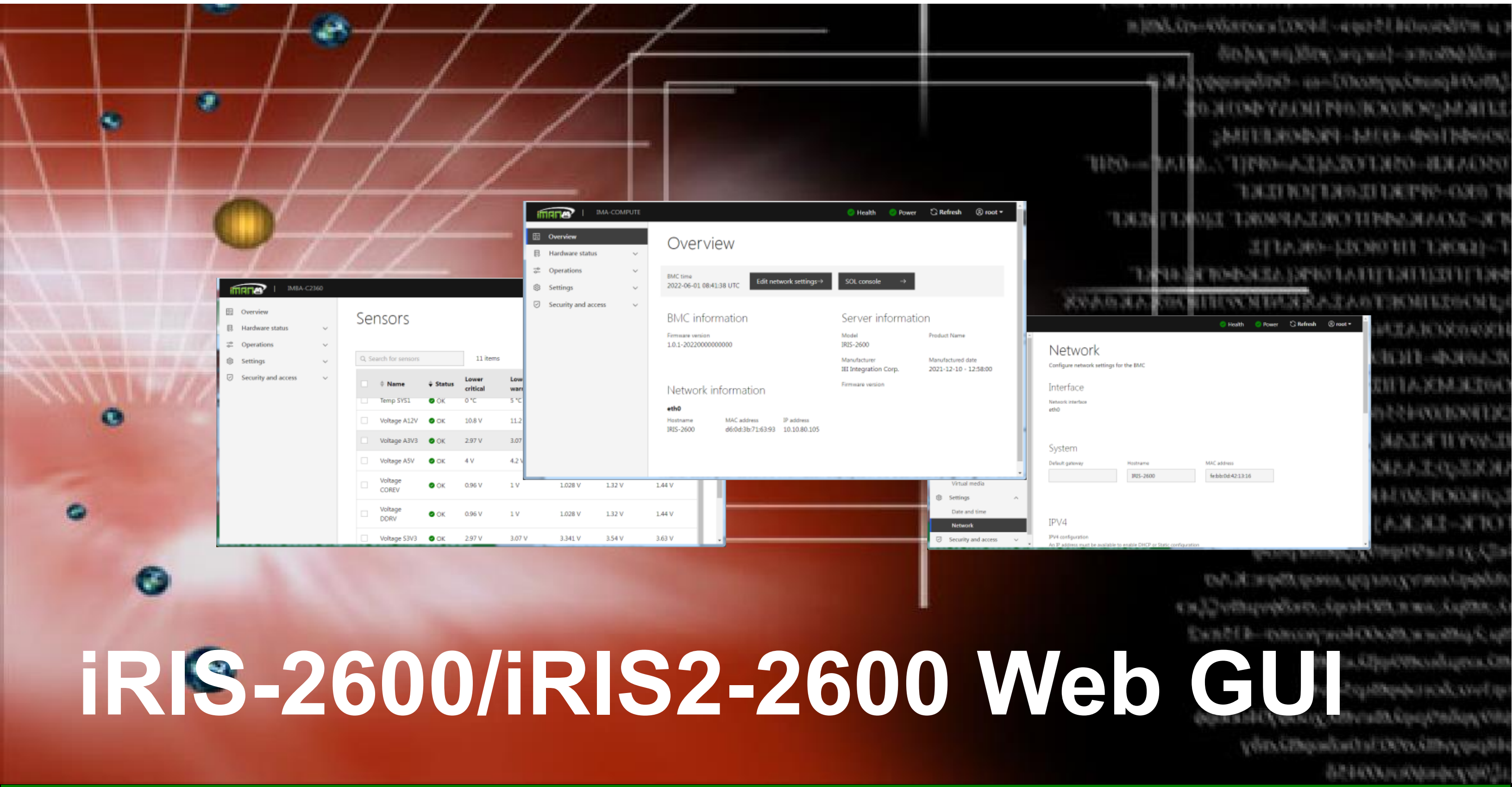
IEI Integration Corp.



iRIS-2600/iRIS2-2600 Web GUI

IEI iMAN V2 Web-based Graphics User Interface (GUI)

User Manual

Rev. 1.02 – September 13, 2023

RoHS Lead Free

Revision

Date	Version	Changes
September 13, 2023	1.02	Updated screenshots to the latest version Updated Section 1.1
July 11, 2023	1.01	Added pinouts of iRIS2 connector and DP connector in Section 1.1
September 1, 2022	1.00	Initial release

Copyright

COPYRIGHT NOTICE

TRADEMARKS

Table of Contents

List of Figures

Chapter

1

Introduction

1.1 iRIS-2600/iRIS2-2600 Overview

The iRIS-2600/iRIS2-2600 series module supports Intelligent Platform Management Interface (IPMI) that helps lower the overall costs of server management by enabling users to maximize IT resources, save time and manage multiple systems. The new IPMI 2.0 is designed to extend customers' IT capabilities and further improve remote management by introducing enhanced functions, including:

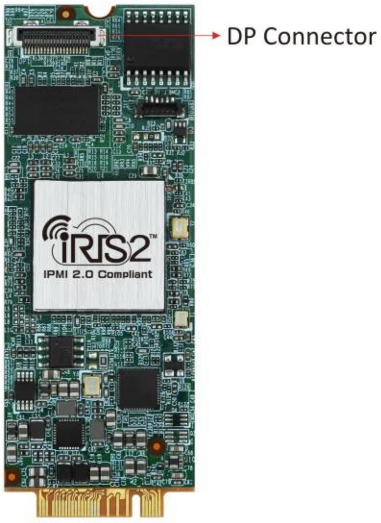
- New authentication and encryption algorithms enhance security for remote management access
- Serial over LAN supports remote interaction with serial-based applications, BIOS, and operating system
- SMBus system interface provides low-pin count connection for low-cost management controllers
- Firmware Firewall supports partitioning and protection of management between blades in modular system implementations

1.1.1 Model Variations

The model variations of the iRIS-2600/iRIS2-2600 series are listed below.

Model Name	Slot Interface	KVM Support	Display Output
iRIS-2600	IEI iRIS slot (204-pin) (compatible with iRIS-2400 slot)	Yes	VGA signal out
iRIS-2620	IEI iRIS slot (204-pin) (compatible with iRIS-2400 slot)	No	No
iRIS2-2600	IEI iRIS2 slot (75-pin)	Yes	Onboard DisplayPort connector
iRIS2-2620	IEI iRIS2 slot (75-pin)	No	No

iRIS-2600

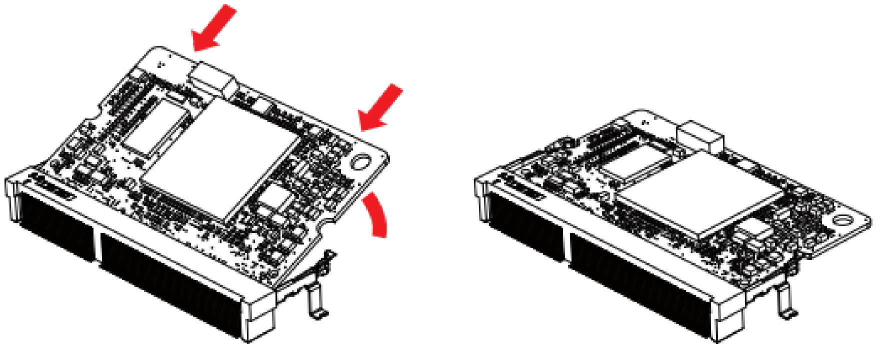


iRIS2-2600

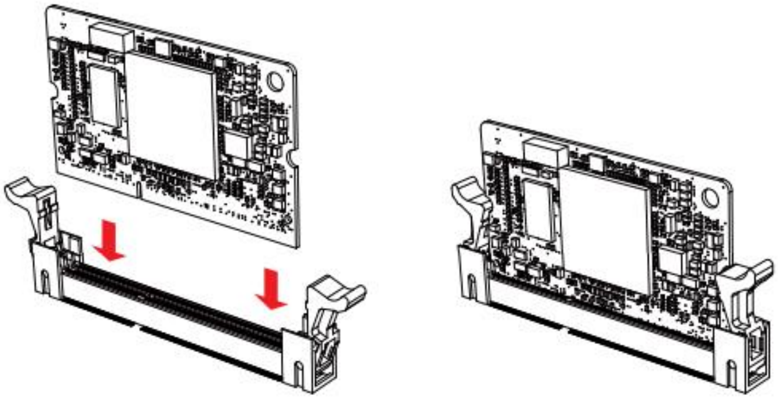
1.1.2 Hardware Installation

The iRIS module can be installed into the iRIS module slot on IEI motherboard that supports IPMI 2.0. The iRIS-2600 is for the IEI iRIS slot, and the iRIS2-2600 module is for the IEI iRIS2 slot. Please refer to the motherboard manual for the hardware installation instruction.

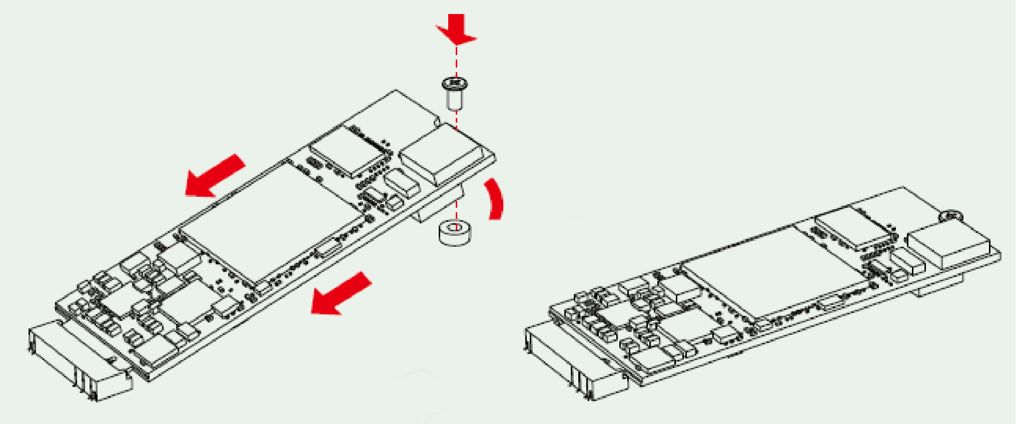
iRIS-2600 Installation (90° Slot)



iRIS-2600 Installation (180° Slot)



iRIS2-2600 Installation



1.1.3 IEI iRIS2 Connector

The IEI iRIS2 connector pinouts are listed below.

