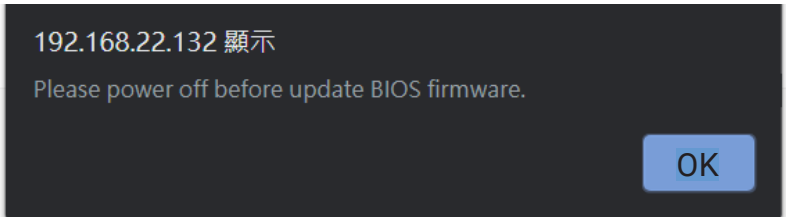
Procedure

1. Click Browse to select BIOS Firmware image.

> **NOTE**
> Firmware update wizard will detect .bin extension as BIOS firmware image.

2. Click Start Firmware Update to load the BIOS firmware image information. A sample screenshot is displayed below.

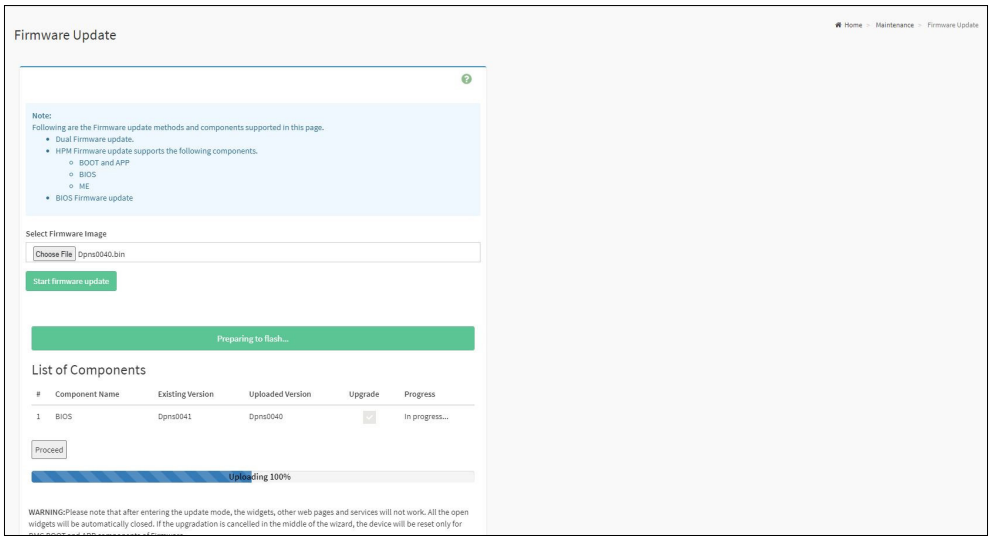
> **NOTE**
> Once you enter Firmware update page, an alert message will pop up if the system is on. The wizard will activate the update process after the user powers off the system.



3. Click Proceed, it will prompt you with the warning message. Click Ok to start the firmware update.

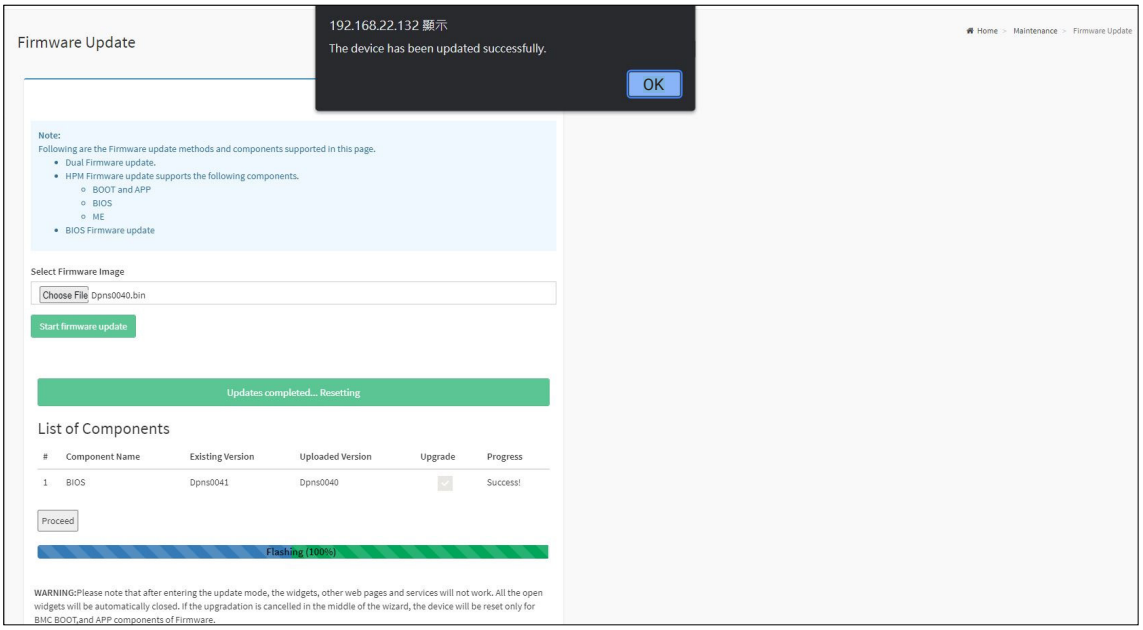
4. The BIOS Firmware Update undergoes the below steps.
    a. Uploading Firmware Image
    b. Getting BIOS existing and uploaded versions (BIOS Tag)
    c. Flashing Firmware Image

A sample screenshot is displayed below.



NOTE
The BIOS Firmware Update page will be disabled and this action will not allow the user to perform any other tasks until firmware upgrade is completed.

Once the BIOS firmware update is completed, it will prompt you with the success message. Click OK to complete the process. A sample screenshot is displayed below.

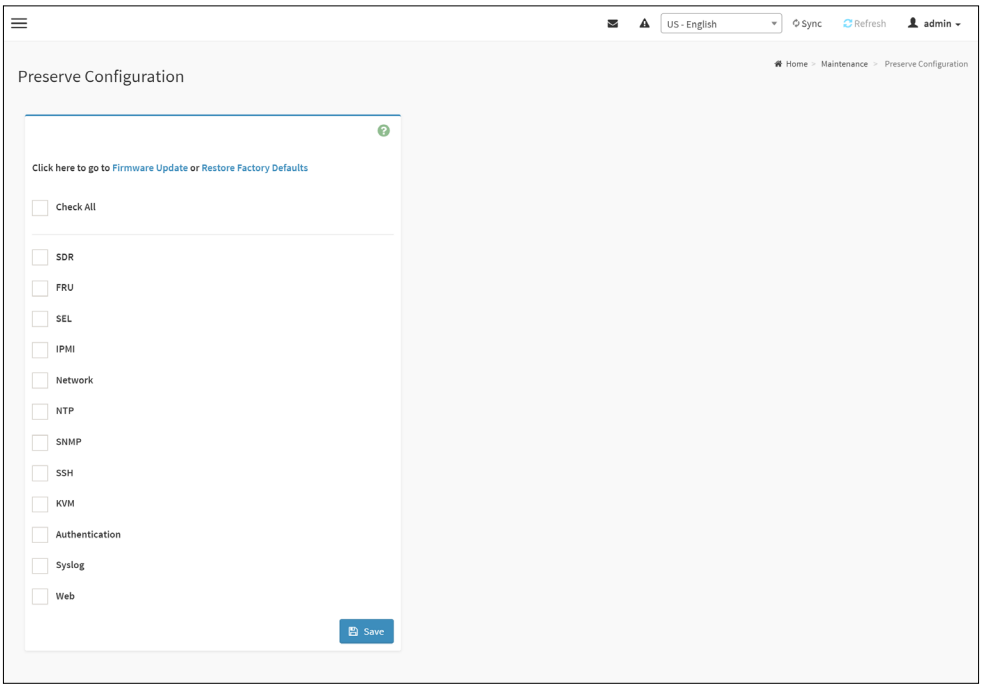


NOTE
You will not be able to perform any other tasks until firmware upgrade is completed and the device is off.

10.6 Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to preserve the existing configuration without overwriting with defaults/ Firmware Upgrade configuration.

To open Preserve Configuration page, click Maintenance → Preserve Configuration from the menu bar. A sample screenshot of Preserve Configuration page is shown below.



NOTE
You can navigate to the Firmware Update page and Restore Factory Defaults by clicking the respective links.

The various fields of Preserve Configuration are as follows.

Click here to go to Firmware Update or Restore Configuration: This link will redirect to the Firmware Update or Restore Configuration page which needs to be preserved.

Check All: To check the entire configuration list.

Save: To save any changes made.

NOTE
This configuration is used by Restore Factory Defaults process.

Files Preserved

SDR

Following files will be preserved.

SDR.dat: This file contains the sensor data record information that is used in IPMI.

Dependency Configurations - NIL

FRU

Following files will be preserved.

FRU.bin: This file contains the logical field replaceable unit data that are used by IPMI

Dependency Configurations - SDR

SEL

Following files will be preserved when Delete SEL reclaim space is disabled. SEL.dat: This file contains the system event logs that are being logged by the IPMI. Following files will be preserved when Delete SEL reclaim space is enabled.

Selreclaiminfo.ini – The file contains the SEL repository information.

SEL folder – This folder contains the multiple files of event logs.

Dependency Configurations – IPMI

IPMI

The following files are preserved in IPMI configuration.

IPMI.conf: This file contains the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.

dcmi.conf: This file contains the DCMI1.5 specification parameters such as DHCP Timing1, DHCP Timing2, DHCP Timing3. The files are preserved only when DCMI1.5 feature is enabled in the MDS project configuration.

pwdEncKey: This file contains the keys that are used to decrypt the passwords. When the user password option is enabled in the MDS project configuration, this file will be preserved.

Dependency Configurations - NIL

Network

To save network settings related with IPMI (LAN IP or DHCP configuration), selecting “IPMI” will automatically select the another option “Network” and it’s vice versa. After restore configuration, the Network Configuration will be preserved successfully. Following files will also be preserved.

dhcp.conf: This file is to configure the host name in the FQDN format.

dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface.

hostname: This file is used to store the Hostname of the BMC.

hostname.conf: This file is used to configure the host name creation method Manual/ Automatic for the BMC.

Vlaninterfaces: This file helps to enable the vlan interface for the particular LAN interface

vlansetting.conf: This file is to store the vlan ID and Vlan priority for the particular VLAN interface entry.

bond.conf: This file is to enable the bond interface for the specified LAN interfaces.

