



Cisco Baseboard Management Controller Configuration Guide for Cisco UCS C885A M8 Rack Server, Release 1.0

First Published: 2024-12-09

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



CONTENTS

PREFACE

Preface	vii
Audience	vii
Conventions	vii

CHAPTER 1

Introduction	1
Overview of the Cisco UCS C885A M8 Rack Server	1
Introduction	1
Requirements	3
Logging into Cisco BMC	3
Navigation and Menu	4
Overview Page	6

CHAPTER 2

Logs	9
Event Logs	9
Viewing Event Logs	9
Exporting Event Logs	10
Deleting Event Logs	10
POST Logs	11
Viewing POST Code Logs	11
Exporting POST Code Logs	11
Tech-support log	12
Downloading Tech Support Logs	12

CHAPTER 3

Hardware Status	13
Viewing Inventory and LEDs	13
CPU Monitoring and Management	19

Cooling Management 20
 Managing Fan Failure Conditions 21
 Viewing Sensor Status 21
 Turning On/Off System Identify LED 22

CHAPTER 4

Operations 23

Resetting Cisco BMC and Server to Factory Settings 23
 Launching KVM Console 24
 BMC Firmware 24
 Viewing BMC Firmware Version 24
 Updating BMC Firmware Version 25
 Updating OEM Firmware 25
 Rebooting BMC 26
 Viewing Serial over LAN (SOL) console 26
 Server Power Operations 27
 Viewing Server Power Status 27
 Rebooting the Server 27
 Shutting Down the Server 28
 Overriding Boot Source 28
 Performing AC Power Cycle on the Server 28
 Adding Virtual Media Image 29

CHAPTER 5

Settings 31

Configuring BMC Date and Time Settings 31
 Network Management in Cisco BMC 32
 Viewing or Configuring Network Settings 32
 Viewing or Adding IPv4 Address 33
 Viewing, Adding, or Deleting Static DNS IP Address 34
 Setting Power Restore Policies 35

CHAPTER 6

Security and Access 37

User Session 37
 Viewing User Sessions 37
 Disconnecting a Session 38

LDAP Configuration	38
Enabling LDAP Authentication	38
Adding Role Group	39
User Management	40
Adding a User	40
Editing a User	41
Enabling or Disabling a User	41
Managing Account Policy Settings	42
Deleting a User	42
Updating Policies	43
Enabling or Disabling BMC Shell through SSH	43
Enabling or Disabling Network IPMI	43
Managing Certificates	43
Viewing Certificate Details	43
Adding a New Certificate	44
Replacing a Certificate	45
Deleting a Certificate	45
Generating a Certificate Signing Request	45

CHAPTER 7**Resource Management 47**

Viewing CPU Power Configuration	47
Applying CPU Power Cap	47

CHAPTER 8**GPU Management 49**

GPU Management	49
Configuring GPU Date and Time Settings	50
Viewing GPU FRU Information	50
Viewing GPU Power and Temperature Sensor	51
Viewing GPU Power Configuration	52
Applying GPU Power Cap	52
Event Logs	53
Viewing GPU Event Logs	53
Exporting GPU Event Logs	53
Updating GPU Firmware	54

APPENDIX A	REST API	55
	HTTP Methods	55
	Status Code	56
	Authentication	59
	Available APIs	60



Preface

This preface includes the following sections:

- [Audience, on page vii](#)
- [Conventions, on page vii](#)

Audience

This guide is intended primarily for data center administrators with responsibilities and expertise in one or more of the following:

- Server administration
- Storage administration
- Network administration
- Network security

Conventions

Text Type	Indication
GUI elements	GUI elements such as tab titles, area names, and field labels appear in this font . Main titles such as window, dialog box, and wizard titles appear in this font .
Document titles	Document titles appear in <i>this font</i> .
TUI elements	In a Text-based User Interface, text the system displays appears in <i>this font</i> .
System output	Terminal sessions and information that the system displays appear in <i>this font</i> .
CLI commands	CLI command keywords appear in this font . Variables in a CLI command appear in <i>this font</i> .
[]	Elements in square brackets are optional.

Text Type	Indication
{x y z}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x y z]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.



Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the document.



Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information, similar to a Timesaver.



Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.



Caution Means *reader be careful*. In this situation, you might perform an action that could result in equipment damage or loss of data.



Warning IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS



CHAPTER 1

Introduction

- [Overview of the Cisco UCS C885A M8 Rack Server, on page 1](#)
- [Introduction, on page 1](#)
- [Requirements, on page 3](#)
- [Logging into Cisco BMC, on page 3](#)
- [Navigation and Menu, on page 4](#)
- [Overview Page, on page 6](#)

Overview of the Cisco UCS C885A M8 Rack Server

The Cisco UCS C885A M8 Rack Server is a dense-GPU server designed to deliver massive, scalable accelerated compute capabilities to address the most demanding AI workloads, including deep learning/ Large Language Model (LLM) training, model fine-tuning, large model inferencing, and Retrieval-Augmented Generation (RAG).

To deliver massive accelerated compute performance in a single server, the server offers a choice of eight GPUs of the following types:

- NVIDIA[®] HGX H200 Server PCI Express Module (SXM) or Nvidia HGX H100 SXM GPUs. SXM is a socket-based GPU interconnect method used by NVIDIA GPUs.
- AMD MI300X OCP Accelerator Model (OAM) GPUs.

For north-south traffic, the server also supports up to two NVIDIA[®] BlueField B3220 DPUs or 2x200G ConnectX-7 NICs to scale AI model training across a cluster of dense-GPU servers. Up to eight NVIDIA[®] 1x400G ConnectX-7 or Bluefield-3 B3140H SuperNIC are supported for east-west traffic between GPUs.

Introduction

The Cisco Baseboard Management Controller (Cisco BMC) web GUI is HTML5 based and added security with SSL (HTTPS). It helps you manage the Cisco UCS C885A M8 Rack Server using the following options:

Hardware and Component Management

The Inventory feature enables administrators to record hardware devices and components on each server, such as central processing units (CPUs), memory modules, hard drives, network cards, and more.

Status and Checks

The Inventory feature also provides status and checks for hardware and software devices. This information can include device health status, temperature, voltage, connection status, and more.

Function	Description
Log in	Username Password
Overview	BMC date and time SOL console System information Status information
Logs	Event logs Post code logs Tech-support logs
Hardware status	Inventory and LEDs Sensors
Operations	Factory reset KVM Firmware update OEM Firmware Reboot BMC SOL console Server power operations Virtual media
Settings	Date and time Network Power restore policy
Security and access	Sessions LDAP User management Policies Certificates
Resource management	Power

Function	Description
GPU Management	Information Sensors Powers Event Logs Firmware Date and Time Note This option is available only for few Cisco UCS C885A M8 Rack Server configurations.

Requirements

Table 1: Operating System and Browser Requirements

Recommended Browser	Version Tested	Minimum Recommended Operating System
Mozilla Firefox	132.0.2 (AArch64)	macOS 15.1 (24B83)
	132.0 (64-bit)	Ubuntu 20.04.3 LTS
	132.0.2 (64-bit)	Microsoft Windows 11 Enterprise
Apple Safari	Version 18.1 (20619.2.8.11.10)	macOS 15.1 (24B83)
Google Chrome	131.0.6778.71 (64-bit)	Microsoft Windows 11 Enterprise
Microsoft Edge	131.0.2903.51 (64-bit)	Microsoft Windows 11 Enterprise

Logging into Cisco BMC

Before you begin

Ensure that all prerequisites are satisfied before attempting to log in.

Procedure

-
- Step 1** In your web browser, type or select the web link for Cisco BMC.
- Step 2** If a security dialog box displays, do the following:
- (Optional) Check the check box to accept all content from Cisco.

b) Click **Yes** to accept the certificate and continue.

Step 3 In the log in window, enter your username and password.

Note

When logging in for the first time to an unconfigured system, use **root** as the username and **password** as the password.

The following situations occur when you login to the Web UI for the first time:

- You cannot perform any operation until you change default credentials on the Web UI.
- You cannot close or cancel the password change pop-up window and opening it in a tab or refreshing the browser page will continue to display the pop-up window. This pop-up window appears when you login after a factory reset.
- You cannot choose the word `password` as your new password. If this creates problems for any scripts you may be running, you could change it to password by logging back into the user management options, but this is ENTIRELY at your own risk. It is not recommended by Cisco.

Step 4 Click **Log In**.

