Dell PowerEdge
C6145

Using the Baseboard Management Controller

Information in this publication is subject to change without notice.
© 2011 Dell Inc. All rights reserved.

Reproduction of these materials in any manner whatsoever without the written permission of Dell Inc. is strictly forbidden.

Trademarks used in this text: Dell™, the DELL logo, and PowerEdge™ are trademarks of Dell Inc. Microsoft® and Windows® are registered trademarks of Microsoft Corporation. Linux® is a registered trademark of Red Hat, Inc. in the United States and/or other countries.

Other trademarks and trade names may be used in this publication to refer to either the entities claiming the marks and names or their products. Dell Inc. disclaims any proprietary interest in trademarks and trade names other than its own.

June 2013 **Rev. A01**

Contents

1

Introduction

This section introduces the BMC and includes the requirements for web-based graphical user interface (GUI), keyboard, video, and mouse (KVM), and virtual media.

BMC Key Features and Functions

The following lists the supported features of the BMC:

- Support for IPMI v1.5 and v2.0
- Out-of-band monitoring and control for sever management over LAN
- Dedicated 10/100 NIC for remote management over a network
- Information which includes main board part number, product name, manufacturer, and so on.
- Health status/hardware monitoring report
- View and clear events log.
- Event notification using chassis LED indicator and Platform Event Trap (PET)
- Platform Event Filtering (PEF) to take selected action for selected events, including NMI and SMI
- Chassis management including power control and status report, front panel buttons, LED control, Secure Mode, and Boot Option
- Watchdog and auto server re-start and recovery
- Multi-session user and alert destination for LAN channel
- IPMB connector to enable advanced server management communication with BMC
- Support for APML v1.03

2

Using the Web UI

The BMC firmware features an embedded web server, enabling users to connect to the BMC using an Internet browser (Microsoft Internet Explorer) without needing to install KVM and virtual storage software on a remote console.

Web-based GUI is supported on the following browsers:

Microsoft Windows:

- Internet Explorer 6 or later
- Mozilla® Firefox® 2.0017 or later

Linux:

Mozilla Firefox 2.0017 or later

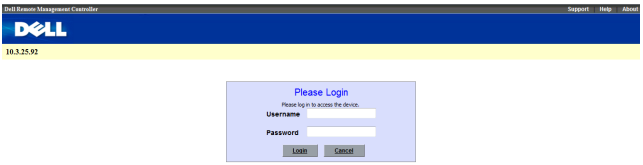
NOTE: Before using the web user interface, ensure that the firewall settings are configured to enable access to the following ports: 7578 (KVM),USB-CDROM: 5120, USB-FLOPPY: 5123.

Logging in to the Web User Interface

Enter the BMC-embedded server IP address or URL into the address bar of the web browser. The BMC interface has a default of (DHCP\Static). Enter the system BIOS setup with <F2> to change these settings.

When connecting to the BMC, the login screen prompts for the username and password. This authentication with Secure Sockets Layer (SSL) protection prevents unauthorized intruders from gaining access to the BMC web server. Once authentication is passed, you can manage the server by privilege. At the same time, the PHP Hypertext Preprocessor (PHP) records all user information, including user ID and privilege.

Using Your Remote Management Controller:



The Remote Management Controller has a user-friendly Graphics User Interface (GUI) called the *Remote Management Controller GUI*. It is designed to be easy to use. It has a low learning curve because it uses a standard Internet browser.

Default User Name and Password

When you first try to access your Remote Management Controller, you are prompted to enter a user name and password. Table 1-1 lists the user name and password for logging on to the Remote Management Controller.

Table 2-1. BMC Default User Name and Password

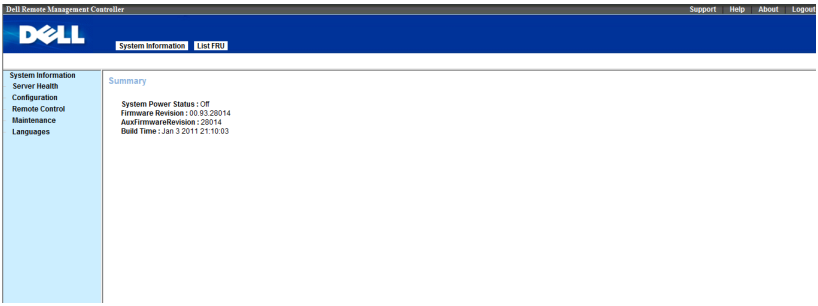
Field	Default
User Name	Root
Password	Root

NOTE: The default user name and password are in lower-case characters.

NOTE: When you log in using the root user name and password, you have administrative powers. Change your root password after logging in for the first time.

Remote Management Controller GUI Explained

After you successfully log in to your Remote Management Controller, you are greeted with the *Remote Management Controller GUI*.



Logout

Log out from your Remote Management Controller

The default timeout value is 30 seconds.

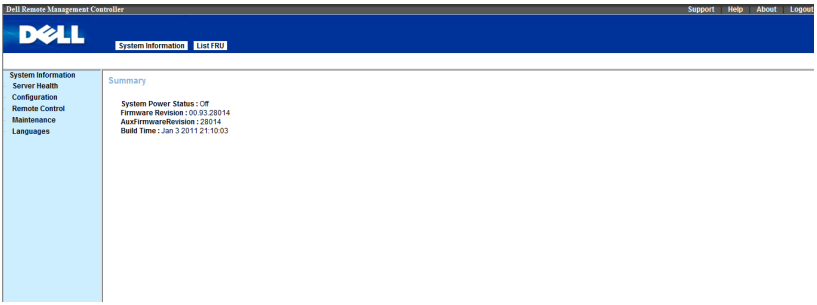
System Information

System Information

Click the **System Information** tab to view the Remote Management Controller. The **System Information** tab enables you to view the System Power Status, firmware revision, aux firmware revision, and build time.

Table 2-2. BMC Information

BMC Information	Description
System Power Status	On or Off
Firmware Revision	Remote Management Controller firmware revision.
Aux Firmware Revision	Remote Management Controller firmware aux revision.
Build Time	Date the firmware was last built in the form: MM DD YYYY HH:MM:SS



List FRU

The List FRU page shows a list of the detected Field Replaceable Units (FRUs) in the system. Select a FRU item from the drop down list to show more information.

Chassis Information

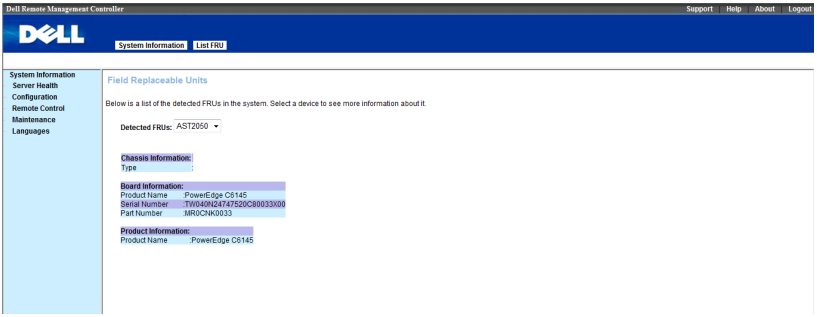
Lists the Type, Part Number and the Serial Number of the FRU.

Board Information

Lists the Manufacturer, Product Name, Serial Number and Part Number.

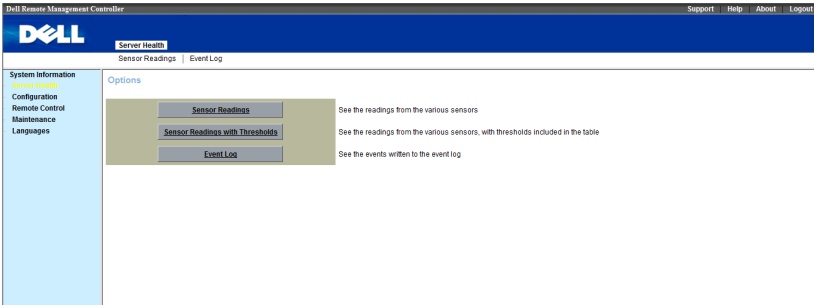
Product Information

Lists the Manufacturer Name, Product Name, Serial Number, Version, and Part Number.



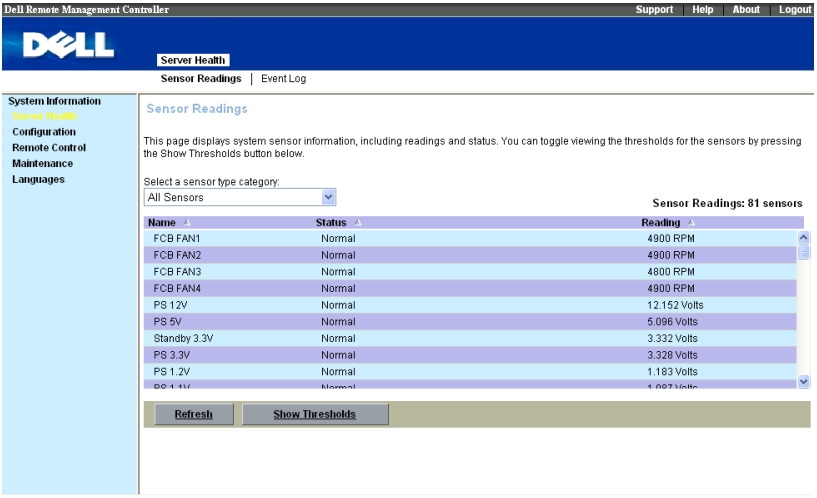
Server Health

The **Sensor** menu provides information about system hardware such as the fan speed, internal temperature, and voltage.



Sensor Readings & Sensor Readings with Thresholds

It reads the sensor information the system. You can **select a sensor type category**. You can click "**Refresh**" to re-read the sensor state. And you can click "**Show Thresholds**" to show the thresholds of every sensor.

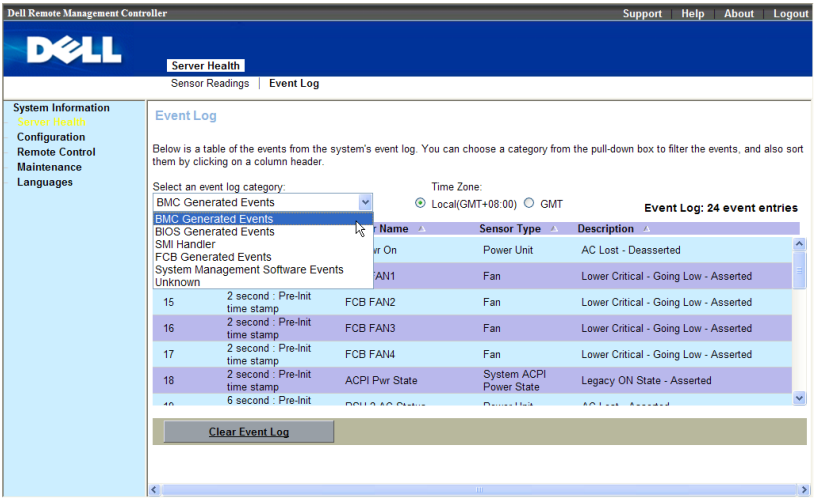


Event Log

The System Event Log (SEL) page displays system events that occur on the managed system. The SEL is generated by the Baseboard Management Controller (BMC) or BIOS on the managed system. The SEL lists the following information about system events: event ID, time stamp, sensor name, sensor type and a short description.

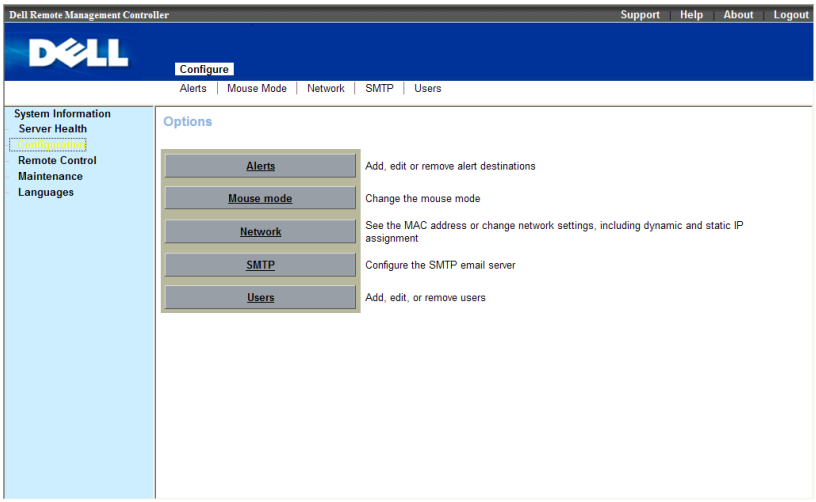
Select **Server Health** in menu bar. Click **Event Log** to view specific event information.

The list can be sorted by **selecting any event log category**. There are six categories, BMC Generated Events, BIOS Generated Events, SMI Handler, FCB Generated Events, System Management Software Events, and Unknown you can select. Subsequent selects Time Zone. There are two options, Local and GMT.



Click **Clear Event Log** to Clear the SEL.

