

Lanner

AST2500 BMC LTS Specification

Version: 0.6

Date of Release: **2023-03-09**

Revision History

Version	Date	Author	Description
0.1	2017/9/21	Luke Kung	Preliminary release
0.2	2021/7/1	Luke Kung	Modify the User List section for SNMP and Current password.
0.3	2021/9/27	Luke Kung	Modify the FTW and dashboard part to fit the current status.
0.4	2021/10/20	Luke Kung	Fix typo.
0.5	2022/09/21	Luke Kung	Add syslog page and modify sensor page picture.
06	2022/10/11	Sony Lee	Modify KVM power settings

Icon Descriptions

The icons are used in the manual to serve as an indication of interest topics or important messages. Below is a description of these icons:



Note: This mark indicates that there is a note of interest and is something that you should pay special attention to while using the product.



Warning: This icon indicates that there is a caution or warning and it is something that could damage your property or product.

Acronyms

Name	Description
IPMI	Intelligent Platform Management Interface
BMC	Baseboard Management Controller
OEM	Original Equipment Manufacturer
SDR	Sensor Device Record
KCS	Keyboard Controller Style
FRU	Field Replaceable Unit
SEL	System Event Log
WebUI	Web-based user interfaces

Table of Contents

Chapter 1: BMC Overview.....	5
BMC Main Features	5
BMC Firmware Functional Description	6
Chapter 2: IPMI Commands Support List	8
Chapter 3: Using BMC Web UI	10
Default User Name and Password.....	11
Chapter 4: First Time Wizard.....	12
Chapter 5: Web UI Layout.....	13
Menu Bar	13
Quick Button and Logged-in User	14
Logged-in user and its privilege level	15
Help.....	15
Chapter 6: Dashboard.....	16
Chapter 7: Appliance	17
FRU Information	17
Sensor Reading	17
Event Log	19
Remote Media Settings	21
KVM RMedia Settings	23
Image Redirection	24
Chapter 8: BMC Config.....	25

Date and Time	25
User List	26
RADIUS Setup	30
LDAP Setup & LDAP Groups	31
Login Block Settings	35
IP Settings	36
DNS Settings	37
Link Settings.....	40
SSL Certificate	41
Services.....	46
Remote Syslog	48
Audit Log.....	49
Firmware Update.....	50
Restore Factory Defaults	54
Preserve Configuration.....	55
Chapter 9: Remote KVM	57
Procedure to Start KVM	57
Settings	58
Chapter 10: Sign Out.....	61
Appendix A: Note and Remark.....	62
Appendix B: Feature List	63
Appendix C: Customization Request Form	64

CHAPTER 1: BMC OVERVIEW

This document specifies the BMC firmware features. The BMC firmware implements IPMI 2.0 based on ASPEED service processor. It performs all the BMC management tasks defined by IPMI 2.0.

In addition, BMC firmware runs an embedded web-server for full configuration using Web UI, which has a low learning curve.

BMC Main Features

Feature		Description
IPMI 2.0 Standard Features	System Interface support	<ul style="list-style-type: none"> • KCS (System Interface Support) • LAN (RMCP+) • BMC stack with an IPMI 2.0 implementation • Sensor monitoring • System power management • Watchdog timer • Fan speed monitor and control • FRU information • System Event Log (SEL) • Support in IPMI stack for SOL to remotely access BIOS and text console before OS booting • IPMI based user management • Multiple user permission level
	IPMI 2.0 based Management	
	System Management	
	Event Log	
	Text Console Redirection: SOL	
User Management		
Non-IPMI functions	Web User Interfaces	<ul style="list-style-type: none"> • BMC management via web user interface • Integrated KVM and Virtual Media • RADIUS support • LDAP support • SSL and HTTPS support • Auto-sync time with NTP server • Remote firmware update by Web UI or Linux tool
	User authorization	
	Security	
	Maintenance	

BMC Firmware Functional Description

System health monitoring

The BMC implements system sensor monitoring feature. It could monitor voltage, temperature, and current of critical components.

System Power Management

The BMC implements chassis power and resets functions for system administrators to control and manage the system power behavior. These functions can be activated by sending the IPMI 2.0 compatible chassis commands to the BMC over messaging interfaces. The following list summaries the supported functions.

- Chassis power on
- Chassis power off
- Chassis power cycle
- Chassis power reset
- Chassis power soft
- Server's power status report

Watchdog Timer

The BMC provides an IPMI 2.0 compatible watchdog timer which can prevent the system from system hanging.

Fan Speed Control

BMC oversees fan speed control. The fan speed can be modified by varying the duty cycle of PWM signal. The fan speed control algorithm mainly refers to the readings of on-board temperature sensors.

Field Replaceable Unit (FRU)

The BMC implements an interface for logical FRU inventory devices as specified in IPMI 2.0 specification. This functionality provides commands for system administrators to access and management the FRU inventory information.

System Event Log (SEL)

A non-volatile storage space is allocated to store system events for system status tracking.

Serial over LAN (SOL)

IPMI 2.0 SOL is implemented to redirect the system serial controller traffic over an IPMI session. System administrators can establish a SOL connection with a standard IPMI client, like IPMITOOL, to remotely interact with serial text-based interfaces such as OS command-line and serial redirected BIOS interfaces.

User Management

The BMC supports 9 IDs for IPMI user accounts. The maximum length of the username and password are 16 and 20 respectively, and the possible privilege levels are Callback, User, Operator, and Administrator. Moreover, the account creator can enable/disable the user account at any time. If not specified, the default user accounts are listed follows:

User Name	Password	User Access	Characteristics
admin	admin	Enabled	Password can be changed

Keyboard, Video, Mouse (KVM) Redirection

- The BMC provides keyboard, video, and mouse (KVM) redirection over LAN. This application is available remotely from the embedded web server.
- Support video recording, recorded videos to be downloaded & playable.

Virtual Media Redirection

- The BMC provides remote virtual CD and HD redirection. CD image could be mounted directly in KVM window. HD could be mounted by NFS and SAMBA.
- Efficient USB 2.0 based CD/DVD redirection with a typical speed of 20XCD.
- Completely secured transmission.

CHAPTER 2: IPMI COMMANDS SUPPORT LIST

COMMANDS	NETFN	CMD
IPM Device “Global” Commands		
Get Device ID	APP (06h)	00h
Cold Reset	APP (06h)	02h
Warm Reset	APP (06h)	03h
Get Device GUID	APP (06h)	08h
BMC Watchdog Timer Commands		
Reset Watchdog Timer	APP (06h)	22h
Set Watchdog Timer	APP (06h)	24h
Get Watchdog Timer	APP (06h)	25h
BMC Device and Messaging Commands		
Get System GUID	APP (06h)	37h
Get Channel Info	APP (06h)	42h
Set User Access	APP (06h)	43h
Get User Access	APP (06h)	44h
Set User Name	APP (06h)	45h
Get User Name	APP (06h)	46h
Set User Password	APP (06h)	47h
Chassis Device Commands		
Get Chassis Capabilities	Chassis (00h)	00h
Get Chassis Status	Chassis (00h)	01h
Chassis Control	Chassis (00h)	02h
Chassis Reset	Chassis (00h)	03h
Sensor Device Commands		
Get Sensor Reading Factors	S/E (04h)	23h
Get Sensor Hysteresis	S/E (04h)	25h
Get Sensor Threshold	S/E (04h)	27h
Get Sensor Event Enable	S/E (04h)	29h
Get Sensor Event Status	S/E (04h)	2Bh
Get Sensor Reading	S/E (04h)	2Dh
Get Sensor Type	S/E (04h)	2Fh
FRU Device Commands		
Get FRU Inventory Area Info	Storage (0Ah)	10h
Read FRU Data	Storage (0Ah)	11h
Write FRU Data	Storage (0Ah)	12h
SDR Device Commands		
Get SDR Repository Info	Storage (0Ah)	20h
Get SDR Repository Allocation Info	Storage (0Ah)	21h
Get SDR	Storage (0Ah)	23h
Get SDR Repository Time	Storage (0Ah)	28h
SEL Device Commands		
Get SEL Info	Storage (0Ah)	40h
Get SEL Allocation Info	Storage (0Ah)	41h

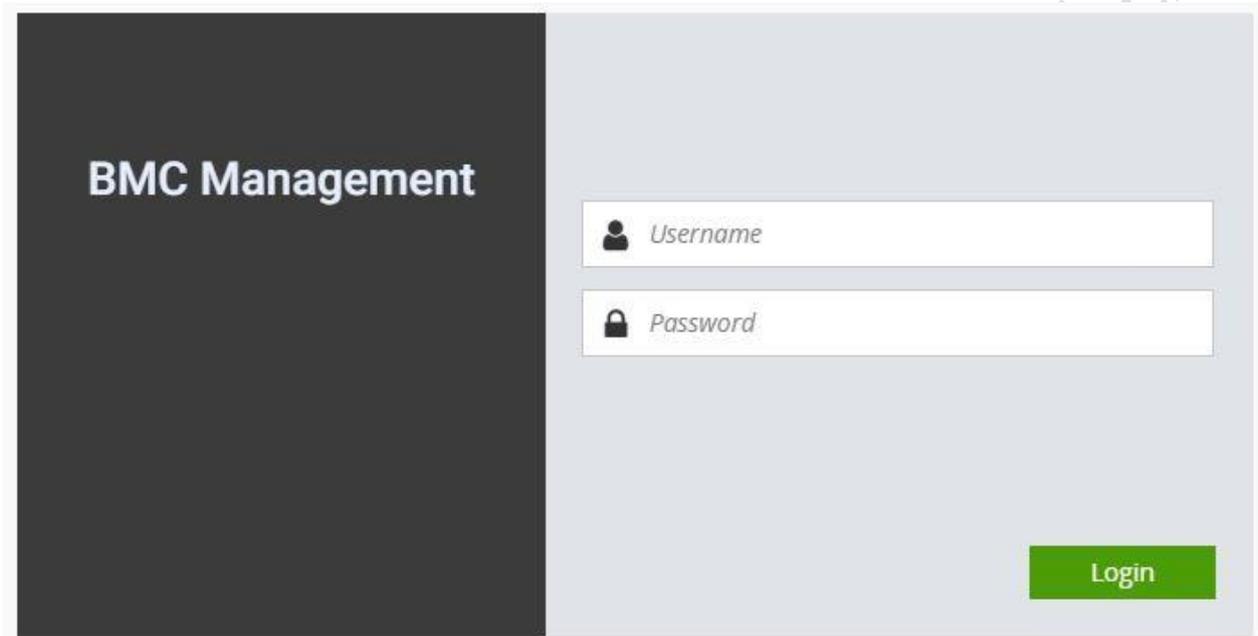
Get SEL Entry	Storage (0Ah)	43h
Delete SEL Entry	Storage (0Ah)	46h
Clear SEL	Storage (0Ah)	47h
Get SEL Time	Storage (0Ah)	48h
Set SEL Time	Storage (0Ah)	49h
Get SEL Time UTC Offset	Storage (0Ah)	5Ch
Set SEL Time UTC Offset	Storage (0Ah)	5Dh
LAN Device Commands		
Set LAN Configuration Parameters	Transport (0Ch)	01h
Get LAN Configuration Parameters	Transport (0Ch)	02h
Serial/Modem Device Commands		
Set User Callback Options	Transport (0Ch)	1Ah
Get User Callback Options	Transport (0Ch)	1Bh
SOL Activating	Transport (0Ch)	20h
Set SOL Configuration Parameters	Transport (0Ch)	21h
Get SOL Configuration Parameters	Transport (0Ch)	22h

CHAPTER 3: USING BMC WEB UI

In the address bar of your Internet browser, input the IP address of the remote server to access the BMC interface of that server.



Initial access of BMC prompts you to enter username and password. A screenshot of the login screen is given below:



Login Page

- ▶ **Username:** Enter your username in this field.
- ▶ **Password:** Enter your password in this field.
- ▶ **Login:** After entering the required credentials, click the **Login** to log in to Web UI.



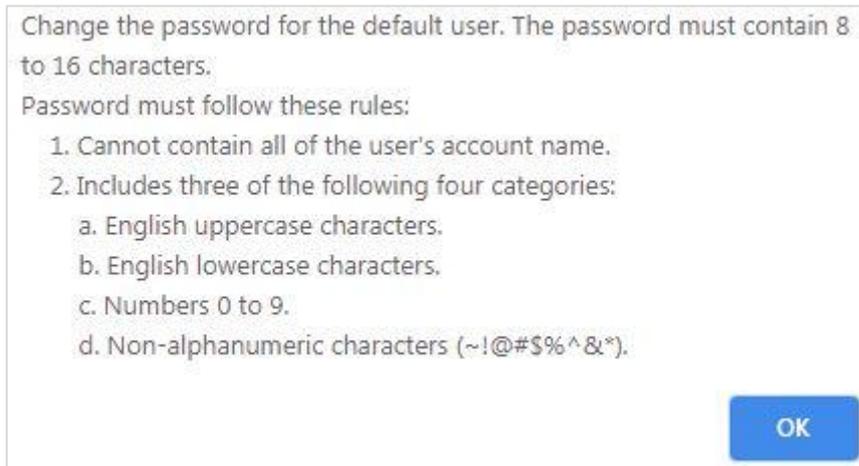
Note: (1) If not specified, the default IP to access BMC is <https://192.168.0.100>.

(2) Please use **https** to access Web UI.

