Intel® Remote Management Module 4 and Integrated BMC Web Console

User Guide

Guide to installing and using Intel® Remote Management Module 4 (Intel® RMM4) and Integrated BMC web console for Intel® Server Boards and Systems based on Intel® Xeon® processor Scalable family.

Rev 1.1

January 2018

Intel® Server Products and Solutions

<Blank page>

Document Revision History

Date	Revision	Changes
December 2017	1.0	Initial release.
January 2018	1.1	Public release.

Disclaimers

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

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

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

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

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

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

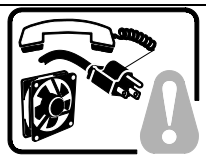
Intel, the Intel logo, Intel Xeon Phi, and Xeon are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

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

Safety Information

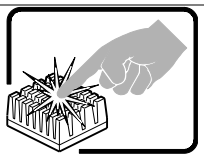
Important Safety Instructions

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.



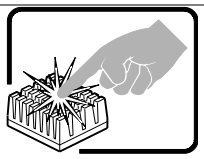
A microprocessor and heat sink may be hot if the system has been running. Also, there may be sharp pins and edges on some board and chassis parts. Contact should be made with care. Consider wearing protective gloves.

Wichtige Sicherheitshinweise

Lesen Sie zunächst sämtliche Warnund 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:

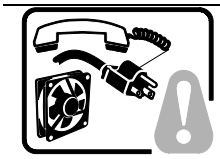
1. Schalten Sie alle an Ihr System angeschlossenen Peripheriegeräte aus.
2. Schalten Sie das System mit dem Hauptschalter aus.
3. Ziehen Sie den Stromanschlußstecker Ihres Systems aus der Steckdose.
4. Auf der Rückseite des Systems beschriften und ziehen Sie alle Anschlußkabel von den I/O Anschlüssen 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 Gehäuseteile scharfe Spitzen und Kanten aufweisen. Arbeiten an Platinen und Gehäuse sollten vorsichtig ausgeführt werden. Sie sollten Schutzhandschuhe tragen.

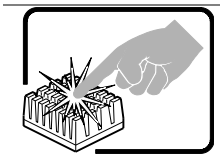
Consignes de sécurité

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:

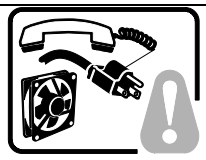
1. Mettez hors tension tous les périphériques connectés au système.
2. Mettez le système hors tension en mettant l'interrupteur général en position OFF (bouton-poussoir).
3. Débranchez tous les cordons d'alimentation c.a. du système et des prises murales.
4. Identifiez et débranchez tous les câbles reliés 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.

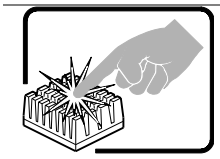
Instrucciones de seguridad importantes

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.

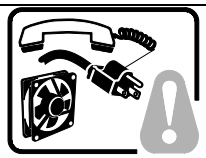


Si el sistema ha estado en funcionamiento, el microprocesador y el disipador de calor pueden estar aún calientes. También conviene tener en cuenta que en el chasis o en el tablero puede haber piezas cortantes o punzantes. Por ello, se recomienda precaución y el uso de guantes protectores.

重要安全指导

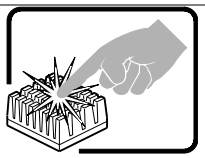
在执行任何指令前，请阅读本文档中所有的注意事项及安全声明。或 https://www.intel.com/content/dam/support/us/en/documents/server-products/g23122-004_safetyregulatory.pdf 上的*Intel Server Boards and Server Chassis Safety Information*（《Intel服务器主板与服务器机箱安全信息》）

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

List of Figures

List of Tables

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 knowledgebase 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 screen capture, 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 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

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*.

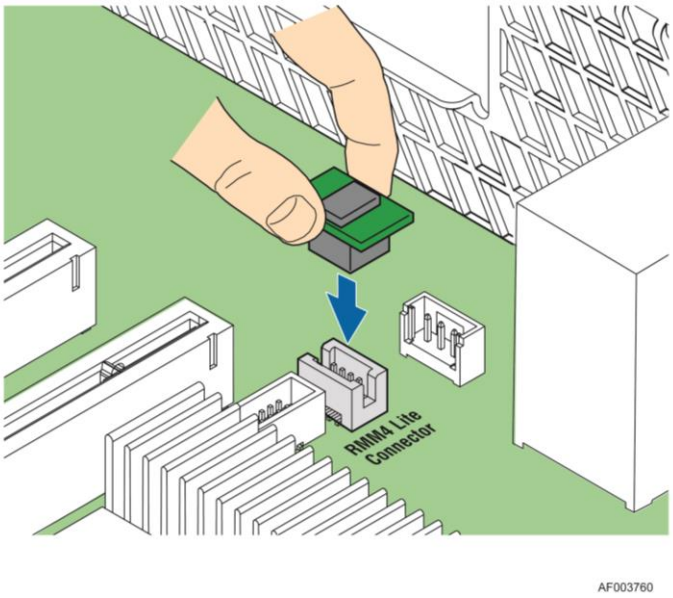


Figure 2. Installing Intel® RMM4 Lite module on Intel® server board

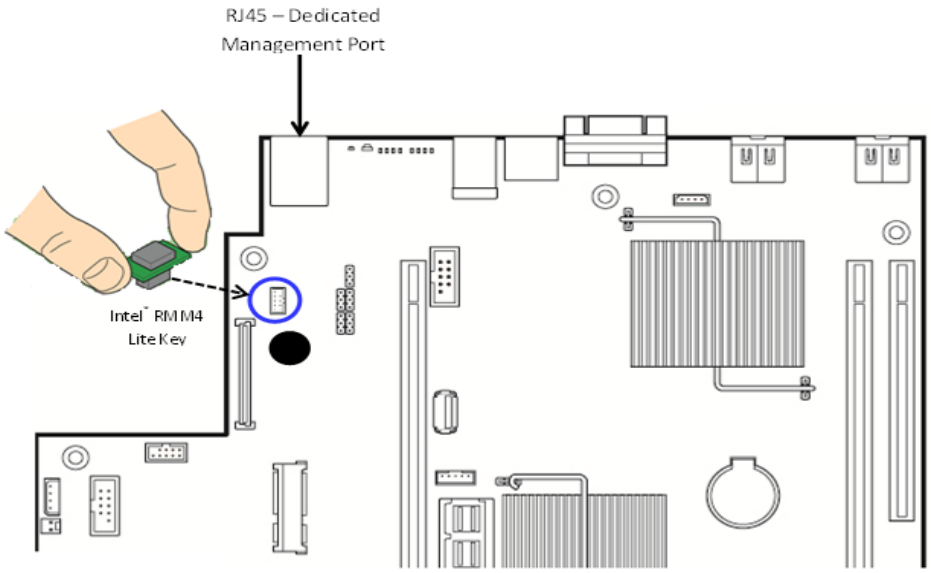


Figure 3. Intel® Server Board S2600WF – Intel® RMM4 Lite connector and Intel® Dedicated Server Management NIC location

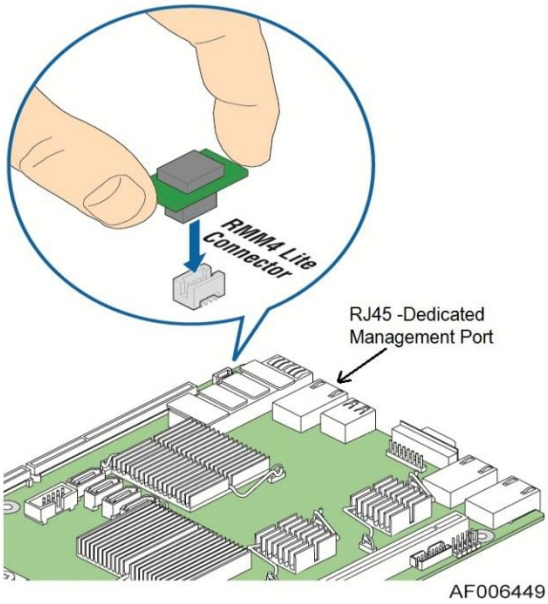


Figure 4. Intel® Server Board S2600BP – Intel® RMM4 Lite connector and Intel® Dedicated Server Management NIC location

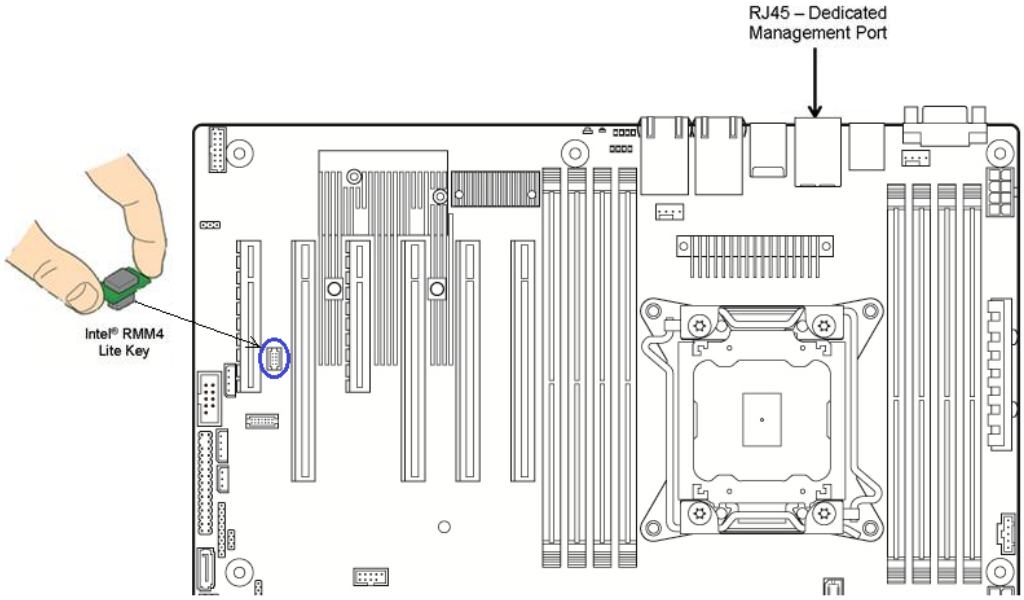


Figure 5. Intel® Server Board S2600ST – Intel® RMM4 Lite connector and Intel® Dedicated Server Management NIC location

3.2 Intel® Dedicated Server Management NIC

For Intel Server Board S2600WF, S2600BP, and S2600ST 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, and Figure 5.

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 6).
3. For an IPv4 network:
    - If configuring the server management BMC LAN, scroll to **Baseboard LAN configuration** > **IP source** and then select either **Static** or **Dynamic**. If **Static** is selected, configure the **IP address**, **Subnet mask**, and **Gateway IP** as needed.
    - If configuring the 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.
4. For an IPv6 network:
    - If configuring the server management BMC LAN, scroll to **Baseboard LAN IPv6 configuration** > **IP source** and then select **Enabled**. Then scroll to **IPV6 source** and select either **Static** or **Dynamic**. If **Static** is selected, configure the **IPV6 address**, **Gateway IPV6**, and **IPV6 Prefix Length** as needed.
    - 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.
5. Select **User Configuration** to enter the User Configuration screen (Figure 7).
6. Under **User ID**, set the following settings as desired:
    - **Privilege** – Select the privilege to be used. (Administrator privilege is required to use KVM or media redirection enabled by the 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.
7. Press **<F10>** to save the configured settings and exit BIOS setup. The server reboots with the new LAN settings.

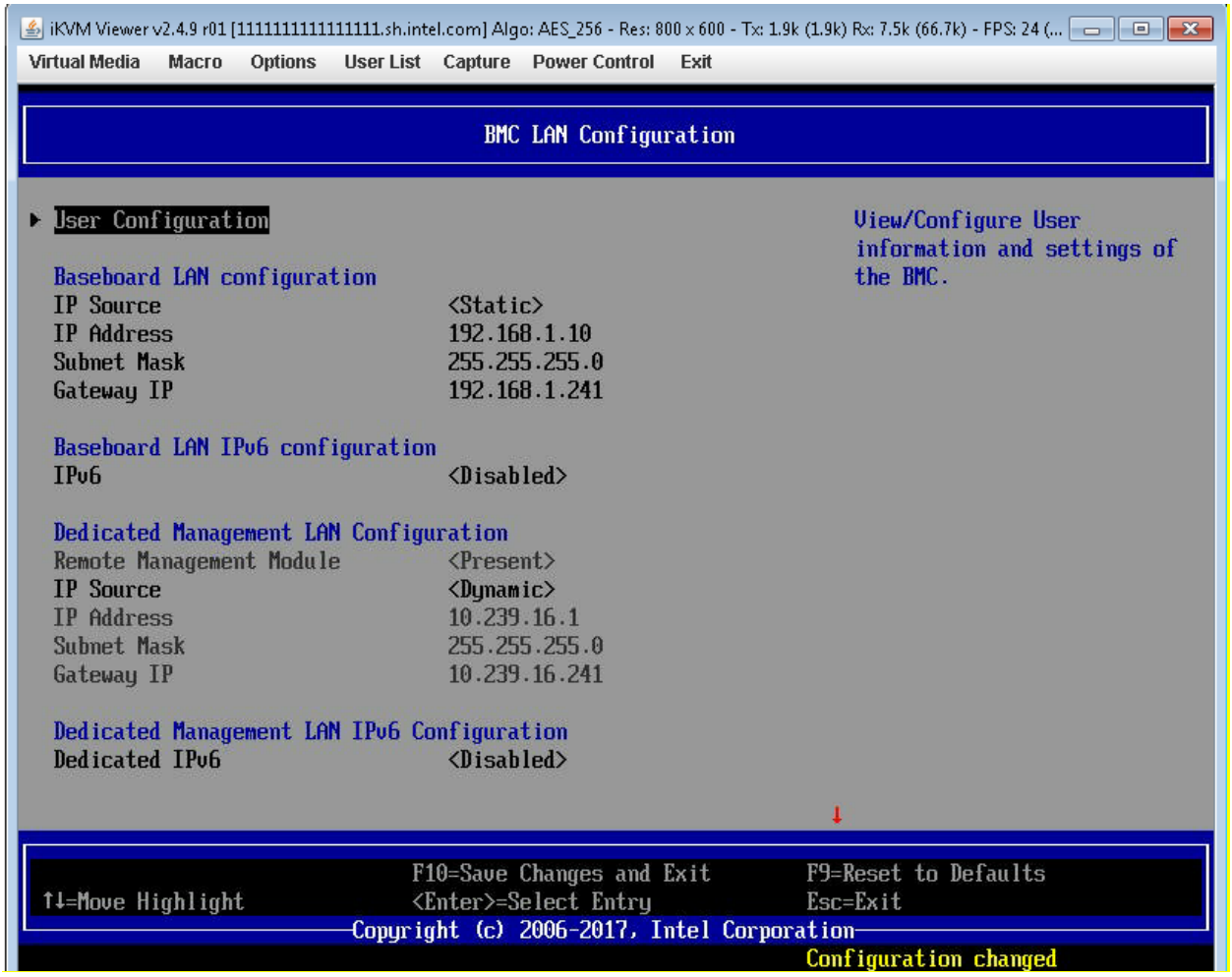


Figure 6. BIOS setup BMC LAN Configuration screen

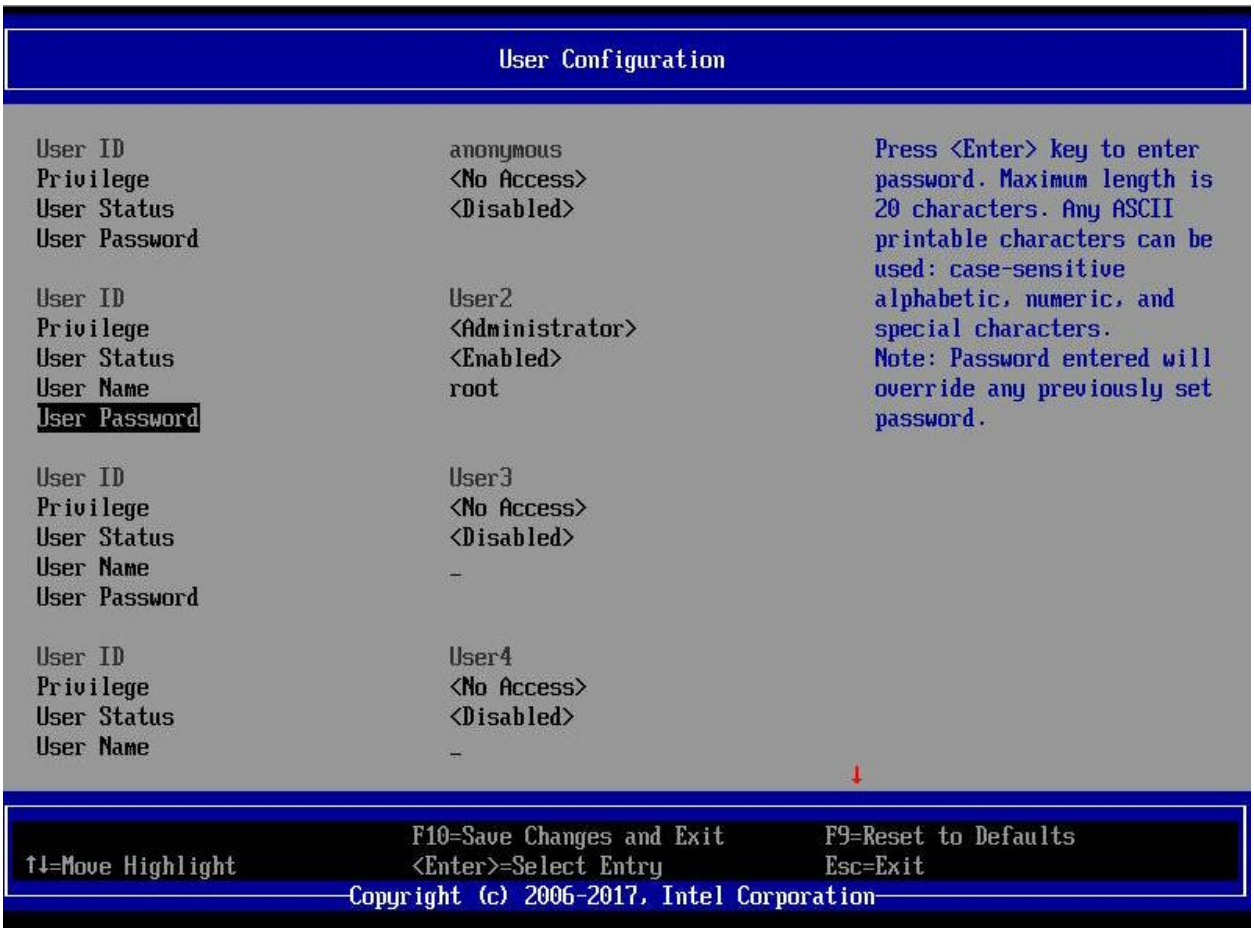


Figure 7. BIOS setup User Configuration screen

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 Sections 6 and 7, respectively.

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

5.1 Client Browsers

The 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 web page.

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 8). 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.

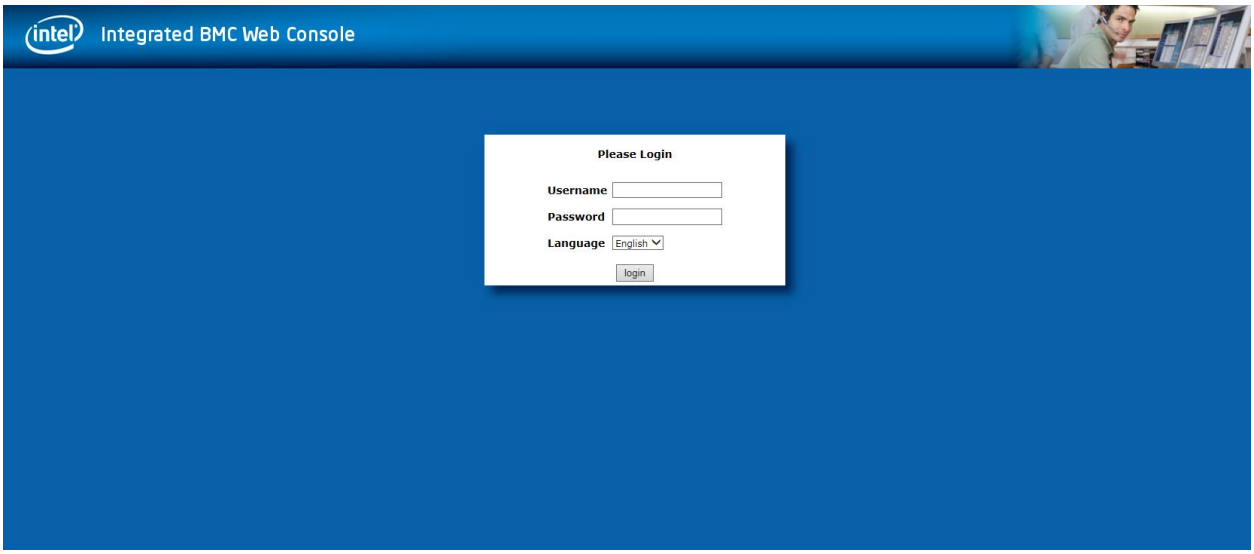


Figure 8. Integrated BMC web console login page

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 six tabs along the top for navigation within the web console (Figure 9). 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.

