Intel® Integrated Baseboard Management Controller Web Console (Intel® Integrated BMC Web Console)

User Guide

For the Intel® Server System M70KLP family.

Rev. 1.0

June 2021

Delivering Breakthrough Data Center System Innovation – Experience What's Inside!

<This page intentionally left blank>

Document Revision History

Date	Revision	Changes
June 2021	1.0	Initial 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.

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

Table of Contents

List of Figures

List of Tables

1. Introduction

This user guide describes how to use the Intel® Integrated Baseboard Management Controller Web Console (Intel® Integrated BMC Web Console). It also offers an overview of the web console features.

The Intel® Integrated BMC Web Console provides both exceptional stability and permanent availability, no matter the present state of the server operating system. As a system administrator, use the Intel® Integrated BMC Web Console to gain location-independent remote access to respond to critical incidents and to undertake necessary maintenance.

From the Intel® Server System M70KLP BMC enabled remote keyboard, video, and mouse (KVM) and media redirection on the server system through the built-in web console, from anywhere, at any time.

1.1 Support Information

Visit https://www.intel.com/content/www/us/en/support.html for support on the Intel® Integrated BMC Web Console. The support page provides the following:

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

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

1.2 Warranty Information

Visit https://www.intel.com/content/www/us/en/support/articles/000006361/services.html to obtain warranty information.

2. Advanced System Management Feature

This section explains the advanced management features supported by the BMC firmware and highlights significant benefits of its features.

2.1 Advanced Management Features Overview

The advanced management features are delivered as part of the BMC firmware image, starting with Intel® Server System M70KLP family moving to a software license key to activate BMC advanced management features.

Advanced manageability features are supported over all NIC ports enabled for server manageability. This includes baseboard integrated BMC-shared NICs that share network bandwidth with the host system, and the LAN channel provided by the onboard Intel® Dedicated Server Management NIC.

Standard features that do not require a key:

- Virtual KVM over HTML5
- Intel® Integrated BMC Web Console
- Redfish* 2.0
- IPMI 2.0
  - Intel® Node Manager (Intel® NM)
- Email Alerting
- Out-of-Band BIOS/BMC Update and Configuration
- System Inventory
- Autonomous Debug Log

Advanced features require software key:

- Software Key to enable features
- Included single system license for Intel® Data Center Manager (Intel® DCM)
  - Intel® DCM is a software solution that collects and analyzes the real-time health, power, and thermals of a variety of devices in data centers. Intel® DCM helps to improve the efficiency and uptime. Go to https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html for more information.
- Virtual Media Image Redirection (HTML5 and Java*)
- Virtual Media over network share and local folder
- Active Directory* (AD*) support

❖ Full system firmware update including drives, memory, and RAID (available in Q4 2021).
❖ Storage and network device monitoring (available in Q4 2021).
❖ Out-of-band hardware RAID Management for latest Intel® RAID cards (available in Q4 2021).

2.1.1 Standard and Advanced System Management Features Details

The following tables present descriptions for the Intel® Integrated BMC Web Console standard and advanced features.

Table 1. Standard System Management Features

Feature	Description
Virtual KVM over HTML5	The BMC firmware supports keyboard, video, and mouse redirection (KVM) over LAN. This feature is available remotely from the embedded web server as an HTML5 application. USB1.1 or USB 2.0 based mouse and keyboard redirection are supported. Another option is to use the KVM-redirection (KVM-r) session concurrently with media-redirection (media-r). This feature allows a user to interactively use the remote server KVM functions as if the user were physically at the managed server. KVM redirection consoles support the following keyboard layouts: English, Chinese (traditional), Japanese, German, French, Spanish, Korean, Italian, and United Kingdom. KVM redirection includes a “soft keyboard” function. The “soft keyboard” simulates an entire keyboard that is connected to the remote system. The “soft keyboard” function supports the following layouts: English, Dutch, French, German, Italian, Russian, and Spanish. The KVM-r feature automatically senses video resolution for the best possible screenshot and provides high-performance mouse tracking and synchronization. It allows remote view and configuration in pre-boot POST and BIOS Setup, once BIOS has initialized video.
Intel® Integrated BMC Web Console	The BMC firmware has an embedded web server that can remotely serve webpages to any supported browser. This web console allows the administrator to view system information including firmware versions, server health, diagnostic information, power statistics. It enables the BMC and BIOS configuration. It lets users perform power actions, launch KVM and set up virtual media redirection.
Redfish*	The BMC supports several Redfish* schemas. The BMC currently supports version 1.8 and schema version 2019.2. DMTF’s Redfish* is a standard that delivers simple and secure management for converged, hybrid IT and the software defined data center (SDDC). Both human readable and machine capable, Redfish* uses common Internet and web services standards to expose information directly to the modern tool chain.
IPMI 2.0	The BMC is IPMI 2.0 compliant including support for Intel® NM. IPMI defines a set of interfaces used by system administrators for computer systems’ out-of-band management and their operation monitoring.
Out-of-band BIOS/BMC update and configuration	The BMC supports Redfish* schemas and embedded web console features that allow administrators to update the BMC, BIOS, Intel® ME and SDR firmware. The BMC firmware also includes Power Supply and Backplane firmware. The BMC update happens immediately and causes a BMC reset to occur at the end. The BIOS and Intel® ME firmware is staged in the BMC and are updated on the next reboot. The BMC also supports Redfish* and embedded web console feature to view and change BIOS settings. On each boot, BIOS provides all its settings and active value to the BMC to be displayed. It also checks if any changes are requested and performs those changes.
System inventory	The BMC supports Redfish* schemas and embedded web console pages to display system inventory. This inventory includes FRU information, CPU, memory, networking, and storage. When applicable, also the firmware version is provided.

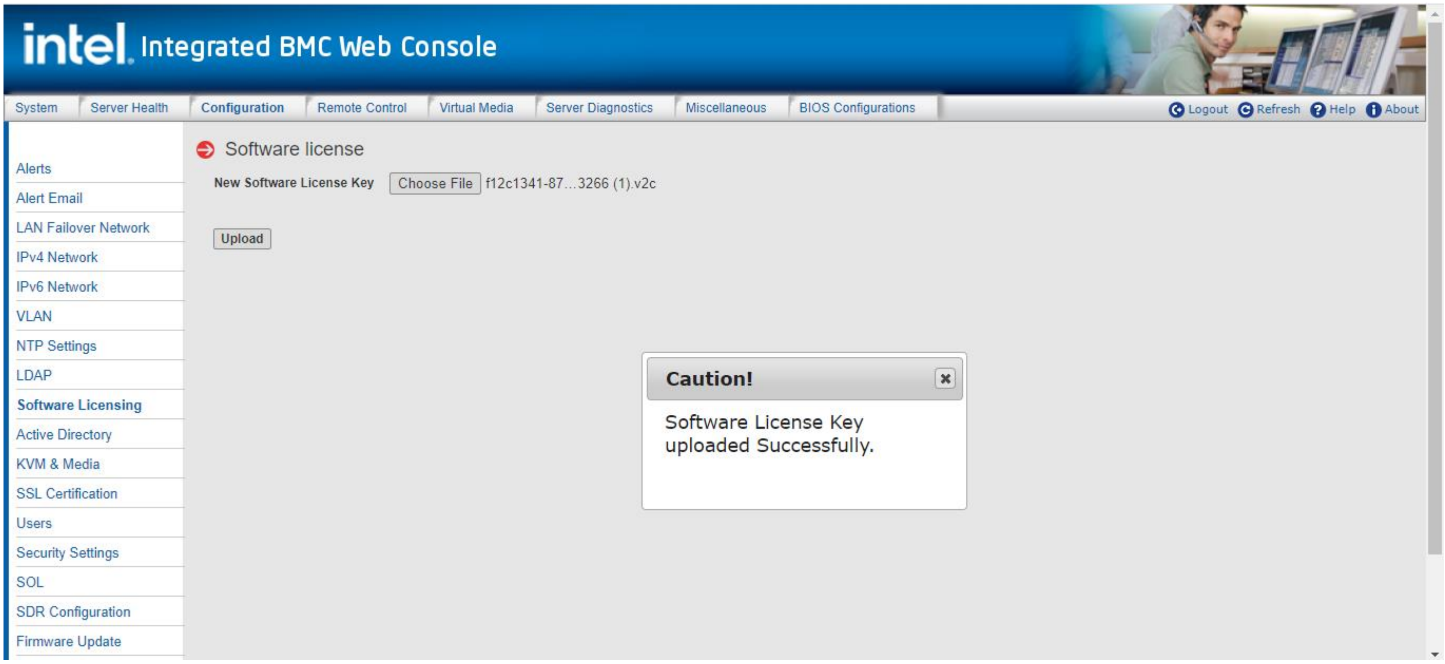
Feature	Description
Autonomous debug log	The BMC has a debug log that can be downloaded to facilitate support issues. This debug log can be downloaded from the embedded web console or via syscfg and Intel® Server Debug and Provisioning Tool (Intel® SDP Tool) utilities. The debug log has configuration data including SDR, SEL, BMC configuration, PCI configuration, power supply configuration and power supply black box data. The debug log also contains SMBIOS data and the POST codes from the last two boots. Finally, when the system has a catastrophic error condition that leads to a system shutdown, the BMC holds the CPU in reset long enough to collect machine check registers of the processor, machine check registers of the memory controller, error registers of the I/O global, and other state information of the processor.
Security features	The BMC contains several security features including OpenLDAP* and AD*, security logs, ability to turn off any remote port, SSL certificate upload, VLAN support, and KCS control. The BMC also supports full user management with the ability to define password complexity rules. Each BMC release is given a security version number to prevent firmware downgrades from going to lower security versions. Intel provides a security guide with best practices, available at https://www.intel.com/content/www/us/en/support/articles/000055785/server-products.html.
Eventing	The BMC supports alerting based on system issues. The BMC supports SNMP traps, email alerting (SMTP) and Redfish* event subscriptions.

Table 2. Advanced System Management Features

Features	Descriptions
Software key to enable features	The BMC supports a method to upload advanced system management license files to enable the following features. The license file can be uploaded via embedded web console, Redfish* and syscfg. *Not all features are available at launch.*
Single license for Intel® DCM	All systems that have the Advanced System Management Key uploaded can be managed by Intel® DCM for free. Intel® DCM comes with a 30-day trial. However, when the trial expires, all systems with this key can continue to be managed. Intel® DCM lets administrators manage and monitor the health, power, thermals, utilization, inventory and firmware versions of servers across the user's entire data center. Go to https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html?wapkw=DCM for more information on Intel® DCM.
Virtual media image redirection (HTML5 and Java*)	The BMC supports media redirection of local folders and .IMG and .ISO image files. This redirection is supported in both HTML5 and Java remote console clients. To enable virtual media redirection over HTML5 or Java*, the software license key should be uploaded to the WebUI. Navigate to **Configuration** > **Software Licensing** and upload the software licensing key. See Figure 1.
Virtual media over HTML5	When the user selects **Virtual Media over HTML5**, a new webpage is displayed. Click **Browse** to select CD Image. After selecting the image, **Select/Unselect** media boost option. Click **Start Media** to redirect the selected CD image file to the Host. A sample screenshot is shown in Figure 2. **Notes:** • If media boost mode is selected, the processes related to media redirection get higher priority than other processes. This improves media performance, but other processes get limited access to CPU cycle. • If CD/DVD instance is started with media boost mode, the next CD/DVD instance is started without any pop-up message. To stop the CD Image redirection, click **Stop Media**.

Features	Descriptions
Virtual media over Java	When the user selects Launch Console in KVM/Console Redirection, the `jviewer.jnlp` file is downloaded. Launch **JViewer***. Select **CD/DVD** or **Hard disk/USB** to start the virtual media redirection. See Figure 3. • **CD/DVD Media.** This tab can be used to start or stop the redirection of a physical DVD/ CD-ROM drive and DVD/CD image file of ISO/NRG file format. • **Hard disk/USB.** This tab can be used to start or stop the redirection of a Hard Disk/USB key image and USB key image such as img/ima.
Virtual media over network share	Besides virtual media redirection from the remote workstation, the BMC supports media redirection of file folders and .IMG and .ISO files hosted on a network file server accessible to the BMC network interface. The current version supports Samba* shares (Microsoft Windows* file shares), and future versions will add support for both CIFS and NFS shares. This feature is more effective for mounting virtual media at scale. Instead of processing all files from the workstation's drive through the HTML5 application and over the workstation's network, each BMC makes a direct network file share connection to the file server and accesses files across that network share directly.
Active Directory* support	The BMC supports AD*. AD* is a directory service developed by Microsoft* for Windows* domain networks. This feature lets users log in to the web console or Redfish* via an AD* username instead of local authentication. This allows administrators to only change passwords on this single domain account, instead of doing so on every remote system.
Full system firmware update including drives, memory, and RAID[1]	The BMC supports a staging area to allow users to upload EFI utilities and supporting files that are silently executed by BIOS on the next reboot. Examples include firmware update for SSD, network, RAID, or other components that have EFI utilities. The user can also use this feature to collect inventory data or configure advanced RAID options. Redfish* schemas support both the uploading and downloading of files. Intel® SDP Tool and Intel® DCM use this region to perform multiple firmware update tasks.
Storage and network device monitoring[1]	The BMC supports the MCTP protocol, which allows the monitoring of storage and networking devices. This includes asset inventory including firmware versions, link status and health.
Out-of-band hardware RAID management[1]	The BMC supports basic RAID management of latest generation Intel® RAID cards. The BMC can see asset inventory of all drives behind RAID controllers, view RAID health and do basic RAID 0/1 configuration intended for boot virtual drives.

[1] Available post launch.



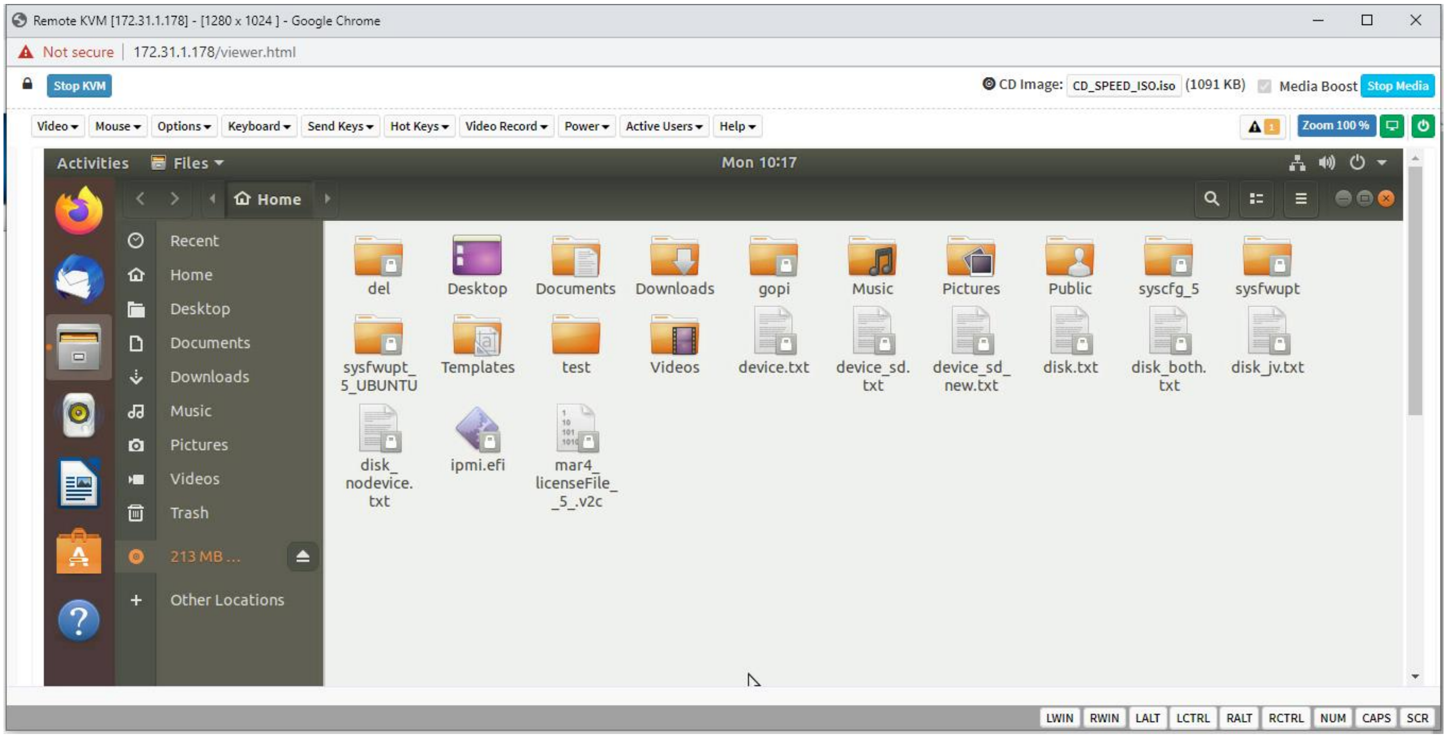
Software license

New Software License Key: f12c1341-87...3266 (1).v2c

Caution!

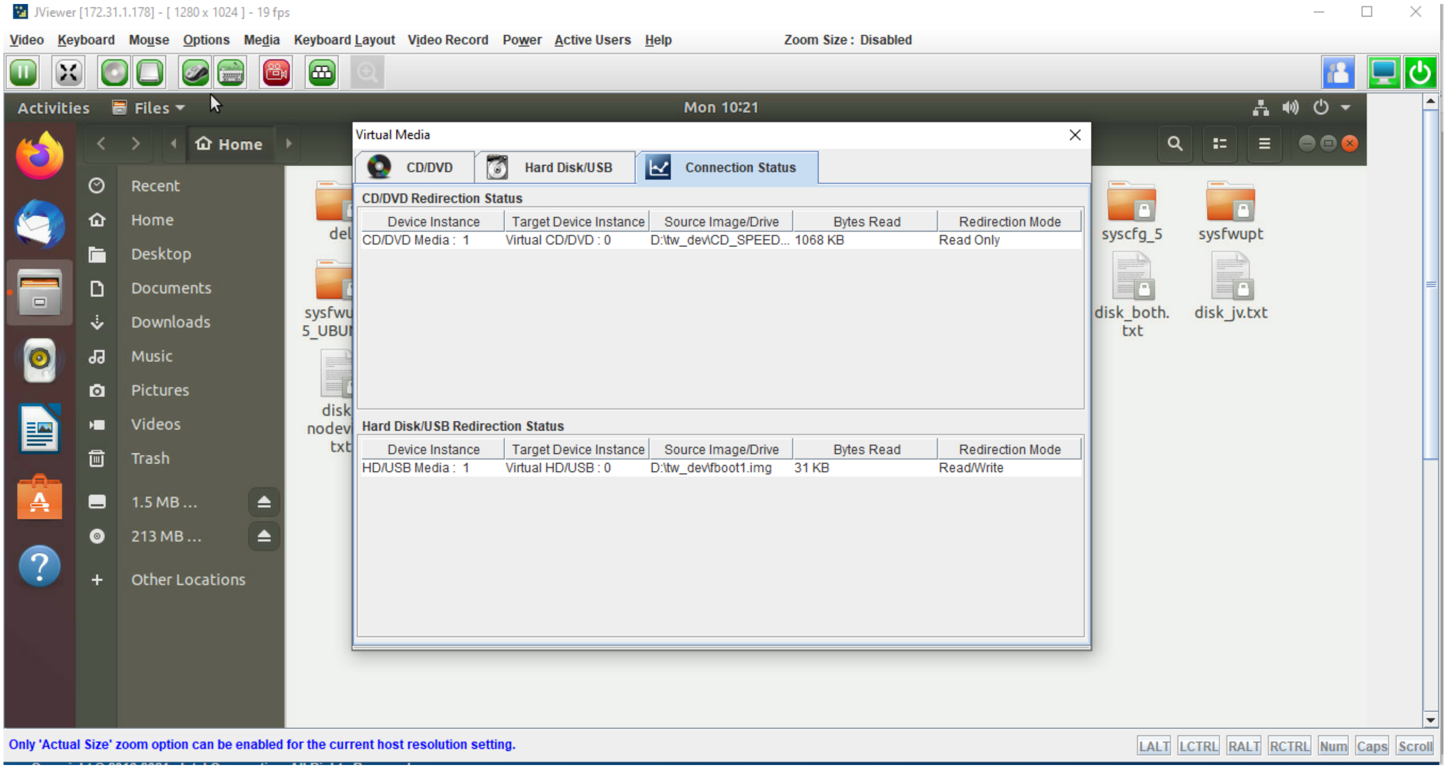
Software License Key uploaded Successfully.

Figure 1. Software License Key Upload to the WebUI



CD Image: CD_SPEED_ISO.iso (1091 KB)

Figure 2. Stop CD Image Redirection for Virtual Media over HTML5



CD/DVD Redirection Status

Device Instance	Target Device Instance	Source Image/Drive	Bytes Read	Redirection Mode
CD/DVD Media : 1	Virtual CD/DVD : 0	D:\tw_dev\CD_SPEED...	1068 KB	Read Only

Hard Disk/USB Redirection Status

Device Instance	Target Device Instance	Source Image/Drive	Bytes Read	Redirection Mode
HD/USB Media : 1	Virtual HD/USB : 0	D:\tw_dev\fboot1.img	31 KB	Read/Write

Only 'Actual Size' zoom option can be enabled for the current host resolution setting.

Figure 3. Start Virtual Media over Java

2.2 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:

- Ubuntu* 16.04 of 64 bit: Chrome* 69.0.3497.100
- Ubuntu* 16.04 of 64 bit: Firefox* 64.0
- Windows Server* 2016 of 64 bit: Chrome* 73.0.3683.86 of 64 bit
- Windows Server* 2016 of 64 bit: Firefox* 66.0.2

3. Advanced Management Key Installation

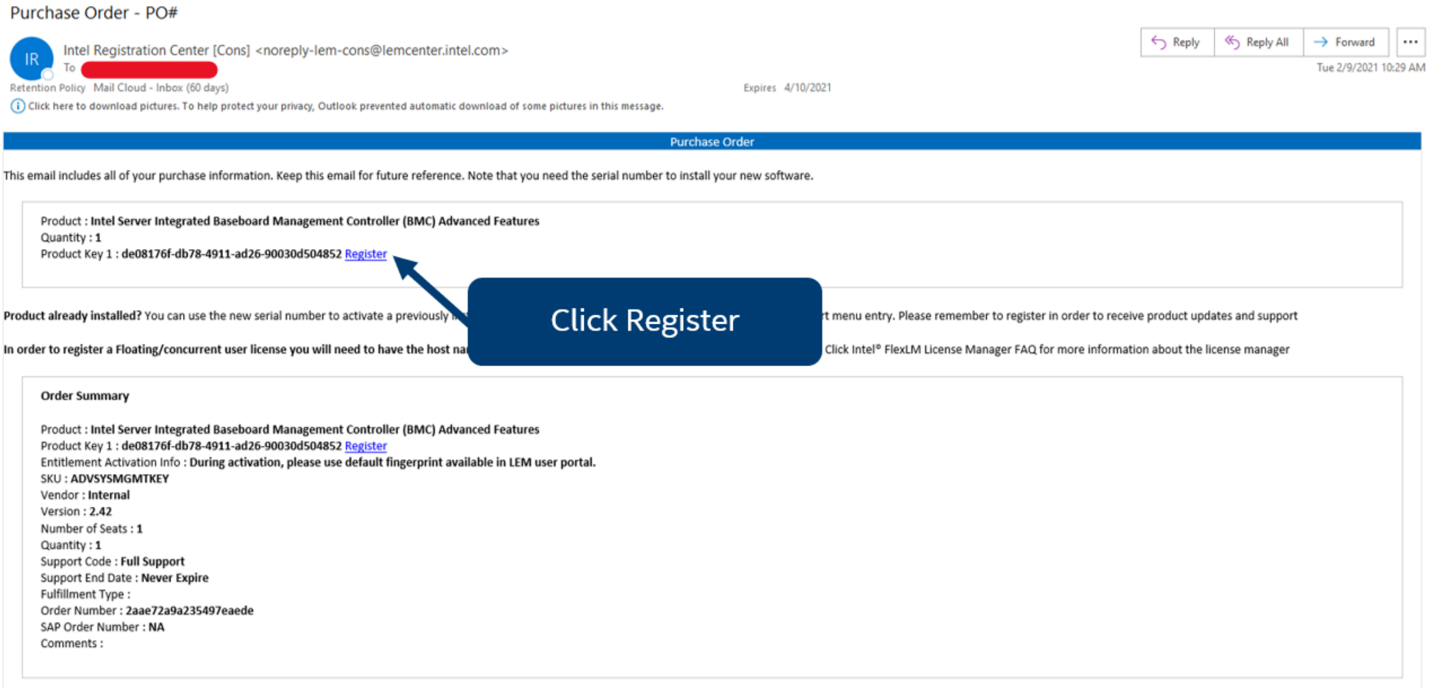
3.1 How to Order Advanced System Management Key

- **Level 9 (L9).** If ordering a fully integrated system, select the **AdvSysMgmtKey** in the Intel® Configure to Order (Intel® CTO) portal. The Intel factory automatically uploads the license key during the system integration.
- **Accessory.** If ordering as an individual accessory via Intel® Web Order Management (Intel® WOM), follow the steps in Section 3.1.1 to receive the license file and upload to the BMC.

3.1.1 Order as an Accessory (Not Via Intel®CTO)

1. Place the order via Intel® WOM like any other component.
2. Receive an email with the product key.
   - ○ Depending on how it was ordered, it can be forwarded from distributor or reseller.
3. Click the link on the email to go to https://lemcenter.intel.com to register, activate and download the license file for that product key.
   - ○ Use an existing Intel account or create one from the website. An email address is required.
4. Use the Intel® Integrated BMC Web Console or syscfg to upload the key to the BMC.
   - ○ Only a 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.



Purchase Order - PO#

Intel Registration Center [Cons] <noreply-lem-cons@lemcenter.intel.com>

To [redacted]

Tue 2/9/2021 10:29 AM

Retention Policy Mail Cloud - Inbox (60 days) Expires 4/10/2021

Click here to download pictures. To help protect your privacy, Outlook prevented automatic download of some pictures in this message.

Purchase Order

This email includes all of your purchase information. Keep this email for future reference. Note that you need the serial number to install your new software.

Product : **Intel Server Integrated Baseboard Management Controller (BMC) Advanced Features**
Quantity : **1**
Product Key 1 : **de08176f-db78-4911-ad26-90030d504852** Register

Product already installed? You can use the new serial number to activate a previously t menu entry. Please remember to register in order to receive product updates and support

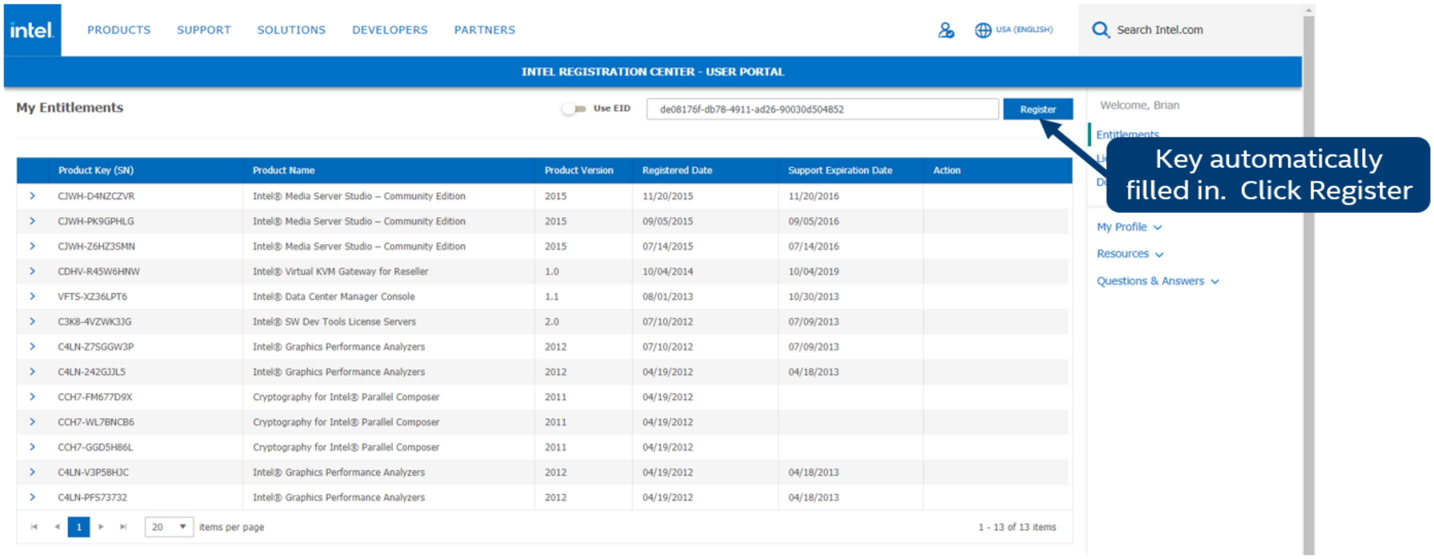
In order to register a Floating/concurrent user license you will need to have the host na Click Intel® FlexLM License Manager FAQ for more information about the license manager

Order Summary

Product : **Intel Server Integrated Baseboard Management Controller (BMC) Advanced Features**
Product Key 1 : **de08176f-db78-4911-ad26-90030d504852** Register
Entitlement Activation Info : **During activation, please use default fingerprint available in LEM user portal.**
SKU : **ADVSYSMGMTKEY**
Vendor : **Internal**
Version : **2.42**
Number of Seats : **1**
Quantity : **1**
Support Code : **Full Support**
Support End Date : **Never Expire**
Fulfillment Type :
Order Number : **2aae72a9a235497eaede**
SAP Order Number : **NA**
Comments :

Click Register

Figure 4. Example Email



My Entitlements

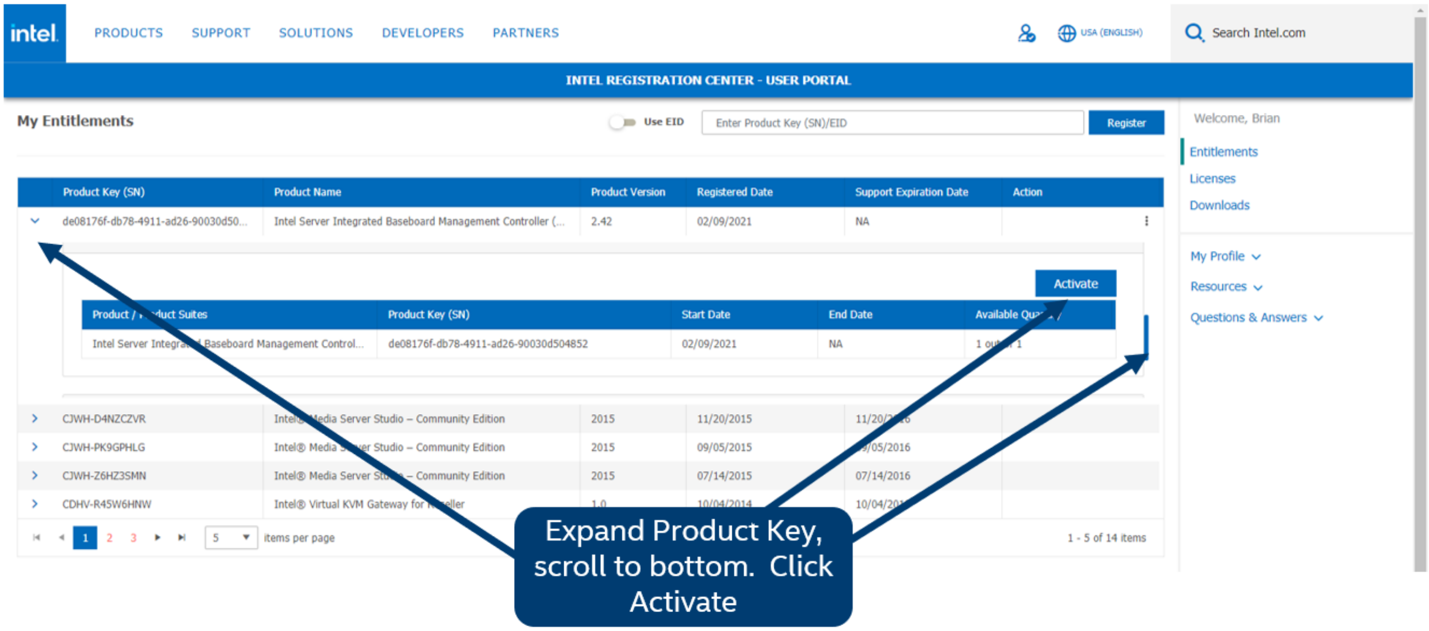
Use EID de08176f-db78-4911-ad26-90030d504852 Register

	Product Key (SN)	Product Name	Product Version	Registered Date	Support Expiration Date	Action
>	CJWH-D4NZCZVR	Intel® Media Server Studio – Community Edition	2015	11/20/2015	11/20/2016	
>	CJWH-PK9GPHLG	Intel® Media Server Studio – Community Edition	2015	09/05/2015	09/05/2016	
>	CJWH-Z6HZ3SMN	Intel® Media Server Studio – Community Edition	2015	07/14/2015	07/14/2016	
>	CDHV-R45W6HNW	Intel® Virtual KVM Gateway for Reseller	1.0	10/04/2014	10/04/2019	
>	VFTS-XZ36LPT6	Intel® Data Center Manager Console	1.1	08/01/2013	10/30/2013	
>	C3K8-4VZWK3JG	Intel® SW Dev Tools License Servers	2.0	07/10/2012	07/09/2013	
>	C4LN-Z7SGGW3P	Intel® Graphics Performance Analyzers	2012	07/10/2012	07/09/2013	
>	C4LN-242GJJL5	Intel® Graphics Performance Analyzers	2012	04/19/2012	04/18/2013	
>	CCH7-FM677D9X	Cryptography for Intel® Parallel Composer	2011	04/19/2012		
>	CCH7-WL7BNCB6	Cryptography for Intel® Parallel Composer	2011	04/19/2012		
>	CCH7-GGD5H86L	Cryptography for Intel® Parallel Composer	2011	04/19/2012		
>	C4LN-V3P58HJC	Intel® Graphics Performance Analyzers	2012	04/19/2012	04/18/2013	
>	C4LN-PFS73732	Intel® Graphics Performance Analyzers	2012	04/19/2012	04/18/2013	

1 | 20 items per page | 1 - 13 of 13 items

Key automatically filled in. Click Register

Figure 5. Register Key



My Entitlements

Use EID Enter Product Key (SN)/EID Register

	Product Key (SN)	Product Name	Product Version	Registered Date	Support Expiration Date	Action
⌄	de08176f-db78-4911-ad26-90030d50...	Intel Server Integrated Baseboard Management Controller (...	2.42	02/09/2021	NA	⋮

Activate

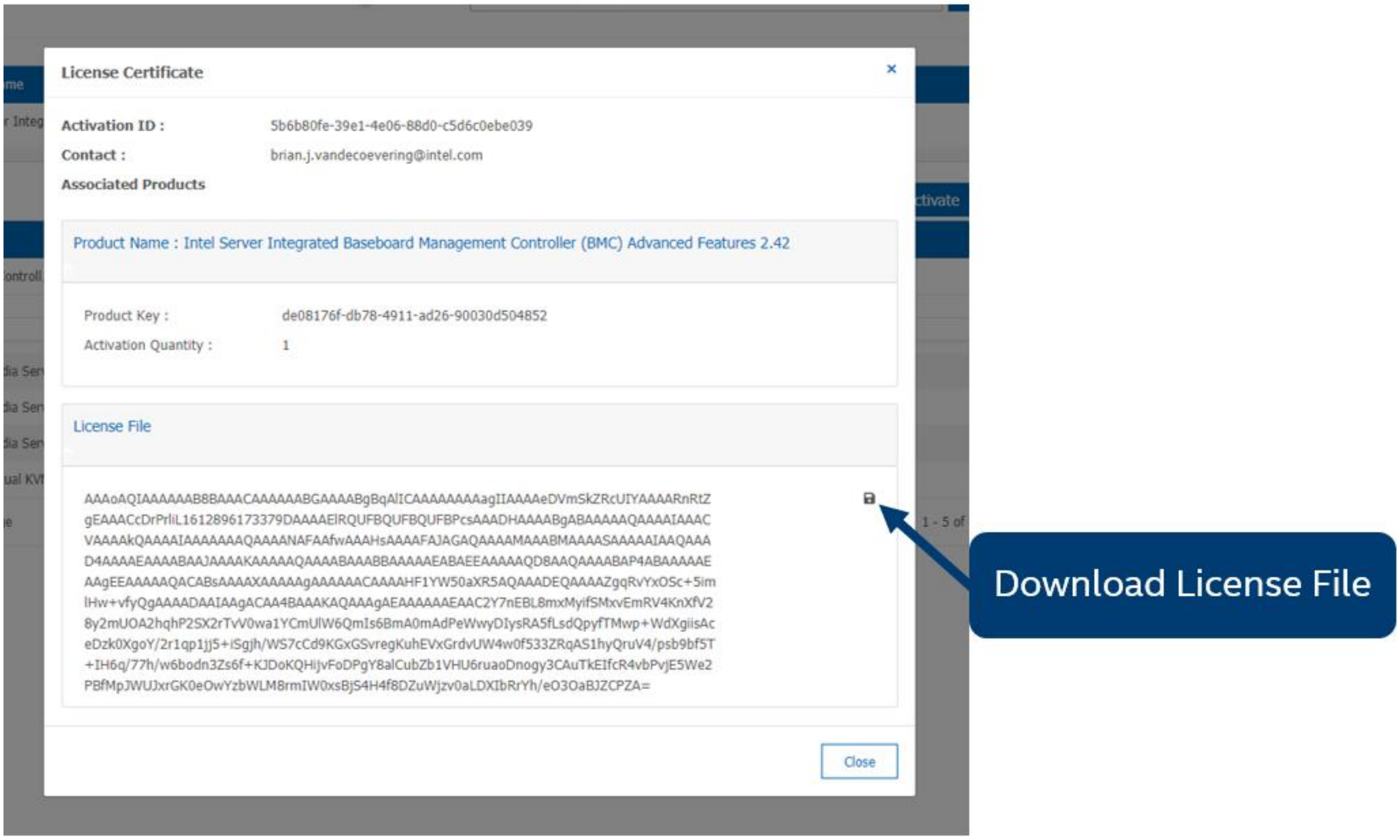
Product / Product Suites	Product Key (SN)	Start Date	End Date	Available Quantity
Intel Server Integrated Baseboard Management Control...	de08176f-db78-4911-ad26-90030d504852	02/09/2021	NA	1 out of 1

	Product Key (SN)	Product Name	Product Version	Registered Date	Support Expiration Date	Action
>	CJWH-D4NZCZVR	Intel® Media Server Studio – Community Edition	2015	11/20/2015	11/20/2016	
>	CJWH-PK9GPHLG	Intel® Media Server Studio – Community Edition	2015	09/05/2015	09/05/2016	
>	CJWH-Z6HZ3SMN	Intel® Media Server Studio – Community Edition	2015	07/14/2015	07/14/2016	
>	CDHV-R45W6HNW	Intel® Virtual KVM Gateway for Reseller	1.0	10/04/2014	10/04/2019	

1 2 3 | 5 items per page | 1 - 5 of 14 items

Expand Product Key, scroll to bottom. Click Activate

Figure 6. Activate Key



License Certificate

Activation ID : 5b6b80fe-39e1-4e06-88d0-c5d6c0ebe039

Contact : brian.j.vandecoevering@intel.com

Associated Products

Product Name : Intel Server Integrated Baseboard Management Controller (BMC) Advanced Features 2.42

Product Key : de08176f-db78-4911-ad26-90030d504852

Activation Quantity : 1

License File

```
AAAoAQIAAAAAAB8BAAACAAAAAABGAAAABgBqAlICAAAAAAAAagIIAAAAeDVmSkZRcUIYAAAARnRtZ
gEAAACcDrPrliL1612896173379DAAAAElRQUFBQUFBQUFBPcsAAADHAAAABgABAAAAAQAAAAIAAAC
VAAAAkQAAAAIAAAAAAAQAAAANAFAAfwAAAHsAAAAFAJAGAQAAAAMAAABMAAAASAAAAAIAAQAAA
D4AAAAEAAAABAAJAAAAKAAAAAQAAAABAAABBAAAAAEABAEEAAAAAQD8AAQAAAABAP4ABAAAAAE
AAgEEAAAAAQACABsAAAAXAAAAAgAAAAAACAAAAHF1YW50aXR5AQAAADEQAAAAZgqRvYxOSc+5im
lHw+vfyQgAAAADAAIAAgACAA4BAAAKAQAAAgAEAAAAAAEAAC2Y7nEBL8mxMyifSMxvEmRV4KnXfV2
8y2mUOA2hqhP2SX2rTvV0wa1YCmUlW6QmIs6BmA0mAdPeWwyDIysRA5fLsdQpyfTMwp+WdXgiisAc
eDzk0XgoY/2r1qp1jj5+iSgjh/WS7cCd9KGxGSvregKuhEVxGrdvUW4w0f533ZRqAS1hyQruV4/psb9bf5T
+IH6q/77h/w6bodn3Zs6f+KJDoKQHijvFoDPgY8alCubZb1VHU6ruaoDnogy3CAuTkEIfcR4vbPvjE5We2
PBfMpJWUJxrGK0eOwYzbWLM8rmIW0xsBjS4H4f8DZuWjzv0aLDXIbRrYh/eO3OaBJZCPZA=
```

Close

Download License File

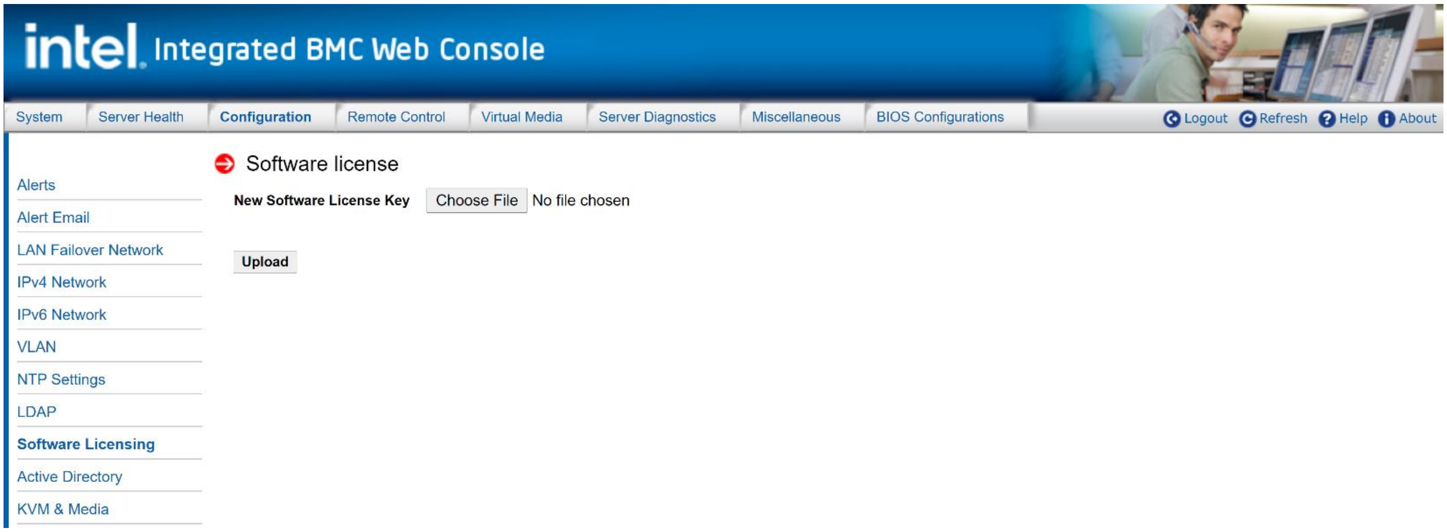
Figure 7. Download Key

3.2 Advanced Management Key Installation

The user has three options to upload the key: Intel® Integrated BMC Web Console, syscfg, and Redfish*.

3.2.1 Installation Procedure

The user can navigate to Software Licensing under Configuration to upload the key. All advanced features are activated immediately after the key upload.



Software license

New Software License Key Choose File No file chosen

Figure 8. Software License Page

4. Server Management Hardware Configuration

This section explains how to use the server utilities to enable a system to use the Intel® Integrated BMC Web Console from a new, unset state to an operational state.

The system default user/password is admin/admin.

One step is necessary before the server management BMC LAN can be used:

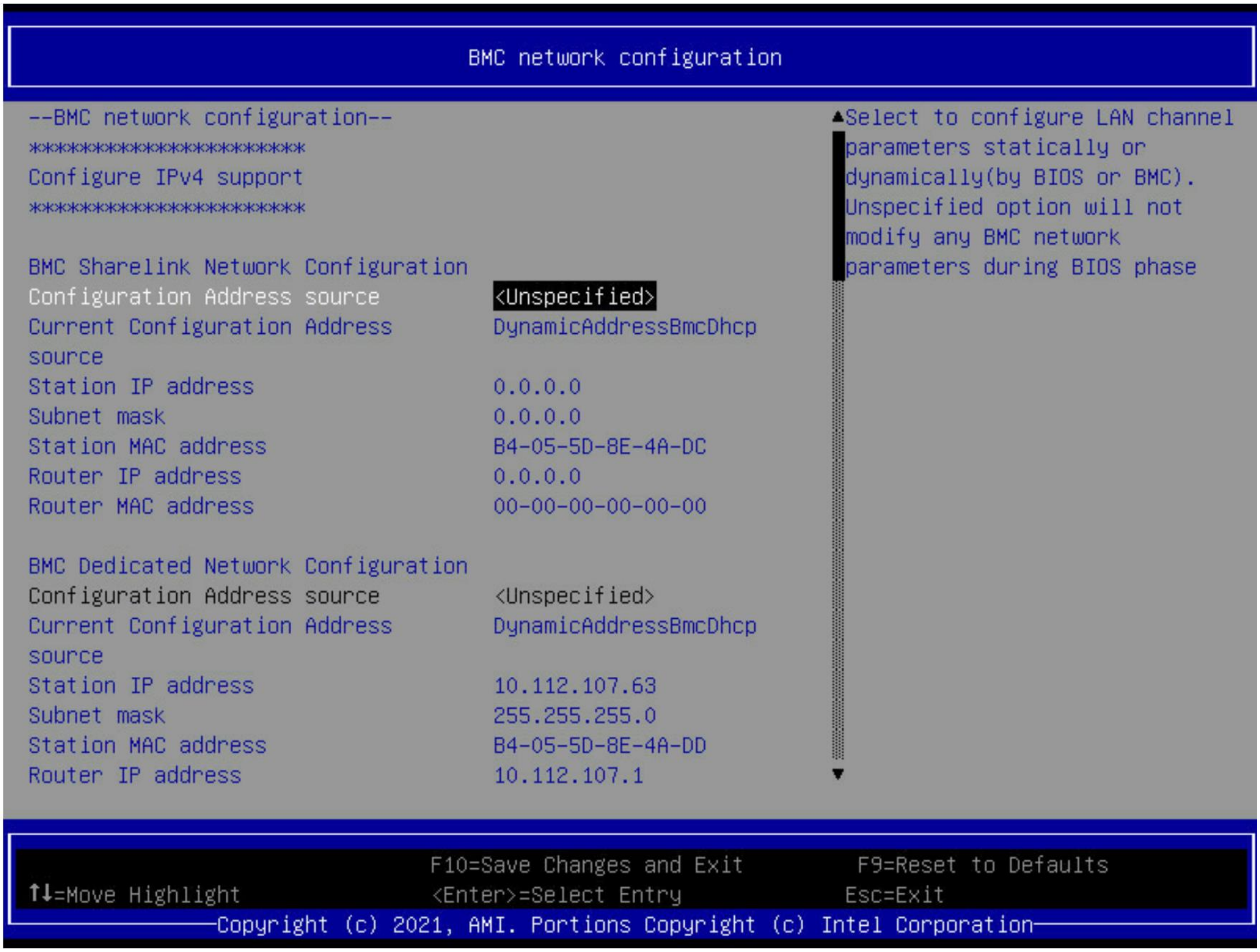
- One or both LAN channels must be configured as either DHCP or static addresses.

The server management BMC LAN can be configured in multiple ways:

- Using BIOS Setup.
- Using Save and Restore System Configuration Utility (syscfg) (available at http://downloadcenter.intel.com/default.aspx).
- Using IPMI commands.

4.1 Server Management Hardware Configuration Using BIOS Setup

1. During POST, press **<Esc>** to go to the BIOS Setup main page.
2. Navigate to the **Server Mgmt** tab and select **BMC network configuration** to enter the **BMC network configuration** screen (see Figure 9).
3. For an IPv4 network:
    - If configuring the server management BMC LAN, scroll to **BMC Sharelink Network Configuration** > **Configuration Address source** then select either **Unspecified**, **Static**, **DynamicBmcDhcp** or **DynamicBmcNonDhcp**. If **Static** is selected, configure the **IP address**, **Subnet mask**, **Router IP** and **Router MAC address** as needed.
    - If configuring the advanced management feature, scroll down to **BMC Dedicated Network Configuration** > **Configuration Address source** and then select either **Unspecified**, **Static**, **DynamicBmcDhcp** or **DynamicBmcNonDhcp**. If **Static** is selected, configure the **IP address**, **Subnet mask**, **Router IP** and **Router MAC address** as needed.
4. For an IPv6 network:
    - If configuring the server management BMC LAN, Set IPv6 **Support = Enabled**, scroll down to **Configuration Address source** and then select either **Unspecified**, **Static** or **DynamicBmcDhcp**. If **Static** is selected, configure the **Station IP address**, **Subnet mask**, **Router IP** and **Router MAC address** as needed. If **Static** is selected, configure the **IPV6 address**, and **IPV6 Prefix Length** as needed.
5. Press **<F10>** to save the configured settings and exit BIOS Setup. The server reboots with the new LAN settings.



```
                              BMC network configuration

--BMC network configuration--                                 Select to configure LAN channel
*********************                                         parameters statically or
Configure IPv4 support                                        dynamically(by BIOS or BMC).
*********************                                         Unspecified option will not
                                                              modify any BMC network
BMC Sharelink Network Configuration                           parameters during BIOS phase
Configuration Address source         <Unspecified>
Current Configuration Address        DynamicAddressBmcDhcp
source
Station IP address                   0.0.0.0
Subnet mask                          0.0.0.0
Station MAC address                  B4-05-5D-8E-4A-DC
Router IP address                    0.0.0.0
Router MAC address                   00-00-00-00-00-00

BMC Dedicated Network Configuration
Configuration Address source         <Unspecified>
Current Configuration Address        DynamicAddressBmcDhcp
source
Station IP address                   10.112.107.63
Subnet mask                          255.255.255.0
Station MAC address                  B4-05-5D-8E-4A-DD
Router IP address                    10.112.107.1

                                 F10=Save Changes and Exit          F9=Reset to Defaults
↑↓=Move Highlight                <Enter>=Select Entry              Esc=Exit
                Copyright (c) 2021, AMI. Portions Copyright (c) Intel Corporation
```

Figure 9. BIOS Setup BMC LAN Configuration Screen

4.2 Server Management Hardware Configuration Using Syscfg

This section describes the basic commands needed to configure the advanced management feature using syscfg commands. This utility is supported in EFI, Linux*, and Microsoft Windows* operating systems. The commands are the same for all versions.

