

# **GIGABYTE™**

## **Gigabyte Server 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](mailto:server.grp@gigabyte.com)

**Facebook:** <https://www.facebook.com/gigabyteserver>

**Twitter:** <https://twitter.com/GIGABYTEServer>

# Table of Contents

Chapter 1 Getting Started .....	5
1-1 Software Requirement .....	5
1-2 Gigabyte Management Console Network Configuration .....	6
1-3 Log In Gigabyte Management Console.....	7
1-3-1 Required Browser Settings:.....	8
1-4 Quick Button and Logged-in User .....	9
1-5 Help.....	10
1-6 Menu Bar.....	10
Chapter 2 Enter Gigabyte Management Console .....	11
2-1 Dashboard.....	11
2-2 Sensor.....	12
2-2-1 Sensor Detail.....	13
2-2-2 Sensor Events .....	14
2-3 System Inventory .....	15
2-3-1 CPU Inventory .....	15
2-3-2 DIMM Inventory .....	17
2-3-3 PCI Inventory.....	18
2-3-4 HDD Inventory.....	19
2-3-5 NIC Inventory.....	20
2-4 FRU Information.....	21
2-5 Logs & Reports .....	23
2-5-1 IPMI Event Log.....	23
2-5-2 System Log.....	24
2-5-3 Audit Log .....	25
2-5-4 Video Log .....	26
2-6 Settings .....	27
2-6-1 Captured BSOD.....	27
2-6-2 Date & Time.....	28
2-6-3 External User Services .....	29
2-6-4 KVM Mouse Settings .....	39
2-6-5 Log Settings.....	40
2-6-6 Manage Licenses .....	43
2-6-7 Media Redirection Settings.....	43
2-6-8 Network Settings .....	48
2-6-9 PAM Order Settings.....	56
2-6-10 Platform Event Filter .....	57
2-6-11 Services.....	65

2-6-12	SMTP Settings.....	69
2-6-13	SSL Settings.....	72
2-6-14	System Firewall.....	77
2-6-15	User Management.....	85
2-6-16	Video Recording.....	89
2-6-17	Fan Profile.....	97
2-6-18	Power Consumption.....	99
2-6-19	IMPI Interfaces.....	100
2-7	Remote Control.....	101
2-8	Images Redirection.....	107
2-8-1	Remote Media.....	108
2-9	Power Control.....	109
2-10	Maintenance Group.....	110
2-10-1	Backup Configuration.....	111
2-10-2	Firmware Image Location.....	112
2-10-3	Firmware Information.....	113
2-10-4	Firmware Update.....	114
2-10-5	Preserve Configuration.....	118
2-10-6	Restore Configuration.....	122
2-10-7	Restore Factory Defaults.....	123
2-10-8	System Administrator.....	124
2-10-9	Sign Out.....	125

# 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.

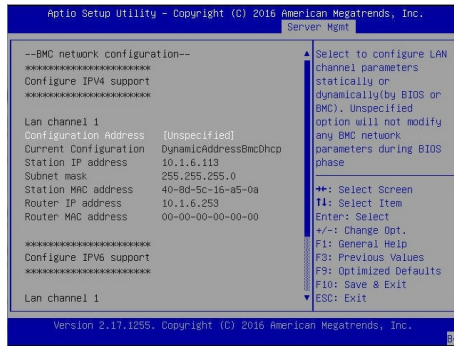
## 1-2 Gigabyte Management Console Network Configuration

Follow the instruction to enable the console redirection function.

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



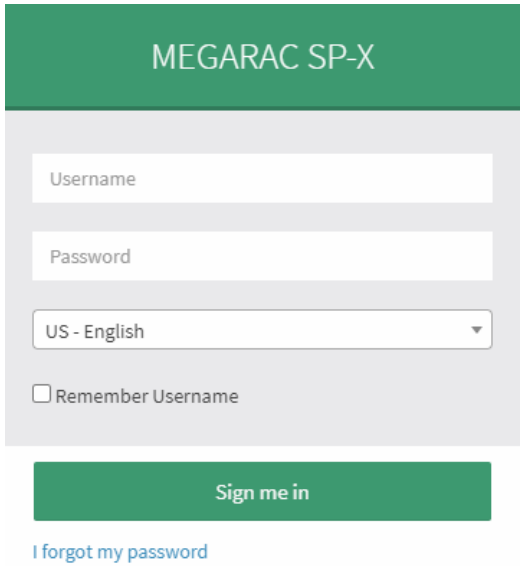
2. Or, Go to BIOS setup menu.
3. Select **Server Management**.
4. Select **BMC network Configuration**.
5. Define Configuration Address source to DynamicBmcDhcp or Static.
6. Save and Exit.
7. The **BMC IP Address** will appear on the **IPv4 Address** parameter.



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.
- **US - English:** Changes the interface language.



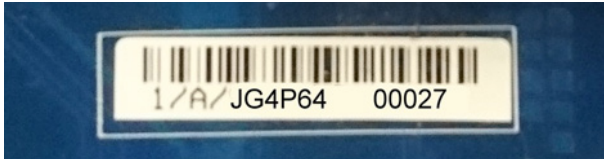
**NOTE!**

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"

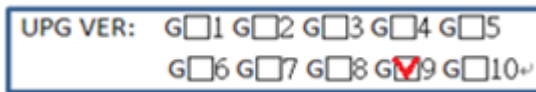


GIGABYTE will also affix new stickers that display the unique BMC password (example below) to both the product box (packaging) and to the CPU cover (for motherboards sold separately) or the server chassis.



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 user name, 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.

**Refresh:** Click the icon to reload the current page.

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

**US - English:** Click to select the language of the Web GUI.

**Warning:** Click to view the warning messages.

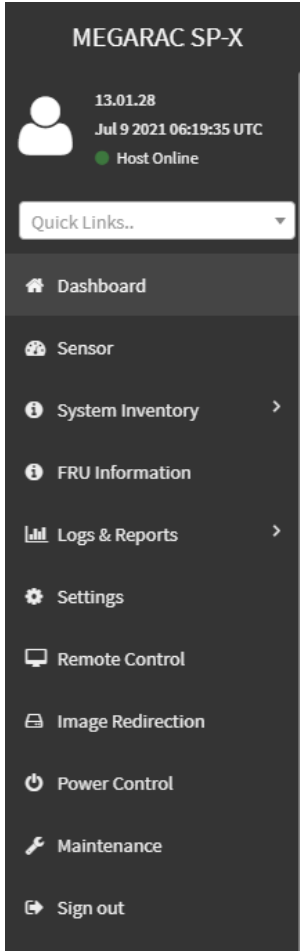
**Notification:** Click the icon to view the notification messages.

## 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:

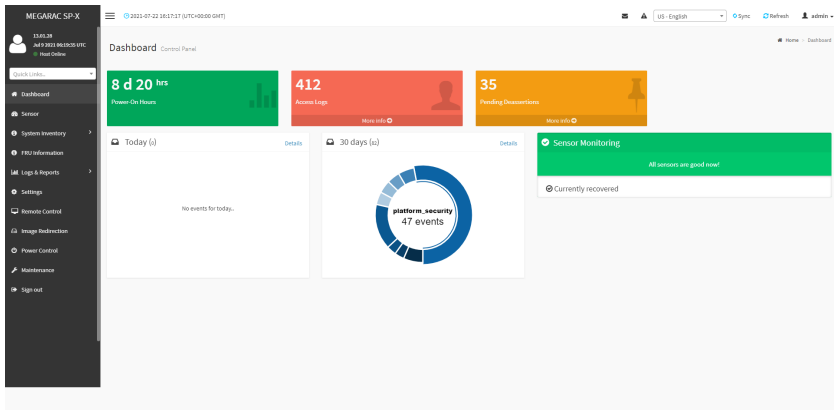


# Chapter 2 Enter Gigabyte Management Console

## 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.

### Power-On Hours

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

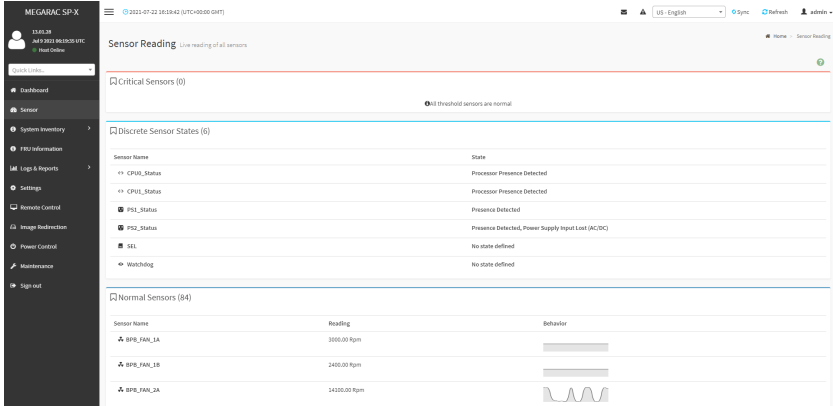
It lists all the critical sensors on the device. If you click on any list sensor, you can view the Sensor detail page with the Sensor information and Sensor Events details.

## 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.



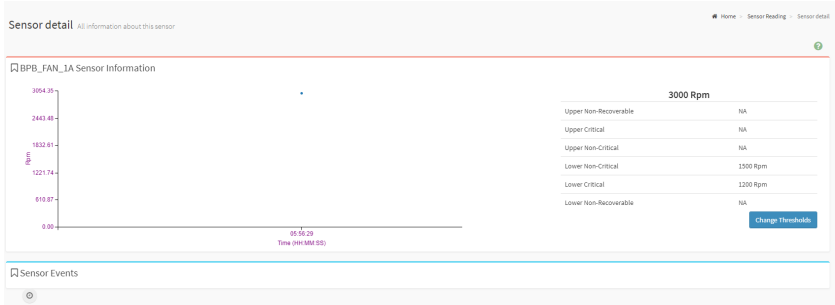
**Note:** Four DIMM Temp sensors are deployed for monitoring the DIMM temperature on the system. Users must take notice that the live reading of each DIMM Temp sensor indicates the temperature of a DIMM group, not the temperature of a specific DIMM.

## 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:

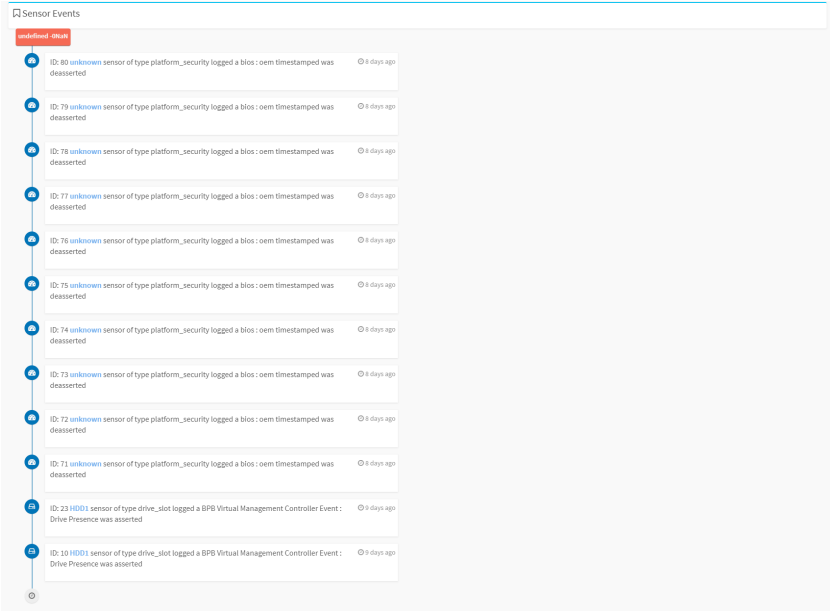
- Lower Non-Recoverable (LNR)
- Lower Critical (LC)
- Lower Non-Critical (LNC)
- Upper Non-Recoverable (UNR)
- Upper Critical (UC)
- Upper Non-Critical (UNC)

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.

## 2-2-2 Sensor Events

The Sensor Events page displays information about events that have triggered the system's sensor. A sample screenshot of Sensor Events page is shown below.

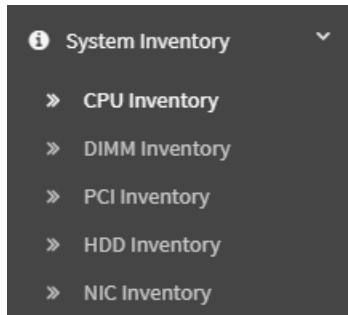


## 2-3 System Inventory

The System Inventory page displays the following information:

- CPU Inventory
- DIMM Inventory
- PCI Inventory
- HDD Inventory
- NIC Inventory

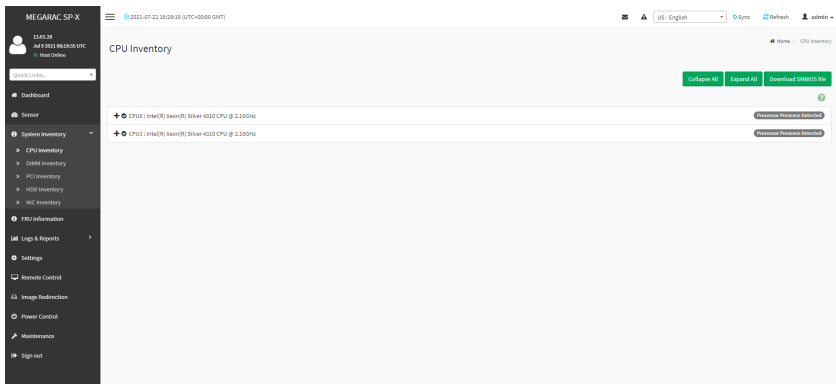
A screenshot displaying the menu items under System Inventory is shown below.



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.



MEGARDAC SP-X | 2023-07-23 14:08:45 (UTC+0800 GMT) | US English | Sync | Refresh | admin

12.61.23 | 8877.920 | 102020 | VPC | Host: Dellie

2023-07-23 14:08:45

Dashboard

Server

System Inventory

CPU Inventory

DIMM Inventory

PCI Inventory

IOCC Inventory

NIC Inventory

FRU Information

Logs & Reports

Settings

Resource Control

Image Redirection

Power Control

Maintenance

Sign out

## CPU Inventory

Home > CPU Inventory

Collapsible | Expand All | Download DRACDCs for

➤ CPU1: 114A(W) Xeon® Silver 4222 CPU @ 2.50GHz Normal Processor Details

➤ Detail information for CPU

Manufacturer	Family	External Clock	Max Speed	Speed	Core Count	Core Enabled	Thread Count
Intel® Corporation	Xeon	100,000 MHz	3,300 GHz	2,500 GHz	12	12	24

➤ Capability information for CPU

CPU Capability Name	Capable	Enabled
Y86L-machine Extensions (Y86L)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hyperthreading(HTT)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Execute Disable (XD)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Turbo Mode	<input checked="" type="checkbox"/>	<input type="checkbox"/>

➤ Cache information for CPU

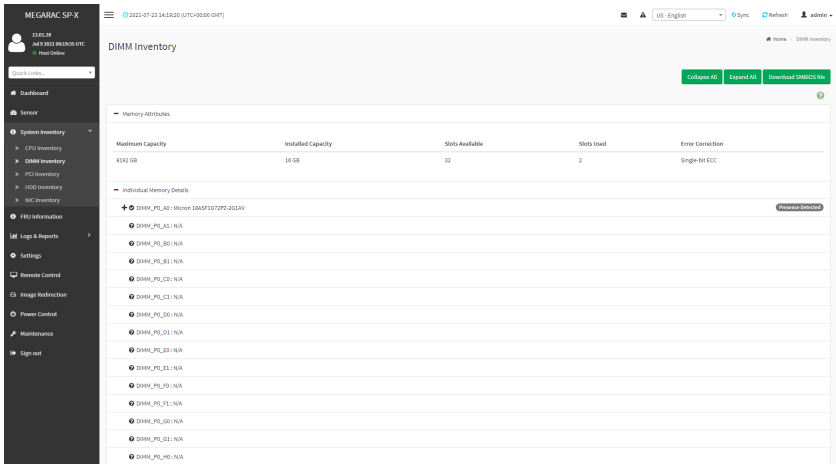
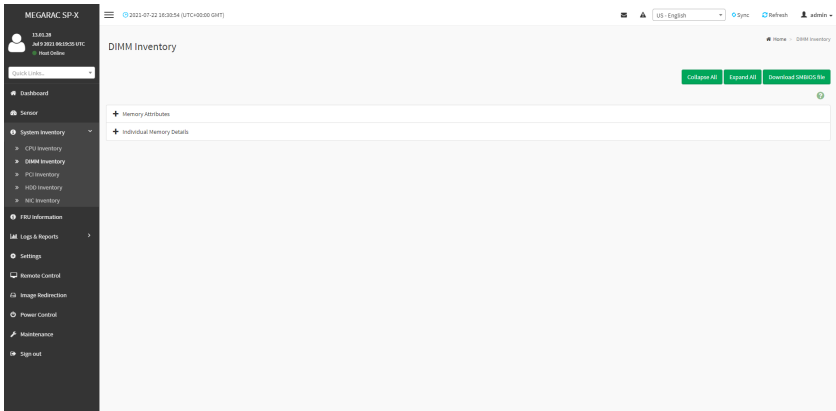
Level	Maximum Size	Installed Size	Type	Write Back Policy	Error Correction Type
1	960	960	Unified	Write Back	Single-bit ECC
2	15360	15360	Unified	Writes With Memory Address	Single-bit ECC
3	16432	16432	Unified	Writes With Memory Address	Single-bit ECC

➤ CPU2: 114A(W) Xeon® Silver 4222 CPU @ 2.50GHz Normal Processor Details



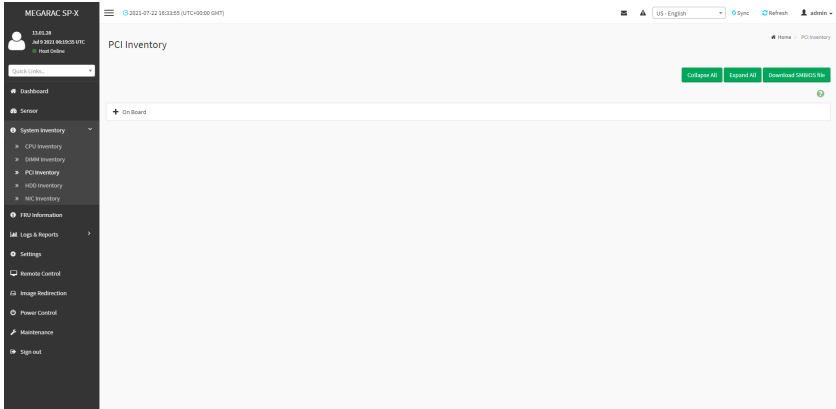
## 2-3-2 DIMM Inventory

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.

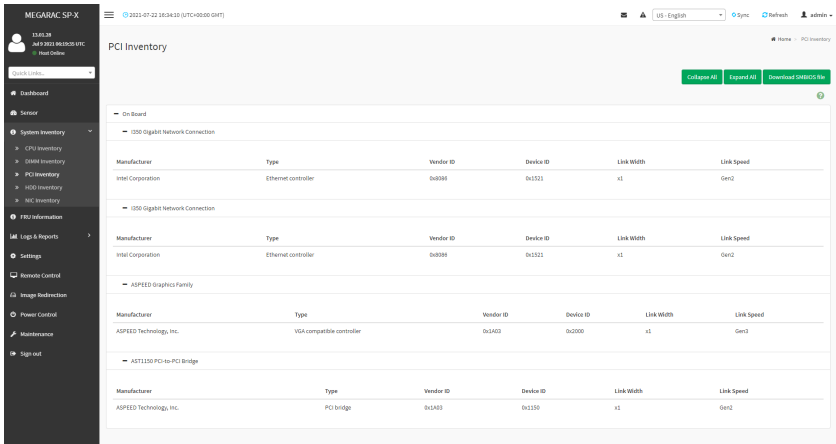


## 2-3-3 PCI Inventory

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.



The screenshot shows the MEGARAC SP-X management console. The left sidebar contains a navigation menu with options like Dashboard, Sensor, System Inventory, CPU Inventory, DIMM Inventory, PCI Inventory, HDD Inventory, NIC Inventory, FRU Information, Logs & Reports, Settings, Remote Control, Image Redaction, Power Control, Maintenance, and Sign out. The main content area is titled 'PCI Inventory' and shows a collapsed 'On Board' section. At the top right, there are buttons for 'Collapse All', 'Expand All', and 'Download SMBIOS file'.