Configuration

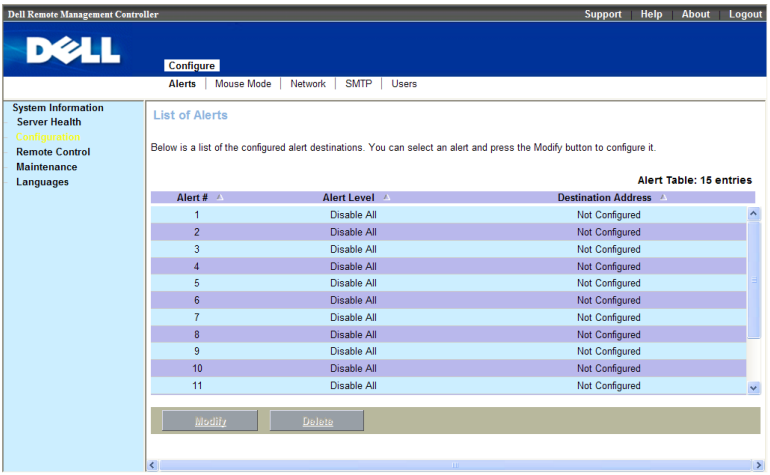


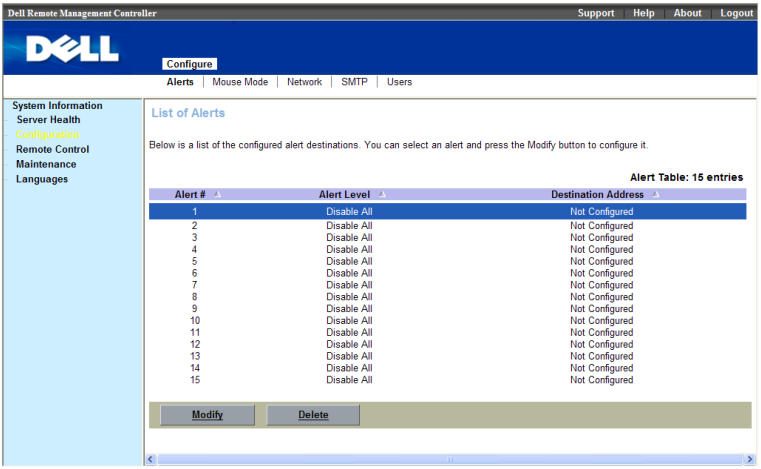
Alerts

When the BMC senses a platform event, such as an environmental warning or a component failure, an alert message can be sent to one or more email addresses. The **Alerts** window enables you to enter email addresses, IP addresses, and to activate the alerts for each address.

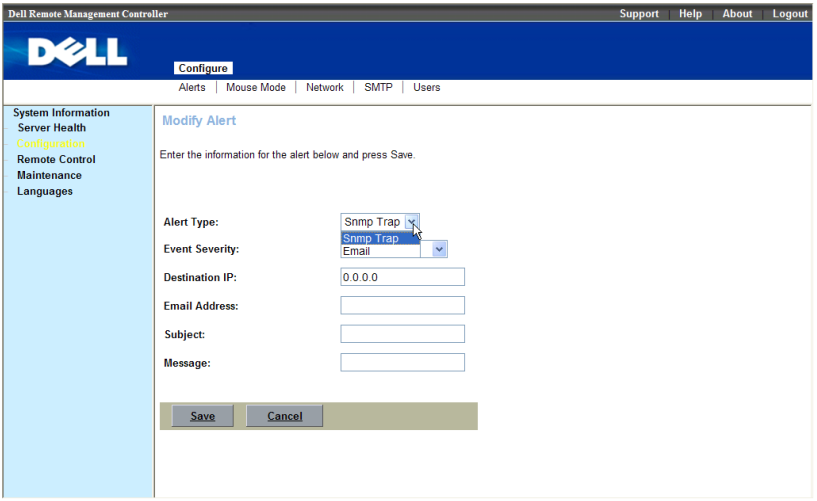
To set up a destination to receive alerts, perform the following procedure

1 Click an **Alert Number**, click **Modify**.

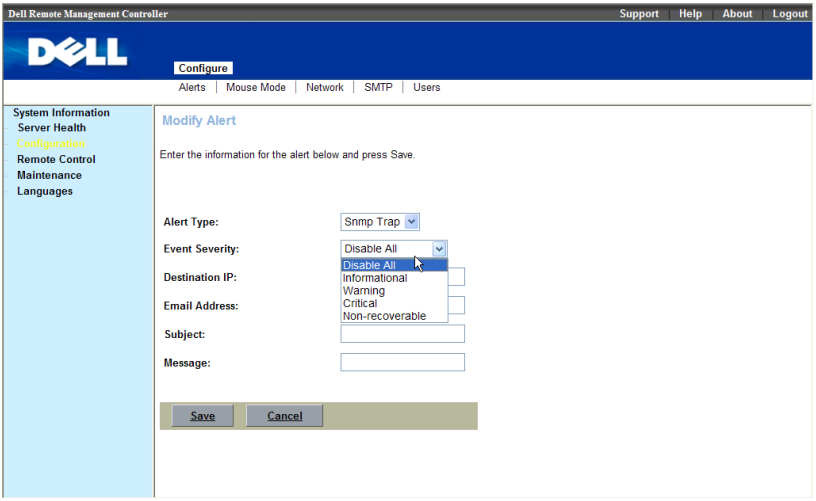

Dell Remote Management Controller
Support | Help | About | Logout
Configure
Alerts | Mouse Mode | Network | SMTP | Users
System Information
Server Health
Configuration
Remote Control
Maintenance
Languages
List of Alerts
Below is a list of the configured alert destinations. You can select an alert and press the Modify button to configure it.
Alert Table: 15 entries
Alert # | Alert Level | Destination Address
1 | Disable All | Not Configured
2 | Disable All | Not Configured
3 | Disable All | Not Configured
4 | Disable All | Not Configured
5 | Disable All | Not Configured
6 | Disable All | Not Configured
7 | Disable All | Not Configured
8 | Disable All | Not Configured
9 | Disable All | Not Configured
10 | Disable All | Not Configured
11 | Disable All | Not Configured
Modify
Delete


Dell Remote Management Controller
Support | Help | About | Logout
Configure
Alerts | Mouse Mode | Network | SMTP | Users
System Information
Server Health
Configuration
Remote Control
Maintenance
Languages
List of Alerts
Below is a list of the configured alert destinations. You can select an alert and press the Modify button to configure it.
Alert Table: 15 entries
Alert # | Alert Level | Destination Address
1 | Disable All | Not Configured
2 | Disable All | Not Configured
3 | Disable All | Not Configured
4 | Disable All | Not Configured
5 | Disable All | Not Configured
6 | Disable All | Not Configured
7 | Disable All | Not Configured
8 | Disable All | Not Configured
9 | Disable All | Not Configured
10 | Disable All | Not Configured
11 | Disable All | Not Configured
12 | Disable All | Not Configured
13 | Disable All | Not Configured
14 | Disable All | Not Configured
15 | Disable All | Not Configured
Modify
Delete

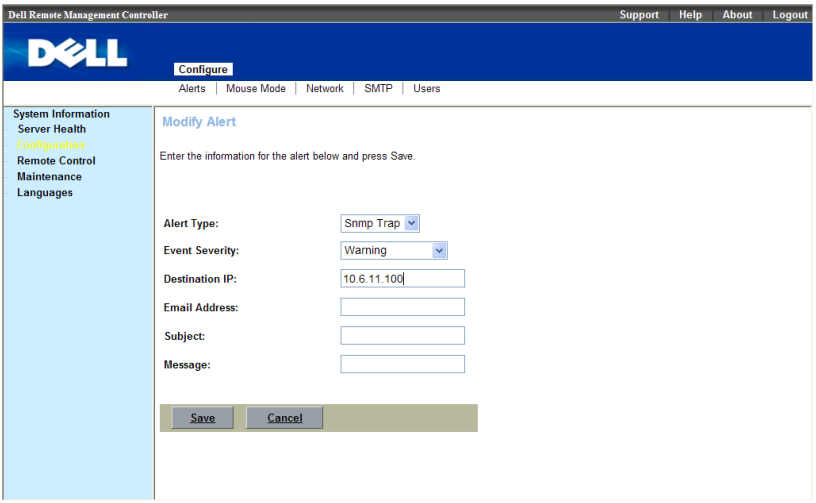
2 Select **Alert Type**, there are two options, **Snmp Trap and Email**.



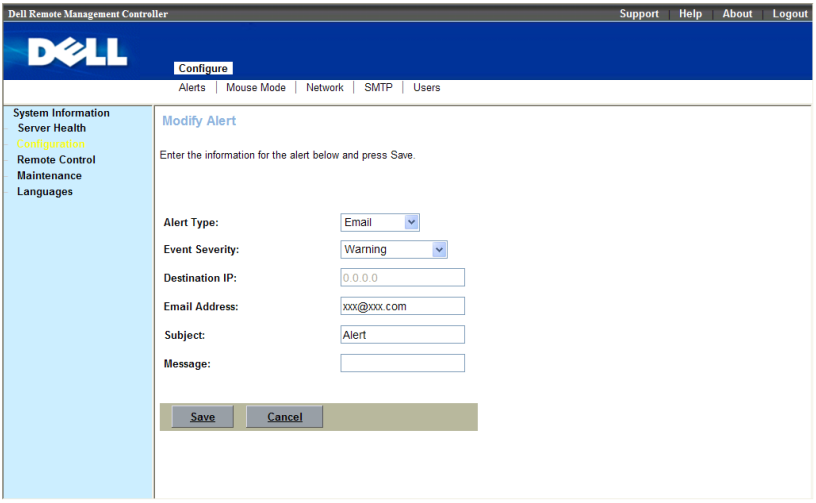
3 Select **Event Severity**, The five options available are, Disable All, Informational, Warning, Critical and Non-recoverable.



4 If your **Alert Type** is Snmp Trap, type the destination IP.



5 If your **Alert Type** is Email, enter the destination email address, and enter a brief description for the **Subject** of the email.



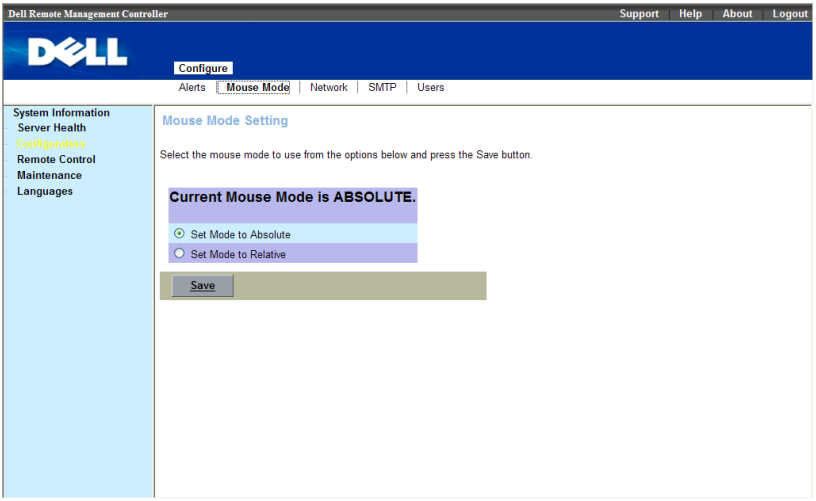
6 Click **Save**.

Mouse mode

It is an option to set up mouse mode which will using in KVM. Setting mouse mode depends on OS can get accurate mouse pointer.

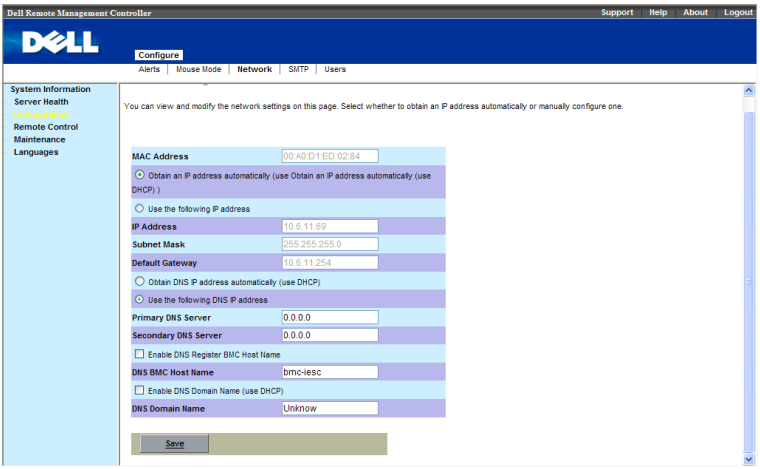
Absolute mode for host's system is Windows OS

Relative mode for host's system is Linux OS.