Navigation and Menu

Upon logging into Cisco BMC, you are directed to the Overview page. You will see the following options are available:

Menu Bar

The top menu bar has the following options:

Name	Description
Health	Allows you to view the Event log .
Power	Allows you to view and configure Server Power Operations .
Refresh	Allows you to refresh the BMC sensor values.
root	Allows you to log out or change password from profile settings.

Navigation Pane

The left navigation pane has the following options:

Function	Description
Log in	Username Password

Function	Description
Overview	BMC date and time SOL console System information Status information
Logs	Event logs Post code logs Tech-support logs
Hardware status	Inventory and LEDs Sensors
Operations	Factory reset KVM Firmware update OEM Firmware Reboot BMC SOL console Server power operations Virtual media
Settings	Date and time Network Power restore policy
Security and access	Sessions LDAP User management Policies Certificates
Resource management	Power

Function	Description
GPU Management	Information Sensors Powers Event Logs Firmware Date and Time Note This option is available only for few Cisco UCS C885A M8 Rack Server configurations.

Overview Page

After logging into the Cisco BMC GUI, you are directed to the **Overview** page. From this page, you can quickly access important features and information. Below are the key properties and sections of the **Overview** page:

BMC Date and Time

Table 2: BMC Date and Time

Name	Description
BMC date and time field	This field allows you to view and set the date and time on the BMC system.
SOL button	This button initiates the Serial over LAN (SOL) session for remote management and troubleshooting. For more information, see Viewing Serial over LAN (SOL) console, on page 26 .

System Information

Table 3: Server Information

Name	Description
Model field	This field displays the model of the server.
Serial number field	This field shows the unique serial number assigned to the server.
Server manufacturer field	This field identifies the manufacturer of the server.

Name	Description
View more link	Click to see more information. Viewing Inventory and LEDs, on page 13.

Table 4: Firmware Information

Name	Description
Running field	This field indicates the current version of the firmware running on the system.
View more link	Click to see more information. Viewing BMC Firmware Version, on page 24.

Table 5: Network Information

Name	Description
Hostname field	This field displays the network hostname assigned to the server.
Link status field	This field shows the current status of the network link (e.g., LinkUp).
Static IPv4 field	This field indicates the static IPv4 address, if configured, for the server.
DHCPv4 field	This field displays the IPv4 address assigned to the server via DHCP.
View more link	Click to see more information. Network Management in Cisco BMC, on page 32.

Table 6: Power Information

Name	Description
CPU 0 Power field	This field shows the power consumption of CPU 0.
CPU 1 Power field	This field shows the power consumption of CPU 1.
View more link	Click to see more information. Viewing CPU Power Configuration, on page 47.

Status Information

Table 7: Event Logs

Name	Description
Critical field	This field displays the number of critical events logged in the system.
Warning field	This field indicates the number of warning events logged in the system.
Export all link	Click to export the logs. Depending on your browser settings, you may be prompted to open or save the JSON log file.
View more link	Click to see more information. Viewing Event Logs, on page 9.

Table 8: Inventory and LEDs

Name	Description
System identify LED field	This field shows the status of the system identification LED, which can be toggled on or off to identify the system physically.
View more link	Click to see more information. Viewing Inventory and LEDs, on page 13.



CHAPTER 2

Logs

- [Event Logs, on page 9](#)
- [POST Logs, on page 11](#)
- [Tech-support log, on page 12](#)

Event Logs

Viewing Event Logs

The Logging and Callouts feature is essential for managing and tracking system events, providing a comprehensive view of operational status by logging and reporting various events such as warnings, errors, and abnormal conditions.

- **Logging:** Records system events and abnormal conditions, storing them in system event logs. Events can include hardware failures, system errors, temperature anomalies, power supply issues, and more.
- **Callouts:** Trigger predefined actions when specific events occur. For example, when a hardware failure or other critical event is detected, callouts can automatically trigger alerts, notify remote management systems, or execute specified commands.

Procedure

Step 1 From the **Navigation Pane**, select **Logs > Event logs**.

Step 2 You can filter the event logs based on the following options:

- **From** and **to** dates
- Based on severity: **OK**, **Warning**, and **Critical**
- Search keyword using the search field

You can view the following log properties:

Name	Description
ID column	Displays the unique identifier for each log entry.

Name	Description
Severity column	Indicates the level of importance or impact of the log entry. This can be one of the following: <ul style="list-style-type: none"> • OK—Indicates that the log entry represents a normal or successful operation. • Critical—Indicates a severe issue that requires immediate attention. • Warning—Indicates a potential issue that should be monitored.
Date column	Shows the date and time when the log entry was recorded.
Description column	Provides a brief summary or details about the log entry.

Exporting Event Logs

Procedure

Step 1 From the **Navigation Pane**, select **Logs > Event logs**.

Step 2 To export all log entries, click **Export all**.

Depending on your browser settings, you may be prompted to open or save the log file.

Deleting Event Logs

Procedure

Step 1 From the **Navigation Pane**, select **Logs > Event logs**.

Step 2 To delete all log entries, click **Delete all**.

Step 3 In the **Delete Log** dialog box, click **Delete** to confirm.

POST Logs

Viewing POST Code Logs

Procedure

Step 1 From the **Navigation Pane**, select **Logs > POST code logs**.

Step 2 You can filter the logs based on the following options:

- **From** and **to** dates
- Search keyword using the search field

You can view the following log properties:

Name	Description
Created column	Displays the date and time when the POST code log was generated.
Time stamp offset column	Indicates the time offset from the system start when the POST code was logged.
Boot count column	Shows the number of times the system has booted up.
POST code column	Displays the Power-On Self-Test (POST) code.
Description column	Provides details about the POST code log entry.

Exporting POST Code Logs

Procedure

Step 1 From the **Navigation Pane**, select **Logs > POST code logs**.

Step 2 To export all log entries, click **Export all**.

Depending on your browser settings, you may be prompted to open or save the log file.

Tech-support log

Downloading Tech Support Logs

Procedure

Step 1 From the **Navigation Pane**, select **Logs > Tech-support code logs**.

Step 2 Click **Download** to start the download process.

Step 3 Click **Confirm** to continue and save the log file.

Depending on your browser settings, you may be prompted to open or save the log file.



CHAPTER 3

Hardware Status

- [Viewing Inventory and LEDs](#), on page 13
- [CPU Monitoring and Management](#), on page 19
- [Cooling Management](#), on page 20
- [Managing Fan Failure Conditions](#), on page 21
- [Viewing Sensor Status](#), on page 21
- [Turning On/Off System Identify LED](#), on page 22

Viewing Inventory and LEDs

Procedure

Step 1 From the **Navigation Pane**, select **Hardware Status > Inventory and LEDs**.

Step 2 You can view the following properties:

Table 9: LED Light Control

Name	Description
Power status field	Displays the current power status of the system.
System identity LED toggle button	Toggles the system identity LED on or off to help locate the system.

Table 10: System

Name	Description
ID column	Displays the unique identifier for each system.
Hardware type column	Indicates the type of hardware for each system.
Health column	Shows the current health status of each system.

Name	Description
Identify LED column	Indicates whether the identify LED is on or off for each system.
Serial number field	Displays the serial number of the system.
Model field	Displays the model of the system.
Asset tag field	Displays the asset tag of the system.
Status (State) field	Indicates the current state of the system.
Power field	Displays the current power status of the system.
Health rollup field	Shows the overall health status of the system.
Manufacturer field	Displays the manufacturer of the system.
Description field	Provides a brief description of the system.
Sub model field	Displays the sub model of the system.
System type field	Indicates the type of system.
Memory summary	Provides a summary of the system memory.
Status (State) field	Indicates the current state of the memory.
Health field	Shows the current health status of the memory.
Health rollup field	Shows the overall health status of the memory.
Total system memory field	Displays the total memory available in the system.
Processor summary	Provides a summary of the system processors.
Status (State) field	Indicates the current state of the processor.
Health field	Shows the current health status of the processor.
Health rollup field	Shows the overall health status of the processor.
Count field	Displays the number of processors in the system.
Core count field	Displays the number of cores per processor.

