



# **Integrated Baseboard Management Controller Web Console**

## ***User Guide***

For Intel® Server M50FCP and Intel® Server D50DNP Families

**Rev. 1.0**

**December 2022**

<Blank page>

## Revision History

Date	Revision	Changes
December	1.0	Production Release

## Disclaimers

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

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

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

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

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

This document contains information on products, services and/or processes in development. All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications.

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

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

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

© Intel Corporation

# Table of Contents

---

<b>1. Introduction</b>	<b>10</b>
<b>2. Server Management Overview</b>	<b>11</b>
2.1 Standard Management Features Overview	11
2.2 Advanced System Management Features Overview	11
2.3 Supported Browsers	12
<b>3. Hardware Configuration for Server Management</b>	<b>13</b>
3.1 Server Management Hardware Configuration Using BIOS Setup Utility	13
3.2 Server Management Hardware Configuration Using Intel® Server Configuration Utility	15
3.2.1 Configuring the IP Address	15
3.2.2 Configuring the User	15
<b>4. Integrated BMC Web Console Overview</b>	<b>16</b>
4.1 Client Browsers	16
4.2 Web Console Access and Login	16
4.3 Web Console Navigation	17
<b>5. Integrated BMC Web Console Options</b>	<b>20</b>
5.1 System Tab	20
5.1.1 System Information	20
5.1.2 System Components	21
5.1.3 CPU Information	22
5.1.4 DIMM Information	22
5.1.5 NIC Information	23
5.1.6 NVMe* Information	23
5.1.7 Storage Information	24
5.1.8 Current Users	24
5.2 Server Health Tab	25
5.2.1 Sensor Readings	25
5.2.2 Event Log	27
5.3 Configuration Tab	28
5.3.1 Email Alert	28
5.3.2 IPv4 Network	29
5.3.3 IPv6 Network	31
5.3.4 VLAN	32
5.3.5 NTP – Network Time Protocol	33
5.3.6 Advanced System Management Key	34
5.3.7 SSL Certification	35
5.3.8 Users	37
5.3.9 Security Settings	39
5.3.10 Sensor Customization	41
5.3.11 BMC Firmware Update	41

5.3.12	BIOS/IFWI Firmware Update .....	43
5.3.13	CPLD Update.....	44
5.3.14	Syslog Server Configuration.....	44
5.3.15	Thermal Customization .....	45
5.4	Remote Control Tab.....	46
5.4.1	KVM.....	46
5.4.2	Server Power Control .....	47
5.4.3	Launch SOL.....	49
5.4.4	Virtual Front Panel.....	50
5.5	Virtual Media Tab .....	51
5.5.1	Local Image.....	51
5.5.2	Web ISO .....	52
5.6	Server Diagnostics Tab.....	53
5.6.1	System Diagnostics .....	53
5.6.2	POST Codes.....	54
5.6.3	System Defaults.....	54
5.7	Miscellaneous Tab .....	55
5.7.1	NM Configuration – Intel® Node Manager .....	55
5.7.2	Power Statistics.....	56
<b>Appendix A. Advanced Management License Key – Order, Registration, and Installation .....</b>		<b>57</b>
	How to Order Advanced System Management Key .....	57
	Order and Register the License Key as an Add-on Accessory (Not via CTO).....	57
	Advanced Management Key Installation .....	59
	Installation Using the Integrated BMC Web Console.....	60
	Installation Using the Intel® Server Configuration Utility.....	61
	Installation Using Redfish* .....	62
<b>Appendix B. Remote Console (KVM) Operation.....</b>		<b>63</b>
	Launch the Redirection Console.....	63
	Main Window .....	64
	Remote Console Control Bar .....	65
<b>Appendix C. Glossary.....</b>		<b>68</b>

## List of Figures

---

Figure 1. BMC LAN Configuration Screen of the BIOS Setup Utility.....	13
Figure 2. User Configuration Screen of the BIOS Setup Utility.....	14
Figure 3. Integrated BMC Web Console Login Page.....	16
Figure 4. Integrated BMC Web Console Homepage.....	17
Figure 5. Integrated BMC Web Console Help.....	18
Figure 6. Busy Indicator Bar.....	18
Figure 7. System Information Page.....	20
Figure 8. System Components Page.....	21
Figure 9. System CPU Information Page.....	22
Figure 10. System DIMM Information Page.....	22
Figure 11. System NIC Information Page.....	23
Figure 12. System NVMe* Information Page.....	23
Figure 13. System Storage Information Page.....	24
Figure 14. System Current Users Page.....	24
Figure 15. Server Health Sensor Readings Page (Thresholds Not Displayed).....	25
Figure 16. Server Health Sensor Readings Page (Thresholds Displayed).....	25
Figure 17. Server History & Live Reading.....	26
Figure 18. Server Health Event Log Page.....	27
Figure 19. Alerts Page.....	28
Figure 20. IPV4 Network DHCP Page.....	29
Figure 21. IPV4 Network Static Page.....	29
Figure 22. IPV6 Network Page.....	31
Figure 23. VLAN Settings Page.....	32
Figure 24. NTP Settings Page.....	33
Figure 25. Advanced System Management Key Page (uninstalled).....	34
Figure 26. Advanced System Management Key Page (installed).....	35
Figure 27. SSL Certification Page.....	35
Figure 28. SSL Certification Page (Add New CA Certificate).....	36
Figure 29. User List Page.....	37
Figure 30. Add New User Page.....	37
Figure 31. Modify User Page.....	38
Figure 32. Delete User Page.....	38
Figure 33. Configuration Security Settings Page.....	39
Figure 34. Server Power Control Page.....	40
Figure 35. Sensor Customization Page.....	41
Figure 36. BMC Firmware Update Page.....	42
Figure 37. BIOS/IFWI Firmware Update Page.....	43
Figure 38. CPLD Update Page.....	44
Figure 39. Syslog Server Configuration Page.....	45

Figure 40. Thermal Customization Page .....	46
Figure 41. Remote Control KVM Page .....	47
Figure 42. Remote Control Server Power Control Page .....	48
Figure 43. Remote Control Launch SOL Page.....	49
Figure 44. Launch SOL in Pop-Up Window.....	49
Figure 45. Remote Control Virtual Front Panel Page.....	50
Figure 46. Local Image Page.....	51
Figure 47. Launch Window to Mount Local Image Page .....	51
Figure 48. Web ISO.....	52
Figure 49. Server System Diagnostics Page.....	53
Figure 50. Server Diagnostics POST Codes Page .....	54
Figure 51. Server Diagnostics Default Page.....	54
Figure 52. Intel® Node Manager Configuration Page .....	55
Figure 53. Power Statistics Page.....	56
Figure 54. Example Email.....	57
Figure 55. Register Key .....	58
Figure 56. Activate Key .....	58
Figure 57. Download Key.....	59
Figure 58. Integrated BMC Web Console Advanced System Management Key Page.....	60
Figure 59. Web Console System Information Page.....	60
Figure 60. Upload Advanced Management License Key Using SYSCFG Utility .....	61
Figure 61. Confirm Activation of Advanced Management Key Using SYSCFG Utility .....	61
Figure 62. Redfish Command to Upload the Advanced System Management Key.....	62
Figure 63. Redfish Command to Verify Activation of Advanced Server Management Key.....	62
Figure 64. Remote Control Console Redirection Page.....	63
Figure 65. Remote Control Console Redirection Page.....	63
Figure 66. Remote Console Window.....	64
Figure 67. Remote Console Main Window .....	64
Figure 68. Remote Console Control Bar .....	65
Figure 69. Remote Console Macro Menu .....	65
Figure 70. Keyboard Options Menu .....	65
Figure 71. Keyboard Option .....	66
Figure 72. Remote Console Power Control Menu .....	66
Figure 73. Force-Enter BIOS Setup Button .....	67
Figure 74. Force-Enter BIOS Setup Pop-Up Window .....	67

## List of Tables

---

Table 1. Integrated BMC Web Console Tabs.....	18
Table 2. Integrated BMC Web Console Toolbar.....	19
Table 3. System Information Fields.....	21
Table 4. Server Health Sensor Readings Options.....	26
Table 5. Server history & Live Reading Options.....	26
Table 6. Server Health Event Log Options .....	27
Table 7. Alerts Options .....	28
Table 8. IPv4 Network Settings Options.....	30
Table 9. IPv6 Network Settings Options.....	31
Table 10. VLAN Settings Options.....	32
Table 11. Date and Time Options .....	33
Table 12. Advanced System Management Key Options .....	34
Table 13. SSL Certificate Options .....	36
Table 14. Configuration Security Settings Options .....	39
Table 15. Sensor Customization Options .....	41
Table 16. BMC Firmware Update Options .....	42
Table 17. BIOS/ME Firmware Update Options .....	43
Table 18. CPLD Update Options.....	44
Table 19. Syslog Server Configuration Options.....	45
Table 20. Thermal Customization Options .....	46
Table 21. KVM Page Options.....	47
Table 22. Server Power Control Options for Remote Control .....	48
Table 23. SOL Options.....	49
Table 24. Remote Control Virtual Front Panel Options.....	50
Table 25. Local Image Options.....	52
Table 26. Web ISO Options .....	52
Table 27. Intel® Node Manager Configuration Options .....	56
Table 28. Remote Console Power Control .....	66

# 1. Introduction

---

Intel server boards and systems include an embedded web server that can be accessed using any supported browser. The user interface for the embedded web server is identified as the Integrated Baseboard Management Controller Web Console (Integrated BMC Web Console), which allows administrators to view system information including firmware versions, server health, diagnostic information, power statistics. It enables configuration of the BMC and BIOS, and also provides the ability for users to perform power actions, launch KVM, and set up virtual media redirection.

This user guide provides an overview of the Integrated BMC Web Console. It describes how to setup the server for secure access, how to access the web console, and how each supported feature is used.

The features and procedures described in this document apply to the following Intel server products:

- Intel® Server M50FCP Family
- Intel® Server D50DNP Family

Integrated BMC Web Console information for previous generation Intel server products can be found in versions of this document specific to those products.

For additional information and downloads visit:

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

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

## 2. Server Management Overview

---

All Intel server products support embedded server management features. Core to the management features is the baseboard management controller (BMC). The BMC supports many system management features including intra-system sensor monitoring, fan speed control, system power management, and system error handling and messaging. It also provides platform management capabilities including remote access, monitoring, logging, and alerting features.

---

**Note:** For in-depth server management information, refer to the Technical Product Specification (TPS) for the specified Intel server product.

---

Server management capabilities of an Intel server board or Intel server system can be split in two groups:

- Standard management features (Included)
- Optional advanced management features that can be enabled with the purchase of an advanced management license key (IPC ADVSYSMGMTKEY).

### 2.1 Standard Management Features Overview

All Intel server products include standard server management features. These include support for:

#### Standard System Features

- Integrated BMC Web Console
- Virtual KVM over HTML5
- Redfish\* 2.0 interface
- Support for IPMI 2.0 protocol
- Intel® Dynamic Power Node Manager
- Out-of-band BIOS/BMC Update and Configuration
- System Inventory
- Email Alerting
- Autonomous Debug Log

### 2.2 Advanced System Management Features Overview

With the purchase of an optional advanced system management license, the BMC supports a method to upload advanced system management files to enable features for real-time data collection and analysis, virtual media redirection and network share, and Out-of-band Hardware RAID Management. The license file can be uploaded through the embedded web console, Redfish, and Intel Server Configuration Utility. See Appendix A for complete installation instructions.

Advanced manageability features are supported over all NIC ports enabled for server manageability. These include on-board BMC-shared LAN ports, which share network bandwidth with the host system, and with the onboard dedicated management port.

#### Advanced Features that Require a Software License Key

- Virtual Media Local Image Redirection
- Virtual media over network share
- Out-of-band hardware RAID management
- License Status command for Intel Data Center Manger, compatible for RMM4/License

## 2.3 Supported Browsers

Virtual KVM over HTML5 and virtual media over HTML5 features require a browser to support the features of WebSocket and HTML5.

The following browsers are tested:

- Red Hat Enterprise\* 8.5 64-bit: Mozilla Firefox\* 91.2
- Ubuntu\* 20.10 64-bit: Mozilla Firefox 90.0
- Windows 10 64-bit: Google Chrome\* 101.0.4951.54 (official build) (64-bit)
- Windows 10 64-bit: Microsoft Edge\* 101.0.1210.39 (official build) (64-bit)

### 3. Hardware Configuration for Server Management

This chapter describes the hardware configuration steps necessary to access the Integrated BMC Web Console remotely.

Two steps are necessary before the server management BMC LAN can be used:

1. One or both LAN channels must be configured as either DHCP or with static addresses.
2. At least one user must be enabled to use the LAN channels.

Configuring these options can be performed using either the embedded <F2> BIOS Setup Utility or by using the Intel® Server Configuration Utility, which can be downloaded from the following Intel website:

<https://www.intel.com/content/www/us/en/support.html> and initiating a search for “Intel® Server Configuration Utility”.

#### 3.1 Server Management Hardware Configuration Using BIOS Setup Utility

1. During the power-on self-test (POST), press <F2> to access the Main page of the embedded BIOS setup utility.
2. Navigate to the **Server Management** tab and select **BMC LAN Configuration** to enter the BMC LAN Configuration screen (see [Figure 1](#)).

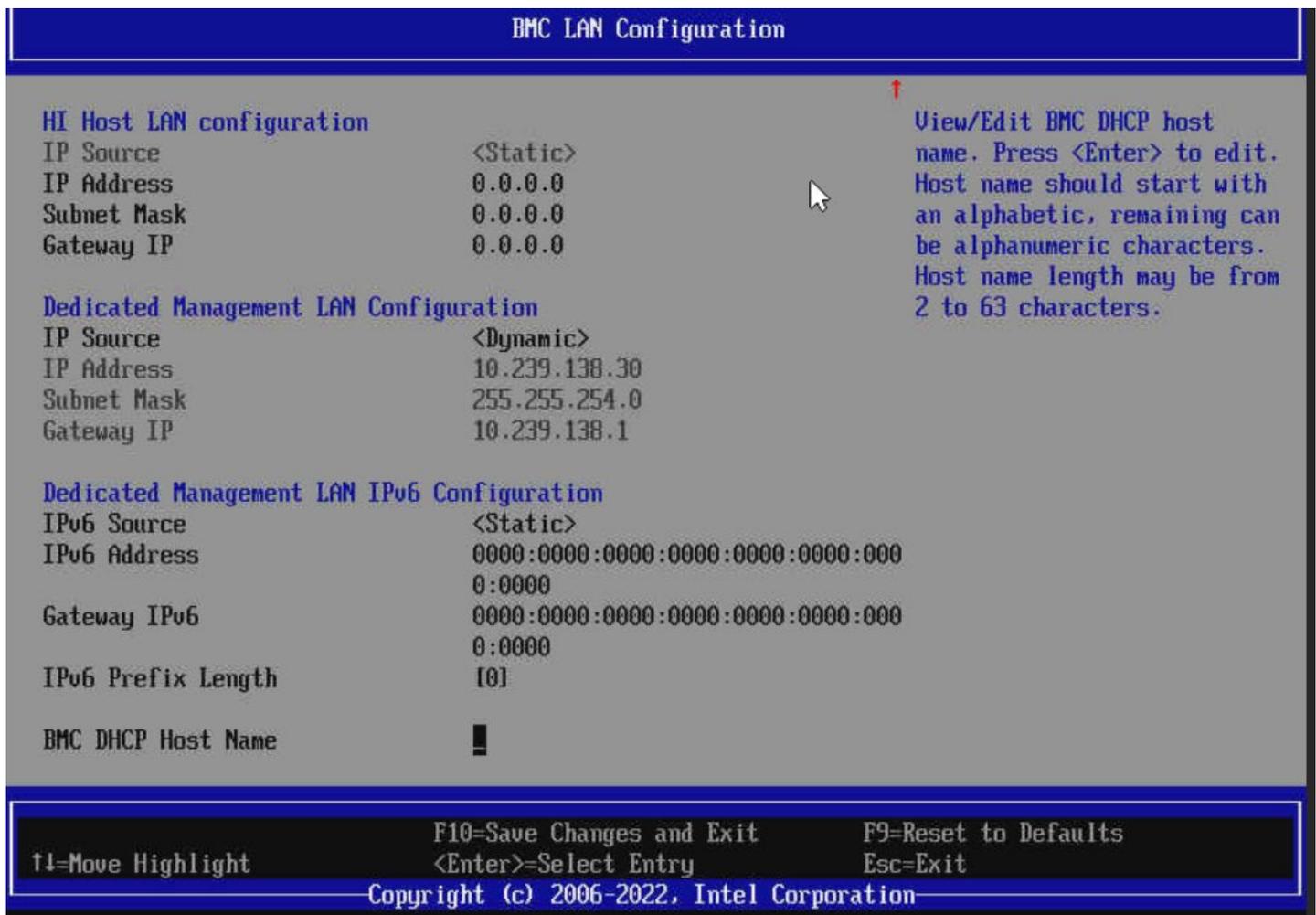
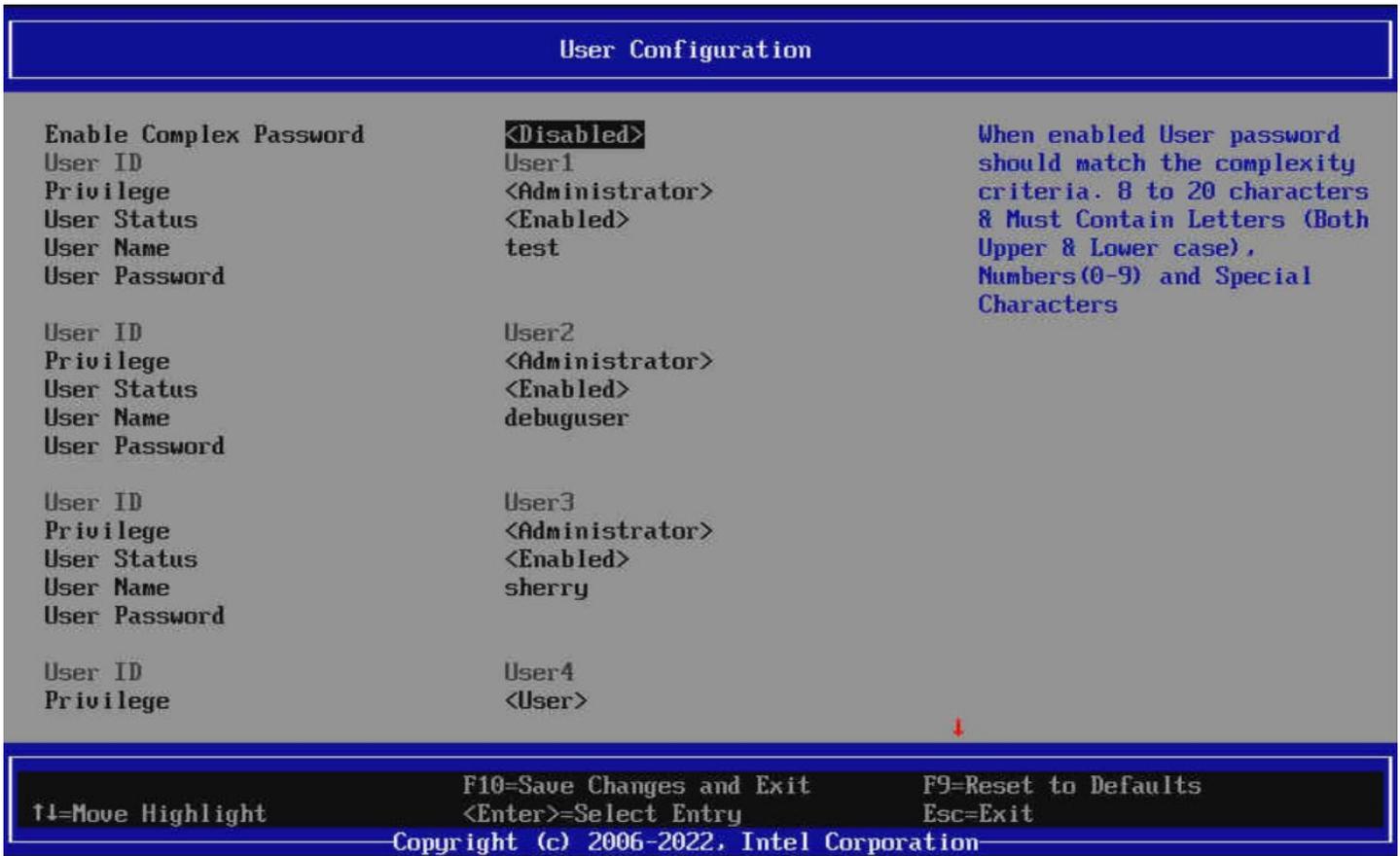


Figure 1. BMC LAN Configuration Screen of the BIOS Setup Utility

3. For an IPv4 network:
  - If configuring the server management BMC LAN, scroll down to **Dedicated Management LAN Configuration > IP source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
4. For an IPv6 network:
  - If configuring the server management BMC LAN, scroll to **Baseboard LAN IPv6 configuration > IP source** and then select **Enabled**. Then scroll to **IPV6 source** and select either **Static** or **Dynamic**. If **Static** is selected, configure the **IPV6 address**, **Gateway IPV6**, and **IPV6 Prefix Length** as needed.
5. Navigate back to the **Server Management** tab then select **User Configuration** to enter the User Configuration screen (Figure 2).



**Figure 2. User Configuration Screen of the BIOS Setup Utility**

6. Under a **User ID**, enter a **User Name**
7. Press **<F10>** to save the configured settings and exit the BIOS setup utility
8. Reboot the server and re-enter the **<F2>** BIOS Setup Utility (See the Notes section on the following page)
9. Navigate back to the **Server Management** tab and select **User Configuration**
10. Under the selected **User ID** configure the following settings: (See the Notes section on the following page)
  - **Privilege** – Select the privilege to be used. Administrator privilege is required to use KVM or media redirection enabled by the advanced management features.
  - **User status** – Select **Enabled**.
  - **User password** – Enter the desired password twice.

11. Press **<F10>** to save the configured settings and exit the BIOS setup utility. Reboot the server to use LAN ports with configured settings.

**Notes:**

- The User Name must be entered and saved before any additional User ID options can be configured. To save the User Name data, the BIOS Utility must be exited and the system must be rebooted, to re-enter the BIOS Utility.
- User names cannot be saved as “Null”, or “root”, or match any other existing user names.
- User names cannot exceed 16 characters and passwords cannot exceed 20 characters.

## 3.2 Server Management Hardware Configuration Using Intel® Server Configuration Utility

The Intel® Server Configuration Utility is a command-line tool that can be used to display and/or set a variety of system BIOS and management firmware settings. This utility can be used to configure the required server management features necessary to access the Integrated BMC Web Console. This utility is supported in EFI, Linux\*, and Microsoft Windows operating systems. The commands used are the same for all versions.

The Intel® Server Configuration Utility can be downloaded from the following Intel website:

<https://www.intel.com/content/www/us/en/support.html> and initiating a search for “Intel® Server Configuration Utility”.

Refer to the Intel® Server Configuration Utility User Guide for addition utility usage information.

**Note:**

The examples in the following sections use the dedicated server management NIC channel 3. If using a different LAN port, substitute the appropriate channel number:

- for NIC1 use channel 1
- for NIC 2 use channel 2

### 3.2.1 Configuring the IP Address

1. Set a static IP address and subnet mask on LAN channel 3.

```
syscfg /le 3 static <STATIC_IP> <SUBNET_MASK>
```

2. If needed, set the default gateway on LAN channel 3.

```
syscfg /lc 3 12 <DEFAULT_GATEWAY_IP>
```

3. Set the DHCP IP address source on LAN channel 3.

```
syscfg /le 3 dhcp
```

### 3.2.2 Configuring the User

1. Enable BMC user 4 on LAN channel 3.

```
syscfg /ue 4 enable 3
```

2. Set the password for BMC user 4. This example sets the password to Test@123.

```
syscfg /u 4 "test" "Test@123"
```

3. Enable the admin privilege BMC user 4 on LAN channel 3.

```
syscfg /up 4 3 admin
```

## 4. Integrated BMC Web Console Overview

---

The Integrated BMC Web Console may be used to access the server sensors, server logs, and to launch a remote console (with keyboard, video, and mouse (KVM) access) to the target server. This section describes connecting to the Web Console and provides an overview of the layout and navigation of the user interface.

The examples in this chapter identify the user as "testuser".

### 4.1 Client Browsers

The Integrated BMC Web Console may be accessed using a standard web browser. To access the web console using a securely encrypted connection, use a browser that supports the HTTPS protocol. Strong security is only assured by using a 256-bit cipher strength (encryption).

---

**Note:** The web console is designed for a screen size of 1280 pixels by 1024 pixels or larger. In smaller screens, use the browser slider controls to see the full content of each webpage.

---

### 4.2 Web Console Access and Login

To access the Login screen of the Web Console, enter the IP address of the management port configured in Chapter 3 onto the address line of a web browser. To use a secure connection, type:

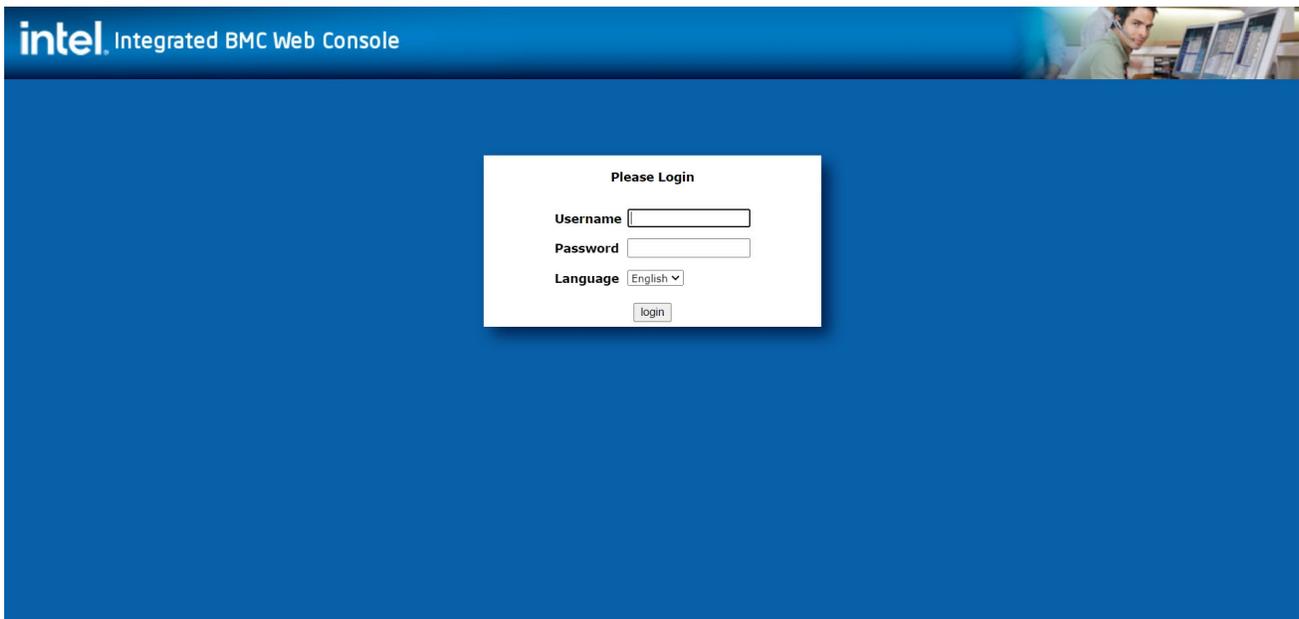
`https://<IPaddress_or_Hostname>/`

On the Web Console Login screen enter the User name and password, as configured in Chapter 3, and select a language option from the drop down box (see [Figure 3](#)).

---

**Note:** The user name and password are case sensitive.

---



**Figure 3. Integrated BMC Web Console Login Page**

Click the **Login** button. With the proper credentials entered, the Web Console home page will be displayed (See [Figure 4](#)).

After the initial login, system administrators can change passwords, create users, and have full control over access to the advanced management features (If enabled – See [Appendix A](#)).

### 4.3 Web Console Navigation

The Web Console homepage includes eight tabs along the top line for navigation within the web console (see Figure 4). A description for each tab can be found in Table 1.

A secondary set of page options specific to the selected tab are displayed on the left edge of the window (see Figure 4). The first item of the secondary page list is the default page that appears when the tab is selected.

A description for each tab's secondary menu options can be found in Chapter 5.

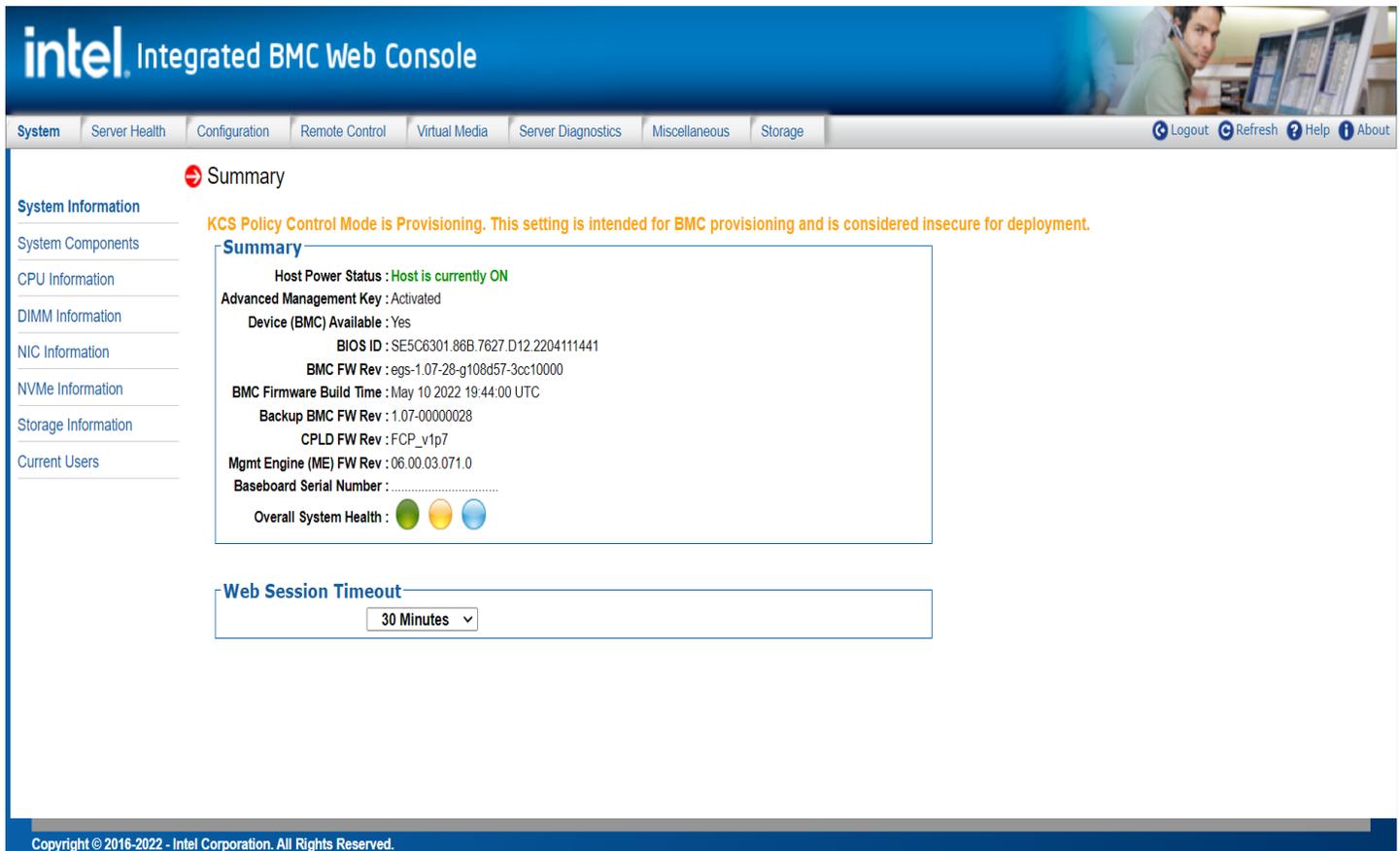


Figure 4. Integrated BMC Web Console Homepage

A tool bar with additional web console usage options can be found on the right side of the top line of every web console page (see Figure 4). For descriptions of each option see Table 2.