Description	Pin No.	Pin No.	Description
3.3 V	74	75	NC
3.3 V	72	73	GND
3.3 V	70	71	NC
BMC_Tx (Uart)	68	69	GND
ESPI_LPC	66	67	BMC_Rx (Uart)
LPC_AD3/ESPID3	64	65	LPC_SERIRQ/ESPIALT_N
LPC_AD2/ESPID2	62	63	LPC_CLK/ESPICK

LPC_AD1/ESPID1	60	61	LPC_FRAME_N/ESPICS_N
LPC_AD0/ESPID0	58	59	LPC_RST_N/ESPIRST_N
SPI_MISO	56	57	GND
PCIE_WAKE#	54	55	DIF_PCIE_EP_CLK_P
CLKREQ#	52	53	DIF_PCIE_EP_CLK_N
PCIE_RST#	50	51	GND
SPI_MOSI	48	49	DIF_PCIE_EP_RX_P
SPI_CLK	46	47	DIF_PCIE_EP_RX_N
SPI_CS0	44	45	GND
SMBUSDAT1_EC(1.8V)	42	43	DIF_PCIE_EP_TX_P
SMBUSCLK1_EC(1.8V)	40	41	DIF_PCIE_EP_TX_N
NC	38	39	GND
GBE_LED_100M	36	37	NC
MDI0_P	34	35	NC
MDI0_N	32	33	GND
MDI1_P	30	31	NC
MDI1_N	28	29	NC
MDI2_P	26	27	GND
MDI2_N	24	25	NC
MDI3_P	22	23	NC
MDI3_N	20	21	GND
	18	19	
	16	17	
	14	15	
	12	13	
	10	11	GND
GBE_LED_LINK_ACT#	8	9	USB2.0-
GBE_LED_1G	6	7	USB2.0+
3.3 V	4	5	GND
3.3 V	2	3	GND
		1	GND

1.1.4 DP Connector (iRIS2-2600 Only)

The DP connector pinouts are listed below.

Pin No.	Description
1	CONFIG 1
2	CONFIG 2
3	GND
4	GND
5	GND
6	NC
7	NC
8	NC
9	VCC
10	VCC
11	DP_HPD-R
12	DIF_DP_AUX-N-C
13	DIF_DP_AUX-P-C
14	GND
15	DIF_DP_CONN_TX1-N
16	DIF_DP_CONN_TX1-P
17	GND
18	DIF_DP_CONN_TX0-N
19	DIF_DP_CONN_TX1-N
20	GND

1.1.5 DP Cable Connector (iRIS2-2600 Only)

The DP connector pinouts of the DP cable are listed below.

IMP.	Signal Data	P1		P2
	CONFIG 1	1		13
	CONFIG 2	2		14
	GND	3		11
	GND	4		16
	GND	5		16
	NC	6		
	NC	7		
	NC	8		
	VCC	9		20
	VCC	10		20
	DP_HPD-R	11		18
100Ω +/-15%	DIF_DP_AUX-N-C	12		17
	DIF_DP_AUX-P-C	13		15
	GND	14		8
100Ω +/-15%	DIF_DP_CONN_TX1-N	15		6
	DIF_DP_CONN_TX1-P	16		4
	GND	17		5
100Ω +/-15%	DIF_DP_CONN_TX0-N	18		3
	DIF_DP_CONN_TX1-N	19		1
	GND	20		2

1.2 IEI iMAN V2 GUI Overview

The IEI iMAN V2 Graphics User Interface (GUI) is designed to manage a client system from a remote console using standard Internet browsers.

1.2.1 System Requirements

Minimum software requirements for using IEI iMAN V2 GUI are listed below.

1.2.1.1 Supported Browsers

- Internet Explorer 11 and above
- Google Chrome 103.0 and above

1.2.1.2 Supported OS

- Windows XP
- Windows Vista
- Windows 7 32-bt/64-bit
- Windows 10 32-bt/64-bit
- Windows 11 32-bt/64-bit
- w2k3 - 32 bit
- w2k3 - 64 bit
- Ubuntu 18.10 -32
- Ubuntu 20.10 -32
- Ubuntu 21.10 -32
- Ubuntu 20.10 -64
- Ubuntu 21.10 -64
- Ubuntu 22.10 -64
- MAC -32
- MAC-64

1.2.2 Access the IEI iMAN V2 Web GUI

To initial access to the IEI iMAN V2 Web GUI, follow the steps below.

Step 1: Obtain the IP address of the managed system. It is recommended to use BIOS or the IPMI Tool to obtain the IP address of the managed system. To use IPMI Tool to obtain IP address, follow the steps below:

a. Copy the **ipmitool.exe or ipmitool.efi** file to a bootable USB flash drive.

b. Insert the USB flash drive to the managed system

c. The managed system boots from the USB flash drive

d. Enter the following command: **ipmitool.efi lan print**

```
          ipmitool.efi lan print

IP Address Source          : Static Address
IP Address                 : 192.168.1.224
Subnet Mask               : 255.255.254.0
MAC Address               : fe:bb:0d:42:13:16
```

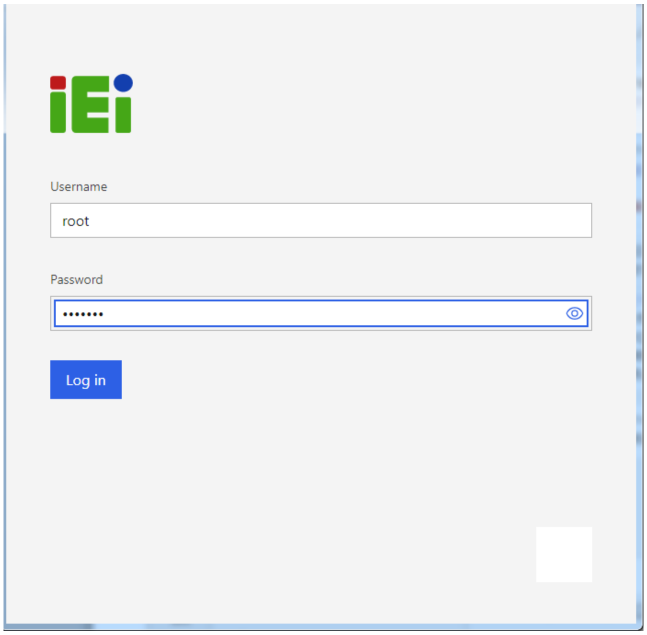
To use BIOS to obtain the IP address, check BMC LAN Network information in BIOS.

Step 2: On the remote management console, open a web browser. Enter the managed system IP address in the web browser (**Figure 1-1**).

https://192.168.1.224

Figure 1-1: IEI iMAN V2 Web Address Sample

Step 3: The login page appears in the web browser (**Figure 1-2**).


Username

root

Password

•••••••

Figure 1-2: IEI iMAN V2 Web GUI Login Page

Step 4: Enter the user name and password to login the system. The default login information is

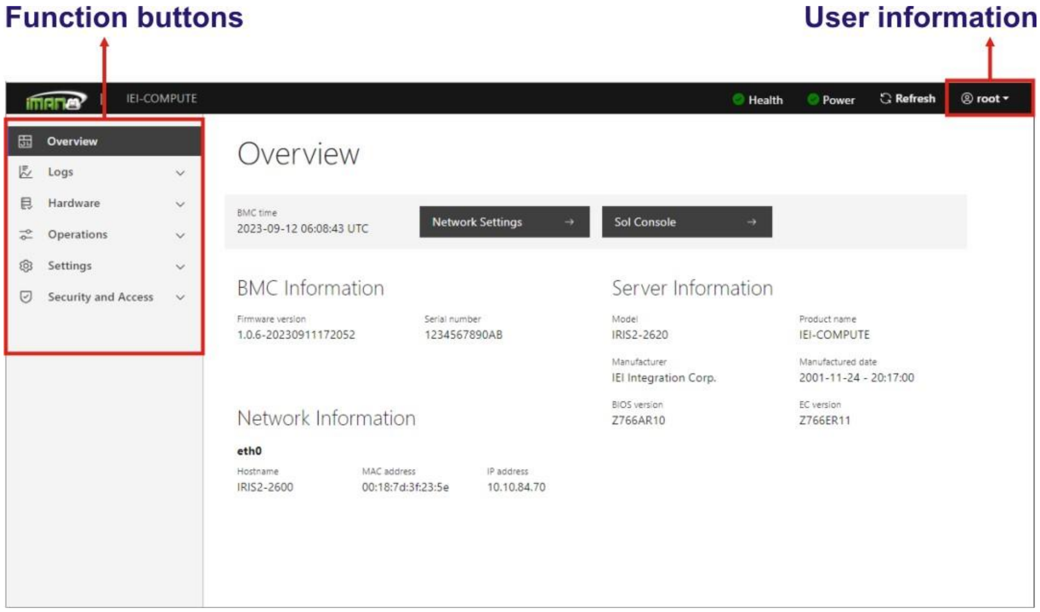
Username: root

Password: IRIS + last 6 digit number of MAC (for example: IRIS421316)

Step 5: Press the **Log in** button to login the system. It is advised to change the password once login.

1.2.3 IEI iMAN V2 GUI Interface

Figure 1-3 shows a screenshot of the IEI iMAN V2 GUI after login. The menu bars contain general function buttons, quick buttons and logged-in user information.



Overview

BMC time
2023-09-12 06:08:43 UTC

BMC Information

Firmware version
1.0.6-20230911172052

Serial number
1234567890AB

Server Information

Model
IRIS2-2620

Product name
IEI-COMPUTE

Manufacturer
IEI Integration Corp.

Manufactured date
2001-11-24 - 20:17:00

BIOS version
Z766AR10

EC version
Z766ER11

Network Information

eth0

Hostname
IRIS2-2600

MAC address
00:18:7d:3f:23:5e

IP address
10.10.84.70

Figure 1-3: IEI iMAN V2 GUI Interface

The logged-in user information shows the logged-in user and his/her privilege. There are four kinds of privileges:

- **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.
- **Read only:** Update password for current user and Login in to the service and read resources.
- **No Access:** Login access denied.

Each general function of IEI iMAN V2 GUI is described in detail in the following chapters.

