# **GIGABYTE**<sup>™</sup>

## **Chassis Management Controller**

User Guide

Rev. 1.0

#### **Copyright**

© 2020 GIGA-BYTE TECHNOLOGY CO., LTD. All rights reserved. The trademarks mentioned in this manual are legally registered to their respective owners.

#### **Disclaimer**

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

#### **Documentation Classifications**

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

- User Manual: detailed information & steps about the installation, configuration and use this product (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. CMC 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	5
1-1 Supported Browsers	5
1-2 Gigabyte Management Console Network Configuration	6
1-3 Gigabyte Chassis Management Controller Web Console	8
1-3-1 Required Browser Settings:	8
1-4 Quick Button and Logged-in User	10
1-5 Help	11
1-6 Menu Bar	11
Chapter 2 Enter Gigabyte CMC Web Console	12
2-1 Dashboard	12
2-2 Sensor	
2-2-1 Sensor Detail	13
2-2-2 Sensor Events	14
2-3 FRU Information	15
2-4 Logs & Reports	17
2-4-1 IPMI Event Log	17
2-4-2 System Log	18
2-4-3 Audit Log	19
2-5 Settings	20
2-5-1 Date & Time	20
2-5-2 External User Services	
2-5-3 Log Settings	
2-5-4 Network Settings	
2-5-5 PAM Order Settings	
2-5-6 Platform Event Filter	
2-5-7 Services	
2-5-9 SSL Settings	
2-5-10 System Firewall	
2-5-11 User Management	
2-5-12 Fan Profile	
2-5-13 Power Consumption	66
2-6 Power Control	67
2-7 Maintenance	68
2-7-1 Backup Configuration	68
2-7-2 Firmware Image Location	69
2-7-3 Firmware Information	70

2-7	7-4	Firmware Update	70
2-7	7-5	Preserve Configuration	73
2-7	7-6	Restore Configuration	77
2-7	7-7	Restore Factory Defaults	78
2-7	7-8	System Administrator	79
2-8	No	des Information	80
2-9	Sig	ın Out	81

## 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.

	O 2021-03-11 08:58:13 (UTC+00:00 GMT)				S A US - English	■ Sync CRefresh L admin -
BMC Eimmware Information 12.41.10 May 26 2020 18.06.49 CST CMC IP	Dashboard Control Panel					Home - Dashboard
10.1.27.128 Host Online	0 d 0 <sup>hrs</sup>	19	I	4		
QuickLinks.	Power-On Hours	Pendir	ig Deassertions	Access Logs	More info O	
Dasnocard	0.54.0			-		
System Inventory	D Today (0)	Details	30 days (o)	Details	<ul> <li>Sensor Monitoring</li> </ul>	
FRU Information					All s	ensors are good now!
Logs & Reports					⊖ Currently recovered	
	No events for today		No events for last 30 days.			
Sottings						
Remote Control						
Image Redirection						
Power Control						
F Maintenance						
😔 Sign out						



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.

admin
US - English 💌
Remember Username
Sign me in
I forgot my 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:

	32018-06-18 12x88:57 (UTC+00:50 UTC)				= A	US - English • • Sync	CRefresh 🛓 admin •
CMC Firmware Information 12.41.54 Nay 26 2220 14:20(31 CST 9 Nati Ciview	Dashboard Control Panel						# Home > Dashboard
Quick Links.	0 d 0 hrs	3		<b>1</b> 9			
<ul> <li>Danhboard</li> </ul>	Power-On Hours	Pendir		Access Logs			
🙆 Semor			Nore Info O		More Info 🔾		
FRU Information	Today (2)	Details	30 days (1)	Details	Sensor Monitoring		
Lait. Logs & Reports >							
<ul> <li>Settings</li> </ul>					⊖ Currently recovered		
Power Control	power_supply		PS2	Status			
	3 events			vents			
Nockis Information							
🕪 Sign out							

#### 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.

G Critical Sensors (0)     Giscrete Sensor States (4)     Sensor Items     P F3_state		Out threshold sensors are normal State		
Discrete Sensor States (4)				
Sensor Name				
Sensor Name		State		
PS1_Status		State		
		Presence Detected		
B PS2_Status		Presence Detected, Power S	upply input Lost (AC/DC)	
■ SEL		No state defined		
Watchdog		No state defined		
-				
Normal Sensors (26)				
Sensor Name	Reading		Schavior	
+ ND01_CUR	0.00 Amps			
© ND01_PWR	8.00 Watts		<u></u>	
* NDQ2_CUR	0.00 Amps			
© ND02_PWR	4.00 Watts		M	
+ ND03_CUR	0.00 Amps			
© ND03_PWR	0.00 Watts			
1 NDM_CPU_DTS	50.00 °C			
1 ND04_CPU_TEMP	50.00 °C			
I NDM_CPU_VR_TEMP	36.00 °C			
+ NDO4_CUR	4.80 Amps			
I ND04_DHMM_TEMP	30.00 °C			
I ND04_GPU_PROC	0.00 °C			
1 ND04_MEM_VR_TEMP	39.00 °C		<b>`</b> ^	
1 ND04_PCH_TEMP	41.00 °C			
© ND04_PWR	60.00 Watts		~	
I PSU1_HOTSPOT	48.00 °C			
I PSU1_INLET_TEMP	28.00 °C			
I PSU2_INLET_TEMP	25.00 °C 12.29 Volts			
-+ P_12V -+ P_12V_STBY	11.29 Volts			
	11.89 VORS			
~ P_1V15_K0X	1.20 Volts			
~ P_2V5_AUX	2.44 Volts			
~ P_3V3_AUX	3.24 Volts			
~ P_NV_AUX	5.04 Volts			
+ sys_power	50.00 Wetts			
Disabled Sensors (42)				
XND01_CPU_TEMP	#NDI2_CPU_TEMP	NND03_CPU_TEMP	ж	ND01_GPU_PROC

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.

Sensor detail All information about this sensor	W Home > Sensor Reading > Sensor data
	0
□ PS1_Status Sensor Information	
0x8001	
Upper Non-Recoverable	NA
Upper Critical	NA
Upper Non-Critical	NA
Lower Non-Critical	NA
Lower Critical	NA
Lower Non-Recoverable	NA
	Change Thresholds



**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.

	9 2018-06-17 15:52:54 (UTC+00:00 UTC)				🛎 🛕 US-English v	● Sync   C Refresh   L admin •
CMC Firmware Information 12.48.98 May 26 2020 54/20/31 CST © Host Online	FRU Field Replacable Units					18 Hone - 177
Quick Units.	Available FRU Devices					
	FRU Device ID	1.*				
n Sensor	FRU Device Name	BMC_FRU				
FRU Information						
Mail Logs & Reports	Chassis Information		Board Information		Product Information	
O Settings	Chassis Information Area Format Version	1	Board Information Area Format Version	1	Product Information Area Format Version	1
	Chassis Type	Rack Mount Chassis	Language	0	Language	0
	Chassis Part Number	01234567	Manufacture Date Time	Fri Jan 7 00:00:00 2000	Product Nanufacturer	NULL
Nockes Information	Chassis Serial Number	01234567890123456789AB	Board Nanufacturer	NULL	Product Name	CNBH0G-00
😥 Sign out	Chassis Extra		Board Product Name	CNBH0G-00	Product Part Number	00000000001
			Board Serial Number	0123456789012345678948	Product Version	0100
			Board Part Number	01234567	Product Serial Number	01234567890123456789AB
			FRU File ID		Asset Tag	01234567890123456789AB
			Board Extra	NULL	FRU File ID	
					Product Extra	

The following fields are displayed here for the selected device:

#### Available FRU Devices

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

#### **Chassis Information**

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

#### **Board Information**

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

#### **Product Information**

- Product Information Area Format Version
- Language
- Product Manufacturer
- Product Name
- Product 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.

