Cisco Baseboard Management Controller 4.0 GUI Configuration Guide, Release 4.0

First Published: 2026-01-16

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

© 2026 Cisco Systems, Inc. All rights reserved.

CONTENTS

PREFACE

Preface vii

Audience vii

Conventions vii

CHAPTER 1

Introduction 1

Overview of the Cisco UCS C880A M8 Rack Server 1

Overview of the Server Software 2

Logging into Cisco BMC 4.0 2

Navigation and Menu 3

Dashboard 8

Server Ports 11

CHAPTER 2

Managing the Server 13

System Information 13

Viewing System Inventory 13

Viewing FRU Information 19

Viewing GPU Information 20

Monitoring and Diagnostics 21

Viewing Critical Sensor Status 21

Viewing Discrete Sensor States 22

Viewing Normal Sensors 23

Viewing Disabled Sensors 24

Configuring Sensor Threshold Values 25

General Settings 26

Configuring Time Zone 26

Power Management 27

Configuring Chassis Identify LED 27
Managing Host Server Power 28
Configuration Management 28
Managing Backup Configuration 28
Preserving a Configuration 29
Restoring Factory Defaults 30

CHAPTER 3 **Managing User Accounts** 33
Local User Management 33
Understanding the User Management Overview 33
Adding a User 33
Modifying User Account Details 35
Deleting a User 36
External Authentication Services 37
Understanding External User Services 37
LDAP/E-Directory Configuration 37
Configuring LDAP/E-Directory General Settings 37
Configuring LDAP/E-Directory Role Groups 39
Active Directory Configuration 39
Configuring Active Directory General Settings 39
Configuring Active Directory Role Groups 40
RADIUS Configuration 41
Configuring RADIUS General Settings 41
Configuring RADIUS Advanced Settings 42
Configuring PAM Authentication Order 43

CHAPTER 4 **Managing Remote Presence** 45
Remote Console Access 45
Launching H5Viewer 45
Using the H5Viewer KVM Console 45
Configuring Remote KVM Session Settings 50
Configuring KVM Mouse Setting 51
Activating Serial Over LAN 52
Virtual Media Management 52

Understanding Image Redirection 52
Configuring Media Support 53
Configuring VMedia Instance Settings 53
Viewing Remote Media Status 54
Viewing Active Media Redirections 55
Video Recording 56
Understanding Video Recording Options 56
Configuring Auto Video Trigger Settings 56
Configuring Video Remote Storage 58
Configuring Pre-Event Video Recording Options 59
Configuring SOL Video Recording Settings 59

CHAPTER 5 **Configuring Network Settings 61**
Understanding Network Settings Overview 61
Configuring Network IP Settings 61
Configuring Network Link Configuration 63
Configuring DNS Settings 64

CHAPTER 6 **Managing Communication Services 67**
Viewing Service Status 67
Configuring Service Settings 68
Configuring SMTP Settings 69

CHAPTER 7 **Managing Server Security and Certificates 71**
SSL Certificate Management 71
Viewing SSL Certificate Information 71
Generating an SSL Certificate 72
Uploading an SSL Certificate 73
Firewall Configuration 74
Configuring General Firewall Settings 74
Configuring IP Firewall Rules 75
Configuring Port Firewall Rules 76
Secure Configuration Management 78
Backing Up or Restoring Key Upload 78

Restoring AES Key 78
Restoring Configuration with AES Key 79

CHAPTER 8 **Managing Faults and Logs** 81
Log Overview and Configuration 81
Understanding Logs and Reports 81
Configuring SEL Log Settings Policy 82
Configuring Advanced Log Settings 82
Platform Event Filter Configuration 83
Understanding Platform Event Filters 83
Configuring Event Filters 84
Configuring Alert Policies 86
Configuring LAN Destinations 87
Viewing System Logs and Diagnostics 88
Viewing IPMI Event Log 88
Viewing System Log 89
Managing Audit Log 89
Viewing Video Log 90
Viewing POST Code 91
Viewing Decoded Event Log 91
Viewing System Diagnostic Logs 92
Viewing Last BSOD Screen Captured 92
Viewing Autonomous Crash Dump Logs 93

CHAPTER 9 **Managing Server Firmware** 95
Understanding Firmware Inventory 95
Viewing Firmware Inventory 95
Updating Server Firmware 96

CHAPTER 10 **Installing the Server OS** 99
OS Installation Methods 99
Remote KVM Console (H5Viewer) 99
Installing an OS Using the KVM Console 100

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 *this font*.
TUI elements	In a Text-based User Interface, text the system displays appears in `this font`.
System output	Terminal sessions and information that the system displays appear in `this font`.
CLI commands	CLI command keywords appear in **this font**. Variables in a CLI command appear in *this font*.
[ ]	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.

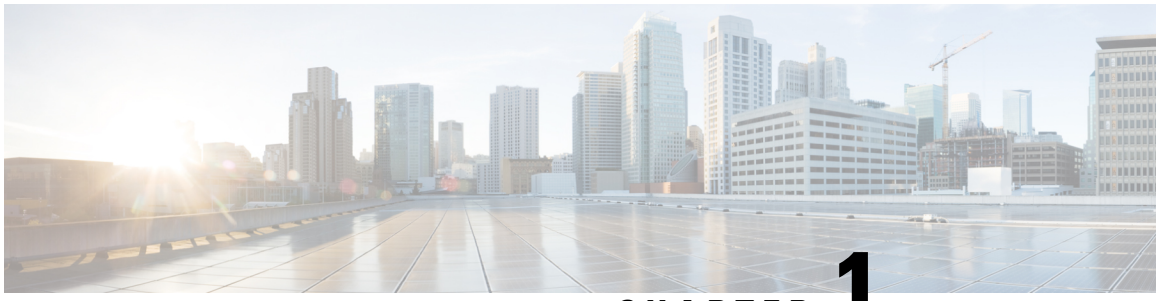
Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

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 C880A M8 Rack Server, on page 1
- Overview of the Server Software , on page 2
- Logging into Cisco BMC 4.0, on page 2
- Navigation and Menu, on page 3
- Dashboard, on page 8
- Server Ports, on page 11

Overview of the Cisco UCS C880A M8 Rack Server

The Cisco UCS C880A M8 Rack Server accelerates advanced AI and High-Performance Computing (HPC) workloads in every data center with next-generation NVIDIA HGX B300 NVL8 GPUs.

Based on the NVIDIA HGX platform, the Cisco UCS C880A M8 Rack Server is a high-density, air-cooled rack server designed to power the most demanding Artificial Intelligence (AI) and High-Performance Computing (HPC) workloads. It integrates the NVIDIA HGX platform with eight NVIDIA HGX B300 (SXM) GPUs and is powered by two Intel® Xeon® 6th Gen Processors, making it ideal for real-time Large Language Model (LLM) inference, next-level training performance, and large-volume data processing. The C880A M8 supports customers across the entire AI stack, from large-scale model training and fine-tuning to real-time inferencing and large-volume data processing. It integrates seamlessly into Cisco's AI strategy, connecting and protecting the AI era by providing robust compute infrastructure. This server expands the Cisco UCS® dense AI server portfolio, offering a powerful solution for enterprises across various industries, including service providers, financial services, manufacturing, healthcare, life sciences, and automotive. With its advanced architecture, the C880A M8 ensures unparalleled performance, scalability, and enterprise manageability, making it ideal for compute-intensive AI use cases such as large-scale AI model training, fine tuning, and inferencing.

The Cisco UCS C880A M8 Rack Server stands out by integrating the cutting-edge NVIDIA HGX platform with eight NVIDIA B300 (SXM) GPUs. This powerful GPU configuration is at the heart of its capability to deliver next-level performance for the most demanding AI workloads, including large-scale AI model training, fine tuning, and real-time inferencing. The B300 GPUs provide immense parallel processing capabilities and high-speed GPU interconnects, which are critical for accelerating complex deep learning models and large language models. This integration ensures that enterprises can achieve higher token throughput and improve the economics of their AI operations, enabling profitable scaling of LLM and agentic workloads.

Beyond raw power, the Cisco UCS C880A M8 Rack Server is architected specifically to meet the unique demands of AI and HPC. Its design supports real-time large language model Inference, enabling rapid deployment and responsiveness for AI-driven applications. It also excels in next-level training performance, significantly reducing the time required to train complex AI models. Furthermore, its capacity for large-volume

data processing makes it an ideal platform for data-science and big-data analytics, including GPU-accelerated ETL processes. This specialized design ensures that organizations can build, optimize, and utilize AI models efficiently, accelerating business growth with scalable and high-performance solutions.

The Cisco UCS C880A M8 Rack Server is a dedicated rack server platform designed to host and accelerate AI and HPC workloads. It supports various operating systems and virtualization platforms typically used in data center environments for AI/HPC deployments. Specific software stack compatibility includes NVIDIA AI Enterprise and NVIDIA NIM (NVIDIA Inference Microservices) for AI application deployment and optimization. For more information, see Cisco UCS C880A M8 Rack Server Data Sheet.

The Cisco UCS C-Series rack server supports operating systems such as Ubuntu, Red Hat Linux, and so on. For more information on supported operating systems, see the UCS Hardware and Software Compatibility. You can use Cisco Baseboard Management Controller 4.0 (Cisco BMC 4.0) to install an OS on the server using the KVM console and vMedia.

Overview of the Server Software

The Cisco Baseboard Management Controller 4.0 (Cisco BMC 4.0) is the management service for the Cisco UCS C880A M8 Rack Server servers. Cisco BMC 4.0 runs within the server.

You can use a web-based GUI, an SSH-based CLI, or a REST API to access, configure, administer, and monitor the server. Each interface offers different capabilities, and the tasks supported by each interface are described in their respective configuration guides.

Logging into Cisco BMC 4.0

Procedure

Step 1 In your web browser, type or select the web link for Cisco BMC 4.0.

Step 2 If a security dialog box displays, do the following:

a) (Optional) (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.

When logging in for the first time to an unconfigured system, use admin 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 admin credentials on the Cisco BMC 4.0 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 4.0, you are directed to the **Dashboard** page. Following options are available:

Menu Bar

The top menu bar has the following options:

Table 1: Menu Bar

Name	Description
Hamburger Menu	Allows you to toggle the visibility of a navigation pane, located on the left side of the interface.
Message icon	Displays system messages, alerts, or communications related to the status or operations.
Notification icon	Shows real-time notifications about events, tasks, or changes within the server management system.
Language drop-down	Allows the user to select and change the display language of the user interface.
Sync	Initiates a synchronization process to update data or configurations between the UI and the server.
Refresh	Reloads the current view or data displayed in the UI to show the most up-to-date information from the server.
admin drop-down	Provides access to administrative functions such as user profile settings, logout options, and other system-wide management tools.

Navigation

The Cisco BMC 4.0 GUI left navigation pane comprises of the following:

Firmware Information

This section provides essential details about the firmware and operational status.

- **Firmware Version** - Displays the current version number of the installed firmware, indicating the software build running on the server hardware.
- **Build Date** - Shows the date and time when the current firmware version was compiled or released.
- **UpTime** - Indicates the total duration (days, hours, minutes) that the server has been continuously operational since the last boot or restart.

- **MAC Address** - Presents the unique Media Access Control address of the primary network interface of the server, used for network identification.
- **Host Status** - Confirms that the server is currently powered on and actively connected to the network, indicating the operational state.
- **Chassis Identify LED** - This control allows you to activate or deactivate a physical LED light on the server chassis, helping to visually locate the specific server in a rack or data center.

Dashboard Control Panel

This section provides an overview of key operational metrics and status indicators for the server.

- **BMC Up Time** - Indicates the total duration (days, hours, minutes) that the Baseboard Management Controller (BMC) has been continuously operational since the last boot or restart.
- **Pending Deassertions** - Displays the number of events or alerts that have been triggered but are awaiting acknowledgment or resolution. Click **More info** to view further details on these deassertions.
- **Access Logs** - Shows the number of recent entries in the access logs of the server, which record user logins, system changes, and other security-related events. Click **More info** to access the detailed log entries.
- **Available GPU** - Indicates the number of Graphics Processing Units (GPUs) that are currently available for use or allocation within the server. Click **More info** to view details on the status and configuration of the GPUs.

Sensor Reading Live reading of all sensors

This section provides a real-time overview of all sensor data within the server, categorizing them by their current status.

- **Critical Sensors** - Displays the number of sensors currently reporting critical conditions. This area highlights specific critical readings, such as power consumption for power supply units (PSUs) and fan speeds. Icons for **PSU** and **Fan** are available, which, when clicked, provide detailed information about the respective components.
- **Discrete Sensor States** - Shows the total count of sensors that report discrete states.
- **Normal Sensors** - Indicates the total count of sensors operating within their expected normal parameters.
- **Disabled Sensors** - Displays the total count of sensors that are currently disabled and not reporting data.

System Inventory

This section provides a detailed inventory of hardware components, organized into various categories for easy access and management. Each tab offers specific information about the respective system part.

- **System** - Displays general information about the server system, including model, serial number, and overall system status.
- **Processor** - Provides details about installed processors, such as manufacturer, model, core count, and current operating status.
- **Memory Controller** - Shows information related to memory controllers, including status and configuration.

- **BaseBoard** - Presents details about the motherboard, including manufacturer, model, and revision information.
- **Power** - Offers information about power supply units (PSUs), power consumption, and power-related settings.
- **Thermal** - Displays data related to thermal management, including fan status, temperature readings, and cooling configurations.
- **PCIE Function** - Provides details about Peripheral Component Interconnect Express (PCIe) devices and functions installed in the server.
- **Storage** - Shows information about installed storage devices, such as hard drives, SSDs, and RAID configurations.
- **Network** - Presents details about network interfaces, including MAC addresses, link status, and network configurations.

FRU Field Replacable Units

This section provides detailed information about the Field Replaceable Units (FRUs) installed in the server.

- **Available FRU Devices** - A dropdown list that allows selection of different Field Replaceable Unit (FRU) devices. It displays the **FRU Device ID** and **FRU Device Name** for each available unit.
- **Board Information** - This subsection presents comprehensive details about the main board, including manufacturing, identification, and part numbers.
- **Product Information** - This subsection provides detailed identification and manufacturing information for the overall product, including name, serial number, and asset tag.

GPU Information Details for all Graphics Processing Units

This section provides comprehensive information about the Graphics Processing Units (GPUs) installed in the server, detailing both summary and individual GPU specifications.

- **Available Graphic Boards** - This subsection displays summary information for the graphic boards, including the **Part Number**, **Serial Number**, **Total GPU** count, and **Available GPU** count.
- **GPU [Index]** - Each of these subsections provides detailed specifications for an individual GPU, including its **GPU Marketing Name**, **GPU PCI VID** (Vendor ID), **GPU PCI DID** (Device ID), **GPU GUID**, **VBIOS Version**, **Inforom Version**, and whether the **GPU Require Reset**.

Firmware Inventory

This section provides a comprehensive list of firmware versions for various components within the server.

- **DGX** - This option filters the firmware inventory to display components specific to DGX systems or related modules.
- **HGX** - This option filters the firmware inventory to display components specific to HGX systems or related modules.

Logs and Reports

This drop-down menu provides access to various logs and reports, offering insights into server events, system activities, and diagnostic information. Each option leads to a dedicated page for viewing the respective log or report.

- **IPMI Event Log** - Accesses the Intelligent Platform Management Interface (IPMI) event log, which records hardware-related events and alerts.
- **System Log** - Accesses the system log, which contains records of operating system events, application activities, and other system-level messages.
- **Audit Log** - Accesses the audit log, which tracks user actions and system changes for security and compliance purposes.
- **Video Log** - Accesses the video log, which may contain recordings or snapshots of server console output.
- **POST Code** - Accesses information related to Power-On Self-Test (POST) codes, which indicate the status of the server during startup.
- **Decoded Event Log** - Accesses a decoded version of server events, providing more user-friendly interpretations of raw log data.

Settings Configure BMC options

This section provides access to various configuration options for the Baseboard Management Controller (BMC), presented as icons with descriptive text.

