



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

User Guide

For the Intel® Server Board D50TNP, M50CYP, and D40AMP Families

Rev. 1.1

September 2021

<Blank page>

Revision History

Date	Revision	Changes
April 2021	1.0	Initial release.
September	1.1	<ul style="list-style-type: none">• Added Intel Server D40AMP family• Updated Figures 14, 41, 43, 66• Minor updates throughout for clarity

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.

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

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

© Intel Corporation

Table of Contents

1. Introduction	13
1.1 Support Information	13
1.2 Warranty Information	13
2. Advanced System Management Feature	14
2.1 Advanced Management Features Overview	14
2.1.1 Advanced Management Features Details	14
2.2 Supported Browsers	18
3. Installing the Advanced Management Key	19
3.1 How to Order Advanced System Management Key	19
3.1.1 Ordering as an Accessory (Not Via CTO)	19
3.2 Advanced Management Key Installation	21
3.2.1 Installation Procedure	21
4. Configuring Server Management Hardware	24
4.1 Configuring Server Management Hardware Using BIOS Setup	24
4.2 Configuring Server Management Hardware Using SYSCFG	26
4.2.1 Configuring the User	26
4.2.2 Configuring the IP Address	26
4.2.3 Configuring Serial Over LAN (SOL)	26
5. Getting Started with Advanced Management Feature Operation	27
5.1 Client Browsers	27
5.2 Logging In	27
5.3 Navigation	28
6. Remote Console (KVM) Operation	32
6.1 Launching the Redirection Console	32
6.2 Main Window	34
6.3 Remote Console Control Bar	34
6.3.1 Virtual Media Menu	34
6.3.2 Macro Menu	36
6.3.3 Options Menu	36
6.3.4 User List Menu	41
6.3.5 Capture Menu	41
6.3.6 Power Control Menu	42
6.3.7 Exit Menu	42
6.4 Remote Console Status Line	42
7. Integrated BMC Web Console Options	43
7.1 System Tab	43
7.1.1 System Information	43
7.1.2 Field Replaceable Unit (FRU) Information	44
7.1.3 CPU Information	45
7.1.4 DIMM Information	45

7.1.5	NVMe* Information.....	46
7.1.6	NIC Information.....	46
7.1.7	Storage Information.....	47
7.1.8	Current Users.....	47
7.2	Server Health Tab.....	48
7.2.1	Sensor Readings.....	48
7.2.2	Event Log.....	50
7.3	Configuration Tab.....	51
7.3.1	Alerts.....	51
7.3.2	Alert Email.....	52
7.3.3	Date & Time.....	53
7.3.4	IPv4 Network.....	54
7.3.5	IPv6 Network.....	56
7.3.6	VLAN Settings.....	58
7.3.7	LDAP Settings.....	59
7.3.8	Active Directory Settings.....	60
7.3.9	KVM & Media.....	61
7.3.10	SSL Certification.....	62
7.3.11	Advanced System Management Key.....	63
7.3.12	Users.....	64
7.3.13	Security Settings.....	66
7.3.14	SOL.....	70
7.3.15	SDR Configuration.....	71
7.3.16	BMC Firmware Update.....	72
7.3.17	BIOS/ME Firmware Update.....	73
7.3.18	CPLD Update.....	74
7.3.19	Syslog Server Configuration.....	75
7.4	Remote Control Tab.....	76
7.4.1	KVM/Console Redirection.....	76
7.4.2	Server Power Control.....	77
7.4.3	Launch SOL.....	78
7.4.4	Virtual Front Panel.....	79
7.4.5	iKVM over HTML5.....	79
7.5	Virtual Media Tab.....	82
7.6	Server Diagnostics Tab.....	83
7.6.1	System Diagnostics.....	83
7.6.2	POST Codes.....	84
7.6.3	System Defaults.....	84
7.6.4	SOL Log.....	85
7.7	Miscellaneous Tab.....	85
7.7.1	NM Configuration.....	85
7.7.2	Power Statistics.....	87

7.7.3	Power Telemetry	87
7.8	BIOS Configurations Tab.....	88
7.8.1	PCI Configuration	88
7.8.2	Serial Port Configuration	89
7.8.3	UPI Configuration.....	89
7.8.4	Integrated IIO Configuration.....	90
7.8.5	Memory Configuration	92
7.8.6	Power n Performance.....	93
7.8.7	Processor Configuration.....	94
7.8.8	Mass Storage Controller Configuration	97
7.8.9	System Acoustic and Performance Configuration	98
7.8.10	System Event Log.....	98
7.8.11	Security.....	99
7.8.12	USB Configuration	100
7.8.13	Server Management.....	100
7.8.14	Advanced Boot Options	102
7.8.15	Main.....	103
Appendix A.	Glossary	104

List of Figures

Figure 1. Example Email	19
Figure 2. Register Key	20
Figure 3. Activate Key	20
Figure 4. Download Key.....	21
Figure 5. System Information Page.....	21
Figure 6. Advanced System Management Key Page	22
Figure 7. Syscfg to Upload Software Key	22
Figure 8. Syscfg to Check Advanced Management Key Status	23
Figure 9. BIOS Setup BMC LAN Configuration Screen.....	25
Figure 10. BIOS Setup User Configuration Screen.....	25
Figure 11. Integrated BMC Web Console Login Page	28
Figure 12. Integrated BMC Web Console Homepage	28
Figure 13. Logging Out of the Integrated BMC Web Console	30
Figure 14. Integrated BMC Web Console Help	31
Figure 15. Remote Control Console Redirection Page.....	32
Figure 16. Remote Console Window.....	33
Figure 17. Remote Console Main Window.....	34
Figure 18. Remote Console Control Bar	34
Figure 19. Remote Console Virtual Media Menu.....	34
Figure 20. Remote Console Virtual Storage Menu	35
Figure 21. Remote Console Virtual Keyboard Menu	35
Figure 22. Remote Console Macro Menu	36
Figure 23. Remote Console Options Menu	36
Figure 24. Remote Console HotKey Settings.....	37
Figure 25. Remote Console Display Settings.....	37
Figure 26. Remote Console Input Settings.....	38
Figure 27. Remote Console Window Settings.....	38
Figure 28. Remote Console Video Stream Settings.....	38
Figure 29. Remote Console Session Timeout Settings	39
Figure 30. Remote Console Debug Log Settings	39
Figure 31. Remote Console Control Panel – OSD UI Style	40
Figure 32. Remote Console User List.....	41
Figure 33. Remote Console Capture Menu	41
Figure 34. Remote Console Power Control Menu	42
Figure 35. Exit the Remote Console	42
Figure 36. Remote Console Status Line.....	42
Figure 37. Busy Indicator Bar	43
Figure 38. System Information Page.....	43
Figure 39. FRU Board Options	44
Figure 40. System FRU Information Page	44

Figure 41. System CPU Information Page.....	45
Figure 42. System DIMM Information Page.....	45
Figure 43. System NVMe* Information Page	46
Figure 44. System NIC Information Page	46
Figure 45. System Storage Information Page.....	47
Figure 46. System Current Users page.....	47
Figure 47. Server Health Sensor Readings Page (Thresholds Not Displayed).....	48
Figure 48. Server Health Sensor Readings Page (Thresholds Displayed)	49
Figure 49. Server Health Event Log Page.....	50
Figure 50. Alerts Page	51
Figure 51. Alert Email Page	52
Figure 52. Date & Time Page	53
Figure 53. IPV4 Network DHCP Page	54
Figure 54. IPv4 Network Static Page	54
Figure 55. IPv6 Network Page.....	56
Figure 56. VLAN Settings Page	58
Figure 57. LDAP Settings Page	59
Figure 58. Active Directory Settings Page.....	60
Figure 59. KVM & Media Page	61
Figure 60. SSL Certification Page	62
Figure 61. Advanced System Management Key Page.....	63
Figure 62. User List Page.....	64
Figure 63. Add New User Page	64
Figure 64. Modify User Page.....	65
Figure 65. Delete User Page	65
Figure 66. Configuration Security Settings page	66
Figure 67. Server Power Control Page	68
Figure 68. BIOS/ME Firmware Update Page	68
Figure 69. BIOS Configuration Page.....	69
Figure 70. CPU Information Page	69
Figure 71. DIMM Information Page	70
Figure 72. SOL Page.....	70
Figure 73. SDR Configuration Page	71
Figure 74. BMC Firmware Update Page	72
Figure 75. BIOS/ME Firmware Update Page	73
Figure 76. CPLD Update Page.....	74
Figure 77. Syslog Server Configuration Page	75
Figure 78. Remote Control KVM Page.....	76
Figure 79. Remote Control Server Power Control Page	77
Figure 80. Remote Control Launch SOL Page.....	78
Figure 81: Remote Control Launch SOL Screen Page	78
Figure 82: Remote Control Virtual Front Panel Page	79

Figure 83. iKVM Over HTML5 Page.....	80
Figure 84: HTML5 Screen Page	80
Figure 85: HTML5 Virtual Keyboard Page.....	80
Figure 86: HTML5 Keyboard Macro menu page.....	81
Figure 87: HTML5 Power Control menu page.....	81
Figure 88. Virtual Media Over HTML5 Page	82
Figure 89. Launch Virtual Media Over HTML5 Page.....	82
Figure 90. Web ISO.....	82
Figure 91. Server System Diagnostics Page	83
Figure 92. Server Diagnostics POST Codes Page	84
Figure 93. Server Diagnostics Default Page	84
Figure 94. Server Diagnostics SOL Log Page.....	85
Figure 95. Intel® NM Configuration Page.....	85
Figure 96. Intel® NM Configuration Suspend Page	87
Figure 97. Power Statistics Page.....	87
Figure 98. Power Telemetry Page	87
Figure 99. Power Telemetry Device Categories.....	88
Figure 100. BIOS PCI Configuration Page	88
Figure 101. BIOS Serial Port Configuration Page	89
Figure 102. BIOS UPI Configuration Page.....	89
Figure 103. BIOS IIO Configuration Page	90
Figure 104. BIOS Memory Configuration Page	92
Figure 105. BIOS PnP Configuration Page.....	93
Figure 106. BIOS Processor Configuration Page	95
Figure 107. BIOS Mass Storage Controller Configuration Page.....	97
Figure 108. BIOS System Acoustic and Performance Configuration Page	98
Figure 109. System Event Log Page	98
Figure 110. BIOS Security Configuration Page	99
Figure 111. BIOS USB Configuration Page	100
Figure 112. BIOS Server Management Page.....	100
Figure 113. BIOS Advanced Boot Page.....	102
Figure 114. BIOS Main Page	103

List of Tables

Table 1. Integrated BMC Web Console Tabs.....	29
Table 2. Integrated BMC Web Console Toolbar.....	30
Table 3. Remote Console Log Level Definition.....	39
Table 4. Remote console OSD UI Style Control Bar Options.....	40
Table 5. Remote Console Power Control.....	42
Table 6. System Information Page Details.....	43
Table 7. Server Health Sensor Readings Options.....	49
Table 8. Server Health Event Log Options.....	50
Table 9. Alerts Options.....	51
Table 10. Alert Email Options.....	52
Table 11. Date & Time Options.....	53
Table 12. IPv4 Network Settings Options.....	55
Table 13. IPv6 Network Settings Options.....	57
Table 14. VLAN Settings Options.....	58
Table 15. LDAP Settings Options.....	59
Table 16. Active Directory Settings Options.....	60
Table 17. KVM & Media Options.....	61
Table 18. Advanced System Management Key Options.....	63
Table 19. Configuration Security Settings Options.....	66
Table 20. SOL Options.....	70
Table 21. SDR Configuration Options.....	71
Table 22. BMC Firmware Update Options.....	72
Table 23. BIOS/ME Firmware Update Options.....	73
Table 24. CPLD Update Options.....	74
Table 25. Syslog Server Configuration Options.....	75
Table 26. Macro Non-Printable Key Names.....	77
Table 27. Remote Control Power Control Options.....	77
Table 28. Remote Control Virtual Front Panel Options.....	79
Table 29. Server Diagnostics SOL Log Options.....	85
Table 30. Intel® NM Configuration Options.....	86
Table 31. BIOS Serial Port Configuration Variables.....	89
Table 32. BIOS UPI Configuration Variables.....	90
Table 33. BIOS IIO Configuration Variables.....	90
Table 34. BIOS Memory Configuration Variables.....	92
Table 35. BIOS PnP Configuration Variables.....	93
Table 36. BIOS Processor Configuration Variables.....	95
Table 37. BIOS Mass Storage Configuration Variables.....	97
Table 38. BIOS System Acoustic and Performance Configuration Variables.....	98
Table 39. BIOS Security Variables.....	99
Table 40. BIOS USB Configuration Variables.....	100

Table 41. Server Management	101
Table 42. BIOS Advanced Boot	102
Table 43. BIOS Main Configuration Variables	103

1. Introduction

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

The Integrated BMC Web Console provides both exceptional stability and permanent availability independent of the present state of the server's operating system. As a system administrator, use the Integrated BMC Web Console to gain location-independent remote access to respond to critical incidents and to undertake necessary maintenance.

From the Intel® Server D50TNP, M50CYP, and D40AMP 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

For support on the Integrated BMC Web Console, visit <https://www.intel.com/content/www/us/en/support.html>. This support page provides the following:

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

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

1.2 Warranty Information

To obtain warranty information, visit <https://www.intel.com/content/www/us/en/support/articles/000006361/services.html>.

2. Advanced System Management Feature

This section explains the advanced management features supported by the BMC firmware and highlights significance 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 D50TNP, M50CYP, and D40AMP families' products 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, which share network bandwidth with the host system, as well as the LAN channel provided by the onboard Intel® Dedicated Server Management NIC.

Standard with system and do not require a key:

- Virtual KVM over HTML5
- Integrated BMC Web Console
- Redfish* 2.0
- IPMI 2.0
 - Node Manager
- 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® Data Center Manager (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 helping you improve the efficiency and uptime. For more information, go to <https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html>
- Virtual Media Image Redirection (HTML5 and Java*)
- Virtual Media over network share and local folder
- Active Directory support
- ❖ Full system firmware update including drives, memory, and RAID (Available Q4 2021)
- ❖ Storage and network device monitoring (Available Q4 2021)
- ❖ Out-of-band hardware RAID Management for latest Intel® RAID cards (Available Q4 2021)

2.1.1 Advanced Management Features Details

Standard System Management Features

- 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. It is also possible to use the KVM-redirection (KVM-r) session concurrently with media-redirection (media-r). This feature allows a user to interactively use the keyboard, video, and mouse (KVM) functions of the remote server 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” is used to simulate an entire keyboard that is connected to the remote system. The “soft keyboard” functionality supports the following layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

The KVM-redirection feature automatically senses video resolution for best possible screen capture and provides high-performance mouse tracking and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS setup, once BIOS has initialized video.

- Integrated BMC Web Console

The BMC firmware has an embedded web server that can remotely serve web pages to any supported browser. This web console allows administrator to view system information including firmware versions, server health, diagnostic information, power statistics. It enables configuration of the BMC and BIOS. It provides the ability for users to perform power actions, launch KVM and set up virtual media redirection.

- Redfish*

The BMC supports several Redfish* schemas. The BMC currently supports version 1.7 and schema version 2019.1. DMTF's Redfish* is a standard designed to deliver simple and secure management for converged, hybrid IT and the Software Defined Data Center (SDDC). Both human readable and machine capable, Redfish* leverages 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 Dynamic Power Node Manager. IPMI defines a set of interfaces used by system administrators for out-of-band management of computer systems and monitoring of their operation.

- 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 Back plan firmware. The BMC update will happen immediately and cause a BMC reset to occur at the end. The BIOS and Intel ME firmware is staged in the BMC and will be updated on the next reboot. The BMC also supports Redfish* and embedded web console feature to view and modify BIOS settings. On each boot BIOS will provide all its settings and active value to the BMC to be displayed. It will also check if any changes are requested and perform 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, NVMe*, networking and storage. When applicable, the firmware version will also be provided.

- 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 SDPTool utilities. The debug log contains 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 2 boots. Finally, when the system has a catastrophic error condition leading to a system shutdown, the BMC will hold the CPU in reset long enough to collect processor machine check registers, memory controller machine check registers, I/O global error registers, and other processor state info.

- Security Features

The BMC contains several security features including OpenLDAP and Active Directory, 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 best practices security guide 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. BMC supports SNMP traps, email alerting (SMTP) and Redfish* event subscriptions.

Advanced System Management Features

- Software Key to enable features

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® Data Center Manager (Intel® DCM)

All systems that have the Advanced System Management Key uploaded can be managed by Intel® Data Center Manager for free. Intel® Data Center Manager comes with a 30 day trial. However, when the trial expires, all systems with this key can continue to be managed. Intel® DCM allows administrators to Manage and monitor the health, power, thermals, utilization, inventory and firmware versions of servers across your entire data center.

For more information on Intel® DCM, go to <https://www.intel.com/content/www/us/en/software/intel-dcm-product-detail.html?wapkw=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. When the user selects “Virtual Media over HTML5”, a new web page will be displayed which provides the user interface to select which type of source media (image file or file folder*) to mount, and then allows the user to select the desired media to make available to the server system. After the type and specific media are selected, the

interface provides a mount/unmount interface so the user can connect the media to or disconnect the media from the server system. Once connected, the selected image file or file folder is presented in the server system as standard removable media, and may be interacted with in the normal fashion based on the operating system running on the server system. This feature allows system administrators to install software (including operating system installation), copy files, perform firmware updates, etc., from media on their remote workstation.

Note: The file folder share is presented to the server system as a UDF file system; the server system operating system must be able to interact with UDF file systems for this feature to be used with the operating system.

- Virtual Media over network share

In addition to supporting virtual media redirection from the remote workstation, the BMC also 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 NFS shares. This virtual media redirection is more effective for mounting virtual media at scale, as 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 Active Directory. **Active Directory (AD)** is a **directory** service developed by Microsoft for Windows* domain networks. This feature allows users to login to the web console or Redfish* via an Active Directory username instead of local authentication. This allows administrators to only change passwords on this single domain account instead on every remote system.

- **Full system firmware update including drives, memory, and RAID

The BMC supports a staging area to allow customers to upload EFI utilities and supporting files, which will be silently executed by BIOS on the next reboot. Examples include firmware update for SSD, Network, RAID or other components that have EFI utilities. User can also use this to collect inventory data or configure advanced RAID options. Redfish* schemas support both the uploading and downloading of files. Intel® Server Debug and Provisioning Tool and Intel® Data Center Manager will use this region to perform multiple firmware update tasks.

- **Storage and network device monitoring

The BMC supports MCTP protocol that allows the monitoring of storage and networking devices. This includes asset inventory including firmware versions as well as link status and health.

- **Out-of-band hardware RAID Management

The BMC supports basic RAID management of latest generation Intel® RAID cards. The BMC will be able to see asset inventory of all drives behind RAID controllers, view RAID health and do basic RAID 0/1 configuration intended for boot virtual drives.

** Available post launch

2.2 Supported Browsers

Virtual KVM over HTML5 and Virtual Media over HTML5 features require browser to support the features of Websocket and HTML5.

The following browsers are tested:

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

3. Installing the Advanced Management Key

3.1 How to Order Advanced System Management Key

CTO/L9: If ordering a fully integrated system, select the AdvSysMgmtKey within the CTO portal and the Intel factory will automatically upload the license key during system integration

Accessory: If ordering as an individual accessory via WOM, follow the steps in chapter 3.1.1 to receive the license file and upload to the BMC.

3.1.1 Ordering as an Accessory (Not Via CTO)

1. Place the order via WOM like any other component
2. Receive an email with the product key
 - Depending on how it was ordered, may be forwarded from distributor or reseller
3. Click link on email to go to <https://lemcenter.intel.com> to register, activate and download the license file for that product key
 - Use existing Intel account or create a new one from the web site. Email address is required.
4. Use the BMC web console or Syscfg to upload the key to the BMC.
 - Only single license file per order is needed to activate multiple systems

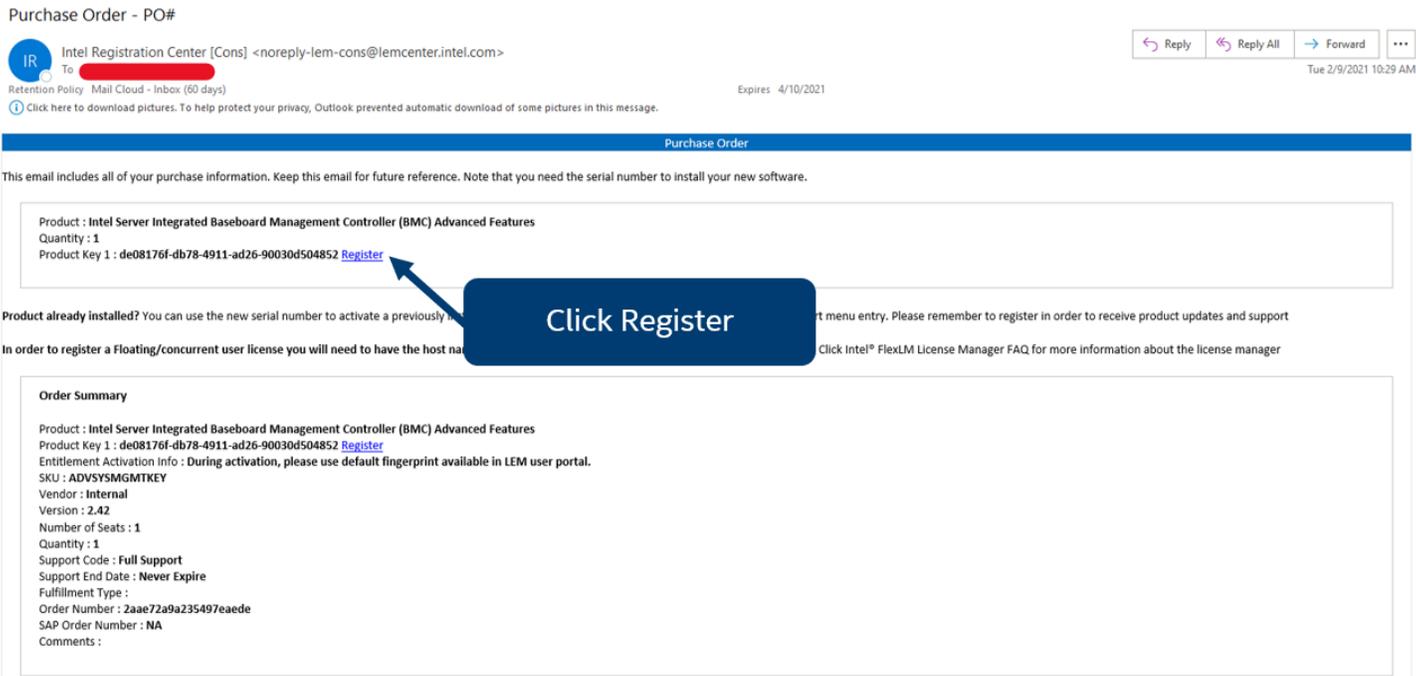


Figure 1. Example Email

Intel® Integrated BMC Web Console User Guide

The screenshot shows the Intel Registration Center User Portal. At the top, there is a navigation bar with 'PRODUCTS', 'SUPPORT', 'SOLUTIONS', 'DEVELOPERS', and 'PARTNERS'. Below this is a blue header with 'INTEL REGISTRATION CENTER - USER PORTAL'. The main content area is titled 'My Entitlements' and features a search bar with 'Use EID' and a 'Register' button. A table lists various product keys with columns for Product Key (SN), Product Name, Product Version, Registered Date, Support Expiration Date, and Action. A callout box with a blue background and white text points to the 'Register' button, stating 'Key automatically filled in. Click 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	
> VF7S-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-Z75GGW3P	Intel® Graphics Performance Analyzers	2012	07/10/2012	07/09/2013	
> C4LN-24ZGJL5	Intel® Graphics Performance Analyzers	2012	04/19/2012	04/18/2013	
> CCH7-FM677DSX	Cryptography for Intel® Parallel Composer	2011	04/19/2012		
> CCH7-WL7BNCB6	Cryptography for Intel® Parallel Composer	2011	04/19/2012		
> CCH7-GGDSH86L	Cryptography for Intel® Parallel Composer	2011	04/19/2012		
> C4LN-V3P58HJC	Intel® Graphics Performance Analyzers	2012	04/19/2012	04/18/2013	
> C4LN-PF573732	Intel® Graphics Performance Analyzers	2012	04/19/2012	04/18/2013	

Figure 2. Register Key

The screenshot shows the Intel Registration Center User Portal. At the top, there is a navigation bar with 'PRODUCTS', 'SUPPORT', 'SOLUTIONS', 'DEVELOPERS', and 'PARTNERS'. Below this is a blue header with 'INTEL REGISTRATION CENTER - USER PORTAL'. The main content area is titled 'My Entitlements' and features a search bar with 'Use EID' and a 'Register' button. A table lists various product keys with columns for Product Key (SN), Product Name, Product Version, Registered Date, Support Expiration Date, and Action. A callout box with a blue background and white text points to the 'Activate' button, stating 'Expand Product Key, scroll to bottom. Click Activate'.

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
> 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	

Figure 3. Activate Key

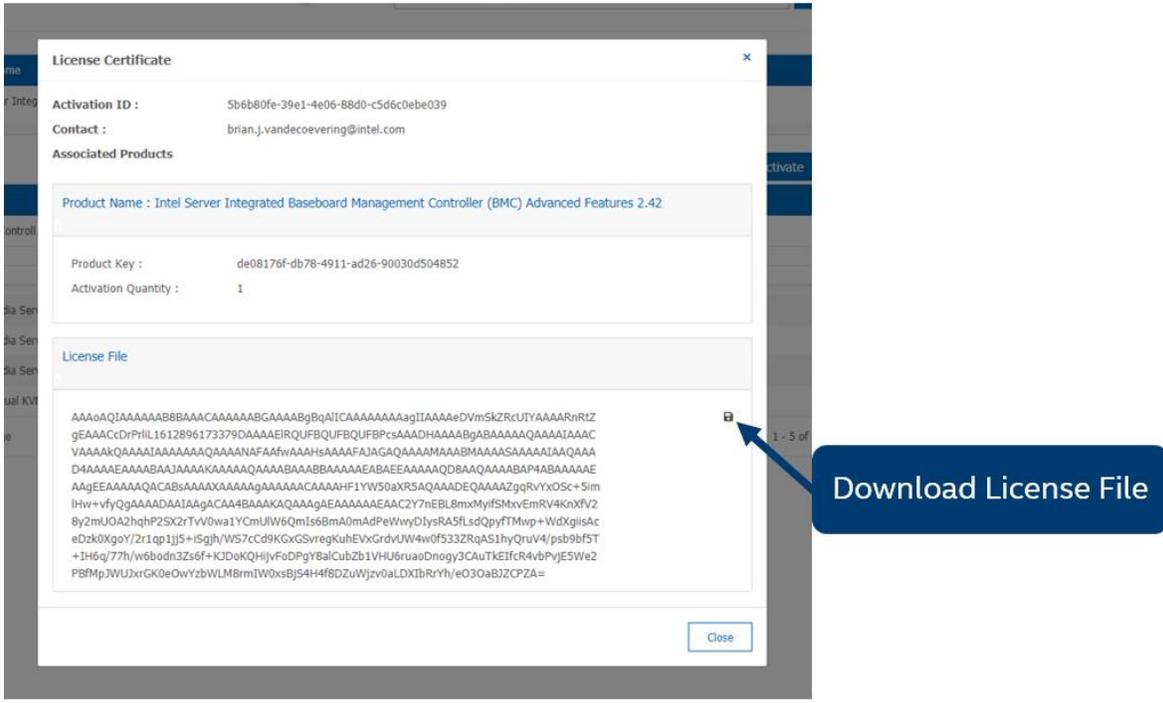


Figure 4. Download Key

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

3.2 Advanced Management Key Installation

There are 3 options (Intel® BMC Web Console, Syscfg, Redfish*) to upload the key.

3.2.1 Installation Procedure

Customer can navigate to *Advanced System Management Key* under *Configuration* to upload their key. All advanced features will be activated immediately after the key upload. The status of *Advanced System Key* is also displayed under *System Information* page.

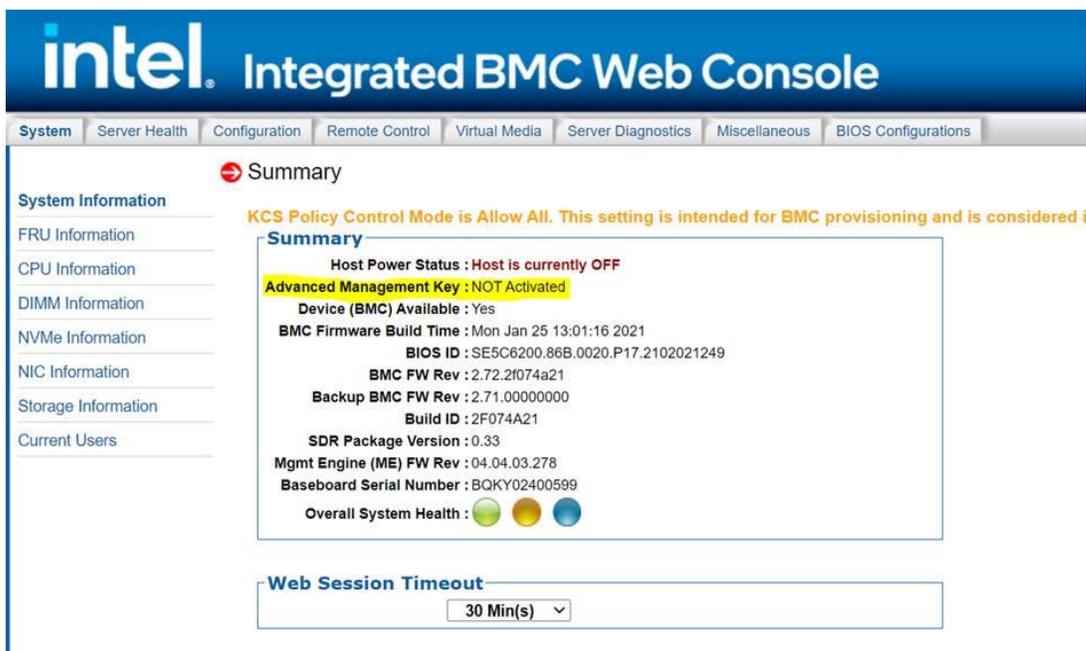


Figure 5. System Information Page

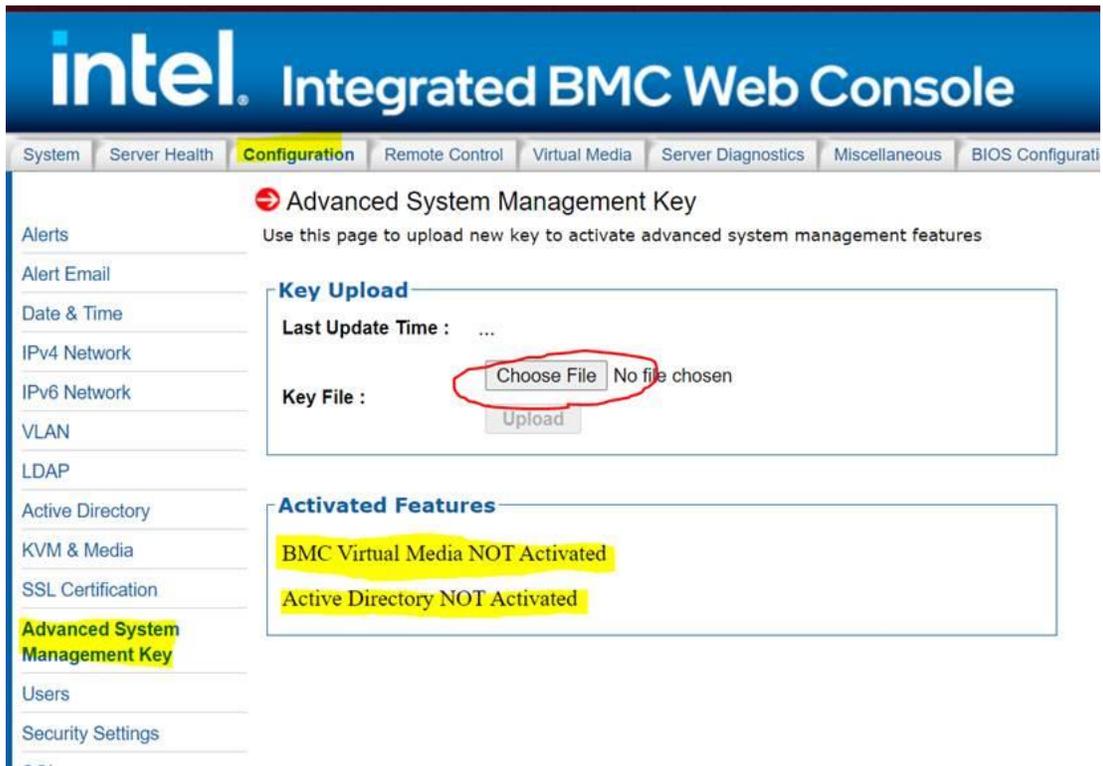


Figure 6. Advanced System Management Key Page

Upload Software Key to BMC via Syscfg example:

```
[root@localhost RHEL_Lib]# ./syscfg /lic AES_licenseFile.v2c

System Configuration Utility Version 14.2 Build 7
Copyright (c) 2020 Intel Corporation

Key Transfer...
Starting key upload...
Check and verify license: done
Program license file: done
Parsing license file: done
Upload ready
```

Figure 7. Syscfg to Upload Software Key

Optional Check Software Key Status via Syscfg:

```
[root@localhost RHEL_Lib]# ./syscfg /d lic  
  
Advanced Management Key Status  
  
Type: ASM key  
  
Active status: Activated  
  
Last upload: 02/05/2021-17:31:38  
  
[root@localhost RHEL_Lib]# █
```

Figure 8. Syscfg to Check Advanced Management Key Status

4. Configuring Server Management Hardware

This section discusses using the server utilities to enable a system to use the Integrated BMC Web Console from a new, unset state to an operational one.

When first powered on, by default, the server management BMC LAN has a static IP address of 172.16.10.10.

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

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

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 Configuring Server Management Hardware Using BIOS Setup

1. During POST, press <F2> to go to the BIOS setup main page.
2. Navigate to the **Server Management** tab and select **BMC LAN Configuration** to enter the BMC LAN Configuration screen (Figure 9).
3. For an IPv4 network:
 - If configuring the server management BMC LAN, scroll to **Baseboard LAN configuration > IP source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
 - If configuring the advanced management feature, scroll down to **Dedicated Management LAN Configuration > IP source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
4. For an IPv6 network:
 - If configuring the server management BMC LAN, scroll to **Baseboard LAN IPv6 configuration > IP source** and then select **Enabled**. Then scroll to **IPV6 source** and select either **Static** or **Dynamic**. If **Static** is selected, configure the **IPV6 address**, **Gateway IPV6**, and **IPV6 Prefix Length** as needed.
5. Select **User Configuration** to enter the User Configuration screen (Figure 10).
6. Under **User ID**, set the following settings as desired:
 - **Privilege** – Select the privilege to be used. (Administrator privilege is required to use KVM or media redirection enabled by the Advanced Management Feature.)
 - **User status** – Select **Enabled**.
 - **User name** – Enter the desired name. Note that the anonymous user cannot be changed.
 - **User password** – Enter the desired password twice.
7. Press <F10> to save the configured settings and exit BIOS setup. The server reboots with the new LAN settings.

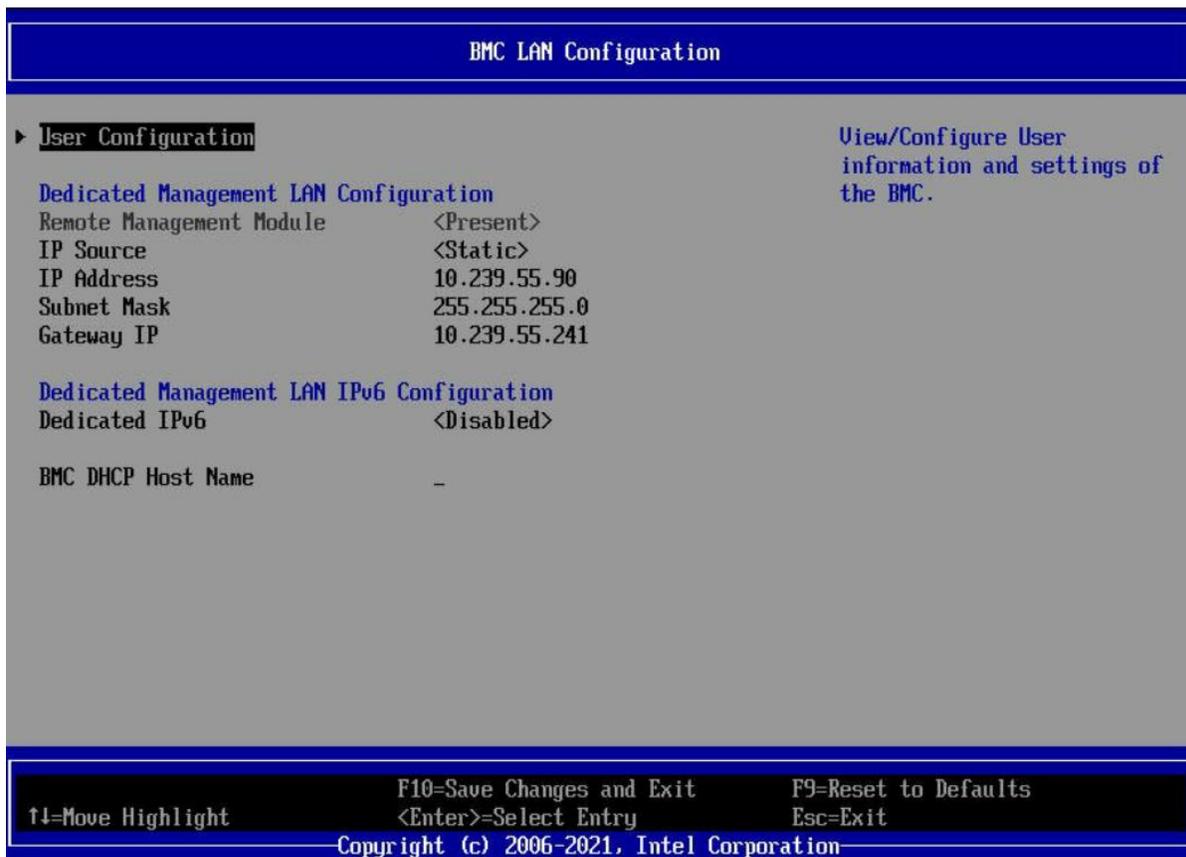


Figure 9. BIOS Setup BMC LAN Configuration Screen



Figure 10. BIOS Setup User Configuration Screen

4.2 Configuring Server Management Hardware 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 Configuring the User

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 Configuring the IP Address

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

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

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

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

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

```
syscfg /le 3 dhcp
```

4.2.3 Configuring Serial Over LAN (SOL)

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. Getting Started with Advanced Management Feature Operation

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

For initial setup information, including enabling the intended user, refer to Section 4. The examples in this chapter use user `root`, but other usernames and passwords could be used.

