BMC User Manual

Version 1.0, June 2026

www.moxa.com/products

BMC User Manual

The software described in this manual is furnished under a license agreement and may be used only in accordance with the terms of that agreement.

Copyright Notice

Trademarks

Disclaimer

- Information in this document is subject to change without notice and does not represent a commitment on the part of Moxa.
- Moxa provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Moxa reserves the right to make improvements and/or changes to this manual, or to the products and/or the programs described in this manual, at any time.
- Information provided in this manual is intended to be accurate and reliable. However, Moxa assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.
- This product might include unintentional technical or typographical errors. Changes are periodically made to the information herein to correct such errors, and these changes are incorporated into new editions of the publication.

Technical Support Contact Information

www.moxa.com/support

Table of Contents

1. Overview 4
2. Getting Started 5
Web UI Login 5
Forgot Password 7
3. Web Interface Configuration 8
Function Introduction 8
Dashboard 9
Logs 11
Event Logs 12
System Event Log 13
POST Code 15
Host Video Recorder 16
System Diagnostics 18
Hardware Status 19
System Information 19
CPU Information 20
DDR Information 20
Sensor Readings 21
PCIe Devices 22
NIC Information (BMC) 23
System Component 24
Operations 25
Factory Reset 25
KVM 27
Firmware 28
Reboot BMC 29
Virtual Front Panel 29
Virtual Media 30
Boot Configuration 31
Settings 32
Alerts 32
Alert Policies 36
Alert Email 38
Date and Time 39
Networks 40
VLAN 45
SNMP 45
iKVM and Virtual Media 46
Dynamic DNS 47
Syslog Settings 48
Backup Restore 51
Security and Access 52
Current Users 52
LDAP 53
User Management 54
Policies 57
Certificate Management 58
Security Settings 61
IP Access Control 63

1. Overview

Baseboard Management Controller (BMC) is a chipset used to independently monitor and control the DA-920E system.

You can access BMC using the following methods:

- IPMI command
- Redfish command
- Web-based UI

This manual covers the web-based user interface (web UI) for BMC.

Web UI Login

There are two ways to log in into the web UI for BMC.

Method A

Power on your DA-920E computer. When the OS is ready, open a browser, such as Google Chrome, Microsoft Edge, or Firefox on the DA-920E computer and connect to the following IP address:

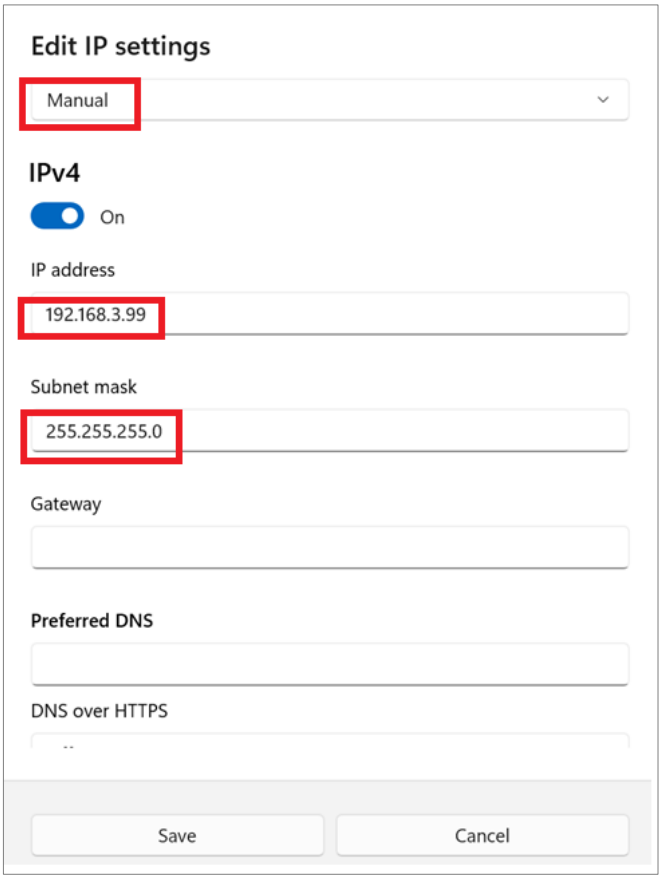
https://10.255.255.253

Method B

You can directly connect a Moxa DA-920E computer to your local computer with a standard network cable or install your computer on the same intranet as your computer. You will then need to manually configure your computer's network settings. The default IP address for a Moxa DA-920E BMC Management Web Interface is:

https://192.168.3.127

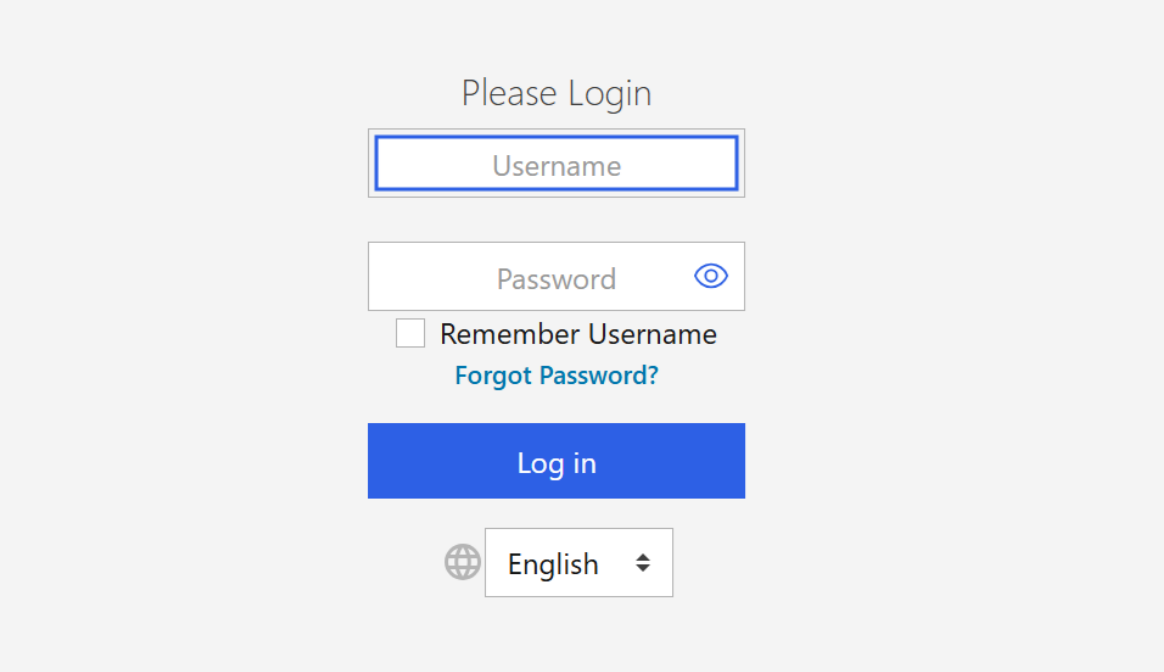
For example, you can configure the local computer's IP setting as **192.168.3.99**, and the subnet mask as **255.255.255.0**.



Click **Save** to save your network settings.

Open a browser, such as Google Chrome, Microsoft Edge, or Firefox, and connect to the following IP address:

https://192.168.3.127



NOTE

To enhance network security, all HTTP connections will be automatically redirected to HTTPS connections. In addition, when a web browser displays a warning message because a certificate has not been signed by a certification authority, you may add an exception rule for that certificate in the web browser or use a custom certificate to continue. To change the security settings, go to Security > Device Security > SSH & SSL > SSL.

The default username and password are:

Username: **moxa**

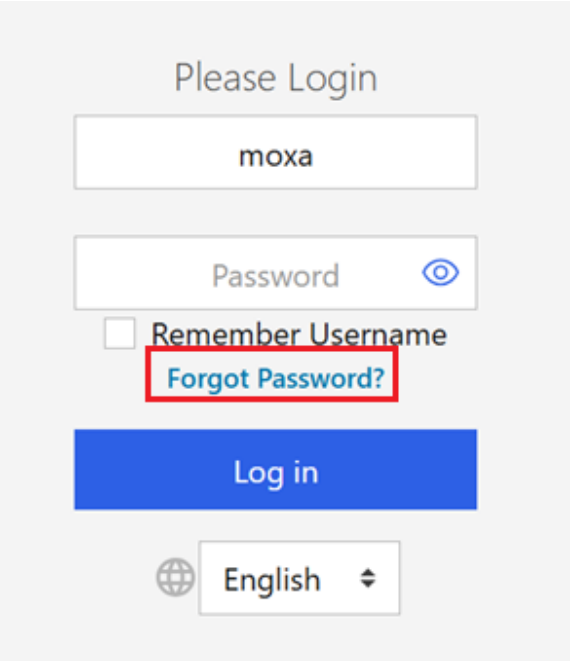
Password: **moxa**

NOTE

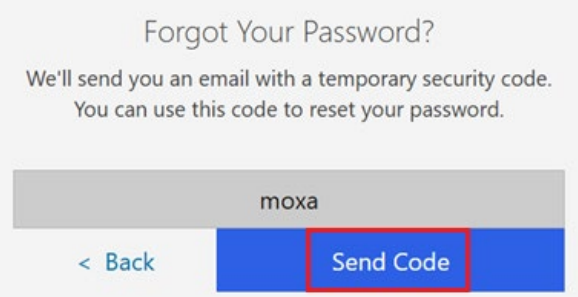
The current version supports English only.

Forgot Password

If you forgot your password, click **Forgot Password** to reset your password.



Click **Send Code**, a one-time code will be sent to your email address.



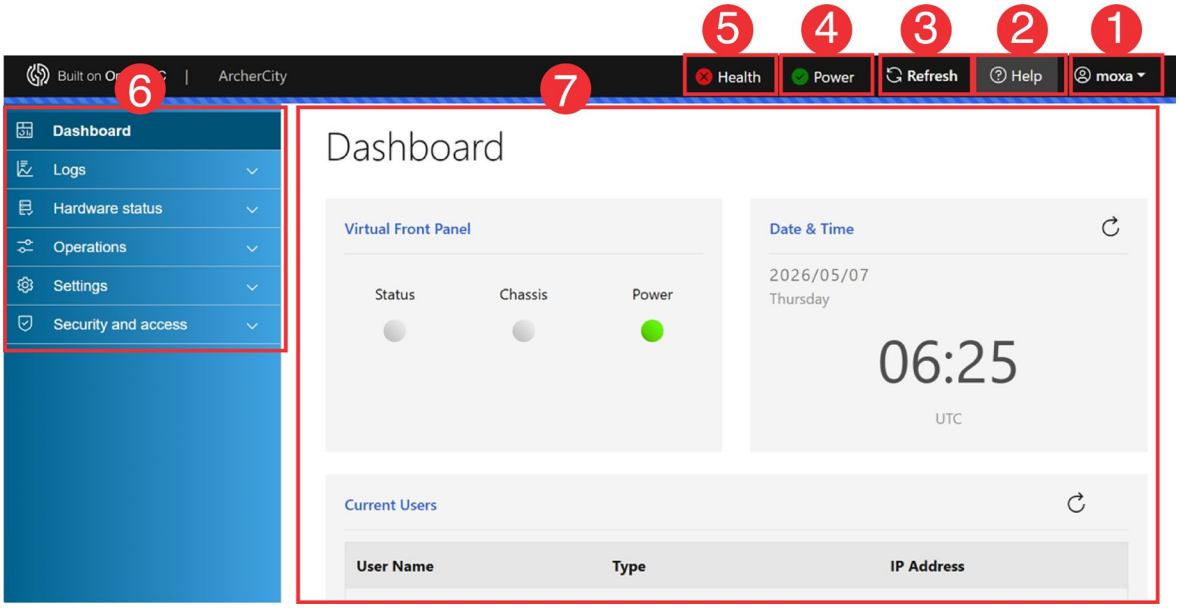
Enter the code, and reset your password.

3. Web Interface Configuration

Moxa's embedded computer offers a user-friendly web interface for easy configurations. Users find it simple to configure various settings over the web interface. All configurations for the Moxa's computers can be easily set up and done via this web interface, essentially reducing system maintenance and configuration effort.

Function Introduction

This section describes the web interface design, providing a basic visual concept for users to understand the main information or configuration menu for the web interface pages.



1. **Login Name:** It shows the name of the account that is logged in. You may also edit the user's profile settings or log out.
2. **Help:** It shows some information that helps you understand the interface of the BMC configurations.
3. **Refresh:** Click to refresh the page.
4. **Power:** It shows the current power status. Green means the power is on; red means the power is off.
5. **Health:** Click to display the BMC health status.
6. **Function Menu:** All functions of the computer are shown here. Click the function you want to view or configure.
7. **Information or Configuration Area:** All information or configuration settings will be shown here.

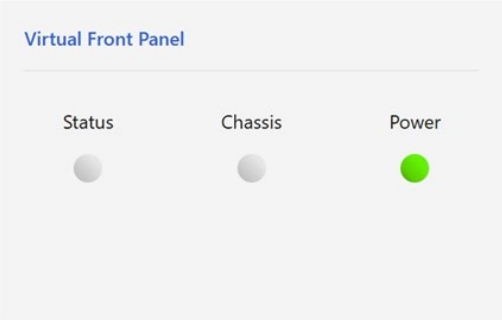
Dashboard

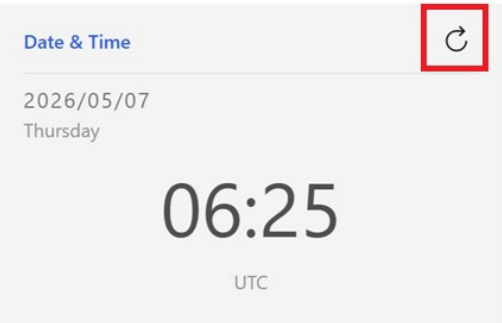
Dashboard shows all information about this computer.

Virtual Front Panel: Show. the status of the computer.

Date & Time: Shows the date and time of the computer.

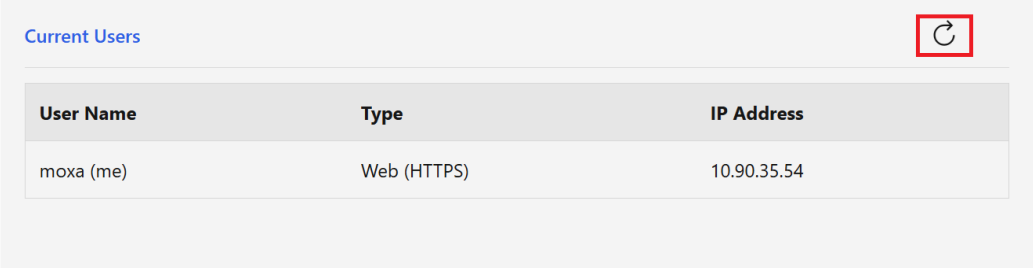
Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date status.





Current Users: Show the information of the users that have logged in to this computer.

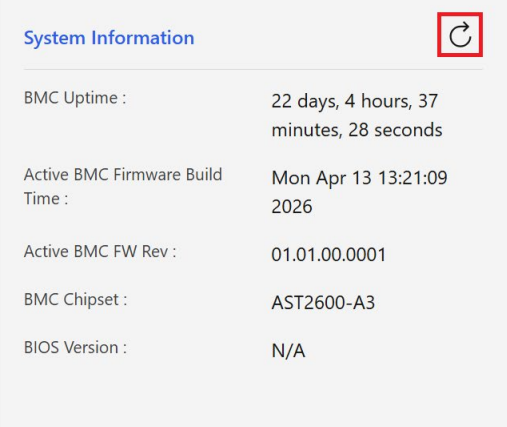
Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date logged in users.

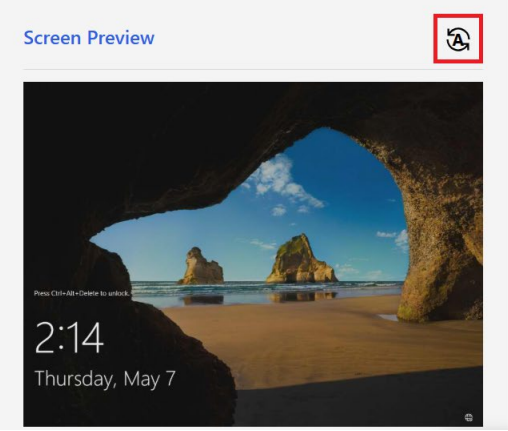


System Information: Shows all information about the computer.

Screen Preview: You may preview the screen of the computer.

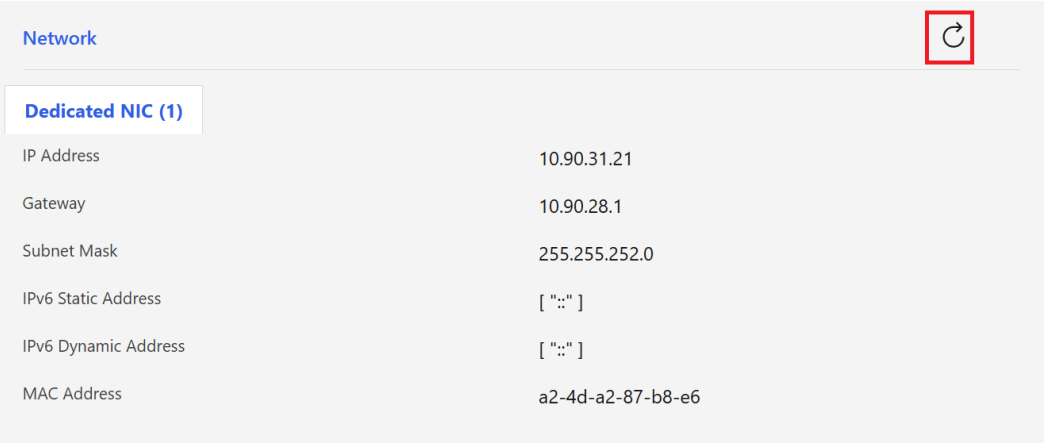
Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date information.





Network: Shows the current network status.

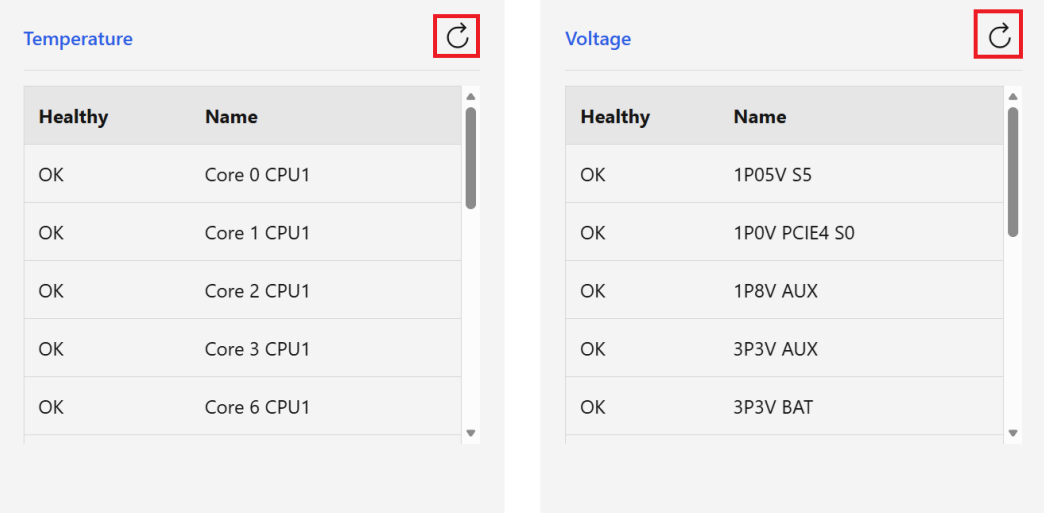
Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date network status.



Temperature: Shows the current temperature of the computer.

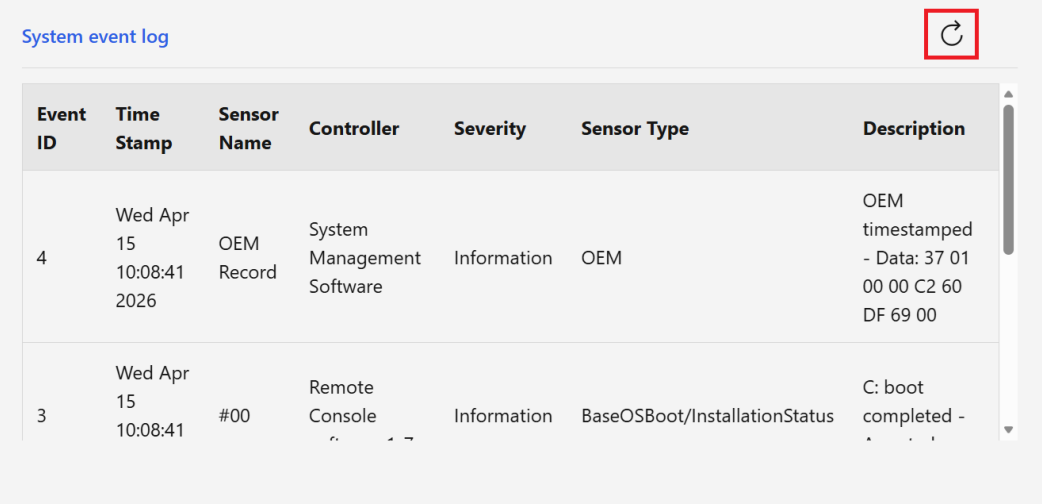
Voltage: Shows the current voltage of the computer.

Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date information.



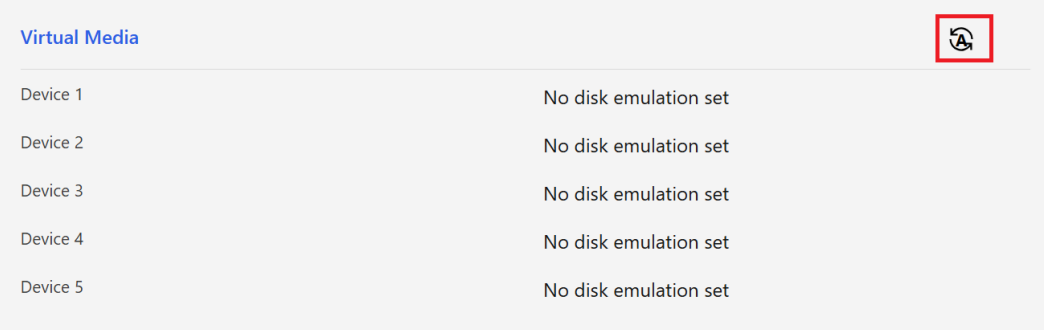
System event log: Shows all system event log information.

Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date information.



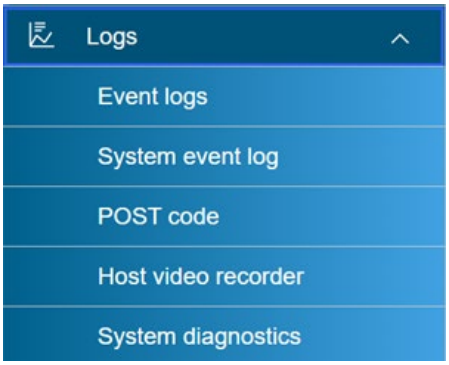
Virtual Media: Shows all virtual media information.

Click **Refresh** icon on the upper right corner to reload the page and check the up-to-date information.



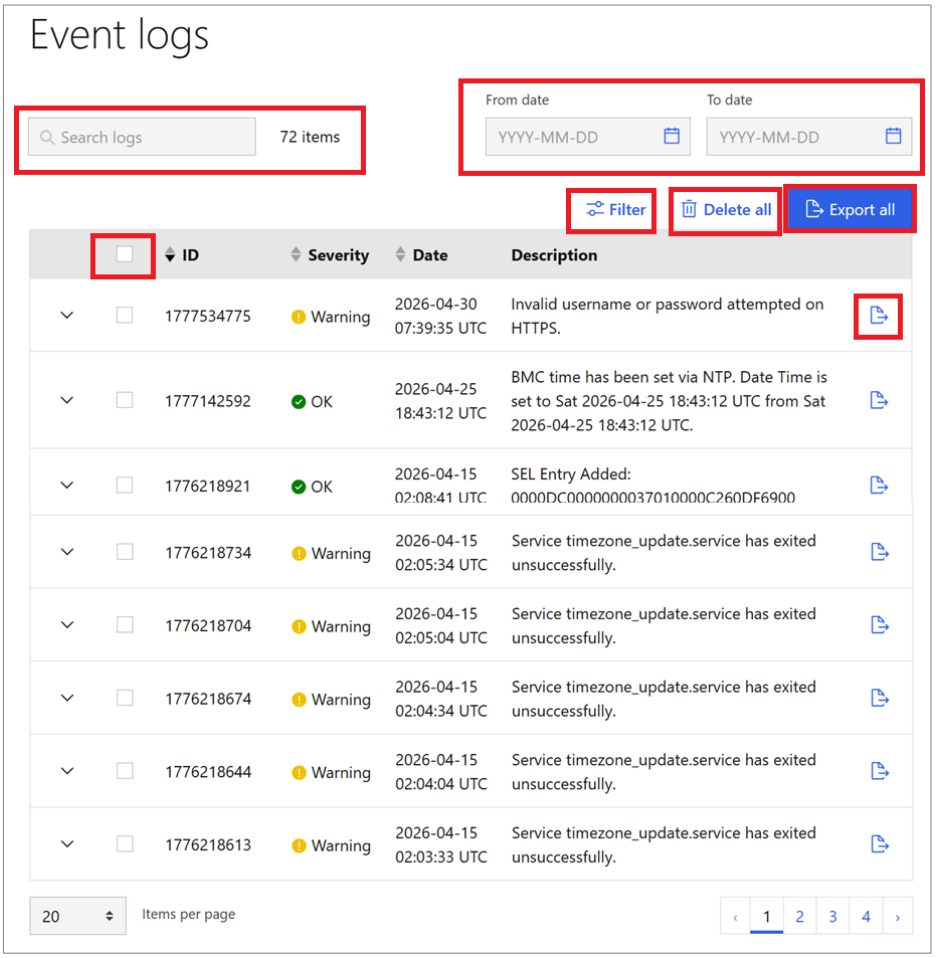
Logs

This section introduces the configurations for log functions, including **Event logs, System event log, POST code, Host video recorder,** and **System diagnostics**.



Event Logs

This page displays Event logs information. The event logs record various changes and critical events related to the server's hardware status, offering detailed insights for monitoring and troubleshooting. These logs assist system administrators in promptly identifying hardware issues, diagnosing failures, and enhancing the server's stability and reliability. They cover a range of events, including hardware status changes, system startups and shutdowns, sensor data, firmware updates, and error warnings, enabling administrators to efficiently track the server's performance and take appropriate actions.



You may perform the following functions:

1. Select a single or multiple event logs and click download icon to download the log information.
2. Search the event log name by Seach column, or search by time period. Click **Filter** to show the event logs you have searched.
3. Select a single or several event logs, click **Delete all** to delete the event logs you have selected.
4. Select a single or multiple event logs, click **Export all** to download the event logs to your local computer.

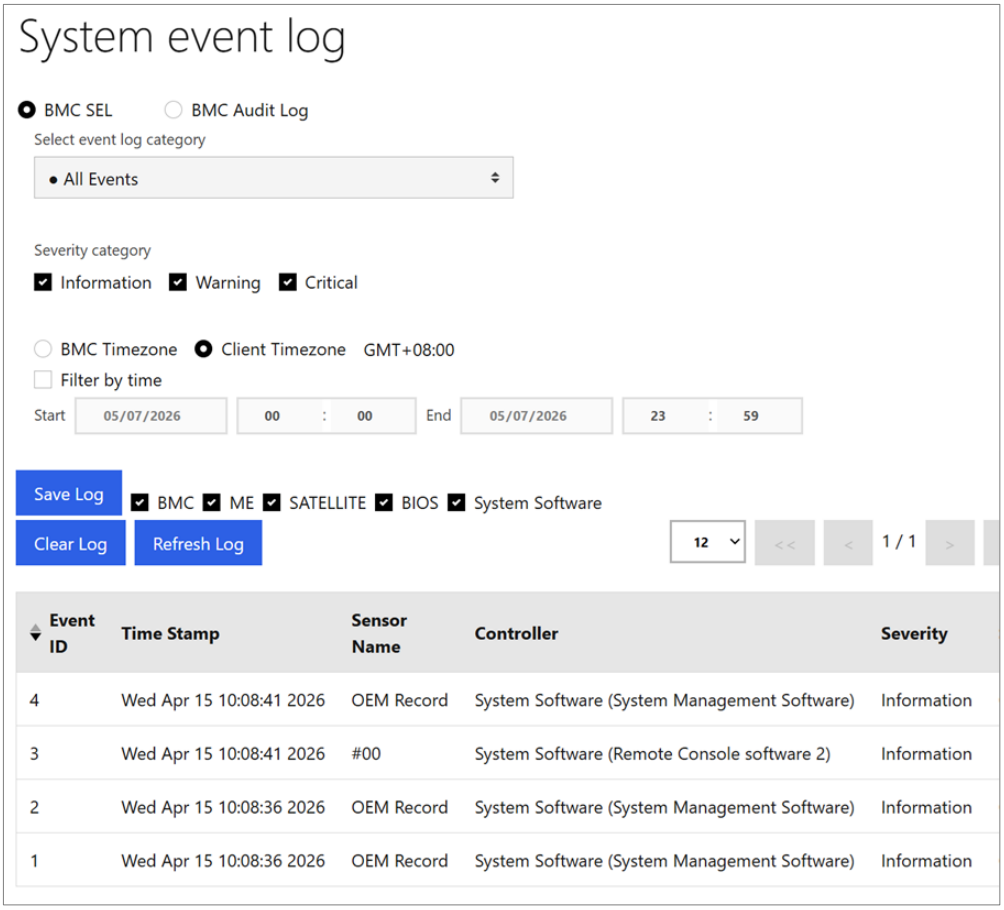
System Event Log

This page is used to display System event log (SEL) information.

The BMC system event log helps track and manage various events related to system hardware and administrative actions. It provides detailed logs for both hardware issues and user activities. There are two key types for viewing these logs:

BMC SEL: Displays logs of hardware-related events, such as power failures, temperature alerts, and hardware issues, typically used for diagnosing system problems.

BMC Audit Log: Displays logs of administrative actions on the BMC, including user logins, configuration changes, and system management activities, helping track security and compliance.



If you select **BMC SEL**, check the following configuration options.

Select event log category: Filter event log by selected categories.

- All Events
  - BMC Generated Events
  - ME Generated Events (Intel only)
  - SATELLITE Generated Events (AMD only)
  - BIOS Events
  - System Software Generated Events
    - SMI Handler Events
    - System Management Software Events
    - OEM Events
    - Remote Console Software Events
    - Terminal Mode Remote Console Software Events

Severity category: Filter event log by selected severity. Below are the available options.

- Information
- Warning
- Critical

BMC Timezone: Use BMC's time zone to display the time of the log.

Client Timezone: Use client's (user's) time zone to display the time of the log.

Filter by time: Allows users to view event logs that occurred within a specific time range, making it easier to analyze and troubleshoot events during that period.

Severity category: Severity category.

Filter by time: Allows users to view event logs that occurred within a specific time range, making it easier to analyze and troubleshoot events during that period.

Save Log: Select the event log source (BMC, ME (Intel only), SATELLITE (AMD only), BIOS, and system software) you want to download and click the download button. It then downloads the logs as a file named SELLOG.zip for further review and analysis.

Clear Log: Deletes all event logs. When clicked, a confirmation dialog will pop up, prompting the user to confirm the action before proceeding.

Refresh All Logs: Reloads the event logs, ensuring that the most up-to-date information is displayed.

 : The options typically appear in sorting settings, allowing you to choose how to arrange the data.
Ascending Order: Arranges items from the smallest to the largest. Descending Order: Arranges items from the largest to the smallest.

: The number of events displayed per page can be adjusted. For optimal performance, it is recommended to keep the record count per page to a minimum to reduce page load times.

Paging: Paging is a feature that divides large sets of data into separate pages, allowing users to navigate through them easily, improving performance and user experience by only loading a subset of the data at a time. For example, "1/50" means the user is currently on page 1 out of 50 pages.

<< (First Page): Navigates to the first page of the event logs.
< (Previous Page): Navigates to the previous page of event logs.
> (Next Page): Navigates to the next page of event logs.
>> (Last Page): Navigates to the last page of the event logs.

If you select **BMC Audit Log**, check the following configuration options.

Save: Click **Save** button, it then downloads the logs as a file named AuditLog.txt for further review and analysis.

Clear Log: Deletes all event logs. When clicked, a confirmation dialog will pop up, prompting the user to confirm the action before proceeding.

Refresh All Logs: Reloads the event logs, ensuring that the most up-to-date information is displayed.

 : The options typically appear in sorting settings, allowing you to choose how to arrange the data.
Ascending Order: Arranges items from the smallest to the largest. Descending Order: Arranges items from the largest to the smallest.

: The number of events displayed per page can be adjusted. For optimal performance, it is recommended to keep the record count per page to a minimum to reduce page load times.

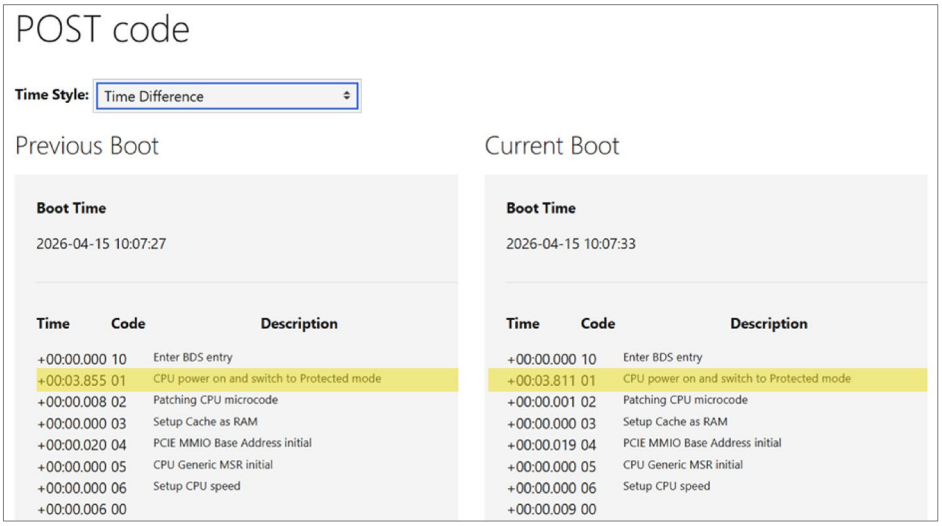
Paging: Paging is a feature that divides large sets of data into separate pages, allowing users to navigate through them easily, improving performance and user experience by only loading a subset of the data at a time. For example, "1/50" means the user is currently on page 1 out of 50 pages.

<< (First Page): Navigates to the first page of the event logs.
< (Previous Page): Navigates to the previous page of event logs.
> (Next Page): Navigates to the next page of event logs.
>> (Last Page): Navigates to the last page of the event logs.

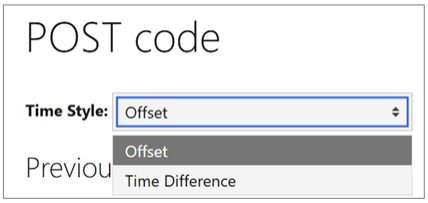
POST Code

This page provides an overview of recent Power-On Self-Test (POST) results, helping users monitor and analyze the host's boot progress. The page displays POST codes for both the previous boot and the current boot. The current boot codes will be moved to the previous boot section when the system is rebooted.

Move the mouse cursor over a record. The web page will automatically highlight other records in the logs with the same code, helping you to identify the specific status (code).



Two options can be selected: **Offset**, and **Time Difference**.

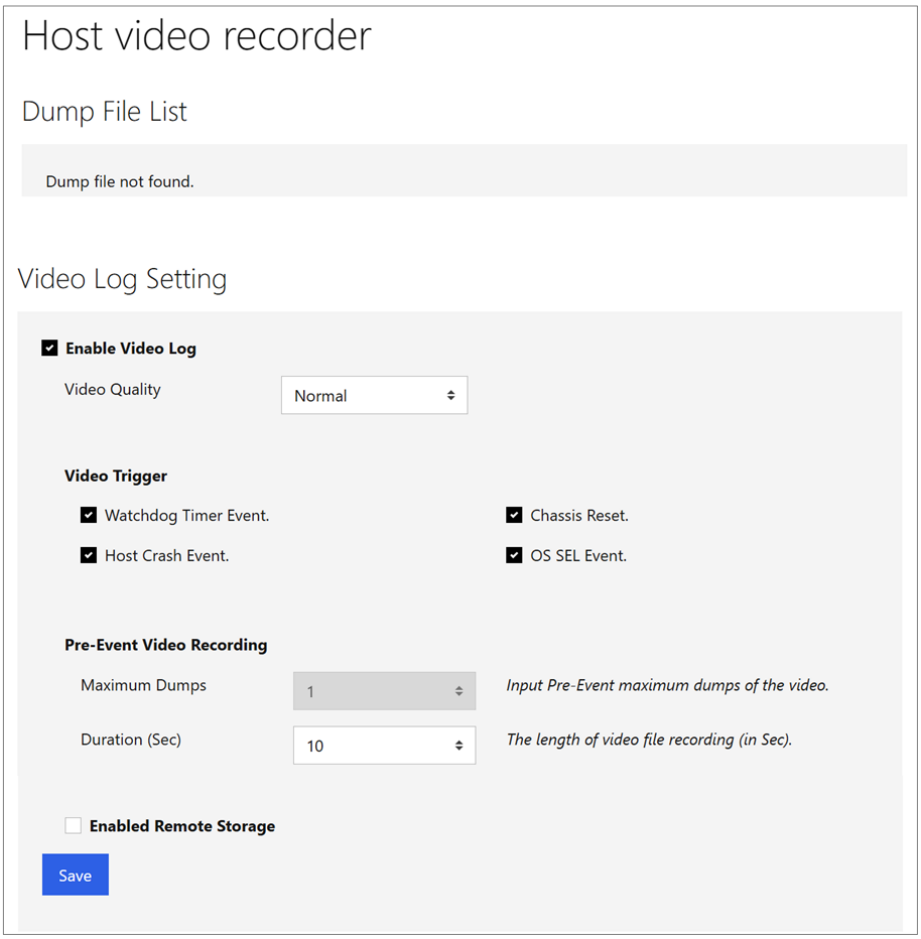


Offset: Shows the time offset from the boot time for each event.

Time Difference: Shows the time difference compared to the previous event.

Host Video Recorder

This page allows users to record and manage the video of the host's critical events. This feature aids in diagnosing issues and monitoring system health by providing a video record of key moments.



If there are dump files in Dump File List, click to download file to the local computer. Click to delete the video file from BMC.

Enable Video Log

Check to enable/disabled host video recorder feature. You need to enable it first to expand and configure the Video Log Setting section below.

Video Quality

Select the video quality as Low, High, and Normal from the Video Quality dropdown menu.

Video Trigger

This option is used to configure the events that will trigger auto video recording function. Event List shows the list of available events to be configured. The events include

Watchdog Timer Event: Triggers video recording when IPMI watchdog commands (such as Hard Reset, Power Down, and Power Cycle) are issued.

Chassis Reset: Triggers video recording when the chassis is reset.

Host Crash Event: Triggers video recording upon detecting a host crash.

> **NOTE**
>
> CATERR/IERR for Intel platform, CPER for Nvidia platform, and RAS error for AMD platform.

OS SEL Event: Triggers video recording when the operating system encounters a critical error (such as a Blue Screen of Death or Kernel Panic).

Pre-Event Video Recording

The Watchdog Timer Event, Chassis Reset Event, Host crash Event and OS SEL Event are called Pre-Event. The **VideoLog** service continuously captures images until an event is triggered, then generates an AVI file, preserving critical moments leading up to the event.

Maximum Dumps: Select the maximum number of event video dumps. If "Enable Remote Storage" is not checked, the default and only selectable option is 1. When "Enable Remote Storage" is checked, you can choose between 1, 2, or 3.

Pre-Event Video Recording - Duration (Sec): Select the duration in seconds (fixed at 10) from the drop-down list.

Notice: Due to considerations of limited BMC memory, currently only the 10-second option is supported.

Enable Remote Storage

Check to enable remote storage support.

NOTE

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

Refer to the following configuration options.

Server Address: Enter the Server Address. The IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx". 'xxx' ranges from 0 to 255. The first 'xxx' must not be 0.

Share Type: Select the Share Type (NFS or CIFS).

Path in server: Enter the path where the video files are stored in the Server field

User (optional): Enter the User account.

Password (optional): Enter the Password.

Save: Click to save the current settings made on the page.

System Diagnostics

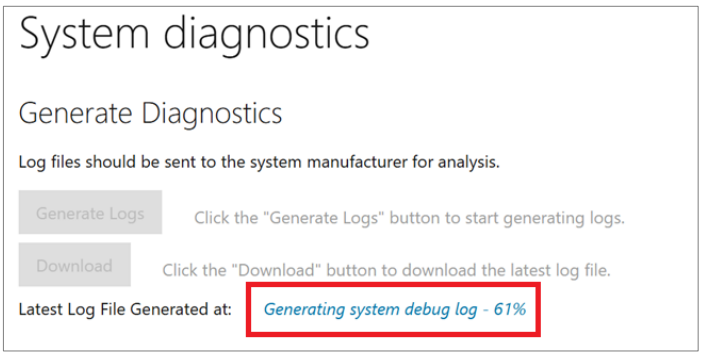
This page offers features designed to assist developers in analyzing and troubleshooting issues. These tools enable efficient debugging and ensure the system operates reliably.

This page includes various platform-specific sections, which may or may not be available depending on the platform. These sections include Intel Dump Log (ACD), RAS Support List, and other related features.

> **NOTE**
>
> Intel Dump Log (ACD) is only supported on Intel platforms. RAS Support List is only supported on the Intel BHS platform.

Generate Logs: Click this button to trigger BMC to collect the latest debug log data. It is recommended to always use Generate Logs to create fresh data for accurate analysis.

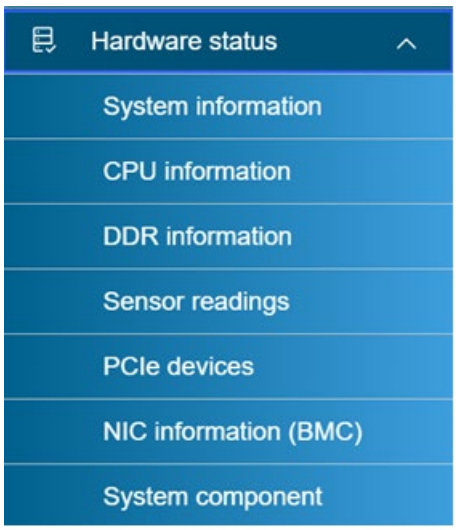
Download: Click this button to download the logs, which are compressed in a file of **tar.xz** format. If the button is greyed out, no log file is available for download. You must generate the log first.



You may check the log generation status.

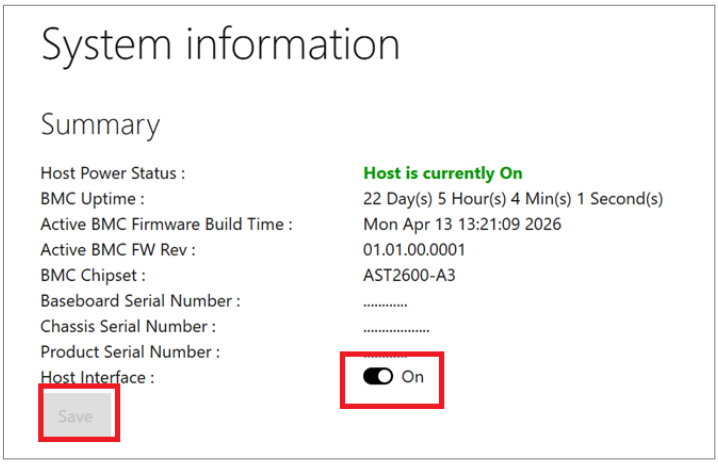
Hardware Status

This section introduces the hardware status, such as **System information, CPU information, DDR information, Sensor readings, PCIe devices, NIC information (BMC),** and **System component**.



System Information

This page shows all system information.



