GIGABYTE™

Chassis Management Controller

User Guide

Rev. 1.0

Copyright

Disclaimer

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 (e.g. motherboard, server barebones), covering hardware and BIOS.
- User Guide: detailed information about the installation & use of an add-on hardware or software component (e.g. BMC firmware, rail-kit) compatible with this product.
- Quick Installation Guide: a short guide with visual diagrams that you can reference easily for installation purposes of this product (e.g. motherboard, server barebones).

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 other 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 technical assistance, please contact your GIGABYTE representative or visit http://esupport.gigabyte.com/ to create a new support ticket.

For any general sales or marketing enquires, you may message GIGABYTE server directly by email: server.grp@gigabyte.com.

Table of Contents

Chapter 1 Getting Started

1-1 Supported Browsers

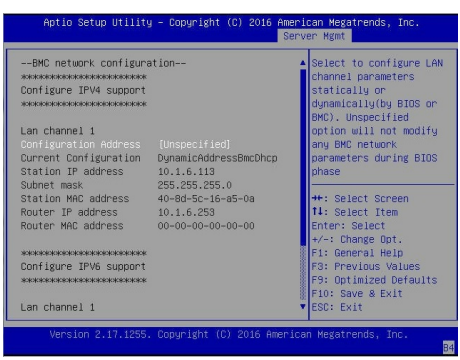
- Chrome latest version.
- IE 11 and above.
- Firefox (with limited support).

1-2 Gigabyte Management Console Network Configuration

Follow the instruction to enable the console redirection function.

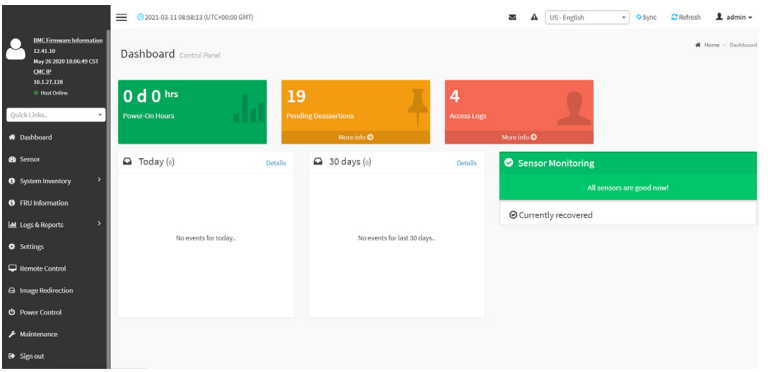
1. You can gather the BMC IP address on the POST screen.

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.

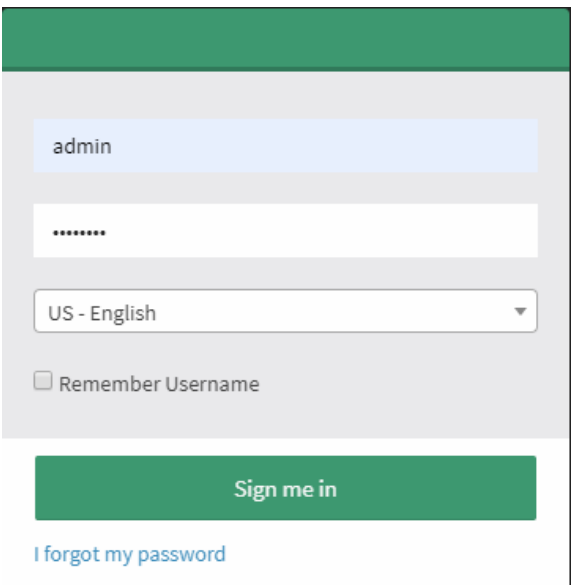
9. Next, logging in to BMC Web Console. You can gather the Chassis Management Controller (CMC) IP address from the menu bar at the left of the BMC Web UI.



Note: To access BMC Web Console, please refer to User Guide - GIGABYTE Management Console (AMI).

1-3 Gigabyte Chassis Management Controller Web Console

Gigabyte Chassis Management Controller(CMC) has a user-friendly Graphics User Interface for the web console. The CMC Web console will prompt you to enter the User Name and Password.



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

- **Username**: admin
- **Password**: password

Language Setting: Select the display language which you would like to use.
Remember Username: Check this option to remember your login credentials.
Sign me in: After entering the required credentials, click the **Sign me in** to login to Web UI.
I forgot my password: If you forget your password, you can generate a new one using this link. Enter the username, click on **Forgot Password** link. This will send the newly generated password to the configured Email-ID for the user.

1-3-1 Required Browser Settings:

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

For all Other Browsers, accept file download when prompted.

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

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

Cookies must be enabled in order to access the website.

1-4 Quick Button and Logged-in User

The user information and quick buttons are located at the top right of the Web UI. 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 CMC commands are allowed except for the configuration commands that can change the behavior of the out-of-hand interfaces.
- **Administrator**: All CMC commands are allowed.
- **No Access**: Login access denied.
- **OEM**: All OEM commands are allowed.

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

Refresh: Click the icon to reload the current page.

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

Language Setting: Select the display language which you would like to use.

Notification: Click the icon to view the notification messages.

Email: Click the icon to view the received messages.

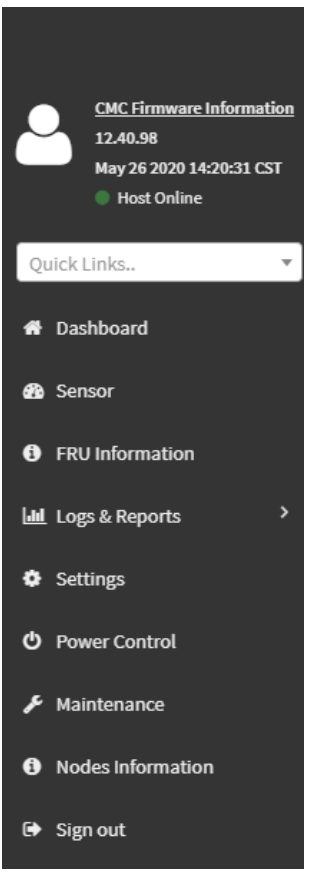
1-5 Help

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

1-6 Menu Bar

The menu bar displays the following:

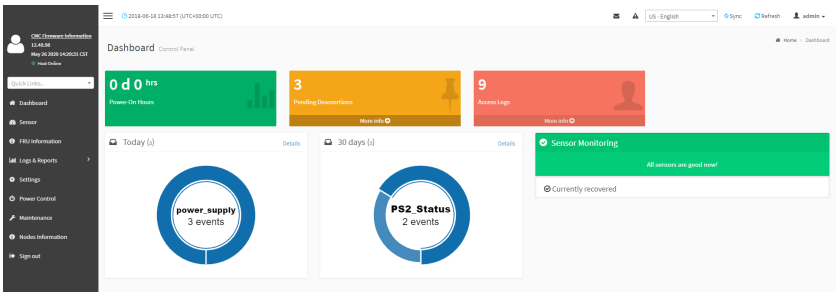
- Dashboard
- Sensor
- FRU Information
- Log & Reports
- Settings
- Power Control
- Maintenance
- Nodes Information
- Sign out



Chapter 2 Enter Gigabyte CMC Web 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.

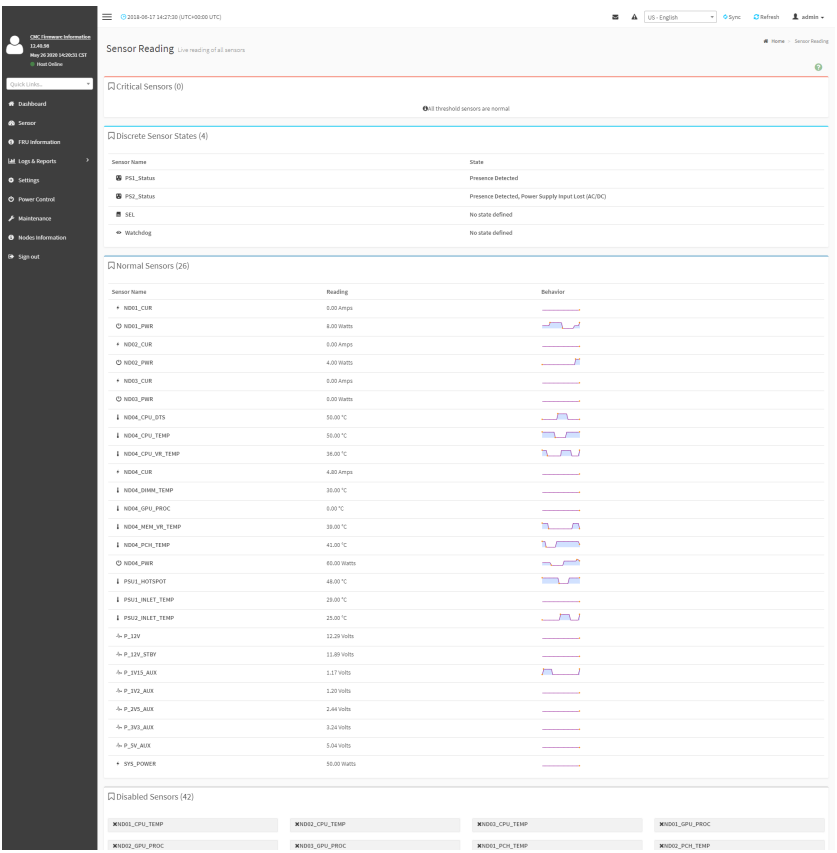
Access Logs
A graphical representation of all events incurred by various sensors and occupied/available space in logs can be viewed, if you click on the More info link, you can view the Audit Log page.

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.

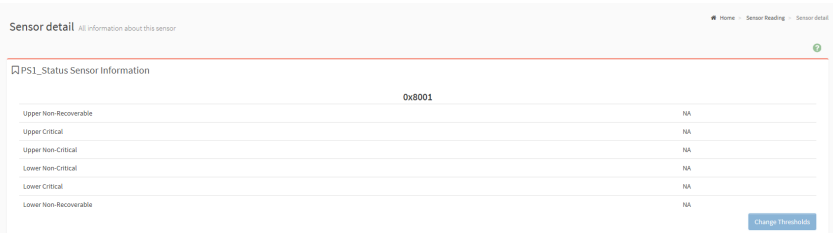


In this Sensor Reading page, Live readings for all the available sensors with details like Sensor Name, Type, Status, Current Reading and Behavior will be appeared.

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.

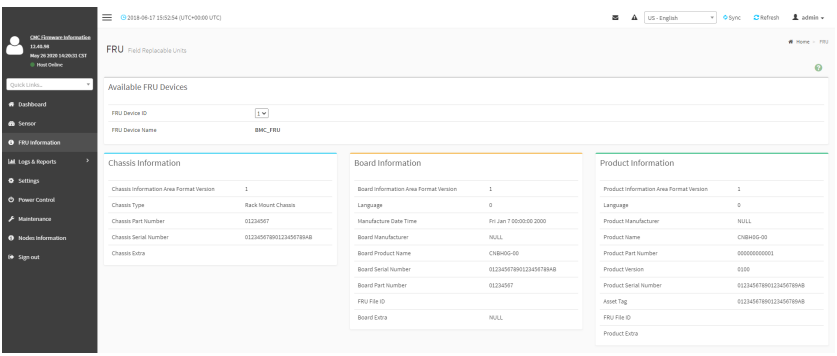
2-2-2 Sensor Events

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 FRU Information

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

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



The following fields are displayed here for the selected device:

Available FRU Devices

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

Chassis Information

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

Board Information

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

Product Information

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

2-4 Logs & Reports

The Logs & Reports page displays the following information:

- IPMI Event Log
- System Log
- Audit Log

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

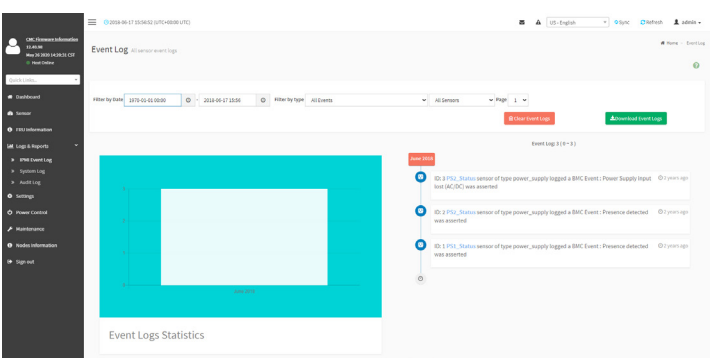
A detailed description of Logs & Reports is given below.

2-4-1 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, SMI Handler Events, System Management Software Events, System Software - OEM Events, Remote Console Software Events, Terminal Mode Remote Console Software Events.

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

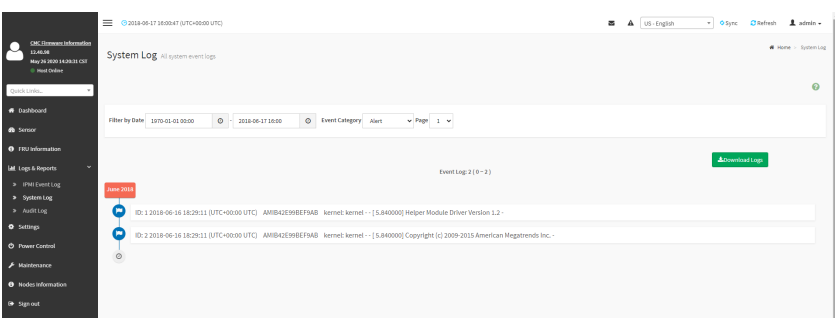
Event Log Statistics: Displays the statistical graph for the selected date.
Clear Event Logs: To delete all the event logs.
Download Event Logs: To download the event logs.

Procedure

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

2-4-2 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.



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: Classification of event severity: Alert, Critical, Error, Notification, Warning, Debug, Emergency and Information.

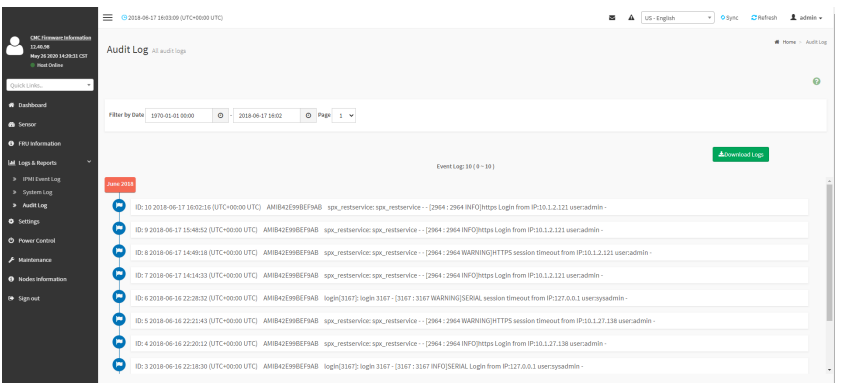
Note:Once the Filter By Date and Event Category are selected, the list of events will be displayed with the Event ID, Time Stamp and Description.
Download Logs: To download the event logs.

Procedure

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

2-4-3 Audit Log

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



The Audit Log page consists of the following fields:
Filter By Date: Filtering can be done by selecting **Start Date** and **End Date**.