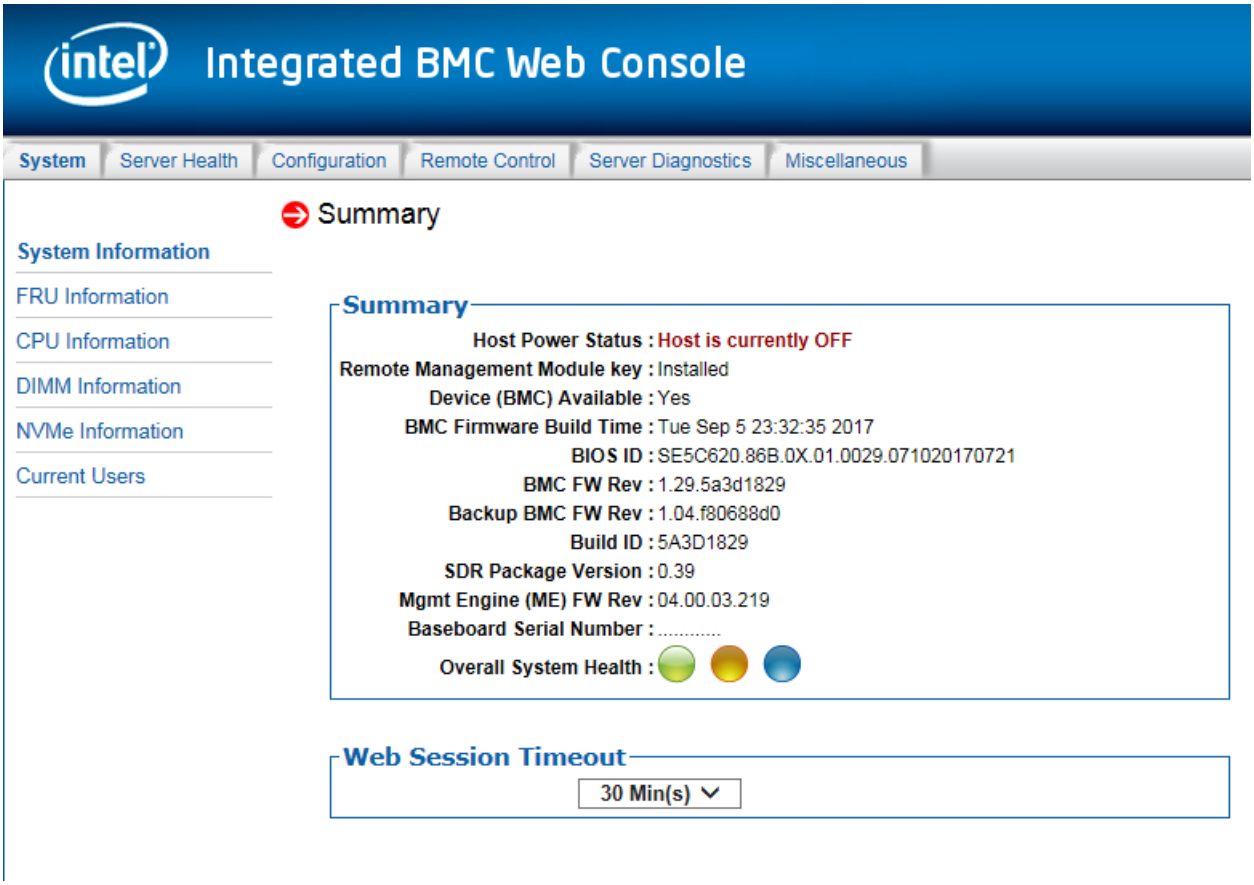


Figure 9. Integrated BMC web console home page

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.	• System Information • FRU Information • CPU Information • DIMM Information • NVMe Information • Current Users
Server Health	Provides access to the sensors and event log. The tab automatically opens the Sensor Readings page.	• Sensor Readings • Event Log
Configuration	Provides access to configure various settings for the server. The tab automatically opens the Alerts page.	• Alerts • Alert Email • IPv4 Network • IPv6 Network • VLAN • KVM & Media • SSL Certification • Users • Security Settings • SOL • SDR Configuration • Firmware Update
Remote Control	Provides access to the remote console and control of the server power state. The tab automatically opens the KVM/Console Redirection page.	• KVM/Console Redirection • Server Power Control • Launch SOL • Virtual Front Panel
Server Diagnostics	Provides access to server diagnostics information. The tab automatically opens the System Diagnostics page.	• System Diagnostics • POST Codes • System Defaults • SOL Log
Miscellaneous	Provides access to node manager configuration, power statistics and power telemetry. The tab automatically opens the NM Configuration page.	• NM Configuration • Power Statistics • Power Telemetry

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

Table 3. Integrated BMC web console toolbar

Button	Function
Logout	End the current web console session. Click **OK** to confirm (Figure 10). After logging out, the web console returns to the login screen.
Refresh	Refresh the current web page, 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 11). 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.

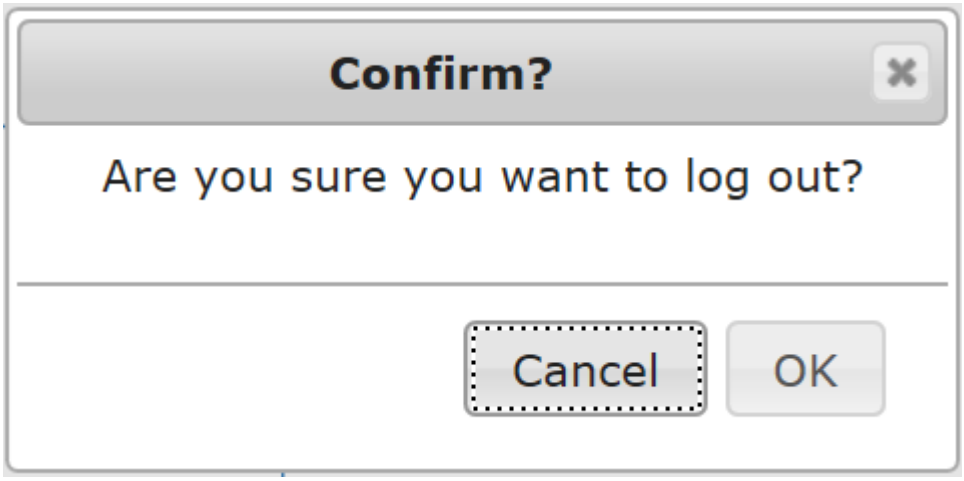


Figure 10. Logging out of the Integrated BMC web console

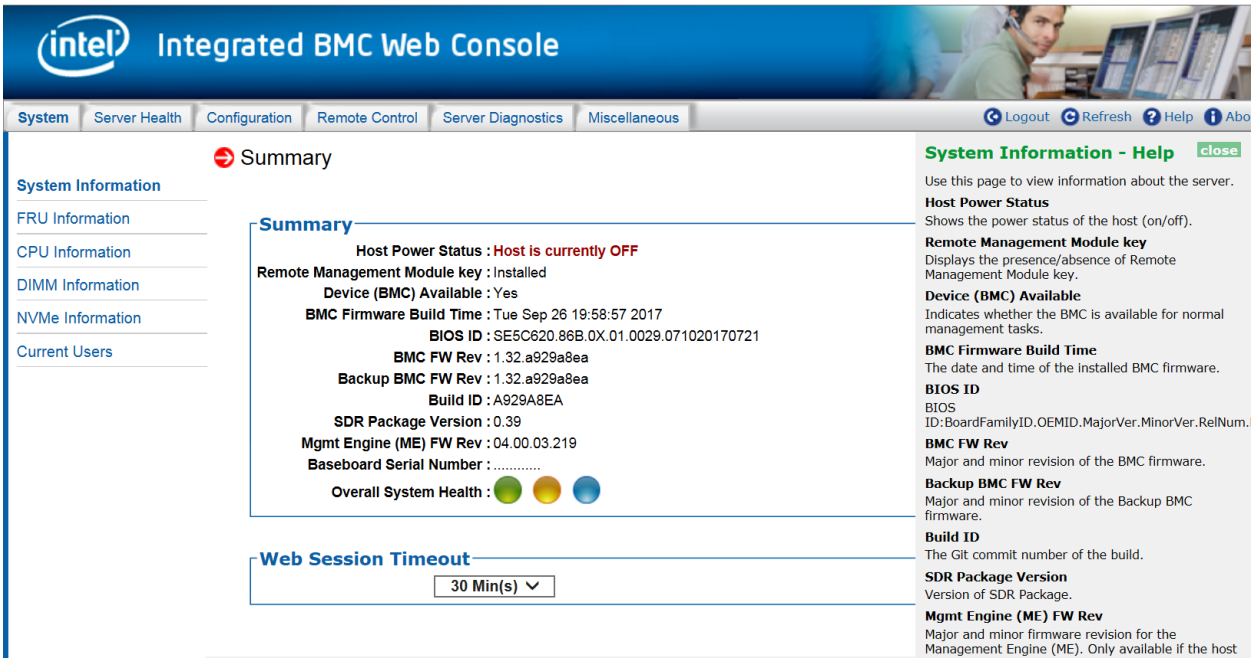


Figure 11. Integrated BMC web console help

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 12).

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

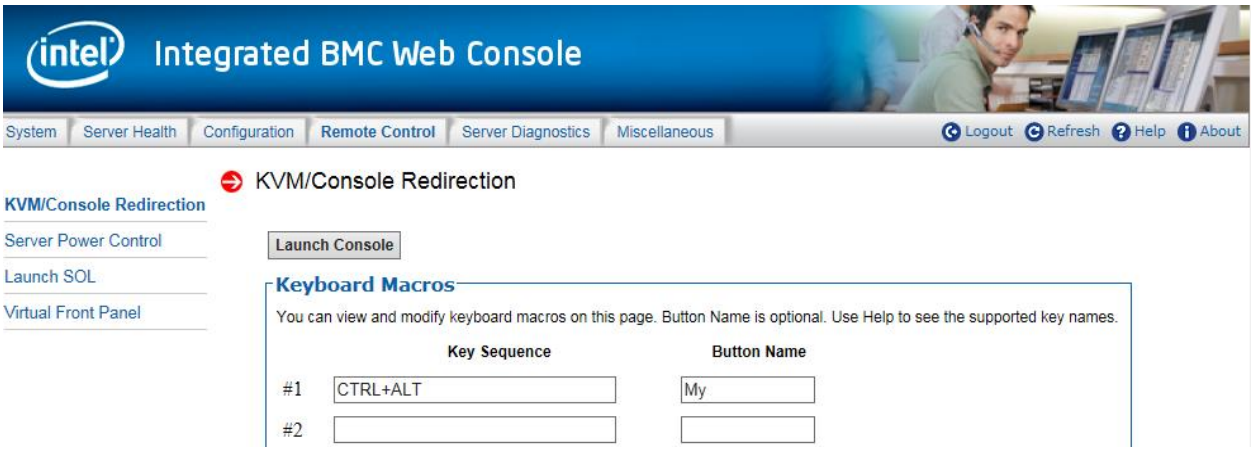


Figure 12. Remote control console redirection page

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

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

Notes:

- Java Runtime Environment* (JRE*, Version 6 Update 22 or higher) must be installed on the client before the launch of a `JNLP` file.
- The client browser must allow pop-up windows from the Integrated BMC web console IP address.
- JCE Unimited 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.

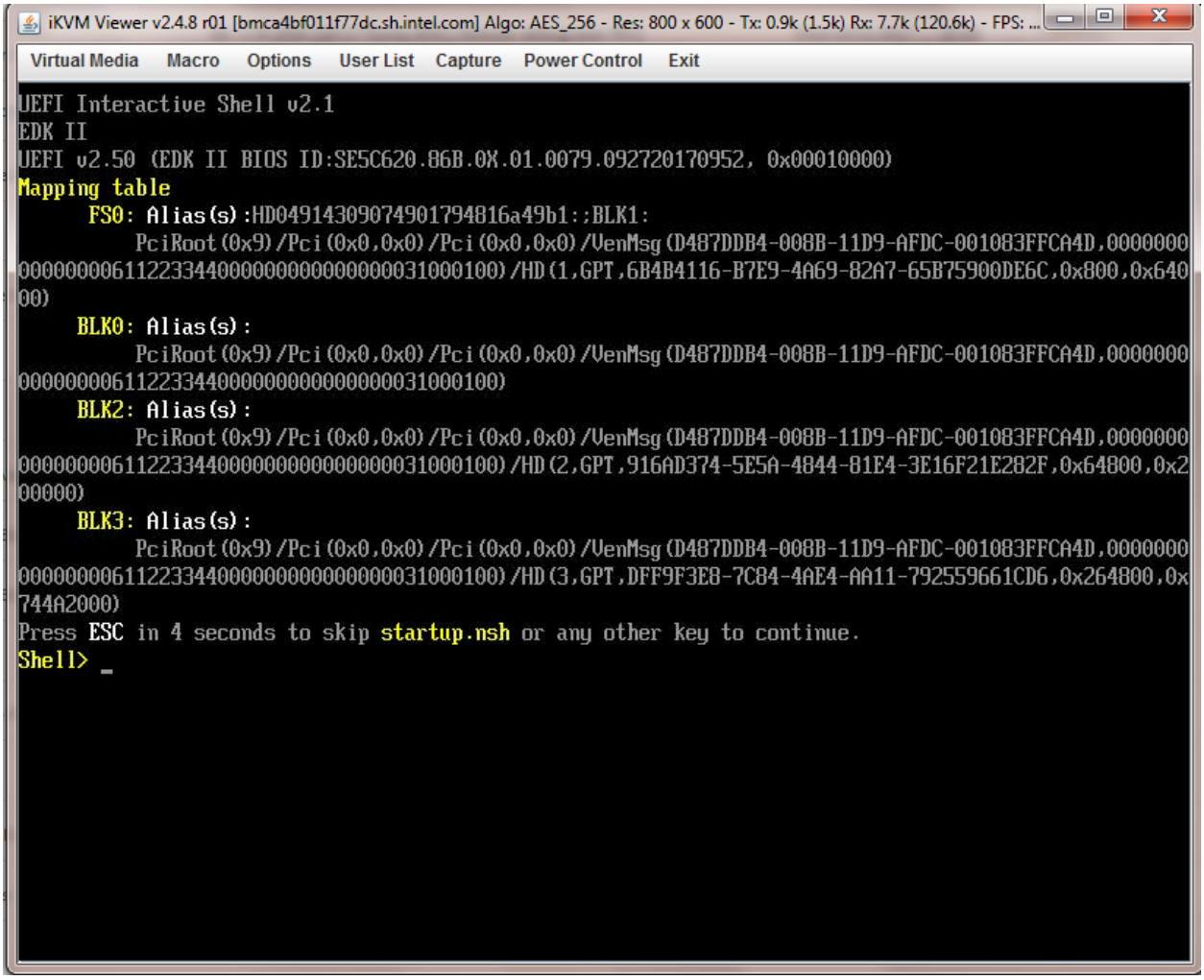


Figure 13. Remote console window

6.2 Main Window

Starting the remote console opens a host window (Linux* operating system window shown in Figure 14).

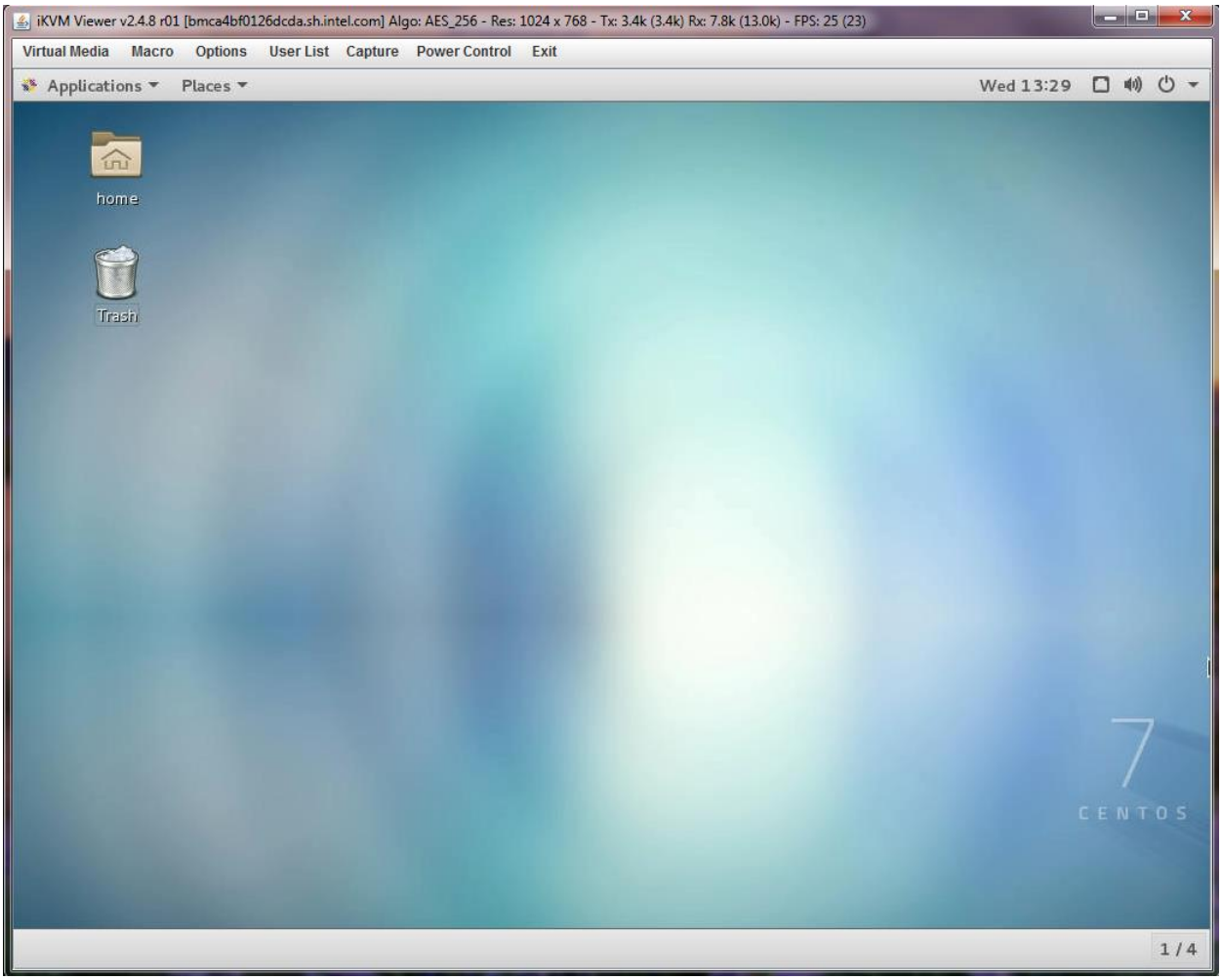


Figure 14. Remote console main window

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 15. 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 16.

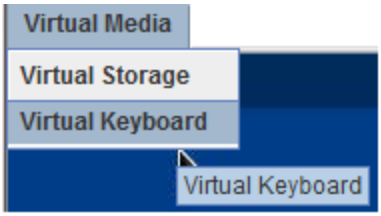


Figure 16. Remote console Virtual Media menu

Use the options in this menu to do the following:

- **Virtual Storage** – Allow starting/stopping remote media redirection as shown in Figure 17. Redirect up to four devices at the same time. Select a logical device from a local CDROM/DVD drive or an ISO image on the local client file system as a virtual CDROM device on the remote system; a local floppy drive; a USB key drive; or a floppy disk or USB key image (`.IMA`/`.IMG`) file on the local client file system as a virtual floppy device on the remote system.

