GIGABYTE™

Gigabyte Management Console

User's Guide

Rev. 1.0

Copyright

© 2021 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved.
The trademarks mentioned in this manual are legally registered to their respective owners.

Disclaimer

Information in this manual is protected by copyright laws and is the property of GIGABYTE. Changes to the specifications and features in this manual may be made by GIGABYTE without prior notice. No part of this manual may be reproduced, copied, translated, transmitted, or published in any form or by any means without GIGABYTE's prior written permission.

Documentation Classifications

In order to assist in the use of this product, GIGABYTE provides the following types of documentation:

- User Manual: detailed information & steps about the installation, configuration and use this product (motherboard), covering hardware, BIOS and BMC firmware.
- Service Guide: detailed information & steps about the installation, configuration and use of this product (server barebones), covering hardware & BIOS
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes

Please see the support section of the online product page to check the current availability of these documents

For More Information

For related product specifications, the latest firmware and software, and related information, please visit our website at:

http://www.gigabyte.com

For GIGABYTE distributors and resellers, additional sales & marketing materials are available from our reseller portal:

http://reseller.b2b.gigabyte.com

For further information & technical assistance, please contact your GIGABYTE sales representative. You may also message GIGABYTE server directly by email, Facebook or twitter

Email: server.grp@gigabyte.com
Facebook: https://www.facebook.com/gigabyteserver
Twitter: https://twitter.com/GIGABYTEServer

Table of Contents

Chapter 1 Getting Started

1-1 Software Requirement

- 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.
- IE 11 and above.
- Firefox (with limited support).

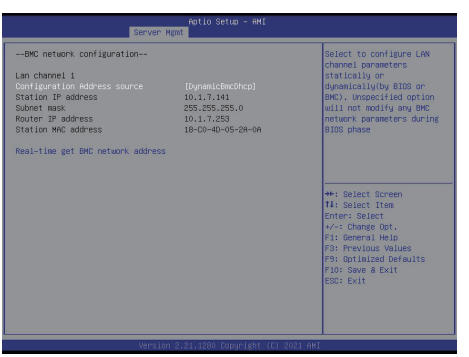
Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations

1-2 Gigabyte Management Console Network Configuration

Follow the instruction to enable the console redirection function.

1. You can gather the IP address on the POST screen.

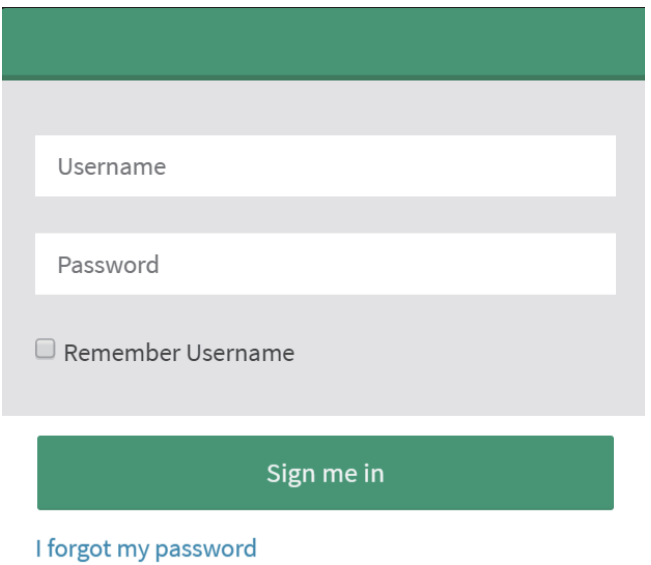
2. Or, Go to BIOS setup menu.
3. Select **Server Management**.
4. Select **BMC network Configuration**.
5. Define Configuration Address source to DynamicBmcDhcp or Static.
6. Save and Exit.
7. The **BMC IP Address** will appear on the **IPv4 Address** parameter.



8. Save the configuration and exit BIOS setup menu.

1-3 Log In Gigabyte Management Console

To access the Gigabyte Management Console, the BMC Web utility will prompt you to enter the User Name and Password.

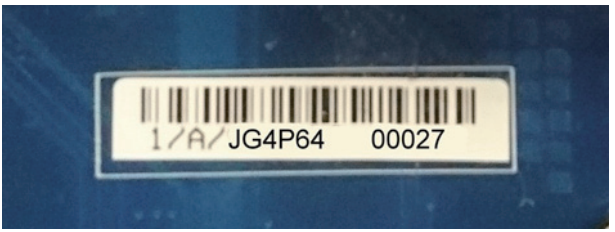


The fields are explained as follows:
For basic login to the BMC Web UI, use the following login:

- **Username**: admin
- **Password**: Refer to unique MB serial number.

NOTE!
If your motherboard / server version is older than G9 (upgrade version), then use the following login:
Username:admin
Password: password

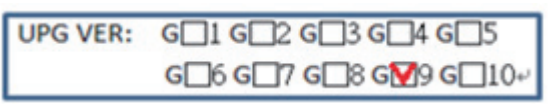
This serial number can be found on the serial number sticker located on the motherboard of every GIGABYTE server motherboard and system. The unique pre-programmed password will be the last 11 characters of the serial number. For example, for the below serial number, the password will be “JG4P6400027



GIGABYTE will also affix new stickers that display the unique BMC password (example below) to both the product box (packaging) and to the CPU cover (for motherboards sold separately) or the server chassis.

Please see the reference guide below / attached for where to find locations of this sticker according to product / model type.

Products that have been implemented with this change will be indicated as version G9 on the "Upgrade Version" sticker located on the motherboard / motherboard anti-static packaging / server chassis / server packaging



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 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.

1-3-1 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.

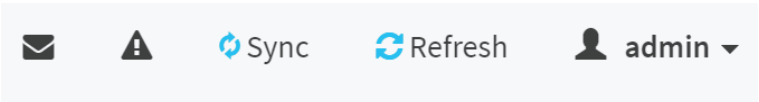
Enable javascript for this site: The icon indicates whether the javascript setting is enabled in browser.

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

Cookies must be enabled in order to access the website.

1-4 Quick Button and Logged-in User

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

Notification: Click the icon to view the notification messages.

Refresh: Click the icon to reload the current page.

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

Sign-out: Click the icon to log out of the Web GUI.

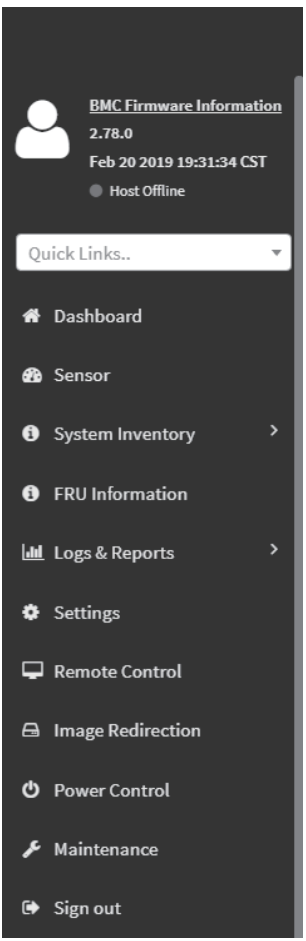
Warning: Click to view the warning messages.

1-5 Help

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

1-6 Menu Bar

The menu bar displays the following:

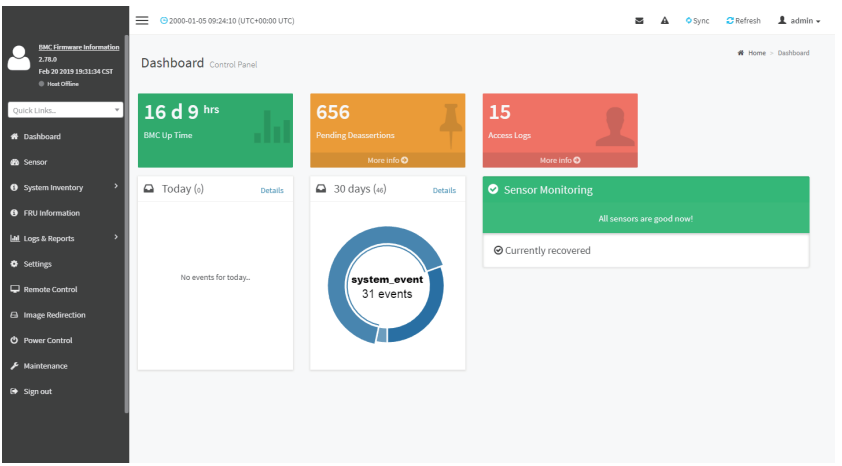


This page intentionally left blank

Chapter 2 Enter Gigabyte Management Console

2-1 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. It displays the following:



Dashboard
A brief description of the Dashboard page is given below.

BMC Up Time
It indicates the Power On time.

Pending Deassertions
It lists the all pending events incurred by various sensors and occupied/available space in logs can be viewed. To know about the pending events details, click the More info link. This navigates to the Event Log page.

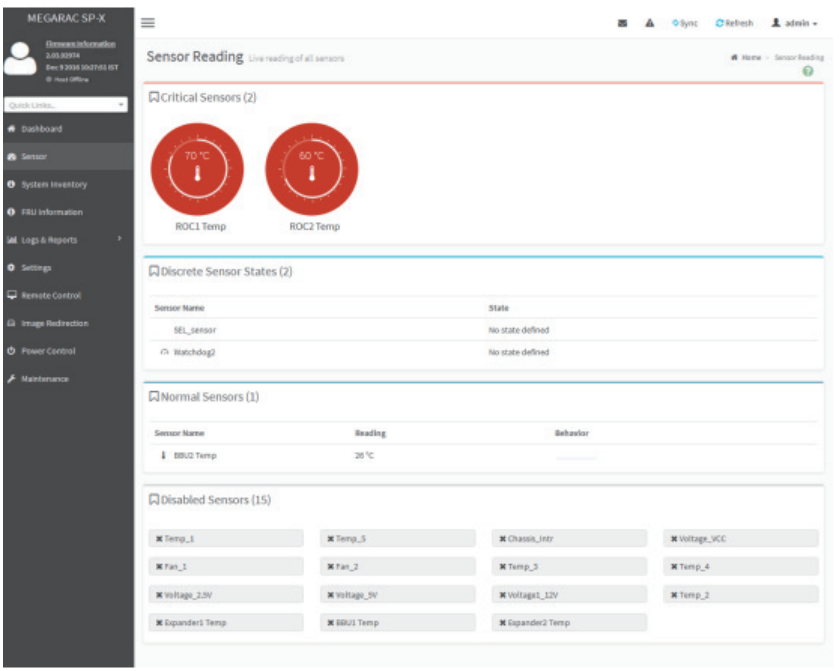
Access Logs
A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed, if you click on the More info link, you can view the Audit Log page.

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.

2-2 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.
A sample screenshot of Sensor Readings page is shown below.



The Sensor Readings page contains the following information:

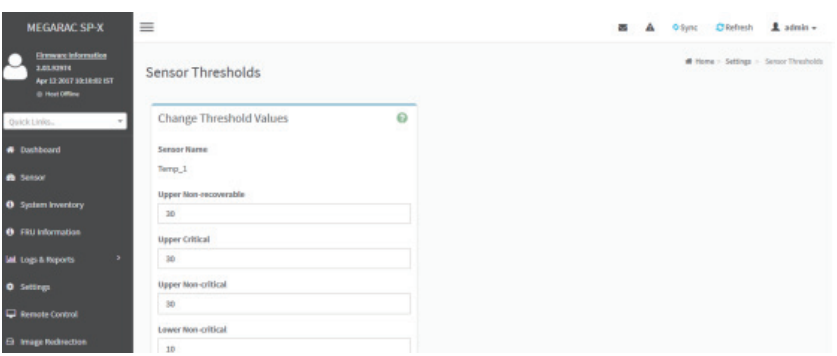
In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Status, Current Reading and Behavior will be appeared, else you can choose the sensor type that you want to display from the list. Some examples for sensors are Temperature Sensors, Fan Sensors, Watchdog Sensors and Voltage Sensors etc.
Note: Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.

Note: Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.

2-2-1 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:For Illustrative Purpose, a sample screenshot of Sensor detail page with Change Thresholds option is shown and explained 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.

There are six types of thresholds:

- 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.

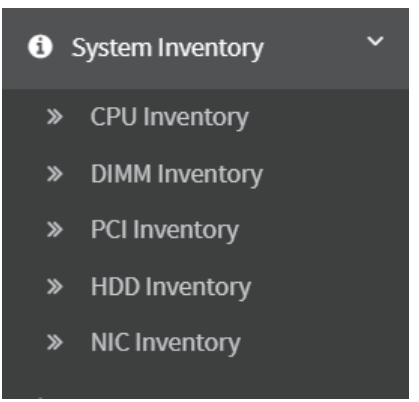
A graphical view of these events (Number of Entries vs. Thresholds) can be viewed as shown in the Sensor Readings page screenshot.

2-3 System Inventory

The System Inventory page displays the following information:

- CPU Inventory
- DIMM Inventory
- PCI Inventory
- HDD Inventory
- NIC Inventory
- GPU Inventory (Nvidia A100 only)

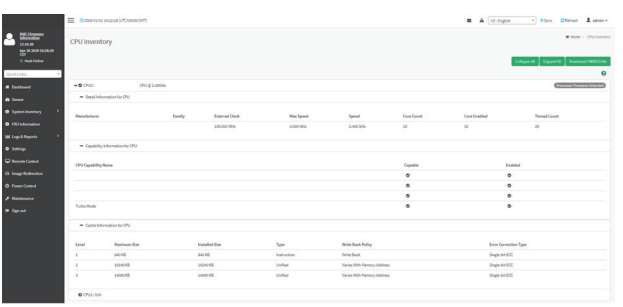
A screenshot displaying the menu items under System Inventory is shown below.



A detailed description of System Inventory is given below.

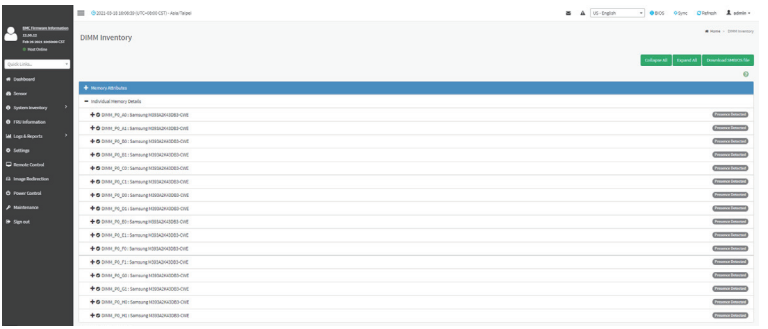
2-3-1 CPU Inventory

This page displays all detected CPUs on this device. Select one CPU to see the details of that entry or click on Expand All to view all entries in details. Click Download **SMBIOS file** to download the SMBIOS file.



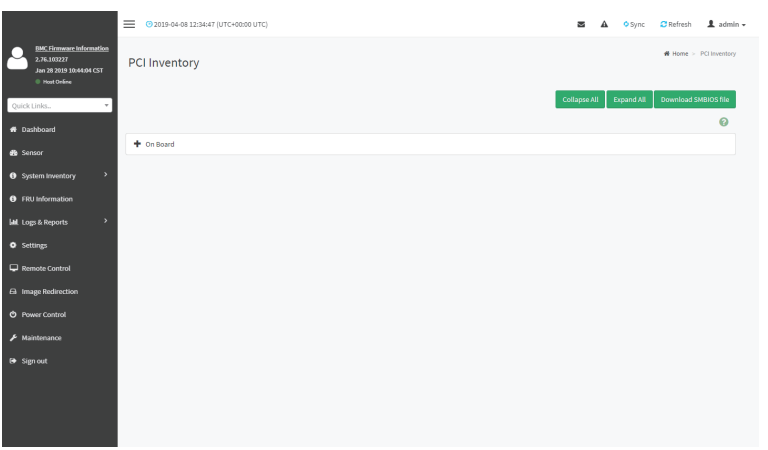
2-3-2 DIMM Inventory

This page displays all detected DIMMs on this device. It allows you to see memory attributes, individual memory details or all entries in detail by clicking on **Expand All**. Click **Download SMBIOS file** to download the SMBIOS file.



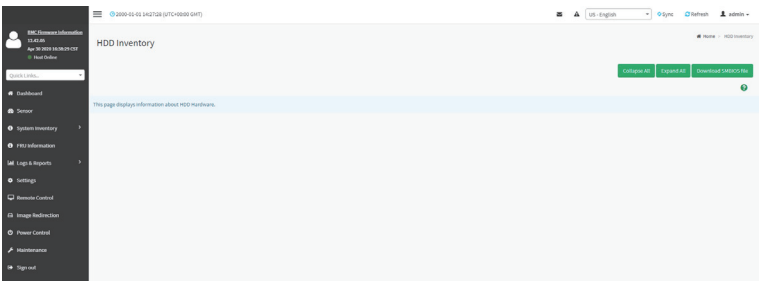
2-3-3 PCI Inventory

This page displays all detected PCI cards on this device. It allows you to see on-board PCI cards, add-on PCI cards or all entries in detail by clicking on **Expand All**. Click **Download SMBIOS file** to download the SMBIOS file.



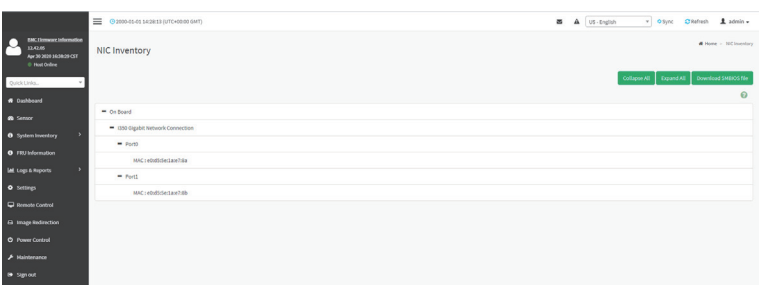
2-3-4 HDD Inventory

This page displays all detected HDDs on this device. It allows you to see on-board HDDs, add-on HDDs or all entries in detail by clicking on **Expand All**. Click **Download SMBIOS file** to download the SMBIOS file.



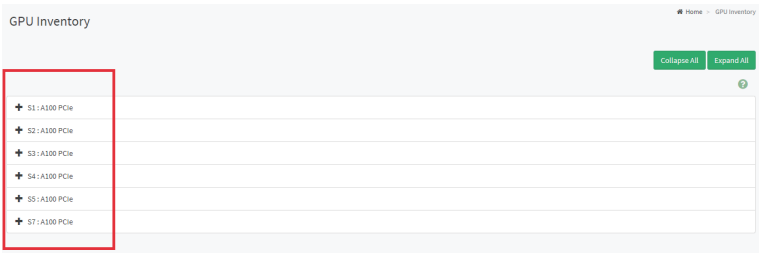
2-3-5 NIC Inventory

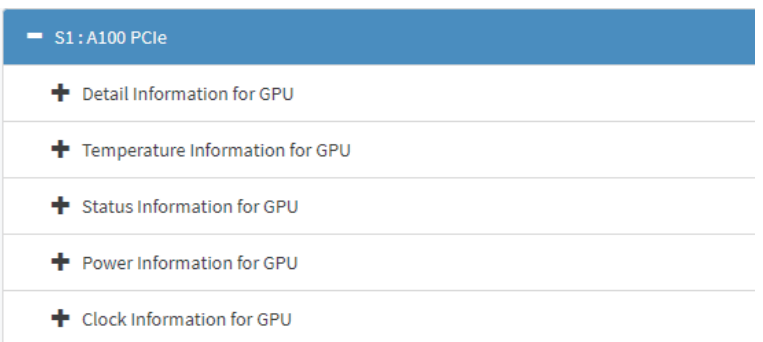
This page displays all detected NICs on this device. It allows you to on-board NICs, add-on NICs or all entries in detail by clicking on **Expand All**. Click **Download SMBIOS file** to download the SMBIOS file.



2-3-6 GPU Inventory

This page displays all detected GPU card on this device. It allows you to view GPU card all entries in detail by clicking on **Expand All**.





Detail information for GPU

- GPU Information
- Capabilities
- NVLink Information

Temperature Information for GPU

- GPU Temperature
- Extended Precision GPU Temperature

Status Information for GPU

- Accumulated Utilization
- Power Supply

Power Information for GPU

- Power Consumption

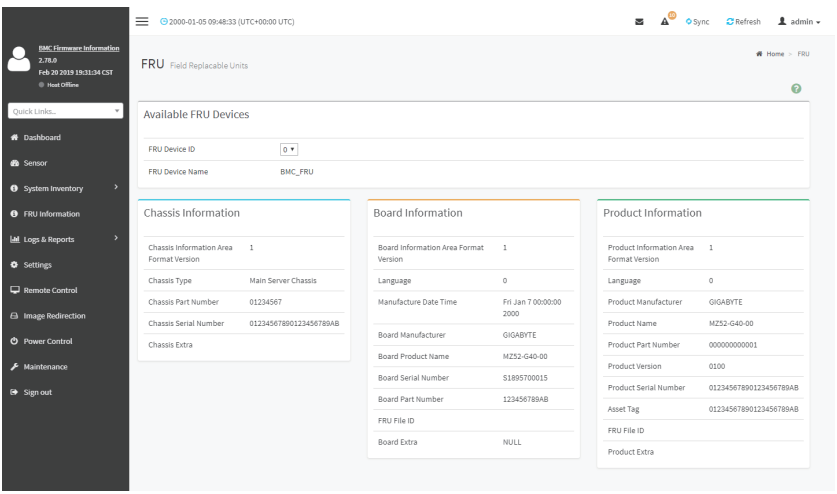
Clock Information for GPU

- Graphics Clock Frequency
- -Memory Clock Frequency

2-4 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 of the 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 shown below.