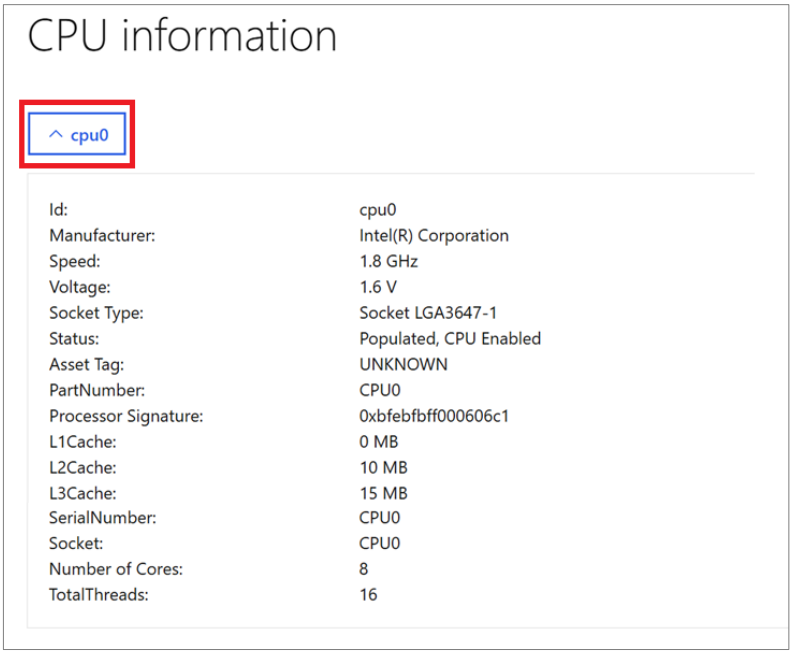
Two options can be configured:

Save: Click to save the settings.

Host Interface: Click to on/off RNDIS interface between BMC and BIOS.

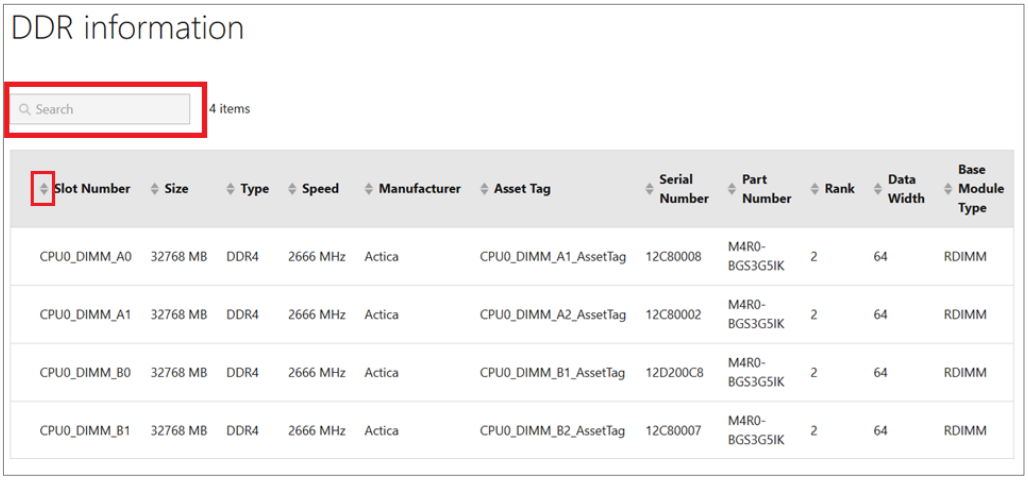
CPU Information

This page shows all CPU information. Select the CPU you want to check if there are multiple CPUs installed.



DDR Information

The page shows the DDR related information.



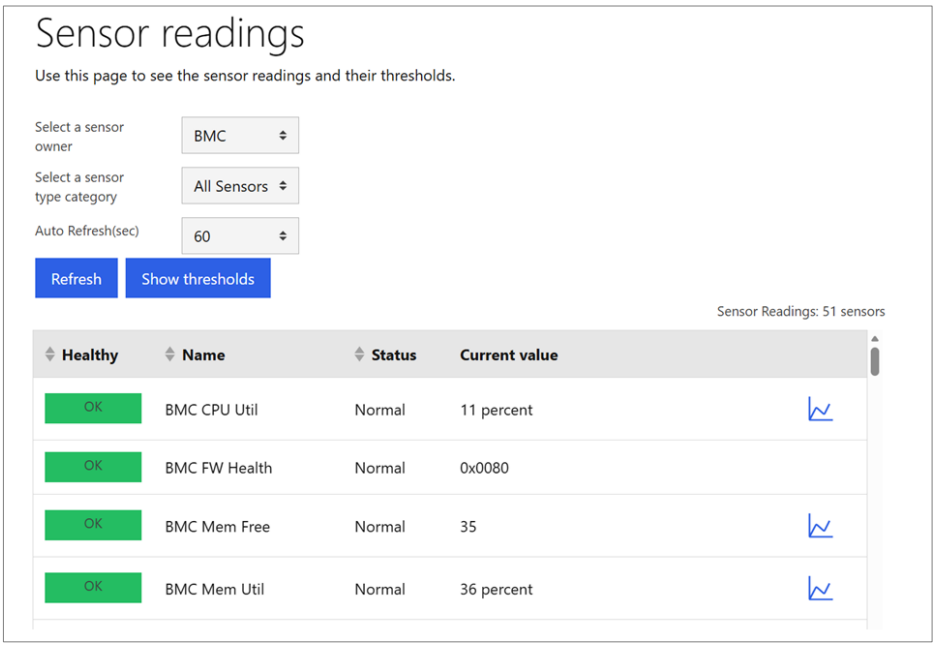
Two options can be used:

Search: Enter the keyword to find the specific data.

: Click this button for sorting settings. Both ascending order and descending order are available.

Sensor Readings

This page displays sensor readings information. The Sensor Readings page typically shows real-time data from server hardware sensors, which monitor and provide crucial information about the system's health. For instance, it can display parameters such as temperature, fan speed, voltage, and power, enabling system administrators to keep track of the server's hardware performance.



The following options are available for configuration.

Select a sensor owner: The default is BMC.

- BMC
- SATELLITE (Only supported on AMD platform)
- ME (Only supported on Intel platform)

Select a sensor type category: The default is to see all sensors. The values in this list will vary depending on the platform.

- All Sensors
- Management Subsystem Health
- System Event
- Event Logging Disabled
- Reserved
- Voltage
- Fan
- Current
- Other Units-based Sensor

Auto Refresh(sec): Automatically updates data at set time intervals (second).

- 5
- 10
- 15
- 30
- 60
- 150
- 300
- Never

Refresh: Updates the real-time data to show the latest information.

Show/Hide thresholds: Click this button to show/hide the threshold fields in the table.

- Lower NR
- Lower C
- Lower NC
- Upper NC
- Upper C
- Upper NR

: The options typically appear in sorting settings, allowing you to choose how to arrange the data.

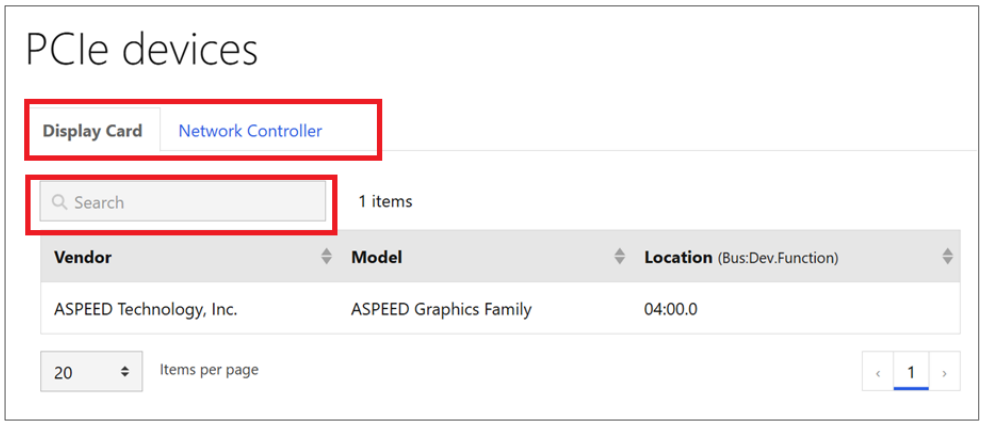
Ascending Order: Arranges items from the smallest to the largest.

Descending Order: Arranges items from the largest to the smallest.

: A sensor line chart displays sensor data trends over time. After clicking, the system will navigate to the chart page and display the data variations of the selected sensor at different time points, presented in a line chart format.

PCIe Devices

This page shows the information of the PCIe devices installed on the computer.



The following options can be used:

Display Card or **Network Controller:** Select to check the information of either the display card or network controller installed on the computer.

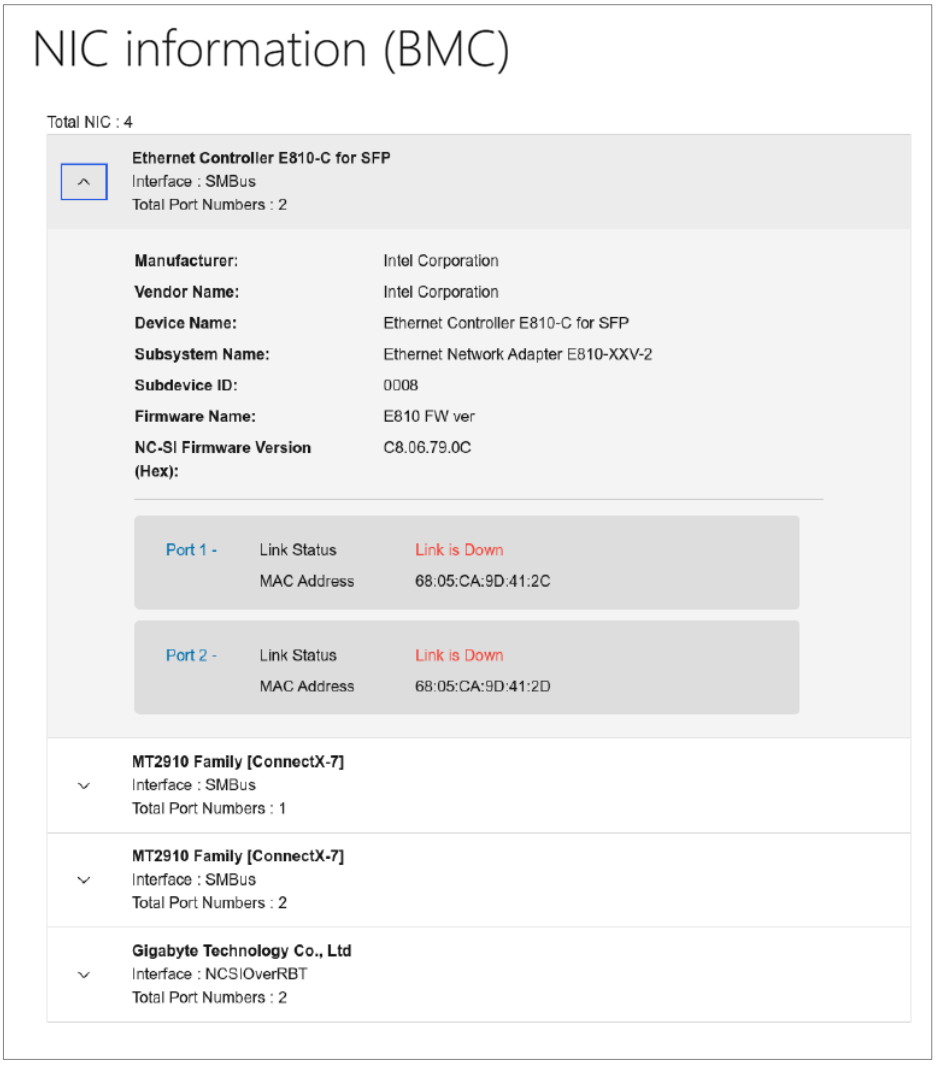
Search: Enter the keyword to find the specific data.

NIC Information (BMC)

NIC information consists of two parts: NIC Entry and Channel Entry.

Each NIC entry will display this NIC's ID, total channels, and device name. By clicking the NIC entry, it will display detailed Manufacturer, Vendor Name, Device Name, Subsystem Name, Subdevice ID, Firmware Name, NC-SI Firmware Version (Hex), and all of its channel entry. The detail manufacturer information and firmware version are from NC-SI Command Get Version ID.

Each channel entry will display this port's ID, link status(up/down) and MAC Address.



Click  icon to collapse the NIC information to hide the additional information.

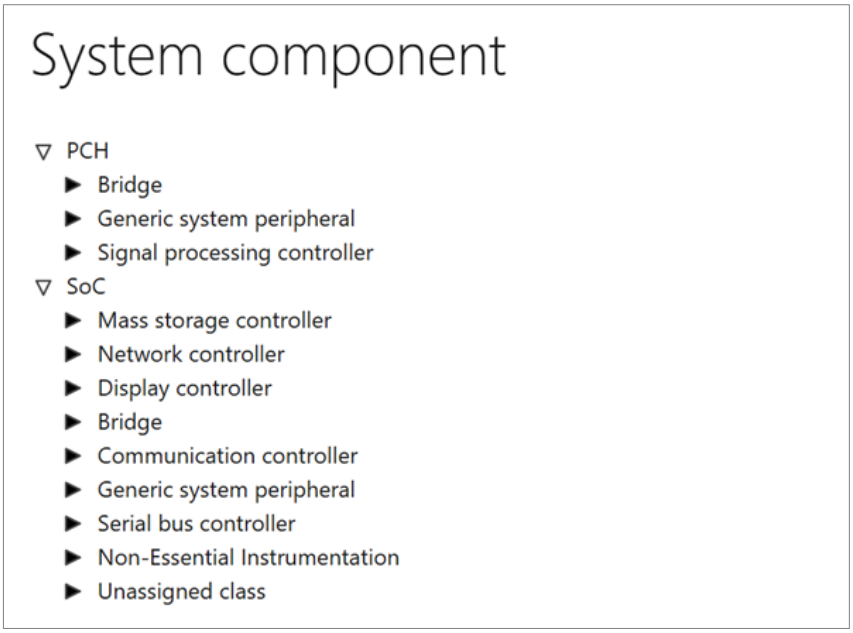
Click icon to expand the NIC information to show all information.

System Component

This page provides detailed information about the hardware components of the system, organized hierarchically for easy navigation.

NOTE

This page is related to Moxa BIOS Joint Features functionality. The content will only be displayed after the BIOS uploads the relevant data to the BMC via the host interface.



Two options can be used to view all information about system components.

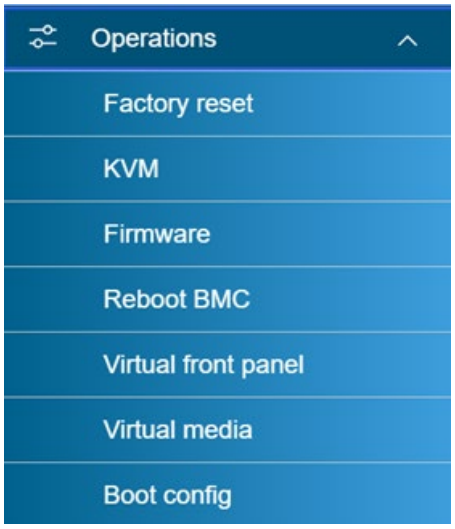
►: Indicates a category that can be expanded. Click to view its subcategories or details.

▽: Indicates that the category or section is currently expanded, displaying its detailed contents. Click again to collapse it, reverting to ►.

The tree view in the System Component interface displays hierarchical data in four distinct levels. Each level represents specific information about the system's PCIe devices and their associated details:

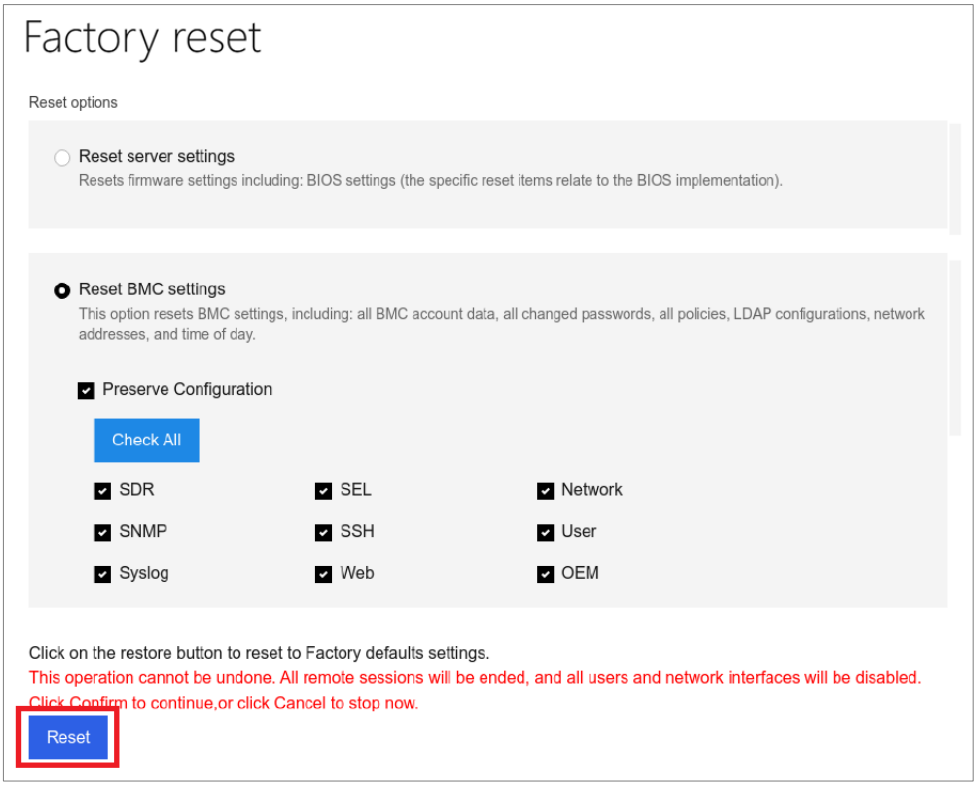
Operations

This section provides a series of functions for remote management and maintenance of servers, enabling efficient remote server administration.



Factory Reset

This page is used to display factory reset options. Click on the **Reset** button to reset factory settings. Offering various reset options.



Reset server settings

Reset BIOS settings (the specific reset items relate to the BIOS implementation). Does not affect BMC or network related configuration.

Reset BMC settings

Preserve Configuration: Select the settings to be preserved.

Check All: Click to select all options below. Click again to un-select all options.

Reset: Click the button to start the reset process. When clicked, a confirmation action dialog will pop up, click **Confirm** to continue, or click **Cancel** to abort.

The following options are available for configurations:

SDR: Preserve the Sensor Data Record (SDR) information.

SEL: Preserve system event log.

Network: Preserve network configuration file.

SNMP: Preserve SNMP configurations.

SSH: SSH RSA key, it will be re-generated if it's not preserved.

User: Preserve user configurations.

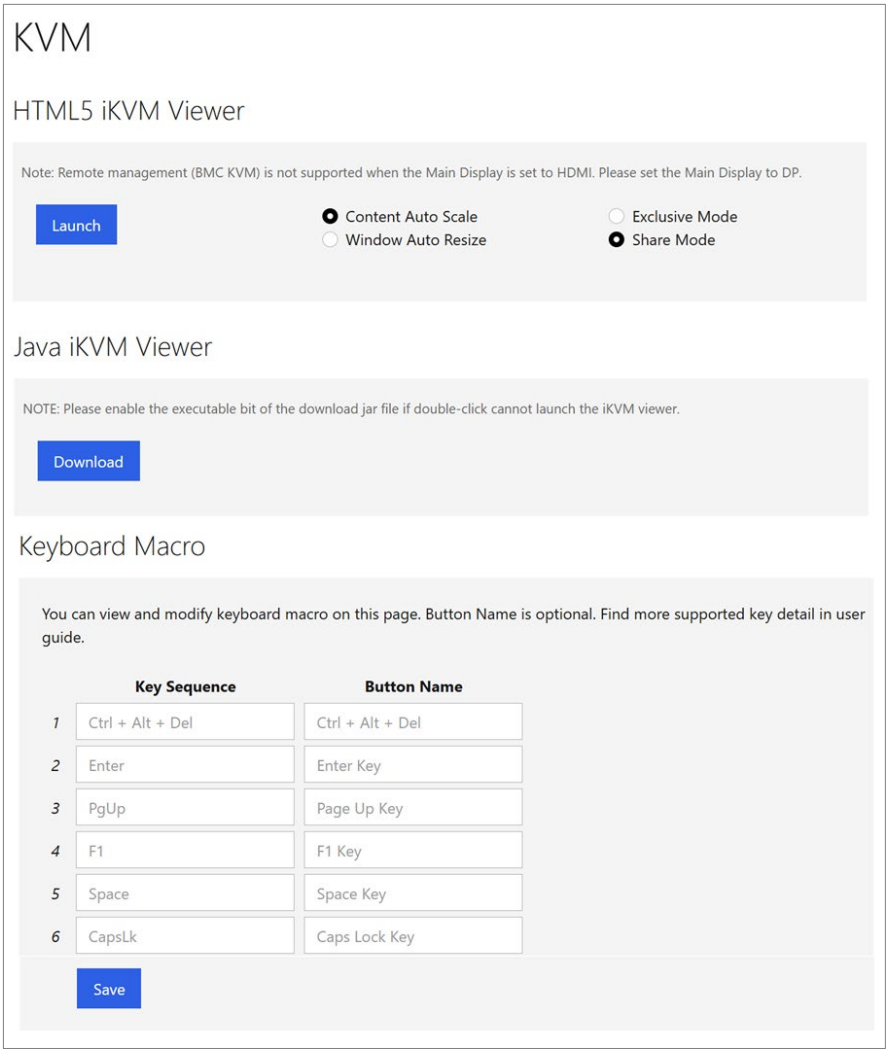
Syslog: Preserve syslog configuration.

Web: Preserve Web UI configuration.

OEM: Preserve files under folder /nv/oem and /nv/oemnv in BMC file system.

KVM

The KVM page provides three main features: two types of KVM viewers (HTML5 iKVM Viewer and Java iKVM Viewer) and the Keyboard Macro setting feature. KVM is used to redirect the client's Keyboard and Mouse inputs to the host system, while the Video is exported the host system display to client. These features enable efficient remote system management with flexible access and customizable keyboard macros.



HTML5 iKVM Viewer

A modern, browser-based remote management tool that requires no installation. It provides quick and easy access to remote systLaunch.

Click **Launch** button to launch the HTML5 iKVM Viewer.

