

Intel® Server Board M10JNP2SB

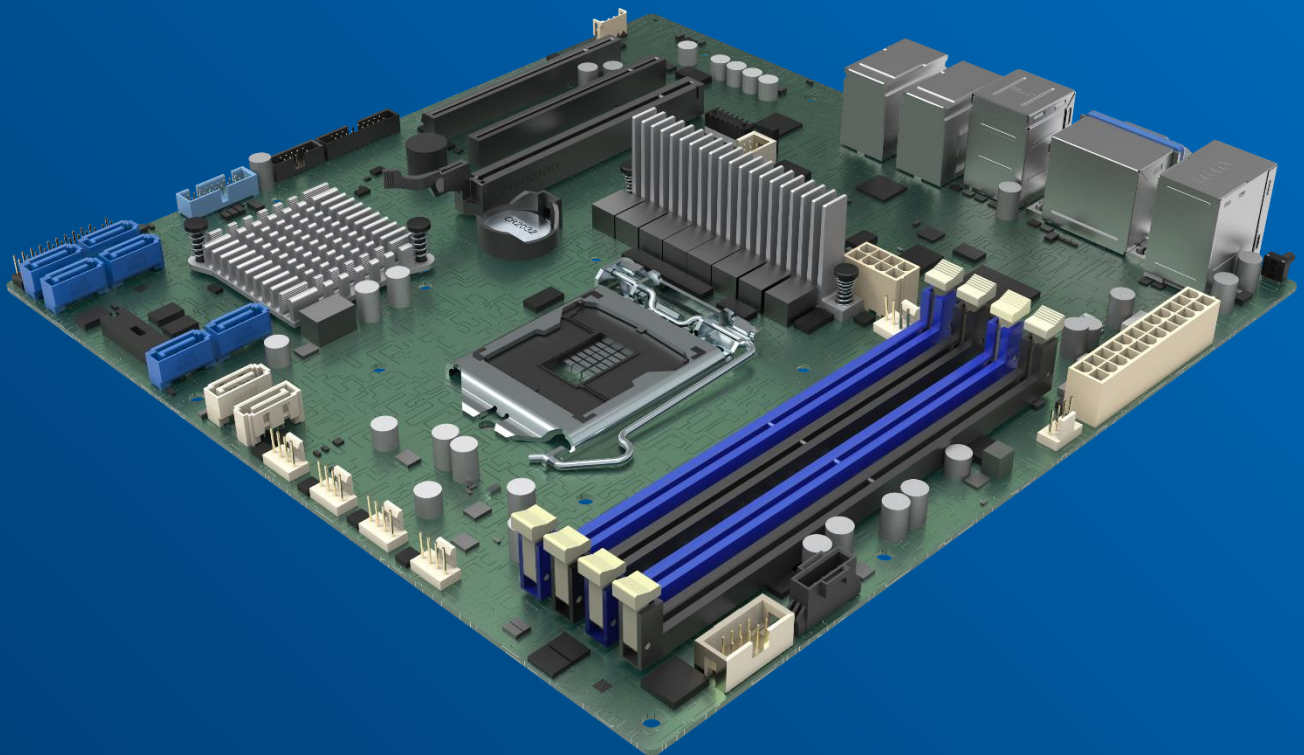
BMC Web Console user guide

A reference manual for access and configuration of
the BMC Web Console.

Rev 1.1

November 2019

M10JNP2SB



<Blank page>

Document Revision History

Date	Revision	Changes
October 2019	1.0	First Release.
November 2019	1.1	Deleted sections: - 3.10 Chassis Identify - 3.11 Set Front Panel Enables. Added note on section 3.9 Power Control

Disclaimers

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Copies of documents which have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Intel, and the Intel logo, are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.

© Intel Corporation

Table of Contents

1. Introduction.....	11
1.1 Support Information	11
1.2 Warranty Information	11
2. Integrated BMC Overview.....	12
2.1 BMC Features Overview.....	12
3. Integrated BMC Web Console Options	13
3.1 Integrated BMC Web Console Overview	13
3.1.1 Accessing the BMC Web Console	13
3.1.2 Main Menu Overview.....	14
3.1.3 Quick Buttons and User Permissions.....	15
3.2 Dashboard	17
3.3 Sensors	17
3.4 System Inventory.....	18
3.5 Field Replaceable Unit (FRU) Information.....	19
3.6 Logs & Reports.....	19
3.7 Settings.....	20
3.7.1 Date and Time.....	21
3.7.2 External User Services.....	22
3.7.3 KVM Mouse Setting	27
3.7.4 Log Settings	27
3.7.5 Media Redirection Settings	28
3.7.6 Network Settings	31
3.7.7 PAM Order Settings.....	33
3.7.8 Platform Event Filter	34
3.7.9 Services.....	38
3.7.10 SMTP Settings.....	39
3.7.11 SSL Settings.....	40
3.7.12 System Firewall	43
3.7.13 User Management.....	47
3.7.14 Video Recording.....	48
3.8 Remote Control	51
3.8.1 Remote KVM menu bar	52
3.9 Power Control.....	55
3.10 Maintenance	56
3.10.1 Backup Configuration	56
3.10.2 Firmware Image Location.....	57
3.10.3 Firmware Information.....	57
3.10.4 BIOS Information	58
3.10.5 Firmware Update	59

3.10.6	Preserve Configuration	60
3.10.7	Restore Configuration	61
3.10.8	Restore Factory Defaults	62
3.11	Sign Out.....	63
4.	BMC Port Number	64
Appendix A.	Glossary.....	65

List of Figures

Figure 1.	Login screen prompt.....	13
Figure 2.	Menu bar	14
Figure 3.	Logged in user information	15
Figure 4.	User management configuration menu	16
Figure 5.	Dashboard page	17
Figure 6.	Sensor reading page	17
Figure 7.	System inventory page.....	18
Figure 8.	FRU information page.....	19
Figure 9.	Logs and reports submenu	19
Figure 10.	IPMI event log page	20
Figure 11.	Video log page	20
Figure 12.	Settings page	20
Figure 13.	Date and time submenu icon.....	21
Figure 14.	Date and time page.....	21
Figure 15.	External user services submenu icon.....	22
Figure 16.	External user services page	22
Figure 17.	LDAP/E-directory settings page	22
Figure 18.	General LDAP settings page.....	23
Figure 19.	Role groups page	23
Figure 20.	Active directory settings page	24
Figure 21.	Active directory general settings page	24
Figure 22.	Active directory role groups page.....	24
Figure 23.	Radius settings page.....	25
Figure 24.	General RADIUS settings page	25
Figure 25.	Radius authorization window.	26
Figure 26.	KVM mouse setting submenu icon.....	27
Figure 27.	KVM mouse setting page.....	27
Figure 28.	Log settings submenu icon.....	27
Figure 29.	Log settings page.....	27
Figure 30.	Advanced log settings page	28
Figure 31.	Media redirection settings submenu icon	28
Figure 32.	Media redirection settings page	28

Figure 33. General settings page	29
Figure 34. VMedia instance settings page	29
Figure 35. Remote session page	30
Figure 36. Network settings submenu icon.....	31
Figure 37. Network settings menu	31
Figure 38. Network IP settings page.....	31
Figure 39. Network link configuration page.....	32
Figure 40. DNS configuration page.....	32
Figure 41. Sideband interface (NC-SI) page.....	33
Figure 42. PAM order settings submenu icon	33
Figure 43. PAM order settings page	33
Figure 44. Platform event filter submenu icon	34
Figure 45. Platform event filter page	34
Figure 46. Event filters page	34
Figure 47. Event filter configuration page.....	35
Figure 48. Alert policies page	35
Figure 49. Alert policies configuration page	36
Figure 50. LAN destinations page.....	36
Figure 51. LAN destination configuration page.....	37
Figure 52. Services submenu icon.....	38
Figure 53. Services page.....	38
Figure 54. SMTP settings submenu icon	39
Figure 55. SMTP settings page	39
Figure 56. SSL settings submenu icon	40
Figure 57. SSL settings page.....	40
Figure 58. View SSL certificate page	40
Figure 59. Generate SSL certificate page	41
Figure 60. Upload SSL certificate page	42
Figure 61. System firewall submenu icon	43
Figure 62. System firewall page	43
Figure 63. General firewall settings page	43
Figure 64. Existing firewall settings page	43
Figure 65. Add firewall settings page.....	44
Figure 66. IP firewall rules page	44
Figure 67. Existing IP rules page	44
Figure 68. Add IP rules page.....	45
Figure 69. Port firewall rules page	46
Figure 70. Existing port rules page.....	46
Figure 71. Add port rules page	46
Figure 72. User management submenu icon.....	47
Figure 73. User management page.....	47

Figure 74. Add user page	47
Figure 75. Video recording submenu icon.....	48
Figure 76. Video recording page.....	48
Figure 77. Auto video settings page	48
Figure 78. Video trigger settings page.....	49
Figure 79. Video remote storage page	49
Figure 80. Pre-event video recordings page.....	50
Figure 81. Remote control page.....	51
Figure 82. JViewer video redirection	51
Figure 83. Remote KVM page	52
Figure 84. Remote KVM menu bar	52
Figure 85. Power control menu	55
Figure 86. Chassis identify page.....	Error! Bookmark not defined.
Figure 87. Set front panel enables.....	Error! Bookmark not defined.
Figure 88. Maintenance page	56
Figure 89. Backup configuration submenu icon.....	56
Figure 90. Backup configuration page.....	56
Figure 91. Firmware image location submenu icon	57
Figure 92. Firmware image location page	57
Figure 93. Firmware information submenu icon	57
Figure 94. Firmware information page	57
Figure 95. BIOS information submenu icon	58
Figure 96. BIOS information page	58
Figure 97. Firmware update submenu icon.....	59
Figure 98. Firmware update page.....	59
Figure 99. Preserve configuration submenu icon.....	60
Figure 100. Preserve configuration page	60
Figure 101. Restore configuration submenu icon	61
Figure 102. Restore configuration page	61
Figure 103. Restore configuration confirmation prompt	61
Figure 104. Restore factory defaults submenu icon.....	62
Figure 105. Restore factory defaults page.....	62
Figure 106. Logout dialog box	63
Figure 107. Root icon logout	63
Figure 108. Logout confirmation prompt	63

List of Tables

Table 1. User permissions	15
Table 2. BMC port numbers	64

<Blank Page>

1. Introduction

This user guide describes the Integrated Baseboard Management Controller (Integrated BMC) web console and its related graphical user interface (GUI) for the Intel® M10JNP2SB Server Board. It provides an overview of the features of the GUI along with instructions on how to configure the BMC for use.

1.1 Support Information

For additional support, visit <https://www.intel.com/content/www/us/en/support.html>. This support page provides the following:

- Latest BIOS, firmware, drivers and utilities.
- Product documentation, installation guides, and quick start guides.
- Full product specifications, technical advisories, and errata.
- Compatibility documentation for memory, hardware add-in cards, chassis support matrices, and operating systems.
- Server and chassis accessory parts list for ordering upgrades and spare parts.
- Searchable knowledgebase of product information.

For further assistance, contact Intel customer support at <http://www.intel.com/support/feedback.htm>.

1.2 Warranty Information

To obtain warranty information, visit

<https://www.intel.com/content/www/us/en/support/articles/000006361/services.html>

2. Integrated BMC Overview

The Integrated BMC web console provides both stability and permanent availability independent of the present state of the server's operating system. The Integrated BMC web console can be used as a tool to gain location-independent remote access to respond to critical incidents and to undertake necessary maintenance.

2.1 BMC Features Overview

The Integrated BMC provides several management features that enable support for the following:

- Control system functions: power system, ACPI, system reset control, system initialization, front panel control, and the system event log.
- Monitor various board and system sensors and regulate platform thermals and performance to maintain (when possible) server functionality in the event of component failure and/or environmentally stressed conditions.
- Monitor and report system health.

The Integrated BMC supports the following features:

- Sensor monitoring
- In-Circuit BMC firmware update
- Chassis intrusion detection
- FRU information
- Logging and reporting
- Remote control
- Image redirection
- Power control
- Chassis identify
- Front panel control
- Configuration backup
- External user services
- Platform event filtering
- SMTP messaging
- Video recording
- User management
- Embedded firewall

Note: The Integrated BMC firmware is fully compliant with the IPMI 2.0 specification.

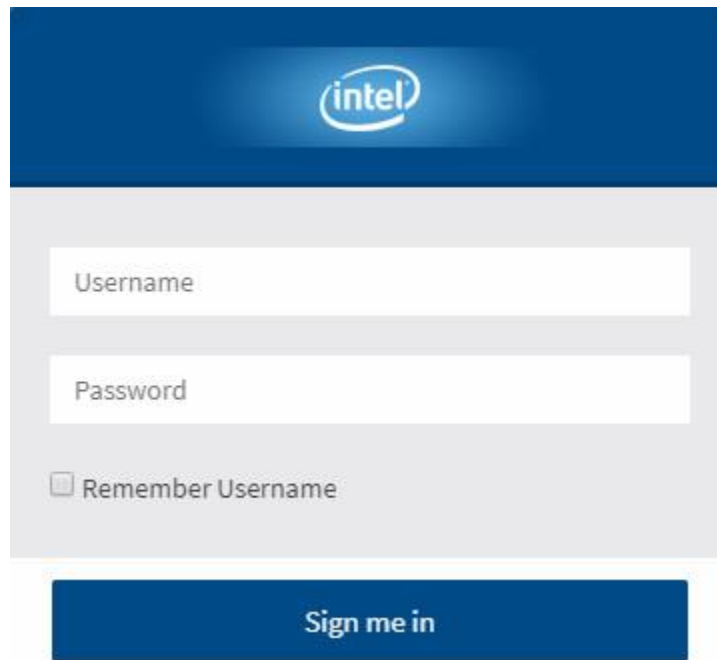
3. Integrated BMC Web Console Options

3.1 Integrated BMC Web Console Overview

The Integrated BMC includes a generic, user-friendly Graphics User Interface (GUI) for the web console. The GUI is accessible via a standard Internet browser for ease of use.

3.1.1 Accessing the BMC Web Console

Initial access of the BMC web console GUI prompts the entering of a user name and a password. Figure 1 shows the authentication dialog.



The image shows a login screen for the BMC Web Console. At the top, there is a dark blue header with the Intel logo. Below the header, there is a light gray background containing the following elements: a white input field labeled "Username", a white input field labeled "Password", a checkbox labeled "Remember Username", and a dark blue button labeled "Sign me in".

Figure 1. Login screen prompt

3.1.2

3.1.2 Main Menu Overview

The Integrated BMC web console consists of various menu items containing submenus and options. The following sections detail the different options of each submenu.

3.1.2.1 Menu Bar

The menu bar displays the following:

- Dashboard
- Sensor
- System Inventory
- FRU Information
- Logs & Reports
- Settings
- Remote Control
- Image Redirection
- Power Control
- Chassis Identify
- Set Front Panel Enables
- Maintenance
- Sign Out

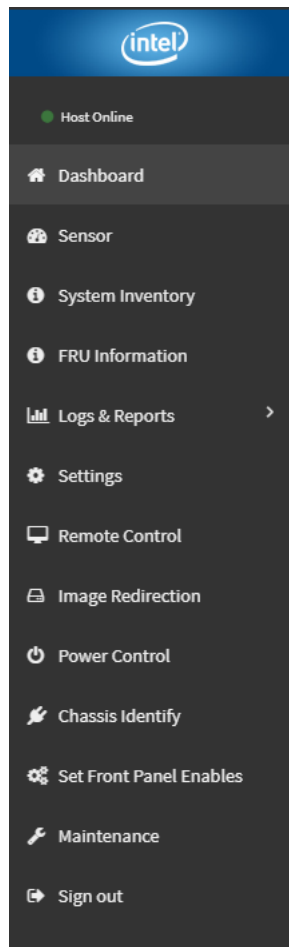


Figure 2. Menu bar

3.1.3 Quick Buttons and User Permissions





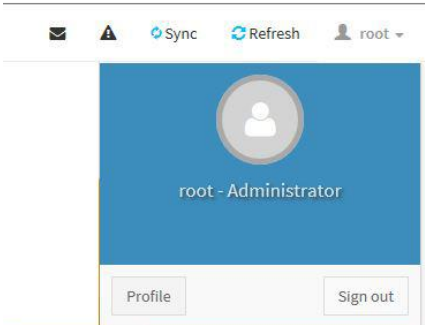
The user information and quick buttons are located at the top right of the MegaRAC* GUI. Figure 3 shows a screenshot of the logged-in user information.



Figure 3. Logged in user information

Table 1 shows the logged-in user, privilege level, and the four quick buttons allowing the user to perform other functions.

