5. Getting Started with Intel® RMM4 Operation

The Intel® RMM4 module features remote KVM access and control through LAN or Internet. The Intel® Integrated BMC Web Console is part of the standard BMC firmware/Server Management Software. The Integrated BMC Web Console feature is used to access the remote KVM.

This section describes both the interfaces and how to use them. The interfaces are accessed using TCP/IP protocol.

5.1 Before You Begin

For initial setup information, refer to Chapter 4. Before you log in, you must enable the intended user. The examples in this chapter will use user “root’, but other usernames and passwords could be used.

The Intel® RMM4 enabled advanced features may be accessed using a standard Java* enabled web browser. You may use the HTTP protocol or a secure encrypted connection from the HTTPS configurable in the embedded web server.

5.1.1 Client Browsers

In order to access the web console using a securely encrypted connection, you will need a browser that supports the HTTPS protocol. Strong security is only assured by using a Cipher Strength (encryption) of 128 - Bit. Some older browsers may not have a strong 128 Bit encryption algorithm.

If you are using Microsoft Windows Internet Explorer 7.0* or higher, you can verify strong encryption by opening the “Help/About” menu to read about the key length that is currently activated. Figure 33 shows the dialog box presented by the Internet Explorer 8.0*.

Figure 33: Internet Explorer 8* displaying encryption key length

In order to use the Remote Console (KVM) window of your 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, the browser will display slider controls to enable the user to see the full content of each web page.

5.2 Logging In

Enter the configured IP address of the Intel® RMM4 or your configured BMC on-board NIC into your web browser. In order to use a secure connection, type https://<IPaddress>/. This will take you to the Intel® Integrated BMC Web Console module login page as shown in Figure 34.

Figure 34: Intel® Integrated BMC Web Console Login Page

Log in by entering the username and password.

For example:

- Username = root
- Password = superuser

Click the **Login** button (shown in Figure 34) to view the home page.

After the initial log in, System Administrators may change passwords, create new users, and have full control over access to the RMM4 enabled advanced features.

Note: The Username and Password are case sensitive. Any username and password could be used (except anonymous).

5.3 Navigation

After successful login to the Integrated BMC Web Console module, the Integrated BMC Web Console home page appears as shown in Figure 35.

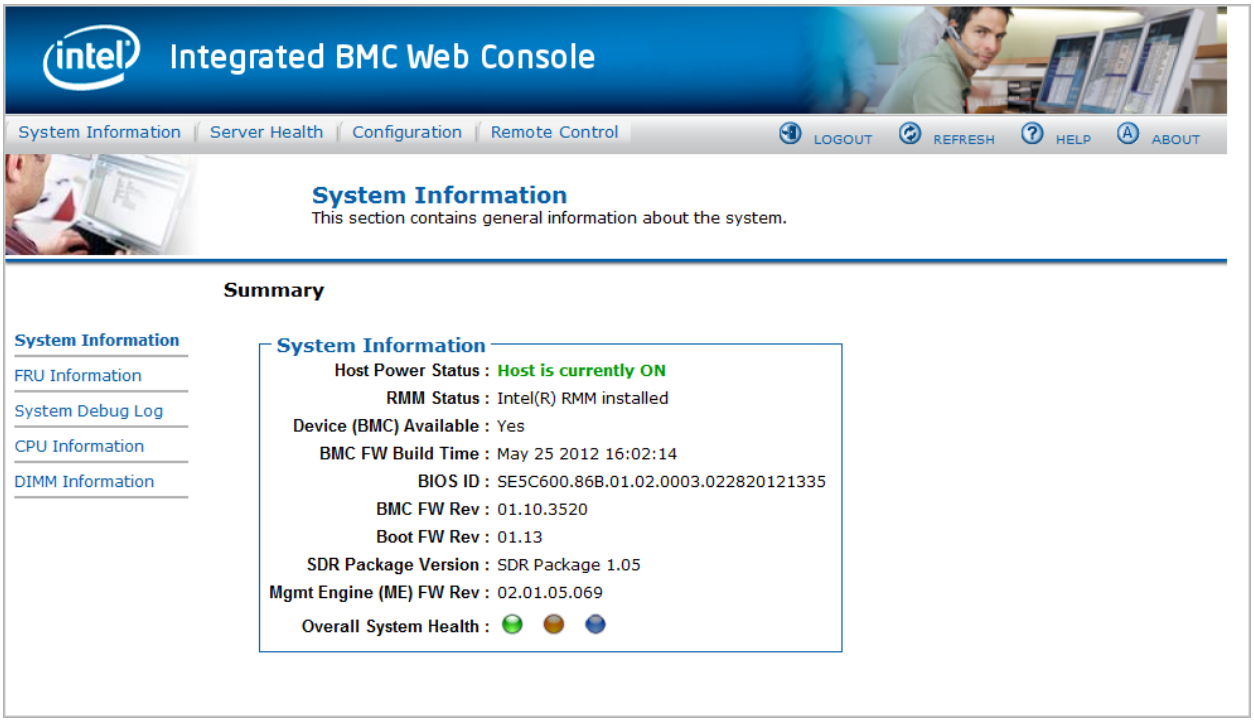

Figure 35: Integrated BMC Web Console Home Page

The top horizontal toolbar within the Integrated BMC Web Console home page has four tabs. Click these tabs to get specific system information and perform tasks as shown in the following table:

Table 8: Integrated BMC Web Console home page tabs

Tab	Function
System Information	Click this tab to access general information about the server. The tab automatically opens the 'System Information' page: • System Information • FRU Information • CPU Information (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families) • DIMM Information
Server Health	Click this tab for access to the sensors and event log. The tab automatically opens the 'Sensor Readings' page. • Sensor Readings • Event Log • Power Statistics

Tab	Function
Configuration	Click this tab to configure various settings for the server. The tab automatically opens the 'Network' configuration page. • Network/IPv4 Network • IPv6 Network (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families) • Users • Login • LDAP • VLAN (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families) • SSL • Remote Session • Mouse Mode • Keyboard Macros • Alerts • Alert Email • Node Manager (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families)
Remote Control	Click this tab for access to the remote console and to control the power state of the server. • Console Redirection. • Server Power Control • Virtual Front Panel (only on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families)

The four tabs on the horizontal menu allow you to navigate within the Integrated BMC Web Console. Each of these tabs contains a secondary menu on the left edge of the browser window. For detailed information on the specific functions of secondary menu item see Chapter 7, Intel® Integrated BMC Web Console Options.

The top horizontal toolbar also has the Logout, Refresh, and Help buttons. Click these buttons to perform tasks as shown in the following table:

Table 9: Horizontal Toolbar Buttons

Button	Function
LOGOUT	Click this button to end the current Web Console session. Note that a remote console (KVM) window, if active, will be closed when you log out. After logging out, the Web Console will return to the Login screen.
REFRESH	Click this button to refresh the current web page, including any data shown on the page. **Note:** Using the web browsers refresh/reload button or pressing the function key F5 to do a refresh/reload are not supported for reloading the Web Console pages. Using either of them can cause unexpected results.
HELP	Click this button to view a brief description of the current page in a frame at the right-hand side of the browser window. Close the Help frame by clicking the 'X' in the upper right corner of the frame or by clicking the HELP button again.
ABOUT	Click this button to view the Intel® copyright information and a statement about the use of open source code.

5.4 Online Help

The Web Console user interface gives specific online help for each page. For additional information on a certain topic or group of options, click the HELP button on the top horizontal toolbar to view the online help as shown in Figure 36. The right Help frame is visible only when the online Help is being accessed.

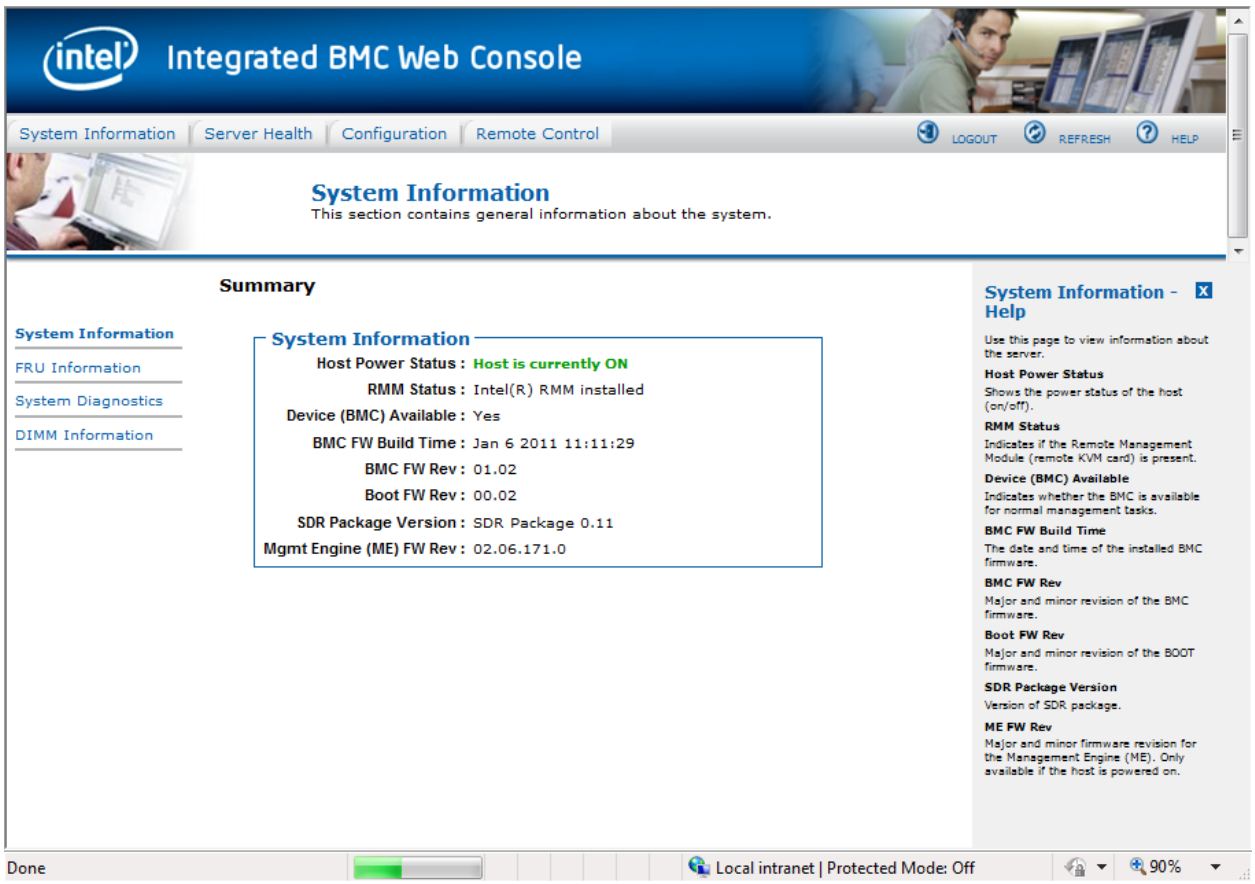

Figure 36: Launching the Online Help

5.5 Logging Out

Click the LOGOUT button to log out the current user and revert to a new login screen as shown in Figure 37 and Figure 38.

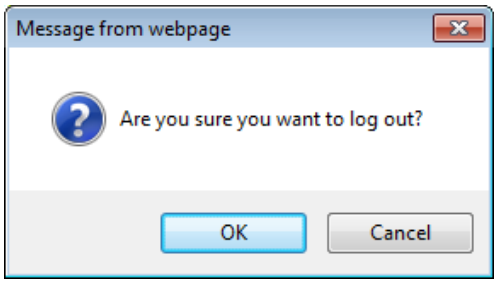

Figure 37: Logging Out of Integrated BMC Web Console – Step 1

Figure 38: Logging Out of Integrated BMC Web Console – Step 2

Note: Automatic Timeout - If there is no user activity detected by the Web Console for 30 minutes, the current session will be automatically terminated. If the user has an open KVM remote console window, the web session will not automatically timeout. The next action attempted by the user after the automatic timeout will inform the user of the need to login again for continued access to the Web Console.

6. Remote Console (KVM) Operation

The Remote Console is the redirected screen, keyboard and mouse of the remote host system where the Intel® RMM4 module is installed. To use the Remote Console window of your 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 his/her remote system. This means the keyboard and mouse can be used in the usual way.

6.1 Launching the Redirection Console

The Remote Console is the redirected keyboard, video and mouse of the remote host system where the Intel® RMM4 module is installed. Launch the remote console KVM redirection window from this page.

Note: If 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.

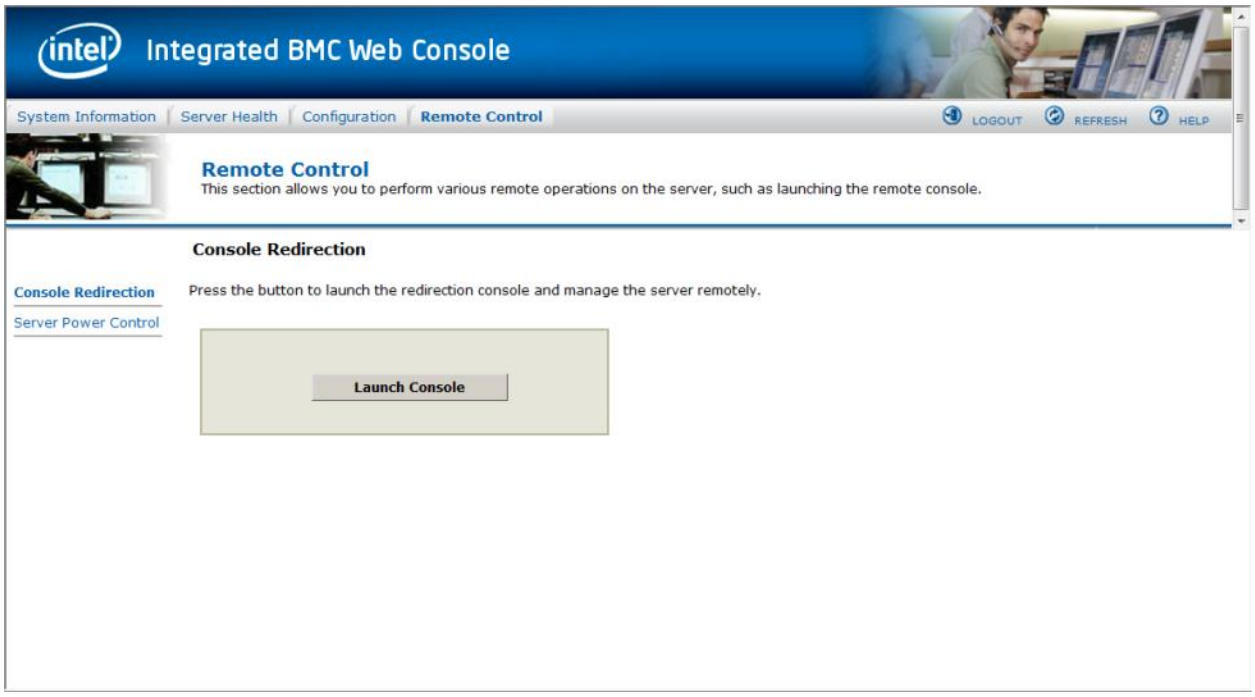

Figure 39: Remote Control Console Redirection Page

Click the **Launch Console** button to launch the redirection console and manage the server remotely.

When the Launch Console button is clicked, a pop-up window is opened to download the Java Network Launch Protocol* jviewer.jnlp file. That in turn downloads the standalone Java* application implementing the Remote Console.

Both Microsoft Internet Explorer* and Mozilla Firefox* browsers are supported.

Notes:

- Java Run-Time Environment* (JRE*, Version 6 Update 22 or higher) must be installed on the client prior to the launch of a JNLP file.
- The client browser must allow pop-up windows from the Integrated BMC Web Console IP address.

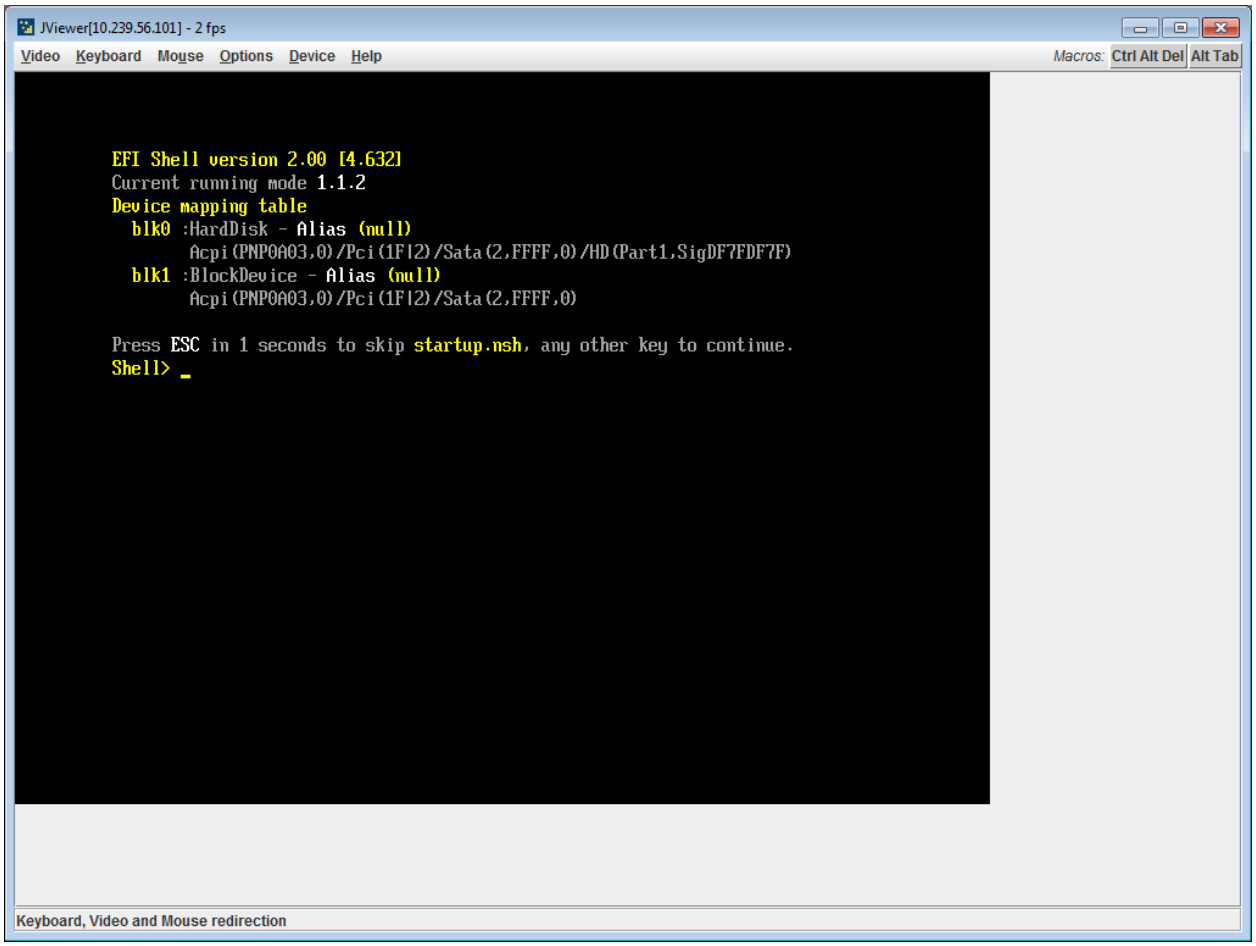

Figure 40: Remote Console

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 #7578 for KVM, #5120 for

CDROM media redirection, and #5123 for Floppy/USB media redirection. Your local network environment must permit these connections to be made, that is, your firewall and, in case you have a private internal network, your NAT (Network Address Translation) settings have to be configured accordingly.

6.2 Main Window

Starting the Remote Console opens an additional window as shown in Figure 41.