Window scale

Select one of the two options: Content Auto Scale or Window Auto Resize. Content Auto Scale: If this function is enabled, the host content in the iKVM display area will automatically scale to match the window size, maintaining the aspect ratio and displaying the entire content within the window. Window Auto Resize: If this function is enabled, the iKVM window will automatically resize to show the full host display. When the window size is reduced, it will focus on a specific area of the host content, and only part of the host screen will be visible.

Session mode

Select one of the two options: **Exclusive Mode** or **Share Mode**. Exclusive Mode: If this function is enabled, the iKVM Server will only accept one connection, and others will be rejected. Shared Mode: If this function is enabled, the iKVM Server will allow multiple clients to connect simultaneously and share the desktop.ems, using HTML5 technology.

Java iKVM Viewer

A traditional remote management tool that requires downloading and running a Java-based JAR file. Click **Download** to download the file.

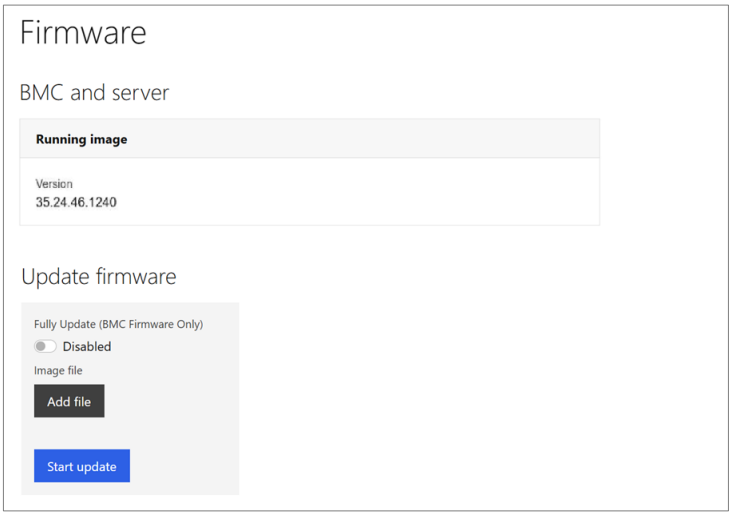
Keyboard Macro

Allows users to set up to 10 custom keyboard macros, enabling quick execution of predefined keyboard events within the viewer windows. Click **Save** to save the settings.

Firmware

The firmware page displays the firmware version and the process of firmware update.

You may check the current firmware version on this page.

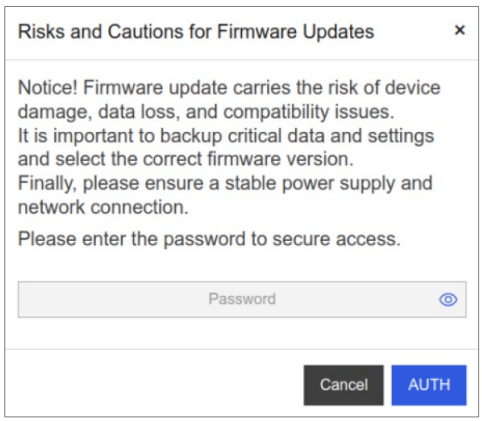


To update the firmware, follow the instructions below:

1. Click the button to **Enable**.
2. Click **Add file:** Choose to update the image source from the client-side disks.
3. **Start Update:** Start the update process and for more information. A warning screen will pop up to remind you of the risk of updating the firmware.

NOTE

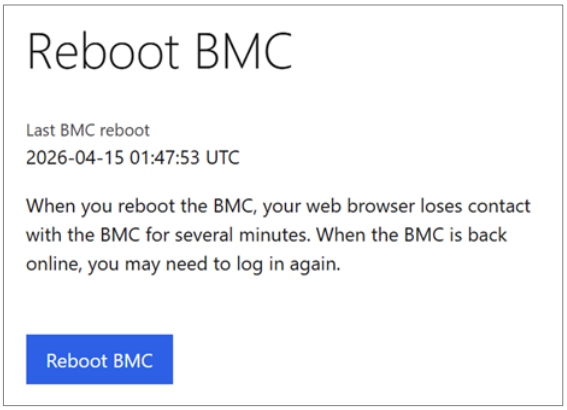
The factory reset is performed after the firmware update. This feature is only applicable to BMC firmware and cannot perform factory updates on other firmware images.



4. Enter the password and click **AUTH** to continue. Wait until the firmware update is complete.

Reboot BMC

This page provides users with the ability to restart the BMC. This feature is essential for troubleshooting and maintaining system stability when configuration changes or unexpected issues occur.

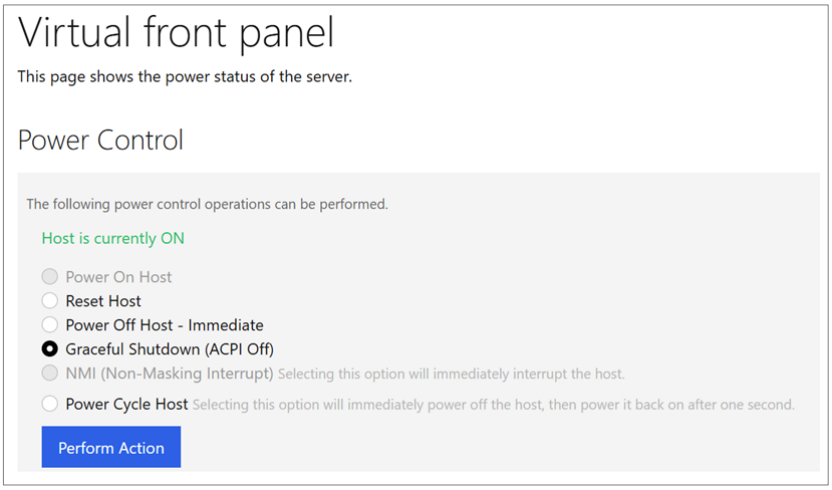


You may view the previous reboot information of the BMC

Click **Reboot BMC** to reboot the BMC.

Virtual Front Panel

This page provides users with remote control and monitoring capabilities for the server's power status. This interface replicates the functionality of a physical front panel, offering a convenient way to manage the server without requiring physical access.



Power Control

It enables users to perform various power operations on the server. The following options can be configured.

Power On Host: Powers on the host server if it is currently off.

Reset Host: Reboots the server by performing a soft reset.

Power Off Host - Immediate: Turns off the host server right away without following the normal shutdown process. This means all running applications and processes will stop abruptly, which could cause data loss or file corruption. Use this option only in emergencies or when an immediate shutdown is absolutely necessary.

Graceful Shutdown (ACPI Off): Initiates a proper shutdown using ACPI signals, allowing the server's operation system to close safely.

NMI (Non-Masking Interrupt): Triggers a non-maskable interrupt on the host, which is typically used for debugging purposes.

Power Cycle Host: Performs a hard power operation by forcibly powering off the host, cutting all power to the system. After a brief delay (typically one second), the host is automatically powered on. This operation is equivalent to physically unplugging and reconnecting the power cable, making it useful for clearing hardware states or recovering from unresponsive system conditions.

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

Virtual Media

This section demonstrates various methods for using Virtual Media, such as HTTPS, Samba, NFS, and HTML5, to share ISO images or folders from a client to a host. You may check the media that is currently mounted on BMC.

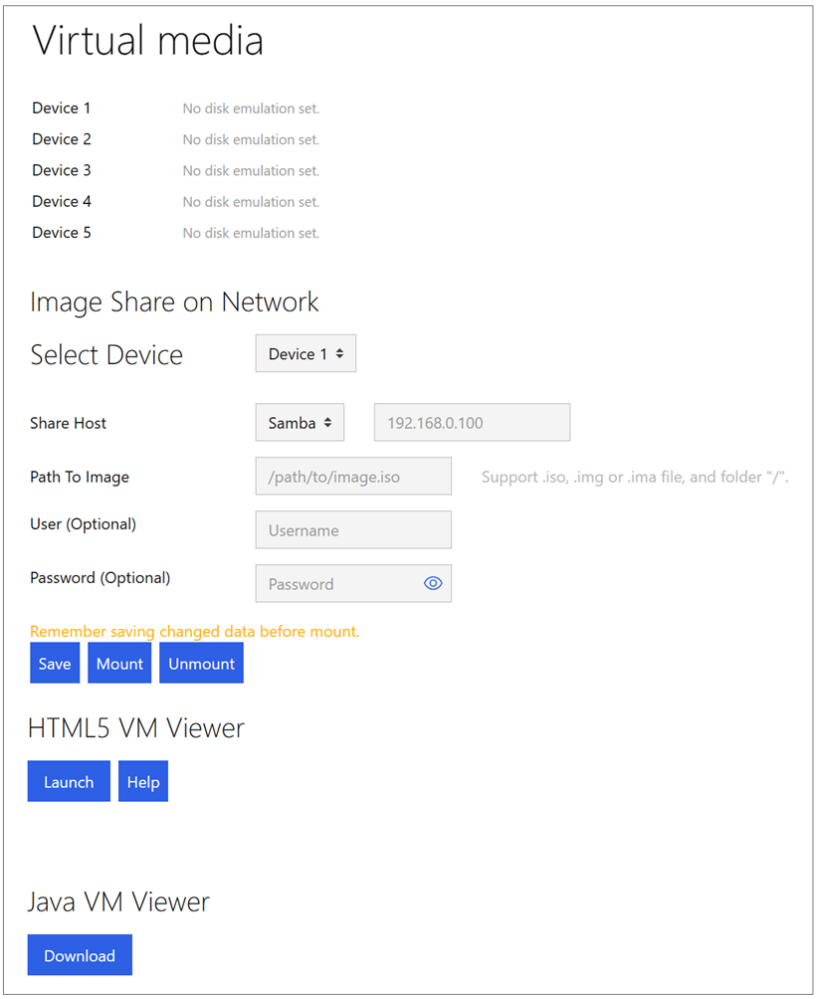


Image Share on Network

Following options can be selected and configured.

1. **Select Device** from the dropdown list.
2. **Select Share Host** from the dropdown list and enter IP address when necessary.
3. Assign **Path To Image**.
4. Click **Save** to save the setting; click **Mount** to mount the device; select **Unmount** to unmount the device.

HTML5 VM Viewer

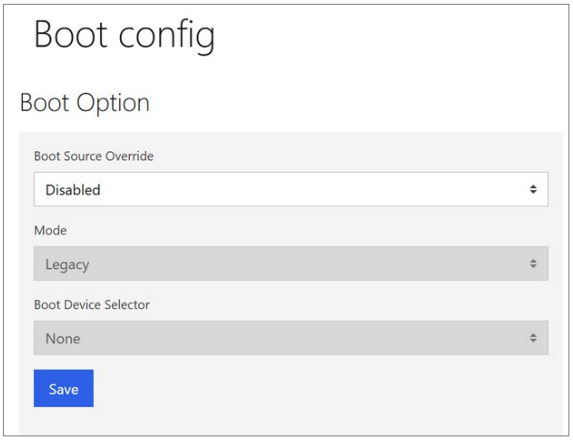
Click **Launch** to activate the HTML5 VM Viewer.

JAVA VM Viewer

Click **Download** to download the JAVA VM Viewer.

Boot Configuration

This page allows users to configure boot options and order for the system. I



Boot Option

Boot Source Override: Temporarily overrides the default boot source.

Options value:

- **Disabled:** No override; use the system's default boot source.
- **Once:** Override the boot source for the next boot only.
- **Continuous:** Continuously override the boot source for all subsequent boots until changed.

Mode

Select either **Legacy** or **UEFI** depending on your system requirements. Legacy for traditional BIOS-based booting and UEFI for modern firmware-based booting with advanced features.

Boot Device Selector

If **Legacy** mode is selected, the Boot Device Selector provides the following options:

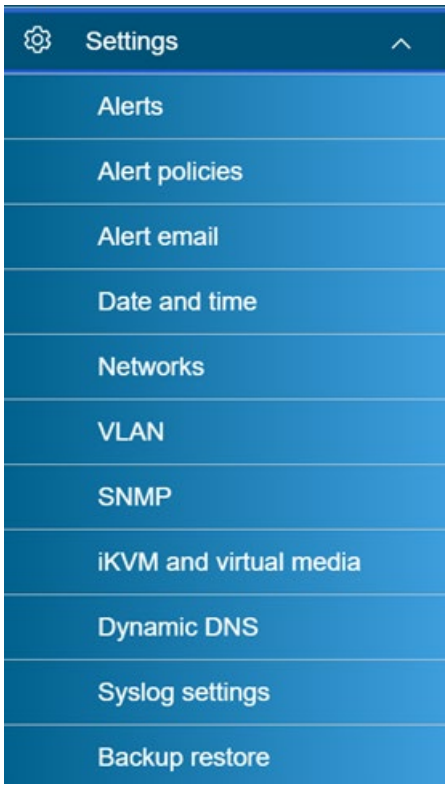
- **None:** No specific boot device override is set. The system follows the configured boot order.
- **PXE:** Boot over the network using the Preboot eXecution Environment (PXE). Useful for network-based OS deployments.
- **Hdd:** Boot from the primary hard disk drive.
- **Cd:** Boot from an optical drive containing a CD or DVD.
- **BiosSetup:** Boot directly into the system’s BIOS/UEFI setup interface.
- **USB:** Boot from a connected USB device. If UEFI mode is selected, the Boot Device Selector expands to include the following additional options:
- **None:** No specific boot device override is set. The system follows the configured boot order.
- **PXE:** Boot over the network using PXE. Supports UEFI-compatible network boot.
- **Hdd:** Boot from a UEFI-enabled hard disk drive.
- **Cd:** Boot from an optical drive containing a UEFI-compatible CD or DVD.
- **BiosSetup:** Boot into the system’s firmware interface (BIOS/UEFI setup).
- **USB:** Boot from a UEFI-enabled USB device.
- **UefiShell:** Launch the UEFI shell environment, providing tools for system management and diagnostics.
- **UefiBootNext:** Boot using the UEFI BootNext option, which allows specifying the next boot device dynamically without modifying the permanent boot order.
- **UefiTarget:** Boot from a specific UEFI boot target, typically configured in the system’s firmware.

Save

Save the current configuration settings. A toast notification will display the result of the save operation (success or failure). If the save is successful, a message box will appear reminding you to restart the host to apply the changes. It will also advise verifying that the system boots from the selected boot device and checking the device status if the boot fails.

Settings

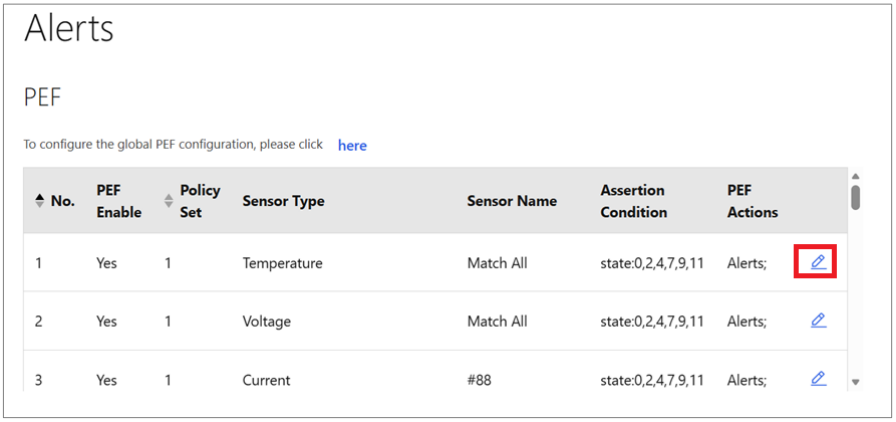
The Settings section contains various options related to system configuration and management. These settings allow you to adjust alert notifications, network configurations, remote management tools, log recording, and other functionalities according to your needs, thereby improving system management efficiency, enhancing system stability, and simplifying troubleshooting.



Alerts

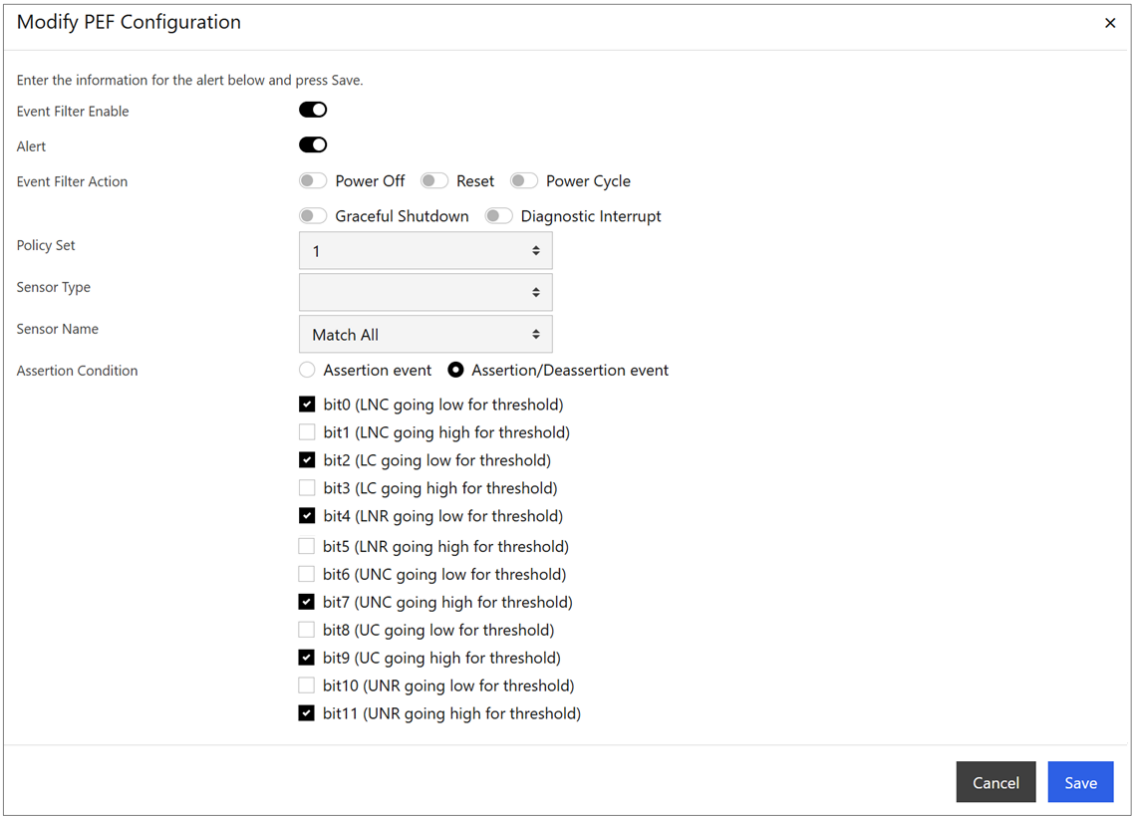
This option is used to configure which system events should trigger alerts and the destination for those alerts. Up to five destinations can be selected for each LAN channel lists the options to select the events that should trigger alerts and where the alerts are to be sent. Alerts page is comprised of three key components: PEF (Platform Event Filtering), SNMP Trap, and Alert Destination. These elements work in tandem to monitor system health and deliver alerts when issues arise.

The following page shows all global PEF configurations. Select the configuration icon on the item of Sensor Type you want to configure.



Modify PEF Configuration

The configuration page shows all available setting details.



The following options can be configured.

Event Filter Enable: If this option is set, each action triggered by a filter will generate an event log for the action.

PEF Actions: The PEF Actions that are about to be taken after the event filters have been matched.

- Alert
- Power Off
- Reset
- Power Cycle
- Graceful Shutdown
- Diagnostic Interrupt

Policy Set: Each policy set corresponds to alert policies specific group number, where different group numbers represent distinct configurations.

Sensor Type: Describes the category of the sensor (e.g., temperature, voltage)

Sensor Name: Specifies the exact component being monitored (e.g., "CPU1 Temperature", "PSU1 Fan Speed").

Assertion Condition: Defines the threshold or criteria that triggers an alert when a monitored value exceeds or falls below a specific limit.

- Assertion event
- Assertion/Deassertion event

Save: Save the current configuration settings.

Cancel: Allows the user to abort the current configuration settings.

SNMP Trap

This section shows how to configure SNMP Trap settings.

The following options can be configured.

LAN Channel: Displays the currently active channel. Select the LAN channel to configure from the dropdown menu.

SNMP Trap: Provide v1/v2c/v3 protocol option to set.

Community String: Used only by devices which support SNMPv1 and SNMPv2c protocol. SNMPv3 uses username/password authentication, along with an encryption key.

User Name: Specifies the identifier used for user authentication and access control.

Authentication Protocol: The Authentication Protocol for SNMPv3 Trap.

- MD5
- SHA-96
- SHA-224
- SHA-256
- SHA-384
- SHA-512

Authentication Passphrase: Secret key is used to authenticate the user and ensure secure communication.

Security Level: Defines the level of security applied.

- authNoPriv
- authPriv

When you select **authPriv**, the system will display additional options to configure the **Privacy protocol** and **Privacy Passphrase**, which will enhance the security of the communication.

Privacy Protocol: Specifies the encryption protocol used to secure the data.