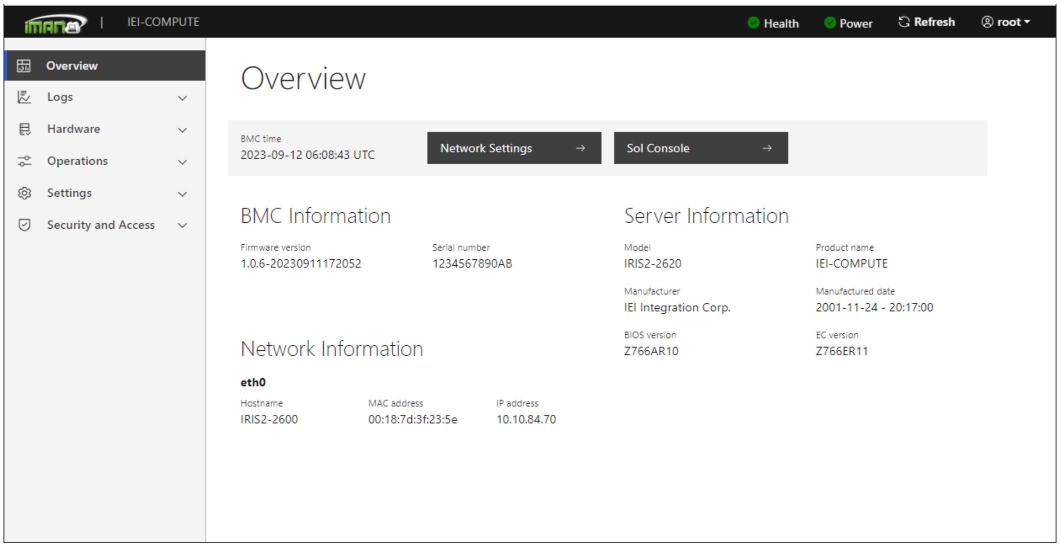
Chapter

2

Overview Page

2.1 Overview Page

The Overview page gives the overall information about the status of a device. To open the Overview page, click **Overview** from the side menu bar.



Overview

BMC time
2023-09-12 06:08:43 UTC

BMC Information

Firmware version: 1.0.6-20230911172052
Serial number: 1234567890AB

Network Information

eth0
Hostname: IRIS2-2600
MAC address: 00:18:7d:3f:23:5e
IP address: 10.10.84.70

Server Information

Model: IRIS2-2620
Product name: IEI-COMPUTE
Manufacturer: IEI Integration Corp.
Manufactured date: 2001-11-24 - 20:17:00
BIOS version: Z766AR10
EC version: Z766ER11

Figure 2-1: Overview Page

A brief description about the information displayed in the Overview page is given below.

- **BMC Information**:
  - ○ Firmware Version: The version of the firmware
- **Server Information**:

  The Server Information displays the following information:
  - ○ Model: The name of the model
  - ○ Product Name: The name of the product
  - ○ Manufacturer: The name of the manufacturer
  - ○ Manufactured Date: The date of manufacturing
  - ○ Firmware Version: The version of the system firmware
- **Network Information**

  The Network Information of the device with the following fields is shown here. To edit the network Information, click the **Edit network settings** button.
  - ○ IP Address: Read only field showing the IP address of the device.
  - ○ MAC Address: Read only field showing the MAC address of the device.

Chapter

3

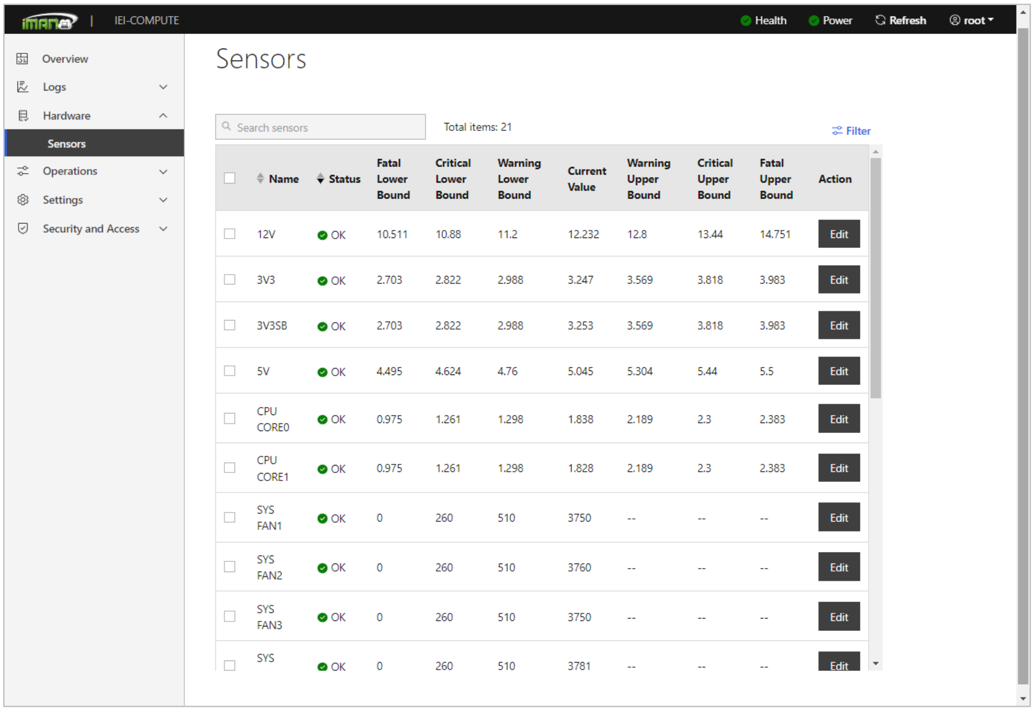
Hardware Status

3.1 Overview

The Hardware Status page contains one subpage – Sensors, which is described in detail in the following section.

3.2 Sensor

The Sensor page displays all the sensor related information (**Figure 3-1)**. To open the Sensor page, click **Hardware status → Sensor** from the side menu. A list of sensors with sensor name, status critical and current value is displayed.



Sensors

Total items: 21

□	Name	Status	Fatal Lower Bound	Critical Lower Bound	Warning Lower Bound	Current Value	Warning Upper Bound	Critical Upper Bound	Fatal Upper Bound	Action
□	12V	OK	10.511	10.88	11.2	12.232	12.8	13.44	14.751	Edit
□	3V3	OK	2.703	2.822	2.988	3.247	3.569	3.818	3.983	Edit
□	3V3SB	OK	2.703	2.822	2.988	3.253	3.569	3.818	3.983	Edit
□	5V	OK	4.495	4.624	4.76	5.045	5.304	5.44	5.5	Edit
□	CPU CORE0	OK	0.975	1.261	1.298	1.838	2.189	2.3	2.383	Edit
□	CPU CORE1	OK	0.975	1.261	1.298	1.828	2.189	2.3	2.383	Edit
□	SYS FAN1	OK	0	260	510	3750	--	--	--	Edit
□	SYS FAN2	OK	0	260	510	3760	--	--	--	Edit
□	SYS FAN3	OK	0	260	510	3750	--	--	--	Edit
□	SYS	OK	0	260	510	3781	--	--	--	Edit

Figure 3-1: Sensor Page

Chapter

5

Operations

4.1 Overview

The Remote Control consists of the following.

- Factory reset
- KVM
- Firmware update
- Reboot BMC
- SOL console
- Server power operations
- Virtual media

A detailed description of each submenu is given below.

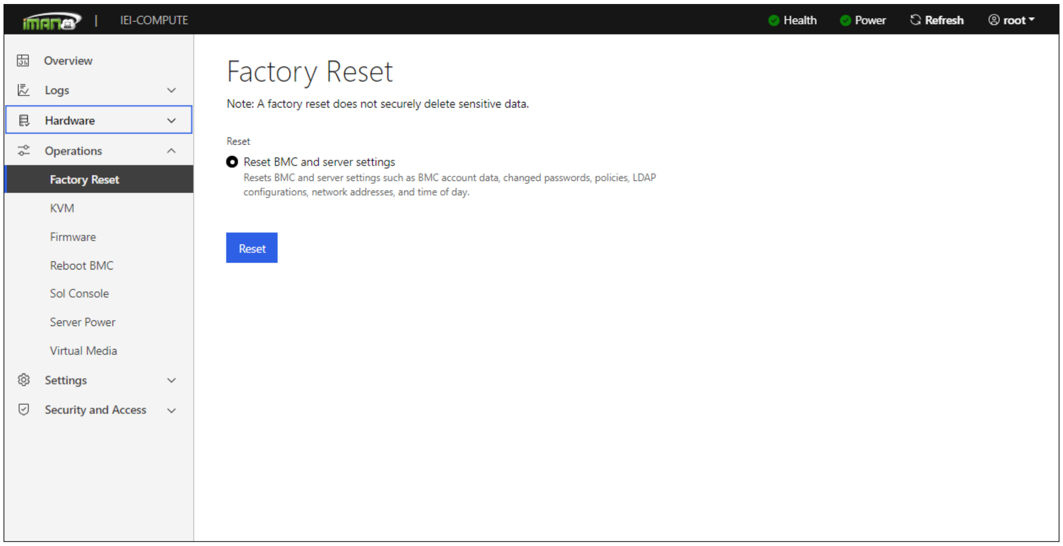
4.2 Factory Reset

The Factory Reset page is used to restore the default configuration of the device. This section lists the configuration items that will be preserved during restore default configuration.

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.

To open the Factory Reset page, click **Operations → Factory Reset** from the side menu bar.



Factory Reset

Note: A factory reset does not securely delete sensitive data.

Reset

● Reset BMC and server settings

Resets BMC and server settings such as BMC account data, changed passwords, policies, LDAP configurations, network addresses, and time of day.

Reset

Figure 4-1: Factory Page

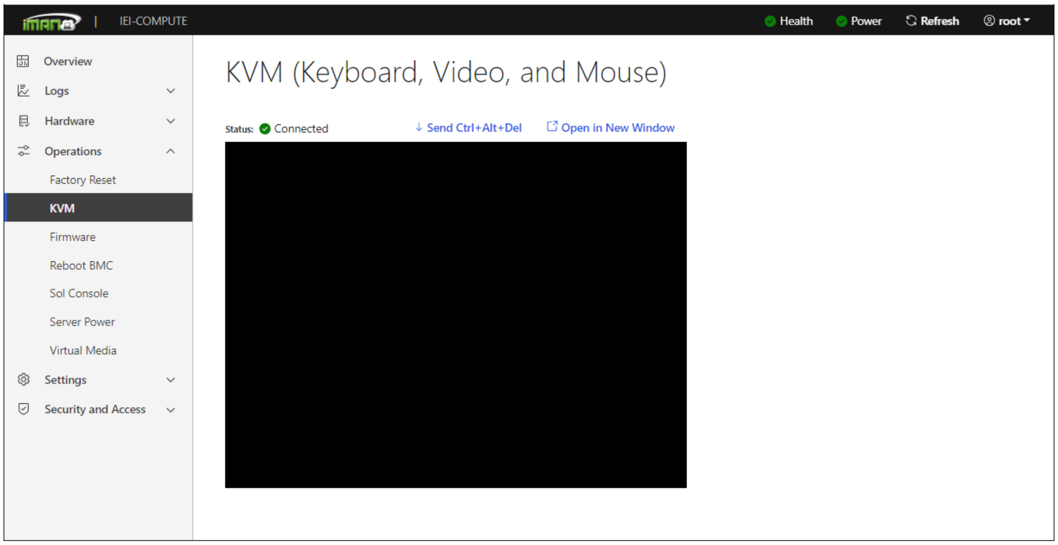
To restore default configuration of the device, click the **Reset** button.