Default User Name and Password

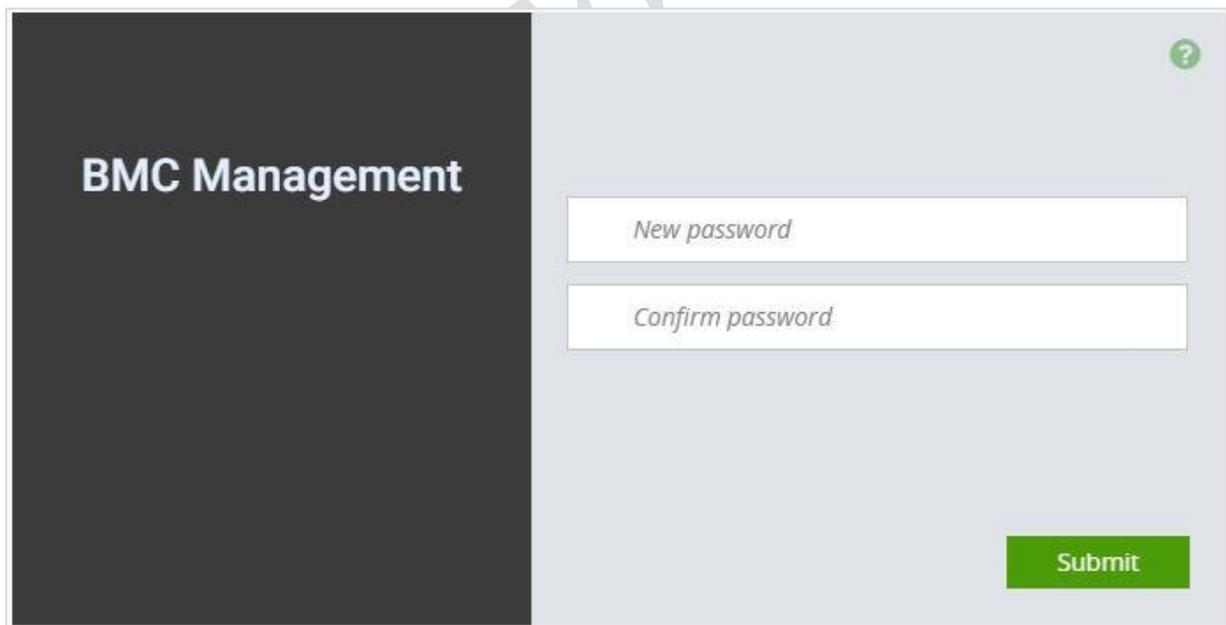
- ▶ **Username:** admin
- ▶ **Password:** admin

The default username and password are in lower-case characters. When you log in using the default username and password, you will get full administrative rights, and it will ask you to change the default password once you log in. The dialog is shown below:



Change the default password - Dialog

Clicking **OK** will take you to set a password.



Change the default password – Set password



Note: Duplicate usernames shouldn't exist across various authentication methods like LDAP, RADIUS or IPMI since the privilege of one Authentication method is overwritten by another authentication method during logging in, and hence the correct privilege cannot be returned properly.

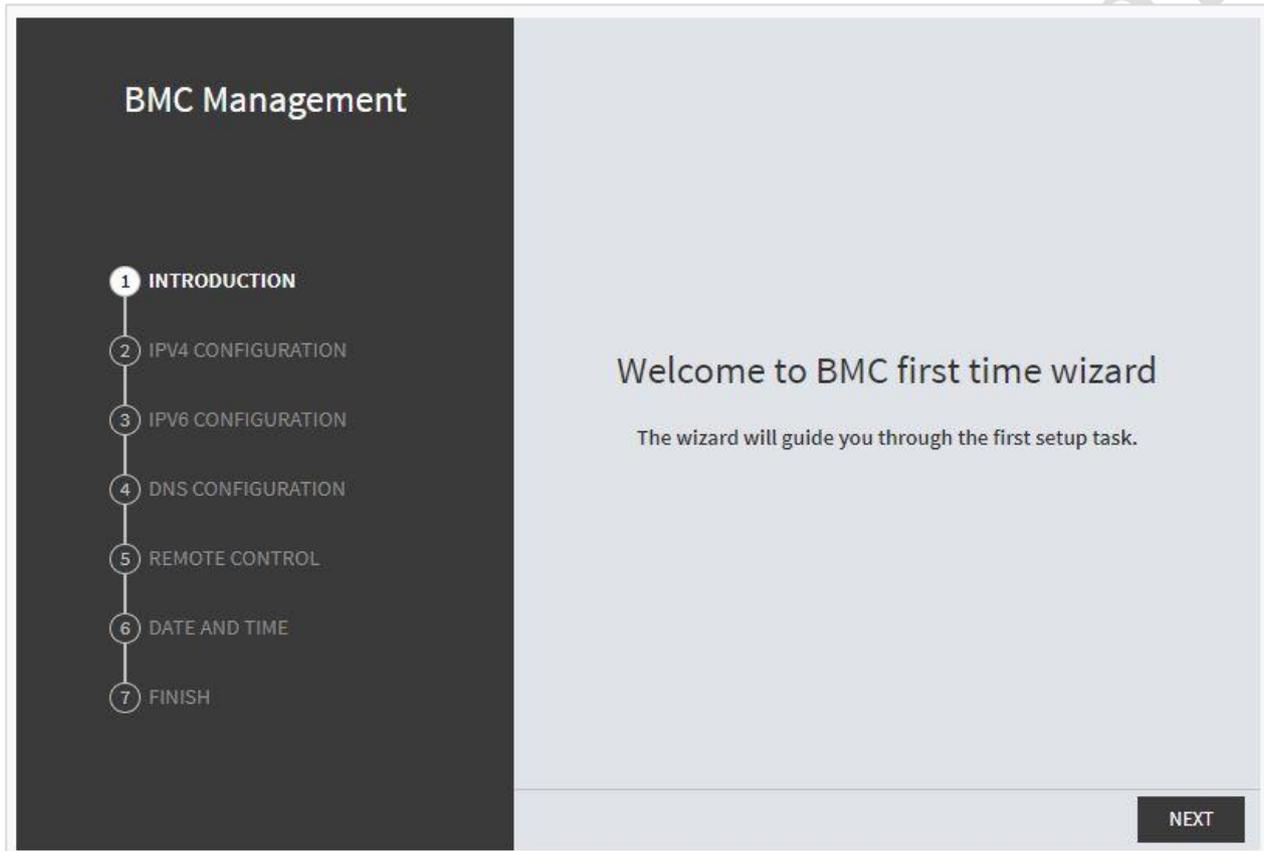
CHAPTER 4: FIRST TIME WIZARD

After the first-time login, you will see first time wizard welcome page as the following picture. Please press the "Next" button and configure your BMC step by step.

On the "IPv4", "IPv6" and "DNS" pages, you could specify the hostname and network settings of BMC.

On the "Remote Control" page, you could specify allowed IP region which could access KVM and Remote media web pages.

On the "Date and Time" page, you could specify the NTP and time settings.



In the final page, please press "Finish" button to complete the first-time wizard. BMC will be rebooted and apply new settings. You could reconnect to the WebUI after a few minutes.

CHAPTER 5: WEB UI LAYOUT

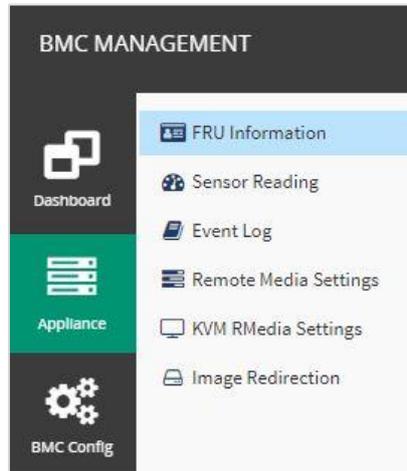
The BMC Web UI consists of various menu items:

Menu Bar

The menu bar displays the following:

- ▶ Dashboard
- ▶ Appliance – FRU Information
- ▶ Appliance – Sensor Reading
- ▶ Appliance – Event Log
- ▶ Appliance – Remote Media Settings
- ▶ Appliance – KVM RMedia Settings
- ▶ Appliance – Image Redirection
- ▶ BMC Config – Date and Time
- ▶ BMC Config – User Configuration – User List
- ▶ BMC Config – User Configuration – RADIUS Setup
- ▶ BMC Config – User Configuration – LDAP Setup
- ▶ BMC Config – User Configuration – LDAP Groups
- ▶ BMC Config – User Configuration – Login Block Settings
- ▶ BMC Config – Network Configuration – IP Settings
- ▶ BMC Config – Network Configuration – DNS Settings
- ▶ BMC Config – Network Configuration – Link Settings
- ▶ BMC Config – Network Configuration – SSL Certificate
- ▶ BMC Config – Network Configuration – Services
- ▶ BMC Config – Network Configuration – Remote Syslog
- ▶ BMC Config – Audit Log
- ▶ BMC Config – Maintenance – Firmware Update
- ▶ BMC Config – Maintenance – Restore Factory Defaults
- ▶ BMC Config – Maintenance – Preserve Configuration

A screenshot of the menu bar is shown below:



Menu Bar

Quick Button and Logged-in User

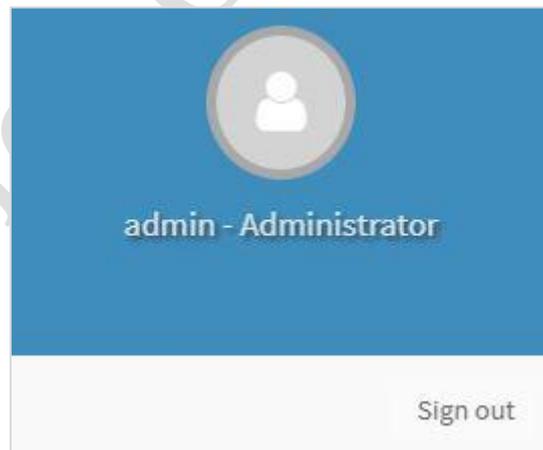
The user information and quick buttons are located at the top right of the Web UI.



User Information

Logged-in user information: Click the icon  to view the logged-in user information.

A screenshot of the logged-in user information is shown below:



Logged-in User Information

The logged-in user information shows the logged-in user's username, privilege, with the quick buttons allowing you to perform the following functions:

- ▶ **Refresh:** Click the icon  to reload the current page.
- ▶ **Sign out:** Click the icon  to log out of the Web UI.

Logged-in user and its privilege level

This option shows the logged-in username and privilege. There are four kinds of privileges:

- ▶ **User:** Only valid commands are allowed.
- ▶ **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.

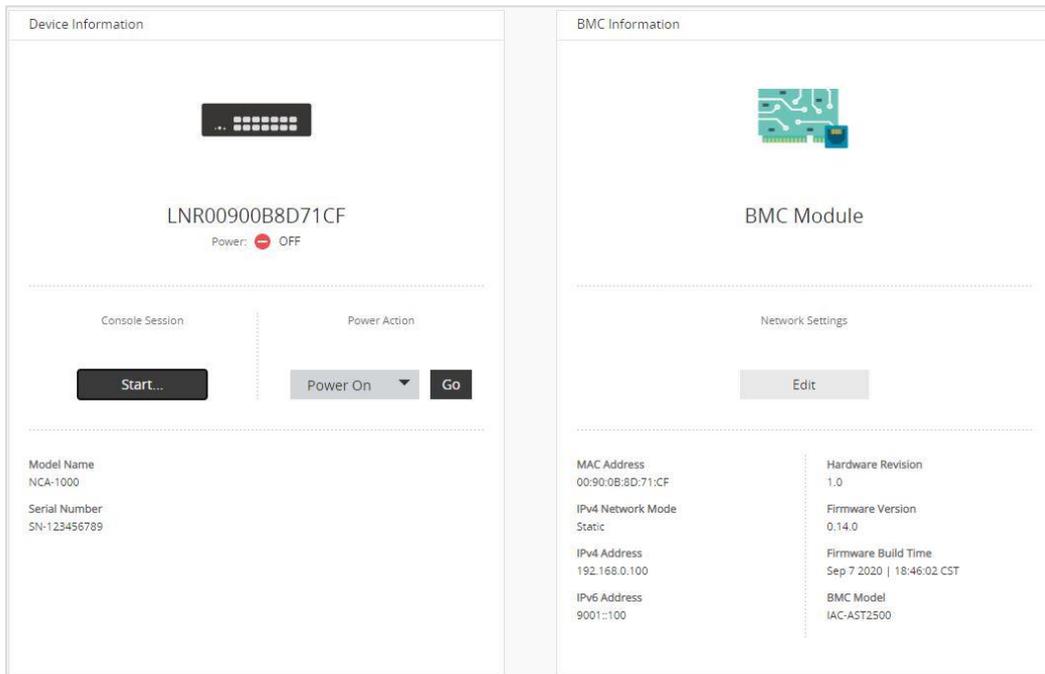
Help

Help: The **Help** icon  is located at the top right of each page in Web UI. Click this help icon to view more detailed field descriptions.

Lanner Confidential

CHAPTER 6: DASHBOARD

The Dashboard page gives the overall information about the status of a device. To open the Dashboard page, click **Dashboard** from the menu bar. A sample screenshot of the Dashboard page is shown below:



Dashboard Page

A brief description of the Dashboard page is given below:

► **Device Information**

This indicates the system information such as power status, model name and serial number. You could also execute power action and remote KVM here.