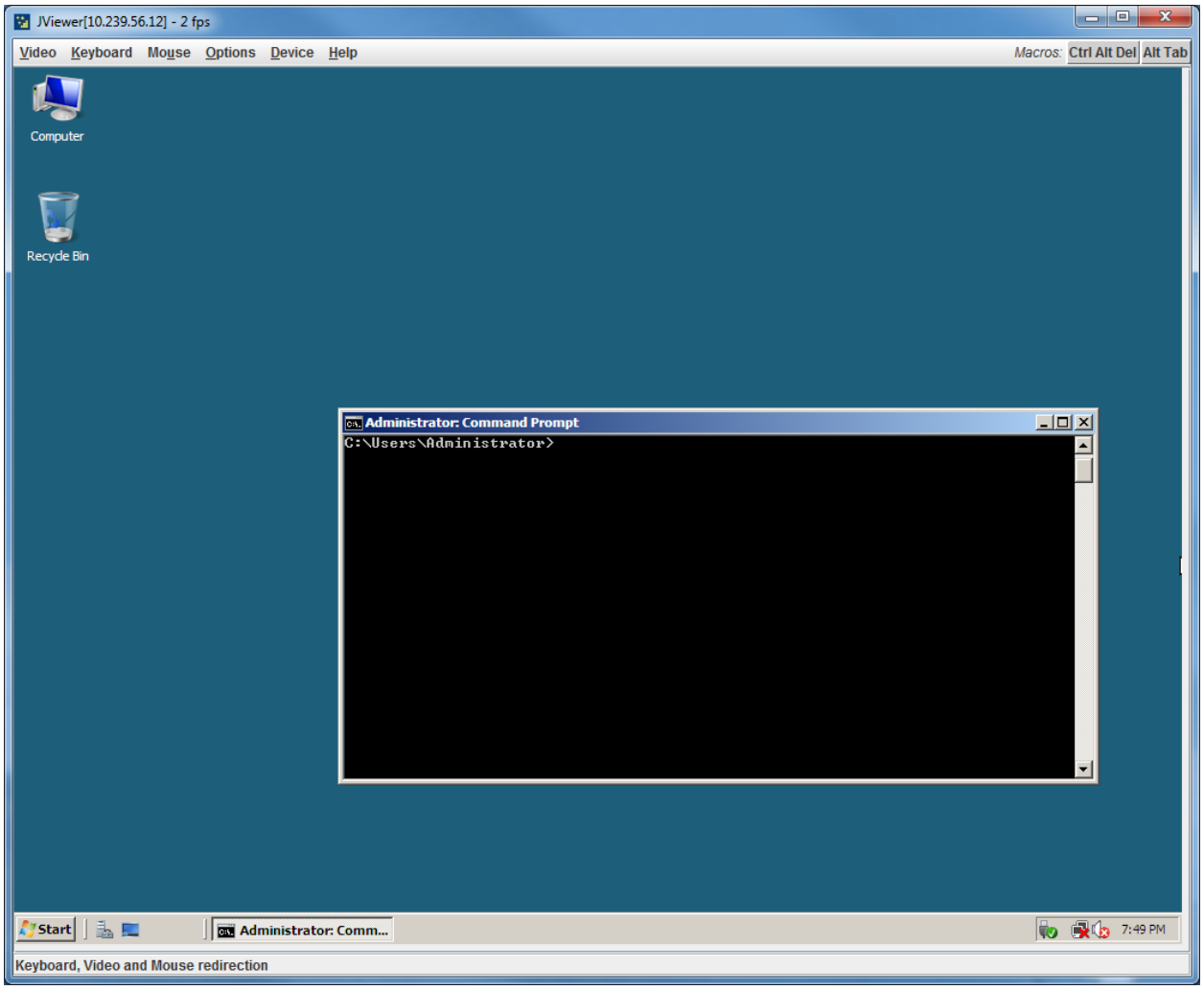

Figure 41: Remote Console Main Window

It displays the screen content of your remote server. The Remote Console will behave as if you were located at 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. Enabling KVM and/or media encryption on the Configuration > Remote Session web page will degrade performance as well.

The Remote Console window always shows the remote screen in its *optimal size*. This means it will adapt its size to the size of the remote screen initially and after the screen resolution of the remote screen has been changed. However, you can always resize the Remote Console window in your local window as usual.

6.3 Remote Console Control Bar

The upper part of the Remote Console window contains a control bar. Using its elements you can see the status of the Remote Console and influence the local Remote Console settings.

Figure 42: Remote Console Control Bar

The following sub sections describe the tasks you can perform within each control.

6.3.1 Remote Console Video Menu

Click **Video** button in the Remote Console control bar to open the Remote console Video menu as shown in Figure 43.

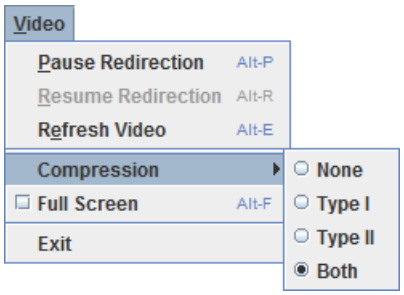

Figure 43: Remote Console Video Menu

Using this menu, you can do the following:

- **Pause Redirection.** Temporarily pauses redirection of keyboard, video, and mouse. The Remote Console window stops being updated. Keyboard shortcut is ALT+P.
- **Resume Redirection.** Resume redirection after a pause. Shortcut is ALT+R.
- **Refresh Video.** Refreshes the Remote Console window. Shortcut is ALT+E.
- **Compression.** Enabling compression improves the responsiveness of the Remote Console. Disabling compression maximizes the quality of the redirected video.
- **Full Screen.** Toggles windowed/full screen mode of the Remote Console. Shortcut is ALT+F.
- **Exit.** Closes Remote Console.

6.3.2 Remote Console Keyboard Menu

Click **Keyboard** to open the Keyboard menu with options to perform tasks as shown in Figure 44:

Figure 44: Remote Console Keyboard Menu

Using this menu, you can do the following:

- **Language.** Controls the keyboard language layout.
- **Soft Keyboard.** Displays and controls the Soft Keyboard window.
- **Hold Ctrl/Alt/Windows* keys.** Allows simulation by holding down these special keys on the remote keyboard. On the local keyboard these special keys are processed by the local OS and not passed on to the remote OS.
- **Ctrl-Alt-Del, Ctrl+Alt+Backspace, Ctrl+Alt+Left, Ctrl+Alt+Right.** Issue a fixed special key combination to the remote OS.

6.3.2.1 Keyboard Language Layout

The Remote Console supports the following keyboard language layouts: English, Dutch, French, German, Italian, Russian, and Spanish.

Figure 45: Remote Console Keyboard Language Sub Menu

In order for local key strokes to be interpreted correctly at the remote end, the client OS, the target OS, and the Remote Console should all be configured for the same language layout.

The Remote Console Java* application reverse translates local key strokes based on the selected language layout. If there is a mismatch sometimes it works fine anyway, otherwise it mostly works except for a few mistranslated or unresponsive keys and in some mismatched configurations most of the keys are mishandled.

6.3.2.1.1 Windows Language Layouts*

The Remote Console supports the Windows* default keyboard variants for the supported languages.

Under Windows*, the language is the current Language Bar setting (initially configured in **Control Panel** > **Regional and Language Options** > **Languages** > **Text Services and Input Languages**). If you are using one of the supported language keyboards, you don't have to manually select the language in the Remote Console as the auto detect automatically and immediately follows any Language Bar changes. Manually setting the language would typically be useful if you are using a keyboard close but not identical to one of the supported ones.

6.3.2.1.2 Linux Language Layouts*

The Remote Console supports the Linux* default keyboard variants for supported languages, except Russian, where it is the "Russian Winkeys" variant. The Dutch layout is "Belgium" in Linux*.

Under Linux* you typically select the language at the login screen; it can also be changed with the "locale" command but not while an application, such as the Remote Console, is running. There is also an OS keyboard layout that can be changed independently of the language. If the OS keyboard layout does not match the OS language setting, you may need to manually select the Remote Console layout.

On the other hand, with Linux* Java*, there is less reverse translation required by the application than under Windows* and is more likely that a mismatched configuration will work anyway.

6.3.2.2 Soft Keyboard

Click **Keyboard** to open the Keyboard menu with options to perform tasks as shown in Figure 46.

Figure 46: Remote Console Keyboard Soft Keyboard Sub Menu

The Soft Keyboard window is displayed and closed either by selecting the **Keyboard** > **Soft Keyboard** > **Show** checkbox or the ALT+S shortcut.

Figure 47: Remote KVM Soft Keyboard

Buttons clicked on the Soft Keyboard window get sent as key strokes to the remote target.

The Soft Keyboard is also a convenient way to see the exact layouts supported for the local keyboards since they are the same.

The Soft Keyboard language layout follows the local keyboard language setting when the default **Keyboard** > **Soft Keyboard** > **Follow Local** option is selected. This can be manually overridden by selecting a language.

Note: The Soft Keyboard keystrokes get retranslated by the remote target OS just like the local physical keystrokes and are subject to the same mismatched configuration issues.

6.3.3 Remote Console Mouse Menu

Click **Mouse** to open the Mouse menu with options to perform tasks as shown in Figure 48.

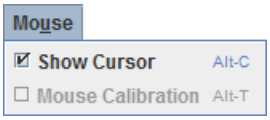

Figure 48: Remote Console Mouse Menu

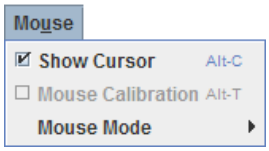

Figure 49: Remote Console Mouse Menu on EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families

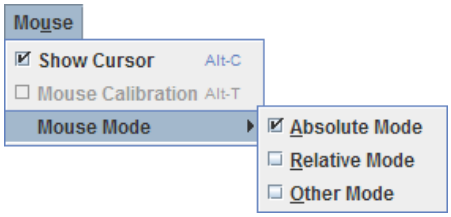

Figure 50: Remote Console Mouse Menu - Mode selection on EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families

The Mouse submenu offers two or three options:

- **Show Cursor**. This option toggles the cursor display in the Remote Console window. It does not affect the remote system cursor. Shortcut is ALT+C.

- **Mouse Calibration**. This option is used to detect the threshold and acceleration settings on the remote system and set the local client's mouse settings accordingly. It only applies when in Relative Mouse Mode, selected on the web page **Configuration** > **Mouse Mode**. Absolute Mouse Mode does not require calibration. Shortcut is ALT+T.

- **Mouse Mode.** This option is only available on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families. See Figure 49. This allows you to select the mouse mode being used. You can select Absolute, Relative, or Other as shown in Figure 50. For a description of these modes, see section 7.3.9. Note that the functionality of this option is the same as changing then saving the mode on the Mouse Mode page. Any selections that you make will be saved for the next time when the remote console window is opened.

Relative Mode Mouse Calibration Procedure

1. If the remote mouse and local mouse cursor are not in synch, start mouse calibration by selection the **Mouse Calibration** menu item or pressing ALT+T.

2. In this step, the mouse threshold settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be IN SYNCH in the beginning.

3. Please use number pad '+' or '-' keys to change the threshold settings until both the cursors go out of synch.

4. Please detect the first reading on which cursors go out of synch.

5. Once detected, use 'ALT-T' to save the threshold value.

6. In this step, the mouse acceleration settings on the remote server will be discovered. The local mouse cursor is displayed in RED color and the remote cursor is part of the remote video screen. Both the cursors will be OUT OF SYNCH in the beginning.

7. Please use number pad '+' or '-' keys to change the acceleration settings in steps of 1, or use 'Alt - +' or 'Alt - -' keys to change the acceleration settings in steps of 0.1 until both the cursors are in synch.

8. Please detect the first reading on which cursors are in synch.

9. Once detected, use 'ALT-T' to save the acceleration value.

6.3.4 Remote Console Options Menu

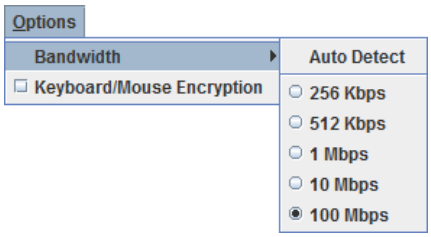

Figure 51: Remote Console Options Menu

Using this menu, you can do the following:

- **Bandwidth.** Changing the bandwidth setting affects low-level connection protocol parameters like fragment size and timeouts. If you experience performance problems when operating over a slow connection such as a modem, the Bandwidth setting may need to be adjusted. Use the Auto Detect option to find the correct setting for your connection.

- **Keyboard/Mouse Encryption.** Keyboard and Mouse data are normally encrypted before being sent over the connection, but this can be disabled for a small performance increase.

6.3.5 Remote Console Device Menu

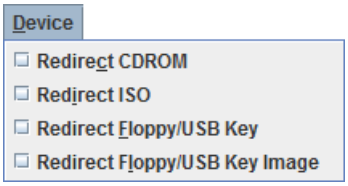

Figure 52: Remote Console Device Menu

This menu option allows starting/stopping remote media redirection. The first two options allow you to redirect either a local CDROM/DVD drive or else an ISO image on your local client file system as a virtual CDROM device on the remote system. The third option allows you to redirect either a local floppy drive or local USB key drive. The fourth option allows you to redirect a floppy or USB Key `.img` file on your local client file system as a virtual floppy device on the remote system.

Note: When trying to attach a local floppy or local USB key drive, if it is in use by the operating system or any other application it will fail to attach.

With Microsoft Windows 2008*, Microsoft Windows Vista*, Microsoft Windows 2008 R2*, and Microsoft Windows 7* if a “Windows Explorer” GUI is opened after the USB Key has been installed in the local system, you may not be able to attach the USB Key as remote media.

With Microsoft Windows 2003*, and Microsoft Windows XP* if a “Windows Explorer*” GUI is opened after the USB Key has been installed in the local system and you then browse through the USB Key, you may not be able to attach the USB Key as remote media.

The virtual devices act just like any other CDROM/DVD or floppy on the remote system. They can be read, written (assuming they are not read-only), and booted. The pair of virtual devices only appears on the remote OS or BIOS setup menus when some media redirection is active. The virtual devices persist across remote system resets and power up/downs. They do not disappear from the remote system until the checkboxes are unchecked in the Remote Console window.

Note: The virtual devices are not limited to normal floppy/CDROM sizes and will be as large as the device or file being redirected. A USB Key drive is redirected as a virtual floppy device rather than a USB device to allow the loading of custom device drivers during remote OS installation which may require a floppy drive.

There is only one virtual CDROM and one virtual floppy device on the remote system allowed so only one local item of each type can be redirected at a time. Only one Remote Console window can be doing media redirection at any given time.

6.4 Remote Console Status Line

The status line at the bottom of the Remote Console screen shows the console state as shown in Figure 53. As you navigate the menu options, the status line gives a more detailed definition of each option.

Figure 53: Status Line

7. Intel® Integrated BMC Web Console Options

This chapter gives you a detailed description of each Integrated BMC Web Console page. It is organized in sections corresponding to the four tabs in the horizontal menu. Within each section, each menu on the left-hand side is illustrated and described in detail.

Notes:

- The first menu item for each tab is the default page which appears when the tab is selected.
- Similar information about each page is available in the Web Console by clicking the HELP button at the right side of the horizontal menu.
- When the Web Console is working on current user request, a busy indicator bar appears as shown in Figure 54.

Figure 54: Busy Indicator Bar

- Not all of the following sections are used by or directly related to the RMM4 enabled features but have been added here for completeness.

7.1 System Information Tab

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

Click on the System Information tab to select the various pages. By default, the Integrated BMC Web Console home page opens the System Information page.

7.1.1 System Information page

The System information page displays a summary of the general system information. This includes the power status and the version of firmware, Figure 55 shows the details for a S1200BTL system.

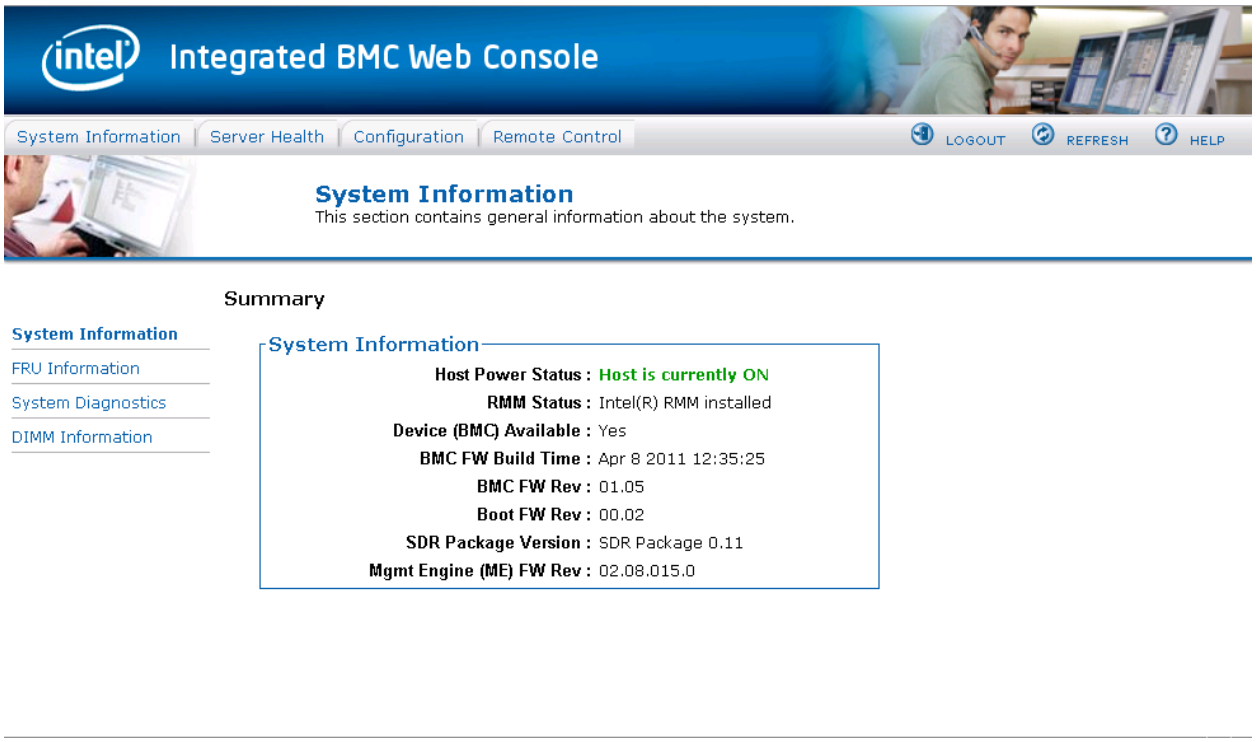

Figure 55: System Information Page on S1200BTL platforms

The System Information page has the following information about the server:

Table 10: System Information Details

Information	Details
Host Power Status	Shows the power status of the host (on/off).
RMM Status	Indicates if the Intel® RMM4 card is present.
Device (BMC) Available	Indicates if the BMC is available for normal management tasks.
BMC FW Build Time	The date and time of the installed BMC firmware.
BMC FW Rev	Major and minor revision of the BMC firmware.
Boot FW Rev	Major and minor revision of the BOOT firmware.
SDR Package Version	Version of the Sensor Data Record.
Mgmt Engine (ME) FW Rev	Major and minor revision of the Management Engine firmware.

On an EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you also get an **Overall System Health** Indication. See Figure 56 for details. These are a general indication of the system heath:

- Left (Green) = System Ready LED
- Center (Amber) = System Fault LED
- Right (Blue) = Chassis ID LED

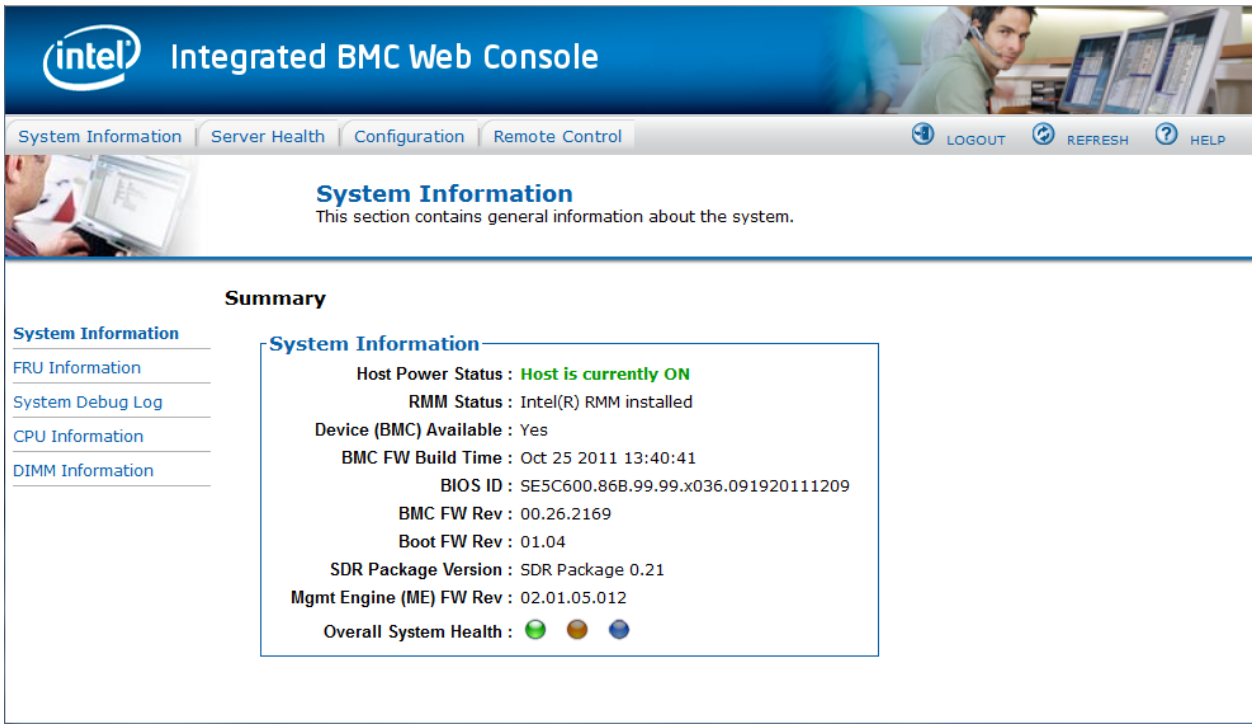

Figure 56: System Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.1.2 Field Replaceable Unit (FRU) Information Page

The Field Replaceable Unit (FRU) Information page displays information from the FRU repository of the host system. See Figure 57 for details:

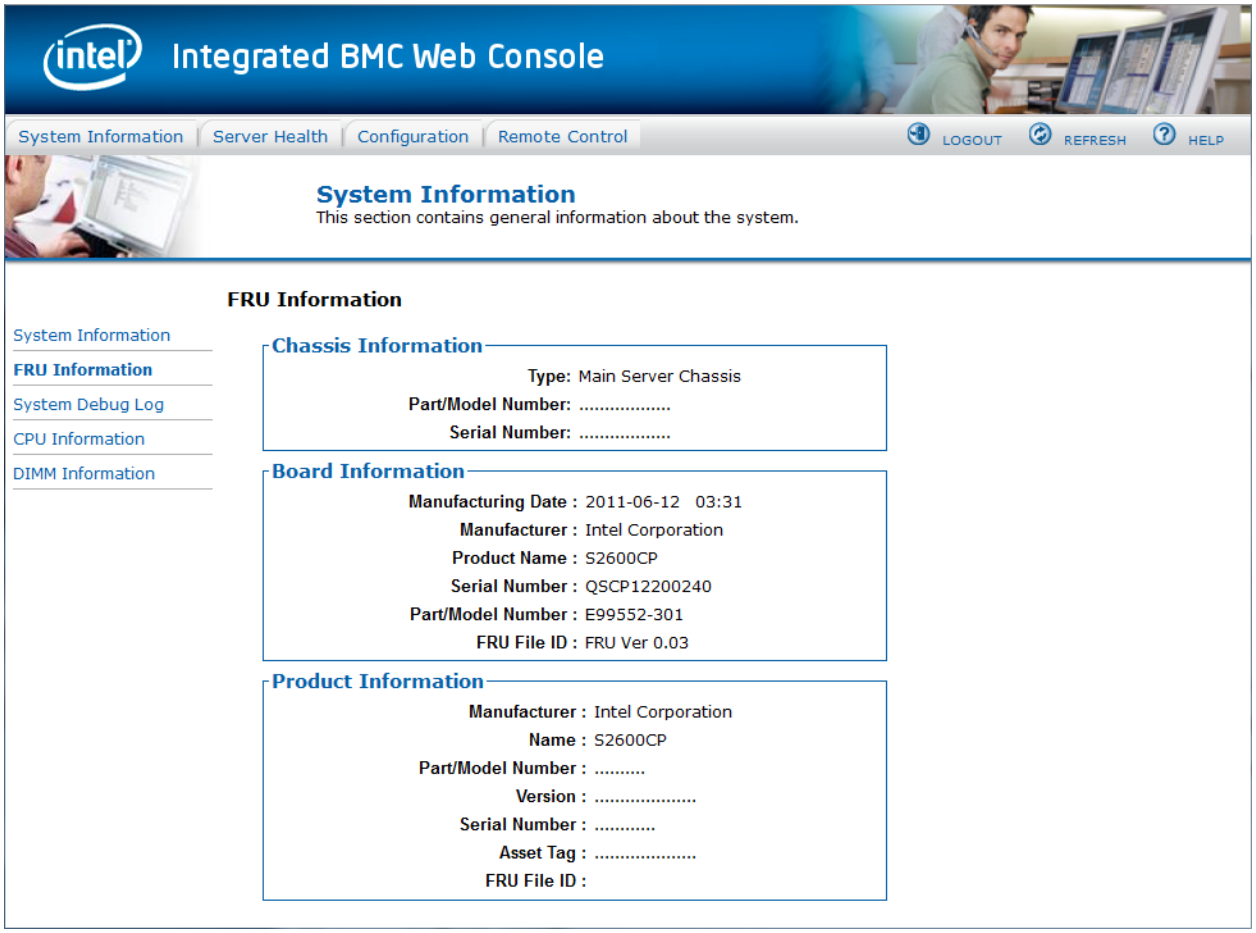

Figure 57: System Information FRU Information Page

7.1.3 System Debug Log Page

The System Debug Log 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 file is not meant to be viewable by the end user but rather to provide additional debugging capability to your system manufacturer or an Intel® support engineer.

7.1.3.1 System Debug Page on S1200BTL platforms.

The System Debug page can be used to collect system debug information on S1200BTL systems. See Figure 58 for details.

From the System Debug page you will be able to run the System Debug Log dump.

Press the **Run** button. It may take some time for the debug information to be collected.

Once the debug log dump is finished you can click the debug log filename to save the results as a .zip file on your client system. The file can then be sent to your system manufacturer or an Intel® support engineer for analysis.

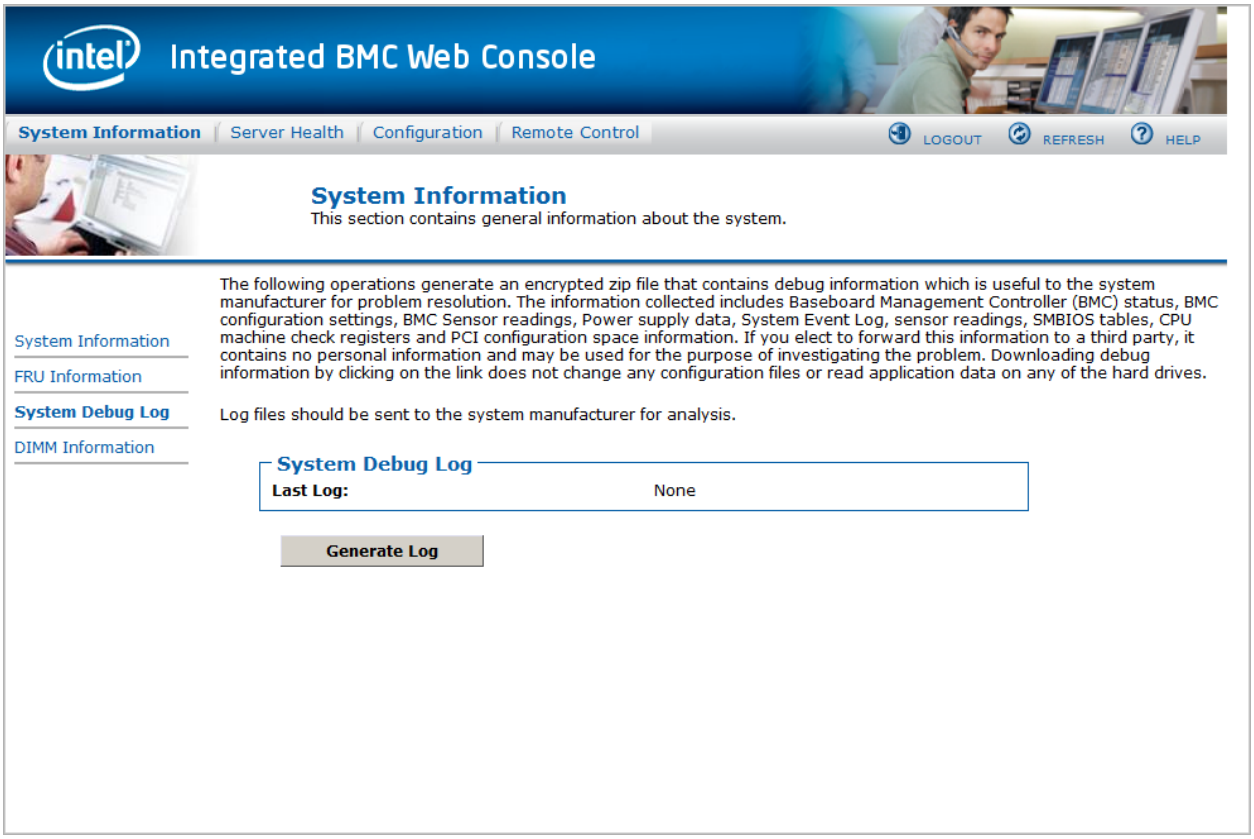

Figure 58: System Information System Debug Log Page on S1200BTL platforms

A list of 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, ERR[2], SMI timeout, PERR, and SERR. The debug data is saved and timestamped for the last 3 occurrences of the error conditions.

a. PCI error registers

b. MSR registers

c. Integrated Memory Controller (iMC) and Integrated I/O (IIO) module registers.

BMC configuration data

BMC FW debug log (that is, SysLog) – Captures FW debug messages.

7.1.3.2 System Debug Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families

The System Debug Log page can be used to collect system debug information on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families. See Figure 59 for details.

Press the **Run** button. It may take some time for the debug information to be collected.

Once the debug log dump is finished you can click the debug log filename to save the results as a .zip file on your client system. The file can then be sent to your system manufacturer or an Intel® support engineer for analysis.

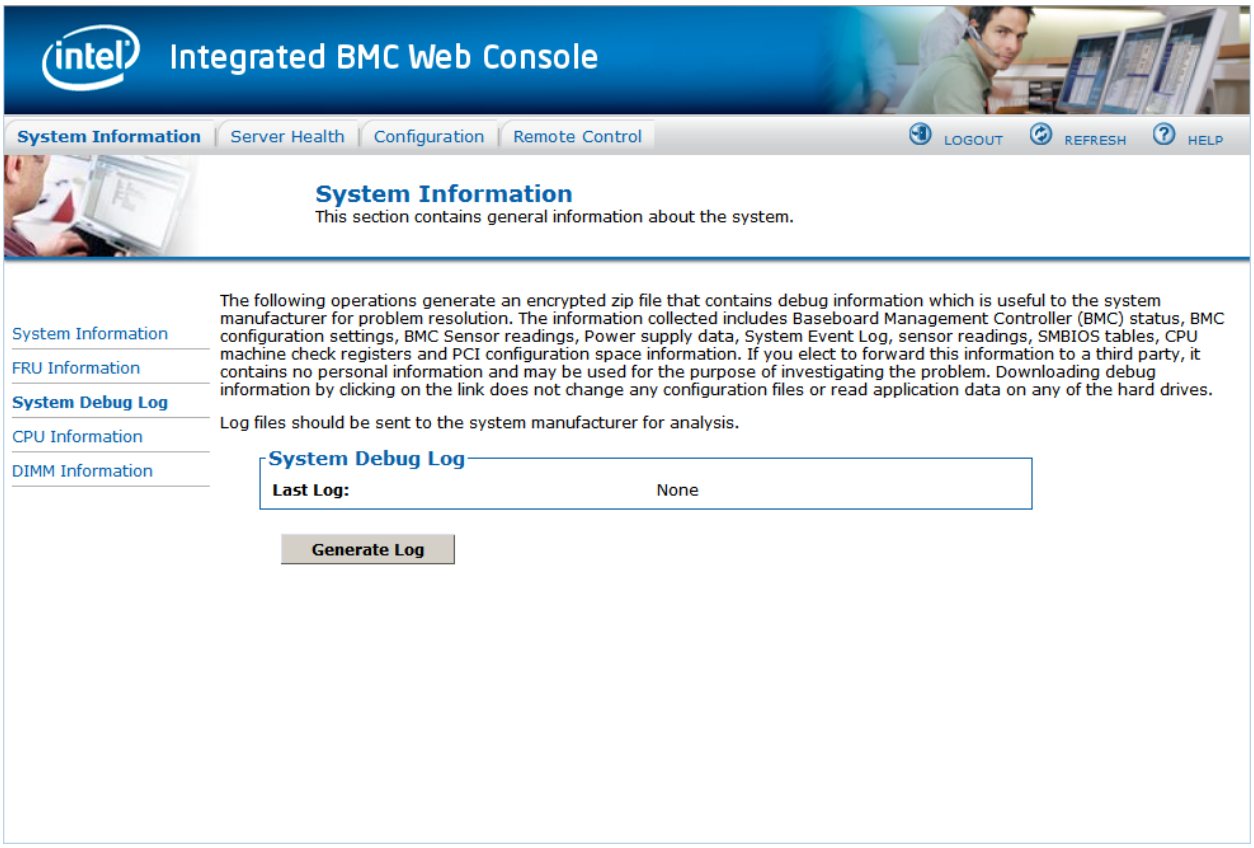

Figure 59: System Information System Debug Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

A list of 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, ERR[2], SMI timeout, PERR, and SERR. The debug data is saved and timestamped for the last 3 occurrences of the error conditions.

a. PCI error registers

b. MSR registers

c. Integrated Memory Controller (iMC) and Integrated I/O (IIO) module registers.

BMC configuration data

BMC FW debug log (that is, SysLog) – Captures FW debug messages.

a. *Non-volatile storage of captured data*. Some of the captured data will be stored persistently in the BMC's non-volatile flash memory and preserved across AC power cycles. Due to size limitations of the BMC's flash memory, it is not feasible to store all of the data persistently.

b. *SMBIOS table data.* The entire SMBIOS table is captured from the last boot.

c. *PCI configuration data for on-board devices and add-in cards*. The first 256 bytes of PCI configuration data is captured for each device for each boot.

d. *System memory map*. The system memory map is provided by BIOS on the current boot. This includes the EFI memory map and the Legacy (E820) memory map depending on the current boot.

e. *Power supply debug capability*

- *Capture of power supply "black box" data and power supply asset information.* Power supply vendors are adding the capability to store debug data within the power supply itself. The platform debug feature provides a means to capture this data for each installed power supply. The data can be analyzed by Intel® for failure analysis and possibly provided to the power supply vendor as well. The BMC gets this data from the power supplies by using PMBus* manufacturer-specific commands.

- *Storage of system identification in power supply.* The BMC copies board and system serial numbers and part numbers into the power supply whenever a new power supply is installed in the system or when the system is first powered on. This information is included as part of the power supply black box data for each installed power supply.

f. *Accessibility using IPMI interfaces*. The platform debug file can be accessed from an external IPMI interface (KCS or LAN).

g. *POST code sequence for the two most recent boots*. This is a best-effort data collection by the BMC as the BMC real-time response cannot guarantee that all POST codes are captured.

h. *Support for multiple debug files*. The platform debug feature provides the ability to save data to 2 separate files that are encrypted with different passwords.

- *System Debug Log* file can be viewed by Intel® partners who have signed an NDA with Intel® and its contents are restricted to specific data items specified in this with the exception of the BMC syslog messages and power supply "black box" data.

- *System and BMC Debug Log* file is strictly for viewing by Intel® engineering and may contain BMC log messages (that is, syslog) and other debug data that Intel® FW developers deem useful in addition to the data specified elsewhere in this document.

7.1.4 DIMM Information Page

The DIMM Information page displays information on DIMM modules installed on the host system. See Figure 60 for details:

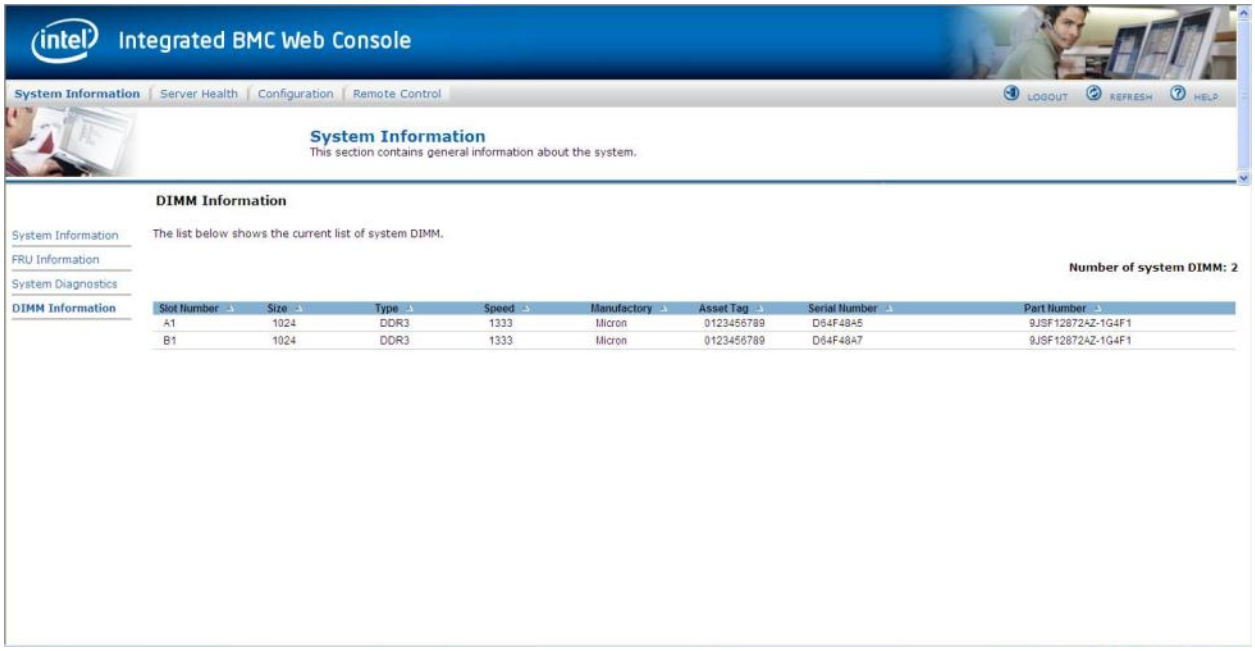

Figure 60: System Information DIMM Information Page

7.1.5 CPU Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families

The CPU Information page displays information on the processors that are installed on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families. See Figure 61 for details:

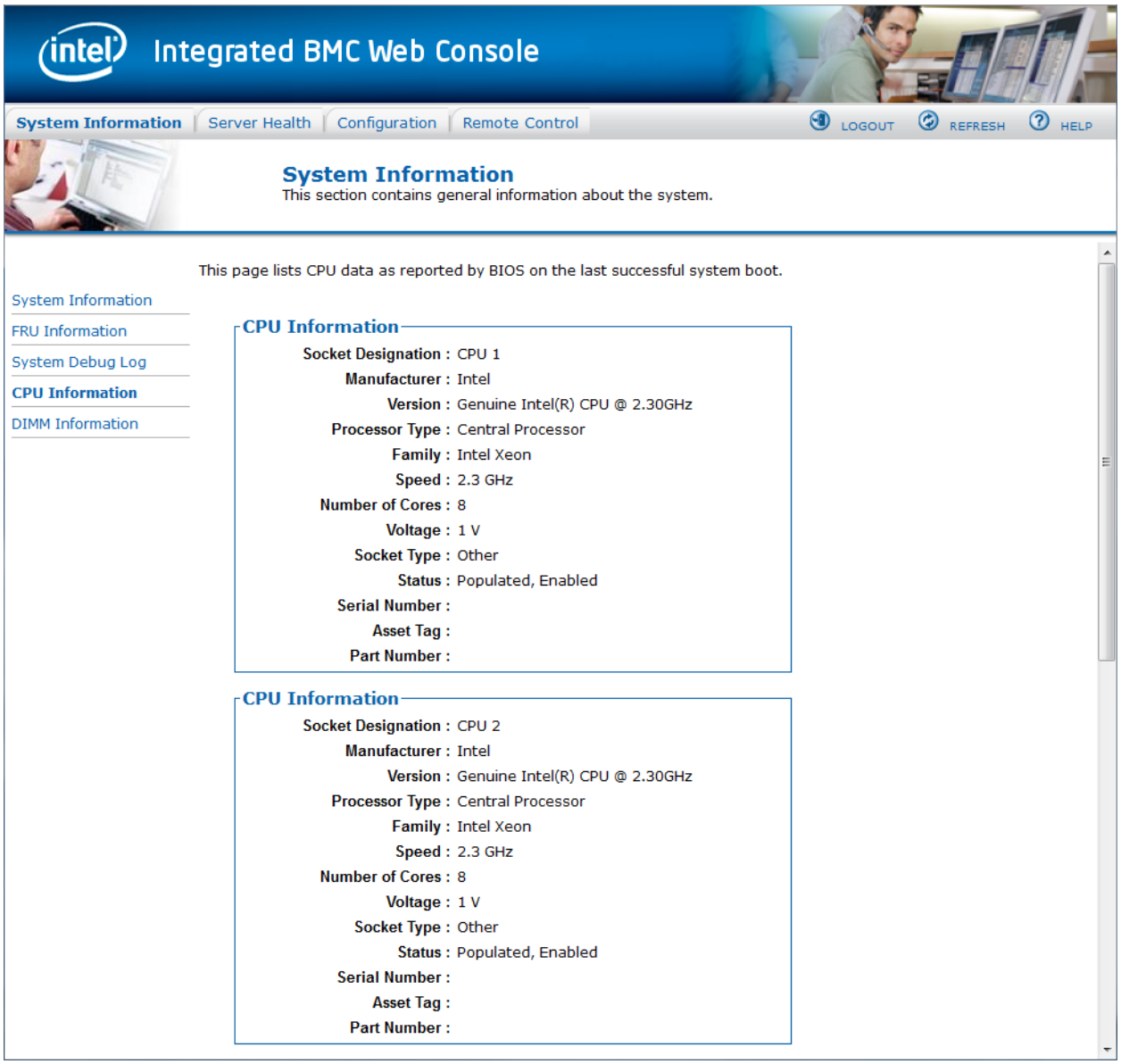

Figure 61: System Information CPU Information Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.2 Server Health Tab

The Server Health tab shows you data related to the server's health, such as sensor readings, the event log, and power statistics as explained in the following sub sections.

Click on the Server Health tab to select the various pages. By default, this tab opens the Sensor Readings page.

7.2.1 Sensor Readings Page

The Sensor Readings page displays system sensor information including status, health, and reading as shown in Figure 62 and Figure 63.

By default, the sensor readings are updated every 60 seconds but this can be changed by entering a value in the **Set auto-refresh in seconds** selection box and then pressing the **Set** button.