Table 1. User permissions

User	Result
Operator	All BMC commands are allowed except for the configuration commands that can change the behavior of the out of hand interfaces.
Administrator	All BMC commands are allowed.
No Access	Login access denied.
	Notification: Select the icon to view the notification messages.
	Warning: Select the icon to view the warning messages.
	Sync: Select the icon to synchronize with Latest Sensor and Event Log updates.
	Refresh: Select the icon to reload the current page.
	<p>root - Administrator</p> <p>Sign out: Select the Sign out icon to log out of the MegaRAC GUI.</p> <p>Profile: Select the icon to enter the User Management Configuration dialog box.</p>

The screenshot displays the 'User Management Configuration' page. At the top, there is a navigation bar with a hamburger menu, notification icons, 'Sync', 'Refresh', and a user profile 'root'. Below the navigation is a breadcrumb trail: Home > Settings > User Management > User Management Configuration. The main content area is titled 'User Management Configuration' and contains a form for configuring a user. The form includes the following fields and controls:

- Username:** A text input field containing 'root'.
- Change Password:** An unchecked checkbox.
- Password Size:** A dropdown menu set to '16 bytes'.
- Password:** A text input field.
- Confirm Password:** A text input field.
- Enable User Access:** A checked checkbox.
- Network Privilege:** A dropdown menu set to 'Administrator'.
- Serial Privilege:** A dropdown menu set to 'None'.
- Email Format:** A dropdown menu set to 'AMI-Format'.
- Email ID:** A text input field.
- Existing SSH Key:** A text input field containing 'Not Available'.
- Upload SSH Key:** A text input field with a blue button containing a file icon and '...'.
- Buttons:** A red 'Delete' button and a blue 'Save' button with a file icon.

Figure 4. User management configuration menu

3.2 Dashboard

The Dashboard page provides general information concerning the status of the server board. To access the Dashboard page, select **Dashboard** from the menu bar.

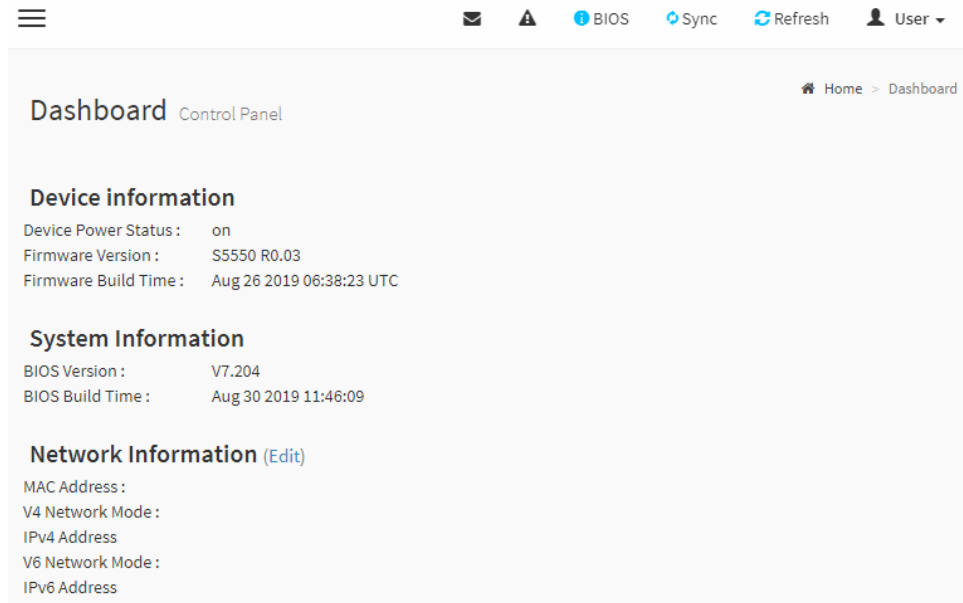


Figure 5. Dashboard page

3.3 Sensors

The Sensor Reading page provides all sensor related information. To access the Sensor Reading page, select **Sensor** from the menu bar. Click on a record to display more information about that particular sensor, including thresholds and a graphical representation of all associated events.

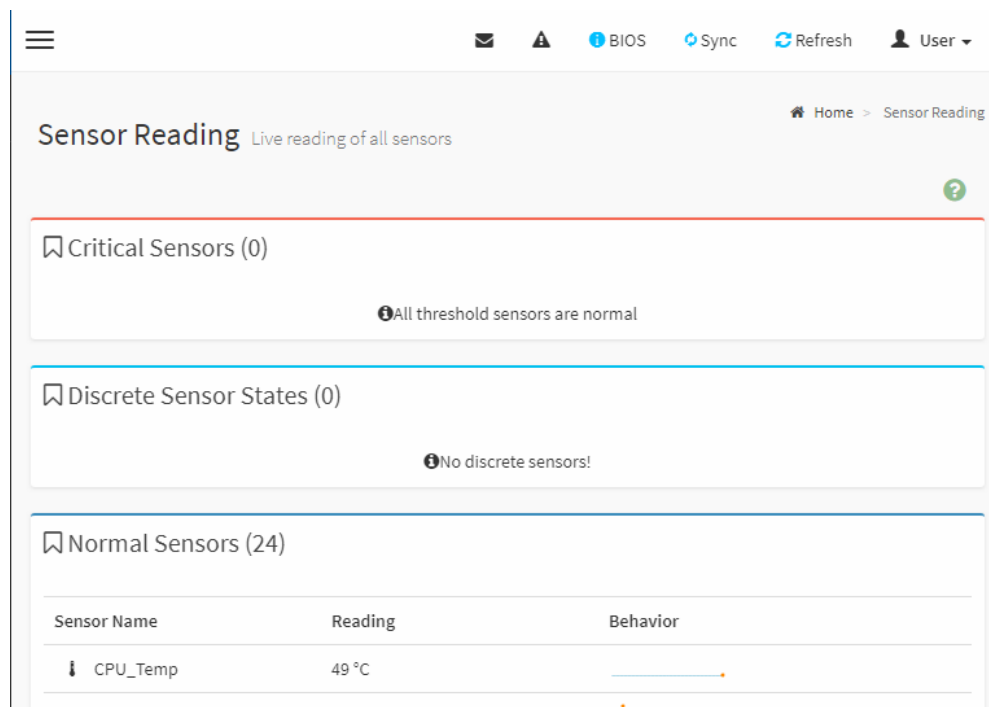


Figure 6. Sensor reading page

3.4 System Inventory

The System Inventory page displays information about the Processor, Memory (DIMMs) and PCIe* devices that are installed on the system, including the vendor name, model, and software version. To access the System Inventory page, select **System Inventory** from the menu bar.

System Inventory Information

Home > System Inventory > System Inventory Information

🔖 CPU Information (1)

CPU Index	Device Present	Brand Name	Core Count	Max Frequency
0	Yes	Intel(R) Xeon(R) E-2236 CPU @ 3.40GHz	6	3400MHz

🔖 DIMM Information (4)

DIMM Slot	Device Present	Frequency	Size	Type	Manufacturer Name	Part Number
P0_MC0_DIM_CH_A0	Yes	2666MHz	32768MB	DDR4	Samsung	M378A4G43MB1-CTD
P0_MC0_DIM_CH_A1	Yes	2666MHz	32768MB	DDR4	Samsung	M378A4G43MB1-CTD
P0_MC0_DIM_CH_B0	Yes	2666MHz	32768MB	DDR4	Samsung	M378A4G43MB1-CTD
P0_MC0_DIM_CH_B1	Yes	2666MHz	32768MB	DDR4	Samsung	M378A4G43MB1-CTD

🔖 PCI Device Information (3)

Figure 7. System inventory page

3.5 Field Replaceable Unit (FRU) Information

The Field Replaceable Unit (FRU) Information page displays information from the FRU repository of the server board. The information provided on this page includes basic information, chassis information, board information and product information of the FRU device. To access the FRU Information page, select **FRU Information** from the menu bar. Select a FRU Device ID from the Basic Information section to view the details of the selected device.

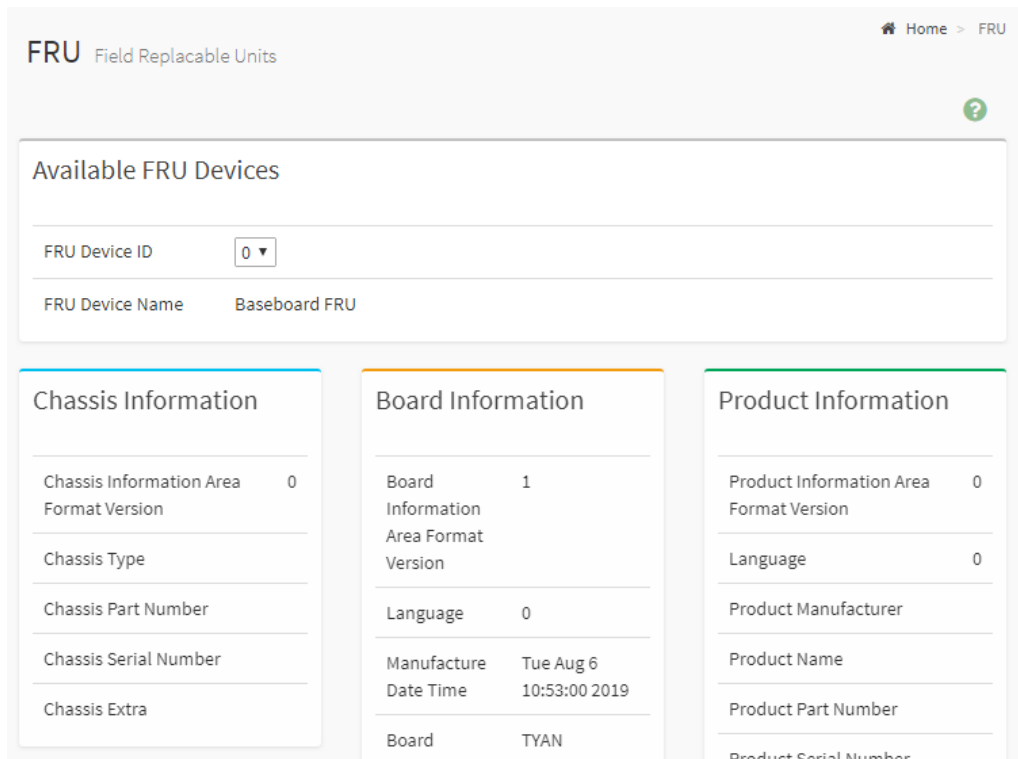


Figure 8. FRU information page

3.6 Logs & Reports

The Logs & Reports page contains both the IPMI Event Log and the Video Log. To access the Logs & Reports page, select **Logs & Reports** from the menu bar. Select **IPMI Event Log**, or **Video Log** to view the contents.

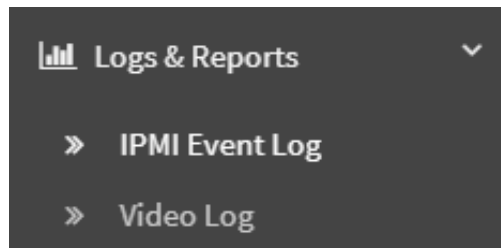


Figure 9. Logs and reports submenu

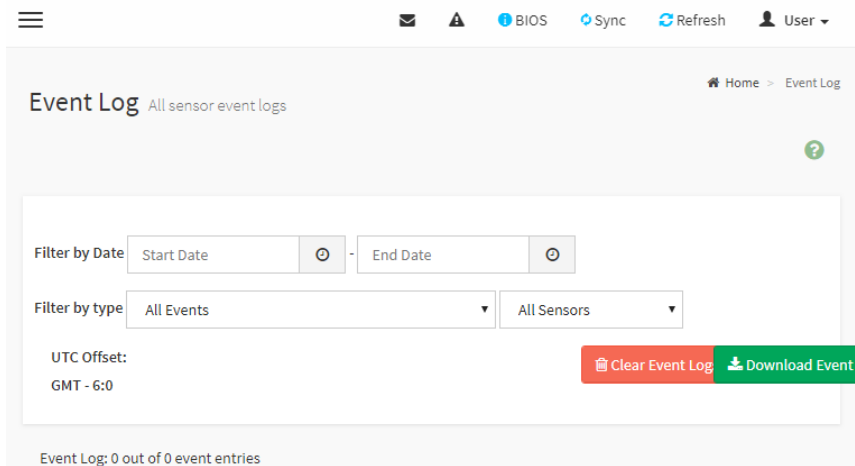


Figure 10. IPMI event log page

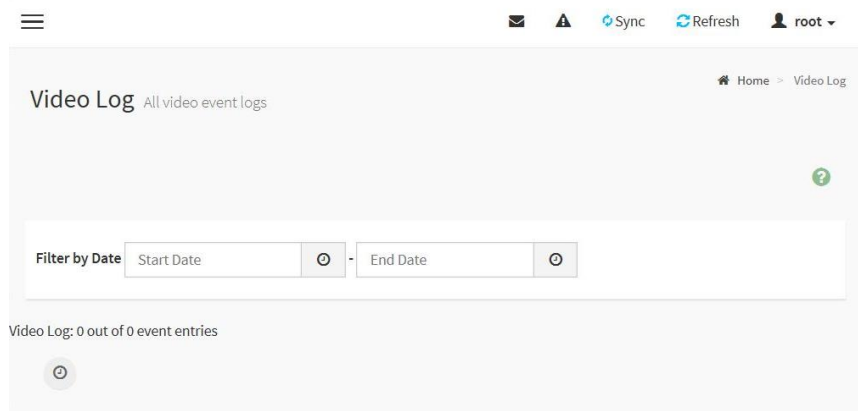


Figure 11. Video log page

3.7 Settings

The Settings page provides access to several submenus described in the following subsections.

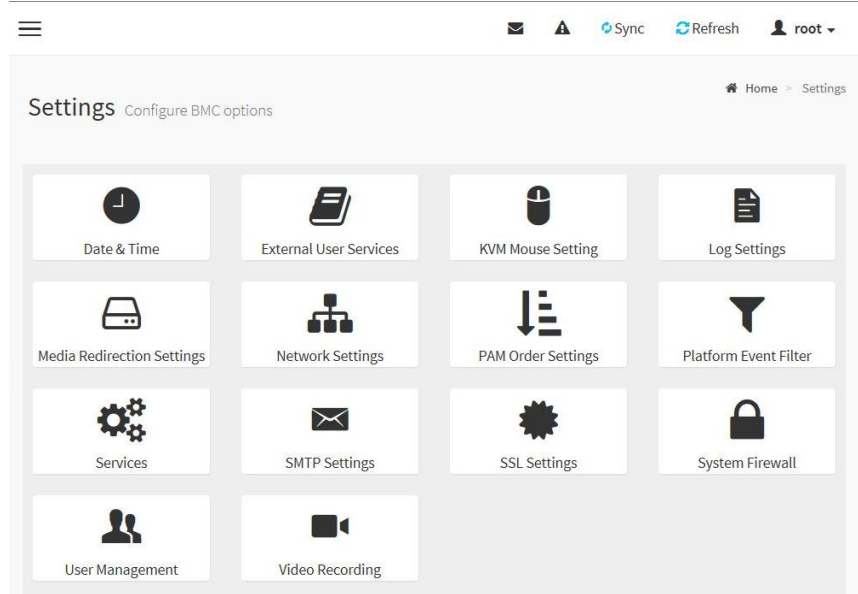


Figure 12. Settings page

3.7.1 Date and Time

Date and time for the server can be set on this configuration page. To access the Date and Time submenu page, select **Settings** → **Date & Time** from the menu bar.

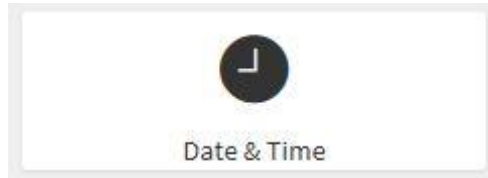


Figure 13. Date and time submenu icon

. An interface with a world map can be used to set a specific time zone as shown in Figure 14..