At a minimum, configure the settings outlined in the following sections.

Note: The examples in the following sections use the Intel® Dedicated Server Management NIC LAN channel 3. If using a different NIC, substitute the appropriate channel number; for NIC1 use channel 1 and for NIC 2 use channel 2.

4.2.1 User Configuration

1. Set the password for BMC user 2. This example sets the password to `superuser`.
   - `syscfg /u 2 “root” “superuser”`
2. Enable BMC user 2 on LAN channel 3.
   - `syscfg /ue 2 enable 3`
3. Enable the admin privilege and set the payload type to SOL+KVM for BMC user 2 on LAN channel 3.
   - `syscfg /up 2 3 admin sol+kvm`

4.2.2 IP Address Configuration

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 Dynamic Host Configuration Protocol`

4.2.3 Serial-Over-LAN (SOL) Configuration

1. If needed, enable serial-over-LAN (SOL) on LAN channel 3.
   - `syscfg /sole 3 Enable Admin <BAUD_RATE> <RETRY_COUNT> <RETRY_INTERVAL_IN_MILLISECONDS>`

5. Advanced Management Feature Operation

The advanced management feature enables remote KVM access and control through LAN or Internet. The Intel® Integrated BMC Web Console is part of the standard BMC firmware/server management software and it gives access to the remote KVM. This section provides basic information needed to access both interfaces. The Intel® Integrated BMC Web Console and the remote console interfaces are respectively described in detail in Section 6 and Section 7.

For initial setup information, including enabling the intended user, see Section 4. The examples in that section use `user root`, but other usernames and passwords could be used.

5.1 Client Browsers

The advanced management features can be accessed using a standard Java*-enabled 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). Some older browsers may not have a strong 128-bit encryption algorithm.

To use the managed server remote console (KVM) window, Java Runtime Environment* (JRE*) version 6 update 22 or higher must be installed.

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.

5.2 Log In

Enter the configured IP address the configured BMC onboard NIC into the web browser to open the Intel® Integrated BMC Web Console module login page (see Figure 10). To use a secure connection, type:

- `https://<IPaddress_or_Hostname>/`

Enter the username and the password, and select a language option. For example:

- **Username:** `admin`
- **Password:** `admin`
- **Language:** English

Note: The username and password are case sensitive. The printable set of ASCII characters can be used for username and password.

Click the **Login** button to view the homepage.

After the initial login, system administrators may change passwords and create users, and have full control over access to the advanced management features.

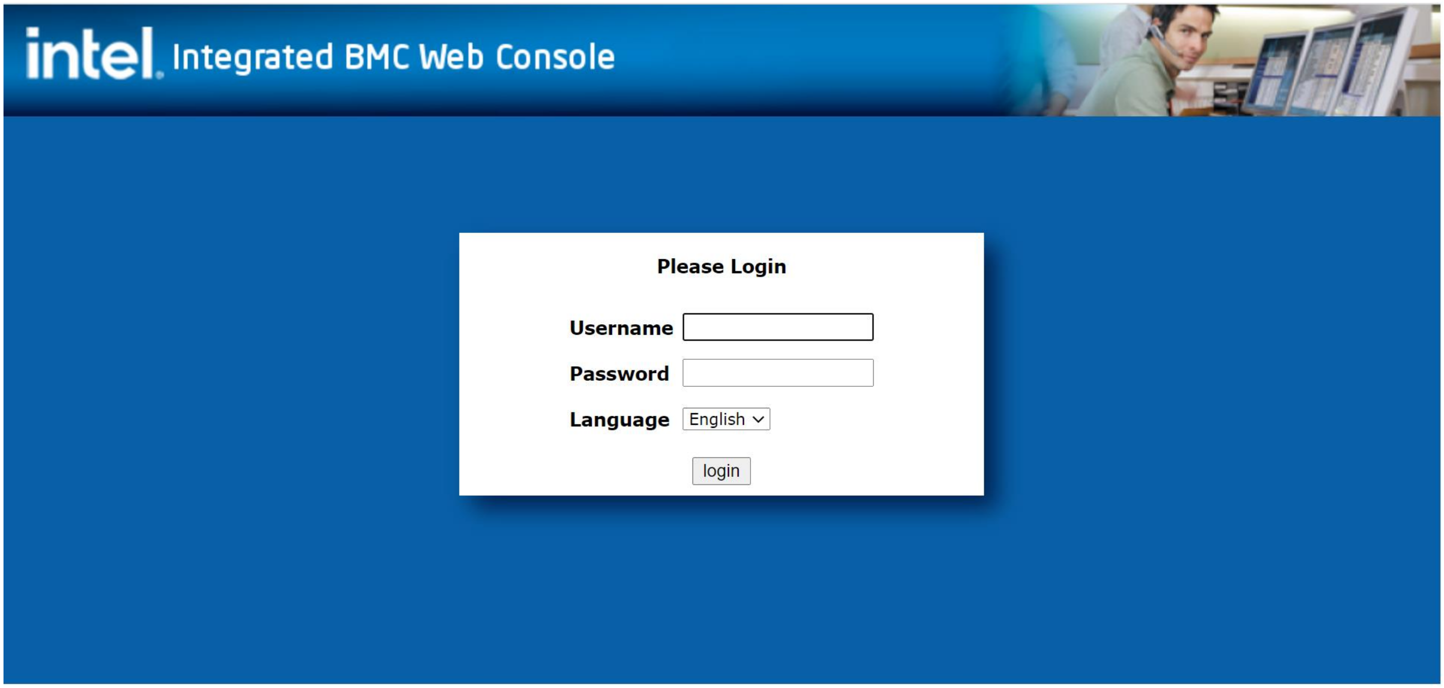
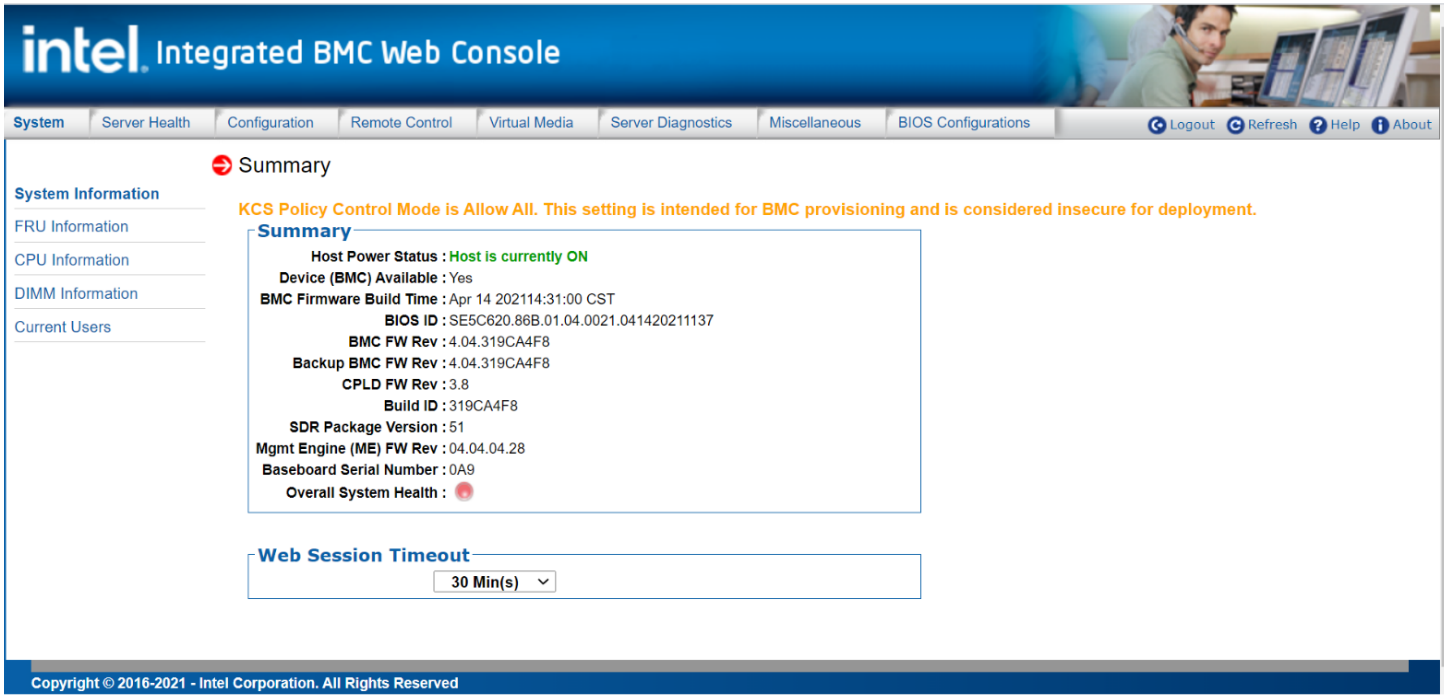


Figure 10. Intel® Integrated BMC Web Console Login Page

5.3 Navigation

The Intel® Integrated BMC Web Console homepage contains eight tabs along the top for navigation (see Figure 11). For details on each tabbed page, see Table 3. Each tab contains a secondary browser on the window left edge. For details on the specific functions of secondary menu items, see Section 7.



KCS Policy Control Mode is Allow All. This setting is intended for BMC provisioning and is considered insecure for deployment.

Summary

Host Power Status : Host is currently ON
Device (BMC) Available : Yes
BMC Firmware Build Time : Apr 14 202114:31:00 CST
BIOS ID : SE5C620.86B.01.04.0021.041420211137
BMC FW Rev : 4.04.319CA4F8
Backup BMC FW Rev : 4.04.319CA4F8
CPLD FW Rev : 3.8
Build ID : 319CA4F8
SDR Package Version : 51
Mgmt Engine (ME) FW Rev : 04.04.04.28
Baseboard Serial Number : 0A9
Overall System Health : ●

Web Session Timeout

30 Min(s)

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 11. Intel® Integrated BMC Web Console Homepage

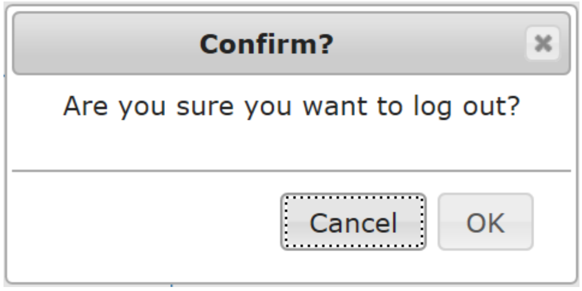
Table 3. Intel® Integrated BMC Web Console Tabs

Tab	Function	Secondary Menu
System	Provides access to general information about the server. The tab automatically opens the System Information page.	• System Information • FRU Information • CPU Information • DIMM Information • Current Users
Server Health	Provides access to the sensors and event log. The tab automatically opens the Sensor Readings page.	• Sensor Readings • Event Log
Configuration	Provides access to configure various settings for the server. The tab automatically opens the Alerts page.	• Alerts • Alert Email • LAN Failover Network • IPv4 Network • IPv6 Network • VLAN • NTP Settings • LDAP • Software Licensing • Active Directory* • KVM & Media • SSL Certification • Users • Security Settings • SOL • SDR Configuration • Firmware Update • Syslog Server Configuration • Thermal Management
Remote Control	Provides access to the remote console and to the server power state control. The tab automatically opens the KVM/Console Redirection page.	• KVM/Console Redirection • Server Power Control • Launch SOL • Virtual Front Panel • iKVM over HTML5
Virtual Media	Allows the user to share an ISO image using the SMB protocol. It allows the user to share the image over a Windows Share*, NFS Share or Linux Samba*. This image is emulated to the host as a USB device.	• Web ISO
Server Diagnostics	Provides access to server diagnostics information. The tab automatically opens the System Diagnostics page.	• System Diagnostics • POST Codes • System Defaults • SOL Log
Miscellaneous	Provides access to Intel® NM configuration, power statistics, and power telemetry. The tab automatically opens the Intel® NM Configuration page.	• Intel® NM Configuration • Power Statistics • Power Telemetry
BIOS Configuration	Provides a method to configure BIOS Setup Variables through the Intel® Integrated BMC Web Console. This submethod helps to configure only this particular BIOS Configuration, there are other options available to configure other BIOS Setup Variables.	• Advanced • Socket Configuration • Platform Configuration • Security • Server Management • Advanced Boot Options

In addition, the top of every page contains a toolbar with options explained in Table 4.

Table 4. Intel® Integrated BMC Web Console Toolbar

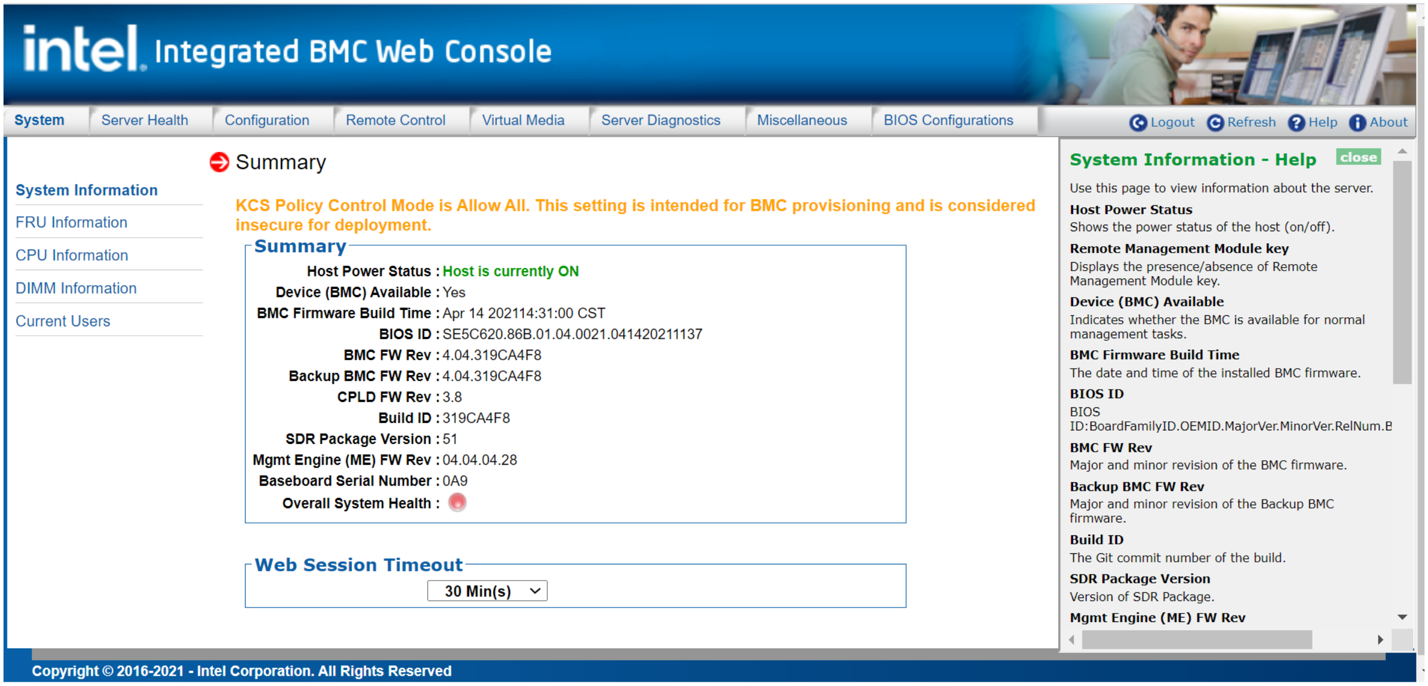
Button	Function
Logout	End the current web console session. Click **OK** to confirm (see Figure 12). After logging out, the web console returns to the login screen.
Refresh	Refresh the current webpage, including any data shown on the page. **Note:** Using the web browser refresh/reload button or pressing 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.
Help	View a brief description of the current page in a frame at the browser window right side (see Figure 13). Close the help frame by clicking the "X" in the frame upper right corner or by clicking the **Help** button again.
About	View the Intel copyright information and a statement about the use of open source code.



Confirm?

Are you sure you want to log out?

Figure 12. Log Out of the Intel® Integrated BMC Web Console



Summary

KCS Policy Control Mode is Allow All. This setting is intended for BMC provisioning and is considered insecure for deployment.

Summary

Host Power Status : Host is currently ON
Device (BMC) Available : Yes
BMC Firmware Build Time : Apr 14 202114:31:00 CST
BIOS ID : SE5C620.86B.01.04.0021.041420211137
BMC FW Rev : 4.04.319CA4F8
Backup BMC FW Rev : 4.04.319CA4F8
CPLD FW Rev : 3.8
Build ID : 319CA4F8
SDR Package Version : 51
Mgmt Engine (ME) FW Rev : 04.04.04.28
Baseboard Serial Number : 0A9
Overall System Health : ●

Web Session Timeout

30 Min(s)

System Information - Help

Use this page to view information about the server.

Host Power Status
Shows the power status of the host (on/off).

Remote Management Module key
Displays the presence/absence of Remote Management Module key.

Device (BMC) Available
Indicates whether the BMC is available for normal management tasks.

BMC Firmware Build Time
The date and time of the installed BMC firmware.

BIOS ID
BIOS ID:BoardFamilyID.OEMID.MajorVer.MinorVer.RelNum.B

BMC FW Rev
Major and minor revision of the BMC firmware.

Backup BMC FW Rev
Major and minor revision of the Backup BMC firmware.

Build ID
The Git commit number of the build.

SDR Package Version
Version of SDR Package.

Mgmt Engine (ME) FW Rev

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 13. Intel® Integrated BMC Web Console Help

Note: If there is no user activity 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.

6. Remote Console (KVM) Operation

The remote console is the remote host system's redirected KVM (keyboard, video, and mouse). To use the managed host system's remote console window, the browser must include a Java Runtime Environment* plug-in. If the browser has no Java* support, such as with a small handheld device, the user can maintain the remote host system using the administration forms displayed by the browser.

Starting the remote console opens a new window to display the host system's screen content. The remote console acts as if the administrator were sitting directly in front of the remote system screen. This means the keyboard and mouse can be used as usual.

6.1 Console Redirection Launch

On the Intel® Integrated BMC Web Console, launch the remote console KVM redirection window by clicking **Launch Console** on the Remote Control tab (see Figure 14).

Note: With Microsoft Internet Explorer*, Windows SmartScreen* is enabled, and the system is on a network with no direct connectivity to the Internet. A KVM window can take an extremely long time to open.

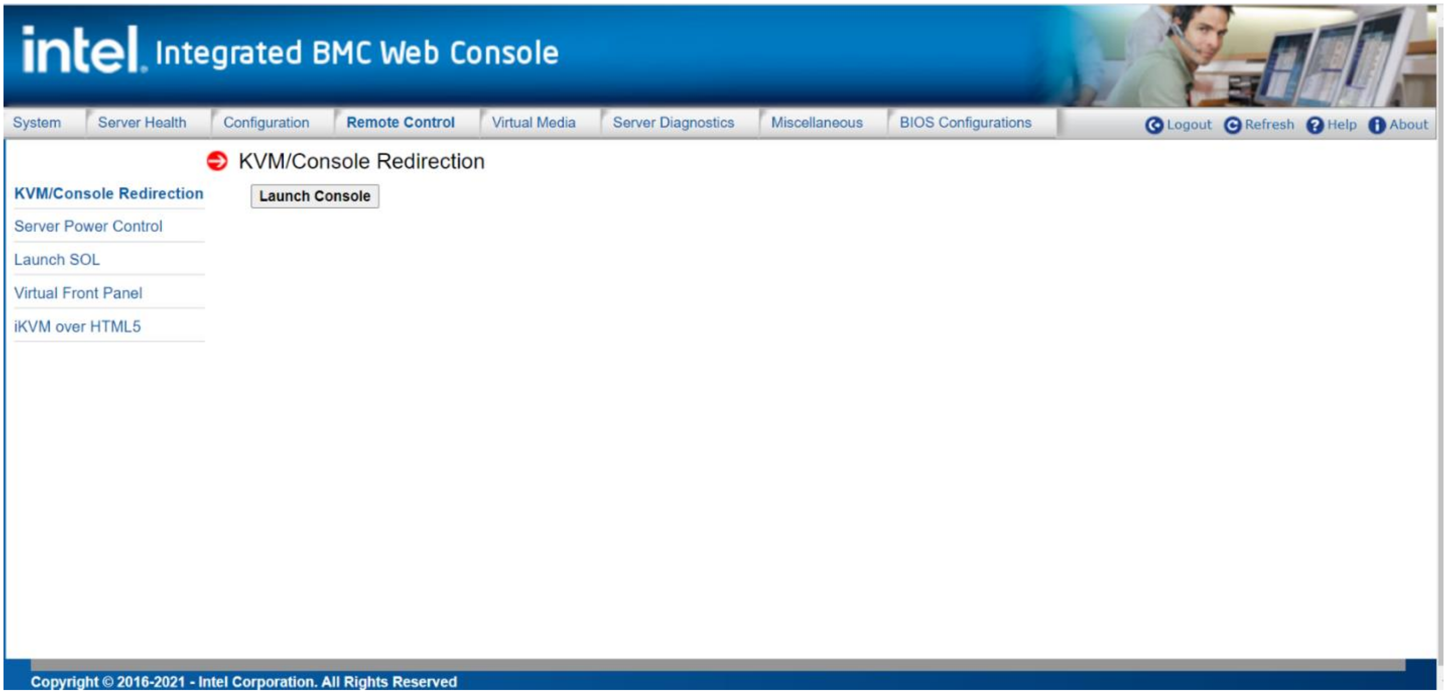


Figure 14. Remote Control Console Redirection Page

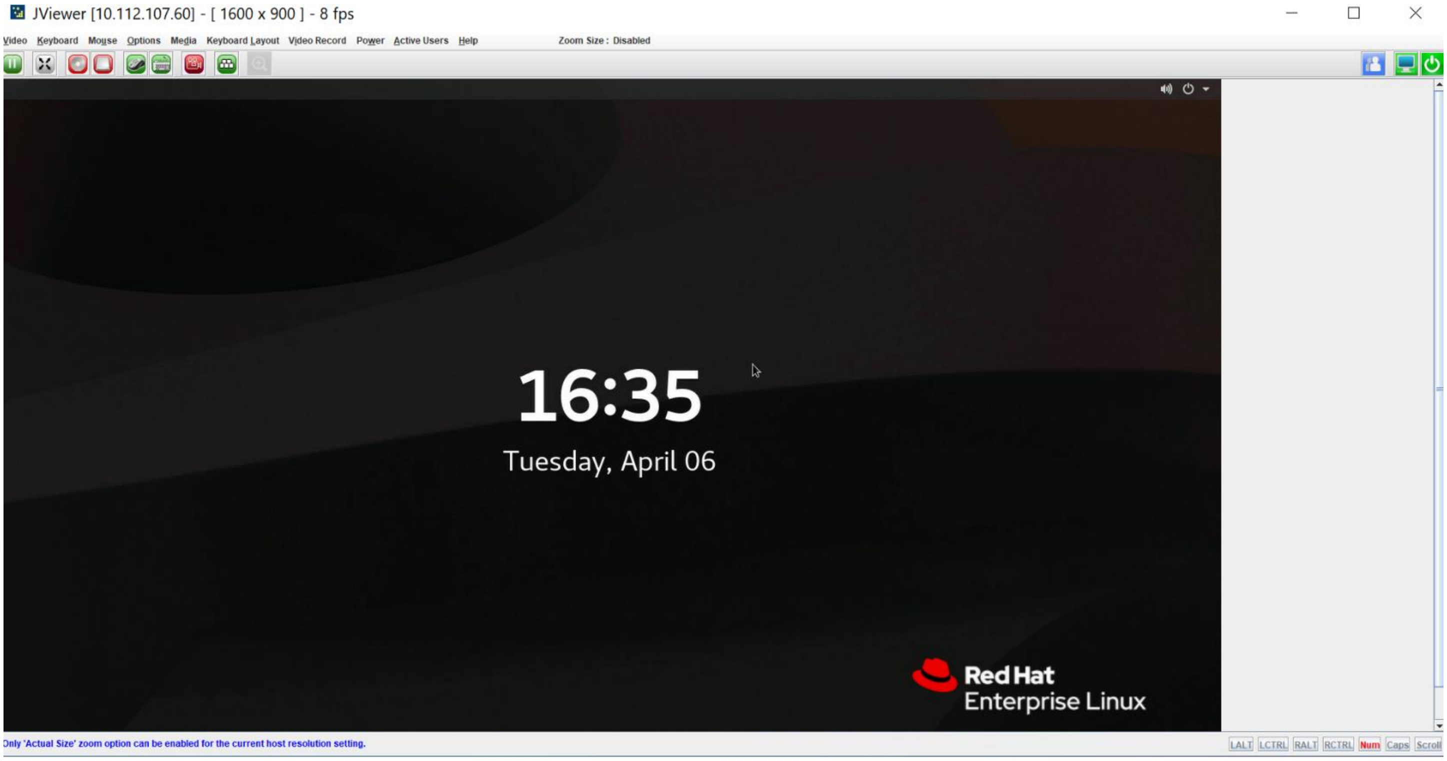
When the **Launch Console** button is clicked, a pop-up window is displayed to download the Java* Network Launch Protocol `jviewer.jnlp` file. This in turn downloads the stand-alone Java application implementing the remote console.

Microsoft Internet Explorer*, Mozilla Firefox*, Google Chrome* and Apple Safari* browsers are supported.

Notes:

- Java Runtime Environment* (JRE*, version 6, update 10 or higher) must be installed on the client before the launch of a JNLP file.
- The client browser must allow pop-up windows from the Intel® Integrated BMC Web Console IP address.
- JCE Unlimited Strength Jurisdiction Policy Files required by AES-256 must be installed on the client side or the KVM automatically downgrades to AES-128. The additional strength is only required for users who need AES-256.

The remote console window is a Java Applet* that establishes TCP connections to the Intel® Integrated BMC Web Console. The protocol used to run these connections is a unique KVM protocol and not HTTP or HTTPS. KVM and media use the BMC default web server port: 443. The local network environment must permit these connections to be made. That is, the firewall and, in case of a private internal network, the network address translation (NAT) settings must be configured accordingly.

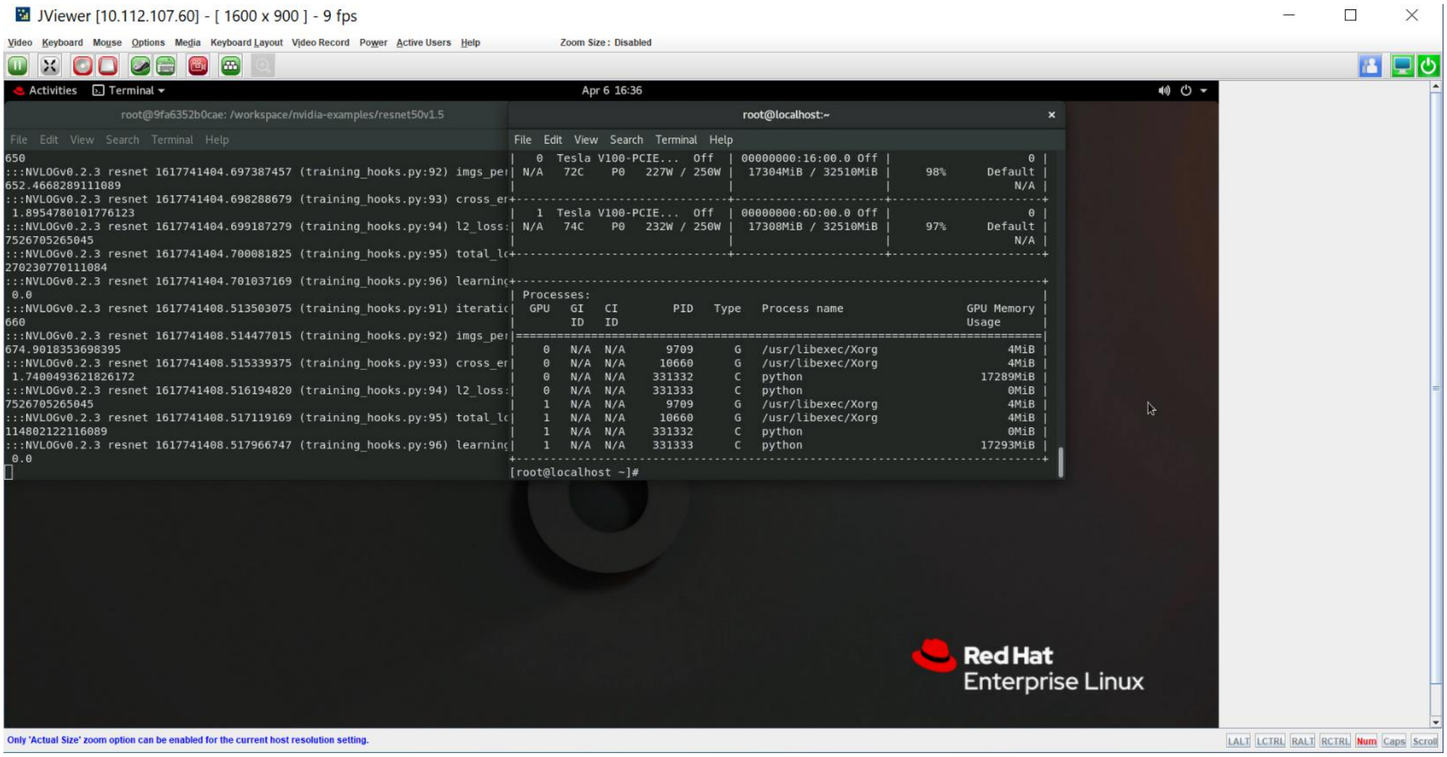


Only 'Actual Size' zoom option can be enabled for the current host resolution setting.

Figure 15. Remote Console Window

6.2 Main Window

Starting the remote console opens a host window (Linux* operating system window is shown in Figure 16).


JViewer [10.112.107.60] - [1600 x 900] - 9 fps
Video Keyboard Mouse Options Media Keyboard Layout Video Record Power Active Users Help
Zoom Size : Disabled
Activities
Terminal
Apr 6 16:36
root@9fa6352b0cae: /workspace/nvidia-examples/resnet50v1.5
root@localhost:~
File Edit View Search Terminal Help
Red Hat Enterprise Linux
LALT LCTRL RALT RCTRL Num Caps Scroll

```
650
:::NVLOGv0.2.3 resnet 1617741404.697387457 (training_hooks.py:92) imgs_per
652.4668289111089
:::NVLOGv0.2.3 resnet 1617741404.698288679 (training_hooks.py:93) cross_er
 1.8954780101776123
:::NVLOGv0.2.3 resnet 1617741404.699187279 (training_hooks.py:94) l2_loss:
7526705265045
:::NVLOGv0.2.3 resnet 1617741404.700081825 (training_hooks.py:95) total_lc
270230770111084
:::NVLOGv0.2.3 resnet 1617741404.701037169 (training_hooks.py:96) learninc
 0.0
:::NVLOGv0.2.3 resnet 1617741408.513503075 (training_hooks.py:91) iteratic
660
:::NVLOGv0.2.3 resnet 1617741408.514477015 (training_hooks.py:92) imgs_per
674.9018353698395
:::NVLOGv0.2.3 resnet 1617741408.515339375 (training_hooks.py:93) cross_er
 1.7400493621826172
:::NVLOGv0.2.3 resnet 1617741408.516194820 (training_hooks.py:94) l2_loss:
7526705265045
:::NVLOGv0.2.3 resnet 1617741408.517119169 (training_hooks.py:95) total_lc
114802122116089
:::NVLOGv0.2.3 resnet 1617741408.517966747 (training_hooks.py:96) learninc
 0.0
```

```
|   0  Tesla V100-PCIE...  Off  | 00000000:16:00.0 Off |                    0 |
| N/A   72C    P0   227W / 250W |  17304MiB / 32510MiB |     98%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+
|   1  Tesla V100-PCIE...  Off  | 00000000:6D:00.0 Off |                    0 |
| N/A   74C    P0   232W / 250W |  17308MiB / 32510MiB |     97%      Default |
|                               |                      |                  N/A |
+-------------------------------+----------------------+----------------------+

+-----------------------------------------------------------------------------+
| Processes:                                                                  |
|  GPU   GI   CI        PID   Type   Process name                  GPU Memory |
|        ID   ID                                                   Usage      |
|=============================================================================|
|    0   N/A  N/A      9709      G   /usr/libexec/Xorg                   4MiB |
|    0   N/A  N/A     10660      G   /usr/libexec/Xorg                   4MiB |
|    0   N/A  N/A    331332      C   python                          17289MiB |
|    0   N/A  N/A    331333      C   python                             0MiB |
|    1   N/A  N/A      9709      G   /usr/libexec/Xorg                   4MiB |
|    1   N/A  N/A     10660      G   /usr/libexec/Xorg                   4MiB |
|    1   N/A  N/A    331332      C   python                             0MiB |
|    1   N/A  N/A    331333      C   python                          17293MiB |
+-----------------------------------------------------------------------------+
[root@localhost ~]#
```

Only 'Actual Size' zoom option can be enabled for the current host resolution setting.

Figure 16. Remote Console Main Window

It displays the remote server's screen content. The remote console responds as if it were at the remote server. The responsiveness may be slightly delayed depending on the network bandwidth and latency between the Intel® Integrated BMC Web Console and the remote console. Enabling KVM and/or media encryption on the Configuration > KVM & Media page slightly degrades performance, as well.

The remote console window always shows the remote screen in its optimal size. This means it adapts its size to the remote screen size initially and after the remote screen resolution has been changed. However, the remote console window can be resized in the local window as usual.

6.3 Remote Console Control Bar

The remote console window top contains a control bar (see Figure 17) to view the remote console status and to configure remote console settings. The following subsections describe each control task.

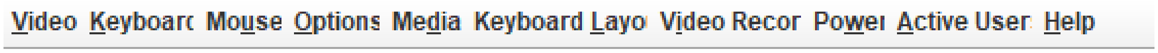


Figure 17. Remote Console Control Bar

6.3.1 Video Menu

Click **Video** in the remote console control bar to open the virtual storage and virtual keyboard menu, as shown in Figure 18.

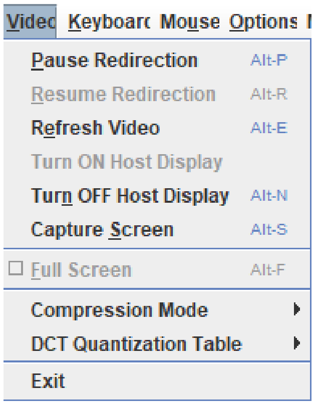


Figure 18. Remote Console Video Menu

Use the options in this menu to do the following:

- Pause Redirection
- Resume Redirection
- Refresh Video
- Turn ON Host Display
- Turn OFF Host Display
- Capture Screen
- Full Screen
- Compression Mode

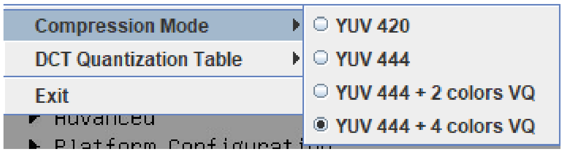


Figure 19. Compression Mode Submenu Option

- DCT Quantization Table

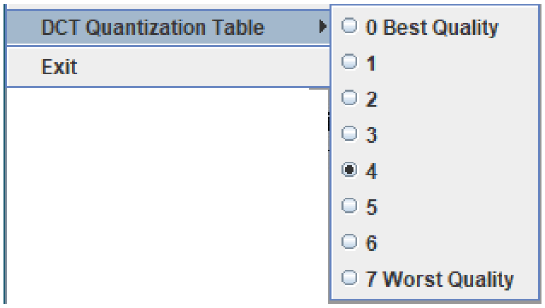


Figure 20. DCT Quantization Table Submenu Option

6.3.2 Keyboard Menu

Click **Keyboard** to open the keyboard macro menu as shown in Figure 21.

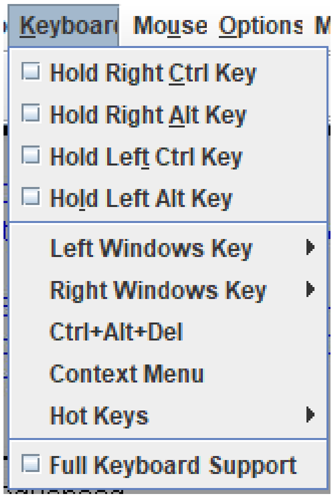


Figure 21: Remote Console Keyboard Menu

Use the options in this menu to do the following:

- **Hold Right Ctrl Key.** Simulate holding down the right <Ctrl> key on the remote keyboard. On the local keyboard, right < Ctrl > key presses are processed by the local operating system and not passed on to the remote operating system.
- **Hold Right Alt Key.** Simulate holding down the right <Alt> key on the remote keyboard. On the local keyboard, right <Alt> key presses are processed by the local operating system and not passed on to the remote operating system.
- **Hold Left Ctrl Key.** Simulate holding down the left <Ctrl> key on the remote keyboard. On the local keyboard, left <Ctrl> key presses are processed by the local operating system and not passed on to the remote operating system.
- **Hold Left Alt Key.** Simulate holding down the left <Alt> key on the remote keyboard. On the local keyboard, left <Alt> key presses are processed by the local operating system and not passed on to the remote operating system.
- **Right Windows Key.** Simulate holding down the right <Win> key on the remote keyboard. On the local keyboard, right <Win> key presses are processed by the local operating system and not passed on to the remote operating system.
- **Left Windows Key.** Simulate holding down the left <Win> key on the remote keyboard. On the local keyboard, left <Win> key presses are processed by the local operating system and not passed on to the remote operating system.
- **Ctrl+Alt+Del.** Simulate press and release of <Ctrl>, <Alt> and <Del> keys combination.
- **Context Menu.** Simulate press and release of <Context Menu> key.
- **Hot Keys.** This menu is used to add the user configurable shortcut keys to invoke in the host machine. The configured key events are saved in the BMC.
- **Full Keyboard Support.** Enable this option to provide full keyboard support. This option is used to trigger the <Ctrl> and <Alt> key directly to host from the local physical keyboard.

6.3.3 Mouse Menu

Click **Mouse** to open the options menu, as shown in Figure 22.

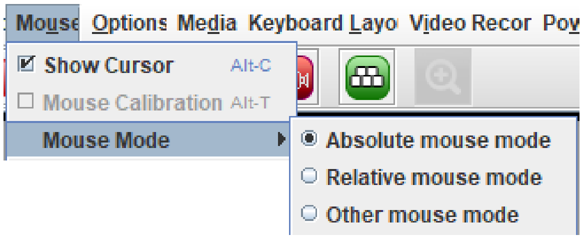


Figure 22. Remote Console Mouse Menu

Use the options in this menu to do the following:

- Show Cursor
- Mouse Calibration
- Mouse Mode
  - Absolute mouse mode
  - Relative mouse mode
  - Other mouse mode

6.3.4 Options Menu

Click **Options** to open the options menu, as shown in Figure 23. Remote Console Options Menu

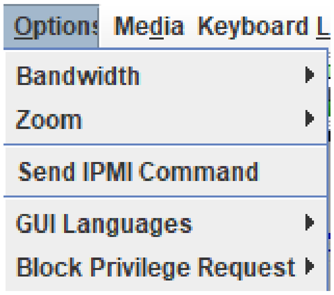


Figure 23. Remote Console Options Menu

Use the options in this menu to do the following:

- Bandwidth

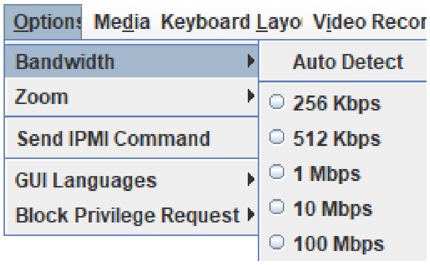


Figure 24. Remote Console Options \ Bandwidth Submenu

- Zoom

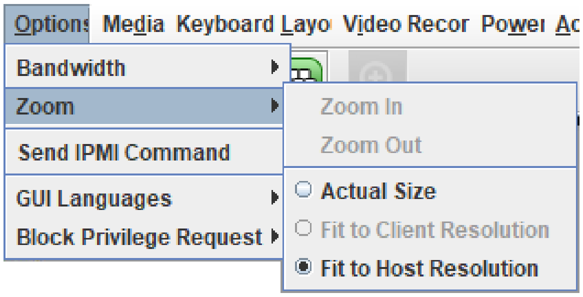


Figure 25. Remote Console Options \ Zoom Submenu

- Send IPMI Command
- GUI Languages
- Block Privilege Request

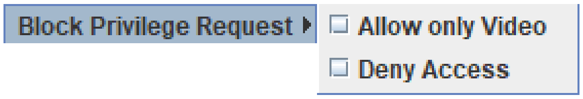


Figure 26. Remote Console Options \ Block Privilege Request Submenu

6.3.5 Media Menu

Click **Media** to open the media menu, as shown in Figure 27.

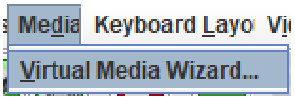
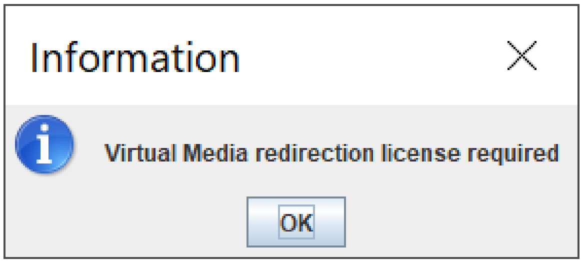


Figure 27. Remote Console Media Menu

A virtual media redirection license is required (see following figure).


Information

Virtual Media redirection license required

Figure 28. Information Window

6.3.6 Keyboard Layout Menu

Click **Keyboard Layout** to open the keyboard layout menu, as shown in Figure 29.

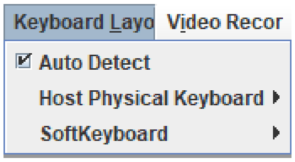


Figure 29. Remote Keyboard Layout Options

Use the options in this menu to do the following:

- Auto Detect
- Host Physical Keyboard

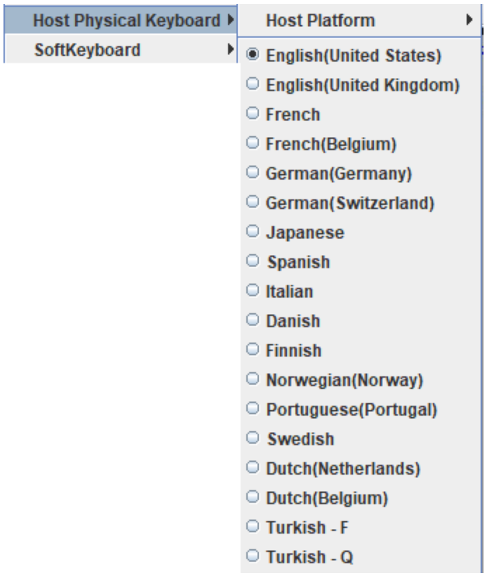


Figure 30. Remote Keyboard Layout Options \ Host Physical Keyboard

- SoftKeyBoard

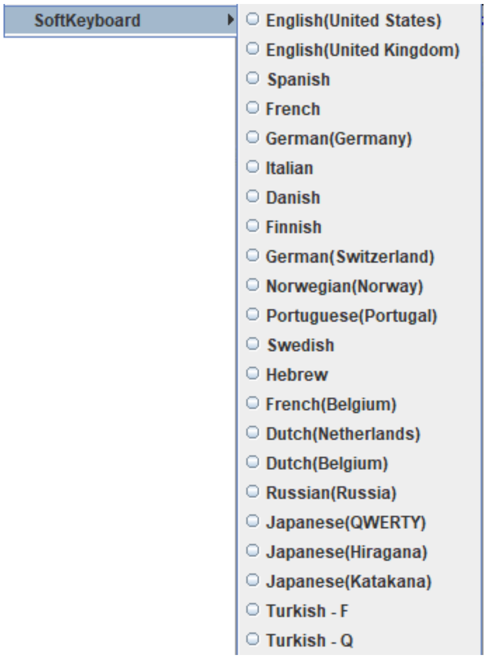


Figure 31. Remote Keyboard Layout Options \ SoftKeyboard

6.3.7 Video Record Menu

Click **Video Record** to open the video record menu, as shown in Figure 32.

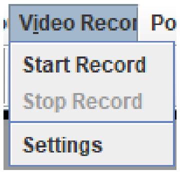
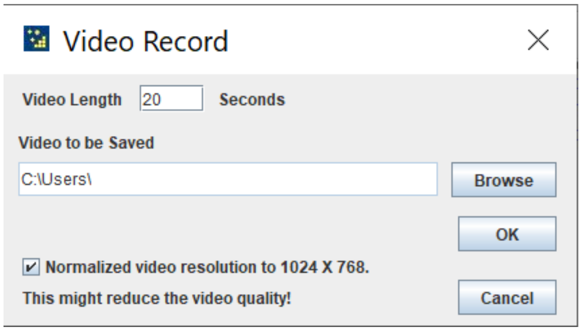


Figure 32. Remote Video Record Options

Use the options in this menu to do the following:

- Start Record
- Stop Record
- Settings



Video Length 20 Seconds

Video to be Saved

C:\Users\

☑ Normalized video resolution to 1024 X 768.

This might reduce the video quality!

Figure 33. Remote Video Record \ Settings

6.3.8 Power Menu

Click **Power** to open the power menu, as shown in Figure 34.

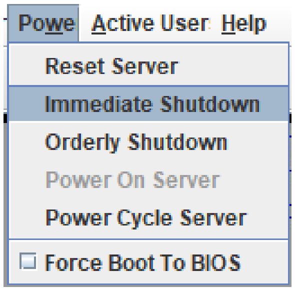


Figure 34. Remote Power Options

Use the options in this menu to do the following:

- Reset Server
- Immediate Shutdown
- Orderly Shutdown
- Power On Server
- Power Cycle Server
- Force Boot to BIOS

6.3.9 Active User Menu

Click **Active User** show the current Active User, as shown in Figure 35.

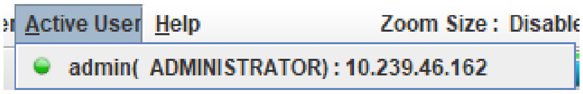


Figure 35. Remote Active User Options

6.3.10 Help Menu

Click **Help** show the About JViewer* menu, as shown in Figure 36.

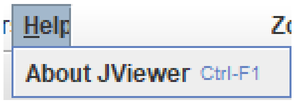
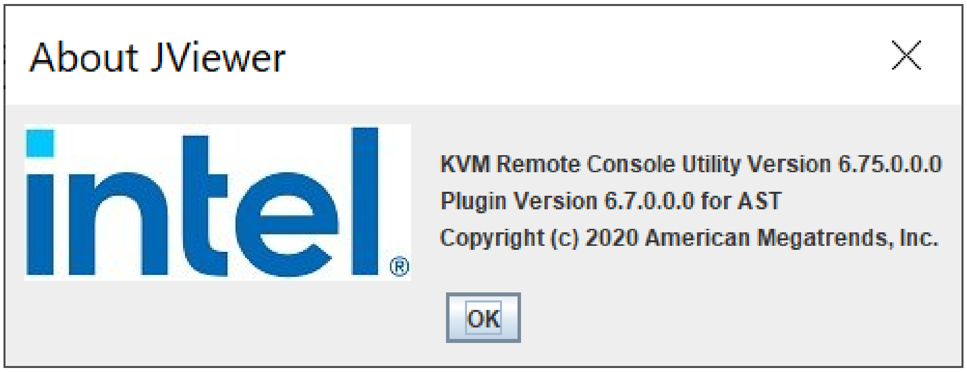


Figure 36. Remote Help Options

Click **About JViewer*** to see the detail version, as shown in Figure 37:



About JViewer

KVM Remote Console Utility Version 6.75.0.0.0
Plugin Version 6.7.0.0.0 for AST
Copyright (c) 2020 American Megatrends, Inc.

Figure 37. Remote Help About JViewer*

6.4 Remote Console Icon bar

The icon bar is below the remote console control bar. The system shows the function name when hovering the mouse over an icon.

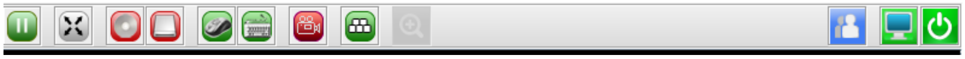
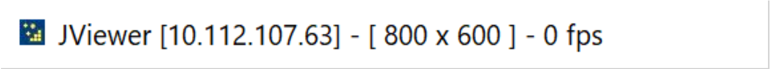


Figure 38. Remote Console Icon Bar

6.5 Remote Console Status Line

The status line at the top of the Remote Console screen displays the console state, as shown in Figure 39. The status line provides BMC host name, resolution, and display frames per second.



JViewer [10.112.107.63] - [800 x 600] - 0 fps

Figure 39. Remote Console Status Line

6.6 Remote Console Function Key Status Line

The function key status line at the bottom of the Remote Console screen displays the function key state, as shown in Figure 40. The status line provides LALT, LCTRL, RALT, RCTRL, Num, Caps and Scroll statuses.

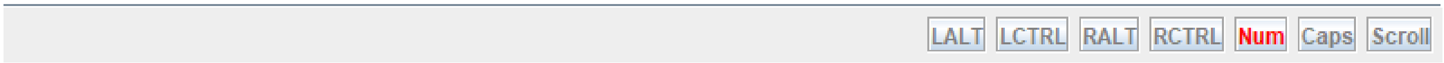


Figure 40. Remote Console Status Line

7. Intel® Integrated BMC Web Console Options

This section gives a detailed description of each Intel® Integrated BMC Web Console page. The section is organized in subsections corresponding to the six tabs in the horizontal menu. To access similar information about each page in the web console, click **Help** from the toolbar.

For information on navigating the web console interface, see Section 5.3. For a brief summary of the available pages and their secondary menus, see Table 3.The first secondary menu item for each tab is the default page that appears when the tab is selected.

When the web console is working on a user request, a busy indicator bar appears as shown in Figure 41.