5.1 Client Browsers

The advanced management features may 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 cipher strength (encryption) of 256-bit. Some older browsers may not have a strong 128-bit encryption algorithm.

To use the remote console (KVM) window of the managed server, 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 web page.

5.2 Logging In

Enter the configured IP address the configured BMC onboard NIC into the web browser to open the Integrated BMC Web Console module login page (Figure 11). To use a secure connection, type:

```
https://<IPaddress_or_Hostname>/
```

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

- Username: `root`
- Password: `superuser`
- Language: **English**

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

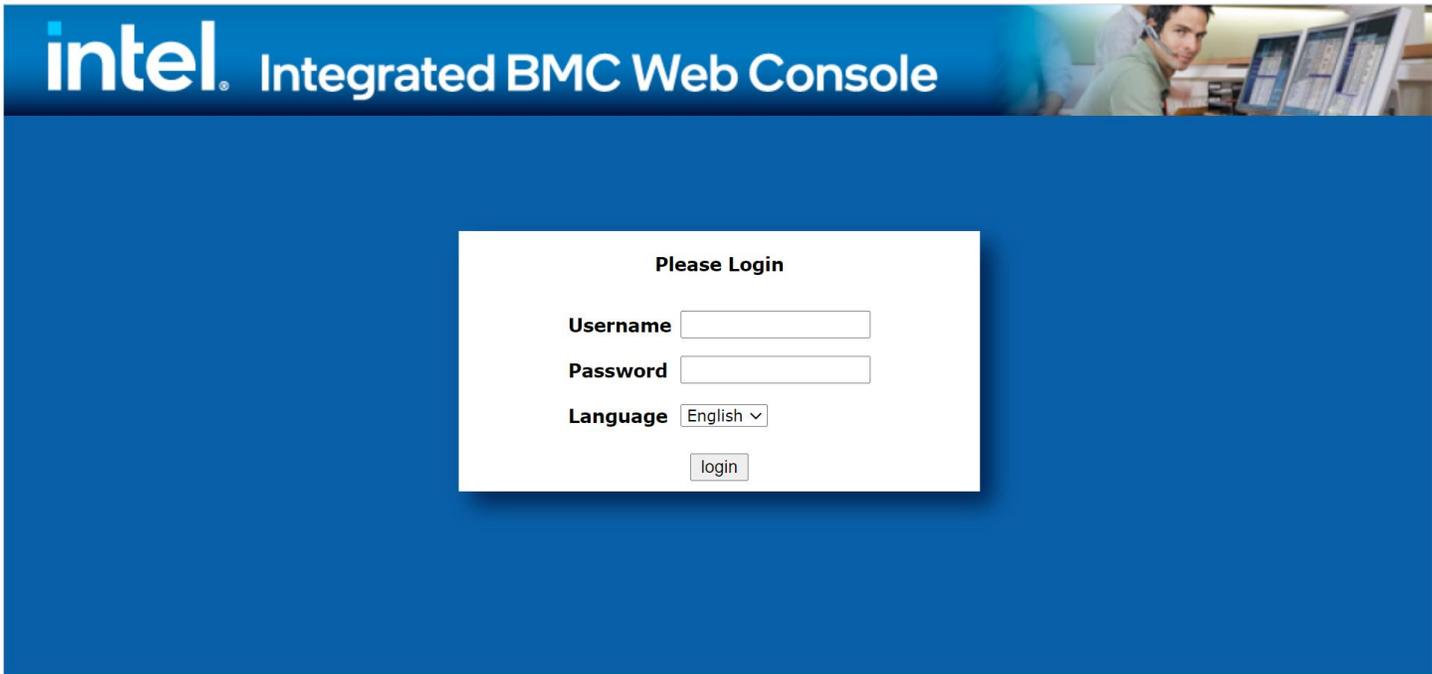


Figure 11. Integrated BMC Web Console Login Page

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

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

5.3 Navigation

The Integrated BMC Web Console homepage contains eight tabs along the top for navigation within the web console (Figure 12). For details on each tabbed page, see Table 1. Each tab contains a secondary browser on the left edge of the window. For details on the specific functions of secondary menu items, see Section 7.

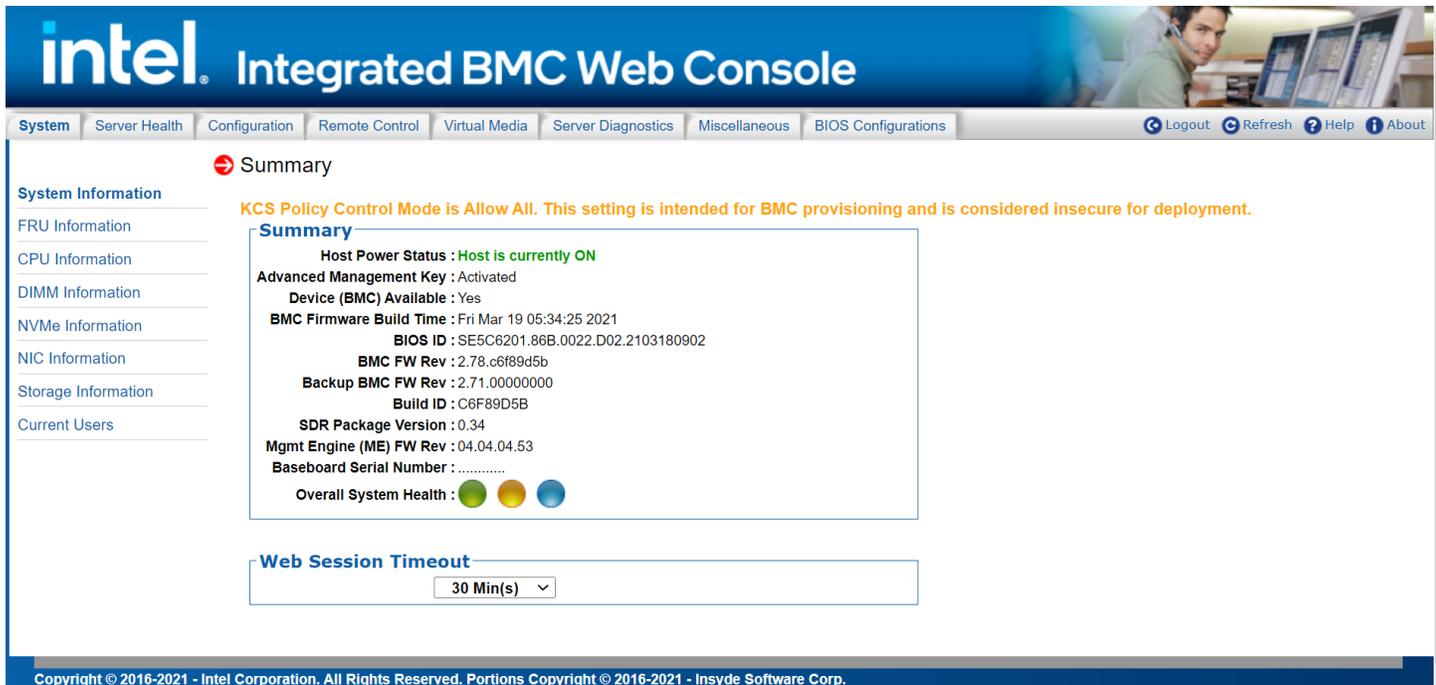


Figure 12. Integrated BMC Web Console Homepage

Table 1. 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.	<ul style="list-style-type: none"> • System Information • FRU Information • CPU Information • DIMM Information • NVMe* Information • NIC Information • Storage Information • Current Users
Server Health	Provides access to the sensors and event log. The tab automatically opens the Sensor Readings page.	<ul style="list-style-type: none"> • Sensor Readings • Event Log
Configuration	Provides access to configure various settings for the server. The tab automatically opens the Alerts page.	<ul style="list-style-type: none"> • Alerts • Alert Email • Date&Time • IPv4 Network • IPv6 Network • VLAN • LDAP • Active Directory • KVM & Media • SSL Certification • Advanced System Management Key • Users • Security Settings • SOL • SDR Configuration • BMC Firmware Update • BIOS/ME Firmware Update • CPLD Update • Syslog Server Configuration
Remote Control	Provides access to the remote console and control of the server power state. The tab automatically opens the KVM/Console Redirection page.	<ul style="list-style-type: none"> • KVM/Console Redirection • Server Power Control • Launch SOL • Virtual Front Panel • iKVM over HTML5
Virtual Media	Allows you to share an ISO image or folder over HTML5. Maximum size of ISO image is 4.7GB, and folder is 2GB. Each image/folder will be emulated to the host as a USB device. The tab automatically opens the Virtual Media over HTML5 page.	<ul style="list-style-type: none"> • Virtual Media over HTML5 • Web ISO
Server Diagnostics	Provides access to server diagnostics information. The tab automatically opens the System Diagnostics page.	<ul style="list-style-type: none"> • System Diagnostics • POST Codes • System Defaults • SOL Log
Miscellaneous	Provides access to node manager configuration, power statistics, and power telemetry. The tab automatically opens the NM Configuration page.	<ul style="list-style-type: none"> • NM Configuration • Power Statistics • Power Telemetry

Tab	Function	Secondary Menu
BIOS Configuration	Provides access to BIOS configuration. The tab automatically opens the NIC Configuration page.	<ul style="list-style-type: none"> • PCI Configuration • Serial Port Configuration • UPI Configuration • Integrated IO Configuration • Memory Configuration • Power n Performance • Processor Configuration • Mass Storage Controller Configuration • System Acoustic and Performance Configuration • System Event Log • Security • USB Configuration • Server Management • Advanced Boot Options • Main

In addition, the top of every page contains a toolbar with options explained in Table 2.

Table 2. Integrated BMC Web Console Toolbar

Button	Function
Logout	End the current web console session. Click OK to confirm (Figure 13). After logging out, the web console returns to the login screen.
Refresh	Refresh the current web page, including any data shown on the page. <hr/> Note: Using the web browser's refresh/reload button or pressing the function key <F5> to do a refresh/reload is not supported for reloading the web console pages. Using either of them returns the web console to the homepage. <hr/>
Help	View a brief description of the current page in a frame at the right side of the browser window (Figure 14). Close the help frame by clicking the "X" in the upper right corner of the frame or by clicking the Help button again.
About	View the Intel copyright information and a statement about the use of open source code.

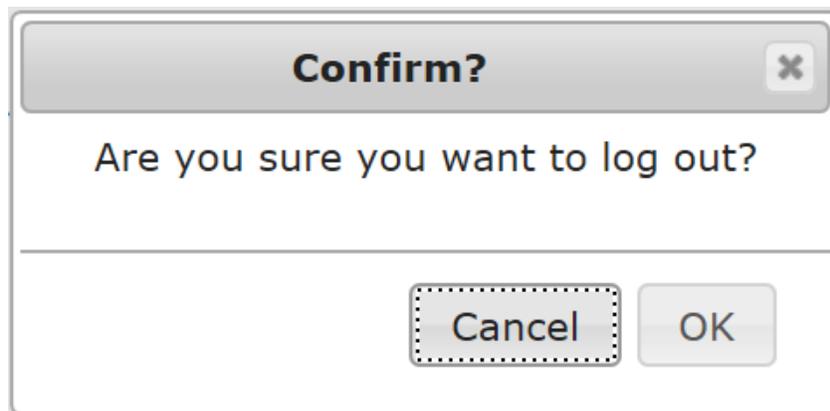


Figure 13. Logging Out of the Integrated BMC Web Console

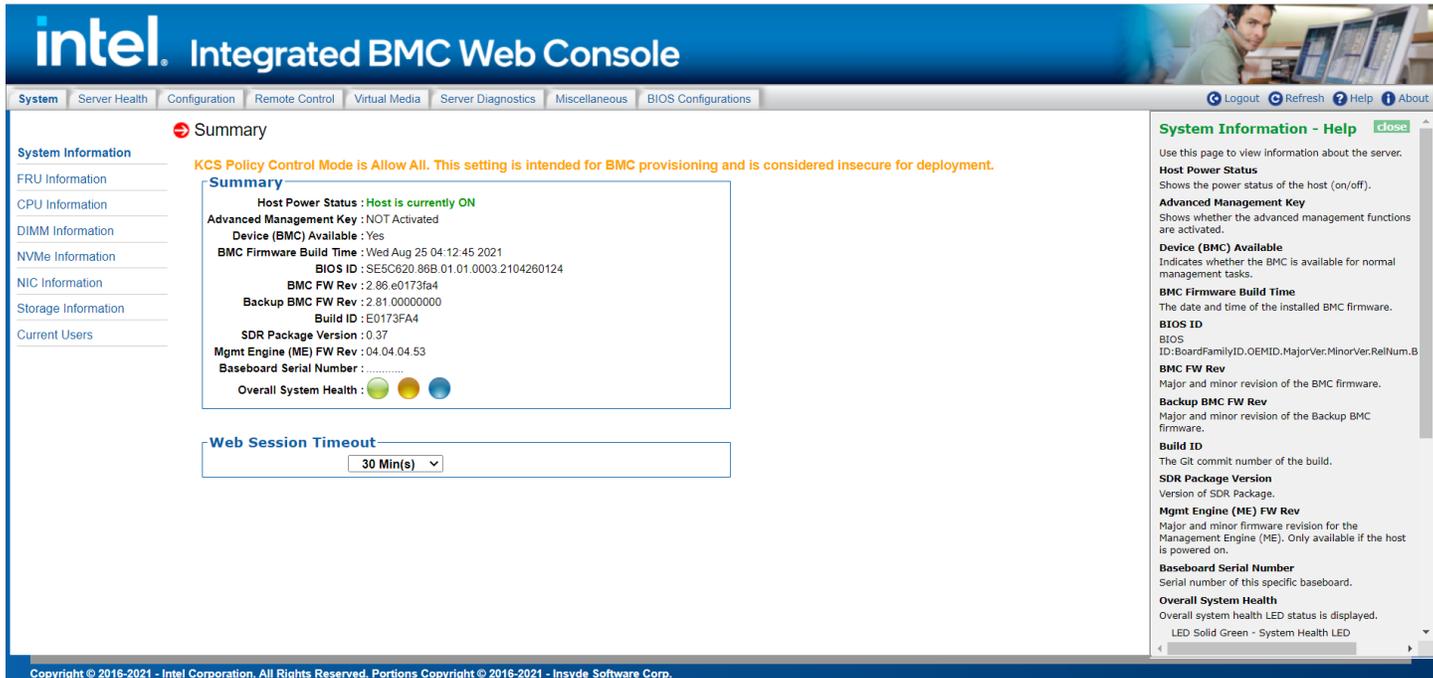


Figure 14. Integrated BMC Web Console Help

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 redirected keyboard, video, and mouse of the remote host system. To use the remote console window of the managed host system, 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 screen content of the host system. The remote console acts as if the administrator were sitting directly in front of the screen of the remote system. This means the keyboard and mouse can be used as usual.

6.1 Launching the Redirection Console

Launch the remote console KVM redirection window by clicking **Launch Console** from the Remote Control tab of the Integrated BMC Web Console (Figure 15).

Note: If you are using Microsoft Windows* Internet Explorer*, Smart Screen is enabled, and the system is on a network with no direct connectivity to the internet, it may take an extremely long time to open a KVM window.

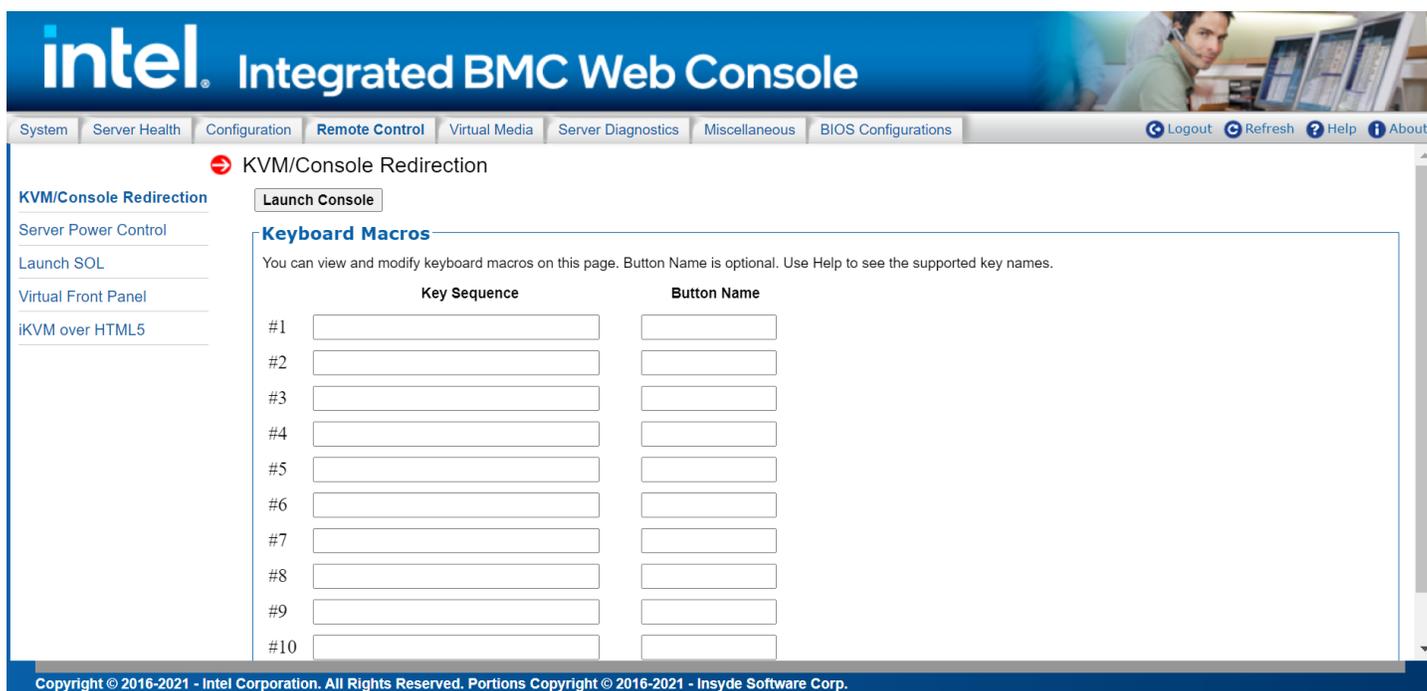


Figure 15. Remote Control Console Redirection Page

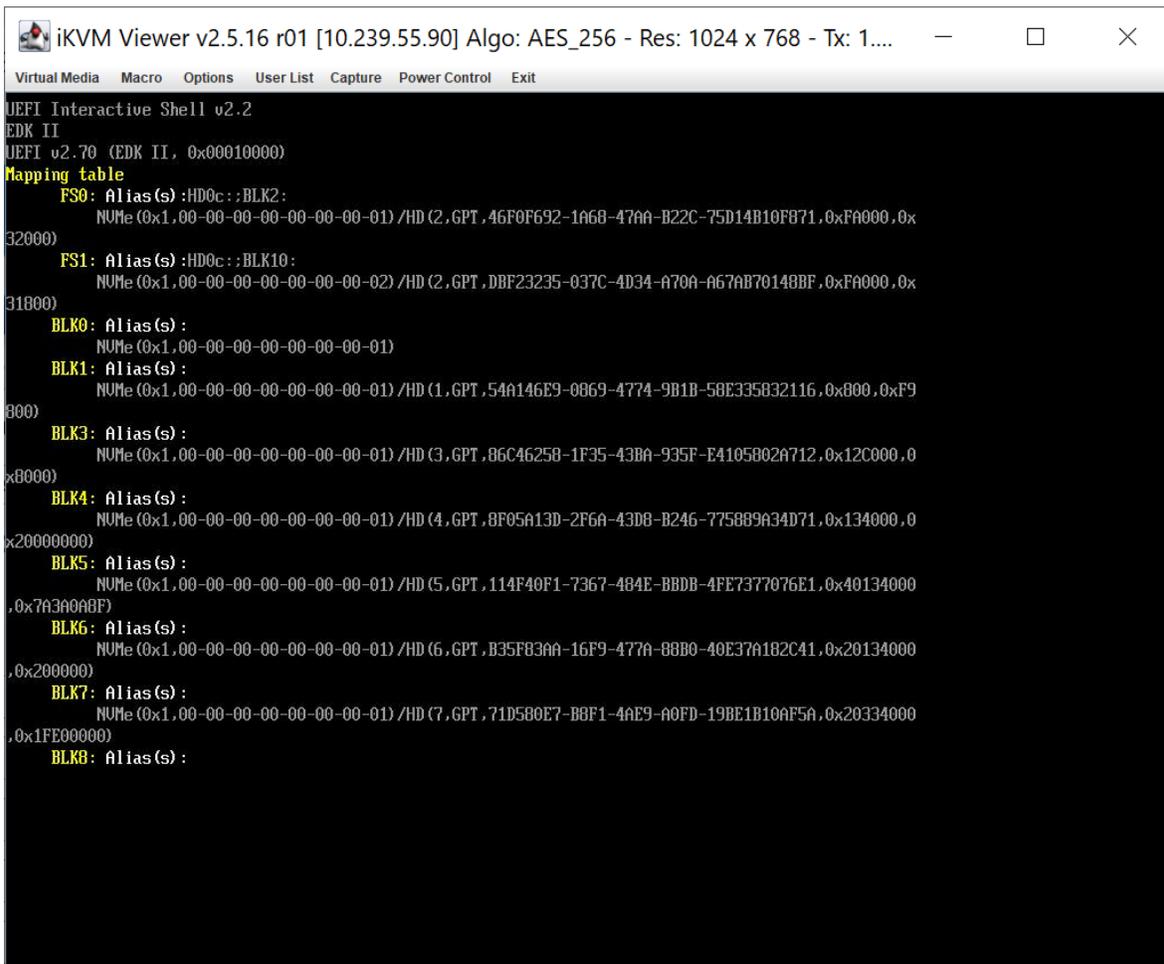
When the **Launch Console** button is clicked, a pop-up window is displayed to download the Java* Network Launch Protocol `launch.jnlp` file. This in turn downloads the standalone Java* application implementing the remote console.

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

Notes:

- Java* Runtime Environment* (JRE*, Version 6 Update 22 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 Integrated BMC Web Console IP address.
- JCE Unlimited Strength Jurisdiction Policy Files required by AES-256 need 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 Integrated BMC Web Console. The protocol that is used to run these connections is a unique KVM protocol and not HTTP or HTTPS. This protocol uses ports #5900 for KVM and #623 for Floppy/USB media redirection. 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.



```

iKVM Viewer v2.5.16 r01 [10.239.55.90] Algo: AES_256 - Res: 1024 x 768 - Tx: 1....
Virtual Media Macro Options User List Capture Power Control Exit
UEFI Interactive Shell v2.2
EDK II
UEFI v2.70 (EDK II, 0x00010000)
Mapping table
FS0: Alias(s) :HD0c::BLK2:
    NUMe (0x1,00-00-00-00-00-00-01) /HD (2.GPT,46F0F692-1A68-47AA-B22C-75D14B10F871,0xFA000,0x
32000)
FS1: Alias(s) :HD0c::BLK10:
    NUMe (0x1,00-00-00-00-00-00-02) /HD (2.GPT,DBF23235-037C-4D34-A70A-A67AB70148BF,0xFA000,0x
31800)
BLK0: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01)
BLK1: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01) /HD (1.GPT,54A146E9-0869-4774-9B1B-58E335832116,0x800,0xF9
800)
BLK3: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01) /HD (3.GPT,86C46258-1F35-43BA-935F-E4105802A712,0x12C000,0
x8000)
BLK4: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01) /HD (4.GPT,8F05A13D-2F6A-43D8-B246-775889A34D71,0x134000,0
x20000000)
BLK5: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01) /HD (5.GPT,114F40F1-7367-484E-BBDB-4FE7377076E1,0x40134000
,0x7A3A0A8F)
BLK6: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01) /HD (6.GPT,B35F83AA-16F9-477A-88B0-40E37A182C41,0x20134000
,0x200000)
BLK7: Alias(s) :
    NUMe (0x1,00-00-00-00-00-00-01) /HD (7.GPT,71D580E7-BBF1-4AE9-A0FD-19BE1B10AF5A,0x20334000
,0x1FE00000)
BLKB: Alias(s) :

```

Figure 16. Remote Console Window

6.2 Main Window

Starting the remote console opens a host window (Linux* operating system window shown in Figure 17).

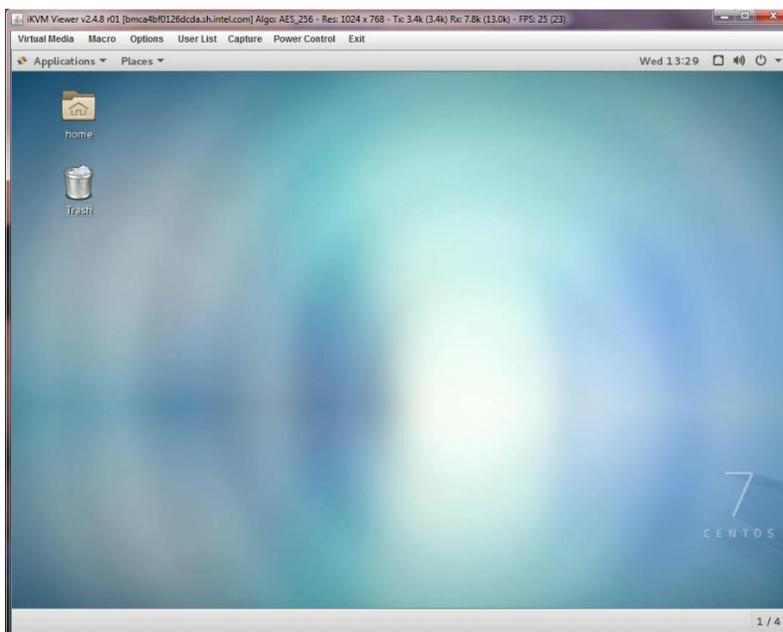


Figure 17. Remote Console Main Window

It displays the screen content of the remote server. The remote console responds as if it were located at the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between the Integrated BMC Web Console and the remote console. 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 size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, the remote console window can be resized in the local window as usual.

6.3 Remote Console Control Bar

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



Figure 18. Remote Console Control Bar

6.3.1 Virtual Media Menu

Click **Virtual Media** in the remote console control bar to open the virtual storage and virtual keyboard menu as shown in Figure 19.

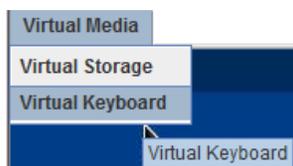


Figure 19. Remote Console Virtual Media Menu

Use the options in this menu to do the following:

- Virtual Storage** – Allow starting/stopping remote media redirection as shown in Figure 20. Redirect up to four devices at the same time. Select a logical device from a local CDROM/DVD drive or an ISO image on the local client file system as a virtual CDROM device on the remote system; a local floppy drive; a USB key drive; or a floppy disk or USB key image (. IMA/. IMG) file on the local client file system as a virtual floppy device on the remote system.

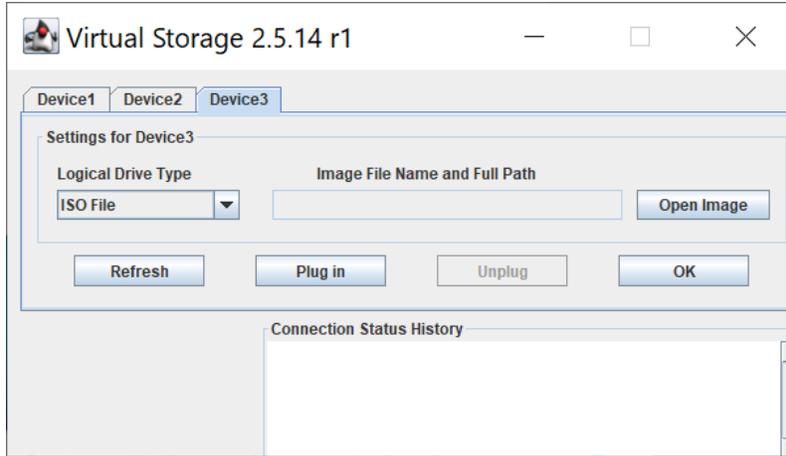


Figure 20. Remote Console Virtual Storage Menu

- Virtual Keyboard** – Display a soft keyboard as shown in Figure 21.



Figure 21. Remote Console Virtual Keyboard Menu

6.3.2 Macro Menu

Click **Macro** to open the keyboard macro menu as shown in Figure 22.

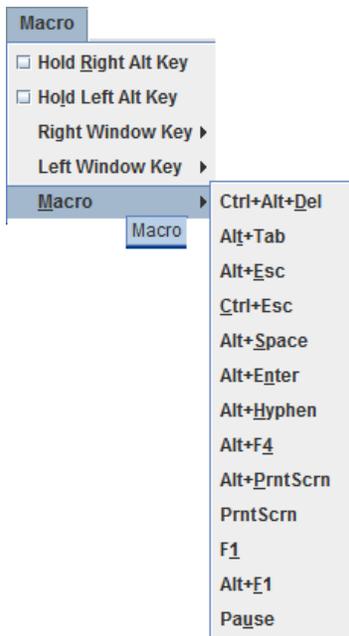


Figure 22: Remote Console Macro Menu

Using the options in this menu, to do the following:

- **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 OS and not passed on to the remote OS.
- **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 OS and not passed on to the remote OS.
- **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 OS and not passed on to the remote OS.
- **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 OS and not passed on to the remote OS.
- **Macro** – Simulate special key combinations to the remote OS, which include **<Ctrl+Alt+Del>**, **<Alt+Tab>**, **<Alt+Esc>**, **<Ctrl+Esc>**, **<Alt+Space>**, **<Alt+Enter>**, **<Alt+Hyphen>**, **<Alt+F4>**, **<Alt+Prntscrn>**, **<PrntScrn>**, **<F1>**, **<Alt+F1>**, **<Pause>**.

6.3.3 Options Menu

Click **Options** to open the options menu as shown in Figure 23.

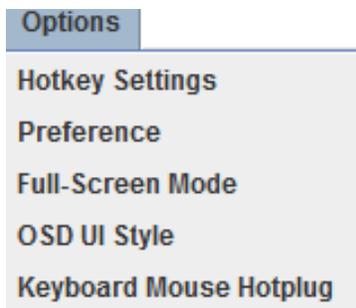


Figure 23. Remote Console Options Menu

Use the options in this menu, to do the following:

- **HotKey Settings** – Configure hotkeys as shown in Figure 24. Configure up to seven hotkeys to perform specific functions including adjust mouse, exit remote location, enter full-screen mode, refresh screen, send Ctrl+Alt+Del, toggle mouse display, and toggle UI display.

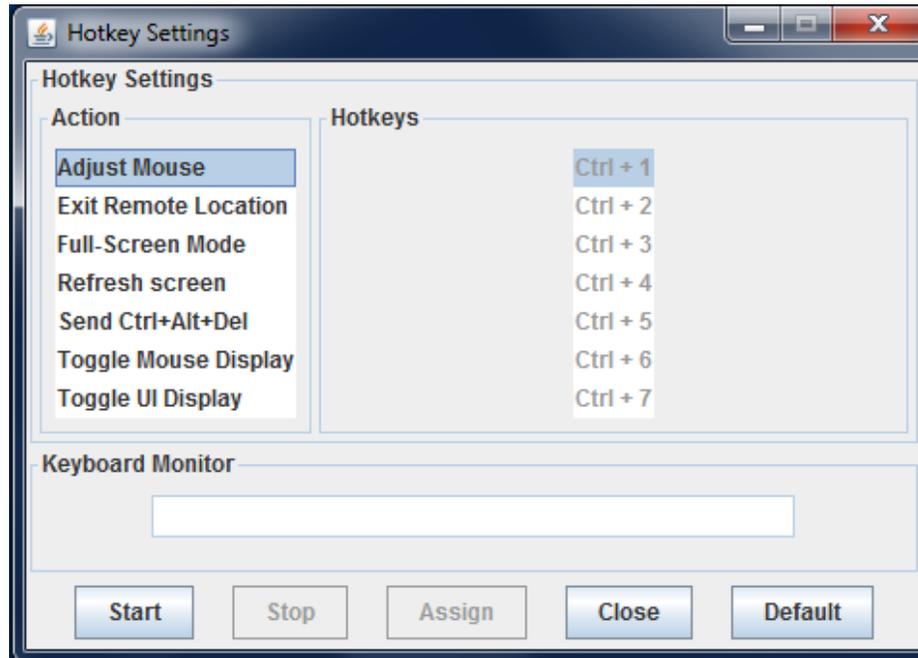


Figure 24. Remote Console HotKey Settings

- **Preference** – Configure the remote console display, mouse and keyboard settings, window, video stream, session timeout, and debug log level. The preference window toolbar has six tabs.
 - **Display** (Figure 25) – Adjust display brightness, image quality, display scale and compression mode and enable FPS control by specifying frames per second.

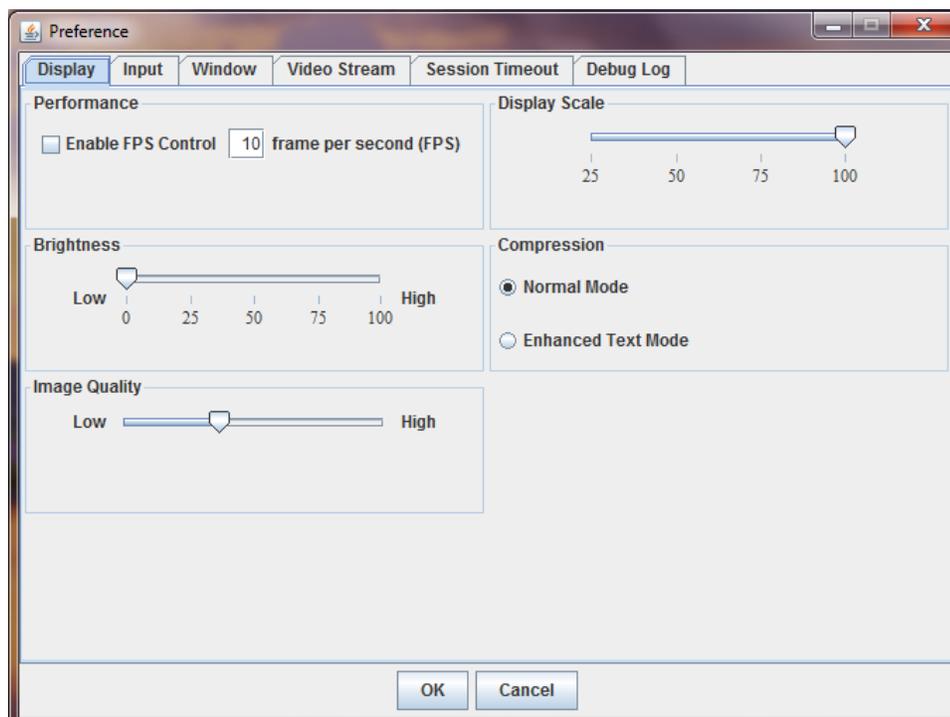


Figure 25. Remote Console Display Settings

- **Input** (Figure 26) – Enable/disable mouse/keyboard input, change the mouse mode, specify keyboard layout, and set repeat key timeout.

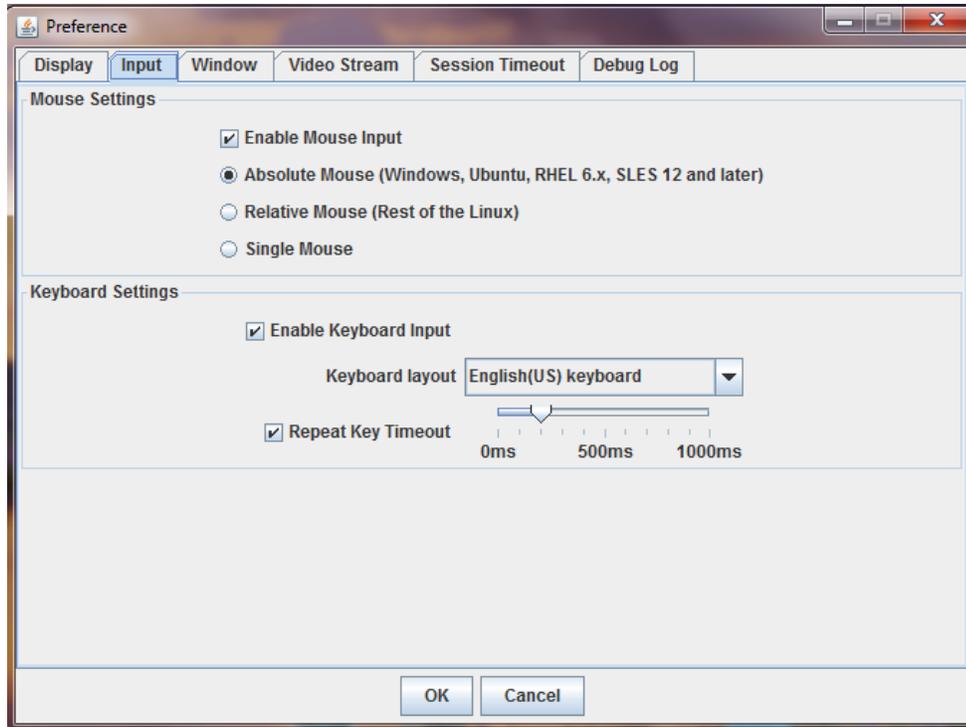


Figure 26. Remote Console Input Settings

- **Window** (Figure 27) – Enable or disable window auto-resize.