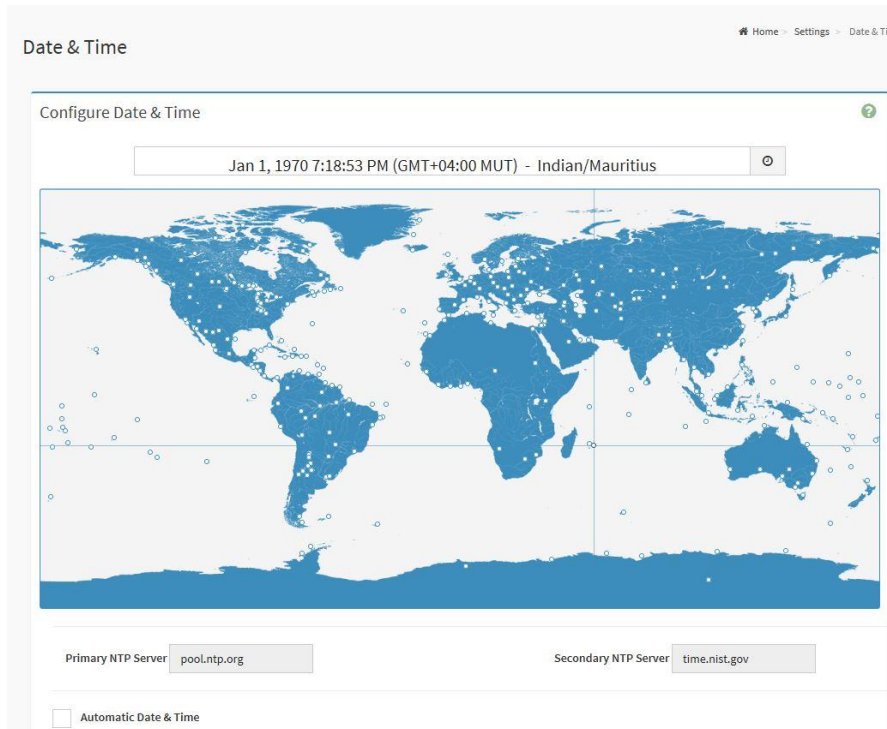


Figure 14. Date and time page

3.7.2 External User Services

The External User Services page displays multiple submenus containing configuration options. To access the External User Services page, select **Settings** → **External User Services** from the menu bar.



Figure 15. External user services submenu icon

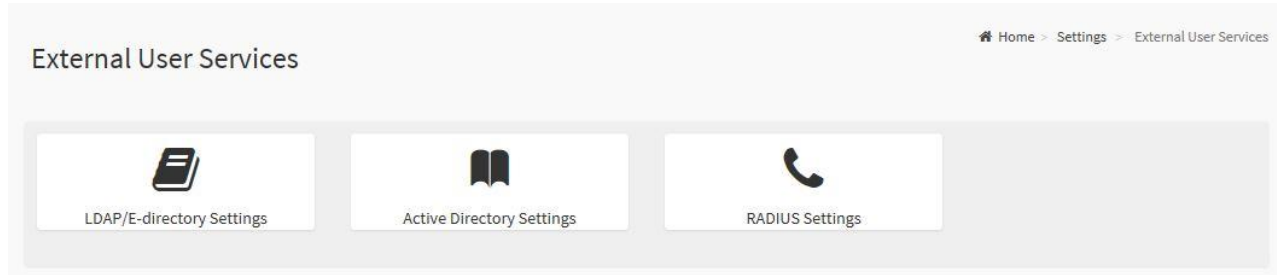


Figure 16. External user services page

3.7.2.1 LDAP/E-directory Settings

The LDAP settings page is used to enable/disable the LDAP settings on the server management LAN. To access the LDAP/E-directory settings page, select **Settings** → **External User Services** → **LDAP/E-directory Settings** from the menu bar.

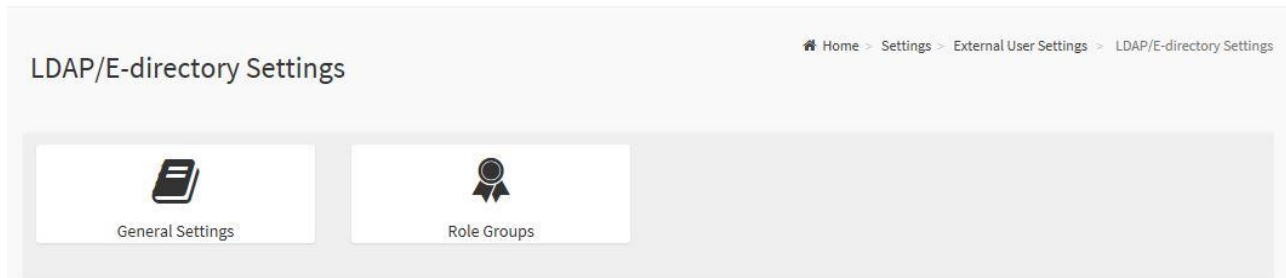


Figure 17. LDAP/E-directory settings page

The following submenus within the LDAP/E-directory settings page can be configured:

- **General Settings:** Configures LDAP/E-directory settings and contains the following elements:
 - Enable LDAP/E-directory Authentication
 - IP Address
 - Port
 - Search base.

Figure 18. General LDAP settings page

- **Role Groups:** Allows to add a new role group to the device. Alternatively, double click a free slot to add a role group.

Figure 19. Role groups page

3.7.2.2 Active Directory Settings

The Active Directory settings page is used to enable/disable the Active Directory settings on the server management LAN. To access the Active directory Settings page, click **Settings** → **External User Services** → **Active directory Settings** from the menu bar.

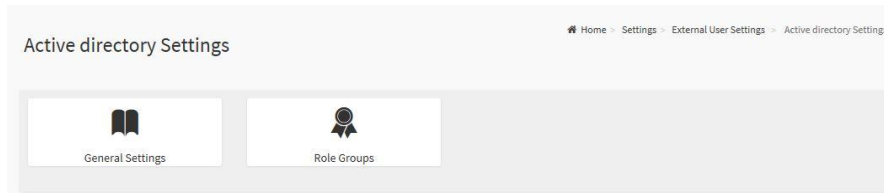


Figure 20. Active directory settings page

The following submenus within the Active directory Settings page can be configured:

- **General Settings:** This submenu is used to configure Active Directory General Settings and contains the following elements:
 - Enable Active Directory Authentication
 - Secret User Name
 - Secret Password
 - User Domain name
 - Up to three Domain Controller Server Addresses.

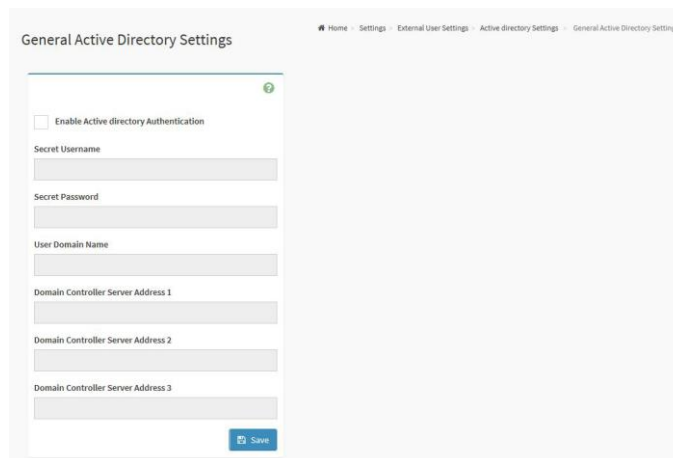


Figure 21. Active directory general settings page

- **Role Groups:** Allows to add a new role group to the device. Alternatively, double click a free slot to add a role group.



Figure 22. Active directory role groups page

3.7.2.3 RADIUS Settings

The RADIUS settings page is used to enable/disable the RADIUS authentication settings on the server management LAN. To access the RADIUS settings page, select **Settings** → **External User Services** → **RADIUS Settings** from the menu bar.

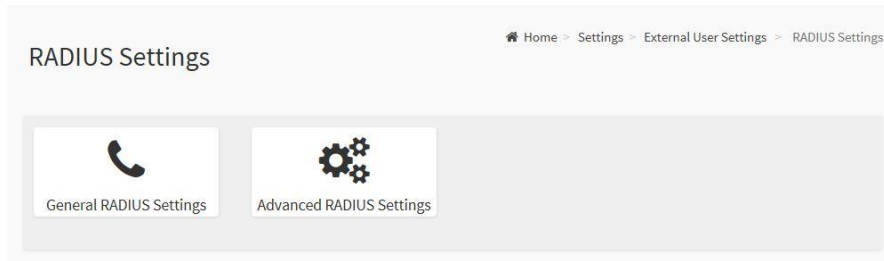


Figure 23. Radius settings page

The following elements within the general RADIUS settings page can be configured:

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

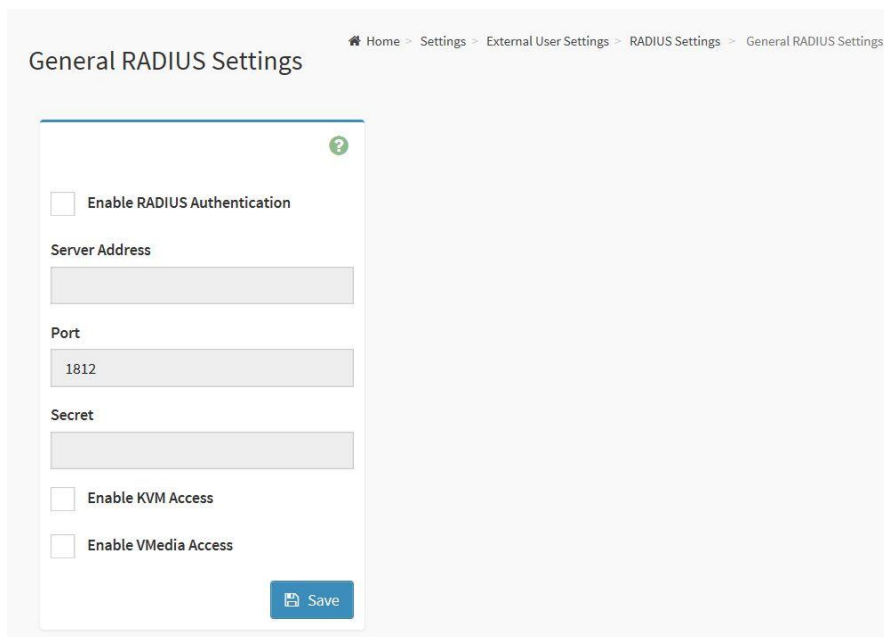


Figure 24. General RADIUS settings page

Note:

- IP Address (Both IPv4 and IPv6 format)
 - FQDN (Fully Qualified Domain Name) format
-

- **Port:** The RADIUS Port number.
-

Note:

- Default Port is 1812.
 - Port value ranges from 1 to 65535
-

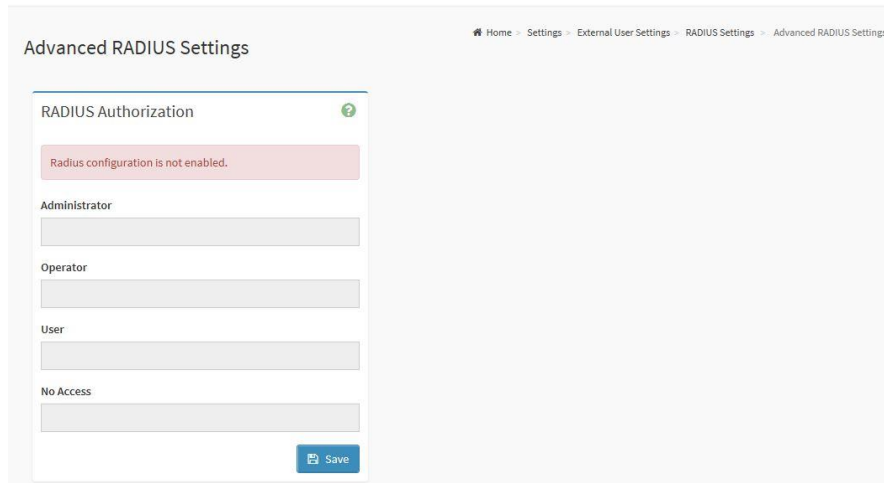
Secret: The Authentication Secret for RADIUS server.

Note:

- This field does not allow more than 31 characters.
- Secret must be at least 4 characters long.
- White space is not allowed.

- **Enable KVM Access:** Access to KVM for RADIUS authentication users.
- **Enable VMedia Access:** Access to VMedia for RADIUS authentication users.
- **Save:** Save the settings.

To access the RADIUS authorization window, select **Advanced RADIUS Settings**.



Advanced RADIUS Settings

Home > Settings > External User Settings > RADIUS Settings > Advanced RADIUS Settings

RADIUS Authorization

Radius configuration is not enabled.

Administrator

Operator

User

No Access

Save

Figure 25. Radius authorization window.

Select **Save** to save the changes made.

3.7.3 KVM Mouse Setting

The KVM Mouse Setting page is used to configure positioning options for the pointer device in a KVM session. To access the KVM Mouse Setting page, select **Settings** → **KVM Mouse Setting** from the menu bar.

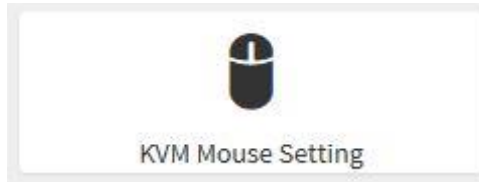


Figure 26. KVM mouse setting submenu icon

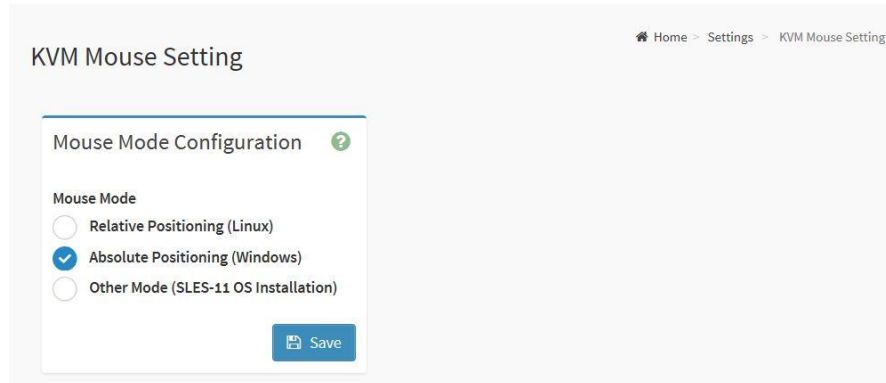


Figure 27. KVM mouse setting page

Select **Save** to save the changes made.

3.7.4 Log Settings

The Log Settings page is used to configure Logging options for the System Event Log (SEL). To access the log settings page, select **Settings** → **Log Settings** from the menu bar.

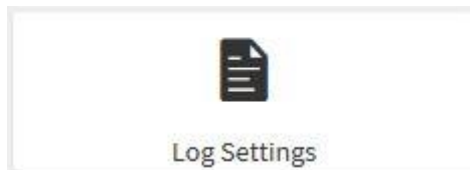


Figure 28. Log settings submenu icon

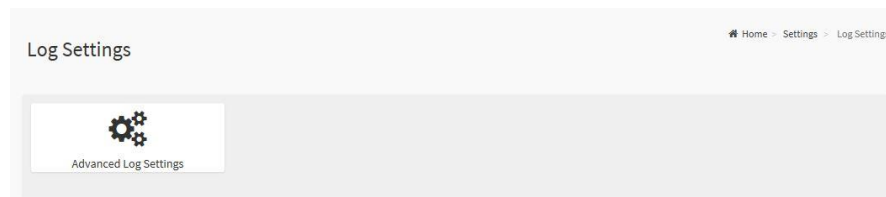


Figure 29. Log settings page

To access the advanced log settings page, select **Settings** → **Log Settings** → **Advanced Log Settings** from the menu bar.

Figure 30. Advanced log settings page

Select **Save** to save changes.

3.7.5 Media Redirection Settings

The Media Redirection Settings page displays multiple submenus containing configuration options. To access the Media Redirection Settings page, select **Settings** → **Media Redirection Settings** from the menu bar.



Figure 31. Media redirection settings submenu icon

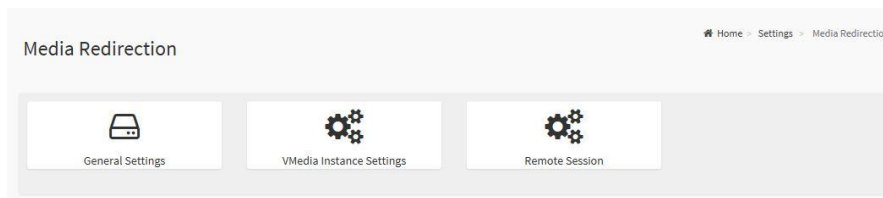


Figure 32. Media redirection settings page

3.7.5.1 General Settings

Use this page to enable or disable remote media support and configure options for the different media origins. If this option is enabled, then following remote media types will be displayed:

- Mount CD/DVD
- Mount Floppy
- Mount Hard disk

Upon selecting the individual media types, their respective configurations will be displayed. To access the general settings page, select **Settings** → **Media Redirection Settings** → **General Settings** from the menu bar.