Table 11: BMC Manager

Name	Description
ID column	Displays the unique identifier for each BMC manager entry.
Health column	Shows the current health status of the BMC manager.
Name field	Cisco Integrated Management Controller

Name	Description
Model field	Displays the model of the BMC manager.
UUID field	Displays the UUID of the BMC manager.
Service entry point UUID field	Displays the service entry point UUID of the BMC manager.
Status (State) field	Indicates the current state of the BMC manager.
Power field	Displays the current power status of the BMC manager.
Health rollup field	Shows the overall health status of the BMC manager.
BMC date and time field	Displays the current date and time of the BMC.
Last reset time field	Displays the last reset time of the BMC.
Description field	Provides a brief description of the BMC manager.
Manager type field	Indicates the type of the BMC manager.
Firmware version field	Displays the firmware version of the BMC manager.
OEM firmware version	
BIOS field	Displays the BIOS version.
SCM FPGA field	Displays the SCM FPGA version.
MB FPGA field	Displays the MB FPGA version.
HIB FPGA field	Displays the HIB FPGA version.
RoT field	Displays the RoT version.
Graphical console	
Connect types supported field	Displays the supported connection types for the graphical console.
Max concurrent sessions field	Displays the maximum number of concurrent sessions for the graphical console.
Service enabled field	Indicates whether the service for the graphical console is enabled.
Serial console	
Connect types supported field	Displays the supported connection types for the serial console.
Max concurrent sessions field	Displays the maximum number of concurrent sessions for the serial console.

Name	Description
Service enabled field	Indicates whether the service for the serial console is enabled.

Table 12: Chassis

Name	Description
ID column	Displays the unique identifier for each chassis entry.
Health column	Shows the current health status of the chassis.
Following properties are displayed for FRU_CHASSIS , FRU_CPUSLED , FRU_SCM , and FRU_SYS :	
Board build date field	Displays the build date of the board.
Board manufacturer field	Displays the manufacturer of the board.
Board product field	Displays the product name of the board.
Board part number field	Displays the part number of the board.
Board serial number field	Displays the serial number of the board.
Board extra field	Displays any additional information about the board.
Product manufacturer field	Displays the manufacturer of the product.
Product name field	Displays the product name.
Product part number field	Displays the part number of the product.
Product serial number field	Displays the serial number of the product.
Product version field	Displays the version of the product.
Product extra field	Displays any additional information about the product.
Product asset tag field	Displays the asset tag of the product.
Chassis type field	Indicates the type of the chassis.
Chassis part number field	Displays the part number of the chassis.
Chassis serial number field	Displays the serial number of the chassis.
Chassis extra field	Displays any additional information about the chassis.
Health rollup field	Shows the overall health status of the chassis.

Table 13: DIMM Slot

Name	Description
ID column	Displays the unique identifier for each DIMM slot entry.
Health column	Shows the current health status of the DIMM slot.
Location number column	Indicates the location number of the DIMM slot.
Part number field	Displays the part number of the DIMM.
Serial number field	Displays the serial number of the DIMM.
Capacity MiB field	Displays the capacity of the DIMM in MiB.
Status (State) field	Indicates the current state of the DIMM slot.
Enabled field	Indicates whether the DIMM slot is enabled.
Description field	Provides a brief description of the DIMM.
Memory type field	Displays the type of memory of the DIMM.
Base module type field	Indicates the base module type of the DIMM.
Bus width bits field	Displays the bus width of the DIMM in bits.
Data width bits field	Displays the data width of the DIMM in bits.
Operating speed Mhz field	Displays the operating speed of the DIMM in MHz.

Table 14: Storage

Name	Description
ID column	Displays the unique identifier for each storage entry.
Health column	Shows the current health status of the storage.
StorageControllers (Name) field	Displays the name of the storage controller.
StorageControllers (FirmwareVersion) field	Displays the firmware version of the storage controller.
Description field	Provides a brief description of the storage.
SpeedGbps field	Displays the speed of the storage in Gbps.
Model field	Displays the model of the storage.
Status (State) field	Indicates the current state of the storage.
SerialNumber field	Displays the serial number of the storage.

Table 15: Fans

Name	Description
ID column	Displays the unique identifier for each fan entry.
Health column	Shows the current health status of the fan.
Name field	Displays the name of the fan.
Part number field	Displays the part number of the fan.
Fan speed field	Displays the speed of the fan in RPM.
Status (State) field	Indicates the current state of the fan.
Status (Health rollup) field	Shows the overall health status of the fan.

Table 16: Power Supplies

Name	Description
ID column	Displays the unique identifier for each power supply entry.
Health column	Shows the current health status of the power supply.
Name field	Displays the name of the power supply.
Part number field	Displays the part number of the power supply.
Serial number field	Displays the serial number of the power supply.
Spare part number field	Displays the spare part number of the power supply.
Model field	Displays the model of the power supply.
Status (State) field	Indicates the current state of the power supply.
Manufacturer field	Displays the manufacturer of the power supply.

Table 17: Processors

Name	Description
ID column	Displays the unique identifier for each processor entry.
Health column	Shows the current health status of the processor.
Name field	Displays the name of the processor.
Part number field	Displays the part number of the processor.
Serial number field	Displays the serial number of the processor.
Model field	Displays the model of the processor.

Name	Description
Asset tag field	Displays the asset tag of the processor.
Status (State) field	Indicates the current state of the processor.
Manufacturer field	Displays the manufacturer of the processor.
Processor type field	Indicates the type of the processor.
Processor architecture field	Displays the architecture of the processor.
Instruction set field	Displays the instruction set supported by the processor.
Max speed MHz field	Displays the maximum speed of the processor in MHz.
Total cores field	Displays the total number of cores in the processor.
Total threads field	Displays the total number of threads in the processor.

Table 18: Network Adapters

Name	Description
ID column	Displays the unique identifier for each network adapter entry.
Health column	Shows the current health status of the network adapter.
Name field	Displays the name of the network adapter.
Vendor field	Displays the vendor of the network adapter.
Serial number field	Displays the serial number of the network adapter.
Part number field	Displays the part number of the network adapter.
Manufacturer field	Displays the manufacturer of the network adapter.
Firmware version field	Displays the firmware version of the network adapter.
Status (State) field	Indicates the current state of the network adapter.

CPU Monitoring and Management

Overview

The CPU is a central component of the system responsible for executing all computational tasks. The BMC monitors aspects of the CPU such as temperature and power consumption to ensure operation within normal ranges. This helps prevent overheating and hardware failures, ensuring system stability and reliability.

Additionally, it allows administrators to understand the system's workload and adjust resource allocation as needed, optimizing performance and response times.

Anomaly Detection and Response

If the CPU encounters anomalies, such as excessively high temperatures, the BMC can monitor and provide warnings, enabling administrators to promptly respond and troubleshoot issues.

Monitored and Controlled Features

The BMC monitors and controls the following CPU features:

- Get CPU temperature
- Get CPU current power consumption
- Get CPU maximum power capping
- Get CPU current power capping
- Set CPU power capping

Cooling Management

The BMC is responsible for managing the cooling system by overseeing temperature sensors and regulating fan speeds based on a Fan Algorithm crafted by the thermal engineering team.

BMC Boot Process and Default Fan Control

During the BMC boot process, if temperature readings from components are not successfully acquired, the BMC implements default fan control. In this scenario, all fans operate at a duty cycle of 80% until temperature data from all system sensors is accessible.

Fan Algorithm Activation

When the fan algorithm is active, the BMC manages fan speeds or initiates a system shutdown under specific conditions:

- Condition for full speed fan operation:
 - A temperature of the component exceeds a specified threshold.
 - Temperature reading fails for more than 60 seconds.
 - A firmware update is initiated.
 - GPU does not align with system specifications.
- Conditions for shut down the system:
 - Temperature exceeds a critical threshold for more than 60 seconds.
 - Temperature exceeds the specified threshold (UNR).

Managing Fan Failure Conditions

The system fans are divided into three fan zones, each serving a specific cooling function:

- **Fan Zone #1:** Used for GPU sled cooling.
- **Fan Zone #2:** Used for CPU sled cooling.
- **Fan Zone #3:** Used for SSD cooling.

Fan Failure Response

When a fan failure condition occurs, the BMC sets all remaining fans to run at full speed or shuts down the system. Once the fan failure condition is cleared, the BMC restores fan speed according to the fan control algorithm. Fan failures are classified into the following scenarios:

- **Fan Zone #1 Failure Conditions:**
 - If either one or both fan rotors in the same fan are below the specified threshold (LC), all remaining fans in Fan Zone #1 run at full speed.
 - If two fan rotors are below the threshold (LC) in different fans, or if three or more fan rotors are below the threshold (LC), the system shuts down.
- **Fan Zone #2 Failure Conditions:**
 - If one fan rotor is below the specified threshold (LC), all remaining fans in Fan Zone #2 run at full speed.
 - If two fan rotors are below the threshold (LC), the system shuts down.
- **Fan Zone #3 Failure Conditions:**
 - If one fan rotor is below the specified threshold (LC), all remaining fans in Fan Zone #3 run at full speed.
 - If two fan rotors are below the threshold (LC), the system shuts down.