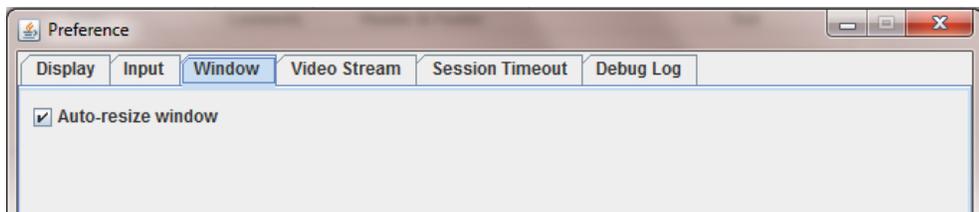


Figure 27. Remote Console Window Settings

- **Video Stream** (Figure 28) – Enable flow control by specifying a speed of T1, T2, or 256K Cable/DSL.

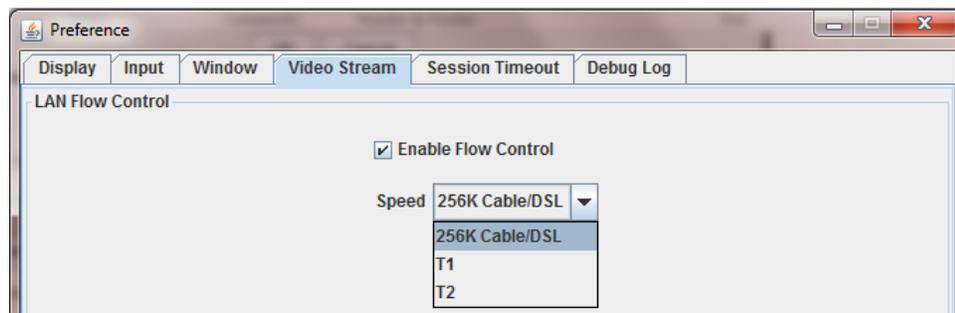


Figure 28. Remote Console Video Stream Settings

- **Session Timeout** (Figure 29) – Enable session timeout by specifying how many minutes for timeout.

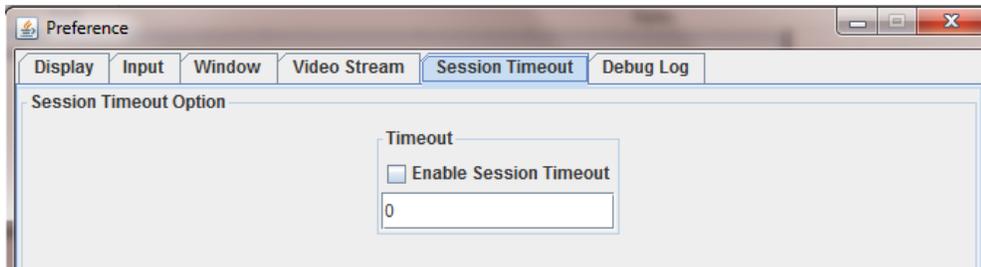


Figure 29. Remote Console Session Timeout Settings

- **Debug Log** (Figure 30) – Select a log level of Disabled, Emergency, Alert, Critical, Error, Warning, Notice, Info or Debug. Table 3 defines each log level. The debug level is only for Java* viewers and log messages will appear on the Java* console, if enabled.

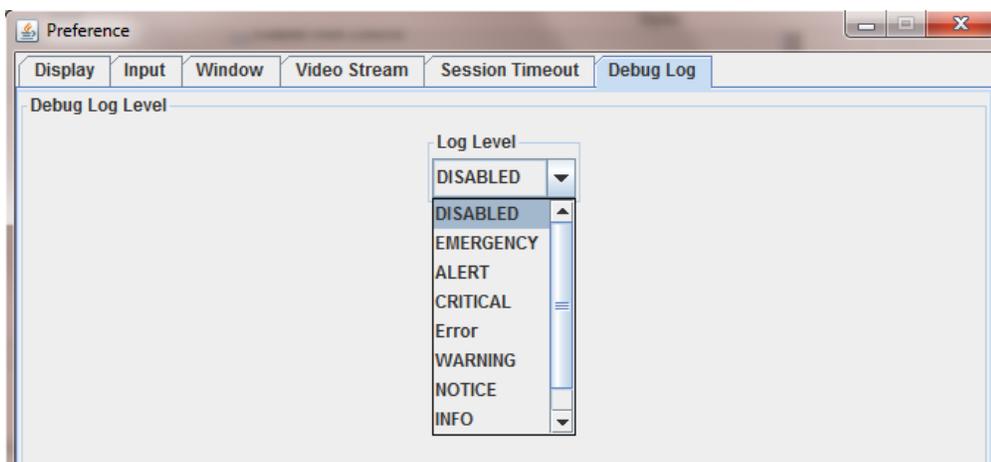


Figure 30. Remote Console Debug Log Settings

Table 3. Remote Console Log Level Definition

Log Level	Definition
Disabled	No debug log.
Emergency	Emergency conditions, such as system hangs, will save to the debug log.
Alert	Alert conditions such as system database corruption will save to debug log.
Critical	Critical conditions such as hard device errors.
Error	Error conditions.
Warning	Warning conditions.
Notice	Normal but significant conditions that are not error conditions.
Info	Informational messages.
Debug	Debug-level messages. Messages that contain information normally of use only when debugging a program.

- **Full-Screen Mode/Leave Full Screen Mode** – Enter or leave full screen mode (depending on the current state).

- **OSD UI Style** – Change the style of the remote console control bar as shown in Figure 31. Clicking the icons on this window performs tasks as shown in Table 4.



Figure 31. Remote Console Control Panel – OSD UI Style

Table 4. Remote console OSD UI Style Control Bar Options

Menu Icon	Function
	Move OSD UI menu
	Hotkey Settings
	Virtual Storage
	Virtual Keyboard
	Preference menu
	Full-screen mode
	Exit
	Show User List
	Switch back to menu UI mode
	Keyboard Mouse Hotplug
	Macro menu
	Power Control menu

- **Keyboard Mouse Hotplug** – Simulate remote console virtual USB keyboard/mouse unplug then plug.

6.3.4 User List Menu

Click **Show User List** to display information about connected users such as user name and client IP address (Figure 32).

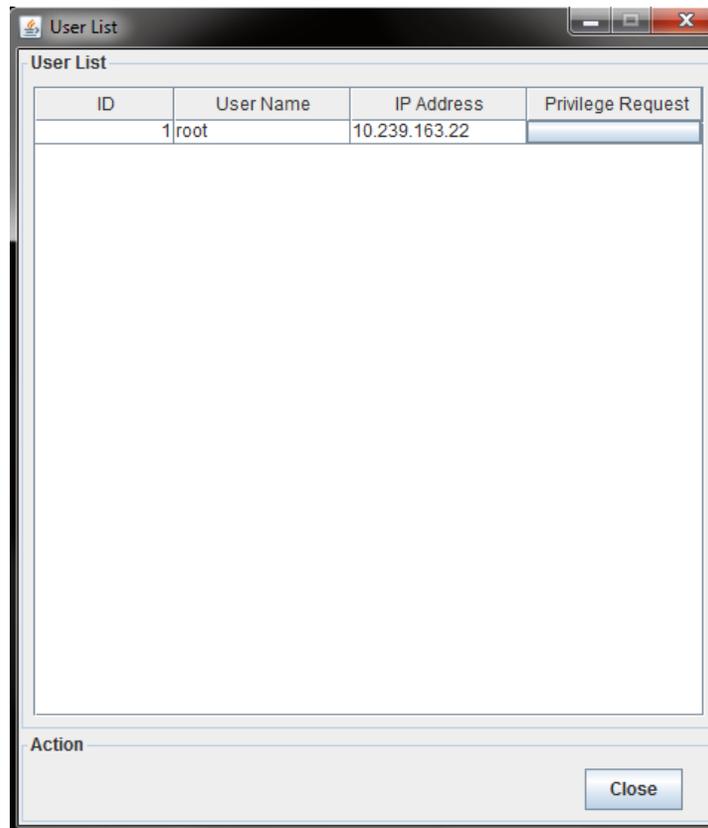


Figure 32. Remote Console User List

6.3.5 Capture Menu

Click **Capture** in the Remote Console control bar to capture a full screen view and save the image to the client. Click **Full screen view** to save the current full screen view of the remote console to the client.

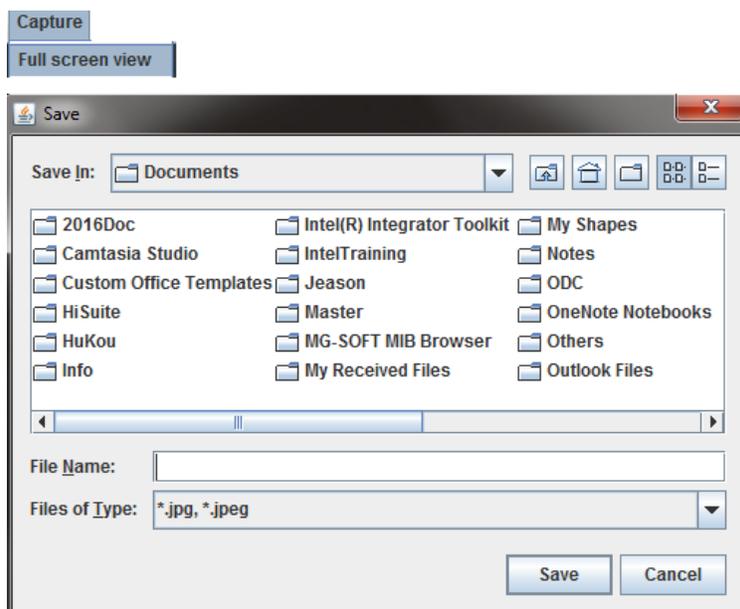


Figure 33. Remote Console Capture Menu

6.3.6 Power Control Menu

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

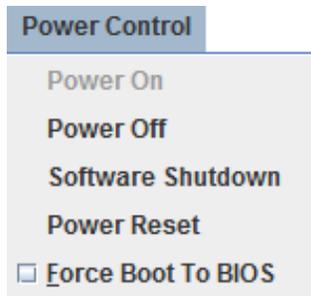


Figure 34. Remote Console Power Control Menu

Table 5 describes the power control operations that can be performed.

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

Table 5. Remote Console Power Control

Option	Task
Power ON	Power on the host.
Power OFF	Immediately power off the host.
Software Shutdown	Soft power off the host.
Power Reset	Hard reset the host without powering off.
Force Boot To BIOS	Enter BIOS setup after resetting the server.

6.3.7 Exit Menu

Click **Exit** and then click **Yes** (Figure 35) to exit the remote console.



Figure 35. Exit the Remote Console

6.4 Remote Console Status Line

The status line at the top of the Remote Console screen displays the console state as shown in figure below. status line provides BMC host name, Java* encryption, resolution, transaction speed and display frames per second.

iKVM Viewer v2.4.8 r01 [bmca4bf0126dcda.sh.intel.com] Algo: AES_256 - Res: 1024 x 768 - Tx: 2.0k (2.9k) Rx: 7.8k (8.6k) - FPS: 25 (23)

Figure 36. Remote Console Status Line

7. Integrated BMC Web Console Options

This chapter provides a detailed description of each Integrated BMC Web Console page. The descriptions are organized in sections 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 1. 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 37.



Figure 37. Busy Indicator Bar

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

7.1 System Tab

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

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 6.

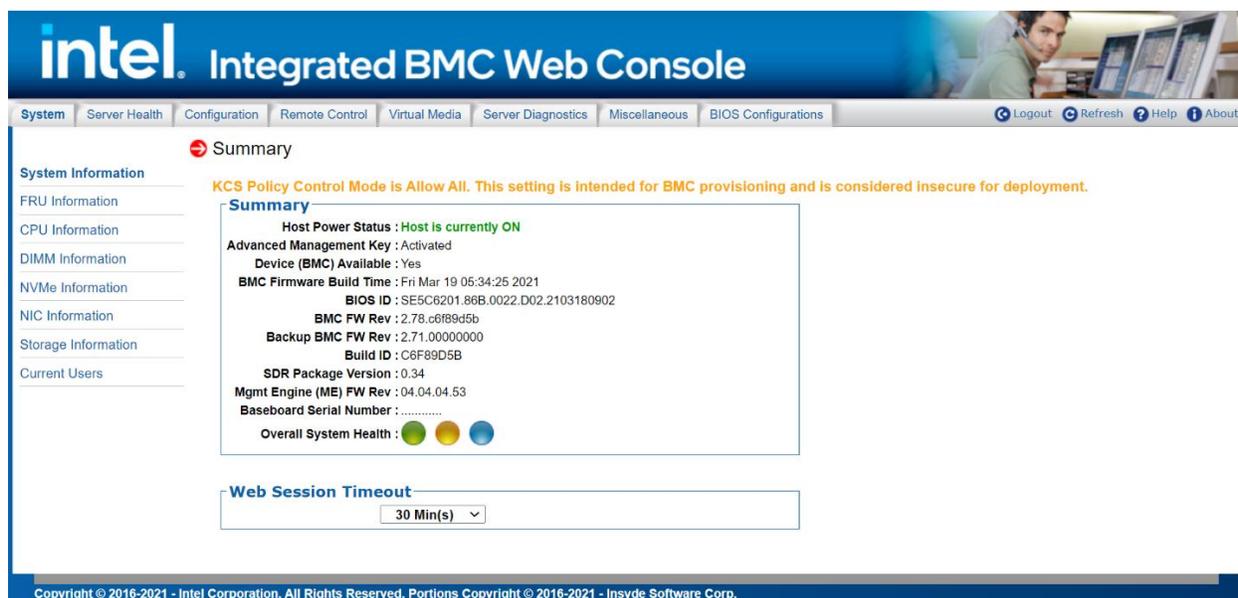


Figure 38. System Information Page

Table 6. System Information Page Details

Information	Details
Host Power Status	Power status of the host (on/off).
Advanced Management Key	Indicates whether the software license has been activated.
Device (BMC) Available	Indicates whether the BMC is available for normal management tasks.

Information	Details
BMC FW Build Time	The build date and time of the installed BMC firmware.
BIOS ID	Major and minor revision of the BIOS.
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 (ME) FW Rev	Major and minor revision of the Intel Management Engine firmware.
Baseboard Serial Number	Serial number of the baseboard in this system.
Overall System Health	A general indication of the system health: <ul style="list-style-type: none"> • Left (Green) = System Ready LED • Center (Amber) = System Fault LED • Right (Blue) = Chassis ID LED

7.1.2 Field Replaceable Unit (FRU) Information

The Field Replaceable Unit (FRU) Information page displays information from the FRU repository of the baseboard, front panel, hot swap backplane, riser card and power supply. Specify the FRU component by clicking the FRU Information pull-down box (Figure 39).

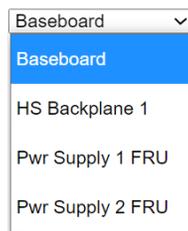


Figure 39. FRU Board Options

All data in the FRU information page is compliant with standard specifications (Platform Management FRU Information Storage Definition). See Figure 40 for details of the baseboard FRU.

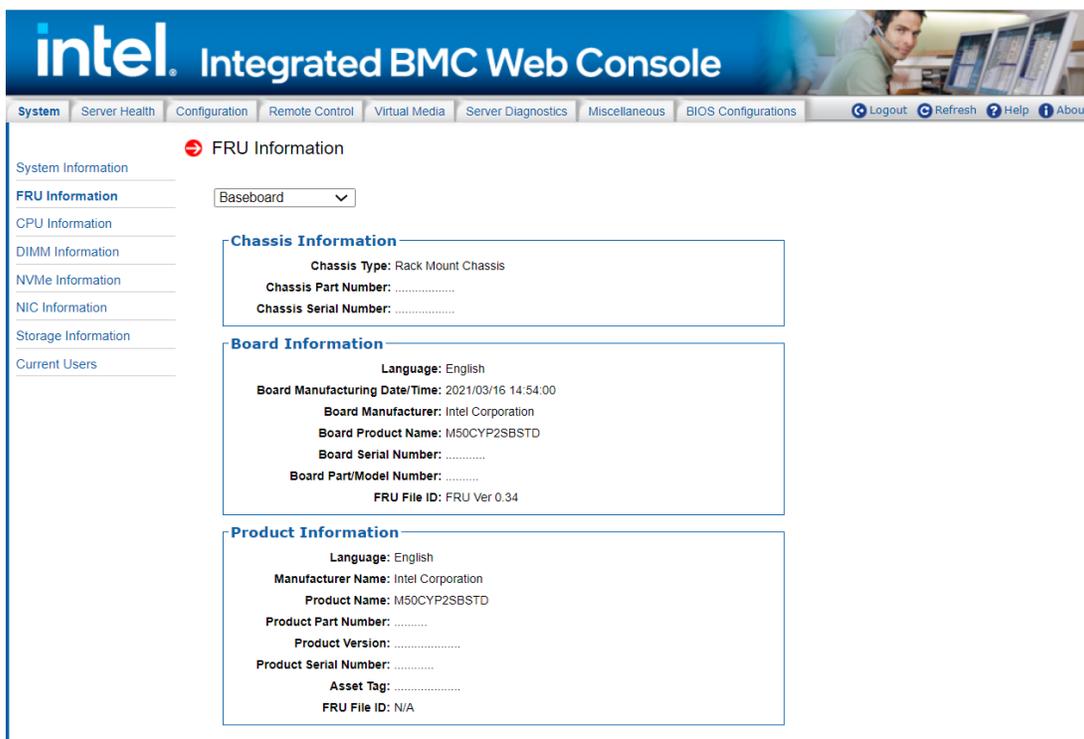


Figure 40. System FRU Information Page

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 41 for details.

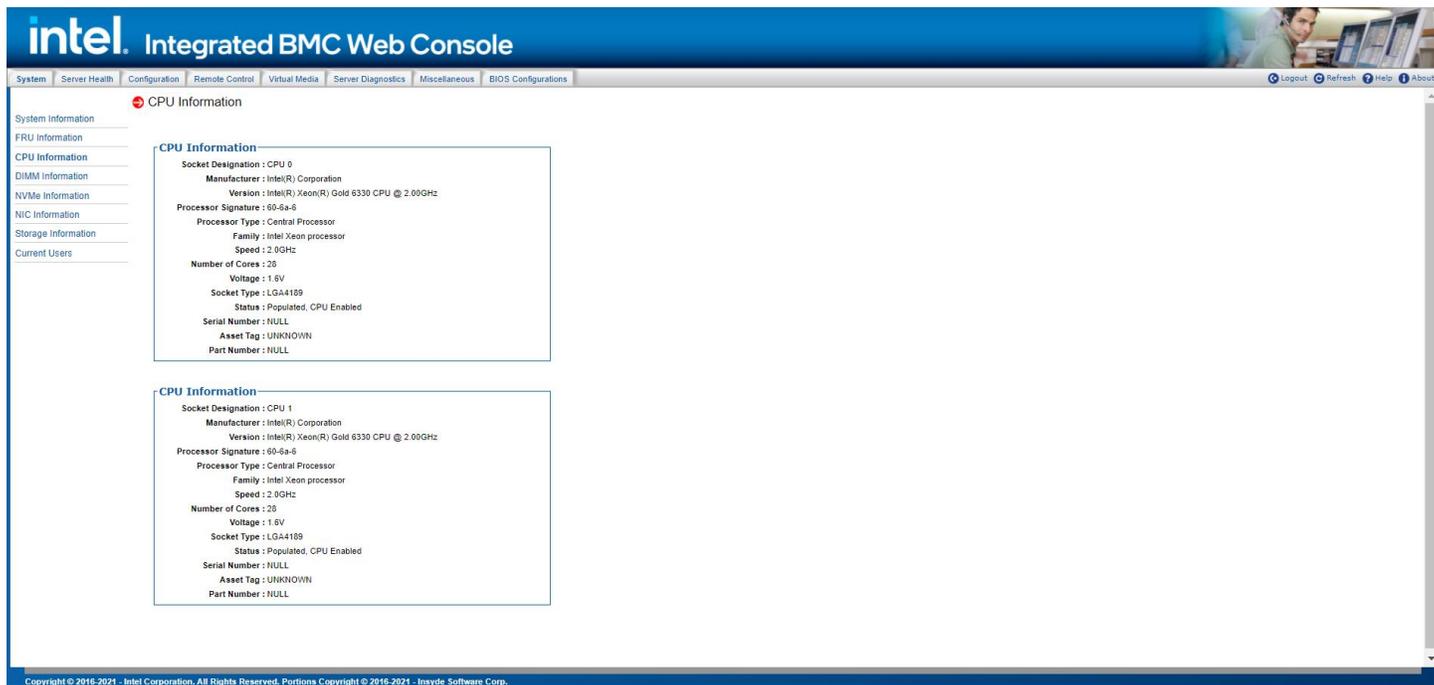


Figure 41. System CPU Information Page

7.1.4 DIMM Information

The DIMM Information page displays information on DIMM modules installed in the host system. The DIMM information includes slot number, size, memory type, manufacturer, asset tag, memory serial/part number. See Figure 42 for details.

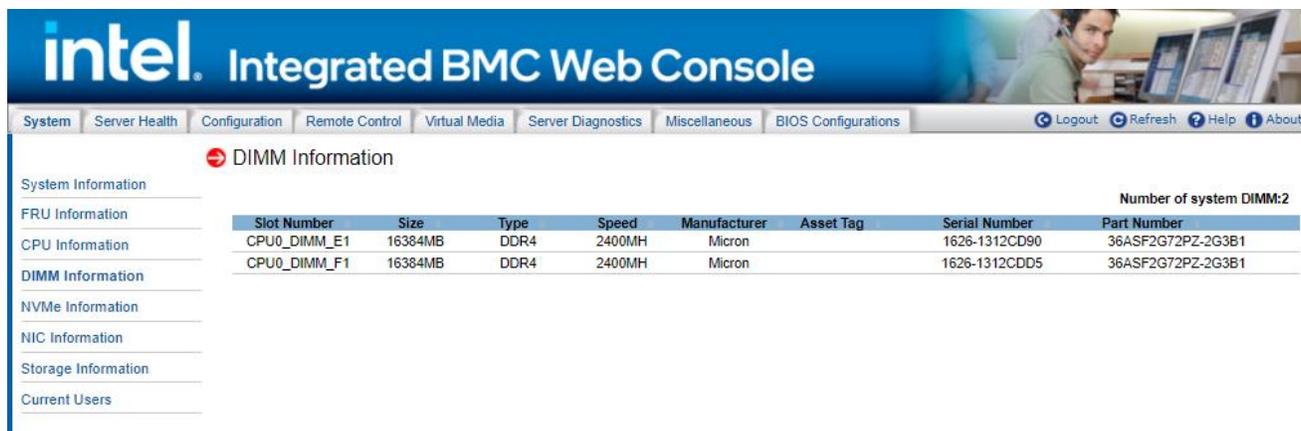


Figure 42. System DIMM Information Page

7.1.5 NVMe* Information

The NVMe* Information page displays information on supported NVMe* drives installed on the host system. See Figure 43 for details. Note that the BMC only displays information about NVMe* drives that meet all of the support requirements.



Figure 43. System NVMe* Information Page

7.1.6 NIC Information

The NIC Information page displays information for NIC modules installed in the host system. The NIC information includes PCI Class code, slot number, Vendor ID, Device ID, Current Speed(Mbps), Portidx, Media State, MAC Address, Firmware Version. See Figure 44 for details.

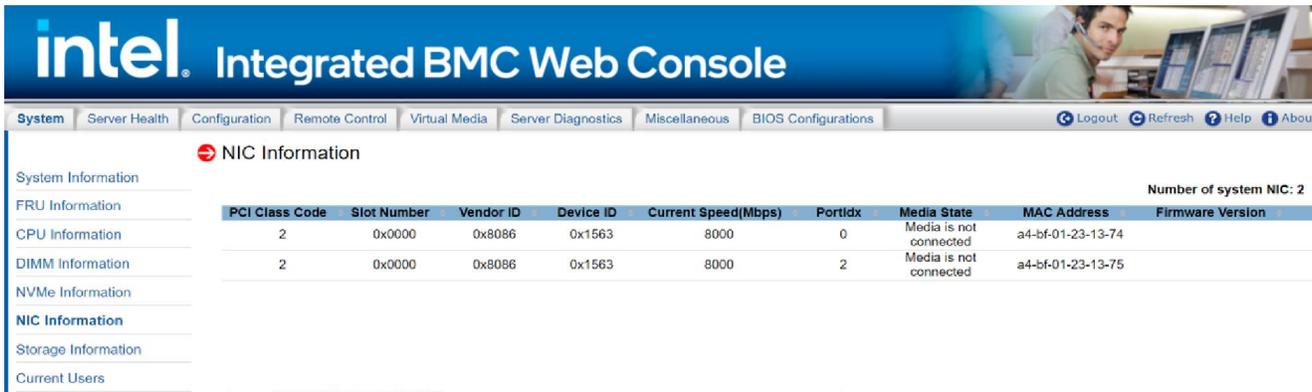


Figure 44. System NIC Information Page

7.1.7 Storage Information

The Storage Information page displays information of Storage devices installed in the host system. The Storage information includes Port Destination, Device Index, Connector Type, Protocol, Device Type, Capacity(GB), RPM, Model, Serial, PCI Class Code, Vendor ID, Device ID. See Figure 45 for details.



Figure 45. System Storage Information Page

7.1.8 Current Users

The Current Users page displays users currently logged in to the BMC via the embedded web server, IPMI 1.5 or IPMI 2.0 session, and Integrated BMC Web Console login type via HTTP or HTTPS. KVM session number, virtual media usage status, and client IP address are also listed in this table. See Figure 46 for details.



Figure 46. System Current Users page

Notice: Intel added to the BMC a new KCS Policy Control Mode; when set to "Deny ALL" on the BMC Integrated BMC Web Console, both the BMC and FRUSDR cannot be upgraded/downgraded as expected behavior. Updates can still be performed via Redfish* or BMC Integrated BMC Web Console. By default, the BMC KCS Policy is set to "Allow All".

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

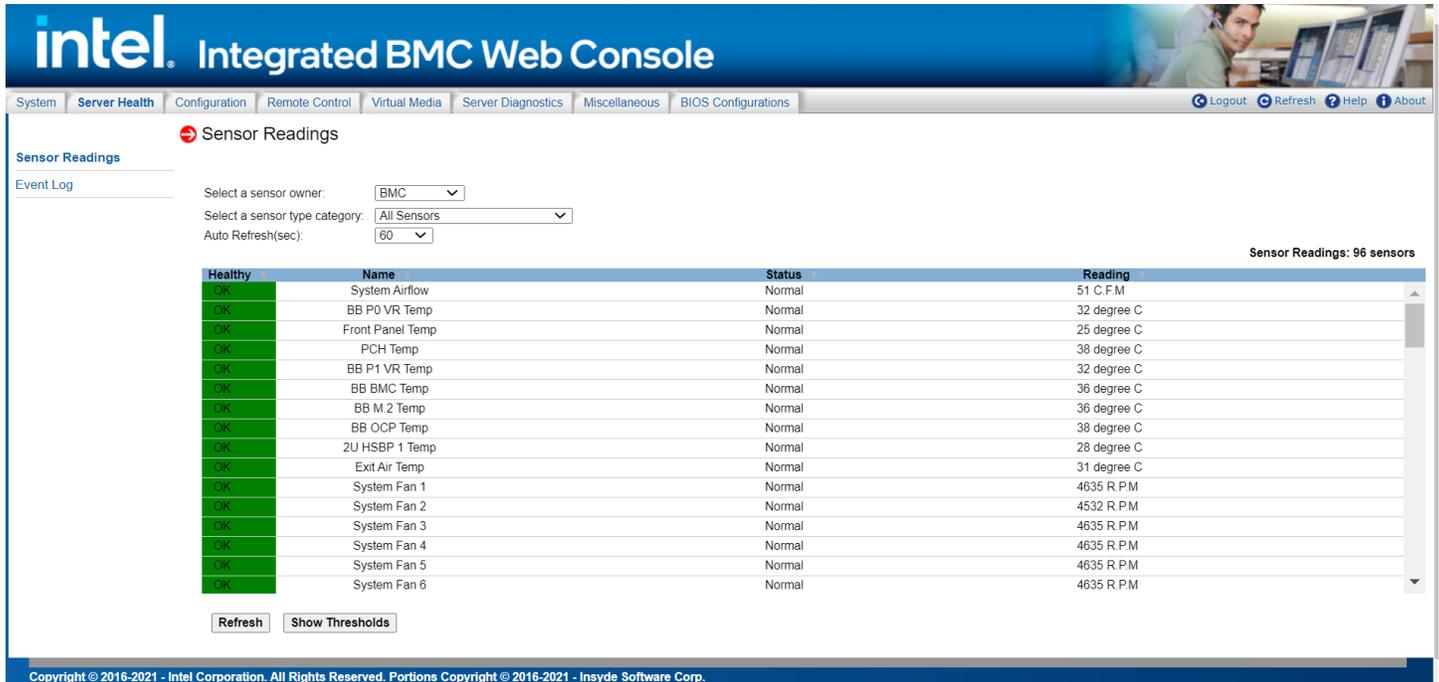


Figure 47 and Figure 48 (with threshold).

Table 7 lists the options available in this page. By default, this page displays all sensors owned by the BMC and auto-refreshes every 60 seconds.

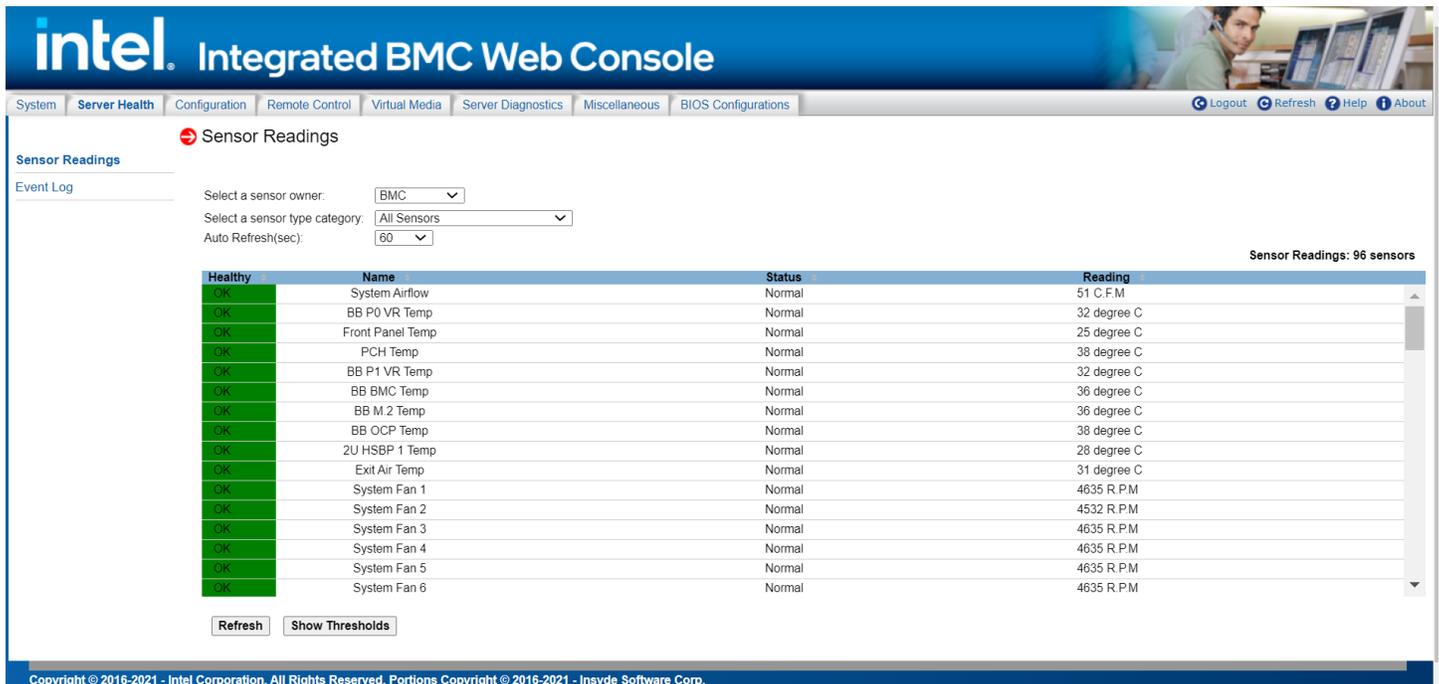


Figure 47. Server Health Sensor Readings Page (Thresholds Not Displayed)

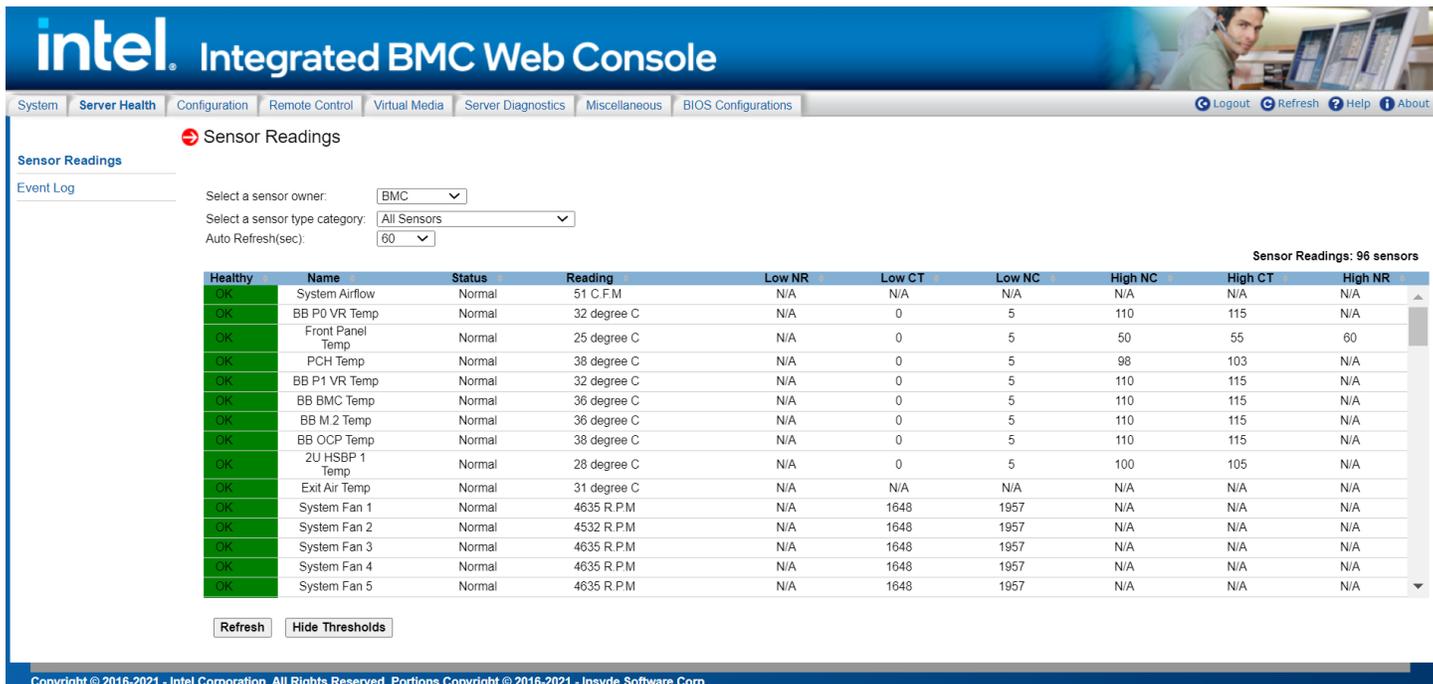


Figure 48. Server Health Sensor Readings Page (Thresholds Displayed)

Table 7. Server Health Sensor Readings Options

Option	Task
Select a sensor owner	Select the owner of sensor readings to display in the list. Choose BMC, ME, or SATELITE. The default owner is 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. The default refresh time is 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 (Figure 49). Table 8 lists the options available in this page.