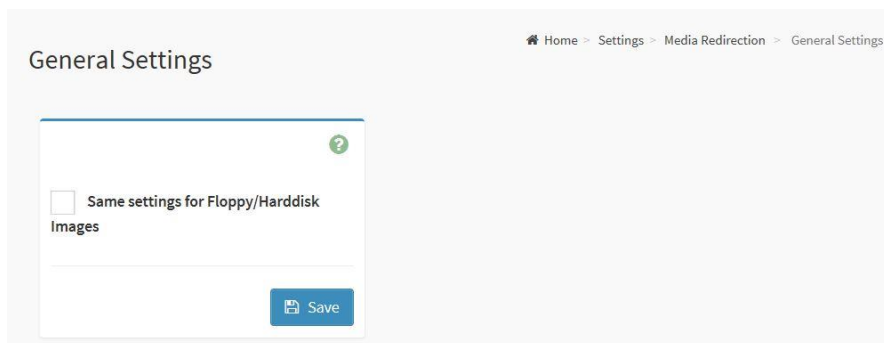


Figure 33. General settings page

Select **Save** to save the changes made.

3.7.5.2 VMedia Instance Settings

Use this page to set the number of virtual device instances to be supported for virtual media redirection. To access the VMedia Instance Settings page, select **Settings** → **Media Redirection Settings** → **VMedia Instance Settings** from the menu bar.

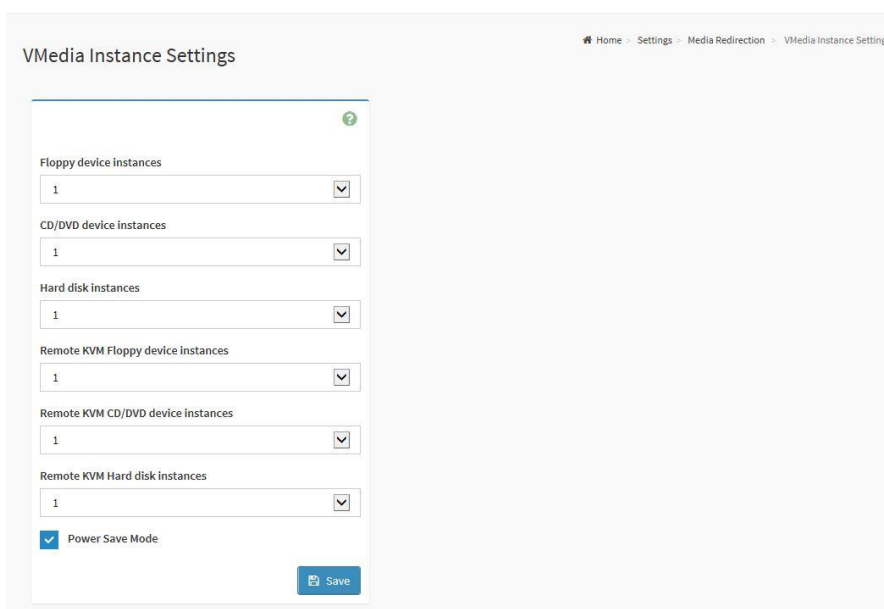


Figure 34. VMedia instance settings page

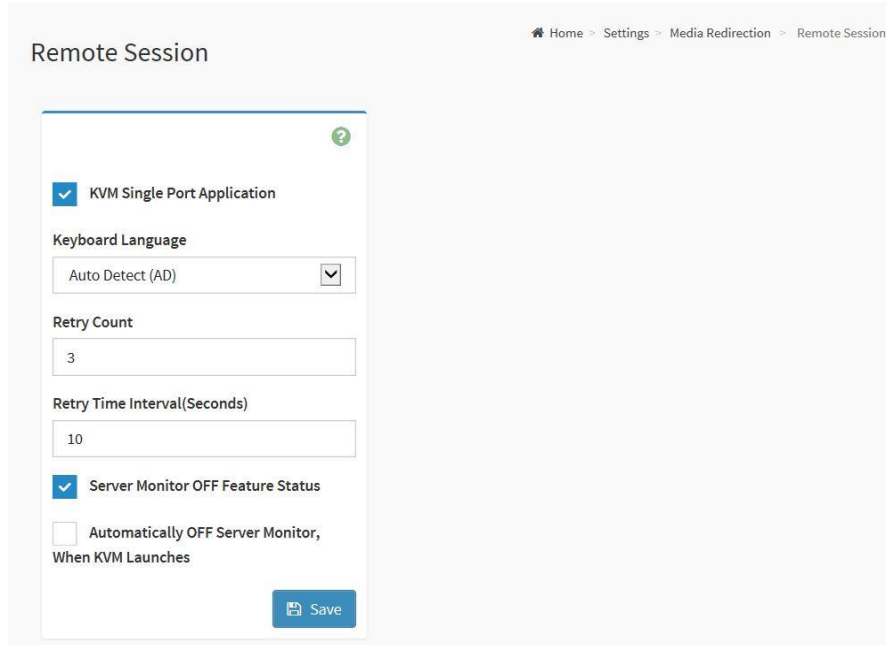
Select **Save** to save the changes made.

3.7.5.3 Remote Session

Use this page to enable/disable KVM Encryption when using H5Viewer.

Note: If Single Port Application support is enabled, KVM Encryption will NOT be set.

To access the Remote Session page, select **Settings** → **Media Redirection Settings** → **Remote Session** from the menu bar.



The screenshot shows the 'Remote Session' configuration page. At the top right, there is a breadcrumb trail: Home > Settings > Media Redirection > Remote Session. The page title is 'Remote Session'. A help icon (?) is in the top right corner of the configuration box. The configuration options are:

- KVM Single Port Application
- Keyboard Language: Auto Detect (AD) (dropdown menu)
- Retry Count: 3 (text input)
- Retry Time Interval(Seconds): 10 (text input)
- Server Monitor OFF Feature Status
- Automatically OFF Server Monitor, When KVM Launches

A 'Save' button is located at the bottom right of the configuration box.

Figure 35. Remote session page

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

3.7.6 Network Settings



Figure 36. Network settings submenu icon

The Network Settings page displays multiple submenus containing configuration options. To access the Network settings page, select **Settings** → **Network Settings** from the menu bar.

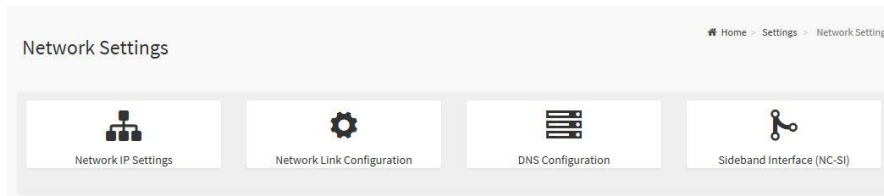


Figure 37. Network settings menu

3.7.6.1 Network IP Settings

Use this page to configure the network settings for the management network.

Note: Enabling/Disabling LAN support for the eth0 device is controlled by BIOS, and enabled by default in this page.

To access the Network IP Settings page, select **Settings** → **Network Settings** → **Network IP Settings** from the menu bar.

Network IP Settings

Home - Settings - Network - Network IP Settings

Enable LAN

LAN Interface: eth0

MAC Address: Ab:42:3f:37:0b:79

Enable IPv4

Enable IPv4 DHCP

IPv4 Address: 10.99.241.135

IPv4 Subnet: 255.255.254.0

IPv4 Gateway: 10.99.241.254

Enable IPv6

Enable IPv6 DHCP

IPv6 Index: 0

IPv6 Address: ::

Subnet Prefix Length

Figure 38. Network IP settings page

Click **Save** to save the entries.

3.7.6.2 Network Link Configuration

To access the Network Link Configuration page, select **Settings** → **Network Settings** → **Network Link Configuration** from the menu bar.

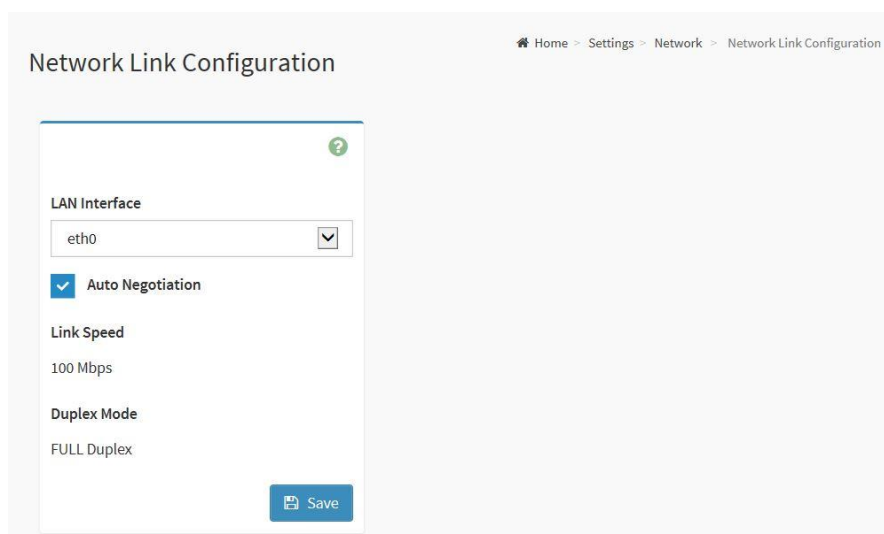


Figure 39. Network link configuration page

Click **Save** to save the entries.

3.7.6.3 DNS Configuration

To access the DNS Configuration page, select **Settings** → **Network Settings** → **DNS Configuration** from the menu bar.

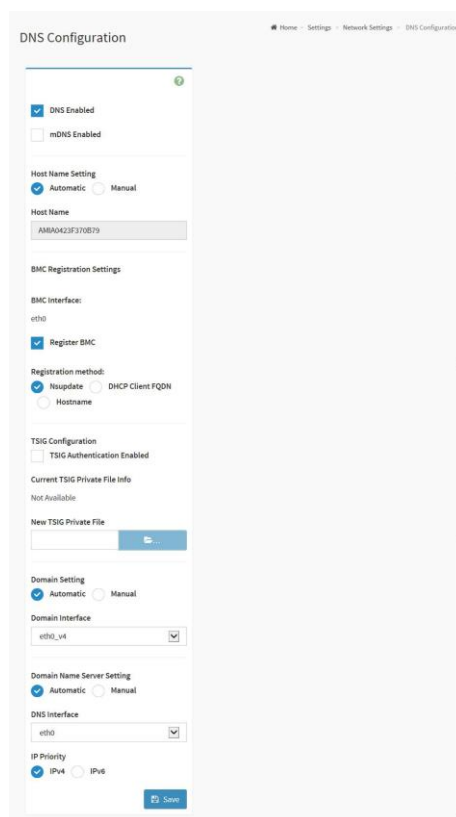


Figure 40. DNS configuration page

Click **Save** to save the entered changes.

3.7.6.4 Sideband Interface (NC-SI)

To access the Sideband Interface (NC-SI) page, select **Settings** → **Network Settings** → **Sideband Interface (NC-SI)** from the menu bar.

Figure 41. Sideband interface (NC-SI) page

Click **Save** to save the current changes.

3.7.7 PAM Order Settings

Use this page to configure the PAM order for user authentication into the Integrated BMC. The configuration page shows the list of available PAM modules supported in the BMC. Click and Drag the required PAM module to change its order.



Figure 42. PAM order settings submenu icon

To access the PAM Order Settings page, select **Settings** → **PAM Order Settings** from the menu bar.

Figure 43. PAM order settings page

Click **Save** to save the changes.

3.7.8 Platform Event Filter

The Platform Event Filter page displays multiple submenus containing configuration options. To access the Platform Event Filter page, select **Settings** → **Platform Event Filter** from the menu bar.

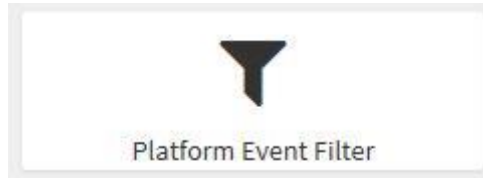


Figure 44. Platform event filter submenu icon

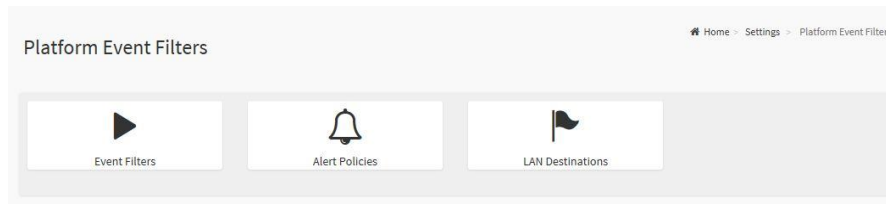


Figure 45. Platform event filter page

3.7.8.1 Event Filters

The Event Filters page shows all configured Event filters and available slots. Use this page to modify or add new event filter entries. By default, 15 event filter entries are configured among the 40 available slots. To access the Event Filters page, select **Settings** → **Platform Event Filters** → **Event Filters** from the menu bar.

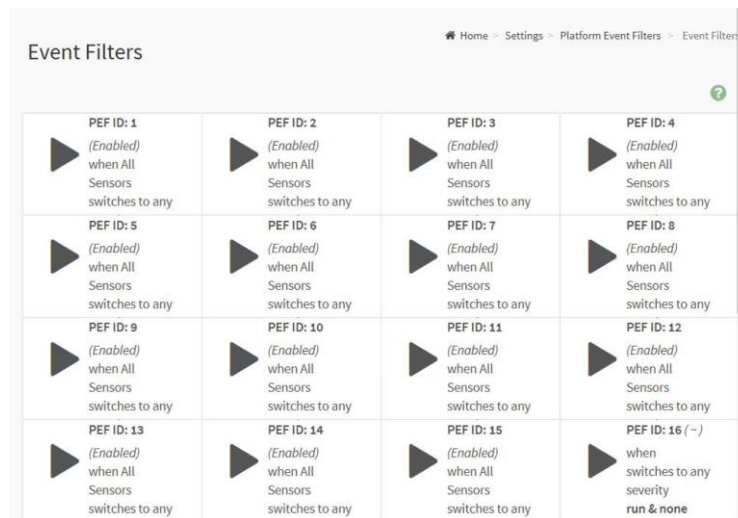


Figure 46. Event filters page

Select a specific event filters section to configure the event filters in the available slots. To add an event filter, select a free section to access the event filter entry page. Select **Save** to save the changes and return to event filter list.

Select **Delete** to delete the existing filter.

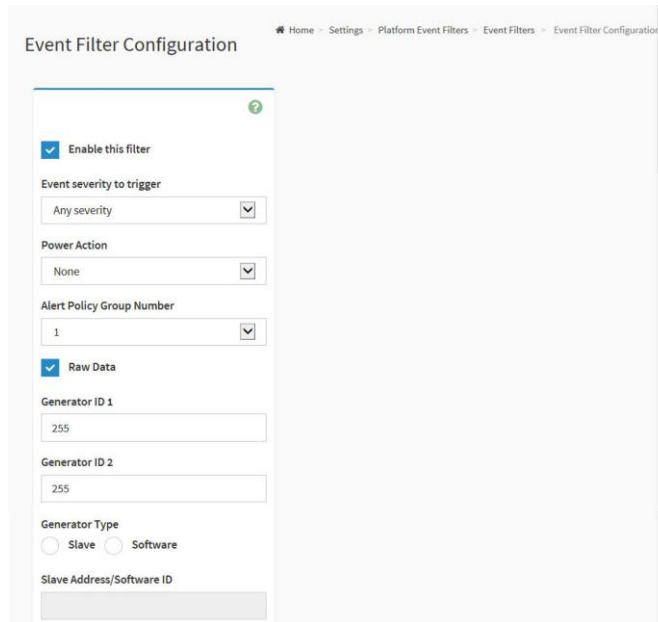


Figure 47. Event filter configuration page

3.7.8.2 Alert Policies

The Alert Policies page shows all configured Alert policies and available slots. Use this page to modify or add new alert policy entries. A maximum of 60 slots are available. To access the Alert Policies page, select **Settings** → **Platform Event Filters** → **Alert Policies** from the menu bar.

