



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

User Guide

Guide to the Integrated BMC Web Console (previously known as embedded web server) for Intel® server boards and systems based on the 1st and 2nd Gen Intel® Xeon® Scalable processor family.

Rev. 2.0

March 2022

<Blank page>

Document Revision History

Date	Revision	Changes
December 2017	1.0	Initial release.
January 2018	1.1	Public release.
May 2018	1.2	Update EWS certificate statement. Update usage for SOL log dump, alerts, alert email settings, and security settings page.
September 2018	1.3	Add LDAP and OOB firmware update page.
January 2019	1.4	Add iKVM over HTML5 page, LDAP settings page, BIOS/ME firmware update page, Syslog server configuration page, Virtual Media, and BIOS configurations tab.
March 2019	1.5	Add caution for switch setting to avoid network duplex mismatch. Update SDR Configuration page to add option for SDR auto configuration enabling and disabling.
May 2020	1.6	Added KCS Policy control. Added Cipher suite. Added figure of S9200WK RMM4 pin and BMC Nic location. Updated Figure 73. HTML5 Keyboard Macro menu page.
July 2020	1.7	Update KCS Policy control
December 2020	1.8	Update Figure picture for Sections 5, 6, 7. Update some table content for Sections 5, 6, 7. Minor changes throughout for clarity.
August 2021	1.9	Add Host Interface information in chapter 4.1. Add Host Interface information and setting in Table 13 and Table 14. Update Virtual Media information for Section 7.5. Minor language and format edits throughout the document.
March 2022	2.0	Updated the document title, replacing “embedded web server” with “Integrated BMC Web Console”. Updated descriptions for KCS policy control modes Deny All and Restrict in Table 19. Edits throughout the document to improve style and formats.

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.

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

Intel, the Intel logo, Intel Xeon Phi, and Xeon 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

Safety Information

Important Safety Instructions

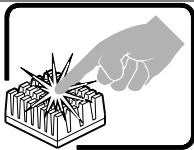
Read all caution and safety statements in this document before performing any of the instructions. See also Intel® Server Boards and Server Chassis Safety Information at

https://www.intel.com/content/dam/support/us/en/documents/server-products/g23122-004_safetyregulatory.pdf.



SAFETY STEPS: When removing the chassis cover to access the inside of the system, follow these steps:

1. Turn off all peripheral devices connected to the system.
2. Turn off the system by pressing the power button.
3. Unplug all AC power cords from the system or from wall outlets.
4. Label and disconnect all cables connected to I/O connectors or ports on the back of the system.
5. Provide some electrostatic discharge (ESD) protection by wearing an antistatic wrist strap attached to chassis ground of the system—any unpainted metal surface—when handling components.
6. Do not operate the system with the chassis covers removed.



A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.

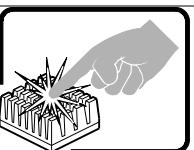
Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warn und Sicherheitshinweise in diesem Dokument, bevor Sie eine der Anweisungen ausführen. Beachten Sie hierzu auch die Sicherheitshinweise zu Intel-Serverplatinen und Servergehäusen unter https://www.intel.com/content/dam/support/us/en/documents/server-products/g23122-004_safetyregulatory.pdf.



SICHERHEISMASSNAHMEN: Immer wenn Sie die Gehäuseabdeckung abnehmen um an das Systeminnere zu gelangen, sollten Sie folgende Schritte beachten:

1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus.
2. Schalten Sie das System mit dem Hauptschalter aus.
3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose.
4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen oder Ports ab.
5. Tragen Sie ein geerdetes Antistatik Gelenkband, um elektrostatische Ladungen (ESD) über blanke Metallstellen bei der Handhabung der Komponenten zu vermeiden.
6. Schalten Sie das System niemals ohne ordnungsgemäß montiertes Gehäuse ein.



Der Mikroprozessor und der Kühler sind möglicherweise erhitzt, wenn das System in Betrieb ist. Außerdem können einige Platinen und Gehäuse Teile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

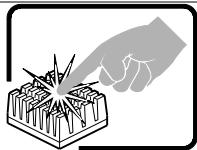
Consignes de sécurité

Lisez attention toutes les consignes de sécurité et les mises en garde indiquées dans ce document avant de suivre toute instruction. Consultez Intel® Server Boards and Server Chassis Safety Information sur le site https://www.intel.com/content/dam/support/us/en/documents/server-products/g23122-004_safetyregulatory.pdf



CONSIGNES DE SÉCURITÉ -Lorsque vous ouvrez le boîtier pour accéder à l'intérieur du système, suivez les consignes suivantes:

1. Mettez hors tension tous les périphériques connectés au système.
2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir).
3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales.
4. Identifiez et débranchez tous les câbles reliés aux connecteurs d'E-S ou aux accès derrière le système.
5. Pour prévenir les décharges électrostatiques lorsque vous touchez aux composants, portez une bande antistatique pour poignet et reliez-la à la masse du système (toute surface métallique non peinte du boîtier).
6. Ne faites pas fonctionner le système tandis que le boîtier est ouvert.



Le microprocesseur et le dissipateur de chaleur peuvent être chauds si le système a été sous tension. Faites également attention aux broches aiguës des cartes et aux bords tranchants du capot. Nous vous recommandons l'usage de gants de protection.

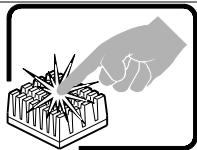
Instrucciones de seguridad importantes

Lea todas las declaraciones de seguridad y precaución de este documento antes de realizar cualquiera de las instrucciones. Vea Intel® Server Boards and Server Chassis Safety Information en https://www.intel.com/content/dam/support/us/en/documents/server-products/g23122-004_safetyregulatory.pdf



INSTRUCCIONES DE SEGURIDAD: Cuando extraiga la tapa del chasis para acceder al interior del sistema, siga las siguientes instrucciones:

1. Apague todos los dispositivos periféricos conectados al sistema.
2. Apague el sistema presionando el interruptor encendido/apagado.
3. Desconecte todos los cables de alimentación CA del sistema o de las tomas de corriente alterna.
4. Identifique y desconecte todos los cables enchufados a los conectores E/S o a los puertos situados en la parte posterior del sistema.
5. Cuando manipule los componentes, es importante protegerse contra la descarga electrostática (ESD). Puede hacerlo si utiliza una muñequera antiestática sujetada a la toma de tierra del chasis — o a cualquier tipo de superficie de metal sin pintar.
6. No ponga en marcha el sistema si se han extraído las tapas del chasis.



Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

重要安全指导

在执行任何指令前，请阅读本文档中所有的注意事项及安全声明。或

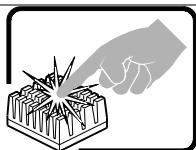
https://www.intel.com/content/dam/support/us/en/documents/server-products/g23122-004_safetyregulatory.pdf 上的 *Intel® Server Boards and Server Chassis Safety Information* (《Intel 服务器主板与服务器机箱安全信息》)

Importanti istruzioni di sicurezza



PASSI DI SICUREZZA: Qualora si rimuovano le coperture del telaio per accedere all'interno del sistema, seguire i seguenti passi:

1. Spegnere tutti i dispositivi periferici collegati al sistema.
2. Spegnere il sistema, usando il pulsante spento/acceso dell'interruttore del sistema.
3. Togliere tutte le spine dei cavi del sistema dalle prese elettriche.
4. Identificare e sconnettere tutti i cavi attaccati ai collegamenti I/O od alle prese installate sul retro del sistema.
5. Qualora si tocchino i componenti, proteggersi dallo scarico elettrostatico (SES), portando un cinghia anti-statica da polso che è attaccata alla presa a terra del telaio del sistema – qualsiasi superficie non dipinta – .
6. Non far operare il sistema quando il telaio è senza le coperture.



Se il sistema è stato a lungo in funzione, il microprocessore e il dissipatore di calore potrebbero essere surriscaldati. Fare attenzione alla presenza di piedini appuntiti e parti taglienti sulle schede e sul telaio. È consigliabile l'uso di guanti di protezione.

Warnings

Heed safety instructions: Before working with your server product, whether you are using this guide or any other resource as a reference, pay close attention to the safety instructions. You must adhere to the assembly instructions in this guide to ensure and maintain compliance with existing product certifications and approvals. Use only the described, regulated components specified in this guide. Use of other products / components will void the UL listing and other regulatory approvals of the product and will most likely result in noncompliance with product regulations in the region(s) in which the product is sold.

System power on/off: The power button DOES NOT turn off the system AC power. To remove power from system, you must unplug the AC power cord from the wall outlet. Make sure the AC power cord is unplugged before you open the chassis, add, or remove any components.

Hazardous conditions, devices, and cables: Hazardous electrical conditions may be present on power, telephone, and communication cables. Turn off the server and disconnect the power cord, telecommunications systems, networks, and modems attached to the server before opening it. Otherwise, personal injury or equipment damage can result.

Electrostatic discharge (ESD) and ESD protection: ESD can damage disk drives, boards, and other parts. We recommend that you perform all procedures in this chapter only at an ESD workstation. If one is not available, provide some ESD protection by wearing an anti-static wrist strap attached to chassis ground, any unpainted metal surface on your server when handling parts.

ESD and handling boards: Always handle boards carefully. They can be extremely sensitive to ESD. Hold boards only by their edges. After removing a board from its protective wrapper or from the server, place the board component side up on a grounded, static free surface. Use a conductive foam pad if available but not the board wrapper. Do not slide board over any surface.

Installing or removing jumpers: A jumper is a small plastic encased conductor that slips over two jumper pins. Some jumpers have a small tab on top that you can grip with your fingertips or with a pair of fine needle-nosed pliers. If your jumpers do not have such a tab, take care when using needle nosed pliers to remove or install a jumper; grip the narrow sides of the jumper with the pliers, never the wide sides. Gripping the wide sides can damage the contacts inside the jumper, causing intermittent problems with the function controlled by that jumper. Take care to grip with, but not squeeze, the pliers or other tool you use to remove a jumper, or you may bend or break the pins on the board.

Caution: Slide/rail mounted equipment is not to be used as a shelf or a work space.

Intel warranties that this product will perform to its published specifications. However, all computer systems are inherently subject to unpredictable system behavior under various environmental and other conditions.

This product is not intended to be the sole source for any critical data and the user must maintain a verified backup. Failure to do so or to comply with other user notices in the product user guide and specification documents may result in loss of or access to data.

Table of Contents

1. Introduction.....	17
1.1 Support Information.....	17
1.2 Warranty Information.....	17
2. Intel® Remote Management Module 4 (Intel® RMM4).....	18
2.1 Intel® RMM4 Lite Overview.....	18
2.2 Intel® RMM4 Lite Features	18
2.3 Supported Operating Systems and Browsers.....	18
2.3.1 Server System.....	19
2.3.2 Client System.....	19
3. Installing the Hardware.....	20
3.1 Intel® RMM4 Lite Installation	20
3.1.1 Required Tools.....	20
3.1.2 Installation Procedure.....	20
3.2 Intel® Dedicated Server Management NIC	23
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	27
4.2.3 Configuring Serial-over LAN (SOL)	27
5. Getting Started with Intel® RMM4 Operation	28
5.1 Client Browsers	28
5.2 Logging In.....	28
5.3 Navigation	29
6. Remote Console (KVM) Operation.....	32
6.1 Launching the Redirection Console	32
6.2 Main Window	34
6.3 Remote Console Control Bar.....	35
6.3.1 Virtual Media Menu	35
6.3.2 Macro Menu.....	36
6.3.3 Options Menu	37
6.3.4 User List Menu.....	42
6.3.5 Capture Menu	43
6.3.6 Power Control Menu.....	43
6.3.7 Exit Menu	44
6.4 Remote Console Status Line	44

7. Integrated BMC Web Console Options.....	45
7.1 System Tab	45
7.1.1 System Information.....	45
7.1.2 Field Replaceable Unit (FRU) Information	46
7.1.3 CPU Information	48
7.1.4 DIMM Information.....	49
7.1.5 NVMe* Information.....	49
7.1.6 NIC Information.....	50
7.1.7 Storage Information.....	50
7.1.8 Current Users.....	50
7.2 Server Health Tab	51
7.2.1 Sensor Readings.....	51
7.2.2 Event Log	53
7.3 Configuration Tab	54
7.3.1 Alerts	54
7.3.2 Alert Email.....	55
7.3.3 Date & Time	56
7.3.4 IPv4 Network.....	57
7.3.5 IPv6 Network.....	59
7.3.6 VLAN Settings.....	61
7.3.7 LDAP Settings	62
7.3.8 Active Directory Settings.....	63
7.3.9 KVM & Media	64
7.3.10 SSL Certification	65
7.3.11 Users.....	66
7.3.12 Security Settings.....	68
7.3.13 SOL.....	72
7.3.14 SDR Configuration	73
7.3.15 BMC Firmware Update	74
7.3.16 BIOS/ME Firmware Update	75
7.3.17 Syslog Server Configuration.....	76
7.4 Remote Control Tab.....	76
7.4.1 KVM/Console Redirection	77
7.4.2 Server Power Control	78
7.4.3 Launch SOL.....	79
7.4.4 Virtual Front Panel.....	80
7.4.5 iKVM over HTML5	81
7.5 Virtual Media Tab	83
7.5.1 Virtual Media over HTML5.....	83
7.5.2 Web ISO	85
7.6 Server Diagnostics Tab	85

7.6.1	System Diagnostics	85
7.6.2	POST Codes.....	86
7.6.3	System Defaults.....	87
7.6.4	SOL Log	88
7.7	Miscellaneous Tab	89
7.7.1	Intel® Node Manager Configuration	89
7.7.2	Power Statistics.....	90
7.7.3	Power Telemetry	91
7.8	BIOS Configurations Tab.....	91
7.8.1	PCI Configuration	92
7.8.2	Serial Port Configuration	92
7.8.3	UPI Configuration.....	93
7.8.4	Integrated IIO Configuration.....	94
7.8.5	Memory Configuration.....	95
7.8.6	Power n Performance.....	97
7.8.7	Processor Configuration	98
7.8.8	Mass Storage Controller Configuration	99
7.8.9	System Acoustic and Performance Configuration	100
7.8.10	System Event Log.....	101
7.8.11	Security.....	101
7.8.12	USB Configuration	102
7.8.13	Server Management.....	103
7.8.14	Advanced Boot Options	104
7.8.15	Main	105
	Appendix A. Glossary.....	106

List of Figures

Figure 1. Intel® RMM4 Lite	18
Figure 2. Installing Intel® RMM4 Lite Module on Intel® Server Board.....	21
Figure 3. Intel® Server Board S2600WF – Intel® RMM4 Lite Connector and Intel® Dedicated Server Management NIC Location	21
Figure 4. Intel® Server Board S2600BP – Intel® RMM4 Lite Connector and Intel® Dedicated Server Management NIC Location	22
Figure 5. Intel® Server Board S2600ST – Intel® RMM4 Lite Connector and Intel® Dedicated Server Management NIC Location	22
Figure 6. Intel® Server Board S9200WK – Intel® RMM4 Lite Connector.....	23
Figure 7. BIOS Setup BMC LAN Configuration Screen.....	25
Figure 8. BIOS Setup User Configuration Screen	26
Figure 9. Integrated BMC Web Console Login Page.....	28
Figure 10. Integrated BMC Web Console Home Page	29
Figure 11. Logging Out of the Integrated BMC Web Console	31
Figure 12. Integrated BMC Web Console Help	31
Figure 13. Remote Control Console Redirection Page	32
Figure 14. Remote Console Window.....	33
Figure 15. Remote Console Main Window	34
Figure 16. Remote Console Control Bar	35
Figure 17. Remote Console Virtual Media Menu.....	35
Figure 18. Remote Console Virtual Storage Menu	35
Figure 19. Remote Console Virtual Keyboard Menu	36
Figure 20. Remote Console Macro Menu	36
Figure 21. Remote Console Options Menu	37
Figure 22. Remote Console HotKey Settings	37
Figure 23. Remote Console Display Settings	38
Figure 24. Remote Console Input Settings.....	39
Figure 25. Remote Console Window Settings.....	39
Figure 26. Remote Console Video Stream Settings.....	40
Figure 27. Remote Console Session Timeout Settings	40
Figure 28. Remote Console Debug Log Settings	40
Figure 29. Remote Console Control Panel – OSD UI style.....	41
Figure 30. Remote Console User List.....	42
Figure 31. Remote Console Capture Menu	43
Figure 32. Remote Console Power Control Menu	43
Figure 33. Exit the Remote Console	44
Figure 34. Remote Console Status Line.....	44
Figure 35. Busy Indicator Bar	45
Figure 36. System Information Page.....	45

Figure 37. FRU Board Options	46
Figure 38. System FRU Information Page	47
Figure 39. System CPU Information Page.....	48
Figure 40. System DIMM Information Page.....	49
Figure 41. System NVMe* Information Page	49
Figure 42. System NIC Information Page	50
Figure 43. System Storage Information Page.....	50
Figure 44. System Current Users Page.....	51
Figure 45. Server Health Sensor Readings Page (Thresholds Not Displayed).....	51
Figure 46. Server Health Sensor Readings Page (Thresholds Displayed)	52
Figure 47. Server Health Event Log Page.....	53
Figure 48. Alerts Page	54
Figure 49. Alert Email Page	55
Figure 50. Date & Time Page	56
Figure 51. IPV4 Network DHCP Page	57
Figure 52. IPv4 Network Static Page	58
Figure 53. IPv6 Network Page.....	59
Figure 54. VLAN Settings Page.....	61
Figure 55. LDAP Settings Page	62
Figure 56. Active Directory Settings Page	63
Figure 57. KVM & Media Page	64
Figure 58. SSL Certification Page	65
Figure 59. User List Page.....	66
Figure 60. Add New User Page	66
Figure 61. Modify User Page.....	67
Figure 62. Delete User Page	67
Figure 63. Configuration Security Settings Page	68
Figure 64. Server Power Control Page	70
Figure 65. BIOS/ME Firmware Update Page	70
Figure 66. BIOS Configuration Page	71
Figure 67. CPU Information Page	71
Figure 68. DIMM Information Page	72
Figure 69. SOL Page	72
Figure 70. SDR Configuration Page	73
Figure 71. BMC Firmware Update Page	74
Figure 72. Configuration BIOS/ME Firmware Update Page	75
Figure 73. Syslog Server Configuration Page	76
Figure 74. Remote Control KVM Page	77
Figure 75. Remote Control Server Power Control Page	78
Figure 76. Remote Control Launch SOL Page.....	79
Figure 77. Remote Control Launch SOL Screen Page	80

Figure 78. Remote Control Virtual Front Panel Page.....	80
Figure 79. iKVM over HTML5 Page	82
Figure 80. HTML5 Screen Page	82
Figure 81. HTML5 Virtual Keyboard Page.....	82
Figure 82. HTML5 Keyboard Macro Menu Page.....	83
Figure 83. HTML5 Power Control Menu page.....	83
Figure 84. Virtual Media over HTML5 Page.....	84
Figure 85. Launch Virtual Media over HTML5 Page.....	84
Figure 86. Plug in ISO	84
Figure 87. Web ISO.....	85
Figure 88. Server System Diagnostics Page.....	86
Figure 89. Server Diagnostics POST Codes Page	87
Figure 90. Server Diagnostics Default Page	87
Figure 91. Server Diagnostics SOL Log Page.....	88
Figure 92. Intel® NM Configuration Page.....	89
Figure 93. Intel® NM Configuration Suspend Page	90
Figure 94. Power Statistics Page.....	90
Figure 95. Power Telemetry page	91
Figure 96. Power Telemetry Device Categories.....	91
Figure 97. BIOS PCI Configuration Page.....	92
Figure 98. BIOS Serial Port Configuration Page	92
Figure 99. BIOS UPI Configuration Page	93
Figure 100. BIOS IIO Configuration Page	94
Figure 101. BIOS Memory Configuration Page.....	95
Figure 102. BIOS PnP Configuration Page.....	97
Figure 103. BIOS Processor Configuration Page	98
Figure 104. BIOS Mass Storage Controller Configuration Page	99
Figure 105. BIOS System Acoustic and Performance Configuration Page	100
Figure 106. System Event Log Page	101
Figure 107. BIOS Security Configuration Page	101
Figure 108. BIOS USB Configuration Page	102
Figure 109. BIOS Server Management Page.....	103
Figure 110. BIOS Advanced Boot Page.....	104
Figure 111. BIOS Main Page	105

List of Tables

Table 1. Intel® RMM4 Lite Connector Locations on Intel® Server Boards.....	20
Table 2. Integrated BMC Web Console Tabs.....	29
Table 3. Integrated BMC Web Console Toolbar.....	30
Table 4. Remote Console Log Level Definition.....	41
Table 5. Remote Console OSD UI Style Control Bar Options.....	41
Table 6. Remote Console Power Control.....	44
Table 7. System Information page details.....	46
Table 8. Server Health Sensor Readings Options	52
Table 9. Server Health Event Log Options	53
Table 10. Alerts Options	55
Table 11. Alert Email Options	56
Table 12. Date & Time Options	57
Table 13. IPv4 Network Settings Options	58
Table 14. IPv6 Network Settings Options	60
Table 15. VLAN Settings Options	61
Table 16. LDAP Settings Options	62
Table 17. Active Directory Settings Options.....	63
Table 18. KVM & Media Options	64
Table 19. Configuration Security Settings Options	68
Table 20. SOL Options.....	72
Table 21. SDR Configuration Options	73
Table 22. BMC Firmware Update Options	74
Table 23. Configuration BIOS/ME Firmware Update Options.....	75
Table 24. Syslog Server Configuration Options.....	76
Table 25. Macro Non-Printable Key Names.....	78
Table 26. Remote Control Power Control Options.....	79
Table 27. Remote Control Virtual Front Panel Options.....	81
Table 28. Virtual Media over HTML5 Options.....	85
Table 29. Web ISO Options	85
Table 30. Server Diagnostics SOL Log Options.....	88
Table 31. Intel® NM Configuration Options.....	89
Table 32. BIOS Serial Port Configuration Variables	93
Table 33. BIOS UPI Configuration Variables.....	93
Table 34. BIOS IIO Configuration Variables	94
Table 35. BIOS Memory Configuration Variables	96
Table 36. BIOS PnP Configuration Variables.....	97
Table 37. BIOS Processor Configuration Variables	99
Table 38. BIOS Mass Storage Configuration Variables	100
Table 39. BIOS System Acoustic and Performance Configuration Variables	100

Table 40. BIOS Security Variables.....	102
Table 41. BIOS USB Configuration Variables	102
Table 42. Server Management.....	103
Table 43. BIOS Advanced Boot	104
Table 44. BIOS Main Configuration Variables.....	105

1. Introduction

This user guide describes how to use the Intel® Remote Management Module 4 (Intel® RMM4) and the Integrated Baseboard Management Controller (Integrated BMC) web console. It provides an overview of the features of the web console and the Intel RMM4 module along with instructions on how to set up and operate the Intel RMM4 module.

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.

Designed to work with the BMC, the Intel RMM4 Lite is a small form-factor mezzanine card that enables remote keyboard, video, and mouse (KVM) and media redirection on the server system through the built-in web console, from anywhere, at any time. Use the Intel RMM4 to install, update, and monitor the operating system.

1.1 Support Information

For support on the Integrated BMC Web Console and the Intel RMM4, 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. Intel® Remote Management Module 4 (Intel® RMM4)

This section provides an overview of the Intel RMM4 and highlights significance benefits of its features.

2.1 Intel® RMM4 Lite Overview

The Intel RMM4 comes in one package – the Intel RMM4 Lite. The Intel® Dedicated Server Management NIC is an onboard dedicated management port.

The Intel RMM4 Lite is a small board that unlocks advanced management features on the RGMII interface when installed on Intel® server boards. It provides an increased level of manageability over the basic server management available to the server board. It works as an integrated solution on the server system.

After the Intel RMM4 Lite has been installed, the advanced management features are available through both the onboard Intel Dedicated Server Management NIC and all onboard Integrated BMC-shared NIC ports.



Figure 1. Intel® RMM4 Lite

2.2 Intel® RMM4 Lite Features

The Intel RMM4 add-on offers convenient, remote KVM access and control through LAN or Internet. It captures, digitizes, and compresses video and transmits it with keyboard and mouse signals to and from a remote computer. Remote access and control software runs in the Integrated Baseboard Management Controller, utilizing expanded capabilities enabled by the Intel RMM4 hardware.