Interfaces: This file is to configure the IP/IPV6 addresses for the LAN interface using static/DHCP method.

activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.

hosts: This file is used to store the host name to map the IP address.

hosts.allow: This file contains the list of hosts that has permission to access the

system hosts.deny: This file contains the list of host that does not allow accessing the system.

resolv.conf: This file is used to store the nameserver and domain name for hostname registration.

dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.

dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.

ncsicfg.conf: This file is to configure the NCSI related configurations.

nsupdate.conf: This file is to configure the channel ID, package ID for the NCSI interface.

phycfg.conf: Thisfileistoconfigurethelinkspeed,duplexandMTUvalueforthespecifiedinterface. dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.

ncml.conf: This file contains service configuration details.

Dependency Configurations - IPMI

NTP

Following files will be preserved.

ntp.conf: This file contains the NTP dameon protocol configuration parameters such as synchronization sources, nodes and other related information

ntp.stat: This file contains the auto or manual network type protocols

adjtime: This file contains the time to synchronize the system clock

Localtime: This file is the system link to the file local time or to the correct time zone in the system timezone directly.

Dependency Configurations - IPMI

SNMP

Following files will be preserved.

snmp_users.conf: This file contains the SNMP user configurations such as user name and password encryption mechanism for the specific users.

snmpcfg.conf: This file contains the SNMP users privilege levels such as ro user and rw user.

Dependency Configurations - NIL

SSH
Following files will be preserved.

snmp_users.conf: This file contains the keyword argument pairs of configurations such as Address family, Accept Env, Allow, users, authorized key files etc.

ssh_host_dsa_key , ssh_host_rsa_key: These files contain the private parts of the host keys.

ssh_host_dsa_key.pub, ssh_host_rsa_key.pub: These files contain the public parts of the host keys.

Dependency Configurations - NIL

KVM & Media
Following files will be preserved.

vmedia.conf: This file contains the modes of media such as cd, fc, hd and enable and disable flags for Imedia, rmedia and sd servers.

adviserd.conf: This file contails the mouse mode configurations and host machine physical keyboard language layout configured in the MDS project configuration.

autorecord.conf: This file contains the maximum size of the video record file, the maximum time length of the video record file and information about the remote machine path if it is enabled in MDS project configuration.

stunnel.conf: This file contains the information about the stunnel configuration. It will also contain advisor and media server's secure port if secure connection is enabled.

usermacro.conf: This file saves the user defined macro from the jviewer.

Dependency Configurations - NIL

Authentication
Following files will be preserved.

activedir.conf: This file contains the configurations such as sslenable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, username, password, and rolegroup information such as name domain and privileges.

openLdapGroup.conf: This file contains the oprnm ldap role group information such as name domain and privilege.

nsswitch.conf: This file contains the sources to obtain the name service information in the range of categories and in what order.

pam_withunix: This file contins the PAM Order of modules such as IPMI, LDAP, RADIUS and UNIX.

pam_wounix: This contains the PAM Order of modules such as IPMI,LDAP and RADIUS.

group: This file contains the Linux group. It stores the group information or defines the user group information in Linux.

passwd: This file contains the user login information for the Linux system

shadow: This file contains the encrypted password information for the clients.

ldap.conf: This file contains the ldap server configuration details such as bindn, binpw, pam_ password, nss_reconnect_tries, port, port secondary, host, host secondary.

radius.conf: This file contains the radius server IP address, port number, secret, timeout, privilege etc.

Dependency Configurations – NIL

Syslog
The following files will be preserved.

- syslog.conf
- rotate.conf
- rsyslog.conf

These files contain the system log configuration details to preserve different event categories such as alert, critical, error notification etc.

Dependency Configurations – NIL

Web
The following files will be preserved.

updatefirmware.conf: This file contains the firmware image location details to update firmware configuration.

Dependency Contains the firmware

Extlog
It preserves Extended SEL Log events.

This file contains Extended SEL events Log details.

Dependency Configurations - IPMI

> **NOTE**
> This support is feature based. If this feature is enabled, then the Extlog option will be displayed in Preserve configuration

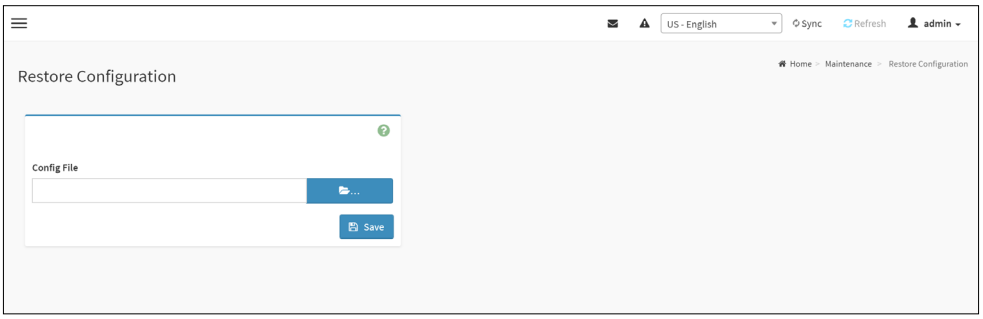
Procedure

1. Click Firmware Update or Restore Configuration link to view Firmware Update or Restore Configuration page accordingly.
2. Select the required Preserve Configuration items by either choosing the items individually by selecting the appropriate check boxes or by selecting all or none using Check All.
3. Click Save to save the changes.

10.7 Restore Configuration

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

To open Restore Configuration page, click Maintenance → Restore Configuration from the menu bar. A sample screenshot of Restore Configuration page is shown below.



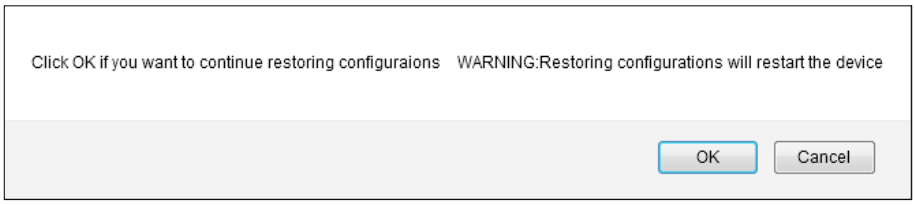
The various fields Restore Configuration page are given below.

Config File - This option is used to select the file which was backup earlier.

Upload - To upload the backup file to restore the backup files.

Procedure for Restore Configuration:

1. Click Browse to select the configuration file that needs to be backup and used to Restore the configuration, when needed.
2. Click Upload to restore the backup files. The Restore Configuration page will appear as shown below.



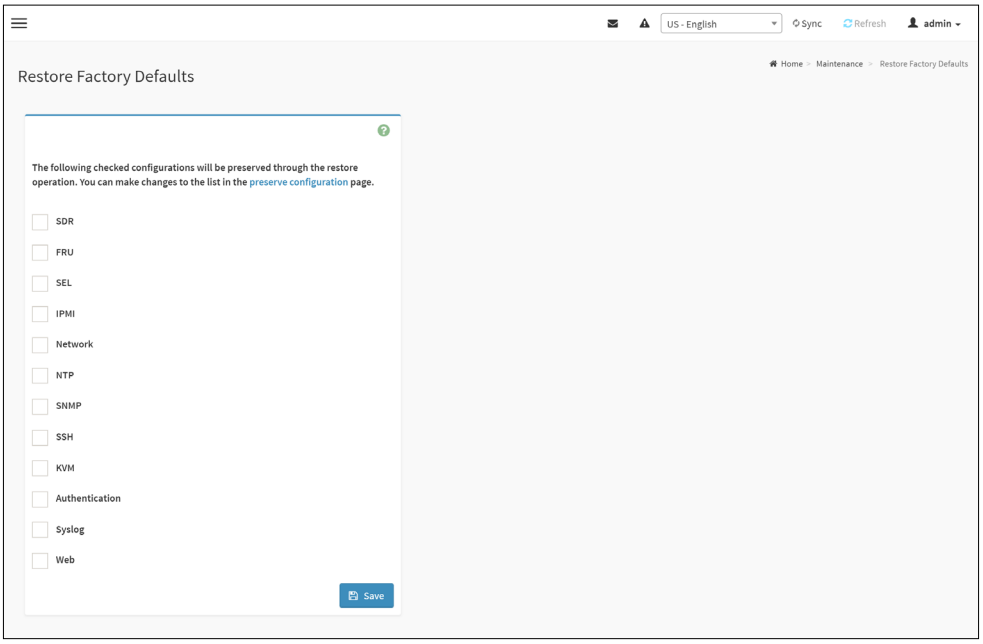
3. Click OK to upload the new configuration file and restore.

10.8 Restore Factory Default

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

Warning: Please note that after entering 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.

To open Restore Factory Defaults page, click Maintenance → Restore Factory Defaults from the menu bar. A sample screenshot of Restore Factory Defaults page is shown below.



Procedure

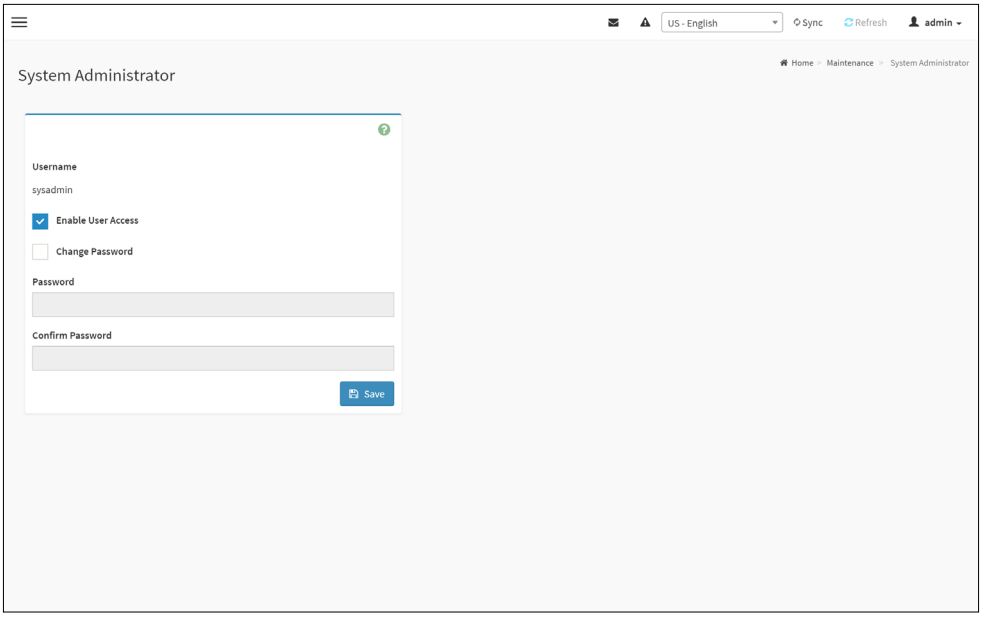
1. Click Preserve Configuration to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click Restore Factory Defaults to restore the factory defaults of the device firmware.