Figure 41. Busy Indicator Bar

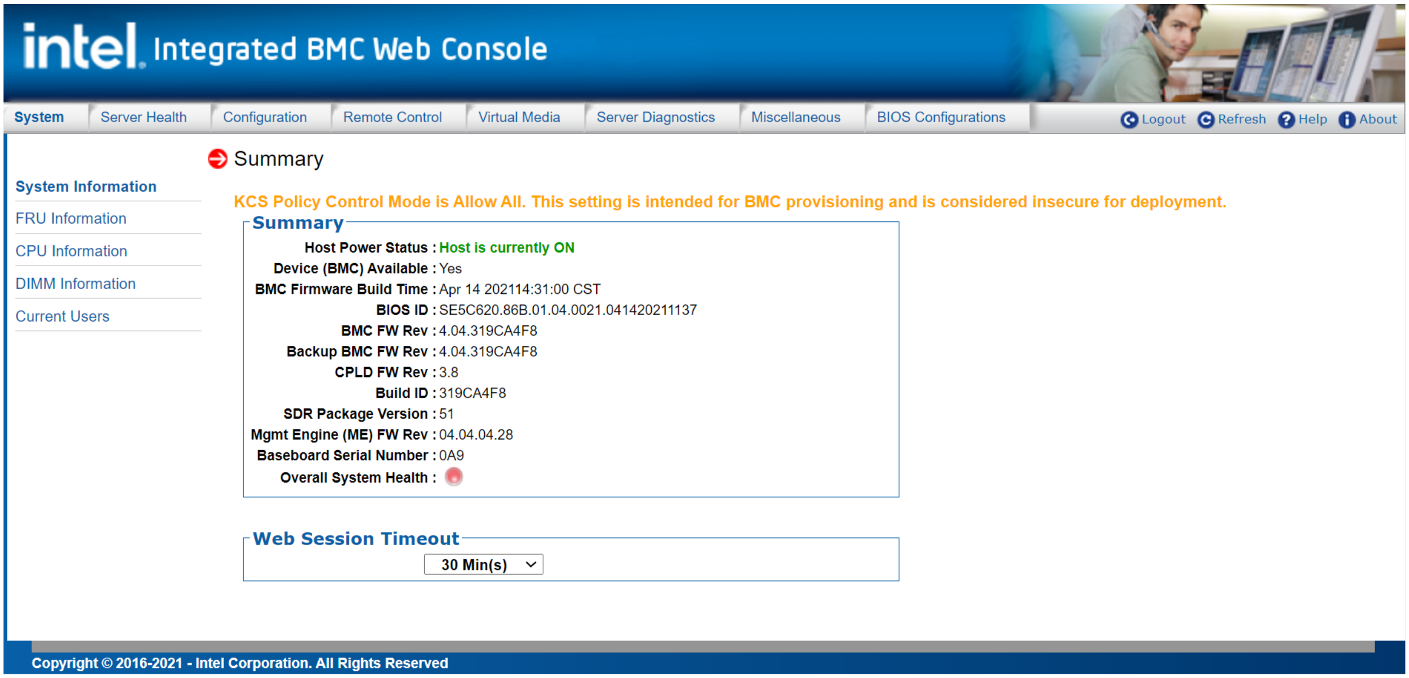
Note: Not all the following sections are used by or are directly related to advanced management enabled features. Such non-advanced-management features are included for completeness.

7.1 System Tab

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

7.1.1 System Information

The System Information page displays a summary of the general system information. This includes the power status, advanced management key status, BMC firmware build time and version, BIOS ID, SDR package version, Intel® Management Engine (Intel® ME) firmware version, baseboard serial number, and overall system health status. For a complete description of the summary information, see Table 5.



Summary

KCS Policy Control Mode is Allow All. This setting is intended for BMC provisioning and is considered insecure for deployment.

Summary

Host Power Status : Host is currently ON
Device (BMC) Available : Yes
BMC Firmware Build Time : Apr 14 202114:31:00 CST
BIOS ID : SE5C620.86B.01.04.0021.041420211137
BMC FW Rev : 4.04.319CA4F8
Backup BMC FW Rev : 4.04.319CA4F8
CPLD FW Rev : 3.8
Build ID : 319CA4F8
SDR Package Version : 51
Mgmt Engine (ME) FW Rev : 04.04.04.28
Baseboard Serial Number : 0A9
Overall System Health : ●

Web Session Timeout

30 Min(s)

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 42. System Information Page

Table 5. System Information Page Details

Information	Details
Host Power Status	Power status of the host (on/off).
Device (BMC) Available	Indicates whether the BMC is available for normal management tasks.
BMC Firmware Build Time	The build date and time of the installed BMC firmware.
BIOS ID	Major and minor revision of the BIOS. `BIOS ID:BoardFamilyID.OEMID.MajorVer.MinorVer.RelNum.BuildDateTime.`
BMC FW Rev	Major and minor revision of the BMC firmware.
Backup BMC FW Rev	Major and minor revision of the backup BMC firmware.
Build ID	The Git commit number of the build.
SDR Package Version	Version of the Sensor Data Record.
Mgmt Engine (Intel® ME) FW Rev	Major and minor revision of the Management Engine firmware.
Baseboard Serial Number	Serial number of the baseboard in this system.
Overall System Health	Overall system health LED status is displayed. • LED Red - System is in Off State • LED Blinking Red - System is in Warning State • LED Solid Red - System is in Critical State
Web Session Timeout	Set the maximum web service timeout in seconds. Timeout should be between 30 minutes and one day. **Default timeout:** 30 minutes. If the web session timeout is disabled, the system does not automatically redirect the user to the web login page. 1. Pull down the timeout values bar 30(mins)/1(hour)/2(hours)/4(hours)/8(hours)/1(day)/Disabled to configure the value. 2. After selection, this web session timeout value takes effect. 3. Once the web session is timed out, the system automatically redirects the user to the web login page. **Note:** The Web Session Timeout settings can only be set by users with administrator privilege. The users with other privilege are prohibited from setting.

7.1.2 FRU Information

The FRU Information page displays information from the field replaceable unit (FRU) repository. The user can select information about the baseboard, front panel, hot swap backplane, riser card, and power supply. To specify the FRU component, click the **FRU Information** drop-down box (see Figure 43).

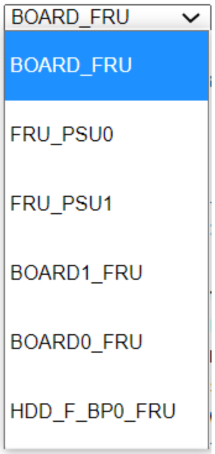
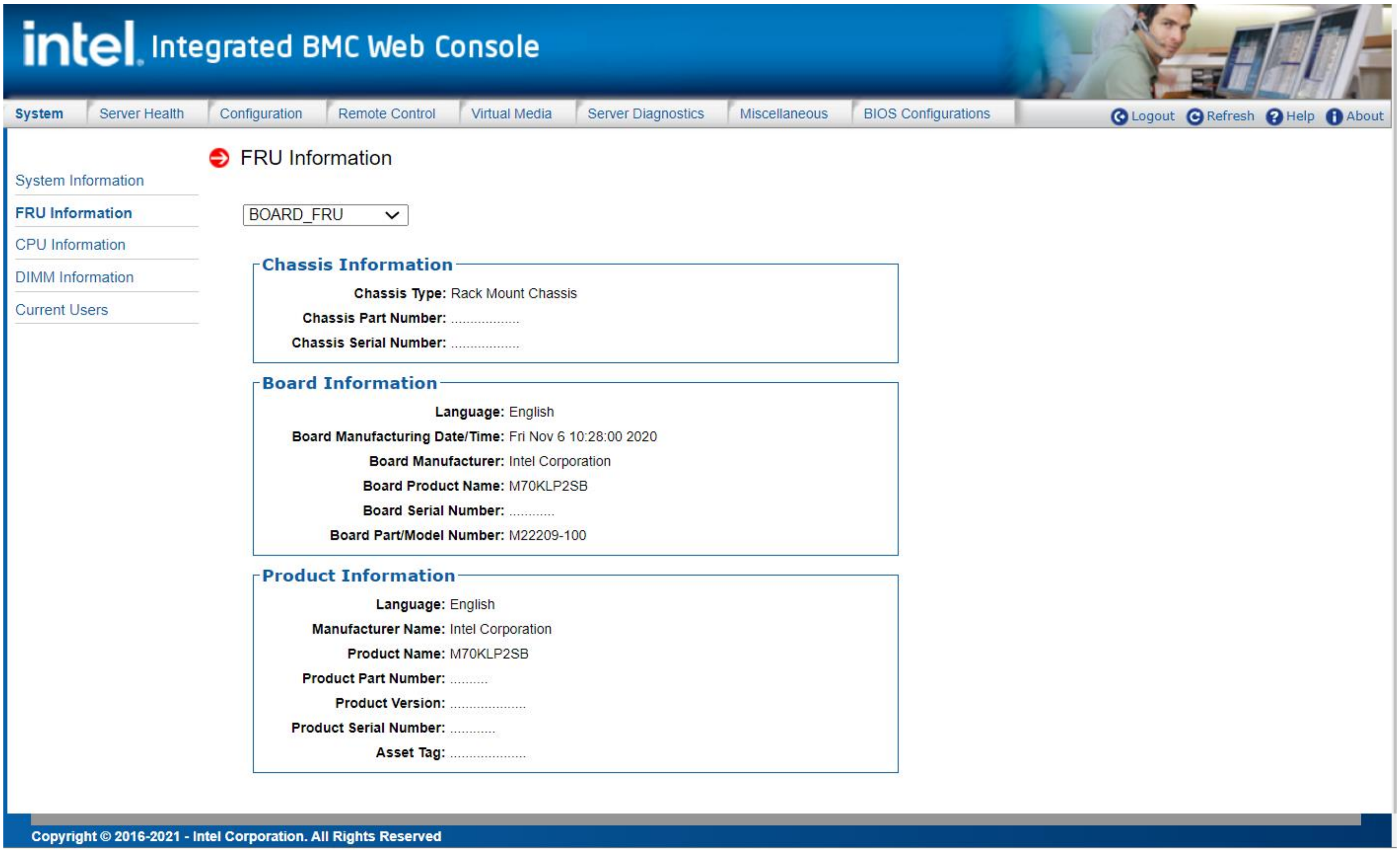


Figure 43. FRU Board Options

All data in the FRU Information page is compliant with standard specifications (consult *Platform Management FRU Information Storage Definition* for details). See Figure 44 for baseboard FRU details.



FRU Information

BOARD_FRU

Chassis Information

Chassis Type: Rack Mount Chassis
Chassis Part Number: ....
Chassis Serial Number: ....

Board Information

Language: English
Board Manufacturing Date/Time: Fri Nov 6 10:28:00 2020
Board Manufacturer: Intel Corporation
Board Product Name: M70KLP2SB
Board Serial Number: ....
Board Part/Model Number: M22209-100

Product Information

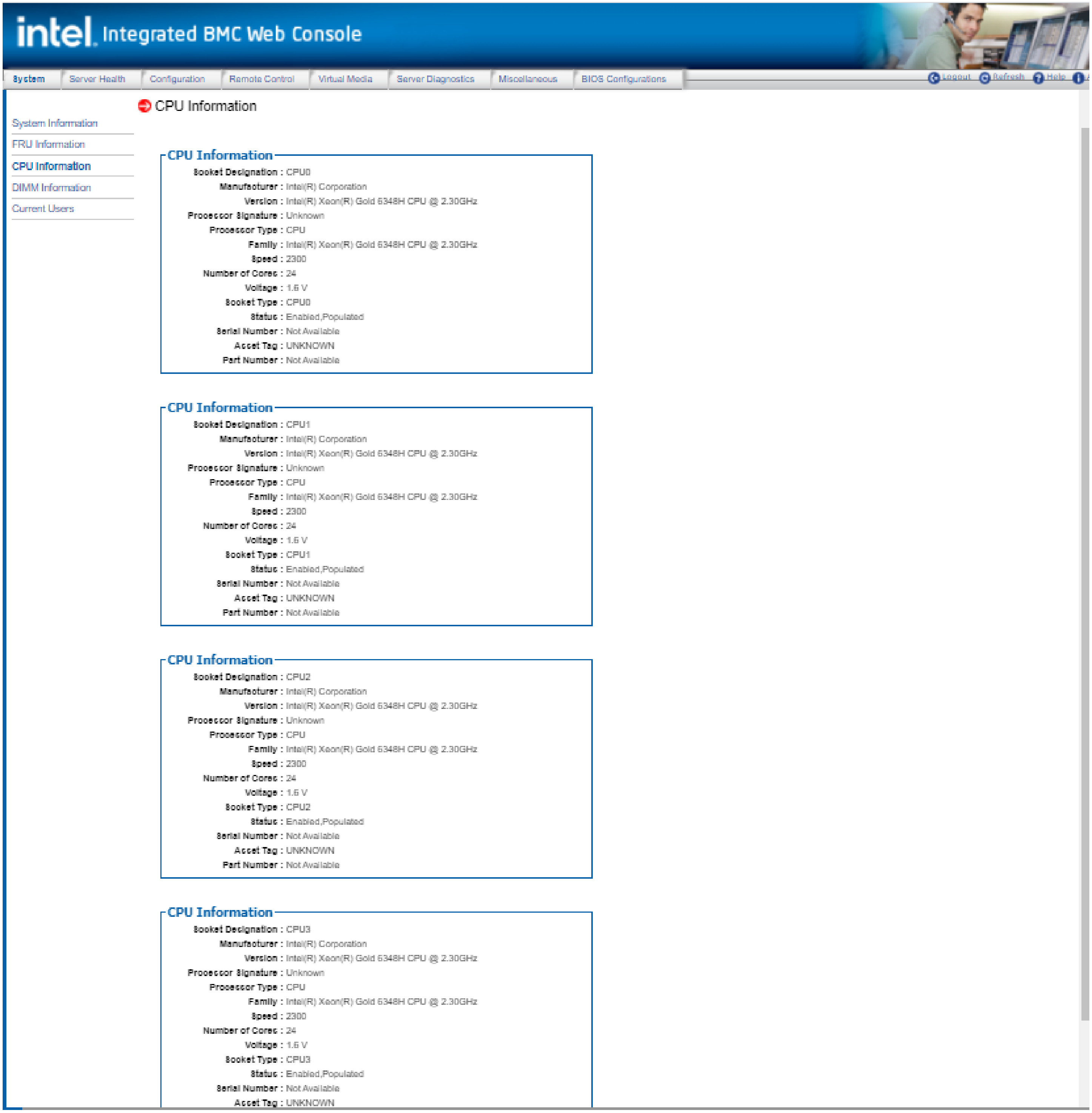
Language: English
Manufacturer Name: Intel Corporation
Product Name: M70KLP2SB
Product Part Number: ....
Product Version: ....
Product Serial Number: ....
Asset Tag: ....

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 44. System FRU Information Page

7.1.3 CPU Information

The CPU Information page displays information on CPUs installed on the host system. The CPU 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. See Figure 45 for details.



CPU Information

CPU Information

Socket Designation : CPU0
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU0
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN
Part Number : Not Available

CPU Information

Socket Designation : CPU1
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU1
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN
Part Number : Not Available

CPU Information

Socket Designation : CPU2
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU2
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN
Part Number : Not Available

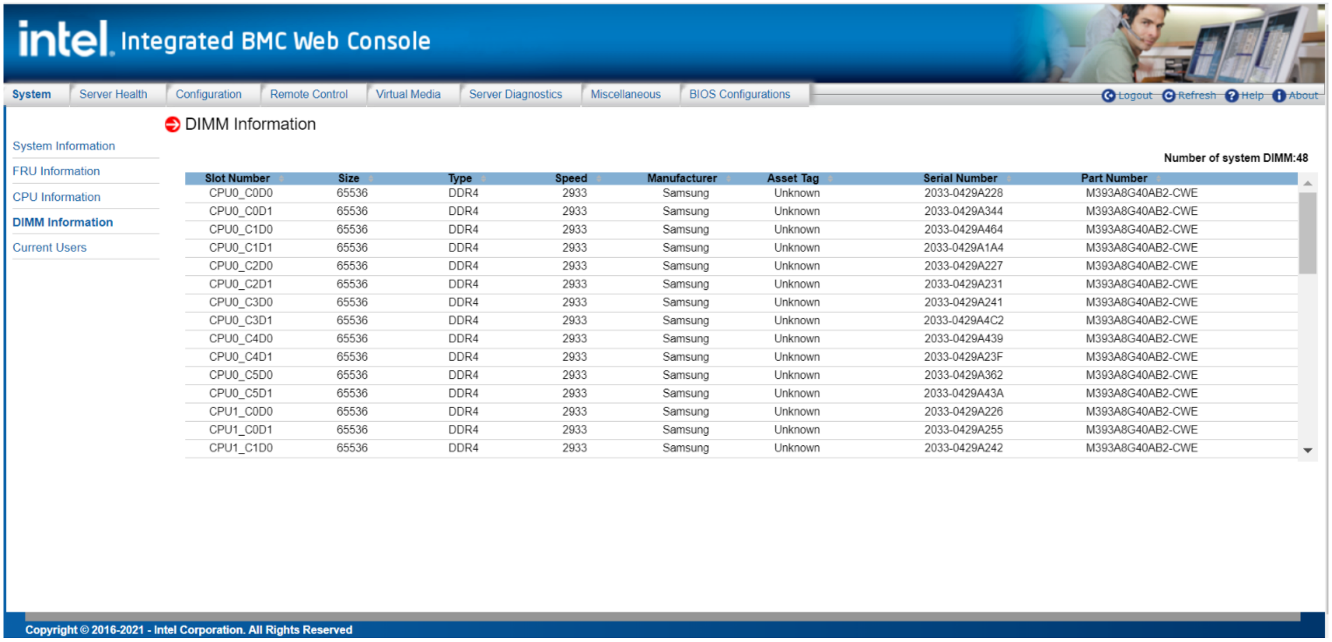
CPU Information

Socket Designation : CPU3
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU3
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN

Figure 45. System CPU Information Page

7.1.4 DIMM Information

The DIMM Information page displays information on dual in-line memory modules (DIMMs) installed in the host system. The DIMM information includes slot number, size, memory type, manufacturer, asset tag, memory serial/part number. See Figure 46 for details.



DIMM Information

Number of system DIMM:48

Slot Number	Size	Type	Speed	Manufacturer	Asset Tag	Serial Number	Part Number
CPU0_C0D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A228	M393A8G40AB2-CWE
CPU0_C0D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A344	M393A8G40AB2-CWE
CPU0_C1D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A464	M393A8G40AB2-CWE
CPU0_C1D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A1A4	M393A8G40AB2-CWE
CPU0_C2D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A227	M393A8G40AB2-CWE
CPU0_C2D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A231	M393A8G40AB2-CWE
CPU0_C3D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A241	M393A8G40AB2-CWE
CPU0_C3D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A4C2	M393A8G40AB2-CWE
CPU0_C4D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A439	M393A8G40AB2-CWE
CPU0_C4D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A23F	M393A8G40AB2-CWE
CPU0_C5D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A362	M393A8G40AB2-CWE
CPU0_C5D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A43A	M393A8G40AB2-CWE
CPU1_C0D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A226	M393A8G40AB2-CWE
CPU1_C0D1	65536	DDR4	2933	Samsung	Unknown	2033-0429A255	M393A8G40AB2-CWE
CPU1_C1D0	65536	DDR4	2933	Samsung	Unknown	2033-0429A242	M393A8G40AB2-CWE

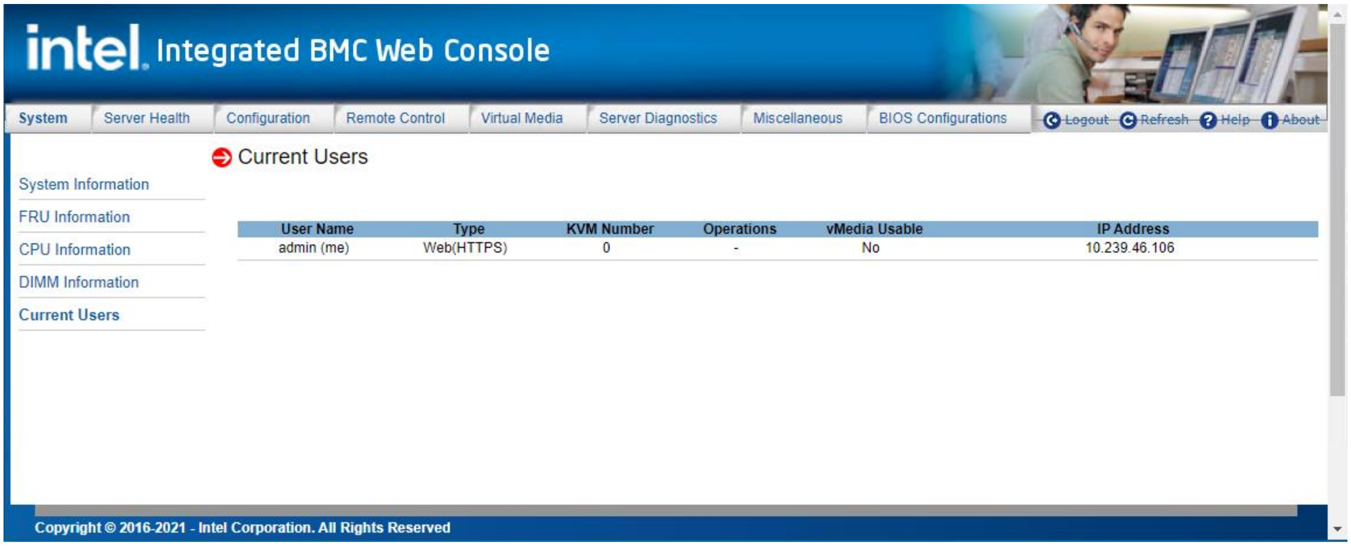
Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 46. System DIMM Information Page

7.1.5 Current Users

The Current Users page shows users currently logged in to the BMC via the embedded web server, IPMI 1.5 or IPMI 2.0 session; and Intel® Integrated BMC Web Console login type via HTTP or HTTPs. This table also lists KVM session number, virtual media usage status, and client IP address. See Figure 47 for details.

Note: Intel added a new Keyboard Controller Style (KCS) Policy Control Mode to the BMC. When set to Deny ALL on the Intel® Integrated BMC Web Console, neither the BMC nor the FRUSDR can be upgraded/downgraded as expected behavior. Updates can still be performed via Redfish* or Intel® Integrated BMC Web Console. By default, the BMC KCS Policy is set to Allow All.



Current Users

User Name	Type	KVM Number	Operations	vMedia Usable	IP Address
admin (me)	Web(HTTPS)	0	-	No	10.239.46.106

Figure 47. System Current Users Page

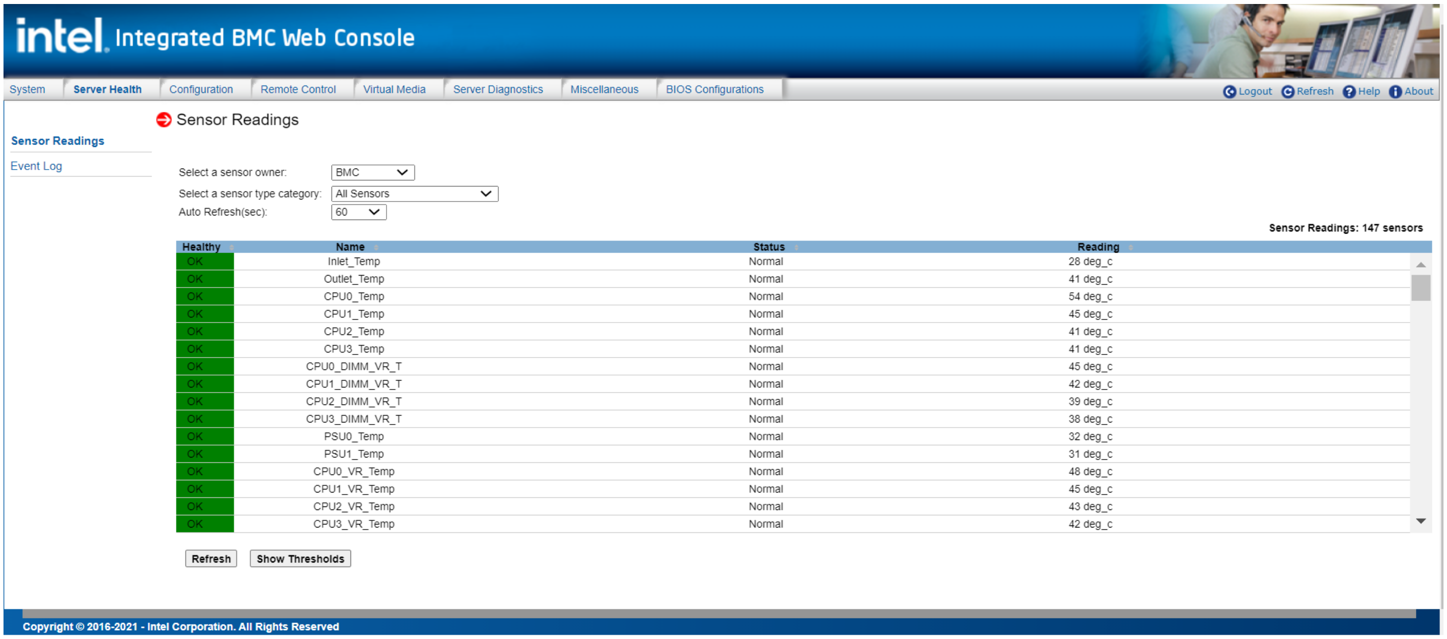
7.2 Server Health Tab

The Server Health tab shows data related to the server's health, such as sensor readings and the event log.

7.2.1 Sensor Readings

The Sensor Readings page displays system sensor information including status, health, and reading, as shown in Figure 48 and Figure 49 (with threshold).

Table 6 lists the options available on this page. By default, this page displays all sensors owned by the BMC and auto-refreshes every 60 seconds.



Sensor Readings

Select a sensor owner: BMC

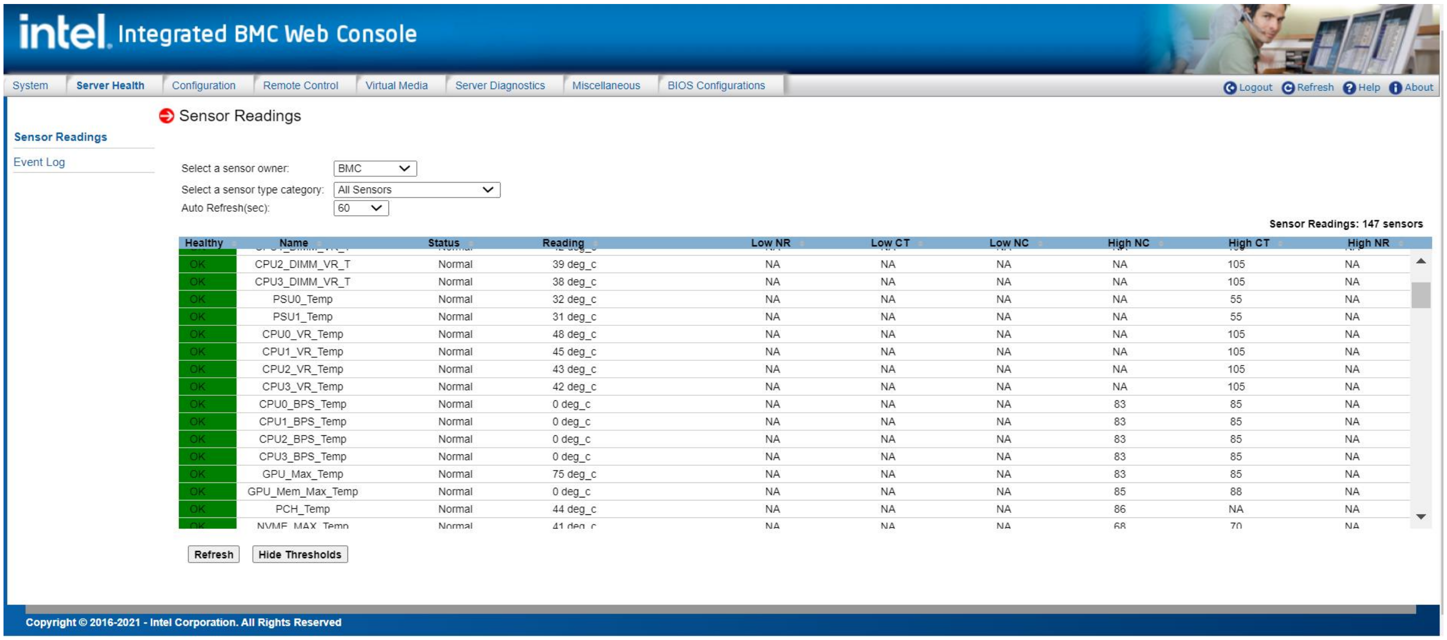
Select a sensor type category: All Sensors

Auto Refresh(sec): 60

Sensor Readings: 147 sensors

Healthy	Name	Status	Reading
OK	Inlet_Temp	Normal	28 deg_c
OK	Outlet_Temp	Normal	41 deg_c
OK	CPU0_Temp	Normal	54 deg_c
OK	CPU1_Temp	Normal	45 deg_c
OK	CPU2_Temp	Normal	41 deg_c
OK	CPU3_Temp	Normal	41 deg_c
OK	CPU0_DIMM_VR_T	Normal	45 deg_c
OK	CPU1_DIMM_VR_T	Normal	42 deg_c
OK	CPU2_DIMM_VR_T	Normal	39 deg_c
OK	CPU3_DIMM_VR_T	Normal	38 deg_c
OK	PSU0_Temp	Normal	32 deg_c
OK	PSU1_Temp	Normal	31 deg_c
OK	CPU0_VR_Temp	Normal	48 deg_c
OK	CPU1_VR_Temp	Normal	45 deg_c
OK	CPU2_VR_Temp	Normal	43 deg_c
OK	CPU3_VR_Temp	Normal	42 deg_c

Figure 48. Server Health Sensor Readings Page (Thresholds Not Displayed)



Sensor Readings

Select a sensor owner: BMC

Select a sensor type category: All Sensors

Auto Refresh(sec): 60

Sensor Readings: 147 sensors

Healthy	Name	Status	Reading	Low NR	Low CT	Low NC	High NC	High CT	High NR
OK	CPU2_DIMM_VR_T	Normal	39 deg_c	NA	NA	NA	NA	105	NA
OK	CPU3_DIMM_VR_T	Normal	38 deg_c	NA	NA	NA	NA	105	NA
OK	PSU0_Temp	Normal	32 deg_c	NA	NA	NA	NA	55	NA
OK	PSU1_Temp	Normal	31 deg_c	NA	NA	NA	NA	55	NA
OK	CPU0_VR_Temp	Normal	48 deg_c	NA	NA	NA	NA	105	NA
OK	CPU1_VR_Temp	Normal	45 deg_c	NA	NA	NA	NA	105	NA
OK	CPU2_VR_Temp	Normal	43 deg_c	NA	NA	NA	NA	105	NA
OK	CPU3_VR_Temp	Normal	42 deg_c	NA	NA	NA	NA	105	NA
OK	CPU0_BPS_Temp	Normal	0 deg_c	NA	NA	NA	83	85	NA
OK	CPU1_BPS_Temp	Normal	0 deg_c	NA	NA	NA	83	85	NA
OK	CPU2_BPS_Temp	Normal	0 deg_c	NA	NA	NA	83	85	NA
OK	CPU3_BPS_Temp	Normal	0 deg_c	NA	NA	NA	83	85	NA
OK	GPU_Max_Temp	Normal	75 deg_c	NA	NA	NA	83	85	NA
OK	GPU_Mem_Max_Temp	Normal	0 deg_c	NA	NA	NA	85	88	NA
OK	PCH_Temp	Normal	44 deg_c	NA	NA	NA	86	NA	NA
OK	NVME_MAX_Temp	Normal	41 deg_c	NA	NA	NA	68	70	NA

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

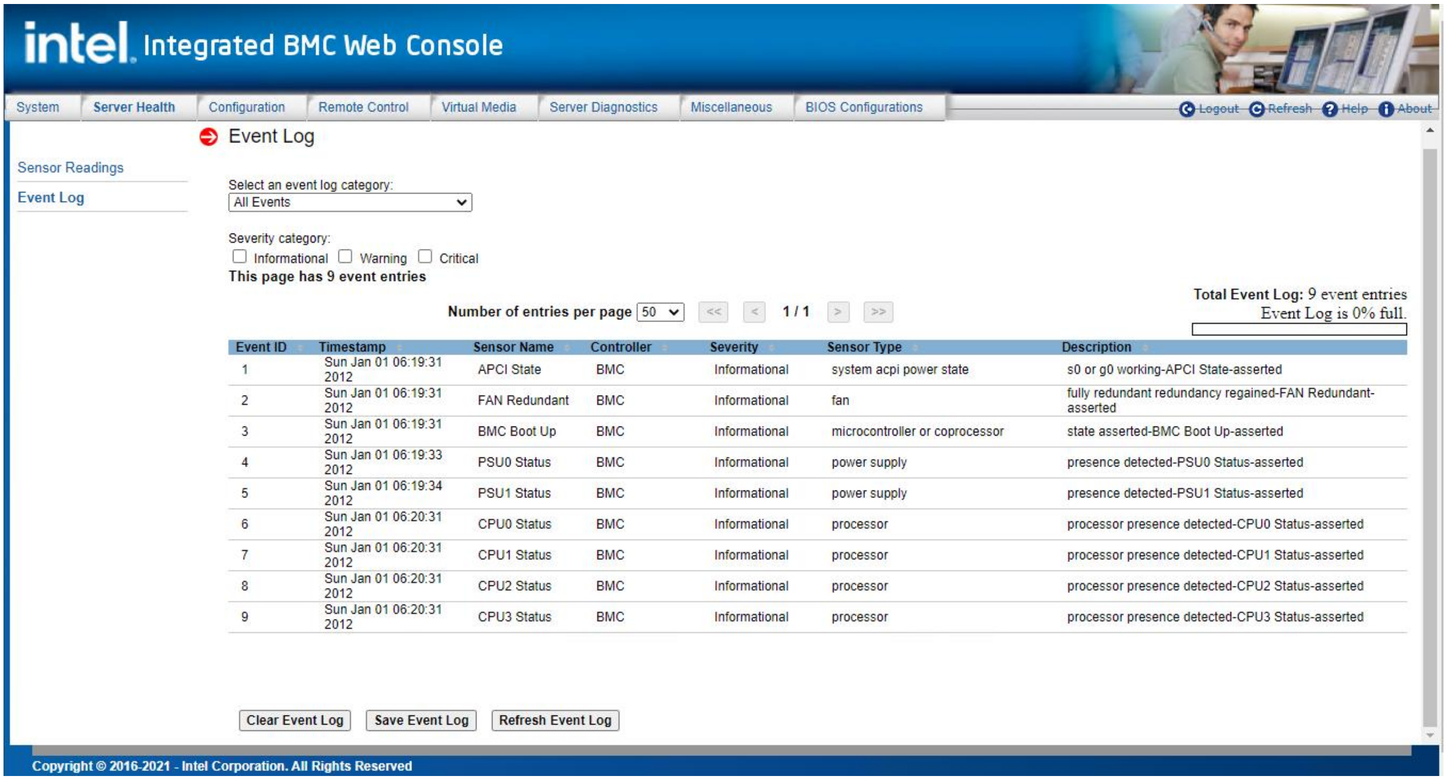
Figure 49. Server Health Sensor Readings Page (Thresholds Displayed)

Table 6. Server Health Sensor Readings Options

Option	Task
Select a sensor owner	Select the owner of sensor readings to display in the list. Choose BMC, Intel® ME, or SATELITE. **Default owner:** BMC.
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 0, 10, 15, 30, 60, 150, 300, or never. **Default refresh time:** 60 seconds.
Refresh	Click to refresh the selected sensor readings.
Show Thresholds	Click to show low and high, critical (CT) and non-critical (NC) threshold assignments. Use the scroll bar at the bottom to move the display left and right.
Hide Thresholds	Click to return to the original display, hiding the threshold values.

7.2.2 Event Log

The Event Log page displays the system server management event log (see Figure 50). Table 7 lists the options available on this page.



Event Log

Select an event log category: All Events

Severity category:
□ Informational □ Warning □ Critical

This page has 9 event entries

Number of entries per page 50   << < 1 / 1 > >>

Total Event Log: 9 event entries
Event Log is 0% full.

Event ID	Timestamp	Sensor Name	Controller	Severity	Sensor Type	Description
1	Sun Jan 01 06:19:31 2012	APCI State	BMC	Informational	system acpi power state	s0 or g0 working-APCI State-asserted
2	Sun Jan 01 06:19:31 2012	FAN Redundant	BMC	Informational	fan	fully redundant redundancy regained-FAN Redundant-asserted
3	Sun Jan 01 06:19:31 2012	BMC Boot Up	BMC	Informational	microcontroller or coprocessor	state asserted-BMC Boot Up-asserted
4	Sun Jan 01 06:19:33 2012	PSU0 Status	BMC	Informational	power supply	presence detected-PSU0 Status-asserted
5	Sun Jan 01 06:19:34 2012	PSU1 Status	BMC	Informational	power supply	presence detected-PSU1 Status-asserted
6	Sun Jan 01 06:20:31 2012	CPU0 Status	BMC	Informational	processor	processor presence detected-CPU0 Status-asserted
7	Sun Jan 01 06:20:31 2012	CPU1 Status	BMC	Informational	processor	processor presence detected-CPU1 Status-asserted
8	Sun Jan 01 06:20:31 2012	CPU2 Status	BMC	Informational	processor	processor presence detected-CPU2 Status-asserted
9	Sun Jan 01 06:20:31 2012	CPU3 Status	BMC	Informational	processor	processor presence detected-CPU3 Status-asserted

Figure 50. Server Health Event Log Page

Table 7. Server Health Event Log Options

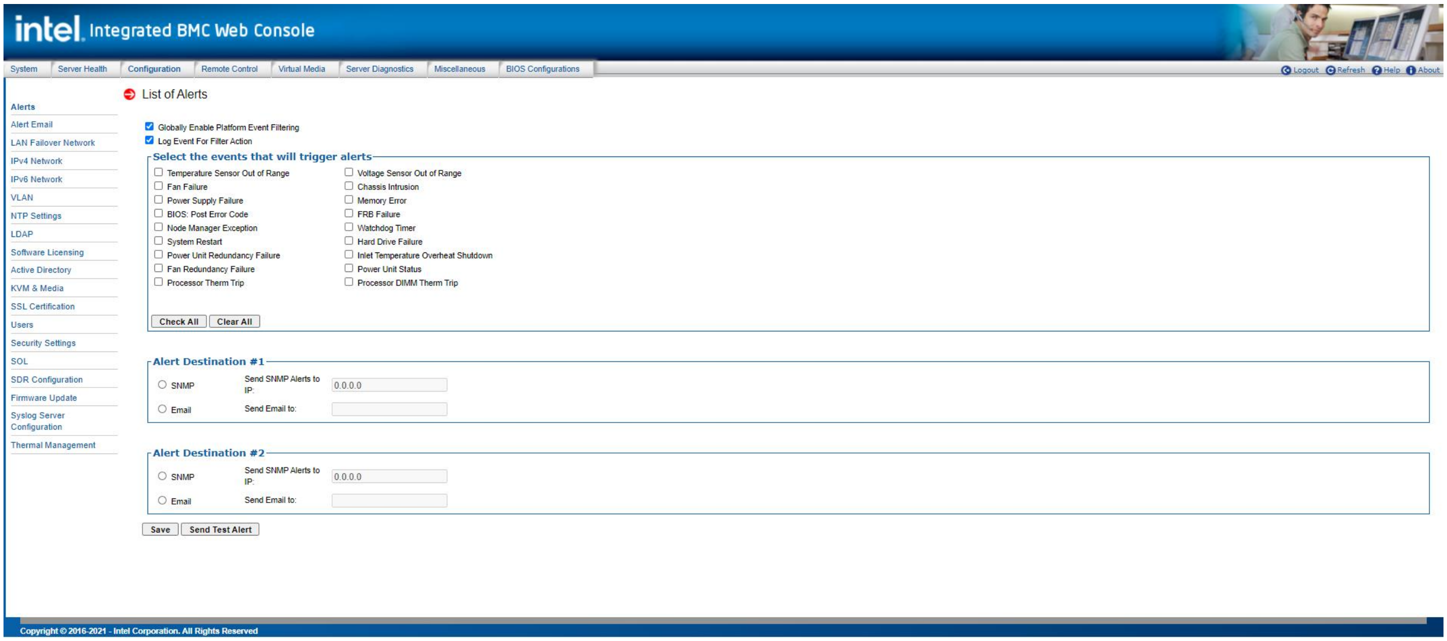
Option	Task
Select an event log category	Select the type of events to display in the list.
Severity category	Select the severity of events to display in the list. Choose informational, warning, or critical.
Number of entries per page	Specify how many events are displayed per page.
Event full indicator	An estimate of how full the event log is.
Page selection	Navigate to other pages of recorded events. The selections are first page, previous page, next page, and last page.
Event log list	Selected sensors are shown with their name, status, and readings. This includes a list of the events with their ID, time stamp, sensor name, controller, severity, sensor type, and description.
Clear Event Log	Clear the event log.
Save Event Log	Save the event log to file.
Refresh Event Log	Refresh the event log.

7.3 Configuration Tab

The Configuration tab allows the user to configure various settings, such as alerts, alert email, IPv4 and IPv6 networks, VLAN, KVM and media, SSL certification, users, security settings, serial-over-LAN (SOL), sensor data record (SDR) configuration, and firmware. These settings are discussed in the following subsections.

7.3.1 Alerts

Use this page to configure which system events should trigger alerts and the destination for those alerts. Up to two destinations can be selected for each LAN channel (see Figure 51). Table 8 lists the options to select the events that should trigger alerts and where the alerts are to be sent.



List of Alerts

☑ Globally Enable Platform Event Filtering
☑ Log Event For Filter Action

Select the events that will trigger alerts

□ Temperature Sensor Out of Range	□ Voltage Sensor Out of Range
□ Fan Failure	□ Chassis Intrusion
□ Power Supply Failure	□ Memory Error
□ BIOS: Post Error Code	□ FRB Failure
□ Node Manager Exception	□ Watchdog Timer
□ System Restart	□ Hard Drive Failure
□ Power Unit Redundancy Failure	□ Inlet Temperature Overheat Shutdown
□ Fan Redundancy Failure	□ Power Unit Status
□ Processor Therm Trip	□ Processor DIMM Therm Trip

Alert Destination #1

○ SNMP Send SNMP Alerts to IP: 0.0.0.0
○ Email Send Email to:

Alert Destination #2

○ SNMP Send SNMP Alerts to IP: 0.0.0.0
○ Email Send Email to:

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

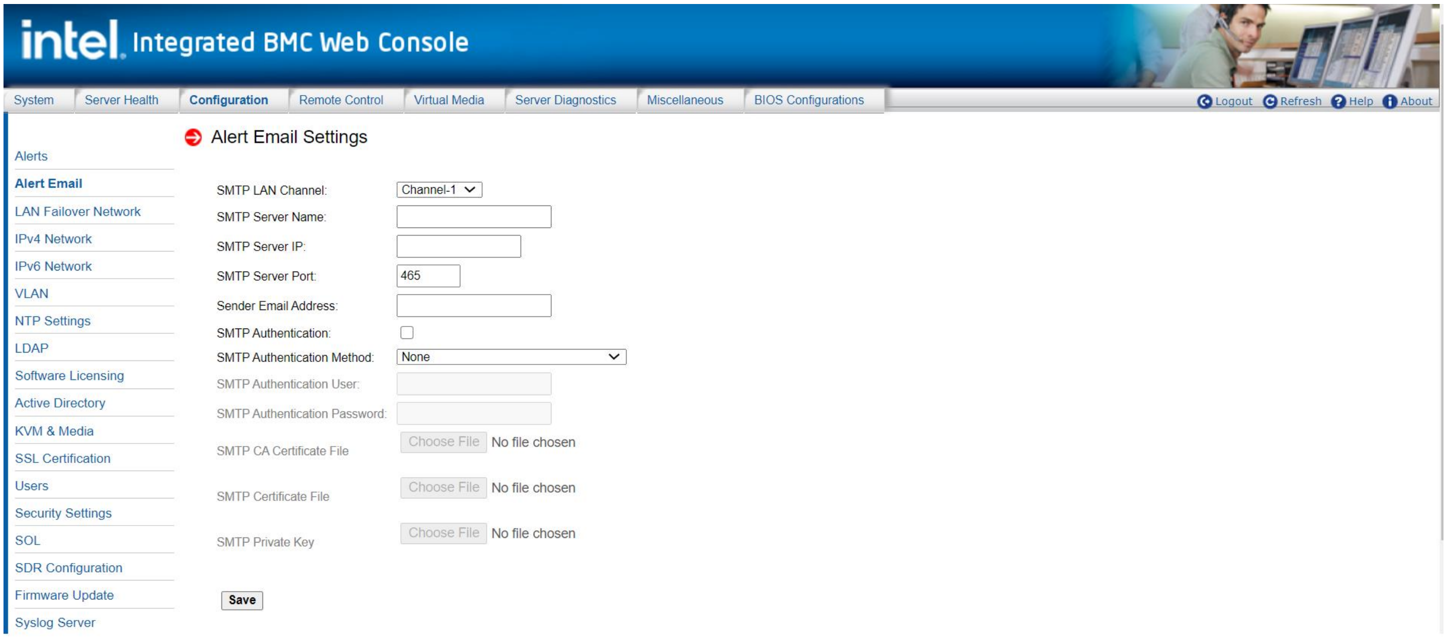
Figure 51. Alerts Page

Table 8. Alerts Options

Option	Task
Globally Enable Platform Event Filtering	This can be used to prevent sending alerts until the user has fully specified the desired alerting policies.
Log Event for Filter Action	This can be used to enable or disable the logging of an event into the System Event Log when a Filter Action is taken.
Select the events that will trigger alerts	Select one or more system events that will trigger an alert.
Check/Clear All	Click to select or clear all events.
Alert Destination #1/#2	Select either SNMP along with the IP address or email address for the alert to be sent to. Up to two destinations can be selected for each LAN channel.
Save	Click to use the selected setup.
Send Test Alerts	After configuring, select this option to send a test alert.

7.3.2 Alert Email

Use this page to configure the parameters for alert emails. Table 9 lists the options to configure alert emails.



Alert Email Settings

SMTP LAN Channel: Channel-1

SMTP Server Name:

SMTP Server IP:

SMTP Server Port: 465

Sender Email Address:

SMTP Authentication: □

SMTP Authentication Method: None

SMTP Authentication User:

SMTP Authentication Password:

SMTP CA Certificate File: No file chosen

SMTP Certificate File: No file chosen

SMTP Private Key: No file chosen

Figure 52. Alert Email Page

Table 9. Alert Email Options

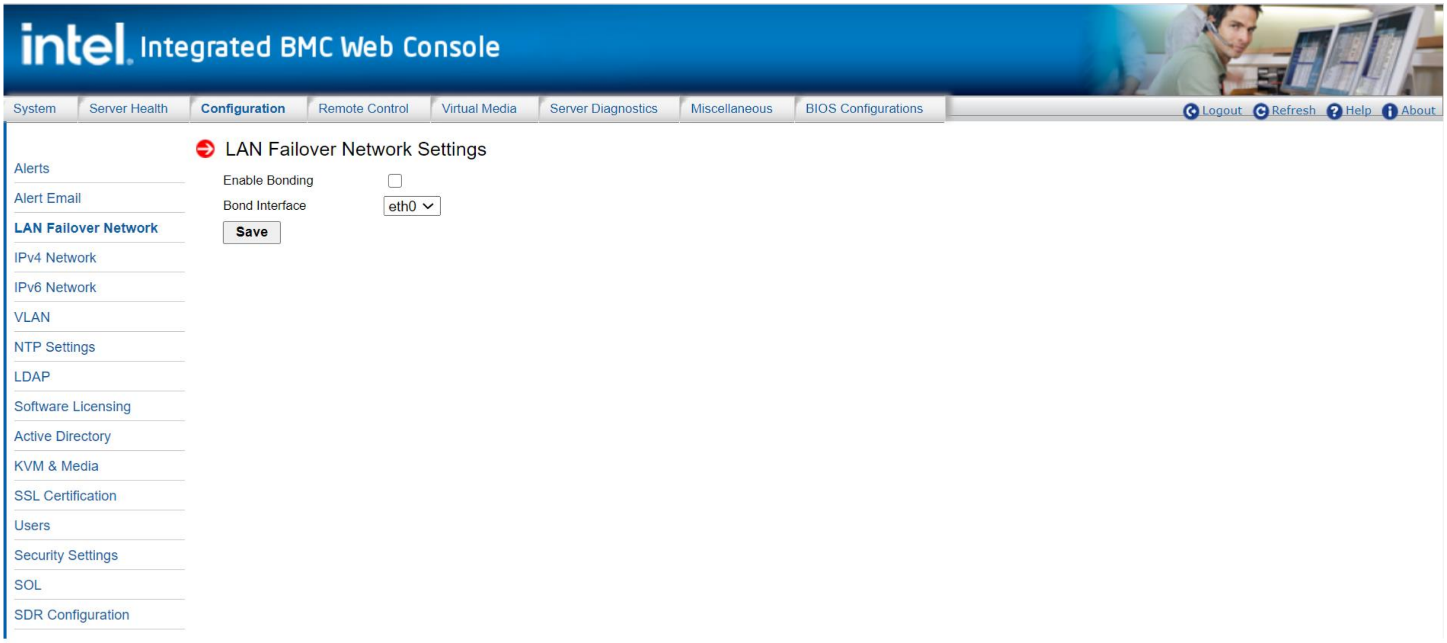
Option	Task
SMTP LAN Channel	Lists the LAN Channel(s) available for server management.
SMTP Server Name	Enter the **Server Name** of the SMTP Server. This field is for Information Purpose Only. • Server Name is a string of 25 alpha-numeric characters maximum. • Spaces and special characters are not allowed.
SMTP Server IP	The IP address of the remote SMTP Mailserver that Alert email should be sent to. • IP address is made of four numbers separated by dots as in "xxx.xxx.xxx.xxx". • “xxx” ranges from 0 to 255. • First “xxx” must not be 0.
SMTP Server Port	The IP port number for which the remote SMTP Mailserver is listening. SMTP servers without encryption and servers supporting STARTTLS generally listen on TCP Port 25. SMTP servers supporting SSL/TLS (SMTPS) generally listen on TCP port 465.
Sender Email Address	The sender address string to be put in the From: field of outgoing alert emails.
SMTP Authentication	Check the option **Enable** to enable SMTP Authentication. **The supported SMTP Server Authentication Types are:** • CRAM-MD5 • LOGIN • PLAIN If the SMTP server does not support any of the above authentication types, the user gets an error message stating: “Authentication type is not supported by SMTP Server”.

Option	Task
SMTP Authentication Method	Use this option to select the SMTP authentication and encryption methods supported by the remote SMTP Mailserver. SMTP authentication without encryption is not supported. **Options:** • **None.** Use this option if the remote SMTP Mailserver does not support STARTTLS or SSL/TLS encryption methods. • **Authentication after STARTTLS.**Use this option if the remote SMTP Mailserver only supports STARTTLS encryption and need to upload certificate for following fields. ○ SMTP CA Certificate File ○ CACERT key file should be of pem type. ○ SMTP Certificate File ○ CERT key file should be of pem or crt type. ○ SMTP Private Key ○ SMTP key file should be of pem or key type. • **Authentication over TLS/SSL Session.** Use this option if the remote SMTP Mailserver supports full SSL/TLS encrypted sessions (SMTPS).
SMTP Authentication User	User email account on the remote SMTP mail server used for SMTP authentication. This option is not available if SMTP Authentication is set to disable.
SMTP Authentication Password	User password on the remote SMTP mail server used for SMTP authentication. This option is not available if SMTP Authentication Method is set to None.
SMTP CA Certificate File	Upload CACERT key file.
SMTP Certificate File	Upload CERT key file.
SMTP Private Key	Upload SMTP key file.
Save button	Click to save any changes made.

7.3.3 LAN Failover Network Settings

Use this page to configure the network bond settings for server management. See Figure 53 for details. Table 10 lists the options to configure Date & Time.

Note: Close any active KVM session before changing the network settings, to avoid disconnection from the server.