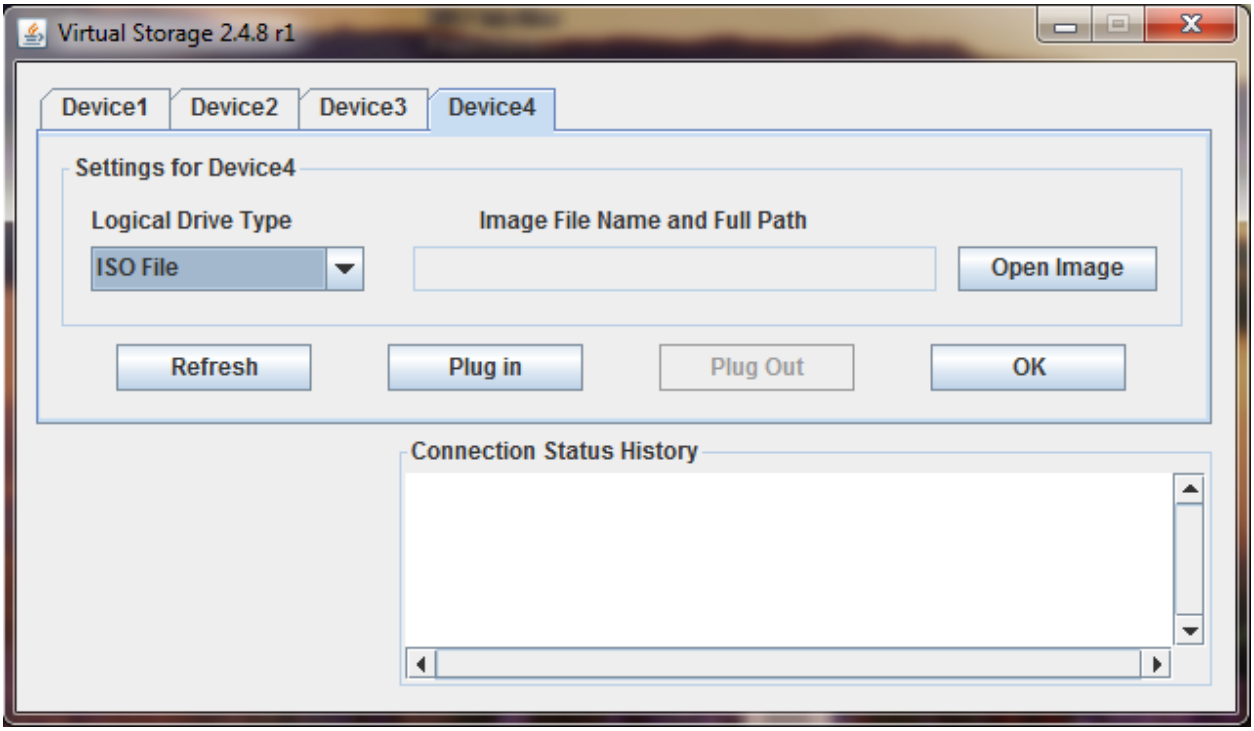


Figure 17. Remote console virtual storage menu

- **Virtual Keyboard –** Display a soft keyboard as shown in Figure 18.

Figure 18. Remote console virtual keyboard menu

6.3.2 Macro Menu

Click **Macro** to open the keyboard macro menu as shown in Figure 19.

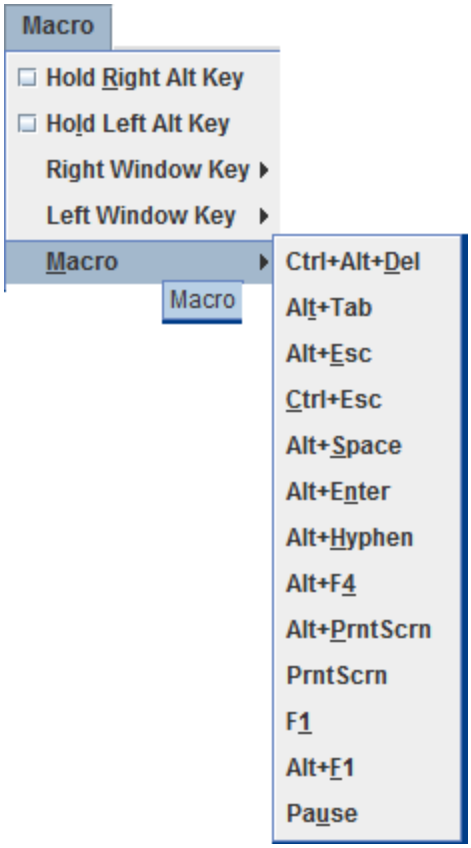


Figure 19: Remote console Macro menu

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 20.

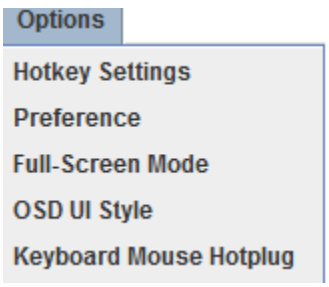


Figure 20. Remote console Options menu

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

- **HotKey Settings –** Configure hotkeys as shown in Figure 21. 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.

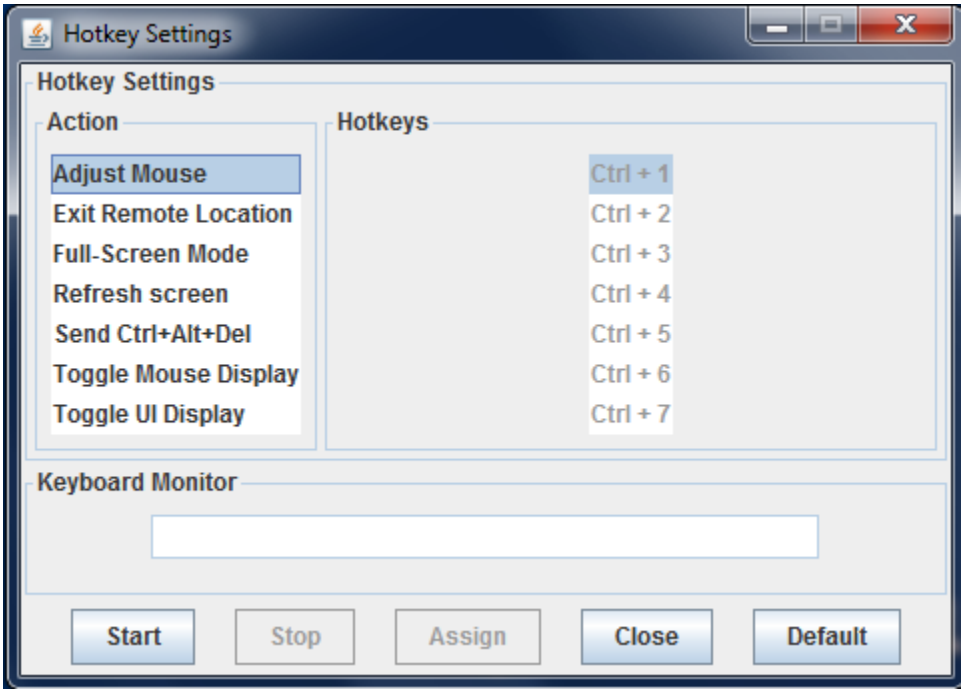


Figure 21. Remote console HotKey settings

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

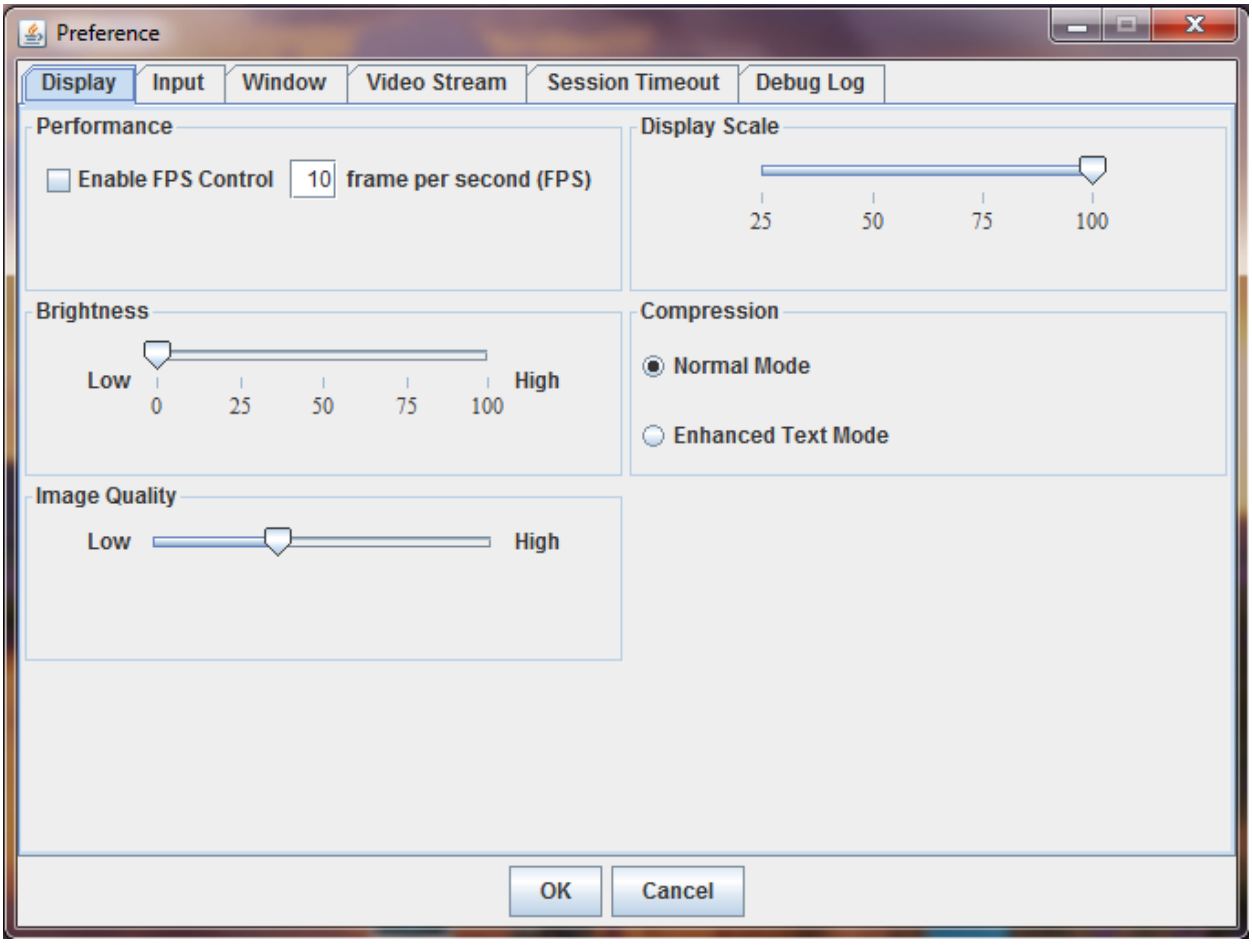


Figure 22. Remote console display settings

- **Input** (Figure 23) – Enable/disable mouse/keyboard input, change the mouse mode, specify keyboard layout, and set repeat key timeout.

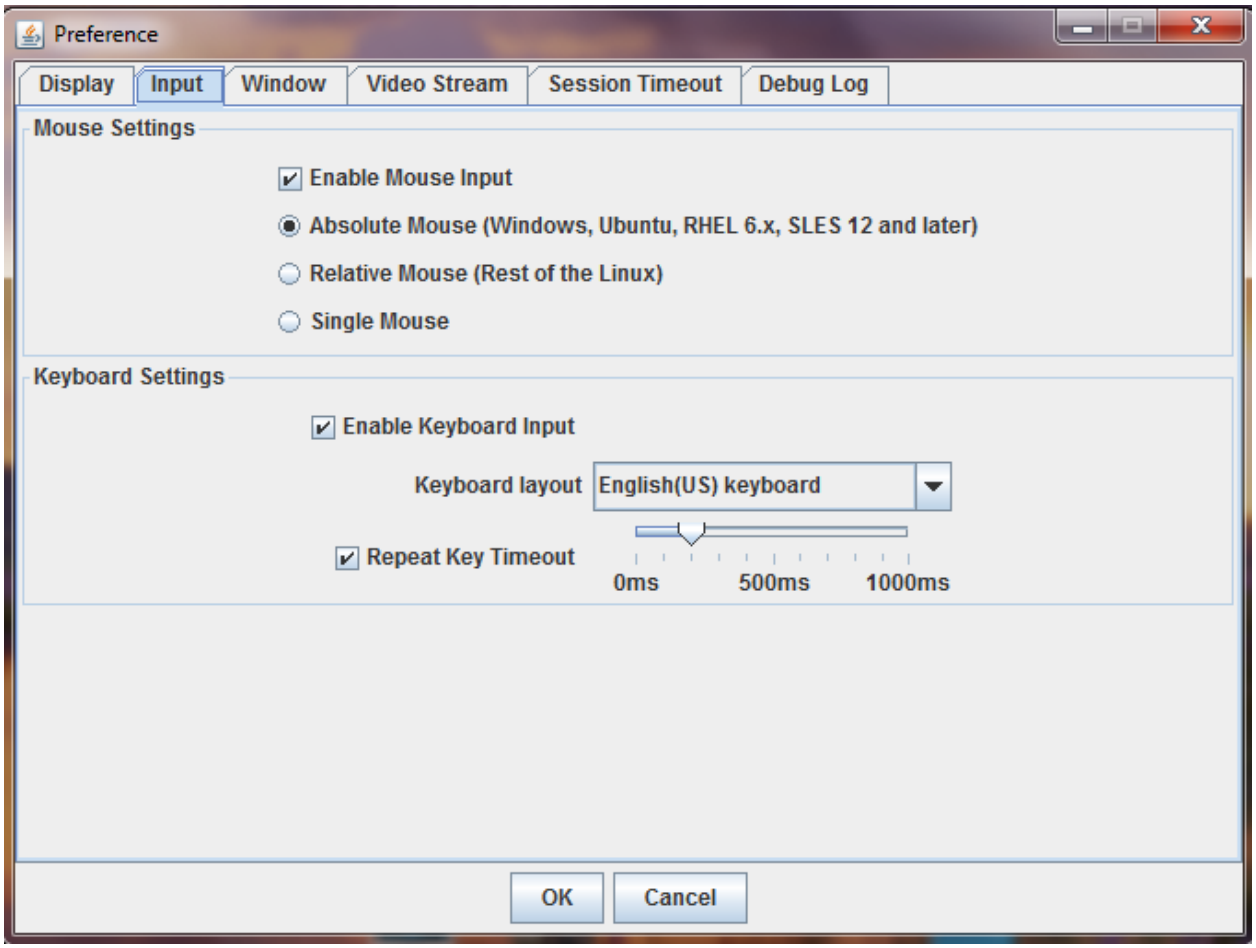


Figure 23. Remote console input settings

- **Window** (Figure 24) – Enable or disable window auto-resize.

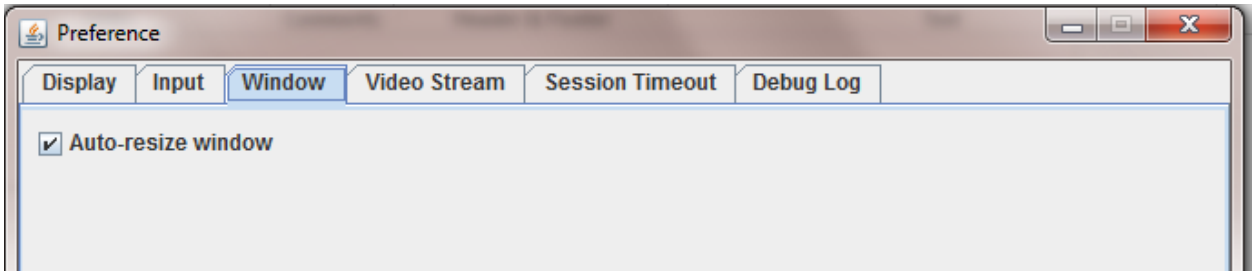


Figure 24. Remote console window settings

- **Video Stream** (Figure 25) – Enable flow control by specifying a speed of T1, T2, or 256K Cable/DSL.

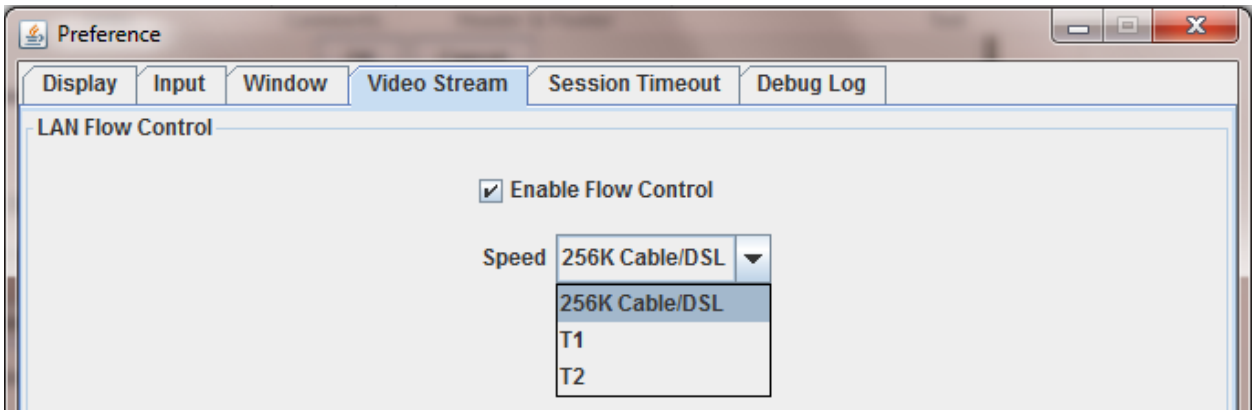


Figure 25. Remote console video stream settings

- **Session Timeout** (Figure 26) – Enable session timeout by specifying how many minutes for timeout.

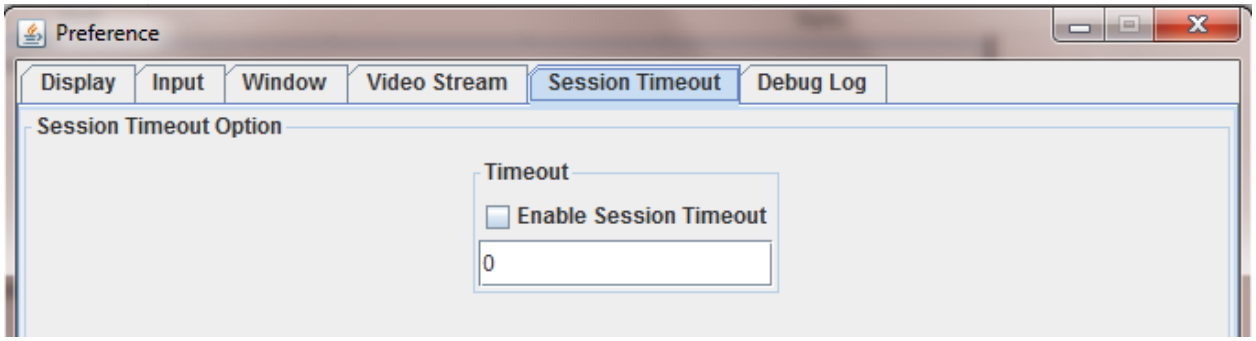


Figure 26. Remote console session timeout settings

- **Debug Log** (Figure 27) – 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.