> **NOTE**
> When Restore Factory Defaults action is performed, there might be some log events present after performing restore operation. Those events might be newly generated which can be verified using its timestamp.

10.9 System Administrator

This page is used to configure the System Administrator settings.

To open System Administrator page, click Maintenance → System Administrator from the menu bar. A sample screenshot of System Administrator page is shown below.



The various fields of System Administrator page are given below.

Username: Username of System Administrator is a read only field.

Enable User Access: To enable user access for system administrator.

Change Password: To change the user's password.

> **NOTE**
> This field will not allow more than 64 characters.
> - Password must be at least 8 characters long and White space is not allowed.

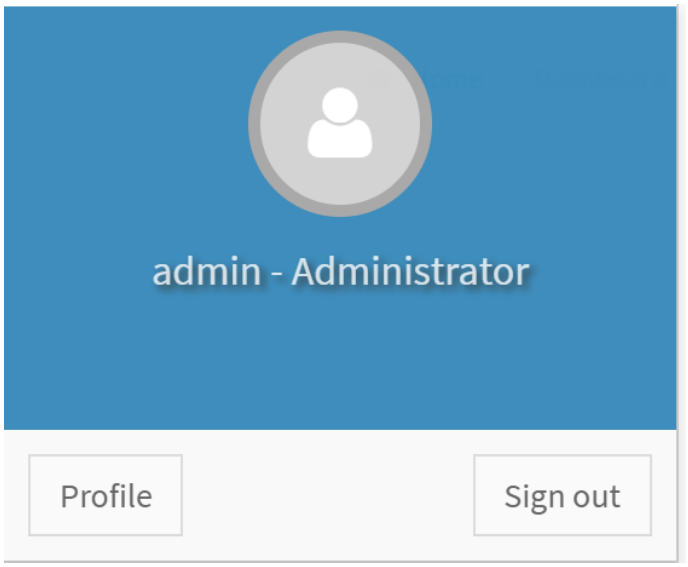
Save: To save the new configuration for system administrator.

Procedure:

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

Chapter 11. Sign Out

To log out from, click the admin on the top right corner of the screen. A sample screenshot of admin option is shown below.



Click Sign Out to perform log out. A Warning message will be prompted you to proceed further, click OK to log out or Cancel to retain the interface.

Chapter 12. Flash Tools

The Flash Tools are command line utility programs used to upgrade the firmware using different medium like KCS, USB, and LAN. There are three tools, which are being used.

• YAFUFlash

YAFUFlash

Yet Another Firmware Upgrade Flash is a tool used for flashing the BMC. This utility is used for flashing in both Linux and Windows environment. There are three types of mediums used to flash the BMC. They are,

- Network
- USB
- KCS

> **NOTE**
> YAFU based firmware update using Signed Hashed image is only possible if enough RAM is available to upload the full firmware image before the update starts.
> In YAFU firmware upgrade, only YAFU command set is allowed if Enable IPMI Command handling during flashing support is disabled in project configuration.
> YAFU flashing process has the following timeout values
> **LAN interface**: 3600 seconds
> **USB interface**: 1800 seconds
> **KCS interface**: 5400 seconds
> If Secure Boot Support is enabled in the PRJ, YAFUFlash options for Section Based Flashing or Interactive mode will not be used. Hence any feature or options that rely on Section Based Flashing or Interactive mode cannot be used when Secure Boot Support is enabled.

Installation in Windows

1. Open the command prompt and enter YafuFlash\Windows path.
2. This contains two files, Yafuflash.exe and LIBIPMI.dll.
3. **Format**: Yafuflash [OPTIONS] [MEDIUM] [FW_IMAGE_FILE], where Perform BMC Flash Update
   - -? Displays the utility usage
   - -h Displays the utility usage
   - -V Displays the version of the tool
   - -e List outs a few examples of the tool

[OPTIONS]

-info	*Displays information about existing FW and new FW.*
-msi, -img-section-info	*Displays information about current FW Sections.*
-mi, -img-info	*Displays information about current FW Versions.*
-fb, -force-boot	*Option to FORCE BootLoader upgrade during full upgrade. Also, skips user interaction in Interactive upgrade mode. This option is not allowed with Interactive upgrade option.*
-pc, -preserve-config	*Option to preserve Config Module during full upgrade. If platform supports Dual Image, this option skips user interaction, preserves config and continues update process. This option is not allowed with interactive upgrade option.*
-q, -quite	*Use the option to show the minimum flash progress details.*
-i	*Option to interactive upgrade (Upgrade only required modules)***
-f, -full	*Performs full upgrade in Interactive Upgrade mode. Skips module wise upgrade*
-ipc, -ignore-platform-check	*If this image is for a different platform, this option skips user interaction and continues update process.*
-idi, -ignore-diff-image	*If this image differs from the currently programmed image, this option skips user interaction and continues update process.*
-isi, -ignore-same-image	*If this image is same as the currently programmed image, this option skips user interaction and continues update process.*
-iml, -ignore-module-location	*If module(s) of this image is/are in different locations, this option skips user interaction and continues update process.*
-ibv, -ignore-boot-version	*If bootloader version is different and -force-boot is not specified, this option skips user interaction and continues update process. The bootloader will be updated.*
-iri, -ignore-reselect-image	*Option skips reselecting the active image.*
-inc, -ignore-non-preserve-config	*Option skips the restore to default factor setting if the image shares the same configuration area.*
-rp, -replace-publickey	*Option to replace the Signed Image Key in Existing Firmware.*
-vcf, -version-cmp-flash	*Option to skip flashing modules only if the versions are same by selecting (N/n). Option (Y/y) Selects full firmware upgrade mode.*

-non-interactive	*This option skips user interaction. This option cannot be used along with 'ignore-diff-image', 'ignore-same- image','- ignore-module-location'&'- ignore- boot-version' options.*
-pXXX, -preserve-XXX	*Option to preserve XXX configuration, where XXX falls in sdr, fru, sel, ipmi, auth, net, ntp, snmp, ssh, kvm and syslog. If the preserve status of the other configuration enabled then it will ask for the other configuration to be preserved.*
-ieo, -ignore-existing-overrides	*Clears the existing overrides and preserves only the overrides given in command line if any.*
-msp, -split-img	*Option to flash the split image.*
-f -XXX, -flash-XXX	*Option to flash specific section in non-interactive mode. If it is split image need to give split-image along with this option, where XXX denotes name of the section, e.g. -flash-conf.*
-sc, -skip-crc	*Option to skip the CRC check*
-sf, -skip-fmh	*Option to skip the FMH check*
-d	*Option to specify the peripheral(Only for Dual Image Support)* *<bit0> - BMC* *<bit1> - BIOS*
-a, -activate	*Option to activate peripheral devices* *<BIT0> - BMC* *<BIT1> - BIOS*
-nr, -no-reboot	*Option to skip the reboot With online-flash support, If conf/extlog is not preserved, BMC will still reboot.*
-bu, -block-upgrade	*Option to Flash using Block by Block method*

[MEDIUM]

-cd	*Option to use USB Medium*
-nw, -ip, -u, -p,-host, _pa	*Option to use Network Medium* *'-ip' Option to enter IP, when using Network Medium* *'-host' Option to enter host name, When using Network Medium* *'-u' Option to enter UserName, When using Network Medium* *'-p' Option to enter Password, When using Network Medium* *'_p' Option to enter Port Number.*

-kcs	*Option to use KCS medium.*
-serial	*Option to use serial interface.*
-term	*Option to use serial command, e.g. /dev/ttyS0.*
-baudrate	*Option to use baudrate of the serial terminal, e.g. 115200.*
[FW_IMAGE_FILE]	*Firmware image file name [rom.ima].*
-pe, -preserve-extlog	*Option to preserve extlog configuration during firmware flash.*

NOTE
-'preserve-config' and '-force-boot' option not be used in interactive upgrade.
*IPv6 Support is added after the tool version 2.7. IPv6 Support can be used with latest Yafu tool and firmware, older version of yafu (and/or) firmware will not work.
**Interactive upgrade is not a default option. This option can be enabled in YafuFlash, if it is built with Enable/Disable Interactive Upgrade YafuFlash option selected in Project Configuration file (*.PRJ) using MDS.

Examples for Network Medium

Eg1: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima -info
Description: This command works with network medium using the ip 155.166.132.12, which displays the details of both existing firmware and new firmware.

Eg2: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware.

Eg3: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –force-boot
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –preserve-config
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with preserve config params.

Eg5: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –force-boot –preserve-config
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg6: ./Yafuflash –nw –host spxbmc –force-boot –preserve-config rom.ima
Description: This command works with network medium using the host name spxbmc, which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserve config params.

Eg7: ./Yafuflash –nw –ip 2000::2005 –force-boot rom.ima
Description:Thiscommand workswithnetwork mediumusing theipv6address 2000::2005,which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg8: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –i
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima using interactive upgrade mode and user will be prompt to select the Number of modules and module names to upgrade.

Eg9: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-section-info
Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg10: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-info
Description: This command works with network medium using the ip 155.166.132.12, which displays the details of existing firmware Version.

Eg11: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin public.pem –replace-publickey
Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in firmware.

Eg12: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-sdr
Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurationswhich are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg13: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-snmp–preserve-ntp
Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg14: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-fru –ignore-existing-overrides
Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg15: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-fru –preserve-snmp –ignore-existing-overrides
Description:This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg16: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-reselect-image
Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg17: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-non-preserve-config
Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg18: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 0 rom.ima
Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg19: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 1 rom.ima
Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg20: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 2 rom.ima
Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg21: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-select 3 rom.ima
Description: This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg22: ./Yafuflash –nw –ip 155.166.132.12 rom.ima -quite
Description: This command works with network medium using the ip 155.166.132.12, which start to flash the new rom.ima with minimum progress details.

Eg23: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –split-img boot.ima
Description: This command works with network medium to flash the boot split image.

Eg24: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin –split-img root.ima
Description: This command works with network medium to flash the root split image.