The following fields are displayed here for the 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

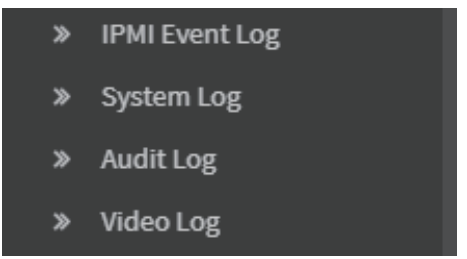
- Board Information Area Format Version
- Language
- Manufacture Date Time
- Board Manufacturer
- Board Product Name
- Board Serial Number
- Board Part Number
- FRU File ID
- Board Extra

2-5 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.



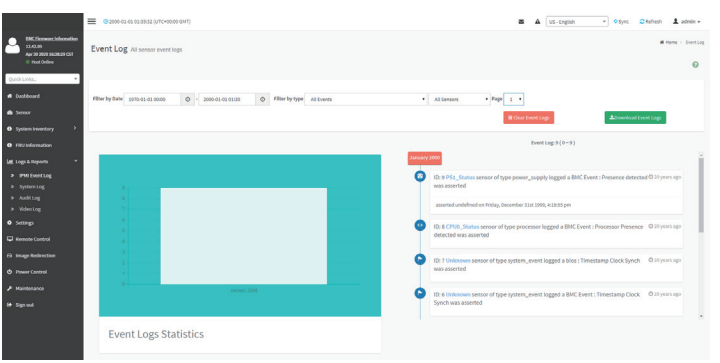
A detailed description of Logs & Reports is given below.

2-5-1 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 > IPMI 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**.

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.

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.

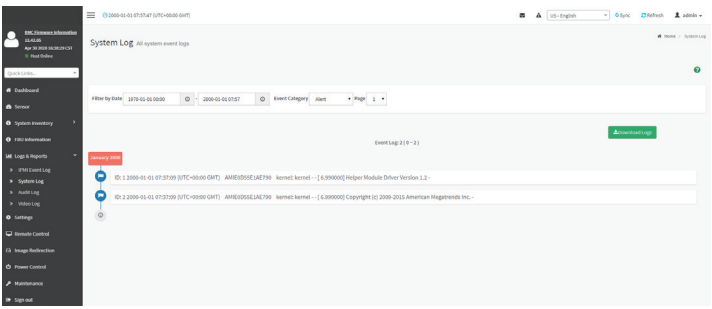
Procedure

1. From the Filter By Date field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
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**.

2-5-2 System Log

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

A sample screenshot of Video Log page is shown below.



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.

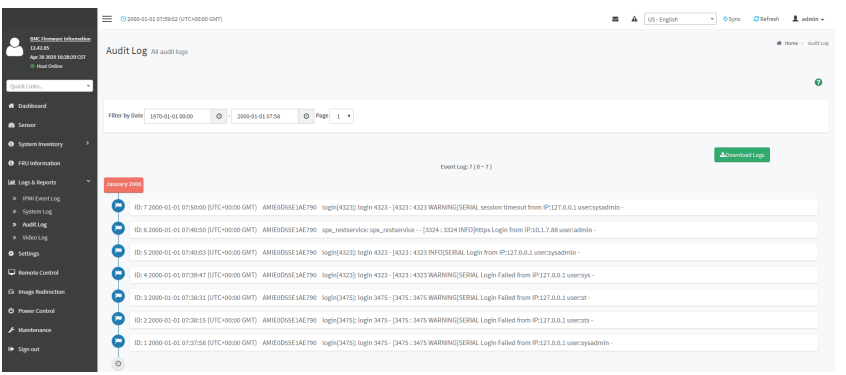
Download Event Logs: To download the event logs.

2-5-3 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.



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

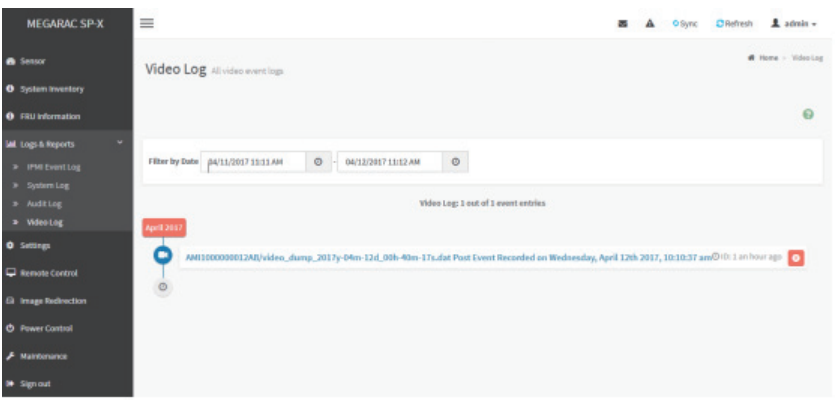
Download Event Logs: To download the event logs.

2-5-4 Video Log

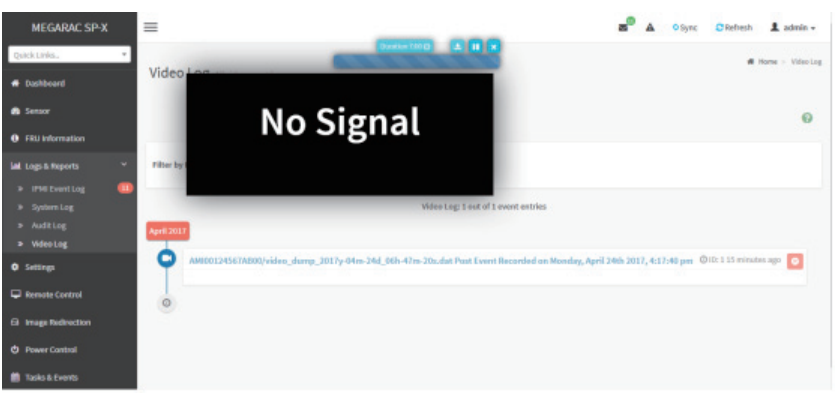
To open the Video Log page, click **Logs & Reports > Video Log** from the menu bar. A sample screenshot of Video Log page is shown below.

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**.

A sample screenshot of Video Log page is shown below.



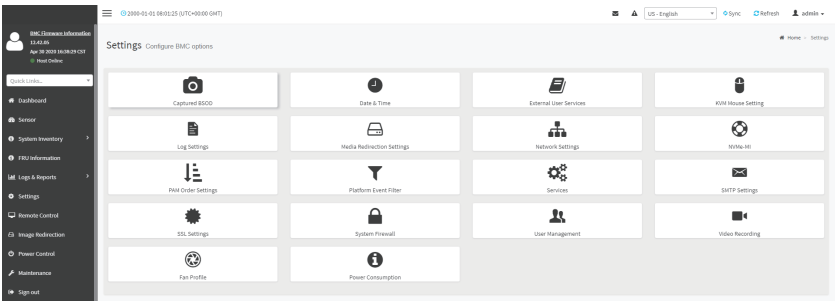
Click on the Video Log entry to view the Video. A sample screenshot of Video Log - Video page is shown below.



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.

2-6 Settings

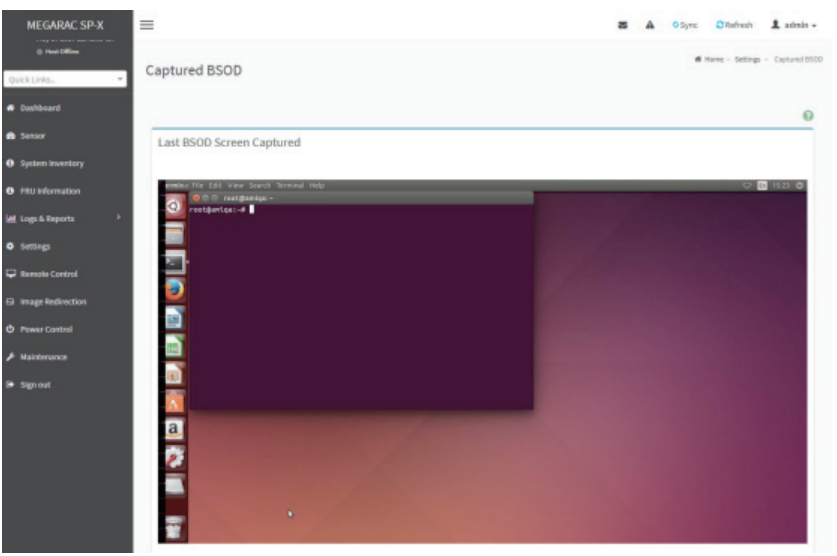
This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



A detailed description of the Settings menu is given below.

2-6-1 Captured BSOD

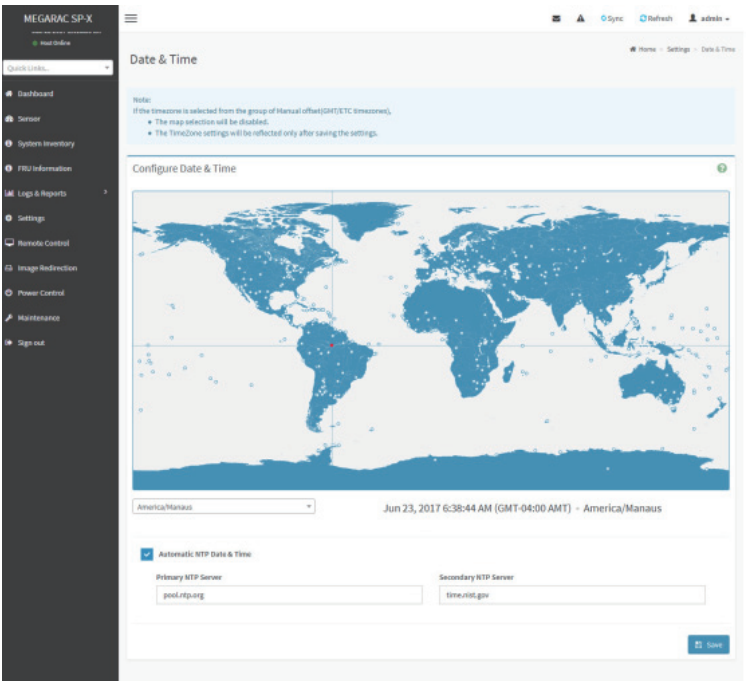
This page displays a snapshot of the blue screen captured if the host system crashed since last reboot. A screenshot of Captured BSOD is shown below.



Note: KVM service should be enabled to display the BSOD screen. KVM Service can be config¬ured under Settings->Services->**KVM**.

2-6-2 Date & Time

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



The Date & Time section consists of the following fields:

Configure Date & Time: Displays Time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.

Select Time Zone: This field is used to set the date and time on the BMC.

Automatic 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 configured 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.

Procedure

1. Select the **Timezone** location either using drop down or Map.
2. Enable Automatic Date & Time option to enable/disable the use of NTP servers to automatically set the date and time.

- In the Primary NTP Server and Secondary NTP Server fields, specify the NTP servers of the device respectively.

Note: Secondary NTP server is optional field. If the Primary NTP server is not working fine, then the Secondary NTP Server will be used.

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

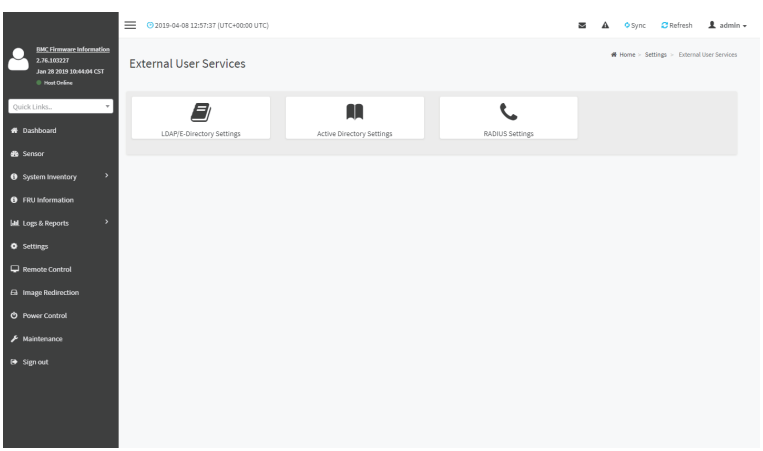
2-6-3 External User Services

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.

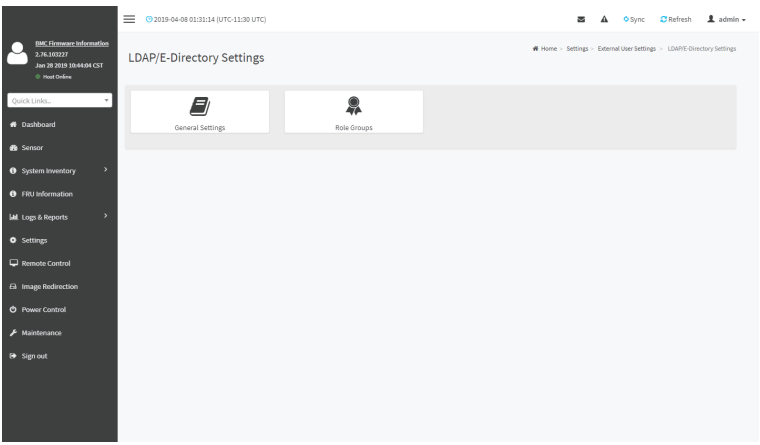
In Web GUI, LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate BMC users. This is done by passing login requests to your LDAP Server. This means that there is no need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

To open 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.

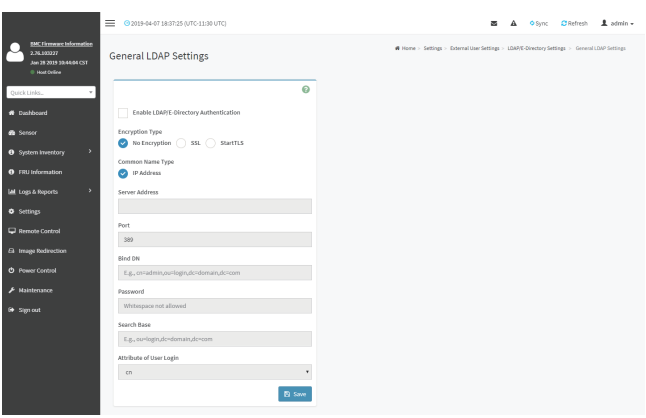
A sample screenshot of External User Services page is shown below.



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

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: Configure proper port number, when SSL is enabled.

3. Select the Common Name Type as IP Address.
4. 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 Address format and IPv6 Address format.
Configure FQDN address, when using StartTLS with FQDN.

5. 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.

6. 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

7. Enter the password in the **Password** field.

Note: Password must be at least 1 character long.
Blank space is not allowed
This field will not allow more than 48 characters.

8. Enter the **Search Base**. The Search base allows the LDAP server to find which part of the external directory tree to be searched. The search base may be something equivalent to the organization, group of external directory.

Note: Search base is a string of 4 to 63 alpha-numeric characters.
It must start with an alphabetical character.
Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
Example: ou-login, dc-domain, dc-com

9. 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.

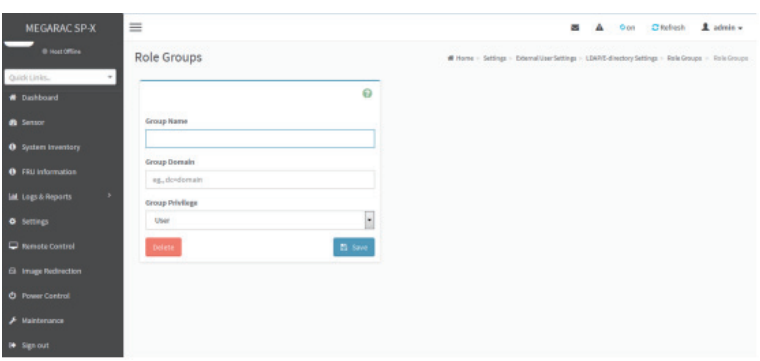
10. Select **CA Certificate File** from the Browse field to identify the certificate of the trusted CA certs.
11. Select the **CA Certificate File** to find the client certificate filename.
12. Select **Private Key** to find the client private key filename.

Note:All the 3 files are required, when StartTLS is enabled.

13. 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

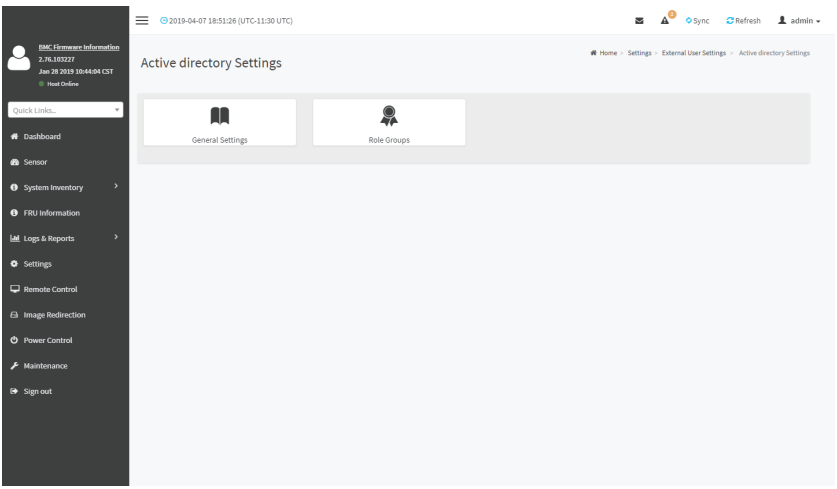
5. In the Group Privilege field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
6. Select one or both of the required options
   - KVM Access
   - VMedia Access
7. Click **Save** to save the new role group and return to the Role Group List.

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.



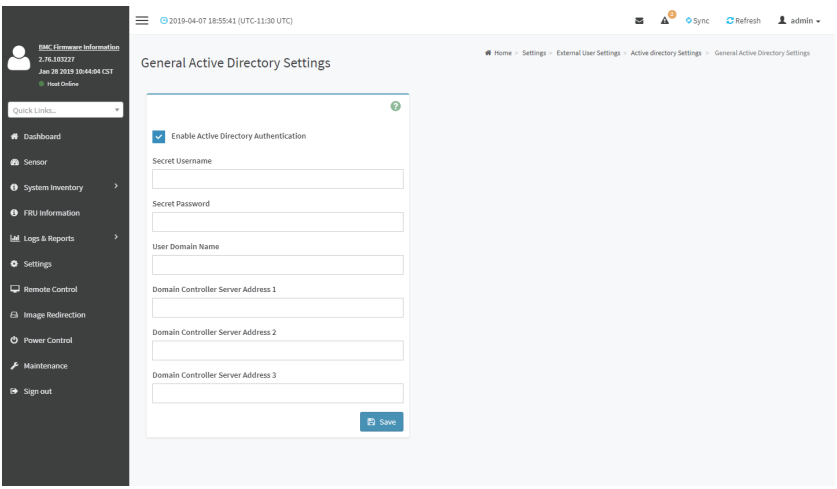
The fields of Active Directory page are explained below.

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 the Active Directory Settings page, check or uncheck the **Enable Active directory Authentication** check box to enable or disable **Active Directory 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 fields 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,
Blank space is not allowed, 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.

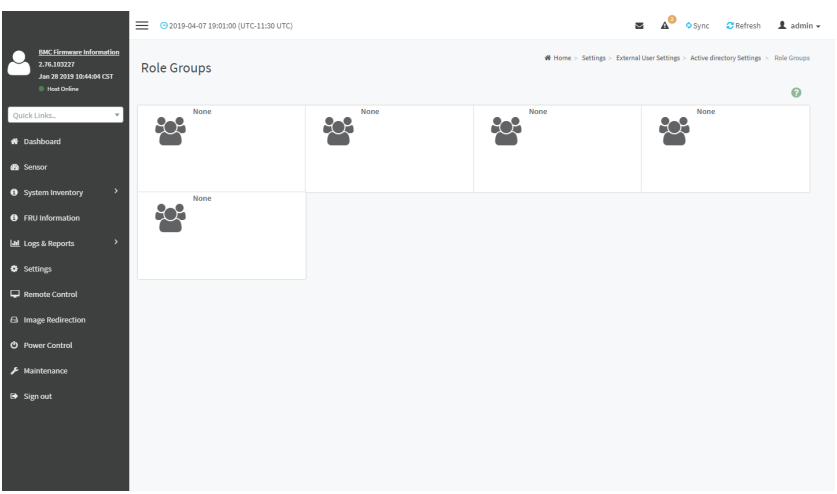
4. Specify the Domain Name for the user in the User Domain Name field. E.g. MyDomain.com
5. Configure IP addresses in Domain **Controller Server Address1, Domain Controller Server Address2 and Domain Controller Server Address3**

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.

