IPMI Configuration Guide

Published June 2018

AST2500 V1.04

TABLE OF CONTENTS

1. Introduction

The User Guide is for system administrators to remotely access computers with BMC (Baseboard Management Controllers) and IPMI (Intelligence Platform Management Interface). System administrators may easily monitor system conditions or manage issues of remote computers via the web-based interface, a web browser on the Internet.

***Note**: All screenshots in this document are provided for illustrative purpose only, and may be different from the actual product.*

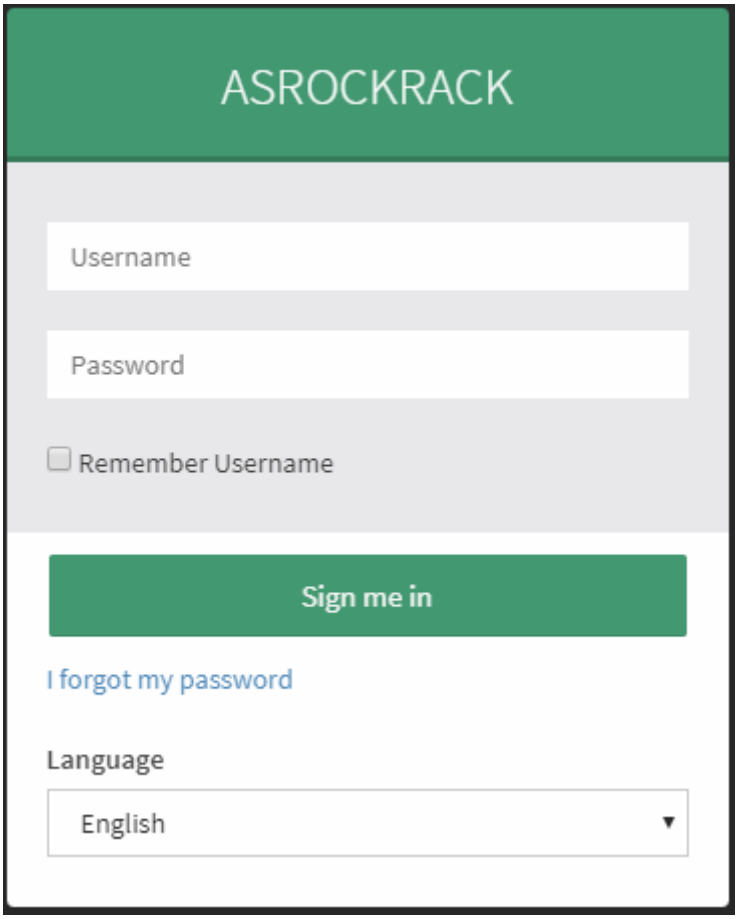
Terminology

Abbreviation	Definition
AD	Active Directory
BIOS	Basic Input Output System
BMC	Baseboard Management Controller
DHCP	Dynamic Host Configuration Protocol
DIMM	Dual-Inline-Memory-Modules
FRU	Field Replaceable Unit
FQDN	Fully Qualified Domain Name
IPMI	Intelligent Platform Management Interface
KVM	Keyboard, Video, and Mouse
LDAP	Lightweight Directory Access Protocol
ME	Intel Management Engine
NCSI	Network Controller Sideband Interface
NTP	Network Time Protocol
PEF	Platform Event Filter
POST	Power On Self-Test
PSU	Power Supply Unit
RADIUS	Remote Authentication Dial In User Service
SEL	System Event Log
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSL	Secure Sockets Layer
TSIG	Transaction Signature
VLAN	Virtual Local Area Network

2. HTML5 Web GUI

Logging in to Web using IPMI user

In order to login the IPMI, you must have a valid Username and a Password. Both fields are required.



Login Page

The default username and password are both “admin”. It is recommended to change the username and password after your first login.

Username: Enter your username in this field.

Password: Enter your password in this field.

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

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

I Forgot my Password: If you forget your password, you can generate a new one using this link. Enter the username, click on **Forgot Password** link. This will send the newly generated password to the configured Email-ID for the user.

Language: Select the language of Web GUI, you can choose English, Traditional Chinese or Simplified Chinese.

Logging in to Web using SSL mutual authentication

You can also login to the IPMI via SSL mutual authentication without entering username/password.

Before you login as SSL mutual authentication, ensure that:

1. Upload CA certificate(.pem), server certificate(.pem) and server private key(.pem) to BMC
2. Install the client certificate(.p12) into the browser
   - **Chrome**: Using "//settings/" to open Manager certificates to import the certificate.
   - **IE11:** Using "Tools>Internet Options>Certificates" to import the certificate.
   - **Firefox:** Using "Tools > Options > Advanced > Certificates" to import the certificate.
3. Login to IPMI using the link *https://[IP address]:[mutual port number]*.

Note:

1. *The default mutual port number is 4433, you can modify it in **Services** page.*
2. *If you want to generate SSL certificate by yourself, please follow the steps below.*
   - *Install OpenSSL in your Linux machine.*
   - *Generate CA certificate:*
     (1) *Type **openssl genrsa -out ./private/ca.key 1024** to generate private key*
     (2) *Type **openssl req -new -x509 -days 365 -key ./private/ca.key -out ./certs/ca.crt** to generate certificate file(contain public key)*
     (3) *Type **cat ./certs/ca.crt > ./certs/ca.pem** to transfers the file format to .pem.*
   - *Generate server certificate:*
     (1) *Type **openssl genrsa -out ./private/server.key 1024** to generate server key.*
     (2) *Type **openssl req -new -key ./private/server.key -out ./certs/server.csr** to generate csr file.*
     (3) *Type **openssl x509 -req -days 365 -in ./certs/server.csr -CA ./certs/ca.crt -CAkey ./private/ca.key -set_serial 01 -out ./certs/server.crt** to sign the file and generate server certificate*
     (4) *Type **cat ./certs/server.crt > ./certs/server.pem** to transfers the file format to .pem.*
     (5) *Type **cat ./private/server.key > ./private/server_key.pem** to transfers the file format to .pem.*
   - *Generate client certificate:*
     (1) *Type **openssl genrsa -out ./private/client.key 1024** to generate client key.*
     (2) *Type **openssl req -new -key ./private/client.key -out ./certs/client.csr** to generate csr file.*
     (3) *Type **openssl x509 -req -days 365 -in ./certs/client.csr -CA ./certs/ca.crt -CAkey ./private/ca.key -set_serial 02 -out ./certs/client.crt** to sign the file and*

generate server certificate.

(4) *Type **cat ./certs/client.crt > ./certs/client.pem** to transfers the file format to .pem.*

(5) *Type **cat ./private/client.key >> ./certs/client.pem** to export the file..*

- *Type **openssl pkcs12 -export -in ./certs/client.crt -out ./certs/client.p12 –name "Client Name" -inkey ./private/client.key** to transfers client certificate format to p12 for browser.*

System Requirements

- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be lag in Video/keyboard/mouse functionality.

Supported Browsers

- Chrome latest version.
- IE11 and above.
- Firefox (with limited support).

Note:

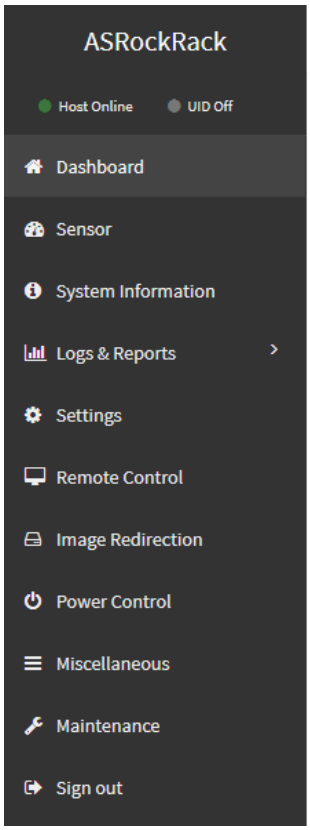
1. *It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations.*
2. *Some icons may not appear on the interface with the IE browser.*
3. *Once you login to the application, it is recommended not using the following options.*
    - *Refresh button of the browser*
    - *Refresh menu of the browser*
    - *Back and Forward options of the browser*
    - *F5 on the keyboard*
    - *Backspace on the keyboard*

3. Web GUI Overview

3.1 Menu bar

The menu bar displays the following items.

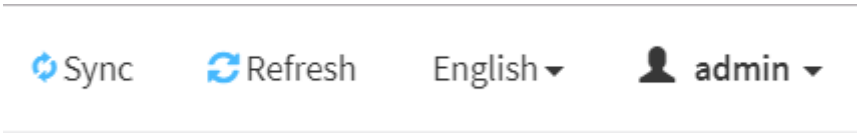
- Power Status / UID Status
- Dashboard
- Sensor
- System Information
- Logs & Reports
- Settings
- Remote Control
- Image Redirection
- Power Control
- Miscellaneous
- Maintenance
- Sign out



Menu bar

3.2 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the Web GUI.

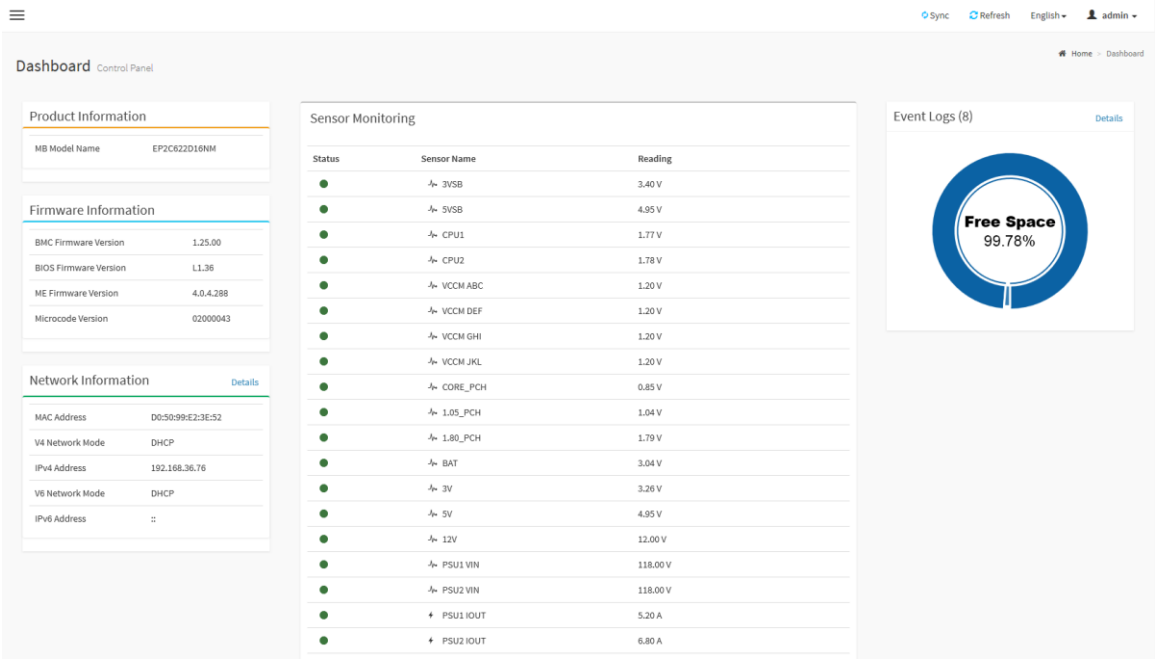


Quick Button and User Information

Sync: Click the button to synchronize with latest chassis state.
Refresh: Click the button to reload the current page.
Language: Click the option to change the language (English, Traditional Chinese or Simplified Chinese) for Web GUI.
User Information: This option shows the logged-in user name and privilege. Click **Profile** to view more information. Click the **Sign out** to log out of the Web GUI.

3.3 Dashboard

The Dashboard displays the overall information about the status of the device.



Dashboard Page

Firmware Information

The Firmware Information displays the following information.
BMC Firmware Version: Displays the BMC firmware version of the device.
BIOS Firmware Version: Displays the BIOS firmware version of the device.

ME Firmware Version: Displays the ME (or PSP) firmware version of the device.
Microcode Version: Displays the microcode version of the device.
CPLD Version: Displays the version of CPLD of the device.

Note:

BIOS version, ME (or PSP) version and Microcode version will be refreshed when the system POST, please restart the system if you see nothing on screen.

Network Information

The Network Information of the device with the following fields is shown here. Click **Details** to view more information.
MAC Address: Read-only field shows the MAC address of the device.
V4 Network Mode: The v4 network mode of the device can be either static or DHCP.
IPv4 Address: The IPv4 address of the device can be static or DHCP.
V6 Network Mode: The v6 network mode of the device can be either static or DHCP.
IPv6 Address: The IPv6 address of the device can be static or DHCP.

Sensor Monitoring

Here lists all the available sensors on the device with the following information.
Status: This column displays the state of the device.

 - Normal state

 - Critical State

 - Not Available

Sensor Name: Displays the name of the sensor.
Reading: Displays the value of sensor readings.

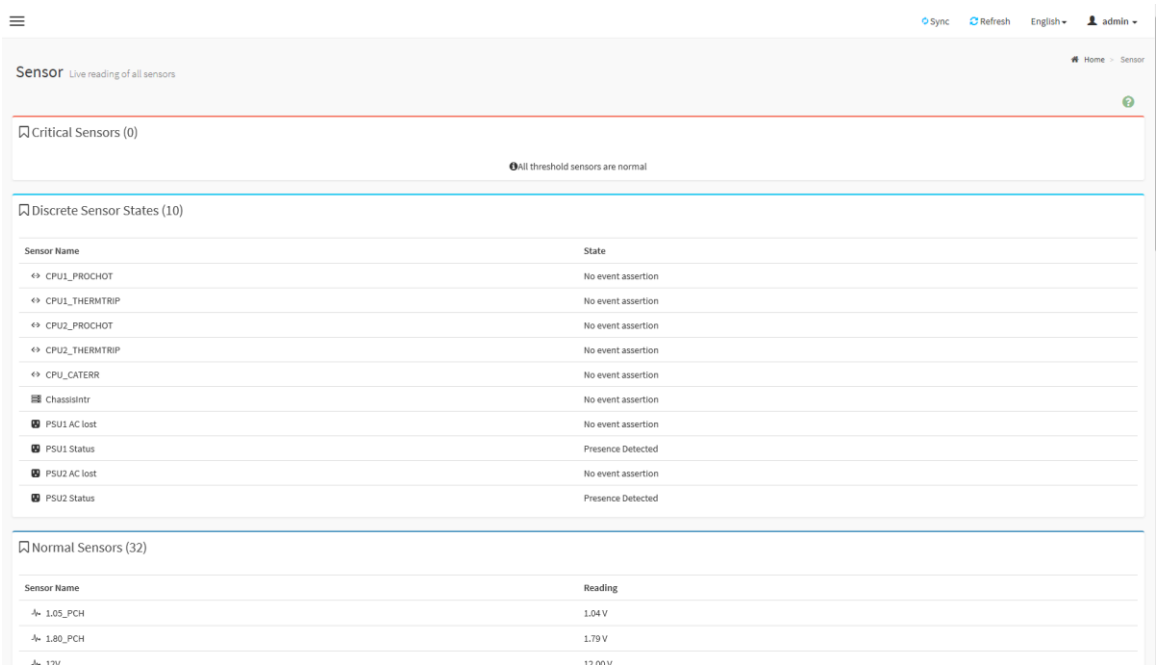
Event Logs

Here displays a graphical representation of all events and occupied/available space in logs. Click **Details** to view more information.

3.4 Sensor

The Sensor Readings page displays all the sensor related information.
To open the Sensor Readings 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.

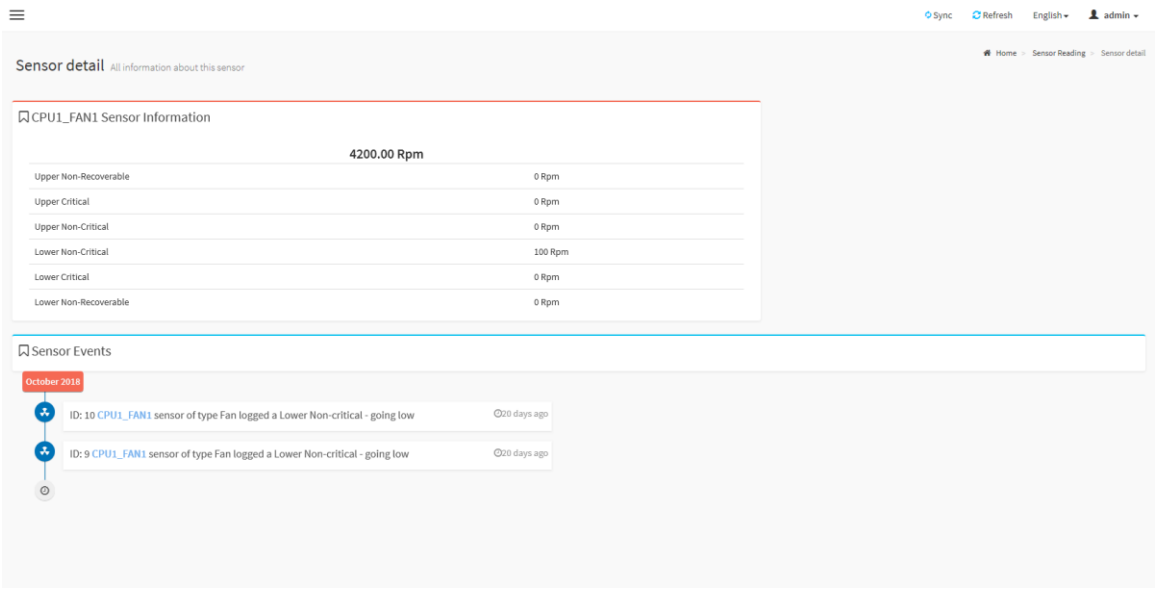


Sensor Page

In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status and Current Reading are shown.

Sensor detail:

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



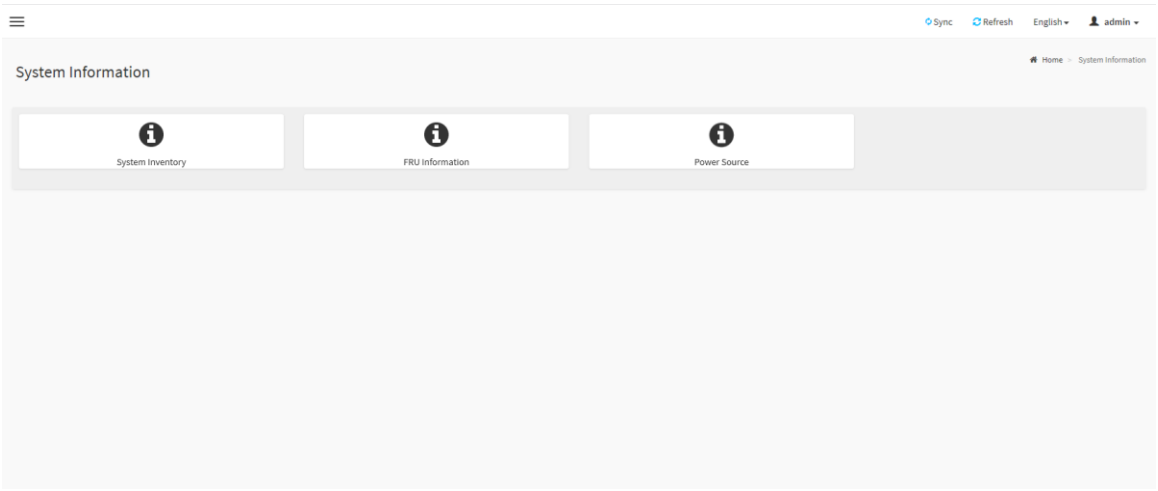
Sensor detail Page

Types of the thresholds:

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

3.5 System Information

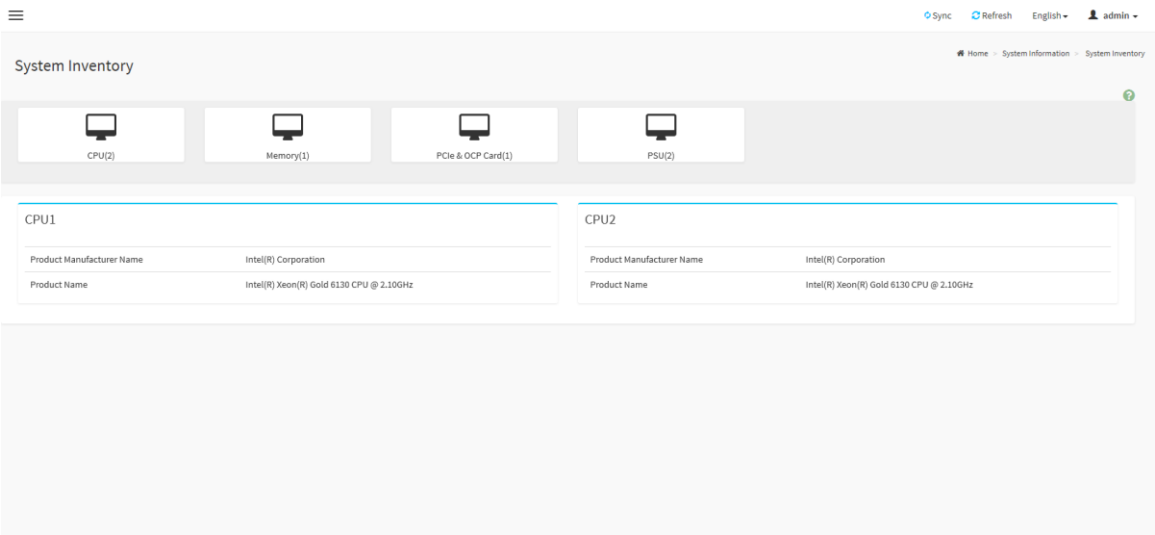
This group of pages allows you to views system information.



System Information Page

3.5.1 System Inventory

This page displays detailed information of active devices. Select a group to view more information.



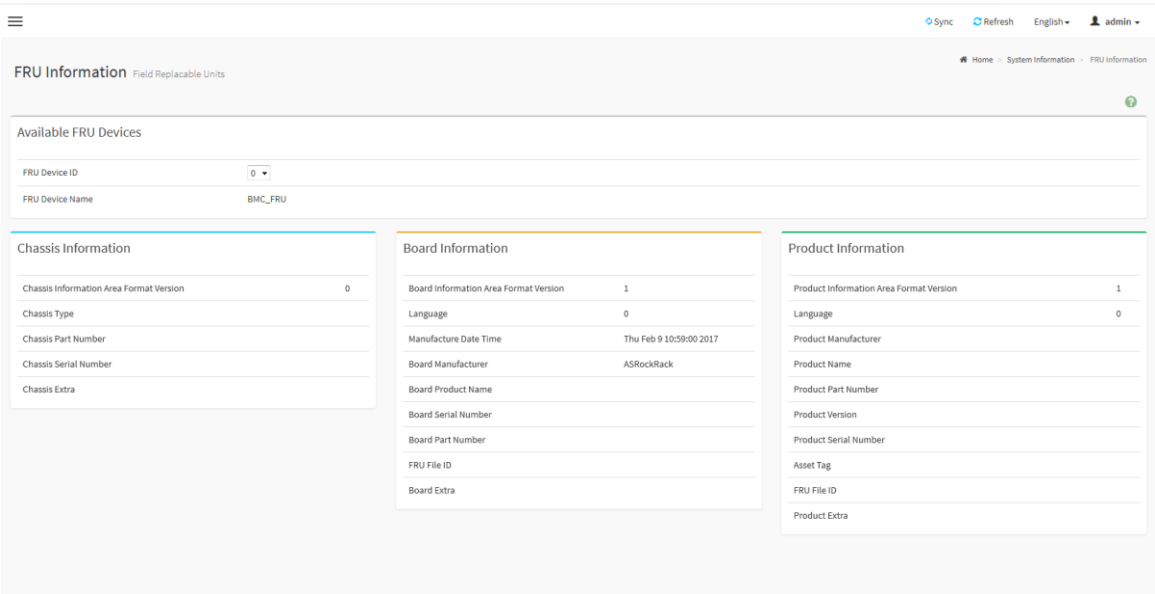
System Inventory Page

Note:

1. *The information will be refreshed when the system POST, please restart the system if you see nothing on screen.*
2. *The information on this page may differ by platforms, and this page may not be available for certain platforms.*

3.5.2 FRU Information

This page displays the FRU information. Select a FRU Device ID from the FRU Information section to view the details of the selected device.