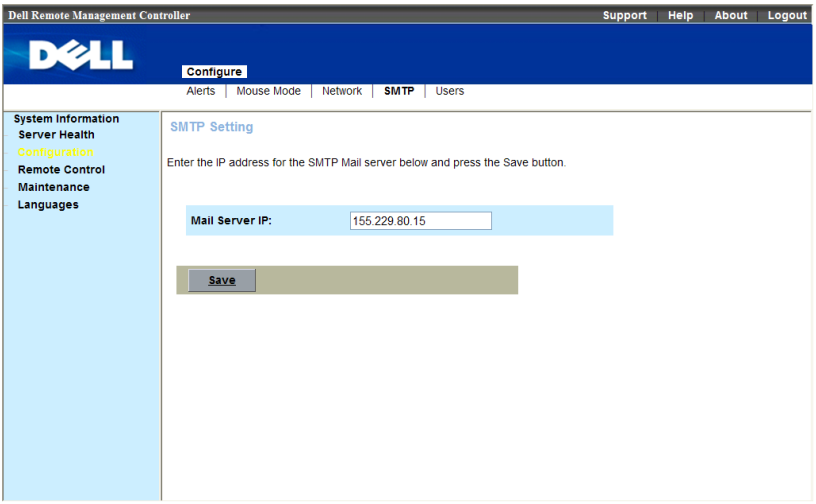
Network

Show the Remote Management Controller IP address information. You can set DHCP or STATIC IP then click "**Save**".



SMTP

Set E-mail (SMTP) server IP address for sending alert notification to user then click "**Save**".



Users

The **Users** page enables you to view information and configure existing BMC users. You can control user who can login Remote Management Controller and accessing privileges.

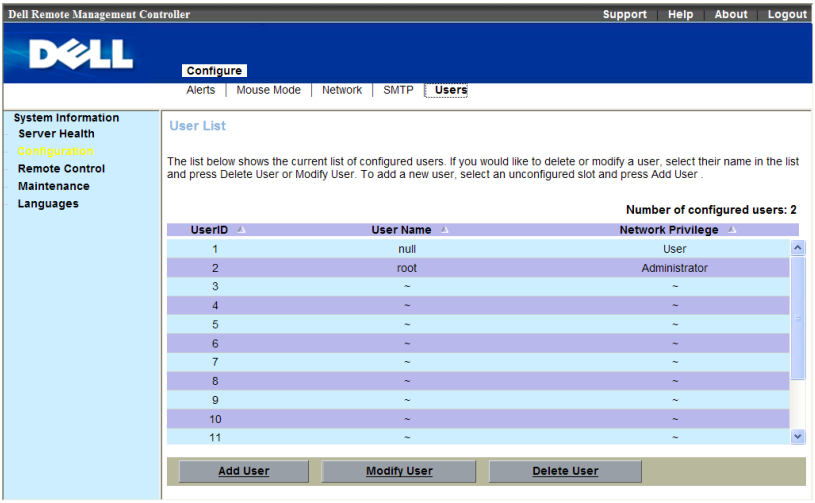
Table 1-28 displays the **Users** list for existing BMC users.

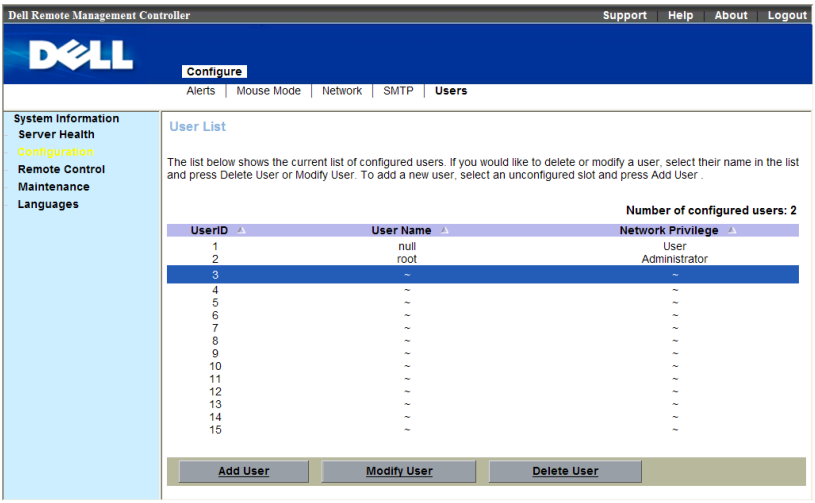
Table 2-3. BMC User Information

BMC Information	Description
User ID	Displays a sequential user ID number.
User Name	Displays the login name of the user.
Network Privilege	Displays the group (privilege level) to which the user is assigned. (Administrator, Operator, User, Custom, or None).

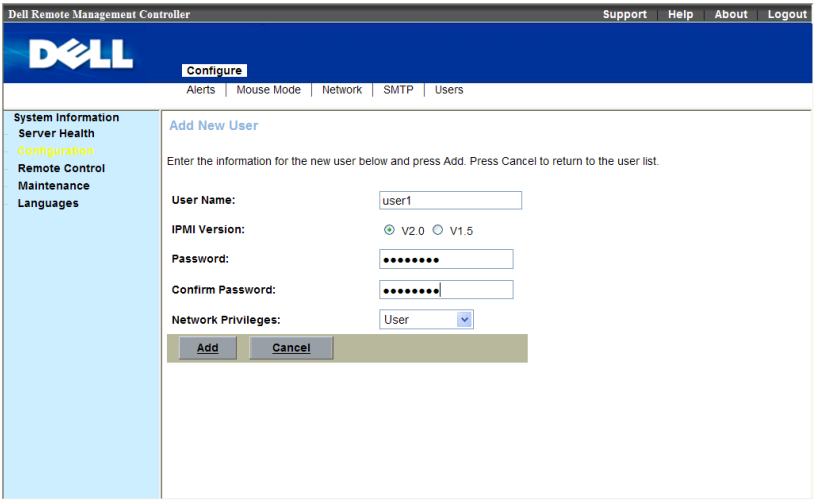
There are three operations in **Users** page: Add User, Modify User and Delete User.

To add new user, click their **user ID number**, in the **Users** list. Click **Add User**.



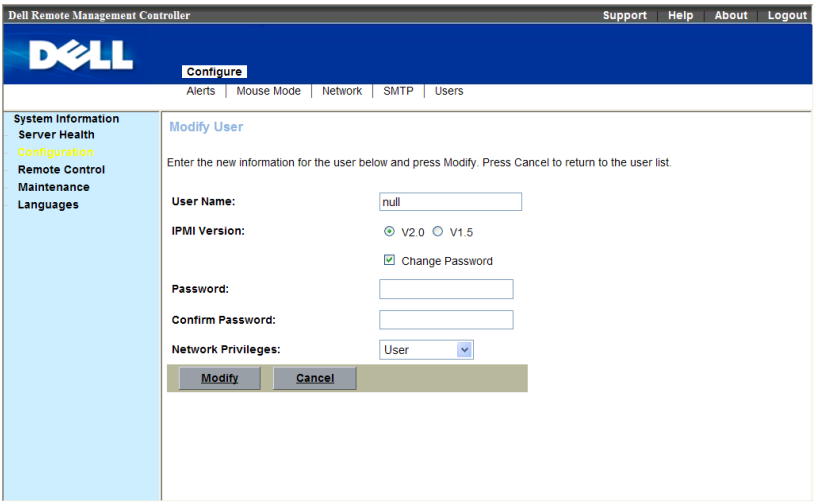


Enter user name, IPMI version, password, confirm password and network privileges, click **Add**.



To change the settings for a user, click their **user ID number**, in the **Users** list. Click **Modify User**.

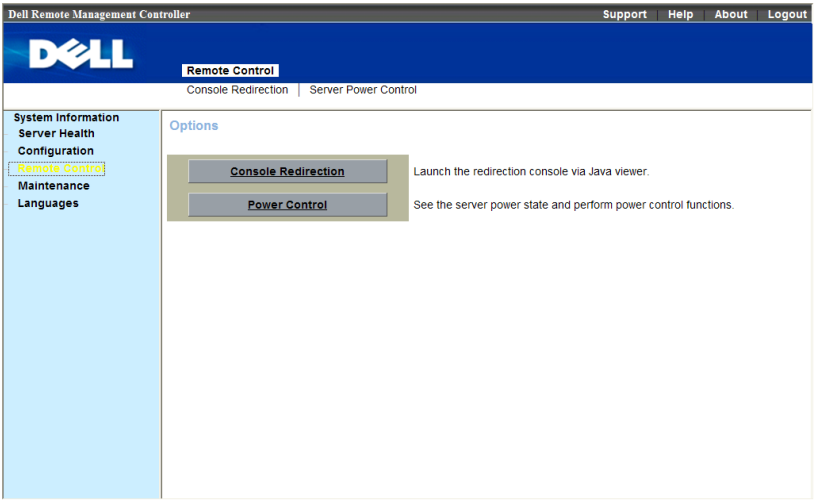
Modify user name, IPMI version, password, confirm password and network privileges, click **Modify**.



To delete new user, click their **user ID number**, in the **Users** list. Click **Delete User**. A dialog box appears**,** click **yes** to delete the user and automatically refresh page.

NOTE: You must have Configure Users permission to configure a BMC user; otherwise these options are not available

Remote Control



Power Control

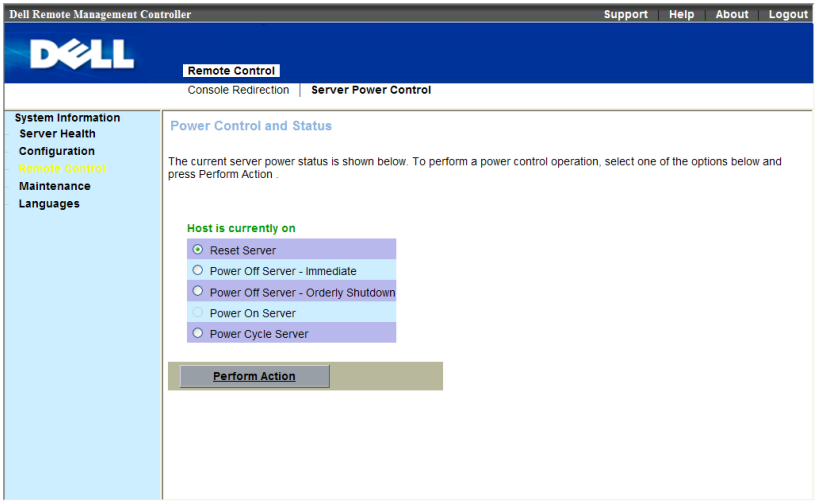
This feature enables the administrator to **power on, power off, power cycle, and reset** the system remotely.

Select **Remote Control** in menu bar. Click **Power Control.** Select a **Power Control Operation**. Table 1-4 list the power control operation;

Table 2-4. Power Control Operation Options

Power Control Operation	Description
Reset System	Reboots system without powering off (warm boot).
Power Off System – Immediate	Powers off the system.
Soft Shutdown – Orderly Shutdown	Shuts down system.
Power On System	Powers on the system.
Power Cycle System	Powers off, then power on system (cold boot).

Click **Perform Action** to enable the selected **Power Control Operation**.



Console Redirection

The **Console Redirection** page enables you to use the display, mouse, and keyboard on the local management station to control the corresponding devices on a remote managed system. You can run a maximum of four simultaneous console redirection sessions.

NOTE: Before you can use the console redirection feature, your browser must have the Java runtime environment installed. This feature needs Java 1.5.15 or later installed on the host system. If the BMC detects that the Java Video Viewer is not installed, you are prompted to install it.

NOTE: Sometimes the Console is referred to as the Session Viewer.

NOTE: The recommended display resolution on the management station (or client) is at least 1280 x 1024 pixels at 60 Hz with 32 bit color. You cannot view the console in full screen mode if your monitor resolution is less than this minimum.

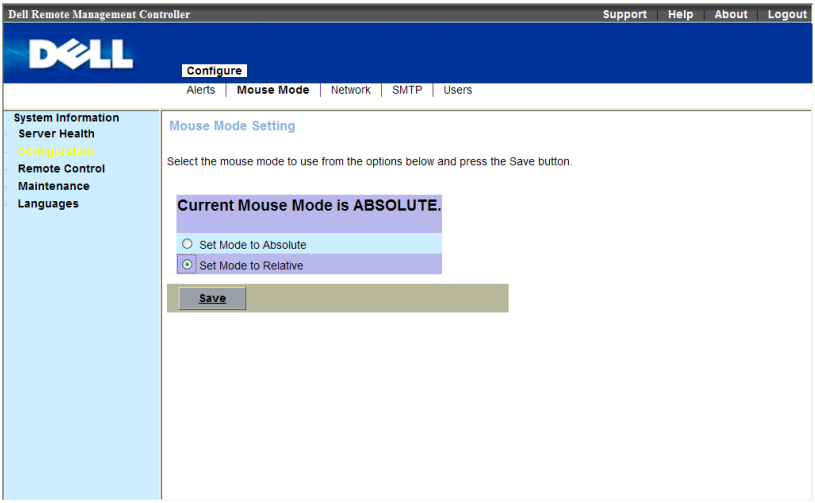
The most powerful feature of your Remote Management Controller is the ability to redirect the host system's console. To redirect the host system's console is the ability to manage your host system as if it were physically in front of you, but not.

Console Redirection Configuration

Before you use Console Redirection, please check your **Mouse mode**.