Viewing Sensor Status

The BMC monitors key system sensors, including temperature, power, fan speeds, and logical sensors. These sensors provide real-time values and statuses, accessible through the GUI .

Procedure

Step 1 From the **Navigation Pane**, select **Hardware Status > Sensors**.

Step 2 Select of the following tabs to view the properties:

- POWER SUPPLY

- Fan
- Temperature
- CPU
- GPU
- Event

You can view the following sensor properties:

Table 19: Threshold Sensors/Discrete Sensors

Name	Description
Name column	Displays the name of the sensor.
Status column	Shows the current status of the sensor.
Lower critical field	Displays the lower critical threshold value for the sensor.
Lower warning field	Displays the lower warning threshold value for the sensor.
Current value field	Displays the current value measured by the sensor.
Upper warning field	Displays the upper warning threshold value for the sensor.
Upper critical field	Displays the upper critical threshold value for the sensor.

Turning On/Off System Identify LED

Procedure

- Step 1** From the **Navigation Pane**, select **Hardware Status > Inventory and LEDs**.
- Step 2** Under **LED light control**, toggle the **System identity LED** button on or off to help locate the system.



CHAPTER 4

Operations

- [Resetting Cisco BMC and Server to Factory Settings, on page 23](#)
- [Launching KVM Console, on page 24](#)
- [BMC Firmware, on page 24](#)
- [Updating OEM Firmware, on page 25](#)
- [Rebooting BMC, on page 26](#)
- [Viewing Serial over LAN \(SOL\) console, on page 26](#)
- [Server Power Operations, on page 27](#)
- [Adding Virtual Media Image, on page 29](#)

Resetting Cisco BMC and Server to Factory Settings

The Cisco BMC system includes a factory reset interface that restores the BMC to its original manufacturer settings. This interface is broadly defined, allowing for varied implementations across different Cisco BMC services. This flexibility enables you to reset individual services to their factory defaults as needed.

If the server is off, you may see the following message:

```
Do you want to reset both the BMC and server settings?
```

Before you begin

Prior to resetting the BMC, consider the following:

- All manual settings are deleted.
- Partition configurations and the platform keystore can be recovered if backups exist.
- All BMC logs are removed.
- Currently active sessions on all network interfaces are disconnected.
- The BMC default account and password settings are restored.

Procedure

Step 1 From the **Navigation Pane**, select **Operations > Factory reset**.

Step 2 Click check box **Continue without shutting down the system**.

Step 3 Click **Reset BMC and server settings**.

If Host is in ON state, following warning message is displayed:

```
Reset BMC and server settings
```

```
Do you want to reset both the BMC and server settings?
```

```
All manual settings will be deleted.
```

```
Partition configurations and the platform keystore may be recovered if backups exist.
```

```
All BMC logs will be removed.
```

```
Currently active sessions on all network interfaces will be disconnected.
```

```
The BMC default account and password settings will be restored.
```

```
Resetting without shutting down the system might cause an unrecoverable error.
```

```
Continue without shutting down the system
```

Step 4 Click **Yes** to continue.

Launching KVM Console

Procedure

Step 1 From the **Navigation Pane**, select **Operations > KVM**.

Step 2 Click **Launch KVM**.

KVM window opens as a new tab or window depending on your browser settings.

BMC Firmware

Viewing BMC Firmware Version

Procedure

Step 1 From the **Navigation Pane**, select **Operations > Firmware**.

Step 2 Under **Firmware Update**, you can view the **Provision Status**.

Step 3 In the **BMC and server** section, under **Running image** you can view the **Version**.

The BMC firmware version is represented as X.Y.Z, where X is the major version, Y is the minor version, and Z represents the BMC Aux firmware version. For example, the BMC firmware version number 1 . 1 . 4.

Updating BMC Firmware Version



Note During the update process, the HTTPS service is temporarily unavailable. You cannot access the WebUI, Redfish, or other related services during this period. Wait until the service is fully restored before attempting to access any resources.

Before you begin

Ensure that the firmware file is available on the client before starting this procedure.

Procedure

-
- Step 1** From the **Navigation Pane**, select **Operations > Firmware**.
- Step 2** Click **Add File** and browse to locate the firmware file.
Select the firmware file.
- Step 3** Click **Start Update** to initiate the firmware update.
-

What to do next

After the firmware update completes, perform an AC power cycle to activate and complete the upgrade.

Updating OEM Firmware

Before you begin

Ensure that the firmware file is available on the client before starting this procedure.



Note Depending on the type of firmware being upgraded, an OEM firmware upgrade may necessitate either an AC power cycle or a host power cycle.

- **BIOS Firmware:** Requires a host power cycle for activation. Ensure this step can be performed after the upgrade.
- **FPGA Firmware:** Requires a server AC power cycle for activation. Be prepared to complete this action following the upgrade.

Procedure

-
- Step 1** From the **Navigation Pane**, select **Operations > OEM Firmware**.
- Step 2** Select a specific device from the drop-down list to update.
- Step 3** Click **Add File** and browse to locate the firmware file.
Select the firmware file.
- Step 4** Click **Start Update** to begin the firmware update.
-

What to do next

After the firmware update completes, perform an AC power cycle to activate and complete the upgrade.

Rebooting BMC



Note Rebooting the BMC causes the web browser to lose contact with the BMC for several minutes. After the BMC is back online, logging in again may be necessary.

Procedure

-
- Step 1** From the **Navigation Pane**, select **Operations > Reboot BMC**.
- Step 2** Click **Reboot BMC**.
Click **Confirm** to continue to reboot.
-

Viewing Serial over LAN (SOL) console

Serial over LAN (SOL), or BMC Serial Traffic Redirection, redirects serial controller traffic from the baseboard to an IPMI session. This protocol enables asynchronous communication within the operating system (OS) and during the pre-OS phase through a connection with the BMC. SOL is particularly useful for engaging with serial text-based interfaces, such as OS command-line interfaces, serial-redirected BIOS interfaces, and other serial text-based applications, all through an IPMI LAN session.

SOL integrates LAN-based access to IPMI platform management with serial text redirection in a unified interface, allowing a single remote console application to support both functionalities. Authorization and access control for SOL are managed through the same user configuration interfaces used for IPMI management. This integration streamlines the development of configuration software, remote management applications, and configuration utilities that work cohesively across various platforms.

Procedure

-
- Step 1** From the **Navigation Pane**, select **Operations > SOL console**.
- Step 2** Use the on-screen interface to monitor and manage the server serial port output as if directly connected.
-

Server Power Operations

Viewing Server Power Status

Procedure

-
- Step 1** From the **Navigation Pane**, select **Operations > Server power operations**.
- Step 2** Under **Current status**, you can view the following properties:

Name	Description
Server status	Indicates whether the server is currently powered on or off.
Last power operation	Records the date and time of the most recent power cycle or shutdown event for the server.

Rebooting the Server

Before you begin

The **Reboot** option is available only when the server is powered on. If the server is powered off, the **Reboot** option is not visible, and **Power On** appears instead.

Procedure

-
- Step 1** From the **Navigation Pane**, select **Operations > Server power operations**.
- Step 2** Under **Reboot server**, only one option is available and, by default, is selected:
- **Orderly** — operating system shuts down, then server reboots
- Step 3** Click **Reboot** to initiate the reboot process.
-

Shutting Down the Server

Before you begin

The **Shut down** option is available only when the server is powered on. If the server is powered off, the **Shut down** option is not visible, and **Power On** appears instead.

Procedure

- Step 1** From the **Navigation Pane**, select **Operations > Server power operations**.
- Step 2** From the shutdown options, choose one of the following:
- **Orderly** — operating system shuts down, then server reboots
 - **Immediate** — Server shuts down without operating system shutting down; may cause data corruption
- Step 3** Click **Shut down** to initiate the shutdown process.
-

Overriding Boot Source

Procedure

- Step 1** From the **Navigation Pane**, select **Operations > Server power operations**.
- Step 2** From the **Boot Source Override** drop-down list, choose the desired boot source.
- Step 3** Select **Enable one time boot** to temporarily change the boot device for the next system startup without altering the default boot sequence.
- Step 4** Click **Save** to apply the changes.
-

Performing AC Power Cycle on the Server

Before you begin

The **Shut down** option is available only when the server is powered on. If the server is powered off, the **Shut down** option is not visible, and **Power On** appears instead.