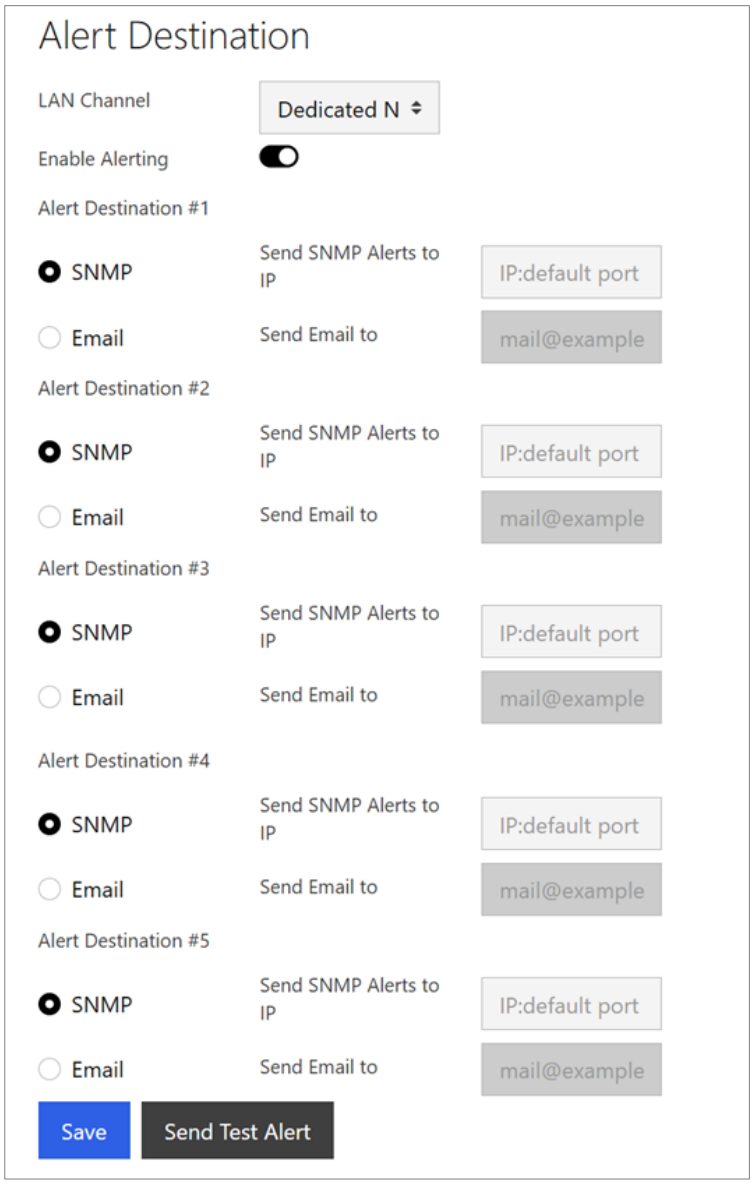
- AES

Privacy Passphrase: A secret key used with the privacy protocol to encrypt and decrypt the data.

Save: Save the current configuration settings.

Alert Destination

- Alert Destination defines where the alerts are sent, such as email, SNMP management systems. BMC allows multiple destinations to be configured, with up to five per LAN channel, ensuring alerts are directed to the appropriate recipients.



- When selected **SNMP**, refer to the following configuration options.

LAN Channel: Displays the currently active channel. Select the LAN channel to configure from the dropdown menu.

- Dedicated NIC
- Share NIC

Enable Alerting: Enables or disables the sending of alerts to the specified destination when certain conditions or events occur.

Alert Destination #1~5: Can be one of two types.

- SNMP (IP address:162) 162 is SNMP trap default port.
- Email (mail@example.com)

Save: Save the current configuration settings.

Send Test Alert: After configuring, select this to send a test alert.

You can use packet analysis tools such as Wireshark in target PC, then Click **Send Test Alert** button, Wireshark will receive a SNMP packet.

When selected **Email**, simply enter an email address. For example, enter testBMC@moxa.com as the target email address.

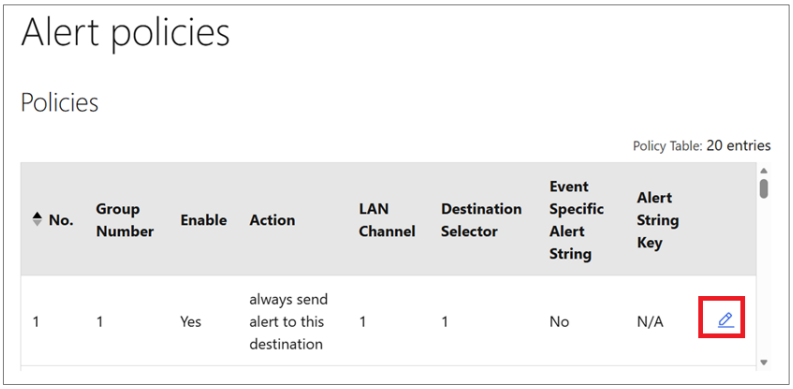
Click **Save** to save the setting and click **Send Test Alert** button, and an alert email will be received in the target mailbox.

Alert Policies

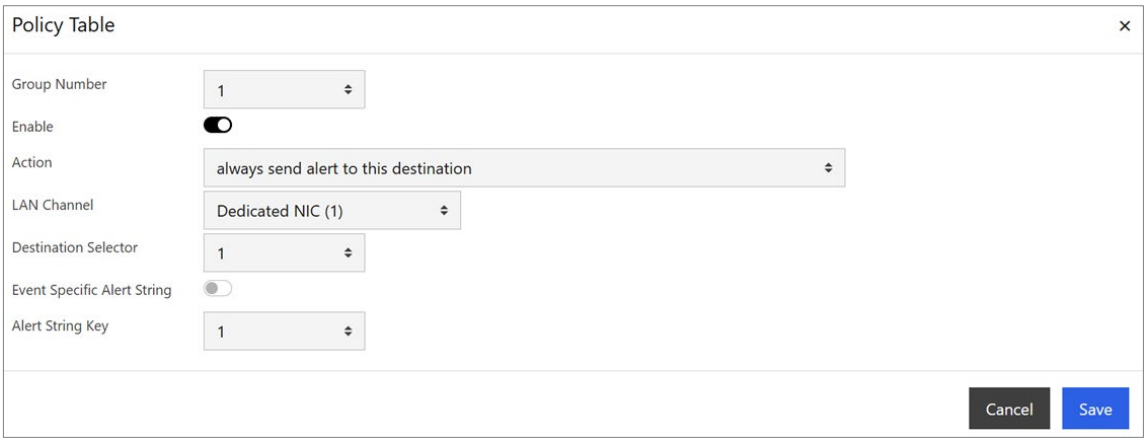
This page is used to display Alert policies related information.

When an alert is triggered via PEF, the alerting process is managed by an alert policy, which consists of one or more alert destinations. These destinations can include various types and channels, processed sequentially. The use of each destination can be configured based on the success or failure of the previous alert.

The Policies data is stored in the Alert Policy Table, a part of the PEF configuration parameters. The system supports multiple policies, each identified by a unique policy number, which is referenced in the Event Filter Entry to determine which policy to apply when a match occurs. The Alert String Key is used to associate an alert with predefined conditions, event filters, or alert policies. It allows the system to recognize the nature of the event, what triggered it, and how it should be handled. Typically, the alert string key follows a specific format to ensure it is distinct and easily identifiable, enabling administrators to quickly diagnose and respond to issues.



Click **Edit** icon, the following page will be displayed.



Refer to the following configuration options.

No.: A unique identifier.

Group Number: The identifier for the group to which the alert policy belongs. Each Group number corresponds to PEF specific policy set number. The Group Number fixed limit of 15.

Enable: A setting that indicates whether the alert policy is active (Yes) or not.

Action: The action to be taken when the alert is triggered, such as sending an email or executing a command.

- Always send alert to this destination.
- Proceed to next entry in this policy set.
- Do not process any more entries in this policy set.
- Proceed to next entry in this policy set that is to a different channel.
- Proceed to next entry in this policy set that is to a different destination selector.

LAN Channel: The network channel through which the alert will be sent.

Destination Selector: Destination Selector for active call-out session. Up to five destinations can be selected for each LAN channel.

Event Specific Alert String: Yes, means to use SEL decoded strings as the result alert string. No, When No is selected, an alert string key must be selected from the Alert String Key options below as the result alert string.

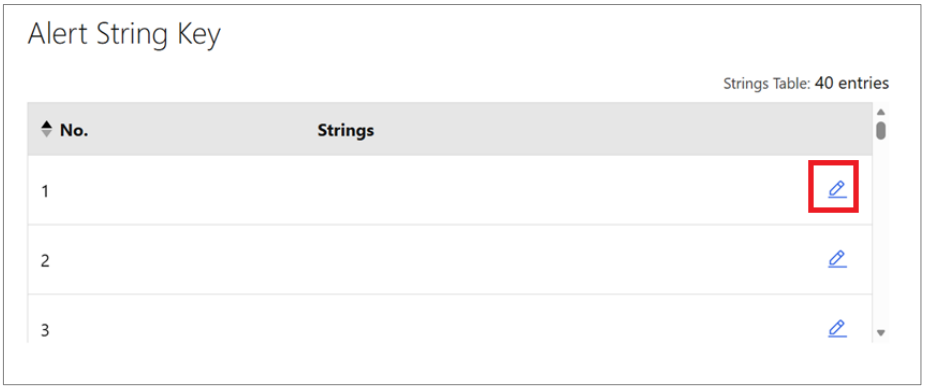
Alert String Key: A key or code that represents the specific alert message or event type.

Save: Save the current configuration settings.

Cancel: Allows the user to abort the current configuration settings.

Alert String Key

Click **Edit** icon.



The following configuration settings can be configured.

No.: A unique identifier.

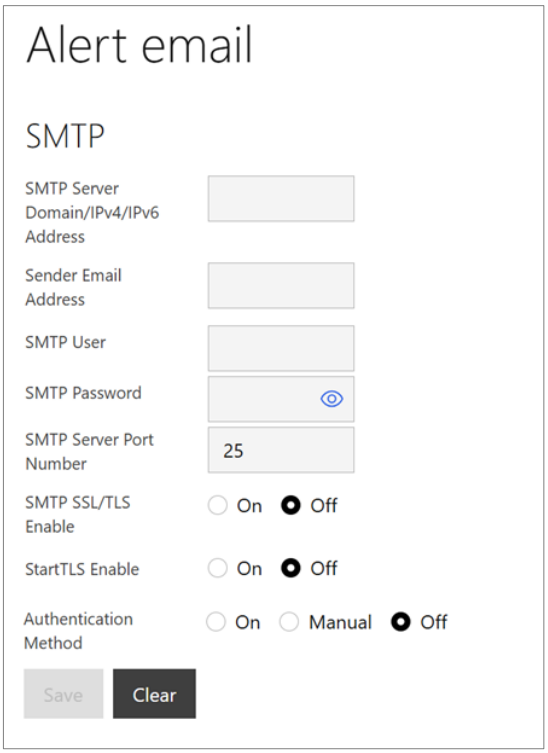
Strings: Specific alert message or event type.

Save: Save the current configuration settings.

Cancel: Allows the user to abort the current configuration settings.

Alert Email

- This page is used to configure alert email related information.



The following options can be configured.

SMTP Server Domain/IPv4/IPv6 Address: The domain or IP address of the remote SMTP mail server used for sending emails. IPv4: The IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx". 'xxx' ranges from 0 to 255. The first 'xxx' must not be 0. IPv6: The IP Address and Gateway are 128-bit fields made of eight hexadecimal numbers separated by colons as in "xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx: xxxx". 'xxxx' ranges from 0 to FFFF. First 'xxxx' must not be 0. One or more consecutive groups of zero value may be replaced with a single empty group using two consecutive colons (::). Domain: RFC 1035 defines the format of domain names.

Sender Email Address: The email address that will appear as the sender of the email.

SMTP User: The username used to authenticate with the SMTP mail server.

SMTP Password: The password associated with the SMTP mail server user for authentication.

SMTP Server Port Number: The IP port number for which the SMTP mail server is listening (e.g., 25, 465, 587).

SMTP SSL/TLS Enable: A setting to enable or disable SSL/TLS encryption for secure email transmission.

StartTLS Enable: A setting to enable the use of the STARTTLS command to upgrade the connection to a secure one.

Authentication Method: The method used to authenticate with the SMTP mail server.

- On
- Manual
- Off

When the **Manual** option is selected, the following four appointed methods will appear for you to choose from.

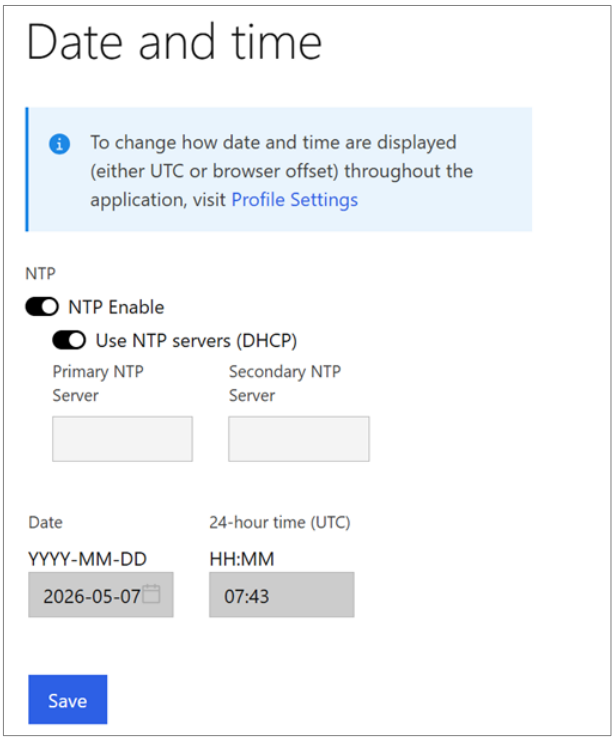
- plain
- login
- cram-md5
- external

Save: Saves the current SMTP mail server settings.

Clear: Clear all the current settings, returning the configuration fields to their default empty state. When clicked, a confirmation dialog will pop up, prompting the user to confirm the action before proceeding.

Date and Time

This page allows you to configure the BMC network settings, including LAN channels, IPv4 and IPv6 configurations, as well as DNS server settings.



The following options can be configured.

Time Zone: Select the time zone of worldwide.

NTP Enable: Enables/disables NTP service.

- If NTP is enabled, you have to set the Use NTP servers (DHCP)、Primary NTP Server、Secondary NTP Server setting fields related to NTP.
- If NTP is disabled, you must manually set the date and time in the Date YYYY-MM-DD、24-hour time (UTC) HH:MM fields or Sync from RTC.

Use NTP servers (DHCP): Enables/disables if use DHCP NTP servers. Configuring the NTP server address through the DHCP (Dynamic Host Configuration Protocol) protocol.

Primary NTP Server: The main server configured in a system to synchronize the system clock with an authoritative time source.

Secondary NTP Server: Backup to the primary NTP server. It is used if the primary server becomes unavailable or unresponsive.

Date YYYY-MM-DD: Modifies the date. You may click the calendar icon to choose the date.

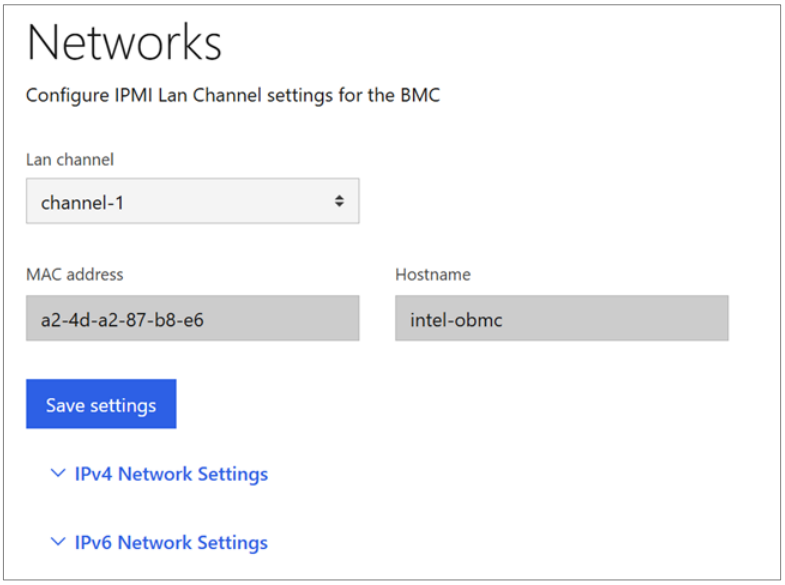
24-hour time (UTC) HH:MM: Modifies the time.

Save: Click this button to save the new Date and Time configurations.

> **NOTE**
>
> The date and time cannot be set more than **Jan 19 03:14:07 2038**. After this point, systems relying on a signed 32-bit integer to track time will experience an **integer overflow**, causing the time to be misrepresented as **Dec 13 20:45:52 1901 (UTC)**.

Networks

This page allows you to configure the BMC network settings, including LAN channels, IPv4 and IPv6 configurations, as well as DNS server settings.



Configure LAN Channel Settings

The following options can be configured.

LAN Channel: Select from the drop-down menu.

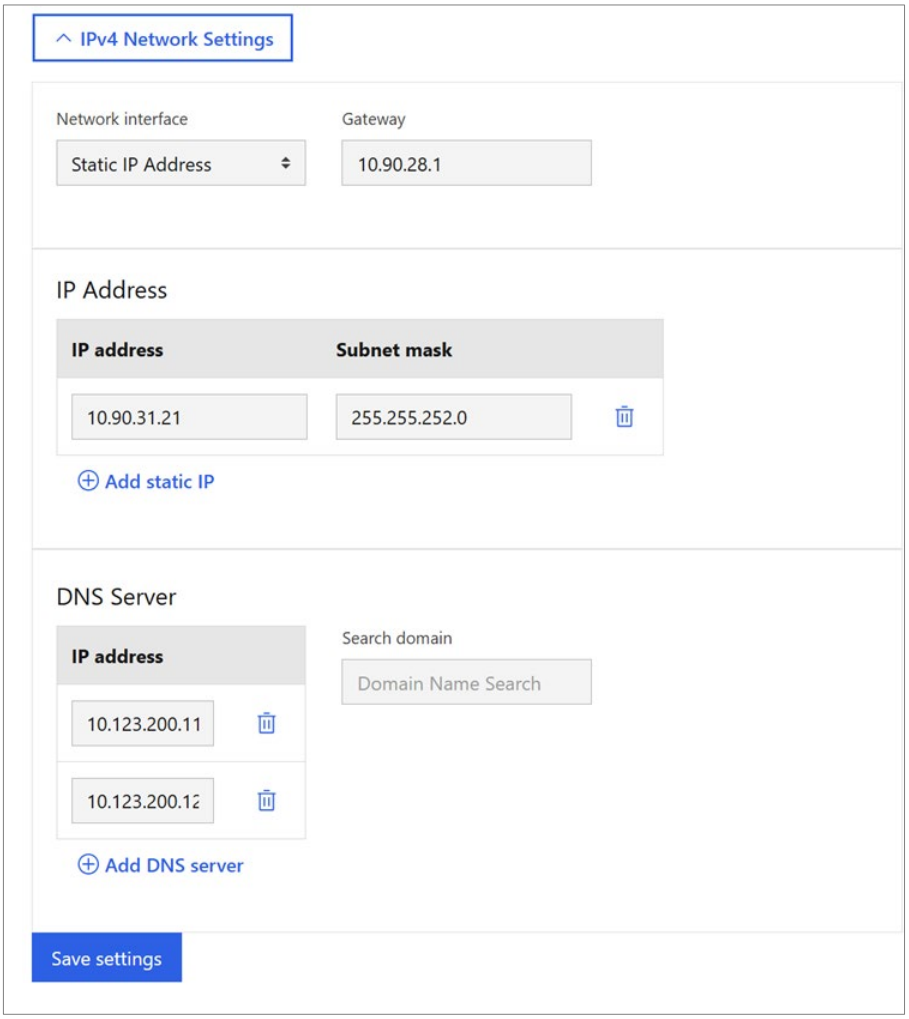
MAC Address: Shows the MAC address of the LAN.

Hostname: Shows the Hostname of the LAN if available.

Click **Save setting** to save the configuration.

IPv4 Network Settings

This page shows how to configure IPv4 Network Settings.



The following options can be configured.

LAN Failover: Allows multiple Ethernet interfaces to work together for redundancy. When enabled, it combines (bonds) selected Ethernet devices into a single primary LAN channel. You can specify the primary LAN channel, and if the connection to the primary interface is lost, one of the secondary interfaces will automatically take its place, maintaining the same IP address.

- **Enable:** All LAN interfaces are grouped into a single, unified interface for failover support.
- **Disable:** Each LAN interface operates independently with its own network configuration.

NOTE

The LAN Failover option will only be displayed when the number of available LAN channels exceeds one. If only one LAN channel is available, this option will not be visible in the UI.

LAN channel: Displays the currently active channels. Select the LAN channel to configure from the dropdown menu.

MAC address: Displays the MAC (Media Access Control) address of the selected LAN channel. This field is read-only.

Hostname: Displays the hostname of the BMC device. This field is read-only.

Network Interface: This setting allows you to configure how the network interface for this LAN channel operates. There are three options to choose from:

- **Link Disabled:** Disables the network interface for this LAN channel. The Gateway field will become read-only. IP address and DNS Server/Search domain become unconfigurable.
- **Static IP Address:** Enables manual configuration of the network settings for this LAN channel. You can specify the IP Address, Subnet mask, Gateway, and DNS Server.
- **DHCP Enabled:** Automatically configures the network interface using settings provided by a DHCP server. The following fields will become grayed out and read-only, as they are managed by the DHCP server: IP Address, Subnet Mask, Gateway, and DNS Server.

Gateway: Specifies the IPv4 gateway for network routing, this field is editable unless the interface is disabled.

IP Address/Subnet mask: Configure the static IPv4 address and its associated subnet mask for the network interface. These fields are editable only when the Network Interface is set to Static. You can add multiple static IP addresses/Subnet mask by clicking Add static IP. To remove an IP address/Subnet mask, click the trash icon next to the entry.

IP Address (DNS Server): Configure the IPv4 addresses of the DNS servers used for domain name resolution. Click Add DNS server to add multiple DNS server addresses. If more than one DNS server address is configured, you can remove an entry by clicking the trash icon next to it.