Key features of the Intel RMM4 add-on card include:

- KVM redirection – Allows up to four simultaneous KVM sessions (one full session and video-only for subsequent sessions) from either the RMM4 NIC or the baseboard NIC used for management traffic.
- Media redirection – Allows system administrators or users to mount a remote IDE or USB CD-ROM, floppy, or a USB flash disk as a remote device to the server. In addition to physical devices, disk images in IMA, IMG, and ISO formats can be virtually mounted. After being mounted, the remote device appears just like a local USB device to the server, allowing system administrators to boot from the device, install software (including operating systems), copy files, update BIOS, and so on.
- KVM – Automatically senses video resolution for best possible screenshot, high-performance mouse tracking, and synchronization. It allows remote viewing and configuration in pre-boot POST and BIOS setup.

2.3 Supported Operating Systems and Browsers

The Intel RMM4 enabled features run independently of the host operating system on the server where it is installed except during remote console (KVM) connections. During remote console connections, the keyboard, video, and mouse of the console system operate just as if they were physically at the server where the Intel RMM4 is connected. During remote console connections, the interaction with the host operating system limits the support to operating systems that have been validated. Those operating systems are listed in the following sub sections.

2.3.1 Server System

The following operating systems are supported on the managed server:

- Microsoft Windows Server* 2012 R2
- Microsoft Windows Server* 2016
- Microsoft Windows* 10 (Redstone 2)
- Red Hat* Enterprise Linux* 6.9 x64
- Red Hat* Enterprise Linux* 7.3 x64
- SUSE* Enterprise Linux* 11 SP4 x64
- SUSE* Enterprise Linux* 12 SP2 x64
- VMware* ESXi 6.5U1
- CentOS* 7.3
- Ubuntu* 17.04

2.3.2 Client System

The following client browsers have been tested:

- Microsoft Internet Explorer* – versions 10 and 11
- Mozilla Firefox* – versions 53 and 54
- Google Chrome* – versions 59 and 60
- Apple Safari* – version 10

3. Installing the Hardware

Before beginning, carefully read the safety information provided in the front matter of this manual.

3.1 Intel® RMM4 Lite Installation

3.1.1 Required Tools

The following tools and supplies are required for installation:

- Phillips* (cross-head) screwdriver (#1 bit and #2 bit)
- Needle-nose pliers
- Antistatic wrist strap and conductive foam pad (recommended)

3.1.2 Installation Procedure

Caution: Intel RMM4 Lite devices are not hot-swappable. Before removing or replacing them, do the following:

1. Take the server out of service.
2. Power off the system.
3. Unplug the AC power cord from the system or wall outlet.
4. Wait for the power supply LEDs to turn off.

To install the Intel RMM4 Lite in Intel® Server Boards S2600WF, S2600BP, and S2600ST product families, follow the steps below:

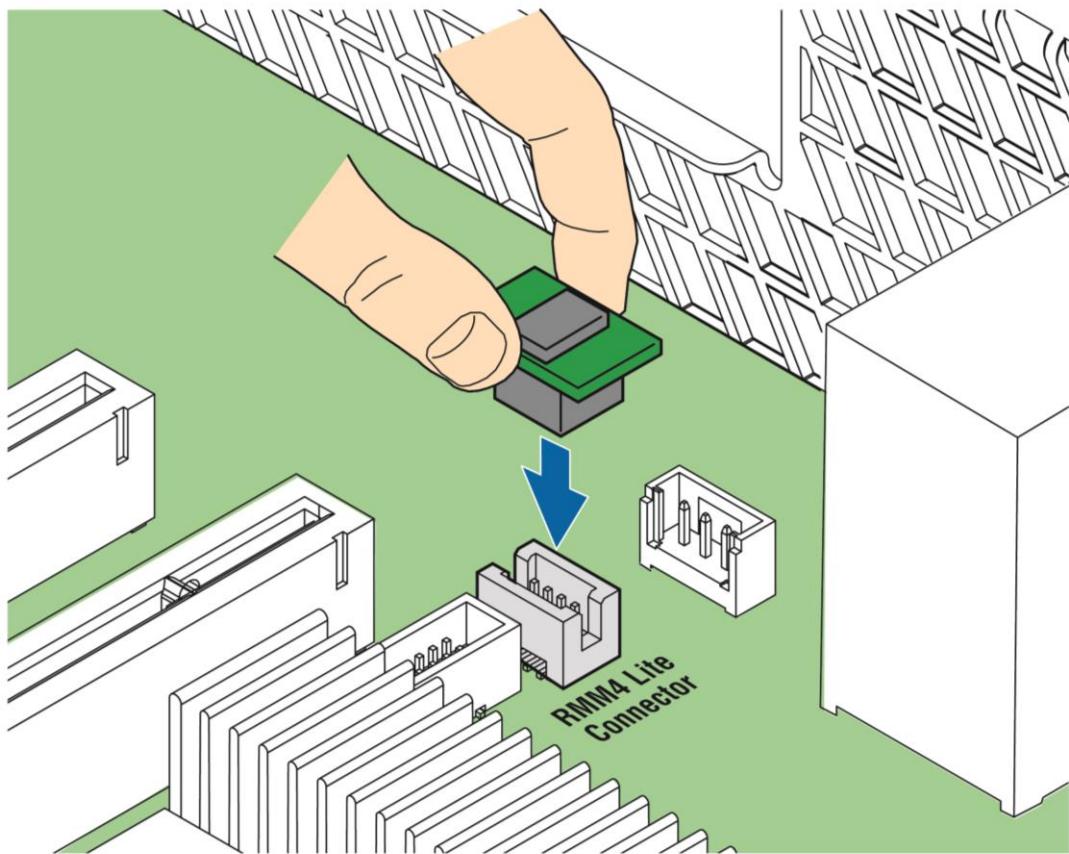
1. Ensure that the AC power is removed from the system and that the power supply LEDs are off.
2. Find the Intel RMM4 Lite connector as specified in [Table 1](#) for each server board product family.

Table 1. Intel® RMM4 Lite Connector Locations on Intel® Server Boards

Intel® Server Board	Intel® RMM4 Lite Connector	Refer to
Intel® Server Board S2600WF	J1D2	Figure 3
Intel® Server Board S2600BP	J2A1	Figure 4
Intel® Server Board S2600ST	J1D1	Figure 5
Intel® Server Board S9200WK	J46X1	Figure 6

3. Carefully pick up the Intel RMM4 Lite module. Verify the location of the Intel RMM4 Lite connector key pin 1 location and insert the Intel RMM4 Lite into the mating connector on the Intel server board ([Figure 2](#)).

Note: For more details, refer to the specific Intel® server system technical product specification (TPS) and service guide.



AF003760

Figure 2. Installing Intel® RMM4 Lite Module on Intel® Server Board

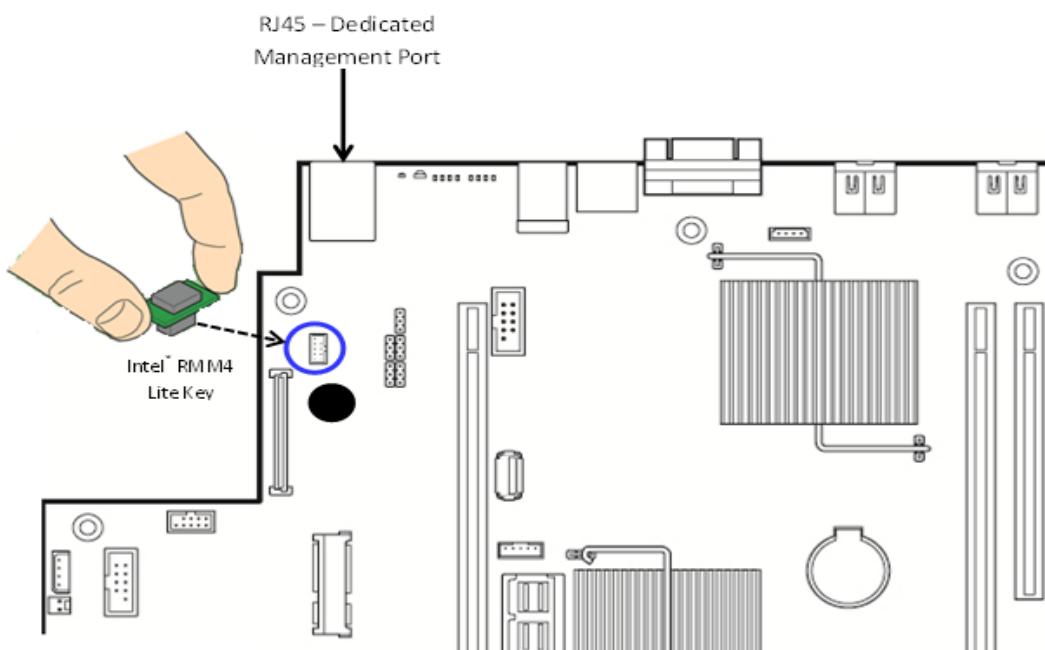


Figure 3. Intel® Server Board S2600WF – Intel® RMM4 Lite Connector and Intel® Dedicated Server Management NIC Location

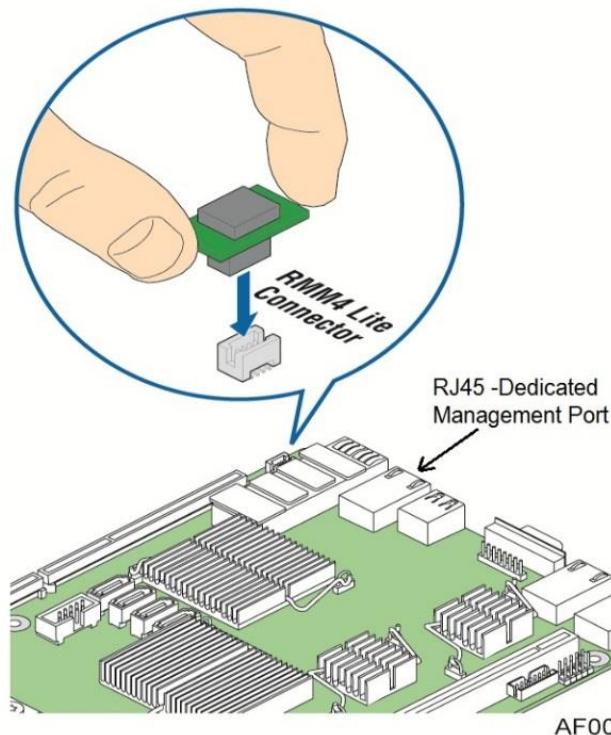


Figure 4. Intel® Server Board S2600BP – Intel® RMM4 Lite Connector and Intel® Dedicated Server Management NIC Location

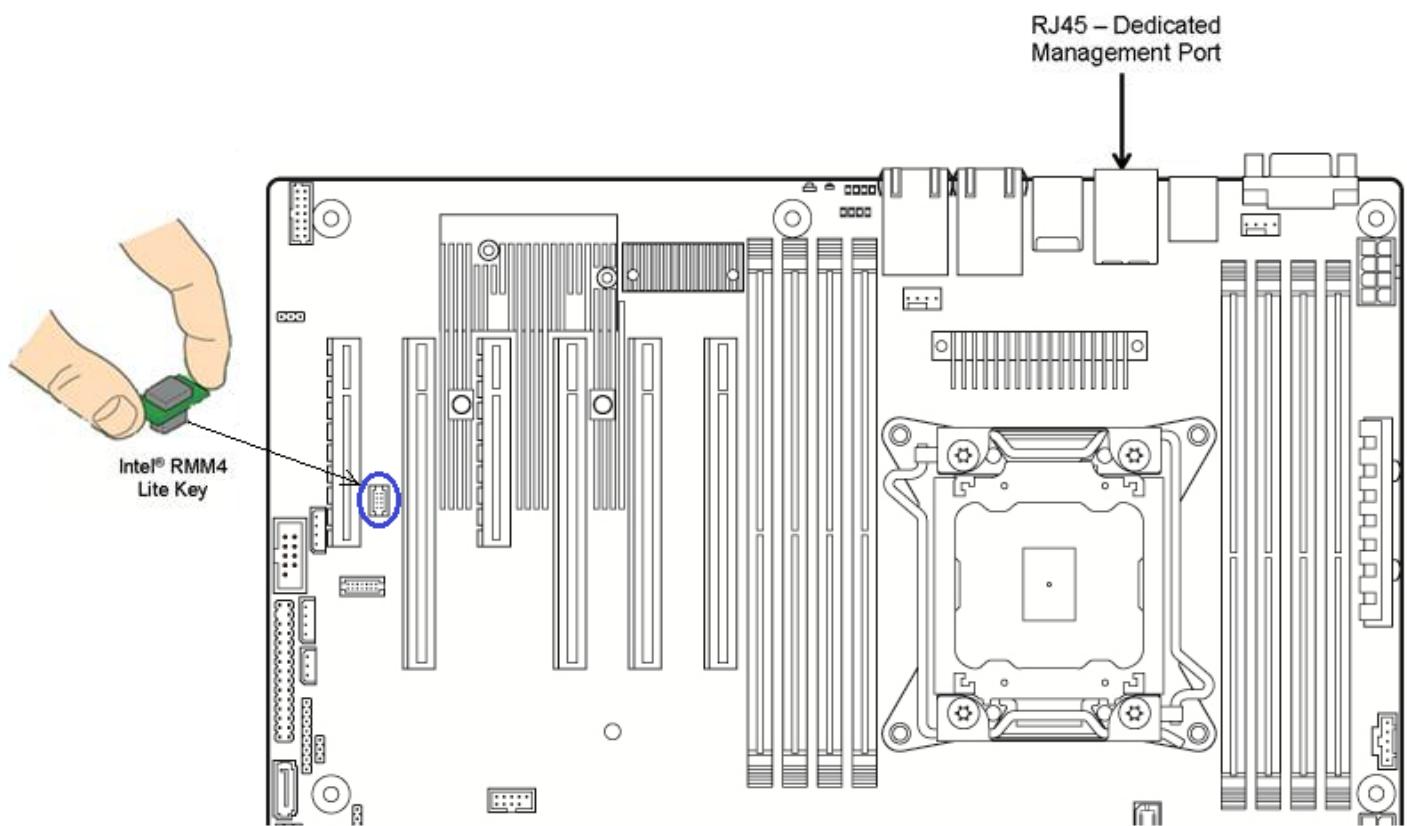


Figure 5. Intel® Server Board S2600ST – Intel® RMM4 Lite Connector and Intel® Dedicated Server Management NIC Location

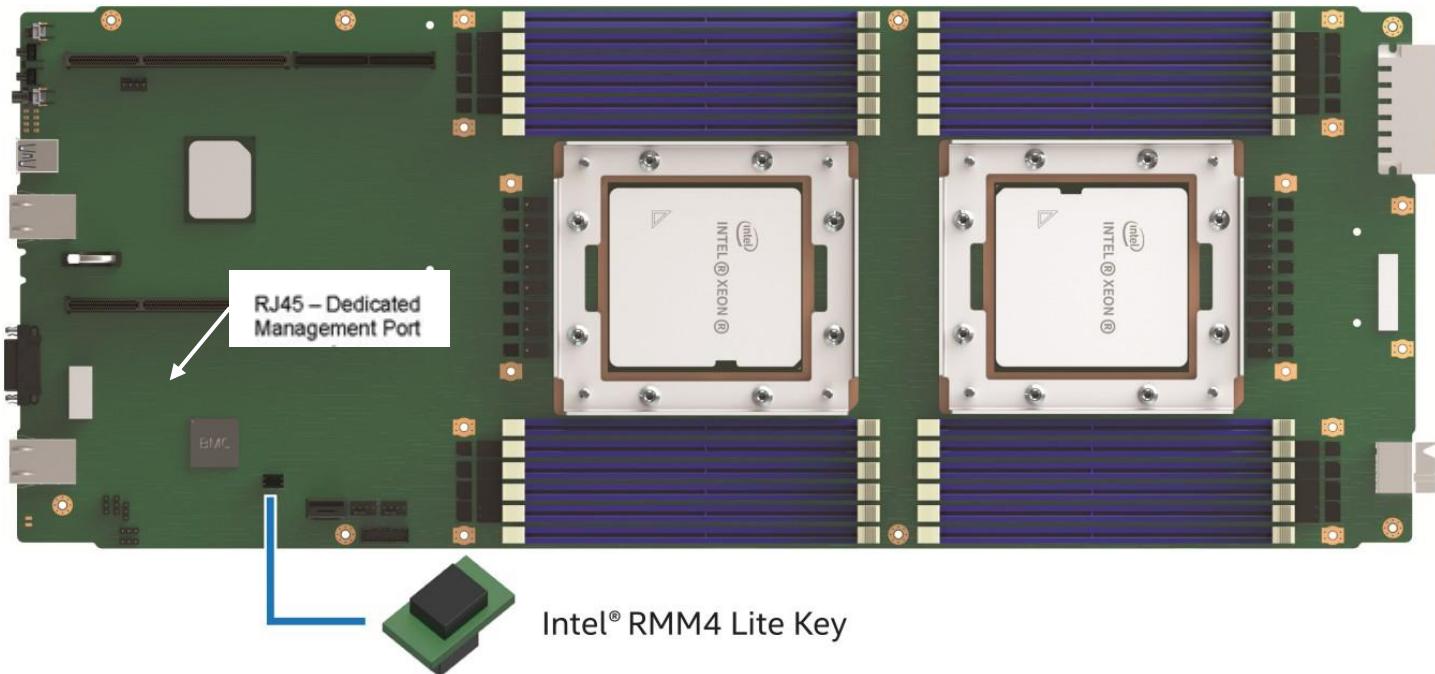


Figure 6. Intel® Server Board S9200WK – Intel® RMM4 Lite Connector

3.2 Intel® Dedicated Server Management NIC

For Intel® Server Boards S2600WF, S2600BP, S2600ST, and S9200WK product families, the Intel® Dedicated Server Management NIC is included onboard and does not need to be manually installed. The Intel® Dedicated Server Management NIC has its own, single and separate, dedicated management port. The port location varies by platform as shown in [Figure 3](#), [Figure 4](#), [Figure 5](#), and [Figure 6](#).

Caution: Because the BMC does not allow for manual configuration of speed and duplex, any switch port to which the BMC is connected must be configured to auto negotiation, which follows industry best practices for 1GbE devices.

4. Configuring Server Management Hardware

This section discusses using the server utilities to enable a system to use the Integrated BMC Web Console or the Intel RMM4 from a new, unset state to an operational one.

When first powered on, by default, the server management BMC LAN and the Intel® RMM4 have a static IP address of 172.16.10.10.

Two steps are necessary before server management BMC LAN or the Intel RMM4 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 and the Intel RMM4 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 7](#)).
3. For a Host Interface (HI) network:
 - Scroll to **HI BMC LAN configuration > IP source**, and then select **Static**. Configure the **IP address**, **Subnet Mask**, and **Gateway IP** as needed.
4. 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 Intel RMM4, 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.
5. 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.
 - If configuring the Intel RMM4, scroll down to **Dedicated Management LAN IPv6 Configuration > IP source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IPV6 address**, **Gateway IPV6**, and **IPV6 Prefix Length** as needed.
6. Select **User Configuration** to enter the User Configuration screen ([Figure 8](#)).
7. 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 Intel RMM4 Lite.)
 - **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.

8. Press <F10> to save the configured settings and exit BIOS setup. The server reboots with the new LAN settings.

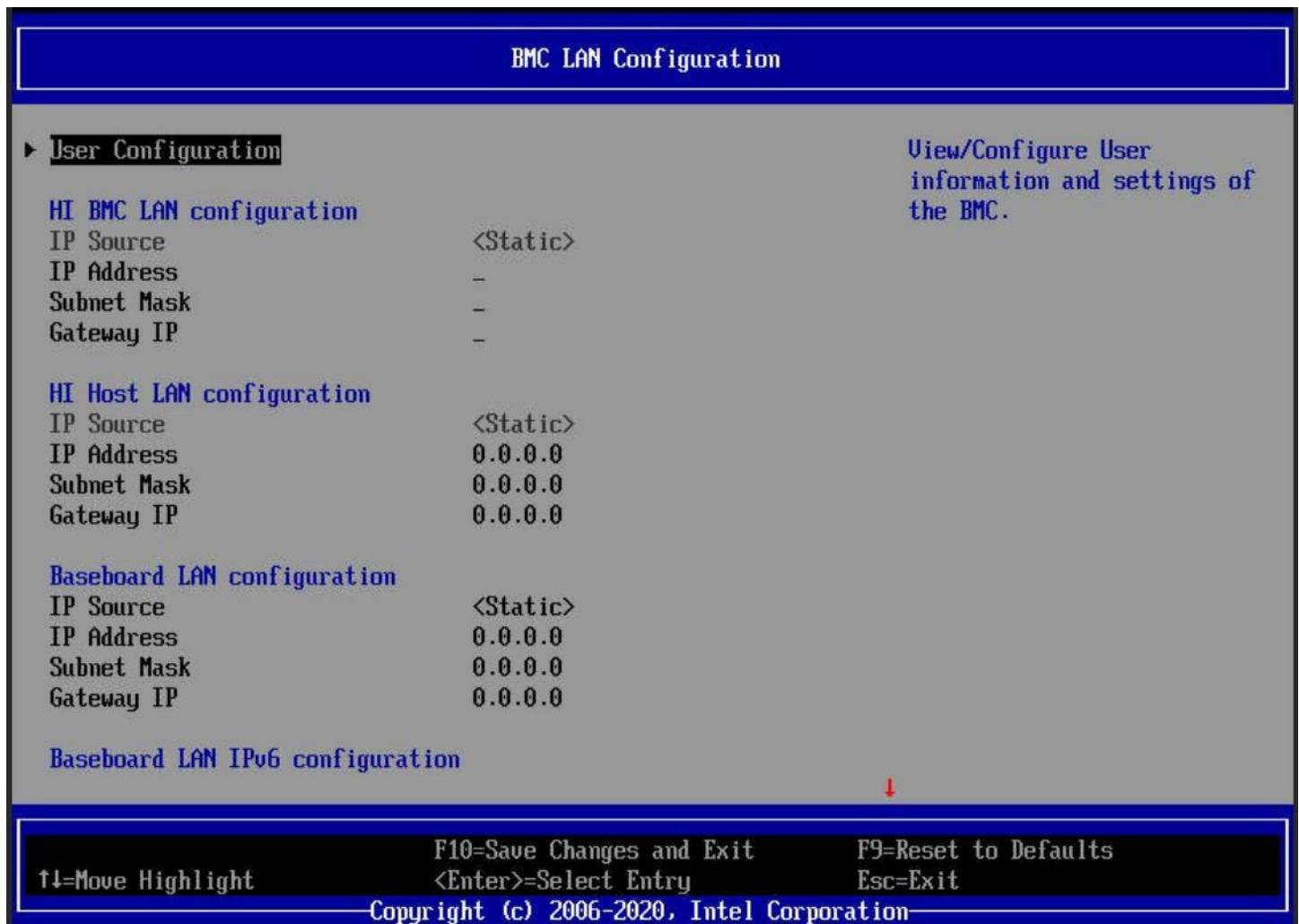


Figure 7. BIOS Setup BMC LAN Configuration Screen



Figure 8. BIOS Setup User Configuration Screen

4.2 Configuring Server Management Hardware Using SYSCFG

This section describes the basic commands needed to configure the Intel RMM4 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 Intel® RMM4 Operation

The Intel RMM4 module 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 [Section 6](#) and [Section 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 Intel RMM4 advanced 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 webpage.

5.2 Logging In

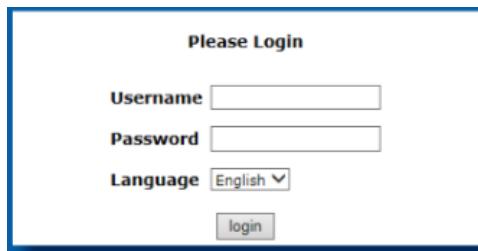
Enter the configured IP address of the Intel RMM4 or the configured BMC onboard NIC into the web browser to open the Integrated BMC Web Console module login page ([Figure 9](#)). To use a secure connection, type:

`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 home page.



Please Login

Username

Password

Language English

Figure 9. 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 Intel RMM4 enabled advanced 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 home page contains eight tabs along the top for navigation within the web console (Figure 10). For details on each tabbed page, see Table 2. 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.