- **Captured BSOD** - Click to view or configure settings for captured Blue Screen of Death (BSOD) information.
- **Date and Time** - Click to configure the date, time, and time zone settings for the BMC.
- **External User Services** - Click to configure external authentication and user management services.
- **KVM Mouse Setting** - Click to access settings for Keyboard, Video, and Mouse (KVM) functionality, specifically for mouse behavior.
- **Log Settings** - Click to configure logging behavior, including log levels and retention policies.
- **Media Redirection Settings** - Click to configure settings related to redirecting local media to the server.
- **Network Settings** - Click to configure options for the BMC's network interfaces, including IP addresses and DNS settings.
- **PAM Order Settings** - Click to configure the Pluggable Authentication Modules (PAM) order for authentication services.
- **Platform Event Filter** - Click to configure filters for platform events, determining which events are logged or trigger alerts.
- **Services** - Click to manage various BMC services, allowing activation or deactivation.
- **SMTP Settings** - Click to configure Simple Mail Transfer Protocol (SMTP) settings for email notifications.
- **SSL Settings** - Click to configure Secure Sockets Layer (SSL) settings for secure communication.
- **System Firewall** - Click to configure the BMC's internal firewall rules.

- **User Management** - Click to manage user accounts, roles, and permissions for BMC access.
- **Video Recording** - Click to configure settings for video recording of server console sessions.

Remote Control Remote KVM and SOL

This section provides options for remotely controlling the server using KVM (Keyboard, Video, Mouse) and Serial Over LAN (SOL) functionality.

- **H5Viewer** - This feature enables remote graphical access to the server console. Click **Remote Session Settings** to configure options for the remote session. Click **Launch H5Viewer** to open the remote KVM console.
- **Serial Over LAN** - This feature provides remote access to the server's serial console. Click **Activate** to enable Serial Over LAN functionality.

Image Redirection

This section allows for the redirection of local image files to the remote server, facilitating tasks such as operating system installation or firmware updates.

- **Remote Images** - Click this icon to manage or mount remote image files for use by the server.

Host System Diagnostics

This section provides tools and features for diagnosing issues and analyzing system behavior on the host server.

- **Autonomous Crash Dump** - Click to configure or manage the autonomous crash dump feature, which enables the system to automatically capture and save diagnostic information, such as memory dumps, when a system crash occurs, aiding in post-mortem analysis.

Power Control on Host Server

This section allows control over the power state of the host server. You can select from various power actions using radio buttons:

- **Force Off** - Immediately powers off the server without a graceful shutdown process.
- **Force Restart** - Immediately restarts the server without a graceful shutdown process.
- **Graceful Restart** - Initiates a controlled restart of the server, allowing the operating system to shut down properly.
- **Graceful Shutdown** - Initiates a controlled shutdown of the server, allowing the operating system to shut down properly.
- **On** - Powers on the server.
- **Power Cycle** - Performs a complete power off and then power on sequence for the server.

After selecting a power action, click **Perform Action** to execute the chosen command.

Chassis Identify LED Control on Host Server

This section provides control over the physical Identify LED on the server chassis, which helps in locating the server within a rack or data center.

Users can select from various LED actions using radio buttons under **LED Actions**:

- **LED Off** - Turns off the chassis Identify LED.
- **LED Solid ON** - Sets the chassis Identify LED to remain continuously lit.
- **LED Blinking ON** - Sets the chassis Identify LED to blink, typically for a specified duration.

The **Identify interval in seconds** field allows specification of the duration for blinking LED actions.

After selecting an LED action, click **Perform Action** to execute the chosen command.

Maintenance

This section provides a suite of tools and functionalities for maintaining the server, including backup, restore, and update operations. Each function is accessible via an icon with descriptive text.

- **Backup/Restore Key upload** - Click to manage the upload of encryption keys for backup and restore operations.
- **Firmware Update** - Click to initiate or manage the process of updating server firmware.
- **Backup Configuration** - Click to create a backup of the current server configuration settings.
- **Preserve Configuration** - Click to manage options for preserving configuration settings during system events like firmware updates.
- **Restore Factory Defaults** - Click to reset the server's configuration to its original factory settings.
- **System Diagnostics** - Click to access tools for running diagnostic tests on the server hardware and software.
- **Restore Configuration** - Click to restore the server's configuration from a previously saved backup file.

Sign out

Click to end the current user session and log out of the system.

Dashboard

After logging into the Cisco BMC 4.0 GUI, you are directed to the **Dashboard** page. From this page, you can quickly access important features and information. Below are the key properties and sections of the Overview page:

BMC Up Time

Indicates the total duration (days, hours, minutes) that the Baseboard Management Controller (BMC) has been continuously operational since the last boot or restart.

Pending Deassertions

Displays the number of events or alerts that have been triggered but are awaiting acknowledgment or resolution. Click **More info** to view further details.

Table 2: Event Log

Name	Description
Sensor drop-down list	Allows filtering of the event log based on specific sensors, enabling viewing of events related to particular components or types of sensors.
ID column	A unique identifier for each event log entry.
Record Type column	Indicates the type of record, categorizing the nature of the event.
Timestamp column	The date and time when the event occurred.
Generator ID column	Identifies the entity or component that generated the event.
Manufacture ID column	Identifies the manufacturer associated with the event or component.
Sensor Name column	The name of the sensor that reported the event.
Sensor Type column	The category or type of the sensor (e.g., temperature, voltage).
Sensor Num column	A numerical identifier for the specific sensor.
Event Dir column	Indicates the direction of the event, such as asserted or deasserted.
Data column	Raw data associated with the event, often in hexadecimal format.
Description column	A human-readable explanation or summary of the event.

Access Logs

Shows the number of recent entries in the access logs of the server, which record user logins, system changes, and other security-related events. Click **More info** to access the detailed log entries.

Table 3: Audit Log

Name	Description
Clear Audit Logs button	Click to clear all entries from the audit log, removing historical records of system activities and user actions.

Name	Description
Download Audit Logs button	Click to download a copy of the audit log entries, typically in a file format for external analysis or archiving.
ID column	A unique identifier for each entry in the audit log.
Timestamp column	The date and time when the audited event occurred.
Host column	Identifies the host or system where the audited event took place.
Description column	A detailed description of the audited event, including user actions or system changes.

Available GPU

Indicates the number of Graphics Processing Units (GPUs) that are currently available for use or allocation within the server. Click **More info** to view details on the status and configuration of the GPUs.

Table 4: Available Graphic Boards

Name	Description
Part Number	Identifies the part number of the manufacturer for the graphic board.
Serial Number	A unique serial number assigned to the graphic board for identification.
Total GPU	Indicates the total number of Graphics Processing Units present on the board.
Available GPU	Shows the number of Graphics Processing Units currently available for use or allocation.

Table 5: GPU Information

Name	Description
GPU Marketing Name	The commercial name of the Graphics Processing Unit.
GPU PCI VID	The PCI Vendor ID of the Graphics Processing Unit.
GPU PCI DID	The PCI Device ID of the Graphics Processing Unit.
GPU GUID	A globally unique identifier for the Graphics Processing Unit.
VBIOS Version	The version of the Video BIOS installed on the Graphics Processing Unit.

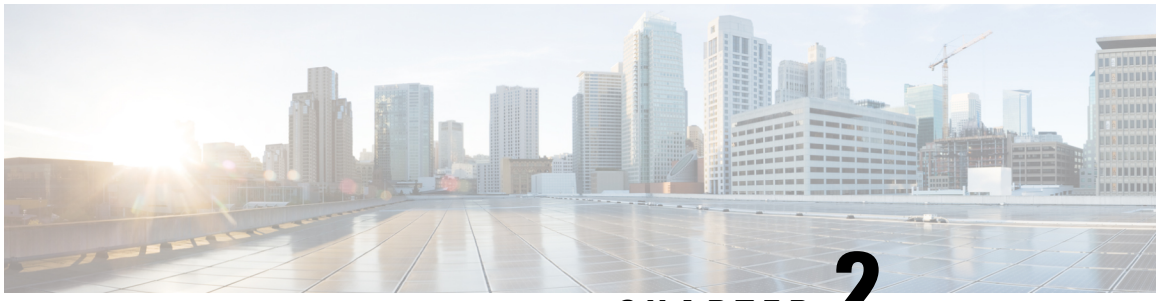
Name	Description
Inforom Version	The version of the Inforom firmware on the Graphics Processing Unit.
GPU Require Reset	Indicates whether the Graphics Processing Unit requires a reset for certain operations or changes.

Server Ports

Following is a list of server ports and their default port numbers:

Table 6: Server Ports

Port Name	Port Number
HTTPS	443
IPMI	623
KVM/vMedia	443
NTP	123
SSH	22



CHAPTER 2

Managing the Server

- System Information, on page 13
- Monitoring and Diagnostics, on page 21
- General Settings, on page 26
- Power Management, on page 27
- Configuration Management, on page 28

System Information

Viewing System Inventory

Procedure

Step 1 From the **Navigation Pane**, click **System Inventory**.

Step 2 You can view the following inventories:

Table 7: System Tab

Name	Description
Name column	The designated name of the server.
Description column	A brief explanation or summary of the server.
Model column	The model identifier of the server hardware.
IndicatorLED column	The current status of the indicator LED on the server.
Manufacturer column	The name of the company that manufactured the server.
PowerState column	The current power status of the server.
SerialNumber column	A unique alphanumeric identifier for the server unit.
PartNumber column	The manufacturer part number for the server.

Name	Description
SystemType column	The type or category of the server.
AssetTag column	A user-defined tag for the server.
BiosVersion column	The version of the BIOS firmware installed on the server.
UUID column	The Universal Unique Identifier for the server.
State column	The current operational state or health status of the server.

Table 8: Processor Tab

Name	Description
Id column	A unique identifier for the processor.
Manufacturer column	The name of the company that manufactured the processor.
MaxSpeedMHz column	The maximum clock speed of the processor, measured in megahertz (MHz).
ProcessorArchitecture column	The architecture of the processor.
ProcessorType column	The type or model of the processor.
Socket column	The physical socket on the motherboard where the processor is installed.
EffectiveFamily column	The effective family code of the processor, used for identification.
TotalCores column	The total number of processing cores within the processor.
State column	The current operational state or health status of the processor.

Table 9: Memory Controller Tab

Name	Description
Socket column	The physical socket on the motherboard associated with the memory controller.
MemCtrl column	The identifier for the specific memory controller.
Channel column	The memory channel to which the memory module is connected.
Slot column	The physical slot number where the memory module is installed.
Id column	A unique identifier for the memory module.

Name	Description
Capacity MiB column	The total capacity of the memory module, measured in mebibytes (MiB).
Manufacturer column	The name of the company that manufactured the memory module.
Serial Number column	A unique serial number for the memory module.
Part Number column	The manufacturer's part number for the memory module.
State column	The current operational state or health status of the memory module.
OperatingSpeed Mhz column	The current operating speed of the memory module, measured in megahertz (MHz).
Memory Type column	The type of memory technology used (e.g., DDR4, DDR5).
AllowedSpeed MHz column	The maximum supported speed of the memory module, measured in megahertz (MHz).

Table 10: Baseboard Tab

Name	Description
Name column	The designated name of the baseboard.
Description column	A brief explanation or summary of the baseboard.
FirmwareVersion column	The version of the firmware installed on the baseboard.
Model column	The model identifier of the baseboard.
State column	The current operational state or health status of the baseboard.
PowerState column	The current power status of the baseboard.

Table 11: Power Tab

Name	Description
Power Control Info	
Name column	The designated name for the power consumption metric.
AvgConsumedWatts column	The average power consumed, measured in watts.
MaxConsumedWatts column	The maximum power consumed, measured in watts.
MinConsumedWatts column	The minimum power consumed, measured in watts.

Name	Description
IntervalInMinutes column	The time interval, in minutes, over which power consumption is measured.
Voltage Info	
Name column	The designated name of the power-related component or sensor.
LUN column	The Logical Unit Number associated with the power component.
SensorId column	A unique identifier for the power sensor.
State column	The current operational state or health status of the power component.
MinReadingRange column	The minimum value of the normal operating range for the sensor reading.
MaxReadingRange column	The maximum value of the normal operating range for the sensor reading.
UNR column	Upper Non-Recoverable threshold for the sensor reading.
UCR column	Upper Critical threshold for the sensor reading.
UNC column	Upper Non-Critical threshold for the sensor reading.
LNC column	Lower Non-Critical threshold for the sensor reading.
LCR column	Lower Critical threshold for the sensor reading.
LNR column	Lower Non-Recoverable threshold for the sensor reading.

Table 12: Thermal Tab

Name	Description
Fan Info	
Name column	The designated name of the fan.
MemberId column	A unique identifier for the fan within its group.
PhysicalContext column	Describes the physical location or context of the fan.
State column	The current operational state or health status of the fan.
Reading(RPM) column	The current rotational speed of the fan, measured in revolutions per minute (RPM).
MinReadingRange column	The minimum value of the normal operating range for the fan speed.

Name	Description
MaxReadingRange column	The maximum value of the normal operating range for the fan speed.
UF column	Upper Fatal threshold for the fan speed.
UC column	Upper Critical threshold for the fan speed.
UNC column	Upper Non-Critical threshold for the fan speed.
LNC column	Lower Non-Critical threshold for the fan speed.
LC column	Lower Critical threshold for the fan speed.
LF column	Lower Fatal threshold for the fan speed.
Temperature Info	
Name column	The designated name of the temperature sensor.
MemberId column	A unique identifier for the temperature sensor within its group.
PhysicalContext column	Describes the physical location or context of the temperature sensor.
State column	The current operational state or health status of the temperature sensor.
Reading(Celsius) column	The current temperature reading, measured in Celsius.
UF column	Upper Fatal threshold for the temperature reading.
UC column	Upper Critical threshold for the temperature reading.
UNC column	Upper Non-Critical threshold for the temperature reading.
LNC column	Lower Non-Critical threshold for the temperature reading.
LC column	Lower Critical threshold for the temperature reading.
LF column	Lower Fatal threshold for the temperature reading.

The PCIE Function tab displays a hierarchical tree view of Peripheral Component Interconnect Express (PCIe) devices and their functions installed in the server. Each entry in the tree represents a PCIe device or bridge, identified by its bus: device, function address and a descriptive type.

Click on a device entry in the tree to reveal a drop-down menu containing detailed information about that specific PCIe function:

Table 13: PCIe Function Details

Name	Description
Id	A unique identifier for the PCIe function.

Name	Description
Vendor Id	The hexadecimal identifier for the manufacturer of the PCIe device.
Device Id	The hexadecimal identifier for the specific device model from the vendor.
Class Code	A hexadecimal code indicating the generic function of the device.
Revision Id	The revision number of the device.
Sub System Vendor Id	The hexadecimal identifier for the sub-system vendor.
Sub System Id	The hexadecimal identifier for the sub-system device.
State	The current operational state of the PCIe function.

Table 14: Storage Tab

Name	Description
Name column	The designated name of the storage device.
SerialNumber column	A unique alphanumeric identifier for the storage device.
Manufacturer column	The name of the company that manufactured the storage device.
Location column	The physical location or slot of the storage device within the server.
Protocol column	The communication protocol used by the storage device.
Model column	The model identifier of the storage device.
Revision column	The firmware or hardware revision of the storage device.
EncryptionStatus column	Indicates whether data encryption is enabled or disabled on the storage device.
MediaType column	The type of storage medium (e.g., HDD, SSD, NVMe).
State column	The current operational state or health status of the storage device.

Table 15: Network Tab

Name	Description
Name column	The designated name of the Network Interface Controller.
Model column	The model identifier of the Network Interface Controller.

Name	Description
MAC Address column	The unique Media Access Control address of the Network Interface Controller.
BDF column	The Bus, Device, Function address of the Network Interface Controller.

Viewing FRU Information

This task describes how to view detailed information about Field Replaceable Units (FRUs) installed in the server. FRU information includes identification details for various hardware components, which is useful for inventory management, troubleshooting, and ordering replacement parts.

Procedure

Step 1 From the **Navigation Pane**, click **FRU Information**.

Step 2 In the **Available FRU Devices** section, select a FRU device from the **FRU Device ID** drop-down list.

The **FRU Device Name** field automatically updates to display the name of the selected device.

Detailed information about the selected FRU device is displayed in two sections: **Board Information** and **Product Information**.

Step 3 Review the **Board Information** table for details about the board:

Table 16: Board Information

Name	Description
Board Information Area Format Version	The format version of the board information area.
Language	The language code used for the board information.
Manufacture Date Time	The date and time when the board was manufactured.
Board Manufacturer	The name of the company that manufactured the board.
Board Product Name	The product name of the board.
Board Serial Number	A unique serial number for the board.
Board Part Number	The part number for the board.
FRU File ID	The identifier for the FRU file associated with the board.
Board Extra	Additional information or notes about the board.