The screenshot shows the MEGARAC SP-X management console with the 'On Board' section expanded. It displays three categories of PCI components, each with a table of details:

- 1000 Gigabit Network Connection:**

Manufacturer	Type	Vendor ID	Device ID	Link Width	Link Speed
Intel Corporation	Ethernet controller	0x8086	0x1521	x1	Gen2
- 100G Gigabit Network Connection:**

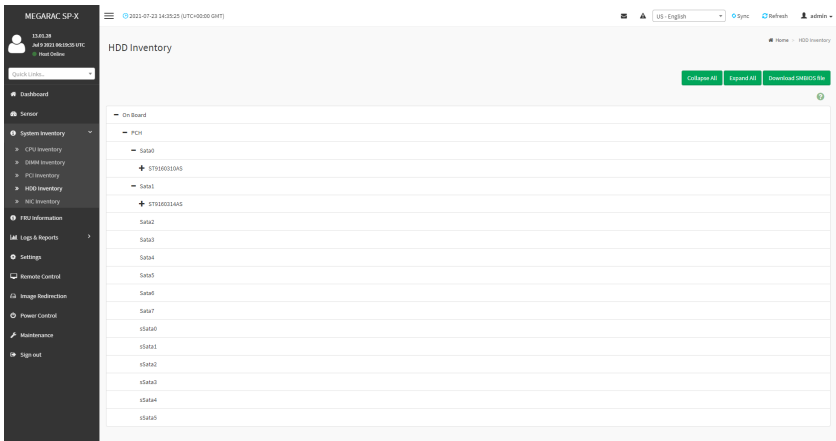
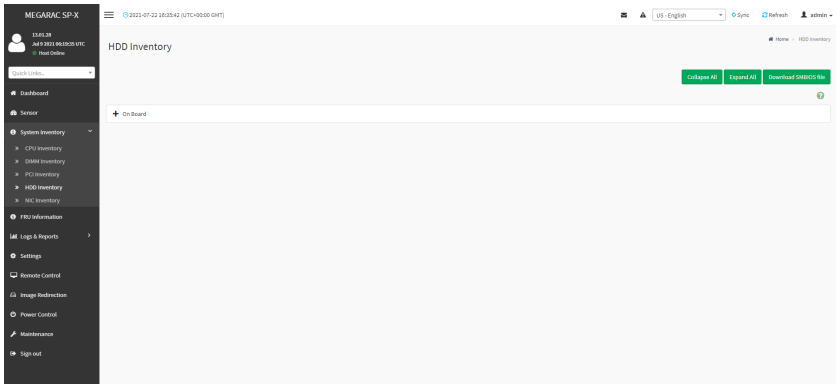
Manufacturer	Type	Vendor ID	Device ID	Link Width	Link Speed
Intel Corporation	Ethernet controller	0x8086	0x1521	x1	Gen2
- ASPEED Graphics Family:**

Manufacturer	Type	Vendor ID	Device ID	Link Width	Link Speed
ASPEED Technology, Inc.	VGA compatible controller	0x1A4D	0x2000	x1	Gen3
- AST1120 PCI-to-PCI Bridge:**

Manufacturer	Type	Vendor ID	Device ID	Link Width	Link Speed
ASPEED Technology, Inc.	PCI bridge	0x1A4D	0x1150	x1	Gen2

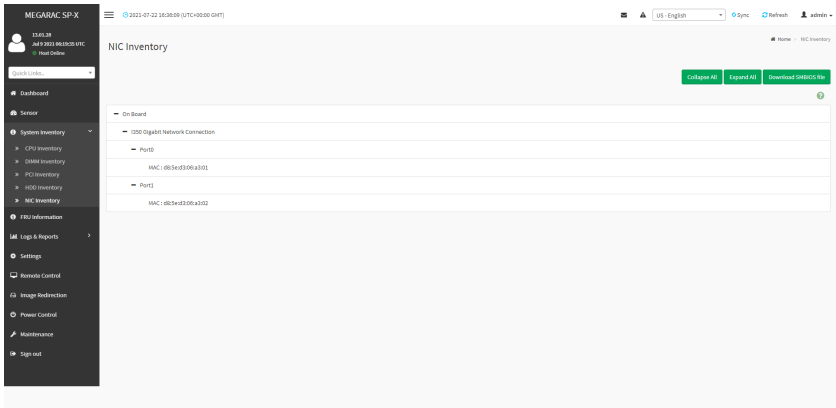
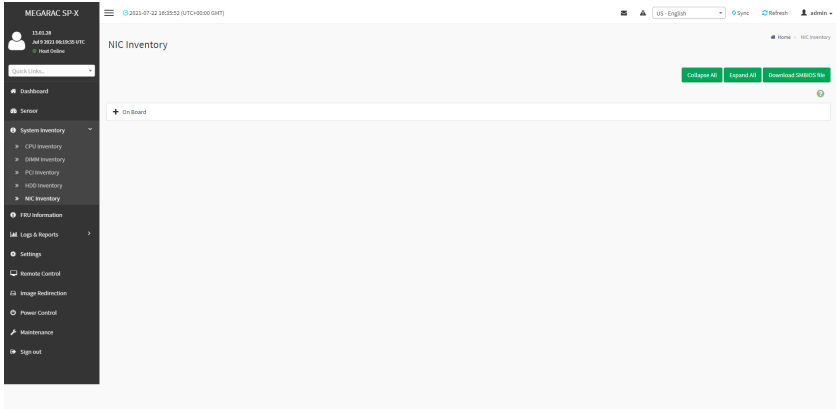
## 2-3-4 HDD Inventory

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.



## 2-4 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 screenshot shows the FRU Information page in the Gigabyte Server Management Console. The page title is "FRU Field Replaceable Units". There is a search bar for "Available FRU Devices" with a dropdown menu showing "FRU Device ID" and "FRU Device Name". The selected device name is "BMC\_FRU".

Chassis Information	Board Information	Product Information
Chassis Information Area Format Version: 1	Board Information Area Format Version: 1	Product Information Area Format Version: 1
Chassis Type: Rack Mount Chassis	Language: 0	Language: 0
Chassis Part Number: 02234567	Manufacture Date Time: Fri Jan 1 00:03:00 2022	Product Manufacturer: 020487TE
Chassis Serial Number: 0223456789012345678901	Board Manufacturer: 020487TE	Product Name: R32-NA1-00
Chassis Extra	Board Product Name: M892-P15-00	Product Part Number: 000000000001
	Board Serial Number: 020487890123	Product Version: 0200
	Board Part Number: 022345678901	Product Serial Number: 02048789012345678901
	FRU File ID	Asset Tag: 0223456789012345678901
	Board Extra: NULL	FRU File ID
		Product Extra

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**

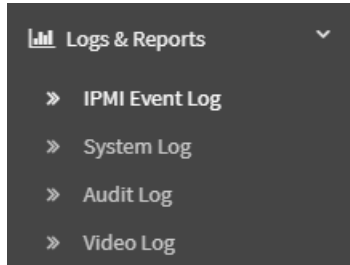
- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product Part Number
- Product Version
- Product Serial Number
- Asset Tag
- FRU File ID
- Product Extra

## 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.

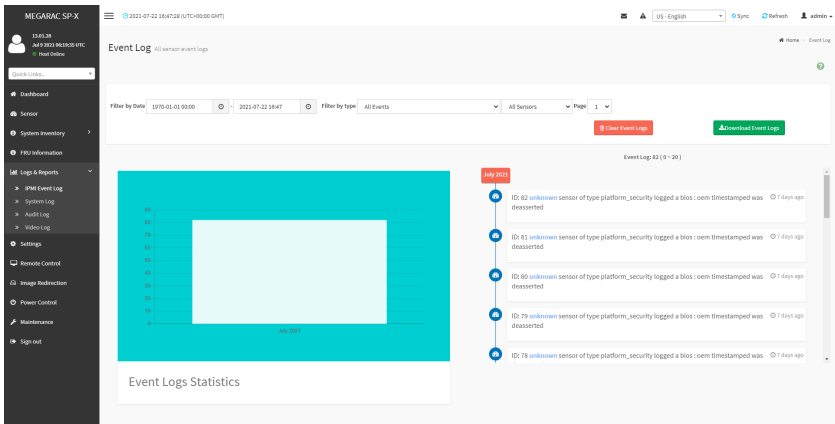


A detailed description of Logs & Reports is given below.

### 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**.

**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:** Deletes all the event logs.

**Download Event Logs:** Downloads 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.

**Note:** Logs must be configured under **Settings > Logs Settings > Advanced Log Settings** to display any entries. Filtering options are also available for this and all logs in this section.



The System Log page consists of the following fields:

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

**Event Category:** Filters the events you want to track based on the type of event. Options include Alert, Critical, Error, Notification, Warning, Debug, Emergency, Information.

**Download Logs:** Allows you to download the system logs.

### Procedure

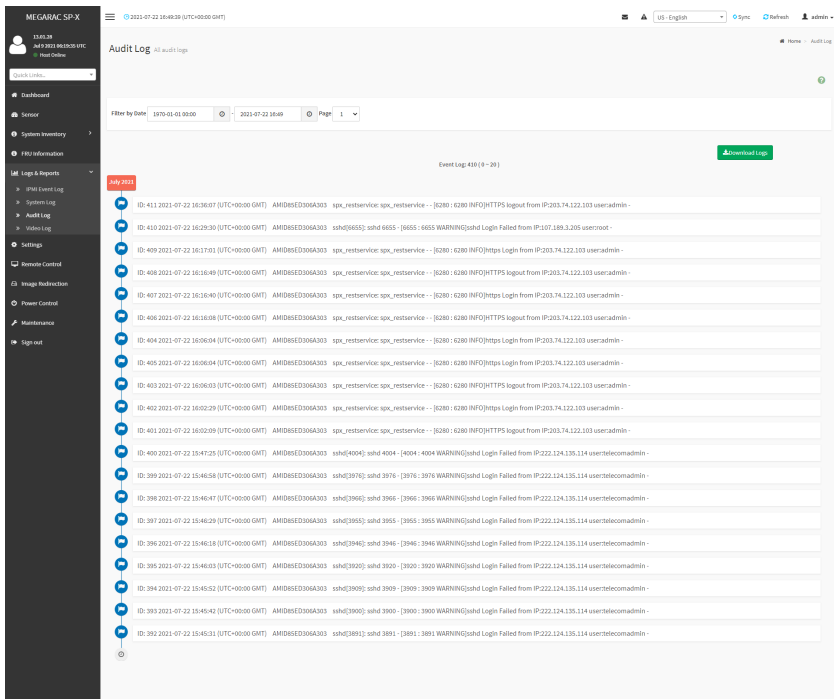
1. From the **Filter By Date** field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
2. From the **Event Category** field, select the **Category** of the event to view the relevant events for the dates. The events will be displayed based on the selected time period.
3. To download the event logs, click **Download Logs**.

## 2-5-3 Audit Log

To open the Audit Log page, click **Logs & Reports > Audit Log** from the menu bar.

A sample screenshot of Video Log page is shown below.

**Note:** For configuration, go to **Settings > Log Settings > Advanced Log Settings**.



The Audit Log page consists of the following fields:

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

**Download Logs:** Allows you to download the audit logs.

### Procedure

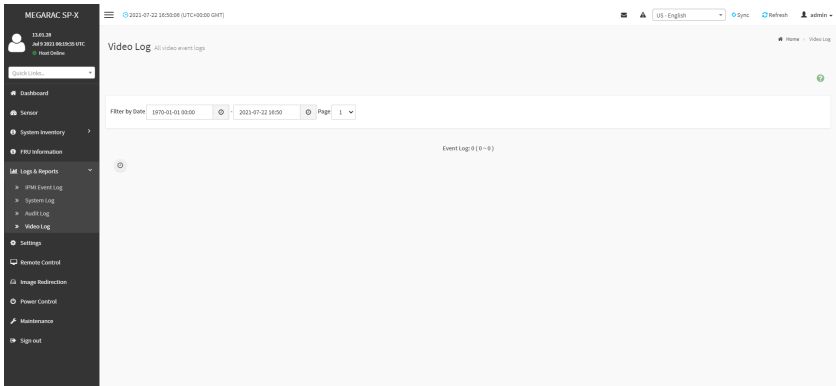
1. From the **Filter By Date** field, select the time period by **Start Date** and **End Date** using Calendar for the event categories.
2. To download the event logs, click **Download Logs**.

## 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.

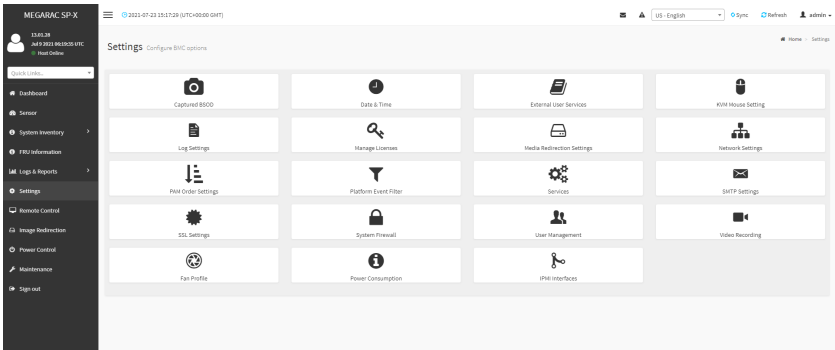
**Note:** Video Trigger Settings should be enabled, to display the Video Log page. Video Trigger Settings can be configured under **Settings > Video Recording > Auto Video Settings > Video Trigger Settings**.



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

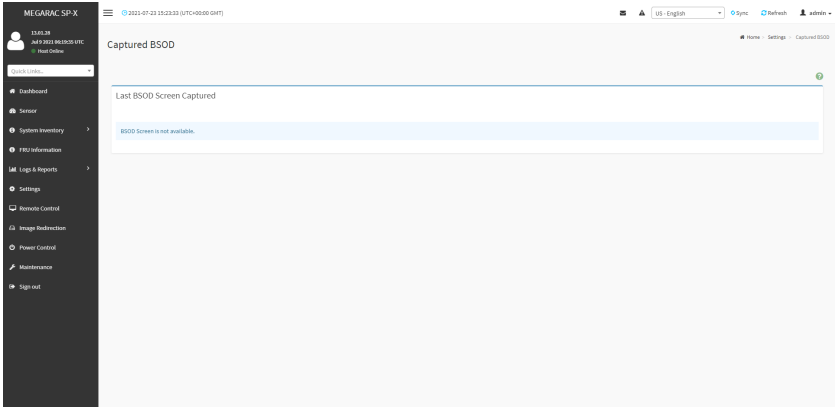
This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



A detailed description of the Settings menu is given below.

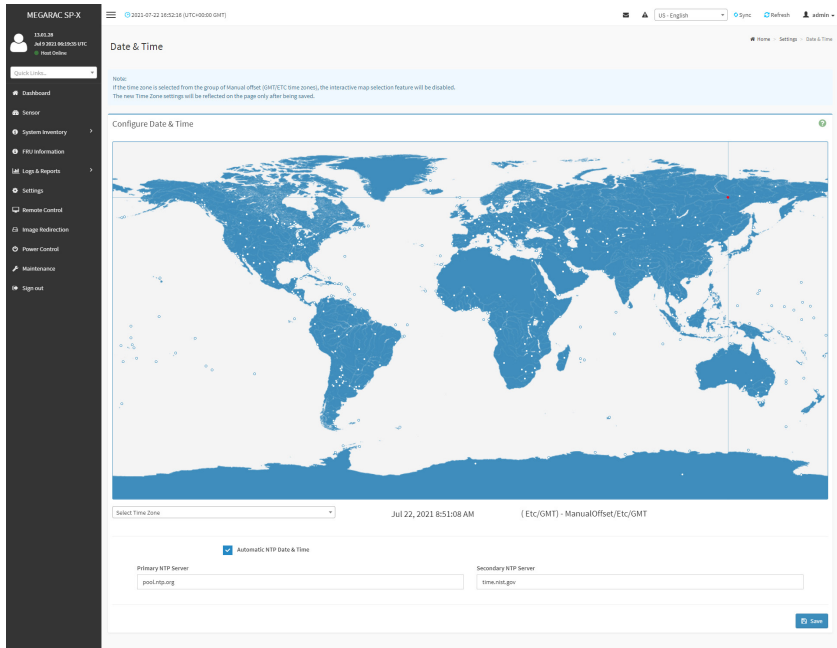
## 2-6-1 Captured BSOD

This menu is used to display a snapshot of the blue screen captured at the time when/if the host system crashed since the last reboot. A sample screenshot of Captured BSOD is shown below. **Note:** KVM service should be enabled to display the BSOD. This can be configured 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.

**Automatic NTP Date & Time:** Automatically synchronizes Date and Time with the NTP Server.

**Primary NTP Server:** Configures a primary NTP server to use when automatically setting the date and time.

**Secondary NTP Server:** Configures a secondary NTP server to use when automatically setting the date and time.

**Save:** Saves the configured settings.

### Procedure

1. Select the Time zone location from the map.
2. Enable **Automatic NTP Date & Time**.

3. In the Primary NTP Server / Secondary NTP Server field, specify the NTP server for the device.



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

4. Enable Automatic Date & Time option.
5. Click Save button to save the settings.

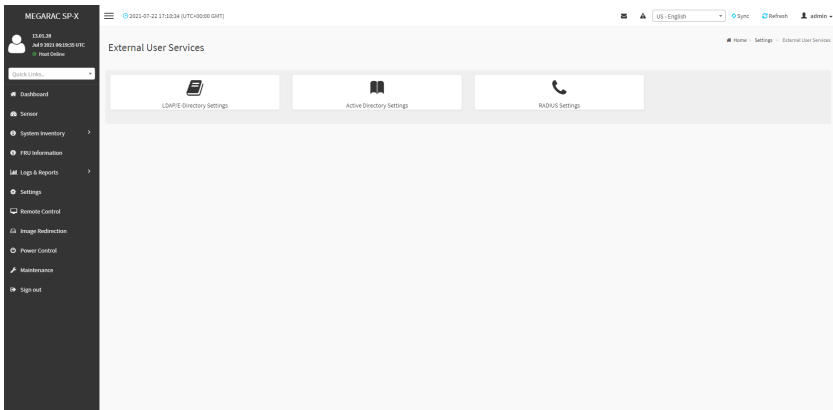
### 2-6-3 External User Services

#### 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.

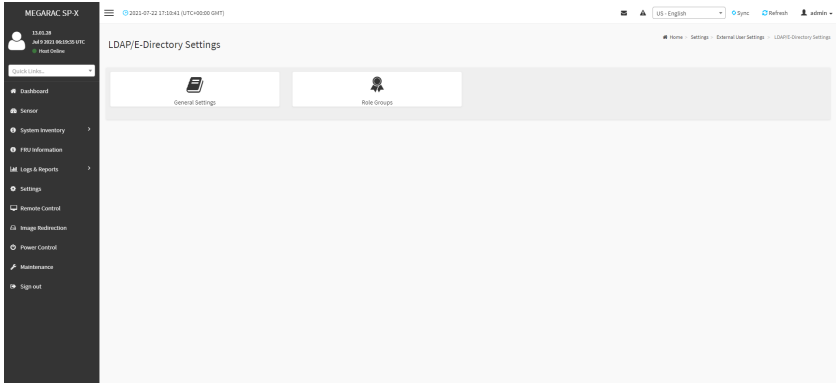
In Web GUI, LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate BMC users. This is done by passing login requests to your LDAP Server. This means that there is no need 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.



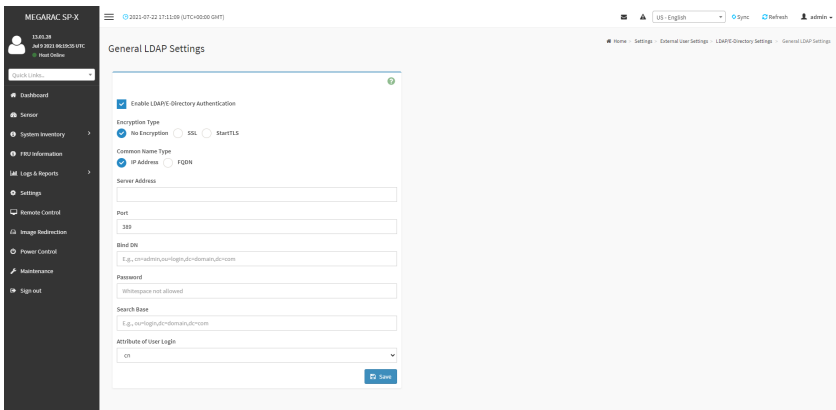
The fields in the LDAP/E-Directory Settings page are explained below.

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

**Role Groups:** Adds 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.
3. Select the Encryption Type for LDAP/E-Directory.



**Note:** Configure the proper port number, when SSL is enabled.

4. Select the Common Name Type.

5. Enter the IP address of LDAP server in the Server Address field.



**Note:** IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.

Each Number ranges from 0 to 255.

First Number must not be 0.

Supports IPv4 Address format and IPv6 Address format.

Configure FQDN address, when using StartTLS with FQDN.

6. Specify the LDAP Port in the **Port** field.



**Note:** Default Port is 389.

For SSL connections, default port is 636.

The Port value ranges from 1 to 65535.

Port 80 is blocked for TCP/UDP protocols.

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



**Note:** Bind DN is a string of 4 to 63 alpha-numeric characters.

It must start with an alphabetical character.

Special Symbols like dot(.), comma(,), hyphen(-), underscore(\_), equal-to(=) are allowed.

Example: cn=manager, ou=login, dc=domain, dc=com

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



**Note:** Password must be at least 1 character long.

Blank space is not allowed.

This field will not allow more than 47 characters.

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



**Note:** Search base 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: ou-login, dc-domain, dc-com

10. Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.



**Note:** It only supports cn or uid.

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

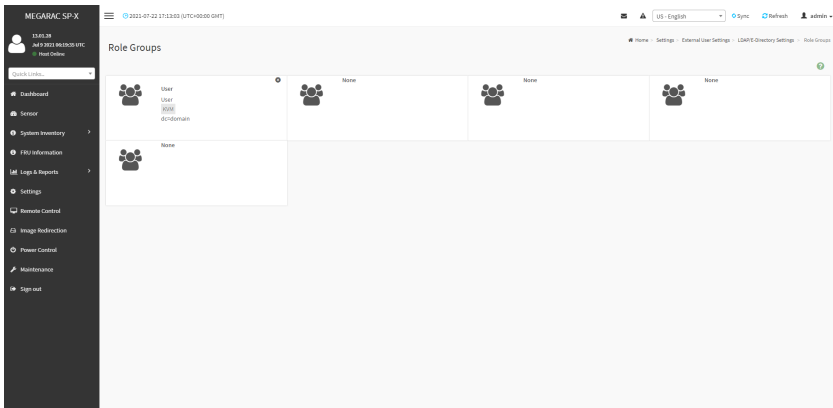


**Note:** All the 3 files are required, when StartTLS is enabled.

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

### To add a new Role Group

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



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



**Note:** Role Group Name is a string of 64 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=loginc, 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.

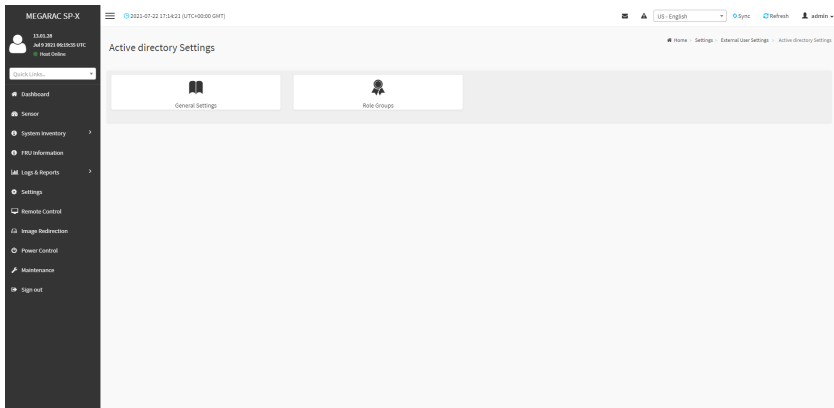
## Active Directory Settings

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 in the Active Directory page are explained below.