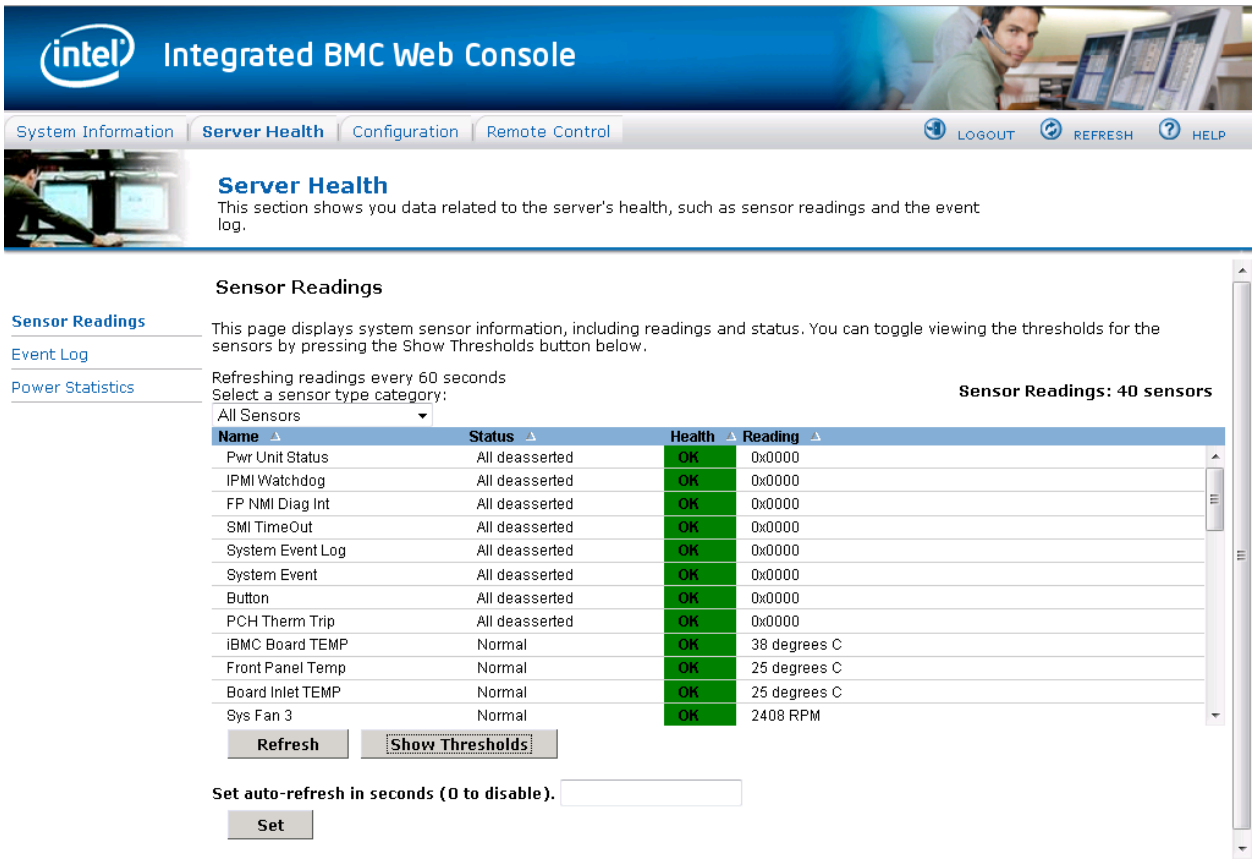

Figure 62: Server Health Sensor Readings Page (Thresholds not displayed)

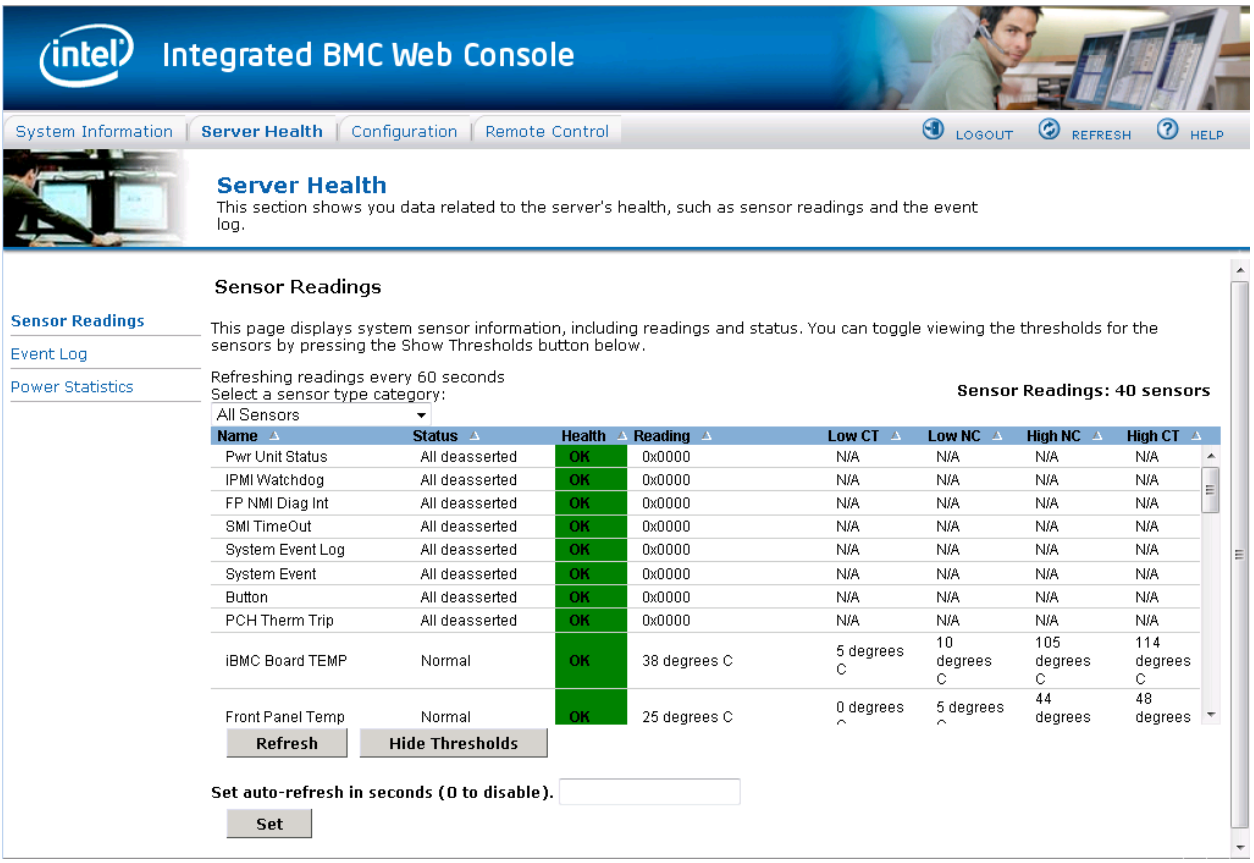

Figure 63: Server Health Sensor Readings Page (Thresholds displayed)

The following table lists the options available in this page:

Table 11: Server Health Sensor Readings Options

Option	Task
Sensor Selection pull-down box	Select the type of sensor readings to display in the list. The default is to see all sensors.
Sensor Readings list	Selected sensors shown with their name, status, health, and readings.
Refresh button	Click to refresh the selected sensor readings
Show Thresholds button	Click to expand the list, showing low and high threshold assignments. Shows the critical (CT) and non-critical (NC) thresholds for the selected sensors Use scroll bar at the bottom to move display left and right.
Hide Thresholds button	Click to return to original display, hiding the threshold values
Set auto-refresh in seconds (0 to disable) selection	Enter the time (in seconds) to wait between updates of the Sensor Readings and then press the **Set** button.

7.2.2 Event Log Page

The Event Log page displays the systems server management Event Log. Figure 64 shows the details for a S1200BTL system.

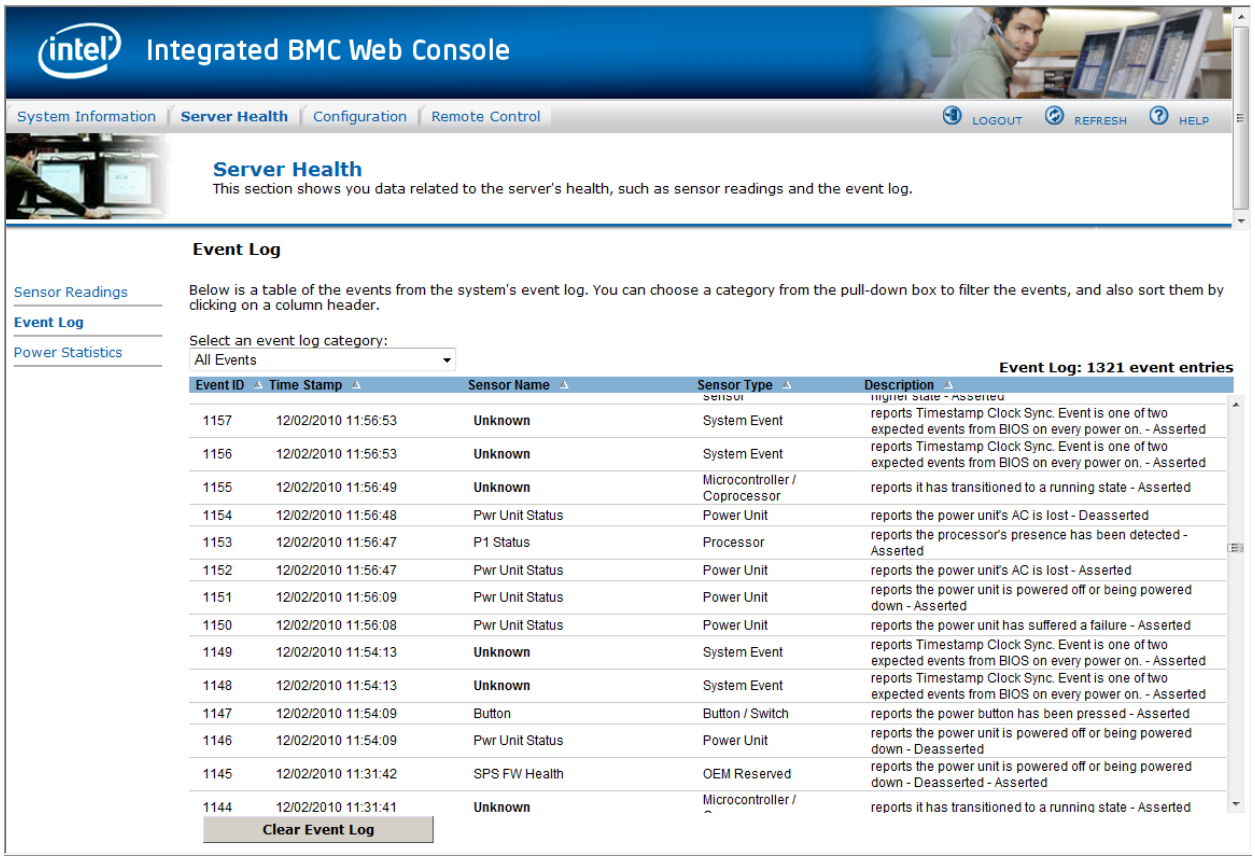

Figure 64: Server Health Event Log Page on S1200BTL platforms

The following table lists the options available in this page:

Table 12: Server Health Event Log Options on S1200BTL platforms

Option	Task
Event Log Category pull-down box	Select the type of events to display in the list
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, sensor type, and description.
Clear Event Log button	Click to clear the event logs.

On an EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you also get a **Save Event Log** button. See Figure 65 for details.

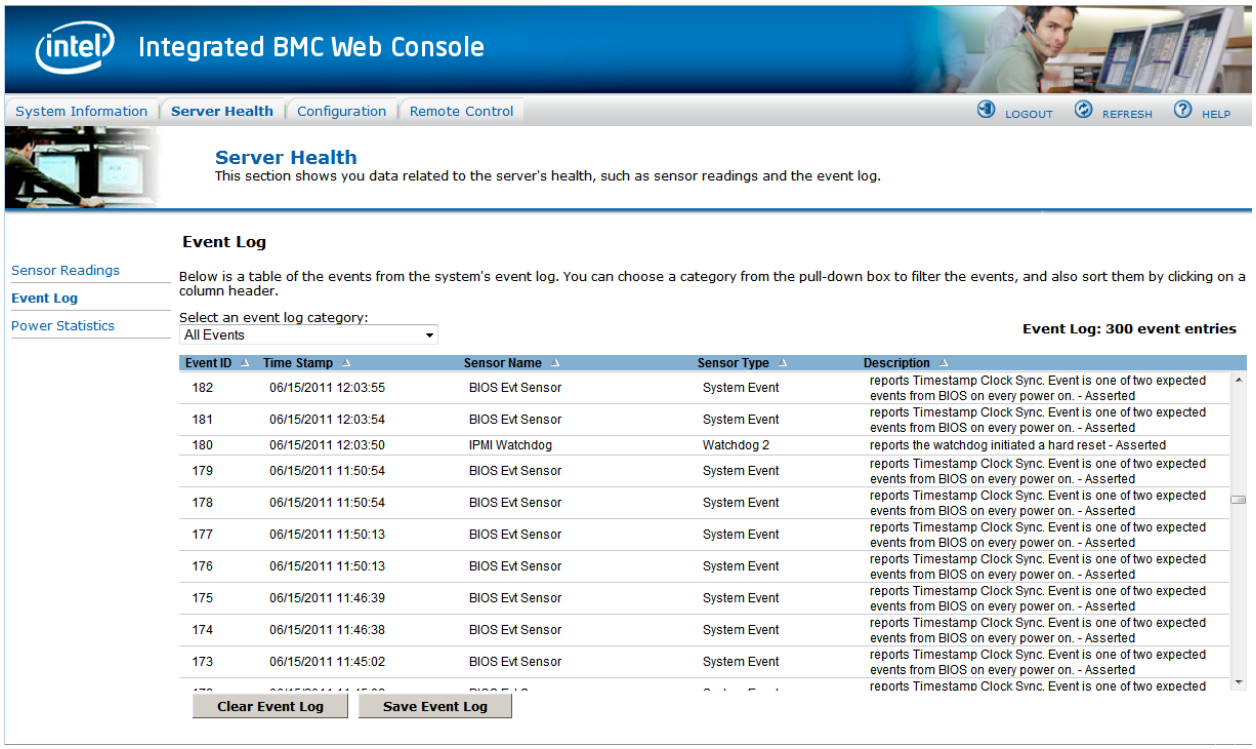

Figure 65: Server Health Event Log Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.2.3 Power Statistics Page

The Power Statistics page displays the systems power statistics in watts as shown in Figure 66.

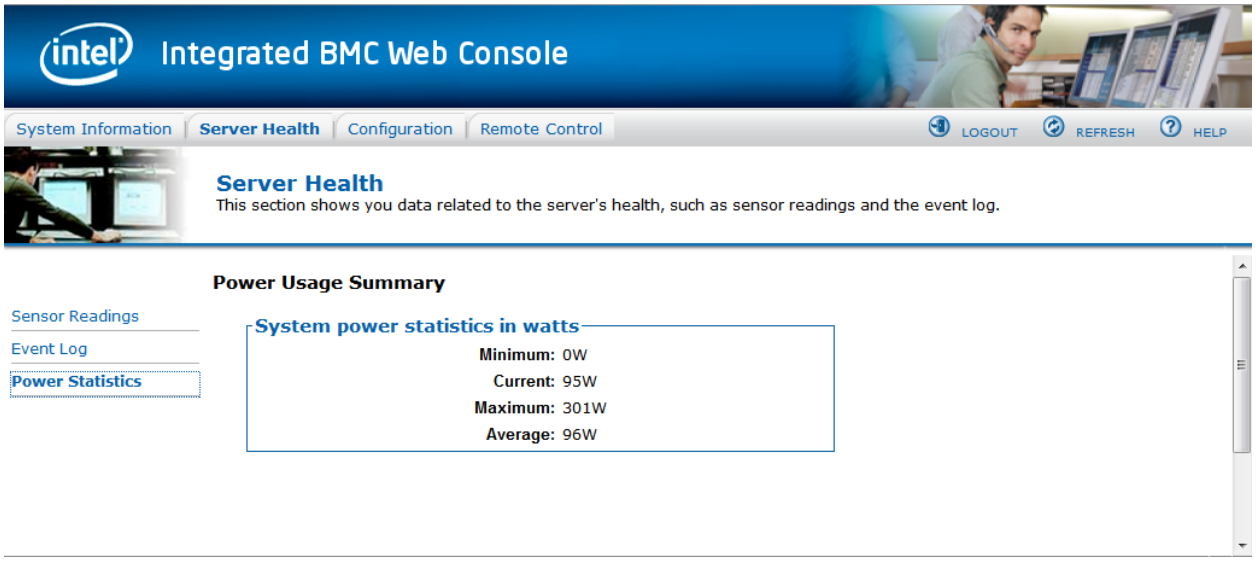

Figure 66: Server Health Power Statistics Page

7.3 Configuration Tab

The Configuration tab is used to configure various settings such as IPv4 Network, Users Login, LDAP SSL, Remote Session, Mouse Mode, Keyboard Macros, Alerts, and Alert Email as discussed in the following subsections. In addition on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families IPv6, VLAN, and Node Manager can also be configured.

Click on the Configuration tab to select the various pages. By default, this tab opens the Network Settings page or the IPv4 Network page.

7.3.1 Network or IPv4 Network Page

The Network or IPv4 settings page is used to configure the IPv4 network settings for the server management LAN interface to the BMC controller. See Figure 67 or Figure 68 for details.

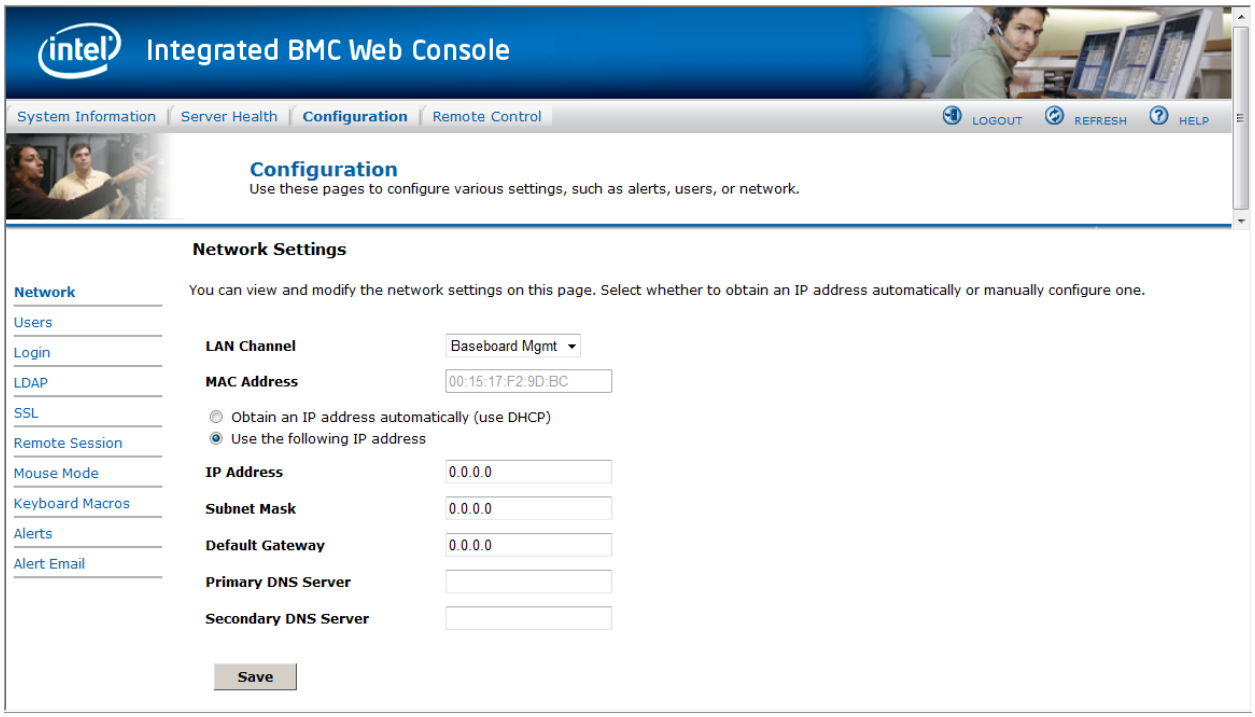

Figure 67: Configuration Network Settings Page on S1200BTL platforms

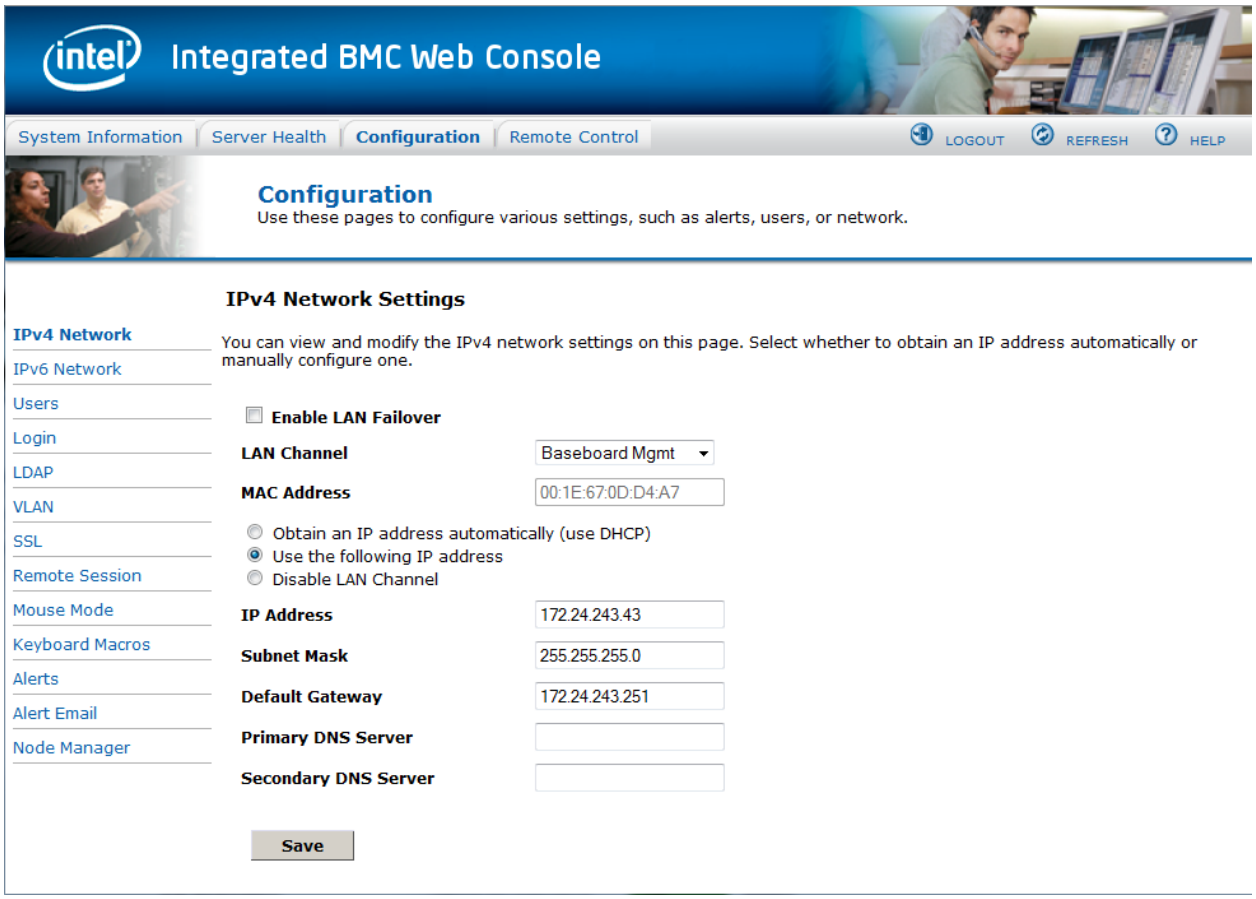

Figure 68: Configuration IPv4 Network Settings Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

⚠ WARNING

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

⚠ WARNING

When LAN failover is enabled the system administrator should 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.