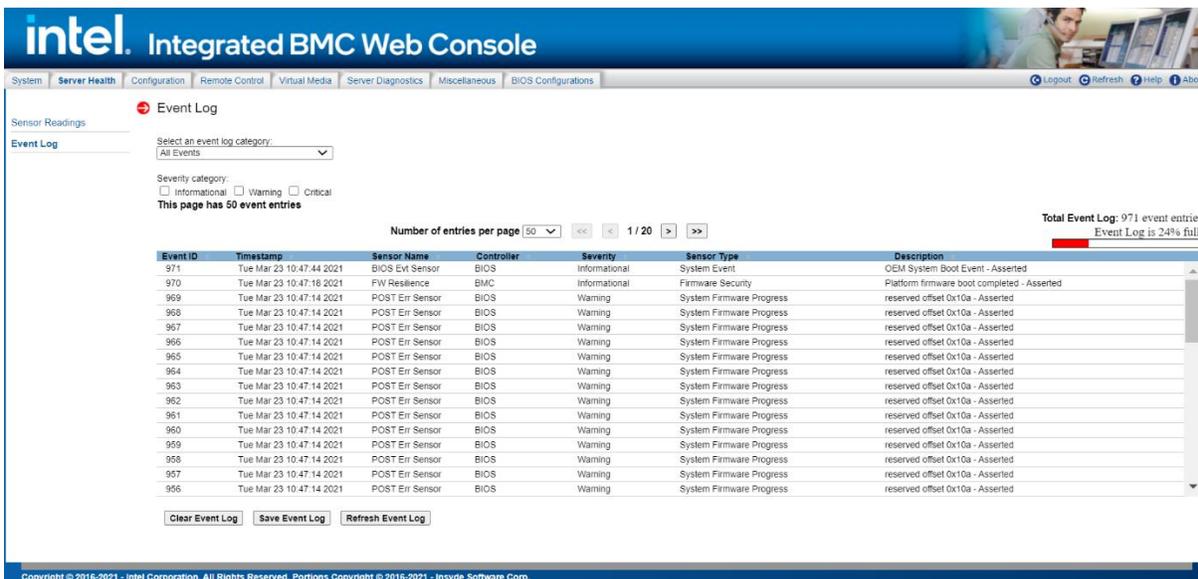


Figure 49. Server Health Event Log Page

Table 8. 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 is used to configure various settings such as alerts, alert email, IPv4 and IPv6 networks, VLAN, KVM and media, SSL certification, users, security settings, SOL, SDR configuration, and firmware as 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 (Figure 50). Table 9 lists the options to select the events that should trigger alerts and where the alerts are to be sent.

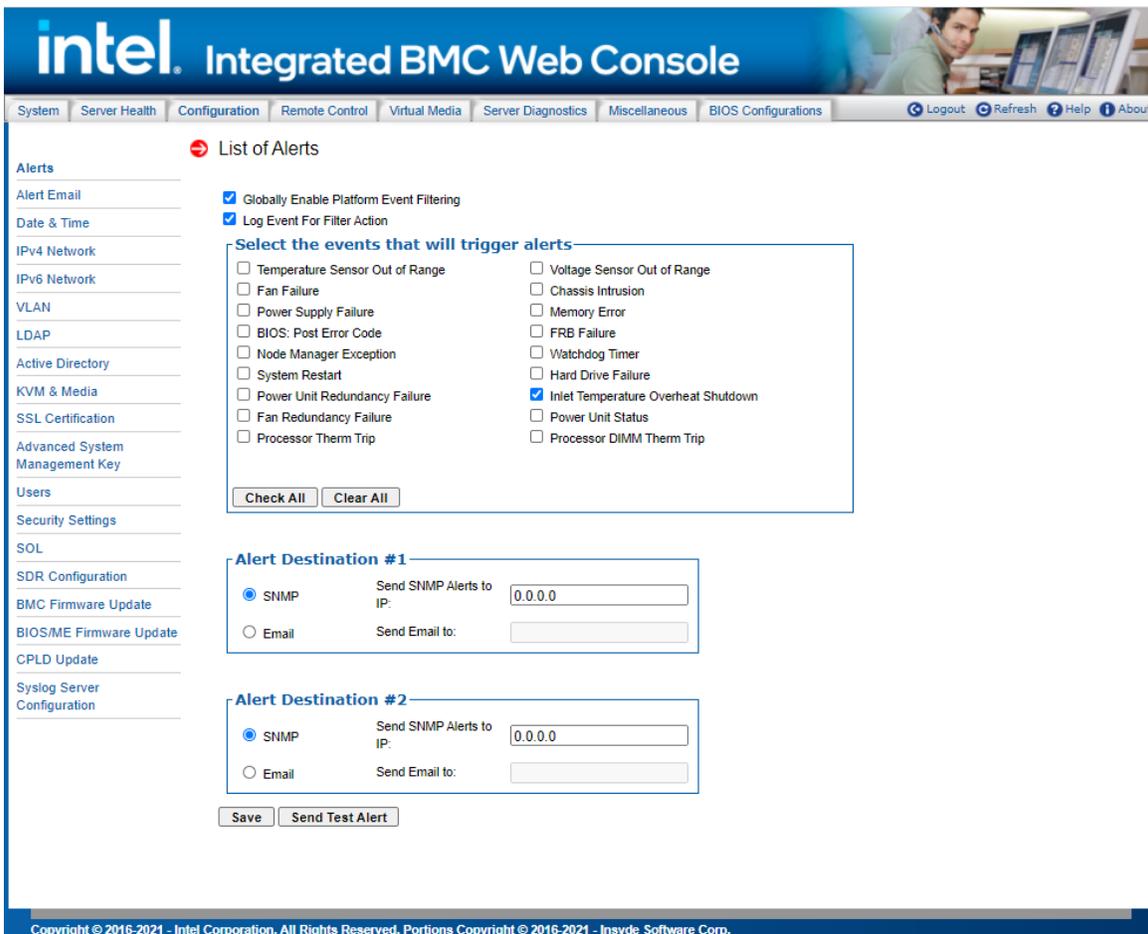


Figure 50. Alerts Page

Table 9. Alerts Options

Option	Task
Globally Enable Platform Event Filtering	This can be used to prevent sending alerts until you have fully specified your 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 that the alert will 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 to send a test alert.

7.3.2 Alert Email

Use this page to configure the parameters for alert emails. Table 10 lists the options to configure alert emails.

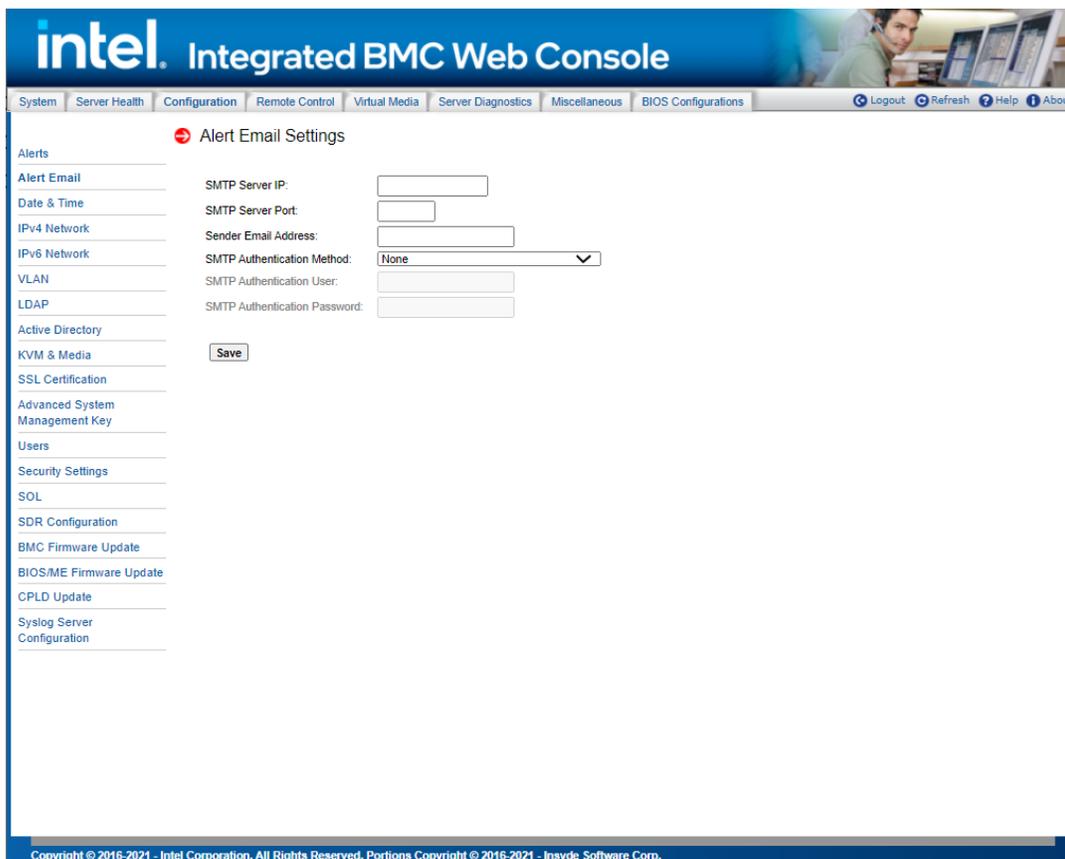


Figure 51. Alert Email Page

Table 10. Alert Email Options

Option	Task
SMTP Server IP	The IP address of the remote SMTP mail server that the alert emails will be sent to. 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.
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 Method	Select the SMTP authentication and encryption methods supported by the remote SMTP Mailserver. SMTP authentication without encryption is not supported. Options: <ul style="list-style-type: none"> None - use this option if the remote SMTP Mailserver does not support authentication or does not support STARTTLS or SSL/TLS encryption methods. Authentication after STARTTLS - Use this option if the remote SMTP Mailserver only supports STARTTLS encryption. 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 Method is set to None.
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.
Save button	Click to save any changes made.

7.3.3 Date & Time

Use this page to view and change the devices' date and time from NTP server or RTC. Table 11 lists the options to configure Date & Time.

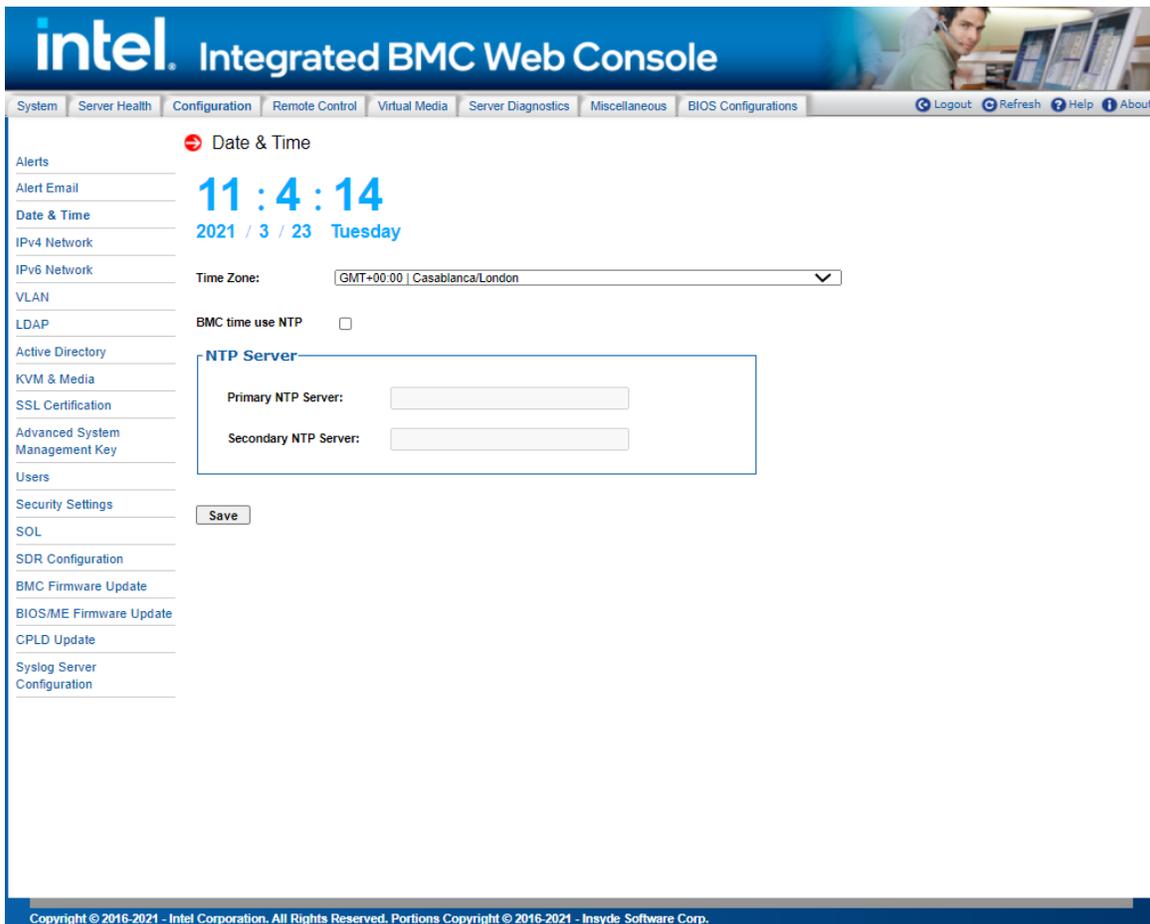


Figure 52. Date & Time Page

Table 11. Date & Time Options

Option	Task
Time Zone	Time zone setting.
BMC time use NTP	Enable/Disable NTP service.
Primary NTP Server	Primary NTP Server address.
Second NTP Server	Second NTP Server address.
Save button	Click to save any changes made.

7.3.4 IPv4 Network

The IPv4 settings page is used to configure the IPv4 network settings for the server management LAN interface to the BMC controller. See Figure 53 or Figure 54 for details. Table 12 lists the options available in this page.

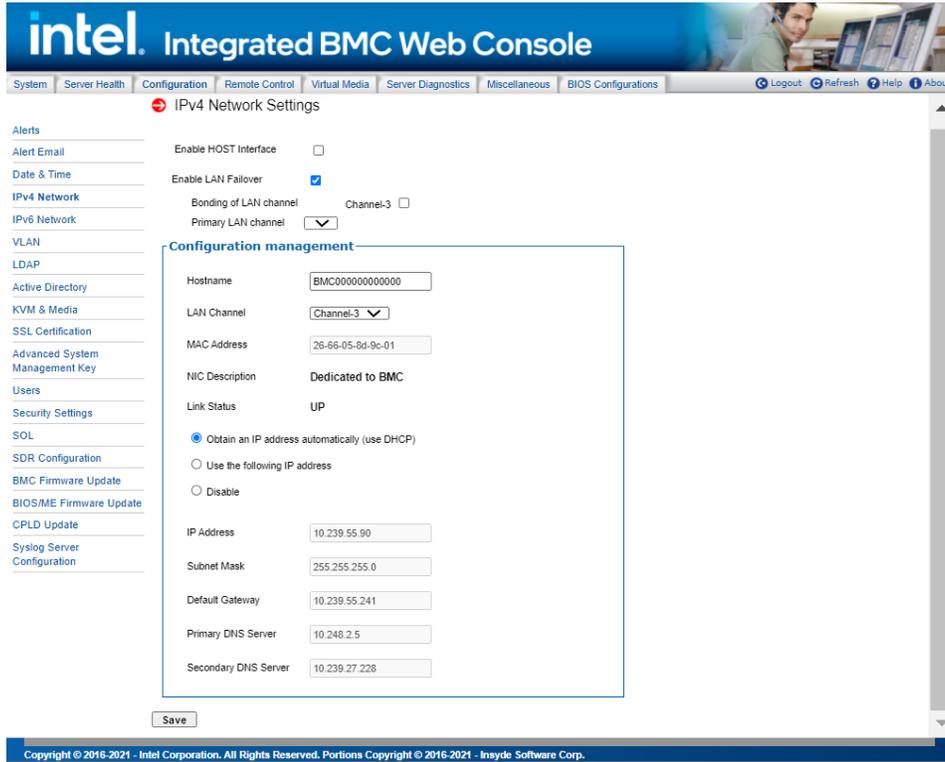


Figure 53. IPV4 Network DHCP Page

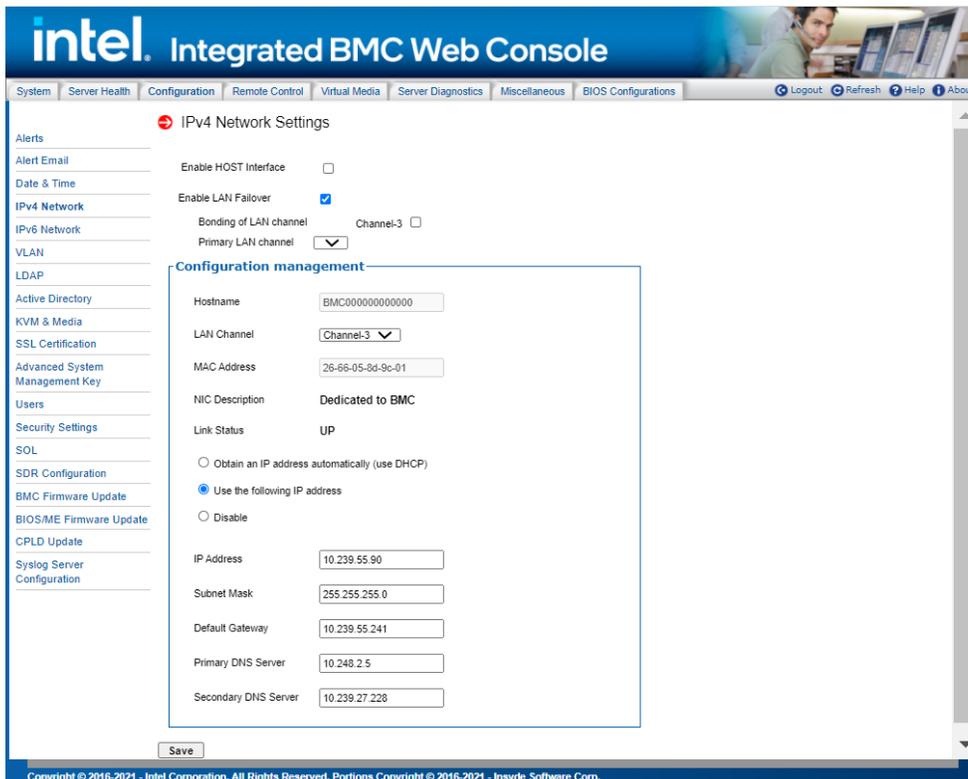


Figure 54. IPv4 Network Static Page

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

WARNING: When LAN failover is enabled, the system administrator must ensure that each network controller connection, which can be seen by the BMC, has connectivity to the same networks. If there is a loss of functionality on the primary network controller channel, it will randomly failover to any of the other network controller channels that are connected and seen by the BMC.

Table 12. IPv4 Network Settings Options

Option	Task
Host Name	The hostname is an RFC 1123 compliant string less than 64 alpha-numeric characters. Hyphen characters are allowed as long as the hyphen is not the first or final character in the hostname. The default value is "BMC" + MAC address.
Enable LAN Failover	Enabling failover bonds Ethernet interfaces into the primary LAN Channel, the Bonding of LAN channel option can select Ethernet device to bond, the Primary LAN channel option can specify a LAN channel to primary LAN channel. When the primary interface's lease is lost, one of the secondary interfaces is activated automatically with the same IP address.
LAN Channel	Select the channel on which to configure the network settings. Lists the LAN Channels available for server management. The LAN channels describe the physical NIC connection on the server. D50TNP/D40AMP: <ul style="list-style-type: none"> Baseboard NIC (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system. Dedicated Management Channel (BMC LAN Channel 3) is Dedicated Management NIC. M50CYP: <ul style="list-style-type: none"> Dedicated Management Channel (BMC LAN Channel 1) is Dedicated Management NIC.
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 three options for configuring the IP address: <ul style="list-style-type: none"> Obtain an IP address automatically (use DHCP) – Uses DHCP to obtain the IP address. Use the following IP address – Manually configure the IP address. Disable LAN Channel – Sets the IP address, Subnet Mask, and Default Gateway to 0.0.0.0.
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

The IPv6 settings page is used to enable and configure the IPv6 network settings and to enable and configure LAN failover (Figure 55) Table 13 lists the options available in this page.

The screenshot displays the 'IPv6 Network Settings' page in the Intel Integrated BMC Web Console. The page is titled 'IPv6 Network Settings' and includes a navigation menu on the left with options like Alerts, Alert Email, Date & Time, IPv4 Network, IPv6 Network, VLAN, LDAP, Active Directory, KVM & Media, SSL Certification, Advanced System Management Key, Users, Security Settings, SOL, SDR Configuration, BMC Firmware Update, BIOS/ME Firmware Update, CPLD Update, Syslog Server Configuration, and a 'Save' button at the bottom.

The main configuration area is titled 'Configuration management' and contains the following settings:

- Enable HOST Interface:
- Enable LAN Failover:
- LAN Channel: Channel-3 (dropdown menu)
- MAC Address: 26-66-05-8d-9c-01 (text input)
- NIC Description: Dedicated to BMC
- Link Status: UP
- Obtain an IP address automatically (use DHCPv6/SLAAC):
- Use the following IP address:
- Disable:
- IP Address: (text input)
- Prefix Length: 64 (text input)
- Default Gateway: (text input)
- Primary DNS Server: ::ffff:10.248.2.5 (text input)
- Secondary DNS Server: ::ffff:10.239.27.228 (text input)

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

Copyright © 2016-2021 - Intel Corporation. All Rights Reserved. Portions Copyright © 2016-2021 - Insyde Software Corp.

Figure 55. IPv6 Network Page

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

WARNING: When LAN failover is enabled, the system administrator must ensure that each network controller connection, which can be seen by the BMC, has connectivity to the same networks. If there is a loss of functionality on the primary network controller channel, it will randomly failover to any of the other network controller channels that are connected and seen by the BMC.

Table 13. IPv6 Network Settings Options

Option	Task
Enable LAN Failover	Enabling failover bonds Ethernet interfaces into the primary LAN Channel, the Bonding of LAN channel option can select Ethernet device to bond, the Primary LAN channel option can specify a LAN channel to primary LAN channel. When the primary interface's lease is lost, one of the secondary interfaces is activated automatically with the same IP address.
LAN Channel	<p>Select the channel on which to configure the network settings. Lists the LAN Channels available for server management. The LAN channels describe the physical NIC connection on the server.</p> <p>D50TNP/D40AMP::</p> <ul style="list-style-type: none"> • Baseboard NIC (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system. • Dedicated Management Channel (BMC LAN Channel 3) is Dedicated Management NIC. <p>M50CYP:</p> <ul style="list-style-type: none"> • Dedicated Management Channel (BMC LAN Channel 1) is Dedicated Management NIC.
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	<p>Select one of the three 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.</p>
IP Address Gateway	<p>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 may be replaced with a single empty group using two consecutive colons (::).</p>
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 is used to enable and configure the VLAN private network settings on the selected server management LAN channels (Figure 56). Table 14 lists the options available in this page.

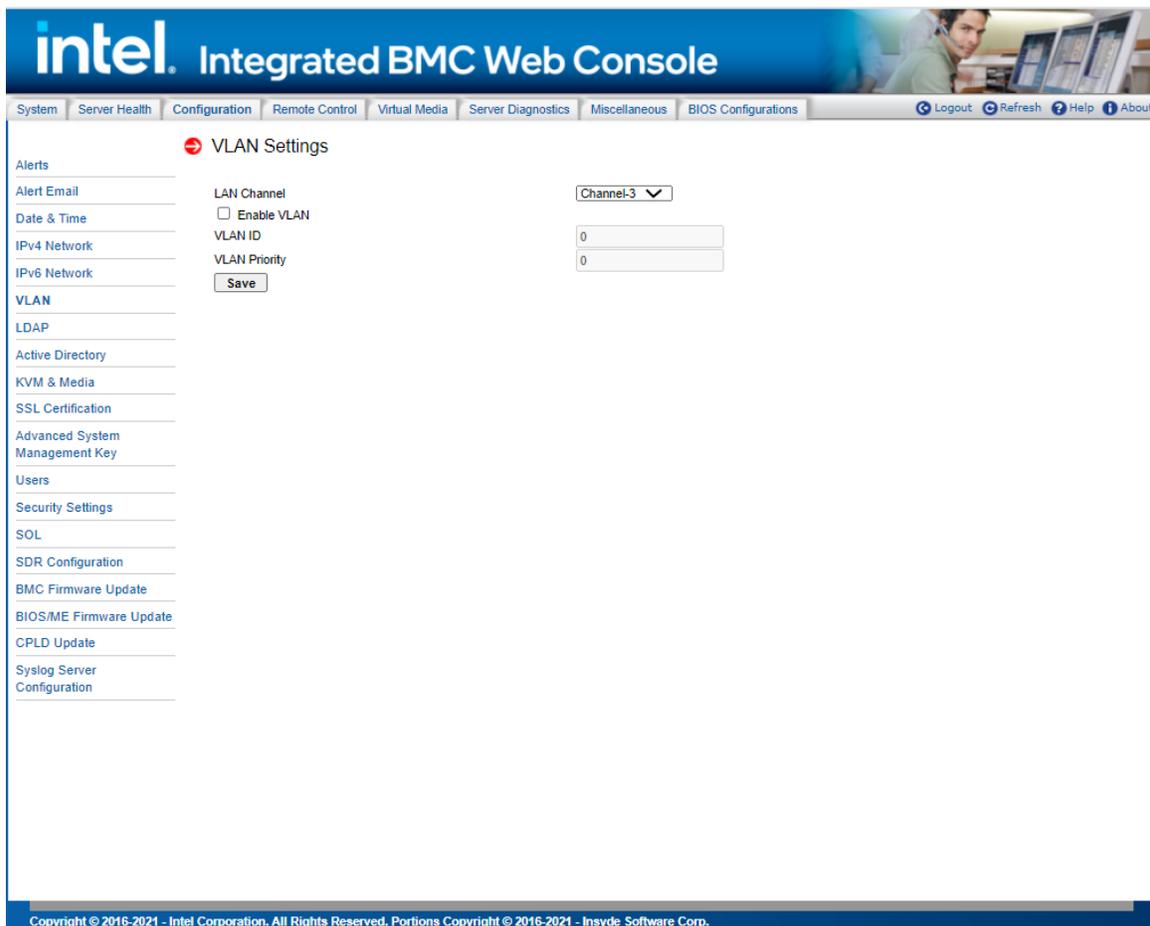


Figure 56. VLAN Settings Page

Table 14. VLAN Settings Options

Option	Task
LAN Channel	<p>Select the channel on which to configure the network settings. Lists the LAN Channels available for VLAN. The LAN channel describes the physical NIC connection on the server. D50TNP/D40AMP::</p> <ul style="list-style-type: none"> Baseboard NIC (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system. Dedicated Management Channel (BMC LAN Channel 3) is Dedicated Management NIC. <p>M50CYP:</p> <ul style="list-style-type: none"> Dedicated Management Channel (BMC LAN Channel 1) is Dedicated Management NIC.
Enable VLAN	Enable VLAN for the LAN channel selected in the drop-down box.
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 LDAP Settings

The LDAP settings page is used to enable/disable the LDAP settings on the selected server management LAN channels. See Figure 57 and Table 15 for available options on this page.

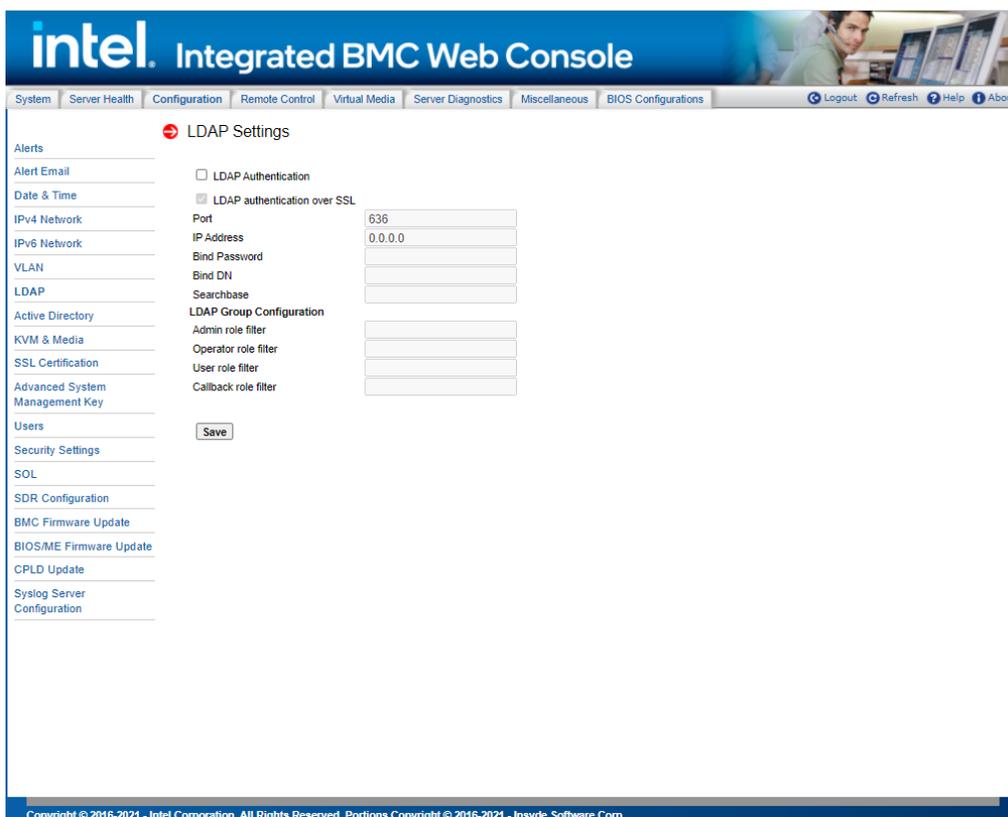


Figure 57. LDAP Settings Page

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. <ul style="list-style-type: none"> IP Address made of 4 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 4 characters long.
Bind DN	The Distinguished Name of the LDAP server, e.g. "cn=Manager, dc=my-domain, dc=com".
Searchbase	The searchbase of the LDAP server, e.g. "dc=my-domain, dc=com".
LDAP Group Configuration	Configure the LDAP search filters associated with BMC network privileges. e.g., "(&(cn=BMCAdminGroup)(memberUid=%s))"
Admin role filter	LDAP query filter for Admin network privilege.
Operator role filter	LDAP query filter for Operator network privilege.
User role filter	LDAP query filter for User network privilege.
Callback role filter	LDAP query filter for callback network privilege.
Save	Click to save the current settings.

7.3.8 Active Directory Settings

The Active Directory Settings page used to config Active Directory Authentication and enable/disable Active Directory Authentication over SSL. See Figure 58 and Table 16 for available options on this page

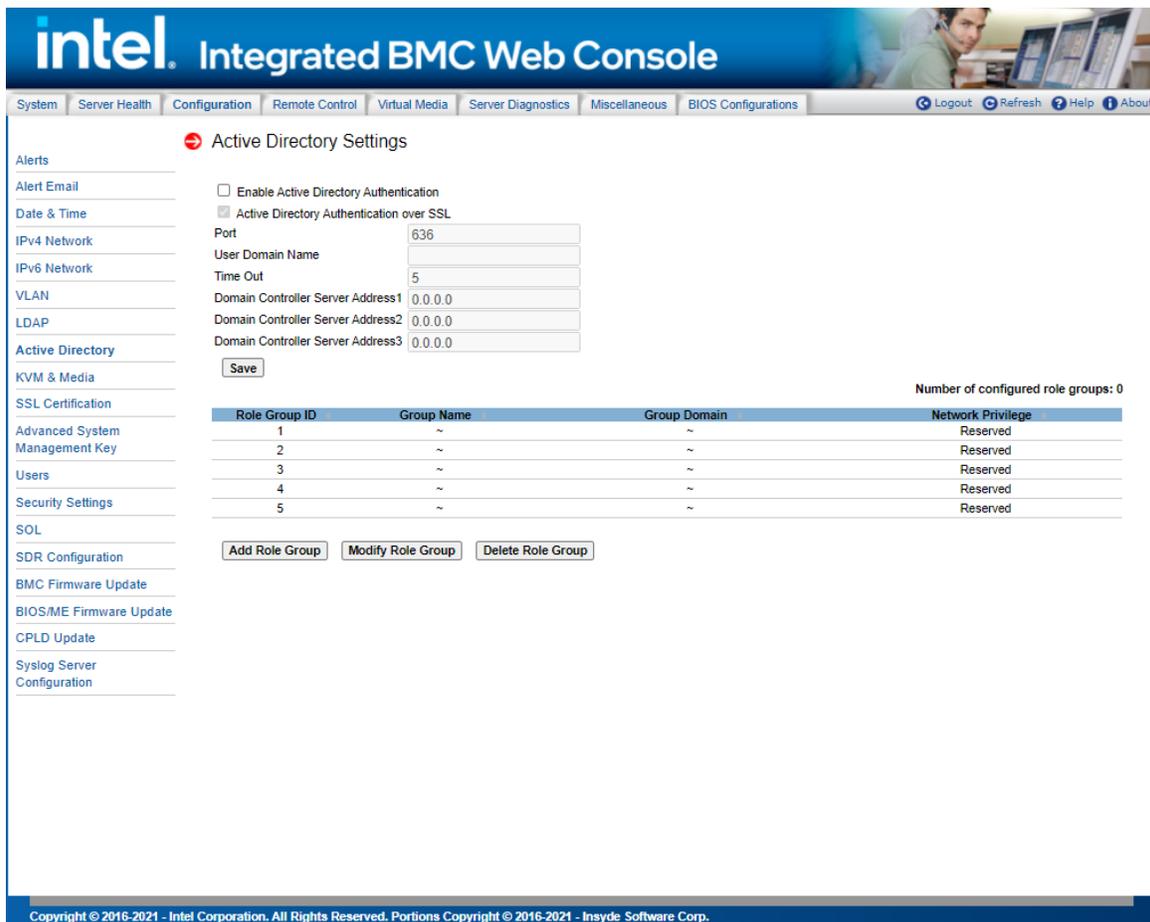


Figure 58. Active Directory Settings Page

Table 16. Active Directory Settings Options

Option	Task
Enable Active Directory Authentication	Click check box to enable.
Active Directory Authentication over SSL	Click check box to enable.
Port	Port 636 (the default LDAP port with SSL)
User Domain Name	User belongs to which domain in Active Directory server
Time Out	Timeout (sec) after request AD Server for authentication
Domain Controller Server Address1/2/3	IP address of a domain controller server. You can enter up to 3 sets of IP addresses.
Save (Remote Session)	Click to save any changes for Remote Session.
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.
Save (Mouse Mode Setting)	Click to save any changes for Mouse Mode Setting.

7.3.9 KVM & Media

Use this page to change the type and port of KVM encryption and the port of media encryption during a redirect session (Figure 59). Table 17 lists option details.

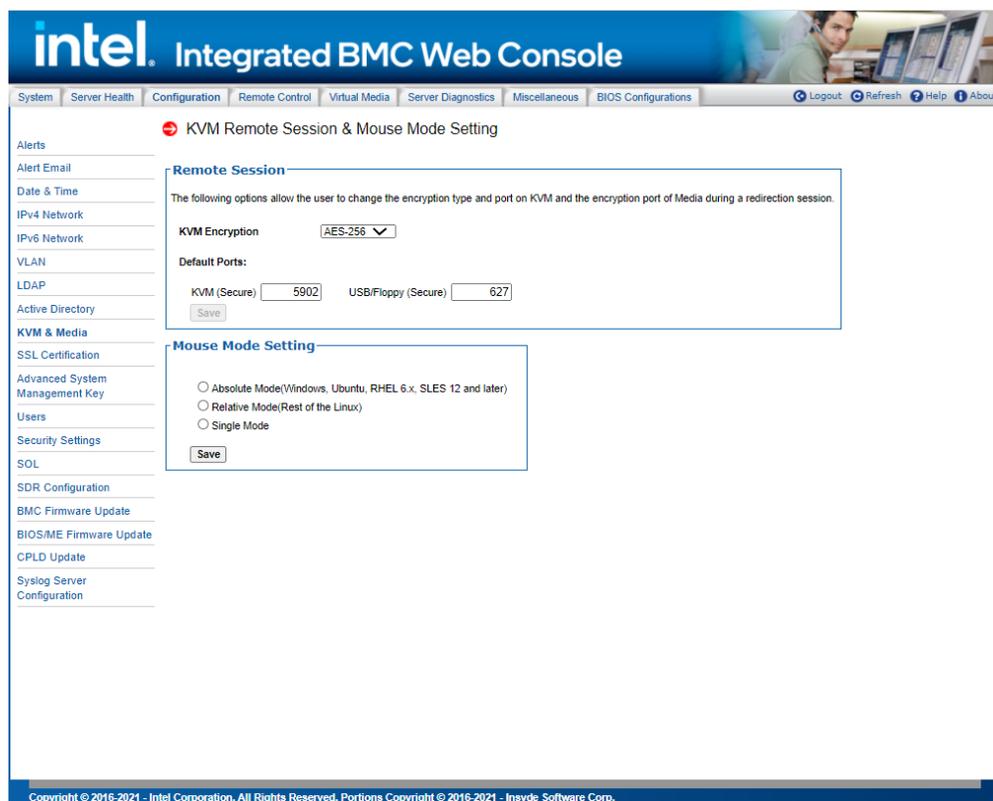


Figure 59. KVM & Media Page

Table 17. KVM & Media Options

Option	Task
KVM Encryption	Enable/disable encryption on KVM data during a redirection session. Choose any one from the supported encryption techniques.
Default Ports	Set the ports used by KVM and remote media (both standard and secure ports). Do not change these values unless you know the new ports are unused.
Save (Remote Session)	Click to save any changes for Remote Session.
Mouse Mode Setting	<p>Redirection Console handles mouse emulation from local window to remote screen in one of the following methods:</p> <ul style="list-style-type: none"> • Absolute Mode - Select to have the absolute position of the local mouse sent to the server. Preferred method where supported. Use this mode for Windows* OS and newer versions of Linux* (Ubuntu, RHEL, SLES). • Relative Mode - Select Relative Mode 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 OS mouse acceleration/threshold settings should match. Alternatively, use the mouse calibration option in JViewer. • Single Mode - Select Single Mode to have the calculated displacement from the local mouse in the center position, sent to the server. Under this mode Ctrl+6 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.

7.3.10 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 authenticity of the BMC. Use this page to upload an SSL certificate and private key, which allows the device to be accessed in a secured mode. See Figure 60 for details.