FRU Page

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

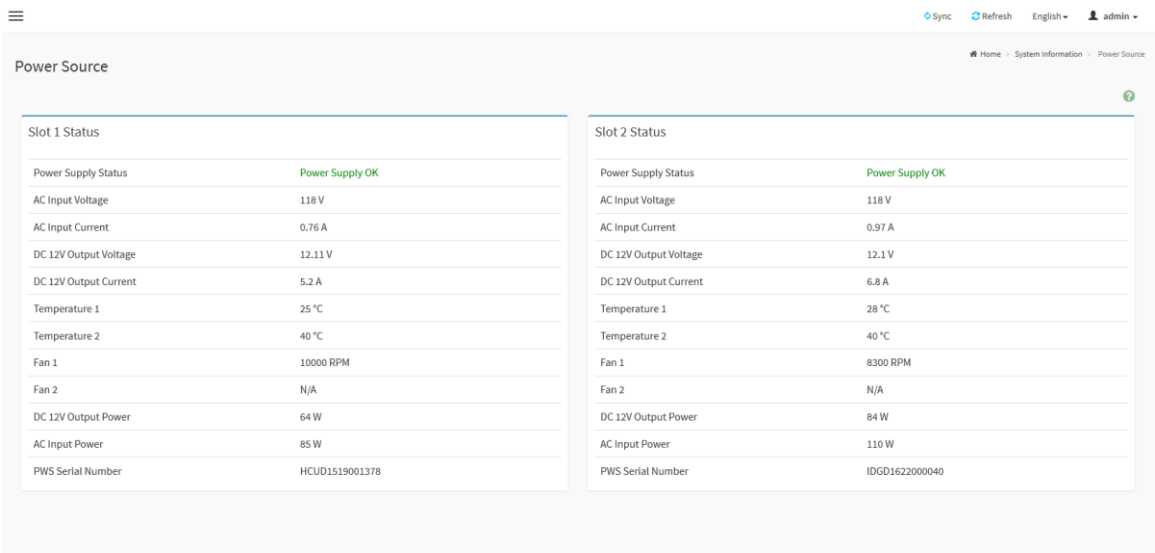
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

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

3.5.3 Power Source

This page displays the PSU information. Please make sure that the PSU supports PMBus.



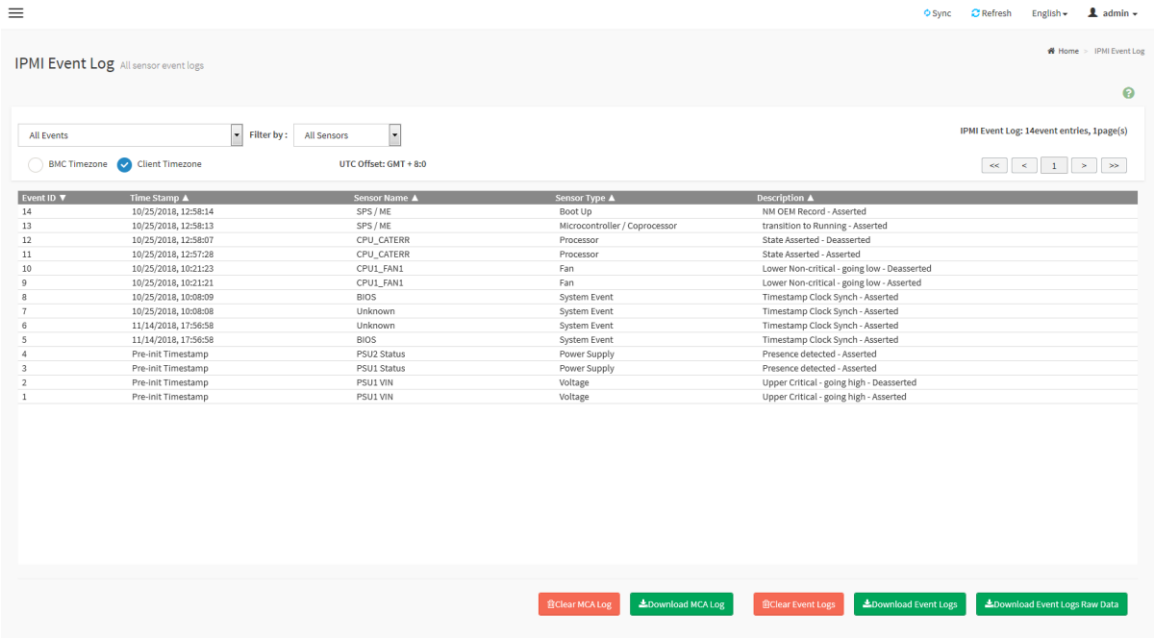
Power Source Page

Power Supply Status: Displays the PSU status is normal or not.
AC Input Voltage: Displays the input voltage of the PSU.
AC Input Current: Displays the input current of the PSU.
DC 12V Output Voltage: Displays the output voltage of the PSU.
DC 12V Output Current: Displays the output current of the PSU.
Temperature 1: Displays the temperature 1 of the PSU.
Temperature 2: Displays the temperature 2 of the PSU.
Fan 1: Displays the fan speed 1 of the PSU.
Fan 2: Displays the fan speed 2 of the PSU.
DC 12V Output Power: Displays the output power of the PSU.
AC Input Power: Displays the input power of the PSU.
PWS Serial Number: Displays the serial number of the PSU.

3.6 Logs & Reports

3.6.1 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.

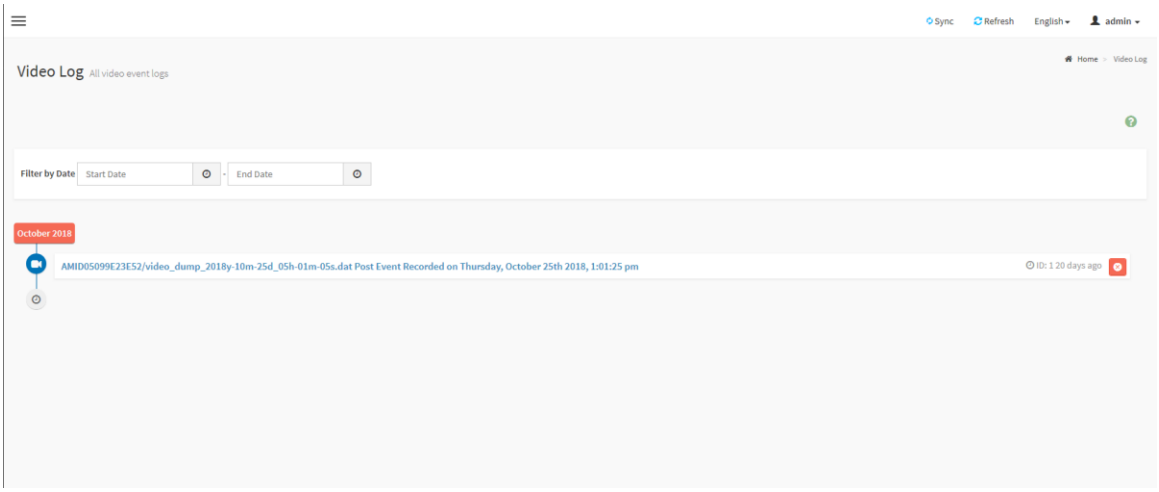


IPMI Event Log Page

Filter By Type: The category can be 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, or Terminal Mode Remote Console software Events.
Filter By Sensor: Filtering can be done with the sensors mentioned in the list.
BMC Timezone: Displays the events with BMC UTC Offset timestamp.
Client Timezone: Displays the events with Client UTC Offset timestamp.
UTC Offset: Displays the current UTC Offset value based on which event Time Stamps will be updated.
Clear MCA Log: To delete MCA log.
Download MCA Log: To download the existing MCA log.
Clear Event Logs: To delete all the event logs.
Download Event Logs: To download all the existing Event Log records as text file.
Download Event Logs Raw Data: To download all the existing Event Log records as hex format file.

3.6.2 Video Log

This page displays the list of video logs occurred by the different events on this device.

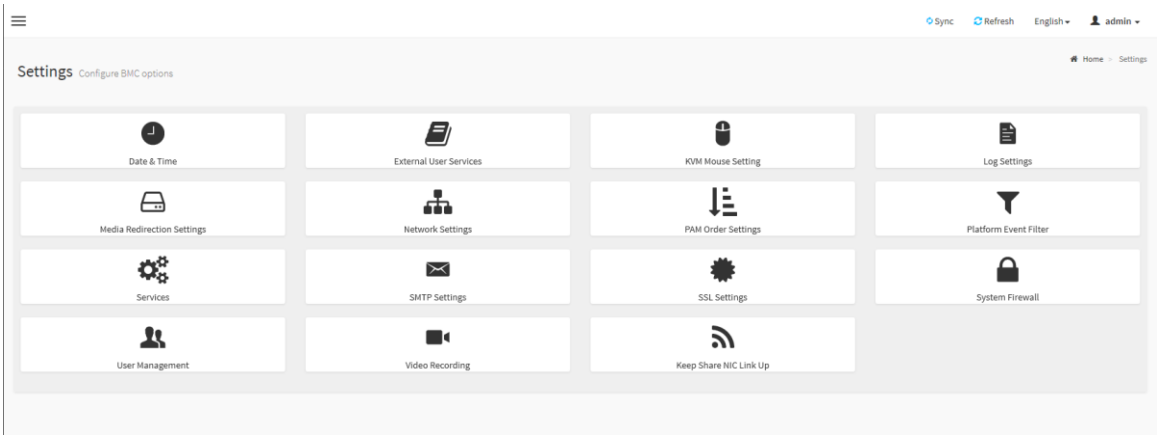


Video Log Page

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

3.7 Settings

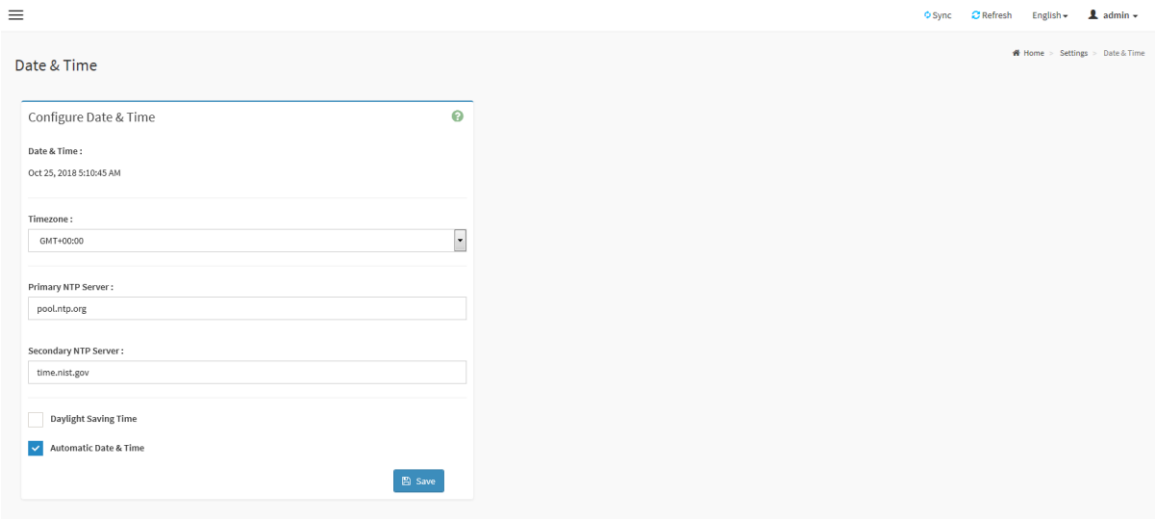
This group of pages allows you to access various configuration settings.



Settings Page

3.7.1 Data & Time

This page allows administrator to set the date and time on the BMC. It can be used to configure either Date & Time or NTP (Network Time Protocol) server settings for the device.

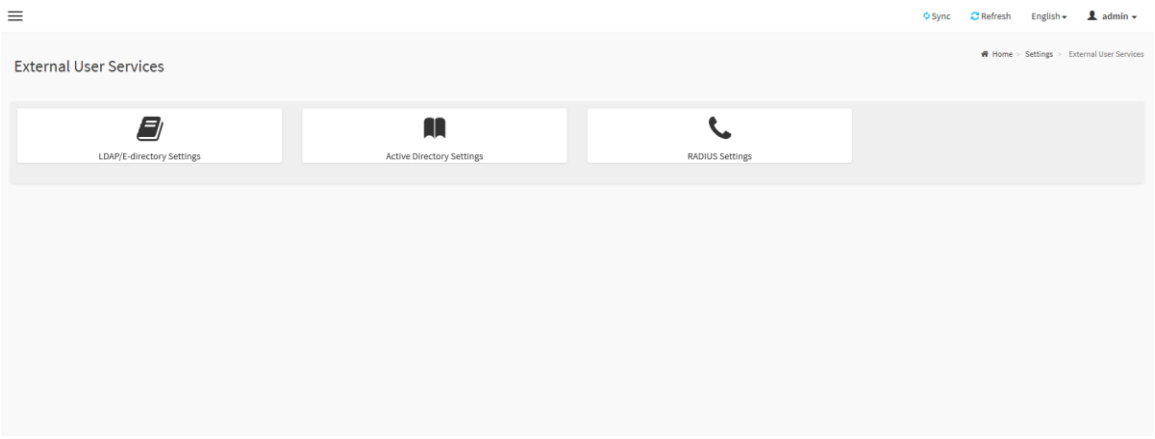


Date & Time Page

Date & Time: To specify the current date and time of the device.
Timezone: Timezone list contains the UTC offset along with the locations and Manual UTC offset for NTP server, which can be used to display the exact local time.
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.
Daylight Saving Time: Enable daylight saving time for the device.
Automatic Date & Time: To automatically synchronize Date and Time with the NTP Server.

3.7.2 External User Services

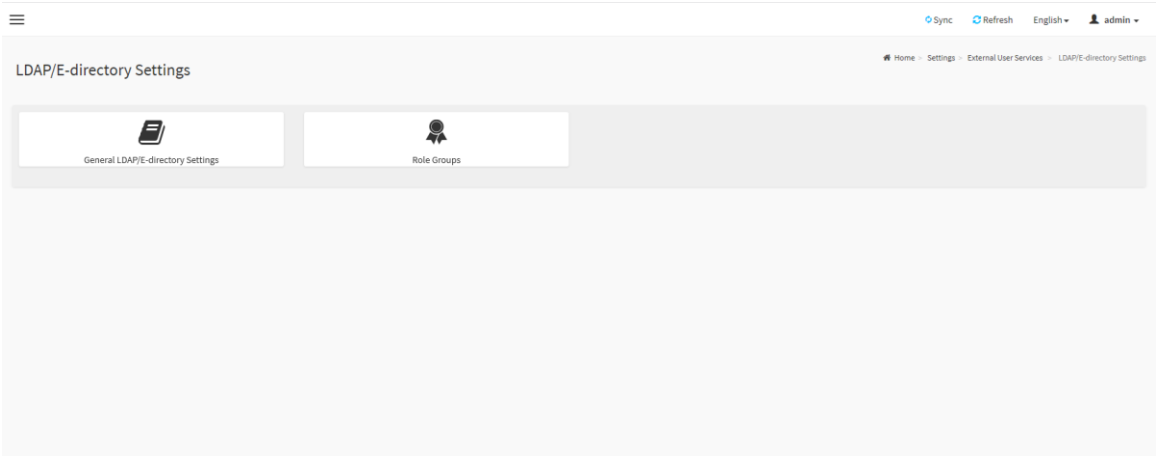
This page is used to configure the external service.



External User Services Page

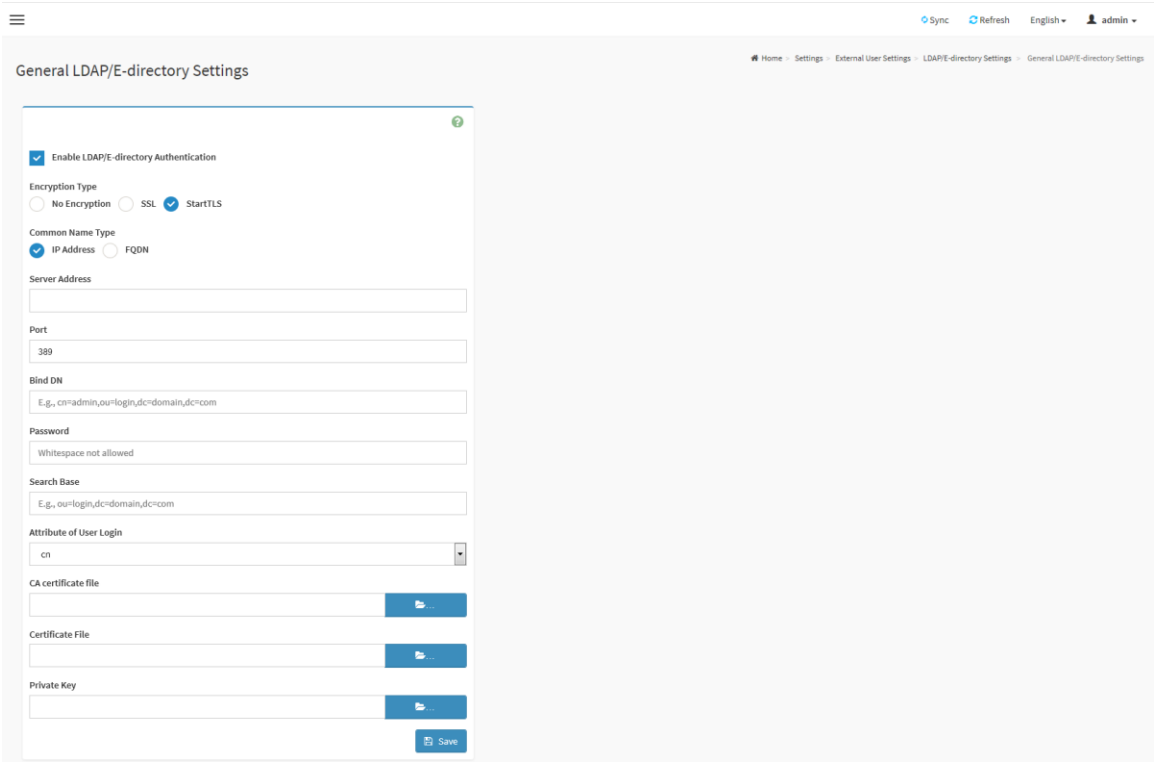
3.7.2.1 LDAP/E-directory Settings

LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate web users. This is done by passing login requests to your LDAP Server.



LDAP/E-directory Settings Page

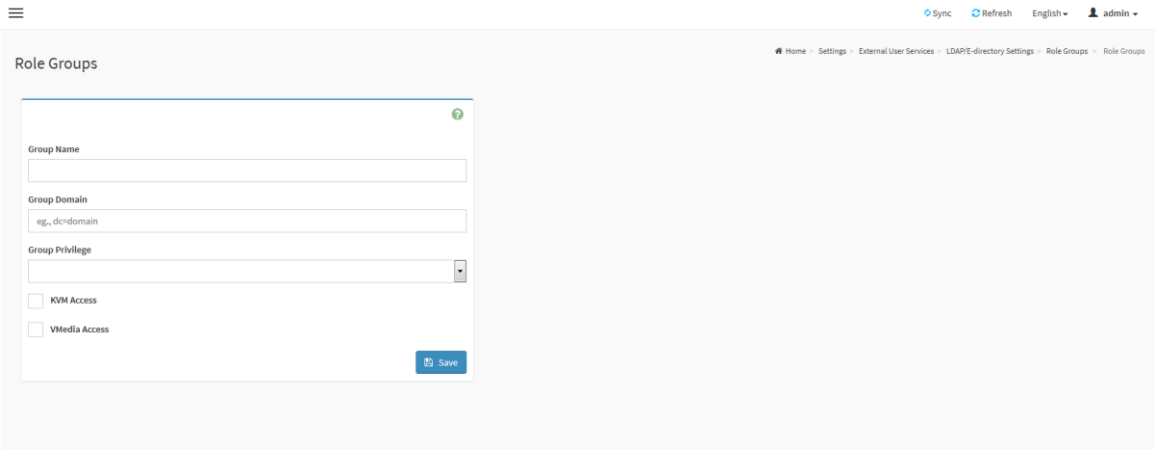
General Settings: This page is used to configure LDAP/E-Directory settings.



General Settings Page

Enable LDAP/E-Directory Authentication: Check the box to enable LDAP/E-Directory authentication.
Encryption Type: Select the encryption type for LDAP/E-Directory.
Common Name Type: Select the Common Name Type for LDAP/E-Directory.
Server Address: The IP address(IPv4 or IPv6) of LDAP/E-Directory server.
Port: The port of LDA/E-Directory server.
Bind DN: The **Bind DN** is used during bind operation, which authenticates the client to the server.
Password: The password of LDA/E-Directory server.
Search Base: The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.
Attribute of User Login: To find the LDAP/E-Directory server which attribute should be used to identify the user.
CA Certificate File: To identify the certificate of the trusted CA certs.
Certificate File: To find the client certificate filename.
Private Key: To find the client private key filename.

Role Groups: This page is used to add a new role group to the device. Alternatively, double click on a free slot to add a role group.

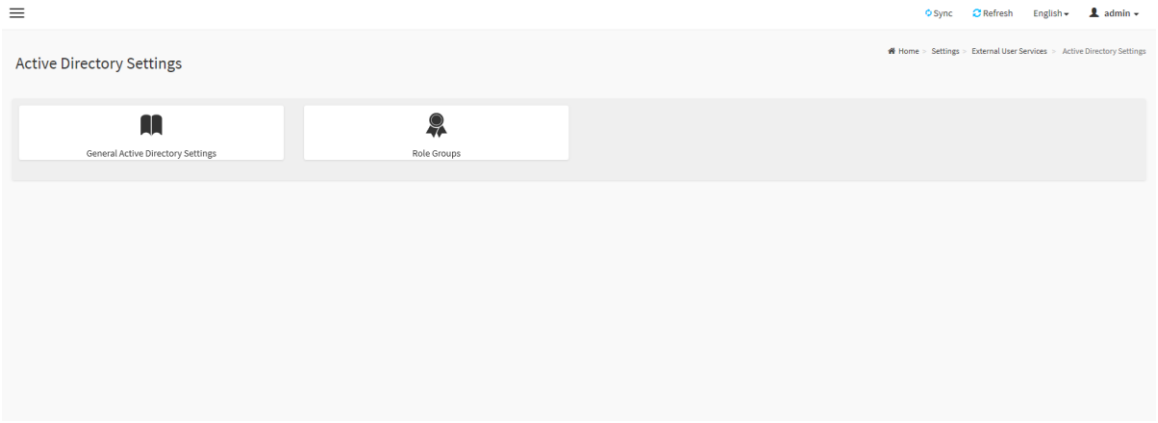


Role Groups Page

Group Name: Enter the name that identifies the role group.
Group Domain: Enter the Role Group Domain where the role group is located.
Group Privilege: Enter the level of privilege (User, Administrator, Operator, OEM, None) to assign to this role group.
KVM Access: Check the box to enable KVM access for the group.
VMedia Access: Check the box to enable VMedia access for the group.

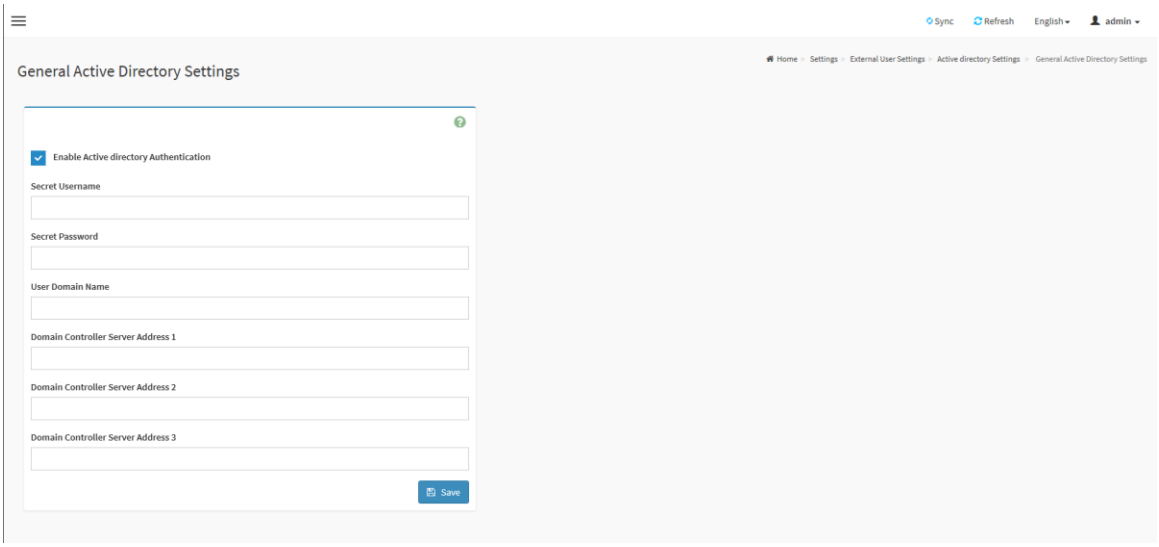
3.7.2.2 Active directory Settings

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. 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.



Active directory Settings Page

General Settings: This page is used to configure Active Directory general settings.