Step 4 Review the **Product Information** table for details about the overall server product:

Table 17: Product Information

Name	Description
Product Information Area Format Version	The format version of the product information area.
Language	The language code used for the product information.
Product Manufacturer	The name of the company that manufactured the product.
Product Name	The product name of the server.
Product Part Number	The part number for the product.
Product Version	The version of the product.
Product Serial Number	A unique serial number for the product.
Asset Tag	A customizable tag for asset tracking.
FRU File ID	The identifier for the FRU file associated with the product.
Product Extra	Additional information or notes about the product.

What to do next

Use the displayed FRU information for hardware identification, inventory management, or troubleshooting purposes.

Viewing GPU Information

This task describes how to view detailed information about Graphics Processing Units (GPUs) installed in the server. This information includes summary details for available graphic boards and individual specifications for each GPU.

Procedure

Step 1 From the **Navigation Pane**, click **FRU Information**.

Step 2 Review the **Available Graphic Boards** table for summary information:

Table 18: Available Graphic Boards Summary

Name	Description
Part Number column	Identifies the part number for the graphic board.
Serial Number column	A unique serial number assigned to the graphic board for identification.

Name	Description
Total GPU column	Indicates the total number of Graphics Processing Units present on the board.
Available GPU column	Shows the number of Graphics Processing Units currently available for use or allocation.

Step 3 Review the individual GPU information sections for detailed specifications:

The page displays multiple sections, each representing a specific GPU. Each section provides the following details:

Table 19: Individual GPU Details

Name	Description
GPU Marketing Name	The commercial name of the Graphics Processing Unit.
GPU PCI VID	The PCI Vendor ID of the Graphics Processing Unit.
GPU PCI DID	The PCI Device ID of the Graphics Processing Unit.
GPU GUID	A globally unique identifier for the Graphics Processing Unit.
VBIOS Version	The version of the Video BIOS installed on the Graphics Processing Unit.
Inforom Version	The version of the Inforom firmware on the Graphics Processing Unit.
GPU Require Reset	Indicates whether the Graphics Processing Unit requires a reset for certain operations or changes.

What to do next

Use the displayed GPU information for hardware identification, inventory management, or performance monitoring.

Monitoring and Diagnostics

Viewing Critical Sensor Status

This task describes how to view the detailed status of individual critical sensors, including their live readings, graphs, and threshold information, particularly for critical sensors.

Procedure

Step 1 From the **Navigation Pane**, click **Sensor**.

Step 2 Under the **Critical Sensors** section, click on a specific sensor icon.

A new page opens, displaying detailed information for the selected sensor.

Step 3 You can review the sensor details on the opened page.

The left section displays a graphical representation of live sensor readings over time. The Y-axis represents the sensor value and the X-axis represents time.

The right section presents a table with detailed threshold information for the sensor:

Table 20: Sensor Thresholds

Name	Description
Upper Non-recoverable	The threshold above which the sensor reading indicates a non-recoverable critical condition.
Upper Critical	The threshold above which the sensor reading indicates a critical condition.
Upper Non-critical	The threshold above which the sensor reading indicates a non-critical warning condition.
Lower Non-critical	The threshold below which the sensor reading indicates a non-critical warning condition.
Lower Critical	The threshold below which the sensor reading indicates a critical condition.
Lower Non-recoverable	The threshold below which the sensor reading indicates a non-recoverable critical condition.
Change Threshold Values button	Click to modify the predefined thresholds for the sensor, allowing adjustment of critical, non-critical, and non-recoverable limits. See .

What to do next

Monitor sensor readings and thresholds for potential issues or performance anomalies.

Viewing Discrete Sensor States

This task describes how to view the status of discrete sensors, which report specific states rather than continuous readings. Monitoring these states helps in understanding the operational status of various server components.

Procedure

Step 1 From the **Navigation Pane**, click **Sensor**.

Step 2 Under the **Discrete Sensor States** section, you can view the following details.

Table 21: Discrete Sensor States

Name	Description
Sensor Name column	The name of the discrete sensor.
State column	The current state reported by the sensor.

Step 3 Click a specific sensor name in the table.

A new page is displayed, showing detailed information for the selected discrete sensor.

The page includes two sections:

- **[Sensor Name] Sensor Information**—Displays general information about the sensor, including its **Sensor State Reading**.
- **[Sensor Name] Sensor Events**—Displays a list of events associated with the sensor.

What to do next

Use discrete sensor state information to diagnose specific component conditions or track changes in system status.

Viewing Normal Sensors

This task describes how to view the status of normal sensors, which report continuous readings and operate within their expected parameters. Monitoring these readings helps in assessing the ongoing health and performance of various server components.

Procedure

Step 1 From the **Navigation Pane**, click **Sensor**.

Step 2 Under the **Normal Sensors** section, you can view the following details.

Table 22: Normal Sensor States

Name	Reading	Behavior
Sensor Name column	**Reading** column	**Behavior** column

Name	Reading	Behavior
The name of the normal sensor.	The current measurement reported by the sensor.	The operational behavior or status of the sensor.

Step 3 Click a specific sensor name in the table.

A new page is displayed, showing detailed information for the selected normal sensor.

The left section displays a graphical representation of live sensor readings over time. The Y-axis represents the sensor value, and the X-axis represents time.

The right section presents a table with detailed threshold information for the sensor:

Table 23: Sensor Thresholds

Name	Description
Upper Non-recoverable	The threshold above which the sensor reading indicates a non-recoverable critical condition.
Upper Critical	The threshold above which the sensor reading indicates a critical condition.
Upper Non-critical	The threshold above which the sensor reading indicates a non-critical warning condition.
Lower Non-critical	The threshold below which the sensor reading indicates a non-critical warning condition.
Lower Critical	The threshold below which the sensor reading indicates a critical condition.
Lower Non-recoverable	The threshold below which the sensor reading indicates a non-recoverable critical condition.
Change Threshold Values button	Click to modify the predefined thresholds for the sensor, allowing adjustment of critical, non-critical, and non-recoverable limits. See .

A is available to modify these settings.

What to do next

Monitor normal sensor readings and thresholds to assess system performance and detect potential issues.

Viewing Disabled Sensors

This task describes how to view a list of sensors that are currently disabled and not reporting data. Monitoring disabled sensors helps in identifying components that are intentionally or unintentionally inactive.

Procedure

Step 1 From the **Navigation Pane**, click **Sensor**.

Step 2 Under the **Disabled Sensors** section, a list is displayed showing the names of all currently disabled sensors.

What to do next

Determine if any listed disabled sensors require re-enabling or further investigation.

Configuring Sensor Threshold Values

This task describes how to modify predefined thresholds for both critical and normal sensors. Adjusting these values allows for customization of critical, non-critical, and non-recoverable limits based on specific operational requirements.

Before you begin

Ensure the server is in a state where sensor threshold modifications are permitted.

Procedure

Step 1 From the **Navigation Pane**, click **Sensor**.

Step 2 Click on the icon or name for the specific sensor whose threshold values require modification. The sensor can be located in either the **Critical Sensors** section or the **Normal Sensors** section.

A new page is displayed, showing detailed information for the selected sensor.

Step 3 Click **Change Threshold Values**.

The **Sensor Thresholds** page is displayed.

Table 24: Change Threshold Values

Name	Description
Sensor Name	Name of the sensor.
Upper Non-recoverable field	The threshold above which a sensor reading indicates a non-recoverable critical condition.
Upper Critical field	The threshold above which a sensor reading indicates a critical condition.
Upper Non-critical field	The threshold above which a sensor reading indicates a non-critical warning condition.

Name	Description
Lower Non-critical field	The threshold below which a sensor reading indicates a non-critical warning condition.
Lower Critical field	The threshold below which a sensor reading indicates a critical condition.
Lower Non-recoverable field	The threshold below which a sensor reading indicates a non-recoverable critical condition.
Retain Threshold Values check-box	Select this checkbox to retain configured threshold values even after a system reset or firmware update.

Step 4 Enter desired values for each threshold.

Step 5 Click **Save** to apply the changes.

What to do next

Verify new threshold values are correctly displayed on the sensor details page.

General Settings

Configuring Time Zone

This task describes how to configure date, time, and time zone settings for the server, either manually or through automatic synchronization using NTP or PTP.

Before you begin

Ensure network connectivity if configuring NTP or PTP for automatic date and time synchronization.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Date and Time**.

The **Date and Time** page is displayed.

Step 3 Configure the time zone using one of the following methods:

a) Use the interactive world map to select a time zone.

Click on a region on the map to automatically select the corresponding time zone.

b) Select a time zone from the **Select Time Zone** drop-down list.

Step 4 Configure date and time synchronization:

a) To use NTP for automatic synchronization, select the **Automatic NTP Date Time** check-box.

   Enter the address for the primary NTP server in the **Primary NTP Server** field.

   Optionally, enter the address for a secondary NTP server in the **Secondary NTP Server** field.

b) To use PTP for automatic synchronization, select the **Automatic PTP Date Time** check-box.

   If both NTP and PTP are enabled, PTP takes precedence for time synchronization.

c) If not using automatic synchronization, manually update the date and time in the **Date/Time** field.

Step 5 Click **Save**.

The date, time, and time zone settings are applied to the server.

What to do next

Verify that date, time, and time zone settings are correctly set on the server.

Power Management

Configuring Chassis Identify LED

This task describes how to control the physical Identify LED on the server chassis. This LED helps visually locate a specific server in a rack or data center environment.

Procedure

Step 1 From the **Navigation Pane**, click **Chassis ID LED Control**.

Step 2 Under **LED Actions**, select the desired LED action:

- **LED Off**—Turns off the chassis Identify LED.
- **LED Solid ON**—Sets the chassis Identify LED to remain continuously lit.
- **LED Blinking ON**—Sets the chassis Identify LED to blink.

Step 3 If **LED Blinking ON** is selected, enter the desired duration in seconds in the **Identify interval in seconds** field.

Step 4 Click **Perform Action**.

The selected LED action is executed on the server chassis.

What to do next

Verify the LED behavior on the physical server chassis.

Managing Host Server Power

This task describes how to control the power state of the host server. Various power actions are available, from graceful shutdowns to immediate power cycles.

Before you begin

Ensure that performing power actions on the host server is safe and does not interrupt critical operations.

Procedure

Step 1 From the **Navigation Pane**, click **Power Control**.

Step 2 Click **Power Control on Host Server**.

The **Power Control on Host Server** page is displayed, showing the current power status.

Step 3 Under **Power Actions**, select the desired power action:

- **Force Off**—Immediately powers off the server without a graceful shutdown process.
- **Force Restart**—Immediately restarts the server without a graceful shutdown process.
- **Graceful Restart**—Initiates a controlled restart of the server, allowing the operating system to shut down properly.
- **Graceful Shutdown**—Initiates a controlled shutdown of the server, allowing the operating system to shut down properly.
- **On**—Powers on the server.
- **Power Cycle**—Performs a complete power off and then power on sequence for the server.

Step 4 Click **Perform Action**.

The selected power action is executed on the host server.

What to do next

Verify the new power state of the host server.

Configuration Management

Managing Backup Configuration

This task describes how to back up server configuration settings. A configuration backup allows for restoration of settings in case of data loss or system misconfiguration.

Before you begin

If encrypting the backup file, ensure an AES key is uploaded. See Backing Up or Restoring Key Upload, on page 78.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Backup Configuration**.

The **Backup Configuration** page is displayed.

If an AES key is not present, a message **AES Key does not exist. Click here to upload the Backup key** is displayed. Click the link to upload a key if encryption is desired.

Step 3 Select the configuration components to include in the backup by checking the corresponding check-boxes:

- **Check All**
- **SNMP**
- **KVM**
- **Network & Services**
- **IPMI**
- **NTP**
- **Authentication**
- **SYSLOG**

Step 4 Click **Download**.

The selected configuration components are backed up and downloaded as a file to a local system.

What to do next

Store the downloaded backup file in a secure location for future restoration if needed.

Preserving a Configuration

This task describes how to select specific configuration settings to be preserved across system events, such as firmware updates or restoration to factory defaults. Preserving configurations ensures continuity of essential settings.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Preserve Configuration**.

The **Preserve Configuration** page is displayed.

A link **Click here to go to Firmware Update or Restore Factory Defaults** is available for related actions.

Step 3 Select the configuration components to preserve by checking the corresponding check-boxes:

- **Check All**—Selects all available configuration components for preservation.
- **SDR**—Preserves Sensor Data Record settings.
- **FRU**—Preserves Field Replaceable Unit information.
- **SEL**—Preserves System Event Log settings.
- **IPMI**—Preserves Intelligent Platform Management Interface settings.
- **Network**—Preserves network interface configurations.
- **NTP**—Preserves Network Time Protocol settings.
- **SNMP**—Preserves Simple Network Management Protocol settings.
- **SSH**—Preserves Secure Shell settings.
- **KVM**—Preserves Keyboard, Video, Mouse settings.
- **Authentication**—Preserves user authentication settings.
- **Syslog**—Preserves system logging configurations.
- **Web**—Preserves web interface settings.
- **Extlog**—Preserves external logging configurations.
- **Redfish**—Preserves Redfish API settings.

Step 4 Click **Save**.

The selected configuration settings are marked for preservation.

What to do next

Proceed with system operations with the assurance that selected configurations are retained.

Restoring Factory Defaults

This task describes how to restore server configuration to original factory default settings. This action resets most configurations, but allows selection of specific settings for preservation.

Before you begin

Back up any critical configuration settings before proceeding, as restoring factory defaults erases most current configurations.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Restore Factory Defaults**.

The **Restore Factory Defaults** page is displayed.

A message **The following checked configurations will be preserved through the restore operation. You can make changes to the list in the preserve configuration page.** is displayed, indicating which settings are exempt from the reset. See Preserving a Configuration, on page 29.

Step 3 Select the configuration components to preserve during the factory reset. Checked items are preserved; unchecked items are reset to factory defaults:

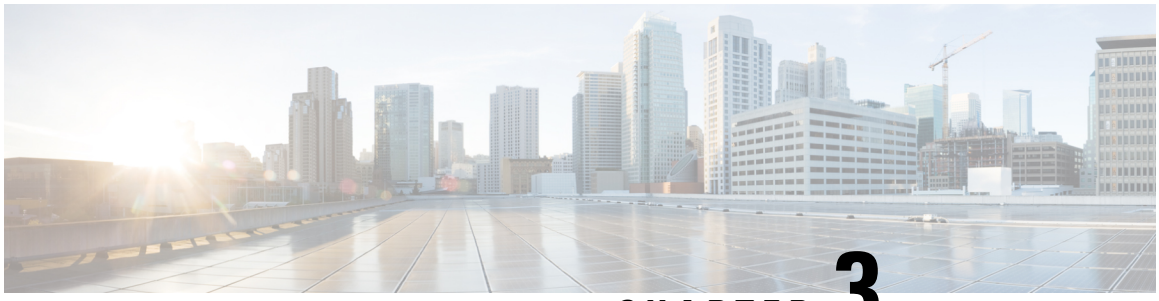
- **SDR**—Preserves Sensor Data Record settings.
- **FRU**—Preserves Field Replaceable Unit information.
- **SEL**—Preserves System Event Log settings.
- **IPMI**—Preserves Intelligent Platform Management Interface settings.
- **Network**—Preserves network interface configurations.
- **NTP**—Preserves Network Time Protocol settings.
- **SNMP**—Preserves Simple Network Management Protocol settings.
- **SSH**—Preserves Secure Shell settings.
- **KVM**—Preserves Keyboard, Video, Mouse settings.
- **Authentication**—Preserves user authentication settings.
- **Syslog**—Preserves system logging configurations.
- **Web**—Preserves web interface settings.
- **Extlog**—Preserves external logging configurations.
- **Redfish**—Preserves Redfish API settings.

Step 4 Click **Save**.

The configuration is reset to factory defaults, with the selected settings preserved.

What to do next

Reconfigure any necessary settings that were not preserved during the factory reset.



CHAPTER 3

Managing User Accounts

- Local User Management, on page 33
- External Authentication Services, on page 37

Local User Management

Understanding the User Management Overview

The **User Management** page provides a central view of all configured user accounts on the server. It allows administrators to quickly assess user status and navigate to detailed configuration pages for individual accounts.