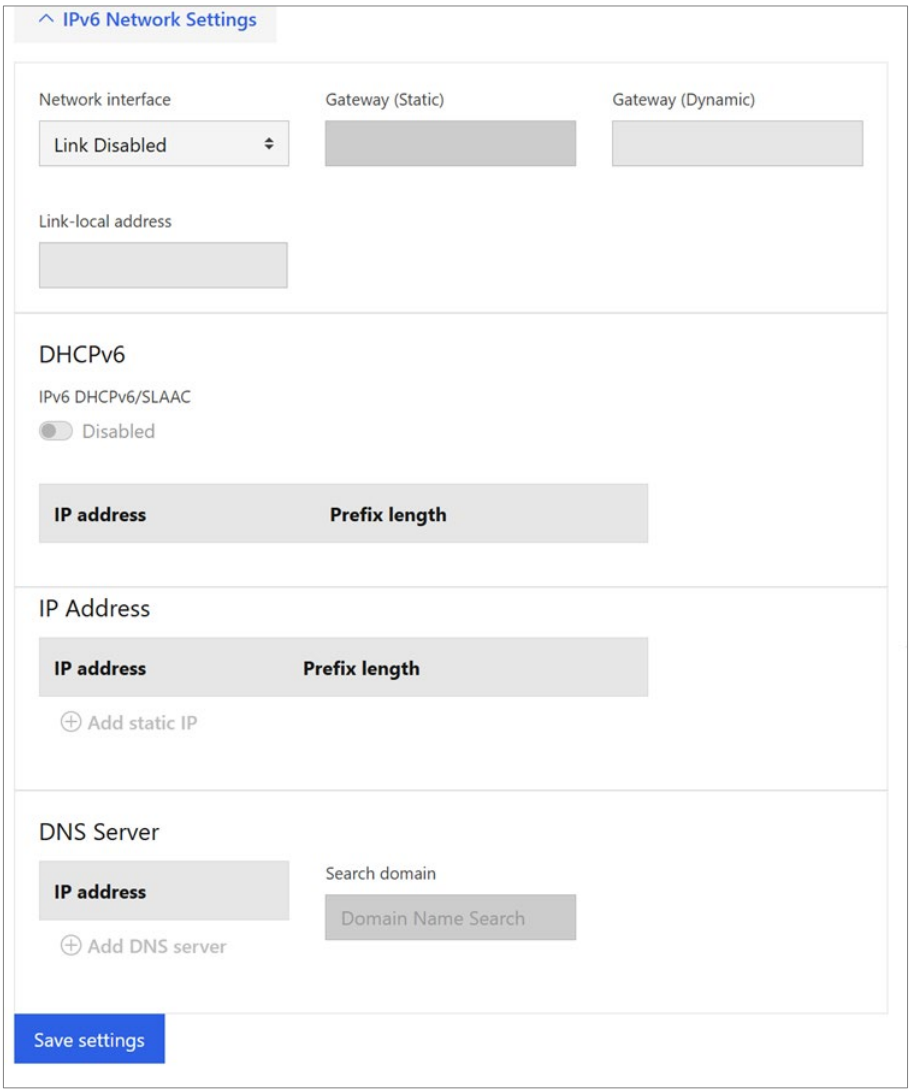
Search domain: Specify the search domain name used for DNS resolution. This helps to automatically complete hostnames without requiring the full domain name. For example, if the search domain is set to example.com and you try to reach host1, the BMC will automatically attempt to resolve it as host1.example.com.

Save Settings: Click **Save Settings** button to apply any changes made to the IPv4 network configuration. After clicking the button, a warning dialog will appear:

Warning: *This action may change your device's network settings, and you may lose connectivity in this browser session. Reconnect using a new browser session after applying the changes. Do you want to continue? Confirming the warning will proceed with the changes. It is recommended to verify the new settings before applying them to ensure uninterrupted access to the BMC.*

IPv6 Network Settings

This page shows how to configure IPv6 Network Settings.



The following options can be configured.

Network Interface: This option allows you to enable or disable the IPv6 network functionality for the selected LAN channel.

- **Link Disabled:** Disables the IPv6 network interface.
- **Link Enabled:** Enables the IPv6 network interface for this LAN channel.

Gateway (Static): Specifies a static IPv6 gateway address for the network.

Gateway (Dynamic): Displays the dynamic gateway address assigned by the DHCP server or SLAAC. (read-only)

Link-Local Address: Displays the automatically generated link-local IPv6 address. (read-only) A **Link-Local Address** in IPv6 is a special type of IP address that is used for communication between devices on the same local network segment (link). These addresses are not routable across different networks, meaning they are only valid and used within the local network segment.

IPv6 DHCP/SLAAC: Allows enabling or disabling IPv6 address assignment via DHCPv6 or SLAAC. IP Address and Prefix Length are dynamically assigned by the DHCP server or SLAAC.

- **DHCPv6:** When enabled, IPv6 addresses and additional network configuration parameters (such as DNS server information) are dynamically assigned by the DHCPv6 server. This is a stateful configuration, meaning the DHCP server maintains a record of the assigned addresses.
- **SLAAC (Stateless Address Autoconfiguration):** When enabled, IPv6 addresses are automatically configured by the device based on the Router Advertisement (RA) messages from the network router. This is a stateless configuration, meaning the device generates its own IP address without the need for a DHCP server. The prefix length (subnet size) is also provided by the router.

IP Address: Manually enter an IPv6 address. The following formats are supported:

- **Compressed Format:** This format allows shortening consecutive zero groups with a double colon (::). For example: ::c0a8:a16:4ab0:2dff:feee:223
- **Full Format:** This format includes all 8 blocks of the IPv6 address, with leading zeros in each block. For example: 2001:0db8:0000:0000:0000:ff00:0042:8329
- **Abbreviated Format:** This format uses shorthand by omitting leading zeros within each block and compressing zero blocks using ::. For example: 2001:db8::ff00:42:8329
- **Embedded IPv4 Format:** This format embeds an IPv4 address in an IPv6 address. The IPv4 address is represented as ::ffff:<IPv4 address>. For example: ::ffff:192.0.2.128
- **Leading Zero Compression Format:** This format omits leading zeros within each block. For example: 2001:db8:0:0:0:ff00:42:8329
- **CIDR Notation Format:** This format specifies the IPv6 address followed by a slash and the prefix length, indicating the network size. For example: 2001:db8::ff00:42:8329/64

Ensure that the IPv6 address is correctly entered in one of the supported formats to ensure proper network configuration. Note that this field is editable only when the **Network Interface** is set to **Link Enabled**. You can add multiple static IP addresses by clicking **Add Static IP** or remove an IP address by clicking the trash icon next to the entry.

Prefix length: Defines the subnet size for the IPv6 address using the prefix length, which specifies the number of bits used to identify the network portion of the address. The prefix length is represented as a decimal number following a slash (/), for example: 2001:db8::/32. The Prefix Length can range from 0 to 128. Note that this field is editable only when the Network Interface is set to Link Enabled. You can add multiple prefix lengths by clicking Add Static IP or remove a prefix length by clicking the trash icon next to the entry.

IP Address (DNS Server): Enter the DNS server's IPv6 address manually. This field is editable only when the Network Interface is set to Link Enabled. You can add multiple prefix lengths by clicking Add Static IP or remove a prefix length by clicking the trash icon next to the entry.

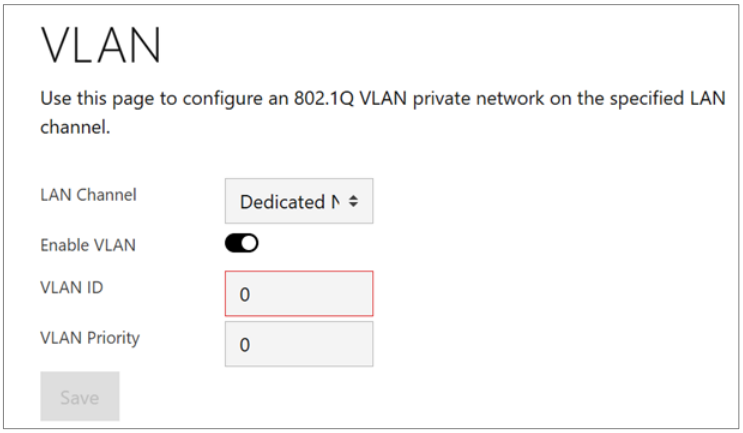
Search Domain: Specifies the search domain name used for DNS resolution. This helps to automatically complete hostnames without requiring the full domain name. For example, if the search domain is set to example.com and you try to reach host1, the BMC will automatically attempt to resolve it as host1.example.com.

Save Settings: Click **Save Settings** button to apply any changes made to the IPv6 network configuration. After clicking the button, a warning dialog will appear:

Warning: *This action may change your device's network settings, and you may lose connectivity in this browser session. Please reconnect using a new browser session after applying the changes. Do you want to continue? Confirming the warning will proceed with the changes. It is recommended to verify the new settings before applying them to ensure uninterrupted access to the BMC.*

VLAN

This page allows you to configure an 802.1Q VLAN private network for a specified LAN channel. This setup is essential for creating isolated virtual networks for better traffic management and security.



The following options are available for configurations.

LAN Channel: Select the channel on which to configure the network settings. Lists the LAN Channels available for VLAN. The LAN channel describes the physical NIC connection in the BMC.

Enable VLAN: Toggles to enable or disable VLAN configuration on the selected LAN channel.

VLAN ID: Enter the VLAN ID (identifier) for the VLAN network. VLAN ID are used to uniquely identify each VLAN on the network. Values are from **1 to 4094**.

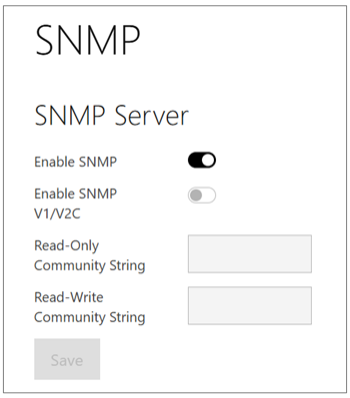
VLAN Priority: Sets the VLAN Priority to define the traffic class for the VLAN. This value determines the priority level of packets sent through the VLAN. Valid Range: **0–7**, where 0 is the lowest priority and 7 is the highest priority.

Save: Click **Save** button to apply and save the VLAN configuration settings. After clicking the button, a warning dialog will appear:

Warning: *This action may change your device's network settings and you may lose connectivity in this browser session. Please reconnect using a new browser session after applying the changes. do you want to continue?*

SNMP

This page shows how to configure SNMP settings.



The following options are available to configure.

Enable SNMP: Enables or disables SNMP.

Enable SNMP V1/V2C: Enables or disables SNMP V1/V2C.

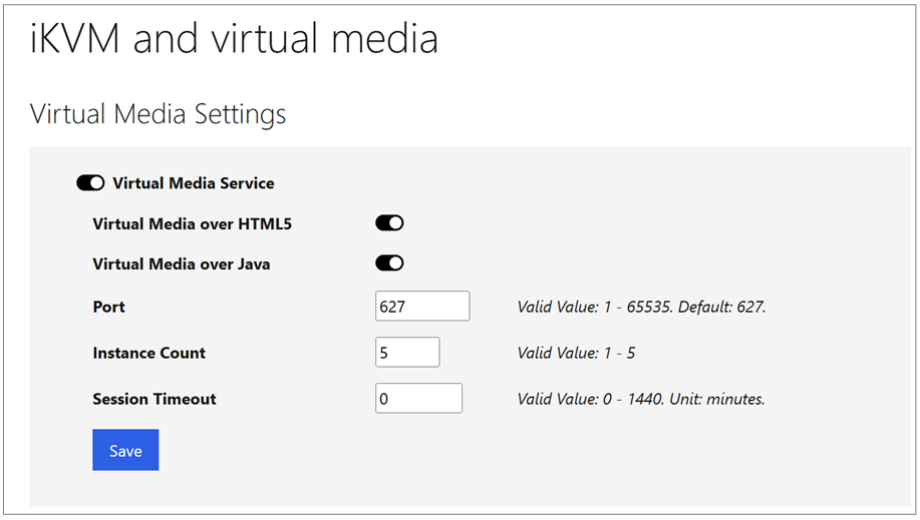
Read-Only Community String: Enters the value for read-only community string.

Read-Only Community String: Enters the value for read-only community string.

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

iKVM and Virtual Media

This page allows you to configure iKVM and Virtual Media settings. iKVM (Integrated Keyboard, Video, and Mouse) enables remote control of the host's keyboard, display, and mouse. The Virtual Media feature allows you to remotely mount media (such as ISO files), facilitating OS installation, recovery, or updates. These settings enable flexible host management and support remote maintenance and troubleshooting.



The following options are available to configure.

Virtual Media Settings

Virtual Media Service: Toggle Virtual Media Service to enable or disable the remote virtual media functionality.

Virtual Media over HTML5: Toggle Virtual Media over HTML5 to enable or disable access to virtual media through an HTML5 interface.

Virtual Media over Java: Toggle Virtual Media over Java to enable or disable access to virtual media through a Java interface.

Port: Enter the port number for the Virtual Media over Java Service (default: 627, range: 1-65535).

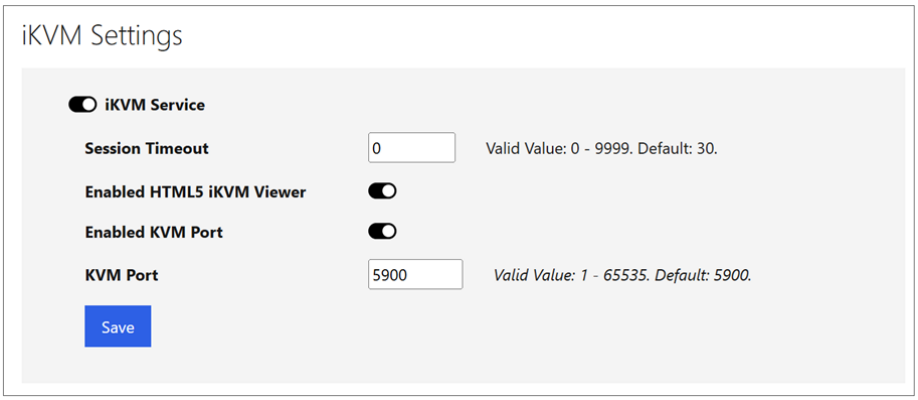
Instance Count: Enter the maximum number of concurrent Virtual Media sessions. (range: 1-5)

Session Timeout: This setting allows you to choose how long a session can stay idle before it automatically terminates. (range: 0-1440, Unit: minutes)

Note: If set to 0, sessions will stay active forever until manually disconnected.

Save: Click **Save** button to save the changes in the Virtual Media Settings.

iKVM Settings



iKVM Service: Toggle iKVM Service option to enable or disable the iKVM functionality. Enabling this service allows remote keyboard, video, and mouse control of the host system.

Session Timeout: This setting allows you to choose how long a session can stay idle before it automatically terminates. (range: 0-9999, Unit: minutes)

Note: If set to 0, sessions will stay active until manually disconnected.

Enabled HTML5 iKVM Viewer: Toggle this setting to enable or disable the HTML5 iKVM Viewer. When enabled, users can access the iKVM console through an HTML5-compatible browser.

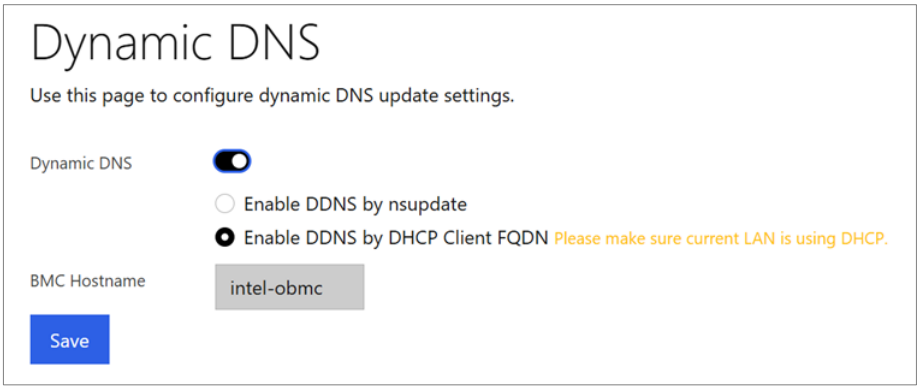
Enabled KVM Port: Toggle this setting to enable or disable the KVM port. When enabled, the system allows remote KVM connections through the specified port.

KVM Port: Enter the port number used for KVM connections. (range: 1-65535, default: 5900)

Save: Click **Save** button to save the changes in the iKVM Settings.

Dynamic DNS

This page allows you to configure settings for Dynamic DNS(updates. Dynamic DNS is a service that automatically updates changing IP addresses to a DNS server so that users can access the device through a fixed domain name even if the IP address changes.



The following options are available to configure.

Dynamic DNS: Enables or disables the DDNS feature.

- **On:** DDNS is active, allowing automatic DNS updates. When enabled, you can choose between:
  - **Enable DDNS by nsupdate:** Uses the nsupdate method to update DNS records dynamically.
  - **Enable DDNS by DHCP Client FQDN:** Updates DNS records using the Fully Qualified Domain Name (FQDN) provided by the DHCP client.
- **Off:** DDNS is inactive.

Enable DDNS by nsupdate: The nsupdate option uses a dynamic DNS update utility to send DNS update packets directly to the DNS server.

Enable DDNS by DHCP Client FQDN: This option allows dynamic DNS updates by utilizing the **DHCP Client's Fully Qualified Domain Name (FQDN)**, simplifying DNS record management by automating updates through the DHCP server. It allows devices to automatically update their DNS records, ensuring accurate mappings between IP addresses and hostnames. When enabled, the DHCP client sends its full hostname (FQDN) to the DHCP server, which updates the DNS server with the client's IP and FQDN, removing the need for manual DNS record updates.

DNS Server IP: Specifies the IP address of the DNS server. Both IPv4 and IPv6 addresses are supported. This IP will be used by the nsupdate utility to communicate with the DNS server.

Domain Name: Specifies the domain name managed by the DNS server. The BMC hostname will be updated within this domain.

BMC Hostname: Displays the hostname of the BMC and is read-only.

TSIG Authentication (Transaction Signature): This setting enables secure communication between the BMC and the DNS server using Transaction Signature (TSIG).

> **NOTE**
>
> TSIG protocol includes a timestamp. Ensure the BMC's system time is accurate, as TSIG uses a timestamp to prevent replay attacks. Incorrect BMC time may cause TSIG authentication to fail.TSIG (transaction signature): is a protocol extension used in DNS to provide secure authentication and integrity for DNS transactions. It achieves this by attaching a cryptographic signature to each DNS message. This signature is computed using a shared secret key and a hashing algorithm, such as HMAC-MD5 or HMAC-SHA256.

TSIG Key (Key name): After uploading the **TSIG Key File** and **TSIG Private Key File**, the Key Name is extracted from the contents of the .key file. This field is read-only.

Example: If the .key file includes a record such as: tsig2. IN KEY 512 3 157 mK6Qhw5eQtA= The **Key name** will be displayed as **tsig2**.

TSIG Key File: Upload the key file for authentication.

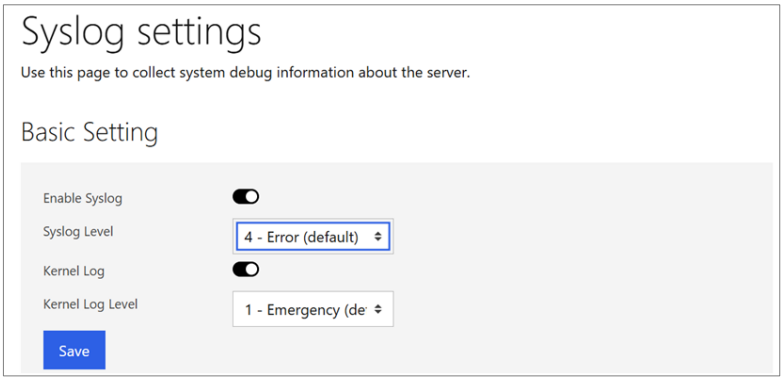
TSIG Private Key File: Upload the private key file for authentication.

Save: Click **Save** button to apply and save the Dynamic DNS configuration settings. After clicking the button, a warning dialog will appear:

Warning: *This action may change your device's network settings and you may lose connectivity in this browser session. Please reconnect using a new browser session after applying the changes. do you want to continue?*

Syslog Settings

This page is used to configure BMC system debug log (syslog) settings.



Basic Setting

Enable Syslog: Used to enable/disable syslog service. After enabling this option, you can modify the Syslog Level, Kernel Log, Kernel Log Level settings.

Syslog Level: Used to change the log level.

- 1 – Emergency
- 2 – Alert
- 3 – Critical
- 4 – Error (default)
- 5 – Warning
- 6 – Notice
- 7 – Informational
- 8 – Debug

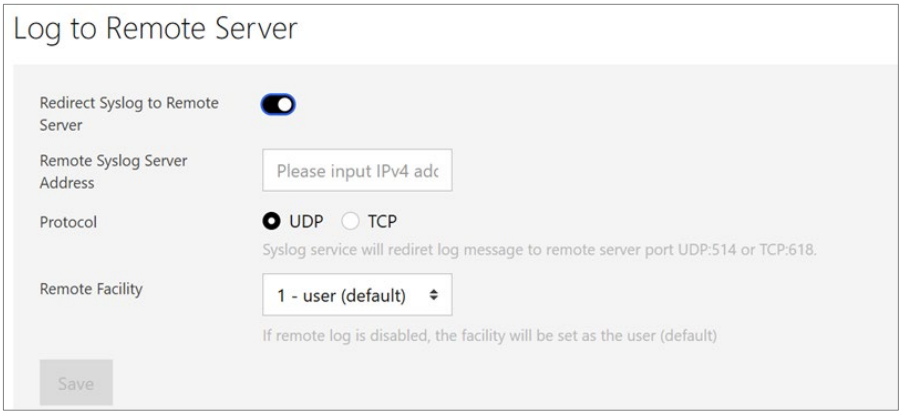
Kernel Log: Enables/Disables the kernel log.

Kernel Log Level: Used to change the kernel log level.

- 1 – Emergency
- 2 – Alert
- 3 – Critical
- 4 – Error (default)
- 5 – Warning
- 6 – Notice
- 7 – Informational
- 8 – Debug

Save: Click to save changes.

Log to Remote Server



Redirect Syslog to Remote Server: Enables/Disables to redirect the syslog message to remote server. When it is enabled, you can modify the Remote Syslog Server Address, Protocol, and Remote Facility settings.

Remote Syslog Server Address: Inputs the remote syslog server IPv4 Address.

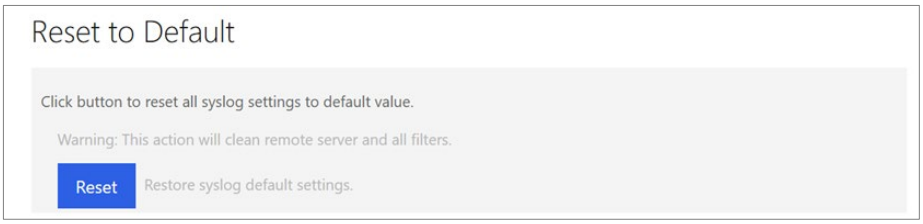
Protocol: Choose what protocol (UDP or TCP) used to redirect the syslog to remote.

Remote Facility: Used to change the facility to assign the subsystem on remote syslog server.