Selecting the **Help** option from the top Tool Bar displays a side-bar on the right side of the window which provides useful information for items on the given page (See Figure 5)

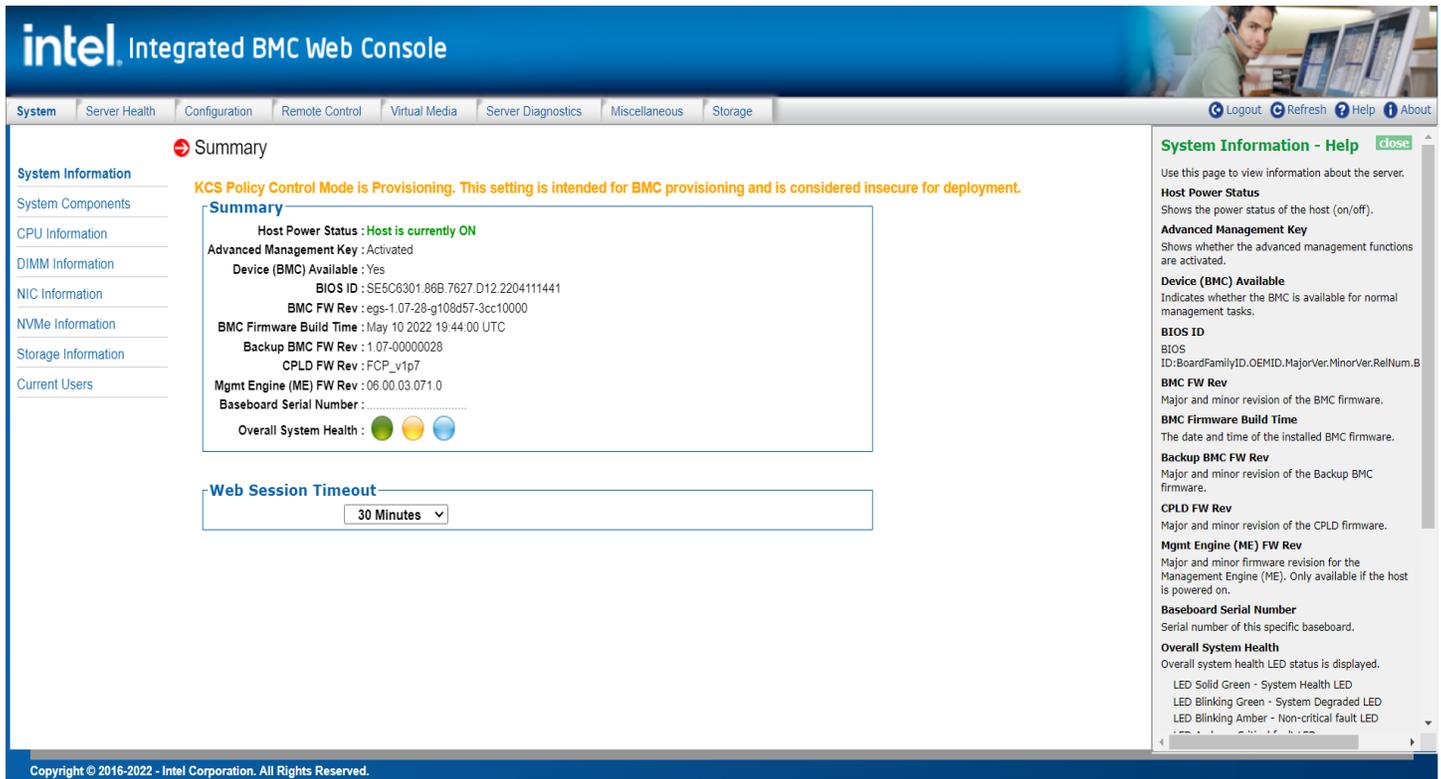


Figure 5. Integrated BMC Web Console Help

When the web console is working on a user request, a busy indicator bar appears as shown in Figure 6.



Figure 6. Busy Indicator Bar

Table 1. Integrated BMC Web Console Tabs

Top Tab	Description	Secondary Page Options
<b>System</b>	Provides access to general information about the server. The tab automatically opens the System Information page.	<ul style="list-style-type: none"> <li>System Information</li> <li>System Components</li> <li>CPU Information</li> <li>DIMM Information</li> <li>NIC Information</li> <li>NVMe Information</li> <li>Storage Information</li> <li>Current Users</li> </ul>
<b>Server Health</b>	Provides access to the sensors and event log. The tab automatically opens the Sensor Readings page.	<ul style="list-style-type: none"> <li>Sensor Readings</li> <li>Event Log</li> </ul>

Top Tab	Description	Secondary Page Options
<b>Configuration</b>	Provides access to configure various settings for the server. The tab automatically opens the Alerts page.	<ul style="list-style-type: none"> <li>Alerts</li> <li>Alert Email</li> <li>IPv4 Network</li> <li>IPv6 Network</li> <li>VLAN</li> <li>NTP Settings</li> <li>LDAP</li> <li>Advanced System Management Key</li> <li>Active Directory</li> <li>SSL Certification</li> <li>Users</li> <li>Security Settings</li> <li>Sensor Customization</li> <li>BMC Firmware Update</li> <li>BIOS/IFWI Firmware Update</li> <li>CPLD Update</li> <li>Syslog Server Configuration</li> <li>Thermal Customization</li> </ul>
<b>Remote Control</b>	Provides access to the remote console and control of the server power state. The tab automatically opens the KVM page.	<ul style="list-style-type: none"> <li>KVM</li> <li>Server Power Control</li> <li>Launch SOL</li> <li>Virtual Front Panel</li> </ul>
<b>Virtual Media</b>	Allows the user to share files locally or in network. Each image/folder will be emulated to the host as a USB device. The tab automatically opens the Local Image page.	<ul style="list-style-type: none"> <li>Local Image</li> <li>Web ISO</li> </ul>
<b>Server Diagnostics</b>	Provides access to server diagnostics information. The tab automatically opens the System Diagnostics page.	<ul style="list-style-type: none"> <li>System Diagnostics</li> <li>POST Codes</li> <li>System Defaults</li> </ul>
<b>Miscellaneous</b>	Provides access to node manager configuration and power statistics. The tab automatically opens the NM Configuration page.	<ul style="list-style-type: none"> <li>NM Configuration</li> <li>Power Statistics</li> </ul>
<b>Storage(M50FCP only)</b>	Provides access to storage configuration. The tab automatically opens the Adapter page.	<ul style="list-style-type: none"> <li>Adapter</li> <li>Physical Device</li> <li>Logical Device</li> </ul>

**Table 2. Integrated BMC Web Console Toolbar**

Button	Function
<b>Logout</b>	End the current web console session. Click <b>OK</b> to confirm. After logging out, the web console returns to the login screen.
<b>Refresh</b>	Refresh the current webpage, including any data shown on the page. <b>Note:</b> Using the web browser's refresh/reload button or pressing the function key <F5> to do a refresh/reload is not supported for reloading the web console pages. Using either of them returns the web console to the homepage.
<b>Help</b>	View a brief description of the current page in a frame at the right side of the browser window (Figure 5). Close the help frame by clicking the "X" in the upper right corner of the frame or by clicking the <b>Help</b> button again.
<b>About</b>	View the Intel copyright information and a statement about the use of open source code.

**Notes:**

- If no user activity is detected by the web console for 30 minutes, the current session is automatically terminated and the user must log in again for continued access to the web console.
- If a KVM remote console window is open, the web session does not automatically time out.

## 5. Integrated BMC Web Console Options

This chapter provides a detailed description for each Integrated BMC Web Console page. The descriptions are organized in sections corresponding to the eight tabs found on the top line of the web console window.

Refer to [Section 4.3](#) for information describing web console interface navigation and for brief descriptions of the available tab pages and their secondary pages.

**Note:** Not all of the following sections are used by or related to features enabled by advanced management but have been added here for completeness.

### 5.1 System Tab

The System tab contains general information about the system as explained in the following subsections.

#### 5.1.1 System Information

The System Information page displays a summary of general system information. This information includes:

- Host power status
- Advanced management key status
- BMC available status
- BIOS ID
- BMC firmware version and build time
- Backup BMC firmware version
- CPLD firmware version
- Intel Management Engine (Intel ME) firmware version
- Server Board serial number
- Overall system health status.

See [Table 3](#) for complete descriptions of each summary field.

The screenshot displays the Intel Integrated BMC Web Console interface. At the top, the Intel logo and 'Integrated BMC Web Console' are visible. A navigation bar contains tabs for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, and Storage. The 'System' tab is selected. Below the navigation bar, a 'Summary' section is shown with a red arrow icon. A warning message in orange text reads: 'KCS Policy Control Mode is Provisioning. This setting is intended for BMC provisioning and is considered insecure for deployment.' The summary box contains the following information:

- Host Power Status : Host is currently ON
- Advanced Management Key : Activated
- Device (BMC) Available : Yes
- BIOS ID : SE5C6301.86B.7627.D12.2204111441
- BMC FW Rev : egs-1.07-7-g0631ed-3cc10000
- BMC Firmware Build Time : May 06 2022 07:36:35 UTC
- Backup BMC FW Rev : 1.03-00000009
- CPLD FW Rev : FCP\_v1p7
- Mgmt Engine (ME) FW Rev : 06.00.03.071.0
- Baseboard Serial Number : .....
- Overall System Health : (Green, Yellow, Blue circles)

Below the summary box, there is a 'Web Session Timeout' section with a dropdown menu currently set to '1 Hour'.

Copyright © 2016-2022 - Intel Corporation. All Rights Reserved.

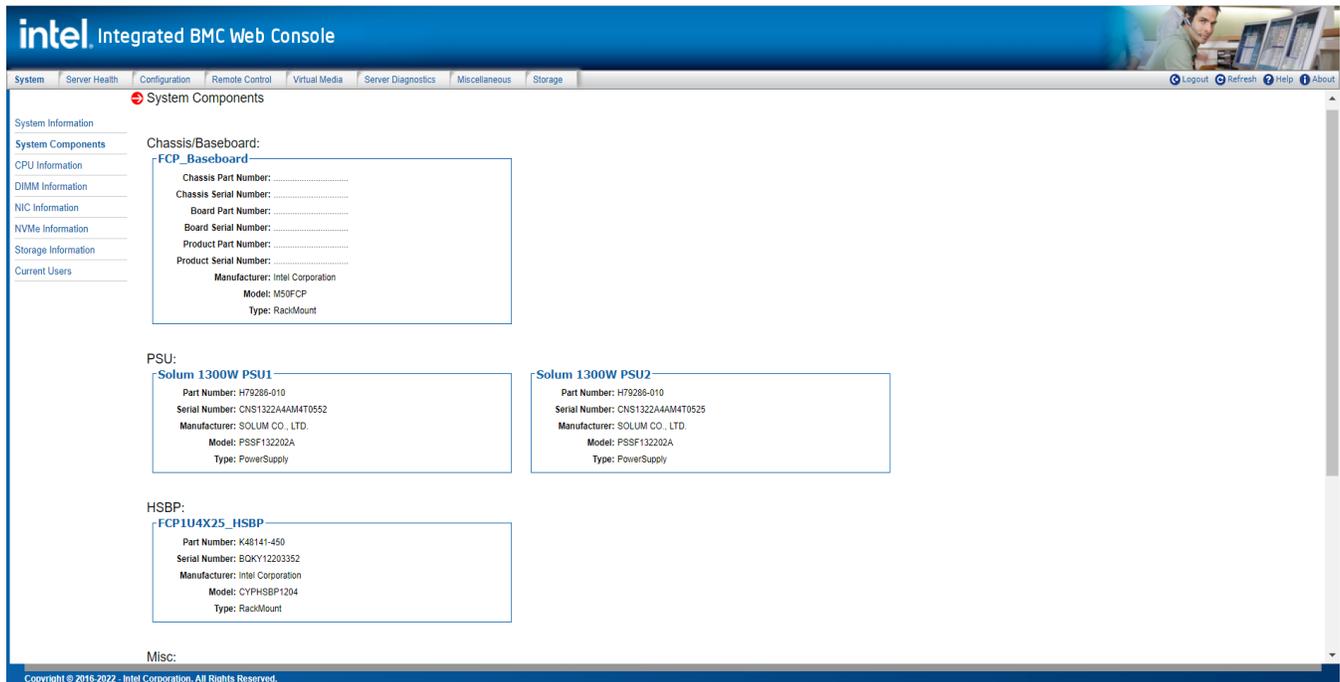
Figure 7. System Information Page

**Table 3. System Information Fields**

Information	Details
Host Power Status	Power status of the host (on/off).
Advanced Management Key	Indicates whether the software license has been activated.
Device (BMC) Available	Indicates whether the BMC is available for normal management tasks.
BIOS ID	Major and minor revision of the BIOS.
BMC FW Rev	Major and minor revision of the BMC firmware.
BMC Firmware Build Time	The build date and time of the installed BMC firmware.
Backup BMC FW Rev	Major and minor revision of the backup BMC firmware.
CPLD FW Rev	Major and minor revision of the CPLD firmware.
Mgmt Engine (ME) FW Rev	Major and minor revision of the Intel Management Engine firmware.
Baseboard Serial Number	Serial number of the baseboard in the system.
Overall System Health	A general indication of the system health: <ul style="list-style-type: none"> <li>• Left (green) = System ready LED</li> <li>• Center (amber) = System fault LED</li> <li>• Right (blue) = Chassis ID LED</li> </ul>

### 5.1.2 System Components

The System Components page displays BMC system component information for: chassis/Server board, power supply unit (PSU), hot-swap backplane (HSBP), riser card, and other miscellaneous devices configured within the system. Information for each device includes: part number, serial number, manufacturer, model, type part. See [Figure 8](#) for details.



**Figure 8. System Components Page**

### 5.1.3 CPU Information

The CPU Information page shows data for each processor installed on the host system. This information includes: socket designation, manufacturer, version, processor signature, processor type, family, speed, number of cores, voltage, socket type, status, serial number, asset tag, and part number.

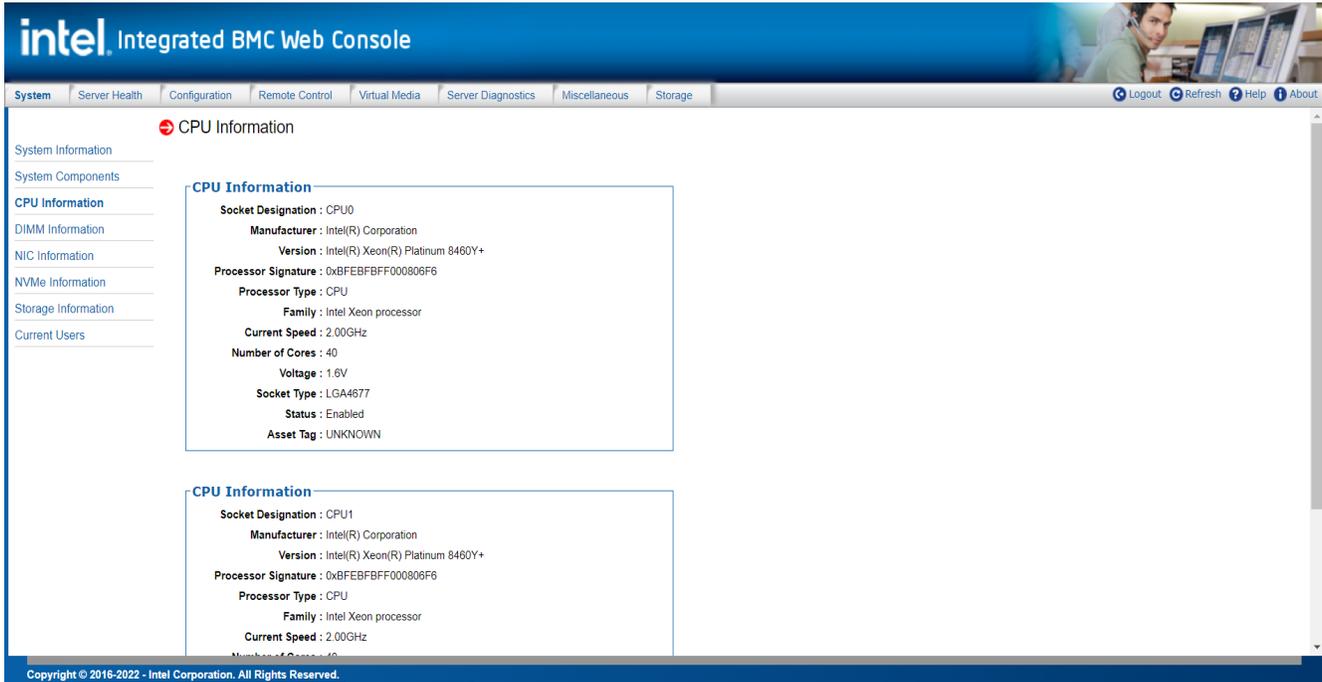


Figure 9. System CPU Information Page

### 5.1.4 DIMM Information

The DIMM Information page displays information for DIMMs installed in the host system. The DIMM information includes slot number, size, memory type, speed, manufacturer, asset tag, also memory serial and part numbers.

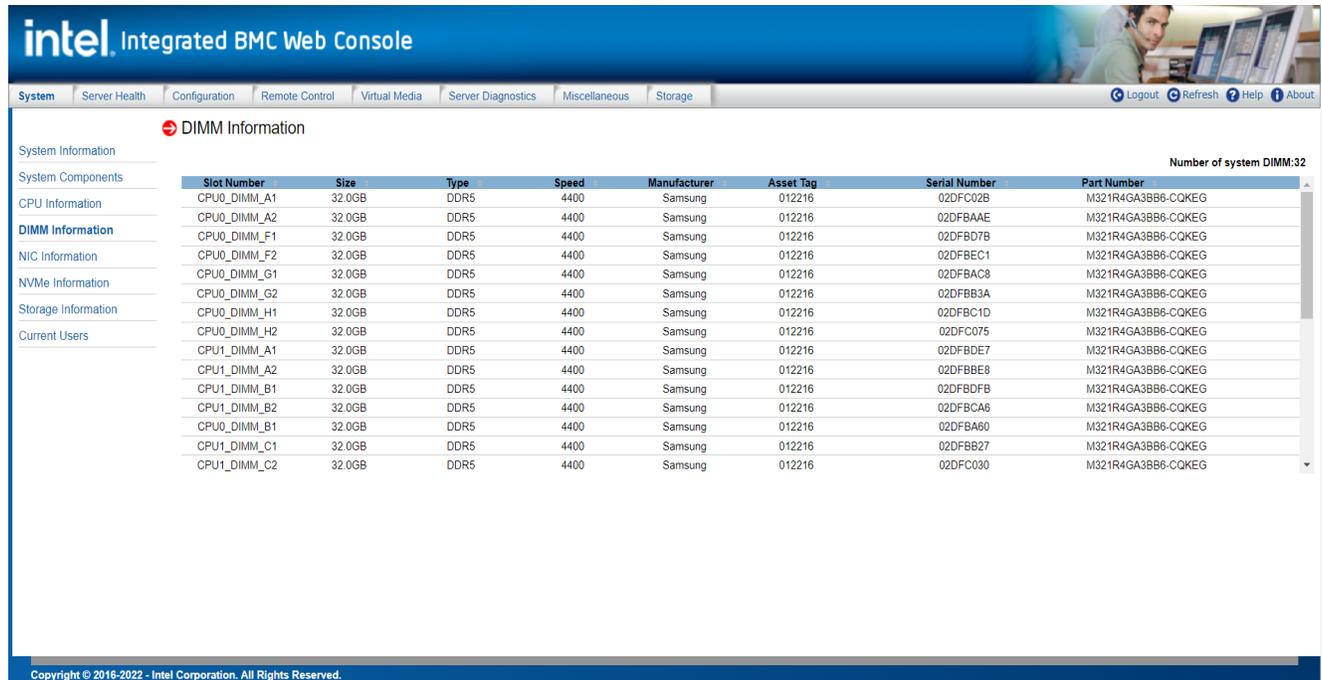


Figure 10. System DIMM Information Page

### 5.1.5 NIC Information

The NIC Information page displays information for Networking add-in cards installed in the host system. This data includes PCI class code, slot number, vendor ID, device ID, current speed (in Mb per second), portIdx, media state, media access controller address (MAC address), firmware version.

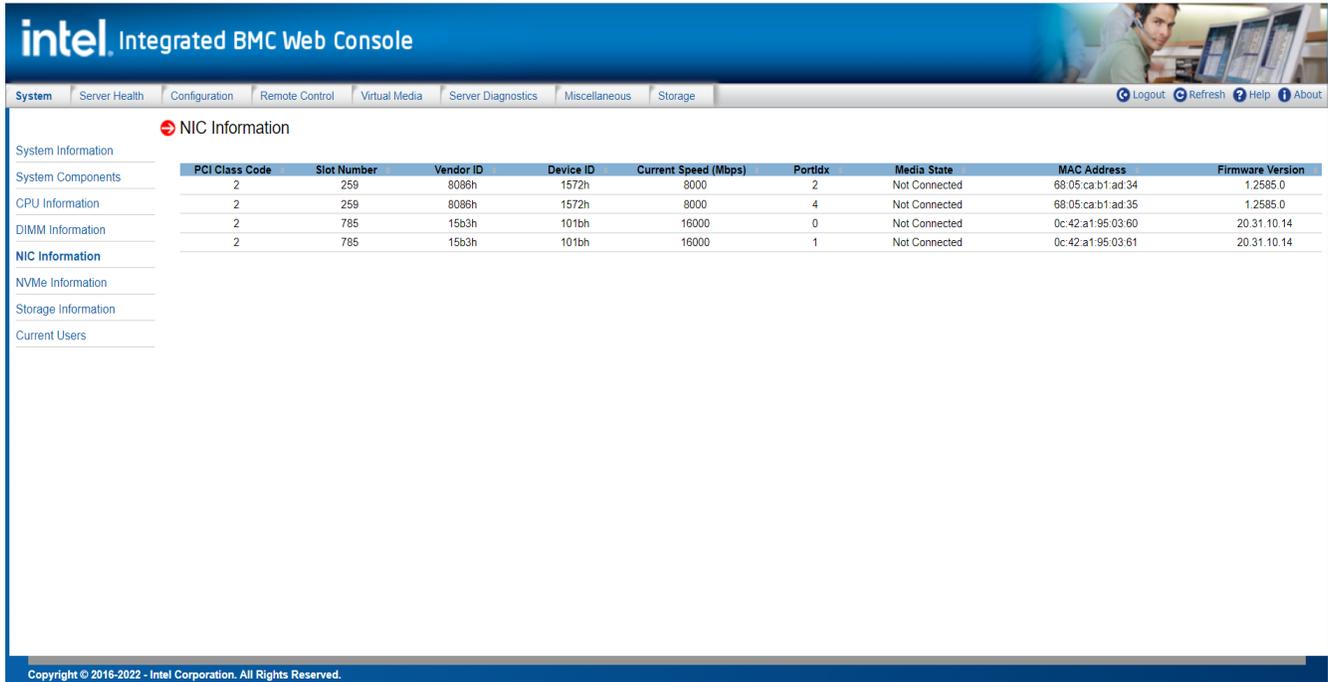


Figure 11. System NIC Information Page

### 5.1.6 NVMe\* Information

The NVMe Information page displays status information for each NVMe drive installed onto a backplane. Each group box displayed contains statistics for a single NVMe drive. The group box identifies the drive by HSBP number, and by drive slot number.

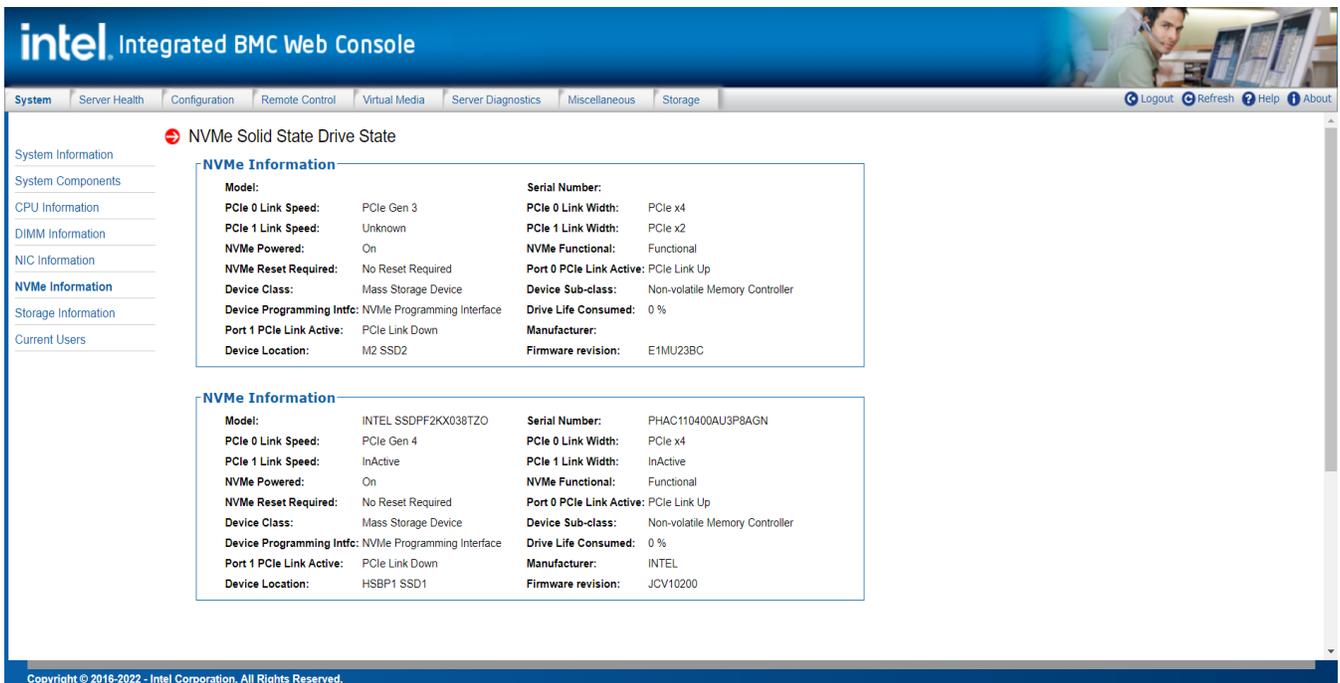


Figure 12. System NVMe\* Information Page

### 5.1.7 Storage Information

The Storage Information page displays information of storage devices installed in the host system. This information includes port destination, device index, connector type, protocol, device type, capacity (in GB), RPM, model, serial, PCI class code, vendor ID, device ID, firmware version.

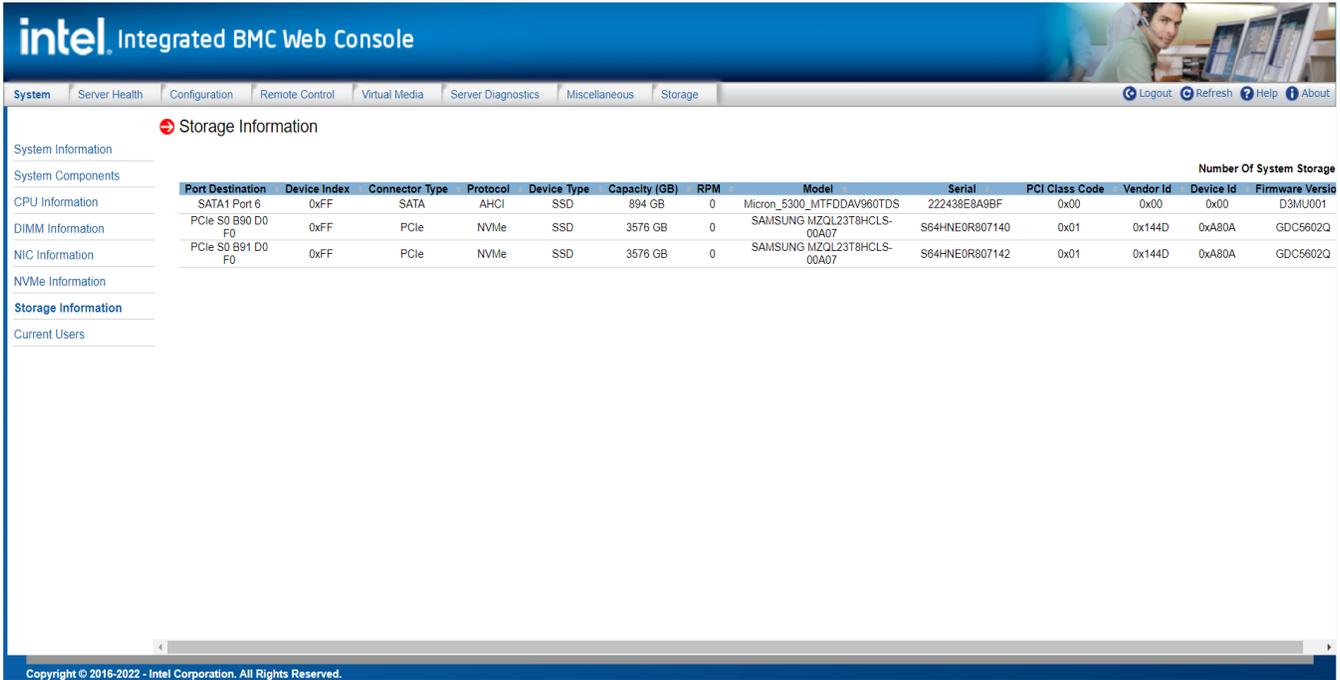


Figure 13. System Storage Information Page

### 5.1.8 Current Users

The Current Users page displays the users currently logged in to the BMC through the embedded web server. This data includes the User Name, connection type, KVM in use or not, local image 1/2 in use, and the User IP address.