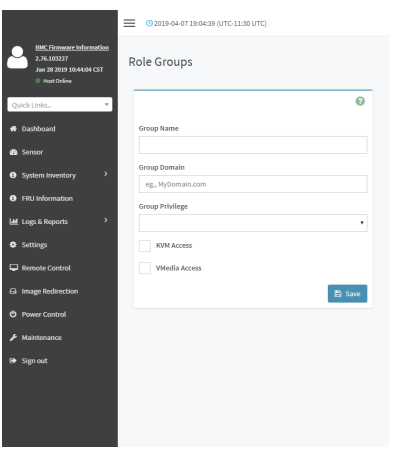
Group Domain: The domain where the role group is located.

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.

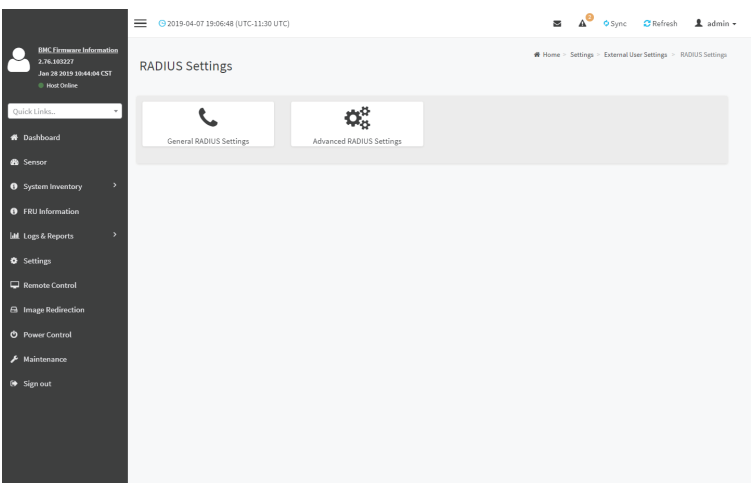
5. Select the required options
   - KVM Access
   - VMedia Access
6. Click **Save** to add the new role group and return to the Role Group List.

To Delete a Role Group

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

RADIUS Settings

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



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.

Blank space is not allowed.

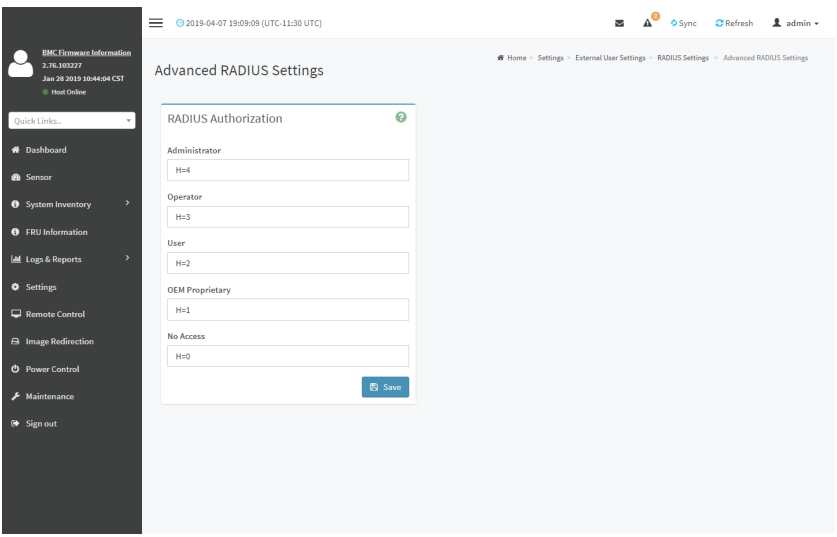
Enable KVM Access: This field provides access to KVM for RADIUS authenticated users.

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

Save: To save the configured 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.



Note: 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

test operator Auth-Type: = PAP, Cleartext-Password:= “operator”

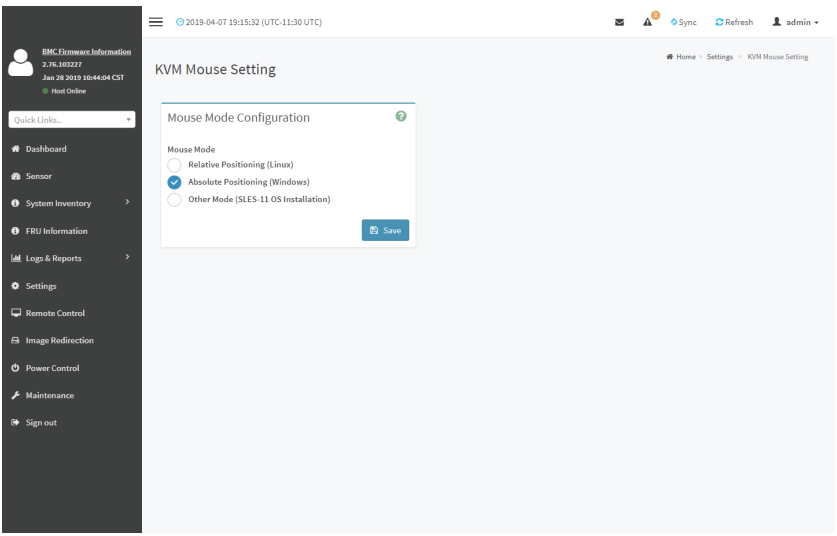
Auth-Type: =PAP, Vendor-Specific= ”H=3 ”

If you change the Vendor-Specific value in server then you should change the same values in this page.

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

2-6-4 KVM Mouse Settings

In BMC Web GUI, 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.
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.
Save: To save the current changes.

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

   - Mode to Other Mode

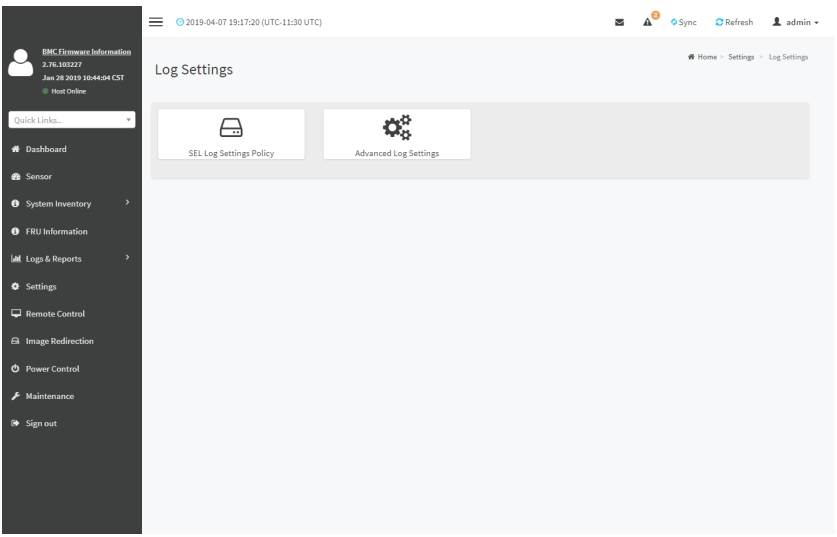
Note: Recommended for SLES-11 OS Installation

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

2-6-5 Log Settings

In BMC Web GUI, System and Audit log page displays a list of system logs and audit logs occurred in this device.

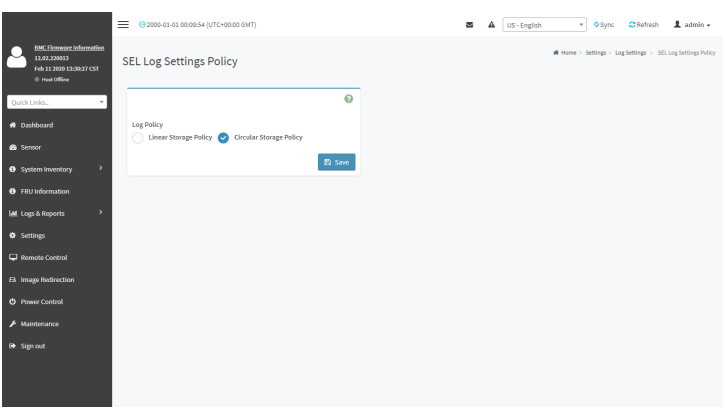
To open Log Settings page, click **Settings > Log Settings** from the menu bar. A sample screenshot of Log Settings page is shown below.



The fields of Log Settings page are explained below.

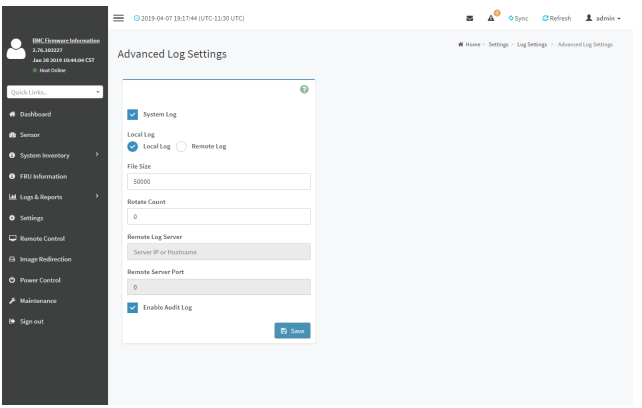
SEL Settings Policy

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



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 follows.
Enable System Log: This field is to enable or disable the System Logs.
Location: Specifies the Location for system logs, whether it should be preserved in a **Local Log** or on a **Remote Log**.

Note: Local file resides at /var/log/

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).

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

Note: Values supported are 0 and 1.
When log information exceeds the file size, the old log information is automatically moved to back up files based on the rotate count value. If rotate count is zero, then old log information gets cleared permanently.
File Size and Rotate Count options will be available only when Local Log is enabled.

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.

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 current 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.

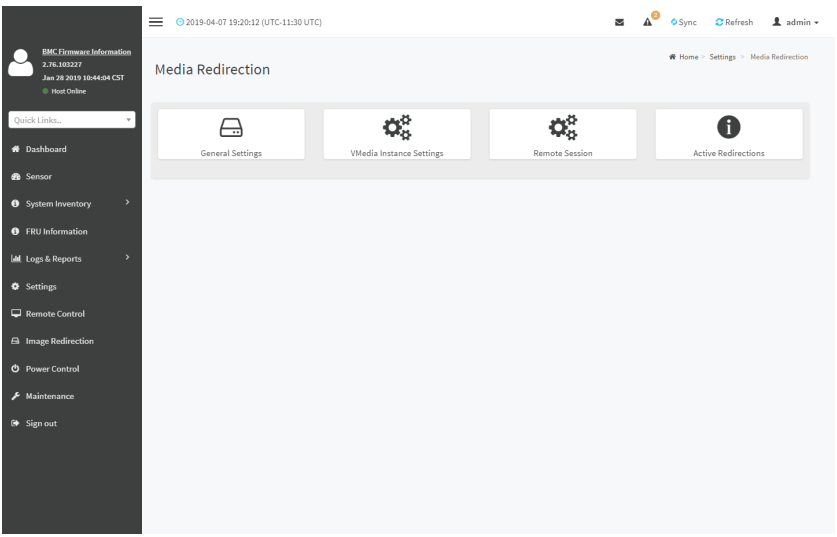
Steps to configure the remote server to enable syslogging

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

2-6-6 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.



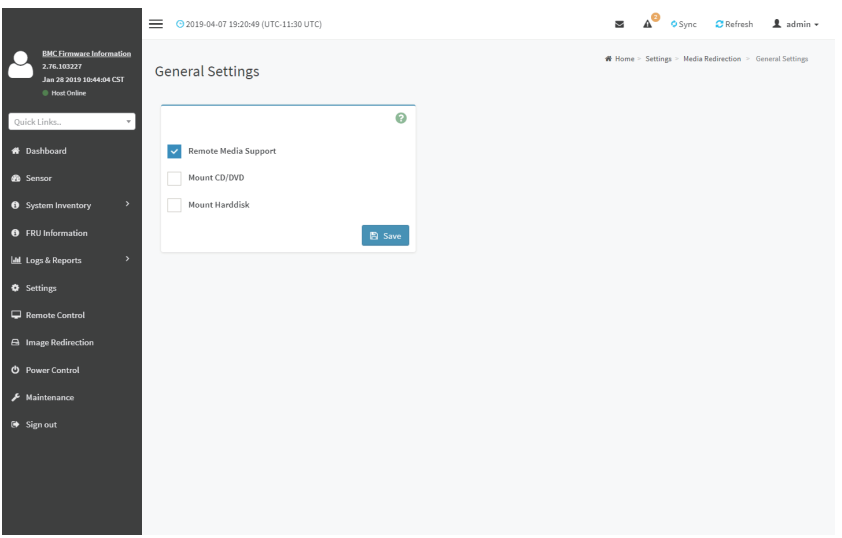
The fields of Media Redirection page are explained below.

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

General Settings

This option is used to configure General Media Settings.

To open General Media Settings section, click **Settings > Media Redirection Settings** > General Settings.

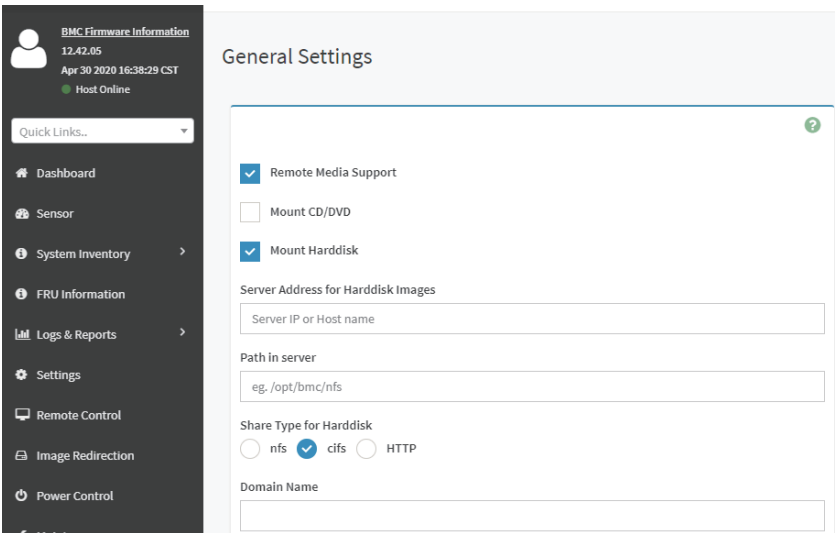


Remote Media Support: To enable or disable Remote Media support, check/uncheck the 'Enable' check box.

If it is selected, then the following Remote Media types will be displayed.

- Mount CD/DVD
- Mount Harddisk

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.



Note: You can also select all the media types simultaneously.
Server Address for CD/DVD Images: Displays the address of the server where the remote media images are stored.

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.

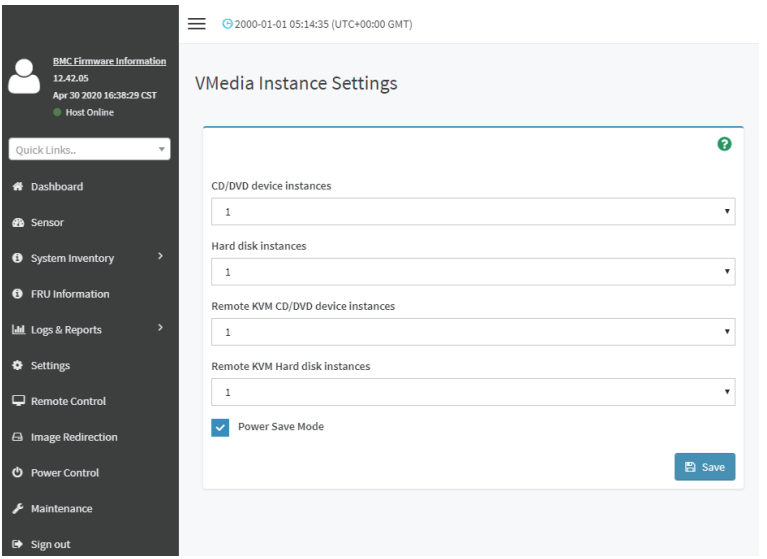
Share Type for Harddisk: To Select Share Type for Floppy.

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

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

Remote KVM Hard disk instances: The number of Hard disk devices supported for KVM 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 will be blocked when any active media redirection is present.

Procedure

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

Note: Maximum of four devices can be added in Floppy, CD/DVD and Harddisk 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.

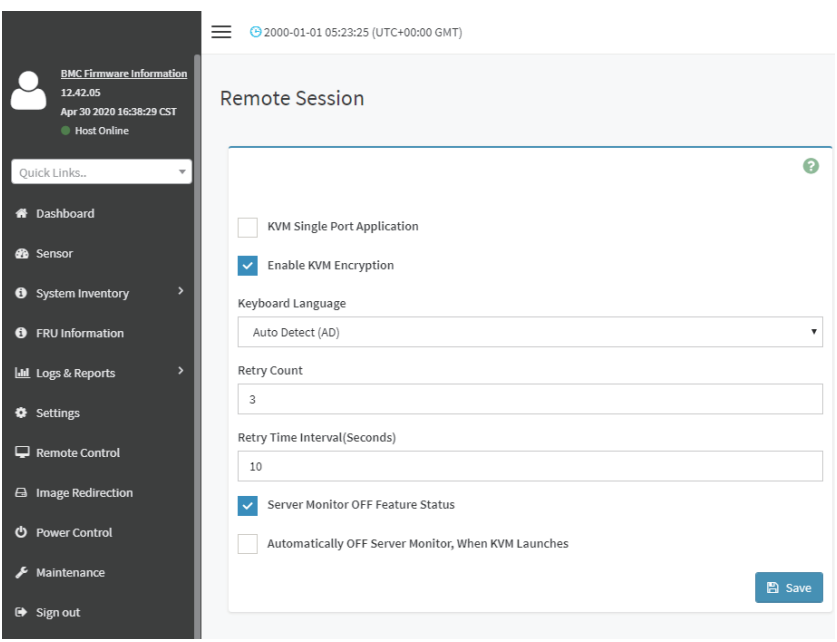
Note: When KVM is launched from Standalone Application, if there are two device panels for each device, and when you click the Connect button, then the redirected device panel will be disabled.
Unmounting device will make the driver disconnect device when using **Auto Attach**. Hence, when unmounting one USB key, the other USB key will be disconnected and then reconnected.

Remote Session

In BMC Web, this page is used to configure Remote Session configuration settings. “KVM Single Port Application” is enabled by default. On disabling, “KVM Single Port Application”, “Encrypt H5Viewer KVM packets” will be enabled by default. On enabling “KVM Single Port Application”, “Encrypt H5Viewer KVM packets” will be disabled if it is enabled already.

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 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.

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.

Note: Installation of Operating System on the servers via BMC CD ISO image over remote KVM may take 1 to 2 hours.

Procedure

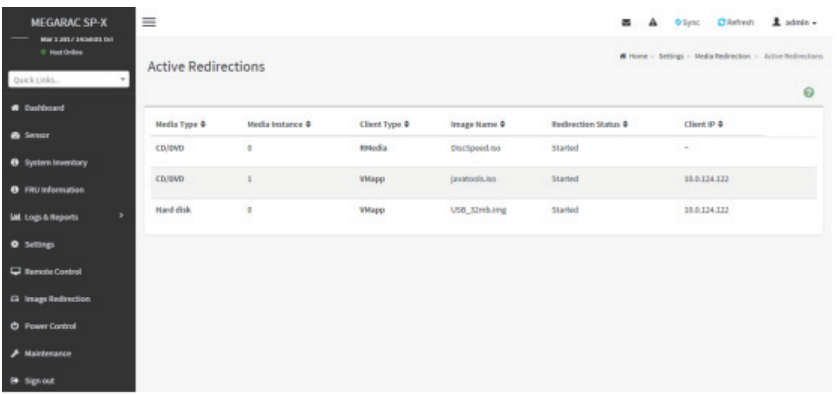
1. Check or uncheck the **KVM Single Port Application** option to enable Single Port Application support in BMC.
2. Choose the **Keyboard Language** from the list of keyboard supported languages.
3. Enter a value in the **Retry Count** field to set the number of attempts for retrying the redirection session.
4. Enter a value in the **Retry Time Interval (Seconds)** field to give time interval for each attempts.
5. Check the **Server Monitor OFF Feature Status** check box to enable Local Monitor ON/

OFF command during runtime.

6. Check the **Automatically OFF Server Monitor**, **When KVM Launches** check box to automatically Lock the local monitor during H5Viewer launch.
7. Click **Save** to save the current changes.

Active Redirections

This page displays a list of Media which are being redirected currently. It shows current status and other basic information about the Media.

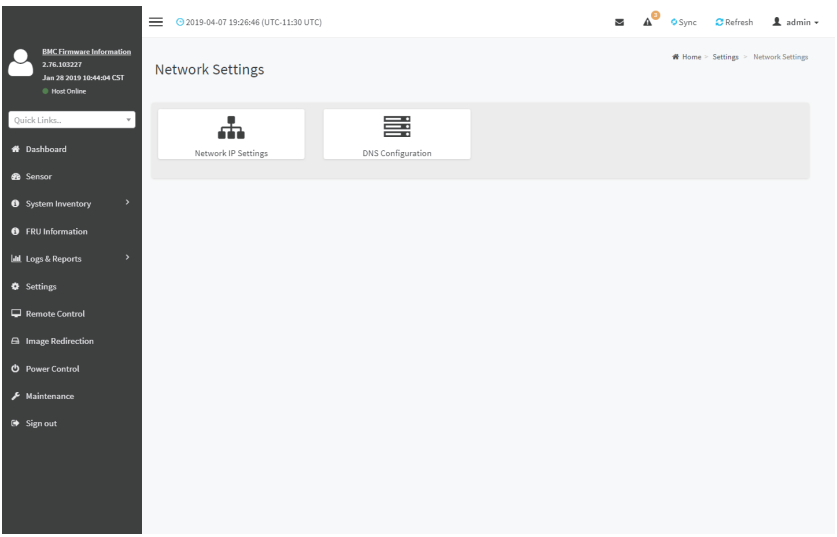


The following fields are displayed in this page.
Media Type: The type Media devices (CD/DVD) supported for Active Redirections.
Media instances: The number of Media devices supported for Active Redirections.
Client Type: The type Media devices (CD/DVD) supported for Active Redirections.
Image Name: The 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.