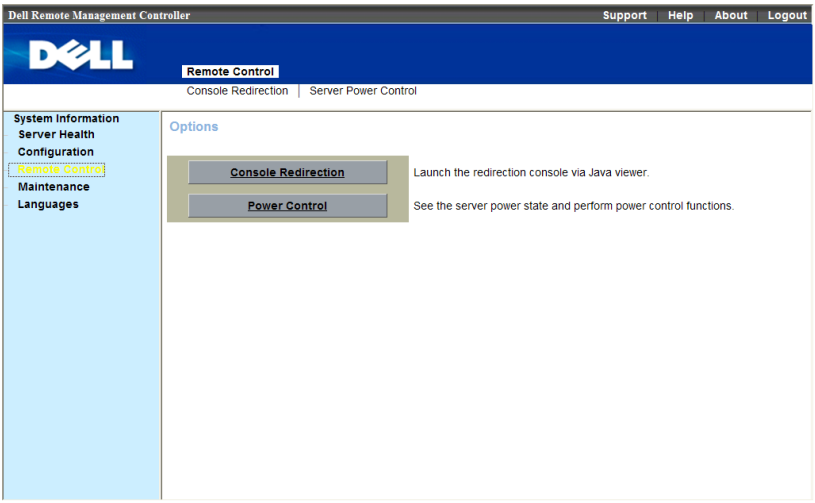
If the host's OS is Linux, please change the **Mouse mode** to **RELATIVE**

If the host's OS is Windows, please change the **Mouse mode** to **ABSOLUTE**

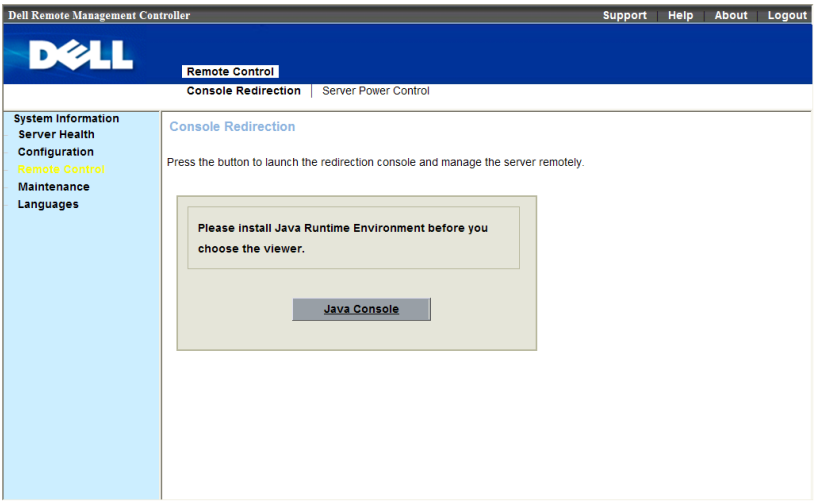


This menu item allows you to start a Remote Console session with the host system.

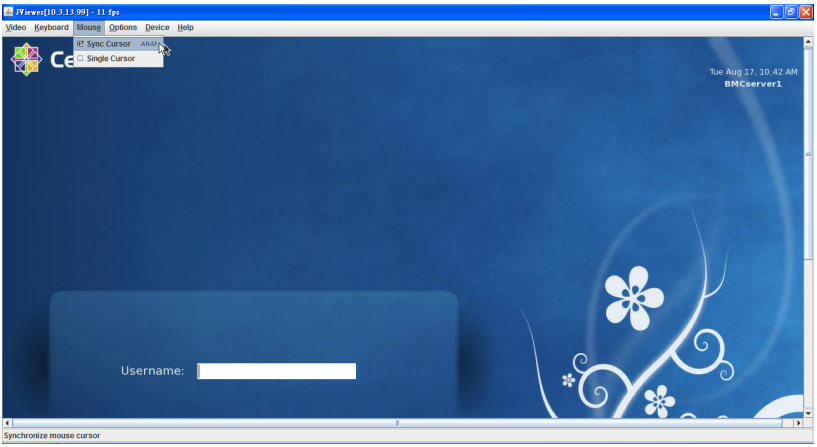
1 Click **Console Redirection**.



2 Click **Java Console**.



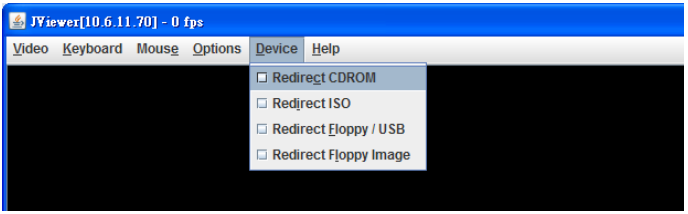
3 And click **Mouse** item to **Sync Cursor**.



BMC Virtual Media

The **Device** menu allows you to virtualize a diskette image or drive. Virtual media enables a floppy image, floppy drive or CD/DVD drive on your system to be available on the managed system's console as if the floppy image or drive were present on the local system.

The **Device** menu in KVM displays the floppy image, floppy drive, CD/DVD drive, or ISO image on the management console that is currently virtualized.

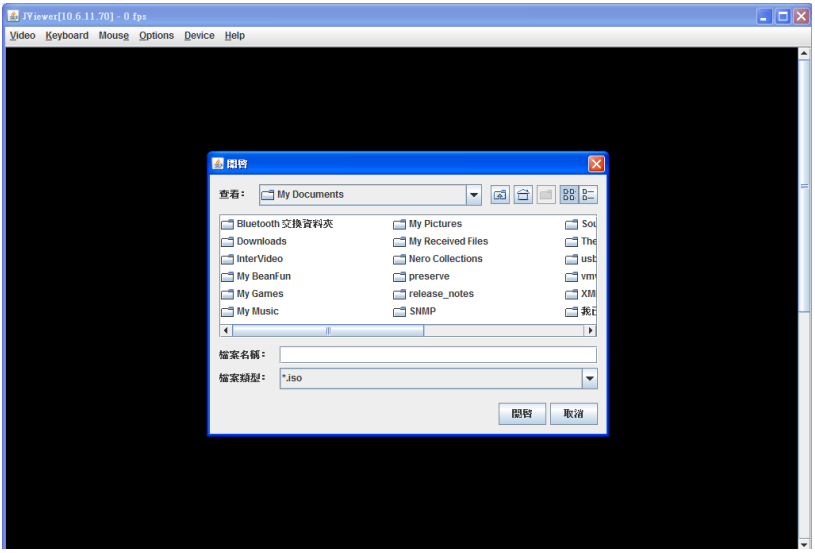


NOTE: You must have Access Virtual Media permission to virtualize or disconnect a drive.

NOTE: You can enable virtual media for one floppy/drive image and one CD/DVD drive/image. Only one drive/image for each media type can be virtualized at a time. A USB key/flash drive is treated as a floppy drive.

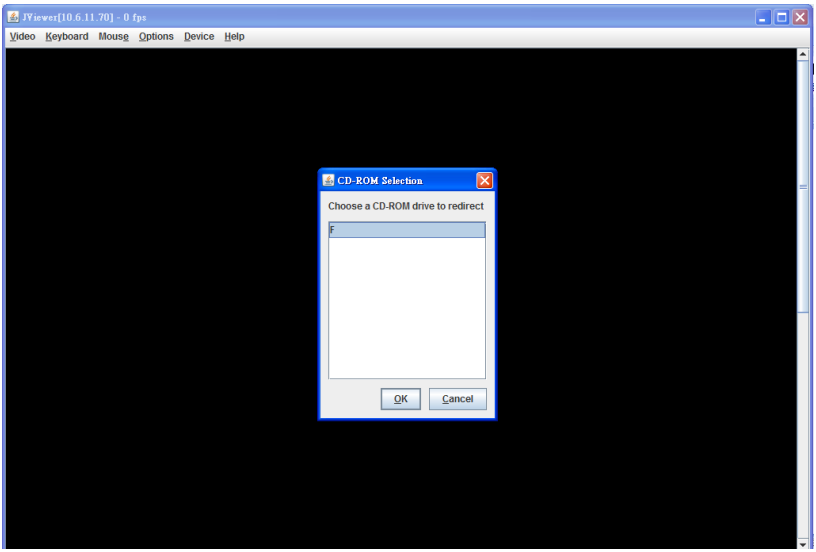
Virtualizing Devices

The **Device** client displays the list of devices available for mapping in the main window. To virtualize a device, select the checkbox in the **Mapped** column of the table. The device maps to the server at this point. To unmap, deselect the checkbox. And then select the image file with the dialog that is displayed. The image is added to the list of available devices.



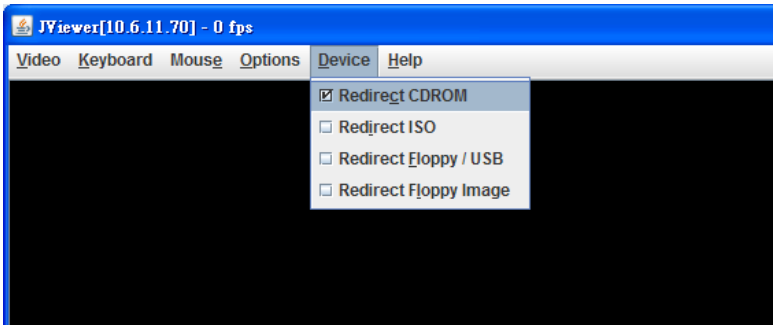
Mapping a Virtual Media Drive

You can select a drive to become a virtual media drive by selecting the **Mapped** check box for a particular drive. CD/DVD Drives and ISO images are always read only which cannot be changed.



Unmapping a Virtual Media Drive

To unmap a virtual media drive, select the **Mapped** check box for a particular drive. Because some interaction might be going on with the drive, you must confirm the action before the drive is unmmapped.



NOTE: The assigned virtual drive letter (Microsoft® Windows®) or device special file (Red Hat® Enterprise Linux®) may not be the same as the drive letter on this system (management console).

BMC KVM

The BMC KVM client main menu consists of five menu options, which are used to provide access to functions available through the viewer: **Video**, **Keyboard**, **Mouse**, **Options**, **Device**, and **Help**. To launch a KVM session, select **Remote Control** tag, click **Console Redirection**.

Video

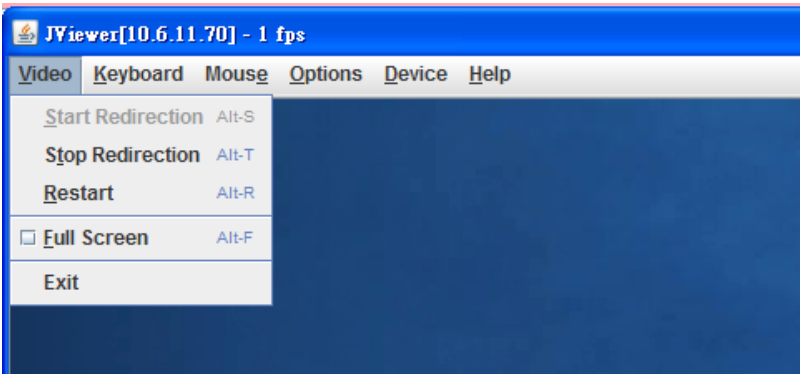


Table 2-5. BMC KVM Video Menu Items

Dropdown Menu Items	Description
Start Redirection	This menu item can be used to begin Console Redirection.
Stop Redirection	This menu item can be used to halt Console Redirection.
Restart	This menu item can be used to stop Console Redirection and then start Console Redirection again.
Full Screen	This menu item can be used to view the Console Redirection in Full Screen mode. **NOTE:** Set your client system's screen resolution to 1024 x 768 so that you can view the host system in true full screen.
Exit	Exit console redirection.

Keyboard

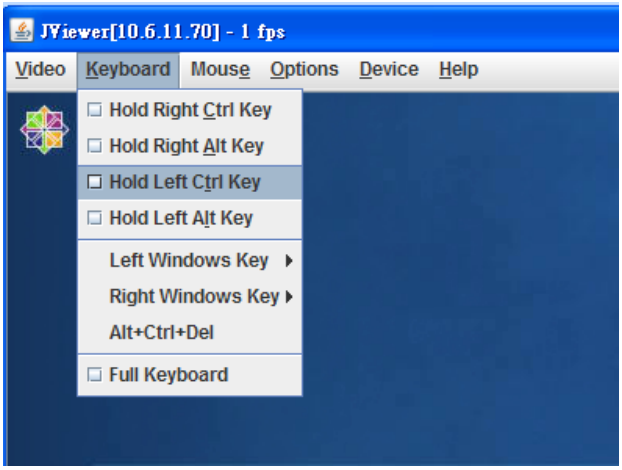
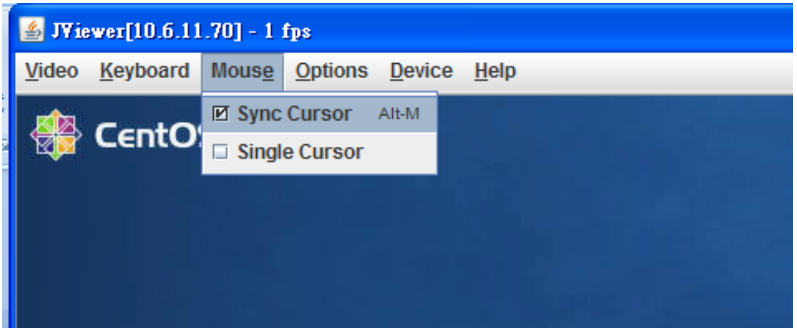


Table 2-6. BMC KVM Keyboard menu items

Dropdown Menu Items	Description
Hold Right CTRL Key	This menu item can be used to act as the right-side <CTRL> key when in Console Redirection.
Hold Right ALT Key	This menu item can be used to act as the right-side <ALT> key when in Console Redirection.
Hold Left CTRL Key	This menu item can be used to act as the left-side <CTRL> key when in Console Redirection.
Hold Left ALT Key	This menu item can be used to act as the left-side <ALT> key when in Console Redirection.
Left Windows Key	This menu item can be used to access the left-side <WINDOWS> key during a Console Redirection session. The following actions can be performed: Hold Down Press and Release

Dropdown Menu Items	Description
Right Windows Key	This menu item can be used to access the right-side <WINDOWS> key during a Console Redirection session. The following actions can be performed: Hold Down Press and Release
ALT+CTRL+DEL	This menu item can be used to act as if you depressed the <CTRL>, <ALT> and <DEL> keys down simultaneously on the host system that you are redirecting.
Full Keyboard	User can key-in function key. For example: Ctrl+C

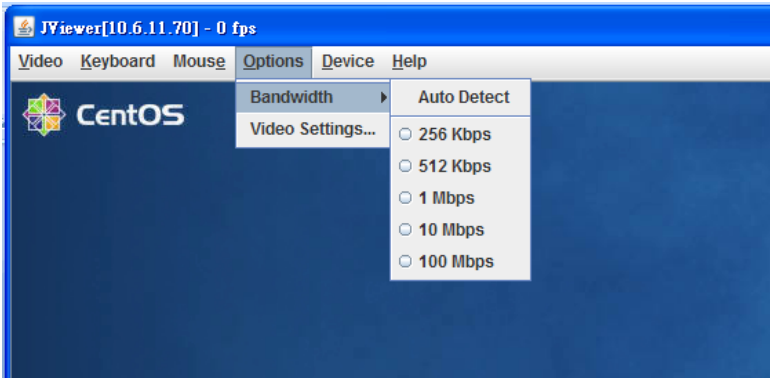
Mouse



Sync Cursor for remote control mouse.