► **BMC Information**

This indicates the BMC module information such as network settings, firmware info and model name.

CHAPTER 7: APPLIANCE

This group of pages allows you to get various appliance information and set configuration.

FRU Information

FRU Information page displays the BMC's FRU device information. FRU page shows information like Basic Information, Board Information and Product Information of the FRU device.

To open the FRU Information page, click **FRU Information** from the menu bar. A screenshot of FRU Information page is given below:

The screenshot shows the 'FRU Field Replaceable Units' page. It features a header with the title and a help icon. Below the header is a descriptive text: 'This Page displays the BMC's FRU device information. FRU page shows information like Chassis Information, Board Information and Product Information of the FRU device.' The main content is divided into three columns:

- Chassis Information:**

Chassis Type	Pizza Box
Chassis Part Number	81B0301003
Chassis Serial Number	23500001J05A
- Board Information:**

Manufacture Date Time	Wed Jan 24 03:14:00 2018
Board Manufacturer	Lanner
Board Product Name	NCB-6210D
Board Serial Number	24400013J05B
Board Part Number	BPN1234
- Product Information:**

Product Manufacturer	Lanner
Product Name	NCA-6210
Product Part Number	PPN
Product Version	PV123
Product Serial Number	24400013J05A
Asset Tag	PA123

FRU Information Page

The FRU data could be modified by IPMI FRU write command.

Sensor Reading

The Sensor Readings page displays all the sensor related information.

To open the Sensor Readings page, click **Sensor Reading** from the menu. Click on any sensor to show more information about that particular sensor, including thresholds and a graphical representation of all associated events.

A screenshot of Sensor Readings page is given below:

SENSOR READING
Live reading of all sensors

Critical Sensors (6)

Sensor Name	Reading
↓ CPU_TEMP0	127 °C
↕ SYS_FAN1	0 Rpm
↕ SYS_FAN2	0 Rpm
↕ SYS_FAN3	0 Rpm
↕ SYS_FAN4	0 Rpm
↕ VBAT	0.00 Volts

Normal Sensors (9)

Filter by type: All Sensors

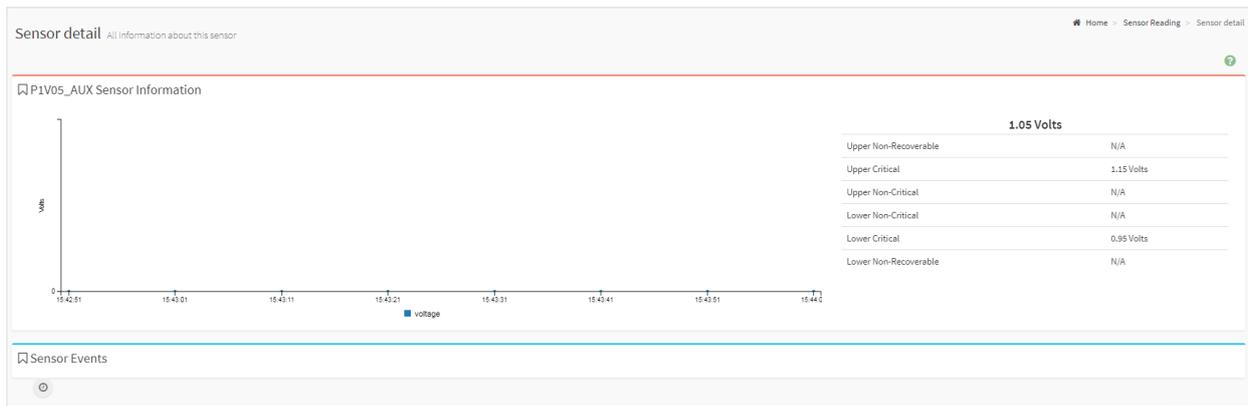
Sensor Name	Reading
↕ +12VIN	12.35 Volts
↕ 3.3V	3.33 Volts
↕ 5V	5.00 Volts
↓ CPU_PECI TEMP	27 °C

Sensor Readings Page

In this Sensor Reading page, live readings for all the available sensors with details like Sensor Name and Current Reading will be displayed, and you can also choose the sensor type that you want to be displayed from the list. Some examples of sensors are Temperature Sensors, Fan Sensors, and Voltage Sensors, etc.

Sensor Detail

Select a particular sensor from the Critical Sensor or Normal Sensor lists. The Sensor Information such as Live Widget and Thresholds for the selected sensor will be displayed as shown below, with an illustration of sample Sensor detail presented.



Sensor Detail Page



Note: Widgets are little gadgets, which provide real-time information about a particular sensor. User can track a sensor's behavior over a specific amount of time at specific intervals. The result will be displayed as a line graph in the widget.

For the selected sensor, this widget gives a dynamic representation of the readings for the sensor. Thresholds are of six types:

- ▶ Lower Non-Recoverable (LNR)
- ▶ Lower Critical (LC)
- ▶ Lower Non-Critical (LNC)
- ▶ Upper Non-Recoverable (UNR)
- ▶ Upper Critical (UC)
- ▶ Upper Non-Critical (UNC)

The threshold states could be Lower Non-critical - going low, Lower Non-critical - going high, Lower Critical - going low, Lower Critical - going high, Lower Non-recoverable - going low, Lower Non-recoverable - going high, Upper Non-critical - going low, Upper Non-critical - going high, Upper Critical - going low, Upper Critical - going high, Upper Non-recoverable - going low, Upper Non-recoverable - going high.

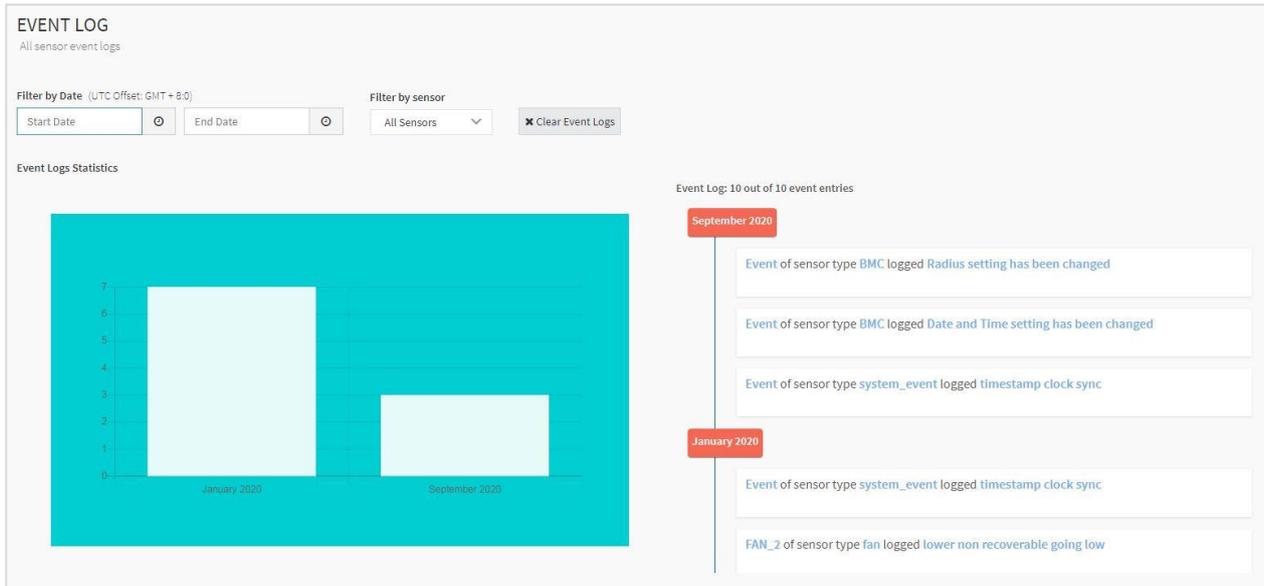
A graphical view of these events (Number of Entries vs. Thresholds) can be viewed as shown in the Sensor Readings Page screenshot.

Event Log

This page displays the list of event logs triggered by the different sensors on this device. Click on a record to see the details of that entry. You can use the date or sensor name filter options to view those specific events, or you can also sort the list of entries by clicking on any of the column headers.

To open the Event Log page, click **Event Log** from the menu bar.

A sample screenshot of Event Log page is shown below:



Event Log Page

The Event Log page consists of the following Fields:

- ▶ **Filter by Date:** Filtering can be done by selecting **Start Date** and **End Date**.
- ▶ **Filter by Sensor:** Filtering can be done by selecting sensor name.
- ▶ **Event Logs Statistics:** Displays the statistical graph for the selected date.
- ▶ **Clear Event Logs:** To delete all the event logs.



Note: The maximum event size is 3639 entries; please clear event logs if needed.

Procedure:

1. From the **Filter by Date** field, select the time period by **Start Date** and **End Date** using the calendar for the event categories.
2. From the **Filter by Sensor** field, select the **Sensor** name to view the events for the date. The events will be displayed based on the selected time period.
3. To clear all events from the list, click **Clear Event Logs** button.

Remote Media Settings

This page is used to configure the media into BMC for redirection. A sample screenshot of Image Redirection page is shown below:

REMOTE MEDIA SETTINGS
Configure the Remote Media settings

Remote Media Support

Mount CD/DVD

Server Address for CD/DVD Images
192.168.0.6

Path in server
/root

Share Type for CD/DVD
 NFS CIFS

Same settings for storage device images

Save

Media Redirection Page

The General Media section consists of the following fields:

- ▶ **Remote Media Support:** To enable or disable Remote Media support, check/uncheck the **Enable** checkbox.
- ▶ **Mount CD/DVD:** To enable or disable Mount CD/DVD support, check/uncheck the **Enable** checkbox.



Note: You can also select all the media types simultaneously.

- ▶ **Server Address for CD/DVD Images:** Displays the address of the server where the remote media images are stored.
- ▶ **Path in server:** Displays the source path to the remote media images.

- ▶ **Share Type for CD/DVD:** Displays the share type of the remote media server either NFS or CIFS.
- ▶ **Domain Name, Username, and Password:** If share type is Samba (CIFS), then enter user credentials to authenticate on the server.
- ▶ **Same settings for storage device images:** Enable/Disable to select same media type data configurations for all the remote media types.
- ▶ **Mount Storage Device:** Enable/Disable to mount hard disk.
- ▶ **Server Address for Storage Device Images:** Address of the server where the remote media images are stored.
- ▶ **Path in server:** Source path to the remote media images.
- ▶ **Share Type for Storage Device:** To Select Share Type for hard disk.
- ▶ **Domain Name, Username, and Password:** If share type is Samba (CIFS), then enter user credentials to authenticate on the server.
- ▶ **Save:** To save the settings.

Lanner Confidential

KVM RMedia Settings

The KVM RMedia Settings page allows you to modify the allowed IP region which could access remote KVM and remote media pages. A sample screenshot of KVM & Virtual Media Subnet page is shown below:

KVM AND REMOTE MEDIA SETTINGS ?

Configure the KVM and Remote Media access settings

KVM

All IP addresses

Disabled

Subnets of specified IP addresses

(Separate multiple subnets with a semicolon)

Remote Media

All IP addresses

Disabled

Subnets of specified IP addresses

(Separate multiple subnets with a semicolon)

Save

Media Redirection Page

The KVM RMedia section consists of the following fields:

- ▶ **All IP addresses:** To allow all IP addresses to access KVM/RMedia.
- ▶ **Disabled:** To disable all IP addresses to access KVM/RMedia.
- ▶ **Subnets of specified IP addresses:** To specify allowed IP range to access KVM/RMedia.

Image Redirection

This page is used to configure the images into BMC for redirection. This can be done by mounting the image from the remote system. The displayed table shows configured images on BMC. You can configure images of the remote media server.

IMAGE REDIRECTION ?

Emulate CD/DVD/HDD images in the network to host as media through BMC.

[Refresh Image List](#)

Media Type	Media Instance	Image Name	Redirection Status	Connected Server Session Index	
CD/DVD	0	<input type="text" value="ubuntu-18.04.4-desktop-amd64.iso"/>	~	N/A	▶ ■ ▲
Hard disk	0	<input type="text" value="activedir.img"/>	~	N/A	▶ ■ ▲

Remote Media

The fields of Remote Media tab are as follows:

- ▶ **Media Type:** Displays type of Media such as CD/DVD, Hard disk.
- ▶ **Media Instance:** Displays total media instance count.
- ▶ **Image Name:** Displays the default recovery image name on the server.
- ▶ **Status:** Displays the status to host as media through BMC.
- ▶ **Session Index:** Displays Media Serve Session Index.
- ▶ **Start/Stop Redirection:** To start or stop Media redirection
- ▶ **Pause:** Pause the Media redirection.

Procedure:

1. To **Start/Stop Redirection** and configure remote media images, click (Start/Stop icon) and make sure **Remote Media Support** option is enabled.



Note: The Start Redirection button is active only for RMedia enabled users.

2. Select a configured slot and click (Start/Stop icon) to start the remote media redirection. It is a toggle button, if the image is successfully redirected, then click (Start/Stop icon) to stop the remote media redirection.



Note: Redirection needs to be stopped to clear the image.

CHAPTER 8: BMC CONFIG

This group of pages allows you to get various BMC information and modify configuration.