Procedure

- Step 1** Identify the Server using the **System Identify LED**:
- On the **Overview** page, under **Inventory and LEDs**, toggle the **System Identify LED** button.

Confirm the physical location of the server before proceeding.

Step 2 From the **Navigation Pane**, select **Operations > Server power operations**.

Step 3 From the shutdown options, choose the following:

- **Immediate** — Server shuts down without operating system shutting down; may cause data corruption

Step 4 Click **Shut down** to initiate the shutdown process.

Step 5 Physically Disconnect the Power Source:

Disconnect the power cables from the back of the server.

If the server has redundant power supplies, ensure that all power cables are disconnected.

Wait for 1–2 minutes to allow any residual power within the server components to fully discharge.

Step 6 Reconnect the power cables securely to the server. If the server has redundant power supplies, reconnect all power cables.

Step 7 From the **Navigation Pane**, select **Operations > Server power operations**.

Step 8 Click **Power On**.

Adding Virtual Media Image

Virtual Media allows you to remotely mount ISO/IMG drive images through the BMC to the server host. The remote drive appears on the host as a USB storage device and operates in either read-only or read-write mode, considering container limitations and write protection switches. This feature is used to install an OS on a server.

Before you begin

Ensure that the image file is available on the client before starting this procedure.



Note Only local images are supported. Mapping images from remote file shares or mapping virtual media (vMedia) outside the client is not supported. Ensure all images are stored locally for proper functionality.

Procedure

Step 1 From the **Navigation Pane**, select **Operations > Virtual media**.

Step 2 Click **Add file** and browse to the image, which you wish to add.

Select the image file.

Step 3 Click **Start**.



CHAPTER 5

Settings

- [Configuring BMC Date and Time Settings, on page 31](#)
- [Network Management in Cisco BMC, on page 32](#)
- [Setting Power Restore Policies, on page 35](#)

Configuring BMC Date and Time Settings

Procedure

Step 1 From the **Navigation Pane**, select **Settings > Date and time**.

Step 2 Under **Configure Settings**, choose between the following options:

- Manual
- NTP

Step 3 For **Manual**, update the following properties:

Name	Description
Date field	Enter in YYYY-MM-DD format.
24-hour time (UTC) field	Enter time in HH:MM format.

Step 4 For **NTP**, update the following properties:

Name	Description
Server 1 field	Specify the first NTP server.
Server 2 field	Specify the second NTP server.
Server 3 field	Specify the third NTP server.

Step 5 Click **Save Settings**.

Network Management in Cisco BMC

Cisco BMC offers diverse interfaces, including Web GUI, Redfish, and IPMI commands, to facilitate comprehensive management of the BMC network. Network configuration involves tasks such as configuring IP addresses, IP address sources, and gateways.

Fundamental network configuration features include:

- IP Addresses Source
- IP Address
- Gateways
- subnet mask

Viewing or Configuring Network Settings



Note The Shared NIC (eth1) is associated with the X710 OCP card. Ensure this configuration is considered when setting up your network interfaces to optimize connectivity and performance.

When using OCP (eth1) for management traffic, the NCSI support is available only on Port 1 of the OCP card.

Procedure

Step 1 From the **Navigation Pane**, select **Settings > Network**.

Step 2 Under **Network Settings**, update the following properties:

Name	Description
Hostname field	Specifies the fully qualified domain name (FQDN) for the BMC. Click the edit button to update the domain name.
Use domain name toggle button	Enable or disable the option to use the domain name for network communications.
Use DNS servers toggle button	Enable or disable the option to use DNS servers for resolving hostnames to IP addresses.
Use NTP servers toggle button	Enable or disable the option to use Network Time Protocol servers to synchronize the BMC's clock

Name	Description
Use Shared NIC (eth1) toggle button	Enable or disable the option to use the shared network interface card (NIC) eth1 for network connectivity.

Step 3 Under **eth0/ehl1**, you can view the following properties:

Name	Description
Link status field	Indicates the current status of the network link, showing whether it is active (LinkUp) or inactive.
Speed (mbps) field	Displays the current speed of the network connection in megabits per second (Mbps).
Interface settings	
FQDN field	Specifies the fully qualified domain name (FQDN) assigned to the interface.
MAC address field	Displays the unique Media Access Control (MAC) address assigned to the network interface.

Viewing or Adding IPv4 Address

Procedure

Step 1 From the **Navigation Pane**, select **Settings > Network**.

Step 2 Under **IPv4**, update the following properties:

Name	Description
DHCP toggle button	Enable or disable the Dynamic Host Configuration Protocol (DHCP) for automatic IP address assignment. When you enable DHCP, Add static IPv4 address windows is displayed.
IP Address field	Specify the Internet Protocol (IP) address assigned to the device, which uniquely identifies it on the network.
Gateway field	Enter the IP address of the network gateway, which serves as the access point or router that passes traffic between the local network and other networks or the internet.
Subnet mask field	Enter the network address range by specifying which portion of the IP address refers to the network and which part refers to the device.

Step 3 Under **IPv4 addresses**, you can view the following properties:

Name	Description
IP address column	Specifies the Internet Protocol (IP) address assigned to the device, which uniquely identifies it on the network.
Gateway column	Refers to the IP address of the network gateway, which serves as the access point or router that passes traffic between the local network and other networks or the internet.
Subnet mask column	Defines the network address range by specifying which portion of the IP address refers to the network and which part refers to the device.
Address origin column	Indicates how the IP address is obtained, whether dynamically assigned by DHCP or statically set by the user.

Viewing, Adding, or Deleting Static DNS IP Address

Procedure

Step 1 From the **Navigation Pane**, select **Settings > Network**.

Step 2 Under **Static DNS**, click **Add IP address**.

Add IP address window is displayed.

Step 3 In the **Add IP address** window, update the following properties:

Name	Description
Static DNS field	Enter the static DNS server addresses to be used for domain name resolution when DHCP is disabled.

Step 4 Click **Add**.

Step 5 (Optional) To delete an IP address, click the delete icon corresponding to the row you want to delete.

Setting Power Restore Policies

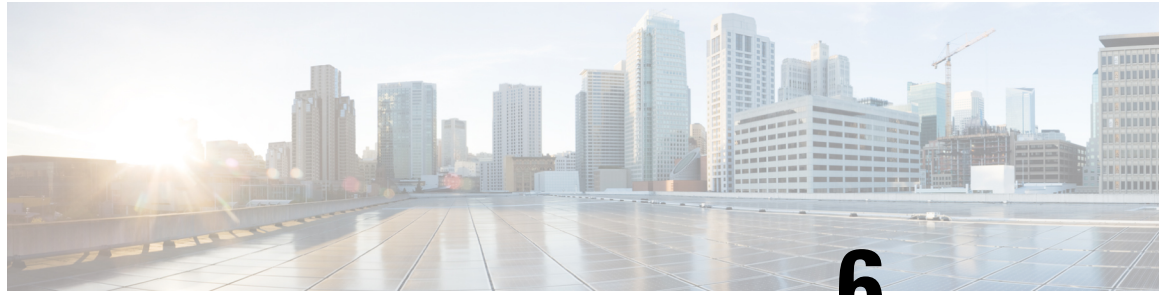
Procedure

Step 1 From the **Navigation Pane**, select **Settings > Power restore policy**.

Step 2 Under **power restore policies** select one of the following:

- Always on—The system powers on whenever power is applied.
- Always off—The system remains powered off when power is applied.
- Last state—The system returns to its last power state (on or off) when power is applied.

Step 3 Click **Save settings**.



CHAPTER 6

Security and Access

- [User Session](#), on page 37
- [LDAP Configuration](#), on page 38
- [User Management](#), on page 40
- [Updating Policies](#), on page 43
- [Managing Certificates](#), on page 43

User Session

Viewing User Sessions

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > Sessions**.

Step 2 You can view the following properties:

Name	Description
Session ID column	A unique identifier assigned to each active web user session for tracking and management purposes.
Username column	The account name associated with the server login session.
IP address column	The network address of the device accessing the server during the session.