LAN Failover Network Settings

Enable Bonding □

Bond Interface eth0

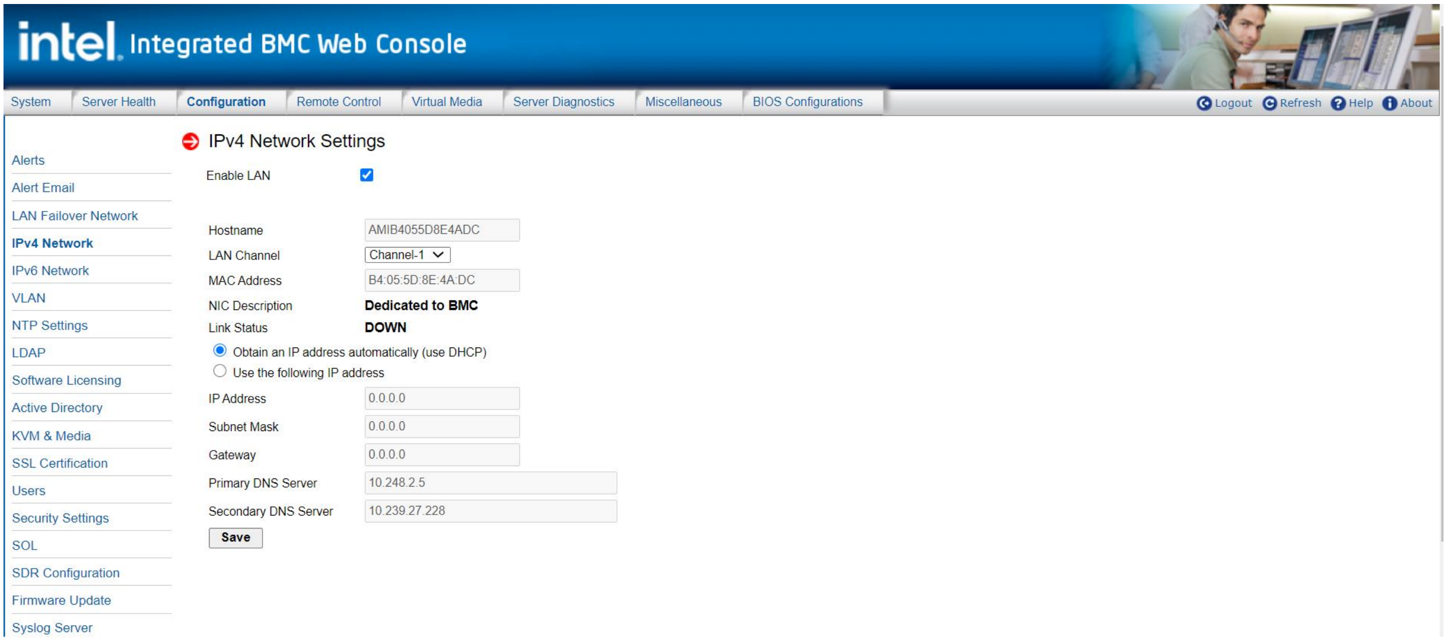
Figure 53. LAN Failover Network Settings Page

Table 10. LAN Failover Network Settings Options

Option	Task
Enable Bonding	Check this option to enable bonding for the network interfaces. **Note:** If VLAN is enabled for either secondary interface, then Bonding cannot be enabled.
Bond Interface	This option lets the user configure bonding for the network interfaces. **This is enabled by default.** **Note:** A minimum of two network interfaces must enable Network bonding for the device.
Save button	Click to save any changes made.

7.3.4 IPv4 Network Settings

Through the IPv4 Network Settings page, the user can configure the IPv4 network settings for the server management LAN interface to the BMC controller. See Figure 54 and Figure 55 for details. Table 11 lists the options available on this page.



IPv4 Network Settings

Enable LAN ☑

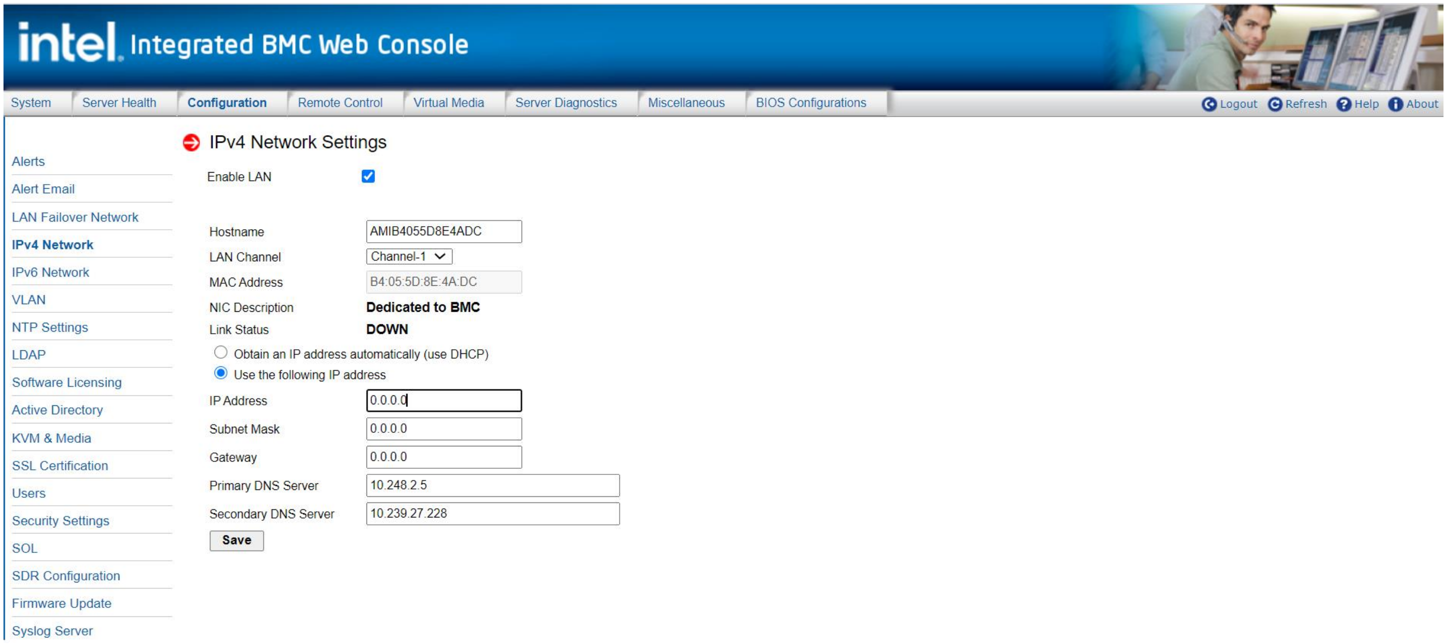
Hostname	AMIB4055D8E4ADC
LAN Channel	Channel-1
MAC Address	B4:05:5D:8E:4A:DC
NIC Description	**Dedicated to BMC**
Link Status	**DOWN**

● Obtain an IP address automatically (use DHCP)

○ Use the following IP address

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS Server	10.248.2.5
Secondary DNS Server	10.239.27.228

Figure 54. IPV4 Network DHCP Page



IPv4 Network Settings

Enable LAN	☑
Hostname	AMIB4055D8E4ADC
LAN Channel	Channel-1
MAC Address	B4:05:5D:8E:4A:DC
NIC Description	Dedicated to BMC
Link Status	DOWN

○ Obtain an IP address automatically (use DHCP)

● Use the following IP address

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
Primary DNS Server	10.248.2.5
Secondary DNS Server	10.239.27.228

Figure 55. IPv4 Network Static Page

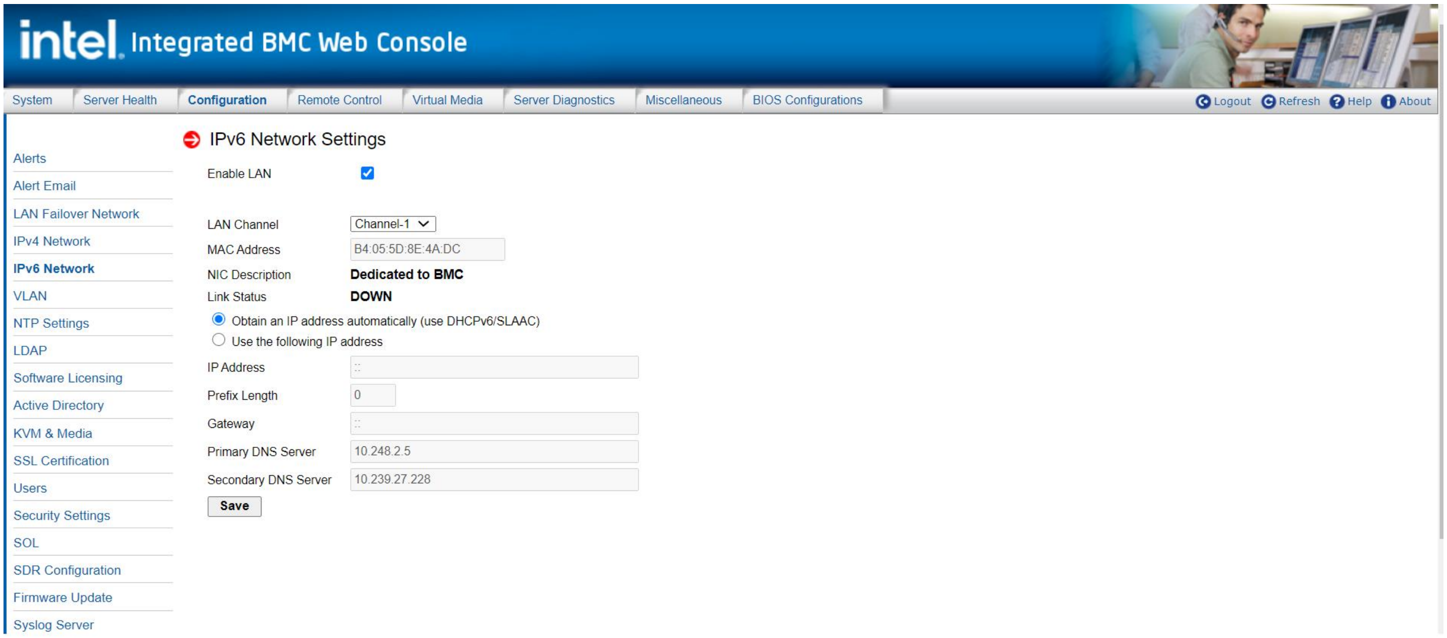
Warning: Each network controller must be on a different subnet than all other controllers used for management traffic.

Table 11. IPv4 Network Settings Options

Option	Task
Enable LAN	Select the LAN interface to be configured.
Host Name	The hostname is an RFC 1123 compliant string less than 64 alpha-numeric characters. Hyphen characters are allowed if the hyphen is not the first or final character in the hostname. **Default value:** BMC + MAC address.
LAN Channel	Lists the LAN Channel(s) available for server management.
MAC Address	The MAC address of the device (read only).
NIC Description	NIC dedicated to BMC / Host or shared between Host and BMC of LAN Channel(s) (read only).
Link Status	NIC Link status of LAN Channel(s) (read only).
IP Address	Select one of the two options to configure the IP address: • **Obtain an IP address automatically (use DHCP).** Uses DHCP to obtain the IP address. • **Use the following IP address.** Manually configure the IP address.
IP Address **Subnet Mask** **Gateway**	If configuring a static IP, enter the requested address, subnet mask, and gateway in the given fields. The IP address is made of four numbers separated by dots as in “xxx.xxx.xxx.xxx”. “xxx” ranges from 0 to 255. The first “xxx” must not be 0.
Primary DNS Server **Secondary DNS Server**	If configuring a static IP, enter the Primary and Secondary DNS servers.
Save	Click to save any changes made.

7.3.5 IPv6 Network Settings

The IPv6 Network Settings page lets the user enable and configure the IPv6 network settings and to enable and configure LAN failover (see Figure 56). Table 12 lists the options available on this page.



IPv6 Network Settings

Enable LAN ☑

LAN Channel: Channel-1

MAC Address: B4:05:5D:8E:4A:DC

NIC Description: **Dedicated to BMC**

Link Status: **DOWN**

● Obtain an IP address automatically (use DHCPv6/SLAAC)

○ Use the following IP address

IP Address: ::

Prefix Length: 0

Gateway: ::

Primary DNS Server: 10.248.2.5

Secondary DNS Server: 10.239.27.228

Figure 56. IPv6 Network Page

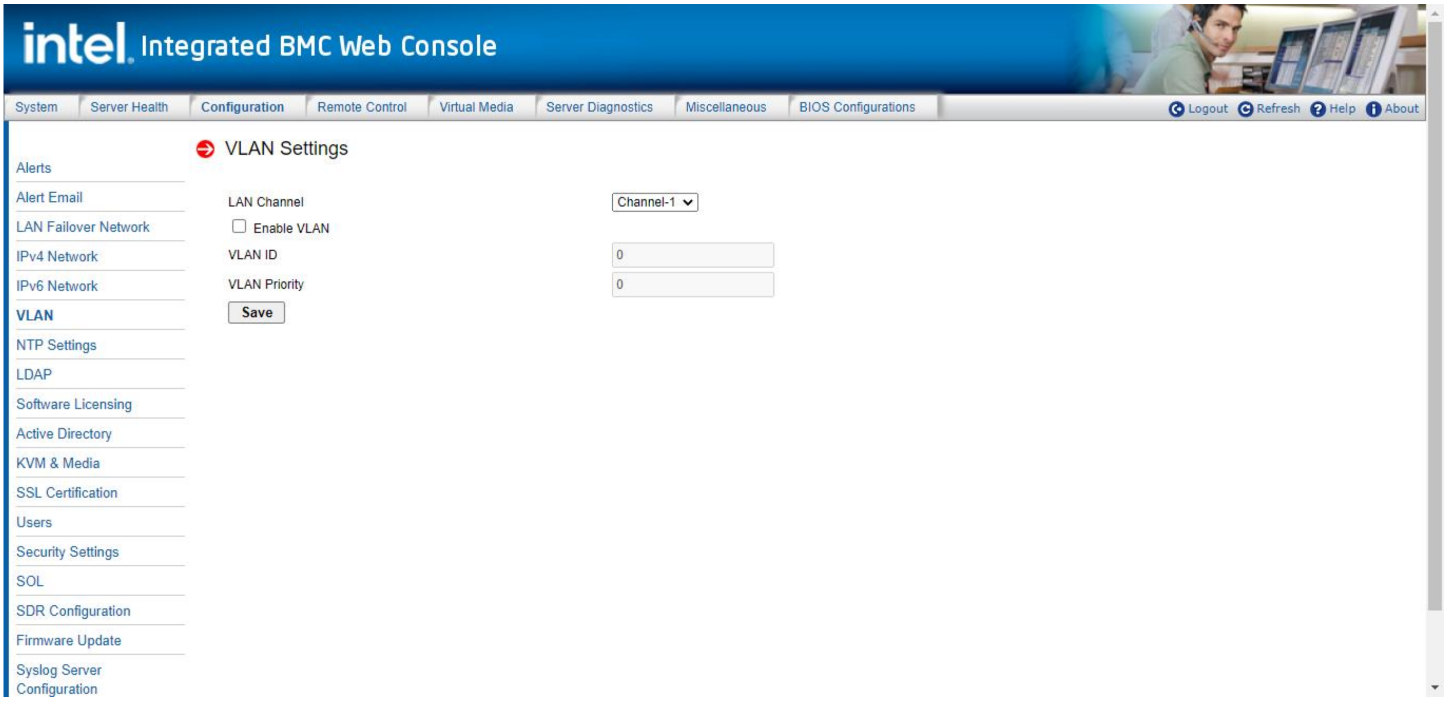
Warning: Each network controller must be on a different subnet than all other controllers used for management traffic.

Table 12. IPv6 Network Settings Options

Option	Task
Enable LAN	Select the LAN interface to be configured.
LAN Channel	Lists the LAN Channel(s) available for server management.
MAC Address	The MAC address of the device (read only).
NIC Description	NIC dedicated to BMC / Host or shared between Host and BMC of LAN Channel(s) (read only).
Link Status	NIC link status of LAN Channel(s) (read only).
IP address	Select one of the two options for configuring the IP address: • **Use IPv6 auto-configuration (stateless ICMPv6 discovery).** Uses ICMPv6 to obtain the IP address. • **Obtain an IP address automatically (use DHCPv6).** Uses DHCPv6 to obtain the IP address. • **Use the following IP address.** Manually configure the IP address.
IP Address **Gateway**	If configuring a static IP, enter the requested address and gateway in the given fields. The IP address and Gateway are 128-bit fields made of eight hexadecimal numbers separated by colons as in “xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx”. “xxxx” ranges from 0 to FFFF. First “xxxx” must not be 0. One or more consecutive groups of zero value can be replaced with a single empty group using two consecutive colons (::).
Prefix Length	Select the routing prefix length.
Primary/Secondary DNS server	If configuring a static IP, enter the Primary and Secondary DNS servers.
Save	Click to save any changes made.

7.3.6 VLAN Settings

The VLAN Settings page lets the user enable and configure the VLAN private network settings on the selected server management LAN channels (see Figure 57). Table 13 lists the options available on this page.



VLAN Settings

LAN Channel: Channel-1

☐ Enable VLAN

VLAN ID: 0

VLAN Priority: 0

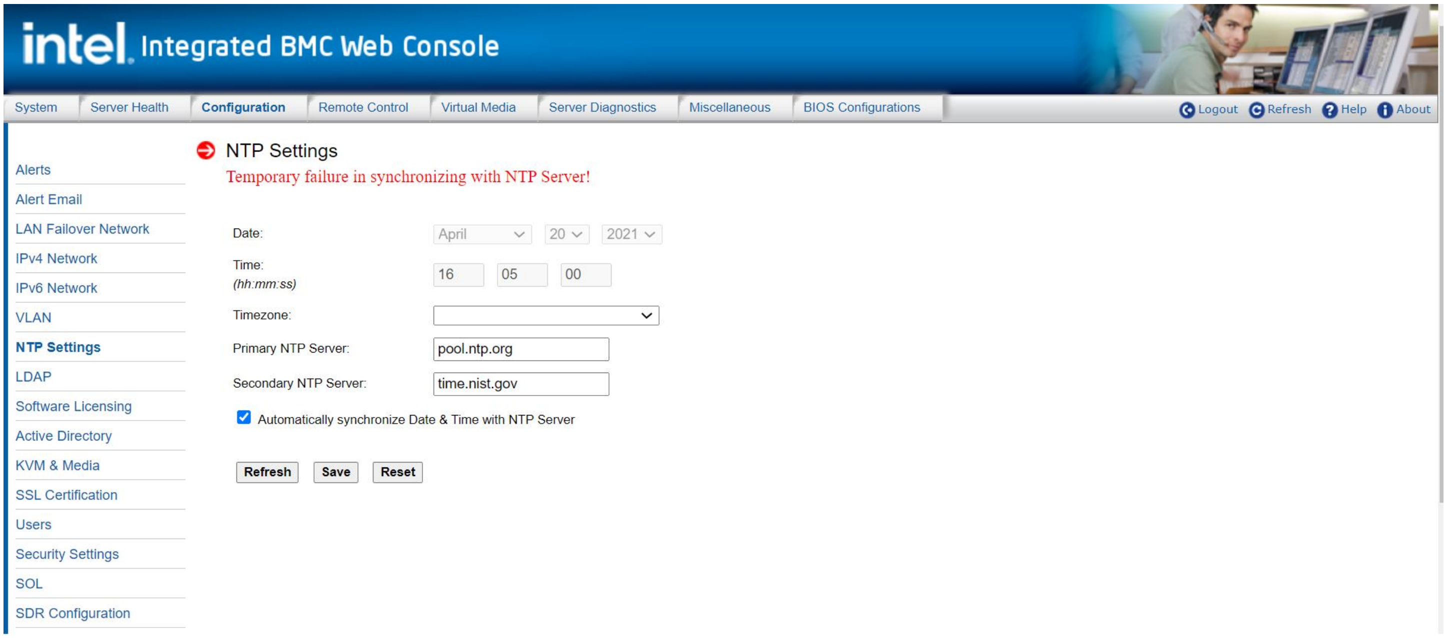
Figure 57. VLAN Settings Page

Table 13. VLAN Settings Options

Option	Task
LAN Channel	Lists the LAN Channel(s) 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.
Enable VLAN	Check to enable VLAN on this channel. When enabled, the BMC only accepts packets with the correct VLAN Identifier field. All outgoing packets are marked with that VLAN ID.
VLAN ID	Specify the VLAN ID to use. Values are from 1 to 4094. Only one ID can be used at a time.
VLAN Priority	Specify the VLAN Priority field to place in outgoing packets. Priority code point (PCP) values in order of priority are: • **1** (background), 0 (best effort) • **2** (excellent effort) • **3** (critical application) • **4** (video) • **5** (voice) • **6** (internetwork control) • **7** (network control) • **0** (best effort) **is the default**
Save	Click to save the current settings.

7.3.7 NTP Settings

This page displays the device's current Date & Time Settings. It can be used to configure either Date & Time or the network time protocol (NTP) server settings for the device. See Figure 58 for details. Table 11 lists the options available on this page.



NTP Settings

Temporary failure in synchronizing with NTP Server!

Date: April 20 2021

Time: (hh:mm:ss) 16 05 00

Timezone:

Primary NTP Server: pool.ntp.org

Secondary NTP Server: time.nist.gov

☑ Automatically synchronize Date & Time with NTP Server

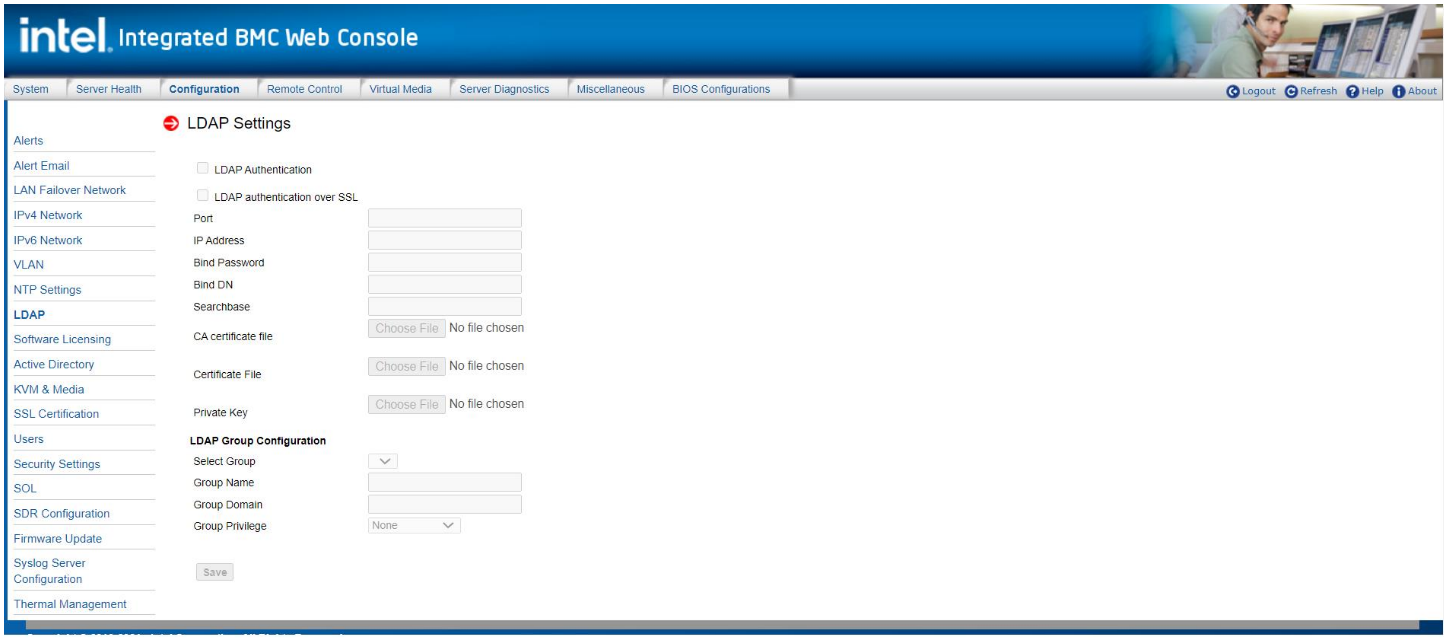
Figure 58. NTP Settings Page

Table 14. NTP Settings Options

Option	Task
Date	Specify the current Date for the device.
Time	Specify the current Time for the device. **Note:** As a year 2038 problem exists, the acceptable date range is from 01-01-2005 to 01-18-2038.
Timezone	Timezone list contains the UTC offset along with the locations and Manual UTC offset for NTP server, which can be used to display the exact local time.
Primary NTP Server & Secondary NTP Server	Specify the NTP Servers for the device. NTP Server fields support the following: • IP address (Both IPv4 and IPv6 format). • FQDN (Fully qualified domain name) format. • FQDN Value ranges from 1 to 128 alpha-numeric characters. **Notes:** • Secondary NTP server is optional field. • If the Primary NTP server is not working fine, then the Secondary NTP Server is tried.
Automatically synchronize	Check this option to automatically synchronize Date and Time with the NTP Server.
Refresh	Click **Refresh** to reload the current Date & Time settings.
Save	Click to save the current settings.
Reset	Click **Reset** to reset the modified changes.

7.3.8 LDAP Settings

The LDAP Settings page lets the user enable/disable the LDAP settings on the selected server management LAN channels. See Figure 59 and Table 15 for available options on this page.



LDAP Settings

□ LDAP Authentication

□ LDAP authentication over SSL

Port

IP Address

Bind Password

Bind DN

Searchbase

CA certificate file: Choose File No file chosen

Certificate File: Choose File No file chosen

Private Key: Choose File No file chosen

LDAP Group Configuration

Select Group

Group Name

Group Domain

Group Privilege: None

Figure 59. LDAP Settings Page

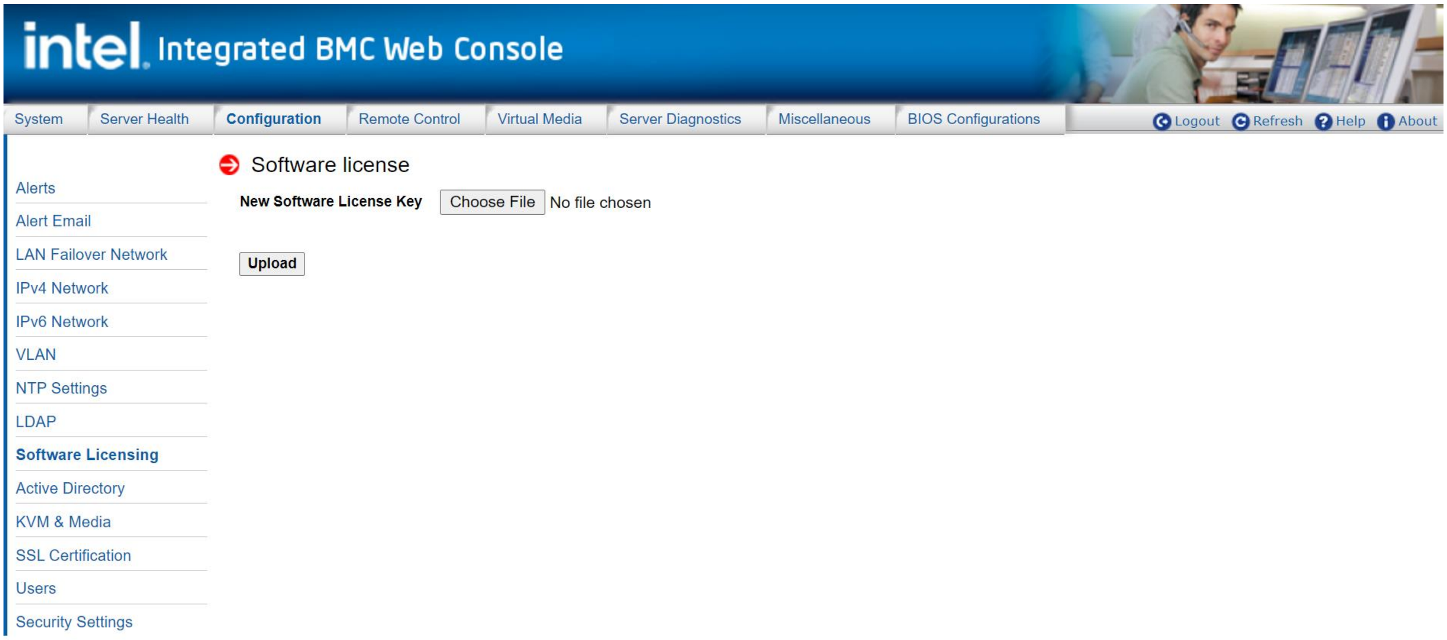
Table 15. LDAP Settings Options

Option	Task
LDAP Authentication	Check this box to enable LDAP authentication, then enter the required information to access the LDAP server.
LDAP authentication over SSL	Check this box to enable LDAP authentication over SSL.
Port	Specify the LDAP Port.
IP Address	The IP address of LDAP server. • IP address made of four numbers separated by dots, as in "xxx.xxx.xxx.xxx". • "xxx" ranges from 0 to 255. • First "xxx" must not be 0.
Bind Password	Authentication password for LDAP server. The password must be at least four characters long.
Bind DN	The Distinguished Name of the LDAP server, like "`cn=Manager, dc=my-domain, dc=com`".
Search base	The search base of the LDAP server, such as "`dc=my-domain, dc=com`". **Note:** If LDAP authentication over SSL is enabled, the user needs to upload the following files: • **CA Certificate File** - File that contains the certificate of the trusted CA certs. - CA certificate file should be pem type • **Certificate File** - Client certificate filename. - Certificate File should be pem type • **Private Key** - Client private key filename. - Private Key should be pem type
CA certificate file	Upload CA Certificate File.
Certificate File	Upload Certificate File.

Option	Task
Private Key	Upload Private Key.
LDAP Group Configuration	Configure the LDAP search filters associated with BMC network privileges. For example, "(&(cn=BMCAdminGroup)(memberUid=%s))"
Select Group	Select the group dropdown to Configure
Group Name	Role Group Name is a string of 64 alpha-numeric characters. Special symbols hyphen and underscore are allowed.
Group Domain	Domain Name is a string of 4–64 alpha-numeric characters. It must start with an alphabetical character. Special symbols like dot (.), comma (,), hyphen (-), underscore (_), equal-to (=) are allowed. Example: "cn=manager,ou=login, dc=domain,dc=com".
Group Privilege	Select the **Role Group Privilege**. This is the level of privilege to be assigned for this role group
Save	Click to save the current settings.

7.3.9 Software License

The Software License page allows the user to upload a new software license key. Use the **Browse** button to navigate to the file and press the **Upload** button. See Figure 60.



New Software License Key: No file chosen

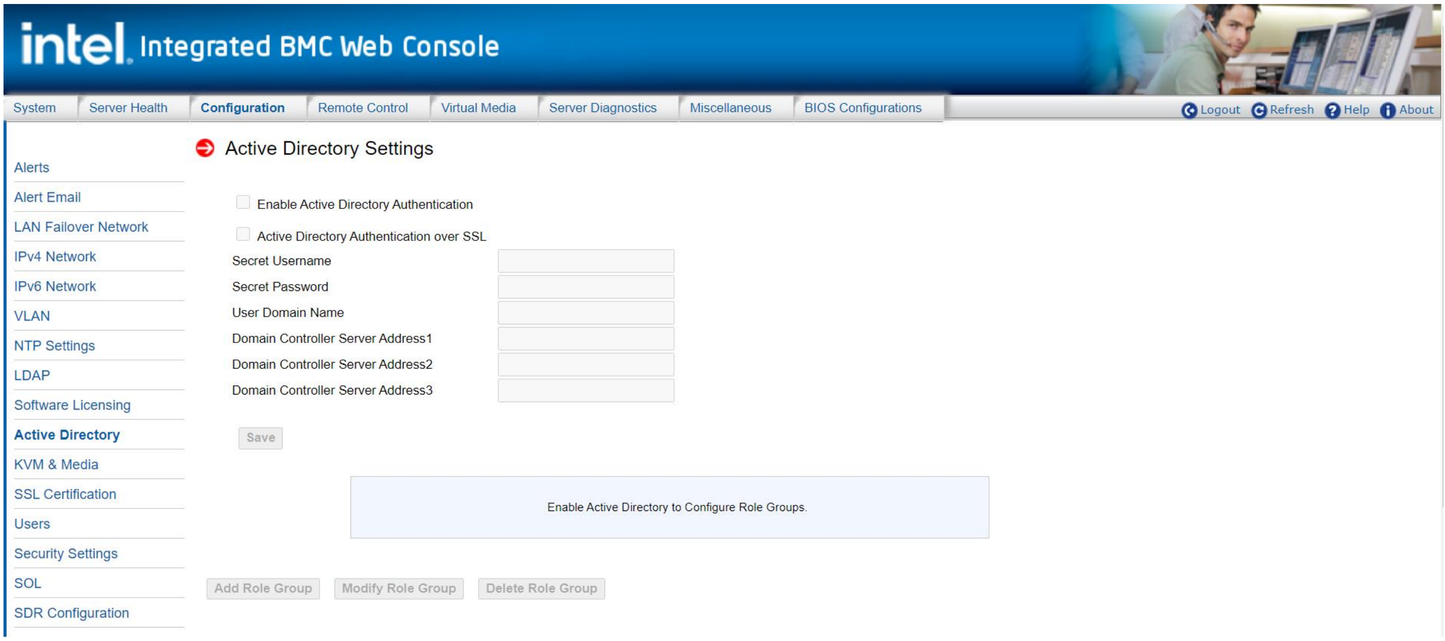
Figure 60. Software Licensing Page

Table 16. Software Licensing Options

Option	Task
Choose File	Choose the file to be uploaded.
Upload	Upload the software license to the BMC for update action.

7.3.10 Active Directory* (AD*) Settings

The Active Directory* Settings page is used to configure the Active Directory* Authentication and to enable/disable Active Directory* Authentication over SSL. See Figure 61 for available options.



Active Directory Settings

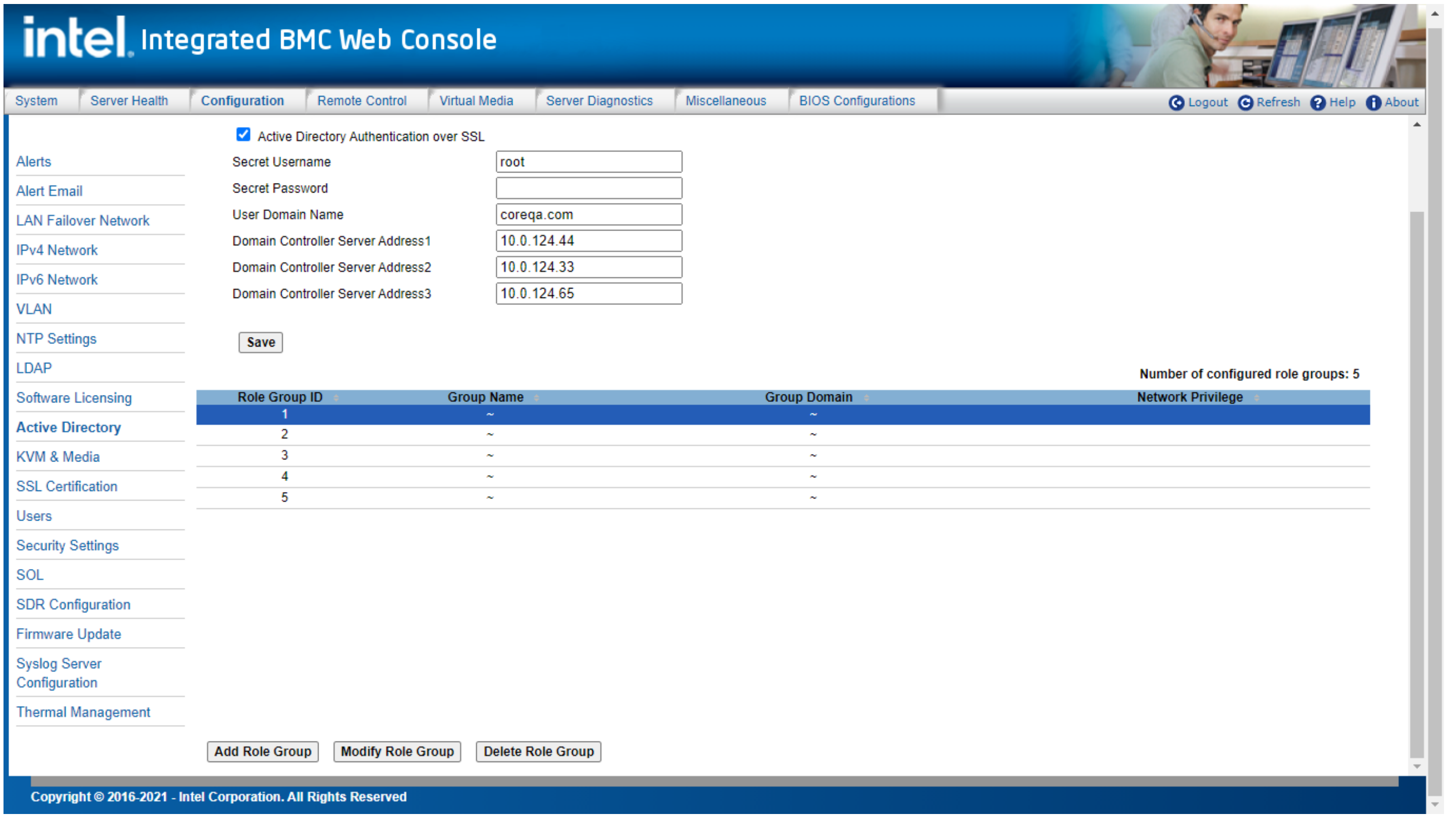
☐ Enable Active Directory Authentication

☐ Active Directory Authentication over SSL

Secret Username	
Secret Password	
User Domain Name	
Domain Controller Server Address1	
Domain Controller Server Address2	
Domain Controller Server Address3	

Enable Active Directory to Configure Role Groups.

Figure 61. Active Directory* Settings Page



☑ Active Directory Authentication over SSL

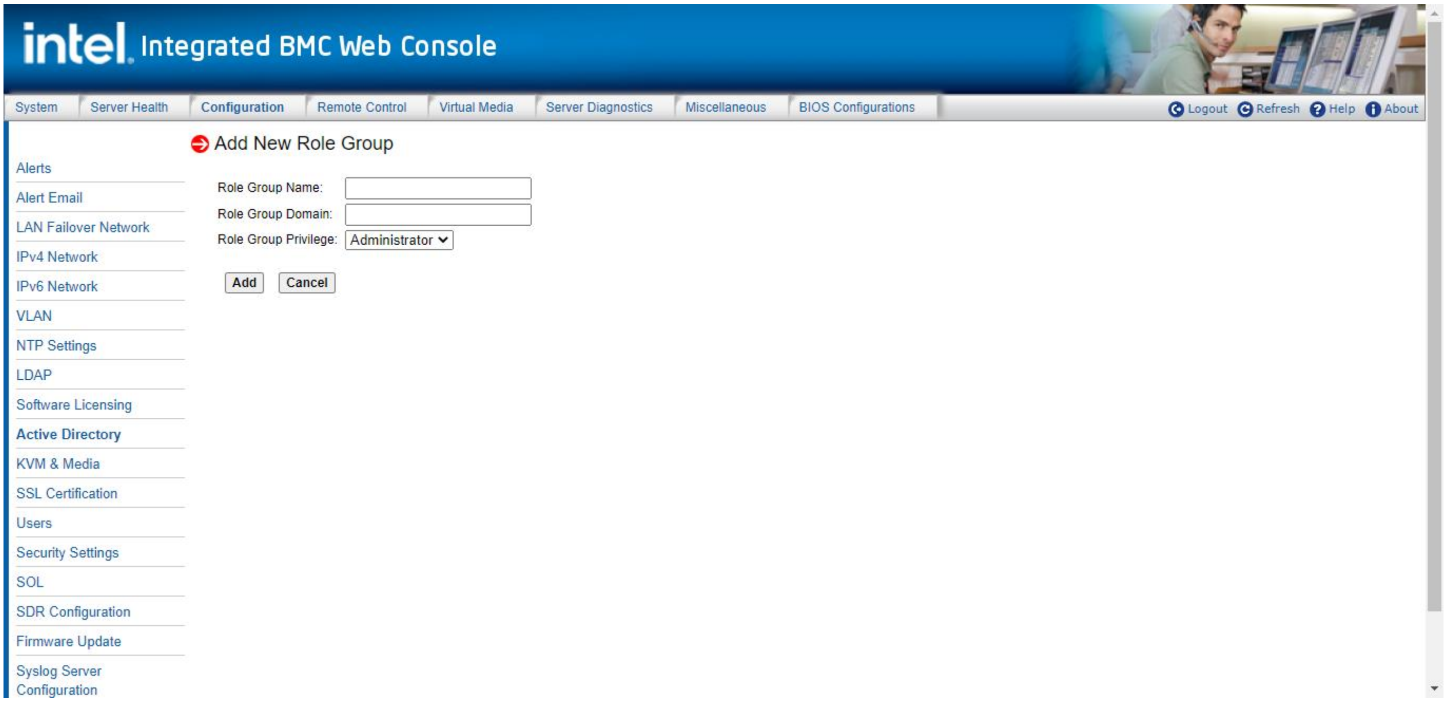
Secret Username	root
Secret Password	
User Domain Name	coreqa.com
Domain Controller Server Address1	10.0.124.44
Domain Controller Server Address2	10.0.124.33
Domain Controller Server Address3	10.0.124.65

Number of configured role groups: 5

Role Group ID	Group Name	Group Domain	Network Privilege
1	~	~	
2	~	~	
3	~	~	
4	~	~	
5	~	~	

Figure 62. Active Directory* Role Group Page

After configuring the Active Directory* Settings, to add a group, select an empty slot in the list and click the **Add Role Group** button. Set **Role Group Name**, **Role Group Domain** and **Role Group Privilege**, as shown in Figure 63.



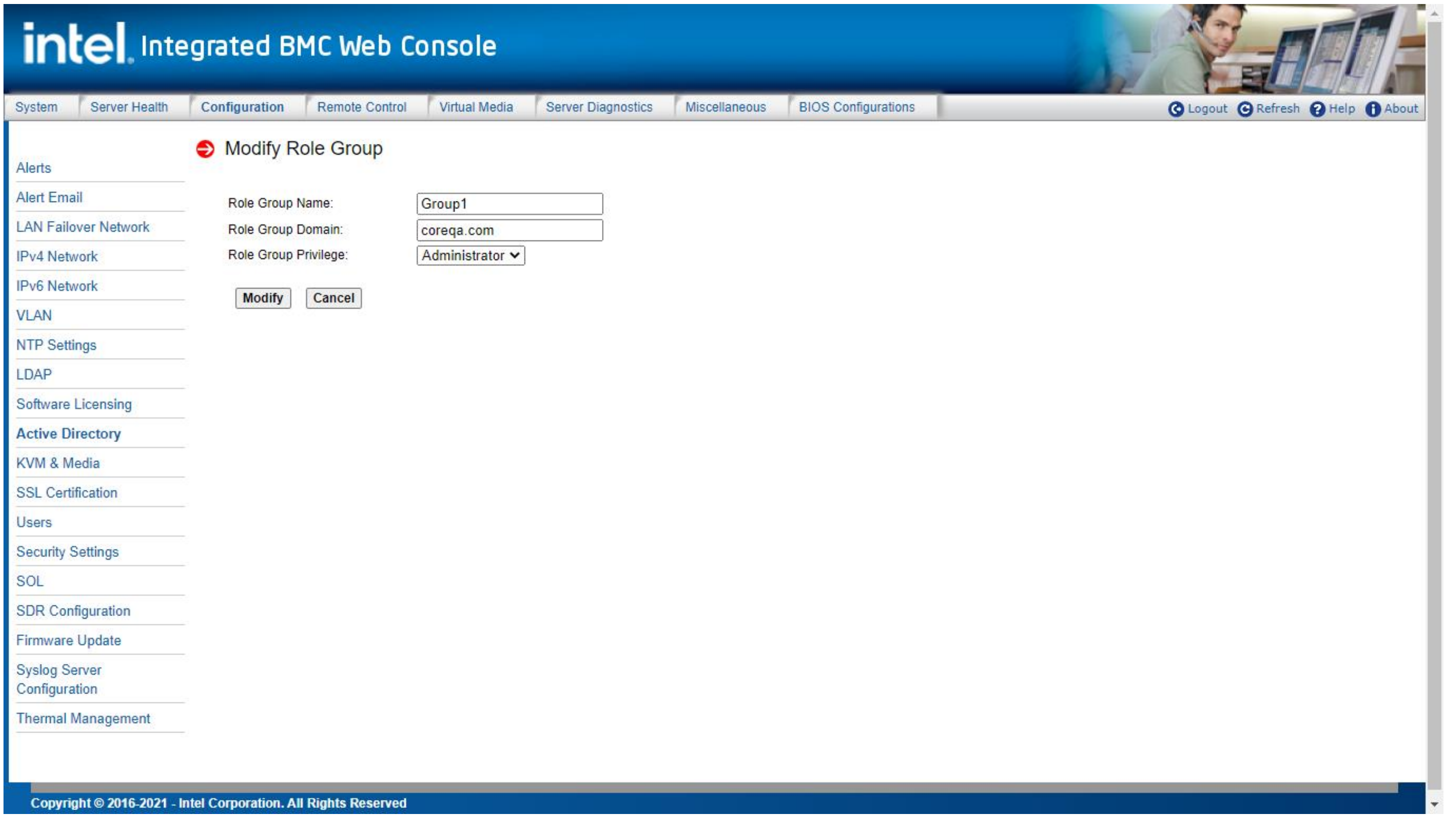
Add New Role Group

Role Group Name:

Role Group Domain:

Role Group Privilege: Administrator

Figure 63. Add Role Group Page



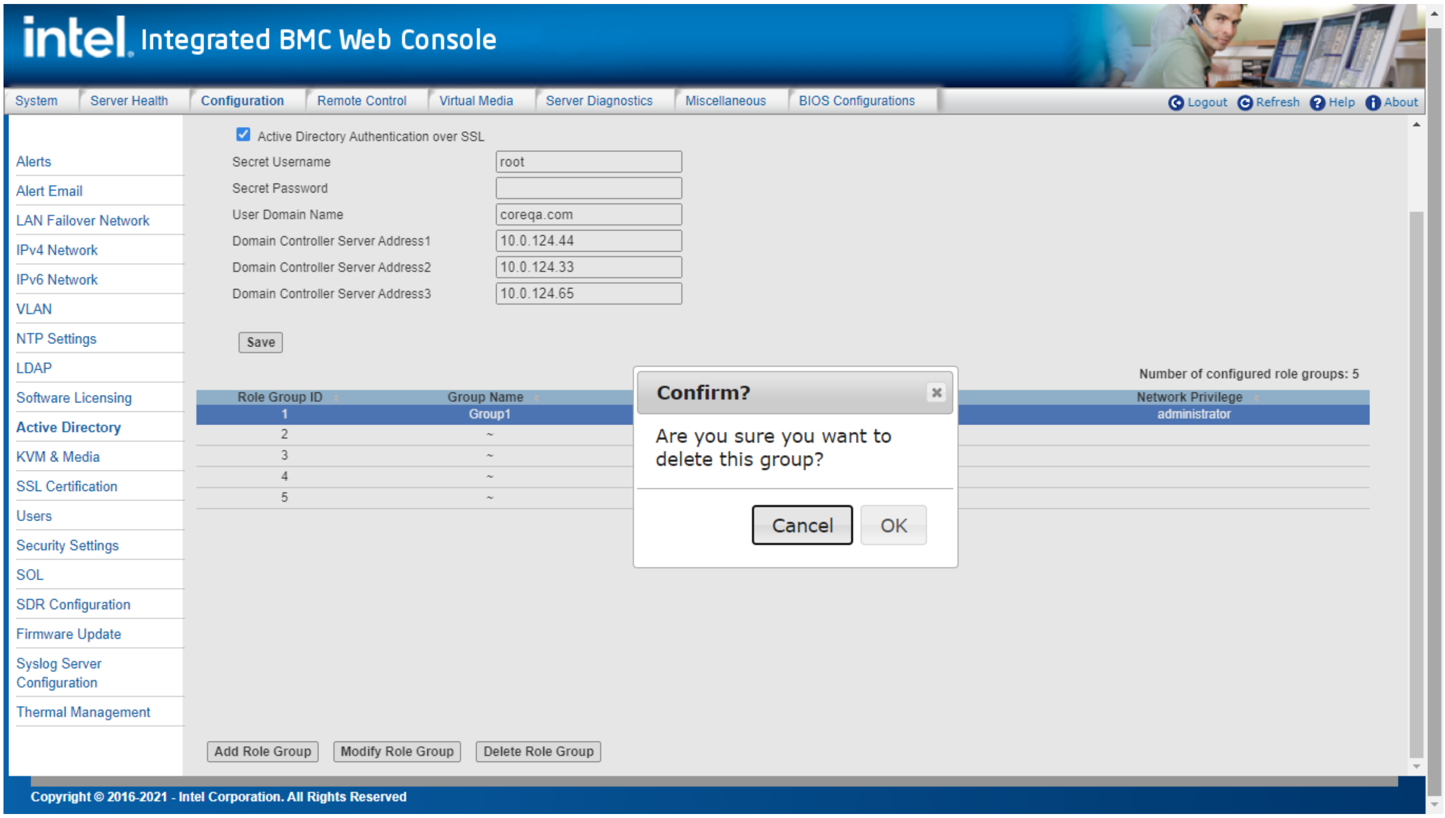
Modify Role Group

Role Group Name: Group1

Role Group Domain: coreqa.com

Role Group Privilege: Administrator

Figure 64. Modify Role Group Page



☑ Active Directory Authentication over SSL

Secret Username	root
Secret Password	
User Domain Name	coreqa.com
Domain Controller Server Address1	10.0.124.44
Domain Controller Server Address2	10.0.124.33
Domain Controller Server Address3	10.0.124.65

Save

Number of configured role groups: 5

Role Group ID	Group Name	Network Privilege
1	Group1	administrator
2	~	
3	~	
4	~	
5	~	

Confirm?

Are you sure you want to delete this group?