Eg25: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin rom.ima –flash-root –flash-conf
Description: This command works with network medium to flash root and conf section from rom. ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg26: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin boot.ima –split-img –flash-boot
Description: This command works with network medium to flash root from boot.ima split image.
-flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg27: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –split-img –flash-www–flash-osimage
Description: This command works with network medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

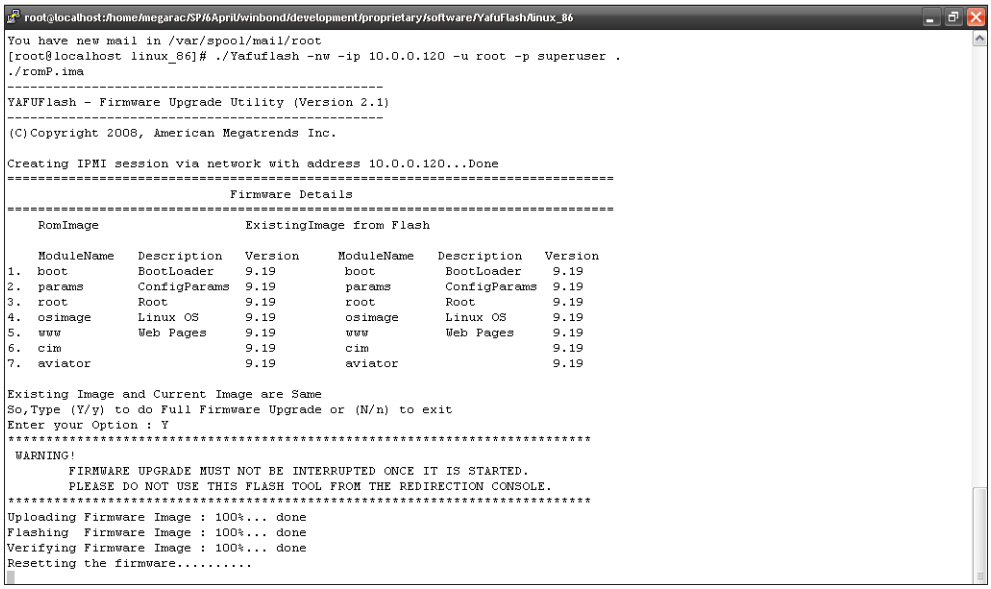
Eg28: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin rom.ima –preserve-extlog
Description: This command works with network mediumto preserve extended log configuration.

Eg29: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –split-img -preserve-extlog
Description: This command works with network medium to preserve extended log configuration from split image.

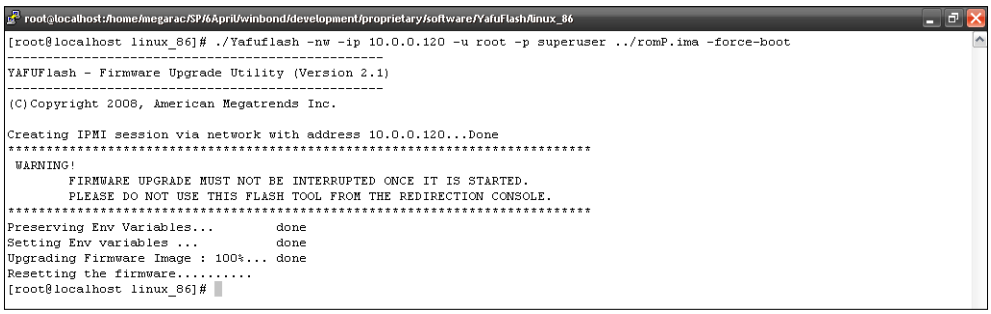
Eg30: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –d 1 rom.ima
Description: This command works with network medium to flash the image on specific peripheral device.

Eg31: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin root.ima –d 1 root.ima –split-img
Description: This command works with network medium to flash the split image on specific peripheral device.

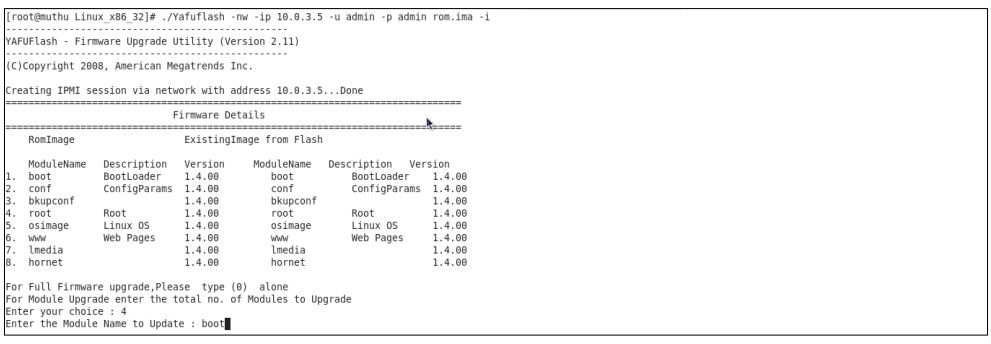
Screen: If Existing and current images are same



FG: 2 - Existing and current are different



FG: 3 - Interactive Upgrade Mode



Eg32: ./Yafuflash –nw–ip 155.166.132.12 –u admin –p admin –bu root.ima.
Description: This command works with network medium to flash the image on specific peripheral device by block by block upgrade.

Examples for USB Medium:
Power Save Mode should be disabled for Flashing with Yafu USB Interface.

Eg1: ./Yafuflash –cd rom.ima –info
Description: This command works with USB medium which displays the details of both Existing Firmware and new firmware.

Eg2: ./Yafuflash –cd rom.ima
Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware.

Eg3: ./Yafuflash –cd rom.ima –force-boot
Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade.

Eg4: ./Yafuflash –cd rom.ima –preserve-config
Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5: ./Yafuflash –cd rom.ima –force-boot –preserve-config
Description: This command works with USB medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader Upgrade and preserving config params.

Eg6: ./Yafuflash –cd rom.ima –i
Description: This command works with USB medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7: ./Yafuflash –cd –img-section-info
Description: This command works with USB medium which displays the details of Existing Firmware.

Eg8: ./Yafuflash –cd –img-info
Description: This command works with USB medium which displays the details of Existing Firmware Version.

Eg9: ./Yafuflash –cd public.pem –replace-publickey
Description: This command works with USB medium which replaces the public key in Existing Firmare.

Eg10: ./Yafuflash–cd rom.ima –preserve-sel –preserve-ipmi
Description: This command works with USB medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11: ./Yafuflash –cd rom.ima –preserve-sel –ignore-existing-overrides
Description: This command works with USB medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only

Eg12: ./Yafuflash –cd rom.ima –ignore-reselect-image
Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13: ./Yafuflash –cd rom.ima –ignore-non-preserve-config
Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14: ./Yafuflash –cd –img-select 0 rom.ima
Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the active image to be flashed.

Eg15: ./Yafuflash –cd –img-select 1 rom.ima
Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the first image to be flashed.

Eg16: ./Yafuflash –cd –img-select 2 rom.ima
Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting the second image to be flashed.

Eg17: ./Yafuflash –cd –img-select 3 rom.ima
Description: This command works with USB medium, which starts to flash the new rom. ima to the existing firmware by selecting both the images to be flashed.

Eg18: ./Yafuflash –cd rom.ima –quite
Description: This command works with USB medium, which start to flash the new rom.ima with minimum progress details.

Eg19: ./Yafuflash –cd –split-img boot.ima
Description: This command works with USB medium to flash the boot split image.

Eg20: ./Yafuflash –cd –split-img root.ima
Description: This command works with USB medium to flash the root split image.

Eg21: ./Yafuflash –cd rom.ima –flash-root –flash-conf
Description: This command works with USB medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg22: ./Yafuflash –cd boot.ima -split-img –flash-boot
Description: This command works with USB medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg23: ./Yafuflash –cd root.ima –split-img –flash-www –flash-osimage
Description: This command works with USB medium to flash www and osimage from root. ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg24: ./Yafuflash –cd rom.ima –preserve-extlog
Description: This command works with USB mediumto preserve extended log configuration.

Eg25: ./Yafuflash –cd root.ima –split-img –preserve-extlog
Description: This command works with USB mediumto preserve extended log configuration from split image.

Eg26: ./Yafuflash –cd root.ima –d 1 rom.ima
Description: This command works with USB medium to flash the image on specific peripheral device.

Eg27: ./Yafuflash –cd root.ima –d 1 root.ima –split-img
Description: This command works with USB medium to flash the split image on specific peripheral device.

Eg28: ./Yafuflash –cd root.ima –d 1 root.ima –split-img
Description: This command works with USB medium to flash the split image on specific peripheral device.

Examples for KCS Medium:

Eg1: ./Yafuflash –kcs rom.ima –info
Description: This command works with KCS medium which displays the details of both Existing Firmware and new firmware.

Eg2: ./Yafuflash –kcs rom.ima
Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware.

Eg3: ./Yafuflash –kcs rom.ima –force-boot
Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader upgrade.

Eg4: ./Yafuflash –kcs rom.ima –preserve-config
Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with preserving config params.

Eg5: ./ Yafuflash –kcs rom.ima –force-boot –preserve-config
Description: This command works with KCS medium which start to flash the new rom.ima to the existing firmware with FORCE BootLoader upgrade and preserving config params.

Eg6: ./Yafuflash –kcs rom.ima –i
Description: This command works with KCS medium, which start to flash the new rom.ima using interactive upgrade mode and user, will be prompt to select the Number of modules and module names to upgrade.

Eg7: ./Yafuflash –kcs –img-section-info
Description: This command works with KCS medium which displays the details of Existing Firmware.

Eg8: ./Yafuflash –kcs –img-info
Description: This command works with KCS medium which displays the details of Existing Firmware Version.

Eg9: ./Yafuflash –kcs public.pem –replace-publickey
Description: This command works with KCS medium which replaces the public key in Existing Firmware.

Eg10: ./Yafuflash –kcs rom.ima –preserve-sel –preserve-ipmi
Description: This command works with KCS medium, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SEL and IPMI as well as selected configurations.

Eg11: ./Yafuflash –kcs rom.ima –preserve-sel –ignore-existing-overrides
Description: This command works with KCS medium, which start to flash the new rom.ima to the existing firmware with preserving FRU configurations only

Eg12: ./Yafuflash –kcs rom.ima –ignore-reselect-image
Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg13: ./Yafuflash –kcs rom.ima –ignore-non-preserve-config
Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg14: ./Yafuflash –kcs –img-select 0 rom.ima

Description: This command starts to flash the new rom.ima to the existing firmware by selecting the active image to be flashed.