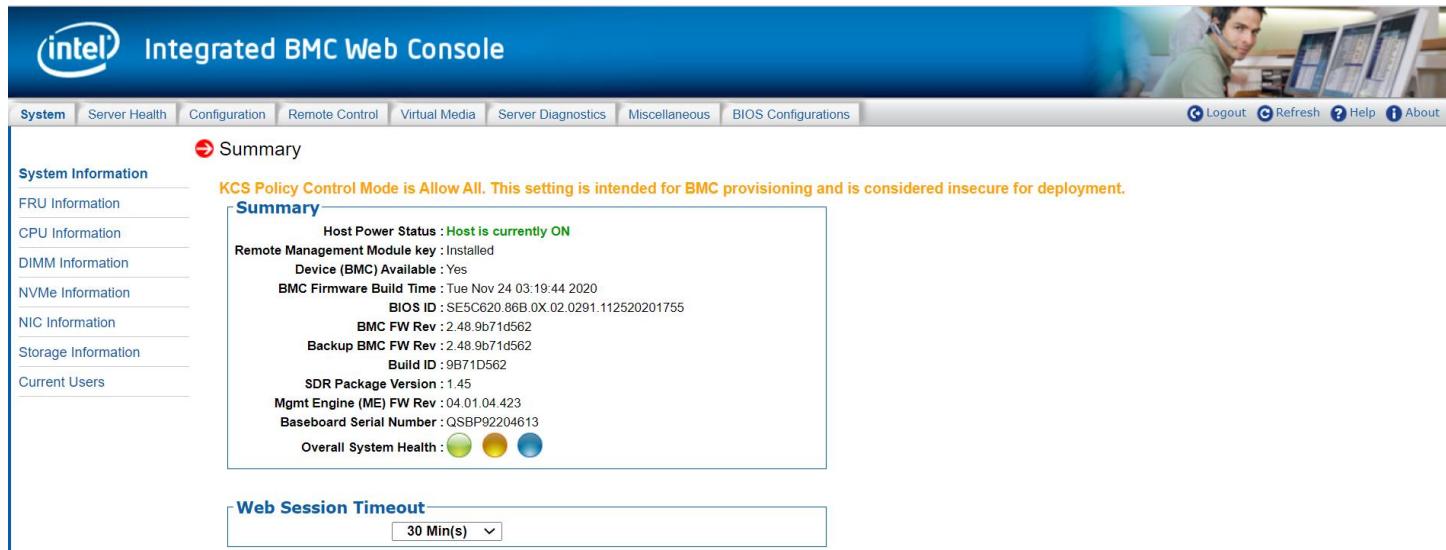


Figure 10. Integrated BMC Web Console Home Page

Table 2. 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 • Users • Security Settings • SOL • SDR Configuration • BMC Firmware Update • BIOS/ME Firmware Update • Syslog Server Configuration

Tab	Function	Secondary Menu
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 the user 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
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 the following table.

Table 3. Integrated BMC Web Console Toolbar

Button	Function
Logout	End the current web console session. Click OK to confirm (Figure 11). After logging out, the web console returns to the login screen.
Refresh	Refresh the current webpage, including any data shown on the page. Note: Using the web browser'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 home page.
Help	View a brief description of the current page in a frame at the right side of the browser window (Figure 12). 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.

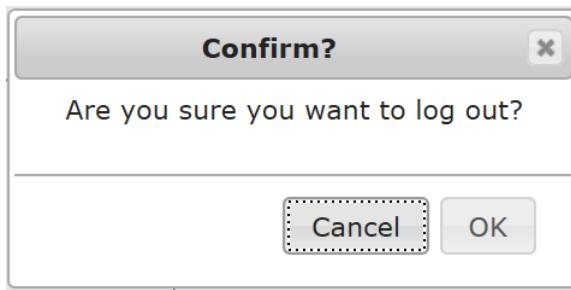


Figure 11. Logging Out of the Integrated BMC Web Console

A screenshot of the Integrated BMC Web Console. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, and BIOS Configurations. On the right, there are links for Logout, Refresh, Help, and About. The main content area shows 'System Information' with sections for FRU, CPU, DIMM, NVMe, NIC, Storage, and Current Users. A 'Summary' section displays system status: Host Power Status (ON), Remote Management Module key (Installed), Device (BMC) Available (Yes), BMC Firmware Build Time (Tue Nov 24 03:19:44 2020), BIOS ID (SE5C620 86B.0X.02.0291.112520201755), BMC FW Rev (2.48.9b71d562), Backup BMC FW Rev (2.48.9b71d562), Build ID (9b71D562), SDR Package Version (1.45), Mgmt Engine (ME) FW Rev (04.01.04.423), and Baseboard Serial Number (QSPB92204613). Below this is a 'Web Session Timeout' field set to 30 Min(s). To the right, a 'System Information - Help' sidebar provides detailed descriptions for each of these parameters.

Figure 12. 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 timeout.

6. Remote Console (KVM) Operation

The remote console is the redirected keyboard, video, and mouse of the remote host system where the Intel RMM4 module is installed. 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 13).

Note: If the user is 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.

The screenshot shows the Integrated BMC Web Console interface. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control (which is highlighted in blue), Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. Below the navigation bar, the main content area has a title 'KVM/Console Redirection' with a 'Launch Console' button. A section titled 'Keyboard Macros' contains a table for defining macros. The table has two columns: 'Key Sequence' and 'Button Name'. There are ten rows, each labeled #1 through #10, with input fields for both columns. A 'Save' button is located at the bottom of the macro table. On the left side of the main content area, there's a sidebar with links for KVM/Console Redirection, Server Power Control, Launch SOL, Virtual Front Panel, and iKVM over HTML5.

Figure 13. 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 stand-alone Java application implementing the remote console.

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

Notes:

- Java Runtime Environment* (JRE*, Version 6 Update 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.

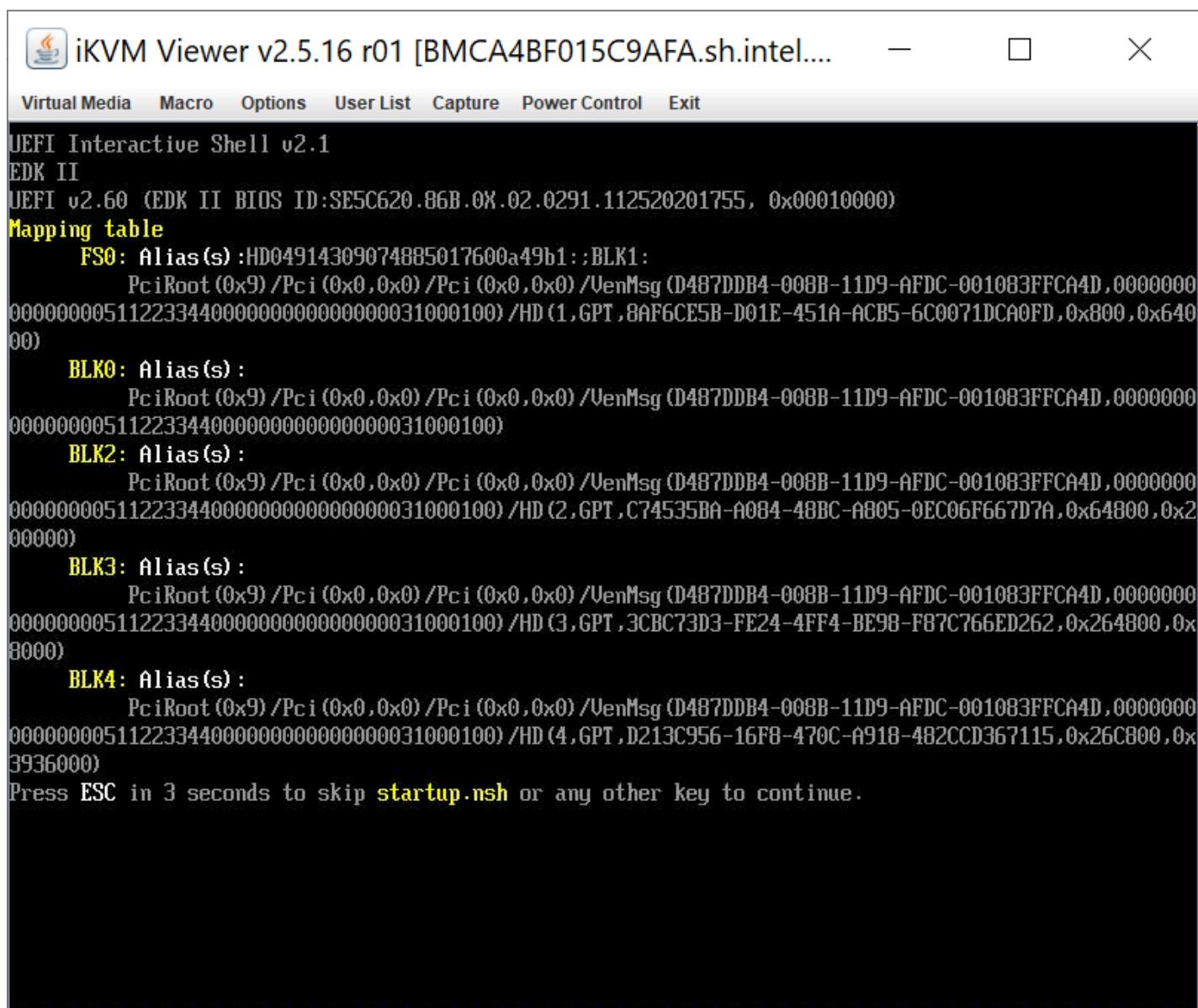
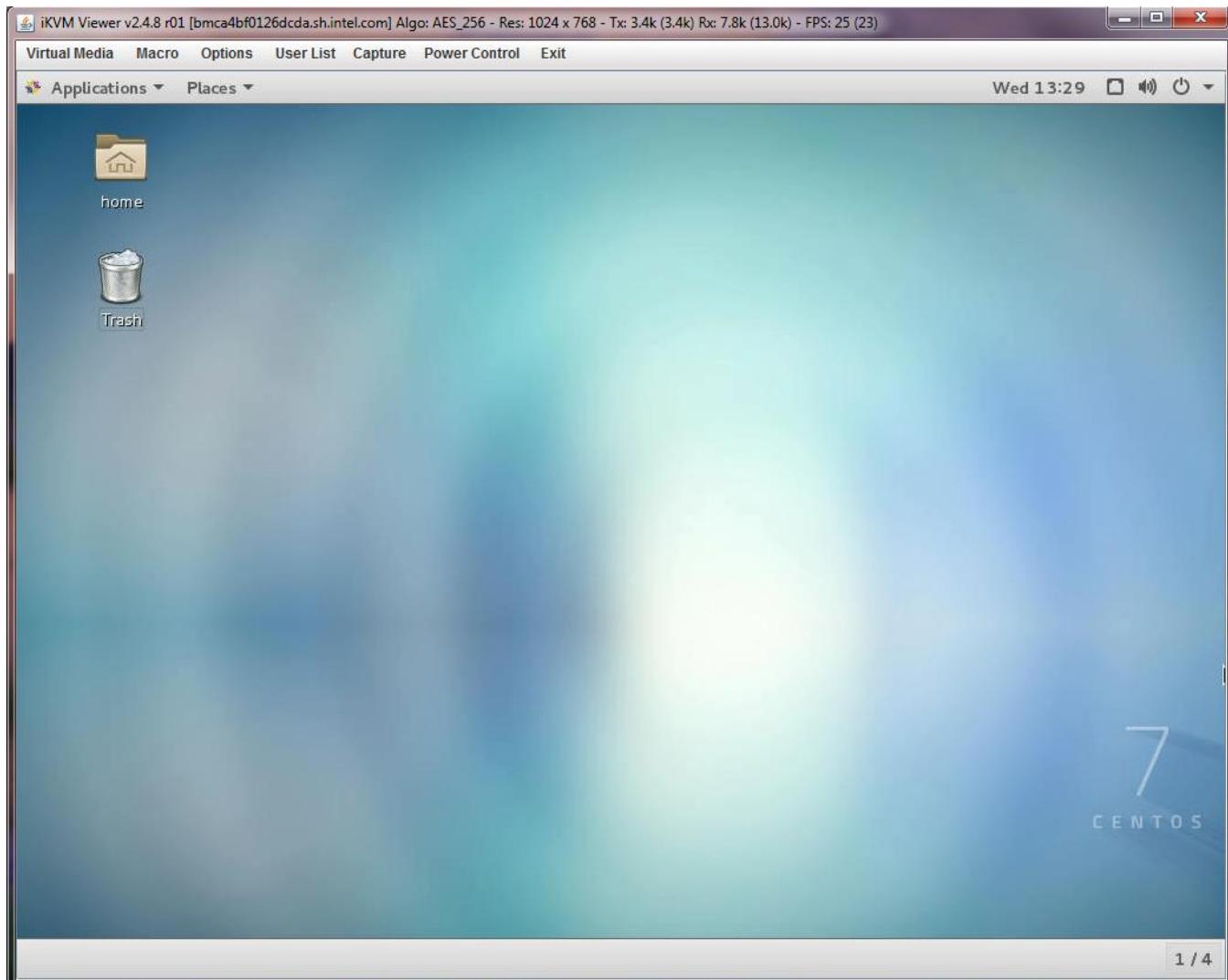


Figure 14. Remote Console Window

6.2 Main Window

Starting the remote console opens a host window (Linux* operating system window shown in [Figure 15](#)).



[Figure 15. 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 16. 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 17](#).

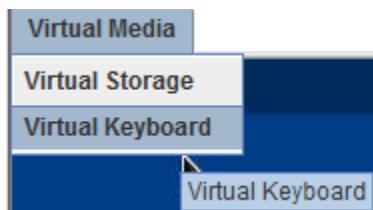


Figure 17. Remote Console Virtual Media Menu

Use the options in this menu to do the following:

- **Virtual Storage** – Allow starting/stopping remote media redirection as shown in [Figure 18](#). Redirect up to four devices at the same time. Select a logical device from a local CD-ROM/DVD drive or an ISO image on the local client file system as a virtual CD-ROM 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.

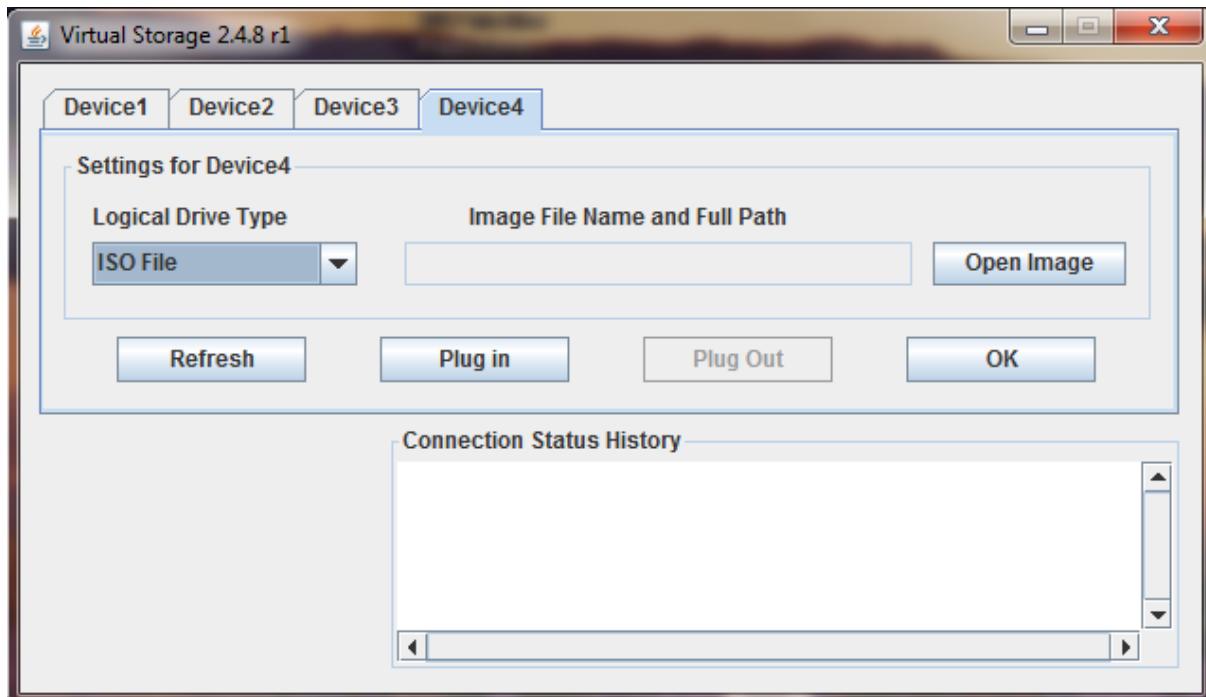


Figure 18. Remote Console Virtual Storage Menu

- **Virtual Keyboard** – Display a soft keyboard as shown in [Figure 19](#).



Figure 19. Remote Console Virtual Keyboard Menu

6.3.2 Macro Menu

Click **Macro** to open the keyboard macro menu as shown in [Figure 20](#).

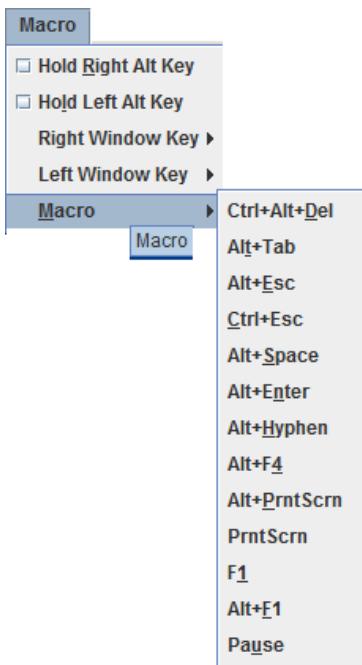


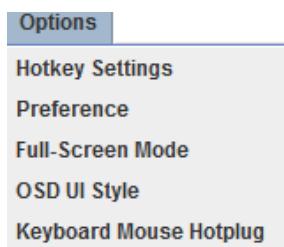
Figure 20. Remote Console Macro Menu

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

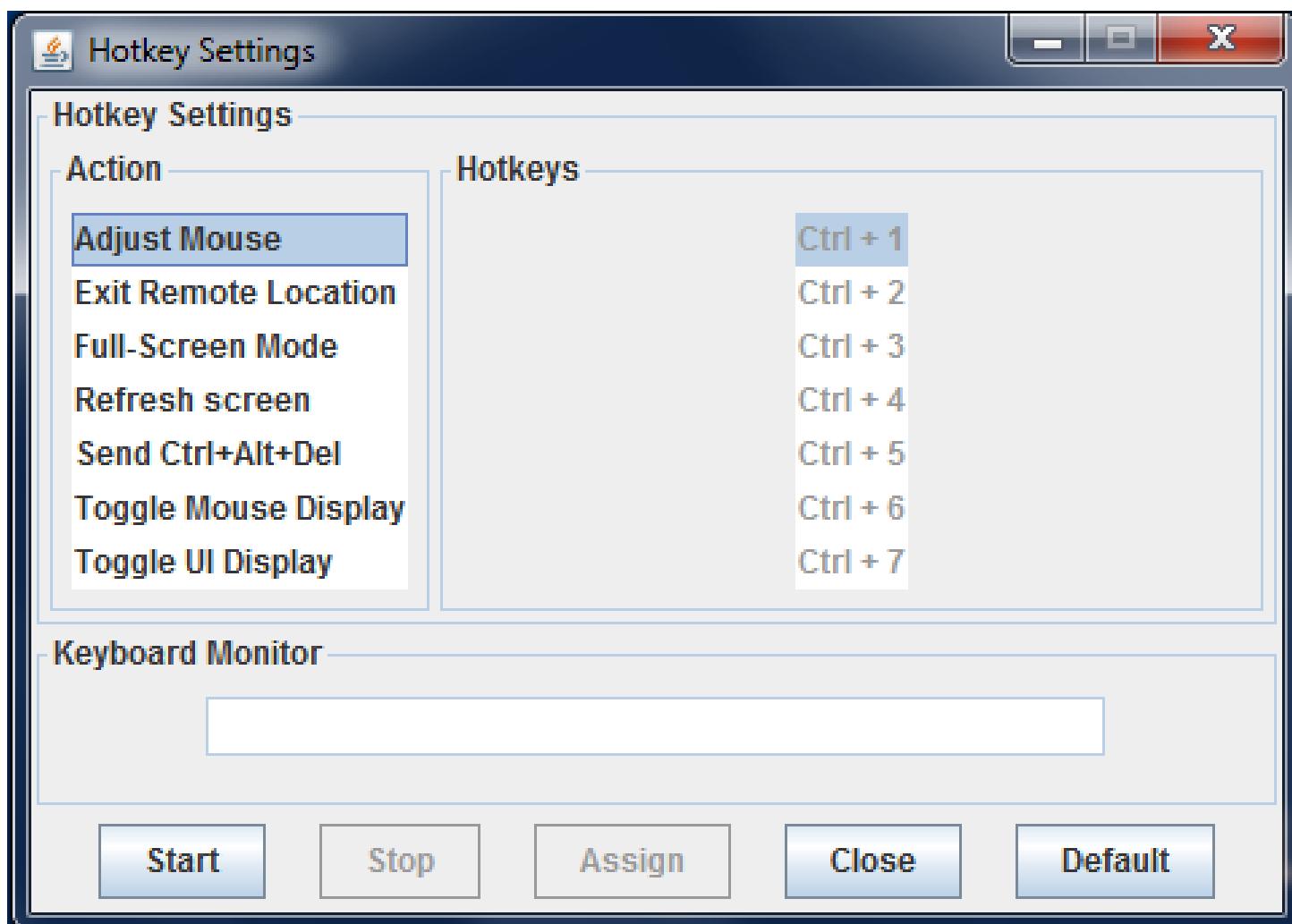
Click **Options** to open the options menu as shown in [Figure 21](#).



[Figure 21. Remote Console Options Menu](#)

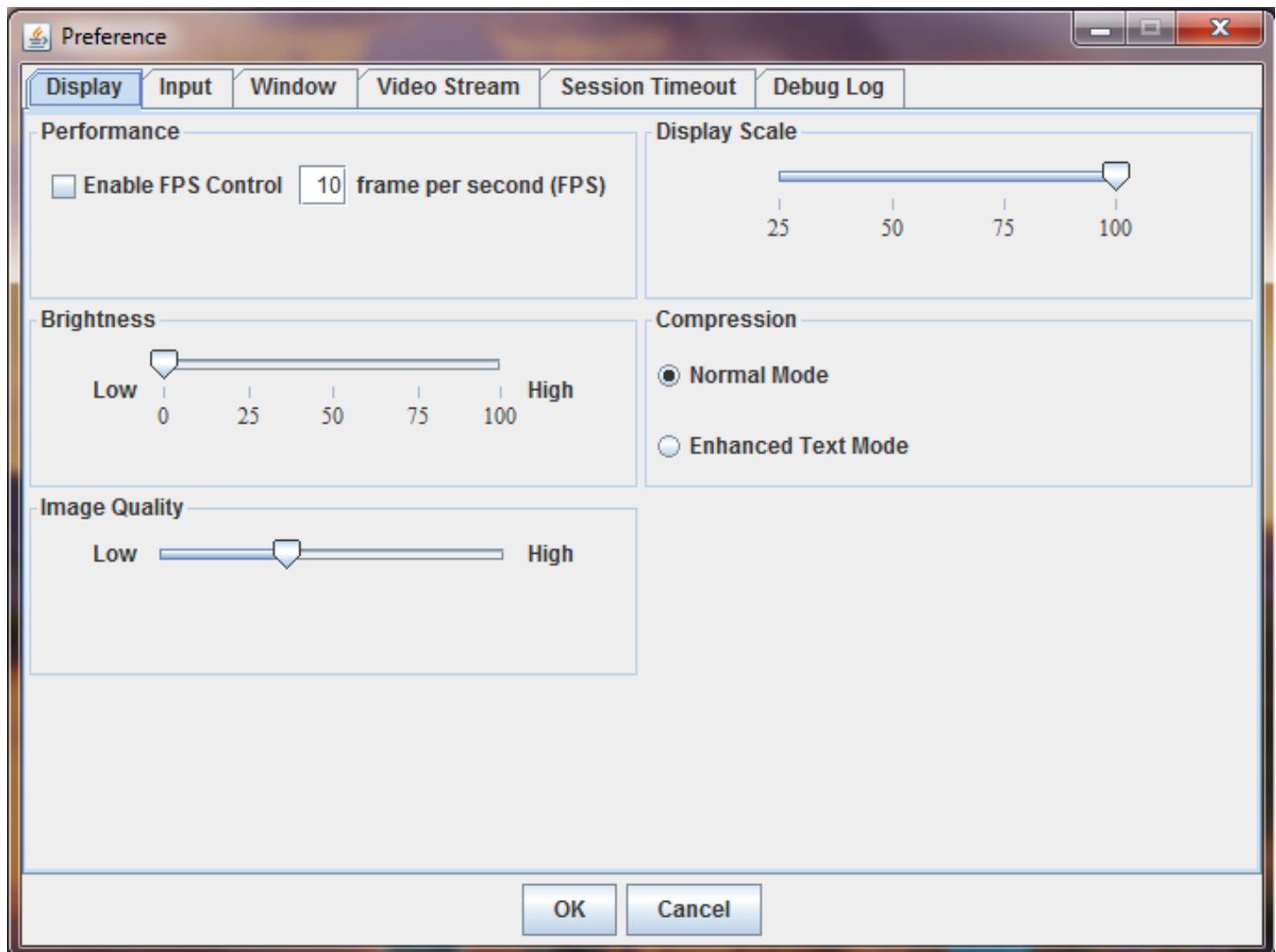
Use the options in this menu, to do the following:

- **HotKey Settings** – Configure hotkeys as shown in [Figure 22](#). 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.