The following table lists the options available in this page:

Table 13: Configuration IPv4 Network Settings Options

Option	Task
Enable LAN Failover	Used to enable LAN Failover (only available on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families)

Option	Task
LAN Channel drop-down box	Used to select the Channel that you would like to configure the network settings. Lists the LAN Channel(s) 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 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)
IP address radio buttons	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 – Will set 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. IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". 'xxx' ranges from 0 to 255 First 'xxx' must not be 0
Primary DNS Server **Secondary DNS Server**	If configuring a Dynamic IP, enter the Primary and Secondary DNS servers.
Save button	Click to save any changes made.

7.3.2 IPv6 Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The IPv6 settings page is used to enable and configure the IPv6 network settings. You can also enable and configure LAN Failover on this page See Figure 69 for details.

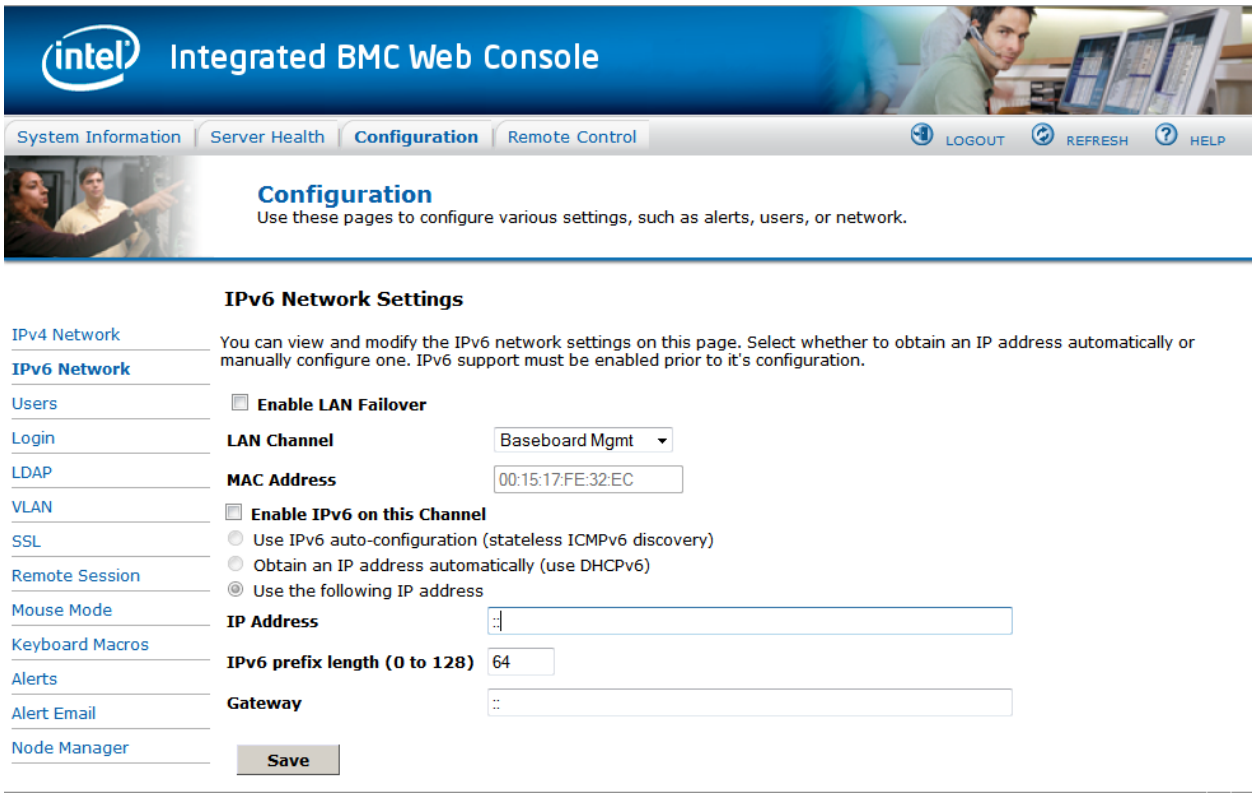

Figure 69: Configuration IPv6 Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

⚠ WARNING

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

⚠ WARNING

When LAN failover is enabled the system administrator should 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.

The following table lists the options available in this page:

Table 14: Configuration IPv6 Network Settings Options

Option	Task
Enable LAN Failover	Used to enable LAN Failover.
LAN Channel drop-down box	Used to select the Channel that you would like to configure the network settings. Lists the LAN Channel(s) available for server management. The LAN channels describe the physical NIC connection on the server. • Intel® RMM (BMC LAN Channel 3) is the add-in RMM4 NIC. • Baseboard Mgmt (BMC LAN Channel 1) is the onboard, shared NIC configured for management and shared with the operating system. • Baseboard Mgmt 2 (BMC LAN Channel 2) is the second onboard, shared NIC configured for management and shared with the operating system.
MAC Address	The MAC address of the device (read only).
Enable IPv6 on this channel selection box	Used to enable IPv6 on the channel selected in the LAN channel drop down box.
IP address radio buttons	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. IP Address and Gateway are 128 bit fields made of 8 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 (: :).
IPv6 prefix length (0 to 128)	Selects the routing prefix length.
Save button	Click to save any changes made.

7.3.3 Users page

The User List page lists the configured users, along with their status and network privilege. It also provides the capability to add, modify, and delete users. See Figure 70 for details.

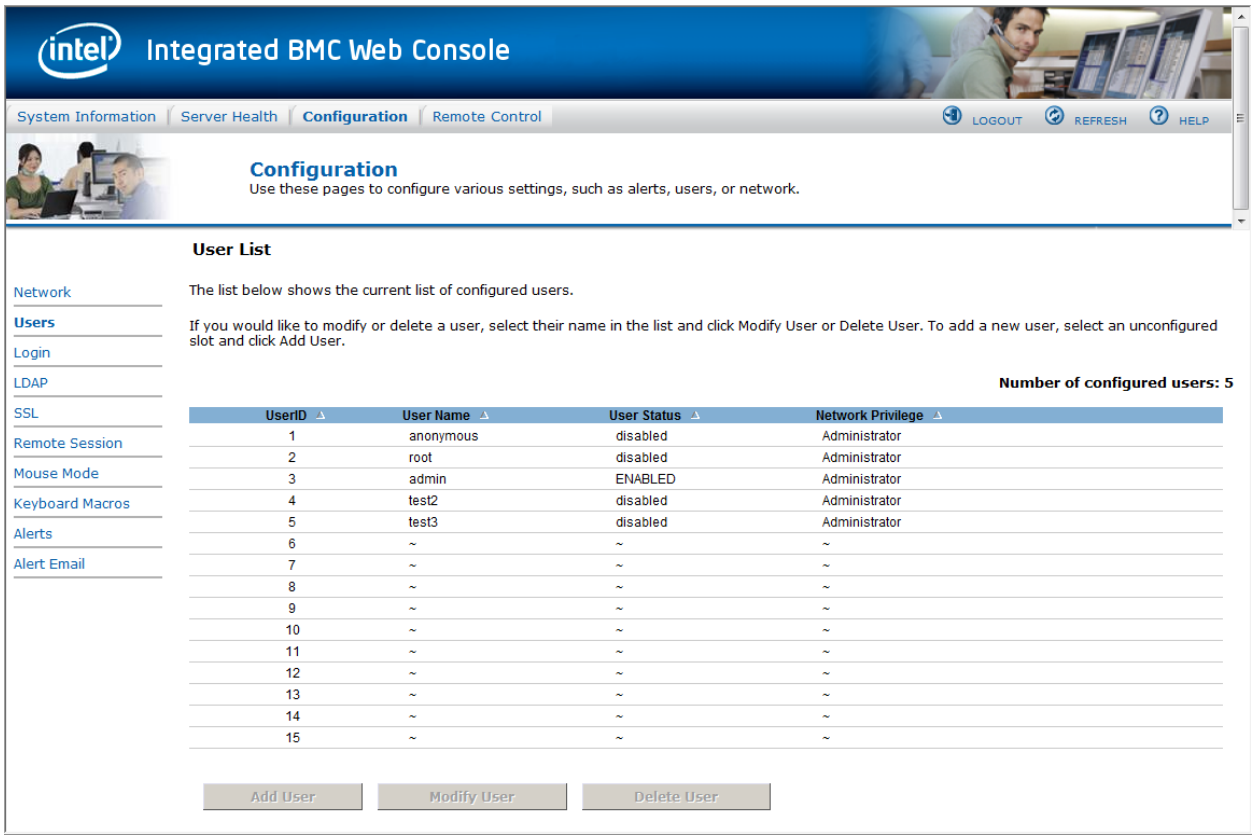

Figure 70: Configuration User List Page

This page allows the operator to configure the IPMI users and privileges for this server:

- UserID 1 (anonymous) may not be renamed or deleted.
- UserID 2 (root) may not be renamed or deleted; nor can the network privileges of UserID 2 be changed.
- User Names cannot be changed. To rename a User you must first delete the existing User, and then add the User with the new name.

To delete a user, select the user in the list and click **Delete User**.

To add a user, select an empty slot in the list and click **Add User**. This allows you to set the User Name, Password, and Network Privileges as shown in Figure 71.

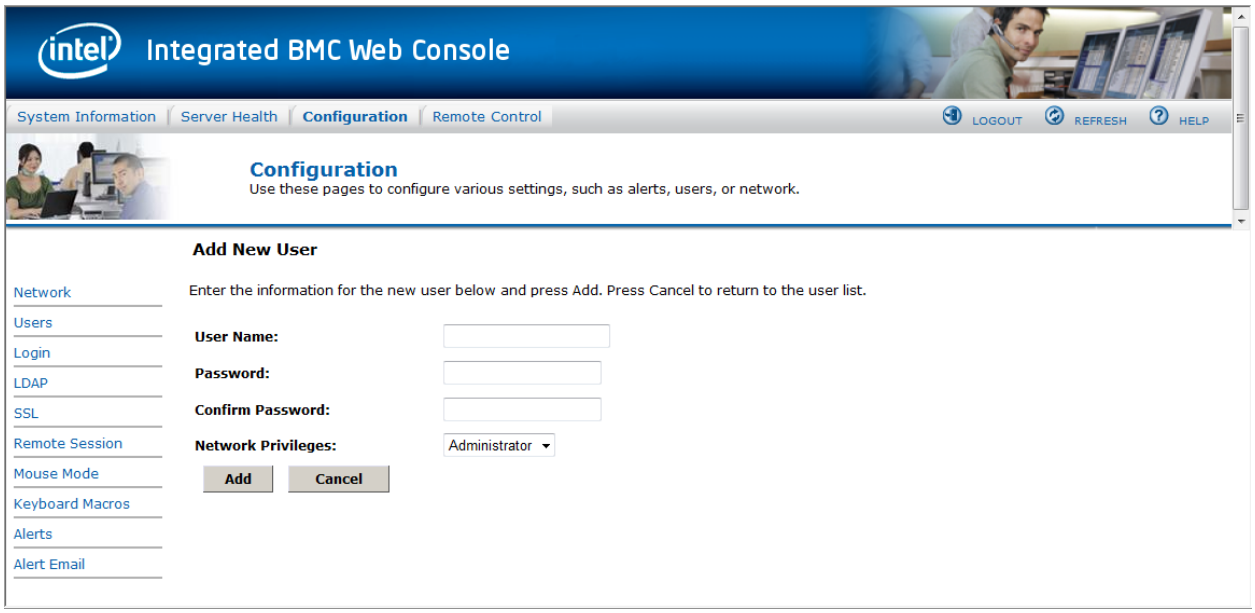

Figure 71: Configuration Users Add User Page

To modify a user, select a user in the list and click Modify User. This allows you to change the Password, Enable Access, and change Network Privileges as shown in Figure 72.

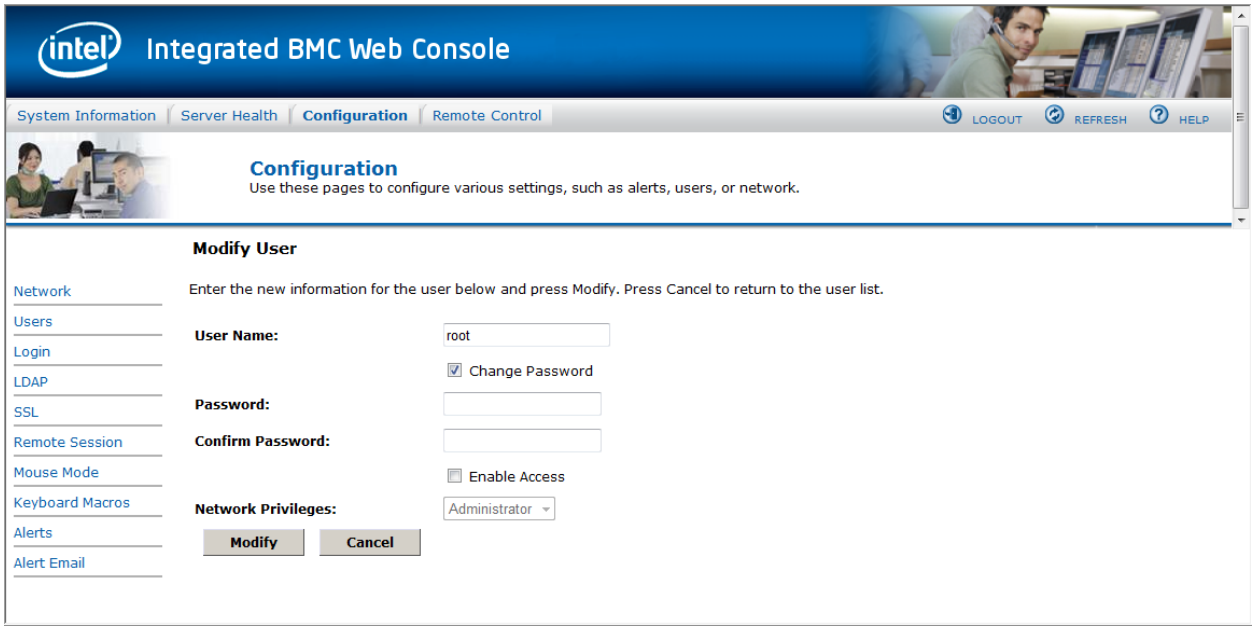

Figure 72: Configuration Users Modify User Page

7.3.4 Login Security Settings Page

Users can be locked out if they supply incorrect passwords too many times in a row. This is a security feature to prevent brute force hacking attacks. Only that user is locked out – other users can still login.

The number of failed attempts before being locked out is configurable; as is the length of time the lockout lasts.

To turn the feature off, set the lockout time to zero. Three default failures will lockout a user for one minute.

Press the **Save** button to save any changes.

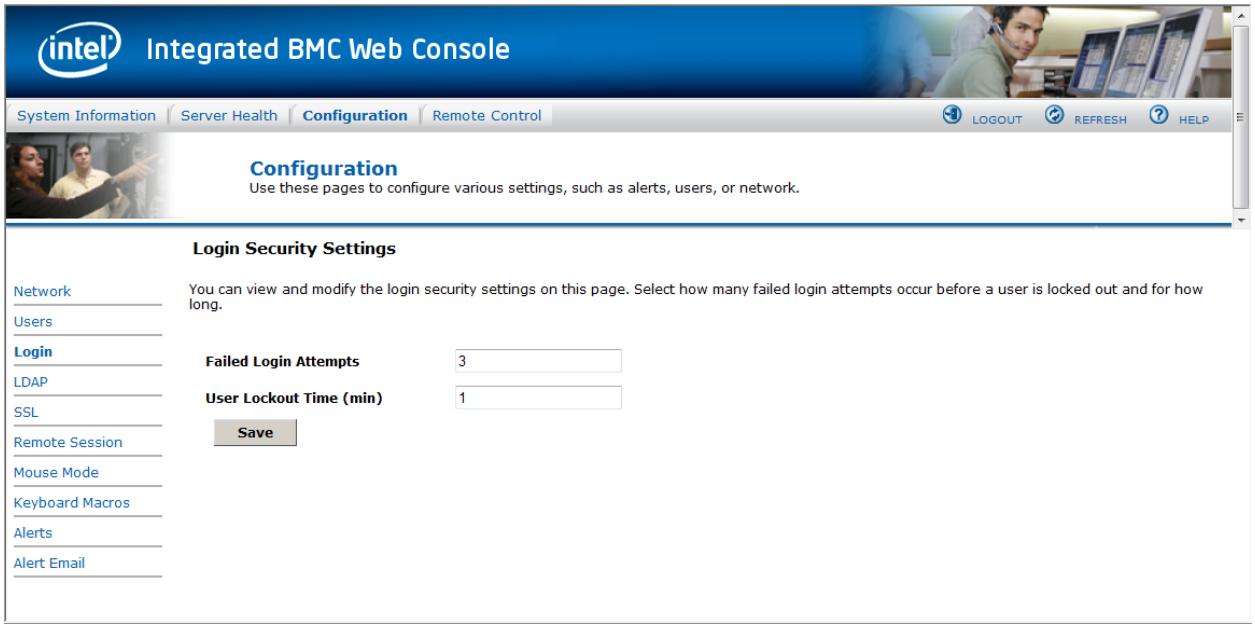

Figure 73: Configuration Login Security Settings Page on S1200BTL platforms

For EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families you can also force the interface to HTTP Secure mode by selecting the **Force HTTPS – Enable** check box. See Figure 74 for details.

In addition the **Web Session Timeout** that locks the web session after a specified time of inactivity can be changed from the default of 30 minutes (1800 seconds) by entering a new value for the number of seconds to wait before locking out the web session.

Click the **Save** button to save any changes.

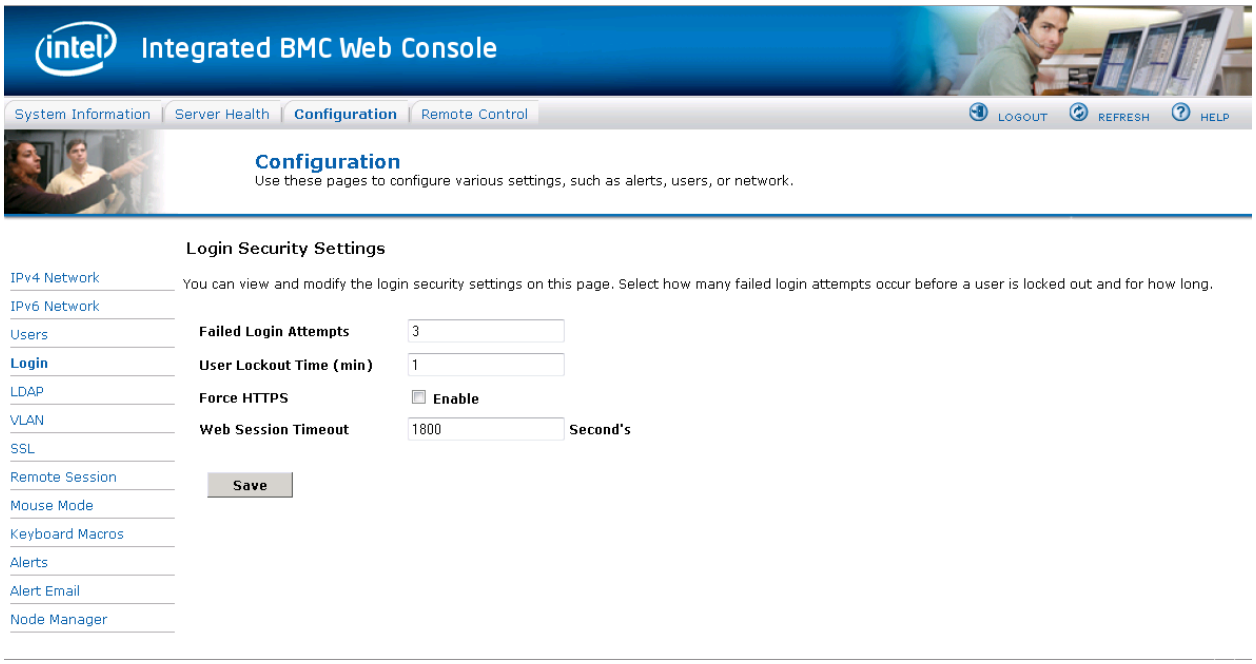

Figure 74: Configuration Login Security Settings Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.3.5 LDAP Settings Page

To enable/disable LDAP, check or uncheck the **Enable LDAP Authentication** checkbox respectively.