Eg15: ./Yafuflash –kcs –img-select 1 rom.ima
Description: This command starts to flash the new rom.ima to the existing firmware by selecting the first image to be flashed.

Eg16: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-section-info
Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware.

Eg17: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin –img-info
Description: This command works with network medium using the ip 155.166.132.12, which displays the details of Existing Firmware Version.

Eg18: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin public.pem –replace-publickey
Description: This command works with network medium using the ip 155.166.132.12, which replaces the public key in Existing Firmware.

Eg19: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-sdr
Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SDR as well as selected configurations.

Eg20: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-snmp –preserve-ntp
Description: This command works with network medium using the ip 155.166.132.12, which will ask for other configurations which are already set to be preserved to preserve or not and after that it will start to flash the new rom.ima to the existing firmware with preserving SNMP and NTP as well as selected configurations.

Eg21: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-fru –ignore-existing-overrides
Description:This command works with network medium using the ip155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU configurations only.

Eg22: ./Yafuflash –nw –ip 155.166.132.12 rom.ima –preserve-fru –preserve-snmp –ignore-existing -overrides
Description: This command works with network medium using the ip 155.166.132.12, which starts to flash the new rom.ima to the existing firmware with preserving FRU and SNMP configurations only.

Eg23: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-reselect-image
Description: Yafuflash start full firmware upgrade with default active image. In this it skips the reselecting active image used to flash.

Eg24: ./Yafuflash –nw –ip 155.166.132.12 –u admin –p admin rom.ima –ignore-non-preserve-config
Description: Yafuflash start full firmware upgrade, If the Images of both flash share the same Configuration area. Not preserving will restore to default factory settings, this option skips it.

Eg25: ./Yafuflash –kcs –img-select 2 rom.ima
Description: This command starts to flash the new rom.ima to the existing firmware by selecting the second image to be flashed.

Eg26: ./Yafuflash –kcs –img-select 3 rom.ima
Description: This command starts to flash the new rom.ima to the existing firmware by selecting both the images to be flashed.

Eg27: ./Yafuflash –kcs rom.ima -quite
Description: This command works with KCS medium, which start to flash the new rom.ima with minimum progress details.

Eg28: ./Yafuflash –kcs –split-img boot.ima
Description: This command works with KCS medium to flash the boot split image.

Eg29: ./Yafuflash –kcs –split-img root.ima
Description: This command works with KCS medium to flash the root split image.

Eg30: ./Yafuflash –kcs rom.ima –flash-root –flash-conf
Description: This command works with KCS medium to flash root and conf section from rom.ima file. -flash-<xxx>, where xxx specifies the modules in rom.ima.

Eg31: ./Yafuflash –kcs boot.ima –split-img –flash-boot
Description: This command works with KCS medium to flash root from boot.ima split image. -flash-<xxx>, where xxx specifies the modules in boot.ima.

Eg32: ./Yafuflash –kcs root.ima –split-img –flash-www –flash-osimage
Description: This command works with KCS medium to flash www and osimage from root.ima split image. -flash-<xxx>, where xxx specifies the modules in root.ima.

Eg33: ./Yafuflash –kcs rom.ima –preserve-extlog
Description: This command works with KCS medium to preserve extended log configuration.

Eg34: ./Yafuflash –kcs root.ima –split-img –preserve-extlog
Description: This command works with KCS medium to preserve extended log configuration from split image.

Eg35: ./Yafuflash –kcs root.ima –d 1 rom.ima
Description: This command works with KCS medium to flash the image on specific peripheral device.

Eg36: ./Yafuflash –kcs root.ima –d 1 root.ima –split-img
Description: This command works with KCS medium to flash the split image on specific peripheral device.

YAFUFlash OS Compatibility

KCS/USB	LAN
Windows Server 2012	Ubuntu 16.04
Windows Server 2008	Windows 8.1
Windows Server 2016 Standard (Exclude Nano Server)	Ubuntu 14.04
Ubuntu Server 16.04	Windows 10
Ubuntu Server 14.04	MACOS 10.10
RHEL 7.2	Fedora 24
RHEL 6.5	Fedora 24
SLES Server 12.1	
SLES Server 11.4	

Chapter 13. VMCLI

The Virtual Media Command Line Interface(VMCLI) utility is a scriptable command-line interface that provides virtual media features from the management station to the Host.

VMCLI is used to redirect the virtual media (Hard Disk, Floppy, CD drive, USB..) from the management station to the host.

> **NOTE**
> VMCLI Tool uses wget tool to communicate with webserver which runs inside BMC in order to fetch media server related configurations.Wget windows tool supports IPv6 link local ip too but Wget Linux tool doesn't support.

Features:

- Removable media devices or image files that are consistent with the Virtual Media plug-ins
- Automatic termination when the host firmware boot once option is enabled
- Secure communication to the host using Secure Sockets Layer (SSL)
- VMCLI utility can run as a service as well as application.

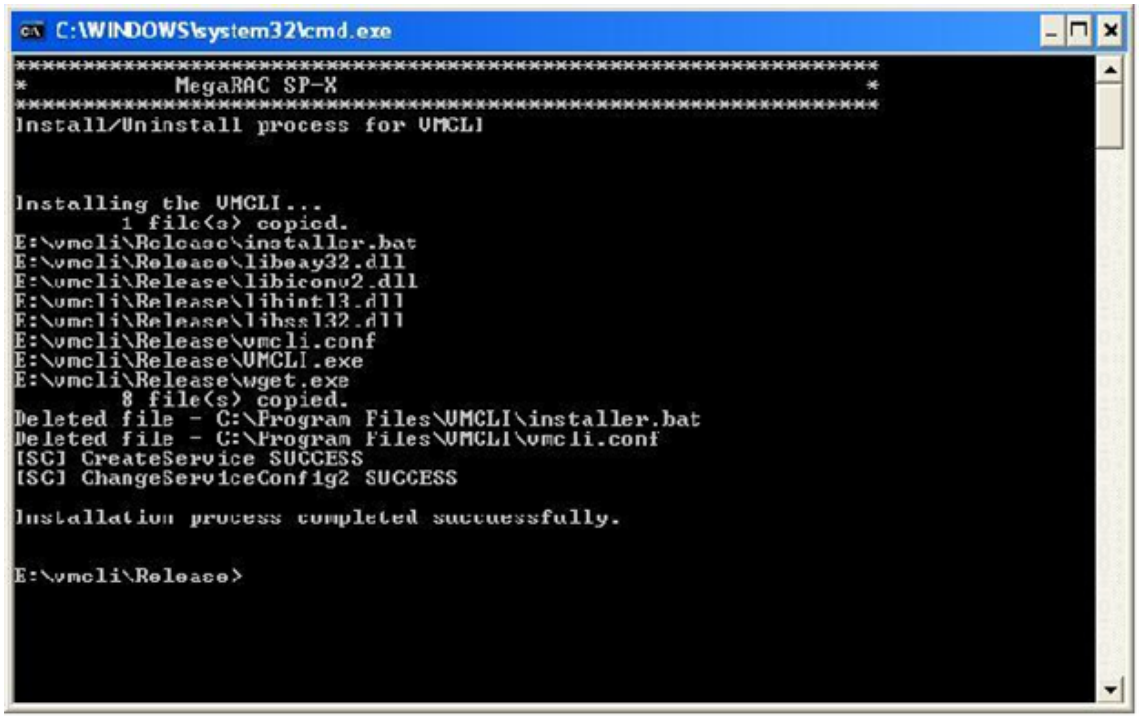
Installation in Windows

> **NOTE**
> Windows VMCLI requires " Microsoft Visual C++ Redistributable Package" to be installed in windows client.

1. VMCLI can be installed in windows using batch file, installer.bat in VMCLI folder.

> **NOTE**
> You must keep wget inside the VMCLI Folder, which is the support Tool for VMCLI

2. Go to VMCLI folder and execute the installer script to install the VMCLI service. Installer. bat –i



3. Installer script will add the VMCLI as windows service and user can start and stop the service using sc command.
4. Start the VMCLI Service.

To start VMCLI utility as service using command line argument
Format:
sc start VMCLI [-r][IP : Web-SSLPort] [-u][USER] [-p] [PASSWORD] [MEDIA TYPE] [MEDIA][-e]

To start as an application using command line argument
Format:
VMCLI.exe [-r][IP : Web-SSLPort] [-u][USER] [-p] [PASSWORD] [MEDIA TYPE] [MEDIA][-e]

To start VMCLI using a configuration file.

VMCLI Configuration fields to start CD redirection.

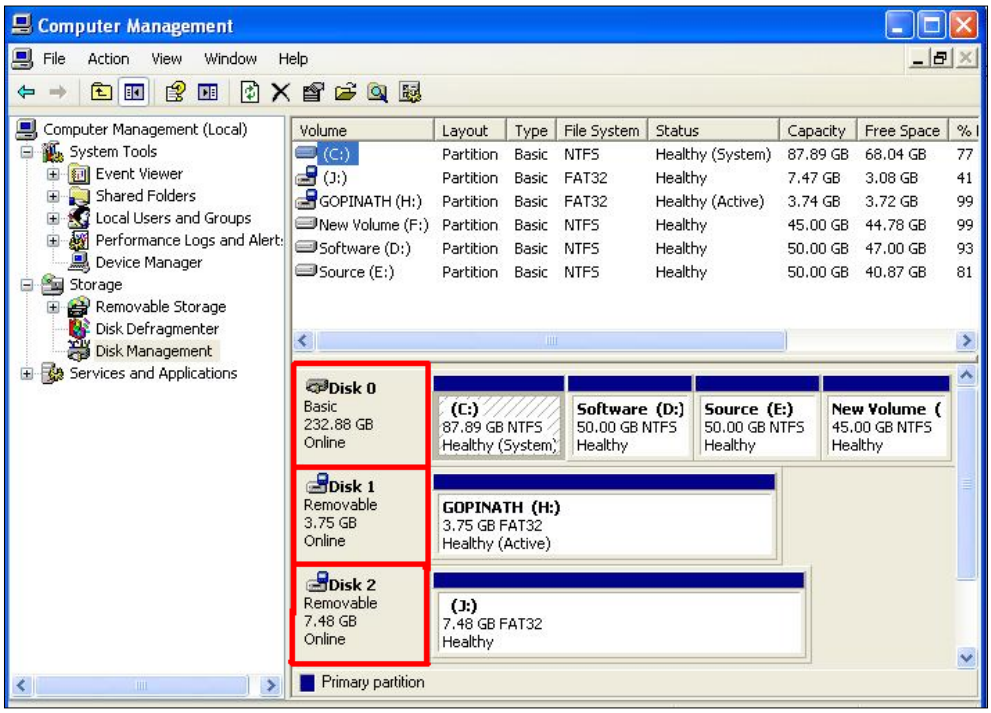
```
# In vmcli.conf file
[config]
ipaddr = [IP]
username = [USER]
password = [PASSWORD]
port = [Web-SSLPort]
encryption = [1/0]
cdredirect = [MEDIA]
hdredirect =
```