4.3 KVM

NOTE:

The KVM function is only supported by the iRIS-2600 and iRIS2-2600 modules, which contain AST2600 BMC.

The KVM page is used to configure virtual media configuration settings for the next redirection session. To open the KVM page, click **Operations → KVM** from the side menu bar.



KVM (Keyboard, Video, and Mouse)

Status: Connected

Figure 4-2: KVM Page

The KVM page contains the following two function buttons.

- **Alt+Ctrl+Del**:
  This menu item can be used to act as if the user pressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the server that are redirecting.
- **Open in new tab**:
  This menu item can be used to act open new KVM web tab.

4.4 Firmware Update

The Firmware Update page allows the user to update BMC image and BIOS image files. To load the Firmware page, click **Operations→ Firmware** from the side menu bar.

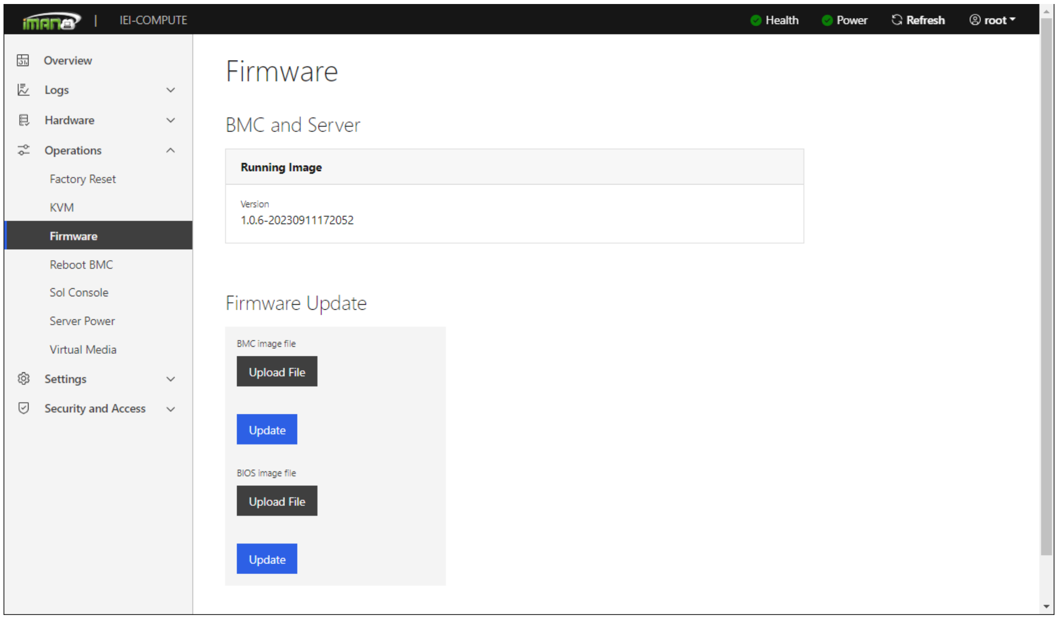
WARNING:

Please note that after firmware update, other web pages and services will not work. All open widgets will be closed automatically. If upgrade process is cancelled 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 iRIS module must be reset. This means that the user must close the Internet browser and log back onto the iRIS module before the user can perform any other types of operations.



Firmware

BMC and Server

Running Image

Version
1.0.6-20230911172052

Firmware Update

BMC image file

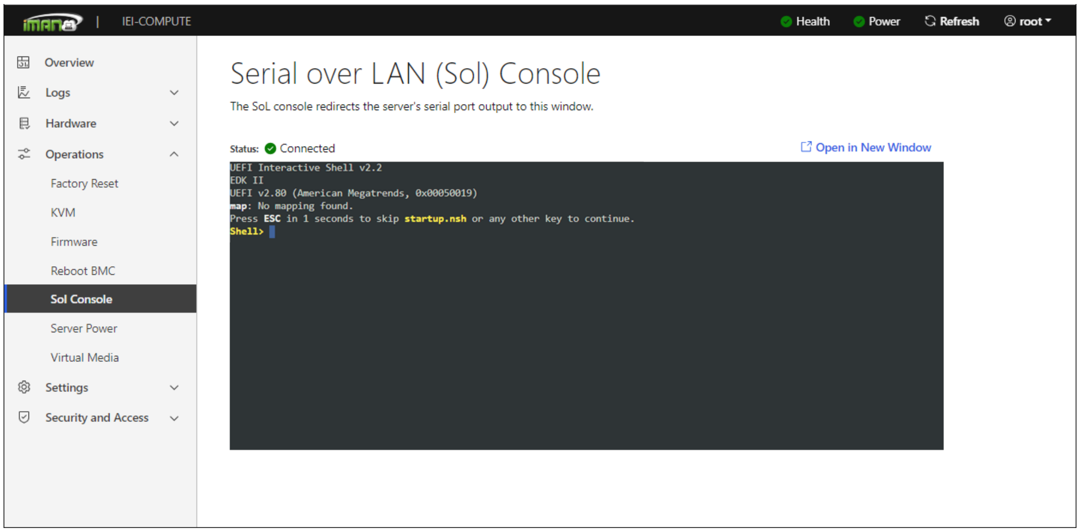
BIOS image file

Figure 4-3: Firmware Page

To update BMC/BIOS image file, click **Upload File** button to select the image file and then click **Update** button to update it.

4.5 SOL

The SOL page allows the user to launch the SOL. The SOL is used to view the host screen using the SOL Redirection. To open SOL page, click **Operations → Sol Console** from the side menu bar.



Serial over LAN (Sol) Console

The SoL console redirects the server's serial port output to this window.

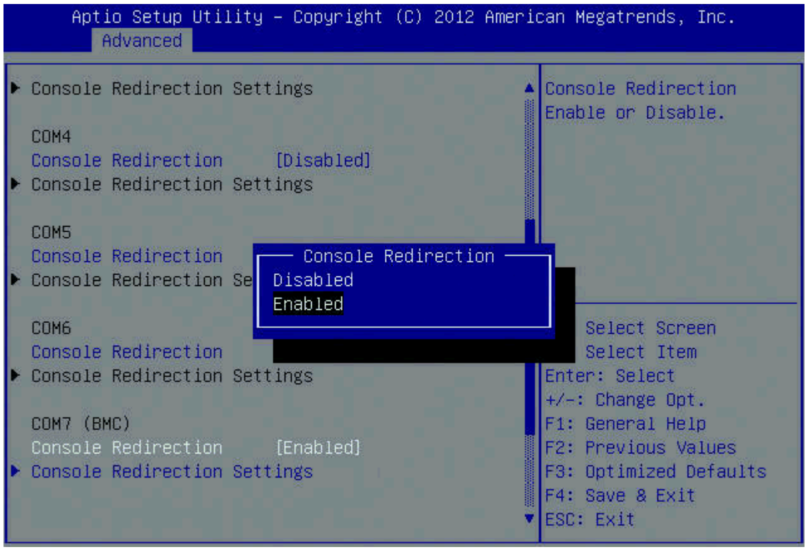
Status: Connected

```
UEFI Interactive Shell v2.2
EDK II
UEFI v2.80 (American Megatrends, 0x00050019)
map: No mapping found.
Press ESC in 1 seconds to skip startup.nsh or any other key to continue.
Shell>
```

Figure 4-4: SOL Page

To launch SOL, follow the steps below.

Step 1: Go to **Advanced → Serial Port Console Redirection** BIOS menu of the managed system. Enable BMC console redirection as shown in **Figure 4-5**.

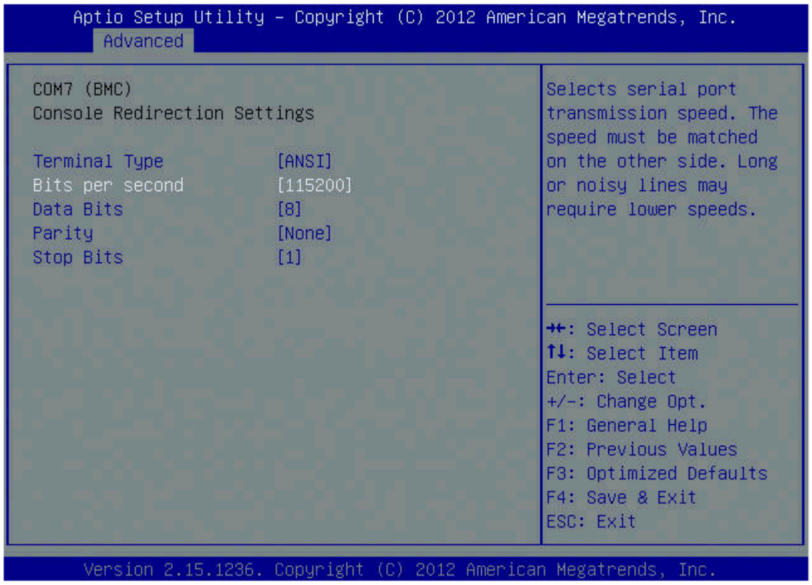


```
Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
       Advanced

▶ Console Redirection Settings                   Console Redirection
                                                 Enable or Disable.
  COM4
  Console Redirection      [Disabled]
▶ Console Redirection Settings

  COM5
  Console Redirection  ┌─ Console Redirection ─┐
▶ Console Redirection Se│ Disabled              │
                        │ Enabled               │
  COM6                  └───────────────────────┘   Select Screen
  Console Redirection                               Select Item
▶ Console Redirection Settings                   Enter: Select
                                                 +/-: Change Opt.
  COM7 (BMC)                                     F1: General Help
  Console Redirection      [Enabled]             F2: Previous Values
▶ Console Redirection Settings                   F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit
```

Figure 4-5: BMC Console Redirection BIOS Option

Step 2: Enter the BMC Console Redirection Settings BIOS menu (**Figure 4-6**).

Configure the BIOS options if necessary.