Date and Time

This field is used to set the date and time on the BMC. A Sample screenshot of Date and Time page is as shown below:

DATE AND TIME
Configure date, time, and NTP server settings

Jan 1, 2020 21:13:12 (GMT-05:00 EST) - America/New York

Select Time Zone
America/New_York

Automatic NTP Date & Time

Primary NTP Server
time.nist.gov

Secondary NTP Server
NTP server IP or domain name

Save

Date & Time Page

The Date & Time section consists of the following fields:

- ▶ **Configure Date & Time:** Displays time zone list containing the UTC offset along with the locations and Navigational line to select the location which can be used to display the exact local time.
- ▶ **Primary NTP Server:** To configure a primary NTP server to use when automatically setting the date and time.
- ▶ **Secondary NTP Server:** To configure a secondary NTP server to use when automatically setting the date and time.
- ▶ **Automatic Date & Time:** To automatically synchronize Date and Time with the NTP Server.
- ▶ **Save:** To save the settings.

Procedure:

1. Select the Time zone location from the map.
2. In the Primary NTP Server / Secondary NTP Server field, specify the NTP server for the device.

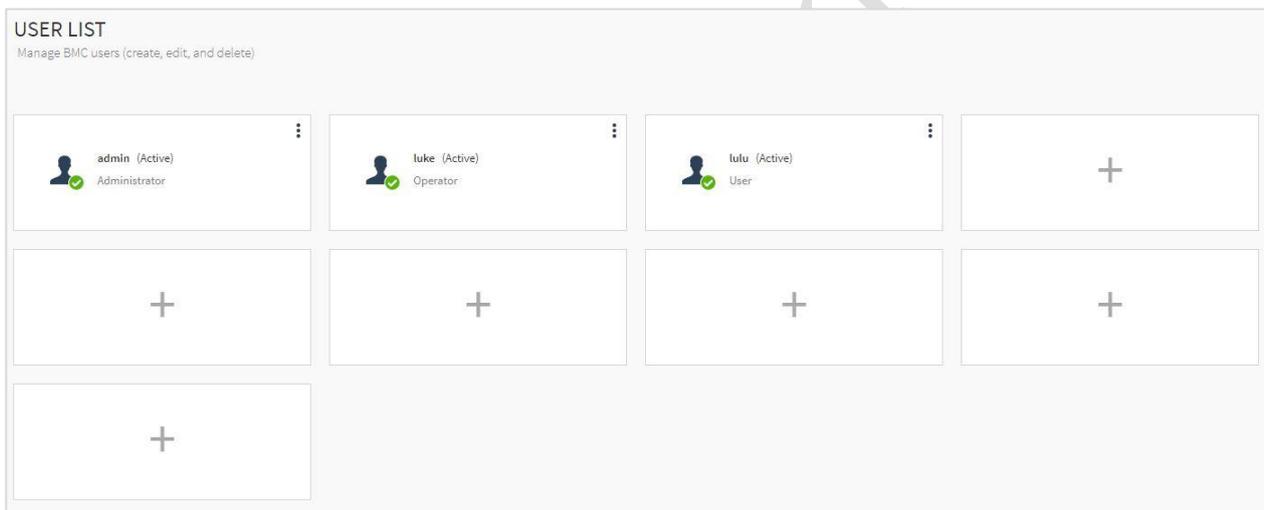


Note: Secondary NTP server is an optional field. If the Primary NTP server is not working well, the Secondary NTP Server will be tried.

3. Enable **Automatic Date & Time** option.
4. Click **Save** button to save the settings.

User List

The User List page allows you to view the current list of user slots for the BMC. You can add a new user, modify or delete the existing users. A sample screenshot of User List page is shown below:



User Management

Click user icon **+** and select any free slot to add a new user from the User Management main page.

The fields of User Management page are explained below:

- ▶ **Username:** Name of the user.
- ▶ **Password Size:** Size of password to be entered in Password field.
- ▶ **Password:** Password of the user.
- ▶ **Skip Complex Password Rules:** Skip complex password rules for the user.
- ▶ **Enable User Access:** To enable or disable the access privilege of the user.
- ▶ **Privilege:** Displays the network access privilege of the user.
- ▶ **Login Block User Management:** Show the current login blocking status, you could also change the status here.
- ▶ **SNMP Access:** To enable or disable the SNMP access for the user.

- ▶ **SNMP Access level:** Choose the access level for the user.
- ▶ **SNMP Authentication Protocol:** Choose an authentication protocol for SNMP settings.
- ▶ **SNMP Privacy Protocol:** Choose the encryption algorithm to use for SNMP settings.

Procedure to add a new user

1. To add a new user, select a free section and click on the empty section. This opens the Add User screen as shown in the screenshot below.

The screenshot shows a 'NEW USER' configuration window with the following fields and options:

- Username:** Text input field.
- Skip Complex Password Rules**
- Password Size:** Dropdown menu set to '16 bytes'.
- Password:** Text input field.
- Confirm Password:** Text input field.
- Enable User Access**
- Privilege:** Dropdown menu set to 'Administrator'.
- Login Block User Management:** Dropdown menu set to 'Enable'.
- SNMP Access**
- SNMP Access level:** Dropdown menu.
- SNMP Authentication Protocol:** Dropdown menu.
- SNMP Privacy Protocol:** Dropdown menu.

At the bottom right, there are 'Cancel' and 'Save' buttons.

User Management Configuration Page

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



Note:

- (1) Username is a string of 1 to 16 alpha-numeric characters.
- (2) It must start with an alphabetical character.
- (3) It is case-sensitive.

3. Set **Password Size** for the new password.

4. In the **Password** and **Confirm Password** fields, enter and confirm your new password.



- Note:** (1) Password should be the combination of alphabets, numbers, symbol and upper case characters. (2) White space is not allowed. (3) This field will not allow more than 16/20 characters based on Password size field value.

5. Enable or Disable the **Skip Complex Password Rules**

6. Enable or Disable the **Enable User Access** Privilege.



- Note:** (1) Enabling User Access will intern assign the IPMI messaging privilege to user.
(2) It is recommended that the IPMI messaging option should be enabled for the user to enable the User Access option, while creating User through IPMI.

7. In the **Privilege** field, select the privileges assigned to the user which could be Administrator, Operator, User or None.

8. Set the **Login Block User Management**, the options are as follows:

Enable: The user follows the rules of Login Block Settings page.

Disable: The user will never be blocked.

Blocked: The user is blocked, who can't log in until timeout.

AlwaysBlocked: The user will be blocked forever.



- Note:** All user status will be reset after updating the firmware. Please reconfiguration the status of all users.

9. Check the SNMP Access check box to enable SNMP access for the user.

10. Choose the SNMP Authentication Protocol to use for SNMP settings from the drop-down list.

11. Choose the Encryption algorithm to use for SNMP settings from the SNMP Privacy protocol drop-down list.

12. Click **Save** to save the new user and return to the users list.

Procedure to modify user

1. To modify the existing user, click on the active user tab. This opens a User screen as shown in the screenshot below.

The screenshot shows a configuration window titled "EDIT" for a user. The fields and their values are as follows:

- Username:** admin
- Logged-In Password:** (empty)
- Change Password:**
- Skip Complex Password Rules:**
- Password Size:** 16 bytes
- Password:** (empty)
- Confirm Password:** (empty)
- Enable User Access:**
- Privilege:** Administrator
- Login Block User Management:** Enable
- SNMP Access:**
- SNMP Access level:** Read Only
- SNMP Authentication Protocol:** SHA512
- SNMP Privacy Protocol:** DES

At the bottom right, there are "Cancel" and "Save" buttons.

User Management Configuration Page

2. Enter the **Current Password** of the current user.
3. Check **Change Password**, if you wish to change the existing Password.
4. Follow the steps (2 to 11) of **Procedure to add a new User**.
5. Click **Save** to save the changes and return to the users list.

RADIUS Setup

RADIUS is a modular, high performance and feature-rich RADIUS suite including server, clients, development libraries and numerous additional RADIUS related utilities. A sample screenshot of RADIUS Settings page is shown below:

The screenshot displays the 'RADIUS SETUP' configuration page. At the top, it says 'Configure RADIUS server settings'. There are two main sections, each for a RADIUS server. The first section is for the primary server, and the second is for a secondary server. Both sections have a checked checkbox to 'Enable RADIUS authentication'. The fields for each server are: Server address (192.168.0.6 for the first, 192.168.0.7 for the second), Port (1812 for both), Secret (masked with dots), and Timeout (3 for both). A 'Save' button is located at the bottom right of the form.

RADIUS SETUP
Configure RADIUS server settings

Enable RADIUS authentication

Server address
192.168.0.6

Port
1812

Secret

Timeout
3

Enable 2nd RADIUS Authentication

Server address
192.168.0.7

Port
1812

Secret

Timeout
3

Save

RADIUS Setup Page

The fields of General RADIUS Settings Page are explained below:

- ▶ **Enable RADIUS Authentication:** Option to enable/disable primary RADIUS authentication.
- ▶ **Enable 2nd RADIUS Authentication:** Option to enable/disable secondary RADIUS authentication.
- ▶ **Server Address:** The IP address of RADIUS server.
- ▶ **Port:** The RADIUS Port number.



Note:

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

- ▶ **Secret:** The Authentication Secret for RADIUS server.



Note:

- (1)This field will not allow more than 31 characters.
- (2) Secret must be at least 4 characters long.
- (3)Space is not allowed.

- ▶ **Timeout:** To specify the timeout value of authentication.
- ▶ **Save:** To save the settings.



Note: Please use the following Reply-Message to specify user privilege:

- (1) Reply-Message="privilege=Administrator"
- (2) Reply-Message="privilege=Operator"
- (3) Reply-Message="privilege=User"
- (4) Reply-Message="privilege=NoAccess"

LDAP Setup & LDAP Groups

The **Lightweight Directory Access Protocol (LDAP)/E-Directory Settings** is an application protocol for querying and modifying data of directory services implemented in Internet Protocol (IP) networks.

In Web UI, LDAP is an Internet protocol that BMC can use to authenticate users. If you have an LDAP server configured on your network, you can use it as an easy way to add, manage and authenticate BMC users. This is done by passing login requests to your LDAP Server. This means that there is no need to define an additional authentication mechanism; when using the BMC. Since your existing LDAP Server keeps an authentication centralized, you will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

LDAP/E-Directory Settings

To open LDAP/E-DIRECTORY Settings page, click **LDAP Setup** from the menu bar. A sample screenshot of LDAP Setup page is shown below:

LDAP SETUP

Configure LDAP server settings

Enable LDAP/E-Directory Authentication

Encryption Type
 No Encryption SSL StartTLS

Common Name Type
 IP Address

Server Address

Port

Bind DN

Password

Search Base

Attribute of User Login

 Save

LDAP Setup Page

Procedure:

1. Click **Enable LDAP/E-Directory Authentication** to enable LDAP/E-Directory Settings.
2. Select the encryption type for LDAP/E-Directory from the **Encryption Type**.



Note: Configure proper port number, when SSL is enabled.

3. Select the **Common Name Type** as **IP Address**.
4. Enter the IP address of LDAP server in the **Server Address** field.



Note:

- (1) IP Address is made of 4 numbers, separated by dots as in 'xxx.xxx.xxx.xxx'.
- (2) Each Number ranges from 0 to 255.
- (3) First Number must not be 0.
- (4) Supports IPv4 Address format and IPv6 Address format.
- (5) Configure FQDN address, when using StartTLS with FQDN.

5. Specify the LDAP Port in the **Port** field.



Note: (1)Default Port is 389. (2)For SSL connections, the default port is 636. (3)The Port value ranges from 1 to 65535.

6. Specify the **Bind DN** that is used during bind operation, which authenticates the client to the server.



Note:

- (1) Bind DN is a string of 4 to 64 alpha-numeric characters.
 - (2) It must start with an alphabetical character.
 - (3) Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
- Example: cn=manager,ou=login,dc=domain,dc=com

7. Enter the password in the **Password** field.



Note:

- (1) Password must be at least 1 character long.
- (2) Space is not allowed.
- (3) This field will not allow more than 48 characters.

Enter the **Search Base**. The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.



Note:

- (1) Search base is a string of 4 to 63 alpha-numeric characters.
- (2) It must start with an alphabetical character.
- (3) Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
- (4) Example: ou=login,dc=domain,dc=com

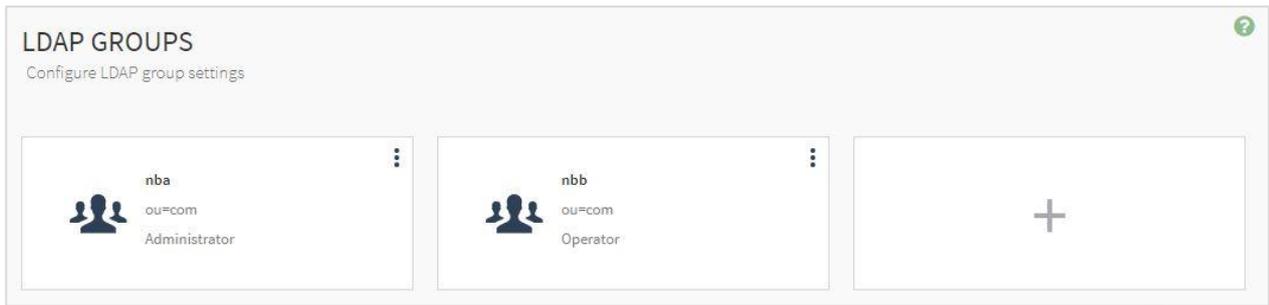
8. Select **Attribute of User Login** to find the LDAP/E-Directory server the attributes of which should be used to identify the user.