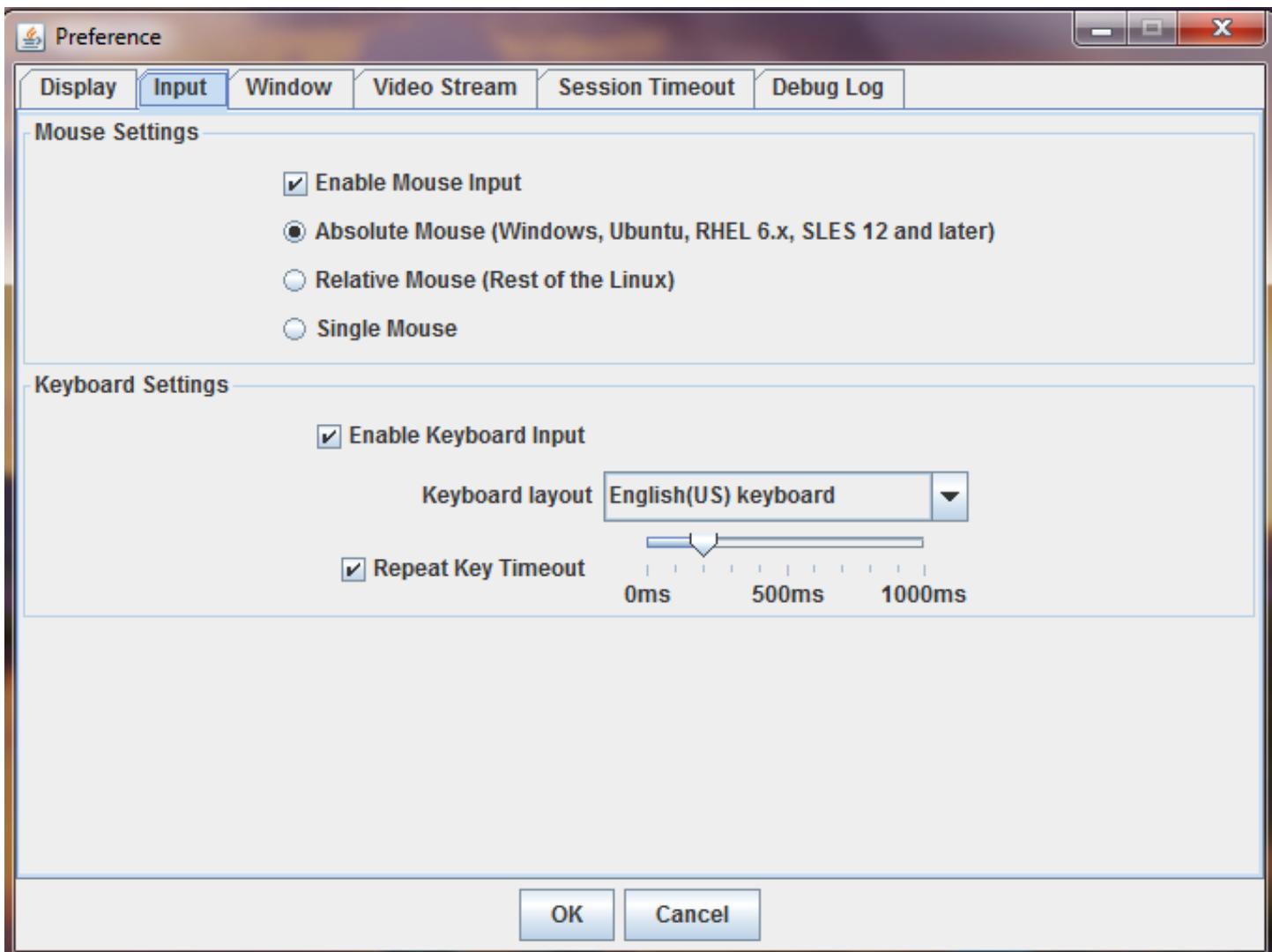
[Figure 22. Remote Console HotKey Settings](#)

- **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 23](#)) – Adjust display brightness, image quality, display scale, and compression mode and enable FPS control by specifying frames per second.



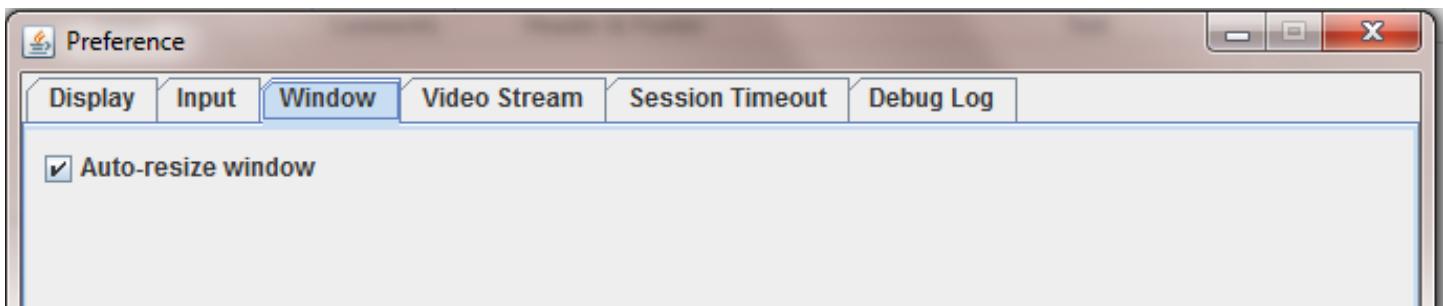
[Figure 23. Remote Console Display Settings](#)

- **Input** ([Figure 24](#)) – Enable/disable mouse/keyboard input, change the mouse mode, specify keyboard layout, and set repeat key timeout.



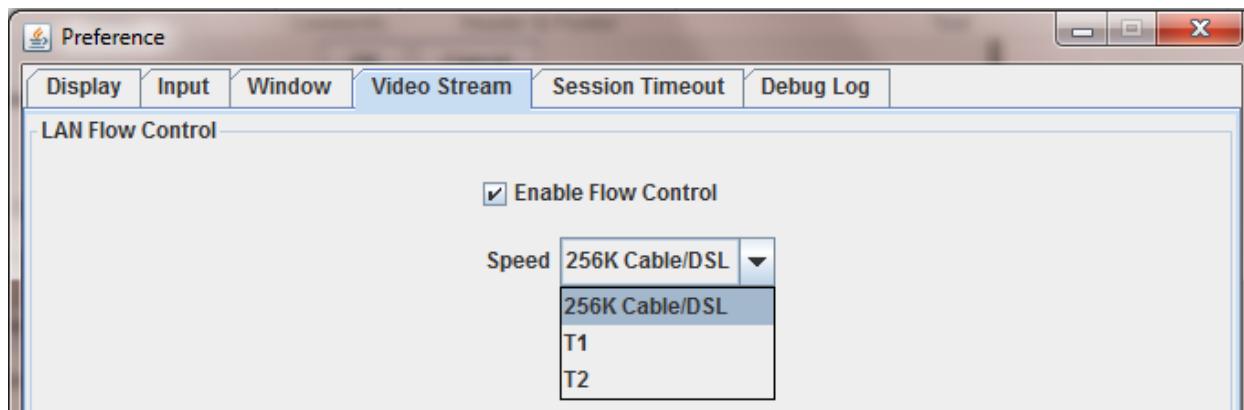
[Figure 24. Remote Console Input Settings](#)

- **Window** ([Figure 25](#)) – Enable or disable window auto-resize.



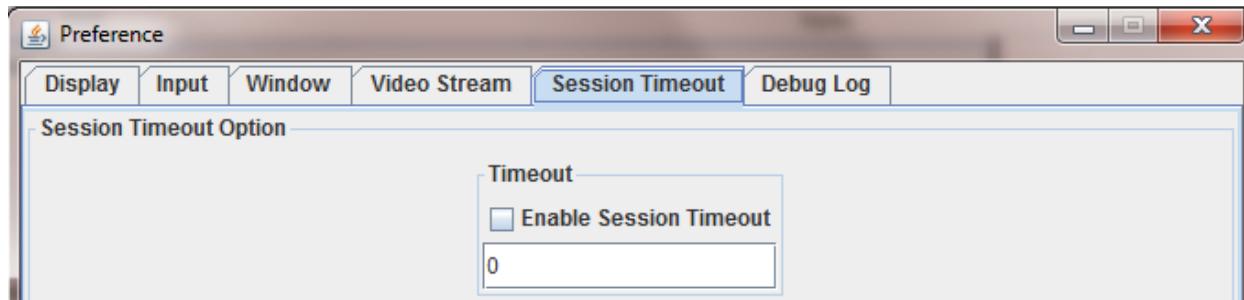
[Figure 25. Remote Console Window Settings](#)

- **Video Stream** ([Figure 26](#)) – Enable flow control by specifying a speed of T1, T2, or 256K Cable/DSL.



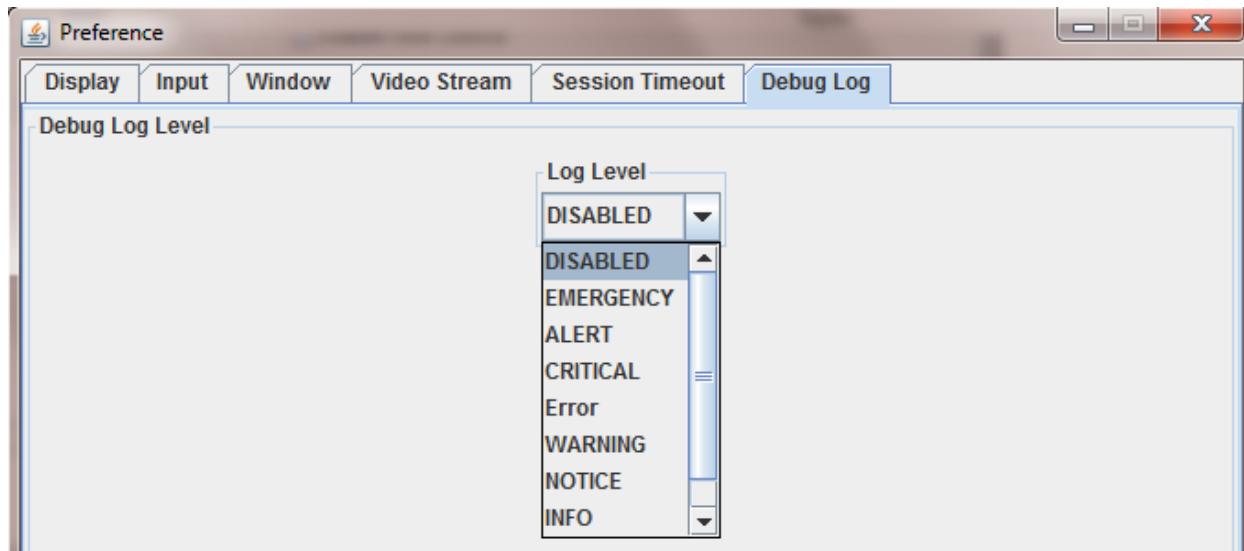
[Figure 26. Remote Console Video Stream Settings](#)

- **Session Timeout** ([Figure 27](#)) – Enable session timeout by specifying how many minutes for timeout.



[Figure 27. Remote Console Session Timeout Settings](#)

- **Debug Log** ([Figure 28](#)) – Select a log level of Disabled, Emergency, Alert, Critical, Error, Warning, Notice, Info, or Debug. [Table 4](#) defines each log level. The debug level is only for Java viewers and log messages will appear on the Java console, if enabled.



[Figure 28. Remote Console Debug Log Settings](#)

Table 4. 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 29. Clicking the icons on this window performs tasks as shown in Table 5.



Figure 29. Remote Console Control Panel – OSD UI style

Table 5. 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 30).

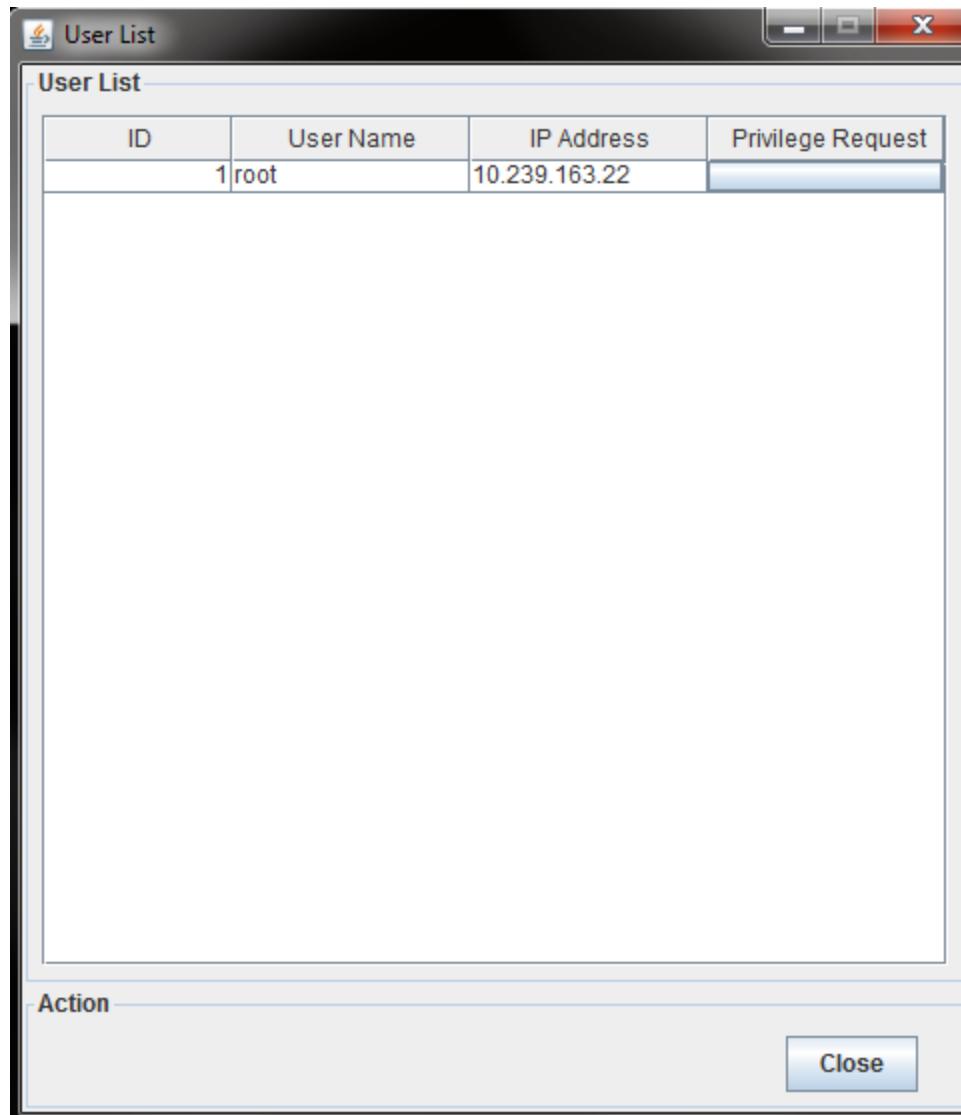


Figure 30. Remote Console User List

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.

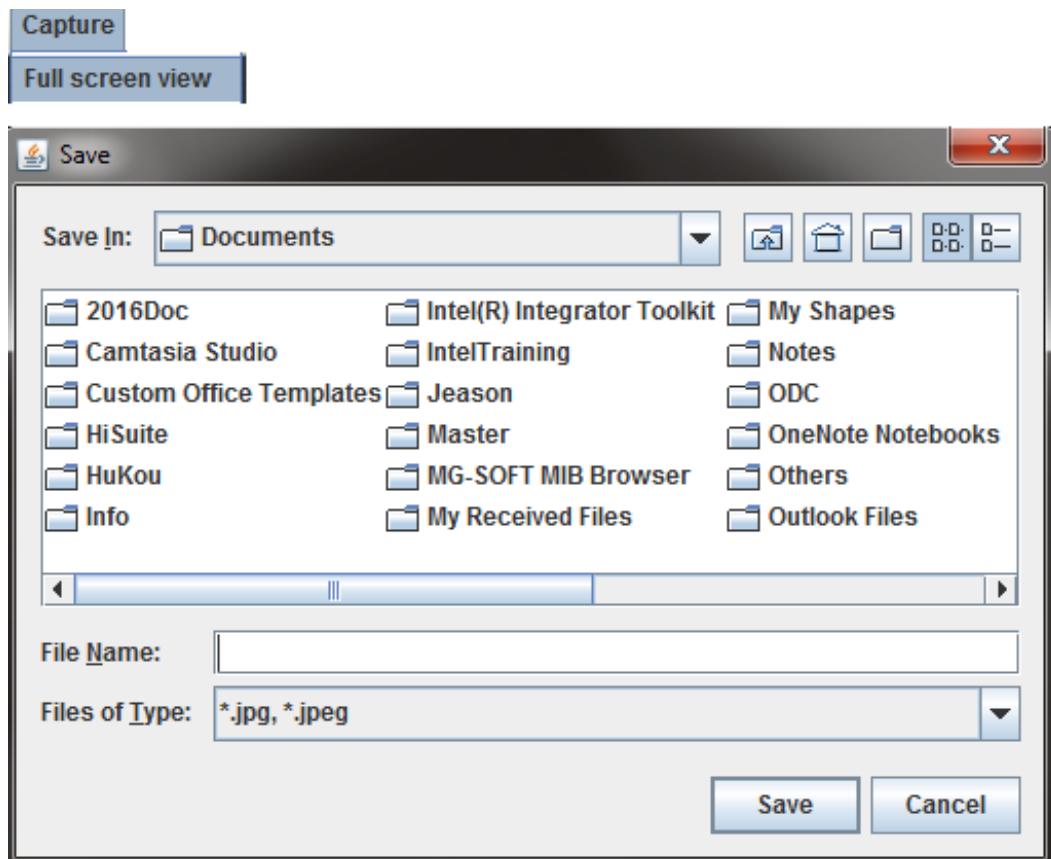


Figure 31. Remote Console Capture Menu

6.3.6 Power Control Menu

Click **Power Control** to open the power control menu as shown in Figure 32.



Figure 32. Remote Console Power Control Menu

Table 6 describes the power control operations that can be performed.

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

Table 6. 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 33) to exit the remote console.



Figure 33. 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. The status line provides BMC host name, Java encryption, resolution, transaction speed, and display frames per second.

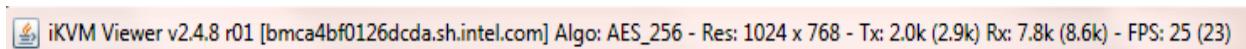


Figure 34. Remote Console Status Line

7. Integrated BMC Web Console Options

This chapter gives a detailed description of each Integrated BMC Web Console page. It is 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 2](#). 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 35](#).



Figure 35. Busy Indicator Bar

Note: Not all of the following sections are used by or directly related to Intel RMM4 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, Intel RMM4 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 7](#).

System Information

Summary

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

Summary

Host Power Status : Host is currently ON
Remote Management Module Key : Installed
Device (BMC) Available : Yes
BMC Firmware Build Time : Tue Nov 24 03:19:44 2020
BIOS ID : SE5C620 86B 0X.02.0291.112520201755
BMC FW Rev : 2.48.9b71d562
Backup BMC FW Rev : 2.48.9b71d562
Build ID : 9b71D562
SDR Package Version : 1.45
Mgmt Engine (ME) FW Rev : 04.01.04.423
Baseboard Serial Number : QSBP92204613
Overall System Health :

Web Session Timeout

30 Min(s)

Figure 36. System Information Page

Table 7. System Information page details

Information	Details
Host Power Status	Power status of the host (on/off).
Remote Management Module Key	Indicates whether the Intel RMM4 card is present.
Device (BMC) Available	Indicates whether the BMC is available for normal management tasks.
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.
SDR Package Version	Version of the Sensor Data Record.
Mgmt Engine (ME) FW Rev	Major and minor revision of the Management Engine firmware.
Baseboard Serial Number	Serial number of the baseboard in this system.
Overall System Health	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 37](#)).

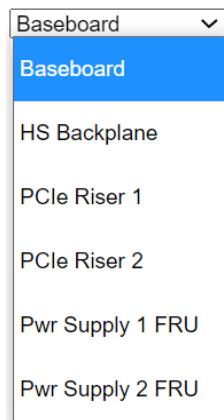


Figure 37. FRU Board Options

All data in the FRU information page is compliant with standard specifications (Platform Management FRU Information Storage Definition). See [Figure 38](#) for details of the baseboard FRU.

The screenshot shows the 'FRU Information' page of the Integrated BMC Web Console. The left sidebar lists navigation options: System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. The main content area is titled 'FRU Information' and has a dropdown menu set to 'Baseboard'. It is divided into three sections: 'Chassis Information', 'Board Information', and 'Product Information'. The 'Chassis Information' section contains fields for Chassis Type (Rack Mount Chassis), Part Number, and Serial Number. The 'Board Information' section contains fields for Language (English), Manufacturing Date/Time (2019/06/02 17:42:00), Manufacturer (Intel Corporation), Product Name (S2600BPB), Serial Number (QSPB92204613), Part Number (H87926-562), and File ID (FRU Ver 1.39). The 'Product Information' section contains fields for Language (English), Manufacturer (Intel Corporation), Product Name (S2600BPB), Part Number, Version, Serial Number, Asset Tag, and File ID (N/A).

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

Board Information	
Language:	English
Board Manufacturing Date/Time:	2019/06/02 17:42:00
Board Manufacturer:	Intel Corporation
Board Product Name:	S2600BPB
Board Serial Number:	QSPB92204613
Board Part/Model Number:	H87926-562
FRU File ID:	FRU Ver 1.39

Product Information	
Language:	English
Manufacturer Name:	Intel Corporation
Product Name:	S2600BPB
Product Part Number:
Product Version:
Product Serial Number:
Asset Tag:
FRU File ID:	N/A

Figure 38. 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 39](#) for details.

The screenshot shows the Integrated BMC Web Console interface. At the top, there is a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. Below the navigation bar, the main content area has a title "CPU Information". On the left, there is a sidebar with links for System Information, FRU Information, CPU Information (which is currently selected), DIMM Information, NVMe Information, NIC Information, Storage Information, and Current Users. The main content area contains two separate sections, each titled "CPU Information", detailing the specifications for two different processors:

CPU Information (Processor 1):

- Socket Designation : CPU 1
- Manufacturer : Intel(R) Corporation
- Version : Intel(R) Xeon(R) Gold 6142 CPU @ 2.60GHz
- Processor Signature : 50-65-4
- Processor Type : Central Processor
- Family : Intel Xeon processor
- Speed : 2.6GHz
- Number of Cores : 16
- Voltage : 1.6V
- Socket Type : LGA3647
- Status : Populated, CPU Enabled
- Serial Number : NULL
- Asset Tag : UNKNOWN
- Part Number : NULL

CPU Information (Processor 2):

- Socket Designation : CPU 2
- Manufacturer : Intel(R) Corporation
- Version : Intel(R) Xeon(R) Gold 6142 CPU @ 2.60GHz
- Processor Signature : 50-65-4
- Processor Type : Central Processor
- Family : Intel Xeon processor
- Speed : 2.6GHz
- Number of Cores : 16
- Voltage : 1.6V
- Socket Type : LGA3647
- Status : Populated, CPU Enabled
- Serial Number : NULL
- Asset Tag : UNKNOWN
- Part Number : NULL

Figure 39. System CPU Information Page

7.1.4 DIMM Information

The DIMM Information page displays information on DIMMs installed in the host system. The DIMM information includes slot number, size, memory type, manufacturer, asset tag, memory serial/part number. See [Figure 40](#) for details.

The screenshot shows the Integrated BMC Web Console interface. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. The main content area is titled "DIMM Information". On the left, there is a sidebar with links for System Information, FRU Information, CPU Information, DIMM Information (which is currently selected), NVMe Information, NIC Information, Storage Information, and Current Users. The main content table has a header row with columns: Slot Number, Size, Type, Speed, Manufacturer, Asset Tag, Serial Number, and Part Number. Below the header, there are 11 rows of data corresponding to the DIMMs installed in the system. The last column of the table header indicates "Number of system DIMM:11".