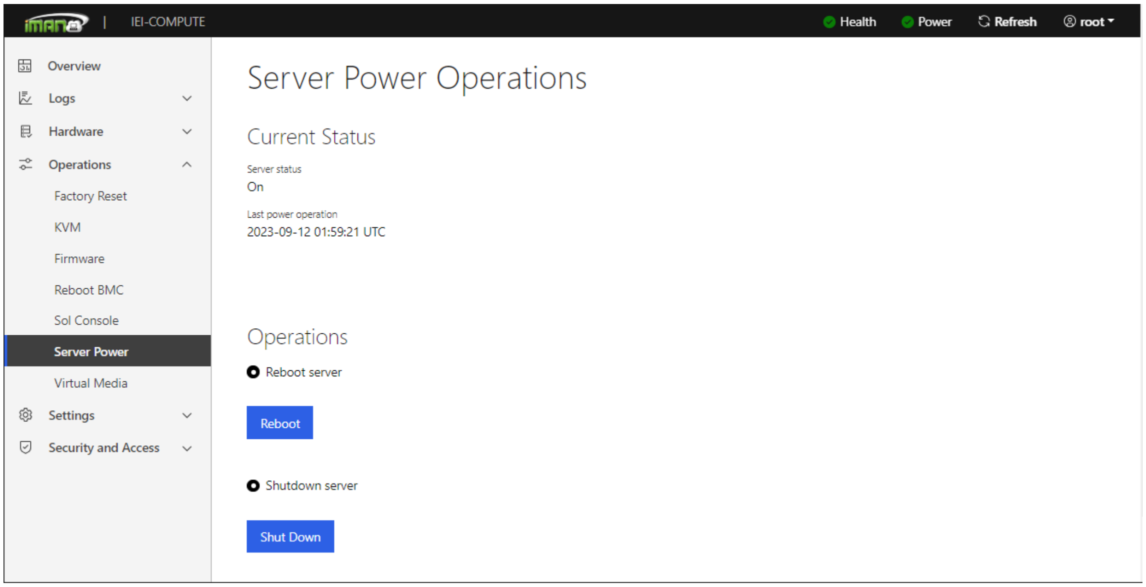


```
Aptio Setup Utility – Copyright (C) 2012 American Megatrends, Inc.
       Advanced

  COM7 (BMC)                                     Selects serial port
  Console Redirection Settings                   transmission speed. The
                                                 speed must be matched
  Terminal Type            [ANSI]                on the other side. Long
  Bits per second          [115200]              or noisy lines may
  Data Bits                [8]                   require lower speeds.
  Parity                   [None]
  Stop Bits                [1]

                                                 →←: Select Screen
                                                 ↑↓: Select Item
                                                 Enter: Select
                                                 +/-: Change Opt.
                                                 F1: General Help
                                                 F2: Previous Values
                                                 F3: Optimized Defaults
                                                 F4: Save & Exit
                                                 ESC: Exit

       Version 2.15.1236. Copyright (C) 2012 American Megatrends, Inc.
```

Figure 4-6: BMC Console Redirection Settings BIOS Menu

4.6 Server Power Operations

The Server Power Operations page allows the user to view and control the power of the server. To open the Server Power Operations page, click **Operations → Server Power** from the side menu bar.



Server Power Operations

Current Status

Server status
On

Last power operation
2023-09-12 01:59:21 UTC

Operations

● Reboot server

● Shutdown server

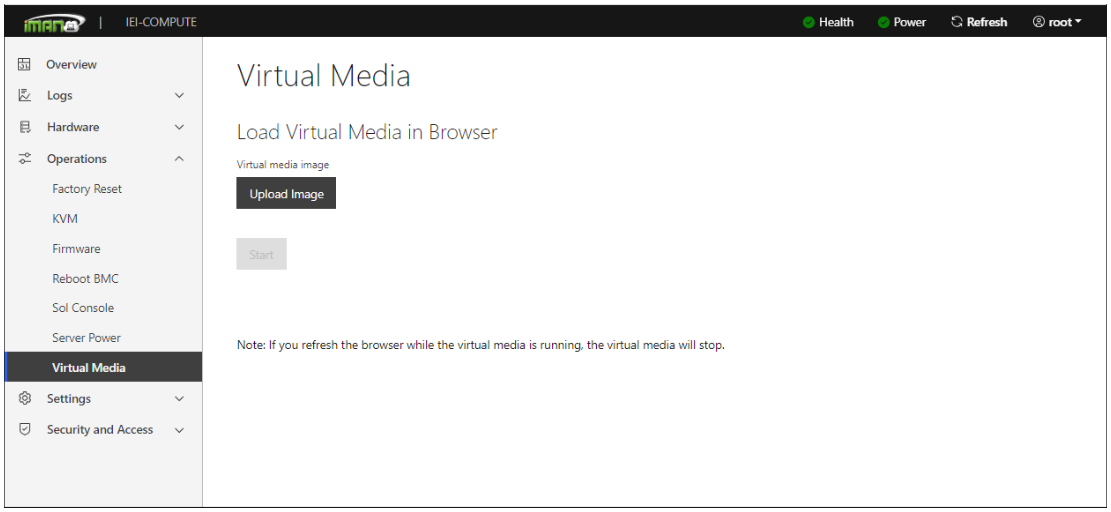
Figure 4-7: Power Control and Status Page

The various options of Server Power Operations are given below.

- **Reboot Server**:
  This option will reboot the system without powering off (warm boot).
  - **Orderly**: initiate operating system shutdown prior to the server reboot.
  - **Immediate**: immediately reboot the server without operating system shutdown.
- **Shutdown Server**:
  This option will shutdown the system.
  - **Orderly**: initiate operating system shutdown prior to the server shutdown.
  - **Immediate**: immediately shutdown the server without operating system shutdown.

4.7 Virtual Media

The Virtual Media screen can be accessed by clicking **Operations → Virtual Media** button. The user can enter the Virtual media for media redirection.



Virtual Media

Load Virtual Media in Browser

Virtual media image

Note: If you refresh the browser while the virtual media is running, the virtual media will stop.

Figure 4-8: Virtual Media Page

To add, remove or modify images, follow the steps below.

Step 1: To add an image, select a free Linux/Windows OS file, and click **Upload Image** to link to the virtual media device.

Step 2: Click **Start** to load the virtual media service.

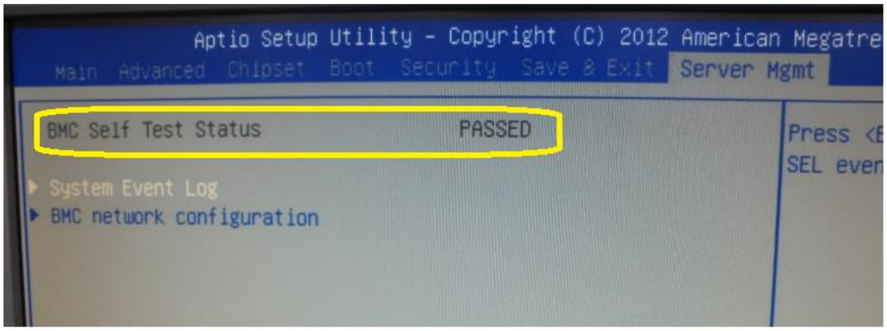
4.8 Checking BMC Test Status in Remote PC

This section describes how to check BMC test pass/fail status of a remote PC. This instruction can be applied to a remote PC where the iRIS module is installed on the IEI board.

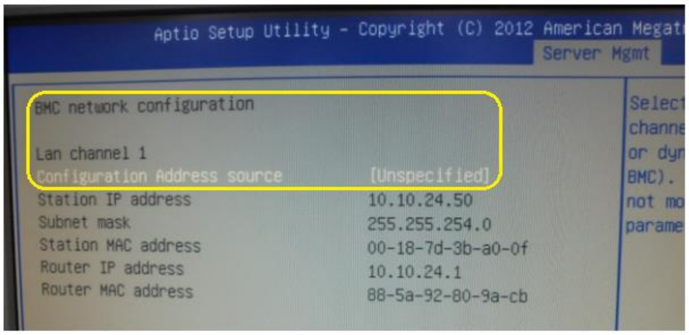
Step 1: Ensure the iRIS module is installed correctly in the iRIS module slot of the board.

Step 2: Ensure the LAN port supporting iRIS is connected with active Ethernet.

Step 3: Verify the BMC test has been passed under BIOS of IEI motherboard. It will take some minutes to recognize at the very first time of use.



```
BMC Self Test Status                    PASSED

▶ System Event Log
▶ BMC network configuration
```



```
BMC network configuration

Lan channel 1
Configuration Address source            [Unspecified]
Station IP address                      10.10.24.50
Subnet mask                             255.255.254.0
Station MAC address                     00-18-7d-3b-a0-0f
Router IP address                       10.10.24.1
Router MAC address                      88-5a-92-80-9a-cb
```

Chapter

4

Settings

5.1 Overview

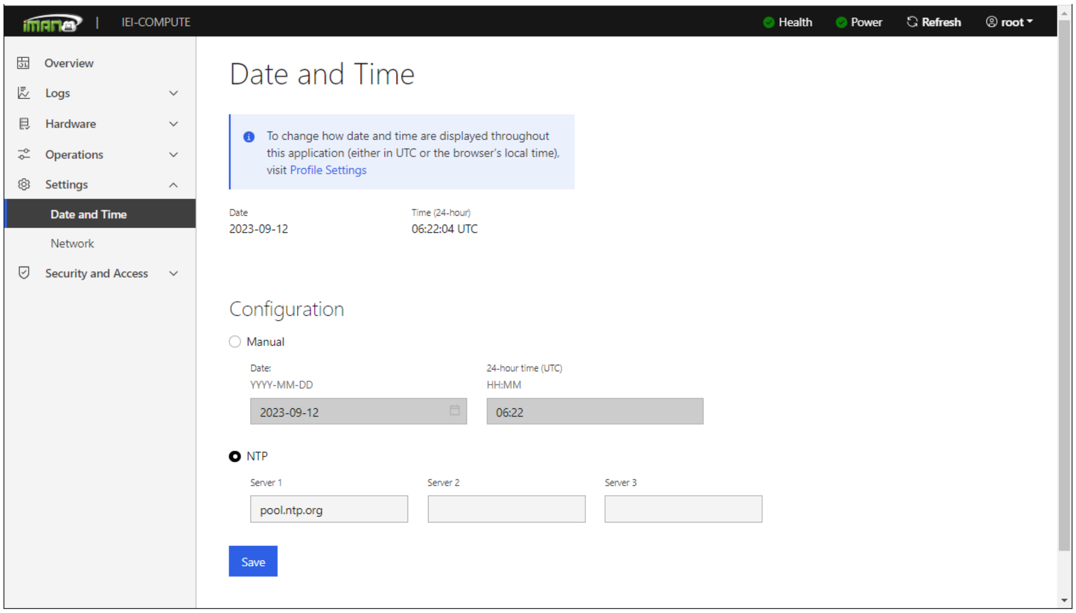
The Settings page consists of the following.