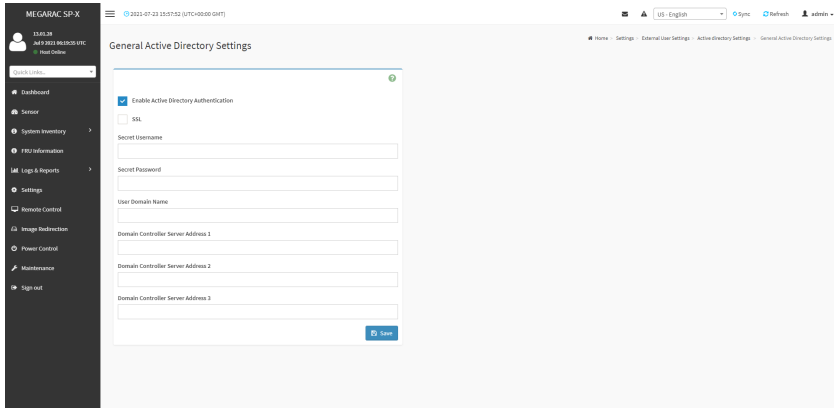
**General Settings:** Configures Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain Name, and up to three Domain Controller Server Addresses.

**Role Groups:** Adds 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.



The screenshot shows the 'General Active Directory Settings' page. The sidebar on the left contains a navigation menu with items like Dashboard, Sensor, System Inventory, FPD Information, Logs & Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign out. The main content area has a header with the title 'General Active Directory Settings' and a breadcrumb trail: Home > Settings > External User Settings > Active Directory Settings > General Active Directory Settings. The form includes a checkbox for 'Enable Active Directory Authentication' (checked), an 'SSL' checkbox (unchecked), and input fields for 'Secret Username', 'Secret Password', 'User Domain Name', and three 'Domain Controller Server Address' fields. A 'Save' button is located at the bottom right of the form.

2. In the Active Directory Settings page, check/uncheck the **Enable Active Directory Authentication** check box to enable/disable Active Directory Authentication.



**Note:** If Active Directory Authentication is enabled, 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 Active Directory 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 Active Directory in the last location in PAM order.

User Name is a string of 1 to 64 alpha-numeric characters.

It must start with an alphabetical character.

It is case-sensitive.

Special characters like comma, period, colon, semicolon, slash, backslash, square brackets, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.

Password must be at least 6 character long and will not allow more than 127 characters.

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 Address 1**, **Domain Controller Server Address 2** and **Domain Controller Server Address 3**.



**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 Settings > Role Groups** from the menu bar. A sample screenshot of Role Groups page is shown below.

The screenshot displays the 'Role Groups' configuration page. On the left is a dark navigation sidebar with options like Dashboard, Sensor, System Inventory, FRU Information, Logs & Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign out. The main content area shows a grid of role groups. The first group is 'dtest administrator' with a domain of 'KVM\_VMedia.sit.com'. The other three groups are labeled 'None'. The top of the page shows the user 'admin' and various system controls like Sync, Refresh, and language settings.

The fields in the 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.

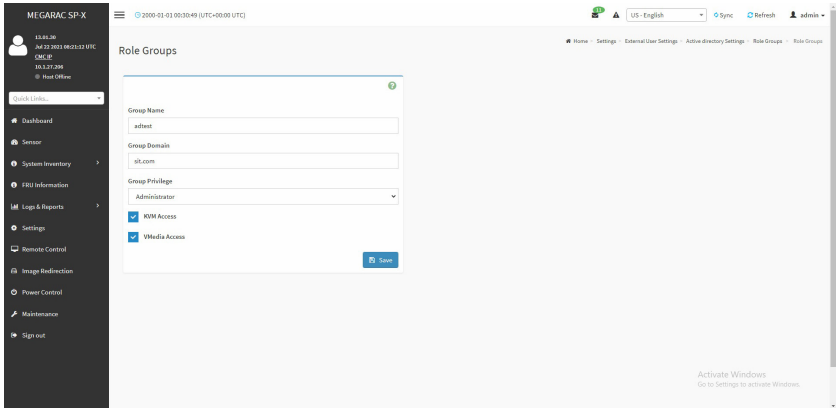
**Group Privilege:** The level of privilege to assign to this role group.

**KVM Access:** Provides access to KVM for AD authenticated role group user.

**VMedia Access:** Provides 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

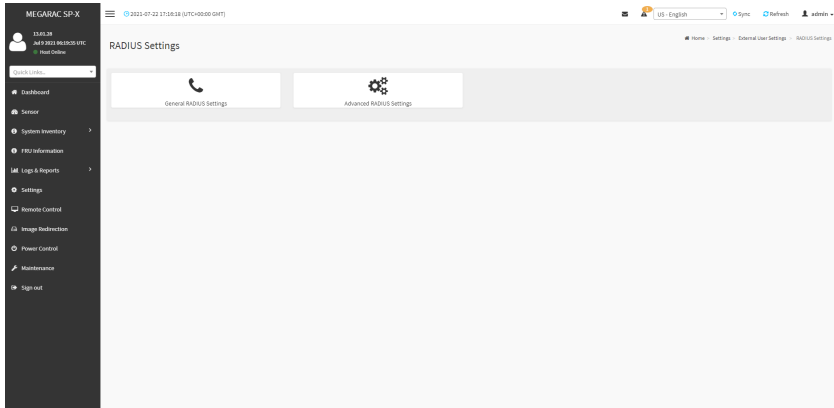
1. In the **Role Groups** Page, select the row that you want to delete.
2. Click Delete Role Group.

## 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 in the 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.  
Port 80 is blocked for TCP/UDP protocols.

**Secret:** The Authentication Secret for RADIUS server.



**Note:** This field will not allow more than 32 characters.  
Secret must be at least 4 characters long.  
Blank space is not allowed.

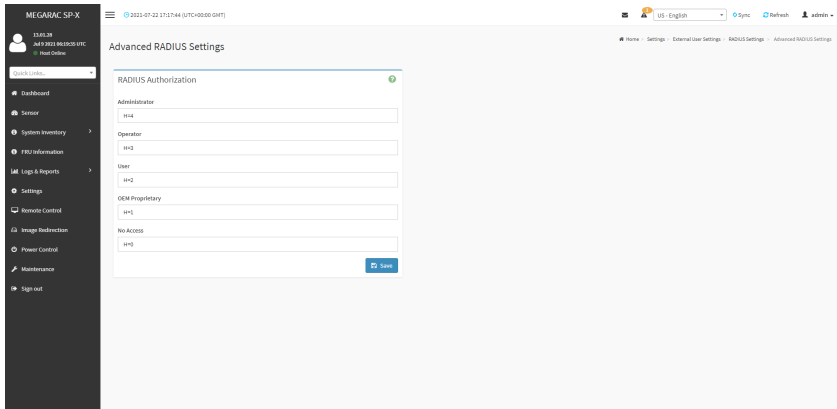
**Enable KVM Access:** This field provides access to KVM for RADIUS authenticated users.

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

**Save:** Saves 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 on the server.

These fields will not allow more than 127 characters and the "#" sign is not allowed.

### Example 1:

Add Vendor-Specific attribute

```
cd/usr/share/freeradius
```

```
vim dictionary.adtest
```

(Add content below)

```
# dictionary.adtest
VENDOR ADTest 58
# Standard attribute
BEGIN-VENDOR ADTest
ATTRIBUTE ADTest-group 1 string
END-VENDOR ADTest
```

```
vim dictionary
```

(Add this line)

```
$INCLUDE dictionary.adtest
```

### Example 2:

Add users

```
vim users
```

(add content below)

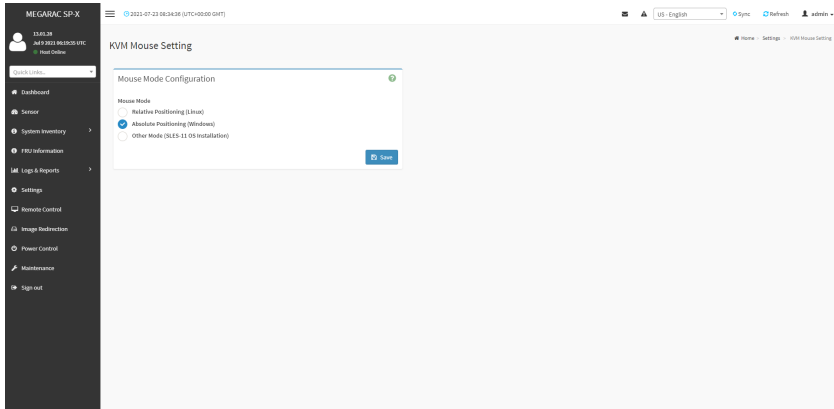
```
"RadiusTest1" Cleartext-Password:="000000"
Service-Type=Administrative-User,
Auth-Type:=System,
ADTest-group:="H=4"
```

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 in the KVM Mouse Settings page are explained below.

**Relative Positioning (Linux):** The 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. Recommended for Windows or later Linux releases.

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

**Save:** Saves the current changes.

### Procedure

1. Choose either of the following as your requirement:

- Set to Absolute Positioning (Windows)



**Note:** Applicable for all Windows versions, versions above RHEL6, and versions above FC14.

- Set to Relative Positioning (Linux).



**Note:** Applicable for all Linux versions, versions less than RHEL6, and versions less than FC14.

- Set to Other Mode (SLES-11 OS Installation).



**Note:** Recommended for SLES-11 OS Installation.

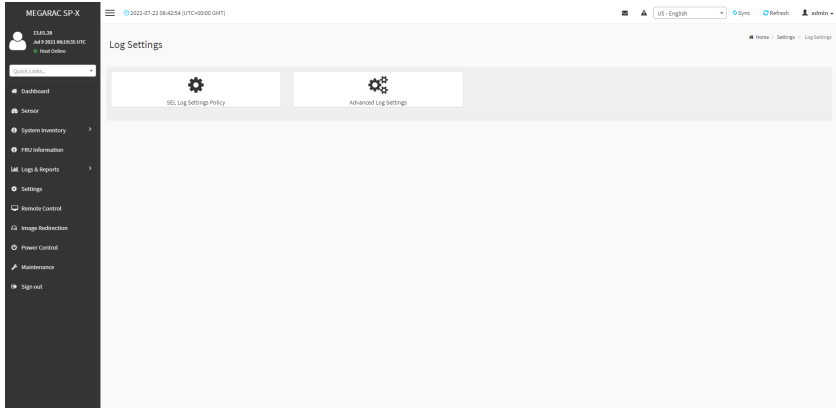
2. Click **Save** button to save the changes made.

## 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 the Log Settings page, click **Settings > Log Settings** from the menu bar.

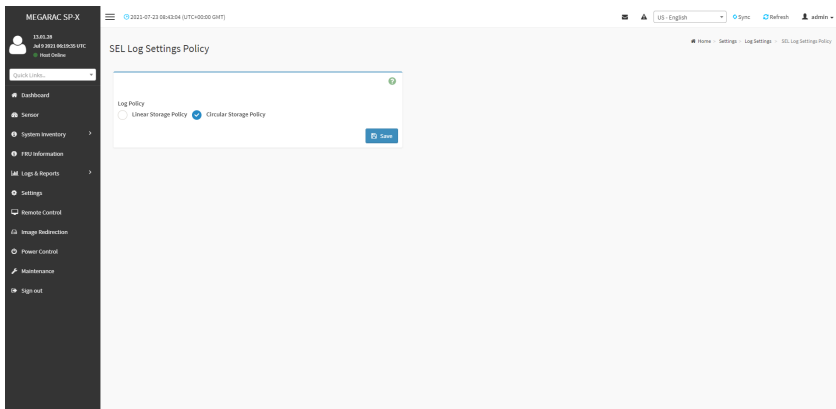
A sample screenshot of Log Settings page is shown below.



The fields in the Log Settings page are explained below.

### SEL Log Settings Policy

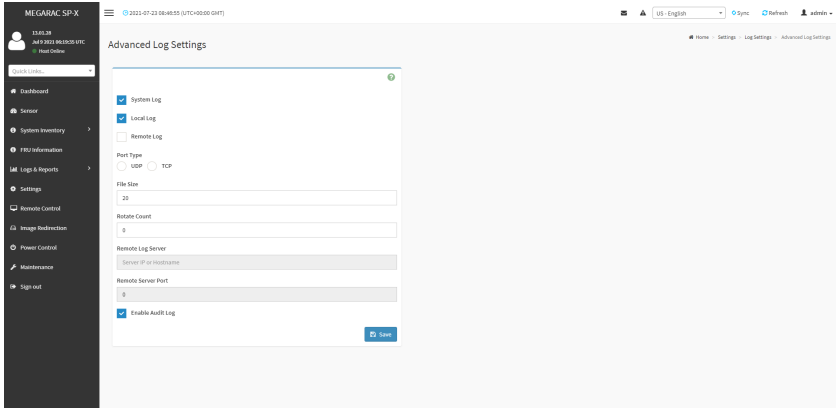
To open SEL Log Settings Policy page, click **Settings > Log Settings > SEL Log Settings Policy** from the menu bar. The SEL Log Settings Policy page is used to configure the log policy for the event log. A sample screenshot of SEL Log Settings Policy page is shown below.





# 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 page is shown below.



The fields in the Advanced Log Settings page are explained below.

**System Log:** Check/uncheck to enable/disable the System Logs.


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

 **Note:** Local file resides at `/var/log/`


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

**Port Type:** When Remote Log is enabled, user can select either UDP or TCP per requirement.

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

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


**Rotate Count:** Backs 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 and IPv6 address format.  
FQDN (Fully qualified domain name) format.

**Remote Server Port:** This field is to specify the remote server port 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:** Enables/Disables the audit log.

**Save:** Saves 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.

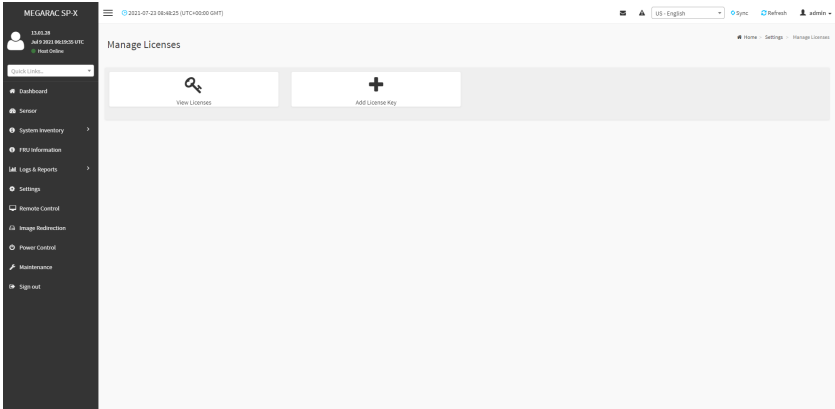


**Note:** If Remote Log is selected, the fields file size and rotate count need not be mentioned.

4. If Remote Log is selected, specify the **Port Type**, **Remote Log Server**, and **Remote Server Port**.
5. In the **Audit Log** field, check or uncheck the **Enable** option as needed.
6. Click **Save** to save the changes.

## 2-6-6 Manage Licenses

This page displays available licenses for this system and the validity period of the licenses. To open the Manage Licenses page, click **Settings > Manage Licenses** from the menu bar. A sample screenshot of Manage Licenses page is shown below.



The fields in the Manage Licenses page are explained below.

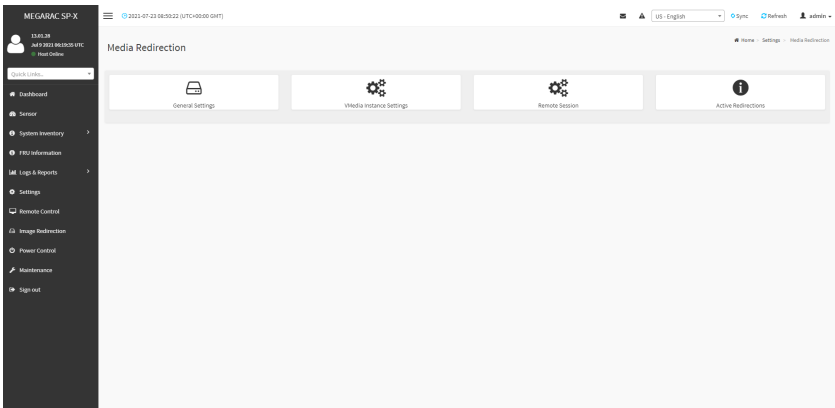
**View Licenses:** Displays the available licenses and the validity period of the licenses.

**Add License Key:** Select to add a license key.

## 2-6-7 Media Redirection Settings

This page is used to configure the media into BMC for redirection. To open the Media Redirection page, click **Settings > Media Redirection Settings** from the menu bar.

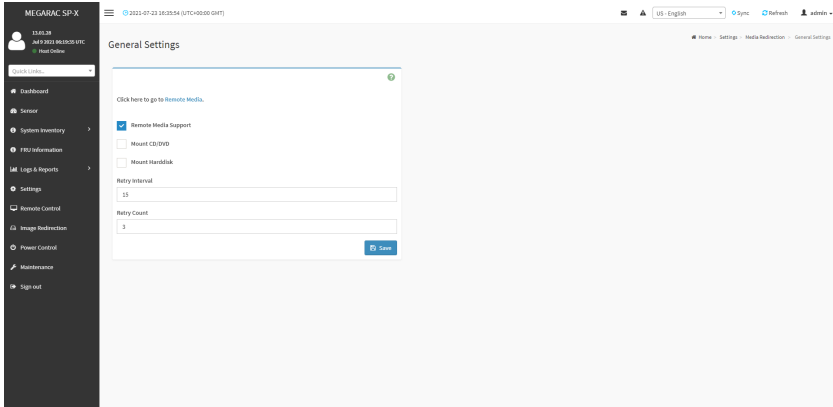
A sample screenshot of Media Redirection page is shown below.



The fields in the Media Redirection page are explained below.

## General Settings

This option is used to configure General Media Settings. To open the General Media Settings section, click **Settings > Media Redirection Settings > General Settings**.



**Remote Media Support:** Enables/Disables Remote Media support, check/uncheck the box. Remote Media emulates CD/DVD/HDD images as media through BMC.

**Mount CD/DVD:** Enables/Disables Mount CD/DVD support, check/uncheck the check box.



**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.

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

**Share Type for CD/DVD:** Selects the Share Type of the remote media server either NFS, CIFS, or HTTP.

**Domain Name, Username, and Password:** If share type is CIFS, then enter user credentials to authenticate on the server.

**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:** Displays the source path to the remote media images.

**Share Type for Harddisk:** Selects the Share Type of the remote media server either NFS, CIFS, or HTTP.

**Domain Name, Username, and Password:** If share type is CIFS, then enter user credentials to authenticate on the server.

**Retry Interval:** Gives time interval for each attempt to reconnect Remote Media.

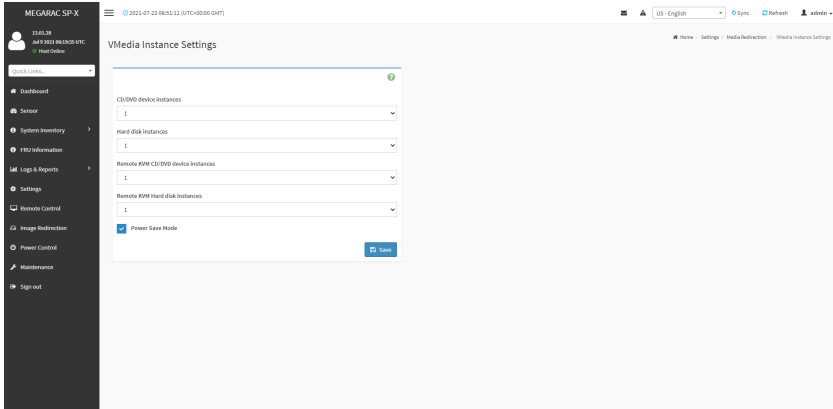
**Retry Count:** Specifies the number of attempts to reconnect Remote Media.

**Save:** Saves the configurations.

## VMedia Instance Settings

This page is used to configure Virtual Media device settings. To open the 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 hard disk 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.

**Power Save Mode:** Enables/Disables 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:** Saves 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 CD/DVD devices, harddisk devices and remote KVM CD/DVD and hard disk devices from the respective drop-down list.



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

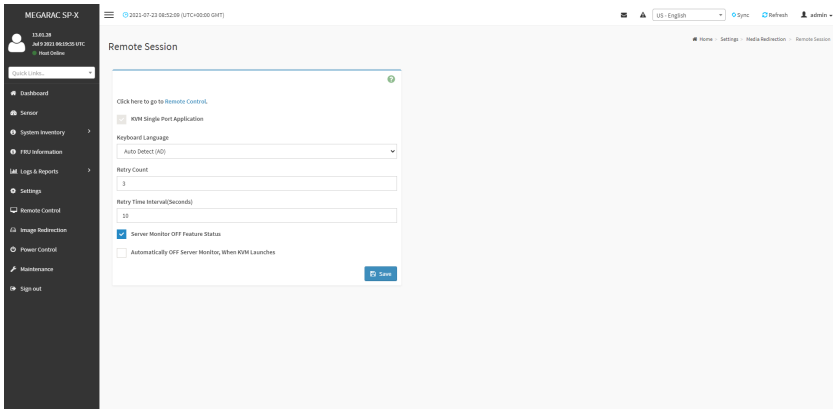
2. Check/uncheck the **Power Save Mode** option to enable/disable the virtual USB devices visibility in the host.
3. Click **Save** to save the changes made.

## Remote Session

In BMC Web, this page is used to configure Remote Session configuration settings. **KVM Single Port Application** is enabled by default.

To open the 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 in the Configure Remote Session page are explained below.

**KVM Single Port Application:** This item is checked (enabled) by default and is not configurable. The KVM session will not use its dedicated port whereas both Web and KVM sessions will be established only via Web Port.

**Keyboard Language:** Select the keyboard supported languages.

**Retry Count:** Retries the redirection session for certain number of attempts.

**Retry Time Interval (Seconds):** Gives time interval for each attempt.

**Server Monitor OFF Feature Status:** Enables/Disables 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:** Enables/Disables Automatically OFF Server Monitor, When KVM Launches.

**Save:** Saves the current changes.



**Note:** It will automatically close the existing remote redirection either KVM or Virtual media sessions on Single Port enable/disable.



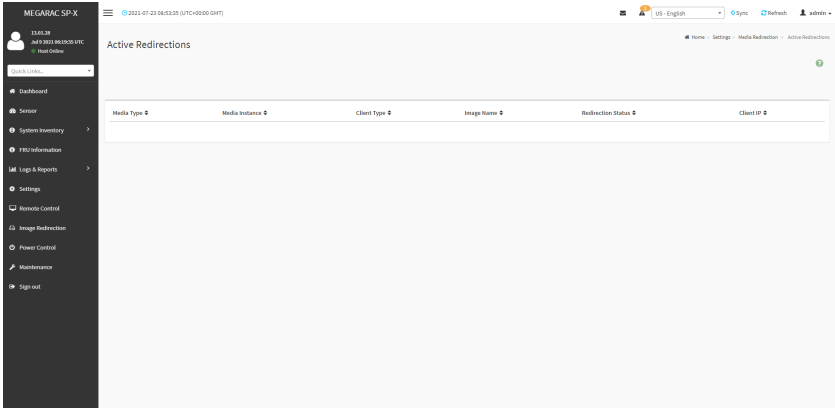
**Note:** Installation of Operating System on the servers via BMC CD ISO image over remote KVM may take 1 to 2 hours.