Single Cursor: To solve problem of remote mouse can't work correctly under LSI 8708EM2 WebBIOS.

Options



Bandwidth: Helps in regulated the network bandwidth.

Video Settings: Helps in adjust video resolution.

Device

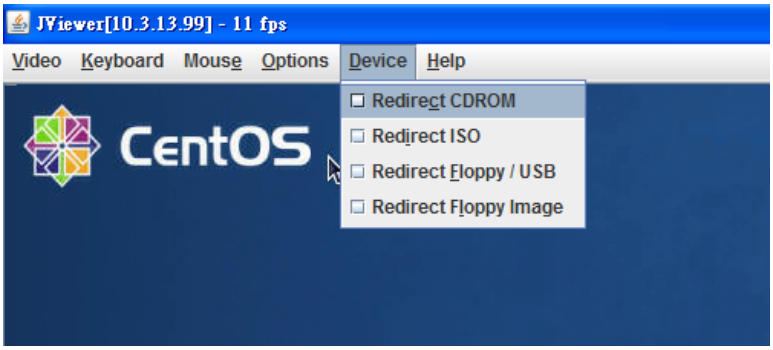


Table 2-7. BMC KVM Device Menu Items

Dropdown Menu Items	Description
Redirect CDROM	Enable you to start or stop the redirection of the CD-ROM drive. You can choose the CD-ROM drive from client computer.

Dropdown Menu Items	Description
Redirect ISO	Enable you to start or stop the redirection of the ISO. You can choose the CD IMAGE file from client computer.
Redirect Floppy / USB	Enable you to start or stop the redirection of the Floppy/USB drive. You can choose the Floppy/USB drive from client computer.
Redirect Floppy Image	Enable you to start or stop the redirection of the floppy drive. You can choose the Floppy IMAGE file from client computer.

Maintenance

Firmware Update

Use the Firmware Update feature to upgrade to the latest firmware version. The following data is included in the BMC firmware package:

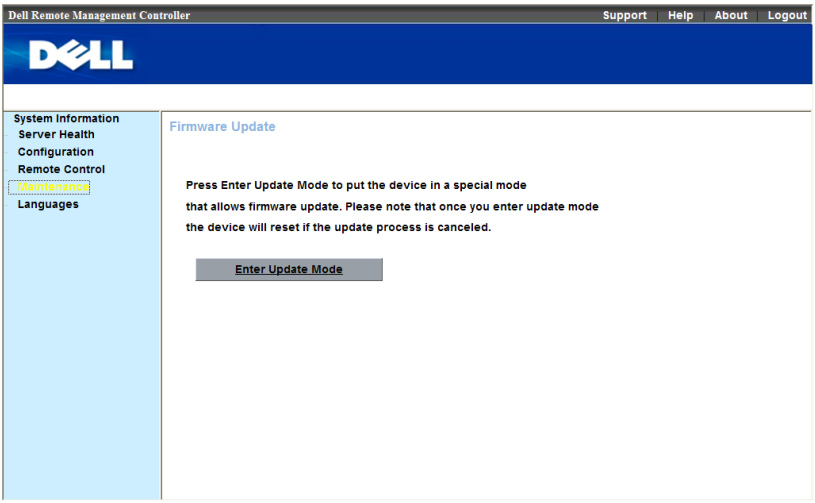
- Compiled BMC firmware code and data
- Web-based user interface, JPEG, and other user interface data files
- Default configuration files

NOTE: The firmware update retains the current BMC settings.

Updating the BMC Firmware

NOTE: Before beginning the firmware update, download the latest firmware version and save it on your local system. During the process of firmware update, the AC power of the managed system cannot be unplugged and the Web GUI cannot be closed.

1 Select "**Maintenance**" in menu bar. Click **Enter Update Mode**



2 Browse to, or Type the path on your system where the firmware image file resides.

Example:

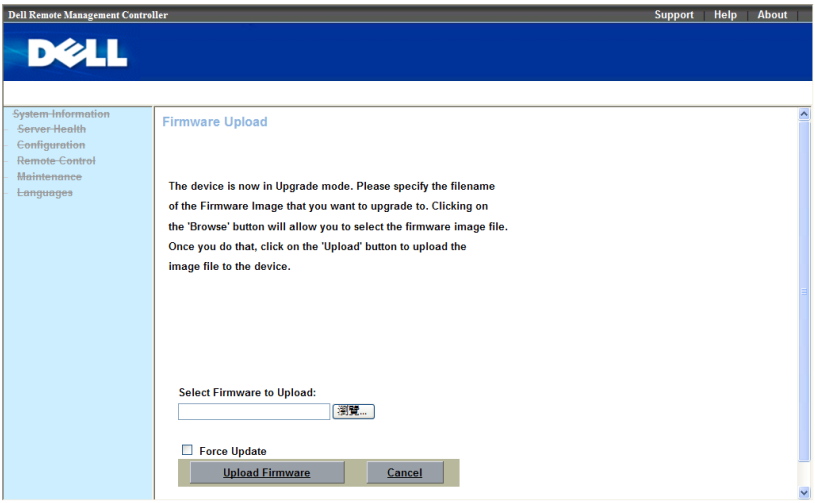
C:\<Product Name>\KCSFlash\<image_name>

3 Select the **Update Type** as **Normal** or **Forced** (The default value is **Normal**).

Normal: An update operation will occur only when the BMC validates the target board, target product and version number.

Forced: Forced update makes the BMC update the image without validating target board, target product and version number.

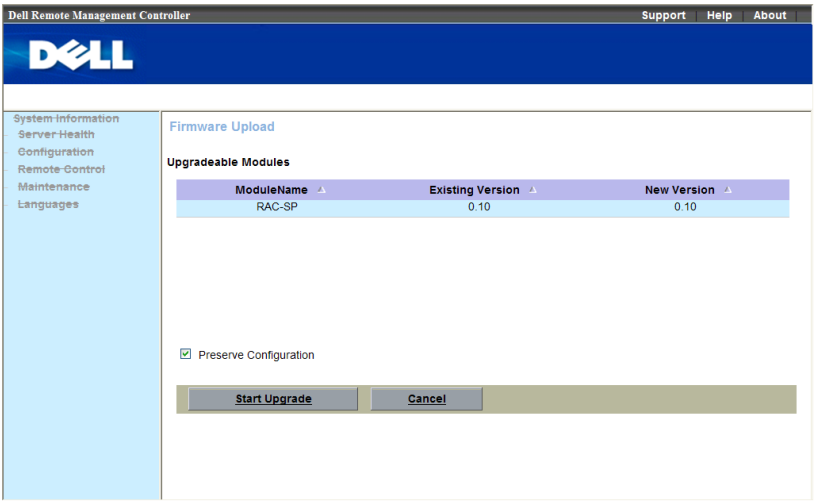
4 Click **Upload Firmware**.



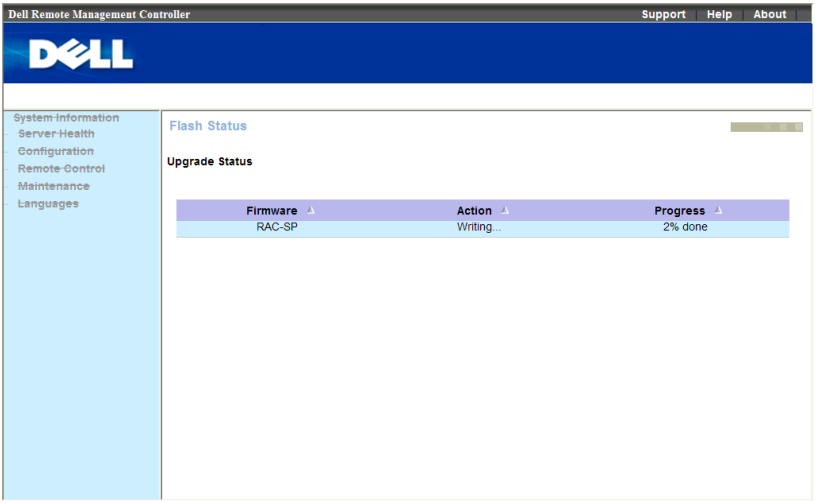
5 A window, telling that the firmware image has been verified, appears. Compare the uploaded image with existing device firmware version.

6 Select the **Preserve Configuration or Don't Preserve Configuration** (The default value is **Preserve Configuration**).

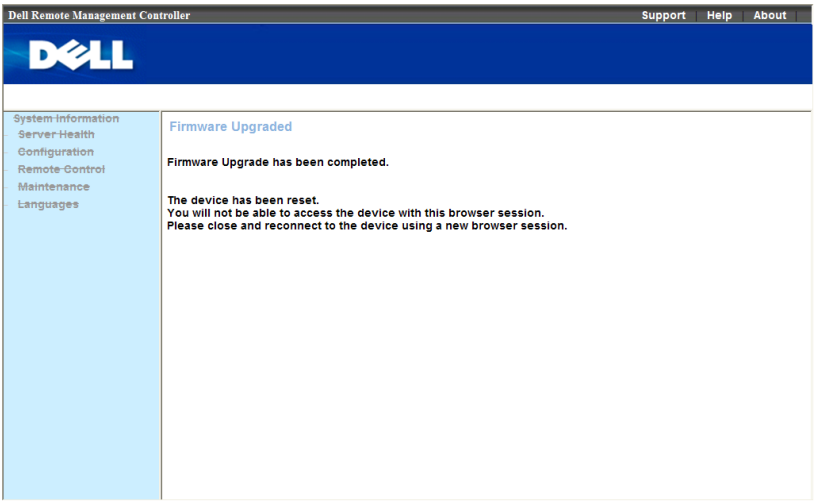
7 Click **Start Upgrade**.



The update might take several minutes.