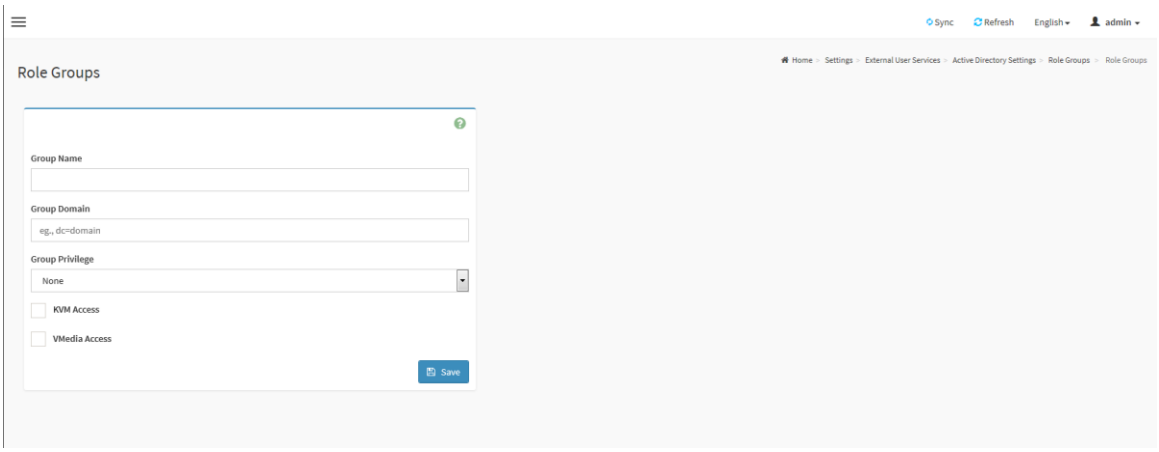


General Settings Page

Enable Active directory Authentication: Check box to enable Active Directory Authentication.

Secret User Name: The Username of the Active Directory Server.
Secret Password: The Password of the Active Directory Server.
User Domain Name: The Domain Name for the user. E.g. MyDomain.com
Domain Controller Server Address1, Domain Controller Server Address2 & Domain Controller Server Address3: The IP address of Active Directory server.

Role Groups: This page is used to add a new role group to the device. Alternatively, double click on a free slot to add a role group.

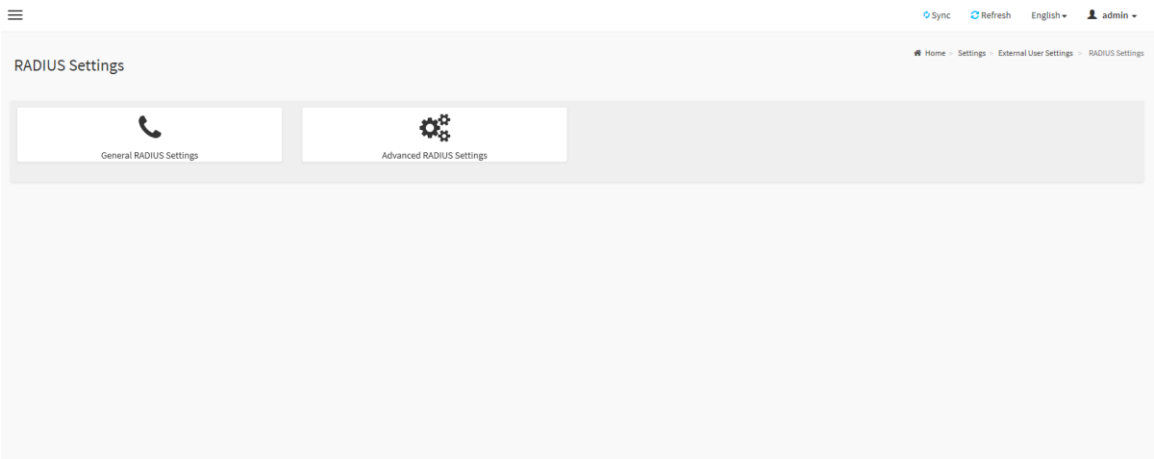


Role Groups Page

Group Name: Enter the name that identifies the role group.
Group Domain: Enter the Role Group Domain where the role group is located.
Group Privilege: Enter the level of privilege (User, Administrator, Operator, OEM, None) to assign to this role group.
KVM Access: Check the box to enable KVM access for the group.
VMedia Access: Check the box to enable VMedia access for the group.

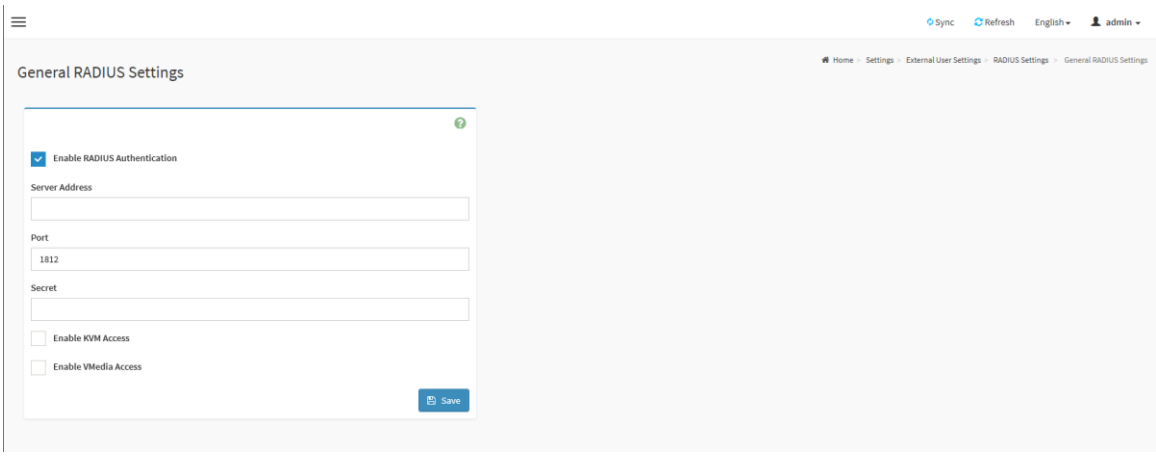
3.7.2.3 RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities. You can set the RADIUS Authentication from here.



RADIUS Settings Page

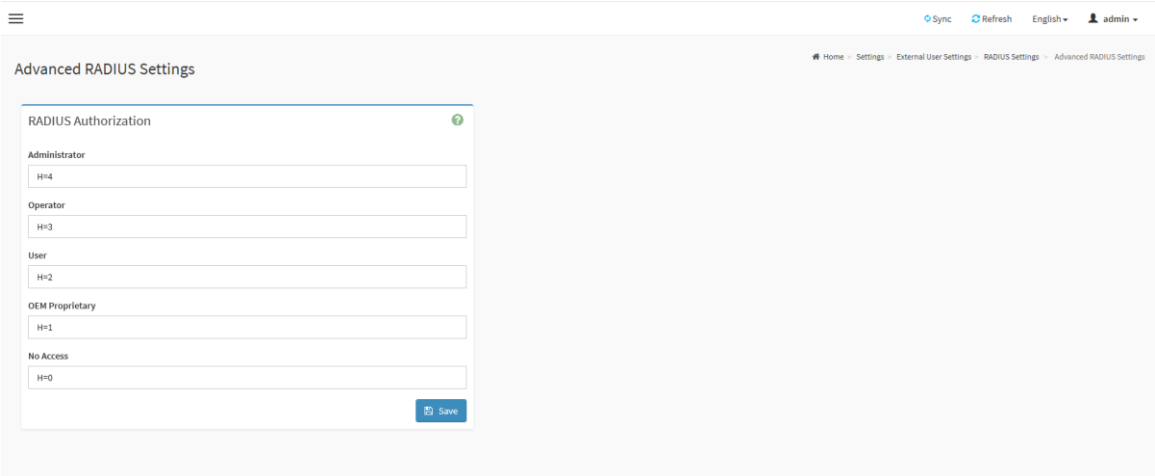
General RADIUS Settings: This page is used to configure Radius general settings.



General RADIUS Settings Page

Enable RADIUS Authentication: Check the box to enable Radius authentication.
Server Address: The IP address of Radius server.
Port: The port number of Radius server.
Secret: The authentication secret of Radius server.
KVM Access: Check the box to enable KVM access for Radius authenticated users.
VMedia Access: Check the box to enable VMedia access for Radius authenticated users.

Advanced RADIUS Settings: This page is used to configure Advanced Radius authorization setting.

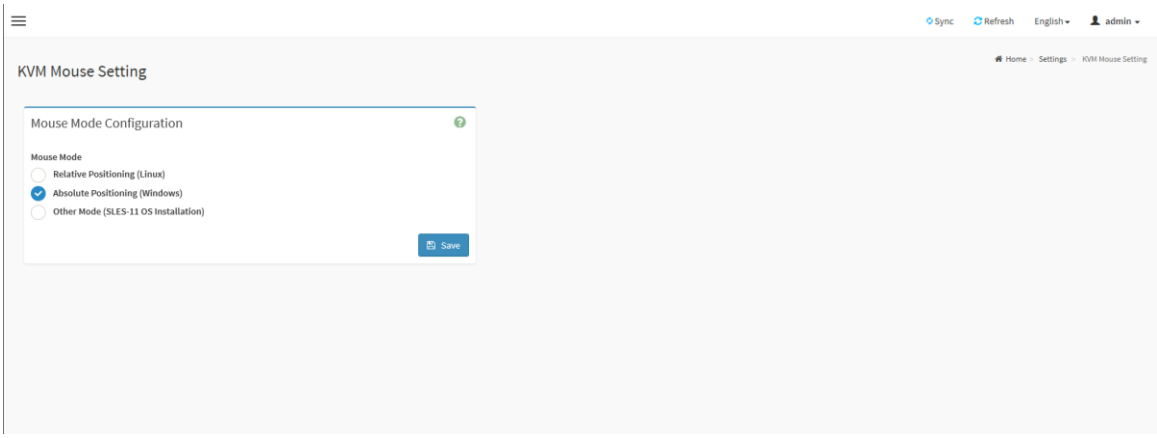


Advanced RADIUS Settings Page

Administrator: Configure Administrator with Vendor Specific Attribute in Server side.
Operator: Configure Operator with Vendor Specific Attribute in Server side.
User: Configure User with Vendor Specific Attribute in Server side.
OEM Proprietary: Configure OEM Proprietary with Vendor Specific Attribute in Server side.
No Access: Configure No Access with Vendor Specific Attribute in Server side.

3.7.3 KVM Mouse Setting

The Redirection Console handles mouse emulation from local window to remote screen in either of three methods.



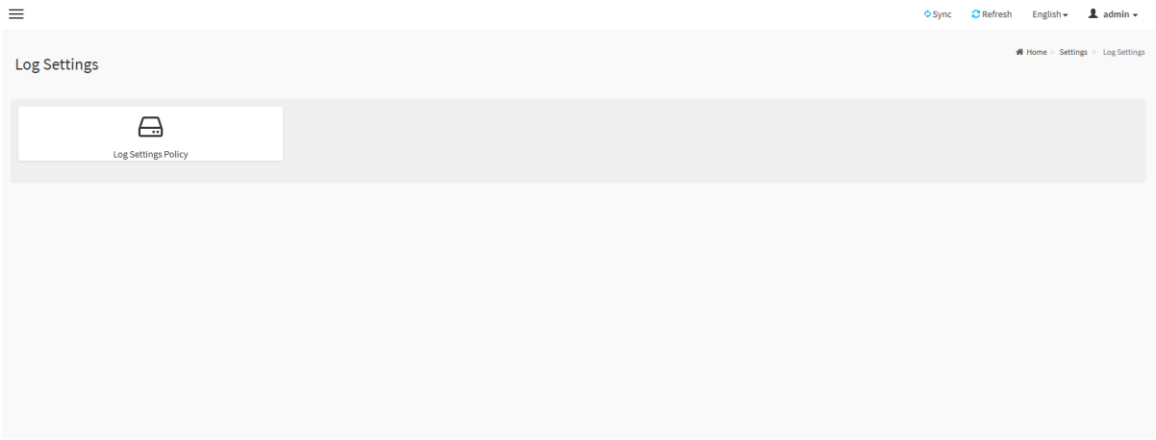
KVM Mouse Setting Page

Relative Positioning (Linux): Relative mode sends the calculated relative mouse position displacement to the server.
Absolute Positioning (Windows): The absolute position of the local mouse is sent to the server.

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

3.7.4 Log Settings

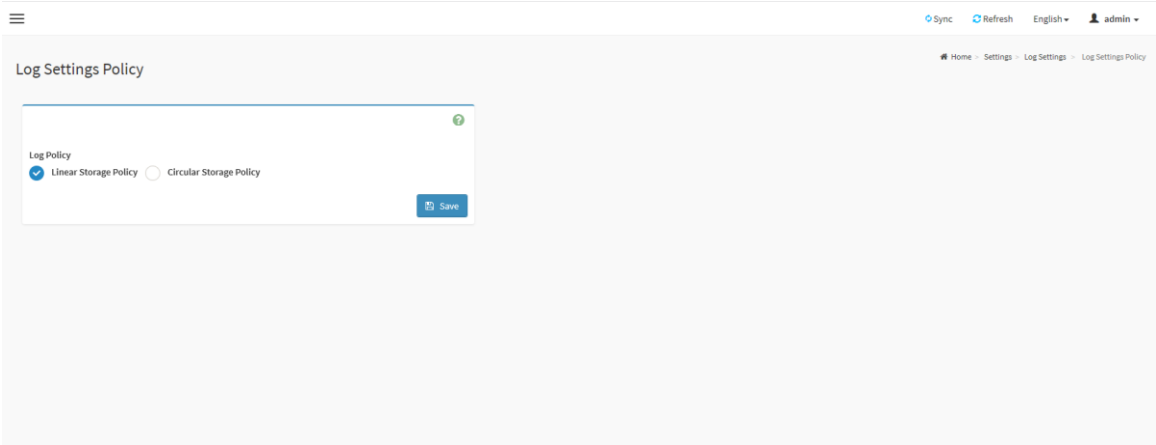
This page is used to configure the log settings.



Log Settings Page

3.7.4.1 Log Settings Policy

This page is used to configure the log policy for the event log.



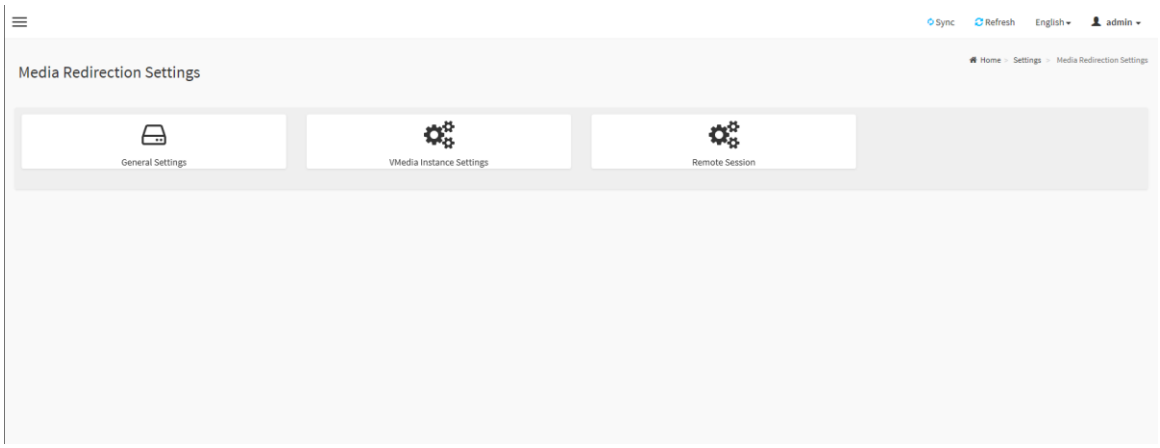
Log Settings Policy Page

Linear Storage Policy: Check the option to enable linear storage policy for the event log.

Circular Storage Policy: Check the option to enable circular storage policy for the event log.

3.7.5 Media Redirection Settings

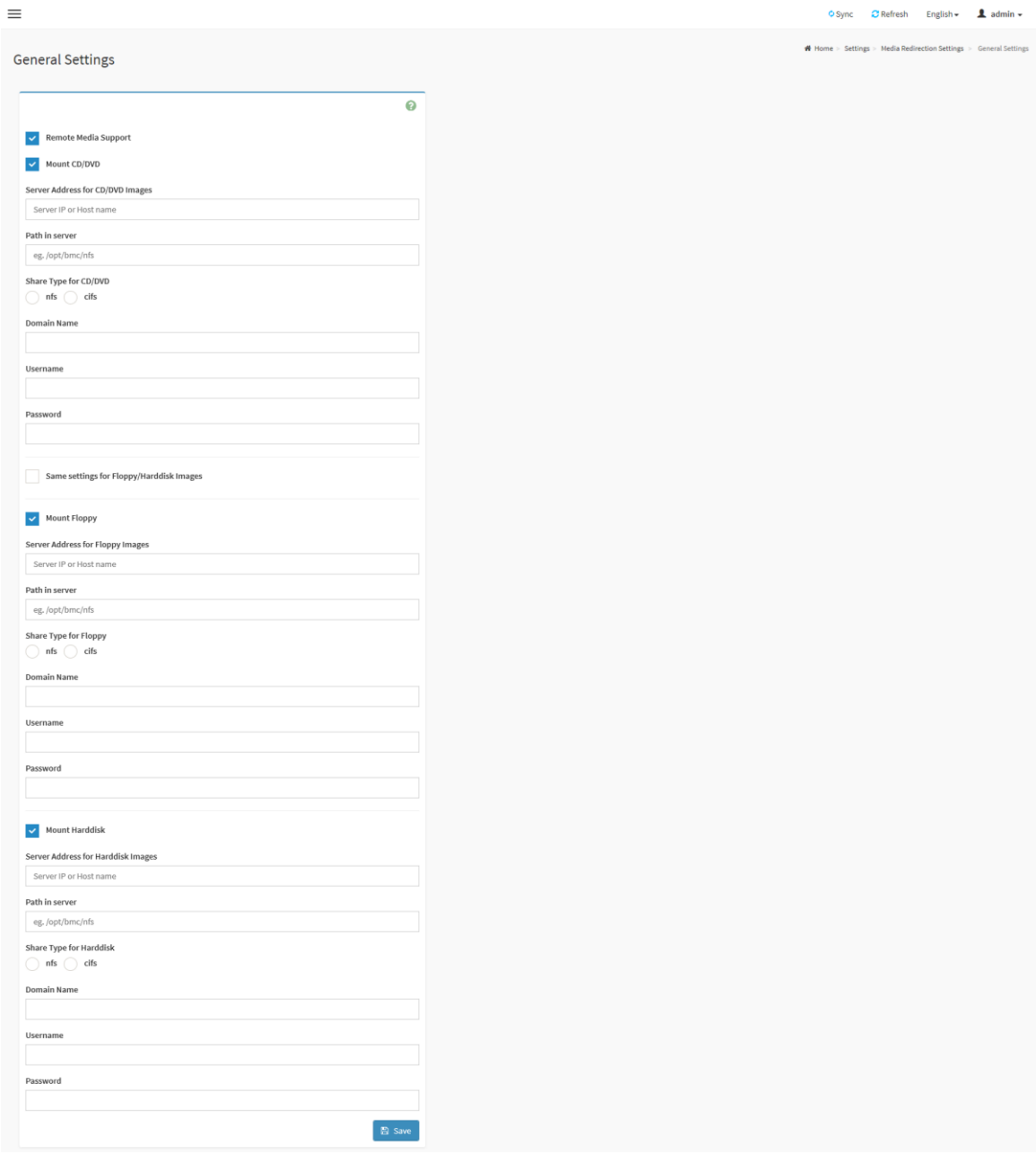
This page is used to configure the media into BMC for redirection.



Media Redirection Settings Page

3.7.5.1 General Settings

This page is used to configure general media settings.



General Settings Page

Remote Media Support: Check the box to enable Remote Media support.

Mount CD/DVD: Check the box to enable Mount CD/DVD support.

Server Address for CD/DVD Images: Displays the address of the server where the remote media images are stored.

Path in server: Displays the Source path to the remote media images.

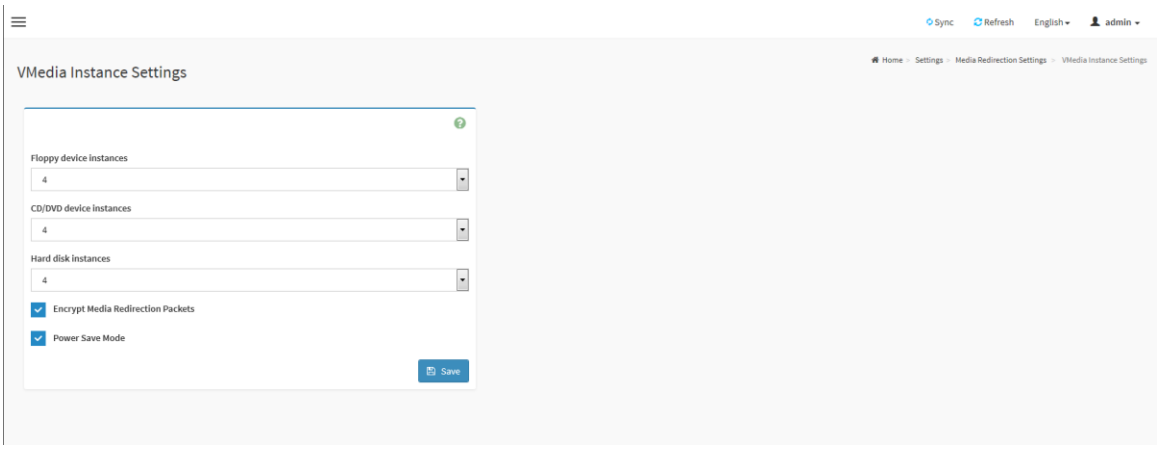
Path in server: Displays the Share Type of the remote media server either NFS or CIFS.

Domain Name: If share Type is Samba(CIFS), then enter domain name to authenticate on the server.

Username: If share Type is Samba(CIFS), then enter username to authenticate on the server.
Password: If share Type is Samba(CIFS), then enter password to authenticate on the server.
Same settings for Floppy/Harddisk Images: Enable/Disable to select same media type data configurations for all the remote media types.
Mount Floppy: Check the box to enable Mount Floppy support.
Server Address for Floppy Images: Displays the address of the server where the remote media images are stored.
Path in server: Displays the Source path to the remote media images.
Share Type for Floppy: Displays the Share Type of the remote media server either NFS or CIFS.
Mount Harddisk: Check the box to enable Mount Harddisk support.
Server Address for Harddisk Images: Displays the address of the server where the remote media images are stored.
Path in server: Displays the Source path to the remote media images.
Share Type for Harddisk: Displays the Share Type of the remote media server either NFS or CIFS.

3.7.5.2 VMedia Instance Settings

This page is used to configure virtual media device settings.



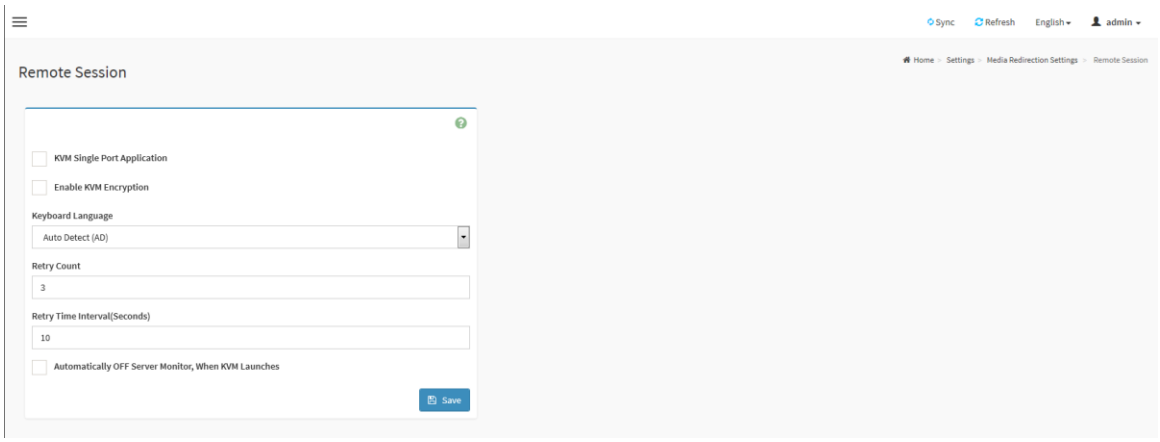
VMedia Instance Settings Page

Floppy device instances: The number of floppy devices supported for Virtual Media redirection.
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.
Encrypt Media Redirection Packets: Check the box to enable Media Encryption support.
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.

3.7.5.3 Remote Session

This page is used to configure remote session configuration settings.



Remote Session Page

KVM Single Port Application: Check the box to enable single port support when using JViewer(Java KVM). 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: Check the box to enable KVM Encryption for the next redirection session when using JViewer(Java KVM). If KVM Encryption is enabled, the KVM session will use the Secure port.
Keyboard Language: This option is used to select the keyboard supported languages for both H5Viewer(HTML5 KVM) and JViewer(Java KVM).
Retry Count: This option is used to retry the redirection session for certain number of attempts.

Retry Time Interval(Seconds): This option is used to give time interval for each attempts.