VMCLI configuration fields to start HD redirection

```
# In vmcli.conf
[config]
ipaddr = [IP]
username = [USER]
password = [PASSWORD]
port = [Web-SSLPort]
encryption = [1/0]
cdredirect =
hdredirect = [MEDIA]
```

To start as service
Format: sc start VMCLI

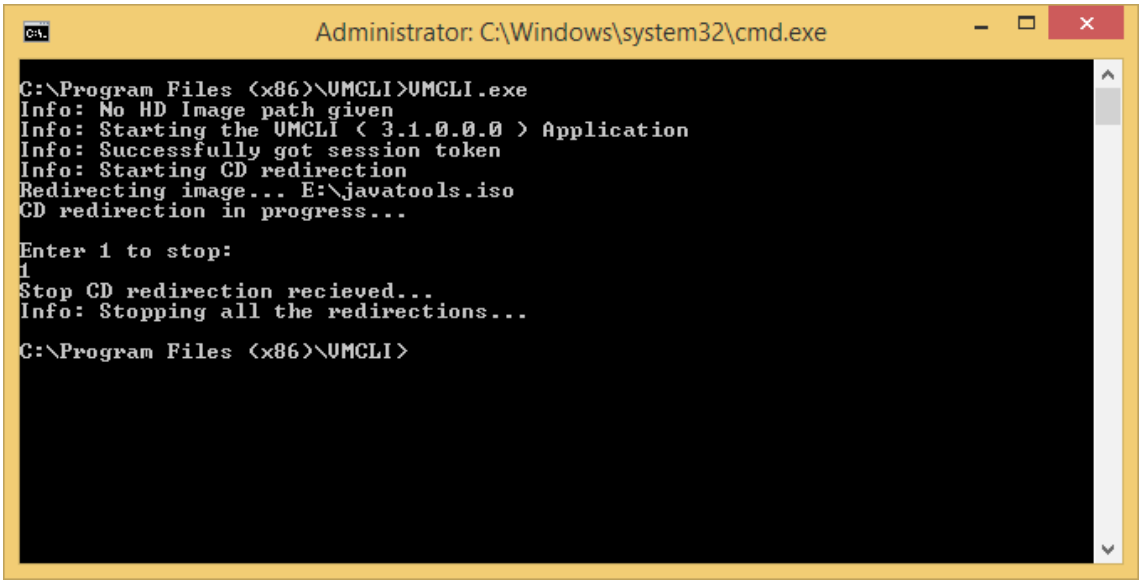
To start as application
Format: VMCLI.exe



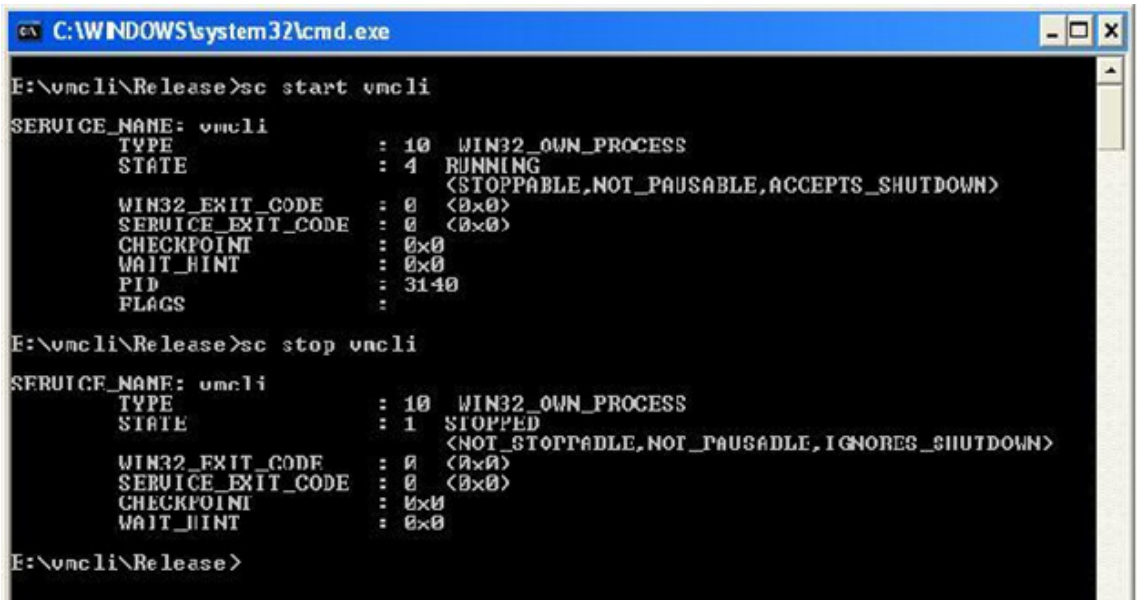
5. To Stop the VMCLI service.
Format: sc stop VMCLI

To stop the VMCLI application.
Format: Press 1 and enter to stop the application. (Reference VMCLI Screen 1)

VMCLI Screen 1

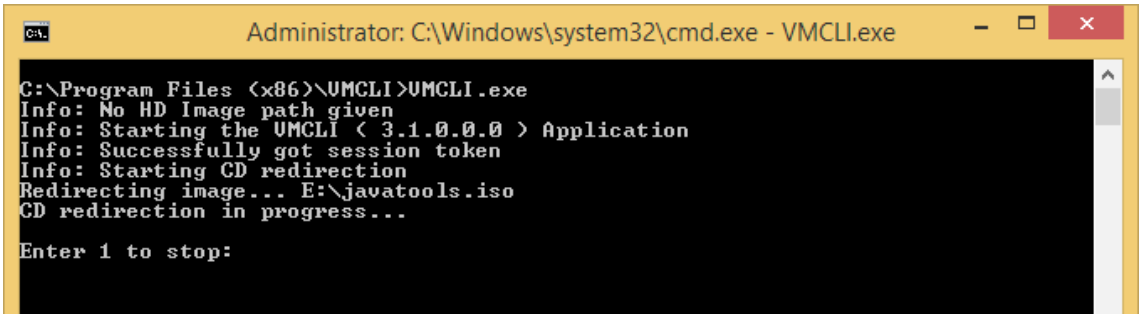


VMCLI Screen 2



The above VMCLI Screen 2 starts VMCLI service without command line argument, i.e, configuration will be read from conf file.

VMCLI Screen 3



The above VMCLI Screen 3 starts VMCLI application without command line argument, i.e, configuration will be read from conf file.

NOTE
If you would like to surround an argument by double quotation marks ("), please notice that a double quotation mark proceeded by a backslash, \", is interpreted as a literal double quotation mark. You have to use a pair of backslash (\\) followed by a double quotation mark, \\", let the double quotation mark interpreted as a string delimiter.
https://msdn.microsoft.com/en-us/library/a1y7w461.aspx
i.e.:
sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd "D:\" ⇨ incorrect (X)
sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd "D:\\" ⇨ correct (O)

Examples of CD-ROM Media redirection

Eg1:

VMCLI as service
IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -f E:\
IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -f E:\
VMCLI as application
IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -c E:\
IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -c E:\
Description: This command is to redirect the CD/DVD drive from the management station to the host.

Eg2:
VMCLI as service
IPv4: sc start VMCLI r 10.0.6.8:443 -u admin -p admin -c E:\ -e
IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -c E:\ -e
VMCLI as application
IPv4: VMCLI.exe r 10.0.6.8:443 -u admin -p admin -c E:\ -e
IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -c E:\ -e
Description: This command is to redirect the CD/DVD drive from the management station to the host. Data will be transfer through ssl.

Eg3:
VMCLI as service
IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -c “/home/cdrom.iso”
IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -c “/home/cdrom.iso”
VMCLI as application
IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -c admin -f FloppyIma
IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -c “/home/cdrom.iso”
Description: This command is to redirect the CD image from the management station to the host.The image file path is full system path.

Eg4: sc stop VMCLI
Description: This command is used to stop the VMCLI service to stop the redirection.

> **NOTE**
> If you would like to surround an argument by double quotation marks ("), please notice that a double quotation mark proceeded by a backslash, \", is interpreted as a literal double quotation
> mark. You have to use a pair of backslash (\\) followed by a double quotation mark, \\", let the double quotation mark interpreted as a string delimiter.
> https://msdn.microsoft.com/en-us/library/a1y7w461.aspx
> i.e.:
> sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd "D:\" ⇨ incorrect (X)
> sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd "D:\\" ⇨ correct (O)

Examples of Hard Disk Drive Media redirection

Eg1:
VMCLI as service
IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd D:/
IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -hd D:/
VMCLI as application
IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -hd D:/
IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -hd D:/
Description: This command is to redirect the Hard disk drive from the management station to the host.

Eg2:
VMCLI as service
IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd D:/ -e
IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -hd D:/ -e
VMCLI as application
IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -hd D:/ -e
IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -hd D:/ -e
Description: This command is to redirect the Hard disk drive from the management station to the host. Data will be transfer through ssl/

Eg3:
VMCLI as service
IPv4: sc start VMCLI -r 10.0.6.8:443 -u admin -p admin -hd “/home/hd.img”
IPv6: sc start VMCLI -r [2004::2000]:443 -u admin -p admin -hd “/home/hd.img”
VMCLI as application
IPv4: VMCLI.exe -r 10.0.6.8:443 -u admin -p admin -hd “/home/hd.img”
IPv6: VMCLI.exe -r [2004::2000]:443 -u admin -p admin -hd “/home/hd.img”
Description: This command is to redirect the floppy image from the management station to the host. The image file path is full system path.

Eg4: sc stop VMCLI
Description: This command is used to stop the VMCLI service to stop the redirection.

Installation in Linux

> **NOTE**
> VMCLI uses TLSv1.2 so it needs openssl1.0.0 (or above) and wget1.16 (or above) to work properly.

The following steps are mentioned for openssl1.0.0 package. If anyother version is installed the steps will vary.