	O 2008-06-17 35(:452 (UTC+0000 UTC)	🐻 🏔 US-English * 0 Sync Dilettesh 🏦 admin -
CMC Homeson Information 22.45.Ml Hey 25 2020 14:29:21 CF © Host Online	Event Log Attacks event logs	a new - bosto
QuickLinks. • • Dashboard • Sensor	Nitiser by Easts 13775-65-64 05000 O 2013-66-17 13556 O Nitiser by Hype All Diverses	AltSenson
		Event Log 3 (+-3 )
PHI Event Log     System Log     Audit Log     Settimes		Ko 2000     Ko 2000, Status sensor of type power_supply logged a BMC Event : Power Supply Input <sup>0</sup> 2 years applied (U/C) was assented
<ul> <li>Secongs</li> <li>Power Control</li> <li>Haintenance</li> </ul>		10: 2 PS2_Status sensor of type power_supply logged a BMC Event : Presence detected 02 yron op- was asserted
<ul> <li>Nodes Information</li> <li>Sign out</li> </ul>		Bit 1951_Status sensor of type power_supply logged a BMC (went : Presence detected 02 yrisin ap- was asserted
	a Anny 2011	٥
	Event Logs Statistics	

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.

	© 2018-06-17 350347 (UTC+0600 UTC)	2 /	US - English	* • Sync	C Refresh	1 admin -
CMC Elementes information 1240.04 May 26 2020 14:20:21 CST 9 Host Civiline	System Log Nitystem event logs				4 H	ome > SystemLog
Qatck Linici						0
<ul> <li>Dashboard</li> <li>Sensor</li> </ul>	Filter by Date 1375 01 01 0500 0 2208-05-17 10:00 0 Event Category Airst v Page 1 v					
FRU Information				<b>≜</b> Down!		
Lad. Logs & Reports 🛛 👻	Event Log: 2 ( 0 - 2 )			2000	oas toga	
<ul> <li>IPNI Event Log</li> <li>System Log</li> </ul>	June 2014					
AuditLog	C: 12018-06-1618:29:11 (UTC+00:00 UTC) AMIB42E99BEF9AB kernel: kernel [5.840000] Helper Module Driver Version 1.2-					
O Settings	D: 2 2018-06-16 18:29:11 (UTC+00:00 UTC) AMIB/42E998EF9AB kernel: kernel: - [5.840000] Copyright (c) 2009-2015 American Megatrends Inc					
O Power Control	0					
Nodes information						
🕒 Sign out						

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.

	🗮 ©2016-06-17 1603209 (vTC+0000 uTC) 🗶 🛦 (v5-1rglinh * ) 05/vC C2	Refresh 💄 admin +
CMC Timment Information 12.40.56 May 35 2000 14:28:211 CST • Incet Celline	Audit Log Hauthtap	# Home > Auditlog
Cashboard     Sensor	Pfler by the 30 to 4 1 4000 0 - 2010 0 4 1 402 0 Pape 1 v	
FRU Information     Lags & Reports     ·	Levertug: (1 (+18)	p.
<ul> <li>IPMI Event Log</li> <li>System Log</li> <li>Audit Log</li> </ul>	See 2015	
Settings     Power Control	10: 32 028-06-17 15-0632 (UTC-00:00 UTC) AMI8-12596E794B: spc, restaurilos: spc, restaurilos:	
<ul> <li>Maintenance</li> <li>Nodes information</li> </ul>	Cr. 3 2018-06-17 14-08:18 (UTC-40:00 UTC) AMBR42998EF988 spt_ressurvice: spt_restervice:[2964-12964 WWRMING)HTT5 session timeout from P1:01.2.121 user-admin-     Cr. 7 2018-06-17 14-14:31 UTC-40:00 UTC) AMBR42998EF988 spt_ressurvice: spt_restervice:[2964-12964 WK7MING)HTT5 session timeout from P1:01.2.121 user-admin-     Cr. 7 2018-06-17 14-14:31 UTC-40:00 UTC) AMBR42998EF988 spt_ressurvice: spt_restervice:[2964-12964 WK7MING)HTT5 session timeout from P1:01.2.121 user-admin-     Distribution timeout from P1:01.2.121 user-admin-	
e Signout	ID: 6 2010 60-16 22-20132 (UTC-9000 UTC) ANDR-02598EFBAB logic(3147) login 3147- (3147 3148 WARNINGSERAL session timeout from IP-3277.0.0.1 user-systemin-	
	0.5.2018-06-18/2221-08 (UTC-V000 UTC) ANIBALEEMBETABL Sign_restantions sign_restantions - [2064-1294 INARINNO]INTTP5 session timeout from P13.1.27.138 useradmin-     0.4.2018-06-18/222012 (UTC-V000 UTC) ANIBALEEMBETABL Sign_restantions-     10.4.2018-06-18/222012 (UTC-V000 UTC) ANIBALEEMBETABL Sign_restantions-     10.4.2018-06-18/22018 (UTC-V000 UTC) ANIBALEEMBETABL Sign_restantions-     10.4.2018-06-18/22018 (UTC-V000 UTC) ANIBALEEMBETABL Sign_restantions-	_
	Ib: 3 2018-06-16 32:18:30 (UTC-00:00 UTC) AMB/02298689888 login(3147) login 3147-(3147) INFO)SERAL login from IP:327.00.1 user:sysadmin-	

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.

	3018-06-17 16:04:46 (UTC+00:00 UTC)		<b>z A</b> U	S-English • OSync ORefresh 🛓 admin •
CHC Elemente information 12.46.56 May 26 2020 14.28.03 CST Not Online	Settings Configure BMC options			W Hane > Settings
Quick Links. v	Dane & Time	External User Services	Log Settings	Network Settings
Sensor     FRU Information	PAM Order Settings	Platform Event Filter	OS Services	SMTP Settings
M Logs & Reports >	SSL Settings	System Firewall	Luser Management	Fan Profile
<ul> <li>Maintenance</li> <li>Nodes Information</li> </ul>	Power Consumption			
Թ Sign out				

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.

	O 2018-06-17 16:05:23 (UTC+00:00 UTC)		s .	▲ US-English • Sync CRefresh & admin •
CHC. Ensures information 12.40.50 May 26 2020 14/20/31 CST 0 Hast Online	External User Services			# Home - Settings - External User Services
QuickLinks.	LDAP/R-Directory Settings	Active Directory Settings	Rubus Settings	
O FitU Information				
Settings     Power Control				
<ul> <li>Maintenance</li> <li>Nodes Information</li> <li>Sign out</li> </ul>				

#### 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.

	O 2018-06-17 16/37/30 (UTC+00:00 UTC)	
CHC Firmmer Information 12.40.04 May 26 2020 14/20:31 CST    Host Online	General LDAP Settings	
QuickLinks.		0
	Enable LDAP/E-Directory Authentication	
Sensor	Encryption Type	
• FRU Information	No Encryption     SSL     SLertTLS	
Left togs & Reports	Common Name Type	
Settings	Server Address	
	Jerrer Moureus	
O Power Control	Part	
	389	
Nodes Information	Bind DN	
	E.g., chradmin,ourlogin,dicrdomain,dicrcom	
	Password	
	Whitespace not allowed	
	Search Base	
	E.g., ouHogin,dc+domain,dc+com	
	Attribute of User Legin	
	ch.	~

2. Click Enable LDAP/E-Directory Authentication, to enable LDAP/E-Directory Settings. Select the Encrytion Type for LDAP/E-Directory: No Encrytion, 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'.

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.

 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.

	G 2018-06-17 16:11:14 (UTC+00:00 UTC)		z 🕫	US-English • OSync ORefresh 1 admin •
CMC:/innware.information 12.48.56 Ney 20 2020 14:20:33 CST Heart Online	Role Groups		đi hor	ne – Settings – External User Settings – LDAR/E Olivectory Settings – Role Groups
Quick Links. • • Duchboard • Sensor	None	None	Nore	Nerve
FRU Information      ML Logs & Reports      Settings	Nore			
<ul> <li>Power Control</li> <li>Maintenance</li> </ul>				
<ul> <li>Nodes Information</li> <li>Sign out</li> </ul>				

#### 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.

	O 2018-06-17 16:12:53 (UTC-60:00 UTC)	
Off. firmware Information 12.46.00 Hey 25 2000 14.20121 CST © Head Online	Role Groups	
Quick Links.		Θ
# Dashboard	Group Name	
Sensor		
FIU Information	Group Domain eg., dc=domain	
	Group Prhillege	
O Settings		~
O Power Control		D Save
🗭 Sign out		

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.

	(0.2018-06-17.3613(34 (UTC+00.00 UTC)	🛎 🎥 us-English 🔹 O Sync 🛛 Refresh 💄 admis +
CMC.Fitzmance.Information 12.48.98 May 26 2020 14/20133 CST Host Online	Active directory Settings	# Hane - Settings - Diternal User Settings - Active directory Settings
Quick Linka.	M .	
# Dashboard	General Settings Role Groups	
a Sensor		
FRU Information		
😹 Loga & Reports 🔷		
O Settings		
O Power Control		
Nodes Information		
🕒 Sign out		

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.