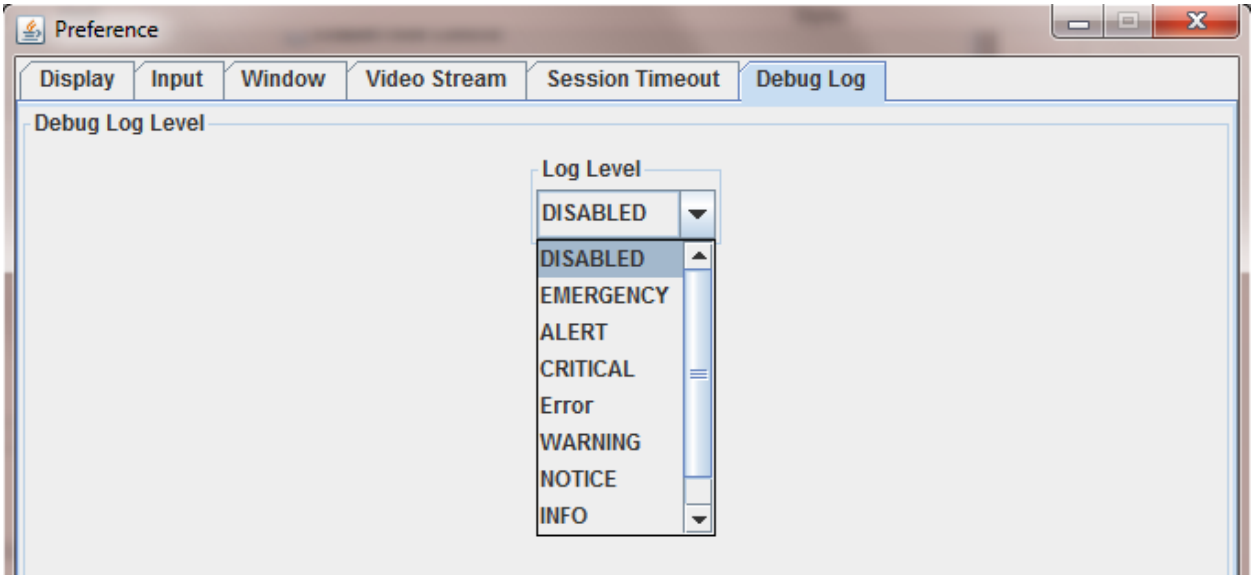


Figure 27. Remote console debug log settings

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

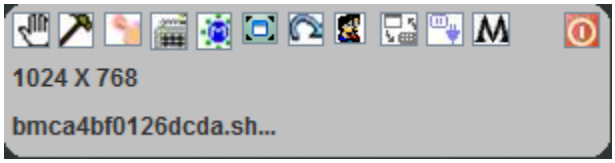


Figure 28. Remote console control panel – OSD UI style

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 29).

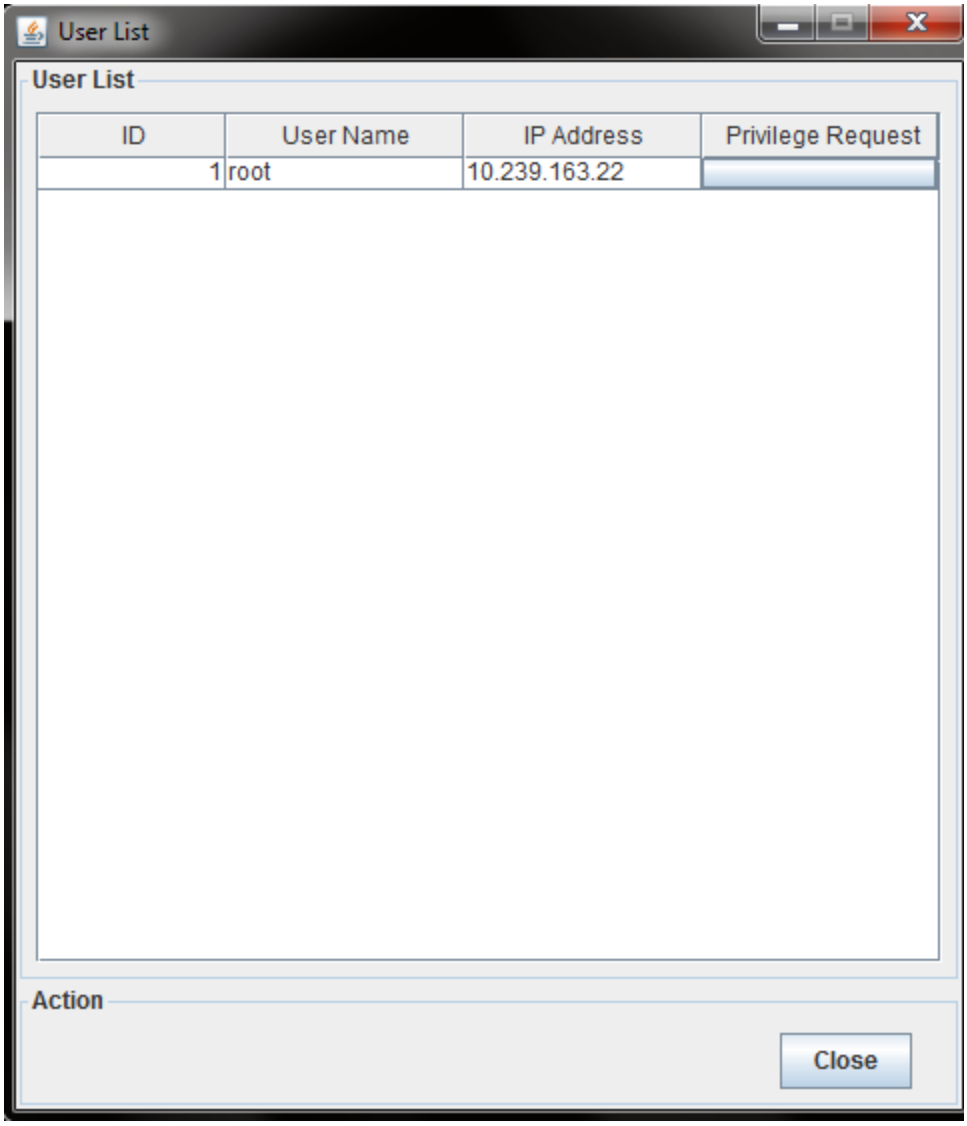


Figure 29. Remote console user list

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.

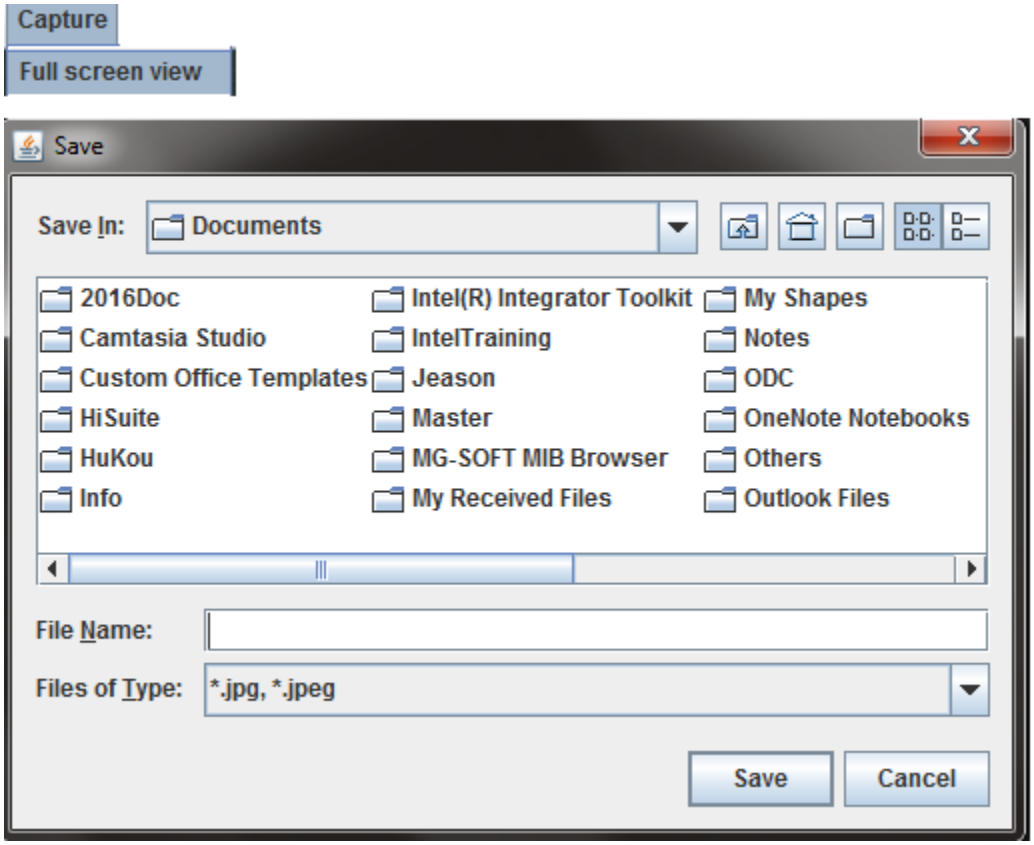


Figure 30. Remote console capture menu

6.3.6 Power Control Menu

Click **Power Control** to open the power control menu as shown in Figure 31.

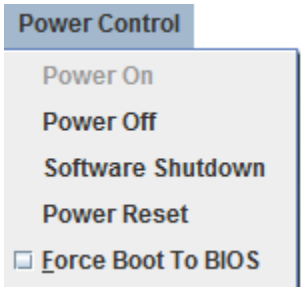


Figure 31. Remote console power control menu

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 32) to exit the remote console.

Figure 32. 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 **Error! eference source not found.**. The status line provides BMC host name, Java encryption, resolution, transaction speed and display frames per second.

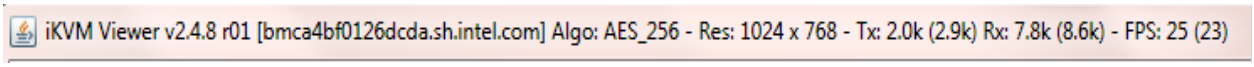


Figure 33. Remote console status line

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 34.

Figure 34. 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.

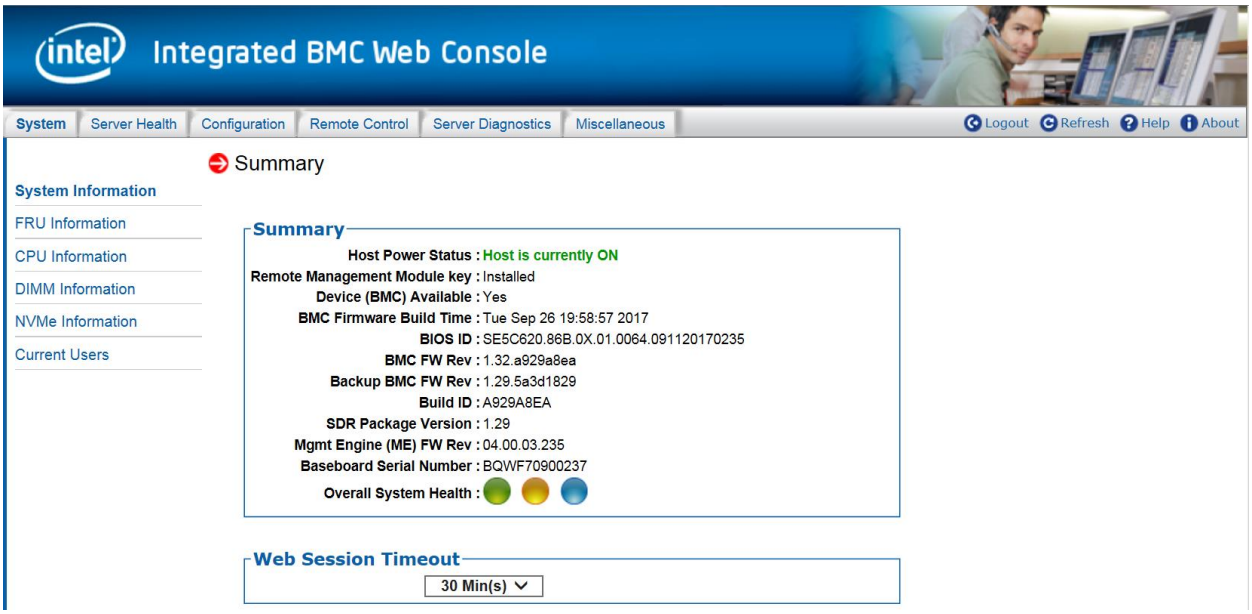


Figure 35. System Information page

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 heath: • 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 36).

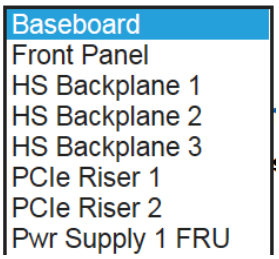


Figure 36. FRU board options

All data in the FRU information page is compliant with standard specifications (Platform Management FRU Information Storage Definition). See Figure 37 for details of the baseboard FRU.

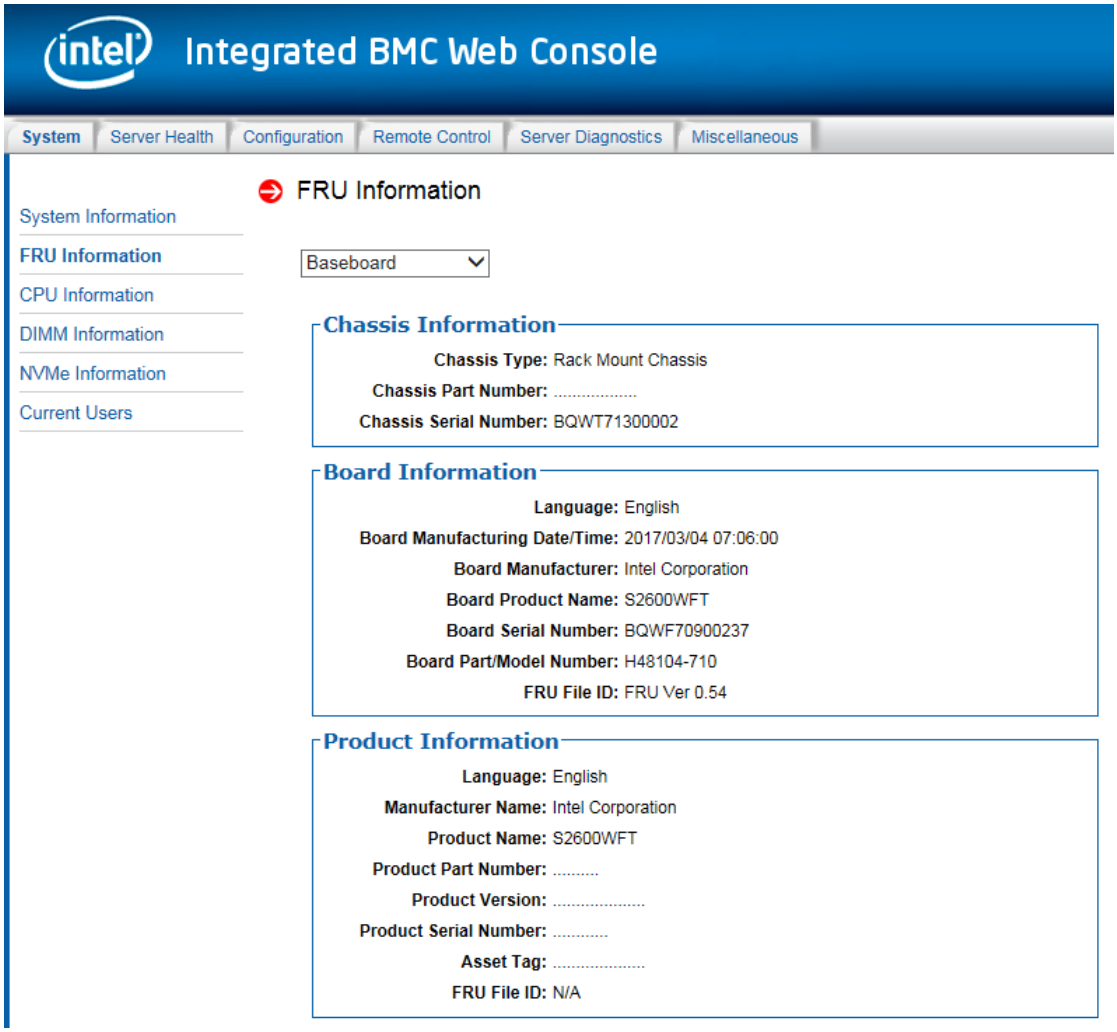


Figure 37. System FRU Information page

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 38Error! Reference source not found. for details.

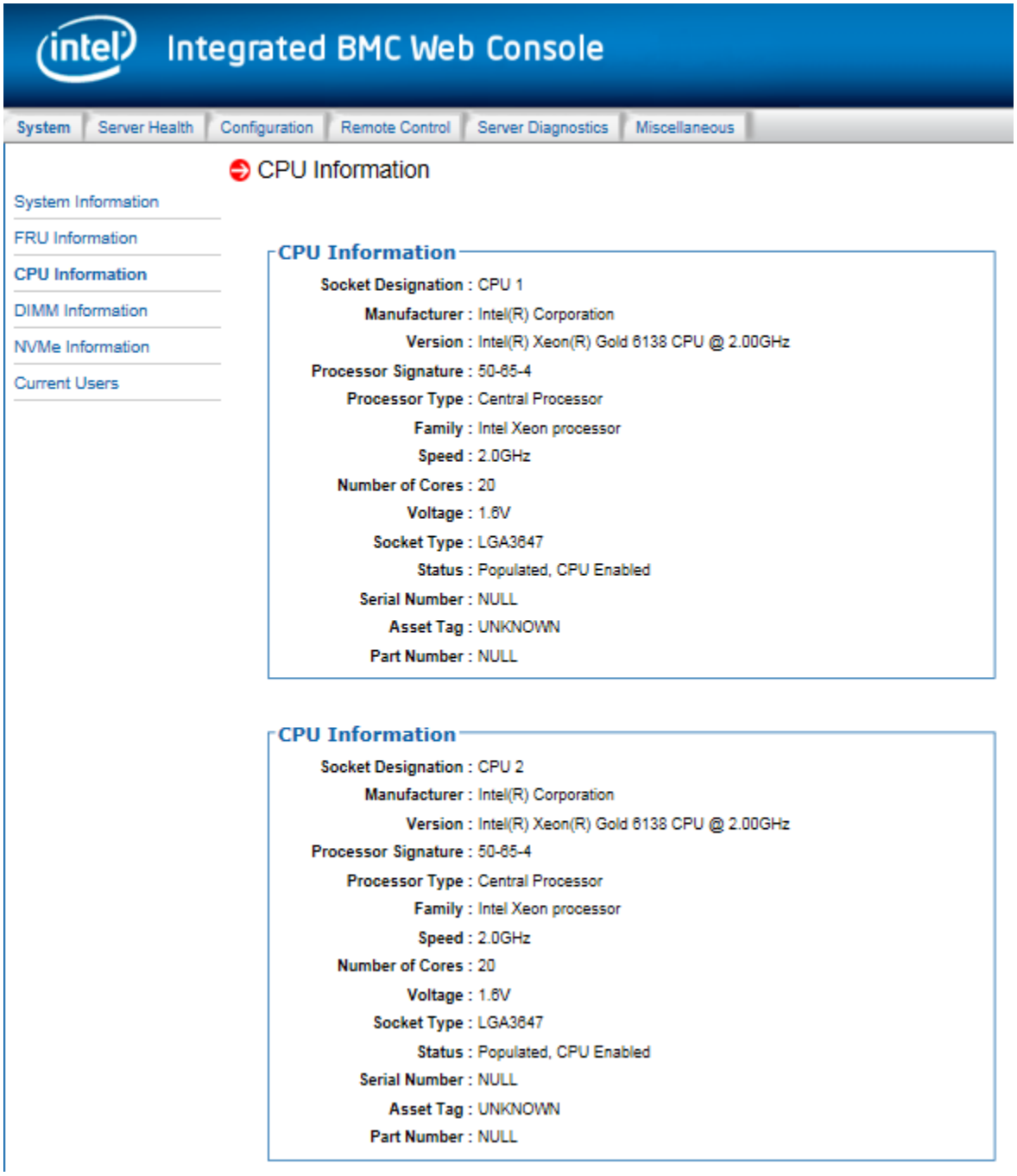


Figure 38. System CPU Information page

7.1.4 DIMM Information

The DIMM Information page displays information on DIMM modules installed in the host system. The DIMM information includes slot number, size, memory type, manufacturer, asset tag, memory serial/part number. See**Error! Reference source not found.** Figure 39 for details.