The page includes the following elements:

- **Channel** drop-down list—Allows filtering the displayed user accounts by specific communication channels.
- User account boxes—Each box represents a user account and displays key information, such as:
  - User ID
  - Current status
  - Assigned privileges or access types

From this page, administrators can click on a user account box to modify its details, or initiate actions to add or delete user accounts.

Adding a User

This task describes how to add a new user account to the server. Creating user accounts allows for controlled access to server resources and management functions.

Before you begin

Access to the server management UI with administrator privileges is available.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **User Management**.

The **User Management** page is displayed, showing an overview of existing user accounts.

Step 3 Select an empty user box from the displayed list of user accounts.

The **User Management Configuration** page is displayed for a new user.

Step 4 Configure the user account details using the following fields and options:

Table 25: User Account Configuration Fields

Name	Description
Username field	Enter a unique username for the new account.
Password field	Enter a password for the new account.
Confirm Password field	Re-enter the password to confirm.
Enable User Access check-box	Select to activate the user account.
Enable Channel Access check-boxes	Select the desired channels for user access. For each enabled channel, select the appropriate privilege level from the corresponding **Privilege (Channel [Number])** drop-down list.
KVM Access check-box	Select to grant KVM access.
VMedia Access check-box	Select to grant VMedia access.
SNMP Access check-box	Select to grant SNMP access. If enabled, configure the following SNMP settings: • **SNMP view** field—Enter a view. • **SNMP Access level** field—Enter an access level. • **SNMP Authentication Protocol** field—Enter an authentication protocol. • **SNMP Privacy Protocol** field—Enter a privacy protocol.
Email Format drop-down list	Select an email format.
Email ID field	Enter an email ID.

Step 5 Click **Save**.

The new user account is created and configured on the server.

What to do next

Verify that the new user account appears in the **User Management** overview and has correct access permissions.

Modifying User Account Details

This task describes how to modify an existing user account's details, including password, access permissions, and other settings. This allows for updating user configurations as requirements change.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **User Management**.

The **User Management** page is displayed, showing an overview of existing user accounts.

Step 3 Select an existing user account box from the displayed list.

The **User Management Configuration** page is displayed, pre-populated with the selected user current details.

Step 4 Modify the user account details using the following fields and options as required:

Table 26: User Account Configuration Fields

Name	Description
Username field	The username for the account. This field is read-only.
Password field	Enter a new password to change the existing one.
Confirm Password field	Re-enter the new password to confirm.
Enable User Access check-box	Select or clear to enable or disable the user account.
Enable Channel Access check-boxes	Select or clear the desired channels for user access. For each enabled channel, select the appropriate privilege level from the corresponding **Privilege (Channel [Number])** drop-down list.
KVM Access check-box	Select or clear to grant or revoke KVM access.
VMedia Access check-box	Select or clear to grant or revoke VMedia access.

Name	Description
SNMP Access check-box	Select or clear to grant or revoke SNMP access. If enabled, configure the following SNMP settings: • **SNMP view** field—Enter a view. • **SNMP Access level** field—Enter an access level. • **SNMP Authentication Protocol** field—Enter an authentication protocol. • **SNMP Privacy Protocol** field—Enter a privacy protocol.
Email Format drop-down list	Select an email format.
Email ID field	Enter an email ID.

Step 5 Click **Save**.

The user account details are updated on the server.

What to do next

Verify that the user account reflects the modified settings in the **User Management** overview and functions as expected.

Deleting a User

This task describes how to delete an existing user account from the server. Deleting user accounts removes access to server resources and management functions.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **User Management**.

The **User Management** page is displayed, showing an overview of existing user accounts.

Step 3 Select the user account box for the user to delete from the displayed list.

The **User Management Configuration** page is displayed, pre-populated with the selected user details.

Step 4 Click **Delete**.

A confirmation dialog is displayed. Confirm the deletion.

The user account is permanently removed from the server.

What to do next

Verify that the deleted user account no longer appears in the **User Management** overview.

External Authentication Services

Understanding External User Services

External user services enable the server to authenticate users against external directories or authentication servers rather than relying solely on local user accounts. This approach centralizes user management, enhances security, and simplifies administration by integrating with existing enterprise authentication infrastructures.

The server supports the following external user services:

- **LDAP/E-Directory Settings**—Lightweight Directory Access Protocol (LDAP) and Novell eDirectory provide a standardized way to access and maintain distributed directory information services. Configuring these settings allows the server to authenticate users against an LDAP or eDirectory server.
- **Active Directory Settings**—Microsoft Active Directory is a directory service developed by Microsoft for Windows domain networks. Integrating with Active Directory allows the server to authenticate users against an Active Directory domain controller, leveraging existing user accounts and group policies.
- **RADIUS Settings**—Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users connecting to a network service. Configuring RADIUS allows the server to authenticate users against a RADIUS server.

Each service offers general settings for connection and authentication parameters, as well as role group configurations to map external user groups to specific server privileges.

LDAP/E-Directory Configuration

Configuring LDAP/E-Directory General Settings

This task describes how to configure the general settings for LDAP/E-Directory authentication. These settings enable the server to connect to and authenticate users against an external LDAP or E-Directory server.

Before you begin

Ensure an LDAP or E-Directory server is accessible and relevant connection details are available.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **External User Services** > **LDAP/E-Directory Settings** > **General Settings**.

The **General LDAP Settings** page is displayed.

Step 3 Configure the following general LDAP/E-Directory settings:

Table 27: General LDAP/E-Directory Settings

Name	Description
Enable LDAP/E-Directory Authentication check-box	Select to enable LDAP/E-Directory authentication.
Encryption Type radio button	Select the encryption method for communication with the LDAP/E-Directory server: • **No Encryption**—Uses unencrypted communication. • **SSL**—Uses Secure Sockets Layer for encrypted communication. • **StartTLS**—Uses Transport Layer Security over an unencrypted connection.
Common Name Type radio button	Select the type of common name used for the LDAP/E-Directory server: • **IP Address**—Uses an IP address as the common name. • **FQDN**—Uses a Fully Qualified Domain Name as the common name.
Server Address field	Enter the IP address or FQDN of the LDAP/E-Directory server.
Port field	Enter the port number for communication with the LDAP/E-Directory server.
Bind DN field	Enter the Distinguished Name (DN) for binding to the LDAP/E-Directory server.
Password field	Enter the password for the Bind DN.
Search Base field	Enter the base DN for user searches on the LDAP/E-Directory server.
Attribute of User Login field	Enter the LDAP attribute used to identify users during login.

Step 4 Click **Save**.

The LDAP/E-Directory general settings are applied.

What to do next

Test LDAP/E-Directory authentication to ensure users can log in successfully.

Configuring LDAP/E-Directory Role Groups

This task describes how to configure role groups for LDAP/E-Directory. Role groups map external LDAP/E-Directory user groups to specific server privileges and access levels, ensuring that users authenticated via LDAP/E-Directory receive appropriate permissions.

Before you begin

LDAP/E-Directory authentication must be enabled in the general settings. See Configuring LDAP/E-Directory General Settings, on page 37.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **External User Services** > **LDAP/E-Directory Settings** > **Role Groups**.

The **Role Groups** page is displayed, showing existing LDAP/E-Directory group mappings.

Step 3 To add a new role group mapping, select an empty group box from the displayed list. To modify an existing role group mapping, click on the group box for the role group to modify.

The **Role Group Configuration** interface is displayed.

Step 4 Configure the role group details. See Configuring Active Directory Role Groups, on page 40.

What to do next

Test user logins from the configured LDAP/E-Directory groups to verify that correct privileges are assigned.

Active Directory Configuration

Configuring Active Directory General Settings

This task describes how to configure the general settings for Active Directory authentication. These settings enable the server to connect to and authenticate users against an external Active Directory domain.

Before you begin

Ensure an Active Directory domain controller is accessible and relevant connection details are available.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **External User Services** > **Active Directory Settings** > **General Settings**.

The **General Active Directory Settings** page is displayed.

Step 3 Configure the following general Active Directory settings:

Table 28: General Active Directory Settings

Name	Description
Enable Active Directory Authentication check-box	Select to enable Active Directory authentication.
TLS check-box	Select to enable Transport Layer Security for secure communication with the Active Directory server.
Secret Username field	Enter the username for binding to the Active Directory server.
Secret Password field	Enter the password for the Secret Username.
User Domain Name field	Enter the domain name for Active Directory users.
Domain Controller Server Address 1 field	Enter the IP address or FQDN of the primary Active Directory domain controller.
Domain Controller Server Address 2 field	Enter the IP address or FQDN of a secondary Active Directory domain controller.
Domain Controller Server Address 3 field	Enter the IP address or FQDN of a tertiary Active Directory domain controller.

Step 4 Click **Save**.

The Active Directory general settings are applied.

What to do next

Test Active Directory authentication to ensure users can log in successfully.

Configuring Active Directory Role Groups

This task describes how to configure role groups for Active Directory. Role groups map external Active Directory user groups to specific server privileges and access levels, ensuring that users authenticated via Active Directory receive appropriate permissions.

Before you begin

Active Directory authentication must be enabled in the general settings. See Configuring Active Directory General Settings, on page 39.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **External User Services** > **Active Directory Settings** > **Role Groups**.

The **Role Groups** page is displayed, showing existing Active Directory group mappings.

Step 3 To add a new role group mapping, select an empty group box from the displayed list.

To modify an existing role group mapping, click on the group box for the role group to modify.

The **Role Group Configuration** interface is displayed.

Step 4 Configure the role group details using the following fields and options:

Table 29: Active Directory Role Group Configuration Fields

Name	Description
Group Name field	Enter the name of the Active Directory group.
Group Domain field	Enter the domain of the Active Directory group.
Group Privilege drop-down list	Select the server privilege level to assign to members of this Active Directory group.
KVM Access check-box	Select to grant KVM access to members of this group.
VMedia Access check-box	Select to grant VMedia access to members of this group.

Step 5 Click **Save**.

The Active Directory role group settings are applied.

What to do next

Test user logins from the configured Active Directory groups to verify that correct privileges are assigned.

RADIUS Configuration

Configuring RADIUS General Settings

This task describes how to configure the general settings for RADIUS authentication. These settings enable the server to connect to and authenticate users against an external RADIUS server.

Before you begin

Ensure a RADIUS server is accessible and relevant connection details are available.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **External User Services** > **RADIUS Settings** > **General RADIUS Settings**.

The **General RADIUS Settings** page is displayed.

Step 3 Configure the following general RADIUS settings:

Table 30: General RADIUS Settings

Name	Description
Enable RADIUS Authentication check-box	Select to enable RADIUS authentication.
Server Address field	Enter the IP address or FQDN of the RADIUS server.
Port field	Enter the port number for communication with the RADIUS server.
Secret field	Enter the shared secret key for authentication with the RADIUS server.
Enable KVM Access check-box	Select to grant KVM access to users authenticated via RADIUS.
Enable VMedia Access check-box	Select to grant VMedia access to users authenticated via RADIUS.

Step 4 Click **Save**.

The RADIUS general settings are applied.

What to do next

Test RADIUS authentication to ensure users can log in successfully.

Configuring RADIUS Advanced Settings

This task describes how to configure advanced settings for RADIUS authentication, specifically defining authorization levels for different user roles. These settings determine the privileges granted to users authenticated via RADIUS.

Before you begin

RADIUS general settings must be configured and enabled. See Configuring RADIUS General Settings, on page 41.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **External User Services** > **RADIUS Settings** > **Advanced RADIUS Settings**.

The **Advanced RADIUS Settings** page is displayed.

If RADIUS general configuration is not enabled, the message **Radius configuration is not enabled.** is displayed, and authorization configuration options are unavailable.

Step 3 Under **RADIUS Authorization**, configure the authorization levels for different user roles:

Table 31: RADIUS Authorization Levels

Name	Description
Administrator	Select to grant full administrative privileges to RADIUS authenticated users.
Operator	Select to grant operator-level privileges to RADIUS authenticated users.
User	Select to grant standard user-level privileges to RADIUS authenticated users.
No Access	Select to deny any access to RADIUS authenticated users.

Step 4 Click **Save**.

The RADIUS advanced settings are applied.

What to do next

Test RADIUS authentication with different user roles to verify that correct authorization levels are applied.

Configuring PAM Authentication Order

This task describes how to configure the order of Pluggable Authentication Modules (PAM). The PAM authentication order determines the sequence in which the server attempts to authenticate users against various sources, such as local accounts, LDAP, Active Directory, and RADIUS.

Before you begin

External authentication services (LDAP, Active Directory, RADIUS) are configured as required.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **PAM Order Settings**.

The **PAM Order** page is displayed, showing a list of available authentication methods.

The list includes:

- **IPMI**
- **LDAP**
- **ACTIVE DIRECTORY**
- **RADIUS**

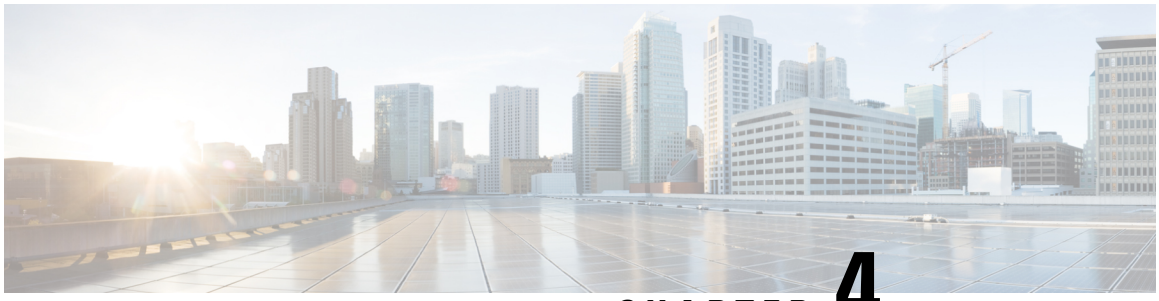
Step 3 Rearrange the authentication methods by dragging them up or down the list to establish the desired authentication priority.

Step 4 Click **Save**.

The new PAM authentication order is applied.

What to do next

Test user logins to verify that authentication proceeds according to the configured PAM order.



CHAPTER 4

Managing Remote Presence

- Remote Console Access, on page 45
- Virtual Media Management, on page 52
- Video Recording, on page 56

Remote Console Access

Launching H5Viewer

This task describes how to launch the H5Viewer, which provides a web-based KVM console for remote access to the server. The H5Viewer allows for remote control of the server's keyboard, video, and mouse.

Before you begin

Ensure network connectivity to the server and that the necessary browser plugins or settings are in place for HTML5-based KVM access.

Procedure

Step 1 From the **Navigation Pane**, click **Remote Control**.

Step 2 Click **Launch H5Viewer**.

The H5Viewer KVM console launches in a different browser tab, displaying the console output.

What to do next

Interact with the console remotely using the H5Viewer.

Using the H5Viewer KVM Console

This task describes how to use the various features and controls available within the H5Viewer KVM console. The console provides comprehensive tools for remote management of the server's video, keyboard, and mouse.

Before you begin

Launch the H5Viewer KVM console. See Launching H5Viewer, on page 45.

Procedure

Interact with the H5Viewer KVM console using the available menus and controls.

The H5Viewer KVM console provides the following menus and controls for remote server management:

Table 32: Main Toolbar Items

Name	Description
CD Image section	Manages CD image redirection. Includes **Browse File** to select an image, **Media Boost** check-box, and **Start Media** to begin redirection.
Stop KVM	Stops the current KVM session.
Request Full Access	Requests full access to the KVM session (typically displayed when in a shared or partial access mode).
Host Display is Unlocked	Indicates the status of the host display lock. Clicking toggles the lock state.
Server is Powered On	Indicates the current power state of the server.
Notifications	Displays system notifications and alerts.

Table 33: Video Menu Options

Name	Description
Pause Video	Pauses the video feed from the server.
Resume Video	Resumes a paused video feed.
Refresh Video	Refreshes the video feed from the server.
Display ON	Turns on the host display.
Display OFF	Turns off the host display.
Capture Screen	Captures a screenshot of the current server display.

Table 34: Mouse Menu Options

Name	Description
Show Client Cursor	Displays the client-side mouse cursor.
Absolute Mouse Mode	Sets the mouse to absolute positioning mode.

Name	Description
Other Mouse Mode	Sets the mouse to an alternative positioning mode.