	Colle 65-12 31:33:30 (UTC+00:00 UTC)	🕿 🎤 US-English 🔹 ØSyre
OHC Flowware informatio 12.40.65 Apr 9.2020 15(1):13 CST © Nost Online	General Active Directory Settings	# None - Settings - Edennilitier Settings - Active directory Settings
Quick Links	0	
	Enable Active Directory Authentication	
b Sensor	554.	
FRU Information	Secret Username	
Settings	Secret Password	
Remote Control	User Domain Name	
	Domain Controller Server Address 1	
Nodes Information	Damain Controller Server Address 2	
	Damain Controller Server Address 3	
	URINARI LERIZORE SETVER ADDRESS 3	
	52 See	

 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". 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.

		≡	32018-06-17 16:12:53 (UTC=00:00 UTC)	
$\sim$	CMC Limment Information 12,45,54 May 25 2000 14,20(21 CST in Heat Online	R	ole Groups	
Quick	Linka. •			0
<b>4</b> 0x			Group Name	
<b>a</b> 50			Group Domain	
<b>0</b> 113			eg, de=domain	
Let Let	p&Reports >		Group Privilege	
• se				~
				E) Save
	interance			
0 No				
9.5				

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.



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.

	@ 2018-06-17 16:10:57 (UTC+00:00 UTC)		
CMC.firmware.information 12.44.94 May 26 2220 14 20:33 CST	General RADIUS Settings		
HestGeline     QuickLinks.     V		θ	
	Enable BADIUS Authentication		
Series	Server Address		
FRU Information	Port		
lad Logs & Reports >	1812		
O Power Control	Secret		
⊁ Maintenance		10 Save	
Nodes Information			
🕒 Sign out			

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.

	O 2008-06-17 10:21:27 (UTC+00:00 UTC)		🕿 🎤 us-English 🔹 ©Sync
CHC. Humaner Information 12.40.54 May 26 2000 14:20:31 CST U Host Online	Advanced RADIUS Settings		W Home > Settings > Econval User Settings > AUDUS Setting
ktinks. •	RADIUS Authorization	Θ	
	Administrator		
	Head		
	Operator		
	H*3 User		
	H+2		
	OEM Proprietary		
	H+1		
is information	No Access		
	HID	E2 Save	



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.

	O 2018-06-17 18:22:38 (UTC+00:50 UTC)		2	🖉 US - English 🔹 🗢 Syr	c 😋 Refresh 💄 admi
CHC Elements Information 12.43.04 May 26 2020 14:20:21 CST 0 Host Online	Log Settings				<b>el</b> Hame > Settings > LogSe
Quick Units.	SEL Leg Sktörgs Palky	Advanced Log Settings			
B FRU information     Mat Logs & Reports					
Settings     Power Control					
<ul> <li>Maintenance</li> <li>Nodes information</li> </ul>					
🕒 Sign out					

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.

	O 2818-06-17 2622324 (UTC-0000 UTC)
CMC firmware information 12.44.58 May 26 2020 14:20:31 CST	SEL Log Settings Policy
Host Online	
Quick Units.	0
<ul> <li>Dashboard</li> </ul>	Log Policy Unear Storage Policy 🥑 Circular Storage Policy
Senor     FRU Information	🕲 Save
Latt Logs & Reports	
O Settings	
Power Control	
Maintanance	
Nodes Information	
🖶 Sign out	

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.

	G 2818-06-17 18:20:49 (UTC+00:00 UTC)
CMC. Einmeane: Information 12.44.54 May 20 2020 14:20:33 C37 0 Host Online	Advanced Log Settings
Qalck Linka.	0
# Dashboard	System Log
da Seroor	V LocalLog
FBU Information	Remote Log
🕍 Loga & Roports 🔷	Part Type TCP
O Settings	The Size
O Power Control	5000
✗ Maintenance	Retate Count
Nodes Information	•
🕞 Sign out	Remote Log Server
	Server IP or Hostname
	Remote Server Port
	Enable Audit Log
	E) Save
	EX Save

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.

- 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.

	G 2018-06-17 18:30:06 (UTC+00:00 UTC)	S A Us-English • \$ Sync Skefrech 1 admin •
CMC Fitzmenze Information 12.48.54 May 20 2220 14/20:33 CST • Host Online	Network Settings	# Reve - Setting - Related Setting
Quick Links. *		
# Dashboard	Network IP Settings DNS Configuration	
Serocr		
FRU Information		
🕍 Logs & Reports 🔹 👌		
• Settings		
O Power Control		
Nodes Information		
Ger Stign out		

#### 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.

Research Advectory We have a second advectory We have a second advectory Method a	O 2018-06-27 18-41-18 (UTC+00:50 UTC)		S A US-English • OSymc Sike
Att       Attorner         Attorner       Index         Attore       Index			
ad   ad   ad   addutt   band   band <td>Network IP Settings</td> <td></td> <td># Home &gt; Settings &gt; Nets</td>	Network IP Settings		# Home > Settings > Nets
Image:	nis. •	Ø	
Image: market in the second	Bound Enable LAN		
<pre>status status stat</pre>	LAN Interface		
Note:       I Subscription	bend0	~	
<pre>statestimation statestimation s</pre>	NAC Address		
audi	84209980F9A8		
Number Providence Conserved Co			
untervalue     PP 4 Maile       u     12 12 12 12       urst value     12 12 12 13       urst value     13 12 12 13       urst value     13 12 13 <tr< td=""><td>Enable IPvI DHCP</td><td></td><td></td></tr<>	Enable IPvI DHCP		
13.27.23       13.27.23       12.27.23.35       12.27.23       12.27.23       12.27.23       12.27.23       12.27.23       12.27.23       12.27.23       12.27.23       13.27.23       14.27.23       15.27.23       15.27.23       16.27.24       17.27.24       18.27.24	and the second se		
In Version   In Version   In State Productor	10.1.27.128		
Productionary   Table Trade			
SALATION         Image: Control of Control	255,255,255,0		
Cable Nd Cable Nd CD Pol Inder Nd Admas Cable OrdCauge Cable OrdCa	IPot Gatescay		
	10.1.27.253		
Préd Indea 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0			
0       Privi Admini       2       Statuta The Largetti       0       0       0       0       0       0       0       0       0       0       0       0       0       0	Enable IPv6 DHCP		
Proj Adorea a back Profile angle a catalon SLAD VAR D a VAR Ponty			
s sudors Profile Legels		*	
Solver Finite Leggitt 0 Contact Yular VAN 10 0 VAN Plotty			
s cation Kual kual kual kual kual kual kual kual k			
Catala XLAN VLAN D 0 VLAN Pónthy			
VAR 0 a CAR Houty			
s NAN Honing	Enable VLAN		
VLAN Priority			
	0		
9			
	0		

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.

#### **CMC Registration Settings**

**CMC Interface**: Options to register the CMC through the Interfaces. **Register CMC**: To register CMC through registration method.

#### **Registration Method**

Options to register the CMC 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 CMC.



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 CMC, choose the CMC's network port to register with DNS settings.
- 5. Check Register CMC 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.
- 7. In **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 CMC.
- 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:

	G 2018-06-17 16H43.52 (UTC-0000 UTC)
CMC Timmware Information 12.40.94 Nay 35 2020 14.28:21 CST 9 Heat Colline	PAM Order
Quick Links.	0
Dashboard	PAM Authentication Order
<ul> <li>Sensor</li> <li>FRU Information</li> </ul>	IPMI
Latt Logs & Reports >	LDAP
O Settings	ACTIVE DIRECTORY
Power Control	RADIUS
₣ Waintenance	🔁 Saw
Nodes Information	
🕒 Sign out	

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

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



 $\label{eq:Note: It is recommended to not to keep same username for different PAM modules.$ 

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.