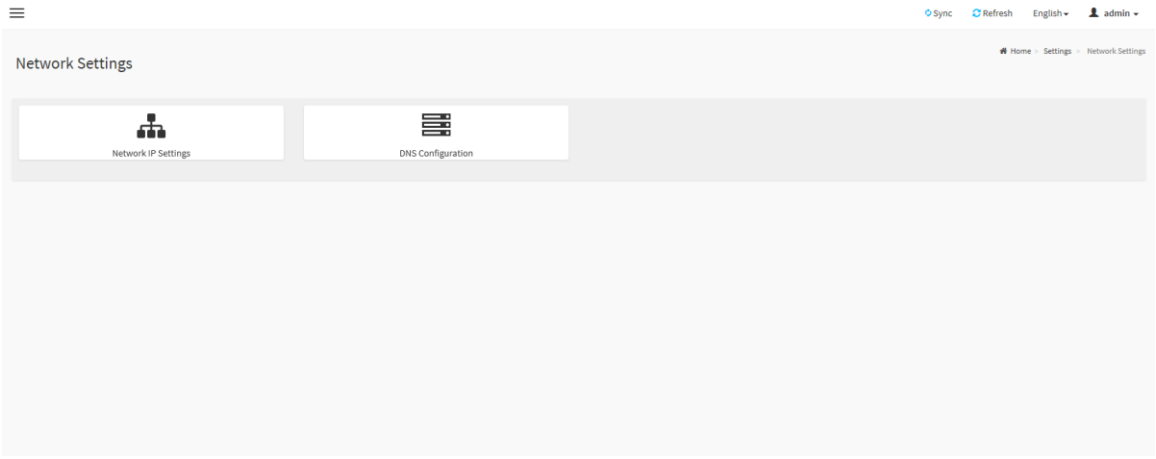
Automatically OFF Server Monitor, When KVM Launches: Check the box to enable Automatically OFF Server Monitor, When KVM Launches.

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.

3.7.6 Network Settings

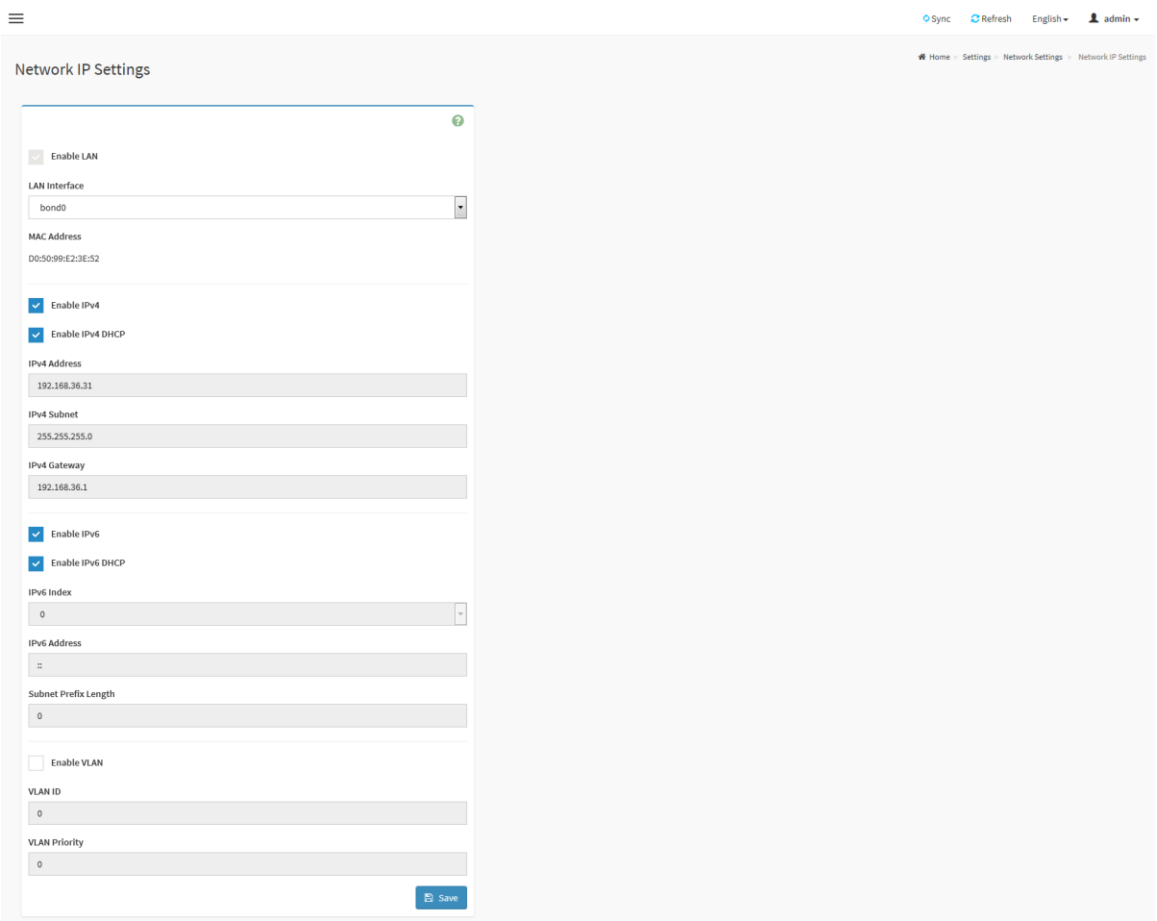
This page is used to configure the network settings for the available LAN channels.



Network Settings Page

3.7.6.1 Network IP Settings

This page is used to configure the network IP settings.



Network IP Settings Page

Enable LAN: Check the box to enable the selected channel.
LAN Interface: Lists the available LAN interfaces.
MAC Address: Displays the MAC Address of the device. This is a read-only field.
Enable IPv4: Check the box to enable the IPv4 for the selected channel.
Enable IPv4 DHCP: Check the box to enable IPv4 DHCP support for the selected channel.
IPv4 Address: Specify the static IPv4 address for the selected channel.
IPv4 Subnet Mask: Specify the static IPv4 subnet mask for the selected channel.
IPv4 Default Gateway: Specify the static IPv4 default gateway for the selected channel.
Enable IPv6: Check the box to enable the IPv6 for the selected channel.
Enable IPv6 DHCP: Check the box to enable IPv6 DHCP support for the selected channel.
IPv6 Index: Specify a static IPv6 Index to be configured for the selected channel. E.g.: 0
IPv6 Address: Specify a static IPv6 address to be configured to the device for the

selected channel. E.g.: 2004::2010

Subnet Prefix length: Specify the subnet prefix length for the IPv6 settings.

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

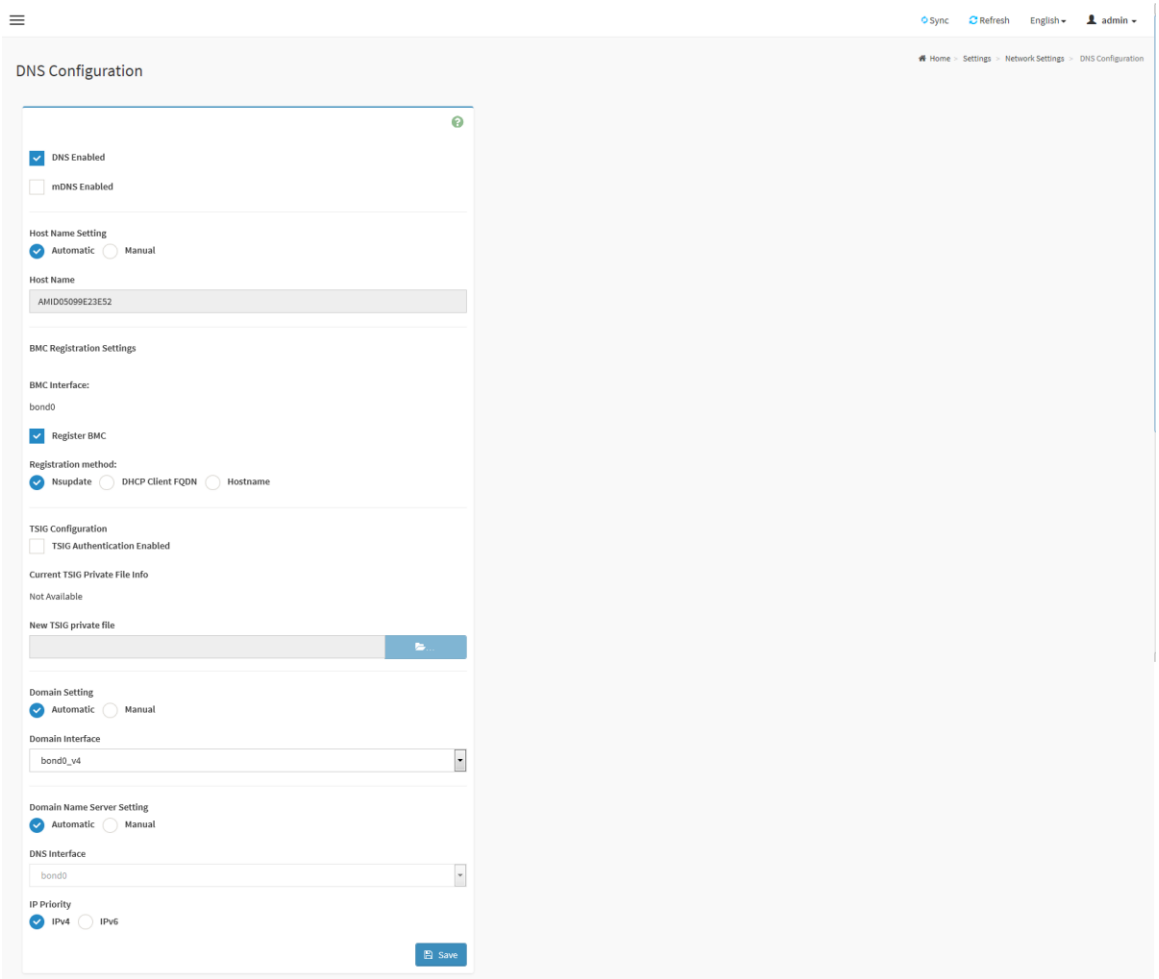
Enable VLAN: Check the box to enable the VLAN support for selected interface.

VLAN ID: The Identification for VLAN configuration.

VLAN Priority: The priority for VLAN configuration.

3.7.6.2 DNS Configuration

This page is used to manage the DNS settings.



DNS Configuration Page

DNS Enabled: Check the box to enable the DNS support.

mDNS Enable: Check the box to enable the mDNS support.

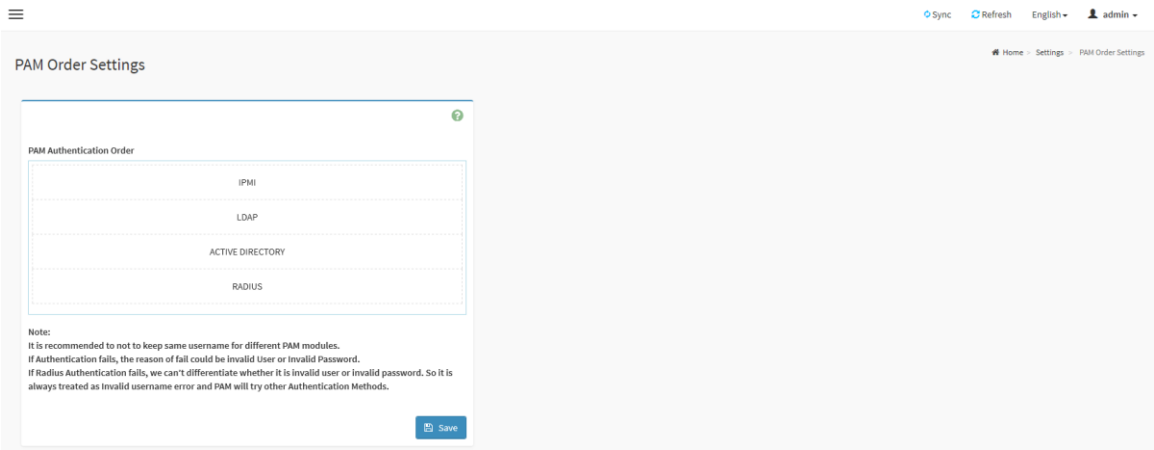
Host Name Settings: Choose either Automatic or Manual settings.

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.

BMC Interface: To register the BMC through the Interfaces.
Register BMC: To register BMC through registration method.
Registration Method: To register the BMC are through **NS Update** or **DHCP Client FQDN** or **Hostname.**
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 (read only).
New TSIG Private File: Browse and navigate to the TSIG private file, the file should be of private type.
Domain Setting: Select whether the domain interface will be configured manually or automatically.
Domain Interface: This field will be present if specify **Domain Setting** to **Automatic,** the field is used to display the domain interface of the device.
Domain Name: This field will be present if specify **Domain Setting** to **Manual,** the field is used to specify the domain name of the device.
Domain Name Server Setting: Select whether the DNS interface will be configured manually or automatically.
DNS Interface: This field will be present if specify **Domain Name Server Setting** to **Automatic**, the field is used to specify the interface to be used.
IP Priority: This field will be present if specify **Domain Name Server Setting** to **Automatic**, the field is used to select the IP Priority. If IP priority is IPv4, 2 IPv4 and 1 IPv6 DNS servers are used. If IP priority is IPv6, 1 IPv4 and 2 IPv6 DNS servers are used.
DNS Server 1, 2 & 3: This field will be present if specify **Domain Name Server Setting** to **Manual**, the field is used to specify the DNS (Domain Name System) server address to be configured for the BMC.

3.7.7 PAM Order Settings

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



PAM Order Settings Page

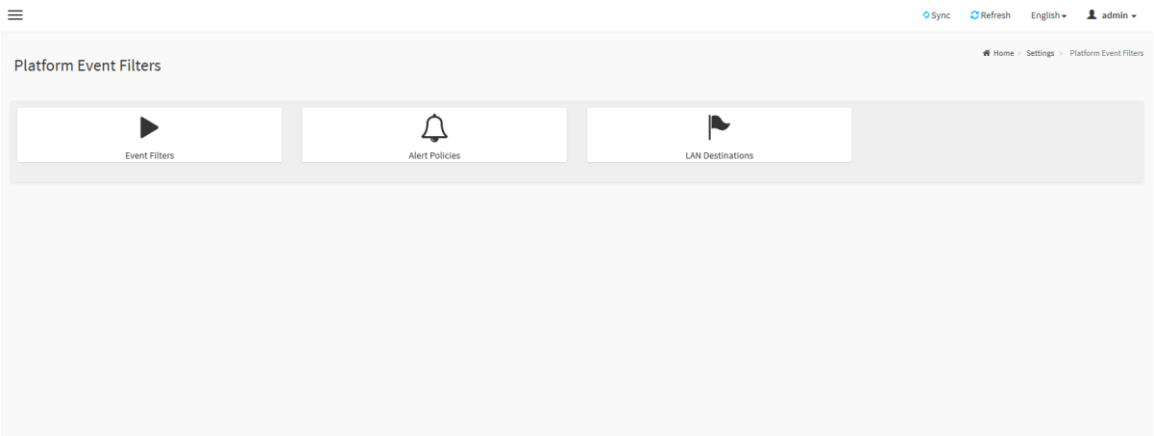
PAM Authentication Order: It shows the list of available PAM modules supported in BMC. Click and Drag the required PAM module to change its order.

Note:

1. *It is recommended not keeping the same username for different PAM modules.*
2. *If Authentication fails, the reason for failure could be invalid user or invalid password.*
3. *If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So it is always treated as Invalid username error and PAM will try other Authentication Methods.*
4. *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 keeping AD in the last location in PAM order.*

3.7.8 Platform Event Filter

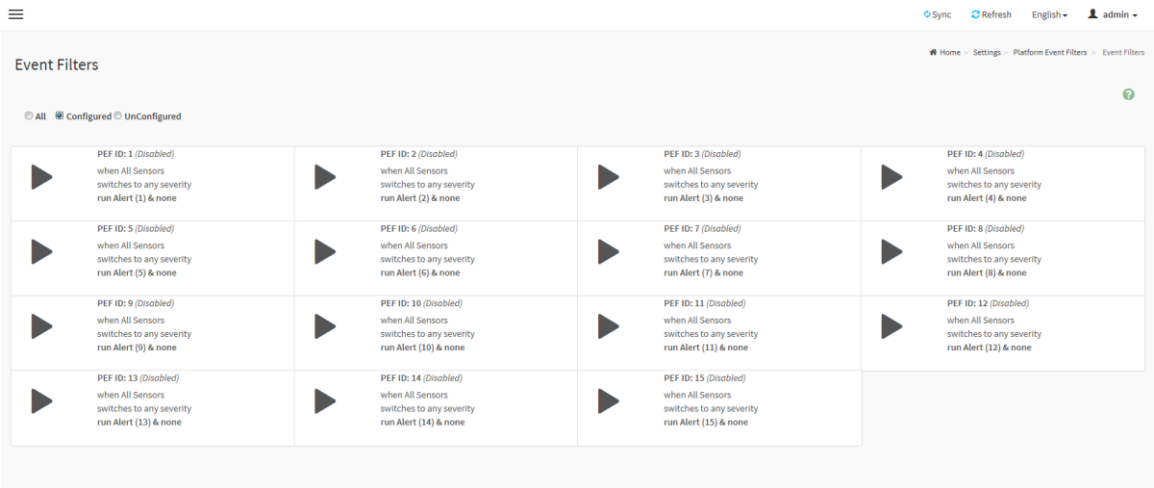
Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.



Platform Event Filter Page

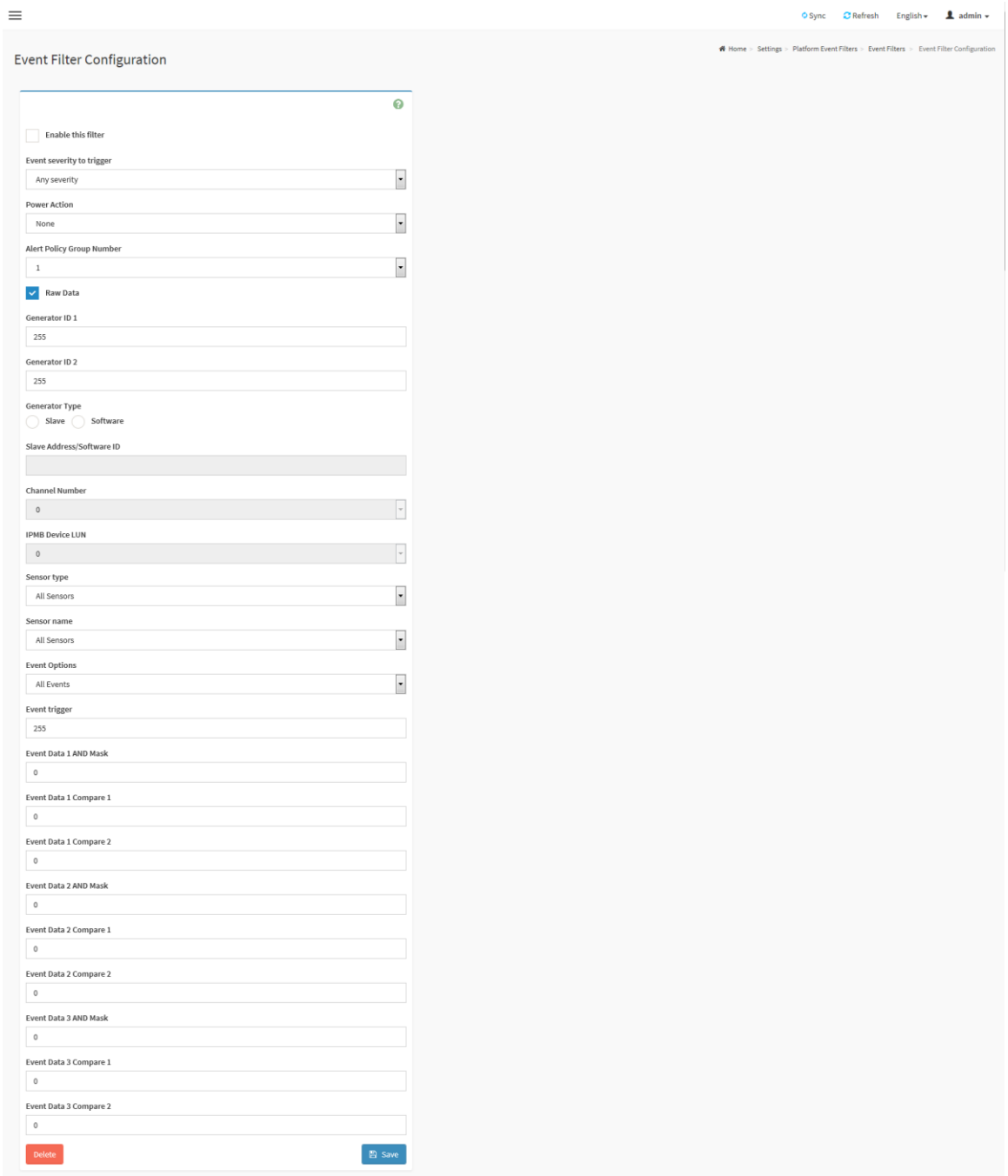
3.7.8.1 Event Filters

This page is used to configure Event filters. You can modify or add new event filter entry from here. By default, 15 event filter entries are configured among the 40 available slots.



Event Filters Page

Event Filter Configuration: Click the **Event Filters** section to configure the event filters in the available slots.



Event Filters Configuration Page

Enable this filter: Check the box to enable the PEF settings.

Event Severity to trigger: Select any one of the Event severity from the list.

Power Action: Select any one of the power action either Power down, Power reset or Power cycle from the drop-down list

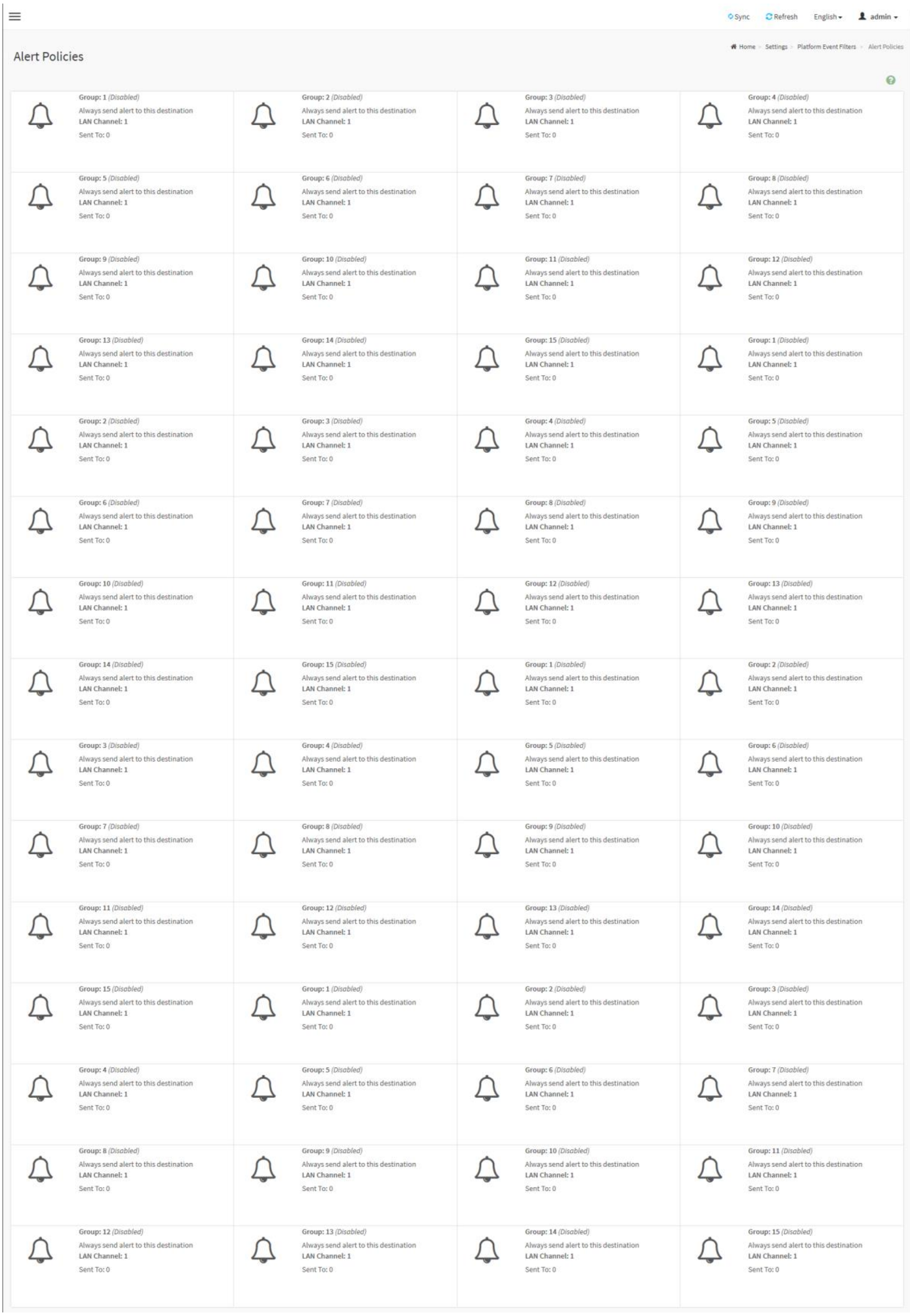
Alert Policy Group Number: Select any one of the alert policy group number from the drop-down list.

Raw Data: Check the box to fill the Generator ID with raw data.