8 The update is completed. Close the session and automatically log out.



9 After the BMC resets, click **Log In** to log in to the BMC again.

3

Sensors Threshold

Table 3-1. Sensors Threshold

Sensor Number	Sensor Name	The Converting Formula					
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
Fan							
01h	FCB FAN1	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
02h	FCB FAN2	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
03h	FCB FAN3	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
04h	FCB FAN4	Actual_Reading (RPM) = Raw_Data x 100					
		0xFF	0xFF	0xFF	0x00	0x0F	0x00
Voltage							
14h	PS 12V	Actual_Reading (Volts) = Raw_Data x 0.062					
		0xD8	0xD4	0xCF	0xAB	0xAF	0xB4
15h	PS 5V	Actual_Reading (Volts) = Raw_Data x 0.026					
		0xD7	0xD3	0xCD	0xA9	0xAE	0xB3
16h	Standby 3.3V	Actual_Reading (Volts) = Raw_Data x 0.0172					
		0xD6	0xD3	0xCD	0xA9	0xAD	0xB3
17h	PS 3.3V	Actual_Reading (Volts) = Raw_Data x 0.026					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
18h	PS 1.2V	Actual_Reading (Volts) = Raw_Data x 0.0087					

Sensor Number	Sensor Name	The Converting Formula					
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
		0x98	0x96	0x92	0x7D	0x7F	0x84
19h	PS 1.1V	Actual_Reading (Volts) = Raw_Data x 0.0087					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
51h	VCORE 1	Actual_Reading (Volts) = Raw_Data x 0.0083					
		0x64	0x62	0x5F	0x00	0x00	0x00
52h	VCORE 2	Actual_Reading (Volts) = Raw_Data x 0.0116					
		0x70	0x6E	0x6B	0x00	0x00	0x00
53h	VCORE 3	Actual_Reading (Volts) = Raw_Data x 0.0083					
		0x64	0x62	0x5F	0x00	0x00	0x00
54h	VCORE 4	Actual_Reading (Volts) = Raw_Data x 0.0116					
		0x70	0x6E	0x6B	0x00	0x00	0x00
Temperature							
21h	MLB TEMP 1	Actual_Reading (degrees C) = Raw_Data					
		0x55	0x50	0x4B	0x00	0x00	0x00
22h	MLB TEMP 2	Actual_Reading (degrees C) = Raw_Data					
		0x55	0x50	0x4B	0x00	0x00	0x00
23h	MLB TEMP 3	Actual_Reading (degrees C) = Raw_Data					
		0x55	0x50	0x4B	0x00	0x00	0x00
24h	MLB TEMP 4	Actual_Reading (degrees C) = Raw_Data					
		0x55	0x50	0x4B	0x00	0x00	0x00
25h	NB1_TEMP	Actual_Reading (degrees C) = Raw_Data					
		0x77	0x75	0x73	0x00	0x00	0x00
26h	NB2_TEMP	Actual_Reading (degrees C) = Raw_Data					
		0x77	0x75	0x73	0x00	0x00	0x00

Sensor Number	Sensor Name	The Converting Formula					
		Upper non-recoverable	Upper critical	Upper non-critical	Lower non-recoverable	Lower critical	Lower non-critical
61h	CPU1_Temp	Actual_Reading (℃) = Raw_Data					
		0x4E	0x4C	0x4B	0x00	0x00	0x00
62h	CPU2_Temp	Actual_Reading (℃) = Raw_Data					
		0x4E	0x4C	0x4B	0x00	0x00	0x00
63h	CPU3_Temp	Actual_Reading (℃) = Raw_Data					
		0x4E	0x4C	0x4B	0x00	0x00	0x00
64h	CPU4_Temp	Actual_Reading (℃) = Raw_Data					
		0x4E	0x4C	0x4B	0x00	0x00	0x00
2Ah	FCB Ambient1	Actual_Reading (degrees C) = Raw_Data (only support Sensor Reading, threshold unsupport)					
		0xFF	0x32	0x00	0x00	0x00	0x00
E0h-FFh	DIMM_A1 to DIMM_D8	Actual_Reading (℃) = Raw_Data					
		0x63	0x61	0x5F	0x00	0x00	0x00
Power Supply							
A1h	MB_12V_Current	Actual_Reading = Raw_Data					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
A3h	PSU 1 POUT	Actual_Reading = Raw_Data					
		0xFF	0xFF	0xFF	0x00	0x00	0x00
A4h	PSU 2 POUT	Actual_Reading = Raw_Data					
		0xFF	0xFF	0xFF	0x00	0x00	0x00

4

Events Table

Table 4-1. Threshold Sensors Event

Sensor Number	Sensor Name	Sensor Type	Events
01h	FCB FAN1	04h(Fan)	Lower Critical – going low asserted Lower Critical – going low deasserted
02h	FCB FAN2		
03h	FCB FAN3		
04h	FCB FAN4		
21h	MLB TEMP 1	01h (Temperature)	Upper Non-critical – going high asserted Upper Non-critical – going high deasserted Upper Critical – going high asserted Upper Critical – going high deasserted Upper Non-recoverable – going high asserted Upper Non-recoverable – going high deasserted
22h	MLB TEMP 2		
23h	MLB TEMP3		
24h	MLB TEMP4		
25h	NB1_TEMP		
26h	NB2_TEMP		
61h	CPU1_TEMP		
62h	CPU2_TEMP		
63h	CPU3_TEMP		
64h	CPU4_TEMP		
E0h-E7h	DIMM_A1-8		
E8h-EFh	DIMM_B1-8		
F0h-F7h	DIMM_C1-8		
F8h-FFh	DIMM_D1-8		

Sensor Number	Sensor Name	Sensor Type	Events
2Ah	FCB Ambient1	01h (Temperature)	Upper Critical – going high asserted Upper Critical – going high deasserted Upper Non-recoverable – going high asserted Upper Non-recoverable – going high deasserted
14h	PS 12V	02h (Voltage)	Upper Non-critical – going high asserted Upper Non-critical – going high deasserted Upper Critical – going high asserted
15h	PS 5V		Upper Critical – going high deasserted Upper Non-recoverable – going high asserted Upper Non-recoverable – going high deasserted
16h	STBY 3.3V		Lower Non-critical – going low asserted Lower Non-critical – going low deasserted Lower Critical – going low asserted Lower Critical – going low deasserted Lower Non-recoverable – going low asserted Lower Non-recoverable – going low deasserted

Table 4-2. Non-threshold Sensors Event Table

Sensor Number	Sensor Name	Sensor Type	Sensor-Specific Offset	Events
71h	PEF Action	12h	O4h	PEF Action
72h	WatchDog2	23h	00h	Timer expired, status only
			01h	Hard Reset
			02h	Power Down
			03h	Power Cycle
			08h	Timer Interrupt
74h	AC Pwr On	09h	04h	AC lost deasserted
73h	ACPI Pwr State	22h	0Bh	Legacy ON state
			0Ch	Legacy OFF state
41h	CPU1Status	07h	01h	Thermal Trip
42h	CPU2Status			
43h	CPU3Status			
44h	CPU4Status			
40h	SEL Fullness	10h	02h	Log Area Reset/Cleared
			04h	SEL Full
			05h	SEL Almost Full
A5h	PCI Bus	13h	04h	PCI PERR
			05h	PCI SERR
60h	Memory	0Ch	00h	Correctable ECC/other

Sensor Number	Sensor Name	Sensor Type	Sensor-Specific Offset	Events
				correctable memory error
			01h	Uncorrectable ECC/other uncorrectable memory error
			05h	Correctable ECC/other correctable memory error logging limit reached
75h	Security	06h	05h	Out-of-band Access Password Violation
AAh	PwrLimitAlert	07h	05h	DCMI Power management exception action

5

IPMI 1.5 / 2.0 Command Support List

Table 5-1. IPMI Device Global Commands

Command	NetFn	CMD	O/M	Supported
Get Device ID	App	01h	M	Yes
Cold Reset	App	02h	O	Yes
Warm Reset	App	03h	O	No
Get Self Test Results	App	04h	M	Yes
Manufacture Test On	App	05h	O	Yes
Set ACPI Power State	App	06h	O	Yes
Get ACPI Power State	App	07h	O	Yes
Get Device GUID	App	08h	O	Yes
Broadcast Commands:				
Broadcast 'Get Device ID'	App	01h	O	No

Table 5-2. BMC Device and Messaging Commands

Command	NetFn	CMD	O/M	Supported
Set BMC Global Enables	App	2Eh	M	Yes
Get BMC Global Enables	App	2Fh	M	Yes
Clear Message Buffer Flags	App	30h	M	Yes
Get Message Buffer Flags	App	31h	M	Yes
Enable Message Channel Receive	App	32h	O	Yes
Get Message	App	33h	M	Yes

Command	NetFn	CMD	O/M	Supported
Send Message	App	34h	M	Yes
Read Event Message Buffer	App	35h	O	Yes
Get BT Interface Capabilities	App	36h	O	No
Get System GUID	App	37h	O	Yes
Get Channel Authentication Capabilities	App	38h	O	Yes
Get Session Challenge	App	39h	O	Yes
Activate Session Command	App	3Ah	O	Yes
Set Session Privilege Level Command	App	3Bh	O	Yes
Close Session	App	3Ch	O	Yes
Get Session Information	App	3Dh	O	Yes
Get Authentication Code Command	App	3Fh	O	Yes
Set Channel Access Commands	App	40h	O	Yes
Get Channel Access Commands	App	41h	O	Yes
Get Channel Info Command	App	42h	O	Yes
Set User Access Commands	App	43h	O	Yes
Get User Access Commands	App	44h	O	Yes
Set User Name Commands	App	45h	O	Yes
Get User Name Commands	App	46h	O	Yes
Set User Password Commands	App	47h	O	Yes
Active Payload Command	App	48h	O	Yes
Deactivate Payload Command	App	49h	O	Yes
Get Payload Activation Status	App	4Ah	O	Yes
Get Payload Instance Info Command	App	4Bh	O	Yes
Set User Payload Access	App	4Ch	O	Yes
Get User Payload Access	App	4Eh	O	Yes
Get Channel Payload Support	App	4Fh	O	Yes
Get Channel Payload Version	App	50h	O	Yes

Command	NetFn	CMD	O/M	Supported
Master Write-Read I2C	App	52h	M	Yes
Get Channel Cipher Suites	App	54h	O	Yes
Suspend/Resume Payload Encryption	App	55h	O	Yes
Set Channel Security Keys	App	56h	O	Yes
Get System Interface Capabilities	App	57h	O	Yes
Set System Info Parameters	App	58h	O	Yes
Get System Info Parameters	App	59h	O	Yes

Table 5-3. BMC Watchdog Timer Commands

Command	NetFn	CMD	O/M	Supported
Reset Watchdog Timer	App	22h	M	Yes
Set Watchdog Timer	App	24h	M	Yes
Get Watchdog Timer	App	25h	M	Yes

Table 5-4. Chassis Commands

Command	NetFn	CMD	O/M	Supported
Get Chassis Capabilities	Chassis	00h	M	Yes
Get Chassis Status	Chassis	01h	M	Yes
Chassis Control	Chassis	02h	M	Yes
Chassis Reset	Chassis	03h	O	No
Chassis Identify	Chassis	04h	O	Yes
Set Chassis Capabilities	Chassis	05h	O	No
Set Power Restore Policy	Chassis	06h	O	Yes
Get System Reset Cause (Note: RESTART CAUSE [3:0] AH= SOFT RESET (E.G. CTRL-ALT-DEL) -UNSUPPORT.	Chassis	07h	O	Yes

Set System Boot Options (Note: PARAMETER #5 DATA3 [6:5]- FIRMWARE VERBOSITY - BIOS UNSUPPORT PARAMETER #7 UNSUPPORT	Chassis	08h	O	Yes
Get System Boot Options (Note: PARAMETER #7 UNSUPPORT	Chassis	09h	O	Yes
Set Front Panel Button Enable	Chassis	0Ah	O	No
Set Power Cycle Interval	Chassis	0Bh	O	Yes
Get POH Counter	Chassis	0Fh	O	Yes

Table 5-5. Event Commands

Command	NetFn	CMD	O/M	Supported
Set Event Receiver	S/E	00h	O	Yes
Get Event Receiver	S/E	01h	O	Yes
Platform Event	S/E	02h	M	Yes

Table 5-6. SEL Commands

Command	NetFn	CMD	O/M	Supported
Get SEL Info	Storage	40h	M	Yes
Get SEL Allocation Info	Storage	41h	O	Yes
Reserve SEL	Storage	42h	O	Yes
Get SEL Entry	Storage	43h	M	Yes
Add SEL Entry	Storage	44h	M	Yes
Partial Add SEL Entry	Storage	45h	O	No
Delete SEL Entry	Storage	46h	O	Yes
Clear SEL	Storage	47h	M	Yes
Get SEL Time	Storage	48h	M	Yes
Set SEL Time	Storage	49h	M	Yes

Get Auxiliary Log Status	Storage	5Ah	O	No
Set Auxiliary Log Status	Storage	5Bh	O	No
Get SEL Time UTC Offset	Storage	5Ch	O	Yes
Set SEL Time UTC Offset	Storage	5Dh	O	Yes

NOTE: Support for Partial Add SEL is not required when Add SEL is supported.