OK Shmeers Informative	○ 2018-06-17 18>49:10 (UTC+00:00 UTC)					S A US-English		-
	ent Filters						# Home > Settings > Platform Event Filte	a - tvetfi
icktinks. 🔹 🗢	All 🔹 Configured 🗆 UnConfigured							
Dashboard Sensor FRU Information Logs & Reports	PEF ID: 1 (Enabled) when All Sensors switches to critical state meas	•	PEF Rb: 2 (Enabled) when All Sensors sentitives to non-critical state none	•	PEF ID: 3 (Enabled) when All Sensors switches to critical state mone	°►	PEF ID: 4 (Enabled) When All Sensors switches to non-critical state none	
Settings Power Control Maintarcance	PEF NC 5 (Enabled) when All Sensors switches to critical state nece	° 🕨	PEP ID: 6 (Znabind) when All Sensors sentches to non-critical state none	° 🕨	PEF HD: T (Enablied) when All Sensors switches to critical state none	° 🕨	PEF ID: 8 (Enabled) when All Sensors switchs to non-critical state none	
Nodes Information	PEF IRC 9 (Enabled) when All Sensors switches to critical state neee	° 🕨	PEF ID: 10 (Enabled) when All Sensors sufficies to non-critical state mone	° 🕨	PEF ID: 11 (Snabled) when All Senaors switches to critical state mone	• ►	PEF ID: 12 (Enabled) when All Sensors switchs to non-critical state none	
	PEF IR: 13 (Enabled) when All Sensors switches to critical state nerve	° 🕨	PEF ID: 14 (Enabled) when All Sensors matches to critical state mone	° 🕨	PEF ID: 15 (Enabled) when All Sensors switches to critical state none	0		

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.
- 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.

	O 2008-06-17 10:46041 (UTC+00:00 UTC)	🛎 🔺 US-English	▼ Sync CR
CMC Formate Information 12.40.M May 26 2020 14 20:31 CM	Event Filter Configuration	<b>el</b> Homa > Settings > Pla	forn Event Filters > Event Filters
Host Online	0		
ickunis. •			
Dashboard	V Enable this filter		
Sensor	Event severity to trigger Critical state		
FBU Information	Event Filter Action Alert		
Logs & Reports	Power Action		
Settings	None v		
Power Control	Alert Policy Group Number		
laintenance	1		
iodes Information	Raw Data		
lign out	Generator ID 1		
age to day	Diff		
	Generator ID 2		
	6477		
	Generator Type		
	Slave Software		
	Slave Address/Software ID		
	Channel Number		
	0 <b>v</b>		
	IDME Device LUN 0 V		
	Sensor type Temperature		
	Sensor name		
	All Sensors v		
	Event Options		
	Sensor Events v		
	Sensor Events		
	Event trigger		
	255		
	Event Data 1 AND Mask		
	0		
	Event Data 1 Compare 1		
	255		
	Event Data 1 Company 2		
	Event Data 2 AND Mask		
	•		
	Event Data 2 Company 1 255		
	Event Data 2 Compare 2		
	v Event Data 3 AND Mask		
	Event Data J AND Mack		
	Event Data 3 Compare 1		
	255		
	Event Data 3 Company 2		
	¢		
	Codeta Di Save		

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.

	<b>≡</b> <sup>(9</sup> 2018-0)	8-17 18-47:18 (UTC+00:00 UTC)						=	<b>A</b> [	IS - English	<ul> <li>◆ Sync</li> <li>⑦ Refresh</li> <li>▲ admin +</li> </ul>
CMC Firmware information 12.44.98 Nay 26 2020 14:20:33 CST	Alert Poli	cies									Home > Settings > Partnern Event Filters > Alext Policies
Quick Units. • Dathboard Sensor	¢	Group: 1 (Duckled) Always send alert to this distination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 2 (Dirabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Group: 3 (Dischled) Always send alert to this destination UNI Channel: 1 Sent To: 0	۰	¢	Greuge 4 (Ditabled) Always send alert to this destination LAN Channels 1 Sent To: 0
FINJ Information     Mill Logs & Reports     Settings     Prover Control	¢	Group: 5 (Dischled) Almays send alert to this distination LAN Channel: 1 Sent To: 0	۰	¢	Geoup: 6 (Dischied) Abays send alert to this destination LAN Channel: 1 Sent To: 0	۰	¢	Group: 7 (Disabled) Aways send alert to this destination UN Channel: 1 Sent To: 0	0	Ţ	Group: 8 (Disabled) Always send alert to this destination UM (Namel: 1 Sent To: 0
Moletenance     Nodes Information     Sign out	¢	Group: 9 (Druchled) Always send alert to this distination LAN Channel: 1 Sent To: 0	۰	¢	Geoup: 10 (Druchled) Always send alert to this distination LAN Channel: 1 Sent To: 0	۰	¢	Group: 11 (Disabled) Always send alert to this destination UAN Channel: 1 Sent To: 0	0	¢	Group: 12 (Disabled) Ahvays send alert to this destination LAN Channel: 1 Sent To: 0
	¢	Group: 13 (Dirichled) Almays seril abort to this distination LAN Channel: 1 Sent To: 0	۰	¢	Geosp: 14 (Disabled) Always send alter to this distination LAN Channel: 1 Sent To: 0	0	¢	Group: 15 (Disabled) Always sind alert to this destination LAN Channel: 1 Sent To: 0	0	Ţ	Group: 1 (Dinabled) Abways sind allert to this destination LAN Channel: 1 Sent To: 0
	¢	Geoup: 2 (Dtruchled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 3 (Drashled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	¢	Group: 4 (Disabled) Always send alert to this destination UNI Channel: 1 Sent To: 0	0	Ţ	Group: 5 (Ditabled) Always send alert to this destination LAN Channel: 1 Sent To: 0
	¢	Geoup: 6 (Druchled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 7 (Dirahled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	¢	Group: 8 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Ţ	Groups 9 (Ditabled) Abays send alert to this destination LAN Channels 1 Sent To: 0
	¢	Group: 10 (Dissibled) Always send alert to this destination LAN Channel: 1 Sent To: 0	•	Ţ	Geosp: 11 (Drochled) Absuys send alert to this destination LAN Channels 1 Sent To: 0	0	¢	Group: 12 (Disabled) Always send alert to this destination LAN Channels 1 Sent To: 0	۰	Ţ	Group: 13 (Bloobind) Always send alert to this destination LAN Channels 1 Sent To: 0
	¢	Group: 14 (Dirochled) Always send aliert to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 15 (Drobled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	¢	Group: 1 (Doubled) Always send alert to this destination LAN Channel: 1 Sent To: 0	٥	Ŷ	Group: 2 (Ditables) Always send alert to this destination LAN Channels 1 Sent To: 0
	¢	Geoup: 3 (Druchled) Always seed alect to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 4 (Dorohled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	Û	Groups 5 (Disobled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	Û	Group: 6 (Diobled) Abways need alert to this destination LAN Channik 1 Sent To: 0
	¢	Geoup: 7 (Dirabled) Always seed alect to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 8 (Dochled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	Ĵ	Groups 9 (Disobled) Always send alert to this destination LAN Channels 1 Sent To: 0	0	Û	Group: 10 (Doubled) Abways send alert to this destination LAN Channik 1 Sent To: 0
	¢	Geoup: 11 (Disobled) Always seed alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 12 (Disobled) Always send alert to this destination LAN Channel: 1 Sent Yo: 0	0	Ĵ	Group: 13 (Noobled) Always send alert to this destination LAN Channel: 1 Sen: To: 0	0	Û	Group: 14 (Disobled) Abways send alert to this destination LAN Channik: 1 Sent To: 0
	¢	Group: 15 (Disobled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Geospic 1 (Distabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Group: 2 (Disobled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Û	Group: 3 (Disobles) Always send alert to this destination LAN Channik 1 Sent To: 0
	¢	Group: 4 (Dirobled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Geoup: 5 (Disobled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Group: 6 (Disobled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Û	Group: 7 (Disobles) Always send alert to this destination LAN Channik 1 Sent To: 0
	¢	Group: 8 (Disobled) Anaryssend alert to this destination LAN Channel: 1 Sent Toc 0	0	¢	Geosp: 9 (Disabled) Always seed alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Group: 10 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Ţ	Group: 11 (Noobled) Always send alert to this destination LUN Channel: 1 Sent Yo: 0
	¢	Group: 12 (Disobled) Anayys send alert to this destination LAN Charmel: 1 Sent To: 0	0	¢	Group: 13 (Disobled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	¢	Group: 14 (Disabled) Always send alert to this destination LAN Channel: 1 Sent To: 0	0	Û	Group: 15 (Disabled) Ahways send alert to this destination LMX Channel: 1 Sent To: 0

### 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.

	O 2008-06-17 38-88:04 (UTC+00:00 UTC)	
CHC. Chromeser, Information 12.40.50 May 26 2020 14:20:31 Cit Host Online	Alert Policies	
QuickLinia.	Alert Policies	0
# Dashboard	Policy Group Number	
& Sensor	1	~
• Fitt Information	Enable this alert	
Mit Logs & Reports >	PelicyAction	
O Settings	Always send alert to this destination	~
Power Control	LAN Channel	
	1	~
Haintenance	Destination Selector	
D Nodes Information		
🕪 Sign out	Event Specific Alert String	
	Alert String Key	
	_	
	Delete	E3 Save

- 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.