Note:Once the Filter By Date and Event Category are selected, the list of events will be displayed with the Event ID, Time Stamp and Description.

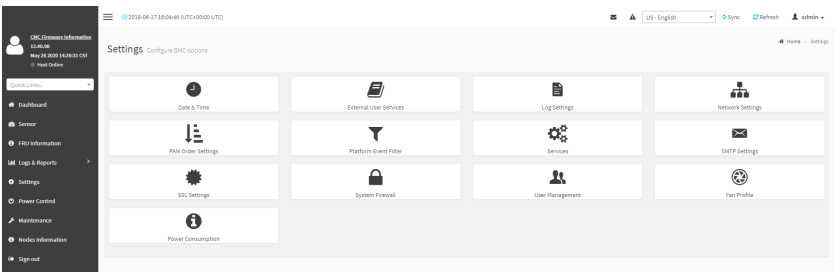
Download Logs: To download the event logs.

Procedure

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

2-5 Settings

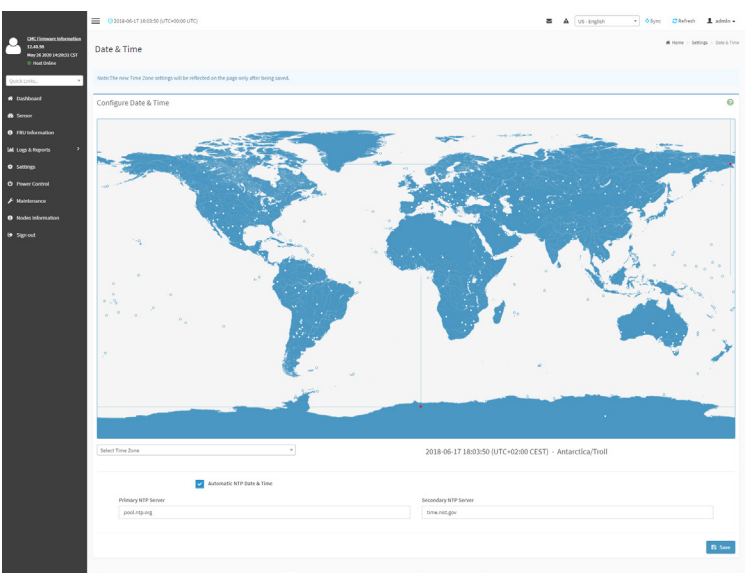
This group of pages allows you to access various configuration settings. A screenshot of Configuration Group menu is shown below.



A detailed description of the Settings menu is given below.

2-5-1 Date & Time

This field is used to set the date and time on the CMC. 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.

Primary NTP Server: To configure a primary NTP server to use when automatically setting the date and time.
Secondary NTP Server: To configure a secondary NTP server to use when automatically setting the date and time.
Automatic Date & Time: To automatically synchronize Date and Time with the NTP Server.
Save: To save the configured settings.

Procedure

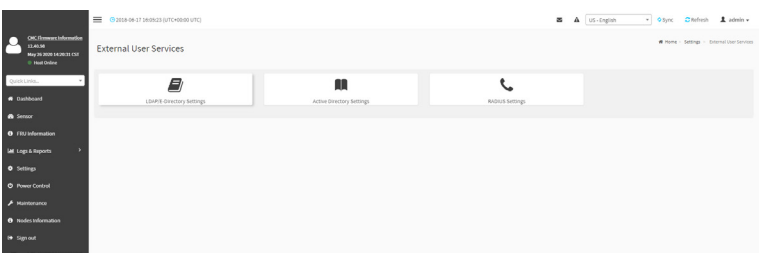
1. Select the Time zone location from the map.
2. In the Primary NTP Server / Secondary NTP Server field, specify the NTP server for the device.

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

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

2-5-2 External User Services

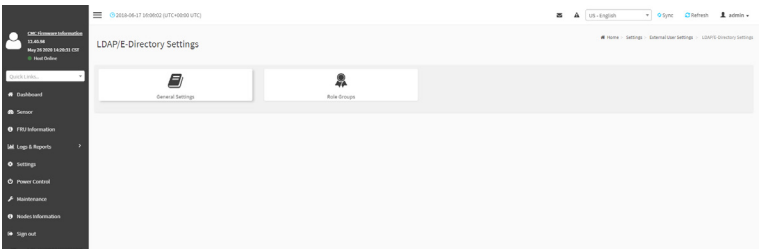
To open External User Services page, click **Settings > External User Services** from the menu bar. A sample screenshot of External User Services page is shown below.



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 UI, LDAP is an Internet protocol that CMC 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 CMC 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 CMC. 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 LDAP/E-Directory Settings page, click **Settings > External User Services > LDAP/E-Directory Settings** from the menu bar.

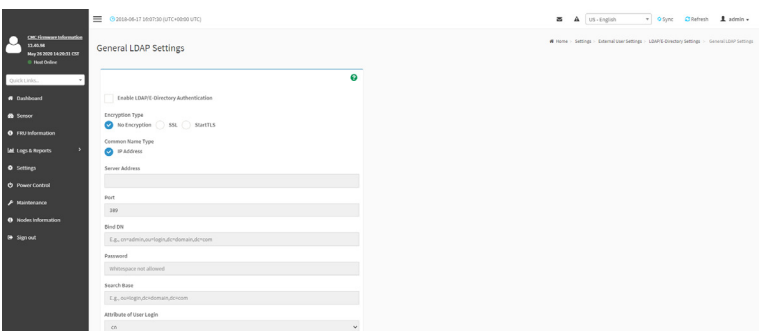
A sample screenshot of LDAP/E-Directory Settings page is shown below.



The fields of LDAP/E-Directory Settings page are explained below.
General Settings: To configure LDAP/E-Directory Settings. Options are Enable LDAP/E-Directory Authentication, IP Address, Port and Search base.
Role Groups: To add a new role group to the device.

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. Select the Encrytion Type for LDAP/E-Directory: No Encrption, SSL or StartTLS.

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

3. Select the Common Name Type as IP Address.
4. Enter the IP address of LDAP server in the Server Address field.

   Note: IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
   Each Number ranges from 0 to 255.
   First Number must not be 0.
   Supports IPv4 Address format and IPv6 Address format.
   Configure FQDN address, when using StartTLS with FQDN.
5. Specify the LDAP Port in the **Port** field.

   Note: Default Port is 389. For SSL connections, default port is 636. The Port value ranges from 1 to 65535.

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

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

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

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

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

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

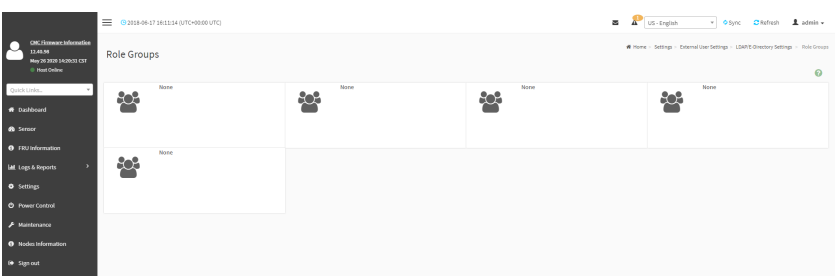
9. Select Attribute of User Login to find the LDAP/E-Directory server which attribute should be used to identify the user.

   Note:It only supports cn or uid.

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

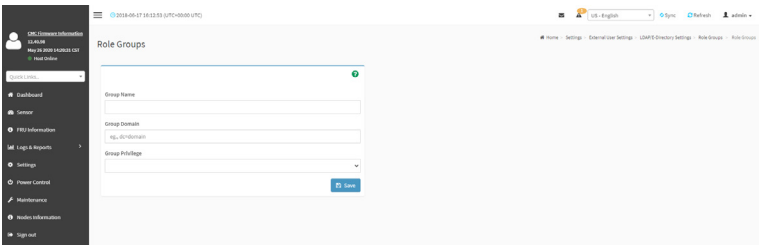
Role Groups

To open Role Group page, click **Settings > External User Settings > LDAP/E-Directory Settings > Role Groups** from the menu bar. A sample screenshot of Role Groups page is shown below.



To add a new Role Group

1. In the Role Groups page, double click on on a free slot 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.

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

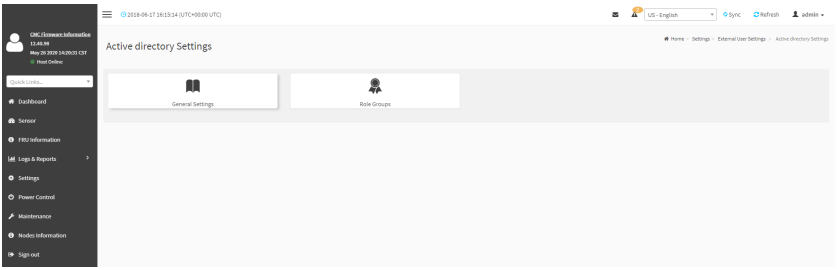
3. In the **Group Domain** field, enter the Role Group Domain where the role group is located.

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

4. In the **Group Privilege** field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
5. Click **Save** to save the new role group and return to the Role Group List.

Active Directory Settings

An active directory is a directory structure used on Microsoft Windows based computers and servers to store information and data about networks and domains. An active directory (sometimes referred to as AD) does a variety of functions including the ability to provide information on objects. It also helps to organize these objects for easy retrieval and access, allows access by end users and administrators and allows the administrator to set security up for the directory.
Active Directory allows you to configure the Active Directory Server Settings. The displayed table shows any configured Role Groups and the available slots. You can modify, add or delete role groups from here. Group domain can be the AD domain or a trusted domain. Group Name should correspond to the name of an actual AD group.
Note: To view the page, you must be at least a User and to modify or add a group, you must be an Administrator.
To open Active Directory Settings page, click **Settings > External User Settings > Active Directory** from the menu bar. A sample screenshot of Active Directory Settings page is shown below.



The fields of Active Directory page are explained below.

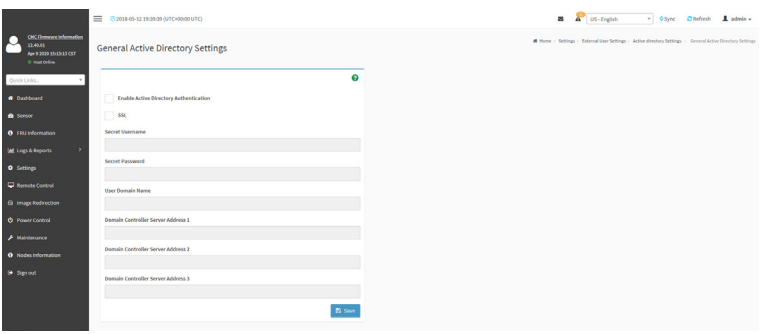
General Settings: This option is used to configure Active Directory General Settings. Options are Enable Active Directory Authentication, Secret User Name, Secret Password, User Domain name, and up to three Domain Controller Server Addresses.

Role Groups: This option is used to add a new role group to the device.

Procedure

Entering the details in General Active Directory Settings page:

1. Click on **General Settings** to open the General Active Directory Settings page.



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

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

3. Enable or disable **SSL cetificates** on the Active Directory server.
4. Specify the Secret user name and password in the **Secret Username** and **Secret Password** fields respectively.

   Note: Secret username/password for AD is not mandatory. When secret username & password is empty, Authentication fails will be always treated as Invalid Password error.

   For Invalid Password error PAM will not try other Authentication Methods. So it

is recommended to keep AD in the last location in PAM order.
User Name is a string of 1 to 64 alpha-numeric characters.
It must start with an alphabetical character.
It is case-sensitive.
Special characters like comma, period, colon, semicolon, slash, backslash, square brackets,
Blank space is not allowed, angle brackets, pipe, equal, plus, asterisk, question mark, ampersand, double quotes, space are not allowed.
Password must be at least 6 character long and will not allow more than 127 characters.

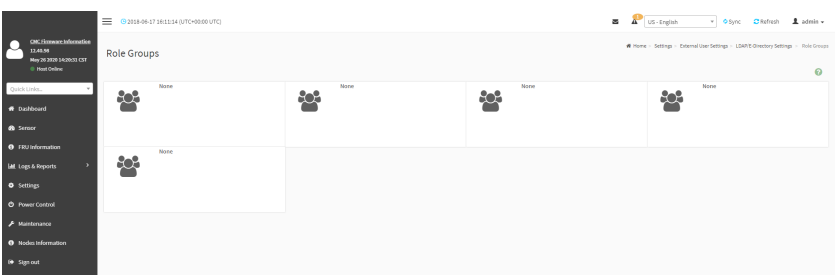
5. Specify the Domain Name for the user in the **User Domain Name** field. E.g. MyDomain.com
6. Configure IP addresses in Domain **Controller Server Address1, Domain Controller Server Address2 and Domain Controller Server Address3**

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

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

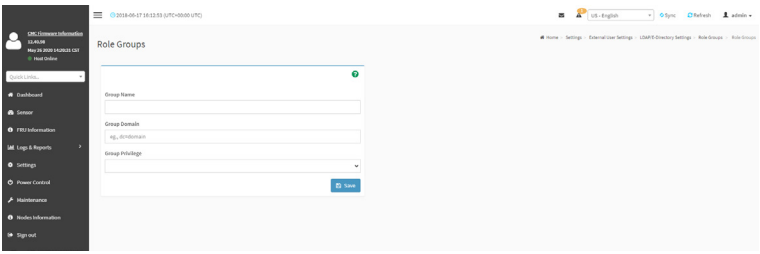
Role Groups

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



To add a new Role Group

1. In the Role Groups page, double click on on a free slot 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.

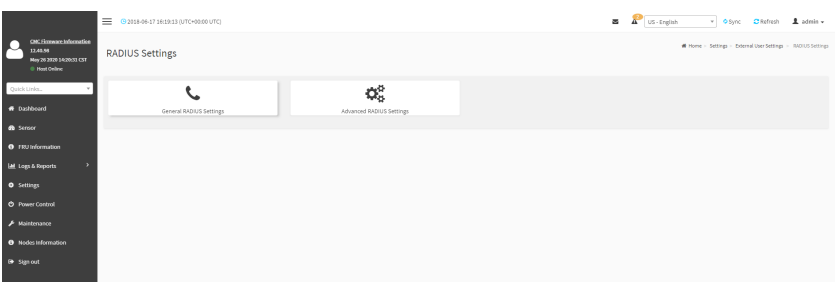
3. In the **Group Domain** field, enter the domain where the role group is located.

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

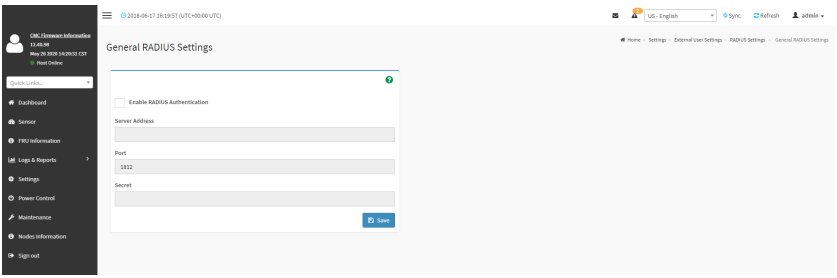
4. In the **Group Privilege** field, enter the level of privilege to assign to this role group.
5. Click **Save** to add the new role group and return to the Role Group List.