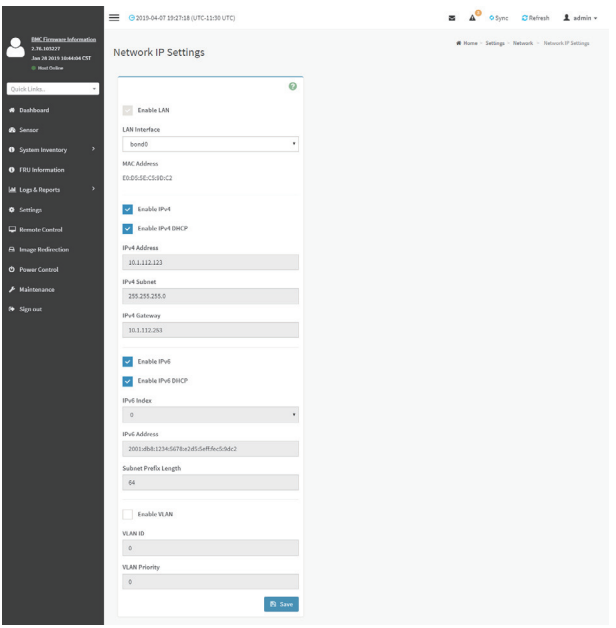
2-6-7 Network Settings

The Network Settings page is used to configure the network settings for the available LAN channels. It also allows users to manage the DNS settings or configure Network Controller Sideband Interface of a device. To open the Network Settings page, click **Settings > Network Settings** from the menu bar.



Network IP Settings

To open Network IP 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 IPv4: 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. E.g.: 0

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

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

Note: Value ranges from 0 to 128.

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

Note: If core feature IPV6_COMPLIANCE is 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

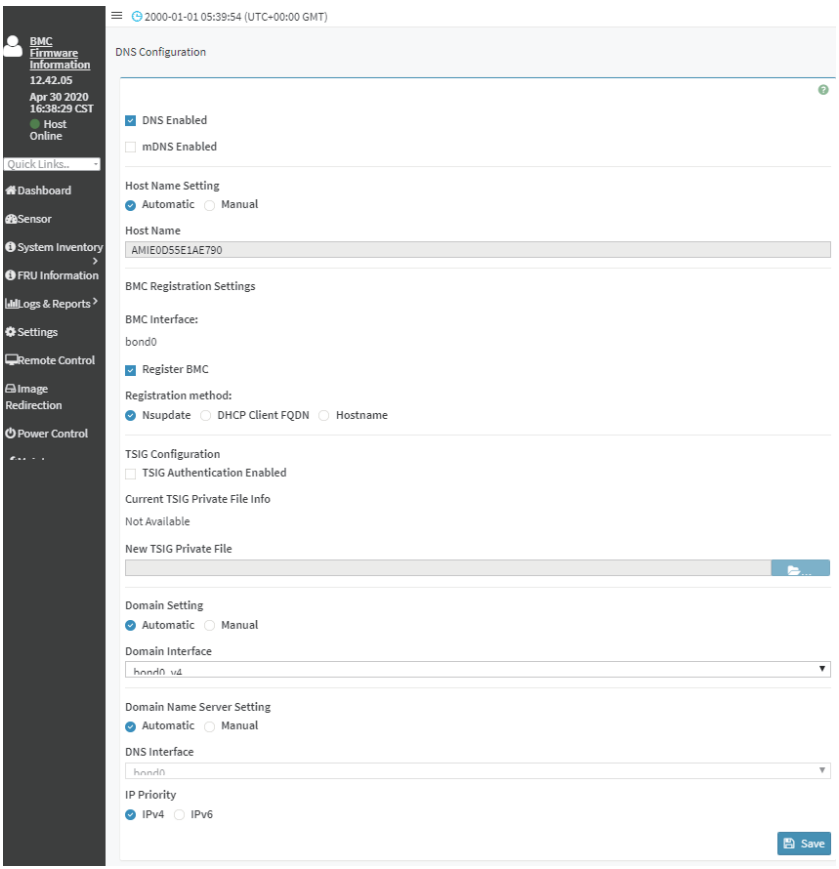
1. Check **Enable LAN** to enable LAN support for the selected interface.
2. Select the **LAN Interface** to be configured.
3. Check Enable IPv4 to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, 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. 11. Enter the **VLAN Priority** in the specified field.
12. Click **Save** to save the entries.

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.



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 through the Interfaces (eth0&eth1).

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 Configuration

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**: It displays the domain name of the device.

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 current 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.

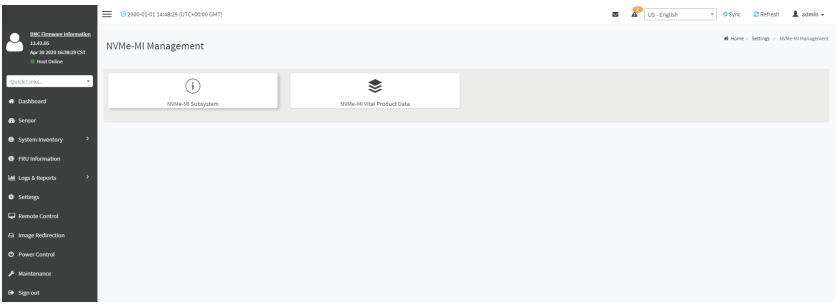
3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
4. Under Register BMC, choose the BMC's network port to register with DNS settings. Check **Register BMC** option to register with DNS settings.
   - **Nsupdate** - Choose Nsupdate option to register with DNS server 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 12.

Note: Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.

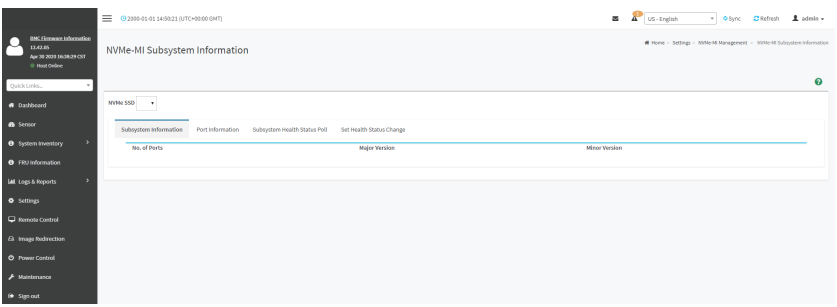
5. Check **Both** option to modify TSIG authentication for both interfaces (eth0&1).
6. In **Eth 0&1 TSIG Configuration**, Check TSIG Authentication Enabled option to enable/ disable TSIG authentication while registering DNS via nsupdate.
   - The current file name will be displayed in Current TSIG Private 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.

2-6-8 NVMe MI Management

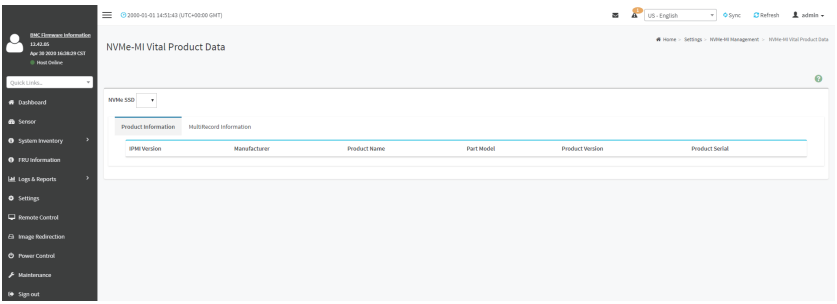


NVMe-MI Subsystem Information



In selecting any particular NVMe SSD, the corresponding NVMe SSD Subsystem Information, Port Information, Subsystem Health Status Poll and Set Health Status Change will be displayed.
Click on 'Clear All' button to clear all Composite Controller Status Flags at a time under 'Subsystem Health Status Poll' information tab.
Click on 'Clear' button to clear individual Composite Controller Status Flags under 'Set Health Status Change' information tab.

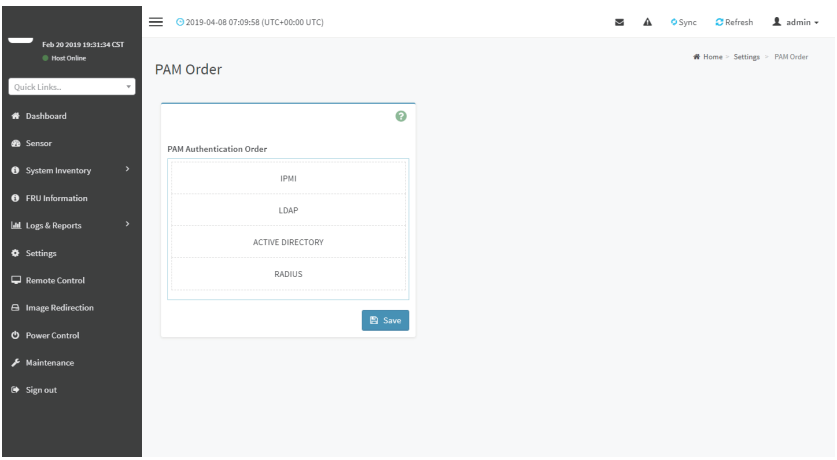
NVMe-MI Vital Product Data



On selecting any particular NVMe SSD, the corresponding SSD's Product Information will be displayed. It displays detailed information like IPMI Version, Product Name, Part Model, Product Version etc.. of the NVMe SSD. On Click of 'Multi Record Informaion' tab NVMe MultiRecord and NVMe PCIe Port MultiRecord will be displayed.

2-6-9 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:



The fields of **Setttings > PAM Ordering** page are explained below.

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

Note: It is recommended to not to keep same username for different PAM modules.
If Authentication fails, the reason of fail could be invalid User or Invalid Password.
If Radius Authentication fails, we can't differentiate whether it is invalid user or invalid password. So it is always treated as Invalid username error and PAM will try other Authentication Methods.
If AD contains secret username & 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.

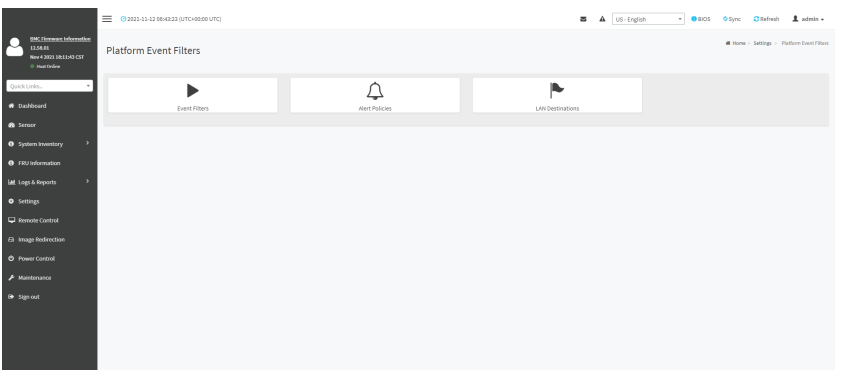
2-6-10 Platform Event Filter

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.

In BMC Web GUI, the PEF Management is used to configure the following:

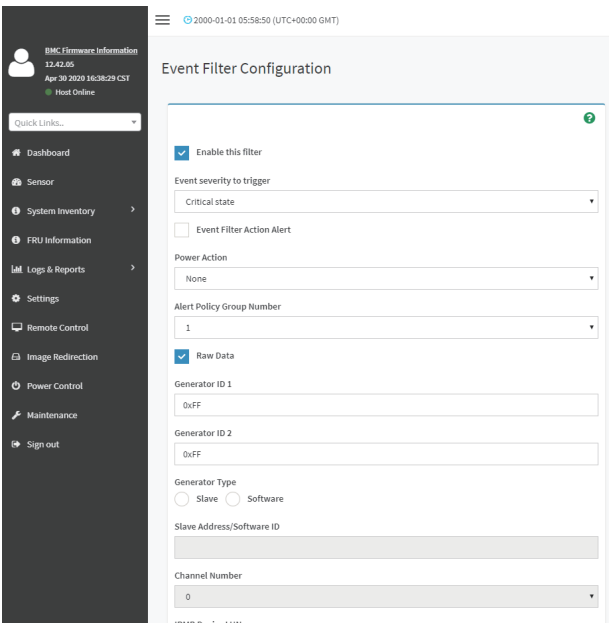
- Event Filters
- Alert Policies
- LAN Destinations

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



Event Filters

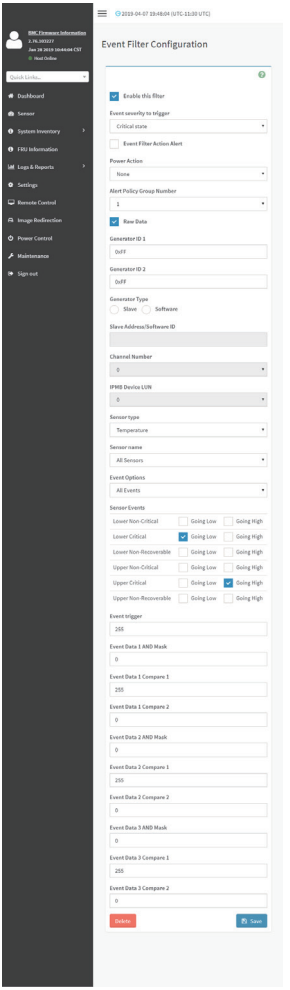
A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM'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



The fields of Platform Event Filters Tab are explained below.
This page contains Pre-configured 40 Events with PEF IDs.

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.



In the Event Filter Configuration section:

- In Enable this filter, check this option to enable the PEF settings.
- In Event Severity to trigger, select any one of the Event severity from the list.
- Check Event Filter Action Alert to enable alerts for event filter actions.
- 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 ID 1 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 **SensorName** field, choose the particular sensor from the sensor list.
- Choose **Event Option** to be either All Events or Sensor Specific Events.
- In the Sensor Events field, choose the type of event levels.
- **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 1 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.

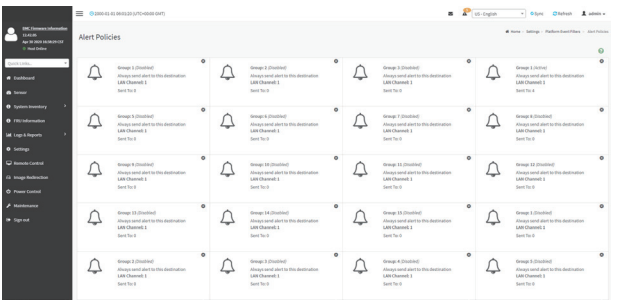
Note: Value ranges from 1 to 255.

- **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.

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.

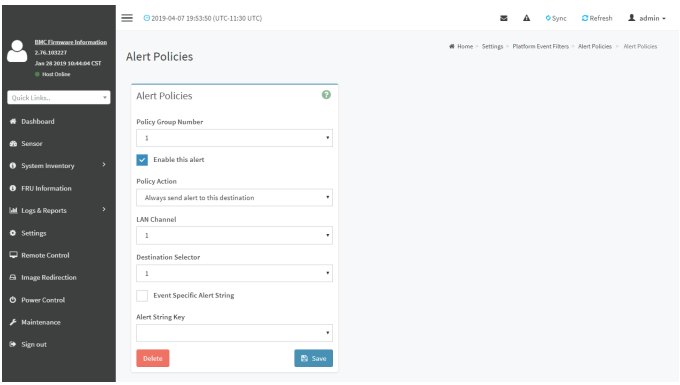
Save: To save the Alert Policies entries.

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.

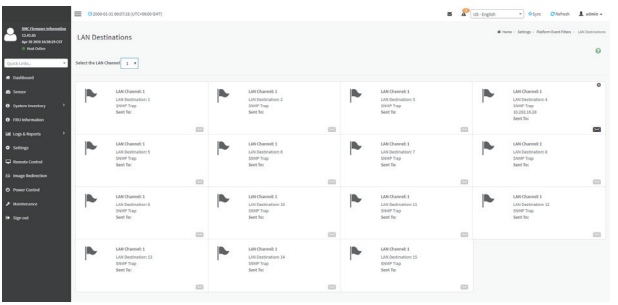
8. Enable **Event Specific Alert String**, if the Alert policy entry is Event Specific.
9. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

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").

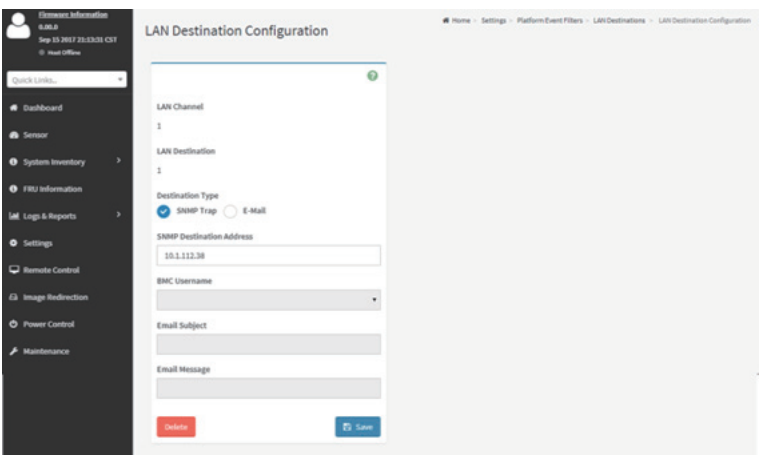
10. Click **Save** to save the new alert policy and return to Alert Policy list.
11. Click **Delete** to delete a configuration.

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 (read-only).
Destination Type: 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. 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-->User Management.

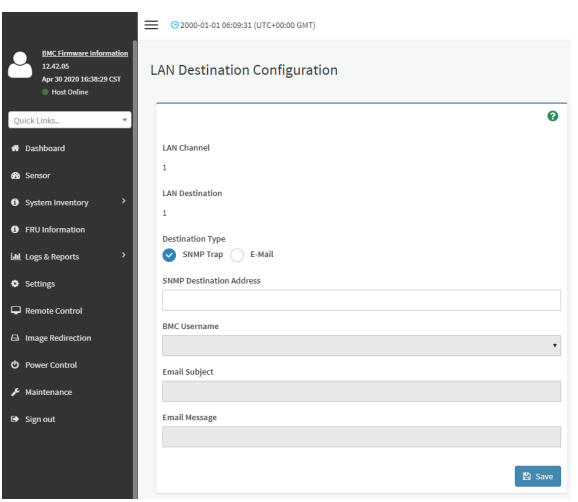
Email Subject & Email Message: These fields must be configured if email alert is chosen as destination type. An email will be sent to the configured email address of the user in case of any severity events with a subject specified in subject field and will contain the message field's content as the email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

Note: User should be configured under Settings-->User 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.
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**.

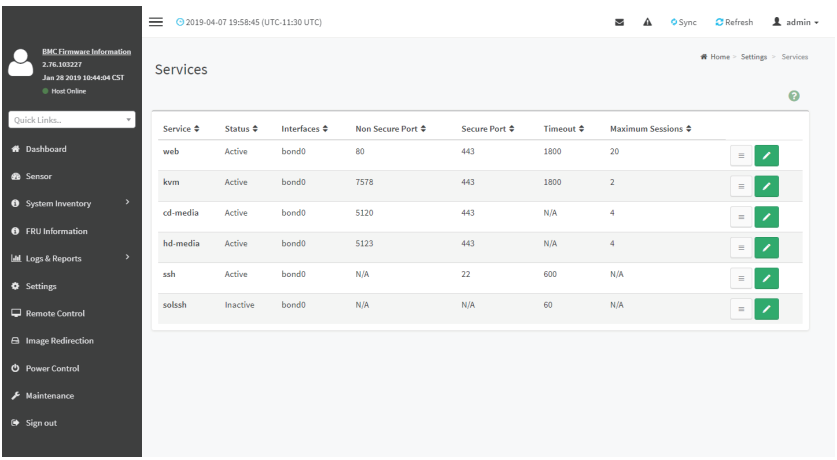
8. In the **Email Subject** field, enter the subject.
9. In the **Email Message** field, enter the message.
10. Click **Save** to save the new LAN destination and return to LAN destination list.
11. Click **Delete** to delete a configuration.
12. Click **Send Test Alert** to send sample alert to configured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

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

2-6-11 Services

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
- FD Media default port is 5122
- 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, FD Media and HD Media ports cannot be edited. Port value ranges from 1 to 65535.