Table 5-7. SDR Repository Commands

Command	NetFn	CMD	O/M	Supported
Get SDR Repository Info	Storage	20h	M	Yes
Get SDR Repository Allocation Info	Storage	21h	O	Yes
Reserve SDR Repository	Storage	22h	M	Yes
Get SDR	Storage	23h	M	Yes
Add SDR	Storage	24h	M	Yes
Partial ADD SDR	Storage	25h	O	Yes
Delete SDR	Storage	26h	O	No
Clear SDR Repository	Storage	27h	M	Yes
Get SDR Repository Time	Storage	28h	O	Yes
Set SDR Repository Time	Storage	29h	O	No
Enter SDR Repository Update Mode	Storage	2Ah	O	Yes
Exit SDR Repository Update Mode	Storage	2Bh	O	Yes
Run Initialization Agent	Storage	2Ch	O	Yes

Table 5-8. FRU Inventory Device Commands

Command	NetFn	CMD	O/M	Supported
Get FRU Inventory Area Info	Storage	10h	M	Yes
Read FRU Inventory Data	Storage	11h	M	Yes

Write FRU Inventory Data	Storage	12h	M	Yes

Table 5-9. Sensory Device Commands

Command	NetFn	CMD	O/M	Supported
Get Device SDR Info	S/E	20h	M	No
Get Device SDR	S/E	21h	M	No
Reserve Device SDR Repository	S/E	22h	M	No
Get Sensor Reading Factors	S/E	23h	M	Yes
Set Sensor Hysteresis	S/E	24h	M	Yes
Get Sensor Hysteresis	S/E	25h	M	Yes
Set Sensor Threshold	S/E	26h	M	Yes
Get Sensor Threshold	S/E	27h	M	Yes
Set Sensor Event Enable	S/E	28h	M	Yes
Get Sensor Event Enable	S/E	29h	M	Yes
Re-arm Sensor Events	S/E	2Ah	M	No
Get Sensor Event Status	S/E	2Bh	M	No
Get Sensor Reading	S/E	2Ch	M	Yes
Set Sensor Type	S/E	2Dh	M	Yes
Get Sensor Type	S/E	2Eh	M	No
Set Sensor Reading and Event Status	S/E	2Fh	O	No
Set Sensor Reading and Event Status (**Note:** ONLY FOR FAN DEVICES.)	S/E	30h	O	Yes

Table 5-10. LAN Commands

Command	NetFn	CMD	O/M	Supported
Set LAN Configuration Parameters (**Note:** Parameter 9 and 25 are not supported.)	Transport	01h	M	Yes
Get LAN Configuration Parameters (**Note:** Parameter 9 and 25 are not supported.)	Transport	02h	M	Yes
Suspend BMC ARP	Transport	03h	O	Yes
Get IP/UDP/RMCP Statistics	Transport	04h	O	No

Table 5-11. PEF/PET Alerting Commands

Command	NetFn	CMD	O/M	Supported
Get PEF Capabilities	S/E	10h	M	Yes
Arm PEF Postpone Timer	S/E	11h	M	Yes
Set PEF Configuration Parameters	S/E	12h	M	Yes
Get PEF Configuration Parameters	S/E	13h	M	Yes
Set Last Processed Event ID	S/E	14h	M	Yes
Get Last Processed Event ID	S/E	15h	M	Yes
Alert Immediate	S/E	16h	O	Yes
PET Acknowledge	S/E	17h	O	Yes

Table 5-12. SOL Commands

Command	NetFn	CMD	O/M	Supported
SOL Activating	Transport	20h	O	Yes
Set SOL Configuration Parameters	S/E	21h	O	Yes
Set SOL Configuration Parameters	S/E	22h	O	Yes

6

IPMI OEM Command List

Table 6-1. OEM1 Commands (NetFn 30H, 31H)

Command	NetFN	cmd	Format
Reserved Extended Configuration	OEM1	01H	**Request:** **Response:** Byte 1 – completion code Byte 2 - Reservation ID
Get Extended Configuration	OEM1	02H	**Request:** Byte 1 - Reservation ID Byte 2 - Configuration ID Byte 3 - Attribute ID. 00h means read entire configuration data. Byte 4 - Index (used by table object only) Byte 5 - Data Offset – LSB Byte 6 - Data Offset – MSB Byte 7 - Bytes to read. FFh means read entire configuration or attribute. **Response:** Byte 1 – Completion code (01h:no more data) Byte 2 – Configuration ID Byte 3 – Attribute ID Byte 4 – Index (valid only for table object only) Byte 5 – Number of bytes returned, 1-based Byte 6~N – Data **(Please check with table 1-25 Extended Configuration)**

Command	NetFN	cmd	Format
Set Extended Configuration	OEM1	03H	**Request:** Byte 1 - Reservation ID Byte 2 - Configuration ID Byte 3 - Attribute ID. 00h means read entire configuration data. Byte 4 - Index (used by table object only) Byte 5 - Data Offset – LSB Byte 6 - Data Offset – MSB Byte 7 - In progress [7:4] reserved [3:0] in progress 0 – in progress 1 – last configuration data being transferred in this request Byte 8~N – Data to be written. **Response:** Byte 1 – Completion code (01h:no more data) **(Please check with table 1-25 Extended Configuration)**

Command	NetFN	cmd	Format
Restore to defaults	OEM1	04H	**Request:** Byte 1 -Configuration to be restored to defaults: [7:5] 111b= Restore the remaining parameters not included in below lists. 000b= Remaining parameters stay what it is. All other values are reserved [4] 1b= Restore PEFs to defaults [3] 1b= Restore serial configuration parameters to defaults [2] 1b= Restore SOL configuration parameters to defaults [1] 1b= Restore LAN configuration parameters to defaults [0] 1b= Restore user accounts to defaults **Response:** Byte 1 –Completion Code CCh = restore to one or more of the configuration not supported. Byte 2 – Task ID. Use the Task ID to get the restore status. The Task ID is automatically become invalid after 120 seconds when the restore requesting is completed. 00h reserved.

Command	NetFN	cmd	Format
Get Restore Status	OEM1	05H	**Request:** Byte 1 – Task ID Task ID, the value returned by previous call to Restore to Defaults command. **Response:** Byte 1 –Completion Code Byte 2 –Default Restore Status: 00h: Restore in progress 01h: Restore completed
SETSYSTEM GUID	OEM1	B3H	**Request:** Byte 1 ~16 – System GUID **Response:** Byte 1 – completion code

Table 6-2. OEM2 Commands (NetFn 34H, 35h)

Command	NetFN	cmd	Format
set web port number	oem2	02H	**Request:** Byte 1 – Https Port Number(Low Byte) Byte 2 – Https Port Number(High Byte) Byte 3 – Http Port Number(Low Byte) Byte 4 – Http Port Number(High Byte) **Response:** Byte 1 – completion code

get web port number	oem2	03H	**Request:** **Response:** Byte 1 – completion code Byte 2 – Https Port Number(Low Byte) Byte 3 – Https Port Number(High Byte) Byte 4 – Http Port Number(Low Byte) Byte 5 – Http Port Number(High Byte)
get board id	oem2	11H	**Request:** **Response:** Byte 1 – completion code Byte 2 – Board ID 01h ~ 04h
Set asset tag	OEM2	12h	**Request:** Byte 1 - Length Byte 2~11 - Data (Max Set Asset Tag Length - 0x0A) **Response:** Byte 1 - Completion Code Byte 2 - Count Written
Set LAN Source	OEM2	13h	**Request:** Byte1 – LAN Source 00h – Shared NIC 01h – Dedicated NIC **Response:** Byte 1 – completion code Byte 2 – LAN Source Setting

GET LAN SOURCE	OEM2	14h	**Request:** **Response:** Byte 1 – completion code Byte 2 – Current LAN Source 00h – Shared NIC 01h – Dedicated NIC
GET FCB FW VERSION	oem2	16H	**Request:** **Response:** Byte 1 – completion code Byte 2 – FCB Fw Major number Byte 3 – FCB Fw Minor number
SET FAN CONTROL	oem2	61H	**Request:** Byte 1 – Fan Control Setting [7] – Enabled/Disabled FAN Control 0: Disabled(Default) 1: Enabled [6:0] – Duty Cycle Setting. The rage is from 0 to 100, others are reserved. **Response:** Byte 1 – completion code
GET FAN CONTROL	oem2	62H	**Request:** **Response:** Byte 1 – completion code Byte 2 – Fan Control Setting [7] – Enabled/Disabled FAN Control 0: Disabled(Default) 1: Enabled [6:0] – Duty Cycle Setting. The rage is from 0 to 100, others are reserved.

SET FSC TABLE	oem2	63H	**Request:** Byte 1 – FSC Table Setting Byte 1 – completion code Byte 2 – FSC Table Setting [7] – Enabled/Disabled FAN Table 0h: Disabled (Default) 1h: Enabled [6:0] – Fan Table Setting(0-based) 80h: 1st FSC fan table (default: 13800RPM) 81h: 2nd FSC fan table (FACEBOOK) 82h: 3rd FSC fan table (Oscillation) 83h: 4th FSC fan table (Western Geco) 84h: 5th FSC fan table (Loki) **Response:** Byte 1 – completion code
GET FSC TABLE	oem2	64H	**Request:** **Response:** Byte 1 – completion code Byte 2 – FSC Table Setting [7] – Enabled/Disabled FAN Table 0h: Disabled (Default) 1h: Enabled [6:0] – Fan Table Setting(0-based) 80h: 1st FSC fan table (default: 138RPM) 81h: 2nd FSC fan table (FACEBOOK) 82h: 3rd FSC fan table (Oscillation) 83h: 4th FSC fan table (Western Geco) 84h: 5th FSC fan table (Loki)

GET FCB SKU INFO	oem2	6aH	**Request:** **Response:** Byte 1 – completion code Byte 2 – FCB SKU Information
GET FCB POWER THROTTLING STATUS	oem2	6bH	**Request:** **Response:** Byte 1 – completion code Byte 2 – FCB Power Throttling status
OEM GET PIC MODEL	oem2	70H	**Request:** **Response:** Byte 1 – completion code Byte 2 – PIC model 10h - PIC16 12h – PIC18
Get PSU Mismatch and type	OEM2	B3H	**Request:** **Response:** Byte 1 – completion code Byte 2 – PSU mismatch 00h – Mismatch 01h – Match Byte 3 – PSU type [7:4] PSU2 type 01h – 470 Watt 02h – 750 Watt 03h – 1100 Watt 04h – 1400 Watt [3:0] PSU1 type 01h – 470 Watt 02h – 750 Watt 03h – 1100 Watt 04h – 1400 Watt

Table 6-3. OEM3 Commands (NetFn 2EH, 2Fh)

Command	NetFN	cmd	Format
OemGetBMCSKU	Oem3	75H	**Request:** **Response:** Byte 1 – completion code Byte 2 - BMC SKU 00h AST2050 01h AST1100

Extended Configurations

Table 6-4. Extended configurations

Extended Configurations				
All strings are in P-String format.				
Configuration ID = 02h, NIC				
Attribute	**ID**	**Size**	**Description**	
NicSelection	1	1	Specifies the current mode of operation for the BMC network interface. 0: Shared NIC (default) 1: Dedicated NIC	R/W
SharedNICSelection	2	1	This parameter is only valid when Attribute ID 1 NICSelection parameter is set to 0h as Shared NIC. 0h: Reserved (Recommend to set to 0h when NICSelection is set to Dedicated NIC.) 1h: NIC-1 (default) 2h: NIC-2 3h: NIC-3 4h: NIC-4 **Note:** According to DCS I/O guide line, RJ45 connectors should be labeled starting from NIC-1. It also requires that Dedicated BMC NIC should always be the largest number (last port number). Therefore this Attribute ID parameter only requires to support the available Shared NIC numbers according to the labeled numbers, regardless of the NC-SI topology (i.e. Single Channel Dual Package	R/W

			or Dual Channel Single Package). When user attempts to set to a NIC value that is not supported on the platform, a completion code CCh should be returned to indicate an invalid data.	
Configuration ID = 03h, SOL				
Attribute	**ID**	**Size**	**Description**	
SOL Idle Timeout	1	2	byte1:2 - Define the inactivity timeout in minutes, 1-based, LSByte first. This parameter only applies to the IPMI over LAN session with SOL payload activated. 0h= session does not timeout and close due to inactivity. Default = 01h	R/W
Telnet/SSH Redirect Enable	2	1	0: Disabled (default) 1: Enabled	R/W
Configuration ID = 04h, Security				
Attribute	**ID**	**Size**	**Description**	
Service Disabled	1	1	Disable or enable services. This attribute takes precedence over the individual feature enabled/disabled. Once one service has been disabled, the BMC must not allow user to enable the corresponding feature and D5h completion code must be returned. For example, if HTTP/HTTPS is disabled, user must not abe able to enable the Web Server through Web Server	R/W

			Configuration (Configuration ID 0Ch). In other words, Web can only be disabled or enabled when HTTP/HTTPS is enabled. [0] - all services except IPMI are disabled. This bit takes precedence over other bits. Default is 0. [1] - KVM/Virtual Storage, enabled by default. [2] - HTTP/HTTPS, enabled by default. [3] - SSH/Telnet, disabled by default.	
Max Authentication Failures	2	1	Specifies the maximum number of allowed authentication failures. Setting this value to 0 will disable the lockout feature. Whenever this setting is modified, the number of authentication failure of each enabled user must be reset to 0. When an account Is locked out, the IPMI Messaging must be disabled on the LAN channel. See Get User Access command. Default = 00h (disable Lockout feature)	R/W
Lockout Window	3	2	Specifies the window, in second, during which if the consecutive maximum number of authentication failures is reached, the account should be disabled. Setting this value to 0 will disable the lockout feature.	R/W

			Whenever this setting is modified, the number of authentication failure of each enabled user must be reset to 0. Default setting is 180 seconds.		
Lockout Time	4	2	Specifies the time period an account should be disabled if the maximum number of authentication failures is reached. The unit is seconds. Setting this value to 0 will disable the lockout feature. Whenever this setting is modified, the number of authentication failures of each enabled user must be reset to 0. Default value is 3600 (1 hour).	R/W	

Configuration ID = 05h, Account Status

Attribute	ID	Size	Description		
Number of User	1	1	Number of users created, including enabled and disabled users. The count Does not include USER ID1.	R	
Number of Enabled User	2	1	Number of enabled users.	R	
User Name	3	1..17	Specify the user name in P-String format. Indexed by user ID.	R	I

Account Status	4	1	Status of the account. This is the supplement to the byte 3 of response data of *Get User Access* command. Indexed by user ID. 00h = status is unspecified 01h = user ID is enabled via *Set User Password* 02h = user ID is disabled via *Set User Password* 03h = user ID is lockout	R	I