For example if openssl1.0.1 is installed then the libssl.so will have libssl.so.1.0.1 and libcryto file name will also be libcrypto.so.1.0.1 etc.

1. Search libssl.so.1.0.0 and libcrypto.so.1.0.0 locate at /usr/lib (if it's not available in /usr/lib, try searching in /usr/lib64) or not. If not, do yum install openssl libssl or rpm -ivh openssl.rpm and rpm -ivh libssl.rpm:
   ls –l /usr/lib/libssl*
   ls –l /usr/lib/libcrypto*

> **NOTE**
> For Ubuntu look in the path /lib/x86_64-linux-gnu or /lib/i386-linux gnu

2. Create a force link as libssl.so.1.0.0 to libssl.so.10:
   ln –sf libssl.so.1.0.0 libssl.so.10
3. Create a force link as libcrypto.so.1.0.0 to libcrypto.so.10:
   ln -sf libcrypto.so.1.0.0 libcrypto.so.10
4. Open Terminal and go to VMCLI folder
5. Install the VMCLI service in Linux system using installer script
   sudo bash ./installer.sh –i
6. To start VMCLI utility using command line arguments.

To start as service
Format:
service vmcli start [-r] [IP:Web-SSLPort] [-u] [USER] [-p][PASSWORD] [MEDIA TYPE] [MEDIA] [-e].

To start as application
Format:
VMCLI.EXE [-r] [IP:Web-SSLPort] [-u] [USER] [-p][PASSWORD] [MEDIA TYPE] [MEDIA] [-e].

To start VMCLI using a configuration file.
VMCLI Configuration fields to start CD redirection.

```
# In vmcli.conf file
[config]
ipaddr = [IP]
username = [USER]
password = [PASSWORD]
port = [Web-SSLPort]
encryption = [1/0]
cdredirect = [MEDIA]
hdredirect =
```

VMCLI configuration fields to start HD redirection

```
# In vmcli.conf
[config]
ipaddr = [IP]
username = [USER]
password = [PASSWORD]
port = [Web-SSLPort]
encryption = [1/0]
cdredirect =
hdredirect = [MEDIA]
```

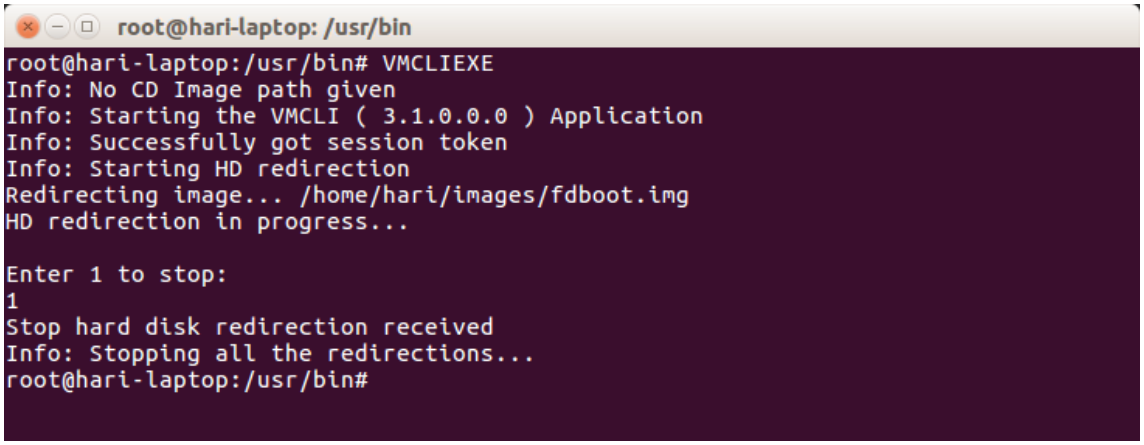
To start as service
Format: service VMCLI start

To start as application
Format: VMCLI.exe

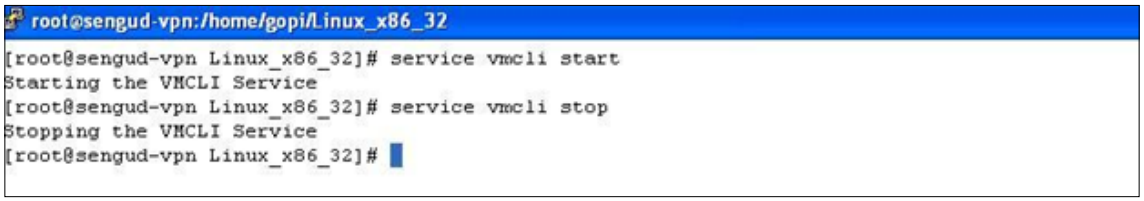
7. To stop the VMCLI service.
Format: service stop vmcli

To stop the VMCLI application.
Format: Press 1 and enter to stop the application. (Reference VMCLI Screen 4)

VMCLI Screen 4

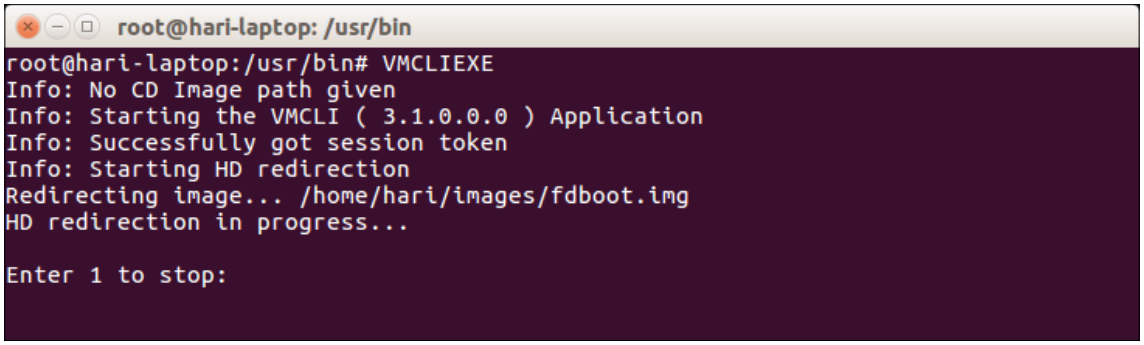


VMCLI Screen 5



The above VMCLI Screen 5 starts VMCLI service without command line argument, i.e, configuration will be read from conf file.

VMCLI Screen 6



The above VMCLI Screen 6 starts VMCLI application without command line argument, i.e, configuration will be read from conf file.

Examples of CD-ROM Media redirection

Eg1:
VMCLI as service
IPv4: service vmcli start -r 10.0.6.8:443 –u admin –p admin -c /dev/sdc
IPv6: service vmcli start -r [2004::2000] :443 –u admin –p admin -c /dev/sdc
V**MCLI as application**
IPv4: VMCLIEXE -r 10.0.6.8:443 –u admin –p admin -c /dev/sdc
IPv6: VMCLIEXE -r [2004::2000] :443 –u admin –p admin -c /dev/sdc
Description: This command is to redirect the CD/DVD drive from the management station to the host.

Eg2:
VMCLI as service
IPv4: service vmcli start -r 10.0.6.8:443 -u admin -p admin -cin -c /dev/sdcev/s
IPv6: service vmcli start -r [2004::2000] :443 –u admin –p admin –c “/home/cdrom.iso”
VMCLI as application
IPv4: VMCLIEXE -r 10.0.6.8:443 -u admin -p admin -c“/home/cdrom.iso”
IPv6: VMCLIEXE -r [2004::2000] :443 –u admin –p admin –c “/home/cdrom.iso”
Description: This command is to redirect the CD/DVD image from the management station to the host. The image file path is full system path.

Eg3:
VMCLI as service
IPv4: service vmcli start -r 10.0.6.8 :443 –u admin –p admin -c CD-RomImage.iso -e
IPv6: service vmcli start -r [2004::2000] :443 –u admin –p admin –c CD-RomImage.iso -e
VMCLI as application
IPv4: VMCLIEXE -r 10.0.6.8 :443 –u admin –p admin -c CD-RomImage.iso -e
IPv6: VMCLIEXE -r [2004::2000] :443 –u admin –p admin –c CD-RomImage.iso -e
Description: This command is to redirect the CD/DVD image from the management station to the host. Data will be transfer through ssl.

Eg4: service vmcli stop
Description: This command is used to stop the vmcli service to stop the redirection.

Examples of Hard Disk Drive Media redirection

Eg1:
VMCLI as service
IPv4: service vmcli start -r 10.0.6.8:443 –u admin –p admin -hd /dev/sda
IPv6: service vmcli start -r [2004::2000] :443 –u admin –p admin -hd /dev/sda
VMCLI as application
IPv4: VMCLIEXE -r 10.0.6.8:443 –u admin –p admin -hd /dev/sda
IPv6: VMCLIEXE -r [2004::2000] :443 –u admin –p admin -hd /dev/sda
Description: This command is to redirect the Hard disk drive from the management station to the host.

Eg2:
VMCLI as service
IPv4: service vmcli start -r 10.0.6.8:443 -u admin -p admin -hd n -hd nt statio
IPv6: service vmcli start - r [2004::2000] :443 –u admin –p admin –hd "/home/hd.img"
VMCLI as application
IPv4: VMCLIEXE -r 10.0.6.8:443 -u admin -p admin -hd n -hd in hd in i
IPv6: VMCLIEXE - r [2004::2000] :443 –u admin –p admin –hd "/home/hd.img"
Description: This command is to redirect the HD/USB image from the management station to the host. The image file path is full system path.

Eg3:
VMCLI as service
IPv4: service vmcli start -r 10.0.6.8 :443 :443 h.ro admin anagement station
IPv6: service vmcli start -r [2004::2000] :443 –u admin –p admin -hd /dev/sda -e
VMCLI as application
IPv4: VMCLIEXE -r 10.0.6.8 :443 –u admin –p admin -hd /dev/sda -e
IPv6: VMCLIEXE -r [2004::2000] :443 –u admin –p admin -hd /dev/sda -e
Description: This command is to redirect the Hard disk drive from the management station to the host. Data will be transfer through ssl.

Eg4: service vmcli stop
Description: This command is used to stop the vmcli service to stop the redirection.

Configuration File Support
VMCLI service is started with no command VMCLI supports the configuration file to pass the argument to the VMCLI service. The VMCLI service will read the configurations from the file, if the VMCLI service is started with no command line argument.