Table 35: Options Menu

Name	Description
Normal	Sets the zoom level to normal (100%).
Zoom In	Increases the zoom level.
Zoom Out	Decreases the zoom level.
Partial Permission	Blocks requests for full access, allowing only partial permission.
No Permission	Blocks all privilege requests, allowing no permission.
keyboard/mouse encryption	Enables or disables encryption for keyboard and mouse input.
Compression Menu (YUV options)	Options for video compression using YUV color space.
DCT Menu (Quality options)	Options for video quality using Discrete Cosine Transform.

Table 36: Keyboard Menu Options

Name	Description
Keyboard Layout (Header)	Options to select the keyboard layout.

Table 37: Send Keys Menu Options

Name	Description
Hold Down (Header)	Options to simulate holding down specific keys.
Right Ctrl Key	Simulates holding down the Right Control key.
Right Alt Key	Simulates holding down the Right Alt key.
Right Windows Key	Simulates holding down the Right Windows key.
Left Ctrl Key	Simulates holding down the Left Control key.
Left Alt Key	Simulates holding down the Left Alt key.
Left Windows Key	Simulates holding down the Left Windows key.
Press and Release (Header)	Options to simulate pressing and releasing specific key combinations.
Ctrl+Alt+Del	Sends the Ctrl+Alt+Del key combination.

Name	Description
Left Windows Key	Sends the Left Windows key.
Right Windows Key	Sends the Right Windows key.
Context Menu Key	Sends the Context Menu key.
Print Screen Key	Sends the Print Screen key.

Table 38: Hot Keys Menu Options

Name	Description
Add Hot Keys	Opens a dialog to define and add user-defined macros or hotkey combinations.
User-defined macros	Displays any previously configured user-defined hotkey combinations.

Table 39: Video Record Menu Options

Name	Description
Record Video	Starts recording the KVM console video feed.
Stop Recording	Stops the active video recording.
Record Settings	Opens a dialog to configure video recording parameters such as video length, compression, and resolution.

Table 40: Power Menu Options

Name	Description
Force Off	Immediately powers off the server without a graceful shutdown process.
Force Restart	Immediately restarts the server without a graceful shutdown process.
Graceful Restart	Initiates a controlled restart of the server, allowing the operating system to shut down properly.
Graceful Shutdown	Initiates a controlled shutdown of the server, allowing the operating system to shut down properly.
On	Powers on the server.
Power Cycle	Performs a complete power off and then power on sequence for the server.

Table 41: Active Users Menu Options

Name	Description
User entries	Displays a list of currently active users connected to the KVM session, including their username, authentication method, and IP address. Includes an option to disconnect a user.

Table 42: Help Menu Options

Name	Description
About H5Viewer	Displays information about the H5Viewer application.

Table 43: Status Bar Items

Name	Description
LWIN	Indicates the state of the Left Windows key.
RWIN	Indicates the state of the Right Windows key.
LALT	Indicates the state of the Left Alt key.
LCTRL	Indicates the state of the Left Control key.
RALT	Indicates the state of the Right Alt key.
RCTRL	Indicates the state of the Right Control key.
NUM	Indicates the state of the Num Lock key.
CAPS	Indicates the state of the Caps Lock key.
SCR	Indicates the state of the Scroll Lock key.

Table 44: H5Viewer Dialogs

Name	Description
OEM Dialog	A dialog for OEM-specific messages or interactions.
Master Dialog	Manages slave permission requests, allowing granting of full, partial, or no permission, or blocking future requests.
Slave Dialog	Displays a message indicating that permission is requested for virtual console access.
Status Dialog	Displays various status messages related to the KVM session.
Switch Master Dialog	Allows transferring master control of the KVM session to another active session.

Name	Description
Video Record Settings Dialog	Configures video recording parameters such as video length, compression, and resolution.
Keyboard Layout Dialog	Prompts to set the current keyboard layout as the default for upcoming KVM sessions.
User Defined Macros Dialog	Manages user-defined macros or hotkey combinations.
Add Macro Dialog	Allows defining new user-defined macros by capturing key events.
About H5Viewer Dialog	Displays information about the H5Viewer application.

Table 45: Touch Keyboard Controls (When displayed)

Name	Description
Function keys (Esc, F1-F12)	Simulates pressing the corresponding function keys.
Navigation/Modifier keys (Tab, Ins, Del, Home, End, Pg Up, Pg Dn, Prt Scn, Pau/Brk, Shift, Ctrl, Win, Alt, Context Menu)	Simulates pressing the corresponding navigation or modifier keys.
Arrow keys (Up, Left, Down, Right)	Simulates pressing the corresponding arrow keys.
Lock keys (Num Lock, Caps Lock, Scr Lock)	Toggles the state of the respective lock keys.
Mouse Pad controls (scroll canvas up/down/left/right)	Provides virtual mouse scrolling functionality.

What to do next

Utilize the H5Viewer KVM console to perform remote management and control tasks on the server.

Configuring Remote KVM Session Settings

This task describes how to configure settings for remote KVM sessions, including keyboard language, virtual media attachment modes, and session management parameters. Proper configuration enhances the remote control experience.

Procedure

Step 1 From the **Navigation Pane**, click **Remote Control**.

Step 2 Under **H5Viewer** section, click **Remote Session Settings**.

The **Remote Session Settings** page is displayed.

Step 3 Configure the following remote KVM session settings:

Table 46: Remote KVM Session Settings

Name	Description
KVM Single Port Application check-box	Select to enable a single port for KVM application access.
Keyboard Language drop-down list	Select the keyboard layout for the remote KVM session.
Virtual Media Attach Mode drop-down list	Select the mode for attaching virtual media to the remote session.
Retry Count field	Enter the number of times to retry a connection attempt.
Retry Time Interval (Seconds) field	Enter the time interval, in seconds, between connection retries.
Server Monitor OFF Feature Status check-box	Select to enable or disable the server monitor OFF feature.
Automatically OFF Server Monitor, When KVM Launches check-box	Select to automatically turn off the server monitor when a KVM session launches.

Step 4 Click **Save**.

The remote KVM session settings are applied.

What to do next

Launch a KVM session to verify that the configured settings are applied.

Configuring KVM Mouse Setting

This task describes how to configure the mouse mode for KVM (Keyboard, Video, Mouse) sessions. Proper mouse mode configuration ensures accurate and responsive cursor control during remote interactions with the server.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **KVM Mouse Setting**.

The **KVM Mouse Setting** page is displayed.

Step 3 Under **Mouse Mode Configuration**, select the desired mouse mode:

Table 47: Mouse Mode Options

Name	Description
Absolute Positioning (Windows) radio button	Select for absolute mouse positioning, typically recommended for Windows operating systems.

Name	Description
Other Mode (SLES-11 OS Installation) radio button	Select for other operating systems or specific scenarios, such as SLES-11 OS installation.

Step 4 Click **Save**.

The KVM mouse mode settings are applied.

What to do next

Launch a KVM session and verify that mouse control functions as expected with the configured mode.

Activating Serial Over LAN

This task describes how to activate Serial Over LAN (SOL) functionality. Activating SOL enables remote access to the server's serial console, which is useful for command-line management and troubleshooting.

Before you begin

Ensure network connectivity to the server for remote access.

Procedure

Step 1 From the **Navigation Pane**, click **Remote Control**.

Step 2 Under the **Serial Over LAN** section, click **Activate**.

Serial Over LAN functionality is activated on the server.

What to do next

Establish a remote serial connection to the server to verify SOL functionality.

Virtual Media Management

Understanding Image Redirection

Image redirection enables administrators to mount local or network-based image files (such as ISOs or virtual hard disk images) to the server's virtual CD/DVD or hard disk drives. This functionality is crucial for tasks like operating system installations, firmware updates, and running diagnostics remotely, eliminating the need for physical media at the server location.

The main **Image Redirection** page, labeled **Remote Media**, displays a table of currently redirected media. This table includes:

- **Media Type** column
- **Server** column
- **Session Index** column
- **Image name** column
- **Redirection Status** column

From this page, administrators can:

- Access **Media General Settings** to enable or disable the overall remote media support.
- Click **Refresh Image List** to update the displayed list of images.
- Click **Sync Image Status** to synchronize the status of redirected images.

Configuring Media Support

This task describes how to enable or disable overall remote media support. Enabling media support allows the server to utilize virtual media for tasks such as operating system installation or firmware updates.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Media Redirection** > **General Settings**.

The **Media General Settings** page is displayed.

Step 3 Select or clear the **Remote Media Support** check-box.

Selecting this check-box enables remote media functionality. Clearing it disables the functionality.

Step 4 Click **Save**.

The remote media support setting is applied.

What to do next

Verify that remote media functionality operates as expected.

Configuring VMedia Instance Settings

This task describes how to configure settings for Virtual Media (VMedia) instances. These settings control how virtual CD/DVD, hard disk, and SD media devices are emulated and presented to the host server.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Media Redirection** > **VMedia Instance Settings**.

The **VMedia Instance Settings** page is displayed.

Step 3 Configure the VMedia instance settings:

The page displays sections for configuring various virtual media device instances:

Table 48: VMedia Instance Configuration Options

Name	Description
CD/DVD device instances drop-down list	Configures virtual CD/DVD drive instances for media redirection.
Hard disk instances drop-down list	Configures virtual hard disk drive instances for media redirection.
Remote KVM CD/DVD device instances drop-down list	Configures virtual CD/DVD drive instances specifically for remote KVM sessions.
Remote KVM Hard disk instances drop-down list	Configures virtual hard disk drive instances specifically for remote KVM sessions.
Emulate SD Media as USB disk to Host check-box	Select or clear to enable or disable the emulation of SD media as a USB disk to the host server.

Step 4 Click **Save**.

The VMedia instance settings are applied.

What to do next

Verify that the configured VMedia instances are accessible and function as expected on the host server.

Viewing Remote Media Status

This task describes how to view the status of remote media (image redirection). Monitoring this status provides information about available and active virtual media connections to the server.

Procedure

Step 1 From the **Navigation Pane**, click **Image Redirection**.

Step 2 Click **Remote Images**.

The **Remote Media** page is displayed, showing a table of available remote media.

Step 3 Review the **Remote Media** table for information about available and redirected images:

Table 49: Remote Media Table

Name	Description
Media type column	The type of virtual media.
Server column	The server hosting the media image.
Session Index column	A unique identifier for the media session.
Image name column	The name of the image file.
Redirection Status column	The current status of the media redirection.

The page also provides the following actions:

- **Click here to go to Media General Settings**—Navigates to the page for configuring overall remote media support. See Configuring Media Support, on page 53.
- **Refresh Image List**—Refreshes the displayed list of images.
- **Sync Image Status**—Synchronizes the status of redirected images.

What to do next

Use the displayed information to monitor the availability and status of remote media.

Viewing Active Media Redirections

This task describes how to view a list of all currently active media redirection sessions. Monitoring active redirections provides insight into current remote media usage and connections.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Media Redirection** > **Active Redirections**.

The **Active Redirections** page is displayed, showing a table of all active media redirection sessions.

Table 50: Active Media Redirections

Name	Description
Media Type column	The type of virtual media being redirected.
Media Instance column	The specific instance of the media being redirected.

Name	Description
Client Type column	The type of client initiating the redirection.
Image Name column	The name of the image file being redirected.
Redirection Status column	The current status of the media redirection session.
Client IP column	The IP address of the client initiating the redirection.

What to do next

Use the displayed information to monitor virtual media usage or troubleshoot redirection issues.

Video Recording

Understanding Video Recording Options

Video recording functionality allows administrators to capture and store visual records of server console sessions. This is valuable for auditing, troubleshooting, and post-event analysis. The system offers various configurations to control when and how video is recorded.

The **Video Recording** section within **Settings** provides access to the following configuration pages:

- **Auto Video Settings**—This section configures automatic video recording based on predefined triggers. It includes:
  - **Video Trigger Settings**—Defines the events that initiate video recording, such as critical, non-critical, or non-recoverable events, fan state changes, watchdog timer events, chassis power events, and date/time events.
  - **Video Remote Storage**—Configures options for saving recorded video to a remote server, including storage limits and server access details.
  - **Pre-Event Video Recordings**—Configures settings for capturing video footage leading up to a triggered event, including video quality, compression mode, frames per second, and duration.
- **SOL Settings**—This section configures video recording specifically for Serial Over LAN sessions. It includes:
  - **SOL Configurations**—Defines parameters such as volatile and non-volatile bit rates for SOL video recordings.

Configuring Auto Video Trigger Settings

This task describes how to configure the triggers for automatic video recording. Event-based triggers ensure that video footage is captured when specific system events occur, aiding in troubleshooting and auditing.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Video Recording** > **Auto Video Settings** > **Video Trigger Settings**.

The **Video Trigger Settings** page is displayed.

Step 3 Select the check-boxes for the events that trigger automatic video recording:

Table 51: Auto Video Trigger Options

Name	Description
Critical Events (Temperature/Voltage) check-box	Select to trigger recording on critical temperature or voltage events.
Non Critical Events (Temperature/Voltage) check-box	Select to trigger recording on non-critical temperature or voltage events.
Non Recoverable Events (Temperature/Voltage) check-box	Select to trigger recording on non-recoverable temperature or voltage events.
Fan state changed Events check-box	Select to trigger recording when a fan's operational state changes.
Watchdog Timer Events check-box	Select to trigger recording on watchdog timer events.
Chassis Power On Events check-box	Select to trigger recording when the server chassis powers on.
Chassis Power Off Events check-box	Select to trigger recording when the server chassis powers off.
Chassis Reset Events check-box	Select to trigger recording when the server chassis resets.
LPC Reset Events check-box	Select to trigger recording on Low Pin Count (LPC) bus reset events.
Date and Time Event check-box	Select to trigger recording at a specific date and time.
Pre-Event Video Recording check-box	Select to enable capturing video footage leading up to a triggered event.

Step 4 Click **Save**.

The automatic video recording trigger settings are applied.

What to do next

Verify that video recording initiates as expected when configured events occur.

Configuring Video Remote Storage

This task describes how to configure settings for storing recorded video to a remote server. Remote storage allows for offloading video files from the server's local storage and centralizing video archives.

Before you begin

Ensure a remote server for video storage is accessible via the network and has appropriate share configurations.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Video Recording** > **Auto Video Settings** > **Video Remote Storage**.

The **Video Remote Storage** page is displayed.

Step 3 Configure the following video remote storage settings:

Table 52: Video Remote Storage Settings

Name	Description
Record Video to Remote Server check-box	Select to enable recording video to a remote server.
Maximum Dumps field	Enter the maximum number of video dumps to store on the remote server.
Maximum Duration (Sec) field	Enter the maximum duration, in seconds, for each recorded video segment.
Maximum Size (MB) field	Enter the maximum size, in megabytes (MB), for each recorded video file.
Server Address field	Enter the IP address or FQDN of the remote server.
Path in server field	Enter the path on the remote server where video files are stored.
Share Type	Select the type of network share protocol used by the remote server: • **NFS**—Network File System. • **CIFS**—Common Internet File System.

Step 4 Click **Save**.

The video remote storage settings are applied.

What to do next

Verify that video recordings are successfully saved to the remote server.

Configuring Pre-Event Video Recording Options

This task describes how to configure options for pre-event video recording. Pre-event recording captures video footage leading up to a triggered event, providing a more complete context for analysis.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Video Recording** > **Auto Video Settings** > **Pre-Event Video Recordings**.

The **Pre-Event Video Recordings** page is displayed.

Step 3 Configure the following pre-event video recording options:

Table 53: Pre-Event Video Recording Options

Name	Description
Video Quality drop-down list	Select the desired video quality for pre-event recordings.
Compression Mode drop-down list	Select the video compression mode.
Frames Per Second field	Enter the number of frames to capture per second.
Video Duration field	Enter the duration of the pre-event video recording.

Step 4 Click **Save**.

The pre-event video recording options are applied.

What to do next

Ensure pre-event video recording is enabled on the **Video Trigger Settings** page for these options to take effect.

Configuring SOL Video Recording Settings

This task describes how to configure video recording settings specifically for Serial Over LAN (SOL) sessions. These settings control the quality and characteristics of video captured during SOL interactions.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Video Recording** > **SOL Settings** > **SOL Configurations**.

The **SOL Configurations** page is displayed.