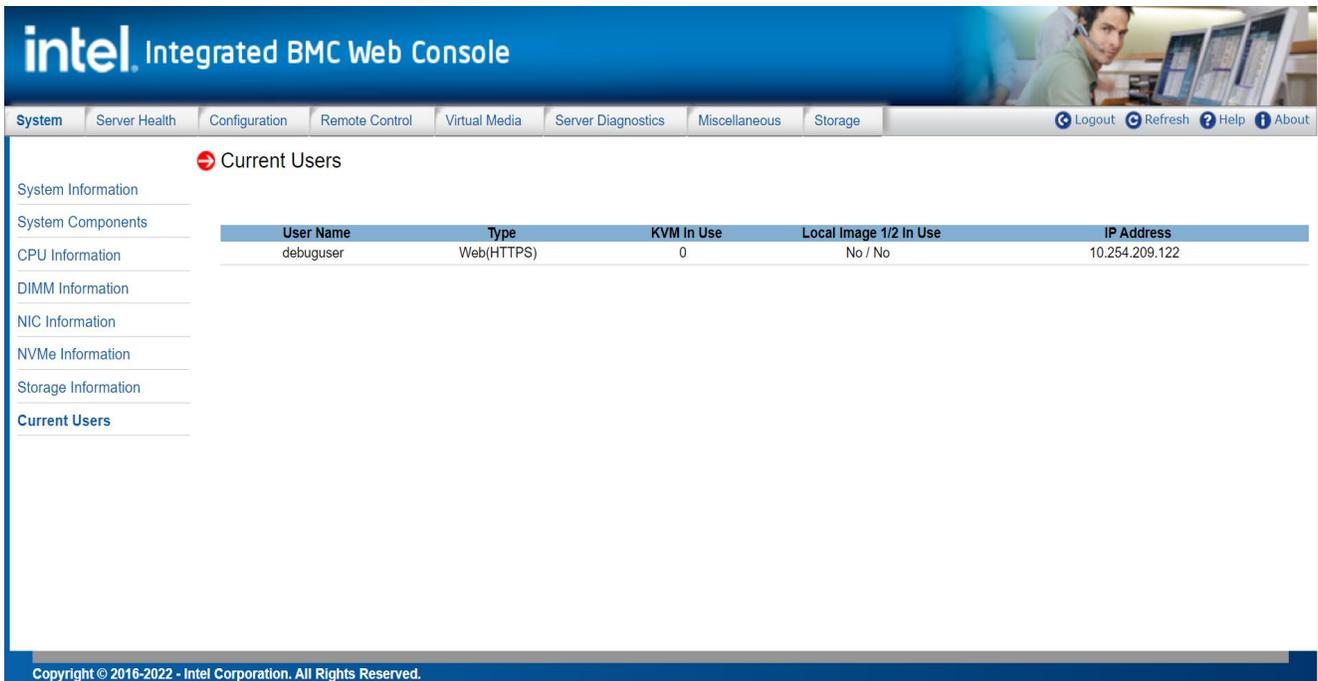


Figure 14. System Current Users Page

## 5.2 Server Health Tab

The Server Health tab includes secondary page options to view the System Sensor Readings and System Event Log windows.

### 5.2.1 Sensor Readings

The Sensor Readings page displays information for all monitored system sensors, including: current sensor state, Sensor Name, Sensor Status, and Current sensor reading See [Figure 15](#).

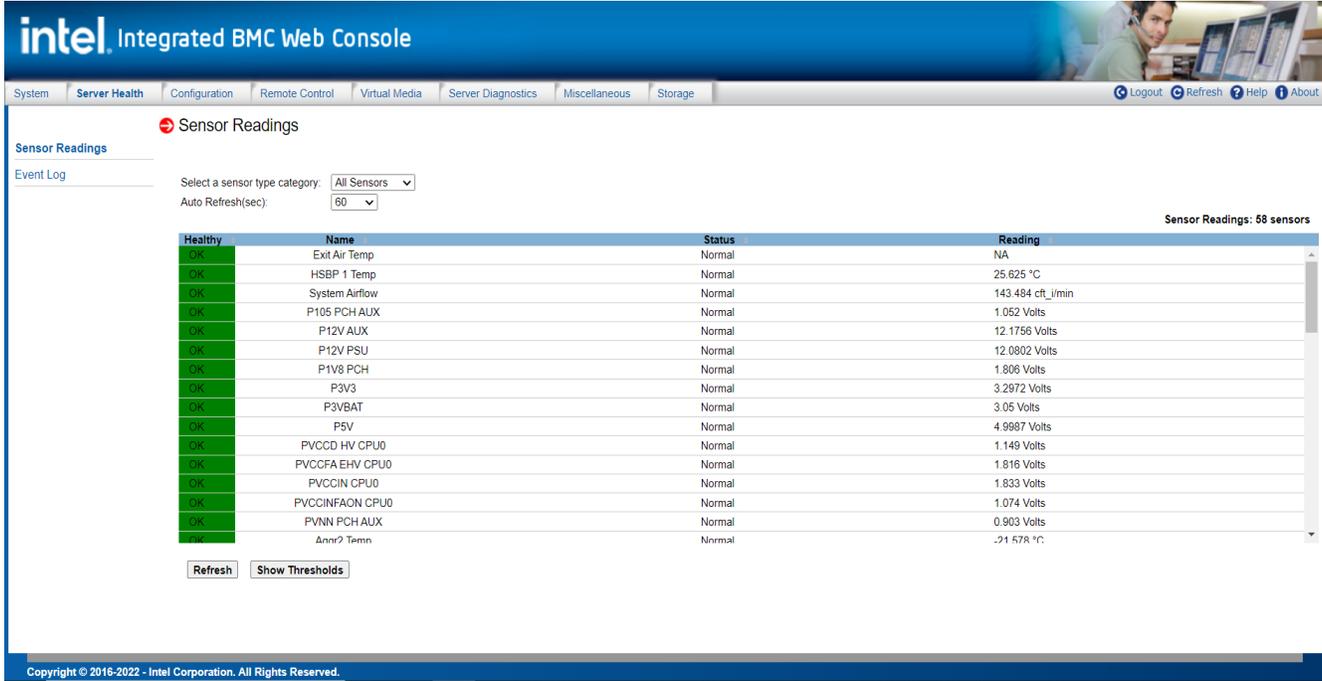


Figure 15. Server Health Sensor Readings Page (Thresholds Not Displayed)

Selecting the “**Show Thresholds**” button on the bottom of the windows will add the programmed threshold information for all monitored sensors to the table (See [Figure 16](#)).

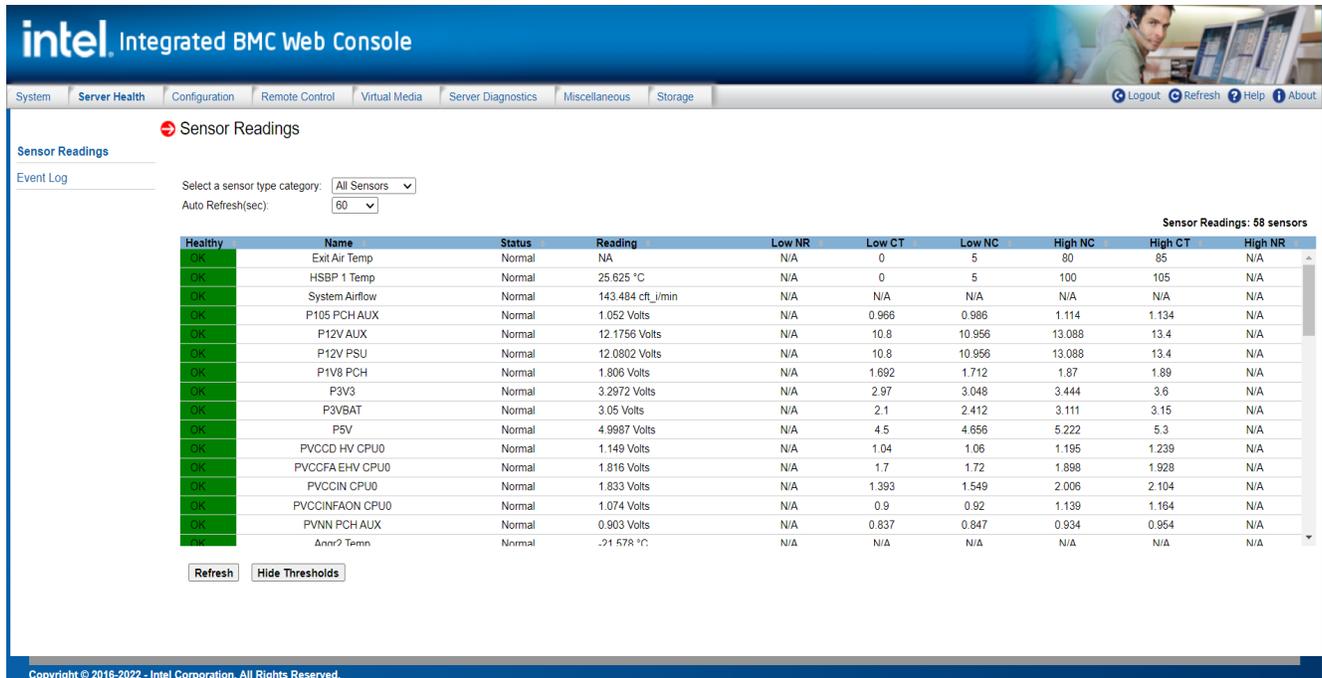


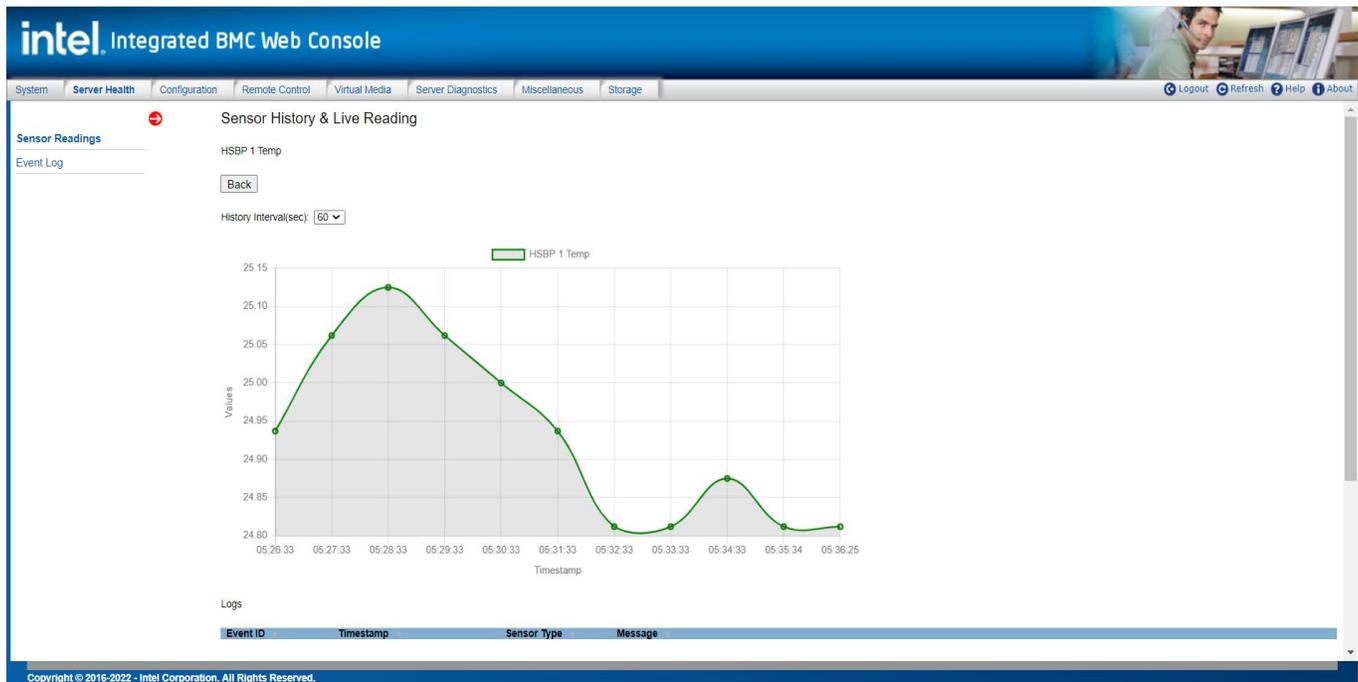
Figure 16. Server Health Sensor Readings Page (Thresholds Displayed)

Table 4 lists the options available in this page

**Table 4. Server Health Sensor Readings Options**

Option	Task
Select a sensor type category	Select the sensor type category to display in the list. The default is to display all sensors.
Auto Refresh (sec)	Select the time (in seconds) to wait between sensor reading updates. Choose 5, 10, 15, 30, 60, 150, 300, or never. The default refresh time is 60 seconds.
Refresh	Click to refresh the selected sensor readings.
Show Thresholds	Click to show the supported threshold assignments: low and high, critical (CT), non-critical (NC) and non-recoverable (NR).
Hide Thresholds	Click to return to the original display, hiding the threshold values.

Selecting a specific sensor from the table will display a new page showing its readings for a specified time interval (See Figure 17). The default time interval is 60 seconds, but can be changed to a different value using the “History Interval(sec)” drop down box.



**Figure 17. Server History & Live Reading**

Table 4 lists the options available on this page.

**Table 5. Server history & Live Reading Options**

Option	Task
Back	Back to sensor reading page.
History Interval (sec)	Select the time (in seconds) to set history interval show in figure. Choose 5, 10, 30, 60. The default value is 60 seconds.

## 5.2.2 Event Log

The Event Log page displays systems events reported by the BMC and saved into a server management event log (See Figure 18). Selecting the “Save Event Log” button will copy the contents of the event log to a file using a JSON format.

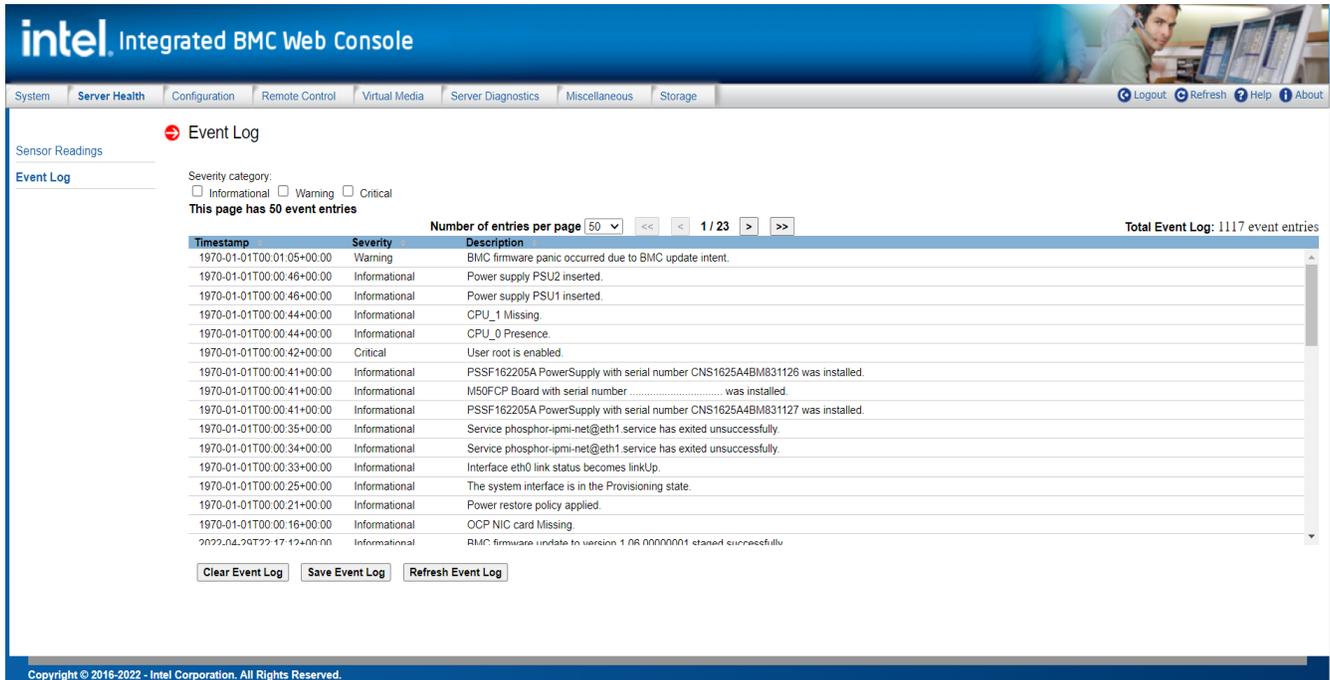


Figure 18. Server Health Event Log Page

Table 6 lists the options available in this page.

Table 6. Server Health Event Log Options

Option	Task
Severity category	Select the severity of events to display in the list. Choose informational, warning, or critical.
Number of entries per page	Specify how many events are displayed per page.
Page selection	Navigate to other pages of recorded events. The selections are first page, previous page, next page, and last page.
Clear Event Log	Clear the event log.
Save Event Log	Save the event log to file.
Refresh Event Log	Refresh the event log.

## 5.3 Configuration Tab

The Configuration tab provides access to secondary page options used to configure various server management features, including: Email Alert, IPv4 and IPv6 networks, VLAN, NTP settings, installing an advanced system management key, SSL certification, users, security settings, sensor customization, system firmware update, system log server configuration, and thermal customization. The following sub-sections provides an overview for each management feature page.

### 5.3.1 Email Alert

The Email Alert page is used to identify system events that should trigger an alert and set the destination to send the alert. Up to two destinations can be selected for each LAN channel (See [Figure 19](#)).

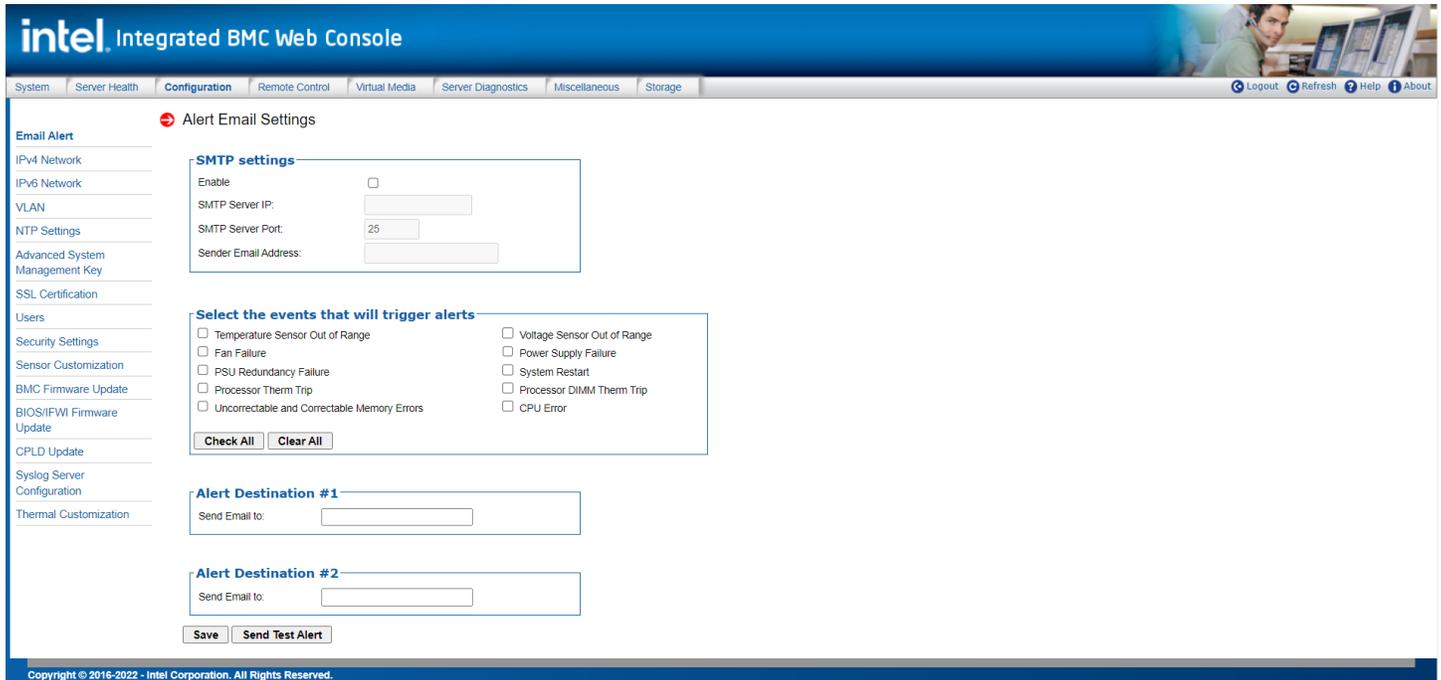


Figure 19. Alerts Page

Table 7 provides a descriptive overview for each configurable page option.

Table 7. Alerts Options

Option	Task
<b>Enable</b>	Enable/Disable SMTP Configuration, default value is unchecked, need to click save button to keep changes.
<b>SMTP Server IP</b>	The IP address of the remote SMTP Mailserver that the Alert email should be sent to, supports host name. <ul style="list-style-type: none"> <li>The IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx".</li> <li>'xxx' ranges from 0 to 255. The first 'xxx' must not be 0.</li> </ul>
<b>SMTP Server Port</b>	The IP port number for which the remote SMTP Mailserver is listening. The default port is 25.
<b>Sender Email Address</b>	The Sender address string is to be put in the "From:" field of outgoing Alert emails. The string should be of the form user@host.domain.tld.
<b>Select the events that will trigger alerts</b>	An alert will be triggered for each selected event.
<b>Check All</b>	Click this option or select all listed events
<b>Clear All</b>	Click this option to clear all listed events
<b>Alert Destination #1/#2</b>	Enter the email address that the alert is to be sent to. Up to two destinations can be selected for each LAN channel.

Option	Task
Save	Click to save any changes made.
Send Test Alerts	Click this option to send a simple test alert message to the configured destination(s).

### 5.3.2 IPv4 Network

The IPv4 Network page is used to configure the IPv4 network settings for the server management LAN interface to the BMC controller. The page includes options to automatically configure the IP address using DHCP (See Figure 20) or to manually enter a static IP Address by entering the required information into the specified fields (See Figure 21).

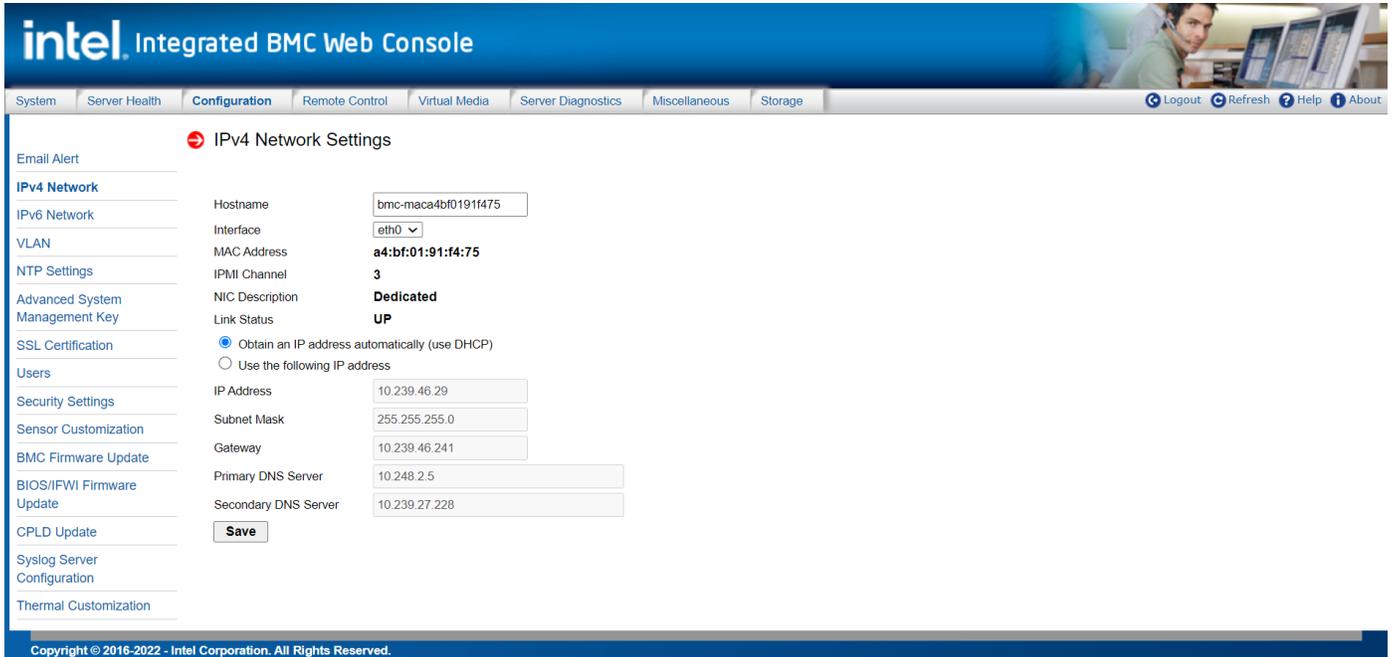


Figure 20. IPV4 Network DHCP Page

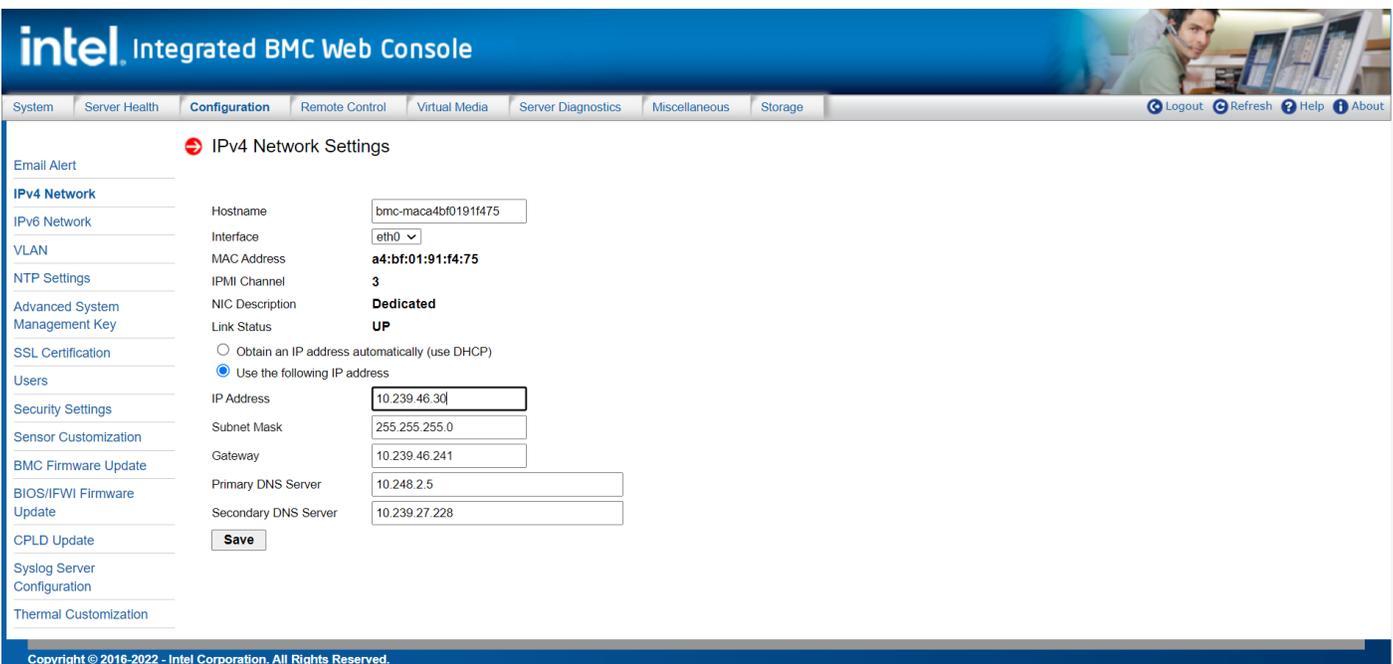


Figure 21. IPv4 Network Static Page

**WARNING:** Each network controller must be on a different subnet than all other controllers used for management traffic.

Table 8 provides a description for all configurable features and input buttons found on the page.

**Table 8. IPv4 Network Settings Options**

Option	Task
<b>Host Name</b>	The hostname is an RFC-1123-compliant string with less than 64 alphanumeric characters. Hyphen characters are allowed as long as the hyphen is not the first or final character in the hostname. The default value is "BMC" + MAC address.
<b>Interface</b>	Select the channel on which to configure the network settings. Lists the LAN channels available for server management. The LAN channels describe the physical NIC connection on the server. All channels are onboard NICs. The Baseboard Mgmt channel is a shared NIC configured for management and shared with the operating system.
<b>MAC Address</b>	The MAC address of the device (read only).
<b>IPMI Channel</b>	IPMI channel number (read only).
<b>NIC Description</b>	NIC dedicated to the BMC / host or shared between the host and BMC of LAN channel(s) (read only).
<b>Link Status</b>	NIC link status of LAN channel(s) (read only).
<b>Obtain an IP address automatically (use DHCP)</b>	Select the option to enable the IPv4 DHCP. IP Address, Subnet Mask, Gateway, and DNS Server input fields are disabled if the "Obtain an IP address automatically (use DHCP)" option is selected.
<b>Use the following IP address</b>	Select the option to configure the static IPv4 address. IP Address, Subnet Mask, Gateway, and DNS Server input fields are enabled to configure if the "Use the following IP address" option is selected.
<b>IP Address</b>	If configuring a static IP, enter an IP address for this channel. <ul style="list-style-type: none"> <li>The IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx".</li> <li>'xxx' ranges from 0 to 255. The first 'xxx' must not be 0.</li> </ul>
<b>Subnet Mask</b>	If configuring a static IP, enter the subnet mask of the device.
<b>Gateway</b>	If configuring a static IP, enter the gateway of the device.
<b>Primary DNS Server</b>	If configuring a static IP, enter the primary DNS server of the device.
<b>Secondary DNS Server</b>	If configuring a static IP, enter the secondary DNS server of the device.
<b>Save</b>	Click to save any changes made.

### 5.3.3 IPv6 Network

The IPv6 Network page is used to configure the IPv4 network settings for the server management LAN interface to the BMC controller (See Figure 22).

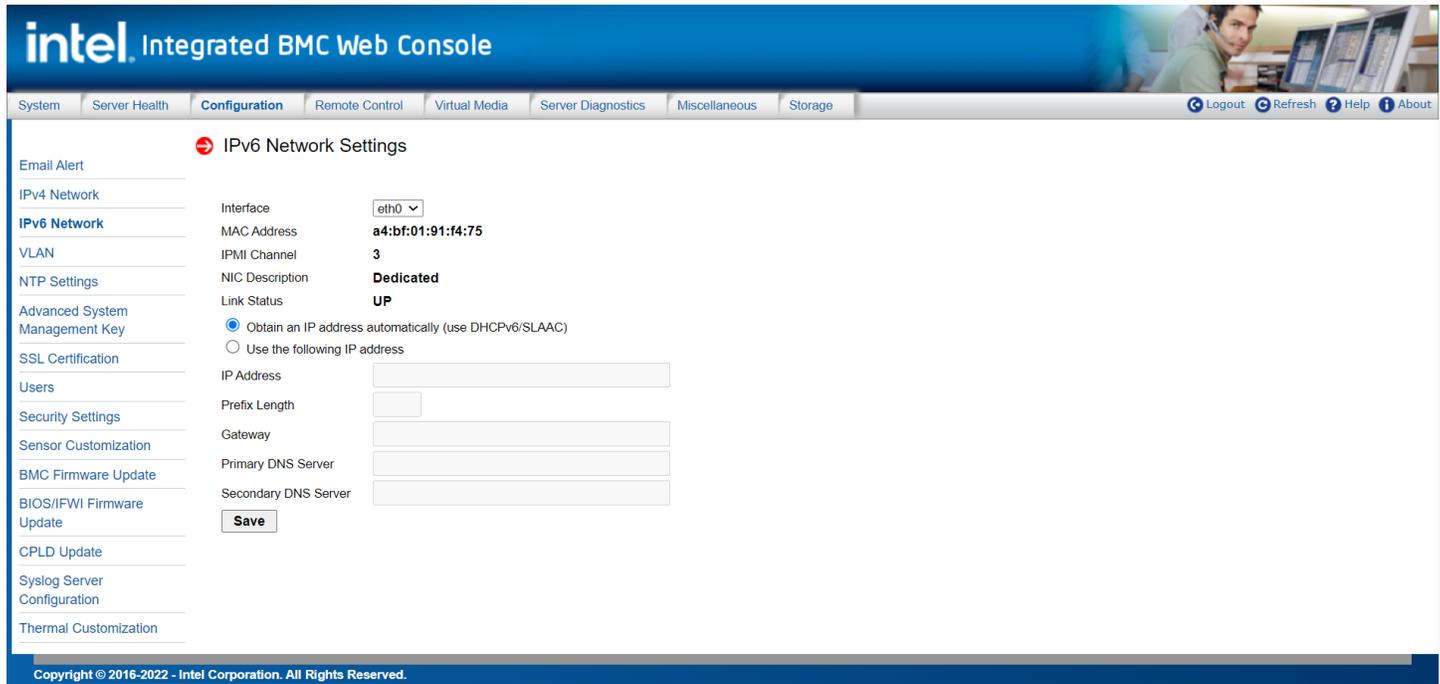


Figure 22. IPv6 Network Page

**WARNING:** Each network controller must be on a different subnet than all other controllers used for management traffic.