Cancel OK

Add Role Group   Modify Role Group   Delete Role Group

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

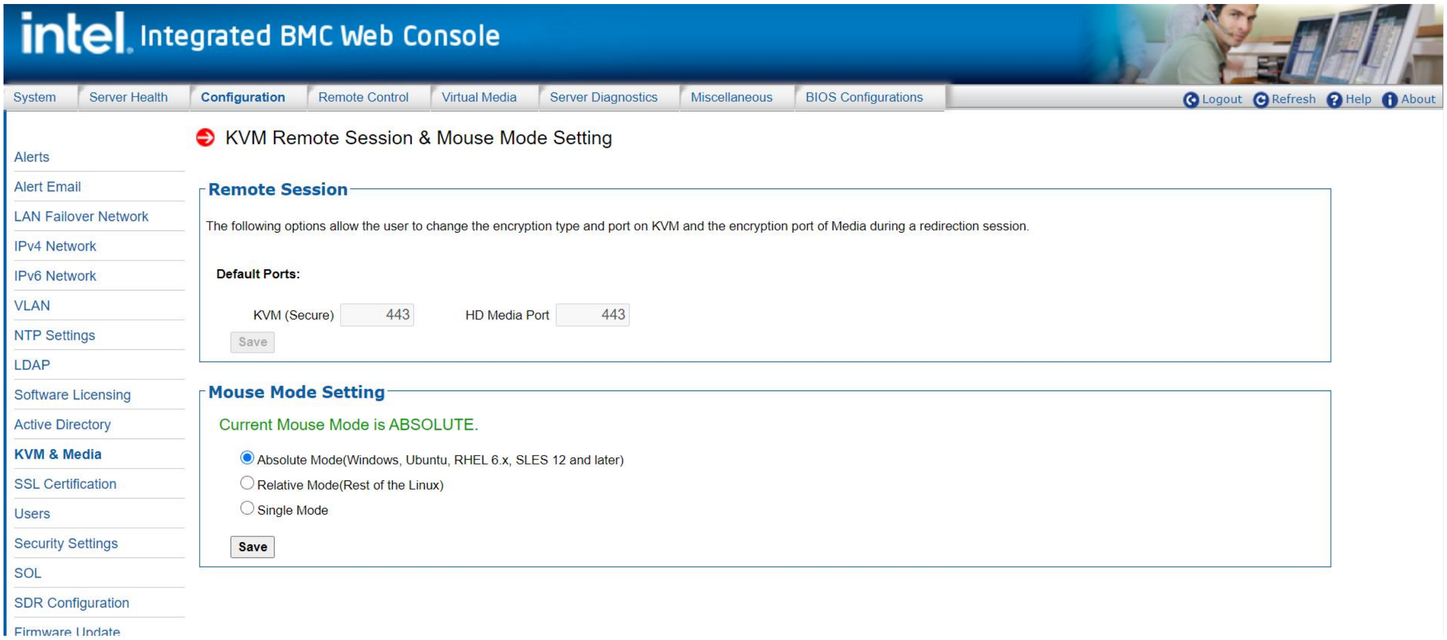
Figure 65. Delete Role Group Page

Table 17. Active Directory* (AD*) Settings Options

Option	Task
Enable Active Directory* Authentication	Select the check box to enable/disable AD* authentication.
Active Directory* Authentication over SSL	Select the check box to enable/disable AD* Authentication over SSL.
Secret Username	Enter the secret username.
Secret Password	Enter the secret password.
User Domain Name	User belongs to which domain in AD* server
Domain Controller Server Address1/2/3	A domain controller server's IP address. The user can enter up to three sets of IP addresses.
Save	Click to save any changes for AD* settings.
Add Role Group	Select an empty role group (`Group Name : "~", Group Domain : "~" and Network Privilege : Reserved`).
Modify Role Group	Modify Role Group Name, Domain and select **Privilege**.
Delete Role Group	Delete role group.
Add/Modify	Click to save any changes for Role Group settings.
Cancel	Click to cancel Add/Modify Role Group settings.

7.3.11 KVM & Media

Use the KVM & Media page to change the type and port of KVM encryption, and the port of media encryption during a redirect session (see Figure 66). Table 18 lists option details.



KVM Remote Session & Mouse Mode Setting

Remote Session

The following options allow the user to change the encryption type and port on KVM and the encryption port of Media during a redirection session.

Default Ports:

KVM (Secure) 443 HD Media Port 443

Save

Mouse Mode Setting

Current Mouse Mode is ABSOLUTE.

● Absolute Mode(Windows, Ubuntu, RHEL 6.x, SLES 12 and later)
○ Relative Mode(Rest of the Linux)
○ Single Mode

Save

Figure 66. KVM & Media Page

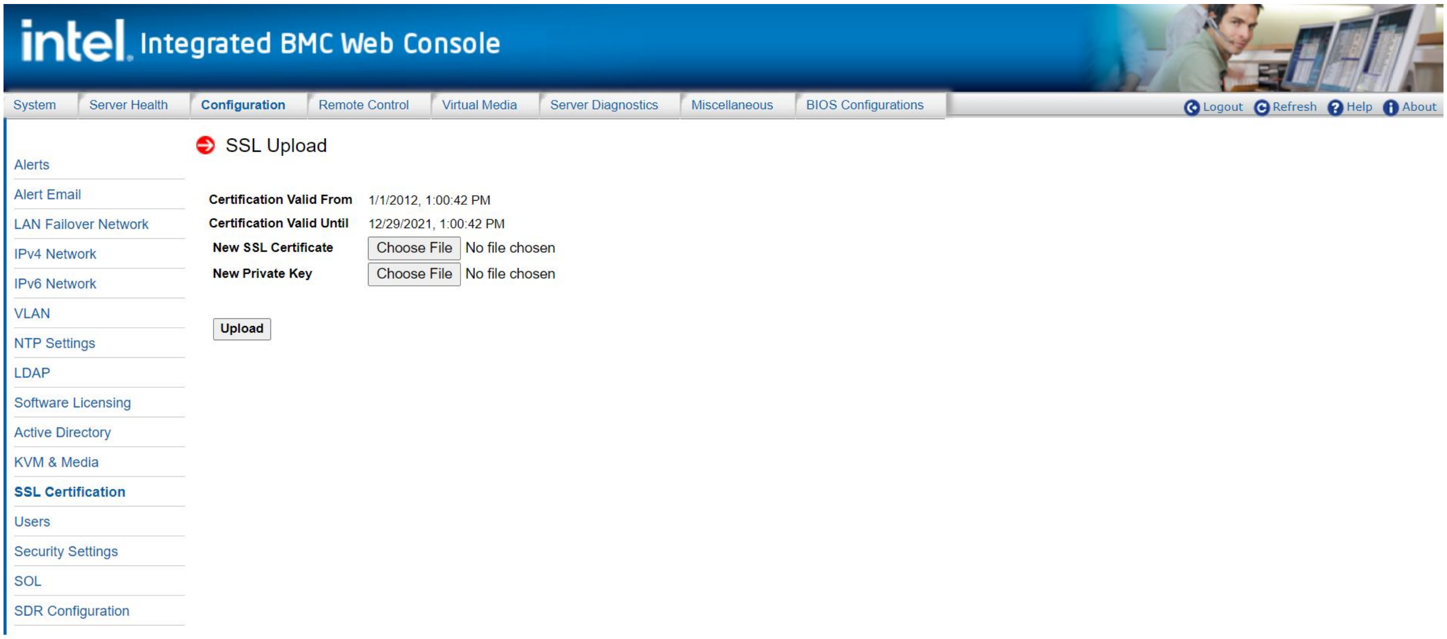
Table 18. KVM & Media Options

Option	Task
Default Ports	Set the ports used by KVM and remote media (both standard and secure ports). Do not change these values unless certain the new ports are unused.
Save (Remote Session)	Click to save any changes for Remote Session.
Mouse Mode Setting	Console Redirection handles mouse emulation from local window to remote screen in one of the following methods: • **Absolute Mode.** Select it to have the absolute position of the local mouse sent to the server. Preferred method where supported. Use this mode for Microsoft Windows* operating system and newer versions of Linux* (Ubuntu*, RHEL*, SLES*). • **Relative Mode.** Select it to have the calculated relative mouse position displacement sent to the server. Use this mode for older Linux* versions such as Red Hat* (RHEL) 5.x. For best results, server and client operating system mouse acceleration/threshold settings should match. Alternatively, use the mouse calibration option in JViewer*. • **Other Mouse Mode.** Select **Single Mode** to have the calculated displacement from the local mouse in the center position, sent to the server. Under this mode, Alt+C should be used to switch between Host and client mouse cursor. Use this mode in special situations such as the SLES* 11 Linux* operating system installation.
Save (Mouse Mode Setting)	Click to save any changes for Mouse Mode Setting.

7.3.12 SSL Certification

The BMC generates a unique, self-signed SSL certificate when the server is first plugged into AC power. This default certificate is less secure than one signed by a certificate authority (CA).

Uploading a CA signed certificate is recommended to allow client software to verify the BMC authenticity. Use this page to upload an SSL certificate and a private key, which allows the device to be accessed in a secured mode. See Figure 67 for details.



SSL Upload

Certification Valid From 1/1/2012, 1:00:42 PM

Certification Valid Until 12/29/2021, 1:00:42 PM

New SSL Certificate No file chosen

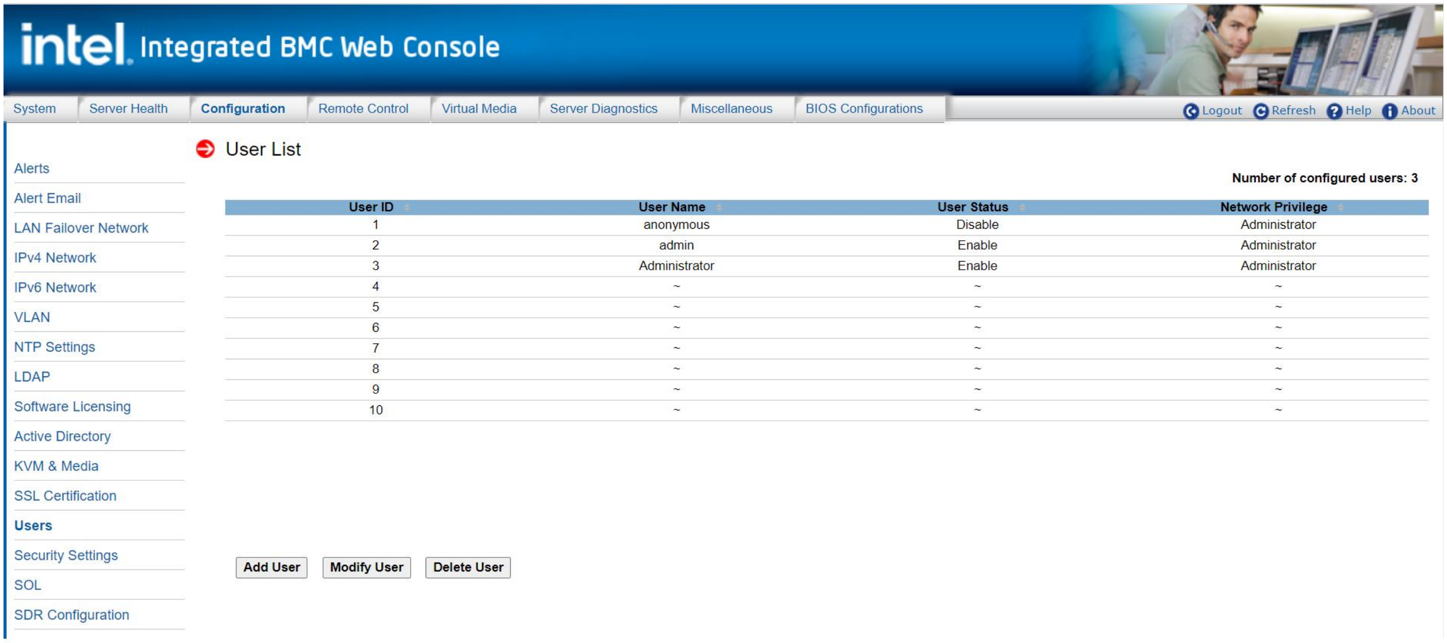
New Private Key No file chosen

Figure 67. SSL Certification Page

First, upload the SSL certificate. The device prompts to upload the private key. A notification is displayed if either of the files is invalid and on successful upload. Click the **Upload** button. On successful upload, the device prompts to reboot. Click **Ok** to reboot or click **Cancel** to cancel the reboot operation.

7.3.13 Users

The Users page lists the configured users, along with their statuses and network privileges. It also provides the capability to add, modify, and delete users. See Figure 68 for details.



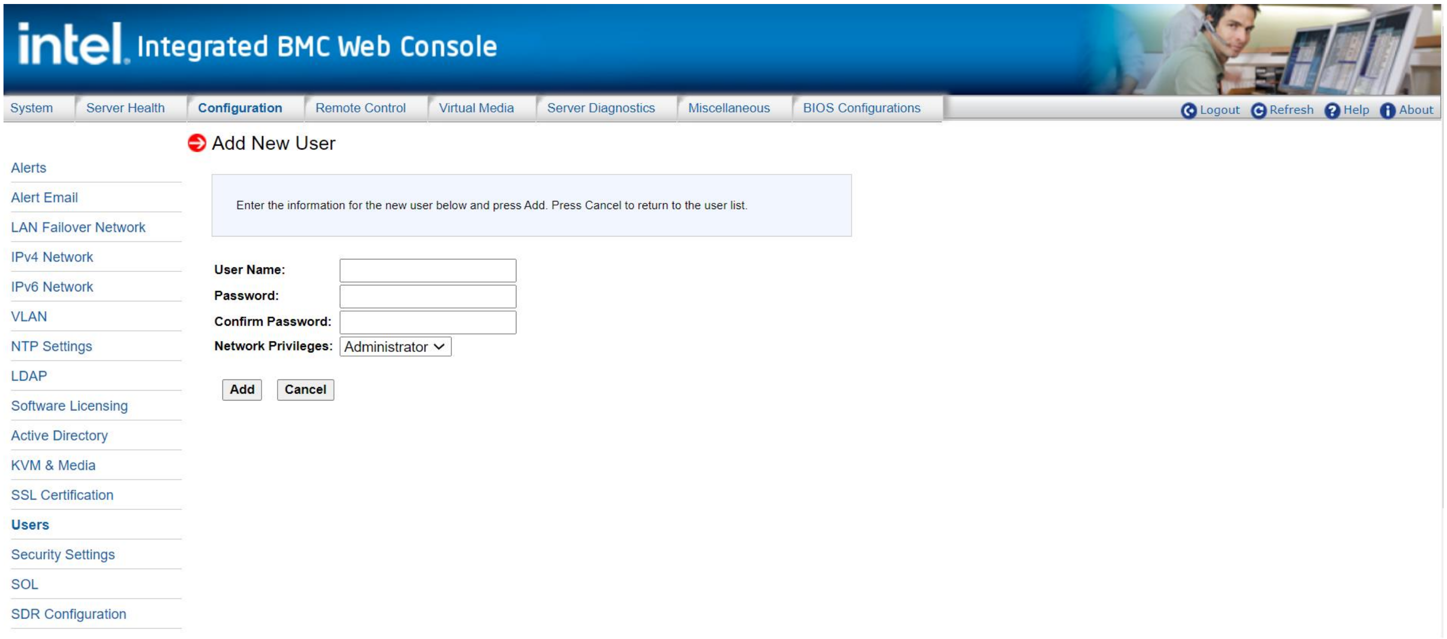
User List

Number of configured users: 3

User ID	User Name	User Status	Network Privilege
1	anonymous	Disable	Administrator
2	admin	Enable	Administrator
3	Administrator	Enable	Administrator
4	~	~	~
5	~	~	~
6	~	~	~
7	~	~	~
8	~	~	~
9	~	~	~
10	~	~	~

Figure 68. User List Page

This page lets the operator configure the IPMI users and privileges for this server. User ID 1 (anonymous) may not be renamed or deleted. To add a user, select an empty slot in the list and click the **Add User** button. Set the **User Name**, **Password**, and **Network Privileges** as shown in Figure 69.



Add New User

Enter the information for the new user below and press Add. Press Cancel to return to the user list.

User Name:

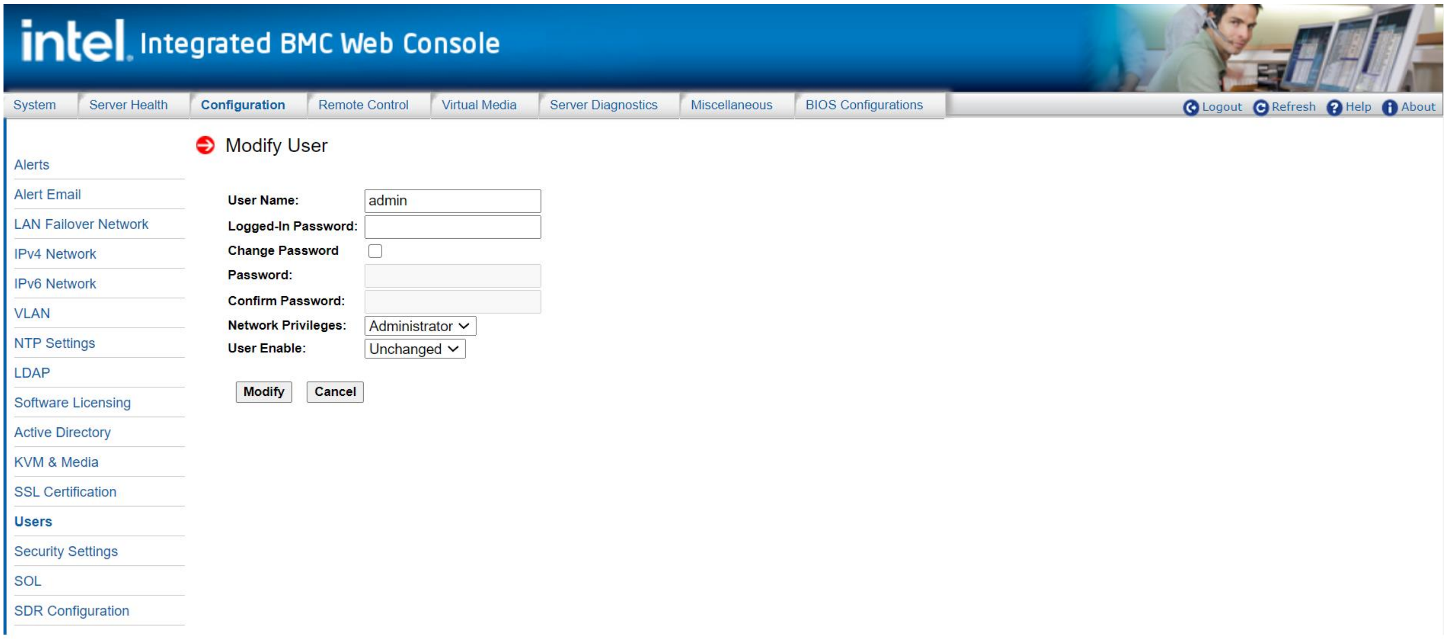
Password:

Confirm Password:

Network Privileges: Administrator

Figure 69. Add New User Page

To modify a user, select a user in the list and click the **Modify User** button. Change the **User Name**, **Password**, **Enable** status, and **Network Privileges**, as shown in Figure 70.

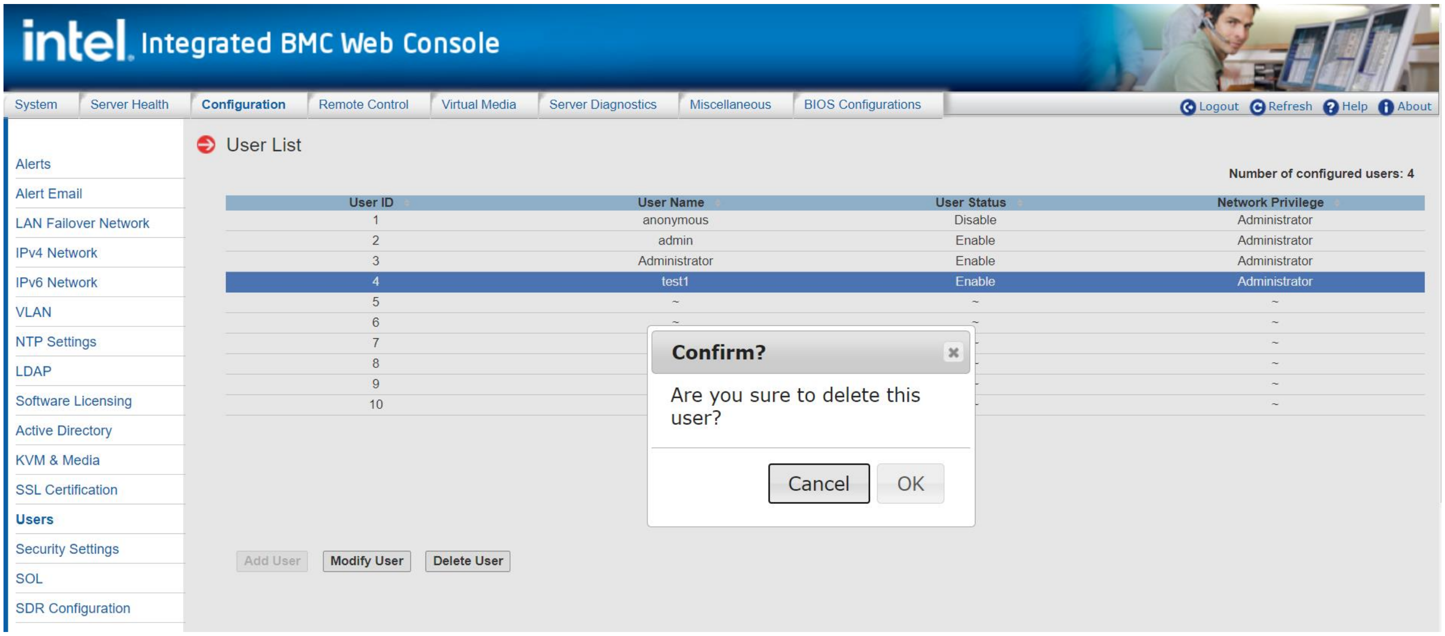


Modify User

User Name:	admin
Logged-In Password:	
Change Password	□
Password:	
Confirm Password:	
Network Privileges:	Administrator
User Enable:	Unchanged

Figure 70. Modify User Page

To delete a user, select the user in the list and click the **Delete User** button (see Figure 71).



User List

Number of configured users: 4

User ID	User Name	User Status	Network Privilege
1	anonymous	Disable	Administrator
2	admin	Enable	Administrator
3	Administrator	Enable	Administrator
4	test1	Enable	Administrator
5	~	~	~
6	~	~	~
7	[illegible]	~	~
8	[illegible]	~	~
9	[illegible]	~	~
10	[illegible]	~	~

Confirm?

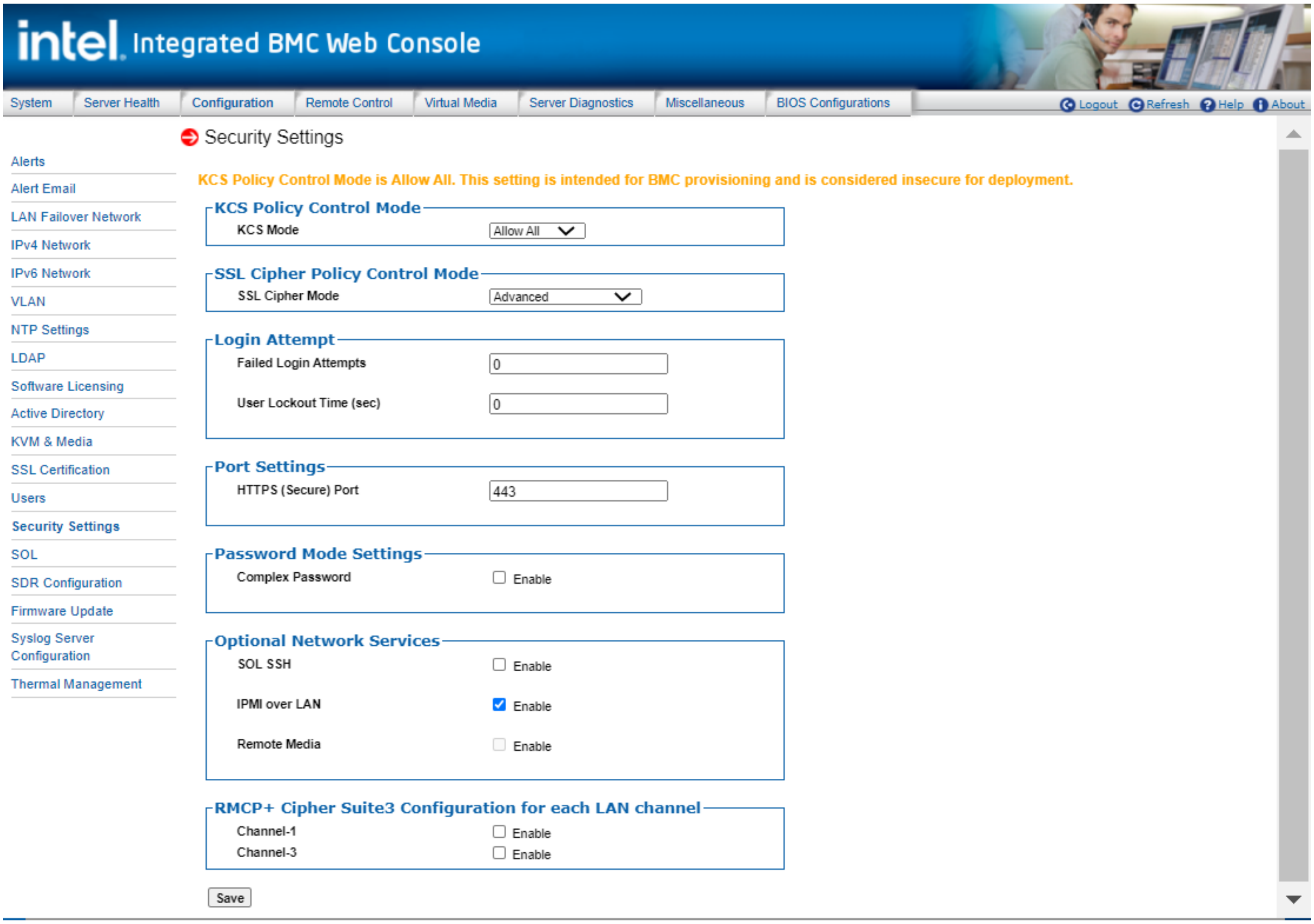
Are you sure to delete this user?

Figure 71. Delete User Page

7.3.14 Security Settings

View and modify the security settings on this page. Configure how many failed login attempts are allowed before a user is locked out, and how long the lock-out must last before the user can attempt to log in again. See Figure 72 for details.

Table 19 lists the options to modify the security settings.



Security Settings

KCS Policy Control Mode is Allow All. This setting is intended for BMC provisioning and is considered insecure for deployment.

KCS Policy Control Mode

KCS Mode	Allow All

SSL Cipher Policy Control Mode

SSL Cipher Mode	Advanced

Login Attempt

Failed Login Attempts	0
User Lockout Time (sec)	0

Port Settings

HTTPS (Secure) Port	443

Password Mode Settings

Complex Password	□ Enable

Optional Network Services

SOL SSH	□ Enable
IPMI over LAN	☑ Enable
Remote Media	□ Enable

RMCP+ Cipher Suite3 Configuration for each LAN channel

Channel-1	□ Enable
Channel-3	□ Enable

Figure 72. Configuration Security Settings Page

Table 19. Configuration Security Settings Options

Option	Task
KCS Mode	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: • **Allow All.** 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. • **Restricted.** This configuration setting disables the IPMI KCS command interfaces between the host operating system and the BMC. This is a non-compliant IPMI configuration that affects 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. • **Deny All.** 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 non-compliant IPMI configuration that may affect 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.
SSL Cipher Mode	Four Cipher modes are provided for different scenarios: • **Advanced:** Wide browser compatibility, such as. to most newer browser versions. • **Board Compatibility:** Check the compatibility to other protocols before using it, like IMAPS. • **Widest Compatibility:** Compatibility to most legacy browsers, legacy libraries (still patched) and other application protocols besides HTTPS, like IMAPS. • **Legacy:** Widest compatibility to old browsers and legacy libraries and other application protocols like SMTP.
Failed Login Attempts	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 must range from 0 to 255. **Default:** three attempts.
User Lockout Time(Sec)	Set the time in seconds that the user is locked out before being allowed to log in again. Zero means User Lockout Time is disabled. If a user was automatically disabled due to the Bad Password threshold, the user remains disabled until re-enablement via the Set User Access command. User Lockout Time must range from 0 to 65535. **Default:** 60 seconds.
HTTPS(Secure) Port	Set the port used for HTTPS (**default:** 443) web sessions. Changing this setting immediately ends all current web sessions.
Complex Password	Checking/Unchecking the check box to enable/disable the complex password service.
SOL SSH	Enable/disable the SOL SSH service.
IPMI Over LAN	Enable/disable the RMCP/RMCP+ service.
Remote Media	Enable/Disable the Virtual Media service.
Channel-1	Enable/Disable Cipher Suite3 Configuration for LAN Channel-1.
Channel-3	Enable/Disable Cipher Suite3 Configuration for LAN Channel-3.
Save	Click to save any changes.

Note: Due to security weaknesses in most of the defined cipher suites, they are disabled by default. Only cipher suites 3 and 17 use algorithms that have not been proven to be cryptographically insecure and are enabled by default.

7.3.14.1 Intel® Integrated BMC Web Console Access Under KCS Restricted/Deny All Mode

Most of the Intel® Integrated BMC Web Console content access is allowed across all KCS modes, except for the pages/options listed below. The following modes are limited to conditional access when KCS mode is set to Restricted Mode/Deny All Mode.

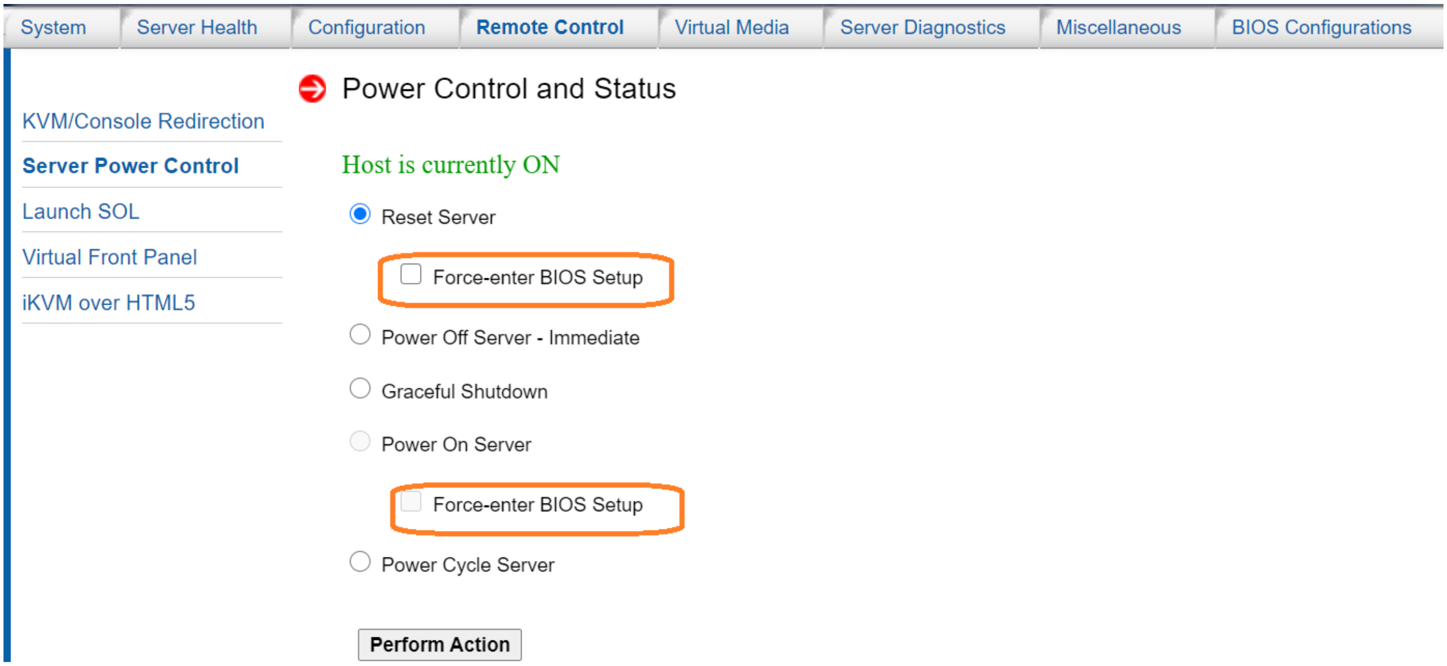
KCS Policy Control Mode – Deny All

This configuration setting disables the IPMI KCS command interfaces between the host operating system and the BMC. This is a non-compliant IPMI configuration that affects 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 – Restricted

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 through the KCS interfaces. This is a non-compliant IPMI configuration that may affect 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 = Deny All`
- Server Power Control Page: Reset Server/**Force-enter BIOS Setup** option is grayed out when:
  - `KCS = Deny All`



Host is currently ON

● Reset Server

□ Force-enter BIOS Setup

○ Power Off Server - Immediate

○ Graceful Shutdown

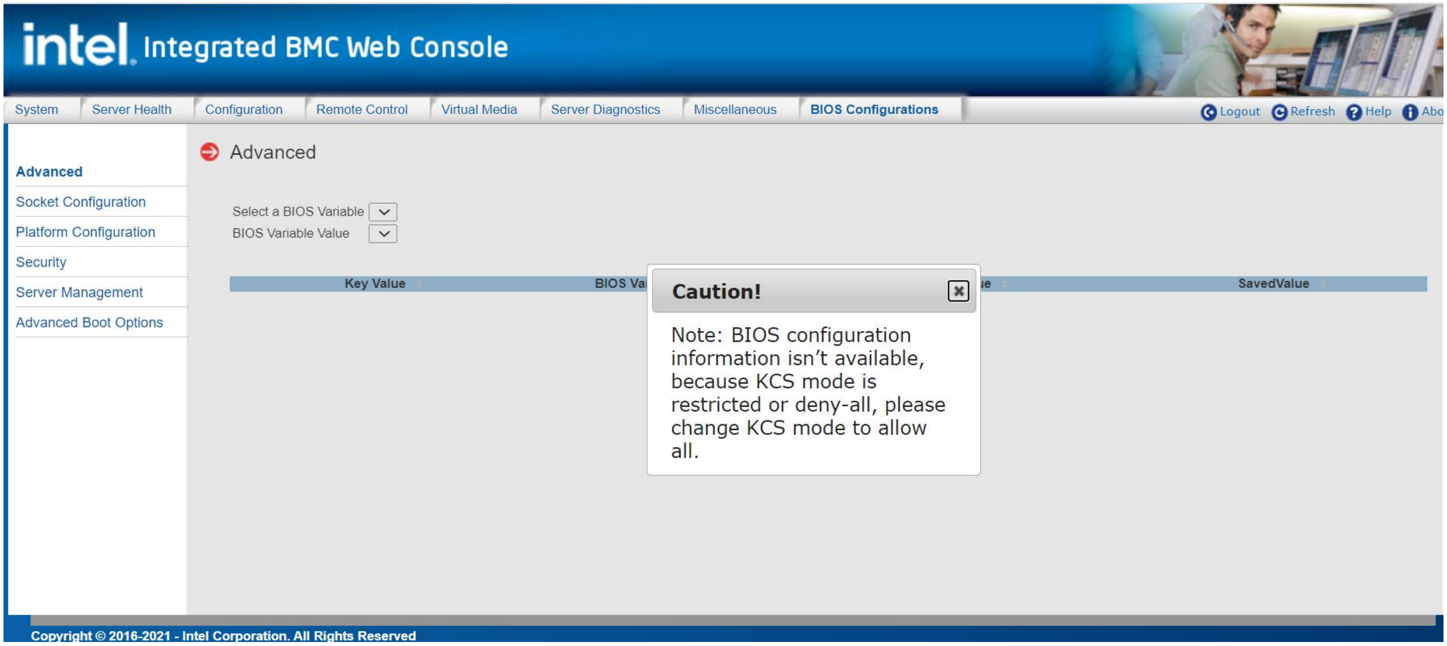
○ Power On Server

□ Force-enter BIOS Setup

○ Power Cycle Server

Figure 73. Server Power Control Page

- BIOS Configuration is unavailable when:
  - o `KCS = Restrict` or `Deny All` mode.

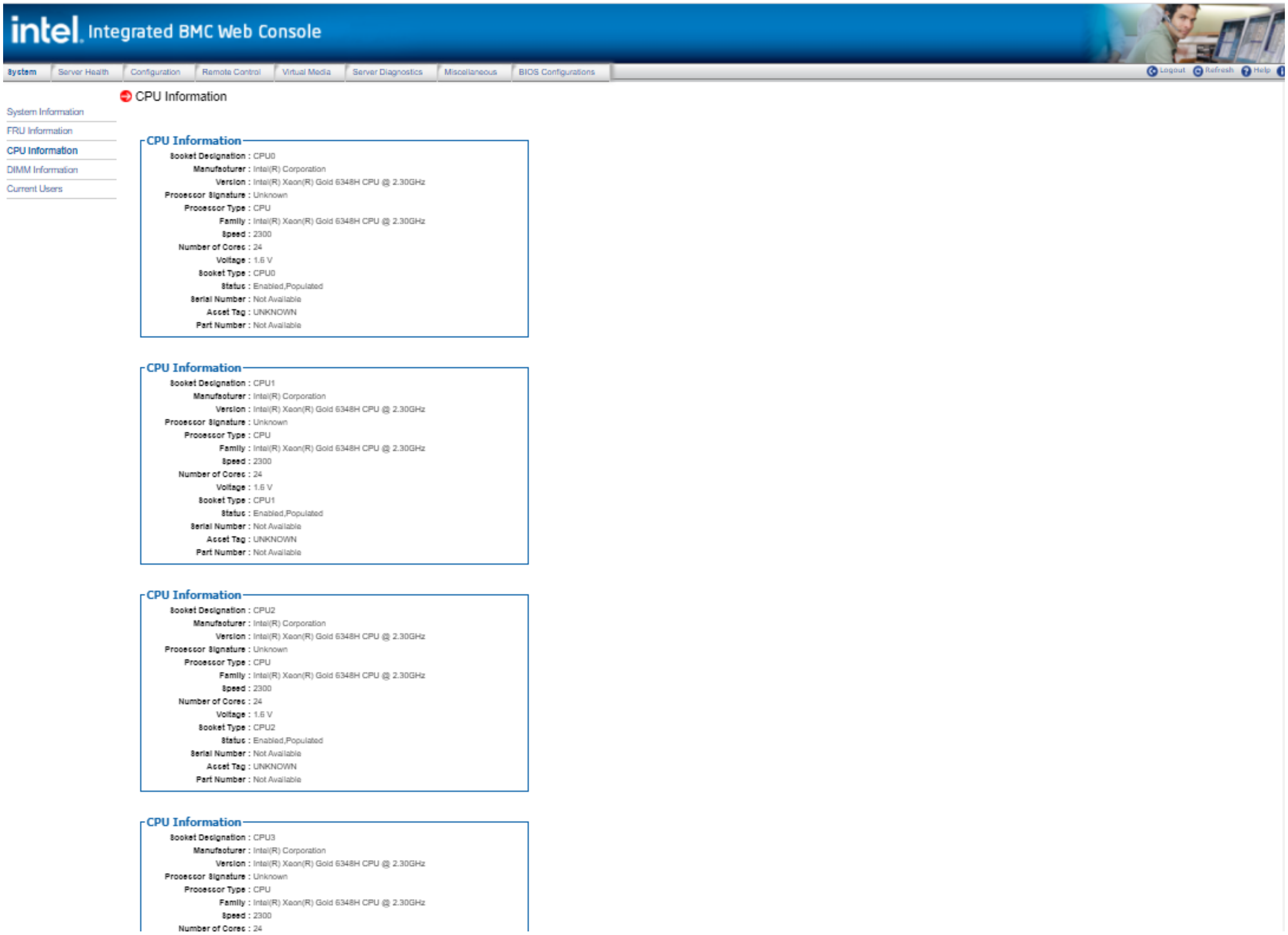


Caution!

Note: BIOS configuration information isn't available, because KCS mode is restricted or deny-all, please change KCS mode to allow all.

Figure 74. BIOS Configuration Page

- CPU Information and DIMM Information pages display contents captured during the last DC when:
  - o `KCS = Restrict` or `Deny All` mode.



CPU Information

CPU Information

Socket Designation : CPU0
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU0
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN
Part Number : Not Available

CPU Information

Socket Designation : CPU1
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU1
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN
Part Number : Not Available

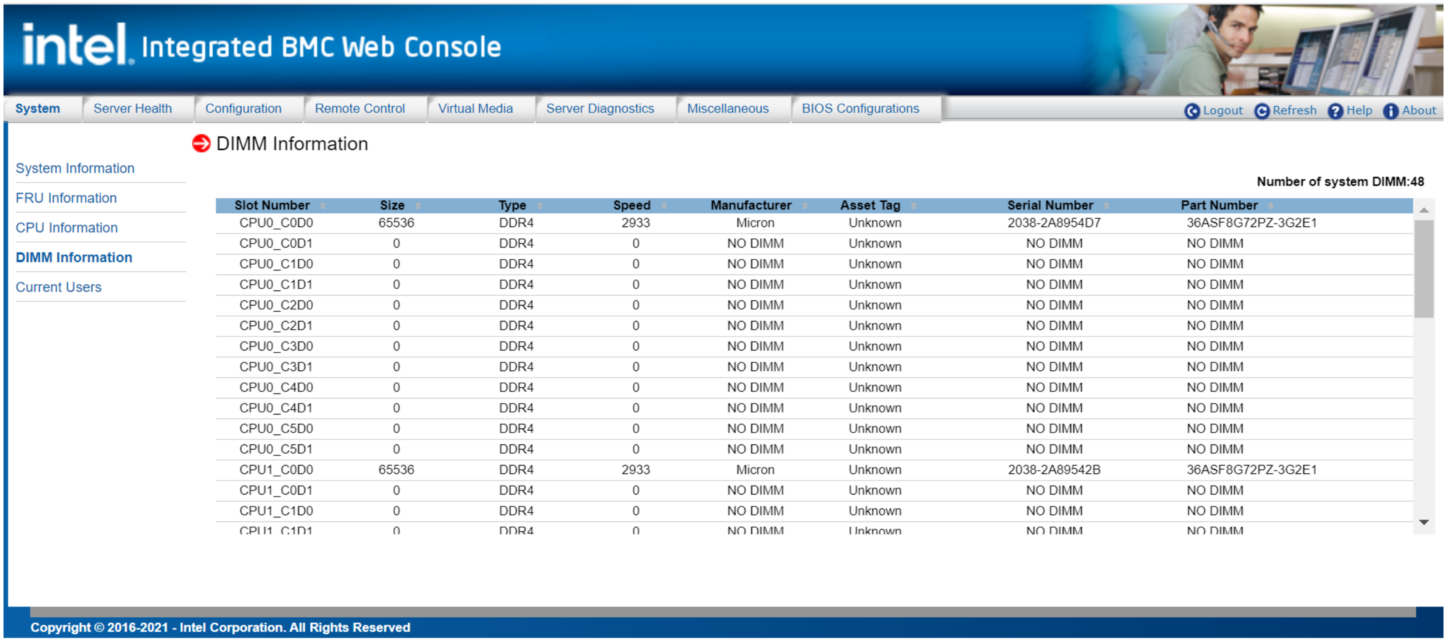
CPU Information

Socket Designation : CPU2
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24
Voltage : 1.6 V
Socket Type : CPU2
Status : Enabled,Populated
Serial Number : Not Available
Asset Tag : UNKNOWN
Part Number : Not Available

CPU Information

Socket Designation : CPU3
Manufacturer : Intel(R) Corporation
Version : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Processor Signature : Unknown
Processor Type : CPU
Family : Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz
Speed : 2300
Number of Cores : 24

Figure 75. CPU Information Page



DIMM Information

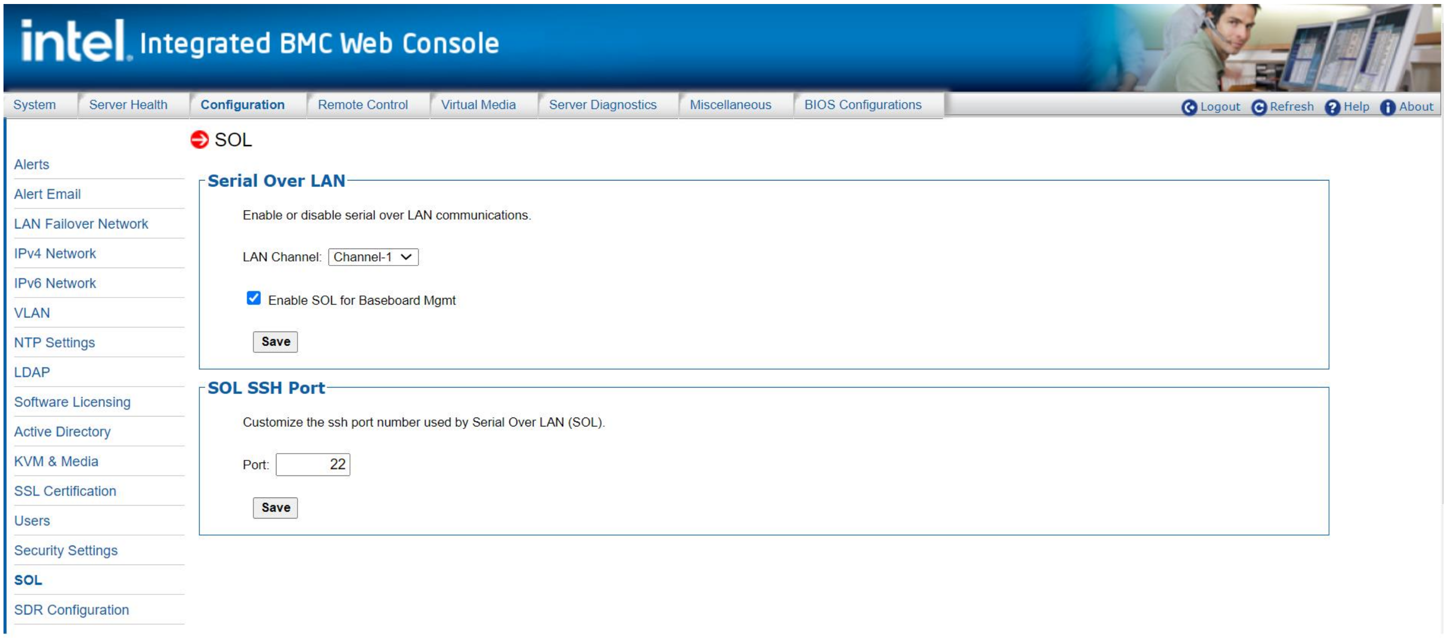
Number of system DIMM:48

Slot Number	Size	Type	Speed	Manufacturer	Asset Tag	Serial Number	Part Number
CPU0_C0D0	65536	DDR4	2933	Micron	Unknown	2038-2A8954D7	36ASF8G72PZ-3G2E1
CPU0_C0D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C1D0	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C1D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C2D0	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C2D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C3D0	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C3D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C4D0	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C4D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C5D0	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU0_C5D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU1_C0D0	65536	DDR4	2933	Micron	Unknown	2038-2A89542B	36ASF8G72PZ-3G2E1
CPU1_C0D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU1_C1D0	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM
CPU1_C1D1	0	DDR4	0	NO DIMM	Unknown	NO DIMM	NO DIMM

Figure 76. DIMM Information Page

7.3.15 SOL

Use the SOL page to enable or disable SOL for each LAN channel (see Figure 77). Table 20 lists the options to modify SOL settings.



SOL

Serial Over LAN

Enable or disable serial over LAN communications.

LAN Channel: Channel-1

☑ Enable SOL for Baseboard Mgmt

SOL SSH Port

Customize the ssh port number used by Serial Over LAN (SOL).

Port: 22

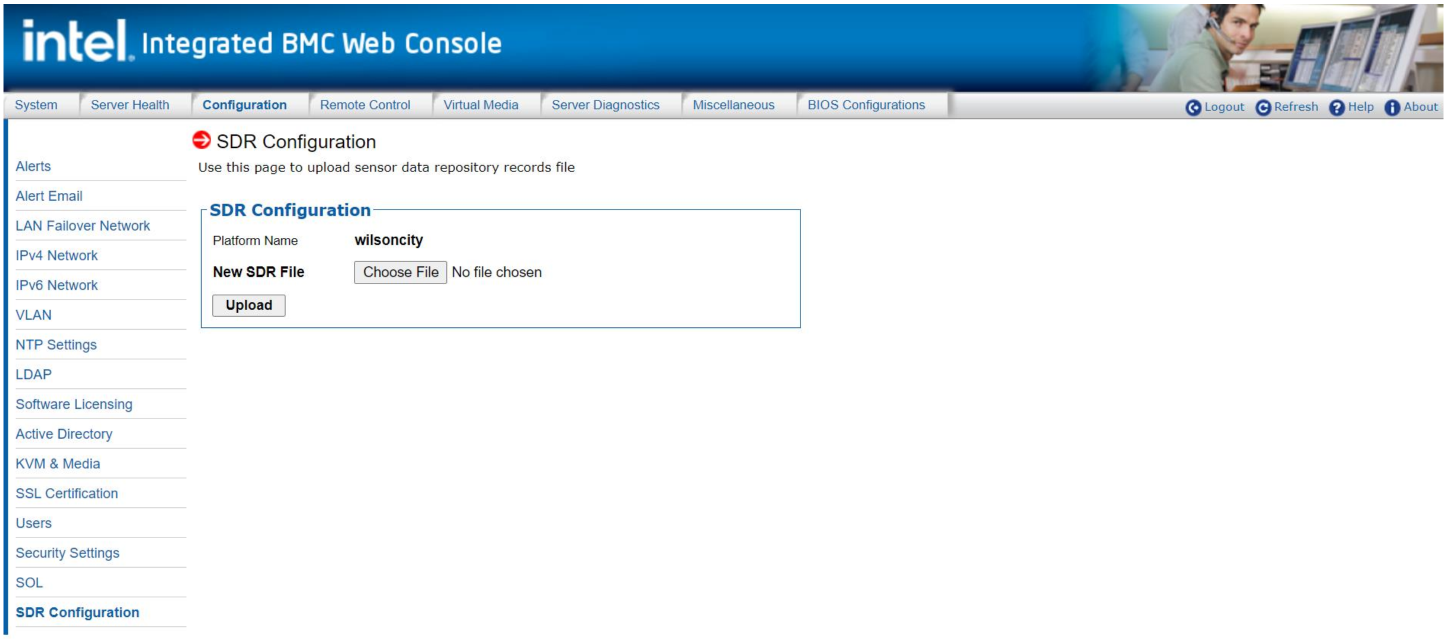
Figure 77. SOL Page

Table 20. SOL Options

Option	Task
LAN Channel	Select the desired channel to configure the network settings. Lists the LAN Channels available for SOL. The LAN channel describes the physical NIC connection on the server. • **Baseboard Mgmt** (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system. • **Baseboard Mgmt 2** (BMC LAN Channel 2) is the second onboard, shared NIC configured for management and shared with the operating system.
Enable SOL for Baseboard Mgmt	Enable or disable SOL for BMC.
Save (Serial Over LAN)	Click to save any changes for SOL Setting.
Port	Change the SSH port number used by SOL.
Save (SOL SSH Port)	Click to save any changes for SOL SSH Port Setting.

7.3.16 SDR Configuration

Use this page to upload sensor data repository records files. See Figure 78 and Table 21 for details.