Generator ID 1: Enter the raw generator ID1 data value.
Generator ID 2: Enter the raw generator ID2 data value.
Generator Type: Choose the event generator as slave address - if event is generated from IPMB.
Slave Address/Software ID: Specify corresponding I2C slave address or system software ID.
Channel Number: Choose the particular channel number through which the event message is received over. Choose “0” if the event message is received via the system interface, primary IPMB, or internally generated by the BMC.
IPMB Device LUN: Choose the corresponding IPMB device LUN if event is generated by IPMB.
Sensor type: Select the type of sensor that will trigger the event filter action.
Sensor name: Choose the particular sensor from the sensor list.
Event Options: Choose event option to be either all events or sensor specific events.
Event Trigger: Enter the raw event/reading type value.
Event Data 1 AND Mask: Indicate wildcarded or compared bits.
Event Data 1 Compare 1 & Event Data 1 Compare 2: Indicate whether each bit position’s comparison is an exact comparison or not.
Event Data 2 AND Mask: Similar to Event Data 1 AND Mask.
Event Data 2 Compare 1 & Event Data 2 Compare 2: Similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.
Event Data 3 AND Mask: Similar to Event Data 1 AND Mask.
Event Data 3 Compare 1 & Event Data 3 Compare 2: Similar to Event Data 1 Compare 1 and Event Data 1 Compare 2 respectively.

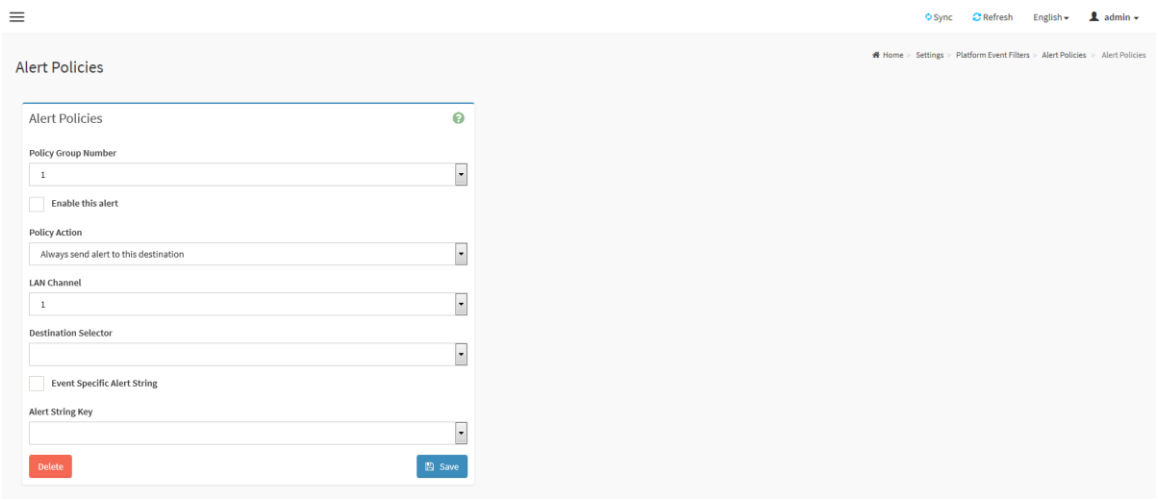
3.7.8.2 Alert Policies

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



Alert Policies Page

Alert Policies: Click the **Alert Policies** section to configure the alert policies in the available slots.

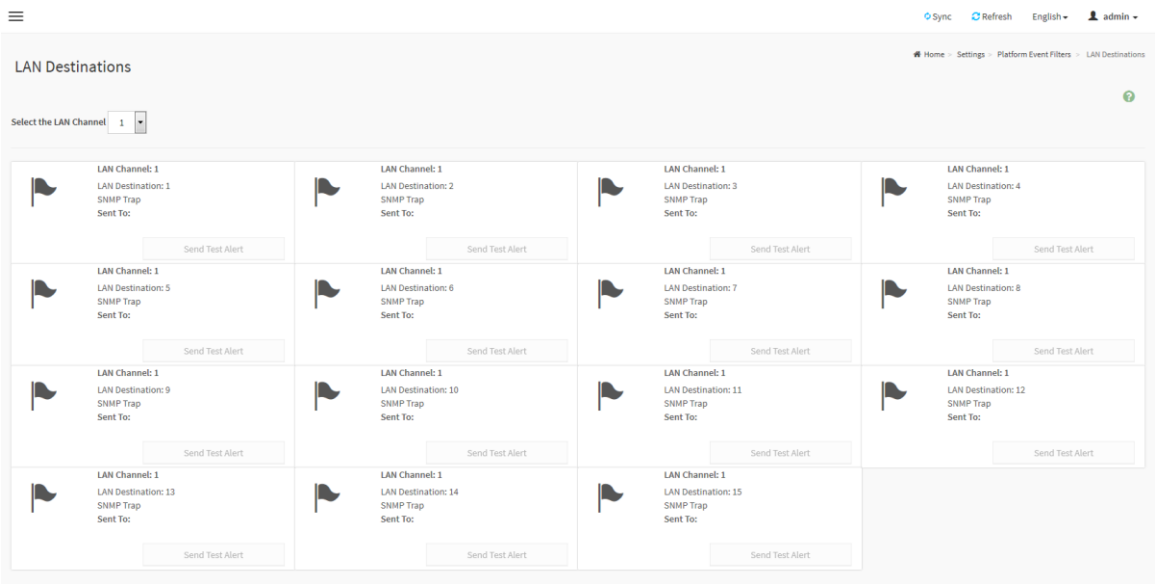


Alert Policies Page

Policy Group Number: Displays the Policy number of the configuration.
Enable this alert: Check the box to enable the policy settings.
Policy Action: Choose any one of the Policy set values from the list.
LAN Channel: Choose a particular channel from the available channel list.
Destination Selector: Choose a particular destination from the configured destination list.
Event Specific Alert String: Check the box to specify event-specific Alert String.
Alert String Key: Specify which string is to be sent for this Alert Policy entry.

3.7.8.3 LAN Destinations

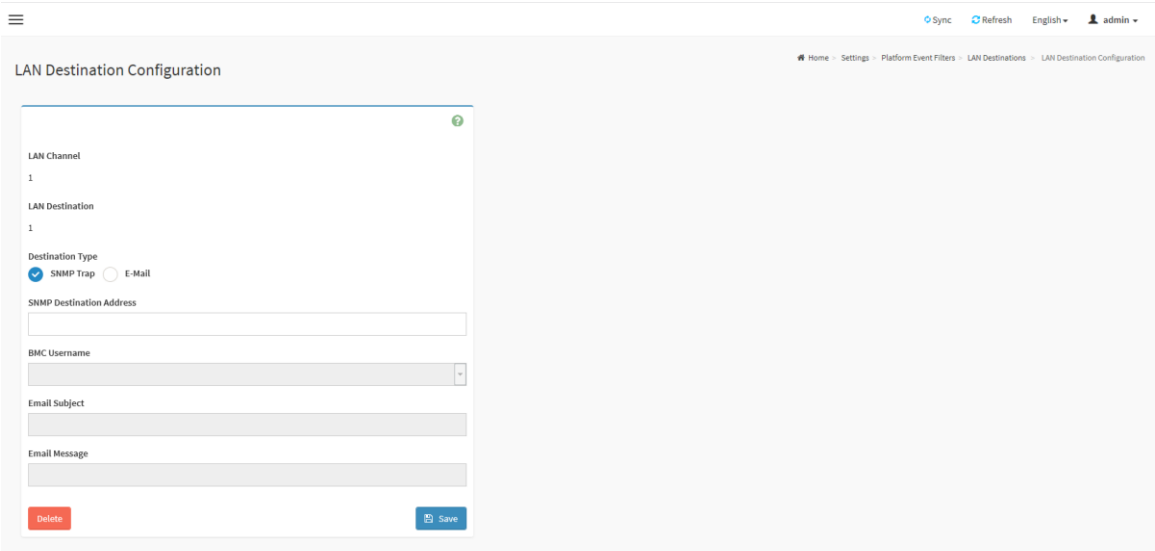
This page is used to configure the LAN destination of PEF configuration.



LAN Destinations Page

Select the LAN Channel: Select the LAN Channel number.

LAN Destination Configuration: Select any empty slot to configure LAN Destinations.



LAN Destination Configuration Page

LAN Channel: Displays LAN Channel Number for the selected slot (read only).
LAN Destination: Displays ID for setting Destination Selector of Alert Policy (read only).
SNMP Destination Address: Destination type can be either an SNMP Trap or an E-mail alert. For E-mail alerts, the four fields - SNMP Destination Address, BMC User

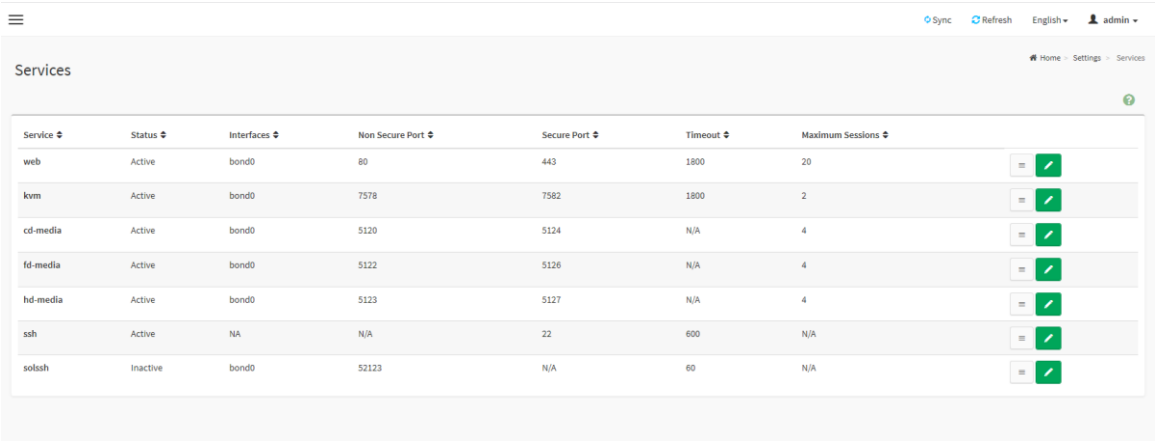
Name, Email subject and Email message needs to be filled. For SNMP Trap, only the SNMP Destination Address has to be filled.

BMC User Name: If Destination type is Email Alert, then choose the user to whom the email alert has to be sent.

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.

3.7.9 Services

This page is used to displays the basic information about services running in the BMC.



Services Page

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.

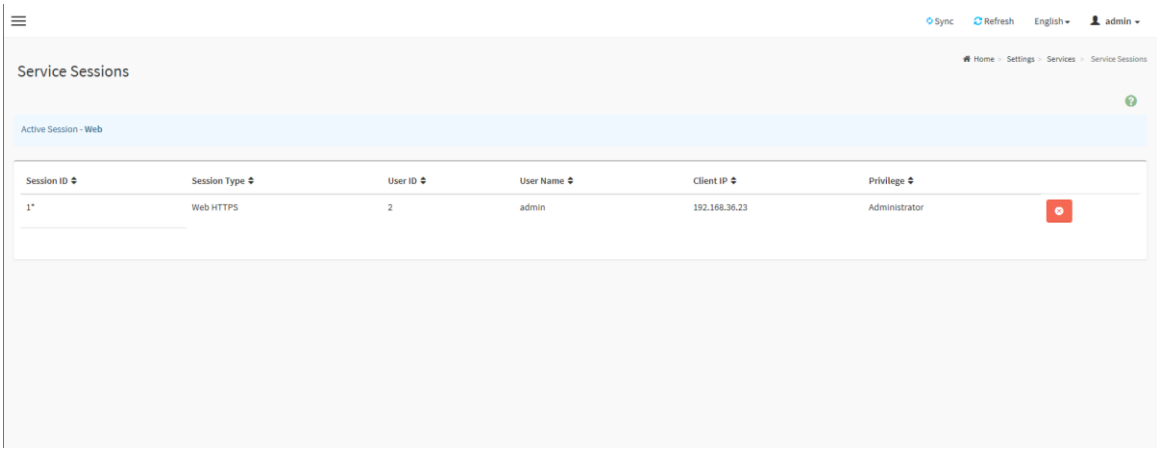
Nonsecure Port: Displays non secure port number of the service.

Secure Port: Displays secure port number of the service.

Timeout: Displays the session timeout value of the service.

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

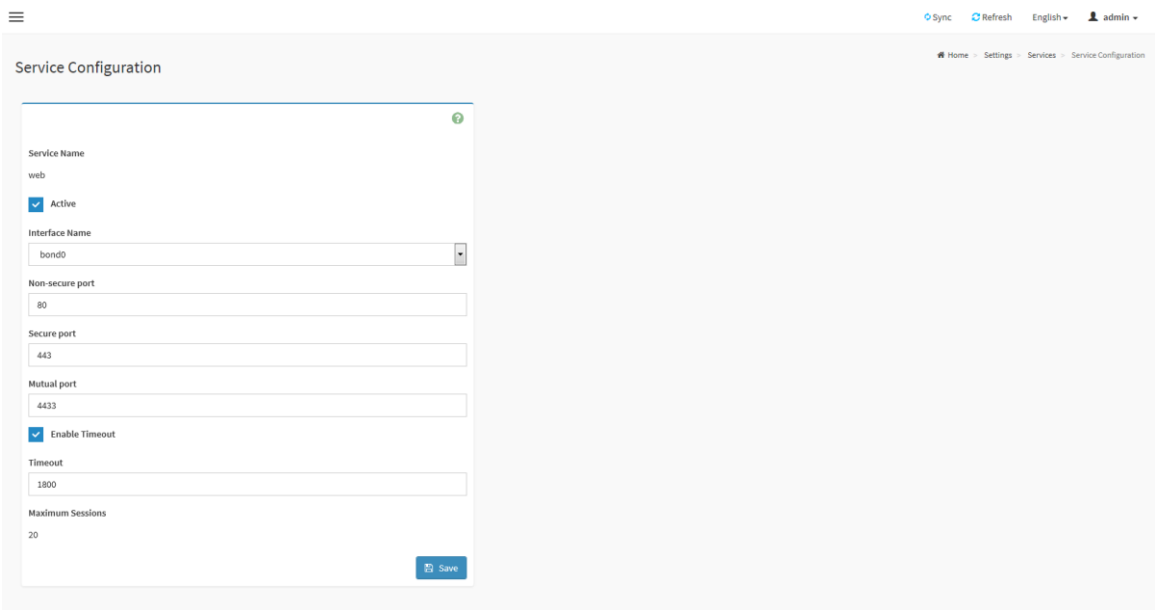
View the active sessions: Click **View** icon ≡ to view the details about the active sessions for the service.



Service Sessions Page

Session ID: Displays the ID of the active sessions.
Session Type: Displays the type of the active sessions.
User ID: Displays the ID of the user.
User Name: Displays the name of the user.
Client IP: Displays the IP addresses that are already configured for the active sessions
Privilege: Displays the access privilege of the user.
Terminate Session: Click **Terminate** icon to terminate the particular session of the service.

Edit the existing service: Click **Edit** icon to modify the configuration of the service.

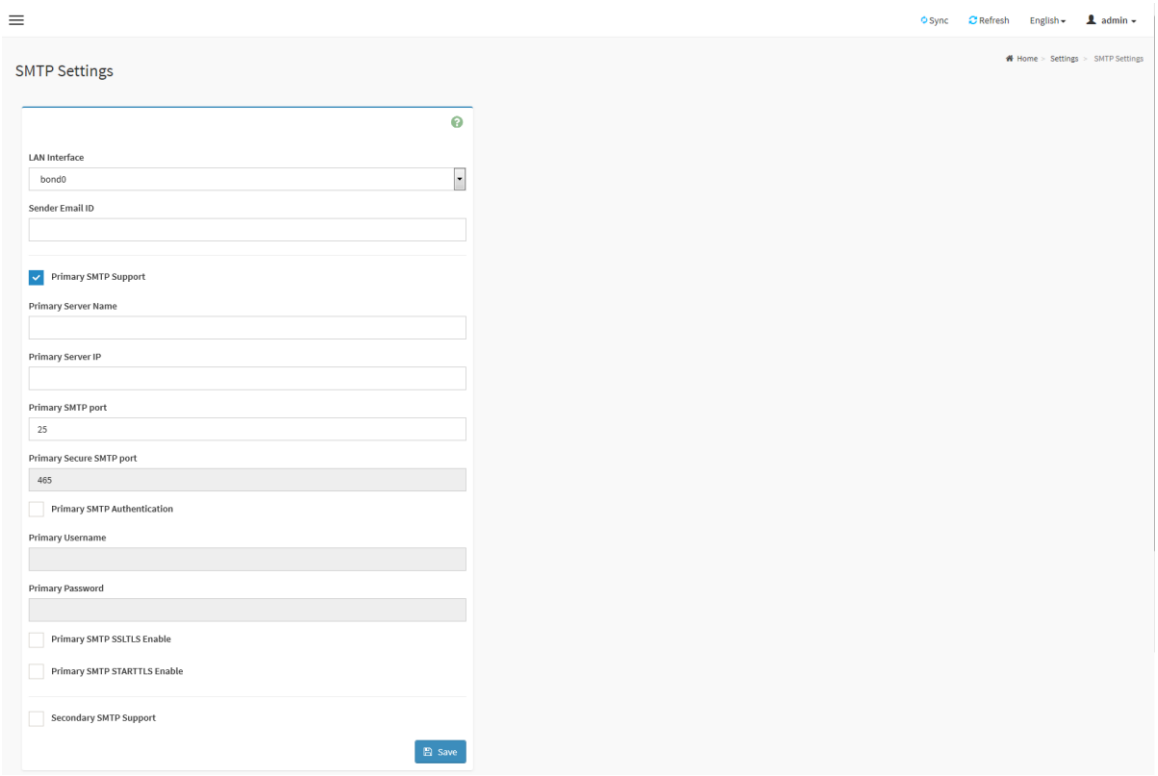


Service Configuration Page

Service Name: Displays service name of the selected slot(read only).
Active: Check the box to enable the service.
Interface Name: Choose any one of the available interfaces from the drop-down list.
Non-secure Port: Configure non secure port number for the service.
Secure Port: Configure secure port number for the service.
Mutual Port: Configure mutual port number for the service.
Enable Timeout: Check the box to enable the timeout function.
Timeout: Configure the session timeout for the service.
Maximum Sessions: Displays the maximum number of allowed sessions for the service.

3.7.10 SMTP Settings

This is used to configure the SMTP settings of the device.



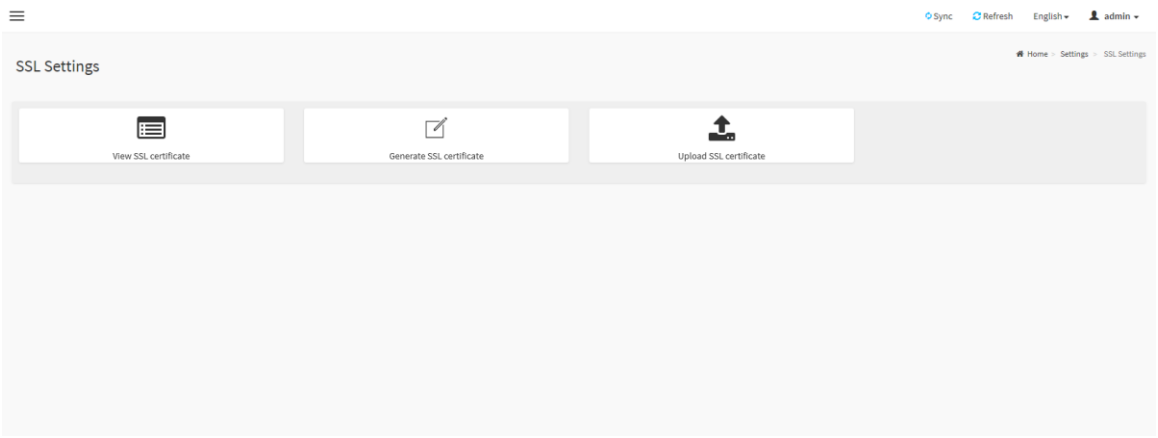
SMTP Settings Page

LAN Interface: Displays the list of LAN channels available.
Sender Email ID: Enter the valid Sender Email ID on the SMTP Server.
Primary SMTP Support: Check the box to enable SMTP support for the BMC.
Primary Server Name: Enter the Machine Name of the SMTP Server.
Primary SMTP IP: Enter the IP address of the SMTP Server.

Primary SMTP Port: Specify the SMTP Port.
Primary Secure SMTP Port: Specify the SMTP Secure Port.
Primary SMTP Authentication: Check the box to enable SMTP Authentication.
Primary Username: Enter the username to access SMTP Accounts.
Primary Password: Enter the password for the SMTP User Account.
Primary SMTP SSLTLS Enable: Check the box to enable SMTP SSLTLS protocol
Primary SMTP STARTTLS Enable: Check the box to enable SMTP STARTTLS protocol.
Upload SMTP CA Certificate File: This field will be present if enable **SMTP SSLTLS Enable** or **STARTTLS Enable,** the field is used to upload CACERT key file.
Upload SMTP Certificate File: This field will be present if enable **SMTP SSLTLS Enable** or **STARTTLS Enable,** the field is used to upload CERT key file.
Upload SMTP Private Key: This field will be present if enable **SMTP SSLTLS Enable** or **STARTTLS Enable,** the field is used to upload SMTP key file.
Secondary SMTP Support: Check the box to enable secondary SMTP support for the BMC.

3.7.11 SSL Settings

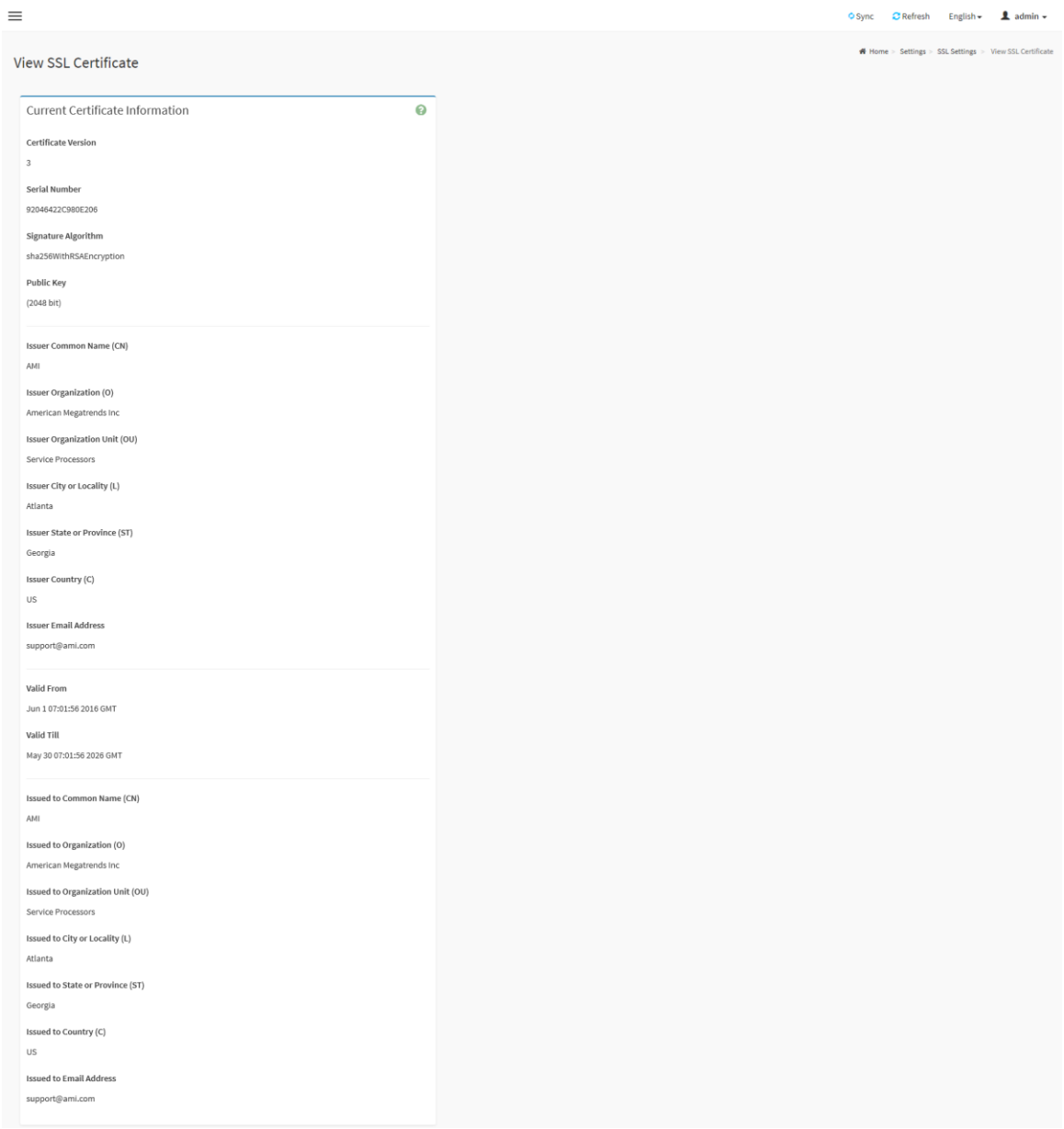
This page is used to configure SSL certificate for the BMC.