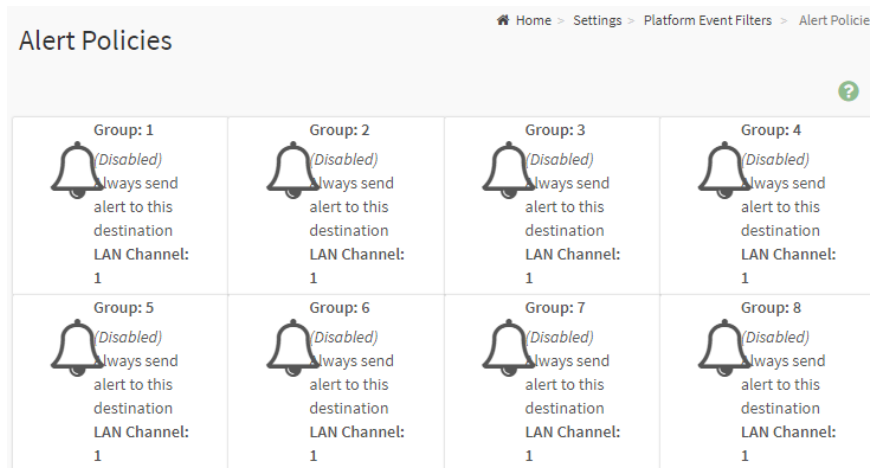


Figure 48. Alert policies page

On the Alert Policies page, select a specific slot to configure the Alert Policy. If alert policy group four is chosen, the fourth slot must be configured (the slot with policy number four) in the alert policy tab.

Select the slot and select the empty slot to access the Alert Policies page as shown in Figure 49. Select **Save** to save the new alert policy and return to Alert Policy list.

Select **Delete** to delete a configuration.

Figure 49. Alert policies configuration page

3.7.8.3 LAN Destinations

This page is used to configure the LAN Destination of a Platform Event Filtering (PEF) configuration. To access the LAN Destinations Page, select **Settings** → **Platform Event Filters** → **LAN Destinations** from the menu bar.

Figure 50. LAN destinations page

On the LAN Destinations page, choose the number of slots to be configured. This should be the same number of slots that are selected in the Alert Policies – Destination Selector field. For example, if the Destination Selector is set to four on the Alert Policies page within the Alert Policies submenu, then the fourth slot of the LAN Destinations page must also be configured.

Select an empty slot, and access the LAN Destination entry. Select **Save** to add a new entry to the device. Alternatively, double click on a free slot.

Select **Delete** to delete the selected configured LAN Destination.

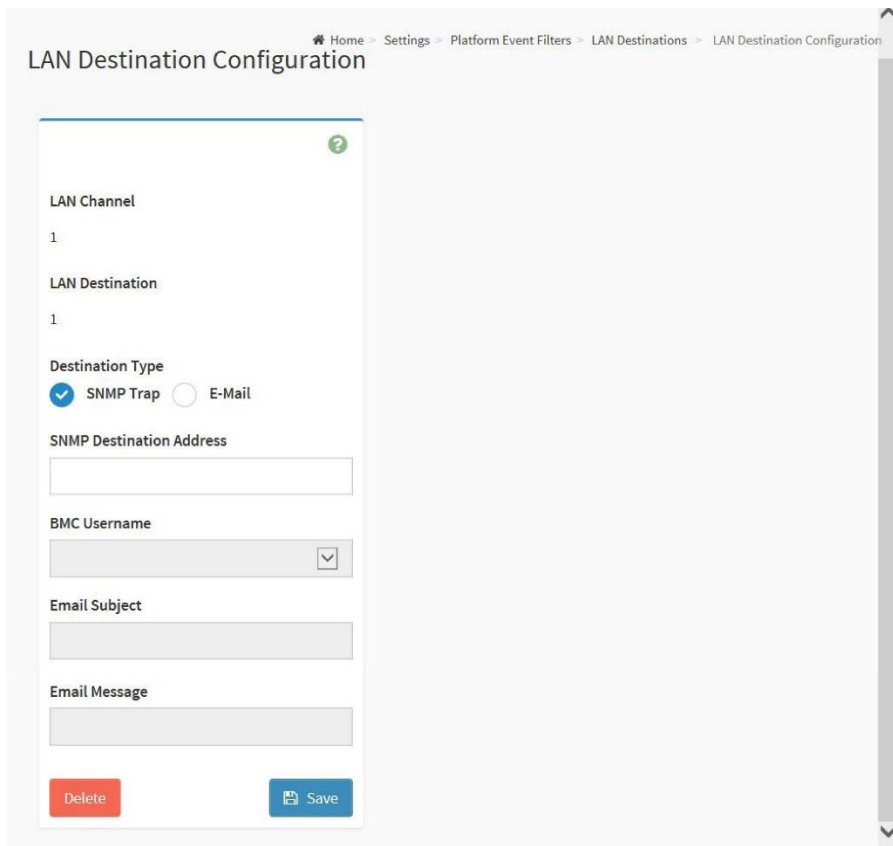


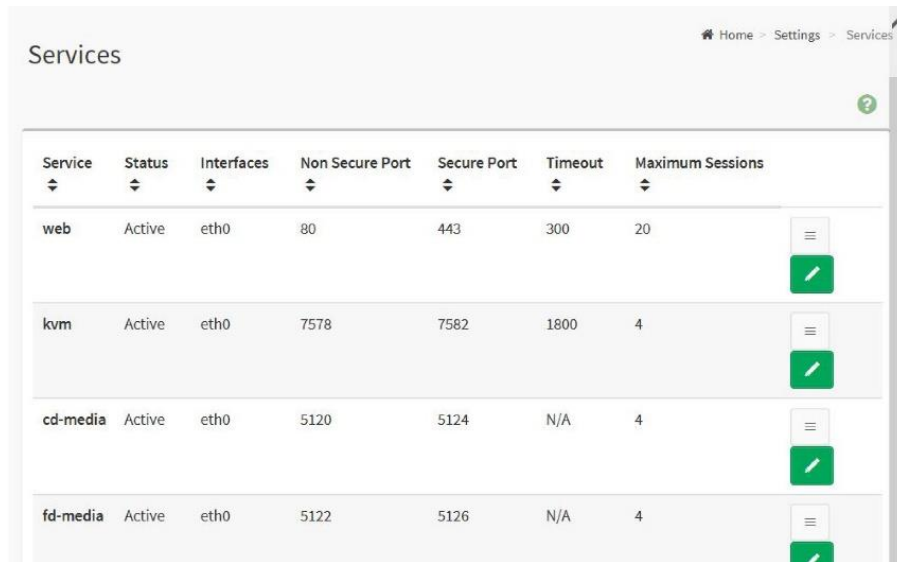
Figure 51. LAN destination configuration page

3.7.9 Services

The Services page displays basic information concerning services running in the Integrated BMC. Only users with administrator privileges can modify services. To access the Services page, select **Settings** → **Services** from the menu bar.



Figure 52. Services submenu icon

A screenshot of the BMC web console's Services page. The page has a breadcrumb trail "Home > Settings > Services" in the top right corner. Below the breadcrumb is a table with columns for Service, Status, Interfaces, Non Secure Port, Secure Port, Timeout, and Maximum Sessions. There are four rows of service data. Each row has a vertical menu icon on the right side, which includes a pencil icon for editing.

Service	Status	Interfaces	Non Secure Port	Secure Port	Timeout	Maximum Sessions
web	Active	eth0	80	443	300	20
kvm	Active	eth0	7578	7582	1800	4
cd-media	Active	eth0	5120	5124	N/A	4
fd-media	Active	eth0	5122	5126	N/A	4

Figure 53. Services page

3.7.10 SMTP Settings

Use this page to enable/disable SMTP support and configure its settings. To access the SMTP Settings page, select **Settings** → **SMTP Settings** from the menu bar.



Figure 54. SMTP settings submenu icon

A screenshot of the SMTP Settings page in a web console. The page title is "SMTP Settings" and the breadcrumb navigation is "Home > Settings > SMTP Settings". The form contains the following fields and options:

- LAN Interface: A dropdown menu with "eth0" selected.
- Sender Email ID: An empty text input field.
- Primary SMTP Support: A checked checkbox.
- Primary Server Name: An empty text input field.
- Primary Server IP: An empty text input field.
- Primary SMTP port: A text input field with "25" entered.
- Primary Secure SMTP port: A text input field with "465" entered.
- Primary SMTP Authentication: An unchecked checkbox.
- Primary Username: An empty text input field.
- Primary Password: An empty text input field.
- Primary SMTP SSLTLS Enable: An unchecked checkbox.
- Primary SMTP STARTTLS Enable: An unchecked checkbox.
- Secondary SMTP Support: An unchecked checkbox.

A blue "Save" button is located at the bottom right of the form.

Figure 55. SMTP settings page

Select **Save** to save the entered details.

3.7.11 SSL Settings

The SSL Settings page offers options to configure an SSL certificate to be used in the Integrated BMC. To access the SSL Settings page, click **Settings** → **SSL Settings** from the menu bar.



Figure 56. SSL settings submenu icon

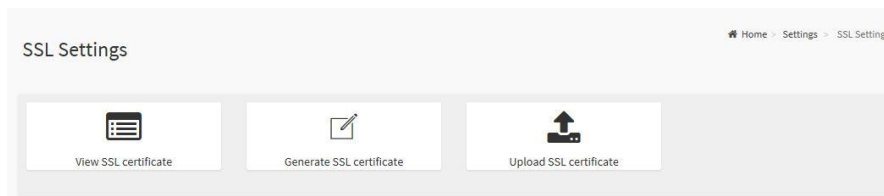


Figure 57. SSL settings page

3.7.11.1 View SSL Certificate

This page displays basic information about the uploaded SSL certificate:

- Version- Serial Number
- Signature Algorithm
- Public Key

To access the View SSL Certificate page, select **Settings** → **SSL Settings** → **View SSL Certificate** from the menu bar.

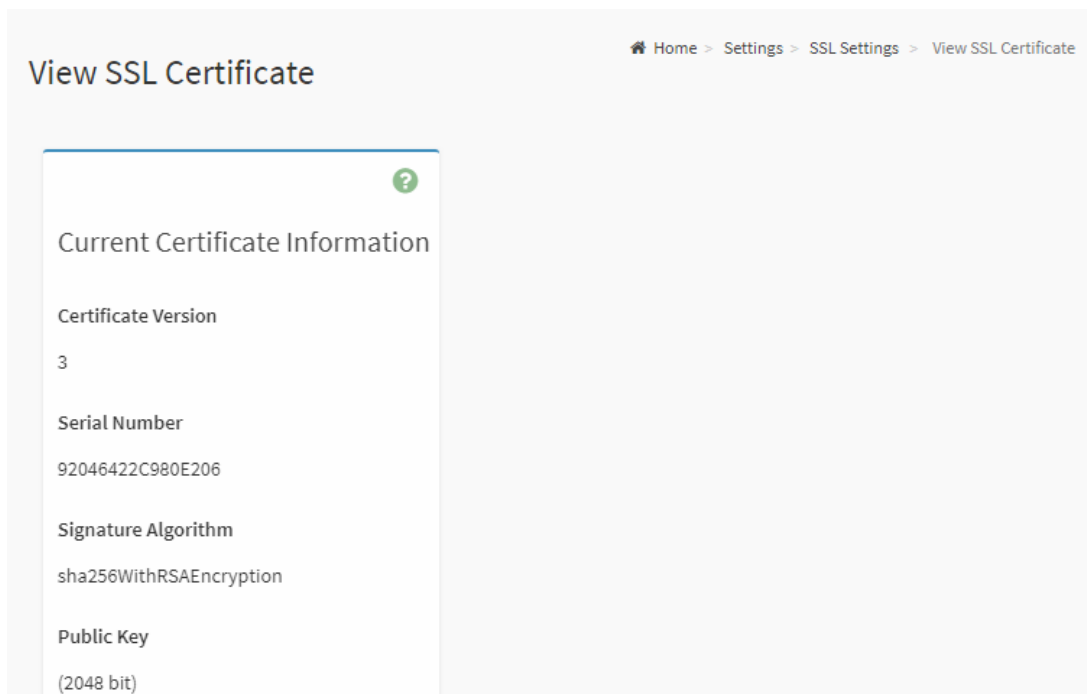
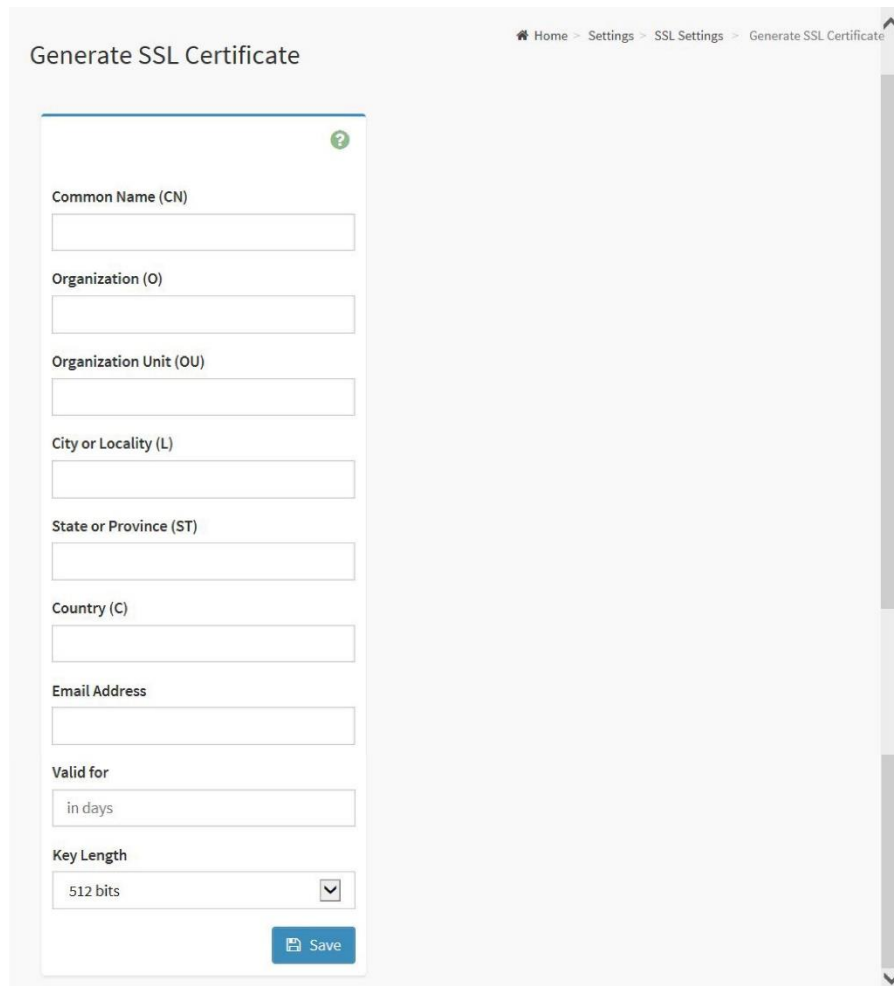


Figure 58. View SSL certificate page

Select **Save** to generate the certificate.

3.7.11.2 Generate SSL Certificate

Use this page to generate an SSL certificate to be used in the Integrated BMC. To access the Generate SSL Certificate page, select **Settings** → **SSL Settings** → **View SSL Certificate** from the menu bar.



The screenshot shows the 'Generate SSL Certificate' page in the BMC web console. The page title is 'Generate SSL Certificate'. The breadcrumb navigation is 'Home > Settings > SSL Settings > Generate SSL Certificate'. The form contains the following fields:

- Common Name (CN):
- Organization (O):
- Organization Unit (OU):
- City or Locality (L):
- State or Province (ST):
- Country (C):
- Email Address:
- Valid for:
- Key Length: (dropdown menu)

A blue 'Save' button is located at the bottom right of the form.

Figure 59. Generate SSL certificate page

Select **Save** to generate the new SSL certificate.

3.7.11.3 Upload SSL Certificate

The Upload SSL Certificate page displays the current SSL certificate information, and allows for the uploading of a new SSL certificate. To access the Upload SSL Certificate page, select **Settings** → **SSL Settings** → **Upload SSL Certificate** from the menu bar.

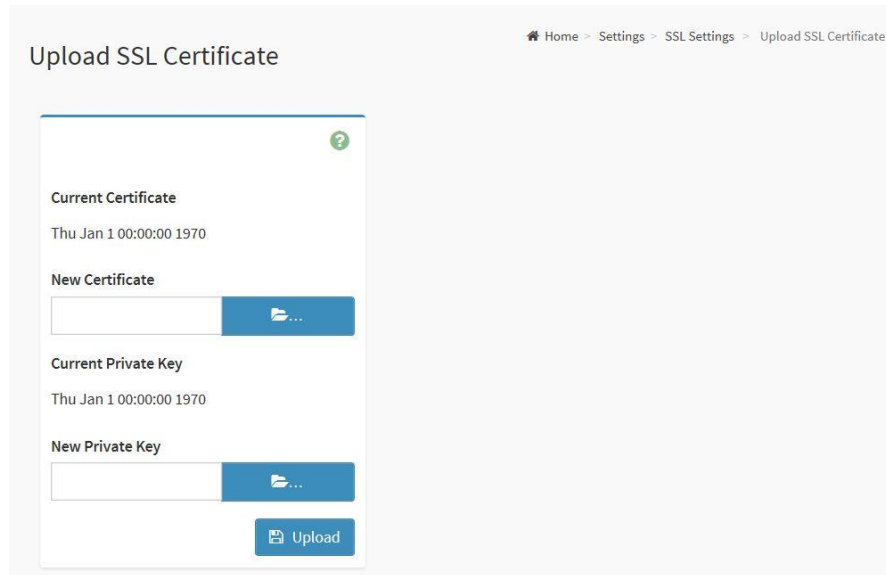


Figure 60. Upload SSL certificate page

Select **Upload** to upload the SSL certificate and privacy key into the BMC.