SDR Configuration

Use this page to upload sensor data repository records file

SDR Configuration

Platform Name wilsoncity

New SDR File [Choose File] No file chosen

[Upload]

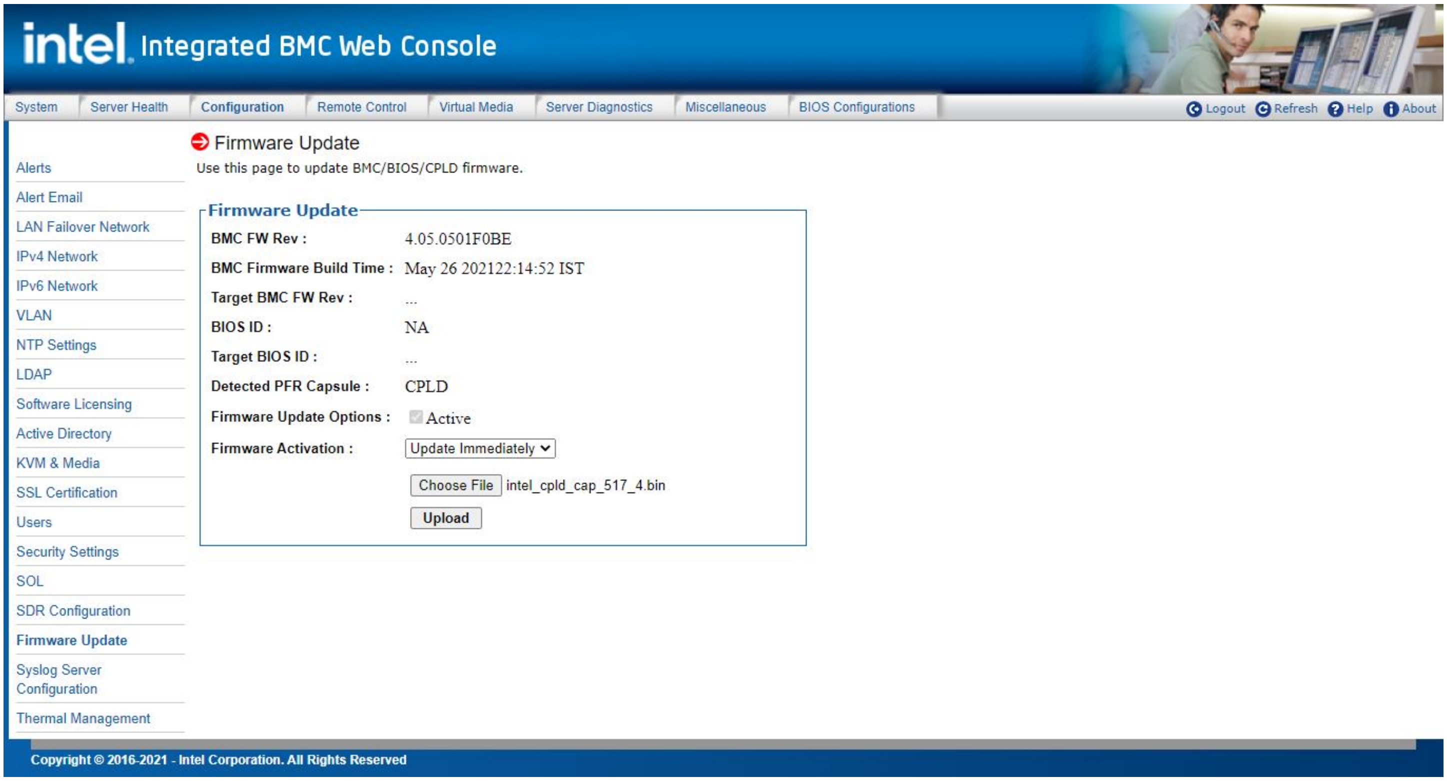
Figure 78. SDR Configuration Page

Table 21. SDR Configuration Options

Option	Task
New SDR File	Specify new SDR file to upload.
Upload	Choose a new sensor data record file and configuration file and click **Upload**. Uploading large files may take some time, depending on the user's network connection speed.

7.3.17 Firmware Update

Use the Firmware Update page to upload new images for online-update of BMC/BIOS firmware (see Figure 79). Table 22 lists the options available in the CPLD Firmware Update page.



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

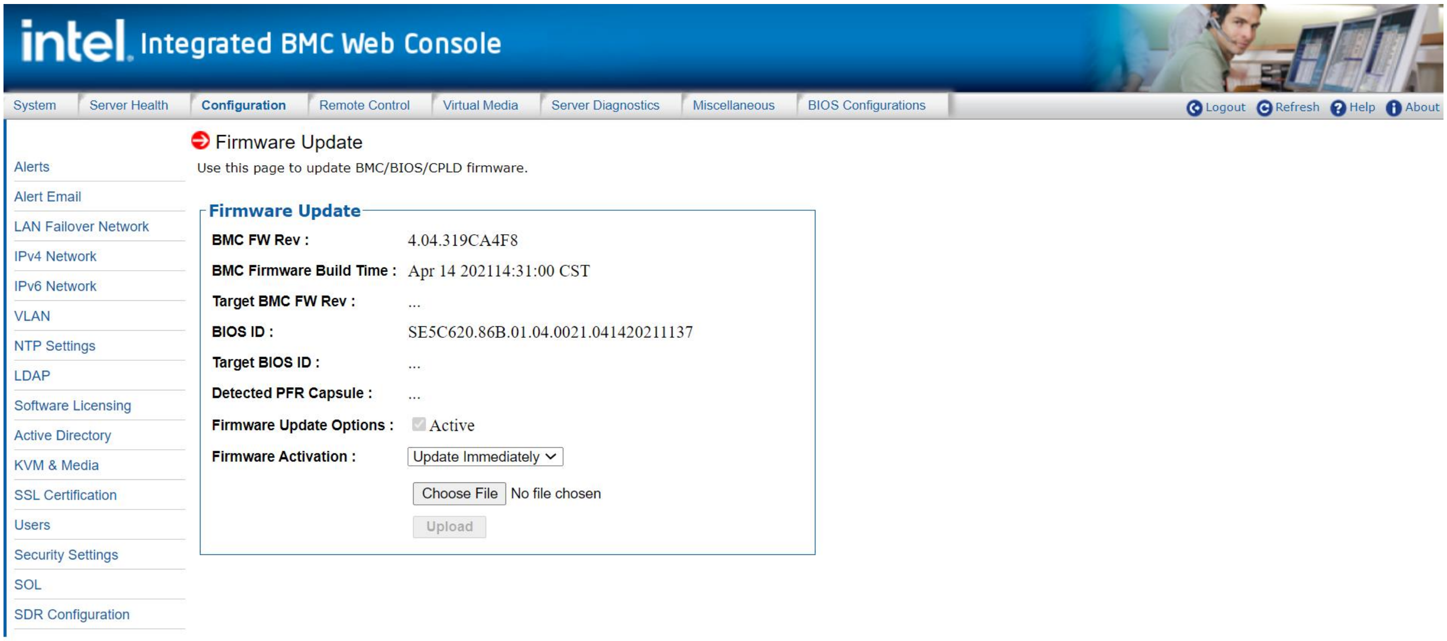
Firmware Update

BMC FW Rev :	4.05.0501F0BE
BMC Firmware Build Time :	May 26 202122:14:52 IST
Target BMC FW Rev :	...
BIOS ID :	NA
Target BIOS ID :	...
Detected PFR Capsule :	CPLD
Firmware Update Options :	☑ Active
Firmware Activation :	Update Immediately
	Choose File intel_cpld_cap_517_4.bin

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 87.CPLD Firmware Update Page

Table 22



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

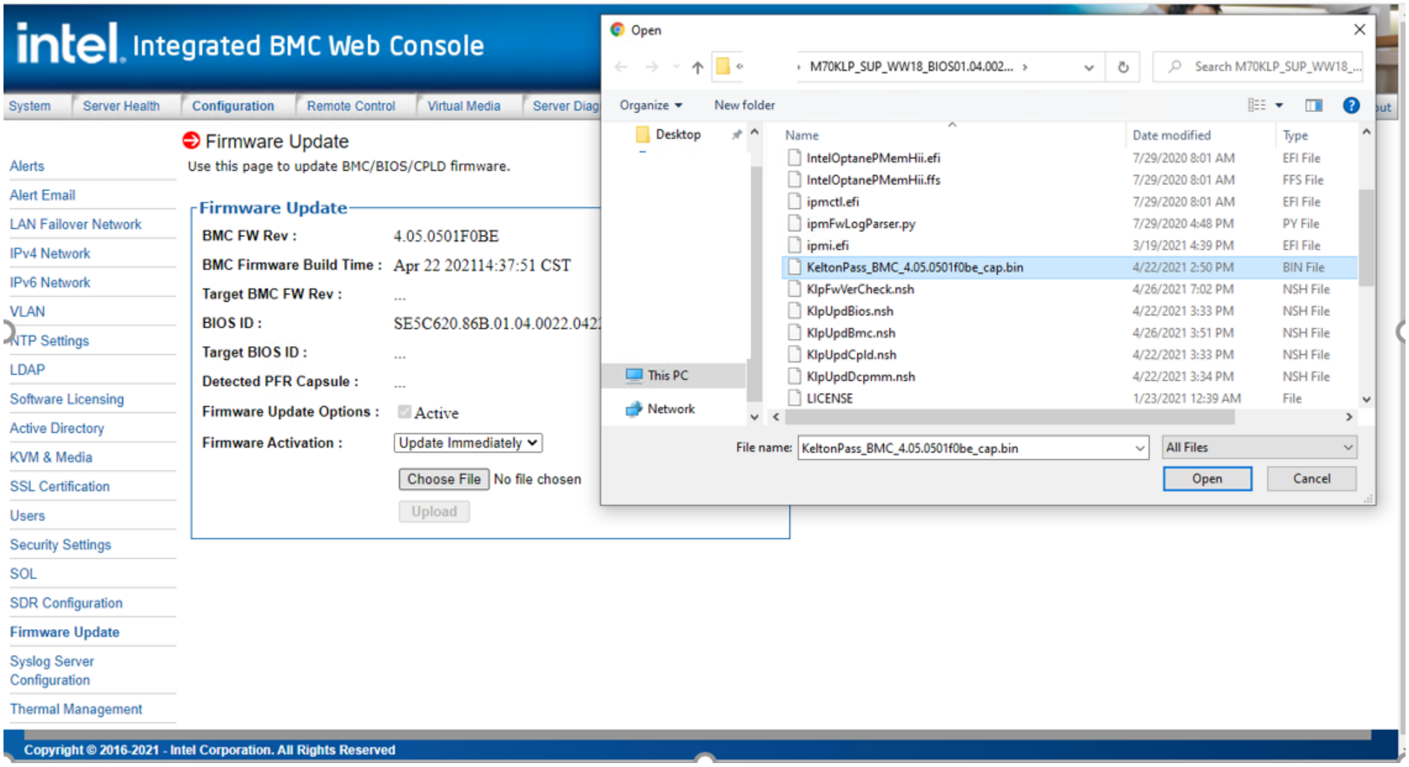
Firmware Update

BMC FW Rev :	4.04.319CA4F8
BMC Firmware Build Time :	Apr 14 202114:31:00 CST
Target BMC FW Rev :	...
BIOS ID :	SE5C620.86B.01.04.0021.041420211137
Target BIOS ID :	...
Detected PFR Capsule :	...
Firmware Update Options :	☑ Active
Firmware Activation :	Update Immediately
	Choose File No file chosen

Figure 79. BMC Firmware Update Page

7.3.17.1 BMC Firmware Online Update

1. Click the **Choose File** button to select the target BMC firmware.



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE

BMC Firmware Build Time : Apr 22 202114:37:51 CST

Target BMC FW Rev : ...

BIOS ID : SE5C620.86B.01.04.0022.042

Target BIOS ID : ...

Detected PFR Capsule : ...

Firmware Update Options : ☑ Active

Firmware Activation : Update Immediately

Choose File No file chosen

Name	Date modified	Type
IntelOptanePMemHii.efi	7/29/2020 8:01 AM	EFI File
IntelOptanePMemHii.ffs	7/29/2020 8:01 AM	FFS File
ipmctl.efi	7/29/2020 8:01 AM	EFI File
ipmFwLogParser.py	7/29/2020 4:48 PM	PY File
ipmi.efi	3/19/2021 4:39 PM	EFI File
KeltonPass_BMC_4.05.0501f0be_cap.bin	4/22/2021 2:50 PM	BIN File
KlpFwVerCheck.nsh	4/26/2021 7:02 PM	NSH File
KlpUpdBios.nsh	4/22/2021 3:33 PM	NSH File
KlpUpdBmc.nsh	4/26/2021 3:51 PM	NSH File
KlpUpdCpld.nsh	4/22/2021 3:33 PM	NSH File
KlpUpdDcpmm.nsh	4/22/2021 3:34 PM	NSH File
LICENSE	1/23/2021 12:39 AM	File

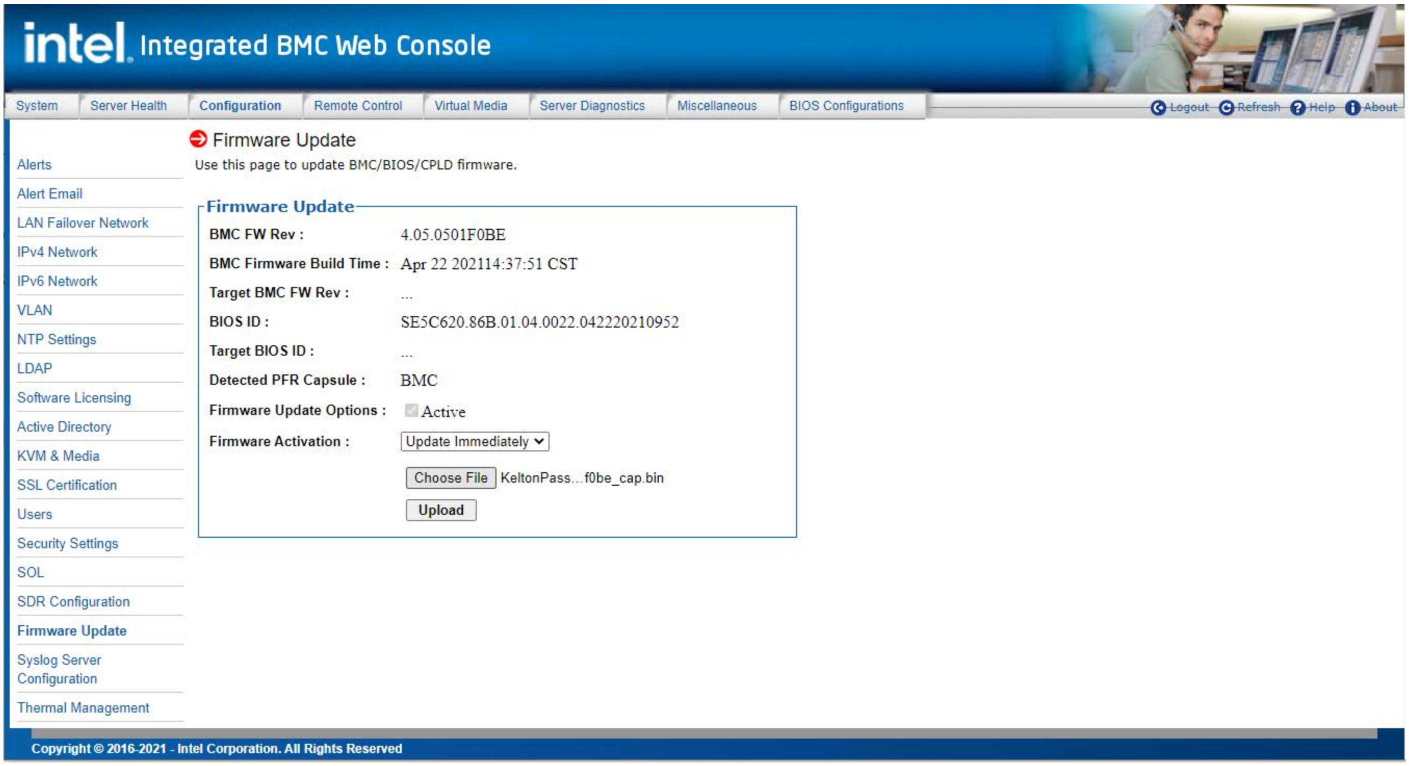
File name: KeltonPass_BMC_4.05.0501f0be_cap.bin

All Files

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 80. Select Target Firmware

2. Click **Upload** to start the firmware uploading.



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE

BMC Firmware Build Time : Apr 22 202114:37:51 CST

Target BMC FW Rev : ...

BIOS ID : SE5C620.86B.01.04.0022.042220210952

Target BIOS ID : ...

Detected PFR Capsule : BMC

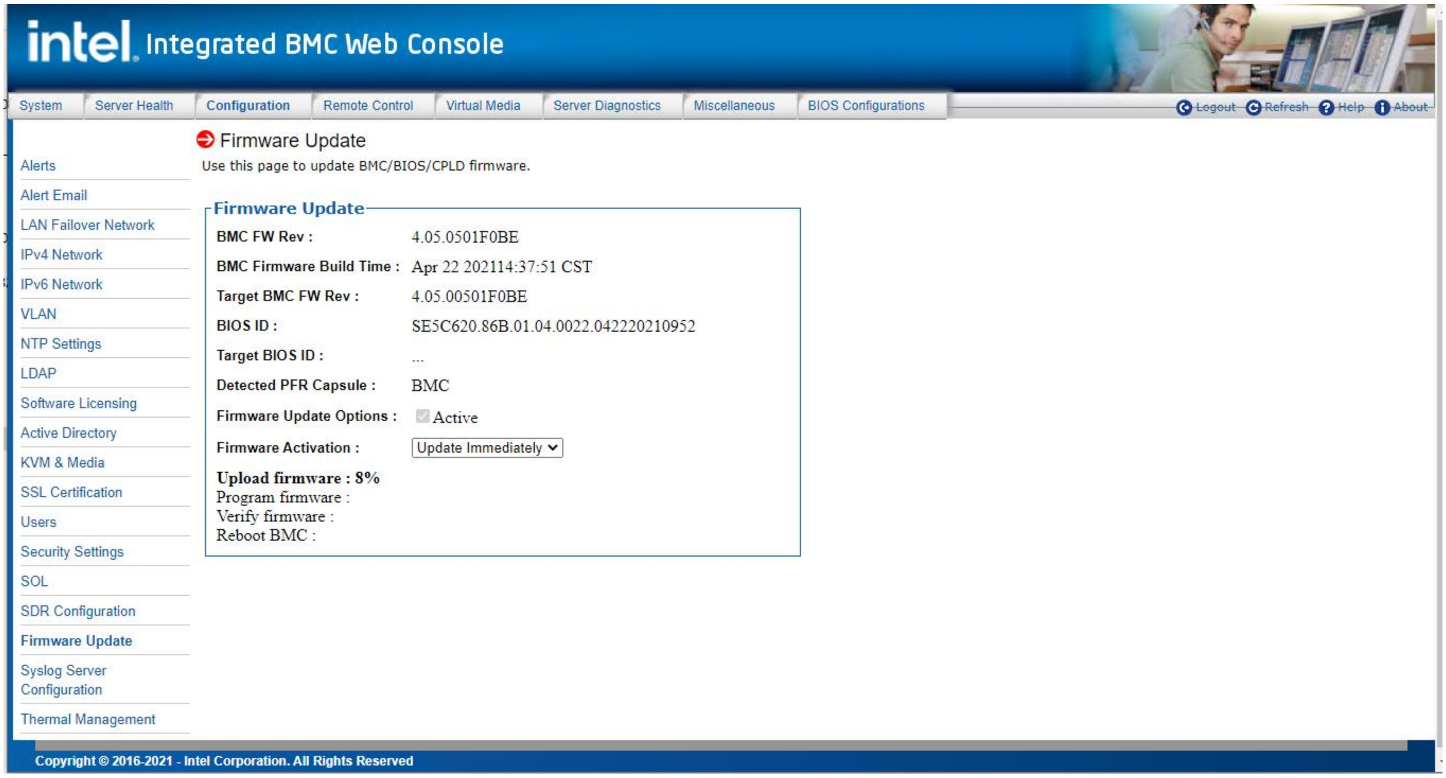
Firmware Update Options : ☑ Active

Firmware Activation : Update Immediately

Choose File KeltonPass...f0be_cap.bin

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 81. BMC Firmware Update Page



Firmware Update

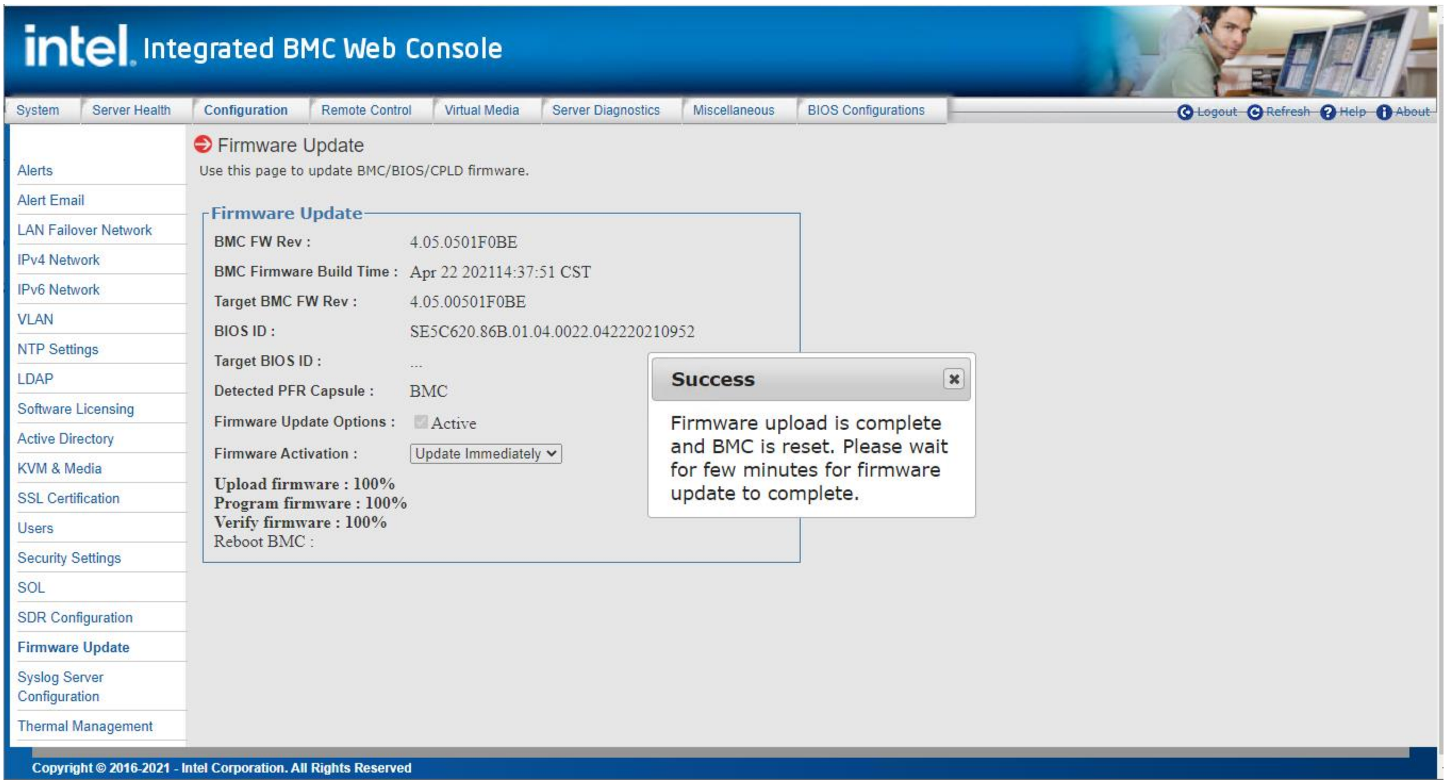
Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE
BMC Firmware Build Time : Apr 22 202114:37:51 CST
Target BMC FW Rev : 4.05.00501F0BE
BIOS ID : SE5C620.86B.01.04.0022.042220210952
Target BIOS ID : ...
Detected PFR Capsule : BMC
Firmware Update Options : ☑ Active
Firmware Activation : Update Immediately

Upload firmware : 8%
Program firmware :
Verify firmware :
Reboot BMC :

Figure 82. BMC Firmware Update in Progress



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE
BMC Firmware Build Time : Apr 22 202114:37:51 CST
Target BMC FW Rev : 4.05.00501F0BE
BIOS ID : SE5C620.86B.01.04.0022.042220210952
Target BIOS ID : ...
Detected PFR Capsule : BMC
Firmware Update Options : ☑ Active
Firmware Activation : Update Immediately

Upload firmware : 100%
Program firmware : 100%
Verify firmware : 100%
Reboot BMC :

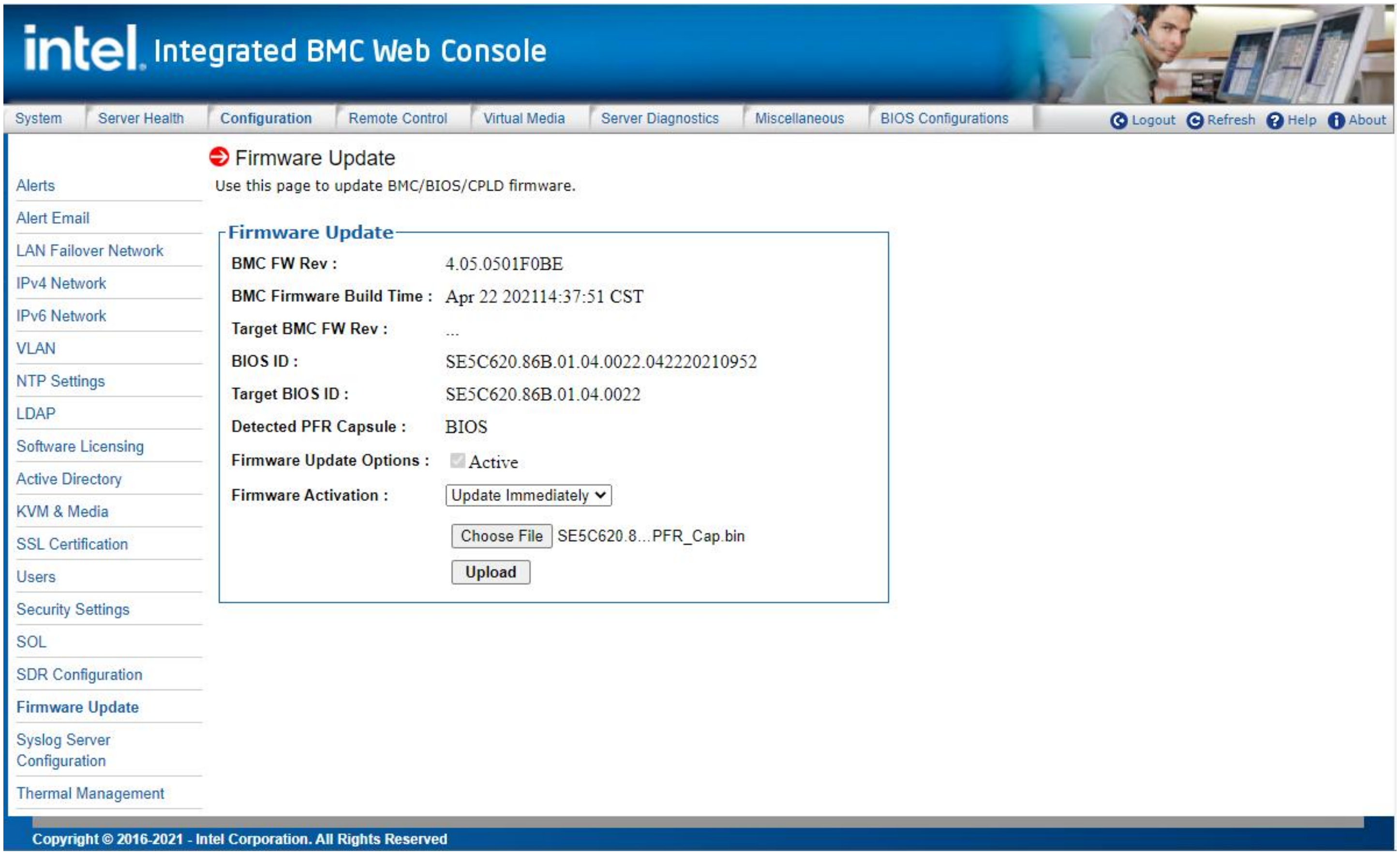
Success

Firmware upload is complete and BMC is reset. Please wait for few minutes for firmware update to complete.

Figure 83. BMC Firmware Update Completed

7.3.17.2 BIOS Firmware Online Update

1. Select **Target BIOS Firmware** and then click **Upload** to start the firmware uploading.



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE

BMC Firmware Build Time : Apr 22 202114:37:51 CST

Target BMC FW Rev : ...

BIOS ID : SE5C620.86B.01.04.0022.042220210952

Target BIOS ID : SE5C620.86B.01.04.0022

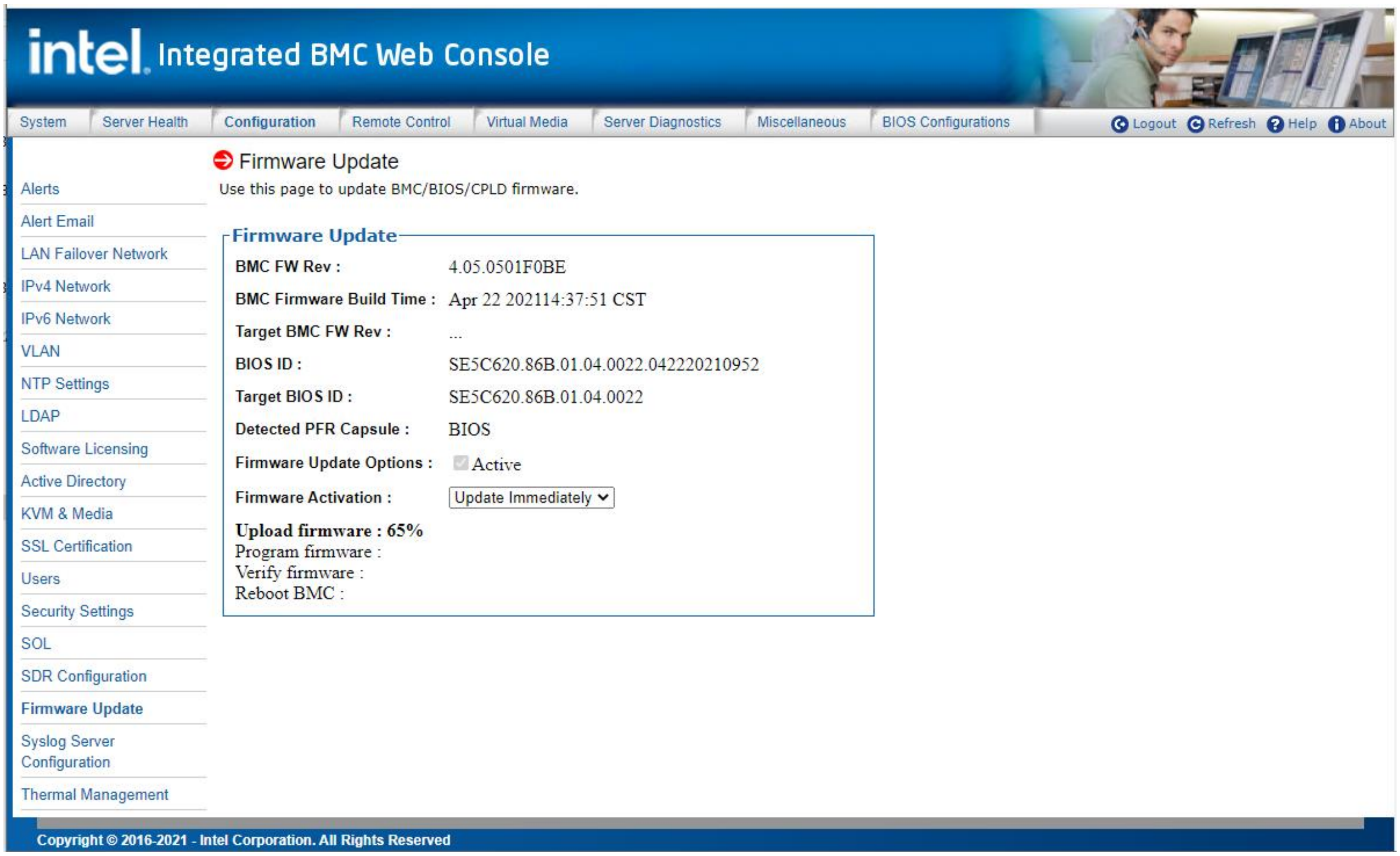
Detected PFR Capsule : BIOS

Firmware Update Options : ☑ Active

Firmware Activation : Update Immediately

SE5C620.8...PFR_Cap.bin

Figure 84. BIOS Update Page



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE

BMC Firmware Build Time : Apr 22 202114:37:51 CST

Target BMC FW Rev : ...

BIOS ID : SE5C620.86B.01.04.0022.042220210952

Target BIOS ID : SE5C620.86B.01.04.0022

Detected PFR Capsule : BIOS

Firmware Update Options : ☑ Active

Firmware Activation : Update Immediately

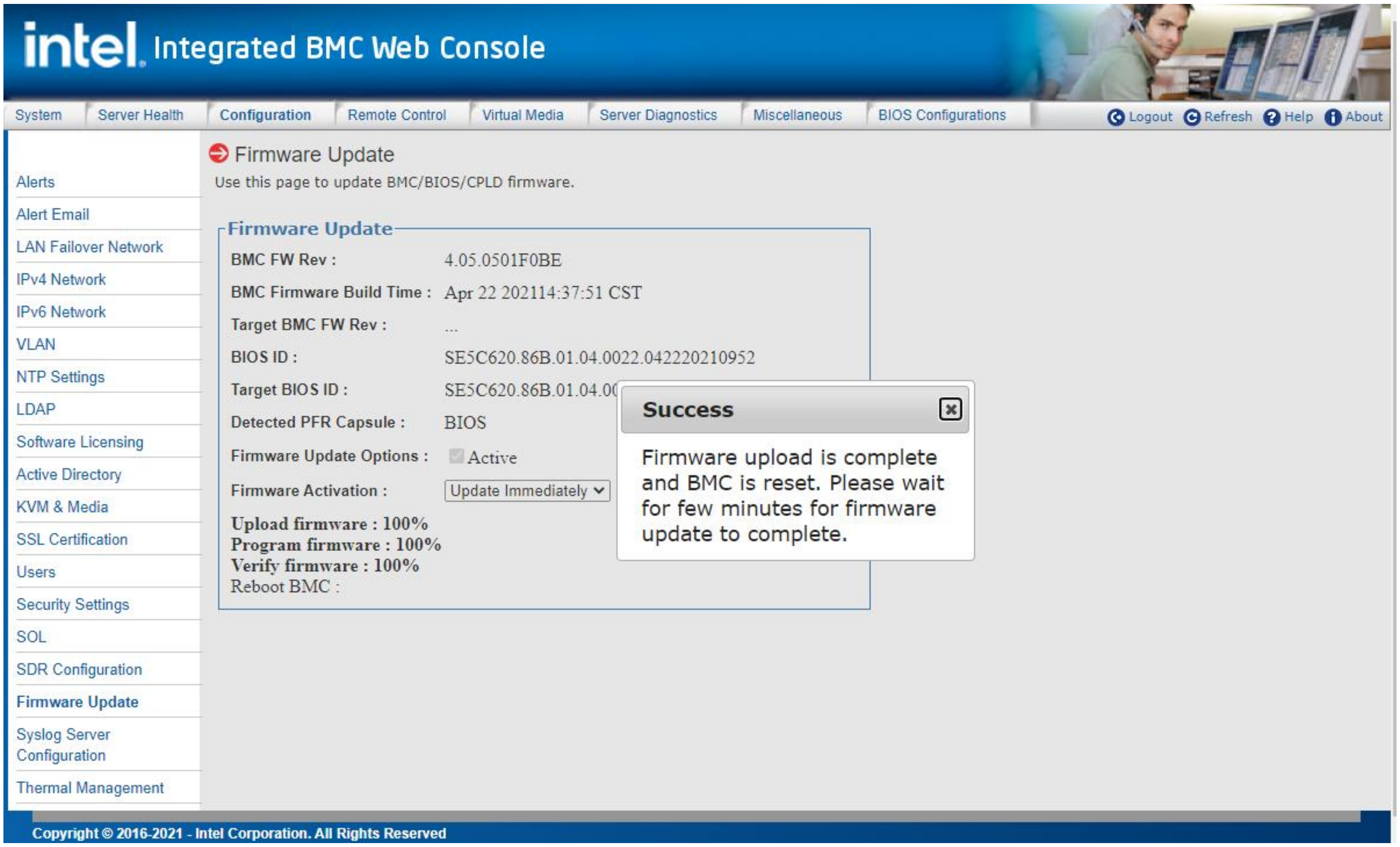
Upload firmware : 65%

Program firmware :

Verify firmware :

Reboot BMC :

Figure 85. BIOS Firmware Update in Progress



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE

BMC Firmware Build Time : Apr 22 202114:37:51 CST

Target BMC FW Rev : ...

BIOS ID : SE5C620.86B.01.04.0022.042220210952

Target BIOS ID : SE5C620.86B.01.04.0(

Detected PFR Capsule : BIOS

Firmware Update Options : ☑ Active

Firmware Activation : Update Immediately

Upload firmware : 100%

Program firmware : 100%

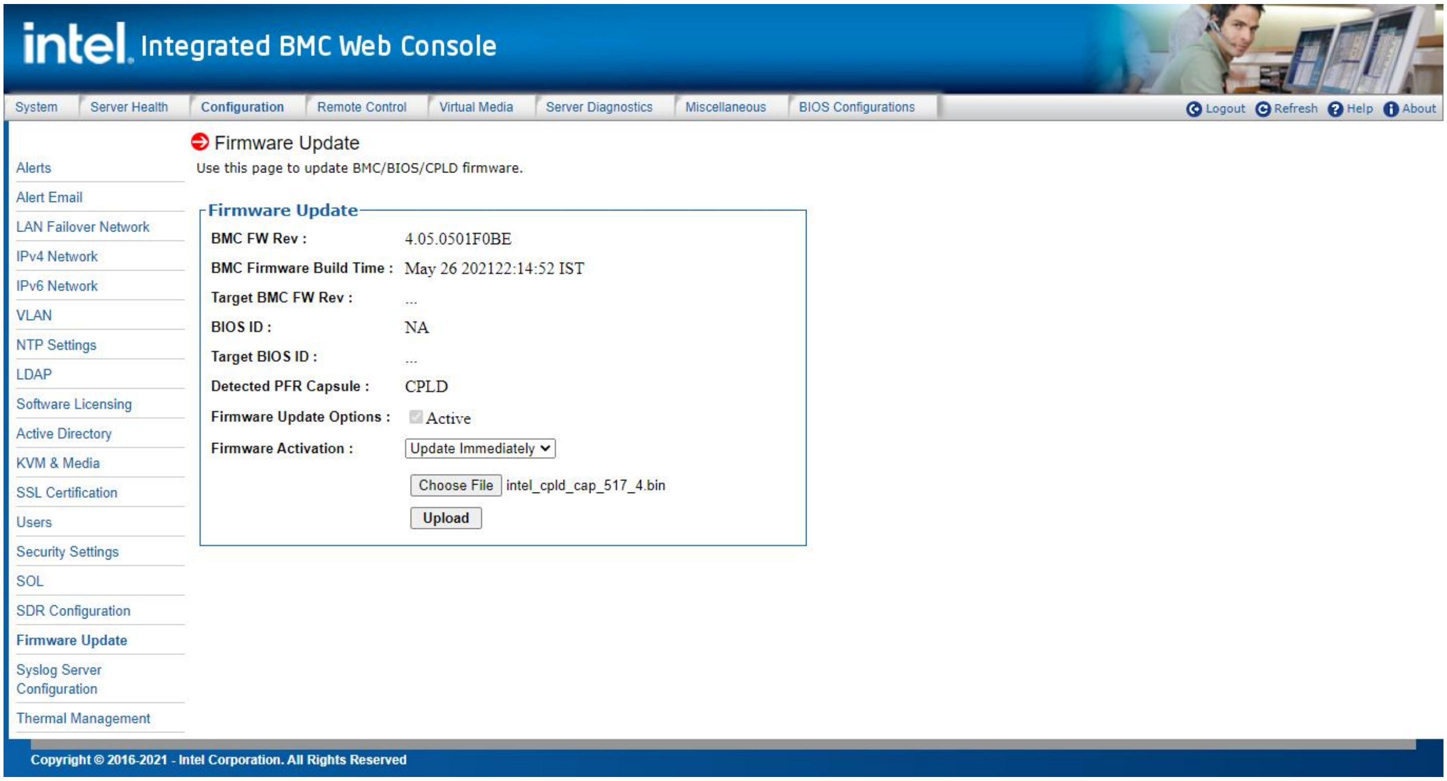
Verify firmware : 100%

Reboot BMC :

Success ☒

Firmware upload is complete and BMC is reset. Please wait for few minutes for firmware update to complete.

Figure 86. BIOS Firmware Update Completed



Firmware Update

Use this page to update BMC/BIOS/CPLD firmware.

Firmware Update

BMC FW Rev : 4.05.0501F0BE

BMC Firmware Build Time : May 26 202122:14:52 IST

Target BMC FW Rev : ...

BIOS ID : NA

Target BIOS ID : ...

Detected PFR Capsule : CPLD

Firmware Update Options : ☑ Active

Firmware Activation : Update Immediately

intel_cpld_cap_517_4.bin

Figure 87.CPLD Firmware Update Page

Table 22. BMC Firmware Update Options

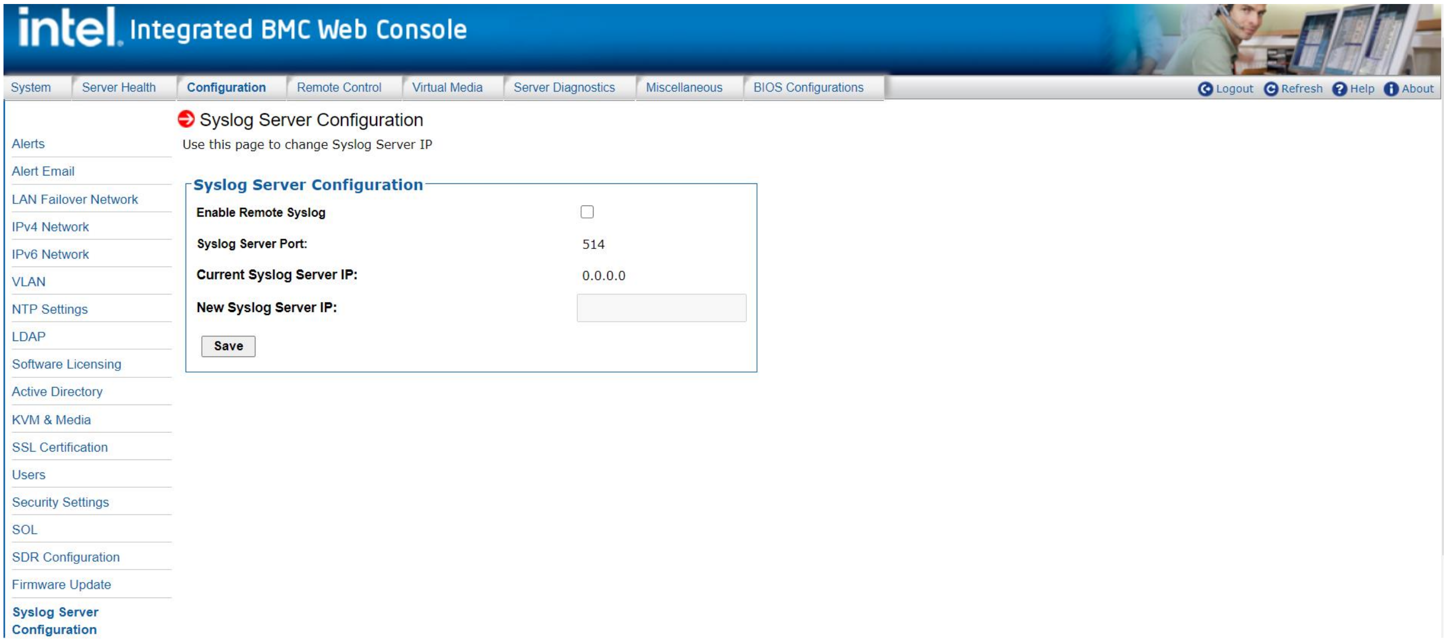
Option	Task
BMC FW Rev	Displays the current firmware version.
BMC Firmware Build Time	Displays the firmware build time.
Target BMC FW Rev	Displays the uploaded BMC firmware version.
BIOS ID	Displays the BIOS ID. `BoardFamilyID.OEMID.MajorVer.MinorVer.RelNum.BuildDateTime` **Note:** Only available if the host is powered on.
Target BIOS ID	Displays the uploaded BIOS ID.
Detected PFR Capsule	Indicates the system to be flashed, and it is detected from the uploaded firmware image file.
Firmware Update Options	**Active:** Active region where the current device is working on.
Firmware Activation	Select the choice to do the action after the post flash. • **Update Immediately.** This halts the BMC on post flash and tries to update the firmware. • **Update at Reset.** This provides the option to flash the device once the device is set to reboot.
Choose File	Choose the file to upload.
Upload	Upload the firmware updates the image file to the BMC for update action.

7.3.18 Syslog Server Configuration

Use the Syslog Server Configuration page to enable the Remote Syslog service or to configure the Syslog Server IP. This page allows the logging of any login to the BMC, or any configurations to be logged to the Syslog Server. See Table 23 for all options available on this page.

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 by `Modload imudp/UDPServeRun 514/ModLoad imtcp/InputTCPServerRun 514`
3. Service syslog restart.
4. Set Syslog Server from **Intel® Integrated BMC Web Console** > **Configuration** > **Syslog Server Configuration**
5. To see the log: `cat/var/log/messages`



Syslog Server Configuration

Use this page to change Syslog Server IP

Syslog Server Configuration

Enable Remote Syslog	□
Syslog Server Port:	514
Current Syslog Server IP:	0.0.0.0
New Syslog Server IP:	

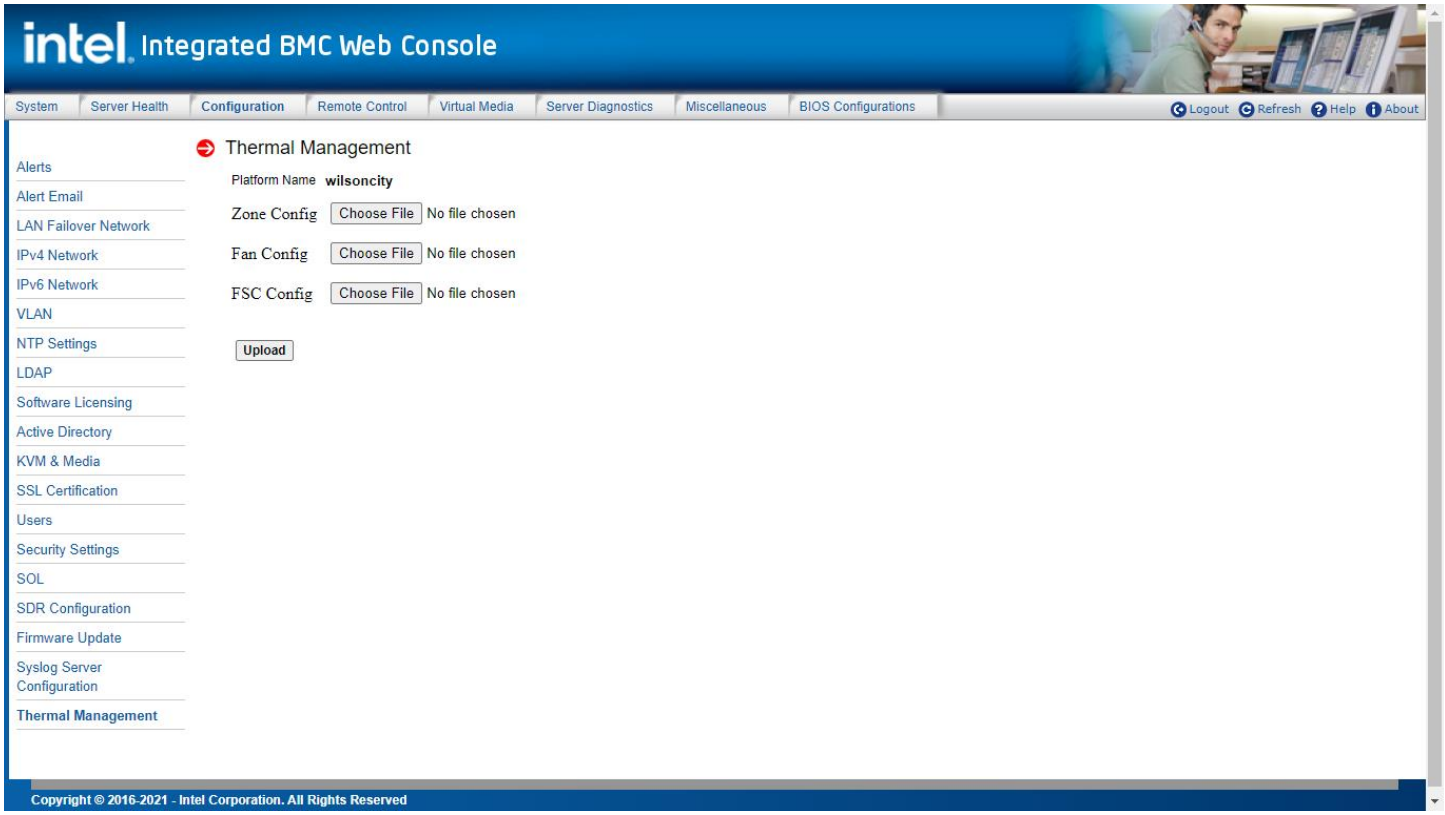
Figure 88. Syslog Server Configuration Page

Table 23. Syslog Server Configuration Options

Option	Task
Enable Remote Syslog	To enable/disable the Remote Syslog, check or uncheck the **Enable Remote Syslog**.
Syslog Server Port	The port number of the remote Syslog Server is 514.
Current Syslog Server IP	Display the Syslog Server current IP address.
New Syslog Server IP	Input the Syslog Server new IP address.
Save button	Save the current settings.

7.3.19 Thermal Management

Use this page to upload thermal configurations of Zone, Fan and FSC. See Figure 78 and Table 21 for details.



Thermal Management

Platform Name wilsoncity

Zone Config [Choose File] No file chosen

Fan Config [Choose File] No file chosen

FSC Config [Choose File] No file chosen

Figure 89. Thermal Configuration Options Page

Table 24. Thermal Configuration Options

Option	Task
Zone Config	Specify the zone configuration file with `ini file extension (.ini format)` to upload.
Fan Config	Specify the fan configuration file with `ini file extension (.ini format)` to upload.
FSC Config	Specify the FSC configuration file with `ini file extension (.ini format)` to upload.
Upload	Choose **Zone**, **Fan** and **FSC** configuration files and click **Upload** for Thermal Configurations.

7.4 Remote Control Tab

The **Remote Control** tab makes it possible to launch the remote console KVM redirection window, initialize power control, launch SOL, and access the virtual front panel.

7.4.1 KVM/Console Redirection

Use this page to launch the remote console KVM redirection window. This requires an Intel® Remote Management Module (Intel® RMM) add-in card to be installed in the remote system; otherwise, the launch button is grayed-out. Clicking **Launch Console** prompts to download a `jviewer.jnlp` file. When the file is downloaded and launched, the Java* redirection window is displayed. Figure 90 shows the details.

Note: Java Runtime Environment* (JRE* Version 6 Update 10 or higher) must be installed on client before launching the JNLP file.