Slot Number	Size	Type	Speed	Manufacturer	Asset Tag	Serial Number	Part Number
CPU1_DIMM_A1	4096MB	DDR4	2400MH	Netlist	001812	45B50007	NLX517T451071D24P1SE
CPU1_DIMM_B1	4096MB	DDR4	2400MH	Netlist	001821	25C70049	NLX517T451071D24P1SE
CPU1_DIMM_C1	4096MB	DDR4	2400MH	Netlist	001821	25A70042	NLX517T451071D24P1SE
CPU1_DIMM_D1	4096MB	DDR4	2400MH	Netlist	001811	25C50076	NLX517T451071D24P1SE
CPU1_DIMM_E1	4096MB	DDR4	2400MH	Netlist	001812	45E50012	NLX517T451071D24P1SE
CPU1_DIMM_F1	4096MB	DDR4	2400MH	Netlist	001745	25A70262	NLX517T451071D24P1SE
CPU2_DIMM_B1	4096MB	DDR4	2400MH	Netlist	001745	25A70191	NLX517T451071D24P1SE
CPU2_DIMM_C1	4096MB	DDR4	2400MH	Netlist	001821	25A70058	NLX517T451071D24P1SE
CPU2_DIMM_D1	4096MB	DDR4	2400MH	Netlist	001811	25A50069	NLX517T451071D24P1SE
CPU2_DIMM_E1	4096MB	DDR4	2400MH	Netlist	001821	25C70041	NLX517T451071D24P1SE
CPU2_DIMM_F1	4096MB	DDR4	2400MH	Netlist	001821	25E70033	NLX517T451071D24P1SE

Figure 40. 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 41](#) for details. Note that the BMC only displays information about NVMe drives that meet all of the support requirements.

The screenshot shows the Integrated BMC Web Console interface. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. The main content area is titled "NVMe Solid State Drive State". On the left, there is a sidebar with links for System Information, FRU Information, CPU Information, DIMM Information, NVMe Information (which is currently selected), and Current Users. The main content table is titled "NVMe Information" and contains the following data:

HSBP:	1	Drive:	5
Model:	INTEL SSDPE2MD400G4	Serial Number:	PHFT53730082400GN
PCIe 0 Link Speed:	PCIe Gen 3	PCIe 0 Link Width:	4 SERDES Lanes
PCIe 1 Link Speed:	PCIe Gen 3	PCIe 1 Link Width:	4 SERDES Lanes
NVMe Powered:	On	NVMe Functional:	Functional
NVMe Reset Required:	No Reset Required	PCIe Link Active:	PCIe Link OK
Device Class:	Mass Storage Device	Device Sub-class:	Non-volatile Memory Controller
Device Programming Intfc:	NVMe Programming Interface	Drive Life Consumed:	0 %
Firmware revision:	8DV10171	Bootloader revision:	8B1B0131

Figure 41. 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 42](#) for details.

Number of system NIC: 2									
PCI Class Code	Slot Number	Vendor ID	Device ID	Current Speed(Mbps)	Portidx	Media State	MAC Address	Firmware Version	
2	0x0000	0x8086	0x1563	8000	0	Media is not connected	a4-bf-01-23-13-74	N/A	
2	0x0000	0x8086	0x1563	8000	2	Media is not connected	a4-bf-01-23-13-75	N/A	

Figure 42. 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 43](#) for details.

Number of system Storage: 1												
Port Destination	Device Index	Connector Type	Protocol	Device Type	Capacity(GB)	RPM	Model	Serial	PCI Class Code	Vendor ID	Device ID	Firmware Version
USB Port 1	0x1	USB	USB	USB	14	0	DataTraveler 3.0	40BD5C162FCC2E251B908E752	0x0	0x0000	0x0000	N/A

Figure 43. 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 EWS 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 44](#) for details.

The screenshot shows the 'Current Users' page of the Integrated BMC Web Console. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists System Information, FRU Information, CPU Information, DIMM Information, and NVMe Information. The main content area is titled 'Current Users' and displays a table with one row:

User Name	Type	KVM Number	vMedia Usable	IP Address
root (me)	Web(HTTPS)	0	No	10.239.163.21

Figure 44. System Current Users Page

Notice: Intel added to the BMC a new KCS Policy Control Mode; when set to "Deny ALL" on the BMC EWS, both the BMC and FRU SDR cannot be upgraded/downgraded as expected behavior. Updates can still be performed via Redfish or BMC EWS. 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 45](#) and [Figure 46](#) (with threshold). [Table 8](#) lists the options available in this page. By default, this page displays all sensors owned by the BMC and auto-refreshes every 60 seconds.

The screenshot shows the 'Sensor Readings' page of the Integrated BMC Web Console. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists Sensor Readings and Event Log. The main content area is titled 'Sensor Readings' and includes filters for 'Select a sensor owner:' (BMC), 'Select a sensor type category:' (All Sensors), and 'Auto Refresh(sec):' (60). A table titled 'Sensor Readings: 77 sensors' lists the following data:

Healthy	Name	Status	Reading
OK	BB Inlet Temp	Normal	30 degree C
OK	BB BMC Temp	Normal	40 degree C
OK	BB CPU1 VR Temp	Normal	51 degree C
OK	BB CPU2 VR Temp	Normal	43 degree C
OK	BB MISC VR Temp	Normal	52 degree C
OK	BB Outlet Temp	Normal	48 degree C
OK	System Airflow	Normal	16 C.F.M
OK	SSB Temp	Normal	51 degree C
OK	HSBP PSOC	Normal	32 degree C
OK	Exit Air Temp	Normal	46 degree C
OK	LAN NIC Temp	Normal	53 degree C
OK	Sys Fan 1A	Normal	9180 R.P.M
OK	Sys Fan 1B	Normal	9579 R.P.M
OK	Sys Fan 2A	Normal	9090 R.P.M
OK	Sys Fan 2B	Normal	9486 R.P.M
OK	Sys Fan 3A	Normal	8910 R.P.M

At the bottom, there are 'Refresh' and 'Show Thresholds' buttons.

Figure 45. Server Health Sensor Readings Page (Thresholds Not Displayed)

The screenshot shows the 'Sensor Readings' page of the Integrated BMC Web Console. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. Below the navigation bar, the main content area has a title 'Sensor Readings' with a back arrow icon.

On the left, there's a sidebar with a 'Sensor Readings' link and an 'Event Log' link. The main content area contains three dropdown menus: 'Select a sensor owner' (set to 'BMC'), 'Select a sensor type category' (set to 'All Sensors'), and 'Auto Refresh(sec)' (set to '60'). To the right of these, it says 'Sensor Readings: 77 sensors'.

The central part of the page is a table with 14 columns. The columns are: Healthy, Name, Status, Reading, Low NR, Low CT, Low NC, High NC, High CT, High NR. The table lists 14 sensor entries, each with a green 'OK' status indicator. The first few rows show temperature sensors like BB Inlet Temp, BB BMC Temp, BB CPU1 VR Temp, etc., followed by other sensors like BB Outlet Temp, System Airflow, SSB Temp, HSBP PSOC, Exit Air Temp, LAN NIC Temp, Sys Fan 1A, and Sys Fan 1B.

At the bottom of the table, there are two buttons: 'Refresh' (gray) and 'Hide Thresholds' (blue).

Figure 46. Server Health Sensor Readings Page (Thresholds Displayed)

Table 8. 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 47). Table 9 lists the options available in this page.

Event Log

Select an event log category: All Events

Severity category: Informational Warning Critical

This page has 50 event entries

Event ID	Timestamp	Sensor Name	Controller	Severity	Sensor Type	Description
22255	Fri Sep 28 03:04:54 2018	BB +3.3V Vbat	BMC	Warning	Voltage	Lower Non-critical - going low - Asserted
22254	Fri Sep 28 03:04:51 2018	BB +3.3V Vbat	BMC	Informational	Voltage	Lower Non-critical - going low - Deasserted
22253	Fri Sep 28 03:04:43 2018	BB +3.3V Vbat	BMC	Warning	Voltage	Lower Non-critical - going low - Asserted
22252	Fri Sep 28 03:04:39 2018	BB +3.3V Vbat	BMC	Informational	Voltage	Lower Non-critical - going low - Deasserted
22251	Fri Sep 28 03:03:58 2018	BB +3.3V Vbat	BMC	Warning	Voltage	Lower Non-critical - going low - Asserted
22250	Fri Sep 28 03:03:52 2018	BB +3.3V Vbat	BMC	Informational	Voltage	Lower Non-critical - going low - Deasserted
22249	Fri Sep 28 03:02:45 2018	BB +3.3V Vbat	BMC	Warning	Voltage	Lower Non-critical - going low - Asserted
22248	Fri Sep 28 02:56:21 2018	HDD 2 Status	BMC	Informational	Bay	Drive Presence - Asserted
22247	Fri Sep 28 02:56:07 2018	Pwr Unit Redund	BMC	Informational	Power Unit	Redundancy Regained - Asserted
22246	Fri Sep 28 02:55:33 2018	PS2 Status	BMC	Informational	Power Supply	Presence detected - Asserted
22245	Fri Sep 28 02:55:33 2018	PS1 Status	BMC	Informational	Power Supply	Presence detected - Asserted

Total Event Log: 2200 event entries
Event Log is 55% full.

Number of entries per page: 50 << < 1 / 44 > >>

Clear Event Log Save Event Log Refresh Event Log

Figure 47. Server Health Event Log Page

Table 9. 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 48). Table 10 lists the options to select the events that should trigger alerts and where the alerts are to be sent.

The screenshot shows the 'Alerts' section of the Integrated BMC Web Console. On the left, a sidebar lists various configuration categories. The main area displays the 'List of Alerts' with two checked checkboxes: 'Globally Enable Platform Event Filtering' and 'Log Event For Filter Action'. Below this is a large list of system events with checkboxes, where 'Inlet Temperature Overheat Shutdown' is also checked. At the bottom of this section are 'Check All' and 'Clear All' buttons. The next sections, 'Alert Destination #1' and 'Alert Destination #2', show configuration for SNMP and Email destinations, both with their respective IP/Email fields and radio button selection. At the very bottom are 'Save' and 'Send Test Alert' buttons.

Figure 48. Alerts Page

Table 10. Alerts Options

Option	Task
Globally Enable Platform Event Filtering	This can be used to prevent sending alerts until the user has fully specified his/her 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 11](#) lists the options to configure alert emails.

The screenshot shows the 'Alert Email Settings' page within the Integrated BMC Web Console. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a vertical sidebar lists various configuration categories: Alerts, Alert Email, Date & Time, IPv4 Network, IPv6 Network, VLAN, LDAP, Active Directory, KVM & Media, SSL Certification, Users, Security Settings, SOL, SDR Configuration, BMC Firmware Update, BIOS/ME Firmware Update, Syslog Server Configuration, and a 'Logout' link. The main content area is titled 'Alert Email Settings' and contains fields for 'SMTP Server IP' (with an input field), 'SMTP Server Port' (with an input field), 'Sender Email Address' (with an input field), 'SMTP Authentication Method' (a dropdown menu set to 'None'), 'SMTP Authentication User' (with an input field), and 'SMTP Authentication Password' (with an input field). A 'Save' button is located at the bottom of the form.

Figure 49. Alert Email Page

Table 11. 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 12 lists the options to configure Date & Time.

The screenshot shows the 'Date & Time' configuration page of the Integrated BMC Web Console. The main display shows the current time as 4:58:48 and the date as 2020 / 1 / 1, Wednesday. Below the time, there is a dropdown menu for the Time Zone, currently set to GMT+00:00 | Casablanca/London. There is also a checkbox labeled 'BMC time use NTP' which is unchecked. A section titled 'NTP Server' contains two input fields: 'Primary NTP Server' and 'Secondary NTP Server'. On the left side, there is a vertical sidebar with a list of navigation links including System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. The 'Configuration' link is currently selected. At the bottom of the page is a 'Save' button.

Figure 50. Date & Time Page

Table 12. Date & Time Options

Option	Task
Time Zone	Time zone setting.
BMC time use NTP	Enable/Disable NTP service.
Primary NTP Server	Primary NTB Server address.
Second NTP Server	Second NTB 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 51](#) or [Figure 52](#) for details. Table 13 lists the options available in this page.

The screenshot shows the 'IPv4 Network Settings' page of the Intel Integrated BMC Web Console. The left sidebar lists various management categories like System, Server Health, Configuration, Remote Control, etc. The main panel shows the following configuration details:

- HOST Interface:** Enabled (checkbox checked).
- LAN Failover:** Disabled (checkbox unchecked).
- Configuration management:**
 - Hostname:** BMC0A4BF012728F4
 - LAN Channel:** Channel-1
 - MAC Address:** a4-bf-01-27-28-14
 - NIC Description:** Shared Between Host and BMC
 - Link Status:** UP
 - DHCP Options:** Obtain an IP address automatically (use DHCP) (radio button selected).
 - IP Address:** 10.239.10.12
 - Subnet Mask:** 255.255.255.0
 - Default Gateway:** 10.239.10.241
 - Primary DNS Server:** 10.248.2.5
 - Secondary DNS Server:** 10.248.2.5

A 'Save' button is located at the bottom left of the form.

Figure 51. IPV4 Network DHCP Page

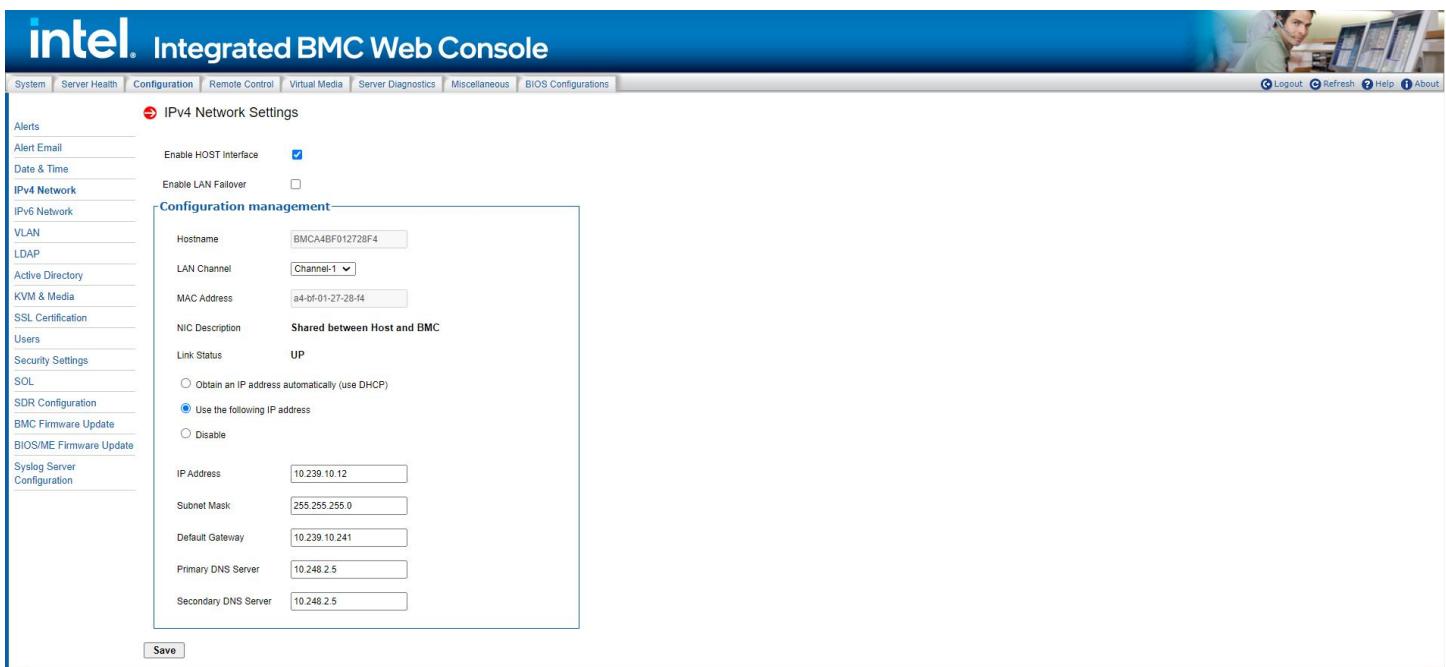


Figure 52. IPv4 Network Static Page

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 13. 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 HOST Interface	Host Interface (HI) is based on Ethernet over USB. It provides an interface between the HOST and the BMC for communication. This allows applications to use the network socket to communicate with each other. If HI is not enabled yet, the user must enable it and save this configuration change. Then, continue to set the host interface configuration. HI only supports Static IP and can only modify IP address and netmask.
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. <ul style="list-style-type: none"> • Intel® RMM (BMC LAN Channel 3) is the add-in RMM4 Dedicated Management NIC. • 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. • HOST Interface (BMC LAN Channel 4) is an internal channel between the HOST and the BMC.

Option	Task
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 53) Table 14 lists the options available in this page.

integrated BMC Web Console

System | Server Health | Configuration | Remote Control | Virtual Media | Server Diagnostics | Miscellaneous | BIOS Configurations | Logout | Refresh | Help | About

IPv6 Network Settings

Alerts

Enable HOST Interface

Enable LAN Failover

Configuration management

LAN Channel: Channel-1

MAC Address: a4-bf-01-27-28-ff

NIC Description: Shared between Host and BMC

Link Status: UP

Obtain an IP address automatically (use DHCPv6/SLAAC)

Use the following IP address

Disable

IP Address: ::ffff:10.248.2.5

Prefix Length: 64

Default Gateway: ::ffff:10.248.2.5

Primary DNS Server: ::ffff:10.248.2.5

Secondary DNS Server: ::ffff:10.248.2.5

Save

Figure 53. 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 14. 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.
Enable HOST Interface	<p>HI is based on Ethernet over USB. It provides an interface between the HOST and the BMC for communication. This allows applications to use the network socket to communicate with each other.</p> <p>If HI is not enabled yet, the user must enable it and save this configuration change. Then continue to set the host interface configuration.</p> <p>HI only supports Static IP and can only modify IP address and prefix length.</p>
LAN Channel	<p>Select the channel on which to configure the network settings.</p> <p>Lists the LAN Channels available for server management. The LAN channels describe the physical NIC connection on the server.</p> <ul style="list-style-type: none"> • Intel® RMM (BMC LAN Channel 3) is the add-in RMM4 Dedicated Management NIC. • 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. • HOST Interface (BMC LAN Channel 4) is an internal channel between the HOST and the BMC.
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:</p> <p>Use IPv6 auto-configuration (stateless ICMPv6 discovery) – Uses ICMPv6 to obtain the IP address.</p> <p>Obtain an IP address automatically (use DHCPv6) – Uses DHCPv6 to obtain the IP address.</p> <p>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.</p> <p>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".</p> <p>'xxxx' ranges from 0 to FFFF.</p> <p>First 'xxxx' must not be 0.</p> <p>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 54). Table 15 lists the options available in this page.

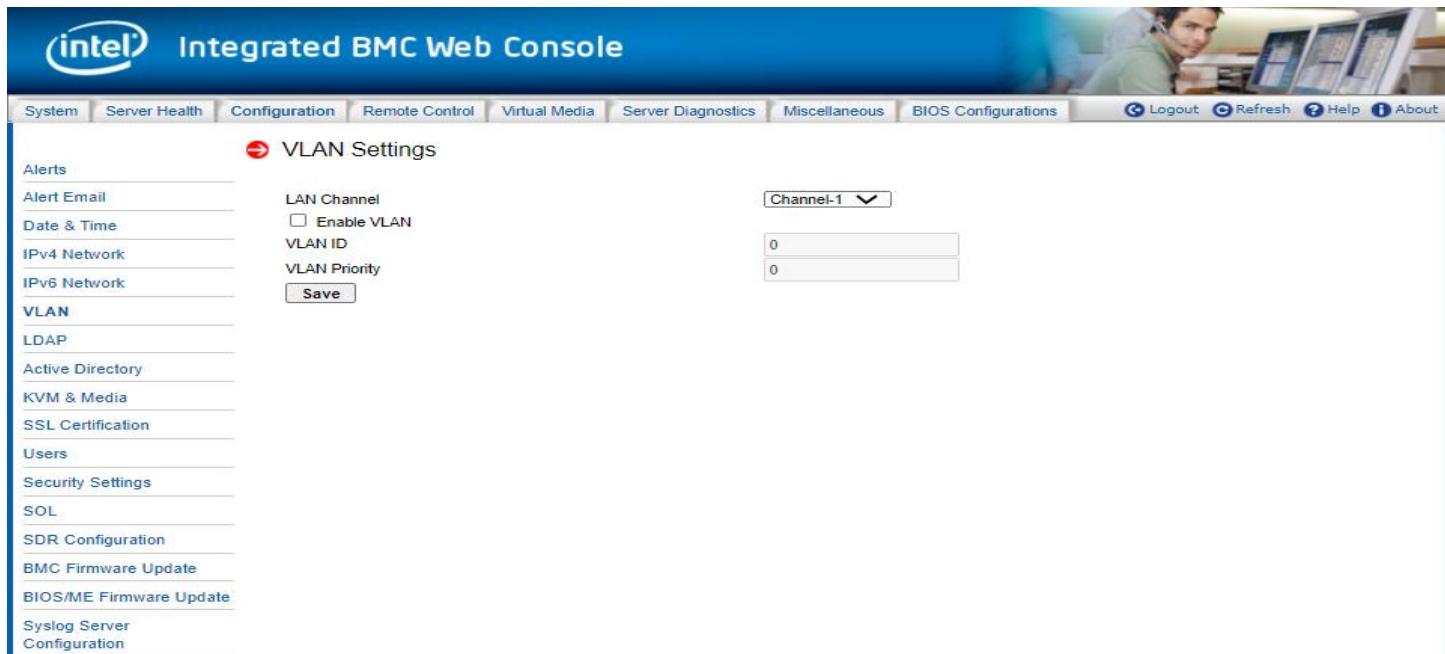


Figure 54. VLAN Settings Page

Table 15. VLAN Settings Options

Option	Task
LAN Channel	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. <ul style="list-style-type: none"> • Intel® RMM (BMC LAN Channel 3) is the add-in RMM4 NIC. • 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 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 55](#) and [Table 16](#) for available options on this page.

The screenshot shows the 'LDAP Settings' page of the Integrated BMC Web Console. On the left is a sidebar with links to various system configurations like System, Server Health, Configuration, and BIOS Configurations. The main area has a title 'LDAP Settings' with a red 'edit' icon. It contains several input fields and dropdown menus for configuring LDAP settings. At the bottom right is a 'Save' button.

Figure 55. LDAP Settings Page

Table 16. LDAP Settings Options

Option	Task
LDAP Authentication	Check this box to enable LDAP authentication, then enter the required information to access the LDAP server.
LDAP authentication over SSL	Check this box to enable LDAP authentication over SSL.
Port	Specify the LDAP Port.
IP Address	The IP address of LDAP server. • IP Address made of 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, like "cn=Manager, dc=my-domain, dc=com".
Searchbase	The searchbase of the LDAP server, like "dc=my-domain, dc=com".
LDAP Group Configuration	Configure the LDAP search filters associated with BMC network privileges. like "(&(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 56](#) and [Table 17](#) for available options on this page.

Active Directory Settings

Enable Active Directory Authentication

Active Directory Authentication over SSL

Port	389
User Domain Name	
Time Out	0
Domain Controller Server Address1	0.0.0.0
Domain Controller Server Address2	0.0.0.0
Domain Controller Server Address3	0.0.0.0

Role Groups

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

Add Role Group Modify Role Group Delete Role Group

Figure 56. Active Directory Settings Page

Table 17. Active Directory Settings Options

Option	Task
Enable Active Directory Authentication	Click checkbox to enable.
Active Directory Authentication over SSL	Click checkbox 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 enable/disable encryption on KVM or media during a redirection session (Figure 57). Table 18 lists the options for enabling or disabling encryption on KVM or media data and configuring the mouse mode setting during a redirection session.

The screenshot shows the 'KVM Remote Session & Mouse Mode Setting' page. On the left, a sidebar lists various configuration categories. The main area has two sections: 'Remote Session' and 'Mouse Mode Setting'. In 'Remote Session', there's a dropdown for 'KVM Encryption' set to 'AES-256'. Below it, 'Default Ports' are listed as 'KVM (Secure)' port 5902 and 'USB/Floppy (Secure)' port 627, with a 'Save' button. In 'Mouse Mode Setting', it says 'Current Mouse Mode is ABSOLUTE.' with three radio button options: 'Absolute Mode(Windows, Ubuntu, RHEL 6.x, SLES 12 and later)' (selected), 'Relative Mode(Rest of the Linux)', and 'Single Mode'. A 'Save' button is also present here.