RADIUS Settings

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities.
In Web GUI, this page is used to set the RADIUS Authentication.
To open RADIUS Settings page, click **Settings > External User Settings > RADIUS Settings** from the menu bar. A sample screenshot of RADIUS Settings page is shown below.



The fields of General RADIUS Settings page are explained below.



Enable RADIUS Authentication: Option to enable/disable RADIUS authentication.
Server Address: The IP address of RADIUS server.

Note: IP Address (Both IPv4 and IPv6 format).
FQDN (Fully Qualified Domain Name) format.

Port: The RADIUS Port number.

Note: Default Port is 1812.
Port value ranges from 1 to 65535.

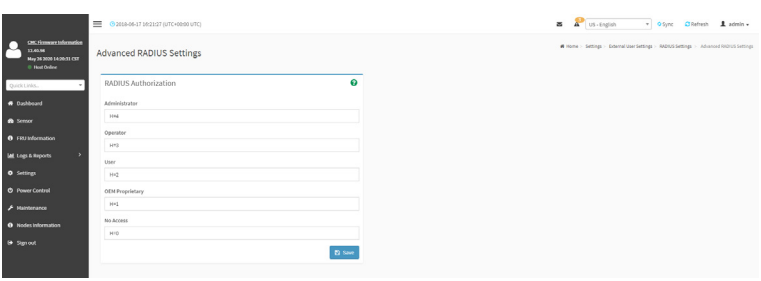
Secret: The Authentication Secret for RADIUS server.

Note: This field will not allow more than 31 characters.
Secret must be at least 4 characters long.
Blank space is not allowed.

Save: To save the configured settings.

Procedure

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



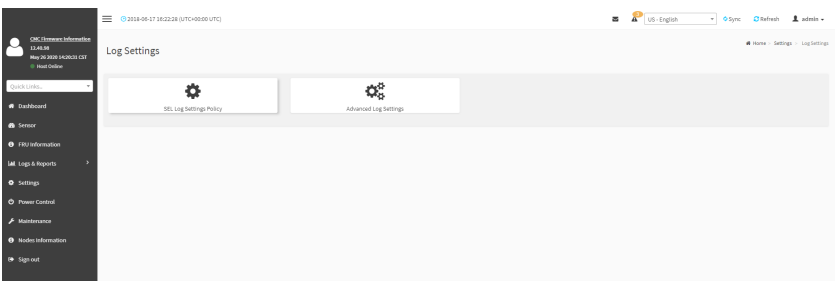
Note: For Authorization Purpose, configure the Radius user with Vendor Specific Attribute in Server side.
Example: 1
testadmin Auth-Type: =PAP, Cleartext-Password:=”admin”
Auth-Type: =PAP, Vendor-Specific= ”H=4 ”

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

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

2-5-3 Log Settings

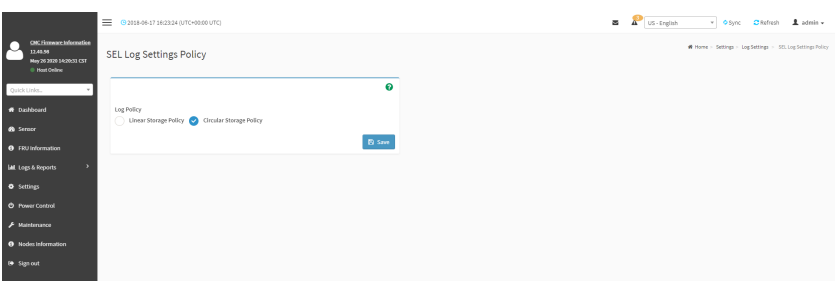
In CMC Web GUI, System and Audit log page displays a list of system logs and audit logs occurred in this device.
To open Log Settings page, click **Settings > Log Settings** from the menu bar. A sample screenshot of Log Settings page is shown below.



The fields of Log Settings page are explained below.

SEL Log Settings Policy

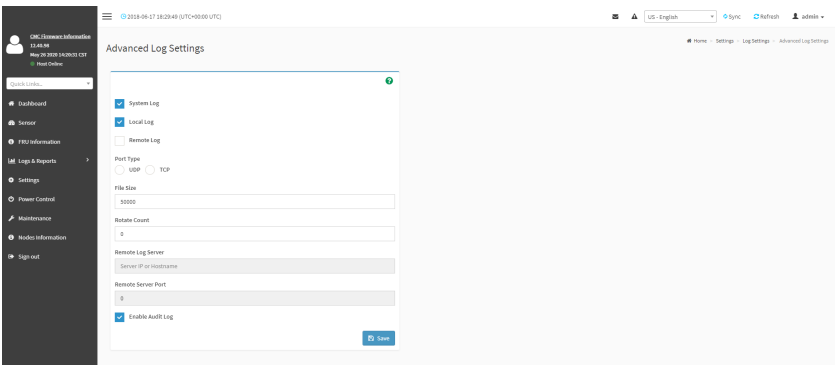
This page is used to configure the log policy for the event log. To open SEL Settings Policy page, click **Settings > Log Settings > SEL Log Settings Policy** from the menu bar. A sample screenshot of SEL Log Settings Policy page is shown below.



Log Policy: Check the option to enable **Linear Storage Policy** or **Circular Storage Policy** for the event log.

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 are as follows.

System Log: Option to enable/disable the System Logs.

Local Log/ Remote Log: Specifies the location for system logs, whether it should be preserved in a local file or on a remote log server.

Note: Local file resides at /var/log/

Port Type: Select the port type to be either **UDP** or **TCP**.

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

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

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

Note: Values supported are 0 and 1.

When log information exceeds the file size, the old log information is automatically moved to back up files based on the rotate count value. If rotate count is zero, then old log information gets cleared permanently.

File Size and Rotate Count options will be available only when Local Log is enabled.

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

Note: Server address will support the following:

IPv4 address format.

FQDN (Fully qualified domain name) format.

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

Note: Remote Log Server and Remote Server Port options will be available only when Remote Log is enabled.

Enable Audit Log: To enable or disable the audit log.
Save: To save the current changes.

Procedure

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

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

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

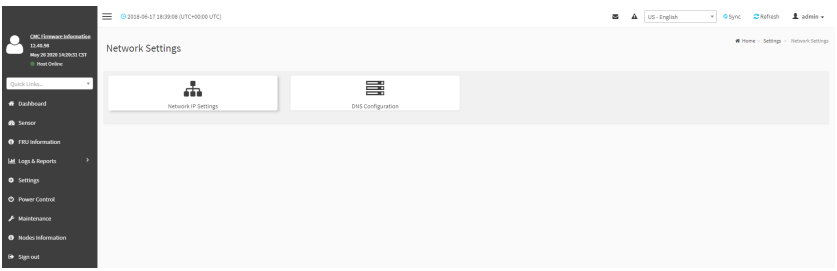
Steps to configure the remote server to enable syslogging

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

1. MODLOAD imudp
2. UDPSERVER 514

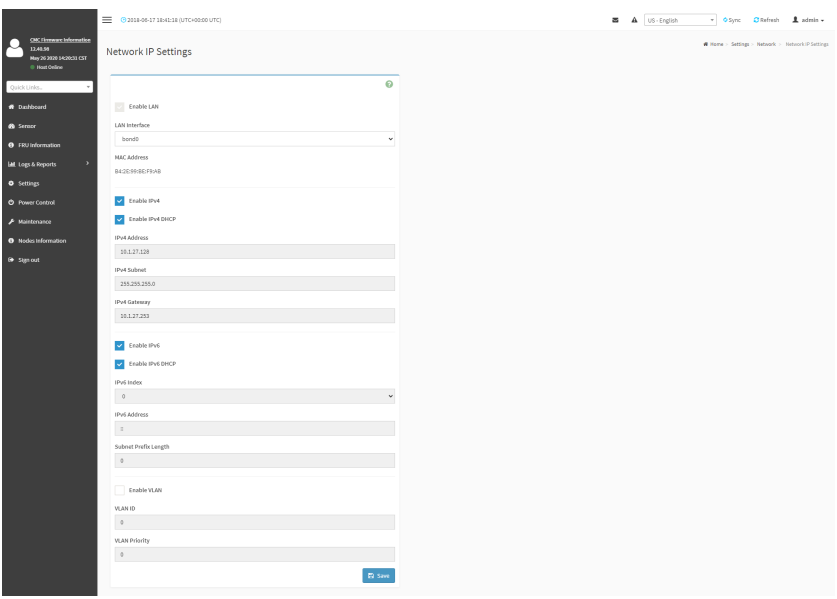
2-5-4 Network Settings

The Network Settings page is used to configure the network settings for the available LAN channels. To open the Network Settings page, click **Settings > Network Settings** from the menu bar.



Network IP Settings

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



The fields of Network IP Settings page are explained below.

Enable LAN: To enable or disable the LAN Settings.

LAN Interface: Lists the LAN interfaces.

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

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

Enable IPv4 DHCP: This option is to enable IPv4 DHCP support for the selected interface.
IPv4 Address, IPv4 Subnet Mask, and IPv4 Default Gateway: These fields are for specifying the static IPv4 address, Subnet Mask and Default Gateway to be configured to the device.

Note: IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".
Each Number ranges from 0 to 255.
First Number must not be 0.

Enable IPv6: To Enable/Disable the IPv6 configuration settings.
Enable IPv6 DHCP: To Enable/Disable the IPv6 settings in the device. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).
IPv6 Index: To specify a static IPv6 Index to be configured to the device. E.g.: 0
IPv6 Address: To specify a static IPv6 address to be configured to the device. E.g.: 2004::2010
Subnet Prefix length: To specify the subnet prefix length for the IPv6 settings.

Note: Value ranges from 0 to 128.

Enable VLAN: To enable/disable the VLAN support for selected interface.
VLAN ID: The Identification for VLAN configuration.

Note: Value ranges from 2 to 4094.

VLAN Priority: The priority for VLAN configuration.

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

Save: To save the entries.

Procedure

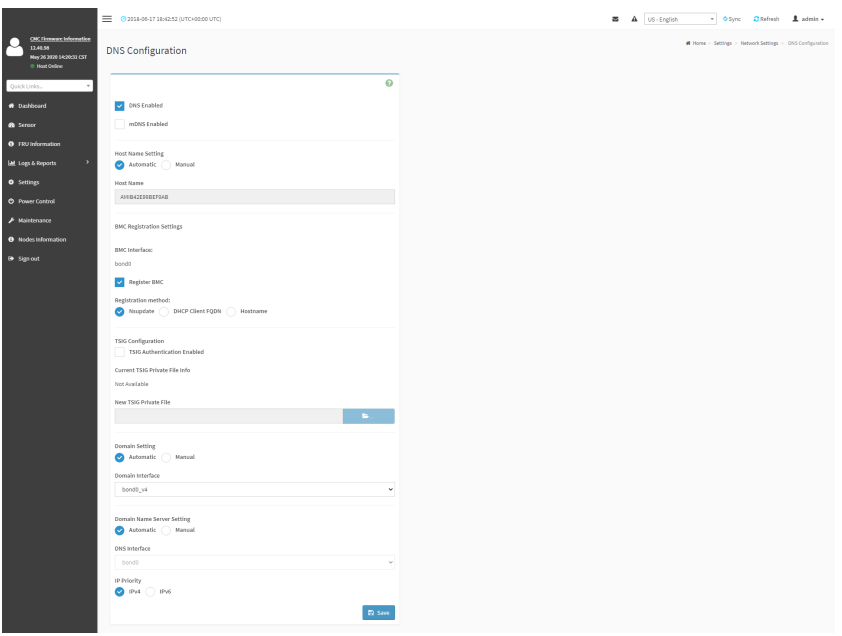
1. Check **Enable LAN** to enable LAN support for the selected interface.
2. Select the **LAN Interface** to be configured.
3. Check Enable IPv4 to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled,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

DNS Configuration

The **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

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

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



The fields of DNS Configuration page are explained below.

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

mDNS Enable: To enable/disable the mDNS Support Configurations.

Host Name Settings: Choose either Automatic or Manual settings.

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

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

BMC Registration Settings
BMC Interface: Options to register the BMC through the Interfaces (eth0&eth1).
Register BMC: To register BMC through registration method.

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

TSIG Configuration

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

Note: TSIG file should be of private type.

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

- **Automatic** - If you Select Automatic, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.
- **Manual** - If the Domain setting is chosen as Manual, then specify the domain name of the device.

Note: If you select "Automatic" it displays the Domain Interface option. If you select "Manual" it displays "Domain name".

Domain Name Server Setting: Select whether the DNS interface will be configured manually or automatically.

- **Automatic -** If you select Automatic "DNS Interface" option should be explained.
- **Manual** - Specify the DNS (Domain Name System) server address to be configured for the CMC.

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: This field will be present if specify Domain Name Server Setting to Manual, this item is used to specify the DNS (Domain Name System) server address to be configured for the BMC.

Note: IPv4 Addresses should be given in dotted decimal representation.
IPv6 Addresses are supported and must be global unicast addresses.
DNS Server Address will support the following:

- IPv4 Address format.

- IPv6 Address format.

Save: To save the current changes.

Procedure

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

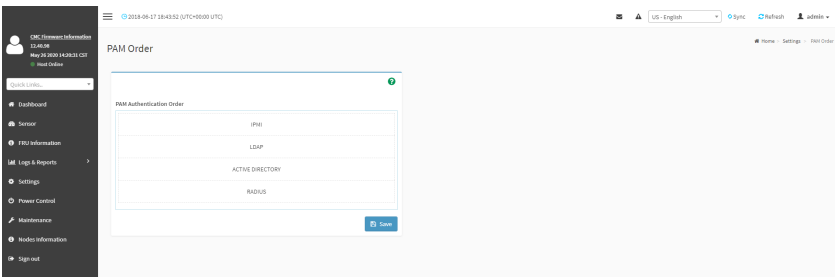
   Note: If you choose Automatic, you need not enter the Host Name and if you choose Manual, you need to enter the Host Name.
3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.
4. Under Register BMC, choose the BMC's network port to register with DNS settings.
5. Check **Register BMC** option to register with DNS settings.
   - **Nsupdate** - Choose Nsupdate option to register with DNS server using nsupdate application.
   - **DHCP Client FQDN** - Choose DHCP Client FQDN option to register with DNS Server using DHCP option 81.
   - **Hostname** - Choose Hostname option to register with DNS server using DHCP option 12.

     Note: Hostname option should be selected, if the DHCP client FQDN option is not supported by DHCP server.
6. Check **Both** option to modify TSIG authentication for both interfaces (eth0&1).
7. In **Eth 0&1 TSIG Configuration**, Check TSIG Authentication Enabled option to enable/ disable TSIG authentication while registering DNS via nsupdate.
   - The current file name will be displayed in Current TSIG Private file info field.
   - To view a new one, click New TSIG private file to browse and navigate to the TSIG private file.
8. In the **Domain Settings**,
   - Select the domain settings (Automatic or Manual).
   - Enter the Domain Name in the given field if the option "Manual" is being selected in domain settings field.
9. In **Domain Name Server Settings**,
   - Select the DNS Name Server Setting.
   - Choose the IP Priority, either IPv4 or IPv6.
   - Enter the DNS Server address.
10. In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC.
11. Click **Save** to save the entries.