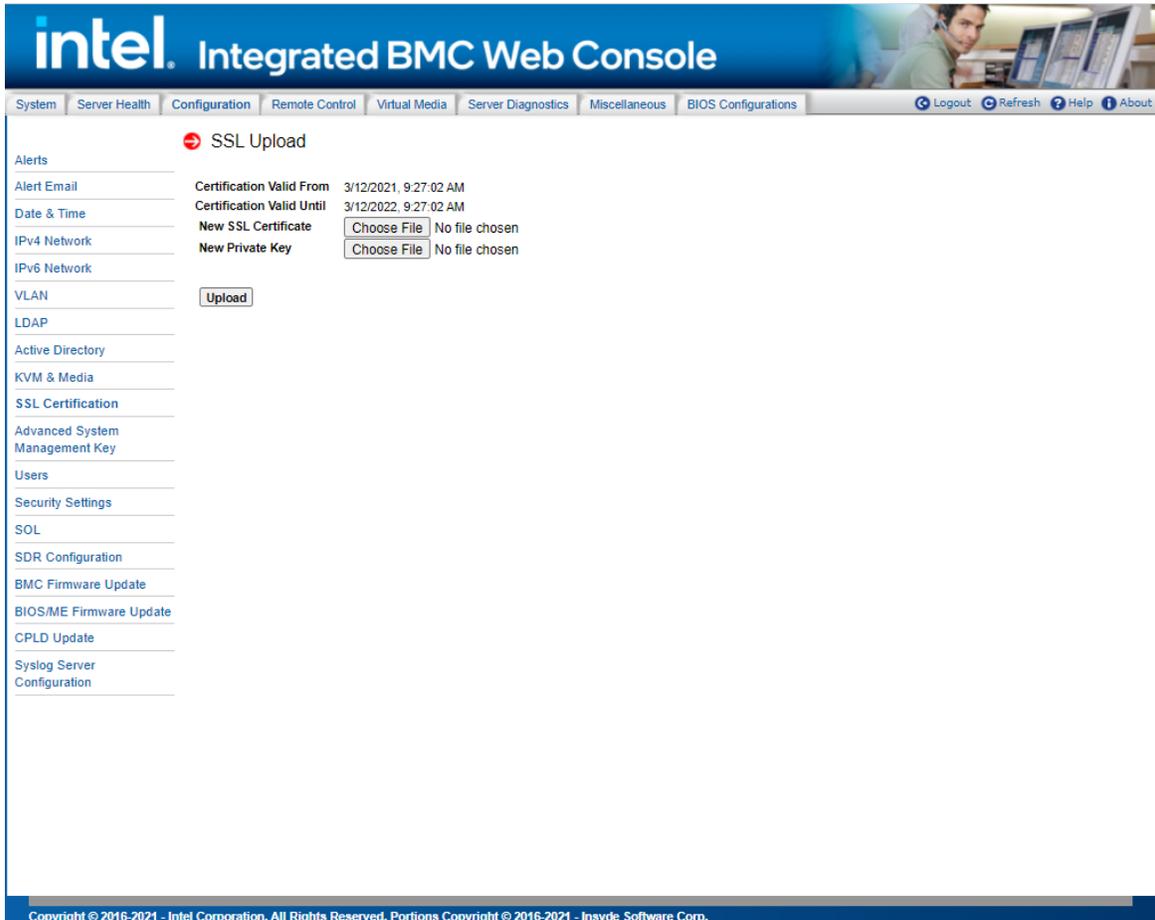


Figure 60. SSL Certification Page

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

7.3.11 Advanced System Management Key

The Users page lists the Advanced System Management Key info, use this page to upload new advanced system management key. See Figure 61 for details.

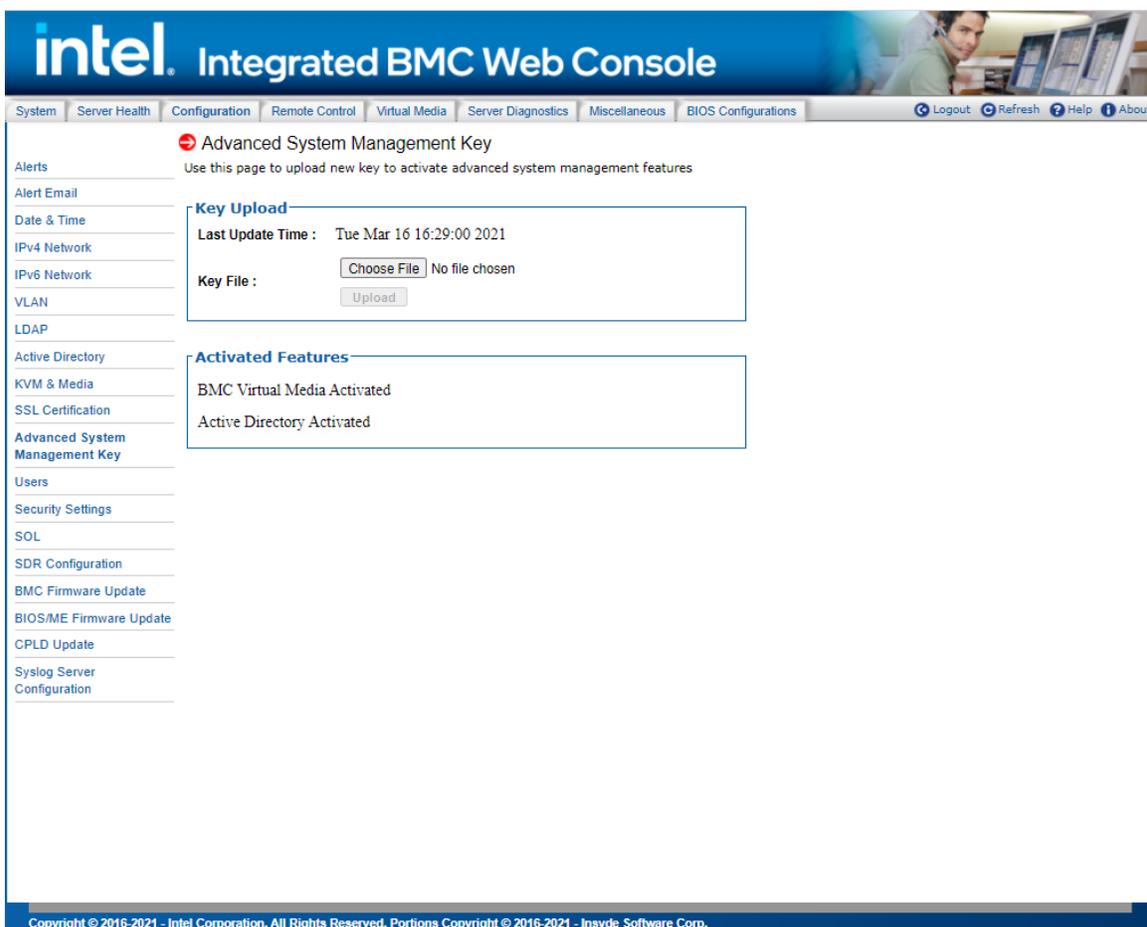


Figure 61. Advanced System Management Key Page

Table 18. Advanced System Management Key Options

Option	Task
Last Upload Time	Show the last upload time of the advanced system management key.
Advanced System Management Key Upload	Set the ports used by KVM and remote media (both standard and secure ports). Do not change these values unless you know the new ports are unused.
Choose File	Choose file to upload.
Upload	Upload the advanced system management key to the BMC for update action.

7.3.12 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 62 for details.

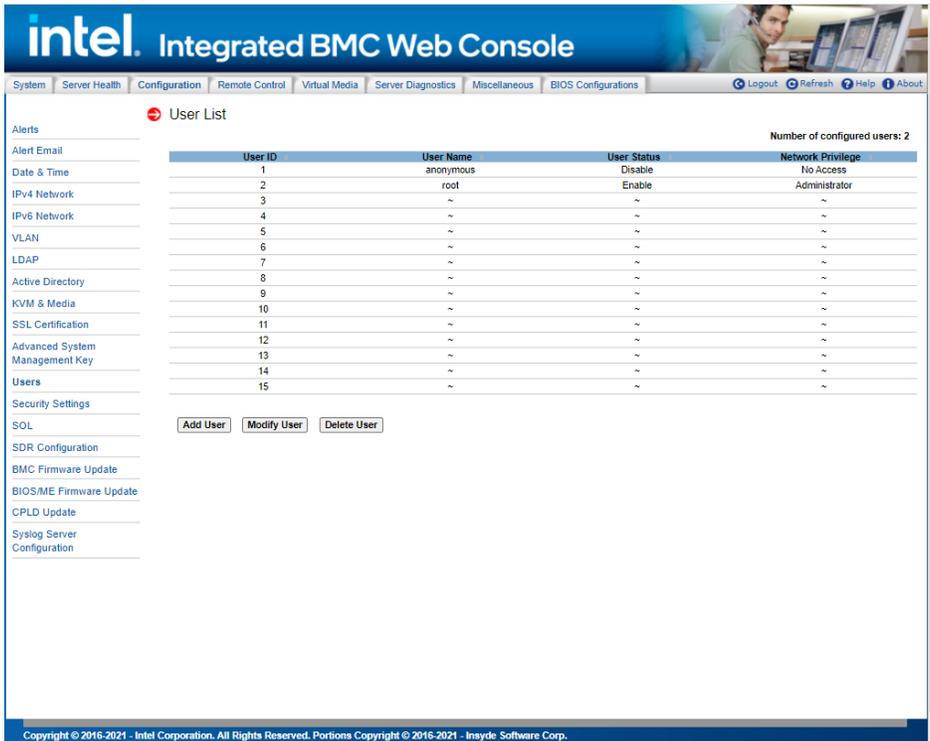


Figure 62. User List Page

This page allows the operator to configure the IPMI users and privileges for this server. UserID 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 63.

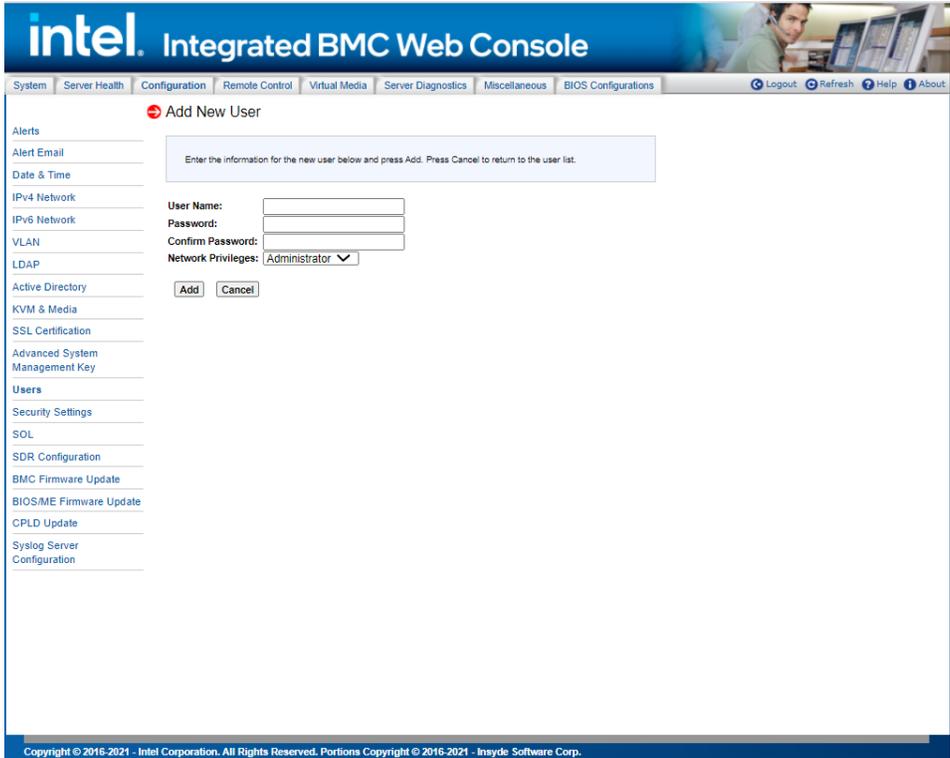


Figure 63. Add New User Page

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 64.

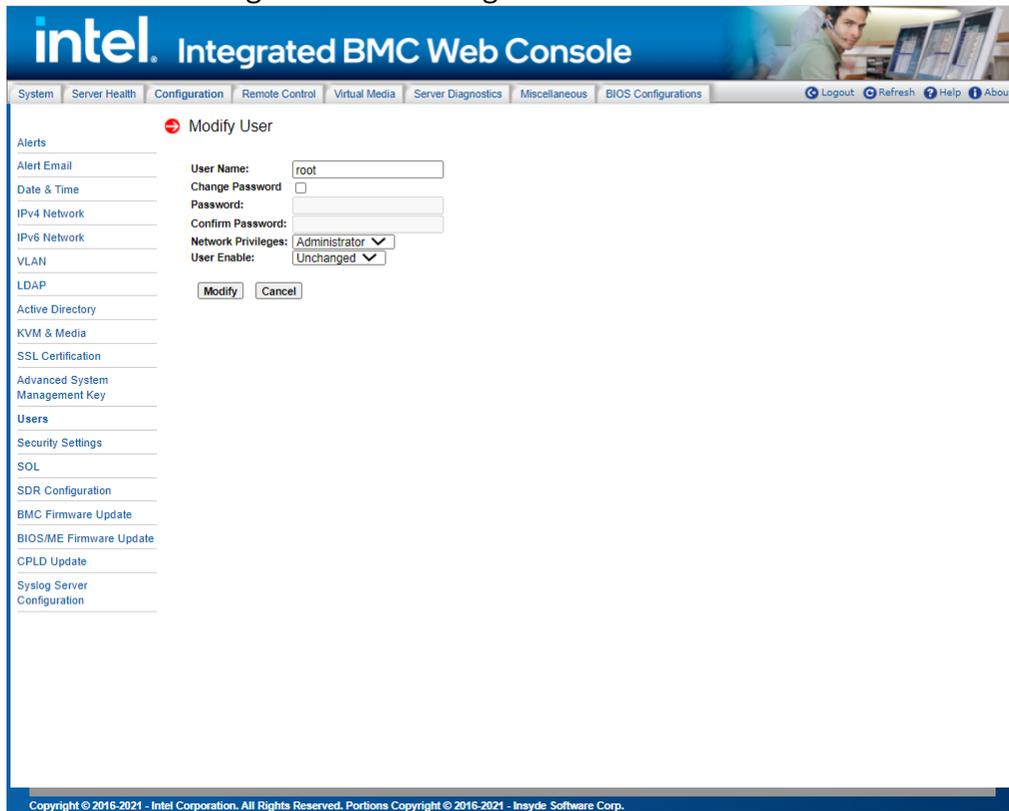


Figure 64. Modify User Page

To delete a user, select the user in the list and click the **Delete User** button (Figure 65).

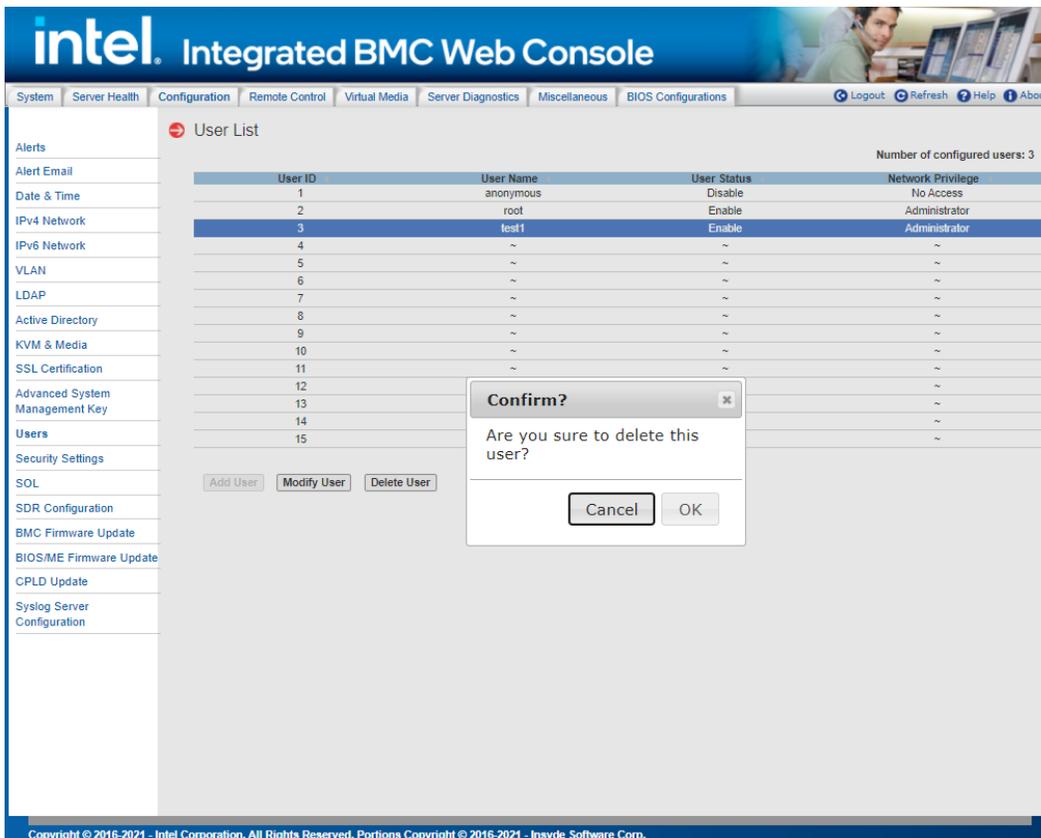


Figure 65. Delete User Page

7.3.13 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 will last before the user can attempt to log in again. See Figure 66 for details. Table 19 lists the options to modify the security settings.

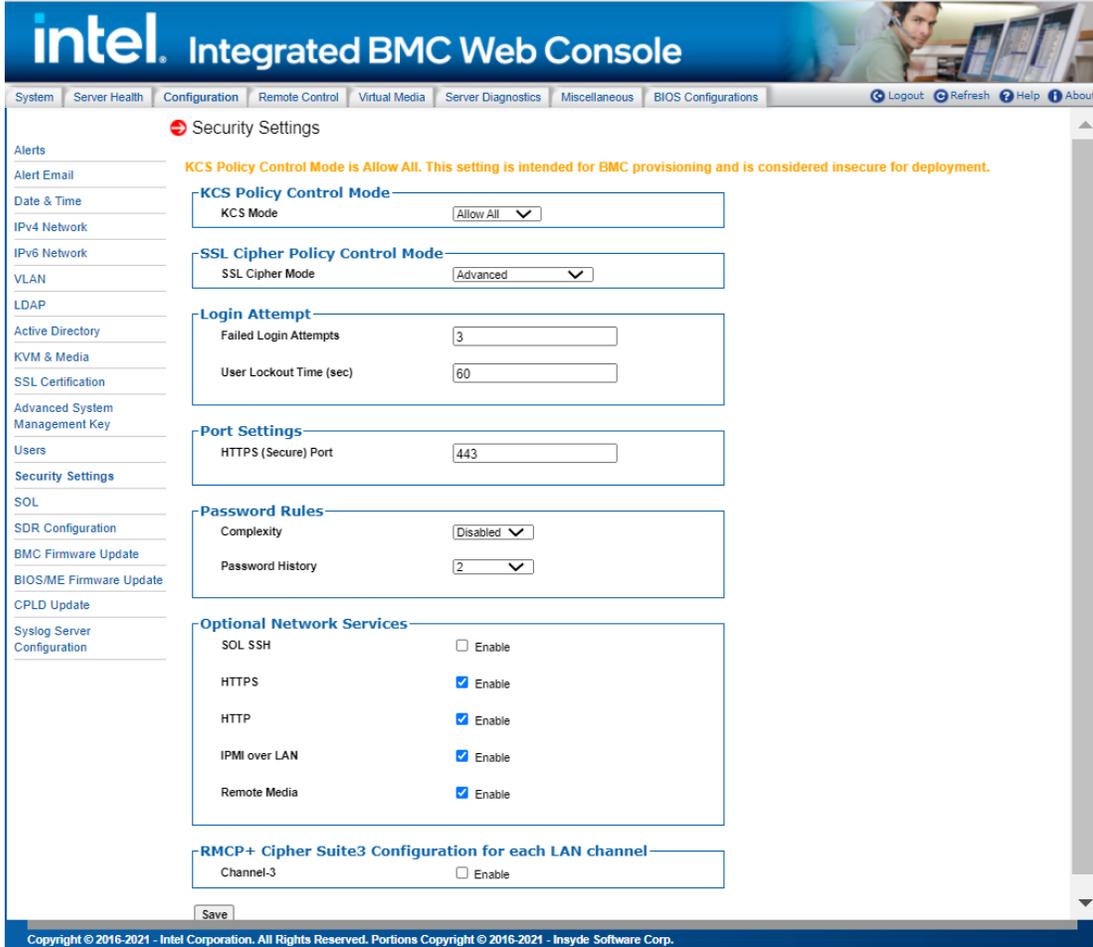


Figure 66. Configuration Security Settings page

Table 19. Configuration Security Settings Options

Option	Task
<p>KCS Mode</p>	<p>KCS Policy Control Modes allow an authenticated BMC administrative user to control the level of protection from IPMI commands executed over the KCS channels. Within this generation of BMC firmware, 3 different KCS Policy Control Modes are supported:</p> <ul style="list-style-type: none"> • Allow All - This configuration setting is intended for normal IPMI compliant communications between the Host OS 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 OS and the BMC. This is a non-compliant IPMI configuration that will impact the operation of the Server Management Software running on the Host OS. 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 OS to have access to a limited set of IPMI commands using the KCS interfaces. This is a non-compliant IPMI configuration that may impact the operation of the Server Management Software running on the Host OS. This only applies to the IPMI commands over the KCS interfaces and does not apply to the authenticated network interfaces to the BMC.

Option	Task
SSL Cipher Mode	<p>There are 4 Cipher modes provided for different scenarios:</p> <ul style="list-style-type: none"> Advanced - wide browser compatibility, e.g. to most newer browser versions. Board Compatibility - check the compatibility to other protocols before using it, e.g. IMAPS. Widest Compatibility - compatibility to most legacy browsers, legacy libraries (still patched) and other application protocols besides https, e.g. IMAPS. Legacy - widest compatibility to real 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 should be from 0 to 255. Default is 3 attempts.
User Lockout Time(Sec)	Set the time in seconds that the user is locked out before being allowed to login again. Zero means User Lockout Time is disabled. If a user was automatically disabled due to the Bad Password threshold, the user will remain disabled until re-enabled via the Set User Access command. User Lockout Time should be from 0 to 65535. Default is 60 sec.
HTTPS(Secure) Port	Set the port used for https (default: 443) web sessions. Changing this setting will immediately terminate all current web sessions.
Complexity	Set Complexity Password level, Medium/High/Low, or Disable Complexity Password feature.
Password History	The feature of password history is to avoid setting a password that is duplicate with one we used earlier for security consideration.
SOL SSH	Enable/disable the SOL SSH service.
HTTPS	Enable/disable the HTTPS service.
HTTP	Enable/disable the HTTP 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-2	Enable/Disable Cipher Suite3 Configuration for LAN Channel-2.
Channel-3	Enable/Disable Cipher Suite3 Configuration for LAN Channel-3.
Save	Click to save any changes.

Note: Due to weaknesses in the security of 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.

7.3.13.1 Integrated BMC Web Console access under KCS Restricted/Deny All Mode

Most of Integrated BMC Web Console content access is allowed across all KCS modes, except for below Integrated BMC Web Console Page/Options, which 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 OS and the BMC. This is a non-compliant IPMI configuration that will impact the operation of the Server Management Software running on the Host OS. 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 OS to have access to a limited set of IPMI commands using the KCS interfaces. This is a non-compliant IPMI configuration that may impact the operation of the Server Management Software running on the Host OS.

- Server Power Control Page: Power On Server/**Force-enter BIOS Setup** option will be grey out when KCS = Deny All
- Server Power Control Page: Reset Server/**Force-enter BIOS Setup** option will be grey out when KCS = Deny All

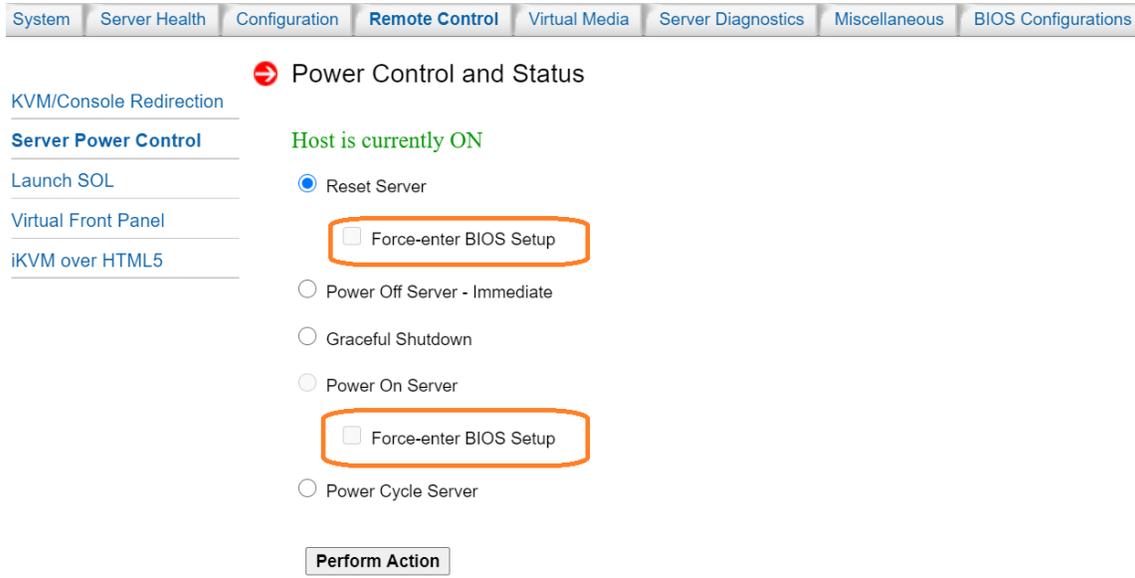
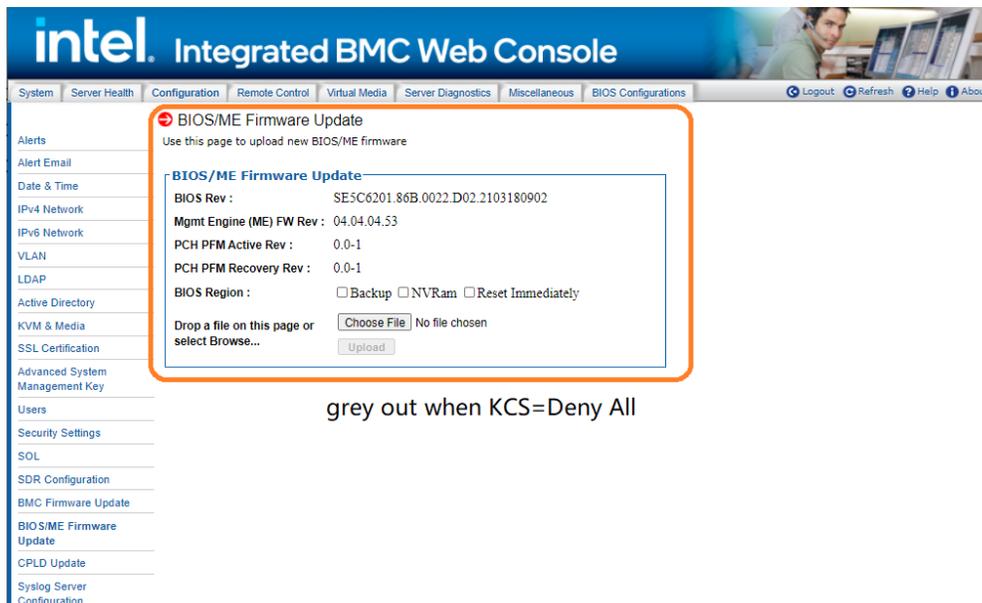


Figure 67. Server Power Control Page

- "BIOS/ME Firmware Update" Page will be grey out when KCS = Deny All.



grey out when KCS=Deny All

Figure 68. BIOS/ME Firmware Update Page

- "BIOS Configuration" will be unavailable when KCS = Restrict or Deny All mode.



Figure 69. BIOS Configuration Page

- "CPU information" and "DIMM information" Pages will display contents captured on last DC when KCS = Restricted or Deny All mode.

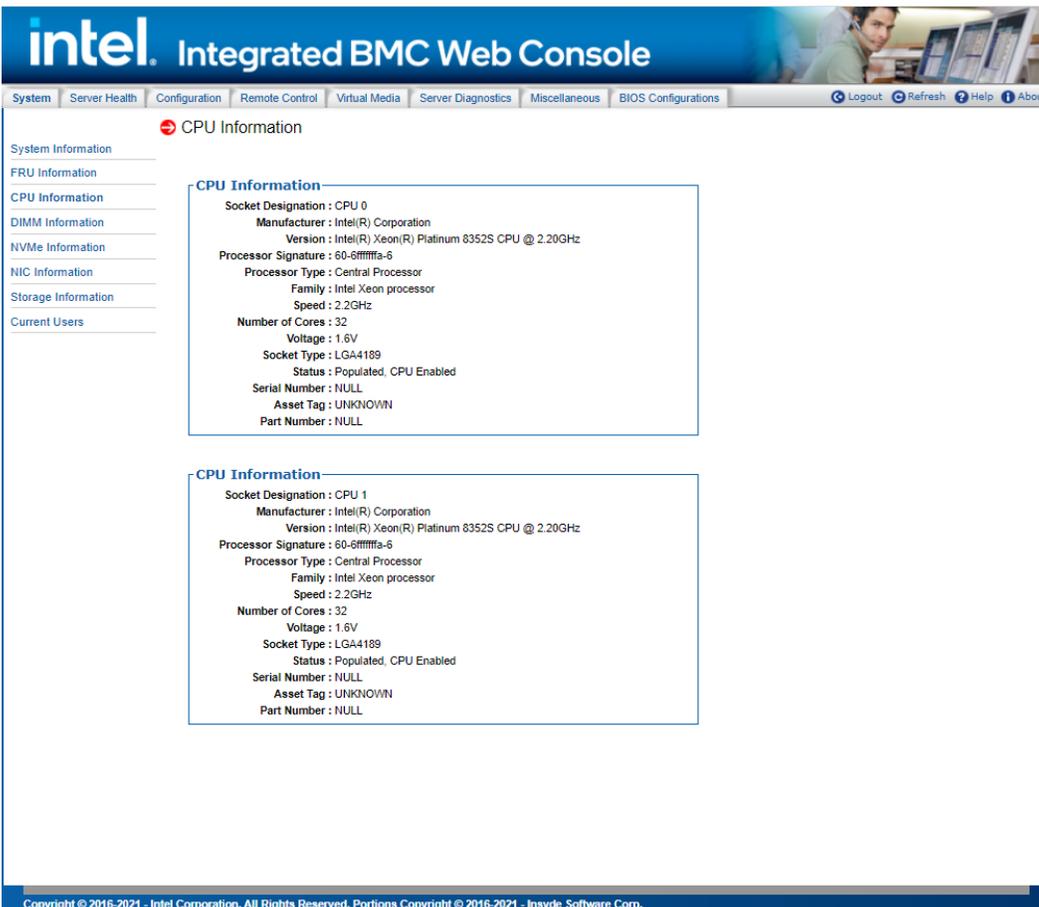


Figure 70. CPU Information Page



Figure 71. DIMM Information Page

7.3.14 SOL

Use this page to enable or disable SOL for each LAN channel (Figure 72). Table 20 lists the options to modify SOL settings.

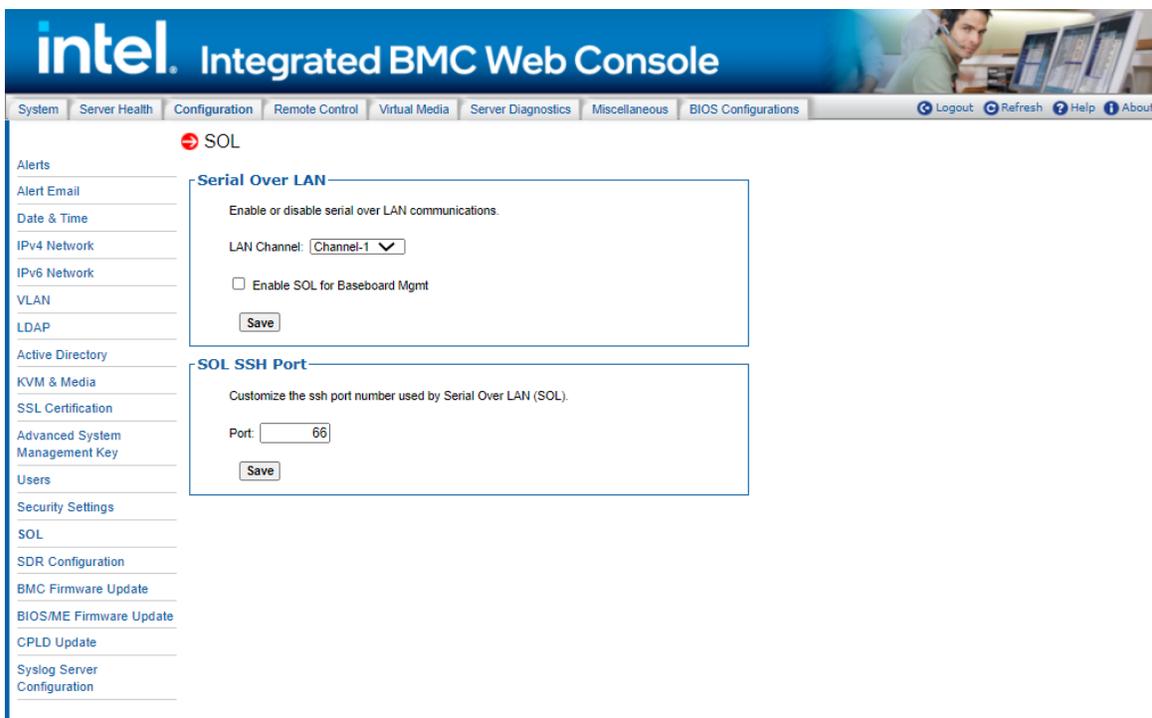


Figure 72. SOL Page

Table 20. SOL Options

Option	Task
LAN Channel	Select the channel on which you want to configure the network settings. Lists the LAN Channels available for SOL. The LAN channel describes the physical NIC connection on the server. <ul style="list-style-type: none"> • 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 Serial Over Lan for baseboard management controller.
Save (Serial Over LAN)	Click to save any changes for Serial Over LAN Setting.
Port	Change the SSH port number used by Serial Over LAN (SOL).
Save (SOL SSH Port)	Click to save any changes for SOL SSH Port Setting.

7.3.15 SDR Configuration

Use this page to upload and parse sensor data repository records and configuration files, which allows updating the FRUSDR package (Figure 73). Table 21 lists the options available on this page.

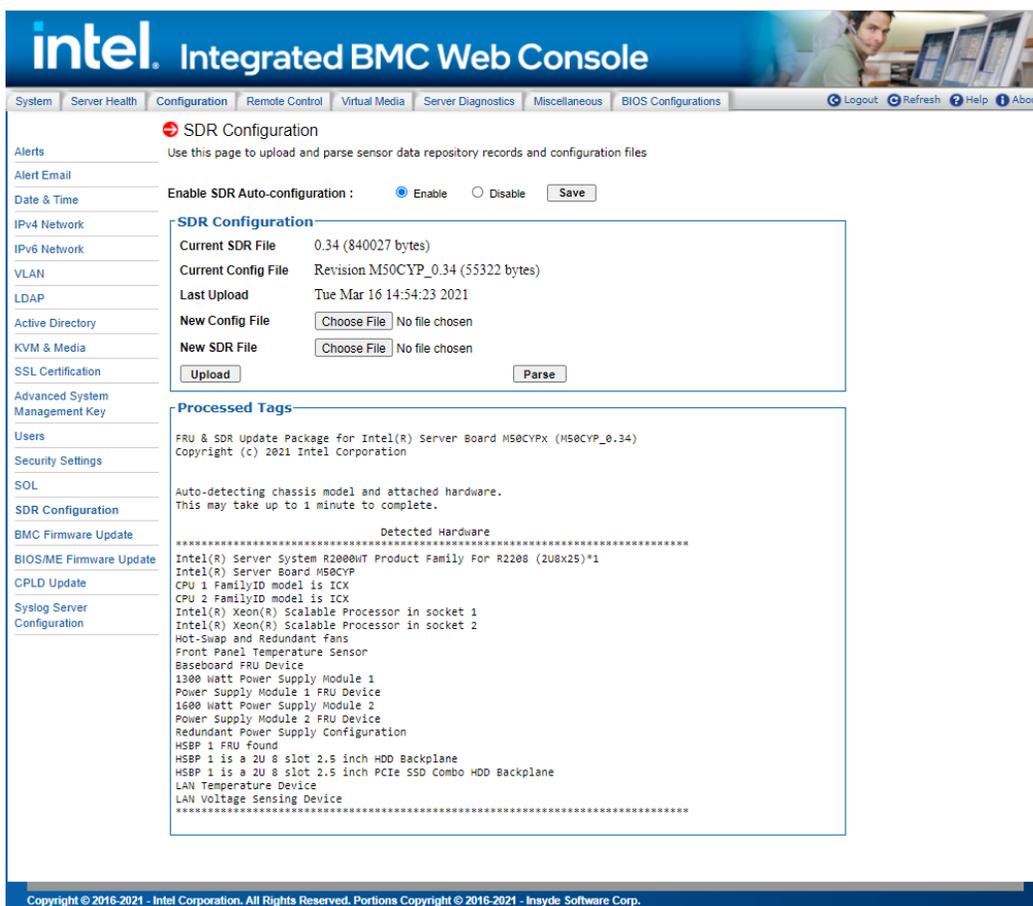


Figure 73. SDR Configuration Page

Table 21. SDR Configuration Options

Option	Task
Current SDR file	Information about the current SDR file is shown here. Version information is only available after a parse has been successfully completed.
Current Config File	Information about the current configuration file is shown here. Version information is only available after a parse has been successfully completed.
Last Upload	The date and time of the last FRUSDR update.
New Config File	Specify new configuration file to upload.
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 your network connection speed.
Parse	Scan and reload SDRs within the BMC. This will cause the BMC to re-arm sensors and may result in duplicate events in the system event log.
Processed Tags	This area shows tags processed on the last successful parse operation. If the parse fails, this area will display the error message.
Enable SDR Auto-configuration	Administrators or operators may enable or disable this feature by clicking the appropriate Enable/Disable radio button and clicking "Save." This section will only be visible to administrators or operators.
Save	Click to save any changes.