- 1 – user (default)
- 2 – Local0
- 3 – Local1
- 4 – Local2
- 5 – Local3
- 6 – Local4
- 7 – Local5
- 8 – Local6
- 9 – Local7

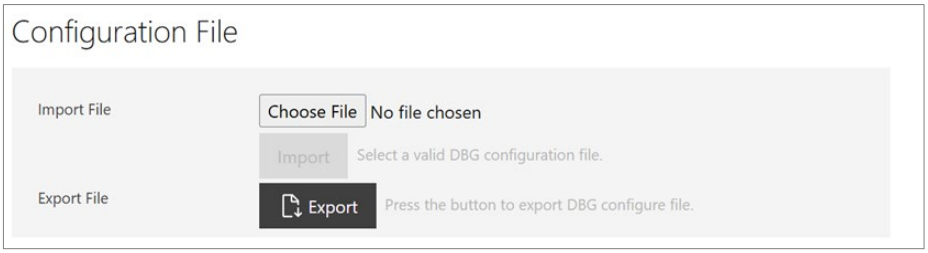
Save: Click to save changes.

Reset to Default



Click **Reset** to restore syslog default settings.

Configuration File



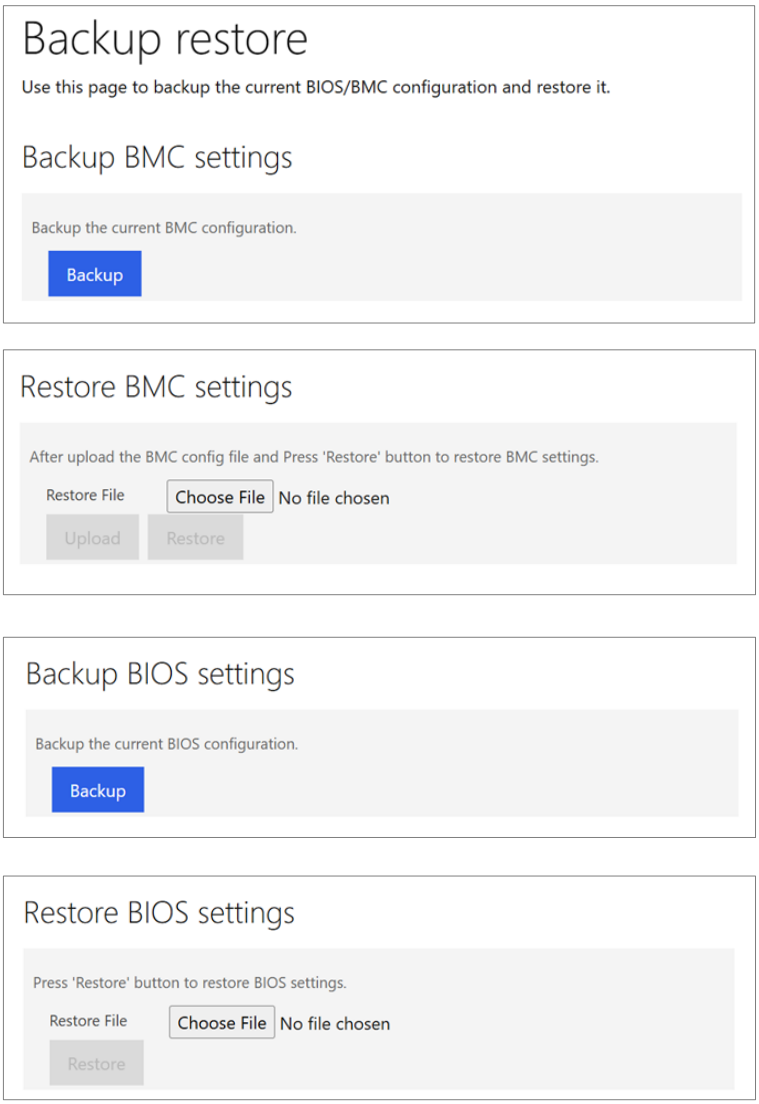
Choose File: Click to choose the local configuration file for import.

Import: Click to import the configuration file. Used to import/restore the syslog settings. The import file must be DBG format.

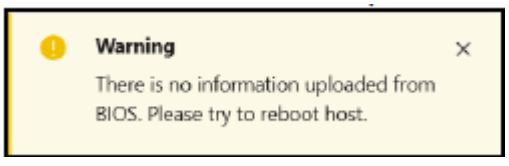
Export: Click to export the configuration file. Used to backup/download the syslog settings. The export file is DBG format.

Backup Restore

This page is used to display Backup restore related information. BMC offers backup and restore functionality for both the BMC/BIOS configuration file. This feature allows users to back up current configurations, ensuring that system settings can be restored in the event of a failure or for recovery purposes. By securely storing backups, BMC provides a reliable method to maintain system stability and quickly recover from potential issues.



Backup: Click this button to download the current BMC/BIOS configuration to a file. BMC backup file name: backup256.bin ('256' that means sha256 checksum.) BIOS backup file name: bios.cfg Notice: If the BIOS Backup button grays out, it means that the BIOS is not uploading data to the BMC. The following warning is displayed. Reboot the host and try again.



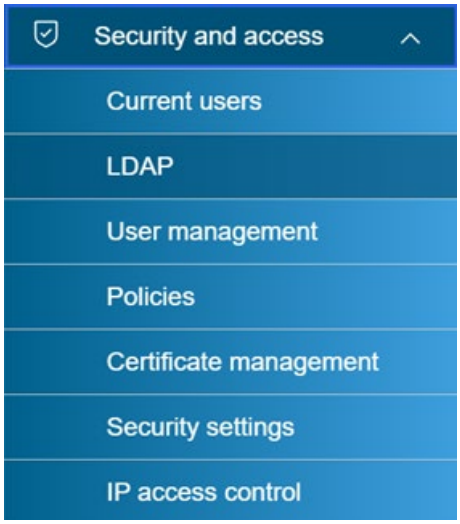
Choose File: Click **Choose File** button to select a file from local device. When clicked, it opens a file selection dialog where the user can navigate through their files and folders. After finding and selecting the desired file, the user confirms the selection by clicking **Open** button, which then references the chosen file for further actions.

Upload: Uploads the selected BMC configuration file to the system.

Restore: Restores the BMC configuration from a previously saved file. When clicked, a confirmation box will appear, prompting the user to confirm the action for BMC restoration. Once confirmed, the BMC will immediately restart, and this action cannot be undone, ensuring the user intentionally restores the previous BMC state. For the BIOS configuration restoration, no confirmation box will appear. The BIOS configuration will be immediately restored without additional prompts, and this action is also irreversible, ensuring the user intentionally restores the previous BIOS state.

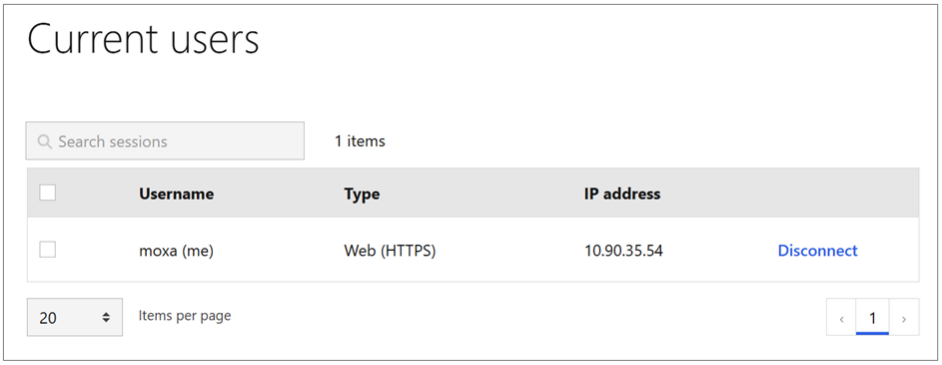
Security and Access

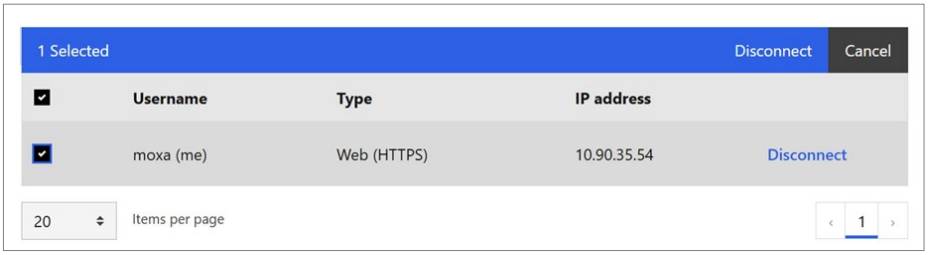
This section refers to the measures and configurations used to protect systems, networks, and data from unauthorized access, while ensuring that legitimate users can access resources when needed. These settings are crucial for maintaining the confidentiality, integrity, and availability of information and services.



Current Users

This page is used to display current users.





The following options can be configured.

Search bar: The search input box allows users to input a keyword to find detailed session information. If any matches are found, only the matching session items will be displayed instantly. There will show total data amount beside.

Table checkbox: Click the checkbox beside the table header to select all data. Click the checkbox beside the user to select this user. After clicking will show as the picture below. Click **Disconnect** to continue, or click **Cancel** to stop.

Disconnect button: Disconnects the selected session. Click Disconnect to disconnect the selected users, or click Cancel to abort.

Item per page: Selects how much data will display per page.

<: Go to the previous page of the list.

Specific Page (1, 2, 3, etc.): Click any numbered button to jump directly to that specific page of the list. This is helpful for quickly accessing a particular section of the list.

>: Go to the next page of the list.

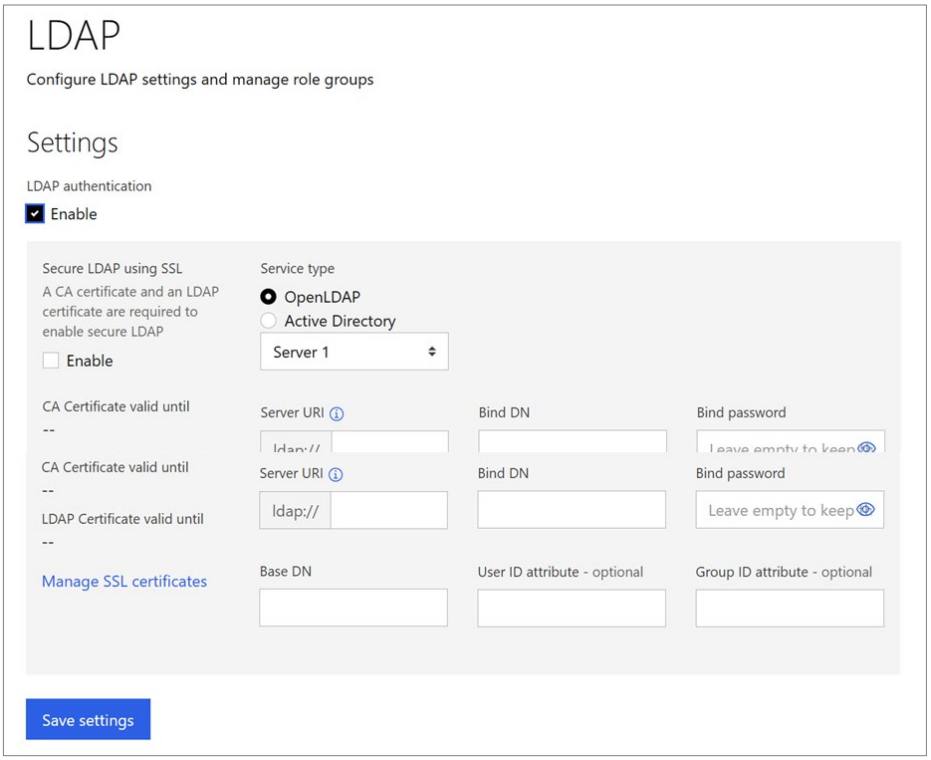
LDAP

This page provides options to configure server settings for OpenLDAP or Active Directory.

LDAP (Lightweight Directory Access Protocol) is an open protocol used to access and manage directory information services. It is commonly used for authentication and user management in systems like OpenLDAP, Active Directory, and similar directory-based services.

OpenLDAP is an open-source implementation of the LDAP, a protocol used for accessing and managing directory information services over a network.

Active Directory (AD) is a directory service developed by Microsoft for Windows domain networks. Active Directory uses LDAP as its primary protocol for directory services and supports authentication mechanisms like Kerberos and NTLM. It is widely used for managing enterprise networks and enabling single sign-on (SSO) capabilities.



Settings

The following options can be configured.

LDAP authentication Enable: Toggle to enable or disable LDAP authentication for the system. When enabled, the system supports the LDAP server to authenticate users.

Secure LDAP using SSL Enable: Toggle to enable or disable secure communication between the system and the LDAP server using SSL/TLS. Enabling this ensures that data is encrypted during transmission.

Notice: Ensure the certificates are valid before enabling this option.

Manage SSL certificates: Goes to the Certificate management page.

Service type: Specifies the type of LDAP service being configured (e.g., OpenLDAP , Active Directory).

Server 1 ~ 3: Defines up to three LDAP servers for redundancy. The system will attempt to connect to the next server if the first one is unavailable.

Server URI: The URI of the LDAP server, including the protocol (e.g., ldap:// or ldaps://) and the server's hostname or IP address.

Bind DN: The Distinguished Name (DN) of the account used to bind to the LDAP server. This account is used for querying or searching the LDAP directory.

Bind password: The password associated with the Bind DN account for LDAP authentication.

Base DN: Specifies the starting point for LDAP searches, typically the root of the directory tree (e.g., dc=example,dc=com).

User ID attribute: The LDAP attribute used to identify users (e.g., uid or sAMAccountName). This is optional and depends on the LDAP schema.

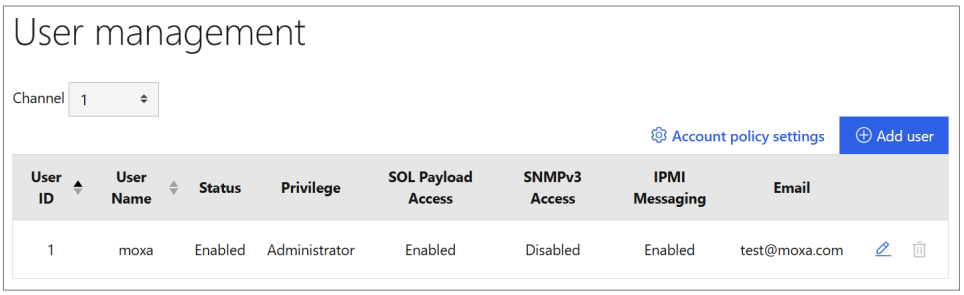
Group ID attribute: The LDAP attribute used to identify groups (e.g., gldNumber or primaryGroupID). This is optional and depends on the LDAP schema.

Save settings: Click this button to save the current LDAP configuration settings. Changes will take effect after saving.

Click **Manage SSL certificates**, you can jump to Certificate Management section.

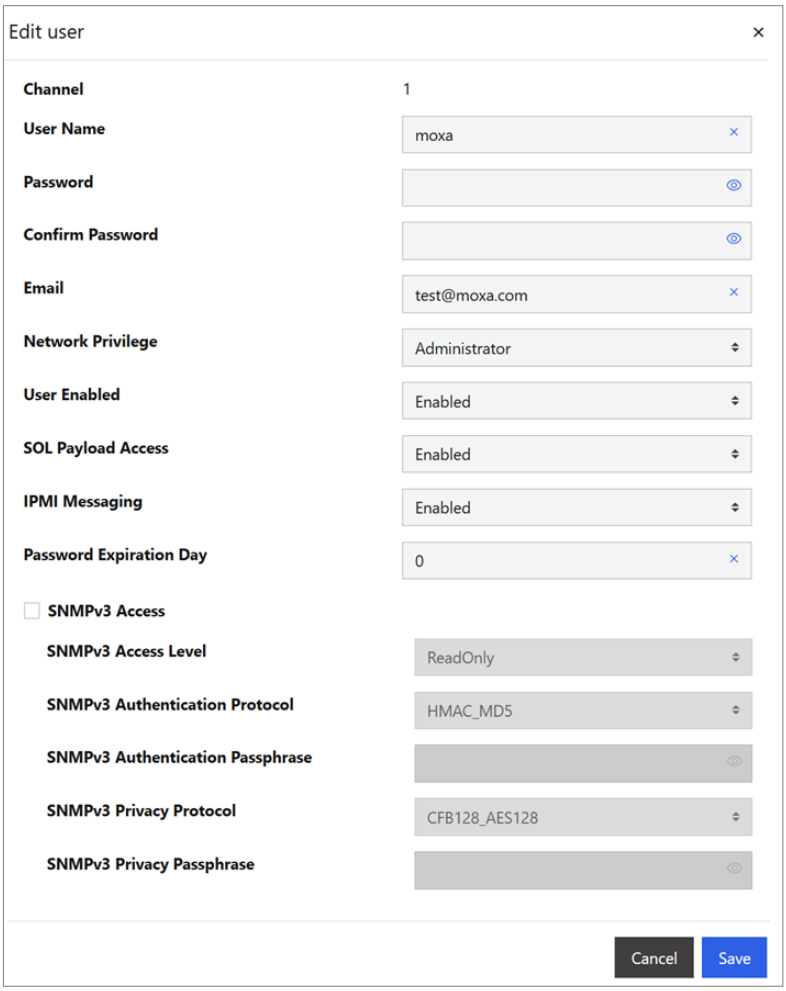
User Management

This section allows you to manage user information.



Manage the Existing User

Click icon to manage the existing user information.



The following options are available to configure.

Channel: 1 (read only)

User Name: The name used to identify a user, often displayed on the system interface.

Password: Enter the password for the user.

Confirm Password: Confirm the password.

Email: Enter the email address for the user.

Network Privilege: The level of access or permissions assigned to a user, determining what actions they can perform in the system.

- Administrator
- Operator
- ReadOnly
- NoAccess

NOTE

Different user permissions are configured for multiple channels. The web login applies the permissions defined in the first available channel (commonly Channel 1).

User Enabled: Enables or disables the user.

SOL Payload Access: Show whether this user has access to SOL Payload.

SNMPv3 Access: Show whether this user has access to SNMPv3.

IPMI Messaging: Show whether this user has access to IPMI.

Password Expiration Day: Specifies the lifetime of the password for the user.

SNMP Settings

Check **SNMP Settings** and configure the following settings.

SNMPv3 Access Level: Specifies the access level from **ReadOnly** or **ReadWrite** options.

SNMPv3 Authentication Protocol: Specified the authentication protocol from **HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_SHA256, HMAC_256_SHA384, HMAC_384_SHA512.**

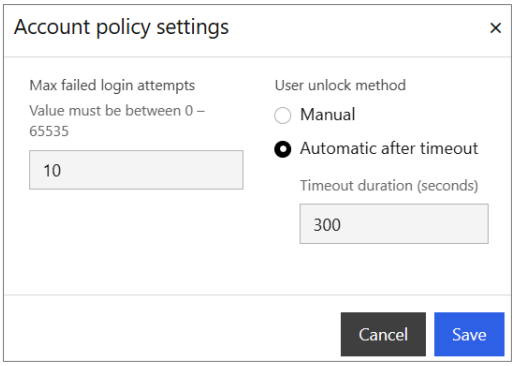
SNMPv3 Authentication Passphrase: Provide SNMPv3 authentication passphrase used in the authentication process to verify user identity.

SNMPv3 Privacy Protocol: A protocol that secures data during transmission by encrypting SNMPv3 communication data, preventing sensitive information from being intercepted. Currently, it only supports **CFB128_AES128**.

SNMPv3 Privacy Passphrase: Provide SNMPv3 privacy passphrases used to encrypt SNMPv3 data, offering privacy protection during data transmission between devices. The input length is in the range from 8 to 12.

Account Policy Settings

Click **Account policy settings**, and configure the following options.



Max failed login attempts: The maximum number of times a user can enter incorrect login credentials before being temporarily locked out. Value range starts from 0 to 65535.

User unlock method: The process used to unlock a user account after it has been locked due to failed login attempts.

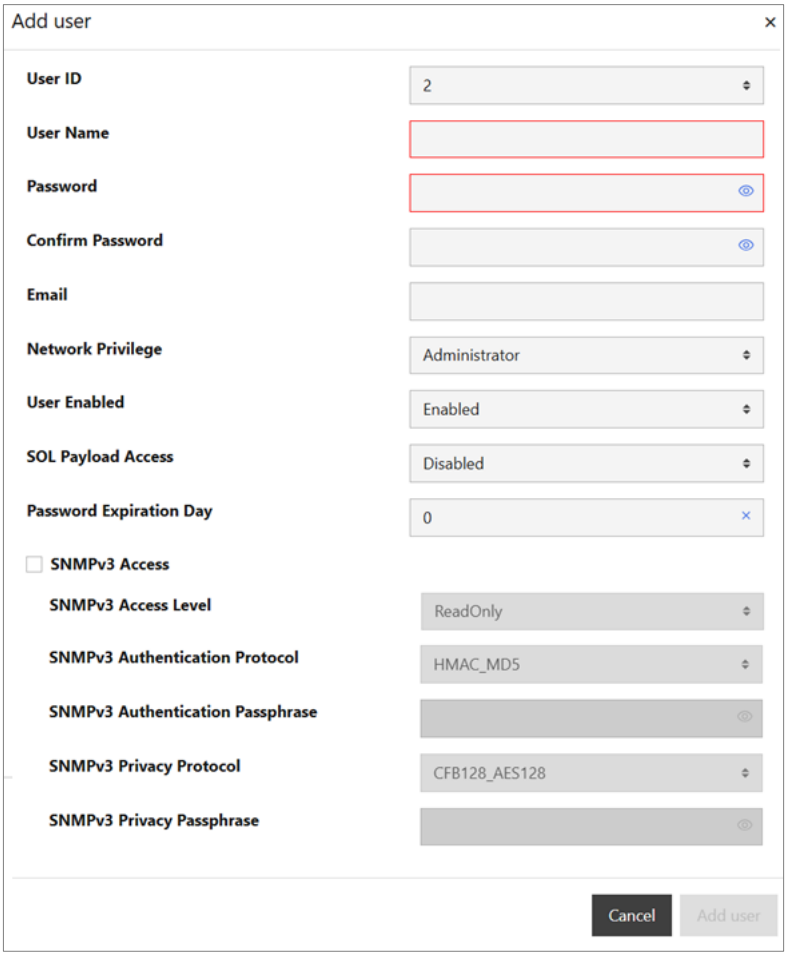
- **Manual:** Login another user to unlock the locked user.
- **Automatic:** System will automatically unlock locked user based on the time set in Timeout duration.

Timeout duration (seconds): The amount of time, in seconds, that the system will automatically unlock a locking session.