### 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.

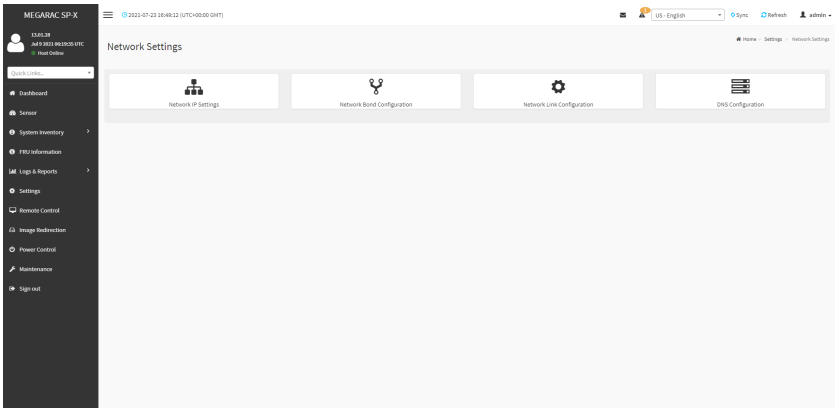
## Active Redirections

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



## 2-6-8 Network Settings

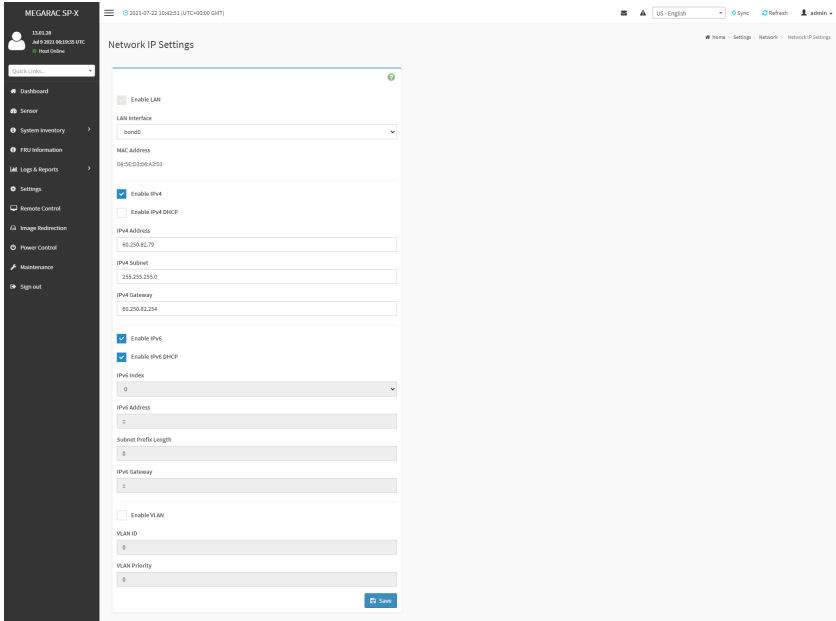
The Network Settings page is used to configure the network settings for the available LAN channels. It also allows users to manage the DNS settings or configure Network Controller Sideband Interface of a device. To open the Network Settings page, click **Settings > Network Settings** from the menu bar.





# 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 in the Network IP Settings page are explained below.

**Enable LAN:** Enables/disables the LAN Settings.

**LAN Interface:** Lists the LAN interfaces.

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

**Enable IPv4:** Enables/disables the IPv4 settings in the device.

**Enable IPv4 DHCP:** Enables IPv4 DHCP support for the selected interface.

**IPv4 Address, IPv4 Subnet, 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:** Enables/disables the IPv6 configuration settings.

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

**IPv6 Index:** Specifies a static IPv6 Index to be configured to the device. E.g.: 0

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

**Subnet Prefix Length:** Specifies the subnet prefix length for the IPv6 settings.



**Note:** Value ranges from 0 to 128.

**IPv6 Gateway:** Specifies IPv6 default gateway.



**Note:** If core feature IPV6\_COMPLIANCE is enabled, the IPV6 default Gateway field will not be displayed.

**Clear IPv6 Address:** Check to clear the IPv6 address.

**Enable VLAN:** Enables/Disables the VLAN support for selected interface.

**VLAN ID:** The Identification for VLAN configuration.



**Note:** Value ranges from 1 to 4094.  
VLAN ID cannot be changed without resetting the VLAN configuration.

**VLAN Priority:** The priority for VLAN configuration.



**Note:** Value ranges from 0 to 7.  
7 is the highest priority for VLAN.

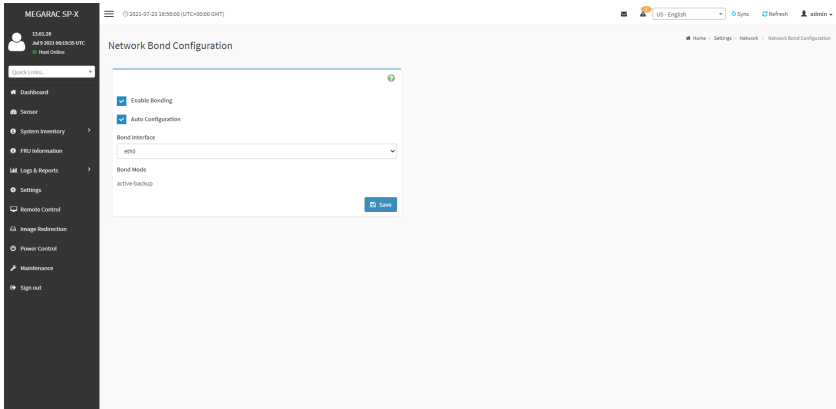
**Save:** Saves the entries.

## 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** and **IPv4 Default Gateway** in the respective fields.
6. In IPv6 Configuration, if you want 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 Index, IPv6 Address, Subnet Prefix length** and **IPv6 Gateway** in the given field.
9. In VLAN Configuration, if you want to enable the VLAN settings, check **Enable LAN**.
10. Enter the **VLAN ID** in the specified field.
11. Enter the **VLAN Priority** in the specified field.
12. Click **Save** to save the entries.

# Network Bond Configuration

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



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

**Enable Bonding:** Check to enable network bonding.



**Note:** If VLAN is enabled for any slave interfaces, Bonding cannot be enabled. To disable VLAN, go to **Configuration > Network > VLAN**.

**Auto Configuration:** Check to enable automatic configuration of network interfaces.

**Bond Interface:** Configures bonding for network interfaces.



**Note:** A minimum of two network interfaces is required to enable Network Bonding for the device.

**Bond Mode:** Displays the network bonding mode in effect. This field is not configurable.

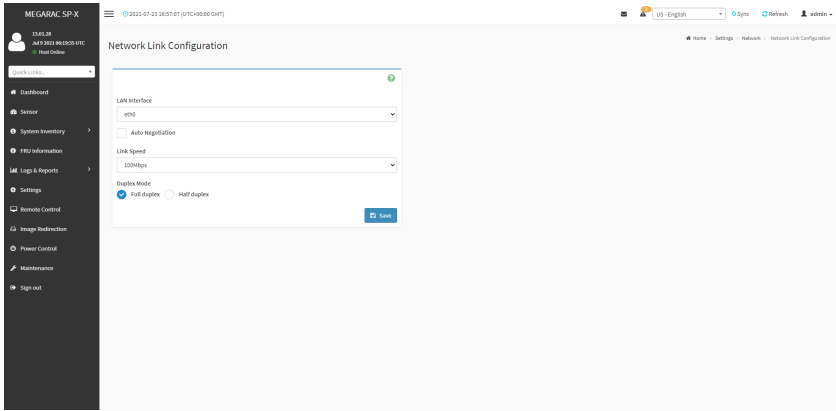
**Save:** Saves the entries.

## Procedure

1. Check **Enable Bonding** to enable network bonding for the network interfaces.
2. Check **Auto Configuration** to enable automatic combination of network interfaces.
3. Select a bond interface.
4. Click **Save** to save the entries.

# Network Link Configuration

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



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

**LAN Interface:** Select a network interface.

**Auto Negotiation:** Check to enable automatic negotiation.

**Link Speed:** Configures the link speed.



**Note:** The link speed can be 10, 100, or 1000 Mbps.  
Link speed of 1000 Mbps is not applicable when Auto Negotiation is disabled.

**Duplex Mode:** Select the duplex mode.



**Note:** This setting option cannot be configured if Auto Negotiation is enabled.

**Save:** Saves the entries.

## Procedure

1. Select a network interface you want to configure from **LAN Interface**.
2. Check **Auto Negotiation** to enable automatic configuration.
3. Configure the link speed.



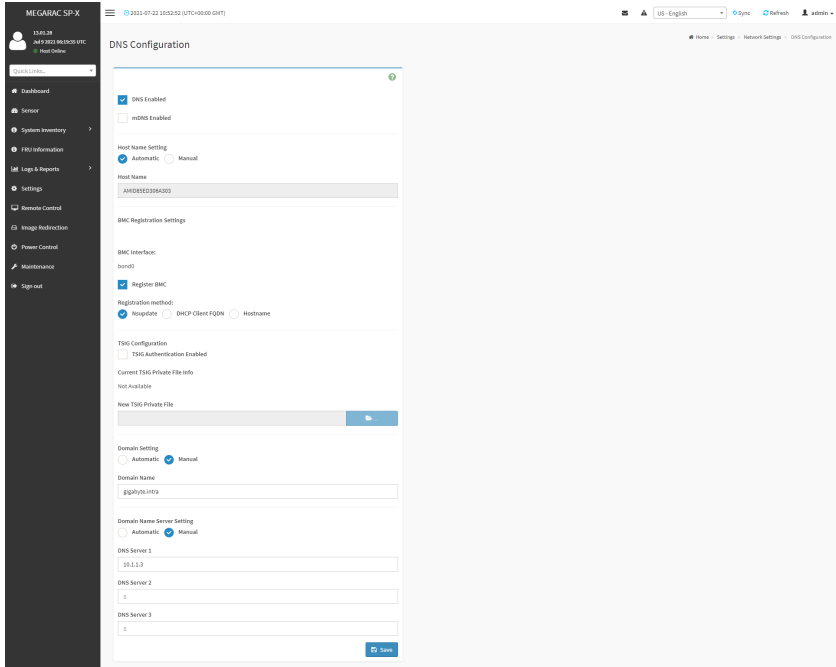
**Note:** This setting option cannot be configured if Auto Negotiation is enabled.

4. Select the duplex mode.
5. 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:** Enables/Disables all the DNS Service configurations.

**mDNS Enabled:** Enables/Disables Multicast DNS.

**Host Name Setting:** 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:** Registers BMC through registration method.

**Registration Method:** Options to register the BMC are through **Nsupdate** or **DHCP Client FQDN** or **Hostname**.

## TSIG Configuration

**TSIG Authentication Enabled:** Check this box to enable TSIG authentication while registering DNS via nsupdate. Separate TSIG files can be uploaded for each LAN interface.

**Current TSIG Private File:** The information of current TSIG private file along with its uploaded date/time will be displayed (read-only).

**New TSIG Private File:** Browse and navigate to the TSIG private file.



**Note:** TSIG file should be of private type.

## Domain Setting

**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, the 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:** Saves the current changes.

## Procedure

1. Check the option **DNS Enabled** to enable all the DNS Service configurations.
2. Check the option **mDNS Enabled** to enable Multicast DNS.
3. 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.

4. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
5. Under Register BMC, choose the BMC's network port to register with DNS settings.
6. Check **Register BMC** 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.



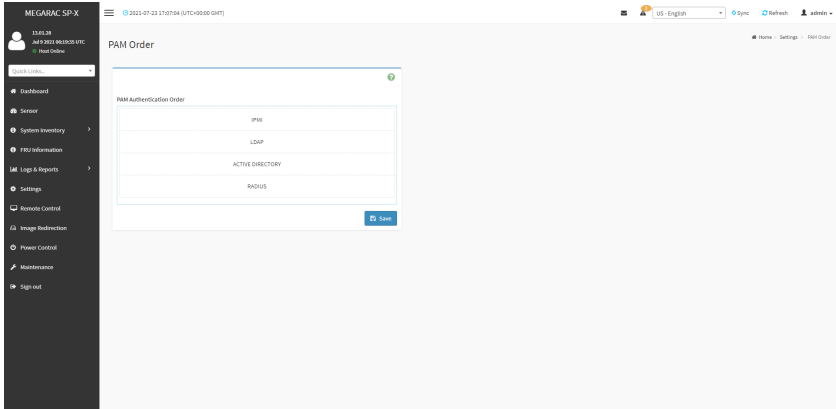
**Note:** Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.

7. In **TSIG Configuration**, check **TSIG Authentication Enabled** enable 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.
8. In **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.
9. In **Domain Name Server Setting**,
  - Select the DNS Name Server Setting (Automatic or Manual).
  - Choose the IP Priority, either IPv4 or IPv6.
  - Enter the DNS Server address.
10. In **DNS Server 1**, **DNS Server 2** and **DNS Server 3**, enter the server addresses to be configured for the BMC.
11. Click **Save** to save the entries.

## 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 in the PAM Order page are explained below.

**PAM Authentication Order:** 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.

**Save:** Saves the configuration.

### 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.



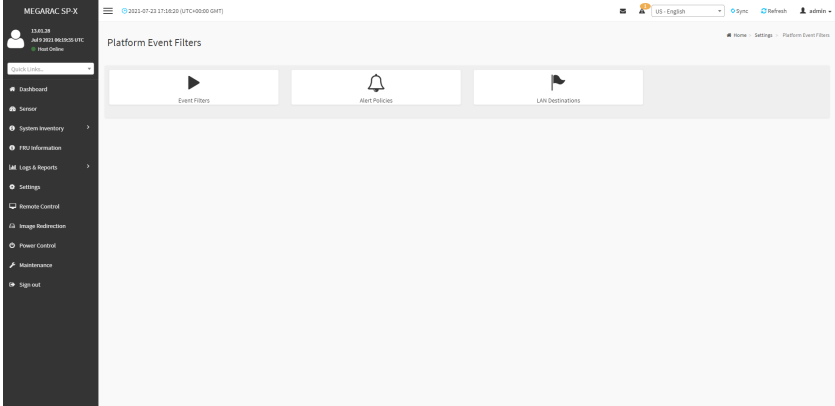
**Note:** Whenever the configuration is modified, the web server will be restarted automatically. Logged-in session will be logged out.



## 2-6-10 Platform Event Filter

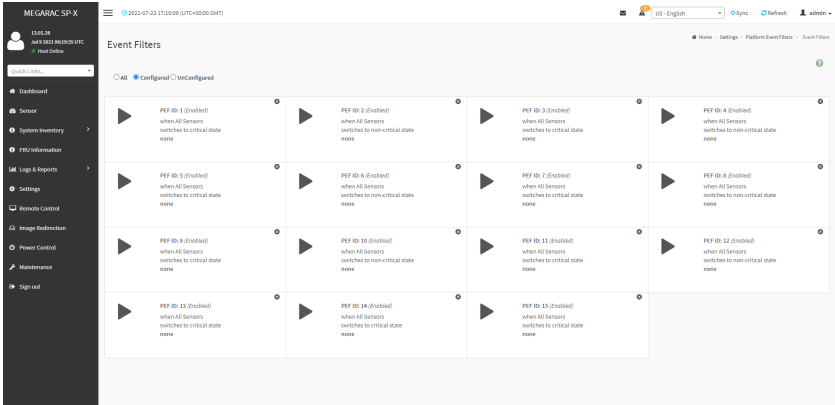
Platform Event Filter (PEF) provides a mechanism for configuring the BMC to take selected actions on event messages that it receives or has internally generated. These actions include operations such as system power-off, system reset, as well as triggering the generation of an alert.

To open PEF Management Settings page, click **Settings > Platform Event Filter** from the menu bar.



### Event Filters

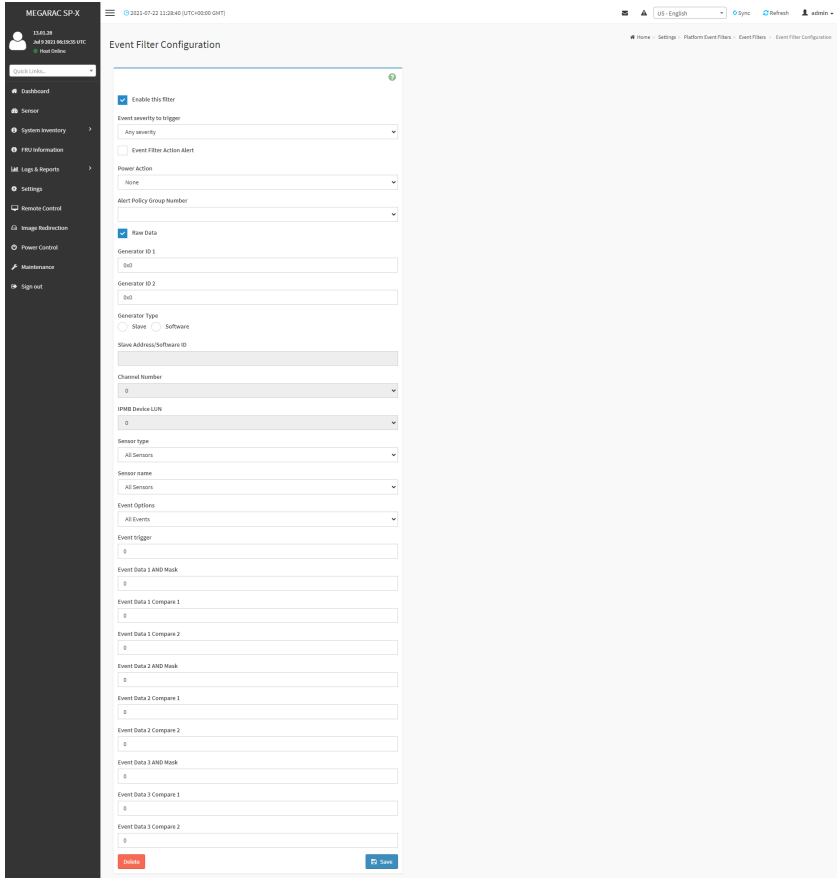
A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM' 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 in the 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 ID 2 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 is generated by IPMB.
- Select the **Sensor type** of sensor that will trigger the event filter action.
- In the **Sensor name** field, choose the particular sensor from the sensor list.
- Choose **Event Option** to be either All Events or Sensor Specific Events.
- **Event Trigger** field is used to give Event/Reading type value.



**Note:** Value ranges from 0 to 255.

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



**Note:** Value ranges from 0 to 255.

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



**Note:** Value ranges from 0 to 255.

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

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

# 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.

Group Number	Status	Action	Destination
Group 1	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 2	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 3	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 4	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 5	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 6	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 7	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 8	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 9	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 10	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 11	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 12	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 13	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 14	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 15	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 16	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 17	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 18	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 19	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 20	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 21	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 22	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 23	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 24	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 25	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 26	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 27	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 28	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 29	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 30	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 31	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 32	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 33	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 34	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 35	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 36	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 37	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 38	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 39	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0
Group 40	(Disabled)	Always send alert to this destination LAN Channel: 1	Sent To: 0

The fields in the Alert Policies page are explained below.

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

**Enable this alert:** Enables/Disables the policy settings.

**Policy Action:** Chooses 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:** Chooses a particular channel from the available channel list.

**Destination Selector:** Chooses 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:** Specifies an event-specific Alert String.

**Alert String Key:** Specifies which string is to be sent for this Alert Policy entry.

**Save:** Saves the Alert Policies entries.

**Delete:** Deletes 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.

The screenshot displays the 'Alert Policies' configuration interface. On the left is a dark sidebar with navigation options like 'Dashboard', 'Sensor', 'System Inventory', 'Firmware Information', 'Log & Reports', 'Settings', 'Remote Control', 'Image Redirection', 'Power Control', 'Maintenance', and 'Sign out'. The main content area shows a form for 'Alert Policies' with the following fields: 'Policy Group Number' (dropdown menu with '1' selected), 'Enable this alert' (checked checkbox), 'Policy Action' (dropdown menu with 'Always send alert to this destination' selected), 'LAN Channel' (dropdown menu with '1' selected), 'Destination Selector' (dropdown menu with '1' selected), 'Event Specific Alert String' (unchecked checkbox), and 'Alert String Key' (dropdown menu with '1' selected). At the bottom of the form are 'Delete' and 'Save' buttons. The top of the page shows the user 'admin' and navigation links for 'Home', 'Settings', 'Platform Event Filters', 'Alert Policies', and 'Alert Policies'.

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

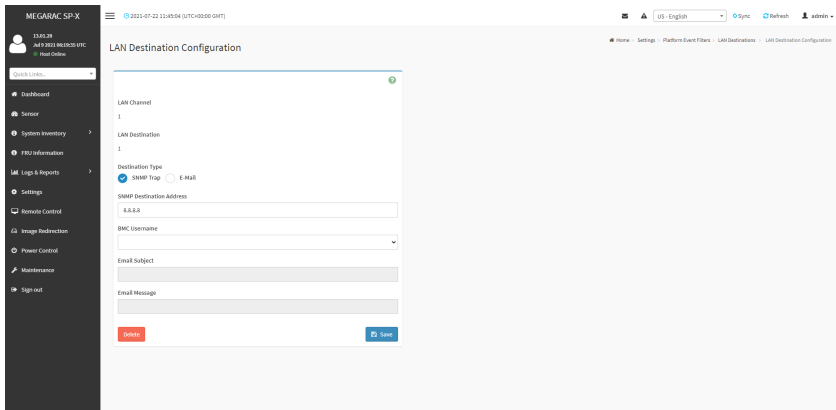
This page is used to configure the LAN destination of PEF configuration.

A sample screenshot of LAN Destination page is given below.

The screenshot displays the 'LAN Destinations' configuration page. On the left is a navigation sidebar with options like Dashboard, Sensor, System Inventory, FRU Information, Log & Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign out. The main content area shows a grid of 20 configuration slots. Each slot contains a dropdown menu for 'LAN Channel' and a 'Select the LAN Channel' dropdown. The first slot is selected, showing 'LAN Channel: 1' and 'LAN Destination: 1'. The other slots are empty, showing 'LAN Channel: 1' and 'LAN Destination: [number]'.

Select any empty slot to configure LAN Destinations.