7.3.16 BMC Firmware Update

Use this page to upload new images for online-update of BMC firmware (Figure 74). Table 22 lists the options available in this page.

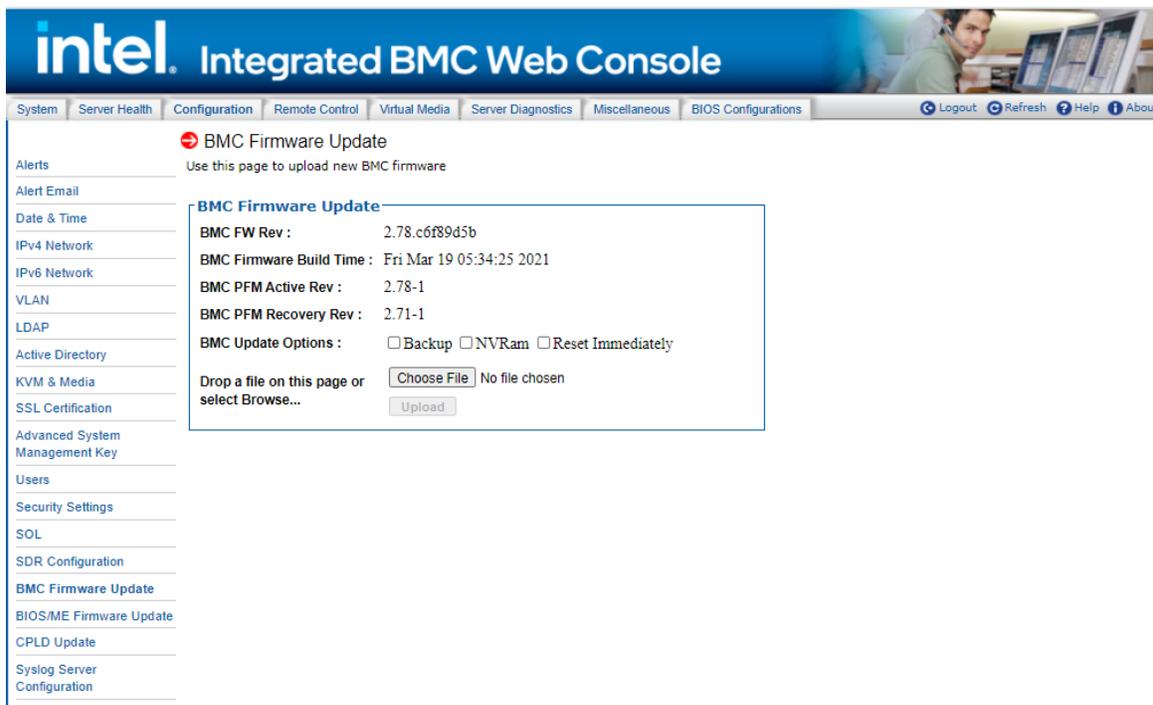


Figure 74. BMC Firmware Update Page

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
BMC PFM Active Rev	Displays the current PCH PFM active version.
BMC PFM Recovery Rev	Displays the current PCH PFM recovery version.
BMC Update Options	<ul style="list-style-type: none"> • Backup When the option is enabled, the Backup region of current BMC will be updated together. • Reset Immediately When the option is enabled, the system will reset immediately after the firmware update is completed. • NVRam When the option is enabled, the NVRam region of current BMC will be updated together.
Drop a file on this page or select Browse...	The option to select and upload or drop a new firmware image on the page.
Upload	Begin the firmware update process, which will take a couple of minutes. When finished the BMC reboots to run the new firmware. Progress is reported up until the time of reboot, after which it takes about one minute for the embedded web server to start responding again. As all web sessions are terminated on a BMC reboot, log in again to verify that the firmware update was successful.

7.3.17 BIOS/ME Firmware Update

Use the BIOS/ME Firmware update page shown in Figure 75 to upload and update new BIOS/ME firmware. The image version information is available for viewing, as well as the option to select, upload, or drag and drop a new firmware image. By dropping a new image on the page or selecting the **Upload** button, the web service takes a few minutes and begins its firmware update process. Once finished, it stores the image inside the BMC. When performing the update server reboot (DC cycle), the BIOS mounts the image as both the USB virtual media and the image. See Table 23 for all options available on this page.

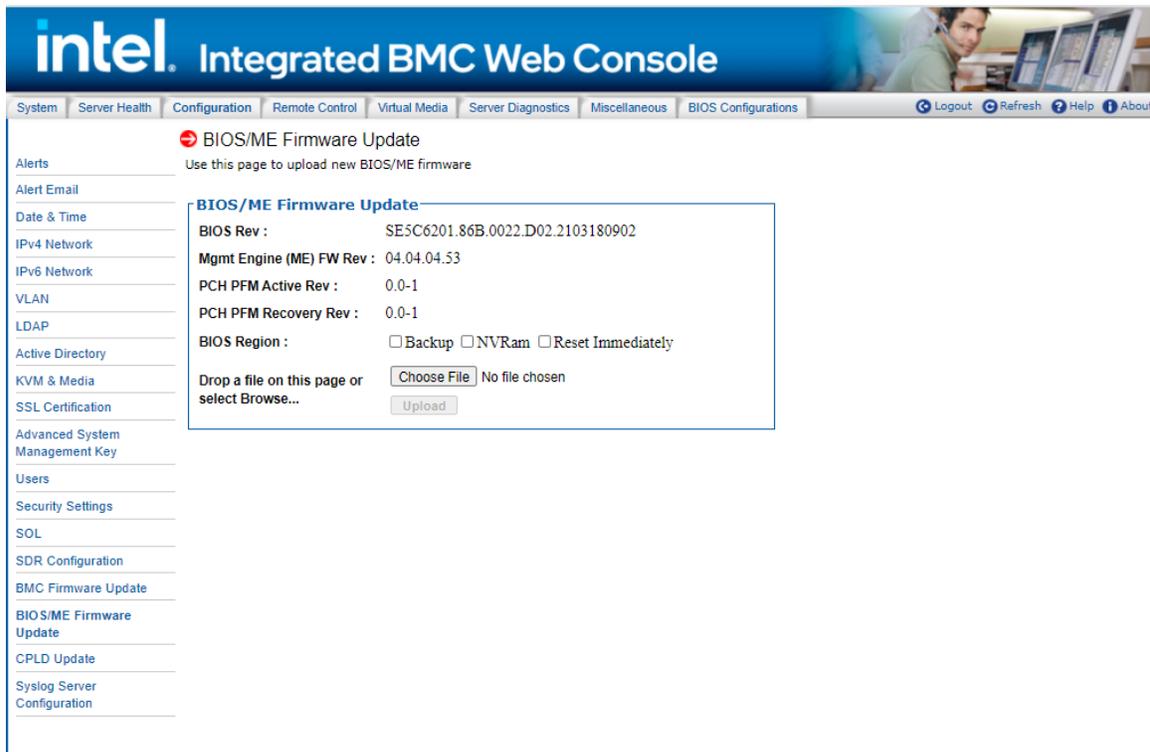


Figure 75. BIOS/ME Firmware Update Page

Table 23. BIOS/ME Firmware Update Options

Option	Task
BIOS Rev	Displays the current BIOS version.
Mgmt Engine (ME) FW Rev	Displays the current ME firmware version.
PCH PFM Active Rev	Displays the current PCH PFM active version.
PCH PFM Recovery Rev	Displays the current PCH PFM recovery version.
BIOS Region	<ul style="list-style-type: none"> • Backup When the option is enabled, the Backup region of current BIOS will be updated together. • NVRam When the option is enabled, the NVRam region of current BIOS will be updated together. • Reset Immediately When the option is enabled, the system will reset immediately after the firmware update is completed.
Password	The option will appear when "Enforce Password Mode" is Enabled in BIOS. Users should input password before uploading the image.
Drop a file on this page or select Browse...	The option to select and upload or drop a new firmware image on the page.
Upload	Upload the firmware image file.

7.3.18 CPLD Update

Use this page to upload new CPLD firmware in Figure 76. Table 24 lists the options available in this page.

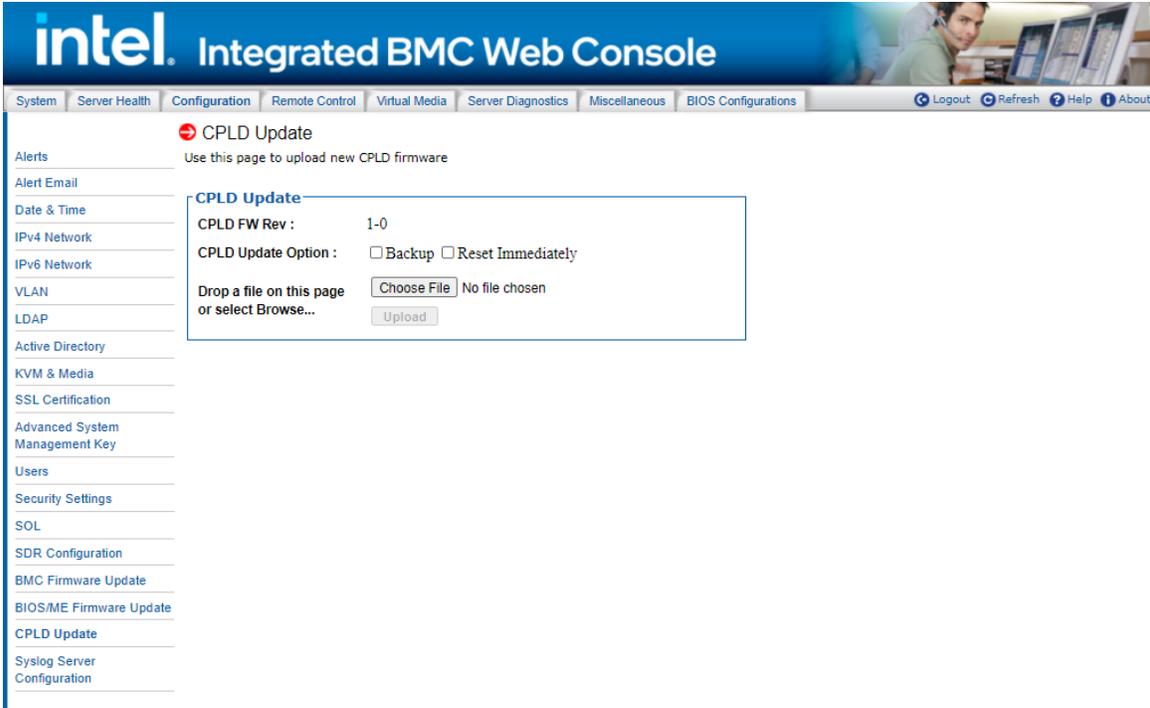


Figure 76. CPLD Update Page

Table 24. CPLD Update Options

Option	Task
CPLD FW Rev	Displays the current firmware version.
CPLD Update Option	<ul style="list-style-type: none"> • Backup When the option is enabled, the Backup region of current CPLD will be updated together. • Reset Immediately When the option is enabled, the system will reset immediately after the firmware update is completed.
Drop a file on this page or select Browse...	The option to select and upload or drop a new firmware image on the page.
Upload	Upload the firmware update image file to the BMC for update action.

7.3.19 Syslog Server Configuration

Use the Syslog Server Configuration page to enable the Remote Syslog service or to configure the IP of the Syslog Server. This page allows the logging of any login to the BMC or any configurations to be logged to the Syslog server. See Table 25 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 Modload `imudp/UDPSeverRun 514/ModLoad imtcp/InputTCPSeverRun 514`
3. Service `syslog` restart
4. Set syslog server from Integrated BMC Web Console --> Configuration--> Syslog Server Configuration
5. `Cat /var/log/messages` to see log

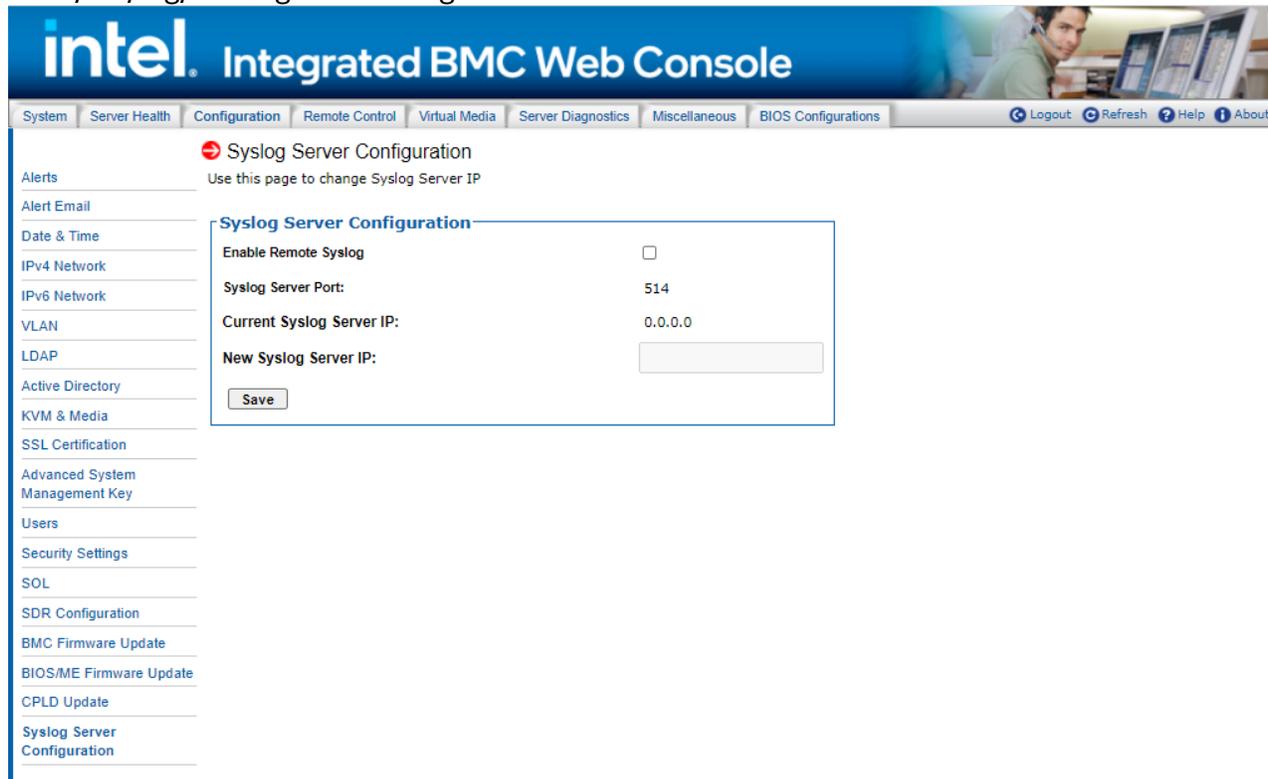


Figure 77. Syslog Server Configuration Page

Table 25. Syslog Server Configuration Options

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

7.4 Remote Control Tab

The Remote Control tab is used 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 a Remote Management Module add-in card to be installed in the remote system; otherwise, the launch button is grayed-out. Clicking on **Launch Console** prompts to download a `launch.jnlp` file. When the file is downloaded and launched, the Java* redirection window is displayed. Figure 78 shows the details.

Note: Java* Runtime Environment* (JRE* Version 6 Update 22 or higher) must be installed on the client before launch of the JNLP file.

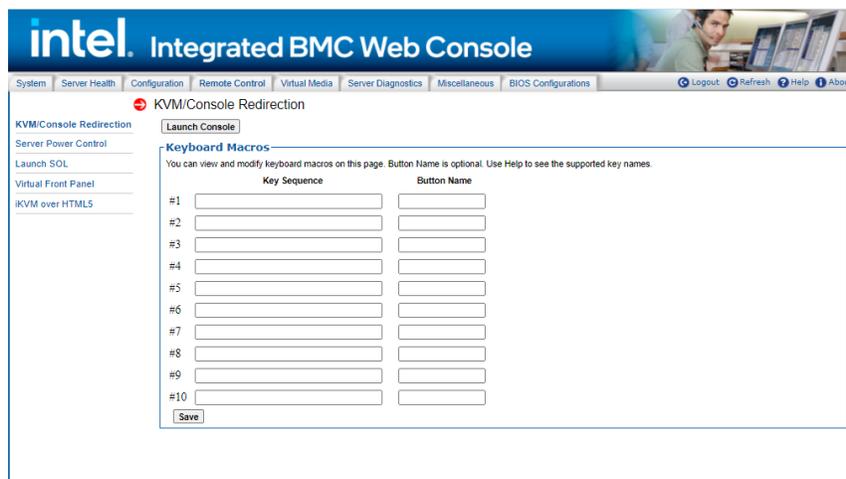


Figure 78. Remote Control KVM Page

Keyboard macros can be configured on this page that appear in the macro menu of the KVM Remote Console application window. Each button is assigned a sequence of keys to execute when the button is clicked.

Each button can optionally be given a short mnemonic name. If this field is blank, the key sequence itself is used as the button label.

Click **Save** to save the changes. If a Remote Console session is open at that time, the changes do not take effect until that session is closed and a new session is opened.

7.4.1.1 Key Sequences

A key sequence is a set of one or more key names separated by a '+' or '-'.

A '+' (plus sign) indicates keep the previous keys pressed while holding down the next key, whereas a '-' (minus sign) indicates release all previous keys first before pressing the next key. A '*' (asterisk) inserts a one second pause in the key sequence.

Key names are either a printable character such as "a", "5", "@", etc. or one of the non-printable keys in the table below. Names in parentheses are aliases for the same key. Numeric keypad keys are prefixed with "NP_".

A plain '*' indicates a pause. Use '*' for the actual '*' key. The '\' key must also be escaped as '\\'.

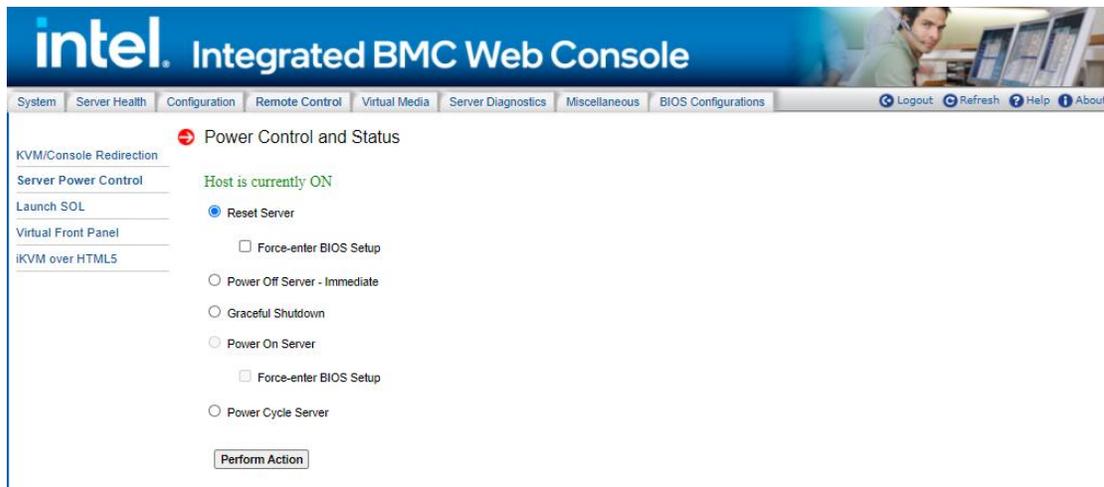
Note: The key sequences are sent to the target as scan codes that get interpreted by the target OS, so they will be affected by modifiers such as Num Lock as well as the target OS keyboard language setting.

Table 26. Macro Non-Printable Key Names

Shift (LShift)	RShift	Ctrl (LCtrl)	RCtrl
Alt (LAlt)	RAlt (AltGr)	Win (LWin)	RWin
Enter	Esc	F1 - F12	
Bksp	Tab	CapsLk	Space
Ins	Del	Home	End
PgUp	PgDn	Context (Menu)	
Up	Left	Down	Right
NumLk	NP_Div	NP_Mult	NP_Minus
NP_Plus	NP_0 - NP_9	NP_Dec	NP_Enter
PrtSc (SysRq)	ScrLk	Pause (Break)	

7.4.2 Server Power Control

The Server Power Control page shows the power status and allows power/reset control of the server Figure 79. Table 27 lists the power control operations that can be performed.

**Figure 79. Remote Control Server Power Control Page****Table 27. 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. For the Graceful Shutdown option to function properly the OS 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. Intel suggests to gracefully shut down the operating system using the KVM interface or other interface before initiating 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 download a `launch.jnlp` file. When the file is downloaded and launched, the Java* SOL window is displayed. See Figure 80 details.



Figure 80. Remote Control Launch SOL Page

Starting the SOL console opens an additional window as shown in Figure 81. It displays the screen content of the remote server. The SOL console behaves as if you were connected to a serial terminal on the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between Integrated BMC Web Console and remote console.

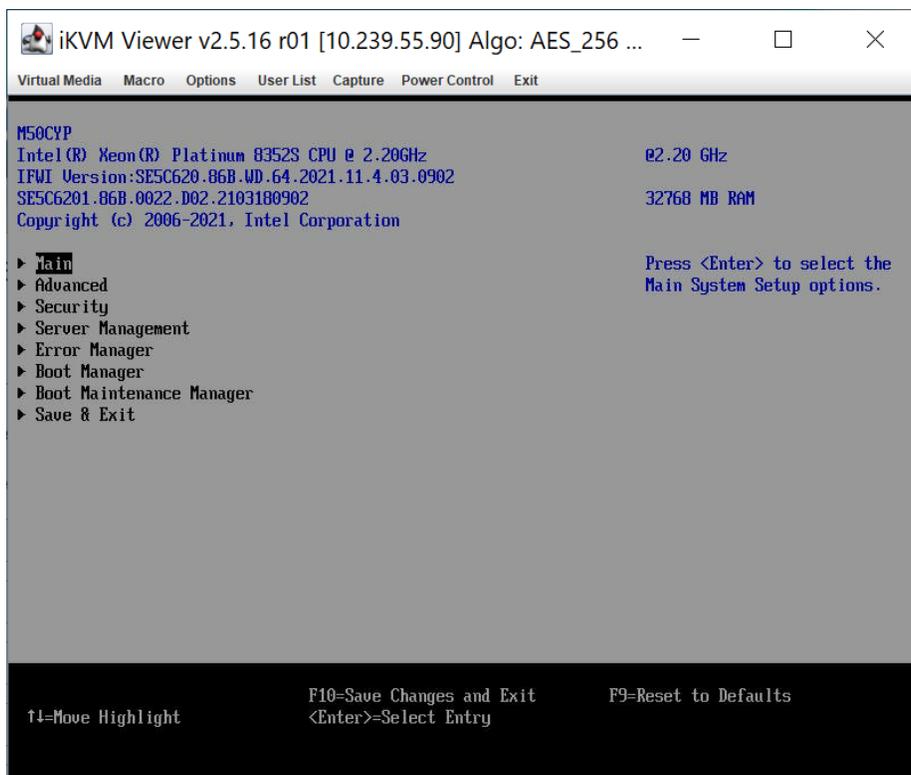


Figure 81: Remote Control Launch SOL Screen Page

Note: Make sure to enable SOL for 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 functionality just like the systems front panel (Figure 82). Table 28 lists the power control operations that can be performed.



Figure 82: Remote Control Virtual Front Panel Page

Table 28. Remote Control Virtual Front Panel Options

Option	Task
Power	Power on or power off.
Reset	Reset the server while system is ON.
Chassis ID	When the Chassis ID button is pressed, the chassis ID LED changes to solid on. If the button is pressed again, the chassis ID LED turns off.
Power LED	The power LED shows the system power status. If the Power LED is green, the system is ON. If the Power LED is gray, the system is OFF.
Status LED	The status LED reflects the system status LED status and it is automatically in sync with the BMC every 60 seconds. This reflects the System Status LED.
Chassis ID LED	The Chassis ID LED shows the current system chassis ID status. If the Chassis ID LED is blue, the Chassis ID is ON. If the Chassis ID LED is gray, the Chassis ID is OFF.

7.4.5 iKVM over HTML5

Launch the remote iKVM over HTML5 redirection window from this page, accessing the two menus listed within: **Keyboard** and **Power Control**.

The two sub-menus within the **Keyboard** menu are:

- **Virtual Keyboard:** Click the submenu **Virtual Keyboard** within the **Keyboard** menu to display a soft keyboard, shown in Figure 85.
- **Keyboard Macro:** Click the submenu **Keyboard Macro** within the **Keyboard** menu to open the keyboard macro menu, shown in Figure 86.

The four sub-menus within the **Power Control** menu (shown in menu shown in Figure 87) are:

- **Power On:** Click the **Power On** menu to start the system.
- **Power Off:** Click the **Power Off** menu to turn the system off.
- **Software Shutdown:** Click the **Software Shutdown** menu to gracefully shut down the system.
- **Power Reset:** Click the **Power Reset** menu to reset the system.

Note: A Remote Management Module add-in card is required in the remote system, otherwise the launch button is grayed-out. See Figure 83 or Figure 84 for more details.

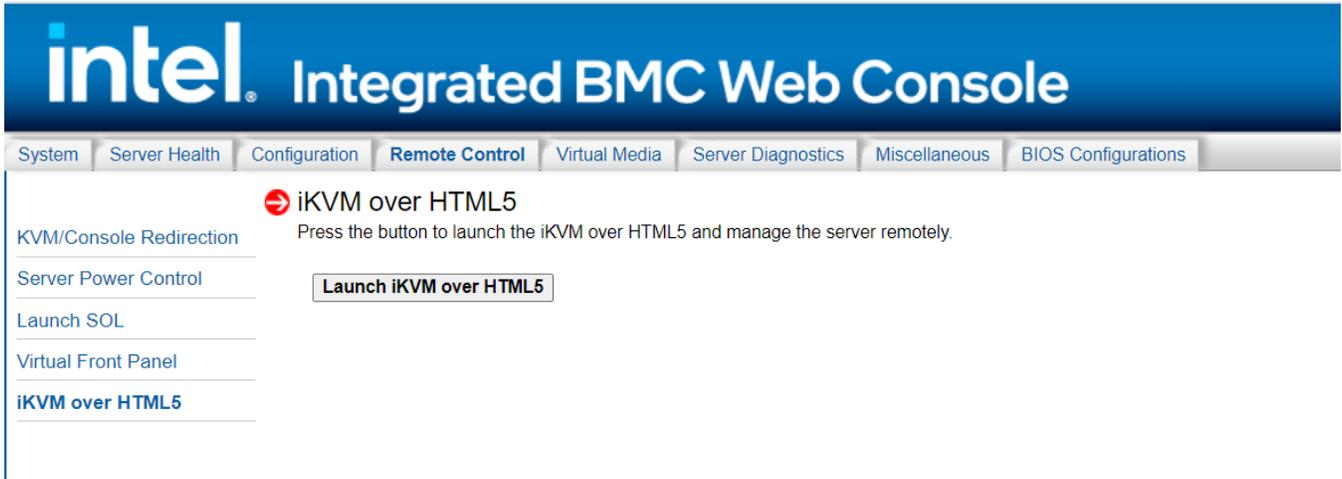


Figure 83. iKVM Over HTML5 Page

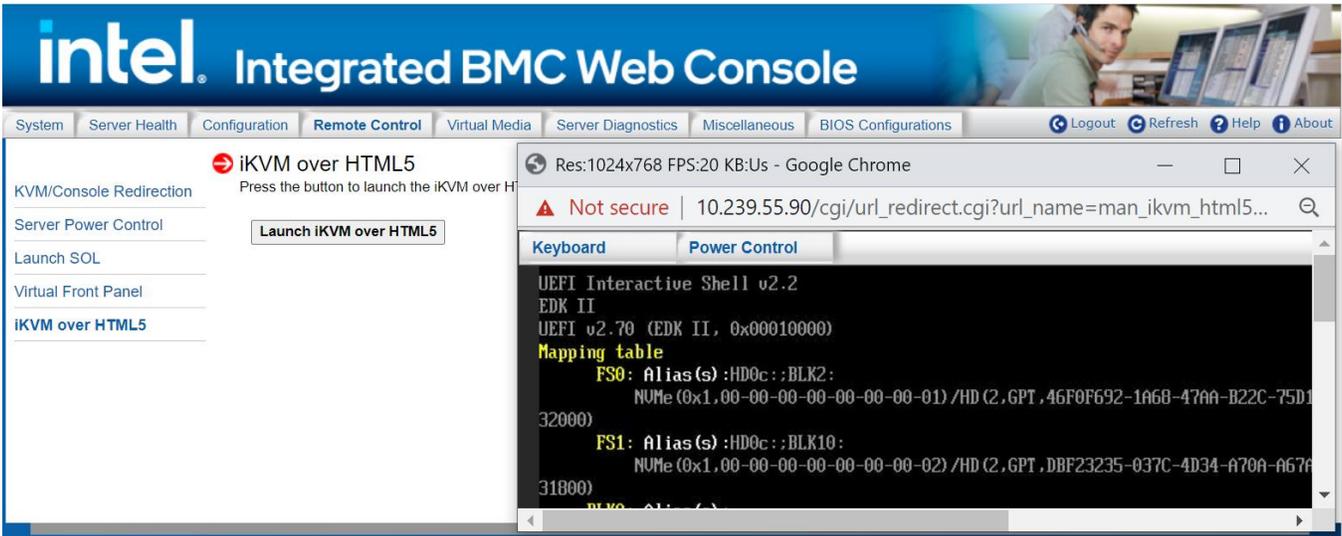


Figure 84: HTML5 Screen Page



Figure 85: HTML5 Virtual Keyboard Page

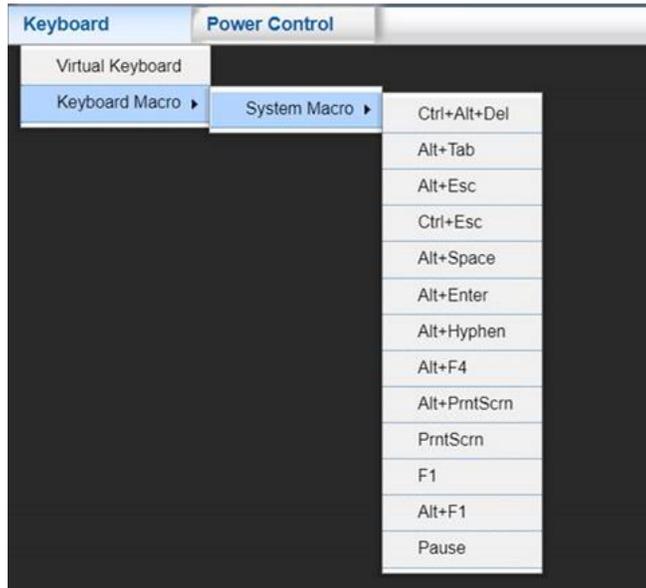


Figure 86: HTML5 Keyboard Macro menu page

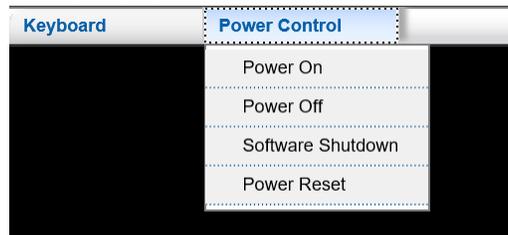


Figure 87: HTML5 Power Control menu page

7.5 Virtual Media Tab

The Virtual Media tab allows you to share an ISO image or folder over HTML5, which only includes one Virtual Media over HTML5 page. Each image/folder is emulated to the host as a USB device with the maximum sizes of 4.7GB for ISO images, and 2GB for folders. See Figure 88 for more details.

To open the operation window, click **the Launch virtual media over HTML5** as shown in Figure 89. To upload ISO files to the BMC over HTML5, click the **Browse** button. Up to three devices may be mounted simultaneously.

Note: A Remote Management Module add-in card is required in the remote system, otherwise the **launch virtual media over HTML5** button is grayed-out.



Figure 88. Virtual Media Over HTML5 Page

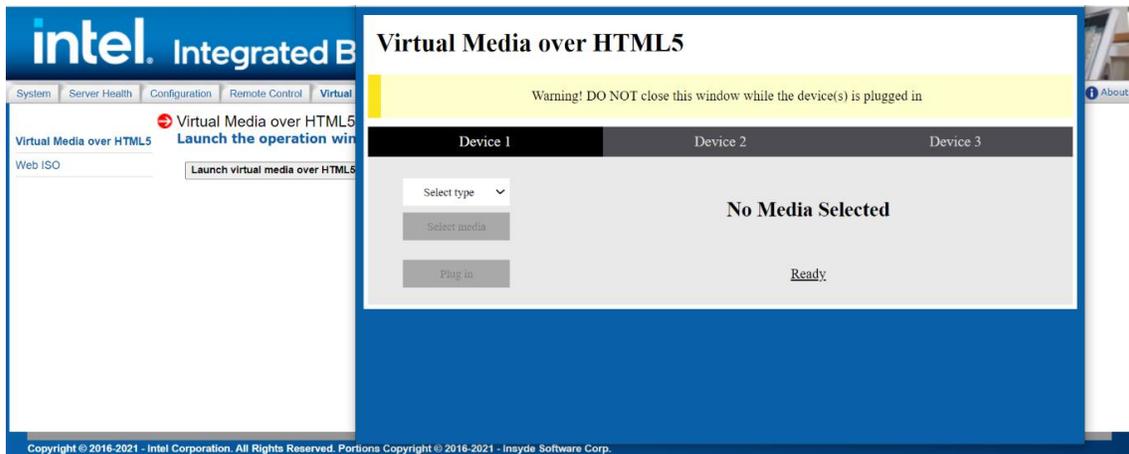


Figure 89. Launch Virtual Media Over HTML5 Page

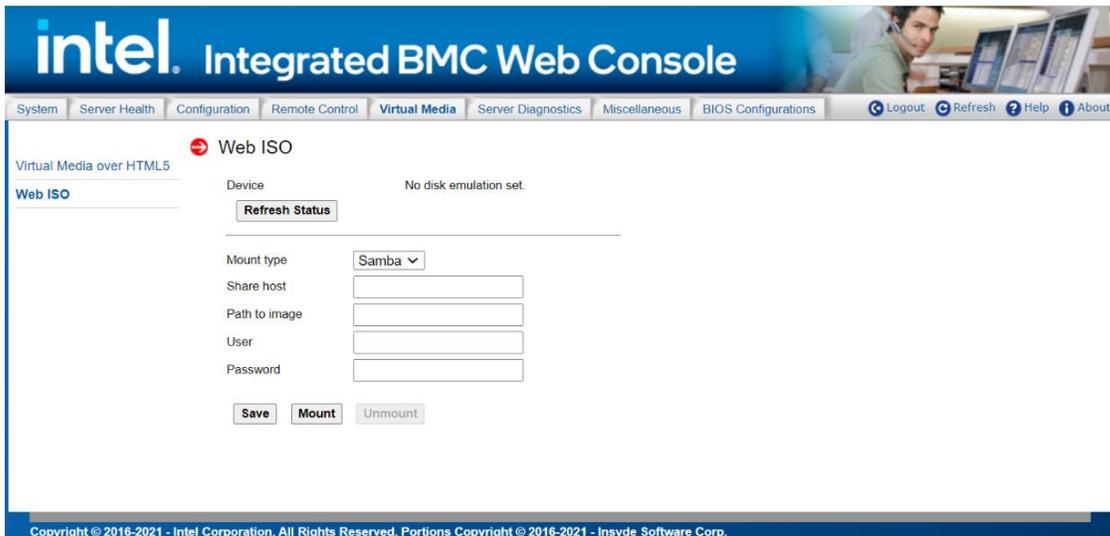


Figure 90. Web ISO

7.6 Server Diagnostics Tab

The Server Diagnostics tab contains general system diagnostics information as explained in the following sub sections.

7.6.1 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 for the purpose of sending to an Intel engineer or Intel partners 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 rather provide additional debugging capability to the system manufacturer or an Intel support engineer. See Figure 91 for details.

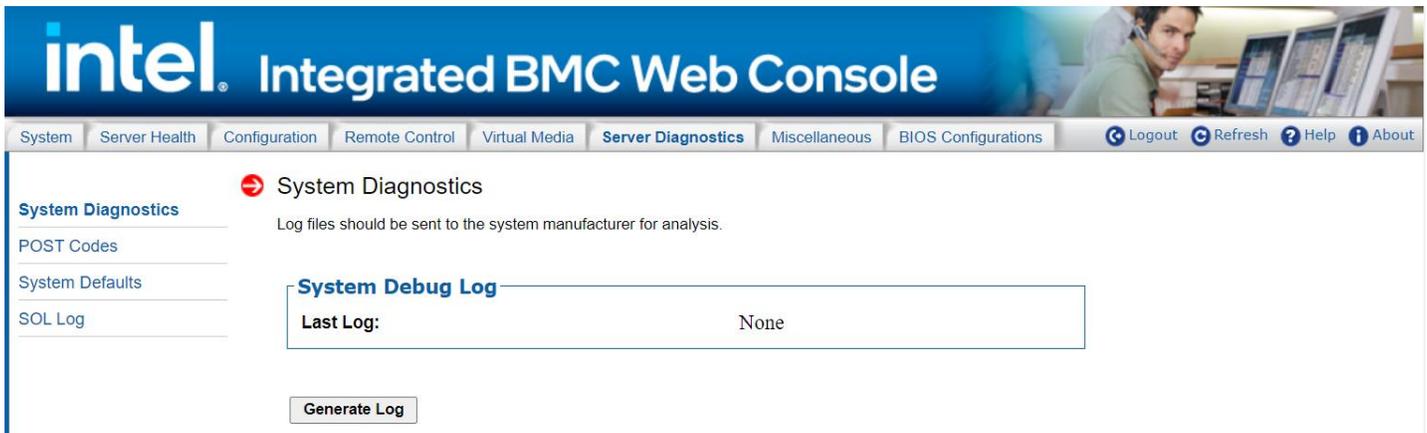


Figure 91. Server System Diagnostics Page

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 an Intel support engineer for analysis.