2-5-5 PAM Order Settings

This page is used to configure the PAM ordering for user authentication in to the CMC.
To open PAM Ordering page, click **Settings > PAM Order Settings** from the menu bar. A sample screenshot of PAM Order page is shown below:



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

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

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

Procedure

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

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

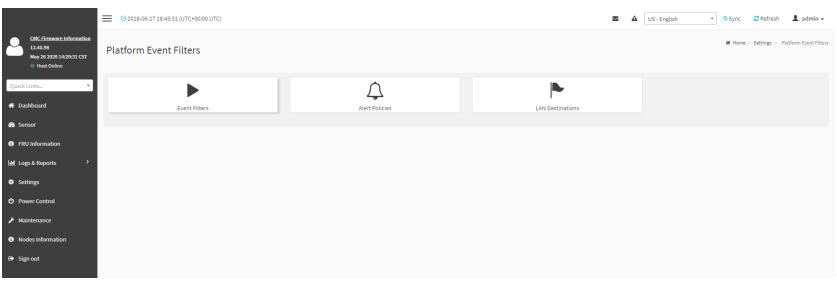
2-5-6 Platform Event Filter

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

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

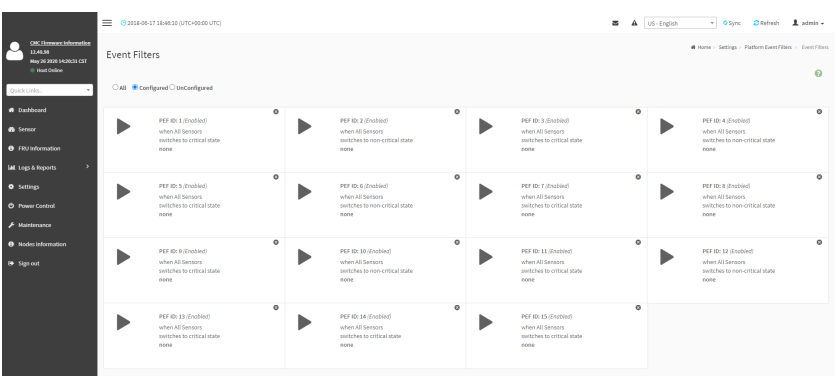
- Event Filters
- Alert Policies
- LAN Destinations

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



Event Filters

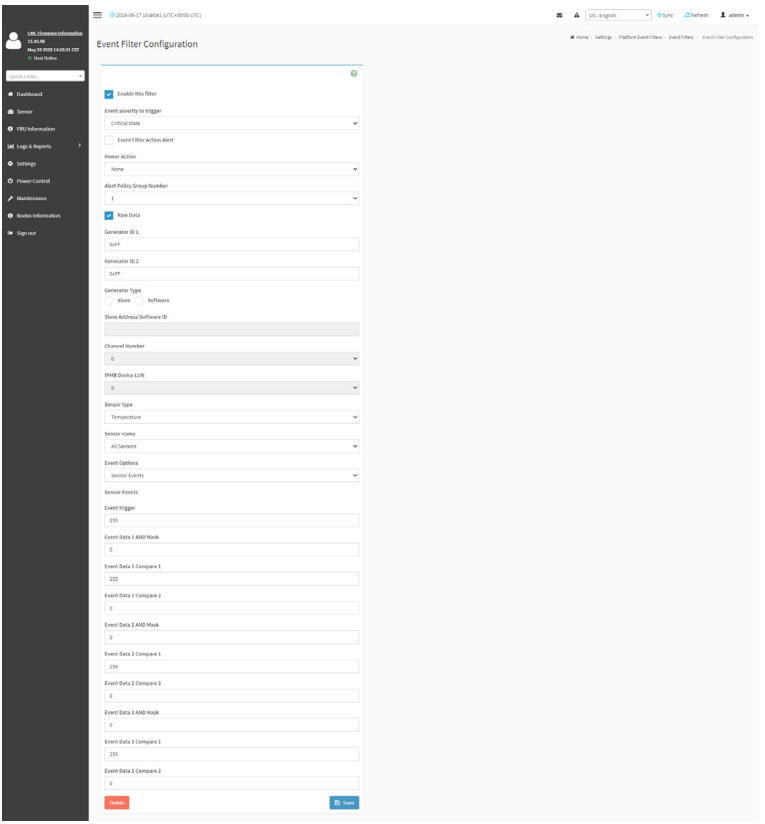
A PEF implementation is recommended to provide at least 40 entries in the event filter table. A subset of these entries should be pre-configured for common system failure events, such as over-temperature, power system failure, fan failure events, etc. Remaining entries can be made available for 'OEM'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



The Event Filters page is used to modify or add new event filter entries.

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 event filter 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->Platform Event Filter->Alert Policy**.

- Check **Raw Data** option to fill the Generator ID with raw data.

- **Generator ID 1** field is used to give raw generator ID 1 data value.
- **Generator ID 2** field is used to give raw generator ID2 data value.

  Note: In **RAW** data field, specify hexadecimal value prefix with '0x '.

- In the **Generator Type** 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 CMC.
- Choose the corresponding **IPMB Device LUN** if event generated by IPMB.
- Select the **Sensor Type** of sensor that will trigger the event filter action.
- In the **Sensor name** field, choose the particular sensor from the sensor list.
- Choose **Event Options** to be either All Events or Sensor Specific Events.
- In the **Sensor Events** field, choose the type of event levels.
- **Event Trigger** field is used to give Event/Reading type value.

  Note: Value ranges from 1 to 255.

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

  Note: Value ranges from 1 to 255.

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

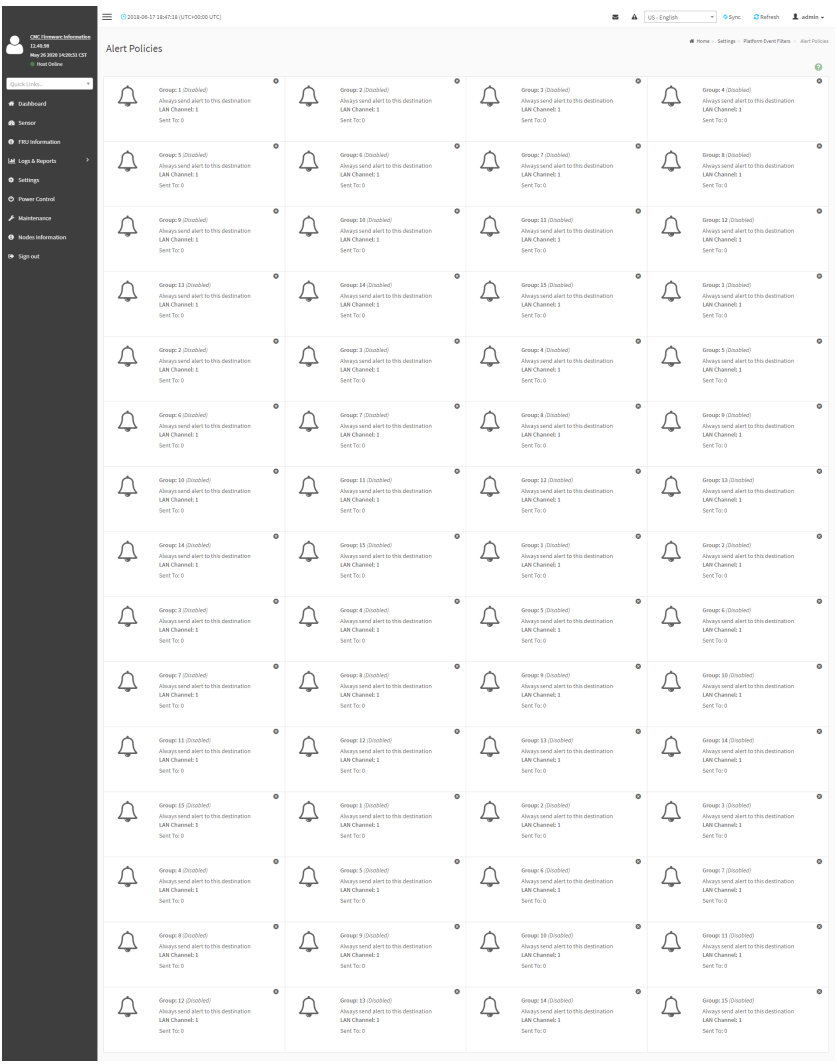
  Note: Value ranges from 1 to 255.

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

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

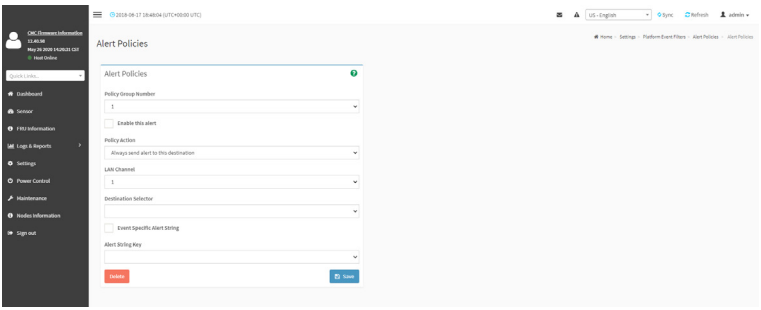
Alert Policies

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



Procedure

1. 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 to open the **Alert Policies** page as shown in the screenshot below.



3. Select **Policy Group Number** from the drop-down list.
4. Check **Enable this alert** to enable the policy settings.
5. Choose any of the **Policy Action** from the list.
6. Choose particular **LAN Channel** from the available channel list.
7. In the **Destination Selector**, choose particular destination from the configured destination list.

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

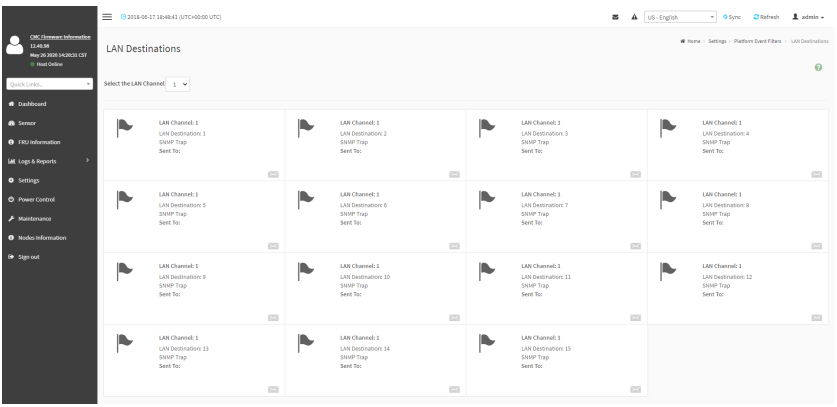
8. Enable **Event Specific Alert String**, if the Alert policy entry is Event Specific.
9. In the **Alert String Key** field, choose any one value that is used to look up the Alert String to send for this Alert Policy entry.

Note: Using Web UI, Alert strings cannot be configured but option for Event Specific alert strings can be enabled/disabled. There is an option to select only the alert string keys, but alert strings has to be configured using IPMI Command (Set PEF Config Parameter 'Alert String").

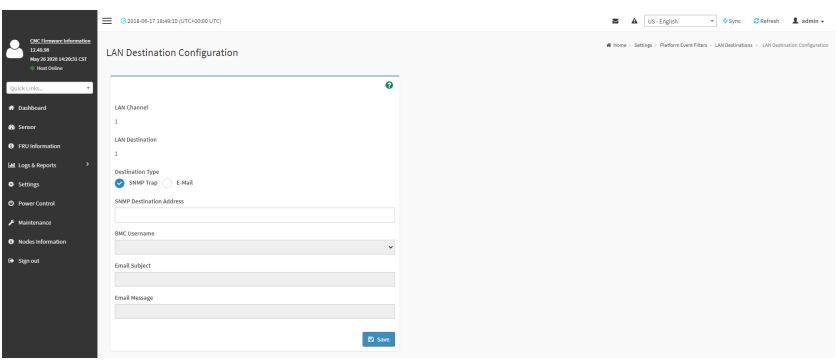
10. Click **Save** to save the new alert policy and return to Alert Policy list.
11. Click **Delete** to delete a configuration.

LAN Destinations

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



The fields of Platform Event Filters - LAN Destinations are explained below.
Select any empty slot to configure LAN Destinations.



LAN Channel: Displays LAN Channel Number for the selected slot (read-only).
LAN Destination: Displays ID for setting Destination Selector of Alert Policy (read-only).
Destination Type: Destination type can be either an SNMP Trap or an E-mail alert.

- For E-mail alerts, the four fields - SNMP Destination Address, BMC User Name, Email subject and Email message needs to be filled. The SMTP server information also has to be added - under **Settings ->SMTP Settings**.
- For SNMP Trap, only the SNMP Destination Address has to be filled.

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

- IPv4 address format.
- IPv6 address format.

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

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

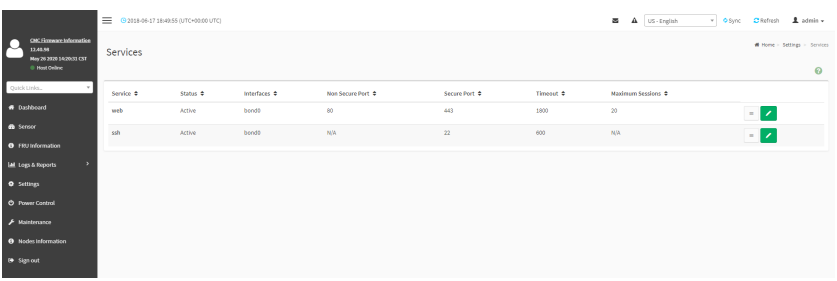
Note: User should be configured under Settings-->User Management

Save: To add a new entry to the device. Alternatively, double click on a free slot.
Delete: To delete the selected configured LAN Destination.

2-5-7 Services

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

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



The fields of Services page are explained below.

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

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

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

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

- Web default port is 80

Note: SSH service will not support non secure port. Port value ranges from 1 to 65535.

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

- Web default port is 443
- SSH default port is 22

Note: Port value ranges from 1 to 65535.

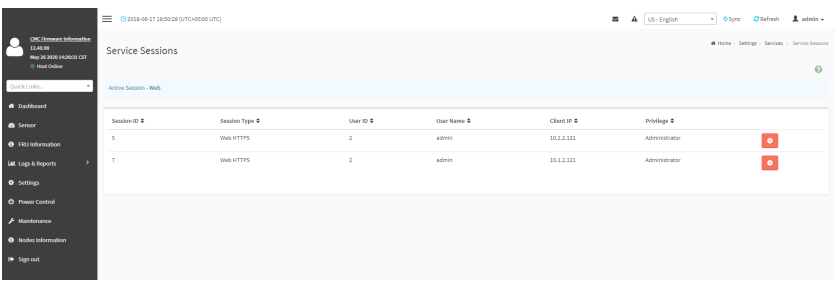
Timeout: Displays the session timeout value of the service. User can configure the session timeout value.