SSL Settings Page

3.7.11.1View SSL certificate

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



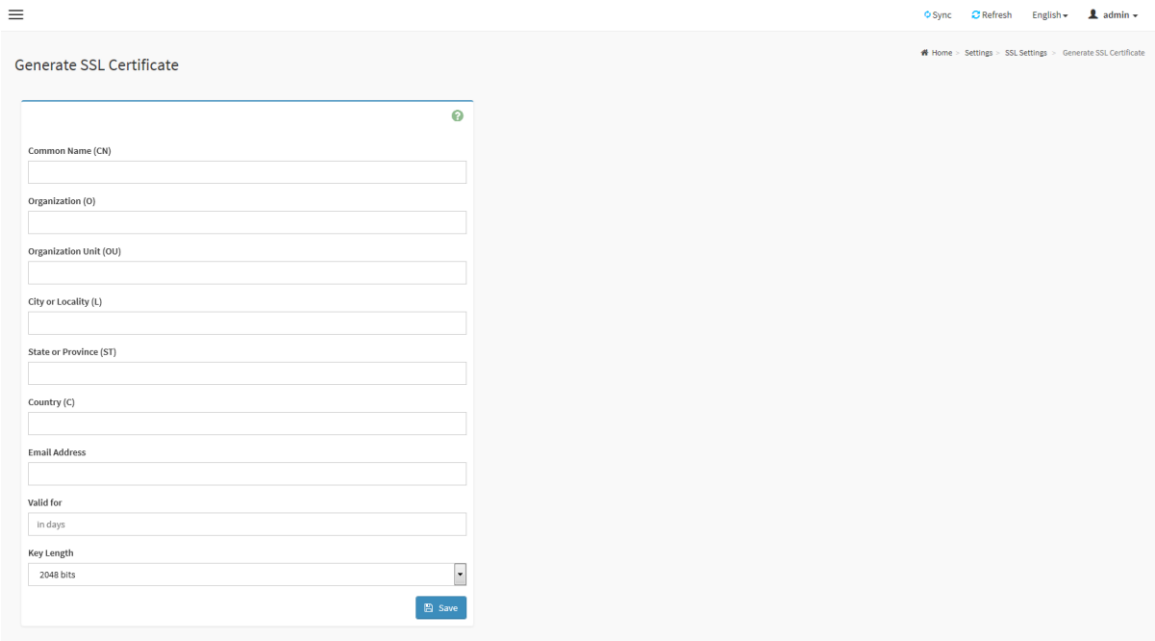
View SSL certificate Page

Note:

This page provides a simple method to generate SSL certificate and it is not issued by a trusted Certificate Authority, you can upload a trusted certificate by yourself, if necessary.

3.7.11.2 Generate SSL certificate

This page is used to generate the SSL certificate based on configuration details.

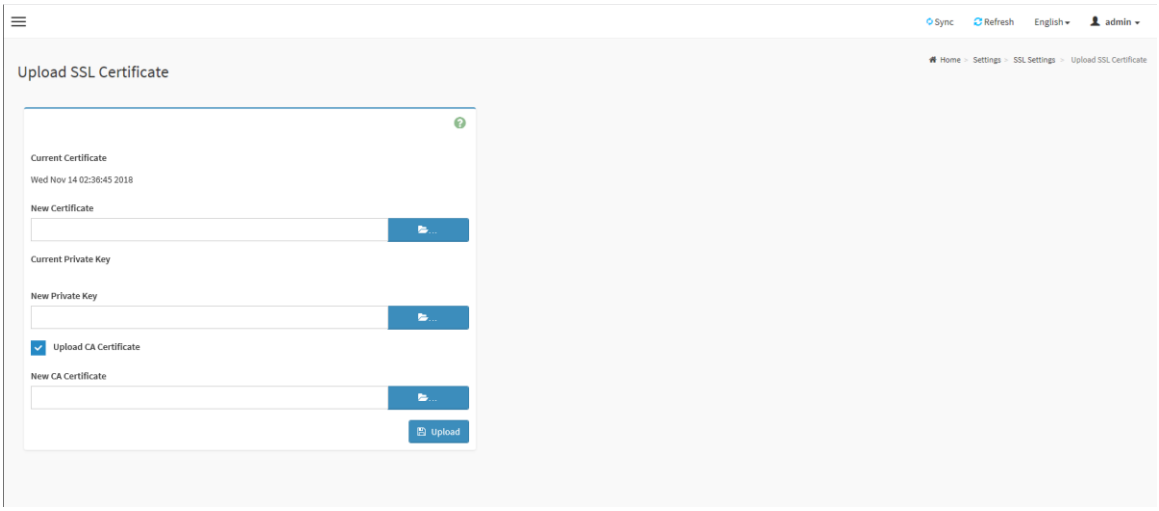


Generate SSL certificate Page

Common Name(CN): Common name for which certificate is to be generated.
Organization(O): Organization name for which the certificate is to be generated.
Organization Unit(OU): Over all organization section unit name for which certificate is to be generated.
City or Locality(L): City or Locality of the organization.
State or Province(ST): State or Province of the organization.
Country(C): Country code of the organization.
Email Address: E-mail Address of the organization.
Valid for: Validity of the certificate.
Key Length: The key length bit value of the certificate.

3.7.11.3 Upload SSL certificate

This page is used to upload the certificate and private key file into the BMC.

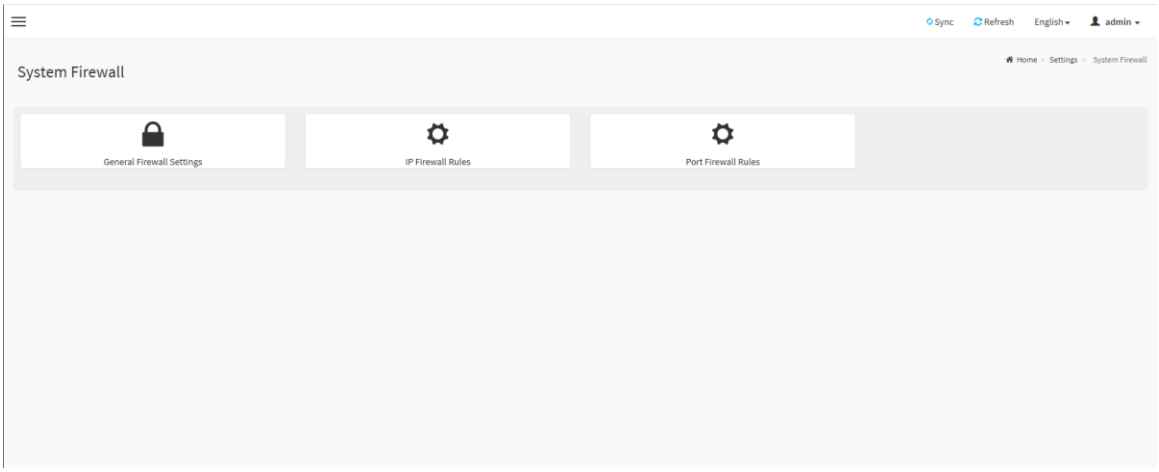


Upload SSL certificate Page

Current Certificate: Displays current certificate and uploaded date/time (read only).
New Certificate: Browse and navigate to the certificate file, the file should be of pem type
Current Private Key: Displays current Private key information (read only).
New Private Key: Browse and navigate to the private key file, the file should be of the type pem.
Upload CA Certificate: Check this option to upload CA Certificate file.
New CA Certificate: Browse and navigate to the CA certificate file.

3.7.12 System Firewall

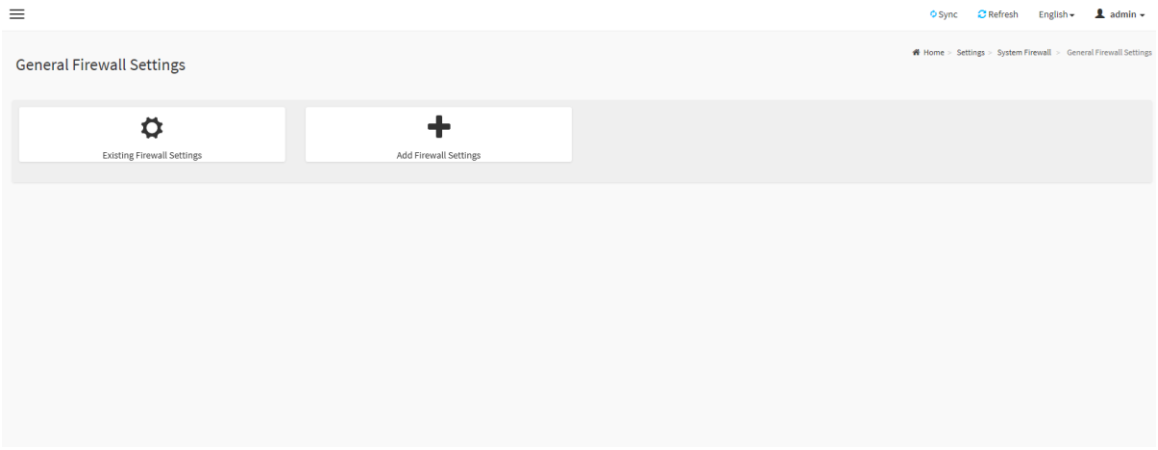
This page is used to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers.



System Firewall Page

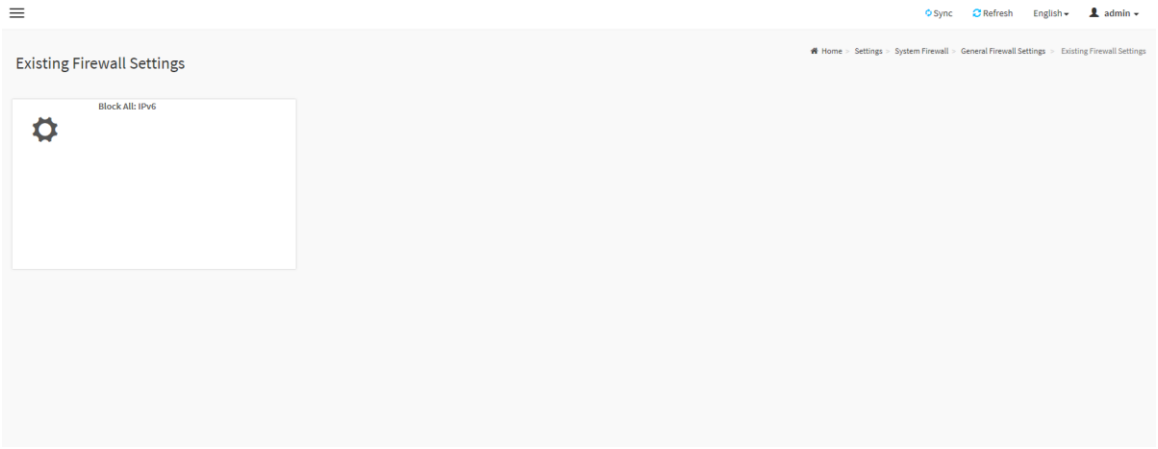
3.7.12.1General Firewall Settings

This page is used to configure general firewall settings.



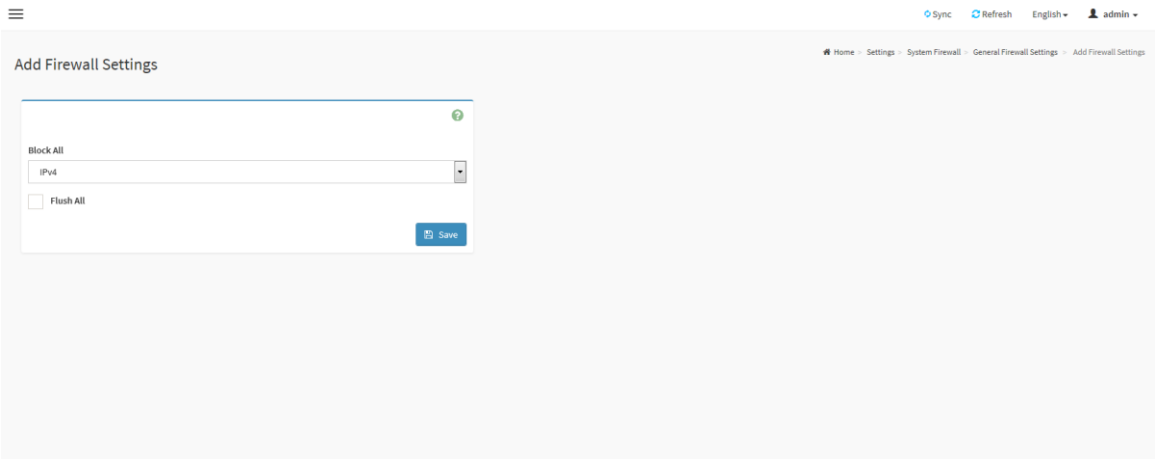
General Firewall Settings Page

Existing Firewall Settings: This page is used to displays existing firewall settings.



Existing Firewall Settings Page

Add Firewall Settings: This page is used to displays add firewall settings.



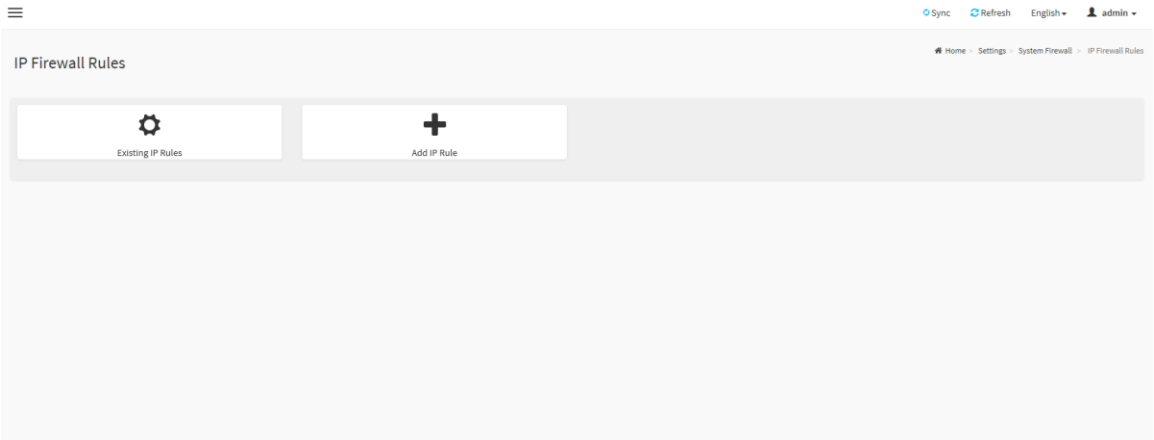
Add Firewall Settings Page

Block All: This option will block all incoming IPs and Ports.

Flush All: This option is used to flush all the system firewall rules.

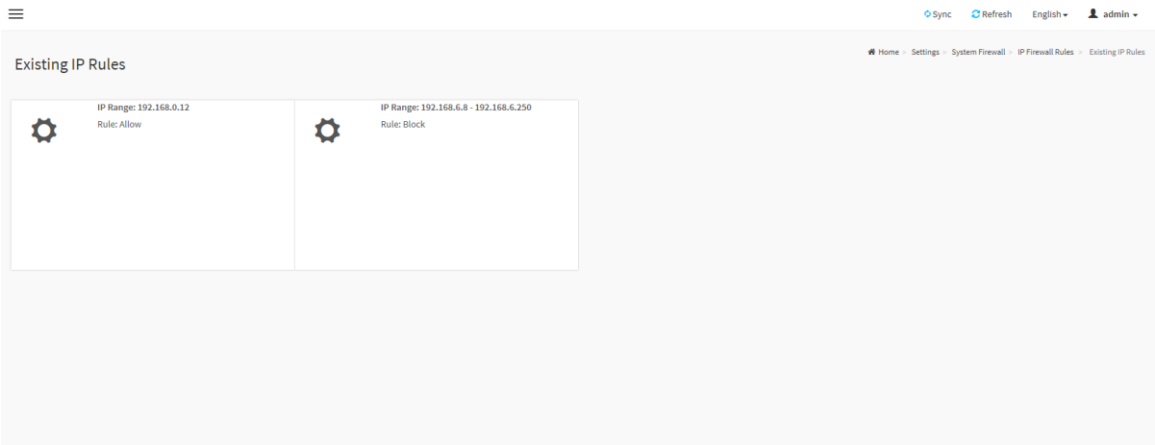
3.7.12.2IP Firewall Rules

This page is used to add a new IP Address or Range to firewall settings.



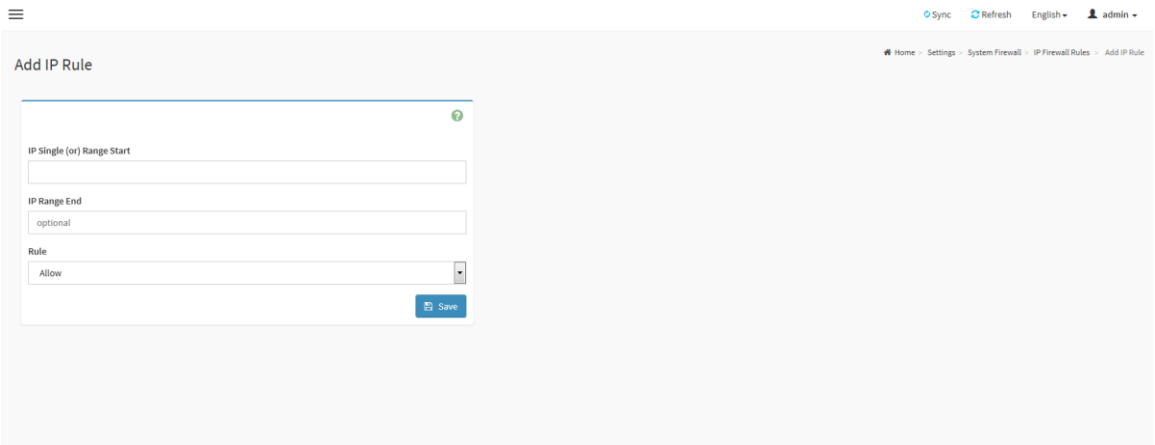
IP Firewall Rules Page

Existing IP Rules: This page is used to displays existing IP rules.



Existing IP Rules Page

Add IP Rule: This page is used to displays add IP rule settings.



Add IP Rule Page

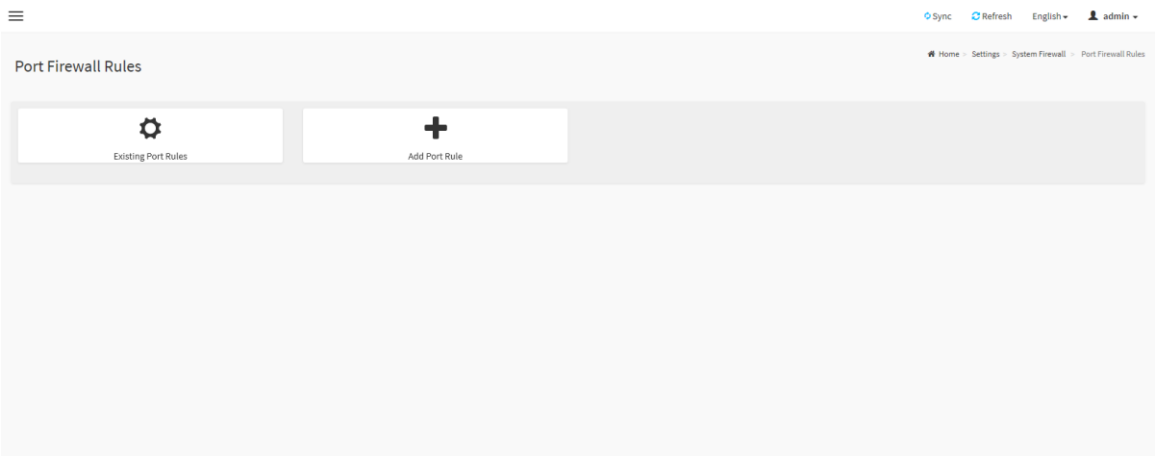
IP Single (or) Range Start: This field is used to configure the IP address or range of IP addresses.

IP Range End: This field is used to configure the IP range end of IP addresses**.**

Rules: This field is used to determine the rule to **Allow** or **Block.**

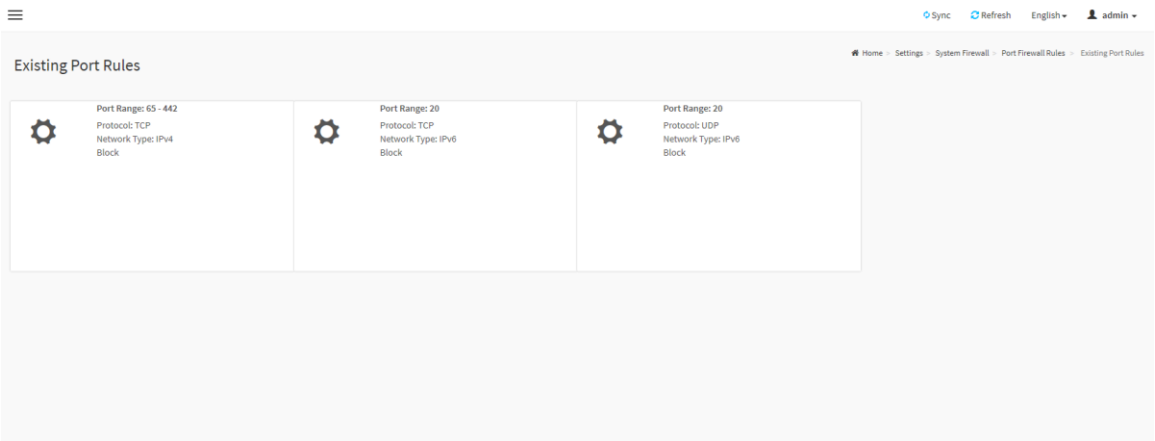
3.7.12.3Port Firewall Rules

This page is used to add a new Port or Range to firewall settings.



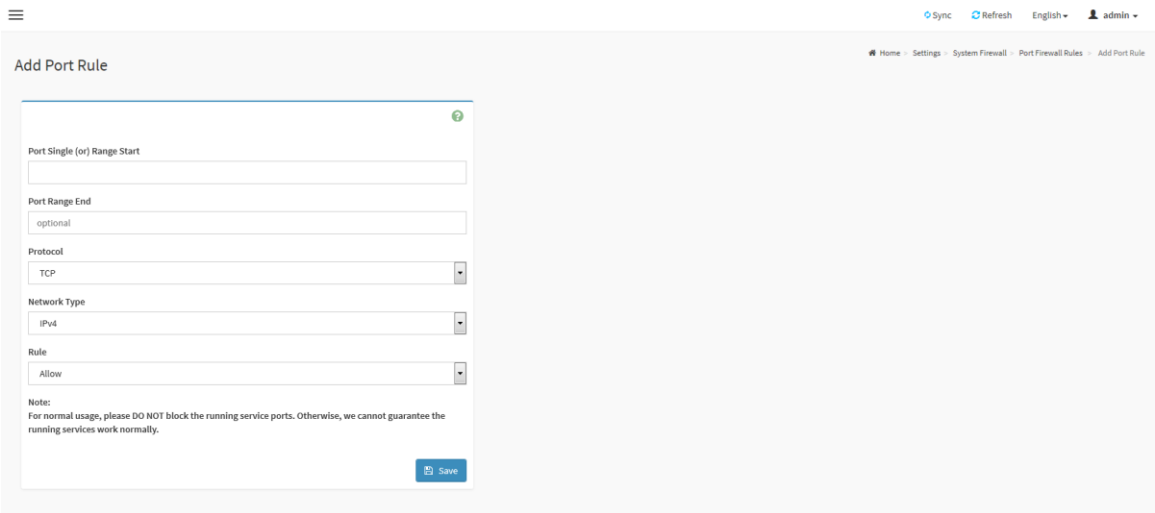
Port Firewall Rules Page

Existing Port Rules: This page is used to displays existing port rules.



Existing Port Rules Page

Add Port Rule: This page is used to displays add port rule settings.



Add Port Rule Page

Port Single (or) Range Start: This field is used to configure the port number or range of port numbers.

Port Range End: This field is used to configure the port range end of port numbers**.**

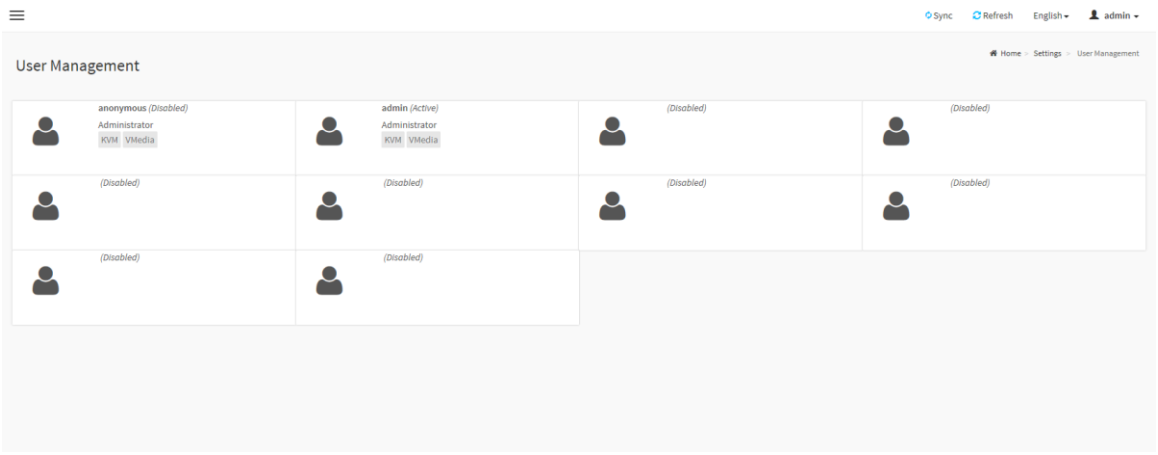
Protocol: This field is used to configure the protocol.