Note: It only supports **cn** or **uid**.

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

To add a new Role Group



Role Groups Page

1. In the LDAP Groups page, click **+** icon and select any free slot to add a new role group from the Add Role Group page.



Note: The Free slots are shown as “None” in all columns for the slot.

Add New Group Page

2. In the **Group Name** field, enter the name that identifies the role group.



Note:

- (1) Role Group Name is a string of 255 alpha-numeric characters.
- (2) Special symbols hyphen and underscore are allowed.

3. In the **Group Domain** field. Enter the Role Group Domain where the role group is located.



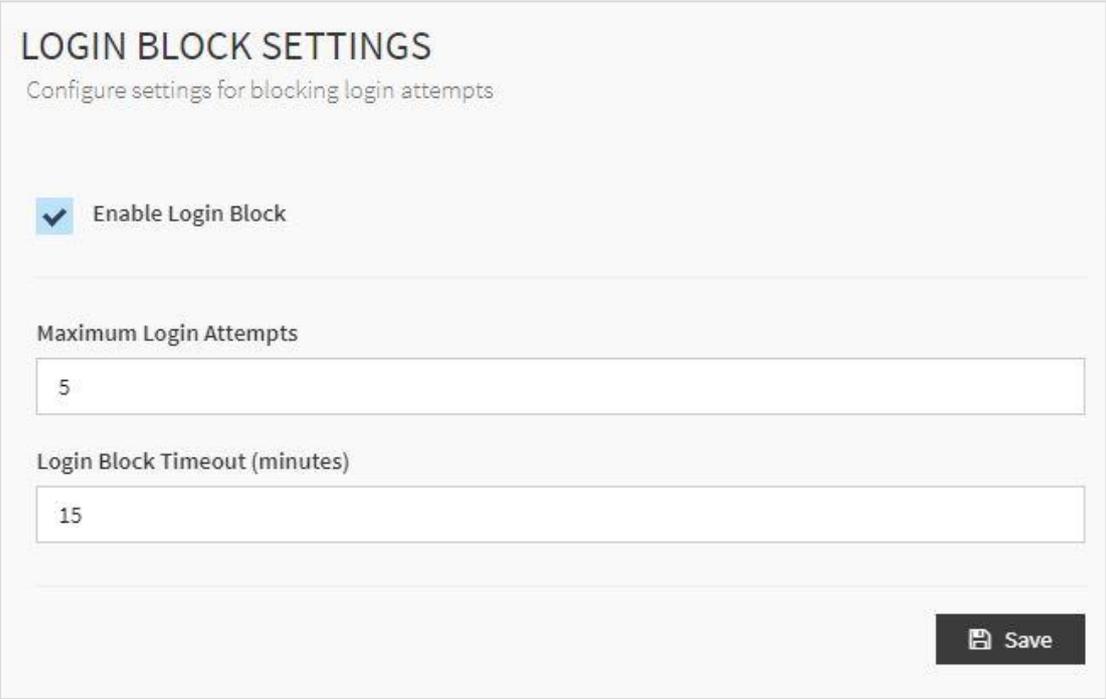
Note:

- (1) Domain Name is a string of 4 to 64 alpha-numeric characters.
- (2) It must start with an alphabetical character.
- (3) Special Symbols like dot(.), comma(,), hyphen(-), underscore(_), equal-to(=) are allowed.
- (4) Example: cn=manager,ou=login, dc=domain,dc=com

4. In the **Group Privilege** field, enter the level of privilege (User, Administrator, Operator, None) to assign to this role group.
5. Click **Save** to save the new role group and return to the Role Group List.

Login Block Settings

Login Block hinders someone from using trial and error method to login WebUI. A sample screenshot of Login Block page is shown below.



LOGIN BLOCK SETTINGS
Configure settings for blocking login attempts

Enable Login Block

Maximum Login Attempts
5

Login Block Timeout (minutes)
15

Save

Login Block Settings Page

- ▶ **Enable Login Block:** Enable or disable the whole login block function.
- ▶ **Max Login Attempt:** Max login attempts (1 ~ 99).
- ▶ **Login Block Timeout:** Time for unlocking block (1 ~ 180 min).

IP Settings

A sample screenshot of Network IP Settings page is shown below:

The screenshot displays the 'IP SETTINGS' configuration page for BMC IP settings. It is organized into three main sections: IPv4, IPv6, and VLAN. Each section has a header and a sub-header. The IPv4 section includes checkboxes for 'Enable IPv4' (checked) and 'Enable IPv4 DHCP' (unchecked), followed by input fields for IPv4 Address (192.168.0.100), IPv4 Subnet (255.255.255.0), and IPv4 Gateway (192.168.0.253). The IPv6 section includes checkboxes for 'Enable IPv6' (checked) and 'Enable IPv6 DHCP' (unchecked), followed by a dropdown for IPv6 Index (0), an input field for IPv6 Address (9001::100), and an input field for Subnet Prefix Length (64). The VLAN section includes a checked 'Enable VLAN' checkbox, followed by input fields for VLAN ID (2) and VLAN Priority (0). A 'Save' button is located at the bottom right of the form.

Network IP Settings Page

- ▶ **Enable LAN:** To enable or disable the LAN Settings.
- ▶ **LAN Interface:** Lists the LAN interfaces.
- ▶ **MAC Address:** This field displays the MAC Address of the device. This is a read-only field.
- ▶ **Enable IPv4:** This option is to enable/disable the IPv4 settings in the device.

- ▶ **Enable IPv4 DHCP:** This option is to enable IPv4 DHCP support for the selected interface.
- ▶ **IPv4 Address, IPv4 Subnet Mask, and IPv4 Default Gateway:** These fields are for specifying the static IPv4 address, Subnet Mask, and Default Gateway to be configured to the device.



Note:

- (1)IP Address is made of 4 numbers, separated by dots as in "xxx.xxx.xxx.xxx".
- (2)Each Number ranges from 0 to 255.
- (3)The first Number must not be 0.

- ▶ **Enable IPv6:** To Enable/Disable the IPv6 configuration settings.
- ▶ **Enable IPv6 DHCP:** To Enable/Disable the IPv6 settings in the device. It dynamically configures IPv6 address using DHCP (Dynamic Host Configuration Protocol).
- ▶ **IPv6 Index:** To specify a static IPv6 Index to be configured to the device. E.g.: 0
- ▶ **IPv6 Address:** To specify a static IPv6 address to be configured to the device. E.g, 2004::2010
- ▶ **Subnet Prefix length:** To specify the subnet prefix length for the IPv6 settings.



Note: This value ranges from 0 to 128.

Procedure:

1. Check **Enable LAN** to enable LAN support for the selected interface.
2. Select the **LAN Interface** to be configured.
3. Check Enable IPv4 to enable IPv4 support for the selected interface.
4. Check **Enable IPv4 DHCP** to dynamically configure IPv4 address using DHCP.
5. If the field is disabled, enter the **IPv4 Address, IPv4 Subnet Mask** and **IPv4 Default Gateway** in the respective fields.
6. In IPv6 Configuration, if you want to enable the IPv6 settings, check **Enable IPv6**.
7. If the IPv6 setting is enabled, enable or disable the option **Enable IPv6 DHCP**.
8. If the field is disabled, enter the **IPv6 Address, Subnet Prefix length** and **IPv6 Index** in the given field.
9. Click **Save** to save the entries.

DNS Settings

The **Domain Name System (DNS)** is a distributed hierarchical naming system for computers, services, or any resource connected to the Internet or a private network. It associates the information with domain names assigned to each of the participants. Most importantly, it translates domain names meaningful to humans into the numerical (binary) identifiers associated with networking equipment for the purpose of locating and addressing these devices worldwide.

The DNS Server settings page is used to manage the DNS settings of a device. A sample screenshot of DNS Configuration page is shown below:

DNS SETTINGS
Configure the DNS settings

DNS Enabled

Host Name Setting
 Automatic Manual

Host Name
luke

Domain Name Setting
 Automatic Manual

Domain Name Server Setting
 Automatic Manual

DNS Server 1
8.8.8.8

DNS Server 2
8.8.4.4

DNS Server 3
8.8.8.2

Save

DNS Configuration Page

- ▶ **DNS Enabled:** To enable/disable all the DNS Service Configurations.
- ▶ **Host Name Settings:** Choose either Automatic or Manual settings. It displays hostname of the device. If the Host setting is chosen as Manual, then specify the hostname of the device.



Note:

(1) This value ranges from 1 to 64 alpha-numeric characters.

(2) Special characters '-'(hyphen) and '_'(underscore) are allowed.

(3) It must not start or end with a '-'(hyphen).

(4) IE browsers won't work correctly if any part of the hostname contains underscore (_) character.

- ▶ **Domain Name Setting:** Select whether the domain interface will be configured manually or automatically.



Note: If you select "Automatic", it displays the "Domain Interface" option. If you select "Manual", it displays "Domain name".

- **Automatic** - If you Select **Automatic**, the Domain Name cannot be configured as it will be done automatically. The field will be disabled.

Domain Interface: Select the network interface the domain of which is to be configured.

- **Manual** - If the Domain setting is chosen as **Manual**, specify the domain name of the device.

Domain Name: It displays the domain name of the device.

- ▶ **Domain Name Server Setting**



Note: If you select "Automatic", it displays the "IP Priority" option. If you select "Manual" it displays "DNS Server 1, 2 & 3".

- **Automatic** - If you select Automatic "DNS Interface" option should be explained.

IP Priority:

If IP Priority is **IPv4**, it will have 2 IPv4 DNS servers and 1 IPv6 DNS server.

If IP Priority is **IPv6**, it will have 2 IPv6 DNS servers and 1 IPv4 DNS server.

- **Manual** - Specify the DNS (Domain Name System) server address to be configured for the BMC.

DNS Server 1, 2 & 3:

DNS Server Address will support the following:

- IPv4 Address format.
- IPv6 Address format.



Note: (1) IPv4 Addresses should be given in dotted decimal representation.
(2) IPv6 Addresses are supported and must be global unicast addresses.

- ▶ **Save:** To save the entered changes.

Procedure:

1. In **Domain Name Service Configuration**, Enable **DNS Service**.

- Check the option **DNS Enabled** to enable all the DNS Service Configurations.

2. Choose the **Host Name Setting** either Automatic or Manual



Note: If you choose Automatic, you need not enter the Host Name; on the other hand, if you choose Manual, you need to enter the Host Name.

3. Enter the **Host Name** in the given field if you have chosen Manual Configuration.

4. In the **Domain Settings**,

- Select the domain settings (Automatic or Manual).

- Enter the **Domain Name** in the given field if the option "**Manual**" has been selected in domain settings field.

5. In **Domain Name Server Setting**,
 - Select the **DNS Name Server Setting**.
 - Choose the IP Priority, either IPv4 or IPv6.
 - Enter the DNS Server address.
6. In DNS Server1, DNS Server2 and DNS Server3, enter the server addresses to be configured for the BMC.
7. Click **Save** to save the entries.

Link Settings

This page is used to configure the network link configuration for available network interfaces. A sample screenshot of Link Settings page is shown below:

LINK SETTINGS
Configure the BMC port link speed and duplex mode settings

Auto Negotiation

Link Speed
100 Mbps

Duplex Mode
FULL Duplex

Save

Network Link Configuration Page

The fields of Network Link Configuration page are explained below:

- ▶ **LAN Interface:** Select the required network interface from the drop-down list.
- ▶ **Auto Negotiation:** This option is enabled to allow the device to perform automatic configuration to achieve the best possible mode of operation (speed and duplex) over a link.
- ▶ **Link Speed:** Link speed will list all the supported capabilities of the network interface.
- ▶ **Duplex Mode:** Duplex Mode could be either Half Duplex or Full Duplex.
- ▶ **Save:** To save the settings.

Procedure:

1. Select the **LAN Interface** from the drop-down list.

2. Select either **Enable** or **Disable** for **Auto Negotiation**.



Note: The Link Speed and Duplex Mode will be active only when Auto Negotiation is OFF.

3. Select the **Link Speed** from the drop-down list.
4. Select the **Duplex Mode** either Full duplex or Half Duplex.
5. Click **Save** to save the configuration.

SSL Certificate

The **Secure Socket Layer** protocol was created by Netscape to ensure secure transactions between web servers and browsers. The protocol uses a third party, a **Certificate Authority (CA)**, to identify one end or both end of the transactions.

Use Web UI to configure SSL certificate into the BMC. Using this, the device can be accessed in a secured mode. A sample screenshot of SSL Certificate page is shown below:

SSL CERTIFICATE

Generate
Upload

Shows SSL certificate information and lets you generate/upload an SSL certificate

Certificate Version	Serial Number
1	AF60B43607294B59
Signature Algorithm	Public Key
sha256WithRSAEncryption	(2048 bit)

Issuer Common Name (CN)	Issuer Organization (O)
00:1C:7F:44:F9:6E	BMC
Issuer Organization Unit (OU)	Issuer City or Locality (L)
BMC	BMC
Issuer State or Province (ST)	Issuer Country (C)
TW	TW
Issuer Email Address	
support@oem.com	

SSL Certificate Page

- ▶ **Generate:** The button is used to generate the SSL certificate based on configuration details.
- ▶ **Upload:** The button is used to upload the certificate and private key file into the BMC.