Disconnecting a Session

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Sessions**.
- Step 2** To disconnect a session, click **Disconnect** corresponding to the session row you want to disconnect.

LDAP Configuration

Enabling LDAP Authentication

In the Cisco BMC, the SSH, Redfish, Webservice, and Host Console interfaces allow authentication against an LDAP directory. However, the IPMI interface cannot authenticate against LDAP, as it requires the password in clear text during session setup. PAM-based authentication is implemented, ensuring that the authentication flow is the same for both LDAP users and local users.

For LDAP user accounts, there is no LDAP attribute type corresponding to the Cisco BMC privilege roles. The preferred method is to group LDAP user accounts into LDAP groups. Privilege roles can then be assigned to the LDAP group using Redfish and the GUI.

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > LDAP**.
- Step 2** Under LDAP authentication, update the following properties:

Name	Description
Enable check box	Check the Enable check box to activate LDAP authentication options.
Service Type radio button	Choose the appropriate service type by selecting a radio button: <ul style="list-style-type: none"> • Select OpenLDAP radio button to use OpenLDAP as the directory service. • Select Active Directory radio button to use Microsoft's Active Directory service.
Server URI field	Enter the URI for the server.
Bind DN field	Enter the Base Distinguished Name.
Bind Password field	Enter the password for the Bind DN.

Name	Description
Base DN field	Enter the Base Distinguished Name.
User ID Attribute - (optional) field	Enter the attribute for user identification.
Group ID Attribute - (optional) field	Enter the attribute for group identification.
Manage SSL Certificate link	Click Adding a New Certificate, on page 44 for more information.

Step 3 Click **Save settings**.

Adding Role Group

Group roles determine the first-level authorization for users, establishing whether access to the required interface is permitted. For example, a user should not be able to log in to SSH if they only belong to the webserver group and not to the SSH group. Having group roles within common user management allows different applications to create roles for each other. For instance, an administrative user can create a new user through the webserver, granting them the ability to log in to webserver, Redfish, IPMI, and other interfaces.

Before you begin

Ensure that LDAP authentication is enabled.

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > LDAP**.

Step 2 Click **Add role group**.

Step 3 Update the following:

Name	Description
Group Name field	Enter the name of the role group to identify it within the system.
Group Privilege field	Select the appropriate level of access for the group from the drop-down list: <ul style="list-style-type: none"> • Administrator • Operator • ReadOnly

User Management

Adding a User

Cisco BMC provides a Web GUI to facilitate effective management of user accounts. This includes tasks such as defining user names, setting and modifying passwords, and configuring privilege levels and channel access. These settings are linked to individual user IDs and are stored as a structured array within the non-volatile storage framework associated with the management controller.

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > User Management**.

Step 2 Click **Add user**.

Add user window is displayed.

Step 3 In the **Add user** window update the following properties:

Name	Description
Account status radio button	Select Enabled radio button to activate the account immediately. Select Disabled radio button to create the account without activation.
Username field	Enter the desired username. Follow the UI instructions for username rules.
User password field	Enter the password for the user. Follow the UI instructions for password rules.
Confirm user password field	Re-enter the password to confirm.
Privilege drop-down list	From the Privilege drop-down list, choose the appropriate role: <ul style="list-style-type: none"> • Administrator—Full access and control. • Operator—Limited operational access. • ReadOnly—View-only access.

Step 4 Click **Add user**.

Editing a User

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > User Management**.

Step 2 To edit a user, click the edit icon corresponding to the user row you want to edit.

Edit user window is displayed.

Step 3 In the **Edit user** window update the following properties:

Name	Description
Account status radio button	Select Enabled radio button to activate the account immediately. Select Disabled radio button to create the account without activation.
Username field	Enter the desired username. Follow the UI instructions for username rules.
User password field	Enter the password for the user. Follow the UI instructions for password rules.
Confirm user password field	Re-enter the password to confirm.
Privilege drop-down list	From the Privilege drop-down list, choose the appropriate role: <ul style="list-style-type: none"> • Administrator—Full access and control. • Operator—Limited operational access. • ReadOnly—View-only access.

Step 4 Click **Save**.

Enabling or Disabling a User

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > User Management**.

Step 2 To enable/disable a user, check the check box corresponding to the user row you want to enable/disable.

When you check the check box, a new header row with additional options appears at the top of the table.

Step 3 Click **Enable/Disable**.

Managing Account Policy Settings

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > User Management**.

Step 2 Click **Account policy settings**.

Account policy settings window is displayed.

Step 3 In the **Account policy settings** window update the following properties:

Name	Description
Max failed login attempts field	Enter a value between 0 and 65535.
User unlock method radio button	Select one of the following options: <ul style="list-style-type: none"> • Manual—Choose the Manual radio button to require manual intervention for unlocking. • Automatic After Timeout—Choose the Automatic After Timeout radio button to unlock automatically after a specified timeout.
Timeout duration (seconds) field	If Automatic After Timeout is selected, enter the duration from the Timeout Duration (seconds) .

Step 4 Click **Save**.

Deleting a User

You cannot delete a root user.

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > User Management**.

Step 2 To delete a user, check the check box corresponding to the user row you want to delete.

When you check the check box, a new header row with additional options appears at the top of the table.

Step 3 Click **Delete**.

Updating Policies

Enabling or Disabling BMC Shell through SSH

The BMC Health Monitor in Cisco BMC tracks and reports the health status of the BMC, providing real-time updates on its operational status. This feature monitors key indicators such as temperature, voltage, fan speed, and hardware health events. It assists administrators in ensuring the proper functioning of the BMC by offering necessary monitoring and alert mechanisms. By delivering comprehensive real-time health reports, it enables administrators to quickly identify and resolve issues, enhancing system maintenance and reliability.

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Policies**.
- Step 2** Use the BMC Shell (via SSH) toggle button to enable or disable access to shell sessions through port 22 on the BMC.
-

Enabling or Disabling Network IPMI

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Policies**.
- Step 2** Use the Network IPMI (Out-of-Band IPMI) toggle button to enable or disable remote management via IPMI.
-

Managing Certificates

Viewing Certificate Details

Certificate management allows easy replacement of existing certificate and private key files with alternatives, which may be issued by a Certification Authority (CA). This feature enables you to deploy both server and client certificates seamlessly. Through the GUI, you can update certificates using unencrypted .pem-formatted certificate and private key files, integrating the private key with the corresponding signed certificate.

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Certificates**.
- Step 2** Under Certificates, you can view the following properties:

Name	Description
Certificate column	Displays the name or identifier of the certificate.
Issued by column	Shows the authority or entity that issued the certificate.
Issued to column	Indicates the recipient or entity to which the certificate was issued.
Valid from column	Start date of the certificate validity period.
Valid until column	End date of the certificate validity period.

Adding a New Certificate

Procedure

Step 1 From the **Navigation Pane**, select **Security and access > Certificates**.

Step 2 Click **Add new certificate**.

Add new certificate window is displayed.

Step 3 In the **Add new certificate** window update the following properties:

Name	Description
Certificate type drop-down list	Select one of the following: <ul style="list-style-type: none"> • LDAP Certificate—Use for LDAP-related authentication. • CA Certificate—Use for Certificate Authority purposes.
Add file button	Click Add file to browse and select the certificate file from the client.

Step 4 Click **Add**.

Replacing a Certificate

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Certificates**.
- Step 2** To replace a certificate, click the replace icon corresponding to the row you want to replace.
Replace certificate window is displayed.
- Step 3** In the **Replace certificate** window, update the following properties:

Name	Description
Certificate type field	You cannot change the certificate type.
Add file button	Click Add file to browse and select the certificate file from the client.

- Step 4** Click **Replace**.

Deleting a Certificate

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Certificates**.
- Step 2** To delete a delete certificate, click the delete icon corresponding to the row you want to delete.
- Step 3** Click **Delete** to confirm.