Figure 57. KVM & Media Page

Table 18. 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 knowing for certain that the new ports are unused.
Save (Remote Session)	Click to save any changes for Remote Session.
Mouse Mode Setting	Redirection Console handles mouse emulation from local window to remote screen in one of the following methods: <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 58 for details.

The screenshot shows the 'SSL Upload' page of the Integrated BMC Web Console. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists various configuration categories: Alerts, Alert Email, Date & Time, IPv4 Network, IPv6 Network, VLAN, LDAP, Active Directory, KVM & Media, SSL Certification (which is currently selected), Users, Security Settings, SOL, SDR Configuration, BMC Firmware Update, BIOS/ME Firmware Update, Syslog Server, and Configuration. The main content area is titled 'SSL Upload' and contains fields for 'Certification Valid From' (1/1/2015, 8:00:18 AM) and 'Certification Valid Until' (12/31/2024, 8:00:18 AM). It also features two file upload fields: 'New SSL Certificate' (labeled 'Choose File | No file chosen') and 'New Private Key' (labeled 'Choose File | No file chosen'). A large blue 'Upload' button is positioned below these fields. In the top right corner of the main content area, there is a small thumbnail image of a person working at a computer.

Figure 58. 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 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 59](#) for details.

User ID	User Name	User Status	Network Privilege
1	anonymous	Disable	No Access
2	root	Enable	Administrator
3	~	~	~
4	~	~	~
5	~	~	~
6	~	~	~
7	~	~	~
8	~	~	~
9	~	~	~
10	~	~	~
11	~	~	~
12	~	~	~
13	~	~	~
14	~	~	~
15	~	~	~

[Figure 59. User List Page](#)

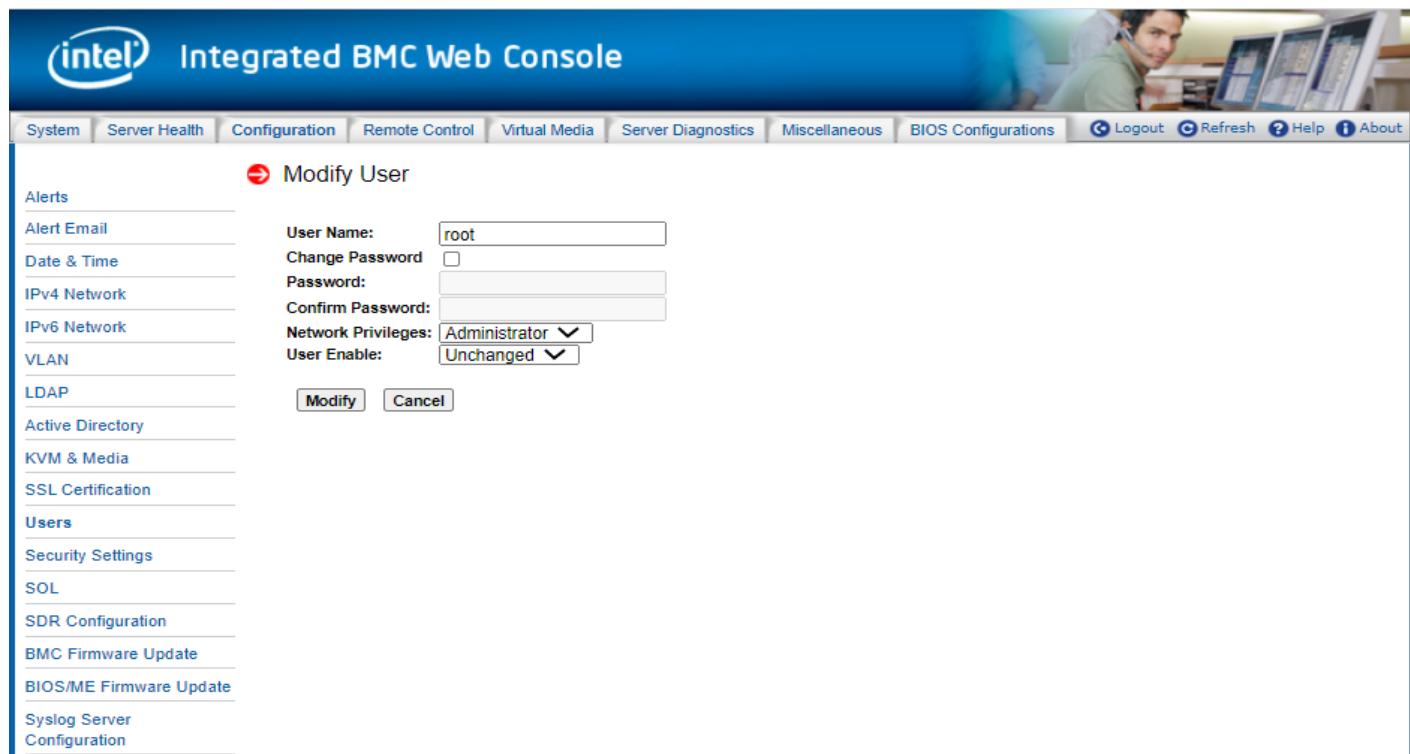
This page allows the operator to configure the IPMI users and privileges for this server. UserID 1 (anonymous) may not be renamed or deleted. To add a user, select an empty slot in the list and click the **Add User** button. Set the User Name, Password, and Network Privileges as shown in [Figure 60](#).

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

User Name:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Network Privileges:	Administrator

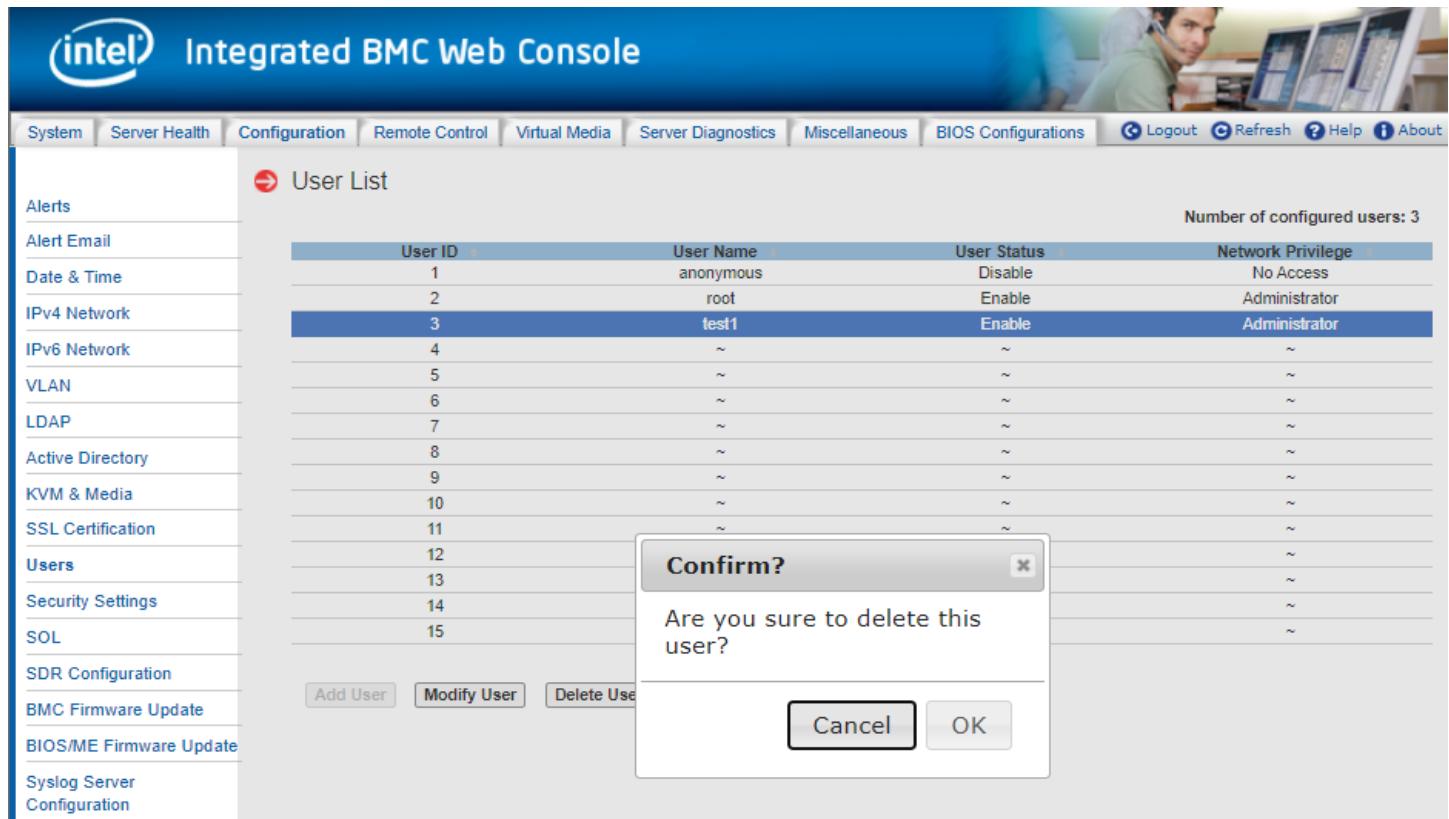
[Figure 60. Add New User Page](#)

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 61](#).



[Figure 61. Modify User Page](#)

To delete a user, select the user in the list and click the **Delete User** button ([Figure 62](#)).



[Figure 62. Delete User Page](#)

7.3.12 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 63](#) for details. [Table 19](#) lists the options to modify the security settings.

Figure 63. Configuration Security Settings Page

Table 19. Configuration Security Settings Options

Option	Task
KCS Mode	<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. Deny All – This configuration setting disables the IPMI KCS command interfaces between the Host OS and the BMC. This is a configuration that does not comply with IPMI and will impact the operation of the Server Management Software running on the Host OS. This mode only applies to the IPMI commands over the KCS interfaces and does not apply to the authenticated network interfaces to the BMC. 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 configuration that does not comply with IPMI and may impact the operation of the Server Management Software running on the Host OS. This mode 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, like to most newer browser versions. Board Compatibility - check the compatibility to other protocols before using it, like IMAPS. Widest Compatibility - compatibility to most legacy browsers, legacy libraries (still patched), and other application protocols besides HTTPS, like IMAPS. Legacy - widest compatibility to 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 0–255. Default is 3 attempts.
User Lockout Time(Sec)	Set the time in seconds that the user is locked out before being allowed to log in again. Zero means User Lockout Time is disabled. If a user was automatically disabled due to the Bad Password threshold, the user will remain disabled until re-enabled via the Set User Access command. User Lockout Time should be 0–65535. Default is 60sec.
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.

7.3.12.1 EWS access under KCS Restricted/Deny All Mode

Most of EWS content access is allowed across all KCS modes, except for below EWS 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 gray out when KCS = Deny All
- Server Power Control Page: Reset Server/**Force-enter BIOS Setup** option will be gray out when KCS = Deny All

KVM/Console Redirection

Server Power Control

Host is currently ON

Reset Server

Force-enter BIOS Setup

Power Off Server - Immediate

Graceful Shutdown

Power On Server

Force-enter BIOS Setup

Power Cycle Server

Perform Action

Figure 64. Server Power Control Page

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

System Server Health Configuration Remote Control Virtual Media Server Diagnostics Miscellaneous BIOS Configurations

BIOS/ME Firmware Update

Use this page to upload new BIOS/ME firmware

BIOS/ME Firmware Update

BIOS Rev : SE5C620.86B.02.01.0011.032620200659

Mgmt Engine (ME) FW Rev : 04.01.04.381

Firmware image type : BIOS image

BIOS Region : Backup

Drop a file on this page or select Browse...

Choose File No file chosen

Upload

Alerts

Alert Email

IPv4 Network

IPv6 Network

VLAN

LDAP

KVM & Media

SSL Certification

Users

Security Settings

SOL

SDR Configuration

BMC Firmware Update

BIOS/ME Firmware Update

Syslog Server Configuration

grey out when KCS=Deny All

Figure 65. BIOS/ME Firmware Update Page

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

The screenshot shows the BIOS Configurations page with a sidebar containing links like PCI Configuration, Serial Port Configuration, UPI Configuration, etc. The main area shows a table with columns: Key, Value, BIOS Variable Description, Value, and SavedValue. A modal window titled 'Caution!' displays the message: 'Note: BIOS configuration information isn't available, because KCS mode is restricted or deny-all, please change KCS mode to allow all.'

Figure 66. BIOS Configuration Page

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

The screenshot shows the CPU Information page with a sidebar containing links like System Information, FRU Information, CPU Information, DIMM Information, NVMe Information, and Current Users. The main area displays two sections for CPU 1 and CPU 2, each listing processor details such as designation, manufacturer, version, processor signature, type, family, speed, number of cores, voltage, socket type, status, serial number, asset tag, and part number.

CPU 1	
Socket Designation :	CPU 1
Manufacturer :	Intel(R) Corporation
Version :	Intel(R) Xeon(R) Platinum 8260L CPU @ 2.40GHz
Processor Signature :	50-65-6
Processor Type :	Central Processor
Family :	Intel Xeon processor
Speed :	2.4GHz
Number of Cores :	24
Voltage :	1.6V
Socket Type :	LGA3647
Status :	Populated, CPU Enabled
Serial Number :	NULL
Asset Tag :	UNKNOWN
Part Number :	NULL

CPU 2	
Socket Designation :	CPU 2
Manufacturer :	Intel(R) Corporation
Version :	Intel(R) Xeon(R) Platinum 8260L CPU @ 2.40GHz
Processor Signature :	50-65-6
Processor Type :	Central Processor
Family :	Intel Xeon processor
Speed :	2.4GHz
Number of Cores :	24
Voltage :	1.6V
Socket Type :	LGA3647
Status :	Populated, CPU Enabled
Serial Number :	NULL
Asset Tag :	UNKNOWN
Part Number :	NULL

Figure 67. CPU Information Page

DIMM Information									
System Information									
CPU Information									
CPU1_DIMM_A1	16384MB	DDR4	2666MHz	Micron	DIMM_A1_AssetTag	1740C043	18ASF2G72PDZ-2G6D1		
CPU1_DIMM_B1	16384MB	DDR4	2666MHz	Micron	DIMM_B1_AssetTag	1740BFD0	18ASF2G72PDZ-2G6D1		
CPU1_DIMM_C1	16384MB	DDR4	2666MHz	Micron	DIMM_C1_AssetTag	1740B617	18ASF2G72PDZ-2G6D1		
CPU1_DIMM_D1	16384MB	DDR4	2666MHz	Micron	DIMM_D1_AssetTag	1740C072	18ASF2G72PDZ-2G6D1		
CPU1_DIMM_E1	16384MB	DDR4	2666MHz	Micron	DIMM_E1_AssetTag	1740C087	18ASF2G72PDZ-2G6D1		
CPU1_DIMM_F1	16384MB	DDR4	2666MHz	Micron	DIMM_F1_AssetTag	1740C095	18ASF2G72PDZ-2G6D1		
CPU2_DIMM_A1	16384MB	DDR4	2666MHz	Micron	DIMM_A1_AssetTag	1740B5E0	18ASF2G72PDZ-2G6D1		
CPU2_DIMM_B1	16384MB	DDR4	2666MHz	Micron	DIMM_B1_AssetTag	1740B614	18ASF2G72PDZ-2G6D1		
CPU2_DIMM_C1	16384MB	DDR4	2666MHz	Micron	DIMM_C1_AssetTag	1740B60B	18ASF2G72PDZ-2G6D1		
CPU2_DIMM_D1	16384MB	DDR4	2666MHz	Micron	DIMM_D1_AssetTag	1740B605	18ASF2G72PDZ-2G6D1		
CPU2_DIMM_E1	16384MB	DDR4	2666MHz	Micron	DIMM_E1_AssetTag	1740C4A7	18ASF2G72PDZ-2G6D1		
CPU2_DIMM_F1	16384MB	DDR4	2666MHz	Micron	DIMM_F1_AssetTag	1740BF1B	18ASF2G72PDZ-2G6D1		

Figure 68. DIMM Information Page

7.3.13 SOL

Use this page to enable or disable SOL for each LAN channel (Figure 69). Table 20 lists the options to modify SOL settings.

Figure 69. SOL Page

Table 20. SOL Options

Option	Task
LAN Channel	Select the channel on which the user wants 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"> Intel® RMM (BMC LAN Channel 3) is the add-in RMM4 NIC. 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.

7.3.14 SDR Configuration

Use this page to upload and parse sensor data repository records and configuration files, which allows updating the FRUSDR package (Figure 70). Table 21 lists the options available on this page.

The screenshot shows the 'SDR Configuration' page of the Integrated BMC Web Console. On the left, a sidebar lists various management options like System, Server Health, Configuration, Remote Control, etc. The main content area has a title 'SDR Configuration' with a sub-instruction: 'Use this page to upload and parse sensor data repository records and configuration files.' Below this is a form with fields for 'Current SDR File' (1.45 (588696 bytes)), 'Current Config File' (Revision S2600BP_145 (29723 bytes)), 'Last Upload' (Thu Jan 1 00:14:30 2015), 'New Config File' (Choose File), 'New SDR File' (Choose File), and 'Upload' and 'Parse' buttons. To the right is a section titled 'Processed Tags' displaying hardware detection results. At the bottom right is a 'Save' button and radio buttons for 'Enable SDR Auto-configuration'.

Figure 70. 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 the user's 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 failed, this area would 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.

7.3.15 BMC Firmware Update

Use this page to upload new images for online-update of BMC firmware (Figure 71). Table 22 lists the options available in this page.

The screenshot shows the Integrated BMC Web Console interface. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists various configuration categories: Alerts, Alert Email, Date & Time, IPv4 Network, IPv6 Network, VLAN, LDAP, Active Directory, KVM & Media, SSL Certification, Users, Security Settings, SOL, SDR Configuration, BMC Firmware Update (which is currently selected), BIOS/ME Firmware Update, and Syslog Server Configuration. The main content area is titled 'BMC Firmware Update' and contains the following information: 'BMC FW Rev : 2.48.9b71d562', 'BMC Firmware Build Time : Tue Nov 24 03:19:44 2020', and a file upload section with 'Choose File' and 'Upload' buttons. A note at the top says 'Use this page to upload new BMC firmware'.

Figure 71. 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
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.

7.3.16 BIOS/ME Firmware Update

Use the BIOS/ME Firmware update page shown in [Figure 72](#) 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 72. Configuration BIOS/ME Firmware Update Page](#)

[Table 23. Configuration 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.
Firmware image type	Select the image type for BIOS/ME firmware update. <ul style="list-style-type: none"> • BIOS image: OOB update BIOS. • ME image: OOB update ME firmware. • FD image: OOB update flash descriptor.
BIOS Region	When user chooses the image type "BIOS", the Backup region option will appear. When the option is enabled, the Backup region of current BIOS 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	Upload the firmware image file.

7.3.17 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 24](#) 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/UDPServeRun 514/ModLoad imtcp/InputTCPServerRun 514
3. Service syslog restart
4. Set syslog server from EWS--> Configuration--> Syslog Server Configuration
5. Cat /var/log/messages to see log

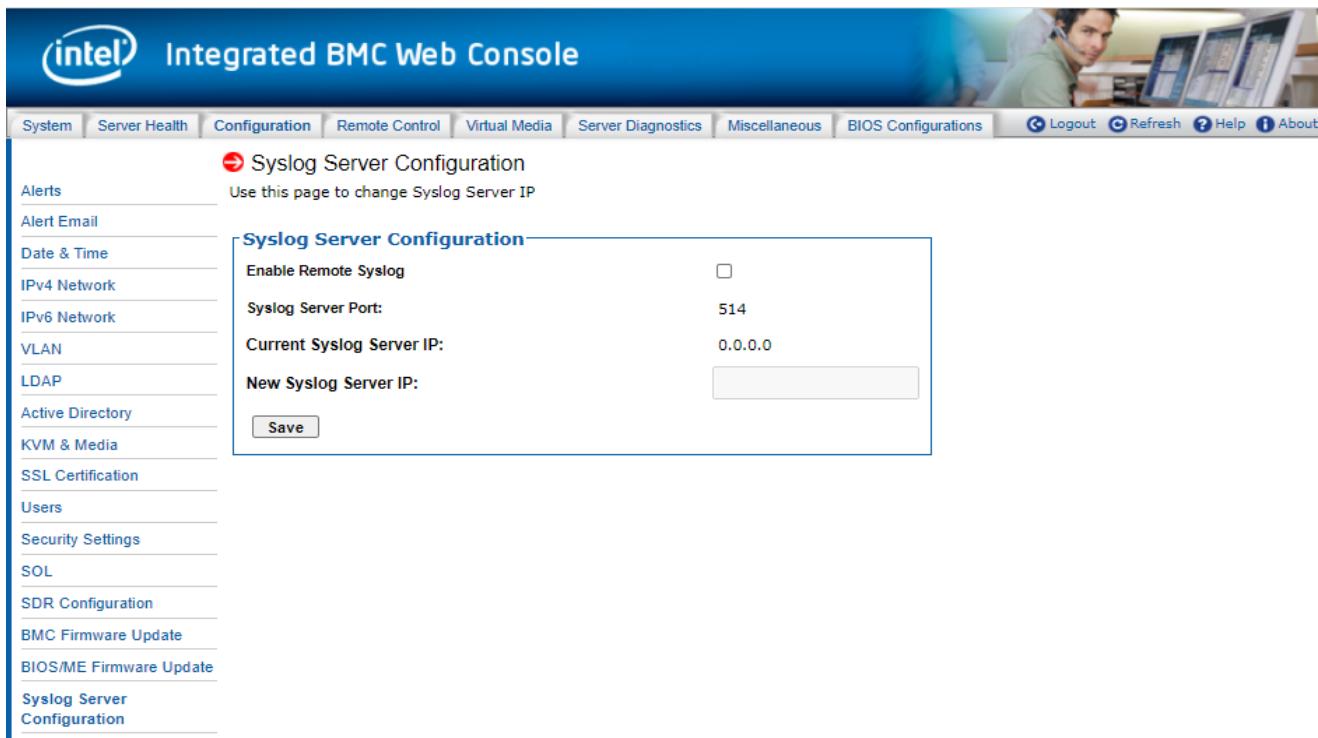


Figure 73. Syslog Server Configuration Page

Table 24. 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 **Launch Console** prompts to download a `launch.jnlp` file. When the file is downloaded and launched, the Java redirection window is displayed. [Figure 74](#) 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.

The screenshot shows the 'KVM/Console Redirection' page of the Integrated BMC Web Console. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists KVM/Console Redirection, Server Power Control, Launch SOL, Virtual Front Panel, and iKVM over HTML5. The main content area has a heading 'KVM/Console Redirection' with a red circular icon. Below it is a 'Launch Console' button. A 'Keyboard Macros' section follows, containing a table with 10 rows. Each row has two columns: 'Key Sequence' and 'Button Name', both represented by input fields. The rows are numbered #1 through #10. At the bottom of this section is a 'Save' button.

[Figure 74. 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 25. 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 75. Table 26 lists the power control operations that can be performed.

The screenshot shows the 'Power Control and Status' section of the BMC Web Console. It indicates that the host is currently ON. There are several options for power control:

- Reset Server**: Selected.
- Force-enter BIOS Setup
- Power Off Server - Immediate
- Graceful Shutdown
- Power On Server
 - Force-enter BIOS Setup
- Power Cycle Server

A 'Perform Action' button is located at the bottom of the form.

Figure 75. Remote Control Server Power Control Page

Table 26. 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. It is suggested 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 78](#) or [Figure 77](#) details.



Figure 76. Remote Control Launch SOL Page

Starting the SOL console opens an additional window as shown in [Figure 78](#). It displays the screen content of the remote server. The SOL console behaves as if the user were connected to a serial terminal on the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between Integrated BMC Web Console and remote console.