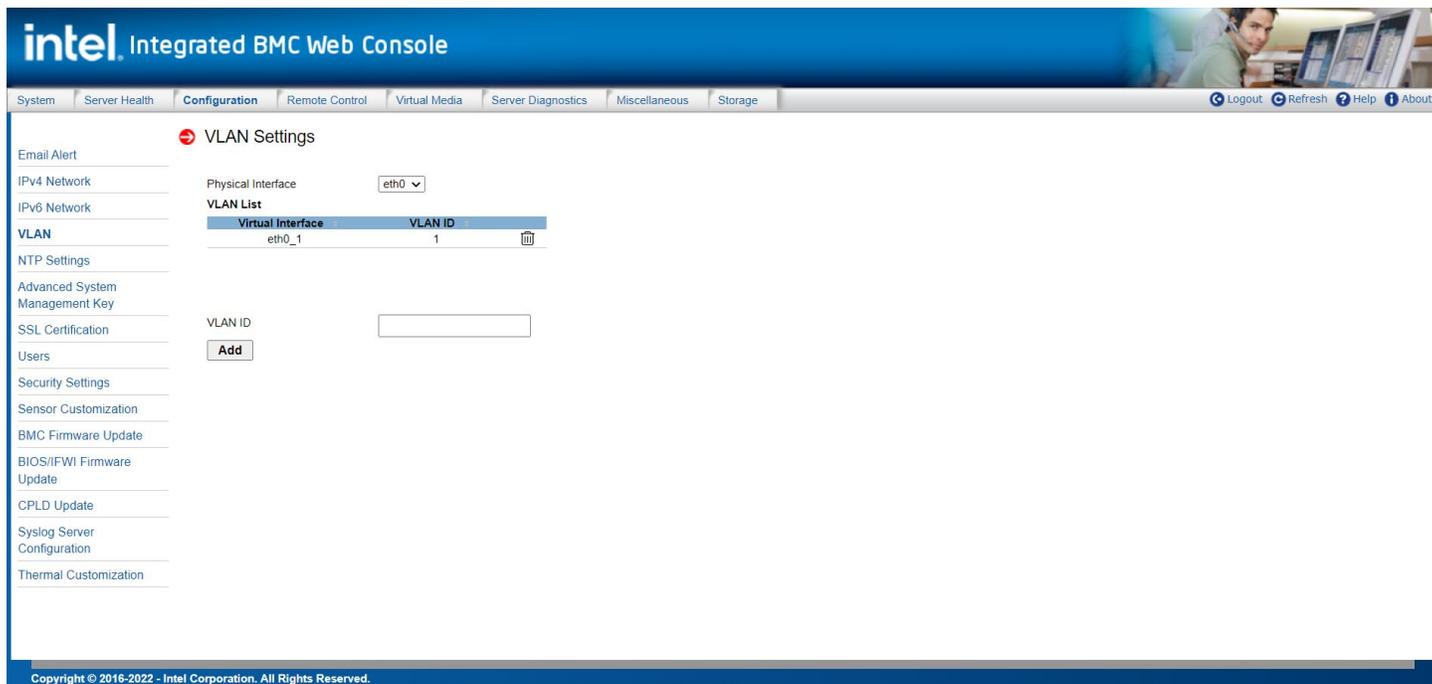
Table 9 provides a description for all configurable features and input buttons found on the page.

Table 9. IPv6 Network Settings Options

Option	Task
<b>Interface</b>	Select the channel on which to configure the network settings. Lists the LAN Channels available for server management. The LAN channels describe the physical NIC connection on the server. All channels are onboard NICs. The Baseboard Mgmt channel is a shared NIC configured for management and shared with the operating system.
<b>MAC Address</b>	The MAC address of the device (read only).
<b>IPMI Channel</b>	IPMI channel number (read only).
<b>NIC Description</b>	NIC dedicated to the BMC / host or shared between the host and BMC of LAN channel(s) (read only).
<b>Link Status</b>	NIC link status of LAN channel(s) (read only).
<b>Obtain an IP address automatically (use DHCP)</b>	Select the option to enable the IPv6 DHCP. IP Address, Prefix, Gateway, and DNS Server input fields are disabled if the "Obtain an IP address automatically (use DHCPv6/SLAAC)" option is selected.
<b>Use the following IP address</b>	Select the option to configure the static IPv6 address. IP Address, Prefix length, Gateway, and DNS Server input fields are enabled to configure if the "Use the following IP address" option is selected.
<b>IP Address</b>	If configuring a static IP, enter an IP address for this channel. <ul style="list-style-type: none"> <li>IPv6 addresses consist of eight 4-digit hexadecimal numbers separated by colons.</li> <li>A "::" can be used for a single sequence of two or more zero fields.</li> </ul>
<b>Prefix Length</b>	If configuring a static IP, enter the routing prefix length.
<b>Gateway</b>	If configuring a static IP, enter the gateway of the device.
<b>Primary DNS Server</b>	If configuring a static IP, enter the primary DNS server of the device.
<b>Secondary DNS Server</b>	If configuring a static IP, enter the secondary DNS server of the device.
<b>Save</b>	Click to save any changes made.

### 5.3.4 VLAN

The VLAN settings page is used to enable and configure the 802.1Q VLAN private network settings on the selected server management Physical Interface (See [Figure 23](#)).



**Figure 23. VLAN Settings Page**

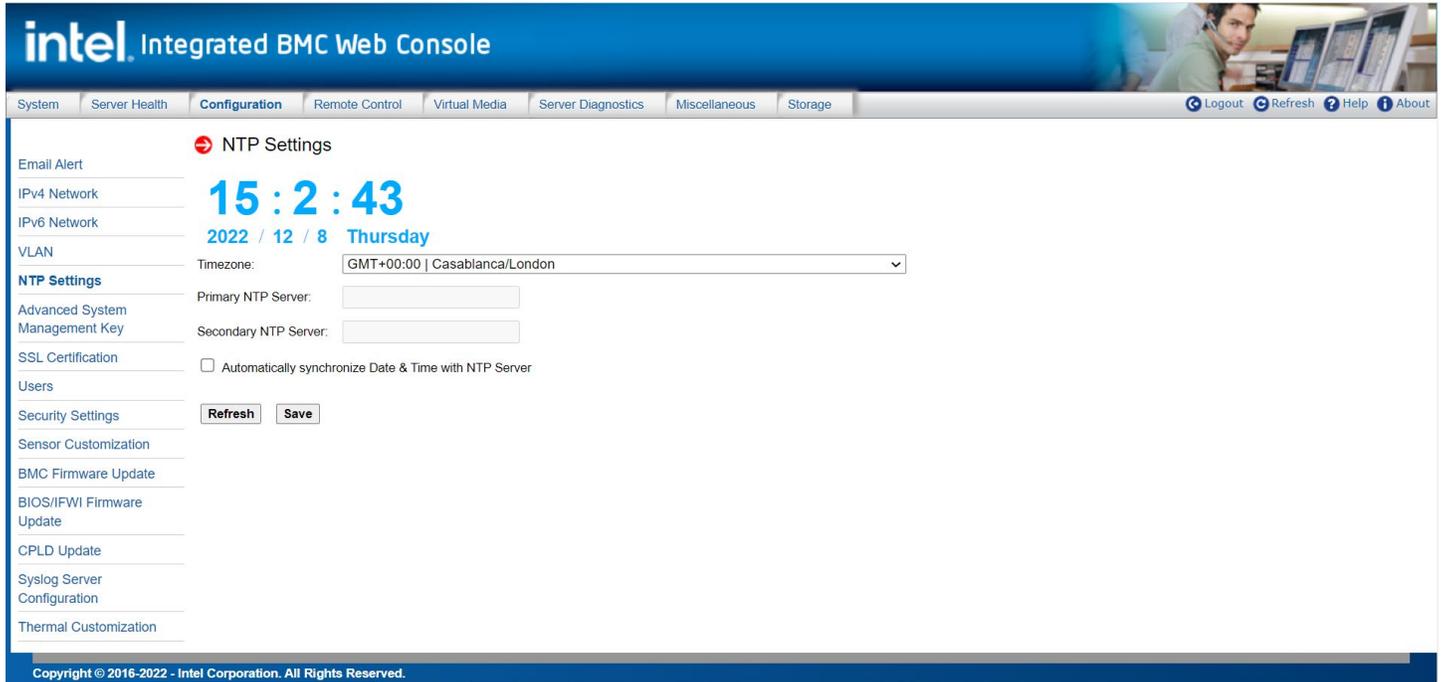
Table 10 provides a description for all configurable features and input buttons found on the page.

**Table 10. VLAN Settings Options**

Option	Task
<b>Physical Interface</b>	Select the channel on which to configure the network settings. Lists the LAN channels available for server management. The LAN channel describes the physical NIC connection on the server. All channels are onboard NICs.
<b>VLAN ID</b>	Specify the VLAN ID to use. Values are from 1 to 4094. Only one ID can be used at a time.
<b>Add</b>	Click to add a new VLAN.
<b>Delete</b>	Click to delete a VALN.

### 5.3.5 NTP – Network Time Protocol

The NTP Settings page is used to change the devices current date and time settings. This page can be used to configure either date and time or the NTP server settings for the device. See [Figure 24](#) for details.



**Figure 24. NTP Settings Page**

Table 11 provides a description for all configurable features and input buttons found on the page.

**Table 11. Date and Time Options**

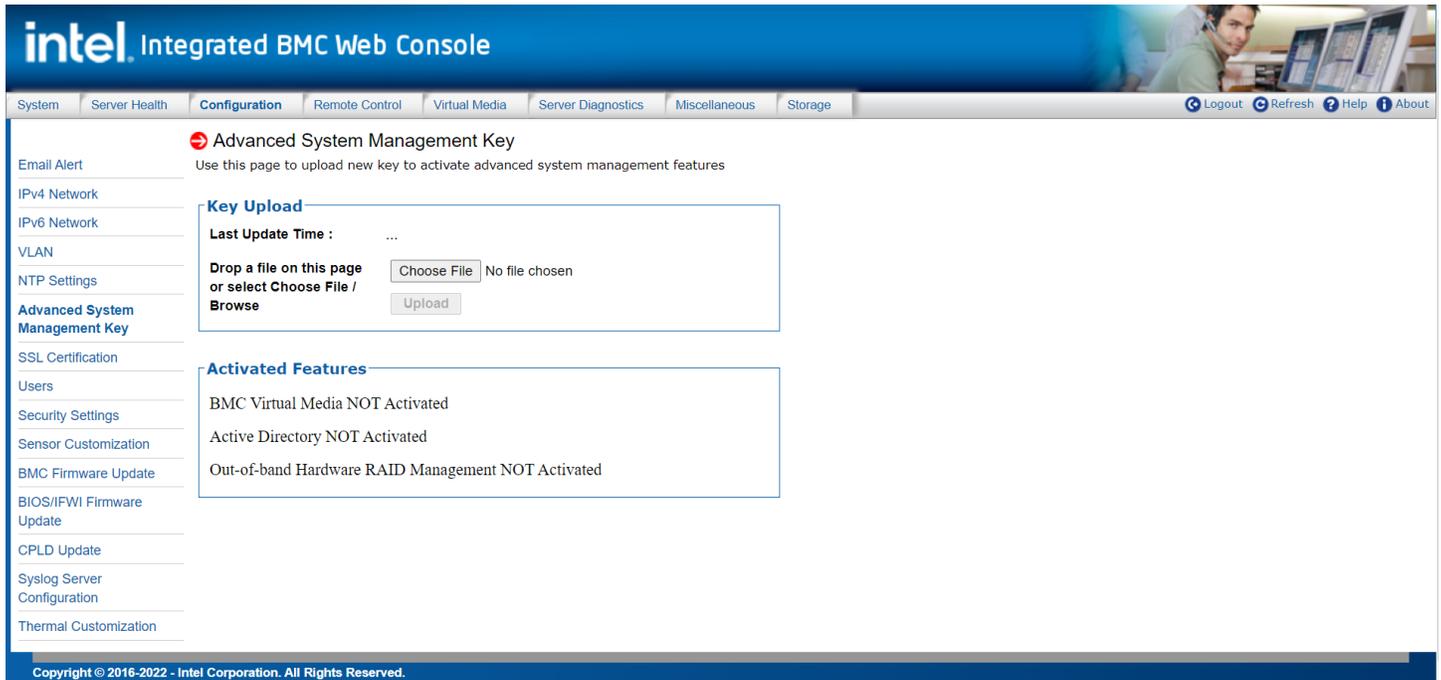
Option	Task
<b>Timezone</b>	Time zone contains the UTC offsets for NTP server, which can be used to display the exact local time.
<b>Primary NTP Server</b>	Specify the primary NTP servers for the device. NTP server fields support the following: <ul style="list-style-type: none"> <li>• IP address (both IPv4 and IPv6 format).</li> <li>• FQDN (fully qualified domain name) format.</li> <li>• FQDN value ranges from 1 to 128 alphanumeric characters.</li> </ul>
<b>Secondary NTP Server</b>	Specify the secondary NTP servers for the device. NTP server fields support the following: <ul style="list-style-type: none"> <li>• IP address (both IPv4 and IPv6 format).</li> <li>• FQDN format.</li> <li>• FQDN value ranges from 1 to 128 alphanumeric characters.</li> </ul>
<b>Automatically synchronize</b>	Check this option to automatically synchronize date and time with the NTP server.
<b>Refresh</b>	Reload the current date and time settings.
<b>Save</b>	Click to save any changes made.

**Notes:**

- Secondary NTP server is an optional field. If the primary NTP server is unavailable or not working, then the secondary NTP server is tried.
- Once the NTP settings configuration is saved successfully, then the system automatically re-directs the user to the web login page.

### 5.3.6 Advanced System Management Key

The Advanced System Management Key page is used to upload a new advanced system management key and show the current activated features (See [Figure 25](#)).



**Figure 25. Advanced System Management Key Page (uninstalled)**

Table 12 provides a description for all configurable features and input buttons found on the page.

**Table 12. Advanced System Management Key Options**

Option	Task
<b>Last Upload Time</b>	Show the last time that the advanced system management key was uploaded (read only).
<b>Choose File</b>	Choose the file to upload.
<b>Upload</b>	Upload the advanced system management key to the BMC for the update to start.
<b>Activated Features</b>	Lists the activation status of the advanced functions before and after the advanced system management key is uploaded.

For more information see [Appendix A Advanced Management License Key – Order, Registration, and Installation](#).

Once the Advanced System Management key is installed, it will show as “**Activated**” on the information screen of the **System** tab (See [Figure 26](#)).

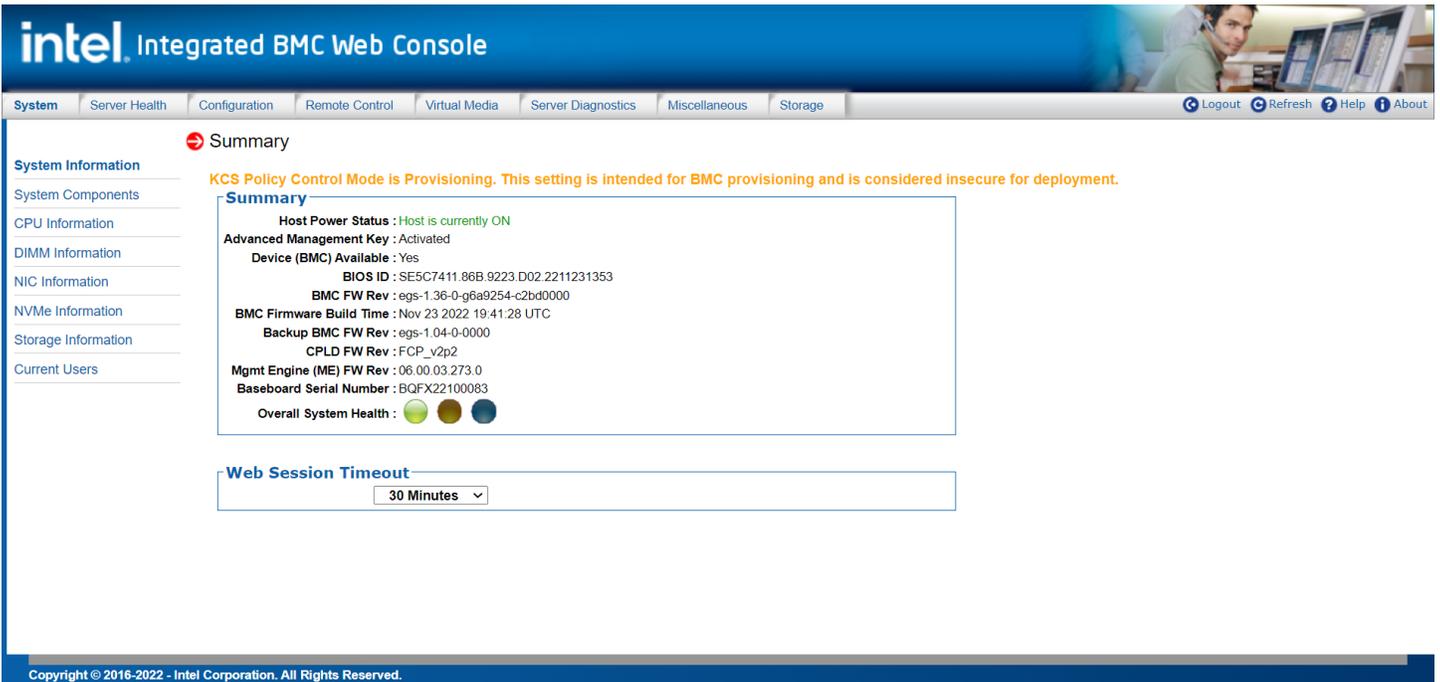


Figure 26. Advanced System Management Key Page (installed)

### 5.3.7 SSL Certification

This page is used to upload certificate to BMC, the certificates include server certificate and CA certificate. Server certificate can only be replaced, only one Server certificate at same time, deleting server certificate is not supported. CA certificate can be added and have multiple CA certificate at same time. See Figure 27, Figure 28 for details.

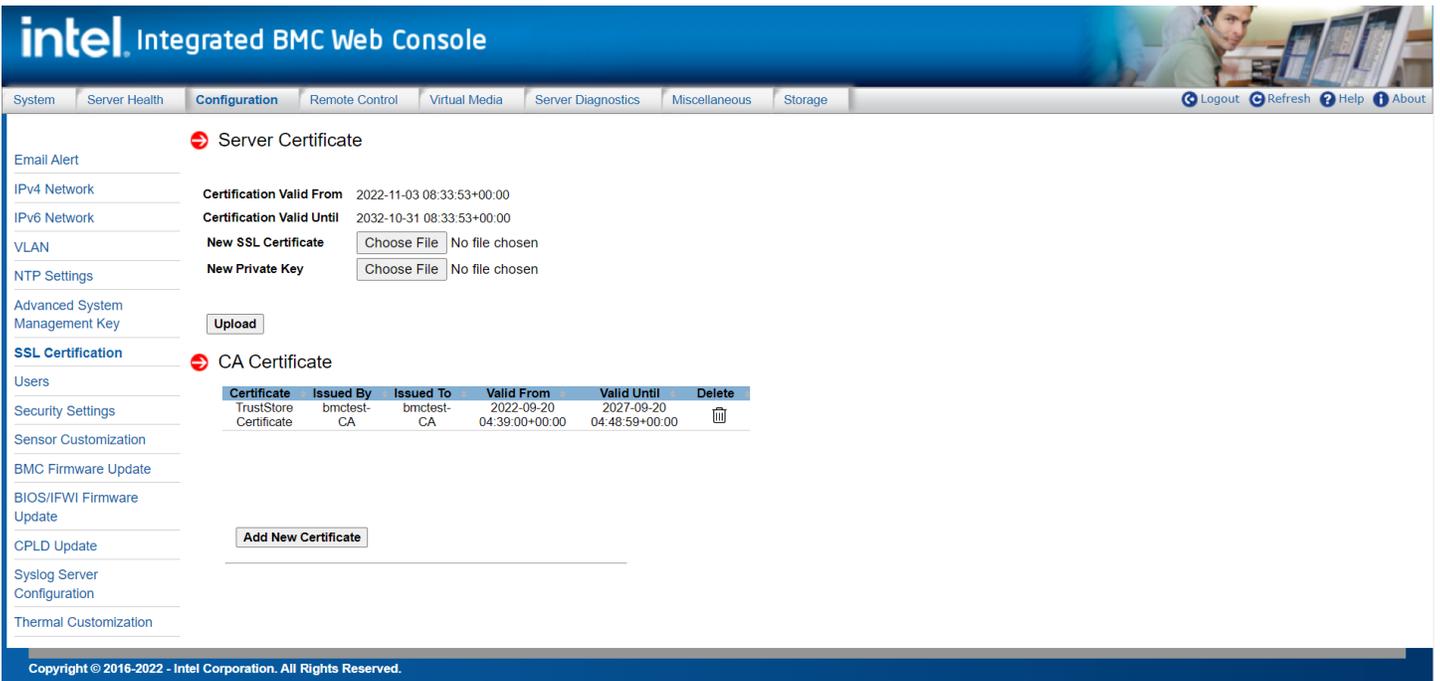


Figure 27. SSL Certification Page

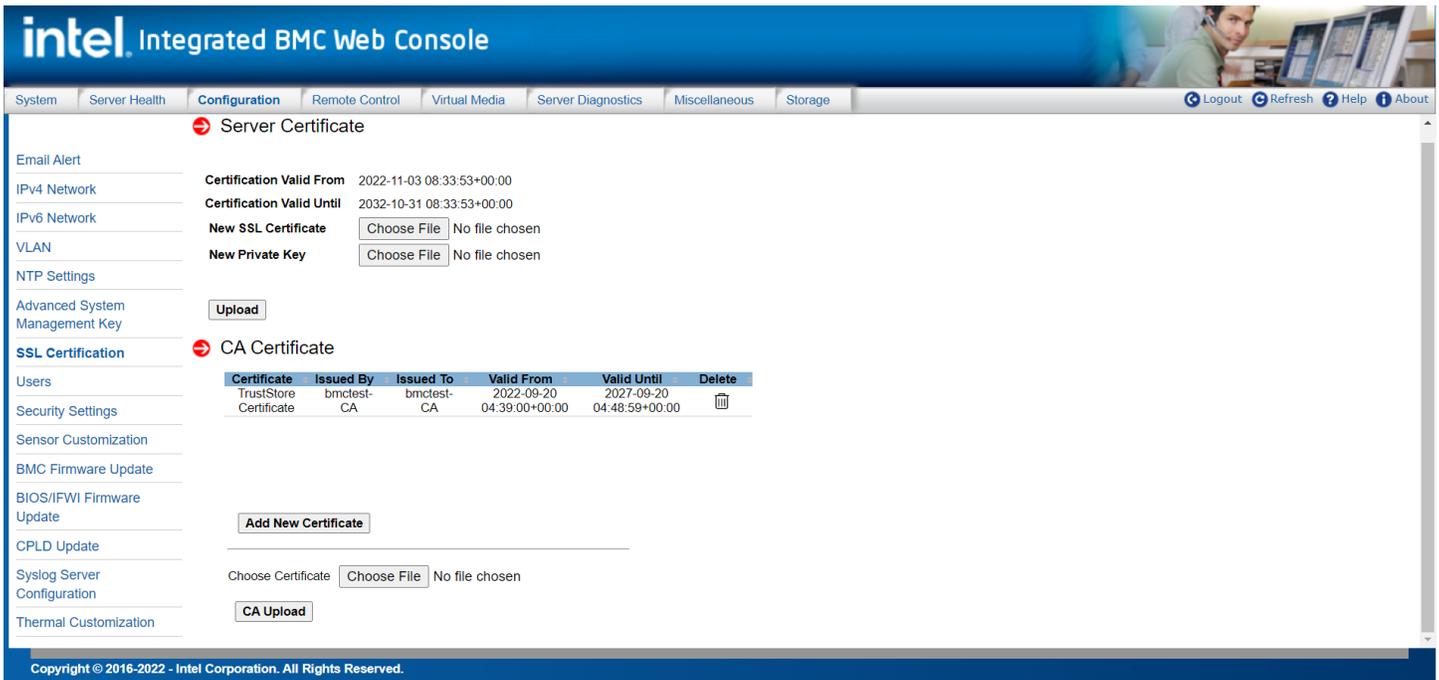


Figure 28. SSL Certification Page (Add New CA Certificate)

Table 13 provides a description for all configurable features and input buttons found on the page.

Table 13. SSL Certificate Options

Option	Task
<b>Choose File (New SSL Certificate)</b>	Select SSL Certificate file to upload.
<b>Choose File (New Private Key)</b>	Select Private Key file to upload
<b>Upload</b>	Click to upload a new server certificate file to the BMC.
<b>Add New Certificate</b>	Click the <b>Add New Certificate</b> button to show the CA upload buttons.
<b>Choose File (New CA Certificate file)</b>	Select CA certificate file to upload.
<b>CA Upload</b>	Click to upload a new CA certificate file to the BMC.
<b>Delete</b>	Click the <b>Delete</b> button in the CA certificate table to delete the individual certificate.

### 5.3.8 Users

The Users page lists all configured users. Information displayed for each User includes: User ID, User Name, User Status, and their Network Privilege designation (See Figure 29).

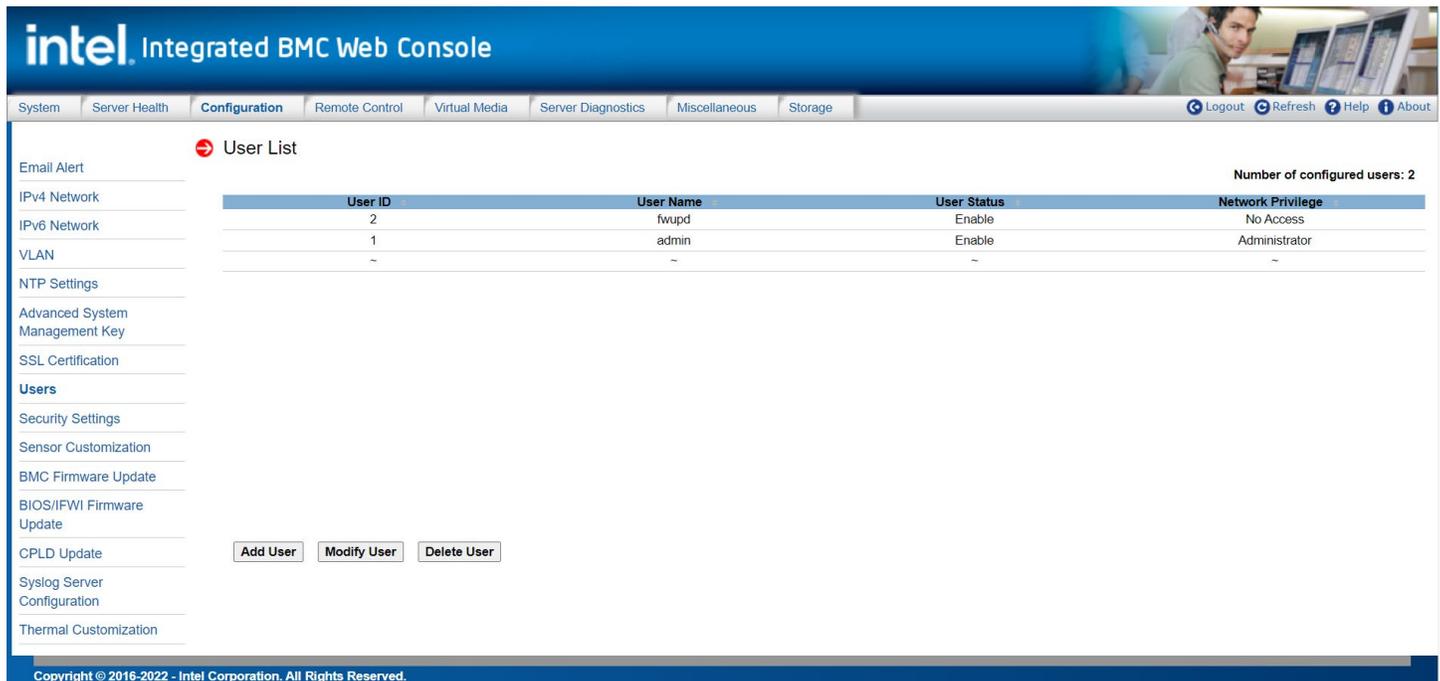


Figure 29. User List Page

This page also provides the options to add, modify, and delete users.

To add a user, select the empty line in the list and click the “Add User” button. An Add New User page will open where the user information can be entered (See Figure 30).