Generating a Certificate Signing Request

Procedure

- Step 1** From the **Navigation Pane**, select **Security and access > Certificates**.
- Step 2** Click **Generate CSR**.
Generate a Certificate Signing Request (CSR) window is displayed.
- Step 3** In the **Generate a Certificate Signing Request (CSR)** window update the following properties:

Name	Description
Certificate Type drop-down list	From the drop-down menu, choose one of the following options: <ul style="list-style-type: none"> • HTTPS Certificate—Use for securing web communications. • LDAP Certificate—Use for LDAP-related authentication.
Country/Region drop-down list	Select the country or region from the drop-down menu.
State field	Enter the state name.
City field	Enter the city name.
Company Name field	Enter the name of the company.
Company Unit field	Enter the unit within the company.
Common Name field	Enter the common name for the certificate.
Contact Person (optional) field	Enter the name of the contact person.
Email Address (optional) field	Enter the email address.
Alternate Name (optional) field	Enter alternate names separated by spaces.
Private Key Key Pair Algorithm drop-down list	From the drop-down menu, choose one of the following: <ul style="list-style-type: none"> • EC—Elliptic Curve cryptography for higher security with shorter keys. • RSA—Rivest-Shamir-Adleman algorithm for a widely-used encryption method.

Step 4 Click **Generate CSR** to create the Certificate Signing Request.



CHAPTER 7

Resource Management

- [Viewing CPU Power Configuration, on page 47](#)
- [Applying CPU Power Cap, on page 47](#)

Viewing CPU Power Configuration

Procedure

Step 1 From the **Navigation Pane**, select **Resource Management > Power**.

Step 2 You can view the following properties:

Name	Description
Name column	Identifies the component or device.
Power Consumption column	Displays the current power usage.
Power Cap column	Indicates the maximum power limit set for the component.
Cap Minimum column	Shows the minimum allowable power limit
Cap Maximum column	Displays the maximum allowable power limit.

Applying CPU Power Cap

Procedure

Step 1 From the **Navigation Pane**, select **Resource Management > Power**.

Step 2 Check the **Apply power cap** check box to activate power capping options.

- Step 3** Under **Power cap value (in watts)**, enter the desired power cap value in watts.
Ensure the value is between the minimum and maximum cap limits.
- Step 4** Click **Save** to apply the power cap settings.
-



CHAPTER 8

GPU Management

- [GPU Management, on page 49](#)
- [Configuring GPU Date and Time Settings, on page 50](#)
- [Viewing GPU FRU Information, on page 50](#)
- [Viewing GPU Power and Temperature Sensor, on page 51](#)
- [Viewing GPU Power Configuration, on page 52](#)
- [Event Logs, on page 53](#)
- [Updating GPU Firmware, on page 54](#)

GPU Management

Overview

GPUs are widely used for high-performance computing and graphics processing in various applications. The BMC monitors the health status of GPUs, such as temperature, to prevent overheating or malfunction during heavy computational loads, thereby ensuring the reliability and longevity of the hardware.

Monitored and Controlled Features

The BMC monitors and controls the following GPU features:

- Monitor GPU temperature
- Monitor GPU current power consumption
- Monitor the temperature of components on the GPU board
- Monitor the power consumption of components on the GPU board
- Display the version of components on the GPU board
- Remotely update the GPU firmware and the component firmware on the GPU board

Configuring GPU Date and Time Settings



Note This option is available only for few Cisco UCS C885A M8 Rack Server configurations.

Procedure

- Step 1** From the **Navigation Pane**, select **Settings > Date and time**.
- Step 2** Under **Configure Settings**, choose between the following options:
- Manual
 - Set GPU Datetime to be the same as BMC Datetime

- Step 3** For **Manual**, update the following properties:

Name	Description
Date field	Enter in YYYY-MM-DD format.
24-hour time (UTC) field	Enter time in HH:MM format.

- Step 4** Select **Set GPU Datetime to be the same as BMC Datetime** to automatically import the settings from BMC.
- Step 5** Click **Set**.

Viewing GPU FRU Information

Procedure

- Step 1** From the **Navigation Pane**, select **GPU Management > Information**.
- Step 2** Under **FRU Assembly**, you can view the following properties:

Name	Description
Model	Displays the GPU model.
Name	Displays the GPU name.
Part Number	Lists the part number associated with the GPU.
Physical Context	Describes the physical context or placement of the GPU.

Name	Description
Serial Number	Displays the serial number of the GPU.
Vendor	Identifies the vendor or manufacturer of the GPU.

Step 3 Under **Versions**, you can view the following properties:

Name	Description
Name column	Identifies the component or software related to the GPU.
Version column	Shows the version number associated with the component or software.

Viewing GPU Power and Temperature Sensor

Procedure

Step 1 From the **Navigation Pane**, select **GPU Management > Sensors**.

Step 2 Under **Power**, you can view the following properties:

Name	Description
Name column	Identifies the power sensor.
Current Value column	Displays the current power reading.
Min Value column	Shows the minimum recorded power value.
Max Value column	Displays the maximum recorded power value.

Step 3 Under **Temperature**, you can view the following properties:

Name	Description
Name column	Identifies the temperature sensor.
Current Value column	Displays the current temperature reading.
Min Value column	Shows the minimum recorded temperature value.
Max Value column	Displays the maximum recorded temperature value.
Critical High column	Indicates the critical high threshold for temperature sensors.

Name	Description
Critical Low column	Indicates the critical low threshold for temperature sensors.

Viewing GPU Power Configuration

Procedure

Step 1 From the **Navigation Pane**, select **GPU Management > Powers**.

Step 2 You can view the following properties:

Name	Description
Name column	Identifies the GPU.
Power Consumption column	Displays the current power usage.
Power Cap column	Indicates the maximum power limit set for the GPU.

Applying GPU Power Cap

Procedure

Step 1 From the **Navigation Pane**, select **GPU Management > Powers**.

Step 2 Check the **Apply power cap** check box.

Step 3 In the **Power cap value (in watts)** field, enter a value between 200 and 750.

Step 4 Click **Save**.

Event Logs

Viewing GPU Event Logs

Procedure

Step 1 From the **Navigation Pane**, select **GPU Management > Event logs**.

Step 2 You can filter the event logs based on the following options:

- **From** and **to** dates
- Based on severity: **OK**, **Warning**, and **Critical**
- Search keyword using the search field

You can view the following log properties:

Name	Description
ID column	Displays the unique identifier for each log entry.
Severity column	Indicates the level of importance or impact of the log entry. This can be one of the following: <ul style="list-style-type: none"> • OK—Indicates that the log entry represents a normal or successful operation. • Critical—Indicates a severe issue that requires immediate attention. • Warning—Indicates a potential issue that should be monitored.
Date column	Shows the date and time when the log entry was recorded.
Description column	Provides a brief summary or details about the log entry.

Exporting GPU Event Logs

Procedure

Step 1 From the **Navigation Pane**, select **GPU Management > Event logs**.

Step 2 To export one log entry, click the export icon corresponding to the row you want to export.

- Step 3** (Optional) To export all log entries, click **Export all**.
Depending on your browser settings, you may be prompted to open or save the JSON log file.
-

Updating GPU Firmware

Before you begin

Ensure that the firmware file is available on the client before starting this procedure.

Procedure

- Step 1** From the **Navigation Pane**, select **GPU Management > Firmware**.
- Step 2** Click **Add File** and browse to locate the firmware file.
Select the firmware file.
- Step 3** Click **Start Update** to initiate the firmware update.
-

What to do next

After the firmware update completes, perform an AC power cycle to activate and complete the GPU upgrade.



APPENDIX **A**

REST API

- [HTTP Methods, on page 55](#)
- [Status Code, on page 56](#)
- [Authentication, on page 59](#)
- [Available APIs, on page 60](#)

HTTP Methods

The following HTTP methods are used to implement different actions, as described below.

HTTP Method	Description
POST	<p>The first method is used to create a new resource. The POST request is submitted to the resource collection in which the new resource is to belong. Submitting a POST request to a resource representing a collection is equivalent to submitting the same request to the Members property of that resource.</p> <p>The last method is used to initiate operations on the object (such as Actions). Services shall support the POST method for sending actions. The POST operation may not be idempotent.</p>
GET	<p>The GET method is used to retrieve a representation of a resource. That representation can either be a single resource or a collection.</p>
PUT	<p>The PUT method is used to completely replace a resource. Properties omitted from the request body are reset to their default value.</p>

HTTP Method	Description
PATCH	The PATCH method is the preferred method used to perform updates on pre-existing resources. Changes to the resource are sent in the request body. Properties not specified in the request body are not directly changed by the PATCH request. The response is either empty or a representation of the resource after the update was done. The implementation may reject the update operation on certain fields based on its own policies and, if so, shall not apply any of the update requested.
DELETE	The DELETE method is used to remove a resource. Services shall support the DELETE method for resources that can be deleted.

Status Code

HTTP defines status codes that can be returned in response messages.