3.7.12 System Firewall

Use the system firewall submenus to configure firewall settings for the Integrated BMC. Firewall rules can be set for an IP or range of IP addresses or port numbers. To view this page, operator clearance is required. Only users with administrator privileges can configure firewall settings. To access the System Firewall page, select **Settings** → **System Firewall** from the menu bar.



Figure 61. System firewall submenu icon

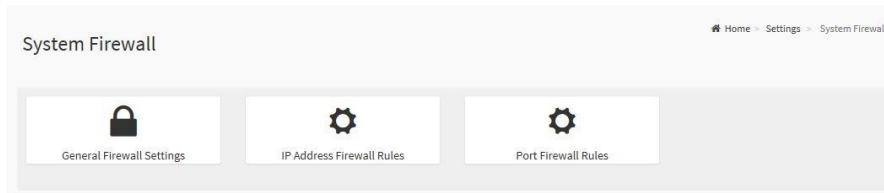


Figure 62. System firewall page

3.7.12.1 General Firewall Settings

To access the General firewall Settings page, click **Settings** → **System Firewall** → **General Firewall Settings** from the menu bar.

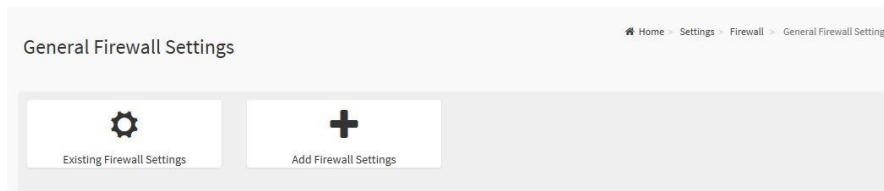


Figure 63. General firewall settings page

3.7.12.2 Existing Firewall Settings

Use this page to view the existing firewall rules in the integrated BMC. To access the Existing Firewall Settings page, select **Settings** → **System Firewall** → **General Firewall Settings** → **Existing Firewall Settings** from the menu bar.

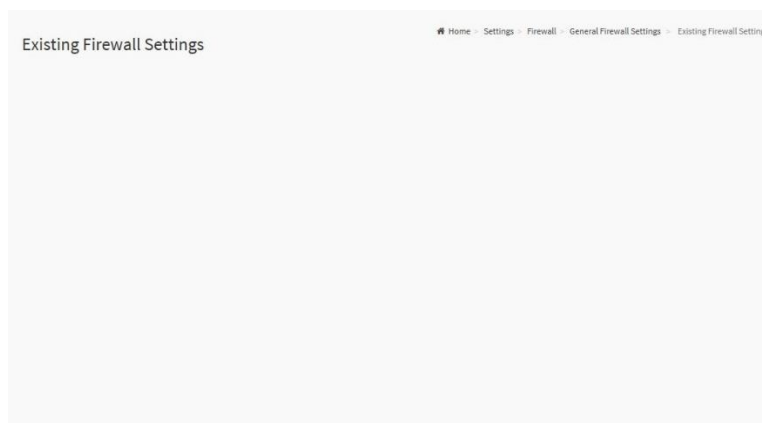


Figure 64. Existing firewall settings page

3.7.12.3 Add Firewall Settings

Use this page to add a new firewall rule. To access the Add Firewall Settings page, select **Settings** → **System Firewall** → **General Firewall Settings** → **Add Firewall Settings** from the menu bar.

Figure 65. Add firewall settings page

Select **Save** to save the changes made.

3.7.12.4 IP Firewall Rules

To access the IP Firewall Rules page, select **Settings** → **System Firewall** → **IP Firewall Rules** from the menu bar.



Figure 66. IP firewall rules page

3.7.12.5 Existing IP Rules

Use this page to view the existing IP rules in the Integrated BMC. To access the Existing IP Rules page, select **Settings** → **System Firewall** → **Firewall Settings** → **IP Firewall Rules** → **Existing IP Rules** from the menu bar.

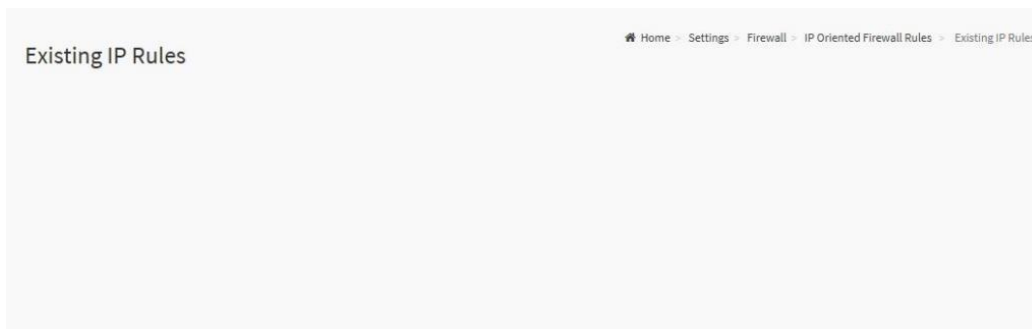
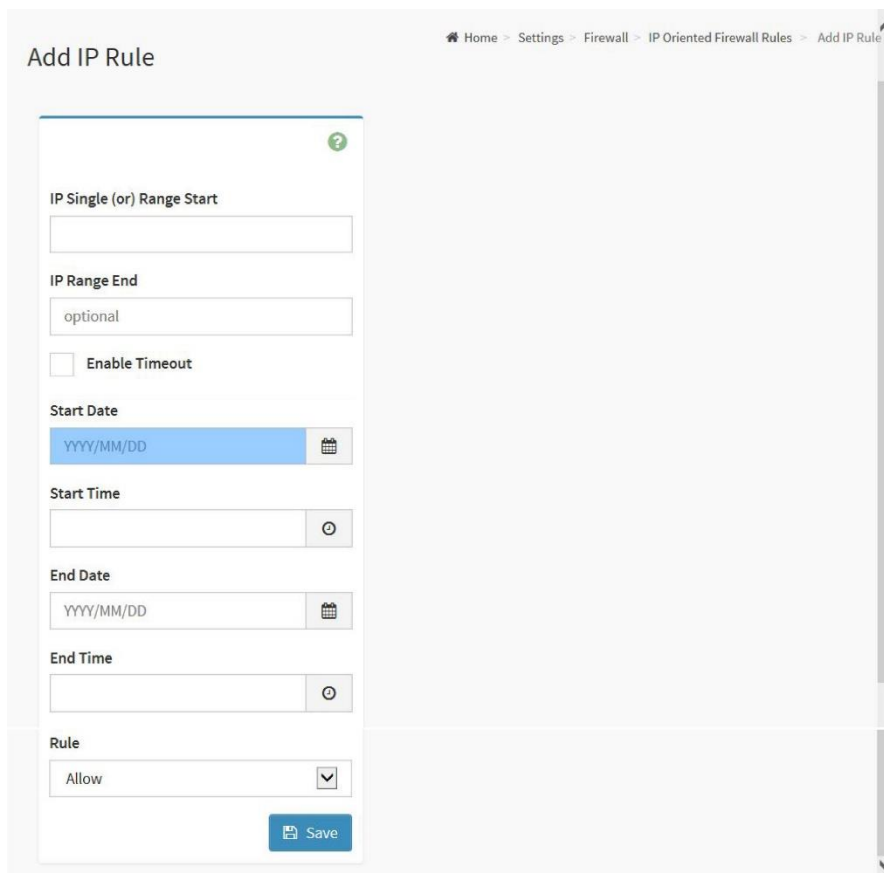


Figure 67. Existing IP rules page

3.7.12.6 Add IP Rules

Use this page to add a new IP rule. To access the Add IP Rules page, select **Settings** → **System Firewall** → **IP Firewall Rules** → **Add IP Rules** from the menu bar.



The screenshot shows the 'Add IP Rule' page in the BMC Web Console. The breadcrumb navigation at the top right reads: Home > Settings > Firewall > IP Oriented Firewall Rules > Add IP Rule. The form contains the following fields and controls:

- IP Single (or) Range Start:** A text input field.
- IP Range End:** A text input field with the placeholder text 'optional'.
- Enable Timeout:** A checkbox that is currently unchecked.
- Start Date:** A date picker field showing 'YYYY/MM/DD'.
- Start Time:** A time picker field with a clock icon.
- End Date:** A date picker field showing 'YYYY/MM/DD'.
- End Time:** A time picker field with a clock icon.
- Rule:** A dropdown menu currently set to 'Allow'.
- Save:** A blue button with a floppy disk icon and the text 'Save'.

Figure 68. Add IP rules page

Select **Save** to save the changes made.

3.7.12.7 Port Firewall Rules

To access the Port Firewall Rules page, click **Settings** → **System Firewall** → **Port Firewall Rules** from the menu bar.

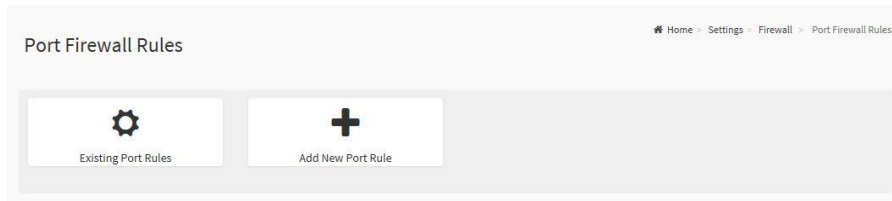


Figure 69. Port firewall rules page

3.7.12.8 Existing Port Rules

Use this page to view the existing port rules in the Integrated BMC. To access the Existing Port Rules page, select **Settings** → **System Firewall** → **Firewall Settings** → **Port Firewall Rules** → **Existing Port Rules** from the menu bar.



Figure 70. Existing port rules page

Select **Delete** to delete an entry to the firewall rules list.

3.7.12.9 Add Port Rules

Use this page to add port rules to the Integrated BMC. Specific ports or port ranges can be configured. The port value range can be from 1 to 65535.

Note: Port 80 is blocked for TCP/UDP protocols.

To access the Add Port Rules page, select **Settings** → **System Firewall** → **Port Firewall Rules** → **Add Port Rule** from the menu bar.

Figure 71. Add port rules page

Select **Save** to save the changes made.

3.7.13 User Management

The User Management page displays the current list of users for the Integrated BMC and allows to add, modify, or delete existing users. To access the User Management page, select **Settings** → **User Management** from the menu bar.



Figure 72. User management submenu icon

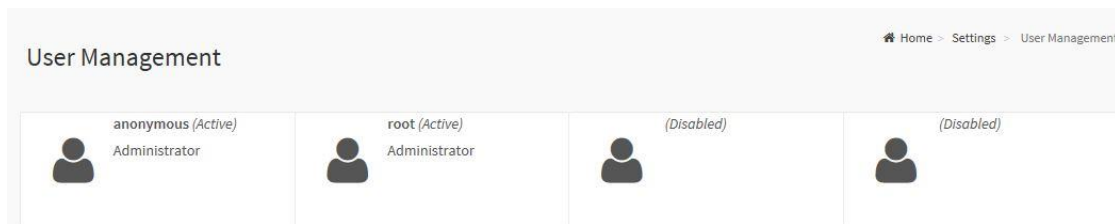


Figure 73. User management page

Select the icon () on any free slot to add a new user from the User Management main page.

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

The User Management Configuration Page displays information about the selected user, and their privileges. To add a new user, select a free section and click on the empty section.

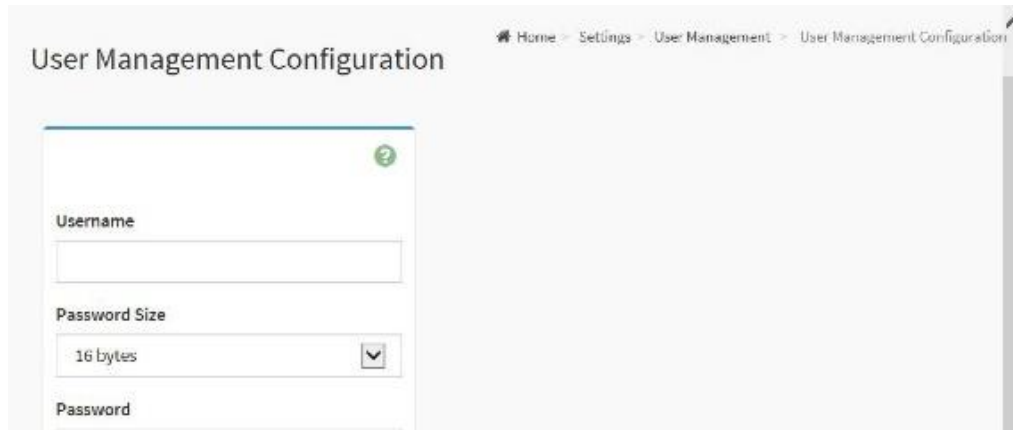


Figure 74. Add user page

Note:

- Username is a string of 1 to 16 alpha-numeric characters.
 - Username must start with an alphabetical character.
 - Username is case-sensitive.
 - Special characters '-', '_' (underscore), '@' (at sign) are allowed.
 - For 20 Bytes password, a LAN session is not established.
-

3.7.14 Video Recording

The Video Recording page displays a submenu containing configuration options. To access the video recording page, click **Settings** → **Video Recording** from the menu bar.



Figure 75. Video recording submenu icon

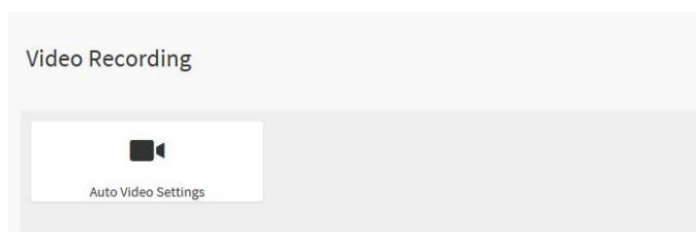


Figure 76. Video recording page

3.7.14.1 Auto Video Settings

To access the Auto Video Settings page, select **Settings** → **Video Recording** → **Auto Video Settings** from the menu bar.

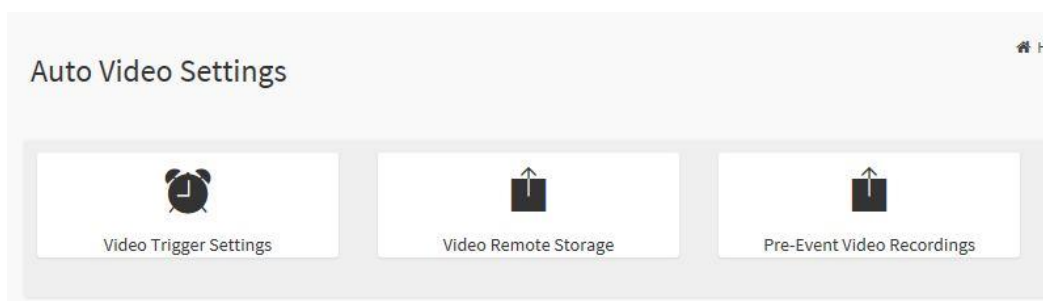


Figure 77. Auto video settings page

3.7.14.2 Video Trigger Settings

Use this page to select different triggers to start video recording.

Note: KVM service should be enabled to perform auto-video recording. The date and time should be in advance of the system date and time.

To access the Video Trigger Settings page, select **Settings** → **Video Recording** → **Auto Video Recording** → **Video Trigger Settings** from the menu bar.