Example:

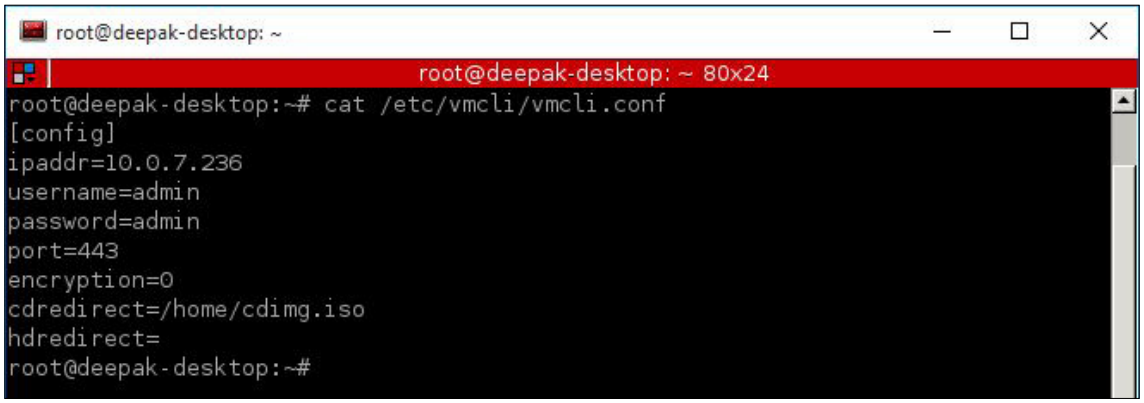
Service
service vmcli start [Linux] – filename is /etc/vmcli/vmcli.conf
sc start vmcli [Windows] – filename is C:\WINDOWS\vmcli.conf

Application
VMCLIEXE [Linux] – filename is <same path as vmcli binary>\vmcli.conf
VMCLI.exe [Windows] – filename is <same path as vmcli binary>\vmcli.conf

Log file support is added to VMCLI service. The VMLCI service's start and stop information can be logged into this file (/var/log/vmcli or C:\WINDOWS\vmcli).

NOTE
VMCLI service will not be started if the command line arguments or configuration file are not configured properly.

In Latest versions of Linux, the systemd in it system requires a service unit file to manage the services and it doesn't accept arguments. Hence configuration file is necessary to pass the arguments to the VMCLI service. It is mandatory for the user to fill the required arguments in the configuration file.



List of Supported OS

OS	System Type
Windows 10 / 8.1 / 7	64bit
Ubuntu 16.04 LTS and later	64bit
Fedora 23 Desktop and later	64bit
CentOS 7	64bit
Windows server 2008 SP2 / 2012	64bit
RHEL 5.4 / 6.0 / 7	64bit
SLES 11 / 12	64bit

Chapter 14. SOL

One of the powerful tools in IPMI is Serial Over LAN (SOL) which provides serial line access over the management LAN. The baseboard management controller (BMC) microcontroller embedded on the server motherboard 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 doesn't 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 functions 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 15. Technical Support

www.aicipc.com

Taiwain, Global Headquarters

Address: No. 152, Section 4, Linghang N. Rd, Dayuan District, Taoyuan City 337, Taiwan
Tel: +886-3-433-9188
Fax: +886-3-287-1818
Sales Email: sales@aicipc.com.tw
Support Email: support@aicipc.com

Shanghai, China

Address: Room 215, Building 4, No.471 Guiping Road, Xuhui District, Shanghai City, 200233 China
Tel: +86-21-54961421
Sales Email: sales@aicipc.com.cn
Support Email: support@aicipc.com

Moscow, Russia

Address: No. 500, 5th Floor, 5th Entrance, 32A, Khoroshevskoye Shosse, Moscow, 123007
Tel: +7-4997019998
Sales Email: support-ru@aicipc.com.tw
Support Email: rma.russia@aicipc.com.tw

North California, United States

Address: 48531 Warm Springs Boulvard Suite 404 Fremont, CA 94539, United States
Tel: +1-510-573-6730
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

South California, United States

Address: 21808 Garcia Lane City of Industry, CA 91789, United States
Toll free: + 1-866-800-0056
Tel: +1-909-895-8989
Fax: +1-909-895-8999
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

New Jersey, United States

Address: 322 Route 46 West Suite 100 Parsippany, NJ 07054 United States
Tel: +1-973-884-8886
Fax: +1-973-884-4794
Sales Email: sales@aicipc.com
Support Email: support@aicipc.com

Houten, The Netherlands

Address: Peppelkade 58, 3992AK, Houten, The Netherlands
Tel: +31-30-6386789
Fax: +31-30-6360638
Sales Email: sales@aicipc.nl
Support Email: support@aicipc.com

Appendix

Ports Usage

Port #	Owner Module	Usage
80	Web server(webgo/ lighttpd)	Listening for network connections on HTTP://
443	Web server(webgo/ lighttpd)	Listening for secured network connections on HTTPS://
23	Telnet	Telnet session
5120	CD media server	To accept regular CD media redirection connections
5124	CD media server	To accept secure (SSL based) CD media redirection connections
5123	HDmedia server	To accept regular HD media redirection connections
5127	HDmedia server	To accept secure (SSL based) HD media redirection connections
7578	KVM server (adviser)	To accept regular KVM redirection connections
7582	KVM server (adviser)	To accept secure (SSL based) KVM redirection connections
623	IPMI	LAN interface
1900	uPnP discovery	Used for uPnP based BMC discovery
50000	uPnP discovery	Used for uPnP based BMC discovery
427	SLPD	Service Locater
123	NTP	Network Time Protocol (NTP) - used for time synchronization (UDP Connection)
161	SNMP	SNMP listens on this port for incoming SNMP requests. (UDP)
199	SNMP	SNMP listens on this port for incoming connect requests (from the SMUX peers and various other TCP end-points connected to SMUX peers to exchange SMUX PDUs)
546	DHCPv6	DHCPv6 clients listen for DHCP messages on this port (UDP)

Mouse Mode

Host OS	Mouse Mode
Windows Server 2016 Standard (exclude Nano Server)	Absolute
Windows Server 2012 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

NOTE
AMI MegaRAC® SP-X suggests users to use Linux version of OS except SUSE 11.4 with BMC to avoid mouse sync issue in absolute mouse mode. Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.

KVM Sharing Scenario

KVM Client	KVM	Vmedia(Jviewer)	VMCLI
Client 1 (Full Privilege)	Connected	Allowed	Allowed
Client 2 (Partial Privilege)	Connected	Not Allowed	Not Allowed

VMedia Sharing Scenario

NOTE
If MULTIPLE_USER_VMEDIA feature is disabled, then only one VMedia client can redirect media at a time. In the following table, KVM represents the video and JViewer/H5Viewer represents the media redirection from the JViewer/H5Viewer client.

Scenario 1:

KVM Client	KVM	JViewer/ H5Viewer Media	VMapp	VMCLI
Client 1	Connected	Connected	Not Allowed	Not Allowed
Client 2 (Partial Privilege)	Connected	Not Allowed		

Scenario 2:

KVM Client	KVM	JViewer/ H5Viewer Media	VMapp	VMCLI
Client 1 (Partial Privilege)	Connected	Not Allowed	Not Allowed	Not Allowed
Client 2 (Partial Privilege)	Connected	Connected		

Scenario 3:

KVM Client	KVM	JViewer/ H5Viewer Media	VMapp	VMCLI
Client 1 (Partial Privilege)	Connected	Not Allowed	Connected	Not Allowed
Client 2 (Partial Privilege)	Connected	Not Allowed		

Scenario 4:

KVM Client	KVM	JViewer/ H5Viewer Media	VMapp	VMCLI
Client 1 (Partial Privilege)	Connected	Not Allowed	Not Allowed	Connected
Client 2 (Partial Privilege)	Connected	Not Allowed		

Default IPMI Channel Numbers

Interface	Channel Number
Primary LAN Channel	0x01
Secondary LAN Channel	0x08
Serial Channel	0x02
Primary IPMB Channel	0x00
Secondary IPMB Channel	0x06
Third IPMB Channel	0x0a
System Interface	0x0f
SMM Interface	0x05

Secured Communication

- AD, LDAP, RADIUS based user authentication support
- Local IPMI user based authentication support
- Role/Privilege based authentication for each user for extra security
- Encrypted password support for AD/LDAP server authentication
- Single port access support for web/KVM/vMedia for enhanced security
- IPMI – Cipher suites support
- System Firewall support for IP/port level or IP/port range based blocking
- IPMI command/sub-command level firewall support
- TSIG authentication support for DNS controlled/seured access to the server
- SMTP-AUTH support
- OpenSSL based encryption – Latest OpenSSL 1.0.1 supported
- Key based Feature licensing/access support
- Secured handshaking support across concurrent KVM client sessions for

Service Listings

Service	User Authentication	Encryption
Web	Yes	Openssl
KVM	Yes	Openssl
vMedia	Yes	Openssl
Standalone KVM Client	Yes	Openssl
Standalone vMedia client	Yes	Openssl
SSL based SOL	Yes	Openssl
SNMP (v3)	Yes	SHA,MD5,AES,DES
SSH	Yes	Openssl
IPMI	Yes	Please refer list of supported cipher suites
YAFUFLASH (Out of band)	Yes	Please refer list of supported cipher suites
Standalone vMedia client	Yes	Openssl
SSL based SOL	Yes	Openssl
SNMP (v3)	Yes	SHA,MD5,AES,DES
SSH	Yes	Openssl
IPMI	Yes	Please refer list of supported cipher suites
YAFUFLASH (Out of band)	Yes	Please refer list of supported cipher suites

List of supported cipher suites in IPMI

ID	Authentication Algorithm	Integrity Algorithm	Confidentiality Algorithm
0	RAKP – NONE	NONE	NONE
1	RAKP-HMAC- SHA1	NONE	NONE
2	RAKP-HMAC- SHA1	HMAC-SHA1-96	NONE
3	RAKP-HMAC- SHA1	HMAC-SHA1-96	AES-CBC-128
6	RAKP-HMAC- MD5	NONE	NONE
7	RAKP-HMAC- MD5	HMAC-MD5-128	NONE
8	RAKP-HMAC- MD5	HMAC-MD5-128	AES-CBC-128
11	RAKP-HMAC- MD5	MD5-128	NONE
12	RAKP-HMAC- MD5	MD5-128	AES-CBC-128
15	RAKP_HMAC_ SHA256	NONE	NONE
16	RAKP_HMAC_ SHA256	HMAC-SHA256-128	NONE
17	RAKP_HMAC_ SHA256	HMAC-SHA256-128	AES-CBC-128