Generate SSL Certificate

GENERATE CERTIFICATE [?] [X]

Common Name (CN)

Organization (O)

Organization Unit (OU)

City or Locality (L)

State or Province (ST)

Country (C)

Email Address

Valid for

Key Length

Generate SSL Certificate Page

The fields of SSL Settings – Generate SSL Certificate are explained below.

- ▶ **Common Name (CN):** Common name for which certificate is to be generated.
 - Maximum length of 64 characters.
 - It is a string of alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- ▶ **Organization (O):** Organization name for which the certificate is to be generated.
 - Maximum length of 64 characters.
 - It is a string of alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- ▶ **Organization Unit (OU):** Overall organization section unit name for which certificate is to be generated.
 - Maximum length of 64 characters.
 - It is a string of alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- ▶ **City or Locality (L):** City or Locality of the organization (mandatory).
 - Maximum length of 128 characters.
 - It is a string of alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- ▶ **State or Province (ST):** State or Province of the organization (mandatory).
 - Maximum length of 64 characters.
 - It is a string of alpha-numeric characters.
 - Special characters '#' and '\$' are not allowed.
- ▶ **Country (C):** Country code of the organization (mandatory).
 - Only two characters are allowed.
 - Special characters are not allowed.
- ▶ **Email Address:** E-mail Address of the organization (mandatory).
- ▶ **Valid for:** Validity of the certificate.
 - Value ranges from 1 to 3650 days.
- ▶ **Key Length: The key length bit value of the certificate.**
- ▶ **Save:** To generate the new SSL certificate.



Note: HTTPs service will restart, to use the newly generated SSL certificate.

Upload SSL Certificate

A sample screenshot of Upload SSL Certificate Page is shown below:

Upload SSL Certificate Page

The fields of SSL Settings – Upload SSL Settings tab are explained below:

- ▶ **Current Certificate:** Current certificate and uploaded date/time will be displayed (read-only).
- ▶ **New Certificate:** Certificate file should be of pem type
- ▶ **Current Private Key:** Current private key information will be displayed (read-only).
- ▶ **New Private Key:** Private key file should be of pem type
- ▶ **Upload:** To upload the SSL certificate and privacy key into the BMC.



Note: After a successful upload, HTTPs service will restart to use the newly uploaded SSL certificate.

Procedure:

1. Click the Upload SSL Certificate tab, Browse the New Certificate and New Private key.
2. Click Upload to upload the new certificate and private key.
3. In Generate SSL Certificate, enter the following details in the respective fields
 - The **Common Name** for which the certificate is to be generated.
 - The **Organization** for which the certificate is to be generated.
 - The **Organization Unit** name for which certificate to be generated.
 - The **City or Locality** of the organization
 - The **State or Province** of the organization
 - The **Country** of the organization
 - The **Email address** of the organization.
 - The number of days the certificate will be valid in the **Valid For** field.
4. Choose the **Key Length** bit value of the certificate
5. Click **Save** to generate the certificate.



Note:

- (1) Once you Upload/Generate the certificates, only HTTPs service will restart.
- (2) You can now access your BMC securely using the following format in your IP Address field from your Internet browser: **https://<your BMC's IP address here>**
- (3) For example, if your BMC's IP address is 192.168.0.30, enter the following: https://192.168.0.30.
- (4) Please append the <s> to <http>. You must accept the certificate before you are able to access your BMC.

Services

This page displays the basic information about services running in the BMC. Only Administrator can modify the service. A sample screenshot of Services Page is shown below:

The screenshot shows a web interface titled "SERVICES" with a subtitle "Shows active/inactive service information". It contains a table with the following columns: Service, Status, Interfaces, Non Secure Port, Secure Port, Timeout, and Maximum Sessions. Each row represents a service and includes edit and delete icons.

Service	Status	Interfaces	Non Secure Port	Secure Port	Timeout	Maximum Sessions
web	Active	eth0	N/A	443	1800	20
kvm	Active	eth0	N/A	443	1800	4
cd-media	Active	eth0	N/A	443	N/A	1
hd-media	Active	eth0	N/A	443	N/A	1

Services Page

The fields of Services Page are explained below:

- ▶ **Services:** Displays service name of the selected slot (read-only).
- ▶ **Status:** Displays the current status of the service, either active or inactive state.
- ▶ **Interfaces:** It shows the interface in which service is running.
- ▶ **Nonsecure Port:** This port is used to configure nonsecure port number for the service.
- ▶ **Secure Port:** Used to configure secure port number for the service.
- ▶ **Timeout:** Displays the session timeout value of the service.
- ▶ **Maximum Sessions:** Displays the maximum number of allowed sessions for the service.

To view the Active Sessions

1. Click icon  to view the details about the active sessions for the service.
2. This opens the **Active Session** screen as shown in the screenshot below.

The screenshot shows a web interface titled "SERVICE SESSIONS" with a subtitle "Active Session - Web". It contains a table with the following columns: Session ID, Session Type, User ID, User Name, Client IP, and Privilege. A red 'X' icon is visible in the bottom right corner of the table area.

Session ID	Session Type	User ID	User Name	Client IP	Privilege
1	Web HTTPS	2	admin	192.168.0.2	Administrator

Service Sessions Page

- ▶ **Session Type:** Displays the type of the active sessions.
- ▶ **User Name:** Displays the name of the user.
- ▶ **Client IP:** Displays the IP addresses that are already configured for the active sessions.
- ▶ **Privilege:** Displays the access privilege of the user.

3. Select a slot and click icon  to terminate the particular session of the service.

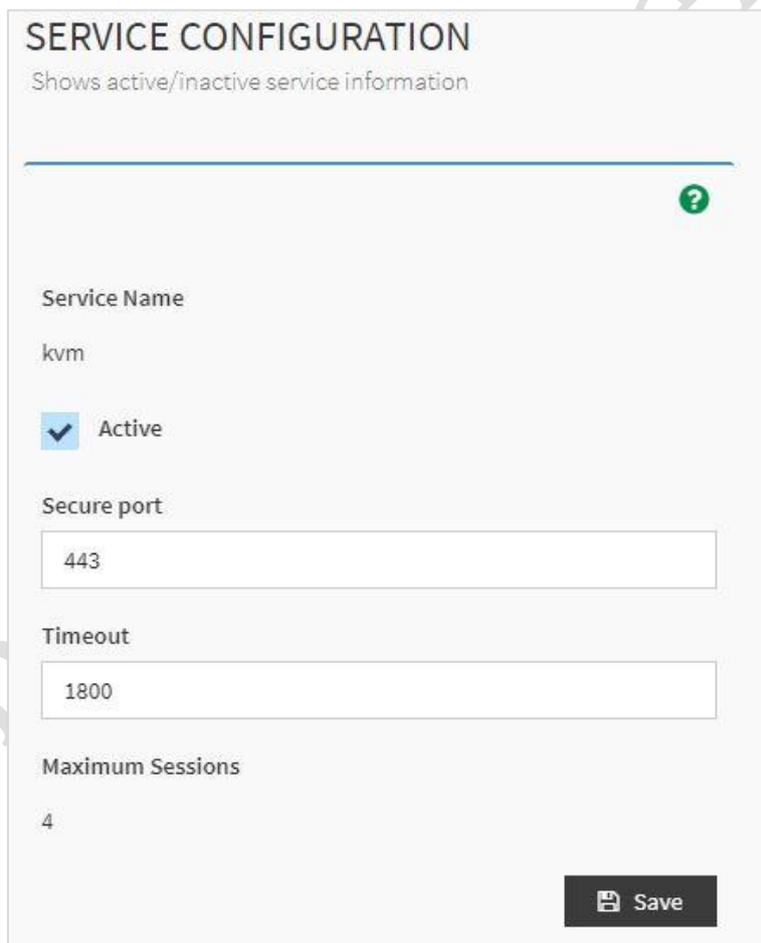
To modify the existing services

1. Select a slot and click icon  to modify the configuration of the service.



Note: Whenever the configuration has been modified, the service will be restarted automatically. User has to close the existing opened session for the service if needed.

2. This opens the **Service Configuration** screen as shown in the screenshot below.



SERVICE CONFIGURATION
Shows active/inactive service information

Service Name
kvm

Active

Secure port
443

Timeout
1800

Maximum Sessions
4

Save

Service Configuration Page

3. **Service Name** is a read-only field.

4. Activate the Current State by enabling the **Active** checkbox.



Note: Interfaces, Time out and Maximum Sessions will not be active unless the current state is active.

5. Choose any one of the available interfaces from the **Interface Name** drop-down list.
6. Enter the timeout value in the **Timeout** field.



Note: The values in the Maximum Sessions field cannot be modified.

7. Click **Save** to save the entered changes else click **Cancel** to exit.

Remote Syslog

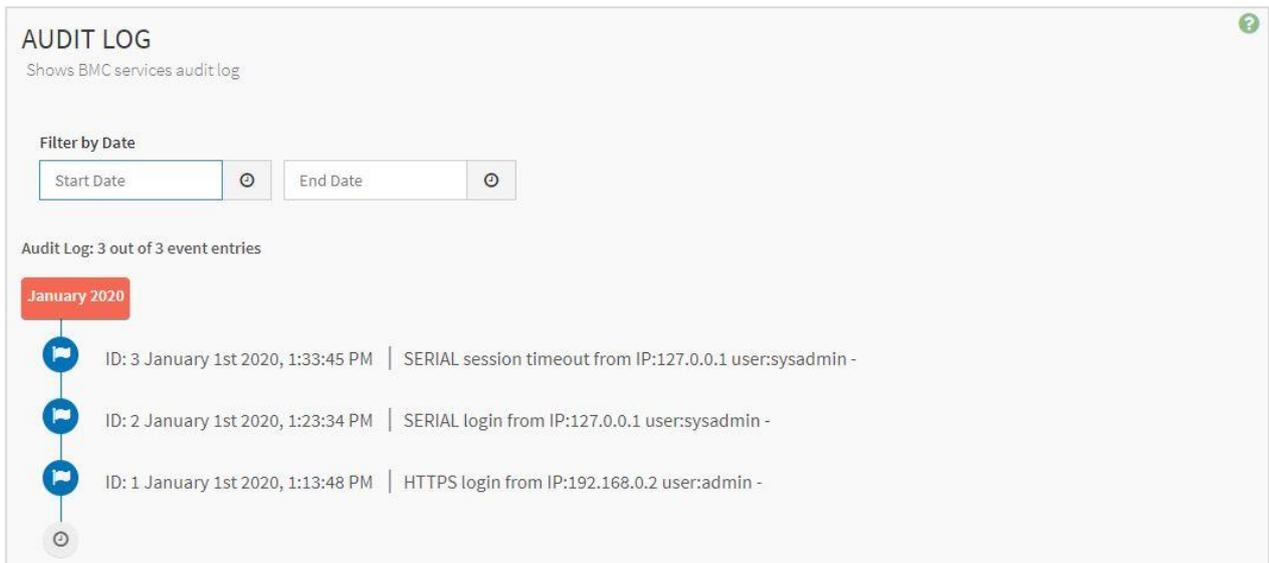
This page is used to configure the remote Syslog configuration for letting BMC send Syslog, such as configuration change and system power status change to the remote. A sample screenshot of the Remote Syslog page is shown below:

The fields of Remote Syslog Page are explained below:

- ▶ **Enable Remote Syslog:** To enable/disable remote Syslog.
- ▶ **Port Type:** Choose either UDP or TCP settings. It determines the transmission protocol.
- ▶ **Remote Log Server:** The IP address of remote Syslog server.
- ▶ **Remote Server Port:** The port of remote Syslog server.

Audit Log

This page records the access event of serial, https and KVM. You can use the date filter option to view those specific events. A sample screenshot of Event Log page is shown below:



Audit Log Page

The Audit Log page consists of the following Fields:

- ▶ **Filter by Date:** Filtering can be done by selecting **Start Date** and **End Date**.

Firmware Update

This wizard takes you through the process of firmware upgrade. A reset of the box will automatically follow if the upgrade is completed or canceled. An option to Preserve All Configuration is available. Enable it, if you wish to preserve configured settings through the upgrade. A sample screenshot of Firmware Update Page is shown below.



Warning: Please note that after entering update mode widgets, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is canceled in the middle of the wizard, the device will be reset.



Note: The firmware upgrade process is a crucial operation. Make sure that the chances of a power or connectivity loss are minimal when performing this operation. Once you enter into Update Mode and choose to cancel the firmware flash operation, the BMC must be reset. This means that you must close the Internet browser and log back onto the BMC before you can perform any other types of operations. Once Firmware upgrade using web is started, the regular IPMI command will not be allowed for safety concern.

FIRMWARE UPDATE

Select the firmware image to upgrade/downgrade

Select Firmware Image

...

Verify Image File

Preserve all Configuration. This will preserve all the configuration settings during the firmware update - irrespective of the individual items marked as preserve/overwrite in the table below.

Click "Edit Preserve Configuration" to modify the Preserve status settings.

[Edit Preserve Configuration](#)

S.No	Preserve Configuration Item	Preserve Status
1	SEL	Overwrite
2	IPMI & NETWORK	Overwrite
3	NTP	Overwrite
4	KVM	Overwrite
5	AUTHENTICATION	Overwrite

Note: When you click 'Upload', the firmware upload process begins and the firmware version is shown. To continue with the actual firmware upgrade, click 'Flash'.

Upload

Firmware Update Page

The various fields of Firmware Update are as follows.

- ▶ **Preserve all Configuration:** To preserve all configuration.
- ▶ **Edit Preserve Configuration:** To modify the Preserve status settings.
- ▶ **Select Firmware Image:** To Select the Firmware image to be uploaded.
- ▶ **Upload:** To Start the Firmware Upload.