Configuration ID = 06h, DNS

Attribute	ID	Size	Description	
DNS Dhcp Enable	1	1	Specifies that the DNS server IP addresses should be assigned from the DHCP server. 0: FALSE (default) 1: TRUE.	R/W
DNS Server1	2	4	Specifies the IP address for DNS server 1. This parameter is read-only if **DNS Dhcp Enable** and **DHCP** are enabled.	R/W
DNS Server2	3	4	Specifies the IP address for DNS server 2. This parameter is read-only if **DNS Dhcp Enable** and **DHCP** are enabled.	R/W
DNS Register BMC	4	1	Enables registering the BMC host name on the DNS server 0: FALSE (default) 1: TRUE.	R/W
DNS BMC Host Name	5	1..64	Specifies the DNS BMC host name. This parameter is read-only if **DNS Register BMC** is set to TRUE. At least one	R/W

			character must be alphabetic. The default name is bmc-*service_tag*, where *service_tag* is the service tag number of the Dell server. For example: bmc-XG3487A.	
DNS Domain Name Dhcp Enable	6	1	Specifies that the DNS domain name should be assigned from the DHCP server. 0: FALSE (default) 1: TRUE.	R/W
DNS Domain Name	7	1.256	The DNS domain name string. This parameter is read-only if **DNS Domain Name Dhcp Enable** is set to TRUE. Characters are restricted to alphanumeric, '-' and '.'. Default is “”	R/W

Configuration ID = 0Ch, WEB Server Configuration

Attribute	ID	Size	Description	
Web Server Enabled	1	1	Disable or enable the BMC Web server. 0: FALSE 1: TRUE (default)	R/W
Max Web Sessions	2	1	The maximum number of simultaneous sessions allowed for this system. This field is READ-ONLY.	R
Active Web Sessions	3	1	The number of current session for GUI on the system. This field is READ-ONLY.	R
Web Server Timeout	4	4	The WEB communication idle timeout, in seconds.	R/W

			Timeout range is 60 to 1920 seconds. A 0 specifies disabling the timeout feature. The default is 300.	
HTTP Port Num	5	2	Specifies the port number to use for HTTP communication with the BMC. Default is 80.	R/W
HTTPS Port Num	6	2	Specifies the port number to use for HTTPS communication with the BMC. Default is 443.	R/W

Configuration ID = 0Eh, Firmware Log, indexed object

Attribute	ID	Size	Description	
Entity	1	1	Refer to Firmware Information configuration.	R
Firmware Version	2	1..16	Refer to Firmware Information configuration.	R
Branch	3	1..16	Refer to Firmware Information configuration.	R
Build Information	4	1..16	Refer to Firmware Information configuration.	R
Update Date / Time	5	3	Number of minutes from 0:00 hrs 1/1/08. LSbyte first (little endian)	R

Configuration ID = 0Fh, Firmware Information, indexed object

Attribute	ID	Size	Description	
Name	1	1..16	Specifies BMC model name, such as AST2050.	R
Description	2	1..256	A text description of the type controller.	R

Entity	3	1	Specifies the physical controller the image is associated with. 0: BMC 1: SYSTEM (BIOS) 2: PDB 3: FCB	R
Product Info	4	1..64	A text string that identifies the product. "Dell DCS Remote Management Controller" (default)	R
Firmware Version	5	1..16	A string containing the BMC firmware version. The firmware version is reading from IPMI Get Device ID command. The format of BMC FW Version string is "<major>.<minor>", where major is one character and minor is two characters.	R
Branch	6	1..16	A string containing the firmware branch information.	R
Build Information	7	1..16	A string containing the firmware build number information. The string format is YYMMDD.	R
User Default Setting	8	1	This attribute enables user to customize various BMC settings and store as user default. It also allows user to erase current settings and restore back to previously set user default settings. User default settings include all write-able settings in Extended Configuration Parameters, IPMI User Account	W

			Settings, and IPMI LAN Configuration Parameters. 0h – Set as User Default 1h – Restore User Default	

Configuration ID = 10h, Firmware Update

Attribute	ID	Size	Description	
Remote Update Enable	1	1	Allow firmware update via TFTP server.	R/W
Protocol	2	1	Specified supported protocols. [7:3] - reserved [2] - HTTP [1] - FTP [0] - TFTP	R
URI	3	1..256	The URI of the image file.	R/W
Connection Retry	4	1	Specify the number of retries for connecting to TFTP server. A zero value means the BMC does not attempt to retry connect to TFTP server.	R/W
Retry Interval	5	1	Define the retry interval in 5 seconds increaments.	R/W
Delay Time	6	1	Define the delay time for connecting to TFTP server. The time is specified in seconds. 00h: BMC connects to TFTP server immediately. FFh: random between 5 and 10 seconds.	R/W

Configuration ID = 11h, Power Management				
Attribute	**ID**	**Size**	**Description**	
Power Management Enable	1	1	Specify the use of power management method. Bit 7: Enable DPNM power management 1b = enable DPNM 0b = disable DPNM Bit 6:0: reserved	R/W
Power Staggering AC Recovery	2	1	This parameter is only effective if the Power Policy is not set to always off. 0x00 : Immediate Power On (No Delay) : Default 0x01 : Auto (Random), the auto generated delay time must be in the range of **Minimum Power On Delay** and **Maximum Power On Delay**. 0x02 : User Defined, the user defined delay time must be in the range of **Minimum Power On Delay** and **Maximum Power On Delay**.	R/W
Power On Delay	3	2	Defines the time to delay power on the system after AC recovered.	R/W
Minimum Power On Delay	4	2	Specifies the minimum power on delay time when AC is restored. This should not be less than the time BMC startup time.	R
Maximum Power On Delay	5	2	Specifies the maximum power on delay time when AC is restored. The number must large than **Minimum Power On Delay**.	R/W

Appendix

SSH/Telnet Enable and Disable

1 Reserved Extended Configuration (NetFn: 30H CMD:01H)

2 Set/Get Extended Configuration(NetFn: 30H CMD:03H/02H)

Configuration ID = 04h, Security				
Attribute	**ID**	**Size**	**Description**	
Service Disabled	1	1	Disables or enables services. This attribute takes precedence over the individual feature enabled/disabled. Once one service has been disabled, the BMC must not allow users to enable the corresponding feature and D5h completion code must be returned. For example, if HTTP/HTTPS is disabled, user must not be able to enable the Web Server through Web Server Configuration (Configuration ID 0Ch). In other words, Web can only be disabled or enabled when HTTP/HTTPS is enabled. [0] - all services except IPMI are disabled. This bit takes precedence over other bits. Default is 0. [1] - KVM/Virtual Storage, enabled by default. [2] - HTTP/HTTPS, enabled by default. [3] - SSH/Telnet, disabled by default.	R/W

Example:

Get SSH/Telnet enable status:

1 Reserved Extended Configuration

ipmitool raw 0x30 0x01

Response: 0x01 (Reservation ID)

2 Get Extended Configuration

ipmitool raw 0x30 0x02 0x01 0x04 0x01 0x00 0x00 0x00 0xFF

Response: 0x04 0x01 0x00 0x01 0x08 (SSH/Telnet disabled)

Set SSH/Telnet Enable:

1 Reserved Extended Configuration

ipmitool raw 0x30 0x01

Response: 0x02 (Reservation ID)

2 Enable SSH/Telnet

ipmitool raw 0x30 0x03 0x02 0x04 0x01 0x00 0x00 0x00 0x01 0x00 (set SSH/Telnet enable)

Response: 0x01

SSH/Telnet Redirect Enable and Disable

1 Reserved Extended Configuration (NetFn: 30H CMD:01H)

2 Set/Get Extended Configuration(NetFn: 30H CMD:03H/02H)

Configuration ID = 03h, SOL

Attribute	ID	Size	Description	
Telnet/SSH Redirect Enable	2	1	0: Disabled (default) 1: Enabled	R/W

Example:

Get SSH/Telnet Redirect enable status:

1 Reserved Extended Configuration

ipmitool raw 0x30 0x01

Response: 0x01 (Reservation ID)

2 Get Extended Configuration

Ipmitool raw 0x30 0x02 0x01 0x03 0x02 0x00 0x00 0x00 0xFF

Response: 0x03 0x02 0x00 0x01 0x00 (SSH/Telnet SOL redirect disabled)

Set SSH/Telnet SOL Redirect enable:

1 Reserved Extended Configuration

ipmitool raw 0x30 0x01

Response: 0x02 (Reservation ID)

2 Enable SSH/Telnet SOL redirect.

ipmitool raw 0x30 0x03 0x02 0x03 0x02 0x00 0x00 0x00 0x01 0x01 (set 1 to enable)

Response: 0x01

VLAN ID

User can use LAN configuration command parameter 14H to Set or Get VLAN ID. More VLAN information, please refer to "IPMI SPEC v2.0 errata revision 4".

Commands	NetFn	CMD	O/M	Supported
Set LAN Configuration Parameters (**Note:** Parameter 9 and 25 are not supported.)	Transport	01h	M	Yes
Get LAN Configuration Parameters (**Note:** Parameter 9 and 25 are not supported.)	Transport	02h	M	Yes

LAN configuration Parameter 14H:

Parameter	#	Parameter Data
802.1q VLAN ID (12-bit)	14H	data 1 [7:0] - Least significant 8-bits of the VLAN ID. 00h if VLAN ID not used. data 2 [7] - VLAN ID enable. 0b = disabled, 1b = enabled. If enabled, the BMC will only accept packets for this channel if they have 802.1q fields and their

	VLAN ID matches the VLAN ID value given in this parameter. [6:4] - reserved [3:0] - most significant four bits of the VLAN ID

Example:

1. Get LAN Configuration Parameter command:
   ipmitool raw 0xC0 0x02 0x01 0x14 0x00 0x00
   Response: 0x00 0x11 0x01 0x80 (VLAN Enable and VLAN ID: 1)
2. Set LAN Configuration Parameter command:
   ipmitool raw 0xC0 0x01 0x01 0x14 0x01 0x80
   Response: 0x00

BMC/BIOS Version Info

BMC Version Info

Get Device ID command can get BMC version Info in response date byte4, 5. More detail about this command please refers to "IPMI SPEC v2.0 errata revision 4" chapter 20.1.

Response Date	Data field
Byte 1	Completion Code
Byte 2	Device ID.
Byte 3	Device Revision [7] 1 = device provides Device SDRs 0 = device does not provide Device SDRs [6:4] reserved. Return as 0. [3:0] Device Revision, binary encoded.

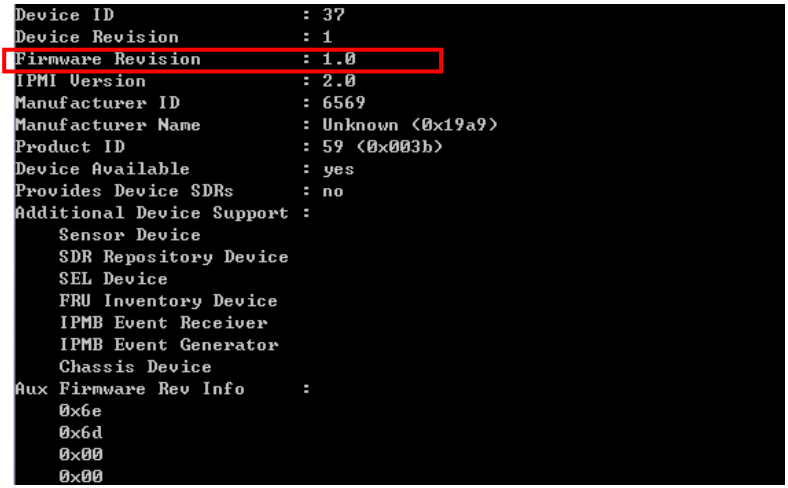
Byte 4	Firmware Revision 1 [7] Device available: 0=normal operation, 1= device firmware, SDR Repository update or self-initialization in progress. [Firmware / SDR Repository updates can be differentiated by issuing a Get SDR command and checking the completion code.] [6:0] Major Firmware Revision, binary encoded.
Byte 5	Firmware Revision 2: Minor Firmware Revision. BCD encoded.
…	…

Example:

Get Device ID command:

Ipmitool raw 0x06 0x01

Response: 0x00 0x25 0x01 **0x01 0x00** 0x02 0xbf 0xa9 0x19 0x00 0x3b 0x00 0x6e 0x6d 0x00 0x00



BIOS version Info

The BIOS enables the system interface to the BMC and logs this event to the BMC early in POST.

User can find the BIOS version in event record byte 15-16 as following table:

POST START Event

Byte	Item	Data
1-2	Record ID	-
3	Record Type	-
4-7	Timestamp	-
8-9	Generator ID	0x01 (BIOS)
10	Event Message Format Version	0x04 (IPMI 1.5)
11	Sensor Type	0xC1 (OEM Reserved)
12	Sensor Number	0x81 (BIOS Start)
13	Event Direction/Event Type	0x70 (OEM)
14	Event Data 1	0xA0
15	Event Data 2	0x01 (BIOS Major Version)
16	Event Data 3	0x01 (BIOS Minor Version)

Example:

1 Issue SEL list command to find post start Entity ID is 9

2 ipmitool sel get 9

```
SEL Record ID          : 0009
 Record Type           : 02
 Timestamp             : 01/13/2011 21:26:28
 Generator ID          : 0001
 EvM Revision          : 04
 Sensor Type           : Unknown
 Sensor Number         : 81
 Event Type            : OEM
 Event Direction       : Assertion Event
 Event Data            : a00101
 Description           :
```

BIOS version is V 1.1