٢	P

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.

	≡ 02018-00	8-17 18:48:41 (UTC+00:00 UTC)					S A US-Engl	ish • • Sync 🖸 Refresh	1 admin
CINC Firmware Information 12.44.54 May 26 2928 14:20:31 CST Hoat Online	LAN Dest	inations						$\boldsymbol{w}$ Home $>$ Settings $>$ Platform Event Filter	a > LAN Destinat
Quick Units.	Select the LAN C	hannel 1 v							
Dathboard     Sensor     FRU Information     Logar & Report	►	LAN Channel: 1 LAN Destination: 1 SNMP Trap Sent To:	P	LAN Channel: 1 LAN Destination: 2 SNIMP Trap Sent To:	P	LAN Channel: 1 LAN Destination: 3 SNUP Trap Sent Tec	P	LAN Channel: 1 LIN Destination: 4 SNMP Trap Sent Tec	
il Logs & Reports >									6
	►	LAN Channel: 1 LAN Destination: 5 SNMP Trap Sent To:	<b>P</b>	LAN Channel: 1 LAN Destination: 6 SNMP Trap Sent To:	•	LAN Channel: 1 LAN Destination: 7 SNIP Trap Sent To:	<b>P</b>	LAN Channels 1 LAN Destination: 8 SNMP Trup Sent To:	
Nodes Information			823		823		823		E
	•	LAN Charmel: 1 LAN Distination: 9 SNIP Trap Sent To:	<b>P</b>	LAN Charmel: 1 LAN Distinution: 10 SMMP Trap Sent To:	P	LAN Channel: 1 LAN Destination: 11 SMMP Trap Sent To:	<b>A</b>	LAN Chamnel: 1 LAN Destination: 12 SNMP Trap Sent Tec	
	►	LAN Channel: 1 LAN Destination: 13 SNMP Trap Sent To:		LAN Channel: 1 LAN Destination: 14 SNUP Trap Sent To:		LAN Channel: 1 LAN Destination: 15 SMMP Trap Sent Tec			E
			23		123				

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

	© 3318-06-17 35/88:20 (UTC) 00200 UTC)	Z US-English → O Sync C Re
CINC Flormware Information 12.46.04 May 26 2020 14/20131 CST I Hoat Online	LAN Destination Configuration	of Home > Settings > Platform Event Filters > LAN Destinations > 1
juick Units. •	0	
Dashboard	LAN Channel	
Serner	1	
FRU Information	LAN Destination	
M Logs & Reports >	1 Destination Type	
Settings	SIMP Trap 🕐 E-Nail	
9 Power Control	SNIP Destination Address	
Maintenance		
Nockes Information	CMC Username	
🕒 Sign out	Email Subject	
	Email Hessage	
	82 Save	

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, CMC 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.

**CMC 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.

	9 2318-06-17 18-49	55 (UTC+00:00 UTC)					S A US-English * \$5yn	c ORefresh J	L admin -
CMC Homeware Information 13.44.59 May 20 2020 14:20:33 CST Host Celline	Services							<b>di</b> Home - Settin	np - Services
Quick Links.	Service ©	Status ¢	Interfaces ¢	Non Secure Port 🗢	Secure Port \$	Timeout ¢	Naximum Sessions 🕈		
<ul> <li>Dushboard</li> </ul>	web	Active	bend0	80	443	1800	20	- /	
a Sensor	ssh	Active	bend0	N/A	22	600	N/A	- /	
FRU Information									
Legs & Ruports >									
<ul> <li>Settings</li> <li>Power Control</li> </ul>									
<ul> <li>F Maintenance</li> </ul>									
Nodes Information									
P Sign out									

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.

	@ 2018-06-17 18:50:28 (UTC+	00:00 UTC)			5	US - English	* O Sync 🖸 Refresh	1 admin -
CMC Fibroware Information 13.46.59 May 26 3220 3420031 CST Hoat Celline	Service Sessions						# Home > Settings > Services :	Service Sessions
Quick Links.	Active Session - Web							
<ul> <li>Dashboard</li> </ul>	Session ID #	Session Type 🗣	User ID \$	User Name 🗘	Client IP 9	Privlinge \$		
Sensor	5	Web HTTPS	2	admin	10.1.2.121	Administrator	_	
FRU Information		WWWITE 2	*	2			•	
LalL Logs & Reports	т	Web HTTPS	2	admin	10.1.2.121	Administrator	•	
• Settings								
O Power Control								
Nodes Information								
😝 Sign out								

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.

		32818-06-17 18:51:03 (UTC+00:00 UTC)	
CMC Firmware: Information 13.48.98 May 20.2920 14:20:33 CST 0 Heat Online		Service Configuration	
Quick Linka.	1		0
# Dashboard		Service Name	
a Serior		web	
1933 Information		Active	
🕍 Loga & Reports 🔷		Interface Name	
O Settings		Non-secure port	~
O Power Control		ao	
✗ Maintenance		Secure part	
Nodes Information		443	
Ge Sign out		Timeout	
-		1800	
		Maximum Sessions	
		20	
			D See

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 (readonly).

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.

	0 2018-06-17 18:51:43 (UTC+00:00 UTC)		
CMC firmware information 12.44.54 May 26 2020 34:2023 1 CST 0 Hoart Celline	SMTP Settings		
Quick Units.		0	
<ul> <li>Dashboard</li> </ul>	LAN Interface		
🚯 Sermor	bond0	٣	
FRU Information	Sender Email ID		
Latt. Logs & Reports 🔹 🔹			
• Settings	Primary SMTP Support		
Power Control	Primary Server Name		
▶ Maintenance			
Nodes Information	Primary Server IP		
🕒 Sign out	Primary SMTP port		
	25		
	Primary Secure SMTP port		
	465		
	Primary SMTP Authentication		
	Primary Username		
	Primary Password		
	Primary SMTP SSXTLS Enable		
	Primary SMTP STARTTLS Enable		
	Secondary SMTP Support		
		R Save	
		11 300	

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.



 $\ensuremath{\textbf{Note:}}$  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.

	O 2018-06-17 18:52:20 (UTC+00:00 UTC)		= 4	US-English • Ø Sync Ø Refresh 🛓 admin •
CAR: Character Information 12.48.58 May 20 2020 14:20031 CST Heat Celline	SSL Settings			# Home > Settings > 552. Settings
QuickUnks. •	View SSL certificate	Generate SSL certificate	Luplood SSL certificate	
🙆 Serace				
FRU Information				
Latt. Logs & Reports >				
• Settings				
O Power Control				
Nodes Information				
🕒 Sign out				

- 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

	@ 3838-06-17 18:5233 (UTC+08:00 UTC)	=	US - English	*
CMC / Instance Information 12.46.54 May 26 5920 14:20:33 CST Inst Online	View SSL Certificate			Home > Set
Quick Units	Current Certificate Information			
# Dashboard	Certificate Version			
n Seroce	3			
• TRU Information	Serial Number EFICFCTTVISF006			
🕍 Logs & Reports 💦 👌	Signature Algorithm			
• Settings	sha256Wth#SAEncryption			
	Public Key			
	(2048 bit)			
Nodes Information	Issuer Common Name (ON)			
	megarac.com			
	Issuer Organization (0) American Megatrends International LLC (AMI)			
	American Megatrenos international LLC (AMI) Issuer Organization Unit (OU)			
	Service Processors			
	Issuer City or Locality (L)			
	Norcross			
	tssuer State or Province (ST) Georgia			
	Issuer Country (C)			
	us			
	Issuer Email Address			
	support@wmi.com			
	Valid From			
	Aug 27 12:03:00 2019 GMT			
	Velid Till Aug 28 10:05:00 2034 GMT			
	700 20 201000 2004 0H1			
	Issued to Common Name (CN)			
	megarac.com			
	Issued to Organization (O) American Negatrends International LLC (AMI)			
	Issued to Organization Unit (OU)			
	Service Processors			
	Issued to City or Locality (L)			
	Norcross			
	Issued to State or Province (ST) Georgia			
	Issued to Country (C)			
	us			
	Issued to Email.Address			
	support;Bami.com			

## Generate SSL Certificate

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

	@ 2018-06-17 18/5R/07 (UTC+00:00 UTC)	
CMC fitmware toformation 12.44.56 May 20 2020 34:20:33 CST 0 Host Online	Generate SSL Certificate	
Quick Linka. 🔻		Θ
Dashboard	Common Name (CN)	
b Seroce		
1933 Information	Organization (0)	
😹 Logs & Reports 🔹 🔸	Organization Unit (OU)	
• Settings		
	City or Locality (L)	
Nodes Information	State or Province (ST)	
	Country (C)	
	Email Address	
	Valid for	
	in days	
	Key Length	
	2048 bits	*
		(D) Save

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.