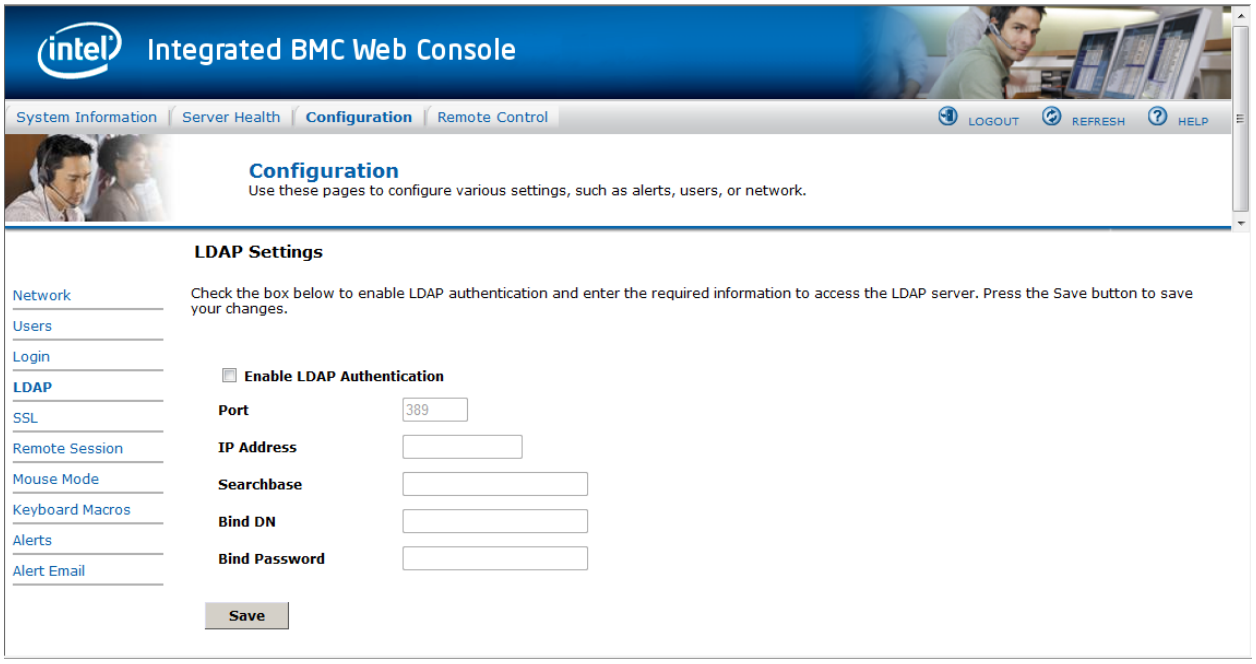

Figure 75: Configuration LDAP Settings Page

The following table lists the options available in this page:

Table 15: Configuration LDAP Settings Options

Option	Task
Enable LDAP Authentication	Check this box to enable LDAP authentication, then enter the required information to access the LDAP server.
Port	Specify the LDAP Port
IP Address	The IP address of LDAP server IP Address made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx" 'xxx' ranges from 0 to 255 First 'xxx' must not be 0
Searchbase	The searchbase of the LDAP server, for example, "dc=my-domain, dc=com"
Bind Password	Authentication password for LDAP server; the password must be at least 4 characters long
Bind DN	The Distinguished Name of the LDAP server, such as, "cn=Manager, dc=my-domain, dc=com"
Save button	Click to save the current settings

7.3.6 VLAN Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families this page is used to enable and configure the VLAN private network settings on the selected server management LAN channels.

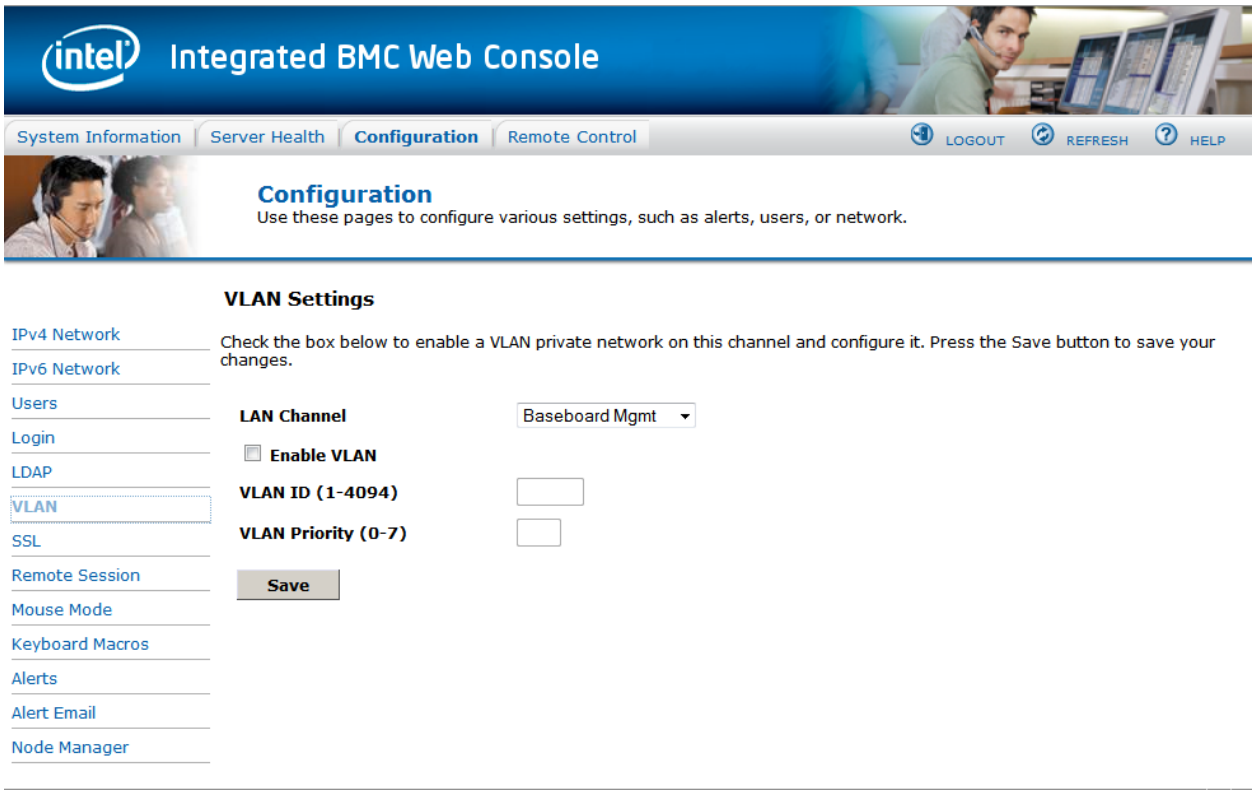

Figure 76: Configuration VLAN Settings on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The following table lists the options available in this page:

Table 16: Configuration VLAN Settings Options

Option	Task
LAN Channel drop-down box	Lists the LAN Channel(s) 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	Used to enable VLAN for the LAN channel selected in the drop down box.
VLAN ID (1 – 4094)	Used to set the VLAN ID.

Option	Task
VLAN Priority (0 – 7)	Used to set the VLAN Priority.
Save button	Click to save the current settings

7.3.7 SSL Upload Page

Use this page to upload an SSL certificate and privacy key, which allows the device to be accessed in secured mode.

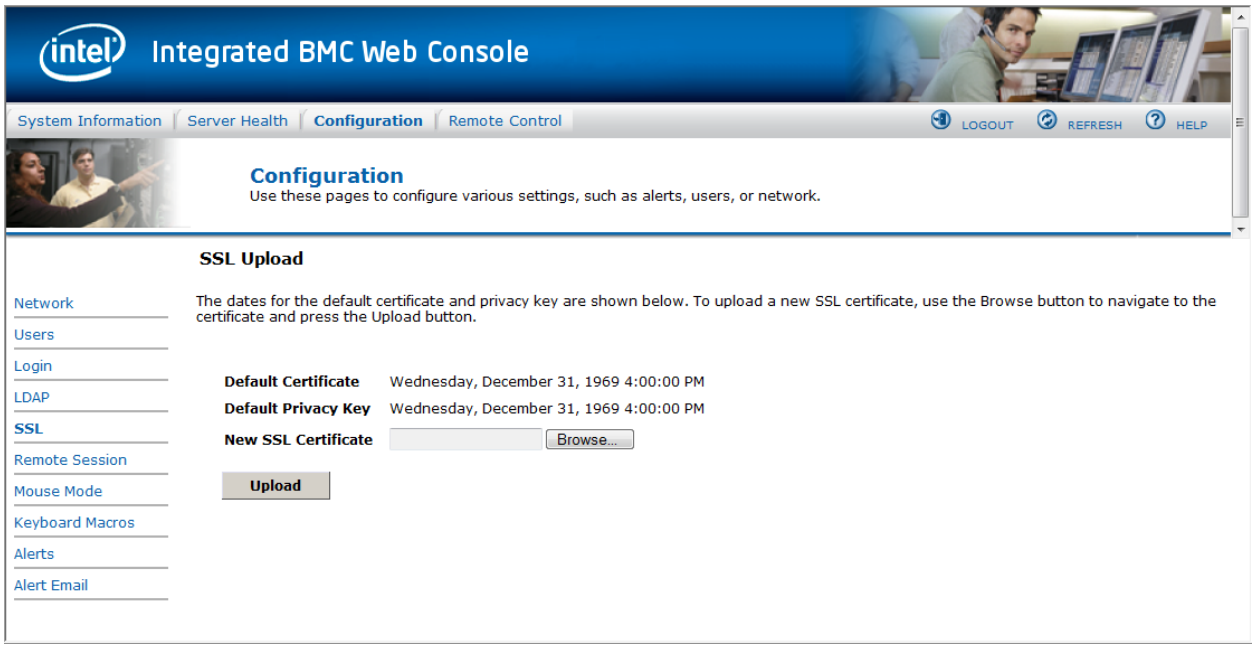

Figure 77: Configuration SSL Upload Page

First upload the SSL certificate and then the device will prompt to upload privacy key. If either of the files is invalid the device will notify. The device will give notification on Successful upload. On successful upload, device will prompt to reboot the device. If you want to reboot click **Ok** or click **Cancel** to cancel the reboot operation.

First upload the SSL certificate and then the device will prompt to upload the privacy key. Click the **Upload** button. On successful upload, a notification appears.

7.3.8 Remote Session Page

Use this page to enable/disable encryption on KVM or Media during a redirection session. Figure 78 shows the details for a S1200BTL system.

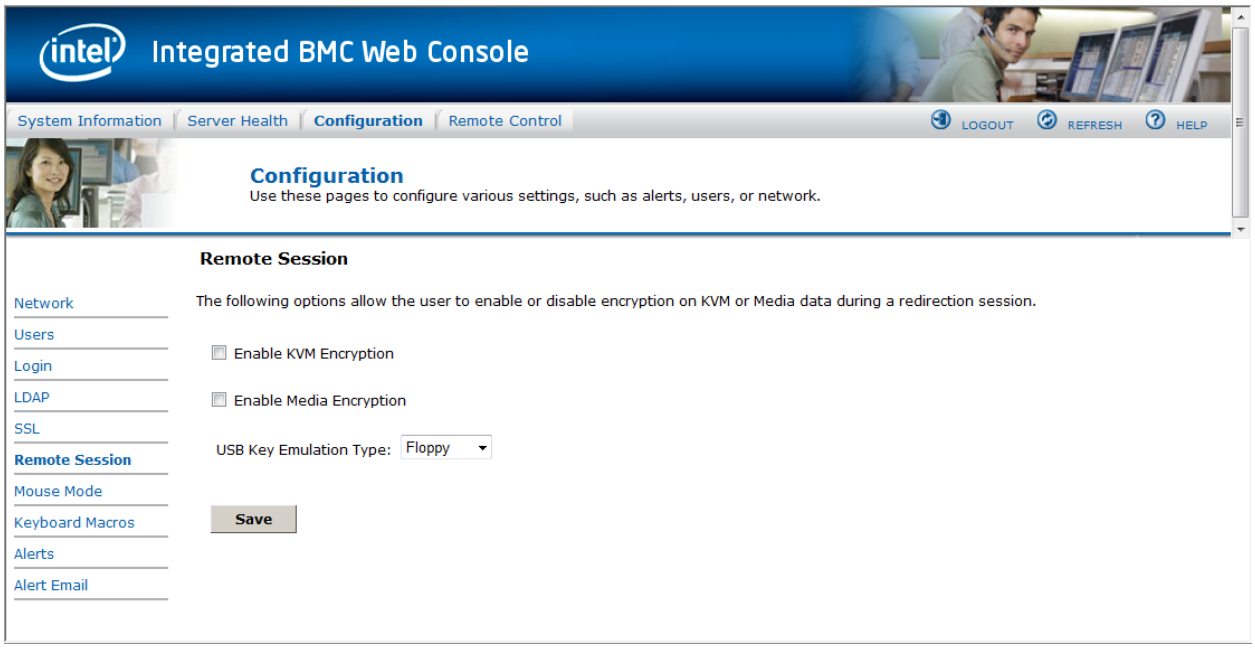

Figure 78: Configuration Remote Session Page on S1200BTL platforms

The following table lists the options allowing you to enable or disable encryption on KVM or media data, and the USB Key Emulation type selection used during a redirection session:

Table 17: Configuration Remote Session Options

Option	Task
Enable KVM Encryption **Enable Media Encryption**	Enable/Disable encryption on KVM or Media data during a redirection session. **Note**: KVM and Media encryption are enabled by default. **Note**: Disabling encryption can improve performance of KVM or Media redirection.
USB Key Emulation Type	Select Floppy or Hard Disk emulation.
Save button	Click to save any changes.

On an EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families you can select the Encryption mode and separately enable/disable keyboard/mouse and Media encryption. See Figure 79 for details.

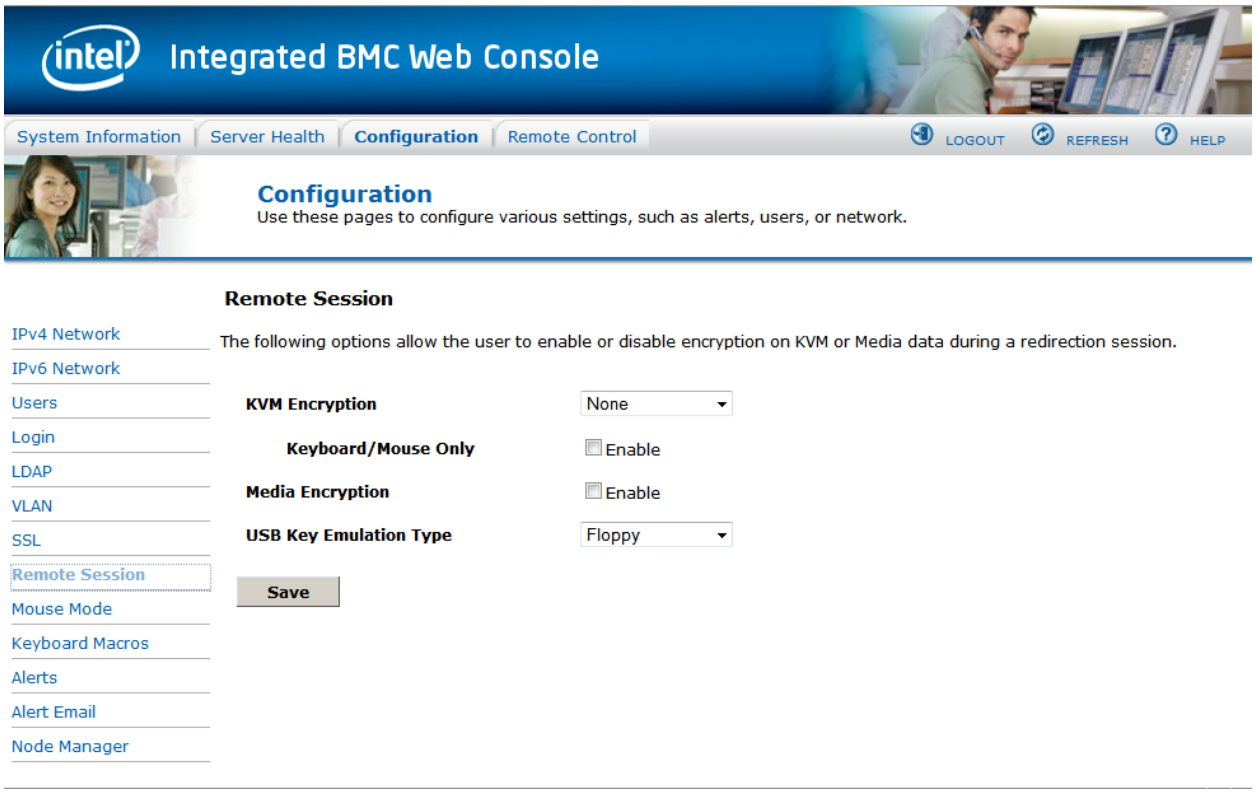

Figure 79: Configuration Remote Session Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The following table lists the options allowing you to enable or disable encryption on KVM or media data, and the USB Key Emulation type selection used during a redirection session:

Table 18: Configuration Remote Session Options

Option	Task
KVM Encryption mode	Disable or select encryption mode on KVM or Media data during a redirection session. Choose any one from the supported encryption techniques (None, Stunnel*, RC4, or AES) **Note**: KVM and Media encryption are enabled by default. **Note**: Disabling encryption can improve performance of KVM or Media redirection.
Keyboard/Mouse Only	If KVM Encryption is set to None, the Keyboard and Mouse data can still be encrypted using Blowfish encryption. **Note**: This option has the least performance impact while still encrypting the most important data.
Media Encryption	Enable/Disable encryption of Media data during a redirection session. **Note:** Disabling encryption can improve performance of KVM or Media redirection.

Option	Task
USB Key Emulation Type	Select Floppy or Hard Disk emulation.
Save button	Click to save any changes.

7.3.9 Mouse Mode Page

Use this page to select the Mouse Mode used during a Remote KVM session.

On a S1200BTL system the Redirection Console handles mouse emulation from local window to remote screen in either of two methods. Figure 80 shows the details.

- **Absolute Mode**. Select to have the absolute position of the local mouse sent to the server. Use this mode for Microsoft Windows* OS.
- **Relative Mode**. Select Relative Mode to have the calculated relative mouse position displacement sent to the server. Use this mode for Linux* OS.

Click **Save** to use selected mode.

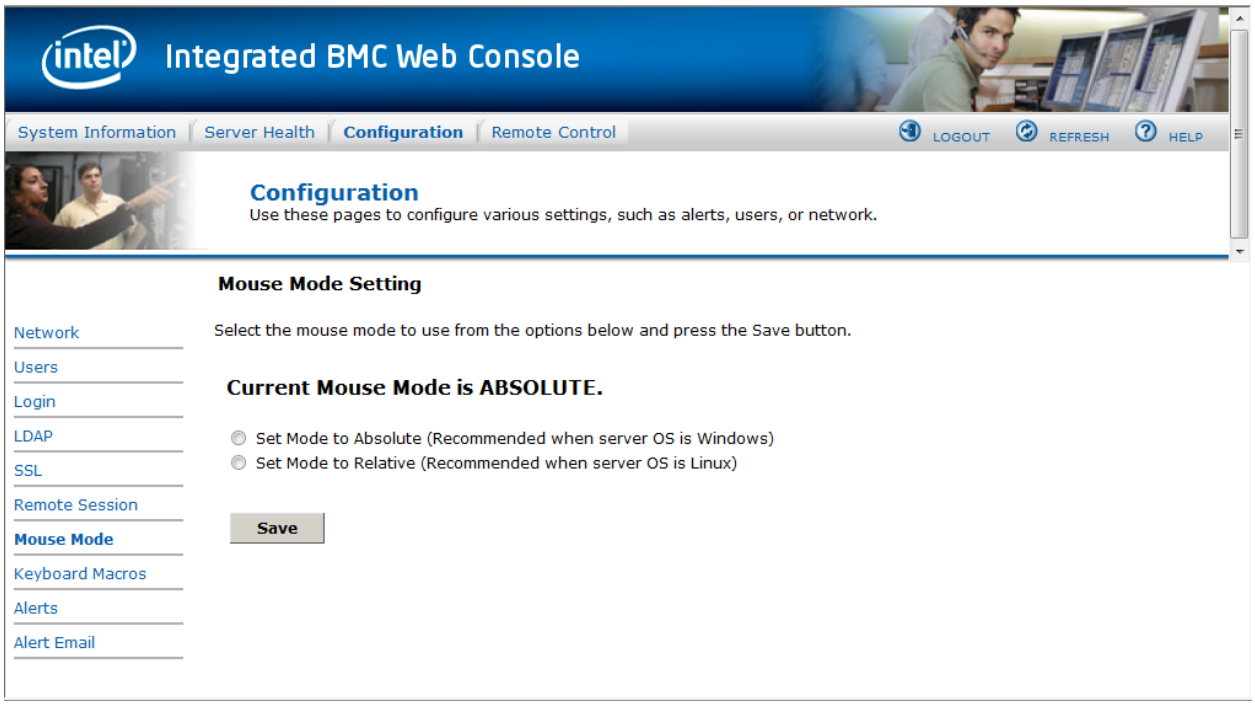

Figure 80: Configuration Mouse Mode Setting Page on S1200BTL platforms

On an EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families the Redirection Console handles mouse emulation from local window to remote screen in either of three methods. Figure 81 shows the details.