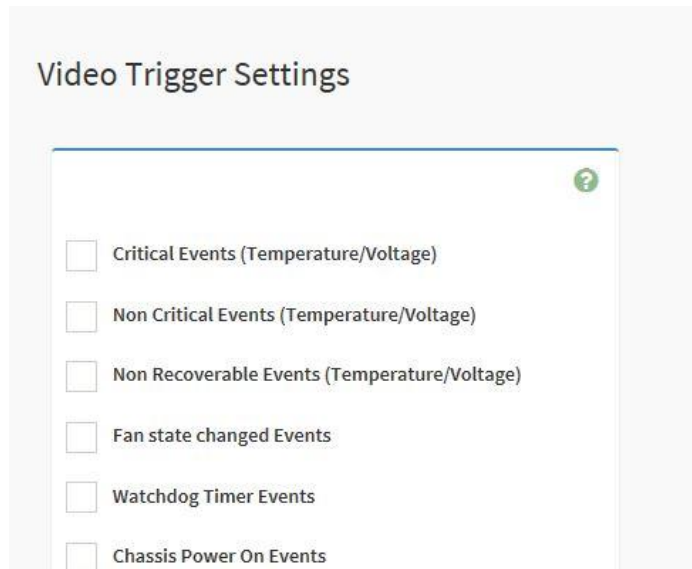


Figure 78. Video trigger settings page

Select **Save** to save the changes made.

3.7.14.3 Video Remote Storage

Use this page to enable or disable remote video support. Video files are stored in the local path of the BMC by default. If remote video support is enabled, the video files will be stored only in the remote path, and not within the BMC. To access the Video Remote Storage page, select **Settings** → **Video Recording** → **Auto Video Recording** → **Video Remote Storage** from the menu bar.

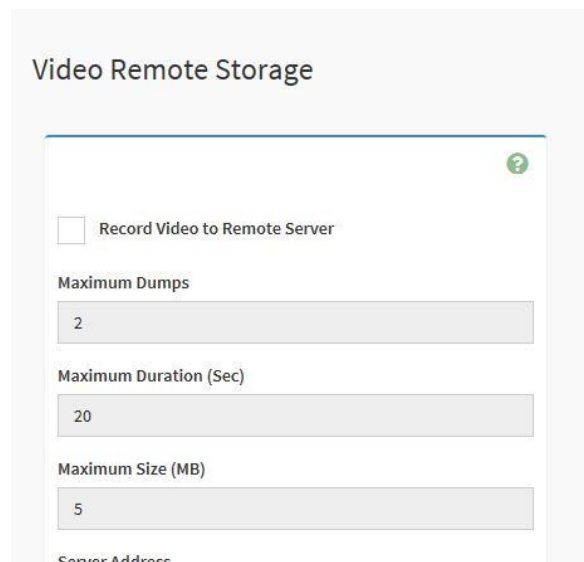


Figure 79. Video remote storage page

Select **Save** to save the changes.

3.7.14.4 Pre-Event Video Recordings

Use this page to configure Pre-Event video recording configurations. Pre-Event video recording is disabled by default. To access the Pre-Event Video Recording page, select **Settings** → **Video Recording** → **Auto Video Recordings** → **Pre-Event Video Recordings** from the menu bar.

Pre-Event Video Recordings

Home > Settings > Video > Auto settings > Pre-Event Video Recordings

This page used to configure the Pre-Event video recording configurations. Pre-Event video recording is currently disabled. To enable the Pre-Event video recording in [Triggers Configuration](#) page and trigger the video.

Video Quality
Very Low

Compression Mode
High

Frames Per Second
1

Video Duration
10

Save

Figure 80. Pre-event video recordings page

Select **Save** to save the changes made.

3.8 Remote Control

Use this page to launch a remote control session. To access the Remote Control page, select **Remote Control** from the menu bar.

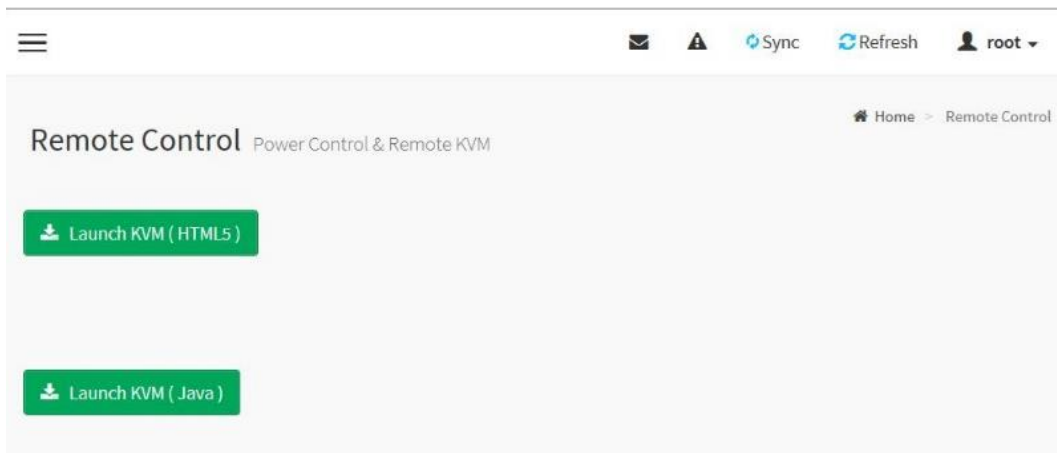


Figure 81. Remote control page

Select **Java Console** to start the JViewer video redirection.

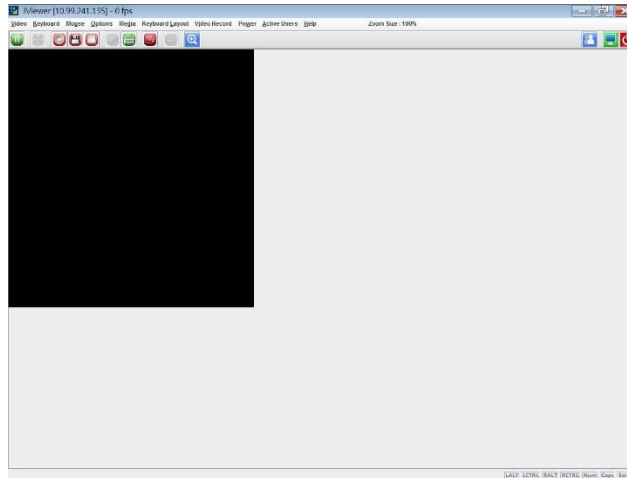


Figure 82. JViewer video redirection

Select **Launch KVM** to access the remote control KVM page.

- **Start KVM:** Starts the H5Viewer video redirection.
- **Stop KVM:** Stops the H5 Viewer video redirection.

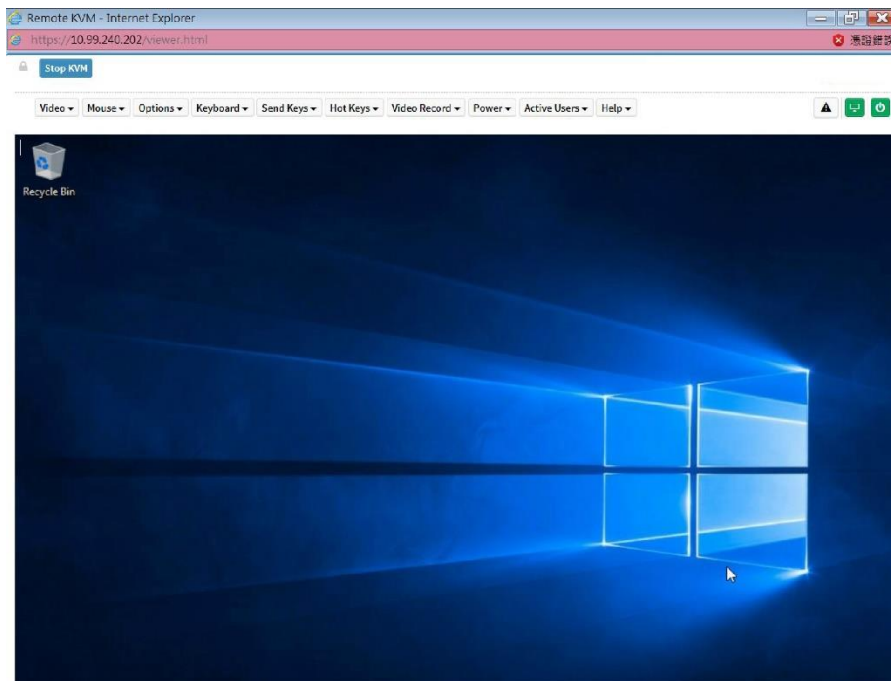


Figure 83. Remote KVM page

3.8.1 Remote KVM menu bar



Figure 84. Remote KVM menu bar

3.8.1.1 Video

The **Video** menu contains the following submenu items.

- **Pause Video:** Use this option for pausing Console Redirection.
- **Resume Video:** Use this option to resume the Console Redirection when the session is paused.
- **Refresh Video:** Use this option to update the display shown in the Console Redirection window.
- **Display on:** If this option is enabled, the display is shown on the screen in Console Redirection.
- **Display off:** If this option is enabled, the server display will be blank but viewable in Console Redirection. If this option is disabled, the display returns to the server screen.
- **Capture Screen:** This option takes a screenshot of the host screen and saves it to the client's system.

3.8.1.2 Mouse

- **Show Client Cursor:** Show or hide the local mouse cursor on the remote client system.
- **Mouse Mode:** Mouse emulation from the local window to the remote screen. Only the administrator has the privileges to configure this option.
 - **Absolute mouse mode:** The absolute position of the local mouse is sent to the server if this option is selected.
 - **Relative mouse mode:** The relative mode sends the calculated relative mouse position displacement to the server if this option is selected.
- **Other mouse mode:** Sets the client cursor in the middle of the client system and will sends any deviation to the host. This mouse mode is specific for a SUSE Linux installation.

Note: The client cursor is always hidden. To enable the display of the client cursor, use **Alt + C** to access the menu.

3.8.1.3 Options

The bandwidth usage option allows for the adjustment of the bandwidth via the following options:

- **Block Privilege Request:** Enable or disable the access privilege of the user.
- **Keyboard/Mouse Encryption:** Encrypt keyboard inputs and mouse movements sent between the connections.

3.8.1.4 Keyboard

List of Host Physical Keyboard languages supported in H5Viewer.

- English
- German
- Japanese

3.8.1.5 Video Record

This menu contains the following submenu items:

- **Record Video:** Start recording the screen.
- **Stop Recording:** Stop the recording.
- **Record Settings:** Set the recording duration of the video.

3.8.1.6 Send Keys

This menu contains the following submenu items:

- **Hold Down**
- **Press and Release**

3.8.1.7 Hold Down

This menu contains the following submenu items:

- **Right Ctrl Key:** Acts as the right-side <CTRL> key when in Console Redirection.
- **Right Alt Key:** Acts as the right-side <ALT> key when in Console Redirection.
- **Right Window Key:** Acts as the right-side <WIN> key when in Console Redirection.
- **Left Ctrl Key:** Acts as the left-side <CTRL> key when in Console Redirection.
- **Left Alt Key:** Acts as the left-side <ALT> key when in Console Redirection.
- **Left Window Key:** Acts as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.

3.8.1.8 Press and Release

- **Ctrl + Alt + Del:** Acts as if you depressed the <CTRL>, <ALT> and keys down simultaneously on the server that you are redirecting.
- **Left Windows Key:** Acts as the left-side <WIN> key when in Console Redirection. You can also decide how the key should be pressed: Hold Down or Press and Release.
- **Right Windows Key:** Acts as the right-side <WIN> key when in Console Redirection.
- **Context Menu Key:** Acts as the context menu key when in Console Redirection.
- **Print Screen Key:** Acts as the print screen key, when in Console Redirection.

3.8.1.9 Hot Keys

This menu adds the user configurable shortcut keys to invoke in the host machine. These configured key events are saved in the BMC.

This menu contains the following submenu items:

- **Add Hot Keys:** Enables macros. Select **Add** to add macros.

3.8.1.10 Power

- **Power Reset:** Reboots the system without powering off (warm boot).
- **Immediate Shutdown:** Power off the server immediately.
- **Orderly Shutdown:** Soft power off.
- **Power On:** Power on the server.
- **Power Cycle:** First power off, and then reboot the system (cold boot).

3.8.1.11 Active Users

Select this option to display the active users and their system IP address.

3.8.1.12 Help

Select this option to display information about the H5Viewer.

3.9 Power Control

The Power Control page provides access to control the system power.

To access the Power Control page, select **Power Control** from the menu bar.

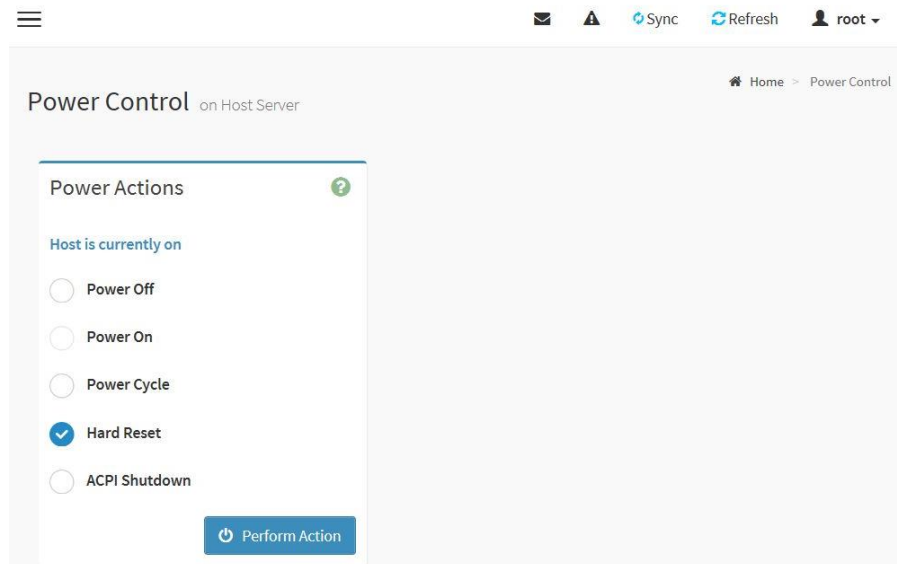


Figure 85. Power control menu

The power control page contains the following options:

- **Power Off:** Immediately power off the server.
- **Power On:** Power on the server.
- **Power Cycle:** First power off, and then reboot the system (cold boot).
- **Hard Reset:** Reboot the system without powering off (warm boot).
- **ACPI Shutdown:** Initiate operating system shutdown prior to the shutdown.
- **Perform Action:** Click this option to perform the selected operation.

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

Note: The BMC Web Console does not support Chassis Identify or Set front Panel enables

3.10 Maintenance

Use this page to access various maintenance options on the Integrated BMC. The maintenance menu contains of the following items:

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

To access the Maintenance page, select **Maintenance** from the menu bar.

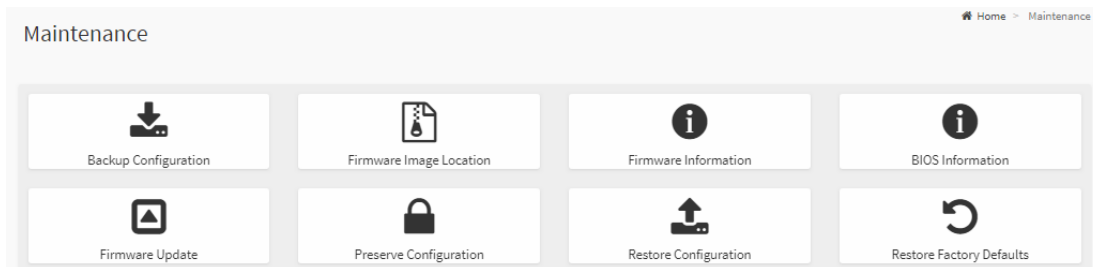


Figure 86. Maintenance page

3.10.1 Backup Configuration

Use this page to select different configuration elements that can be backed up. When a configuration element is selected, the configuration backup can be downloaded. The downloaded configuration backup can be used to restore the configuration later. To access the Backup Configuration page, select **Maintenance** → **Backup Configuration** from the menu bar.



Figure 87. Backup configuration submenu icon

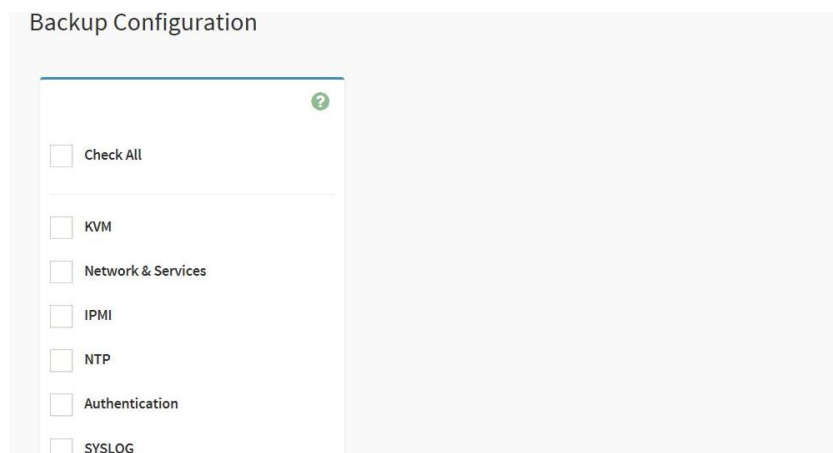


Figure 88. Backup configuration page

1. Select **Check All** to backup the selected configuration items. The Backup Configuration page will appear as shown in Figure 88.
2. Select **Download Config** to save the backup file to the client system.
3. Select **OK** to perform the backup action. The backup file is saved in the client system.
4. Select **Cancel** to cancel the backup process.