	© 2018-06-17 18:56:51 (UTC+00:00 UTC)		Sync CRefre
CMC Ennounce Information 12.46.54 May 26 2020 14.20.31 CST Host Celline	Unload SSI Certificate		# Hone $\times$ Settings $\times$ 50, Settings
Juick Linka.		Θ	
Dashboard	Current Certificate		
Sermor	Tue May 26 00:19:04 2020		
	New Certificate	<b>b</b>	
	Current Private Key		
attings	Tue May 26 08:19:04 2020		
	New Private Key		
		<b>E</b>	
		E Save	
Sign out			

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.

	G 2818-06-17 18:55:25 (UTC+00:00 UTC)		3 4	. US-English • • Sync Stafresh 1 admin •
CMC fitmware information 12,48,59 May 20 2920 14/20/33 CST Host Online	System Firewall			# Home - Settings - System Prevail.
QuickUnks. •	General Frewall Settings	IP Address Frewall Rules	Port Firewall Rules	
Sensor				
FRU Information				
Lall. Logs & Reports >				
O Settings				
Power Control				
✗ Maintenance				
Nodes Information				
🖶 Sign out				

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.

	@ 2018-06-17 18:59:12 (UTC+00:00 UTC)	S ▲ US-English • OSync Øfefresh ▲ admin •
CMC Elementer Information 12.48.98 May 26 2220 14/20/33 CST Host Online	General Firewall Settings	(# Here - Settep - Freval - Consultreval Settep
Quick Links.	o +	
<ul> <li>Dashboard</li> </ul>	Existing Firewall Settings Add Firewall Settings	
n Sensor		
FRU Information		
Lail. Logs & Reports		
O Settings		
Power Control		
₽ Maintanance		
Nodes Information		
🕪 Sign out		

### **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.

	O 2018-06-18 12:10:07 (UTC+00:00 UTC)		S 🛦 US-English - O-Sync 🖸 Refresh
CMC Elements Information 12.46.54 Nay 26 2020 14:20:23 CST Host Online	Existing Firewall Settings		W Home $>$ Settings $>$ Finance $>$ Section Finance Settings $>$ Soluting Finance Settings $>$ Soluting
ikk Unis. •		0	
Dashboard	Block All		
Sermor	IPv6		
FBJ Information	Flush All		
Logs & Reports >	Timeout		
Settings	Start Date&Time Non Jun 18 2018 21:07:00		
Power Control	End Date&Time		
Maintanance	Mon May 04 2020 13:42:00		
Nodes Information	Dointe		
Sign out			

#### Add Firewall Settings

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

	@ 2018-06-18 15:00:26 (UTC+00:00 UTC)	
CMC.Firmware.toformation 12.44.54 May 20 2020 14/20/31 CST Host Online	Add Firewall Settings	
Quick Linka.		0
e Dashboard	Block All	
n Sensor	IPp4	÷
FRU Information	Flush All	
M Logs & Reports	Timeout	
• Settings	Start Dote	
Power Control	2018-08-18	m
	Start Time	
	13:09	0
Nodes Information	End Date	
🕒 Sign out	2018-00-18	
	End Time	
	13:09	٥
		ED Save

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.

	O 2018-06-18 13:10:50 (UTC+00:00 UTC)			S A US-English	<ul> <li>♥ Sync</li> <li>■ Refresh</li> </ul>	L admin -
CMC //immence information 12248-54 May 26 2020 14:20:33 CST Hourt Gellow	IP Firewall Rules				# Home - Settings - Risevall	<ul> <li>IP Preval Pales</li> </ul>
Quick Unics.	0		+			
n Dushboard	Existing IP Rules	_	Add New IP Rule			
Sernor						
FRU Information						
LalL Logs & Reports >						
O Settings						
O Power Control						
Nodes Information						
læ Sign out						

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.

Lixed With Control     Market Production     Market Produc	IAMB		O 2018-06-18 12:32:27 (UTC+00:00 UTC)		a /	US - English *	• Sync	C Refres
Kolonicov     P/P Brogin RALIDUZ - Mallud Z       Bohkovať     Preskovánov       Francisk Couldati     Preskovánov       Francisk Couldati     Preskovánov       Francisk Couldati     Preskovánov	Arrow Constraints     Arrow Constraints	CMC Firmware information 12.46.54 May 25 2120 14:20:31 CST Heat Online	Existing IP Rules			iii Home > Settings > Result	> IP Oviented	Firewall Rule
		Ack Links.	Rate: Allow Trimeost: Enabled From: 2058-06-58 53:11:00 (UTC+00:00 UTC					

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.

Statisticational Statistication Statistin Statistin Statistication Statistication Statisticatio		O 2018-06-18 13:12:55 (UTC+00:00 UTC)		■ A US-English v OSync ORefresh L adm
	12,48,58 Ney 20 2020 14:20:31 CST	Existing IP Rules		- # Here $\times$ Setting $\times$ Thenell $\times$ IP Oriented Finenal Rules $\times$ Dating IP Rules $\times$ Dating IP
Status     Status	Quick Links. *		0	
Inclusion         Inclusion <t< td=""><td></td><td></td><td></td><td></td></t<>				
Portug         Scale Marsina	FRU Information			
Predictored         Statisfield (Statisfield (Stati		Enable Timeout		
Notes Information         2020 Ho 54 ki 44 do (07.100 UTC)           Signard         main				
A Acide Internation - Sign out		End Date&Time		
Sign out		2020-05-04 14:46:00 (UTC+00:00 UTC)		
The second s		Delizer		

#### 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.

245.5 Economic Information 2,45.58				# Home - Settings - Firewall - IP Oriented Fire	cool Fale
4ey 26 2020 14:20:31 CST	Add IP Rule				
Hast Online					
ka. •		Ø			
board	IP Single (or) Range Start				
e e					
formation	IP Range End				
Reports >	optional				
	Enable Timeout				
ę.	Start Date				
r Control	2018-06-18	m			
enance	Start Time				
sinformation	13:13	٥			
ut	End Date				
	2018-00-18				
	End Time				
		٥			
	Rule				
	Allow	~			

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.

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

**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.

	@ 2018-06-18 13:14:00 (UTC+00:00 UTC)		S A US-English	<ul> <li>♥ Sync ■Refresh</li> </ul>	1 admin •
CMC.Einswarz.Information 22,43,58 May 28 2029 14:28:31 CST Host Online	Port Firewall Rules			# Home - Settings - Frewall -	Port Pirewall Rules
Quick Links. •	Dotsting Port Rules	Add New Port Rule			
Sensor					
FILU Information     Int Logs & Reports					
O Settings					
Power Control     Maintenance					
Nodes Information					
🖶 Signout					

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.

	0 2018-08-18 13:10:38 (UTC+00:00 UTC)		8	▲ US-English *	Sync 🗧 Refresh	1 admin -
CARC Elements Information 12.44.50 May 26 2020 (4:20:3) CST i Host Celline	Existing Port Rules			<b>W</b> Home > Settings > Finwall > Po	Oriented Firewall Rules	> Existing Port Ra
QuickUnites. • Duahboard Sensor FRU Information Litt Logs & Deports > Settings	Pert / Pert Respc 22 - 05 Protocil: TO* Protocil:	•				
<ul> <li>Power Control</li> <li>Maintenance</li> <li>Nodes Information</li> <li>Sign out</li> </ul>						

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.