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

- Web default port is 443

- KVM default port is 7582
- CD Media default port is 5124
- FD Media default port is 5126
- HD Media default port is 5127
- SSH default port is 22

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 (LP) 7578 (EO)	7578 (LP) 7578 (EO)	7578(LP) 7578 (EO)	7578(LP) 7582 (EO)
Cdserver	5120 (LP)	5120 (LP) 5120 (EO)	5120 (LP) 5120 (EO)	5120 (LP) 5124 (EO)	5120 (LP) 5124 (EO)
Fdserver	5122 (LP)	5122 (LP) 5122 (EO)	5122 (LP) 5122 (EO)	5122 (LP) 5126 (EO)	5122 (LP) 5126 (EO)
Hdserver	5123 (LP)	5123 (LP) 5123 (EO)	5123 (LP) 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 Imedia/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.

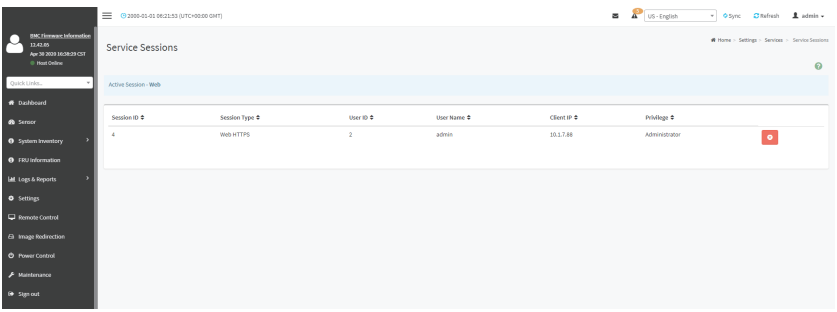
Note: Web timeout value ranges from 300 to 1800 seconds.
KVM timeout value ranges from 300 to 1800 seconds.
SSH and Telnet timeout value ranges from 60 to 1800 seconds.
SSH and Telnet timeout value ranges from 60 to 1800 seconds.
SSH and telnet service will be using the same timeout value. If you configure 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.

Procedure to view the Active Sessions:

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.



Session Type: Displays the type of the active sessions.
User: 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.

3. Select a slot and click Terminate icon ( ) to terminate the particular session of the service.
   To modify the existing services:
4. Select a slot and click Edit icon ( ) to modify the configuration of the service.

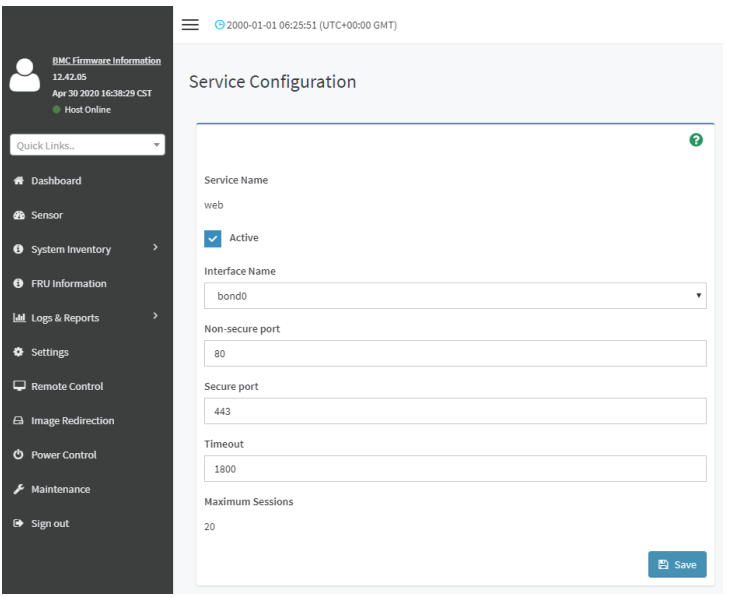
Note: Whenever the configuration is modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

Procedure to modify the existing services:

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, Non-secure 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.

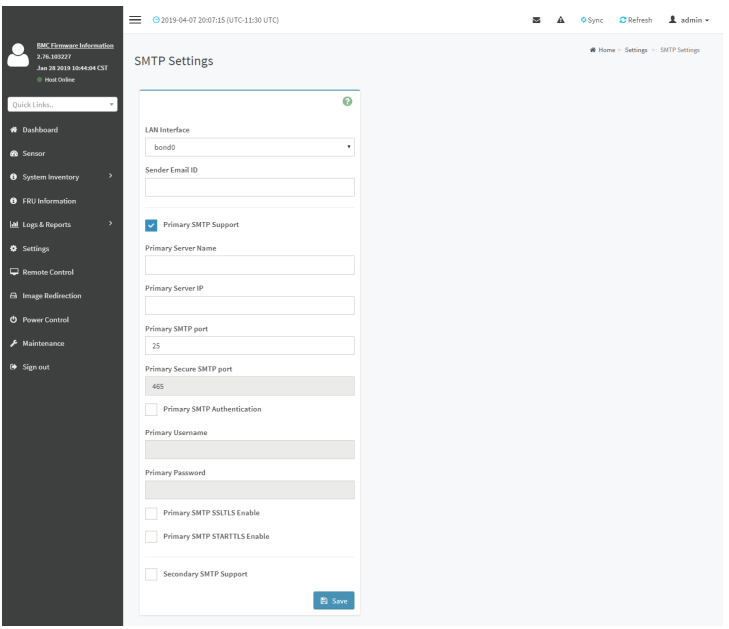
9. Click **Save** to save all changes you have made, else click **Cancel** to exit.

2-6-12 SMTP Settings

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

Using BMC Web GUI, you can configure the SMTP settings of the device.

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 Characters are not allowed.

Primary Password: Enter password for the SMTP User Account.

Note: Password must be at least 4 characters long.
Blank 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,LOGIN
- **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 uses 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.

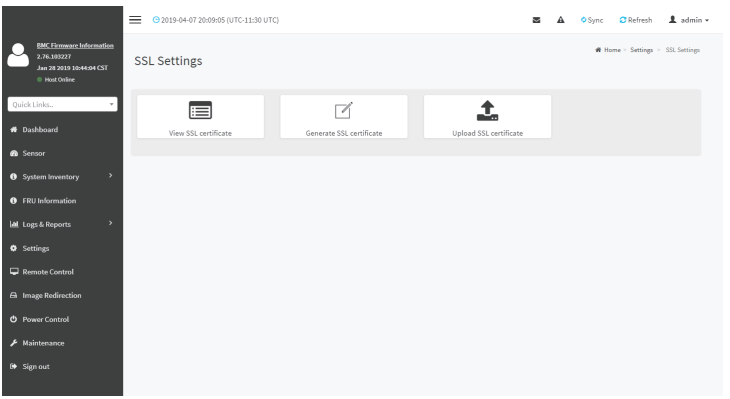
16. Click **Save** to save the entered details.

2-6-13 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.

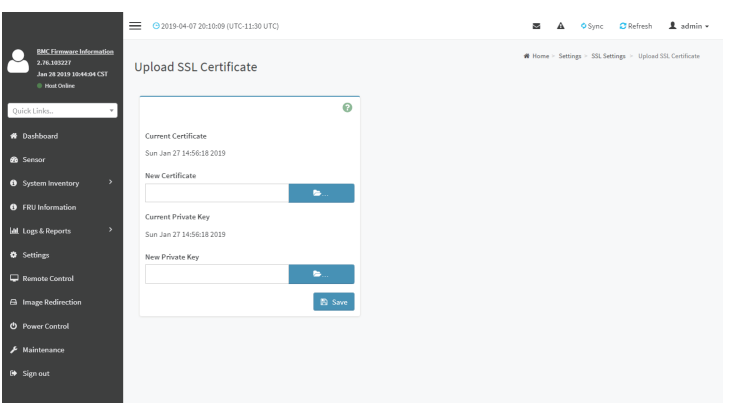
Using BMC Web GUI, configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode.

To open the 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.

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).

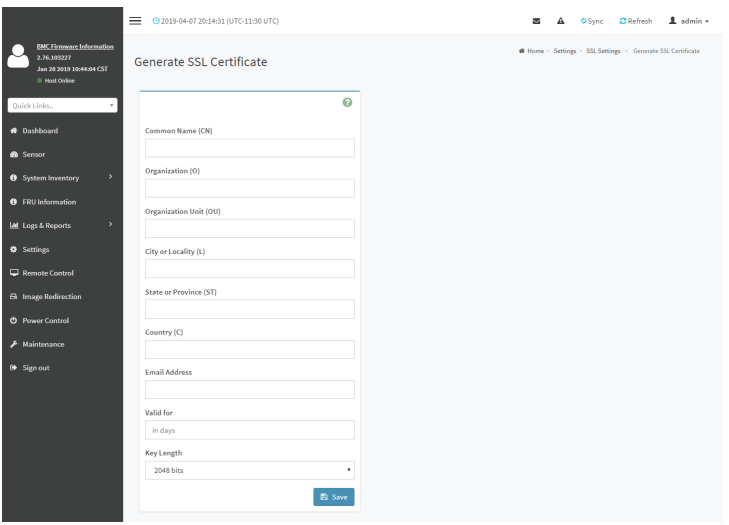
New Certificate: Certificate file should be of pem type

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 restart to use the newly uploaded SSL certificate.



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.

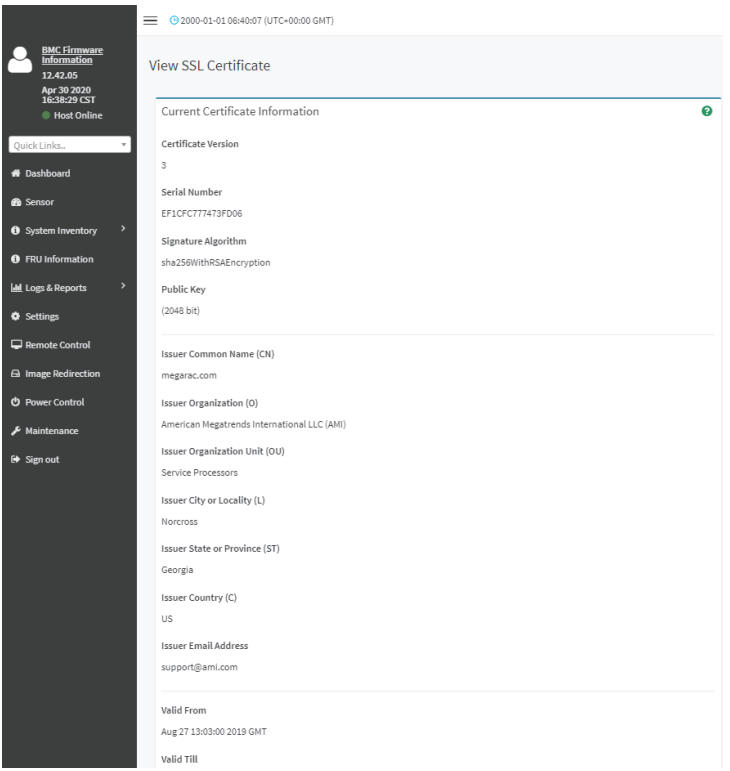
Email Address: E-mail Address of the organization (mandatory).
Valid for: Validity of the certificate.

- 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.

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

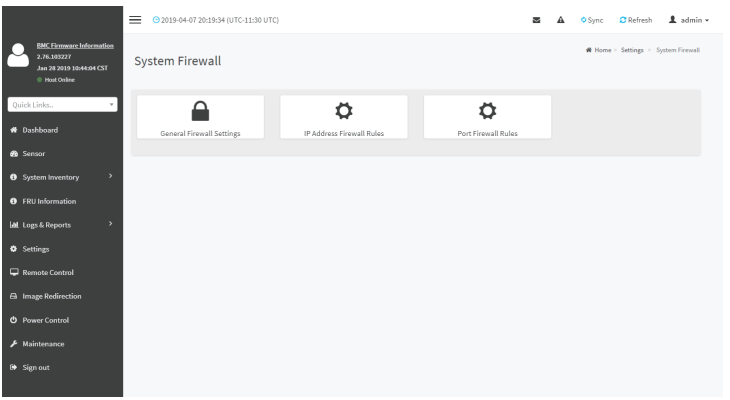
1. Click the Upload SSL Certificate tab, Browse the New Certificate and New Private key.
2. Click Upload to upload the new certificate and private key.
3. In Generate SSL Certificate, enter the following details in the respective fields:
   - The **Common Name** for which the certificate is to be generated.
   - 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 Web securely using the following format in your IP Address field from your Internet browser: https://<your BMC's IP address here>
For example, if your BMC's IP address is 192.168.0.30, enter the following: https://192.168.030
Please note the <s> after **<http>**. You must accept the certificate before you are able to access your Web.

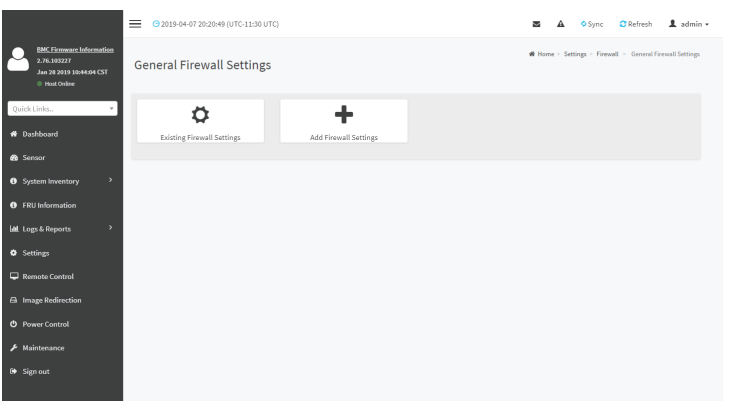
2-6-14 System Firewall

In MegaRAC GUI, 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.



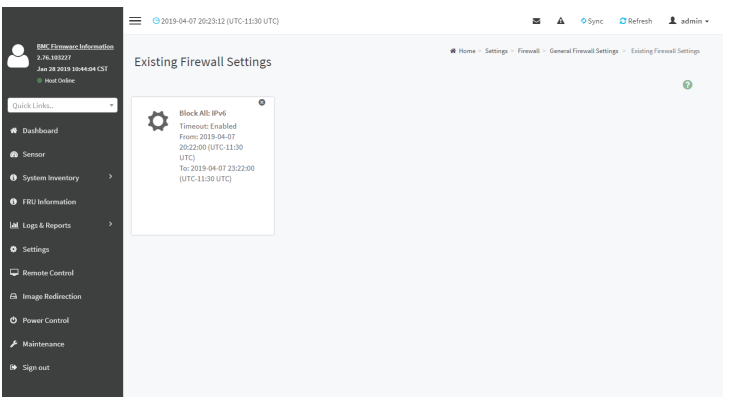
General Firewall Settings

Click **General Firewall Settings** page. A sample screenshot of General Firewall Settings page is shown below.



To View Existing Firewall Settings

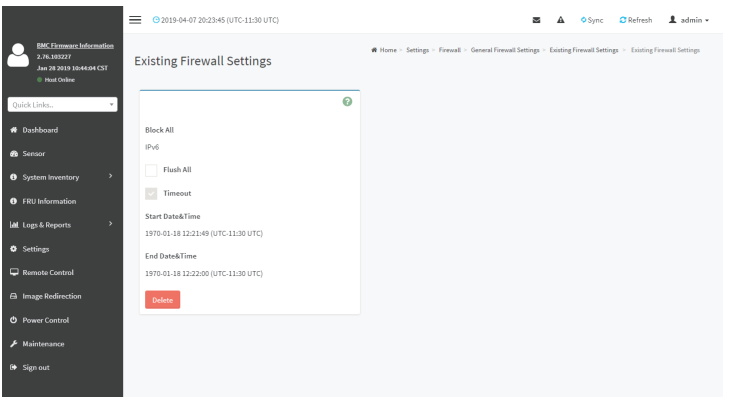
Click **General Firewall Settings > Existing Firewall Settings** icon. A blank page will be opened if you did not add anything in “Add Firewall Settings”. If any settings are added, then the added rule will be listed in “Existing Firewall Settings” page. A sample screenshot of Existing Firewall Settings page is shown below.



The Existing Firewall Settings page allows you to remove any particular Existing Firewall Settings.

Procedures

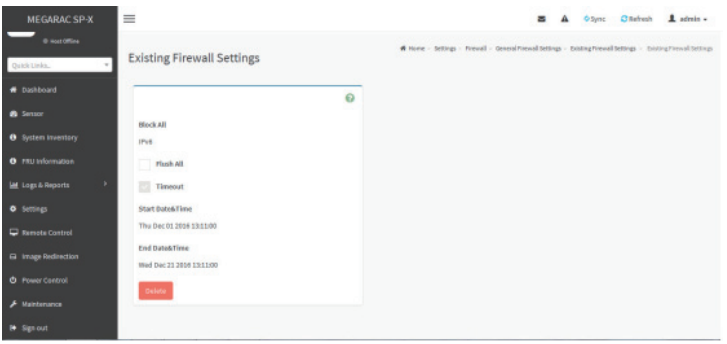
1. Click General Firewall Settings > Existing Firewall Settings icon. A sample screenshot of Existing Firewall Settings page is shown below.



- **Block All**: The blocked incoming IP's and Port's can be viewed.
- **Flush All**: To flush all the system firewall rules (Read-Only).
- Select Timeout to enable or disable firewall rules with timeout.
- **Time Out** :The respective firewall rule effect Start Time, End Date, Start Time, End Time will be displayed.
- **Delete**: To Delete the system firewall rules.

Add Firewall Settings

Click **General Firewall Settings > Add Firewall Settings**. This opens the Add Firewall Settings page as shown below.



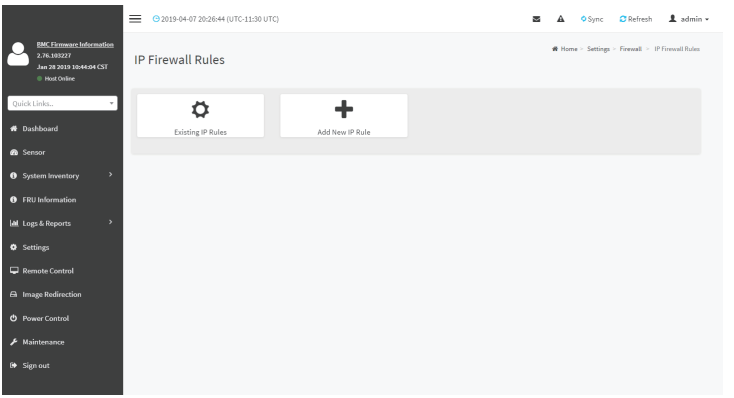
1. Select **Block All** to block all the incoming IP's and Port's.
2. Select **Flush All** to flush all the system firewall rules.
3. Select **Timeout** to enable or disable firewall rules with timeout.
4. Enter **Start Time** to start the respective firewall rule effect from this time.
5. Enter **End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

Note: The time should be in the dd-mm-yy:hh-mm format.

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

IP Address Firewall Rules

Click **IP Firewall Rules** page. A sample screenshot of IP Firewall Rules page is shown below.

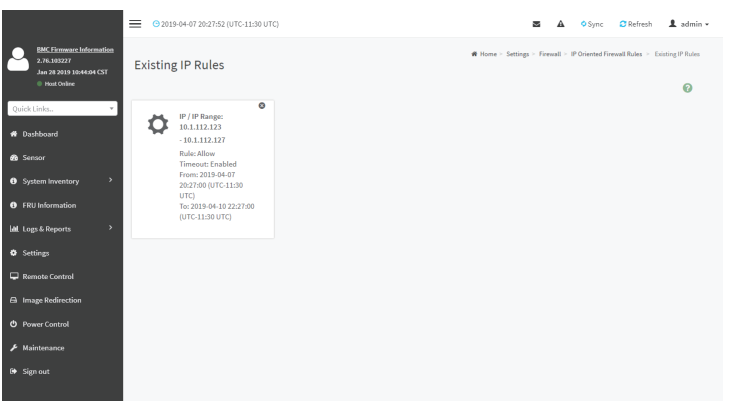


The fields of **IP Address Firewall** tab are explained below.

To View Existing IP Rules or a range of IP Addresses

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.

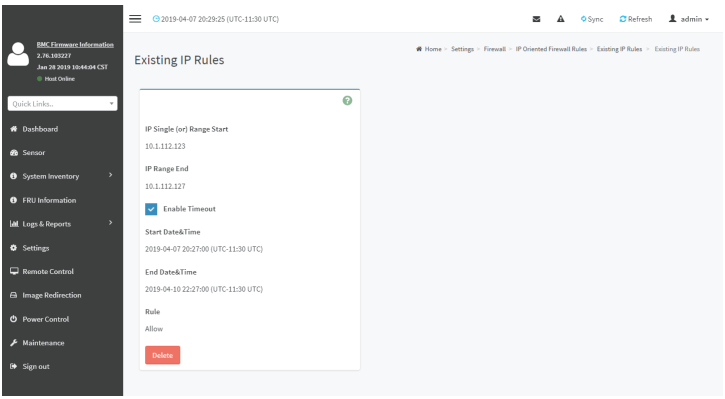
A sample screenshot of Existing IP Rules page is shown below.



The Existing IP Rules page allows you to remove any particular Existing IP Rules.

Procedures

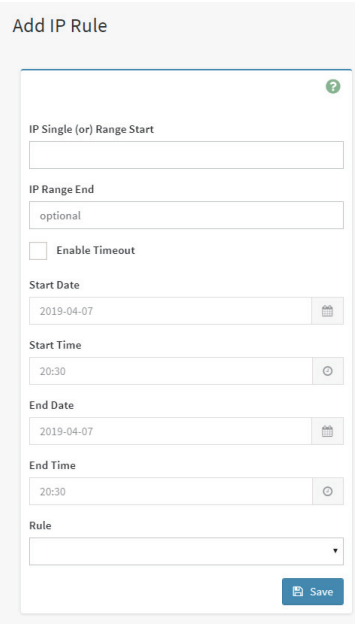
1. Select the Existing IP Rules you want to remove.
2. Click on Delete to remove the selected Existing IP Rules.