3.10.2 Firmware Image Location

Use this page to configure the firmware image on the BMC. To access the Firmware Image Location Page, select **Maintenance** → **Firmware Image Location** from the menu bar.



Figure 89. Firmware image location submenu icon



Figure 90. Firmware image location page

Select **Save** to save any changes made.

3.10.3 Firmware Information

The Firmware Information page displays current firmware information. To access the Firmware Information page, select **Maintenance** → **Firmware Information** from the menu bar.



Figure 91. Firmware information submenu icon

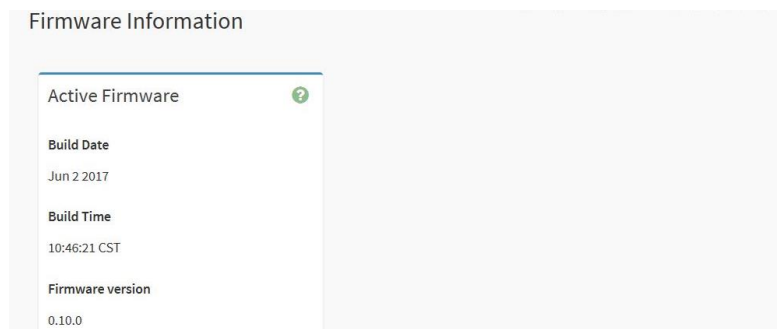


Figure 92. Firmware information page

3.10.4 BIOS Information



Figure 93. BIOS information submenu icon

The BIOS Information page displays current BIOS Information. To access the BIOS Information page, select **Maintenance** → **BIOS Information** from the menu bar.

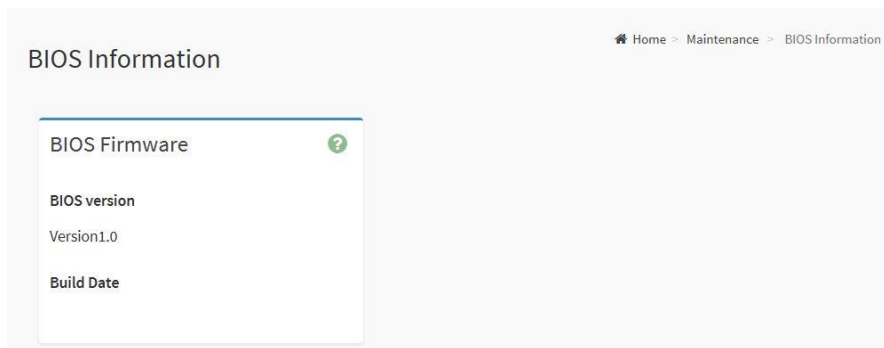


Figure 94. BIOS information page

3.10.5 Firmware Update

The Firmware Update page provides a tool for remotely updating the BMC. An automatic reset of the system occurs if the upgrade is completed or cancelled. An option to Preserve All Configuration is available. Enable it to preserve configured settings through the upgrade. To configure, select **Maintenance** → **Firmware Update** from the menu bar.



Figure 95. Firmware update submenu icon

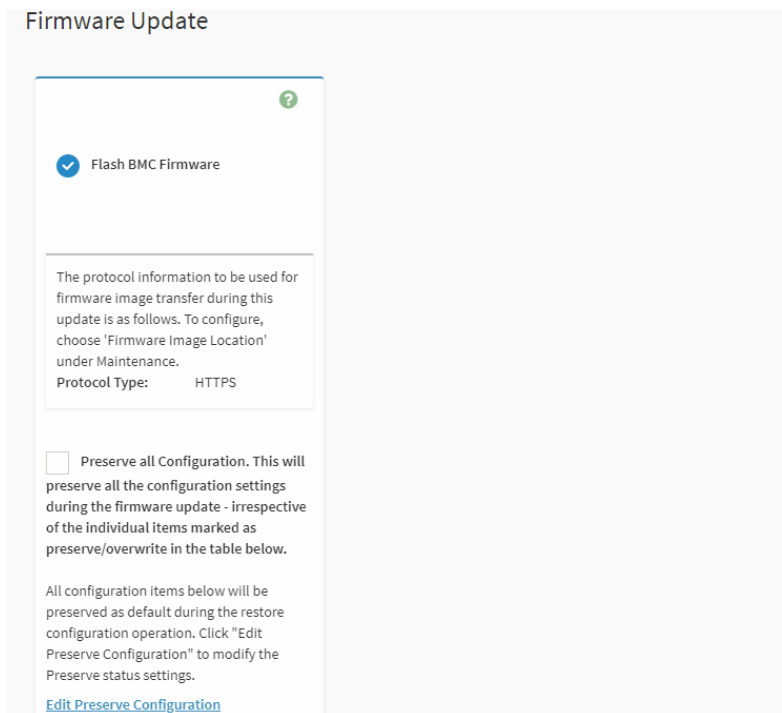


Figure 96. Firmware update page

Select **Start Firmware Update** to begin the firmware update process.

3.10.6 Preserve Configuration

Use this page to select parts of the configuration for preservation without overwriting with default/Firmware Upgrade configuration. To access the Preserve Configuration page, select **Maintenance** → **Preserve Configuration** from the menu bar.



Figure 97. Preserve configuration submenu icon

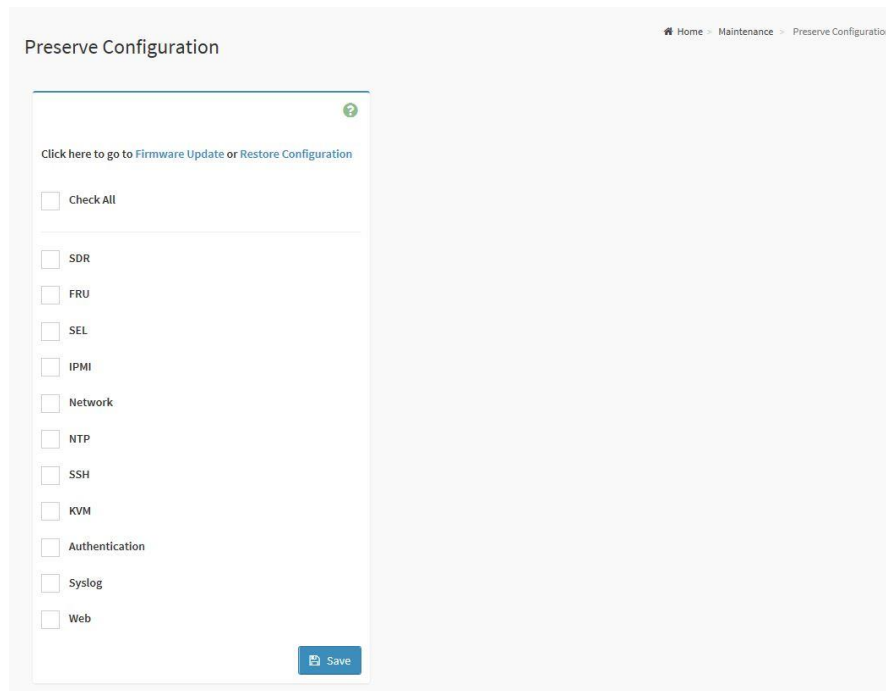


Figure 98. Preserve configuration page

Select **Save** to save the changes.

3.10.7 Restore Configuration

Use this page to restore configuration files from a connected client system to the BMC. To access the Restore Configuration page, select **Maintenance** → **Restore Configuration** from the menu bar.



Figure 99. Restore configuration submenu icon

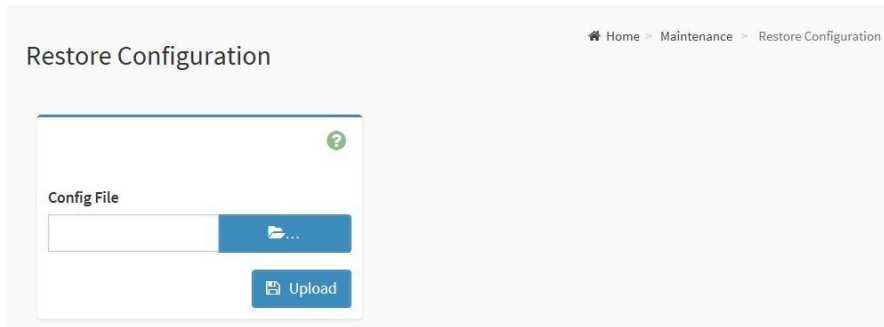


Figure 100. Restore configuration page

Select **Upload** to restore the backup files. The Restore Configuration page prompt appears as shown in Figure 101.

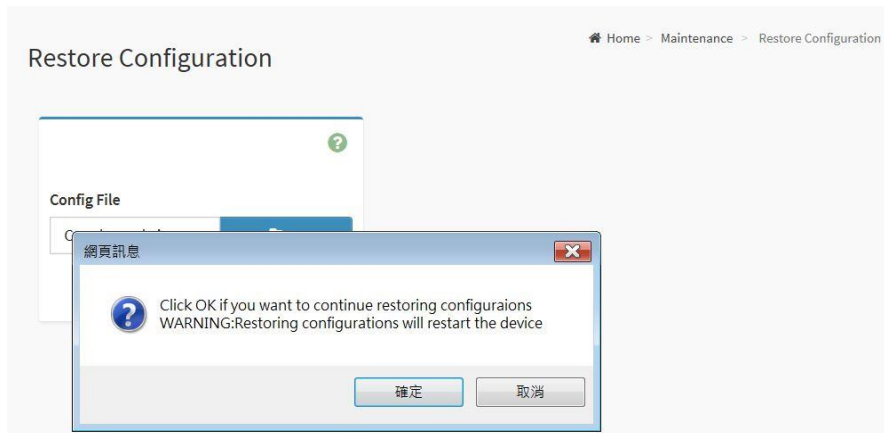


Figure 101. Restore configuration confirmation prompt

Select **OK** to upload the new configuration file and restore.

3.10.8 Restore Factory Defaults

This section lists the configuration items that are preserved during the restoration of factory default configurations. To access the Restore Factory Defaults page, select **Maintenance** → **Restore Factory Defaults** from the menu bar.



Figure 102. Restore factory defaults submenu icon

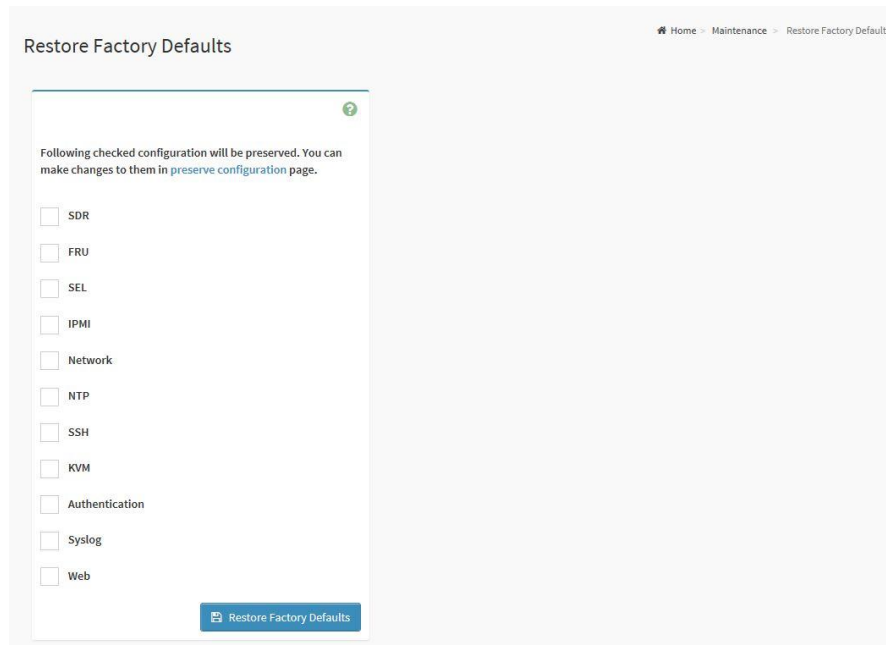


Figure 103. Restore factory defaults page

Select **Restore Factory Defaults** to restore the factory defaults of the device's firmware.

3.11 Sign Out

To log out of the GUI, select **Sign Out** from the menu bar. A confirmation prompt appears as shown in Figure 104.

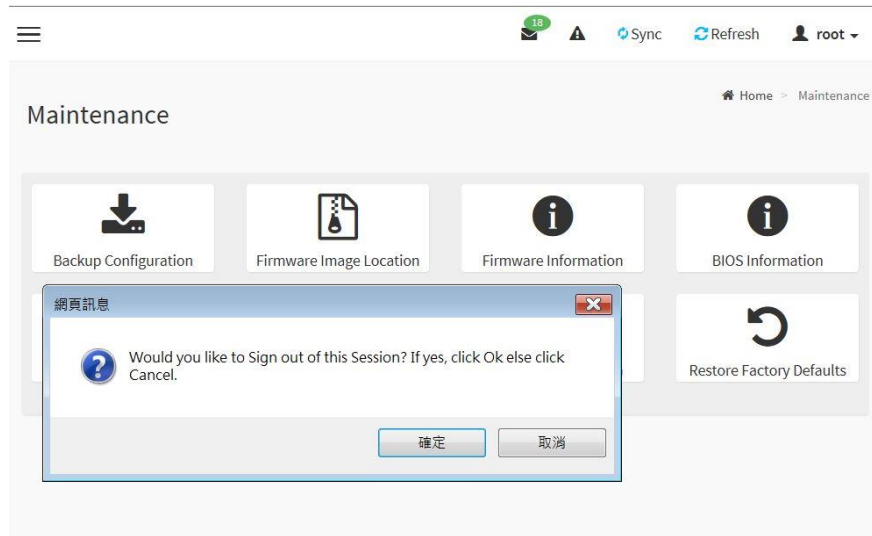


Figure 104. Logout dialog box

Alternatively, select the **root** icon on the top right corner of the screen as shown in Figure 105.

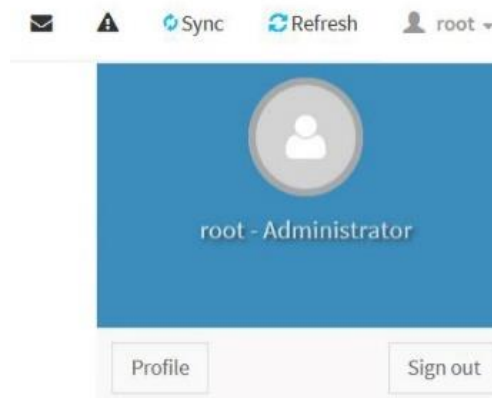


Figure 105. Root icon logout

Select **Sign Out** to log out of the GUI, to display a confirmation prompt as shown in Figure 106. Select **OK** to log out, or **Cancel** to return to the GUI.

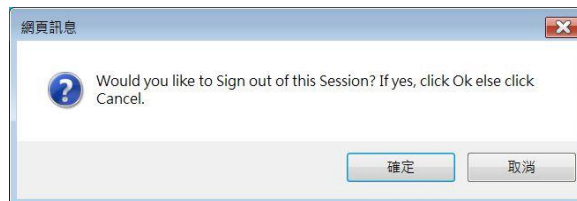


Figure 106. Logout confirmation prompt

4. BMC Port Number

This section lists a table of the BMC Port numbers.

Table 2. BMC port numbers

BMC Port Numbers	Web Server: 443
	KVM: 7578, 7582
	CD Media: 5120, 5124
	FD Media: 5123, 5127
	HD Media: 5122, 5126
	IPMI: 623
	UPnP Discovery: 1900, 50000

Appendix A. Glossary

Term	Definition
BMC	Baseboard Management Controller
GUI	Graphical User Interface
BIOS	Basic Input/Output System
ACPI	Advanced Configuration and Power Interface
FRU	Field Replaceable Unit
SMTP	Simple Mail Transfer Protocol
IPMI	Intelligent Platform Management Interface
LDAP	Lightweight Directory Access Protocol
LAN	Local Area Network
RADIUS	Remote Authentication Dial-In User Service
FQDN	Fully Qualified Domain Name
KVM	Keyboard Video and Mouse
SEL	System Event Log
DNS	Domain Name System
PAM	Pluggable Authentication Modules
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
SSI	Server System Infrastructure