Note: Web timeout value ranges from 300 to 1800 seconds.
SSH timeout value ranges from 60 to 1800 seconds.

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

View the Active Sessions

Select a slot and click **View** icon ( ) to view the details about the active sessions for the service. This opens the Active Session screen as shown in the screenshot below.



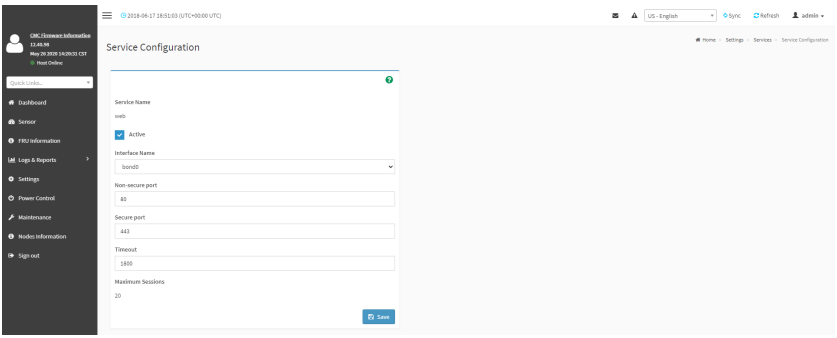
Session ID: Displays the ID of the active sessions.
Session Type: Displays the type of the active sessions.
User ID: Displays the ID of the user.
User Name: Displays the name of the user.
Client IP: Displays the IP addresses that are already configured for the active sessions.
Privilege: Displays the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

Modify the existing services:

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.

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



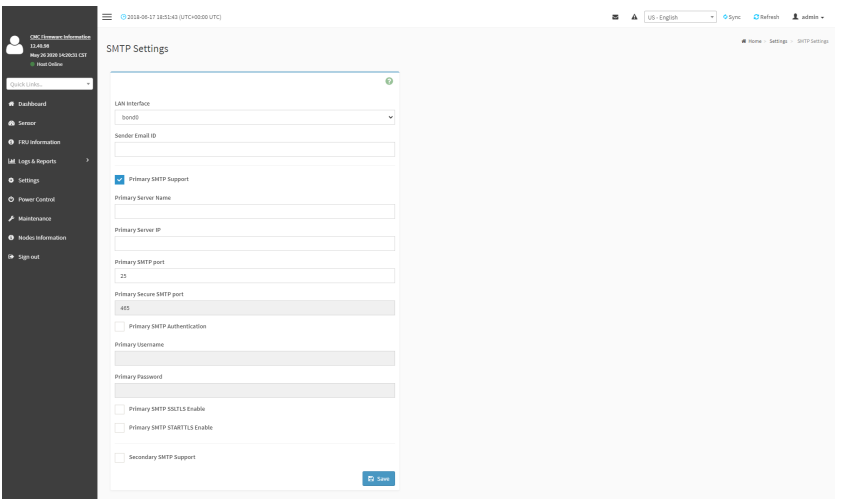
Service Name: Displays service name of the selected slot (read-only).
Active: Activate the Current State by enabling the Active check box.

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

Interface Name: Select any one of the available interfaces from the drop-down list.
Non-secure port: Configure non secure port number for the service.
Secure port: Configure secure port number for the service.
Timeout: Enter the timeout value for the service.
Maximum Sessions: Displays the maximum number of allowed sessions for the service (read-only).
Save: To save all changes you have made.

2-5-8 SMTP Settings

Simple Mail Transfer Protocol (SMTP) is an Internet standard for electronic mail (e-mail) transmission across Internet Protocol (IP) networks.
Using CMC Web GUI, you can configure the SMTP settings of the device.
To open SMTP Settings page, click **Settings > SMTP Settings** from the menu bar. A sample screenshot of SMTP Settings page is shown below.



The fields of SMTP Settings page are explained below.
LAN Interface: Displays the list of LAN channels available
Sender Email ID: A valid 'Sender Address' to indicate the CMC, whenever e-mail is sent.
Primary SMTP Support: To enable/disable SMTP support for the CMC.
Primary Server Name: The 'Machine Name' of the CMC, from where the e-mail is sent.

Note: Machine Name is a string of maximum 15 alpha-numeric characters. Space, special characters are not allowed.

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

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

Primary SMTP Authentication: To enable/disable SMTP Authentication.

Note: SMTP Server Authentication Types supported are:

- CRAM-MD5
- LOGIN
- PLAIN

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

Primary Username: Enter username to access SMTP Accounts.

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

Primary Password: Enter password for the SMTP User Account.

Note: Password must be at least 4 characters long.
Blank space is not allowed.
This field will not allow more than 64 characters.

Primary SMTP SSLTLS Enable: To enable SSL/TLS support for the SMTP Client.
Primary SMTP STARTTLS Enable: To enable STARTTLS support for the SMTP Client.

- **Upload SMTP CA Certificate File**: File that contains the certificate of the trusted CA certs. CACERT key file should be of pem type,LOGIN
- **Upload SMTP Certificate File**: Client certificate filename. CERT key file should be of pem type.
- **Upload SMTP Private Key**: Client private key filename. SMTP key file should be of pem type.

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

Secondary SMTP Support: It lists the Secondary SMTP Server configuration. It is an optional field. If the Primary SMTP server is not working fine, then it uses Secondary SMTP Server configuration.

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

Save: To save the new SMTP server configuration.

Procedure

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

Note: - Machine Name is a string of maximum 15 alpha-numeric characters. Space, special characters are not allowed.

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

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

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

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

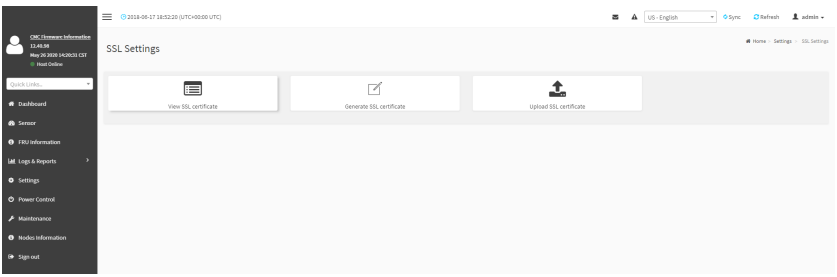
17. Click **Save** to save the entered details.

2-5-9 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 CMC Web GUI, configure SSL certificate into the CMC. 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.



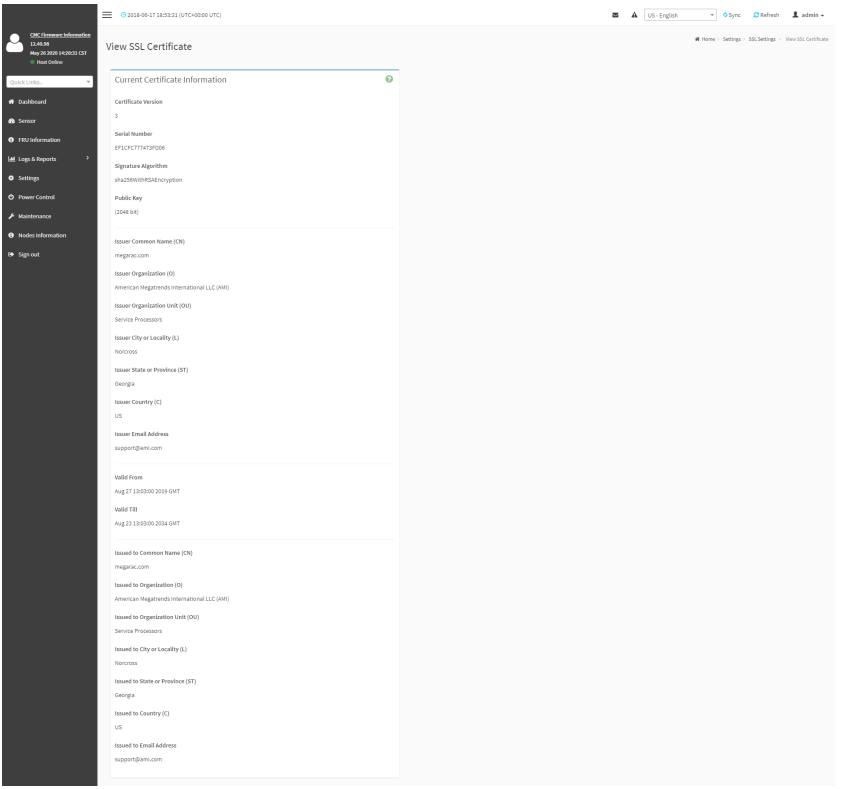
- **View SSL Certificate** option is used to view the uploaded SSL certificate in readable format.
- **Generate SSL Certificate** option is used to generate the SSL certificate based on configuration details.
- **Upload SSL Certificate** option is used to upload the certificate and private key file into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

View SSL Certificate

This section displays the basic information about the uploaded SSL certificate. It displays the following fields:

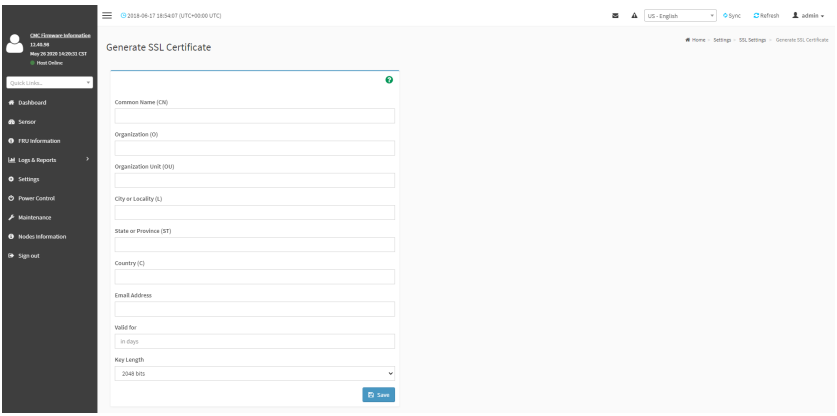
- Certificate Version
- Serial Number
- Signature Algorithm
- Public Key
- Issuer Common Name(CN)
- Issuer Organization(O)
- Issuer Organization Unit(OU)
- Issuer City or Locality(L)
- Issuer State or Province(ST)
- Issuer Country(C)
- Issuer E-mail Address
- Valid From
- Valid Till
- Issued to Common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

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



Common Name(CN): Common name for which certificate is to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization(O): Organization name for which the certificate is to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Organization Unit(OU): Over all organization section unit name for which certificate is to be generated.

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

City or Locality(L): City or Locality of the organization (mandatory).

- Maximum length of 128 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

State or Province(ST): State or Province of the organization (mandatory).

- Maximum length of 64 characters.
- It is a string of alpha-numeric characters.
- Special characters '#' and '$' are not allowed.

Country(C): Country code of the organization (mandatory).

- Only two characters are allowed.
- Special characters are not allowed.

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

Valid for: Validity of the certificate.

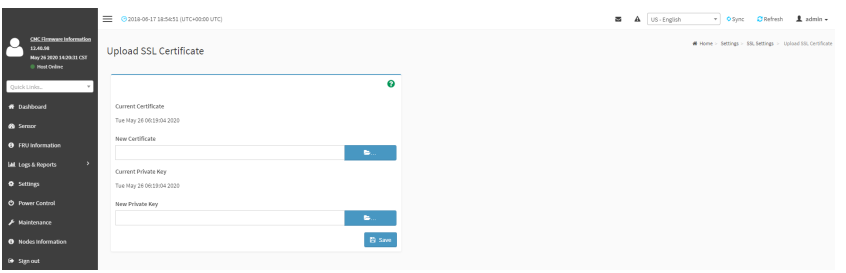
- Value ranges from 1 to 3650 days.

Key Length: The key length bit value of the certificate.
Save: To generate the new SSL certificate.

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

Upload SSL Certificate

This section is used to upload the certificate and private key file into the CMC.

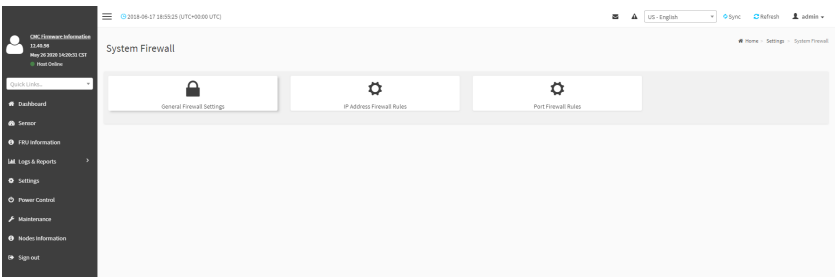


Current Certificate: Current certificate and uploaded date/time will be displayed (read-only).
New Certificate: Browse and navigate to the certificate file which should be of pem type.
Current Private Key: Current Private key information will be displayed (read-only).
New Private Key: Browse and navigate to the private key file which should be of pem type
Save: To upload the SSL certificate and privacy key into the CMC.

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

2-5-10 System Firewall

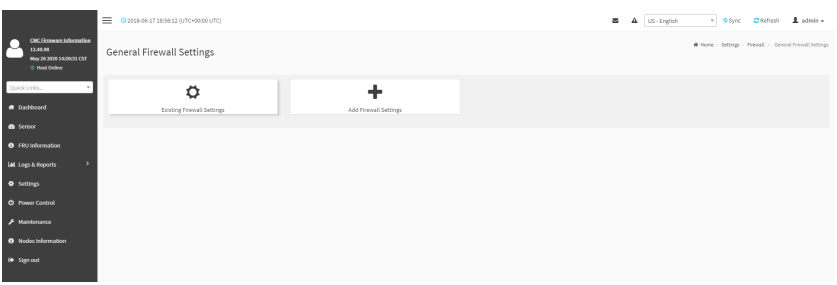
In CMC Web GUI, the System Firewall page allows you to configure the firewall settings. The firewall rule can be set for an IP or range of IP Addresses or Port numbers. To view this page, you must at least be an operator. Only administrators can add or delete a firewall.
To open System Firewall page,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



The fields of Firewall Settings tab are explained below.