Network Type: This field is used to configure the network type.

Rule: This field is used to determine the rule to **Allow** or **Block.**

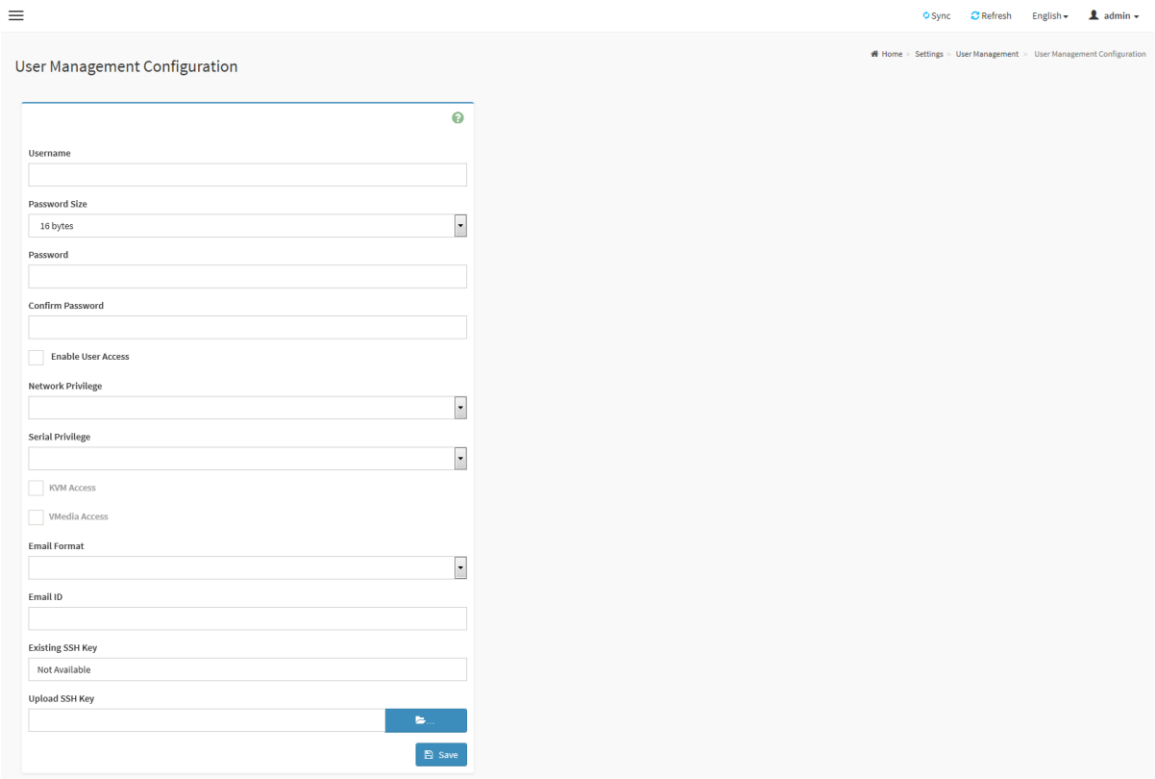
3.7.13 User Management

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



User Management Page

Add a new user: To add a new user, select a free section and click on the empty section.



Add User Page

Username: Enter the name of the user.

Password Size: Either 16 Bytes or 20 Bytes password size can be chosen.

Password: Enter the password of the user.

Confirm Password: Confirm the password.

Enable User Access: Enabling user access will intern assign the IPMI messaging privilege to user.

Network Privilege: Select the network privileges assigned to the user.

Serial Privilege: Select the serial privileges assigned to the user.

KVM Access: Assign the KVM privilege for the user.

VMedia Access: Assign the VMedia privilege for the user.

Note:

Both KVM and VMedia privilege will enable(disable) automatic when Network Privilege is administrator(other).

Email Format: Specify the format for the email. 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

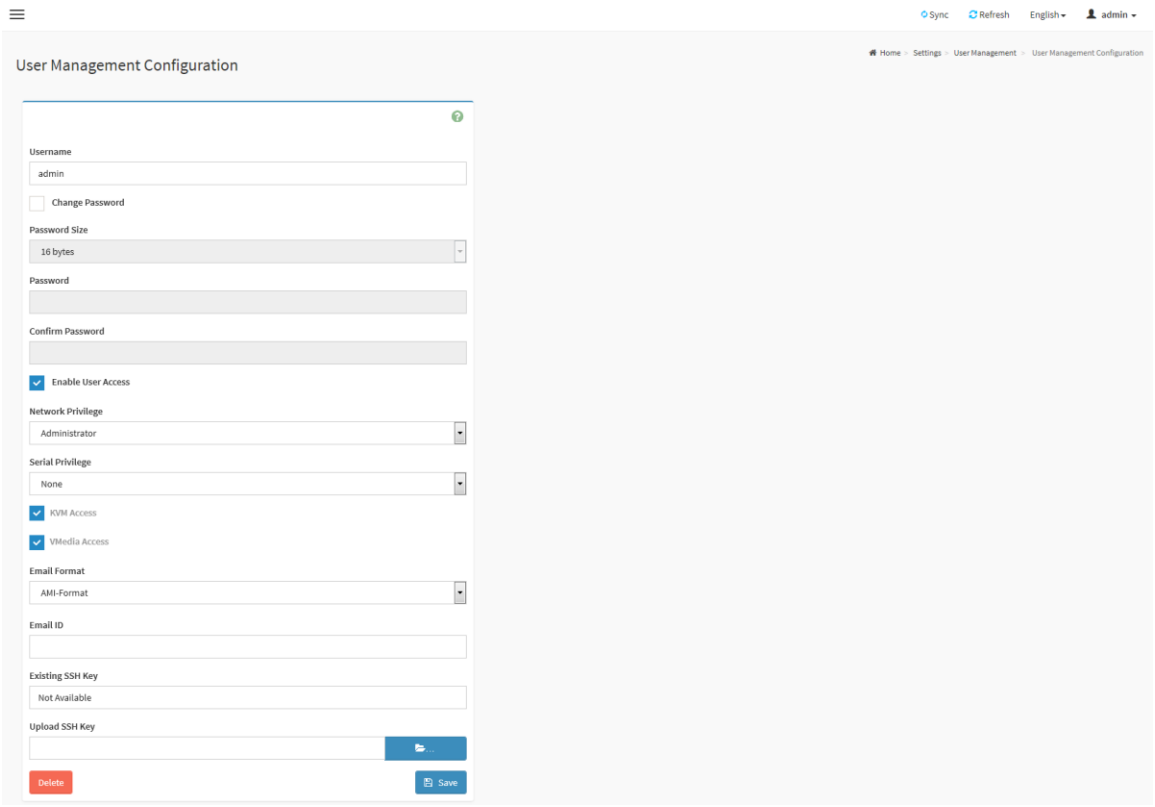
subject and message for email alert.

Email ID: Enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

Existing SSH Key: Displays the uploaded SSH key information(read only).

Upload SSH Key: Upload the public SSH key file.

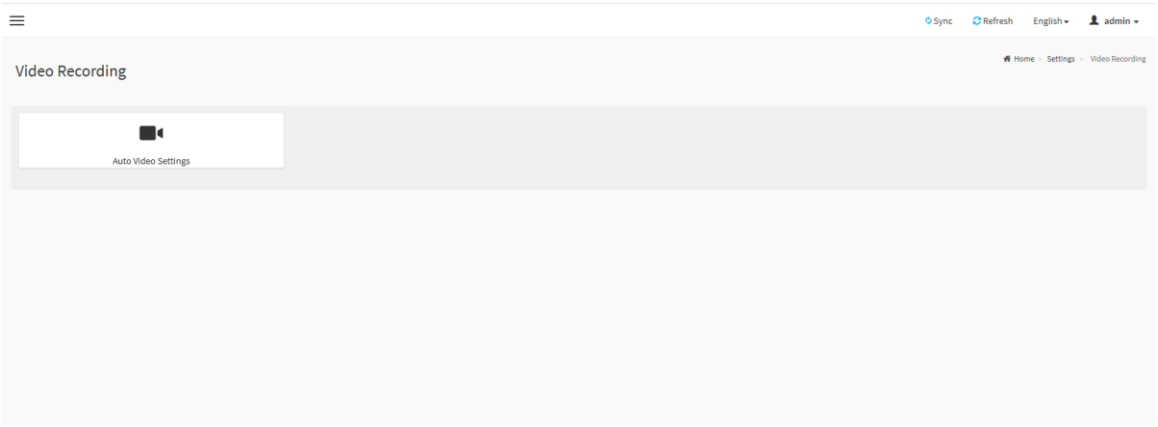
Modify user: To modify the existing user, click on the active user tab.



Modify User Page

3.7.14 Video Recording

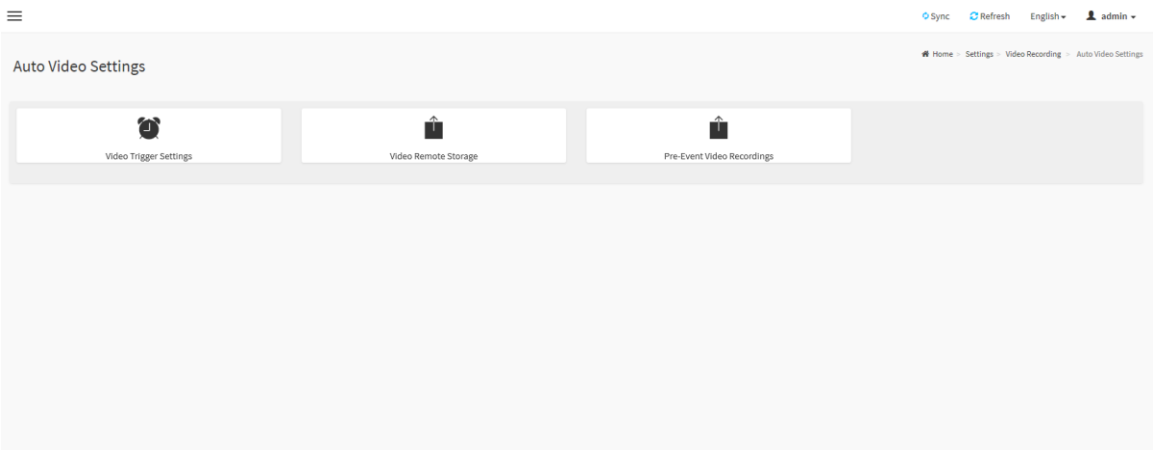
This page is used to configure video recording settings.



Video Recording Page

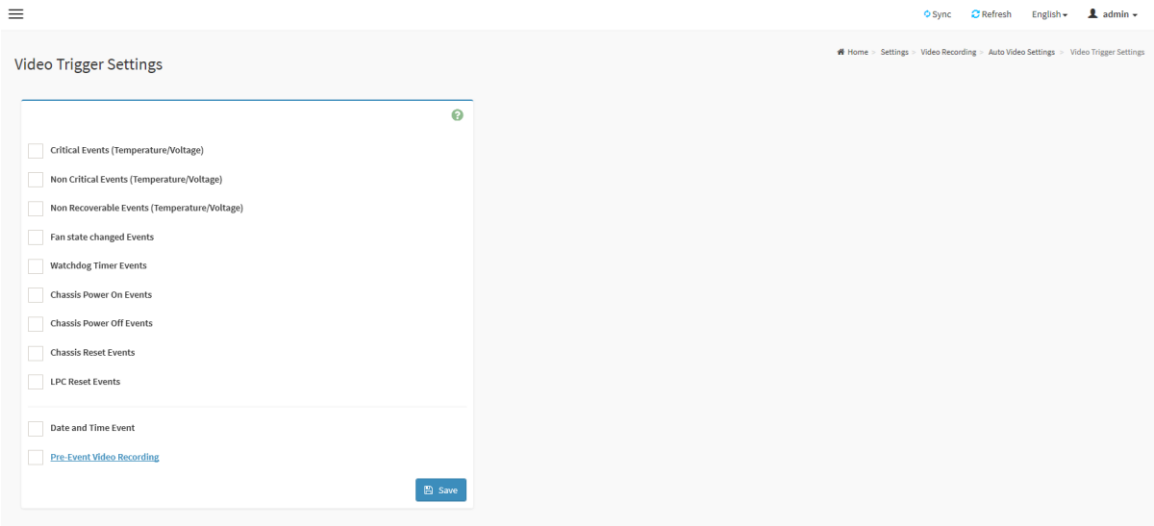
3.7.14.1Auto Video Settings

This page is used to configure auto video recording settings.



Auto Video Settings Page

Video Trigger Settings: This page is used to configure the events that will trigger auto video recording function of the KVM server.



Video Trigger Settings Page

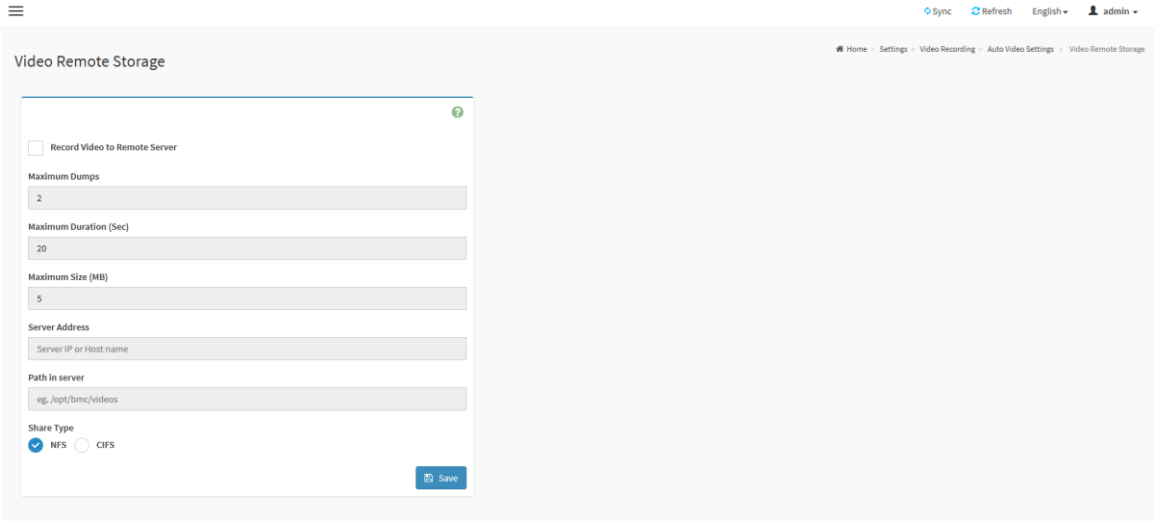
Critical Events (Temperature/Voltage): Trigger the recording by the critical events for Temperature/Voltage sensor.

Non Critical Events (Temperature/Voltage): Trigger the recording by the non-critical events for Temperature/Voltage sensor.

Non Recoverable Events (Temperature/Voltage): Trigger the recording by the non-recoverable events for Temperature/Voltage sensor.

Fan state changed Events: Trigger the recording by all fan sensor events
Watchdog Timer Events: Trigger the recording when watchdog timer be triggered.
Chassis Power On Events: Trigger the recording by system power on events (DC on).
Chassis Power Off Events: Trigger the recording by system power off events (DC off).
Chassis Reset Events: Trigger the recording by system reset events.
LPC Reset Events: Trigger the recording by Host LPCRESET event.
Date and Time Event: Trigger the recording by specific date and time.
Pre-Event Video Recording: Select Crash Reset either **Pre-crash** or **Pre-reset**.

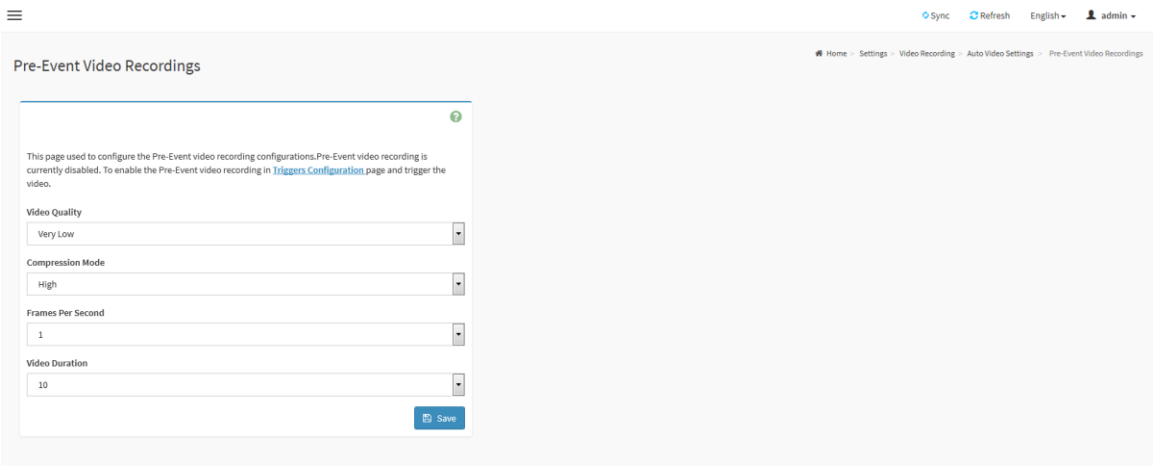
Video Remote Storage: This page is used to configure the remote storage path.



Video Remote Storage Page

Record Video to Remote Server: Check the box to enable remote video support. If remote video support is enabled, then the video files will be stored in remote path.
Maximum Dumps: Enter maximum dumps of the video.
Maximum Duration(Sec): Enter maximum duration of the video.
Maximum Size(MB): Enter maximum size of the video.
Server Address: Specify server address of the server.
Path in Server: 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.

Pre-Event Video Recordings: This page used to configure the Pre-Event video recording configurations.

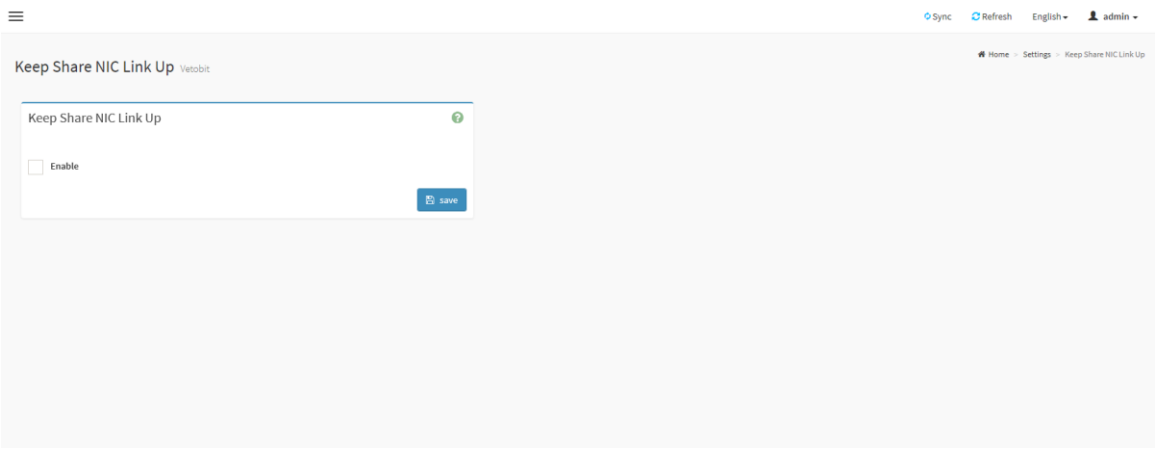


Pre-Event Video Recording Page

Video Quality: To set video quality, select ranges from the drop-down list.
Compression Mode: To set compression mode, select modes from the drop-down list.
Frames Per Second: To set number of frames per second, select frames/sec (1-4) from the drop-down list.
Video Duration: To set duration of video, select second (10-60) from the drop-down list.

3.7.15 Keep Share NIC Link Up

This page is used to configure share NIC(NCSI) PHY link up setting.

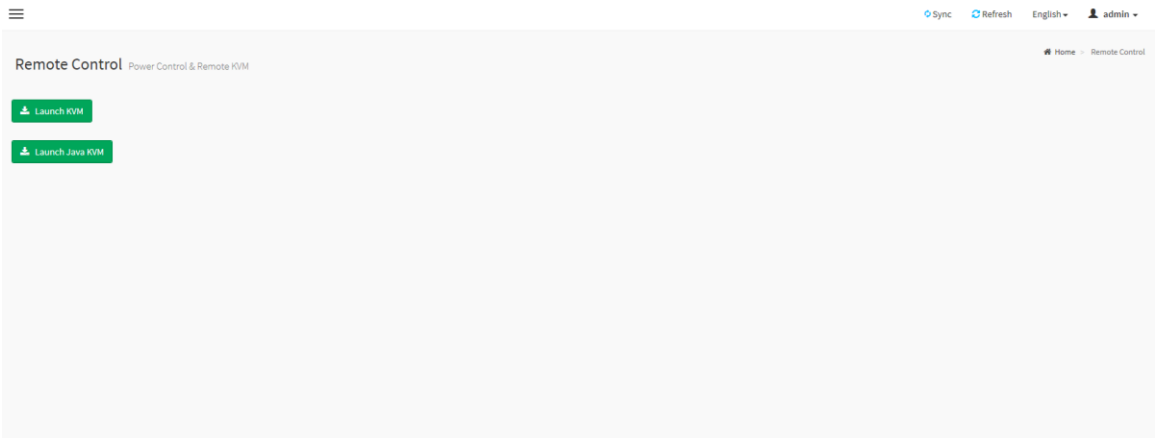


Keep Share NIC Link Up Page

Enable: Check the box to enable Keep Share NIC Link Up, share NIC PHY will keep link up, and it could avoid share NIC disconnection while system reset.

3.8 Remote Control

This page is used to launch the remote console redirection.



Remote Control Page

Launch KVM: Click the button to open remote control KVM page.
Launch Java KVM: Click the button to open Java KVM application.

3.9 Image Redirection

This page is used to configure the images into BMC for redirection.

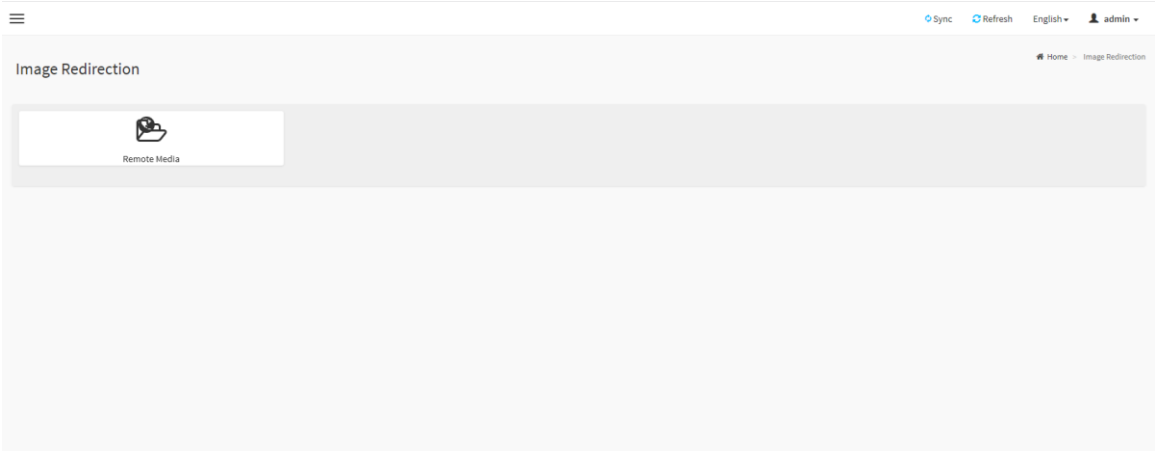
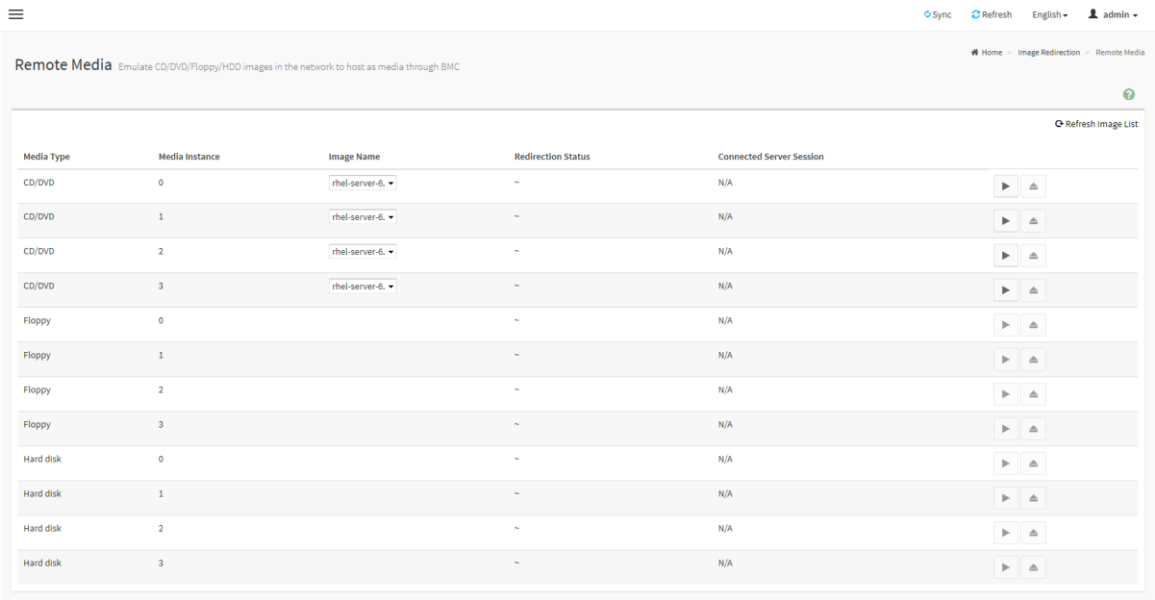


Image Redirection Page

3.9.1 Remote Media

This page is used to configure the remote images into BMC for redirection.