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

Procedures

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 xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx.

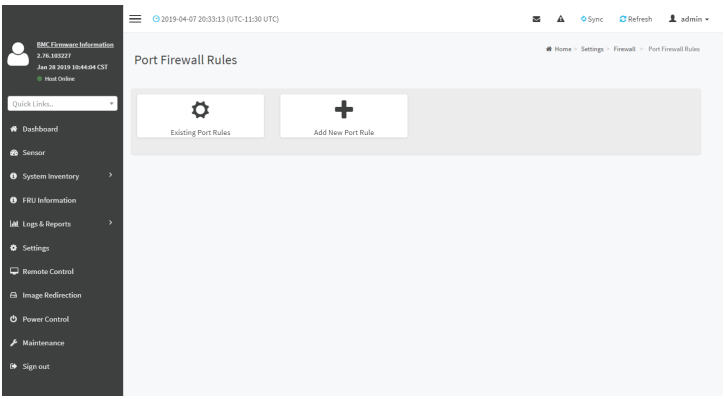
3. Enter IP range end value in the **IP Range End** field.
4. Enable **Timeout** to enable firewall rules with timeout.
5. Enter **Start Date** to start the respective firewall rule effect from this date.
6. Enter **End Date** to end the respective firewall rule effect from this date.
7. Enter **Start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

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

Port Firewall Rules

Click **Port Firewall Rules** page. A sample screenshot of Port Firewall Rules page is shown below.

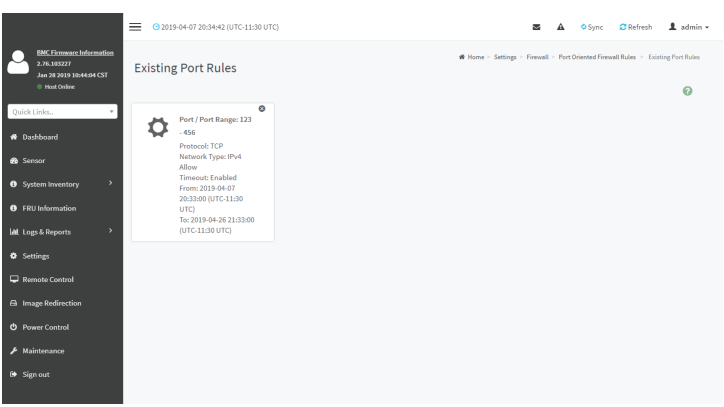


The fields of Port Firewall Rules tab are explained below.

To view Existing Port Rules

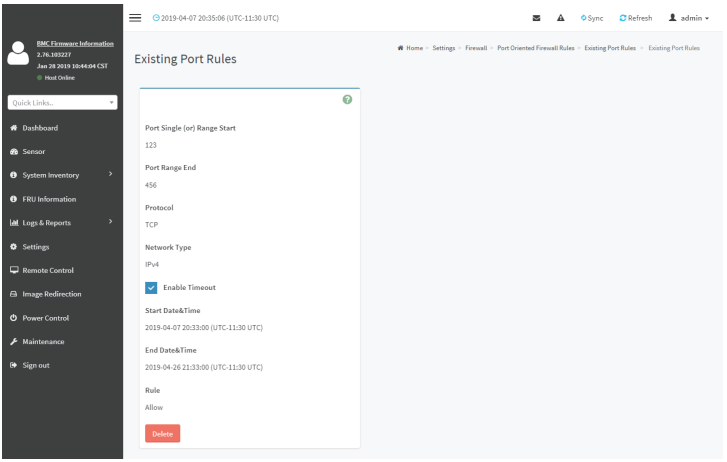
Click **Settings > System Firewall > Port Firewall Rules > Existing Port Rules**. A blank page will be opened if you did not add anything in “Add New port Rule”. If any rule is added, then the added rule will be listed in “Existing Port Rules” page.
A sample screenshot of Existing Port Rules is shown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

The Existing Port Rules page allows you to remove any particular Existing Port Rules.



Procedures

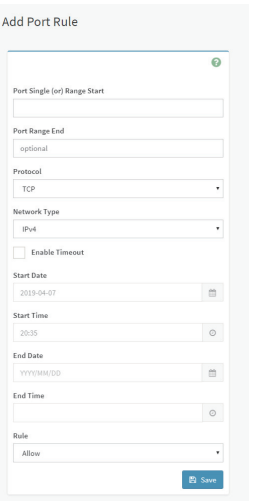
1. Select the Existing Port Rules you want to remove.
2. Click on Delete to remove the selected Existing Port Rules.



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 range 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.
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.

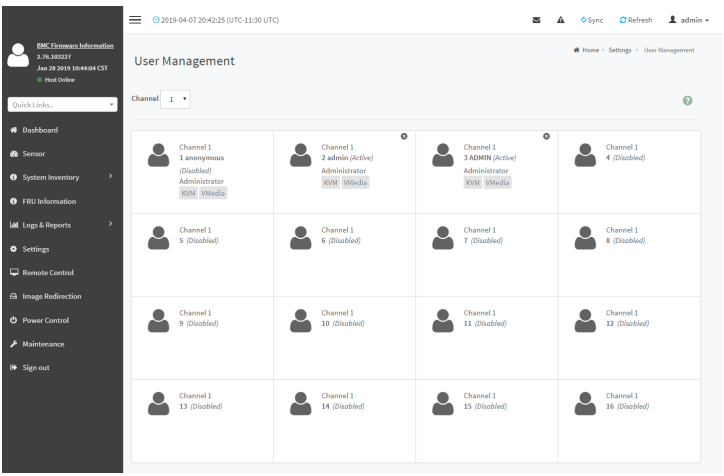
Note: The time should be in the YYYY/MM/DD:hh-mm format.

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

2-6-15 User Management

In BMC Web GUI, 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.

Note: The Free slots are shown as “Disabled” in all columns for the slot.
The fields of User Management page are explained below.

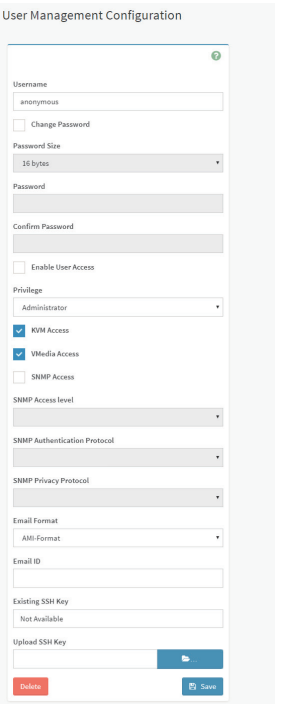
User ID: Displays the ID number of the user.

Note: The list contains a maximum often 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 l 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.
Blank 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 lab)
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	IDC2 (device control 2)
13	DG3 (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)
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. Enable or Disable the **Enable User Access** Privilege.

Note: Enabling User Access will intern assign the IPMI messaging privilege to user. It is recommended that the IPMI messaging option should be enabled for the user to enable the User Access option, while creating User through IPMI.

6. In the Network Privilege and Serial Previlege fields, select the privileges assigned to the user which could be Administrator, Operator, User, OEM or None.
7. Check **KVM Access** to assign the KVM privilege for the user.
8. Check **VMedia Access** assign the VMedia privilege for the user.

Note: 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.

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

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

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

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

12. Choose the Encryption algorithm to use for SNMP settings from the SNMP Privacy protocol (AES or DES) drop-down list.
13. 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.

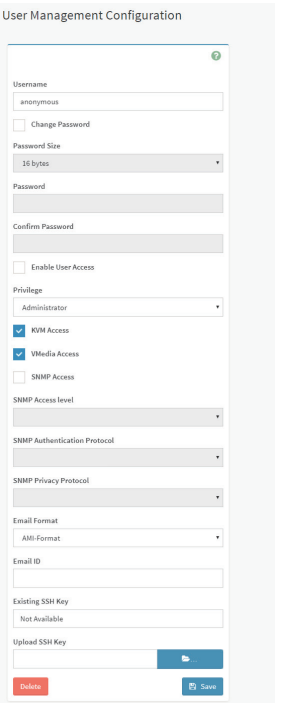
14. In the **Upload SSH Key** field, click Browse and select the SSH key file.

Note: SSH key file should be of pub type.

15. 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.



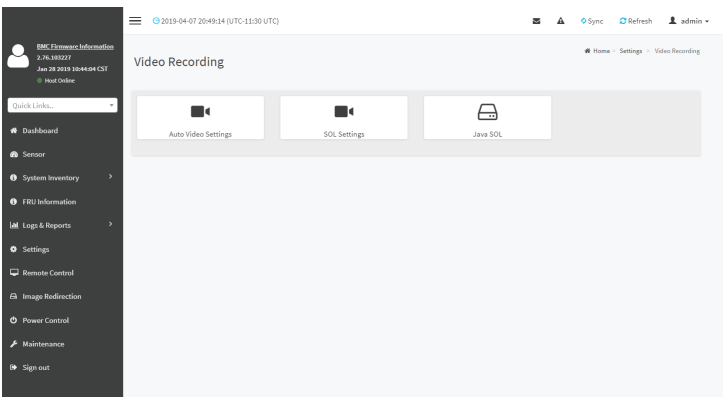
2. Check **Change Password**, if you wish to change the existing Password.
3. Follow the steps (3 to 15) of Procedure to add a new User.
4. Click **Save** to save the changes and return to the users list.
5. Click **Delete** to delete the user.

2-6-16 Video Recording

The Video Recording consists of the following:

1. Auto Video Settings
   - Video Trigger Settings
   - Video Remote Storage
   - Pre-Event Video Recordings
2. SOL Settings
   - SOL Trigger Settings
   - SOL Video Remote Storage
   - SOL Recorded Video
3. JAVA SOL

A sample screenshot of the Video Recording is given below.

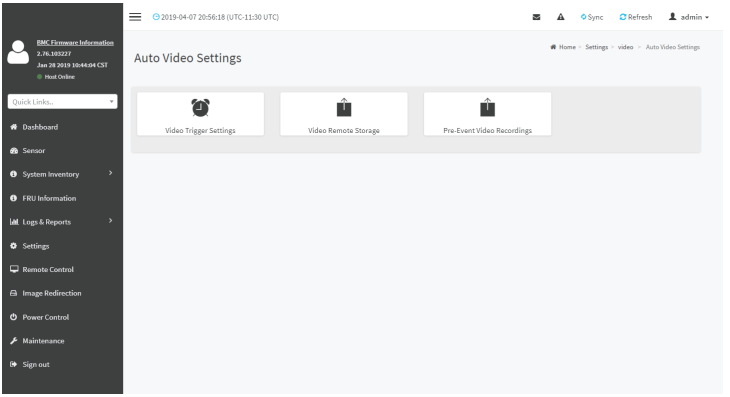


A detailed description of the menu items are given below.

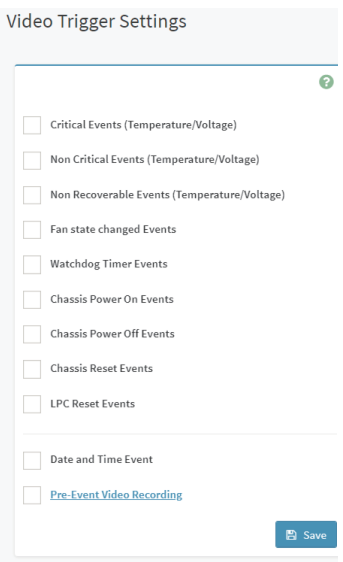
Auto Video Settings

The Auto Video Settings page allows you to configure the events that will trigger auto video recording function of the KVM server and view the current list of user slots for the server. You can add a new user and modify or delete the existing users.

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



To triggers for Auto Video Recording, click **Video Recording > Auto Video Settings > Video Trigger Settings** from the menu bar. A sample screenshot of Video Trigger Settings page is shown below.



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

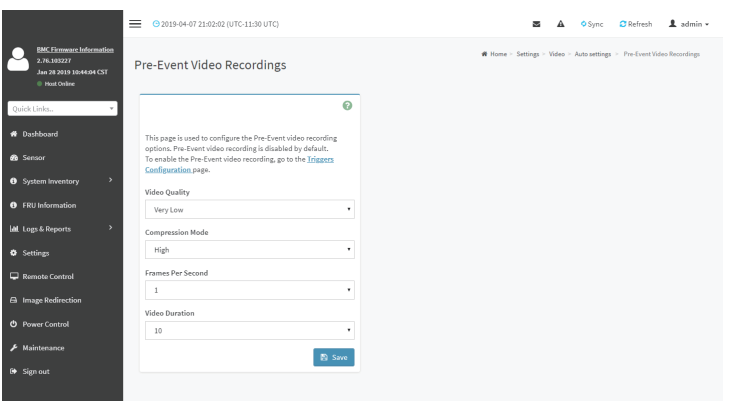
Save: To save the current changes.

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, normal, 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.

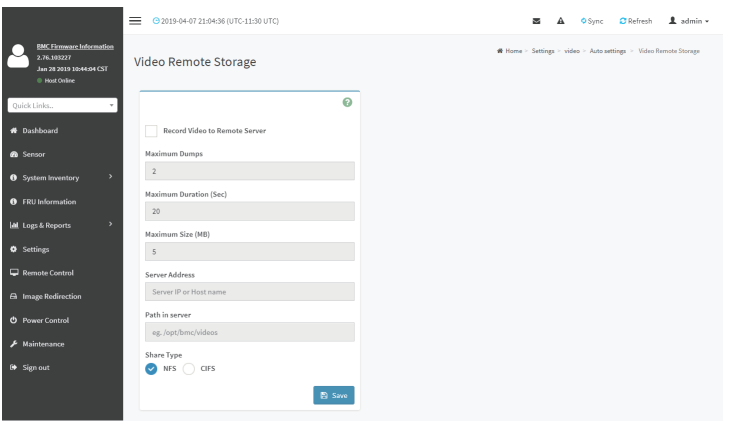
e) Click **Save** to save the changes made on the Pre-Event Video Recording.

4. Select Crash Reset either Pre-crash or Pre-reset.
5. 5. Click **Save** to save the changes.

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 constraint 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 recorded file will be named as **pre_crash_video_x.dat**, where x is file count, similarly if it is recorded for reset event it will be named as pre_reset_video_x.dat.

Post-Event

Post-Event video recording files will be named as shown below.

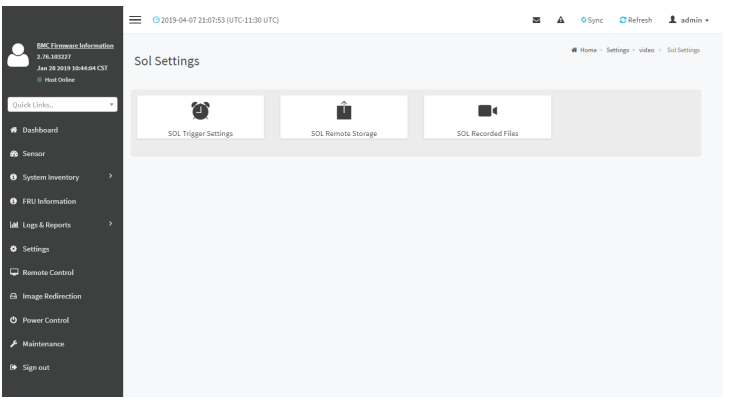
video_dump_<Hostname>_%Y%m%dT%H%M%S.dat.

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.	

SOL Settings

To open SOL Set page, click **Settings > Video Recording > SOL Settings** from the menu bar. A sample screenshot of SOL Settings page is shown below.



The SOL Settings consists of three fields:

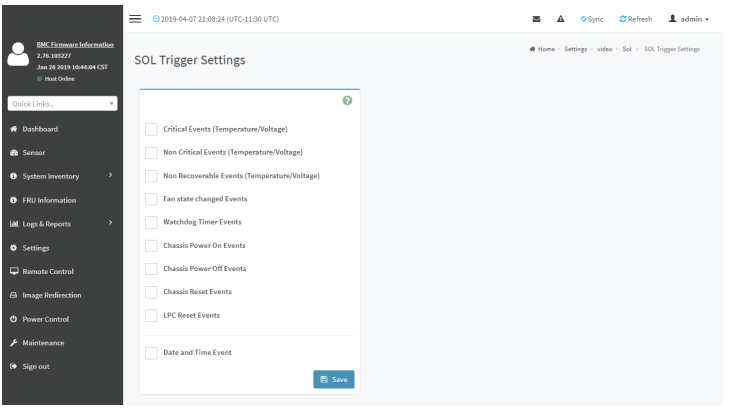
- SOL Trigger Settings
- SOL Video Remote Storage
- SOL Recorded Video

SOL Trigger Settings

Event List: It shows the list of available events to be configured. The events are shown 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 Event
- Chassis Power off Event
- Chassis Reset Events
- LPC Reset Events
- Date and Time Events
- **Save**: To save the current changes.

A sample screenshot of SOL Trigger Settings page is shown as below.



Procedure

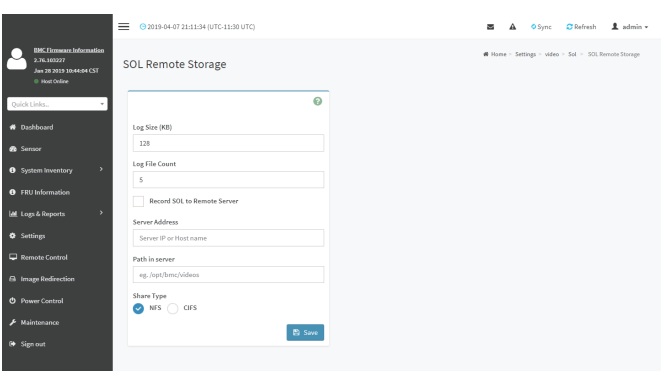
1. Check the events to be enabled to configure which event on the page will trigger the SOL video recording option to start.
2. To set particular Date and Time Event, check the option **Date and Time Event**.
   a) Choose the month, day and year from the **Date** field
   b) Enter the **Time** in hh:mm:ss format in the respective fields.

Note: The date and time should be in advance to the system date and time.

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

SOL Video Remote Storage

This page allows you to configure recorded video files. The sample screenshot and various fields of **SOL Video Remote Storage** are given below.

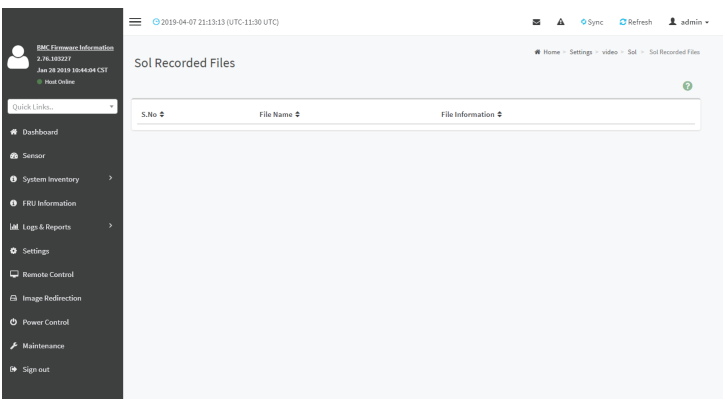


Procedure for SOL Video Remote Storage:

1. Click SOL Video Remote Storage.
2. Enter Log Size (KB). The value will support maximum length of 10 digits.
3. Enter Log File Count. The default number of Log files count ranges from 1 to 10.

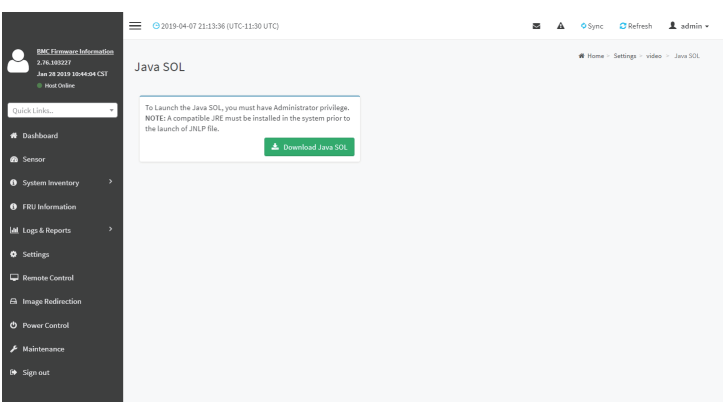
SOL Recorded Video

This page displays the list of available recorded video files on the system. Click on **Download** icon to download and save the video. Click on **Delete** icon to delete the selected video.
A sample screenshot of **SOL Recorded Video** is given below.



JAVA SOL

This page allows you to download JAVA SOL. A sample screenshot of JAVA SOL is given below.