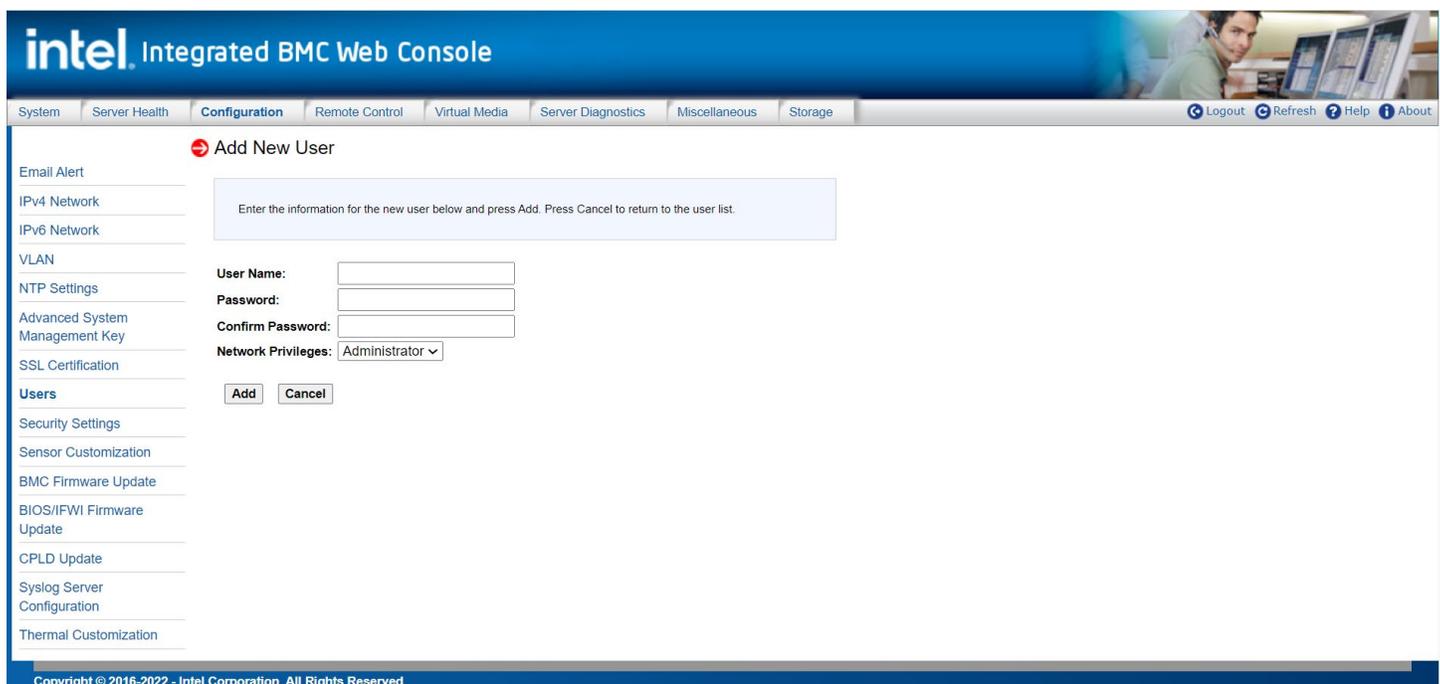
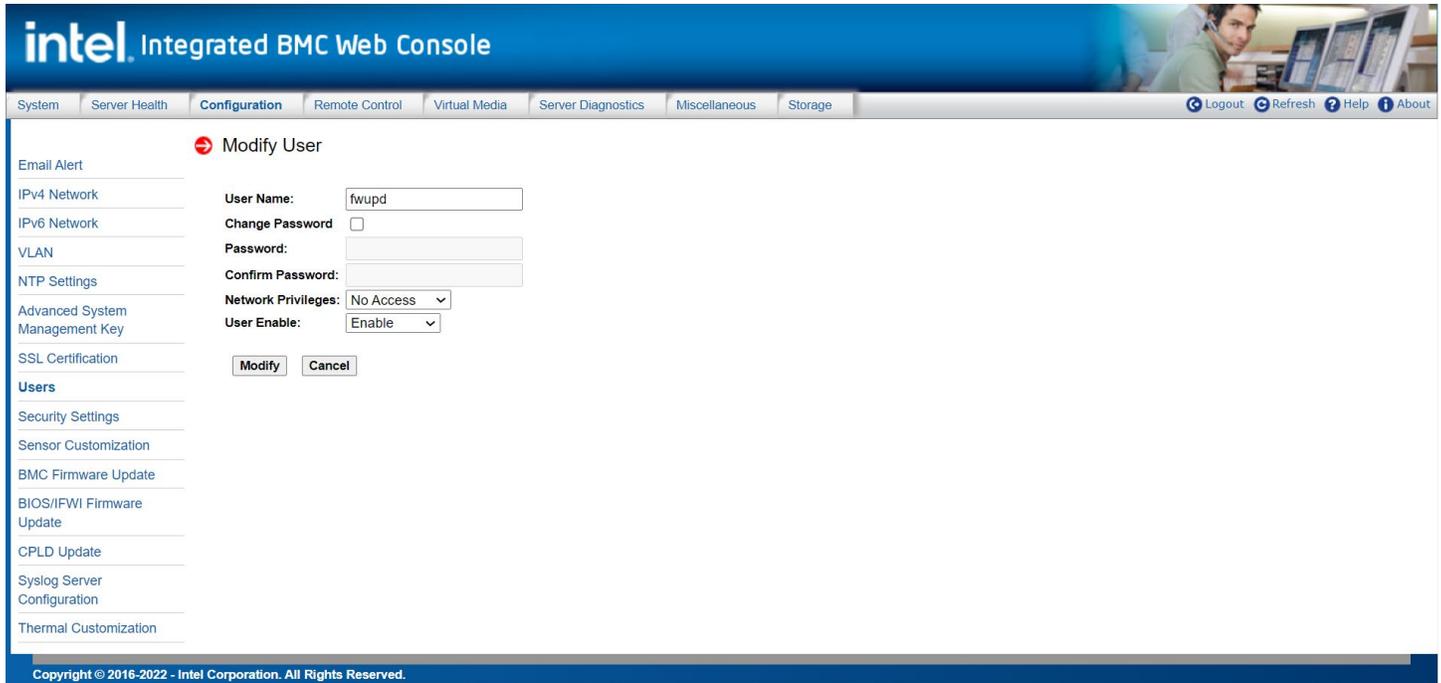


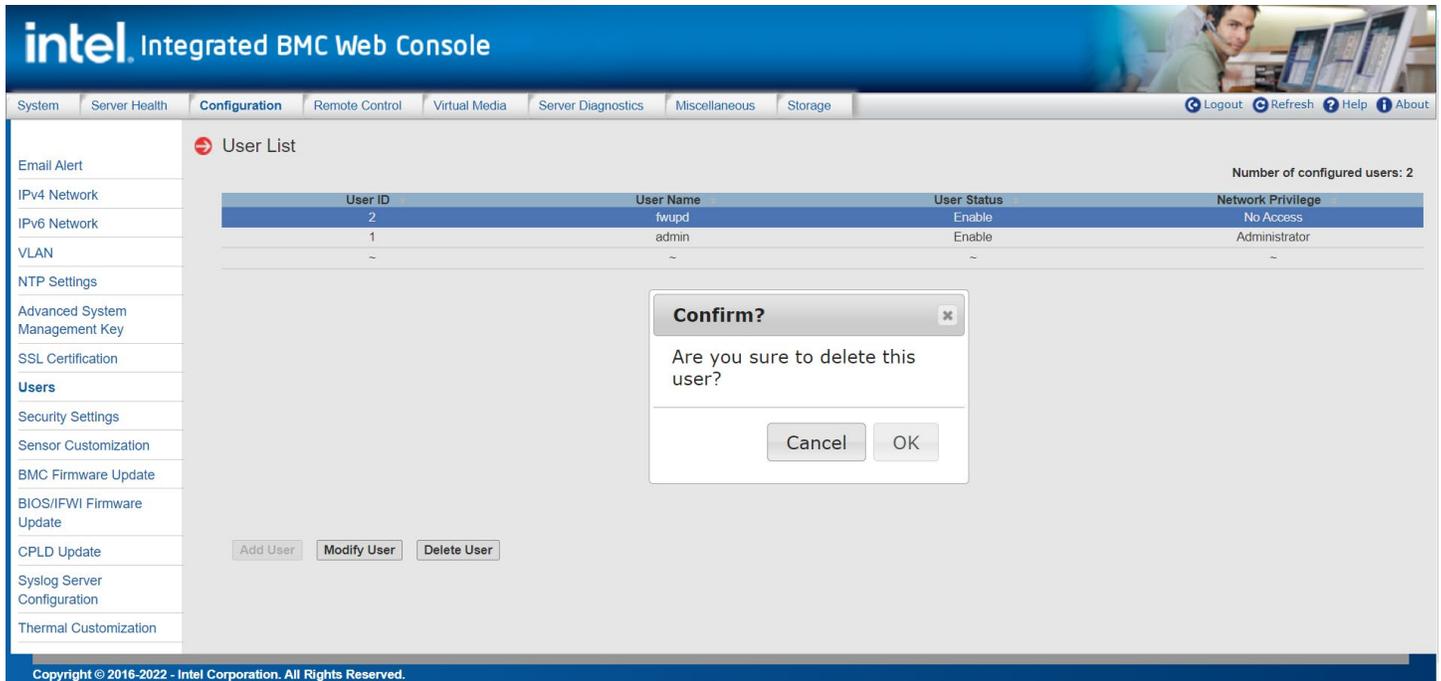
Figure 30. Add New User Page

To modify a user, select a user in the list and click the **“Modify User”** button. A Modify User page will open where the information of the selected user can be changed (See [Figure 31](#)).



**Figure 31. Modify User Page**

To delete a user, select the user in the list and click the **“Delete User”** button. A pop-up box will appear asking for confirmation to delete the selected user (See [Figure 32](#)).



**Figure 32. Delete User Page**

### 5.3.9 Security Settings

The Security Settings page is used to view and modify the following security settings: KCS policy control mode, host interface, login attempt, port settings, password rules, and optional network services (See [Figure 33](#)).

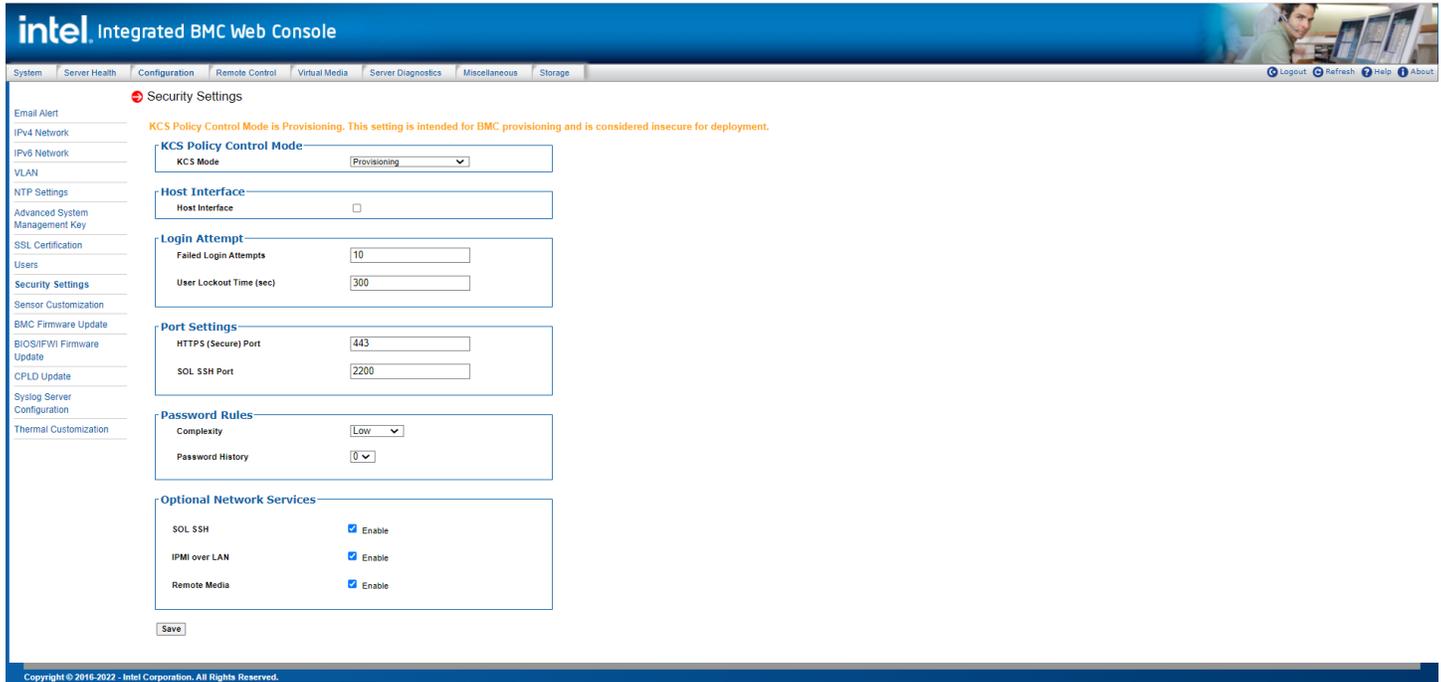


Figure 33. Configuration Security Settings Page

Table 14 provides a description for all configurable features and input buttons found on the page.

Table 14. Configuration Security Settings Options

Option	Task
<b>KCS Mode</b>	<p>KCS policy control modes allow an authenticated BMC administrative user to control the level of protection from IPMI commands executed over the KCS channels. Within this generation of BMC firmware, three different KCS policy control modes are supported:</p> <ul style="list-style-type: none"> <li>• <b>Provisioning</b> – This configuration setting is intended for normal IPMI-compliant communications between the host operating system and the BMC. This mode should be used when provisioning the BMC configuration for deployment.</li> <li>• <b>Provisioned Host Disabled</b> – This configuration setting disables the IPMI KCS command interfaces between the host operating system and the BMC. This is a configuration that does not comply with IPMI and impacts the operation of the server management software running on the host operating system. This mode only applies to the IPMI commands over the KCS interfaces and does not apply to the authenticated network interfaces to the BMC.</li> <li>• <b>Provisioned Host Allowlist</b> – This configuration setting enables the use of an access control list by the BMC firmware that allows applications executing on the host operating system to have access to a limited set of IPMI commands using the KCS interfaces. This is a configuration that does not comply with IPMI and may impact the operation of the server management software running on the host operating system. This mode only applies to the IPMI commands over the KCS interfaces and does not apply to the authenticated network interfaces to the BMC.</li> </ul>
<b>Host Interface</b>	Enable/disable host interface for eth2.
<b>Failed Login Attempts</b>	Input the allowed number of failed login attempts. This is the number of failed login attempts a user is allowed before being locked out. Zero means no lockout. Failed login attempts should be from 0 to 255. The default is 3 attempts.
<b>User Lockout Time (sec)</b>	Set the time in seconds that the user is locked out before being allowed to log in again. Zero means that user lockout time is disabled. If a user is automatically disabled due to the bad password threshold, the user remains disabled until re-enabled via the <code>Set User Access</code> command. User lockout time should be from 0 to 65535 seconds. The default is 60 seconds.

Option	Task
<b>HTTPS (Secure) Port</b>	Set the port used for HTTPS web sessions (default: 443). Changing this setting immediately terminates all current web sessions.
<b>SOL SSH Port</b>	Set the port used for serial-over-LAN secure socket shell sessions.
<b>Complexity</b>	Set complexity password level: medium, high, or low.
<b>Password History</b>	For security considerations, the feature of password history (0–5) helps to avoid setting a password that is duplicate with one used earlier.
<b>SOL SSH</b>	Enable/disable the SOL SSH service.
<b>IPMI over LAN</b>	Enable/disable the RMCP/RMCP+ service.
<b>Remote Media</b>	Enable/disable the virtual media service.
<b>Save</b>	Click to save any changes.

### 5.3.9.1 Integrated BMC Web Console Access under KCS Provisioned Host Allowlist/Provisioned Host Disabled Modes

Access to most of the Integrated BMC Web Console contents is allowed across all KCS modes, except for Web Console page options that are limited to conditional access when the KCS mode is set to Provisioned Host Disabled mode or Provisioned Host Allowlist mode

#### KCS Policy Control Mode – Provisioned Host Disabled

This configuration setting disables the IPMI KCS command interfaces between the host operating system and the BMC. This is a configuration that is non-compliant with IPMI that impacts the operation of the server management software running on the host operating system. This only applies to the IPMI commands over the KCS interfaces and does not apply to the authenticated network interfaces to the BMC.

#### KCS Policy Control Mode – Provisioned Host Allowlist

This configuration setting enables the use of an access control list by the BMC firmware that allows applications executing on the host operating system to have access to a limited set of IPMI commands using the KCS interfaces. This is a configuration that is non-compliant with IPMI and may impact the operation of the server management software running on the host operating system.

- **Server Power Control page** – Power On Server/**Force-enter BIOS Setup** option is grayed out when KCS = Provisioned Host Disabled.
- **Server Power Control page** – Reset Server/**Force-enter BIOS Setup** option is grayed out when KCS = Provisioned Host Disabled.

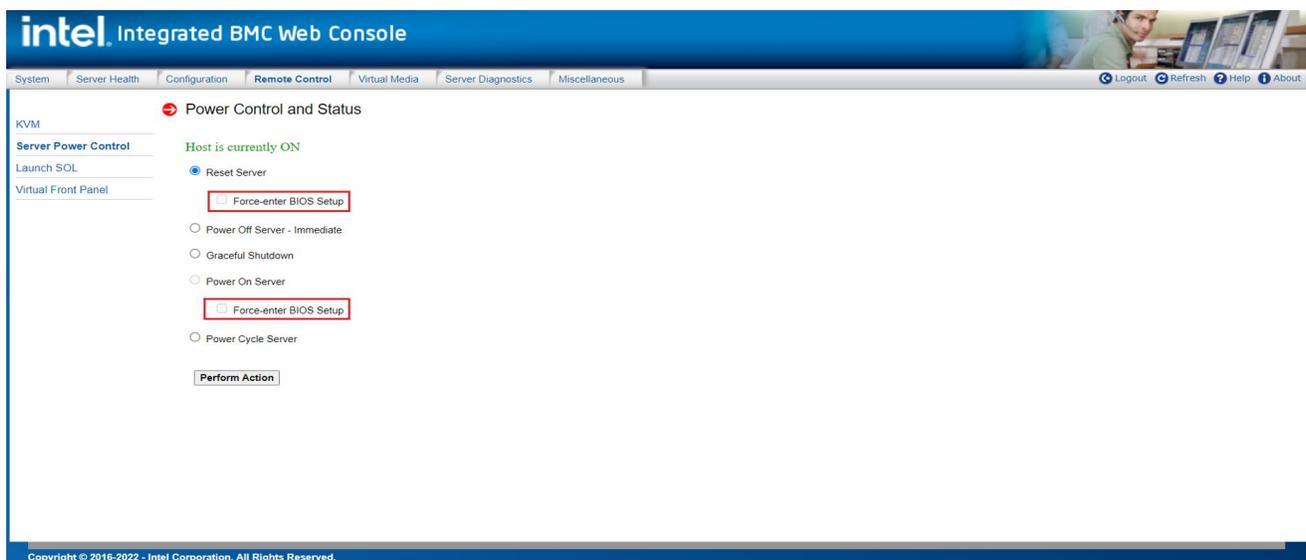
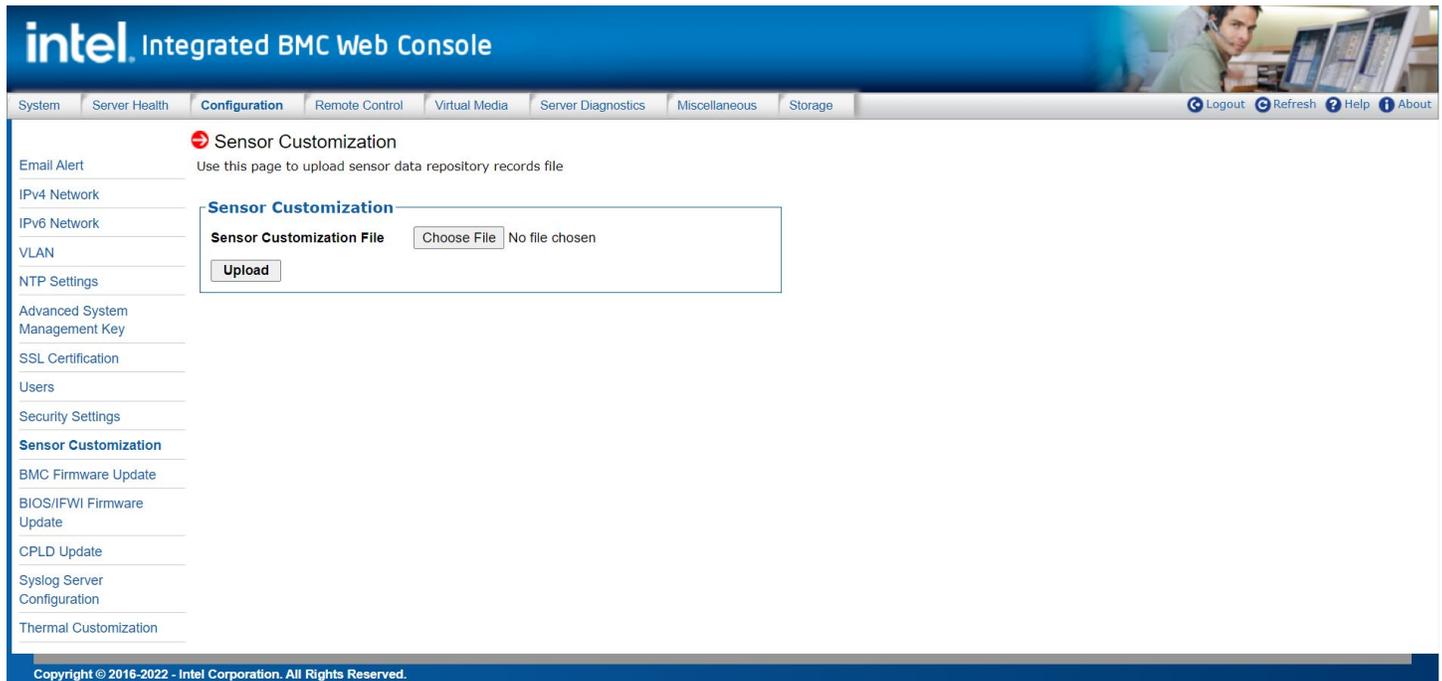


Figure 34. Server Power Control Page

### 5.3.10 Sensor Customization

The Sensor Customization page is used to upload a sensor data repository (SDR) records file to the BMC. The file is used to load customized sensor information for both existing monitored sensors as well as sensors supported by third party add-in cards (See [Figure 35](#)).



**Figure 35. Sensor Customization Page**

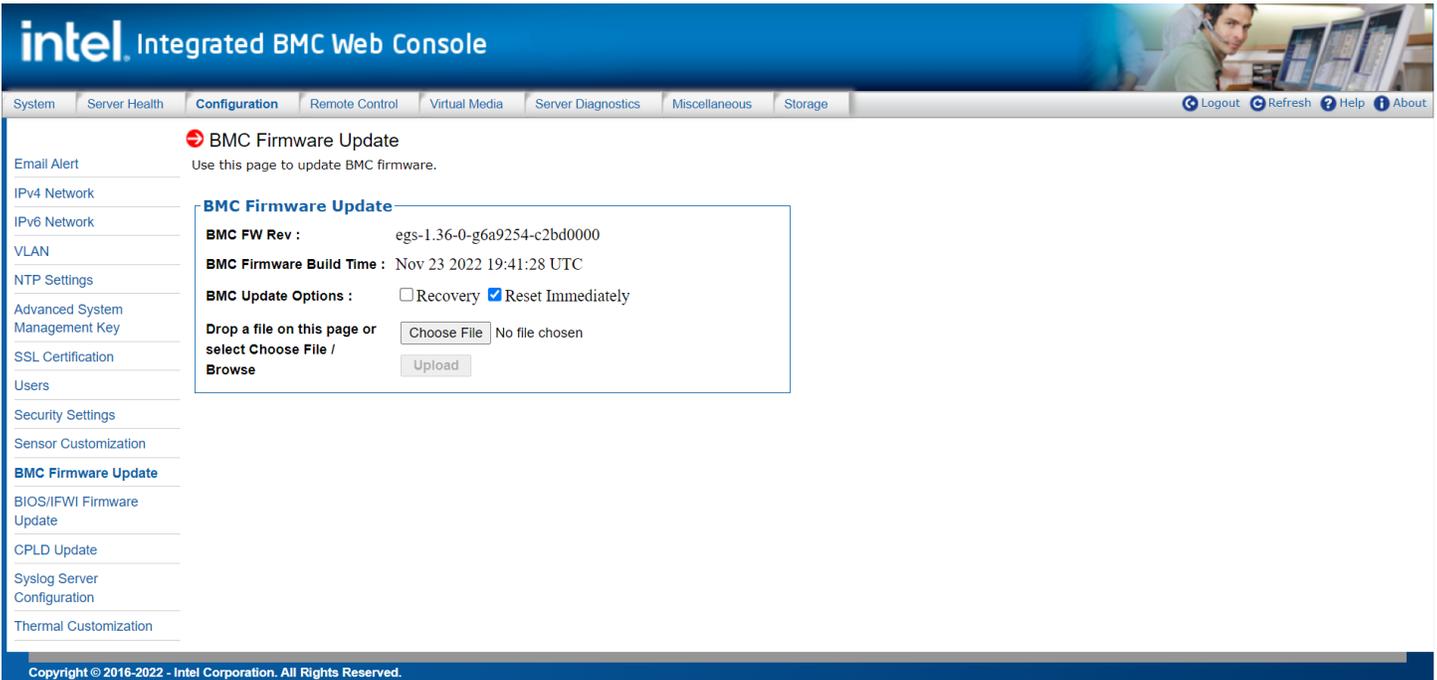
[Table 15](#) provides a description for all configurable features and input buttons found on the page.

**Table 15. Sensor Customization Options**

Option	Task
<b>Sensor Customization File</b>	Click the <b>Choose File button</b> to select the sensor data record JSON file to upload.
<b>Upload</b>	Click to upload file to the BMC.

### 5.3.11 BMC Firmware Update

The BMC Firmware Update page is used to upload new BMC firmware images for an online-update of the BMC firmware (See [Figure 36](#)).



**Figure 36. BMC Firmware Update Page**

After a BMC firmware file has been selected or dropped on to the page, and the **“Upload”** option has been selected, the BMC will begin the update process. An upload progress bar will appear on the page.

The update process can take several minutes to complete. When finished, the BMC will restart to run the new firmware version. Depending on if **“Reset Immediately”** is checked, BMC restart will happen immediately, or on next host DC cycle. Progress is reported up until the time of the restart, after which it takes a couple of minutes for the embedded web server to start responding again. All web sessions are terminated with a BMC restart. Users must log in again to verify that the firmware update was successful.

Table 16 provides a description for all configurable features and input buttons found on the page.

**Table 16. BMC Firmware Update Options**

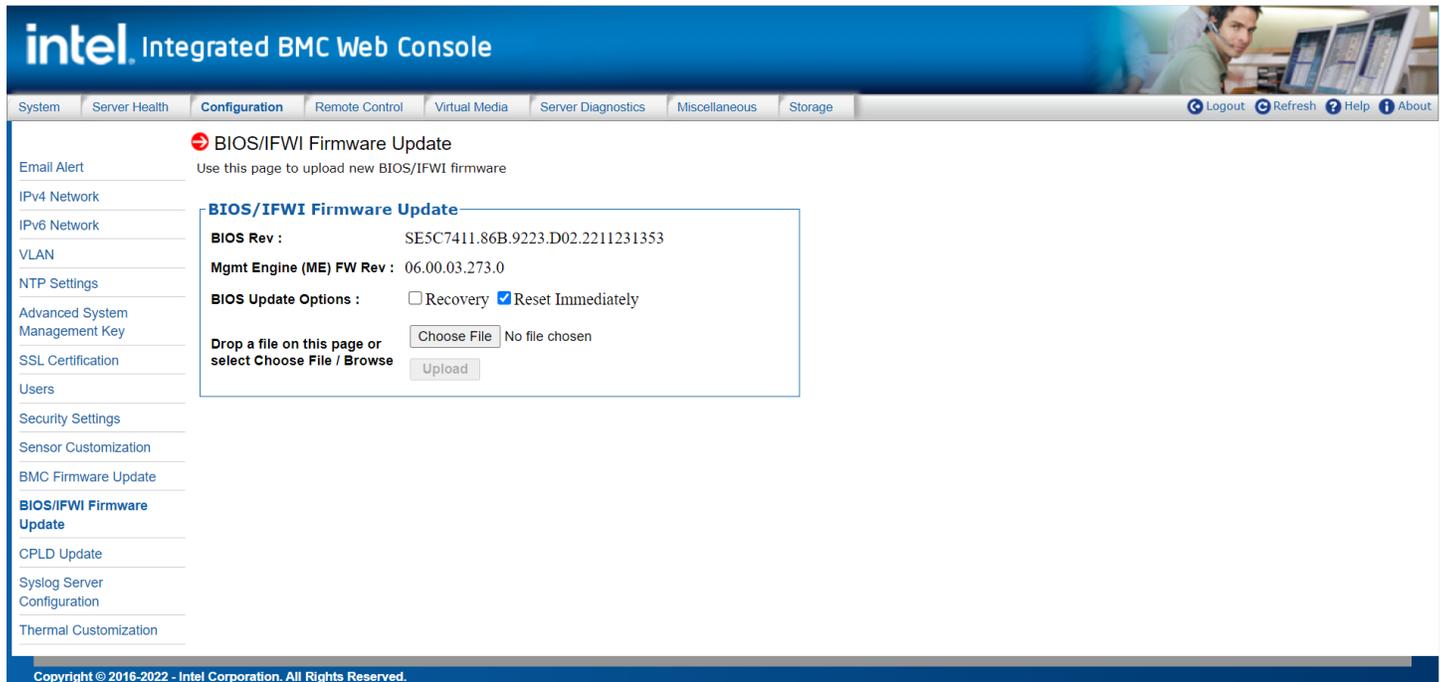
Option	Task
<b>BMC FW Rev</b>	Displays the current firmware version (read only).
<b>BMC Firmware Build Time</b>	Displays the firmware build time (read only).
<b>BMC Update Options</b>	<ul style="list-style-type: none"> <li>• Recovery Select this option to update both the primary and recovery regions of the BMC firmware.</li> <li>• Reset Immediately Select this option to reset the system immediately after the firmware update has completed.</li> </ul>
<b>Drop a file on this page or select Browse...</b>	Use this option to browse for a file to upload or to drop a new firmware image on to the page.
<b>Upload</b>	Upload the BMC firmware update image file to the BMC for the update to start.

**Notes:**

- By default, the BMC Update option **“Reset Immediately”** is unchecked, allowing other operations to be performed after the firmware image is uploaded successfully. With this option the system must be rebooted to load and check the new firmware.
- By selecting the **“Reset Immediately”** update option, the BMC will automatically reset and load the new firmware directly after the BMC updated has completed.

### 5.3.12 BIOS/IFWI Firmware Update

The BIOS/IFWI Firmware Update page is used to upload and update the BIOS/IFWI firmware (See [Figure 37](#)).



**Figure 37. BIOS/IFWI Firmware Update Page**

After a new image file as been selected or dropped onto the page, and the **“Upload”** button has been selected, the web service will begin the update process which may take several minutes to complete.

If the BIOS update option **“Reset Immediately”** is selected, the system will automatically reboot directly after the update process has completed. Login to the web console to verify that the BIOS/IFWI firmware update was successful.