The fields in the LAN Destination Configuration page are explained below.



**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. 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:** Email address for the user should be configured under **Settings > User Management**.

**Save:** Saves a new entry to the device.

**Delete:** Deletes the selected configured LAN Destination.

## Procedure

1. In the **LAN Destinations** page, 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.



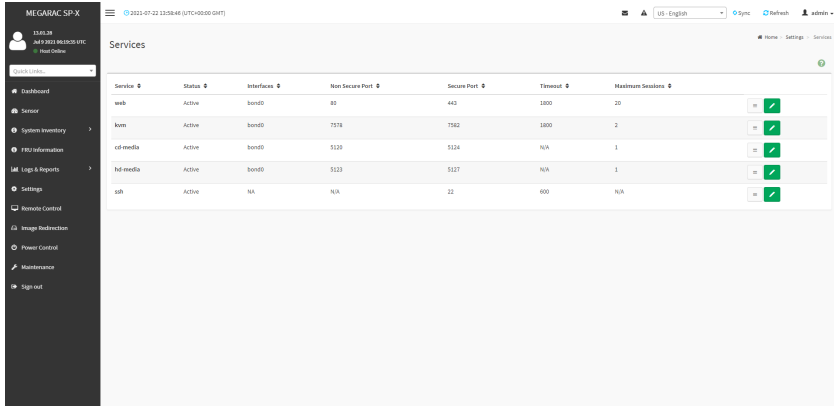
**Note:** Test alert can be sent only with enabled SMTP configuration. SMTP support can be enabled under **Settings > SMTP Settings**.



## 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.



Service	Status	Interfaces	Non Secure Port	Secure Port	Timeout	Maximum Sessions	
web	Active	bond0	80	443	1800	20	<input type="checkbox"/> <input checked="" type="checkbox"/>
kvm	Active	bond0	7578	7582	1800	2	<input type="checkbox"/> <input checked="" type="checkbox"/>
cd-media	Active	bond0	5120	5124	N/A	1	<input type="checkbox"/> <input checked="" type="checkbox"/>
hd-media	Active	bond0	5123	5127	N/A	1	<input type="checkbox"/> <input checked="" type="checkbox"/>
ssh	Active	NA	N/A	22	600	N/A	<input type="checkbox"/> <input checked="" type="checkbox"/>

The fields in the Services page are explained below.

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

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

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

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

- Web default port is 80.
- KVM default port is 7578.
- CD Media default port is 5120.
- HD Media default port is 5123.



**Note:** SSH service will not support non secure port. If single port feature is enabled, KVM, CD Media, and HD Media ports cannot be edited. Port value ranges from 1 to 65535.

**Secure Port:** This port is used to configure secure port number for the service.

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



**Note:** Telnet Port 80 is blocked for TCP/UDP protocols. 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)
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. Users 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.

Web timeout value can be ignored if there is any ongoing KVM session.

SSH timeout value ranges from 60 to 1800 seconds.

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

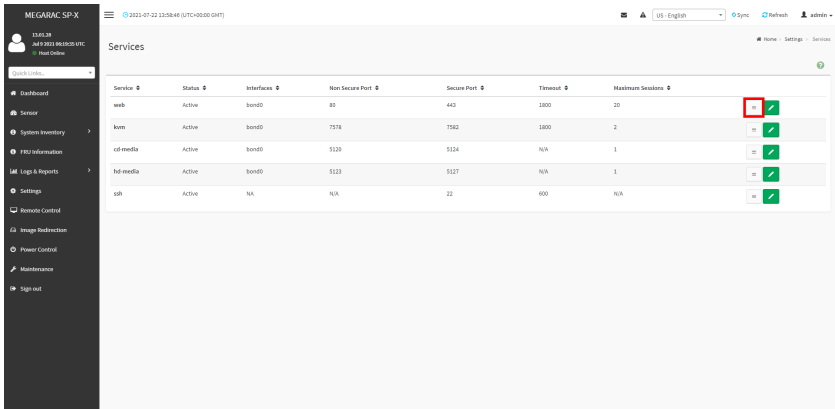
**Save:** Saves the configuration.

**Service Sessions**

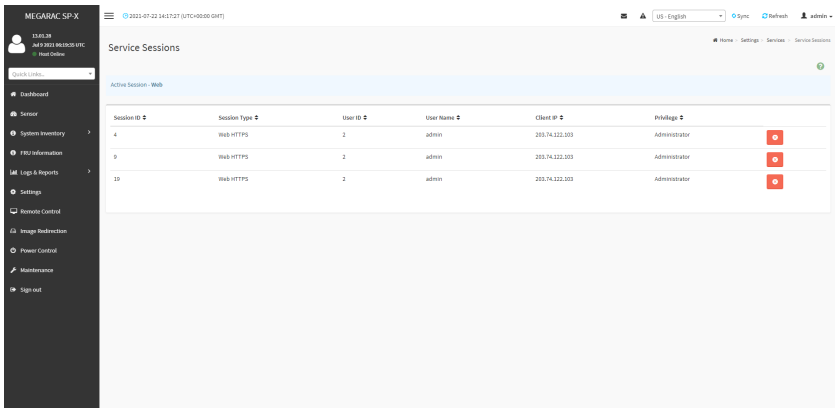
The Service Sessions page is used to view the current active sessions for the service.

## Procedure to open Service Sessions

1. Click the View icon to view the details about the active sessions for the service.



2. This opens the Service Session screen (for example - **Web** service sessions) as shown in the screenshot below.



**Session ID:** Displays the ID of the active sessions.

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

**User ID:** Displays the ID of the user.

**User Name:** Displays the name of the user.

**Client IP:** Displays the IP addresses that are already configured for the active sessions.

**Privilege:** Displays the access privilege of the user.

## 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.

The screenshot shows the MEGARAC SP-X console interface. The left sidebar contains navigation options: Dashboard, Sensor, System Inventory, FPD Information, Log & Reports, Settings, Remote Control, Image Redaction, Power Control, Maintenance, and Sign out. The main area displays a table of services. The 'web' service is highlighted with a red box, and its edit icon is also highlighted with a red box.

Service	Status	Interfaces	Non Secure Port	Secure Port	Timeout	Maximum Sessions
web	Active	bond0	80	443	1800	20
kvm	Active	bond0	7578	7582	1800	2
cd-media	Active	bond0	5120	5124	N/A	1
hd-media	Active	bond0	5123	5127	N/A	1
ssh	Active	N/A	N/A	22	600	N/A

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

The screenshot shows the MEGARAC SP-X console interface with the Service Configuration screen open for the 'web' service. The left sidebar is the same as in the previous screenshot. The main area shows the configuration fields for the selected service.

Service Name	web
<input checked="" type="checkbox"/> Active	
Interface Name	bond0
Non-secure port	80
Secure port	443
Timeout	1800
Maximum Sessions	20

3. The **Service Name** field is read-only.
4. Check the **Active** check box to activate the service.



**Note:** Interfaces, Non-secure port, Secure port, Time out and Maximum Sessions will not be active unless the current state is active.

5. Select an available interface in the **Interface Name** field.
6. Enter the Non-secure 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.

## 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 screenshot shows the 'SMTP Settings' configuration page in the BMC Web GUI. The interface includes a dark sidebar on the left with navigation links such as 'Dashboard', 'Sensor', 'System Inventory', 'FRU Information', 'Log & Reports', 'Settings', 'Remote Control', 'Image Reduction', 'Power Control', 'Maintenance', and 'Sign out'. The main content area is titled 'SMTP Settings' and contains the following fields and options:

- LAN Interface:** A dropdown menu showing 'bond0'.
- Sender Email ID:** An empty text input field.
- Primary SMTP Support:** A checked checkbox.
- Primary Server Name:** An empty text input field.
- Primary Server IP:** An empty text input field.
- Primary SMTP port:** A text input field containing '25'.
- Primary Secure SMTP port:** A text input field containing '455'.
- Primary SMTP Authentication:** An unchecked checkbox.
- Primary Username:** An empty text input field.
- Primary Password:** An empty text input field.
- Primary SMTP SSL/TLS Enable:** An unchecked checkbox.
- Primary SMTP STARTTLS Enable:** An unchecked checkbox.
- Secondary SMTP Support:** A checked checkbox.
- Secondary Server Name:** An empty text input field.
- Secondary Server IP:** An empty text input field.
- Secondary SMTP port:** A text input field containing '25'.
- Secondary Secure SMTP port:** A text input field containing '455'.
- Secondary SMTP Authentication:** A checked checkbox.
- Secondary Username:** An empty text input field.
- Secondary Password:** An empty text input field.
- Secondary SMTP SSL/TLS Enable:** An unchecked checkbox.
- Secondary SMTP STARTTLS Enable:** An unchecked checkbox.

A blue 'Save' button is located at the bottom right of the form.

The fields in the 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 SMTP Support:** Enables/Disables SMTP support for the BMC.

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



**Note:** Machine Name is a string of maximum 25 alpha-numeric characters. Space, special characters are not allowed.

**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 Port:** Specifies the SMTP Normal Port.



**Note:** Default Port is 25, and the Port value ranges from 1 to 65535.

**Primary Secure SMTP Port:** Specifies the SMTP Secure Port.



**Note:** Default Port is 25, and the Port value ranges from 1 to 65535.

**Primary SMTP Authentication:** Enables/Disables 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 SSLTLS Enable:** Enables SSLTLS support for the SMTP Client.

**Primary SMTP STARTTLS Enable:** Enables 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:** Saves 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 25 alpha-numeric characters. Spaces and special characters are not allowed.

5. Enter IP address of the SMTP Server in the **Primary Server IP** field. It is a mandatory field.
6. Enter the **Primary SMTP Port** in the specified field.
7. Enter the **Primary Secure SMTP Port** in the specified field.
8. Check to enable **Primary SMTP Authentication** if you want to authenticate SMTP Server.
9. Enter your **Primary Username** 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 **Secondary SMTP Secure Port** in the specified fields.
13. Check to enable **Secondary SMTP Server Authentication** if you want to authenticate SMTP Server.
14. Enter your **Secondary Username** and **Password** in the respective fields.
15. Check to enable **Secondary SMTP SSLTLS** to send data through secure Port.



**Note:** If this option is selected, STARTTLS option and Normal Port will be hidden.

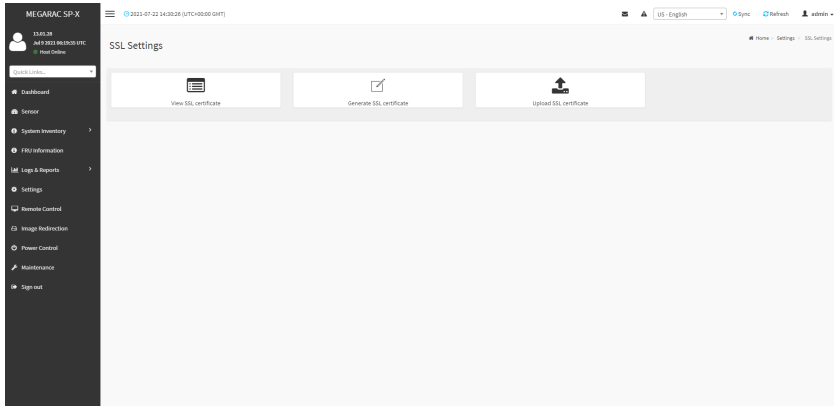
16. Click **Save** to save the entered details.

## 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.



The fields in the SSL Settings page are explained below.

**View SSL Certificate:** Displays the uploaded SSL certificate's information.

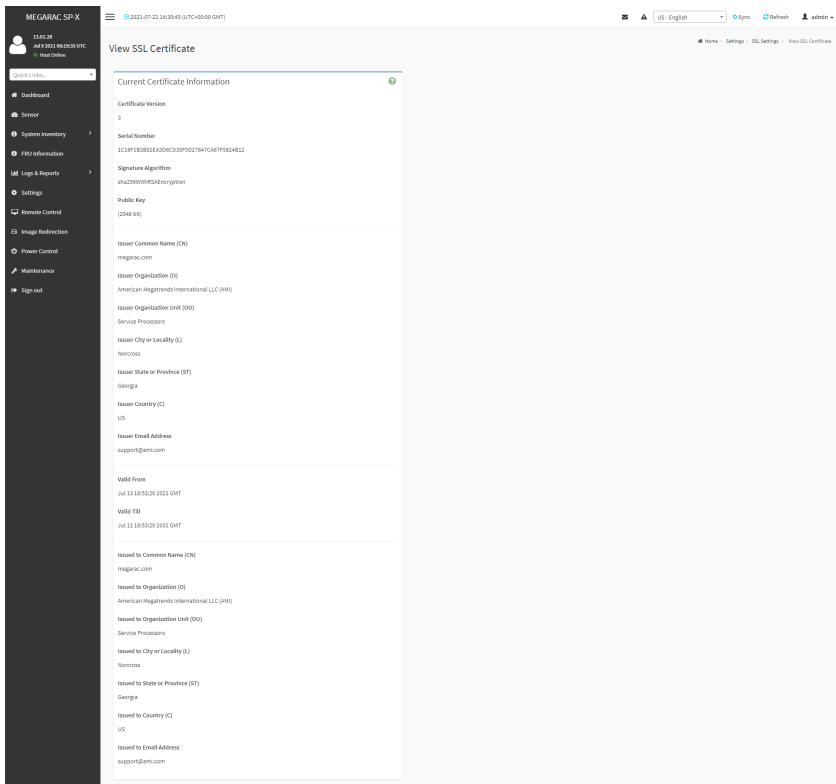
**Generate SSL Certificate:** Generates the SSL certificate based on configuration details.

**Upload SSL Certificate:** Uploads SSL certificate in readable format.



## View SSL Certificate

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



The fields in the View SSL Certificate page are explained below.

**Current Certificate Information:** This section displays the basic information about the uploaded SSL certificate. It displays the following fields:

- Certificate Version
- Serial Number
- Signature Algorithm
- Public Key
- Issuer Common Name (CN)
- Issuer Organization (O)
- Issuer Organization Unit (OU)
- Issuer City or Locality (L)
- Issuer State or Province (ST)
- Issuer Country (C)
- Issuer E-mail Address
- Valid From

- Valid Till
- Issued to Common Name (CN)
- Issued to Organization (O)
- Issued to Organization Unit (OU)
- Issued to City or Locality (L)
- Issued to State or Province (ST)
- Issued to Country (C)
- Issued to Email Address

## Generate SSL Certificate

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

The screenshot displays the 'Generate SSL Certificate' page in the MEGARMC SP-X console. The page features a dark sidebar on the left with navigation options like Dashboard, Settings, System Inventory, and more. The main content area contains a form with the following fields:

- Common Name (CN)
- Organization (O)
- Organization Unit (OU)
- City or Locality (L)
- State or Province (ST)
- Country (C)
- Email Address
- Valid For (in days)
- Key Length (2048 bits)

A 'Save' button is located at the bottom right of the form.

The fields in the Generate SSL Certificate page 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 128 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.

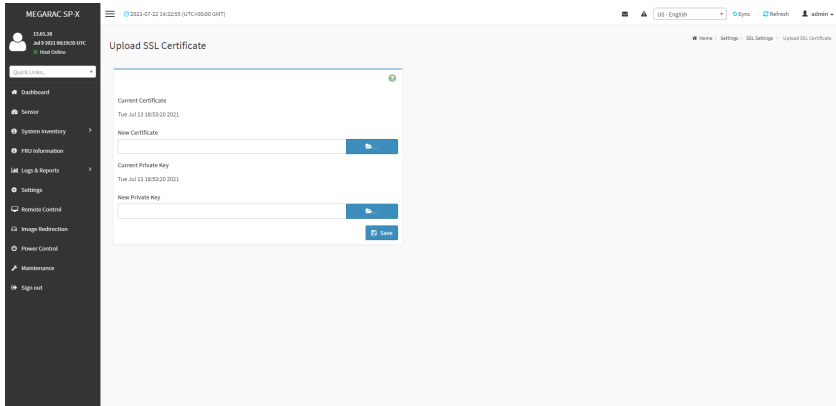
**Save:** Generates the new SSL certificate.



**Note:** HTTPs service will get restarted, to use the newly generated SSL certificate.

## Upload SSL Certificate

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



The fields in the Upload SSL Certificate page are explained below.

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

**New Certificate:** Browse the new certificate file. The certificate file should be of pem type.

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

**New Private Key:** Browse the new private key. The private key file should be of pem type.

**Save:** Uploads the SSL certificate and privacy key into the BMC.



**Note:** After successful upload, HTTPs service will restart to use the newly uploaded SSL certificate.

### Procedure

1. Click the Upload SSL Certificate tab, browse the New Certificate and New Private key.
2. Click **Save** 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:

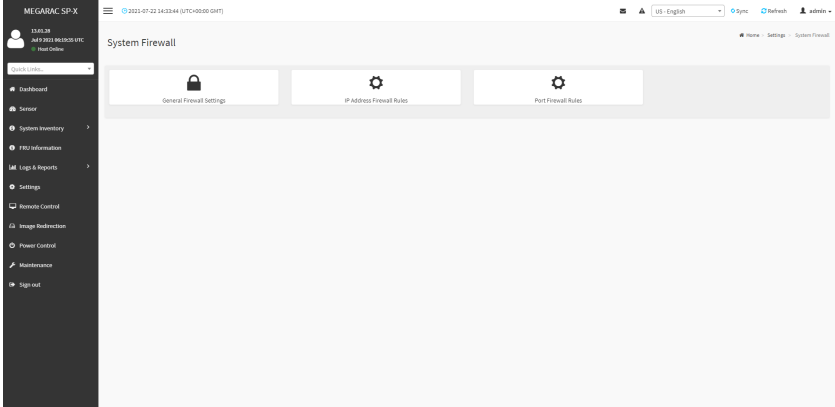
`https://192.168.030`

Please note the `<s>` after `<http>`. You must accept the certificate before you are able to access your Web.

## 2-6-14 System Firewall

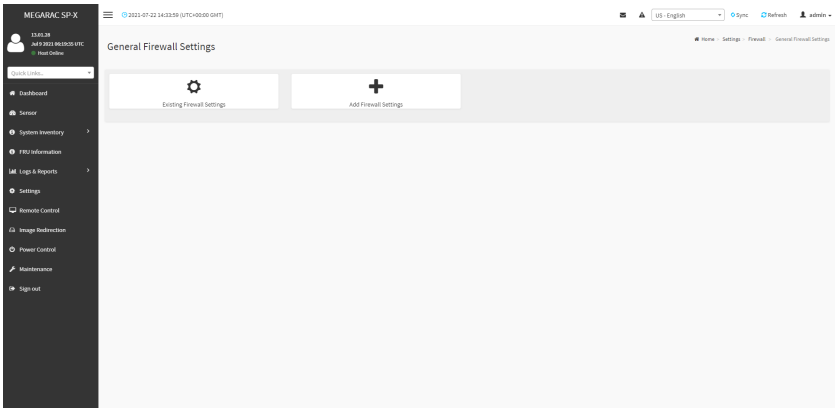
In BMC Web GUI, the System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.

To open System Firewall page, click **Settings > System Firewall** from the menu bar.



## General Firewall Settings

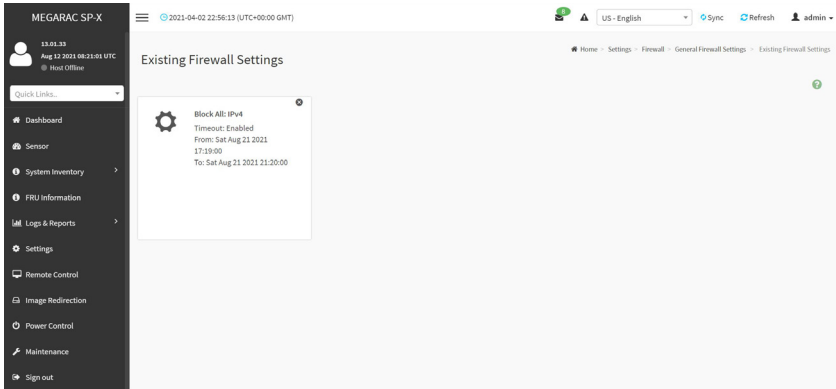
Click **General Firewall Settings** page. A sample screenshot of General Firewall Settings page is shown below.



The fields in the Firewall Settings page are explained below.

### Existing Firewall Settings

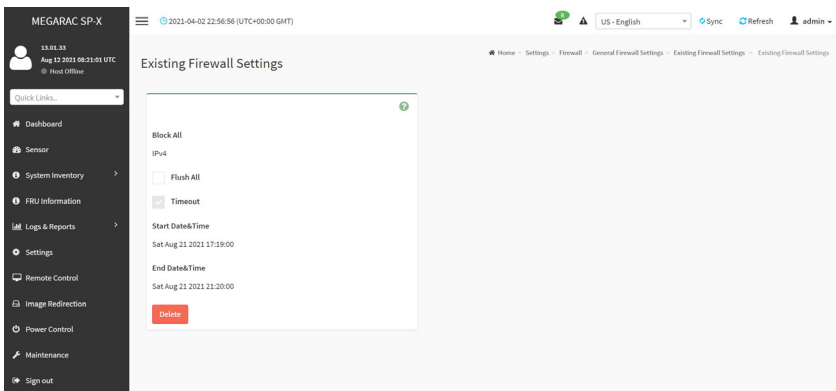
Click **General Firewall Settings > Existing Firewall Settings** icon. A blank page will be opened if you did not add anything in Add Firewall Settings. If any settings are added, then the added rule will be listed in Existing Firewall Settings page. A sample screenshot of Existing Firewall Settings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



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

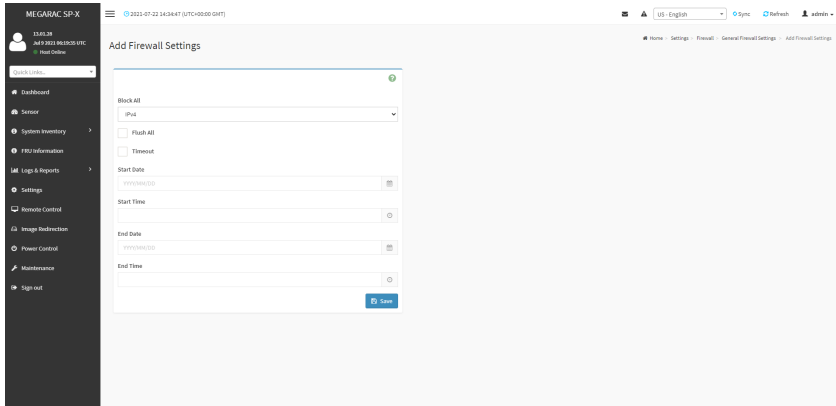
### Procedures

1. Select the Existing Firewall Settings you want to remove.
2. Click on **Delete** to remove the selected Existing Firewall Settings.