	() 2018-06-18 1211706 (UTC+00100 UTC)	🖀 🛦 US-English - OSymc 🕻 Size
CIRC firmware information 12.44.54 May 26 2020 14/20/33 CST Hoat Online	Existing Port Rules	${\pmb \theta}$ Home $>$ Settings $>$ Finnel $>$ Port Colored Finnell Rules $>$ Existing Port
uick Unics. •	0	
Dashboard	Port Single (or) Range Start	
	123	
FRU information	Port Range End	
Logs & Reports >	456	
Settings	Protocol TCP	
Power Control	Notwork Type	
Maintenance	19/4	
Nodes Information	Enable Timeout	
	Start Date&Time	
Sign out	2018-06-18 13:34:00 (UTC+00:00 UTC)	
	End Date&Time	
	2020-05-01-09-48:00 (UTC+00:00 UTC)	
	Rule	
	Allow	
	Delete	

### Add New Port Rule

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

	O 2018-06-18 12:15:07 (UTC+00:00 UTC)	
OK firmure information	Add Port Rule	
Quick Links.		0
# Dashboard	Port Single (or) Range Start	
🚳 Sernor		
FRU Information	Port Range End	
Laff. Logs & Reports >	optional	
• Settings	Protocol	
Fower Control		
	Network Type	~
🗲 Maintenance	Enable Timeout	
Nodes Information	Start Date	
😥 Sign out	2038-06-38	
	Start Time	
	13:14	٥
	End Date	
		•
	End Time	
		0
	Rule	
	Allow	~
		D Save

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.

	<b>Ξ</b> @2018-06	-18 13:17:39 (UTC+00:00 UTC)				8 A	US - English	• Sync □Refresh ▲ admin •
CMC.Fizzware.Information 12.48.58 May 20 2020 14:20:33 CST Host Online	User Man	agement						# Home > Settings > User Management
Quick Links.	Channel 1 V							Θ
Dashboard     Sensor     FRU Information     ML Legs & Noports	4	Channel 1 1 anonymous (Disobled) No Access	4	Channel 1 2 admin (Active) Administrator	4	Channel 1 3 (Disobled)	4	Channel 1 4 (Disabled)
<ul> <li>Settings</li> <li>Power Control</li> <li>Maintenance</li> </ul>	4	Charmel 1 5 (Discobled)	*	Channel 1 6 (Disabled)	4	Channel 1 7 (Disabled)	4	Channel 1 8 (Disabled)
<ul> <li>Nodes information</li> <li>Sign out</li> </ul>	-	Channel 1 9 (Dischled)	*	Channel 1 10 (Ditabled)	*	Channel 1 11 (Ditabled)	*	Channel 1 12 (Disabled)
	-	Channel I 13 (Disabled)	4	Channel 1 14 (Dinabled)	<b>.</b>	Channel 1 13 (Dinabled)	<b>.</b>	Channel 1 36 (Chuzbied)

#### 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.

	О 2018-06-18 12:18:52 (UTC+00:00 UTC)	
CHC Timmurc Information 12,48,50 Nay 26 2020 14:20:31 CST Nay 26 2020 14:20:31 CST	User Management Configuration	
Quick Units.		0
Dashboard	Username	
Sernor	- Contraine	
	Password Size	
FRU Information	16 bytes	v
Latt. Logs & Reports >	Password	
O Settings		
O Power Control	Confirm Password	
✗ Maintenance	L	
Nodes Information	Enable User Access	
🕞 Sign out	Enable Channel Access	
	Chansel 1 Chansel 2	
	Prhilege(Channel 1)	
	User	•
	Privilege(Channel 2)	
	User	~
	SNMP Access	
	SNNP Access level	
		~
	SNNP Authentication Protocol	
		*
	SNMP Privacy Protocol	
		*
	Email Format	
		*
	Email ID	
	Existing SSH Key Not Available	
	Upload SSH Ney	
	shows you say	<b>B</b>
		ED Save

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



**Note:** User Name is a string of I to 16 alpha-numeric characters. It must start with an alphabetical character. It is case-sensitive. Special characters '-2'(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.

_		O 2018-08-18 13:18:08 (UTC+00:00 UTC)	
12.4 Nay 0 1	C Firmware Information 48.59 y 26 2820 14:20:33 CST Hoat Online	User Management Configuration	
Quick Units	s. •		0
Database	ard	Username	
		anonymous	
		Change Password	
FRU Info			
Logs & F	Reports >	Password Size	
		10 bytes	¥
Settings		Password	
nisteo	vance	Confirm Password	
Nodes II			
Sign out		Enable User Access	
		Enable Channel Access	
		Channel 1	
		Channel 2	
		Privilege(Channel 1)	
		None	*
		Privilege(Channel 2)	
		Administrator	~
		SNMP Access	
		SNMP ACCESS	
		SNMP Access level	
			~
		SNMP Authentication Protocol	
			*
		and block brand	
		SNMP Privacy Protocol	Ý
			¥
		Email Format	
		AMI-Format	v
		Email ID	
		Existing SSH Key	
		Not Available	
		Upload SSH Key	
			<b>B</b>
		Delete	🔛 Sive

- 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.

	<b>■</b> <sup>@</sup> 2018-06-	18 13:22:14 (UTC+00:00 UTC)						2	5 ▲	US - English	* OSync	C Refresh	1 admin -
CMC Historeact Information 12.46.56 May 20 2020 14:20:53 CST Histo Celline	Fan Profile	e										₩ Home > Se	attings > Pan Profile
Quick Units.				<b>.</b>	D import	A Download	Manager Target PCIE device options						0
# Dashboard			~			/ 1							
FRU Information	+	New fan profile		Name: default Status: Run									
Lail. Logs & Reports													
• Settings													
O Power Control													
Nodes Information													
🝽 Sign out													

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

ON: Firmware Information 12.41.58	Edit New Fan Profile	■ ▲ US-English • O'Sync: O'Refmanh ▲ add # Home > Settings > FastPartie > Editionaria
May 26 2020 14:20:33 CST Hout Online		
Unks. •	Back Save New policy Delete selected policy	
Nourd	0	Sensor Reading Value: 243 Duty (%): 100.000
nor	Natte	500
Information	NEW_PROPILE	80
s & Reports >	Policy Algorithm Sensor Type Initialize Duty	
	0 * Step * Temperature 1 * 100	(%) Ang au
tings	Sensor	£ a
ver Control		20
internance	Fan	
kes Information		0 250 200 150 100 50
rout		Sensor Reading Value
	Policy Execute Condition	
	Policy Execute Condition	
	CPU Tóp (W)	
	0	
	Ambient Sensor	
	PCIE Device	
	PCIE Device Not check pcie device, ignore this execute condition	
	Policy Reference Table New	
	Reference 0 Daty (%)	
	127 100 Delete	

- 1. Name the the profile
- 2. Select the Algorithm.
- 3. Select **Sensor Type**, current or temperature.
- 4. Set the Initialize 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.

	<b>○</b> 2028-06	-58 13:27:10 (UTC+00:00 UTC)					= #	US - English	* O Sync 🖸 Refresh	1 admin -
CMC fitmware information 12.46.90 May 20 2020 14:20:31 CST Heat Celline	Fan Profil	le							W Home > S	ettings > Fan Profile
QalckUnks.			<b>b</b>	🗈 import 🔺 Download	/ Nanagor 1	Target PCIE device option	8			Θ
<ul> <li>Danhbourd</li> <li>Sermor</li> </ul>	-		Name: default	/ #		Name: test	/ # + ×			
FRU Information	т	New fan profile	Status: Run			Status: Stop				
LML Logs & Reports >										
Settings     Power Control										
Nodes Information										
🕒 Sign out										

#### 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.

	© 2018-06-18 22:22:13 (UTC H00:00 UTC)	🛎 🧟 US-English 👻 👁 Syn	rnc 😋 Refresh 🏦 admin •
CMC Firmware Information 12.46.56 Nay 20 2020 14:20:23 CST Host Online	Power Consumption		# Home > Power Consumption
Quick Units.	€ Ever		
Senace     FRU information	Power Consumption Reading		
	Current Power Consumption (W) 60		
Settings     Power Control	Minimal Power Consumption (M) 68		
<ul> <li>Maintenance</li> <li>Nocks Information</li> </ul>	Maxmail Power Consumption (H) 71		
	Average Power Cessumption (N) 68		

# 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.

	@ 2018-06-18 13:32:56 (UTC+00:00 UTC)	
CHC Elements Information 12/43/8 May 26 3220 14/20/31 CST I Host Online	Power Control on Host Server	
Qaick Links.	Power Actions	Û
<ul> <li>Dashboard</li> </ul>	Host is currently on	
📾 Sensor	O Power Off	
FRU Information	Power On	
Last Logs & Reports	Power Cycle	
O Settings	Hard Reset	
O Power Control	ACPI Shutdown	
🗲 Maintenance		O Perform Action
Nodes Information		
🕒 Sign out		

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.