If the BIOS update option **“Reset Immediately”** is not selected, the system must be manually rebooted after the update process has completed. . Login to the web console to verify that the BIOS/IFWI firmware update was successful

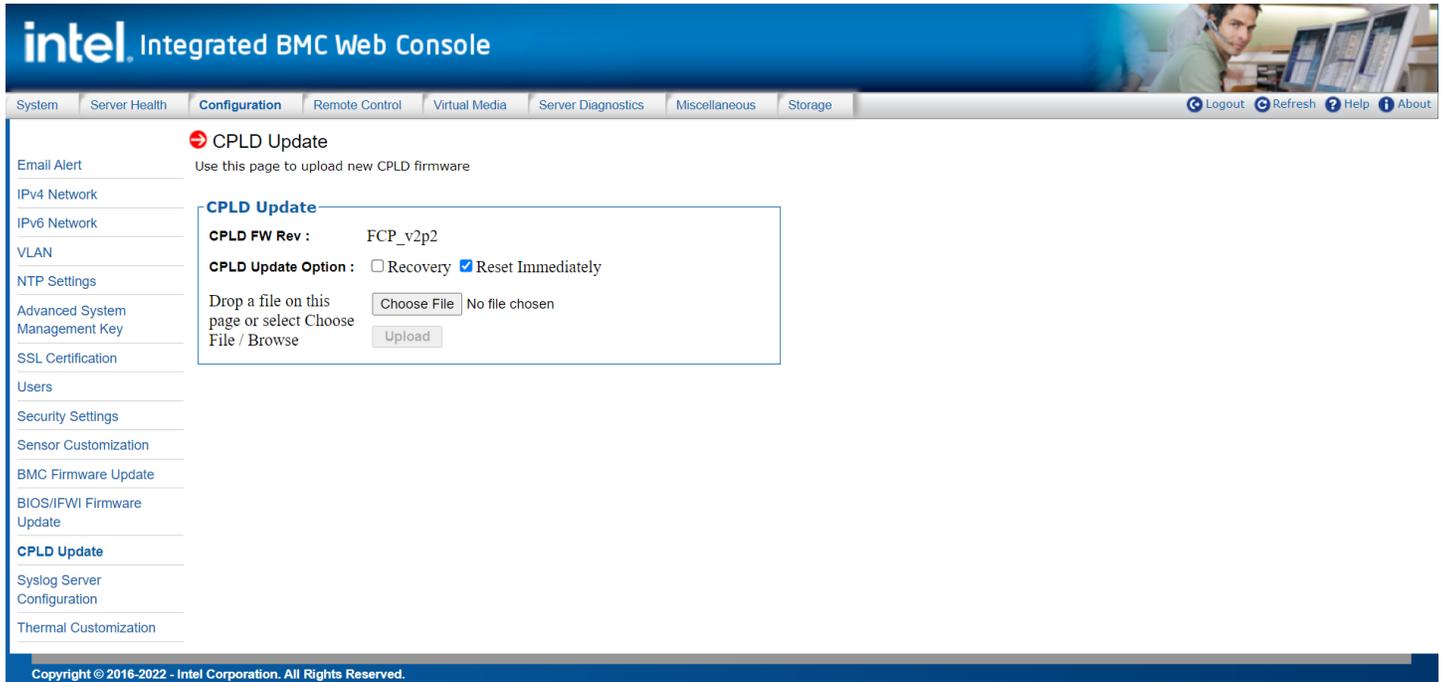
[Table 17](#) provides a description for all configurable features and input buttons found on the page.

**Table 17. BIOS/ME Firmware Update Options**

Option	Task
<b>BIOS Rev</b>	Display the current BIOS version (read only).
<b>Mgmt Engine (ME) FW Rev</b>	Display the current ME firmware version (read only).
<b>BIOS Update Option</b>	<ul style="list-style-type: none"> <li>• <b>Recovery.</b> Select this option so the backup region of the current BIOS is updated together.</li> <li>• <b>Reset Immediately.</b> Select this option so the system resets immediately after the BIOS update is completed.</li> </ul>
<b>Drop a file on this page or select Browse...</b>	The option to select and upload or drop a new firmware image on the page.
<b>Upload</b>	Upload the BIOS/IFWI firmware image file.

### 5.3.13 CPLD Update

The CPLD Update page is used to upload and update the new complex programmable logic device (CPLD) firmware (See [Figure 38](#)).



**Figure 38. CPLD Update Page**

When dropping a new CPLD firmware image on the page or selecting one to upload, the BMC begins its CPLD firmware image upload process, which takes a couple of minutes. A message is displayed after the firmware image is uploaded successfully.

If the CPLD update option is set to “Reset Immediately”, the system will reboot immediately after the firmware update process has completed. Log in to the web console to verify that the CPLD firmware update was successful.

If the CPLD update option “Reset Immediately” is not selected, then a manual system reboot (DC cycle) is required after the CPLD firmware update has completed. Log in to the web console to verify that the CPLD firmware update was successful.

[Table 18](#) provides a description for all configurable features and input buttons found on the page.

**Table 18. CPLD Update Options**

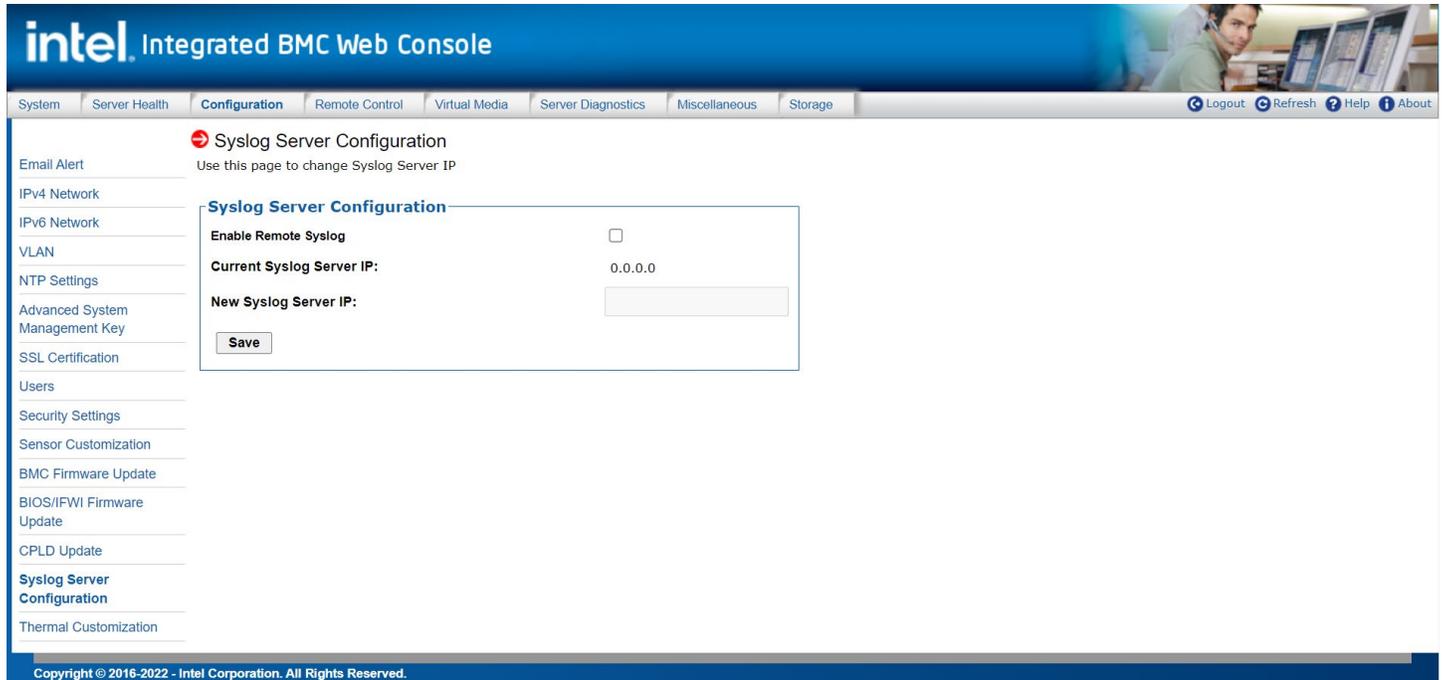
Option	Task
<b>CPLD FW Rev</b>	Display the current firmware version (read only).
<b>CPLD Update Option</b>	<ul style="list-style-type: none"> <li>• <b>Recovery.</b> Select this option so the backup region of the current CPLD is updated together.</li> <li>• <b>Reset Immediately.</b> Select this option so the system resets immediately after the firmware update is completed.</li> </ul>
<b>Drop a file on this page or select Browse...</b>	The option to select and upload or drop a new firmware image on the page.
<b>Upload</b>	Upload the CPLD firmware update image file to the BMC for the update to start.

### 5.3.14 Syslog Server Configuration

Use the Syslog Server Configuration page to enable the Remote Syslog service or to configure the IP of the Syslog Server. This page allows logging of all logins to the BMC or any configurations to be logged to the Syslog server (See [Figure 39](#)).

Before using the syslog service in the server, it must be configured with the following steps:

1. Open the configuration file by `vim /etc/rsyslog.conf`
2. Open `Modload imudp/UDPServeRun 514/ModLoad imtcp/InputTCPServerRun 514`
3. Service `syslog restart`
4. Set syslog server from **Integrated BMC Web Console > Configuration > Syslog Server Configuration**
5. Type `/var/log/messages` to see the log



**Figure 39. Syslog Server Configuration Page**

Table 19 provides a description for all configurable features and input buttons found on the page.

**Table 19. Syslog Server Configuration Options**

Option	Task
<b>Enable Remote Syslog</b>	To enable/disable remote syslog, check or uncheck Enable Remote Syslog.
<b>Current Syslog Server IP</b>	Display the current IP address of the syslog server.
<b>New Syslog Server IP</b>	Input the new syslog server IP address.
<b>Save</b>	Save the current settings.

### 5.3.15 Thermal Customization

The Thermal Customization page is used to optimize the thermal/acoustic solution for a particular chassis/board combination. Customized sensors can be added, deleted, or modified (See [Figure 40](#)).



Figure 40. Thermal Customization Page

Table 20 provides a description for all configurable features and input buttons found on the page.

Table 20. Thermal Customization Options

Option	Task
Thermal Customization File	Choose thermal customization JSON file to upload.
Upload	Click to upload the file to the BMC.

## 5.4 Remote Control Tab

The Remote Control tab provides access to secondary page options used to launch various server management control features, including: remote console KVM redirection, power control initialization, Serial-Over-Lan (SOL), and to access the virtual front panel. The following sub-sections provides an overview for each management feature page.

### 5.4.1 KVM

The KVM page is used to launch the remote console for keyboard, video, and mouse (KVM) redirection. Once launched, the keyboard, video, and mouse functions of a remote server can be utilized within the local window.

---

Note: See [Appendix B. Remote Console \(KVM\) Operation](#), for additional information.

---

Click the **Start button** to implement the KVM window on the current page, and then click **Open In New Window** to open on screen a new KVM window. [Figure 41](#) shows the details.

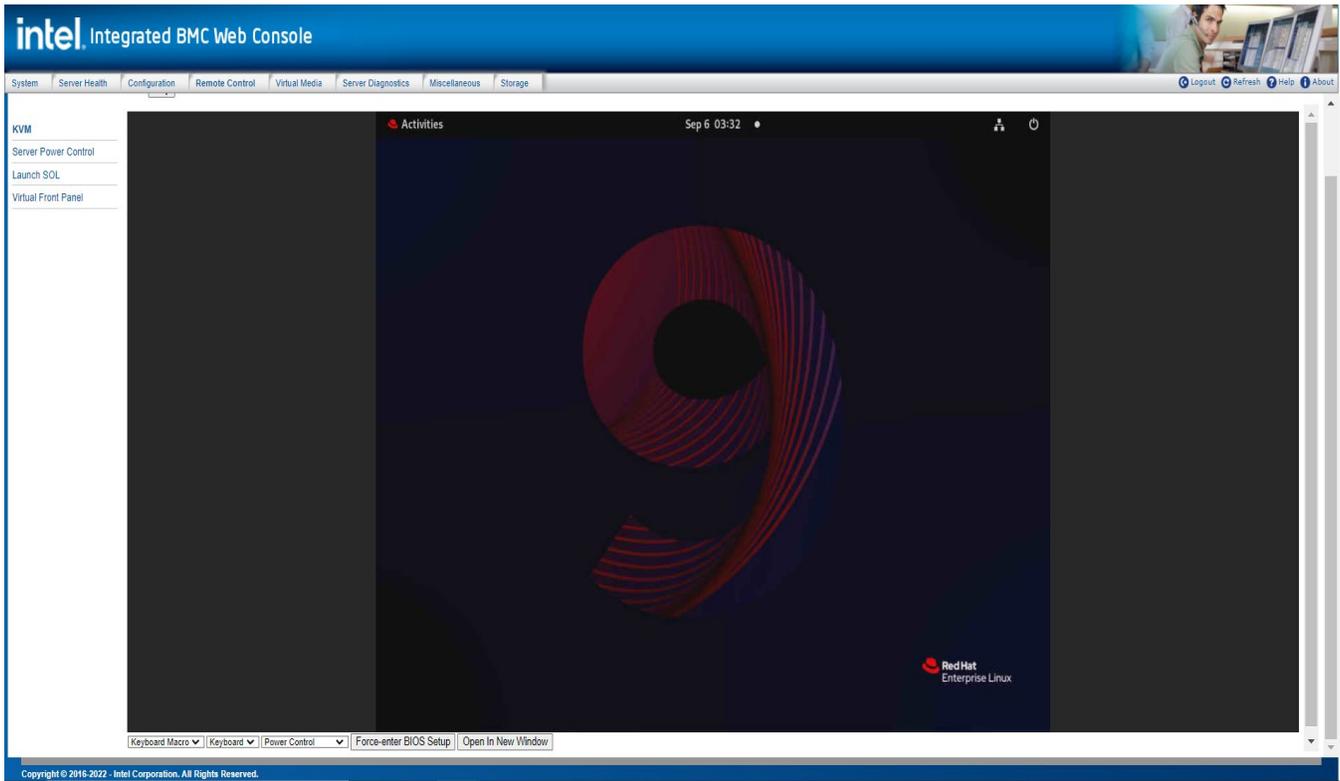


Figure 41. Remote Control KVM Page

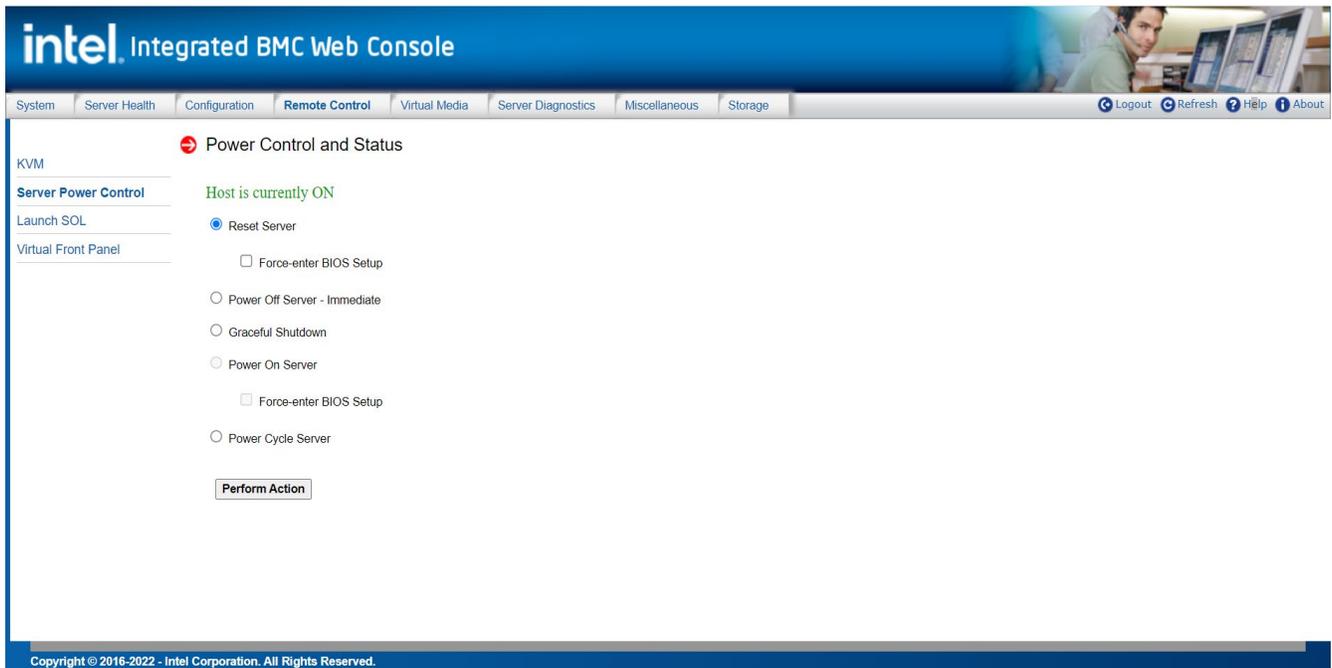
Table 21 provides a description for all configurable features and input buttons found on the page.

Table 21. KVM Page Options

Option	Task
<b>Start/Stop</b>	Activate or stop the KVM function.
<b>Send Macro</b>	Send the keyboard macro selected in this drop-down list to the KVM remote console.
<b>Keyboard</b>	Select a language from the different languages available for the virtual keyboard.
<b>Power Control</b>	Control the host power.
<b>Force-Enter BIOS Setup</b>	DC cycle the server and force to enter in the BIOS setup utility page.
<b>Open In New Window</b>	Open the KVM remote console in a pop-up window.

### 5.4.2 Server Power Control

The Server Power Control page shows power status and provides power/reset control of the server (See Figure 42).



**Figure 42. Remote Control Server Power Control Page**

Table 22 provides a description for all power control operations that can be performed from the page.

**Table 22. Server Power Control Options for Remote Control**

Option	Task
<b>Reset Server</b>	Hard reset the host without powering off.
<b>Power Off Server - Immediate</b>	Immediately power off the host.
<b>Graceful Shutdown</b>	Soft power off the host.
<b>Power On Server</b>	Power on the host.
<b>Power Cycle Server</b>	Immediately power off the host and power it back on after one second.
<b>Force-enter BIOS Setup</b>	Enter the BIOS setup utility after resetting/powering on the server.
<b>Perform Action</b>	Execute the selected remote power command.

**Note:** All power control actions are done through the BMC and are immediate actions. Intel suggests to gracefully shut down the operating system using the KVM interface or other interface before initiating power actions.

### 5.4.3 Launch SOL

The Launch SOL page is used to initialize the serial-over-LAN (SOL) console to manage a server remotely. This page displays the screen content of the remote server (See Figure 43).



Figure 43. Remote Control Launch SOL Page

Table 23 provides a description for each SOL operations that can be performed from the page.

Table 23. SOL Options

Option	Task
<b>Start/Stop SOL</b>	Start or stop the SOL console function.
<b>Open In New Window</b>	Open the SOL console in a new pop-up window.
<b>Close Window</b>	Close the SOL pop-up window.

To open an additional window, click the **Open In New Window** button (see Figure 44).

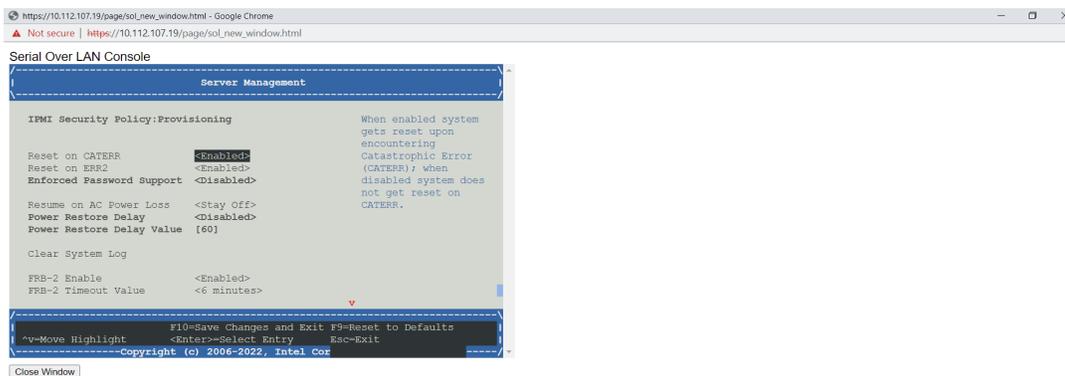


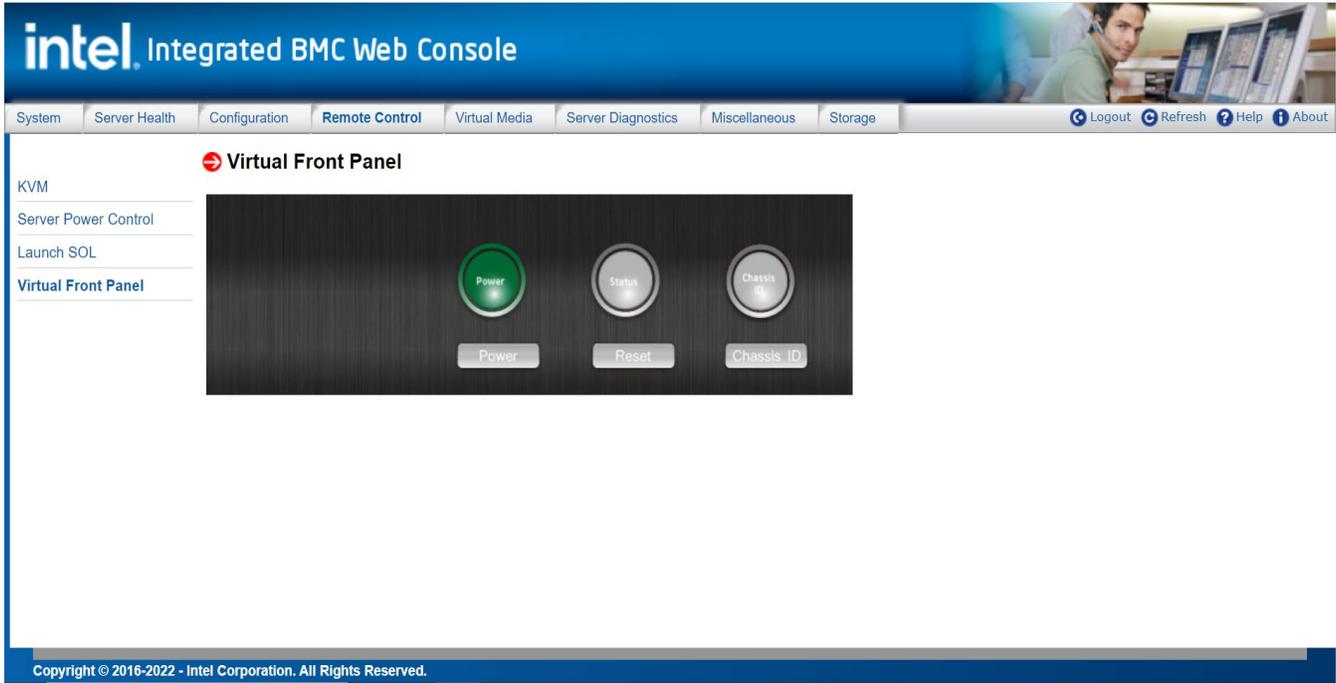
Figure 44. Launch SOL in Pop-Up Window

The SOL console emulates connection to a serial terminal on the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between the Integrated BMC Web Console and remote console.

**Note:** Before launching SOL, ensure that SOL for baseboard management control is **Enabled** on the **Configuration > SOL** page.

### 5.4.4 Virtual Front Panel

The Virtual Front Panel page provides virtual access to the system front panel, providing the ability to virtually view LED states and provide the ability to perform the functions of all front panel buttons (See Figure 45).



**Figure 45. Remote Control Virtual Front Panel Page**

Table 24 provides a description for all configurable features and input buttons found on the page.

**Table 24. Remote Control Virtual Front Panel Options**

Option	Task
<b>Power</b>	Power on or power off.
<b>Reset</b>	Reset the server while the system is on.
<b>Chassis ID</b>	<ul style="list-style-type: none"> <li>When the Chassis ID button is pressed, the chassis ID LED changes to solid on.</li> <li>If the button is pressed again, the chassis ID LED turns off.</li> </ul>
<b>Power LED</b>	<ul style="list-style-type: none"> <li>The power LED shows the system power status.</li> <li>If the power LED is green, the system is on.</li> <li>If the power LED is gray, the system is off.</li> </ul>
<b>Status LED</b>	<ul style="list-style-type: none"> <li>The status LED reflects the system status LED status and it is automatically in synchronization with the BMC every 2 seconds.</li> <li>If any abnormal occurs in the system, then the Status LED state changes accordingly.</li> </ul>
<b>Chassis ID LED</b>	<ul style="list-style-type: none"> <li>The chassis ID LED shows the current system chassis ID status.</li> <li>If the chassis ID LED is blue, the chassis ID is indefinite on.</li> <li>If the chassis ID LED is gray, the chassis ID is off.</li> </ul>

## 5.5 Virtual Media Tab

**Note:** This tab option and its secondary pages will only be available after the feature is enabled with the installation of the optional Advanced Management License Key.

The Virtual Media tab provides access to secondary page options to share local ISO and IMG/IMA files over HTML5 and share ISO/IMG/IMA file from the network using other supported protocols. The following subsections provides an overview for each.

### 5.5.1 Local Image

The Local Image page is used to share local ISO and IMG/IMA files over HTML5, which only includes one Virtual Media over HTML5 page. Each image/folder is emulated to the host as a USB device (See [Figure 46](#)).

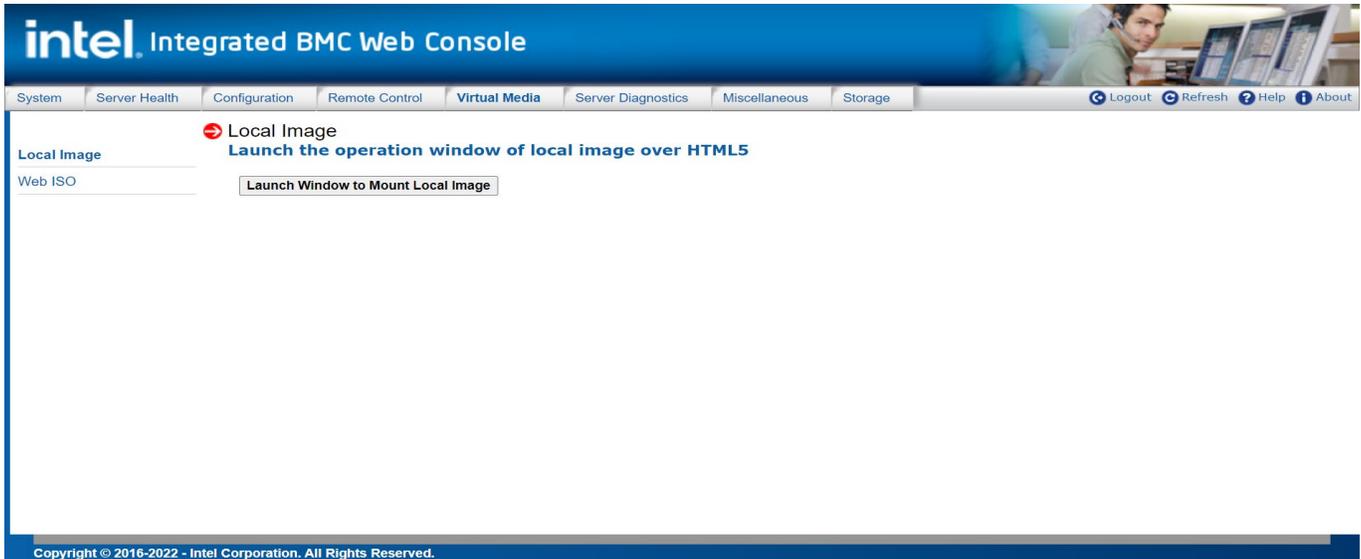


Figure 46. Local Image Page

To open the operation window, click the “**Launch Window to Mount Local Image**” button. This action starts the upload of local files to the BMC over HTML5. Up to two devices may be mounted simultaneously (See [Figure 47](#)).

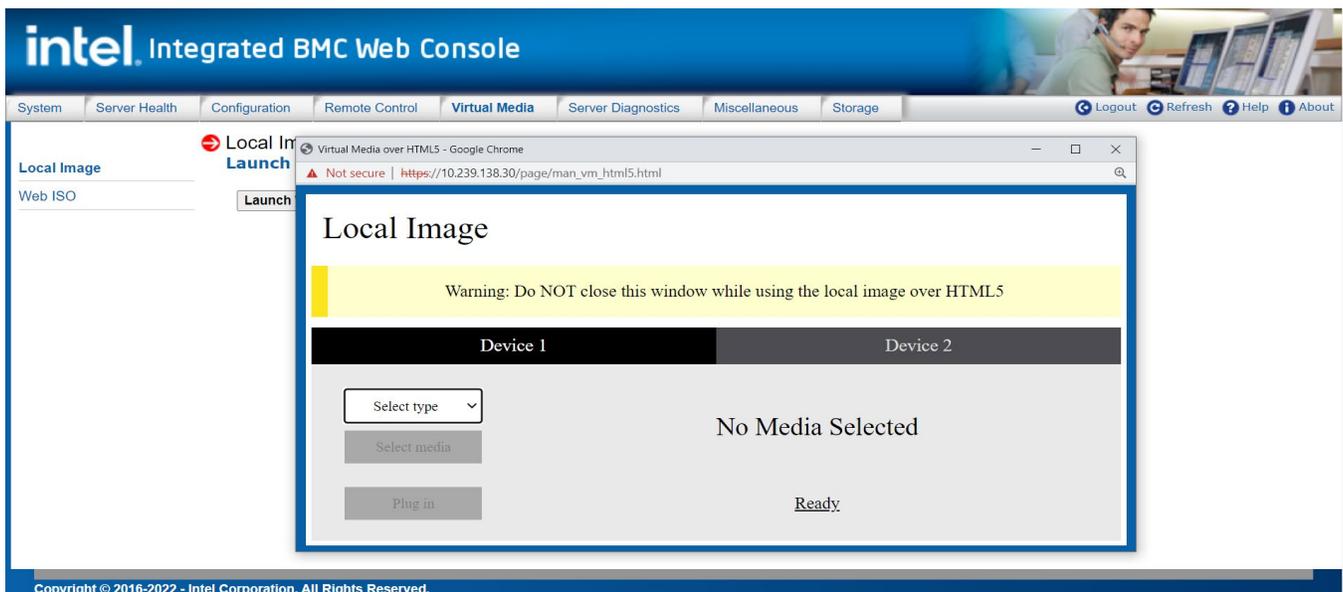


Figure 47. Launch Window to Mount Local Image Page

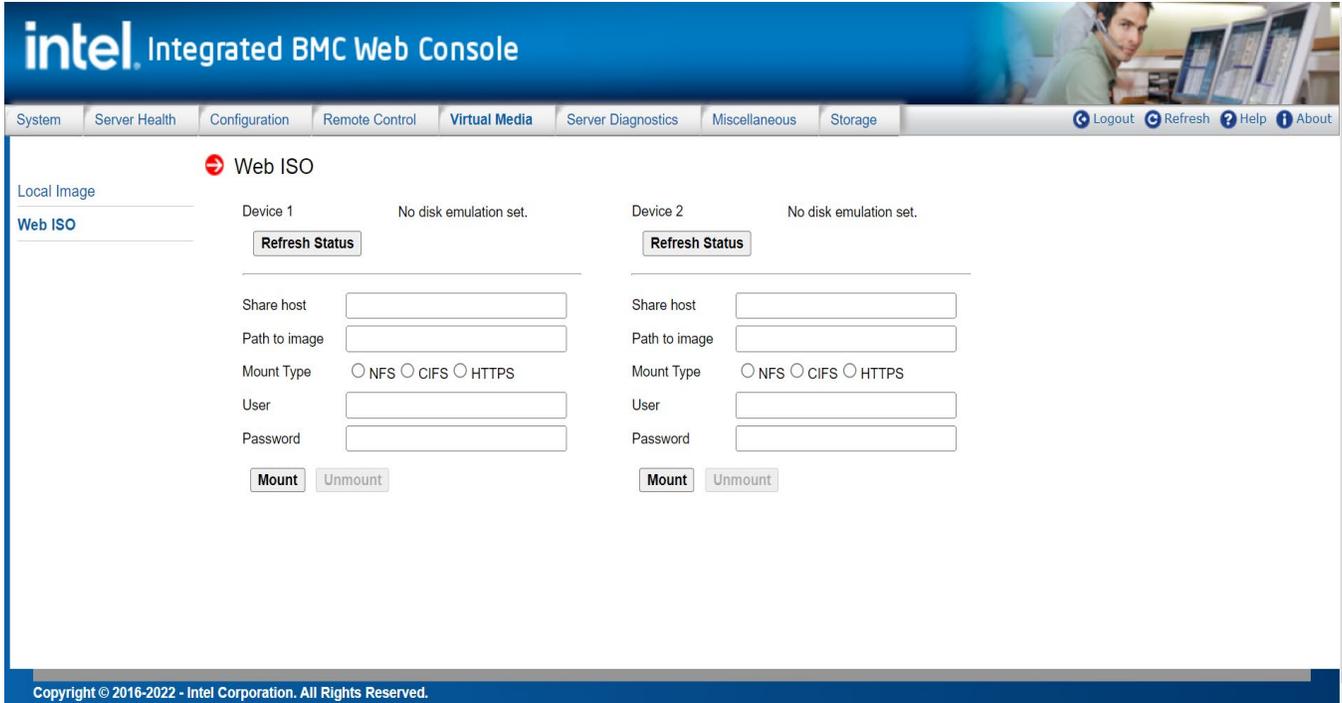
Table 25 provides a description for all configurable features and input buttons found on the page.