## Add Firewall Settings

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

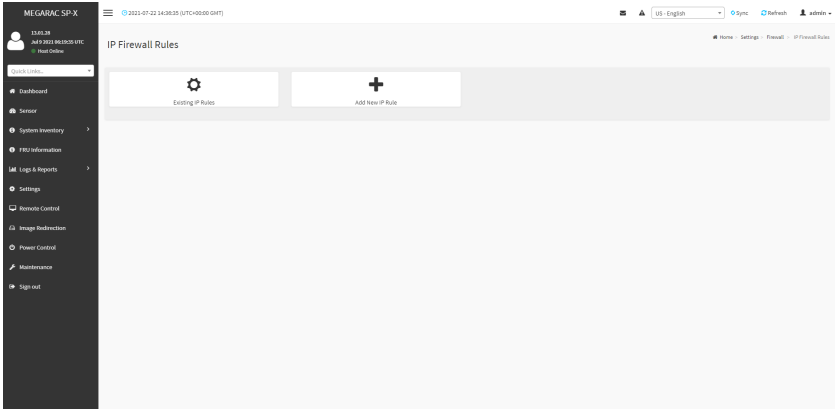


### Procedures

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 Date** to start the respective firewall rule effect from this date.
5. Enter **Start Time** to start the respective firewall rule effect from this time.
6. Enter **End Date** to end the respective firewall rule effect from this date.
7. Enter **End Time** to end the respective firewall rule effect from this time.
8. Click **Save** to save the changes made.

# IP Address Firewall Rules

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

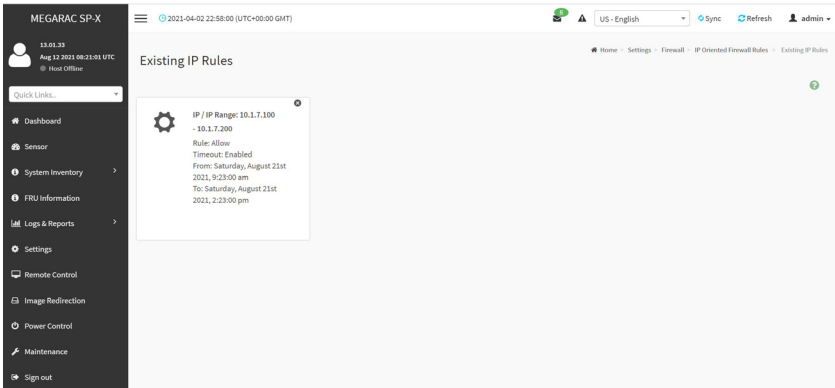


The fields in the IP Address Firewall page are explained below.

## Existing IP Rules

To view Existing IP Rules, 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.

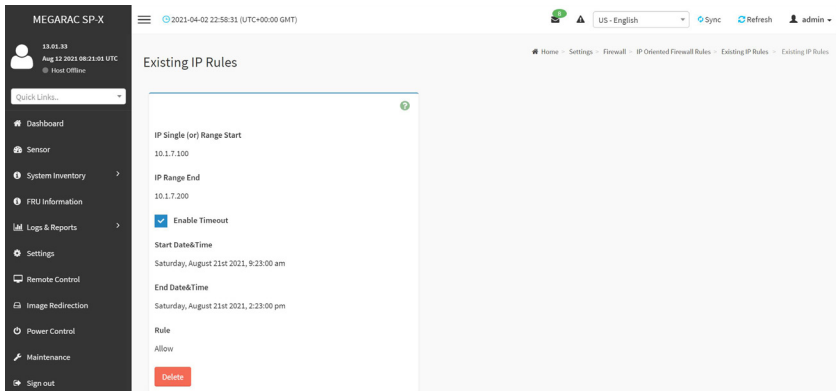


The Existing IP Rules page allows you to remove any particular Existing IP Rules.

## Procedure

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:** Shows the configured Port Address or Range of Ports.

**IP Range End:** Shows the configured Port Address or Range of Ports.

**Enable Timeout:** Enables/Disables 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.

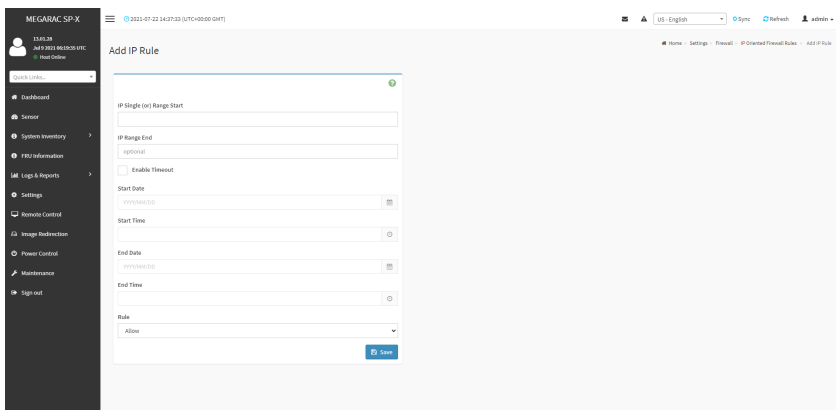
**Rule:** Indicates the current setting of the listed Port or Range of Port rules (Allow or Block) status.

**Delete:** Deletes the selected slot.

## Add IP Rule

To add a new IP rule, click **Settings > System Firewall > IP Address Firewall Rules > Add New IP Rule**. If any rule is added, then the added rule will be listed in Existing IP Rules page.

A sample screenshot of Add IP Rule page is shown below.



## Procedure

1. In the **Add IP Rule** 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 xxx.xxx.xxx.xxx.  
Each number ranges from 0 to 255.  
First number must not be 0.

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

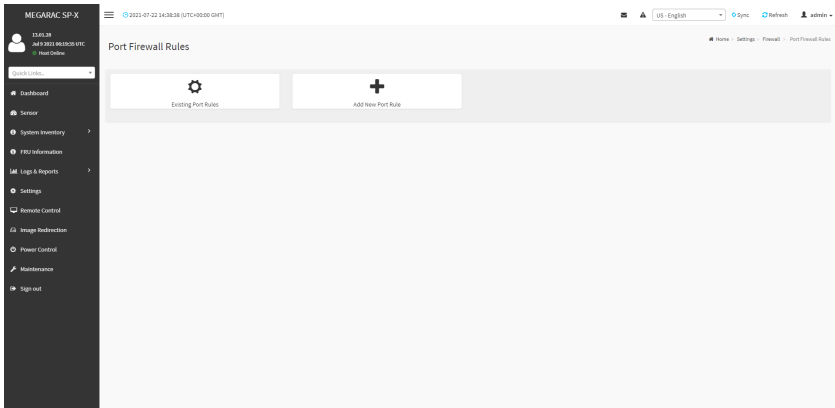


**Note:** The date and time should be in the YYYY/MM/DD and hh-mm format respectively.

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

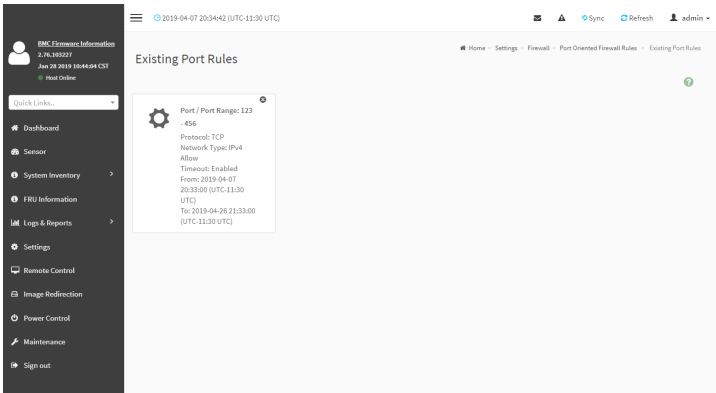
## Port Firewall Rules

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



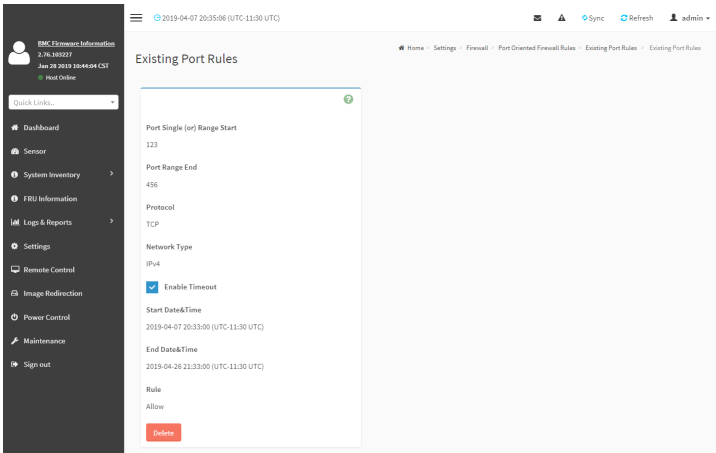
## Existing Port Rules

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.



## Procedure

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



The fields in the Existing Port Rules page are explained below.

**Port Single (or) Range Start:** Configures the Port or Range of Port Addresses.

**Port Range End:** Configures 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:** Enables/Disables 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:** Indicates Allow or Block status.

**Delete:** Deletes the entry to the firewall rules list.

## Add New Port Rule

To add a new port rule, click **Settings > System Firewall > Port Firewall Rules > Add New Port Rule**. A sample screenshot of Add New Port Rule is shown below.

The screenshot shows the 'Add Port Rule' configuration page. The left sidebar contains navigation options like Dashboard, Sensor, System Inventory, FRU Information, Logs & Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign out. The main content area has the following fields: 'Port Single (or) Range Start' (text input), 'Port Range End' (text input), 'Protocol' (dropdown menu with 'TCP' selected), 'Network Type' (dropdown menu with 'IPv4' selected), 'Enable Timeout' (checkbox, currently unchecked), 'Start Date' (calendar icon), 'Start Time' (clock icon), 'End Date' (calendar icon), 'End Time' (clock icon), and 'Rule' (dropdown menu with 'Allow' selected). A blue 'Save' button is located at the bottom right of the form.

## Procedure

1. In the **Port Single (or) Range Start** field, enter the port number or a range of port addresses.



**Note:** Port value ranges from 1 to 65535.  
Port 80 is blocked for TCP/UDP protocols.

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



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

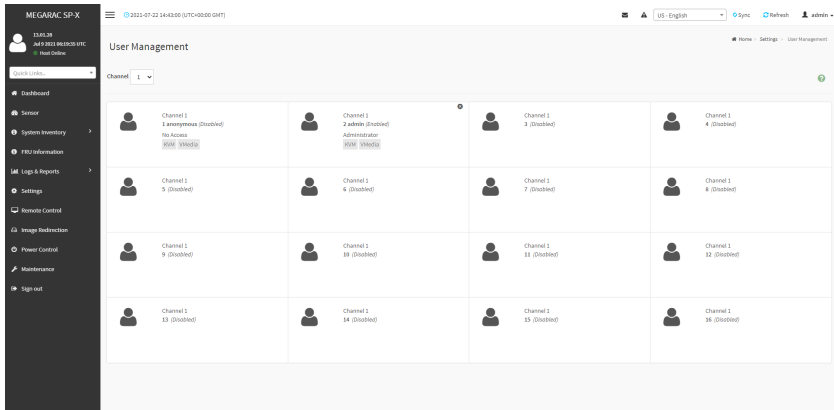
10. Select either **Block** or **Allow** in the **Rule** field.

11. 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.



The fields in the User Management page are explained below.



**Note:** The free slots are shown as “Disabled” in all columns for the slot.

**User ID:** Displays the ID number of the user.



**Note:** The list contains a maximum of ten users only.

**User Name:** Displays the name of the user.

**User Access:** Enables/Disables the access privilege of the user.

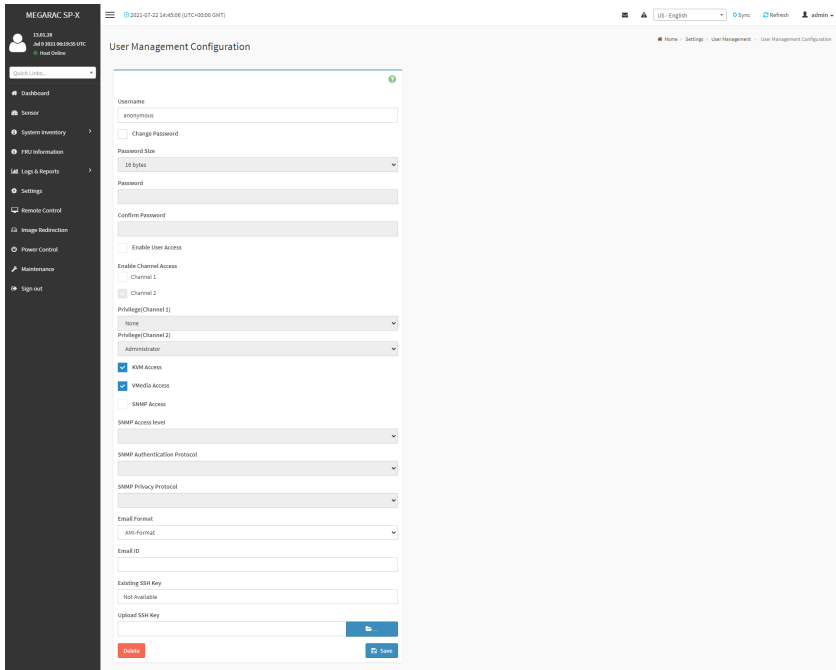
**Network Privilege:** Displays the network access privilege of the user.

**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:** Adds a new user.

**Delete User:** Deletes an existing user.



## Procedure

1. To add a new user, select an empty slot on the User Management page. The User Management Configuration screen will appear,
2. Enter user name in the **Username** field.



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

3. Check **Change Password** if you want to change the password.
4. Set **Password Size** for the new password.
5. In the **Password** and **Confirm Password** fields, enter and confirm the 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 tab)
0A	LF '\n' (new Line)
0B	VT '\v' (vertical tab)
0C	FF '\f' (form feed)
0D	CR '\r' (carriage ret)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)
11	DC1 (device control 1)
12	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

6. Enable or disable the **Enable User Access**.
7. Enable or disable the **Enable Channel Access**.



**Note:** Enabling channel access will assign the IPMI messaging privilege to user. It is recommended that the IPMI messaging option should be enabled as well if user is created through IPMI.

8. In the **Privilege (Channel 1)** and **Privilege (Channel 2)** fields, select a privilege level.
9. Check **KVM Access** to assign the KVM privilege.
10. Check **VMedia Access** assign the VMedia privilege.



**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.

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



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

12. 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.
13. 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.

14. Choose the Encryption algorithm to use for SNMP settings from the **SNMP Privacy Protocol** drop-down list.
15. 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.



16. The **Existing SSH Key** field displays information of an existing SSH key.

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



**Note:** SSH key file should be of pub type.

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

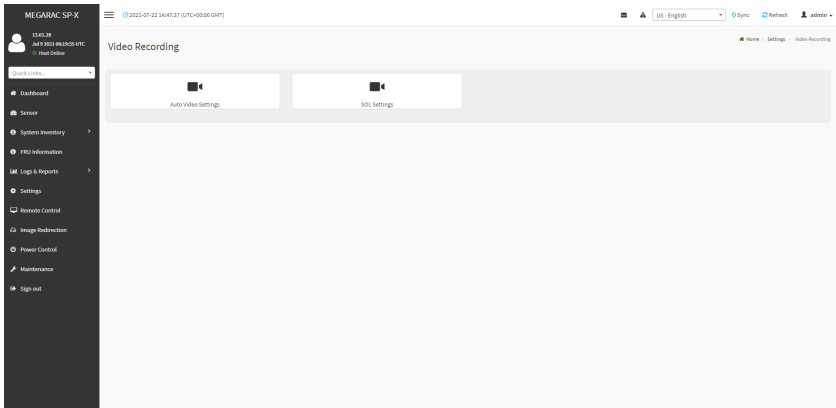
If you need to modify the privilege or information of an existing user, select the user on the User Management page to open the User Management Configuration screen and modify the configurations accordingly.

## 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

A sample screenshot of the Video Recording is given below.

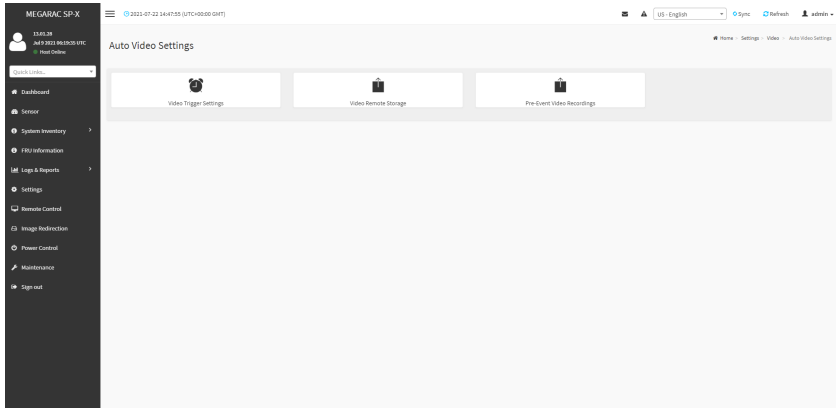


A detailed description of the menu items are given below.

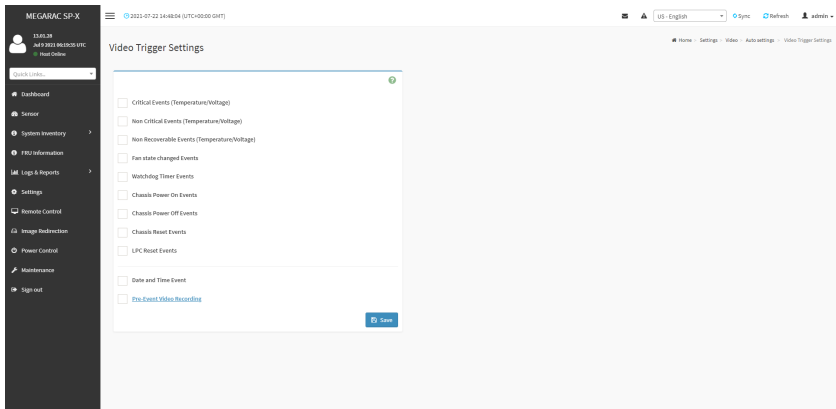
## Auto Video Settings

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

**Save:** Saves 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 **Time** field.



**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.

The screenshot displays the 'Pre-Event Video Recordings' configuration page. The left sidebar contains a navigation menu with items like 'Dashboard', 'Sensor', 'System Inventory', 'FRU Information', 'Logs & Reports', 'Settings', 'Remote Control', 'Image Redaction', 'Power Control', and 'Maintenance'. The main content area has a title 'Pre-Event Video Recordings' and a message: 'This page is used to configure the Pre-Event video recording options. Pre-Event video recording is disabled by default. To enable the Pre-Event video recording, go to the Triggers Configuration page.' Below this is a 'Note' box: 'Disable/Enable pre-event recording selection for newly modified configuration to take effect.' There are four dropdown menus: 'Video Quality' (set to 'Very Low'), 'Compression Mode' (set to 'High'), 'Frames Per Second' (set to '1'), and 'Video Duration' (set to '10'). A 'Save' button is at the bottom right of the form.

- a) To set video quality, select a resolution (Very Low, Low, Average, Normal, High) from the drop-down list of **Video Quality**.

- b) To set compression mode, select a compression mode (high, normal, low, no) from the drop-down list of **Compression Mode**.
- c) To set number of frames per second, select frames/sec (1-4) from the drop-down list of **Frames Per Second**.
- d) To set duration of video, select second (10-60) from the drop-down list of **Video Duration**.
- e) Click **Save** to save the changes made on Pre-Event Video Recording.

4. Click **Save** to save the changes made on Video Trigger Settings.

## Video Remote Storage

To configure Video Remote Storage, click **Video Recording > Auto Video Settings > Video Remote Storage**. A Sample screenshot of Video Remote Storage is as shown below.

## Procedure

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, the video files will be stored only in remote path, not within BMC.

2. Enter Dumps value of the video in the **Maximum Dumps** field.
3. Enter maximum duration of the video in the **Maximum Duration (Sec)** field.
4. Enter maximum size of the video in the **Maximum Size (MB)** field.



**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 in the **Server Address** field.



**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 domain name, user name, and password in the **Domain Name, Username, Password** field respectively.
8. Click **Save** to save the settings.

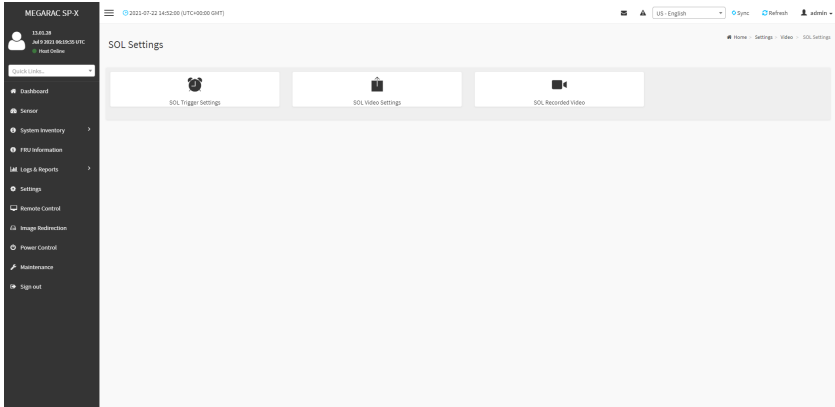
### Pre-Event Video Recording

Pre-Event Video Recordings is used to configure the Pre-Event video recording options. Pre-Event video is disabled by default. To enable the Pre-Event video recording, go to **Settings > Video Recording > Auto Video Settings > Video Trigger Settings**.

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**.

## 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.



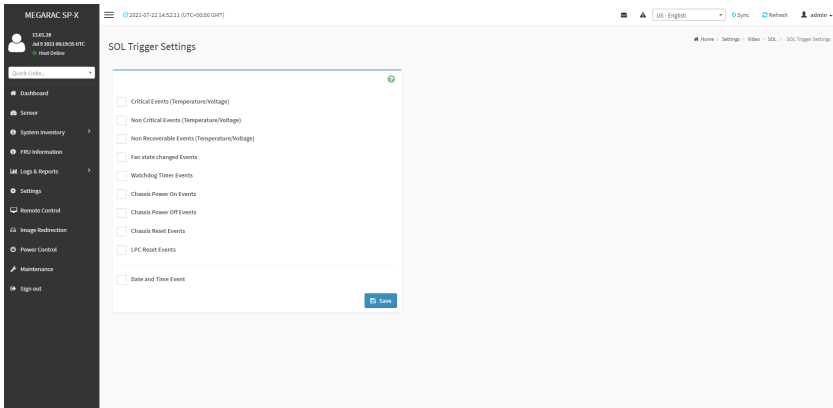
The fields in the SOL Settings page are explained below.