- Date and time
- Network

A detailed description of each submenu is given below.

5.2 Date and Time

The Date and Time page displays the device current date and time settings. It can be used to configure Date, Time or NTP server settings for the device. To open the Date and Time page, click **Settings → Date and Time** from the side menu bar.



Date and Time

To change how date and time are displayed throughout this application (either in UTC or the browser's local time), visit Profile Settings

Date
2023-09-12

Time (24-hour)
06:22:04 UTC

Configuration

○ Manual

Date:
YYYY-MM-DD
2023-09-12

24-hour time (UTC)
HH:MM
06:22

● NTP

Server 1
pool.ntp.org

Server 2

Server 3

Figure 5-1: Date and Time Page

The fields of Date and Time page are explained below.

- **Manual**
  - **Date**: To specify the current date of the device
  - **Time**: Specify the current Time for the device.

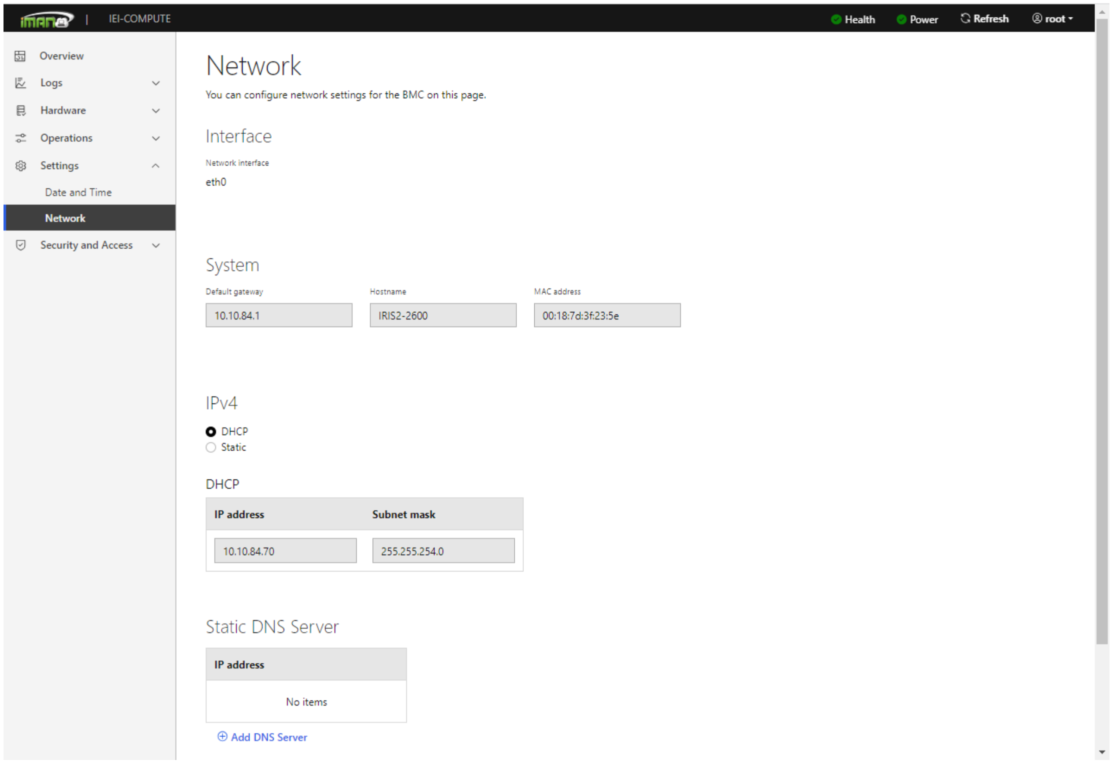
    Note: As Year 2038 Problem exists, Date and Time should be configured within the range.
- **NTP**:

  Specify the primary NTP Server for the device. The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of computer systems over packet-switched, variable-latency data networks. It is designed particularly to resist the effects of variable latency by using a jitter buffer.
  - **Server 1**: Specify the primary NTP Server for the device.
  - **Server 2**: Specify the secondary NTP Server for the device.
  - **Server 3**: Specify the third NTP Server for the device.
- **Save**:

  To save the settings.

5.3 Network

The Network page is used to configure the network settings for the available LAN channels. To open the Network page, click **Settings** → **Network** from the side menu bar.



Network

You can configure network settings for the BMC on this page.

Interface

Network interface: eth0

System

Default gateway: 10.10.84.1

Hostname: IRIS2-2600

MAC address: 00:18:7d:3f:23:5e

IPv4

● DHCP
○ Static

DHCP

IP address	Subnet mask
10.10.84.70	255.255.254.0

Static DNS Server

IP address
No items

Figure 5-2: Network Page

The fields of Network Settings page are explained below.

- **Interface**:

  Lists the LAN interfaces.

- **System**:

  Lists the information of the device. Click the field to change the settings.

  - **Default gateway**: the default gateway of the device.
  - **Hostname**: the name of the device.
  - **MAC Address**: the MAC Address of the device.

- **IPv4**:

  Lists the IPv4 configuration settings.

  ○ **DHCP**: This option is to dynamically configure IPv4 address using DHCP (Dynamic Host Configuration Protocol).

- ○ **Static**: These fields are for specifying the static IPv4 address and Subnet Mask to be configured to the device.

  - IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".

  - Each Number ranges from 0 to 255.

  - First Number must not be 0.

- **Static DNS**:

  Specify the static DNS (Domain Name System) server address to be configured to the device.

  - IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx".

  - Each Number ranges from 0 to 255.

  - First Number must not be 0.

- **Save**:

  To save the entries.

Chapter

4

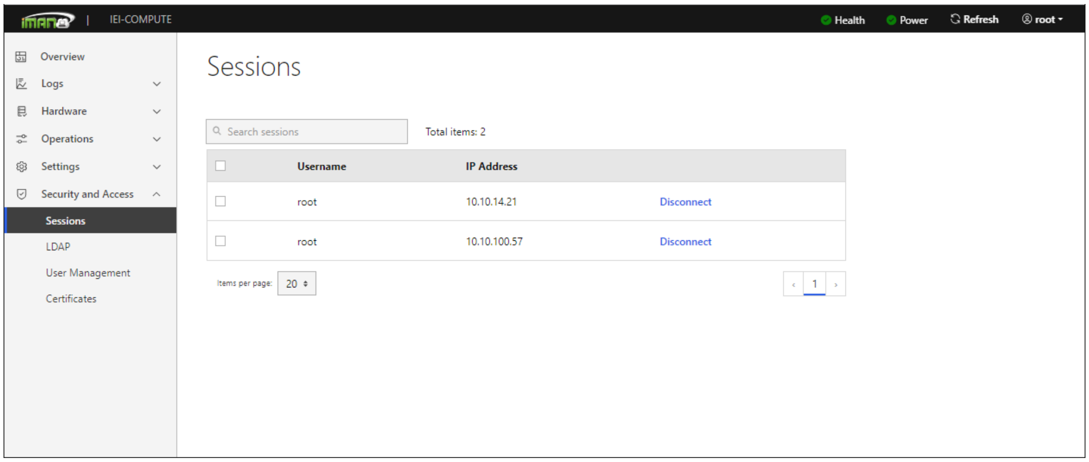
Security and Access

6.1 Overview

The Security and Access allows users to access various configuration settings. Each configuration setting is described in detail in the following sections.

6.2 Sessions

The Sessions page allows users to manage session server settings. To open Sessions page, click **Security and access → Sessions** from the side menu bar.



Total items: 2

□	Username	IP Address	
□	root	10.10.14.21	Disconnect
□	root	10.10.100.57	Disconnect

Items per page: 20

Figure 6-1: Sessions Page

The button on the Sessions page is explained below.

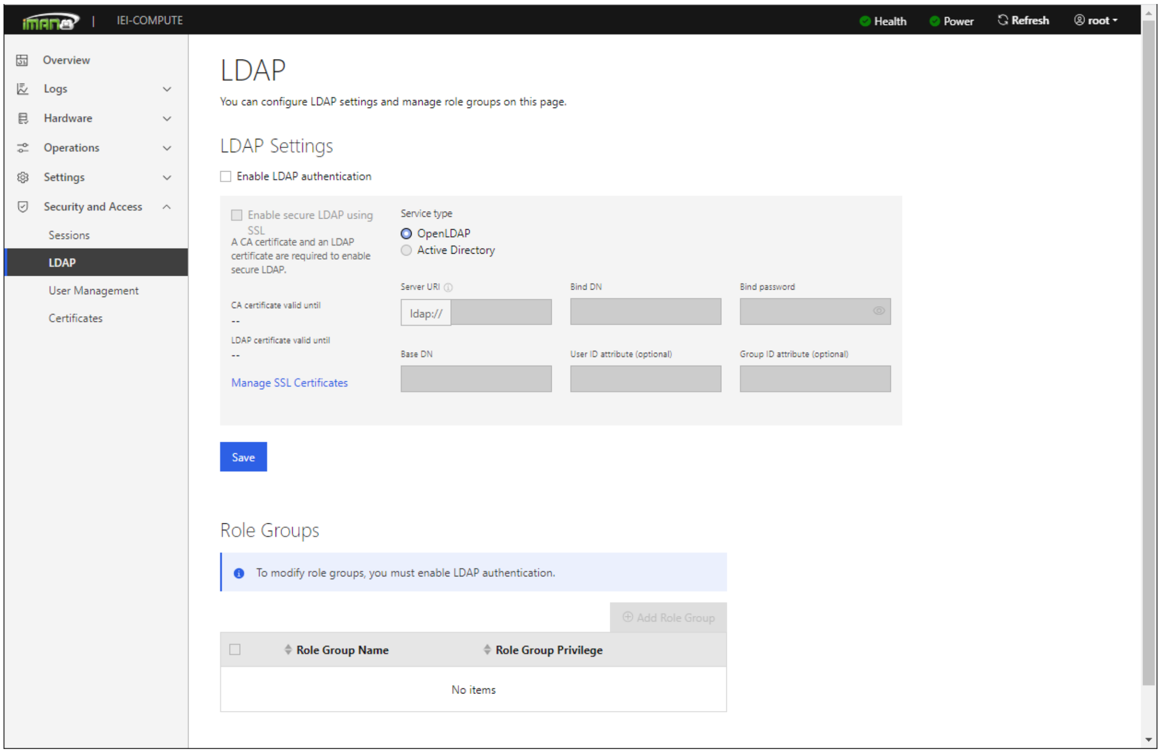
- **Disconnect**: use this button to disconnect the session.