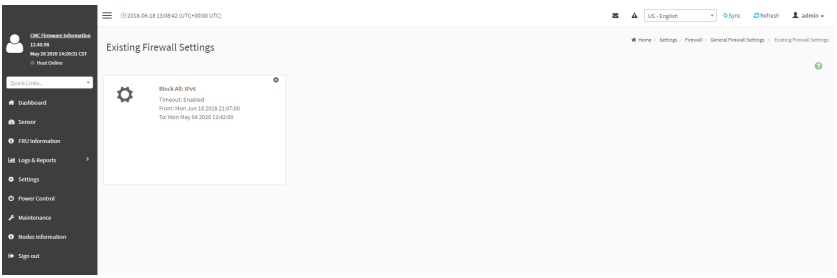
General Firewall Settings

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



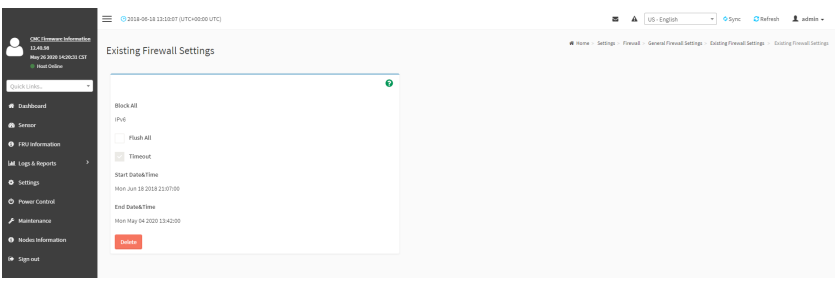
View Existing Firewall Settings

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



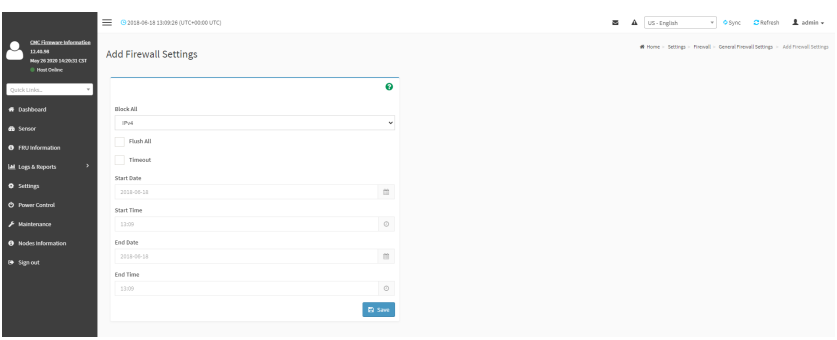
The Existing Firewall Settings page allows you to remove any particular Existing Firewall Settings.

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.



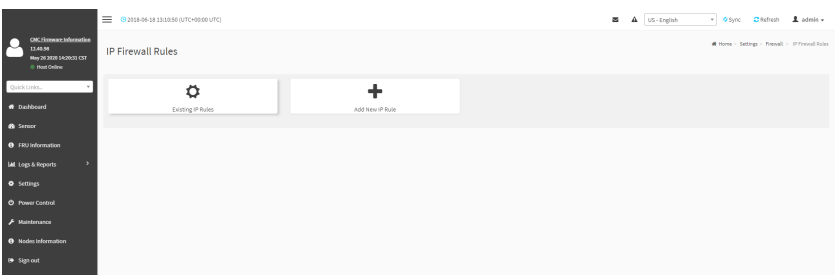
Block All: To block all the incoming IPs and Ports.
Flush All:To flush all the system firewall rules.
Timeout: To enable or disable firewall rules with timeout.
Start Date: The respective firewall rule effect will start from this date.
Start Time: The respective firewall rule effect will start from this 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.

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

Save: To save the changes made.

IP Address Firewall Rules

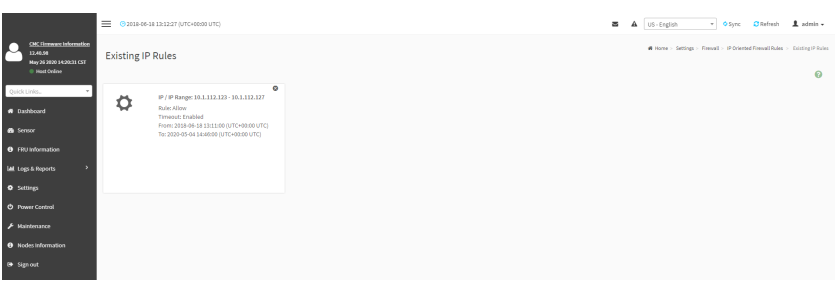
Click **IP Firewall Rules** page. A sample screenshot of IP Firewall Rules page is shown below.



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

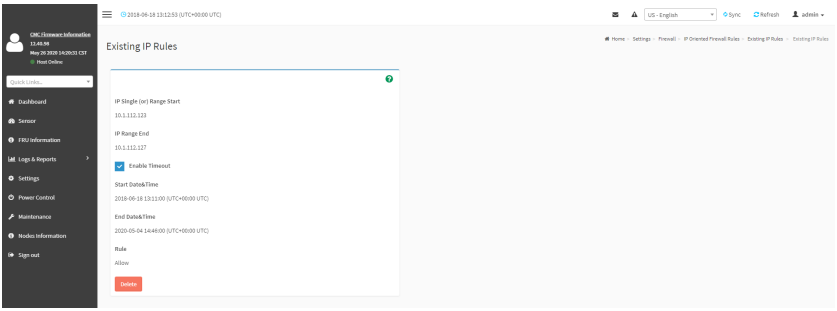
View Existing IP Rules

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.



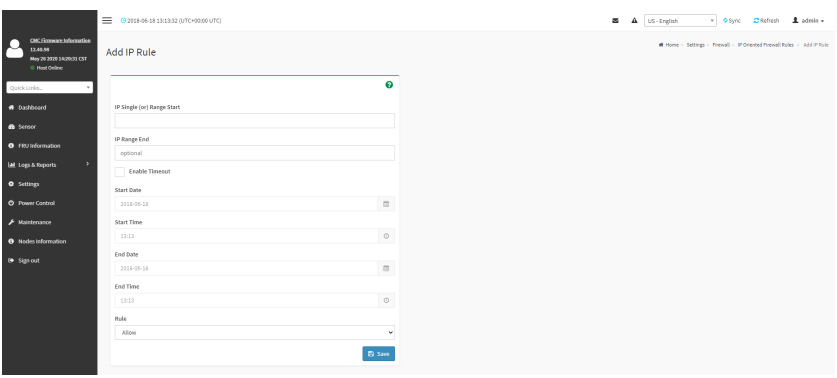
The Existing IP Rules page allows you to remove any particular Existing IP Rules.

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



Add New IP Rule

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



IP Single (or) Range Start: Configure the IP address or range of IP addresses.

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

IP Range End: Configure the IP range end of IP addresses.
Enable Timeout: Check this option to enable firewall rules with 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.

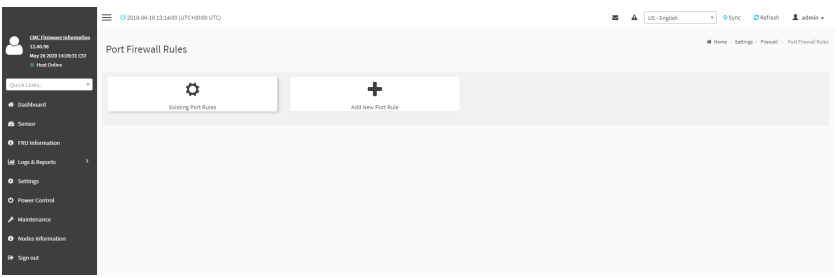
End Date: The respective firewall rule effect will end from this date.
End Time: The respective firewall rule effect will end from this time.

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

Rule: Determine the rule to **Block** or **Allow**.
Save: To save the changes made.

Port Firewall Rules

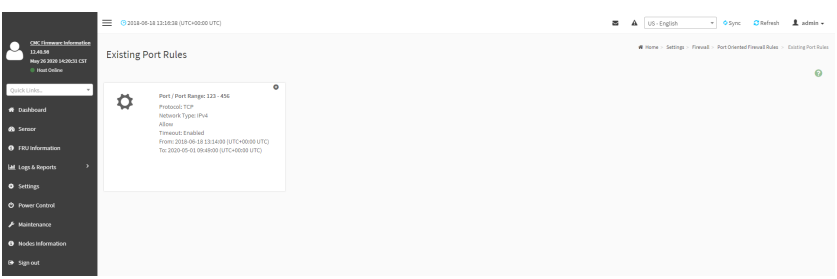
Click **Port Firewall Rules** page. A sample screenshot of Port Firewall Rules page is shown below.



The fields of Port Firewall Rules tab are explained below.

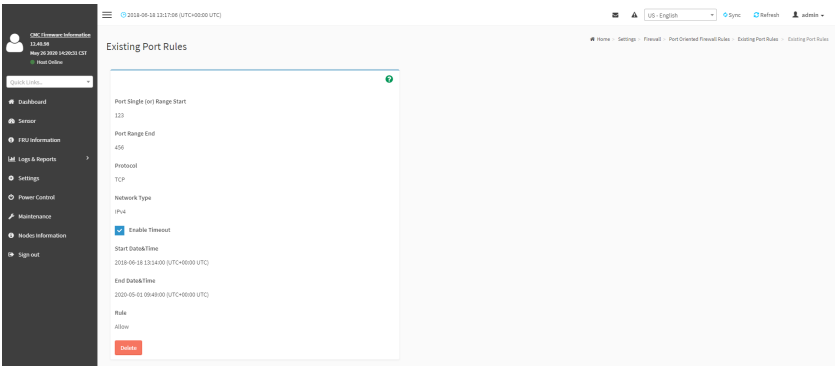
View Existing Port Rules

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



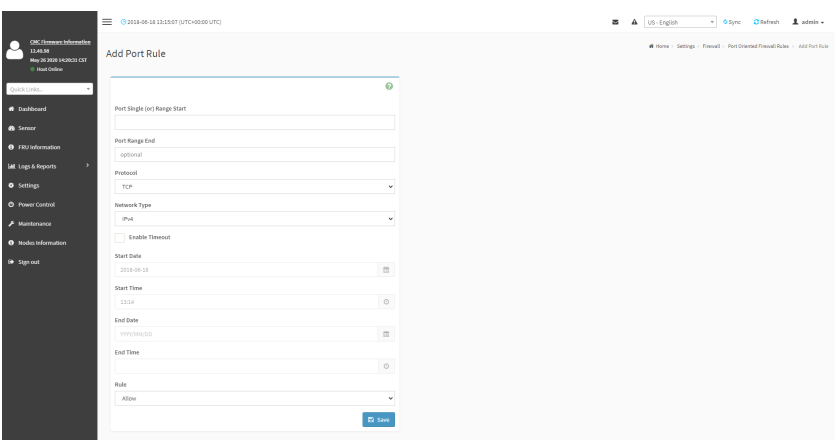
The Existing Port Rules page allows you to remove any particular Existing Port Rules.

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



Add New Port Rule

Click **Settings > System Firewall > Port Firewall Rules > Add New Port Rule** to add a new port rule



Port Single (or) Range Start: To configure the port number or a range of port numbers.
Port Range End: To configure the port range end of port numbers.
Protocol: This field specifies the protocols for the configured Port or Port Ranges.
Network Type: This field specifies the affected network type for the particular Port or Port Ranges.
Enable Timeout: To enable or disable firewall rules with timeout.
Start Date: The respective firewall rule effect will start from this time.

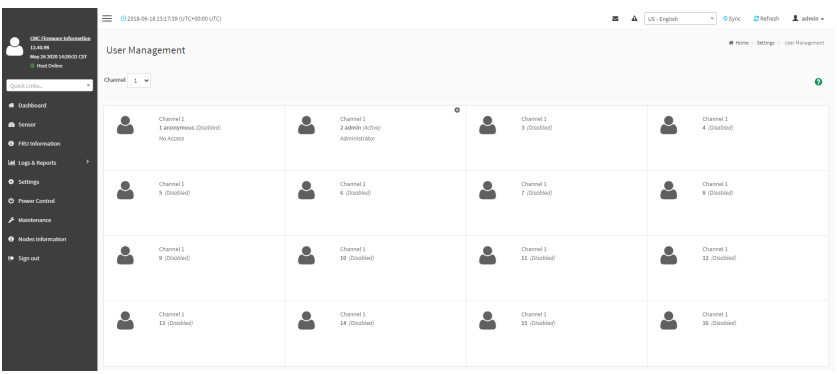
Start Time: The respective firewall rule will start from this time.
End Date: The respective firewall rule effect will end on this date.
End Time: The respective firewall rule will end at this time.

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

Rule: To indicate Allow or Block status.
Save: To save the changes made.

2-5-11 User Management

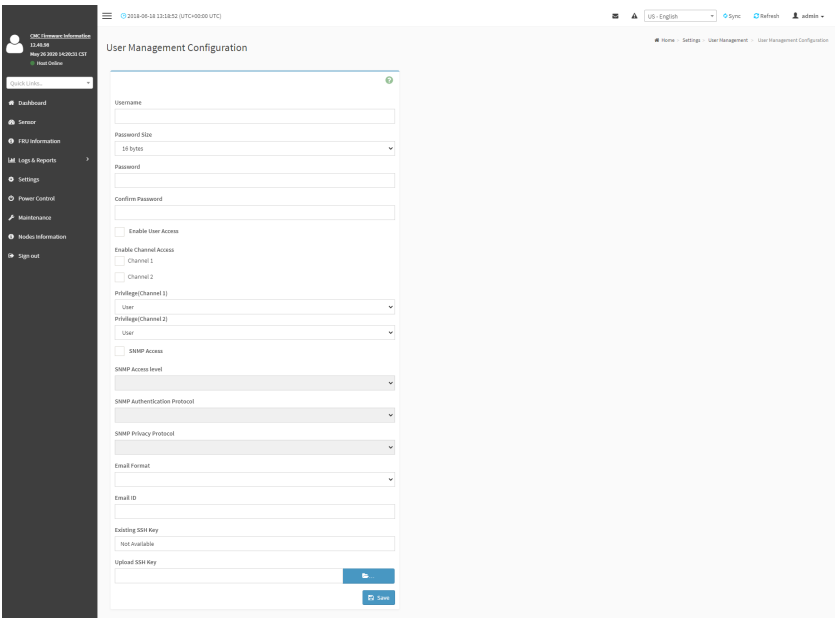
In CMC Web UI, the User Management page allows you to view the current list of user slots for the server. You can add a new user and modify or delete the existing users.
To open User Management page, click **Settings > User Management** from the menu bar. A sample screenshot of User Management page is shown below.



Procedure to add a new User

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

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



2. Enter the name of the user in the **Username** field.

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

3. Set **Password Size** for the new password.
4. In the **Password** and **Confirm Password** fields, enter and confirm your new password.

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

Hex	Char
00	NUL '\0'
01	SOH (start of heading)
02	STX (start of text)
03	ETX (end of text)

04	EOT (end of transmission.)
05	ENQ (enquiry)
06	ACK (acknowledge)
07	BEL '\a' (bell)
08	BS '\b' (backspace)
09	HT '\t' (horizontal lab)
0A	LF '\n' (new Line)
0B	VT '\v' (vertical tab)
0C	FF '\f' (form feed)
0D	CR '\r' (carriage ret)
0E	SO (shift out)
0F	SI (shift in)
10	DLE (data link escape)
11	DC1 (device control 1)
12	IDC2 (device control 2)
13	DG3 (device control 3)
14	DC4 (device control 4)
15	NAK (negative ack.)
16	SYN (synchronous idle)
17	ETB (end of trans. blk)
18	CAN (cancel)
19	EM (end of medium)
19	EM (end of medium)
1A	SUB (substitute)
1B	ESC (escape)
1C	FS (file separator)
1D	GS (group separator)
1E	RS (record separator)
1F	US (unit separator)
20	SPACE
7F	DEL

5. Enable or Disable the **Enable User Access** privilege.

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

6. Enable or Disable the **Enable Channel 1/2 Access**.

7. In the **Privilege (Channel 1)** and **Privilege (Channel 2)** fields, select the privileges assigned to the user which could be Administrator, Operator, User, OEM or None..
8. Check the **SNMP Access** check box to enable SNMP access for the user.
9. Choose the **SNMP Access level** for user from the drop-down list.
10. Choose the **SNMP Authentication Protocol** to use for SNMP settings from the drop down list.