**Table 25. Local Image Options**

Option	Task
Device 1/Device 2	Select the virtual device to mount the file.
Select type	Choose the file type (ISO or IMG/IMA) of the file to mount.
Select media	Choose the local file to mount.
Plug in/Plug out	Mount/unmount the file.

### 5.5.2 Web ISO

The Web ISO page is used to share ISO/IMG/IMA file from the network by using NFS, SMB, or HTTPS protocols. Two devices are available to use (See Figure 48).



**Figure 48. Web ISO**

Table 26 provides a description for all configurable features and input buttons found on the page.

**Table 26. Web ISO Options**

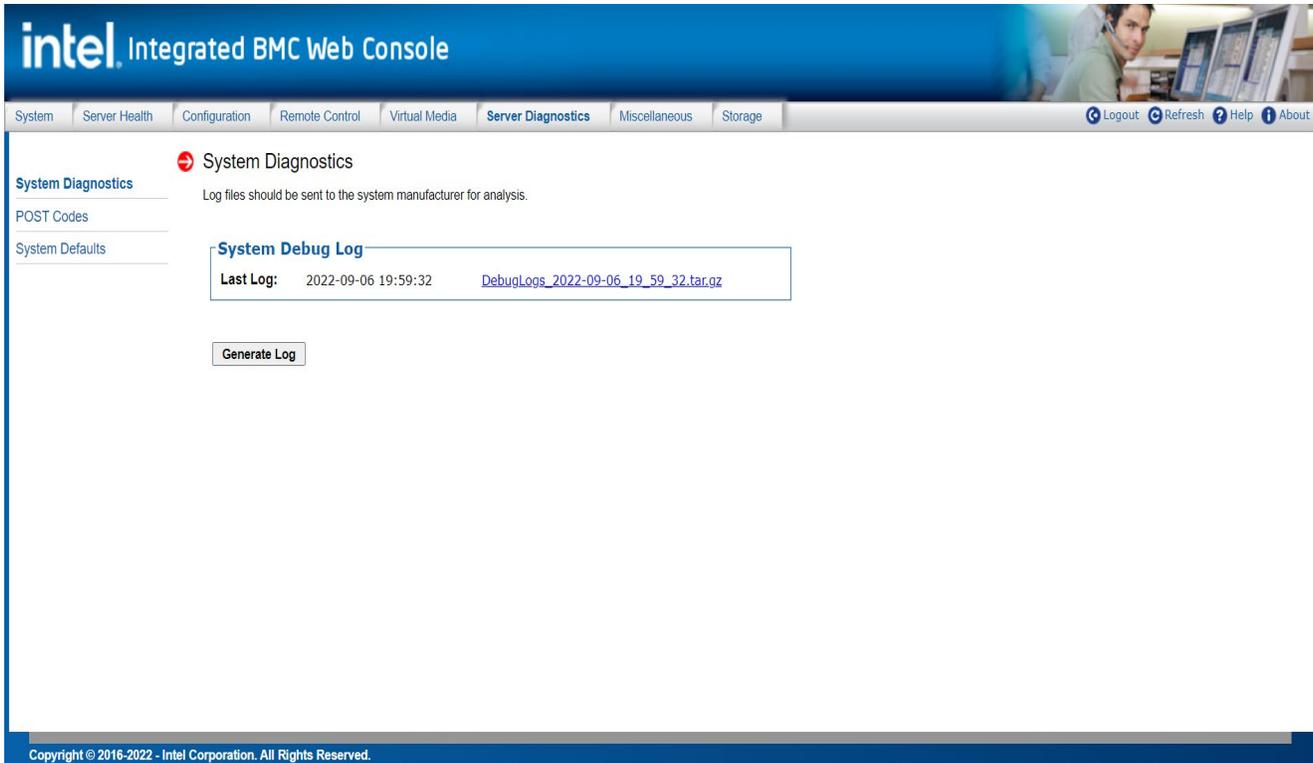
Option	Task
Refresh Status	Refresh the device status.
Share host	The host IP of the NFS/CIFS/HTTPS server.
Path to image	The file path in the NFS/CIFS/HTTPS server.
Mount Type	Select one protocol in NFS, CIFS, and HTTPS.
User	User name of the NFS/CIFS/HTTPS server user.
Password	Password of the NFS/CIFS/HTTPS server user.
Mount/Unmount	Mount/unmount the selected file.

## 5.6 Server Diagnostics Tab

The Server Diagnostics tab provides access to secondary pages used to access various server diagnostic support options, including: a page to generate enhanced system debug log files, a page to view POST codes for the last two boot system cycles, and a page to reset all BMC settings back to their factory defaults. The following sections provide an overview for each page options.

### 5.6.1 System Diagnostics

The System Diagnostics page allows administrators to collect enhanced system debugging information for analysis by an Intel engineer or Intel partner for enhanced debugging support. The files generated are compressed, encrypted, and password protected and are not intended to be viewable by the end user. See [Figure 49](#) to view the page layout.



**Figure 49. Server System Diagnostics Page**

To generate the diagnostic log files, click the “**Generate Log**” button. It may take several minutes for the debugging information to be collected. After the debug data collection has completed, the resulting compressed archive file can then be downloaded to the system by clicking the displayed “**Last Log**” link. The downloaded file can then be sent to the system manufacturer or an Intel support engineer for analysis.

The data that may be captured using this feature includes but is not limited to:

- System version information
- CPU Crash Dump
- IPMI FRU information
- BIOS POST code
- System Event Log
- System Management BIOS (SMBIOS) tables
- BMC sensor readings
- BMC journal log

### 5.6.2 POST Codes

The POST Codes page displays the power-on self-test (POST) results for the last two system boot cycles. See Figure 50 to view the page layout.

Holding the cursor over a POST code or description highlights all other occurrences of that same POST code. Selecting a POST code or description causes the highlight to persist until another code is selected.

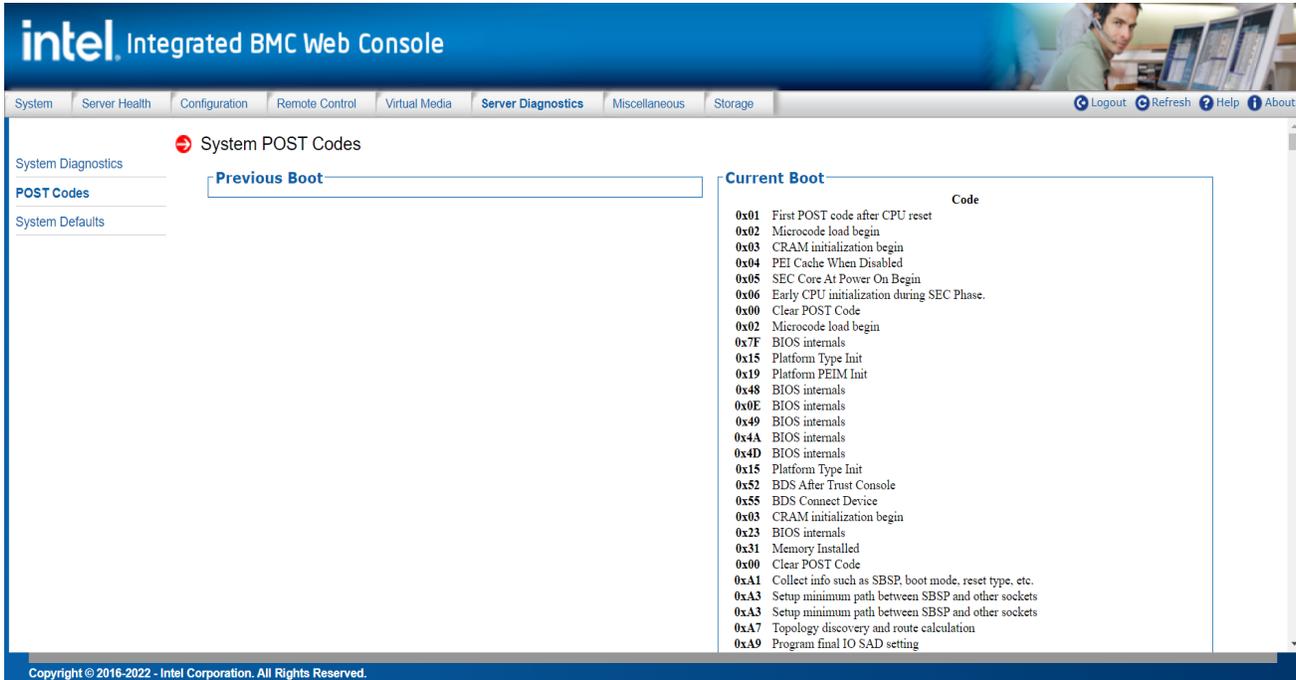


Figure 50. Server Diagnostics POST Codes Page

### 5.6.3 System Defaults

The System Defaults page provides options to reset all or partial BMC settings to their factory defaults. See Figure 51 to view the page layout.

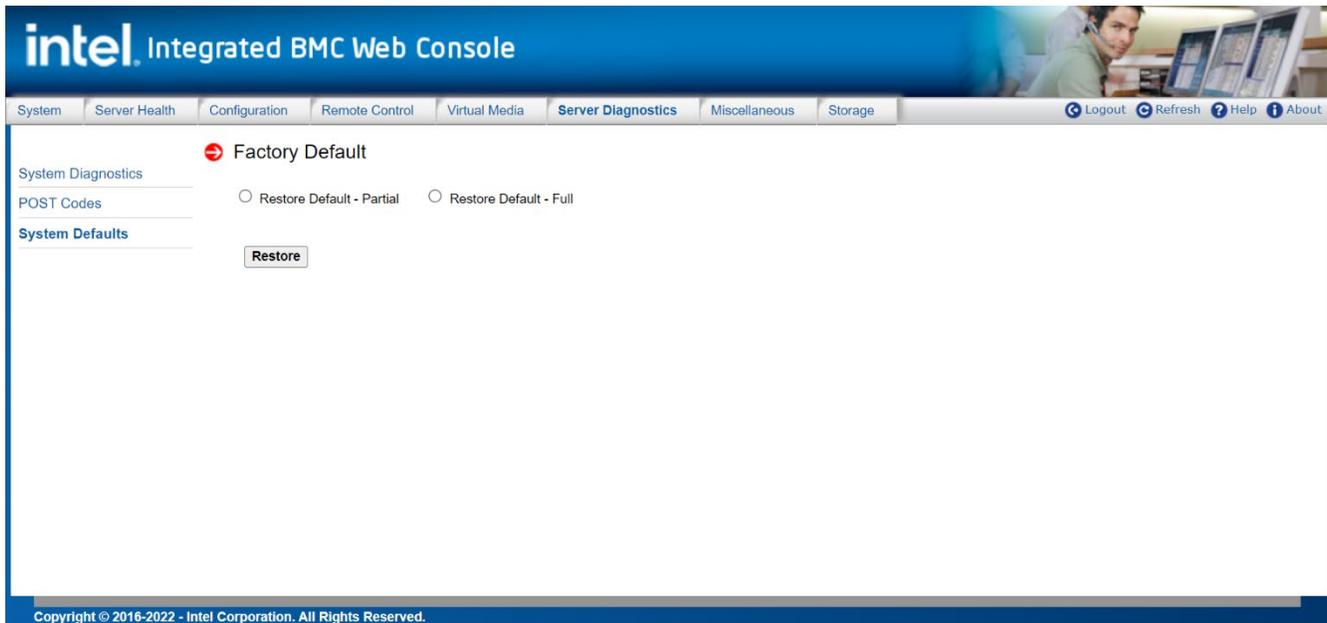


Figure 51. Server Diagnostics Default Page

The “**Restore Default – Partial**” option keeps the existing LAN and User settings and resets all other settings to their factory defaults.

The “**Restore Default – Full**” option resets all BMC settings to their factory defaults.

To reset all BMC settings to factory defaults, click the “**Restore**” button.

---

**Caution:** Once the action to reset BMC settings to factory defaults has completed, the action cannot be undone.

---

Once complete, all remote management, including the web server, are not accessible until users and network settings are restored locally. Settings reset include, but are not limited to:

- All network addresses and settings.
- Power restore policies.
- Platform event filters.
- Alert destinations.

---

**Note:** Restore BMC setting to factory defaults does not affect the BMC system event log (SEL), sensor data repository, or any Intel® Node Manager (Intel® NM) settings and policies.

---

## 5.7 Miscellaneous Tab

The **Miscellaneous** tab provides access to secondary pages used to set Intel Node Manager policies and view the latest power consumption statistics of the server. The following subsections provide an overview for each page..

### 5.7.1 NM Configuration – Intel® Node Manager

The NM page is used to view, add, and configure Intel® Node Manager policies. See Figure 52 to view the page layouts.

The policy table in the window lists all policies previously configured. If no policies have been created, enter the desired policy information into the data fields below the table. See [Table 27](#) for information about each data field. Selecting a previous configured policy from the policy list will automatically fill in the policy data fields.

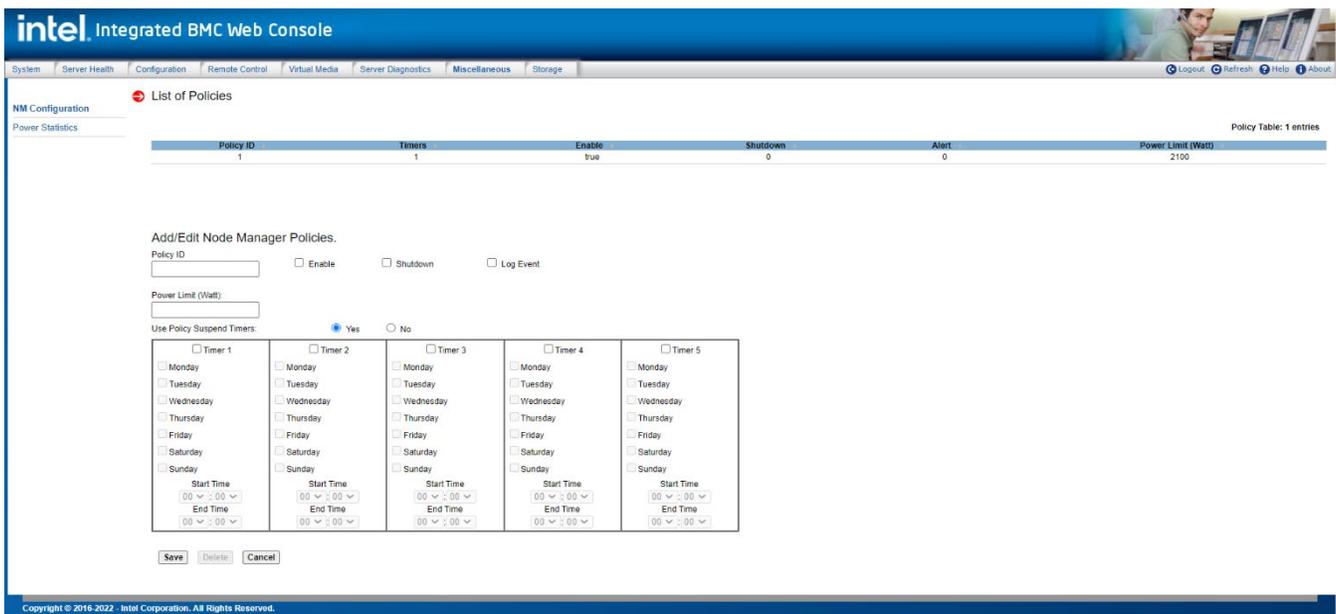


Figure 52. Intel® Node Manager Configuration Page

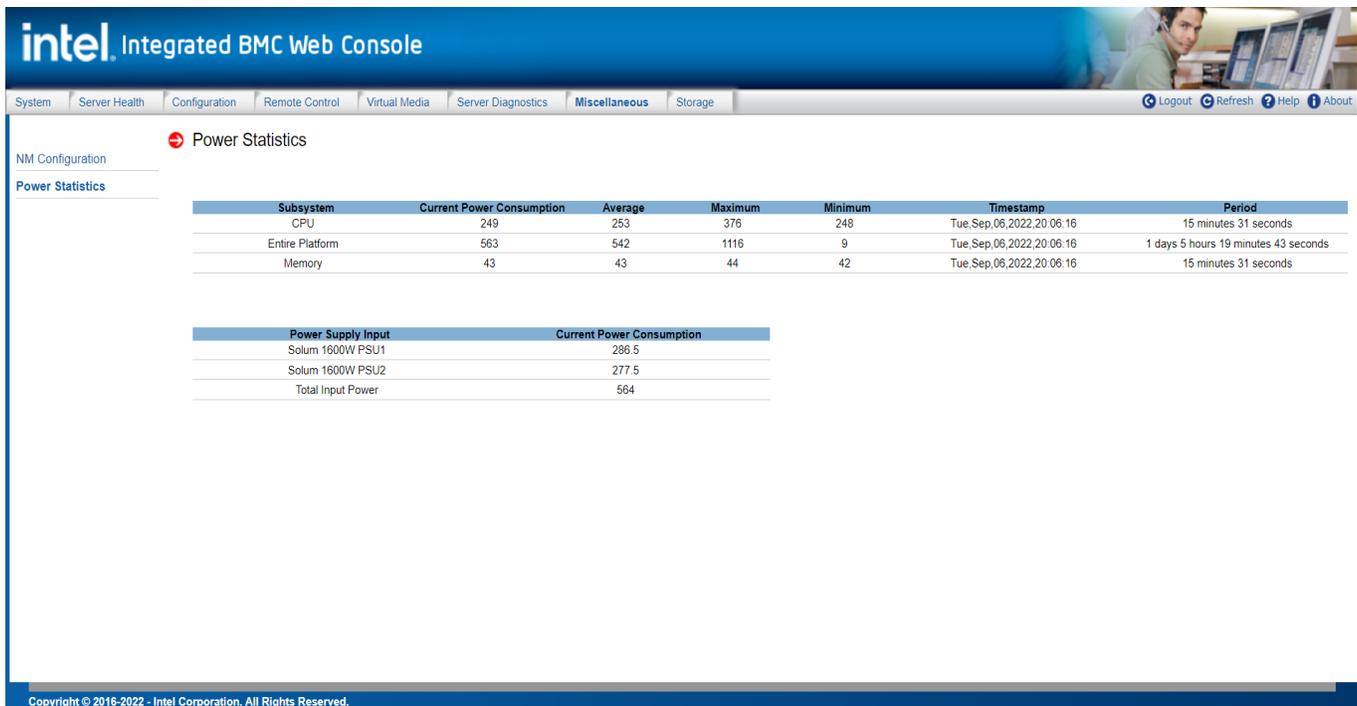
Table 27 provides a description for all configurable features and input buttons found on the page.

**Table 27. Intel® Node Manager Configuration Options**

Option	Task
List of Policies	This table lists the currently configured policies. Selecting an item from the table populates the editable fields in the following settings section.
Policy ID	<ul style="list-style-type: none"> <li>The policy ID to add/edit/delete. Valid range is 0–255.</li> <li>In the policy table, policy IDs with an asterisk (*) are policies set externally using a non-platform domain.</li> <li>Changing parameters on these policies does not affect their triggers, trigger limits, reporting periods, correction timeouts, or aggressive CPU throttling settings.</li> </ul>
Enabled	Check this box if the policy is to be enabled immediately.
Shutdown	Enable a system shutdown if the policy is exceeded and cannot be corrected within the correction timeout period. The operating system is given 30 seconds to shut down gracefully. If the system is still not shut down after 30 seconds, the BMC initiates an immediate shutdown.
Log Event	Enable the node manager to send a platform event message to the BMC when a policy is exceeded.
Power Limit (Watt)	The desired platform power limit, in watts.
Use Policy Suspend Periods	<ul style="list-style-type: none"> <li>If enabled, configure policy suspend periods.</li> <li>Each policy may have up to five suspend periods (see Figure 52).</li> <li>Suspend periods are repeatable by day-of-week.</li> <li>Start and stop times are designated in 24-hour format, in increments of 6 minutes.</li> <li>To specify a suspended period crossing midnight, two suspend periods must be used.</li> </ul>
Save	Click to save any changes made.
Delete	Select a policy in the list and click to delete.
Cancel	Click to discard the changes.

### 5.7.2 Power Statistics

The Power Statistics page displays data tables for the latest system power consumption statistics by sub-system (CPU, Memory, and Entire Platform), and power input for each installed power supply. See Figure 53 to view the page layout.



**Figure 53. Power Statistics Page**

## Appendix A. Advanced Management License Key – Order, Registration, and Installation

### How to Order Advanced System Management Key

There are two options available to order the Advanced Management License Key:

- **CTO/L9:** When ordering a fully integrated system from Intel using its on-line Configure-to-Order (CTO) tool, select the **AdvSysMgmtKey** as an additional option. The Intel factory will then automatically upload the license key on to the system during the system integration process.
- **Add-on Accessory:** The Advanced Management License Key (iPC **ADVSYSMGMTKEY**) can be ordered separately from the system as an add-on accessory. This option requires that the license key be manually installed on the system. See for following sections for complete ordering and installation instructions.

### Order and Register the License Key as an Add-on Accessory (Not via CTO)

1. Place an order for the Intel® Advanced Management License Key (Electronic Delivery). Intel Product Code: **ADVSYSMGMTKEY**
2. Receive an email with instructions to download the product key.
3. From the email, Click the **Register** link (see [Figure 54](#)) to go to <https://lemcenter.intel.com>

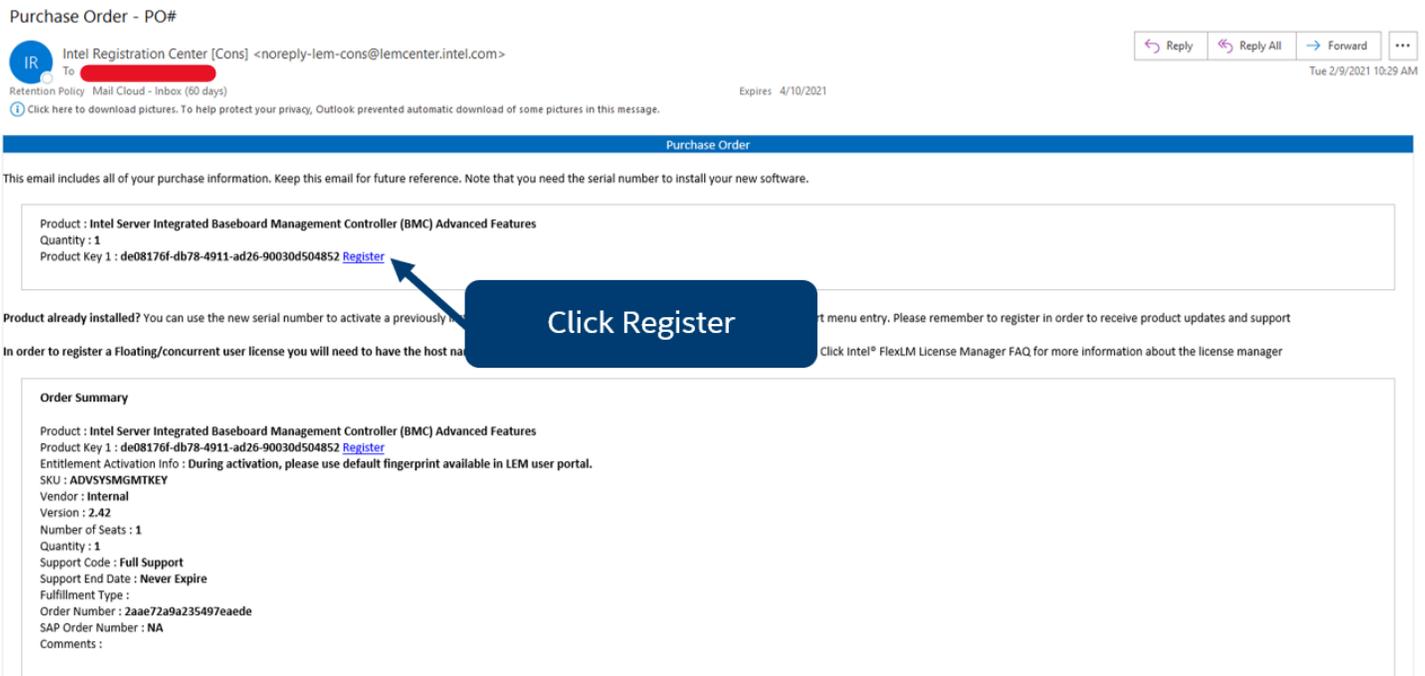


Figure 54. Example Email

4. Login using an existing Intel account or Create a new one. An email address is required

- From the Registration Screen, Click the “Register” button to register the pre-entered license key number (see Figure 55)

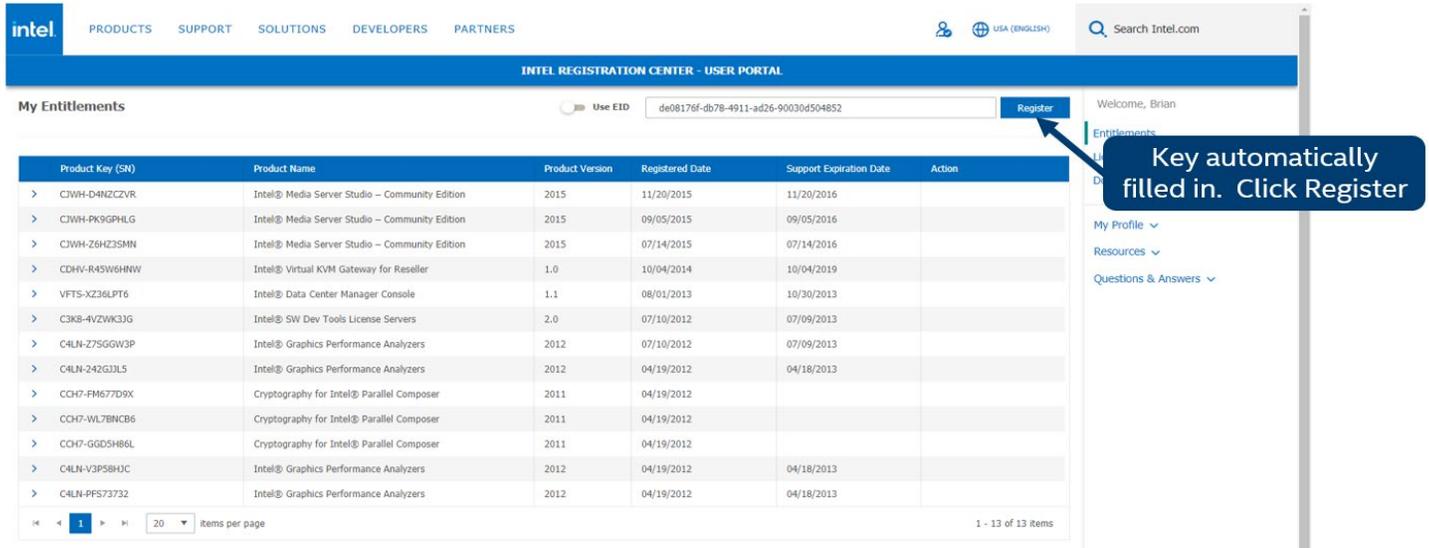


Figure 55. Register Key

- Activate the license (see Figure 56)

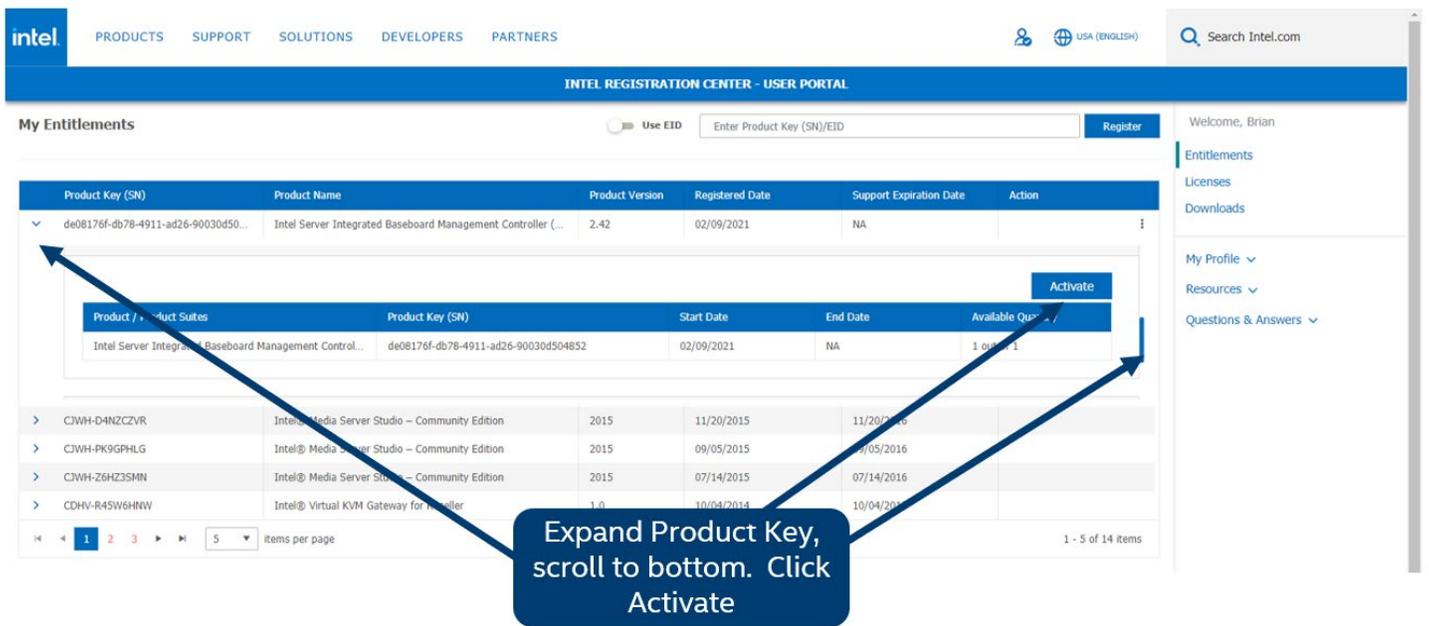


Figure 56. Activate Key

7. Download the license associated with the specified product key (see [Figure 57](#))

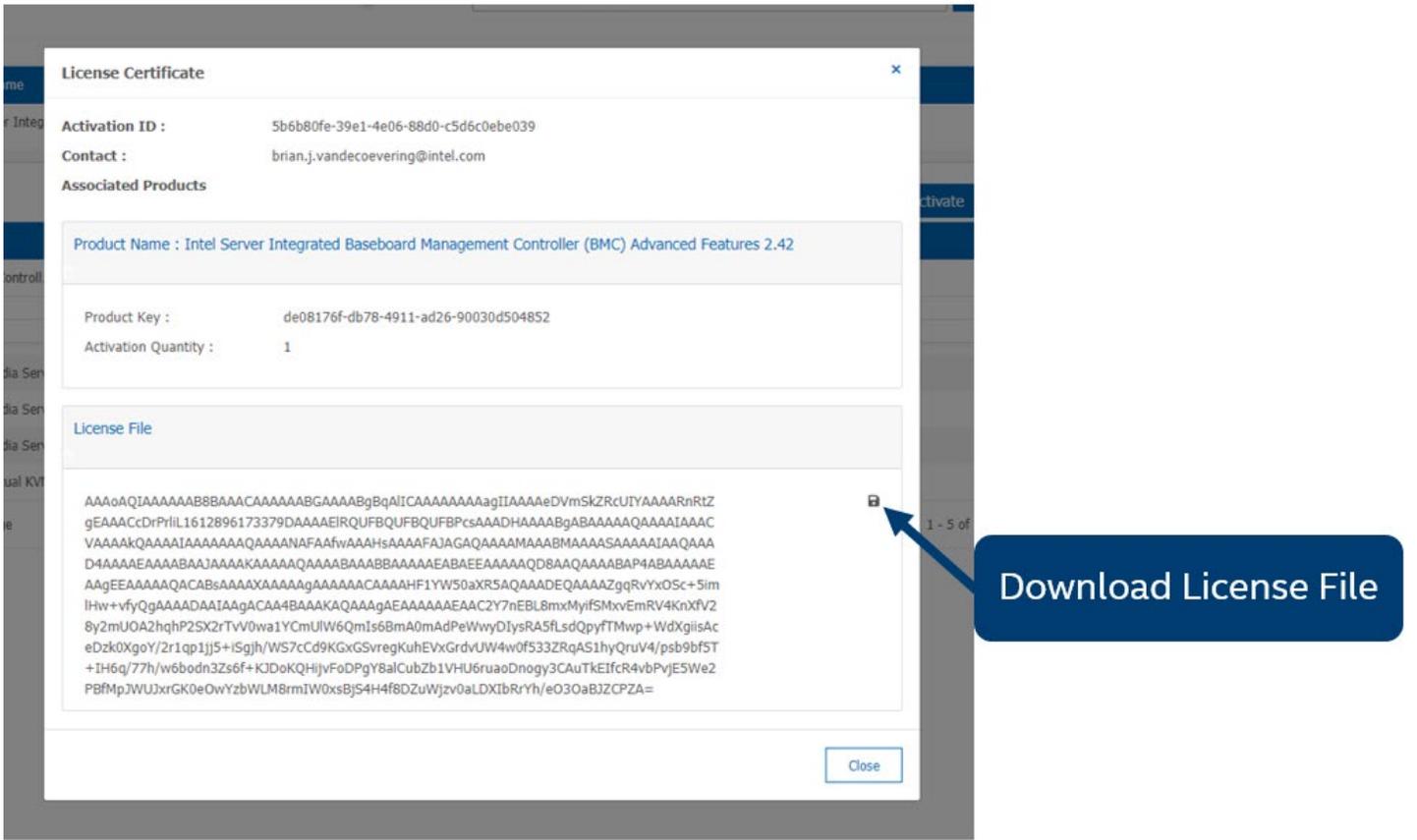


Figure 57. Download Key

8. Use the Integrated BMC Web Console or Intel Server Configuration Utility to upload the key to the BMC.
  - Only single license file per order is needed to activate multiple systems.