6.3 LDAP

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 IEI iMAN V2 GUI, LDAP is an Internet protocol that the iRIS module can use to authenticate users. If there is an LDAP server configured on the network, the user can use it as an easy way to add, manage and authenticate the iRIS module users. This is done by passing login requests to the LDAP Server. This means that there is no need to define an additional authentication mechanism, when using the iRIS module. Since the existing LDAP Server keeps an authentication centralized, the user will always know who is accessing the network resources and can easily define the user or group-based policies to control access.

To open the LDAP setting page, click **Security and access → LDAP** from the side menu bar.



LDAP

You can configure LDAP settings and manage role groups on this page.

LDAP Settings

☐ Enable LDAP authentication

☐ Enable secure LDAP using SSL

A CA certificate and an LDAP certificate are required to enable secure LDAP.

CA certificate valid until
--

LDAP certificate valid until
--

Manage SSL Certificates

Service type
● OpenLDAP
○ Active Directory

Server URI: ldap://
Bind DN:
Bind password:
Base DN:
User ID attribute (optional):
Group ID attribute (optional):

Save

Role Groups

To modify role groups, you must enable LDAP authentication.

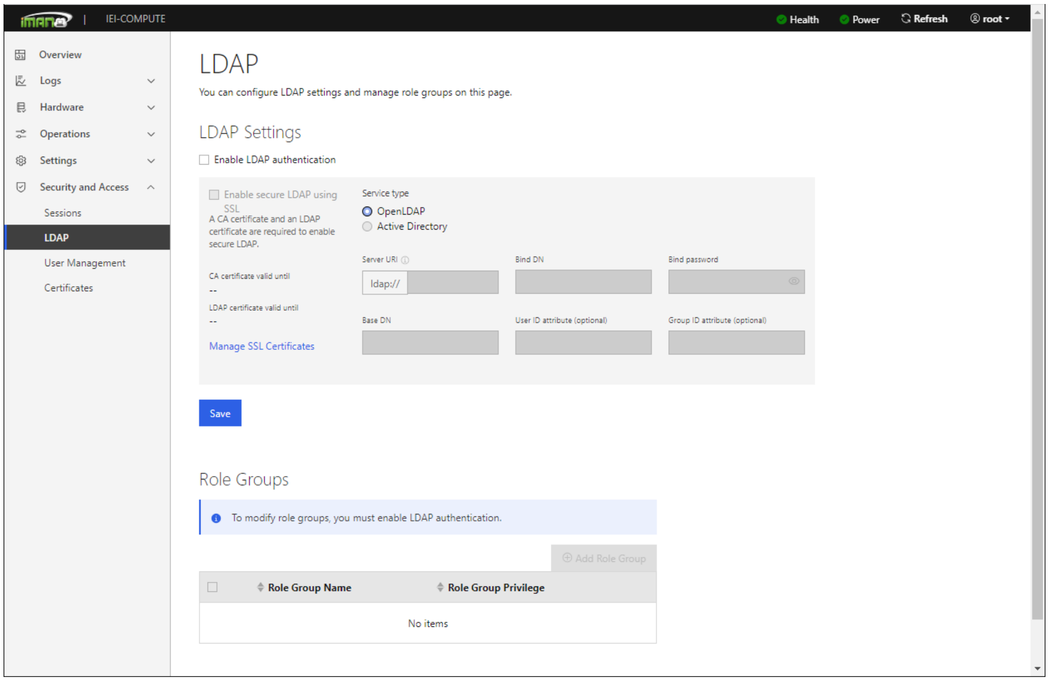
Add Role Group

☐	Role Group Name	Role Group Privilege
	No items	

Figure 6-2: LDAP Page

To input information in the LDAP page, follow the steps below:

Step 1: Click **LDAP** on the side menu bar to open the LDAP setting page.



LDAP

You can configure LDAP settings and manage role groups on this page.

LDAP Settings

☐ Enable LDAP authentication

☐ Enable secure LDAP using SSL

A CA certificate and an LDAP certificate are required to enable secure LDAP.

CA certificate valid until: --

LDAP certificate valid until: --

Manage SSL Certificates

Service type: ● OpenLDAP ○ Active Directory

Server URI: ldap://

Bind DN

Bind password

Base DN

User ID attribute (optional)

Group ID attribute (optional)

Role Groups

To modify role groups, you must enable LDAP authentication.

☐	Role Group Name	Role Group Privilege
No items		

Figure 6-3: LDAP Authentication

Step 2: Click to select **Enable** to enable the LDAP authentication settings.

NOTE: During login prompt, use username to login as an LDAP Group member

Step 3: Enter the server information. Click **Save settings** to save the entered settings.

NOTE:

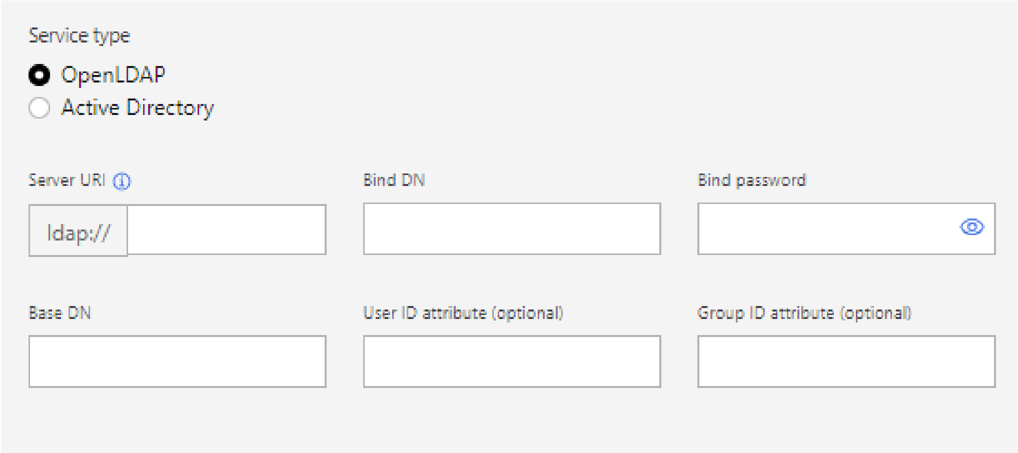
IP address of Active Directory server:

- At least one Domain Controller Server Address must be configured.
- IP Address made of four numbers separated by dots as in "xxx.xxx.xxx.xxx".
- Each number ranges from 0 to 255.
- First number must not be 0.

6.3.1 LDAP Settings

To enter the details in the LDAP page, follow the steps below.

Step 1: In the LDAP page, select **OpenLDAP**.



Service type

● OpenLDAP

○ Active Directory

Figure 6-4: OpenLDAP Settings page

Step 2: Follow the rules below to enter the IP address of LDAP server in the **Server URI** field.

- IP Address made of 4 numbers separated by dots as in 'xxx.xxx.xxx.xxx'.
- Each Number ranges from 0 to 255.
- First Number must not be 0.
- Supports IPv4 Address format and IPv6 Address format.

Step 3: Specify the **Bind DN**:

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

Step 4: Enter the Bind password in the **Bind Password** field.

- Password must be at least 1 character long.
- White space is not allowed.
- This field will not allow more than 48 characters.

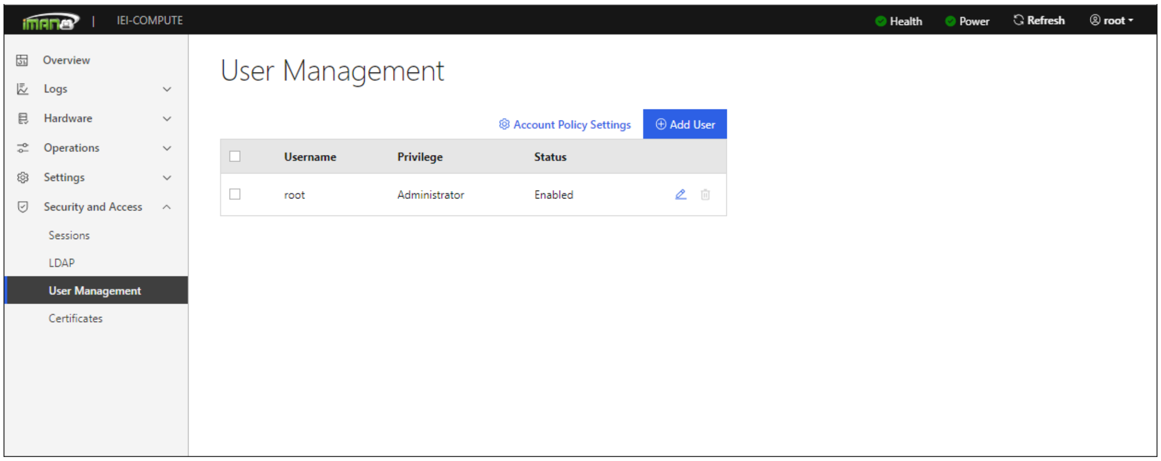
Step 5: Enter the **Base DN**. The Search base tells the LDAP server which part of the external directory tree to search. The search base may be something equivalent to the organization, group of external directory.

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

Step 6: Click **Save setting** to save the settings.

6.4 User Management

The User Management page allows users to view the current list of user slots for the server. You can add a new user and modify or delete the existing users. To open User Management page, click **Security and access → User Management** from the side menu bar.



User Management

☐	Username	Privilege	Status
☐	root	Administrator	Enabled

Figure 6-5: User Management Page

The fields of User Management Page are explained below.

- **User Name**:
  Displays the name of the user.

- **Privilege**:

  Displays the network access privilege of the user.
- **Status**:

  User status

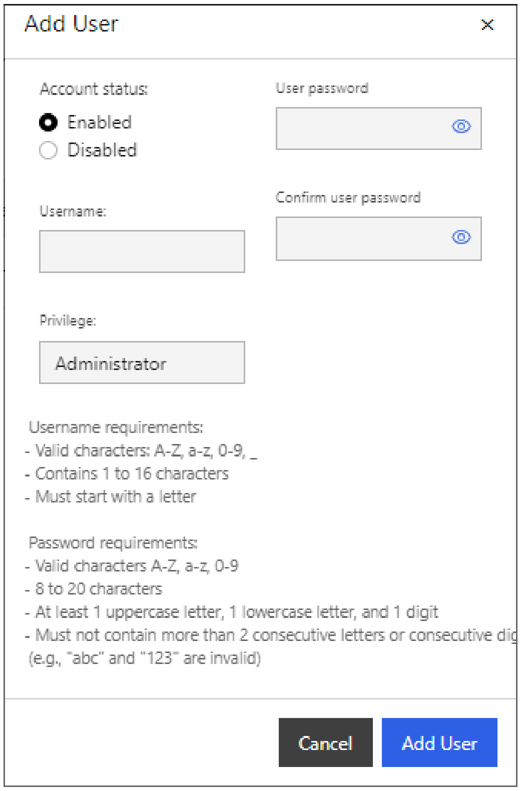
NOTE:

The Free slots are denoted by "~" in all columns for the slot.