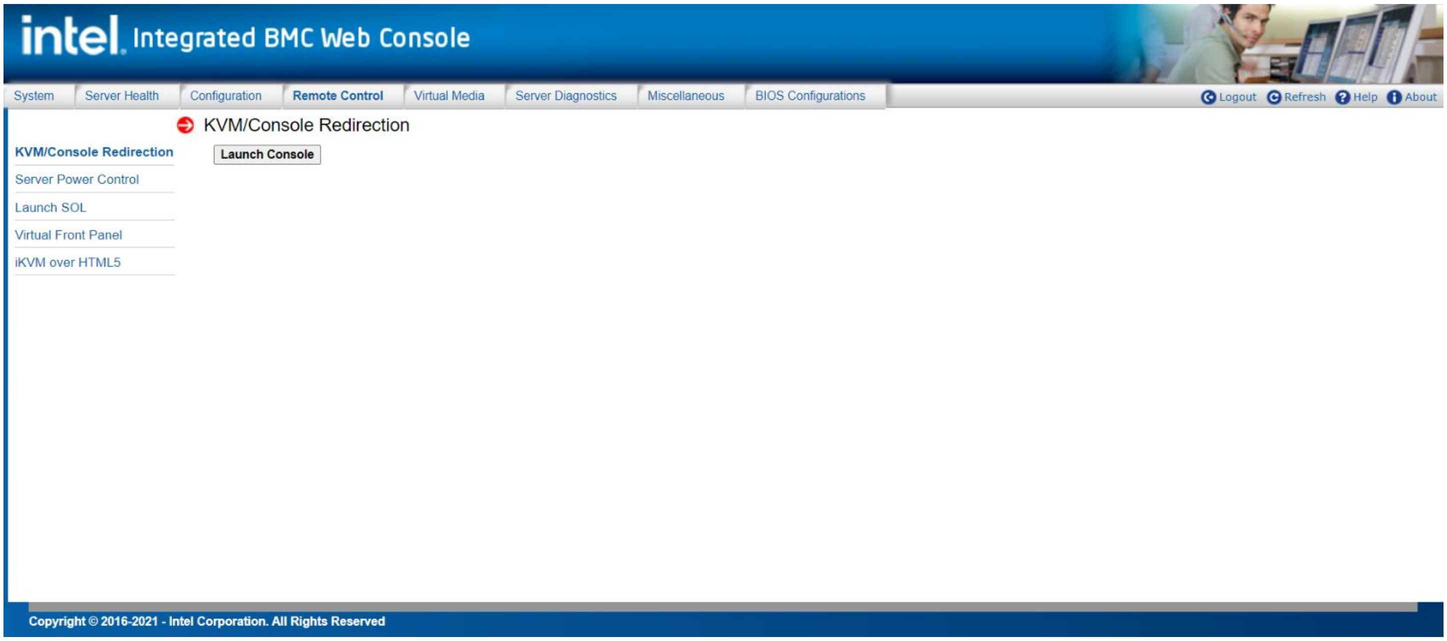
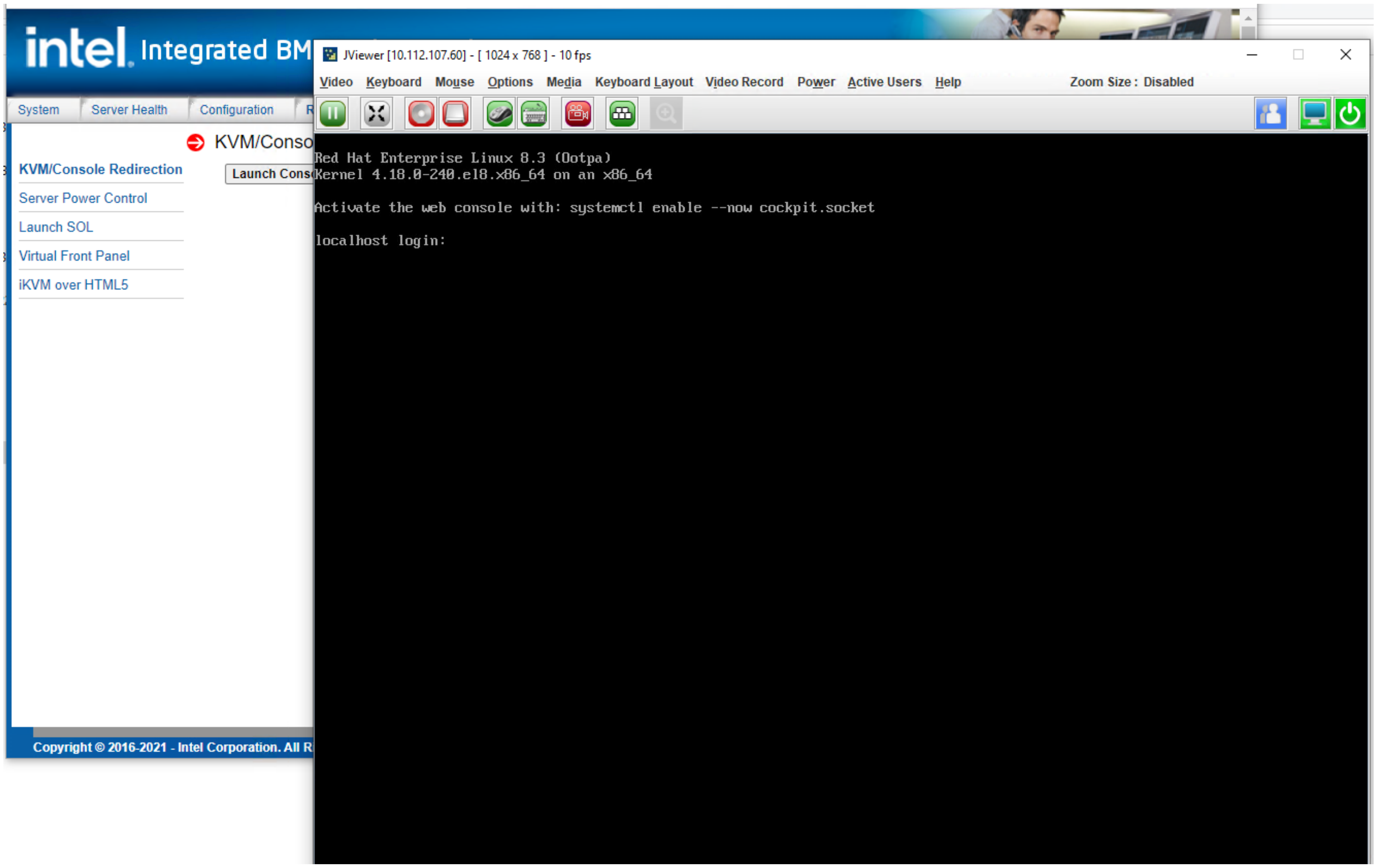


Figure 90. Remote Control KVM Page

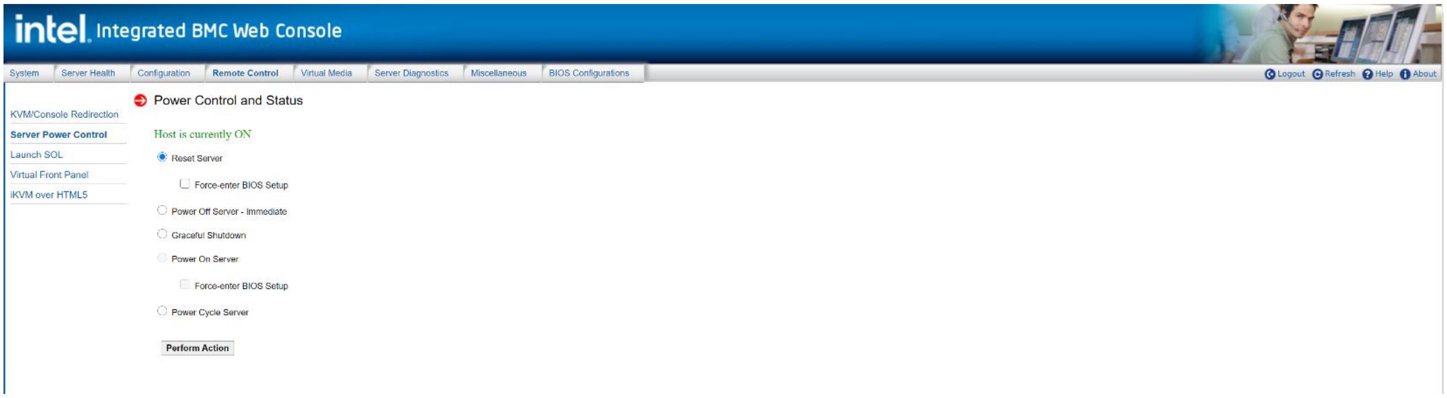


```
Red Hat Enterprise Linux 8.3 (Ootpa)
Kernel 4.18.0-240.el8.x86_64 on an x86_64

Activate the web console with: systemctl enable --now cockpit.socket

localhost login:
```

Figure 91. KVM Console Window

7.4.2 Server Power Control

The Server Power Control page shows the power status and makes it possible to control the server power/reset, as shown on Figure 92. Table 25 lists the power control operations that can be performed.



Power Control and Status

Host is currently ON

● Reset Server

□ Force-enter BIOS Setup

○ Power Off Server - Immediate

○ Graceful Shutdown

○ Power On Server

□ Force-enter BIOS Setup

○ Power Cycle Server

Figure 92. Remote Control Server Power Control Page

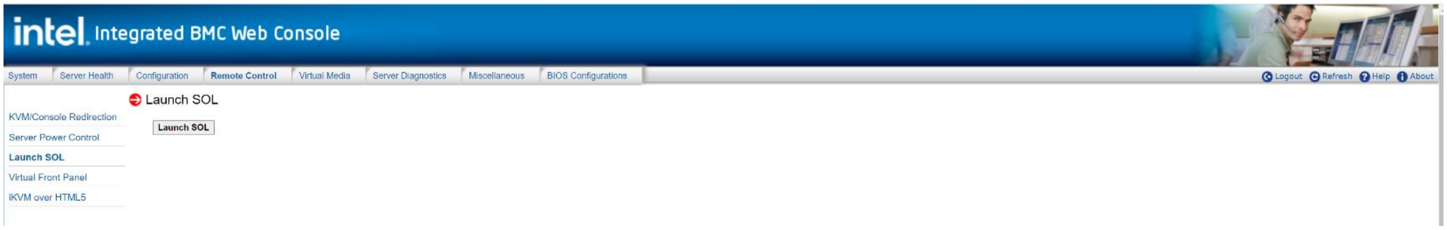
Table 25. Remote Control Power Control Options

Option	Task
Reset Server	Hard reset the host without powering off.
Power OFF Server - Immediate	Immediately power off the host.
Graceful Shutdown	Soft power off the host. **Note:** For the Graceful Shutdown option to function properly, the operating system must be ACPI aware and be configured to shut down without operator intervention. After a graceful shutdown has been requested, if the system does not shut down as requested, the command cannot be executed again for five minutes.
Power ON Server	Power on the host.
Power Cycle Server	Immediately power off the host and power it back on after one second.
Force-Enter BIOS Setup	Enter **BIOS Setup** after powering on the server.
Perform Action	Execute the selected remote power command.

Note: All power control actions are done through the BMC and are immediate actions. Gracefully shut down the operating system using the KVM interface or other interface before starting power actions.

7.4.3 Launch SOL

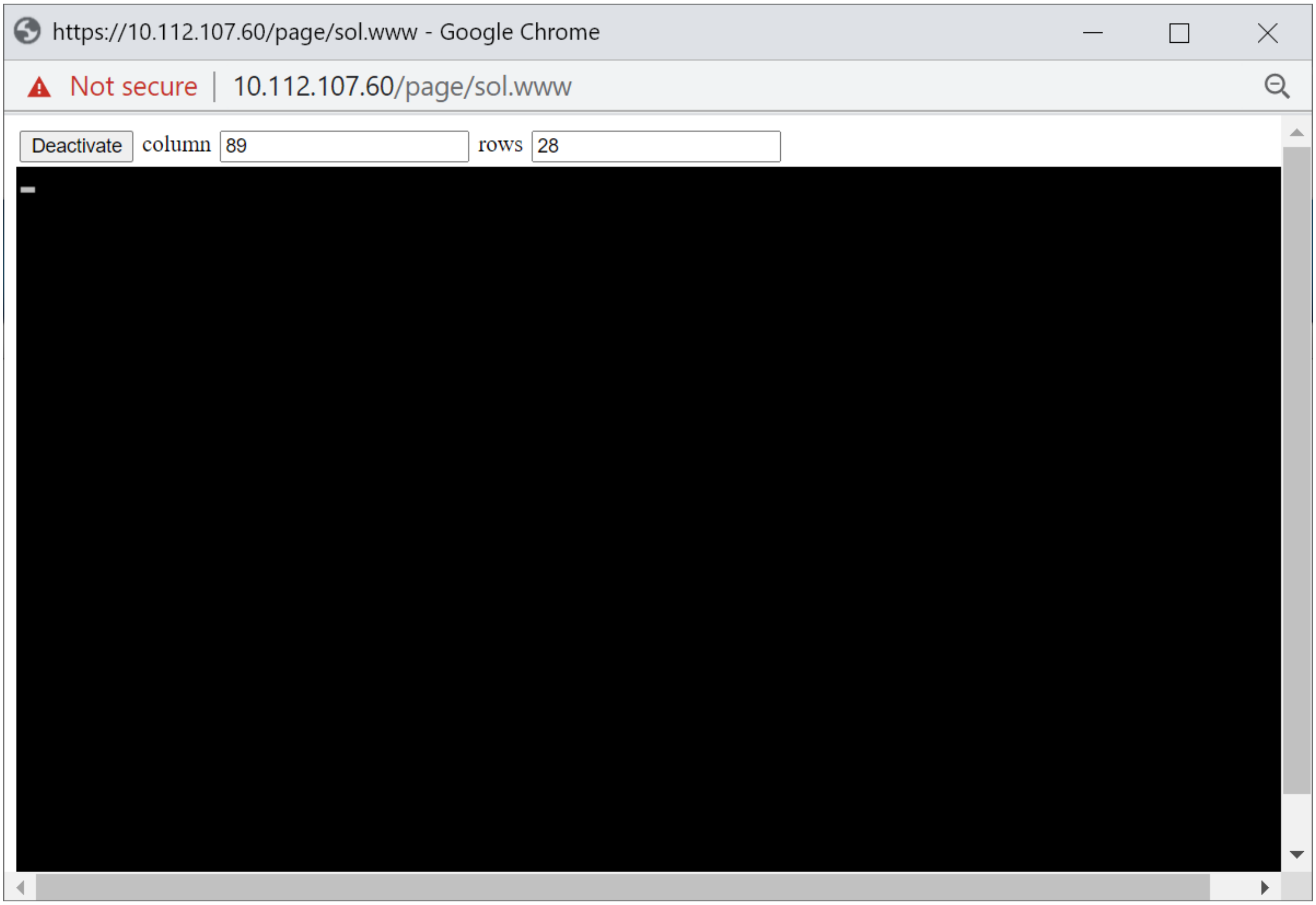
The Launch SOL page allows launching the SOL console to manage the server remotely. Click **Launch SOL** to open SOL window. See Figure 93 for details.



Launch SOL

Figure 93. Remote Control Launch SOL Page

Starting the SOL console opens an additional window, as shown in Figure 94. It displays the remote server's screen content. The SOL console behaves as if the user were connected to a serial terminal on the remote server. The responsiveness may be slightly delayed depending on the network's bandwidth and latency between the Intel® Integrated BMC Web Console and the remote console.



https://10.112.107.60/page/sol.www - Google Chrome
Not secure
10.112.107.60/page/sol.www
Deactivate

column 89 rows 28

Figure 94: Remote Control Launch SOL Screen Page

Note: Make sure to enable SOL for the baseboard management control from **Configuration > SOL** before launching SOL.

7.4.4 Virtual Front Panel

The Virtual Front Panel page provides virtual access to the front panel function. See Figure 95 and Table 26 for details.

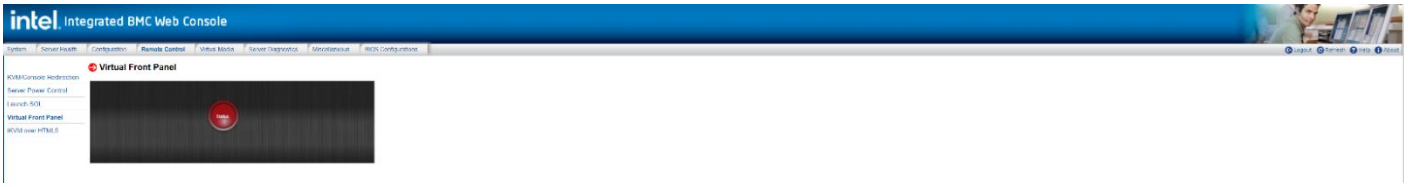


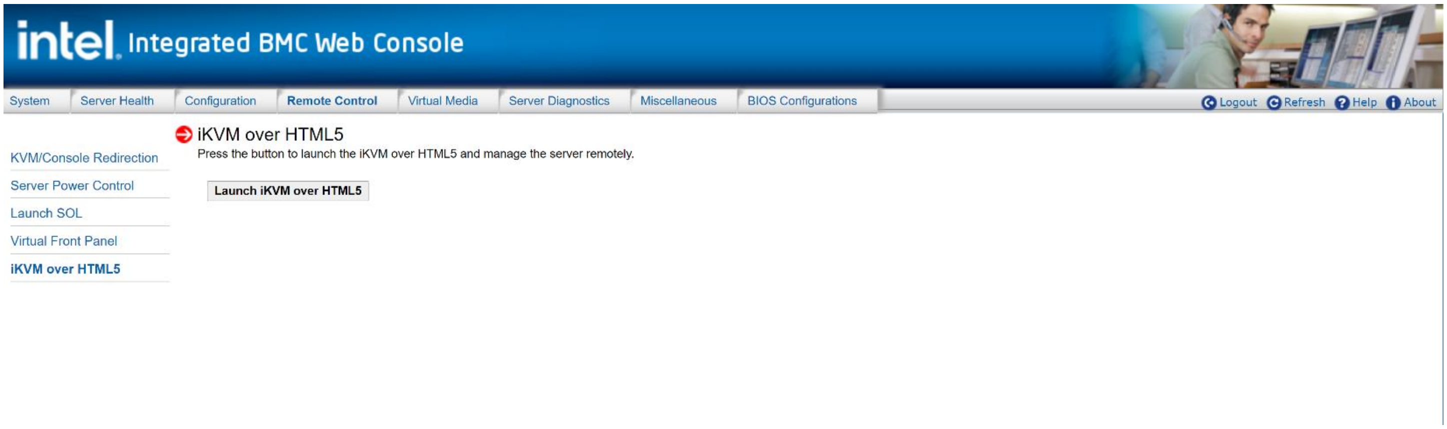
Figure 95: Remote Control Virtual Front Panel Page

Table 26. Remote Control Virtual Front Panel Options

Option	Task
Status LED	Status LED reflects the system status and it automatically synchronizes with BMC every 20 seconds. If any abnormality occurs in the system, then Status LED changes accordingly: • **LED red.** The system is in Off State. • **LED blinking red.** The system is in Warning State. • **LED solid red.** The system is in Critical State.

7.4.5 iKVM over HTML5

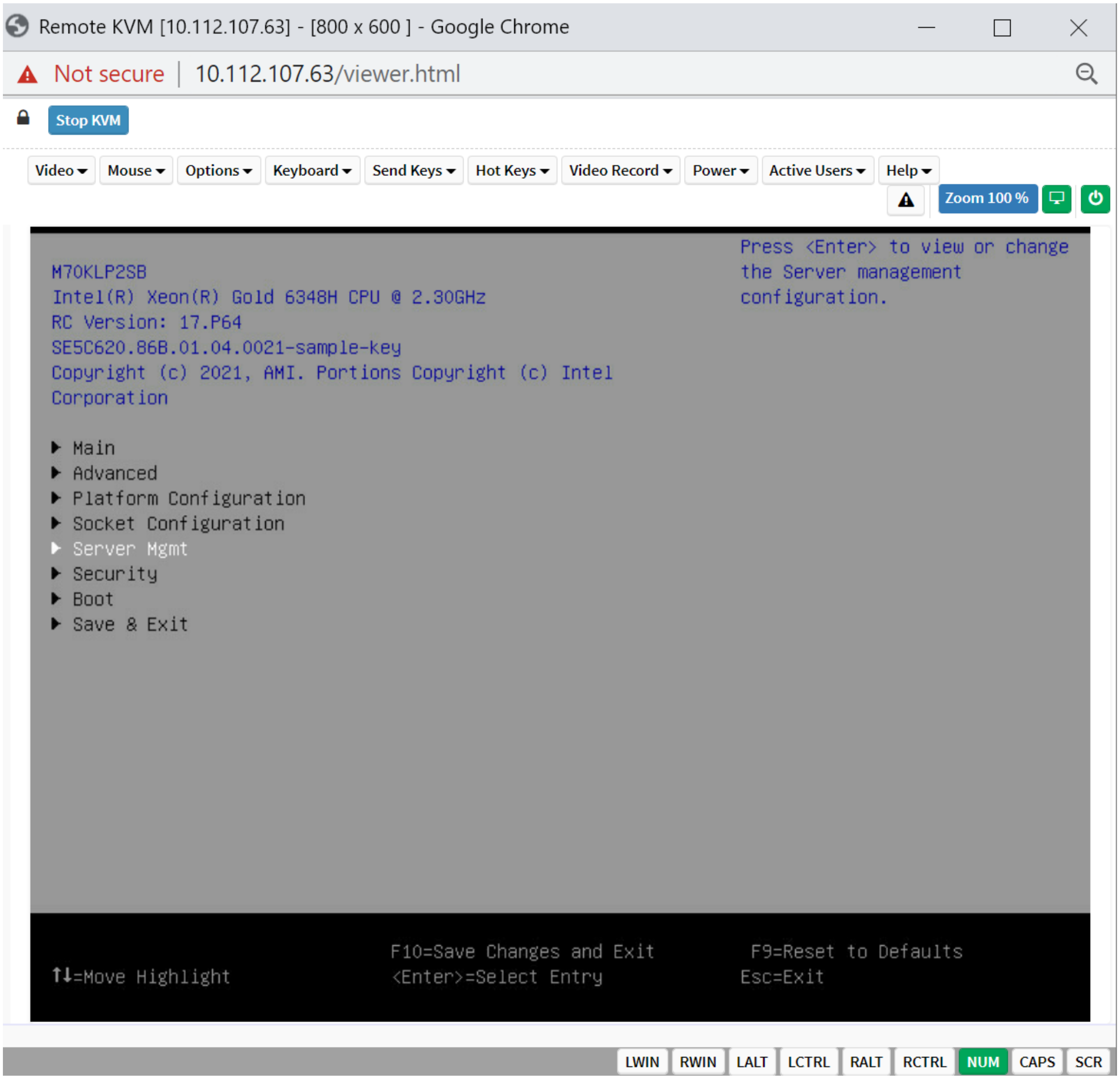
This page has the redirection window from which the user can launch the remote iKVM over HLTM5. See Figure 96 and Figure 97 for details.



iKVM over HTML5

Press the button to launch the iKVM over HTML5 and manage the server remotely.

Figure 96. iKVM Over HTML5 Page



```
                                                      Press <Enter> to view or change
M70KLP2SB                                             the Server management
Intel(R) Xeon(R) Gold 6348H CPU @ 2.30GHz             configuration.
RC Version: 17.P64
SE5C620.86B.01.04.0021-sample-key
Copyright (c) 2021, AMI. Portions Copyright (c) Intel
Corporation

▶ Main
▶ Advanced
▶ Platform Configuration
▶ Socket Configuration
▶ Server Mgmt
▶ Security
▶ Boot
▶ Save & Exit


                               F10=Save Changes and Exit     F9=Reset to Defaults
↑↓=Move Highlight              <Enter>=Select Entry         Esc=Exit
```

Figure 97. HTML5 Screen Page

7.5 Remote KVM Control Bar

The remote KVM window top contains a control bar to view the remote KVM status and to configure remote KVM settings. The following subsections describe each control task.

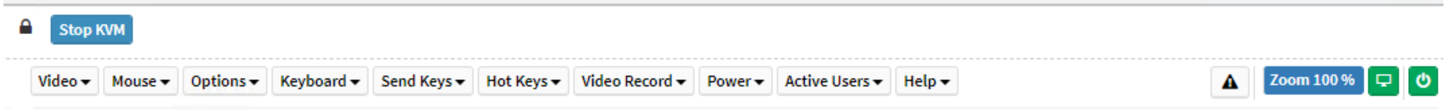


Figure 98. Remote KVM Control Bar

7.5.1 Video Menu

Click **Video** in the remote KVM control bar to open the virtual storage and virtual keyboard menu, as shown in Figure 99.

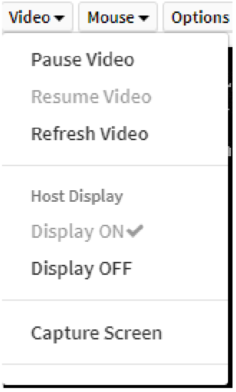


Figure 99. Video Menu

Use the options in this menu to do the following:

- Pause Video
- Resume Video
- Refresh Video
- Host Display
- Display ON
- Display OFF
- Capture Screen

7.5.2 Mouse Menu

Click **Mouse** in the remote KVM control bar to open the Mouse menu, as shown in Figure 100.

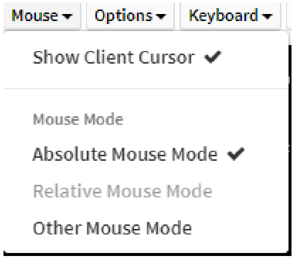


Figure 100. Mouse Menu

Use the options in this menu to do the following:

- Show Client Cursor
- Mouse Mode
- Absolute Mouse Mode
- Relative Mouse Mode
- Other Mouse Mode

7.5.3 Options Menu

Click **Options** in the remote KVM control bar to open the Options menu, as shown in Figure 101.

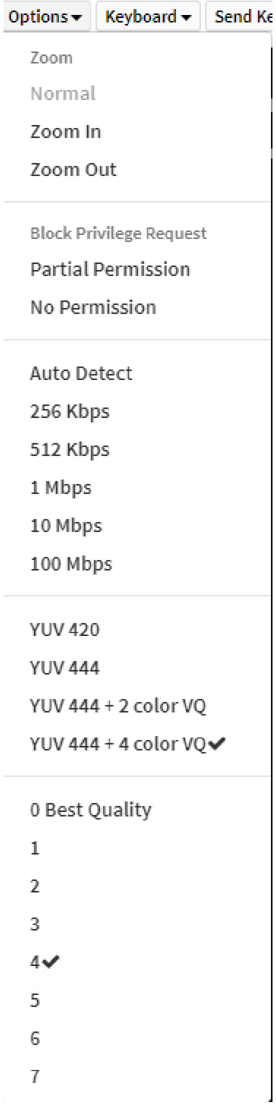


Figure 101. Options Menu

Use the options in this menu to do the following:

- Zoom
- Normal
- Zoom In
- Zoom Out
- Black Privilege Request
- Partial Permission
- No Permission
- Auto Detect
- 256 Kbps
- 512 Kbps
- 1 Mbps
- 10 Mbps
- 100 Mbps
- YUV 420
- YUV 444
- YUV 444+2 color VQ
- YUV 444+4 color VQ
- 0~7

7.5.4 Keyboard Menu

Click **Keyboard** in the remote KVM control bar to open the Keyboard menu, as shown in Figure 102.

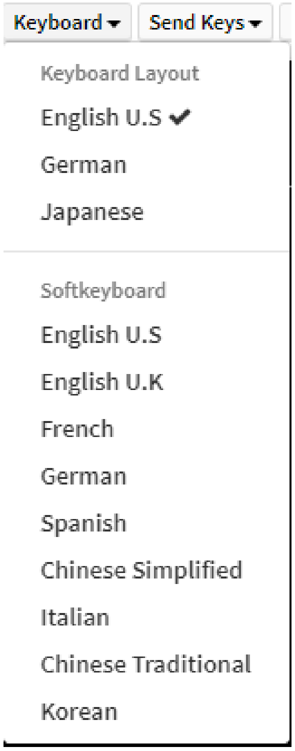


Figure 102. Keyboard Menu

Use the options in this menu to do the following:

- Keyboard Layout
  - English U.S
  - German
  - Japanese
- Softkeyboard
  - English U.S
  - English U.K
  - French
  - German
  - Spanish
  - Chinese Simplified
  - Italian
  - Chinese Traditional
  - Korean

7.5.5 Send Keys Menu

Click **Send Keys** in the remote KVM control bar to open the Send Keys menu, as shown in Figure 103.

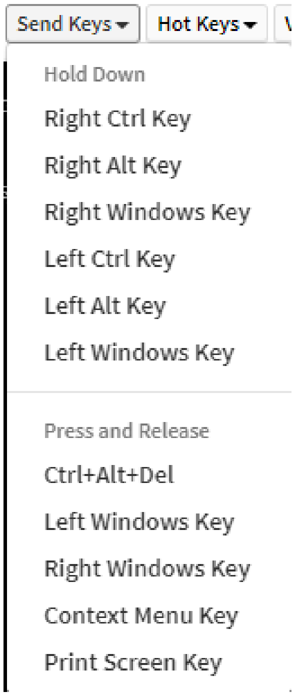


Figure 103. Send Keys Menu

Use the options in this menu to do the following:

- Hold Down
- Right Ctrl Key
- Right Alt Key
- Right Windows Key
- Left Ctrl Key
- Left Alt Key
- Left Windows Key
- Press and Release
- Ctrl+Alt+Del
- Left Windows Key
- Right Windows Key
- Context Menu Key
- Print Screen Key

7.5.6 Hot Keys Menu

Click **Hot Keys** in the remote KVM control bar to open the Hot Keys menu, as shown in Figure 104.

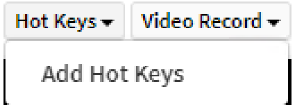


Figure 104. Hot Keys Menu

Use the options in this menu to do the following:

- Add Hot Keys

7.5.7 Video Record Menu

Click **Video Record** in the remote KVM control bar to open the Video Record menu, as shown in Figure 105.

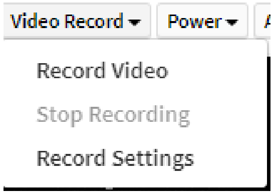


Figure 105. Video Record Menu

Use the options in this menu to do the following:

- Record Video
- Stop Recording
- Record Settings

7.5.8 Power Menu

Click **Power** in the remote KVM control bar to open the Power menu, as shown in Figure 106.

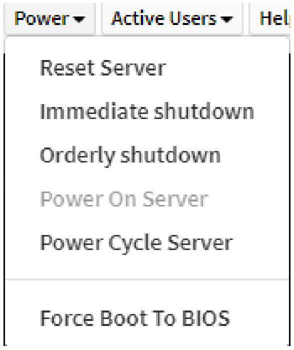


Figure 106. Power Menu

Use the options in this menu to do the following:

- Reset Server
- Immediate shutdown
- Orderly shutdown
- Power On Server
- Power Cycle Server
- Force Boot To BIOS

7.5.9 Active Users Menu

Click **Active Users** in the remote KVM control bar to open the Active Users menu, as shown in Figure 107.

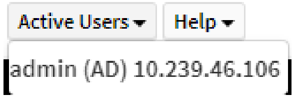


Figure 107. Active Users Menu

Use the options in this menu to do the following:

- Active User Name(ID)

7.5.10 Help Menu

Click **Help** in the remote KVM control bar to open the Help menu, as shown in Figure 108.

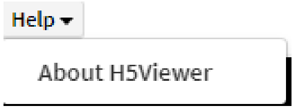
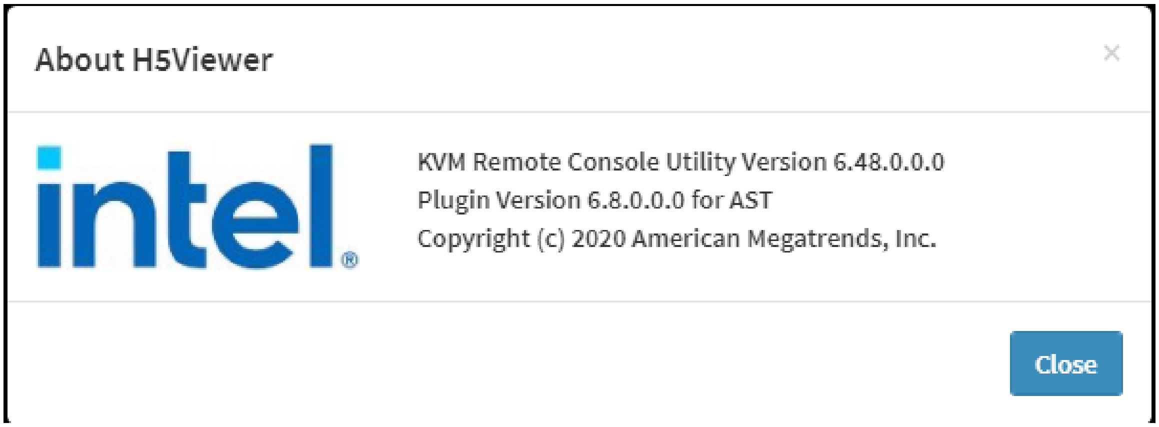


Figure 108. Help Menu

Use the options in this menu to do the following:

- About H5Viewer



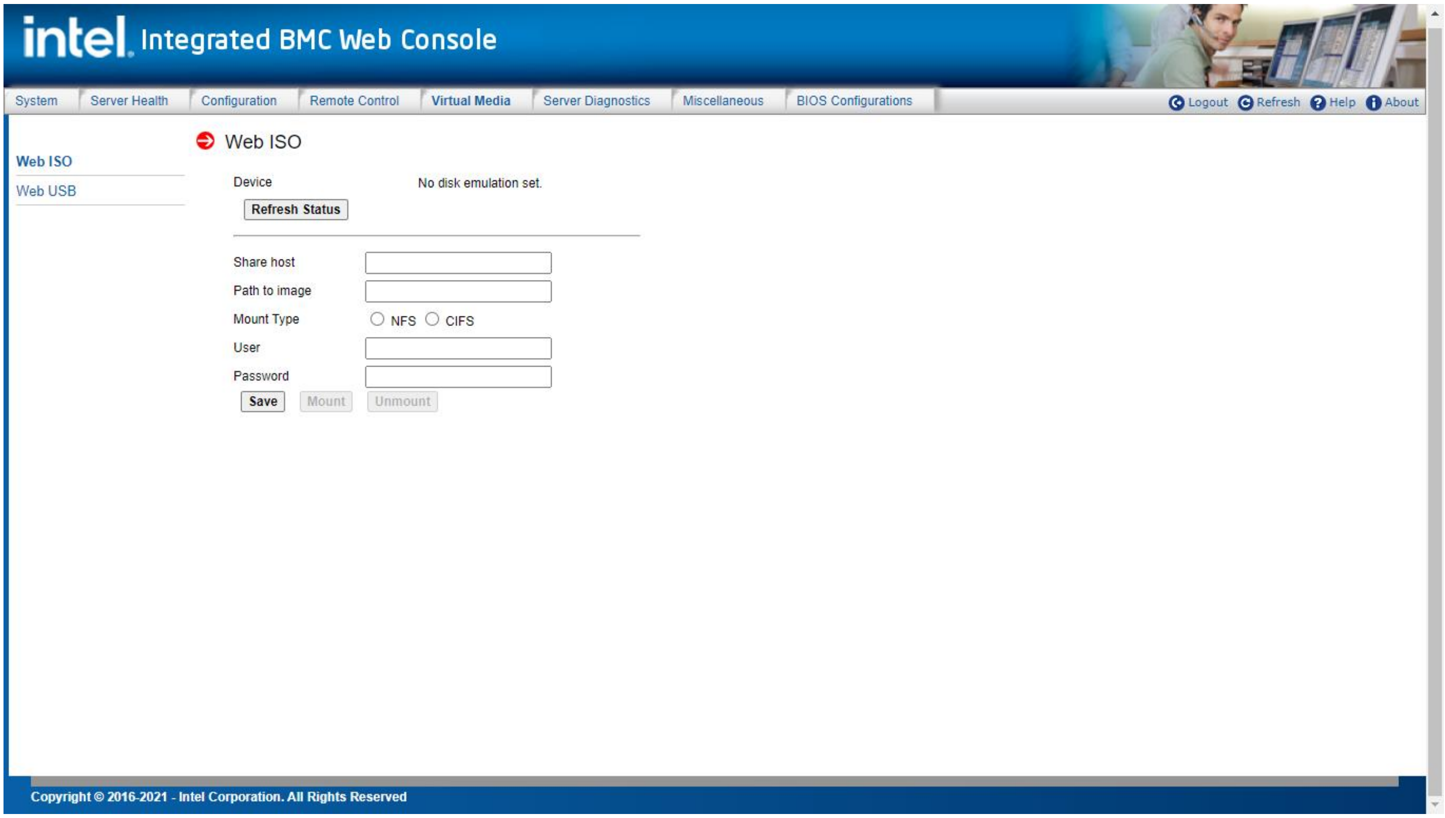
KVM Remote Console Utility Version 6.48.0.0.0
Plugin Version 6.8.0.0.0 for AST
Copyright (c) 2020 American Megatrends, Inc.

Figure 109. H5Viewer Help

7.6 Virtual Media Tab

The Virtual Media tab allows the user to share an ISO image using the SMB or NFS protocol. It allows the user to share the image via Windows Share* or Linux Samba*. This image is emulated to the host as a USB device. See Figure 110 for more details.

Note: License Key is required in the remote system. Otherwise, the Web ISO Page is grayed out.



Web ISO

Device No disk emulation set.

Share host

Path to image

Mount Type ○ NFS ○ CIFS

User

Password

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 110. Virtual Media Web ISO Page

Table 27. Web ISO Option

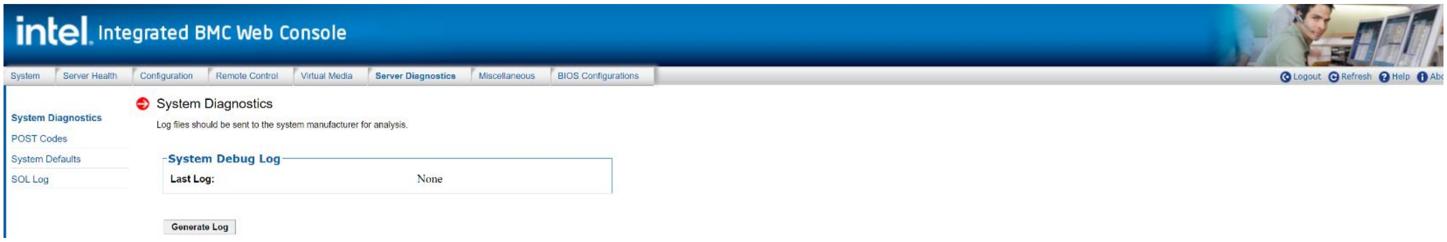
Option	Task
Device	Showing the virtual media status.
Share host	Share host IP address.
Path to image	Image name with path.
Mount Type	Choose the share type of remote media server: • **NFS**: Choose NFS if `iso`/`img` file is present in NFS share. • **CIFS:** If share type is `Samba (CIFS)`, then enter user credentials to authenticate the server. **Note:** Domain Name field is optional.
User	User name is required only for CIFS mount.
Password	User password is required only for CIFS mount.
Refresh Status	Button to get all virtual media status.
Save	Button to save the shared image information.
Mount	Button to mount a shared image.
Unmount	If a device has been mounted, click the **Unmount** button to unmount.

7.7 Server Diagnostics Tab

The Server Diagnostics tab contains general system diagnostics information, as explained in the following subsections.

7.7.1 System Diagnostics

The System Diagnostics page allows administrators to collect system debugging information. This feature allows a user to export data into a file that is retrievable. Such file can be sent to your Intel support representative for enhanced debugging capability. The files are compressed, encrypted, and password protected. The files are not meant to be viewable by the end user but provide additional debugging capability to the system manufacturer or your Intel support representative. See Figure 111 for details.



System Diagnostics

Log files should be sent to the system manufacturer for analysis.

System Debug Log

Last Log: None

Figure 111. Server System Diagnostics Page

Click the **Generate Log** button. It may take some time for the debugging information to be collected. After the debug log dump is finished, click the debug log filename to save the results as a `.zip*` file on the client system. The file can then be sent to the system manufacturer or your Intel support representative for analysis.

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

- **Platform sensor readings.** This includes all "readable" sensors that can be accessed by the BMC firmware and have associated SDRs populated in the SDR repository. This does not include any "event-only" sensors.

Note: All BIOS sensors and some BMC and Intel® ME sensors are "event-only". Such sensors are not readable using an IPMI `Get Sensor Reading` command but rather are used just for event logging purposes.

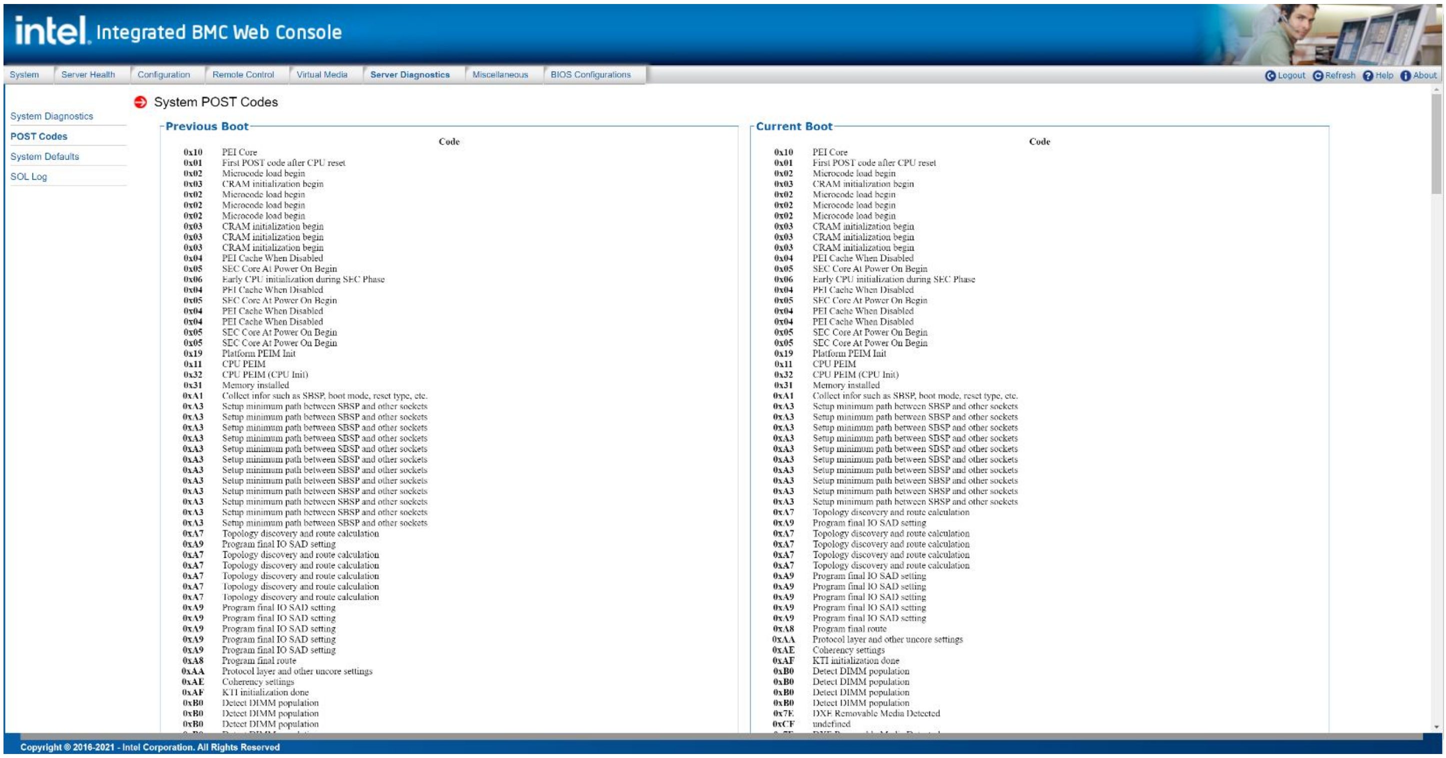
- **SEL.** The current SEL contents are saved in both hexadecimal and text format.
- **CPU/memory register data.** Useful for diagnosing the cause of the following system errors: CATERR, ERR2, SMI timeout, PERR, and SERR. The debug data is saved and time stamped for the last three occurrences of the error conditions.
  - PCI error registers.
  - MSR registers.
  - Integrated memory controller (IMC) and integrated I/O (IIO) module registers.
- BMC configuration data.
- **BMC firmware debug log** (syslog)**.** Captures firmware debug messages.

7.7.2 POST Codes

The POST Codes page displays recent power-on self-test (POST) results. See Figure 112 for details. The time base can be viewed as the time from POST start, or the time since the previous POST code was logged. Select this by clicking the **Show time** drop-down box.

All time formats are in `minutes:seconds.milliseconds`. Previous and current boot POST codes are shown. The current boot codes become previous codes when the system is reset or shut down.

Holding the cursor over a time, POST code, or description highlights all other occurrences of that same POST code. Clicking on a time, POST code, or description causes the highlighting to persist until another code is clicked.



System POST Codes

Previous Boot

	Code
0x10	PEI Core
0x01	First POST code after CPU reset
0x02	Microcode load begin
0x03	CRAM initialization begin
0x02	Microcode load begin
0x02	Microcode load begin
0x02	Microcode load begin
0x03	CRAM initialization begin
0x03	CRAM initialization begin
0x03	CRAM initialization begin
0x04	PEI Cache When Disabled
0x05	SEC Core At Power On Begin
0x06	Early CPU initialization during SEC Phase
0x04	PEI Cache When Disabled
0x05	SEC Core At Power On Begin
0x04	PEI Cache When Disabled
0x04	PEI Cache When Disabled
0x05	SEC Core At Power On Begin
0x05	SEC Core At Power On Begin
0x19	Platform PEIM Init
0x11	CPU PEIM
0x32	CPU PEIM (CPU Init)
0x31	Memory installed
0xA1	Collect infor such as SBSP, boot mode, reset type, etc.
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA7	Topology discovery and route calculation
0xA9	Program final IO SAD setting
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA8	Program final route
0xAA	Protocol layer and other uncore settings
0xAE	Coherency settings
0xAF	KTI initialization done
0xB0	Detect DIMM population
0xB0	Detect DIMM population
0xB0	Detect DIMM population

Current Boot

	Code
0x10	PEI Core
0x01	First POST code after CPU reset
0x02	Microcode load begin
0x03	CRAM initialization begin
0x02	Microcode load begin
0x02	Microcode load begin
0x02	Microcode load begin
0x03	CRAM initialization begin
0x03	CRAM initialization begin
0x03	CRAM initialization begin
0x04	PEI Cache When Disabled
0x05	SEC Core At Power On Begin
0x06	Early CPU initialization during SEC Phase
0x04	PEI Cache When Disabled
0x05	SEC Core At Power On Begin
0x04	PEI Cache When Disabled
0x04	PEI Cache When Disabled
0x05	SEC Core At Power On Begin
0x05	SEC Core At Power On Begin
0x19	Platform PEIM Init
0x11	CPU PEIM
0x32	CPU PEIM (CPU Init)
0x31	Memory installed
0xA1	Collect infor such as SBSP, boot mode, reset type, etc.
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA3	Setup minimum path between SBSP and other sockets
0xA7	Topology discovery and route calculation
0xA9	Program final IO SAD setting
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA7	Topology discovery and route calculation
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA9	Program final IO SAD setting
0xA8	Program final route
0xAA	Protocol layer and other uncore settings
0xAE	Coherency settings
0xAF	KTI initialization done
0xB0	Detect DIMM population
0xB0	Detect DIMM population
0xB0	Detect DIMM population
0xB0	Detect DIMM population
0x7E	DXE Removable Media Detected
0xCF	undefined

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 112. Server Diagnostics POST Codes Page

7.7.3 System Defaults

The System Defaults page allows resetting all BMC settings to factory defaults. See Figure 113 for details. Click the **Restore** button to reset all BMC settings to factory defaults. Once completed, all remote management, including the web server, is not accessible until users and network settings are restored locally. Settings lost include, but are not limited to:

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

This does not affect the BMC's system event log, sensor data repository, or any Intel® Node Manager (Intel® NM) settings and policies.

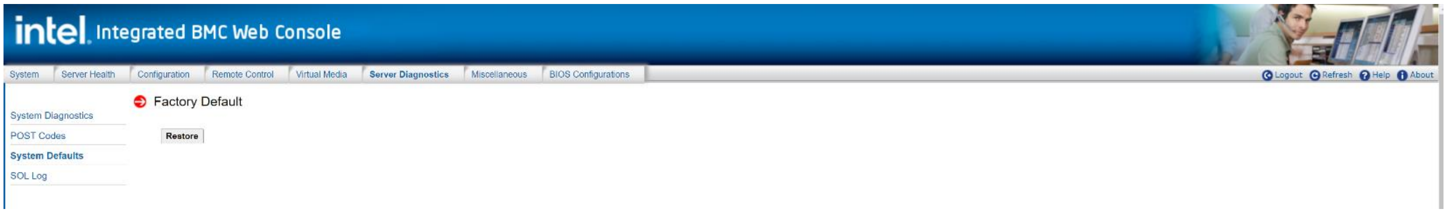


Figure 113. Server Diagnostics Default Page

Warning: This action resets all the BMC settings to factory defaults and cannot be undone.

7.7.4 SOL Log

The SOL Log page allows to enable or disable SOL logging and to download the log (see Figure 114). Table 28 lists the SOL log operations that can be performed.