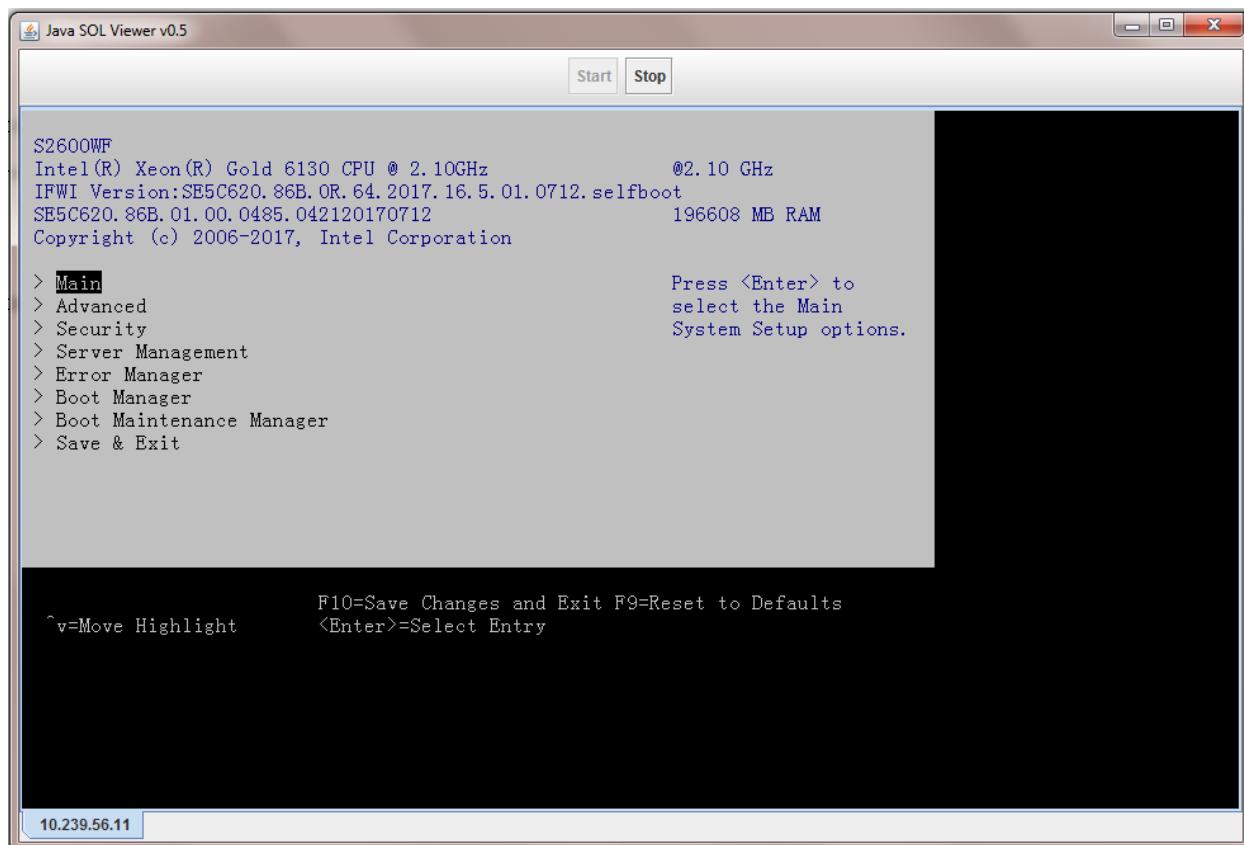


Figure 77. Remote Control Launch SOL Screen Page

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 78). Table 27 lists the power control operations that can be performed.



Figure 78. Remote Control Virtual Front Panel Page

Table 27. 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 HLTM5 redirection window from this page, accessing the two menus listed within: **Keyboard** and **Power Control**.

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

- **Virtual Keyboard:** Click the submenu **Virtual Keyboard** within the **Keyboard** menu to display a soft keyboard, shown in [Figure 81](#).
- **Keyboard Macro:** Click the submenu **Keyboard Macro** within the **Keyboard** menu to open the keyboard macro menu, shown in [Figure 82](#).

There are four sub-menus within the **Power Control** menu (shown in menu shown in [Figure 83](#)):

- **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 79](#) or [Figure 80](#) for more details.

The screenshot shows the 'iKVM over HTML5' page. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists KVM/Console Redirection, Server Power Control, Launch SOL, Virtual Front Panel, and iKVM over HTML5. The main content area has a heading 'iKVM over HTML5' with a sub-instruction: 'Press the button to launch the iKVM over HTML5 and manage the server remotely.' Below this is a large 'Launch iKVM over HTML5' button.

Figure 79. iKVM over HTML5 Page

The screenshot shows the 'HTML5 Screen' page. It features a similar navigation bar and sidebar as Figure 79. The main content area displays a window titled 'iKVM_over_HTML5 - Internet Explorer'. This window contains a 'Keyboard' tab and a 'Power Control' tab, with the 'Keyboard' tab currently selected. The window is set against a background of the BMC interface.

Figure 80. HTML5 Screen Page

The screenshot shows the 'Virtual Keyboard' page. It includes a standard QWERTY keyboard layout with function keys F1-F12 at the top. To the right is a numeric keypad and a set of special characters. A small 'Us' label is visible in the top right corner of the keyboard area. Navigation keys like Home, End, PgUp, PgDn, and arrow keys are located at the bottom right.

Figure 81. HTML5 Virtual Keyboard Page

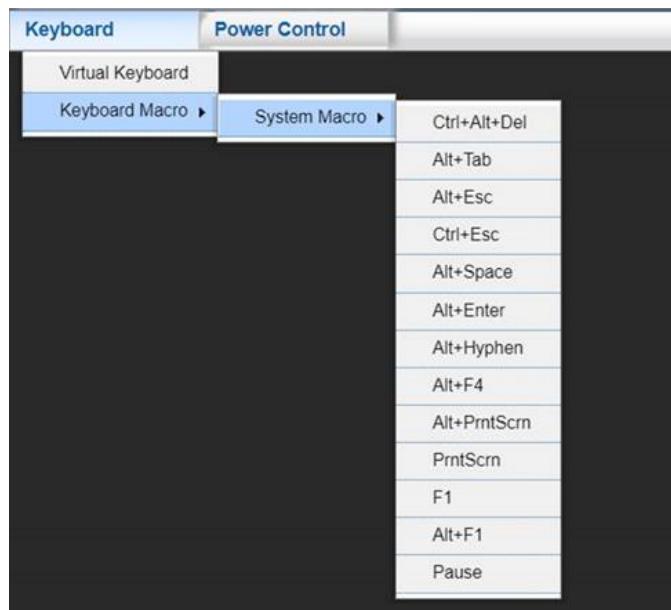


Figure 82. HTML5 Keyboard Macro Menu Page

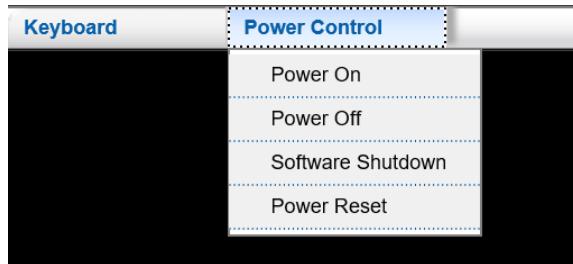


Figure 83. HTML5 Power Control Menu page

7.5 Virtual Media Tab

7.5.1 Virtual Media over HTML5

The Virtual Media tab allows the user to mount a remote drive image file (.img/ima or .iso) as a remote device to the server, and it is similar to Media Redirection.

Virtual Media over HTML5 also provides an HTML5 webpage to mount a folder as a remote device to the server. The filesystem of the remote device is UDF.

Once Virtual Media over HTML5 mounted a remote driver image file, the remote device appears just like a local device to the server, allowing system administrators to install software (including operating systems), copy files, update BIOS, and so on, or boot the server from this device. See [Figure 84](#) for more details.

To open the operation window, click **Launch Virtual Media over HTML5** as shown in [Figure 85](#). To upload files to the BMC over HTML5, select file type, click the **Select Media** button then click **Plug in** button as shown in [Figure 86](#). Up to three devices may be mounted simultaneously. [Table 28](#) lists the options available in this page.

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 84. Virtual Media over HTML5 Page

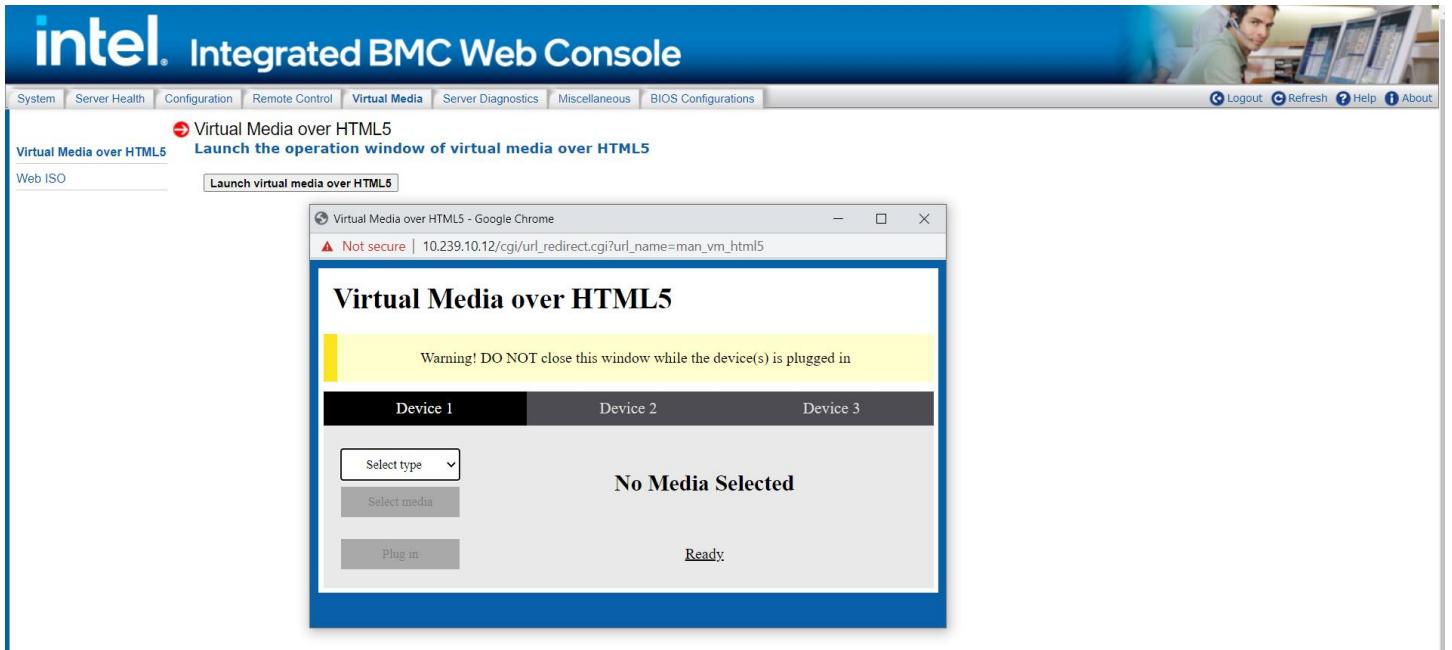


Figure 85. Launch Virtual Media over HTML5 Page

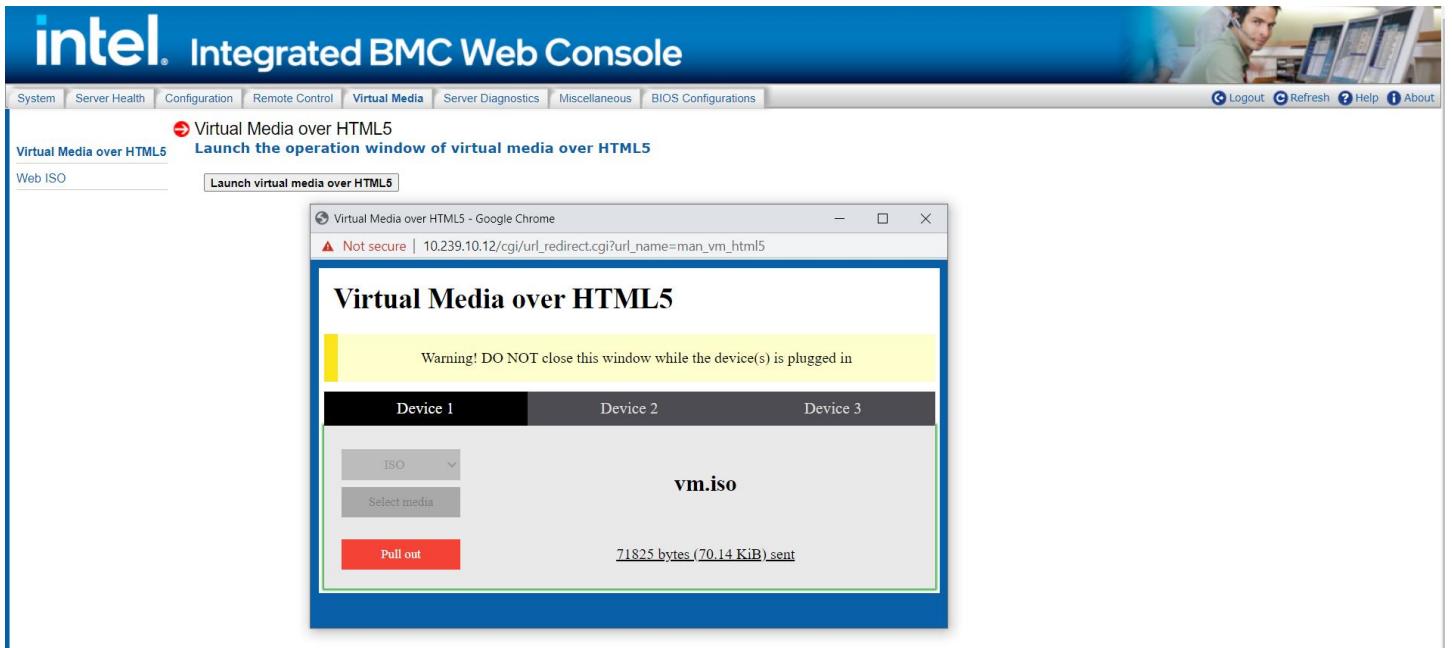


Figure 86. Plug in ISO

Table 28. Virtual Media over HTML5 Options

Option	Task
Device	Select one of three devices.
Select type	Select file type (Folder or ISO or IMG/IMA).
Select media	Choose the file path.
User	User name of Samba* or NFS.
Plug in/Pull out	Mount/umount file.

7.5.2 Web ISO

Web ISO allows the user to share an ISO image using the SMB or the NFS protocol. It allows the user to share the image over a Windows Share* or Linux* Samba* or NFS. This image will be emulated to the host as a USB device.

The screenshot shows the 'Web ISO' configuration page within the Integrated BMC Web Console. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media (which is highlighted in blue), Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. The main content area is titled 'Web ISO' and contains a sub-section 'Virtual Media over HTML5'. A message 'No disk emulation set.' is displayed above a 'Refresh Status' button. Below this are fields for 'Mount type' (set to 'Samba'), 'Share host', 'Path to image', 'User', and 'Password'. At the bottom are buttons for 'Save', 'Mount', and 'Unmount'.

Figure 87. Web ISO

Table 29. Web ISO Options

Option	Task
Device	Showing the VM status.
Mount type	Samba* or NFS.
Share host	Share host IP address.
Path to image	Image name with path.
User	User name of Samba* or NFS.
Password	Password of Samba* or NFS.

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 debug 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 88](#) for details.

The screenshot shows the 'System Diagnostics' section of the BMC Web Console. On the left, there's a sidebar with links for 'POST Codes', 'System Defaults', and 'SOL Log'. The main content area has a heading 'System Debug Log' with a sub-section 'Last Log' showing 'None'. At the bottom, there's a 'Generate Log' button.

[Figure 88. Server System Diagnostics Page](#)

Click the **Generate Log** button. It may take some time for the debug 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 firmware and have associated SDRs populated in the SDR repository. This does not include any “event-only” sensors. (All BIOS sensors and some BMC and 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 89](#) 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.

The screenshot shows the 'Server Diagnostics' section of the BMC Web Console. On the left, a sidebar lists 'System Diagnostics', 'POST Codes' (which is selected), 'System Defaults', and 'SOL Log'. The main area is titled 'System POST Codes' and includes a dropdown menu 'Show time from start of POST'. Below it, a 'Previous Boot' section says 'No Post Codes available yet'. To its right, a 'Current Boot' section shows a table of POST codes:

Time	Code	Description
00:00.000	0x9B	DXE USB reset
00:00.060	0x9C	DXE USB detect
00:00.280	0x9C	DXE USB detect
00:28.700	0x9C	DXE USB detect

Figure 89. Server Diagnostics POST Codes Page

7.6.3 System Defaults

The System Defaults page allows resetting all BMC settings to factory defaults. See [Figure 90](#) 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.

The screenshot shows the 'Server Diagnostics' section of the BMC Web Console. On the left, a sidebar lists 'System Diagnostics', 'POST Codes', 'System Defaults' (which is selected), and 'SOL Log'. In the center, there is a 'Factory Default' link next to a red circular arrow icon. A 'Restore' button is located below the sidebar. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, BIOS Configurations, Logout, Refresh, Help, and About.

Figure 90. Server Diagnostics Default Page

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 91). Table 30 lists the SOL log operations that can be performed.

The screenshot shows the 'Server Diagnostics' section of the BMC Web Console. On the left, there's a sidebar with links for System Diagnostics, POST Codes, System Defaults, and SOL Log. The main area is titled 'SOL Log' and contains two sections: 'Enable SOL log' and 'View & Dump SOL log'. The 'Enable SOL log' section has a checkbox labeled 'Enable SOL log' and a 'Save' button. The 'View & Dump SOL log' section has a sub-section titled 'SOL Log View' and a 'Save SOL Log' button.

Figure 91. Server Diagnostics SOL Log Page

Table 30. 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 Intel® Node Manager Configuration

Intel® NM configuration is used to view, add, and configure the Intel® Node Manager Policies. See [Figure 92](#) for details. [Table 31](#) lists the options to view, add, and edit the Intel® NM power policies.

The screenshot shows the 'Miscellaneous' tab selected in the top navigation bar. On the left, there's a sidebar with 'NM Configuration' and two collapsed sections: 'Power Statistics' and 'Power Telemetry'. The main area is titled 'Add/Edit Node Manager Policies.' It contains the following fields:

- Policy ID:** A text input field.
- Enable:** A checked checkbox.
- Shutdown:** An unchecked checkbox.
- Log Event:** An unchecked checkbox.
- Power Limit (Watt):** A text input field.
- Use Policy Suspend Timers:** A radio button group with 'Yes' and 'No' options, where 'No' is selected.

At the bottom are three buttons: 'Save', 'Delete', and 'Cancel'.

Figure 92. Intel® NM Configuration Page

Table 31. 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 93). 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).

The screenshot shows the 'NM Configuration' section of the BMC Web Console. At the top, there are checkboxes for 'Policy ID', 'Enable', 'Shutdown', and 'Log Event'. Below this, the 'Power Limit (Watt)' field is empty. Under 'Use Policy Suspend Timers:', the 'Yes' radio button is selected. A large grid follows, containing two columns of five timer entries each. Each entry includes a checkbox for the timer number, a day of the week, and a start/end time selection. At the bottom are 'Save', 'Delete', and 'Cancel' buttons.

Figure 93. 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, timestamp and period in [Figure 94](#).

The screenshot shows the 'Power Statistics' section of the BMC Web Console. The table has columns for Subsystem, Current, Average, Maximum, Minimum, Timestamp, and Period. The data is as follows:

Subsystem	Current	Average	Maximum	Minimum	Timestamp	Period
Entire platform	220	128	319	1	Thu Dec 20 15:08:28 2018	2 days 8 hours 56 minutes 8 seconds
CPU	125	125	213	112	Thu Dec 20 15:08:29 2018	2 days 8 hours 56 minutes 8 seconds
Memory	13	13	14	13	Thu Dec 20 15:08:29 2018	1 days 8 hours 56 minutes 0 seconds

Figure 94. 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 95](#) for details. To select a device category, use the **Select a device category** drop-down box ([Figure 96](#)).



Figure 95. Power Telemetry page

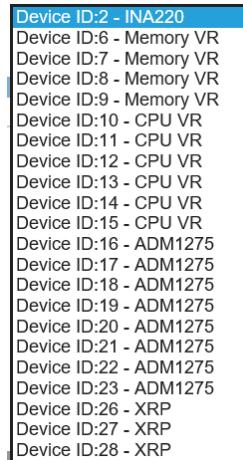


Figure 96. Power Telemetry Device Categories

7.8 BIOS Configurations Tab

The **BIOS Configurations** tab provides a method to configure any BIOS Setup Variables through the BMC EWS, 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 97](#) for details.

Key	Value	BIOS Variable Description	Value	Saved Value
Memory Mapped I/O above 4 GB	Enable or disable memory mapped I/O of 64-bit PCI devices to 4 GB or greater address space.	0x1 (Enabled)	0x1 (Enabled)	
MMIO High Base	Select MMIO High Base	0x0 (56T)	0x0 (56T)	
Memory Mapped I/O Size	Sets the size of MMIO space above 4GB.	0x4 (256G)	0x4 (256G)	
Add-in Video Adapter	When Onboard Video is Enabled, and Add-in Video Adapter is also Enabled, both can be active. The onboard video is still the primary console and active during BIOS POST; the add-in video adapter would be active under an OS environment with the video driver support. When Onboard Video is Enabled, and Add-in Video Adapter is Disabled, then only the onboard video would be active. When Onboard Video is Disabled, and Add-in Video Adapter is Enabled, then only the add-in video adapter would be active.	0x2 (Disabled)	0x2 (Disabled)	
Onboard Video	Enable or disable onboard video controller. Warning: System video is completely disabled if this option is disabled and an add-in video adapter is not installed.	0x1 (Enabled)	0x1 (Enabled)	
Fast Video	Enable/disable fast video. Fast video allows the screen light up in early phase. Note Fast Video only appears when Onboard Video is Enabled.	0x1 (Enabled)	0x1 (Enabled)	

Figure 97. 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 98](#) for details. [Table 32](#) lists all serial port configuration variables that can be viewed and edited.

Key	Value	BIOS Variable Description	Value	Saved Value
Serial A Enable	Enable or Disable Serial port A.	0x1 (Enabled)	0x1 (Enabled)	
Serial A Address	Select Serial port A base I/O address.	0x0 (3F8h)	0x0 (3F8h)	

Figure 98. BIOS Serial Port Configuration Page

Table 32. 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 99](#) for details.

[Table 33](#) lists all UPI configuration variables that can be viewed and edited.

The screenshot shows the 'UPI Configuration' page within the Integrated BMC Web Console. The left sidebar contains navigation links for various configuration categories. The main content area is titled 'UPI Configuration' and displays a table of BIOS variables. The table has columns for 'Key Value', 'BIOS Variable Description', 'Value', and 'SavedValue'. The variables listed include Intel(R) UPI Frequency Select, IO Directory Cache (IODC), KTI Prefetch, Stale AtoS, LLC Dead Line Alloc, Direct To Core (D2C), and Direct To UPI (D2K). At the bottom of the table are 'Save' and 'Cancel' buttons.

Key Value	BIOS Variable Description	Value	SavedValue
Intel(R) UPI Frequency Select	Allows for selecting the Intel(R) UltraPath Interconnect Frequency. Recommended to leave in [Auto Max] so that the BIOS can select the highest common Intel(R) UltraPath Interconnect frequency.	0x2 (Auto Max)	0x2 (Auto Max)
IO Directory Cache (IODC)	IO Directory Cache (IODC): generate snoops instead of memory lookups, for remote InvitoM (IIO) and/or WCILF (cores). Auto - Auto sets to WCILF.	0x1 (Auto)	0x1 (Auto)
KTI Prefetch	KTI Prefetch.	0x1 (Enabled)	0x1 (Enabled)
Stale AtoS	Stale A to S Dir optimization.	0x0 (Disabled)	0x0 (Disabled)
LLC Dead Line Alloc	Enable - opportunistically fill dead lines in LLC. Disable - never fill dead lines in LLC.	0x1 (Enabled)	0x1 (Enabled)
Direct To Core (D2C)	Direct To Core (D2C)	0x2 (Auto)	0x2 (Auto)
Direct To UPI (D2K)	Direct To UPI (D2K)	0x2 (Auto)	0x2 (Auto)

Figure 99. BIOS UPI Configuration Page

Table 33. 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 100](#) for details. [Table 34](#) lists all IIO configuration variables that can be viewed and edited.

The screenshot shows the 'Integrated IO Configuration' page. At the top, there are dropdown menus for 'Select a BIOS Variable' (set to 'NTB PCIe Port 1a on CPU socket 1') and 'BIOS Variable Value' (set to '0x0 (Transparent Bridge)'). The main area contains a table with columns: Key, Value, BIOS Variable Description, Value, and SavedValue. The table includes rows for NTB PCIe ports (1a, 2a, 3a) on both sockets, Intel(R) VT for Directed I/O, PCIe PII SSC, Relaxed Ordering, and multiple No Snoop (Sck0 IOAT Function 0-7) entries. Buttons for 'Save' and 'Cancel' are at the bottom left.