- **Absolute Mode**. Select to have the absolute position of the local mouse sent to the server. Use this mode for Windows* and newer Red Hat* Linux versions (RHEL 6.x).

- **Relative Mode**. Select Relative Mode to have the calculated relative mouse position displacement sent to the server. Use this mode for other Linux* versions such as SUSE (SLES) and older versions of Red Hat* (RHEL 5.x). For best results, server OS mouse acceleration/threshold settings can be reduced, or use mouse calibration in the remote console window.
- **Other Mode.** Select Other Mode to have the calculated displacement from the local mouse in the center position, sent to the server. Under this mode ALT+C should be used to switch between Host and client mouse cursor. Use this mode for SLES 11 Linux* OS installation. See section 7.3.9.1 for more details on this mode.

Click **Save** to use selected mode.

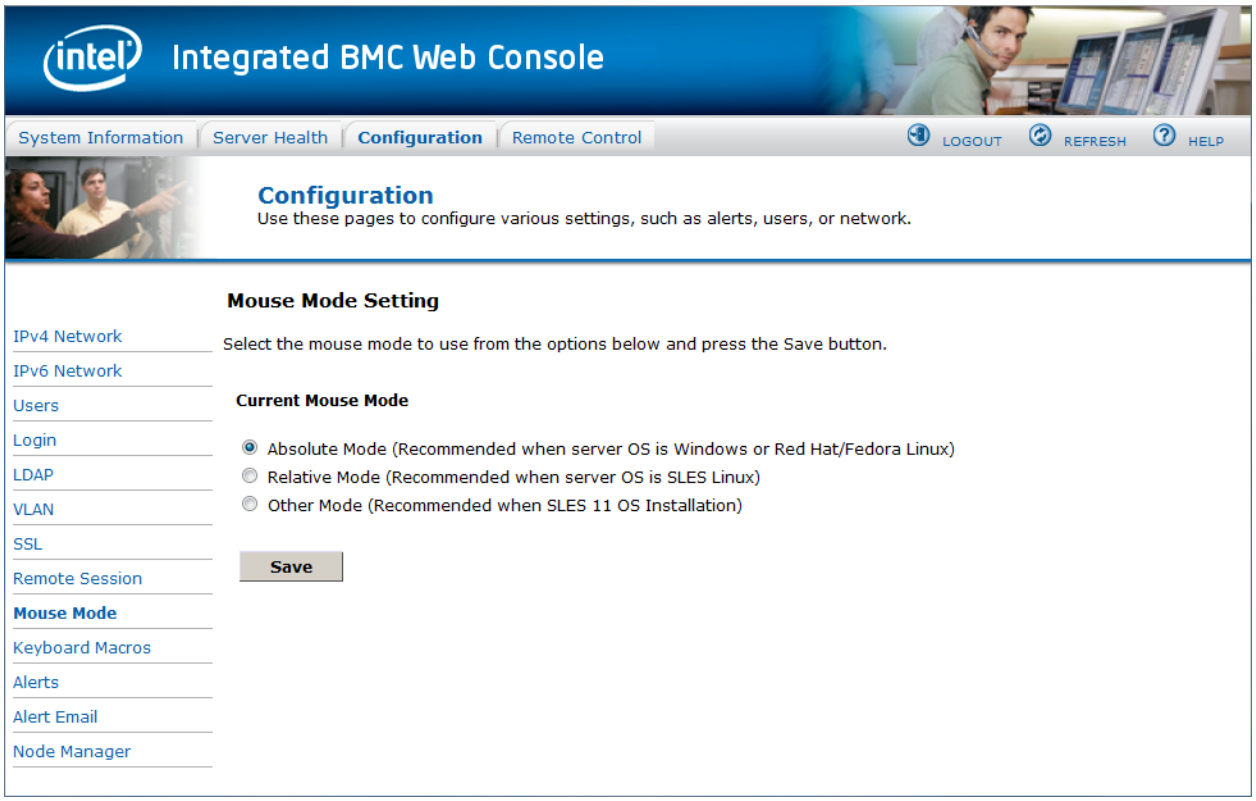

Figure 81: Configuration Mouse Mode Setting Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.3.9.1 Mouse Mode Setting – Other Mode Description

This mode should only be used for a SLES* 11 OS installation, and once this has been completed, the Mouse Mode Setting should be changed to the suggested Relative Mode for use within the SLES 11 OS.

In this mode, the KVM window will be maximized to the full screen. Note that the windows resizing button in the top right corner is grayed out.

To use the mouse within the KVM window you must press ALT-C. The first time that Alt-C is pressed the mouse should appear close to the center of the window. Pressing Alt-C after that

will switch between using the mouse within the KVM window and using the mouse on your host system. The mouse in the KVM window will remain in the last position that it was at when the operation is switched between the KVM Window, to the host system, and then back to the KVM window. There is a reminder of using Alt-C key in the Remote Console control bar to the left of the keyboard macros. See Figure 82 for details. During installation, the mouse response in the KVM will be slow. This is normal and expected.

Note: If the top bar of the KVM window is double clicked, the window will be resized. If this occurs, since there is no resize window button, the operator can use the Remote Console Control Bar to select Video and then perform a Full Screen (or press Alt –F) operation to go to the full screen mode.

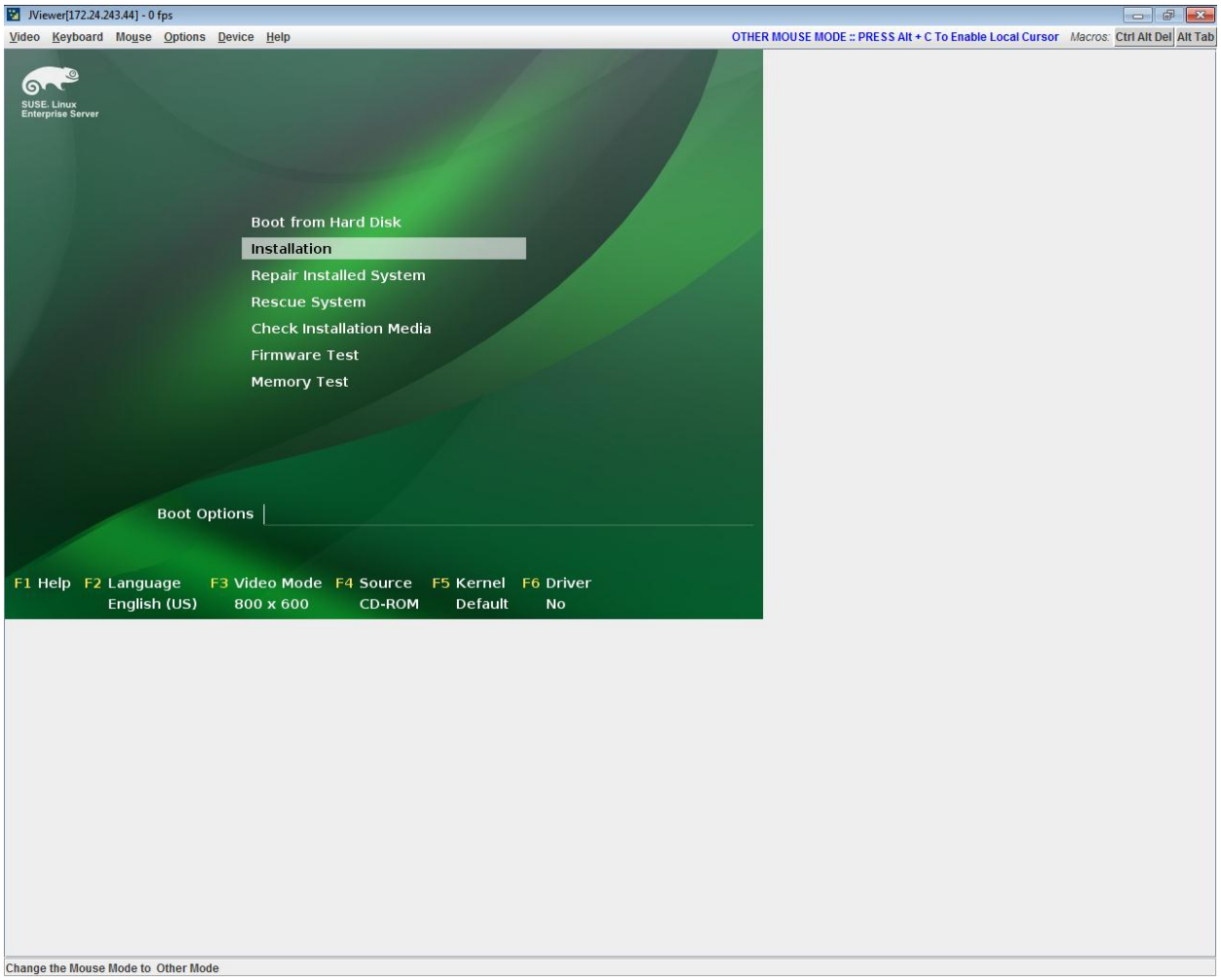

Figure 82: KVM window with Mouse Other Mode selected on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.3.10 Keyboard Macros Page

Macro buttons can be defined on this page that will appear in the upper right corner of the KVM Remote Console application window. Each button is assigned a sequence of keys to execute when the button is clicked.

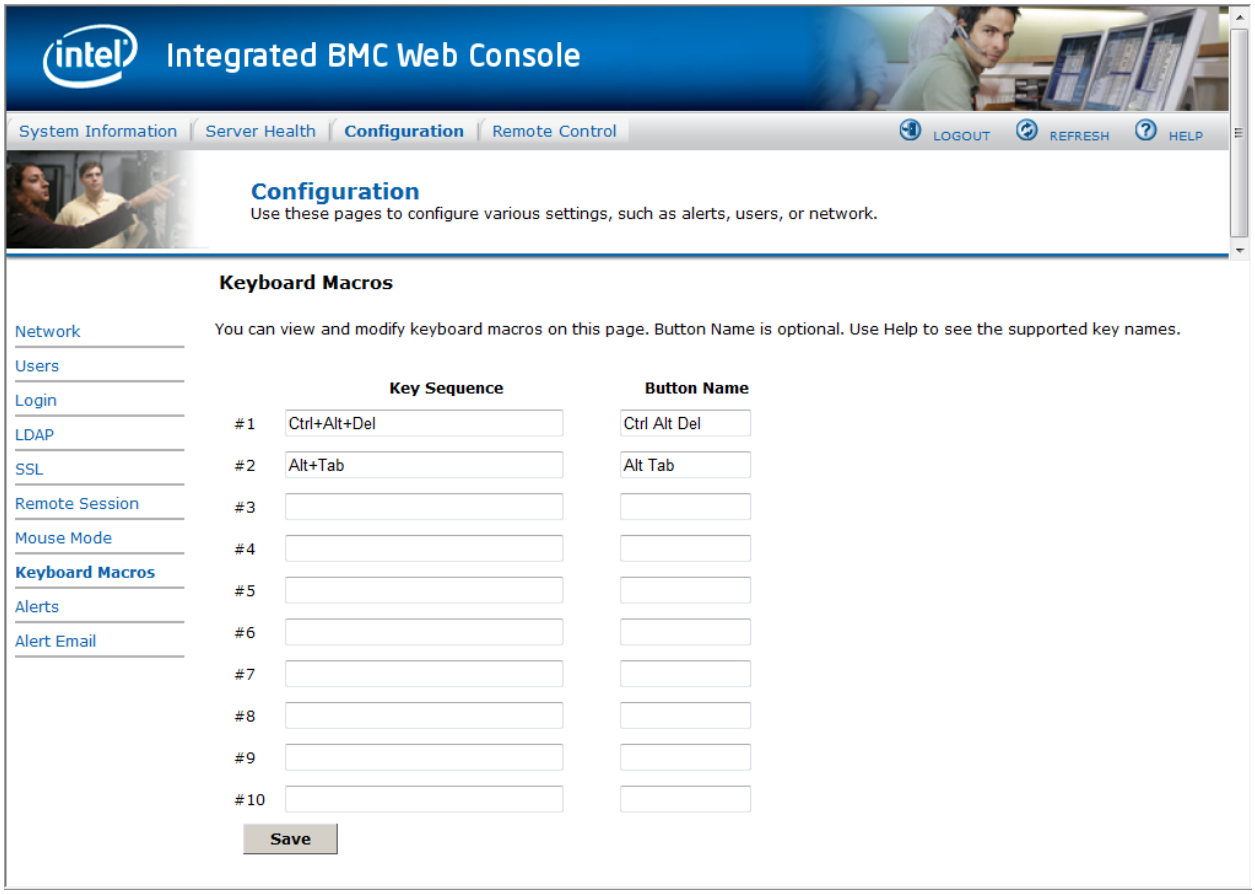

Figure 83: Configuring Keyboard Macros Page

This makes it convenient to quickly do oft repeated typing as well as execute key combos that aren't possible directly from the local client keyboard. Alt and Win key combos such as Ctrl+Alt+Del get interpreted by the local client OS and aren't passed through to the remote target OS. However, a macro can be set up to take care of this.

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

You must save changes before they take effect. If a Remote Console session is open at that time you will not see the changes until that session is closed and a new session is opened.

7.3.10.1 Key Sequences

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

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

Key names are either a printable character such as a, 5, @, and so on or else 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 Numlock as well as the target OS keyboard language setting.

Table 19: 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)	

7.3.11 Alerts Page

Use this page to configure which system events an alert should be sent for and the destination for the alerts. Up to two destinations can be selected for each LAN channel. Figure 84 shows the details for a S1200BTL system.

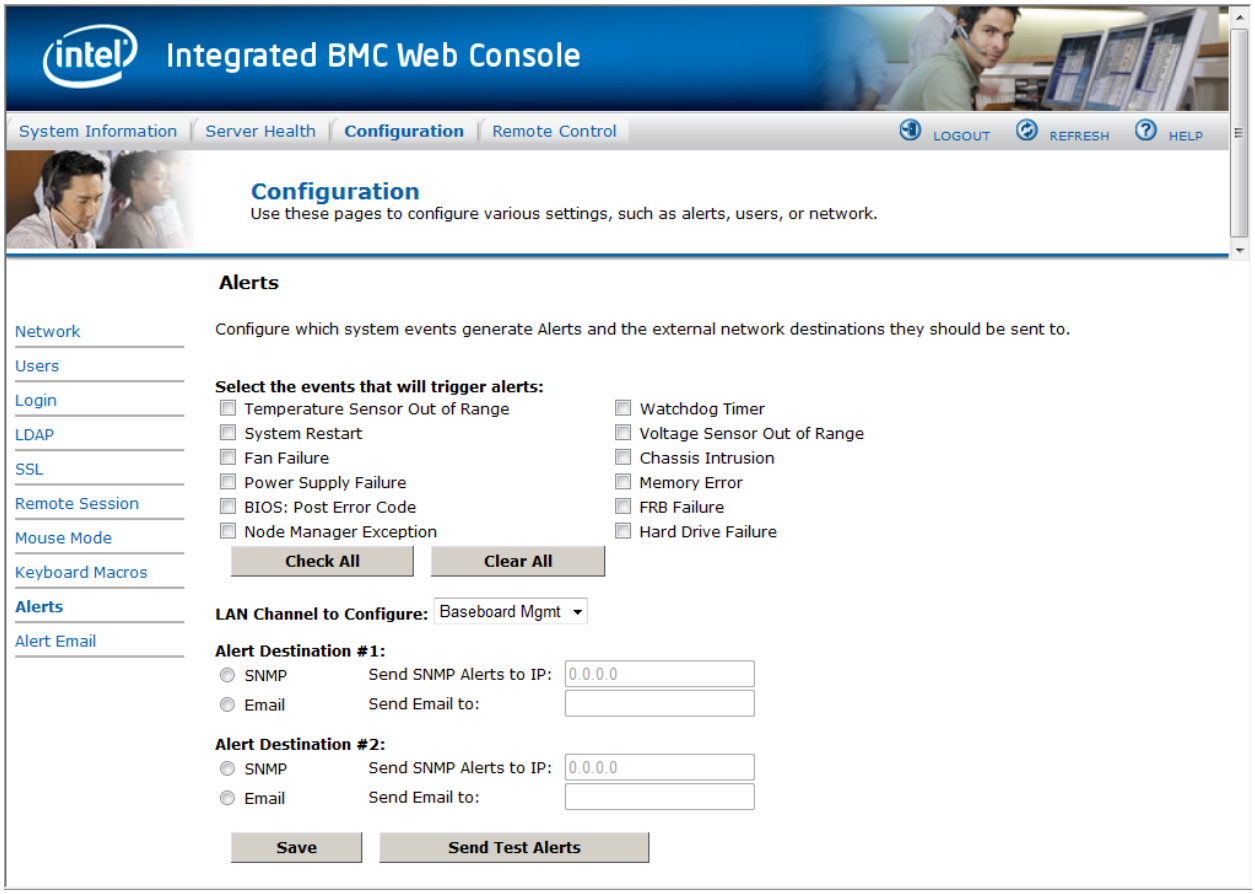

Figure 84: Configuration Alerts Page on S1200BTL platforms

The following table lists the options allowing you to select the events that alerts should be sent on and selection of where the alerts are to be sent:

Table 20: Configuration Alerts Options

Option	Task
Select the events that will trigger alerts.	Select one or more system events that will trigger an alert.
Check/Clear All buttons	Click to select or clear all events.
LAN Channel to Configure	Select either the BMC or RMM4 to configure the destination.

Option	Task
Alert Destination #1/#2	Select either SNMP along with the IP address or email address that the alert should be sent to. Up to two destinations can be selected for each LAN channel.
Save button	Click to use selected setup.
Send Test Alerts button	After configuring select this to send a test alert.

On an EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families there is an additional option to **Globally Enable Platform Event Filtering**. This can be used to prevent sending alerts until you have fully specified your desired alerting policies. See Figure 85 for details.

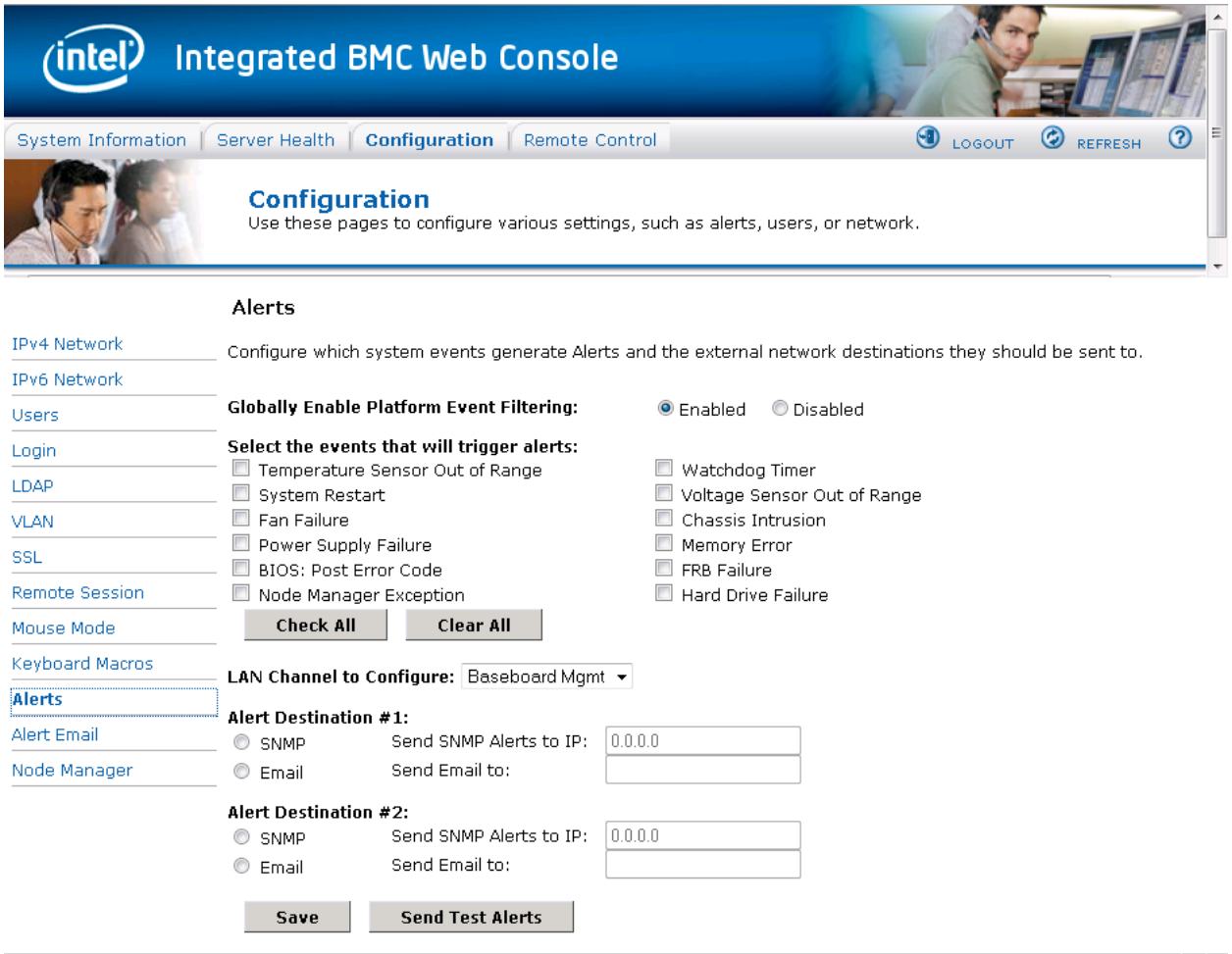

Figure 85: Configuration Alerts Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

7.3.12 Alert Email Page

Use this page to configure the parameter for Alert Emails.