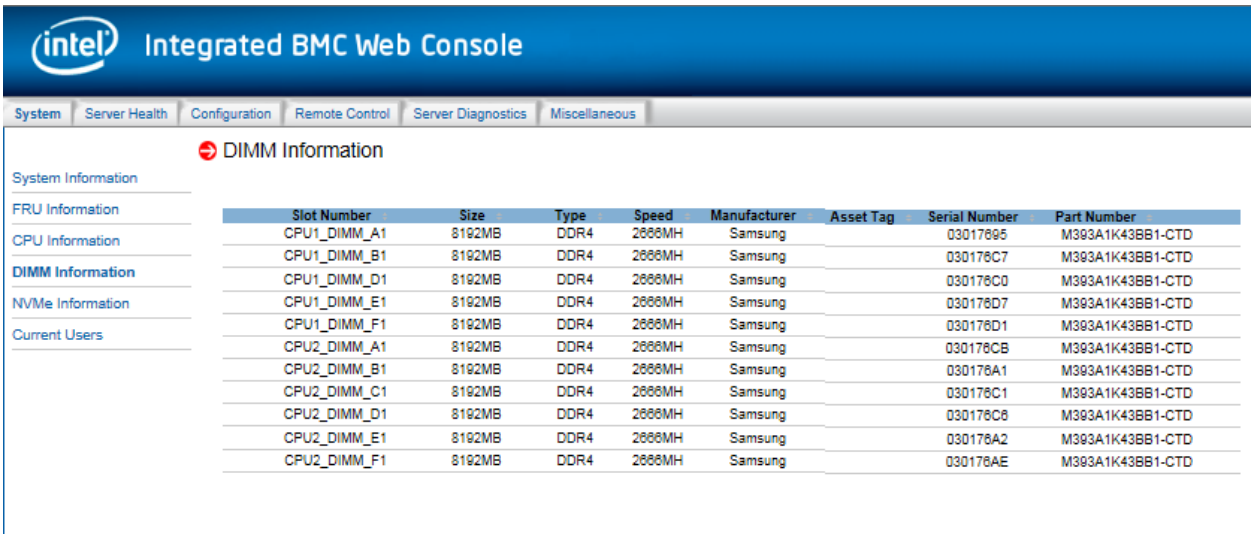


Figure 39. System DIMM Information page

7.1.5 NVMe* Information

The NVMe* Information page displays information on supported NVMe drives installed on the host system. See**Error! Reference source not found.** Figure 40 for details. Note that the BMC only displays information about NVMe drives that meet all of the support requirements.

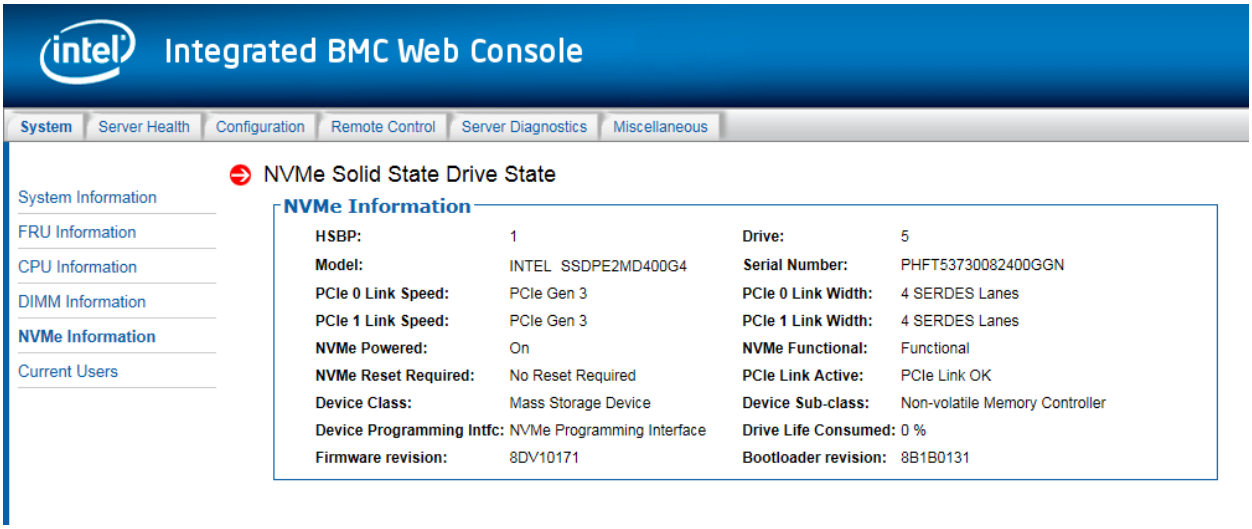


Figure 40. System NVMe* Information page

7.1.6 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 **Error! Reference source not found.**Figure 40 for details.

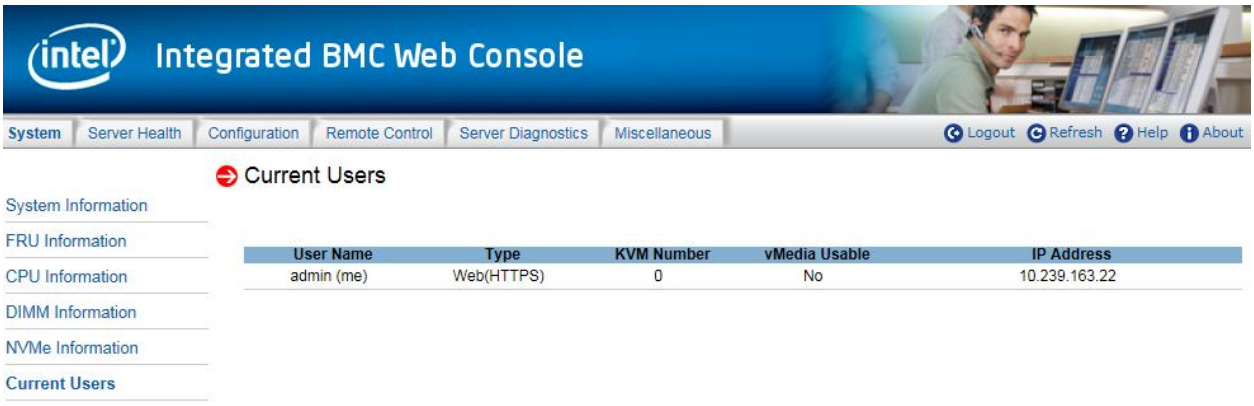


Figure 41. System Current Users page

7.2 Server Health Tab

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

7.2.1 Sensor Readings

The Sensor Readings page displays system sensor information including status, health, and reading as shown in

Figure 42 and Figure 43 (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.

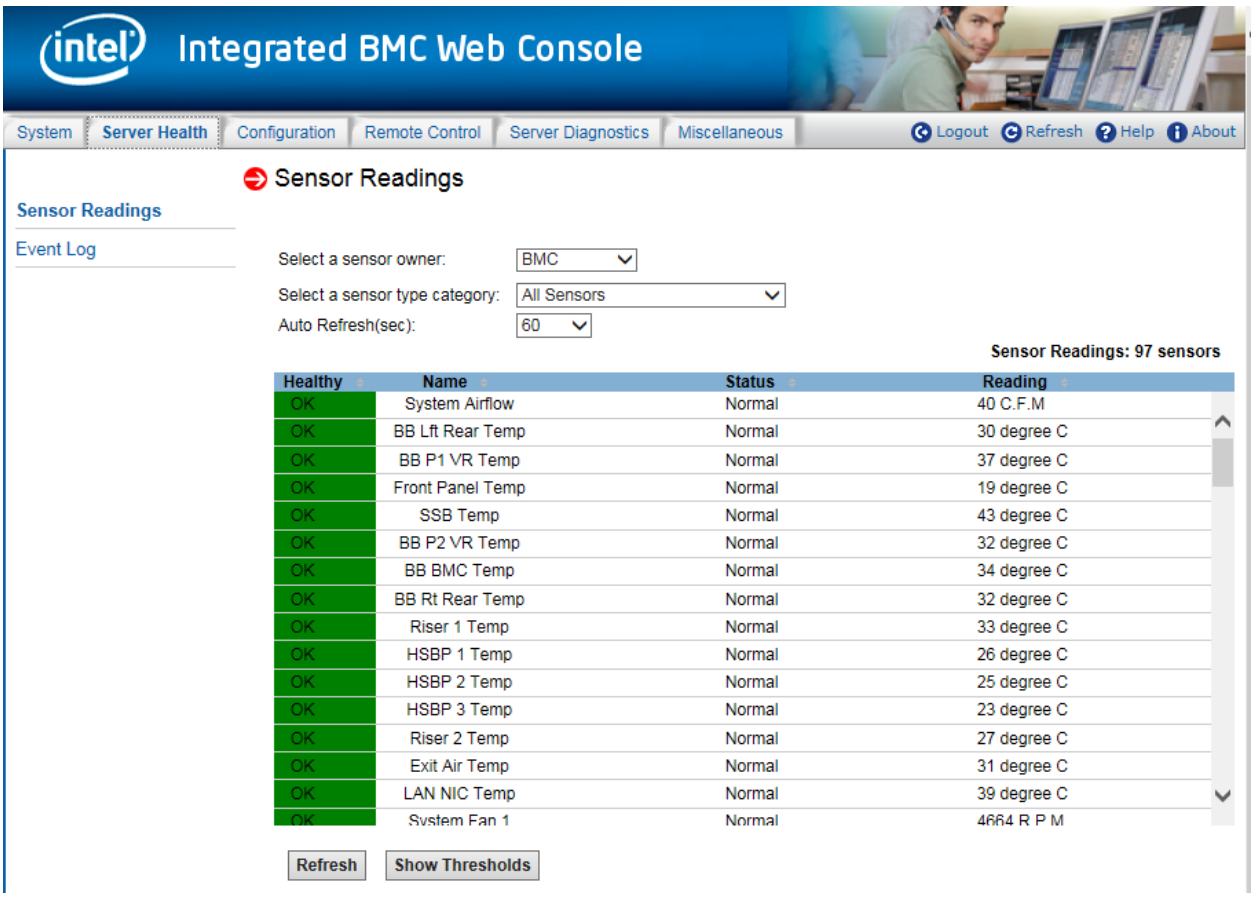


Figure 42. Server Health Sensor Readings page (thresholds not displayed)

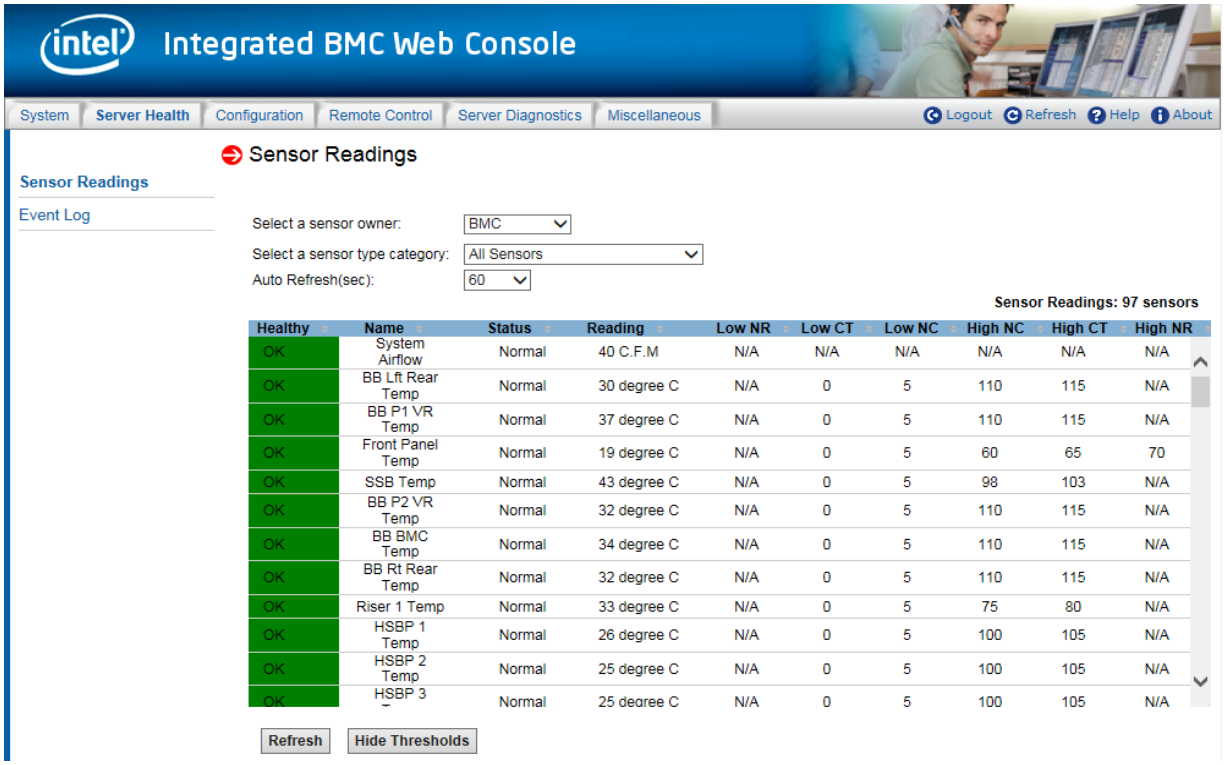


Figure 43. Server Health Sensor Readings page (thresholds displayed)

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 44). Table 9 lists the options available in this page.

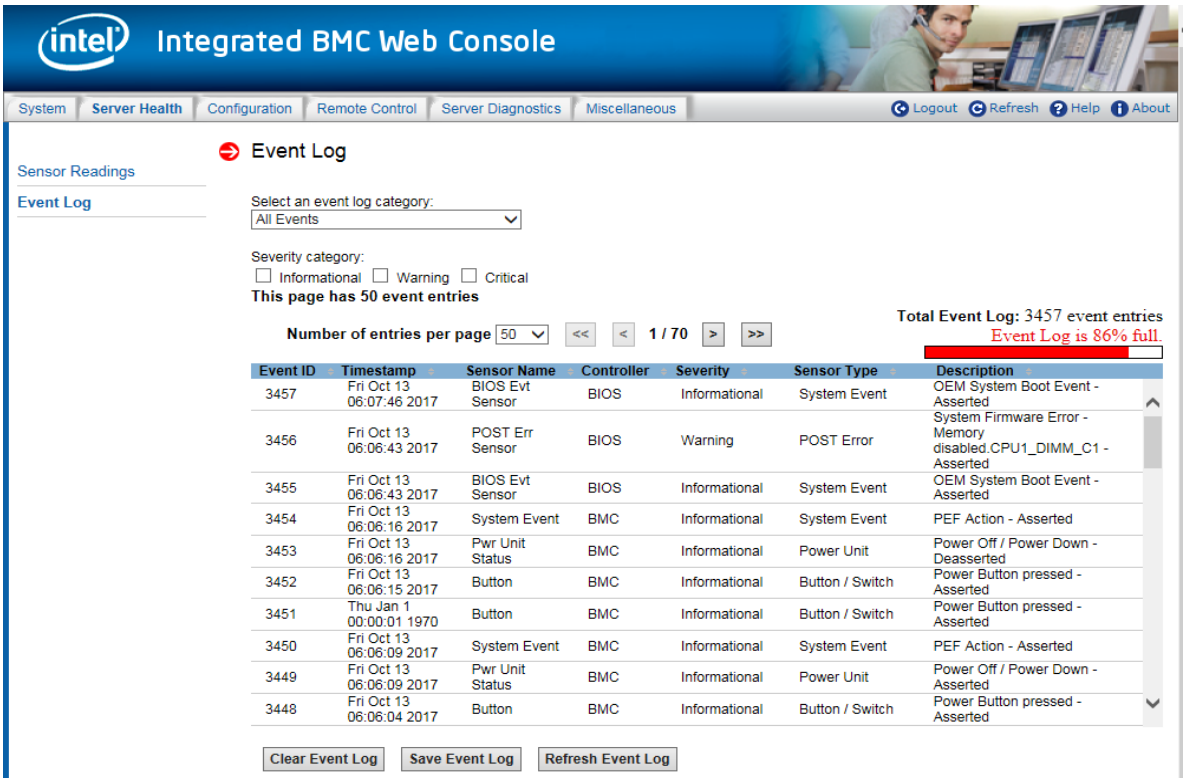


Figure 44. Server Health Event Log page

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 (**Error! Reference source not found.**Figure 45). Table 10 lists the options to select the events that should trigger alerts and where the alerts are to be sent.

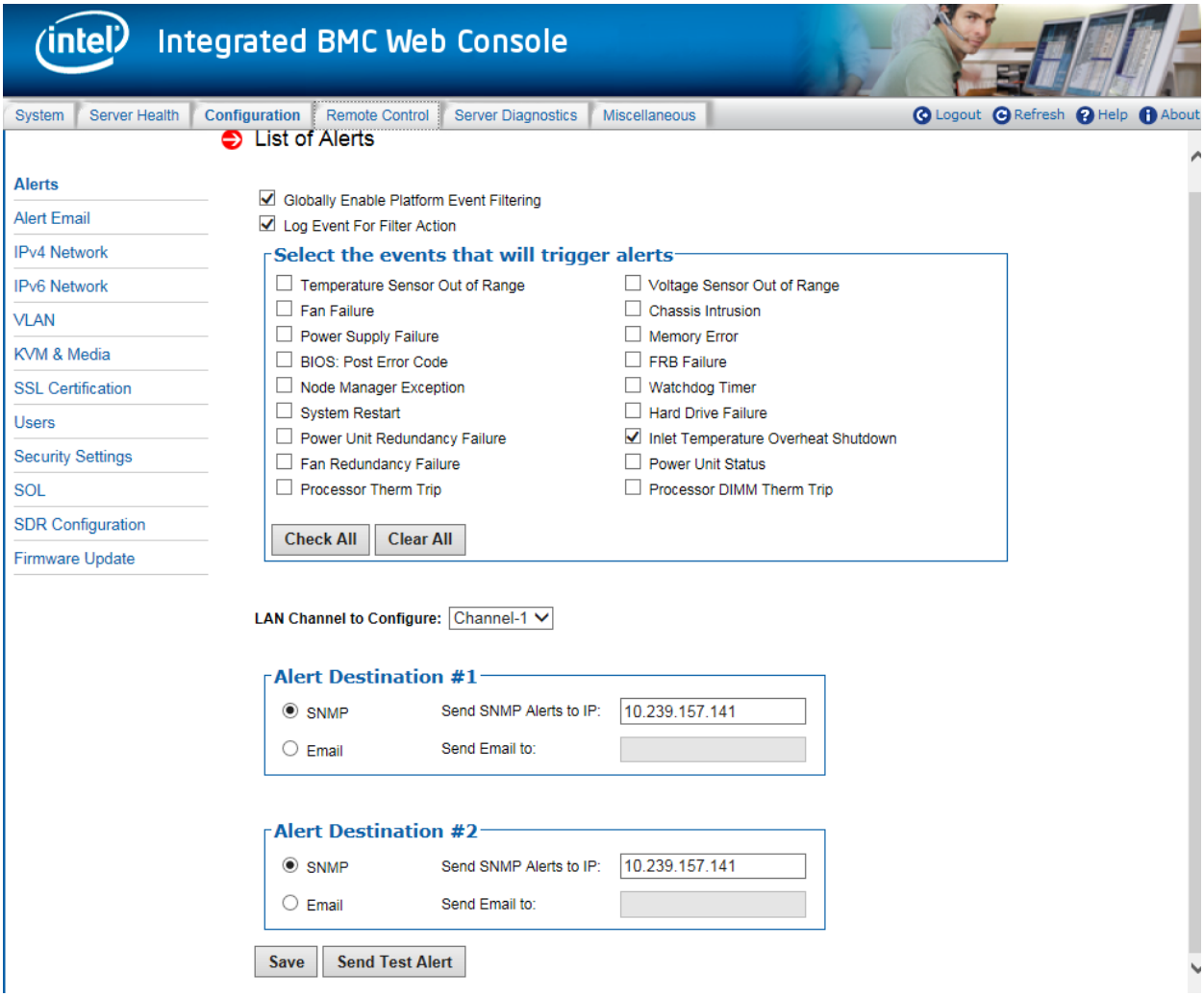


Figure 45. Configuration Alerts page

Table 10. Configuration Alerts options

Option	Task
Globally Enable Platform Event Filtering	This can be used to prevent sending alerts until you have fully specified your desired alerting policies.
Log Event For Filter Action	This can be used to enable or disable the logging of an event into the System Event Log when a Filter Action is taken.
Select the events that will trigger alerts	Select one or more system events that will trigger an alert.
Check/Clear All	Click to select or clear all events.
LAN Channel to Configure	Select either the BMC shared NIC (Channel-1, Channel-2) or RMM4 (Channel-3) to configure the destination.
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.