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

11. Choose the Encryption algorithm to use for SNMP settings from the **SNMP Privacy Protocol** drop-down list.
12. In the **Email Format field**: 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.
13. In the **Email ID** field, enter the email ID of the user. If the user forgets the password, the new password will be mailed to the configured email address.

Note: SMTP Server must be configured to send emails.

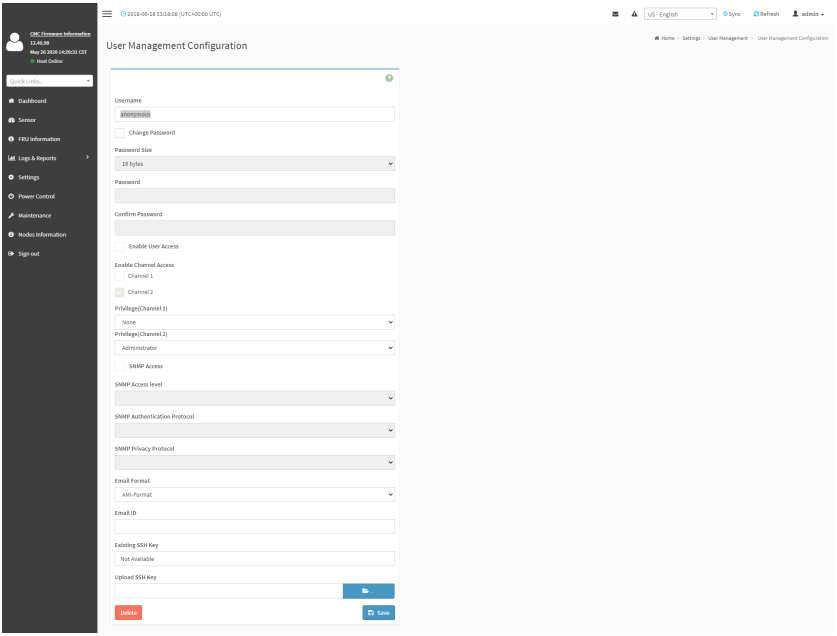
14. The **Existing SSH Key** field displays the uploaded SSH key information.
15. In the **Upload SSH Key** field, click Browse and select the SSH key file.

Note: SSH key file should be of public type.

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

To Modify User

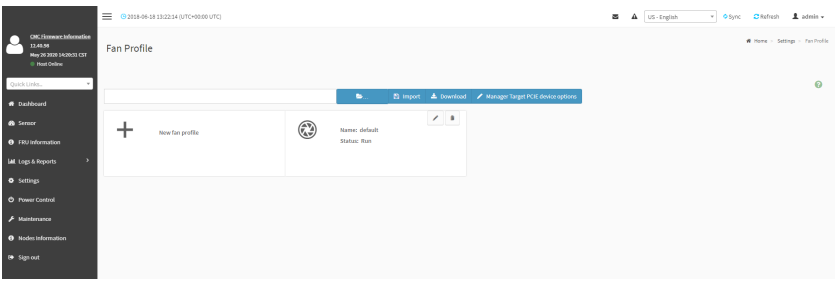
1. To modify the existing user, click on the active user tab. This opens a User screen as shown in the screenshot below.



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

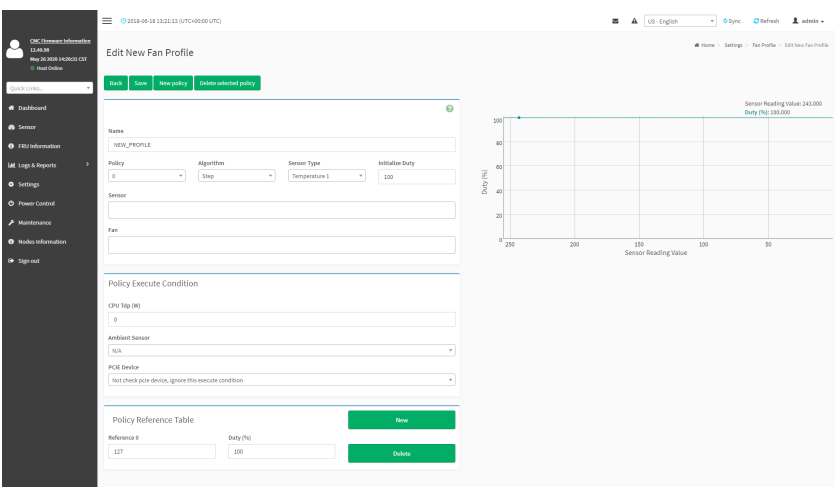
2-5-12 Fan Profile

This page is used to configure Fan Profile settings. To open Fan Policy page, click **Settings > Fan Profile** from the menu bar. A sample screenshot of Fan Profile page is given below.



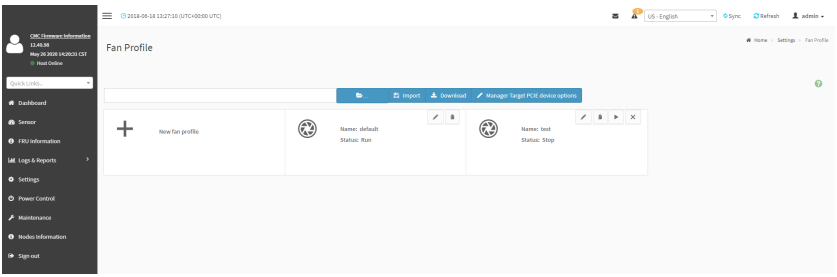
Import: To import the selected fan profile from the browse field.
Download: To download the selected fan profile.
Manager Target PCIE device options : To manage target PCIE devices.

Procedure to add New Fan Profile



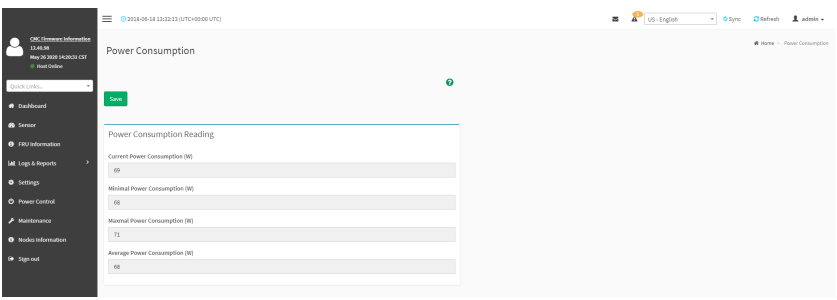
1. Name the the profile
2. Select the **Algorithm**.
3. Select **Sensor Type**, current or temperature.
4. Set the I**nitialize Duty**.
5. Select the reference device sensor.
6. Select the controlled fan.
7. Click **New** to a new policy reference table
8. Set reference temperature and fan speed duty

9. Click **Save** to save the configuration and return to **Fan Profile** main page.
10. Click arrow icon to run the fan profile.



2-5-13 Power Consumption

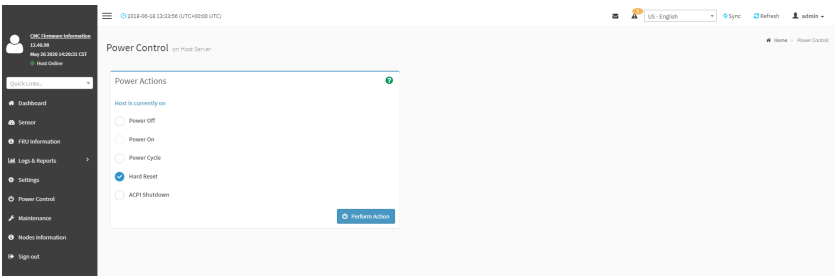
The Power Consumption is a simple display page for basic power consumption reading information. Item on this page are non-configurable.



2-6 Power Control

This page allows you to view and control the power of your server.

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



The various options of Power Control are given below.

Power Off: To immediately power off all server nodes.

Power On: To power on all server nodes.

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

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

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

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

Procedure

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

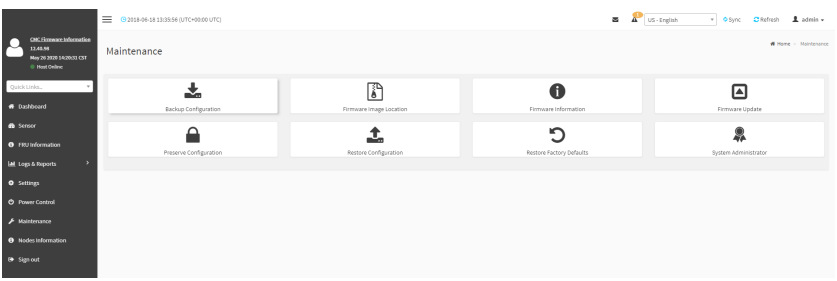
Note: During Execution you will be asked to confirm your choice. Upon confirmation, you will be informed about the status after few minutes.

2-7 Maintenance

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

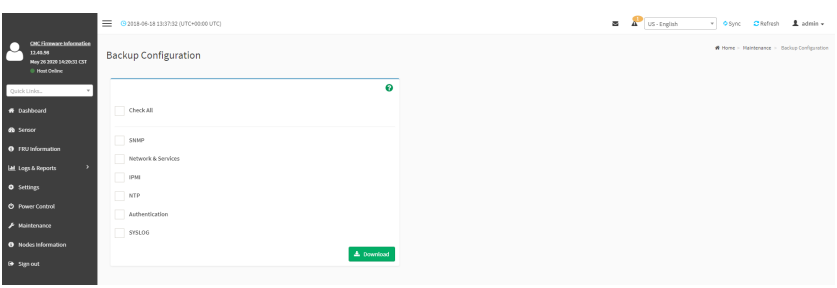
- Backup Configuration
- Firmware Image Location
- Firmware Information
- Firmware Update
- Preserve Configuration
- Restore Configuration
- Restore Factory Defaults
- System Administrator

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



2-7-1 Backup Configuration

This page allows you to select the specific configuration items to be backed up in case of “Backup Configuration”.
To open Backup Configuration page, click **Maintenance > Backup Configuration** from the menu bar. A sample screenshot of Backup Configuration page is shown below.



The various fields of Backup Configuration page are given below.

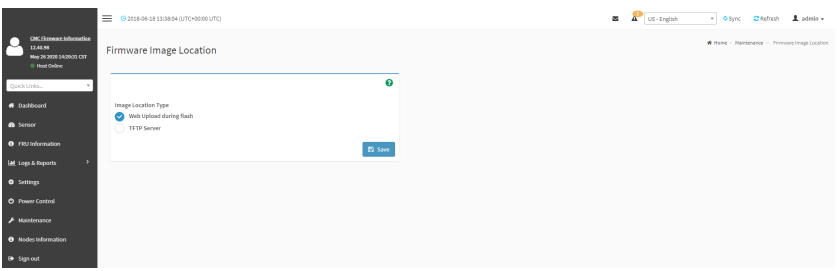
Check All - To select all the configuration list.
Download - To download and save the configuration files backup from CMC to client system.

Procedure

1. Click **Check All** to backup the selected configuration items. The Backup Configuration page will appear as shown above screenshot.
2. Click **Download** to save the backup file to the client system.

2-7-2 Firmware Image Location

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



The various options of Image Transfer Protocol are given below.
Image Location Type: Type of location to transfer the firmware image into the CMC either Web Upload during Flash or TFTP Server.
TFTP Server Address: Address of the server where the firmware image is stored.

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

TFTP Image Name: Full Source path with filename of the firmware image is stored on TFTP Server.
TFTP Retry Count: Number of times to be retried in case a transfer failure occurs. Retry count ranges from 0 to 255.
Save: To save the configured settings.

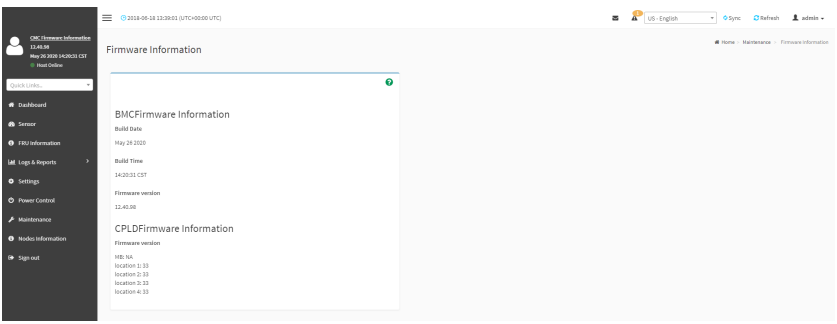
Procedure

1. Select the **Image Location Type (Web Upload during flash/ TFTP Server)**.
2. If the protocol selected is TFTP, enter the IP address of the server in the **TFTP Server Address** field.

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

2-7-3 Firmware Information

This page is used to display the current firmware information.
To open Firmware Information page, click **Maintenance > Firmware Information** from the menu bar. A sample screenshot of Firmware Information page is shown below.



The various fields of Firmware Information page are given below.
BMC Firmware Information:
Build Date: Describes the Build Date of the active BMC image.
Build Time: Describes the Build Time of the active BMC image.
Firmware version: Describes the Firmware version of the active BMC image.
CPLD Firmware Information:
Firmware version: Describes the CPLD Firmware version.

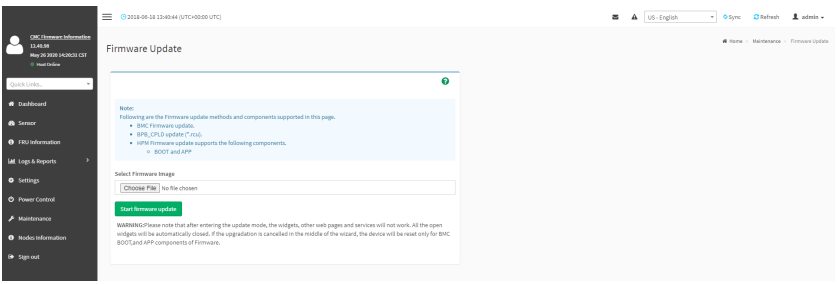
2-7-4 Firmware Update

This wizard takes you through the process of firmware upgradation. A reset of the box will automatically follow if the upgrade is completed or cancelled.

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

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

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



The various fields of Firmware Update are as follows:

- **Choose File**: To select the Firmware image to be uploaded.
- **Start Firmware Update**: To start the Firmware Update.