Step 3 Configure the following SOL video recording settings:

Table 54: SOL Video Recording Settings

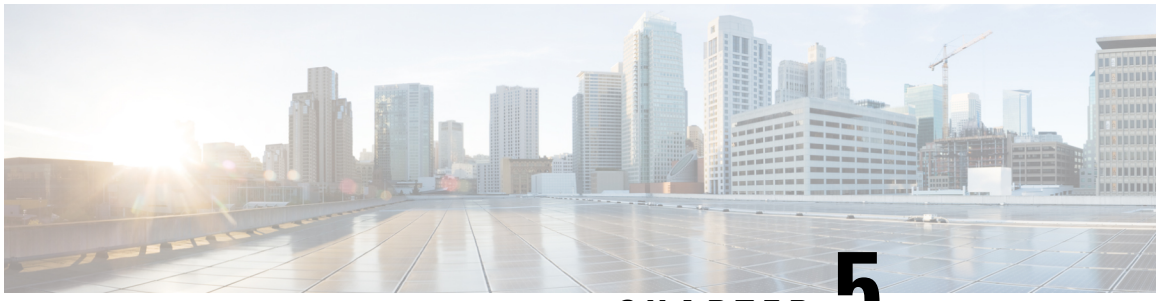
Name	Description
Volatile Bit Rate drop-down list	Select the bit rate for volatile SOL video recording. Available values include 9600, 19200, 38400, 57600, and 115200.
Non-Volatile Bit Rate drop-down list	Select the bit rate for non-volatile SOL video recording. Available values include 9600, 19200, 38400, 57600, and 115200.

Step 4 Click **Save**.

The SOL video recording settings are applied.

What to do next

Verify that SOL video recordings are captured with the configured bit rates.



CHAPTER 5

Configuring Network Settings

- Understanding Network Settings Overview, on page 61
- Configuring Network IP Settings, on page 61
- Configuring Network Link Configuration, on page 63
- Configuring DNS Settings, on page 64

Understanding Network Settings Overview

Network settings are crucial for establishing and maintaining server connectivity within a network environment. These configurations define how the server communicates with other devices, accesses external resources, and makes its services available.

Network settings include options for configuring:

- **Network IP Settings**—Options for managing the server's IP address (IPv4 and IPv6), including static assignments or dynamic allocation via DHCP. This also includes settings for VLANs and enabling or disabling the LAN interface.
- **Network Link Configuration**—Options for defining the physical characteristics of the network connection, such as auto-negotiation, specific link speeds, and duplex modes.
- **DNS Configuration**—Options for setting up Domain Name System resolution, including primary and secondary DNS server addresses, hostname management (automatic or manual), mDNS, and BMC registration settings for network discovery.

Proper configuration of these network parameters ensures reliable and efficient network operation for the server.

Configuring Network IP Settings

This task describes how to configure the server network IP settings, including IPv4 and IPv6 addressing, DHCP, and VLAN settings. Proper IP configuration is essential for network connectivity.

Before you begin

Ensure valid IP address, subnet, and gateway information is available for static IP configuration.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Network Settings** > **Network IP Settings**.

The **Network IP Settings** page is displayed.

Step 3 Configure the following network IP settings:

Table 55: Network IP Configuration Fields

Name	Description
Enable LAN check-box	Select to enable the LAN interface.
LAN Interface drop-down list	Select a specific network interface to configure.
MAC Address field	Displays the Media Access Control (MAC) address of the LAN interface.
Enable IPv4 check-box	Select to enable IPv4 addressing.
Enable IPv4 DHCP check-box	Select to obtain IPv4 address settings automatically via DHCP.
IPv4 Address field	Enter the static IPv4 address.
IPv4 Subnet field	Enter the IPv4 subnet mask.
IPv4 Gateway field	Enter the IPv4 default gateway address.
Enable IPv6 check-box	Select to enable IPv6 addressing.
IPv6 Index drop-down list	Select a specific IPv6 address entry for configuration or review.
IPv6 Address field	Enter the static IPv6 address for the interface.
Subnet Prefix Length field	Enter the subnet prefix length for the IPv6 address.
IPv6 Gateway field	Enter the IPv6 default gateway address.
Clear IPv6 Address check-box	Click to remove the configured IPv6 address.
Enable VLAN check-box	Select to enable VLAN tagging.
VLAN ID field	Enter the VLAN identifier.
VLAN Priority field	Enter the VLAN priority value.

Step 4 Click **Save**.

The network IP settings are applied.

What to do next

Verify network connectivity and IP address configuration after applying settings.

Configuring Network Link Configuration

This task describes how to configure the physical link parameters of the server's LAN interface. Configuring link speed and duplex mode ensures optimal network performance and compatibility.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Network Settings** > **Network Link Configuration**.

The **Network Link Configuration** page is displayed.

Step 3 Configure the following network link settings:

Table 56: Network Link Configuration Fields

Name	Description
LAN Interface drop-down list	Select to enable the LAN interface.
Auto Negotiation check-box	Select to enable automatic negotiation of link speed and duplex mode with the connected network device.
Link Speed drop-down list	Select the desired link speed. This option is available when **Auto Negotiation** is cleared. Supported values include 100 Mbps and 10 Mbps.
Duplex Mode radio buttons	Select the desired duplex mode. This option is available when **Auto Negotiation** is cleared. Options include **FULL Duplex** and **HALF Duplex**.

Step 4 Click **Save**.

The network link configuration settings are applied.

What to do next

Verify network connectivity and link status after applying settings.

Configuring DNS Settings

This task describes how to configure Domain Name System (DNS) settings for the server. Proper DNS configuration enables the server to resolve hostnames to IP addresses and allows for network discovery of the BMC.

Before you begin

Ensure network connectivity and valid DNS server addresses are available.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Network Settings** > **DNS Configuration**.

The **DNS Configuration** page is displayed.

Step 3 Configure the following DNS settings:

Table 57: DNS Configuration Fields

Name	Description
DNS Enabled check-box	Select to enable or disable DNS resolution.
mDNS Enabled check-box	Select to enable or disable multicast DNS (mDNS) for local network service discovery.
Host Name Setting	Select the method for setting the hostname: • **Automatic**—The hostname is assigned automatically. • **Manual**—Allows manual entry of the hostname.
Host Name field	Enter the desired hostname for the server (available when **Manual** is selected for Host Name Setting).
BMC Registration Settings	Configures how the BMC registers itself on the network.
BMC Interface	Displays the BMC network interface.
Register BMC check-box	Select to enable BMC registration on the network.
Registration method	Select the method for BMC registration: • **Nsupdate** • **DHCP Client FQDN** • **Hostname**

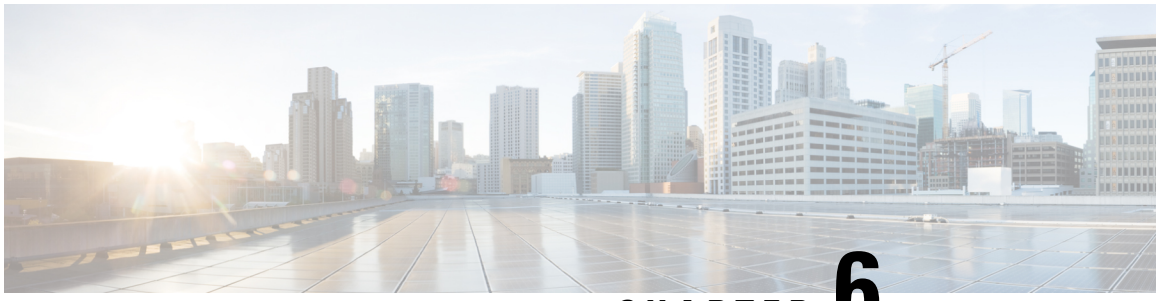
Name	Description
Eth0 TSIG Configuration	Configures TSIG (Transaction Signature) for DNS updates on the eth0 interface.
TSIG Authentication Enabled check-box	Select to enable TSIG authentication.
Current TSIG Private File Info field	Displays information about the currently used TSIG private file.
New TSIG Private File field	Allows uploading a new TSIG private file.
Domain Setting	Select the method for setting the domain name: • **Automatic** • **Manual**
Domain Name field	Enter the domain name (available when **Manual** is selected for Domain Setting).
Domain Name Server Setting	Select the method for setting DNS server addresses: • **Automatic** • **Manual**
DNS Server 1 field	Enter the IP address of the primary DNS server (available when **Manual** is selected for Domain Name Server Setting).
DNS Server 2 field	Enter the IP address of the secondary DNS server.
DNS Server 3 field	Enter the IP address of the tertiary DNS server.

Step 4 Click **Save**.

The DNS settings are applied.

What to do next

Verify that hostname resolution and network discovery function correctly after applying DNS settings.



CHAPTER 6

Managing Communication Services

- Viewing Service Status, on page 67
- Configuring Service Settings, on page 68
- Configuring SMTP Settings, on page 69

Viewing Service Status

This task describes how to view the status of various BMC services and monitor active sessions for each service. Monitoring service status helps in understanding server connectivity and usage.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Services**.

The **Services** page is displayed, showing a table of all configured BMC services.

Table 58: BMC Services Status

Name	Description
Service column	The name of the BMC service.
Status column	The current operational status of the service (Active or Inactive).
Interfaces column	The network interface the service is bound to.
Secure Port column	The port number for secure communication (if applicable).
Timeout column	The session timeout value for the service.
Maximum Sessions column	The maximum number of concurrent sessions allowed for the service.
Edit icon	Click to modify the configuration settings for the service.

Name	Description
Active Sessions icon	Click to view details of currently active sessions for the service.

Step 3 To view details of active sessions for a specific service, click the active sessions icon (typically an icon indicating active sessions) in the row of the desired service.

The **Service Sessions** page is displayed, showing a table of active sessions for that service.

Table 59: Active Service Sessions

Name	Description
Session ID column	A unique identifier for the active session.
Session Type column	The type of session.
User ID column	The internal identifier for the user.
User Name column	The username associated with the session.
Client IP column	The IP address of the client connected to the session.
Privilege column	The privilege level of the user in the session.
Delete icon	Click to terminate the active session.

What to do next

Monitor service statuses and manage active sessions as required.

Configuring Service Settings

This task describes how to configure settings for individual BMC services. Configuring service settings allows for control over service activation, network interfaces, port numbers, timeouts, and session limits.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Services**.

The **Services** page is displayed, showing a table of all configured BMC services.

Step 3 In the row of the desired service, click the **Edit** icon.

The **Service Configuration** page is displayed for the selected service.

Step 4 Configure the following service settings:

Table 60: Service Configuration Fields

Name	Description
Service Name field	Displays the name of the service being configured.
Active check-box	Select or clear to activate or deactivate the service.
Interface Name drop-down list	Select the network interface to which the service is bound.
Secure port field	Enter the port number for secure communication for the service.
Timeout field	Enter the session timeout value for the service.
Maximum Sessions field	Enter the maximum number of concurrent sessions allowed for the service.

Step 5 Click **Save**.

The service settings are applied.

What to do next

Verify that the service operates with the configured settings.

Configuring SMTP Settings

This task describes how to configure Simple Mail Transfer Protocol (SMTP) settings. Configuring SMTP enables the server to send email notifications for alerts, system events, and reports.

Before you begin

Ensure an SMTP server is accessible and relevant connection details (server address, port, authentication credentials) are available.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **SMTP Settings**.

The **SMTP Settings** page is displayed.

Step 3 Configure the following SMTP settings:

Table 61: SMTP Configuration Fields

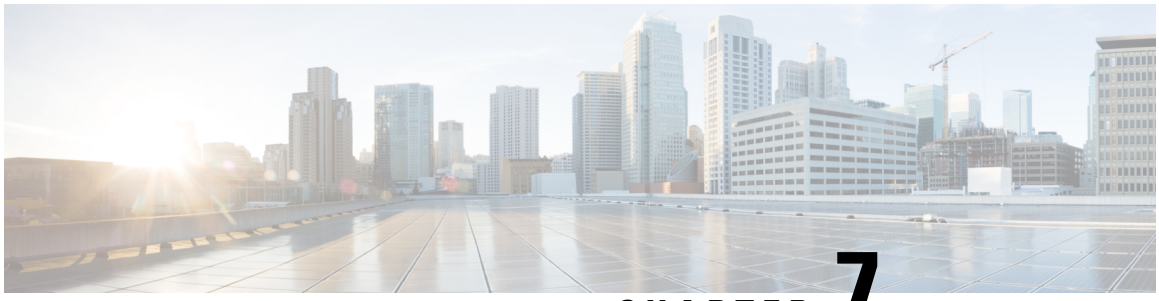
Name	Description
LAN Interface drop-down list	Select the network interface used for sending SMTP emails.
Sender Email ID field	Enter the email address that appears as the sender of notifications.
Primary SMTP Support check-box	Select to enable or disable support for the primary SMTP server.
Primary Server Name field	Enter the hostname or FQDN of the primary SMTP server.
Primary Server IP field	Enter the IP address of the primary SMTP server.
Primary SMTP port field	Enter the port number for non-secure communication with the primary SMTP server.
Primary Secure SMTP port field	Enter the port number for secure communication with the primary SMTP server.
Primary SMTP Authentication check-box	Select to enable authentication for the primary SMTP server.
Primary Username field	Enter the username for primary SMTP authentication (available when Primary SMTP Authentication is selected).
Primary Password field	Enter the password for primary SMTP authentication (available when Primary SMTP Authentication is selected).
Primary SMTP SSLTLS Enable check-box	Select to enable SSL/TLS encryption for the primary SMTP server.
Primary SMTP STARTTLS Enable check-box	Select to enable STARTTLS encryption for the primary SMTP server.
Secondary SMTP Support check-box	Select to enable or disable support for a secondary SMTP server. Additional fields for secondary server configuration are displayed when this option is selected.

Step 4 Click **Save**.

The SMTP settings are applied.

What to do next

Send a test email to verify that SMTP notifications function correctly.



CHAPTER 7

Managing Server Security and Certificates

- SSL Certificate Management, on page 71
- Firewall Configuration, on page 74
- Secure Configuration Management, on page 78

SSL Certificate Management

Viewing SSL Certificate Information

This task describes how to view detailed information about the currently installed SSL certificate. Reviewing certificate details helps verify its validity, issuer, and other security parameters.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **SSL Settings** > **View SSL Certificate**.

The **View SSL Certificate** page is displayed, showing the current certificate information.

Table 62: Current Certificate Information

Name	Description
Certificate Version	The version of the SSL certificate.
Serial Number	A unique serial number assigned to the certificate.
Signature Algorithm	The algorithm used to sign the certificate.
Public Key	Details about the public key, including its length.
Issuer Common Name (CN)	The common name of the certificate issuer.
Issuer Organization (O)	The organization name of the certificate issuer.
Issuer Organization Unit (OU)	The organizational unit name of the certificate issuer.

Name	Description
Issuer City or Locality (L)	The city or locality of the certificate issuer.
Issuer State or Province (ST)	The state or province of the certificate issuer.
Issuer Country (C)	The country of the certificate issuer.
Issuer Email Address	The email address of the certificate issuer.
Valid From	The date and time from which the certificate is valid.
Valid Till	The date and time until which the certificate is valid.
Issued to Common Name (CN)	The common name to which the certificate is issued.
Issued to Organization (O)	The organization name to which the certificate is issued.
Issued to Organization Unit (OU)	The organizational unit name to which the certificate is issued.
Issued to City or Locality (L)	The city or locality to which the certificate is issued.
Issued to State or Province (ST)	The state or province to which the certificate is issued.
Issued to Country (C)	The country to which the certificate is issued.
Issued to Email Address	The email address to which the certificate is issued.

What to do next

Use the displayed certificate information to verify the SSL certificate's details and validity.

Generating an SSL Certificate

This task describes how to generate a new self-signed SSL certificate. Generating an SSL certificate provides secure communication for the server web interface and other services.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **SSL Settings** > **Generate SSL Certificate**.

The **Generate SSL Certificate** page is displayed.

Step 3 Enter the required information for the new SSL certificate:

Table 63: SSL Certificate Generation Fields

Name	Description
Common Name (CN) field	Enter the fully qualified domain name (FQDN) or IP address of the server.
Organization (O) field	Enter the name of the organization.
Organization Unit (OU) field	Enter the name of the organizational unit.
City or Locality (L) field	Enter the city or locality.
State or Province (ST) field	Enter the state or province.
Country (C) field	Enter the two-letter country code.
Email Address field	Enter the email address for the certificate administrator.
Valid for field	Enter the number of days the certificate is valid.
Key Length drop-down list	Select the desired key length for the certificate.