Status Code	Status Name	Description
200	OK	The request was successfully completed and includes a representation in its body.
201	Created	A request that created a new resource completed successfully. The Location header shall be set to the canonical URI for the newly created resource. A representation of the newly created resource may be included in the response body.
202	Accepted	The request has been accepted for processing, but the processing has not been completed. The Location header shall be set to the URI of a Task resource that can later be queried to determine the status of the operation. A representation of the Task resource may be included in the response body.
204	No Content	The request succeeded, but no content is being returned in the body of the response.
301	Moved Permanently	The requested resource resides under a different URI.

Status Code	Status Name	Description
302	Found	The requested resource resides temporarily under a different URI.
304	Not Modified	The service has performed a conditional GET request where access is allowed, but the resource content has not changed. Conditional requests are initiated using the headers If-Modified-Since and/or If-None-Match to save network bandwidth if there is no change.
401	Unauthorized	The authentication credentials included with this request are missing or invalid.
403	Forbidden	The server recognized the credentials in the request, but those credentials do not possess authorization to perform this request.
404	Not Found	The request specified a URI of a resource that does not exist.
405	Method Not Allowed	The HTTP verb specified in the request (e.g., DELETE, GET, HEAD, POST, PUT, PATCH) is not supported for this request URI. The response shall include an Allow header which provides a list of methods that are supported by the resource identified by the Request-URI.
406	Not Acceptable	The Accept header was specified in the request and the resource identified by this request is not capable of generating a representation corresponding to one of the media types in the Accept header.

Status Code	Status Name	Description
409	Conflict	A creation or update request could not be completed because it would cause a conflict in the current state of the resources supported by the platform (for example, an attempt to set multiple attributes that work in a linked manner using incompatible values).
410	Gone	The requested resource is no longer available at the server and no forwarding address is known. This condition is expected to be considered permanent. Clients with link editing capabilities SHOULD delete references to the Request-URI after user approval. If the server does not know, or has no facility to determine, whether or not the condition is permanent, the status code 404 (Not Found) SHOULD be used instead. This response is cacheable unless indicated otherwise.
411	Length Required	The request did not specify the length of its content using the Content-Length header (perhaps Transfer-Encoding: chunked was used instead). The addressed resource requires the Content-Length header.
412	Precondition Failed	Precondition (such as OData-Version, If Match or If Not Modified headers) check failed.
415	Unsupported Media Type	The request specifies a Content-Type for the body that is not supported.
500	Internal Server Error	The server encountered an unexpected condition that prevented it from fulfilling the request.

Status Code	Status Name	Description
501	Not Implemented	The server does not (currently) support the functionality required to fulfill the request. This is the appropriate response when the server does not recognize the request method and is not capable of supporting the method for any resource.
503	Service Unavailable	The server is currently unable to handle the request due to temporary overloading or maintenance of the server.

Authentication

The BMC is required to use authentication to access specific Redfish resources. Redfish offers a method of access known as HTTPS Basic Authentication, as defined by RFC7617, enabling users to access Redfish resources. This method uses only connections that conform to TLS to transport the data between any third-party authentication service and clients. Use local BMC authentication or remote authentication like LDAP or Active Directory to log in.

Example of applying for HTTPS basic Authentication using curl:

```
#
#UCS-Server: /logs$ curl -k -X GET https://<username>:<password>@<BMC IP>/redfish/v1 | jq.
%Total %Received %xferd Average Speed   Time    Time       Time   Current
           Dload   Upload   Total   Spent    Left     Speed
100 1532 100 1532 0 0 10281      0---:--:--:--:--:  :--:  :--:  10281{
  "@odata.id": "/redfish/v1",
  "@odata.type": "#ServiceRoot.v1_11_0.ServiceRoot",
  "AccountService": {
    "@odata.id": "/redfish/v1/AccountService"
  },
  "Cables": {
    "@odata.id": "/redfish/v1/Cables"
  },
  "CertificateService": {
    "@odata.id": "/redfish/v1/CertificateService"
  },
  "Chassis": {
    "@odata.id": "/redfish/v1/Chassis"
  },
  "EventService": {
    "@odata.id": "/redfish/v1/EventService"
  },
  "Id": "RootService",
  "JsonSchemas": {
    "@odata.id": "/redfish/v1/JsonSchemas"
  },
  "Links": {
    "Sessions": {
      "@odata.id": "/redfish/v1/SessionService/Sessions"
    }
  }
}
```

```

    }
  },
  "Managers": {
    "@odata.id": "/redfish/v1/Managers"
  },
  "Name": "Root Service",
  "ProtocolFeaturesSupported": {
    "DeepOperations": {
      "DeepPATCH": false,
      "DeepPOST": false
    },
    "ExcerptQuery": false,
    "ExpandQuery": {
      "ExpandAll": false,
      "Levels": false,
      "Links": false,
      "NoLinks": false
    },
    "FilterQuery": false,
    "OnlyMemberQuery": true,
    "SelectQuery": true
  },
  "RedfishVersion": "1.9.0",
  "Registries": {
    "@odata.id": "/redfish/v1/Registries"
  },
  "SessionService": {
    "@odata.id": "/redfish/v1/SessionService"
  },
  "Systems": {
    "@odata.id": "/redfish/v1/Systems"
  },
  "Tasks": {
    "@odata.id": "/redfish/v1/TaskService"
  },
  "TelemetryService": {
    "@odata.id": "/redfish/v1/TelemetryService"
  },
  "UUID": "1b187d13-66a7-4429-8496-b497d28931ba",
  "UpdateService": {
    "@odata.id": "/redfish/v1/UpdateService"
  }
}

```

Available APIs

The following Redfish defined URIs are supported:

Resource	Resource URI
Service Root	/redfish/v1/
Account Service	/redfish/v1/AccountService
Manager Account Collection	/redfish/v1/AccountService/Accounts
Manager Account	/redfish/v1/AccountService/Accounts/{account_instance}
Role Collection	/redfish/v1/AccountService/Roles

Resource	Resource URI
Role	/redfish/v1/AccountService/Roles/{role_instance}
Certificate Management	/redfish/v1/CertificateService
Chassis Collection	/redfish/v1/Chassis
Chassis	/redfish/v1/Chassis/{chassis_instance}
Manager Collection	/redfish/v1/Managers
Manager	/redfish/v1/Managers/{manager_instance}
Managers Network Protocol	/redfish/v1/Managers/{manager_instance}/NetworkProtocol
Log Service Collection (Manager)	/redfish/v1/Managers/{manager_instance}/LogServices
Log Service Collection (Systems)	/redfish/v1/Systems/{System_Instance}/LogServices
Log Service	/redfish/v1/Managers/{manager_instance}/LogServices/{manager_log_instance}
Task Service	/redfish/v1/TaskService
Task Collection	/redfish/v1/TaskService/Tasks
Task	/redfish/v1/TaskService/Tasks/{Task_Instance}
Log Entry Collection	/redfish/v1/Managers/{manager_instance}/LogServices/{manager_log_instance}/Entries
Log Entry Collection (Systems)	/redfish/v1/Systems/{System_Instance}/LogServices/{LogService_Instance}/Entries redfish/v1/Managers/{Manager_Instance}/LogServices/{LogService_Instance}/Entries
Log Entry (Systems)	/redfish/v1/Managers/{Manager_Instance}/LogServices/{LogService_Instance}/Entries/{Entry_Instance} /redfish/v1/Systems/{System_Instance}/LogServices/{LogService_Instance}/Entries/{Entry_Instance}
Log Entry (Manager)	/redfish/v1/Managers/{manager_instance}/LogServices/{manager_log_instance}/Entries/{manager_logentry_instance}
Ethernet Interface Collection	/redfish/v1/Managers/{manager_instance}/EthernetInterfaces

Resource	Resource URI
Ethernet Interface	/redfish/v1/Managers/{{manager_instance}}/EthernetInterfaces/{{manager_ethifc_instance}}
Event Service	/redfish/v1/EventService
Session Service	/redfish/v1/SessionService
Session Collection	/redfish/v1/SessionService/Sessions
Session	/redfish/v1/SessionService/Sessions/{{session_id}}
Update Service	/redfish/v1/UpdateService
FirmwareInventory Collection	/redfish/v1/UpdateService/FirmwareInventory
FirmwareInventory	/redfish/v1/UpdateService/FirmwareInventory/{{firmwareinventory_instance}}
Registries	/redfish/v1/Registries
System	/redfish/v1/Systems