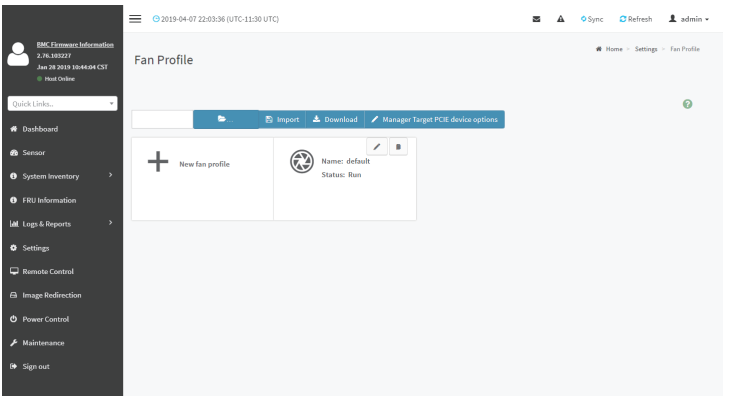
Note: A compatible JRE must be installed in the system prior to the launch of JNLP file.

2-6-17 Fan Policy

The Fan Policy consists of the following:

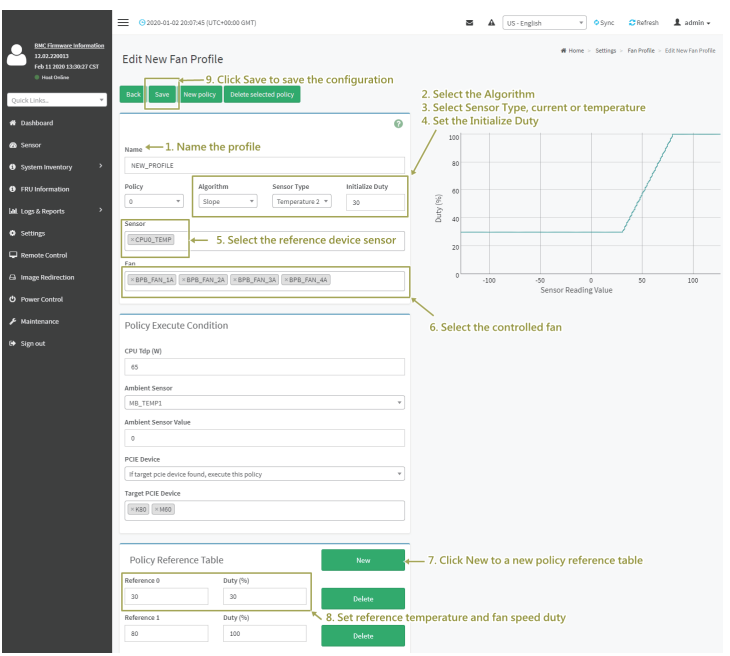
1. Add New Fan Profile

A sample screenshot of the Fan Profile is given below.

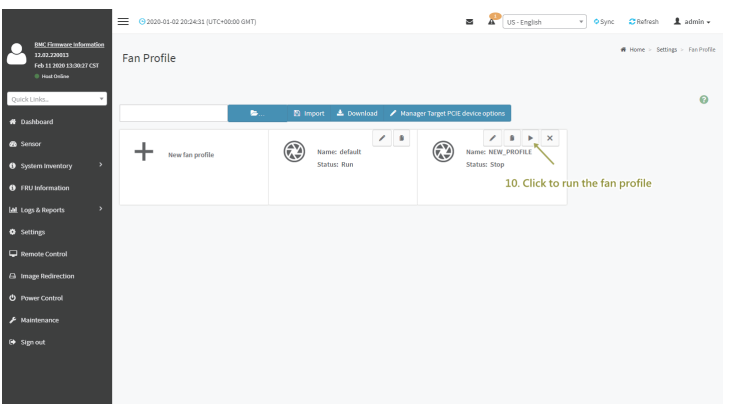


Procedure to add Fan Profile

To add fan profile:

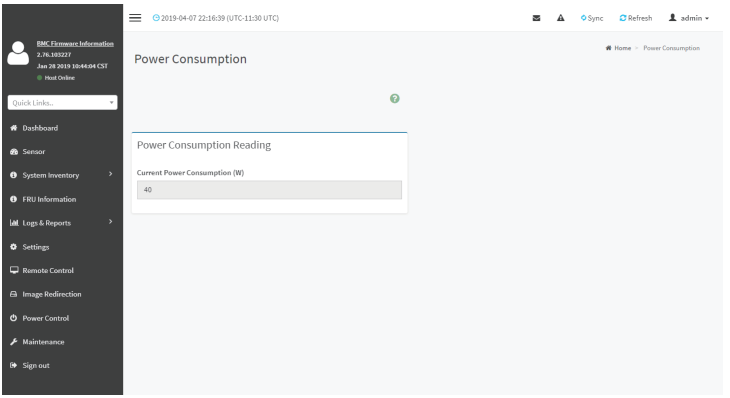


1. Name the the profile
2. Select the **Algorithm**. Choose the mapping function of temperature and fan speed at this policy.
3. Select **Sensor Type**, current or temperature.
4. Set the **Initialize Type**.
5. Select the reference device sensor.
6. Select the controlled fan.
7. Click **New** to a new policy reference table
8. Set reference temperature and fan speed duty
9. Click **Save** to save the configuration.
10. Click arrow icon to run the fan profile.



2-6-18 Power Consumption

The Power Consumption is a simple display page for basic power consumption reading information. Item on this page are non-configurable.



This page intentionally left blank

2-7 Remote Control

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

System Requirements

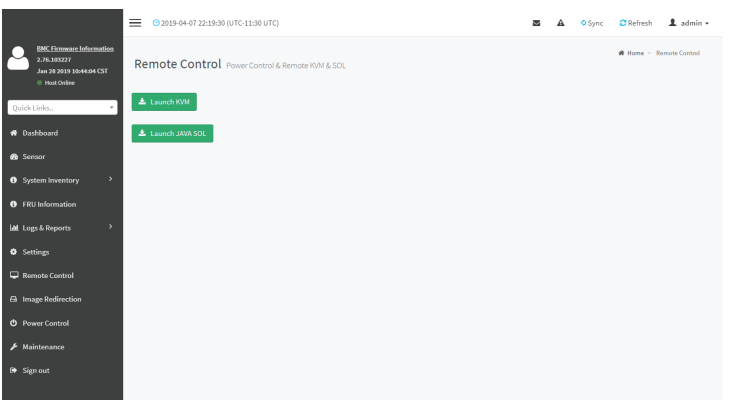
- Client machine with 8GB RAM.
- If the client machine has 4GB RAM, there will be lag in Video/keyboard/mouse functionality.

Supported Browsers

- Chrome latest version.
- IE 11 and above.
- Firefox (with limited support).

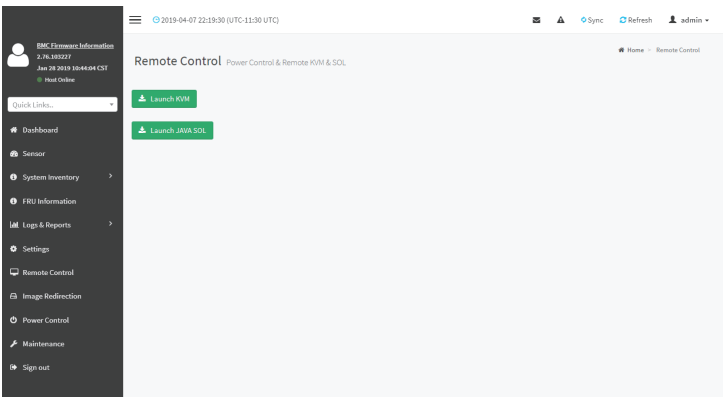
Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations.

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



A detailed description of the menu items are given on the next page.

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



Click **Launch KVM** to open the Remote Control KVM page.

Stop KVM: Stops the H5Viewer video redirection.

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 Recording Duration.

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.
Users have to take care of saving the video files in different browsers.
When H5viewer focus is lost and if video recording is in progress, the recording will be stopped with a notification message and the recorded video file will be discarded. Due to browser limitation, Set timeout/set interval will be delayed from specified time of interval when browser window loses focus, Hence, video server will not send the video packets to H5viewer and so the video recording will be stopped.

Note: Windows 2016 installation takes 1 hour and 52 minutes to install on Ironman through the BMC ISO redirection.

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

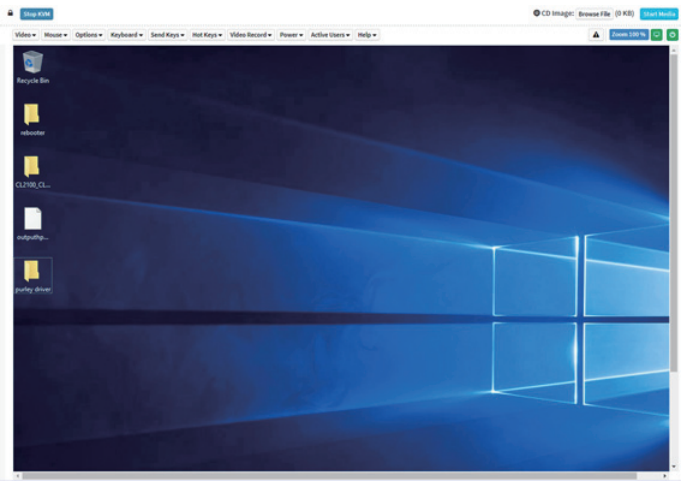
Ctrl+Alt+Del: This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.
Left Windows Key: This menu item can be used to act as the left-side <WIN> key when in Console Redirection. You can also decide how the key 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.

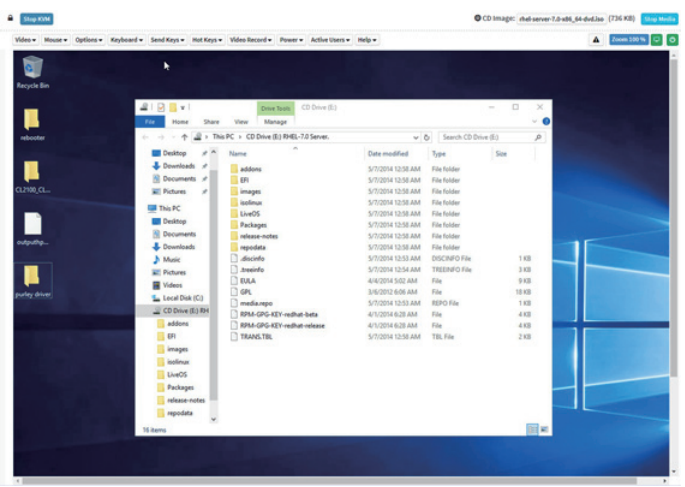
Browse File: Used to select the CD image file to be redirected to the host.
Start Media: Redirects the selected CD image file to the host.
Stop Media: Stops the CD media redirected to the host.

Procedure To Start KVM

1. Click Start KVM to start the H5Viewer video redirection. A sample screenshot is as shown below.



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



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

Settings

Keyboard Layout

List of Host Physical Keyboard languages supported in SPX H5Viewer.

- English U.S
- German
- Japanese

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

Options

The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following options:

Block Privilege Request: To enable or disable the access privilege of the user.
Keyboard/Mouse Encryption: This option allows you to encrypt keyboard inputs and mouse movements sent between the connections.
0 Best Quality - 7: This option allows you to adjust the screen resolution.

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 server in proper order.
Power ON Server: To Power ON the server.

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.

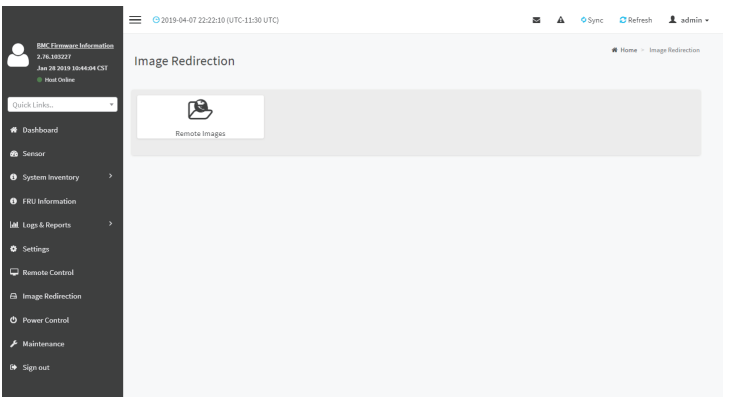
Zoom 100%
Displays the zoom percentage. Users can click Options from the menu bar and then select Zoom In or Zoom Out to adjust the zoom percentage.

Power ON/OFF
Click this option to Power ON/OFF the server.

2-8 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 I**mages Redirection** from the menu bar. A sample screenshot of Images Redirection page is shown below.



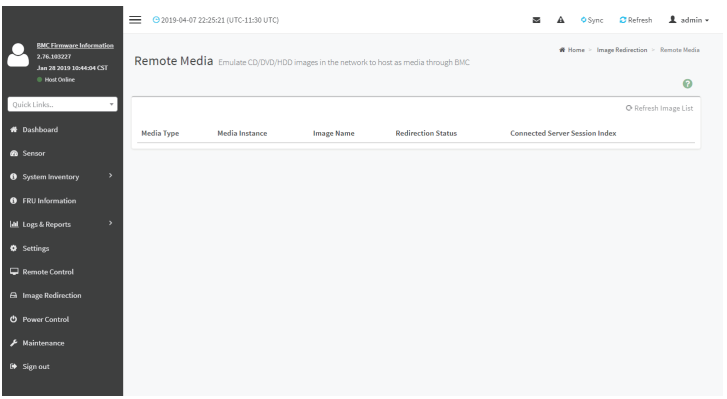
The fields of Images Redirection page are explained below.

- Local Images
- Remote Images

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.

2-8-1 Remote Media

The displayed table shows configured images on BMC. You can configure images of 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 "~"

The fields of Remote Media tab are as follows:
Media Type: Displays type of Media such as CD/DVD, Floppy 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.

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

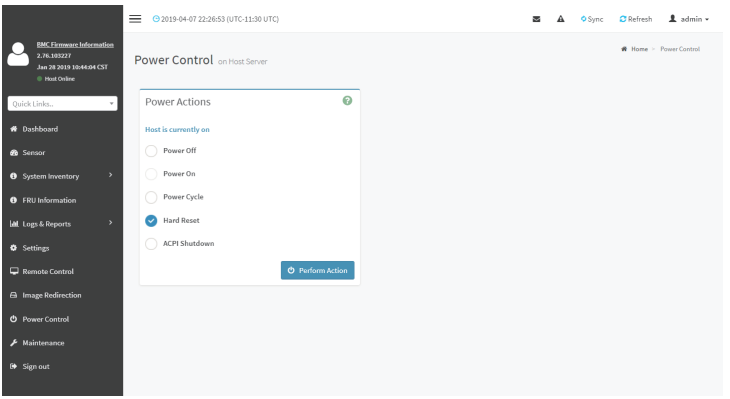
2. Select a configured slot and click (Start/Stop icon) to start the remote media redirection. It is a toggle button, if the image is successfully redirected, then click (Start/Stop icon) to stop the remote media redirection.

Note: Redirection needs to be stopped to clear the image.

2-9 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.

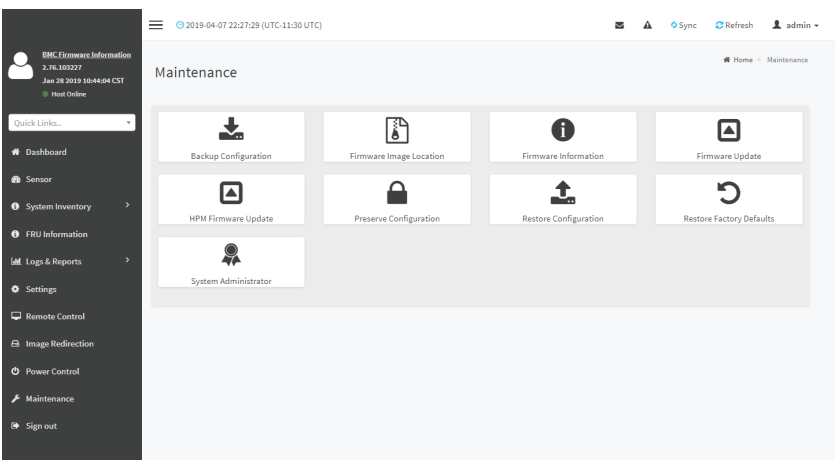
Note: It is advisable to use Chrome or IE for H5Viewer, since Firefox has its own memory limitations.

2-10 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
- HPM Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- System Administrator

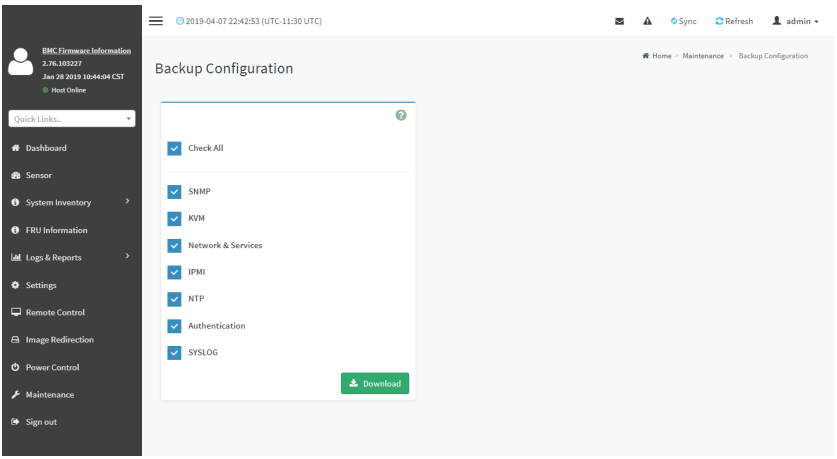
A sample screenshot of Maintenance is shown below.
A detailed description is given below.



2-10-1 Backup Configuration

This page allows you to select the specific configuration items to be backed up 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 download and save the configuration files backup from BMC to client system.

Procedure

1. Click **Check All** to backup the selected configuration items. The Backup Configuration page will appear as shown above screenshot.
2. Click **Download Config** to save the backup file to the client system.
3. Cick **OK** to perform the backup action. The Backup file will be saved in the client system.
4. Click **Cancel** to cancel the backup process.

TFTP server configuration

The TFTP server configuration is used for exporting the backup file.

Note: Ensure that no other TFTP servers are enabled, if so remove all other servers with all configuration files. Login as “super” user means “root” user.

Procedure to make the default tftp server

1. Install the application which is 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
>vi /etc/inetd.conf

ftp stream tcp nowait root /usr/sbin/tcpd /usr/sbin/ in.ftpd
tftp dgram udp wait nobody /usr/sbin/tcpd /usr/sbin/ in.tftpd <DIR>

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

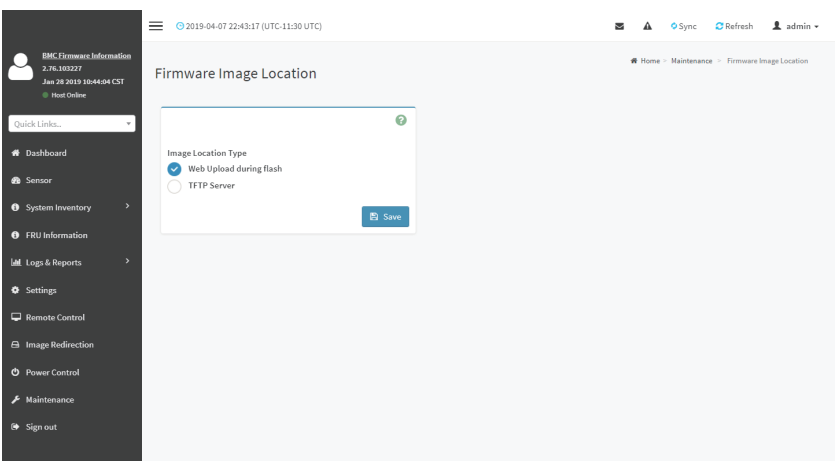
6. Even after all this step has been done and still facing error of timeout:
   a) Check with /etc/xinetd.d/tftp file and uncomment the EOF (Remove the '#' before the EOF alone).
   b) Restart the server.

2-10-2 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 filename 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 Image Name** in the given field
4. Enter the **TFTP Retry Count** value.
5. Click **Save** to save the changes.

2-10-3 Firmware Update

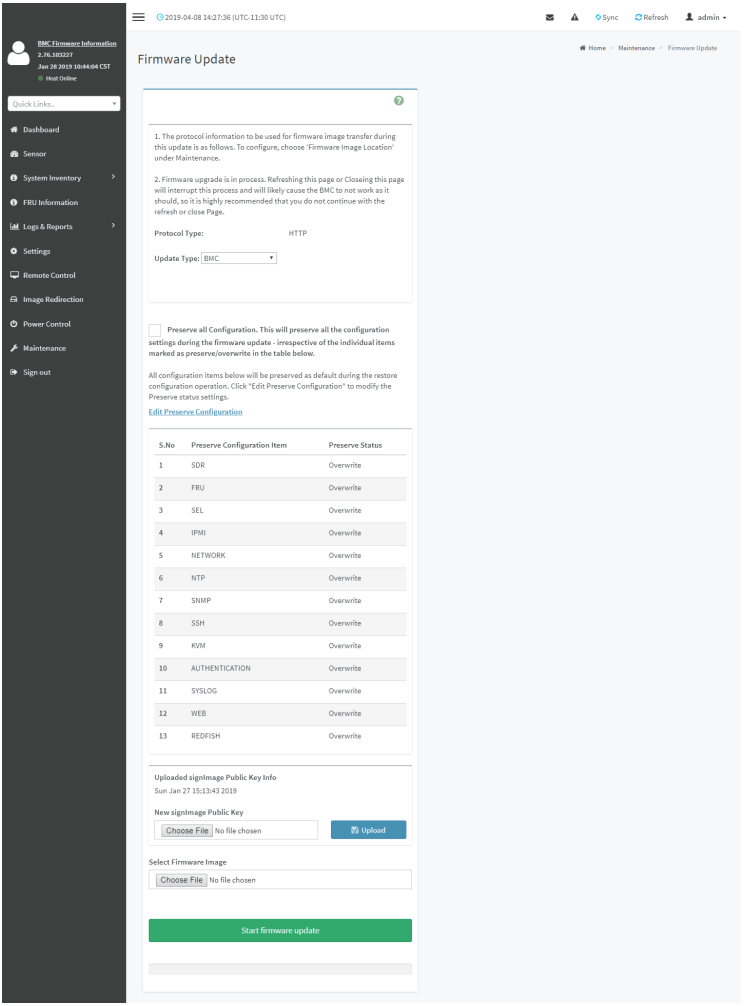
This wizard takes you through the process of firmware upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade.