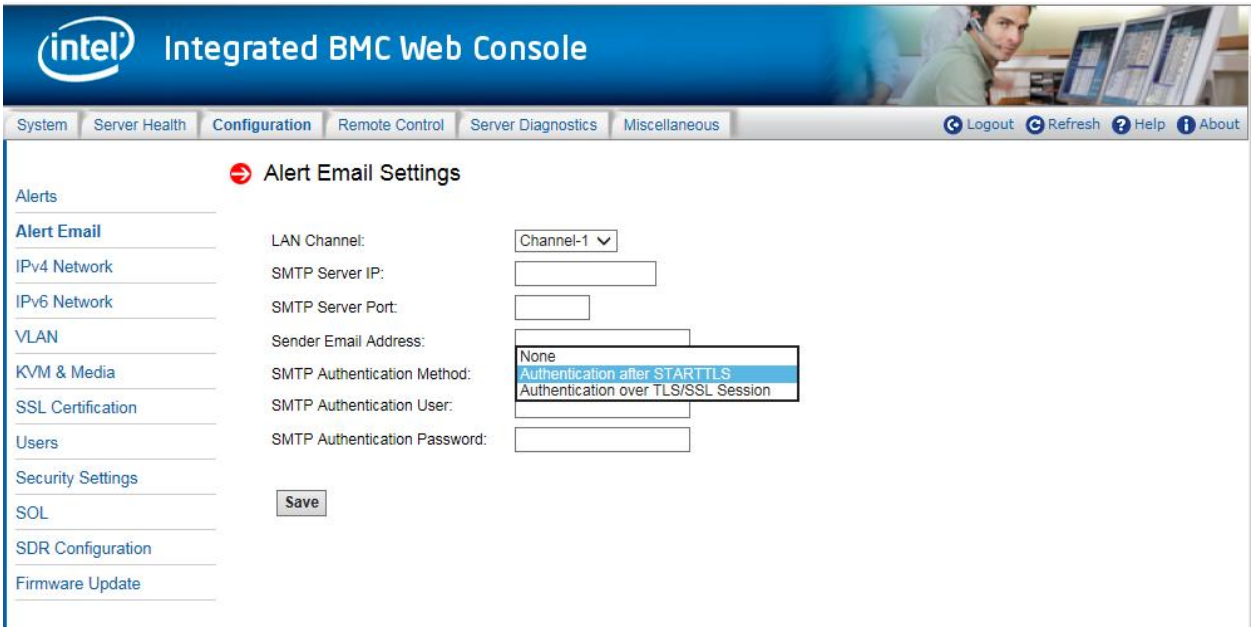


Figure 46. Configuration Alert Email page

Table 11. Configuration Alert Email options

Option	Task
LAN Channel	Select either the NIC (Channel-1, Channel-2) or RMM4 to configure the destination.
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: • 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 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 47 or Figure 48 for details. Table 12 lists the options available in this page.

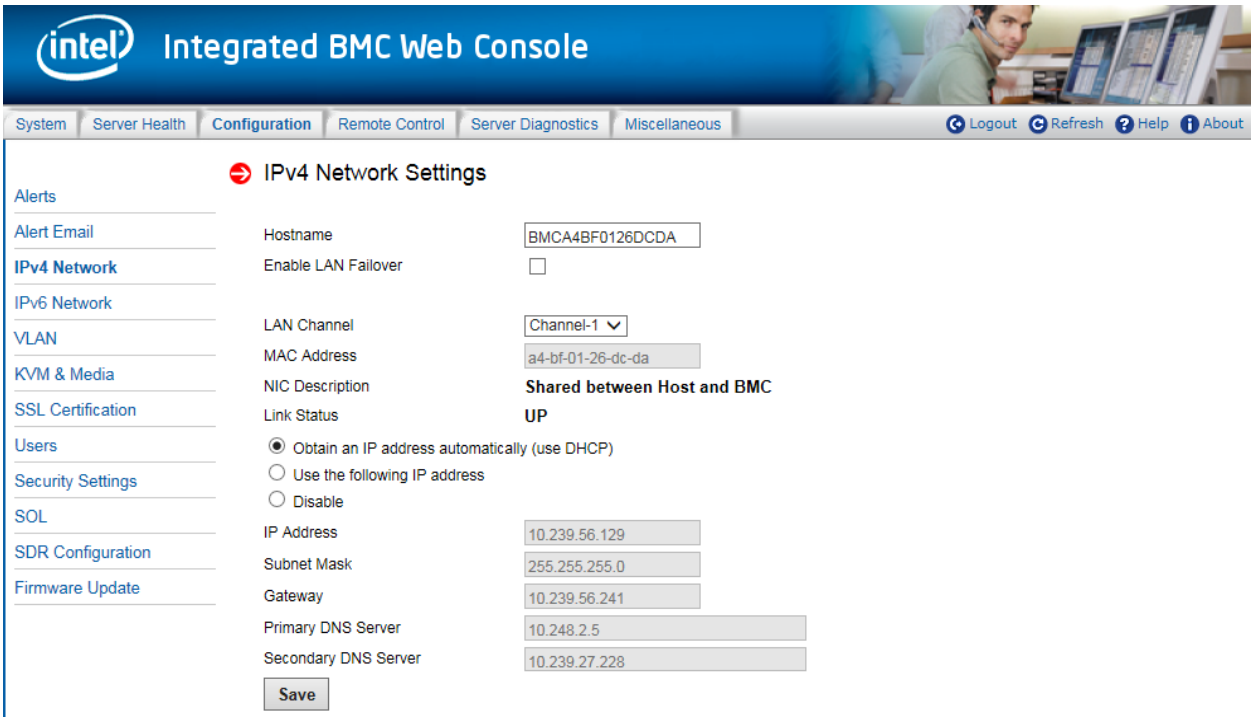


Figure 47. Configuration IPV4 Network DHCP page

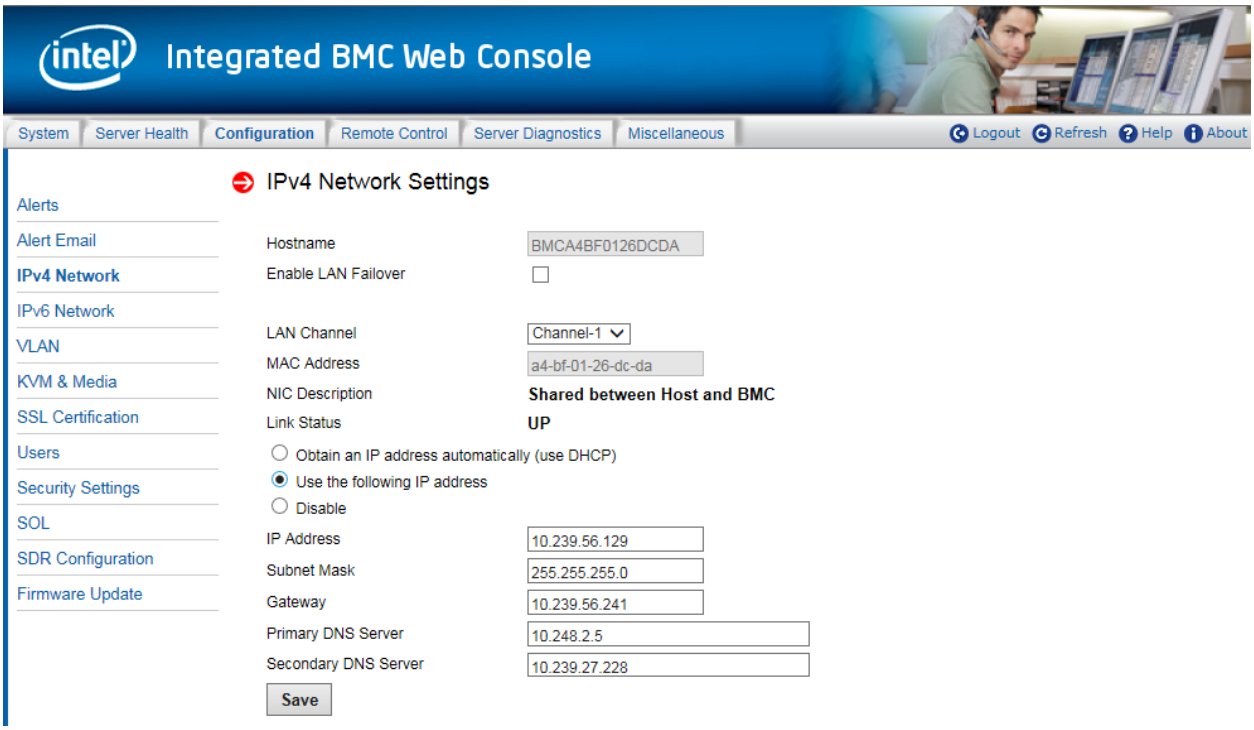


Figure 48. Configuration IPv4 Network static page

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

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

Table 12. Configuration IPv4 Network settings options

Option	Task
Host Name	The hostname is a RFC 1123 compliant string less than 64 alpha-numeric characters. Hyphen characters are allowed as long as the hyphen is not the first or final character in the hostname. The default value is "BMC" + MAC address.
Enable LAN Failover	Enabling failover bonds all available Ethernet interfaces into the first LAN Channel. When the primary interface's leash 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. • Intel(R) 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.
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: • 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.

7.3.4 IPv6 Network

The IPv6 settings page is used to enable and configure the IPv6 network settings and to enable and configure LAN failover (Figure 49)**Error! Reference source not found.**. Table 13 lists the options available in this page.

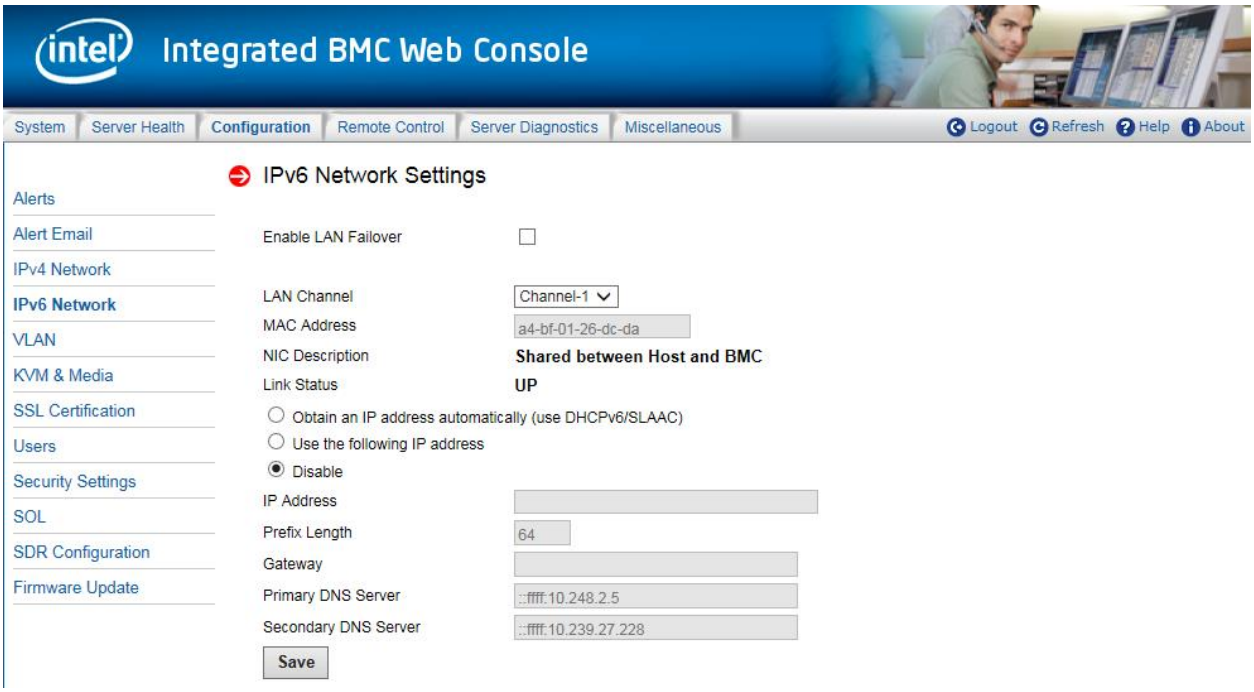


Figure 49. Configuration IPv6 Network page

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

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

Table 13. Configuration IPv6 Network settings options

Option	Task
Enable LAN Failover	Enable LAN failover.
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. Intel(R) RMM (BMC LAN Channel 3) is the add-in RMM4 Dedicated Management NIC. Baseboard Mgmt (BMC LAN Channel 1) is the on-board, shared NIC configured for management and shared with the operating system. Baseboard Mgmt 2 (BMC LAN Channel 2) is the second on-board, shared NIC configured for management and shared with the operating system.
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: Use IPv6 auto-configuration (stateless ICMPv6 discovery) – Uses ICMPv6 to obtain the IP address. Obtain an IP address automatically (use DHCPv6) – Uses DHCPv6 to obtain the IP address. Use the following IP address – Manually configure the IP address.
IP Address **Gateway**	If configuring a static IP, enter the requested address and gateway in the given fields. The IP Address and Gateway are 128-bit fields made of eight hexadecimal numbers separated by colons as in "xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx". 'xxxx' ranges from 0 to FFFF. First 'xxxx' must not be 0. One or more consecutive groups of zero value may be replaced with a single empty group using two consecutive colons (::).
Prefix Length	Select the routing prefix length.
Primary/Secondary DNS server	If configuring a static IP, enter the Primary and Secondary DNS servers.
Save	Click to save any changes made.

7.3.5 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 50). Table 14 lists the options available in this page.

Figure 50. Configuration VLAN settings page

Table 14. Configuration 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. • Intel(R) 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.

7.3.6 KVM & Media

Use this page to enable/disable encryption on KVM or media during a redirection session (Figure 51).**Error! Reference source not found.** Table 15 lists the options for enabling or disabling encryption on KVM or media data, and configuring the mouse mode setting during a redirection session.

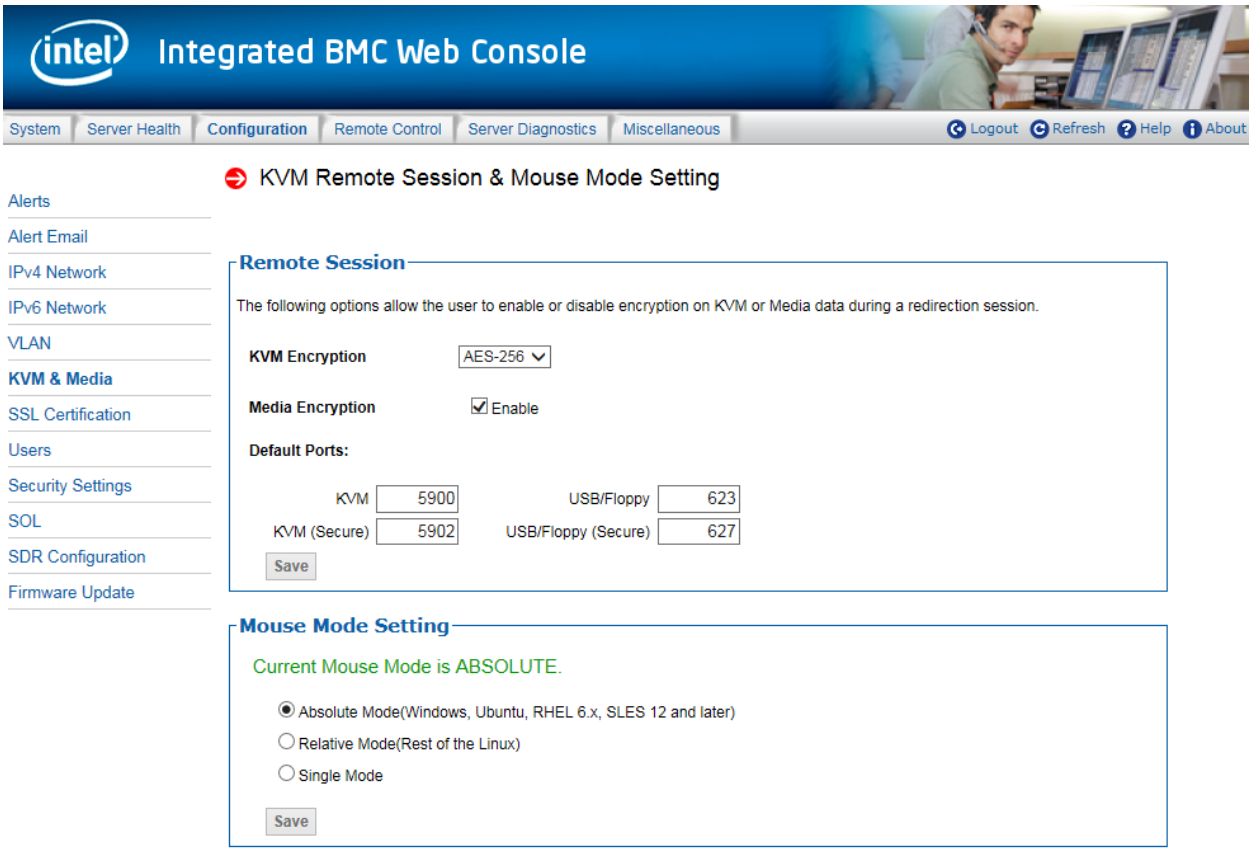


Figure 51. Configuration KVM & Media page

Table 15. Configuration 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.
Enable Encryption	Enable/disable encryption of Media data during a redirection session. Disabling encryption can improve performance of KVM or Media redirection.
Default Ports	Set the ports used by KVM and remote media (both standard and secure ports). Do not change these values unless you know the new ports are unused.
Save (Remote Session)	Click to save any changes for Remote Session.
Mouse Mode Setting	Redirection Console handles mouse emulation from local window to remote screen in one of the following methods: • 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.

7.3.7 SSL Certification

Use this page to upload an SSL certificate and private key, which allows the device to be accessed in a secured mode. See Figure 52 for details.

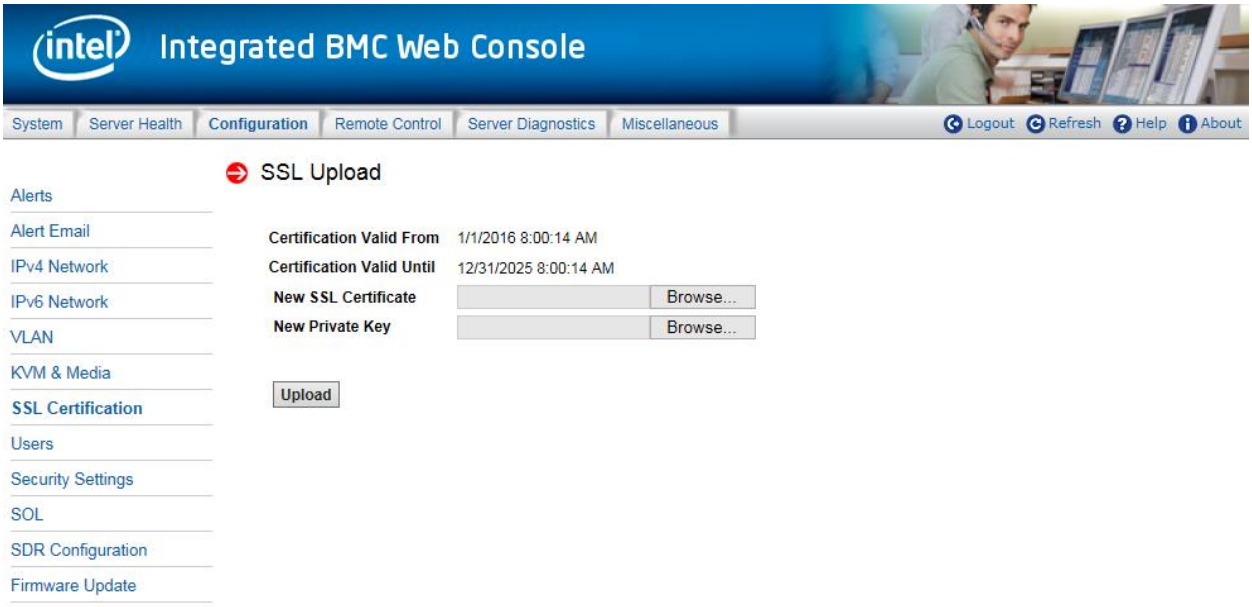


Figure 52. Configuration SSL Certification page

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.

7.3.8 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 53 for details.