	@ 2018-06-18 13:35:56 (UTC+00:00 UTC)		= <b>2</b>	S-English • O Sync O Refresh 🛔 admin •
CMC.Eiconwater.Information 32,48,58 May 20,2272 5422033 CST I Host Cellure	Maintenance			<b>W Home</b> - Maintenance
Quick Linica. V	*	A state	0	
A Sensor	Rackup Configuration	Firmware Image Location	Firmware Information	Firmware Update
FRU Information	Preserve Configuration	Restore Configuration	D Restore Factory Defaults	System Administrator
🕍 Logs & Reports 🔹 🔸				
O Settings				
Power Control				
Nodes Information				
🕒 Sign out				

## 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.

	G 2018-06-18 13/37/32 (UTC+00.00 UTC)		🕿 🧟 US-English	v OSync
CML Firmware Information 12.48.58 May 20 28220 14:20:33 CST Brast Online	Backup Configuration			# Home - He
ck Linka. 🔻		0		
Dashboard	CheckAll			
Seroce	SNMP			
FRU Information	Network & Services			
Logs & Reports >	IPMI			
iettings	NTP			
ower Control	Authentication			
Maintenance	\$Y5L06			
Nodes Information		▲ Download		
ign out		and commission		

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.

	G 2018-06-18 13:38:04 (UTC+00:00 UTC)		🕿 🧟 US-English	<ul> <li>♥ Sync CRefresh ▲ admin</li> </ul>
CMC.Firmware.Information 12.44.54 May 26 2020 14/20/33 CST Host Online	Firmware Image Location			# Home - Heinfenence - Timmerc ImageLoc
Quick Links.		Θ		
	Image Location Type			
a Serbor	TFIP Server			
190 Information		E2 Save		
🕍 Loga & Reports 🔹 👌				
• Settings				
Power Control				
✗ Maintenance				
Nodes Information				
🕒 Sign out				

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



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:xxx."

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.

	© 2028-06-18 12:39:01 (UTC+00:00 UTC)		🕿 🧟 US-Er	glish • • Sync 😋 Refr
CBC Firmware Information 12:41:58 Hay 26 2020 14:20:21 CST Hour Online	Firmware Information			# Home > Maintenance
Quick Units. •		0		
# Dashboard	CMCFirmware Information			
🚯 Serator	Build Date			
FRU Information	May 26 2020			
🕍 Logs & Reports 🔹 👌	Build Time			
O Settings	14/20:31 CST			
Power Control	Firmware venion 12.42.98			
✗ Maintenance	CPLDFirmware Information			
Nodes Information	CPLDFIrmware Information			
Ge Sign out	NR 36 Horanon 4: 13 Horanon 2: 13 Horanon 2: 13 Horanon 2: 13 Horanon 4: 13			

The various fields of Firmware Information page are given below.

#### CMC Firmware Information:

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

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

Firmware version: Describes the Firmware version of the active CMC 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.

	© 2018-06-38 33:48:44 (UTC+00:00 UTC)
CHC Firmware Information 12.41.58 Nay 26 2220 34:20:31 CST 9 Nati Union	Firmware Update
Quick Units.	0
Dualabound     Dualabound     Sensor     FRU information	Note: Frankring are the Transace update methods and components supported in this page. Both Transace update. Provide Transace update. Provide Transace update the Materia components. Provide Transace Update Provide Transace Update Updat
<ul> <li>Settings</li> </ul>	Select Firmware Image Choose File No file chosen
O Power Control	Start ferrevore update
<ul> <li>Maintenance</li> <li>Nodes Information</li> </ul>	WWRNINGSPlease note that after entering the update mode, the widgets, other web pages and services will not work. All the open widgets will be automatically closed. If the upgradulors is cancelled in the middle of the intand, the donce will be react only for BMC
Ge Sign out	800T, and APP components of Firmware.
t# Sign out	

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:

Section Name	Existing version	Uploaded version	~
boot	2.4.000000	2.4.000000	~
conf	2.4.000000	2.4.000000	~
conf	2.4.000000	0.0.	~
root	2.4.000000	2.4.000000	~
osimage	2.4.000000	2.4.000000	~
www	2.4.000000	2.4.000000	~
testapps	2.4.000000	2.4.000000	~
ast2500e	0.1.000000	0.1.000000	~

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.

		RC v1.0.0.1\CL3150 G4 BHK	
Only the selected se	ctions will be updated:		
Section Name	Existing version	Uploaded version	
boot	2.4.000000	2.4.000000	Message from webpage
conf	2.4.000000	2.4.000000	Firmware reset has been called. Close the current session, and open a
conf	2.4.000000	2.4.000000	new session after a couple of minutes.
toot	2,4,000000	2.4.000000	
osimage	2.4.000000	2.4.000000	OK
www	2.4.000000	2.4.000000	
ast2500e	1.0.103227	1.0.303227	

**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 CMC.

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

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 CMC.

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

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 Imedia, 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.

**Idap.conf**: This file contains the Idap 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.

	= •	2018-06-18 13:42:01 (UTC+00:00 UTC)	
CMC Chromatic Information 12.41.54 Nay 26 2020 14:20:231 CST © Hard Christe	Rest	ore Configuration	
Quick Units.			0
<ul> <li>Dathboard</li> <li>Sensor</li> </ul>	Cor	rfig File	۵
FRU Information			D Save
Latt. Logs & Reports >			
Settings     Power Control			
<ul> <li>Power consta</li> <li>Maintenance</li> </ul>			
Nodes Information			
🕞 Sign out			

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.

10.1	.112.37 says:			,
		o continue restoring con configurations will restar		
			ОК	Cancel

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.

	G 2018-06-28 23x43x02 (UTC+00x00 UTC)	
CMC.Firmware.Information 12.44.58 May 20.2220 14:20:33 CST 0 Hust Online	Restore Factory Defaults	
Quick Links		0
# Dashboard	The following checked configurations will be preserved through the restore operation. You can make changes to the list in the preserve configuration page.	
n Serier	SDR	
● FRU Information	FRU FRU	
• Settings	SEL	
Power Control	IPM	
	Network	
Nodes Information	NTP SNMP	
Ge Sign out	SSH	
	Authentication	
	Synlog	
	Web	
	Redish	_
		Save

### 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.

	@ 2558-06-38 13-4334 (UTC+00:00 UTC)	3	▲ US-English • © Sync C Refresh L admin •
CMC Finnware Information 12.44.56 May 20.2220 14/2013 CST 9 Hust Online	System Administrator(BMC Debug console)		# Home - Haintenance - System Administrator(SHC Debug console)
Qaick Links. •	0		
# Dashboard	Username		
a Serocr	sysadmin		
TRU Information	Enable User Access		
🕍 Logs & Reports 🔹 🔸	Change Password		
• Settings	Password		
O Power Control	Confirm Password		
✗ Maintenance			
Nodes Information	ED Save		
🕀 Sign out			

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.

=	○ 2018-06-18 12:48:21 (UTC+	00:00 UTC)						2	US - English	* OSync	C Refresh	1 admin -
CBC Firmware Information 12245.58 May 26 2020 54:20:23 CST Not Colore	lodes Information										# Home >	Nodes information
Quick Links.											Collapse All	Expand All
	- • Node:4											
FRU Information	Firmware Ver	HLAN NAC	IPv4	IPv6	LAN 1 MAC	LAN 2 MAC	LAN 3 MAC	LAN 4 MAC				
Lat. Logs & Reports >	c.43	20:20:04:17:14:00	192.168.0.100	-	N/A	N(A	N/A	N/A				
O Settings												
Power Control												
🖌 Maintersance												
Nodes Information												
🕒 Sign out												

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.