Warning: 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 BMC must be reset. This means that you must close the Internet browser and log back onto the BMC 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.

A sample screenshot of Firmware Update page is shown below.



The various fields of Firmware Update are as follows:

- **Preserve all Configuration**: To preserve all configuration.
- **New signimage Public Key**: To select the signimage Public Key to be uploaded.

- **Edit Preserve Configuration**: To modify the Preserve status settings.
- **Select Firmware Image**: To select the Firmware image to be uploaded.
- **Start Firmware Update**: To start the Firmware Update.

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:

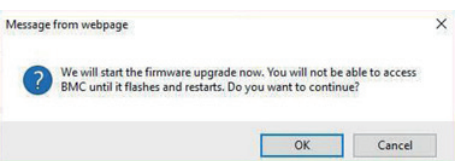
Note: All configuration items will be preserved/overwrite as default during the restore configuration operation.

Procedure

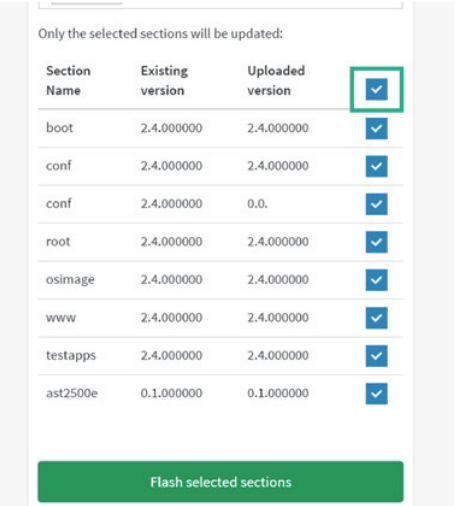
1. Click **Preserve all Configuration** to preserve all configuration.
2. Click Browse to select firmware image. The Firmware update undergoes the following steps:
   a) Closing all active client requests
   b) Preparing Device for Firmware Upgrade
   c) Uploading Firmware Image

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

   d) Browse and select the Firmware image to flash and click **Upload**.
   e) Click **Start firmware update** start the Firmware Update. A warning message will be prompted you to proceed further.
   f) Click **OK** to start the Firmware Update. The sample screenshot is shown below
   g) Verifying Firmware Image

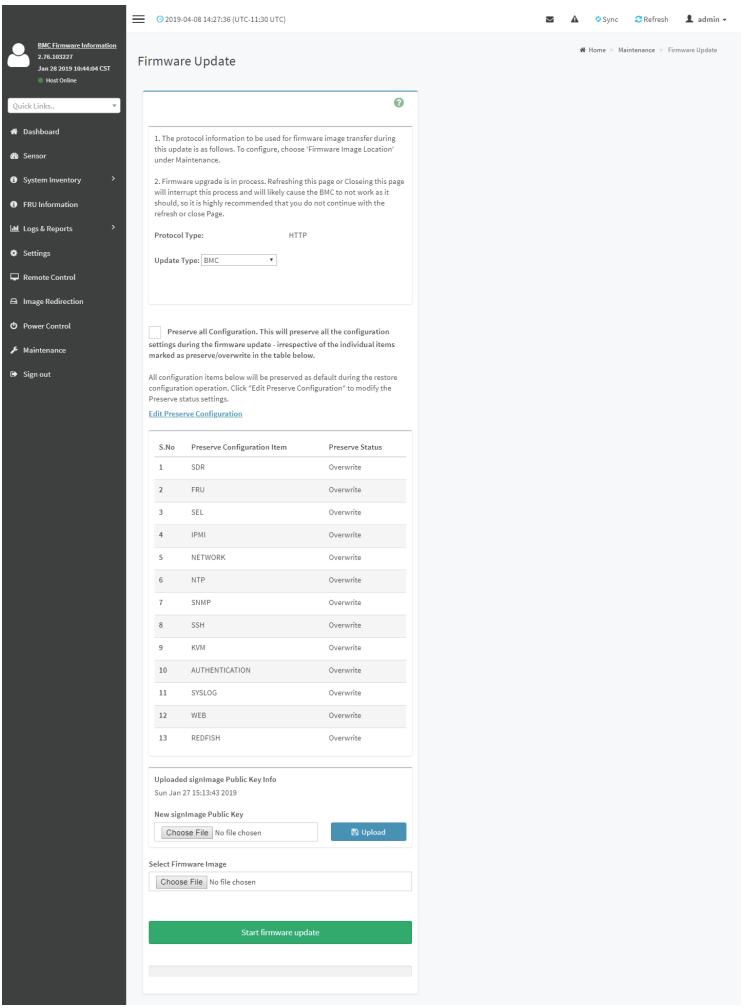


If flashing is required for all images, please select the following checkbox:



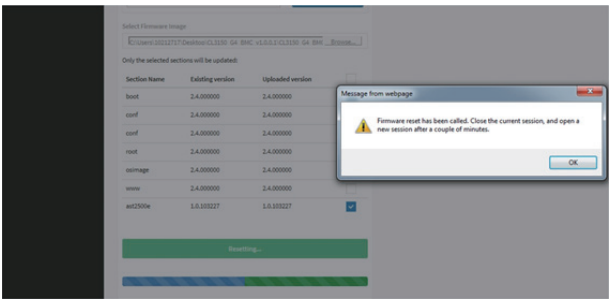
If only few module versions are different, those modules will be flashed.

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



h) Flashing Firmware Image.

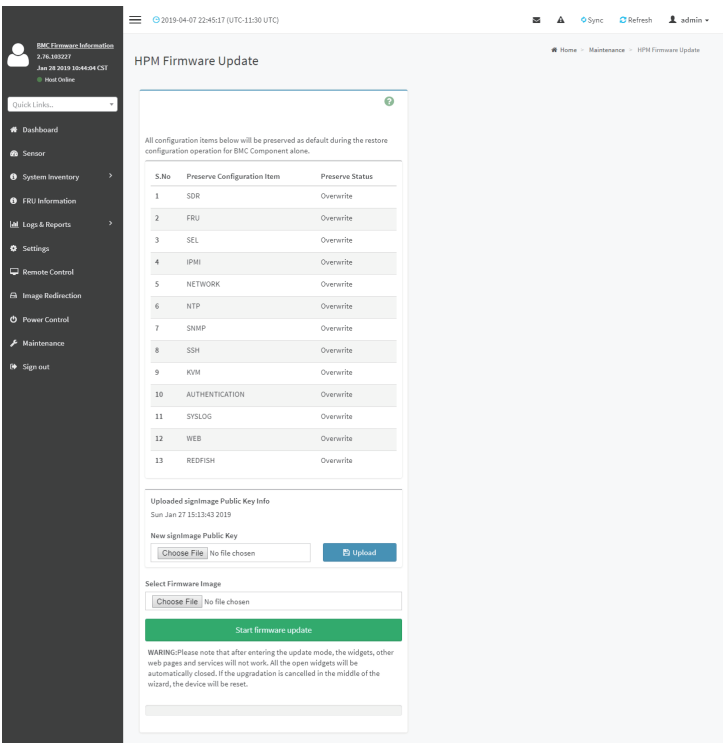
i) Resetting the image. The sample screenshot of Firmware update is as shown below.



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 instructions 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.

2-10-4 HPM Firmware Update

This page allows you to update the HPM (Hardware Platform Management) firmware.
To configure, choose '**HPM Firmware Image Location**' under **Maintenance**. To open HPM Firmware Update page, click **Maintenance > HPM Firmware Update** from the menu bar.
A sample screenshot of HPM Firmware Update page is shown below.



The various fields of HPM Firmware Update are as follows:

- **New signimage Public** Key: To select the signimage Public Key to be uploaded.
- **Select Firmware Image**: To select the Firmware image to be uploaded.
- **Start Firmware Update**: To start the Firmware Update.

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.

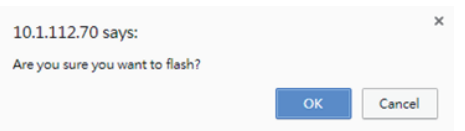
Procedure

1. Click **Preserve all Configuration** to preserve all configuration.
2. Click **Browse** to select firmware image. The Firmware update undergoes the following steps:

a) Closing all active client requests
b) Preparing Device for Firmware Upgrade
c) Uploading Firmware Image

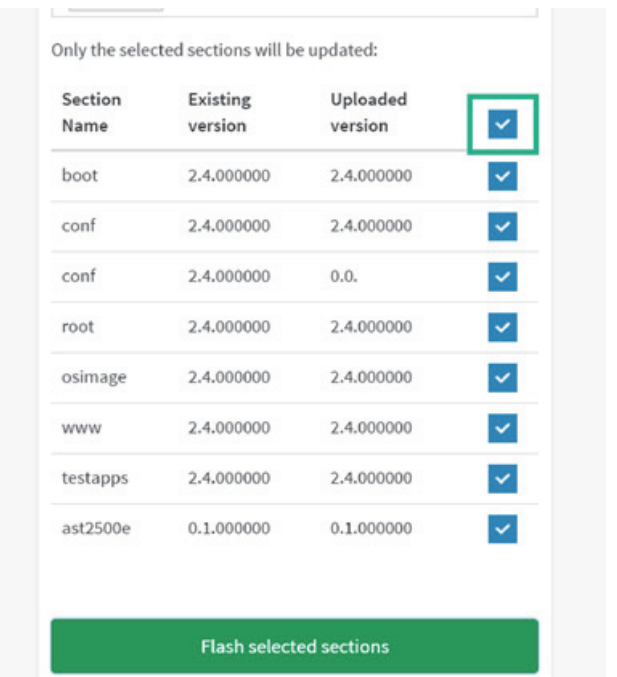
Note: A file upload pop-up will be displayed for http/https but in the case of tftp files, the file is automatically uploaded displaying the status of upload.

d) Browse and select the Firmware image to flash and click **Upload**.
e) Click **Start firmware update** start the Firmware Update. A warning message will be prompted you to proceed further.
f) Click **OK t**o start the Firmware Update. The sample screenshot is shown below.



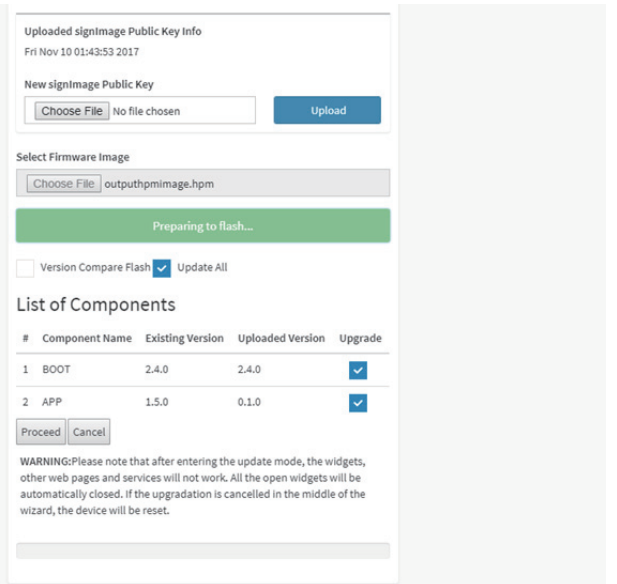
g) Verifying Firmware Image.

If flashing is required for all images, please select the following checkbox:



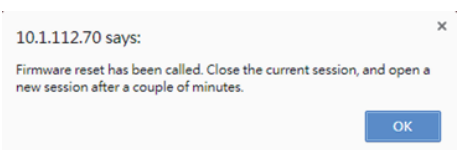
If only few module versions are different, those modules will be flashed.

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



h) Flashing Firmware Image.

i) Resetting the image. The sample screenshot of Firmware update is as shown below.

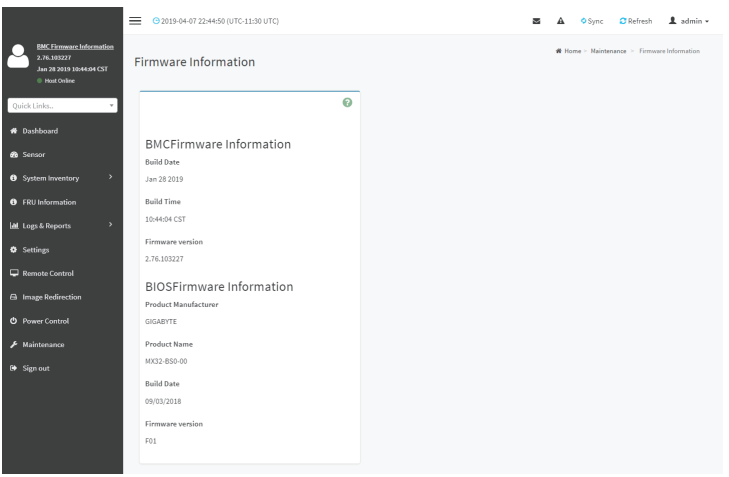


Note: The HPM Firmware Update page will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset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

2-10-5 Firmware Information

This wizard takes you through the process of firmware upgradation. A reset of the box will 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.

BMC Firmware Information:

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.

BIOS Firmware Information:

Product Manufacturer: Describes the hardware manufacturer.

Product Name: Describes the model name of the device.

Build Date: Describes the Build Date of the device.

Firmware version: Describes the BIOS version of the device.

CPLD Firmware Information:

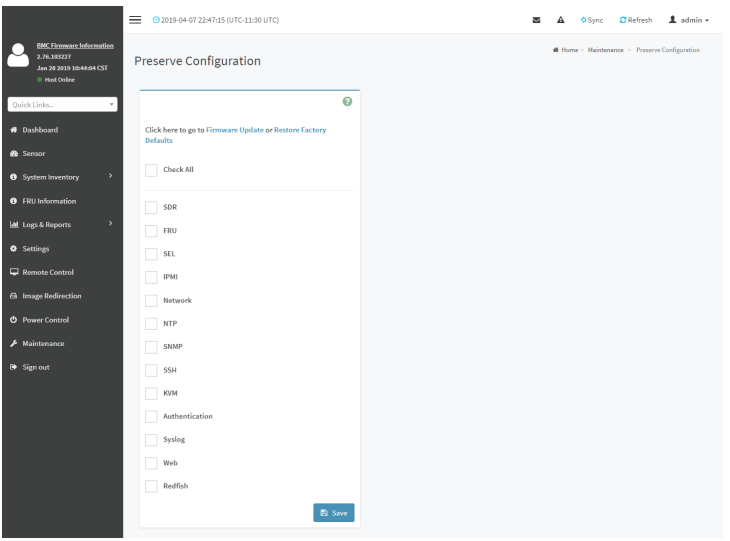
Firmware version: Describes the CPLD Firmware version.

2-10-6 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.



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 the current changes.

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

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.
Dependency Configurations - NIL

Network

To save network settings related with IPMI (LAN IP or DHCP configuration), select “IPMI” and “Network” options simultaneously. 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: This file is to configure the link speed, duplex and MTU value for the specified interface.
dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.
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: This file is to configure the link speed, duplex and MTU value for the specified interface.
dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.

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:

sshd_config: 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

Following files will be preserved:

vmedia.conf: This file contains the modes of media such as cd,fd,hd and enable and disable flags for lmedia, rmedia and sd servers.

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.

rmedia.conf: This file contains the image name and the remote machine information like IP address, user name, password, domain name and share type.

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 contains 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
System Event Log

Web
Web Settings

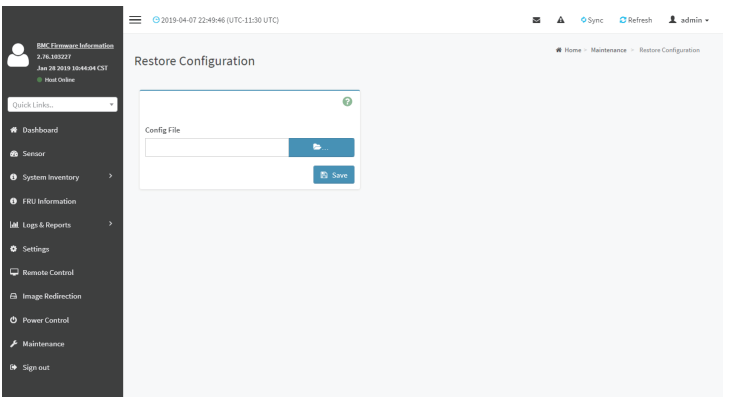
Extlog
Audit Log & System Log

Redish
Redfish Audit Log

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.

2-10-7 Restore Configuration

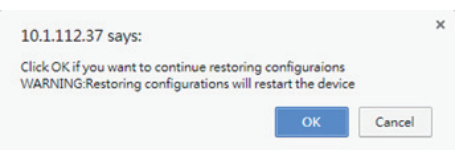
This page allows you to restore the configuration files from the client system to the BMC.
To open Restore Configuration page, click **Maintenance > Restore Configuration** from the menu bar. A sample screenshot of Restore Configuration page is shown below.



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.



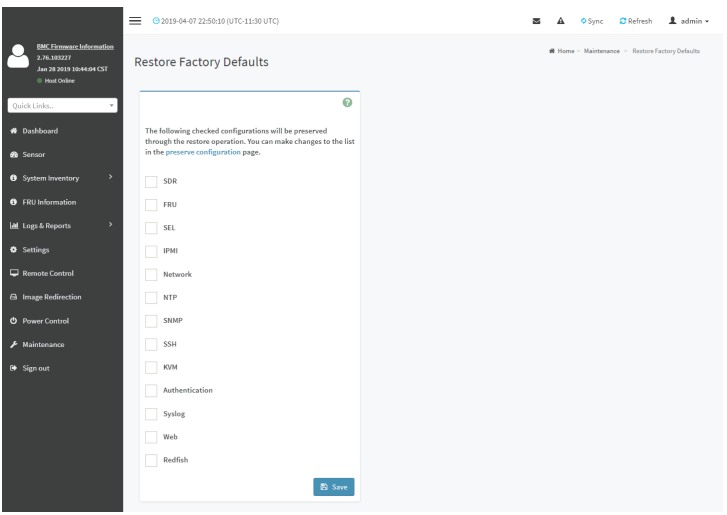
3. Click OK to upload the new configuration file and restore.

2-10-8 Restore Factory Defaults

In BMC Web GUI, 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.

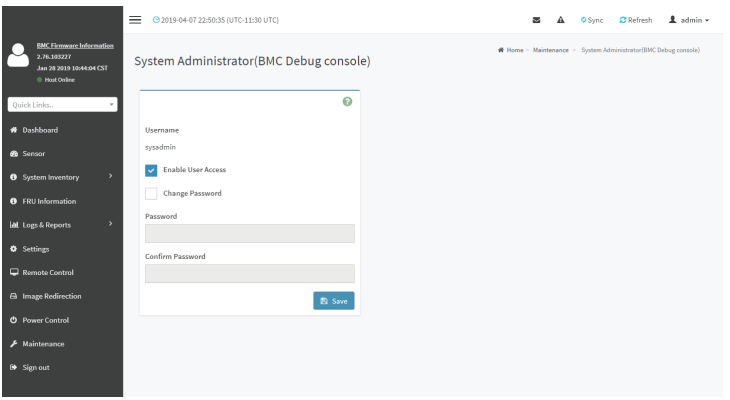


Procedure

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

2-10-9 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 blank space is not allowed.

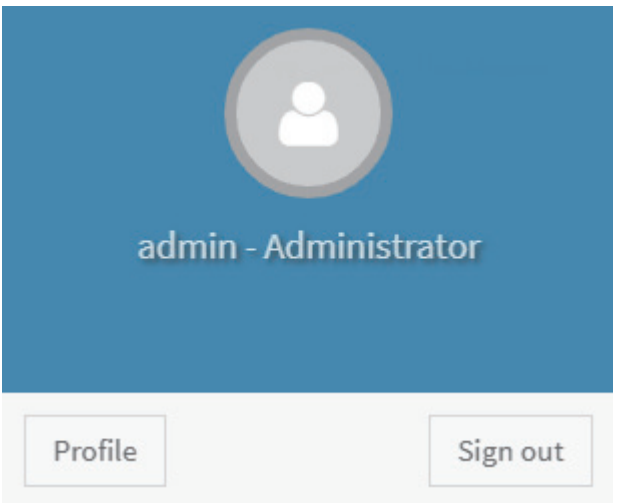
Save: To save the new configuration for system administrator.

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.

2-10-10 Sign Out

To log out from the Web GUI, 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 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.