### SOL Trigger Settings

The SOL Trigger Settings page shows the list of available events.

- 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

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 in the **Date** field.
  - b) Enter the **Time** in hh:mm:ss format in the **Time** field.

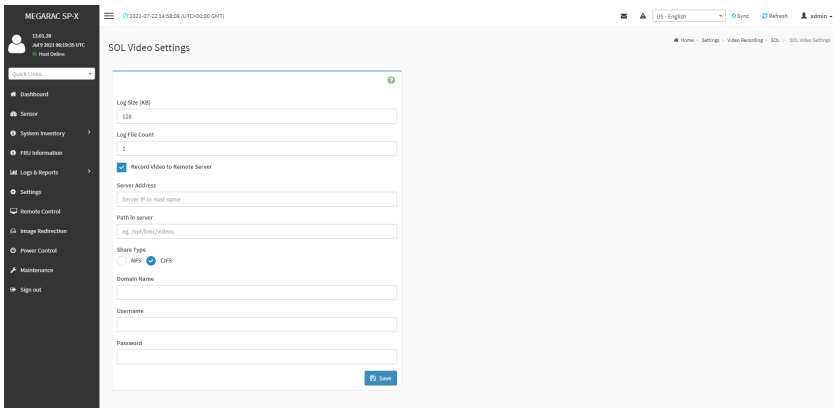


**Note:** The date and time should be in advance to the system date and time.

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

## SOL Video Settings

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



## Procedure

1. Enter the preferred log size in the **Log Size (KB)** field. The maximum log size supported is 128 KB.
2. Enter log file count in the **Log File Count** field. The maximum log file count is 1.
3. Check/uncheck **Record Video to Remote Server** to enable/disable Remote Video support.



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

4. Enter server address in the **Server Address** field.



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

5. Enter the source path in **Path in Server** field.



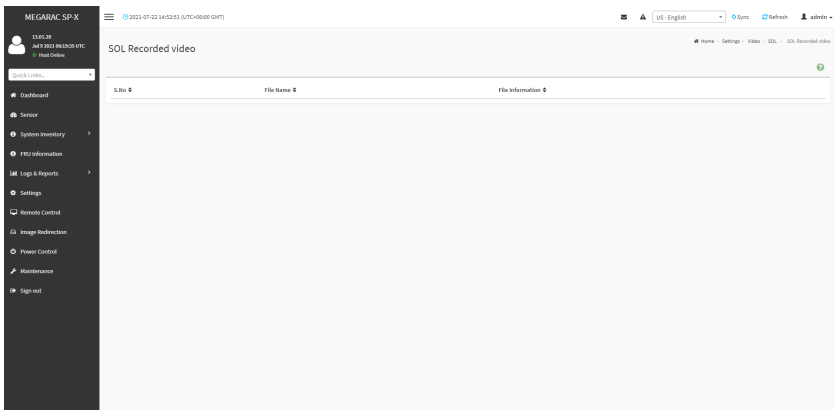
**Note:** Path must be alpha-numeric and the special characters '-'(hyphen), '\_'(underscore), '@'(at sign) are allowed.

6. Select the **Share Type** (NFS/CIFS). If the selected share type is (CIFS), enter the domain name, user name, and password in the **Domain Name**, **Username**, **Password** field respectively.
7. Click **Save** to save the settings.

## 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.

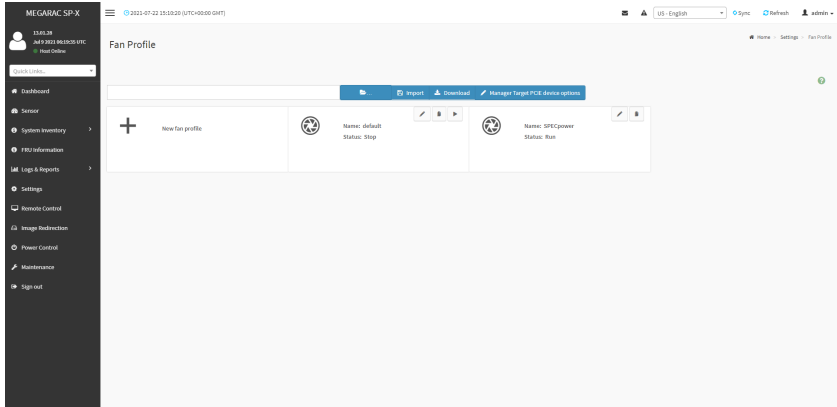
A sample screenshot of **SOL Recorded Video** is given below.





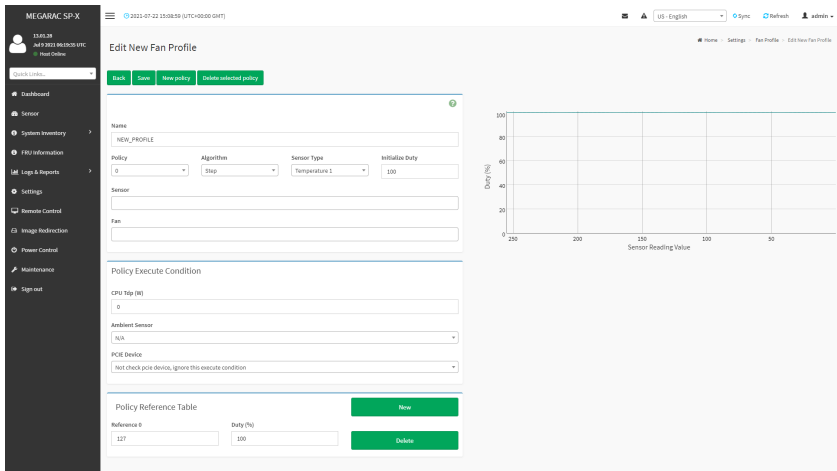
## 2-6-17 Fan Profile

The Fan Profile page allows you to add new fan profile or edit fan profile. A sample screenshot of the Fan Profile is given below.



## New Fan Profile

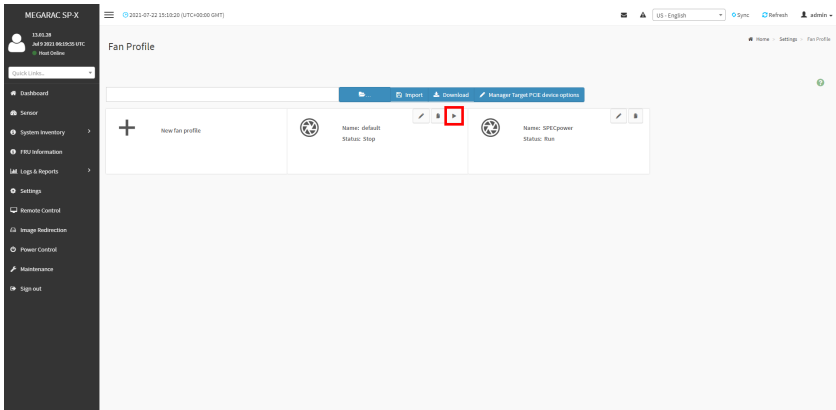
To add new fan profile, click the **New fan profile** tab.



## Procedure

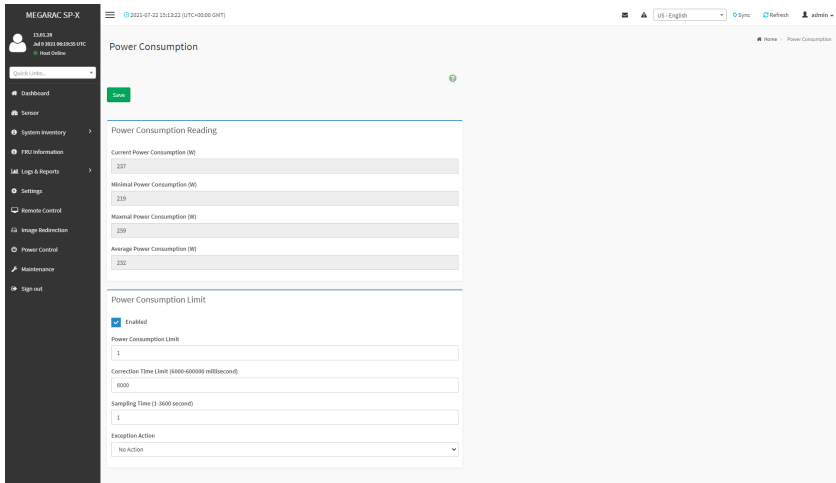
1. Name the fan profile in the **Name** field.
2. Choose the mapping function of temperature and fan speed for the fan profile in the **Algorithm** field.
3. Select sensory type in the **Sensor Type** field.

4. Set the fan speed when the system is powering on in the **Initialize Duty** field.
5. Select the sensor you want to include in this profile in the **Sensor** field.
6. Select the fan you want to include in this profile in the **Fan** field.
7. Click **New** in the **Policy Reference Table** field to create a new sensor value & fan speed duty mapping table.
8. Set reference temperature and fan speed duty in the **Policy Reference Table** field.
9. Click **Save** on the top side to save the configuration.
10. Click the arrow icon to run the fan profile.



## 2-6-18 Power Consumption

Items in **Power Consumption Reading** displays current power consumption reading. You are allowed to configure power limit in the **Power Consumption Limit** field.



The screenshot displays the MEGARMC SP-X interface for configuring power consumption. The left sidebar contains navigation options: Dashboard, Sensor, System Inventory, FPD Information, Log & Reports, Settings, Remote Control, Image Redirection, Power Control, Maintenance, and Sign-out. The main content area is titled 'Power Consumption' and includes a 'Sync' button. Below this, the 'Power Consumption Reading' section shows a table with the following data:

Reading Type	Value (W)
Current Power Consumption	237
Min/Max Power Consumption	219
Normal Power Consumption	259
Average Power Consumption	232

The 'Power Consumption Limit' section is currently enabled. The configuration fields are as follows:

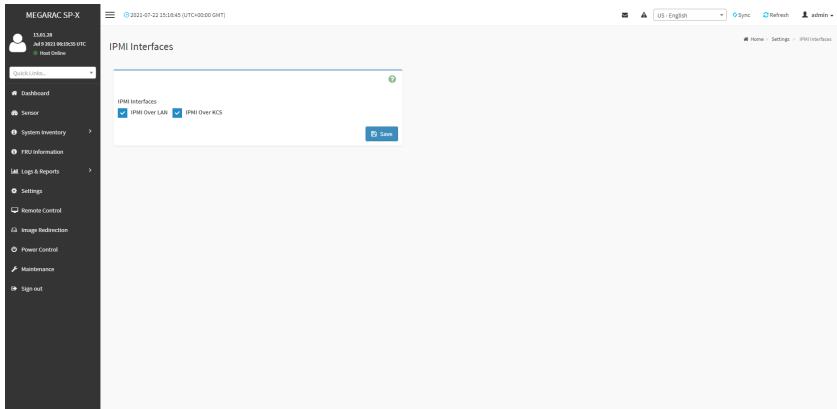
- Power Consumption Limit:** 1
- Correction Time Limit (6000-600000 millisecond):** 6000
- Sampling Time (1-3600 second):** 1
- Exception Action:** No Action

### Procedure

1. Check **Enabled** to enable Power Consumption Limit.
2. Set **Power Consumption Limit**.
3. Set **Correction Time Limit (6000-600000 millisecond)**.
4. Set **Sampling Time**.
5. Set **Exception Action** (No Action, Hard Power Off system and log event to SEL, Log event to SEL only).

## 2-6-19 IMPI Interfaces

You are allowed to configure the IPMI interfaces in this page.



### Procedure

1. Check **IPMI Over LAN** to enable IPMI over LAN.
2. Check **IPMI Over KCS** to enable IPMI over KCS.
3. Click **Save** to save the configuration.

## 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.

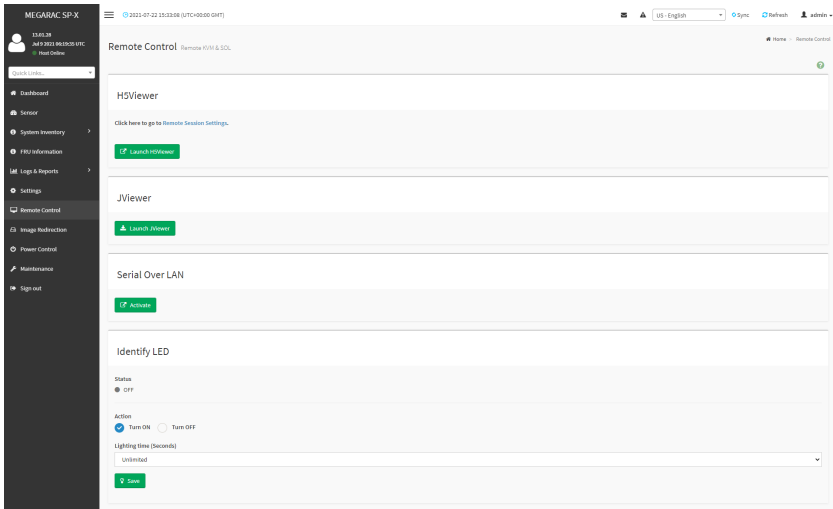
### Supported Browsers

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



The fields in the Remote Control page are explained below.

**H5Viewer:** Launches the KVM.

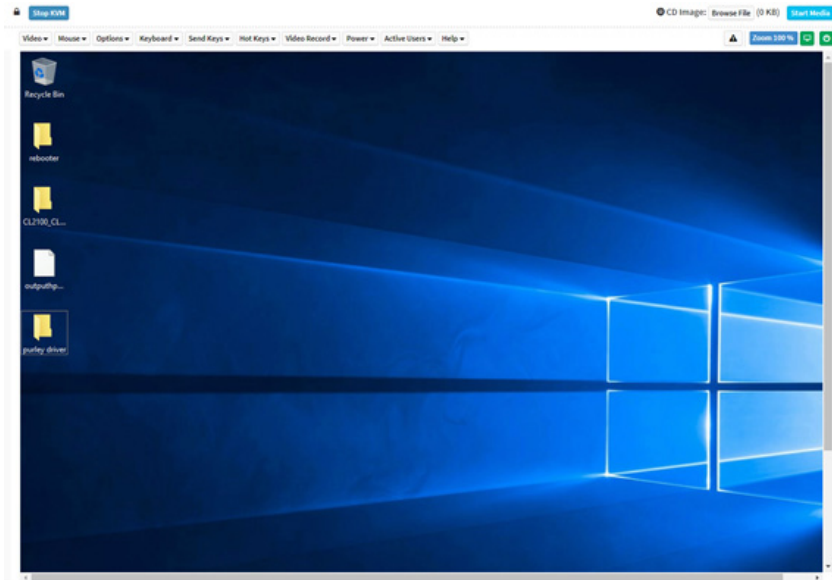
**JViewer:** Downloads the jviewer file.

**Serial Over LAN:** Launches the HTML5 Serial Over LAN window.

**Identify LED:** Turns on/off the chassis identification LED.

## H5Viewer

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



**Stop KVM:** Stops the H5Viewer.

**Video:** Consists of the following items:

- **Pause Video:** Pauses Console Redirection.
- **Resume Video:** Resumes the Console Redirection when the session is paused.
- **Refresh Video:** Updates the display shown in the Console Redirection window.

**Mouse:** Contains the following items:

- **Show Client Cursor:** Shows or hides the local mouse cursor on the remote client system.
- **Mouse Mode:** 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.
- **Other mouse mode:** Sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.



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

## Options

**Zoom In / Zoom Out:** Allows you to adjust zoom level.

**Partial Permission / No Permission:** Enables/Disables the access privilege of the user.

**Auto Detect / 256 Kbps / 512 Kbps / 1 Mbps / 10 Mbps / 100 Mbps:** Adjusts the bandwidth.

**YUV 420 / YUV 444 / YUV 444 + 2 color VQ / YUV 444 + 4 color VQ:** Adjusts the color encoding mode.

**0 Best Quality - 7:** Allows you to adjust the screen resolution.

**Keyboard:** lists the host physical keyboard languages supported in H5Viewer.

- English U.S
- German
- Japanese

**Send Keys:** Enters items.

This menu contains the following sub menu items:

- **Hold Down**
- **Press and Release**

**Hold Down:** Contains the following items:

- **Right Ctrl Key:** Acts as the right-side <CTRL> key when in Console Redirection.
- **Right Alt Key:** Acts as the right-side <ALT> key when in Console Redirection.
- **Right Windows Key:** Acts as the right-side <WIN> key when in Console Redirection.
- **Left Ctrl Key:** Acts as the left-side <CTRL> key when in Console Redirection.
- **Left Alt Key:** Acts as the left-side <ALT> key when in Console Redirection.
- **Left Windows Key:** Acts 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:** Acts as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that you are redirecting.
- **Left Windows Key:** Acts 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:** Acts as the right-side <WIN> key when in Console Redirection.
- **Context Menu Key:** Acts as the context menu key, when in Console Redirection.
- **Print Screen Key:** Acts as the print screen key, when in Console Redirection.

**Hot Keys:** Adds the user configurable shortcut keys to invoke in the host machine.

The configured key events are saved in the BMC.

- **Add Hot Keys:** Enables **User Defined Macros**. Click **Add** to add a User Defined Macro.

**Video Record:** Contains the following items:

- **Record Video:** Starts recording the screen.
- **Stop Recording:** Stops the recording.
- **Record Settings:** Sets 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.

**Power:** Performs any power cycle operation.

- **Reset Server:** Reboots the system without powering off (warm boot).
- **Immediate Shutdown:** Turns off the server immediately.
- **Orderly Shutdown:** Turns off the server in proper order.
- **Power ON Server:** Powers on the server.
- **Power Cycle Server:** Performs server power control operation.

**Active Users:** Displays 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:** Displays information about H5Viewer.

**Browse File:** Selects 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.

**Zoom 100%:** Displays the zoom level.

### Host Display

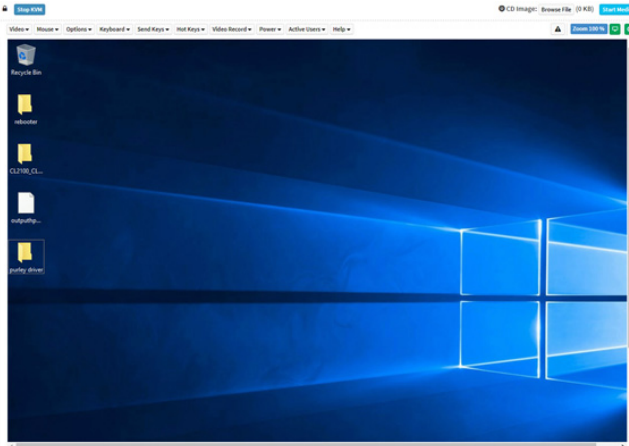
- **Display on:** If you disable this option, the display will be shown on the screen in Console Redirection
- **Display off:** If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back in the server screen.
- **Capture Screen:** Takes the screenshot of the host screen and save it in the client's system.

**Power ON/OFF:** Power ON/OFF the server.

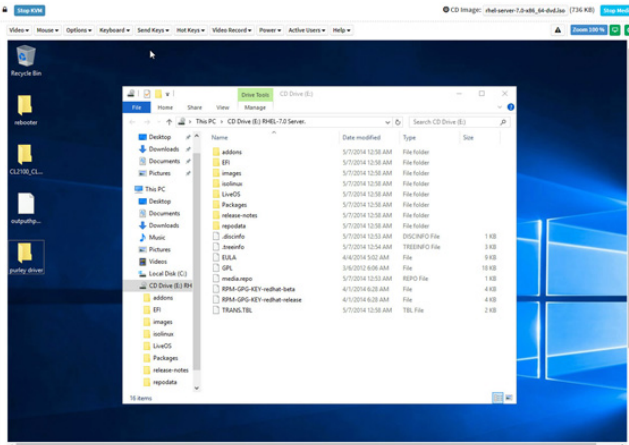


## Procedure

1. Click **Launch H5Viewer** to start video redirection.



2. Click **Browse File** 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**.

## JViewer

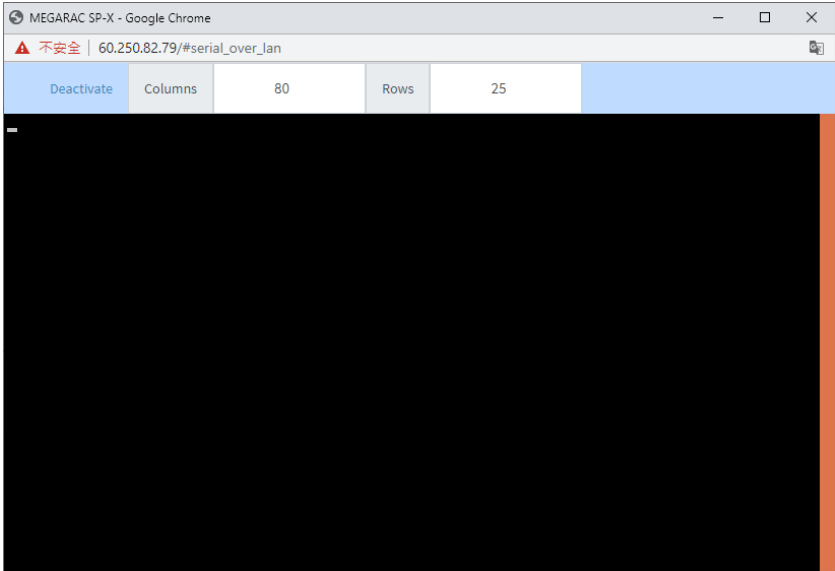
JViewer allows you to download the jviewer file. Click **Launch JViewer** to download the jviewer file.