Key	Value	BIOS Variable Description	Value	SavedValue
NTB PCIe Port 1a on CPU socket 1		Configures port as TB, NTB-NTB	0x0 (Transparent Bridge)	0x0 (Transparent Bridge)
NTB PCIe Port 2a on CPU socket 1		Configures port as TB, NTB-NTB	0x0 (Transparent Bridge)	0x0 (Transparent Bridge)
NTB PCIe Port 3a on CPU socket 1		Configures port as TB, NTB-NTB	0x0 (Transparent Bridge)	0x0 (Transparent Bridge)
NTB PCIe Port 1a on CPU socket 2		Configures port as TB, NTB-NTB	0x0 (Transparent Bridge)	0x0 (Transparent Bridge)
NTB PCIe Port 2a on CPU socket 2		Configures port as TB, NTB-NTB	0x0 (Transparent Bridge)	0x0 (Transparent Bridge)
NTB PCIe Port 3a on CPU socket 2		Configures port as TB, NTB-NTB	0x0 (Transparent Bridge)	0x0 (Transparent Bridge)
Intel(R) VT for Directed I/O		Enable/Disable Intel(R) Virtualization Technology for Directed I/O (Intel(R) VT-d). Report the I/O device assignment to VMM through DMAR ACPI Tables.	0x0 (Disabled)	0x0 (Disabled)
Pcie PII SSC		Pcie PII SSC percentage or Disable SSC. Range is 0.0%-1.9%. Last one is the POR for LBG.	0x14 (POR - Reg. Value 0x1F)	0x14 (POR - Reg. Value:0x1F)
Relaxed Ordering		Relaxed Ordering Enable/Disable	0x0 (Disabled)	0x0 (Disabled)
No Snoop(Sck0 IOAT Function 0)		No Snoop Enable/Disable for each CB device	0x0 (Disabled)	0x0 (Disabled)
No Snoop(Sck0 IOAT Function 1)		No Snoop Enable/Disable for each CB device	0x0 (Disabled)	0x0 (Disabled)
No Snoop(Sck0 IOAT Function 2)		No Snoop Enable/Disable for each CB device	0x0 (Disabled)	0x0 (Disabled)
No Snoop(Sck0 IOAT Function 3)		No Snoop Enable/Disable for each CB device	0x0 (Disabled)	0x0 (Disabled)
No Snoop(Sck0 IOAT Function 4)		No Snoop Enable/Disable for each CB device	0x0 (Disabled)	0x0 (Disabled)

Figure 100. BIOS IIO Configuration Page

Table 34. 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	Configure NTB PCIe* port for socket 1 and socket 2.
NTB PCIe Port 1a on CPU socket 2	
NTB PCIe Port 2a on CPU socket 2	
NTB PCIe Port 3a on CPU 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	Select BAR23/4/5/45 size for each PCIe* port on the socket 1 and socket 2.
Secondary BAR 4 Size	
Secondary BAR 5 Size	
Secondary BAR 45 Size	
Intel(R) VT for Directed I/O	Enable or disable Intel® 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)	Enable or disable for each CB device on sock0.
No Snoop(Sck0 IOAT Function 7)	

Variables	BIOS Variable Description
No Snoop(Sck1 IOAT Function 1)	
No Snoop(Sck1 IOAT Function 2)	
No Snoop(Sck1 IOAT Function 3)	
No Snoop(Sck1 IOAT Function 4)	Enable or disable for each CB device on sock1.
No Snoop(Sck1 IOAT Function 5)	
No Snoop(Sck1 IOAT Function 6)	
No Snoop(Sck1 IOAT Function 7)	
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
Positioned TLP Mask	Enable or disable for Positioned 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 101](#) for details. [Table 35](#) lists all memory configuration variables that can be viewed and edited.

The screenshot shows the 'Memory Configuration' section of the BMC Web Console. On the left, a sidebar lists various configuration categories. The main area shows a table of BIOS variables with their descriptions, current values, and saved values. The table includes columns for Key Value, BIOS Variable Description, Value, and Saved Value. Buttons for Save and Cancel are at the bottom.

Key Value	BIOS Variable Description	Value	Saved Value
Memory Operating Speed Selection	Force specific Memory Operating Speed or use Auto setting.	0x0 (Auto)	0x0 (Auto)
IMC Interleaving	Select IMC Interleaving setting.	0x0 (Auto)	0x0 (Auto)
Page Policy	Select Page Policy.	0x3 (Auto)	0x3 (Auto)
Volatile Memory Mode	Selects whether LLM or 2LM memory mode should be enabled.	0x2 (Auto)	0x2 (Auto)
Intel(R) Optane(TM) PMem Error Injection	Enable/Disable Intel(R) Optane(TM) PMem Error injection.	0x0 (Disabled)	0x0 (Disabled)
Publish ARS capability	Enable/Disable publishing of the Address Range Scrub capability to the OS.	0x2 (Auto)	0x2 (Auto)
Skip ARS on Boot	Enabled: prevent BIOS from starting system-wide ARS on boot.	0x0 (Disabled)	0x0 (Disabled)
Background ARS	Auto: go background on initial short ARS sequence. Sets the power management policy for average power (must be an increment of 250 mW). Warning: 128GB DIMM will work on MAX 15W and 256GB/512GB cannot go below 10W. If value outside the range are set, the default will fall into the range.	0x2 (Auto)	0x2 (Auto)
Average Power Budget (in mW)	Sets the power management policy for average power (must be an increment of 250 mW). Warning: 128GB DIMM will work on MAX 15W and 256GB/512GB cannot go below 10W. If value outside the range are set, the default will fall into the range.	0x3A98	0x3A98
SMB Clock Frequency	Sets DDR4 SMBus Clock Frequencies For SPD Access. Auto - Sets it to the MRC default setting, current default is 400K.	0x0 (Auto)	0x0 (Auto)

Figure 101. BIOS Memory Configuration Page

Table 35. BIOS Memory Configuration Variables

Variables	BIOS Variable Description
Memory Operating Speed Selection	Force specific Memory Operating Speed or use Auto setting.
IMC Interleaving	Select IMC Interleaving setting.
Page Policy	Select page policy.
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.
Skip ARS on Boot	Enabled: prevent BIOS from starting system-wide ARS on boot.
Background ARS	Auto: go background on initial short ARS sequence.
Average Power Budget(in mW)	Sets the power management policy for average power (must be an increment of 250 mW). Warning: 128GB DIMM will work on MAX 15W and 256GB/512GB cannot go below 10W. If value outside the range is set, the default will fall into the range
SMB Clock Frequency	Sets DDR4 SMBus Clock Frequencies For SPD Access. Auto - Sets it to the MRC default setting; current default is 400K.
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 (Appdirect) specific feature to avoid directory updates to DDRT memory from non-NUMA optimized workloads.
NVM Performance Setting	NVM baseline performance settings depending on the workload behavior
CR FastGo Configuration	Select CR QoS Configuration Profiles.
CR Latch System Shutdown State	Latch System Shutdown State.
CR QoS	CR QoS tuning recipes.
Thermal Throttling Thresholds Offset	Auto - T_crit-(2/3)C Enable - T_crit-(1/2)C Threshold limits.
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 NVMDIMM receives surprise clock stop.
MRC Promote Warnings	Determines if MRC warnings are promoted to system level.
Promote Warnings	Determines if warnings are promoted to system level.
Halt on mem Training Error	Halt on mem Training Error Disable/Enable.
Thermal Monitor	Enable/Disable Thermal Monitor.
PPR Type	Selects Post Package Repair Type - Hard / Soft / Disabled. Auto - Sets it to the MRC default setting; current default is Soft PPR.
MemTest	Enable - Enables memory test during normal boot. Disable - Disables this feature. Auto - Sets it to MRC default setting; current default is Enable.
MemTest Loops	Number of memory test loops during normal boot, set to 0 to run memory test infinitely
Adv MemTest Options	This option is a bit mask[15:0]: All 0 - disabled: bit-0-XMATS8, bit-1-XMATS16, bit-2-XMATS32, bit-3-XMATS64, bit-4-WCMATS8, bit-5-WCMCH8, bit-6-GNDB64, bit-7-MARCHCM64, bit-11-TWR, bit-12-DATARET, bit-13-MATS8TC1, bit-14-MATS8TC2, bit-15-MATS8TC3
Adv MemTest Reset Failure Tracking List	Enable/disable Reset of the Row Failure Tracking List after each Adv MemTest option. Useful for testing performance of multiple options.
Adv MemTest Conditions	Auto - set test conditions based on test type; Manual - specify global test conditions; Disable - Do not apply test conditions.

Variables	BIOS Variable Description
NUMA Optimized	If enabled, BIOS includes ACPI tables that are required for NUMA-aware Operating Systems.
Sub_NUMA Cluster	When enabled, sub NUMA cluster enabled. If any memory controller has no memory attached, this feature cannot be enabled.
Patrol Scrub	When enabled, performs periodic checks on memory cells and proactively walks through populated memory space, to seek and correct soft ECC errors.
Cloaking	If disabled, CMCI event appears when CE happens. If enabled, CMCI event is blocked when CE happens.

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® SpeedStep® tech/Intel® configurable TDP/Turbo Boost/C1E /processor C6. See [Figure 102](#) for details. [Table 36](#) lists all PnP configuration variables that can be viewed and edited.

Key	Value	BIOs Variable Description	Value	Saved Value
CPU Power and Performance Policy	0x0 (Balanced Performance)	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.	0x0 (Balanced Performance)	0x0 (Balanced Performance)
Workload Configuration	0x0 (Balanced)	Controls the aggressiveness of the energy performance BIAS settings. This bit field allows BIOS to choose a configuration that may improve performance on certain workloads.	0x0 (Balanced)	0x0 (Balanced)
Uncore Frequency Scaling	0x0 (Enabled)	Allows the voltage and frequency of Uncore to be programmed independently. The Uncore activity is monitored to optimize the frequency in real-time.	0x0 (Enabled)	0x0 (Enabled)
Performance P-limit	0x1 (Enabled)	Allows the Uncore frequency coordination of two processors when enabled.	0x1 (Enabled)	0x1 (Enabled)

Figure 102. BIOS PnP Configuration Page

Table 36. 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.
Workload Configuration	Controls the aggressiveness of the energy performance BIAS settings. This bit field allows BIOS to choose a configuration that may improve performance on certain workloads.
Uncore Frequency Scaling	Allows the voltage and frequency of Uncore to be programmed independently. The Uncore activity is monitored to optimize the frequency in real-time.
Performance P-limit	Allows the Uncore frequency coordination of two processors when enabled.
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 the corresponding OS vendor regarding OS support of this feature.

Variables	BIOS Variable Description
Intel Configurable TDP	Allows the user to disable/enable Intel Config TDP.
Configurable TDP Level	Allows the user to select Intel Config TDP level - Nominal is the default TDP.
Intel(R) Turbo Boost Technology	Intel® Turbo Boost Technology allows the processor to automatically increase its frequency if it is running below power, temperature, and current specifications.
Energy Efficient Turbo	When Energy Efficient Turbo is enabled, the CPU cores only enter the turbo frequency when the PCU detects high utilization.
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	Enable/Disable core parameter based per core power budgeting. PPO-Budget allocates power budget to cores based on their scalability/EPP.
Package C-State	Enable/Disable RAPL Prioritization allows creating core groups of different priority
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(R) 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 103](#) for details. [Table 37](#) lists all processor configuration variables that can be viewed and edited.

Key Value	BIOS Variable Description	Value	SavedValue
Intel(R) Hyper-Threading Tech	Intel(R) Hyper-Threading Technology allows multithreaded software applications to execute threads in parallel within each processor. Contact your OS vendor regarding OS support of this feature.	0x0 (Enabled)	0x0 (Enabled)
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 will cause 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)
Enhanced Error Containment Mode	Enable Enhanced Error Containment Mode (Data Poisoning) - Erroneous data coming from memory will be poisoned. If disabled (default), will be in Legacy Mode - No data poisoning support available.	0x0 (Disabled)	0x0 (Disabled)
MLC Streamer	MLC Streamer is a speculative prefetcher 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. [Enabled] - Only fetches cache line with data required by the processor.	0x1 (Enabled)	0x1 (Enabled)

Figure 103. BIOS Processor Configuration Page

Table 37. BIOS Processor Configuration Variables

Variables	BIOS Variable Description
Intel(R) Hyper-Threading Tech	Intel® Hyper-Threading Technology allows multithreaded software applications to execute threads in parallel within each processor. Contact the corresponding OS vendor regarding OS support of this feature.
Intel(R) Virtualization Technology	Intel® 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® Trusted Execution Technology. Takes effect after reboot.
Enhanced Error Containment Mode	Enable Enhanced Error Containment Mode (Data Poisoning) - Erroneous data coming from memory will be poisoned. If disabled (default), will be in Legacy Mode - No data poisoning support available.
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.
LLC Prefetch	Enable/Disable LLC Prefetch on all threads.
RDT CAT Opportunistic Tuning	Cache Allocation Technology mask tuning options. NOTE: If IOT is enabled on any socket this option will override to 0x003.
3StrikeTimer	The 3 strike counter can be turned off by writing into the MISC_FEATURE_CONTROL_DISABLE_THREE_STRIKE_CNT(MSR 0x01a4).

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 104](#) for details. [Table 38](#) lists all mass storage controller configuration variables that can be viewed and edited.

The screenshot shows the 'Mass Storage Controller Configuration' page. At the top, there's a navigation bar with links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, BIOS Configurations, Logout, Refresh, Help, and About. On the left, a sidebar lists various configuration categories like PCI Configuration, Serial Port Configuration, UPI Configuration, Integrated IO Configuration, Memory Configuration, Power n Performance, Processor Configuration, and several System and Security options. The main content area is titled 'Mass Storage Controller Configuration' and contains a table with the following data:

Key Value	BIOS Variable Description	Value	SavedValue
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.	0x0 (AHCI)	0x0 (AHCI)
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.	0x0 (Disabled)	0x0 (Disabled)
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.	0x0 (AHCI)	0x0 (AHCI)
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.	0x0 (Disabled)	0x0 (Disabled)

At the bottom of the page are 'Save' and 'Cancel' buttons.

Figure 104. BIOS Mass Storage Controller Configuration Page

Table 38. 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 105](#) for details. [Table 39](#) lists all system acoustic and performance configuration variables that can be viewed and edited.

Key	Value	BIOS Variable Description	Value	Saved Value
Set Fan Profile	0x2 (Acoustic)	[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.	0x2 (Acoustic)	0x2 (Acoustic)

Figure 105. BIOS System Acoustic and Performance Configuration Page

Table 39. 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 106](#) for details.

Key Value	BIOS Variable Description	Value	SavedValue
System Errors	System Error Enable/Disable setup options.	0x1 (Enabled)	0x1 (Enabled)
EMCA Logging Support	Enable/Disable EMCA Logging	0x1 (Enabled)	0x1 (Enabled)
Ignore OS EMCA Opt-in	Enable/Disable Ignore OS EMCA Opt-in and log	0x0 (Disabled)	0x0 (Disabled)
EMCA CMCI-SMI Morphing	Enable/Disable EMCA CSMI	0x2 (EMCA gen 2 CSMI)	0x2 (EMCA gen 2 CSMI)
EMCA MCE-SMI Enable	Enable/Disable EMCA Uncorrected SMI for gen1 and gen2	0x2 (EMCA gen 2 - MSMI)	0x2 (EMCA gen 2 - MSMI)
Corrected Error eLog	Enable/Disable Corrected Error eLog	0x1 (Enabled)	0x1 (Enabled)
Memory Error eLog	Enable/Disable Memory Error eLog	0x1 (Enabled)	0x1 (Enabled)
Processor Error eLog	Enable/Disable Processor Error eLog	0x1 (Enabled)	0x1 (Enabled)
WHEA Support	Enable/Disable WHEA support	0x1 (Enabled)	0x1 (Enabled)
Whea Log Memory Error	Enable/Disable Whea Log Memory Error	0x1 (Enabled)	0x1 (Enabled)
Whea Log Processor Error	Enable/Disable Whea Log Processor Error	0x1 (Enabled)	0x1 (Enabled)
Whea Log PCI Error	Enable/Disable Whea Log PCI Error	0x1 (Enabled)	0x1 (Enabled)
Mca Bank Error Injection Support	Enable/Disable Mca Bank Error Injection Support.	0x0 (Disabled)	0x0 (Disabled)
WHEA Error Injection Support	Enable/Disable WHEA Error Injection Support. Please disable DIRECTORY MODE for Memory	0x1 (Enabled)	0x1 (Enabled)

Save **Cancel**

Figure 106. 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 107](#) for details. [Table 40](#) lists all security variables that can be viewed and edited.

Key Value	BIOS Variable Description	Value	SavedValue
Power On Password	Enable Power On Password support. If enabled, password entry is required in order to boot the system	0x0 (Disabled)	0x0 (Disabled)
Front Panel Lockout	If enabled, locks the power button OFF function and the reset and NMI Diagnostic Interrupt buttons on the front panel of the system. If [Enabled] is selected, power-off and reset must be controlled via a system management interface, and the NMI Diagnostic Interrupt is not available.	0x0 (Disabled)	0x0 (Disabled)

Save **Cancel**

Figure 107. BIOS Security Configuration Page

Table 40. 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 108](#) for details. [Table 41](#) lists all USB configuration variables that can be viewed and edited.

The screenshot shows the Integrated BMC Web Console interface. The top navigation bar includes links for System, Server Health, Configuration, Remote Control, Virtual Media, Server Diagnostics, Miscellaneous, and BIOS Configurations. The BIOS Configurations link is highlighted. The main content area is titled "USB Configuration". A sidebar on the left lists various configuration categories: 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, and Main. The "USB Configuration" category is currently selected. The main content area displays a table with the following data:

Key	Value	BIOS Variable Description	Value	Saved Value
Legacy USB Support	0x0 (Enabled)	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. Disable option will only keep USB Keyboard devices available for EFI applications.	0x0 (Enabled)	0x0 (Enabled)
Port 60/64 Emulation	0x1 (Enabled)	Enables I/O port 60h/64h emulation support. This may be needed for legacy USB keyboard support when using an OS that is USB unaware.	0x1 (Enabled)	0x1 (Enabled)
Make USB Devices Non-Bootable	0x0 (Disabled)	Exclude USB in Boot Table. [Enabled] - This will remove all USB Mass Storage devices as Boot options. [Disabled] - This will allow all USB Mass Storage devices as Boot options.	0x0 (Disabled)	0x0 (Disabled)
Device Reset Timeout	0x1 (20 seconds)	USB Mass Storage device Start Unit command timeout. Setting to a larger value provides more time for a mass storage device to be ready, if needed.	0x1 (20 seconds)	0x1 (20 seconds)

At the bottom of the table are "Save" and "Cancel" buttons.

Figure 108. BIOS USB Configuration Page

Table 41. BIOS USB Configuration Variables

Variables	BIOS Variable Description
Legacy USB Support	Enables Legacy USB support. AUTO option disables legacy support if no USB devices are connected. Disable option will only keep USB Keyboard devices available for EFI applications.
Port 60/64 Emulation	Enables I/O port 60h/64h emulation support. This may be needed for legacy USB keyboard support when using an OS that is USB unaware.
Make USB Devices Non-Bootable	Exclude USB in Boot Table. [Enabled] - This will remove all USB Mass Storage devices as Boot options. [Disabled] - This will allow all USB Mass Storage devices as Boot options.
Device Reset Timeout	USB Mass Storage device Start Unit command timeout. Setting to a larger value provides more time for a mass storage device to be ready, if needed.

7.8.13 Server Management

The page allows the user to configure server management features, such as Console redirection enabling. See [Figure 109](#) for details. [Table 42](#) lists all options that can be viewed and edited.

Figure 109. BIOS Server Management Page

Table 42. Server Management

Variables	BIOS Variable Description
Assert NMI on SERR	On SERR, generate an NMI and log an error. Note: [Enabled] must be selected for the Assert NMI on PERR setup option to be visible.
Assert NMI on PERR	On PERR, generate an NMI and log an error. Note: This option is only active if the Assert NMI on SERR option has [Enabled] selected.
PCIe AER Support	[Enabled] - PCIe* AER (Advanced Error Reporting) is enabled. [Disabled] - PCIe* AER is disabled. All PCIe* AER errors will be masked once PCIe AER is disabled.
Log Correctable Errors	[Enabled] - Processor n PCH PCIe* correctable error logging is enabled. [Disabled] - Processor n PCH PCIe* correctable error logging is disabled.
PCIE Correctable Error Threshold	Threshold value for logging Correctable Errors(CE) - Threshold of 20/10/5 logs 20th/10th/5th CE, 0(default) logs every CE.
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 the 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.
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.

Variables	BIOS Variable Description
Plug n Play BMC Detection	If enabled, the BMC will be detectable by operating systems that support plug and play loading of an IPMI driver. Do not enable this option if the corresponding 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 110](#) for details. [Table 43](#) lists all Advanced Boot Options that can be viewed and edited.

The screenshot shows the 'Advanced Boot Options' section of the BIOS configuration. It includes a table with columns for Key, Value, BIOS Variable Description, Value, and SavedValue. The table rows correspond to the variables listed in Table 43.

Key	Value	BIOS Variable Description	Value	SavedValue
System Boot Timeout	0x0001	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.	0x0001	0x0001
Early System Boot Timeout	0x0000	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.	0x0000	0x0000
Boot Mode	0x1 (UEFI)	When Boot Mode is Legacy, the BIOS only loads modules required for booting Legacy Operating Systems. When Boot Mode is UEFI, the BIOS only loads modules required for booting UEFI-aware Operating Systems.	0x1 (UEFI)	0x1 (UEFI)
Video BIOS	0x0 (UEFI)	If Video BIOS is Legacy, the BIOS uses the legacy video ROM instead of the EFI video ROM when Boot Mode is UEFI.	0x0 (UEFI)	0x0 (UEFI)
Boot Option Retry	0x0 (Disabled)	If enabled, this continually retries non-EFI-based boot options without waiting for user input.	0x0 (Disabled)	0x0 (Disabled)
USB Boot Priority	0x1 (Enabled)	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.	0x1 (Enabled)	0x1 (Enabled)

Figure 110. BIOS Advanced Boot Page

Table 43. 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.
Video BIOS	When Boot Mode is Legacy, the BIOS only loads modules required for booting Legacy Operating Systems. When Boot Mode is UEFI, the BIOS only loads modules required for booting UEFI-aware Operating Systems.
Boot Option Retry	If enabled, this continually retries non-EFI-based boot options without waiting for user input.
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 111](#) for details. [Table 44](#) lists all main BIOS variables that can be viewed and edited.

The screenshot shows the 'Main' configuration page of the Integrated BMC Web Console. On the left, a sidebar lists various configuration categories. The 'Main' category is selected and highlighted in blue. In the center, there's a table showing BIOS variable settings. The first row shows 'Quiet Boot' set to 'Enabled'. The second row shows 'POST Error Pause' set to 'Disabled'. At the bottom of the table are 'Save' and 'Cancel' buttons.

Key	Value	BIOS Variable Description	Value	Saved Value
Quiet Boot	Enabled	[Enabled] - Display the logo screen during POST. [Disabled] - Display the diagnostic screen during POST.	0x1 (Enabled)	0x1 (Enabled)
POST Error Pause	Disabled	[Enabled] - Go to the Error Manager for critical POST errors. [Disabled] - Attempt to boot and do not go to the Error Manager for critical POST errors.	0x0 (Disabled)	0x0 (Disabled)

Figure 111. BIOS Main Page

Table 44. BIOS Main Configuration Variables

Variables	BIOS Variable Description
Quiet Boot	[Enabled] - Display the logo screen during POST. [Disabled] - Display the diagnostic screen during POST.
POST Error Pause	[Enabled] - Go to the Error Manager for critical POST errors. [Disabled] - Attempt to boot and do not go to the Error Manager for critical POST errors.

Appendix A. Glossary

Term	Definition
ARP	Address Resolution Protocol
Intel® ASMI	Intel® Advanced Server Management Interface
BMC	Baseboard Management Controller
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
HI	Host Interface
ICMP	Internet Control Message Protocol
IPMI	Intelligent Platform Management Interface
KVM	Keyboard, Video, Mouse
LAN	Local Area Network
LDAP	Lightweight Directory Address Protocol
MAC	Media Access Controller
MII	Media Independent Interface
NIC	Network Interface Controller
Intel® NM	Intel® Node Manager
OOB	Out Of Band – no operating system interaction on server
Intel® RMM4	Intel® Remote Management Module 4
SDR	Sensor Data Record
SOL	Serial-over-LAN
TCP/IP	Transmission Control Protocol/Internet Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
KCS	Keyboard Controller Style