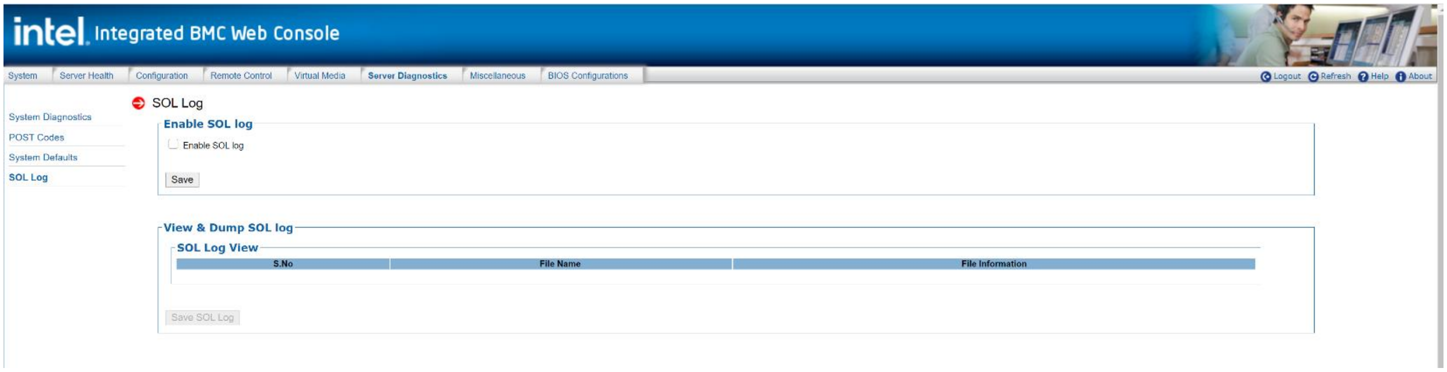


Figure 114. Server Diagnostics SOL Log Page

Table 28. Server Diagnostics SOL Log Options

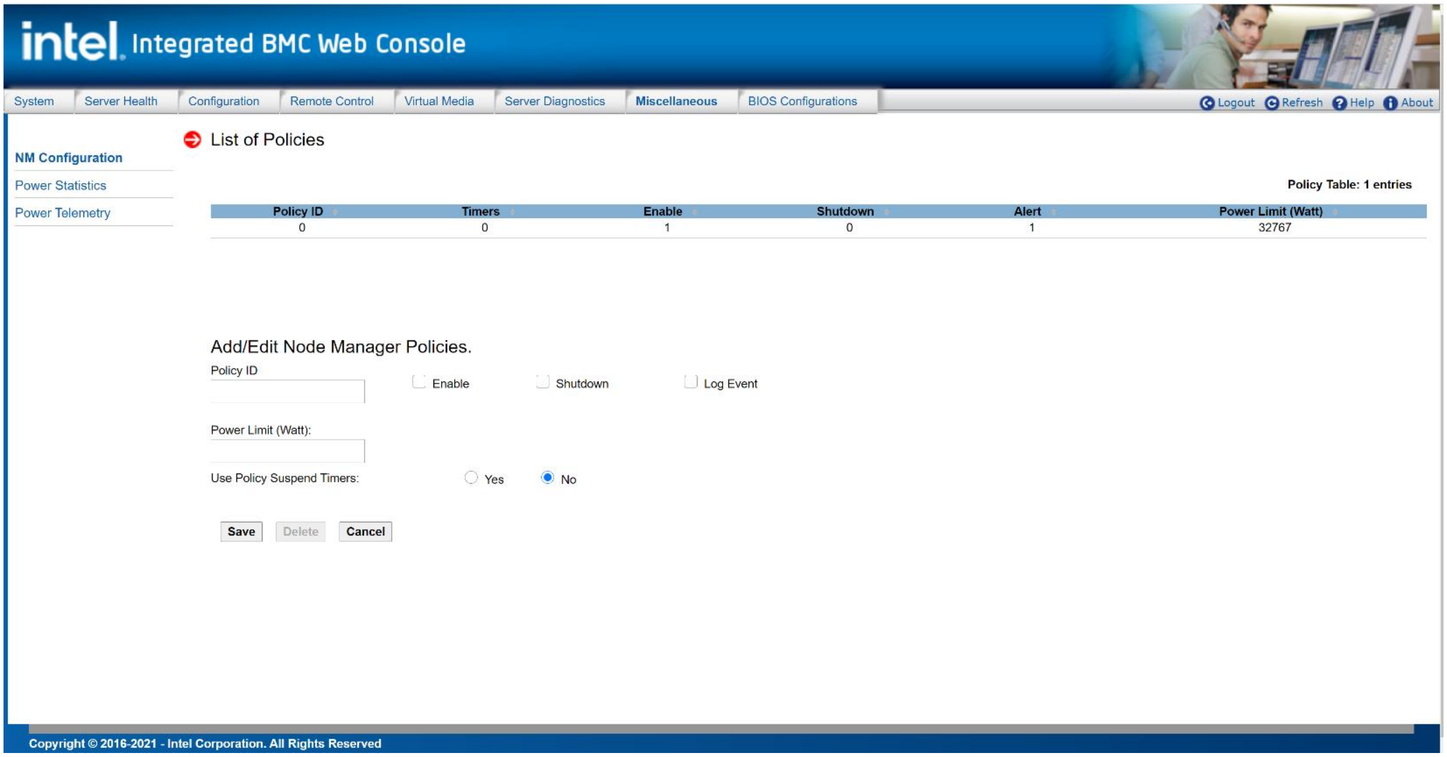
Option	Task
Enable SOL Log	Enable or disable SOL log.
Save Button for Enable SOL Log	Save the enable/disable setting for SOL log.
View&Dump SOL Log	SOL log is displayed.
Save SOL Log Button for Enable SOL Log	Save the log to the local device.

7.8 Miscellaneous Tab

The **Miscellaneous** tab contains the Intel® NM configuration, power statistics and power telemetry information, as explained in the following subsections.

7.8.1 Configuration of Intel® Node Manager

Intel® NM configuration lets the user view, add, and configure the Intel® NM policies. See Figure 115 for details. Table 29 lists the options to view, add, and edit the Intel® NM power policies.



List of Policies

Policy Table: 1 entries

Policy ID	Timers	Enable	Shutdown	Alert	Power Limit (Watt)
0	0	1	0	1	32767

Add/Edit Node Manager Policies.

Policy ID ☐ Enable ☐ Shutdown ☐ Log Event

Power Limit (Watt):

Use Policy Suspend Timers: ○ Yes ● No

Save
Delete
Cancel
Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

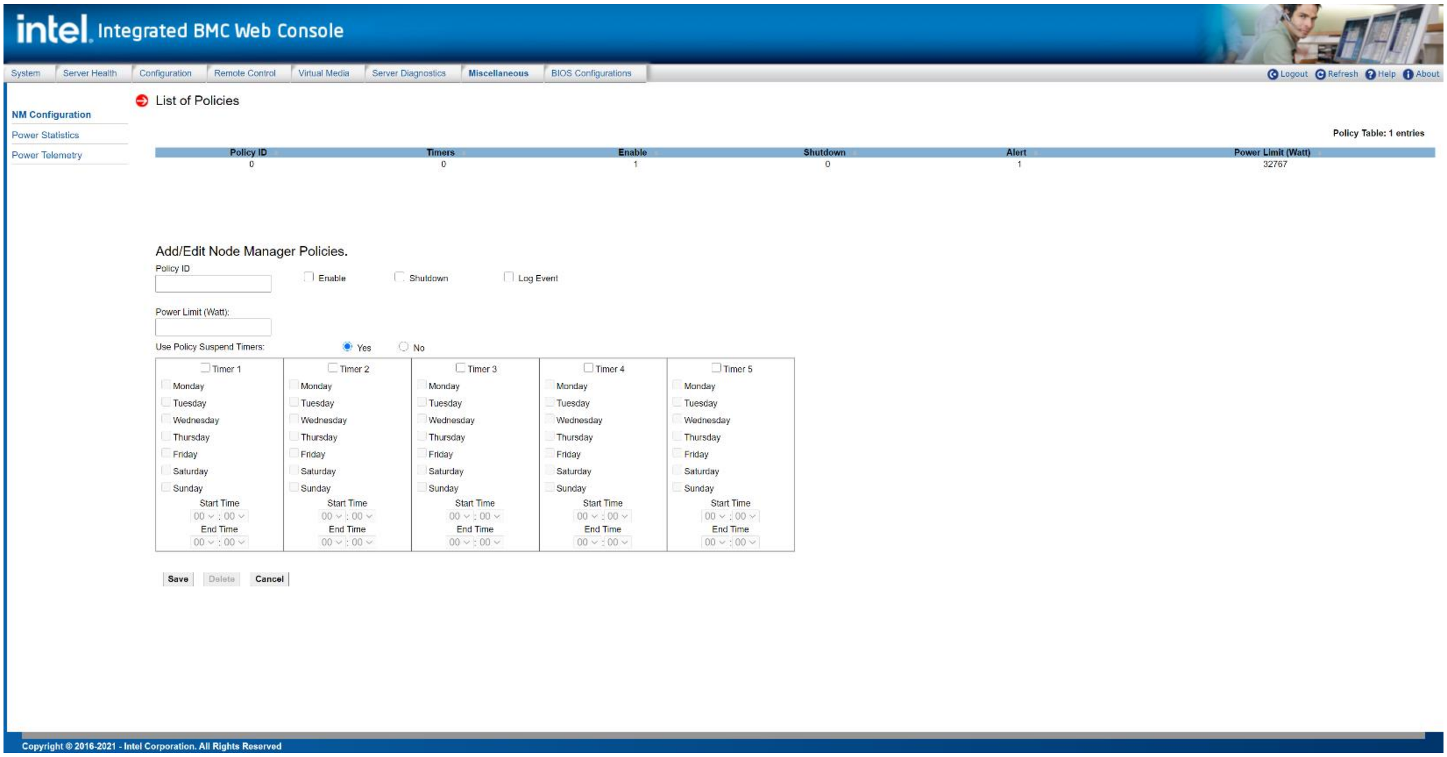
Figure 115. Intel® Node Manager Configuration Page

Table 29. 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 settings section below.
Policy ID	The policy ID to add/edit/delete. Valid range is 0–255. In the policy table, policy IDs with an asterisk (*) are policies set externally using a non-platform domain. Changing parameters on these policies does not affect their triggers, trigger limits, reporting periods, correction timeouts, or aggressive CPU throttling settings.
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 starts an immediate shutdown.
Log Event	Enable the Intel® NM 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	If enabled, configure policy suspend periods. Each policy may have up to five suspend periods (see Figure 116). Suspend periods are repeatable by day-of-week. Start and stop times are designated in 24-hour format, in increments of 6 minutes. To specify a suspended period crossing midnight, two suspend periods must be used.
Save	Click to save any changes made.
Delete	Select a policy in the list and click to delete.
Cancel	Click to discard changes.

For all policies set through this page, the following default values are applied:

- **Domain:** Platform. Power for the entire platform.
- **Trigger:** None. Always monitor after the end of POST.
- **Aggressive CPU Power Correction:** AUTO. Use of T-states and memory throttling controlled by policy exception actions.
- **Trigger Limit:** None.
- **Reporting Period:** 10 seconds. This is a rolling average for reporting only. It does not affect the average power monitored by the Intel® NM.
- **Correction Timeout:** 22.555 seconds. Maximum time for the Intel® NM to correct power before taking an exception action (that is, shutdown or alert).



List of Policies

Policy Table: 1 entries

Policy ID	Timers	Enable	Shutdown	Alert	Power Limit (Watt)
0	0	1	0	1	32767

Add/Edit Node Manager Policies.

Policy ID □ Enable □ Shutdown □ Log Event

Power Limit (Watt):

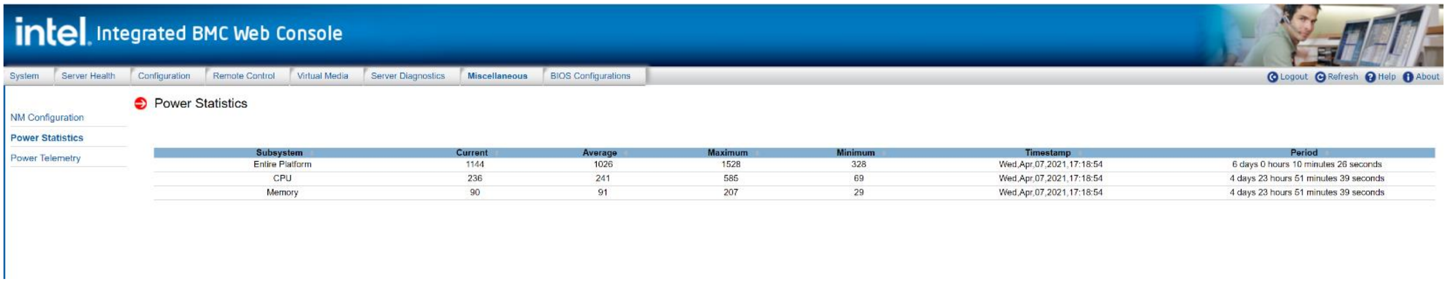
Use Policy Suspend Timers: ● Yes ○ No

□ Timer 1	□ Timer 2	□ Timer 3	□ Timer 4	□ Timer 5
□ Monday	□ Monday	□ Monday	□ Monday	□ Monday
□ Tuesday	□ Tuesday	□ Tuesday	□ Tuesday	□ Tuesday
□ Wednesday	□ Wednesday	□ Wednesday	□ Wednesday	□ Wednesday
□ Thursday	□ Thursday	□ Thursday	□ Thursday	□ Thursday
□ Friday	□ Friday	□ Friday	□ Friday	□ Friday
□ Saturday	□ Saturday	□ Saturday	□ Saturday	□ Saturday
□ Sunday	□ Sunday	□ Sunday	□ Sunday	□ Sunday
Start Time 00 : 00	Start Time 00 : 00	Start Time 00 : 00	Start Time 00 : 00	Start Time 00 : 00
End Time 00 : 00	End Time 00 : 00	End Time 00 : 00	End Time 00 : 00	End Time 00 : 00

Figure 116. Intel® Node Manager Configuration Suspend Page

7.8.2 Power Statistics

The Power Statistics page displays the entire platform, CPU, and memory power statistics. The page shows statistics for current, average, maximum, minimum, timestamp, and period. See Figure 117 for an example.



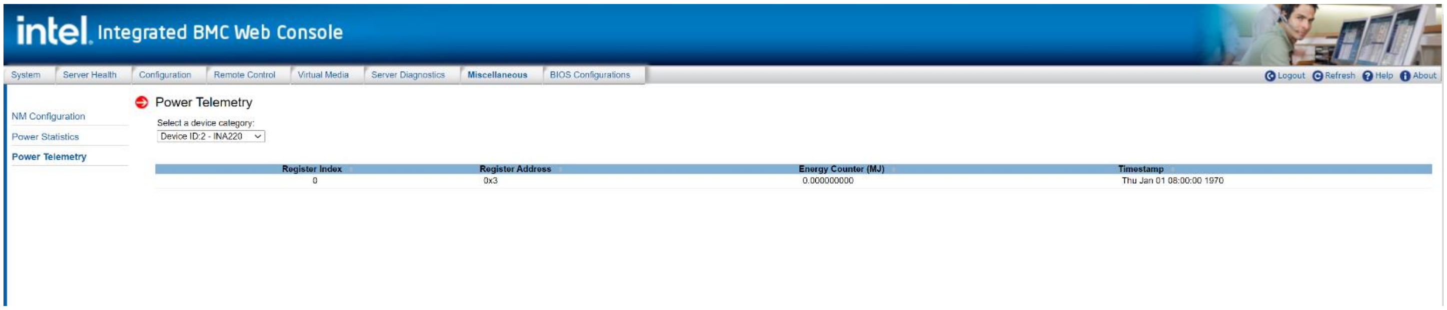
Power Statistics

Subsystem	Current	Average	Maximum	Minimum	Timestamp	Period
Entire Platform	1144	1026	1528	328	Wed,Apr,07,2021,17:18:54	6 days 0 hours 10 minutes 26 seconds
CPU	236	241	585	69	Wed,Apr,07,2021,17:18:54	4 days 23 hours 51 minutes 39 seconds
Memory	90	91	207	29	Wed,Apr,07,2021,17:18:54	4 days 23 hours 51 minutes 39 seconds

Figure 117. Power Statistics Page

7.8.3 Power Telemetry

The Power Telemetry page provides a method to get onboard component power, including PSU, CPU, memory, PCH, BMC, and other components. See Figure 118 for details. To select a device category, use the **Select a device category** drop-down box (see Figure 119).



Power Telemetry

Select a device category: Device ID:2 - INA220

Register Index	Register Address	Energy Counter (MJ)	Timestamp
0	0x3	0.000000000	Thu Jan 01 08:00:00 1970

Figure 118. Power Telemetry Page

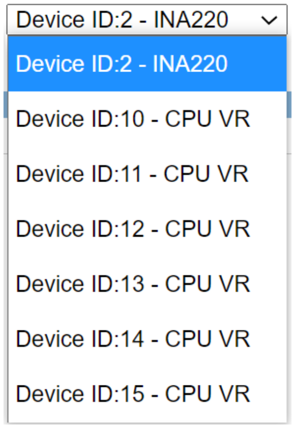


Figure 119. Power Telemetry Device Categories

7.9 BIOS Configurations Tab

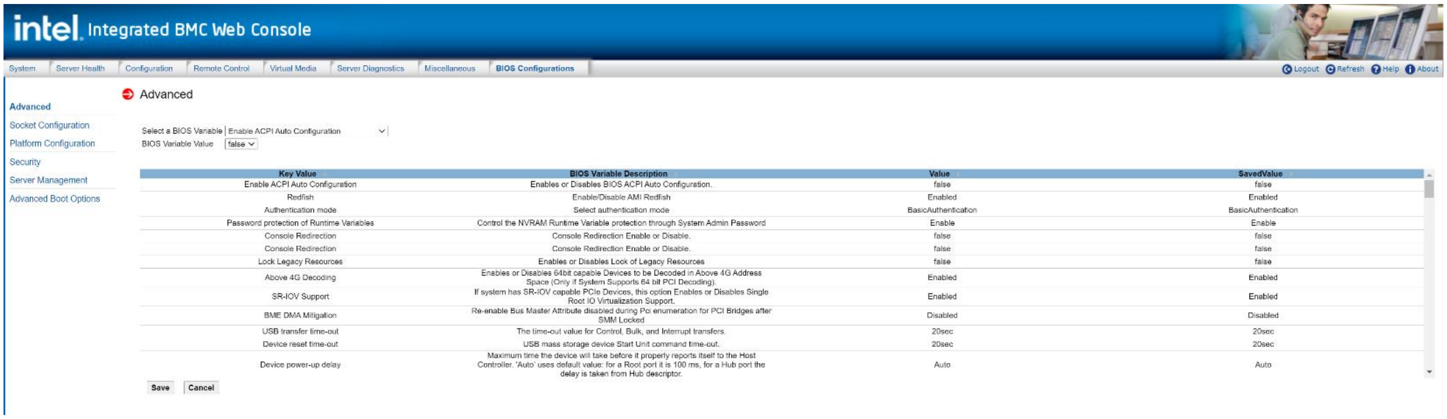
The **BIOS Configurations** tab provides a method to configure any BIOS Setup variables through the Intel® Integrated BMC Web Console, including the advanced, socket configuration, platform configuration, security and advanced boot options.

To select a BIOS variable, click the **Select a BIOS Variable** drop-down menu. Once a BIOS variable is selected, the corresponding current values are displayed in the BIOS Variable Value drop-down box.

To see other available options for the corresponding BIOS Variable, click the **BIOS Variable Value** drop-down box. If the value needs to be changed for the above variable, other available values can be selected from this drop-down box. Once the BIOS Variable Value has been chosen, click the **Save** button and the changed value is then reflected in the grid table.

7.9.1 Advanced

This page allows the user to change BIOS settings like Above 4G Decoding/Serial Port/CPU C6 report. See Figure 120 for details.



Advanced

Select a BIOS Variable: Enable ACPI Auto Configuration
BIOS Variable Value: false

Key Value	BIOS Variable Description	Value	SavedValue
Enable ACPI Auto Configuration	Enables or Disables BIOS ACPI Auto Configuration.	false	false
Redfish	Enable/Disable AMI Redfish	Enabled	Enabled
Authentication mode	Select authentication mode	BasicAuthentication	BasicAuthentication
Password protection of Runtime Variables	Control the NVRAM Runtime Variable protection through System Admin Password	Enable	Enable
Console Redirection	Console Redirection Enable or Disable.	false	false
Console Redirection	Console Redirection Enable or Disable.	false	false
Lock Legacy Resources	Enables or Disables Lock of Legacy Resources	false	false
Above 4G Decoding	Enables or Disables 64bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64 bit PCI Decoding).	Enabled	Enabled
SR-IOV Support	If system has SR-IOV capable PCIe Devices, this option Enables or Disables Single Root IO Virtualization Support.	Enabled	Enabled
BME DMA Mitigation	Re-enable Bus Master Attribute disabled during Pci enumeration for PCI Bridges after SMM Locked	Disabled	Disabled
USB transfer time-out	The time-out value for Control, Bulk, and Interrupt transfers.	20sec	20sec
Device reset time-out	USB mass storage device Start Unit command time-out.	20sec	20sec
Device power-up delay	Maximum time the device will take before it properly reports itself to the Host Controller. 'Auto' uses default value: for a Root port it is 100 ms, for a Hub port the delay is taken from Hub descriptor.	Auto	Auto

Figure 120. BIOS Advanced Page

Table 30. BIOS Advanced Variables

Variables	BIOS Variable Description
VT-UTF8 Combo Key Support	Enable VT-UTF8 Combination Key Support for ANSI/VT100 terminals.
USB transfer timeout	The timeout value for Control, Bulk, and Interrupt transfers.
Unpopulated Links	To save power, if this option is set to Disable Link, the software disables unpopulated PCI Express* links.
Turbo Mode	Enable or disable processor Turbo Mode (requires EMTTM enabled, too).
Terminal Type EMS	Character formatting used for console redirection. This setting must match the remote terminal application. VT-UTF8 is the preferred terminal type for out-of-band management. The next best choice is VT100+ and then VT100.
Terminal Type	Emulation: • **ANSI.** Extended ASCII char set. • **VT100.** ASCII char set. • **VT100+.** Extends VT100 to support color, function keys, and so on. • **VT-UTF8.** Uses UTF8 encoding to map Unicode chars onto 1 or more bytes.
Target Link Speed	If supported by hardware and set to Force to X.X GT/s for Downstream Ports, this variable sets an upper limit on Link operational speed. The limit is set by restricting the values advertised by the Upstream component in its training sequences. When Auto is selected, HW initialized data is used.
Stop Bits	Stop bits indicate the end of a serial data packet. A start bit indicates the beginning. The standard setting is one (1) stop bit. Communication with slow devices may require more than one (1) stop bit.
SR-IOV Support	If system has SR-IOV capable PCI Express* Devices, this option Enables or Disables Single Root IO Virtualization Support.
Intel SpeedStep® (P-states)	Enable or disable Enhanced Intel SpeedStep® Technology (P-states).
Slot # 9 Empty	Enable or disable Option ROM execution for the selected Slot.
Slot # 8 Mass Storage Controller	Device on Slot has: UEFI [X] Legacy [X] Option ROM(s). VIDx1000;DIDx14 @ s0|Bx44|Dx0|Fx0
Slot # 7 Empty	Enable or Disable Option ROM execution for the selected Slot.
Slot # 6 Empty	
Slot # 4 Empty	
Slot # 3 Empty	
Slot # 2 Empty	
Serial Port	Enable or Disable Serial Port (COM).

Variables	BIOS Variable Description
Restore if Failure	If the system does not boot and this option is set to Enabled, the software automatically resets the settings of this page and CSM page to its default values.
Resolution 100x31	Enable or disable extended terminal resolution.
Relaxed Ordering	Enable or disable PCI Express* Device Relaxed Ordering.
Redfish*	Enable or disable AMI Redfish*.
Recorder Mode	With this mode enabled, only text is sent. This is to capture Terminal data.
PuTTY KeyPad	Select Function Key and KeyPad on PuTTY.
Primary Video Ignore	If the software detects that, due to the policy settings, Option ROM of Primary Video Device does not dispatch, it ignores this device's policy settings and automatically restores it to Enable.
Power Performance Tuning	Options to decide who Controls EPB. • In **operating system mode**: IA32_ENERGY_PERF_BIAS is used. • In **BIOS mode**: ENERGY_PERF_BIAS_CONFIG is used. • In **PECI mode**: PCS53 is used.
PL2 Limit	Enable or disable PL2. If this option is disabled, BIOS programs the default values for PL2 Power Limit and PL2 Time Window.
PL1 Limit	Enable or disable PL1. If this option is disabled, BIOS programs the default values for PL1 Power Limit and PL1 Time Window.
PECI PCS EPB	Control whether PECI has control over EPB.
Password protection of Runtime Variables	Control the NVRAM Runtime Variable protection through System Admin Password.
Parity	A parity bit can be sent with the data bits to detect some transmission errors. • **Even:** parity bit is 0 if the number of 1's in the data bits is even. • **Odd:** parity bit is 0 if the number of 1's in the data bits is odd. • **Mark:** parity bit is always 1. • **Space:** Parity bit is always 0. Mark and Space Parity do not allow for error detection. They can be used as an additional data bit.
Package C State	Package C State limit.
Out-of-Band Mgmt Port	Microsoft Windows EMS* allows for remote management of a Windows Server* operating system through a serial port.
On Board Mass Storage Controller	Onboard Device has: UEFI [X] Legacy [X] Embedded ROM(s). VIDx8086;DIDxA1D2 @ s0|Bx0|Dx11|Fx5
On Board Display Controller	Onboard Device has: UEFI [X] Legacy [X] Embedded ROM(s). VIDx1A03;DIDx2000 @ s0|Bx4|Dx0|Fx0
No Snoop	Enable or disable PCI Express* Device No Snoop option.
Network Stack	Enable or disable UEFI Network Stack.
Maximum Read Request	Set Maximum Read Request Size of PCI Express* Device or allow System BIOS to select the value.
Maximum Payload	Set Maximum Payload of PCI Express* Device or allow System BIOS to select the value.
LTR Mechanism Enable	If supported by the hardware and set to Enabled, this variable enables the latency tolerance reporting (LTR) Mechanism.
Lock Legacy Resources	Enable or disable Lock of Legacy Resources.
Link Training Retry	Define the number of Retry Attempts the software takes to retrain the link if the previous training attempt was unsuccessful.
IPv6 PXE Support	Enable or disable IPv6 PXE boot support. If disabled, IPv6 PXE boot support is not available.
IPv6 HTTP Support	Enable or disable IPv6 HTTP boot support. If disabled, IPv6 HTTP boot support is not available.
IPv4 PXE Support	Enable or disable IPv4 PXE boot support. If disabled, IPv4 PXE boot support is not available.
IPv4 HTTP Support	Enable or disable IPv4 HTTP boot support. If disabled, IPv4 HTTP boot support is not available.
IDO Request Enable	If supported by hardware and set to Enabled, this variable allows the user to set the number of ID-based ordering (IDO) bit (Attribute[2]) requests to be initiated.
IDO Completion Enable	If supported by the hardware and set to Enabled, this variable allows the user to set the number of IDO bit (Attribute[2]) requests to be initiated.
Hardware P-States	**Disable:** Hardware chooses a P-state based on operating system Request (Legacy P-States). **Native Mode:** Hardware chooses a P-state based on operating system guidance. **Out of Band Mode:** Hardware autonomously chooses a P-state (no operating system guidance).
Hardware Autonomous Width	If supported by the hardware and set to Disabled, this disables the hardware's ability to change link width except width size reduction for the purpose of correcting unstable link operation.

Variables	BIOS Variable Description
Hardware Autonomous Speed	If supported by the hardware and set to Disabled, this disables the hardware's ability to change link speed, except speed rate reduction, for the purpose of correcting unstable link operation.
Flow Control EMS	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signals.
Flow Control	Flow control can prevent data loss from buffer overflow. When sending data, if the receiving buffers are full, a "stop" signal can be sent to stop the data flow. Once the buffers are empty, a "start" signal can be sent to restart the flow. Hardware flow control uses two wires to send start/stop signals.
Extended Tag	If it is set to Enabled, allows Device to use 8-bit Tag field as a requester.
Extended Synch	If it is set to Enabled, allows generation of Extended Synchronization patterns.
Enhanced Halt State (C1E)	Core C1E auto promotion Control. Takes effect after reboot.
End-End TLP Prefix Blocking	If supported by the hardware and set to Enabled, this function blocks the forwarding of TLPs that contain End-End TLP Prefixes.
Enable ACPI Auto Configuration	Enable or disable BIOS ACPI Auto Configuration.
Device Reset Timeout	USB mass storage device Start Unit command timeout.
Device Power-Up Delay	Maximum time the device takes before it properly reports itself to the Host Controller. Auto uses these **default values**: • For a Root port, 100 ms. • For a Hub port, the delay is taken from the Hub descriptor.
Data Bits	Data bits.
CPU C6 report	Enables or disables CPU C6(ACPI C3) report to operating system.
Console Redirection	Enables or disables Console Redirection.
Compliance SOS	If supported by the hardware and set to Enabled, this forces LTSSM to send SKP Ordered Sets between sequences when sending Compliance Pattern or Modified Compliance Pattern.
Clock Power Management	If supported by the hardware and set to Enabled, the device is permitted to use `CLKREQ#` signal for power management of Link clock, in accordance to protocol defined in appropriate form factor specification.
Change Settings	Select an optimal setting for Super I/O Device.
BME DMA Mitigation	Re-enable Bus Master Attribute disabled during PCI enumeration for PCI Bridge after SMM Locked.
Bits per second EMS	Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Bits per second	Select serial port transmission speed. The speed must be matched on the other side. Long or noisy lines may require lower speeds.
Authentication mode	Select authentication mode.
AtomicOp* Requester Enable	If supported by the hardware and set to Enabled, this function initiates AtomicOp* Requests only if Bus Master Enable bit is in the Command Register Set.
AtomicOp* Egress Blocking	If supported by hardware and set to Enabled, outbound AtomicOp* Requests via Egress Ports are blocked.
ASPM Support	Set the ASPM Level: • **Force L0s.** Forces all links to L0s. • **State AUTO.** BIOS auto configure. • **DISABLE.** Disables ASPM.
ARI Forwarding	If supported by the hardware and set to 'Enabled', the Downstream Port disables its traditional Device Number field. Such default value means 0 enforcement when turning a Type1 Configuration Request into a Type0 Configuration Request. Once enabled, the value grants access to Extended Functions in an ARI Device placed immediately below the Port. **Default value:** Disabled.
Above 4G Decoding	Enable or disable 64-bit capable Devices to be Decoded in Above 4G Address Space (Only if System Supports 64-bit PCI Decoding).

7.9.2 Socket Configuration

This page allows the user to enable or disable: legacy USB support, port 60 and port 64 emulation, make USB device non-bootable, configure device reset timeout for USB device. See Figure 121 for details. Table 31 lists all USB configuration variables that can be viewed and edited.

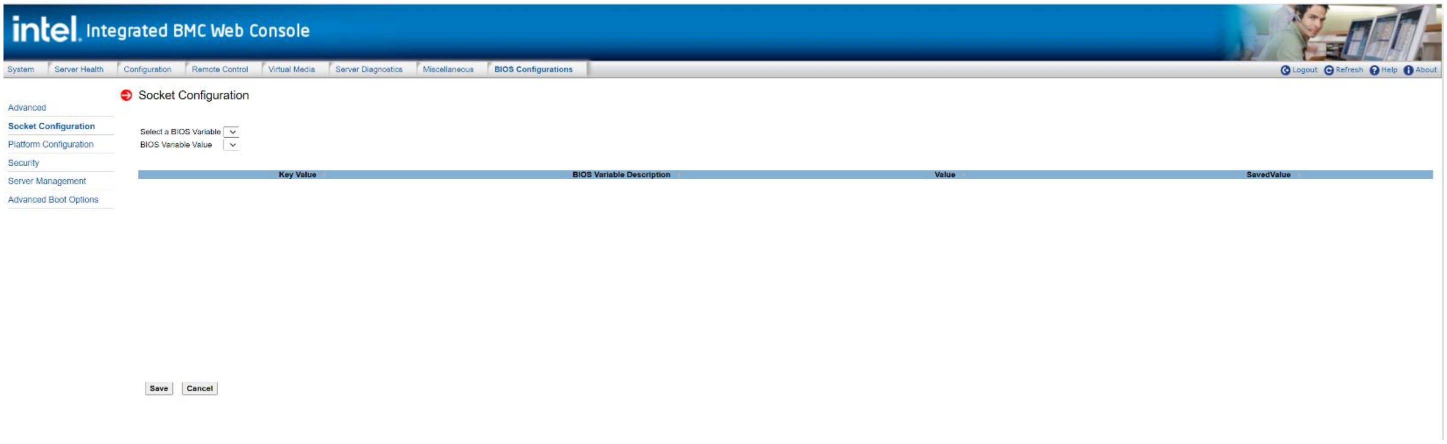


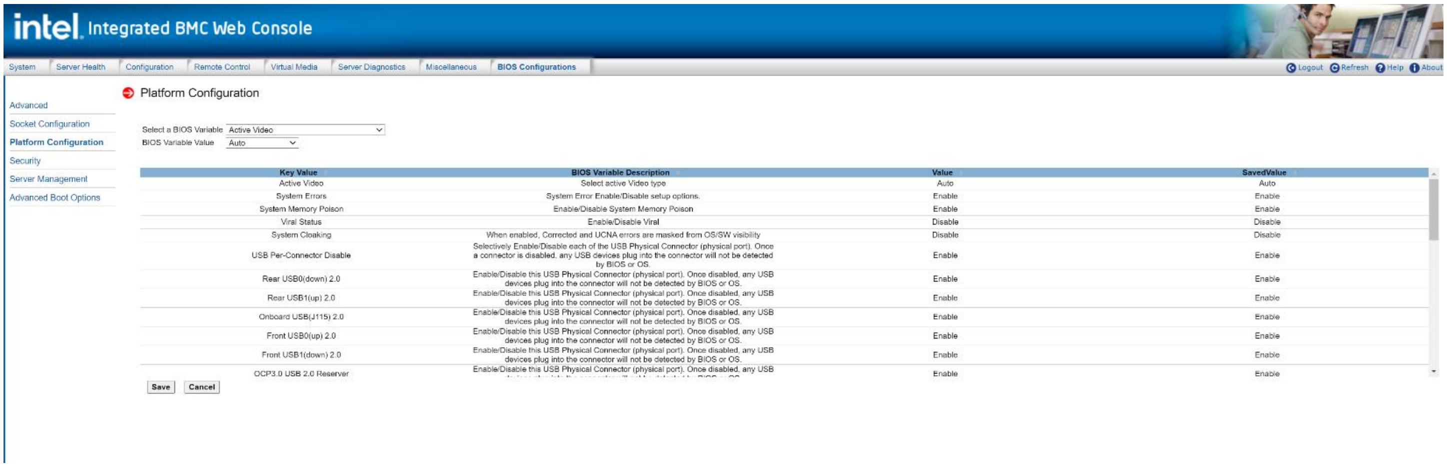
Figure 121. BIOS Socket Configuration Page

Table 31. BIOS Socket Configuration Variables

Variables	BIOS Variable Description
Select a BIOS Variable	Select a BIOS variable from the drop-down menu.
BIOS Variable Value	Once a BIOS variable is selected using the above-mentioned option (Select a BIOS Variable), the corresponding current values are displayed in the drop-down box. Other available options for the corresponding BIOS Variable can be seen by clicking the drop-down box. If the value needs to be changed for the above variable, other available values can be selected from the drop-down box.
Key Value	Selected BIOS Variable Value.
BIOS Variable Description	BIOS Variable Value corresponds to configure parameter value.
Value	Current selected BIOS Variable Value.
Save Value	Saved parameter value in the system.
Save	Click to save any changes made.
Cancel	Click to discard changes.

7.9.3 Platform Configuration

This page allows the user to change the configuration for PCH, PFR, Intel® ME. See Figure 122 for details. Table 31 and Table 32 list all the USB configuration variables that can be viewed and edited.



Platform Configuration

Select a BIOS Variable: Active Video

BIOS Variable Value: Auto

Key Value	BIOS Variable Description	Value	SavedValue
Active Video	Select active Video type	Auto	Auto
System Errors	System Error Enable/Disable setup options.	Enable	Enable
System Memory Poison	Enable/Disable System Memory Poison	Enable	Enable
Viral Status	Enable/Disable Viral	Disable	Disable
System Cloaking	When enabled, Corrected and UCNA errors are masked from OS/SW visibility	Disable	Disable
USB Per-Connector Disable	Selectively Enable/Disable each of the USB Physical Connector (physical port). Once a connector is disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	Enable	Enable
Rear USB0(down) 2.0	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	Enable	Enable
Rear USB1(up) 2.0	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	Enable	Enable
Onboard USB(J115) 2.0	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	Enable	Enable
Front USB0(up) 2.0	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	Enable	Enable
Front USB1(down) 2.0	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB devices plug into the connector will not be detected by BIOS or OS.	Enable	Enable
OCP3.0 USB 2.0 Reserver	Enable/Disable this USB Physical Connector (physical port). Once disabled, any USB	Enable	Enable

Figure 122. BIOS Platform Configuration Page

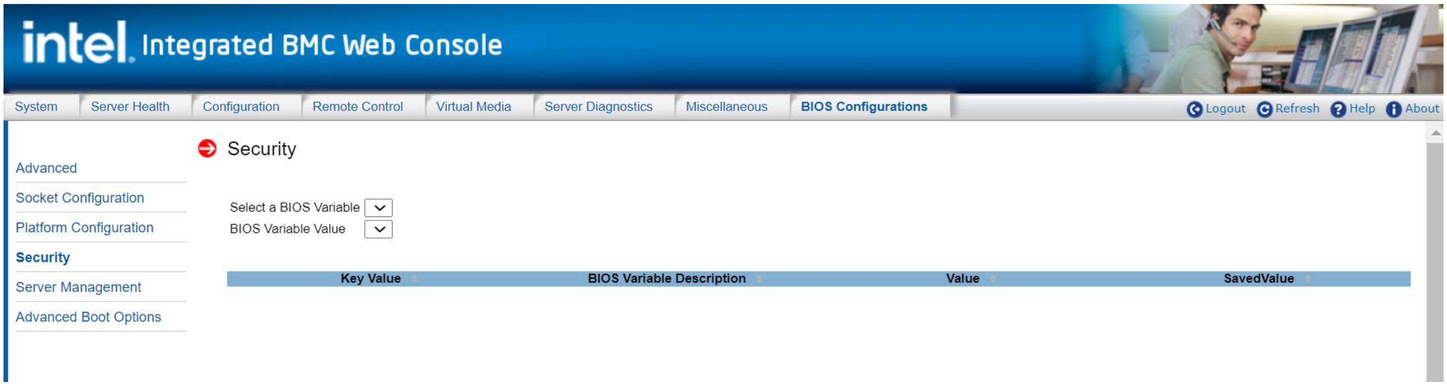
Table 32. BIOS Platform Configuration Variables

Variables	BIOS Variable Description
Active Video	Select active Video type.
System Errors	System Error Enable/Disable setup options.
System Memory Poison	Enable/Disable System Memory Poison.
Viral Status	Enable/Disable Viral.
System Cloaking	When enabled, Corrected and UCNA errors are masked from operating system or software visibility.
USB Per-Connector Disable	Selectively Enable/Disable each of the USB Physical Connector (physical port). **Note:** Once a connector is disabled, no USB devices plug into the connector is detected by BIOS or operating system.
Rear USB0(down) 2.0	Enable/Disable the corresponding USB Physical Connector (physical port). **Note:** Once disabled, no USB devices plug into the connector is detected by BIOS or the operating system.
Rear USB1(up) 2.0	
Onboard USB(J115) 2.0	
Front USB0(up) 2.0	
Front USB1(down) 2.0	
OCP3.0 USB 2.0 Reserver	
Connect to TF Card USB 2.0	
Connect to BMC USB 2.0	
Rear USB0(down) 3.0	
Rear USB1(up) 3.0	
Onboard USB(J115) 3.0	
Front USB0(up) 3.0	
SATA Controller	Enable/Disable the SATA Controller.
Configure SATA as	Identify if the SATA port is connected to Solid State Drive or Hard Disk Drive.
sSATA Controller	Enable/Disable SATA Controller.
Configure sSATA as	Identify if the SATA port is connected to Solid State Drive or Hard Disk Drive.
Ignore OS EMCA Opt-in	Enable/Disable Ignore OS EMCA Opt-in and log.
EMCA CMCI-SMI Morphing	Enable/Disable EMCA CSMI.
EMCA MCE-SMI Enable	Enable/Disable EMCA Uncorrected SMI for gen2.
WHEA Support	Enable/Disable WHEA support.
Memory Error	Enable/Disable Memory Error.

Variables	BIOS Variable Description
Memory Corrected Error	Enable/Disable Memory Corrected Error.
IIO/PCH Global Error Support	Enable/Disable IIO/PCH Error Support.
IIO Coherent Interface Error	Enable/Disable IIO Coherent Interface Error.
IIO Misc. Error	Enable/Disable IIO Misc. Error.
IIO Vtd Error	Enable/Disable IIO Vtd Error.
IIO Dma Error	Enable/Disable IIO Dma Error.
IIO Dmi Error	Enable/Disable IIO Dmi Error.
PCIE Error	Enable/Disable PCIe* Error.
IIO PCIE Additional Corrected Error	Enable/Disable IIO PCIe* Additional Corrected Error.
IIO PCIE Additional Uncorrected Error	Enable/Disable IIO PCIe* Additional Uncorrected Error.
PCIE Corrected Error Threshold Counter	Enable/Disable PCIe* Corrected Error Counter.
PCIE AER Corrected Errors	Enable/Disable PCIe* AER Corrected Errors.
PCIE AER Non Fatal Error	Enable/Disable PCIe* AER Non Fatal Error.
PCIE AER Fatal Error	Enable/Disable PCIe* AER Fatal Error.
PCIE AER Advisory Nonfatal Error	Enable/Disable PCIe* AER Advisory Nonfatal Error.
Save	Click to save any changes made.
Cancel	Click to discard changes.

7.9.4 Security

The Security page allows the user to configure BIOS security variables, such as power-on password, TPM, and others. See Figure 123 for details. Table 33 lists all security variables that can be viewed and edited.



Security

Select a BIOS Variable

BIOS Variable Value

Key Value	BIOS Variable Description	Value	SavedValue

Figure 123. BIOS Security Page

Table 33. BIOS Security Variables

Variables	BIOS Variable Description
Select a BIOS Variable	Select a BIOS Variable from the drop-down menu.
BIOS Variable Value	Once a BIOS Variable is selected using above option (select a BIOS Variable), the corresponding current values are displayed in the drop-down box. Other available options for the corresponding BIOS Variable can be seen by clicking the drop-down box and if value needs to be changed for the above variable then, other available values can be selected from the dropdown box.
Key Value	Selected BIOS Variable Value.
BIOS Variable Description	BIOS Variable Value corresponds to configure parameter value.
Value	Current selected BIOS Variable Value.
Save Value	Saved parameter value in the system.
Save	Click to save any changes made.
Cancel	Click to discard changes.

7.9.5 Server Management

The page allows the user to configure server management features. See Figure 124 for details. Table 34 lists all the options that can be viewed and edited.

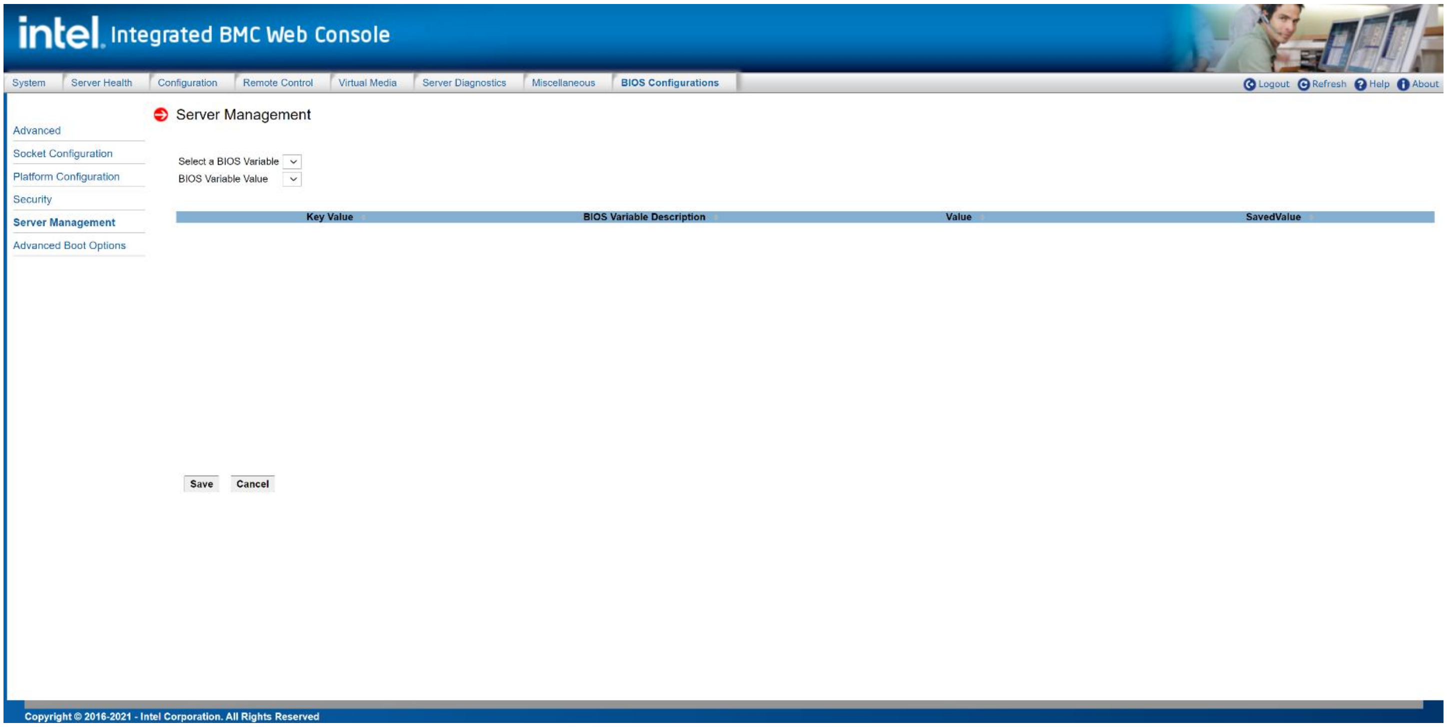


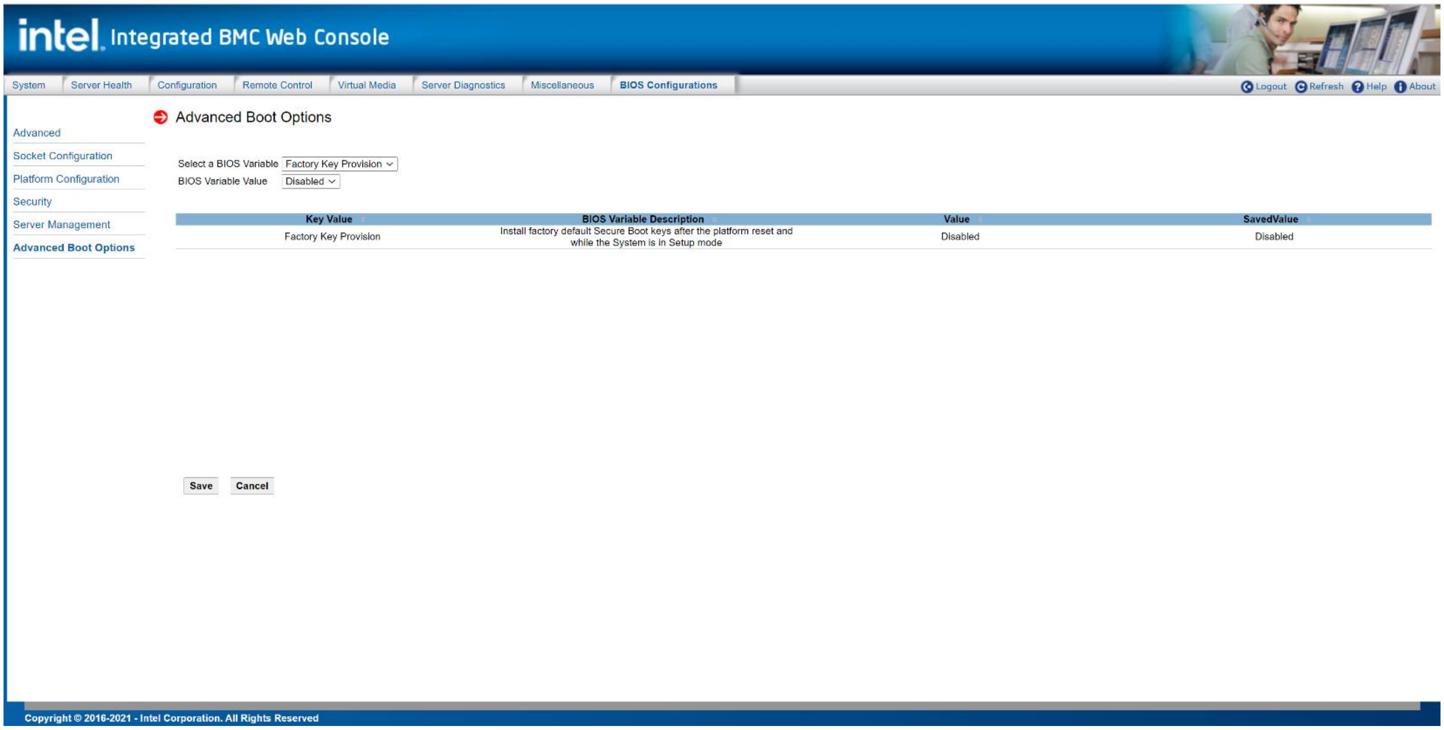
Figure 124. BIOS Server Management Page

Table 34. Server Management

Variables	BIOS Variable Description
Select a BIOS Variable	Select a BIOS Variable from the drop-down menu.
BIOS Variable Value	Once a BIOS Variable is selected using above option (Select a BIOS Variable), the corresponding current values are displayed in the drop-down box. Other available options for the corresponding BIOS Variable can be seen by clicking the drop-down box and if value needs to be changed for the above variable then, other available values can be selected from the dropdown box.
Key Value	Selected BIOS Variable Value.
BIOS Variable Description	BIOS Variable Value corresponds to configure parameter value.
Value	Current selected BIOS Variable Value.
Save Value	Saved parameter value in the system.
Save	Click to save any changes made.
Cancel	Click to discard changes.

7.9.6 Advanced Boot Options

The Advanced Boot Options page lets the user configure advanced boot options. See Figure 125 for details. Table 35 lists all the Advanced Boot Options that can be viewed and edited.



Advanced Boot Options

Select a BIOS Variable: Factory Key Provision

BIOS Variable Value: Disabled

Key Value	BIOS Variable Description	Value	SavedValue
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode	Disabled	Disabled

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved

Figure 125. BIOS Advanced Boot Options Page

Table 35. BIOS Advanced Boot

Variables	BIOS Variable Description
Select a BIOS Variable	Select a BIOS Variable from the drop-down menu.
Factory Key Provision	Install factory default Secure Boot keys after the platform reset and while the System is in Setup mode.
BIOS Variable Value	Once a BIOS Variable is selected using above option (Select a BIOS Variable), the corresponding current values are displayed in the drop-down box. Other available options for the corresponding BIOS Variable can be seen by clicking the drop-down box. If a value needs to be changed for the above variable, other available values can be selected from the drop-down box.
Key Value	Selected BIOS Variable Value.
BIOS Variable Description	BIOS Variable Value corresponds to configure parameter value.
Value	Current selected BIOS Variable Value.
Save Value	Saved parameter value in the system.
Save	Click to save any changes made.
Cancel	Click to discard changes.

Appendix A. Glossary

Term	Definition
AD*	Active Directory*
ARP	Address resolution protocol
BMC	Baseboard management controller
CPLD	Complex programmable logic device
CSM	Compatibility support module
DHCP	Dynamic host configuration protocol
DIMMs	Dual in-line memory modules
DNS	Domain name system
EFI	Extensible firmware interface
EMS	Emergency management services
FRU	Field replaceable unit
ICMP	Internet control message protocol
IDO	ID-based ordering
IMC	Integrated memory controller
IPMI	Intelligent platform management interface
KCS	Keyboard controller style
KVM	Keyboard, video, mouse
KVM-r	KVM-redirection
LAN	Local area network
LDAP	Lightweight directory address protocol
MAC	Media access controller
Intel® ME	Intel® Management Engine
MII	Media independent interface
NAT	Network address translation
NIC	Network interface controller
NTP	Network time protocol
Intel® NM	Intel® Node Manager
OOB	Out of Band – no operating system interaction on server
PCP	Priority code point
Intel® RMM	Intel® Remote Management Module
SDDC	Software defined data center
SDR	Sensor data record
SEL	System event log
SMM	System management mode
SMTP	Simple mail transfer protocol
SOL	Serial-over-LAN
Syscfg	System configuration utility
TCP/IP	Transmission control protocol/internet protocol
UDP	User datagram protocol
UEFI	Unified EFI
VLAN	Virtual local area network
KCS	Keyboard controller style