**Note:** The jviewer file is used for launching Java executable files over the web or network.

## Serial Over LAN

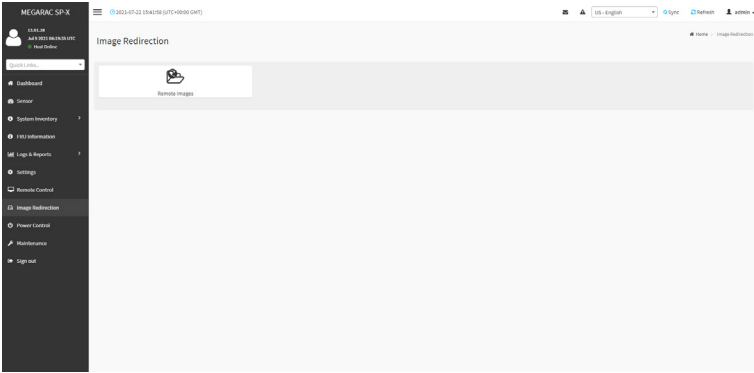
Serial Over LAN can launch the HTML5 Serial Over LAN window. Click **Activate** to launch the HTML5 Serial Over LAN window. A sample screenshot of the HTML5 Serial Over LAN window is shown below.



## 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 or by mounting the image from the remote system.

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



The fields in the Image Redirection page are explained below.

**Remote Images:** Allows you to configure images of remote media servers.



**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 Remote Media tab displays the configured images of remote media server on BMC.

Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index
CD/DVD	0	R272P30.iso	-	0
CD/DVD	1	R272P30.iso	-	N/A
CD/DVD	2	R272P30.iso	-	N/A
CD/DVD	3	R272P30.iso	-	N/A
Hard disk	0	-	-	N/A
Hard disk	1	-	-	N/A
Hard disk	2	-	-	N/A
Hard disk	3	-	-	N/A



**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 in the Remote Media page are explained below:

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

**Media Instance:** Displays total media instance count.

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

**Redirection Status:** Displays the status of the media.

**Connected Server Session Index:** Displays Media Server Session Index.

**Start/Stop Redirection:** Starts/stops the image redirection.

**Pause:** Pauses the image redirection.

**Refresh Image List:** Gets the latest image list from the remote storage.

**Sync Image Status:** Synchronizes the image status.

### 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.

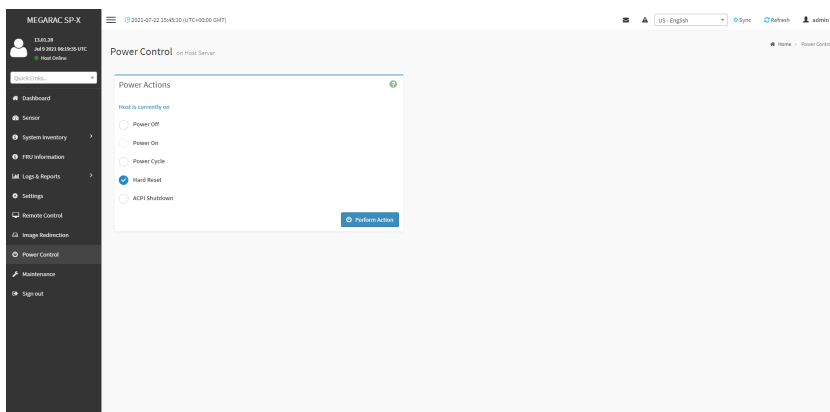


**Note:** Redirection needs to be stopped to clear the image.

## 2-9 Power Control

The Power Control page allows you to view and control the power of your server.

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



The setting options of Power Control are explained below.

**Power Off:** Powers off the server immediately.

**Power On:** Powers 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:** Initiates operating system shutdown prior to the shutdown.

**Perform Action:** Performs 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.

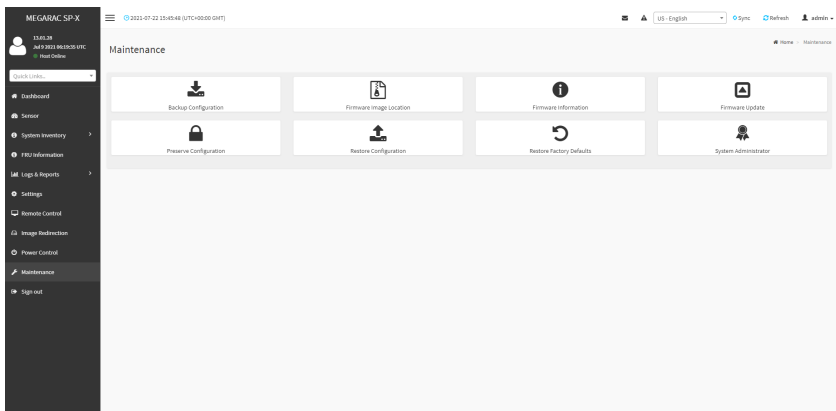
## 2-10 Maintenance Group

The Maintenance Group page allows you to do maintenance tasks on the device. To open the Maintenance Group page, click **Maintenance Group** from the menu bar.

Maintenance Group contains the following items:

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

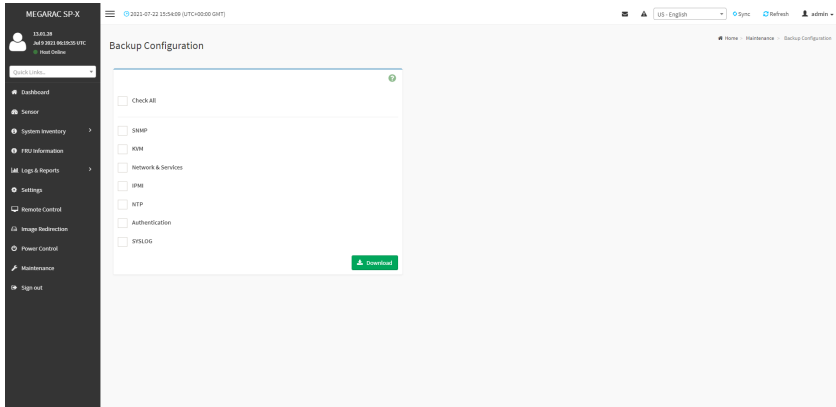
A sample screenshot of Maintenance Group is shown below.



## 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 the Backup Configuration page, click **Maintenance > Backup Configuration** from the menu bar. A sample screenshot of Backup Configuration page is shown below.



The fields in the Backup Configuration page are explained below.

**Check All:** Selects all setting options.

**Download:** Downloads and saves the configuration files backup from BMC to client system.

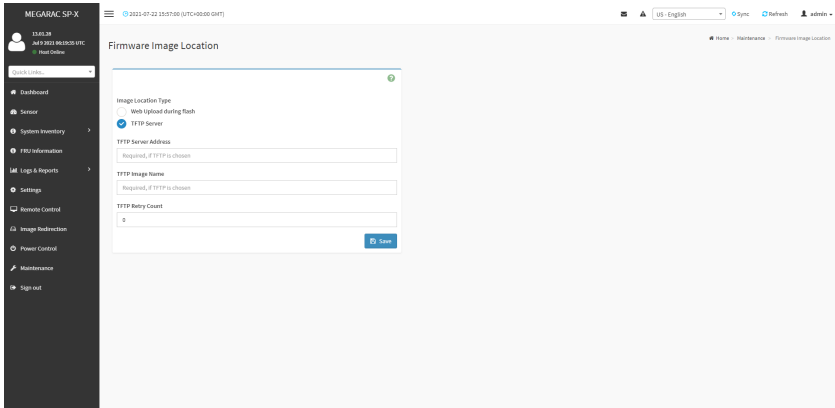
### Procedure

1. Click **Check All** to back up all setting option or check individual setting option to back up the selected items.
2. Click **Download** to save the backup file to the client system.

## 2-10-2 Firmware Image Location

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


To open the **Firmware Image Location** page, click **Maintenance > Firmware Image Location** from the menu bar. A sample screenshot of Firmware Image Location page is shown below.



The fields in the Firmware Image Location page are explained 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:** Saves the configured settings.

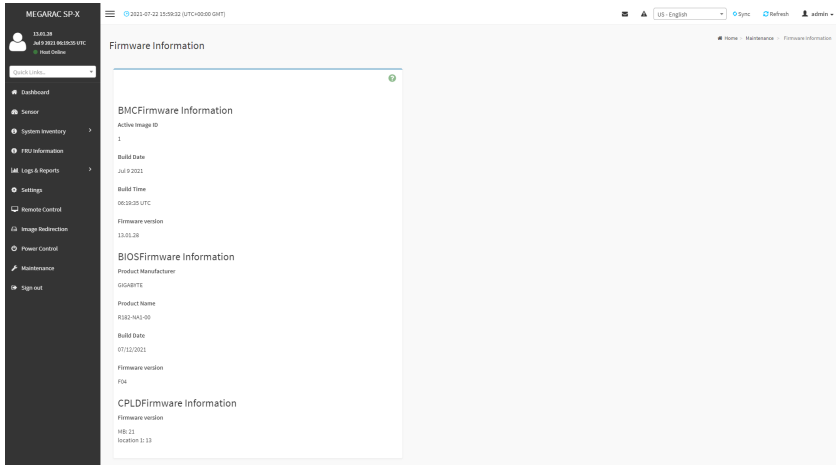
### Procedure

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 Information

To open the Firmware Information page, click **Maintenance > Firmware Information** from the menu bar. A sample screenshot of the Firmware Information page is shown below.



The fields in the Firmware Information page explained below.

### **BMC Firmware Information**

**Active Image ID:** Displays the active image ID.

**Build Date:** Displays the build date of the active BMC image.

**Build Time:** Displays the build time of the active BMC image.

**Firmware version:** Displays the firmware version of the active BMC image.

### **BIOS Firmware Information**

**Product Manufacturer:** Displays the hardware manufacturer.

**Product Name:** Displays the model name of the device.

**Build Date:** Displays the build date of the device.

**Firmware version:** Displays the BIOS version installed on the device.

### **CPLD Firmware Information**

**Firmware version:** Displays the CPLD Firmware version.

## 2-10-4 Firmware Update

To open the Firmware Update page, click **Maintenance > Firmware Update** from the menu bar. The update wizard will take you through the update process. 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 already configured settings through the upgrade.



**Warning:** Please note that after entering the update mode wizard, other web pages and services will not work. All open widgets will be closed automatically. If the 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 connectivity 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.

A sample screenshot of Firmware Update page is shown below.

The screenshot displays the MEGARAC SP-X Firmware Update interface. On the left is a dark sidebar menu with navigation options. The main content area features a 'Firmware Update' title, a 'Dump BIOS' button, a 'Note' section detailing supported update methods, a 'Select Firmware Image' dropdown menu, and a 'Start firmware update' button. A warning message is visible at the bottom of the update section.

The fields in the Firmware Update page explained below.

**Dump BIOS:** Click to dump the current BIOS image.

**Select Firmware Image:** Selects the firmware image to be uploaded.

**Start firmware update:** Starts the firmware update.

## Procedure

1. Click **Select Firmware Image** to select the firmware image to be uploaded.
2. Click **Start firmware update** to proceed.
3. Click **Preserve all Configuration** if you want to preserve all configuration settings during the firmware update and then click **Proceed to Flash** at the bottom to proceed.

Sign out

Protocol Type: HTTPS

Update Type: BMC

Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

All configuration items below will be preserved as default during the restore configuration operation. Click "Edit Preserve Configuration" to modify the Preserve status settings.

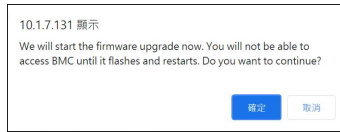
[Edit Preserve Configuration](#)

S.No	Preserve Configuration Item	Preserve Status
1	SDR	Overwrite
2	FRU	Overwrite
3	SEL	Overwrite
4	IPMI	Overwrite
5	NETWORK	Overwrite
6	NTP	Overwrite
7	SNMP	Overwrite
8	SSH	Overwrite
9	KVM	Overwrite
10	AUTHENTICATION	Overwrite
11	SYSLOG	Overwrite
12	WEB	Overwrite
13	REDFISH	Overwrite

**Proceed to Flash**

WARNING:Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT,and APP components of Firmware.

- When the message requesting your confirmation prompts, click **OK** to proceed. The BMC will begin to verify and upload the firmware.



- When the firmware is uploaded completely, check **Full Flash** in the **Section Based Firmware Update** field and then click **Flash selected sections**.



**Note:** If you only want to update the firmware for certain sections, check the **Upgradable/Non-Upgradable** box for the individual sections instead of checking **Full Flash**.

Section Based Firmware Update

All the module section versions in the existing image and uploaded image are the same.

Version Compare Flash
  Full Flash

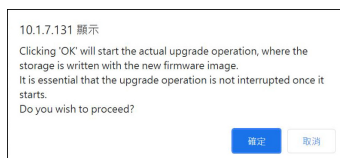
Section Name	Existing version	Uploaded version	Upgradable/Non-Upgradable
boot	13.1.000000	13.1.000000	<input type="checkbox"/>
conf	13.1.000000	13.1.000000	<input type="checkbox"/>
conf	13.1.000000	13.1.000000	<input type="checkbox"/>
ec	1.17.000000	1.17.000000	<input type="checkbox"/>
dtb	13.1.000000	13.1.000000	<input type="checkbox"/>
root	13.1.000000	13.1.000000	<input type="checkbox"/>
osimage	13.1.000000	13.1.000000	<input type="checkbox"/>
www	13.1.000000	13.1.000000	<input type="checkbox"/>
testapps	13.1.000000	13.1.000000	<input type="checkbox"/>
dre	13.1.000000	13.1.000000	<input type="checkbox"/>
ast2600e	13.1.13	13.1.13	<input type="checkbox"/>

Flash selected sections

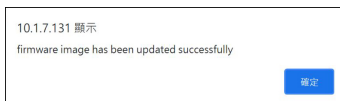
Uploading 100%

WARNING: Please note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradation is cancelled in the middle of the wizard, the device will be reset only for BMC BOOT, and APP components of Firmware.

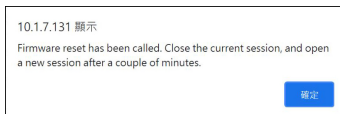
- When the message requesting your confirmation prompts, click **OK**. The BMC will start updating the firmware.



7. A confirmation message will appear once the firmware has been successfully updated. Click **OK** to proceed.

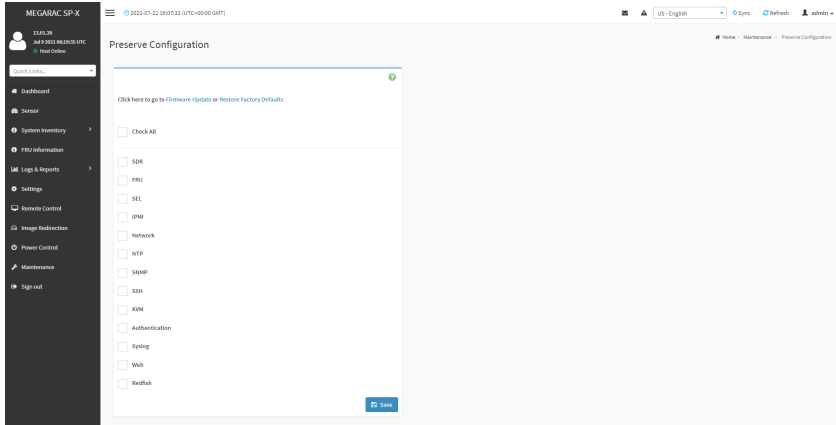


8. Click **OK**. The BMC will close all sessions displayed on the screen and automatically reboot the system.



## 2-10-5 Preserve Configuration

Preserve Configuration allows users to preserve the existing configuration so that the current configurations on the BMC will not be overwritten during the firmware update process. To open the Preserve Configuration page, click **Maintenance > Preserve Configuration** from the menu bar. A sample screenshot of the Preserve Configuration page is shown below.



The fields in the Preserve Configuration page are explained below.

**Check All:** Selects all items.

**Save:** Saves the changes.



**Note:** This configuration is used by Restore Factory Defaults process.

### SDR

Following files will be preserved:

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

**Dependency Configurations - NIL**

### FRU

Following files will be preserved:

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

**Dependency Configurations - SDR**

### SEL

Following files will be preserved when Delete SEL reclaim space is disabled:

**SEL.dat:** This file contains the system event logs that are being logged by the IPMI.

Following files will be preserved when Delete SEL reclaim space is enabled:

**Selreclaiminfo.ini** - The file contains the SEL repository information.

**SEL folder** - This folder contains the multiple files of event logs.

**Dependency Configurations - IPMI**

## IPMI

The following files are preserved in IPMI configuration:

**IPMI.conf:** This file contains the IPMI configurations such as SEL rep size, SDR rep size, interface specific, enable/disable, Primary/Secondary, IPMB Bus number etc.

**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 daemon 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

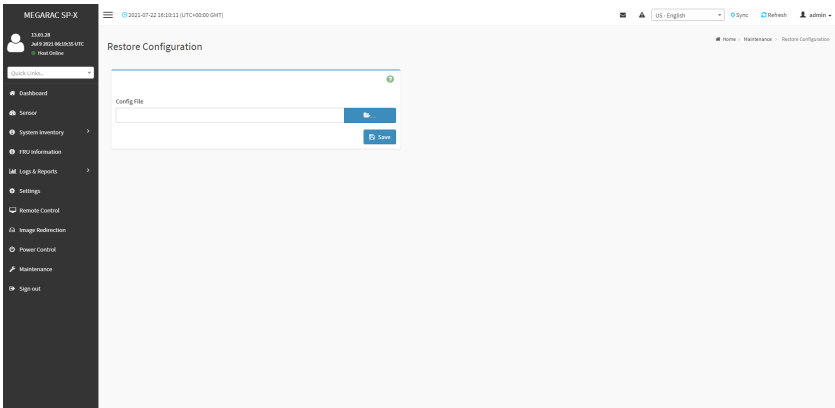
## Redfish Audit Log

### Procedure

1. Click **Firmware Update** or **Restore Configuration** to open the Firmware Update or Restore Configuration page accordingly.
2. Select **Check All** or the individual configuration items you want to preserve.
3. Click **Save** to save the changes.

## 2-10-6 Restore Configuration

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



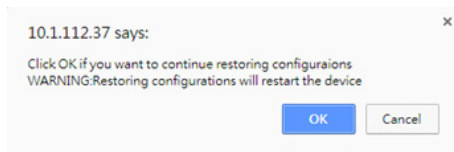
The fields in the Restore Configuration page are explained below.

**Config File:** Select the file which was backup earlier.

**Save:** Confirms to upload the selected configuration file.

### Procedure

1. Click Browse to search for the previously saved configuration file.
2. Click **Save**. A warning message will appear on the screen.



3. Click **OK** to upload the new configuration file and the device will restart automatically.

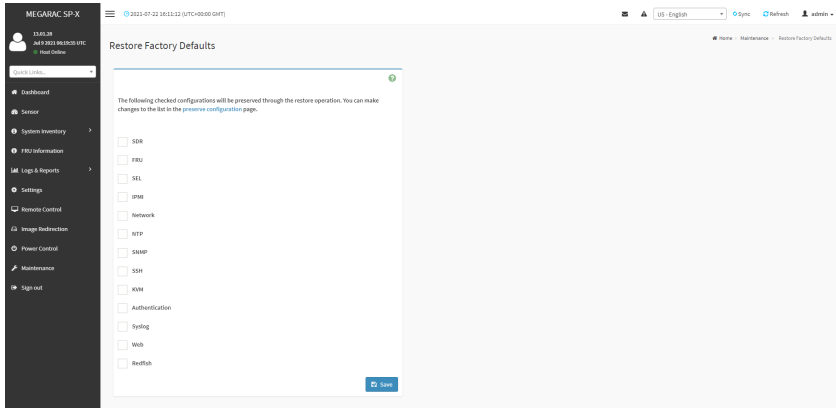
## 2-10-7 Restore Factory Defaults

Restore Factory Defaults lists the configuration items that can be preserved during the restore process.



**Warning:** Please note that after entering restore factory widgets, all other web pages and services will not work. All active widgets will be closed automatically. The device will reset and reboot within few minutes.

To open the Restore Factory Defaults page, click **Maintenance > Restore Factory Defaults** from the menu bar. A sample screenshot of the Restore Factory Defaults page is shown below.



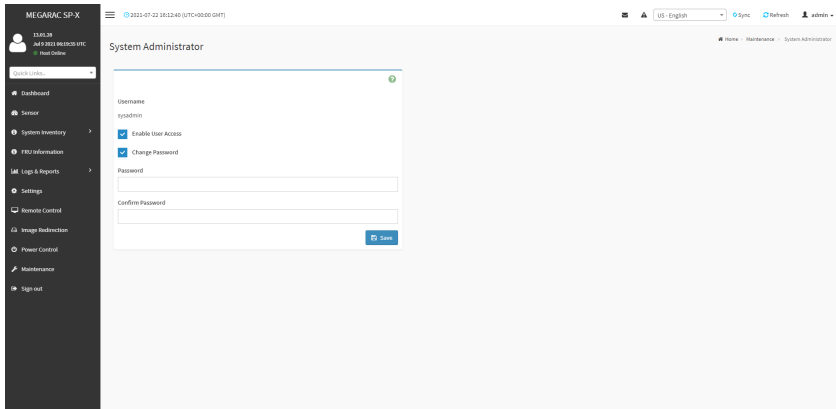
### Procedure

1. Click **Preserve Configuration** to open the Preserve Configuration page, which is used to preserve the particular configuration so that the configuration will not be overwritten by the default configuration.
2. Select the individual configuration items you want to preserve.
3. Click **Save** to save the changes.

## 2-10-8 System Administrator

This page is used to configure the System Administrator settings.

To open the System Administrator page, click **Maintenance > System Administrator** from the menu bar. A sample screenshot of the System Administrator page is shown below.



The fields in the System Administrator page are explained below.

**Username:** Displays user name of System Administrator. It is read-only.

**Enable User Access:** Enables user access for system administrator.

**Change Password:** Allows users to change the 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.

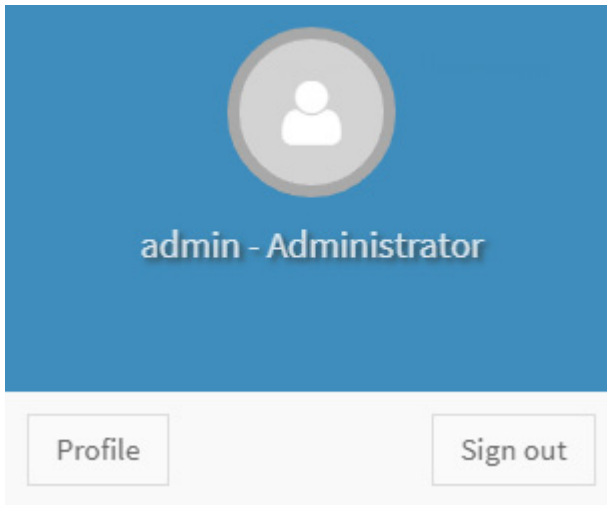
**Save:** Saves the new configuration for system administrator.

### Procedure

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

## 2-10-9 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.