Step 4 Click **Generate**.

The new SSL certificate is generated and installed on the server.

What to do next

Verify that the new SSL certificate is active by viewing its information.

Uploading an SSL Certificate

This task describes how to upload a new SSL certificate and its private key to the server. Uploading a custom SSL certificate allows for secure communication using a trusted certificate authority.

Before you begin

Ensure the new SSL certificate file and its corresponding private key file are available on a local system.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **SSL Settings** > **Upload SSL Certificate**.

The **Upload SSL Certificate** page is displayed.

Step 3 Review the **Current Certificate** and **Current Private Key** information.

These fields display details about the currently installed certificate and private key.

Step 4 To upload a new SSL certificate, click **Browse** next to the **New Certificate** field.

A file selection dialog is displayed. Navigate to and select the new SSL certificate file (.pem, .crt, or similar) from the local system.

Step 5 To upload a new private key, click **Browse** next to the **New Private Key** field.

A file selection dialog is displayed. Navigate to and select the private key file (.key, .pem, or similar) from the local system.

Step 6 Click **Upload**.

The new SSL certificate and private key are uploaded and installed on the server.

What to do next

Verify that the new SSL certificate is active by viewing its information and testing secure connections to the server.

Firewall Configuration

Configuring General Firewall Settings

This task describes how to configure general firewall settings, including adding new rules, modifying existing ones, and setting options to block or flush network traffic with time-based rules. Proper firewall configuration is essential for securing the server from unauthorized network access.

Before you begin

Understand the impact of firewall rules on network connectivity and server access.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **System Firewall** > **General Firewall Settings**.

The **General Firewall Settings** page is displayed.

Step 3 Perform one of the following actions:

- To add new general firewall settings, click **Add Firewall Settings**.
- To modify existing general firewall settings, click on the desired rule listed under **Existing Firewall Settings**.

The **Add Firewall Settings** page (for new rules) or the configuration page for the selected existing rule is displayed.

If no firewall settings exist, a message **No Firewall Settings Exists. To add a new Firewall settings goto Add Firewall Settings page.** is displayed under **Existing Firewall Settings**.

Step 4 Configure the general firewall settings:

Table 64: General Firewall Configuration Fields

Name	Description
Block All drop-down list	Select to block all incoming and outgoing network traffic for a specific IP version. Options include **IPv4**, **IPv6**, and **Both**.
Flush All check-box	Select to clear all existing firewall rules.
Timeout check-box	Select to enable a time-based duration for the firewall rule.
Start Date field	Enter the start date for the firewall rule (available when **Timeout** is selected).
Start Time field	Enter the start time for the firewall rule (available when **Timeout** is selected).
End Date field	Enter the end date for the firewall rule (available when **Timeout** is selected).
End Time field	Enter the end time for the firewall rule (available when **Timeout** is selected).

Step 5 Click **Save**.

The general firewall settings are applied.

What to do next

Verify that network access to the server is controlled according to the configured firewall rules.

Configuring IP Firewall Rules

This task describes how to configure IP firewall rules, which control network traffic based on IP addresses or IP address ranges. These rules enhance server security by restricting access from specified IP sources.

Before you begin

Understand the impact of IP-based firewall rules on network connectivity and server access.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **System Firewall** > **IP Address Firewall Rules**.

The **IP Address Firewall Rules** page is displayed.

Step 3 Perform one of the following actions:

- To add a new IP rule, click **Add New IP Rule**.
- To modify an existing IP rule, click on the desired rule listed under **Existing IP Rules**.

The **Add IP Rule** page (for new rules) or the configuration page for the selected existing rule is displayed.

If no IP rules exist, a message **No IP Rules Exists. To add a new IP Rules goto Add IP Rule page.** is displayed under **Existing IP Rules**.

Step 4 Configure the IP firewall rule settings:

Table 65: IP Firewall Rule Configuration Fields

Name	Description
IP Single (or) Range Start field	Enter a single IP address or the starting IP address of a range.
IP Range End field	Enter the ending IP address of a range (if configuring an IP range).
Enable Timeout check-box	Select to enable a time-based duration for the firewall rule.
Start Date field	Enter the start date for the firewall rule (available when **Enable Timeout** is selected).
Start Time field	Enter the start time for the firewall rule (available when **Enable Timeout** is selected).
End Date field	Enter the end date for the firewall rule (available when **Enable Timeout** is selected).
End Time field	Enter the end time for the firewall rule (available when **Enable Timeout** is selected).
Rule drop-down list	Select the action for the IP rule.

Step 5 Click **Save**.

The IP firewall rule is applied.

What to do next

Verify that network access from specified IP addresses is controlled according to the configured rules.

Configuring Port Firewall Rules

This task describes how to configure port firewall rules, which control network traffic based on port numbers and protocols. These rules enhance server security by restricting access to specific services.

Before you begin

Understand the impact of port-based firewall rules on network connectivity and server services.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **System Firewall** > **Port Firewall Rules**.

The **Port Firewall Rules** page is displayed.

Step 3 Perform one of the following actions:

- To add a new port rule, click **Add New Port Rule**.
- To modify an existing port rule, click on the desired rule listed under **Existing Port Rules**.

The **Add Port Rule** page (for new rules) or the configuration page for the selected existing rule is displayed.

If no port rules exist, a message **No Port Rules Exists. To add a new Port Rules goto Add Port Rule page.** is displayed under **Existing Port Rules**.

Step 4 Configure the port firewall rule settings:

Table 66: Port Firewall Rule Configuration Fields

Name	Description
Port Single (or) Range Start field	Enter a single port number or the starting port number of a range.
Port Range End field	Enter the ending port number of a range (if configuring a port range).
Protocol drop-down list	Select the network protocol for the rule.
Network Type drop-down list	Select the network type.
Enable Timeout check-box	Select to enable a time-based duration for the firewall rule.
Start Date field	Enter the start date for the firewall rule (available when **Enable Timeout** is selected).
Start Time field	Enter the start time for the firewall rule (available when **Enable Timeout** is selected).
End Date field	Enter the end date for the firewall rule (available when **Enable Timeout** is selected).
End Time field	Enter the end time for the firewall rule (available when **Enable Timeout** is selected).
Rule drop-down list	Select the action for the port rule.

Step 5 Click **Save**.

The port firewall rule is applied.

What to do next

Verify that network access to specific services is controlled according to the configured rules.

Secure Configuration Management

Backing Up or Restoring Key Upload

This task describes how to upload an AES key file to the server. This key is typically used for encrypting and decrypting configuration backup and restore files, ensuring the security of configuration data.

Before you begin

Ensure the AES key file for backup or restore operations is available on a local system.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Backup/Restore Key upload**.

The **Backup/Restore Key upload** page is displayed.

Step 3 In the **AES Key File** field, click **Browse**.

A file selection dialog appears.

Step 4 Navigate to and select the AES key file from the local system.

Step 5 Click **Upload**.

The selected AES key file is uploaded to the server.

What to do next

Proceed with backup or restore operations that require the uploaded AES key.

Restoring AES Key

This task describes how to upload an AES key file to the server for use during configuration restoration. This key ensures the secure decryption of backed-up configuration data.

Before you begin

Ensure the AES key file required for configuration restoration is available on a local system.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Backup/Restore Key upload**.

The **Backup/Restore Key upload** page is displayed.

Step 3 In the **AES Key File** field, click **Browse**.

A file selection dialog appears.

Step 4 Navigate to and select the AES key file from the local system.

Step 5 Click **Upload**.

The selected AES key file is uploaded to the server.

What to do next

Proceed with restoring the server configuration, which now uses the uploaded AES key for decryption.

Restoring Configuration with AES Key

This task describes how to restore a previously saved configuration to the server, especially when the backup file is encrypted and requires an AES key for decryption. Restoring a configuration applies a known good state to the server, which is useful for recovery from misconfigurations or system failures.

Before you begin

Ensure the backup configuration file is available on a local system.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Restore Configuration**.

The **Restore Configuration** page is displayed.

Step 3 If a message **AES Key does not exist. Click here to upload the Restore key** is displayed, perform the following substeps:

a) Click the **Click here to upload the Restore key** link.

A file selection dialog is displayed for the AES key.

b) Navigate to and select the AES key file from the local system.

c) Click **Upload**.

The AES key file is uploaded. The page returns to the **Restore Configuration** view.

Step 4 In the configuration file field, click **Browse**.

A file selection dialog is displayed.

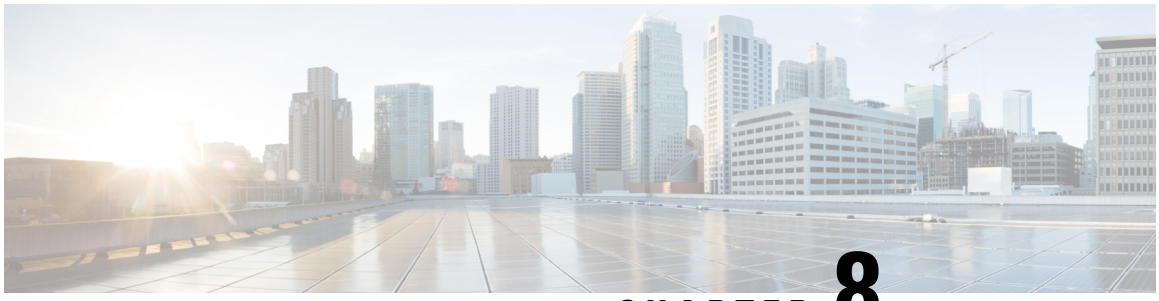
Step 5 Navigate to and select the backup configuration file from the local system.

Step 6 Click **Restore**.

The selected configuration file is uploaded and applied to the server. Server configuration settings are restored to the state saved in the backup file.

What to do next

Verify that the server is operating with the restored configuration settings.



CHAPTER 8

Managing Faults and Logs

- Log Overview and Configuration, on page 81
- Platform Event Filter Configuration, on page 83
- Viewing System Logs and Diagnostics, on page 88

Log Overview and Configuration

Understanding Logs and Reports

Logs and reports provide historical records of events, system activities, and diagnostic information. These records are essential for understanding server behavior, identifying the root cause of problems, tracking user actions, and fulfilling auditing requirements.

The **Logs & Reports** drop-down menu provides access to the following types of logs:

- **IPMI Event Log**—Records hardware-related events and alerts managed by the Intelligent Platform Management Interface (IPMI).
- **System Log**—Contains records of operating system events, application activities, and other general system-level messages.
- **Audit Log**—Tracks user actions, system changes, and security-related events for accountability and compliance.
- **Video Log**—May contain recordings or snapshots of server console output, useful for reviewing remote sessions.
- **POST Code**—Provides information related to Power-On Self-Test (POST) codes, indicating the server's status during startup.
- **Decoded Event Log**—Offers a more user-friendly, interpreted view of raw server event data.

Additionally, other diagnostic logs and reports, such as System Diagnostics Logs, BSOD captures, and Autonomous Crash Dumps, provide further insights into server operation and fault conditions.

Configuring SEL Log Settings Policy

This task describes how to configure the storage policy for the System Event Log (SEL). The SEL log policy determines how new log entries are handled when the log becomes full.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Log Settings**.

The **Log Settings** page is displayed.

Step 3 Under **SEL Log Settings Policy**, select the desired log policy:

Table 67: SEL Log Policy Options

Name	Description
Linear Storage Policy	When the SEL becomes full, new events are discarded. The log stops recording until entries are cleared.
Circular Storage Policy	When the SEL becomes full, new events overwrite the oldest entries. The log continues to record new events by rotating its storage.

Step 4 Click **Save**.

The SEL log settings policy is applied.

What to do next

Monitor SEL behavior to ensure log entries are handled according to the configured policy.

Configuring Advanced Log Settings

This task describes how to configure advanced settings for various system logs, including audit, system, local, and remote logs. Configuring these settings helps manage log retention, size, and remote delivery.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Advanced Log Settings**.

The **Advanced Log Settings** page is displayed.

Step 3 Under **Advanced Log Settings**, configure the following options:

Table 68: Advanced Log Settings

Name	Description
Enable Audit Log check-box	Select to enable logging of user actions and system changes for auditing purposes.
System Log check-box	Select to enable logging of general system events and messages.
Local Log check-box	Select to enable logging to a local storage location on the server.
Remote Log check-box	Select to enable logging to a remote syslog server. Additional fields for remote server configuration typically appear when this option is selected.
File Size field	Enter the maximum size for log files before rotation or archiving occurs.
Rotate Count field	Enter the number of log files to retain before old logs are overwritten or deleted.

Step 4 Click **Save**.

The advanced log settings are applied.

What to do next

Verify that log files are being generated and managed according to the configured settings.

Platform Event Filter Configuration

Understanding Platform Event Filters

Platform Event Filters (PEF) provide a mechanism to define conditions for various system events and specify automated actions or alerts when those conditions are met. This enables proactive monitoring and response to potential issues, enhancing server reliability and reducing manual intervention.

The **Platform Event Filter** section within **Settings** is organized into three main components:

- **Event Filters**—These define the specific criteria for an event, such as sensor readings, severity levels, and event data. When an event matches a configured filter, it triggers a specified action. Event filters can be enabled or disabled.
- **Alert Policies**—These define the actions to take when an event filter is triggered. Policies are grouped and specify whether to send an alert to a destination, and can include details like the LAN channel destination selector and custom alert strings.

- **LAN Destinations**—These define the network addresses and protocols for sending alerts generated by the alert policies. Destinations can be configured for various types, such as SNMP Traps or E-Mail, with specific server addresses, subjects, and messages.

Together, these components allow for a highly customizable and automated event management system, ensuring that administrators are promptly notified of critical system changes.

Configuring Event Filters

This task describes how to configure event filters, which define the specific criteria for system events that trigger alerts or actions. Event filters enable proactive monitoring and response to server conditions.

Before you begin

Ensure alert policies and LAN destinations are configured as required for event actions. See Configuring Alert Policies, on page 86 and Configuring LAN Destinations, on page 87.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Platform Event Filter** > **Event Filters**.

The **Event Filters** page is displayed, showing a list of existing event filters.

Radio buttons **All**, **Configured**, and **UnConfigured** allow filtering the displayed list of event filters.

Step 3 To configure an event filter, select an existing filter box or create a new one.

The **Event Filter Configuration** page is displayed.

Step 4 Configure the following event filter settings:

Table 69: Event Filter Configuration Fields

Name	Description
Enable this filter check-box	Select to enable or disable the event filter.
Event severity to trigger drop-down list	Select the severity level of the event that triggers this filter.
Event Filter Action Alert check-box	Select to enable an alert action when the filter is triggered.
Power Action drop-down list	Select a power action to perform when the filter is triggered.
Alert Policy Group Number drop-down list	Select the associated alert policy group to execute.
Raw Data check-box	Select to include raw data for the event filter.
Generator ID 1 field	Enter the first part of the generator ID.
Generator ID 2 field	Enter the second part of the generator ID.

Name	Description
Generator Type	Select the type of event generator: • **Slave** • **Software**
Slave Address/Software ID field	Enter the slave address or software ID.
Channel Number drop-down list	Select the channel number associated with the event.
IPMB Device LUN field	Enter the Logical Unit Number (LUN) for the IPMB device.
Sensor type drop-down list	Select the type of sensor associated with the event.
Sensor name drop-down list	Select the name of the sensor associated with the event.
Event Options drop-down list	Select event-specific options.
Event trigger field	Enter an event trigger.
Event Data 1 AND Mask field	Enter the AND mask for Event Data 1.
Event Data 1 Compare 1 field	Enter the first comparison value for Event Data 1.
Event Data 1 Compare 2 field	Enter the second comparison value for Event Data 1.
Event Data 2 AND Mask field	Enter the AND mask for Event Data 2.
Event Data 2 Compare 1 field	Enter the first comparison value for Event Data 2.
Event Data 2 Compare 2 field	Enter the second comparison value for Event Data 2.
Event Data 3 AND Mask field	Enter the AND mask for Event Data 3.
Event Data 3 Compare 1 field	Enter the first comparison value for Event Data 3.
Event Data 3 Compare 2 field	Enter the second comparison value for Event Data 3.
Delete button	Click to permanently remove the currently selected event filter.

Step 5 Click **Save**.

The event filter settings are applied.

What to do next

Verify that event filters trigger as expected and associated alert policies are executed.