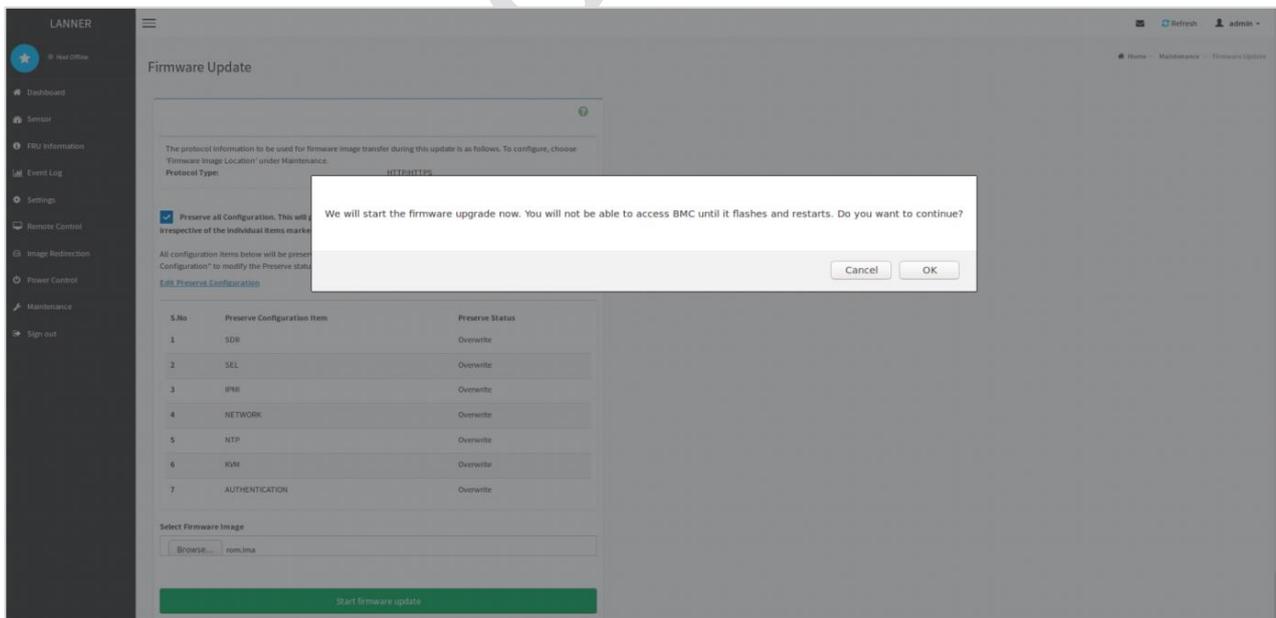
This wizard takes you through the process of firmware upgrade. The protocol information to be used for firmware image transfer during this update is as follows.



Note: All configuration items will be preserved/overwrite as default during the restore configuration operation.

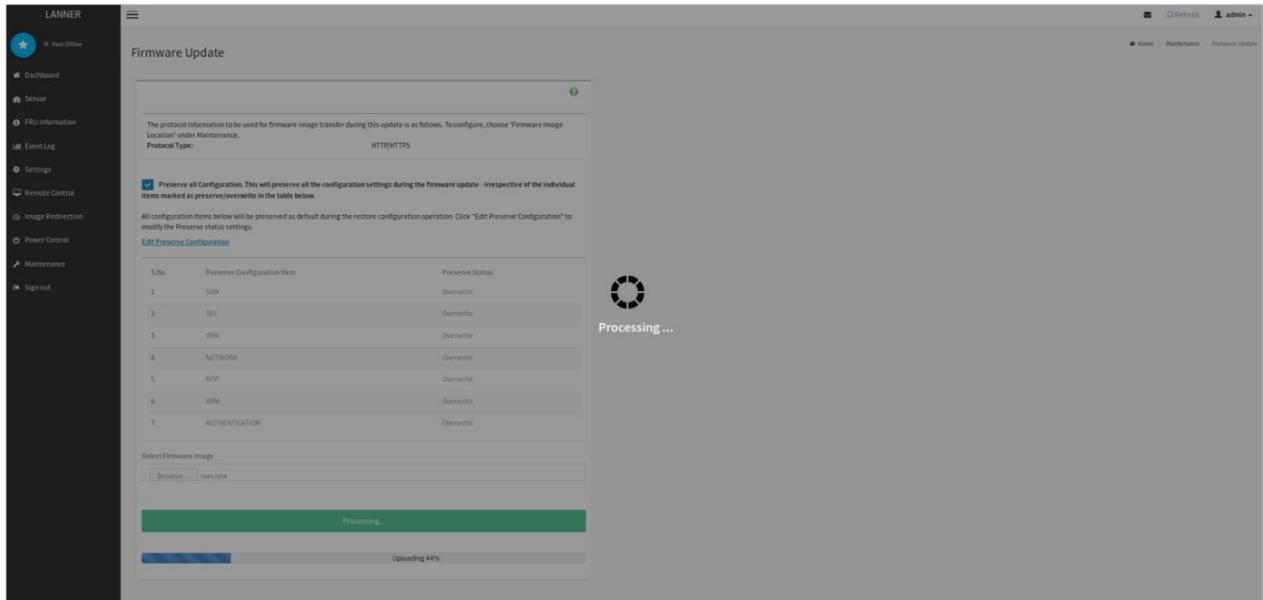
Procedure:

1. Click **Preserve all Configuration** to preserve all configurations.
2. Click **Browse** to select firmware image. The Firmware update undergoes the following steps:
 - A. Closing all active client requests
 - B. Preparing Device for Firmware Upgrade
 - C. Uploading Firmware Image
 - D. Browse and select the Firmware image to flash and click Upload.
 - E. Click **Upload** to start the Firmware Update. A warning message will be prompted you to proceed further, which is shown below.



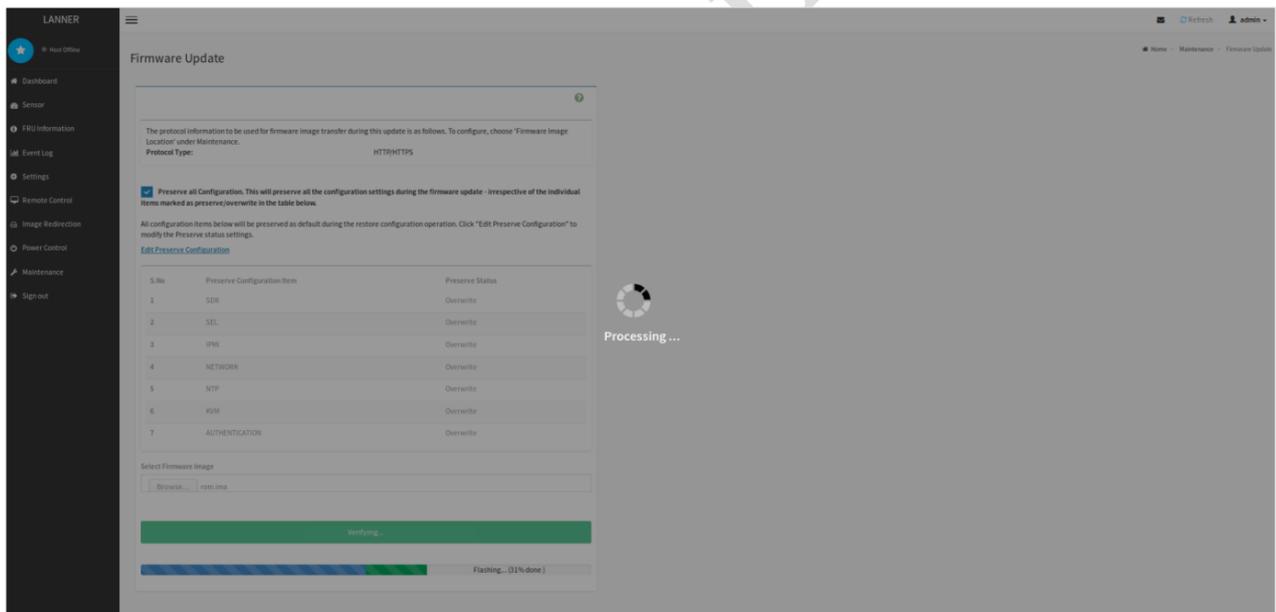
Firmware Update – Warning

F. Click **OK** to start the Firmware Update. The sample screenshot is shown below:



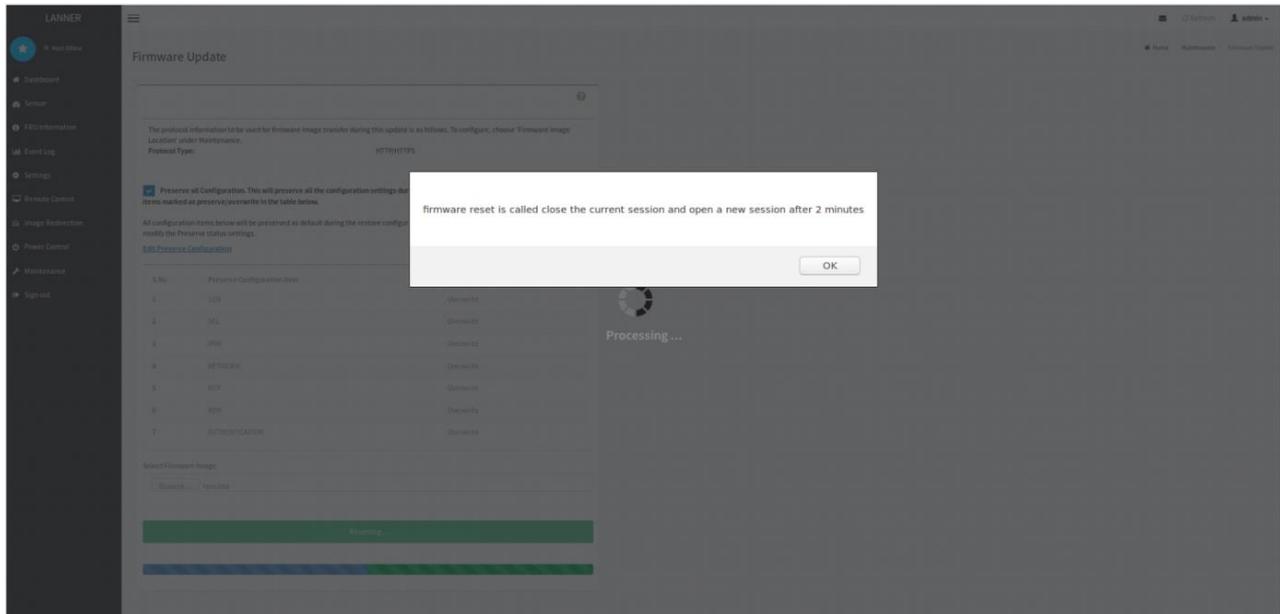
Firmware Update - Image Upload

G. Verifying and Flashing Firmware Image



Firmware Update - Image Flashing

H. Resetting the image. The screenshot of Firmware update is as shown below.



Firmware Update - Resetting



Note: The Firmware Update page will be disabled and you will not be able to perform any other tasks until firmware upgrade is completed and the device is rebooted. You can now follow the instructions presented in the subsequent pages to successfully update the BMC firmware. The device will reset if update is canceled. The device will also reset upon successful completion of firmware update.

Restore Factory Defaults

The option is used to restore the factory defaults of the device firmware. This section lists the configuration items that will be preserved during restore factory default configuration. A sample screenshot of Restore Factory Defaults Page is shown below:

 **Warning:** Please note that after entering restore factory widgets, other web pages and services will not work. All open widgets will be closed automatically. The device will reset and reboot within few minutes.



RESTORE FACTORY DEFAULTS

The selected configuration options are preserved when restoring factory defaults or updating firmware.

- SEL
- IPMI & Network
- NTP
- SNMP
- KVM
- Authentication

Restore

Restore Factory Defaults

Procedure

1. Click **Preserve Configuration** to redirect to Preserve Configuration page, which is used to keep the particular configuration from being overwritten by the default configuration.
2. Click **Restore** to restore the factory defaults of the device firmware.

Preserve Configuration

This page allows the user to configure the preserve configuration items, which will be used by the Restore factory defaults to keep the existing configuration from being overwritten by defaults/ Firmware Upgrade configuration. A sample screenshot of Preserve Configuration page is shown below.



Note: You can navigate to the [Firmware Update Page](#) and [Restore Factory Defaults](#) by clicking the respective links.

PRESERVE CONFIGURATION

Select the options to preserve when restoring factory defaults or updating firmware

Click here to go to [Firmware Update](#) or [Restore Factory Defaults](#)

Check All

SEL

IPMI & Network

NTP

SNMP

KVM

Authentication

Preserve Configuration Page

The various fields of Preserve Configuration are as follows.

- ▶ **Click here to go to Firmware Update or Restore Configuration:** This link will redirect to the Firmware Update or Restore Configuration page which needs to be preserved.
- ▶ **Check All:** To check the entire configuration list.
- ▶ **SEL:** Files contain the system event logs that are being logged by the IPMI.
- ▶ **IPMI & Network:** Contain the IPMI and network configurations such as user, IP and DNS settings.