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

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

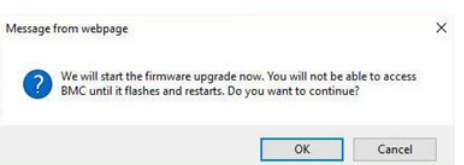
Procedure

The Firmware update undergoes the following steps:

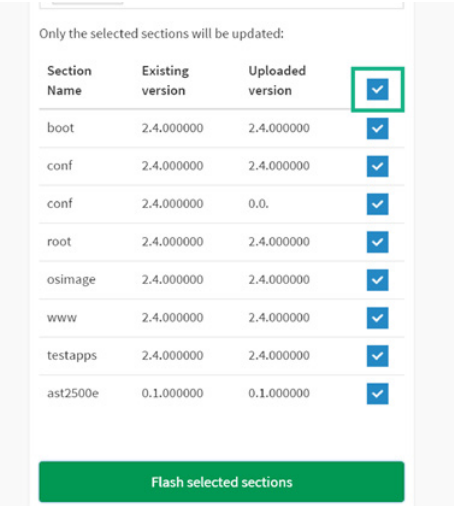
a) Closing all active client requests
b) Preparing Device for Firmware Upgrade
c) Uploading Firmware Image

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

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



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

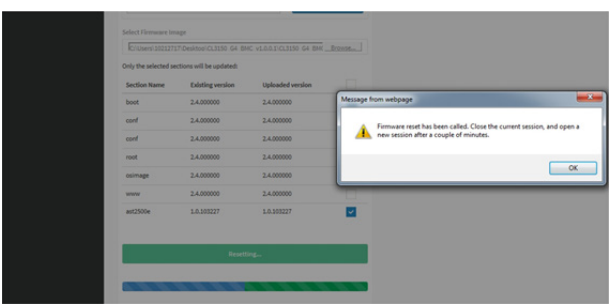


If only few module versions are different, those modules will be flashed.

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

h) Flashing Firmware Image.

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



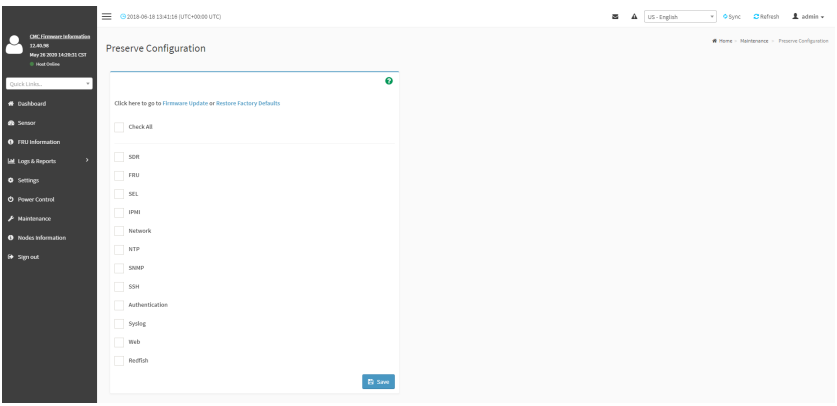
Note: The Firmware Update page will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the card's firmware. The device will reset if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

2-7-5 Preserve Configuration

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

To open Preserve Configuration page, click **Maintenance > Preserve Configuration** from the menu bar.

A sample screenshot of Preserve Configuration page is shown below.



The various fields of Preserve Configuration are as follows:

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

Check All: To check the entire configuration list.

Save: To save the current changes.

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

Files Preserved

SDR

Following files will be preserved:

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

Dependency Configurations - NIL

FRU

Following files will be preserved:

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

Dependency Configurations - SDR

SEL

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

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

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

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

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

Dependency Configurations - IPMI

IPMI

The following files are preserved in IPMI configuration:

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

Dependency Configurations - NIL

Network

To save network settings related with IPMI (LAN IP or DHCP configuration), select "IPMI" and "Network" options simultaneously. After restore configuration, the Network Configuration will be preserved successfully. Following files will also be preserved:

dhcp.conf: This file is to configure the host name in the FQDN format.

dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface, hostname: This file is used to store the Hostname of the BMC.

hostname.conf: This file is used to configure the host name creation method Manual/Automatic for the BMC.

Vlaninterfaces: This file helps to enable the vlan interface for the particular LAN interface

vlansetting.conf: This file is to store the vlan ID and Vlan priority for the particular VLAN interface entry.

bond.conf: This file is to enable the bond interface for the specified LAN interfaces.

Interfaces: This file is to configure the IP/IPV6 addresses for the LAN interface using static/ DHCP method.

activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.

hosts: This file is used to store the host name to map the IP address.

hosts.allow: This file contains the list of hosts that has permission to access the system

hosts.deny: This file contains the list of host that does not allow accessing the system

resolv.conf: This file is used to store the nameserver and domain name for hostname registration.

dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.

dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.

ncsicfg.conf: This file is to configure the NCSI related configurations.

nsupdate.conf: This file is to configure the channel ID, package ID for the NCSI interface.

phycfg.conf: This file is to configure the link speed, duplex and MTU value for the specified interface.

dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.
dns.conf: This file is used to configure the DNS registration method and DNS server for the particular interface.
hostname: This file is used to store the Hostname of the BMC.
hostname.conf: This file is used to configure the host name creation method Manual/Automatic for the BMC.
Vlaninterfaces: This file helps to enable the vlan interface for the particular LAN interface
vlansetting.conf: This file is to store the vlan ID and Vlan priority for the particular VLAN interface entry.
bond.conf: This file is to enable the bond interface for the specified LAN interfaces.
Interfaces: This file is to configure the IP/IPV6 addresses for the LAN interface using static/ DHCP method.
activeslave.conf: This file is to configure the active interface for the specified bond interface. This file depends on bond.conf.
hosts: This file is used to store the host name to map the IP address.
hosts.allow: This file contains the list of hosts that has permission to access the system
hosts.deny: This file contains the list of host that does not allow accessing the system
resolv.conf: This file is used to store the nameserver and domain name for hostname registration.
dhcp6c-script: This file is used to configure the domain name, DNS server IPv6 address and NTP address.
dhcp6c.conf: This file is to configure the IPv6 parameters for the DHCPv6 clients.
ncsicfg.conf: This file is to configure the NCSI related configurations.
nsupdate.conf: This file is to configure the channel ID, package ID for the NCSI interface.
phycfg.conf: This file is to configure the link speed, duplex and MTU value for the specified interface.
dhcp.preip_4: This file is to store the pre IPv4 address. This file will be created at runtime.

NTP

Following files will be preserved:
ntp.conf: This file contains the NTP dameon protocol configuration parameters such as synchronization sources, nodes and other related information
ntp.stat: This file contains the auto or manual network type protocols
adjtime: This file contains the time to synchronize the system clock
Localtime: This file is the system link to the file local time or to the correct time zone in the system timezone directly.
Dependency Configurations - IPMI

SNMP

Following files will be preserved:
snmp_users.conf: This file contains the SNMP user configurations such as user name and password encryption mechanism for the specific users.
snmpcfg.conf: This file contains the SNMP users privilege levels such as ro user and rw user.
Dependency Configurations - NIL

SSH

Following files will be preserved:

sshd_config: This file contains the keyword argument pairs of configurations such as Address family, Accept Env, Allow, users, authorized key files etc.

ssh_host_dsa_key, ssh_host_rsa_key: These files contain the private parts of the host keys.

ssh_host_dsa_key.pub, ssh_host_rsa_key.pub: These files contain the public parts of the host keys.

Dependency Configurations - NIL

KVM

Following files will be preserved:

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

stunnel.conf: This file contains the information about the stunnel configuration. It will also contain advisor and media server's secure port if secure connection is enabled.

usermacro.conf: This file saves the user defined macro from the jviewer.

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

Dependency Configurations - NIL

Authentication

Following files will be preserved:

activedir.conf: This file contains the configurations such as sslenable, timeout, racdomain, adtype, adfilterdc1, adfilterdc2, adfilterdc3, username, password, and rolegroup information such as name domain and privileges.

openLdapGroup.conf: This file contains the oprnm ldap role group information such as name domain and privilege.

nsswitch.conf: This file contains the sources to obtain the name service information in the range of categories and in what order

pam_withunix: This file contains the PAM Order of modules such as IPMI,LDAP, RADIUS and UNIX.

pam_wounix: This contains the PAM Order of modules such as IPMI, LDAP and RADIUS.

group: This file contains the Linux group. It stores the group information or defines the user group information in Linux.

passwd: This file contains the user login information for the Linux system

shadow: This file contains the encrypted password information for the clients.

ldap.conf: This file contains the ldap server configuration details such as bindn, binpw, pam_password, nss_reconnect_tries, port, port secondary, host, host secondary.

radius.conf: This file contains the radius server IP address, port number, secret, timeout, privilege etc.

Dependency Configurations – NIL

Syslog
System Event Log

Web
Web Settings

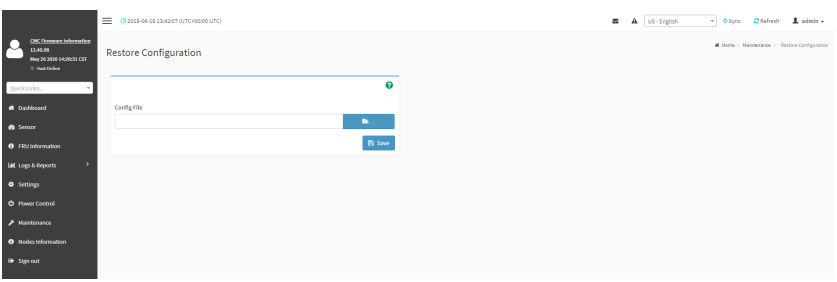
Redish
Redfish Audit Log

Procedure

1. Click **Firmware Update or Restore Configuration** link to view Firmware Update or Restore Configuration page accordingly.
2. Select the required Preserve Configuration items by either choosing the items individually by selecting the appropriate check boxes or by selecting all or none using **Check All**.
3. Click **Save** to save the changes.

2-7-6 Restore Configuration

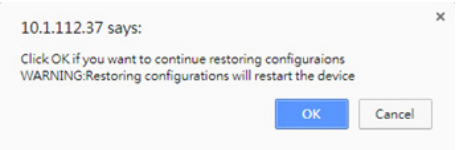
This page allows you to restore the configuration files from the client system to the CMC.
To open Restore Configuration page, click **Maintenance > Restore Configuration** from the menu bar. A sample screenshot of Restore Configuration page is shown below.



The various fields Restore Configuration page are given below.
Config File - This option is used to select the file which was backup earlier.
Save - To save the backup file to restore the backup files.

Procedure for Restore Configuration:

1. Click Browse to select the configuration file that needs to be backup and used to restore the configuration, when needed.
2. Click Upload to restore the backup files. The Restore Configuration page will appear as shown below.



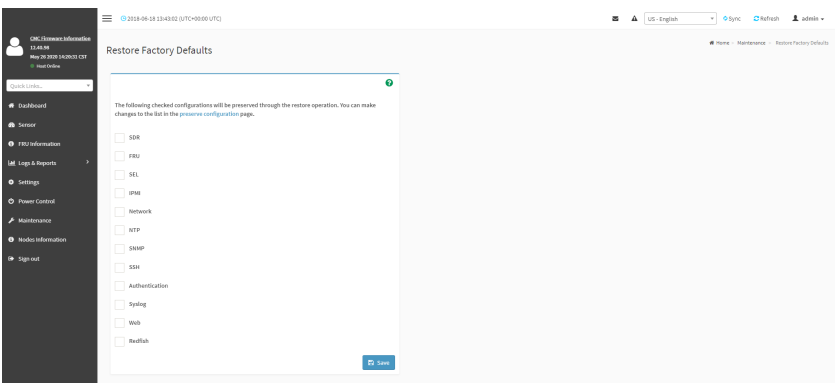
3. Click OK to upload the new configuration file and restore.

2-7-7 Restore Factory Defaults

In CMC Web GUI, this option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration.

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

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

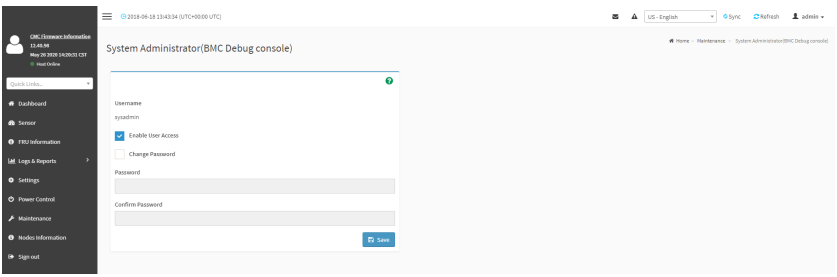


Procedure

1. Click **Preserve Configuration** to redirect to Preserve Configuration page, which is used to preserve the particular configuration not to be overwritten by the default configuration.
2. Click **Save** to restore the factory defaults of the device firmware

2-7-8 System Administrator

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



The various fields of System Administrator page are given below.
Username: Username of System Administrator is a read only field.
Enable User Access: To enable user access for system administrator.
Change Password: To change the user's password.

Note: This field will not allow more than 64 characters.
Password must be at least 8 characters long and blank space is not allowed.

Save: To save the new configuration for system administrator.

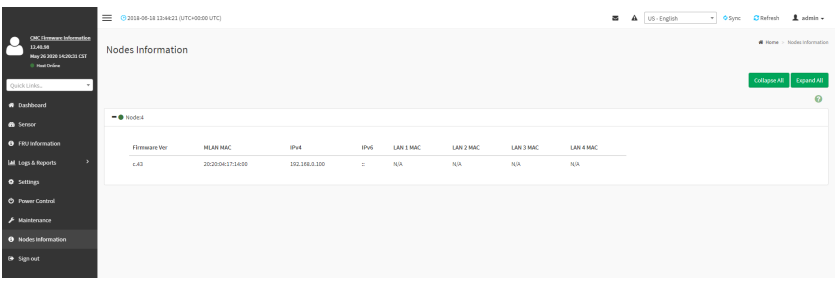
Procedure

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

2-8 Nodes Information

This page allows you to view the information for each node.

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



The fields of Nodes Information are as follows:

Collapse All/Expand All: To collapse/expand all lists.

Firmware Ver: Displays the firmware version of the node.

MLAN MAC: Displays the Management LAN MAC address of the node.

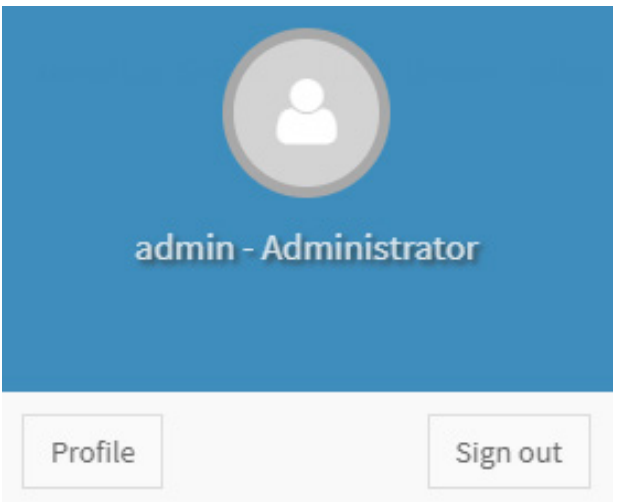
IPv4: Displays the IPv4 address of the node.

IPv6: Displays the IPv6 address of the node.

LAN1/2/3/4 MAC: Displays the LAN MAC address of the node.

2-9 Sign Out

To log out from the Web UI, 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 UI. A Warning message will be prompted you to proceed further, click **OK** to log out else **Cancel** to retain the Web UI.