Remote Media Page

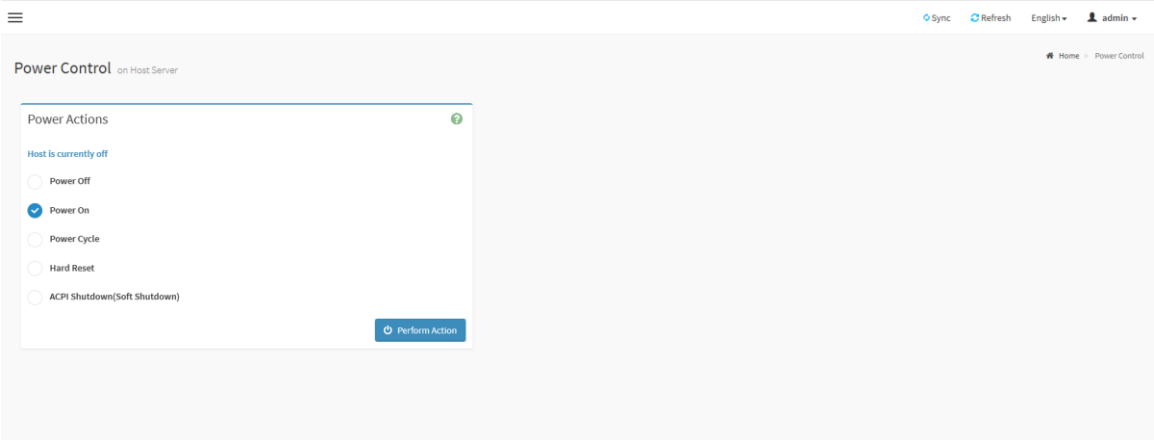
Media Type: Displays type of Media such as CD/DVD, Floppy and Hard-disk.
Media Instance: Displays total media instance count.
Image Name: Displays the default recovery image name on the server.
Status: Displays the status of the media.
Session Index: Displays Media Server Session Index.
Start/Stop Redirection: To start or stop media redirection.
Pause: To pause the media redirection.
Refresh Image List: To get latest Image lists from the Remote Storage.

Note:

To configure the image, you need to enable Remote Media support first.

3.10 Power Control

This page is used to view and control the power of the server.

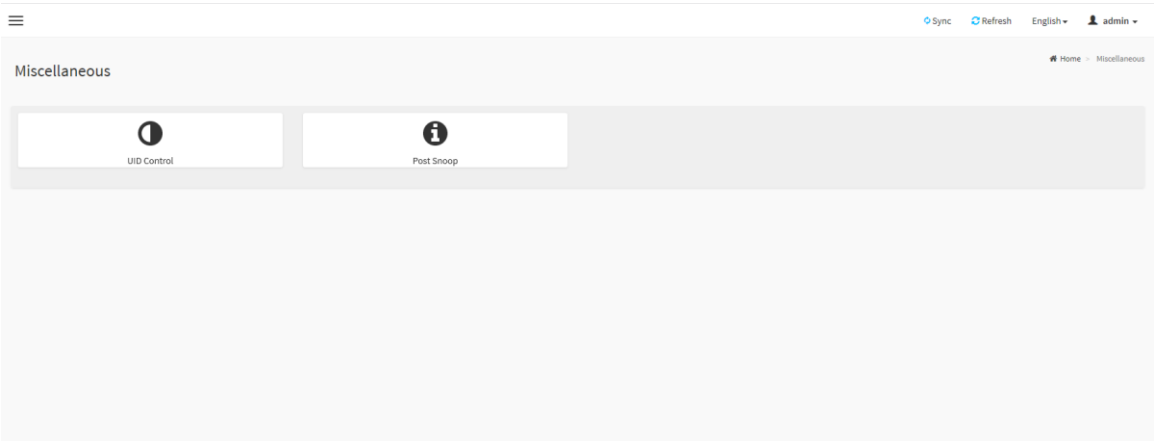


Power Control Page

Power Off: Select this option to immediately power off the server.
Power On: Select this option to power on the server.
Power Cycle: Select this option to first power off, and then reboot the system (cold boot).
Hard Reset: Select this option to reboot the system without powering off (warm boot).
ACPI Shutdown(Soft Shutdown): Select this option to initiate operating system shutdown prior to the shutdown.

3.11 Miscellaneous

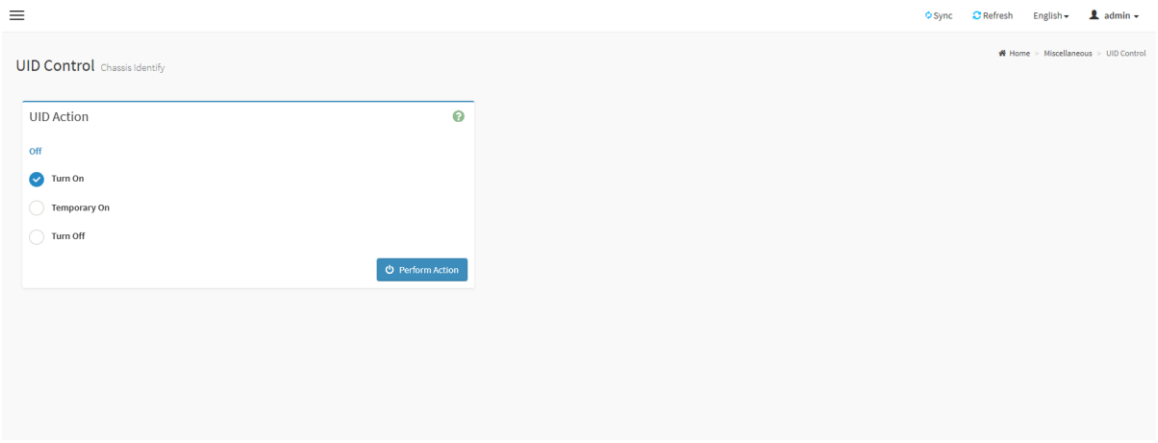
This page is used to configure miscellaneous settings.



Miscellaneous Page

3.11.1 UID Control

This page is used to control the UID of the chassis.



UID Control Page

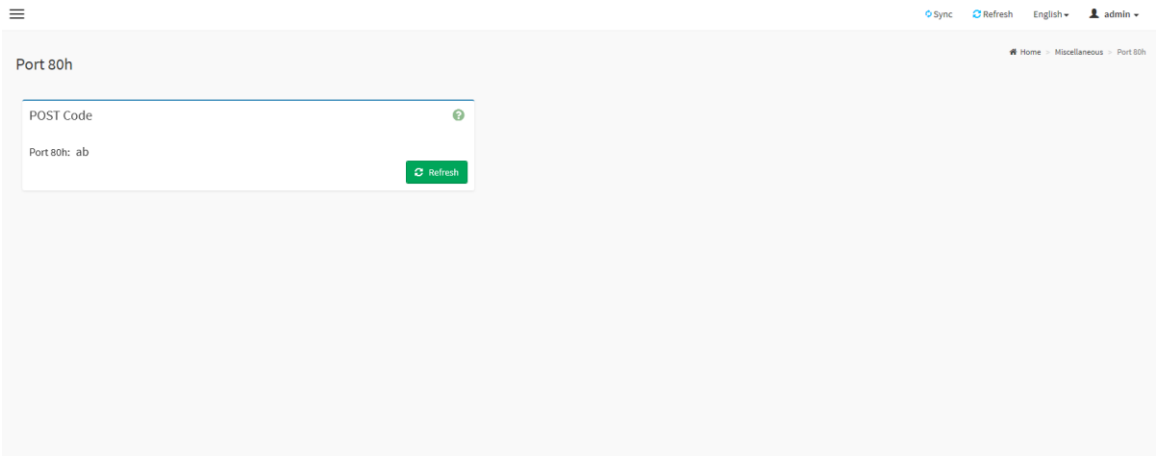
Trun On: Select this option to turn on UID.

Temporary On: Select this option to temporary turn on UID.(15 sec blink)

Turn Off: Select this option to turn off UID.

3.11.2 Post Snoop

This page is used to display the last POST code of BIOS.

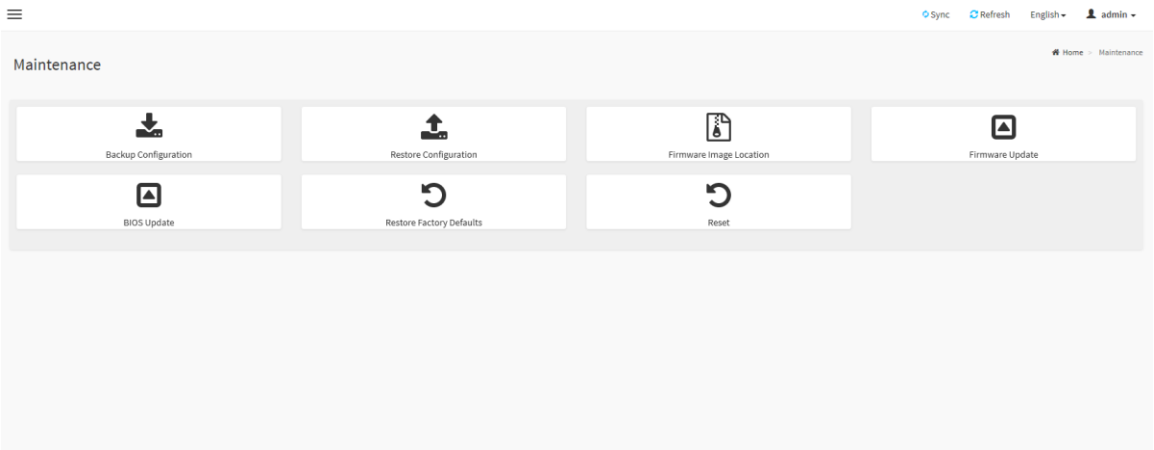


Post Snoop Page

Post 80h: Click **Refresh** button to get the last POST code of BIOS.(read only)

3.12 Maintenance

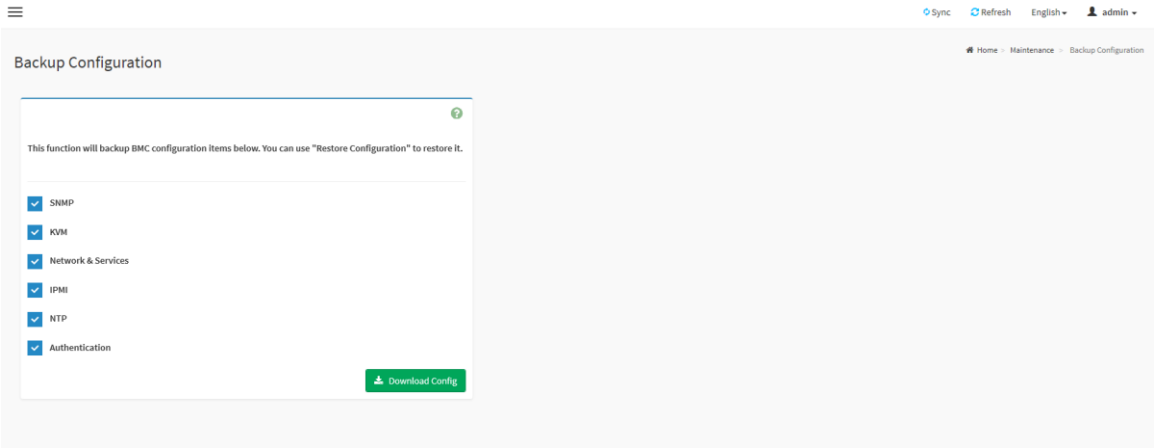
This page is used to do maintenance tasks on the device.



Maintenance Page

3.12.1 Backup Configuration

This page is used to back up the configuration.

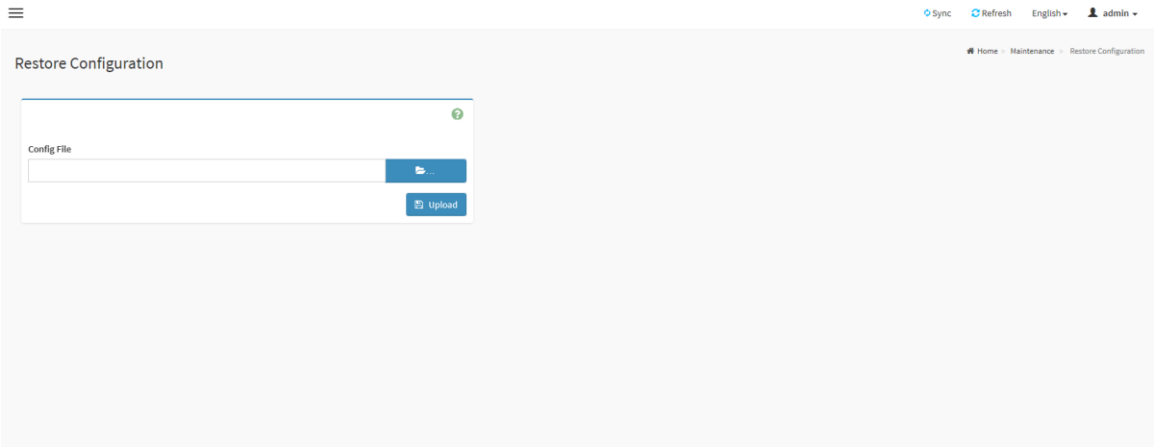


Backup Configuration Page

Download Config: To download and save the configuration files backup from BMC to client system.

3.12.2 Restore Configuration

This page is used to restore the configuration files from the client system to the BMC.

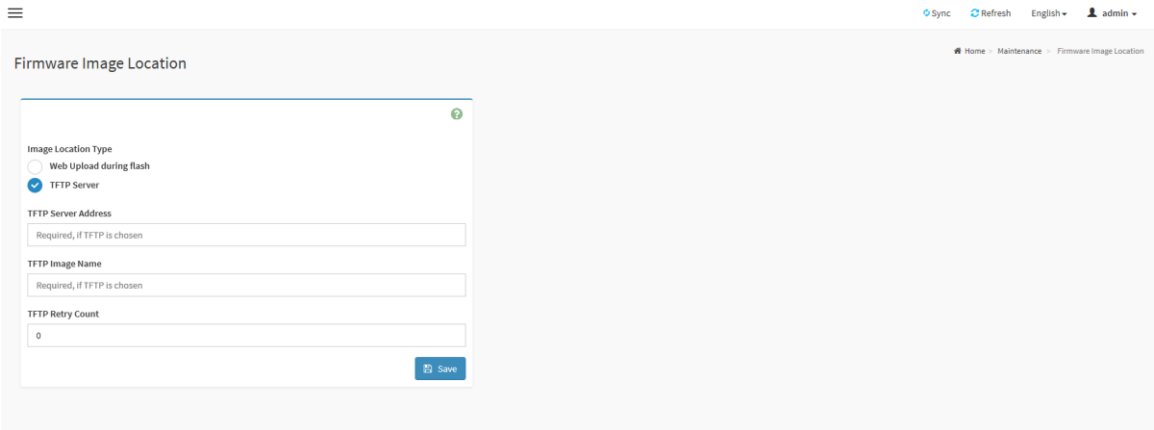


Restore Configuration Page

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.

3.12.3 Firmware Image Location

This page is used to configure firmware image into the BMC.



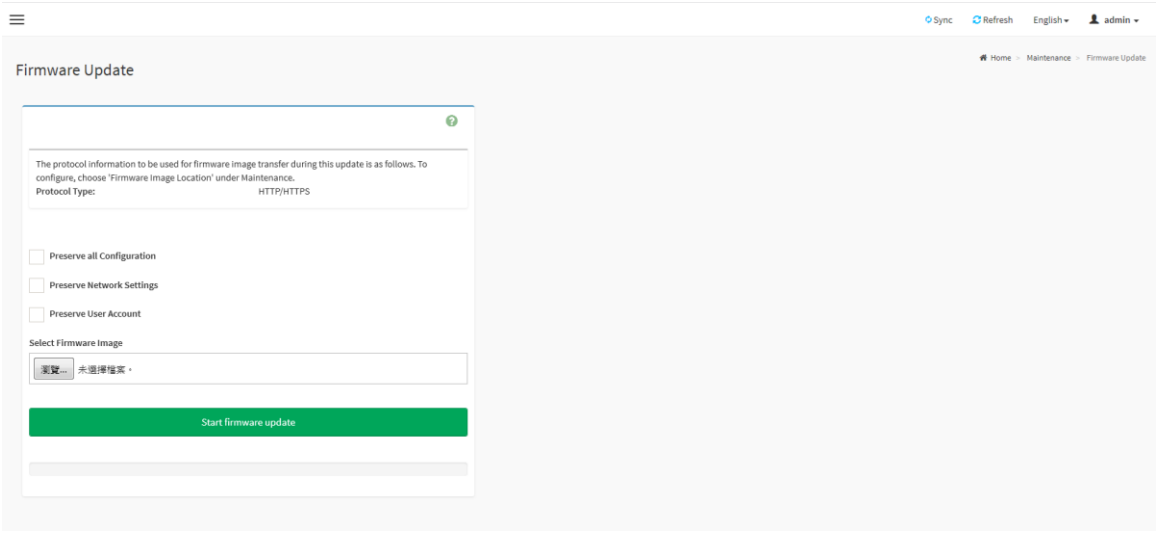
Firmware Image Location Page

Web Upload during flash: Select the option to transfer the firmware image into the BMC via HTTP/HTTPS.
TFTP Server: Select the option to transfer the firmware image into the BMC via TFTP.
TFTP Server Address: This field will be present if enable **TFTP Server,** the field is used to configure the address of TFTP server.
TFTP Image Name: This field will be present if enable **TFTP Server,** the field is used to configure full source path with filename of TFTP server.

TFTP Retry Count: This field will be present if enable **TFTP Server,** the field is used to configure the number of times to be retried in case a transfer failure occurs.

3.12.4 Firmware Update

This page is used to update BMC firmware.

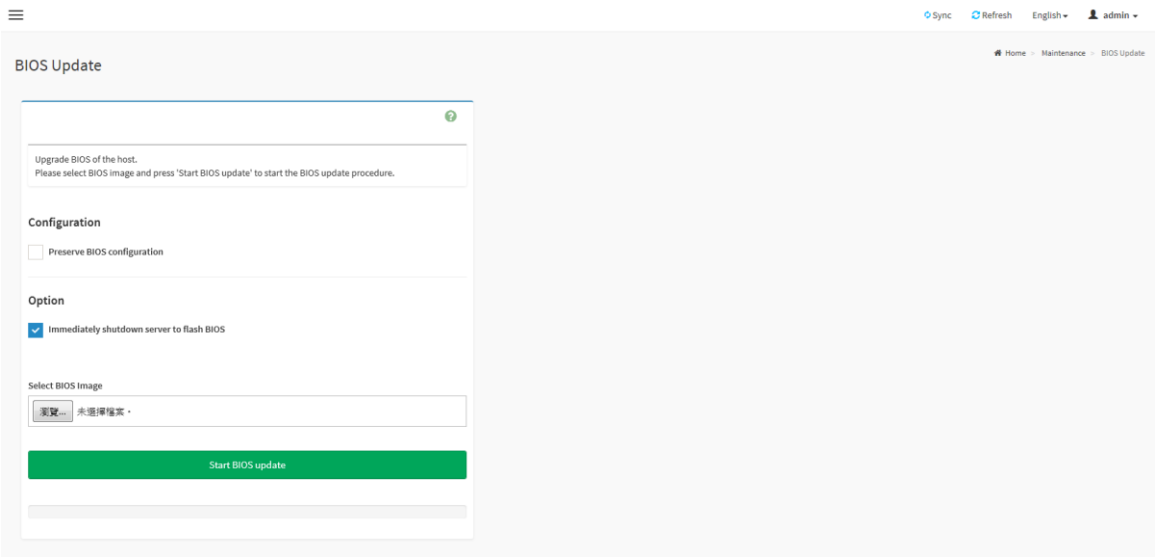


Firmware Update Page

Preserve all Configuration: To preserve all configuration.
Preserve Network Settings: To preserve network settings.
Preserve User Account: To preserve user accounts.
Select Firmware Image: To Select the firmware image to be uploaded.
Start Firmware Update: To Start the firmware update.

3.12.5 BIOS Update

This page is used to update BIOS firmware.

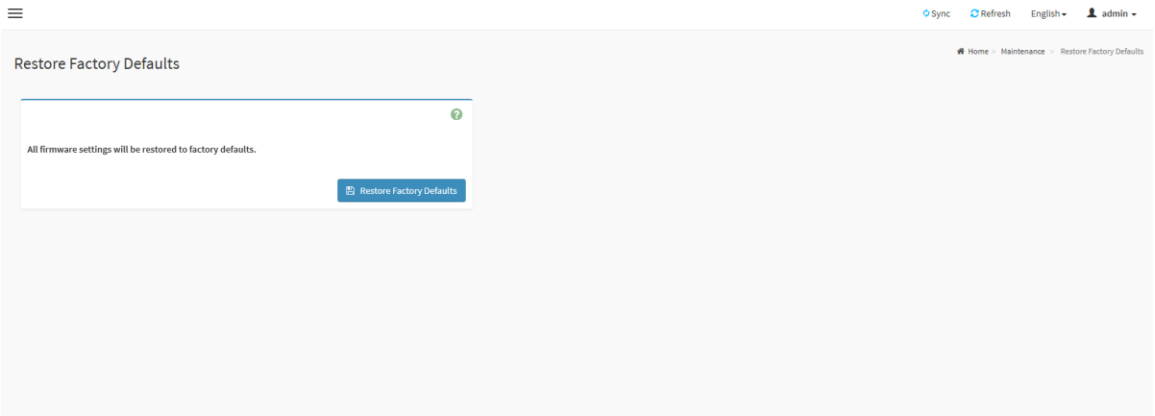


BIOS Update Page

Preserve BIOS configuration: To preserve BIOS configuration.
Immediately shutdown server to flash BIOS: To shutdown server immediately to flash BIOS.
Start Firmware Update: To Start the BIOS update.

3.12.6 Restore Factory Defaults

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



Restore Factory Defaults Page

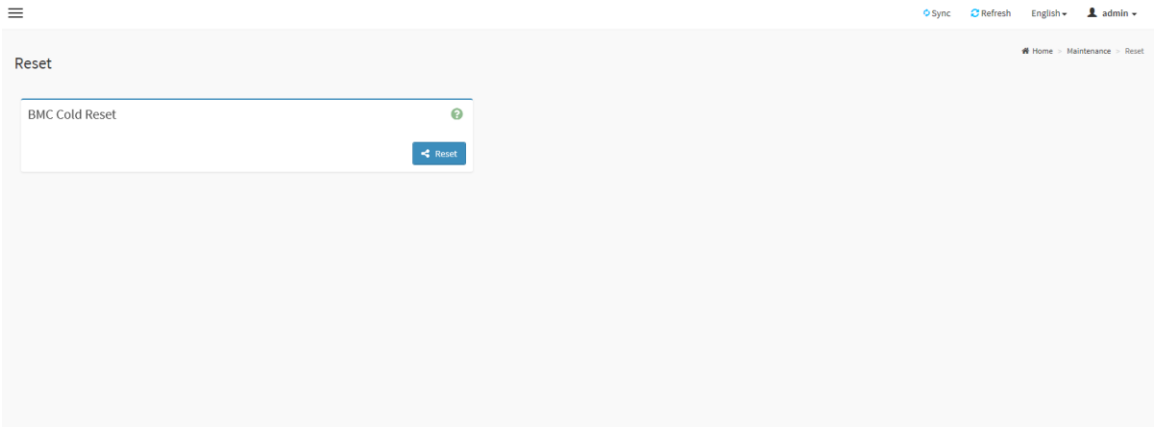
Restore Factory Defaults: Click the button to restore configuration to factory default settings, the following settings will be restored.

- **SDR**
- **SEL**
- **IPMI**

- **Network**
- **NTP**
- **SSH**
- **KVM**
- **Authentication**
- **Syslog**
- **Web**

3.12.7 Reset

This page is used to reset BMC device.



Reset Page

Reset: Click the button to reset the device.

3.13 Sign out

Click **Sign Out** to perform log out from the Web GUI. A Warning message will be prompted you to proceed further, click **OK** to log out else **Cancel** to retain the Web GUI.