- ▶ **NTP:** Contain the NTP daemon protocol configuration parameters such as synchronization sources.
- ▶ **KVM:** Contain the image name and the remote machine information like IP address, username, password, domain name and share type, the mouse mode configurations and host machine physical keyboard.
- ▶ **Authentication:** Contain the radius, LDAP, username, password, role group, and user login information.
- ▶ **Save:** To save any changes made.



Note: This configuration is used by Restore Factory Defaults process.

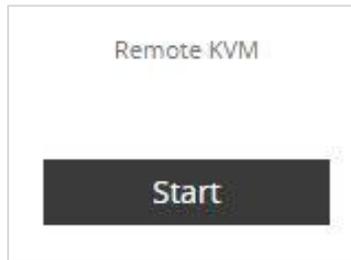
Procedure:

1. Click **Firmware Update** or **Restore Configuration** link to view Firmware Update or Restore Configuration page accordingly.
2. Select the required Preserve Configuration items by either choosing the items individually by selecting the appropriate checkboxes or by selecting all or none using **Check All**.
3. Click **Save** to save the changes.

Lanner Confidential

CHAPTER 9: REMOTE KVM

To open Remote Control page, click **Stark** from the Remote KVM of the Dashboard page. A sample screenshot is shown below.



Remote KVM button

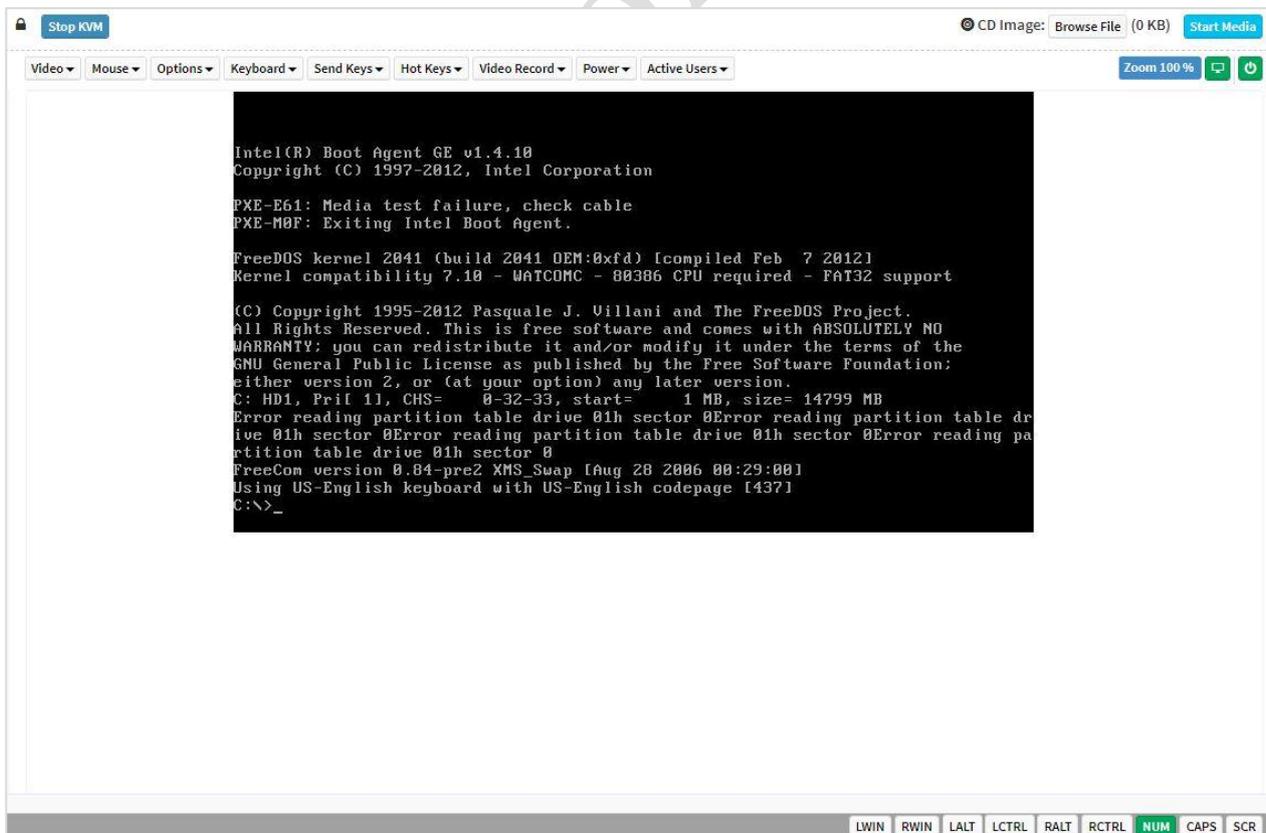
A detailed description of the menu items are given below.

Click **Stark** to open the Remote KVM page:

- ▶ **Start KVM:** Starts the video redirection.
- ▶ **Stop KVM:** Stops the video redirection.
- ▶ **Browse File:** Used to select the CD image file to be redirected to the host.
- ▶ **Start Media:** Redirects the selected CD image file to the host.
- ▶ **Stop Media:** Stops the CD media redirected to the host.

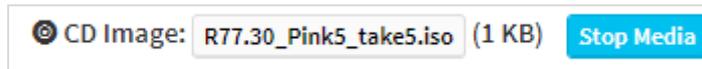
Procedure to Start KVM

1. Click **Start KVM** to start the video redirection. A sample screenshot is as shown below.



Start KVM

2. Click **Browse** to select **CD Image**.
3. Click **Start Media** to redirect the selected CD image file to the Host. A sample screenshot is as shown below.



Start Media

4. To stop the recording, click **Stop Record**.

Settings

Video

This menu contains the following sub menu items:

- ▶ **Pause Video:** This option is used for pausing Console Redirection.
- ▶ **Resume Video:** This option is used to resume the Console Redirection when the session is paused.
- ▶ **Refresh Video:** This option can be used to update the display shown in the Console Redirection window.
- ▶ **Host Display:**
 - **Display on:** If you disable this option, the display will be shown on the screen in Console Redirection
 - **Display off:** If you enable this option, the server display will be blank but you can view the screen in Console Redirection. If you disable this option, the display will be back on the server screen.
- ▶ **Capture Screen:** This option helps to take the screenshot of the host screen and save it in the client's system.

Mouse

- ▶ **Show Client Cursor:** This menu item can be used to show or hide the local mouse cursor on the remote client system.
- ▶ **Mouse Mode:** This option handles mouse emulation from local window to remote screen using either of the two methods. Only 'Administrator' has the right 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:** This mouse mode sets the client cursor in the middle of the client system and will send the deviation to the host. This mouse mode is specific for SUSE Linux installation.



Note: Client cursor will be hidden always. If you want to enable, use Alt + C to access the menu.

Options

The Bandwidth Usage option allows you to adjust the bandwidth. You can select one of the following options.

- ▶ **Block Privilege Request:** To enable or disable the access privilege of the user.

Keyboard

List of Host Physical Keyboard languages supported in H5Viewer.

-English U.S

-German

-Japanese

Send Keys

This option is used to key items. This menu contains the following sub menu items.

- Hold Down

- Press and Release

▶ Hold Down

This menu contains the following sub menu items.

-**Right Ctrl Key:** This menu item can be used to act as the right-side <CTRL> key when in *Console Redirection*.

-**Right Alt Key:** This menu item can be used to act as the right-side <ALT> key when in *Console Redirection*.

-**Right Windows Key:** This menu item can be used to act as the right-side <WIN> key when in *Console Redirection*.

-**Left Ctrl Key:** This menu item can be used to act as the left-side <CTRL> key when in *Console Redirection*.

-**Left Alt Key:** This menu item can be used to act as the left-side <ALT> key when in *Console Redirection*.

-**Left Windows Key:** This menu item can be used to act 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.

▶ Press and Release

This menu contains the following sub menu items.

-**Ctrl+Alt+Del:** This menu item can be used to act as if you depressed the <CTRL>, <ALT> and keys down simultaneously on the server that you are redirecting.

-**Left Windows Key:** This menu item can be used to act 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:** This menu item can be used to act as the right-side <WIN> key when in *Console Redirection*.

-**Context Menu Key:** This menu item can be used to act as the context menu key, when in *Console Redirection*.

-Print Screen Key: This menu item can be used to act as the print screen key, when in Console Redirection.

-Hot Keys: This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.

Add Hot Keys

This menu is used to enable macros. Click **Add** to macros.

Video Record

This menu contains the following sub menu items.

-Record Video: This option is to start recording the screen.

-Stop Recording: This option is used to stop the recording.

-Record Settings: This option is used to set Video Recording Duration.

Power

The power options are to perform any power cycle operation. Click on the required option to perform the following operation.

-Hard Reset: To reboot the system without powering off (warm boot).

-Power Off: To power off system immediately.

-Orderly Shutdown: To power off system orderly.

-Power On: To power on the server.

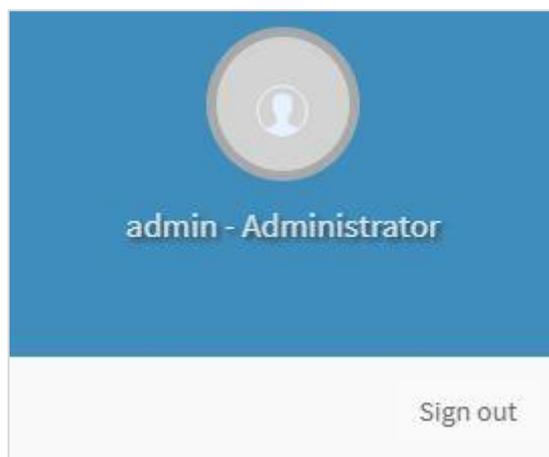
-Power Cycle: To first power off, and then reboot the system (cold boot).

Active Users

Click this option to displays the active users and their system IP address.

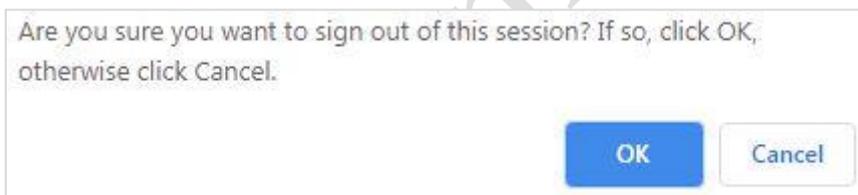
CHAPTER 10: SIGN OUT

To log out from the WebUI, click **admin** on the top right corner of the screen. A sample screenshot of **admin** option is shown below:



admin – Sign out

Click **Sign Out** to log out from the Web UI. A warning message will prompt you to proceed, click **OK** to log out, else click **Cancel** to retain the Web UI.



Warning message – Sign out

APPENDIX A: NOTE AND REMARK

1. KVM timeout mechanism

KVM will not timeout when there is mounting image or keyboard/mouse signal; however, the VGA signal will not reset timeout counter.

2. KVM usage in IPv6+IE11 situation

In Microsoft Windows operating systems, IPv4 addresses are valid location identifiers in Uniform Naming Convention (UNC) path names. However, the colon ':' is an illegal character in a UNC path name. Thus, the use of IPv6 addresses is also illegal in UNC names.

For Internet Explorer 11 web browser, in order to launch an IPV6 https H5Viewer session, the domain name in the certificate should be in IPV6 literal address format. Otherwise, H5Viewer won't be able to launch properly.

Example: If IPv6 address is "fe80::238:28ff:fe33:4858", you need to use "fe80--238-28ff-fe33-4858.ipv6-literal.net" in IE11.

3. NCSI setting limitation

BMC could not control NCSI LAN port (include speed and duplex) when host on due to the control has been taken from host.

APPENDIX B: FEATURE LIST

- Sensor Monitor
- Smart Fan Control
- FRU Information
- LAN/NCSI Configuration
- UART/Super IO Configuration
- Serial over LAN (SOL)
- KVM and Virtual Media
- Net-SNMP
- BIOS Remote Update
- First Time Wizard
- Transceiver Information

Lanner Confidential

APPENDIX C: CUSTOMIZATION REQUEST FORM

Lanner Customization BMC Request Form			
Project Name		Customer	
SKU		Request Date	
Item	Modify	Description	
1. Network Settings	<input type="checkbox"/>	IP address: _____ Netmask: _____ Gateway IP: _____	
2. Remote Media	<input type="checkbox"/>	Number of CD/DVD Devices (Max:3): _____ Number of Floppy Devices (Max:3): _____ Number of HDD Devices (Max:3): _____ Device Vendor Name (Max 8 Chars): _____	
3. Web Logo&String	<input type="checkbox"/>	Include left side, right side (optional) and background of banner. Picture heights are 73 pixels, width are without limitation.	
	<input type="checkbox"/>	WebUI Vendor Name (Max 17 Chars): _____	
4. FRU	<input type="checkbox"/>	Chassis Info Area Chassis Type: _____ Part Number: _____	
	<input type="checkbox"/>	Board Info Area Manufacturer: _____ Product Name: _____ Part Number: _____	
	<input type="checkbox"/>	Product Info Area Manufacturer: _____ Product Name: _____ Part Number: _____ Product Version: _____ Asset Tag: _____	
5. SSL Certificate	<input type="checkbox"/>	Common Name (CN): _____ Organization (O): _____ Organization Unit (OU): _____ City or Locality (L): _____ State or Province (ST) : _____ Country (C): _____ Email Address: _____ Key Length(1024 bits or 2048 bits): _____	
6. First Time Wizard	<input type="checkbox"/>	<input type="checkbox"/> Not needed	
7. Remarks			