Configuring Alert Policies

This task describes how to configure alert policies, which define the actions to take when an event filter is triggered. Alert policies specify how and where notifications are sent for system events.

Before you begin

Ensure LAN destinations for alerts are configured as required. See Configuring LAN Destinations, on page 87.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Platform Event Filter** > **Alert Policies**.

The **Alert Policies** page is displayed, showing a list of existing alert policy groups.

Step 3 To configure an alert policy, select an existing policy group or create a new one.

The **Alert Policies** configuration interface is displayed.

Step 4 Configure the following alert policy settings:

Table 70: Alert Policy Configuration Fields

Name	Description
Policy Group Number field	The identifier for the alert policy group.
Enable this alert check-box	Select to enable the alert policy.
Policy Action drop-down list	Select the action to perform when the policy is triggered.
LAN Channel Destination Selector drop-down list	Select the LAN channel destination to send the alert.
Event Specific Alert String check-box	Select to use an event-specific alert message.
Alert String Key field	Enter the key for the alert string.
Delete button	Click to permanently remove the currently selected alert policy group.

Step 5 Click **Save**.

The alert policy settings are applied.

What to do next

Verify that event filters trigger alerts according to the configured policies and are sent to the correct destinations.

Configuring LAN Destinations

This task describes how to configure LAN destinations for sending alerts and notifications. LAN destinations define the network addresses and protocols for delivering system event messages.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Platform Event Filter** > **LAN Destinations**.

The **LAN Destinations** page is displayed, showing a list of existing LAN destinations.

A **Select the LAN Channel** drop-down list is available to filter destinations by channel.

Step 3 To configure a LAN destination, select an existing destination box or create a new one.

The **LAN Destination** configuration interface is displayed.

Step 4 Configure the following LAN destination settings:

Table 71: LAN Destination Configuration Fields

Name	Description
LAN Channel field	The LAN channel identifier.
LAN Destination field	The identifier for the LAN destination.
Destination Type	Select the type of destination: • **SNMP Trap** • **E-Mail**
SNMP Trap Versions drop-down list	Select the SNMP Trap version.
SNMP Destination Address field	Enter the IP address or FQDN of the SNMP trap destination.
BMC Username field	Enter the BMC username for authentication with the destination.
Email Subject field	Enter the subject line for email notifications.
Email Message field	Enter the body of the email message for notifications.

Step 5 Click **Save**.

The LAN destination settings are applied.

What to do next

Verify that alerts are sent to the configured LAN destinations as expected.

Viewing System Logs and Diagnostics

Viewing IPMI Event Log

This task describes how to view the Intelligent Platform Management Interface (IPMI) event log. The IPMI event log records hardware-related events and alerts, which are crucial for diagnosing system hardware issues.

Procedure

Step 1 From the **Navigation Pane**, click **Logs and Reports** > **IPMI Event Log**.

Step 2 A **Sensor** drop-down list is available to filter the event log based on specific sensors.

Table 72: IPMI Event Log Entries

Name	Description
ID column	A unique identifier for each event log entry.
Record Type column	Indicates the type of record, categorizing the nature of the event.
Timestamp column	The date and time when the event occurred.
Generator ID column	Identifies the entity or component that generated the event.
Manufacture ID column	Identifies the manufacturer associated with the event or component.
Sensor Name column	The name of the sensor that reported the event.
Sensor Type column	The category or type of the sensor.
Sensor Num column	A numerical identifier for the specific sensor.
Event Dir column	Indicates the direction of the event, such as asserted or deasserted.
Data column	Raw data associated with the event, often in hexadecimal format.
Description column	A human-readable explanation or summary of the event.

Step 3 Perform one of the following actions:

- Click **Clear Event Logs** to remove all entries from the event log.
- Click **Download Event Logs** to download a copy of the event log entries as a ZIP file.

What to do next

Use the IPMI event log to diagnose hardware-related issues and monitor system health.

Viewing System Log

This task describes how to view the system log. The system log records operating system events, application activities, and other general messages, which are useful for monitoring server operations and troubleshooting software-related issues.

Procedure

Step 1 From the **Navigation Pane**, click **Logs and Reports** > **System Log**.

Step 2 Under **System Log**, you can review the following settings.

Table 73: System Log Entries

Name	Description
ID column	A unique identifier for each entry in the system log.
Timestamp column	The date and time when the system event occurred.
Source column	The source component or application that generated the log entry.
Message column	The detailed message of the system event.

What to do next

Use the system log to monitor server operations and troubleshoot software-related issues.

Managing Audit Log

This task describes how to manage the audit log, including viewing entries, clearing the log, and downloading log files. The audit log tracks user actions and system changes for security and compliance purposes.

Procedure

Step 1 From the **Navigation Pane**, click **Logs and Reports** > **Audit Log**.

Step 2 Under **Audit Log**, you can review the following settings.

Table 74: Audit Log Entries

Name	Description
ID column	A unique identifier for each entry in the audit log.
Timestamp column	The date and time when the audited event occurred.
Host column	Identifies the host or system where the audited event took place.
Description column	A detailed description of the audited event, including user actions or system changes.

Step 3 Perform one of the following actions:

- Click **Clear Audit Logs** to remove all entries from the audit log.
- Click **Download Audit Logs** to download a copy of the audit log entries as a ZIP file.

What to do next

Review downloaded audit logs for compliance or security analysis, or confirm that the log is cleared.

Viewing Video Log

This task describes how to view the video log. The video log contains recordings or snapshots of server console output, which is useful for reviewing remote sessions and troubleshooting.

Before you begin

Video recording functionality is enabled and configured, and video logs are generated.

Procedure

Step 1 From the **Navigation Pane**, click **Logs and Reports** > **Video Log**.

Step 2 Under **Video Log**, you can review the following settings.

Table 75: Video Log Entries

Name	Description
Timestamp column	The date and time when the video log entry was created.
Source column	The source of the video recording.
Duration column	The duration of the video recording.
Description column	A description of the video log entry.

Name	Description
Action column	Provides options to play, download, or delete the video log.

What to do next

Review video logs to analyze server console activities or troubleshoot issues.

Viewing POST Code

This task describes how to view Power-On Self-Test (POST) codes. POST codes indicate the status of the server during startup, which is useful for diagnosing boot-related issues.

Procedure

Step 1 From the **Navigation Pane**, click **Logs and Reports** > **POST Code**.

Step 2 Under **POST Code**, you can review the following settings.

Table 76: POST Code Entries

Name	Description
Timestamp column	The date and time when the POST code was generated.
Code column	The specific POST code value.
Description column	A description of the POST code, indicating the system's status at that point.

What to do next

Use POST codes to diagnose server startup issues.

Viewing Decoded Event Log

This task describes how to view the decoded event log. The decoded event log provides a more user-friendly interpretation of raw system event data, simplifying troubleshooting and event analysis.

Procedure

Step 1 From the **Navigation Pane**, click **Logs and Reports** > **Decoded Event Log**.

Step 2 Under **Decoded Event Log**, you can review the following settings.

Table 77: Decoded Event Log Entries

Name	Description
Event ID column	A unique identifier for the event.
Timestamp column	The date and time when the event occurred.
Severity column	The severity level of the event.
Message column	A human-readable message describing the event.
Resolution column	Suggested steps or information for resolving the event.

What to do next

Use the decoded event log for easier interpretation and analysis of system events.

Viewing System Diagnostic Logs

The **System Diagnostics** page allows generation and download of system diagnostic information and log files. This information is crucial for troubleshooting and monitoring server health.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Generate Log**.

The page displays a **Last Log File** section, which initially shows **No Log Found** if no logs have been generated recently.

The system begins generating the diagnostic log file. A progress bar and percentage display the generation status.

Step 3 After log generation is complete, click **Download Log**.

The diagnostic log file downloads in ZIP format to a local system.

What to do next

Analyze the downloaded log file for system diagnostic information.

Viewing Last BSOD Screen Captured

This task describes how to view information about the last captured Blue Screen of Death (BSOD) event. This feature assists in diagnosing system crashes and identifying potential causes.

Procedure

Step 1 From the **Navigation Pane**, click **Settings**.

Step 2 Click **Captured BSOD**.

The **Captured BSOD** page is displayed.

Step 3 Review the **Last BSOD Screen Captured** section.

If no BSOD event was captured, the message **BSOD Screen is not available.** is displayed.

If a BSOD event was captured, the captured image or details of the last BSOD event are displayed for analysis.

What to do next

Use the captured BSOD information for troubleshooting system stability issues.

Viewing Autonomous Crash Dump Logs

This task describes how to view Autonomous Crash Dump (ACD) logs. ACD logs contain diagnostic information captured automatically when the host operating system crashes, which is critical for root cause analysis.

Before you begin

An Autonomous Crash Dump event must have occurred and been captured by the system.

Procedure

Step 1 From the **Navigation Pane**, click **Host System Diagnostics**.

Step 2 Click **Autonomous Crash Dump**.

The **ACD Autonomous Crash Dump** page is displayed.

If no ACD data is found, the message **No Data Found** is displayed.

If ACD logs are available, a table is displayed with the following columns:

Table 78: Autonomous Crash Dump Log Entries

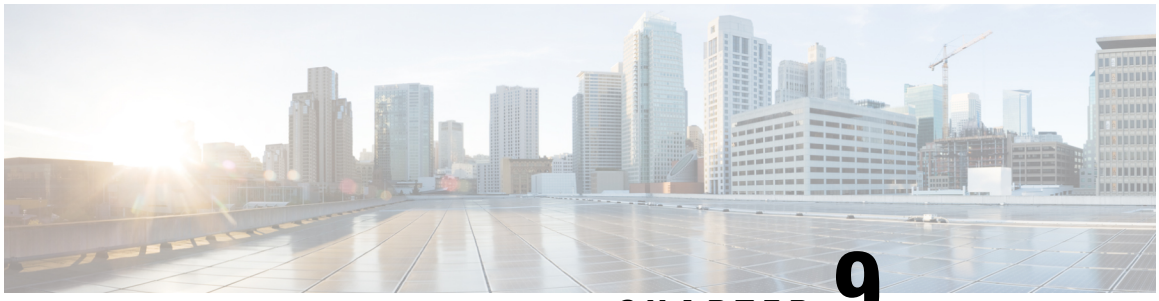
Name	Description
S. NO. column	The serial number of the log entry.
File Name column	The name of the crash dump file.
File Information column	Details about the crash dump file.

Step 3 Click **Download All Logs**.

All available Autonomous Crash Dump logs are downloaded to a local system.

What to do next

Analyze the downloaded crash dump logs for host operating system troubleshooting.



CHAPTER 9

Managing Server Firmware

- Understanding Firmware Inventory, on page 95
- Viewing Firmware Inventory, on page 95
- Updating Server Firmware, on page 96

Understanding Firmware Inventory

The firmware inventory provides a comprehensive list of the firmware versions currently installed on different components within the server. This information is essential for verifying system configurations, ensuring compatibility, and troubleshooting hardware-related issues.

The **Firmware Inventory** page is organized into tabs, typically including:

- **DGX** tab—Displays firmware information specific to DGX systems or related modules.
- **HGX** tab—Displays firmware information specific to HGX systems or related modules.

Each tab presents a table with the following columns:

Table 79: Firmware Inventory Details

Name	Description
Components column	Lists the names of various hardware or software components with installed firmware.
Version column	Displays the current firmware version installed on each listed component.

Viewing Firmware Inventory

This task describes how to view the firmware inventory of the server. The firmware inventory provides a list of installed firmware versions for various hardware components, which is useful for verification and troubleshooting.

Procedure

Step 1 From the **Navigation Pane**, click **Firmware Inventory**.

Step 2 Click the **Firmware Inventory** link in the left navigation pane.

The **Firmware Inventory** page is displayed, showing tabs for different system types.

Step 3 Select the desired tab **DGX** or **HGX**.

A table is displayed listing the firmware **Components** and their respective **Version**.

What to do next

Use the displayed firmware information to verify installed versions or identify components requiring updates.

Updating Server Firmware

This task describes how to update the server firmware. Updating firmware ensures the server operates with the latest features, performance enhancements, and security fixes.

Before you begin

Download the appropriate firmware bundle file to a local system.

Ensure the server is powered on for a successful firmware update.

Procedure

Step 1 From the **Navigation Pane**, click **Maintenance**.

Step 2 Click **Firmware Update**.

The **Firmware Update** page is displayed.

Notes regarding firmware update methods, supported components, and estimated completion time are displayed.

Step 3 Click **Browse** to select the firmware bundle.

A file selection dialog is displayed. Navigate to and select the firmware bundle file from the local system.

Step 4 Configure the following update options:

Table 80: Firmware Update Options

Name	Description
Force Update check-box	Select to force the firmware update, even if the version is the same or older.

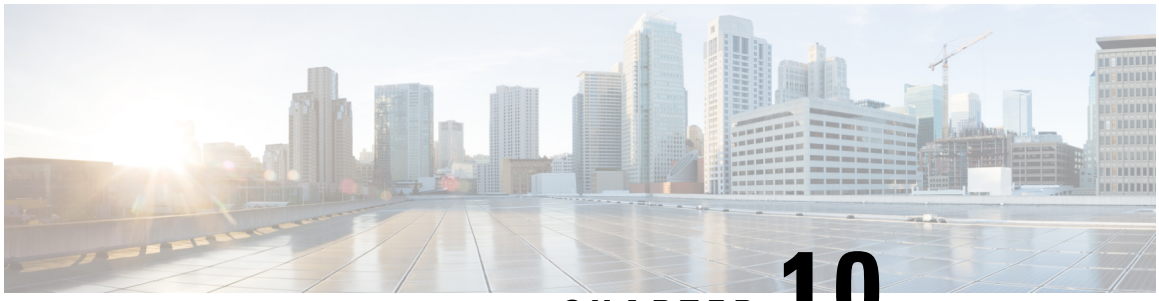
Name	Description
Restore BMC To Default check-box	Select to restore BMC settings to factory defaults after the firmware update.

Step 5 Click **Start Firmware update**.

The firmware update process begins. The server may restart multiple times during the update.

What to do next

After the update completes, an AC power cycle of the system is recommended. Verify the new firmware versions in the firmware inventory.



CHAPTER 10

Installing the Server OS

- OS Installation Methods, on page 99
- Remote KVM Console (H5Viewer), on page 99
- Installing an OS Using the KVM Console , on page 100

OS Installation Methods

Cisco UCS C880A M8 Rack Server supports several operating systems. Regardless of the OS being installed, you can install it on your server using one of the following tools:

- KVM console

For more information on Cisco UCS Server Configuration Utility, see Cisco UCS Server Configuration Utility Quick Start Guide.

Remote KVM Console (H5Viewer)

The **H5Viewer** KVM console is a web-based interface accessible from the Cisco BMC 4.0 GUI that emulates a direct keyboard, video, and mouse (KVM) connection to the server. This HTML5-based KVM console allows you to connect to the server from a remote location without the need for additional plugins.

Instead of using CD/DVD or floppy drives physically connected to the server, the KVM console uses virtual media, which are actual disk drives or disk image files that are mapped to virtual CD/DVD or floppy drives. You can map any of the following to a virtual drive:

- CD/DVD or floppy drive on a local computer
- Disk image files (ISO or IMG files) on a local computer
- USB flash drive on a local computer
- CD/DVD or floppy drive on the network
- Disk image files (ISO or IMG files) on the network
- USB flash drive on the network

The KVM console can be used to install an OS on the server.

Installing an OS Using the KVM Console

Before you begin

- Locate the OS installation image file.
- You must log in as a user with admin privileges to install an OS.

Procedure

Step 1 Load the OS installation disk into your CD/DVD drive, or copy the disk image files to your computer.

Step 2 From the **Navigation Pane**, click **Remote Control**.

Step 3 Under **H5Viewer**, click **Launch H5Viewer**.

KVM console is launched in separate browser window.

Note
You may need to disable pop up blocker.

Step 4 In the KVM console, from the top menu bar, click **Browse File**.

Step 5 Reboot the server and select the virtual CD/DVD drive as the boot device.

When the server reboots, it begins the installation process from the virtual CD/DVD drive. Refer to the installation guide for the OS being installed to guide you through the rest of the installation process.

What to do next

After the OS installation is complete, reset the LAN boot order to its original setting. Always follow your OS vendors recommended configuration, including software interoperability and driver compatibility. For more information on driver recommendations and installation, follow the Cisco UCS Hardware Compatibility.