The data that may 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 FW and have associated SDRs populated in the SDR repository. This does not include any “event-only” sensors. (All BIOS sensors and some BMC and Intel® ME sensors are “event-only”, meaning that they 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.

7.6.2 POST Codes

The POST Codes page displays recent power-on self-test (POST) results. See Figure 92 for details. The time base may be viewed as the time from start of POST, or 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 a time, POST code, or description causes the highlighting to persist until another code is clicked.

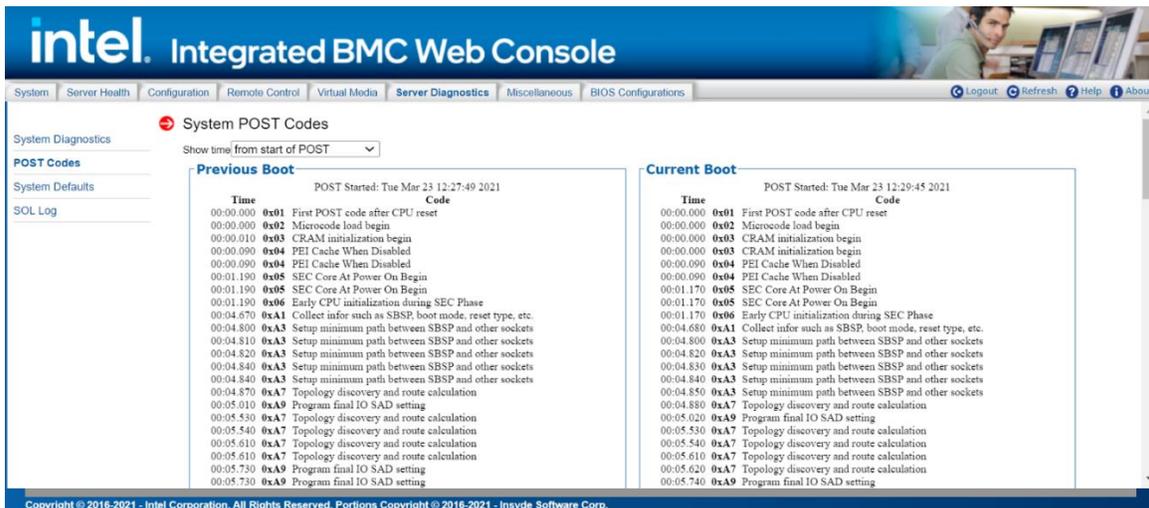


Figure 92. Server Diagnostics POST Codes Page

7.6.3 System Defaults

The System Defaults page allows resetting all BMC settings to factory defaults. See Figure 93 for details. Click the **Restore** button to reset all BMC settings to factory defaults. Once complete, all remote management, including the web server, will not be 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 Node Manager Settings and policies.



Figure 93. Server Diagnostics Default Page

Check "**Keep User and LAN configuration**" to reset other BMC settings to factory defaults, and retain the current user and LAN settings.

WARNING: This action will reset all BMC settings to factory defaults and cannot be undone.

7.6.4 SOL Log

The SOL Log page allows enabling/disabling SOL logging and downloading the log (Figure 94). Table 29 lists the SOL log operations that can be performed.

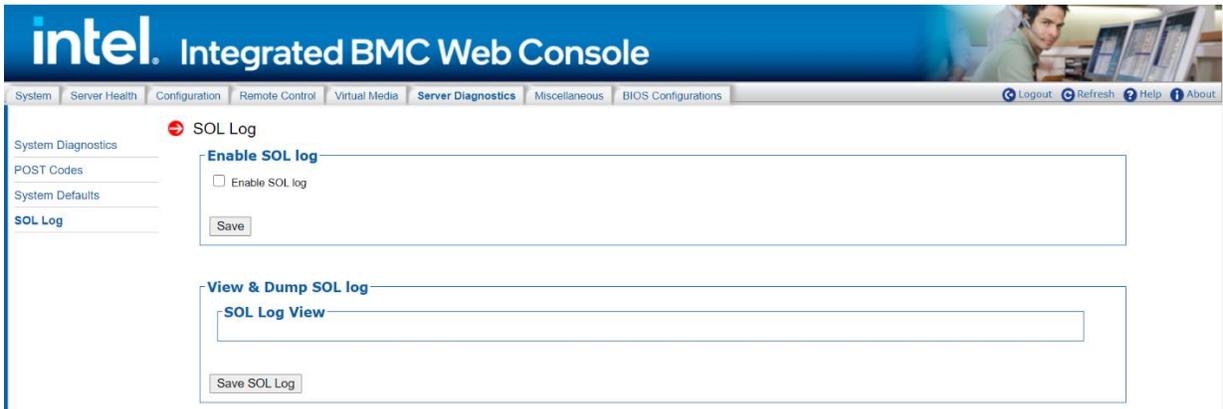


Figure 94. Server Diagnostics SOL Log Page

Table 29. Server Diagnostics SOL Log Options

Option	Task
Enable SOL Log	Enable or disable SOL log.
Save Button for Enable SOL Log	Save the setting of enable/disable SOL log.
Save SOL Log Button for Enable SOL Log	Save the log to the local device.

7.7 Miscellaneous Tab

The **Miscellaneous** tab contains Intel® Node Manager (Intel® NM) configuration, power statistics and power telemetry information as explained in the following sub sections.

7.7.1 NM Configuration

Intel NM configuration is used to view, add and configure the Intel Node Manager Policies. See Figure 95 for details. Table 30 lists the options to view, add, and edit the Intel NM power policies.



Figure 95. Intel® NM Configuration Page

Table 30. Intel® NM Configuration Options

Option	Task
List of Policies	This table lists the currently configured policies. Selecting an item from the table will populate 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 will 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 initiates an immediate shutdown.
Log Event	Enable the node manager to send a platform event message to the BMC when a policy is exceeded.
Power Limit (Watt)	The desired platform power limit, in watts.
Use Policy Suspend Periods	If enabled, configure policy suspend periods. Each policy may have up to five suspend periods (see Figure 96). 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 will be applied:

- **Domain:** Platform – Power for the entire platform.
- **Trigger:** None – Always monitor after 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 will not affect the average power monitored by the node manager.
- **Correction Timeout:** 22.555 seconds – Maximum time for the NM to correct power before taking an exception action (that is, shutdown or alert).

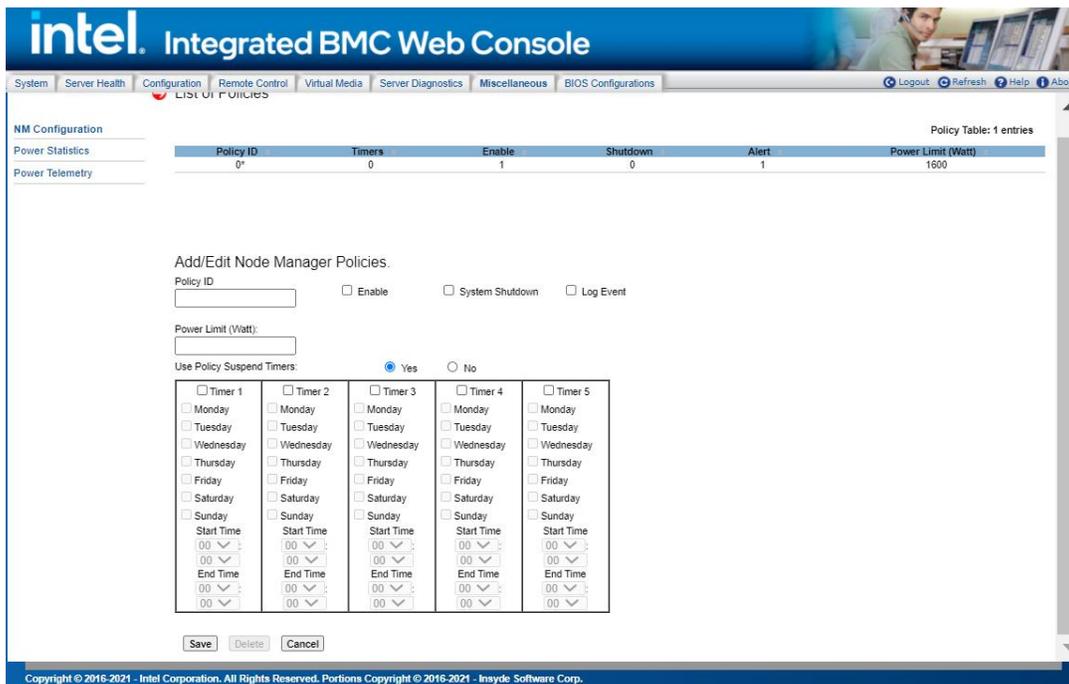


Figure 96. Intel® NM Configuration Suspend Page

7.7.2 Power Statistics

The Power Statistics page displays the entire platform, CPU and memory power statistics as shown with current, average, maximum, minimum, time stamp and period in Figure 97.

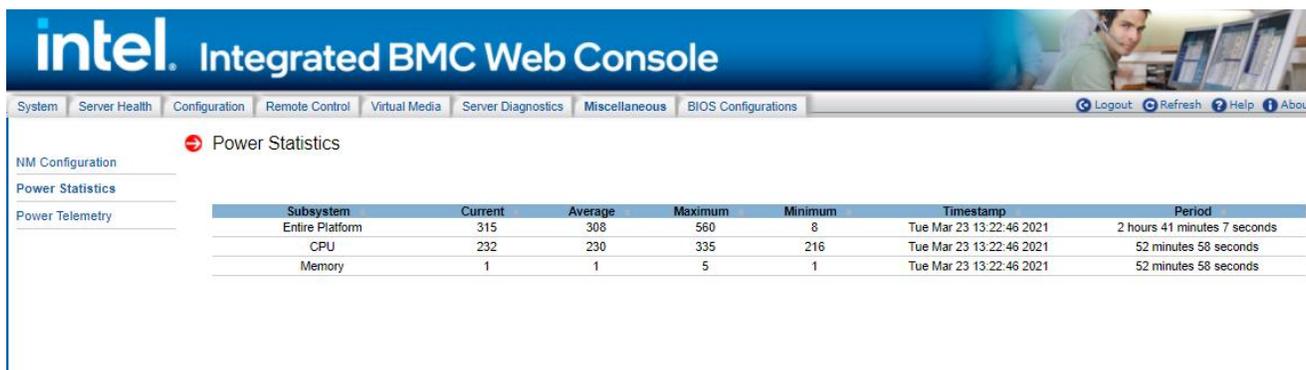


Figure 97. Power Statistics Page

7.7.3 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 98 for details. To select a device category, use the **Select a device category** drop-down box (Figure 99).

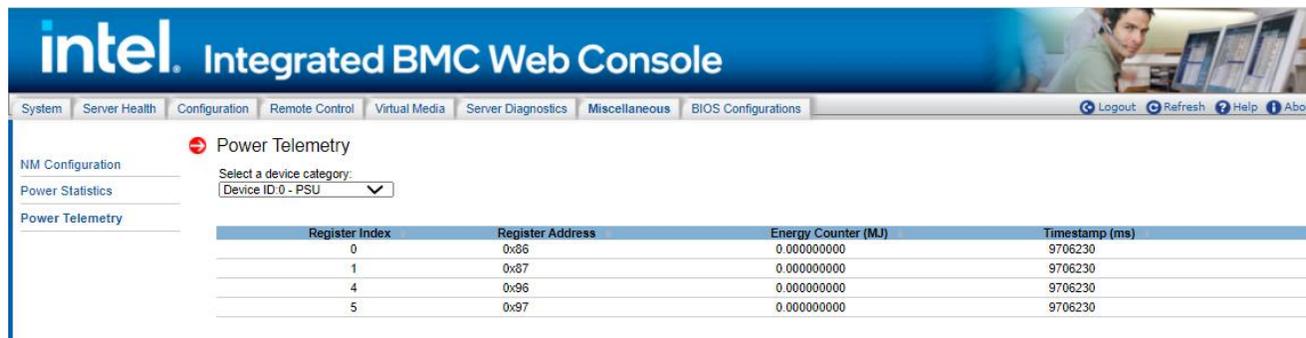


Figure 98. Power Telemetry Page

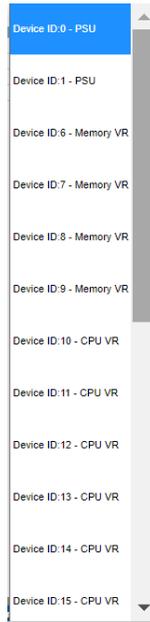


Figure 99. Power Telemetry Device Categories

7.8 BIOS Configurations Tab

The **BIOS Configurations** tab provides a method to configure any BIOS Setup Variables through the BMC Integrated BMC Web Console, containing the PCI, Serial Port, UPI, IIO, Memory, PnP, Processor, Mass Storage Controller, System Acoustic and Performance, SEL, Security and USB configuration options. To select a BIOS variable, click the **Select a BIOS Variable** drop-down menu. Once a BIOS Variable is selected, the corresponding BIOS Variables Current Value will be displayed in the **BIOS Variable Value** drop-down box. Other available options for the corresponding BIOS Variable can be viewed by clicking the **BIOS Variable Value** drop-down box, and 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 will then be reflected in the Grid Table.

7.8.1 PCI Configuration

This page allows the user to enable or disable MMIO above 4G/MMIO High base/MMIO Size/Add in video controller/Onboard Video/Fast video/Onboard VGA Always O/ARI Support/SR-IOV Support/UEFI Network Stack/IPv4 PXE Support/IPv6 PXE Support/CPU VMD and so on. See Figure 100 for details.

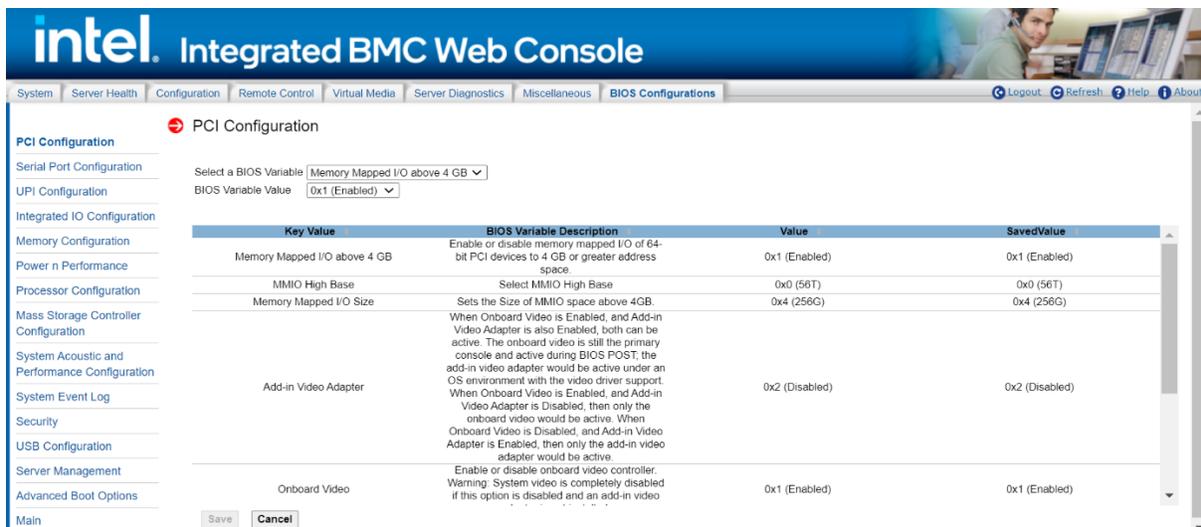


Figure 100. BIOS PCI Configuration Page

7.8.2 Serial Port Configuration

This page allows the user to enable or disable serial port, select serial base I/O address. See Figure 101 for details. Table 31 lists all serial port configuration variables that can be viewed and edited.

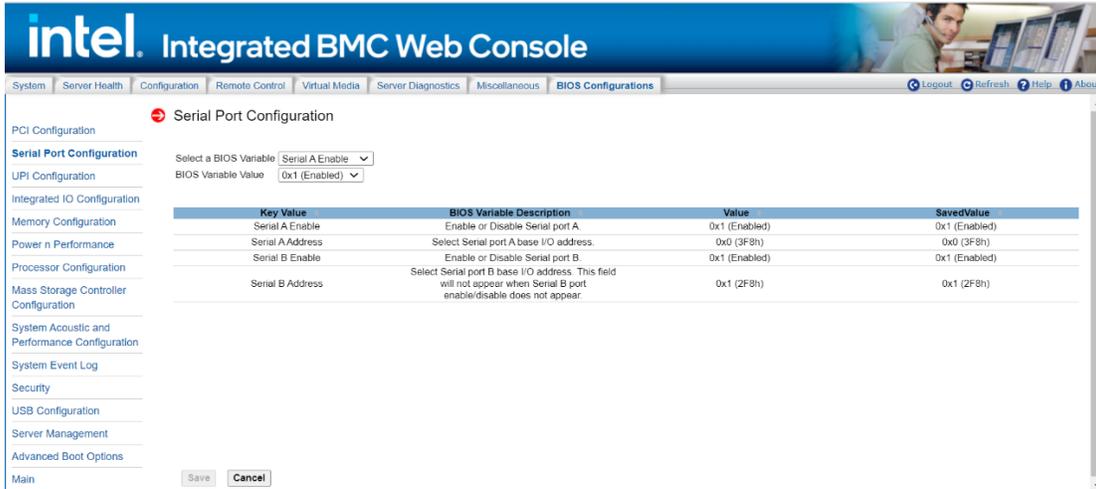


Figure 101. BIOS Serial Port Configuration Page
Table 31. BIOS Serial Port Configuration Variables

Variables	BIOS Variable Description
Serial A Enable	Enable or Disable Serial port A.
Serial A Address	Select Serial port A base I/O address.
Serial B Enable	Enable or Disable Serial port B.
Serial B Address	Select Serial port B base I/O address. This field will not appear when Serial B port enable/disable does not appear

7.8.3 UPI Configuration

This page allows the user to select the UPI frequency/ IO Directory Cache(IODC)/KTI Prefetch/Stale A to S Dir optimization/LLC dead line allocation/Direct To Core(D2C) /Direct To UPI(D2K). See Figure 102 for details. Table 32 lists all UPI configuration variables that can be viewed and edited.

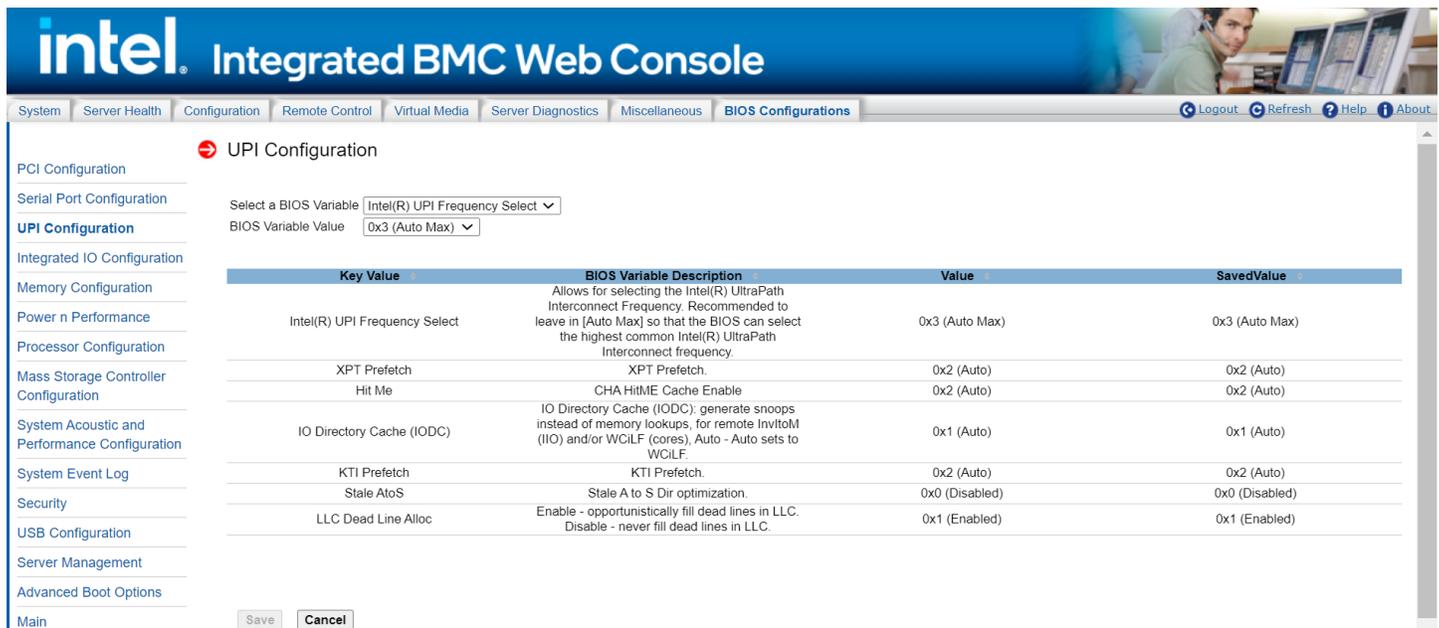


Figure 102. BIOS UPI Configuration Page

Table 32. BIOS UPI Configuration Variables

Variables	BIOS Variable Description
Intel(R) UPI Frequency Select	Select UPI frequency from 0x1(Auto Max), 0x0(9.6GT/s), 0x1(10.4GT/s).
IO Directory Cache(IODC)	Enable or disable IO Directory Cache(IODC).
KTI Prefetch	Enable or disable KTI Prefetch.
Stale AtoS	Enable or disable Stale AtoS.
LLC Dead Line Alloc	Switch the LLC Dead Line Alloc mode to enable, disable or auto.
Direct To Core(D2C)	Switch the Direct To Core(D2C) mode to enable, disable or auto.
Direct To UPI(D2K)	Switch the Direct To UPI(D2K) mode to enable, disable or auto.

7.8.4 Integrated IIO Configuration

This page allows the user to configure NTB PCIe* port and BAR23/4/5/45 size, enable/disable NTB Bars/SPLIT Bars. See Figure 103 for details. Table 33 lists all IIO configuration variables that can be viewed and edited.

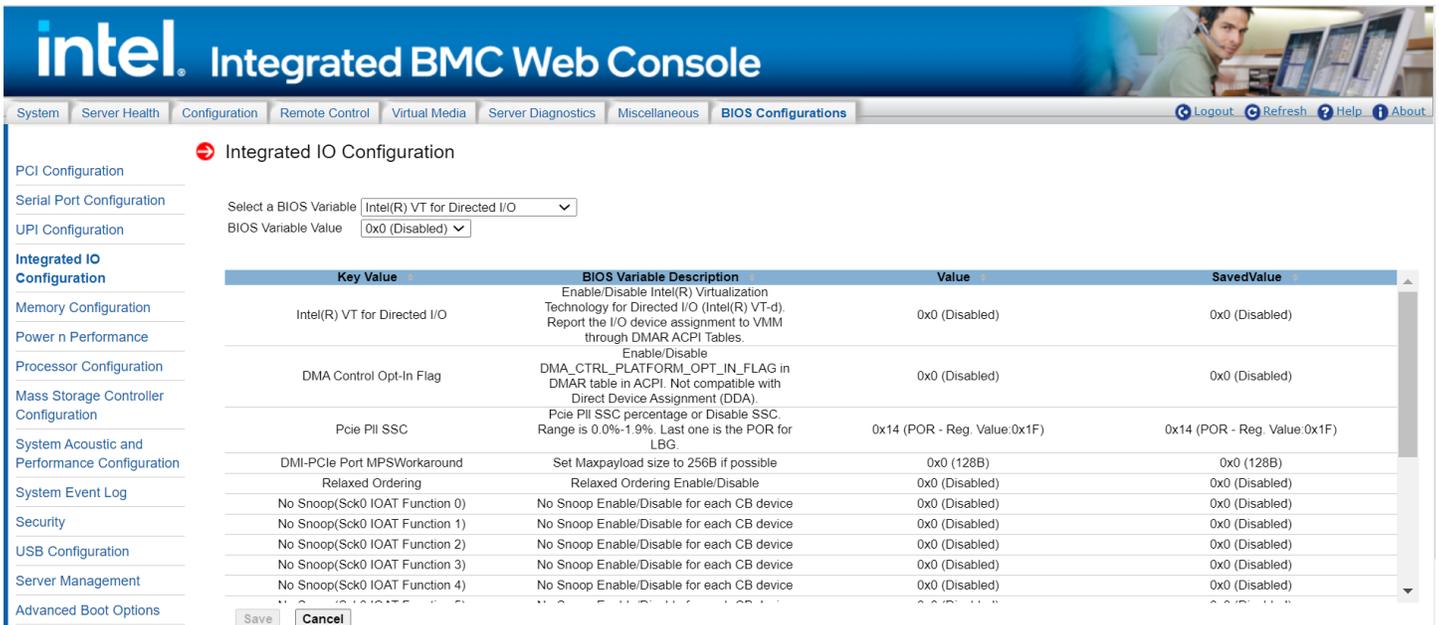


Figure 103. BIOS IIO Configuration Page

Table 33. BIOS IIO Configuration Variables

Variables	BIOS Variable Description
NTB PCIe* Port 1a on CPU socket 1 NTB PCIe* Port 2a on CPU socket 1 NTB PCIe* Port 3a on CPU socket 1 NTB PCIe* Port 1a on CPU socket 2 NTB PCIe* Port 2a on CPU socket 2 NTB PCIe* Port 3a on CPU socket 2	Configure NTB PCIe port for socket 1 and socket 2.
Enable NTB Bars	Enable or disable NTB Bars.
Enable SPLIT BARs	Enable or disable NTB SPLIT Bars.
Primary BAR 23 Size Primary BAR 4 Size Primary BAR 5 Size Primary BAR 45 Size Secondary BAR 23 Size Secondary BAR 4 Size	Select BAR23/4/5/45 size for each PCIe* port on the socket 1 and socket 2.

Variables	BIOS Variable Description
Secondary BAR 5 Size Secondary BAR 45 Size	
Intel(R) VT for Directed I/O	Enable or disable Intel(R) VT for Directed I/O.
PCIe* PII SSC	Enable or disable PCIe* PII SSC
Relaxed Ordering	Enable or disable Relaxed Ordering
No Snoop(Sck0 IOAT Function 0) No Snoop(Sck0 IOAT Function 1) No Snoop(Sck0 IOAT Function 2) No Snoop(Sck0 IOAT Function 3) No Snoop(Sck0 IOAT Function 4) No Snoop(Sck0 IOAT Function 5) No Snoop(Sck0 IOAT Function 6) No Snoop(Sck0 IOAT Function 7)	Enable or disable for each CB device on sock0.
No Snoop(Sck1 IOAT Function 1) No Snoop(Sck1 IOAT Function 2) No Snoop(Sck1 IOAT Function 3) No Snoop(Sck1 IOAT Function 4) No Snoop(Sck1 IOAT Function 5) No Snoop(Sck1 IOAT Function 6) No Snoop(Sck1 IOAT Function 7)	Enable or disable for each CB device on sock1.
DMI- PCIe* Port MPSWorkaround	Enable or disable for DMI- PCIe* Port MPSWorkaround
Data Link Protocol Error Mask	Enable or disable for Data Link Protocol Error Mask
Surprise Down Error Mask	Enable or disable for Surprise Down Error Mask
Poisoned TLP Mask	Enable or disable for Poisoned TLP Mask
Flow Control Protocol Error Mask	Enable or disable for Flow Control Protocol Error Mask
Completion Timeout Mask	Enable or disable for Completion Timeout Mask
Unexpected Completion Mask	Enable or disable for Unexpected Completion Mask
Receiver Overflow Mask	Enable or disable for Receiver Overflow Mask
Malformed TLP Mask	Enable or disable for Malformed TLP Mask
ECRC Error Mask	Enable or disable for ECRC Error Mask
ACS Volation Mask	Enable or disable for ACS Volation Mask
Uncorrectable Internal Error Mask	Enable or disable for Uncorrectable Internal Error Mask
MC Blocked TLP Mask	Enable or disable for MC Blocked TLP Mask
AtomicOp Egress Blocked Mask	Enable or disable for AtomicOp Egress Blocked Mask
TLP Prefix Blocked Error Mask	Enable or disable for TLP Prefix Blocked Error Mask

7.8.5 Memory Configuration

This page allows the user to select memory operation speed/IMC interleaving/page policy and enable or disable ADR/Erase-Arm NVDIMMS/restore NVDIMMS/ADDDC sparing/memory sparing/Multi-Rank sparing/memory Corrected Error. See Figure 104 for details. Table 34 lists all memory configuration variables that can be viewed and edited.

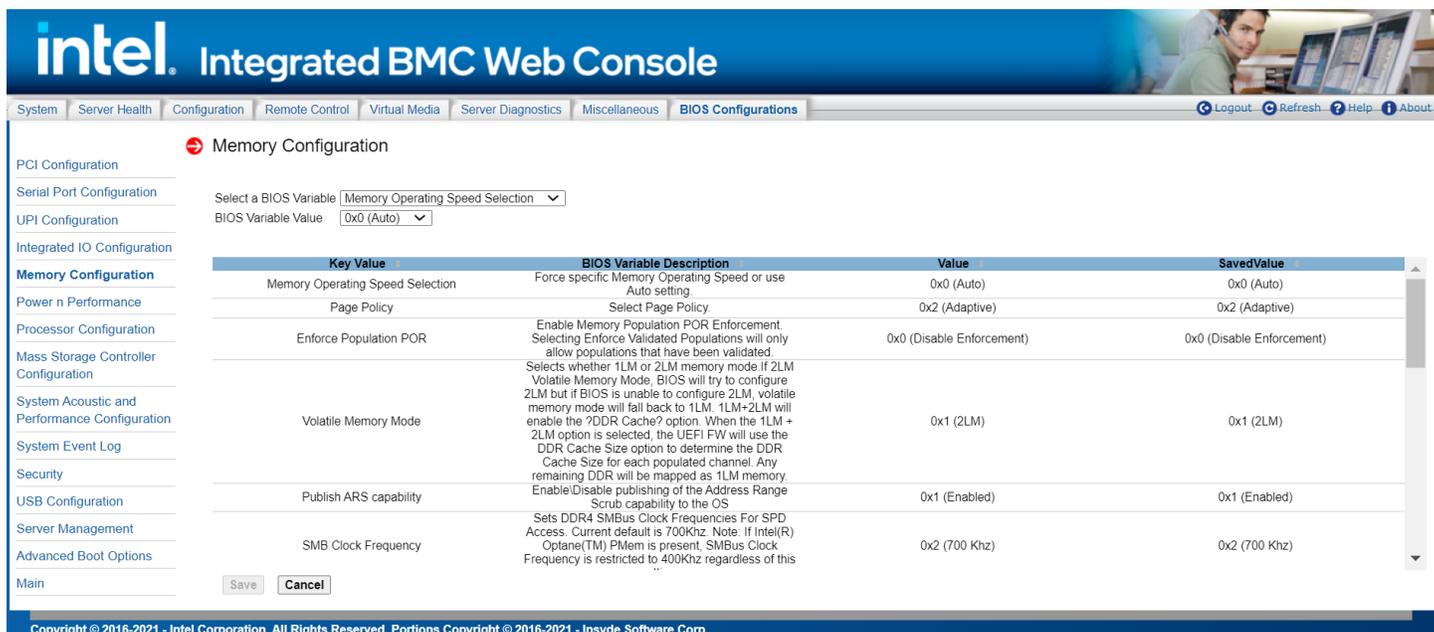


Figure 104. BIOS Memory Configuration Page

Table 34. BIOS Memory Configuration Variables

Variables	BIOS Variable Description
Memory Operating Speed Selection	Force specific Memory Operating Speed or use Auto setting.
Page Policy	Select page policy.
Enforce Population POR	Enable Memory Population POR Enforcement.
Volatile Memory Mode	Select whether 1LM or 2LM memory mode should be enabled.
Intel® Optane™ PMem Error Injection	Enable/Disable Intel® Optane™ PMem Error Injection.
Publish ARS capability	Enable\Disable publishing of the Address Range Scrub capability to the OS.
Background ARS	Auto: go background on initial short ARS sequence.
SMB Clock Frequency	Sets DDR4 SMBus Clock Frequencies For SPD Access. Auto - Sets it to the MRC default setting; current default is 400K.
Attempt Fast Boot	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on warm boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enabled.
Attempt Fast Cold Boot	Enable - Portions of memory reference code will be skipped when possible to increase boot speed on cold boots. Disable - Disables this feature. Auto - Sets it to the MRC default setting; current default is Enabled.
Enable Power Cycle Policy	Enable/Disable power cycle policy when PMem receive surprise clock stop
Halt on mem Training Error	Halt on mem Training Error Disable/Enable
ADDDC Sparing	Enable/Disable Adaptive Double Device Data Correction Sparing.
UMA-Based Clustering	UMA Based Clustering options include Disable (ALL2ALL), Hemisphere (2 cluster), and Quadrant (4 cluster, not supported on ICX). These options are only valid when SNC is disabled. If SNC is enabled, UMA-Based Clustering is automatically disabled by BIOS.

Variables	BIOS Variable Description
Patrol Scrub	When enabled, performs periodic checks on memory cells and proactively walks through populated memory space, to seek and correct soft ECC errors.
Memory Corrected Error	Enable/Disable Memory Corrected Error
Memory Error	Enable/Disable Memory Error.
Cloaking	If disabled, CMCI event appears when CE happens. If enabled, CMCI event is blocked when CE happens.
Snoopy mode for 2LM	Enables new 2LM specific feature to avoid directory updates to far-memory from non-NUMA optimized workloads
Snoopy mode for AD	Enables new AD specific feature to avoid directory updates to PMem memory from non-NUMA optimized workloads
PMem Performance Setting	PMem baseline performance settings depending on the workload behavior
PMem Factory Reset/Clear	Enable\Disable Factory Reset/Clear
PMem FastGo Configuration	Select PMem QoS Configuration Profiles

7.8.6 Power n Performance

This page allows the user to configure CPU power and performance policy/workload configuration/TDP level/hardware P-State/, enable or disable uncore frequency scaling/performance P-limit/enhanced Intel tech/Intel® configurable TDP/Turbo Boost/C1E /processor C6. See Figure 105 for details. Table 35 lists all PnP configuration variables that can be viewed and edited.

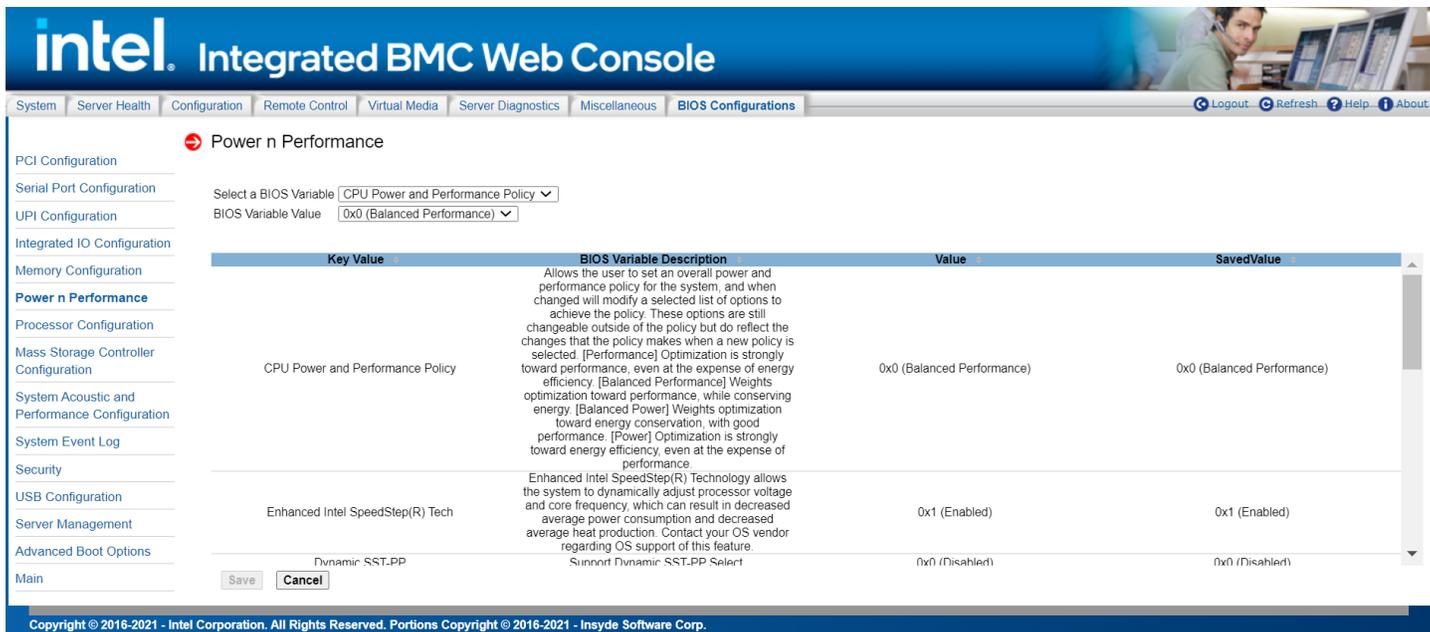


Figure 105. BIOS PnP Configuration Page

Table 35. BIOS PnP Configuration Variables

Variables	BIOS Variable Description
CPU Power and Performance Policy	Allows the user to set an overall power and performance policy for the system, and when changed will modify a selected list of options to achieve the policy. These options are still changeable outside of the policy but do reflect the changes that the policy makes when a new policy is selected. [Performance] Optimization is strongly toward performance, even at the expense of energy efficiency. [Balanced Performance] Weights optimization toward performance, while conserving energy. [Balanced Power] Weights optimization toward energy conservation, with good performance. [Power] Optimization is strongly toward energy efficiency, even at the expense of performance.