**Note:** If any key or email is lost, Intel can generate new product keys as needed.

## Advanced Management Key Installation

Three available options can be used to upload the key onto the server:

- Integrated BMC Web Console for Intel server boards
- Intel Server Configuration Utility
- Redfish\* Interface

## Installation Using the Integrated BMC Web Console

The following procedure may be used to upload and confirm activation of the Advanced System Management Key using the Integrated BMC Web Console.

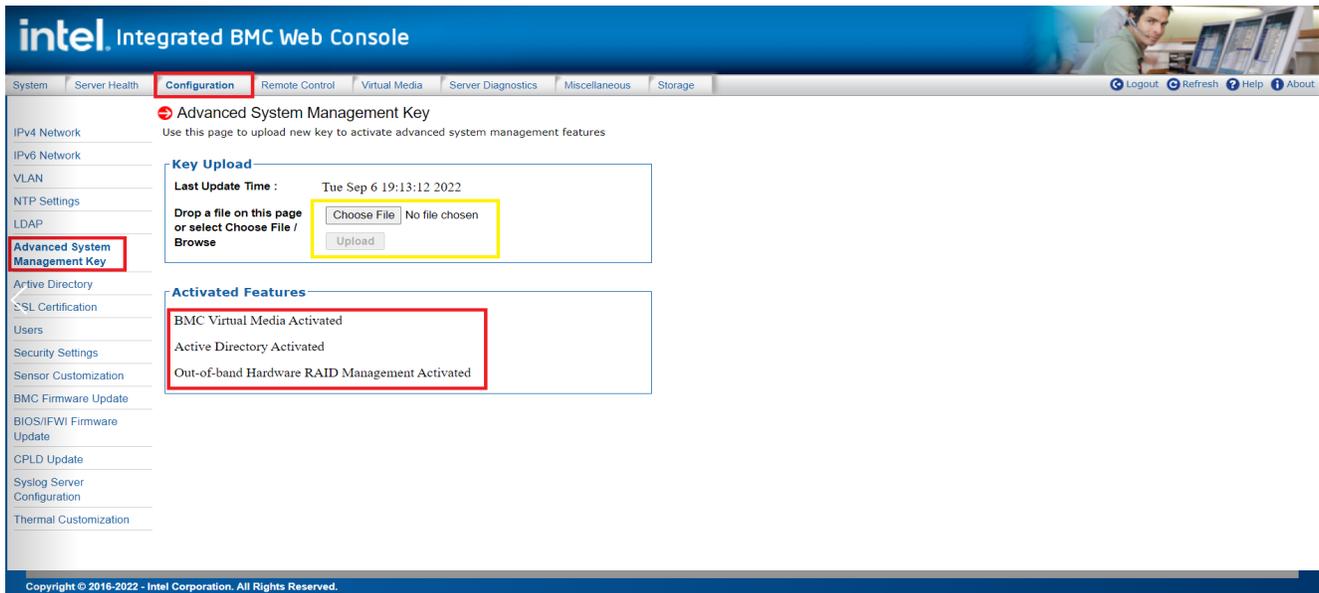


Figure 58. Integrated BMC Web Console Advanced System Management Key Page

Use Figure 63 as a reference for the following procedure.

1. Login to the Integrated BMC Web Console
2. Navigate to the **Configuration** tab and select the **Advanced System Management Key** page
3. Click the **Choose File** button to select the software key file
4. Select the **.v2c** license key file from the file browser, then click the **Open** button
5. Click the **Upload** button to upload the License Key to the BMC.
6. Navigate back to the **System** Tab. On the **System Information** page, view the **System Summary** information box to confirm the **Advanced Management Key** was successfully **Activated**. See Figure 63.



Figure 59. Web Console System Information Page

## Installation Using the Intel® Server Configuration Utility

The following procedure may be used to upload and confirm activation of the Advanced System management Key using the syscfg command line utility.

To download the latest utility package, go to <https://downloadcenter.intel.com/> and initiate a search for “Intel Server Configuration Utility”.

Prerequisites:

- Ensure the user has Administrator or Root privileges for the chosen operating system
- Ensure the KCS Policy Control Mode is set to “**Provisioning**”

Procedure:

1. Install the Intel® Server Configuration Utility on to the target server system. See the Intel® Server Configuration Utility User Guide for complete utility installation instructions.
2. Navigate to the sub-directory where the Server Configuration Utility was installed
3. From a command prompt type the following command line (See Figure 64)

***syscfg /lic <key file name>***

Where “file name” can just be the name of the license file if copied to the same directory as the syscfg command file, or the complete path of where the license key was copied can be entered along with the file name.

Examples:

- `syscfg /lic file_name.v2c`
- `syscfg /lic /directory_name/file_name.v2c`

```
[root@localhost Syscfg_V16.0.6_AllOS]# syscfg /lic ASM.v2c

Server Configuration Utility Version 16.0.6
Copyright (c) 2022 Intel Corporation

Key Transfer...
Starting key upload:
Key Upload done
```

**Figure 60. Upload Advanced Management License Key Using SYSCFG Utility**

4. To confirm activation of the Advanced Management License Key, type the following command line. See Figure 65.

***syscfg /d lic***

```
[root@localhost Syscfg_V16.0.6_AllOS]# syscfg /d lic

Advanced Management Key Status

Type: ASM key

Active status: Activated

Last upload: 09/07/2022-06:49:41
```

**Figure 61. Confirm Activation of Advanced Management Key Using SYSCFG Utility**

## Installation Using Redfish\*

The following steps may be used to upload and confirm activation of the Advanced System Management Key using Redfish\*.

Prerequisites:

- If not already present, install the “curl” utility onto the system from which the commands will be run.

Issue the following command to upload the Advanced management Key to the BMC

```
curl -k -u username:password
https://BMC_IP/redfish/v1/UpdateService/SoftwareInventory/AdvancedSystemManagementKey/Acti
ons/Oem/Intel.Oem.AdvancedSystemManagementKey -H "Content-Type: multipart/form-data" -F
'updateFile=@filepath' -X POST
```

See screenshot in Figure 66, where:

- username = admin
- password = Password@123
- BMC\_IP = 10.239.46.29
- filepath = /home/test/ASM.v2c

Notes:

- The command line above is a single command line, no return after “password ” and “ https...”
- username:password in the command line above should be replaced with the name of the user and their password

```
[~]$curl -k -u admin:Password@123 https://10.239.46.29/redfish/v1/UpdateService/
SoftwareInventory/AdvancedSystemManagementKey/Actions/Oem/Intel.Oem.AdvancedSyst
emManagementKey -H "Content-Type: multipart/form-data" -F 'updateFile=@/home/te
st/ASM.v2c' -X POST | python -m json.tool
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100   931   100   151   100   780     631   3263  --:--:--  --:--:--  --:--:--  3911
{
  "@odata.id": "/redfish/v1/TaskService/Tasks/0",
  "@odata.type": "#Task.v1_4_3.Task",
  "Id": "0",
  "TaskState": "Running",
  "TaskStatus": "OK"
}
```

**Figure 62. Redfish Command to Upload the Advanced System Management Key**

Issue the following command to verify the activation status of the Advanced System Management key.

```
curl -k -u username:password
https://BMC_IP/redfish/v1/UpdateService/SoftwareInventory/AdvancedSystemManagementKey -H
"content-type: application/json" -X GET | grep LicenseStatus
```

```
[~]$curl -k -u admin:Password@123 https://10.239.46.29/redfish/v1/UpdateService/
SoftwareInventory/AdvancedSystemManagementKey -H "content-type: application/json
" -X GET | grep LicenseStatus
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100   1023   100   1023    0    0   4942    0  --:--:--  --:--:--  --:--:--  4942
  "LicenseStatus": "ACTIVATED",
```

**Figure 63. Redfish Command to Verify Activation of Advanced Server Management Key**

## Appendix B. Remote Console (KVM) Operation

The remote console is the redirected keyboard, video, and mouse (KVM) of a remote host system. Starting the remote console KVM to display the screen content of the host system, the remote console acts as if the administrator were sitting directly in front of the screen of the remote system with .

### Launch the Redirection Console

From the KVM Page under the **Remote Control** tab of the Web Console, launch the remote console KVM redirection window by clicking the **Start** button (Figure 64).

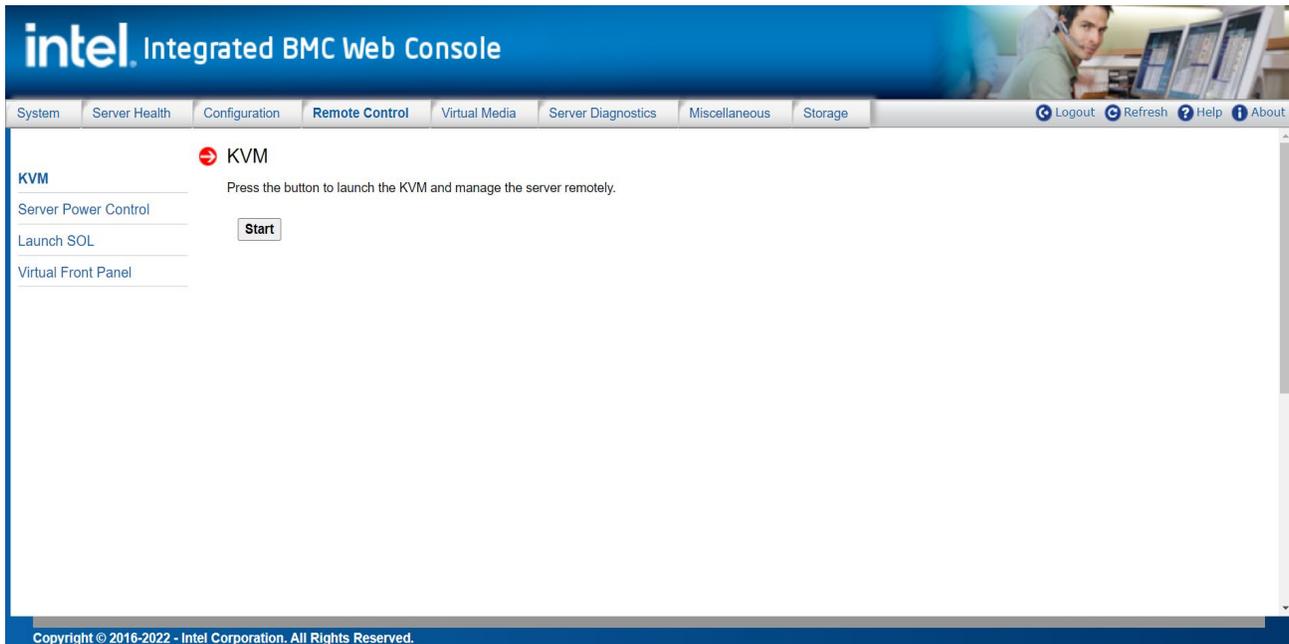


Figure 64. Remote Control Console Redirection Page

When the Start button is clicked, the remote server screen displays in the current page. See Figure 65.

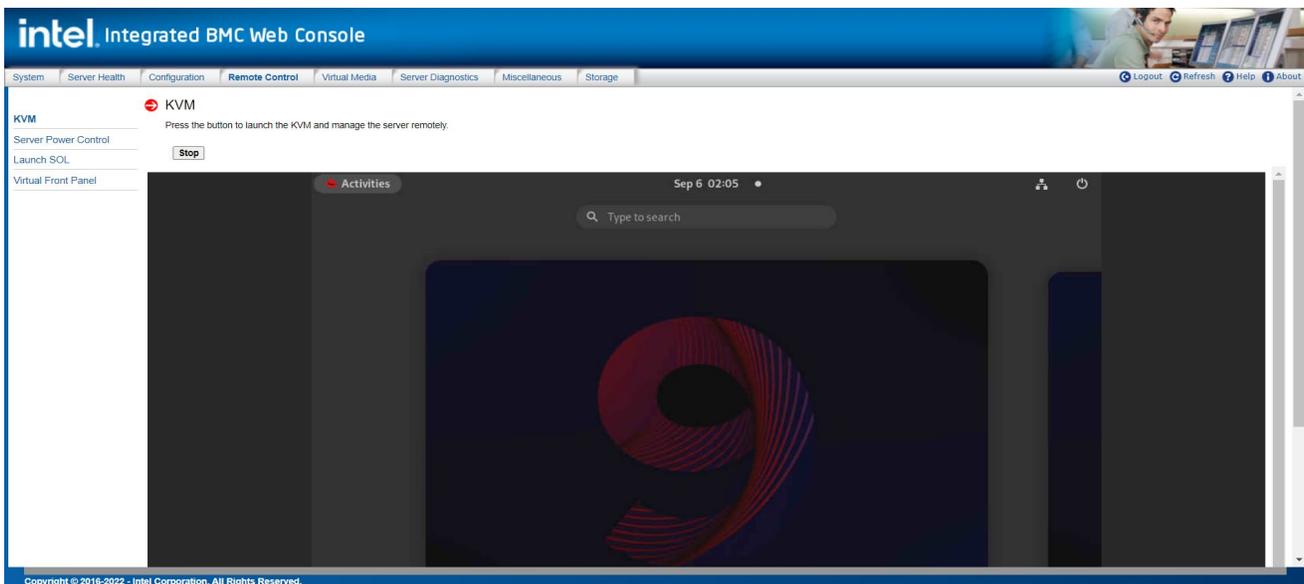


Figure 65. Remote Control Console Redirection Page

The “**Open In New Window**” button at the bottom of the page can be used to pop-up a new window. See Figure 66.

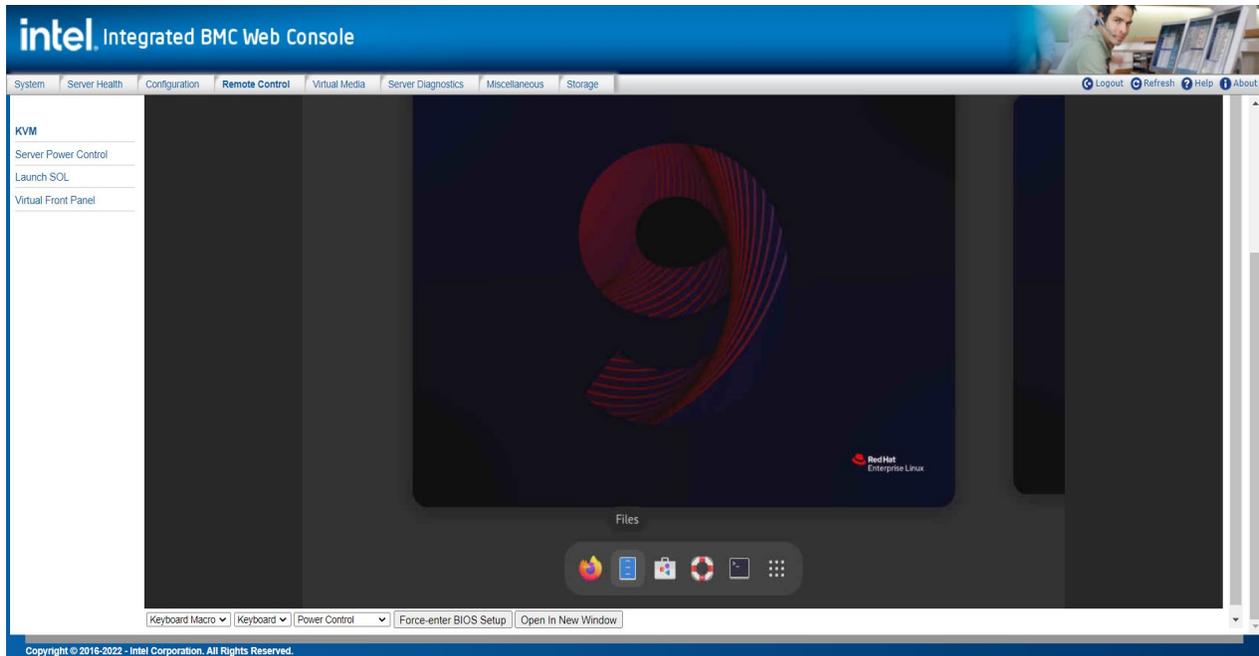


Figure 66. Remote Console Window

## Main Window

Starting the remote console opens a host window like the Linux\* operating system window shown in Figure 67.

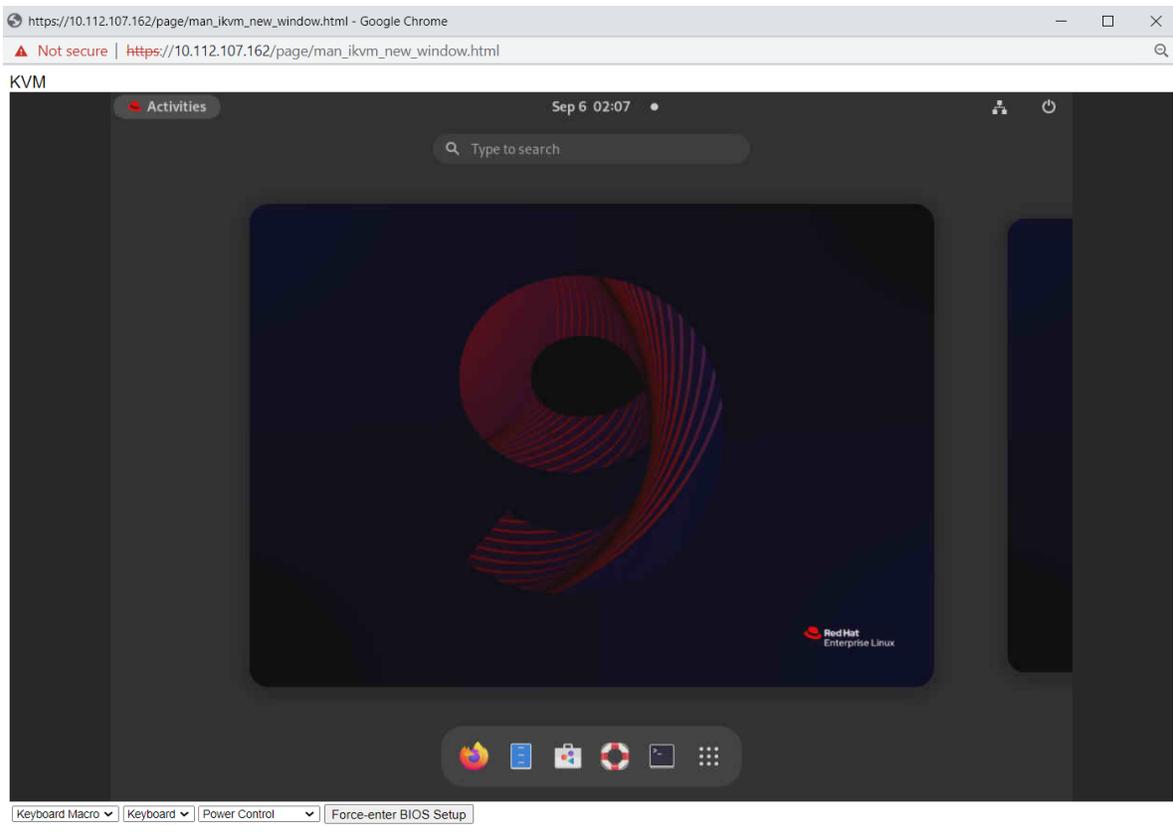


Figure 67. Remote Console Main Window

The host window displays the screen content of the remote server. The remote console responds as if it were at the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between the Integrated BMC Web Console and the remote console.

## Remote Console Control Bar

The bottom of the remote console window contains a control bar for viewing the status of the remote console and to configure remote console settings. The following subsections describe each control task.

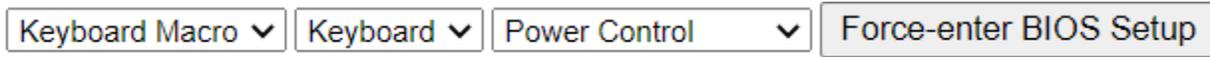


Figure 68. Remote Console Control Bar

### Macro Menu

Click the **Keyboard Macro** drop-down list to open the keyboard macro menu as shown in Figure 69.



Figure 69. Remote Console Macro Menu

Using the options in this menu, the user can simulate special key combinations to the remote operating system, which include:

- <Alt+Tab>
- <Ctrl+Alt+Del>
- <Alt+Space>
- <Alt+Esc>
- <Alt+Enter>
- <Print>
- <Alt+F4>
- <Ctrl+Esc>
- <Ctrl+Tab>

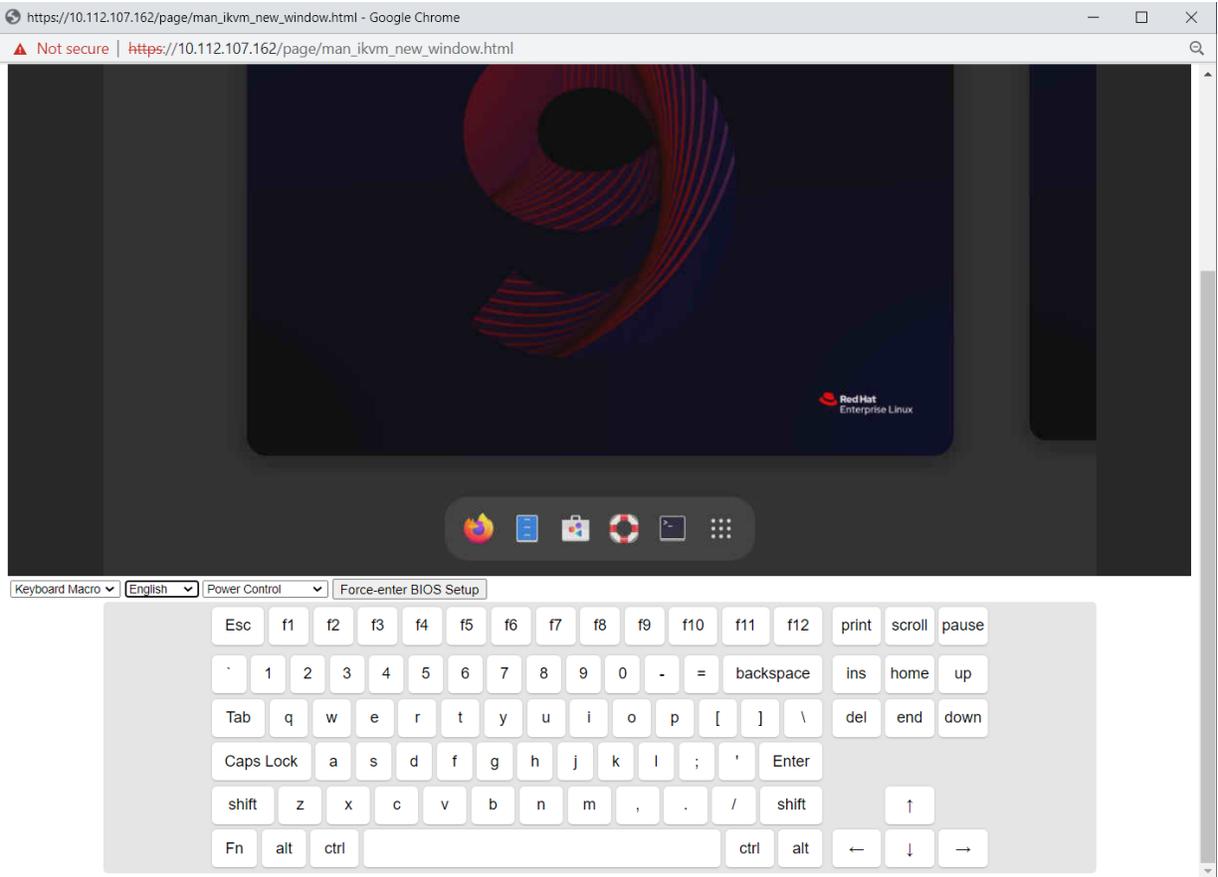
### Keyboard Menu

Click the **Keyboard** drop-down list to open the keyboard menu as shown in Figure 70.



Figure 70. Keyboard Options Menu

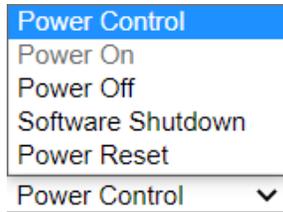
Use the options in this menu to open a virtual keyboard and specify its language. See [Figure 71](#) for details.



**Figure 71. Keyboard Option**

### Power Control Menu

Click the **Power Control** drop-down list to open the power control menu as shown in [Figure 72](#).



**Figure 72. Remote Console Power Control Menu**

[Table 28](#) describes the power control operations that can be performed.

---

**Note:** All power control actions are immediate actions done through the BMC. Intel suggests to gracefully shut down the operating system using the KVM interface or other interface before initiating power actions.

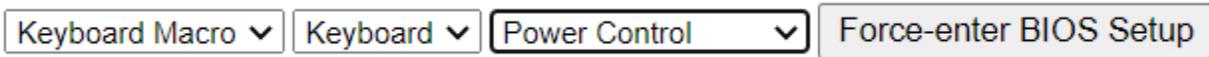
---

**Table 28. Remote Console Power Control**

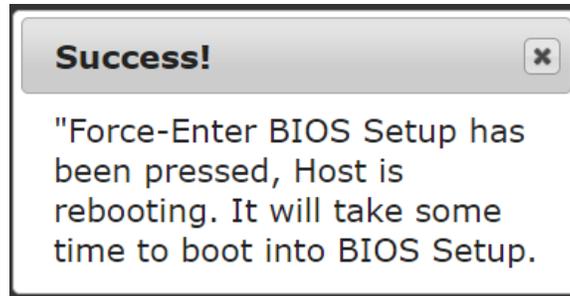
Option	Task
<b>Power ON</b>	Power on the host.
<b>Power OFF</b>	Immediately power off the host.
<b>Software Shutdown</b>	Soft power off the host.
<b>Power Reset</b>	Hard reset the host without powering off.

## Force-Enter BIOS Setup Utility Option

KVM also provides a Force-Enter BIOS Setup button. Clicking the button triggers a system DC cycle and stops in the BIOS Setup page. At the same time a pop-up window shows in the KVM page. See [Figure 73](#) and [Figure 74](#) for details.



**Figure 73. Force-Enter BIOS Setup Button**



**Figure 74. Force-Enter BIOS Setup Pop-Up Window**

## Appendix C. Glossary

Term	Definition
<b>BMC</b>	Baseboard Management Controller
<b>CPLD</b>	Complex programmable logic device
<b>Intel® CTO</b>	Intel Configure To Order Tool – An on-line tool used to order fully integrated L9 systems directly from Intel.
<b>Intel® DCM</b>	Intel® Data Center Manager
<b>DHCP</b>	Dynamic Host Configuration Protocol
<b>DNS</b>	Domain Name System
<b>FQDN</b>	Fully qualified domain name
<b>HBA</b>	Host bus adapter
<b>HSBP</b>	Hot-swap backplane
<b>I/O</b>	Input/output.
<b>IPMI</b>	Intelligent Platform Management Interface
<b>KCS</b>	Keyboard Controller Style
<b>KVM</b>	Keyboard, Video, Mouse
<b>LAN</b>	Local Area Network
<b>LDAP</b>	Lightweight Directory Address Protocol
<b>MAC</b>	Media access controller
<b>Intel® ME</b>	Intel® Management Engine
<b>NIC</b>	Network Interface Controller
<b>Intel® NM</b>	Intel® Node Manager
<b>NTP</b>	Network Time Protocol
<b>NVMe*</b>	Non-Volatile Memory Express*
<b>OOB</b>	Out of band – no operating system interaction on server
<b>PCIe*</b>	Peripheral Component Interconnect Express*
<b>POST</b>	Power-on self-test
<b>SEL</b>	System event log
<b>SDDC</b>	Software-defined data center
<b>SDR</b>	Sensor data record
<b>SMBIOS</b>	System Management BIOS
<b>SOL</b>	Serial-over-LAN
<b>SSH</b>	Secure socket shell
<b>SSL</b>	Secure Sockets Layer
<b>TCP/IP</b>	Transmission Control Protocol/Internet Protocol
<b>UDP</b>	User Datagram Protocol
<b>VLAN</b>	Virtual Local Area Network