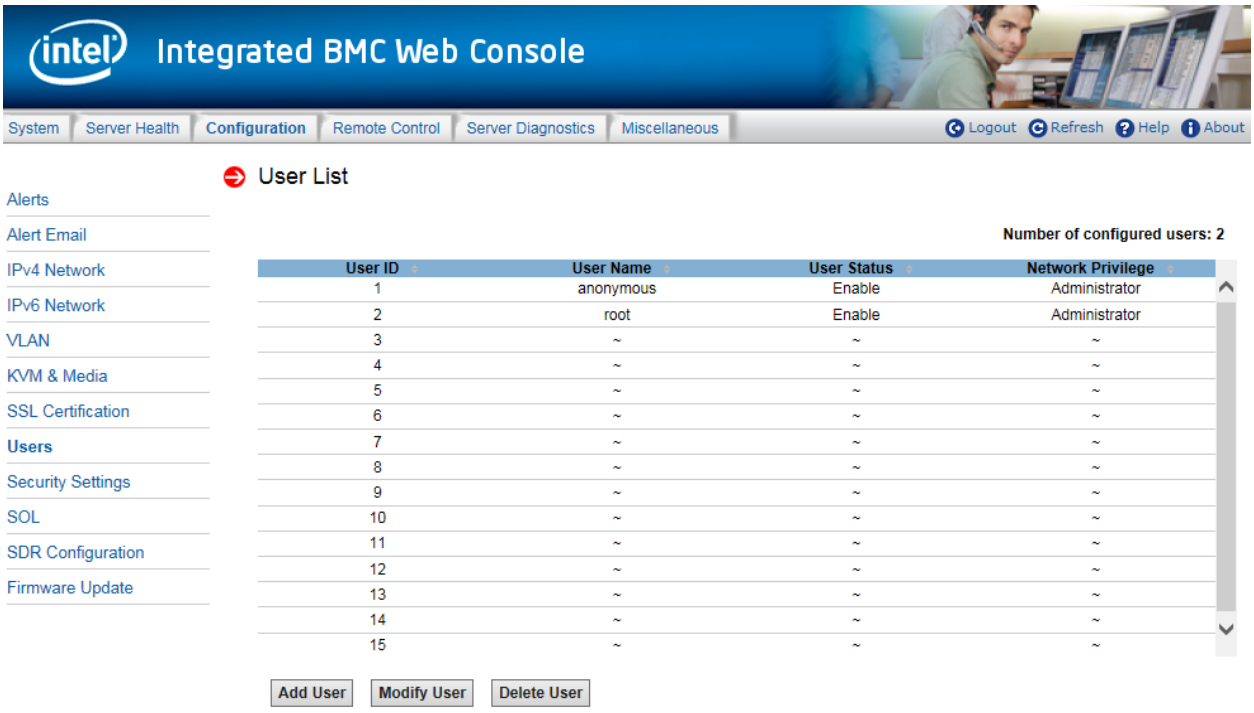


Figure 53. Configuration User List page

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 54.

Figure 54. Configuration Users 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 55.

Figure 55. Configuration Users Modify User page

To delete a user, select the user in the list and click the **Delete User** button (Figure 56).

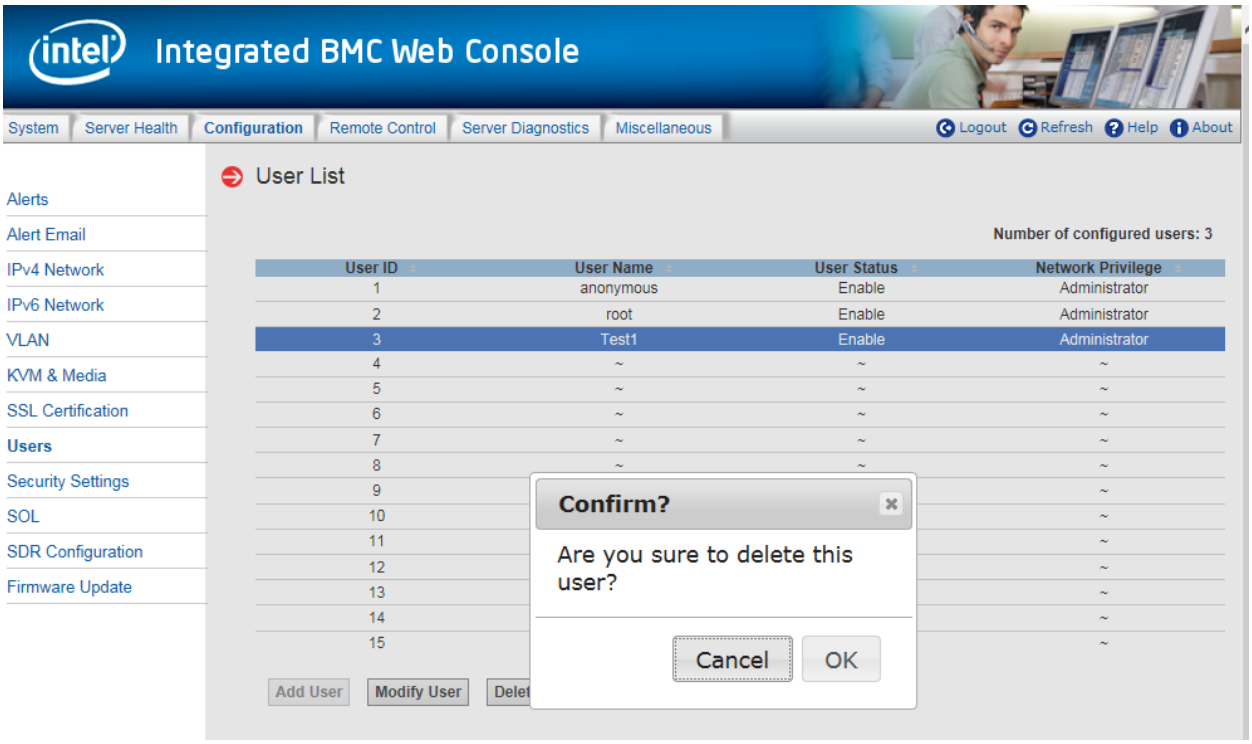


Figure 56. Configuration Users Delete User page

7.3.9 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 57 for details. Table 16 lists the options to modify the security settings.

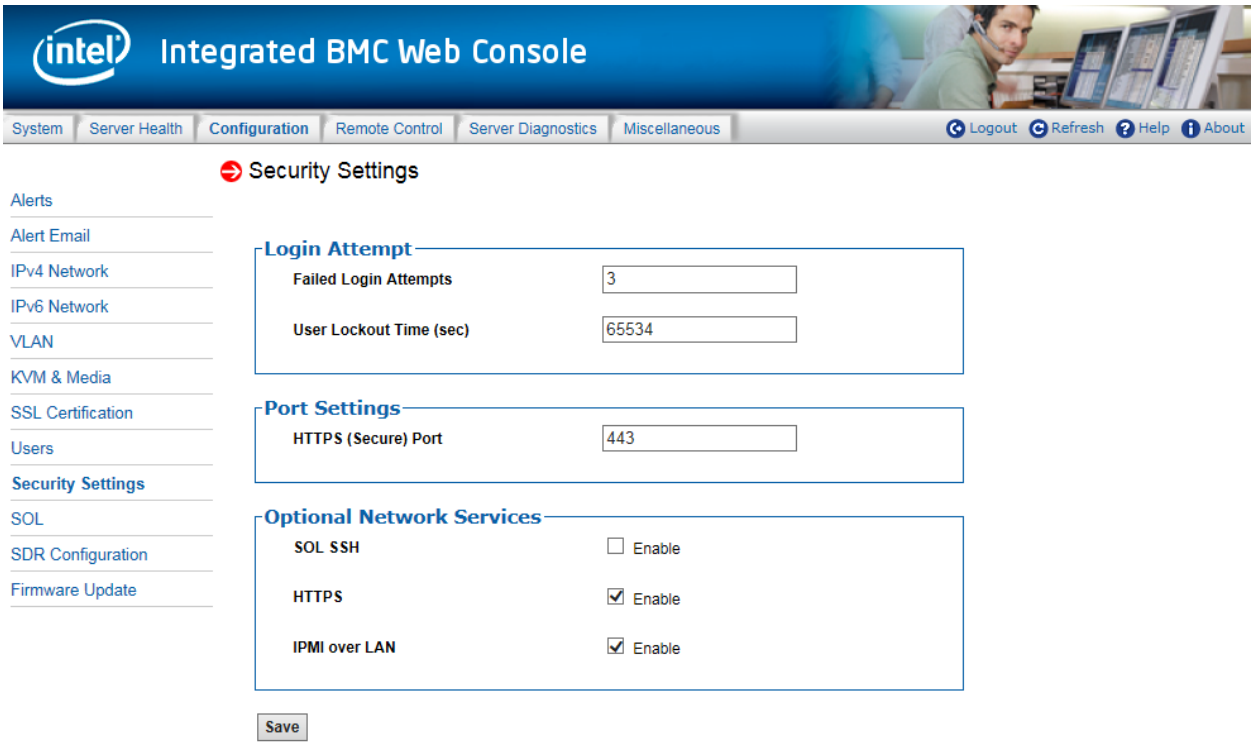


Figure 57. Configuration Security Settings page

Table 16. Configuration Security Settings options

Option	Task
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 between 0 and 255. Default is 3 attempts.
User Lockout Time(Sec)	Set the time in seconds that the user is locked out before being allowed to login again. Zero means User Lockout Time is disabled. If a user was automatically disabled due to the Bad Password threshold, the user will remain disabled until re-enabled via the Set User Access command. User Lockout Time should be between 0 and 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.
SOL SSH	Enable/disable the SOL SSH service.
HTTPS	Enable/disable the HTTPS service.
IPMI Over LAN	Enable/disable the RMCP/RMCP+ service.
Save	Click to save any changes.

7.3.10 SOL

Use this page to enable or disable SOL for each LAN channel (Figure 58). Table 17 lists the options to modify SOL settings.

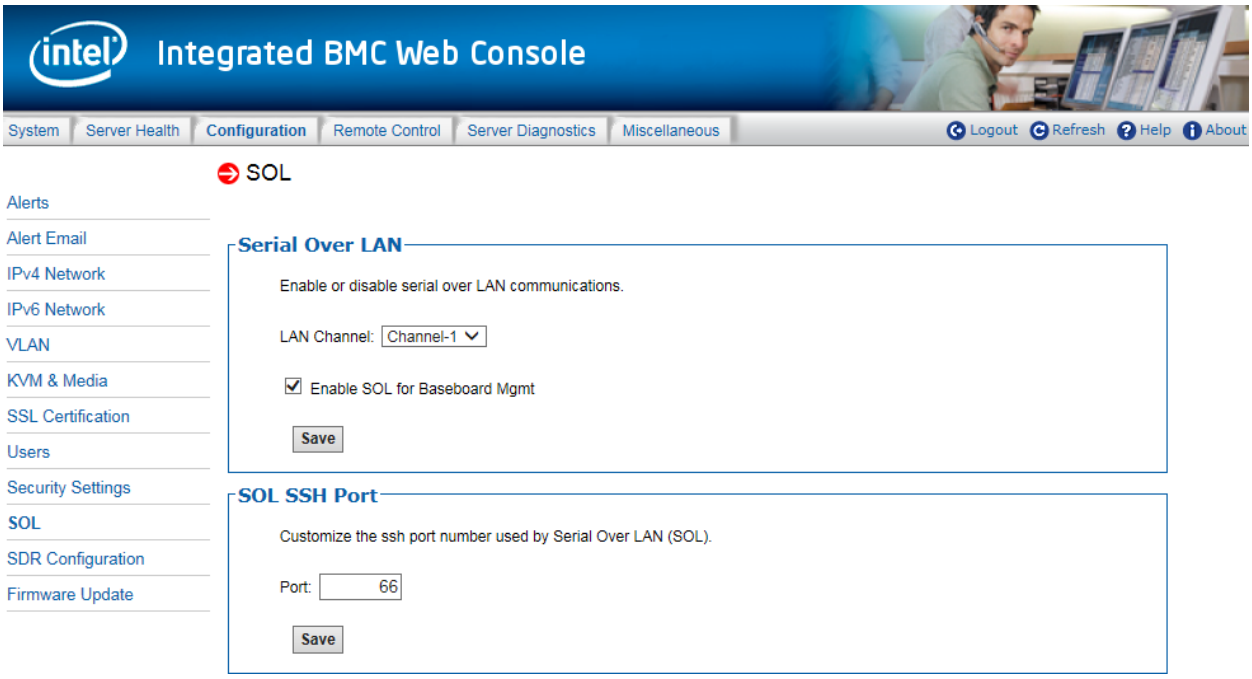


Figure 58. Configuration SOL page

Table 17. Configuration SOL options

Option	Task
LAN Channel	Select the channel on which you want to configure the network settings. Lists the LAN Channels available for SOL. The LAN channel describes the physical NIC connection on the server. • Intel(R) 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.

7.3.11 SDR Configuration

Use this page to upload and parse sensor data repository records and configuration files, which allows updating the FRUSDR package (Figure 59). Table 18 lists the options available on this page.

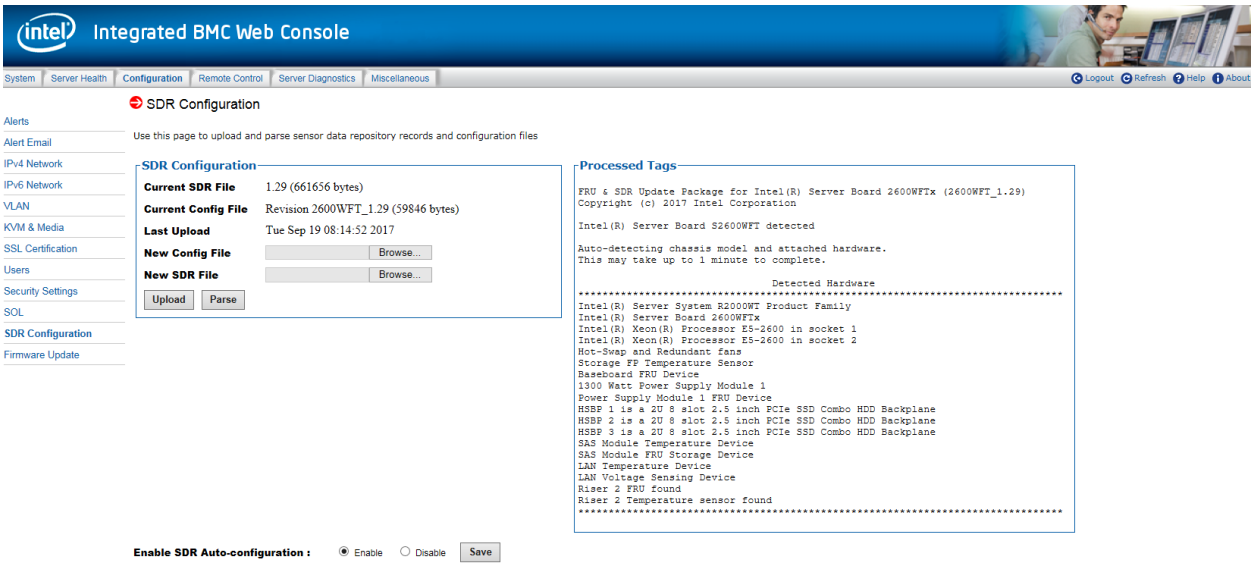


Figure 59. Configuration SDR Configuration page

Table 18. Configuration SDR Configuration options

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

7.3.12 Firmware Update

Use this page to upload new images for online-update of BMC firmware (Figure 60). Table 19 lists the options available in this page.

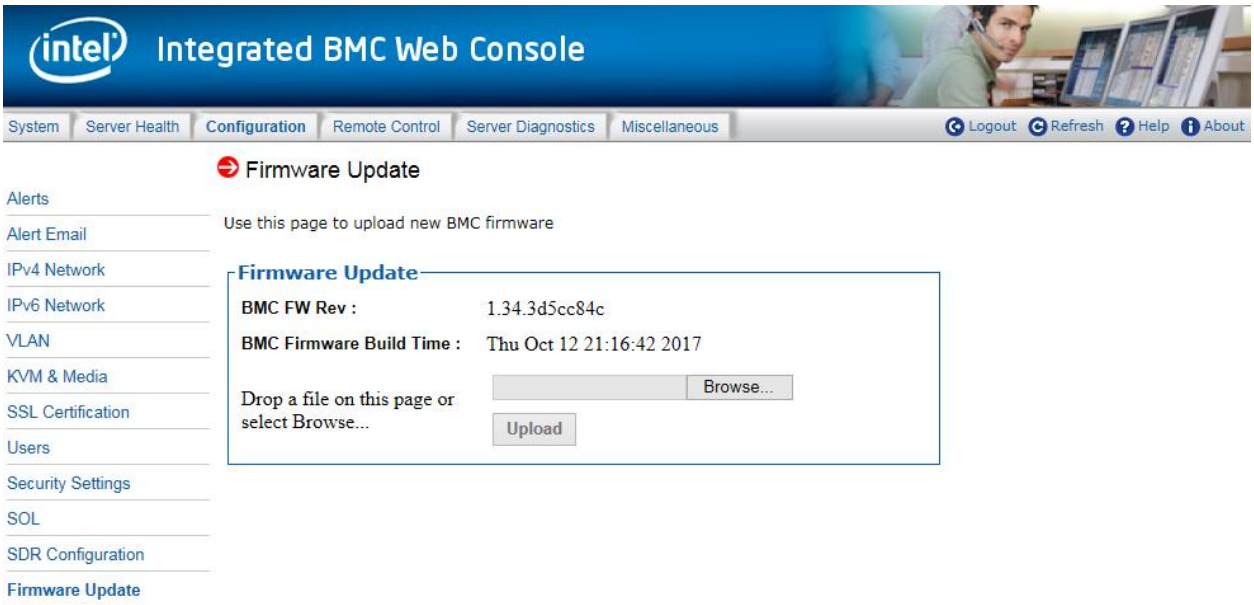


Figure 60. Configuration Firmware Update page

Table 19. Configuration 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.

7.4 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 Page

Use this page to launch the remote console KVM redirection window. This requires a Remote Management Module add-in card to be installed in the remote system; otherwise, the launch button is grayed-out. Clicking on **Launch Console** prompts to download a `launch.jnlp` file. When the file is downloaded and launched, the Java redirection window is displayed.**Error! Reference source not found.** Figure 61 shows the details.

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

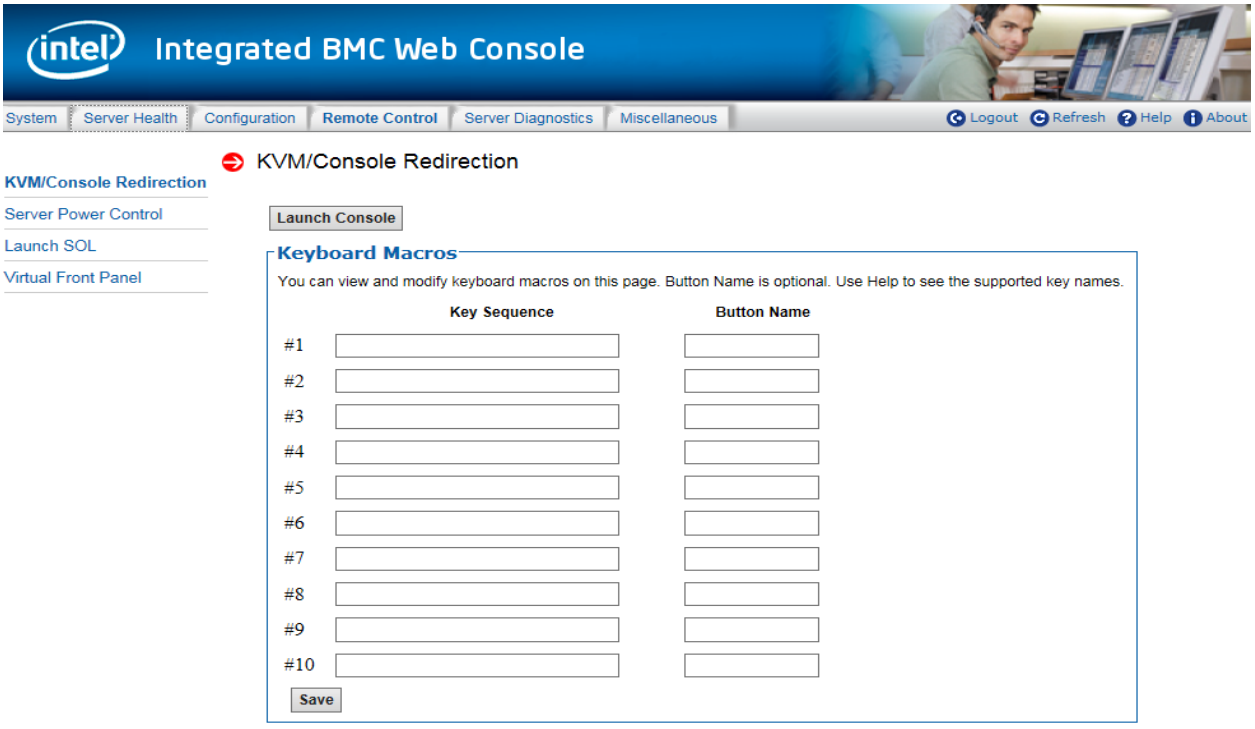


Figure 61. Remote Control KVM page

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 20. 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 62)Error! Reference source not found.. Table 21 lists the power control operations that can be performed.