Variables	BIOS Variable Description
Enhanced Intel SpeedStep(R) Tech	Enhanced Intel SpeedStep(R) Technology allows the system to dynamically adjust processor voltage and core frequency, which can result in decreased average power consumption and decreased average heat production. Contact your OS vendor regarding OS support of this feature.
Dynamic SST-PP	Support Dynamic SST-PP Select.
Activate SST-BF	This Option allows Activate SST-BF to be enabled.
Configure SST-BF	This Option allows BIOS to configure SST-BF High Priority Cores so that SW does not have to configure.
EIST PSD Function	Choose HW_ALL/SW_ALL in _PSD return
Hardware P-states	Disable: Hardware chooses a P-state based on OS Request (Legacy P-states) Native Mode: Hardware chooses a P-state based on OS guidance. Out of Band Mode: Hardware autonomously chooses a P-state (no OS guidance).
HardwarePM Interrupt	Enable/Disable Hardware PM Interrupt.
EPP Enable	When enabled, HW masks EPP in CPUID[6].10 and uses the Energy Performance Bias Register for Energy vs. Performance Preference input.
APS rocketing	Enable/Disable the rocketing mechanism in the HWP P-state selection pcode algorithm. Rocketing enables the core ratio to jump to max turbo instantaneously as opposed to a smooth ramp up.
Scalability	Enable/Disable the use of scalability in HWP pcode power efficiency algorithms. Scalability is the measure of estimated performance improvement for a given increase in core frequency.
RAPL Prioritization	This knob controls whether RAPL balancer is enabled. When enabled it activates per core power budgeting.
Package C-state	Set and specifies the lowest C-state for Processor package. C0/C1 state is no package C-state support. C6 retention state provides more power saving than C6 non retention state. No Limit is no package C-state limit.
C1E	When Enabled, the CPU will switch to the Minimum Enhanced Intel SpeedStep(R) Technology operating point when all execution cores enter C1. Frequency will switch immediately, followed by gradual Voltage switching. When Disabled, the CPU will not transit to the minimum Enhanced Intel SpeedStep® Technology operating point when all cores enter C1.
Processor C6	Enable/Disable Processor C6 (ACPI C3) report to OS.

7.8.7 Processor Configuration

This page allows the user to configure the number of cores to enable in each processor package, enable/disable Intel(R) Hyper-Threading/execute disable bit/Intel(R) virtualization/Intel(R) TXT. See Figure 106 for details. Table 36 lists all processor configuration variables that can be viewed and edited.

Processor Configuration

Select a BIOS Variable:

BIOS Variable Value:

Key Value	BIOS Variable Description	Value	SavedValue
Direct To Core (D2C)	Direct To Core (D2C)	0x2 (Auto)	0x2 (Auto)
Direct To UPI (D2K)	Direct To UPI (D2K)	0x2 (Auto)	0x2 (Auto)
Intel(R) Virtualization Technology	Intel(R) Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions. Note: A change to this option requires the system to be powered off and then back on before the setting takes effect.	0x0 (Disabled)	0x0 (Disabled)
Intel(R) TXT	Enable/Disable Intel(R) Trusted Execution Technology. Takes effect after reboot.	0x0 (Disabled)	0x0 (Disabled)
MLC Streamer	MLC Streamer is a speculative prefetch unit within the processor(s). Note: Modifying this setting may affect performance.	0x1 (Enabled)	0x1 (Enabled)
MLC Spatial Prefetcher	[Enabled] - Fetches adjacent cache line (128 bytes) when required data is not currently in cache. [Disabled] - Only fetches cache line with data required by the processor (64 bytes).	0x1 (Enabled)	0x1 (Enabled)
DCU Data Prefetcher	The next cache line will be prefetched into L1 data cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data. [Disabled] - Only fetches cache line with data required by the processor (64 bytes).	0x1 (Enabled)	0x1 (Enabled)
DCU Instruction Prefetcher	The next cache line will be prefetched into L1 instruction cache from L2 or system memory during unused cycles if it sees that the	0x1 (Enabled)	0x1 (Enabled)

Figure 106. BIOS Processor Configuration Page

Table 36. BIOS Processor Configuration Variables

Variables	BIOS Variable Description
Direct To Core (D2C)	Direct To Core (D2C)
Direct To UPI (D2K)	Direct To UPI (D2K)
Intel(R) Virtualization Technology	Intel(R) Virtualization Technology allows a platform to run multiple operating systems and applications in independent partitions. Note: A change to this option requires the system to be powered off and then back on before the setting takes effect.
Intel(R) TXT	Enable/Disable Intel(R) Trusted Execution Technology (Inte(R) TXT). Takes effect after reboot.
MLC Streamer	MLC Streamer is a speculative prefetch unit within the processor(s). Note: Modifying this setting may affect performance.
MLC Spatial Prefetcher	[Enabled] - Fetches adjacent cache line (128 bytes) when required data is not currently in cache. [Disabled] - Only fetches cache line with data required by the processor (64 bytes).
DCU Data Prefetcher	The next cache line will be prefetched into L1 data cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data. [Disabled] - Only fetches cache line with data required by the processor (64 bytes).
DCU Instruction Prefetcher	The next cache line will be prefetched into L1 instruction cache from L2 or system memory during unused cycles if it sees that the processor core has accessed several bytes sequentially in a cache line as data.
X2APIC	Enable/disable extended APIC support
Limit CPU PA to 46 bits	Limit CPU physical address to 46 bits to support older Hyper-V.
LLC Prefetch	Enable/Disable LLC Prefetch on all threads.
Hyper-Threading [ALL]	Enables Hyper Threading (Software Method to Enable/Disable Logical Processor threads.
IED Trace memory	Option to allocate memory for PSMI trace
Skip Flex Ratio Override	Skip Flex Ratio overrides to use power-on default Flex Ratio values. In multi-socket systems, this will allow mixed flex ratio limits.
Check CPU BIST Result	Disable failed BIST core when enabled, otherwise, ignore BIST result
Core Failover	Enable spare core(s) in place of core(s) that fail BIST
3StrikeTimer	The 3 strike counter can be turned off by writing into the MISC_FEATURE_CONTROL_DISABLE_THREE_STRIKE_CNT(MSR 0x01a4).
Fast String	When enabled, enable fast strings for REP MOVSB/STOS

Variables	BIOS Variable Description
Machine Check	Enable or Disable the Machine Check
Max CPUID Value Limit	This should be enabled in order to boot legacy OSeS that cannot support CPUs with extended CPUID functions.
Hardware Prefetcher	- MLC Streamer Prefetcher (MSR 1A4h Bit[0])
L2 RFO Prefetch Disable	- L2 RFO Prefetch (MSR 972h Bit[3])
Adjacent Cache Prefetch	- MLC Spatial Prefetcher (MSR 1A4h Bit[1])
DCU Streamer Prefetcher	DCU streamer prefetcher is an L1 data cache prefetcher (MSR 1A4h [2]).
DCU IP Prefetcher	DCU IP prefetcher is an L1 data cache prefetcher (MSR 1A4h [3]).
LLC Prefetch	Enable/Disable LLC Prefetch on all threads
DCU Mode	Normal: The whole DCU used for caching; Mirror-Mode: DCU organized as 2x16KB mirrored copies
Bsp Selection	Choose the method to select BSP
Extended APIC	Enable/disable extended APIC support Note: This will enable VT-d automatically if x2APIC is enabled
APIC Physical Mode	Enable/Disable the APIC physical destination mode
Down Stream PECl	Enable PCIe* Down Stream PECl Write
PECl	PECl in trust bit enables
Legacy Agent	Legacy PECl agent in trust bit enables
SMBus Agent	SMBus PECl agent in trust bit enables
IE Agent	IE PECl agent in trust bit enables
Generic Agent	Generic PECl agent in trust bit enables
eSPI Agent	ESPI PECl agent in trust bit enables
DBP-F	The DBP-F can be turned off by writing into the (MSR 792h [5:6] for CLX, CPX, and MSR 6Dh [2:3] for ICX).
IIO LLC Ways [19:0](Hex)	MSR CBO_SLICE0_CR_IIO_LLC_WAYS bitmask
Remote Ways [22:12](Hex)	MSR INGRESS_SPARE bitmask[26:16], Value 0 means no override
SMM Blocked and Delayed	Enable/Disable SMM Blocked and Delayed
eSMM Save State	Enable or Disable the eSMM Save State Feature
Smbus Error Recovery	Enable or Disable Smbus Error Recovery
Enable Intel(R) TXT	Enables Intel® TXT.
VMX	Enables the Vanderpool Technology, takes effect after reboot.
Enable SMX	Enables Safer Mode Extensions.
Lock Chipset	Lock or Unlock chipset
MSR Lock Control	Enable - MSR 3Ah and CSR 80h will be locked. Power Good reset is needed to remove lock bits.
PKG CST CONFIG CONTROL MSR Lock	Enable - MSR E2h will be locked. Power Good reset is needed to remove lock bits.
PPIN Control	Unlock and Enable/Disable PPIN Control
AES-NI	Enable/disable AES-NI support
TSC Reset	Enable or Disable TSC reset during warm reboot
Total Memory Encryption (TME)	Enable/Disable Intel® Total Memory Encryption (Intel® TME)
Limit CPU PA to 46 bits	Limit CPU physical address to 46 bits to support older Hyper-V. If enabled, automatically disables Intel TME-MT.
RDT CAT Opportunistic Tuning	Cache Allocation Technology mask tuning options. Note: If IOT is enabled on any socket this option will override to 0x003
Global PSMI Enable	Global PSMI Enable
PSMI Enable	PSMI Enable
Disable Bitmap	0: Enable all cores. FFFFFFFF: Disable all cores

7.8.8 Mass Storage Controller Configuration

This page allows the user to configure the AHCI capable SATA controller/SATA RAID options/AHCI capable sSATA controller and enable/disable SATA HDD staggered Spin-up/sSATA HDD Staggered Spin-Up. See Figure 107 for details. Table 37 lists all mass storage controller configuration variables that can be viewed and edited.

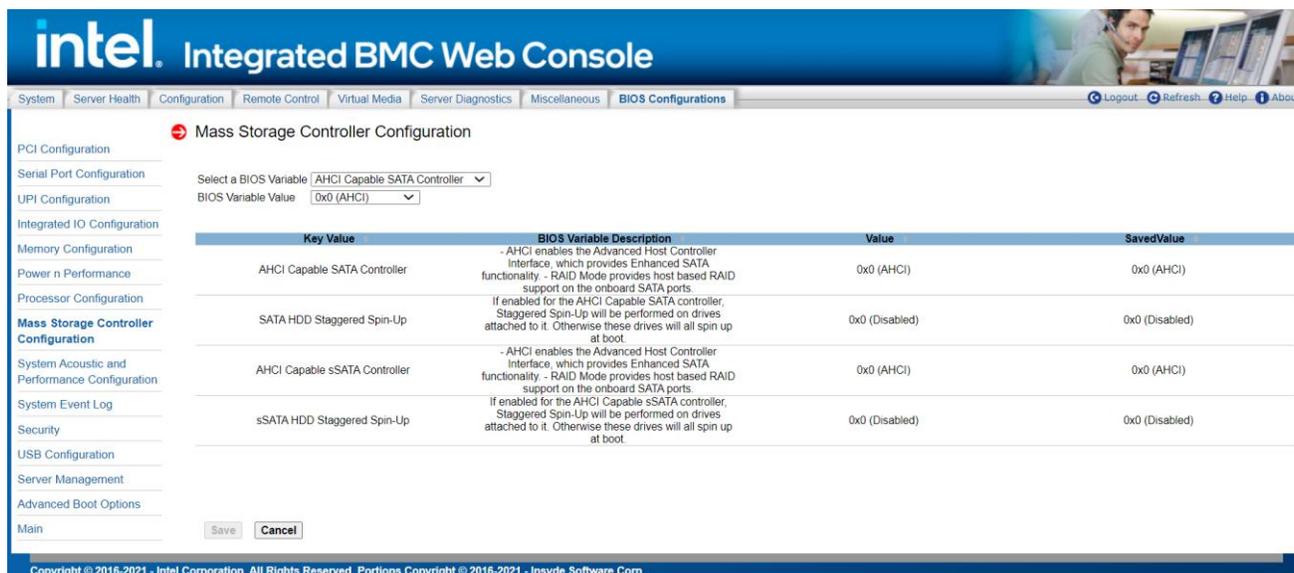


Figure 107. BIOS Mass Storage Controller Configuration Page

Table 37. BIOS Mass Storage Configuration Variables

Variables	BIOS Variable Description
AHCI Capable SATA Controller	AHCI enables the Advanced Host Controller Interface, which provides Enhanced SATA functionality. - RAID Mode provides host based RAID support on the onboard SATA ports.
SATA HDD Staggered Spin-Up	If enabled for the AHCI Capable SATA controller, Staggered Spin-Up will be performed on drives attached to it. Otherwise these drives will all spin up at boot.
AHCI Capable sSATA Controller	AHCI enables the Advanced Host Controller Interface, which provides Enhanced SATA functionality. - RAID Mode provides host based RAID support on the onboard SATA ports.
sSATA HDD Staggered Spin-Up	If enabled for the AHCI Capable sSATA controller, Staggered Spin-Up will be performed on drives attached to it. Otherwise these drives will all spin up at boot.

7.8.9 System Acoustic and Performance Configuration

This page allows the user to configure fan speed control profile. See Figure 108 for details. Table 38 lists all system acoustic and performance configuration variables that can be viewed and edited.

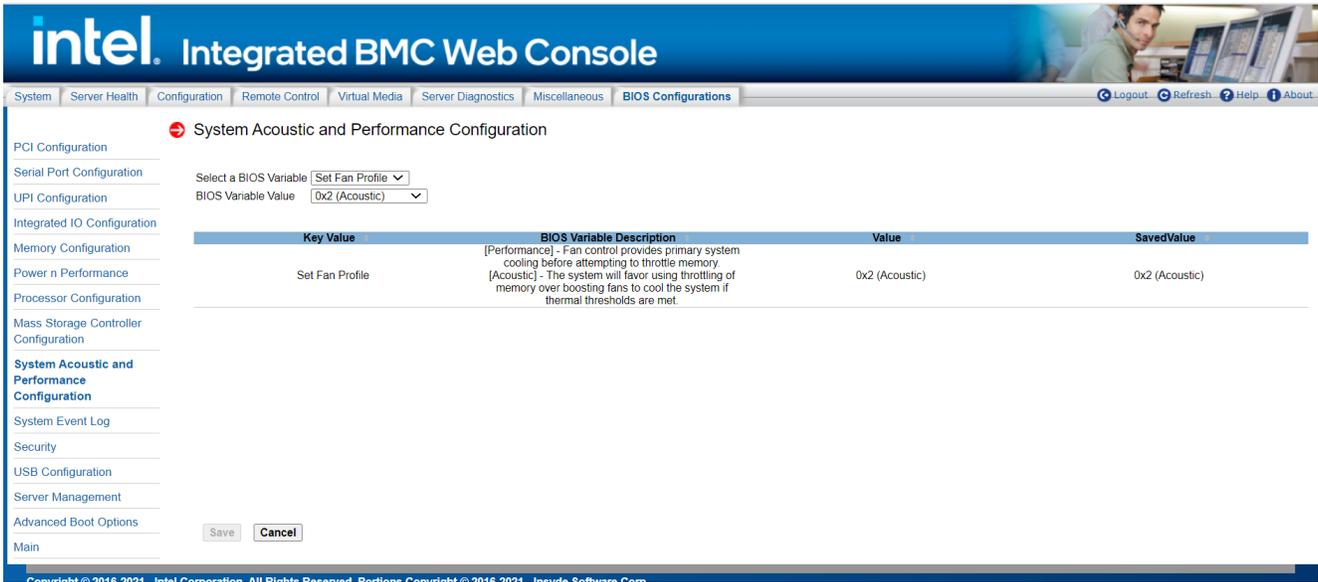


Figure 108. BIOS System Acoustic and Performance Configuration Page

Table 38. BIOS System Acoustic and Performance Configuration Variables

Variables	BIOS Variable Description
Set Fan Profile	[Performance] - Fan control provides primary system cooling before attempting to throttle memory. [Acoustic] - The system will favor using throttling of memory over boosting fans to cool the system if thermal thresholds are met.

7.8.10 System Event Log

This page allows the user to configure what Event types to monitor by System Event log. See Figure 109 for details.

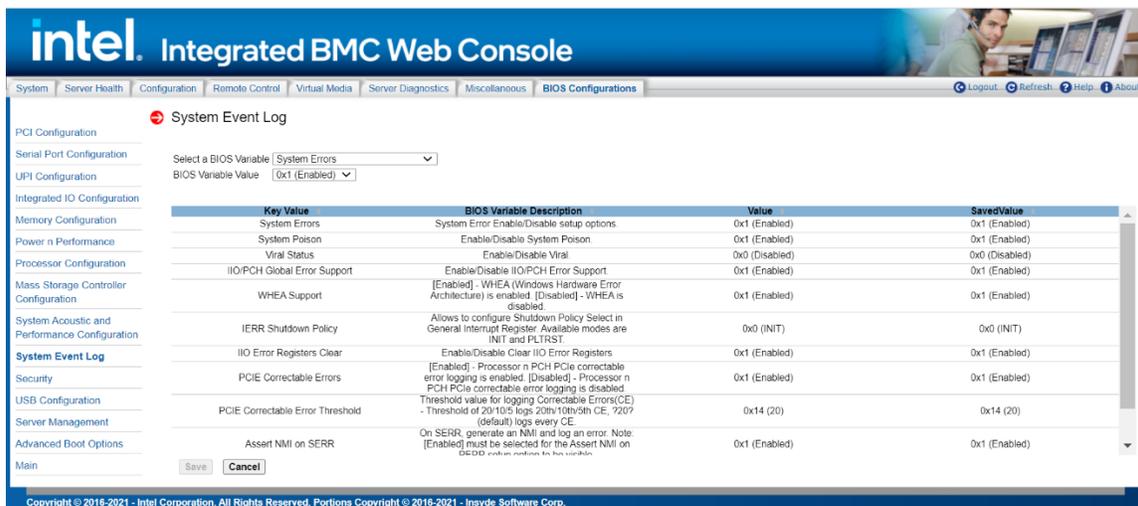


Figure 109. System Event Log Page

7.8.11 Security

This page allows the user to configure BIOS security variables, such as power on password, front panel lockout, TPM administrative control. See Figure 110 for details. Table 39 lists all security variables that can be viewed and edited.

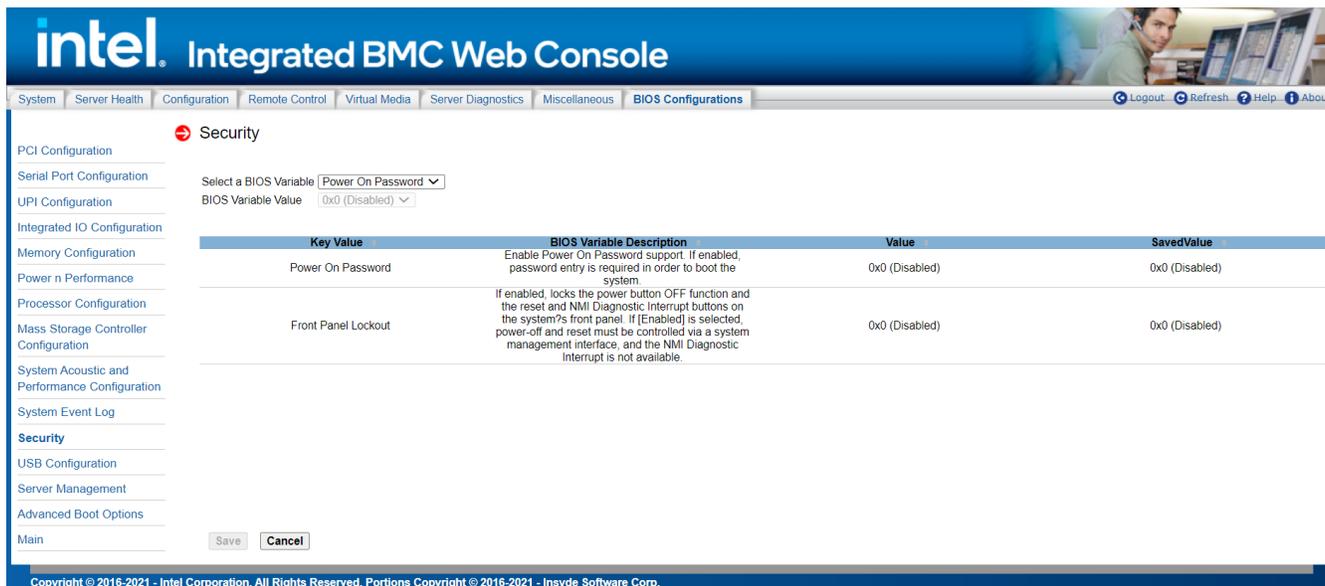


Figure 110. BIOS Security Configuration Page

Table 39. BIOS Security Variables

Variables	BIOS Variable Description
Power On Password	Enable Power On Password support. If enabled, password entry is required in order to boot the system.
Front Panel Lockout	If enabled, locks the power button OFF function and the reset and NMI Diagnostic Interrupt buttons on the system's front panel. If [Enabled] is selected, power-off and reset must be controlled via a system management interface, and the NMI Diagnostic Interrupt is not available.

7.8.12 USB Configuration

This page allows the user to enable/disable legacy USB support/port 60 and port 64 emulation/make USB device non-bootable, configure device reset timeout for USB device. See Figure 111 for details. Table 40 lists all USB configuration variables that can be viewed and edited.

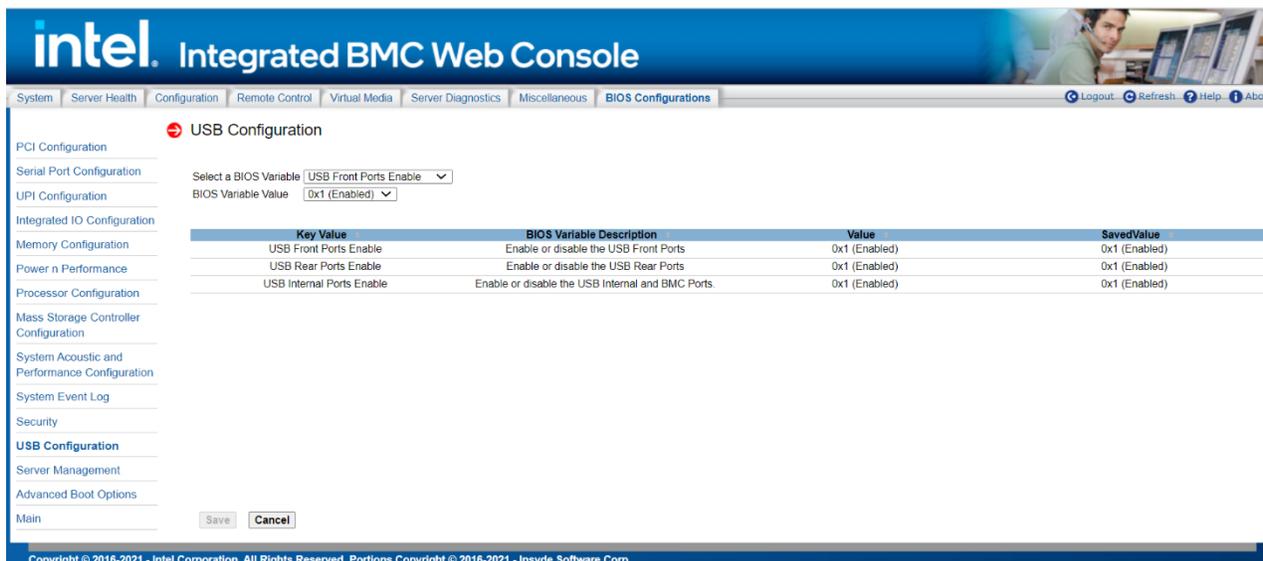


Figure 111. BIOS USB Configuration Page

Table 40. BIOS USB Configuration Variables

Variables	BIOS Variable Description
USB Front Ports Enable	Enable or disable the USB Front Ports
USB Rear Ports Enable	Enable or disable the USB Rear Ports
USB Internal Ports Enable	Enable or disable the USB Internal and BMC Ports.

7.8.13 Server Management

The page allows the user to configure server management features, such as Console redirection enabling. See Figure 112 for details. Table 41 lists all options that can be viewed and edited.

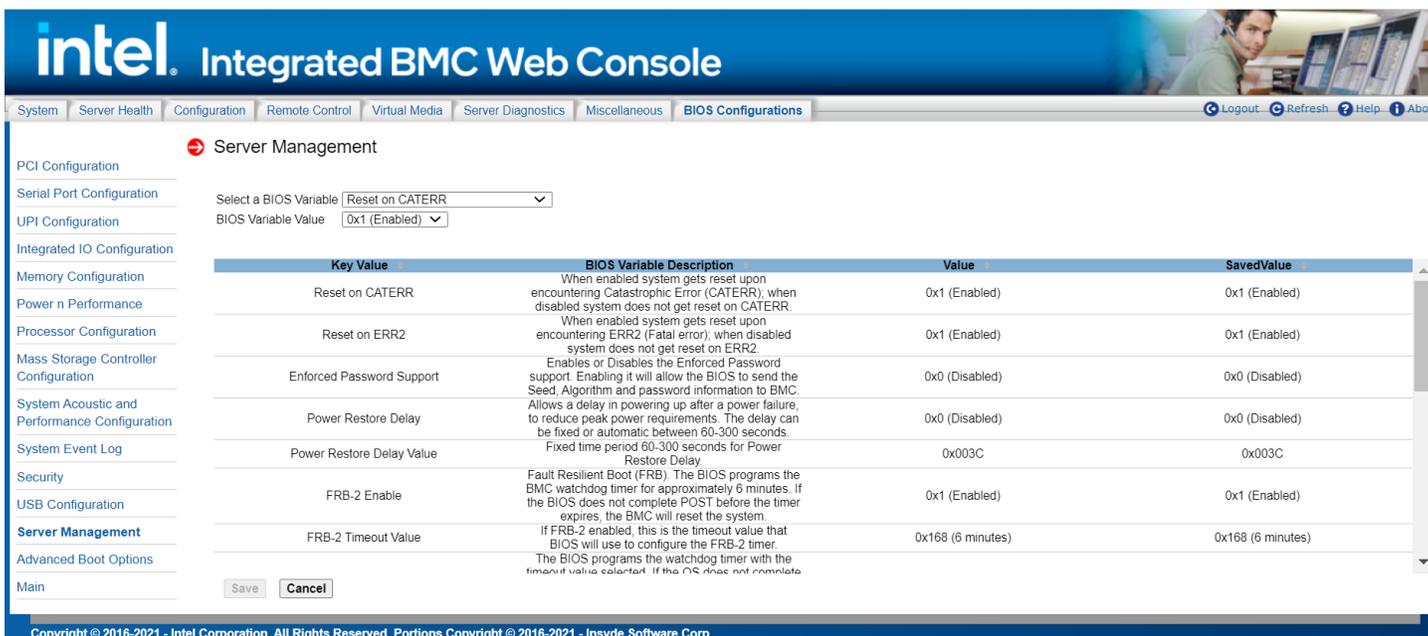


Figure 112. BIOS Server Management Page

Table 41. Server Management

Variables	BIOS Variable Description
Reset on CATERR	When enabled system gets reset upon encountering Catastrophic Error (CATERR); when disabled system does not get reset on CATERR.
Reset on ERR2	When enabled system gets reset upon encountering ERR2 (Fatal error); when disabled system does not get reset on ERR2.
Enforced Password Support	Enables or Disables the Enforced Password support. Enabling it will allow the BIOS to send the Seed, Algorithm and password information to BMC.
Power Restore Delay	Allows a delay in powering up after a power failure, to reduce peak power requirements. The delay can be fixed or automatic between 60-300 seconds.
Power Restore Delay Value	Fixed time period 60-300 seconds for Power Restore Delay.
FRB-2 Enable	Fault Resilient Boot (FRB). The BIOS programs the BMC watchdog timer for approximately 6 minutes. If the BIOS does not complete POST before the timer expires, the BMC will reset the system.
FRB-2 Timeout Value	If FRB-2 enabled, this is the timeout value that BIOS will use to configure the FRB-2 timer.
OS Boot Watchdog Timer	The BIOS programs the watchdog timer with the timeout value selected. If the OS does not complete booting before the timer expires, the BMC will reset the system and an error will be logged. Requires OS support or Intel Management Software Support.
OS Boot Watchdog Timer Policy	If the OS watchdog timer is enabled, this is the system action taken if the watchdog timer expires. [Reset] - System performs a reset. [Power Off] - System powers off.
OS Boot Watchdog Timer Timeout	If the OS watchdog timer is enabled, this is the timeout value the BIOS will use to configure the watchdog timer.
Plug n Play BMC Detection	If enabled, the BMC will be detectable by OSeS, which support plug and play loading of an IPMI driver. Do not enable this option if your OS does not support this driver.
Console Redirection	Console redirection allows a serial port to be used for server management tasks. [Disabled] - No console redirection. [Serial Port A/B] - Configure serial port A/B for console redirection. Enabling this option will disable display of the Quiet Boot logo screen during POST. [Advanced - Serial Port Configuration - Serial A/B Enable] needs be enabled before enabling this option.
Flow Control	Flow control is the handshake protocol. This setting must match the remote terminal application. [None] - Configure for no flow control. [RTS/CTS] - Configure for hardware flow control.
Baud Rate	Serial port transmission speed. This setting must match the remote terminal application.
Terminal Type	Character formatting used for console redirection. This setting must match the remote terminal application.
Legacy OS Redirection	This option enables legacy OS redirection (i.e., DOS) on serial port. If it is enabled, the associated serial port is hidden from the legacy OS.
Terminal Resolution	Remote Terminal Resolution.

7.8.14 Advanced Boot Options

This page allows the user to configure advanced boot options. See Figure 113 for details. Table 42 lists all Advanced Boot Options that can be viewed and edited.

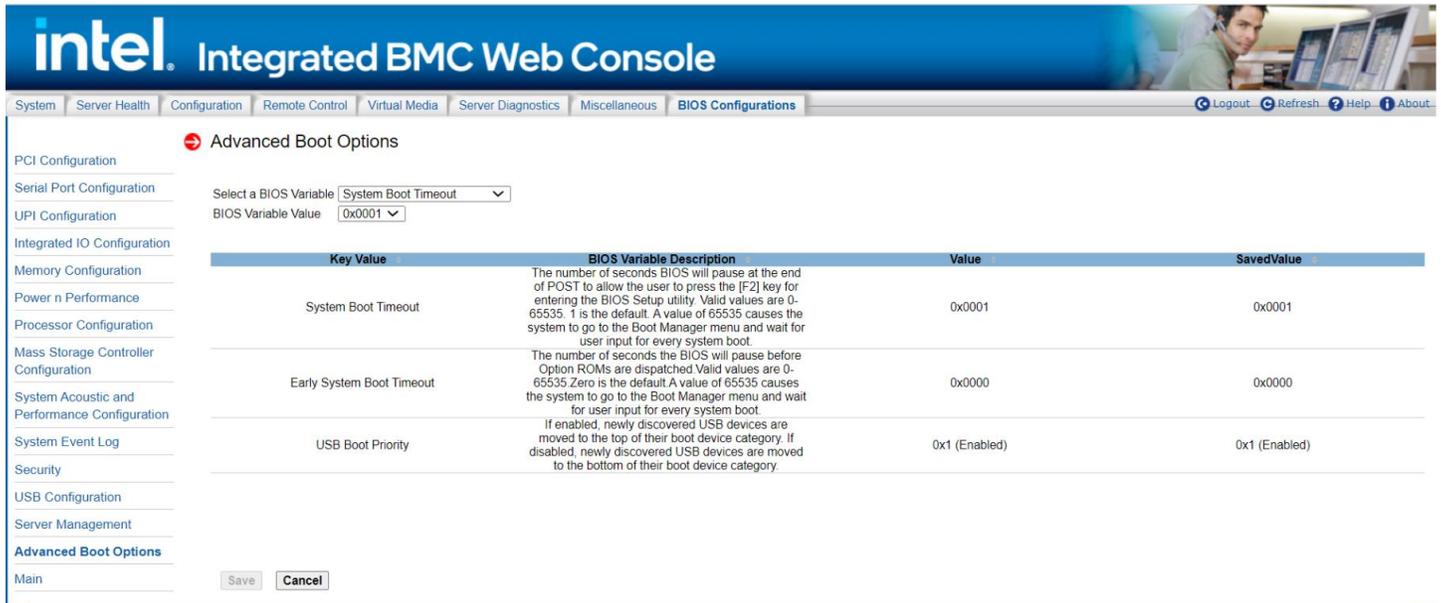


Figure 113. BIOS Advanced Boot Page

Table 42. BIOS Advanced Boot

Variables	BIOS Variable Description
System Boot Timeout	The number of seconds BIOS will pause at the end of POST to allow the user to press the [F2] key for entering the BIOS Setup utility. Valid values are 0–65535. 1 is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.
Early System Boot Timeout	The number of seconds the BIOS will pause before Option ROMs are dispatched. Valid values are 0–65535. Zero is the default. A value of 65535 causes the system to go to the Boot Manager menu and wait for user input for every system boot.
USB Boot Priority	If enabled, newly discovered USB devices are moved to the top of their boot device category. If disabled, newly discovered USB devices are moved to the bottom of their boot device category.

7.8.15 Main

This page allows the user to configure main BIOS variables, such as quiet boot. See Figure 114 for details. Table 43 lists all main BIOS variables that can be viewed and edited.

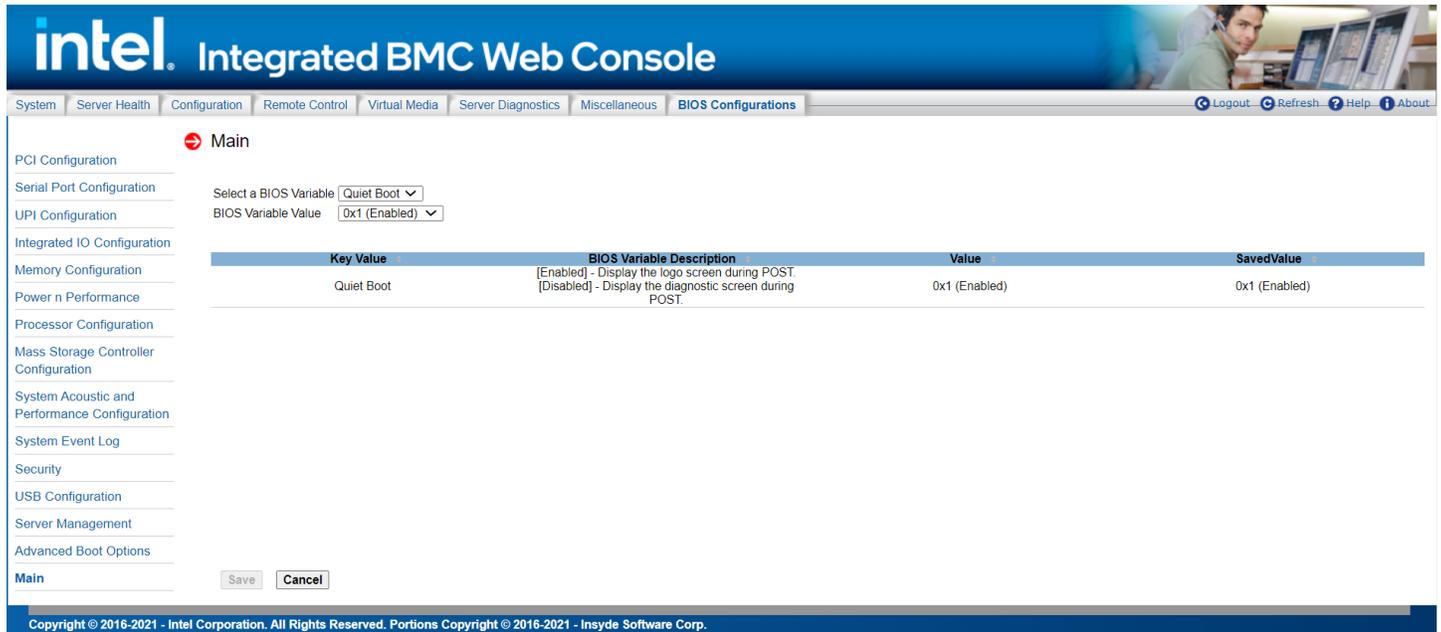


Figure 114. BIOS Main Page

Table 43. BIOS Main Configuration Variables

Variables	BIOS Variable Description
Quiet Boot	[Enabled] - Display the logo screen during POST. [Disabled] - Display the diagnostic screen during POST.

Appendix A. Glossary

Term	Definition
ARP	Address Resolution Protocol
Intel® ASMI	Intel® Advanced Server Management Interface
BMC	Baseboard Management Controller
Intel® DCM	Intel® Data Center Manager
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ICMP	Internet Control Message Protocol
IPMI	Intelligent Platform Management Interface
KCS	Keyboard Controller Style
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Address Protocol
MAC	Media Access Controller
Intel® ME	Intel® Management Engine
MII	Media Independent Interface
NIC	Network Interface Controller
Intel® NM	Intel® Node Manager
OOB	Out Of Band – no operating system interaction on server
Intel® RMM	Intel® Remote Management Module
SDR	Sensor Data Record
SOL	Serial Over LAN
TCP/IP	Transmission Control Protocol/Internet Protocol
Intel® TME	Intel® Total Memory Encryption
Intel® TXT	Intel® Trusted Execution Technology
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
Intel® VT	Intel® Virtualization Technology