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

User Settings

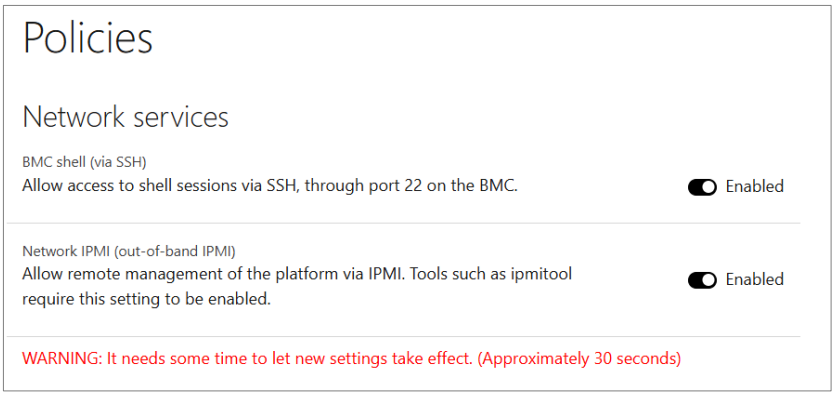
Click **Add user** to add a new user.



For the configurations, refer to **Manage the Existing User** section. When finished, click **Add user**.

Policies

This page is used to configure the ways to access BMC.



The following options are available to configure.

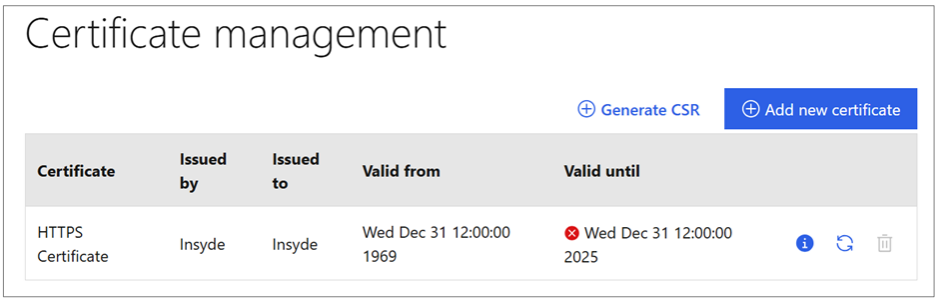
BMC shell (via SSH): Enables/Disables access to shell sessions via SSH, through port 22 on the BMC.

Network IPMI (out-of-band IPMI): Enables/Disables remote management of the platform via IPMI.

Certificate Management

Certificate Management is a security feature within the BMC system, designed to ensure encrypted and secure communication between the server hardware and the BMC. By managing and handling certificates, BMC provides robust authentication and encryption mechanisms to protect the system from unauthorized access and ensure that data is not tampered with during transmission. Certificate management is particularly important in data centers and high-security environments, ensuring the security and integrity of remote management operations.

The following figures show the currently available certificate information on the BMC.



The following options can be configured.

Generate CSR: Initiates the creation of a Certificate Signing Request, which is used to obtain an SSL/TLS certificate for secure communication between the BMC and other systems. Refer to the following sections for detailed operations.

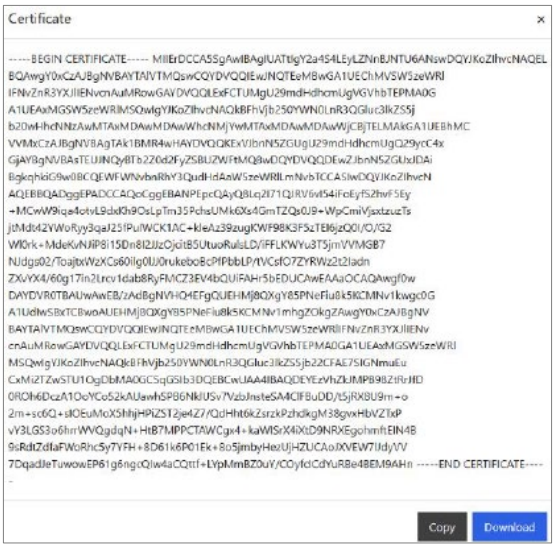
Add new certificate: Allows the user to upload or add a new SSL/TLS certificate to the BMC for secure communication.

: Displays the certificate information.

: Allows the user to replace or update the existing certificate with a new one.

: Provides the option to remove the current certificate from the system. When clicked, a confirmation box will appear, prompting the user to confirm the action. Once confirmed, the certificate will be immediately deleted, and this action cannot be undone, ensuring the user intentionally deletes certificate.

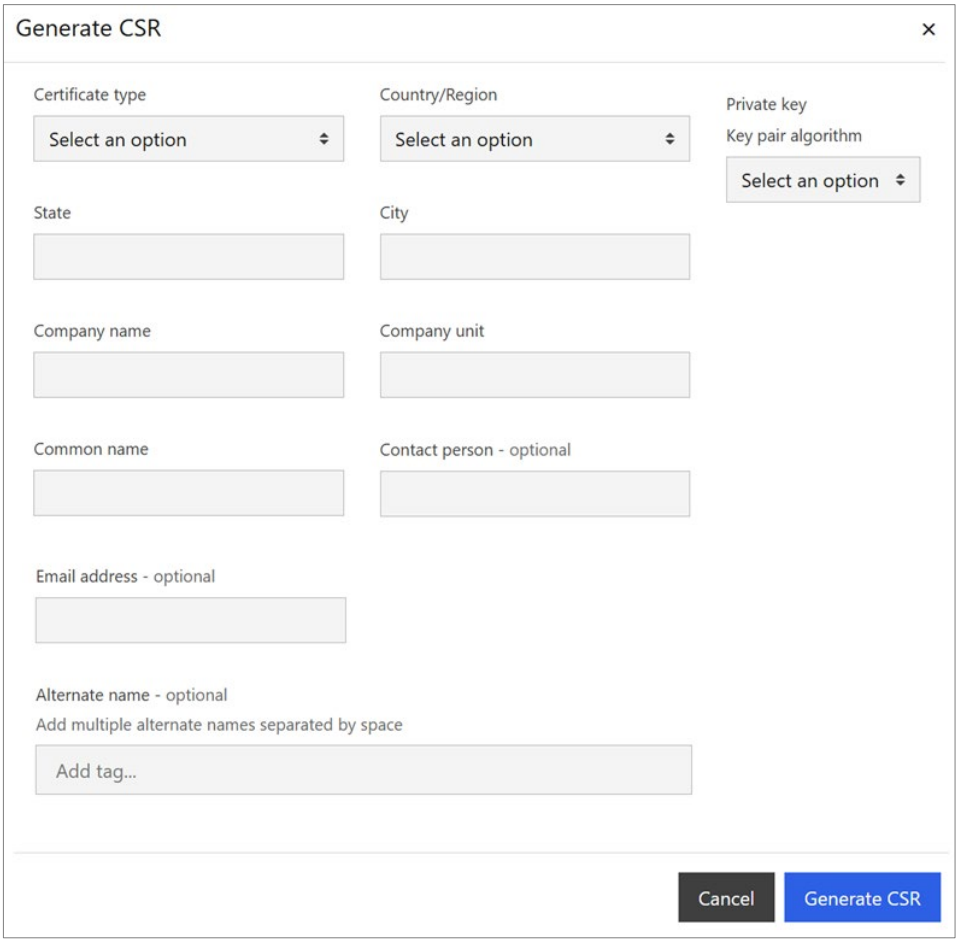
Click icon, you can view the certificate content:



Click **Copy** to copy the certificate, or **Download** to down the certificate.

Generate CSR

Click **Generate CSR** to generate a certificate signing request (CSR) with fields fills in page.



Configure the following settings.

Certificate type: Specifies the type of certificate.

- HTTPS Certificate
- LDAP Certificate

Country/Region: Indicates the country or region where the organization is located. Field required

State: Specifies the state or province of the organization. Field required

City: Defines the city where the organization is based. Field required

Company name: The official name of the organization requesting the certificate. Field required

Company unit: Refers to a specific division or department within the company. Field required

Common name: The fully qualified domain name (FQDN) or hostname associated with the certificate. Field required

Contact person-optional: An optional field to provide the name of the contact person for certificate-related matters.

Email address-optional: An optional field to provide the email address for certificate-related communication.

Alternate name-optional: An optional field for additional domain names or identifiers that the certificate should cover (e.g., Subject Alternative Name).

Private key/Key pair algorithm: The private key associated with the certificate, used for encryption and authentication. Specifies the algorithm used for generating the public-private key pair.

- EC
- RSA

Select the EC/RSA parameters that display as **Key curve ID** or **Key bit length**.

Key curve ID: The EC Key Curve ID is used to specify or identify elliptic curve keys, typically in protocols like TLS, SSH, or for digital signatures. The chosen curve defines the parameters and structure of the key generation, directly impacting the cryptographic strength and security of the system.

- prime256v1
- secp521r1
- secp384r1

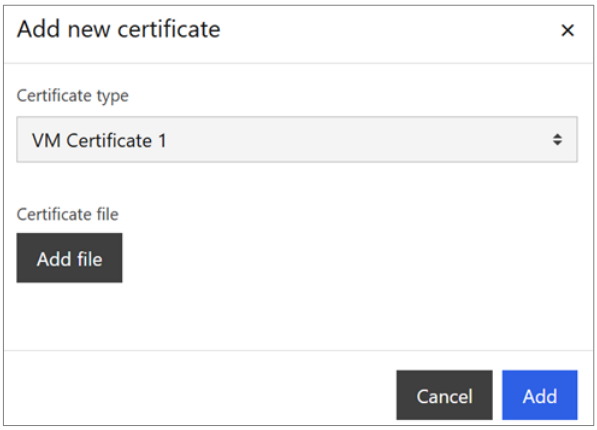
Key bit length: RSA key bit length refers to the size of the encryption key in bits, which affects both the strength of the encryption and system performance. Longer keys offer stronger security but also require more computational resources. The choice of key length should strike a balance between security needs and performance requirements.

- 2048

Generate CSR: Initiates the creation of a Certificate Signing Request, used to obtain an SSL/TLS certificate for secure communication between the BMC and other systems. You will submit this CSR to the CA for validation, and they will issue your SSL certificate.

Cancel: Allows the user to abort the current configuration settings.

Add New Certificate



Click **Add new certificate**, and do the following configurations.

Certificate type: Choose the certificate type to apply for uploaded certificate (.pem) file.

- HTTPS Certificate
- LDAP Certificate
- CA Certificate
- VM Certificate (A maximum of 5 certificates are supported.)

Add file: Click **Add file** button to select a file from local device. When clicked, it opens a file selection dialog where the user can navigate through their files and folders. After finding and selecting the desired file, the user confirms the selection by clicking the "Open" button, which then references the chosen file for further actions.

Cancel: Allows the user to abort the current configuration settings.

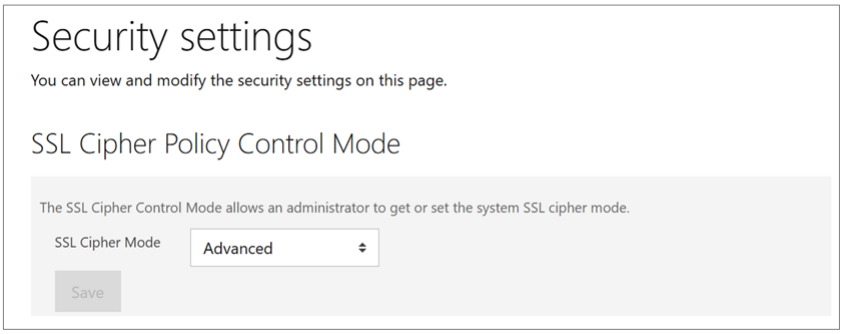
Add: Uploads the selected certificate file to the system.

Security Settings

This page is used to configure security settings related information. In the security settings of the BMC, three components are provided, primarily used to protect the BMC from unauthorized access and attacks.

SSL Cipher Policy Control Mode

The SSL Cipher Control Mode in BMC systems allows administrators to configure SSL/TLS encryption settings for secure communication between the BMC and remote systems. This feature ensures that all data exchanged is encrypted, preventing eavesdropping, tampering, and unauthorized access. By selecting specific encryption protocols and cipher suites, administrators can enforce strong security standards, protecting sensitive information and maintaining the integrity of communication channels across the network.



Configure the following settings.

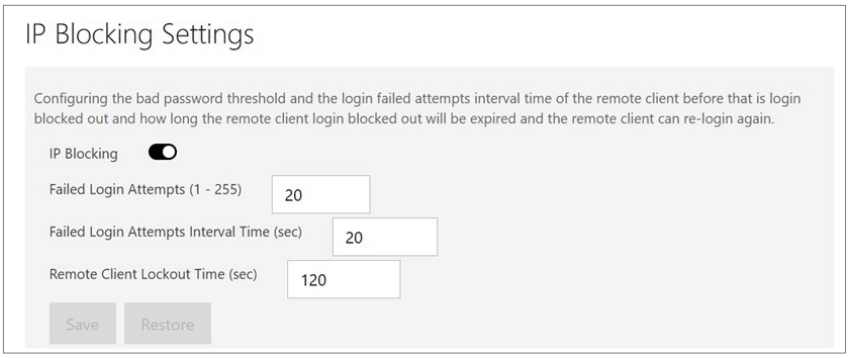
SSL Cipher Mode: Allows to set the web SSL cipher mode. When the system starts for the first time, "Advanced" is the default mode. Available options:

- **Advanced: Highest Security with Wide Compatibility**. Ensures wide browser compatibility, like most newer browser versions. This mode exclusively supports modern, secure GCM (Galois/Counter Mode) cipher suites and enforces ECDHE (providing Forward Secrecy).
- **Broad Compatibility: Higher Security with Balanced Compatibility**. Extends the Advanced set to include CBC cipher suites with stronger hash algorithms (SHA256/SHA384), helping check the compatibility to other protocols before using it, like IMAPS.
- **Widest Compatibility: Medium Security with Broadest Compatibility**. Further extends the cipher list to include ECDHE-CBC suites using the older SHA1 hash algorithm, ensuring compatibility to most legacy browsers, legacy libraries, and other application protocols besides HTTPS, like IMAPS.
- **Legacy: Lowest Security with Widest Compatibility**. Provides maximum compatibility to real old browsers and legacy libraries and other application protocols like SMTP. This mode includes RSA Key Exchange suites which do not support Forward Secrecy, making it highly vulnerable to retrospective decryption. Use is strongly discouraged.

Save: Saves the current configuration settings.

IP Blocking Settings

By configuring the bad password threshold, login failed attempts interval time, and login locked out duration, administrators can effectively mitigate brute force attacks while ensuring that legitimate users aren't unfairly locked out. The settings provide a balance between security and usability, preventing unauthorized access while allowing users a chance to re-authenticate after a brief locked out.



Configure the following settings.

IP Blocking: Enables or disables the IP blocking feature to prevent access from IPs with repeated failed login attempts.

Failed Login Attempts (1 - 255): Input the number of failed login attempts allowed before being locked out. Value ranges from 1 to 255.

Failed Login Attempts Interval Time (sec): Input the number of failed logins attempts interval time allowed before being locked out. This setting is used to define the number of consecutive failed login attempts that the system will monitor within a specific time interval. Value ranges from 20 to 4095.

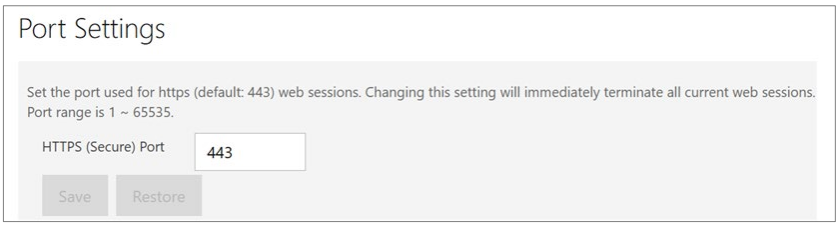
Remote Client Lockout Time (sec): Sets the duration (in seconds) for which an IP address is blocked after exceeding the failed login attempts threshold. Value ranges from 120 to 65535.

Save: Saves the current configuration settings.

Restore: Restores previously saved configuration settings, allowing the system to revert to a prior configuration. If you have to apply the previous configuration settings, you still have to click the save button.

Port Settings

The BMC tool typically provides management functions through multiple network ports. By configuring the port settings, you can control which port number is used, effectively restricting unauthorized access and enhancing system security.



Configure the following settings.

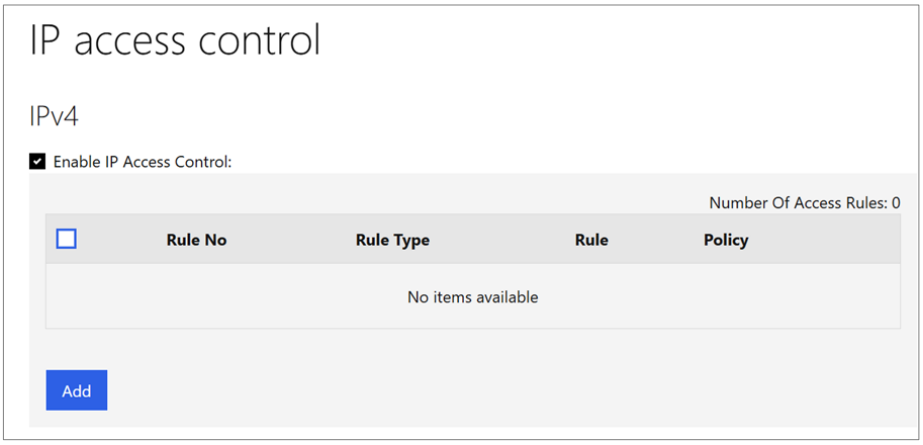
HTTPS (Secure) Port: Specifies the port number used for secure HTTPS communication with the BMC interface, typically set to 443 for encrypted access over the network. Value ranges from 1 to 65565.

Save: Saves the current configuration settings, ensuring that any changes made are stored for future use. When clicked, a confirmation dialog will pop up, prompting the user to confirm the action before proceeding. Warning: Changing port values may cause a loss of connection to the web server. A redirect attempt will be made to connect to the new port. If this redirect attempt fails, you will need to reconnect using the new port.

Restore: Restores previously saved configuration settings, allowing the system to revert to a prior configuration. If you have to apply the previous configuration settings, you still have to click **Save** button.

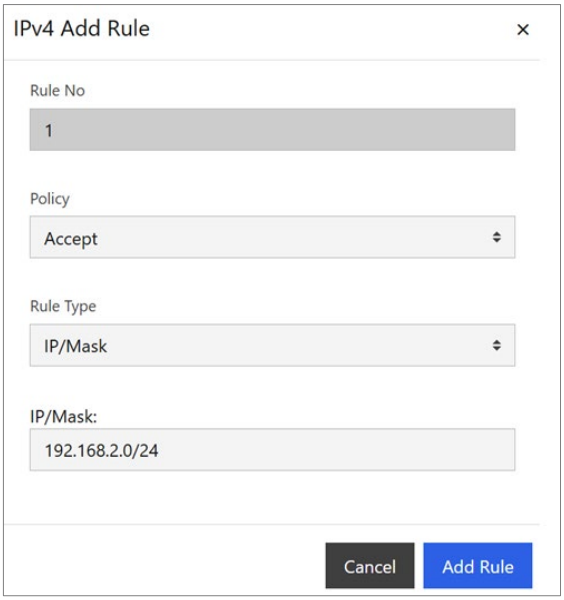
IP Access Control

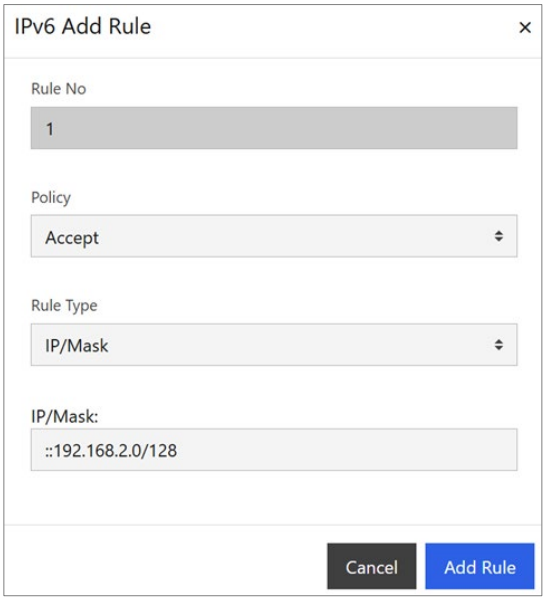
IP access control is a security feature that allows administrators to manage and restrict access to a system based on IP addresses, MAC addresses, and network ports. This provides more granular control over which devices can connect to the system, adding extra layers to prevent unauthorized access.



IPv4 Settings/IPv6 Settings

Click **Add** to create a new access control rule. The following dialog box will appear for both **IPv4 Add Rule** and **IPv6 Add Rule** pages. Fill in the details according to the field names and descriptions provided above in the dialog. Then, click **Add Rule** to complete the operation, or click **Cancel** to abort it.





Configure the following settings.

IPv4 Enable IP Access Control: Enables or disables access control for IPv4 addresses. A confirmation dialog will appear when making changes.

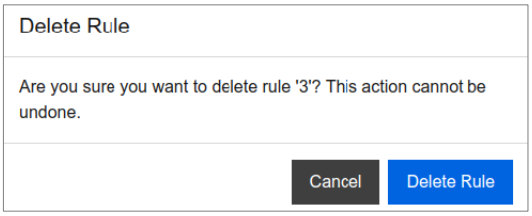
IPv6 Enable IP Access Control: Enables or disables access control for IPv6 addresses. Similar to the IPv4 option but applied to IPv6 rules.

Add: Add a new access control rule to the end of the rule list. The user must specify details such as rule type, IP address or range, and policy when adding a new rule. A dialog box will pop up as shown in the image above.

: Inserts a new access control rule before the selected rule. The user must specify details such as rule type, IP address or range, and policy when inserting a new rule. A dialog box will pop up, similar to the Add dialog box shown above.

: Modifies the selected access control rule. This option allows the user to change the rule's details (e.g., rule type, rule value, or policy) for a specific rule number. A dialog box will pop up, similar to the Add dialog box shown above

: Deletes the selected access control rule. Once deleted, the rule is no longer enforced. A confirmation dialog will appear for verification, as shown in the screenshot below.



: Unselected/Selected/Unselect All: The selected items can either be deleted or the operation can be canceled. The total number of selected items is also displayed. See the screenshot below. When deleting, a confirmation dialog will appear.