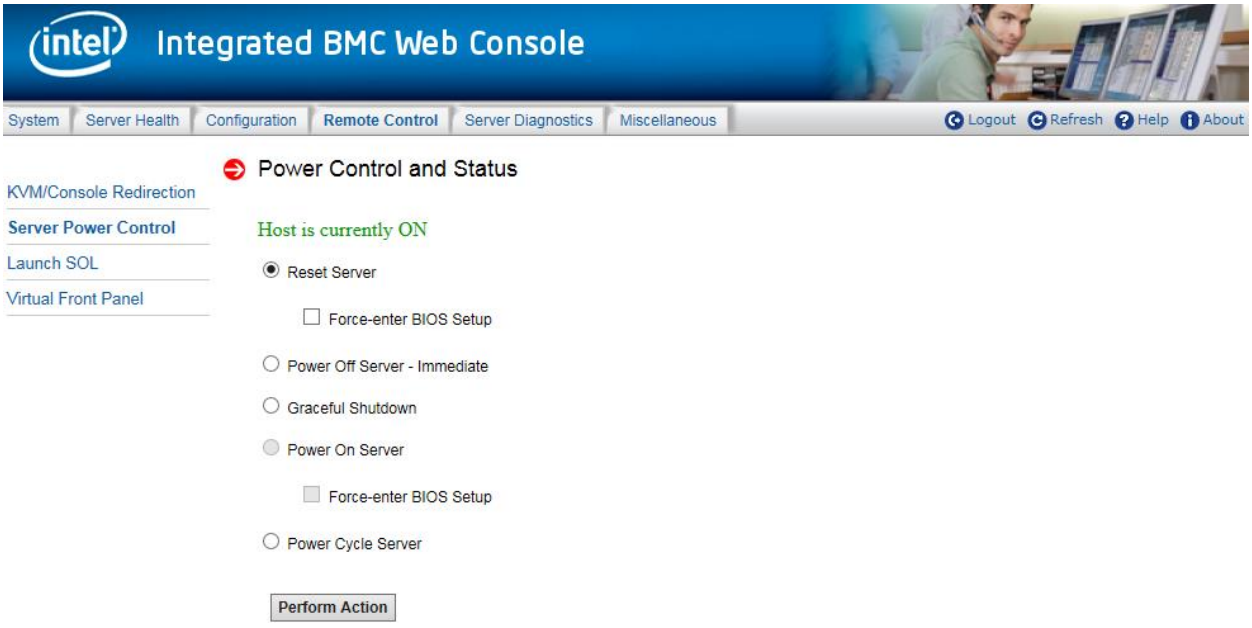


Figure 62. Remote Control Server Power Control page

Table 21. 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 on **Launch SOL** to download a `launch.jnlp` file. When the file is downloaded and launched, the Java SOL window is displayed. See Figure 63Error! Reference source not found. for details.

Figure 63. Remote Control Launch SOL page

Starting the SOL console opens an additional window as shown in Figure 65. It displays the screen content of the remote server. The SOL console behaves as if you were connected to a serial terminal on the remote server. The responsiveness may be slightly delayed depending on the bandwidth and latency of the network between Integrated BMC web console and remote console.

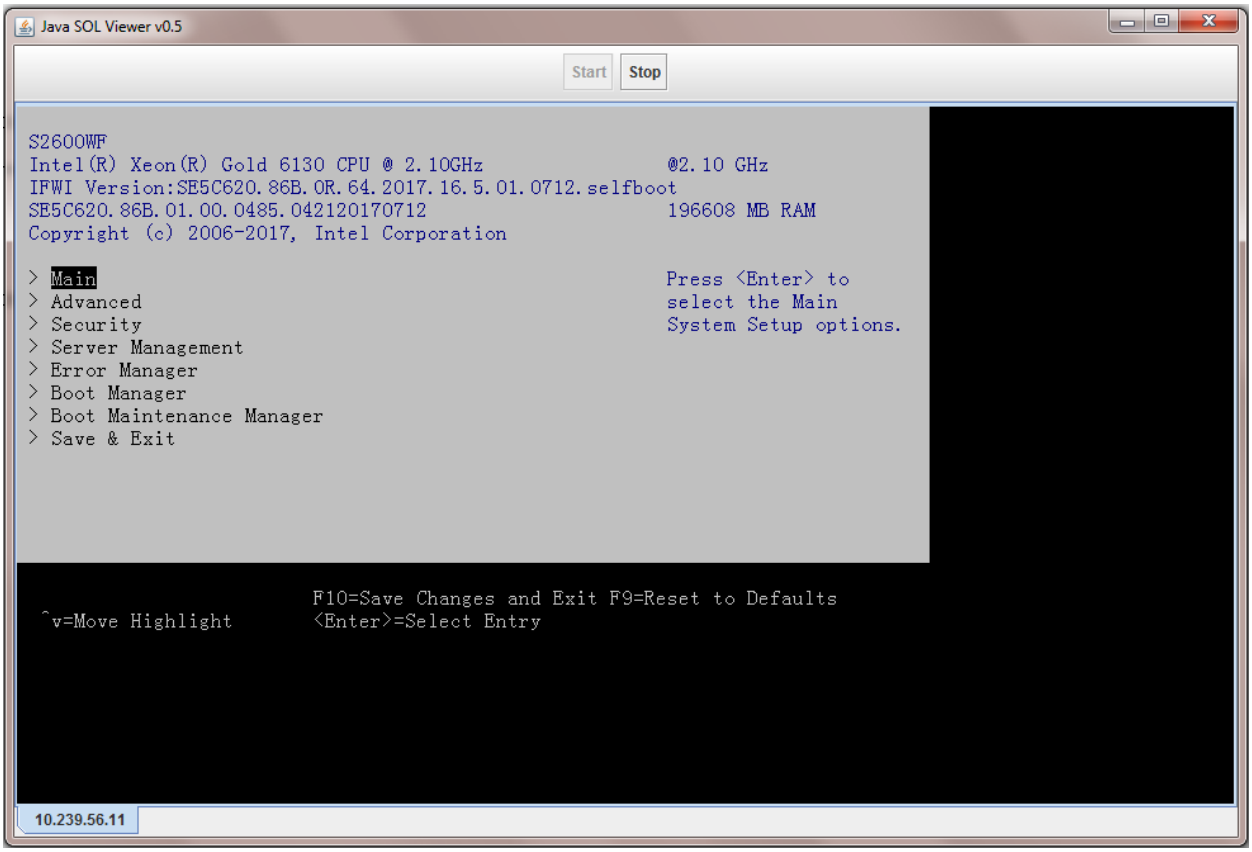


Figure 64: Remote control launch SOL screen page

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 65)Error! Reference source not found.. Table 22 lists the power control operations that can be performed.

Figure 65: Remote Control Virtual Front Panel page

Table 22. 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 grey, 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 grey, the Chassis ID is OFF.

7.5 Server Diagnostics Tab

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

7.5.1 System Disagnostics Page

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 66**Error! Reference source not found.** for details.

Figure 66. 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 FW and have associated SDRs populated in the SDR repository. This does not include any “event-only” sensors. (All BIOS sensors and some BMC and 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.

7.5.2 POST Codes Page

The POST Codes page displays recent power-on self test (POST) results. See Figure 67 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 on a time, POST code, or description causes the highlighting to persist until another code is clicked.

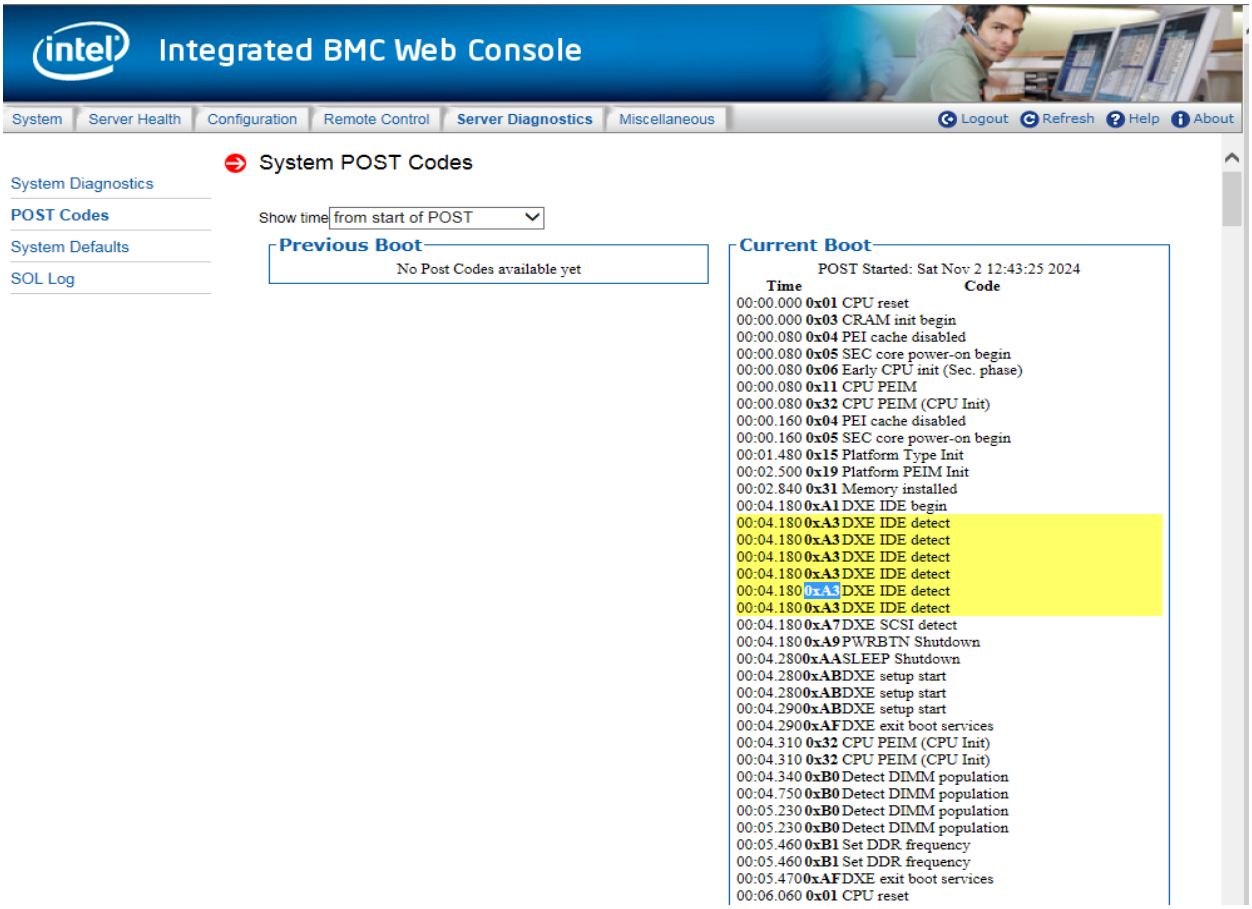


Figure 67. Server Diagnostics POST Codes page

7.5.3 System Defaults

The System Defaults page allows resetting all BMC settings to factory defaults. See Figure 68 for details. Click the **Restore** button to reset all BMC settings to factory defaults. Once complete, all remote management, including the web server, will not be accessible until users and network settings are restored locally. Settings lost include, but are not limited to:

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

This does not affect the BMC's system event log, sensor data repository, or any Node Manager Settings and policies.

Figure 68. Server Diagnostics Default page

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

7.5.4 SOL Log

The SOL Log page allows enabling/disabling SOL logging and downloading the log (Figure 69). Table 23 lists the SOL log operations that can be performed.

Figure 69. Server Diagnostics SOL Log page

Table 23. 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 Button for Enable SOL Log	Save the log to the local device.

7.6 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.

7.6.1 Intel® NM Configuration Page

Intel NM configuration is used to view, add and configure the Intel Node Manager Policies. See Figure 70**Error! Reference source not found.** for details. Table 24 lists the options to view, add, and edit the Intel NM power policies.

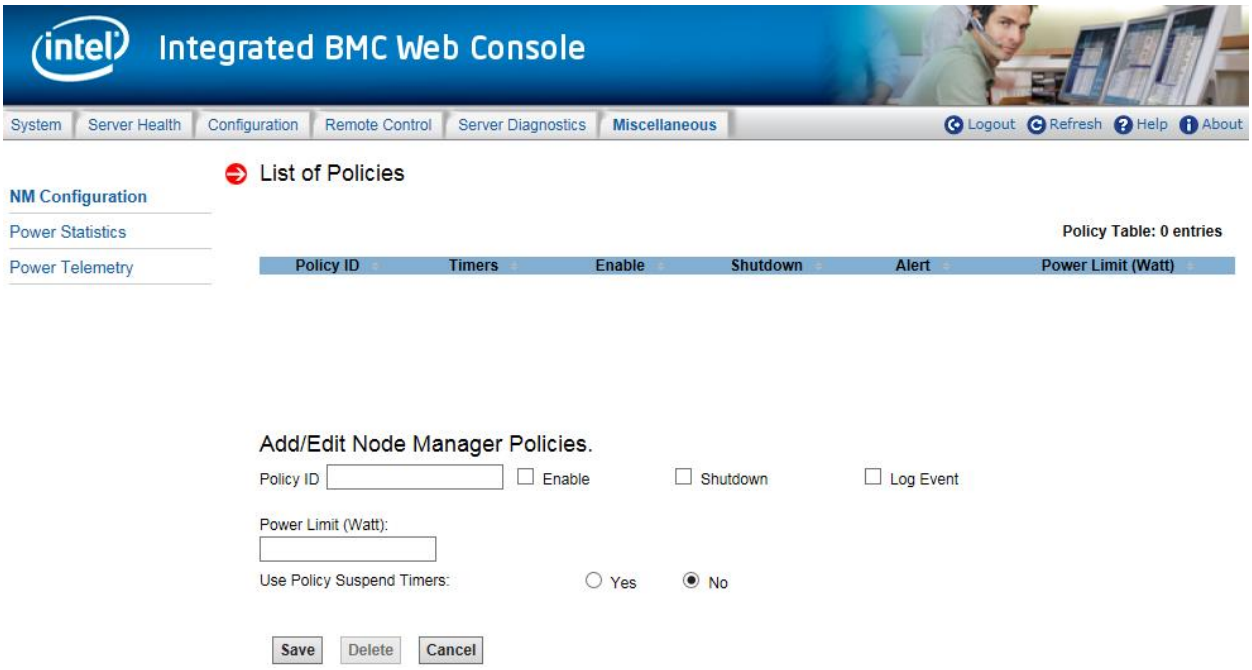


Figure 70. Intel® NM configuration page

Table 24. 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 ID 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 71). Suspend periods are repeatable by day-of-week. Start and stop times are designated in 24-hour format, in increments of 6 minutes. To specify a suspended period crossing midnight, two suspend periods must be used.
Save	Click to save any changes made.
Delete	Select a policy in the list and click to delete.
Cancel	Click to discard changes.

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

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

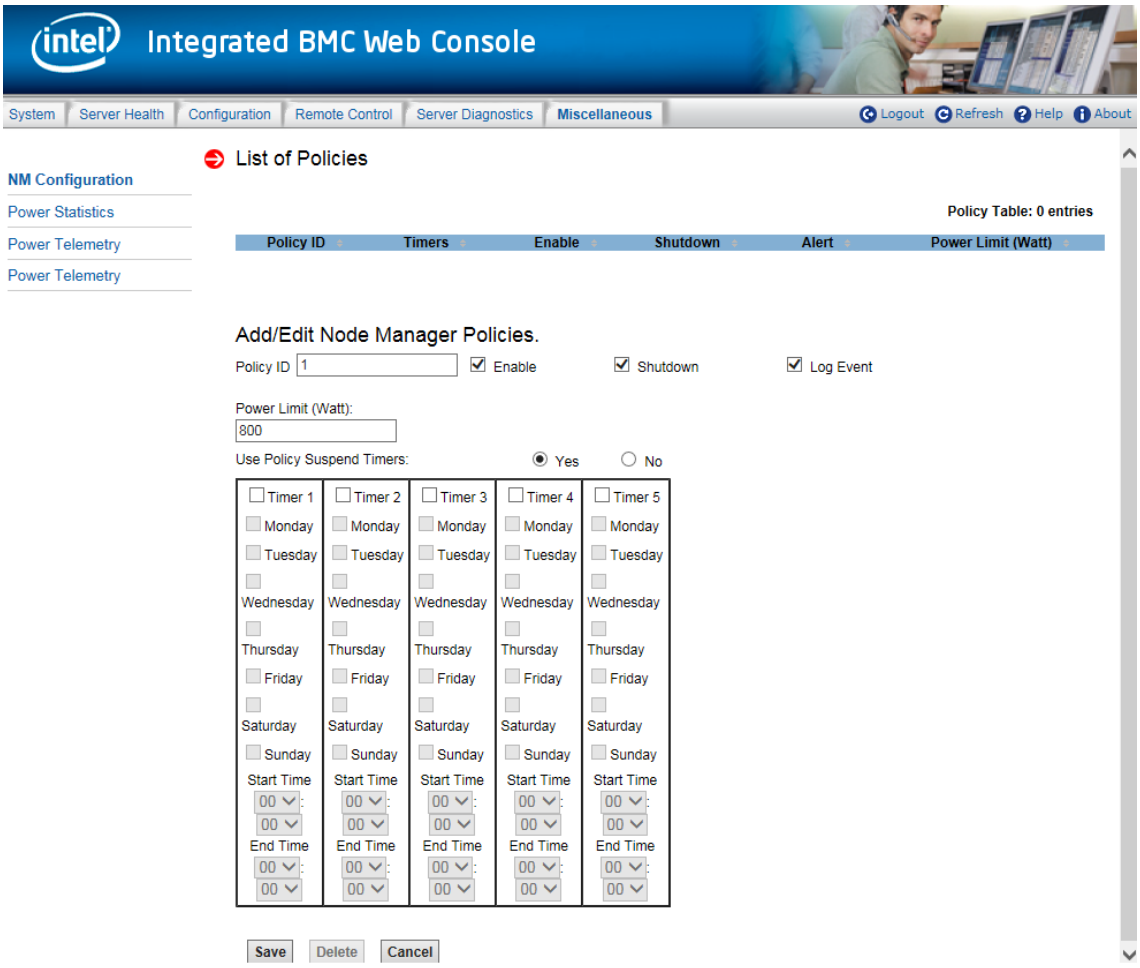


Figure 71. Intel® NM Configuration suspend page

7.6.2 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 72.**

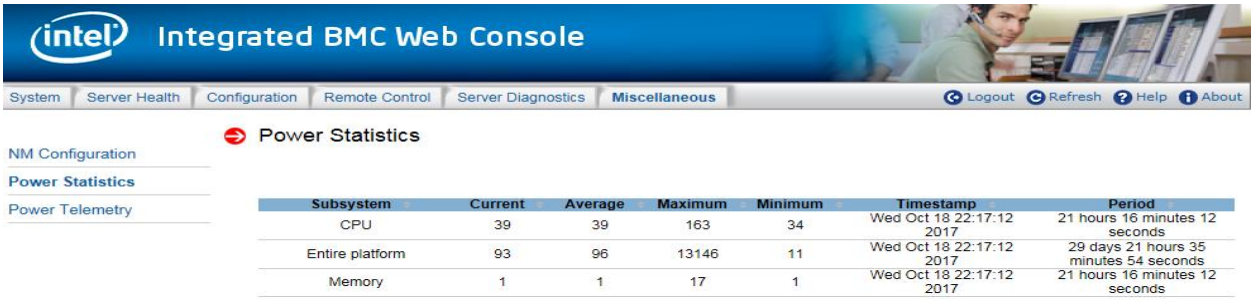


Figure 72. Power Statistics page

7.6.3 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 73** for details. To select a device category, use the **Select a device category** drop-down box (Figure 74).

Figure 73. Power Telemetry page

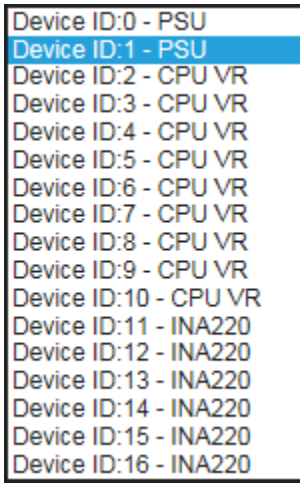


Figure 74. Power Telemetry device categories

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
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