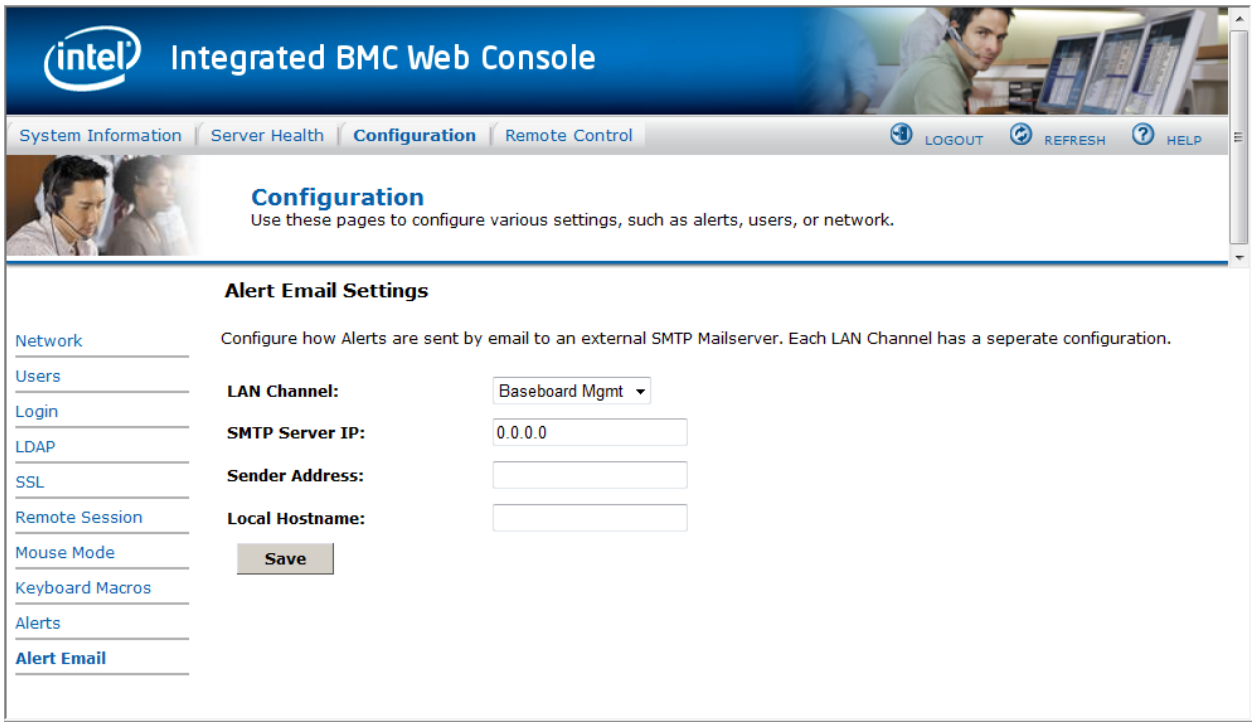

Figure 86: Configuration Alert Email Page

Table 21: Configuration Alert Email Options

Option	Task
LAN Channel	Select either the BMC or RMM4 to configure destination for.
SMTP Server IP.	The IP address of the remote SMTP Mail server that Alert email should be sent to. • IP Address is made of 4 numbers separated by dots as in "xxx.xxx.xxx.xxx". • 'xxx' ranges from 0 to 255. • First 'xxx' must not be 0.
Sender Address	The Sender address string to be put in the "From:" field of outgoing Alert emails.
Local Hostname	The hostname of the local machine that is generating the alert. It is put into the outgoing Alert email. • The Local Hostname is a string of maximum 31 alpha-numeric characters. • Space, Special Characters are not allowed.
Save button	Click to use selected setup.

7.3.13 Node Manager Power Polices Page on EPSD Platforms Based on Intel® Xeon® Processor E5–4600/2600/2400/1600/1400 Product Families

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families this page is used to view, add, and configure the Node Manager Power Policies.

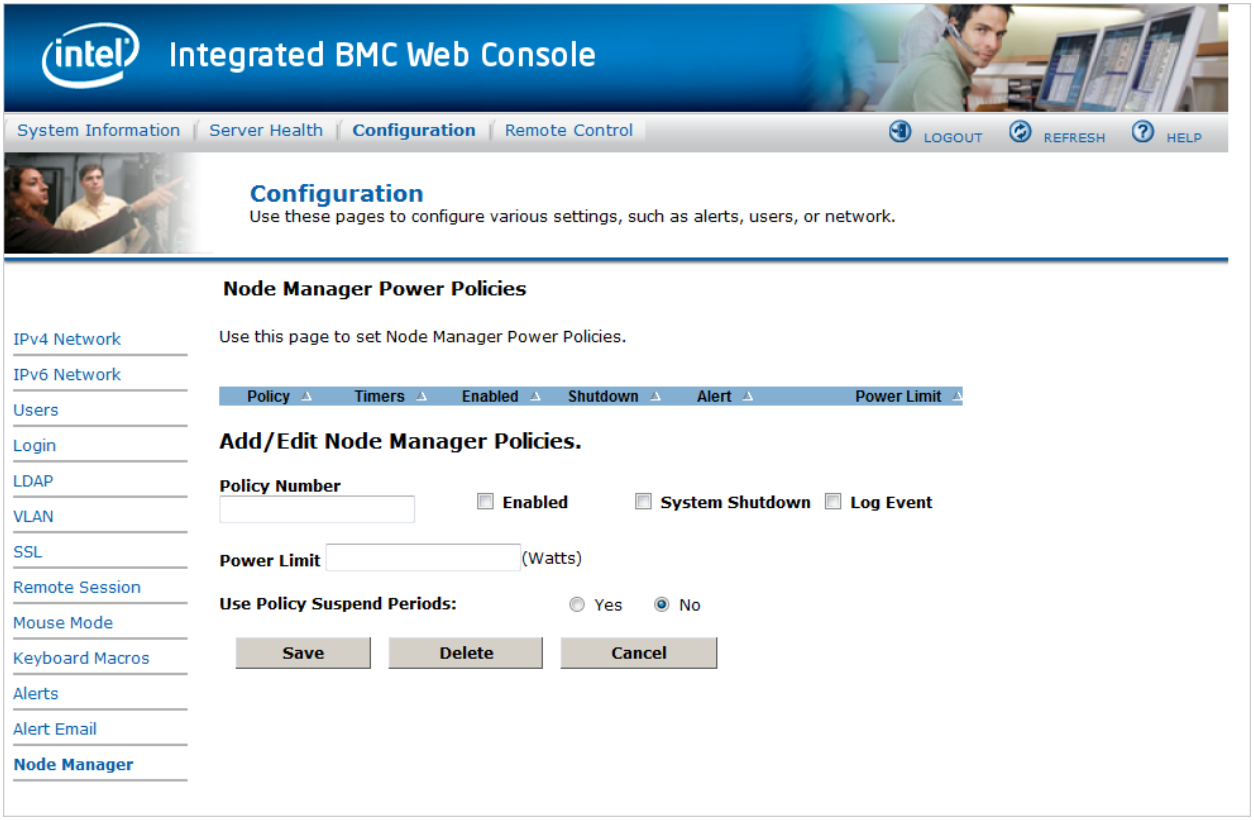

Figure 87: Configuration Node Manager Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The following table lists the options allowing you to view, add, and edit the Node Manager Power Policies:

Table 22: Configuration Node Manager Options

Option	Task
Node Manager Power 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 Number	The policy number to add/edit/delete. Valid range is 0-255. In the policy table, policy numbers 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.

Option	Task
Enabled check box	Check this box if the policy is to be enabled immediately.
System Shutdown check box	Check this box to enable a system shutdown if the policy is exceeded and cannot be corrected within the correction timeout period. The operating system will be given 30 seconds to shut down gracefully. If the system is still not shut down after 30 seconds, the BMC will initiate an immediate shutdown.
Log Event check box	Check this box to enable the node manager to send a platform event message to the BMC when a policy is exceeded.
Power Limit	The desired platform power limit, in watts.
Use Policy Suspend Periods	If enabled, you may configure policy suspend periods. Each policy may have up to five suspend periods (see Figure 88). 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.

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).

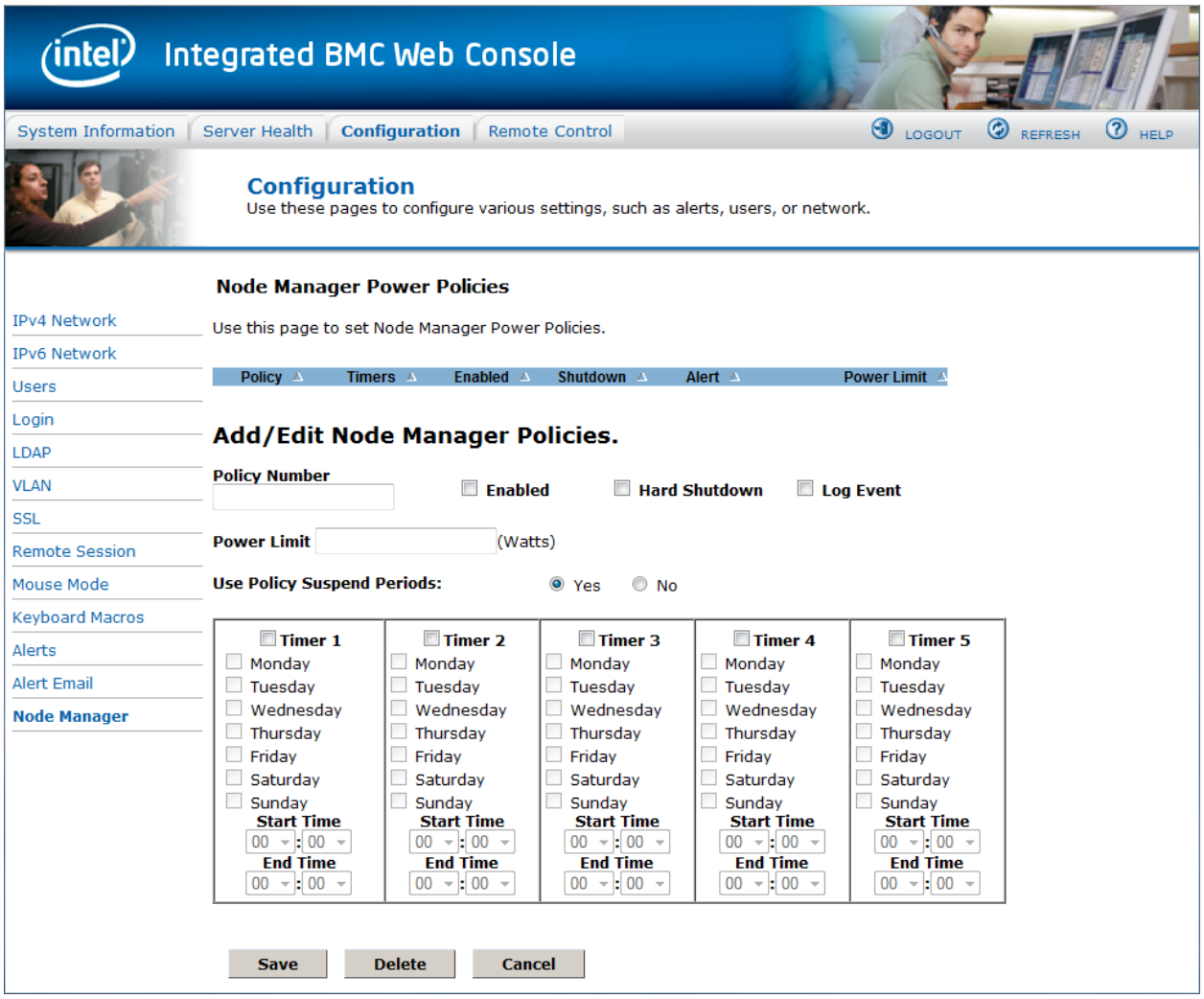

Figure 88: Configuration Node Manager Page with Use Policy Suspend Period selected

7.4 Remote Control tab

The Remote Control tab helps you perform the following remote operations on the server:

- Console redirection
- Server power control

7.4.1 Console Redirection Page

By default, the Remote control tab opens in the Console Redirection page. Launch the remote console KVM redirection window from this page.

Note that the **Launch Console** button will be grayed out and non-functional if the RMM4 Lite is not present.

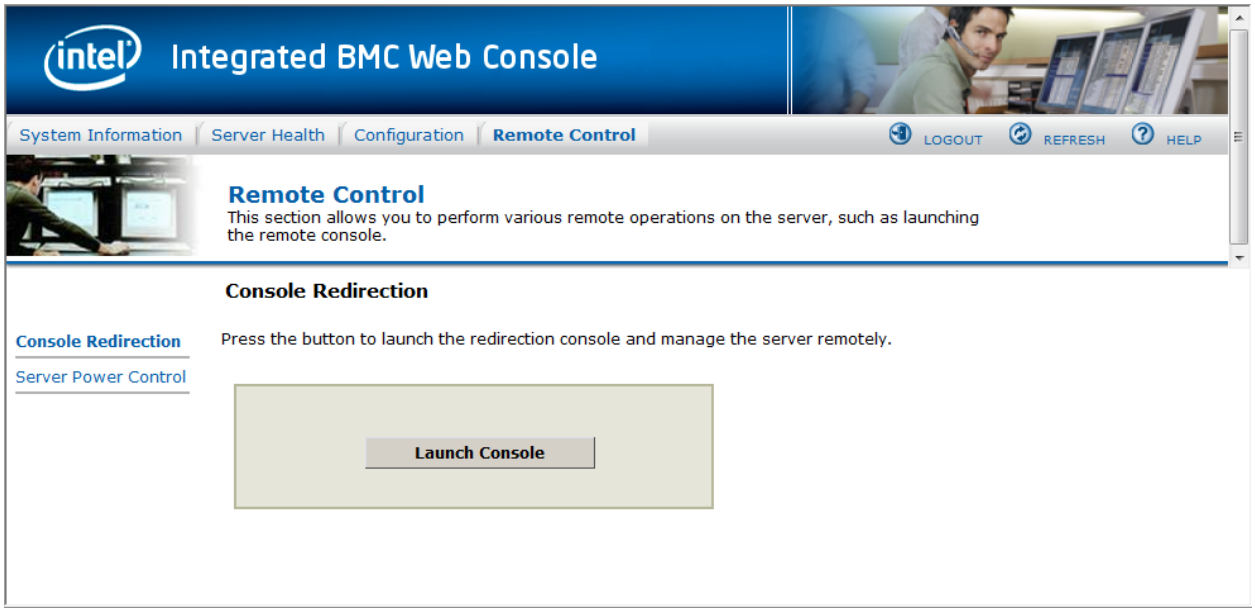

Figure 89: Remote Control Console Redirection Page

Click the **Launch Console** button to launch the redirection console and manage the server remotely.

Note: Java Run-Time Environment* (JRE* Version 6 Update 22 or higher) must be installed on the client prior to launch of JNLP file.

7.4.2 Server Power Control Page

The Server Power Control page shows the power status and allows power/reset control of the server. Figure 90 shows the details for a S1200BTL system.

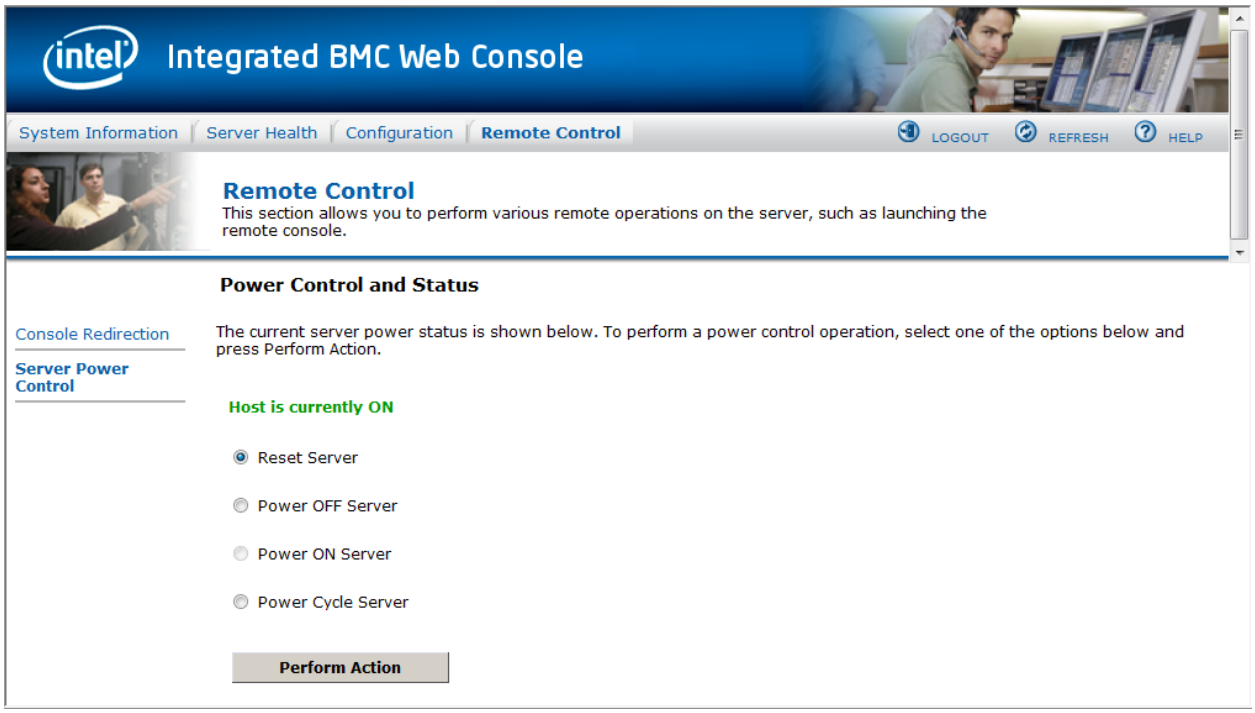

Figure 90: Remote Control Server Power Control Page on S1200BTL platforms

The following power control operations can be performed:

Table 23: Remote Control Power Control Options on S1200BTL platforms

Option	Task
Reset Server	Select option to hard reset the host without powering off.
Power OFF Server	Select option to. immediately power off the host
Power ON Server	Select option to power on the host
Power Cycle Server	Select option to immediately power off the host, then power it back on after one second
Perform Action button	Click to 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.	

On an EPSD Platforms Based on Intel® Xeon® Processor E5 4600/2600/2400/1600/1400 Product Families you have two additional options, one is to **Force-enter BIOS Setup** on a reset and the second is to request a **Graceful Shutdown**. See Figure 91 and Table 24 for details.

For the Graceful OS Shutdown to function properly the OS must be ACPI aware and be configured to do the shutdown without operator intervention. Once a Graceful Shutdown has been requested, if the system does not shutdown as requested, the command cannot be executed again for five minutes.

Figure 91: Remote Control Server Power Control Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

Table 24: Remote Control Power Control Options on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

Option	Task
Reset Server	Select option to hard reset the host without powering off.
Force-Enter BIOS Setup	Check this option to enter into the BIOS setup after resetting the server.
Power OFF Server	Select option to. immediately power off the host
Graceful Shutdown	Selecting this option will soft power off the host.
Power ON Server	Select option to power on the host
Power Cycle Server	Select option to immediately power off the host, then power it back on after one second
Perform Action button	Click to execute the selected remote power command
Note: All power control actions are done through the BMC and are immediate actions.	

7.4.3 Virtual Front Panel Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

On EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families this page can be used just like the systems front panel.

Figure 92: Remote Control Virtual Front Panel Page on EPSD Platforms Based on Intel® Xeon® Processor E5-4600/2600/2400/1600/1400 Product Families

The following power control operations can be performed:

Table 25: Remote Control Virtual Front Panel Options

Option	Task
Power Button	Power button is used to Power ON or Power Off.
Reset Button	Reset Button is used to reset the server while system is ON.
Chassis ID Button	When Chassis ID button is pressed then the chassis ID LED changes to solid on If the button is pressed again the chassis ID LED turns off.
NMI Button	At present, NMI button is disabled.
Power LED	Power LED shows system power status. If LED is green then System is ON. If LED is grey then System is OFF.
Status LED	Status LED will reflect the system status LED status and It automatically sync with BMC every 60 seconds. This reflects the System Status LED.
Chassis ID LED	Chassis ID LED shows the current system chassis ID status If Chassis ID is blue then Chassis ID is Indefinite ON If Chassis ID is grey then Chassis ID is OFF.