6.4.1 Add User

To add a new user, follow the steps below.

Step 1: To add a new user, click the **Add User** button. The Add User screen appears (**Figure 6-6**).



Add User ×

Account status:

● Enabled

○ Disabled

User password

Confirm user password

Username:

Privilege:

Administrator

Username requirements:
- Valid characters: A-Z, a-z, 0-9, _
- Contains 1 to 16 characters
- Must start with a letter

Password requirements:
- Valid characters A-Z, a-z, 0-9
- 8 to 20 characters
- At least 1 uppercase letter, 1 lowercase letter, and 1 digit
- Must not contain more than 2 consecutive letters or consecutive dig
(e.g., "abc" and "123" are invalid)

Figure 6-6: Add User Page

Step 2: Follow the rules below to enter the name of the user in the **Username** field.

- Username is a string of 4 to 16 alpha-numeric characters.

- It must start with an alphabetical character.

- It is case-sensitive.

- Special characters ','(comma), '.'(period), ':'(colon), ';'(semicolon), ' '(space), '/'(slash), '\'(backslash), '('(left bracket) and ')'(right bracket) are not allowed.

Step 3: In the **User password** and **Confirm user password** fields, enter and confirm your new password. Password rules are:

- Password must be at between 8-20 characters

- Password must include uppercase and lowercase letters and numbers

Step 4: Select user privilege.

Step 5: Click **Add User** to save the new user and return to the users list. Click **Cancel** to cancel the modification and return to the users list.

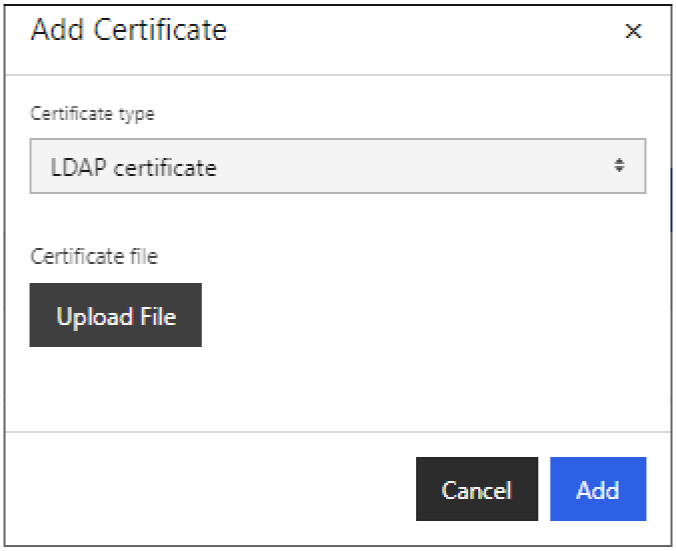
6.5 Certificates

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. The user can use the SSL Certificate page to configure SSL certificate into the BMC, then the device can be accessed in a secured mode.

To open SSL Certificate Configuration page, click **Security and access → Certificates** from the side menu bar. This page contains two functions:

- **Add Certificate** option is used to upload the certificate and private key file into the BMC.
- **Generate CSR** option is used to generate CSR for the SSL certificate based on configuration details.

6.5.1 Add new certificate



Add Certificate

Certificate type: LDAP certificate

Certificate file

Figure 6-7: Certificate – Add Certificate

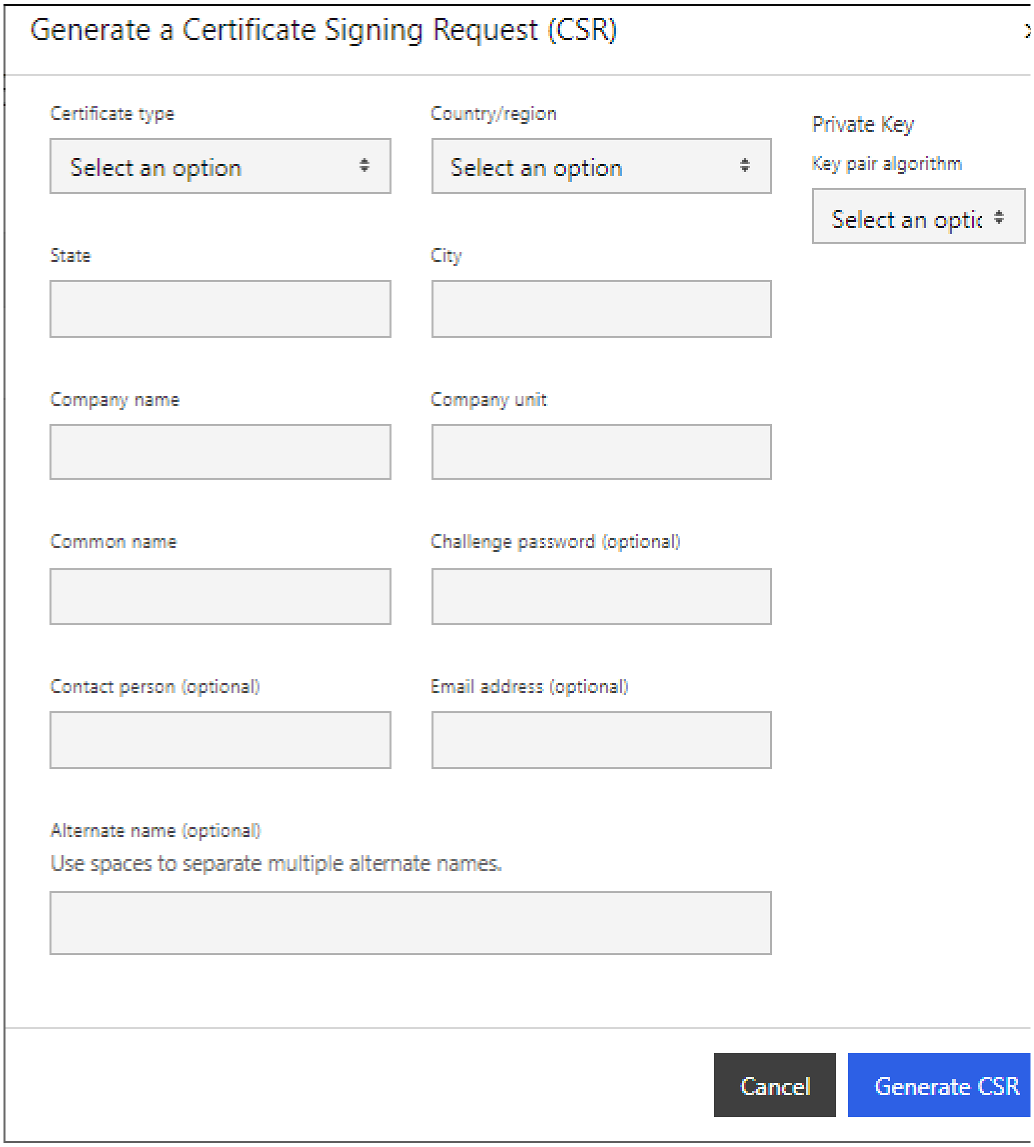
The fields in **Certificate – Add Certificate** window are explained below.

- **Certificate type**:
  Support LDAP Certificate and CA Certificate.
- **Upload File**:
  Click to browse a certificate file which should be of pem type
- **Add**
  To upload the SSL certificate and privacy key into the BMC.

NOTE:

Upon successful upload, HTTPs service will get restarted to use the newly uploaded SSL certificate.

6.5.2 Generate CSR



Generate a Certificate Signing Request (CSR)

Use spaces to separate multiple alternate names.

Figure 6-8: Certificate – Generate CSR

The fields in **Certificate – Generate CSR** window are explained below.

- **Certificate type**: select HTTPS Certificate or LDAP Certificate.
- **Country/Region**: Country or Region of the organization

  - Maximum length of 64 characters.

  - Special characters '#' and '$' are not allowed.

- **State**: State or Province of the organization

  - Maximum length of 64 characters.

  - Special characters '#' and '$' are not allowed.
- **City**: City or Locality of the organization

  - Maximum length of 64 characters.

  - Special characters '#' and '$' are not allowed.
- **Company name**: Company name for which the certificate is to be generated.

  - Maximum length of 64 characters.

  - Special characters '#' and '$' are not allowed.
- **Company unit**: Over all Company section unit name for which certificate is to be generated.

  - Maximum length of 64 characters.

  - Special characters '#' and '$' are not allowed.
- **Common name**: Company common name.

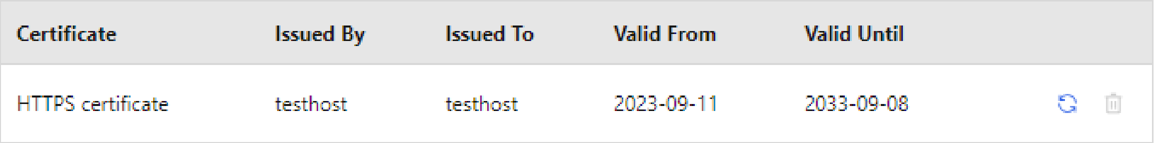
  - Only two characters are allowed.

  - Special characters are not allowed.
- **Challenge password**: The key length bit value of the certificate.
- **Email address**: Email Address of the organization
- **Alternate name**: Add multiple alternate names separated by space
- **Generate CSR**: To generate the new CSR for SSL certificate.

NOTE:

HTTPs service will get restarted, to use the newly generated SSL certificate.

6.5.3 View SSL



Certificate	Issued By	Issued To	Valid From	Valid Until
HTTPS certificate	testhost	testhost	2023-09-11	2033-09-08

Figure 6-9: Certificate – View SSL

The fields in the **Certificate Configuration** page are explained below.

- **Certificate**: Displays the basic information about the uploaded SSL certificate. It displays the field of certificate type.
- **Issued by**: Describes the certificate issuer information (company name)
- **Issued to**: Display the information about the certificate receiver (company name)
- **Valid From / Valid Until**: Displays the validity period of the uploaded certificate.